MOISÉS NEVES CAMÊLO

WARDRIVING:
Rastreando e mapeando redes sem fios inseguras

Monografia apresentada ao curso de Pós-graduação Lato Sensu em Segurança da Informação, na Faculdade de Tecnologia IBRATEC de João Pessoa - IBRATEC, como requisito parcial para obtenção do título de especialista.

Orientador: Prof. M.S.c. Márcio Luiz Machado Nogueira

João Pessoa – PB
2009

MOISÉS NEVES CAMÊLO

WARDRIVING:
Rastreando e mapeando redes sem fios inseguras

Trabalho de Conclusão de Curso, apresentado a IBRATEC – Faculdade de Tecnologia João Pessoa, como requisito parcial para obtenção do título de Especialista em Segurança da Informação.

Aprovado em de de 2009

BANCA EXAMINADORA

Prof. M.S.c. Márcio Luiz Machado Nogueira
Orientador

Prof.
Examinador(a)

Prof.
Examinador(a)

DEDICATÓRIA

Dedico este trabalho a Deus, por te me dado o dom da vida, e por sempre estar comigo guiando os meus caminhos, levando-me a fazer o que for de melhor e correto. E por ter me presenteado com muita saúde, paz de espírito, uma família espetacular e muitos amigos.

A minha mãe pelo apoio, não só na vida profissional, mas em todos os momentos da minha vida. A todos os meus familiares, por estarem sempre ao meu lado, apoiando-me e incentivando-me nos momentos mais difíceis.

A minha eterna namorada, Raquel, por me dar o apoio necessário com, muito amor, carinho, para que eu consiga alcançar todos os nossos sonhos com muito esforço e garra. E pela paciência e compreensão em todos os momentos de ausência, em que não me fiz presente por estar dedicado a esta especialização.

AGRADECIMENTOS

Ao meu orientador, Professor M.S.c. Márcio Luiz Machado Nogueira, pelo seu auxílio, compreensão e dedicação.

Aos professores que me passaram com muito profissionalismo e sapiência os seus mais valiosos conhecimentos e experiências.

Aos meus colegas de turma, com quem muito aprendi, troquei experiências, e desfrutei de momentos que ficarão guardados na minha memória, como as sessões de estudo na UFPB e os almoços de sábado.

A minha namorada, Raquel, pelo grande auxílio e disponibilidade como motorista de wardriving, pois a sua contribuição foi essencial na pesquisa de campo.

CAMÊLO, Moisés Neves. **WARDRIVING:** rastreando e mapeando redes sem fio inseguras: 2008 – nºp74. Monografia (Especialização em Segurança da Informação) IBRATEC – Faculdade de Tecnologia IBRATEC de João Pessoa.

RESUMO

As redes sem fio estão em larga expansão, por oferecerem expressivas vantagens, como a mobilidade e a praticidade. Isto porque elas proporcionam liberdade para que as pessoas se locomovam e mesmo assim permaneçam conectadas e, ainda, viabiliza a troca de dados em locais onde passar o cabeamento de fios já não é mais possível, a exemplo do que ocorre em prédios tombados pelo patrimônio histórico. Ao lado desses benefícios, surgem, entretanto, questões preocupantes. A imprensa, entre os anos de 2002 a 2004, relatou diversos casos relacionados à segurança neste tipo de redes, como os publicados pela Info exame que revelaram em São Paulo sérios problemas nas redes encontradas, principalmente, no protocolo WEP de segurança *wireless*, que demonstrou grande fragilidade. Em 2009, após a consagração do atual padrão de criptografia internacional, AES, embutido dentro do novo protocolo de segurança de rede sem fio, WPA, casos de violação em redes sem fio tornaram-se raros. Ficam, então, as seguintes indagações no ar: As redes sem fio estão agora totalmente seguras? As invasões estão mais sofisticadas e silenciosas?As atividades de explorar as vulnerabilidades das redes *wireless* não são tão simples? Neste estudo, que serve como base para a monografia de conclusão do curso de especialização em Segurança da Informação, foi feita uma pesquisa de campo com o objetivo mapear as redes sem fio de alguns bairros da cidade de João Pessoa e identificar o grau de segurança em que elas se encontram. Nesta pesquisa, foram analisados os dados coletados, verificando-se o nível de preocupação dos administradores de redes sem fio desta localidade, em especial no quesito segurança da informação. Este trabalho foi realizado com o uso do ato de *wardrinving*, que é a prática de dirigir pelas ruas buscando por redes sem fio inseguras

Palavras-chaves: Redes sem fio, IEEE 802.11, WEP, WPA, *Wardriving* e Wi-Fi.

CAMÊLO, Moisés Neves. **WARDRIVING:** rastreando e mapeando redes sem fio inseguras: 2008 – nºp.74 Monografia (Especialização em Segurança da Informação) IBRATEC – Faculdade de Tecnologia IBRATEC de João Pessoa.

ABSTRACT

The wireless networks are to a large expansion, by providing significant benefits such as mobility and convenience. This is because they provide freedom for people to move and still remain connected, and also enables the exchange of data in places where the wires pass the cabling is no longer possible, as occurs in buildings fallen by historical. Beside these benefits, appear, however, concerns. The press, between the years 2002 to 2004, reported several cases related to security in such networks, such as those published by Info examination that revealed serious problems in Sao Paulo in networks found mainly in WEP wireless security, which has very fragile. In 2009, after the consecration of the current international encryption standard, AES, embedded within the new security protocol for wireless network, WPA cases of rape in wireless networks have become rare. Are then the following questions in the air: The wireless networks are now completely safe? The intrusions are more sophisticated and quiet? Activities to exploit the vulnerabilities of wireless networks are not so simple? In this study, which serves as the basis for the conclusion of the monograph of the specialization course in Information Security, was a field research with the objective map the wireless networks in some neighborhoods of the city of João Pessoa and identify the degree of safety in they are. In this study, we analyzed the data collected, with the level of concern for administrators of wireless networks in this town, especially in the aspect of information security. This work was carried out using the act of wardrinving, which is the practice of driving the streets looking for insecure wireless networks.

Keywords: networks wireless, IEEE 802.11, WEP, WPA, and WiFi wardriving

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AES	*Advanced Encryption Standard*
AMD	*Advanced Micro Devices*
APs	*Access Point*
CRC-32	*Cyclical Redundancy Check*
DoS	*Deny of Service*
EAP	*Extensible Authentication Protocol*
EAP – TLS	EAP – *Transport Layer Security*
EAP – TTLS	EAP – *Tunneled Transport Layer Security*
EUA	Estados Unidos da América
HP	*Hewlett-Packard*
IEEE	*Institute of Electrical and Eletronics Engineers*
IDS	*Intrusion Detection System*
IVs	*Initalization Vector*
LAN	*Local Area Network*
LEAP	*Lightweight Extensible Authentication Protocol*
Mbps	Mega bits por segundo
PEAP	*Protected Extensible Authentication Protocol*
PSK	*Pre-Shared Key*
RADIUS	*Remote Authentication Dial In User Server*
RC4	Algoritmo de criptografia de fluxo
RNP	Rede Nacional de Pesquisa
SSID	*Service Set Identifier*
TKI	*Temporal Key Integrity*
TKPI	*Temporal Key Integrity Protocol*
USB	*Universal Serial Bus*
VOIP	Voz Sobre IP

WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity* – Fidelidade Sem Fio
WLAN	*Wireless Local Area Network*
WPA	*Wi-Fi Protected Access*

SUMÁRIO

INTRODUÇÃO

As redes do padrão 802.11 hoje são uma realidade no nosso cotidiano, devido a sua praticidade e mobilidade em ambientes domésticos, coorporativos e públicos.

Essa tecnologia, que usa o ar como meio de comunicação, apresenta uma série de vantagens sobre a de cabos. A revista Info exame fez referência a essas vantagens em várias reportagens, registrando na edição de novembro de 2003, que

> "As redes locais wireless estão pegando para valer. O espaguete de fios começa a ser superado. Não se trata apenas de colocar os fios para escanteio, é claro. Com a mobilidade das redes locais wireless, o poder da computação vai para onde quiser, no ato, com o máximo de flexibilidade". (Fortes, 2003, p.60)

Além da flexibilidade, essa tecnologia destaca-se pela, escalabilidade, mobilidade e usabilidade, como pontos marcantes. Mas é importante considerar algumas ressalvas, uma vez que a falta de um planejamento para uma rede segura pode causar grandes riscos ou prejuízos, pois a maioria das vulnerabilidades em um *wireless* (Sem fio) é causada por uma má configuração dos equipamentos ou falta de conhecimento da prática de segurança adotada, facilitando então o mau uso por parte de usuários maliciosos. E como hoje a informação é a moeda da vez, a segurança deve prevalecer para proteger esse patrimônio de valor incalculável.

Reforçando o que foi mencionado anteriormente, vale lembrar que, a norma Iso 17799 diz que a implementação da segurança da informação é conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software e hardware.* Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e a segurança da organização sejam atendidos, segundo essa norma convém que isto seja feito em conjunto com outros processos de gestão do negócio. (ISO, 2005, p. 9)

O objetivo do presente estudo é mapear as redes sem fio de alguns bairros residenciais e comerciais de João Pessoa, com a prática de Wardriving, identificando as redes abertas, fechadas com o padrão WEP ou WPA. A partir desse mapeamento, pode-se verificar quais os problemas que uma rede *wireless* mal

configurada pode acarretar, e constatar-se um percentual se os administradores de redes sem fio estão se preocupando com a segurança da informação, tendo como base os seus três pilares básicos desta: integridade, confidencialidade e disponibilidade.

Ressalte-se, que este estudo e mapeamento não têm o objetivo de expor os nomes das redes vulneráveis, e nem o de expor as suas informações, pois o seu intuito é servir como base de comparação de dados coletados, em outras capitais ou nesta mesma, verificando então a preocupação dos administradores de redes sem fio com relação à segurança da informação.

O Capítulo 1 constitui uma sumária fundamentação teórica, apresentando uma explanação das diversas tecnologias sobre redes *wireless*. Analisando desde os seus fundamentos, padrões e modelos de redes sem fio.

O Capítulo 2 reporta à história da evolução das ameaças às redes sem fio.

O Capítulo 3 faz uma pequena retrospectiva dos principais incidentes reportados pela imprensa, causados pela falha de segurança nas redes sem fio.

O Capítulo 4 descreve os mecanismos de segurança das redes sem fio: o padrão WEP e o seu tipo de criptografia com as suas fragilidades; o WPA com uma criptografia mais forte, que veio para o melhoramento do WEP; e o padrão IEEE 802.1X, que é relativo ao nível de segurança de portas.

O Capítulo 5 descreve as ameaças às redes *wireless* e suas fragilidades, analisando as principais ferramentas utilizadas, seu funcionamento e técnicas de invasão.

O Capítulo 6 enfoca do desenvolvimento desta monografia, com os procedimentos utilizados, na pesquisa e a metodologia utilizada.

E por fim, apresenta-se a conclusão desse estudo, registrando os resultados obtidos na pesquisa.

1 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, abordar-se-ão diversas tecnologias envolvendo o padrão IEEE 802.11.

1.1 Fundamentos de Redes Sem Fio

A WLAN é uma rede que não utiliza fios para se interligar, isto é, ela utiliza o próprio ar como meio de transmissão de informações. (RNP, 2007, p.235)

Quase na mesma época em que surgiram os notebooks, muitas pessoas sonhavam com o dia em que entrariam em um ambiente corporativo ou domiciliar e magicamente seu notebook se conectaria a internet ou a sua rede local. Nesse momento, diversos grupos começaram a trabalhar para descobrir maneiras de alcançar esse objetivo. A abordagem mais prática foi equipar o escritório e os notebooks com transmissores e receptores de rádio de ondas curtas para permitir a comunicação entre eles. Esse trabalho levou rapidamente à comercialização de LANs sem fio (WLANs).

Mas para que essa comercialização não perdesse um padrão, a IEEE (Institute of Electrical and Eletronics Engineers) formou um grupo de trabalho com objetivo de definir padrões de uso em redes sem fio, que foi chamado de 802.11 e suas variações das suas extensões, como: 8012.11a, 802.11b, 802.11g. (RUFINO, 2007, p.25)

1.2 Padrões Atuais

Com o passar do tempo, o padrão 802.11 recebeu algumas extensões com características técnicas especificas, citadas a seguir:

- 802.11a: destinado ao alto desempenho com taxa máxima de 54 Mbps por canal, usando banda de rádio de 5GHz. (RNP, 2007, p.236)

- 802.11b: atinge 11Mbps por canal, usando uma banda de rádio de 2.4GHz. (RNP, 2007, p.236)
- 802.11c: destinado para definir procedimentos de operações de ponte entre pontos de acesso. (RNP, 2007, p.236)
- 802.11d: destinado a uso geral, para promover o uso do padrão *wireless* em países onde os requisitos para o uso da banda são diferentes dos EUA. Esse padrão está em discussão. (RNP, 2007, p.236)
- 802.11e: destinado à qualidade de serviço, com características de diferenciação de tráfego, para o uso futuro em áudio e vídeo, por exemplo. É aplicável aos padrões 802.11a, 802.11b e 802.11g. (RNP, 2007, p.236)
- 802.11f: trata-se da interoperabilidade entre produtos de diferentes fabricantes. (RNP, 2007, p.236)
- 802.11g: trata do desempenho e da compatibilidade com o padrão 802.11b e possui velocidade similar ao padrão 802.11a, de 511a, de 54Mbps. E usam as bandas de 2.4GHz e 5GHz, com três canais de rádio disponíveis. (RNP, 2007, p.236)
- 802.11h: trata da operabilidade na Europa, atuando na banda de 5GHz e do gerenciamento de espectro e controle de energia. (RNP, 2007, p.236)
- 802.11i: trata de mecanismos de segurança e autenticação. (RNP, 2007, p.236)
- 802.11j: trata da operação nas novas bandas de 4.9GHz e 5GHz disponíveis no Japão. (RNP, 2007, p.236)
- 802.11n: trata-se de uma rede com taxa de transferência acima de 200Mbps e banda de 2.4GHz e 5GHz. (RNP, 2007, p.236)
- 802.1X: é um padrão que define um *framework* para autenticação baseada em portas e distribuição de chaves para LANs sem fio e com fio. (RNP, 2007, p.236)

1.3 Modelos de redes sem fio

As redes w*ireless* têm sido uma excelente alternativa para as tradicionais redes cabeadas, pois agrega mobilidade, flexibilidade e principalmente um menor investimento em infraestrutura (cabos, conectores, etc) quando comparada a soluções cabeadas. A facilidade e menor tempo de instalação também são benefícios proporcionados pela tecnologia, que pode estar presente tanto em ambientes internos (*Indoor*), como residências, escritórios e hotéis, como em ambientes externos (*Outdoor*), como provedores de acesso a rádio e *links* ponto-a-ponto entre matriz e filiais. Nos itens posteriores 1.3.1 e 1.3.2 serão estudados os conceitos em nível de conhecimento para distinguir as redes *indoor* e *outdoor.*

1.3.1 Indoor

A propagação dos sinais em recintos fechados é dominada pelos mesmos mecanismos das áreas abertas *(outdoor)*, que são a reflexão, a refração e a dispersão, mas sem dúvida as condições variam mais em função de diferentes fatores físicos, que envolvem tanto o desenho dos edifícios como os materiais que são usados para construí-los. (SANCHES, 2007, p.157)

Os sinais em ambientes fechados parecem mais fáceis de serem transportados que os sinais de locais externos, devido a suas reduzidas dimensões, mas o campo elétrico nesses ambientes é formado por um número muito maior de componentes indiretos que no caso de ambientes ao ar livre. Então apesar desta distância entre o transmissor receptor ser bem menor a sua alta atenuação causada por paredes internas e mobília, além da grande variedade de ambiente. (SANCHES, 2007, p.157)

Nesse tipo de ligação utilizado em ambientes internos encontram-se algumas vantagens, como:

- Mobilidade - Alcance de até 300m para aplicações *Indoor*. (WINSERV, 2008)

- Flexibilidade - É possível utilizar redes sem fio em lugares fisicamente impossíveis de ser ter uma rede cabeada. Mudanças de *layout* são facilitadas por não utilizar em fios. (WINSERV, 2008)
- Uso em pequenos, médios e grandes escritórios, fábricas, eventos, aeroportos, cibers-café, *shoppings centers*, hotéis e muitos outros tipos de negócios. (WINSERV, 2008)

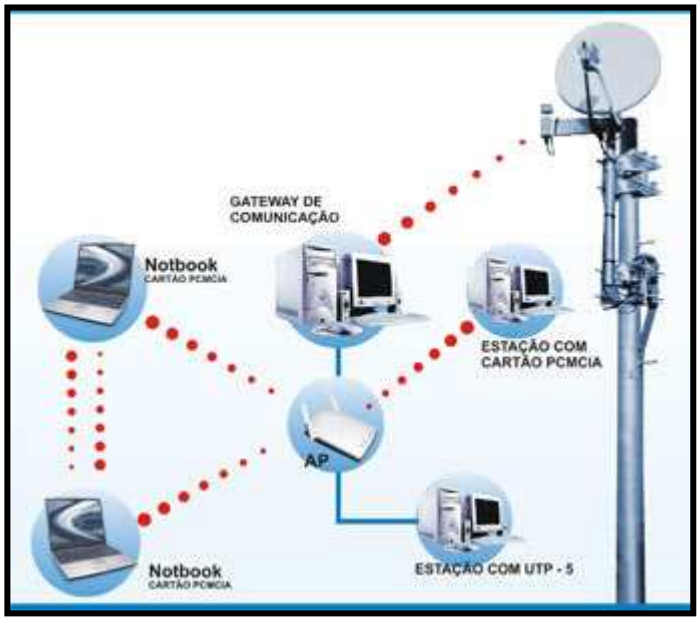

Figura 1. Rede sem fio interna *(indoor).* (WINSERV, 2008)

1.3.2 Outdoor

As redes sem fio para ambientes externos (*Outdoor*) são um grande atrativo para soluções de interligações de redes para baixo custo, em prédios localizados em pontos diferentes, como matriz e filial, comparando-se à tecnologia com uso de cabos que geralmente utiliza fibras ópticas ou cabos metálicos próprios para ambiente externo. (WINSERV, 2008)

As redes *outdoor* têm mecanismos e equipamentos semelhantes aos utilizados em uma rede interna, no entanto conectam-se a uma antena externa e possuem alto desempenho e robustez.

Esse tipo de conexão é comum em:

- Interligação de LANs em alta velocidade sem custos fixos mensais. (WINSERV, 2008)

- Utilização de aplicações como VOIP (Voz sobre IP). (WINSERV, 2008)
- Monitoramento de Sistemas de Câmeras (vigilância patrimonial). (WINSERV, 2008)

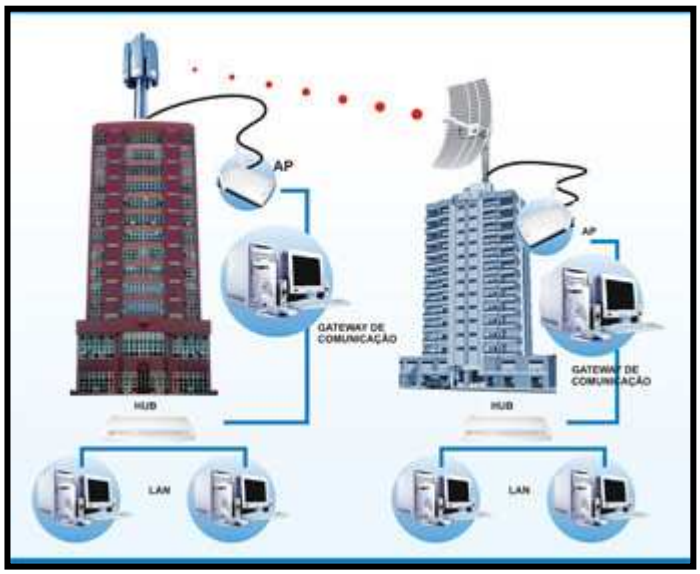

Figura 2. Redes externas *(outdoor)* (WINSERV, 2008)

Na conexão multiponto, um ponto central irradia o sinal para vários outros pontos. Solução usada principalmente por provedores de internet a rádio. (WINSERV, 2008)

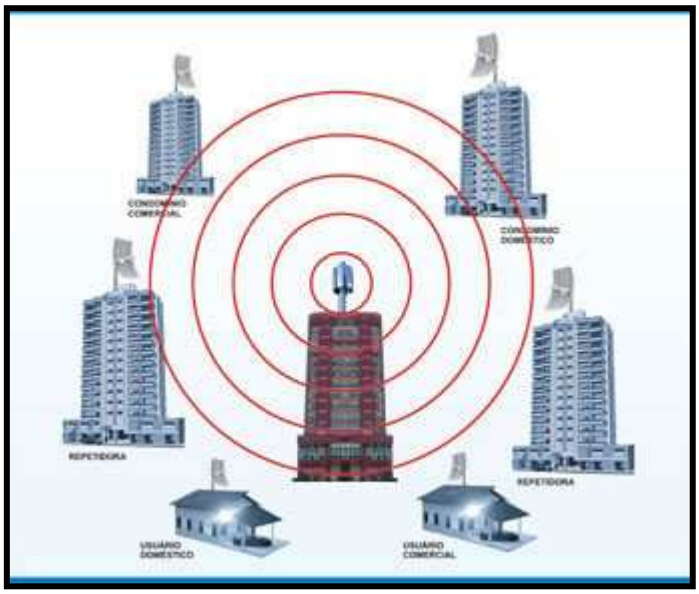

Figura 3. Redes externas multipontos *(outdoor).* (WINSERV, 2008)

2 HISTÓRICO DA EVOLUÇÃO DAS AMEAÇAS ÀS REDES SEM FIO

Em agosto de 2001, Scott Fluhrer, Itzik Mantin e Adi Shamir publicaram uma análise para quebra criptográfica do WEP, que explora a forma como o RC4 e os IV (vetores de inicialização) são usados no WEP, o resultado foi o ataque passivo, que consiste em capturar pacotes usando o modo RFMON (modo monitor) e aproveitar-se das falhas dos IVs. A partir dessa publicação alguns incidentes foram reportados pelos meios de comunicação, como: revistas, jornais e sites especializados. Essas reportagens, trataram do histórico das ameaças às redes sem fio, cuja evolução pode ser vista no capítulo seguinte.

3 PRICIPAIS INCIDENTES REPORTADOS NA IMPRENSA

A imprensa teve papel importante no registro de incidentes causados pelas fragilidades das redes sem fio.

Em material da RNP, faz-se um relato desse incidente, assim registrado um caso interessante que demonstra a fraqueza do WEP que aconteceu nos EUA: análises de segurança em redes sem fio foram conduzidas por empresas especializadas nos aeroportos internacionais de Denver e de San Jose. A análise em Denver revelou que a American Airlines operava uma rede sem fio totalmente em claro (sem o uso de criptografia) no aeroporto. Um fato agravante foi o testemunho de um ataque em tempo real durante a análise. Em San Jose, o exame revelou resultados semelhantes aos de Denver: pouca ou nenhuma proteção contra ataques. Os especialistas puderam monitorar o tráfego de informações confidenciais como operações de check-in da American Airlines e Southwest Airlines. As implicações dessas vulnerabilidades podem ser gravíssimas: no caso do aeroporto, dependendo das comunicações existentes, um atacante pode, a partir de uma rede sem fio não protegida, obter acesso à rede operacional, que pode incluir operações de vôo, controle de bagagem ou reserva de passageiros. (RNP, 2007, p.237)

Reuters, apud **Info exame**, afirma que, no ano de 2001, “Redes sem fio estão vulneráveis a *hackers*” Nessa reportagem, o autor diz que uma equipe de pesquisadores constatou falhas de segurança nos padrões de segurança para redes sem fio de computadores. As falhas facilitam a invasão por *hackers* para roubos ou modificação de dados. Os pesquisadores descobriram meios de espionar ou até de interferir nas redes, conhecidas com *Wireless*, através do uso de um algoritmo de segurança chamado Privacidade de Equivalência Conectada. Mesmo que a informação transmitida através dessas redes seja criptografada para impedir acesso sem autorização, os *hackers* podem usar equipamentos com *Wireless* modificado para interceptar e decodificar os dados, disse o grupo de pesquisadores. (Disponível em http://info.abril.com.br, acesso em 04/11/2008)

Os pesquisadores, dois da Universidade da Califórnia em Berkeley e um da empresa privada de segurança Zero-Knowledge, também disseram que os invasores podem modificar outros equipamentos de Wi-Fi e transmitir potencialmente dados perigosos para as redes. O padrão *wireless* ficou popular no ano 2000, com companhias revelando planos de fornecer acesso a redes corporativas e à Internet para funcionários de qualquer lugar do escritório. Mais de trinta empresas, incluindo Cisco, Apple e Compaq, fazem produtos para a tecnologia Wi-Fi, segundo a organização do setor *Wireless Ethernet Compatibility Alliance*. (Disponível em http://info.abril.com.br, acesso em 04 nov. 2008)

Figura 4. Site da **Info exame** (Disponível em http://info.abril.com.br, acesso em 04 nov. 2008)

Outra reportagem importante é encontrada no site especializado em segurança da informação www.viaseg.com.br, no ano de 2002, como a seguinte manchete: “EUA usam lata de batatas fritas para procurar falhas em redes”.

A reportagem diz que agentes do serviço secreto querem adotar tecnologia de ponta para os policiais: com um notebook e uma antena feita com uma lata de batatas fritas Pringles, é possível encontrar furos nas redes sem fio, em Washington. A agência que protege o presidente e caça contraventores já começou a direcionar seu trabalho para essas falhas. O esforço é parte de um novo plano do governo para criar um elo com as empresas e sentir-se mais à vontade para relatar tentativas de invasão às autoridades. Uma legislação contra o terrorismo, aprovada recentemente, deu ao FBI (Polícia Federal Norte-Americana) e ao serviço secreto jurisdição sobre crimes eletrônicos. (Disponível em http://www.viaseg.com.br/noticia/1043-eua_usam_lata_de_batatas_fritas_para_procurar_falhas_em_redes.html, acesso em 04 nov. 2008)

Com menos de US$ 200 é possível fazer uma rede sem fio. Quem circula com um notebook ou micro de mão pode se conectar, em trânsito, à rede do seu trabalho. Essas redes estão se tornando comuns em aeroportos, universidades, cafés, residências e até em parques públicos. O problema é que elas são vendidas sem medida de segurança, e proteger uma rede sem fio de *hackers* exige mais instruções do que os guias de instalação de rede oferecem. Devido à questão de segurança, a Casa Branca propôs recentemente banir algumas redes sem fio em agências federais. Depois de enfrentar protestos da indústria, o governo abandonou a idéia quando anunciou um projeto do seu plano de *cyber* segurança. Isso levou alguns pesquisadores independentes na área de segurança a circular por cidades para mapear as redes. Esses mapas disponíveis em sites revelam onde obter uma conexão gratuita de internet em uma rede privada. O serviço secreto quer avisar as empresas que suas conexões de internet e suas redes privadas podem correr riscos. Alertadas sobre furos na segurança, as companhias podem configurar suas redes e torná-las mais seguras. (Disponível em http://www.viaseg.com.br/noticia/1043-eua_usam_lata_de_batatas_fritas_para_procurar_falhas_em_redes.html, acesso em 04 nov. 2008)

As ferramentas de Peterson são um *notebook*, um cartão de rede sem fio e três antenas montadas em seu carro. Uma delas é um fio de metal pequeno; a segunda é um tubo branco; a terceira é caseira e feita com uma lata de batatas fritas Pringles. As antenas captam os sinais do cartão de rede e permitem apontar para diferentes direções até conseguir o sinal. A lata de Pringles é ideal por ter o interior de alumínio e por ter um formato de um tubo longo, permitindo que qualquer pessoa aponte a antena para locais específicos para o ato de *wardriving*. E seu interior como é de alumínio, funciona como se fosse um satélite, coletando sinais e enviando-os ao receptor, que é depois conectado a um *notebook*. Peterson recentemente circulou por uma rua de Washington e encontrou mais de 20 redes sem fio, muitas sem nenhuma segurança. O agente afirmou que seus testes eram parte de um bom trabalho da polícia, como um patrulheiro fazendo a ronda pela vizinhança. O ato de "*wardriving*", termo derivado do antigo "wardialing" que são programas que ligavam aleatoriamente para números de telefone

buscando *modems* fora da lista telefônica, pegou bem entre *hackers* e mesmo entre pesquisadores não interessados em acesso clandestino. Eles chegam a marcar com giz nas ruas áreas em que é possível entrar em redes sem fio desprotegidas. (Disponível em http://www.viaseg.com.br/noticia/1043-eua_usam_lata_de_batatas_fritas_para_procurar_falhas_em_redes.html, acesso em 04 nov. 2008)

Figura 5. Site da **viaseg**

(Disponível em http://www.viaseg.com.br/noticia/1043-eua_usam_lata_de_batatas_fritas_para_procurar_falhas_em_redes.html, acesso em 04/11/2008)

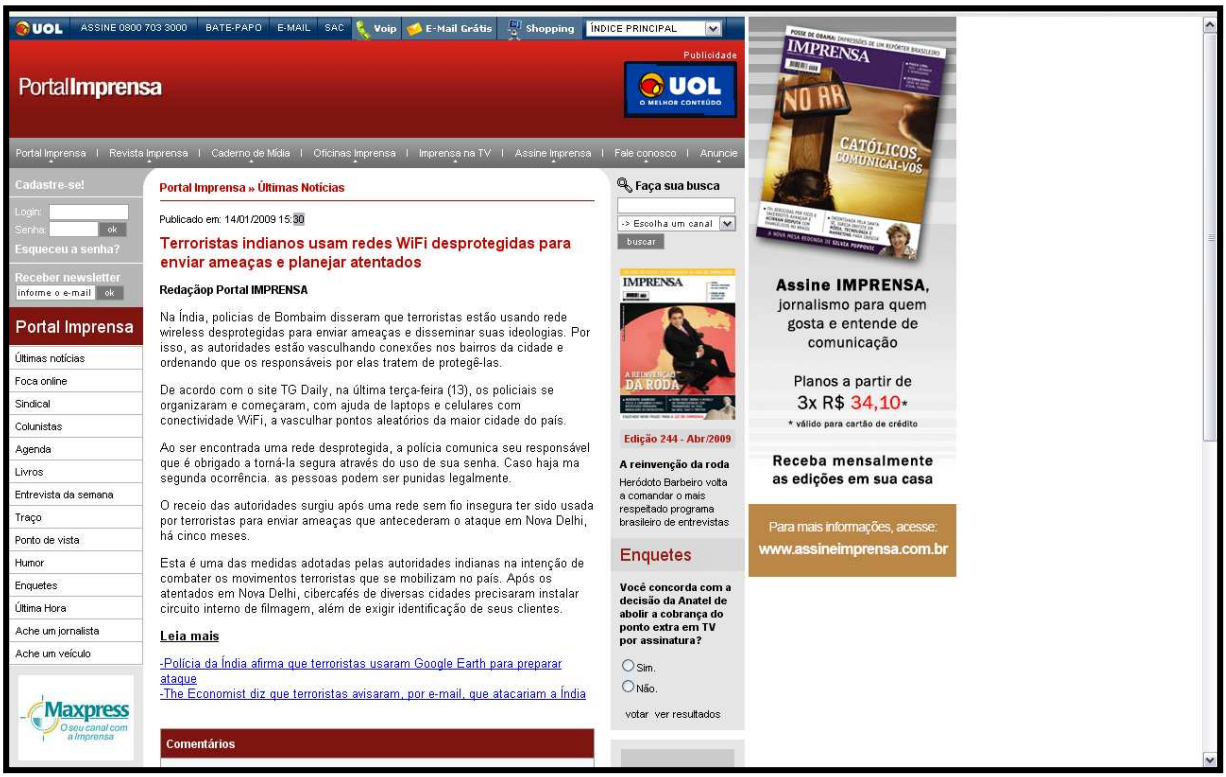

Figura 6. Site Portal imprensa
(Disponível em
http://portalimprensa.com.br/portal/ultimas_noticias/2009/01/14/imprensa25437.shtml, acesso em 22 abr. 2009)

A figura 6 ilustra o site portal imprensa, que relatou no início de janeiro de 2009, que terroristas indianos estão aproveitando redes sem fios desprotegidas para planejar atentados e enviar ameaças. Diante deste problema, policiais indianos estão praticando o *Warwalking*, que é o ato similar do *Wardriving*, com a variação de não ter o carro para deslocamento, mas a prática de andar pelas ruas identificando as redes vulneráveis, desde então, estes policiais andam equipados com *laptops* e celulares com conectividades *wireless*, rastreando essas redes desprotegidas, chamando atenção dos seus respectivos responsáveis para adotar alguma medida de proteção. Caso haja uma segunda advertência, os responsáveis dessas redes serão punidos legalmente.

Em uma matéria na revista **Info exame**, John C. Dudrak chama atenção sobre a sua preocupação em relação à segurança nas redes wireless, pois na sua matéria, contando que em uma passagem por Hannover na Alemanha, ele precisou usar a internet no seu hotel onde estava

hospedado, mas o seu valor não era nada especial, mas curiosamente no hotel do outro lado da rua havia uma conexão sem fio que podia ser acessada do seu quarto. O serviço era pago, mas algum escritório desse prédio havia instalado um equipamento *wireless*, como um *Access Point,* deixando assim a rede aberta sem nenhum tipo de mecanismo de segurança. Segundo ele, essa prática vem acontecendo na maior parte do mundo, pois as pessoas compram os equipamentos de redes com padrão 802.11, mas não dão a mínima para criptografia. (DUDRAK, 2004, p.38)

Essa reportagem revela que às vezes, mesmo existindo uma política de segurança, as redes podem estar vulneráveis, pois com a escalabilidade e usabilidade das redes sem fio, nas mãos de pessoas sem capacitação, podem resultar em uma má configuração dos equipamentos sem fio, gerando pontos falhos da segurança.

O próximo capítulo tratará dos mecanismos de segurança para um ambiente confiável, evitando os problemas de vulnerabilidades, como constatadas pelos meios de comunicação.

4 REDES SEM FIO: AMEAÇAS E FRAGILIDADES

Nesse capítulo, serão apresentadas as principais técnicas de exploração das fragilidades que envolvem as tecnologias *wireless.*

4.1 DoS (*Denial of Service*)

Atacantes potenciais que não obtêm acesso a rede sem fio podem assim mesmo colocar ameaças de segurança ao inundar sua rede *wireless* com ruído estático que façam com que os sinais colidam e produzam erros de CRC. Esses ataques de negação de serviço fazem efetivamente cair ou diminuir a velocidade da rede sem fio da mesma forma semelhante à rede cabeada.

Ainda hoje é comum outros dispositivos de mesma frequência sem fio provocarem de forma não intencional um suspensão de serviço de uma rede *wireless*, por exemplo: quando um telefone sem fio que opera na faixa de 2,4GHz, ou a colocação de pontos de acesso próximo a dispositivos que gerem interferência e afetam a operação, como é o caso do aparelho de microondas. Nem toda redução de conectividade sem fio está relacionada a ataques.

4.2 WarChalking

WarChalking é uma prática que os *hackers* europeus criaram um alfabeto especial para identificar redes sem fio com giz na calçada, com os pontos de acesso (posição e orientação da antena) para uma melhor conexão à rede alheia. (CARMONA, 2006, p.112)

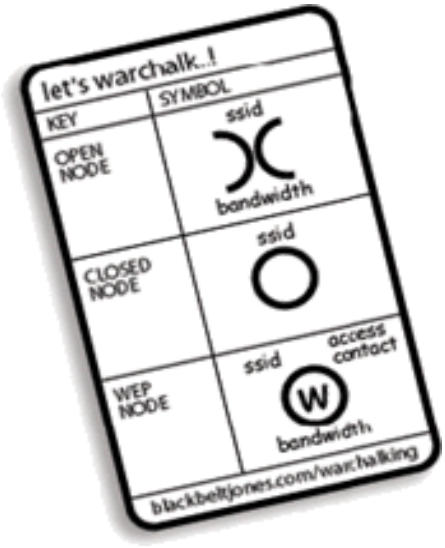

Figura 7 Tabela de simbolos *WarChalking* (Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2 acesso em 30/10/2008)

O símbolo com dois semicírculos, um de costas para o outro, mostra que naquele local há uma rede aberta. (TOMAS, 2007, p.265)

O símbolo fechado de uma circunferência mostra que, no local onde foi desenhado, encontra-se uma rede fechada. (TOMAS, 2007, p.265)

O terceiro e ultimo símbolo, de uma circunferência com um W dentro, mostra que há uma rede utilizando criptografia WEP. (TOMAS, 2007, p.265)

O SSID encontra-se na arte superior e a largura da banda é mostrada abaixo dele. (TOMAS, 2007, p.265)

4.3 WarDrinving

O *Wardriving* é uma prática na qual redes sem fio são identificadas apenas usando um *notebook*, um amplificador de sinais (que pode ser uma lata de Pringles), um *software* apropriado e um carro. O mapeamento é feito passeando-se de carro, enquanto o *notebook* captura informações sobre redes identificadas por ele. O mapeamento dessas redes, com a devida posição GPS de cada rede, pode ser compartilhado via internet, em sites como da própria Netstumbler. (RNP, 2007, p.238)

Essa é uma técnica que utiliza o mesmo princípio do *Scanning* e consiste em dirigir ao redor de uma área específica, mapeando a população de *Access Points* com um propósito estatístico [Hurley 2007].

O *Wardriving* foi inventado por um homem chamado Peter Shipley, que teve a visão de levar o *WarChalking* a um outro nível, pois em suas andanças, constatou que apenas 15 % das redes faziam o uso do WEP, e após um ano de publicação dos seus achados, esse número aumentou para 33%, levando a crer que as pessoas estão captando a mensagem que é preciso proteger as suas redes e informações. (TOMAS, 2007, p.268)

4.4 WarFlying

O *Warflying* é uma prática apelidada por se tratar de uma expansão do *Wardriving* que ganhou os céus. (RNP, 2007, p.238)

Um grupo usou um avião privado em San Diego em agosto de 2002 para mapear as *WLANs* da região. Eles identificaram 437 pontos de acesso e determinaram que apenas 23% das redes possuíam WEP habilitado. É interessante notar que, sobrevoando a uma altura de 750 metros, eles foram capazes de detectar pontos de acesso a uma distância entre cinco e oito vezes maior que o especificado no padrão, provavelmente devido à ausência de obstruções. (RNP, 2007, p.238)

4.5 Força Bruta

O ataque de força bruta corresponde a uma análise sistemática de todas as possibilidades de chaves para quebrar o código. Considerada a forma mais rudimentar de tentativa de quebra de códigos. (NOGUEIRA, 2008, p.6)

5 MECANISMOS DE SEGURANÇA

Esse capítulo pretende mostrar os mecanismos de segurança disponíveis para as redes sem fio. Fazendo uma pequena explanação do que será dado e seguindo uma ordem cronológica, essas técnicas são apresentadas pelo o padrão WEP, passando pelo padrão WPA e finalizando no padrão 802.1X.

5.1 WEP

O protocolo WEP, utilizado no padrão 801.11, usa uma chave secreta para autenticação e uma chave compartilhada para cifragem de comunicação entre a estação *wireless* e o ponto de acesso. Todos os dados enviados e recebidos podem ser cifrados por essa chave compartilhada. Esse compartilhamento é feito manualmente, com a chave sendo definida no momento da configuração. (NAKAMURA, 2007, p.171)

O algoritmo de criptografia usado pelo WEP é o RC4, com chaves que variam entre 40 e 128 bits. O pacote gerado por esse protocolo pode ser visto na figura 1, é formado por quatro componentes:

I – Vetor de inicialização (v); (NAKAMURA, 2007, p.171)

II – Byte de identificação da chave (*Key ID Byte*), para controle; (NAKAMURA, 2007, p.171)

III – Algoritmo de integridade CRC-32 aplicado na *payload*; (NAKAMURA, 2007, p.171)

IV – Algoritmo criptográfico RC4 aplicado na *payload* e no resultado do RC-32. (NAKAMURA, 2007, p.171)

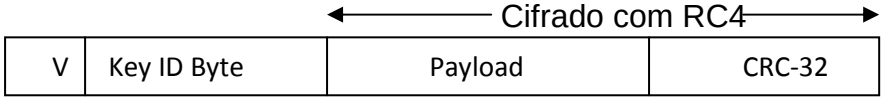

Figura 8. Pacote padrão IEEE 802.11 (RNP, 2007, p.242)

Na figura acima pode-se ver que o vetor de inicialização é transmitido em claro juntamente com o *payload* protegido pelo RC4. A montagem do pacote é feita da seguinte maneira: (RNP, 2007, p.242)

- A chave secreta (k) é concatenada a um vetor de inicialização (v) aleatório, que adiciona 24 *bits* a uma chave resultante; (v,k); (RNP, 2007, p.242)
- O resultado é fornecido ao RC4, que gera um *Key stream* pseudo aleatório; (RNP, 2007, p.242)
- Para garantir a integridade da mensagem o algoritmo de verificação CRC-32 é usado, um valor de integridade é gerado ICV e concatenado com o texto claro (p); (RNP, 2007, p.242)
- O texto cifrado (c) é um resultado de uma operação XOR do texto concatenado com o texto concatenado com (ICV), com o *key stream* produzido pelo RC4. (RNP, 2007, p.242)

Algebricamente, a cifragem WEP é representada da seguinte maneira: c = p XOR RC4(v,k) . (RNP, 2007, p.242)

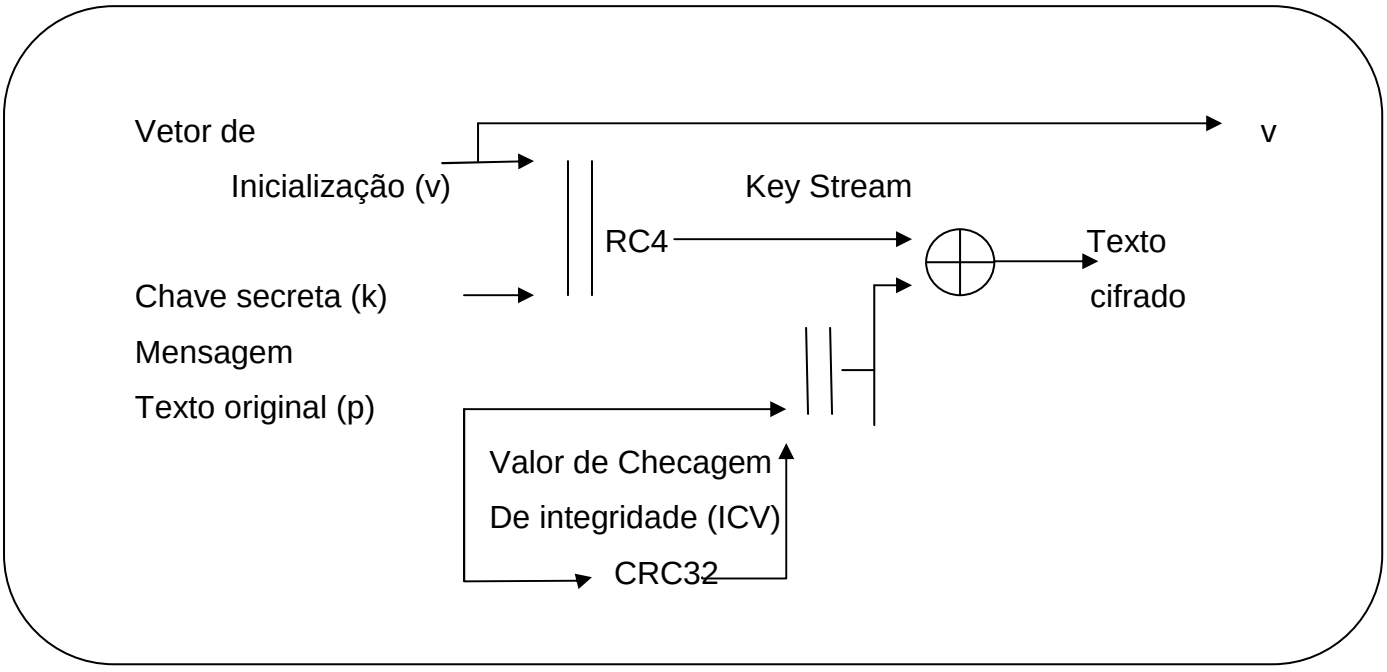

Figura 9. Cifragem do WEP (RNP, 2007, p.242)

O WEP é um padrão de segurança que foi concebido para tornar a comunicação sem fio equivalente à comunicação com fio. Tendo como um dos principais problemas a serem resolvidos em redes sem fio o ataque

passivo, como a escuta clandestina. (RNP, 2007, p.238) E isso servirá como base de estudo das vulnerabilidades das redes sem fio.

5.1.1 Explorando Fragilidades do padrão WEP

Como foi visto no item 4.1, o padrão WEP utiliza uma cifra de fluxo RC4 para criptografar e o CRC-32 para verificar a integridade dos pacotes. E um vetor de inicialização de 24 bits, mais uma chave de 40 bits para quando for WEP 64-bits, ou de 104 bits para WEP 128-bits, e assim a lógica segue para o WEP-256-bits.

Devido à cifra RC4, a mesma chave de tráfego nunca deve ser usada duas vezes, o propósito do IV é prevenir qualquer repetição da chave de tráfego, porém o IV é transmitido como *plain-text*, ou seja, como texto “limpo”, essa forma de transmissão do IV abre uma brecha para ataques do tipo chave-relacionada “*Ataque related-key*”. (TOMAS, 2007, p.282)

Os 24-bits do IV não são suficientes para evitar a repetição em uma rede com tráfego elevado, o que abre possibilidades de colisão de pacotes, e pacotes alterados, tornando possíveis ataques do tipo fluxo-cifra (“Ataque *stream-cipher*”). (TOMAS, 2007, p.282)

Segundo as informações aqui mostradas, baseadas em obras de literatura específica, que o padrão WEP possui uma cifra fraca. No próximo parágrafo, é mostrado como pode ser explorada esta vulnerabilidade, apenas usando um *notebook* com a interface de rede sem fio em modo monitor para capturar o tráfego, e isto adequando a algumas ferramentas que auxiliam desde a captura à quebra das chaves.

Essa vulnerabilidade é mostrada através de uma comunidade criada na internet chamada de *Warchalking*, que tem o propósito de apresentar e discutir assuntos relacionados à segurança de redes sem fio. Nesta prática foi usado o modo monitor no *Windows* com a ferramenta aircrack e airodump. (THINKER, 2006)

Primeiro passo, com o uso do Airodump, serão perguntados qual interface usará, indicando através de um número correspondente com o nome da interface, o seu tipo de *chipset*, o canal correspondente que queira

explorar a criptografia, e por fim o nome do arquivo que será gravado com os pacotes. (THINKER, 2006)

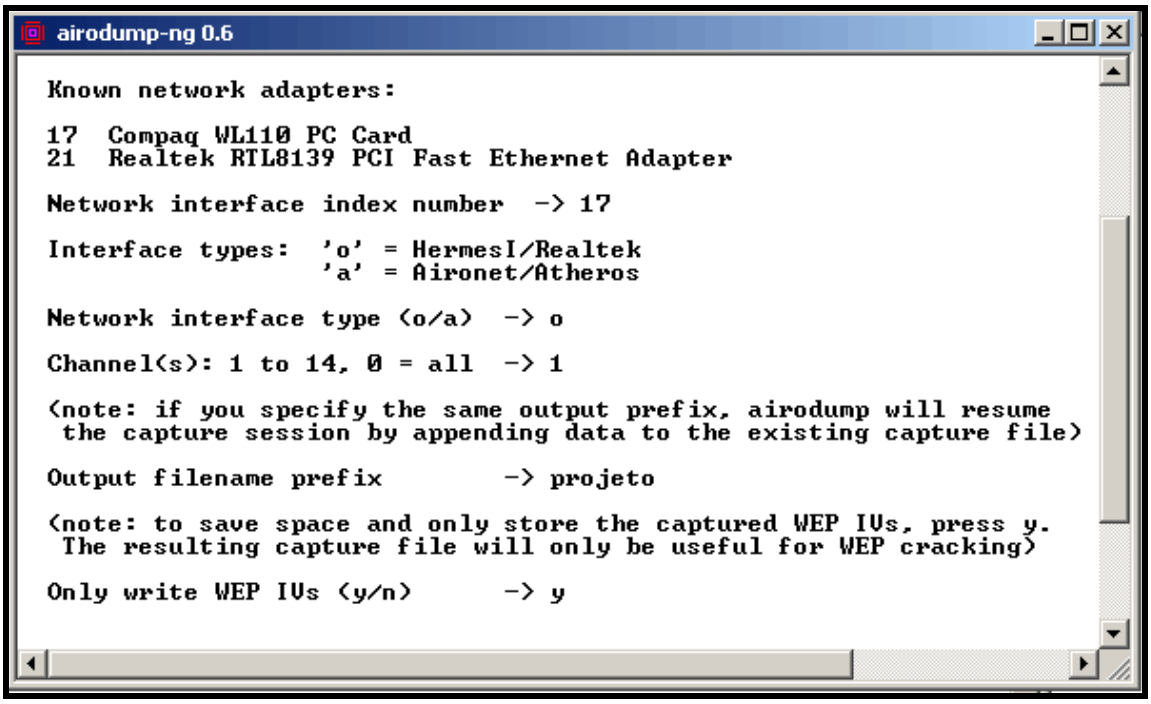

Figura 10. Adequando ao Airodump para captura dos IV (Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2 acesso em 30 out. 2008)

Com o Airodump capturando os pacotes, a interface mostra três campos interessantes, o BSSID (endereço MAC do provedor), o ESSID (nome da rede para conexão) e o # Data, representa o numero de pacotes pegos, que se trata do numero de IV. O número necessário varia de 300 mil até 1,5 milhão, dependendo de quantos *bits* tem a chave, como o aircrack pode usar vários arquivos ao mesmo tempo, é interessante primeiro capturar 300 mil, depois com 700 mil e por ultimo com 1,5 milhão. (THINKER, 2006)

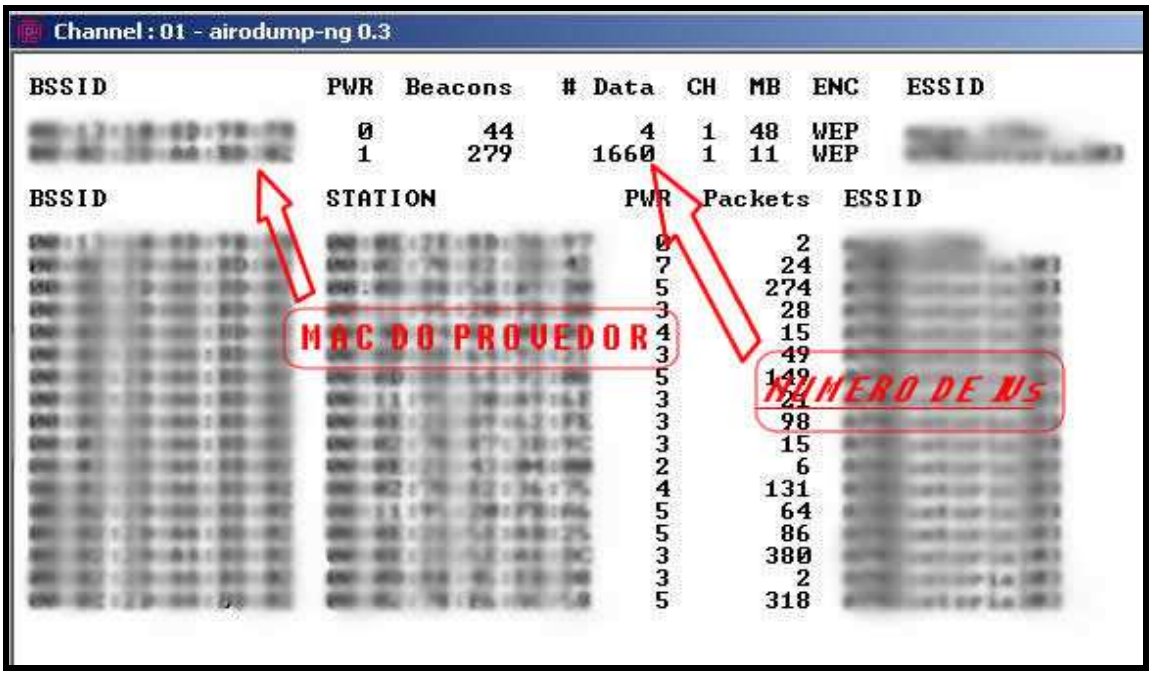

Figura 11. Capturando pacotes (Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2 acesso em 30 out. 2008)

Concluída a captura, é necessário fazer o uso da ferramenta aircrack, para tal, então com o uso do prompt de comandos do Windows, basta entrar na pasta correspondente do aircrack. (THINKER, 2006)

Na pasta correspondente do aircrack, utiliza-se o comando especificado abaixo: (THINKER, 2006)

C:\aircrack-ng –n64/128/256 NomeDoArquivo.ivs NomeDoArquivo2.ivs

NomeDoArquivo é o nome do arquivo gerado com a captura dos IVs pelo Airodump. E na opção "–n" é especificando quantos *bits* de criptografia, podendo ser de 64 bits, 128 *bits* ou 256 *bits*. É importante lembrar que o Aircrack pode ser usado simultaneamente com o Airodump.

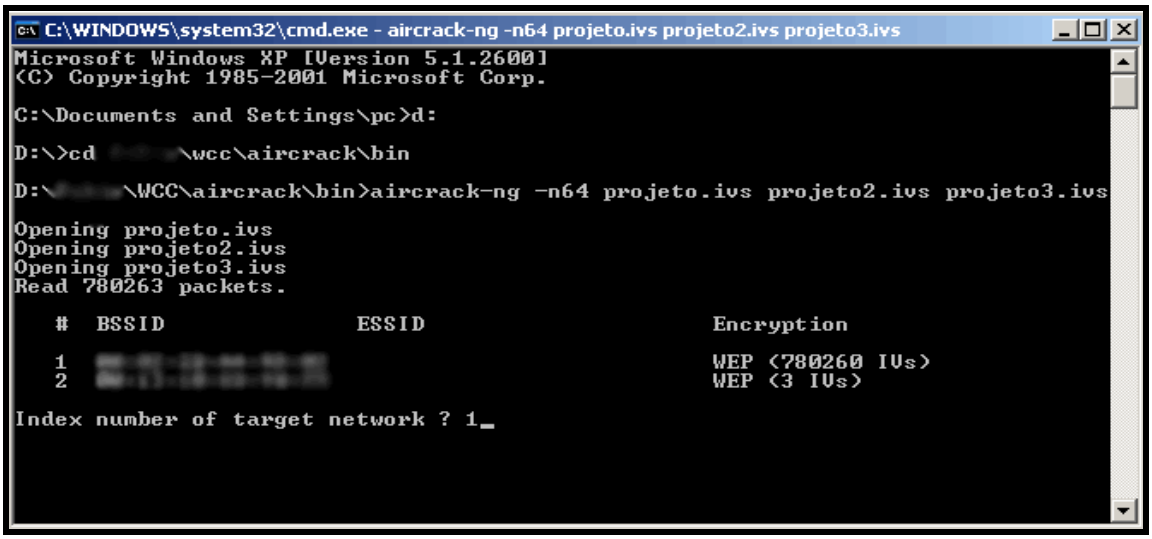

Figura 12. Selecionando a rede (Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2, acesso em 30 out. 2008)

O programa começará a rodar, e, ao final, terá um resultado como a figura abaixo. Apresentando a chave de duas formas, Hexadecimal (0-9 e A-F) e ASCII.

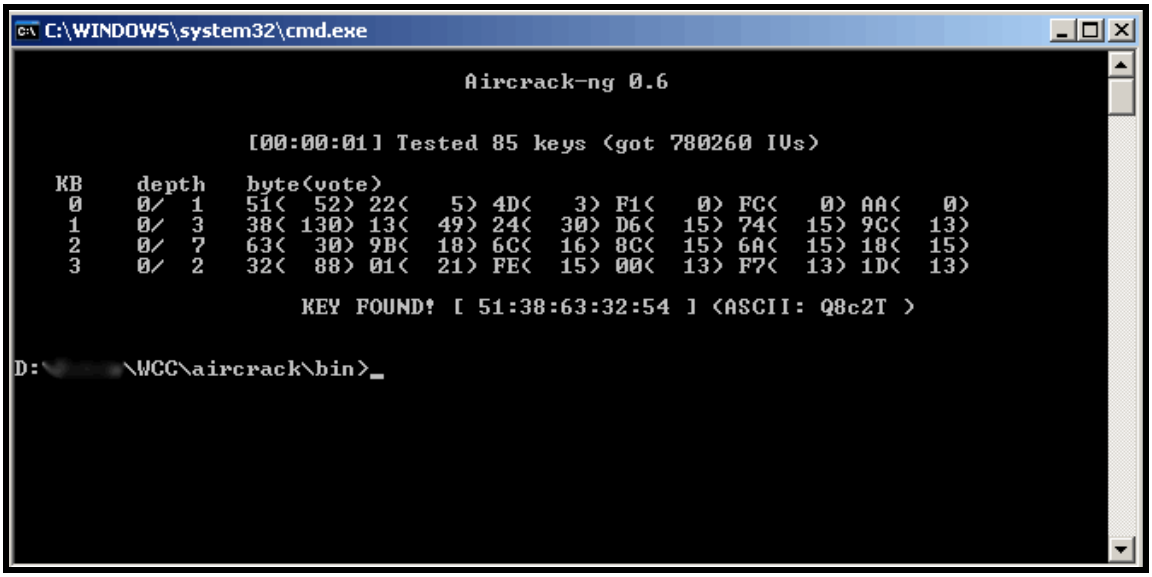

Figura 13. Gerando as chaves (Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2, acesso em 30 out. 2008)

Ao final dessa seção, conclui-se que é possível quebrar o WEP, mas por que ainda são encontradas redes sem fio com esse padrão? Pois novas

tecnologias sugiram no mercado, com o intuito de corrigir esses problemas, como é o caso do WPA.

5.2 WPA (*Wi-Fi Protected Access*), TKI e 802.11i

Como foi visto no item 2.6.1, o WEP possui falhas de projetos que envolvem o uso de chaves estáticas, a falta de autenticação mútua e o uso de criptografia fraca.

> O WPA é direcionado para o melhoramento dos problemas existentes no WEP; o padrão possui um subconjunto dos mecanismos de segurança especificados no padrão 802.11i, e foi projetado para utilizar um servidor de autenticação, como o RADIUS (*Remote Autenteication Dial-In User Service*), mas também pode-se fazer uso em um modo menos seguro, no caso de redes pequenas, utilizando-se uma chave pré compartilhada PSK (*Pre Shared Key*). Concluindo os aperfeiçoamentos do WPA sobre o WEP, tem-se: os algoritmos criptográficos fortes como o AES; vetor de inicialização de 128 *bits* e o TKPI. (SANCHES, 2007, p.239)

O TKPI (*Temporal Key Intergrid Protocol*), que é dada pela troca de chaves dinamicamentes a medida que o sistema é utilizado, combina-se com um vetor de inicialização muito maior, evitando-se os ataques de recuperação de chaves aos os quais o WEP é susceptível. (SANCHES, 2007)

A checagem de integridade das mensagens *Message Integrity Code* (MIC), chamado *Michael*, é projetada para prevenir que um atacante capture pacotes de dados, altere os e os retransmita. O MIC provê uma função matemática forte a qual o receptor e o transmissor computam e comparam o MIC, pois se não são iguais, assume-se que os dados foram falsificados e o pacote é descartado. (SANCHES, 2007, p.239)

Os processos de criptografia e descriptografia do WPA são descritos a seguir e ilustrados com as figuras, que foram retiradas do site da Microsoft.

O WPA precisa dos seguintes valores para criptografar e proteger a integridade de um quadro de dados sem fio:

- O IV, que é iniciado em 0 e incrementado para cada quadro subseqüente; (MICROSOFT, 2004)

- A chave de criptografia de dados (para tráfego em *unicast*) ou a chave de criptografia de grupo (tráfego em *multicast* ou de difusão); (MICROSOFT, 2004)
- O endereço de destino (DA) e o endereço de origem (SA) do quadro sem fio; (MICROSOFT, 2004)
- O valor do campo *Priority* (Prioridade), que é definido como 0 e é reservado para objetivos futuros; (MICROSOFT, 2004)
- A chave de integridade de dados (para tráfego em *unicast*) ou a chave de integridade de grupo (tráfego em *multicast* ou de difusão); (MICROSOFT, 2004)

A figura seguinte mostra o processo de criptografia do WPA para um quadro de dados *unicast*.

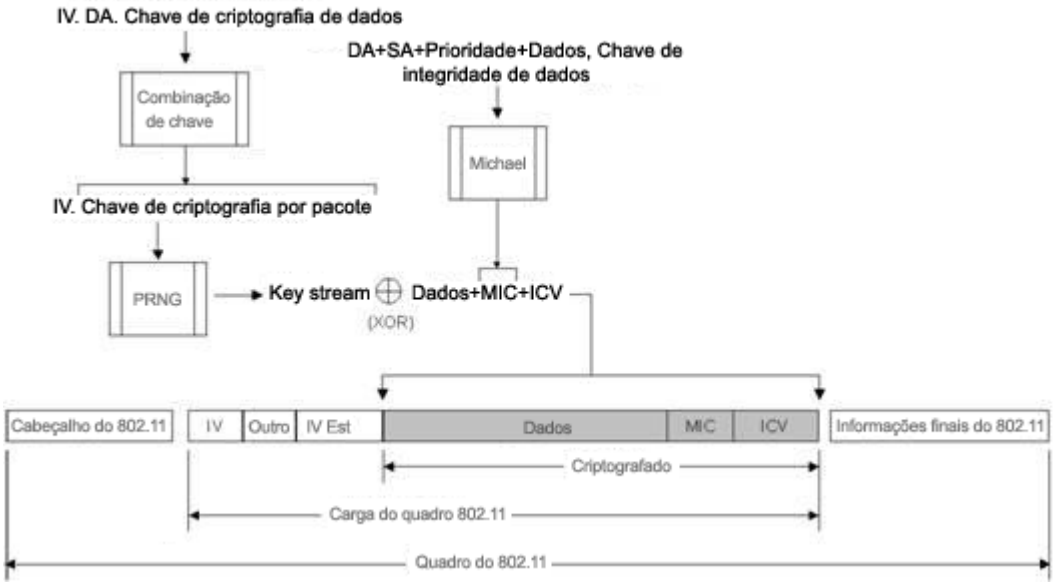

Figura 14. Criptografia WPA (SANCHES, 2007, p.239)

O processo de criptografia é descrito nas linhas abaixo:

I – O IV, o DA e a chave de criptografia de dados são inseridos em uma função de combinação de chave WPA, que calcula a chave de criptografia por pacote. (MICROSOFT, 2004)

II – O DA, SA, *Priority* (Prioridade), os dados (a carga 802.11 não criptografada), e a chave de integridade de dados são inseridos no algoritmo de integridade de dados *Michael* para produzir o MIC. (MICROSOFT, 2004)

III – O ICV é calculado da soma de verificação do CRC-32. (MICROSOFT, 2004)

IV – O IV e a chave de criptografia por pacote são inseridos na função RC4 PRNG para produzir um *keystream* do mesmo tamanho que os dados, o MIC e o ICV. (MICROSOFT, 2004)

V – O *keystream* é ORed (XORed) exclusivamente com a combinação de dados, do MIC e do ICV para produzir a parte criptografada da carga 802.11. (MICROSOFT, 2004)

VI – O IV é adicionado à parte criptografada da carga 802.11 nos campos IV e Extended IV (IV Estendido) e o resultado é encapsulado com o cabeçalho e informações finais sobre o 802.11. (MICROSOFT, 2004)

Já a figura seguinte mostra o processo de descriptografia do WPA para um quadro de dados.

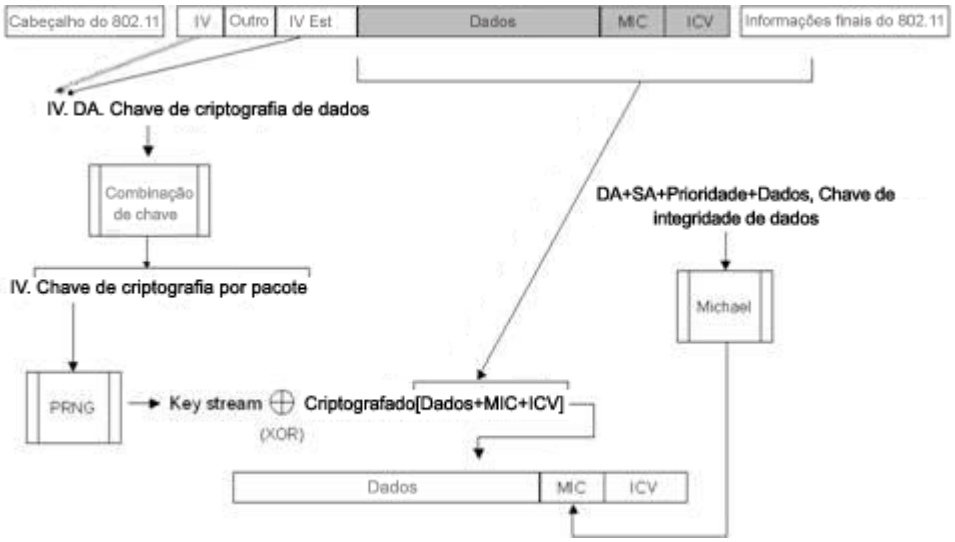

Figura 15. Descriptografia WPA (SANCHES, 2007, p.240)

I – O valor IV é extraído dos campos IV e *Extended* IV (IV Estendido) na carga do quadro 802.11 e inserido junto com o DA e a chave de criptografia de dados na função de combinação de chave, produzindo a chave de criptografia por pacote. (MICROSOFT, 2004)

II – O IV e a chave de criptografia por pacote são inseridos na função RC4 PRNG para produzir um *keystream* do mesmo tamanho que os dados criptografados, o MIC e o ICV. (MICROSOFT, 2004)

III – O *keystream* é XORed com dados criptografados, MIC e ICV para produzir dados não criptografados, MIC e ICV. (MICROSOFT, 2004)
IV – O ICV é calculado e comparado ao valor do ICV não criptografado. Se os valores do ICV não coincidirem, os dados serão descartados silenciosamente. (MICROSOFT, 2004)
V – O DA, o SA, os dados e a chave de integridade de dados são inseridos no algoritmo de integridade *Michael* para produzir o MIC. (MICROSOFT, 2004)
VI – O valor calculado do MIC é comparado ao valor do MIC não criptografado. Se os valores do MIC não coincidirem, os dados serão descartados silenciosamente. Se os valores do MIC coincidirem, os dados serão passados para as camadas de rede superiores para processamento. (MICROSOFT, 2004)

5.2 Padrão IEEE 802.1X

O padrão IEEE 802.1X é relativo ao nível de segurança de portas; inicialmente essa segurança era em redes cabeadas, mas logo foi aplicada nas redes sem fio. (NAKAMURA, 2007, p.178)

O EAP (*Extensible Authentication Protocol*) é um protocolo de segurança de camada 2, que existe no estágio de autenticação do processo de segurança e, nele está incluída a geração dinâmica de chaves e a autenticação mútua entre clientes e pontos de acesso. (NAKAMURA, 2007, p.178)

Os métodos mais comuns de EAP são:

- EAP-MD5: este usa o algoritmo de *hash* MD5 sobre o nome do usuário e a senha para passar as credenciais para o servidor RADIUS. O EAP-MD5 não oferece gerenciamento de chaves ou geração dinâmica de chaves, sendo necessário o uso de chaves WEP estáticas. O uso do de MD5 previne que usuários não-autorizados acessem as redes sem fio diretamente, porém não protegem a chave WEP, que ainda pode ser descoberta. Nesse método ainda não prevê a autenticação mútua, deixando a autenticação do ponto de acesso de lado, o que possibilita a

inserção de pontos de acesso não-autorizados na rede. (NAKAMURA, 2007, p.178)

- LEAP (*Lighweight Extensible Autentication Protocol*): este padrão é desenvolvido pela Cisco, em conjunto com o padrão 802.1X. Aqui, ele programa a geração dinâmica de chaves WEP para cada sessão, sendo possível sua renovação de acordo com o seu intervalo de tempo, e ainda especifica a autenticação mútua, tanto do dispositivo sem fio quanto do ponto de acesso. O risco existente no LEAP, baseado no MS-CHAPv1, que possui vulnerabilidades conhecidas, está no mecanismo de passagens de credenciais usada. (NAKAMURA, 2007, p.178)
- EAP-TLS (*Transport Layer Sevurity*): desenvolvido pela Microsoft, usa certificados digitais X.509 para autenticação. O TLS é utilizado para transmitir as informações de autenticação, e ainda existe a geração dinâmica e chaves WEP e a autenticação mútua. (NAKAMURA, 2007, p.179)
- EAP-TTLS (*Tunneled* TTL): o ponto de acesso identifica-se usando certificados digitais; porém, os usuários usam senhas para a autenticação. (NAKAMURA, 2007, p.179)
- PEAP (*Protected* EAP): está sendo desenvolvido pela Microsoft e Cisco, e funciona de maneira similar ao EAP-TTLS. (NAKAMURA, 2007, p.179)

6 METODOLOGIA

A principal motivação para esta pesquisa é compreender a real situação de risco em segurança em que se encontram as redes sem fio e como está a preocupação dos administradores de redes com relação à segurança da informação. Uma vez que é crescente a aplicação destas redes, nos mais diversos sistemas de informação críticos, o objetivo proposto desse estudo é alertar para a necessidade de proteção contra ataques, fraudes e outros crimes eletrônicos. Desta forma, a intenção é obter uma análise crítica e real das condições em que se encontram as redes sem fio em determinadas regiões de João Pessoa, onde se encontram estabelecimentos comerciais, órgãos públicos e residenciais, de tal forma que esse estudo possa ser utilizado para identificar e mapear as redes sem fio de acordo com o seu grau de segurança. Com base nos dados coletados, é possível identificar o grau de preocupação dos administradores de redes *wireless*.

Para a execução da pesquisa utilizou-se o ato do *Wardriving*. O *Wardriving* que permitiu uma leitura passiva das informações difundidas publicamente, através das redes sem fio dispersas nas regiões pesquisadas. Essa pesquisa foi feita para identificar redes desprotegidas, visando analisar a situação atual dessas redes, sua configuração, o nível de exposição, bem como descobrir a quais ataques estão mais susceptíveis, e em que contexto podem ser evitados.

6.1 Métodos

Os métodos utilizados para a prática do *Wardriving* exigiram as seguintes ferramentas:

- *Netstumbler* é uma *scanner* para o *Windows* usado na detecção de redes wireless que usem as normas 802.11b, 802.11a e 802.11g. Pode ser integrado com GPS e imagens de mapas. O *Netstumbler* é também conhecido por Network Stumbler;

- *Back track 2*, é uma distribuição *Linux* baseado na distribuição *Slackware* e funciona como *Live-CD*, que é focada em testes de penetração;
- *Kismet* é um analisador de rede (*sniffer*), e um sistema de detecção de intrusão (IDS - *Intrusion detection system*) para redes 802.11 *wireless*. *Kismet* pode trabalhar com as placas *wireless* no modo monitor, capturando pacotes em rede dos tipos: 802.11a, 802.11b e 802.11g;
- *AirCrack-ng* é um detector de redes, *sniffer* de pacote, aplicativo de quebra de WEP e WPA (Busca por Força-bruta) e é ferramenta de análise para redes locais sem fios 802.11. Funciona com qualquer placa *wireless* cujo driver suporta modo de monitoramento bruto (para uma lista, visite o website do projeto) e pode capturar e analisar (*sniff*) tráfego 802.11a, 802.11b e 802.11g;
- *Airodump*, coloca tráfego do ar em um arquivo .cap e mostra informação das redes;
- *Airmon-ng*,coloca placas diferentes em modo monitor;
- *Aireplay-ng*, injeção de pacotes (Somente em Linux);
- *Airtun-ng*, é um criador de interface de túnel virtual.

6.2 Metodologia Científica

A pesquisa de campo foi realizada através do ato de *Wardriving*, utilizando um automóvel de modelo Volkswagen Polo e um *notebook* de modelo SEMP TOSHIBA de processador AMD Turion64 X2 com 2 Gb de memória RAM e antena *wireless* de *chipset* Broadcom e um adaptador USB *wireless* de *chipset* Ralink, com uma antena uma de 8 Dbi, para obter um alcance maior das redes sem fio.

Uma das grandes dificuldades para a prática do *Wardriving* foi o fator tempo, pois com os horários restritos devido as atividades laborais, os rastreamentos das redes foram feitos nos turnos noturnos dos dias úteis da

semana e nos turnos diurno e vespertino dos sábados e domingos. Diante desta dificuldade do horário, são considerados que alguns concentradores (APs e Roteadores sem fio) estavam desligados, pois diante desta hipótese acredita-se que seriam encontradas mais redes sem fios, caso fosse feito o *Wardriving* no horário comercial dos dias úteis. E a segunda atividade foi fazer testes de acesso indevido, em um cenário montado para testes.

Com o *Wardriving* em prática, o primeiro rastreamento foi realizado no Bairro dos Estados, o bairro residencial com moradores de um bom poder aquisitivo, considerada de classe média. Na figura 16, é ilustrada a ferramenta *netstumbler* em ação.

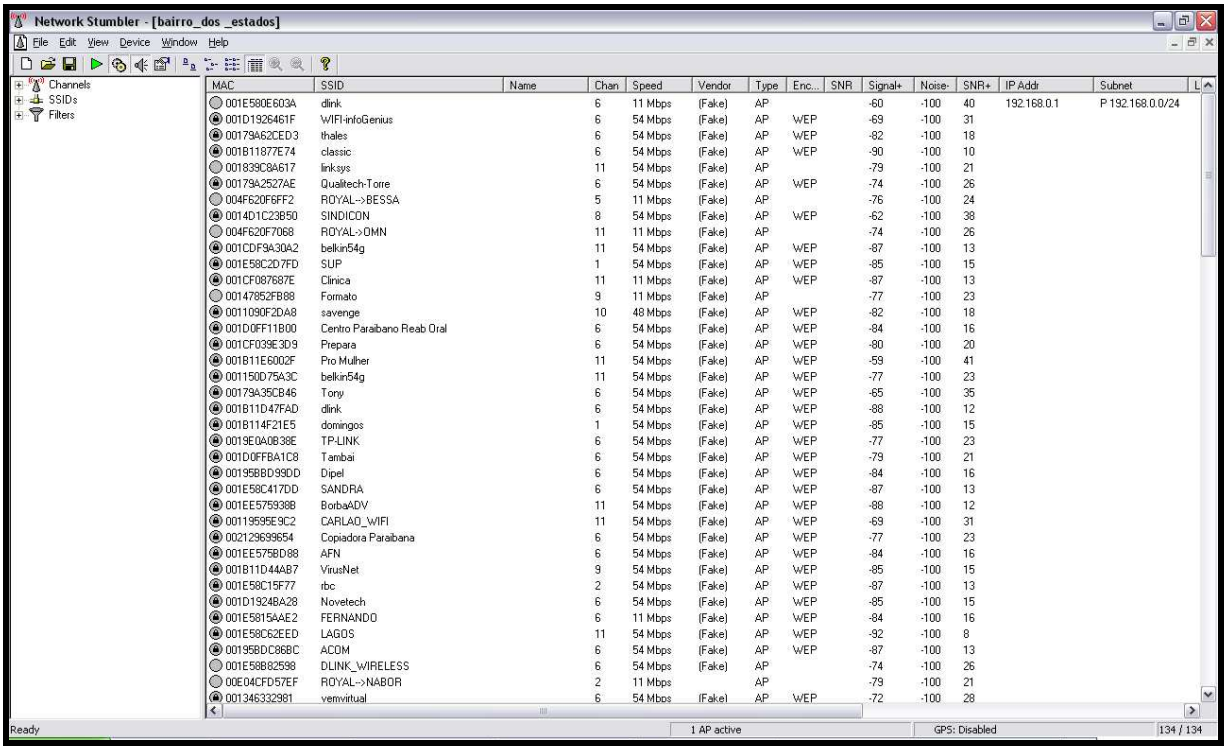

Figura 16. Ferramenta Netstumbler usada para rastrear as redes do Bairro dos Estados

No *Wardriving* feito no Bairro dos Estados, foram encontradas cento e trinta e quatro redes sem fio, das quais trinta e sete destas redes estavam abertas sem nenhum tipo de mecanismo, de segurança e noventa e sete estavam fechadas mostrando o seu SSID e usando algum tipo de mecanismo de segurança.

Na figura 17, ilustra-se o rastreamento dos bairros do Centro e da Torre, onde o que prevalece são os estabelecimentos comerciais e órgãos públicos. Neste *Wardriving* foram detectadas cento e oito redes sem fio, sendo que vinte e sete destas redes estavam abertas sem nenhum tipo de mecanismo de segurança e oitenta e uma fechadas possuíam algum tipo de mecanismo de segurança, e apenas duas destas oitenta e uma que não apresentavam o seu SSID.

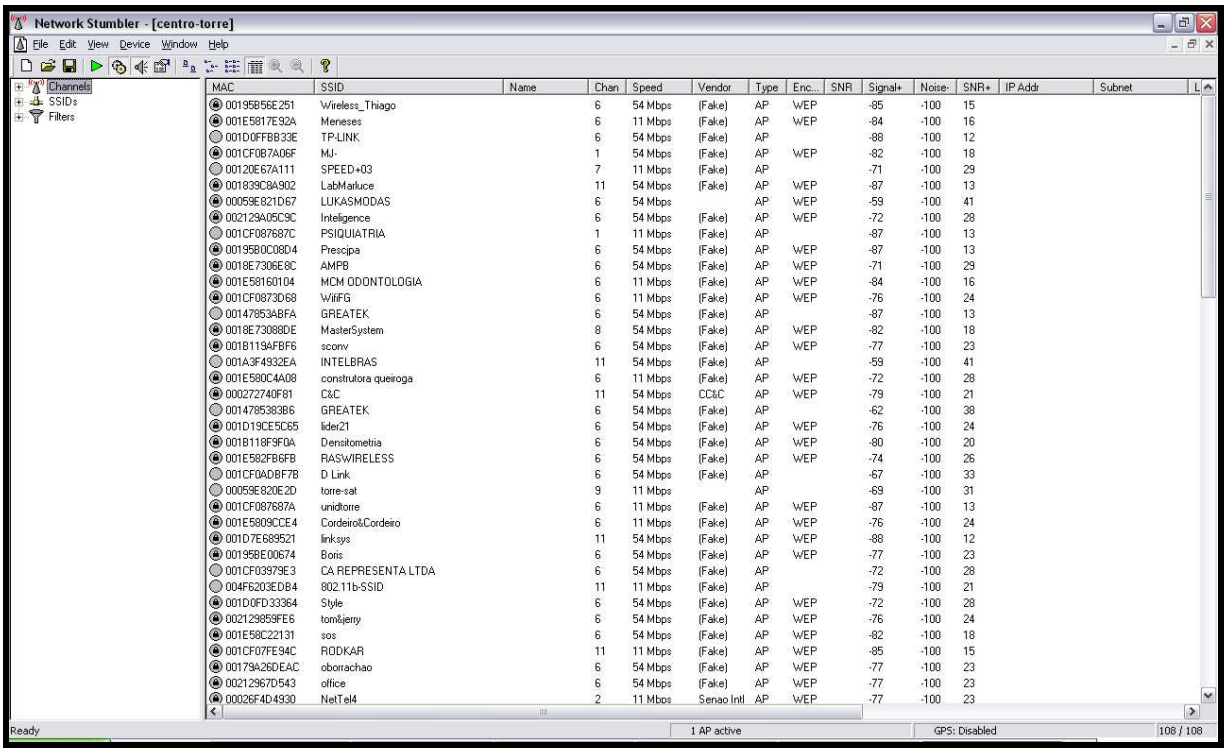

Figura 17. Ferramenta *Netstumbler* usado para rastrear as redes dos bairros do Centro e Torre

Na figura 18, ilustra-se o rastreamento do bairro de Jaguaribe, que é tradicionalmente conhecido por ser um bairro residencial de pessoas simples com um poder aquisitivo mais baixo. Nesse *Wardriving,* foram detectadas trinta e três redes sem fio, onde dezessete destas redes estavam abertas sem nenhum tipo de mecanismo de segurança e suscetíveis à invasão, enquanto dezesseis encontravam-se fechadas com algum tipo de mecanismo de segurança, incluindo-se uma que se encontrava com o recurso de não apresentar o SSID.

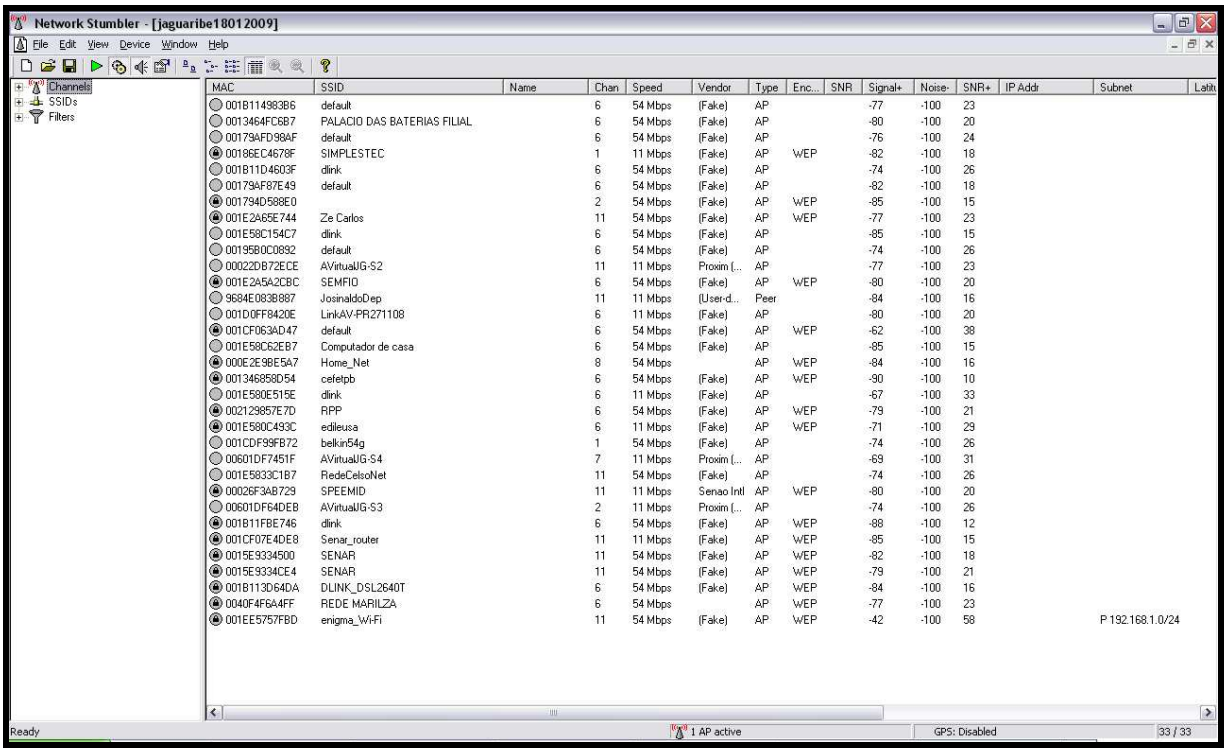

Figura 18. Ferramenta *Netstumbler* usada para rastrear as redes do bairro de Jaguaribe

Na figura 19, ilustra-se o rastreamento do bairro de Tambaú, bairro residencial da via litorânea de classe média alta, que também se destaca pela sua rede hoteleira. Nesse *Wardriving,* foram detectados duzentas e setenta redes sem fio, das quais cinquenta e cinco estavam abertas sem nenhum tipo de mecanismo de segurança e suscetíveis à invasão, enquanto duzentas e quinze encontravam-se fechadas com algum tipo de mecanismo de segurança.

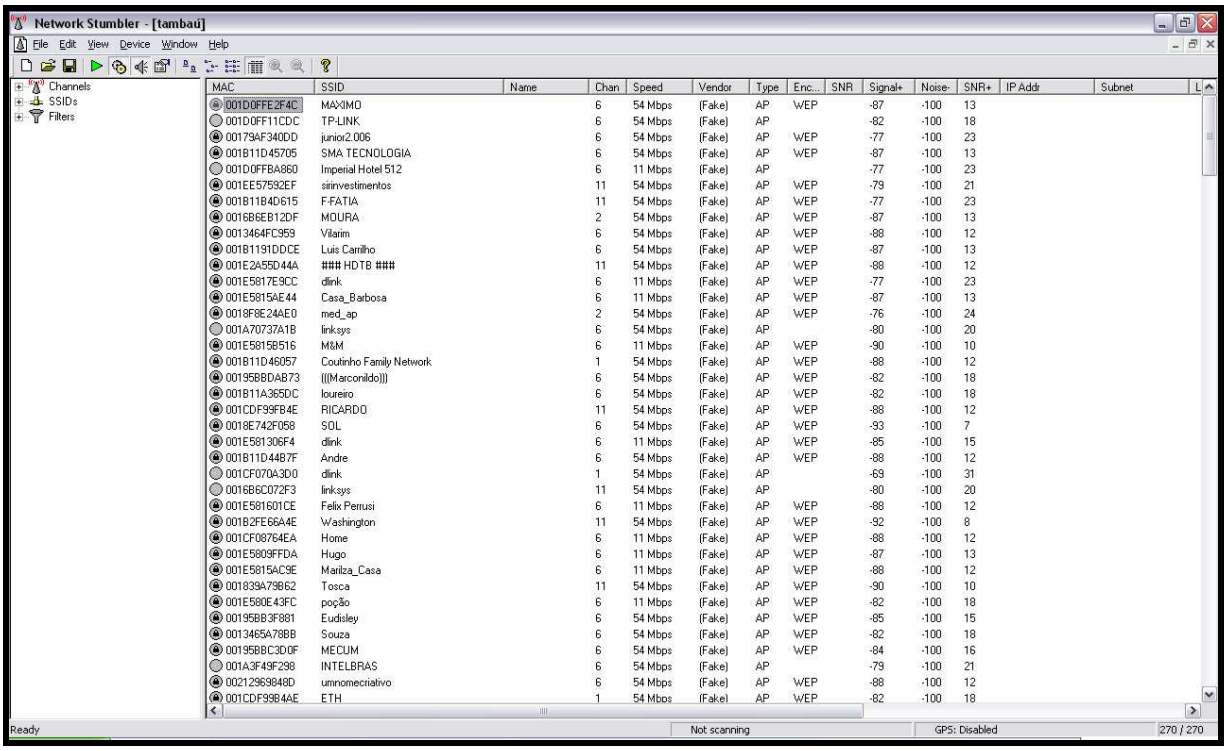

Figura 19. Ferramenta *Netstumbler* usada para rastrear as redes do bairro de Tambaú

Na figura 20, ilustra-se o rastreamento do bairro do Cabo Branco, é também por ser um bairro residencial da via litorânea de classe média alta, que se destaca pela sua rede hoteleira. Neste *Wardriving* foram detectadas cento e noventa e uma redes sem fio, das quais cinquenta e uma estavam abertas sem nenhum tipo de mecanismo de segurança e suscetíveis à invasão, enquanto cento e quarenta encontravam-se fechadas com algum tipo de mecanismo de segurança.

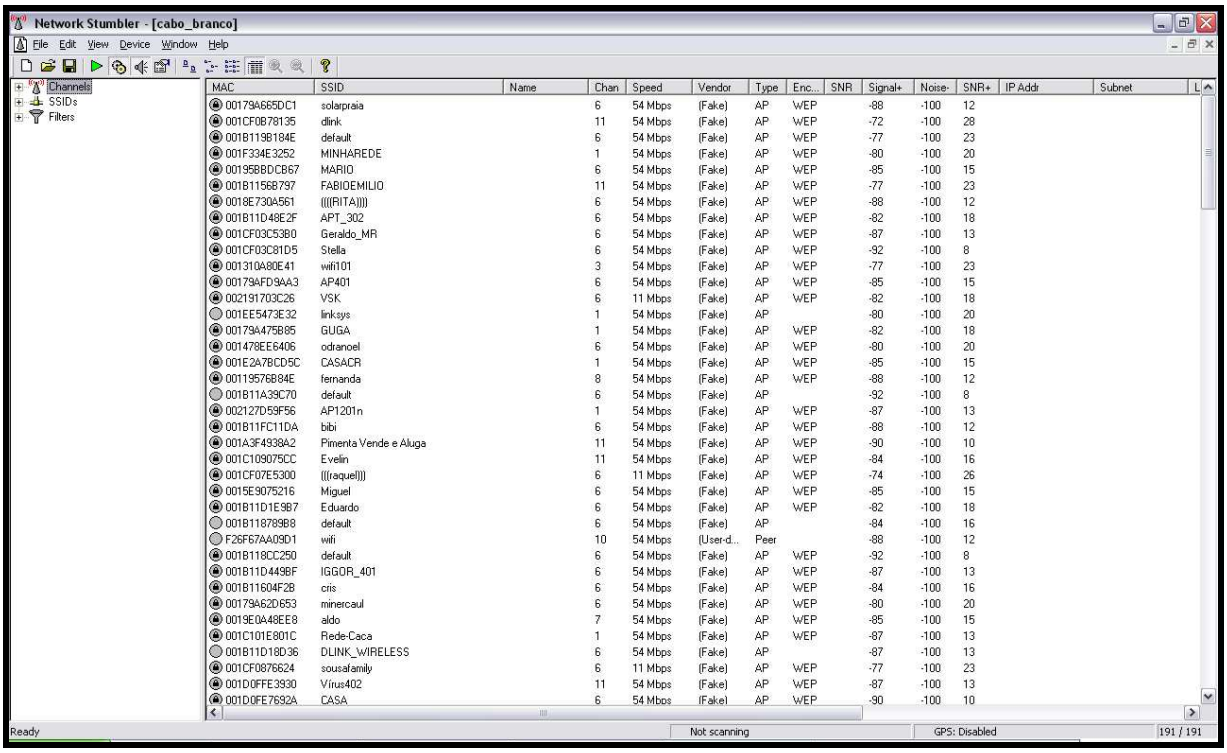

Figura 20. Ferramenta *Netstumbler* usada para rastrear as redes do bairro do Cabo Branco

O mapeamento destas redes estão ilustradas nas figuras 31 à 55 na parte de apêndices, pois onde se pode visualizar a realizada das redes destes bairros rastreados.

Nessa pesquisa, analisou-se o número de redes abertas, protegidas com padrão WEP ou WPA. Decidimos analisar esses tipos de redes, para identificar a dificuldade em fazer um acesso indevido. Então, através de um cenário montado com as realidades encontradas nas ruas, foi utilizado um laboratório para verificar e testar a usabilidade e facilidade das técnicas de invasão em redes *wireless* que estão disponíveis na internet e na literatura.

Segue abaixo o fluxograma desde a montagem do cenário aos testes realizados em laboratório.

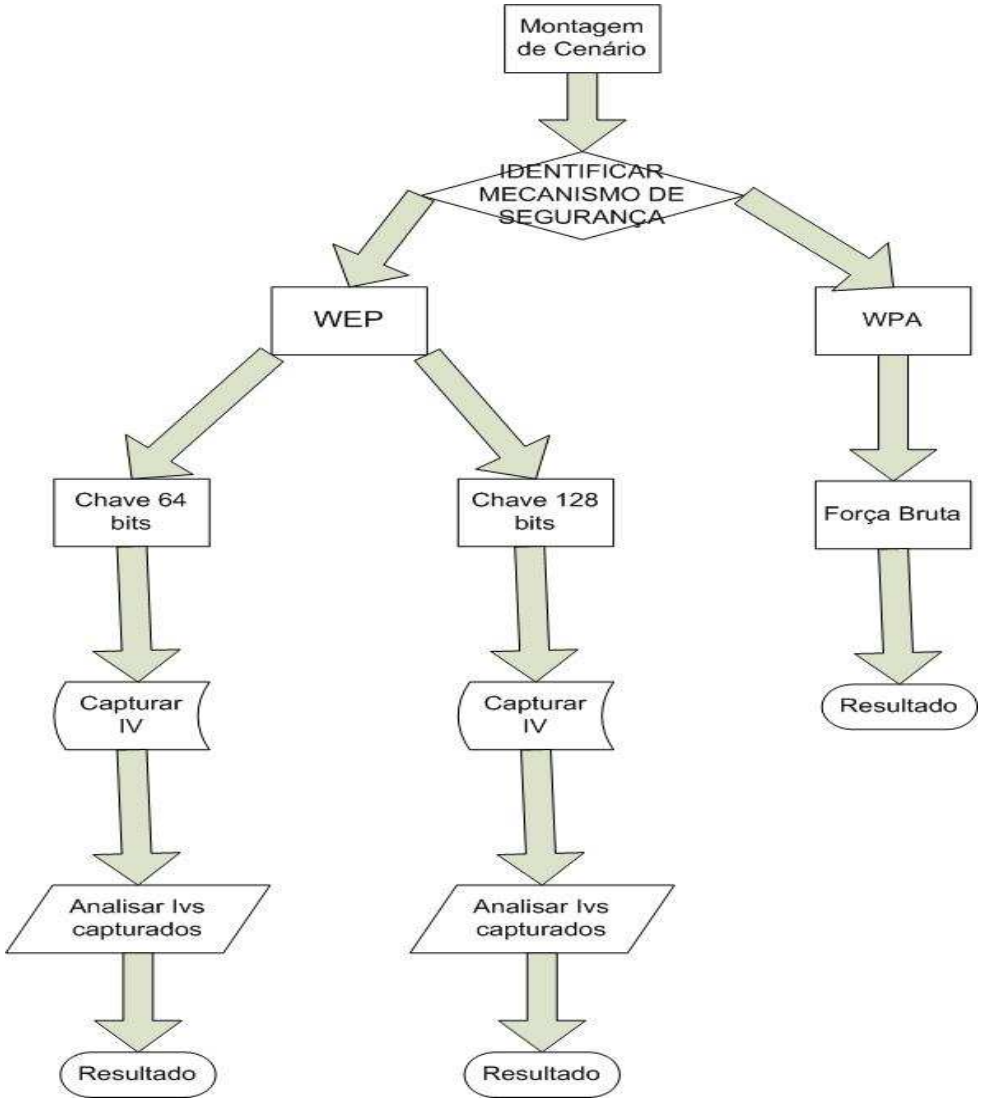

Figura 21. Fluxograma das atividades em laboratório

Seguindo o fluxograma das atividades, o primeiro passo foi montar um cenário que simulasse uma rede *wireless* em pleno tráfego e uma máquina invasora para capturar os pacotes, vetores de inicialização e quebrar as suas criptografias. Na rede *wireless*, foram testados os padrões WEP 64, WEP 128, WPA – TKIP, WPA – AES, WPA + Mac Filter. Nesse cenário, foram utilizados quatro máquinas e um concentrador *wireless*. As máquinas utilizadas foram: um *notebook* de modelo SEMP TOSHIBA de processador AMD Turion64 X2 com 2 Gb de memória RAM e placa Wireless de *chipset* Broadcom, um *notebook* de modelo HP de processador Pentium 4 com 1Gb de memória RAM e placa wireless de *chipset* Broadcom, um *notebook* de modelo HP de processador Pentium 4 com 1Gb de memória RAM e placa rede wireless de *chipset* Intel e um

desktop de processador Pentium 4 com 2Gb de memória RAM e um adaptador USB *wireless* de *chipset Ralink*. Nesse cenário foram usados três modelos de concentradores, pois existia a dúvida se a marca ou modelo influenciava quanto à segurança ou a facilidade de ser invadido.

Vejamos na figura 22, como foi montada a estrutura do cenário de teste de acesso indevido.

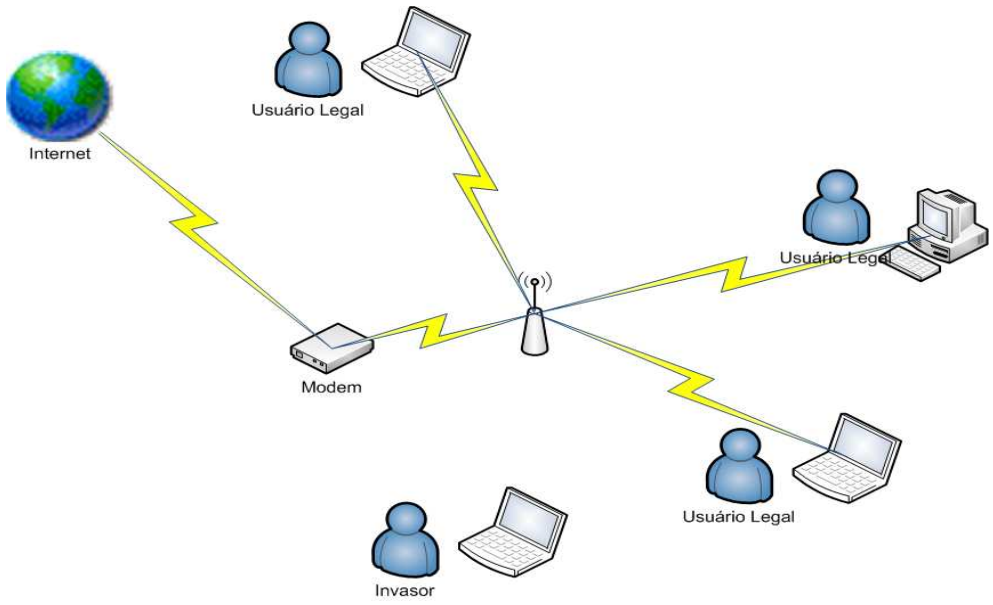

Figura 22. Cenário de testes de invasão

Ainda na montagem do cenário, o próximo passo foi deixar três máquinas conectadas ao concentrador *wireless*, baixando arquivos da internet com a média de volume de 4Gb e trocando dados de pastas compartilhadas entre si.

O último passo da montagem foi preparar a máquina que testará as vulnerabilidades; esse equipamento funcionou como *man-in-the-middle*, que é o ato de tentar interceptar o tráfego da rede sem ser identificado. Essa máquina foi equipada com o sistema operacional *backtrack* 3, que já vem com vários *softwares* com testes de penetração; nesse laboratório, foram utilizados o *kissmet*, *airodump-ng*, *aireplay-ng, aircrack-ng, airmon-ng*.

As ferramentas citadas acima foram exploradas da seguinte maneira:

O comando *kismet* foi utilizado para habilitar o modo monitor da interface de rede sem fio, e identificar as redes disponíveis com os seus SSID, BSSID, Canal,

criptografia usada e sua infra-estrutura. Como podemos verificar na ilustração da figura 23.

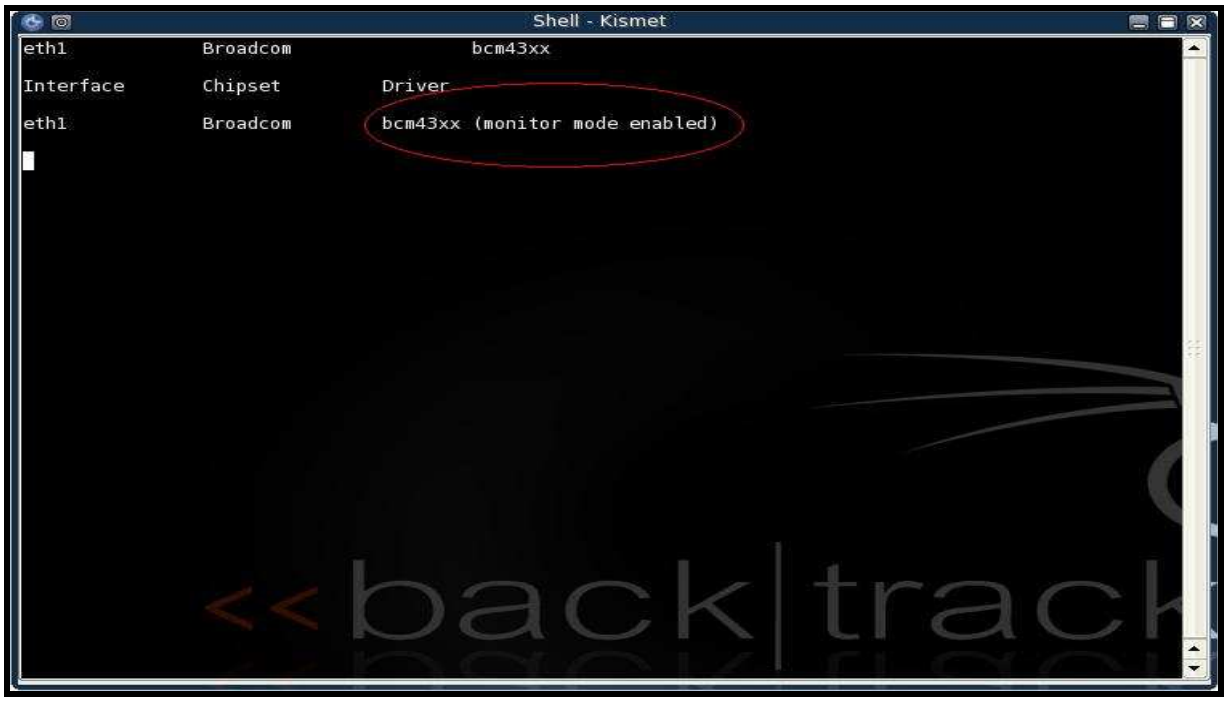

Figura 23. Inicializando o *kismet* ativando modo monitor

Após habilitado o modo monitor da interface de rede, a figura 24 mostra a ferramenta *kismet* em pleno funcionamento.

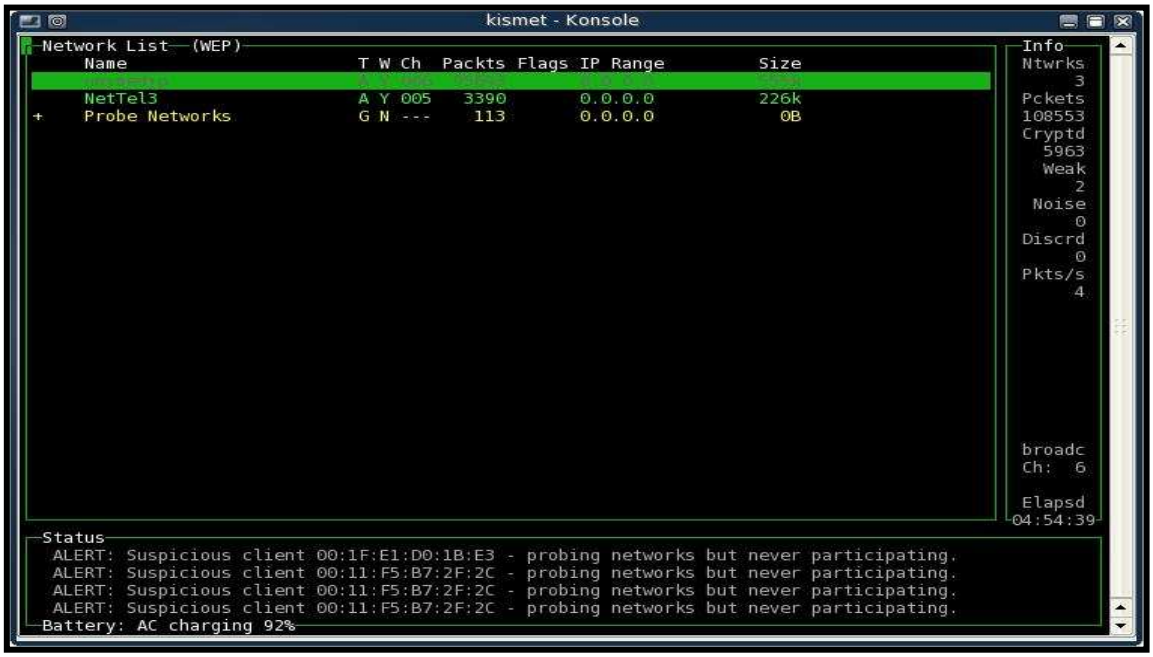

Figura 24 *kismet* ativado identificando as redes

Identificadas as redes que seriam usadas como alvo de teste de vulnerabilidades, foi feito então o uso da ferramenta *airodump* para capturar os IVs, gerando então um arquivo, que serviu para ser analisado pelo *aircrack*, com o intuito de ter o acesso indevido quebrando as chaves.

Apesar das máquinas com os usuários legais estarem gerando tráfego, a máquina de testes de vulnerabilidades utilizou uma ferramenta chamada *airreplay* que tem uma opção de gerar o próprio tráfego para facilitar a captura mais rápida dos IVs. Na figura 25, é ilustrado com o destaque em vermelho o tráfego gerado pelo airreplay.

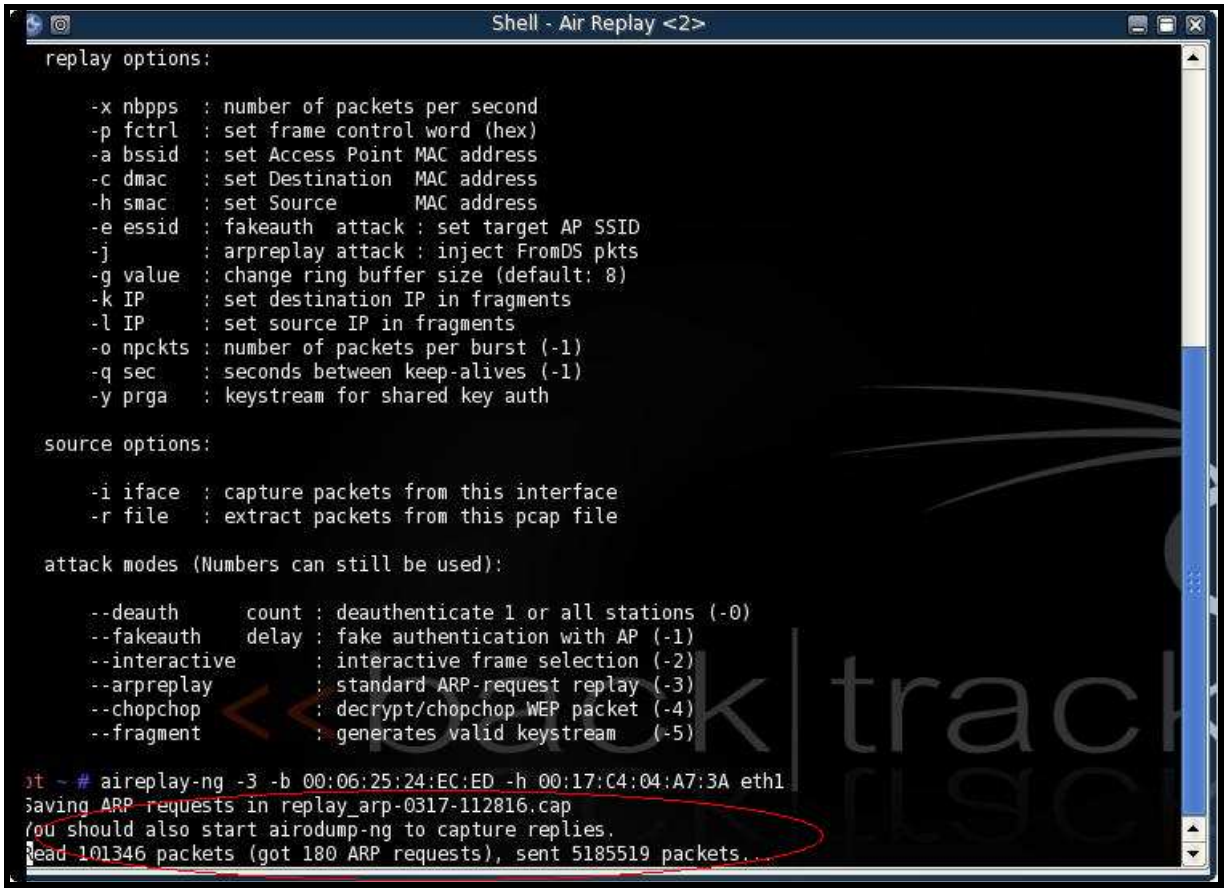

Figura 25. aireplay gerando tráfego

Com o *aircrack* em mãos, estamos na última etapa que é constituída do arquivo com os pacotes capturados pelo *airodump*, contendo os vetores de inicialização, e obter o resultado, que seria quebrar as chaves e ter o acesso indevido.

Diante dos testes realizados com as ferramentas anteriormente citadas no padrão WEP 64 e 128 *bits*, foi encontrada a primeira dificuldade ao se detectar que o processo de captura de vetores de inicialização é muito demorado, pois neste primeiro teste foi preciso um tempo aproximado de três horas e quinze minutos (03:15) para se capturar os IVs e quebrar a segurança, onde o tráfego de dados era intenso. No segundo teste com WEP 128, que durou mais de vinte sete horas, ilustrado na figura 26, pode ser visto o detalhe do tempo destacado em vermelho. Essas ferramentas tornaram possível a quebra, mas inviável a sua prática, pois se trata de uma atividade demorada e imprevisível. Pois a mesma chave WEP 64 bits que foi quebrada no início dos testes, em uma segunda tentativa não foi obtido o mesmo sucesso. Então se entende que na análise dos IVs é feita através de análise de freqüência. A análise de frequência é o método de substituir códigos por dados reais que se repetem com frequência.

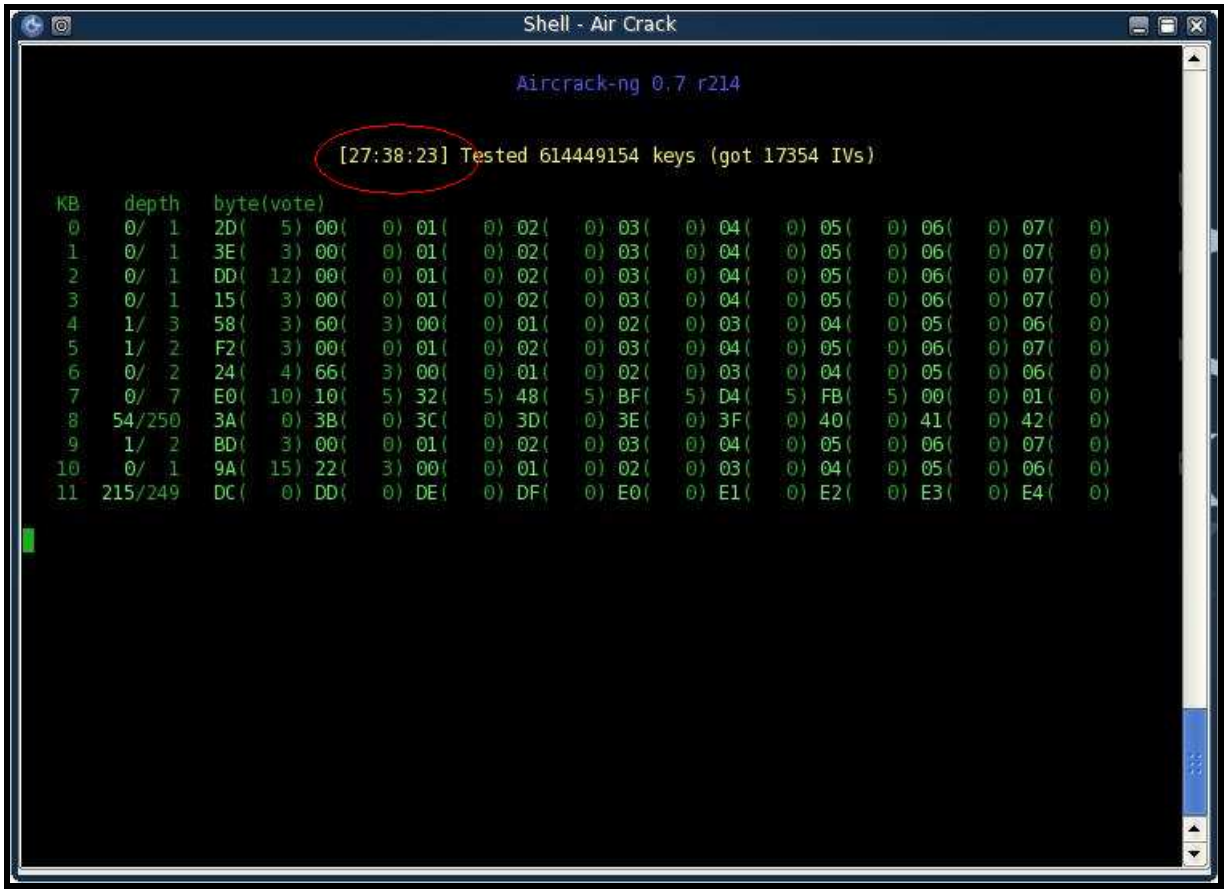

Figura 26. *Aircrack* tentando quebrar uma senha há mais de 27 horas

No que diz respeito ao WPA, como já foi descrito anteriormente no capítulo sobre mecanismos de segurança, esse padrão possui características de segurança superiores ao WEP, mas, segundo algumas literaturas, ainda sim apresenta algumas vulnerabilidades e de menos impacto que o WEP. Apesar de não ser uma falha específica do protocolo WPA, o uso de senhas pequenas e de fácil adivinhação, pode ser explorada através do ataque de força bruta ou de dicionário de dados.

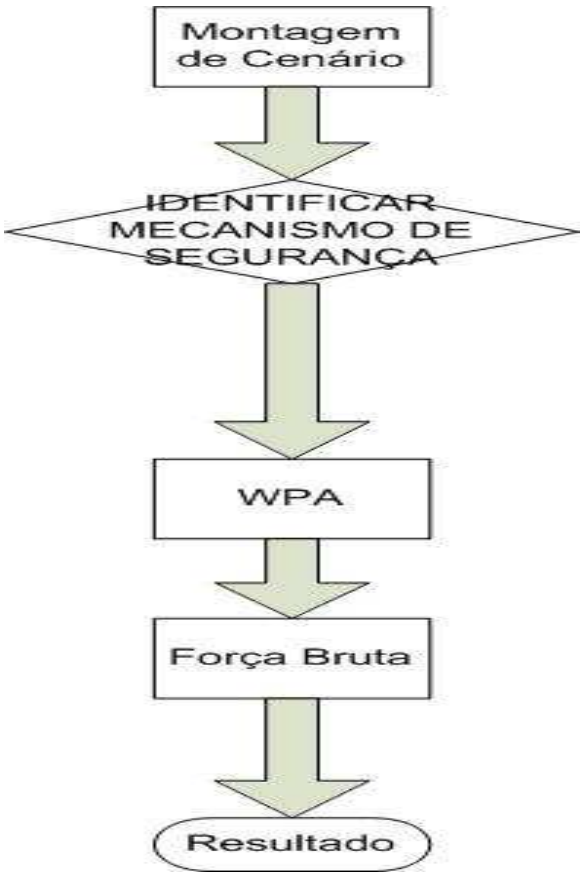

Figura 27. Fluxograma de tentativa de acesso indevido a chaves WPA

Nos testes realizados no nosso cenário, foi utilizada uma ferramenta chamada de *John the ripper* que tem como funcionalidades o acesso indevido através de força bruta ou ataque de dicionário. Em tentativas com senhas pequenas e de fácil combinação, como: acb123, 123456, adcdef, foi constatado que é possível fazer este tipo de ataque, mas no caso de senhas grandes e com combinações de outros caracteres, já não houve o mesmo sucesso na exploração desta vulnerabilidade. Então apesar de existirem pequenas fragilidades nesse protocolo, o WPA pode ser considerado seguro, pois baseam-se nas notas de

aulas de criptografia moderna do M.S.c Marcio Nogueira, conclui-se que: “Um sistema é dito seguro quando só é possível vencê-lo através de força bruta, e mesmo assim sendo inviável pelo tempo necessário para sua descoberta.” (**NOGUEIRA,** 2008, p.6)

CONCLUSÃO

Esse trabalho apresenta evidências concretas de que atualmente os administradores de redes sem fio evoluíram na preocupação com segurança destas. A pesquisa mostra claramente que a grande maioria das redes *wireless* está usando algum tipo de padrão de segurança, como, WEP ou WPA, sabendo-se,contudo não significa que a segurança é cem por cento, pois a literatura e os fatos relatados pelos meios de comunicação confirmam que a segurança das redes *wireless* é possível de serem quebradas.

Considerando a cidade de João Pessoa, as áreas pesquisadas representam um pequeno espaço amostral. Entretanto, em função da importância estratégica das regiões estudadas, onde se concentram estabelecimentos comerciais, órgãos públicos e residências, constata-se que há uma preocupação por parte dos administradores de redes *wireless* com relação à segurança da informação. O mesmo estudo foi feito na cidade de São Paulo no ano de 2004, onde a situação era grave e inversa, pois a maioria das redes sem fio era aberta, com riscos reais e imediatos.

Nesse estudo foi detectado um total de setecentos e trinta e seis redes sem fios, nos bairros de Jaguaribe, Torre, Centro, Bairro dos Estados, Cabo Branco e Tambaú. Como pode ser analisado na figura 28, que ilustra o total de redes rastreadas.

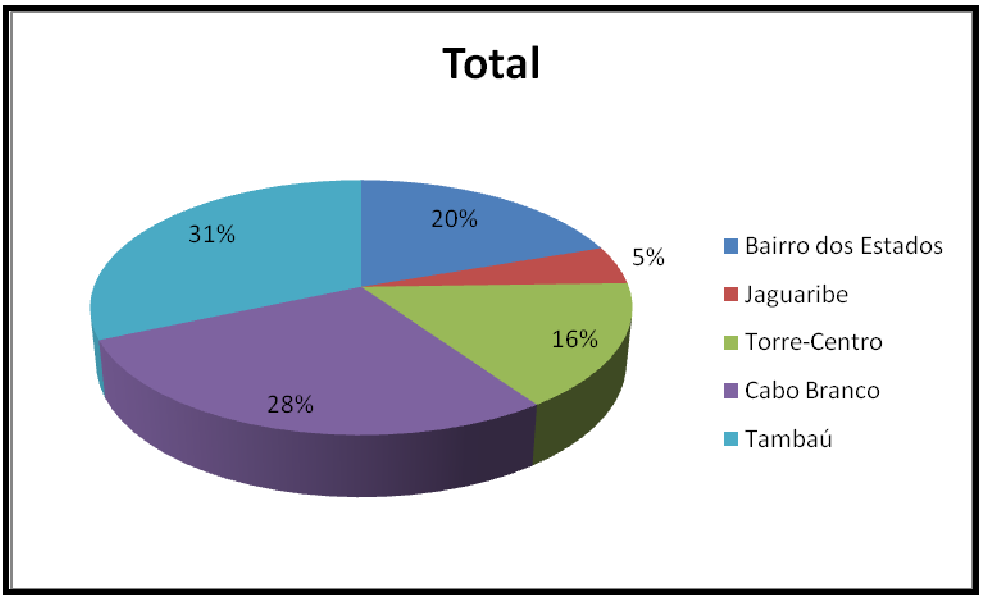

Figura 28. Dados estatístico com o total de redes sem fio

Na figura 29, ilustram-se os dados estatísticos em uma amostragem para redes abertas sem algum tipo de mecanismo de segurança. Tornando-se um alvo fácil daqueles que queiram tirar proveito, explorando-as.

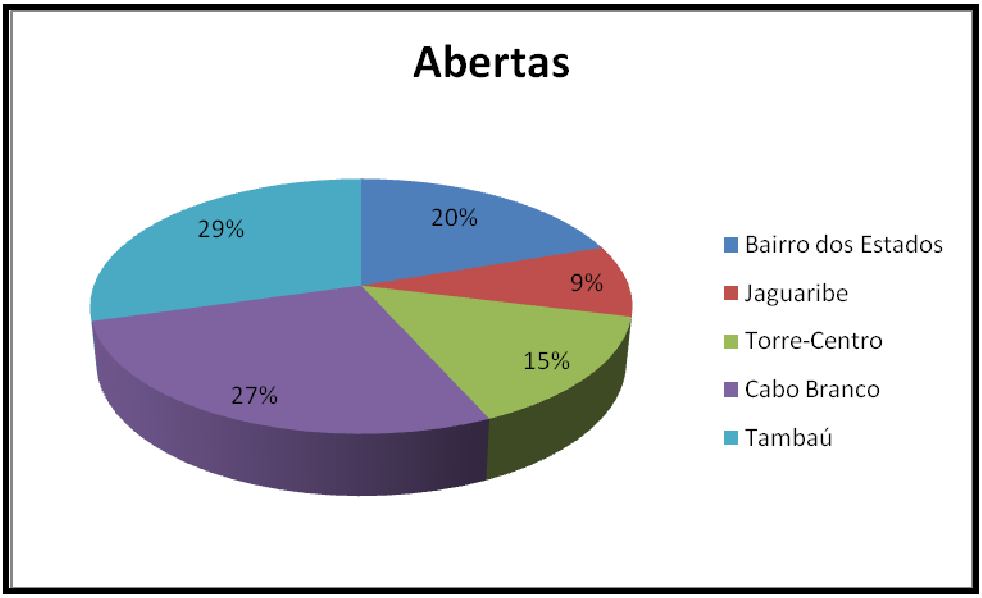

Figura 29. Dados estatísticos com percentual por bairro de redes abertas

Na figura 30, mostram-se os dados estatísticos com número de redes fechadas, e ao comparar com os da figura 29 nota-se, que estes números das redes fechadas que estão usando algum tipo de mecanismo de segurança é superior aos das redes abertas.

Com base nesses dados, conclui-se que os administradores de redes sem fio estão mais cientes da real importância da segurança da informação.

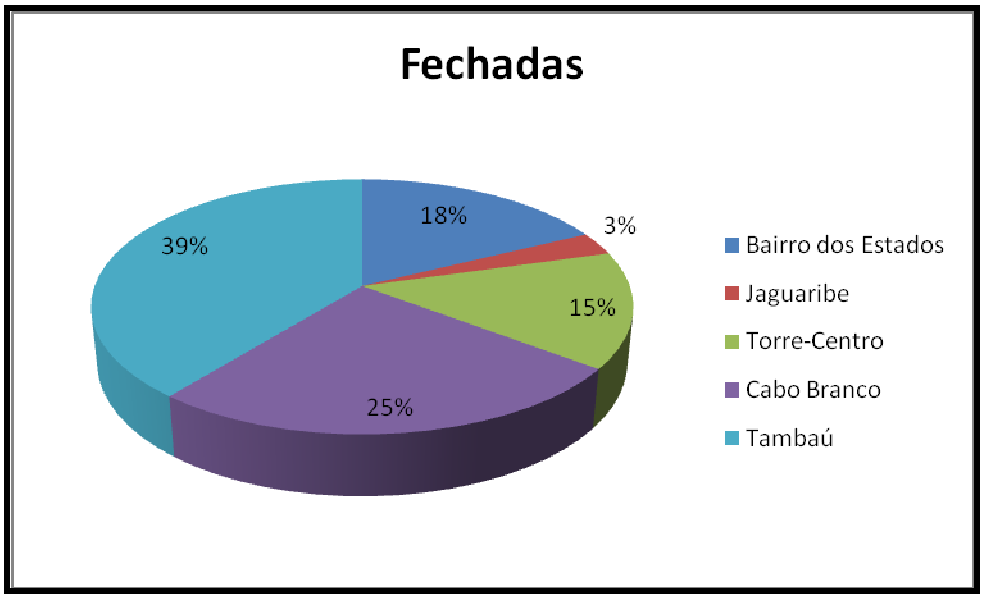

Figura 30. Dados estatísticos com percentual de redes fechadas

Nessa pesquisa, além do *Wardriving*, um laboratório de testes foi montado para se constatar as fragilidades das redes sem fio e o quanto seria viável essa prática. Com os testes conclui-se que essas ferramentas apresentam baixa usabilidade e facilidade. Nos testes de vulnerabilidades *wireless* com padrão WEP, constatou-se que são possíveis de serem quebradas, mas com um agravante da demora de captura dos IVs, pois a sua demora está relacionada à disponibilidade de um trafego intenso para poder capturá-los.

E quanto ao padrão WPA, verificou-se que é mais difícil de explorar as suas fragilidades, já que o problema não está no protocolo, pois, a sua fragilidade está no uso de senhas pequenas e de fácil combinação que podem ser exploradas pela prática de força bruta ou ataque de dicionário.

Então diante do estudo feito, conclui-se que os administradores de redes sem fio estão mais conscientes e preocupados com a segurança da informação. E que as redes *wireless* tem as suas fragilidades de segurança, mas a sua prática de explorar as suas vulnerabilidades com suas respectivas ferramentas torna-se uma atividade inviável.

Apesar de ser um estudo de conclusão de curso, para obtenção do título de especialista em segurança da informação, esse trabalho deve servir como um

sinal de alerta no sentido de uma adequação dos sistemas existentes, seja no sentido do aprimoramento e evolução tecnológica que eventualmente se torne disponível, seja no correto treinamento e capacitação dos administradores de redes para lidarem com esse problema. E esse último caso, parece estar mudando o perfil da administração, como mostra a indicação dos resultados aqui apresentados.

REFERENCIA BIBLIOGRAFICA

- ABNT NBR Iso Iec 17799 – 2005, p. 9, 49, 57, 72, 74, 82.

- BABOO, http://www.baboo.com.br/absolutenm/templates/content.asp?articleid=30215&zoneid=276&resumo. Acesso em 04 nov. 2008.

- CARMONA, Tadeu; **Universo Hacker –** 2. Ed., 2006, Digerati Books , p. 112.

- DUDRAK, John C. Info Exame, Surfe no Wi-Fi enquanto dura – Editora Abril, 2004, p.38.

- FORTES, Débora. **Info Exame**, Wi-Fi de a a g, as redes sem fio entram nas empresas, nos hotéis, nos escritórios – Editora Abril, 2004, p.60

- INFO, Revista info da editora abril, http://info.abril.com.br/aberto/infonews/022001/05022001-14.sh, Acesso em 04 nov 2008.

- HURLEY, Chris; **PUCHOL**, Michael; **ROGERS** Russ and **THORNTON,** Frank.

- MICROSOFT, TechNet, Integridade e criptografia de dados do WPA, http://technet.microsoft.com/pt-br/library/bb878126.aspx , Acesso em 20 jan 2009.

- NAKAMURA, Emílio Tissato. **Segurança de Redes em Ambientes Cooperativos** / Emílio Tissato Nakamura, Paulo Lício de Geus. - Novatec Editora, 2007, p. 165, 166, 171, 172, 177 - 179.

- NOGUEIRA, Márcio, Histórico e Evolução da Criptologia – Slides de notas de aulas, 2008, p.5 e p.6

- PORTALIMPRENSA, Terroristas indianos usam redes WiFi desprotegidas para enviar ameaças e planejar atentados, http://portalimprensa.com.br/portal/ultimas_noticias/2009/01/14/imprensa25437.shtml , Acesso em 22 abr. 2009.

- RNP - Rede Nacional de Pesquisa. **Segurança em Redes sem Fio**, 2007, p. 237 - 251.

- RUFINO, Nelson Murilo de O. **Segurança em Redes sem Fio –** Editora Novatec, 2007, p.25.

- SANCHES, Carlos Alberto. **Projetando Redes WLAN** – Editora Érica, 2007, p.239.

- THINKER, Comunidade warchalking- https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2, Acesso em 30 out. 2008.

- TOMAS, Tom. **Segurança de Redes Primeiros Passos –** Editora Ciência Moderna, 2007, p. 263 - 191.

- VIASEG, Portal de Negócios, http://www.viaseg.com.br/noticia/1043-eua_usam_lata_de_batatas_fritas_para_procurar_falhas_em_redes.html, Acesso em 04 nov. 2008.

- WINSERV – Tecnologia da Informação, http://www.winserv.com.br/index.php?option=com_content&view=article&id=9&Itemid=15, Acesso em 20 jan. 2009.

-

BIBLIOGRAFIA CONSULTADA

- ANDRADE, Maria Margarida de. **Como Preparar Trabalhos para Cursos de Pós-Graduação** – Atlas, 7. Ed., 2008.

- CANSIAN, Adriano Mauro; **GRÉGIO,** André Ricardo Abed; **PALHARES,** Carina Tebar; **SOUZA,** Aleck Zander Tomé de; **FILHO,** Antônio Montes. **Falhas em Políticas de Configuração: uma análise do risco para as redes sem fio na cidade de São Paulo** – Anais do Simpósio de Segurança em Informática - 2004.

- HURLEY, Chris; **PUCHOL**, Michael; **ROGERS** Russ and **THORNTON,** Frank. **WarDriving & Wireless, Penetration Testing** – 2007.

- TANENBAUM, Adrew S. **Redes de Computadores –** Campos, 4. Ed.

- WarDriving: Drive, Detect, Defend: A Guide to Wireless Security – 2004.

APENDICES

	Redes abertas
	Redes com criptografia e mostrando o SSID
	Redes fechadas sem SSID

Quadro 1. Tabela de referência de segurança wireless

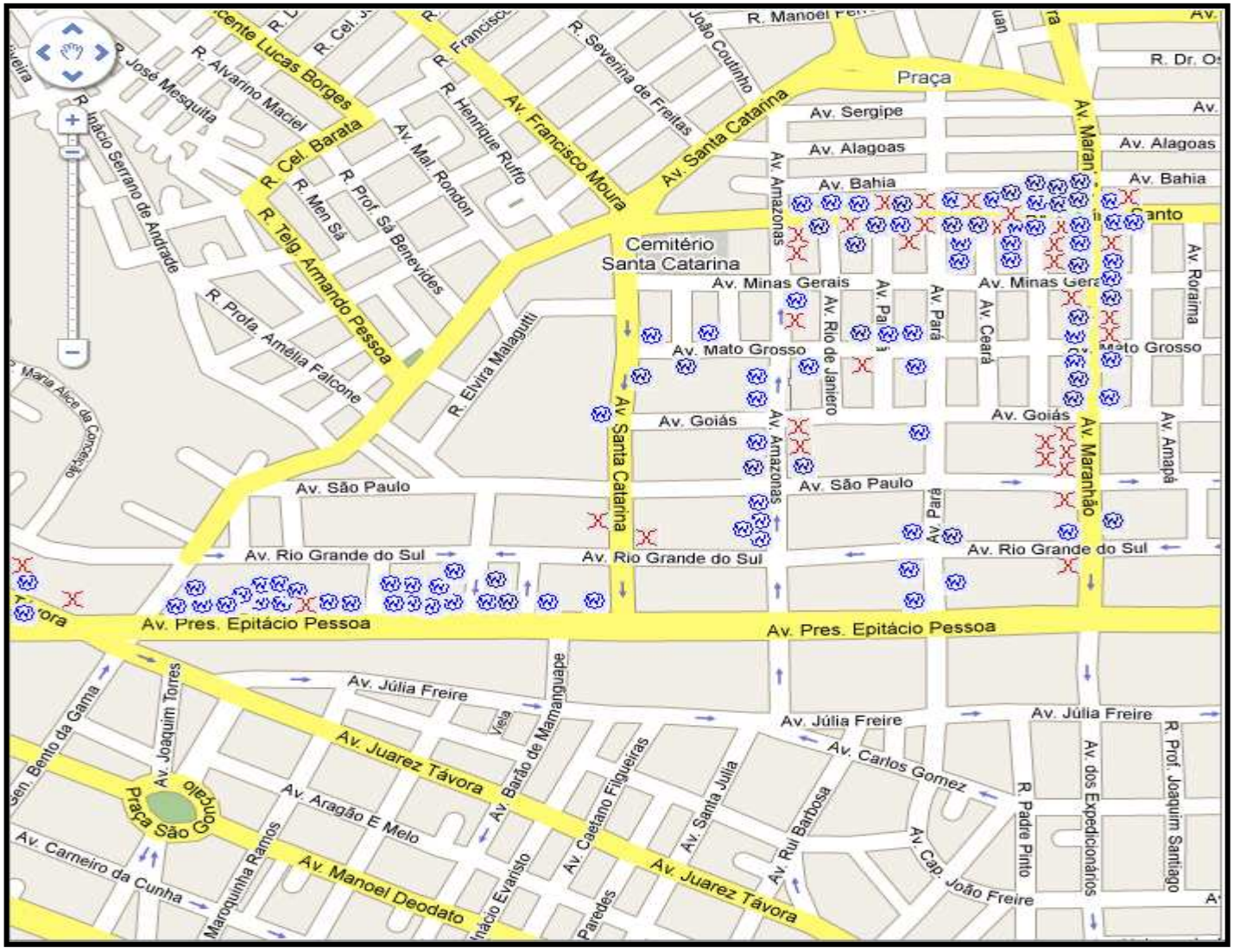

Figura 31. Wardrinving Bairro dos Estados

Figura 32. Locais de redes detectadas

Figura 33. Locais de redes detectadas

Figura 34. Locais de redes detectadas

Figura 35. Locais de redes detectadas

Figura 36. Locais de redes detectadas

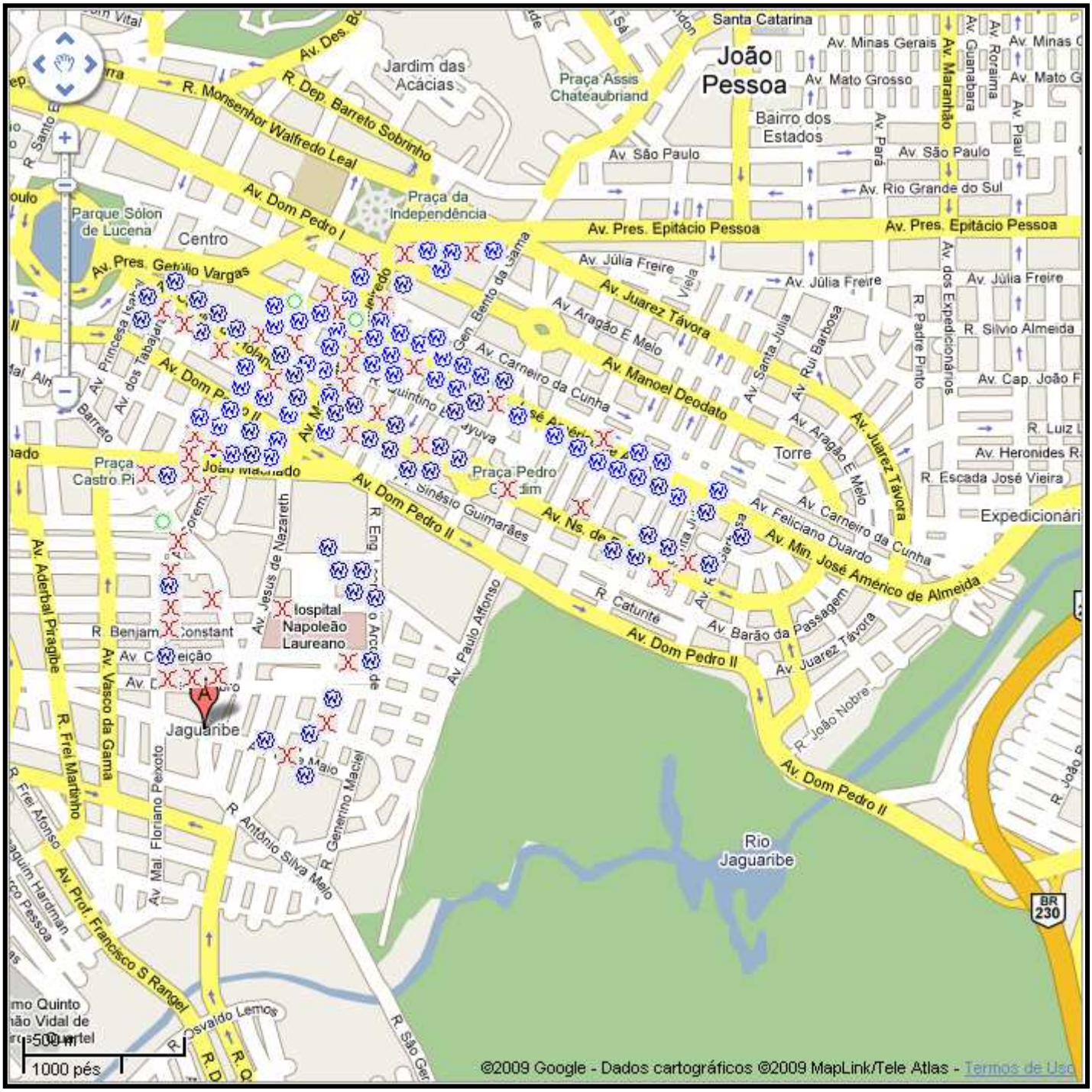

Figura 37. WarDrinving Jaguaribe - Centro

Figura 38. Locais de redes detectadas

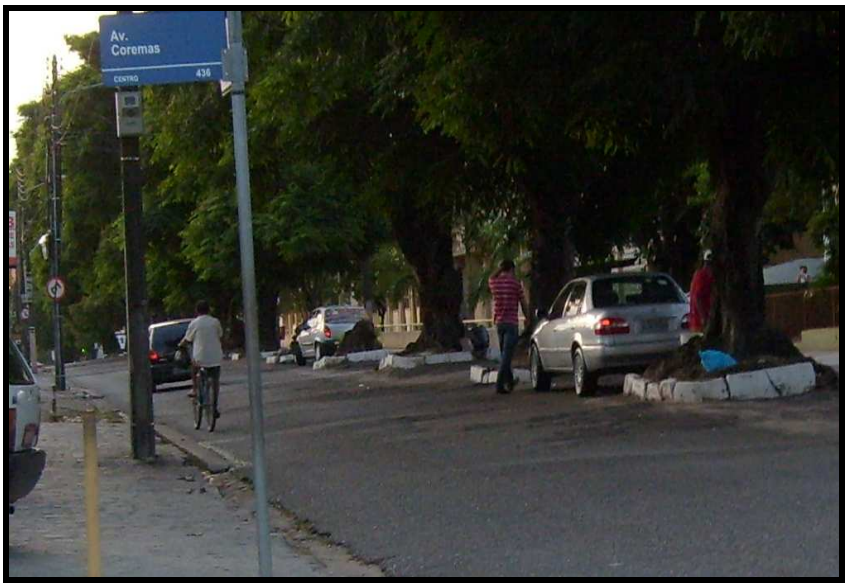

Figura 39. Locais de redes detectadas

Figura 40. Locais de redes detectadas

Figura 41. Locais de redes detectadas

Figura 42. Locais de redes detectadas

Figura 43. Locais de redes detectadas

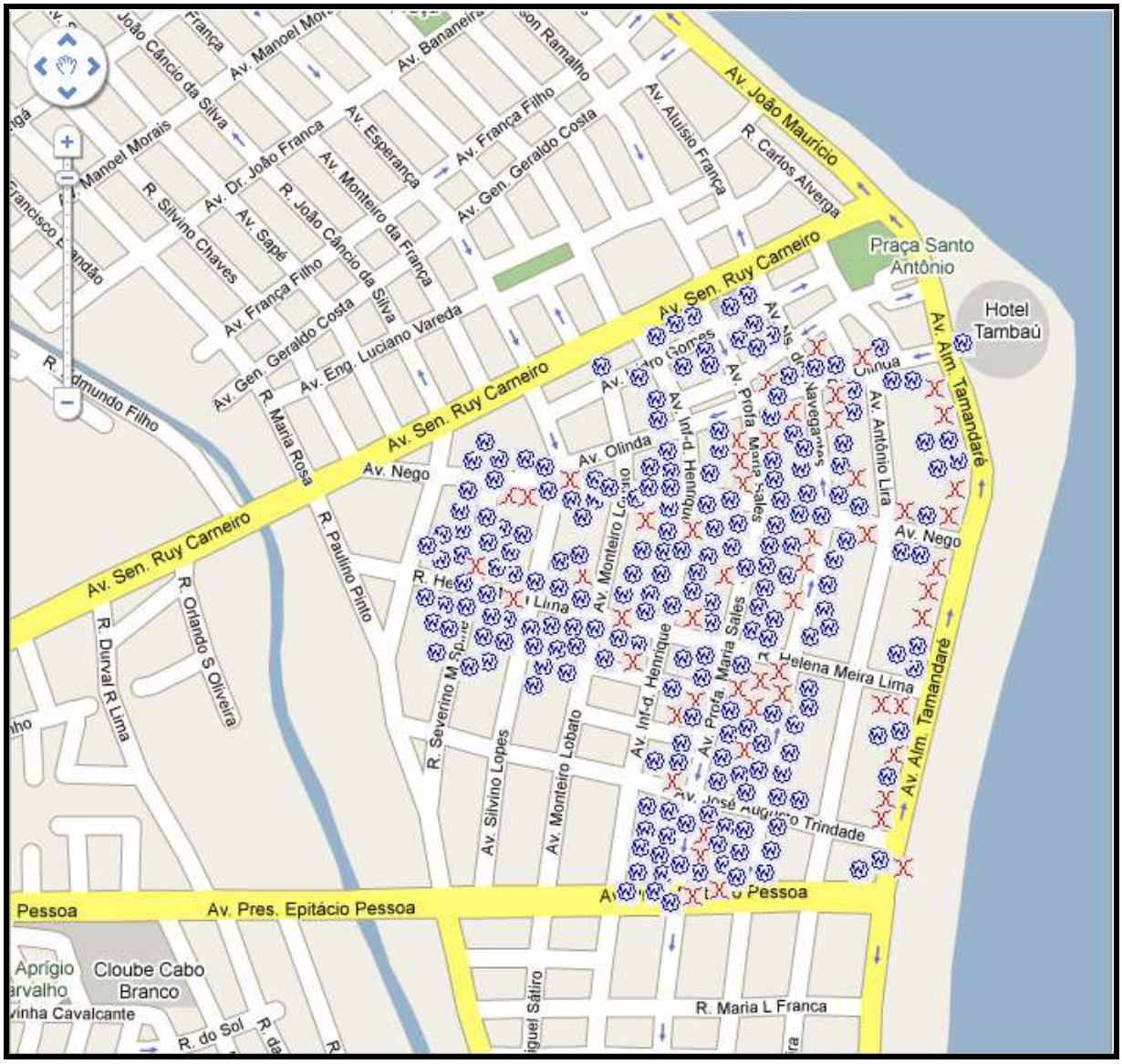

Figura 44. WarDriving Tambaú

Figura 45. Locais de redes detectadas

Figura 46. Locais de redes detectadas

Figura 47. Locais de redes detectadas

Figura 48. Locais de redes detectadas

Figura 49. Locais de redes detectadas

Figura 50. Locais de redes detectadas

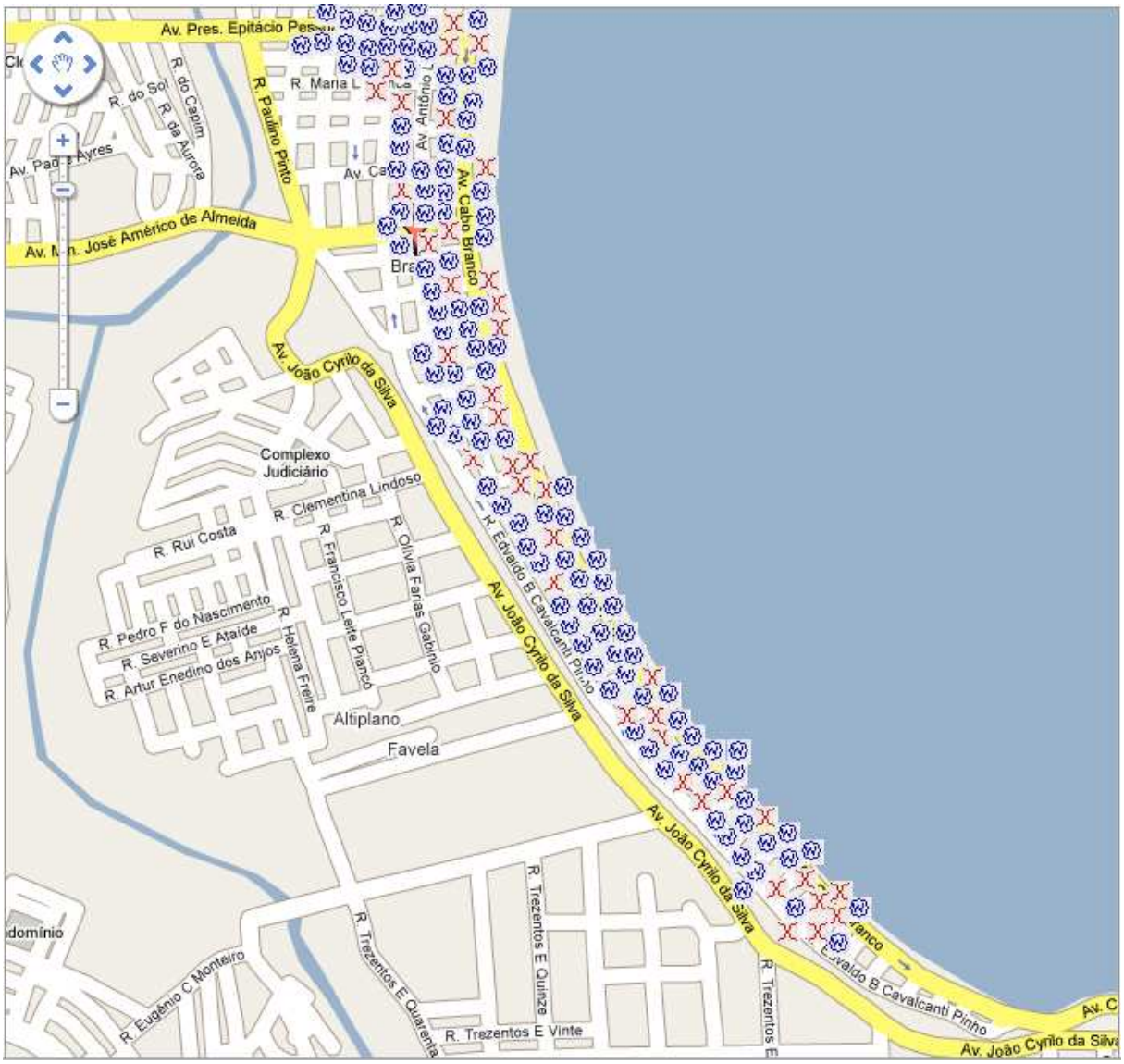

Figura 51. WarDriving Cabo Branco

Figura 52. Locais de redes detectadas

Figura 53. Locais de redes detectadas

Figura 54. Locais de redes detectadas

Figura 55. Locais de redes detectadas