UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ANA PAULA BIZ

ANÁLISE DE VULNERABILIDADES DE REDES SEM FIO E MÉTODO DE DEFESA POR MEIO DE SENHAS SEGURAS

CRICIUMA, JULHO DE 2010

ANA PAULA BIZ

ANÁLISE DE VULNERABILIDADES DE REDES SEM FIO E MÉTODO DE DEFESA POR MEIO DE SENHAS SEGURAS

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. Msc. Paulo João Martins

CRICIUMA, JULHO DE 2010

ANA PAULA BIZ

ANÁLISE DE VULNERABILIDADES DE REDES SEM FIO E MÉTODO DE DEFESA POR MEIO DE SENHAS SEGURAS

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Prof. Esp. Sérgio Coral (UNESC)

Dedico este trabalho aos meus pais Enedir e Lúcia e ao meu marido Clédison, pela paciência e incentivo para que eu pudesse conquistar esse passo tão importante na minha vida.

AGRADECIMENTOS

Agradeço a Deus por todas as oportunidades e por me dar força.

Ao meu pai Enedir e a minha mãe Lúcia pelo incentivo e apoio durante todos os momentos, sem medir esforços, principalmente por me concederem uma boa educação.

Agradeço ao meu marido Clédison pela paciência e compreensão durante essa fase, por sempre estar presente e me apoiando.

A todos os professores que me forneceram o conhecimento necessário para que eu pudesse concluir essa etapa, em especial ao meu orientador Paulo pela paciência e dedicação.

Agradeço também a todos os colegas, pela amizade e companheirismo.

Muito Obrigado a Todos!

“É mais fácil obter o que se deseja com um sorriso do que à ponta da espada.”

William Shakespeare

RESUMO

Os usuários de Internet cada vez mais optam pelo uso das redes sem fio, buscando comodidade e flexibilidade. As *wireless* podem ser encontradas tanto no meio corporativo quanto no uso doméstico. A evolução da tecnologia voltada para dispositivos móveis com acesso a Internet foi quem deu grande estimulo para essa mudança. Mas junto com os benefícios encontrados muitos problemas também surgiram, como os dados trafegam pelo ar muitas vulnerabilidades foram exploradas, trazendo problemas relacionados a segurança das informações. Neste trabalho foram realizados alguns testes, para verificar o desempenho da segurança das redes sem fio analisando as senhas utilizadas para proteção das redes. Algumas informações sobre a criação de senhas seguras também foram descritas. A importância das políticas de segurança nas organizações também são citadas, bem como a configuração bem feita nos *Access Points*, utilizando todos os recursos disponíveis para assim tornar a rede menos vulnerável.

Palavras-chave: Redes sem fio; Segurança; Senhas.

ABSTRACT

The internet users more and more choose to use wireless networks, searching comfort and flexibility. The wireless can be found as many as in the corporate environment and in household. The evolution of technology directed to mobile devices with Internet access was who gave great stimulus to this change. But together with the benefit found many problems appeared also, like data travels through the air many vulnerabilities were exploited, bringing problems related to information security. We carried out some tests, to check the security performance of wireless networks analyzing the passwords used to protect networks. Some information about creating secure passwords were also described. The importance of security policies in organizations are also quoted, well as the configuration done well in Access Points, using all available resources to turn the network least vulnerable.

Keywords: Wireless Networks, Security, Passwords.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CRC – 32	Cyclic Redundancy Check
DES	Data Encryption Standard
DSSS	Direct Sequence Spread Spectrum
ESSID	Extended Service Set ID
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertz
GPS	Global Positioning System
HR-DSSS	High Rate Direct Sequence Spread Spectrum
Hz	Hertz
IBM	International Business Machines
IDEA	International Data Encryption Algorithm
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
ISM	Industrial, Scientific and Medical
IV	Inicialization Vector
Mbps	Megabits por segundo
MAC	Media Access Control
MHz	Megahertz

OFDM	Orthogonal frequency-division multiplexing
OS	Operational System
OTP	One-Time Password
PA	Ponto de Acesso
PRNG	Pseudo Random Number Generator
PSK	Pre Shared Key
PDAs	Personal Digital Assitant
QoS	Quality of Service
RC	Ron's Code ou Rivest Cipher
RSA	Rivest, Shamir e Adleman
RSN	Robust Security Network
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection Systems
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

SUMÁRIO

1 INTRODUÇÃO

A utilização das redes sem fio está em expansão. Cada vez mais os usuários optam por este tipo de conexão, buscando comodidade e flexibilidade, e como resultados surgem novas tecnologias, acompanhadas com uma grande queda nos preços (TANENBAUM, 1997).

Com a popularização dos *Notebooks*, PDAs *Personal Digital Assistants* (PDAs), celulares, entre outros, alguns estabelecimentos como bares, aeroportos, *shoppings*, estão investindo na implantação de redes sem fio, para que seus clientes tenham acesso à informação como se estivessem em casa, buscando a satisfação e a fidelização (KUROSE; ROSS, 2006).

A facilidade na implantação desta rede em relação às cabeadas é um ponto positivo para a instalação das mesmas. Sem a necessidade de passagem de cabos este modelo acaba se tornando uma opção mais rápida. A flexibilidade é outra vantagem encontrada, sendo possível alterar ou adicionar estações na rede sem a necessidade de modificar o cabeamento (TANENBAUM, 1997).

Motivados pela facilidade de instalação muitos empresários optaram pela implantação dessas redes buscando maior rendimento e conforto para seus funcionários, porém as atenções em relação à segurança devem ser redobradas, pois muitos desses dados que ficam disponíveis na rede são de grande importância, e acabam ficando expostos a ataques (HAYDEN, 1999).

O aumento da utilização deste modelo de rede tornou os usuários alvo de pessoas mal intencionadas, onde estas buscam causar alguma instabilidade ao sistema, por exemplo, a utilização se senhas fracas, ou configurações mal feitas nos *Access Points*.

Com essa mudança cultural de acesso à Internet, é necessário conhecer as vulnerabilidades e as formas de proteção para as mesmas. Não se alcança a imunidade apenas com o uso de antivírus e *firewall*. Uma forma bem comum que auxilia a proteção é a ativação dos protocolos *Wired Equivalent Privacy* (WEP) e *Wi-Fi Protected Access* (WPA), no *Access Point* (AP), uma vez que estes fazem a criptografia dos pacotes trafegados e assim aumentam a confiabilidade dos dados, porém ainda não garantem a segurança, problema como quebra da criptografia podem ocorrer.

Assim este trabalho tem o objetivo de analisar e descrever as vulnerabilidades existentes em redes sem fio, bem como instruir os usuários na criação de senhas seguras, de forma que este documento sirva para auxiliar os administradores de redes, e os demais usuários, e que contribua com os acadêmicos do curso de Ciência da Computação, na compreensão e utilização do material aqui produzido.

1.1 OBJETIVO GERAL

Analisar as vulnerabilidades existentes em redes sem fio, e mostrar uma forma de proteção por meio de senhas seguras.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos da pesquisa são os seguintes:

a) descrever sobre segurança em redes sem fio;

b) descrever os métodos de segurança para redes sem fio;

c) analisar e estudar as vulnerabilidades que uma rede está sujeita;

d) estudar e aplicar os métodos de segurança por meio de senhas confiáveis.

1.3 JUSTIFICATIVA

A necessidade de estar permanentemente *online*, a busca pela liberdade durante as conexões e a utilização de equipamentos portáteis que possibilitam conexão à Internet impulsionaram o crescimento das redes sem fio exponencialmente (RISCHPATER, 2001).

Um grande problema encontrado pelos usuários de *networks wireless* (rede sem fio) é a segurança. Com isso houve a necessidade do desenvolvimento de novos métodos contra essas vulnerabilidades, porém acompanhando esta evolução novas ferramentas de ataque são desenvolvidas a cada dia, ameaçando a integridade das informações. Para proteger-se é necessário estar bem informado, identificar, analisar e utilizar ferramentas disponíveis para proteção.

Os ataques à rede podem ser ativos e passivos. Ataques passivos invadem a rede, porém não alteram seus dados, eles apenas monitoram e espionam o tráfego de informações, geralmente realizados por pessoas, sem intenção de fazer mal ao usuário, fazem apenas por esporte. Os ataques ativos trazem maiores prejuízos, alterando ou copiando dados das transmissões, geralmente são realizados por pessoas contratadas para descobrir alguma informação sigilosa visando lucros (HAYDEN, 1999).

Não é possível afirmar que existem redes completamente seguras, mas, no entanto existem métodos para proteção disponíveis até mesmo gratuitamente, uma configuração bem feita e uma senha bem elaborada podem trazer uma tranqüilidade maior ao usuário. Porém por falta de informação ou até mesmo por acreditarem que nunca sofrerão um ataque vários usuários acabam tendo suas redes invadidas por ações que poderiam ter sido evitadas.

Com o objetivo de apresentar e esclarecer formas de segurança fundamentais para os usuários, esta pesquisa analisará as vulnerabilidades em redes sem fio, a fim de fornecer

informações necessárias para a compreensão do funcionamento destes ataques, e por outro lado serão apresentados métodos para criação de senhas mais fortes para tornar uma rede sem fio mais segura.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é distribuído em seis capítulos voltados para ameaças e seguranças em redes sem fio, sendo que o primeiro é constituído pela introdução que traz os objetivos e a justificativa para a realização deste trabalho.

No segundo capítulo é encontrada uma abordagem sobre redes sem fios, algumas de suas características e os padrões mais utilizados.

O capítulo três trata das ameaças e vulnerabilidades encontradas neste tipo de rede, nele são encontradas as principais ameaças e ferramentas utilizadas para atacar as WLANs.

Os métodos de defesa são encontrados no quarto capítulo. Neste são mostrados algumas formas de proteção e ferramentas para monitoramento de ataques a essas redes.

Os trabalhos correlatos, realizados por acadêmicos desta e de outras universidades podem ser vistos no capítulo cinco.

No sexto capítulo contém o trabalho desenvolvido, nele estão as informações obtidas por meio dos testes práticos com as senhas com o objetivo de testar o grau de segurança que elas fornecem.

O capítulo a seguir da inicio a fundamentação teórica, parte essencial para a concretização do trabalho proposto trazendo algumas informações sobre redes sem fio.

2 REDES SEM FIO

O crescimento das redes sem fio vem acontecendo de forma explosiva em todo mundo. Há algumas décadas a Internet era projeto de pesquisa, envolvia apenas dezenas de sites. Porém, seu crescimento foi estonteante e se tornou instrumento essencial na vida das pessoas, milhões de sites já existem fornecendo serviços e lazer para pessoas de todas as partes do mundo (COMER, 2001).

Os usuários desta ferramenta têm necessidade de informação e buscam cada vez mais comodidade e flexibilidade, com isso houve um grande aumento na procura de equipamentos móveis, como resultado essas ferramentas se tornaram mais populares e de fácil aquisição, porém para tornarem-se completamente portáveis há a necessidade da utilização de redes sem fio (TANENBAUM, 1997).

O aumento de ligações de computadores, *notebooks*, celulares, por meio de redes contribuiu para o aumento das redes sem fio. Hoje é comum em escolas, aeroportos, restaurantes, hotéis, disponibilizarem *Wireless* para facilitar o acesso das pessoas à Internet. As redes domésticas cada vez mais vêm conquistando seu espaço, os usuários buscam interligar seus equipamentos ou distribuir o sinal por toda sua residência (NAKAMURA; GEUS, 2003).

Segundo Tanenbaum (1997) a fácil instalação, sem a necessidade de passagens de fios, muitas vezes por locais onde a estrutura não permite essa ação, é um motivo que favorece a expansão desta tecnologia.

2.1 FREQÜÊNCIAS DE TRANSMISSÃO

As *Wireless* trafegam suas informações por meio de ondas eletromagnéticas, quebrando as barreiras dos fios e cabos. Estas ondas são fáceis de criar, percorrem longas distâncias e penetram os ambientes fechados (COMER, 2001).

Essas ondas são geradas a partir da movimentação dos elétrons, onde as oscilações delas são chamadas de freqüência, medidas em Hertz (Hz), e o conjunto destas é chamado de espectro eletromagnético, conforme a Figura 1 (TANENBAUM, 1997).

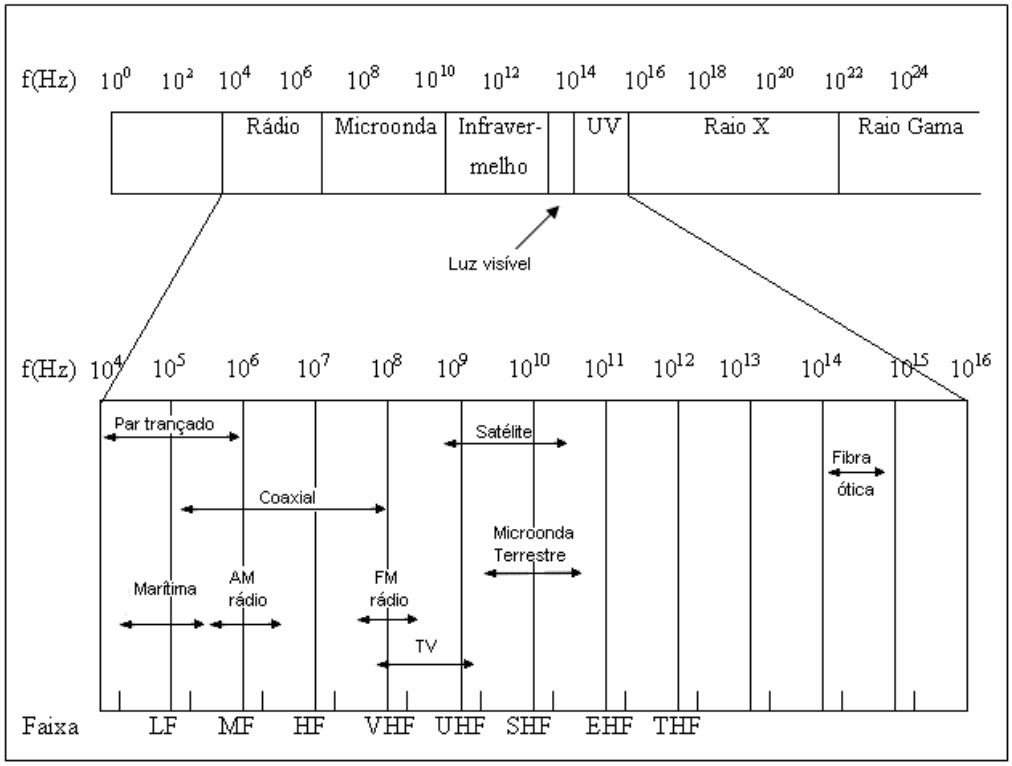


Figura 1. Espectro eletromagnético e a maneira de como ele é usado na comunicação
Fonte: Adaptado de TANENBAUM, A. S. (1997, tradução nossa)

Segundo Soares, Lemos e Colcher (1995) as transmissões sem fio normalmente usam freqüências altas, porém deve-se ter atenção com a existência de interferência, provocada por fontes que geram sinais na mesma freqüência da rede.

2.2 ARQUITETURA DO PROTOCOLO IEEE 802.11

Todas as atividades realizadas pelo protocolo IEEE 802.11 acontecem na camada física e na camada de enlace, mostrada na Figura 2, mais especificamente na subcamada MAC. As outras camadas controlam outros fatores como endereçamento, integridade, formato dos dados, não interferindo se a transmissão esta sendo realizada por meio de cabos ou por uma rede sem fios (ANDRADE, 2004).

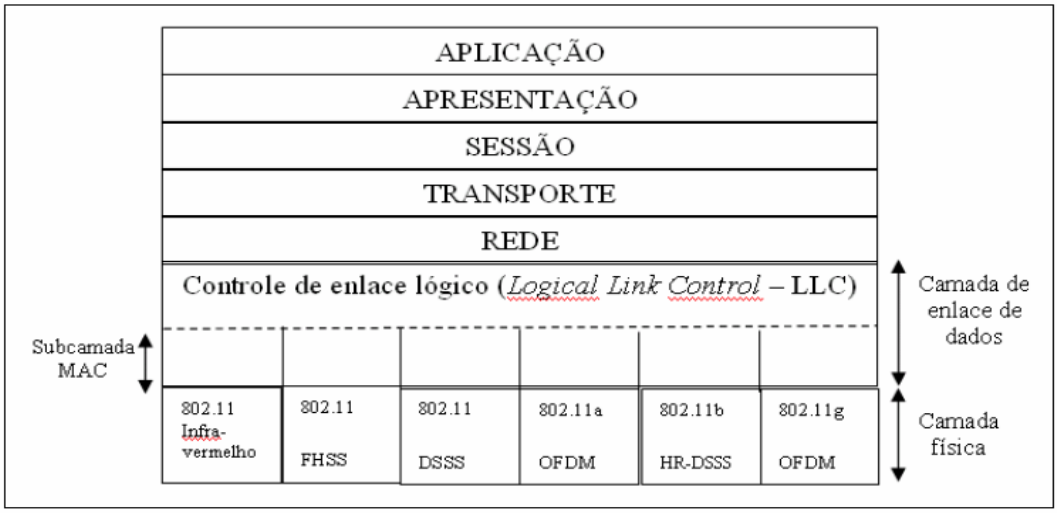


Figura 2. Pilha de Protocolo IEEE 802.11
Fonte: Adaptado de TANENBAUM, Andrew S. (2003, tradução nossa).

O padrão 802.11 lançado em 1997 utilizava os recursos de modulação *Frequency Hopping Spread Spectrum* (FHSS) e *Direct Sequence Spread Spectrum* (DSSS). Já em 1999 novas técnicas de modulação de sinal foram desenvolvidas, sendo elas, *Orthogonal Frequency Division Multiplexing* (OFDM) e *Hight Rate Direct Sequence Spread Spectrum* (HR-DSSS).

2.2.1 Modulação de Sinal FHSS

O *Frequency Hopping Spread Spectrum* (FHSS*) ou* espectro de dispersão de saltos de freqüência, utiliza 79 canais, começando na extremidade baixa da banda *Industrial*

Scientific and Medical (ISM) de 2,4 GHz, cada um contém 1 MHz de largura. A seqüência de freqüência de saltos é definida por meio de um gerador de saltos aleatórios, que são definidos por um gerador de números pseudoaleatórios, onde cada um desses números corresponde a uma freqüência, como mostra a Figura 3. A randomização oferece segurança, pois um invasor que não conhece a seqüência dos saltos não poderá espionar as transmissões (TANENBAUM, 2003).

Este tipo de modulação apresenta bom desempenho quando realizado em longas distâncias. Sua principal desvantagem é a baixa largura de banda.

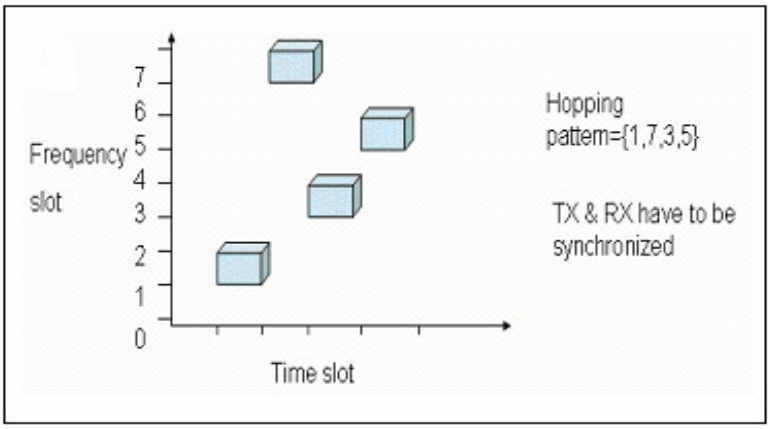


Figura 3. Modulação de Sinal FHSS
Fonte: MALBURG (2004).

2.2.2 Modulação de Sinal DSSS

Este método de modulação, o espectro de dispersão de seqüência direta, da mesma forma que o FHSS utiliza banda ISM de 2,4 GHz. A modulação deste é realizada por meio de quebra de seqüência conhecida como código de Barker.

O código de Barker consiste em substituir cada bit de valor 1 (um) por uma seqüência de bits, e o bit de valor 0 (zero), pela seqüência oposta. Com essa redundância de valores fica muito mais fácil de corrigir e controlar erros ocorrentes nas transmissões.

O DSSS é utilizado no padrão IEEE 802.11b e é menos vulnerável a ruídos e ataques. A Figura 4 está apresentado o funcionamento da modulação de sinal DSSS.

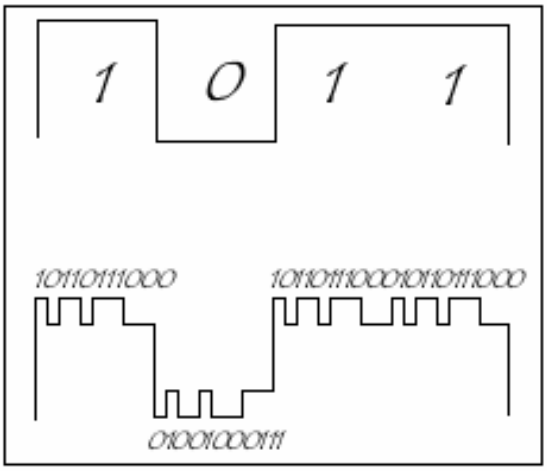


Figura 4. Modulação de Sinal DSSS
Fonte: Kioskea.net (2009).

2.2.3 Modulação de Sinal OFDM

A multiplexação ortogonal por divisão de freqüência pode transmitir até 54 Mbps na banda ISM mais larga, de 5 GHz. São utilizadas 42 freqüências para dados e 4 para sincronização. Uma melhor imunidade à interferência é alcançada por meio da divisão de uma banda larga em varias bandas estreitas (TANENBAUM, 2003).

Essa técnica tem boa eficiência de bits/Hz e boa imunidade em longas distâncias utilizando vários caminhos. Sendo esta modulação utilizada pelo IEEE 802.11a.

A Figura 5 mostra a técnica de modulação OFDM.

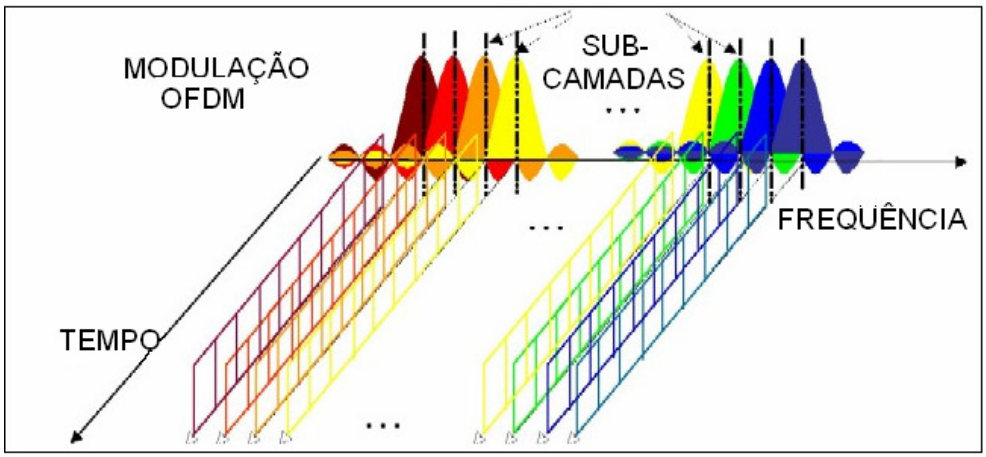


Figura 5. Modulação de Sinal OFDM
Fonte: Adaptado de HOADLEY, John. (2005, tradução nossa).

2.2.4 Modulação de Sinal HR-DSSS

A modulação *High Rate Direct Sequence Spread Spectrum* (HR-DSSS) é uma versão derivada da modulação DSSS, foi criada com a intenção de aumentar a velocidade de transmissão. Nela são utilizados 11 milhões de chips para alcançar 11 Mbps na banda de 2,4 GHz. As taxas de dados admitidos são 1, 2, 5, 11, Mbps e podem ser adaptadas durante a operação para alcançar a melhor velocidade sob as condições atuais de carga e ruído. Este tipo de modulação é utilizado no padrão IEEE 802.11b (TANENBAUM, 2003).

2.3 PADRÕES PARA REDES SEM FIO 802.11

O sinal sem fio trafega por meio de ondas de rádio, porém muitos outros meios de transmissão usam este método, com isso existem riscos de interferência nas transmissões (PETERSON; DAVIE, 2004).

Com o objetivo de evitar que estes danos prejudicassem as transmissões os sinais de radiofreqüência foram divididos em faixas, geralmente por sua categoria de serviços, e definidos por órgãos regulamentadores ou padrões internacionais (COZER, 2006).

Este tipo de sinal existe há muitos anos, porém no inicio os equipamentos comercializados não respeitavam um padrão tornando mais difícil a comunicação entre equipamentos, e obrigando o cliente a utilizar sempre a mesma marca para não ter problemas.

Os padrões de redes sem fio mais conhecidos foram criados pelo *Institute of Electrical and Electronics Engineers* (IEEE), instituto muito respeitado, criador de padrões utilizados por outros tipos de redes. O IEEE foi eleito para criá-los a partir da década de 90.

Em 1997 baseado em regras existentes foi lançado o IEEE 802.11, com normas específicas para as redes sem fios, buscando aumento na confiabilidade de transmissão,

qualidade de sinal e padronização de equipamentos (COSTA, 2009). Como característica possuía taxa de transmissão de 2 Mbps e freqüência de 2,4 GHz (SILVA, 2006).

Na Tabela 1, é possível visualizar as extensões existentes ao padrão IEEE 802.11, um breve resumo sobre suas características e seu estado no momento (FREITAG, 2004).

Tabela 1. Extensões do Padrão IEEE 802.11

Extensão	Descrição	Estado
802.11	Padrão original que oferece taxas de 1 e 2 Mbps.	Aprovado em 1997
802.11a	Extensão para prover 54 Mbps na banda 5 GHz.	Aprovado em 1999
802.11b	Extensão para prover 11 Mbps na banda 2.4 GHz.	Aprovado em 1999
802.11d	Modificações para atender a regulamentação internacional.	Aprovado em 2001
802.11e	Extensão à camada MAC para prover QoS.	Em debate
802.11f	Recomendações para comunicação entre PAs.	Fase final
802.11g	Extensão para prover 54 Mbps na banda 2.4 GHz.	Fase final
802.11h	Extensão ao 802.11a para atender a regulamentação na Europa.	Fase final
802.11i	Extensão para aumentar a segurança.	Em debate
802.11j	Modificações para atender a regulamentação no Japão.	Fase inicial
802.11k	Sistema de gerenciamento da WLAN.	Fase inicial
802.11m	Revisão e re-edição do padrão existente em andamento.	Em andamento
802.11?	Padrão para prover taxas acima de 100 Mbps.	Em andamento

Fonte: Adaptado de FREITAG, J. (2004)

Nos próximos itens será apresentado um pouco sobre as características dos sub-padrões da IEEE 802.11 mais conhecidas: 802.11b, 802.11a, 802.11g, 802.11i, 802.11n (COSTA, 2009).

2.3.1 IEEE 802.11b

Este foi o primeiro sub-padrão lançado, especificado em 1999, tendo como velocidade máxima de transmissão 11 Mbps, mas também podendo se comunicar com velocidades mais baixas utilizando a banda de 2,4 GHz (JUNIOR, 2008).

Por trabalhar em uma faixa mais baixa tem como desvantagem a interferência de outros dispositivos que usam a mesma faixa. Neste padrão são permitidos conexões para 32 clientes por AP (COSTA, 2009).

Mesmo contendo algumas desvantagens, o padrão IEEE 802.11b está classificado como o mais popular, com uma tecnologia simples e de baixo investimento, para clientes que buscam mobilidade e locais onde não há viabilidade para passagem de cabos (COZER, 2006).

2.3.2 IEEE 802.11a

Esta foi a segunda versão lançada do padrão 802.11, tem freqüência de 5,8 GHz, porém sua área de alcance é menor. Neste padrão são aceitos 64 clientes conectados por AP, sua modulação consiste em 12 canais sobrepostos que permite uma melhor cobertura de áreas mais povoadas (COSTA, 2009). Sendo que sua segurança é baseada no protocolo WEP de 256 bits (COZER, 2006).

O diferencial do padrão IEEE 802.11a está relacionado ao desempenho, sendo que esta pode alcançar uma taxa de transferência de 54 Mbps, cinco vezes mais rápida que o padrão IEEE 802.11b (ANDRADE, 2004).

Porém, mesmo com as mudanças realizadas alguns problemas ainda foram encontrados, como por exemplo, a incompatibilidade com outros dispositivos, pois opera em faixa de 5 GHz (JUNIOR, 2008).

2.3.3 IEEE 802.11g

O mais recente padrão para redes sem fio, surgindo como o sucessor do padrão IEEE 802.11b (SOUZA, 2005).

Utilizando a banda ISM de 2,4 GHz permite que equipamentos dos padrões IEEE 802.11 e IEEE 802.11b sejam compatíveis, tornando menos traumática e mais econômica a migração entre os padrões. Porém não é compatível entre equipamentos de outras marcas (RUFINO, 2005).

Este padrão usa a modulação *Orthogonal Frequency Division Multiplexing* (OFDM) com uma taxa de transmissão de 54 Mbps (FREITAG, 2004).

2.3.4 IEEE 802.11i

Segundo Costa (2009) este padrão se destaca pela busca da segurança e a autenticação dos dados por meio dos protocolos de segurança *Robust Security Network* (RSN) e *Wi-Fi Protected Access* (WAP), que foi criado para ter um melhor desempenho que o até então existente WEP.

2.3.5 IEEE 802.11n

O padrão IEEE 802.11n se destaca pela velocidade que pode chegar a 500 Mbps. Não tem grandes novidades em relação à segurança, seu diferencial esta na ampliação da área de cobertura (JUNIOR, 2008).

Esta expansão da cobertura pode se tornar um problema, pois aumenta a área vulnerável a ataques da rede.

2.4 TOPOLOGIA DE REDES WIRELESS

A topologia é um mapa da rede, sendo o posicionamento dos computadores e dos equipamentos definidos por meio da topologia física. Um planejamento mal feito de uma rede

pode trazer posteriormente gastos desnecessários e comprometer o desempenho dos recursos oferecidos.

As redes sem fio levam como critério de organização dois modos distintos, o Ad-Hoc e a Infra-Estrutura.

2.4.1 Rede *Ad-Hoc*

O modo *Ad-Hoc* é utilizado em redes que não possuem uma estrutura estabelecida, e não impõe limite máximo de equipamentos conectados a ela. Esse modo não disponibiliza conexão via cabo e todos os equipamentos podem se comunicar entre si (ALVES, 2009).

Este tipo de rede vem sendo estudada com mais freqüência, isso acontece devido sua fácil instalação, grande mobilidade, e fácil conexão do usuário, já que este pode se conectar desde que o sinal esteja a seu alcance (ANDRADE; COLLI, 2003).

Porém ainda contêm algumas falhas, como a velocidade que ainda é baixa, a segurança, a administração e o gerenciamento da rede, que ainda precisam ser melhorados (ALVES, 2009).

A Figura a 6 mostra o funcionamento e a estruturação da topologia *Ad-Hoc*.

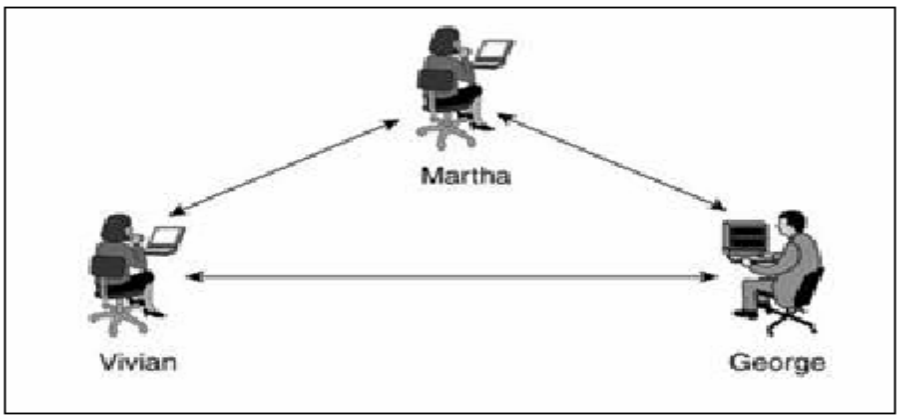


Figura 6. Rede *Ad-Hoc*
Fonte: (ALVES, 2009).

2.4.2 Rede Infra-Estrutura

O modo infra-estrutura não permite que os equipamentos se comuniquem entre si diretamente, essa troca de informações é feita por um *Access Point,* que facilita o controle da rede, pois isso pode ser feito em apenas um local (ALVES, 2009).

Algumas vantagens podem ser encontradas nesse tipo de estrutura, a facilidade de interligação de redes sem fio e redes cabeadas existentes, controle e configuração das conexões feitas em um único local, facilitando assim o controle e gerenciamento da rede.

A estruturação de uma rede infra-estruturada pode ser observada na Figura 7.

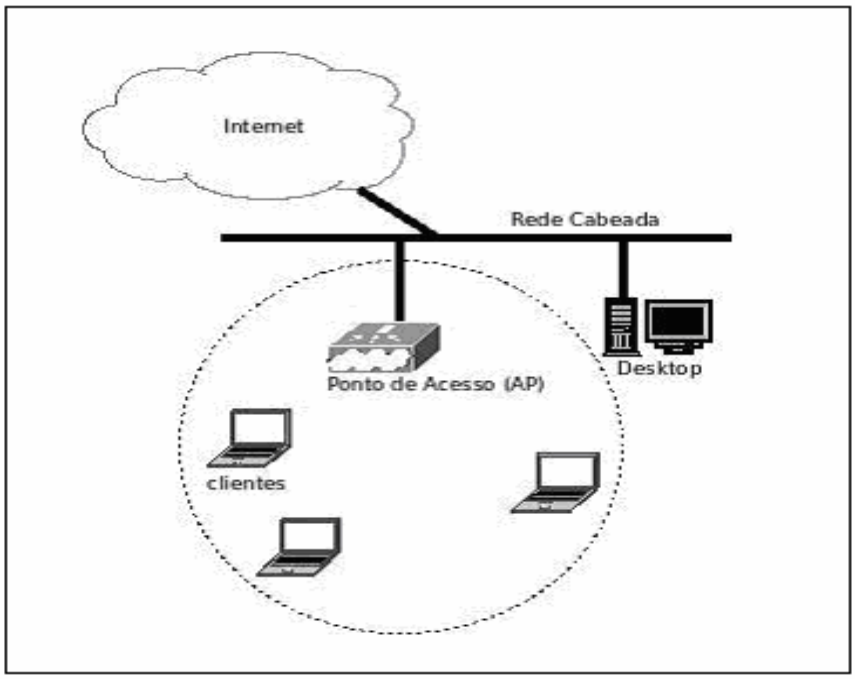


Figura 7. Rede Infra-Estruturada
Fonte: (PEREIRA, 2009).

Em um comparativo entre os dois tipos de topologia de rede podem ser encontradas várias diferenças, que serão descritos na Tabela 2:

Tabela 2. Comparativo entre Rede *Ad-Hoc* e Rede Infra-Estruturada

Característica	***Ad-Hoc***	**Infra-Estrutura**
Alcance de sinal	Por não possuir uma estrutura bem definida, pode ter perda de sinal de forma brusca conforme a distância do acesso.	Mantém uma estabilidade maior na intensidade do sinal, já que seu alcance pode ser definido por configuração no concentrador.
Segurança	Não possui segurança de forma significativa, por não ter estruturação e nem controle de acesso. Tem uma alta taxa de erros.	Possui um nível de segurança considerado razoável, já que suas definições podem ser feitas de forma geral diretamente no *Access Point*.
Instalação	Fácil instalação, já que este tipo de rede não necessita de uma infra-estrutura previamente instalada.	Para uma instalação bem sucedida necessita de um estudo do ambiente e de um planejamento da rede.
Tolerância à falhas	A constante troca de conexões faz que ao perder a conexão com um ponto, possa ser conectado outro sem maiores problemas, desde que esse esteja disponível.	As redes infra-estruturadas têm um controle maior de falhas, pois qualquer ação a ser realizada deve ter uma autorização do concentrador.
Conectividade	A comunicação entre dois pontos ou mais pode acontecer diretamente, desde que estes estejam dentro da área de cobertura da rede.	A comunicação entre dois pontos só ocorre por meio da estação de suporte a mobilidade.

Fonte: Adaptado de ANDRADE, M; COLLI, R (2003).

Algumas vulnerabilidades existentes em redes sem fio podem ser observadas no capítulo a seguir, onde são descritos alguns ataques comuns e ferramentas que podem ser utilizadas para que esses sejam executados.

3 VULNERABILIDADES EM REDES SEM FIO

Este modelo de rede exige de seus usuários um cuidado maior que as cabeadas, por terem um alcance maior e transmitirem seus dados com sinais via rádio por meio do ar, acabam sofrendo os mesmos ataques encontrados nas redes cabeadas e alguns específicos foram inseridos (ANDRADE, 2004).

Apesar de os usuários estarem cada vez mais preocupados com a segurança de suas informações, e os fabricantes investirem cada vez mais em novas tecnologias para deixar seus equipamentos mais seguros, a realidade é que não existem redes completamente seguras, mas sim redes mais protegidas e difíceis de atacar (COZER, 2006).

Segundo Duarte (2003) uma rede sem fio deve levar em conta alguns fatores fundamentais para um bom funcionamento:

a) confiabilidade: proteger a informação de acessos não autorizados;

b) disponibilidade: garantir a disponibilidade de recursos e informações;

c) integridade: evitar que mudanças sejam feitas em documentos sem permissão;

d) usabilidade: impedir que um recurso ou serviço tenha sua utilidade distorcida ou prejudicada devido a restrições de segurança.

Alguns tipos de vulnerabilidades são descritos na Tabela 3.

Tabela 3. Tipos de Vulnerabilidades

Tipos	Descrição
Físicas	Instalações fora de padrão, falta de estrutura, incêndios, alagamentos e outros
Naturais	Qualquer estrago realizado por força da natureza, enchentes, vendavais e outros.
Hardware	Falha em recursos tecnológicos, por falha ou má utilização.
Software	Instabilidade nos dados por má instalação ou configuração indevida.
Mídias	A perda ou danificação do dispositivo de armazenamento de dados.
Comunicação	Acesso não autorizado ou perda de comunicação.
Humano	Problemas causados por erros de usuários, vândalos, roubo entre outros.

Fonte: Adaptado de SÊMOLA, Marcos (2003).

3.1 ATAQUES A REDES SEM FIO

Os ataques às redes sem fio geralmente ocorrem quando uma vulnerabilidade é explorada, juntamente com alguma falha nos fatores fundamentais da rede, como integridade e confiabilidade (COSTA, 2009).

As *Wireless* são o maior alvo de ataques maliciosos da atualidade, pois com o grande número de usuários ocorreu o aumento do interesse sobre os dados que trafegam nestas redes, sendo estas empresariais ou até mesmo domésticas (GIMENES, 2005).

Segundo o Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil (2009) é assustador o aumento nos ataques a redes no Brasil. A Figura 8 mostra a evolução dos incidentes reportados ao CERT.br de 1999 até junho de 2009.

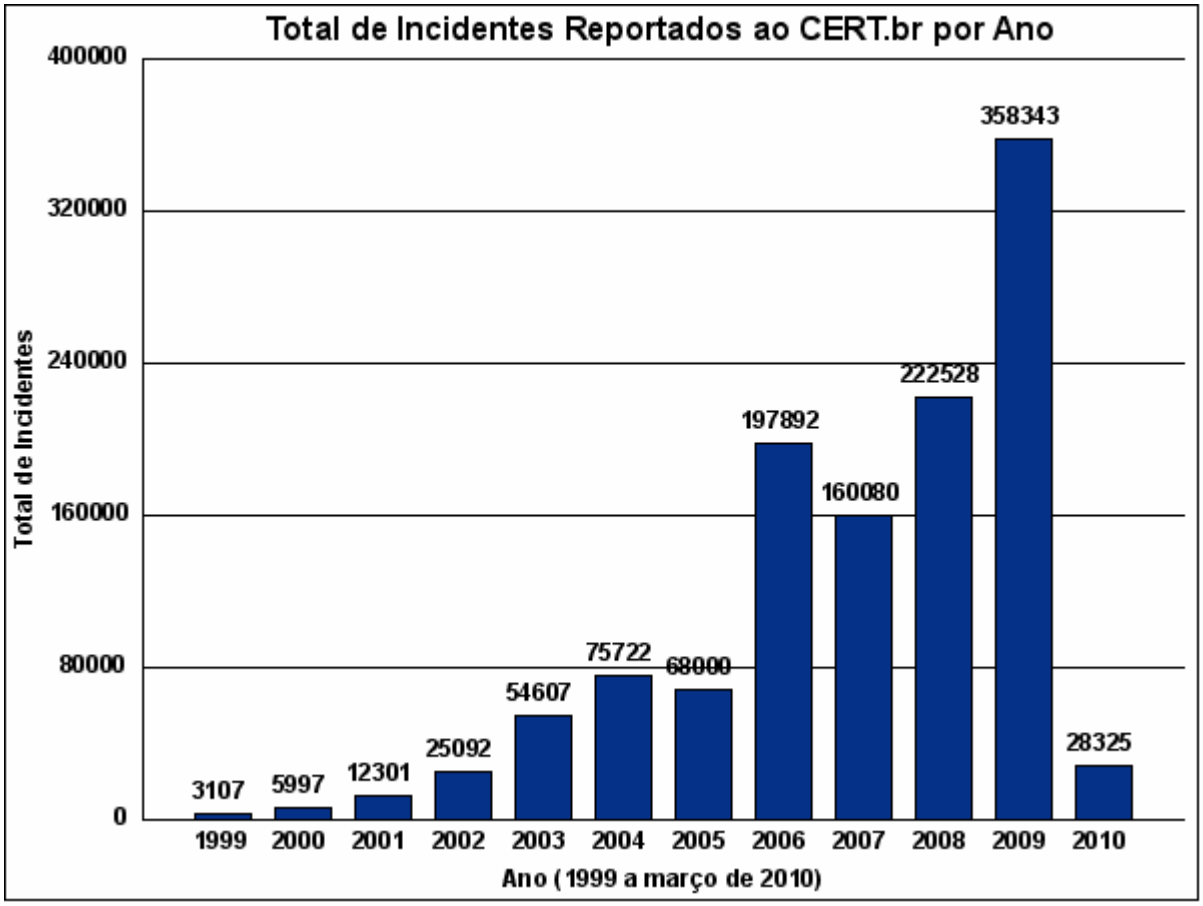


Figura 8. Incidentes reportados ao CERT.br no período de 1999 até março de 2010
Fonte: (CERT.br, 2010)

3.2 AMEAÇAS A REDES SEM FIO

As ameaças são todas as ações que podem por em risco as informações que trafegam na rede. Uma forma de garantir a integridade da informação e combater ataques maliciosos é impedindo que as vulnerabilidades existentes na rede sejam exploradas (MAIOR; SANTOS; LACQUA, 2006).

A qualquer momento uma ameaça pode se concretizar por meio de alguma falha existente na rede, e de acordo com o impacto que esta ação pode causar ela pode ser classificada. Segundo Maior, Santos e Lacqua (2006) elas são classificadas em três grupos:

a) naturais: causadas por condições da natureza, que podem ocasionar na destruição de itens que compõem a rede. Por exemplo: incêndios, enchentes, terremotos, vendavais, entre outros;
b) involuntárias: acontecem por acaso, sem consciência, na maioria das vezes por falta de conhecimento do usuário. Por exemplo: exclusão de arquivos importantes, e outros erros acidentais;
c) intencionais: ocasionadas por pessoas com o objetivo de prejudicar quem está sendo atacado. Por exemplo: sabotagens, fraudes, roubos de informações, invasões, entre outras ações que podem prejudicar a integridade da rede;

Algumas ameaças que merecem destaque, por serem mais evidentes, serão citadas a seguir.

3.2.1 Access Point Spoofing (Associação Maliciosa)

A Associação Maliciosa ocorre quando um atacante mal intencionado se passa por um *Access Point*, induzindo o usuário a se conectar na intenção de estar realizando uma

conexão com uma *Wireless Local Area Network* (WLAN) real. Com a ajuda de um *software*, como o FakeAP, o atacante é capaz de enganar um sistema, mostrando um dispositivo de rede padrão como um ponto de acesso (DUARTE, 2003).

3.2.2 ARP Poisoning

O ataque de envenenamento do protocolo de resolução de endereços *Address Resolution Protocol* (ARP) ocorre na camada de enlace de dados e só pode ocorrer quando o usuário e o atacante estão conectados na mesma rede local. As redes conectadas por roteadores e *gateways* estão imunes a este ataque, porém as redes conectadas por *hubs*, *switches* e *bridges* são vulneráveis (ANDRADE, 2004).

O ARP Poisoning, que pode ser vista na Figura 9, é um ataque que tem origem nas redes cabeadas, que redireciona o tráfego para o impostor via falsificação/personificação do endereço MAC (LACERDA, 2007).

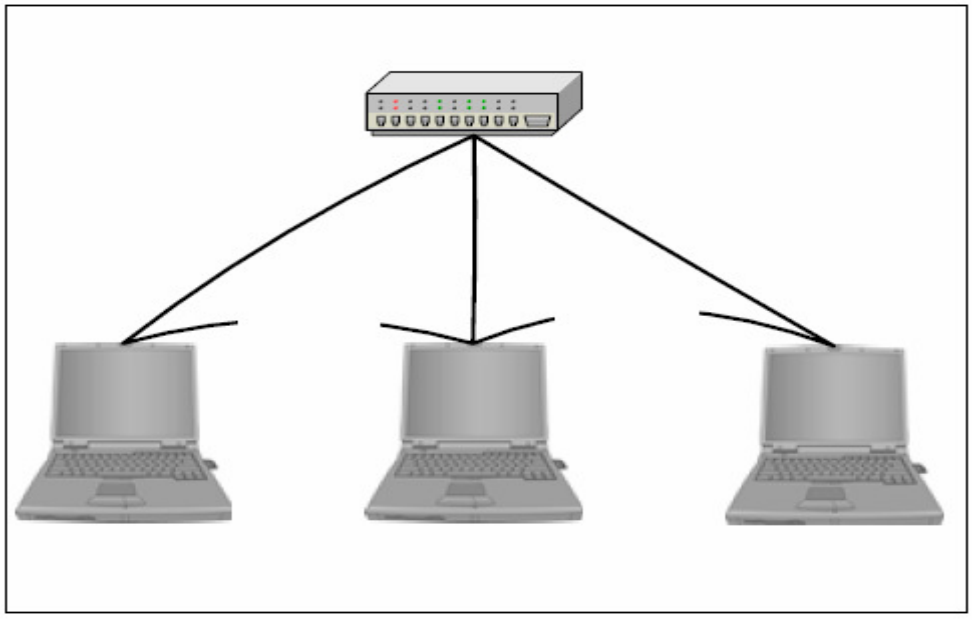


Figura 9. ARP Poisoning em redes guiadas
Fonte: (DUARTE, 2003).

3.2.3 MAC Spoofing

Os dispositivos sem fio possuem a particularidade de permitir a troca de endereço físico, assim atacantes mal intencionados alteram o endereço da placa de rede, pelo do atacado e utilizam a rede (LACERDA, 2007). O endereço MAC do usuário atacado pode ser capturado por meio de *Eavesdropping & Espionage*, tendo em mãos este endereço o atacante pode usufruir da rede e de todos seus recursos (DUARTE, 2003).

3.2.4 Ataques de Negativa de Serviços

Este tipo de ataque também conhecido por *Denail of Service* (D.o.S), como o próprio nome diz, é utilizado por pessoas mal intencionadas para impedir que os usuários possam acessar alguns recursos existentes na rede (DUARTE, 2003).

Estes ataques podem ser disparados em qualquer lugar dentro da cobertura da WLAN, as redes que utilizam IEEE 802.11b ou IEEE 802.11g por utilizarem freqüência de 2,4 GHz podem sofrer ataques com mais facilidade por estarem na faixa de freqüência de equipamentos como forno microondas e celulares, estes equipamentos podem interferir no acesso por meio de inserção de ruídos (DUARTE, 2003).

3.2.5 Ataques de Vigilância

Também conhecido como WLAN *Scanner*, este tipo de busca não é considerado um ataque, dependendo da finalidade desta invasão pode se tornar um ataque com efeitos negativos de grandes dimensões (DUARTE, 2003).

Este ataque é realizado quando uma pessoa sai em busca de WLANs disponíveis no ambiente de seu interesse, podendo ser na sua cidade, universidade, ou empresa. Para esta busca não há a necessidade de possuir nenhum dispositivo especial, apenas possuir um dispositivo com acesso sem fio (GIMENES, 2005).

Após este período de investigação, as redes sem fio encontradas podem ser testadas ou atacadas em um próximo momento, onde os dados de sua configuração de segurança serão analisados e possivelmente roubados (GIMENES, 2005).

3.2.6 Ataques de Força Bruta

É uma ameaça que consegue quebrar a senha de segurança por meio de várias tentativas, usando senhas de forma dedutiva até que a verdadeira seja descoberta. Várias ferramentas existem para que os administradores das redes possam constatar a solidez das senhas aplicadas, mas grande parte dos usuários desta ferramenta são pessoas não autorizadas que tentam ingressar na rede.

3.2.7 Ataques de Dicionário

Este ataque é realizado quando o atacante pega os dados de um dicionário já existente e compara com o arquivo de senhas do usuário até que consiga desvendar a senha ativa na rede. Existem ferramentas que testam as opções individualmente e também realiza combinações para obter um número maior de possibilidades.

O ataque de dicionário é mais eficaz que os de força bruta, principalmente em casos de senhas mais longas, onde o tempo para testar as seqüências possíveis se tornar inviável.

3.2.8 Eavesdropping & Espionage

O objetivo desta ameaça é capturar e analisar os dados que trafegam na rede e utilizá-los em futuros ataques. O funcionamento nas redes sem fio é muito parecido com o das guiadas, sendo que nesta o atacante necessita estar ligado diretamente a uma máquina da rede que será atacada, já nas WLANs isso não é necessário tornando esse ataque muito mais simples.

3.2.9 Wardriving

O Wardriving é bem semelhante ao ataque de vigilância, sendo que este utiliza equipamentos geralmente *Global Positioning System* (GPS) para realizar a busca de redes sem fio no território escolhido (LACERDA, 2007).

3.2.10 Warchalking

Com a identificação de redes realizadas com técnicas de Wardriving, o atacante marca em muros ou calçadas os pontos em elas estão disponíveis para um futuro ataque. Estas marcas são feitas por meio de códigos com intuito de mantê-las em segredo.

Na Figura 10 é possível visualizar o símbolos utilizados nas marcações. Sendo que o desenho de dois semicírculos significa que a rede é vulnerável, um círculo completo significa que naquele local se encontra uma rede fechada, já o último com um W dentro do circulo fechado significa que a rede é fechada e protegida com criptografia WEP. O *Service Set Identifier* (SSID) encontra-se na parte superior e a largura da banda é mostrada abaixo dele.

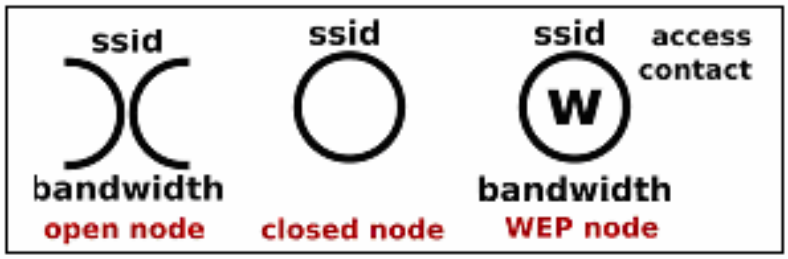


Figura 10. Símbolos de warchalking
Fonte: Adaptado de Pinheiro, José Mauricio Santos (2004)

3.3 FERRAMENTAS PARA ATAQUES

Várias ferramentas foram criadas para utilização em redes sem fio. Essas ferramentas podem ser utilizadas tanto para o bem quanto para o mal, elas podem realizar monitoramento ou quebra de chaves em redes sem fio. Essas podem ser classificadas em três categorias: *scanners* (detectam redes para futuros ataques), *sniffers* (capturam e analisam o tráfego da rede) *e crackers* (realizam quebra de chaves) (DIAS NETO, 2006). A seguir serão descritas algumas delas.

3.3.1 NetStumbler

Este é o tipo mais conhecido de scanner em WLANs (redes sem fio). Segundo Dias Neto (2006), esta ferramenta utilizada em ambiente *Windows* inclui muitas características como potência do sinal, *Extended Service Set ID* (ESSID[1]) da rede em questão, além de suporte a GPS. Porém esta não é utilizada somente por pessoas mal intencionadas, o gerente da rede também a utiliza para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição.

[1] É um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede.

Segundo Lacerda (2007) algumas limitações também são encontradas, as mais expressivas são de não realizar captura de tráfego e não possuir métodos para quebra de chaves WEP.

3.3.2 Kismet

Um sniffer (farejador) muito conhecido, desenvolvido com tecnologia *open souce*2, com funcionamento em ambientes Linux/Unix, inclui muitas ferramentas e opções. Este é projetado com arquitetura cliente/servidor, e além de monitorar muitas origens diferentes pode também armazenar pacotes capturados. Por meio da união das suas características com um GPS, podem ser gerados dados relacionados à localização do dispositivo monitorado.

Segundo Duarte (2003) o Kismet disponibiliza várias das informações necessárias para que um ataque possa ser realizado, e por meio de análises, pode ser constatado que o Kismet é a melhor ferramenta para utilização em Linux (COZER, 2006). Algumas das informações disponibilizadas são:

a) número de WLANs detectadas;

b) total de pacotes capturados por WLAN;

c) ausência ou não de criptografia WEP;

d) número de pacotes irreconhecíveis;

e) pacotes descartados e tempo decorrido desde a execução do programa;

f) número de pacotes com o vetor de inicialização (I.V);

g) nome da rede (SSID).

h) nível de sinal;

i) taxa máxima suportada pela rede;

[2] Possui código aberto, ou seja, qualquer pessoa que conheça pode realizar alterações.

j) BSSID (relaciona-se ao endereço MAC do *Access Point*);

k) Qual o canal que a WLAN esta configurada;

l) Se o dispositivo monitorado é um *Access Point*, ou não;

m) Padrão utilizado (802.11 a/b/g).

Algumas das características citadas acima podem ser visualizadas na Figura 11.

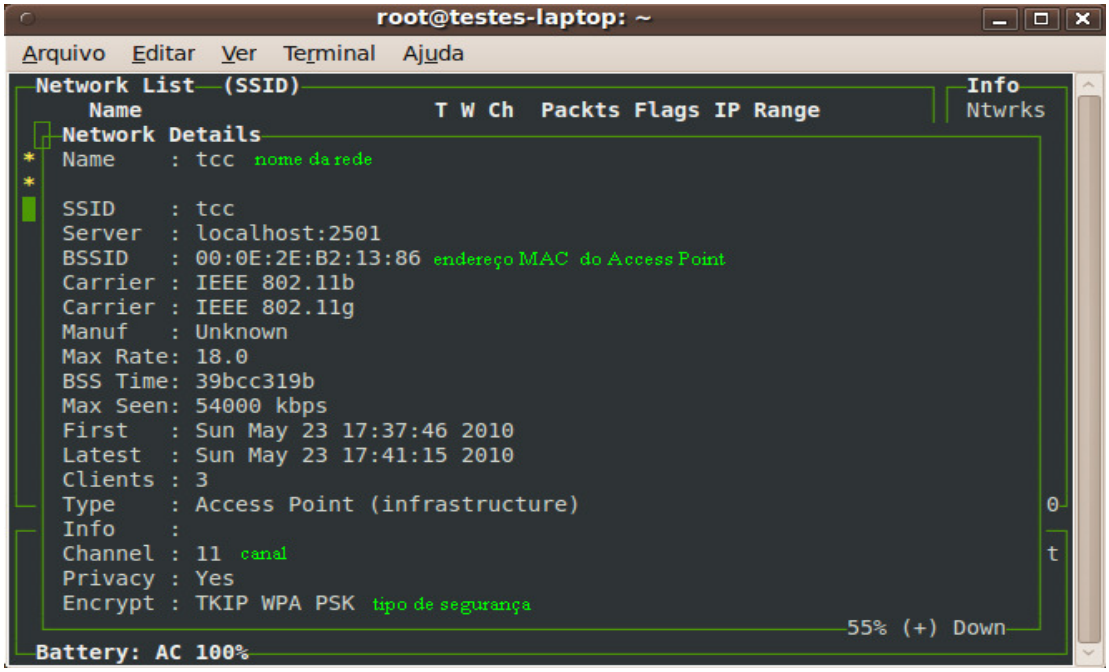


Figura 11. Tela do Kismet em execução

3.3.3 WEPCrack

Segundo Cozer (2006) este programa que funciona em ambientes *Linux* e *Windows*, é utilizado geralmente por pessoas mal intencionadas, que por meio de vulnerabilidades encontradas no protocolo WEP se apoderarem de informações vitais da rede, como por exemplo, o SSID, para realizar ataques posteriormente.

3.3.4 AirSnort

Esta ferramenta foi lançada após a divulgação das falhas no protocolo WEP, considerada antiga, porém ainda muito utilizada, ela realiza a quebra de chaves WEP, essa quebra acontece após obter entre três e cinco milhões de pacotes trocados (MOURA, 2005).

3.3.5 Aircrack

Segundo Moura (2005) o Aircrack esta classificada entre as ferramentas mais eficientes disponíveis para quebra de chaves WEP, capaz de mostrar o tráfego usando a chave descoberta, gerando assim um arquivo com a mensagem decifrada.

Esta ferramenta também é muito utilizada para tentativas de quebra WPA e WP2.

3.3.6 FakeAP

Este é um programa capaz de transformar um dispositivo de rede sem fio em um *Access Point*, falsificando algumas características que fazem com que o usuário pense estar conectado ao concentrador correto (SOUZA, 2005). Dentre suas características ganham destaque:

a) Receber conexões em um canal específico;
b) Usar ESSID específico;
c) Utilizar um endereço MAC específico ou o padrão de um fabricante;
d) Usar uma determinada chave WEP;
e) Permitir configuração de potência de saída.

Segundo Souza (2005) o FakeAP geralmente é utilizado por pessoas mal intencionados buscando dados para atacar a rede em uma ocasião futura.

3.3.7 Airtraf

O Airtraf permite que sejam coletadas muitas informações sobre as redes identificadas em tempo real. Para invasores ele traz diversas vantagens como número de clientes conectados e serviços utilizados além de quebrar a chave do protocolo WEP no padrão 802.11b. Quando utilizada por administradores permite que sejam monitoradas as atividades pelas quais são responsáveis.

No próximo Capítulo algumas formas de proteção contra ataques serão descritos, buscando que os usuários e administradores de redes possam alcançar uma maior segurança em suas informações.

4 SEGURANÇA EM REDES SEM FIO

Cada vez mais a informática é vista como aliada da evolução econômica. Muitas empresas vêem nessas ferramentas uma forma de tornar o trabalho de seus funcionários mais fácil e rápido, assim tornando seu negócio mais competitivo (NAKAMURA, 2000).

As redes são fundamentais neste processo, tornando possível a ligação entre esses computadores. Sendo que as sem fio possuem um grande diferencial em relação às cabeadas, pois esta disponibiliza mobilidade e assim permite que os usuários possam encontrar mais liberdade no trabalho enquanto usam a rede e como resultado acabam produzindo mais e gerando mais lucros para a organização (NAKAMURA, 2000).

Com o aumento do interesse dos usuários em relação às conexões sem fio teve-se que aumentar as ferramentas para diminuir as vulnerabilidades que estas redes estão expostas. E uma das formas de manter uma rede segura esta em prevenir os ataques, já que sua área vulnerável é bem maior que a das redes cabeadas por ultrapassar o espaço físico, e com isso a dificuldade de controle de invasores é bem maior (ANDRADE, 2004). Na Tabela 4 serão descritas três modalidades que classificam as medidas de segurança.

Tabela 4. Medidas de Segurança

Medidas de Segurança	Descrição
Preventivas	Visam prevenir que ataques venham a ocorrer, para isso são realizadas palestras, treinamentos, configurações de equipamentos entre outros.
Detectáveis	Analisam os focos que podem estar causando as ameaças.
Corretivas	Correção das estruturas buscando que se adaptem a política da organização.

Fonte: Adaptado de SÊMOLA, M. (2003).

4.1 FERRAMENTAS PARA DETECÇÃO DE ATAQUES E MONITORAMENTO

A prevenção é uma arma muito forte contra os ataques a redes, para isso muitos softwares de monitoramento vem sendo criados para que as invasões possam ser impedidas ou encontradas antes de concluídas, e também para que se encontre o foco em que falhas podem estar ocorrendo. Abaixo serão descritas algumas ferramentas para detecção e monitoramento de ataques.

4.1.1 WIDS

A *Wireless Intrusion Detection Systems* (WIDS) segundo Lacerda (2007), é uma ferramenta que consegue detectar não apenas ataques, mas diversas outras irregularidades. Abaixo estão descritos os tipos de tráfegos monitorados por esta ferramenta.

a) estudo do intervalo de tempo entre os *beacons* de cada concentrador encontrado;

b) detecção de requisições encontradas;

c) detecção da freqüência de requisições de reassociação;

d) localização de repetidas requisições de autenticação em um intervalo de tempo muito pequeno.

4.1.2 Snort Wireless

Esta ferramenta é utilizada para identificar ataques baseados em assinaturas, pacotes mal formados e tráfego suspeito. Trata-se de um sistema de detecção de intruso que é capaz de fazer o registro dos pacotes e a análise do tráfego de uma rede em tempo real.

4.1.3 AirMagnet

Este *Software* de monitoramento permite o reconhecimento de dispositivos estranhos conectados á rede possibilitando que alarmes sejam acionados quando algum evento estranho for detectado.

Segundo Lacerda (2007) o AirMagnet ajuda a organizar os níveis de segurança das WLANS com uma rotina que facilite o entendimento do administrador. Quando uma rede não é projetada de forma correta vários problemas podem ser detectados no decorrer da utilização.

4.1.4 AirStrike

Esta ferramenta tem o objetivo de promover a segurança durante o acesso a *Wireless* por meio do ponto de acesso sem comprometer a conexão. O AirStrike é baseado no padrão 802.11a, 802.11b e 802.11g, e realiza o gerenciamento das redes sem fio com confiabilidade garantindo que apenas usuários autorizados possam ter acesso.

O funcionamento desta ferramenta leva em consideração sete princípios listados abaixo:

a) autenticação: certifica a legitimidade do usuário e a do *gateway*[3] de segurança;
b) autorização: apenas usuários autorizados têm acesso aos recursos da rede;
c) privacidade: os dados que trafegam na rede são criptografados e não podem interceptados por invasores;

[3] É o endereço que faz a conexão entre os usuários da rede.

d) mobilidade: os usuários podem se descolar pela rede sem fio livremente desde que exista cobertura de pelo menos um ponto de acesso;

e) gerenciamento: todos os parâmetros de segurança podem ser gerenciados de forma integrada;

f) portabilidade: suporte a diversas plataformas de clientes, como *Windows*, *Linux*, Mac OS, PDAs (*Assistente Pessoal Digital*) e *Smartphones*;

g) interoperabilidade: o sistema suporta dispositivos proprietários, integrando-se a uma rede sem fio existente, como também provê a funcionalidade de um dispositivo sem fio proprietário. De toda forma, o resultado é a redução de custos.

Na Figura 12 os componentes da arquitetura desta ferramenta de segurança.

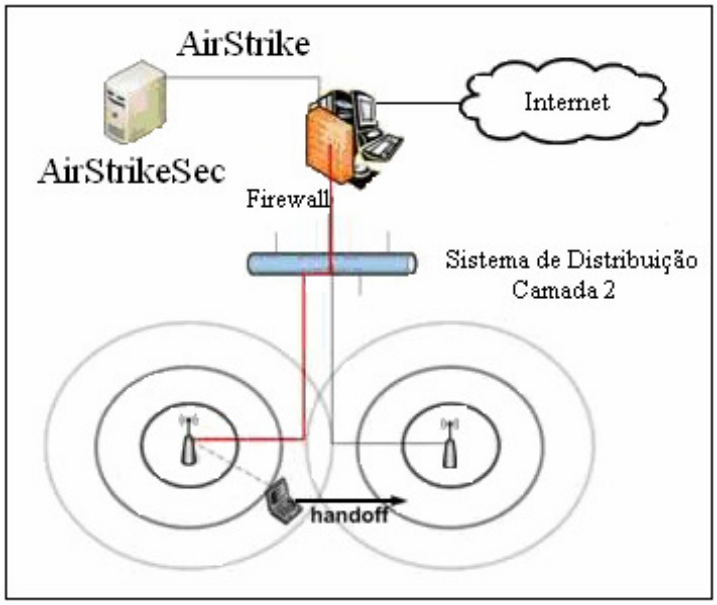


Figura 12. Componentes da arquitetura do AirStrike
Fonte: (AIRSTRIKE, 2009).

4.2 CRIPTOGRAFIA

Uma forma de aumentar a segurança dos dados que trafegam na rede é utilizando a criptografia. Com esta forma de proteção o tráfego de dados na rede é feito sem uma

combinação lógica, tornando impossível seu entendimento imediato, assim se for atacado o invasor não terá acesso ao seu conteúdo.

Segundo Lacerda (2007) o objetivo de se realizar a criptografia computacional é buscar:

a) sigilo dos dados: onde somente usuários autorizados possam ter acesso;
b) integridade: garantindo ao usuário que a informação esta está correta;
c) identidade do usuário: onde o sistema pode verificar a identidade do usuário ou do dispositivo que esta em contato.

A criptografia dos dados é realizada como mostra a Figura 13.

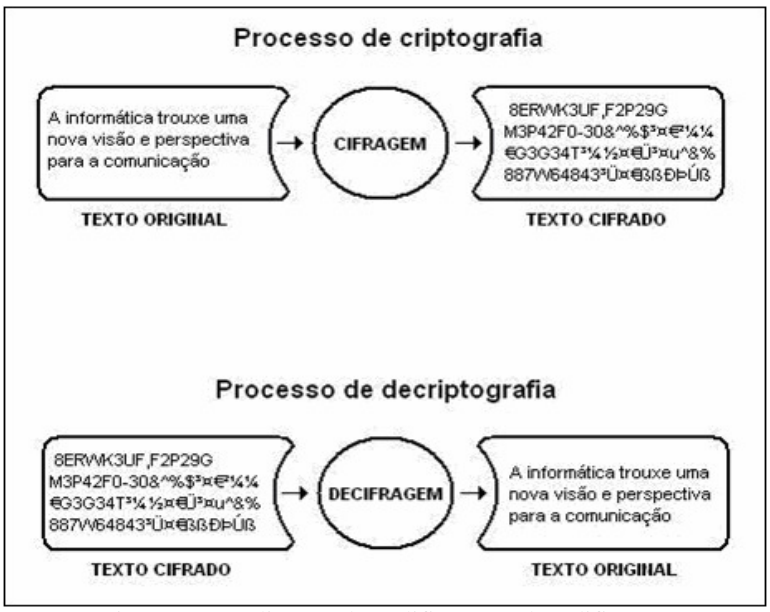


Figura 13. Realização da codificação e decodificação
Fonte: (Costa, 2009).

Nesta forma os dados enviados passam por um processo de cifragem, onde seu conteúdo sofre influência de códigos e símbolos para que seu sentido original seja perdido. Ao chegar ao seu destino os dados criptografados passam pelo processo inverso, onde a mesma técnica é aplicada, transformando o código no seu formato original para se tornar entendível pelo recebedor.

Existem duas formas criptografia, a de chave privada e a de chave pública, mais sobre elas será relatado a seguir.

4.2.1 Criptografia de Chave Privada (Simétrica)

Este tipo de criptografia também conhecido como criptografia tradicional utiliza o mesmo fundamento da criptografia antiga, por meio de transposição e substituição, porém os algoritmos utilizados atualmente são tão complexos que até mesmo os criptoanalistas sentem dificuldades em desvendar o código sem possuir a chave (TANENBAUM, 2003).

Na criptografia simétrica a chave para criptografar e descriptografar é a mesma, assim o receptor e o transmissor têm que estar cientes da chave a ser utilizada (FIGUEIREDO; DINIZ; COROA, 2005).

Os alguns algoritmos utilizados neste tipo de criptografia são listados na tabela 5:

Tabela 5. Alguns algoritmos de chave simétrica

Cifra	Autor	Comprimento da chave	Comentários
Blowfish	Bruce Schneier	1 a 448 bits	Antigo e muito lento
DES	IBM	56 bits	Já se tornou muito fraco
IDEA	Massey e Xuejia	128 bits	Bom, mas patenteado
RC4	Ronald Rivest	1 a 2048 bits	Algumas chaves são fracas
RC5	Ronald Rivest	128 a 256 bits	Bom, mas patenteado
Rijndael	Daemen e Rijmen	128 a 256 bits	Melhor escolha
Serpent	Anderson, Biham, Knudsen	128 a 256 bits	Muito forte
DES triplo	IBM	168 bits	Segunda melhor escolha
Twofish	Bruce Schneier	128 a 256 bits	Muito forte; amplamente utilizado

Fonte: Adaptado de Tanenbaum, A. (2003)

4.2.2 Criptografia de Chave Pública (Assimétrica)

A criptografia de chave pública, ou assimétrica, é uma forma de criptografia que exige duas chaves, uma para criptografar e outra para descriptografar, sendo que uma é sigilosa e outra é disponibilizada para todos os usuários, e uma não pode ser derivada da outra.

Este modelo funciona de forma simples, uma pessoa cria duas chaves uma para criptografar e outra para descriptografar, a primeira é divulgada e a segunda fica em posse apenas do criador, assim apenas ele poderá ter acesso as mensagens enviadas.

O algoritmo mais utilizado nesta forma de segurança de dados é o RSA, criado em 1976 e utilizado até hoje.

4.3 PROTOCOLOS DE CRIPTOGRAFIA

A utilização dos protocolos de criptografia existentes nas redes sem fio é uma ação muito importante para estabelecer um índice razoável de segurança para suas informações.

Os protocolos WEP, WAP e WAP2 são disponibilizados para utilização dos usuários das WLANs, esses protocolos serão apresentados a seguir.

4.3.1 Protocolo WEP

Com o aumento da busca por segurança este protocolo esta presente em todos os equipamentos que seguem o padrão das redes sem fios.

Este protocolo foi aprovado em 1999, utiliza algoritmos simétricos para realizar a cifragem de seus dados, sendo assim a chave deve ser compartilhada com todas as estações de trabalho e com o *Access Point* (LACERDA, 2007).

O protocolo WEP atua na camada de enlace, usa o algoritmo de criptografia *Ron's Code 4* (RC4), seu vetor de inicialização (IV) é de 24 bits e sua chave secreta compartilhada (*secret shared key*) é de 40 ou 104 bits, assim somando o IV com a chave secreta tem-se a

chave de 64 ou 128 bits, o algoritmo *Cyclic Redundancy Check* (CRC-32) atua em conjunto e é utilizado para fornecer integridade quanto aos pacotes (GIMENES, 2006).

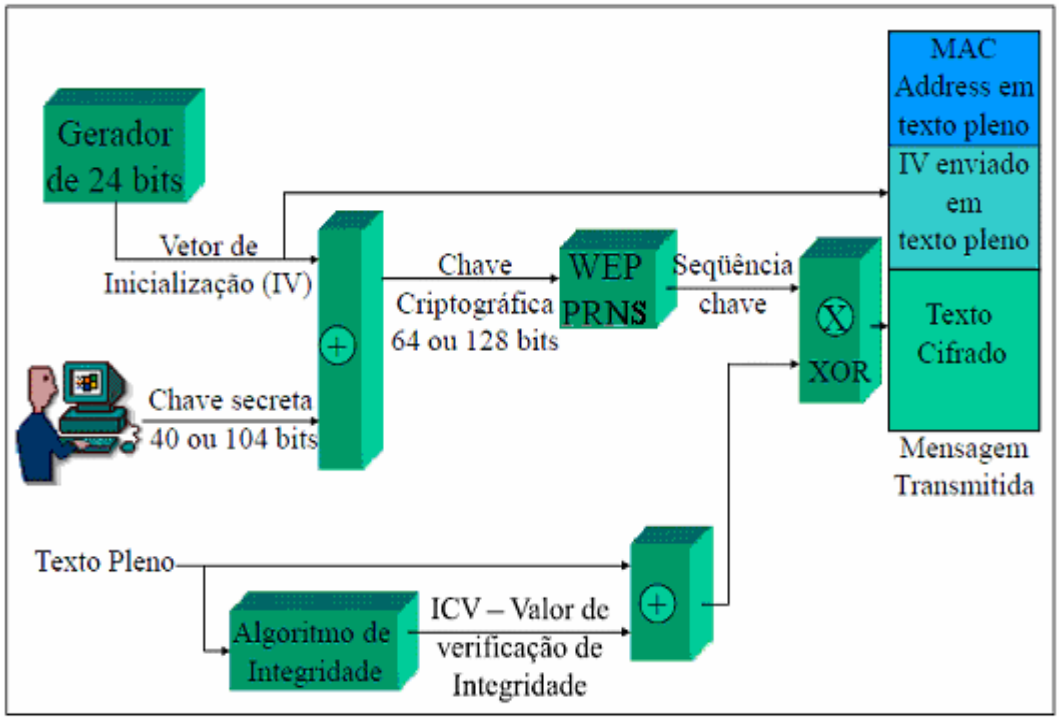


Figura 14. Realização da codificação com o WEP
Fonte: (JÚNIOR SANTOS, 2008).

Como pode-se observar na figura 14 o IV tem sempre 24 bits e é concatenado com a chave secreta que é configurada manualmente e pode ter 40 ou 104 bits. Esta chave concatenada é inserida no algoritmo RC4, que transforma em uma seqüência de números pseudo-randomica, que pode ser chamada de RC4 (IV,K) ou PRNS. Sendo que não existe uma ordem para que o IV seja iniciado, ele adquire um novo valor geralmente quando a placa de rede se conecta ao AP.

O texto enviado passa por um algoritmo de integridade, gerando o CRC-32 (*Cyclic Redundancy Checks*), valor de verificação de integridade, que é concatenado com o texto. Na seqüência um XOR é realizado com o PRNS e o resultado da concatenação entre texto e o CRC-32, só assim o pacote pode ser enviado criptografado, porém preservando o IV sem criptografia.

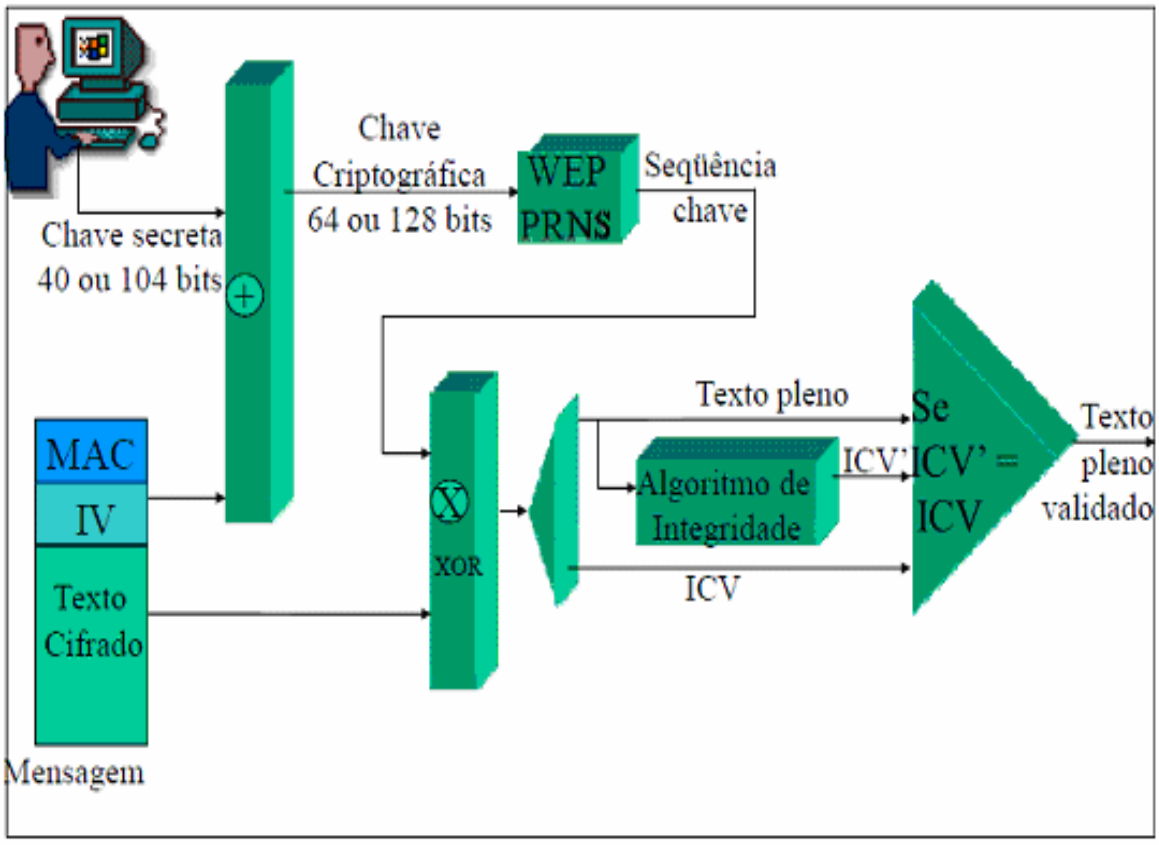


Figura 15. Realização da decodificação com o WEP

Fonte: (JÚNIOR SANTOS, 2008).

Após a mensagem enviada, como pode ser visto na Figura 15, o receptor concatena o IV com a chave compartilhada e passa pelo algoritmo RC4 para encontrar a mesma PRNS criada para a transmissão. Então um XOR é feito com o texto e o PRNS. Assim o texto enviado é recuperado juntamente com o *Integrity Check Value* (ICV) que é comparado ao CRC-32 de origem que é analisado para verificar a legitimidade, se esta for alcançada o texto é enviado para o *host*, senão é desconsiderado.

Este protocolo possui suas falhas e vulnerabilidades, porém é um item a mais na busca pelo aumento na segurança dos dados (LACERDA, 2007). Sua maior vulnerabilidade esta relacionada com alguns valores do IV, que podem tornar a chave fácil de ser desvendada (COSTA, 2009).

4.3.2 Protocolo WPA

Também conhecido como WEP2, esta primeira versão do WPA foi criada em 2003, busca de corrigir vulnerabilidades encontradas no WEP. Esta versão funciona em todos os equipamentos que utilizavam o protocolo antigo.

Este protocolo não disponibiliza utilização para *Ad-Hoc*, somente pode ser utilizado em redes onde concentradores são utilizados.

Segundo Costa (2009) WPA continua utilizando o algoritmo RC4, porém algumas melhorias foram encontradas como:

a) vetor de inicialização maior;

b) utilização de um novo código de verificação de integridade das mensagens (IV);

c) gerenciamento de chaves;

d) modo de autenticação corporativo e pessoal (doméstico).

Uma comparação entre a cifragem com WEP e com o WPA TKIP pode ser observado na Figura 16.

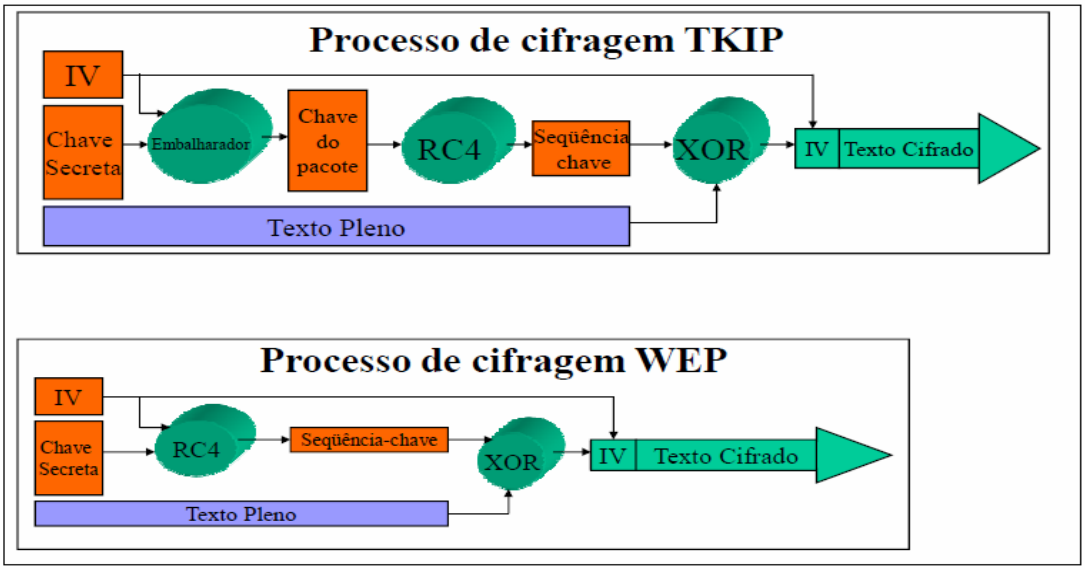


Figura 16. Comparativo entre a codificação com o WEP e com o WPA (TKIP)

Fonte: (JÚNIOR SANTOS, 2008).

Segundo Costa (2009), a principal vulnerabilidade do WPA está relacionada a forma de autenticação *Pre-Shared Key* (PSK), onde deve haver uma ligação por meio de senha entre o usuário e o AP, assim o atacante pode capturar os pacotes com o uso de captura passiva, e utilizar o ataque de dicionário para conhecer a senha. Como a maioria dos usuários usam senhas muito fracas a quebra se torna uma tarefa fácil, se as senhas tivessem um grau de dificuldade maior o atacante ficaria limitado ao tamanho do dicionário.

4.3.3 Protocolo WPA2

O protocolo WPA2 ou 802.11i, foi lançado em 2004 com a proposta de extinguir os problemas encontrados nos protocolos anteriores. Este tem como diferencial utilizar o algoritmo de criptografia *Advanced Encryptation Standart* (AES) e o *Temporal Key Integrity Protocol* (TKIP) em conjunto, com uma chave de 256 bits, e com essa chave mais extensa torna este padrão mais eficiente. Este protocolo permite a utilização de chaves de 128, 192 e 256 bits. A certeza da integridade das mensagens é obtida por meio do algoritmo *Michael Message Integrity Check*, que analisa se algum fator pode ter interferido na autenticidade da mensagem.

O algoritmo AES faz a combinação da chave em blocos de 128 bits e em seguida transforma em outro bloco de 128 bits completamente diferente do original. O processo de encriptação e desencriptação é o mesmo, ou seja, os fabricantes precisam implementar o processo uma única vez.

Um novo *hardware* se tornou necessário com a utilização deste novo algoritmo, pois este necessita de um co-processador para que os cálculos criptográficos sejam calculados (LACERDA, 2007).

A vulnerabilidade está ligada ao tamanho da chave utilizada pelo usuário, da mesma forma que o WPA, se as senhas forem pequenas podem ser facilmente desvendadas por ataques de dicionário.

4.4 POLITICAS DE SEGURANÇA

As políticas de segurança são uma forma preventiva de prezar pela segurança das informações de uma organização. É um documento onde todas as normas e regras a serem seguidas são documentadas. Assim todos os usuários da rede devem ter conhecimento desse documento e tem dever de segui-lo.

O inicio de uma política de segurança envolve uma visão abrangente, que possa analisar todos os problemas que a rede está exposta, deixando bem claro o que cada usuário pode ou não realizar, estas informações após serem aprovadas devem ser expostas e divulgadas a todos os usuários.

Segundo Spanceski (2004) quatro elementos devem ser seguidos para garantir a segurança em uma organização:

a) vigilância: todos os funcionários devem entender a importância do cumprimento das regras, e fiscalizar se os outros usuários estão seguindo as normas definidas;
b) atitude: o fácil acesso as informações contidas na política e o seu planejamento adequado são muito importantes para o sucesso das regras estipuladas;
c) estratégia: a política deve ser ampla e bem planejada que possa suportar todas as necessidades da organização, em nenhum momento as normas devem influenciar de forma negativa no andamento da empresa;

d) tecnologia: os equipamentos utilizados deverão suprir as necessidades, equipamentos desatualizados podem por em risco toda a estrutura.

Além das normas que os usuários devem seguir devem estar inclusos neste documento as formas de prevenção contra acidentes naturais, armazenamento e acesso das informações, controle de acesso físico, políticas de uso entre outras que podem ser observadas na tabela 6.

Tabela 6. Normas presentes nas Políticas de Segurança

Controles	Precauções
Acidentes Naturais	Os equipamentos principalmente do centro de informática devem estar protegidos de incêndios, enchentes e outros desastres, mas preparados que na ocorrência destes fenômenos os estragos sejam o menor possível.
Armazenamento e acesso das informações	O armazenamento das informações deve ser realizado em locais bem protegidos, onde *backups* possam ser realizados com freqüência, e somente possas autorizadas possam ter acesso.
Controle de acesso físico	O acesso físico pode ser menos prejudicial que o lógico, porém não pode ser esquecido, as pessoas que tem acesso aos dados devem ser identificadas e autorizadas.
Políticas de uso	O usuário deve saber prezar pelos equipamentos da organização, e ter ética ao utilizá-los, os equipamentos estão disponíveis para fins da organização, interesses pessoais não devem ser realizados utilizando essas ferramentas.

Fonte: Adaptado de Wanderley, D. (2005)

Segundo Wanderley (2005) deve-se ter muito cuidado na criação da política de segurança, pois ela não deve conter dados nem expressões técnicas, mas também não deve conter um passo a passo de acesso, deve conter informações diretas e simples, para que seja compreendida por todos os usuários, mas que não se torne uma arma contra a própria segurança da organização. No Capitulo a seguir serão relatadas algumas características de trabalhos anteriores que trazem características semelhantes a este.

5 TRABALHOS CORRELATOS

Com a expansão da utilização das redes sem fio, os ataques vêm ficando cada vez mais eficientes e métodos de defesa são desenvolvidos para tornar os clientes menos vulneráveis. Para que isso aconteça cada vez mais estudos e pesquisas vem sendo realizados nesta área.

Neste capítulo são relacionados alguns trabalhos que realizaram pesquisas relacionadas à segurança em redes sem fio.

5.1 SEGURANÇA REDES SEM FIO

Trabalho de Conclusão de Curso de Ciência da Computação, como requisito para obtenção do titulo de Bacharel em Ciência da Computação, realizado em 2006, na Faculdade de Jaguariúna, São Paulo.

O trabalho tem como objetivo aumentar o conhecimento dos usuários de redes sem fio sobre segurança e configuração de equipamentos, visando diminuir as falhas e ataques que acontecem a essas redes por pessoas mal intencionadas. Também são realizados testes usando ferramentas para ataques e defesas (COZER, 2006).

5.2 ANÁLISE DE PRADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11

Trabalho de Conclusão de Curso de Ciência da Computação, como requisito para obtenção do titulo de Bacharel em Ciência da Computação, realizado em 2009, na Universidade do Extremo Sul Catarinense, Criciúma, Santa Catarina.

Este trabalho aborda a importância das redes sem fio para a organização das informações, e a importância da segurança neste tipo de rede. Com o objetivo de abordar os padrões e protocolos mais conhecidos. Também foram realizados testes em ambientes projetados utilizando algumas ferramentas com objetivo de capturar senhas e analisar o desempenho das ferramentas (COSTA, 2009).

5.3 ANÁLISE DE VULNERABILIDADES E ATAQUES INERENTES A REDES SEM FIO 802.11X

Trabalho de Conclusão de Curso de Ciência da Computação, realizado em 2003, na Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, São Paulo.

O objetivo deste trabalho é mostrar e analisar as vulnerabilidades e ferramentas de ataque a redes sem fio, realizando testes e mostrando seu funcionamento, para servir como base para que ferramentas de defesa sejam desenvolvidas. Também são mostrados alguns padrões Wireless e a importância deste tipo de rede (DUARTE, 2003).

5.4 ANÁLISE DE SEGURANÇA EM REDES WIRELESS 802.11X

Trabalho de Conclusão de Curso de Ciência da Computação, realizado em 2007 na Universidade Federal de Juiz de Fora, em Minas Gerais.

O trabalho é constituído por estudos das fragilidades dos protocolos utilizados em Wireless, levantamento de ferramentas desenvolvidas especificamente para realizar ataques e verificações de mecanismos de defesa disponíveis que apresentam soluções eficazes para a segurança dessas redes (LACERDA, 2007).

6 ANÁLISE DE SEGURANÇA NOS CONCENTRADORES DE REDE SEM FIO

Na pesquisa realizada foram estudados vários fatores sobre as *Wireless*, sendo eles relacionados a vulnerabilidades e proteção, envolvendo o estudo teórico e prático. Com base nisso foram estudadas formas de proteção por meio de senhas seguras e de configuração corretas no AP.

Alguns testes práticos serão realizados, utilizando as informações obtidas nos capítulos anteriores. Iniciando com a análise de dos ataques que os protocolos de redes sem fio são vulneráveis, sendo o primeiro o ataque de força bruta, que é uma ameaça ao protocolo WEP, e o segundo o ataque de dicionário que ameaça os protocolos WPA e WPA2.

Os testes serão realizados utilizando a ferramenta Aircrack-ng, que contém um pacote de programas utilizados para análise da rede, captura, e quebra de chaves. Os protocolos utilizados nos testes serão o WEP, WPA, WPA2.

6.1 AMBIENTE E FERRAMENTAS UTILIZADAS

Os testes foram realizados em um ambiente projetado para a captura dos pacotes sem causar danos a outras redes ao alcance do atacante. Tendo como base o sistema operacional Linux Ubuntu 10.04, e utilizando as ferramentas Kismet, e o pacote Aircrack-ng, que inclui os seguintes componentes:

a) Airmon-ng: colocar a interface sem fio em modo monitor;
b) Airodump-ng: analisa e captura os IVs da rede;
c) Aireplay-ng: envia pacotes ao ponto de acesso com o objetivo de gerar mais tráfego e assim quebrar a chave de forma mais rápida;
d) Aircrack-ng: realiza a quebra das chaves.

Todos os programas utilizados, o sistema operacional e as ferramentas são disponibilizados gratuitamente.

A Figura 17 mostra o ambiente utilizado para realizar os testes.

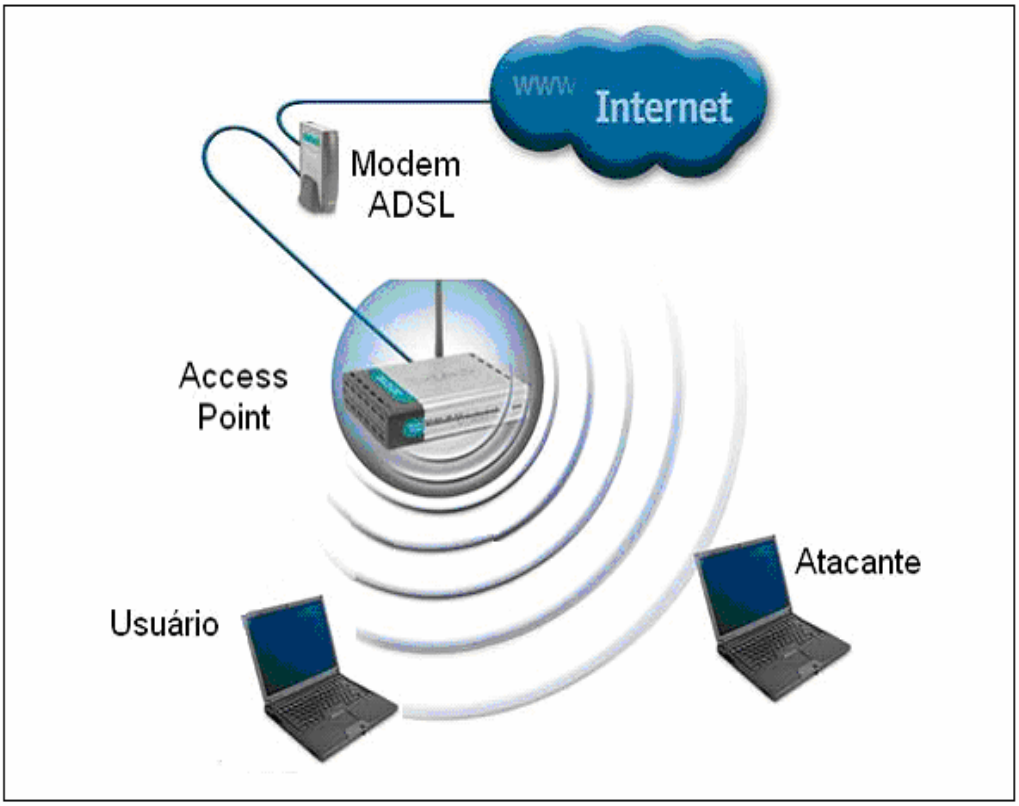


Figura 17. Ambiente utilizado para realização dos testes

Para que os testes pudessem ser executados foram utilizados os seguintes equipamentos:

a) D-Link DSL-500b: modem ADSL;

b) Air Live WL-5460AP: roteador sem fio;

c) Broadcom: placa sem fio;

d) Atheros: placa de rede sem fio;

e) notebook HP: utilizado na função de usuário;

f) notebook Samsung: utilizado como atacante;

6.2 CENÁRIOS E MÉTRICAS

As métricas a serem analisadas serão as seguintes:

a) análise do ataque de força bruta: examinar como esse ataque pode acontecer e uma forma de proteção;

b) análise do ataque de dicionário: observar quais fatores permitem que aconteça esse tipo de ataque e uma forma de proteção;

c) avaliação dos protocolos: aplicar os protocolos disponíveis e analisar o nível de segurança oferecido pelos mesmos;

d) construção correta de senhas: trazer informações importantes para que os usuários possam construir senhas capazes se fornecer segurança a sua rede;

e) configuração do *Access Point*: orientar o usuário em relação as configurações disponíveis em alguns APs;

f) políticas de segurança: mostrar aos usuários e administradores de redes a importância da elaboração de políticas de segurança para utilização de redes sem fio.

Para que essas análises sejam realizadas alguns cenários precisam ser elaborados:

a) presença do protocolo WEP: este primeiro teste conta com a existência do protocolo WEP utilizando chaves de 64 e 128 bits, sendo testadas três chaves para cada opção;

b) presença do protocolo WPA: existência do protocolo WPA TKIP realizando testes com senhas diferenciadas;

c) presença do protocolo WPA2: existência do protocolo WPA AES analisando senhas com características diferentes;

d) presença do protocolo WPA2 Mixed: que conta com a existência do protocolo WPA2 AES e WPA TKIP analisando senhas diferenciadas.

6.2.1 Ataque de Força Bruta

Esse ataque acontece por meio da captura dos IVs que trafegam pela rede, pode ser utilizado em redes que utilizam o protocolo WEP em todas as suas versões. Após a captura de aproximadamente 25.000 IVs para o protocolo WEP de 64 bits e 50.000 para a versão 128 bits, inicia um processo de tentativas seguidas até que a senha possa ser desvendada.

O ataque de força bruta não pode ser utilizado quando o protocolo utilizado é o WPA ou WPA2, pois nesse caso são permitidas chaves mais extensas, o que tornaria inviável esse método, uma quebra poderia levar meses (KIOSKEA, 2009).

6.2.2 Ataque de Dicionário

Esse ataque também acontece com a captura dos IVs que trafegam pela rede, é utilizado nos protocolos WPA e WPA2. Esse tipo de ataque exige além da captura dos IVs a captura do *handshake*[4] da rede (COSTA, 2009).

Esse ataque analisa os IVs capturados e compara com um arquivo de dicionário, também conhecido como Word List, para tentar desvendar a senha, porém a senha só será desvendada se a chave estiver contida no dicionário, sendo que as vezes um ataque bem sucedido só é obtido quando vários dicionários são testados (KIOSKEA, 2009).

[4] Autenticação que garante a comunicação entre o Access Point e o computador, onde está armazenada a criptografia utilizada na autenticação da rede.

6.2.3 Captura de IVs

Para que os ataques citados anteriormente possam ser executados é necessário que sejam capturados um número significativo de IVs. Os IVs trafegam de forma que todos os computadores ao alcance da rede podem "ouvi-los", mas só o destinatário pode recebê-lo. Então o atacante configura sua placa para modo monitor[5] e com auxilio de um software começa a capturar os pacotes que trafegam na rede. Sendo que não existe uma forma de inibir a captura dos pacotes, a única forma de evitar que a senha da rede seja descoberta é usando uma chave segura, difícil de ser desvendada.

6.3 CRIANDO SENHAS SEGURAS

Uma das formas utilizadas para que a segurança em uma rede sem fio seja mais robusta é a utilização de senhas fortes, mas um significativo número de pessoas não sabe escolher ou ter os cuidados básicos para que a senha se torne à chave da sua segurança (POMPERMAYER JUNIOR, 2002).

A integridade relacionada à Internet está vinculada nas senhas utilizadas como uma pessoa está aos seus documentos, e ao perdê-los ou ter sua senha desvendada está exposto a varias vulnerabilidades (UFPEL, 2009).

Grande parte dos usuários acredita que as senhas são desvendadas por uma falha no sistema, mas na verdade não é isso que acontece, a maioria dos ataques e invasões ocorrem por ter uma senha mal elaborada.

A criação de uma senha segura depende do bom senso do seu criador, levando em conta que há alguns anos uma senha segura era composta por seis dígitos, mas essa realidade

[5] Modo que pode ser ativado na placa de rede que permite que sejam capturados todos os pacotes que trafegam na rede, neste modo o navegação na Internet não é permitida.

mudou, com auxilio da evolução tecnológica muitas técnicas foram desenvolvidas e esse tipo de senha pode ser desvendada em poucos segundos, a indicação feita hoje é que as senhas tenham no mínimo 8 caracteres (ALBERTO, 2006).

Segundo Alberto (2006) senhas que realmente são chaves de segurança somente são obtidas com a combinação de alguns fatores citados a seguir:

a) Não utilizar dados pessoais como seu nome ou de parentes, datas de nascimento de integrantes da família, mesmo que haja combinações entre as informações ou pequenas alterações na escrita;
b) Dados que possam ser desvendados facilmente incluindo endereços, placa do carro, número de documentos também são alvo fácil;
c) Nunca anote senhas em papéis, agendas ou algum lugar que outras pessoas possam ter acesso, o melhor lugar para armazenar senhas sem nenhum risco é na sua memória;
d) Senhas criadas a partir de palavras existentes em dicionários, tanto nacionais quanto estrangeiros podem ser desvendadas com ataques de dicionário;
e) Não utilizar senhas com apenas um tipo de caractere, chaves fortes devem conter letras maiúsculas e minúsculas, caracteres especiais e números;
f) Uma senha deve combinar no mínimo 8 caracteres;
g) Nunca utilizar seqüências de dígitos do teclado, como, “qwe123” ou “qwerty”, nem seqüência de números “123456”;
h) Não utilize a mesma senha em lugares diferentes, pois se a senha for desvendada apenas um local será atacado;
i) A troca das senhas deve acontecer regularmente, no período de aproximadamente 3 meses;

j) Muito cuidado ao digitar uma senha em público, muitos invasores usam esse método para coletar senhas.

Obedecendo a essas regras e usando algumas técnicas que serão descritas a seguir a senha criada terá um nível de segurança considerado razoável, podendo assim aumentar a segurança das informações. Segundo Arantes (2006) essas técnicas têm como função a criação de senhas fortes e que o usuário possa lembrá-la com facilidade.

6.3.1 Senhas Baseadas na Geometria do Teclado

Esse método de criação de senhas tem uma grande aceitação dos usuários, existem pessoas que já formam suas senhas utilizando essa técnica há anos. A criação é bem simples, basta olhar para o teclado e imaginar uma forma geométrica qualquer, sempre evitando linhas retas, e apertar as teclas que equivalem às linhas da figura. Várias formas podem ser criadas, isso só depende da criatividade do usuário (triângulos, letras em tamanho grande, ziguezagues).

Porém deve-se tomar muito cuidado para que ninguém saiba que sua senha está baseada nessa técnica, pois por meio de várias tentativas ela poderá ser desvendada, o cuidado na hora da digitação é fundamental.

6.3.2 Senhas Pronunciáveis

As senhas pronunciáveis são palavras escritas com a mistura de vogais e consoantes, criando uma palavra que possa ser pronunciada, mas que não existe em nenhum dicionário. Também pode-se misturar as letras com números e caracteres especiais, como "T3m1@viaono@r!"

Várias chaves podem ser formadas, a indicação é que sejam grandes para que sejam resistentes a ataques de força bruta, e que realmente não existam para que não possam ser desvendadas por ataques de dicionário.

6.3.3 Senhas Derivadas de Frases

Essa técnica constrói senhas por meio de frases conhecidas, ou textos que podem ser lembrados de forma fácil, como uma poesia ou em trecho de uma música famosa. A senha é formada por meio de alguma letra de cada palavra, como por exemplo, “Debaixo dos caracóis dos seus cabelos, Uma história pra contar, De um mundo tão distante.”, ficaria “Ddcdsc,Uhpc,Dumtd.”. Neste caso a conservação das vírgulas e pontos dificultam ainda mais a quebra das senhas.

A vantagem desta técnica é que senhas bem diferentes são criadas, podendo ser extensas e lembradas facilmente.

6.3.4 Palavras em Conjunto

Esse tipo de senha é criada a partir da junção de palavras existentes, como “cachorro+jeep+passarinho”, gerando a seguinte senha, “cachojeessarinho”, ou outras combinações que sejam fáceis de lembrar. Misturar letras maiúsculas e minúsculas, números e caracteres especais também é uma opção válida.

6.3.5 Chaves Significativas

Como foi dito anteriormente uma chave não deve ser composta por datas nem números que estejam diretamente ligadas ao usuário, mas alguma data ou combinação de

números que seja significante e não foi divulgada em nenhum momento nem está documentada em nenhum lugar pode ser utilizada, desde que alcance um número razoável de caracteres, por exemplo, a data em que comprou seu primeiro carro, ficaria "01101999carro1", lembrando que informações sobre a data podem ser acrescentadas à senha para que aumentar ainda mais a relevância.

6.3.6 Caracteres "ALT"

Senhas fortes podem ser criadas com o auxílio de caracteres criados pressionando a tecla "ALT" juntamente com uma outra tecla, como por exemplo, pressionando a tecla "ALT" junto com a tecla "c" obtemos o caractere "©".

Esses caracteres podem tornar uma senha bem mais complexa, já que a maioria dos softwares responsáveis por realizar quebra de senhas não se preocupa muito com esses caracteres, geralmente estão preparados para realizar quebras que incluem letras, números e caracteres especiais que estão amostra no teclado.

6.3.7 Senhas Geradas por Programas

Buscando auxiliar os usuários na criação de senhas seguras, vários *softwares* foram desenvolvidos para gerar senhas de forma aleatória, a desvantagem deste tipo de *software* é que as senhas geradas não tem nenhuma ligação com o usuário podendo ser esquecidas facilmente.

Alguns programas serão listados abaixo:

a) MakePassword: este gerador de senhas pode ser acessado no *link* "http://maord.com/", e disponibiliza algumas preferências, como, tamanho da

senha, quantidade de senhas geradas, quais caracteres utilizados, caracteres que não devem ser utilizados, intensidade da senha e forma da exibição da senha. Imagens do gerador sendo utilizado podem ser vistas na Figura 18 e 19;

Figura 18. MakePassword gerando senha

Figura 19. Senhas geradas pelo MakePassoword

b) Atory Password Generator: esse software gera senhas aleatórias, de acordo com a preferência do usuário, com a inclusão de números, letras maiúsculas, minúsculas, e outros símbolos, e especificando a quantidade de caracteres.

A Figura 20 mostra o Atory Password Generator em execução;

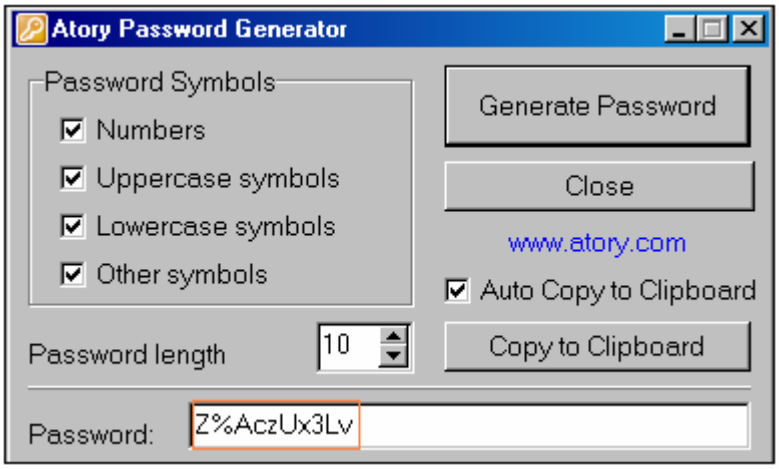


Figura 20. Gerando senhas com o Atory Password Generator

c) XPassGen 0.5: este é um dos geradores com mais opções, permitindo que sejam escolhidos caracteres entre maiúsculos, minúsculos, números, símbolos, caracteres que não devem ser utilizados, e entre incluir e excluir caracteres personalizados, também podem ser selecionados o número de caracteres, a quantidade de senhas, e a intensidade. O *software* em execução pode ser visto na Figura 21;

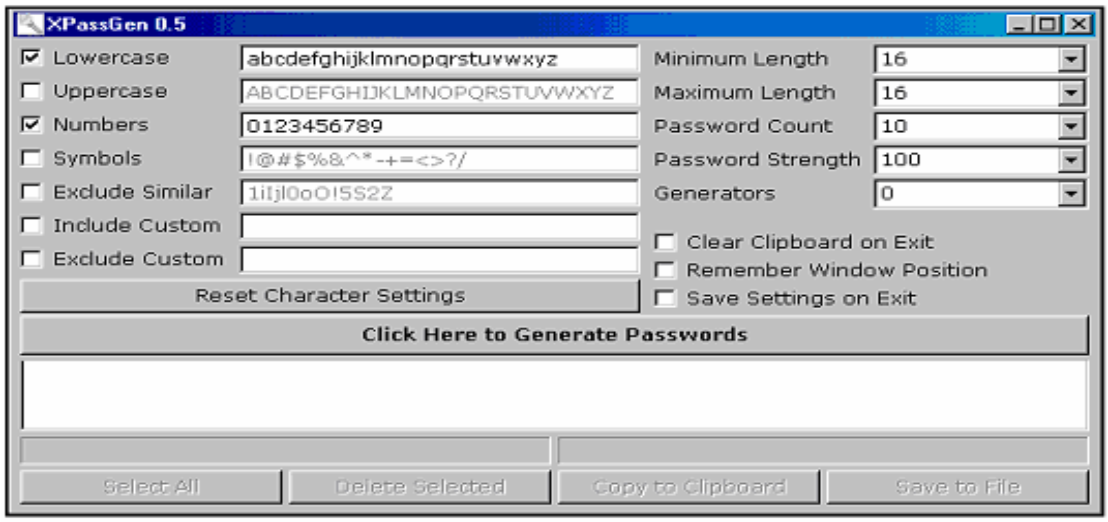


Figura 21. Estabelecendo parâmetros para geração de senhas no XPassGen 0.5

Seguindo as especificações feitas acima a senha pode ser gerada como mostra a Figura 22.

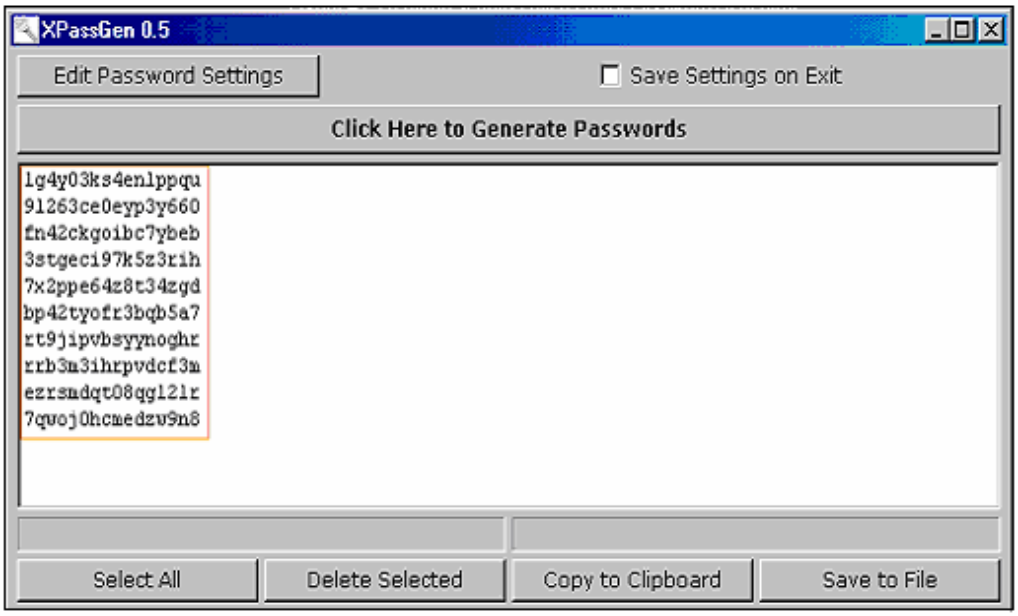


Figura 22. Chaves geradas pelo XPassGen 0.5

d) SoftFuse Password Generator Free 2.1: da mesma forma que os *softwares* anteriores, este gerador também forma chaves seguindo algumas preferências do usuário, a Figura 23 mostra o programa em execução.

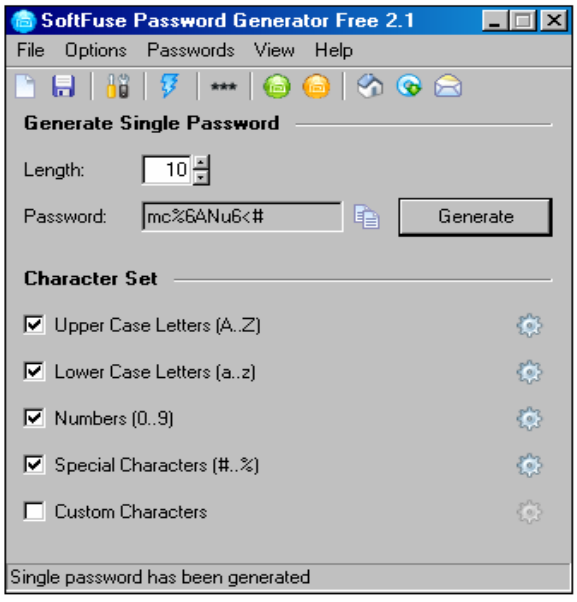


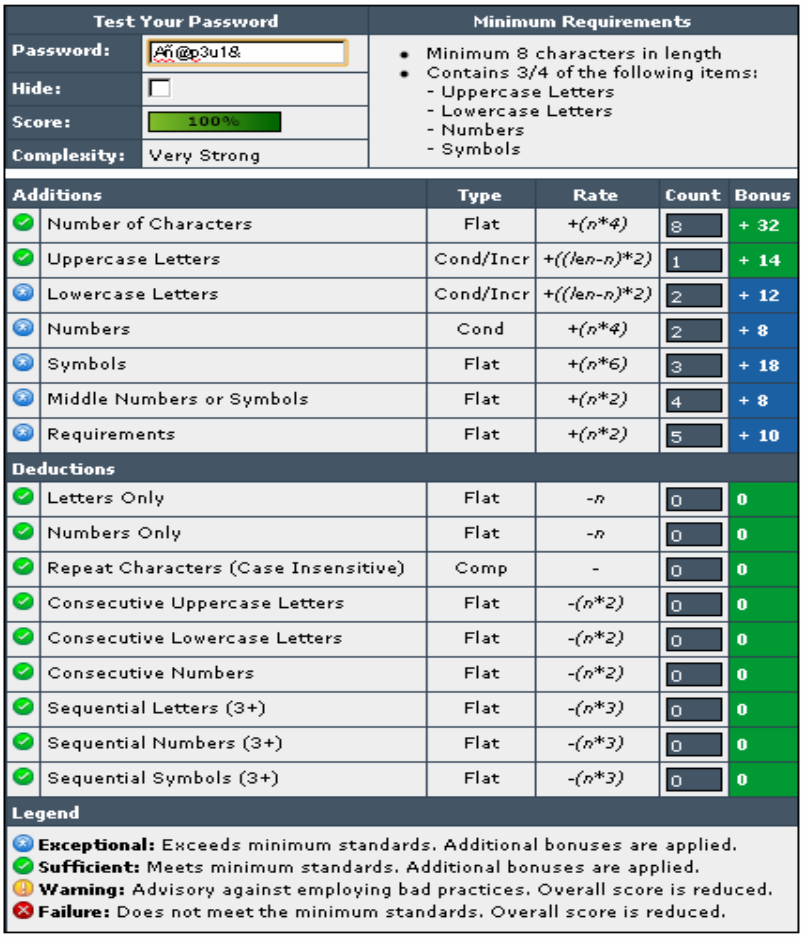
Figura 23. SoftFuse Password Generator Free 2.1 em execução

6.3.8 Complexidade das Senhas

Alguns programas foram criados para auxiliar o usuário na seleção das suas senhas, o PASSWORD METER é um deles, ele é capaz de classificar a sua senha conforme a intensidade durante a digitação.

A força da senha é avaliada de acordo com cada caractere agrupado instantaneamente após a digitação, fornecendo também uma dica para que a senha possa ser melhorada, tendo uma atenção para evitar senhas criadas por vícios de digitação.

Esse programa não tem um resultado infalível, já que não existe uma senha completamente segura, mas visa melhorar o desempenho da segurança por meio da chave escolhida. A Figura 24 mostra o PASSWORD METER em execução.



Test Your Password		Minimum Requirements
Password:	Aí@p3u1&	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

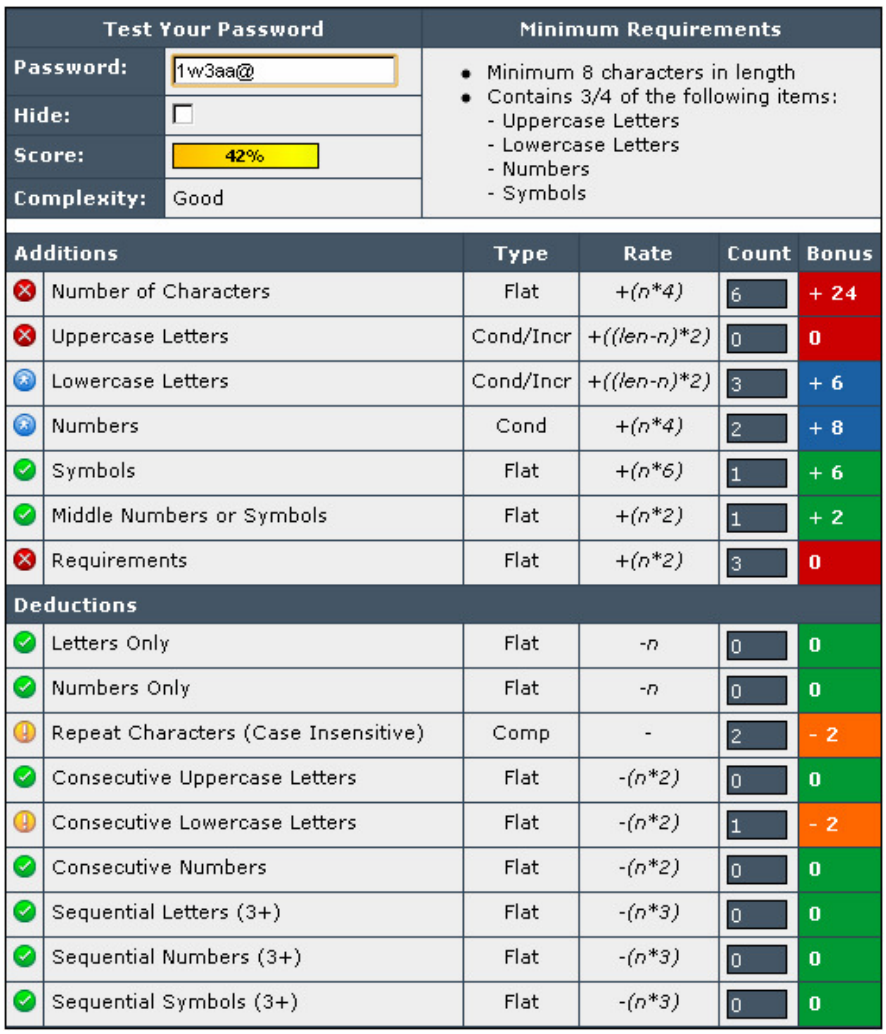
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 12
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Figura 24. PASSWORD METER fazendo análise da senha escolhida

Na Figura 24 pode-se observar a análise da senha inserida que é “Añ@p3u1&”, onde o resultado é de uma senha é excelente. Já na Figura 25 o resultado não foi positivo, o software avaliou a senha “1w3aa@” com apenas 42% de segurança.



Test Your Password		Minimum Requirements
Password:	1w3aa@	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	42%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 6
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Figura 25. PASSWORD METER fazendo análise da senha escolhida

Com a análise da senha algumas melhorias foram indicadas para alcançar um nível maior de segurança, neste caso são indicadas às utilizações de mais caracteres, utilizando letras maiúsculas, e separando as minúsculas digitadas em seqüência.

Este analisador de senhas pode ser acessado no endereço “http://www.passwordmeter.com/”, é um programa gratuito que pode ajudar muito na escolha de uma senha forte.

6.4 DETECTANDO AS REDES COM O KISMET

O Kismet é uma ferramenta de monitoramento de redes com caráter passivo, que pode ser utilizada para ataque ou para defesa. É considerada uma das ferramentas mais completas e eficazes das disponíveis gratuitamente. Pode ser utilizada em sistemas operacionais Linux e Windows.

Sua instalação no Linux Ubuntu pode ser realizada por meio do comando inserido no terminal “apt-get install Kismet” ou pelo Synaptic, que já traz todos os pacotes necessários para uma execução com sucesso.

Após realizada a instalação o primeiro passo a ser dado é entrar no arquivo de configuração do Kismet e alterar os dados relacionados a placa de rede e *driver* utilizado por ela. O caminho do pacote a ser alterado é “/etc/Kismet/Kismet.conf”, ele deve ser acessado via terminal no modo super usuário (root).

Com o arquivo já aberto deve-se substituir a linha que contém a seguinte informação, “source = none, none, addme”, por source = driver da placa de rede, a interface utilizada, e o apelido escolhido para identificar a placa durante a varedura. Neste caso a linha ficará com as seguintes informações, source = rt8180, wlan0, atheros.

Para que o Kismet possa ser executado sua placa deve estar em modo monitor, para isso deve-se utilizar o terminal e inserir os seguintes códigos:

a) ifconfig <nome da interface> down;

b) iwconfig <nome da interface> mode monitor.

E para utilizar a interface após encerrar o Kismet deve-se utilizar o seguinte código:

a) ifconfig <nome da interface> down;

b) iwconfig <nome da interface> mode manager;

c) ifconfig <nome da interface> up.

A execução do Kismet é realizada por meio do terminal no modo super usuário (root), inserindo o código Kismet, em seguida uma janela abrirá como mostra a Figura 26.

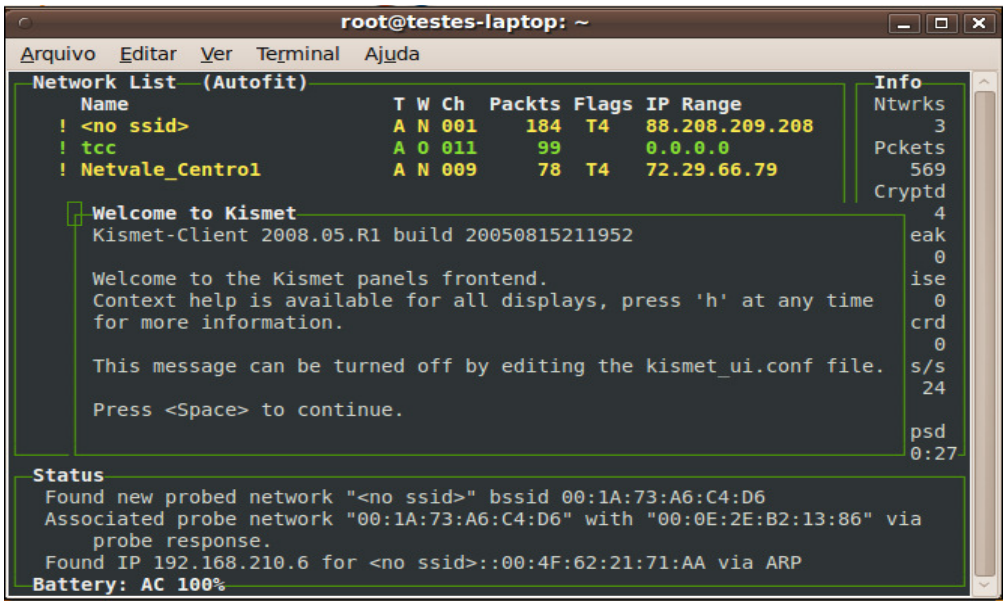


Figura 26. Tela inicial do Kismet

A captura dos pacotes começa automaticamente após a execução do programa, a partir deste momento podem ser observados algumas informações importantes sobre a rede, como, nome da rede, canal, se existe segurança habilitada e o número de pacotes capturados.

Os pacotes capturados são salvos com a data do dia da captura e seguidos pelo número do pacote que é gerado na seqüência iniciando em 1 a cada dia, sua extensão é .dump, por exemplo, “Kismet-may-05-2010-2.dump”, e se preservada a configuração inicial podem ser encontrados na pasta “/var/log/Kismet”.

Para que uma rede com segurança WEP ou WPA seja invadida é necessário que sua senha seja descoberta, para que isso aconteça utilizando os pacotes capturados pelo Kismet é necessário utilizar um programa que leia esse tipo de arquivo, como o John the Ripper entre outros.

Uma amostra de quebra de senhas poderá ser observado a seguir com a utilização do Aircrack-ng e seus componentes.

6.5 UTILIZANDO O AIRCRACK-NG PARA QUEBRA DE CHAVES

O Aircrack-ng é um do programas mais utilizados para captura e quebra de chaves por conter um grupo de ferramentas que juntas se completam, tornando mais fácil a execução desde a captura até a quebra das senhas. A instalação do pacote Aircrack-ng pode ser feita por meio do terminal com o código “apt-get install Aircrack-ng”, ou pelo Synaptic, das duas formas a instalação é feita de forma completa, sem a necessidade de acrescentar mais nenhum pacote.

6.5.1 Iniciando o Airmon-ng

Após a instalação do Aircrack-ng, o primeiro passo é colocar a sua interface em modo monitor, como mostra a Figura 27, isso pode ser feito com o Airmon-ng, por meio da inserção do seguinte código no terminal em modo super usuário (root).

a) airmon-ng stop <nome da interface>: para assegurar que o modo monitor já não está ativo;

b) airmon-ng start <nome da interface>: para ativar o modo monitor.

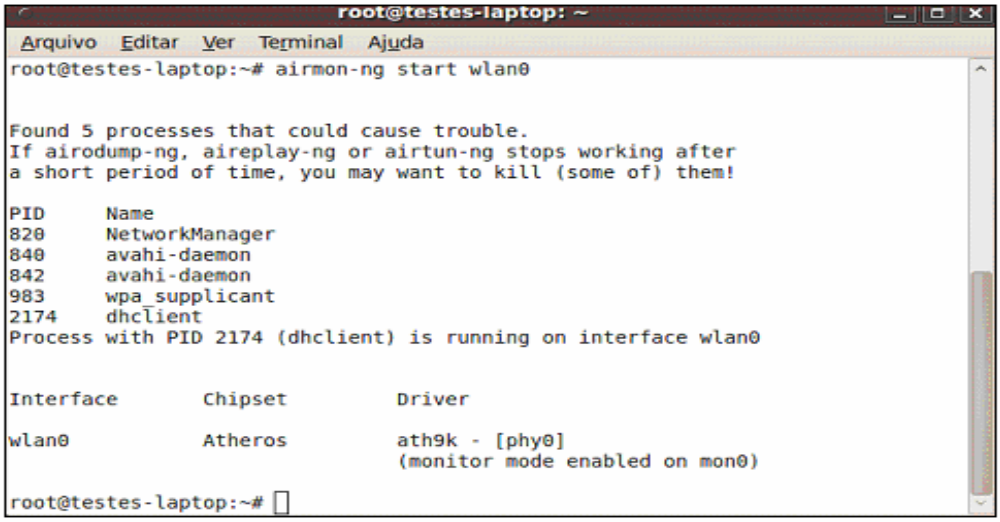


Figura 27. Airmon-ng ativando o modo monitor

Este procedimento deve ser repetido sempre antes de executar o Airodump-ng para garantir o sucesso da captura.

6.5.2 Capturando Pacotes com o Airodump-ng

A captura dos pacotes é realizada com o Airodump-ng, este programa tem basicamente as mesmas características do Kismet, mostrado anteriormente, sua execução é feita por meio do terminal, após colocar a interface em modo monitor, por meio do seguinte código, “airodump-ng --channel 6 – w nomedopacote.cap mon0”, onde “-- channel” filtra a busca de acordo com o canal, “- w” indica o nome do arquivo e o seu formato e “mon0” representa o nome da interface.

6.5.3 Quebrando chaves com o Aircrack-ng

O Aircrack-ng é o responsável pela leitura dos pacotes capturados, e assim realizar a quebra das chaves. Também é executado por meio do terminal, após ser realizado o seguinte comando, “aircrack-ng nomedopacote*.cap”, onde o “*” é utilizado para agrupar as capturas realizadas com o mesmo nome.

6.6 DESVENDANDO CHAVES WEP, WPA, WPA2 COM AIRCRACK-NG

No decorrer do trabalho foram descritas várias vulnerabilidades, e métodos de defesa, entre eles serão analisados a importância das senhas e a configuração dos *Access Points*, para isso a intensidade da segurança que os protocolos WEP e WPA podem nos proporcionar diante de um ataque realizado pelo Aircrack-ng será analisada.

6.6.1 Segurança com o Protocolo WEP 64 bits

Nesta primeira análise o protocolo a ser testado será o WEP de 64 bits. Este protocolo aceita combinações de senhas de apenas cinco caracteres, nestes testes foram utilizadas três senhas, uma considerada fraca, contendo apenas números em seqüência, iniciando em um, outra composta por letras, números e caracteres especiais e a última gerada por *software*.

As opções de protocolo e senhas são realizadas no AP como mostra a Figura 28.

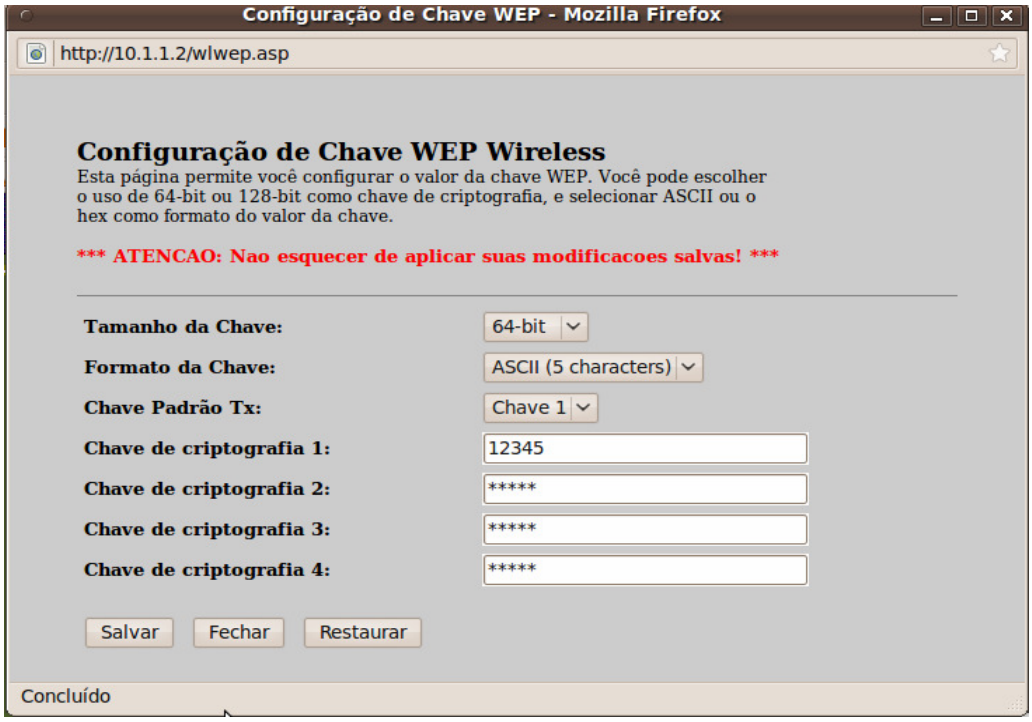


Figura 28. Configurando a chave WEP no AP

Após selecionar nos campos de configuração do AP o protocolo WEP de 64 bits, deve-se inserir a senha para aumentar a segurança da rede, neste primeiro teste a senha escolhida foi “12345”. O SSID da rede e o canal utilizado também podem ser escolhidos, como mostra a Figura 29.

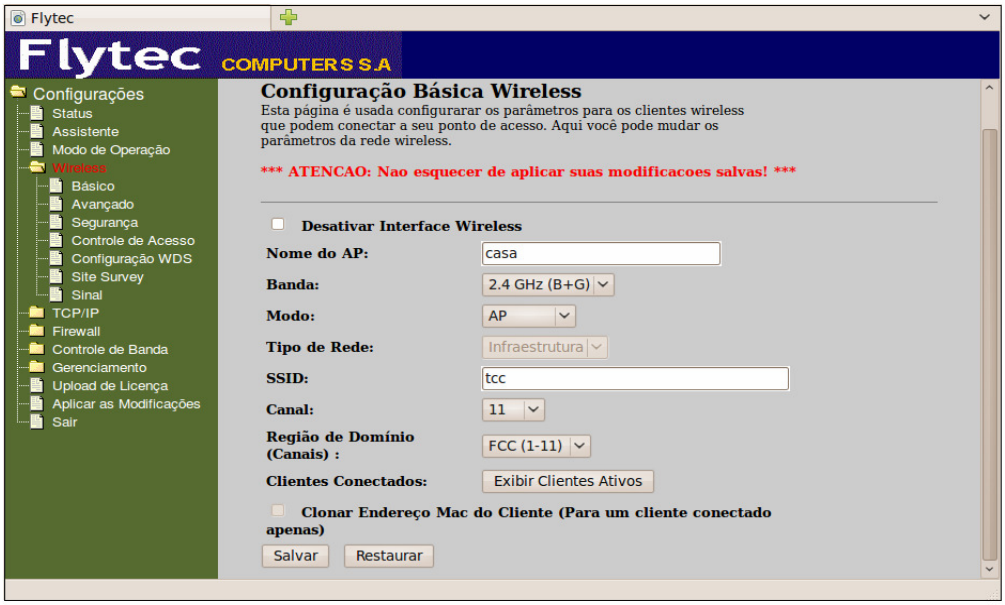


Ilustração 29. Configurando a canal e o SSID

As informações da rede como mostra a Figura 30, são obtidas com o comando "iwlist scan" inserido no terminal. Com esse comando informações importantes para captura dos pacotes podem ser visualizadas.

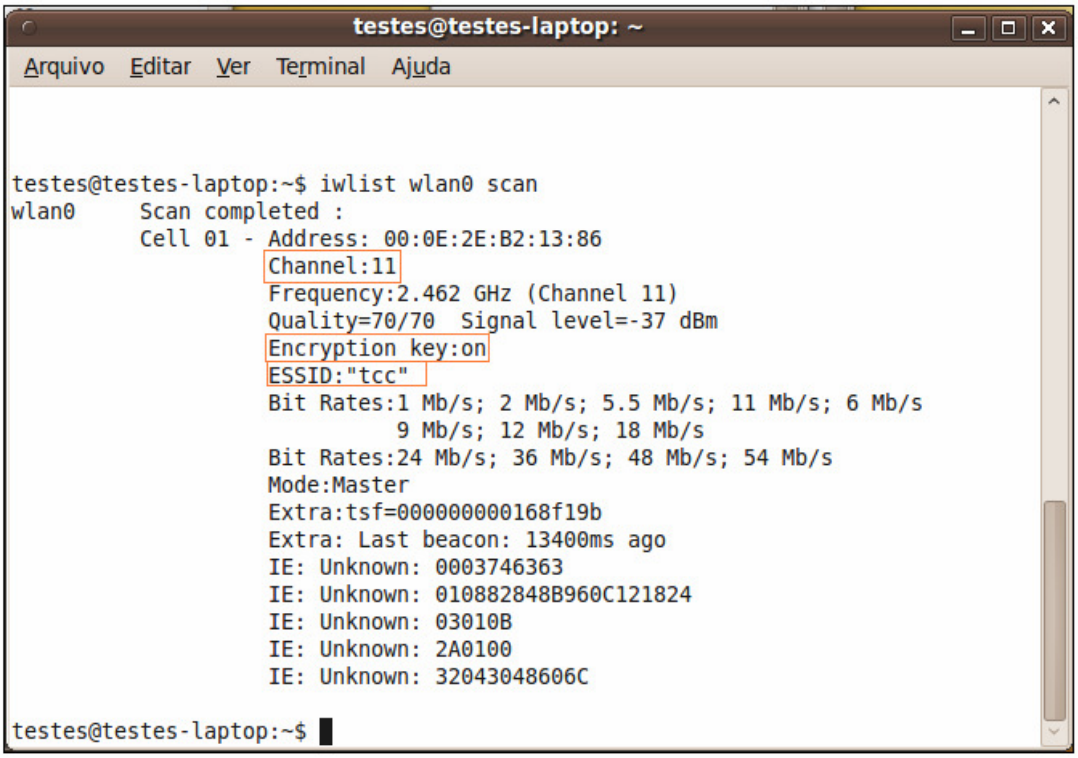


Figura 30. Informações da rede

Com todas as informações necessárias obtidas, e após colocar a interface em modo monitor, a captura é iniciada com o comando “airodump-ng --channel 11 –w wep64fraca.cap mon0”, onde “--channel” seleciona o canal onde a busca deve ser centralizada, “-w” especifica o nome e a extensão escolhidos para a captura e “mon0” a interface. A Figura 31 mostra a captura realizada.

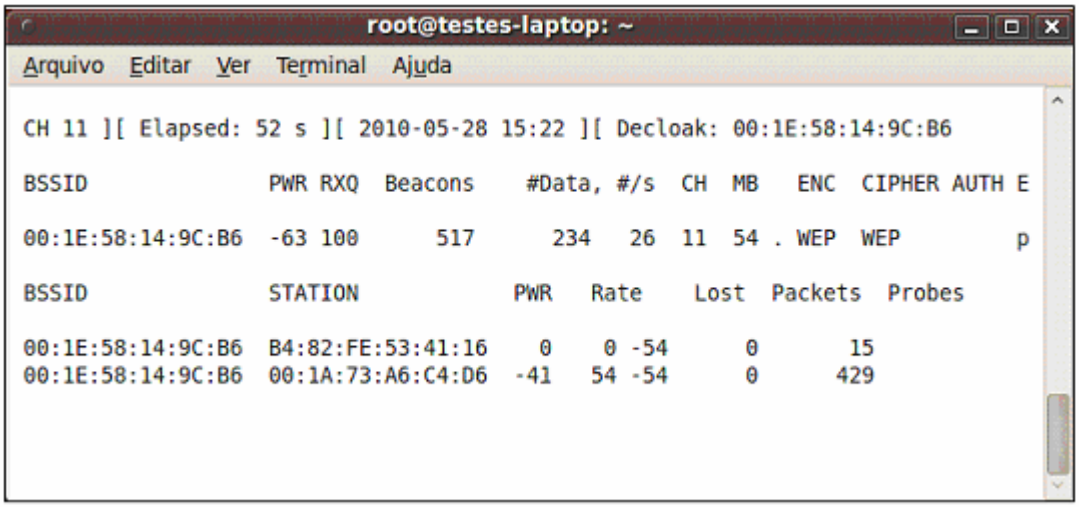


Figura 31. Captura de pacotes WEP 64 bits

Devem ser capturados cerca de 25.000 pacotes para que uma chave WEP de 64 bits possa ser descoberta. O comando “aircrack-ng wep64fraca.cap” inicia o Aircrack-ng que é o responsável pela quebra da chave. Neste caso após analisar 30.496 IVs, testando 102 chaves durante 4 segundos foi desvendada a chave como mostra a Figura 32.

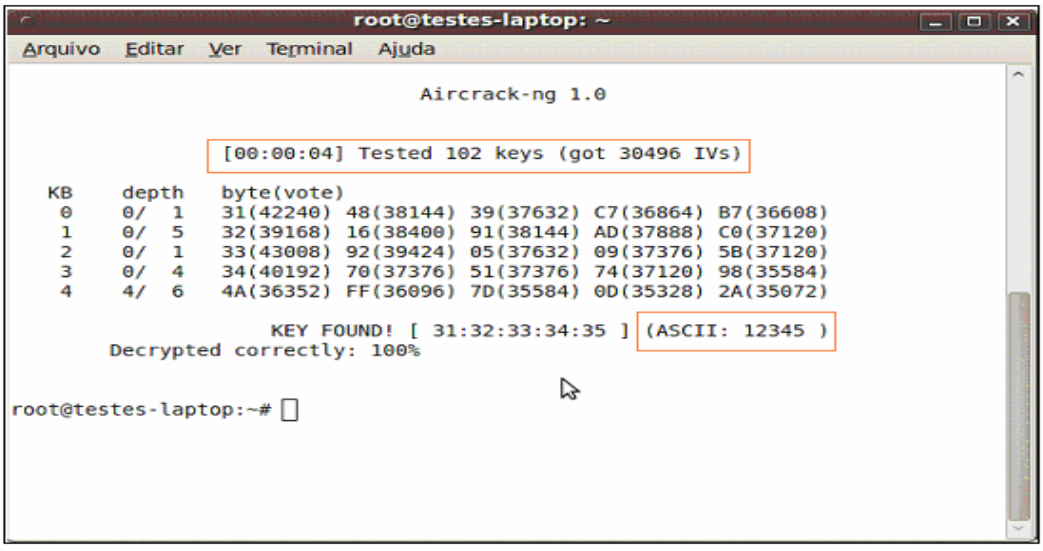


Figura 32. Quebra da senha WEP por força bruta

Observando a facilidade que o Aircrack-ng teve para quebrar uma senha com apenas caracteres numéricos uma nova tentativa foi realizada, mas agora com uma senha mais complexa, utilizando caracteres especiais, letras maiúsculas e minúsculas e números, mas como mostra a Figura 33, a senha foi quebrada com a mesma facilidade encontrada na tentativa anterior, como apenas 4 segundos a chave pode ser desvendada.

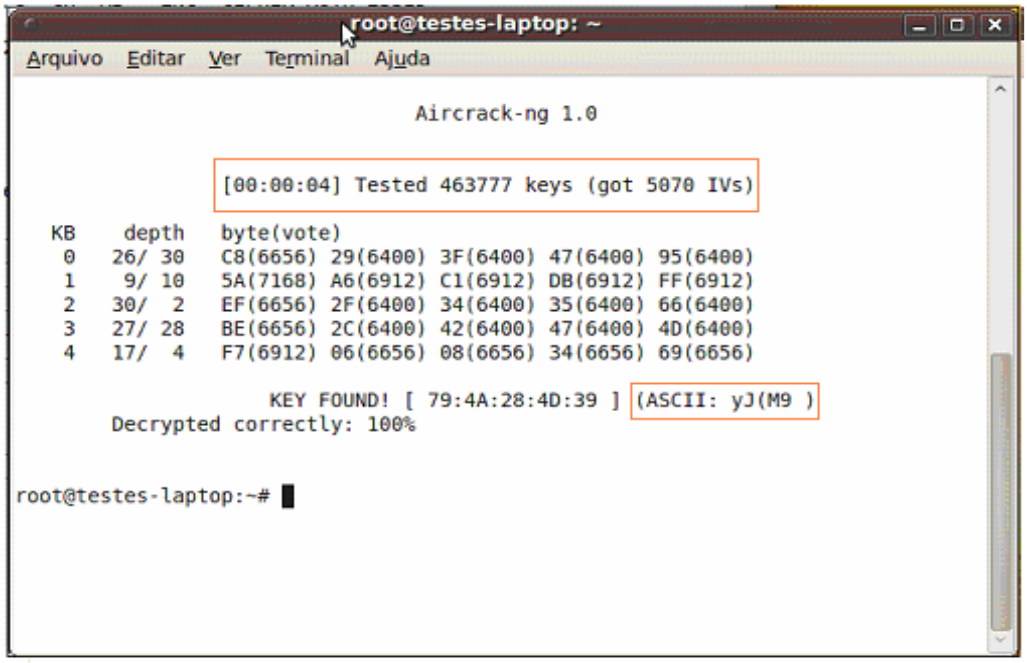


Figura 33. Quebra da senha WEP com caracteres especiais por força bruta

Para finalizar os testes com o WEP de 64 bits uma senha foi gerada pelo software SolftFuse, foram incluídos todos os tipos de caracteres disponibilizados pelo gerador formando a chave “A@q~2” como pode ser observado na Figura 34. Essa senha obteve um grau de segurança de 56%, que é considerado baixo, porém o mais alto alcançado levando em conta o baixo número de caracteres.

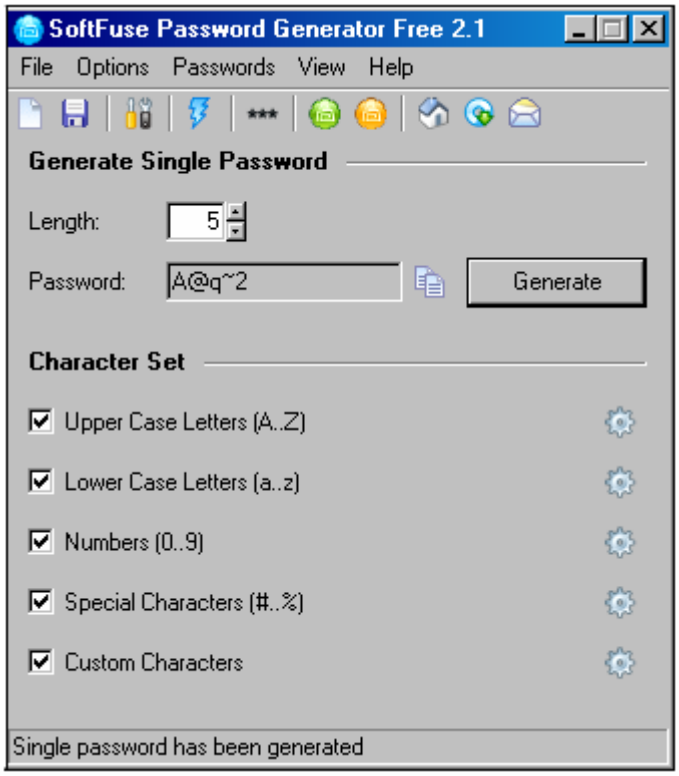


Figura 34. SoftFuse gerando senha com cinco caracteres

O procedimento realizado foi o mesmo das capturas anteriores, e após o Aircrack-ng testar 7.048 chaves em quatro segundos a chave pode ser desvendada, como pode ser observado na Figura 35.

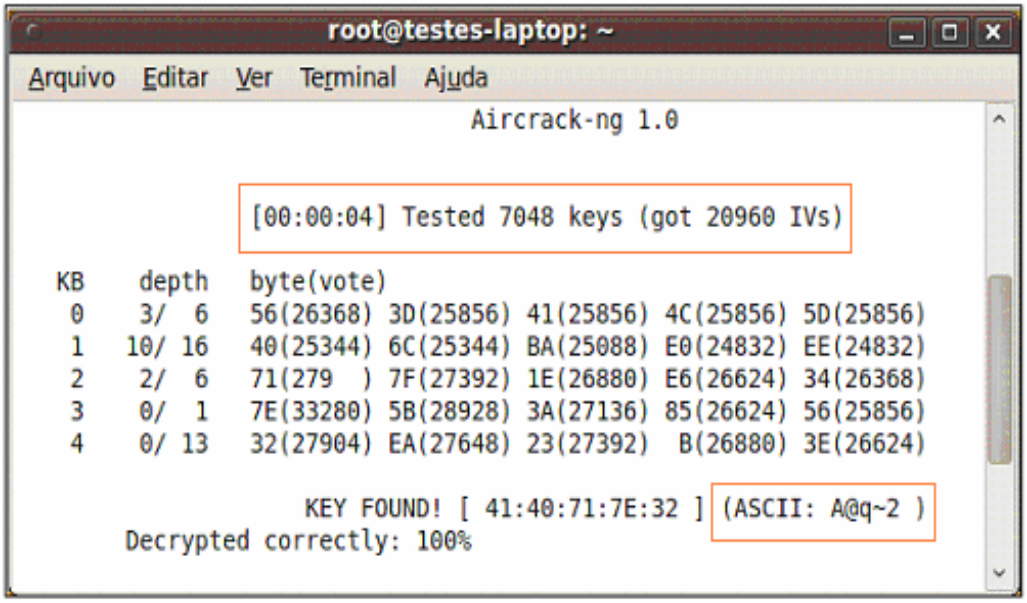


Figura 35. Quebra da senha WEP com caracteres especiais por força bruta

Com esses testes pode ser analisado que a segurança da chave WEP de 64 bits não é confiável, pois mesmo uma senha mais elaborada pode ser desvendada sem dificuldades.

6.6.2 Segurança com o Protocolo WEP 128 bits

Para esses testes foram realizadas as mesmas etapas dos testes anteriores com as chaves WEP de 64 bits. Foram criadas duas senhas uma mais fraca construída apenas por uma seqüência de números, que como vimos anteriormente não é um procedimento adequado para criação de senhas, e outra com caracteres especiais, letras e números, sendo que o protocolo WEP de 128 bits permite combinações de 13 caracteres para formação das senhas. Uma senha gerada pelo SoftFuse também foi utilizada.

As informações da rede são observadas na Figura 36, que foi obtida com o uso do comando “iwlist scan”.

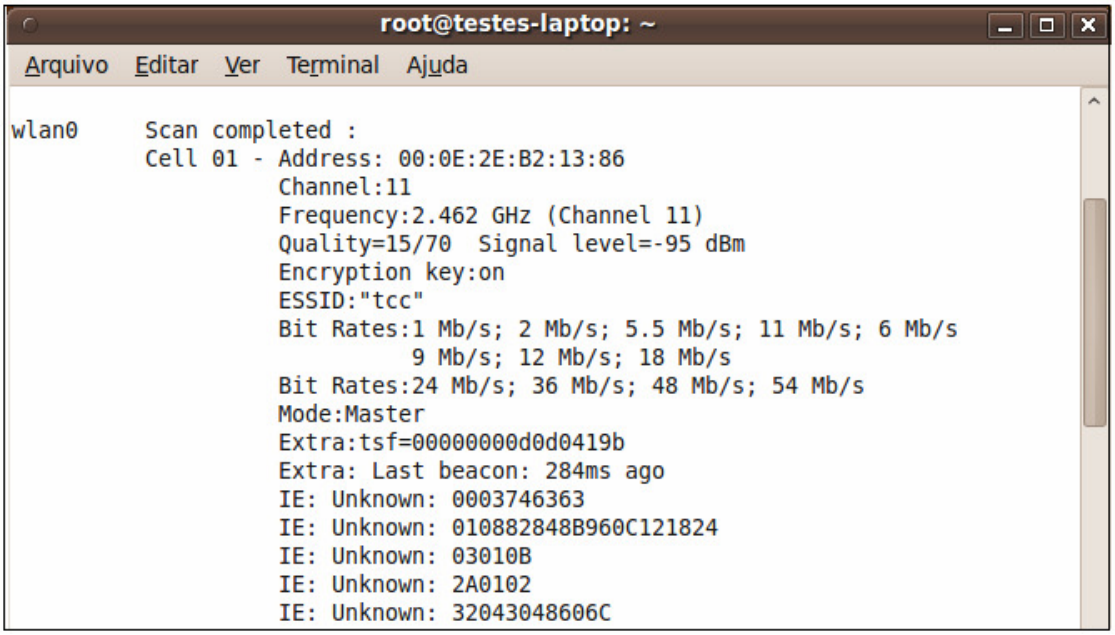


Figura 36. Informações da rede obtidas com o comando iwlist scan

Com os dados da rede analisados e a interface em modo monitor a captura pode ser iniciada com o comando “airodump-ng --channel 11 -w wep128fraca.cap mon0”, sendo

que para a quebra de senhas WEP de 128 bits é indicado que se capture cerca de 50.000 pacotes. Na Figura 37 a captura dos pacotes pode ser observada.

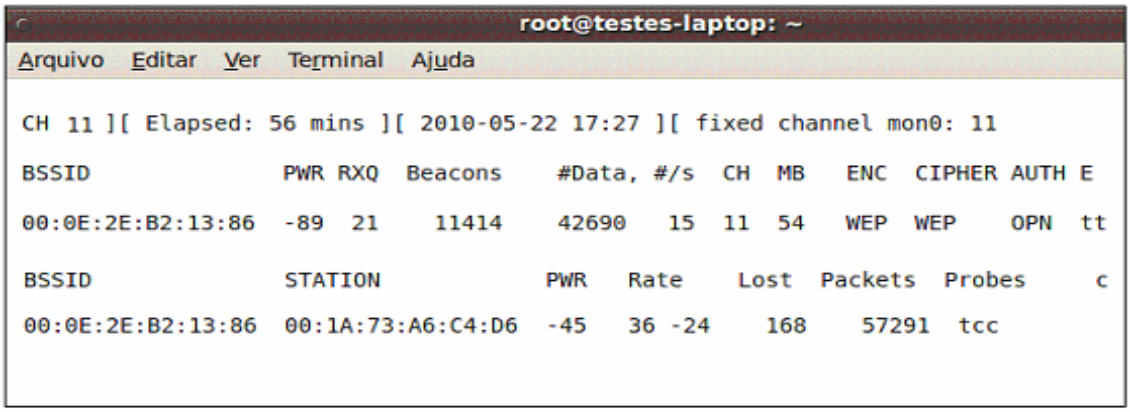


Figura 37. Captura dos pacotes WEP 128 bits

Após a captura realizada em 56 minutos a quebra pode ser iniciada. Por meio do comando “aircrack-ng wep128fraca.cap”, sendo que neste teste a senha utilizada é composta por apenas números em uma seqüência que inicia em 1 e segue até 11 (1234567891011), e sua quebra pode ser visualizada na Figura 38.

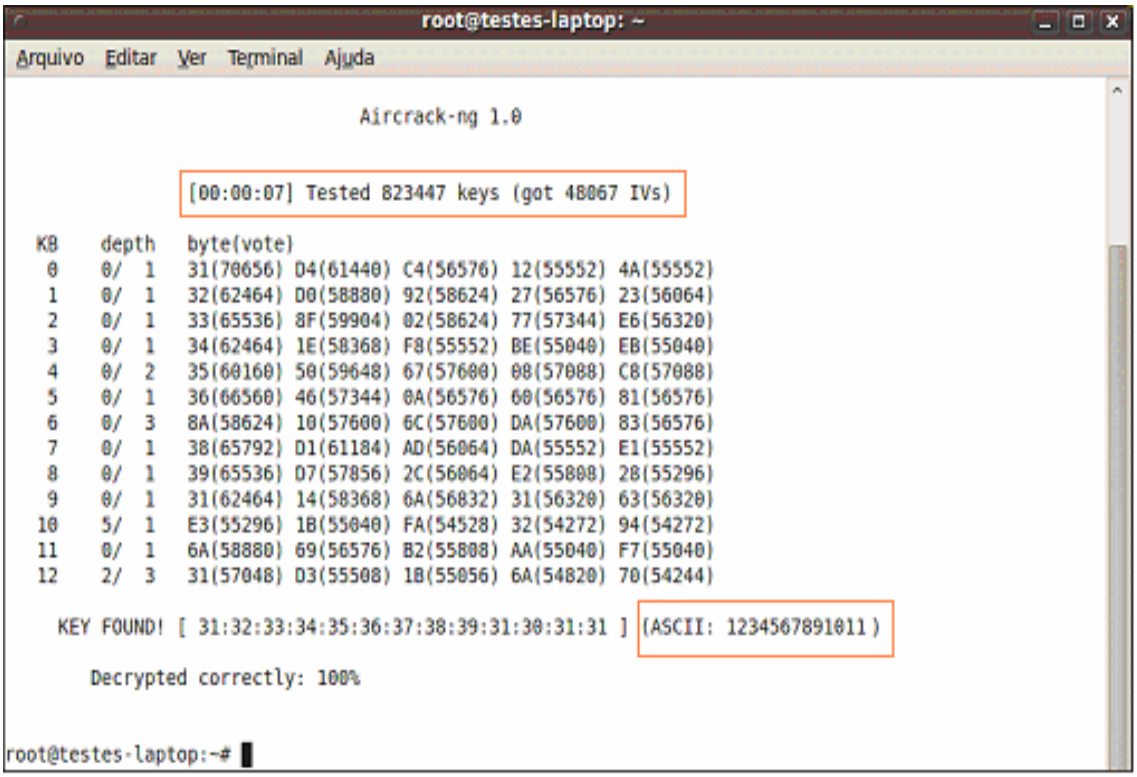


Figura 38. Quebra de senha WEP 128 bits por força bruta

A quebra da chave WEP de 128 bits foi realizada com a análise de 48.076 IVs, com o teste de 823.447 chaves em apenas 7 segundos. Para finalizar essa etapa de quebras será testada uma chave WEP de 128 bits composta por 13 caracteres contendo caracteres mais elaborados, formando a senha “An@p@^!?25Cl3”.

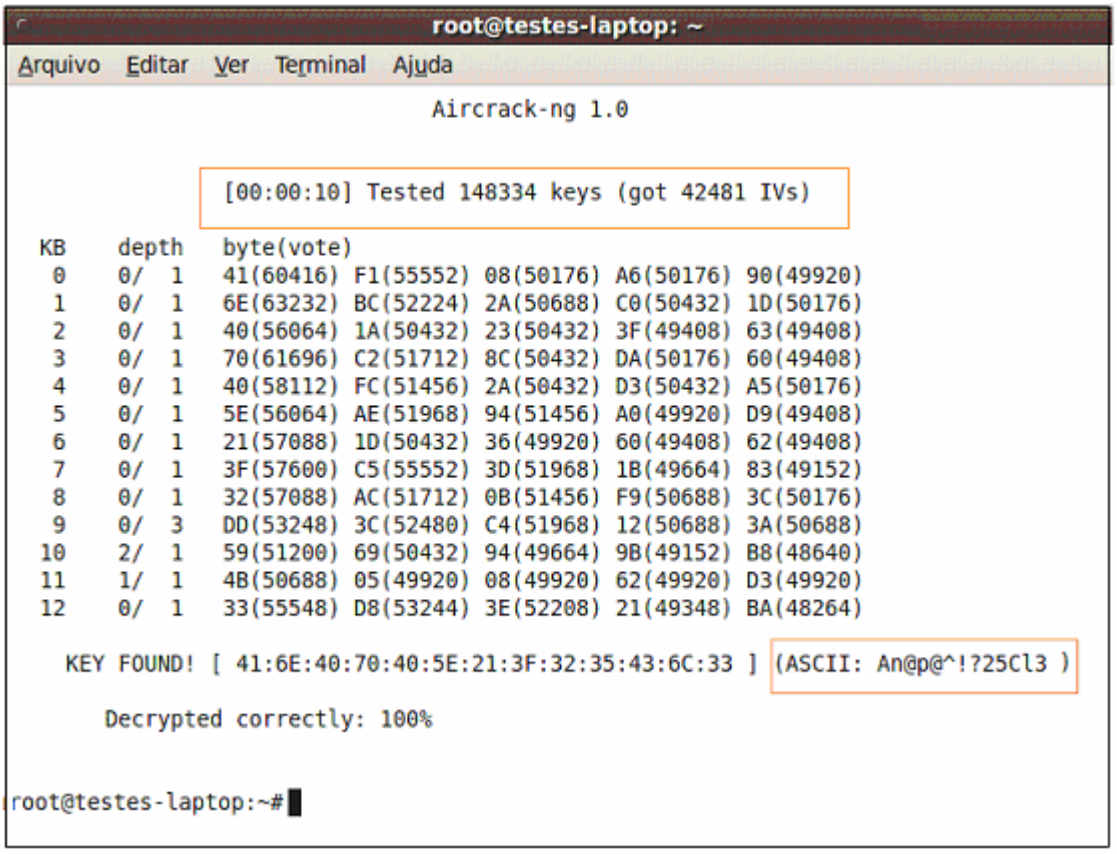


Figura 39. Desvendando senha WEP 128 bits por força bruta

Como mostra a Figura 39 a senha foi desvendada em apenas 10 segundos, sendo testados 42.481 IVs e 148.334 chaves. Da mesma forma que os testes anteriores a senha foi desvendada rapidamente sem nenhum problema.

Agora a seqüência a ser analisada foi gerada pelo software SoftFuse, e analisada pelo Password Metter, que classificou a chave como forte, com 100% de segurança, como pode ser observado na figura 40.

Test Your Password		Minimum Requirements
Password:	Ry&@74Nm[g*%y	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	13	+ 52
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 22
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 18
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	5	+ 30
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	1	- 2
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Figura 40. Analisando força da senha

O analisador classificou a senha com um alto nível de segurança, porém como pode ser observado na figura 41 a senha pode ser desvendada com uma analise 152.652 chaves em 52 segundos.

```
root@testes-laptop: ~
Arquivo  Editar  Ver  Terminal  Ajuda

                          Aircrack-ng 1.0

             [00:00:52] Tested 152652 keys (got 40755 IVs)

 KB    depth   byte(vote)
  0    0/  1   52(57344) 00(49152) B7(49152) 09(48128) 5D(47872)
  1    0/  1   79(60928) 06(48128) 82(48128) 9D(48128) 6C(47872)
  2    0/  2   B0(50944) F1(50176) 27(49152) 01(48896) 92(47872)
  3    0/  1   40(52736) 26(49920) BA(49152) FB(47872) E2(47616)
  4    0/  1   37(54784) 1C(51456) 67(49408) 12(47872) 7F(47872)
  5    0/  1   34(58880) 3B(48896) 0B(48384) 65(47872) 3F(47616)
  6    0/  1   4E(53504) 8C(49664) 1B(49408) F2(49408) 63(47360)
  7    0/  1   6D(62464) D6(49920) 84(49664) 2F(47872) 99(47616)
  8    0/  1   5B(50432) A3(49664) 9A(48896) 4F(47872) 7E(47616)
  9    0/  1   67(53248) EA(49152) E9(47872) F9(47872) F0(47616)
 10   12/  1   83(45824) 09(45568) 39(45568) 7D(45568) A7(45568)
 11    0/  1   2C(49920) 6C(49152) 1E(48128) 30(48128) AF(47872)
 12    0/  2   59(49456) 63(48700) E6(47644) C4(47260) 5C(47244)

   KEY FOUND! [ 52:79:26:40:37:34:4E:6D:5B:67:2A:25:59 ] (ASCII: Ry&@74Nm[g*%Y )

      Decrypted correctly: 100%
```

Figura 41. Desvendando senha WEP 128 bits por força bruta

Esses testes comprovam a fragilidade das redes que optam pela segurança do protocolo WEP, mesmo sendo ela composta por uma seqüência mais elaborada de caracteres não são fortes o suficiente para resistir a um ataque de força bruta.

6.6.3 Segurança com o Protocolo WPA

O protocolo WPA trás além de outras melhorias vistas no trabalho anteriormente, o aumento o tamanho da sua chave, que tem como critério no mínimo 8 caracteres, suportando combinações de 64 caracteres, tornando inviável a quebra da sua chave por força bruta.

Este primeiro teste utilizando o protocolo WPA utiliza a versão com *Temporal Key Protocol* (TKIP), este algoritmo tem como característica a alteração dinâmica da chave a cada novo envio do pacote.

Iniciando os testes foi alterado o SSID da rede buscando uma diferenciação dos testes anteriores, como pode ser visto na Figura 42.

Figura 42. Configuração do AP para testes com o WPA

A escolha da senha e do protocolo também foi realizada como mostra a Figura 43, neste teste a senha utilizada contém 10 caracteres, sendo composta por 5 letras minúsculas e cinco números, formando assim a combinação “teste12345”, essa é considerada uma senha de baixa intensidade, já que não possui caracteres especiais e nem letras maiúsculas e contém uma quantidade pequena de caracteres levando em conta a quantidade suportada.

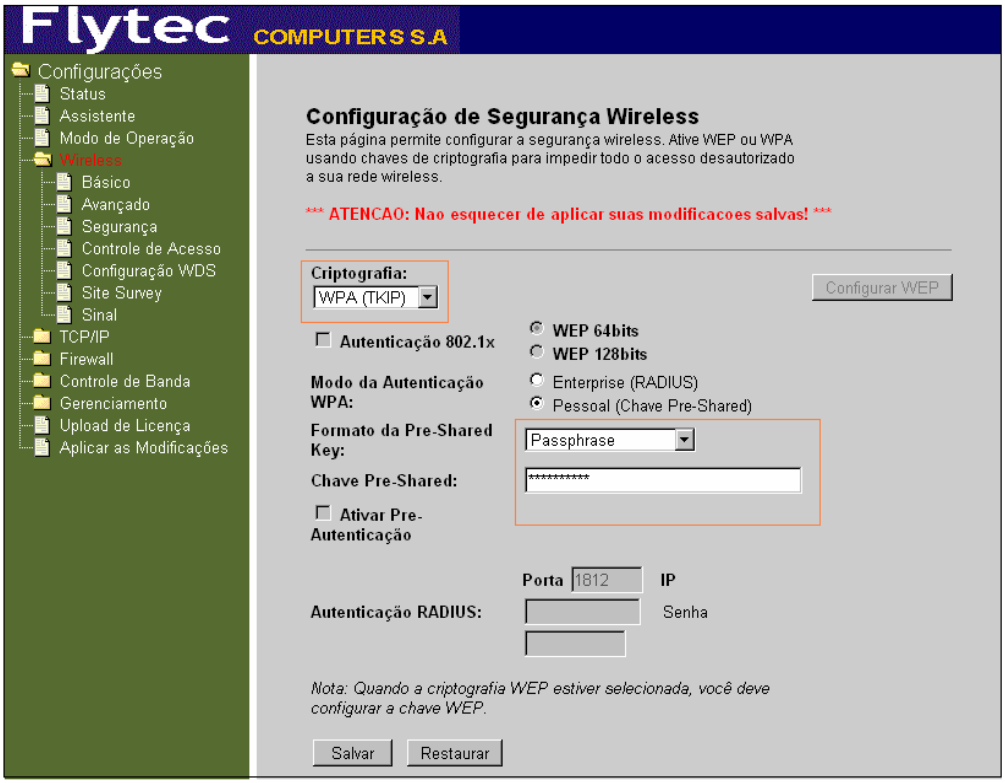


Figura 43. Escolhendo a senha WPA

Após obter as informações da rede por meio do comando “iwlist scan”, como mostra a Figura 44, pode ser iniciado os testes com o protocolo WPA, utilizando basicamente os mesmos passos do teste com o protocolo WEP.

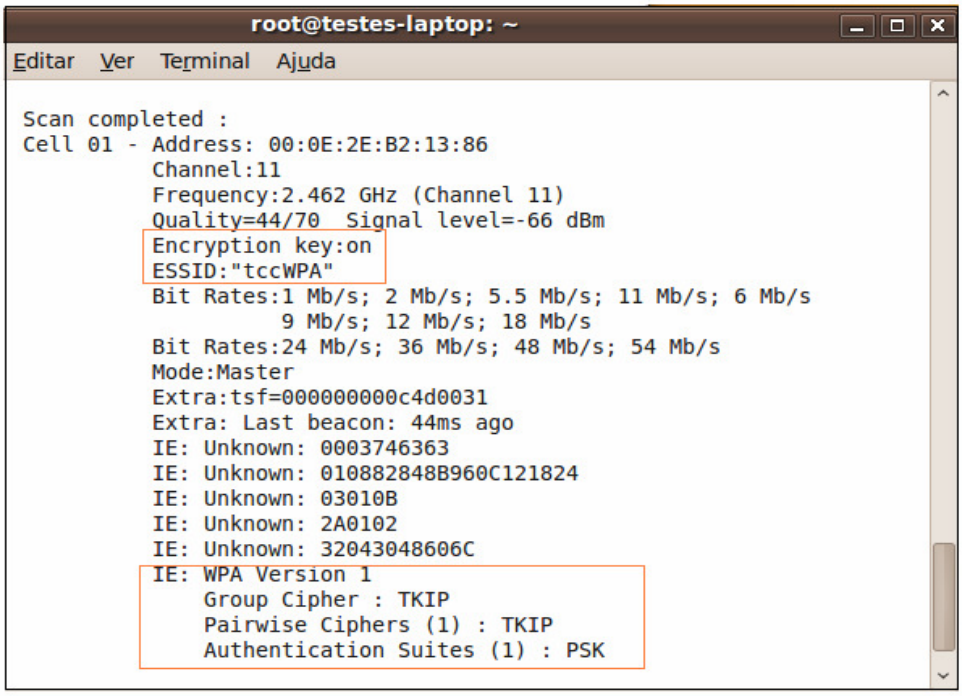


Figura 44. Informações da rede com o comando iw list scan

Primeiramente foi colocada a interface em modo monitor com o Airmon-ng, e após iniciada a captura com o Airodump-ng, por meio do comando “airodump-ng -- channel 11 -w wpatkipfraca.cap mon0”, onde o parâmetro “--channel” especifica o canal onde deve ser concentrar a captura, e “-w wpatkipfraca.cap” se refere ao nome do pacote onde os IVs serão armazenados.

Na seqüência é necessário capturar o *handshake*, ou “aperto de mão”, que é uma autenticação que garante a comunicação entre o computador e o AP, e onde está armazenada a criptografia utilizada na autenticação da rede, sem essa informação o Aircrack-ng não pode desvendar a chave WPA.

O *handshake* é obtido com a ajuda do Aireplay-ng, por meio do comando “aireplay-ng -0 5 -a MAC do AP -c MAC do cliente <interface>” inserido em outro terminal aberto, neste caso foi utilizado “aireplay-ng -0 5 -a 00:0E:2E:B2:13:84 - c 00:1A:73:A6:C4:D6 mon0”, assim um pacote de desconexão do usuário é enviado pelo

atacante para o AP, forçando o usuário a realizar uma nova autenticação para permanecer conectado, essa autenticação é armazenada nos pacotes capturados.

A Figura 45 mostra o Aireplay-ng em execução.

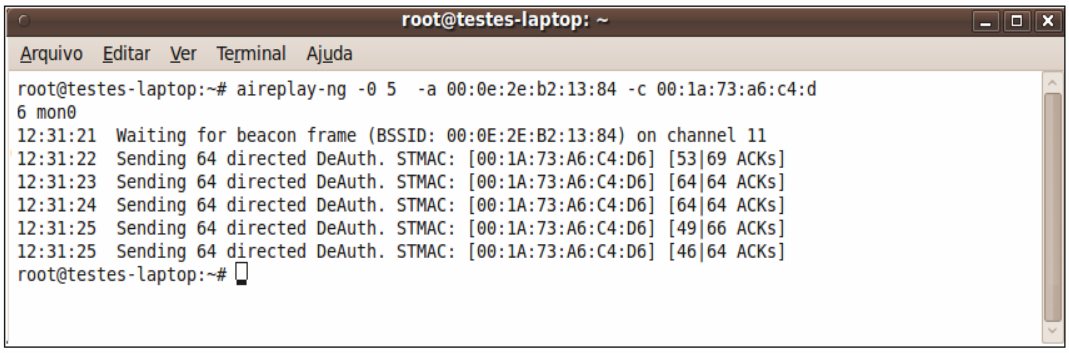


Figura 45. Aireplay-ng capturando o handshake

A Figura 46 mostra o WPA *handshake* já capturado, porém para que a quebra da chave aconteça é necessário capturar aproximadamente 50.000 pacotes.

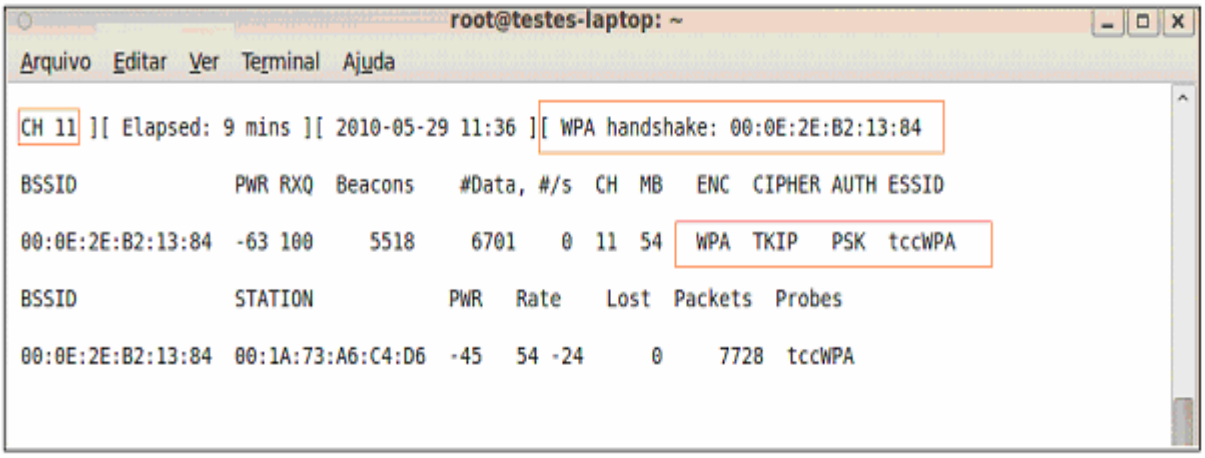


Figura 46. Captura dos pacotes já com as informações do handshake

Utilizando o comando "aircrack-ng -e tccWPA -w WORD1.LST wpatkipfraca.cap", onde o parâmetro "-e" especifica o ESSID da rede, "-w" o dicionário utilizado para auxiliar a quebra, e em seguida o nome do pacote que contém os IVs para realizar a quebra, a chave pode ser desvendada.

O dicionário utilizado é uma concatenação de vários pequenos dicionários contendo aproximadamente 50 MB, um deles pode ser encontrado no endereço,

“http://addagram.mytestbench.com/WORD.LST”, alguns outros podem ser encontrados no endereço “http://natura.di.uminho.pt/download/sources/Dictionaries/misc/wordlist/”.

Como mostra a Figura 47, foram testadas 225.392 chaves em um pouco mais de 3 minutos.

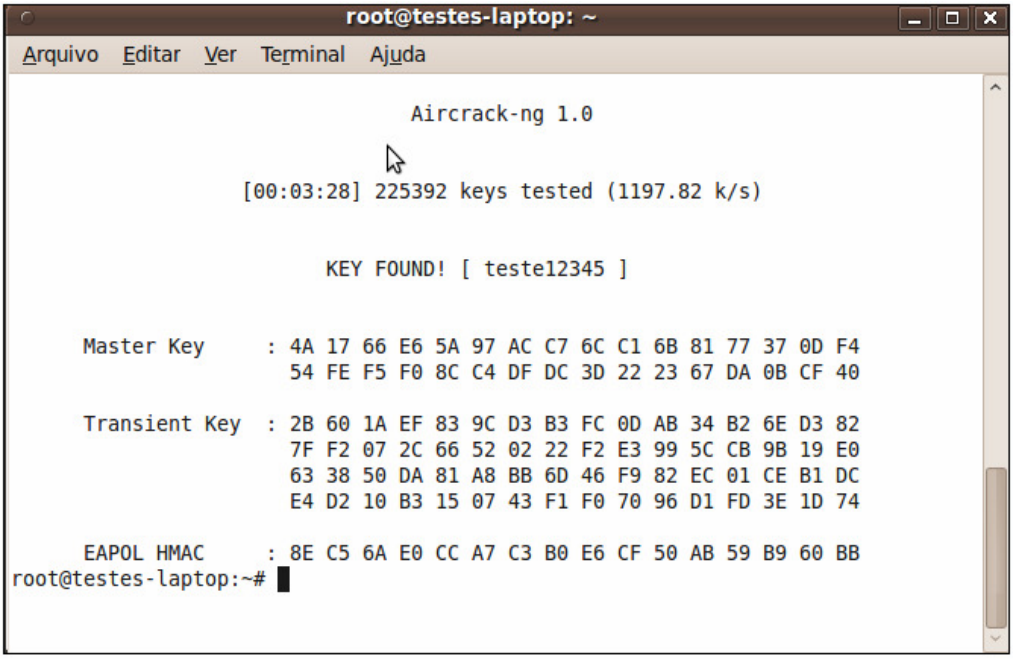


Figura 47. Quebra da chave WPA por meio de ataque de dicionário

Analisando a facilidade em que a senha foi desvendada, um novo teste foi realizado com os mesmos passos realizados anteriormente, porém com uma chave maior e com caracteres mais elaborados, composta por caracteres especiais, letras e números, sendo ela, An@p@^!?&Cl3d150n.

A Figura 48 mostra a tentativa fracassada de quebra da chave, sendo que a mesma não se encontra no dicionário utilizado, mesmo sendo ele composto por milhares de combinações, neste caso um novo dicionário deve ser testado.

Para uma quebra se senha WPA bem sucedida muitas vezes é necessário utilizar vários dicionários com características diferentes, confirmando assim a importância do dicionário utilizado pelo Aircrack-ng.

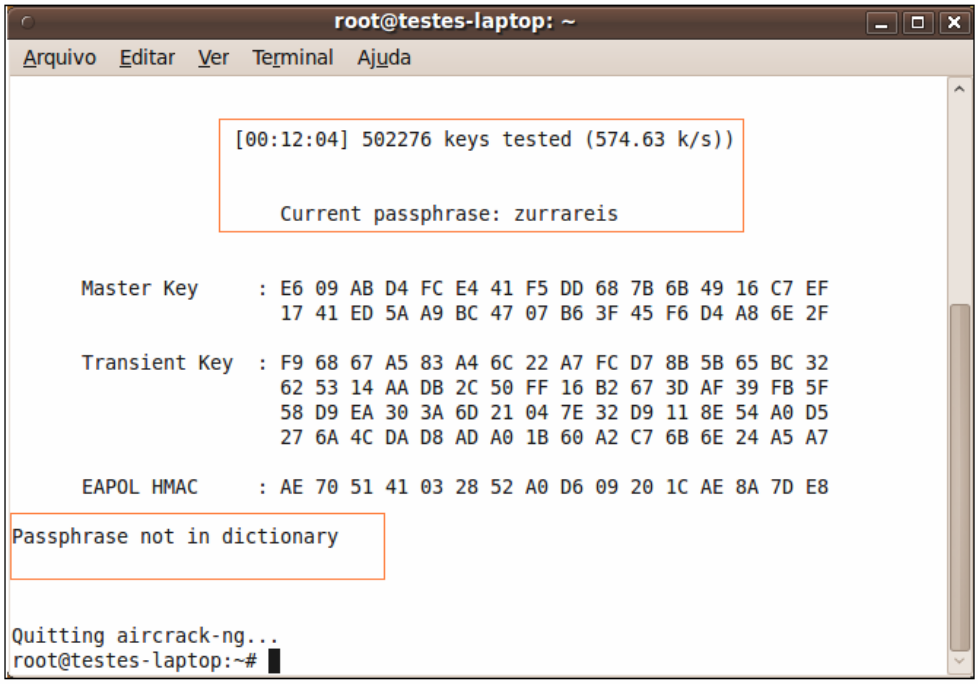


Figura 48. Quebra fracassada de chave WPA

Neste caso foram testadas 502.276 chaves em mais de 12 minutos com uma média de 574 chaves por segundo.

Também foi realizado um teste com uma senha gerada pelo SoftFuse, com uma seqüência de 15 caracteres como pode ser observado na Figura 49.

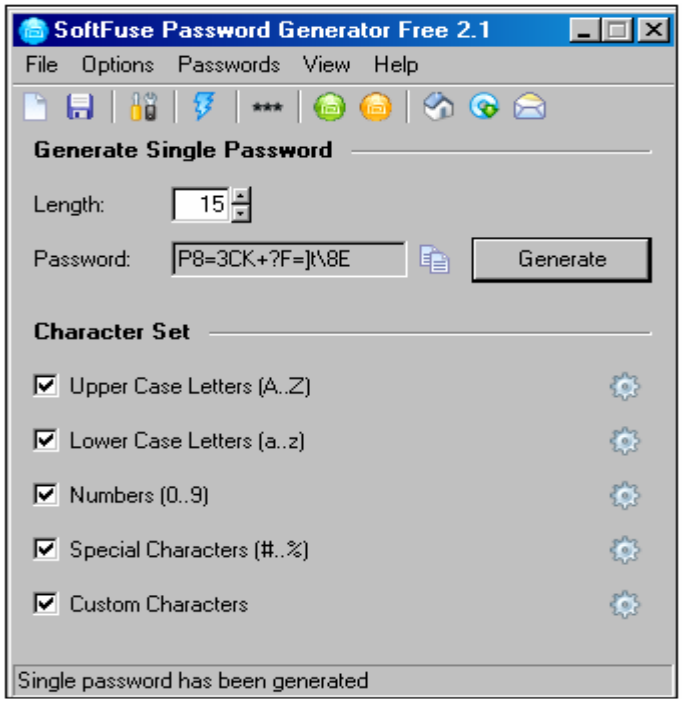


Figura 49. SoftFuse gerando senha

A senha gerada pelo software desta vez garantiu a segurança da rede, como pode-se ver na Figura 50.

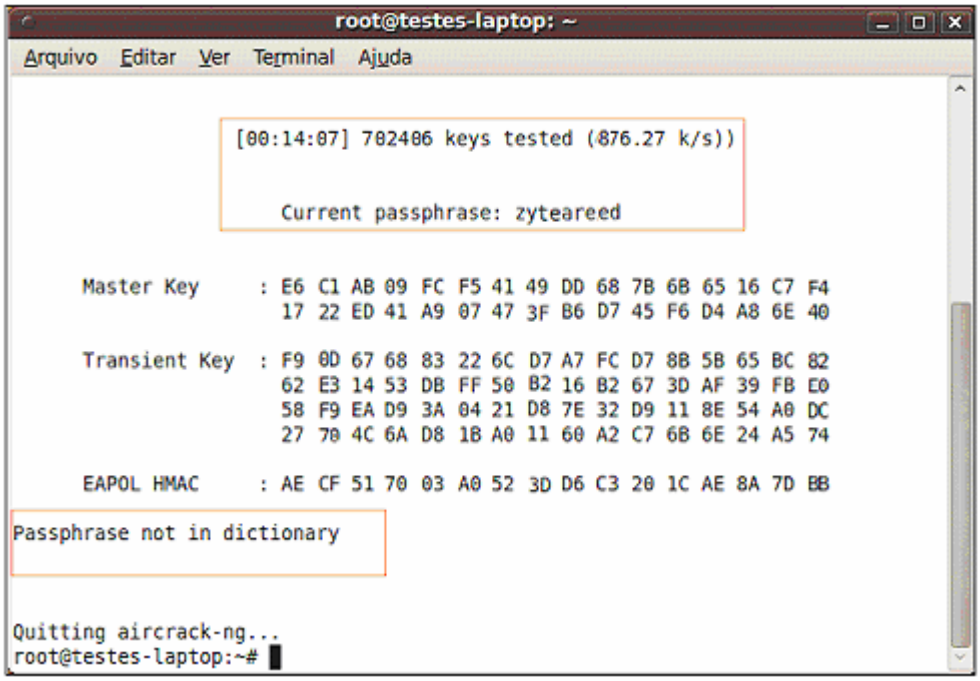


Figura 50. Tentativa fracassada de quebra da senha gerada por software

Os testes realizados na seqüência envolvem o protocolo WPA2 com a criptografia AES.

6.6.4 Segurança com o Protocolo WPA2

A seqüência de testes se dá com o protocolo WPA2, juntamente com a criptografia AES, que tem como características separar os blocos para realizar a criptografia separadamente tornando a quebra mais difícil e demorada, está combinação também suporta chaves de até 64 caracteres.

Os passos são os mesmos realizados nas análises anteriores, a Figura 51 mostra as informações obtidas por meio do comando “iwlist scan”.

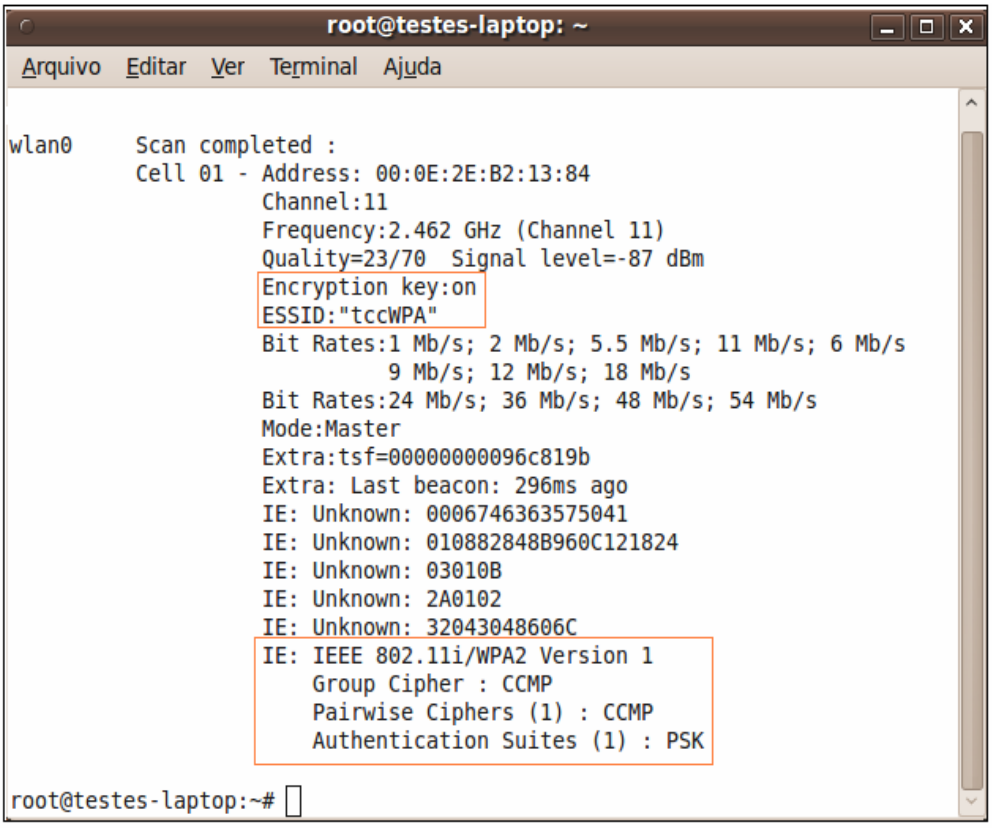


Figura 51. Informações da rede obtidas por meio do comando “iwlist scan”

Com os dados da rede coletados, o próximo passo é a escolha da senha que pode ser visto na Figura 52.

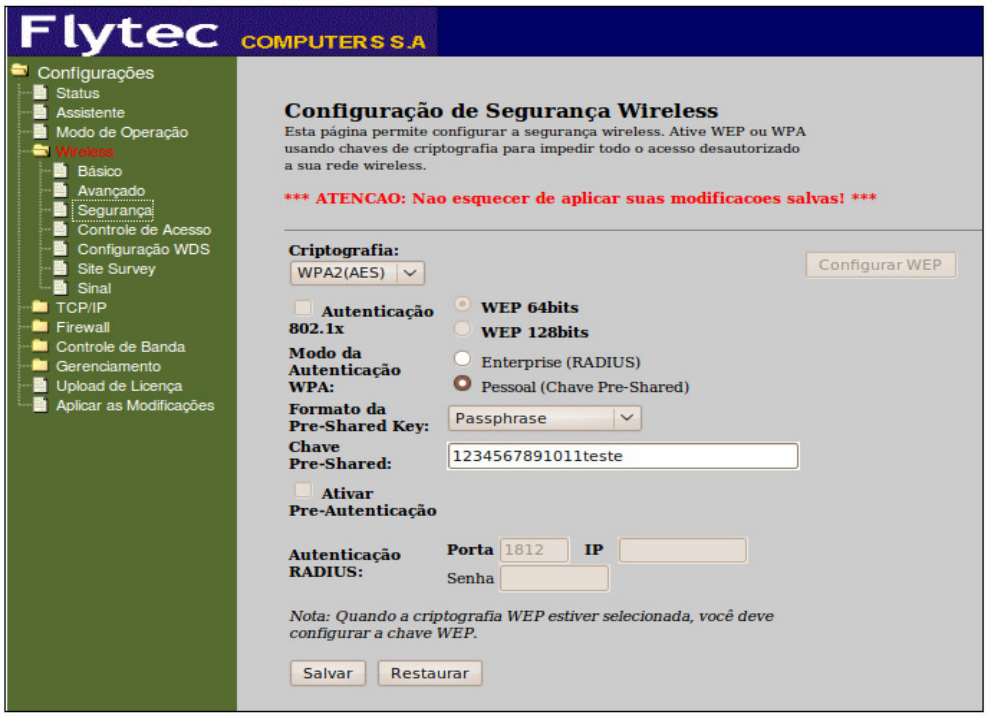


Figura 52. Ativando protocolo WPA2 (AES) e escolhendo a senha

A primeira senha testada é uma combinação de números e letras, considerada uma senha com grau de complexidade baixo, que após capturarmos aproximadamente 50.000 IVs pode ser quebrada como mostra a Figura 53.

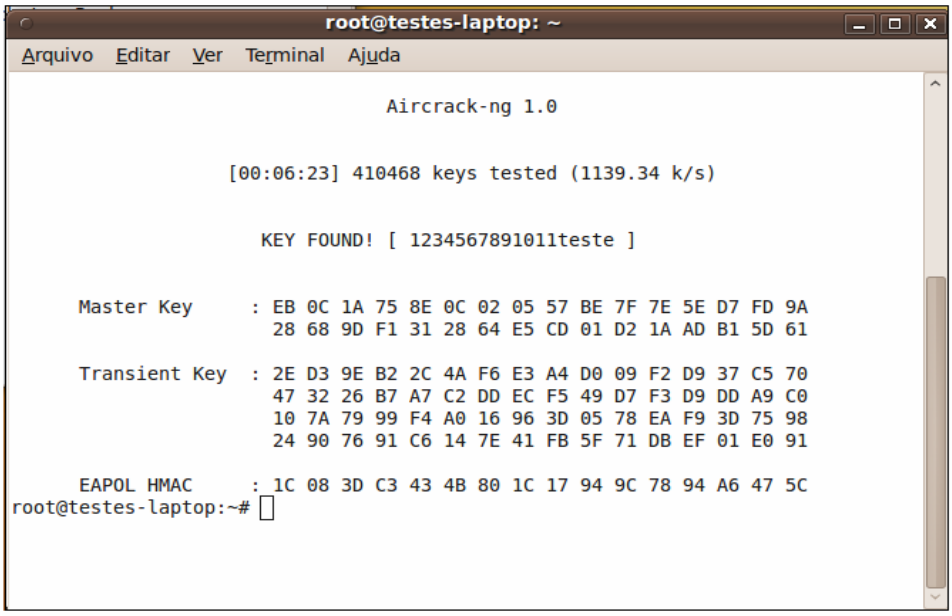


Figura 53. Desvendando uma chave WPA2 (AES)

Observando a facilidade da quebra da chave em aproximadamente 6 minutos testando 410.468 chaves, foi então testada uma chave um pouco mais elaborada como mostra a Figura 54, esta contendo letras números e caracteres especiais.

Figura 54. Escolhendo a chave WPA2 (AES)

Para esta chave também foram capturados aproximadamente 50.000 pacotes com Airodump-ng por meio do comando “airodump-ng -- channel 11 -w wpa2media.cap mon0” como mostra a Figura 55. A captura do *handshake* também pode ser observada, esta informação é adquirida por meio do comando “aireplay-ng -0 5 -a 00:0E:2E:B2:13:84 - c 00:1A:73:A6:C4:D6 mon0”. Nesta mesma figura foram identificadas às informações referentes as seguranças da rede, onde o algoritmo utilizado é chamado de CCMP, sendo ele o mesmo AES, pois este também pode ser chamado por AES-CCMP, mas no Linux sua representação é feita somente por CCMP.

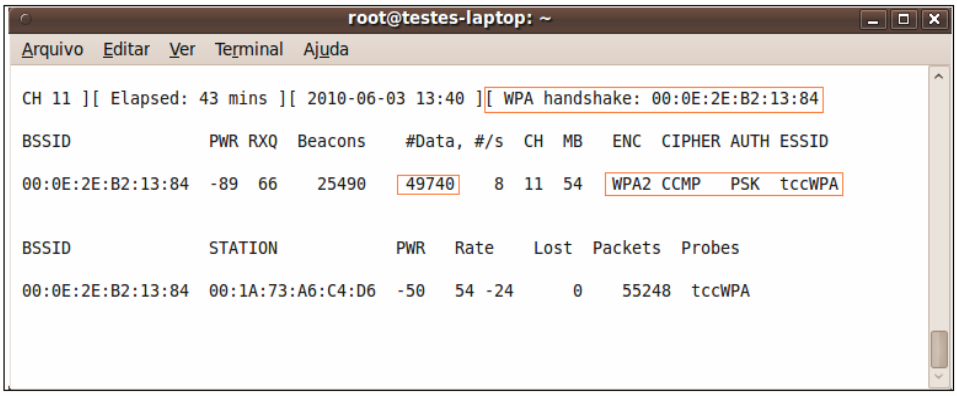


Figura 55. Capturando pacotes com a criptografia WPA2 (AES)

Por meio comando “aircrack-ng -e tccWPA -w WORD1.LST wpa2media.cap” pode-se observar que mesmo essa senha com um nível de dificuldade mais elevado, pode ser quebrada em 20 segundos e testando 20.136 chaves, com uma média de 950 chaves por segundo, como mostra a Figura 56.

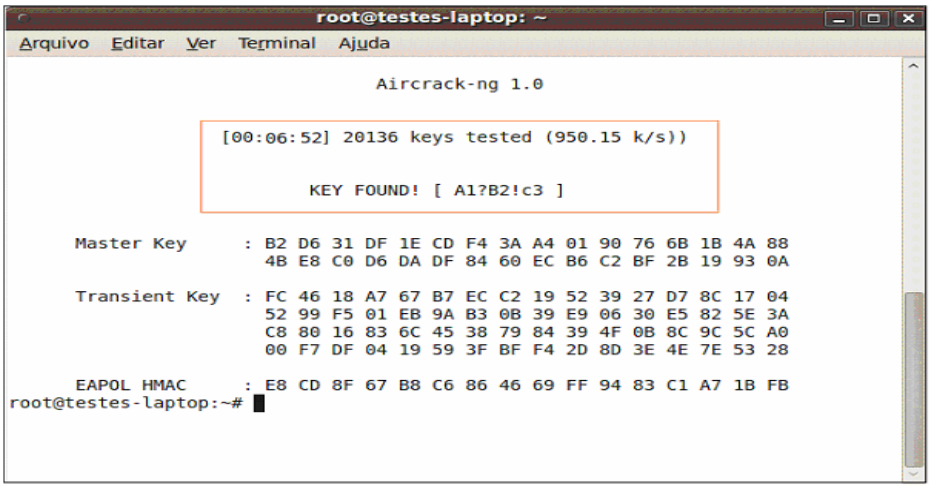


Figura 56. Quebrando uma chave WPA2 (AES) com caracteres especiais

Assim realizamos uma nova tentativa, agora com uma chave complicada, que inclui letras, números e caracteres especiais, numa combinação de 17 caracteres.

Após aproximadamente 12 minutos e testar 757.464 combinações, numa média de 1.184 testes por segundo, o Aircrack-ng não pode realizar a quebra da chave escolhida, como mostra a Figura 57.

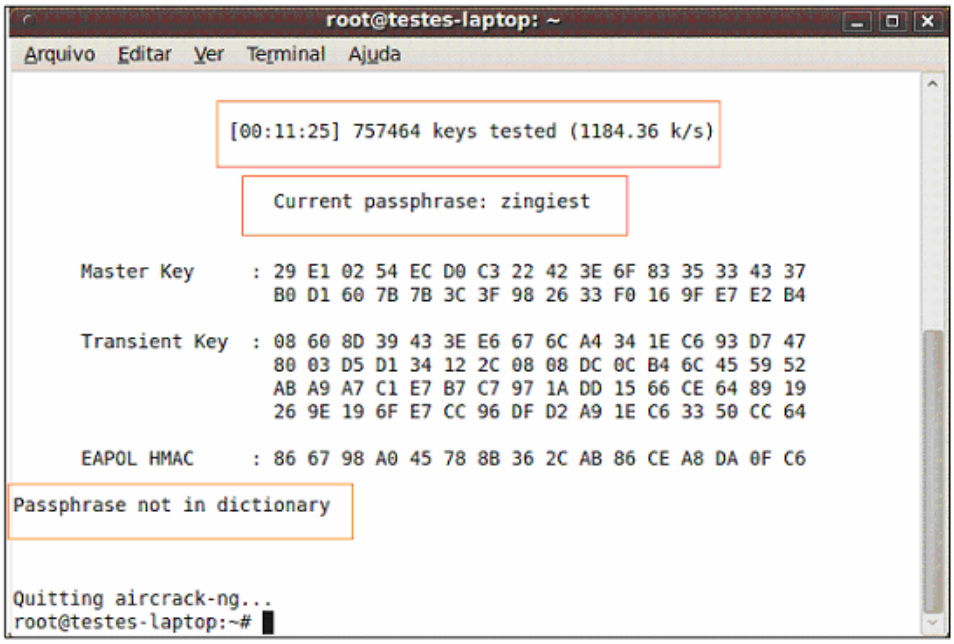


Figura 57. Quebra de senha WPA2 (AES) sem sucesso

Assim pode ser observada a importância da extensão das senhas, como os testes nos mostraram que quanto maior o número e a diversidade dos caracteres existentes em uma senha mais difícil será a sua quebra.

6.6.5 Segurança com o Protocolo WPA2 Mixed

Os últimos testes a serem realizados no trabalho analisam a segurança da rede levando em conta a criptografia WPA2 Mixed, que trás uma mistura da chave WPA TKIP com a WPA2 AES, como pode ser visto na Figura 58.

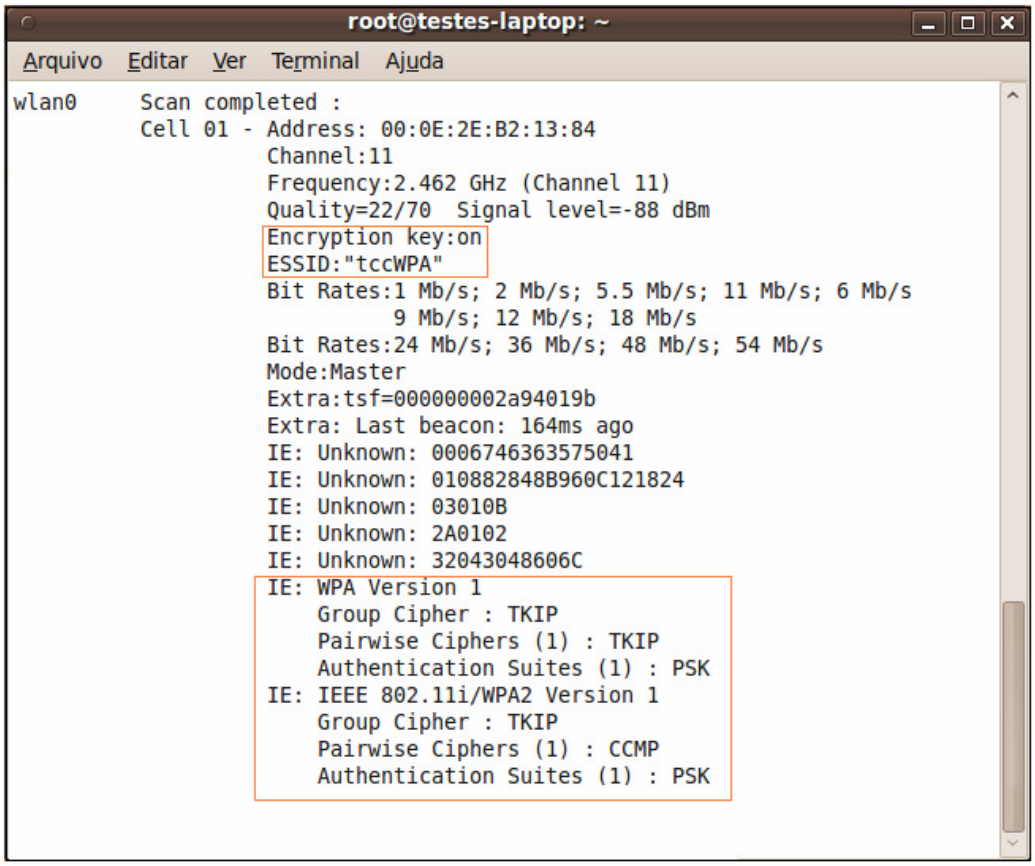


Figura 58. Dados da rede obtidos por meio do comando iwlist scan

A execução dos testes é realizada da mesma forma que os anteriormente, ou seja, com a interface em modo monitor, a captura dos pacotes com o Airodump-ng, apanhando o *handshake* com o Aireplay-ng, e quebrando as chaves com o Aircrack-ng.

Duas senhas foram utilizadas para que o nível de segurança pudesse ser observado com o uso dessa criptografia, a escolha da primeira a ser testada pode ser vista na Figura 59.

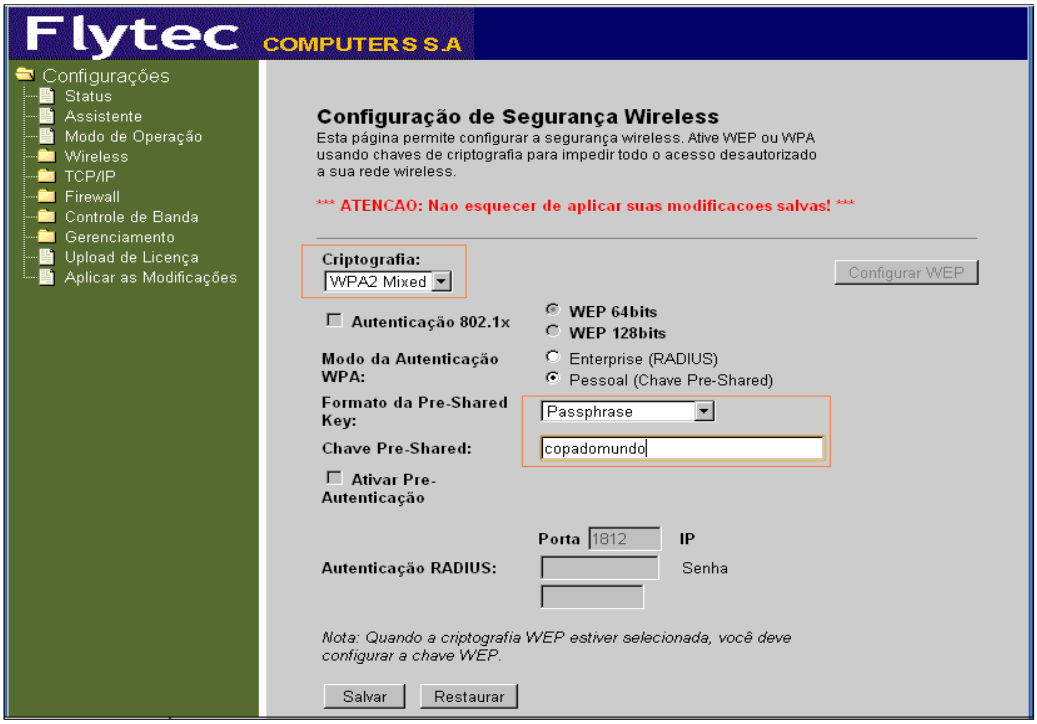


Figura 59. Criptografia WPA2 Mixed

Com a escolha da senha “copadomundo”, foi iniciado os testes, sendo que aproximadamente 50.000 pacotes e o handshake foram capturados, e após 4 minutos e 50 segundos a quebra da chave foi realizada como mostra a Figura 60.

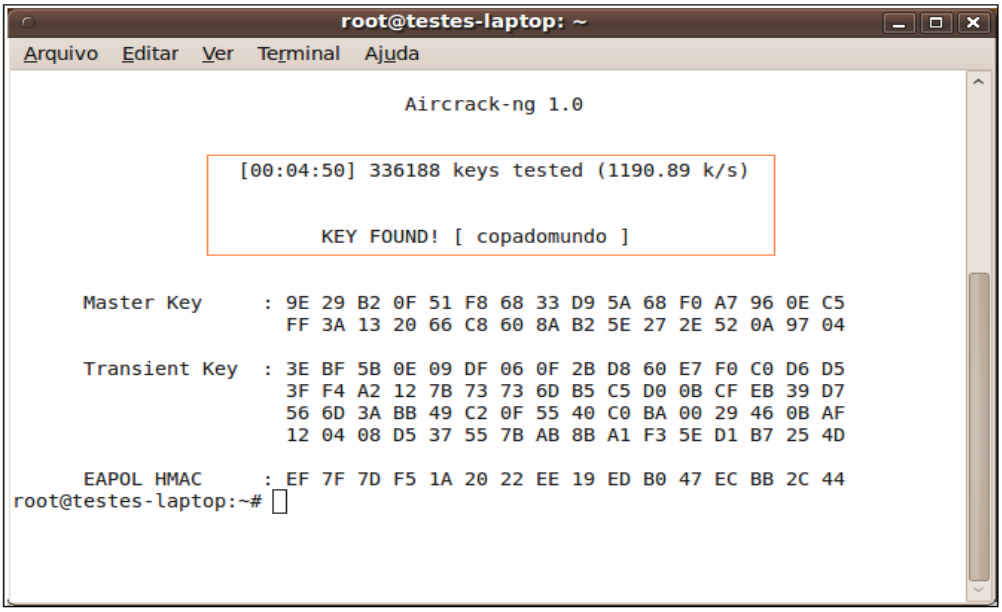


Figura 60. Quebra da chave WPA2 Mixed por ataque de dicionário

Como pode ser analisado na Figura 60, foram necessárias a utilização de 336.188 chaves, e analisadas 1190 chaves por segundo para que a senha fosse desvendada.

Tendo base nos testes anteriores uma nova senha foi escolhida para um último teste, essa com caracteres especiais, letras e números, em uma seqüência de 21 combinações, dando origem à senha “An@p@uL@A1#b2#C312345”, que pode ser vista na Figura 61.

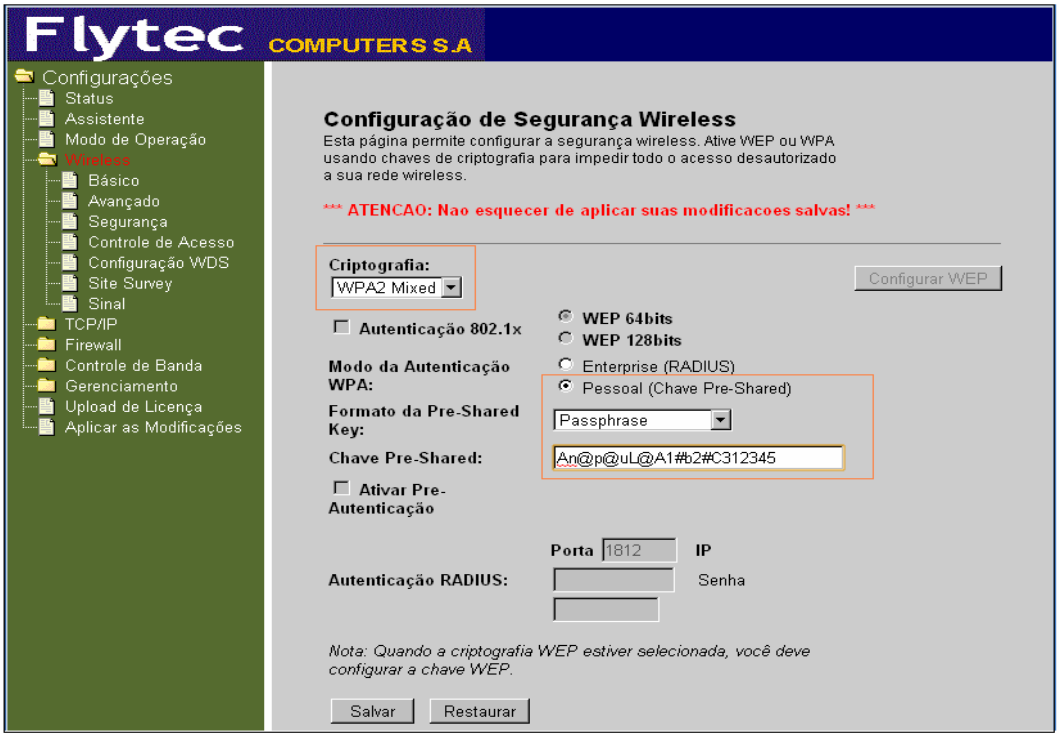


Figura 61. Escolha da senha com a criptografia WPA2 Mixed

Nesta análise foram coletados cerca de 112.000 pacotes, em 15 minutos, as informações referentes ao *handshake* da conexão também foram coletadas, como mostra a Figura 62.

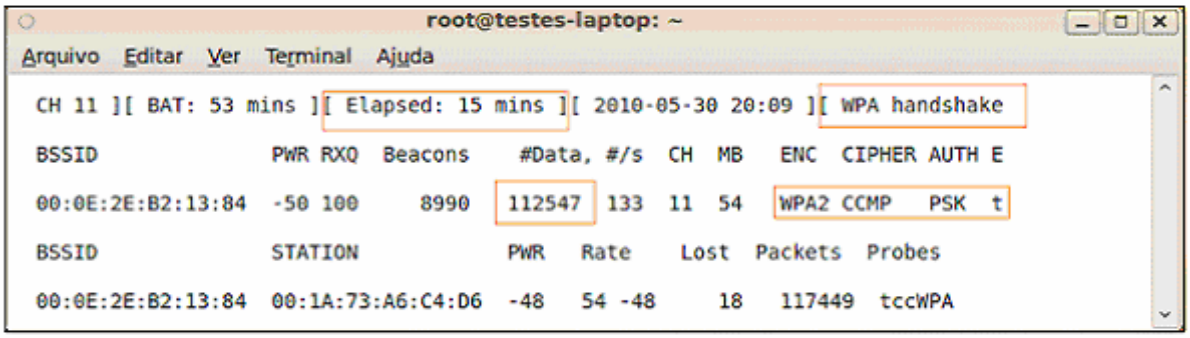


Figura 62. Captura dos pacotes e do *handshake*

Desta vez a chave não pode ser quebrada como mostra a Figura 63, isso significa que a seqüência não se encontra no dicionário testado, da mesma forma que foi explicado anteriormente, a melhor solução para um caso assim é a escolha de um novo dicionário.

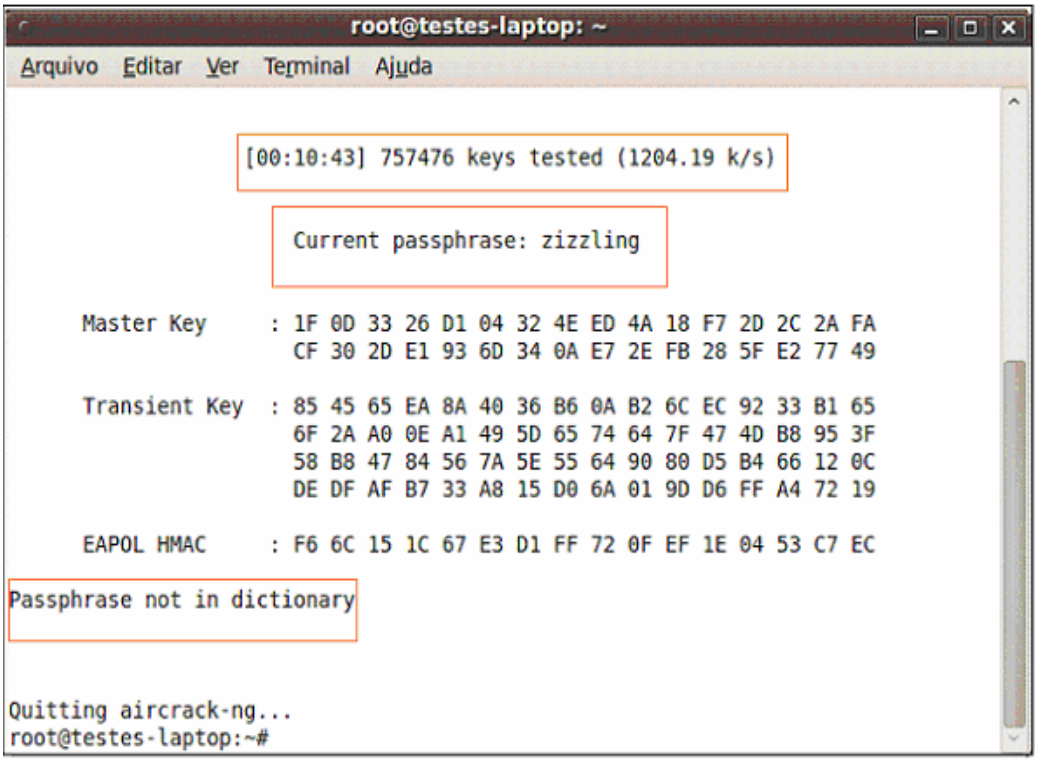


Figura 63. Quebra de senha WPA2 (AES) sem sucesso

Com isso pode-se observar que a segurança de uma rede tem relação com a senha utilizada, neste caso utilizando uma senha de um tamanho apropriado, aproveitando os recursos disponíveis pelo protocolo utilizado pode-se garantir um bom desempenho relacionado a segurança.

Na Tabela 7 pode ser analisado o desempenho de todas as senhas e protocolos utilizados.

Tabela 7. Testes Realizados

Protocolo	Chave	Tempo de Análise	Gerada por Software	Análise do Passwordmeter	Quebra da Senha
WEP 64 bits	12345	00:04	Não	4%	Sim
WEP 64 bits	yJ(M9	00:04	Não	46%	Sim
WEP 64 bits	A@q~2	00:04	Sim	56%	Sim
WEP 128 bits	1234567891011	00:07	Não	13%	Sim
WEP 128 bits	An@P@^!?25Cl3	00:10	Não	100%	Sim
WEP 128 bits	Ry&@74Nm[g*%Y	00:52	Sim	100%	Sim
WPA	teste12345	03:28	Não	52%	Sim
WPA	An@P@^!?&Cl3d150n	12:04	Não	100%	Não
WPA	P8=3CK+?F=)t\8E	14:07	Sim	100%	Não
WPA 2	1234567891011	06:23	Não	13%	Sim
WPA 2	A1?B2!c3	06:52	Não	95%	Sim
WPA 2	An@P@^!?&Cl3d150n	11:25	Não	100%	Não
WPA Mixed	copadomundo	04:50	Não	12%	Sim
WPA Mixed	An@P@^!?&Cl3d150n	10:43	Não	100%	Não

6.7 EVOLUÇÃO DOS EQUIPAMENTOS

Buscando uma tranqüilidade maior para o usuário em relação a sua rede sem fio muitas inovações surgiram. Entre eles novos protocolos, formas de criptografia, mas inovações de hardware também foram necessárias, novos equipamentos foram desenvolvidos para suportar essas evoluções e trazer outras (MIYANO NETO, 2004).

6.7.1 Access Points

Os *Access Points*, também conhecidos como centralizadores têm suas configurações pré-definidas na fábrica buscando trazer facilidade no momento de instalação, porém esta facilidade pode causar problemas posteriormente. As configurações realizadas pelo fabricante não ativam os mecanismos de segurança, tornando esta rede um alvo de fácil invasão. Então a primeira atitude a ser tomada após a configuração de uma rede é alterar as

configurações de segurança, para assim alcançar um nível de segurança mais confortável (COSTA, 2009).

A evolução dos APs em relação a hardware deu seu maior passo em 2004, quando foi necessário a troca dos equipamentos para quem optasse por utilizar o novo protocolo, o WPA2 ou 802.11i, já que na evolução anterior onde o protocolo WEP passou por alterações e se transformou em WPA apenas uma atualização do software foi necessária (MIYANO NETO, 2004).

Comparando os APs atuais com os de alguns anos atrás é possível observar a evolução, buscando cada vez mais segurança e comodidade do usuário.

Entre as diversas opções de segurança estão:

a) WEP: alguns *Access Points* oferecem chaves de 64 até 512 bits, a ativação deste protocolo é indicada apenas para equipamentos que não suportam outras formas de segurança, pois apesar de contribuir para uma rede um pouco mais segura, não fornece uma segurança necessária para que o usuário fique tranqüilo;

b) WPA: essa evolução do WEP está disponível em todos os APs já que para obter esse protocolo apenas uma atualização é necessária. Esse protocolo fornece uma garantia maior de segurança para a rede, como vimos nos testes anteriores a quebra das senhas que utilizam esse protocolo é mais difícil que no WEP;

c) WPA2: esse protocolo é encontrado em equipamentos fabricados a partir de 2004, que é a data em que iniciou a utilização desta ferramenta. Esse protocolo é uma das alternativas mais eficazes, desde que o usuário escolha uma senha que seja capaz de fornecer segurança, que respeite as regras citadas no Item 6.3;

d) WPA2 Mixed: alguns equipamentos trazem essa opção que encapsula os dois protocolos (WPA e WPA2) visando permitir o acesso à rede computadores que não possuem acesso ao WPA2. A Figura 64 mostra as opções de protocolos

encontradas no AP em que os testes foram realizados, na Figura 65 pode-se visualizar as opções de protocolos de segurança disponíveis no AP TP-LINK, para que possa realizar uma observação;

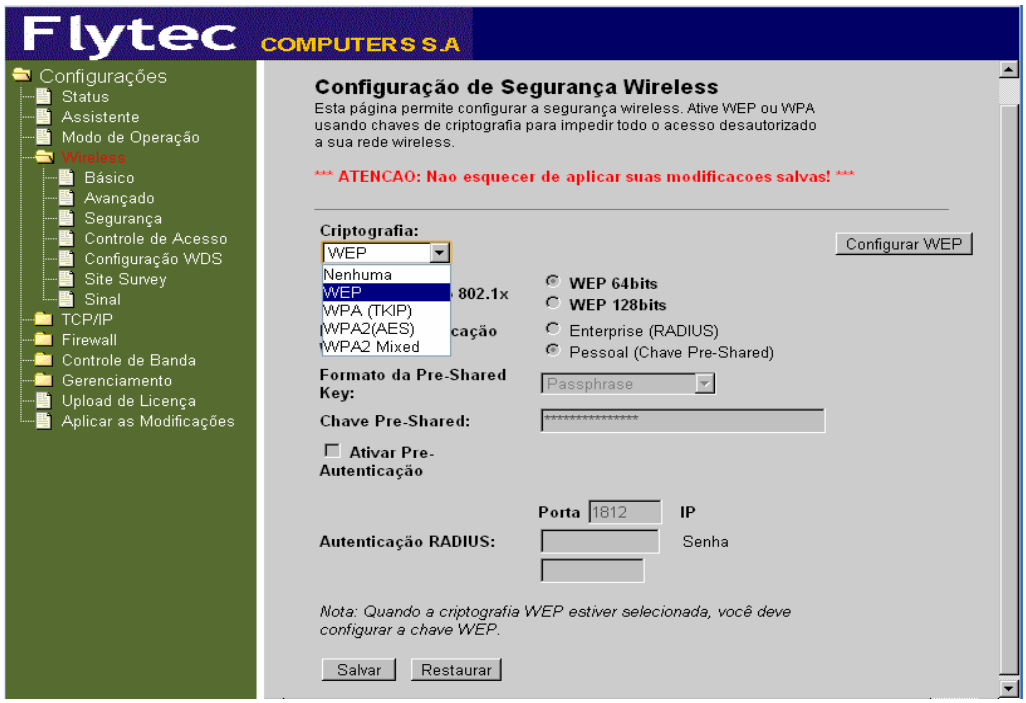


Figura 64. Opções de protocolos disponíveis no AP

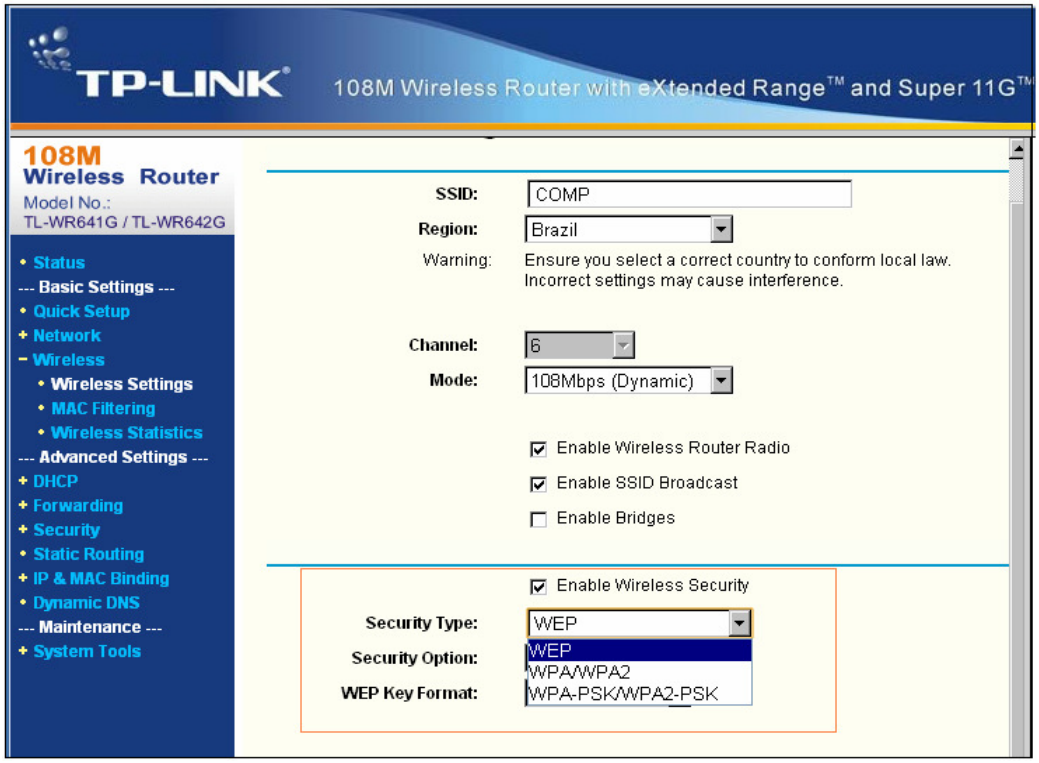


Figura 65. Opções de protocolos disponíveis no AP com a marca TP-LINK

e) RADIUS: o *Remote Authentication Dial In User Service* uma forma de criptografia que utiliza chaves com 128 bits reais, que filtra seus usuários por meio de um processo com usuário e senha. Um grande problema encontrado nessa opção é que nem todos os equipamentos a disponibilizam (NAKAMURA; GEUS, 2003). Esse protocolo oferece acesso a redes com Autenticação, Autorização, Contabilização (*Authentication, Authorization e Accounting* - AAA).

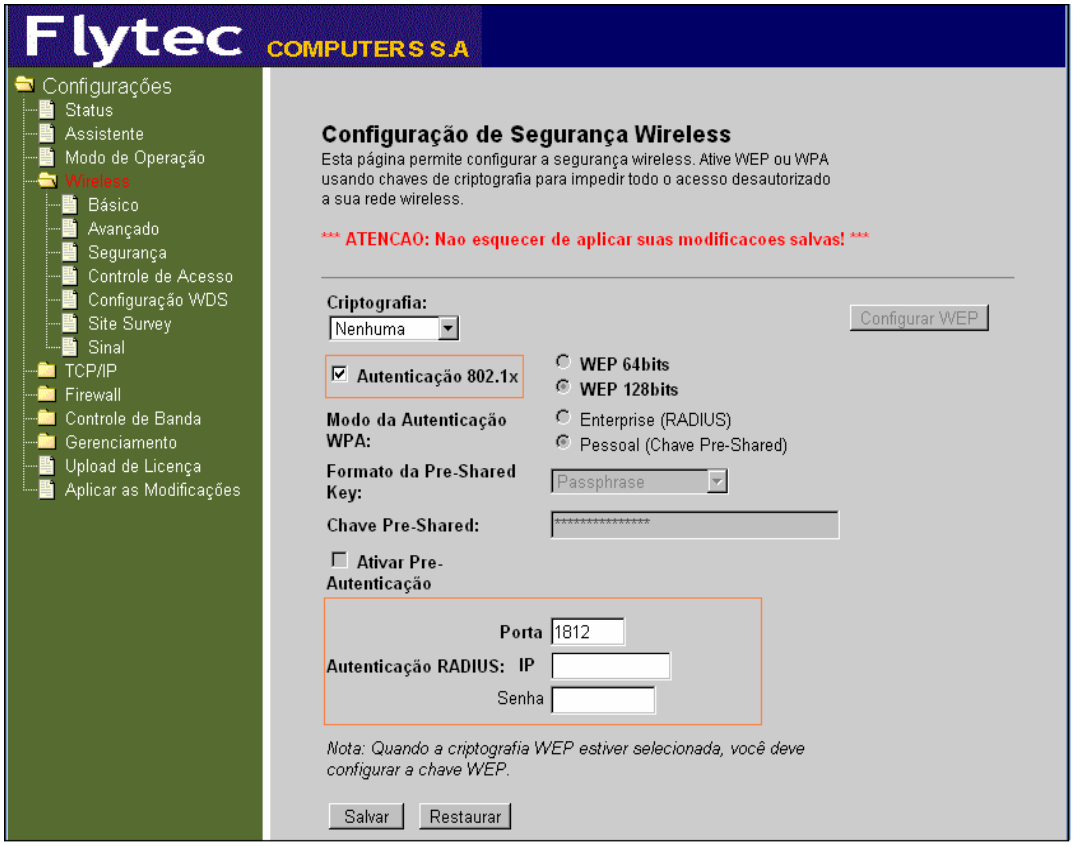


Figura 66. Opções de configuração RADIUS

d) *firewall*: este item de segurança disponibiliza algumas opções de filtro de rede, ou seja, só permite a conexão na rede de usuários que se enquadrem nas configurações realizadas no AP. As restrições podem ser feitas por meio de filtro de portas, de IPs, de endereço MAC, entre outros, dependendo dos recursos disponibilizados pelo AP utilizado na rede. A Figura 67 e 68 mostra os recursos disponíveis em dois APs, para que uma análise possa ser realizada;

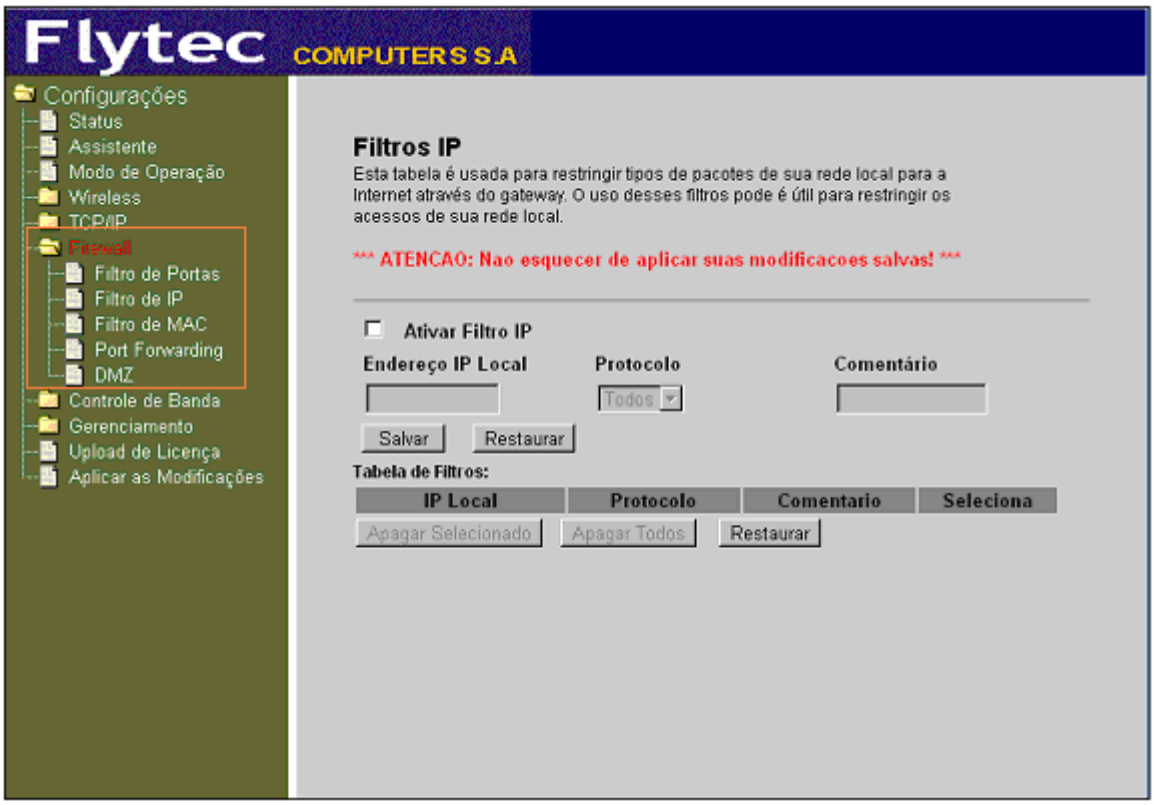


Figura 67. Opções de *Firewall*

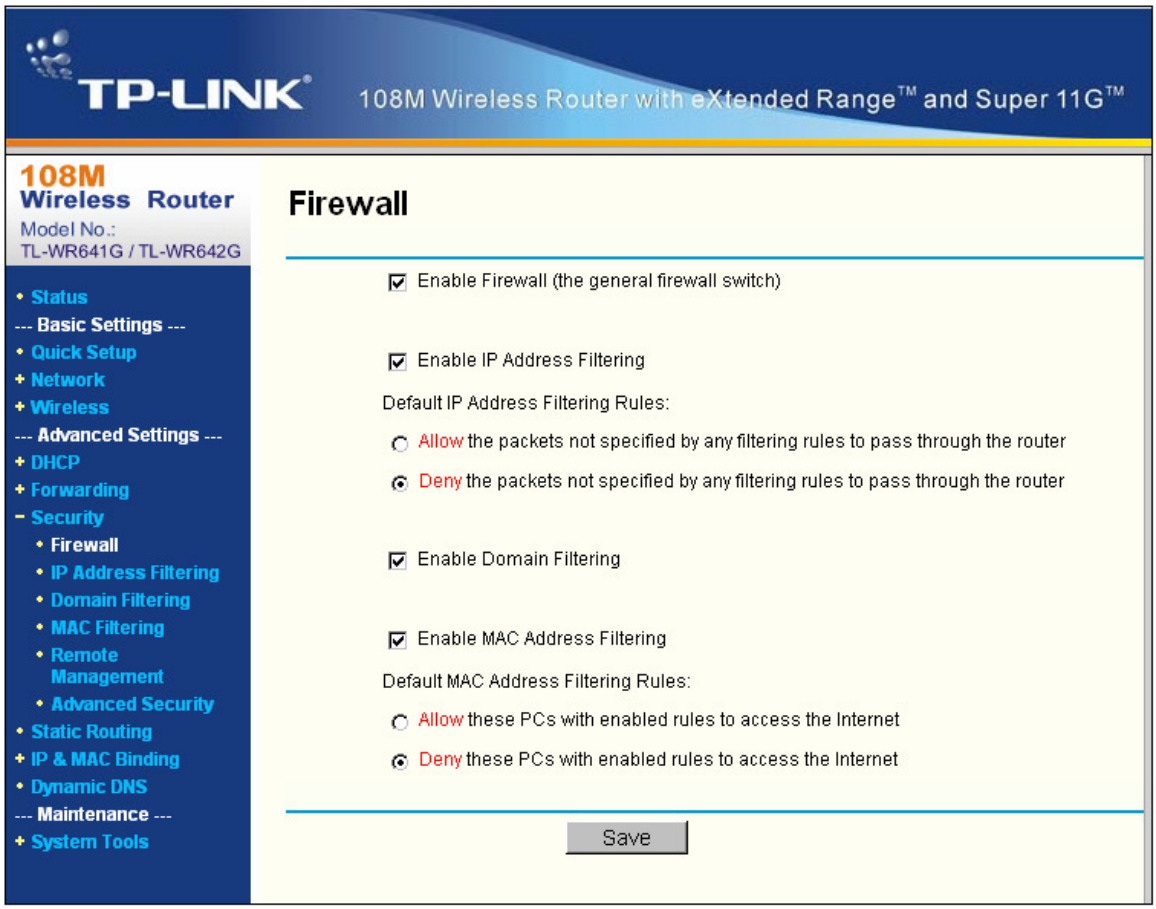


Figura 68. Opções de Firewall no AP com a marca TP-LINK

e) controle de banda: essa opção permite que sua banda seja dividida entre os usuários com acesso permitido em sua rede. Essa restrição pode ser realizada por IP, por interface ou por MAC como mostra a Figura 69;

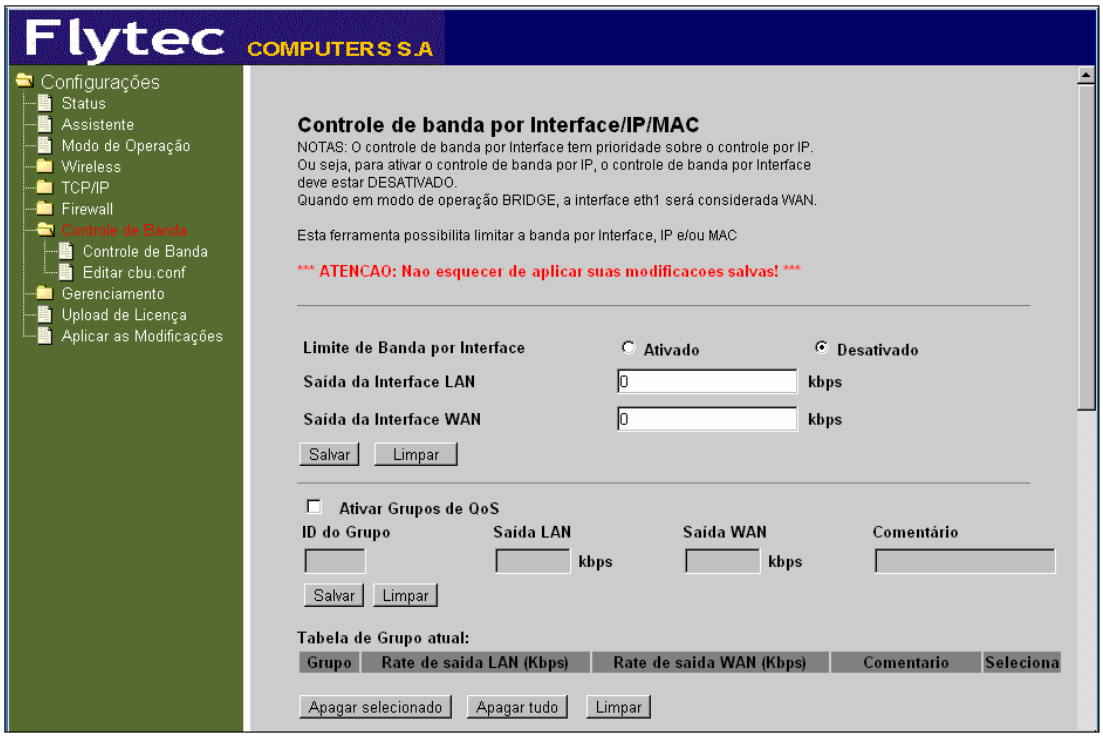


Figura 69. Controle de banda no AP

j) Ocultar o SSID: é uma das opções de segurança disponíveis nos APs. Cada fabricante utiliza um valor default, mas a primeira ação do usuário após a instalação é alterá-lo para um valor difícil de ser desvendado. Optando por desativar essa opção apenas usuários que conhecem a rede podem realizar a conexão. A Figura 70 mostra as opções disponibilizadas pelo AP.

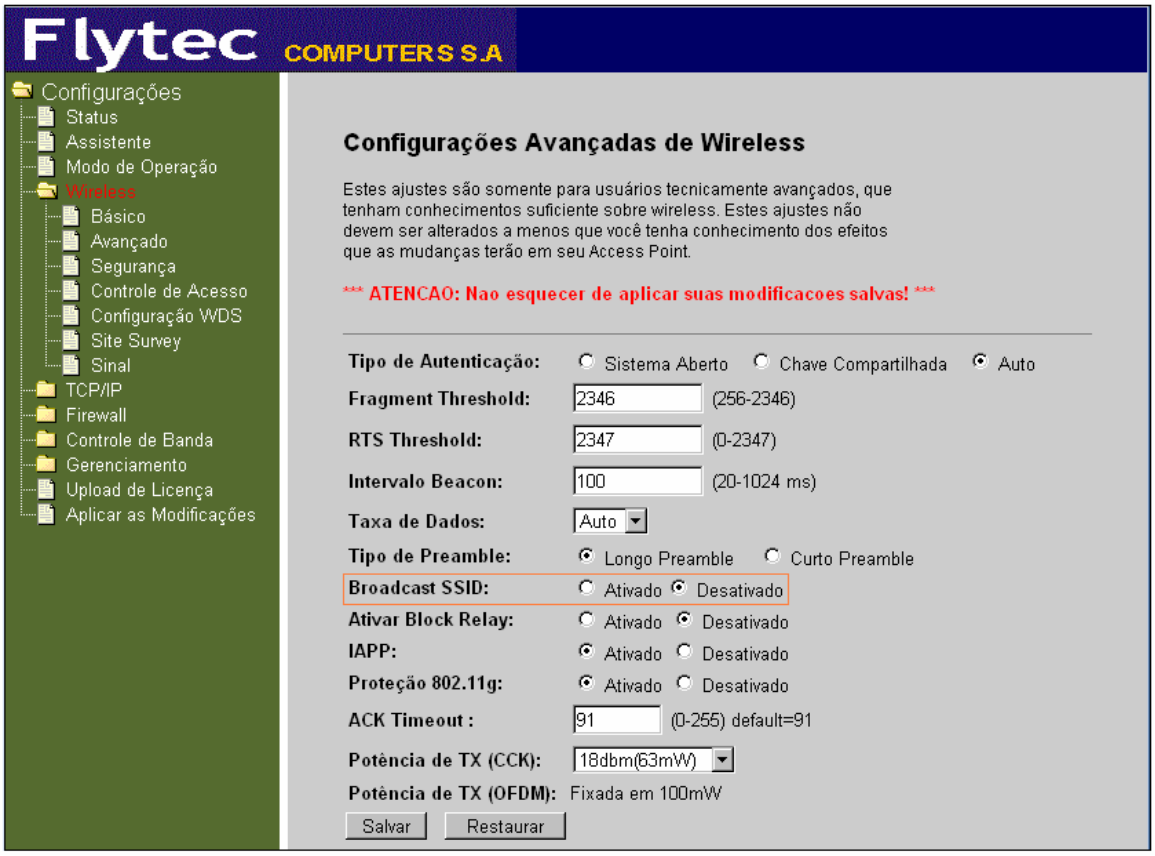


Figura 70. Ocultar SSID no AP

6.8 POLITICAS DE SEGURANÇA

O uso de políticas de segurança em organizações tem uma grande importância e está diretamente relacionado ao nível de proteção da sua rede, pois é por meio delas que são definidas as questões de segurança das informações que ali trafegam.

É necessário analisar o custo beneficio causado pela política de segurança, bem como se suas regras não interferem de forma significativa na produtividade dos usuários, pois uma segurança total não pode ser alcançada, mas uma análise do risco é um papel fundamental (NAKAMURA; GEUS, 2003).

Segundo Wadlow (2000) algumas ações importante para garantir a segurança de uma rede organizacional são:

a) sempre requisitar autenticação do usuário, para que o administrador tenha as informações de acessos realizados;
b) o acesso ao sistema de um ex-funcionário deve ser eliminado imediatamente;
c) os usuários não devem conhecer as características de segurança da rede;
d) deve-se deixar bem claro o que está sendo protegido;
e) a contratação de novos funcionários exige cuidados, um funcionário com má intensão pode por a perder toda a segurança da rede.

Uma estratégia bem proveitosa que deve ser tomada é oferecer cursos, palestras e treinamentos para habilitar os usuários, e conscientizá-los da importância de preservar a segurança da rede, medidas preventivas são muito mais proveitosas e são a forma mais indicada quando o assunto é segurança, pois os prejuízos causados por um ataque podem ser incalculáveis.

6.9 RESULTADOS OBTIDOS

Por meio da pesquisa desenvolvida e dos testes realizados pode-se observar a fragilidade do protocolo WEP, que mesmo utilizando senhas bem elaboradas tem suas chaves quebradas facilmente com a utilização de ataques de força bruta. Com isso, deve-se sempre que possível evitar o uso desse protocolo, independente de a chave ser de 64 ou 128 bits, para evitar que suas vulnerabilidades comprometam a segurança da rede.

O protocolo WPA e WPA2 têm um nível de segurança bem mais elevado, porém o usuário deve explorar sua capacidade de aceitar senhas mais longas como forma de dificultar sua quebra. Nos testes realizados com esses protocolos pode-se observar que as senhas que resistiram aos ataques são senhas mais extensas e elaboradas, como uma mistura

de um maior número de chaves. Porém deve-se levar em conta que a quebra da chave WPA e WPA2 depende do dicionário utilizado.

As senhas devem ser criadas com o intuído de que sejam o mais forte possível, pois elas são a chave que aumenta de forma significativa a segurança do usuário e dos dados que ali trafegam. Os usuários devem ter a responsabilidade de cuidar de uma forma especial do armazenamento dessas chaves.

Todas as opções de segurança disponíveis no AP devem ser utilizadas, como forma de buscar uma rede mais segura. Na hora da compra desse aparelho os aspectos de segurança devem ser analisados. As configurações devem ser bem feitas, bem como as alterações das opções de segurança que existem em modo *default.*

Uma política de segurança bem feita também é muito importante em casos de organizações, os usuários devem estar cientes das regras e normas para que as informações possam ser preservadas e também devem conhecer a importância do cumprimento dos itens da política.

Sabe-se que uma rede completamente segura não existe, porém se todos os itens citados forem respeitadas e seguidos o nível de segurança será muito elevado, e assim um equilíbrio em relação à segurança da rede será obtido.

CONCLUSÃO

A pesquisa realizada apresentou algumas vulnerabilidades encontradas em redes sem fio, e por meio de testes mostrou as fragilidades e as falhas encontradas no protocolo WEP, WPA e WPA2, bem como uma forma de proteção por meio de senhas seguras.

Novas formas de proteção vêm surgindo para tentar suprir as falhas que existem nos protocolos anteriores, mas acompanhando essa evolução novas vulnerabilidades vêm sendo descobertas. Para que isso não comprometa a utilização das redes sem fio, os usuários devem estar atentos e aplicando todas as formas de segurança possíveis em sua rede.

Também pode ser observada a importância das opções de segurança disponibilizada pelos *Access Points*, pois eles oferecem diversas formas de aumentar a segurança das redes, que devem ser observadas no momento da compra, que se utilizadas corretamente podem diminuir as vulnerabilidades que este tipo de rede está sujeita.

As organizações devem sempre almejar por uma rede mais segura, cada vez mais ativando formas de proteção, treinando e conscientizando funcionários, para assim proteger seus dados e seu patrimônio. Também pode ser visto a importância das políticas de uso, onde os usuários da rede devem saber e entender seus deveres, pois não adianta tomar cuidado na criação de senhas seguras e possibilitar que usuários mal intencionados tenham acesso a elas.

Uma atenção especial foi dada para as senhas, pois elas podem ser uma forma muito eficaz de evitar ataques as *Wireless,* pois é uma tarefa muito difícil garantir a segurança de informações que trafegam pelo ar. Senhas fortes exigem atenção do seu criador, pois necessita que várias características sejam exploras, para dar origem a chaves que realmente podem ser mais resistentes a ataques. Sendo assim o usuário deve se empenhar e aplicar as sugestões dadas neste trabalho buscando aumentar o nível de segurança da rede.

Sugere-se para trabalhos futuros que outras vulnerabilidades e formas de proteção sejam estudadas e sugeridas, trazendo mais informações e opções para os usuários dessas redes. Alguns estudos podem ser realizados sobre RADIUS, trazendo mais informações e os benefícios alcançados com a utilização desta opção de criptografia.

REFERÊNCIAS

ALBERTO, F et al. **Segurança da Informação**. Curso de Sistemas de Informação, Sociedade Paranaense de Ensino e Informática. Dez, 2006.

AIRSTRIKE. **O que é o AirStrike?**
Disponível em: http://www.airstrike.ravel.ufrj.br/br/conteudo_osistema.htm. Acessado em: 23 de Nov. de 2009.

ALVES, Walter Francisco Andrade. **Segurança em redes sem fio: O caso da Assembléia Nacional de Cabo Verde.** Trabalho de Conclusão de Curso – Curso de Engenharia de Sistemas e Informática, Universidade Jean Piaget de Cabo Verde, Cidade da Praia, Santiago, Dez. 2009.

ANDRADE, Lidiane Parente. **Análise das Vulnerabilidades de Segurança Existentes nas Redes Locais Sem Fio: Um Estudo de Caso do Projeto Wlaca.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Federal do Pará, Belém, Pará, 2004.

ANDRADE, Marcelo Borges; COLLI, Rodrigo. **REDES AD-HOC**. Curso de Engenharia de Redes, Instituto de Educação Superior de Brasilia, Brasilia, 2003.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 5 de Out. 2009.

Criando Senhas Seguras. **UFPEL.**
Disponível em: < http://ci.ufpel.edu.br/treinamento/apostilas/seguranca/senhas.pdf>. Acesso em: 5 de Jun 2010.

COMER, Douglas E. **Redes de computadores e internet: abrange transmissão de dados, ligação inter-redes e web.** 2.ed Porto Alegre: Bookman, 2001.

COSTA, Flávio Wesler de. **Análise de Padrões de Segurança em Redes sem Fio IEEE 802.11.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, Santa Catarina, 2009.

COZER, Fábio Luiz. **Segurança Redes sem Fio.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Faculdade de Jaguariúna, Jaguariúna, São Paulo, 2006. Disponível em: < http://bibdig.poliseducacional.com.br/document/?down=100>. Acesso em 4 de jun. 2009.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, São Paulo, 2003.

FIGUEIREDO, Marcio Edmar Girard; DINIZ, Palmenas Costa; COROA, Sérgio Vinícius. **Segurança em Redes sem Fio Utilizando VPN Baseado em SSL.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade da Amazônia, Belém, Pará, 2005.

FREITAG, Juliana. **Provisão de Qualidade de Serviço em Redes IEEE 802.11.** Dissertação de Mestrado – Curso de Ciência da Computação, Universidade Estadual de Campinas, Campinas, São Paulo, 2004.

GIMENES, Eder Coral. **Segurança de Redes Wireless.** Trabalho de Conclusão de Curso – Curso de Tecnologia em Informática com ênfase em Gestão de Negócios, Centro de Educação Tecnológica Paula Souza Faculdade de Tecnologia de Mauá, Mauá, São Paulo, 2005.

HAYDEN, Matt. **Aprenda em 24 horas redes**. Rio de Janeiro: Ed. Campus, 1999.

HOADLEY, John. **Building future networks with MIMO and OFDM.** Connectedplanet, set. 2005. Disponível em: <http://connectedplanetonline.com/wireless/technology/mimo_ofdm_091905/> Acesso em: 10 abr. 2010.

IEEE STANDARS ASSOCIATION. IEEE 802.11: **LAN/MAN Wireless LANS**. Disponível em: <http://standards.ieee.org/getieee802/802.11.html>. Acesso em: 07 out. 2009.

JUNIOR, Arthur Santos. **Cabeamento Estruturado. Instituto online** , nov. 2008. Disponível em: <http://www.instonline.com.br/download/Palestra_seguranca_wireless_Workshop_Camehil_e_Instituto_Online.pdf>. Acesso em: 10 abr. 2010.

JUNIOR, David Frasson. **Análise de Vulnerabilidades Envolvendo Aplicações Móveis: Estudo de Caso na Aplicação Móvel de Acesso à Base de Dados de um Sistema de Registro Eletrônico em Saúde para UTI.** Trabalho de Conclusão de Curso - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, Santa Catarina, 2008.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-down. 3. ed São Paulo: Pearson Addison Wesley, 2006.

LACERDA, Pablo de Souza. **Análise de Segurança em Redes Wireless 802.11x.** Trabalho de Conclusão de Curso – Curso de Ciências da Computação, Universidade Federal de Juiz de Fora, Juiz de Fora, Minas Gerais, 2007.

MAIOR, Alex de Oliveira Barros; SANTOS, Fábio Antonio dos; LACQUA, Sabrina Cristiane Dal. **Gestão da Segurança da Informação.** Trabalho de Conclusão de Curso – Curso de Sistema de Informação, Faculdade Gennari & Peartree, Pedreneiras, São Paulo, 2006.

MALBURG, Maria Moura. **Modulação.** GTA/UFRJ, Rio de Janeiro, nov, 2004. Disponível em: <http://www.gta.ufrj.br/grad/04_2/Modulacao/>. Acesso em: 10 abr. 2010.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2008.

NAKAMURA, Emilio Tissato. **Um Modelo de Segurança de Redes para Ambientes Cooperativos.** Dissertação de Mestrado – Instituto de Computação, Universidade Estadual de Campinas, Campinas, São Paulo, 2000.

NETO, Francisco Dias. **Análise de Vulnerabilidade em Redes sem Fio.** Trabalho de Conclusão de Curso – Curso de Especialização em Redes de Computadores e Comunicação de Dados, Universidade Estadual de Londrina, Londrina, Paraná, 2006.

NETO, Roberto Miyano. **A Evolução dos Mecanismos de Segurança para Redes sem fio 802.11.** Monografia - Curso Introdução a Computação Móvel, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2004.

PEREIRA, Marcos Heyse. **Segurança de redes sem fio, uma proposta com serviços integrados de autenticação LDAP e RADIUS.** Redes e Segurança de Sistemas Pontifícia Universidade Católica do Paraná, Paraná, nov. 2009.

PETERSON, Larry L; DAVIE, Bruce S. **Redes de computadores:** uma abordagem de sistemas. Rio de Janeiro: Elsevier, 2004.

PINHEIRO, José Mauricio Santos. **Vulnerabilidades em Redes Wireless**. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_vulnerabilidades_em_redes_wireless.php>. Acesso em: 07 nov. 2009.

POMPERMAYER JUNIOR, Jorge Luiz. **Protótipo de Software para a Monitoração de Pacotes em uma Rede TCP/IP em Ambientes Linux.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Regional de Blumenau, Blumenau, Santa Catarina, 2002

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes Sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec, 2005.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

Senhas (br) Palavra Passe (pt). **Kiokea.net**, out. 2009. Disponível em: <http://pt.kioskea.net/contents/attaques/passwd.php3>. Acesso em: 15 abr. 2010.

SILVA, Adevaldo Queiros da. **Planejando Redes com Acesso sem Fio à Internet Utilizando a Tecnologia Wimax Integrada a Tecnologia Wi-Fi.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Federal de Pará, Belém, Pará, 2006.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de cumputadores das LANs, MANs e WANs às Redes ATM.** 2 ed. Rio de Janeiro: Campus, 1995.

SOUZA, Ricardo de Moura. **Análise das Vulnerabilidades e Ataques Existentes em Redes sem Fio.** Trabalho de Conclusão de Curso - Curso de Sistemas de Informação, Faculdades de Ciências Aplicadas de Minas, Uberlândia, Minas Gerais, 2005.

SPANCESKI, Francini Reitz. **Política de Segurança da Informação – Desenvolvimento de um Modelo Voltado para Instituições de Ensino.** Trabalho de Conclusão de Curso - Curso de Sistemas de Informação, Instituto Superior Tupy, Joinvile, Santa Catarina, 2004.

TANENBAUM, Andrew S. **Redes de computadores.** 4 ed. Rio de Janeiro: Campus, 2003.

Técnicas de transmissão de dados nas redes sem fios Wi-Fi. **KIOKEA,** out. 2009. Disponivel em:<http://pt.kioskea.net/contents/wifi/wifitech.php3>. Acesso em 18 fev. 2010.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Ed. Campus, 2000.

WANDERLEY, Danillo Lustosa. Políticas de Segurança. Lavras, MG, 2005. Monografia, Universidade Federal de Lavras.

APÊNDICE A

Análise de Segurança em Redes sem Fio e Método de Defesa por meio de Senhas Seguras

Ana Paula Biz[1], Paulo João Martins[2]

1Acadêmica do curso de Ciência da Computação – Unidade Acadêmica de Ciências Engenharias e Tecnologias – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma - SC - Brasil

[2]Professor do curso de Ciência da Computação – Unidade Acadêmica de Ciências Engenharias e Tecnologias – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma - SC - Brasil

anapaulabiz@msn.com, pjm@unesc.net

Abstract: *The internet users more and more choose to use wireless networks, searching comfort and flexibility. The wireless can be found as many as in the corporate environment and in household. The evolution of technology directed to mobile devices with Internet access was who gave great stimulus to this change. But problems related to information security were found and simple ways to use strong passwords can provide a more stable level of security to the user.*

Keywords: *Wireless Networks, Security, Passwords..*

***R*esumo**. *Os usuários de Internet cada vez mais optam pelo uso das redes sem fio, buscando comodidade e flexibilidade. As wireless podem ser encontradas tanto no meio corporativo quanto no uso doméstico. A evolução da tecnologia voltada para dispositivos móveis com acesso a Internet foi quem deu grande estimulo para essa mudança. Mas problemas relacionados a segurança das informações foram encontrados, e formas simples como utilização de senhas fortes e pode proporcionar um nível de segurança mais estável para o usuário.*

Palavras-*chave:* *Redes sem fio; Segurança; Senhas*.

1. Introdução

A utilização das redes sem fio está em expansão. Cada vez mais os usuários optam por este tipo de conexão, buscando comodidade e flexibilidade, e com o surgimento de equipamentos como *Notebooks*, celulares e outros, alguns estabelecimentos como bares, aeroportos, shoppings, estão investindo na implantação de redes sem fio, para que seus clientes tenham acesso à informação como se estivessem em casa, buscando a satisfação e a fidelização (KUROSE; ROSS, 2006).

A facilidade na implantação desta rede em relação às cabeadas é um ponto positivo para a instalação das mesmas tanto em meios corporativos como domésticos. Sem a necessidade de passagem de cabos este modelo acaba se tornando uma opção mais rápida. A flexibilidade é outra vantagem encontrada, sendo possível alterar ou adicionar estações na rede sem a necessidade de modificar o cabeamento (TANENBAUM, 1997).

A segurança é um ponto negativo encontrado nessas redes, pois o aumento da utilização deste modelo tornou os usuários alvo de pessoas mal intencionadas, onde estas buscam causar alguma instabilidade na rede, explorando vulnerabilidades encontradas como

configurações mal feitas em *Access Points* e senhas fracas. A utilização de senhas seguras é uma das formas de aumentar o nível de segurança das redes, acompanhada de configurações adequadas dos *Access Points* no momento da instalação dos equipamentos utilizados na rede.

2. Redes sem Fio

O crescimento das redes sem fio vem acontecendo de forma explosiva em todo mundo. Há algumas décadas a Internet era projeto de pesquisa, envolvia apenas dezenas de sites. Porém, seu crescimento foi estonteante e se tornou instrumento essencial na vida das pessoas, milhões de sites já existem fornecendo serviços e lazer para pessoas de todas as partes do mundo (COMER, 2001).

Os usuários desta ferramenta têm necessidade de informação e buscam cada vez mais comodidade e flexibilidade, com isso houve um grande aumento na procura de equipamentos móveis, como resultado essas ferramentas se tornaram mais populares e de fácil aquisição, porém para tornarem-se completamente portáveis há a necessidade da utilização de redes sem fio (TANENBAUM, 1997).

As redes sem fio oferecem a seus usuários mais comodidade e mobilidade que as redes cabeadas, porém a preocupação com segurança deve ser muito maior, já que seus dados trafegam por ondas eletromagnéticas por meio do ar.

A principal preocupação dos usuários está na configuração dos equipamentos e na escolha das senhas utilizadas, uma boa política de segurança também é importante, já que nelas são encontradas informações importantes para a saúde da rede, sendo elas direitos e deveres dos usuários, e algumas regras impostas pela organização.

3. Vulnerabilidades em redes sem fio

Este modelo de rede exige de seus usuários um cuidado maior que as cabeadas, pois acabam sofrendo os mesmos ataques encontrados nas redes cabeadas e alguns específicos foram inseridos (KUROSE; ROSS, 2006).

Apesar de os usuários estarem cada vez mais preocupados com a segurança de suas informações, e os fabricantes investirem cada vez mais em novas tecnologias para deixar seus equipamentos mais seguros, a realidade é que não existem redes completamente seguras, mas sim redes mais protegidas e difíceis de atacar.

Os ataques às redes sem fio geralmente ocorrem quando uma vulnerabilidade é explorada, juntamente com falhas nos fatores fundamentais da rede, como integridade e confiabilidade, sendo que alguns taques podem ser vistos na Tabela 1.

Tabela 2. Alguns ataques existentes para rede sem fio

Ataque	Descrição
Ataque de força bruta	Tem como objetivo desvendar a chave da rede com base em tentativas, usando uma forma dedutiva até que a senha real possa ser encontrada.
Ataque de dicionário	Desvenda a senha com auxilio de um arquivo de texto, também conhecido como *wordlist,* realizando a comparação da palavra existente no arquivo com os dados coletados nos pacotes que trafegam na rede.
Ataque de Vigilância	Tem caráter passivo, analisa os dados da rede para futuros ataques.
MAC Spoofing	O atacante realiza a troca da identificação da sua placa de rede pela do atacado, assim podendo usufruir dos recursos disponibilizados pela rede.

Algumas ferramentas também podem ser utilizadas para ataques nas redes, esses softwares realizam a identificação da rede, capturam dados que ali trafegam e também realizam os ataques para desvendar as chaves. A Tabela 2 mostra algumas informações sobre algumas dessas ferramentas.

Tabela 2. Ferramentas para ataques a rede sem fio

Ferramenta	Descrição
Aircrack	Um pacote de ferramentas com alguns softwares responsáveis pela captura dos pacotes que trafegam na rede e pela quebra da chave utilizada.
Kismet	Software responsável pela identificação e captura de pacotes que trafegam na rede, sendo necessário um outro software para que a chave seja desvendada.
WEPcrack	Captura dados importantes para que possam ser realizados futuros.
FakeAP	Este é um programa capaz de transformar um dispositivo de rede sem fio em um *Access Point*, falsificando algumas características que fazem com que o usuário pense estar conectado ao concentrador correto.

Os usuários devem utilizar algumas ferramentas e métodos para proteger sua rede dessas e outras vulnerabilidades existentes.

4. Segurança em redes sem fio

Cada vez mais a informática é vista como aliada da evolução econômica. Muitas empresas vêem nessas ferramentas uma forma de tornar o trabalho de seus funcionários mais fácil e rápido, assim tornando seu negócio mais competitivo (NAKAMURA, 2008).

As redes são fundamentais neste processo, tornando possível a ligação entre esses computadores. Sendo que as sem fio possuem um grande diferencial em relação às cabeadas, pois esta disponibiliza mobilidade e assim permite que os usuários possam encontrar mais liberdade no trabalho enquanto usam a rede e como resultado acabam produzindo mais e gerando mais lucros para a organização (NAKAMURA, 2008).

Com o aumento do interesse dos usuários em relação às conexões sem fio teve-se que aumentar as ferramentas para diminuir as vulnerabilidades que estas redes estão expostas. Uma das formas de manter uma rede segura esta em prevenir os ataques, já que sua área vulnerável é bem maior que a das redes cabeadas por ultrapassar o espaço físico, e com isso a dificuldade de controle de invasores é bem maior (RUFINO, 2005).

Segunda Sêmola (2003) algumas medidas de segurança devem ser tomadas para evitar ataques, elas podem ser vistas na Tabela 3.

Tabela 3. Medidas de Segurança

Medidas de Segurança	Descrição
Preventivas	Visam prevenir que ataques venham a ocorrer, para isso são realizadas palestras, treinamentos, entre outros.
Detectáveis	Analisam os focos que podem estar causando as ameaças.
Corretivas	Correção das estruturas buscando que se adaptem a política da Organização

Uma forma de aumentar a segurança dos dados que trafegam na rede é utilizando a criptografia. Com esta forma de proteção o tráfego de dados na rede é feito sem uma combinação lógica, tornando impossível seu entendimento imediato, assim se for atacado o invasor não terá acesso ao seu conteúdo.

O objetivo de se realizar a criptografia computacional é buscar:

a) sigilo dos dados: onde somente usuários autorizados possam ter acesso;

b) integridade: garantindo ao usuário que a informação esta está correta;

c) identidade do usuário: onde o sistema pode verificar a identidade do usuário ou do dispositivo que esta em contato.

Alguns protocolos de criptografia são utilizados para aumentar a segurança das informações em redes sem fio o WEP, o WPA e o WPA2, a ativação de um deles no *Access Point* é simples, porém é muito importante para aumentar o nível de segurança da rede.

4.1. Protocolo WEP

Este protocolo foi criado em 1999, utiliza algoritmos simétricos para realizar a cifragem de seus dados, sendo assim a chave deve ser compartilhada com todas as estações de trabalho e com o *Access Point*.

O protocolo WEP atua na camada de enlace, usa o algoritmo de criptografia *Ron's Code 4* (RC4), seu vetor de inicialização (IV) é de 24 bits e sua chave secreta compartilhada (*secret shared key*) é de 40 ou 104 bits, assim somando o IV com a chave secreta tem-se a chave de 64 ou 128 bits, o algoritmo *Cyclic Redundancy Check* (CRC-32) atua em conjunto e é utilizado para fornecer integridade quanto aos pacotes.

Um problema encontrado neste protocolo é que ele apresenta vulnerabilidades e por aceitar chaves com combinações pequenas de caracteres pode ter sua senha desvendada com facilidade utilizando um ataque de dicionário.

4.2. Protocolo WPA

Também conhecido como WEP2, foi criado em 2003 buscando corrigir vulnerabilidades encontradas no protocolo anterior. Esta versão é disponível para todos os equipamentos que continham o protocolo WEP, pois apenas uma atualização de *software* é necessária.

O protocolo WPA continua utilizando o algoritmo RC4, porém algumas melhorias foram encontradas como:

a) vetor de inicialização maior;

b) utilização de um novo código de verificação de integridade das mensagens (IV);

c) gerenciamento de chaves;

d) modo de autenticação corporativo e pessoal (doméstico).

Este protocolo ainda apresenta algumas vulnerabilidades, mas por exigir que suas senhas tenhas mais que oito caracteres torna suas chaves bem mais resistentes a ataques que o protocolo WEP.

4.3. Protocolo WPA2

O protocolo WPA2 ou 802.11i, foi lançado em 2004 com a proposta de extinguir os problemas encontrados nos protocolos anteriores. Este tem como diferencial utilizar o algoritmo de criptografia *Advanced Encryptation Standart* (AES) e o Temporal *Key Integrity Protocol* (TKIP) em conjunto, com uma chave de 256 bits, e com essa chave mais extensa torna este padrão mais eficiente. Este protocolo permite a utilização de chaves de 128, 192 e 256 bits. A certeza da integridade das mensagens é obtida por meio do algoritmo *Michael*

Message Integrity Check, que analisa se algum fator pode ter interferido na autenticidade da mensagem.

A vulnerabilidade está ligada ao tamanho da chave utilizada pelo usuário, da mesma forma que o WPA, se as senhas forem pequenas podem ser facilmente desvendadas por ataques de dicionário.

5. Senhas seguras

Uma das formas utilizadas para que a segurança em uma rede sem fio seja mais robusta é a utilização de senhas fortes, mas um significativo número de pessoas não sabe escolher ou ter os cuidados básicos para que a senha se torne à chave da sua segurança (WADLOW, 2000).

A criação de uma senha segura depende do bom senso do seu criador, levando em conta que há alguns anos uma senha segura era composta por seis dígitos, mas essa realidade mudou, com auxilio da evolução tecnológica muitas técnicas foram desenvolvidas e esse tipo de senha pode ser desvendada em poucos segundos, a indicação feita hoje é que as senhas tenham no mínimo 8 caracteres.

Segundo Alberto (2006) senhas que realmente são chaves de segurança somente são obtidas com a combinação de alguns fatores citados a seguir:

a) Não utilizar dados pessoais;

b) Dados que possam ser desvendados facilmente incluindo endereços, placa do

carro, número de documentos também são alvo fácil;

c) Nunca anote senhas em papéis, agendas ou algum lugar que outras pessoas possam ter acesso;

d) Senhas criadas a partir de palavras existentes em dicionários, tanto nacionais quanto estrangeiros podem ser desvendadas com ataques de dicionário;

e) Não utilizar senhas com apenas um tipo de caractere;

f) Nunca utilizar seqüências de dígitos do teclado;

g) Não utilize a mesma senha em lugares diferentes;

h) A troca das senhas deve acontecer regularmente;

Para auxiliar o usuário na escolha de suas senhas algumas técnicas podem ser utilizadas, e serão descritas na Tabela 4.

Tabela 4. Técnicas para criação de senhas

Técnica	Descrição
Geometria do teclado	Essa técnica pede que o usuário olhe para o teclado e imagine uma figura, então aperte as teclas correspondentes às linhas da figura.
Senhas pronunciáveis	Utiliza palavras que são pronunciáveis, mas que não existem em nenhum dicionário, tanto nacionais, quanto estrangeiros.
Caracteres “Alt”	Caracteres gerados quando se pressiona a tecla ALT e uma outra tecla, dando origem a um caractere especial que não está exposto no teclado.
Palavras em Conjunto	Realiza a junção de várias palavras pegando trechos diferentes de cada uma.
Geradas por software	Utiliza softwares disponíveis para que a senha seja criada, porém deve-se ter cuidado com esse tipo de senhas, pois por não ter nenhuma ligação com o usuário pode ser difícil lembrá-la.

6. Análise da segurança em redes sem fio

Algumas análises fora realizadas utilizando os protocolos disponíveis em redes sem fio, sendo eles WEP, WPA e WPA2. Para isso foi utilizado o Aircrack-ng, que é um pacote de softwares responsáveis pela captura e quebra de chaves. Essas quebras são realizadas por meio de ataque de dicionários e ataque de força bruta.

Para que a execução dos testes um ambiente foi projetado para que a captura dos pacotes pudesse ser feita sem apresentar riscos as redes encontradas ao alcance dos equipamentos, como pode ser observado na Figura 1.

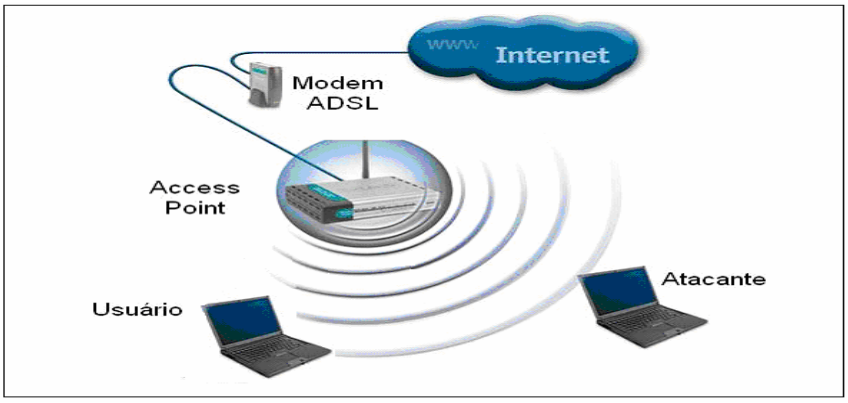


Figura 1. Ambiente utilizado para realização dos testes.

O primeiro passo para a realização dos testes é capturar os dados referentes à rede por meio do comando “iwlist scan” inserido no terminal.

Na seqüência utilizando o Airmon-ng, um dos softwares disponíveis no pacote Aircrack-ng, deve-se colocar a interface em modo monitor, utilizando o comando “airmon-ng start <nome da interface>”.

A captura dos pacotes que trafegam na rede também é realizada utilizando o Airodump-ng, por meio do comando “airodump-ng --channel 6 – w nomedopacote.cap mon0”. Esses dados serão responsáveis pelas informações necessárias para que a senha possa ser desvendada, no caso do protocolo WEP de 64 bits devem ser capturados aproximadamente 25.000 pacotes, e para os outros protocolos é indicado à captura de aproximadamente 50.000 pacotes.

A captura dos pacotes depende do fluxo de dados que estão trafegando na rede, ou seja, quanto mais pacotes estão sendo enviados e recebidos mais rápido será a captura dos pacotes necessários para que a tentativa de quebra possa ser realizada.

A Figura 2 mostra a captura dos pacotes sendo realizada em rede que utiliza o protocolo WEP.

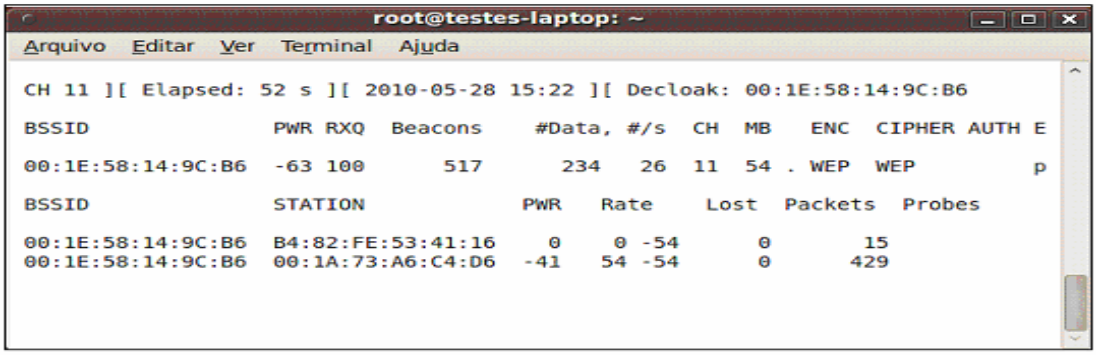


Figura 2. Captura dos pacotes utilizando o Airodump-ng com a presença do WEP

Em capturas que os protocolos WPA e WPA2 estão presentes é necessário a captura do *handshake*, que é uma espécie de acordo de comunicação dos equipamentos, onde está armazenada a criptografia utilizada na rede. Essa informação é obtida por meio do comando "aireplay-ng -0 5 -a MAC do AP -c MAC do cliente <interface>" inserido em outro terminal aberto no momento em que a captura dos pacotes está sendo realizada. Este comando força o usuário a fazer novamente a autenticação na rede, permitindo que a chave fique registrada nos pacotes que estão sendo capturados.

A Figura 3 mostra a captura de pacotes com o protocola WPA e o *handshake* já capturado.

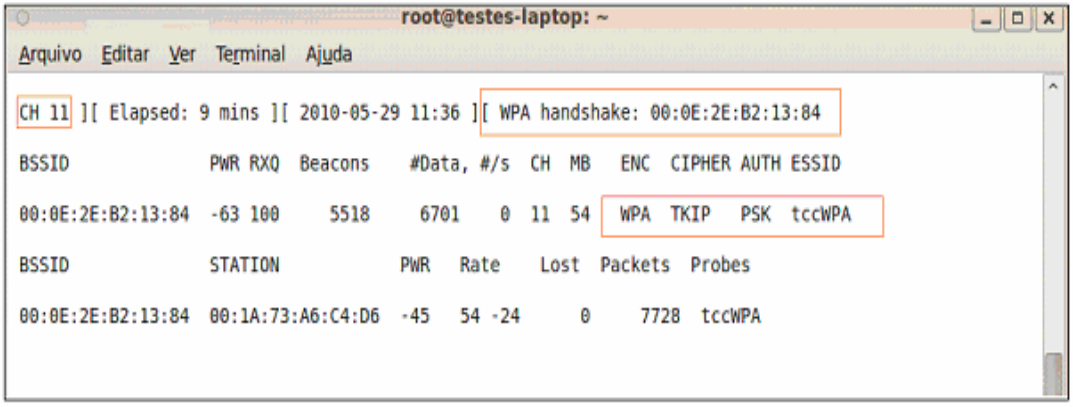


Figura 3. Captura dos pacotes utilizando o Airodump-ng com a presença do WPA

Após a captura dos pacotes a tentativa de quebra pode ser realizada utilizando o *software* Aircrack-ng inserindo o comando no terminal, no caso de quebra de chaves que tem a proteção WEP deve-se inserir o código "aircrack-ng nomedopacote.cap", que efetua a quebra por meio de ataque de força bruta. Em caso de chaves que utilizam os protocolos WPA e WPA2 o comando a ser inserido é "aircrack-ng -w nomedodicionario nomedopacote.cap".

A Figura 4 mostra a tentativa de quebra com sucesso de uma chave WEP de 128 bits, onde a chave foi desvendada em apenas sete segundos.

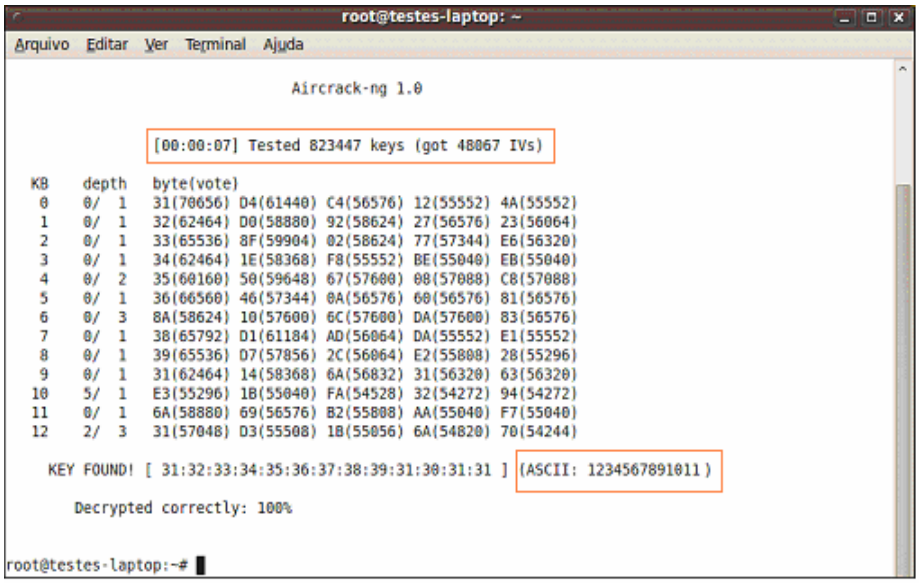


Figura 4. Quebra com sucesso de uma chave com protocolo WEP de 128 bits

Vários testes foram realizados alguns com resultados positivos para quebra outros não. Mais sobre esses resultados poderá ser observado a segui dicionário.

7. Resultados Obtidos

Por meio da pesquisa desenvolvida e dos testes realizados pode-se observar a fragilidade do protocolo WEP, que mesmo utilizando senhas bem elaboradas tem suas chaves quebradas facilmente com a utilização de ataques de força bruta. Como pode ser observado na Tabela 5. Com isso, deve-se sempre que possível evitar o uso desse protocolo, independente de a chave ser de 64 ou 128 bits, para evitar que suas vulnerabilidades comprometam a segurança da rede.

Tabela 6. Resultados obtidos nos testes realizados

Protocolo	Chave	Tempo de Análise	Gerada por Software	Quebra da Senha
WEP 64 bits	12345	00:04	Não	Sim
WEP 64 bits	yJ(M9	00:04	Não	Sim
WEP 64 bits	A@q~2	00:04	Sim	Sim
WEP 128 bits	1234567891011	00:07	Não	Sim
WEP 128 bits	An@P@^!?25Cl3	00:10	Não	Sim
WEP 128 bits	Ry&@74Nm[g*%Y	00:52	Sim	Sim
WPA	teste12345	03:28	Não	Sim
WPA	An@P@^!?&Cl3d150n	12:04	Não	Não
WPA	P8=3CK+?F=)t\8E	14:07	Sim	Não
WPA 2	1234567891011	06:23	Não	Sim
WPA 2	A1?B2!c3	06:52	Não	Sim
WPA 2	An@P@^!?&Cl3d150n	11:25	Não	Não
WPA Mixed	copadomundo	04:50	Não	Sim
WPA Mixed	An@P@^!?&Cl3d150n	10:43	Não	Não

O protocolo WPA e WPA2 são opções mais aconselháveis aos usuários, pois mesmo apresentando algumas vulnerabilidades se mostram muito mais eficientes que o protocolo WEP. Sendo que quando utilizadas senhas bem elaboradas e com tamanhos significativos possibilitam que a rede alcance um nível desejável relacionado a segurança, pois neste ataque a senha só será desvendada se a senha da rede estiver contida no dicionário utilizado no momento do ataque.

Configurações adequadas e bem feitas nos equipamentos desde o momento da instalação também podem ajudar a elevar o índice de segurança da rede, bem como o cumprimento das normas estipuladas na política de segurança existente na organização, pois não existe um a maneira de criar uma rede sem fio completamente segura, mas todos as ações tomadas para dificultar invasões e aumentar a segurança da mesma ajudam para que se torne uma rede com um alto nível de segurança.

8. Conclusão

Este artigo apresentou os testes realizados para que uma análise da segurança em redes sem fio pudesse ser realizada, medindo a confiabilidade dos protocolos disponíveis para redes sem fio. Tendo como resultado a ineficiência do protocolo WEP diante de ataques de força bruta devido à utilização de chaves com poucos caracteres.

Uma atenção especial foi dada para as senhas, pois elas podem ser uma forma muito eficaz de evitar ataques as *wireless*, pois é uma tarefa muito difícil garantir a segurança de informações que trafegam pelo ar. Sendo assim o usuário deve se empenhar e aplicar as sugestões dadas neste trabalho buscando aumentar o nível de segurança da rede.

Sendo que a eficiência dos protocolos WPA e WPA2 só é alcançada quando explorada a capacidade de aceitar senhas com mais de oito caracteres, por isso para aumentar o nível de segurança da rede não basta apenas ativar um bom protocolo, mas sim utilizar uma senha que não possa ser desvendada de forma fácil.

Referências

ALBERTO, F et al. **Segurança da Informação**. Curso de Sistemas de Informação, Sociedade Paranaense de Ensino e Informática. Dez, 2006.

COMER, Douglas E. Redes de computadores e internet: abrange transmissão de dados, ligação inter-redes e web. 2.ed Porto Alegre: Bookman, 2001.

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet: uma abordagem top-down. 3. ed São Paulo: Pearson Addison Wesley, 2006.

WADLOW, Thomas A. Segurança de redes: projeto e gerenciamento de redes seguras. Rio de Janeiro: Ed. Campus, 2000.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de Redes em

Ambientes Cooperativos. São Paulo: Novatec, 2008

RUFINO, Nelson Murilo de Oliveira. Segurança em Redes Sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec, 2005.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

TANENBAUM, Andrew S. Redes de computadores. 4 ed. Rio de Janeiro: Campus, 2003.