CENTRO UNIVERSITÁRIO FEEVALE

RICARDO DALMORO BASSO

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Novo Hamburgo, junho de 2009.

RICARDO DALMORO BASSO

rdbasso@gmail.com

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Professor orientador: Vandersilvio da Silva

Novo Hamburgo, junho 2009.

AGRADECIMENTO

Gostaria de agradecer a todos que contribuíram para a realização deste trabalho, em especial aos meus pais, por toda dedicação direcionada a minha educação e formação profissional; a minha irmã que me concedeu muito apoio; a todos os amigos que fazem parte da minha vida.

RESUMO

Devido à crescente necessidade por mobilidade houve uma vasta expansão das redes sem fio, sendo estas, tecnologias que oferecem a promessa de transferência de dados cada vez mais rápidas e de baixo custo através de ligações bastante abrangentes. Muito se tem alcançado no que se diz respeito a montar ou controlar estas redes, mas as ferramentas fundamentais que permitem a confiabilidade e a autenticidade dos dados transportados ainda não estão bem explicadas. Comunicação sem fio no que diz respeito à segurança ainda é um enorme desafio para investigação. Os protocolos conhecidos hoje no mercado e que são atualmente os mais utilizados para segurança de redes sem fio são o WEP, WPA WPA2. Diversos problemas com estes protocolos já são conhecidos. O presente trabalho pretende aprofundar os estudos no que diz respeito à confiabilidade destes protocolos, fazer uma analise de viabilidade em um ambiente real, além disso, elaborar um relatório para analise de vulnerabilidades das redes sem fio.

Palavras-Chave: Análise, Vulnerabilidades, *Wireless*

ABSTRACT

Due to the increasing necessity for mobility it had a vast expansion of wireless networks, being these, technologies that offer the promise of data transfer increasingly fast and low-cost connections through quite comprehensive. Much has been achieved as concerns mount or control these networks, but the basic tools that enable the trustworthiness and the authenticity of data stored has not yet clearly explained. Wireless communication in regard to security is still an enormous challenge for inquiry. The protocols known in the market today and are currently used mostly for the security of wireless networks are the WEP, WPA and WPA2. Several problems with these protocols are already known. This final paper aims to deepen the studies regarding the reliability of these protocols, to analyze the feasibility in a real environment and also prepare a report for analysis of vulnerabilities of wireless networks.

Key Words: Analysis, Vulnerabilities, Wireless

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES	Encryption Standard (Padrão de Criptografia Avançada)
AP	Access Point (Ponto de Acesso)
ARP	Address Resolution Protocol (Protocolo de Resolução de Endereços)
BSS	Basic Service Set (Conjunto de Serviços Básicos)
CRC-32	Cyclic Redundance Check 32 (Checagem de Redundância Cíclica 32)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuração de Servidor Dinâmico)
DoS	Denial of Service (Negação de Serviço)
DSSS	Direct Sequence Spread Spectrum (Espalhamento Espectral em Seqüência Direta)
EAP	Extensible Authentication Protocol (Protocolo de Autenticação para o acesso a rede)
ESS	Extended Service Set (Conjunto de Serviços Estendido)
ESSID	Extended Service Set Identifier (Identificador da rede)
FHSS	Frequency – Hopping Spread Spectrum
GPS	Global Positioning System (Sistema de Posicionamento Global)
HTML	HyperText Markup Language (Língua de Marcação de Hipertexto)
HTTP	HyperText Transfers Protocol (Protocolo de Transferência de Hipertexto)
IDS	Intrusion Detection System (Sistema de Detecção de Intruso)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Elétricos e Eletrônicos)
ICV	Integrity Check Value
IP	Internet Protocol (Protocolo Internet)
IV	Initialization Vector (Vetor de inicialização)
LAN	Local Area Network (Rede de Computadores Local)

LLC	Logical Link Control (Controle Lógico de Enlace)
MAC	Media Access Control (Controle de Acesso ao Meio)
PC	Personal Computer (Computador Pessoal)
QoS	Quality of Service (Qualidade de Serviço)
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher Version 4
SSID	Service Set Identifier
TCP	Transmission Control Protocol (Protocolo de Controlo de Transmissão)
TKIP	Temporal Key Integrity Protocol (Protocolo Temporal de Integridade de Chave)
USB	Universal Serial BUS
VPN	Virtual Private Network (Rede Privada Virtual)
WAN	Wide Area Network (Rede Remota de Computadores)
WEP	Wired Equivalency Privacy (Privacidade Equivalente ao sistema com cabo)
Wi-Fi	Wireless Fidelity (Fidelidade Sem Fio)
WIRELESS	Sem Fio
WLAN	Wireless Local Area Network (Redes Locais Sem Fio)
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WWW	World Wide Web (Rede de Alcance Mundial)
WWAN	Wide Area Network (Rede de longa Distância sem fio)

SUMÁRIO

INTRODUÇÃO

Com o avanço da comunicação nos últimos anos, a todo o momento, estão surgindo novas tecnologias de redes *wireless*, visando a atender as necessidades dos usuários com a melhor qualidade de transferência e segurança possíveis. Ao longo do tempo muito se evoluiu até chegar às redes de computadores da atualidade. As empresas e universidades estão apostando cada vez mais nesta tecnologia considerada revolucionária.

O crescimento da tecnologia *wireless* em ambientes empresariais vem acontecendo de maneira rápida. Em 2007, segundo o Instituto Gartner, o uso desta modalidade de redes aumentaria cerca de 64% nas organizações. Entre os participantes da pesquisa 44% citaram que a mobilidade iria alavancar a produtividade. Apesar do aumento do numero de adeptos as redes sem fio, 70% dos entrevistados relataram que não utilizam nenhum tipo de proteção contra invasores. Logo, a segurança torna-se o maior motivo de preocupação. http://www.silicon.com/

Quando o autor deste estudo ingressou em seu curso superior no ano de 2001, pouco se falava em conexões sem fio, tão pouco poderia prever a vasta expansão destes ambientes. Atualmente encontramos pontos de acesso *wireless* nos mais variados espaços sociais, desde o Aeroporto Internacional, até as praças públicas. O baixo custo e a qualidade do sinal oferecido tornam-se um grande atrativo para disseminar esta tecnologia.

Atualmente o autor atua profissionalmente em uma Prefeitura Municipal do interior do Estado, onde muito se fala em cidade digital. É compreendida por uma conexão de alta velocidade que chega a um ponto, via link de uma operadora de telefonia, e se distribui no município por uma rede sem fio a lugares como escolas, postos de saúde e órgão da administração municipal. Diversos tipos de informações trafegam diariamente por essas redes, transmitindo desde dados confidenciais como folha de pagamento dos colaboradores e prontuários médicos, como simples arquivos de e-mail.

Estas redes sem fio, de fácil montagem e simples configuração, levantam uma dúvida quando se pensa em sigilo dos dados trafegados. O mercado atual disponibiliza diversos modelos de equipamentos, de diversos fabricantes. Todos estes, tendo como seus protocolos padrões de segurança WEP e WPA.

Redes *wireless* podem usar criptografia para proteger o tráfego entre a estação cliente e a base. Este ponto de acesso pode ser configurado para usar uma chave autenticadora que é armazenada e transmitida quando o cliente tenta se conectar. A maioria esmagadora das redes sem fio utiliza como protocolo de segurança o WEP, que suas falhas já são conhecidas e com algumas descobertas recentes permitiram que passassem de horas para minutos o tempo levado para sua quebra.

> Existem várias ferramentas desenvolvidas para descobrir chaves WEP, com maior ou menor grau de eficiência. Utilizam, em geral, uma combinação de força bruta, ataques baseados em dicionário e exploração de vulnerabilidades conhecidas. Por outro lado, chaves simples são mais fáceis de ser quebradas, independentemente da eficácia da ferramenta, e chaves-padrão não necessitam sequer de ferramentas para isso. (RUFINO, 2005 p.101)

Tendo em vista estes já divulgados problemas de segurança, o protocolo WEP caiu em descrédito. Antes do fechamento do padrão 802.11i o Wi-Fi Alliance liberou o protocolo WPA. Diversas mudanças e avanços foram incorporados a este novo protocolo, além de possuir diversos modelos que são moldáveis as necessidades do ambiente.

> Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Porém, dados a diversidade e os ambientes onde uma rede sem fio pode existir (ambientes domésticos, pequenos escritórios, pequenas e grandes indústrias etc.), pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades. (RUFINO, 2005 p.35)

Embora o protocolo WPA seja mais seguro que seu antecessor WEP, algumas vulnerabilidades de seu método já são conhecidas nos dias de hoje, e estão reportadas em artigos e sites de busca na internet. É muito importante para seus adeptos, que sejam conhecidas estas informações para que possam se precaver em caso de qualquer tentativa de invasão. Entretanto até onde os dados criptografados por estas ferramentas estão realmente seguros? È possível garantir a integridade destas informações?

Para comprovar estas questões relacionadas à segurança será feito um estudo sobre ferramentas e técnicas que podem ser usadas em algum tipo de ação maliciosa sobre essa rede

sem fio, além disso, será feito um experimento em ambiente real, onde poderemos ter uma verdadeira reposta para estas perguntas.

Após o estudo dos métodos será proposto um relatório para a análise de vulnerabilidade das redes sem fio, com os principais pontos que podem tornar estas redes sucessivas a ataques. Este relatório será aplicado na rede em questão para ser possível tirar as devidas conclusões.

1 REDES WI-FI

Neste capitulo será feito uma introdução as redes *wireless*, será apresentada as topologias disponíveis para a rede sem fio, alem de serem descritos os principais padrões do protocolo 802.11.

1.1 Conceito

As redes denominadas Wi-Fi (*Wireless Fidelity*) são uma alternativa para as redes convencionais com cabos, proporcionando as mesmas funcionalidades, mas de forma mais flexível. Essas redes seguem um padrão desenvolvido pelo IEEE (*Institute of Electrical and Eletronics Eginners*) conhecido como 802.11 (e seus sub-padrões), que foi homologado no ano de 1997. Um dispositivo Wi-Fi pode ser reconhecido pelo símbolo característico apresentado na figura 1.

Figura 1: Emblema do padrão Wi-Fi.

1.2 Topologia

Em uma rede 802.11 podemos destacar dois tipos de estruturas; a chamada *Basic Service Set* – BSS, que nada mais é que um conjunto de dispositivos sem fio, comunicando entre si. Essa comunicação pode ser feita diretamente entre as estações ou através de um ponto de acesso (AP – *Access Point*).

Outro tipo de estrutura seria a *Extended Service Set* – ESS, que são vários BSS conectados entre si, através de AP. Utilizando esse modo, os AP devidamente interligados permitem aos seus usuários se movimentar de uma BBS para outra sem perder o sinal.

1.2.1 Ad hoc

Essas redes conhecidas por *Independent Basic Service Set* (IBSS) utilizam como métodos a conexão entre si de dispositivos, sem a necessidade de usar um ponto de acesso para interligá-las. O maior problema enfrentado pelos adeptos é não ter controle de acesso e segurança das informações que estão sendo trafegadas, devido a não possui um equipamento que tenha este propósito na rede. A figura 2 mostra um cenário Ad-Hoc

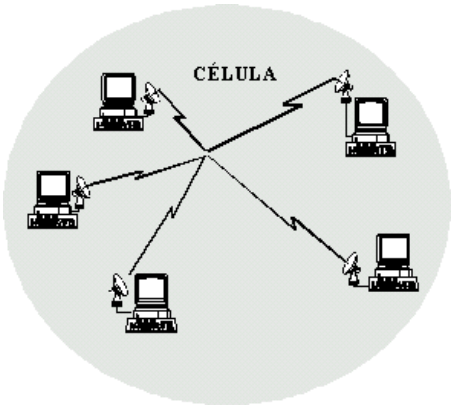

Figura 2: Estrutura de rede Ad-Hoc.
Fonte: http://www.wirelessbrasil.org

1.2.2 Infra-Estrutura

Conhecidas como *Infraestruture Basic* Service Set (*Infraestruture* BSS), essas redes utilizam-se de pontos de acesso para interligar as estações podendo também usar os AP para fazer comunicação entre de rede sem fio e uma rede tradicional com cabos. Adeptos a esse modo têm como grande vantagem uma maior segurança através de criptografia dos dados e filtragem de dispositivos por IP ou MAC. A figura 3 mostra um ambiente de infra-estrutura.

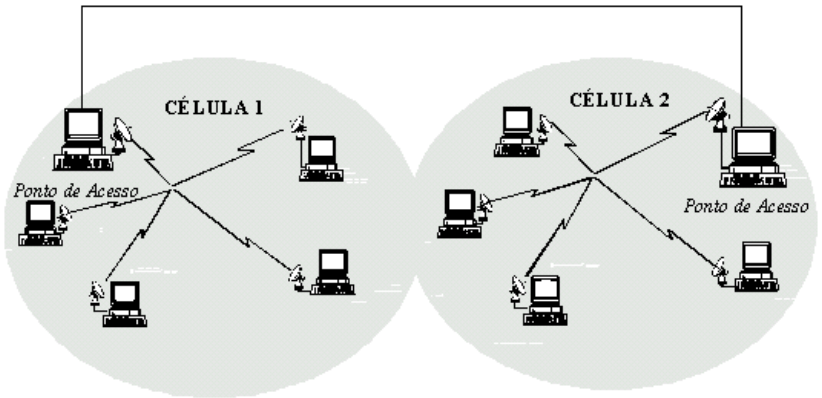

Figura 3: Estrutura de rede Infra-Estrutura.
Fonte: http://www.wirelessbrasil.org

1.3 Principais Padrões

As Wi-Fi IEEE 802.11, foram umas das maiores novidades tecnológicas dos últimos anos. Esse sucesso todo é visível através do crescente numero de pontos de acesso nos mais variados lugares e com a maioria dos computadores portáteis novos já saírem de fabrica com os dispositivos IEEE 802.11. Serão citados abaixo os principais padrões para as redes 802.11.

1.3.1 Padrão 802.11b

Padrão para redes Wi-Fi que alcança uma velocidade de 11Mbps padronizada pelo IEEE, utiliza a freqüência de 2.4 GHz para trafegar informações e suporta até 32 usuários por ponto de acesso. Seus aspectos positivos seriam o baixo custo para implantação e a largura de banda gratuita, o inconveniente deste padrão seria a alta interferência gerada tanto na transmissão quanto na recepção devido a freqüência utilizada 2.4 GHz são equivalente a dos telefones móveis e dispositivos *Bluetooth*. Abaixo na figura 4 temos um exemplo de uma rede que utiliza o protocolo 802.11b

Figura 4: Exemplo de uma rede 802.11b
Fonte: http://www.babooforum.com.br

1.3.2 Padrão 802.11a

Esse padrão alcança velocidade de 54 Mbps dentro dos padrões e até 108 Mbps por fabricantes não padronizados. Suporta até 64 usuários por ponto de acesso e opera na freqüência de 5 GHz. As principais vantagens seriam a velocidade proporcionada e a ausência de interferências. Sua maior desvantagem seria a incompatibilidade com os padrões 802.11b e 802.11g quando se fala em *Access Point*.

1.3.3 Padrão 802.11g

Padrão de tem base a compatibilidade com os dispositivos 802.11b, sua velocidade é de 54 Mbps e utiliza a freqüência de 2.4 GHz. Possui as mesmas vantagens e desvantagens principais do 802.11b. Aceita para autenticação o WEP estática e também o WPA com criptografia dinâmica.

1.3.4 Padrão 802.11i

Foi criado para aperfeiçoar a segurança do protocolo 802.11, fazendo assim uma avaliação nos protocolos de segurança: *Wired Equivalent Protocol* (WEP), *Temporal Key Integrity Protocol* (TKIP) *Advanced Encryption Standard* (AES) e IEEE 802.1x para autenticação e segurança. Todo o trabalho em cima do 802.11i vem sendo feito para integrar o AES com a subcamada MAC, para melhorar a segurança das informações trafegadas na rede sem fio, já que o padrão utilizado pelo WEP e WPA, o RC4 não possui a robustez necessária para garanti-la.

1.4 Sistemas de Transmissão

Segundo Earle (2006) as redes Wi-Fi utilizam três sistemas de transmissão de rádio de espalhamento de espectro diferentes, denominados FHSS (*Frequency-Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Sprectrum*) e OFDM (*Orthogonal Frequenciy Division Multiplexing/Modulation*).

Esse tipo de modulação por espelhamento espectral atua aumentando a quantidade de bits usados para efetuar a transmissão de uma mesma informação, fazendo com que o sinal seja espalhado pelo espectro de freqüência. Aumentando assim a banda de freqüência na qual o sinal é transmitido.

Também são utilizados códigos de espelhamento para fazer a transmissão digital, principalmente em WLANs. Conseguindo espalhar o sinal de freqüência é proporcionada uma serie de vantagens que contribuem no aumento do desempenho da transmissão. Entre estas vantagens estão:

- Imunidade com relação a ruídos e interferências;

- Imunidade a distorções devido à multipercursos;

- Imunidade a interferências e de desvanecimentos de banda estreita;

- Diversos usuários podem compartilhar a mesma banda de freqüência, com baixa interferência;

- Podem ser usados para a criptografia dos sinais. (MALBURG, 2004)

As redes Wi-Fi trabalham em freqüências que sua utilização não depende de autorização. No Brasil a freqüência mais utilizada por adeptos das redes sem fio opera em 2.4 GHz.

1.4.1 *Frequency-Hopping Spread Spectrum*

FHSS é uma técnica de espelhamento que faz uso de um salto de freqüência, utilizando uma determinada freqüência por um período de transmissão e uma diferente durante outra. Essa característica da FHSS faz com que perca um pouco seu desempenho, mas oferece uma vantagem que seria a transmissão menos sujeita a interferências visto que a freqüência utilizada muda constantemente.

País	Canal	Frequência (GHz)	Tamanho do Canal (MHz)
Estados Unidos	2 a 79	2.402 – 2.479	26
Canadá	2 a 79	2.402 – 2.479	26
Inglaterra	2 a 79	2.402 – 2.479	26
França	48 a 82	2.448 – 2.482	27
Espanha	47 a 73	2.473 – 2.495	35
Japão	73 a 95	2.473 – 2.495	23

Quadro 1: *Frequency Hopping World Channel Allocation*
Fonte: EARLE (2006, p. 54)

1.4.2 *Direct Sequence Spread Spectrum*

A técnica de DSSS é um esquema de modulação que gera um padrão de bits redundante a cada bit transmitido. Segundo Rufino (2005, p.19): “Utilizado no padrão 802.11b, o DSSS utiliza uma técnica denominada *code chips*, que consiste em separar cada bit de dados em 11 sub-bits, que são enviados de forma redundante por um mesmo canal em diferentes freqüências, e a banda 2,4 GHz é dividida em três canais”. O DSSS tem melhor desempenho que o FHSS, devido a utilizar mais canais durante a transmissão dos dados, pode tem maior chance de sofrer algum tipo de interferência.

1.4.3 *Orthogonal Frequency Division Multiplexing/Modulation*

Está técnica de modulação de freqüência baseia-se na idéia de multiplexação por divisão de freqüências, onde envia diversos sinais em diferentes freqüências. O OFDM consegue dividir uma transmissão em diversos sinais, assim utilizando uma menor ocupação espectral. Está forma é a mais eficiente é utilizada tanto em redes sem fio quanto em redes cabeadas.

2 PROTOCOLOS DE SEGURANÇA

Segundo Soares (2005, p.448): “segurança são procedimentos para minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos, onde vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém”.

Neste capítulo serão abordados separadamente os mecanismos de segurança disponíveis para redes Wi-Fi. O objetivo principal é conceituar e descrever os protocolos, bem como suas características e funcionalidades.

2.1 WEP

O protocolo WEP (*Wired Equivalent Privacy*) é bastante utilizado por adeptos a redes Wi-Fi, para impedir que seja possível ler os dados transmitidos, e para evitar que intrusos tenham acesso à rede sem fio.

Este protocolo possui três atributos básicos:

- Confidencialidade: Através de uma chave secreta que cada estação de trabalho possui, este serviço que é opcional nos dispositivos permite que somente pessoas autorizadas tenham acesso as informações trafegadas;
- Integridade: Garante que o receptor receberá as informações corretas, sem modificações ou perda de dados;
- Autenticidade: Este serviço permite um alto padrão de segurança, para evitar que dispositivos não autorizados tenham acesso a rede.

O algoritmo utilizado para fazer a criptografia dos dados é o RC4, projetado por Ron Rivest, em 1987. Este algoritmo é de fluxo, ou seja, faz a criptografia dos dados na medida em que são transmitidos, aumentando assim seu desempenho. O código deste algoritmo foi mantido em segredo até ser postado na internet em 2001.

A segurança dos dados do protocolo WEP é composta por dois métodos: chave estática, que deve ser a mesma em todos os dispositivos de rede além de possuir um componente dinâmico, que juntos formam a chave criptográfica. Segundo Rufino (2005, p.36): “WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas”.

Um vetor de inicialização (IV – *Initialization Vector*) de 24 bits é utilizado junto à chave secreta de 40 ou 104 bits para gerar as informações criptografadas. Este vetor IV é enviado junto à mensagem cifrada, formando uma chave de 64 ou 128 bits pra que o receptor possa reverter o processo de criptografia. O IV também permite uma variação da chave estática em 24 bits, tornado diferenciado o resultado de mensagens idênticas. O esquema do funcionamento do WEP é apresentado abaixo sendo 5a esquema de cifragem e 5b decifragem.

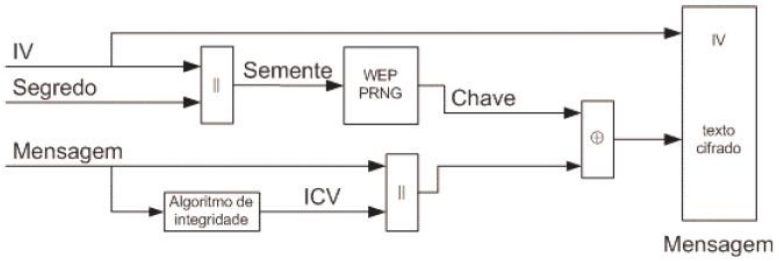

Figura 5a: Cifragem

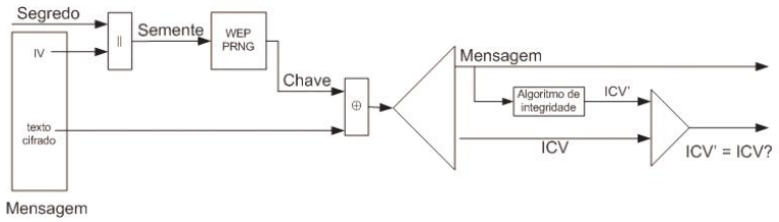

Figura 5b: Decifragem

Para que o protocolo WEP possa proporcionar segurança, a sua chave nunca deve ser reutilizada. Isto é muito imprescindível, pois quando se esgotarem o numero de possíveis IVs, a chave secreta deverá ser modificada. O motivo deste fato vem da possibilidade de um atacante obter uma chave (não a semente, mas a chave utilizada nas operações XOR) e com ela obter os dados cifrados com a mesma chave em outro momento.

Além disso, para tratar da integridade dos dados o WEP utiliza CRC-32 (*Cyclic Redundance Check 32*), para calcular o *checksum* da mensagem, que é adicionado no quadro,

para garantir que a mensagem não foi alterada durante a transmissão. Dessa forma, o receptor recalcula o *checksum* para garantir a total integridade dos dados.

2.2 WPA

O WPA (*Wi-Fi Protected Access*) surgiu devido à necessidade de aumentar o nível de segurança nas redes sem fios, resolvendo alguns dos principais problemas do WEP. Criado em 2003, através de um conjunto de membros da *Wi-Fi Alliance* e de membros do IEEE, o propósito principal deste protocolo é a mudança constante da chave de encriptação dificultando a invasão ou descoberta da chave.

Este protocolo resolve a questão dos cabeçalhos fracos do WEP, que são chamados de vetores de inicialização (IV), e oferece uma forma de garantir a integridade das mensagens transmitidas pelo MIC (*Message Integrity Code*) usando TKIP (*Temporal Key Integrity Protocol)* para melhorar a criptografia de dados.

O WPA é compatível com o padrão de redes sem fio 802.11i e realiza melhorias em encriptação de dados e autenticação do usuário, porém para efetuar migração requer um upgrade de software. Ele pode ser utilizado numa rede híbrida que tenha WEP instalado. Segundo Rufino (2005, p.35): “Várias mudanças e avanços foram incorporados a esse protocolo, porém a maior parte deles exige a inclusão de outros elementos à infra-estrutura”.

Esse protocolo atua em duas áreas distintas:

• Primeira área - Onde visa substituir completamente o WEP. Essa primeira área trata da cifração dos dados, que tem por objetivo garantir a privacidade das informações que são trafegadas

• Segunda área - Foca a autenticação do usuário (área não coberta pelo WEP), utilizando os padrões 802.1x e EAP. (RUFINO, 2005)

É obrigatória no WPA a autenticação 802.1x; no padrão 802.11 era opcional. Essa autenticação é uma combinação de sistema aberto e autenticação 802.1x que possui duas etapas: a primeira é realizada pela autenticação de sistema aberto e indica ao usuário da rede sem fio que ele pode enviar quadros para a base e a segunda fase utiliza o 802.1x para realizar a autenticação do usuário.

Outro método de autenticação que o protocolo disponibiliza para ambientes domésticos onde não existe um servidor, é o chamado PSK (*Pre-Shared Key*), que possibilita ao usuário digitar manualmente suas chaves e senhas

Mesmo o WPA possuindo características de segurança superior ao protocolo WEP, ainda têm vulnerabilidades já conhecidas e reportadas, exigindo assim dos adeptos um conhecimento dessas técnicas para tentar minimizar ao máximo os estragos.

2.3 WPA2

O protocolo WAP corrigiu diversos problemas do WEP, mas seu desempenho foi prejudicado em termos de estabilidade, com isso, surgiu o WPA2 com a promessa de ser a solução definitiva de estabilidade e segurança para as redes sem fio. Sua principal mudança em relação ao seu antecessor WAP é o método criptográfico utilizado.

O WAP2 utiliza o AES (*Advanced Encryptation Standart*) junto com o TKIP com chave de 256 bits, um método mais poderoso que o WAP que utilizava o TKIP com o RC4. O AES permite ser utilizada chave de 128, 192 e 256 bits, o padrão no WPA2 é 256 bits, sendo assim, uma ferramenta muito poderosa de criptografia. Utilizando o AES surgiu a necessidade de novo hardware para processamento criptográfico, devido a isso, os dispositivos WP2 tem um co-processamento para realizar os cálculos criptográficos.

3 ANÁLISE DE VULNERABILIDADES

Neste capitulo serão tratadas às vulnerabilidades do protocolo 802.11, apresentando características que por sua vez podem causar riscos a rede sem fio. Também será feito um estudo sobre ferramentas e métodos para exploração dos pontos fracos de segurança.

3.1 Vulnerabilidades dos Protocolos

Diversas vulnerabilidades dos protocolos de segurança WEP e WPA já foram descobertas e reportadas. Esses problemas precisam ser conhecidos pelos administradores de redes para assim poder minimizar os prejuízos que podem ser ocasionados devido a essas falhas.

3.1.1 Vulnerabilidades do Protocolo WEP

O protocolo de segurança de redes sem fio WEP possui diversas vulnerabilidades, entre os principais já reportados destaca-se o fato de utilizar uma chave única e estática que deve ser compartilhada entre todos os dispositivos de rede. Em ambientes de pequeno porte (pequenos escritórios ou uso doméstico), o compartilhamento dessas chaves não chega ser um grande problema, mas em ambientes maiores ou em lugares que precisam de grande mobilidade o processo fica bem dispendioso.

Outra questão seria o algoritmo de criptografia utilizado RC4, que mesmo fazendo um processamento e devolvendo mensagens diferentes da original, permite que sejam identificadas essas informações através de seu tamanho. Segundo Rufino (2005, p.60): “Ao utilizar uma técnica de equivalência numérica, o RC4 recebe um byte que realiza um processamento e gera como saída também um byte, só que diferente do original. Essa função permite identificar quantos bytes tem a mensagem original, já que a informação gerada terá o mesmo número de bytes que a original”.

O vetor de inicialização VI foi criado para evitar que quando uma mensagem é cifrada com uma chave fixa idêntica a anterior tenha o mesmo resultado. Seu grande problema seria transmitir mensagens em puro texto, que é facilmente capturado por um software, deixando as informações disponíveis para qualquer intruso montar um ataque. O WEP também permite que seja reutilizado o VI, permitindo assim decifrar dados. A integridade (*Integrity Check Value*) sendo baseada em CRC32 permite que seja alterada a mensagem e o ICV sem que as estações de trabalho que utilizam a rede percebam.

3.1.2 Vulnerabilidades do Protocolo WPA

Mesmo possuindo características de segurança superiores as do WEP, ainda assim possui vulnerabilidades já conhecidas. A principal seria o ataque de força bruta ou dicionário, onde o intruso testa diversas senhas ou simples palavras em seqüência. As chaves utilizadas que possuem menos de 20 caracteres são mais susceptíveis a ataques. Segundo Rufino (2005, p.62) “É muito comum fabricantes usarem senhas pequenas (de 8 a 10 posições) imaginando que o administrador irá modificá-las quando colocar o equipamento em produção, porém isso não ocorre na prática, o que torna redes mesmo com WPA tão ou mais vulneráveis que redes que utilizam WEP.”

3.1.3 Vulnerabilidades do Protocolo WPA2

Conforme foi visto anteriormente o WPA2 possui um bom mecanismo de segurança. Os dispositivos que disponibilizam o WPA2 ainda não são amplamente utilizados, assim poucas vulnerabilidades são conhecidas o que proporciona uma maior sensação de proteção para quem o utiliza.

3.2 Ferramentas

Será feito uma conceituação de algumas das ferramentas mais utilizadas para analise de pacotes em redes sem fio. Os softwares descritos têm características tanto de ataque quanto de monitoramento preventivo da Wi-Fi.

3.2.1 *Kismet*

URL: http://www.kismetwireless.net

Esse sniffer é um detector de redes sem fio e um sistema de descoberta de intrusão. Desenvolvido em plataforma opensource trabalha com as redes 802.11b, 802.11a, e 802.11g,

possui em seu conjunto um grande numero de opções. Segundo Rufino (2005, p.80): “Por ser uma das ferramentas com maior velocidade de atualizações e adição de novas funcionalidades, o Kismet pode ser utilizado para vários fins, todos relacionados a redes sem fio. Possui poucos competidores em relação à quantidade de funcionalidades, número de chipsets suportados entre outras características.”

Esse software tem a característica de monitorar diversas origens diferentes. Foi projetado com a estrutura cliente-servidor e pode ter como base um único cliente para diversos servidores espalhados. Os pacotes capturados podem ser salvos em diversos formatos diferentes, também tem por padrão armazenar todas as redes encontradas durante a pesquisa.

Entre suas funcionalidades o sniffer pode mostrar em um estudo de trafego, quando o ultimo pacote foi recebido, alem da qualidade do sinal durante a transmissão dos dados. Também consegue fazer relações dos clientes de uma determinada rede, com seus devidos IP, que podem ser descobertos através de requisições ARP, UDP e TCP. Esse software é considerado pelas pesquisas feitas um dos melhores opensources da atualidade.

3.2.2 *Aircrack*

URL: http://www.aircrack-ng.org

Esse software é uma ferramenta para análise de trafego em redes sem fio, sua plataforma permite rodar tanto em Linux como em Windows. Tem como sua função descobrir ou recuperar chaves WEP e WPA-PSK de redes 802.11 a partir de dados capturados de qualquer ambiente Wi-Fi. *Aircrack* é na verdade um conjunto de ferramentas, entre elas estão: *Airodump* e *Wzcook*.

Seu novo modelo conhecido como *Aircrack-ng* já implementa o padrão FMS de ataque em conjunto como inúmeras otimizações como o *KereK*, alem dos novos PTW tornando assim o ataque muito mais rápido se comparado a outras ferramentas. Para utilização completa deste programa é necessário a captura de alguns dados de uma rede sem fio. Esta coleta de trafego poder ser executada por qualquer dispositivo wireless capaz de entrar um modo RFMON. Abaixo na figura 6 podemos visualizar a tela do *Aircrack-ng*.

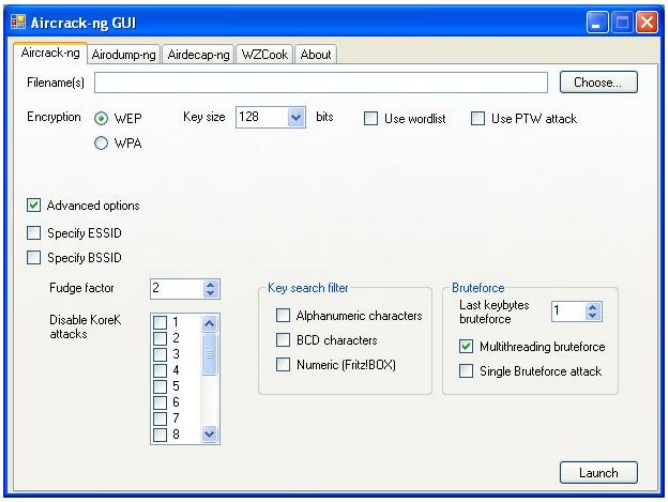

Figura 6: Tela principal do *Aircrack-ng*
Fonte: http://www.vivasemfio.com

3.2.3 *WireShark*

URL: www.wireshark.org

Mais conhecido como *ethereal* por adeptos, essa é a mais nova versão deste analisador de trafego de redes. Esse programa verifica pacotes transmitidos pelas interfaces de comunicação do PC e tem como objetivo detectar problemas de rede, conexões suspeitas, auxiliar no desenvolvimento de aplicações entre outras.

Wireshark também conhecido por tubarão dos fios é uma ferramenta totalmente livre, é muito utilizada por usuários de Linux. São inúmeras as funcionalidades desta ferramenta entre filtros e muitas informações, o utilizador consegue ter um controle total sobre os dados que são transmitidos na rede em diferentes protocolos.

3.2.4 *Wellenreiter*

URL: http://www.wellenreiter.net

O software *Wellenreiter* é uma ferramenta para monitorar e localizar redes sem fio. Possui uma excelente interface gráfica que permite a fácil visualização dos dados disponibilizados pelo programa. As informações trafegadas na rede como: canal de comunicação, marca do AP, criptografia utilizada entre outras; são passíveis de identificação utilizando esse programa. Alem disso a ferramenta registra todo o trafego da rede analisada.

Entre as funcionalidades do *sniffer Wellenreiter* está à capacidade de fazer um ataque de força bruta nos SSID, fazendo assim com que pacotes sejam enviados de maneira que o software fique oculto enquanto observa as informações solicitadas.

3.2.5 *Airodump-ng*

URL: http://www.aircrack-ng.org

A ferramenta *Airodump-ng* tem como sua função principal à captura de pacotes trafegados da rede sem fio. Normalmente esse software é utilizado em conjunto com o aircrack-ng, pois necessita de programa adequado para decifrar os dados capturados. Consegue capturar os quadros do vetor de inicialização IV do WEP, alem de criar um arquivo de texto contendo detalhes de todos os *Access Points* e clientes vistos.

3.2.6 *Ettercap*

URL: http://ettercap.sourceforge.net

Esta ferramenta pode ser considerada um canivete suíço, pois é um aplicativo com inúmeras funções. Trabalho explorando largamente o protocolo ARP e pode realizar vários ataques diferentes. Como envia um ARP *REQUEST* para o IP da LAN, não consegue executar suas funções oculto.

Entre as funções que o *Ettercap* possui estão: Permitir a colocação de caracteres em uma conexão estabelecida; Permite filtrar os pacotes trafegados na rede, alterando ou descartando; Permite a realização de *scanning* passivo da LAN; Permite a verificação de existência de outros *poisoner*s na rede.

3.2.7 *WEPCrack*

URL: http://sourceforge.net/projects/wepcrack/

Este programa explora a vulnerabilidade encontrada no protocolo de segurança WEP no começo do ano 2001. Funciona em qualquer sistema que possua suporte aos scripts Perl. Quem utiliza o *WEPCrack* normalmente são pessoas mal intencionadas que coletam informações essenciais da rede como, por exemplo, a BSSID, para programar ataques futuros a rede sem fio.

3.2.8 *HostAP*

URL: http://hostap.epitest.fi/

Host AP é um modulo disponível para LINUX que consegue transformar dispositivo wireless em *acess points*. Não exige qualquer especificação especial da placa de rede sem fio e consegue trabalhar com os protocolos de segurança padrão. Opera tanto em *notebooks* quanto em *desktops*, transformando estes em uma ferramenta excelente para ataques do tipo associação maliciosa entre outros.

3.3 Métodos

Ataques as redes de computadores não são novidade, com o amplo crescimento da utilização da internet estas tentativas de roubos de informações acontecem de forma cada vez mais impiedosa. A maior parte destes métodos não sofreu nenhuma adaptação do tempo dos tradicionais cabos para o wireless, no entanto, alguns tiveram alterações para obterem melhores resultados.

Atualmente, as redes possuem excelentes mecanismos de defesa como, por exemplo, o firewall que propriamente configurado oferece ótimos resultados. A utilização deste mecanismo de defesa não contribui em nada se for instalado na mesma rede um ponto de acesso wireless mal configurado. Por isso deve haver um cuidado constante para ter uma segurança eficiente a fim de não deixar um *backdoor* nesta rede.

As redes sem fio são mais sucessivas a ataques, dificilmente existe alguma WLAN que não tenha ou não irá ser alvo de um atacante. Isso ocorre devido ao alto numero de adeptos a tecnologia que está presente em ambientes empresariais, domésticos ou públicos. A seguir serão apresentados alguns tipos de ataques que se destacam atualmente nas redes sem fio. (BABOO, 2005)

3.3.1 Ataque dicionário

Nesta forma especifica de ataque, os responsáveis pela tentativa de intrusão utilizam um *sniffer* para capturar o trafego em transito de uma determinada rede sem fio entre uma estação de trabalho e um ponto de acesso. Com isso, fazem uso de uma ferramenta adequada para adivinhar senhas. Já existem sites na internet que possuem uma lista de palavras excelentes para o ataque dicionário, normalmente estas listas não têm palavras repetidas o que

ajuda muito na hora de utilizá-la. Uma delas está disponível em: ftp://ftp.se.kde.org/pub/security/tools/net/Openwall/wordlists/

Segundo Rufino (2005, p.62): “No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque.” Em redes que utilizam o protocolo WPA basta capturar quatro pacotes específicos de dados para tentar descobrir as senhas, enquanto no WEP é necessário pegar uma quantia grande de trafego. Uma maneira para tentar fugir destes ataques seria utilizando senha de um tamanho considerável e misturando caracteres com números, outra forma seria utilizando servidor de autenticação.

3.3.2 Ataque DoS.

Ataque *Denail of Sercice* (DoS – Negativa de Serviço) este método faz com que o usuário perca o acesso ao servidor. O problema afeta principalmente as redes Wi-Fi que operam em banda de 2.4 GHz e com velocidade baixa, menos de 20 Mbps.

Os ataques podem ser efetuados de qualquer lugar dentro da cobertura da rede sem fio, durante um ataque o dispositivo se mantém de maneira que o canal fica sempre ocupado o que impede a transmissão de informações na Wi-Fi. Segundo Duarte (2003, p.41): “enviando as requisições de dissociação em períodos curto de tempo o DoS é concretizado. Isso, pois os clientes não conseguiriam permanecer conecta por muito tempo”.

3.3.3 Ataque *Men-in-the-Middle*

O ataque *Men-in-the-Middle* (MITM) é um método no qual o hacker invade o sistema e fica alojado entre o usuário e o servidor conseguindo comprometer a comunicação sem que nenhuma das partes perceba. Normalmente o atacante fica no meio da transmissão entre dois pontos, dessa forma podendo ler, inserir e modificar os dados, qualquer informação que o usuário tiver acesso o atacante também terá.

Este ataque possui dois tipos de classificação: *full-duplex* que é quando o *hacker* consegue interceptar ambos os sentidos da comunicação e *half-duplex* que consiste na interceptação de um sentido somente, deixando o outro trafegar de forma normal. Além disso, o *hacker* durante o ataque pode ter uma posição transparente que seria ficar invisível enquanto é realizada a transmissão ou servir de proxy se expondo as entidades.

3.3.4 Ataque *eavesdropping*

Esse método de ataque também conhecido por *Sniffing*, consiste na analise de trafego entre cliente e servidor. Todas as informações trafegadas são monitoradas para utilizadas posteriormente para propósitos diversos. Com o uso de ferramentas de *sniffing* na rede, pode-se facilmente fazer uma leitura dos dados trafegados, alem de ter acesso aos pacotes, mesmo que sendo encriptados podem ser decifrados dependendo do algoritmo utilizado.

Um das formas para tentar minimizar o problema de *eavesdropping*, é usar VPN dificultando assim a escuta das informações, pois é possível analisar o trafego da rede sem fio pelo responsável.

3.3.5 *Wardriving*

Neste método de ataque, são utilizados dispositivos para encontrar todas as redes que estão dentro do raio de atuação do equipamento de monitoração. Um dos principais objetivos deste tipo de ataque é mapear todos os pontos detectados com o auxilio de um GPS.

> WarDriving é o ato de mover-se ao redor de uma específica área e mapear a população de pontos de acesso wireless para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança associados a estes tipos de rede (tipicamente wireless). (HURLEY, CHRIS et al, 2004, p.12).

O *WarDiving* na verdade pode ser considerado um método que auxilia quem necessita buscar redes Wi-Fi, alem de possibilitar acesso a essas redes de fio pesquisadas. Sem previa autorização dos proprietários da rede não é possível acessar nenhum tipo de recurso dos pontos de acesso.

3.3.6 *Access Point Spoofing* (Associação Maliciosa)

Access Point Spoofing ou Associação Maliciosa ocorre quando o atacante se faz passar por um ponto de acesso e com isso a cliente pensa estar conectando-se a uma rede WLAN verdadeira. Este tipo de ataque é mais comum em redes *Ad-Hoc*.

“Esta associação maliciosa consta de duas máquinas com dispositivos para redes sem fio e segue o seguinte conjunto de passos:

- A vítima envia pacotes de *Probe Request* (pacotes que busca conexão com um *access point*) à procura de *access points* para conexão;

- O atacante, com o auxílio de um software de conexão, se passa por um acess point;

- A vítima requisita a associação e se associa ao atacante;

- O atacante responde com as informações de rede necessária como endereço IP;

- O atacante envia uma requisição de *NET USE*;

- A vítima responde com *LOGIN*;

- Qualquer vulnerabilidade de qualquer serviço do cliente pode ser agora explorada". (BABOO, 2005).

3.3.7 Envenenamento ARP

Esta forma de ataque acontece na camada de *enlace*, fazendo assim com que o atacante necessariamente esteja conectado a mesma rede local que a vitima. Desta forma redes conectadas por roteadores e *gateways* ficam livres, pois o ataque se limita a redes que sejam interligadas por *hubs, switches e bridges*. (BABOO,2005).

O ataque de envenenamento (*ARP Poisoning*) é a forma mais fácil para executar o conhecido Homem-no-Meio, pois a maioria dos dispositivos para rede sem fio da atualidade atua como uma *bridge* entre a rede ethernet básica e a *wireless*. Desta forma a tentativa de ataque pode ser disparada diretamente de uma estação WLAN para uma estação que se encontra da rede cabeada. (BABOO 2005)

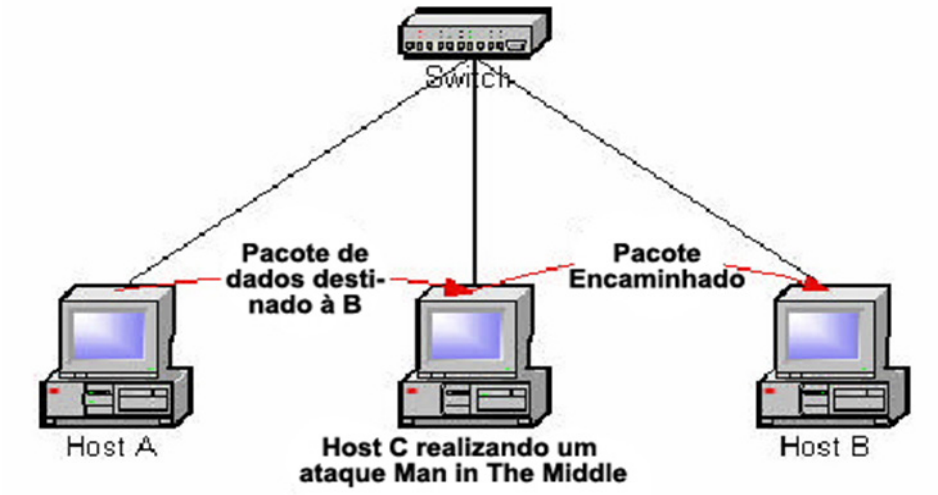

Figura 7: ARP Poisoning
Fonte: www.vivaolinux.com.br

O funcionamento desta técnica baseia-se em enviar uma resposta ARP falsa a uma requisição original, fazendo com que o roteador passe a manda informações que eram destinadas ao *host* 1 para o *host* 2, que reenvia os dados para o *host* 1. Se o envenenamento funcionar de forma correta o *host* 1 não consegue perceber o redirecionamento das

informações. È chamado de *poisoning* a atualização com uma entrada falsa do *cache* do *host* alvo do ataque. (VIEIRA, 2008)

Alguns sistemas operacionais permitem que outros sistemas consigam sobrescrever as entradas existentes ou até mesmo escrever novas se não existir nenhuma com uma falsa, entre eles estão: Windows XP e Linux. O sistema Sun Solaris Systems não é vulnerável a este tipo de ataque. (VIEIRA, 2008)

3.3.8 *MAC Spoofing*

Está técnica de *Spoofing* acontece quando o atacante consegue clonar o MAC de um servidor ou roteador para filtrar as informações trafegadas da rede sem fio. Dados como senhas, *logins* ou qualquer outro tipo de informação importante pode ser capturado utilizando este método.

Muitas empresas possuem um controle rigoroso, possuindo listas de MAC validos para conexão banindo assim o acesso indevido de outros dispositivos. Também é sabido, que estes dispositivos para rede sem fio possuem uma particularidade: a de permitir a troca de endereço físico. Desta forma um atacante utilizado uma técnica de espionagem pode capturar um endereço MAC valido e alterar o seu, a fim de poder acessar a rede como um usuário permitido. (RUFINO, 2005)

A figura XXX abaixo mostra a facilidade da alteração do endereço MAC da placa wireless no sistema operacional LINUX Ubuntu 8.10. Este teste foi executado em ambiente experimental.

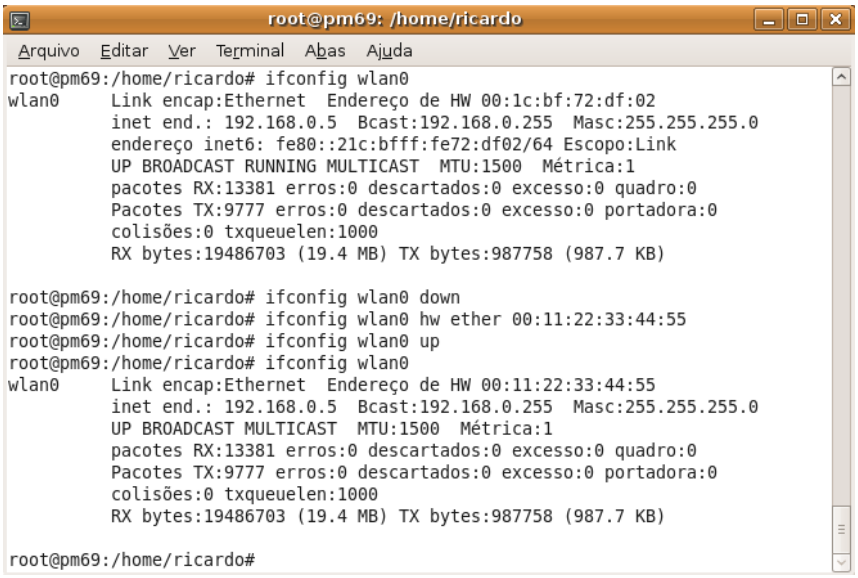

Figura 8: Alteração do Endereço MAC
Fonte: Elaboração do Autor

Com a utilização do MAC *Spoofing* de maneira correta os dispositivos de rede terão a impressão que o computador que está atacado seja um *gateway*, roteador ou um servidor e enviaram o trafego para ele. Está técnica acontece na camada 2 (*enlace*), e muito semelhante ao *spoofing* por IP que acontece na camada 3 (rede).

4 MÉTODOS DE ACESSO SEGURO

Neste capitulo serão apresentados métodos que reduzem o acesso indevido as redes Wi-Fi.

4.1 RADIUS (*Remote Authentication Dial-In User Service*)

O protocolo RADIUS foi desenvolvido pela empresa Livingston, mais tarde passou a pertencer à empresa Lucent Technologies e hoje faz parte dos padrões em desenvolvimento no IETF (*Internet Engineering Task Force*). O protocolo pode ser utilizado de forma integrada a diversos serviços garantindo segurança e restrição no acesso a uma rede. (ALBUQUERQUE, 2003)

Para um adequado funcionamento do protocolo RADIUS, todas as informações a respeito dos usuários da rede devem estar devidamente cadastradas no servidor de autenticação. Existem duas formas básicas de autenticação de usuários, a primeira seria o modo *challenge* onde deverá ser respondida uma requisição ao servidor, a segunda seria o modo usuário e senha que para autenticar deve ser informado os dados para validação.

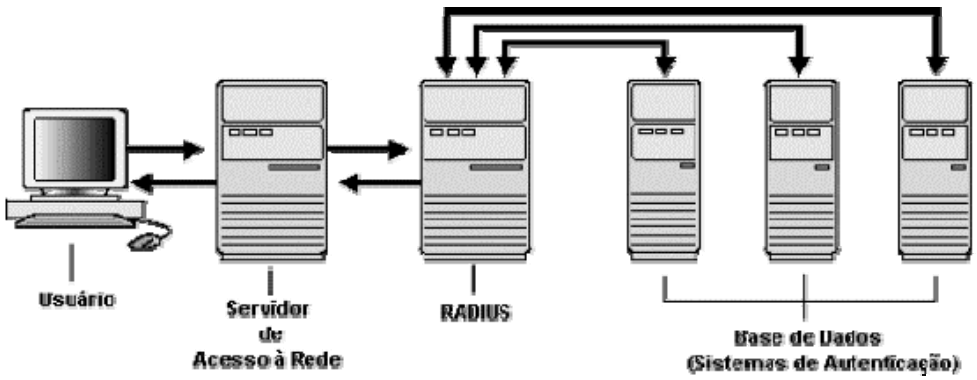

Figura 9: Protocolo RADIUS
Fonte: ALBUQUERQUE, 2003

Os principais objetivos do RADIUS eram:

- Ser um protocolo aberto, ou seja, qualquer fabricante poderia utilizá-lo sem custos.

- Ser um protocolo independente de máquina.

- Ser seguro e confiável.

- Ser escalonável e expansível, sendo capaz de acompanhar as necessidades futuras.

- Ser simples de se implementar, tanto no lado do servidor RADIUS como no cliente.

RADIUS é uma excelente alternativa para assegurar que uma rede e seus serviços serão acessados devidamente, por usuários cujo acesso é realmente garantido. Por se tratar de um padrão em desenvolvimento pelo IETF, pode-se ter certeza de que é uma ferramenta amplamente divulgada e avaliada ostensivamente. (ALBUQUERQUE, 2003).

4.2 VPN (Virtual Private Network)

A *Virtual Private Network* ou Rede Privada Virtual é uma denominação dada para a idéia de se utilizar uma rede publica como, por exemplo, a internet, para a implementação de redes corporativas. Estas VPN´s são na verdade túneis de criptografia entre pontos autorizados para transferência de informações. A segurança é uma das principais funções da VPN, pois dados confidenciais trafegam na internet que é uma rede insegura.

Nas VPN´s todo o trafego de rede é criptografado, o que é uma desvantagem, pois torna mais lenta a velocidade de conexão. Para fazer a criptografia de informações existem alguns protocolos utilizados como o IPSec, PPTP e L2TP e *Socks* v5.

Uma grande vantagem do uso de VPN´s é a interligação entre dois pontos sem o uso de links dedicados, por isso está solução é bastante interessante sobre o ponto de vista econômico. Abaixo serão apresentadas as três mais importantes aplicações para as VPN´s:

4.2.1 Acesso Remoto Via Internet.

Segundo Chin, “acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso (Internet Service Provider - ISP).” Neste caso a estação de trabalho remota faria uma ligação para o provedor de acesso conectando-se a internet, logo após isso o software de VPN cria uma rede privada entre o usuário remoto e o servidor de VPN corporativo.

A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

O protocolo mais utilizado para esse tipo de acesso remoto na internet é o PPP (*Ponit-to-Point*), que deu origem ao PPTP (*Point-to-Point Tunneling Protocol*). O PPTP possui em uma base diversas funcionalidades do PPP fazendo assim com que o acesso remoto seja tunelado através da internet para um definido site de destino.

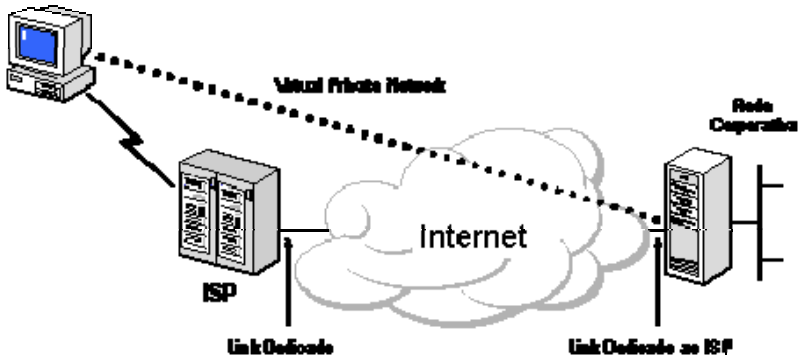

Figura 10: Esquema para VPN de acesso remoto via Internet.
Fonte: http://www.rnp.br

4.2.2 Conexão de LANs via internet

Segundo Chin, Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a WAN corporativa.”

Esta forma é a mais simples de ser implementada e a que traz o maior retorno em relação aos custos. Conectando duas redes distintas por VPN através da internet eliminam-se os links dedicados de longa distancia que normalmente tem um alto custo de manutenção.

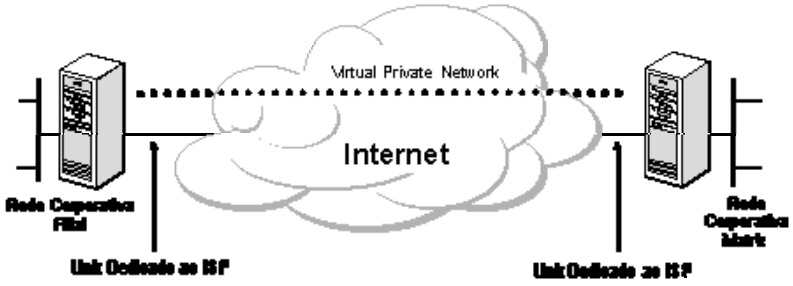

Figura 11: Esquema para VPN Conexão de LANs via Internet.
Fonte: http://www.rnp.br

4.2.3 Conexão de computadores numa Intranet

Segundo Chin, “Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa.”

Mesmo oferecendo uma grande segurança das informações que trafegam pela rede, está solução pode criar problemas indesejados de acesso a dados. O controle sobre a rede fica na mão do administrador que pode ou não dar direitos de acesso a determinado usuário a arquivos que sejam classificados como confidenciais.

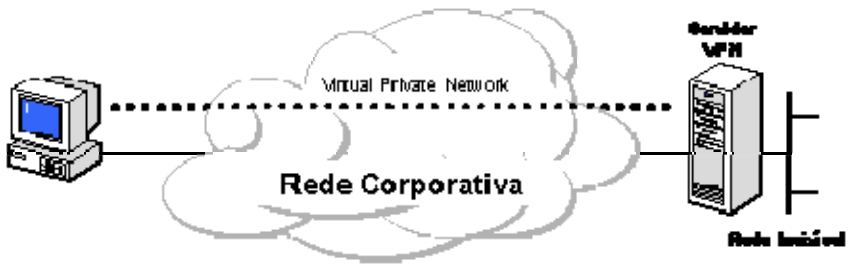

Figura 12: Esquema para VPN Conexão de computadores numa Intranet.
Fonte: http://www.rnp.br

.

5 RELATÓRIOS PARA ANÁLISE DE VULNERABILIDADES DAS REDES SEM FIO

Este relatório é o principal objetivo deste presente trabalho, nele serão abordados os principais itens que garantem a segurança em uma rede sem fio. Com o preenchimento total deste documento será mais fácil de interpretar e avaliar à capacidade da rede em oferecer a devida segurança para os dados que nela trafegam.

Os itens do relatório foram obtidos a partir das características observadas nas ferramentas estudadas.

5.1 Informações Gerais

A primeira parte visa o conhecimento do ambiente onde está localizada a rede e informações primárias, conta com os campos:

- Local da Rede;
- Responsável pela Rede;
- Fabricante do Rádio;
- Modelo de Rádio Utilizado;
- Freqüência do Rádio;
- Modo de Operação;
- SSID da Rede.

Todas estas informações são básicas para conhecer a rede que está sendo estudada.

5.2 Segurança

Após passar as informações gerais, o relatório aborda questões relacionadas à segurança da rede, que são fundamentais para o administrador manter ela segura. Estes

campos serão citados a seguir em forma de itens com suas justificativas mostrando a importância de cada um deles.

- Periodicidade para troca de senha: Não existe um período aconselhável para que seja feita esta troca, basta que seja efetuada. Quanto menor o tempo de troca maior a segurança, pois se algum atacante estiver fazendo tentativas que quebra de senha, com a troca terá de refazê-las.

- Utiliza algum método para conexão segura: Segundo Rufino (2005, p.107): “Consideradas exemplos de segurança forte, as Vans têm sido a solução preferida para garantir acesso a ambientes remotos por meios inseguros.” É extremamente interessante utilizar a ajuda das VPN´s para fazer interligações de redes através que WLAN´s quando está é feita por rede publica, aumentando assim consideravelmente o nível de segurança.

- Protocolo de segurança: A fim de garantir a segurança da rede podemos optar pelo uso dos protocolos de segurança. Seu uso depende da necessidade do usuário e da qualidade do seu dispositivo. Para os usuários que procuram um nível de segurança mais reduzido, mas estável é aconselhado que use o WEP. Mesmo com sua proposta de melhor o nível de segurança do WEP o protocolo WPA não é aconselhável, pois quando configurado afeta consideravelmente o desempenho da rede. Para quem necessita de uma ótima segurança e estabilidade, é interessante o uso do WPA2 que vem conseguindo cumprir seu papel. (OZORIO, 2007)

- Utiliza Antena Externa para Transmissão: O uso de antenas para transmissão tem a finalidade de aumentar o campo de atuação do sinal. Assim fazendo com que atacantes com dispositivos mais potentes, consigam interceptar o sinal com uma maior distancia do acess point. (RUFINO, 2005)

- Filtro MAC: O filtro por endereçamento MAC é uma ótima alternativa para evitar entradas indevidas na rede wireless. Mesmo sabendo que possuem formas para burlar o código está ferramenta ainda é bastante utilizada para aumentar a segurança.

- *Hide* SSID: é uma opção de segurança onde é escondido o SSID da rede, utilizado normalmente em redes genéricas de 2.4GHz.

A seguir segue o modelo de relatório proposto.

Relatório para Análise de Vulnerabilidades das Redes sem Fio					
1	**Informações Gerais**				
1.1	Local da Rede:				
1.2	Responsável pela Rede:				
1.3	Fabricante do Rádio:				
1.4	Modelo de Rádio Utilizado:				
1.5	Freqüência do Rádio:				
1.6	Modo de Operação:				
1.7	SSID da Rede:				
2	**Segurança**				
2.1	Período de Troca de Senha:				
2.2	Método para Conexão Segura	VPN	RADIUS	OUTROS	NÃO
2.3	Protocolo de Segurança Utilizado	WEP	WPA	WPA2	NÃO
2.4	Antena Para Transmissão	SIM	NÃO		
2.5	Filtro MAC	SIM	NÃO		
2.6	Hide SSID	SIM	NÃO		

Preparado por:	Data: _____/_____/_____

6 ESTUDO DE CASO

Neste capitulo será descrito o ambiente onde será realizado o experimento, onde serão abordados tópicos como antenas utilizadas, rádios e *switches*. Alem disso será mostrado como o cenário está configurado para minimizar os problemas.

6.1 Ambiente

O ambiente onde serão efetuados os testes experimentais em busca de alguma vulnerabilidade à rede sem fio está localizado nas dependências de uma Prefeitura Municipal do estado do Rio Grande do Sul. Este experimento consiste em validar as técnicas e ferramentas encontradas na pesquisa deste trabalho. Para isso serão descritos todos dispositivos utilizados nesta rede além dos equipamentos necessários para efetuar os testes.

A prefeitura conta com diversas redes para interligação de pontos externos. Focaremos os testes na rede wireless da Secretária Municipal de Saúde. Esta rede interliga o sistema de gestão dos quatro postos municipais de saúde existentes da cidade de Portão/RS com a base de dados central que está no CPD do prédio administrativo. Por essa rede trafegam diariamente todo o tipo de informação referente a consultas médicas, receitas, além de documentos diversos.

6.1.1 Antenas

A rede conta com sete antenas para emissão do sinal wireless, a principal delas que faz a interligação da rede física com a rede sem fio está localizada na parte superior do prédio da Secretária Municipal da Saúde. A figura 13 mostra a rede e a freqüência utilizada entre postos, os interligados por linha preta são 2.4GHz e o marcado por linha vermelha é 5.8GHz.

Figura 13: Pontos da rede.
Fonte: Google Earth

6.1.1.1 Antena Parábola Grade USB 25 dbi

A Antena Parábola Grade USB 25 dbi da Aquario é quem manda o sinal 2.4Ghz entre os diferentes pontos da rede. Está antena é responsável por amplificar o sinal dos rádios para uma melhor qualidade e menor taxa de perda, cada um dos quatro pontos possui uma. Abaixo na figura 14 observa-se à antena fabricada pela Aquario.

Figura 14: Antena Parábola Grade USB 25 dbi
Fonte: http://www.aquario.com.br

6.1.1.2 Antena WLL60

Este modelo de antena o WLL60 da Zirok Eletrônica é que fica responsável pelo *backbone* de 5.8 GHz entre a Prefeitura Municipal e a antena do provedor de sinal de internet. Esta antena é responsável pela chegada da web ao *switch* de onde é distribuída aos pontos interligados. Abaixo é apresentada uma imagem da antena fabricada pela Zirok.

Figura 15: Antena WLL60
Fonte: www.zirok.com.br

6.1.2 Rádios Outdoor

Os rádios utilizados são dois modelos diferentes do mesmo fabricante. O primeiro deles conhecido como Nano Station 2 fica responsável pela transmissão de sinal 2.4GHz, e o segundo Nano Station 5 é o transmissor 5.8GHz. Estes *acess points* estão configurados para utilizar restrição de MAC entre eles, além de usar criptografia wap2. Assim gerando maior segurança dos dados que trafegam na rede. Abaixo na figura 16 está o Nano 2 de diferentes ângulos.

Figura 16: *Nano Station* 2
Fonte: http://www.ubnt.com

Este rádio *Nano Station* 2 é o mais utilizado, pois é com ele que e montado o circuito de 2.4GHz que interliga os pontos. Além de utilizar dispositivos de segurança os acess points estão ligados em forma de bridge, fazendo do sinal sem fio uma ponte entre as redes. Abaixo se observa as principais especificações do NS2.

CPU	Atheros 180MHz MIPS
RAM	16MB RAM
Flash	4MB FLASH
Wireless	2.4GHz, 802.11b/g
Channel width	5/10/20MHz
Antenna Gain	10dBi x2
Polarity	Adaptive Vertical/Horizontal
Ext. Ant. Option	Yes, RP-SMA Connector
Range	15km+ (100km using ext ant.)
Throughput	25Mbps+ TCP/IP
Mounting	Pole Mount (straps included)

Accessories	Ubiquiti Window/Wall Mount (sold seperately)
Size	26.4cm x 8cm x 3cm
Weight	0.4 kg
Power Supply	12V, 1A POE (included)
Approvals	FCC 15.247, IC, CE

Quadro 2: Especificações do Rádio *Nano Station* 2
Fonte: www.ubnt.com

6.1.3 Rádios Indoor

Além da estrutura externa são utilizados rádios para conexão dos *notebooks indoor*. Estes dispositivos são mais sucessivos a ataques, pois são de responsabilidade dos profissionais internos da Prefeitura ao contrário dos *outdoors* que estão sob responsabilidade de uma empresa terceirizada.

Os acess points utilizados são da marca D-link modelo DWL-2100, configurados com autenticação WPA2, também contam com DHCP Server ativo, mas sem restrição por MAC, pois a rotatividade de equipamentos é grande. Cada um dos pontos aonde chega o sinal sem fio das torres possuem um rádio desses que trabalha na freqüência 2.4GHz para distribuição na rede interna. Abaixo na figura 17 podemos visualizar o dispositivo.

Figura 17: AP D-link DWL-2100
www.dlink.com

O experimento será exatamente feito nestes pontos de acesso, pois o sinal é forte o suficiente para ser recebido do lado de fora dos prédios. Fazendo assim, que qualquer pessoa que esteja munida de um equipamento com dispositivo *wireless*, possa tentar fazer uma tentativa de ataque as redes. Na tabela abaixo estão às principais características do D-link 2100AP.

Standards	• IEEE 802.11g • IEEE 802.11b • IEEE 802.11 • IEEE 802.3 • IEEE 802.3u
Device Management	• Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java- enabled browsers. • SNMP v.3
Wireless Distribution System	• AP Client • PtP Bridge • PtMP Bridge • Repeater
Security	• 64, 128, 152-bit WEP • 802.1X (EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP) • WPA —Wi-Fi Protected Access • MAC Address Access Control (WPA-TKIP and WPA-AES)
Media Access Control	• CSMA/CA with ACK
Wireless Frequency Range	• 2.4GHz to 2.4835GHz
Wireless Signal Range	• Indoors: Up to 328 ft (100 meters) • Outdoors: Up to 1312 ft (400 meters)
Modulation Technology	• Orthogonal Frequency Division Multiplexing (OFDM) • Complementary Code Keying (CCK) • DQPSK • DBPSK
Wireless Transmit Power	• 15dBm (32mW) ± 2dB (Control TX power level from full, 50%, 25%, 125% and min.)
Receiver Sensitivity*	• 54Mbps OFDM, 10% PER,-66dBm) • 48Mbps OFDM, 10% PER,-71dBm • 36Mbps OFDM, 10% PER,-76dBm • 24Mbps OFDM, 10% PER,-80dBm • 18Mbps OFDM, 10% PER,-83dBm • 12Mbps OFDM, 10% PER,-85dBm • 11Mbps CCK, 8% PER,-83dBm • 9Mbps OFDM, 10% PER,-86dBm • 6Mbps OFDM, 10% PER,-87dBm
	• 2Mbps QPSK, 8% PER,-89dBm
External Antenna Type	• 1.0dB Dipole with reverse SMA connector

Quadro 3: Especificações do Rádio D-link 2100AP
Fonte: www.d-link.com

6.1.4 Switches

Os switches utilizados para interligar os rádios com a rede local são os: Micronet SP1678. Possuem 24 portas 10/100 e 1 porta 10/100/1000, que faz a interligação *gigabit* desde rack via fibra óptica com a central onde ficam os servidores. Além de ser possível gerenciá-los remotamente estes *switches* possuem filtro por MAC que é uma excelente ajuda para segurança das informações por eles trafegadas.

Abaixo na figura 18 está o rack com os *switches* e também com os *patch panels* que fornecem flexibilidade a instalação.

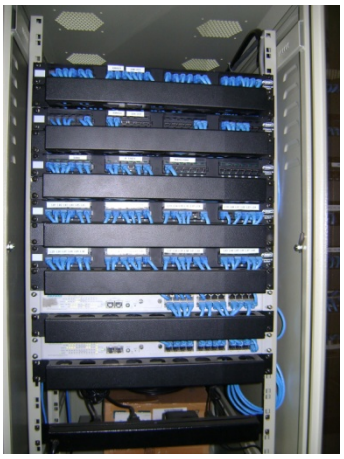

Figura 18: Rack da Secretaria de Saúde
Fonte: Elaboração do Autor

6.2 Equipamentos Utilizados

Os equipamentos abaixo citados foram utilizados para validação dos métodos de ataque as redes sem fio, a fim de comprovar sua eficácia.

- *Notebook1*: O modelo utilizado é o Acer Aspire 5920, que esta operando com o sistema da Microsoft Windows Vista e conta também com o LINUX Ubuntu 8.10. O dispositivo de acesso wireless que veio de fabrica instalado é o Intel Wireless 3945ABG Network Connetion.

- *Notebook2*: Foi utilizado como segundo computador para efetuar os testes um modelo da HP o Pavilion dv6263, rodando o Windows XP sem nenhuma atualização feita. O dispositivo Wi-Fi de fabrica é o Intel Wireless 3945ABG.

- *Acess Point*: Foi utilizado nos testes o D-Link 2100AP com freqüência de 2.4GHz.

6.3 Explorando as vulnerabilidades

Com a ajuda dos dispositivos *wireless* disponíveis serão testadas algumas técnicas estudadas neste trabalho, para avaliar a segurança oferecida pela rede aos seus usuários.

6.3.1 Explorando Associação Maliciosa

Mesmo mantendo todo o cuidado com a segurança da rede sem fio, ninguém está a salvo do ataque de associação maliciosa. Os usuários que não possuem conhecimento específico podem facilmente conectar seus computadores a uma rede distinta sem perceber que está não é de fato a rede correta.

Para realizar este experimento foi instalado o modulo *Host AP* instalado no *notebook1* com o Linux Ubuntu 8.10. Este módulo permite que um computador com dispositivo *wireless* trabalhe de forma semelhante a um *acess point*. Abaixo na figura 19 se pode observar o modulo sendo iniciado.

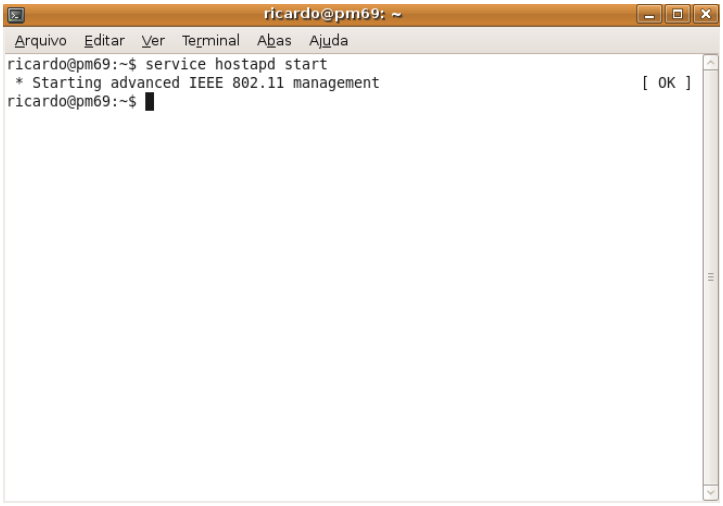

Figura 19: Modulo *HostAP* sendo iniciado
Fonte: Elaboração do Autor

Para comprovação da falha se segurança, foi instalado no *notebook2* uma cópia do Windows XP sem atualizações. Foi observado que o computador conecta-se ao falso *acess point*, comprovando que a associação maliciosa funciona mesmo sem intervenção do usuário. Neste caso basta ao atacante analisar o trafego de rede ou capturar as informações que desejar.

No caso prático foi preparado um ambiente para que fosse possível realizar o ataque, mas nada impede que uma das máquinas internas faça acidentalmente a conexão no falso *acess point* permitindo que dados sejam de fato capturados.

6.3.2 Explorando *eavesdropping*

Para comprovar a possibilidade da captura de pacotes da rede sem fio, foi utilizado o *notebook1* com o software *Kismet* instalado, rodando em modo *console* no LINUX Ubuntu 8.10. No Ubuntu que é derivado do *Debian* o *Kismet* é facilmente instalado usando o *apt-get*. Na figura 20 observa-se que o programa consegue localizar além da rede a qual estamos estudando o comportamento (PM_Portao_01) outra rede distinta (CaiwebR).

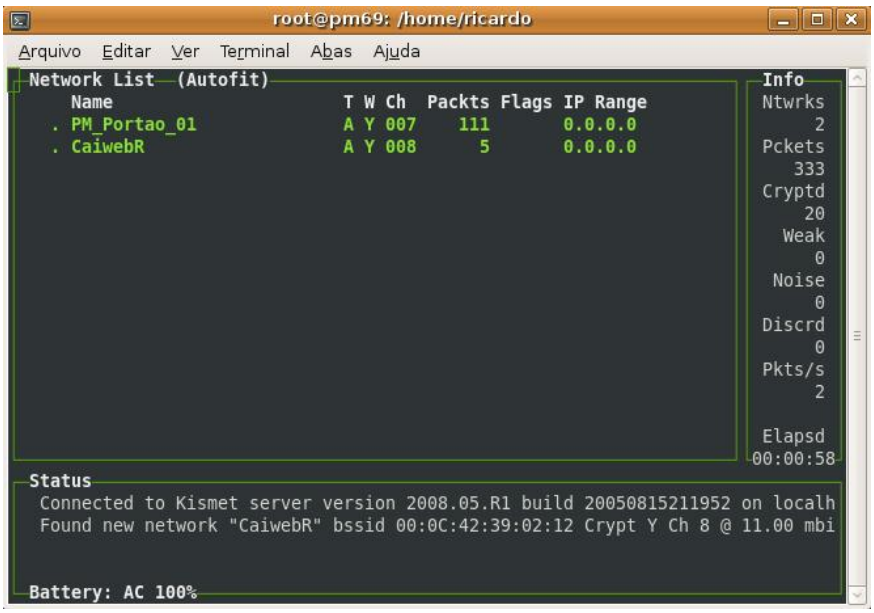

Figura 20: Software *Kismet*
Fonte: Elaboração do Autor

Para conseguir total atenção para a rede em questão, foi utilizado o comando de seleção com as teclas *Shift*+L e as setas, pois mesmo sem querer o *Kismet* estava obtendo dados da outra rede. Todo esse trafego de rede fica salvo em disco para depois ser utilizado para exploração de informações com outros softwares.

Avaliando os arquivos gravados pelo programa nota-se que o *Kismet* facilmente conseguiu encontrar e exibir informações importantes como: ESSID, BSSID, *Encryption*, *Range* de IP e *NetType* entre outras. Isso comprova a falta de segurança na rede, pois um atacante que tenha conhecimento deste software terá a possibilidade de capturar pacotes de informações que conseqüentemente permitiram a ele ter acesso a *wireless*.

6.3.3 Explorando o ataque de força bruta

Para a realização deste método, foi utilizado o *Notebook1* com o software *Kismet* para capturar o trafego de rede durante 24 horas. Nesse período o programa gerou um arquivo

com a extensão .dump de 500mb. Para efetuar o ataque de força bruta foi utilizado o software *Aircrack-ng* instalado no mesmo *notebook1* só que rodando no Windows Vista.

Este experimento foi realizado em ambiente simulado reduzindo o numero de caracteres da senha da rede sem fio e também foi alterado o protocolo de WPA para WEP 128bits tentando assim ter êxito no teste. Abaixo é mostrada na figura 21 a tela do software Aircrack-ng onde podemos observar o trabalho na tentativa de quebra de senha além do tempo total da pesquisa.

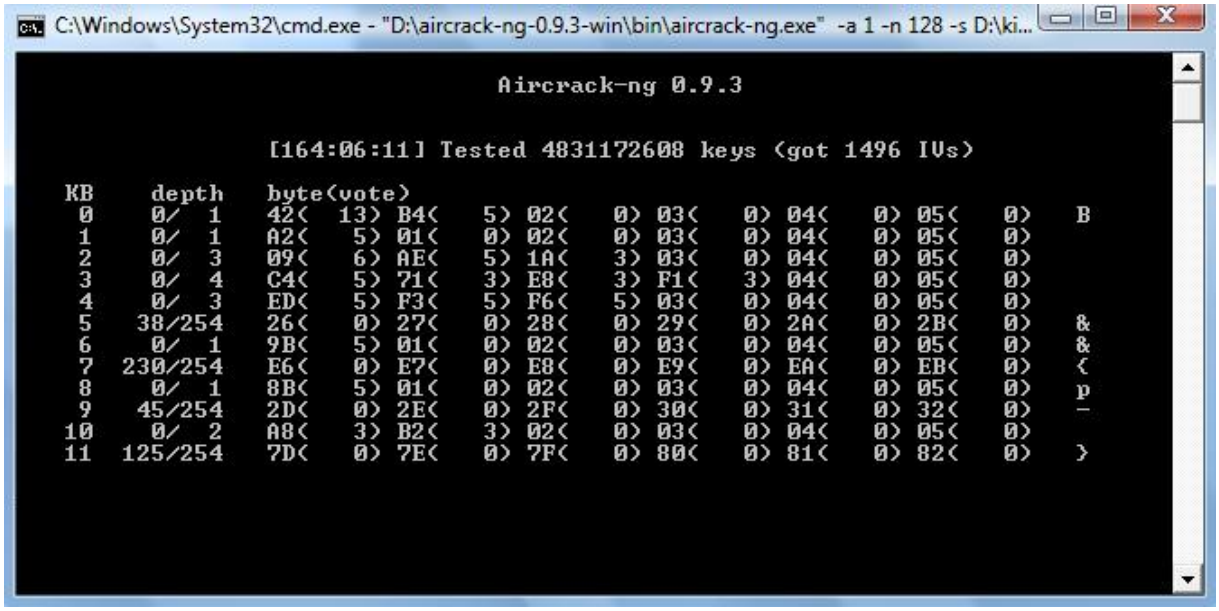

Figura 21: Tela do Aircrack-ng
Fonte: Elaboração do Autor

Mesmo reduzindo a segurança, alterando as configurações padrões não se obteve êxito no experimento. O programa trabalhou por um longo período de tempo e não conseguiu trazer o resultado esperado.

6.4 Análises das Redes

Será utilizado o relatório de analise de vulnerabilidades proposto por este trabalho para fazer uma avaliação das redes indoor e outdoor deste cenário apresentado.

6.4.1 Análise da rede *Indoor*

Para uma perfeita análise da rede *indoor*, será preenchido o relatório de análise de vulnerabilidades para ajudar a obter os resultados, além de serem consultados os experimentos feitos sobre a *wireless* em questão.

Relatório para Análise de Vulnerabilidades das Redes sem Fio					
1	**Informações Gerais**				
1.1	Local da Rede: Rua 9 de Outubro, nº229 - Portão, RS				
1.2	Responsável pela Rede: Ricardo Dalmoro Basso				
1.3	Rádio Utilizado: D-Link 2100AP				
1.4	Freqüência do Rádio: 2.4GHz				
1.5	Modo de Operação: AP Router				
1.6	SSID da Rede: PM_Portao_01				
2	**Segurança**				
2.1	Período de Troca de Senha: 7 dias				
2.2	Método para Conexão Segura	VPN	RADIUS	OUTROS	**NÃO**
2.3	Protocolo de Segurança Utilizado	WEP	**WPA**	WPA2	NÃO
2.4	Antena Para Transmissão	SIM	**NÃO**		
2.5	Filtro MAC	SIM	**NÃO**		
2.6	Hide SSID	SIM	**NÃO**		

Preparado por: Ricardo Dalmoro Basso	Data: 01/06/2009

Como se pode observar no relatório o rádio trabalha em 2.4 GHz com segurança WPA. Com foi visto no capitulo anterior não é aconselhável a utilização do protocolo WPA, pois a uma grande perde de desempenho no trafego de rede por conta de sua encriptação dos dados. Neste caso o roteador possui suporte a WPA2 é aconselhável a mudança de protocolo para o aumento de performance e considerável ganho de segurança.

O período para troca de senha fixado em sete dias é fundamental para evitar que caso os atacantes consigam descobri-la possam utilizá-la de maneira indevida por um largo período de tempo. Além da atenção de trocá-la com freqüência, também é utilizada uma forma padrão para construção que conta com caracteres alfanuméricos dificultando a tarefa para os softwares.

Nesta rede não é utilizado nenhum meio de conexão segura e também não conta com filtro MAC. Como o acess point é utilizado de modo a transformar o sinal do meio físico para o sem fio e fornecer-lo para dispositivos diversos e alternados seria complicado o uso de alguma dessas técnicas. Mesmo assim, poderia ser utilizada a técnica de hide SSID a fim de aumentar a segurança da rede.

A antena utilizada para transmissão do sinal é a própria do aparelho que consegue ter uma boa qualidade de sinal nos pontos onde é previsto o Wi-Fi.

Como foi visto nos experimentos feitos na rede, pode-se observar que está rede é segura mesmo sendo possível capturar informações com os softwares testados, não foi possível quebrar a senha mesmo deixando ela em processamento por um grande período de tempo. Com isso não foi possível acessá-la e utilizar outro *sniffer* para filtrar informações vitais.

6.4.2 Análise da Rede Outdoor

A análise da rede outdoor foi feita através do preenchimento do relatório pela empresa responsável pelo circuito de dados para chegar às devidas conclusões. A rede em questão é uma das bridges que interligam a Secretaria de Saúde do Município com um dos postos de saúde. As outras três redes são exatamente iguais a está, com a mesma configuração e os mesmos dispositivos.

Abaixo Segue o relatório preenchido por completo e a seguir as conclusões tiradas a partir dele.

Relatório para Análise de Vulnerabilidades das Redes sem Fio					
1	**Informações Gerais**				
1.1	Local da Rede: Rua 9 de Outubro, nº229 - Portão, RS				
1.2	Responsável pela Rede: CaiWEB				
1.3	Fabricante do Rádio: Ubiquiti				
1.4	Modelo de Rádio Utilizado: Nano Station 2				
1.5	Freqüência do Rádio: 2.4GHz				
1.5	Modo de Operação: Bridge				
1.6	SSID da Rede: linkpref1				
2	**Segurança**				
2.1	Período de Troca de Senha: 1 mês				
2.2	Método para Conexão Segura	VPN	RADIUS	OUTROS	**NÃO**
2.3	Protocolo de Segurança Utilizado	WEP	WPA	**WPA2**	NÃO
2.4	Antena Para Transmissão	**SIM**	NÃO		
2.5	Filtro MAC	**SIM**	NÃO		
2.6	Hide SSID	SIM	**NÃO**		

Preparado por: Ricardo Dalmoro Basso	Data: 01/06/2009

Está rede está muito bem configurada que se diz respeito à segurança. Pois conta com o protocolo de segurança WPA2 que fornece ótima proteção e estabilidade a rede sem fio. Trabalha também com filtro MAC entre os rádios, conseguindo fazer um circuito fechado com as demais antenas somente de MAC´s válidos.

Todas as antenas utilizadas para transmissão do sinal são direcionais, uma apontada para outra dando assim melhor desempenho e menor perda de pacotes. Este circuito de dados funciona com os rádios configurados para *bridge* fazendo com que a rede sem fio se torne um cabo através do ar.

Outro fator determinante em se tratando de segurança de rede é o fato da limitação da linha de visada, ou seja, o potencial intruso teria que se posicionar entre a linha de visada dos dois aparelhos, transmissor e receptor, para conseguir captar o sinal, limitando em muito sua atividade e disponibilidade.

A senha de criptografia é trocada a cada um mês, pois possui 25 posições, intercalando números, letras e caracteres alfanuméricos dificultado bastante o trabalho de quem por ventura tende atacar esta rede.

Além disso, esta rede conta com monitoramento constante do sinal. Utilizando o software *Winbox*, a empresa terceirizada tem uma visão completa do cenário e de como ele esta se comportando com as diversas variáveis ambientes. Abaixo se observa a tela do *Winbox* com o circuito de dados.

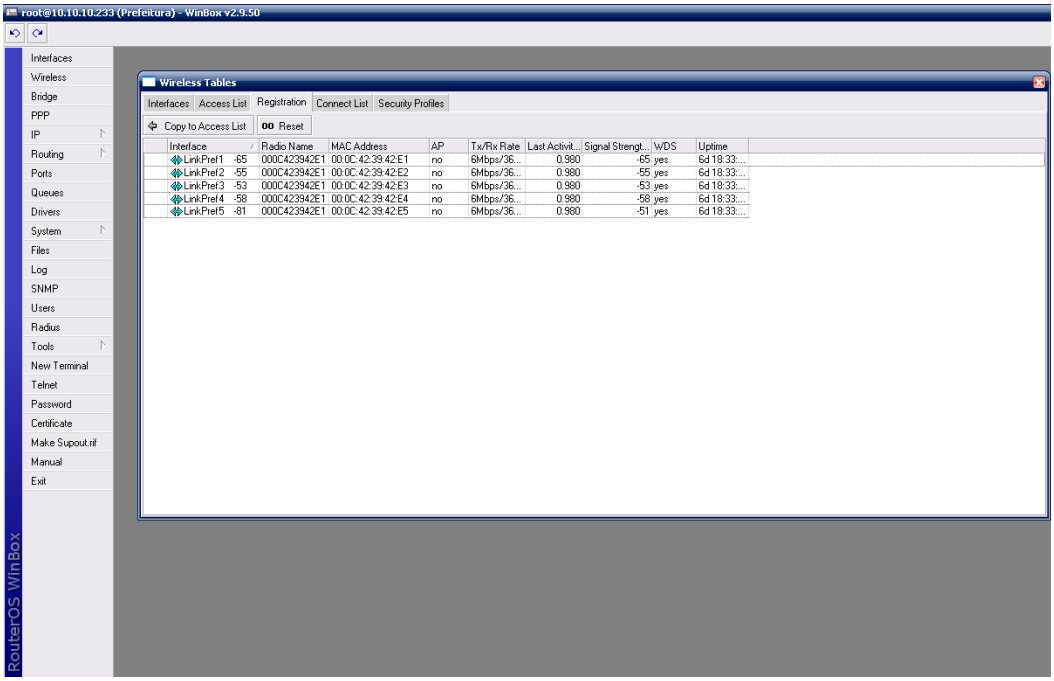

Figura 22: Software *Winbox*
Fonte: Elaboração do Autor

Existe um funcionário capacitado nesta empresa que é responsável por este monitoramento constante. Abaixo na figura 23 está ampliada a tela do *Winbox* e podemos ver somente a tela *Wireless Tables* onde mostra circuito de dados com suas especificações.

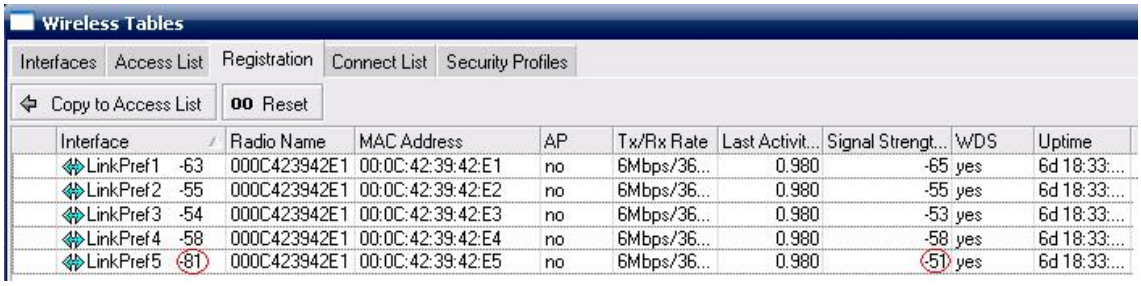

Figura 23: Software *Winbox - Wireless Tables*

Na figura 23 acima, observa se que foi circulado em vermelho dois valores referentes ao Linkpref5. A intenção disso em ambiente simulado é mostrar a detecção de alteração no meio de transmissão acima do normal, no nível 1 camada física. Existem duas possibilidades possíveis para isto estar acontecendo.

- Possibilidade 1 – Falha de segurança: outro receptor com a mesma criptografia ou utilizando clone MAC para transpor o filtro, porém em locais e distâncias diferentes.

- Possibilidade 2 – Problemas no equipamento: interferência no meio de transmissão, mal contato de um conector, desalinhamento das antenas entre outros problemas.

Por esses motivos citados podemos dar uma avaliação positiva desta rede, pois com todos estes cuidados dificilmente alguém conseguira burlar todos estes mecanismos de segurança.

CONCLUSÃO

Este trabalho de pesquisa teve como objetivo estudar os meios de segurança para as redes sem fio e fazer um estudo em ferramentas e métodos maliciosos. Este projeto possibilitou um aprofundamento em diversas áreas referentes às redes *wireless*.

O experimento realizado serviu para validar as técnicas que ficaram em maior evidência e também para verificar a real situação de segurança da rede abordada. A elaboração do relatório com os principais pontos estudados ofereceu maior simplicidade para verificar o tipo de proteção oferecida pelos diferentes métodos descritos.

Todas as ferramentas desta pesquisa são encontradas em sites na internet aumentando assim a insegurança das redes sem fio. Além dos softwares estas páginas possuem documentação e fóruns de ajuda, que contribuem desde a instalação até a utilização.

Mesmo com todo o material disponível na internet sobre as vulnerabilidades das redes sem fio, também contando com a pesquisa deste presente trabalho, pode-se afirmar que existem métodos que não são de fácil exploração. Ou seja, somente alguém com um bom conhecimento específico na área de tecnologia têm a capacidade de utilizá-los, fazendo assim com que estás falhas de segurança continuem inexploradas.

Os métodos e ferramentas explorados neste trabalho são comuns e bem conhecidos. Mesmo que fosse descritos e explorados todos, isto não seria uma indicação de que outros não pudessem ocorrer.

Além do uso dos protocolos de segurança ou de qualquer outro método, é extremamente importante uma boa política de administração de rede, com autenticação de usuários em domínios, *firewalls*, entre outros. Isso é imprescindível para minimizar os problemas nas redes e assim deixá-las mais confiáveis.

Para dar continuidade a está pesquisa, abaixo são apresentadas algumas propostas de trabalhos futuros.

Com a conclusão deste projeto de pesquisa foi observado que poderia ser elaborado um relatório em que fosse possível dar notas para cada um dos itens, assim conseguindo chegar a um resultado mais simples sem a necessidade de análise. Dessa forma poderia até mesmo ser elaborado um software onde o utilizador responderia perguntas e ao final teria uma resposta.

Outra idéia seria desenvolver um software para monitorar o nível de sinal das redes sem fio, medindo e chegando a uma média. Com isso seria possível disparar um alarme quando este sinal estivesse com uma alteração de potência maior que a média, identificando algo errado na rede. Problemas como mal contato nos conectores e desalinhamento das antenas entre outros, poderiam ser detectados através deste software.

BIBLIOGRAFIA

AIRCRACK. **Tutorial**. Disponível via URL em: http://www.aircrackng.org/doku.php?id=simple_wep_crack. Acesso em: 30/03/2009.

ALBUQUERQUE, Luciano Renovato de. **Uma Visão Geral do Funcionamento do Protocolo RADIUS.** 2003. Disponivel em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=81. Acessado em: 10/05/2009

BABOO, Fórum. 5. **Ataques às Redes Sem Fio**. 2005. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=335352. Acessado em: 02/05/2009.

CHIN, Liou Kuo. **Rede Privada Virtual – VPN.** 1998. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acessado em: 10/03/2009.

D-LINK. Building Networks for People. **DWL-2100AP.** Disponível em: http://www.dlinkla.com/home/productos/producto.jsp?idp=497. Acessado em: 15/05/2009.

DUARTE, Luiz Otávio. **Análise das Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão de Curso. São José do Rio Preto: UNESP, 55p.

EARLE, Aaron E. **Wireless Security Handbook**. United States of America: Auerbach Publications, 2006. 354p.

IEE, Institute of Electrical and Electronics Engineers. **IEE Standards**. Disponível em <http://www.ieee.org/standards> Acesso em: outubro de 2008

KISMET. **Documentation**. Disponível via URL em: http://www.kismetwireless.net/. Acesso em:18/04/2009.

MALBURG, Maria Moura. **Modulação**. Trabalho Final de Redes I. UFRJ 2004.

OZORIO, Wellington Cesar. **Análise Comparativa entre os Protocolos de Segurança WEP,WPA e WPA2.** Trabalho de Conclusão de Curso. Jaguariuna, FAJ 2007. 66p.

PRODANOV, Cleber Cristiano. **Manual de metodologia científica.** 3.ed. Novo Hamburgo: Feevale, 2006. 77 p.

ROSS, John. **Wi-Fi – Instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003. 246p.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. 2.ed. São Paulo: Novatec, 2005. 224p.

SILVA, Lino Sarlo da. **Virtual Private Network.** São Paulo: Novatec, 2002.

SOARES, Alcenir Barbosa, **Analise de qualidade de serviço VPN – Redes Privadas Virtuais – Utilizando redes sem fio**. Minas Gerais: 2004, 69p. Monografia (Graduação em Sistemas de Informação) – Faculdade de Ciências Aplicadas de Minas, UNIMINAS, 2004.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003

TORRES, Gabriel. **Redes de Computadores Curso Completo**. Rio de Janeiro: Axcel Books, 2001. 664p.

UBIQUITI. Ubiquiti Networks. **NanoStation.** Disponível em: http://www.ubnt.com/products/nano.php. Acessado em: 20/05/2009.

VIEIRA, Luiz. **ARP Poisoning.** 2008. Disponível em: http://imasters.uol.com.br/artigo/10117/seguranca/arp_poisoning. Acessado em: 20/05/2009

WI-FI Alliance. **Wi-Fi standards**. Disponível em <http://www.wi-fi.org > Acesso em: Setembro de 2008.