CENTRO UNIVERSITÁRIO FEEVALE

ISRAEL TIAGO FERRASSO

SEGURANÇA E VULNERABILIDADE EM REDES WIRELESS PROTEGIDAS COM WEP

Novo Hamburgo

2011

ISRAEL TIAGO FERRASSO

SEGURANÇA E VULNERABILIDADE EM REDES WIRELESS PROTEGIDAS COM WEP

Trabalho de Conclusão de Curso
apresentado como requisito parcial
à obtenção do grau de Bacharel em
Sistemas de Informação pela
Universidade Feevale

Orientador: Vandersilvio da Silva

Novo Hamburgo
2011

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial minha família, amigos, professores e ao meu orientador, que não deixou que eu desanimasse em nenhum momento.

RESUMO

Hoje em dia a crescente necessidade de estarmos conectados ao mundo virtual, compartilhando dados de forma cada vez mais rápida, em maior quantidade e onde quer que estejamos, torna o acesso às redes wireless (sem fio) um grande avanço para suprir tal necessidade. O crescimento destas redes, cada vez mais utilizadas pelas pessoas em suas residências e ainda mais pelas empresas, faz com que a necessidade de segurança das informações trafegadas seja cada vez melhor e de grande eficiência. Atualmente são utilizados os protocolos de segurança WEP, WPA e WPA II. Até que ponto eles provêm à segurança dos dados na rede sem fio? O foco central da pesquisa e experimentos foi para mostrar a deficiência do protocolo WEP, que serviu para comprovar através de quebra de senhas e criptografias utilizando técnicas e ferramentas próprias para este fim, a grande vulnerabilidade deste protocolo.

Palavras-chave: Segurança. Wireless. Criptografia. Cracking. WEP.

ABSTRACT

Today the growing need to stay connected to the virtual world, sharing data with ever faster, in greater quantity and wherever we are, makes access to wireless networks (wireless) to supply a major breakthrough this need. The growth of these networks, increasingly used by people in their homes and even more companies, makes the need for information security is getting better trafficked and high efficiency. Are currently used security protocols WEP, WPA and WPA II. To what extent do they provide data security on the wireless network? The central focus of research and experiments was to show the deficiency of the WEP protocol, which served to prove through password cracking and encryption techniques and tools for this purpose, the great vulnerability of this protocol.

Keywords: Security. Wireless. Cracking. WEP.

LISTA DE FIGURAS

LISTA DE ABREVEATURAS E SIGLAS

AES	*Advanced Encryption Standart*
APs	*Acsses points*
ARP	*Address Resolution Protocol*
CPU	*Central Unit Processor*
Gbps	*Gigabits por Segundo*
Ghz	*Giga Hertz*
GPS	*Global Positioning System*
IDS	*Iintrusion detection system*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IP	*Internet Protocol*
IV	Vetor de Inicialização
LAN	*Local Area Network*
MAC	*Media Access Control*
Mbps	*Megabits por Segundo*
MIC	*Message Integrity Code*
MIMO	*Multiple Input – Multiple Output*
MIT	*Massachusetts Institute of Technology*
OFDM	*Orthogonal frequency-division multiplexing*
OSI	*Open Systems Interconnection*
PSK	*Pre-Shared Key*
RC4	*Ron's Code 4 ou Rivest Cipher 4*
RFMON	*Radio Frequency Monitor*
SSID	*Service Set Identifier*
TCP	*Transmission Control Protocol*
TKIP	*Temporal Key Integrity Protocol*
UDP	*User Datagram Protocol*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	*Wi-fi Protected Access*
WPAII	*Wi-fi Protected Access II*

SUMÁRIO

INTRODUÇÃO

A necessidade de troca de informação cada vez mais rápida e eficiente, fez com que houvesse um grande avanço nas transmissões de dados com computadores através da internet, tornando também o acesso à rede sem fio uma escolha que facilitasse a conexão de forma rápida e prática.

Esta facilidade e praticidade tornaram estas redes muito populares nas casas e empresas e também em locais de grande circulação como aeroportos, restaurantes, hotéis e shoppings. Isso acaba fazendo com que poucas pessoas venham a se preocupar com a segurança da rede na qual estão conectadas, navegando e trocando informações de forma aparentemente sigilosa e segura.

Estes equipamentos são facilmente encontrados e possuem diversos fabricantes e configurações diferenciadas. Em questão de segurança de redes Wireless, temos hoje os protocolos padrões WEP (*Wired Equivalent Privacy*), WPA (*Wi-fi Protected Access*) e WPA II (*Wi-fi Protected Access II*).

Os equipamentos para estas instalações possuem grande facilidade de instalação. Esta facilidade acaba fazendo com que as configurações de segurança do equipamento não sejam adotadas corretamente, seja por receio ou mesmo desconhecimento de tais funções por parte do usuário.

Hoje em dia, a grande facilidade na captura de sinas de Wireless, trouxe a tona diversos estudos e ferramentas de Cracking, buscando encontrar vulnerabilidades de segurança em redes wireless. Sendo isto executado por profissionais na área de segurança ou até hobbistas que querem divulgar falhas ou prover informações ao publico, como pessoas que queiram se aproveitar dessas falhas para tirar proveito próprio ou mesmo causar danos em redes públicas e privadas.

As redes sem fio se tornaram um dos principais alvos de ataques para se chegar aos sistemas das empresas, principalmente por ser uma das portas de entrada mais fácil, pois para se tentar acesso à rede desejada, basta estar ao alcance do sinal.

Da mesma forma que redes cabeadas, os riscos das redes sem fio precisam ser conhecidos, para então serem minimizados, uma vez que as redes sem fio ganham um risco

extra devido o meio de transporte ser o próprio ar. Basta que o invasor esteja na área de abrangência do sinal. (RUFINO, 2005)

Com isso, se exige cada vez mais cuidado em relação à segurança para que os protocolos escolhidos venham atender aos requisitos mínimos de segurança necessários para garantir a integridade das informações.

Uma rede Wi-fi precisa ter pelo menos três serviços básicos de segurança:

- **Autenticação:** Garantir que somente clientes pertencentes à rede poderão acessar está após serem autenticados;

- **Privacidade:** Garantir a privacidade dos dados disponíveis na rede, avaliando se estes poderão ser vistos por clientes que tiverem autorização.

- **Integridade:** Garantir que os dados transmitidos não sejam modificados no caminho de ida e volta entre os clientes e os APs (*Acsses points*).

Para ter uma rede nessas condições, é necessário configurar recursos adicionais, como criptografia e autenticação forte, elementos esses que não fazem parte da configuração básica e que demandam tempo e trabalho para configuração e manutenção, tanto no concentrador quanto nos clientes e demais equipamentos que dessa rede façam uso. (RUFINO, 2005)

Sendo assim, este projeto irá verificar quão fácil é para alguém que tenha uma ferramenta de intrusão acessar um Ponto de Acesso de uma rede Wireless protegida com o protocolo de segurança WEP.

1. REDES SEM FIO

1.1 Redes Ad-hoc

As redes ad-hoc (também conhecidas como redes Manet), são redes sem fio que não tem a necessidade de um ponto de acesso comum aos computadores conectados a ela, não são estruturadas. Dessa forma, todos os dispositivos da rede funcionam como se fossem um roteador, encaminhando as informações que vêm de dispositivos. Na figura abaixo um exemplo de conexões ad-hoc:

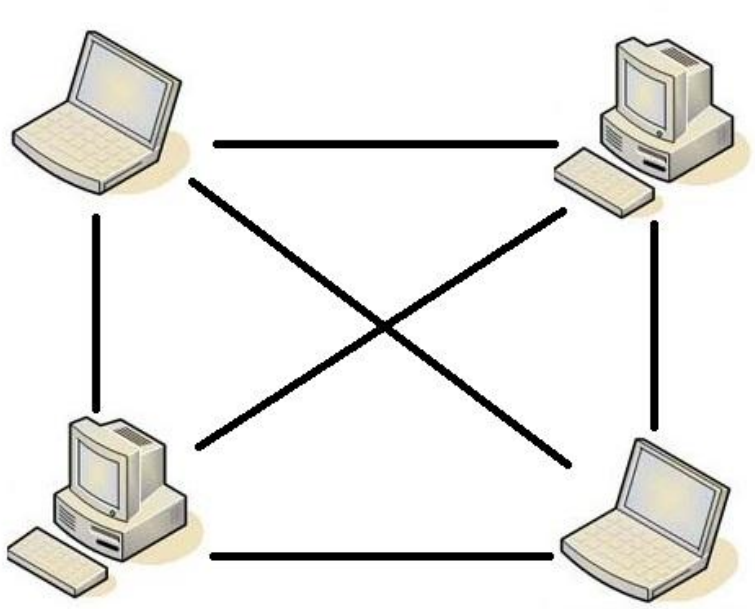

Figura 1 – Rede Wireless não estruturada (Ad-hoc)

A definição de rede Ad-hoc conforme Microsoft (2008) é:

> "Uma rede Ad-hoc é uma conexão temporária entre computadores e dispositivos usados para uma finalidade específica, como compartilhamento de documentos durante uma reunião ou jogos de computador com vários jogadores. Você também pode compartilhar temporariamente uma conexão de Internet com outras pessoas da sua rede Ad-hoc, para que essas pessoas não precisem fazer suas próprias configurações de Internet. As redes Ad-hoc são somente sem fio, portanto, você deve ter um adaptador de rede sem fio instalado no computador para configurar ou ingressar em uma rede Ad-hoc."

O acesso a esta rede não é limitado a computadores e notebooks. Diversos modelos de aparelhos celulares, impressoras e outros dispositivos, já vêm com suporte a redes ad-hoc, tornando essa rede mais prática para uso.

Já as redes sem fio estruturadas, dependem de um ponto de acesso (AP), centralizado para poderem fazer a comunicação entre si, conforme a figura abaixo:

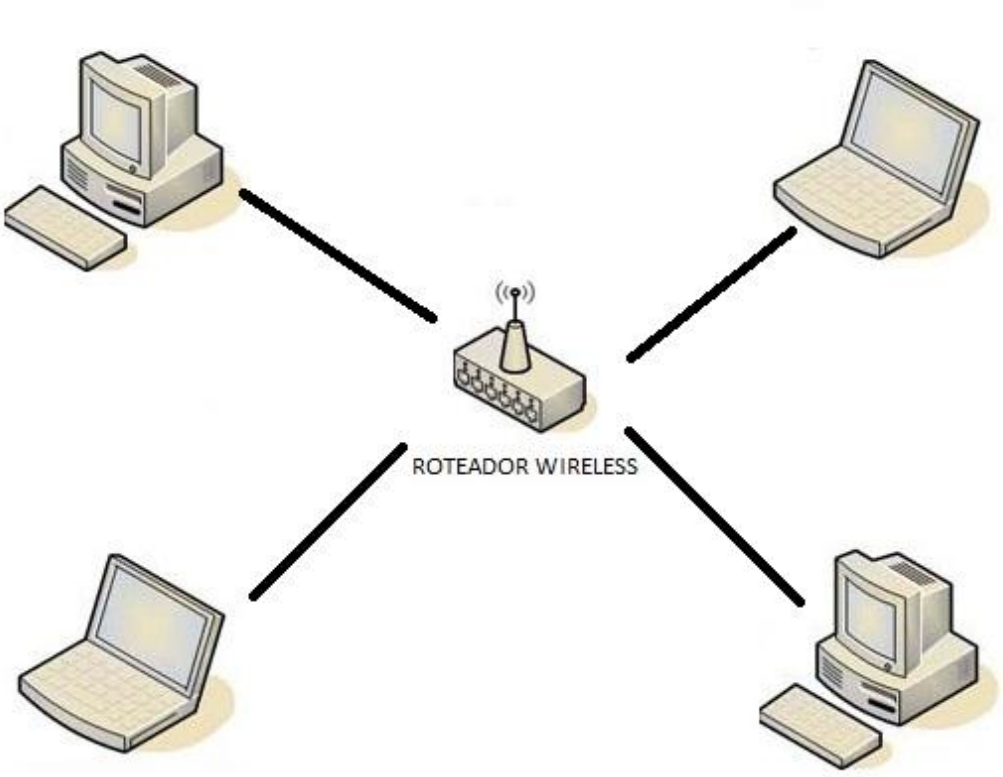

Figura 2 – Rede Wireless Estruturada

Vantagens e Desvantagens de Redes Ad-hoc

Várias vantagens e desvantagens podem ser citadas ao se comparar redes ad hoc com redes estruturadas e com redes fixas (cabeamento estruturado). Segundo Pinheiro (2005), estas são as principais vantagens e desvantagens encontradas nessas redes:

Vantagens:

- Instalação rápida: Redes ad hoc podem ser estabelecidas dinamicamente em locais onde não haja previamente uma infraestrutura instalada;

- Tolerância à falhas: A permanente adaptação e reconfiguração das rotas em redes ad hoc permitem que perdas de conectividade entre os nós possam ser facilmente resolvidas desde que uma nova rota possa ser estabelecida;

- Conectividade: Dois nós móveis podem se comunicar diretamente desde que cada nó esteja dentro da área de alcance do outro;

- Mobilidade: esta é uma vantagem primordial com relação às redes fixas.

Desvantagens:

- Roteamento: A mobilidade dos nós e uma topologia de rede dinâmica contribuem diretamente para tornar a construção de algoritmos de roteamento um dos principais desafios em redes ad hoc;

- Localização: Uma questão importante em redes as hoc é a localização de um nó, pois além do endereço da máquina não ter relação com a posição atual do nó, também não há informações geográficas que auxiliem na determinação do posicionamento desse nó;

- Taxa de erros: A taxa de erros associada a enlaces sem-fio é mais elevada quando comparada aos enlaces em redes estruturadas;

- **Banda passante**: Com cabeamento convencional, a banda passante pode chegar a 1Gbps. Nos enlaces via redes wireless temos taxas de até 2Mbps tipicamente.

1.2 Redes 802.11b

Publicado em outubro de 1999, o 802.11b foi o primeiro padrão wireless usado em grande escala e a popularizar a tecnologia, permitindo que placas de diferentes fabricantes se tornassem compatíveis e os custos caíssem, graças ao aumento na demanda e à concorrência.

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na frequência de 2.4 GHz e é justamente ai seu ponto mais negativo, segundo Rufino:

Faixa de frequência utilizada por uma vasta quantidade de equipamentos e serviços, como aparelhos de telefone sem fio, bluetooth , forno de micro-ondas, babás eletrônicas e pelos padrões 802.11b e 802.11g, este monte de equipamentos utilizando esta frequência torna esta faixa de frequência cada vez mais suja. [RUFINO, 2005].

1.3 Redes 802.11a

O padrão seguinte foi o 802.11a (que na verdade começou a ser desenvolvido antes do 802.11b, mas foi finalizado poucos dias depois).

O padrão 802.11a tem como uma das grandes vantagens a taxa de transmissão de 54 Mbps e opera na frequência de 5Ghz, sendo que não é uma frequência muito utilizada por outros equipamentos, sofrendo menos problemas em relação a interferência; em contrapartida, quanto maior a frequência, menor será o alcance. Este padrão se torna incompatível com o padrão 802.11b por não operarem na mesma frequência.

1.4 Redes 802.11g

O padrão 802.11g foi ratificado em junho de 2003 e, assim como o 802.11b, também possui problemas em relação a interferência, pela fato de também operar na frequência de 2,4GHz.

Ao contrário do padrão IEEE 802.11a, que possui incompatibilidade com o 802.11b, o IEEE 802.11g pode operar junto com o padrão IEEE 802.11b. Pelo fato de também utilizar a frequência 2,4GHz, a velocidade de transmissão do 802.11g é de 54Mbps e também utiliza modulação OFDM; porém, quando o padrão IEEE 802.11g opera junto com o 802.11b, a sua velocidade diminui para 11Mbps, já que a velocidade em que o IEEE 802.11b opera é de 11 Mbps (RUFINO, 2005).

1.5 Redes 802.11n

Opera nas faixas de 2,4Ghz e 5Ghz. Promete ser o padrão wireless para distribuição de mídia, pois oferecerá, através do MIMO (Multiple Input, Multiple Output - que significa entradas e saídas múltiplas), taxas mais altas de transmissão (até 300 Mbps), maior eficiência na propagação do sinal (com uma área de cobertura de até 400 metros outdoor) e ampla compatibilidade reversa com demais protocolos.

2. PROTOCOLOS DE SEGURANÇA

2.1 Protocolo WEP

O protocolo WEP é destinando a servir três funções: evitar o acesso não autorizado à rede; proteger os dados de interceptadores; realizar uma verificação de integridade de cada pacote (ROSS, 2003).

2.1.1 Características Protocolo WEP

O WEP atua na camada dois (enlace) do modelo Interconexão de Sistemas Abertos/Open Systems Interconnection (ISO/OSI), criado com o objetivo de possibilitar o uso de criptografia para transmissão dos dados, autenticação na rede sem-fio e controle de integridade dos dados (MARTINS, 2003).

Este protocolo está presente em todos os aparelhos que utilizam o padrão wi-fi, mas já teve muitas falhas divulgadas em sites, tornando a sua quebra facilitada com o auxilio de softwares não sendo um protocolo muito confiável.

Para Rufino (2005):

> "Existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Portanto, caso seja necessária a troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável. Outro problema vincula-se ao fato de que, na época em que o padrão foi definido (1997), havia restrição dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. E finalmente, foram revelados outros problemas técnicos, que permitem ataques ao próprio algoritmo." (RUFINO, 2005, p.65).

Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados, nesse caso o RC4.

O RC4 foi desenvolvido por Ronald Linn Rivest, professor do MIT (*Massachusetts Institute of Technology*), em 1987. É um algoritmo de fluxo, isto é, o algoritmo criptografa os dados à medida que eles são transmitidos, o que faz com que o RC4 seja um algoritmo de alto desempenho.

Chaves de criptografia WEP podem ser de dois tipos: 64 e 128 bits. Muitas vezes elas serão referenciadas como 40 e 104 bits respectivamente. A razão para isso, é que WEP é implementado da mesma forma para ambos os tipos. Cada um usa um vetor de inicialização (IV) de 24 bits concatenado com uma chave secreta. A chave secreta pode ter um comprimento de 40 bits ou 104 bits.

O IV também é transmitido junto com cada pacote criptografado. E a norma do padrão sugere que esse IV seja variado a cada pacote enviado. O vetor é transmitido em texto puro, sem passar por qualquer tipo de criptografia. Logo, dos 64 bits apenas os 40 bits são efetivamente secretos sob o ponto de vista do tráfego. O receptor, que também conhece a chave fixa, recebe o pacote, retira o IV e aplica o processo inverso para descriptografar o pacote e revelar a mensagem.

Esse processo que ocorre dentro do protocolo WEP é chamado de Autenticação Shared Key (chave compartilhada). Nesta autenticação a chave de cifragem é a mesma de decifragem que ocorre da seguinte maneira como podemos ver na descrição e figura abaixo:

1. O cliente (requisitante) e o AP (autenticador) devem compartilhar uma senha secreta, previamente configurada;
2. O Ponto de acesso responde a esta requisição com um texto desafio contendo uma chave de informações;
3. O cliente deve então provar que conhece o segredo compartilhado, utilizando-o para criptografar a chave enviada pelo Ponto de acesso e devolvendo estes dados ao Ponto de acesso;
4. O Ponto de acesso conhece o segredo, então compara o texto originalmente enviado com a resposta da estação;
5. Se a criptografia da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

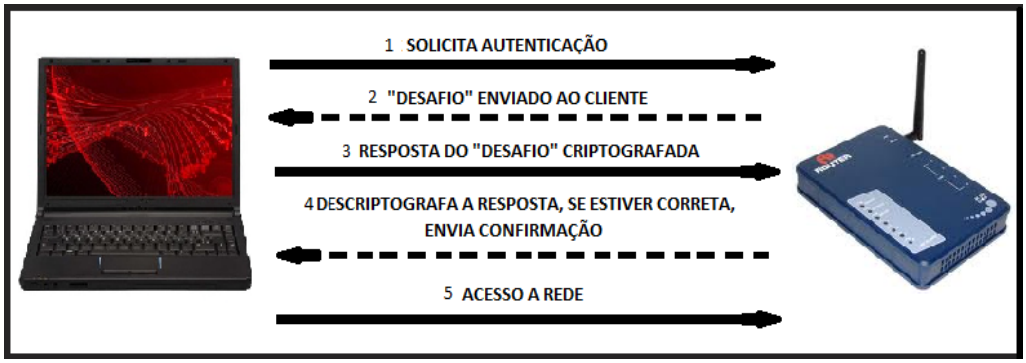

Figura 3 – Autenticação entre cliente e AP.

2.1.2 Vulnerabilidades do protocolo WEP

Vulnerabilidades são as falhas ou falta de segurança. Através destas vulnerabilidades, pessoas mal intencionadas podem invadir, subtrair, acessar ilegalmente, adulterar ou até mesmo destruir informações confidenciais. Mesmo com os avanços da tecnologia, os riscos inerentes a esta tecnologia se apresentam de forma significativa e devem ser devidamente analisados e minimizados na implantação da rede. Aspectos antes irrelevantes, como o posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados sob o risco de comprometer o bom funcionamento da rede (RUFINO, 2005).

Desta maneira, de acordo com Rufino, um concentrador colocado em uma parede enviará sinal tanto para dentro, quanto para fora do ambiente. Quanto mais ao centro estiver o concentrador, melhor será o aproveitamento do sinal pelas estações. Caso o concentrador tiver o sinal sendo extravasado para fora do ambiente, o atacante terá esse acesso, sendo suficiente para seus propósitos.

Caso as redes não estejam com sua segurança habilitada, ou corretamente configurada o tráfego pode ser analisado assim como seu conteúdo pode ser copiado ou alterado. Dessa forma, podemos ver a clara importância do protocolo de rede wireless WEP. Ainda que sejam úteis para a segurança da rede, eles apresentam vulnerabilidades.

Um teste de propagação do sinal é muito viável para a segurança, mas não deve ser o único fator de prevenção a ataques, visto que o atacante pode utilizar um equipamento mais moderno ou com características distintas existentes nos utilizados nos testes, conseguindo então sinal onde os testes não obtiveram.

O protocolo WEP utiliza uma chave única e estática conhecida por ambos os lados da comunicação. Caso tenha necessidade de trocar a chave, o processo pode ser inviável, dependendo do tamanho da rede.

Tendo conhecimento destas informações, criptografias e funcionamento do protocolo de segurança WEP, podemos analisar e entender melhor as formas com que serão feitas as tentativas de quebra desse protocolo no capitulo posterior, se utilizando de algumas ferramentas para este propósito.

2.2 Protocolo WPA

Após o descrédito do protocolo WEP, foi desenvolvido o protocolo WPA. Este teve diversas mudanças e avanços incorporados além de possuir vários 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 WPA seja mais seguro que seu antecessor WEP, já é conhecido algumas vulnerabilidades deste protocolo que podem ser encontradas em diversos artigos e sites na internet. Tendo conhecimentos de tais vulnerabilidades, os usuários deste protocolo podem dessa forma se proteger de uma maneira mais eficiente contra tentativas de invasões minimizando danos. O WPA resolve o problema dos cabeçalhos fracos do WEP, que são chamados de vetores de inicialização (IV), e garante a integridade das mensagens transmitidas pelo MIC (Message Integrity Code) usando TKIP (Temporal Key Integrity Protocol) para melhorar a criptografia de dados.

O WPA também pode ser utilizado numa rede híbrida que tenha WEP instalado e recebeu a obrigatoriedade de 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 é o chamado PSK (Pre-Shared Key), que possibilita ao usuário digitar manualmente suas chaves e senhas.

2.3 Protocolo WPA II

Após o protocolo de segurança WPA, foi desenvolvido o WPA II, sendo a grande diferença entre os dois, o método de criptografia. Mais seguro que o WPA, pois necessita de maior poder de processamento para sua criptografia, utiliza um protocolo denominado Advanced Encryption Standard (AES), junto com o TKIP com chave de 256 bits, um método mais poderoso que o WAP que utilizava o TKIP com o RC4, o que é muito seguro e eficiente, mas possui a desvantagem de exigir bastante processamento.

3. FERRAMENTAS DE ANÁLISE DE REDES WIRELESS

Antes de estudar algumas técnicas de cracking, serão apresentadas algumas ferramentas que servem tanto para identificação e tentativas de ataques, quanto para a segurança e análises de redes wi-fi. A grande maioria dos ataques a redes wi-fi utilizam ferramentas "softwares hacks", e algumas destas ferramentas servirão posteriormente para testes e análises de vulnerabilidades de redes wi-fi.

São elas: Netstumbler, Kismet, Wellenreiter, Aircrack, Wireshark/Ethereal, Hostap, Ettercap, Airtraf e Backtrack, as quais serão estudadas em detalhes a seguir.

3.1 Netstumbler

A Netstumbler é uma das ferramentas mais usadas para mapeamento e identificação das redes sem fio, por permitir a integração com equipamentos GPS, gerando assim mapas precisos de pontos de acesso identificados.

Além disso, uma das grandes vantagens dessa ferramenta é que permite identificar as redes sem fio em todos os padrões comerciais e aceita uma grande variedade de interfaces de rede. (RUFINO, 2005).

Ainda existe um problema quanto à segurança dessa ferramenta. Quando se utiliza do método de sondagem ativa da rede há o envio de informações que facilitam a identificação destes softwares por meio de análise do tráfego da rede, ou seja, se alguém estiver utilizando o Netstumbler para analisar redes próximas para qualquer que seja o fim, este poderá ser detectado através do monitoramento dessas redes por seus administradores.

Como é ilustrada na figura abaixo, esta ferramenta permite identificar a rede, endereço MAC, e outras informações.

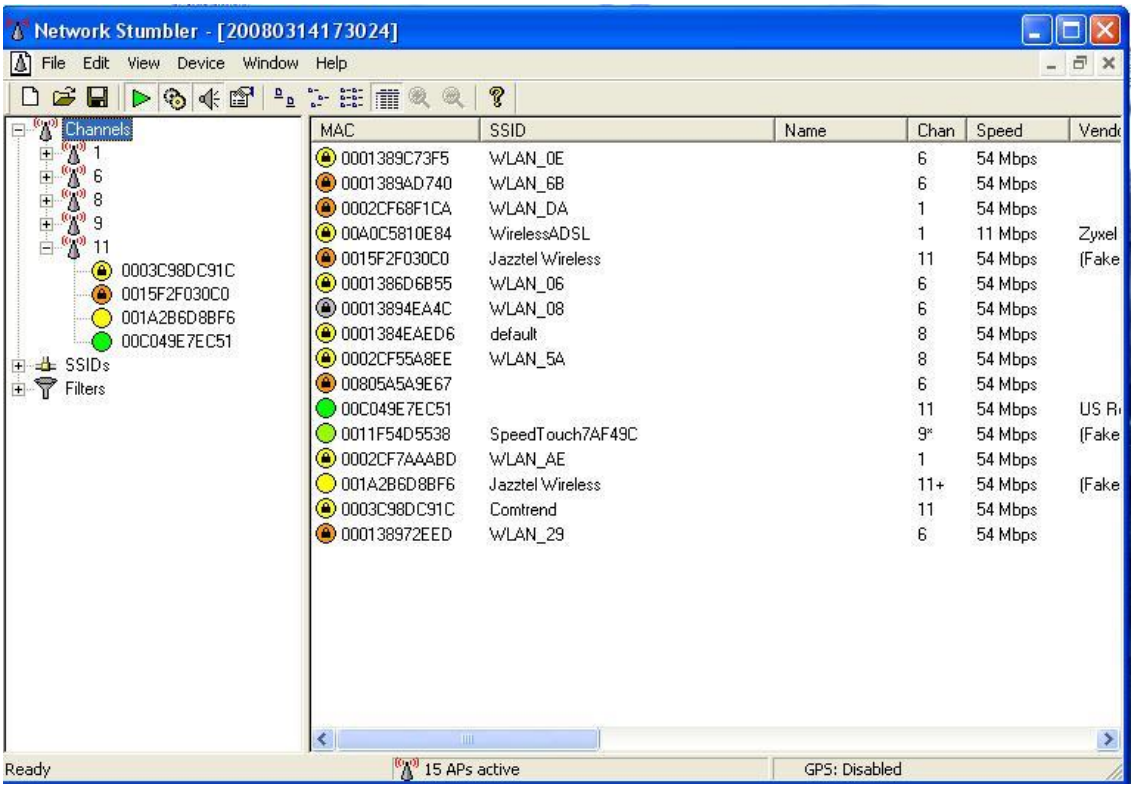

Figura 4 – Ferramenta Netstumbler

Fonte - http://www.taringa.net/posts/downloads/4309571/Network-Stumbler.html

3.2 Kismet

Esse sniffer (farejador, analisador de redes) é um detector de redes sem fio e um sistema de descoberta de intrusão.

Desenvolvido para ambiente Linux, concentra um grande número de ferramentas e aliado a um GPS, consegue fornecer informações precisas dos pontos wi-fi monitorados.

“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.” (RUFINO, 2005).

O Kismet pode ainda disponibilizar informações, quando o último pacote de determinada WLAN é recebido, e assim verificar qual a qualidade do sinal deste ultimo pacote, qual a melhor qualidade de sinal já recebida e a pior disponível. Mais um ponto favorável que podemos relacionar são os clientes das WLANs, bem como os IPs de cada um dos dispositivos. Estes endereços IPs podem ser descobertos através de requisições via ARP, via UDP e TCP, além de trabalhar com sondagem passiva dificultando sua detecção. Estas inúmeras características fazem com que o Kismet seja considerado a ferramenta de fonte aberta (opensource) para Linux mais completa e eficaz da atualidade.

Na figura abaixo, podemos ver a interface do Kismet, com as redes ao alcance listadas.

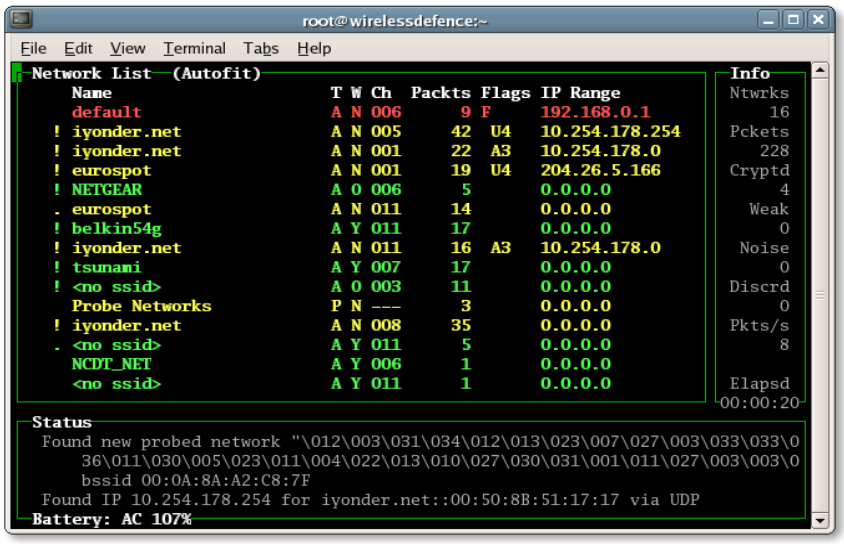

Figura 5 – Ferramenta Kismet

Fonte - http://linuxkismet.files.wordpress.com/2008/08/kismet1.png

3.3 Wellenreiter

Na primeira versão da ferramenta Wellenreiter, considerou-se que esta possuía grande capacidade para “descriptografar” todos os dados e realizar auditoria de redes sem fio. Os testes realizados mostraram que esta não difere das demais como: insere poucas funcionalidades adicionais, possibilita identificar redes sem fio, clientes, mecanismos de segurança como WEP e, caso tenha um dispositivo GPS, associa cada rede a respectiva coordenada (RUFINO, 2005).

Uma de suas funcionalidades é a capacidade de realizar um ataque por força bruto (brute force) dos SSIDs. A maioria dos SSIDs padrões é enviada por dispersão (broadcast) em pacotes de requisição de sondagem forjados com endereços MAC de origem adulterados.

Atualmente, existe uma nova versão do Wellenreiter chamada de Wellenreiter II, a qual está disponível tanto em um script em PERL e GTK como em C++, bem mais aceita, e com outra interface melhorada, supera o modelo anterior. Outra característica peculiar ao Wellenreiter II é a transparência da forma de trabalhar desta ferramenta, dificultando o escaneamento dos detectores.

Nas figuras abaixo, podemos ver a interface do wellenreiter II.

Figura 6 – Ferramenta Wellenreiter

Fonte - http://wellenreiter.sourceforge.net/screenshots.html

3.4 Aircrack-ng

Esse software é uma ferramenta para análise de tráfego em redes sem fio 802.11a, 802.11b, 802.11g e sua plataforma permite rodar tanto em Linux como em Windows. Tem como sua função descobrir ou recuperar chaves WEP e WPA-PSK a partir de dados capturados de qualquer ambiente Wi-Fi. Utiliza também o recurso de wordlist (lista de palavras), para ataques com auxilio de um dicionário de palavras. Para utilização completa deste programa é necessário a captura de alguns dados de uma rede sem fio. Esta coleta de tráfego poder ser executada por qualquer dispositivo wireless capaz de entrar um modo monitoramento.

Na figura abaixo, vemos a interface do Aircrack-ng para Windows.

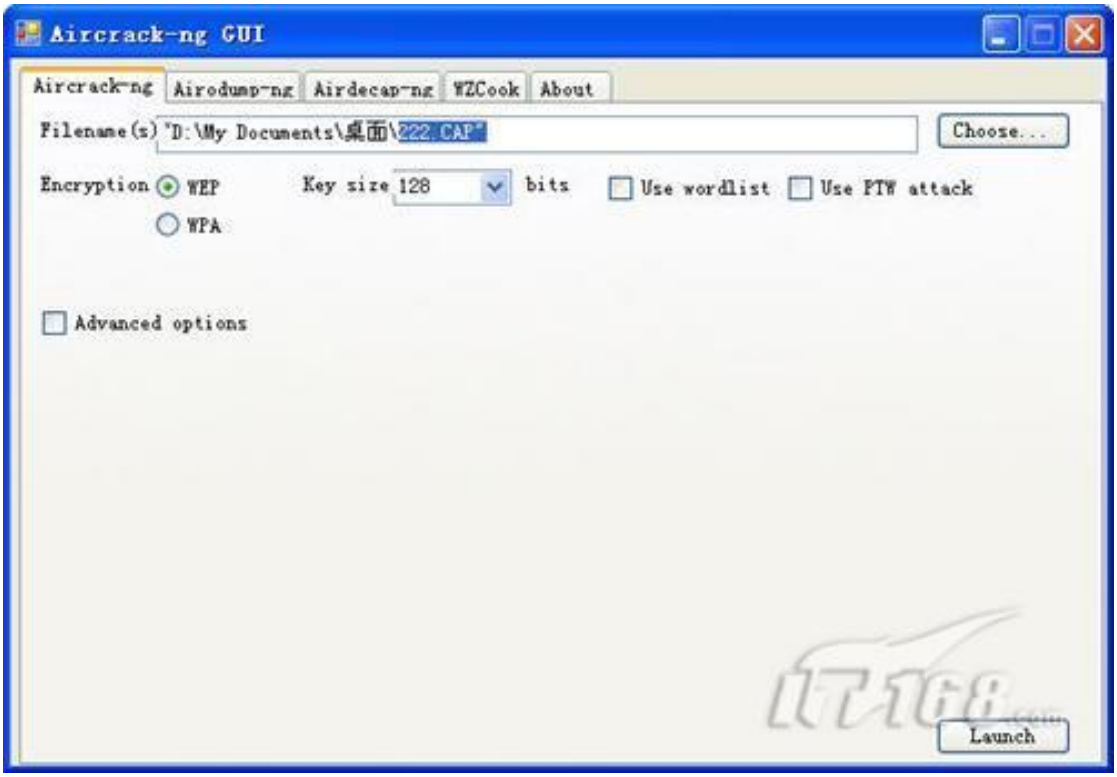

Figura 7 – Ferramenta Aircrack-ng

Fonte - http://safe.it168.com/a2009/0312/268/000000268376_3.shtml

Aircrack-ng é na verdade um conjunto de ferramentas que são listadas a seguir, com seus comandos e opções para uso:

Airmon-ng - Altera uma placa de rede sem fio para o modo de monitoramento.	
Uso : Airmon-ng <start | stop | check> <interface> [channel or frequency]	
star, stop ou check : indica se você deseja iniciar ou parar a interface. A função "check" mostra todos os processos que possam interferir com o pacote Aircrack-ng.	
Interface: Define qual interface de rede será utilizada (wlan0, eth1...).	
Airodump-ng - O sniffer de pacotes, captura e salva em um arquivos;	
Uso: airodump-ng <options> <interface> [, <interface>,...]	
--ivs	Guardar apenas IVs capturado
--gpsd	Use DSGP
--write	prefixo do arquivo de despejo, gravar em arquivo essas informações
-w	o mesmo que –write
-beacons	registra todos os beacons em arquivo de despejo
-update	atraso atualização display em segundos
-showack	mostra na tela as estatísticas
-h	oculta estações conhecidas
-f	Tempo em ms entre canais
--berlim <segundos>	Tempo antes de remover o AP cliente /a partir do ecrã quando não há mais pacotes são recebidos (Padrão: 120 segundos)
<file>-r	Lê os pacotes a partir desse ficheiro
-x <msegundos>	Active Scanning Simulation
-output-format	Formato de saída. Os valores possíveis: pcap, ivs, csv, gps, kismet, netxml . Short format "-o". A opção pode ser especificada várias vezes. Neste caso, o formato de cada arquivo especificado será a saída. Ivs somente ou pcap pode ser usado, mas não ambos.
Aireplay-ng - O injetor de pacotes, para realizar ataques ativos para gerar tráfico;	
Uso: aireplay-ng <options> <replay interface>	

Options:	
-b BSSID	endereço MAC, o Access Point
-d DMAC	endereço MAC, Destino
-s SMAC	endereço MAC, Fonte
-m len	comprimento mínimo de pacote
-n len	comprimento máximo de pacote
-u type	controle de frame, tipo de campo
-v subt	controle de frame, campo subtipo
-t tods	controle de frame, para DS bit
-f fromds	controle de quadro, de pouco DS
-w iswep	controle de frame, bit WEP
Replay options:	
bpps-x	número de pacotes por segundo
-p	a palavra de controle do quadro (hex)
-a bssid	definir o Access Point endereço MAC
-c	conjunto de destino endereço MAC
-h	escolher Fonte endereço MAC
-j	ataque arpreplay: injetar pkts FromDS
-g	alterar o tamanho do buffer (padrão: 8)
-l	IP de origem no conjunto de fragmentos
-o	número de pacotes por rajada (-1)
-q	segundos entre manter-alives (-1)
-y	keystream para autenticação de chave compartilhada
-bittest	teste de taxa de bits (Aplica-se apenas para o modo de teste)
-D	desativa a detecção AP. Algumas modalidades não vai avançar se o farol AP não é rd. Isso desativa essa funcionalidade.
-F	escolhe o pacote que combina em primeiro lugar. Para o modo de teste, ele apenas verifica a injeção de base e ignora todos os outros testes.
-R	desativa / dev / rtc uso. Alguns sistemas de experiência de travamentos ou outros problemas com RTC. Isso desativa o uso.

Aircrack-ng - É o cracker que implementa os ataques descritos. Pode funcionar em modo on-line (simultaneamente à captura) ou off-line (com um arquivo de captura salvo de outro momento).

Opção – Parâmetro - Descrição		
-a	Modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-b	Bssid	Selecione a rede alvo baseada no endereço MAC do Access Point.
-c	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres alfanumérico somente (0×20 - 0x7F).
-d	Início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-e	Essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.
-h	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0×30-0×39). Essas chaves são usadas por padrão na maioria dos Fritz!Boxes.
-i	Índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, … -k 17 para desabilitar cada ataque seletivamente.
-m	end. MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique -m ff:ff:ff:ff:ff:ff para usar cada um e todos IVs, independente da rede.
-n	Nº de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-p	Nº de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	Nenhum	Habilita modo quieto (não mostrar status até que a chave seja encontrada, ou não).

-t	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-x/-x0	Nenhum	[Quebra WEP] Desabilita força-bruta dos últimos bytes de chave.
-x1	Nenhum	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	Nenhum	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	Nenhum	[Quebra WEP] Desabilita multi-processamento da força-bruta (somente SMP).
-y	Nenhum	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	Palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou ”-” sem as aspas para padronizar em (stdin).
-z	Nenhum	Invoca o método PTW de quebrar chaves WEP.
Packetforge-ng – Cria pacotes encriptados para uso em ataques de injeção. Não requer a chave, apenas uma sequência de bytes do RC4 para um IV qualquer (visto que		
no protocolo WEP o cliente escolhe seus IVs);		
Uso: packetforge-ng <mode> <options><source>		
Options		
-p <fctrl>	palavra de controlo conjunto de quadros (hex)	
-a <bssid>	definir o Access Point endereço MAC	
-c <dmac>	conjunto de destino endereço MAC	
-h <smac>	Fonte endereço MAC	
-e:	desativa a criptografia WEP	
-k <ip[:port]>	conjunto de destino IP [Porta]	
-l <ip[:port]>	set IP de origem [Porta]	
t-TTL	Time definido para Live	
-w <file>	escrever pacote para esse arquivo pcap	
Mode		

-arp	forjar um pacote ARP (-0)
-udp	forjar um pacote UDP (-1)
-icmp	forjar um pacote ICMP (-2)
-nulo	construir um pacote nulo (-3)
-custom	construir um pacote personalizado (-9)
Source	
-r <file>	leia pacote deste arquivo raw
<file>-y	leia prga deste arquivo

Airdecap-ng – Decripta pacotes WEP e WPA salvos com uma chave conhecida. Após um ataque bem sucedido, pode ser usado para revelar o texto pleno que trafegava;

Opção – Parâmetro - Descrição		
-l	nenhum	não remover o cabeçalho 802,11
-b	bssid	ponto de acesso filtro de endereços MAC
-k	pmk	WPA/WPA2 Chave Mestra em hexadecimal
-e	wssid	identificador de destino de rede
-p	pass	alvo senha WPA/WPA2 rede
-w	key	alvo chave de rede WEP em hexadecimal

Airtun-ng – Cria uma interface virtual como um túnel para uma rede sem fio. Pode ser usado para decifrar uma rede protegida com WEP ou WPA (cuja chave seja conhecida) e direcionar o tráfego a um sistema de detector de intrusos (IDS); também pode ser usado para injetar tráfego a partir de ferramentas convencionais;

Opção – Parâmetro – Descrição		
-x	nbpps	número máximo de pacotes por segundo (opcional)
-a	bssid	definir o Access Point endereço MAC (obrigatório)
-i	iface	capturar pacotes a partir desta interface (opcional)

-w wepkey	use este WEP-chave para criptografar os pacotes (opcional / um dos y-ou-w deve ser definido)
-t tods	enviar quadros a AP (1) ou para o cliente (0) (opcional / default 0)
-h mac	endereço MAC de origem
-H	exibir ajuda
Airolib-ng - Gerencia um banco de dados de senhas e pré-computa chaves a partir delas. Usado para aumentar a eficiência de ataques de dicionário a redes WPA;	
Uso: airolib <database> <operation>	
Database é o nome do arquivo de banco de dados.	
--stats	Mostra algumas informações sobre o banco de dados.
--sql	Executa o comando SQL especificado.
--clean [all]	Realize os passos para limpar o banco de dados a partir de sucata velha. A opção "todos" também irá reduzir o tamanho do arquivo, se possível, e executar uma verificação de integridade.
--batch	Início de processamento em lote todas as combinações de ESSIDs e senhas. Este deve ser executado antes de usar o banco de dados dentro Aircrack-ng ou depois de ter adicionado SSIDs adicionais ou senhas.
- verify-[all]	Verificar um conjunto de PMKs escolhidos aleatoriamente. Se a opção 'all ' for dado, todos PMKs no banco de dados são verificados e as incorretas, estão excluídos.
- exportação cowpatty {essid} {file}	Exportar para um arquivo cowpatty.
- Importação-{file} cowpatty	Importar um arquivo cowpatty e criar o banco de dados se ele não existir.
- Importação-{essid | passwd} {file} -	Importar um arquivo de texto simples como uma lista de qualquer ESSIDs ou senhas e criar o banco de dados se ele não existir. Este arquivo deve conter um essid ou senha por linha.

Airdecloak-ng – Usado para remover pacotes espúrios que podem ser injetados por equipamentos que tentam prevenir que a chave seja quebrada;	
uso: airdecloak-ng [options]	
-i Caminho arquivo	entrada para o arquivo de captura.
-bssid	BSSID da rede para filtrar.
-ssid	ESSID da rede de filtro (ainda não implementado).
-filter	aplique filtros nesta ordem específica. Eles têm que ser separados por uma ','. Exemplo: sinal de filtros, consecutive_sn
-null-packets	suponha que os pacotes nulos podem ser encobertos (ainda não implementado).
-disable-base_filter	desativar a base do filtro.
-Drop-frag	Ignorar todos os pacotes fragmentados. Na maioria das redes, a fragmentação não é necessária
Airdriver-ng - Usado para gerenciar os drivers das placas de rede sem fio do sistema;	
Uso: airdriver-ng <command>	
-suported	lista todos os drivers suportados
-kernel	lista todos os drivers do kernel
-installed	lista todos os drivers instalados
-load	lista todos os drivers carregados
-unload	carrega um driver
-load	descarrega um driver
-update	recarrega um driver
-Install	instala um driver
-remover	remove um driver
-remove_stack	remove uma pilha
-install_stack	instala uma pilha
-details	imprime detalhes do driver

-detect detecta placas wireless
Airserv-ng - Servidor TCP para que clientes possam acessar uma placa de rede sem fio remotamente;
Uso: airserv-ng <options>
-p <port> porta TCP para escuta, padrão 666
-d <dev> dispositivo wifi para servidor
-c <chan> canal para iniciar.
-v <level> nivel de depuração
Easside-ng – Usada para comunicar com uma rede sem fio com WEP sem saber a chave. Utiliza um servidor auxiliar disponível na Internet para "pedir" para o access point decriptar pacotes por ele;
Usage: easside-ng <args>
-h Exibe a lista de opções. -v endereço MAC do Access Point (Opcional) -m fonte endereço MAC para ser utilizado (Opcional) -i endereço IP de origem para ser utilizado na rede wireless. Padrões para o nettwork decodificado plus "0,123"(Opcional) -r endereço IP do roteador AP. Este poderia ser o IP WAN do AP ou um roteador IP real, dependendo da topologia. Padrões "0,1". (Opcional) -s endereço IP do "amigo" do servidor (obrigatório) -f nome da interface sem fio. (Obrigatório) -c bloqueia o cartão para o canal especificado (Opcional)
Wesside-ng – Utiliza uma combinação de ataques para automaticamente obter uma chave WEP em poucos minutos. Os ataques podem ser feitos manualmente mas a ferramenta os automatiza;
Uso: wesside-ng <opts> -i <wireless interface name>

-h	Exibe a lista de opções.
-i	nome da interface sem fio. (Obrigatório)
-n	rede IP, como em "quem tem IP de destino (NetIP) diga IP de origem (myip) ". O padrão é o IP de origem no pedido ARP que é captada e decifrada. (Opcional)
-a	fonte de endereço MAC (Opcional)
-c	sem precisar iniciar o Aircrack-ng, capturara os pacotes até que o controll+c é acionado para parar o programa! (Opcional)
-f	Permite que o maior canal de digitalização a ser definido. Padrões para o canal 11. (Opcional)
-t	Para cada número de IVs especificado, reinicie o airecrack-ng motor PTW. (Opcional)
-v	Ponto de Acesso Wireless endereço MAC (Opcional)
Tkiptun-ng – Uma prova de conceito de ataque ao WPA/TKIP, esta ferramenta é capaz de injetar alguns quadros em uma rede WPA TKIP com QoS.	
Usage: tkiptun-ng <options> <replay interface>	
Options	
-d	endereço MAC, Destino
-s	endereço MAC, Fonte
-m-len	comprimento mínimo de pacote
-n len	comprimento máximo de pacote
-t tods	controle de frame
-f fromds	controle de quadro
-D	desativar detecção de AP
Replay Interface	
-x	número de pacotes por segundo
-a	definir o Access Point endereço MAC
-c	conjunto de destino endereço MAC
-h	fonte endereço MAC

-F	escolher o pacote que combina primeiro
-e	conjunto de alvos AP SSID
Debug options	
-k	keystream para a continuação
-y	arquivo keystream para a continuação
-j	injetar pacotes
-p	psk para calcular pmk com essid
Source Options	
-i	capturar pacotes a partir desta interface
-r	extrair os pacotes a partir deste arquivo pcap
- help	Mostra esta tela de uso

3.5 Wireshark / Ethereal

Antigo Ethereal e hoje conhecido como wireshark, possui como característica principal a remontagem de sessões, trabalhando em diversas plataformas, como em Windows, em Linux, em Solares dentre outras.

Nesta ferramenta, é possível controlar o tráfego de uma rede e saber tudo o que entra e sai do computador, em diferentes protocolos. Se você estiver numa rede local, com micros ligados através de um hub ou switch, outro usuário pode usar o wireshark para capturar todas as suas transmissões.

A Ethereal “é uma ferramenta com alta capacidade de evolução que faz parte da lista de ferramentas indispensáveis para um administrador de rede sem fio ou não” (RUFINO, 2005).

Abaixo podemos ver a interface do wireshark monitorando transmissões:

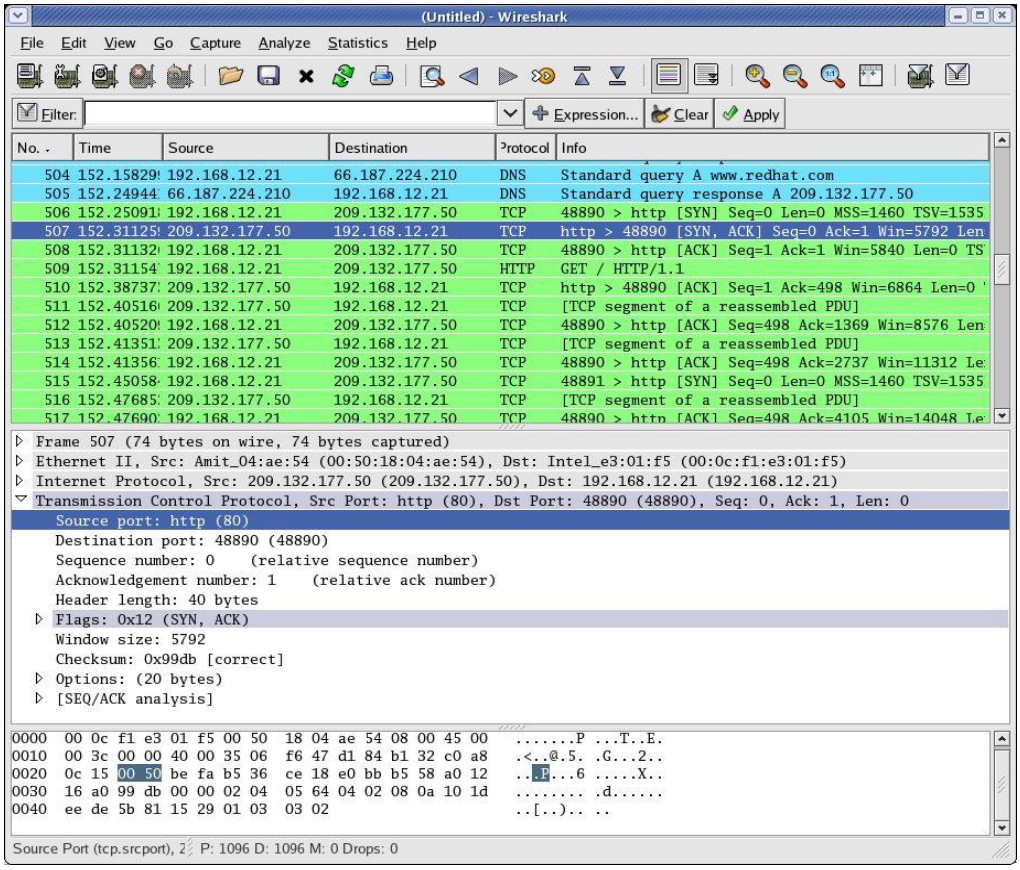

Figura 8 – Ferramenta Ethereal

Fonte - http://www.ethereal.com/docs/eug_html_chunked/ChUseMainWindowSection.html

3.6 Hostap

Hostap é, na realidade, um módulo de kernel capaz de transformar um dispositivo de rede sem fio padrão em um Access point. O Hostap, além de ser utilizado em computadores, também pode ser instalado em Access point via modificação do firmware.

Esta ferramenta é muito utilizada em ataques de associação maliciosa, pois possibilitam uma reconexão com concentradores falsos após uma conexão com pontos de acesso (concentradores) reais.

Pode ser utilizado com todos protocolos de rede sem fio conhecidos.

Na figura podemos ver a interface e configurações disponíveis do hostap:

Figura 9 – Ferramenta Hostap

Fonte - http://www.gentoo-portage.com/up_img/img_800px/1862.jpg

3.7 Ettercap

Ettercap é uma suíte de funções para redes. Possui sniffing de conexões ao vivo, filtragem de conteúdo, suporta dissecação ativa e passiva de muitos protocolos (mesmo aqueles cifrados) e inclui a análise de muitos recursos para a rede e host.

Cada conexão tem um atributo que informa se há atividade nessa conexão. Explora 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. Permite a colocação de caracteres em uma conexão estabelecida e também filtrar os pacotes trafegados na rede, alterando ou descartando. Realiza scanning passivo da LAN e permite a verificação de existência de outros poisoners (envenenadores) na rede, servindo como um ótimo monitor.

O asterisco indica que uma senha foi coletada nessa conexão (conforme imagem abaixo).

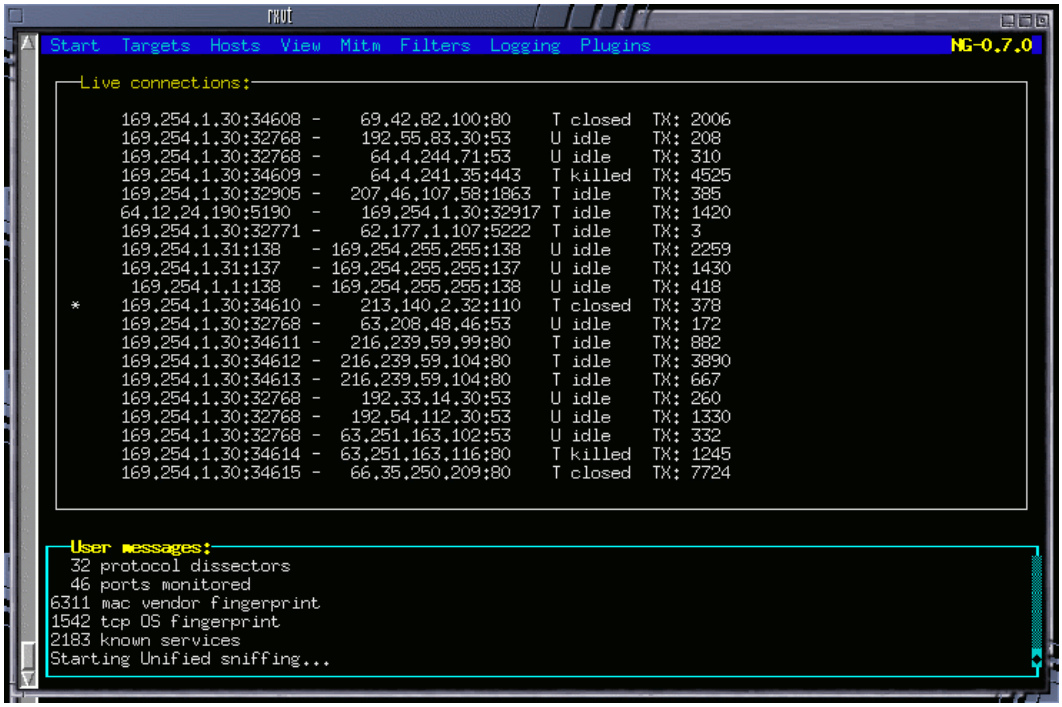

Figura 10 – Ferramenta Ettercap

Fonte - http://ettercap.sourceforge.net/screenshots.php

3.8 Airtraf

Esta ferramenta foi desenvolvida para farejar (sniffar) redes sem fio com o objetivo de descobrir e capturar dados que trafegam na rede, coletando inúmeras informações como clientes conectados, tipo de serviços dentre outros.

A outra característica de Airtraf inclui controle de acesso gerado na área, que controla todos os pedidos de associação a um ponto de acesso a dados, e observando a reação, fazer um juízo quanto à natureza da atividade podendo determinar se a atividade é hostil ou amigável.

Foi desenvolvida com exclusividade para a plataforma Linux, porém possui código aberto, o que lhe permite ser utilizada por outras plataformas.

Abaixo a ferramenta Airtraf mostrando as características de uma rede capturada:

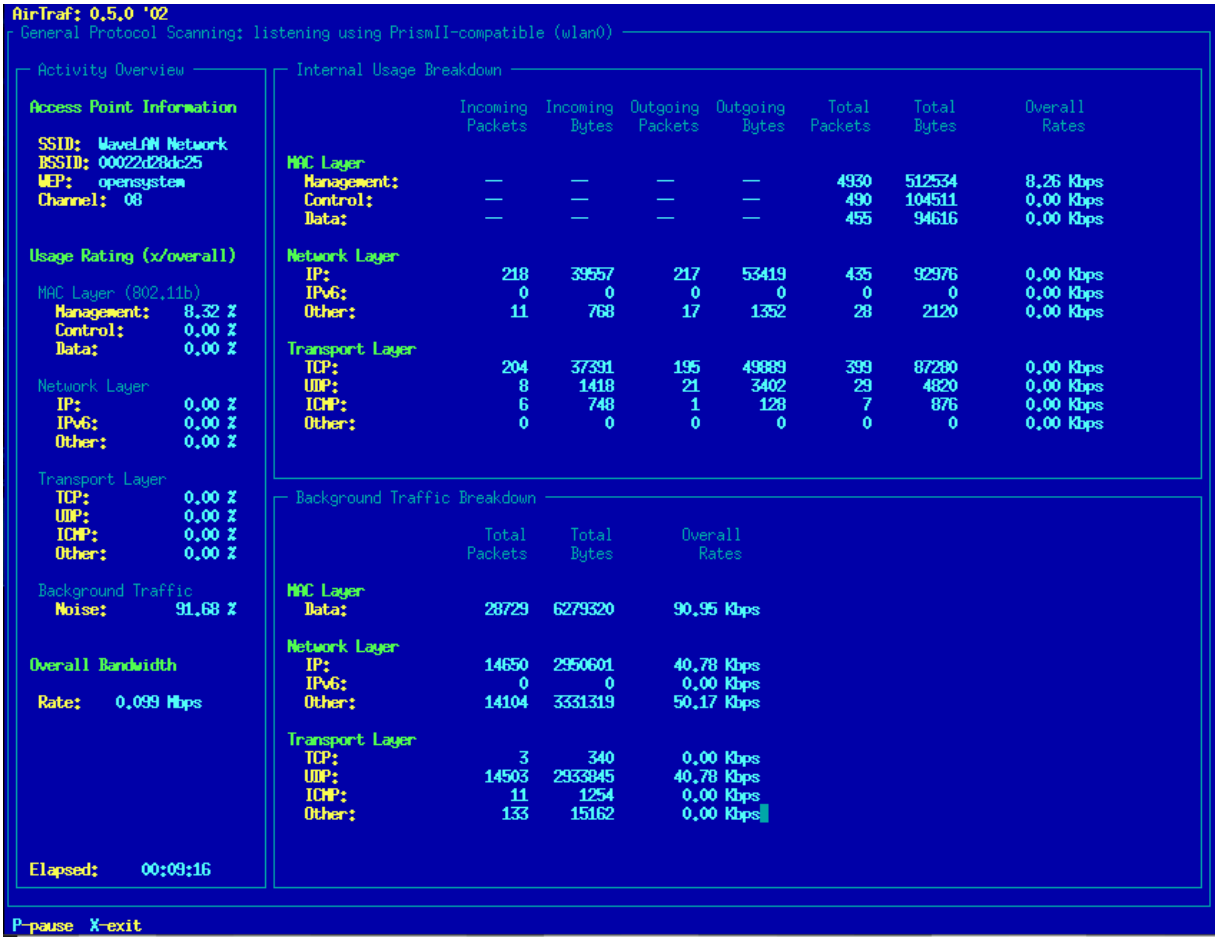

Figura 11 – Ferramenta Airtraf

Fonte - http://airtraf.sourceforge.net/images/general_protocol_analysis.gif

3.9 BackTrack

Uma distribuição GNU/Linux distribuída como Live CD (ou Live USB), ou seja, pode ser utilizada a partir de uma inicialização por CD ou USB, não sendo necessária a instalação do sistema e suas ferramentas no computador.

É muito usada para testes de penetração, reunindo mais de 300 ferramentas para análise e testes de vulnerabilidades prontas para serem usadas e que abrangem uma variedade de diferentes tipos de alvos e técnicas de ataque.

Essas ferramentas são estruturadas de acordo com o fluxo de trabalho de profissionais de segurança. Essa estrutura permite encontrar facilmente as ferramentas relacionadas a uma tarefa específica para ser cumprida. Novas tecnologias e técnicas de teste são combinadas no BackTrack o mais rápido possível para mantê-lo sempre atualizado.

Na figura abaixo, podemos observar algumas das funções e ferramentas disponíveis no BackTrack versão 4, a qual foi utilizada nos experimentos deste trabalho e esta disponível para download em http://www.backtrack-linux.org .

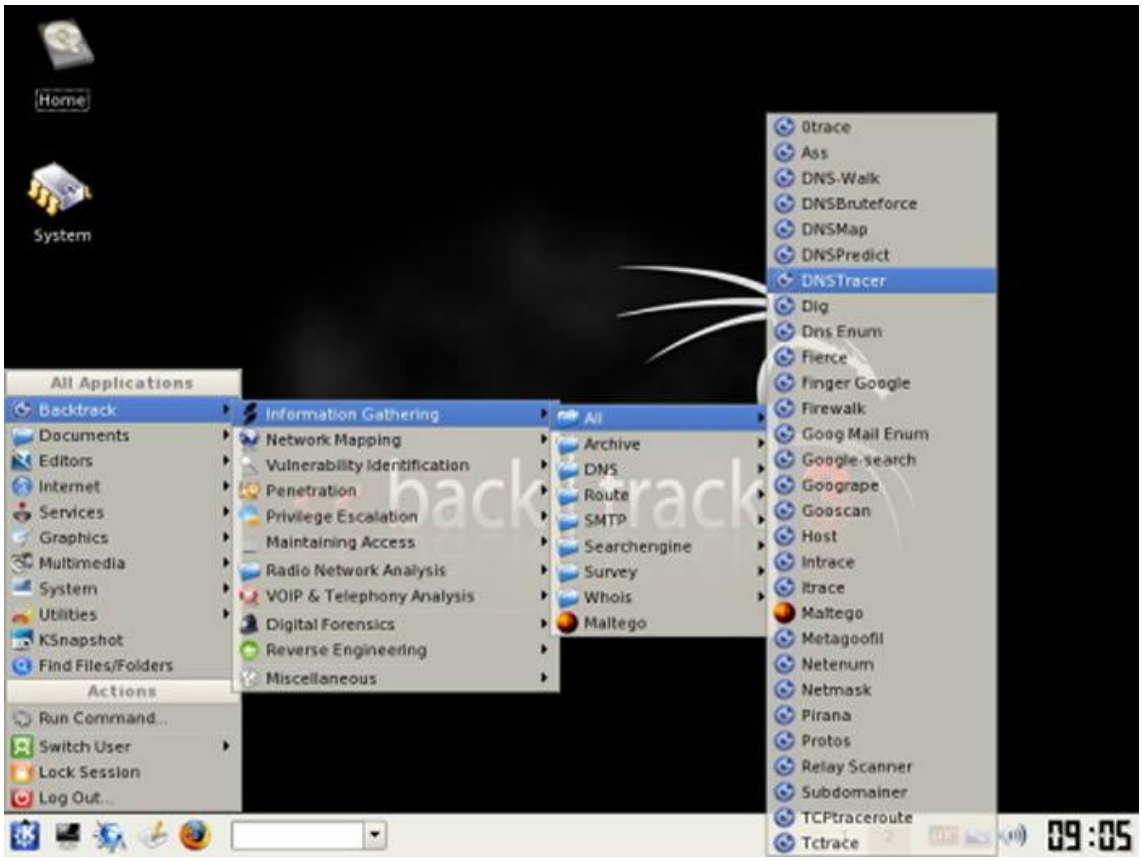

Figura 12 – Ferramenta Backtrack

http://pplware.sapo.pt/wp-content/images2008/imagem_backtrack05.jpg

4. APLICAÇÃO E RESULTADOS

Neste capítulo serão vistos os equipamentos escolhidos para os testes de segurança, detalhes do ambiente utilizado, as ferramentas testadas, descrição do experimento, resultados e análise dos resultados obtidos com o experimento.

4.1 Equipamentos Utilizados

Serão utilizados neste experimento em laboratório dois equipamentos, os quais foram escolhidos por serem comuns no mercado e principalmente por serem bastante utilizados pelos usuários domésticos e pequenas empresas.

São eles: D-Link Dir-600 e Linksys WRT54G

Figura 13 – Roteador wireless D-Link Dir-600

Figura 14 – Roteador wireless Linksys WRT54G

Os dois aparelhos possuem características parecidas, a grande diferença esta na transferência de dados que no Dir-600 atinge até 150mbps e o Linksys mantém o padrão 54mbps. Ambos suportam criptografia WEP, WPA e WPA2.

4.2 Ambiente do Experimento

Será utilizado um notebook conectado ao roteador wireless, simulando uma rede comum de uma empresa ou mesmo doméstica. O notebook estará enviando um arquivo de 4.3Gb para o computador desktop, gerando assim um tráfego constante na rede, evitando que resultados sejam alterados por questão de ter menos ou mais trafego no momento da captura dos pacotes. Enquanto isso outro notebook, não pertencente a esta rede, estará analisando os dados dessa transação tentando fazer a quebra da proteção utilizando as ferramentas anteriormente listadas.

O ambiente possui uma área de aproximadamente 25m² e não possui obstáculos do AP aos hosts.

Na figura abaixo temos a topologia do experimento:

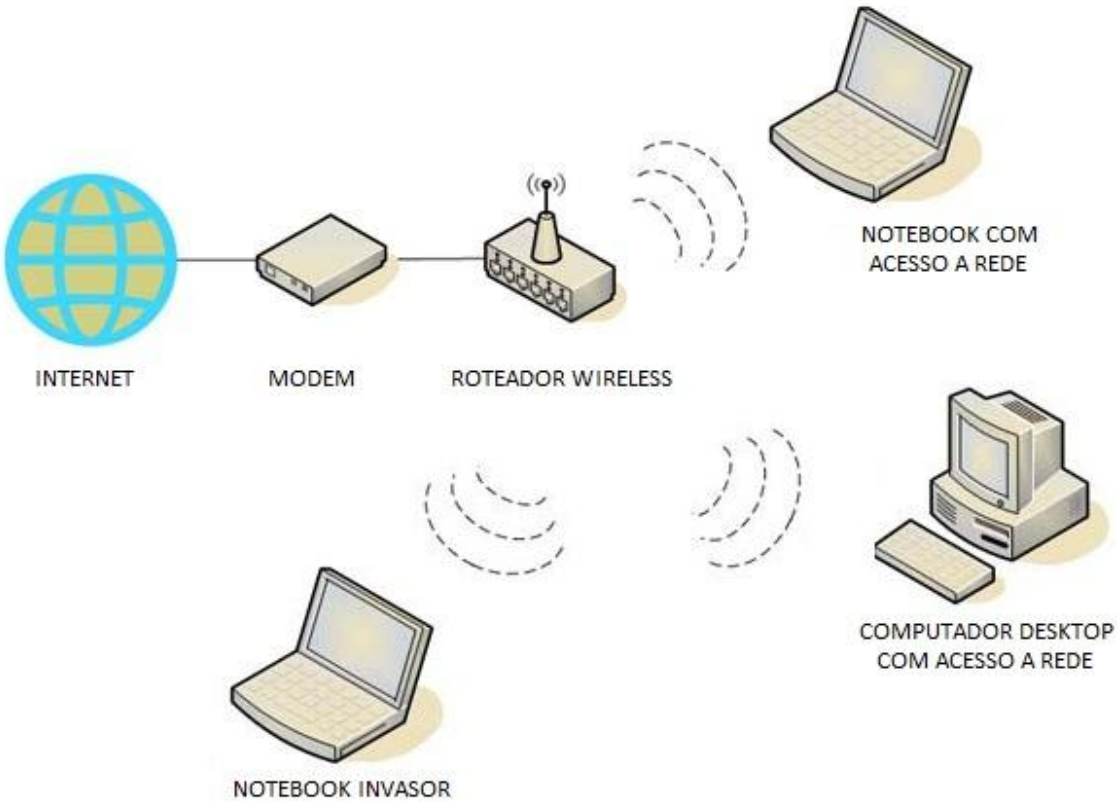

Figura 15 – Topologia do experimento

4.3 Ferramentas Utilizadas no Experimento

Foram utilizadas as seguintes ferramentas, airmon-ng, airodump-ng, aireplay-ng, packetforge-ng e aircrack-ng. Todas estas estão incluídas no pacote de ferramentas Aircrack-ng.

4.4 Descrição do Experimento

Utilizou-se duas chaves de rede geradas uma em cada aparelho. Utilizando a maior criptografia oferecida, de 128bits, com 26 caracteres alfanuméricos. Permitindo assim obter resultados mais verossímeis já que esta sendo utilizada a criptografia máxima oferecida.

Cada item do teste foi executado três vezes, de 30 em 30 mil pacotes até 150 mil, para mostrar um detalhamento melhor da captura. Gerando assim três tabelas mostrando o número necessário de pacotes para conseguir obter as chaves, os vetores capturados desses pacotes e o tempo gasto nessas operações, podendo assim mostrar uma média dos resultados obtidos para cada fornecedor.

Ao final dos experimentos espera-se que os dados revelem não só a insegurança do protocolo WEP, que já é conhecida, mas também dados que demonstrem o quanto vulnerável esta uma rede que utiliza esse protocolo como proteção, mostrando dados como a quantidade média de pacotes capturados necessários para burlar a segurança bem como o tempo médio para que a chave de segurança fosse encontrada e a segurança da rede comprometida pelo invasor.

O experimento esta dividido em seis passos que são descritos a seguir:

Primeiro passo – preparar o ambiente (roteador ativo e criptografia WEP (habilitada e conectado ao computador e notebook). Notebook invasor, utilizando uma distribuição Linux Bactrack 4.0 com o pacote de ferramentas aircrack-ng instalado;

Segundo passo – abrir um console de comando e iniciar a placa de rede wireless utilizando o comando “airmon-ng start wlan0”.

Caso tenha mais de uma placa wi-fi (wlan1, wlan2 e assim por diante). Após iniciar a interface wi-fi, já estará habilitado o modo monitoramento em mon0, mon1, mon2, conforme a interface habilitada;

Terceiro passo – utilizar a ferramenta airodump-ng para iniciar o monitoramento da rede wireless detectada através do comando "airodump-ng mon0". Após esse comando, será listada as redes wi-fi ao alcance, assim como o endereço MAC dos roteadores BSSID (Basic Service Set Identifier), o canal de atuação dessa rede e o tipo de criptografia e o ESSID (Extended Service Set Identifier);

Quarto passo – após identificada as redes, escolher o alvo. Fazer isso através do seguinte comando, ainda utilizando a ferramenta airodump-ng, marcando o BSSID e Canal da rede selecionada:

"airodump-ng - -bssid 00:06:25:C4:73:CD - -channel 6 - - ivs -w linksys mon0"

Onde: -- bssid : Indica o endereço MAC do AP;
-- channel : indicar o canal de frequência;
-- ivs : salva os vetores capturados;
- w : grava os vetores capturado em um arquivo.

Fazendo isso, será iniciado o monitoramento da rede alvo com a estação que quer fazer a penetração e gerar um arquivo onde ficarão os vetores encontrados, nesse caso linksys-01.ivs (o nome do arquivo .ivs é gerado de acordo com o nome da rede alvo). Este console deverá permanecer aberto e ativo, por isso será necessário abrir outro console para continuar o processo.

Quinto passo – Já na nova janela de console, utilizar agora a ferramenta aireplay-ng com o seguinte comando:

"aireplay-ng -5 -b 00:06:25:C4:73:CD mon0"

Onde : -5 : para gerar chaves de fluxo validas;
-b : indicar o endereço MAC do AP.

Este comando irá capturar um pacote de dados da rede alvo e irá enviar um pacote de dados fragmentado e aguardara a autenticação deste.

Em seguida em um novo console digitar, com a opção (-1) para uma falsa autenticação no AP:

"aireplay-ng -1 1 –a 00:06:25:C4:73:CD mon0".

Onde: -1 : para fazer falsas autenticações no AP;
1 : tempo de atraso entre as autenticações;
-a : para marcar o endereço MAC do AP.

Após a falsa autenticação, tem-se que construir com esses dados um pacote com as chaves capturadas que serão salvas em um arquivo com extensão .xor.

Sexto passo - Utilizar agora a ferramenta packetforge-ng com o comando: "packetforge-ng –0 –a 00:06:25:C4:73:CD –h 00:11:50:35:79:11 –k 255.255.255.255 – l (lesse éle) 255.255.255.255 –y (arquivo.xor) –w arpy" .

Onde: -0 : forjar um pacote ARP (Address Resolution Protocol);
-a : marcar o endereço MAC do AP;
-h : setar a origem do MAC;
-k : setar o ip de destino;
-l (lesse éle) : setar o ip de origem;
-y : com está opção para ler o arquivo.xor criado anteriormente com as informações das chaves capturadas;
-w : para escrever as informações obtidas e gerar com elas o arquivo arpy.

Após gerado o aquivo arpy com os dados, iniciar requisições automáticas para o roteador através da ferramenta aireplay, usando o comando a seguir:

“aireplay-ng -3 –r arpy –b (Bssid) mon0”

Onde: -3 : para repetir requisições padrão;
-r : para extrair pacotes do arquivo arpy;
-b : indicar o endereço MAC do AP.

A partir daqui será recebido os pacotes com as requisições. Em média, 40.000 vetores capturados dos pacotes da rede, é o suficiente para podermos começar a tentativa de descoberta da chave de rede WEP, utilizando a ferramenta aircrak-ng com o seguinte comando:

“aircrack-ng linksys-01.ivs”

Será aberto assim o arquivo com os vetores gravados e começarão as tentativas de descoberta da chave WEP.

4.5 Resultados

Serão observados abaixo, os resultados obtidos com a análise dos equipamentos listados, divididos em: Teste 01, teste 02 e teste 03, mostrando o número necessário de pacotes para conseguir obter as chaves, os vetores capturados desses pacotes e o tempo gasto nessas operações e no final uma tabela mostrando a média obtida desses resultados.

4.5.1 Tabela de Resultados 01

Equipamento Testado	Pacotes Capturados	Tempo Captura Pacotes	Tempo de Teste das Chaves	Chaves Testadas	Vetores Capturados	Chave Encontrada?
Linksys WRT54G	30.000	22 seg	34 seg	137.874	16.871	NÃO
Linksys WRT54G	60.000	44 seg	42 seg	94.375	22.685	NÃO
Linksys WRT54G	90.000	1 min e 6 seg	17 seg	741	36.128	SIM
Linksys WRT54G	120.000	1 min e 28 seg	1 seg	29	48.582	SIM
Linksys WRT54G	150.000	1 min e 50 seg	1 seg	18	58.317	SIM
D-Link Dir-600	30.000	22 seg	36 seg	150.007	17.174	NÃO
D-Link Dir-600	60.000	44 seg	44 seg	107.542	25.329	NÃO
D-Link Dir-600	90.000	1 min e 6 seg	21 seg	812	39.877	SIM
D-Link Dir-600	120.000	1 min e 28 seg	2 seg	32	53.114	SIM
D-Link Dir-600	150.000	1 min e 50 seg	1 seg	14	63.367	SIM

4.5.2 Tabela de Resultados 02

Equipamento Testado	Pacotes Capturados	Tempo Captura Pacotes	Tempo de Teste das Chaves	Chaves Testadas	Vetores Capturados	Chave Encontrada?
Linksys WRT54G	30.000	22 seg	34 seg	135.762	18.721	NÃO
Linksys WRT54G	60.000	44 seg	43 seg	95.432	21.102	NÃO
Linksys WRT54G	90.000	1 min e 6 seg	16 seg	762	35.217	SIM
Linksys WRT54G	120.000	1 min e 28 seg	0 seg	22	51.462	SIM
Linksys WRT54G	150.000	1 min e 50 seg	1 seg	19	57.659	SIM
D-Link Dir-600	30.000	22 seg	29 seg	162.394	15.422	NÃO
D-Link Dir-600	60.000	44 seg	44 seg	109.101	23.789	NÃO
D-Link Dir-600	90.000	1 min e 6 seg	21 seg	873	37.532	SIM
D-Link Dir-600	120.000	1 min e 28 seg	1 seg	33	52.974	SIM
D-Link Dir-600	150.000	1 min e 50 seg	0 seg	11	65.711	SIM

4.5.3 Tabela de Resultados 03

Equipamento Testado	Pacotes Capturados	Tempo Captura Pacotes	Tempo de Teste das Chaves	Chaves Testadas	Vetores Capturados	Chave Encontrada?
Linksys WRT54G	30.000	22 seg	37 seg	142.722	16.566	NÃO
Linksys WRT54G	60.000	44 seg	42 seg	93.753	22.974	NÃO
Linksys WRT54G	90.000	1 min e 6 seg	17 seg	722	35.679	SIM
Linksys WRT54G	120.000	1 min e 28 seg	1 seg	27	47.244	SIM
Linksys WRT54G	150.000	1 min e 50 seg	1 seg	18	57.932	SIM
D-Link Dir-600	30.000	22 seg	31 seg	157.532	16.463	NÃO
D-Link Dir-600	60.000	44 seg	43 seg	98.775	24.772	NÃO
D-Link Dir-600	90.000	1 min e 6 seg	21 seg	808	44.672	SIM
D-Link Dir-600	120.000	1 min e 28 seg	1 seg	29	57.656	SIM
D-Link Dir-600	150.000	1 min e 50 seg	1 seg	13	66.472	SIM

4.5.4 Tabela com a Média dos Resultados Obtidos

Equipamento Testado	Pacotes Capturados	Tempo Captura Pacotes	Tempo de Teste das Chaves	Chaves Testadas	Vetores Capturados	Chave Encontrada?
Linksys WRT54G	30.000	22 seg	35 seg	138.786	17.386	NÃO
Linksys WRT54G	60.000	44 seg	42,33 seg	94.520	22.254	NÃO
Linksys WRT54G	90.000	1 min e 6 seg	16,66 seg	741,66	35.675	SIM
Linksys WRT54G	120.000	1 min e 28 seg	0,66 seg	26	49.096	SIM
Linksys WRT54G	150.000	1 min e 50 seg	1 seg	18,33	57.969	SIM
D-Link Dir-600	30.000	22 seg	32 seg	156.644	16.353	NÃO
D-Link Dir-600	60.000	44 seg	43,66 seg	105.139	24.630	NÃO
D-Link Dir-600	90.000	1 min e 6 seg	21 seg	831	40.694	SIM
D-Link Dir-600	120.000	1 min e 28 seg	1,33 seg	31,33	54.581	SIM
D-Link Dir-600	150.000	1 min e 50 seg	0,66 seg	12,66	65.183	SIM

4.6 Análise dos Resultados

Com os resultados obtidos nos experimentos documentados nas tabelas vistas anteriormente, é visto que o protocolo WEP tem sua segurança facilmente quebrada se o invasor possuir o conhecimento e ferramentas adequadas.

4.6.1 Tempo de Captura de Pacotes

O tempo de captura de pacotes, não variou nas marcas testadas e foram idênticos em todos os testes. Esse tempo mediu a leitura que o notebook invasor fazia da rede wireless, enquanto nesta trafegava dados. Como a rede wireless e o adaptador de rede wi-fi no note trabalharam todos na velocidade padrão de 54mbps essa velocidade de transferência permaneceu estática.

4.6.2 Tempo de Teste das Chaves

O tempo de teste das chaves no roteador alvo não teve grande variação entre as marcas de roteadores testadas. Para encontrar a chave e conseguir a penetração na rede alvo, o Roteador Linksys WRT54G, conseguiu retirar com êxito em média 741,66 chaves de 35.675 vetores capturados de 90.000 pacotes da rede, enquanto o D-Link Dir-600 concluiu a penetração utilizando 831 chaves de 40.694 vetores capturados de 90.000 pacotes da rede. A média de tempo necessário para a quebra da segurança no roteador Linksys WRT54G foi de 1 minuto e 22,66 segundos, enquanto que para o mesmo objetivo o roteador D-Link Dir-600 suportou as tentativas de invasão durante 1 minuto e 27 segundos.

Mesmo sendo de fabricantes diferentes, viu-se que não há grande diferença em fabricantes que utilizem o protocolo WEP em seus equipamentos, sendo que qualquer um que utilize esse protocolo como forma de proteção, estará correndo um risco de ter sua rede facilmente invadida.

CONCLUSÃO

Este projeto de pesquisa teve como objetivo apresentar os mecanismos de proteção das redes sem fio focando no protocolo de segurança WEP. Também foram abordadas ferramentas e métodos para tentar quebrar a proteção oferecida por este dispositivo.

A necessidade de aprofundamento bibliográfico em diversas áreas referentes das Wi-Fi proporcionou um bom conhecimento sobre o assunto assim como o estudo das ferramentas para tentativa de quebra, que trouxe diversas novidades em matéria de conhecimento nesse assunto, pouco explorado normalmente.

A grande facilidade na captura de sinas de Wireless trouxe a tona diversos estudos e ferramentas para estas tentativas de quebra, buscando encontrar vulnerabilidades de segurança em redes wireless. Redes estas que acabam sendo mais visadas por se tratar de redes ao alcance de qualquer pessoa que esteja dentro do raio de acesso, ou que tenha informações de identificação da rede (SSID).

O protocolo estudado, o WEP, está presente em todos os aparelhos que utilizam o padrão wi-fi, mas já teve muitas falhas divulgadas em sites, o que tornou a sua quebra facilitada com o auxilio de softwares, não sendo um protocolo muito confiável.

Ao término deste trabalho, após os testes com ferramentas de análise e captura de pacotes e vetores para adquirir chaves desta rede, pode-se afirmar que mesmo sendo diferentes, os dois fornecedores testados, não mostraram maior ou menor eficiência na segurança daqueles que utilizem o protocolo WEP em seus equipamentos, sendo que qualquer um que utilize esse protocolo como forma de proteção, estará correndo um risco de ter sua rede facilmente invadida.

REFERÊNCIAS BIBLIOGRÁFICAS

ROSS, John. WI-FI. **Instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003.

RUFINO, Nelson Murilo de Oliveira. **Segurança em redes sem fio.** 2.ed. São Paulo: Novatec, 2005.

LUCCHESE, Felipe. **Análise de Vulnerabilidade de Rede Sem Fio 802.11: Estudo de Caso em um Orgão Público Municipal** 2009. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Centro Universitário Feevale, Novo Hamburgo, RS, 2009.

WARCHALKING. **Wireless Discussion Fórum**. Disponível na Internet via <http://www.warchalking.com.br>. Acesso em: 27 outubro. 2010

BACKTRACK. **Distribuição Linux**. Disponível na internet via <http://www.backtrack-linux.org>. Acesso em 05 de abril de 2011

MARTINS, Marcelo. **Protegendo Redes Wireless 802.11b**. Março de 2003. Disponível na internet via <http://www.planetarium.com.br/planetarium/noticias/2003/3/1048024279/protegendo_redes_wireless.pdf>. Acesso em: 16 outubro. 2010.

Quebrar Wep. Disponível na Internet via <http://www.vivasemfio.com/blog/category/quebrar_wep/>. Junho de 2007. Acesso em: 19 Novembro 2010.

FARIAS, Paulo César Bento. **Redes Wireless.** Dezembro de 2006. Disponível na internet via <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless032.asp>. Acesso em: 19 Novembro. 2010.

PINHEIRO, José Maurício Santos. **Guia Completo de Cabeamento de Redes.** Abril de 2005. Disponível na internet via <http://www.projetoderedes.com.br/artigos/artigo_redes_moveis_ad_hoc.php>.Acesso em: 06 Junho . 2011.

MORIMOTO, Carlos E. **Redes Wireless.** Janeiro de 2008. Disponível na internet via < http://www.hardware.com.br/tutoriais/padroes-wireless/pagina5.html>. Acesso em: 07 Junho. 2011.

Netstumbler. 2009**.** Disponível na internet via <http://www.netstumbler.com>. Acesso em: 17 Setembro. 2010.

Kismetwireless. 2010**.** Disponível na internet via <http://www.kismetwireless.net>. Acesso em: 17 Setembro. 2010.

Wellenreiter. 2010**.** Disponível na internet via <http://wellenreiter.sourceforge.net/>. Acesso em: 17 Setembro. 2010.

Aircrack. 2010**.** Disponível na internet via <http://www.aircrack-ng.org>. Acesso em: 18 Setembro. 2010.

Wireshark. 2010**.** Disponível na internet via <http://www.wireshark.org>. Acesso em: 18 Setembro. 2010.

Hostap. 2010**.** Disponível na internet via <http://hostap.epitest.fi>. Acesso em: 24 Setembro. 2010.

Airtraf. 2010**.** Disponível na internet via <http://airtraf.sourceforge.net/>. Acesso em: 26 Setembro. 2010.

Ettercap. 2010**.** Disponível na internet via <http://ettercap.sourceforge.net>. Acesso em: 26 Setembro. 2010.

Wireless Defence. 2010**.** Disponível na internet via <http://www.wirelessdefence.org>. Acesso em: 3 Outubro. 2010.