UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FLÁVIO WESLER DE COSTA

ANÁLISE DE PADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11

CRICIÚMA, JULHO DE 2009

FLÁVIO WESLER DE COSTA

ANÁLISE DE PADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11

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

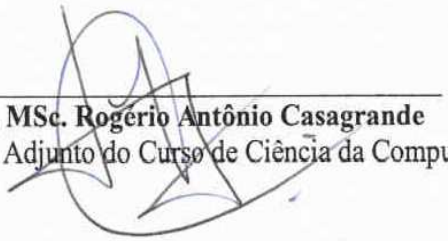
Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, JULHO DE 2009

FLÁVIO WESLER DE COSTA

ANÁLISE DE PADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11

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.

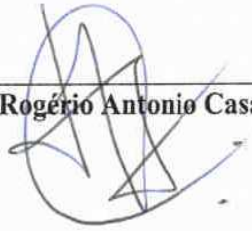


Prof. MSc. Rogério Antônio Casagrande
Coordenador Adjunto do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. MSc. Ricardo Portes (SERPRO)



Prof. MSc. Rogério Antonio Casagrande (UNESC)

Dedico esta conquista aos meus pais e irmãos, pois sempre me incentivaram, mostrando que o estudo é a chave para o sucesso.

AGRADECIMENTOS

Primeiramente agradeço a Deus pela força e sabedoria que me foi dada no decorrer desse trabalho.

Agradeço essa conquista aos meus pais Valdelar e Erica pelo incentivo, não só nessa etapa de conclusão, mas durante todo o curso. Sem esse incentivo nada disso seria possível. Também agradeço esta vitória a meus irmãos Fernando e Patrícia que, apesar de algumas intrigas, me ajudaram no decorrer de todo o curso.

Ao meu orientador Paulo João Martins por ter me direcionado para que esse trabalho pudesse ser bem sucedido.

A minha tia Elaine que me auxiliou na correção ortográfica e normas da ABNT.

Não posso deixar de agradecer a todos os meus amigos que no decorrer desta vida acadêmica sempre me ajudaram nos momentos difíceis, dando incentivo e conselhos para que não olhasse para trás, fazendo-me acreditar que este momento chegaria.

“Eu aprendi que para se crescer como pessoa é preciso me cercar de gente mais inteligente do que eu.”

William Shakespeare

RESUMO

A informação no mundo atual tem um papel fundamental na vida das pessoas e empresas, o seu uso estratégico acaba sendo um diferencial na competitividade e sobrevivência das mesmas. Devido a essa importância da informação existe uma necessidade de atualização constante, fazendo com que essas pessoas estejam conectadas aonde quer que estejam. Mediante isso, a tecnologia das redes sem fio é uma realidade que vem crescendo de forma considerável, tanto no uso corporativo como no uso doméstico. Esse crescimento se dá devido a mobilidade e agilidade que as redes sem fio proporcionam. O grande problema das redes sem fio está relacionado à segurança dessas informações. Esse trabalho teve o objetivo de realizar um estudo sobre a análise e padrões dos protocolos de segurança de redes sem fio WEP, WPA e WPA2 de forma a avaliar o seu grau de vulnerabilidades dentro do padrão 802.11, visto que os mesmos apresentam falhas de implementação e na forma de utilização. Foram definidos cenários para realizar os testes de captura e descoberta de senhas, SSID, MAC, entre outros. O resultado foi o projeto de um guia de boas práticas e recomendações acerca da segurança em redes sem fio.

Palavras-Chave: Segurança; Redes sem fio; Criptografia; Padrão 802.11.

ABSTRACT

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DAS SIGLAS

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
ATM	Asynchronous Transfer Mode
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CRC	Cyclic Redundancy Check
DHPC	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
FMS	Fluhrer, Mantin e Shamir
GHz	Giga Hertz
HDSL	High bit rate digital Subscriber Line
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Initialization Vector
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
Mbps	Megabytes por segundo

MIC	Message Integrity Code
MIMO	Multiple Input, Multiple Out
OFMD	Orthogonal frequency-division multiplexing
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistants
PPP	Point to Point Protocol
PRNG	Pseudo Random Number Generator
PSK	Pre Shared Key
RC	Ron's Code ou Rivest Cipher
RSN	Robust Security Network
SDSL	Symetric Digital Subscriber Line
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
DSL	Digital Subscriber Lines
XOR	eXclusive OR
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access versão 2

WWiSE World Wide Spectrum Effciency

SUMÁRIO

1 INTRODUÇÃO

O avanço tecnológico, aliado à vida moderna, exige do homem atual mobilidade, agilidade e liberdade. Ele precisa cada vez mais comunicar-se aonde quer que esteja. Por essa razão, os dispositivos móveis, tais como telefones celulares, notebooks, PDAs e outros, têm se tornado mais comuns no mercado, pois, além de atender às necessidades atuais, apresentam uma significativa diminuição nos seus custos.

Desse modo, as redes sem fio (*wireless networks*) vêm crescendo de maneira rápida. Trabalhar livremente dentro do ambiente corporativo na posse de um PDA ou notebook conectado a redes sem fio já é uma realidade em várias empresas no Brasil.

Rufino (2005) ressalta que a mobilidade permite que dispositivos dentro de uma empresa possam permanecer conectados, sem perda de acesso aos sistemas e dados da rede. A flexibilidade que esse ambiente proporciona diz respeito à facilidade que os dispositivos têm de acessar a rede sem a utilização de uma estrutura física de cabos, ampliando, assim, a produtividade do funcionário. Isso faz com que processos de negócios aconteçam mais rapidamente e de forma mais eficiente, além da possibilidade de que novos processos de negócios aconteçam na totalidade.

Dias (2002) relata que devido ao crescimento e à popularização dessas redes, um desafio para a comunicação sem fios são as questões referentes à segurança. Uma rede sem fio é muito vulnerável a ataques, possui algumas falhas, que são exploradas geralmente por curiosos e intrusos, muitas vezes conhecidos como *hackers*.

Cuidar das informações que trafegam por essas redes sem fio é essencial, pois são informações muito pertinentes à vida da empresa. Em posse de concorrentes ou pessoas mal intencionadas podem causar sérios problemas à empresa.

Segundo Soares (2004) o padrão IEEE 802.11 destaca-se das demais opções de acesso móvel por sua elevada popularidade, pelas altas taxas de transmissão de dados que oferece e pelo custo relativamente baixo.

No padrão 802.11 existem os protocolos de privacidade *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA) e *IEEE* 802.11i (WPA2) que buscam nas redes sem fio a mesma privacidade obtida em redes cabeadas. Esses protocolos são uma forma de proteção dos usuários autorizados contra eventuais ataques de interceptação de sinal. Porém, apresentam algumas vulnerabilidades que podem ser prejudiciais à segurança.

Neste contexto, o trabalho em questão baseia-se na necessidade de se pesquisar as vulnerabilidades, documentar técnicas de proteção, implementar essas técnicas e, por fim, realizar testes para analisar se a segurança está de acordo com as técnicas implementadas no ambiente que utiliza rede sem fio.

É muito importante que todo ambiente sem fio tenha alguma técnica de proteção para evitar manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

1.1 OBJETIVO GERAL

Pesquisar, analisar, implementar e testar as técnicas de segurança no padrão IEEE 802.11, utilizando os protocolos *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA) e *IEEE* 802.11i (WPA2), documentando as vulnerabilidades e respectivas técnicas de correção.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são:

a) destacar a importância da segurança das informações;

b) identificar as características e funcionalidades do padrão IEEE 802.11;

c) pesquisar a segurança dentro do padrão IEEE 802.11;

d) desenvolver estudo de caso, utilizando segurança dentro do padrão IEEE 802.11;

e) analisar as características, vulnerabilidades, e sugerir técnicas de segurança dos protocolos WEP, WPA e WPA2;

f) implementar técnicas de segurança nos protocolos WEP, WPA e WPA2;

g) testar, por meio de softwares, a segurança implementada no ambiente sem fio;

h) documentar os resultados dos testes.

1.3 JUSTIFICATIVA

As redes sem fio vêm se destacando no mercado de maneira rápida, e um item que deve ser levado em consideração é a segurança da informação que trafega nessas redes.

Segundo Menezes (2007) a segurança é um item que deixa a desejar, o que acaba classificando uma rede sem fio como ruim. Porém, muitas vezes o que há é um

descuido nas políticas de segurança e implementação ou falta de uma técnica de segurança no ambiente sem fio.

O protocolo WEP possui problemas administrativos e técnicos. Um deles é relacionado ao fato de se utilizar uma chave única e estática compartilhada entre todos os dispositivos da rede. Caso a mudança dessa chave seja necessária, o processo é trabalhoso e algumas vezes inviável, principalmente no que diz respeito a provedores. Outro problema refere-se ao algoritmo que é passivo a ataques (SOARES, 2004).

Em 2001 foram executados testes utilizando o programa chamado *AirSnort*, que roda em ambientes *Linux*, e em segundos pôde-se determinar a chave do protocolo WEP (VERÍSSIMO, 2002).

O WPA foi criado com objetivo de corrigir todos os problemas do WEP, antecipando as melhorias que seriam implementadas pelo protocolo IEEE 802.11i (WPA2). No entanto, ele também contém vulnerabilidades e é passivo de ataques. Segundo Rufino (2005) a principal vulnerabilidade do protocolo WPA é a utilização do método de autenticação PSK. A autenticação PSK consiste em uma senha pré-compartilhada pelos usuários da rede. Essa senha é utilizada pelo ponto de acesso para obter as chaves de criptografia e deve ser digitada nas máquinas dos usuários para que obtenham acesso sem a necessidade de um servidor. Porém, um atacante poderá usufruir de ataques de dicionário por meio da captura passiva de tráfego da rede. Pelo fato da maioria dos usuários utilizarem senhas fracas, fica fácil quebrar a senha.

Percebe-se que o nível de vulnerabilidade em redes sem fio é bastante intenso. Diante das situações expostas, sente-se a necessidade de se realizar um estudo das principais vulnerabilidades no padrão 802.11 e protocolos WEP, WPA e WPA2.

Esse trabalho tem o objetivo de analisar os protocolos de segurança dentro do padrão 802.11, pesquisar as vulnerabilidades e técnicas de proteção das mesmas nos

protocolos WEP, WPA e WPA2, contribuindo, assim, para escolha e implementação da técnica de proteção mais adequada à necessidade que se busca.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por sete capítulos voltados para a segurança em ambientes sem fios 802.11, distribuídos em:

a) **introdução:** apresenta ao leitor o objetivo do trabalho, fazendo uma abordagem panorâmica do trabalho;
b) **tecnologia das redes:** aborda os principais tipos de redes utilizadas atualmente, descrevendo algumas características de cada uma;
c) **redes sem fio:** explica de forma detalhada o que é e como funciona uma rede sem fio;
d) **segurança em redes sem fio:** mostra o funcionamento e as características da segurança da informação em uma rede sem fio;
e) **protocolos para redes sem fio:** nesse capítulo os protocolos criptográficos WEP, WPA e WPA2 serão definidos e comparados detalhadamente, levando em consideração a confiabilidade, integridade, autenticidade e vulnerabilidades;
f) **trabalhos correlatos:** serão descritos alguns trabalhos sobre segurança em redes sem fios que foram realizados com os mesmos objetivos;
g) **validação dos protocolos WEP, WPA e WPA2:** completando o trabalho, esse capítulo apresenta o desenvolvimento de testes práticos sobre os protocolos, a fim de validá-los.

2 TECNOLOGIA DE REDES

As redes de computadores são parte do cotidiano de muitas pessoas e empresas de todo mundo. Desde as primeiras experiências, na década de 60, até os dias de hoje, as tecnologias de comunicação entre computadores evoluíram substancialmente (TANEMBAUM, 2003).

A facilidade de comunicação proporcionada pela Internet tem modificado o cenário de escritórios, fábricas, escolas e residências. Este cenário se torna cada vez mais interessante a partir da evolução das tecnologias para interligar pontos remotos. Nakamura e Geus (2003) destacam que a busca crescente por comunicação aliada à facilidade, comodidade e praticidade, culminou na popularização de tecnologias de rede sem fio.

De acordo com Tanenbaum (2003) estas tecnologias se utilizam de ondas de rádio para a transmissão dos dados, ou seja, todas as informações são transmitidas por meio do ar, meio este que pode ser facilmente interceptado por terceiros.

Do ponto de vista da abrangência, as redes de computadores podem ser classificadas em quatro grandes grupos: *Wide Area Network* (WAN), *Metropolitan Area Network* (MAN), *Local Area Network* (LAN) e *Wireless Local Area Network* (WLAN).

2.1 *LOCAL AREA NETWORK* - LAN

Mais conhecida como rede local, tem como finalidade a troca de dados entre estações de trabalho, servidores, dispositivos de rede (roteadores, *switches*, *bridges*, placas de rede, pontos de acesso, entre outros) e protocolos de comunicação. É

denominada local por cobrir áreas de até dez quilômetros, quando passa a ser denominada WAN.

2.*2 WIDE AREA NETWORK* - WAN

WAN é uma rede de longa distância que abrange uma grande área geográfica. Surgiu quando as LANs se tornaram inviáveis às empresas em crescimento que necessitavam de um serviço de qualidade que atendesse à demanda de informações por toda a área geográfica de suas unidades de negócio.

2.3 *METROPOLITAN AREA NETWORK* - MAN

Denominada uma rede de área metropolitana, a rede MAN pode abranger toda uma cidade, e dentro de uma distância determinada podem interligar diversos escritórios (LANs) de uma mesma empresa.

2.4 *WIRELESS LOCAL AREA NETWORK* - WLAN

Rede de área local sem fio que faz conexão por meios de ondas de rádio. Inicialmente, devido ao alto custo, surgiu apenas em aeroportos, universidades, alguns principais lugares públicos e em demais LANs, onde era difícil o acesso por cabo.

Com a redução dos custos e ainda com a padronização dos protocolos de comunicação, que dificultavam a compatibilidade entre dispositivos, as WLANs estão bem mais próximas de usuários domésticos (NAKAMURA; GEUS, 2003).

A conexão destas redes é realizada por meio de um *access point* (ponto de acesso) ligado ao *hotspot* (estação base) como, por exemplo, um *laptop,* que recebe a conexão por ondas de rádio liberadas pela antena do *access point* e então estabelece conexão com a rede.

2.5 A INTERNET E O IMPACTO SOCIAL

É notável que nos últimos anos a informática revolucionou a sociedade em diversos aspectos. Empresas puderam se aproximar cada vez mais de seus clientes, parentes distantes podem se comunicar gratuitamente por meio da Internet, equipamentos foram rapidamente ultrapassados, força bruta foi substituída por máquinas, entre tantas outras mudanças.

Nakamura e Geus (2003) retratam todas essas mudanças, dando ênfase aos aspectos e relações com o novo valor da informação, formas de armazenagem, transmissão, compartilhamento, disponibilidade, sobre a ótica da Segurança da Informação. Devido à popularização da Internet, o dia-a-dia da população vem se transformado em um constante aprendizado. Em poucos anos, de artigo de luxo, os computadores passaram a ser equipamentos indispensáveis em lojas, fábricas, empresas e até mesmo em casas, de qualquer classe social.

Entretanto, junto com tamanha mudança e transformação, o meio eletrônico tornou-se alvo de ataques dos mais variados tipos, e infelizmente, segundo o CERT.BR (2008), o Brasil tem um índice extremamente elevado de incidentes reportados.

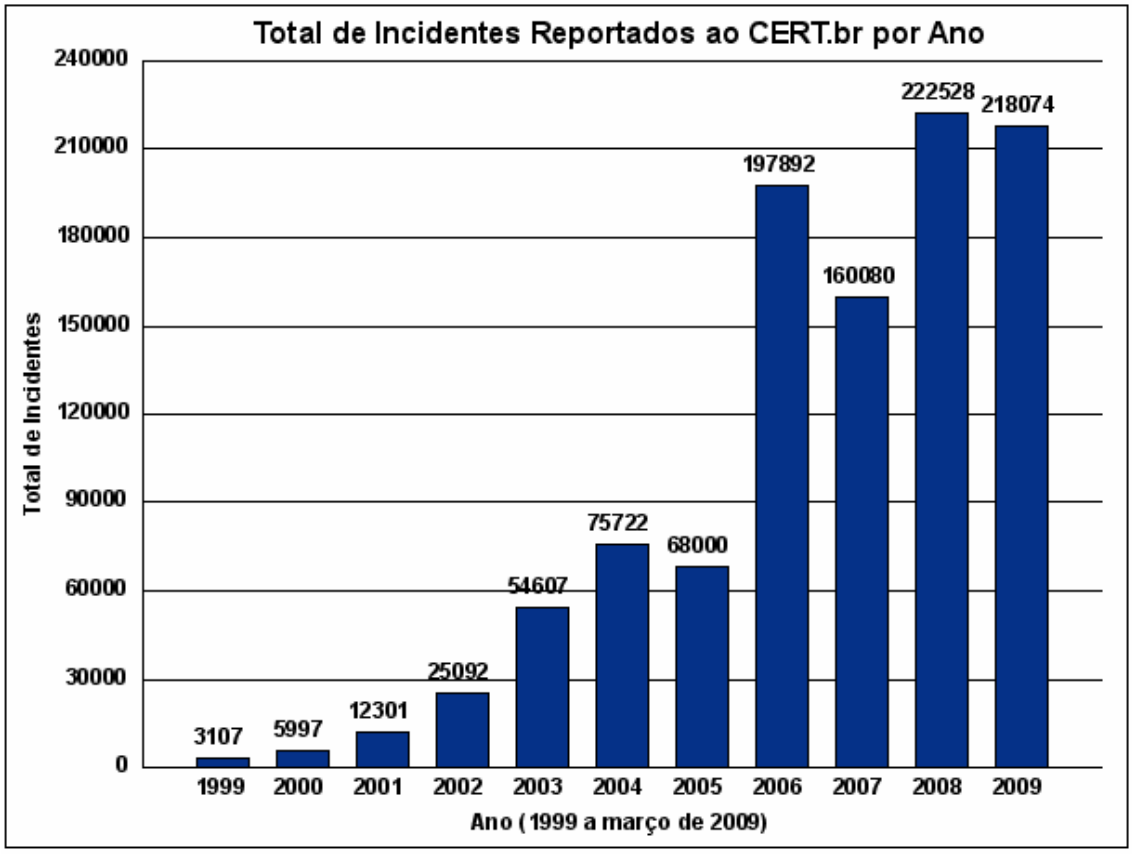


Figura 1. Incidentes reportados por ano ao CERT.br
Fonte: CERT.br (2009)

3 REDES SEM FIOS

Nakamura e Geus (2003) retratam que as redes de computadores, apesar de oferecerem uma mobilidade até então nunca vista, acabam por esbarrar num obstáculo relativamente simples, em se tratando de movimentação: os cabos.

Durante anos um dos maiores problemas dos usuários era passar informações de um computador para outro. Eram necessários disquetes e outros meios, os quais não tinham praticidade nenhuma. Com o advento das redes, essa troca de informações passou a ser algo extremamente fácil.

A partir daí a dificuldade passou a ser outra, principalmente com a explosão no número de *notebooks*; o mercado passou a exigir uma mobilidade ainda maior. As pessoas, acostumadas com telefones sem fio, os celulares, passaram a exigir que em suas conexões também não fosse necessário o uso de cabos. Perante esse cenário, surgiram às redes sem fio.

3.1 VISÃO GERAL

Redes sem fio são redes de computadores na qual não se utilizam a infra-estrutura convencional dos cabos, cujo “os dados são modulados na portadora de rádio e transmitidos por meio de ondas eletromagnéticas” (SILVA, 1998, p. 34). Tais redes têm como grande vantagem a mobilidade que elas oferecem a seus usuários, uma vez que não existe a barreira de movimentação imposta pelos cabos.

Segundo Tanenbaum (2003) as ondas eletromagnéticas são formadas por íons em movimento. O número de oscilações dessas ondas é chamado de freqüência, e é

medido em Hertz (Hz). O Espectro eletromagnético varia entre ondas de rádio e raios gama, entre 10^{o} e 10^{24}Hz.

As redes sem fio se utilizam de freqüências que variam entre 2,4 x 10^{7} e 5 x 10^{7}, sendo classificadas como ondas de rádio, conforme a Figura 2.

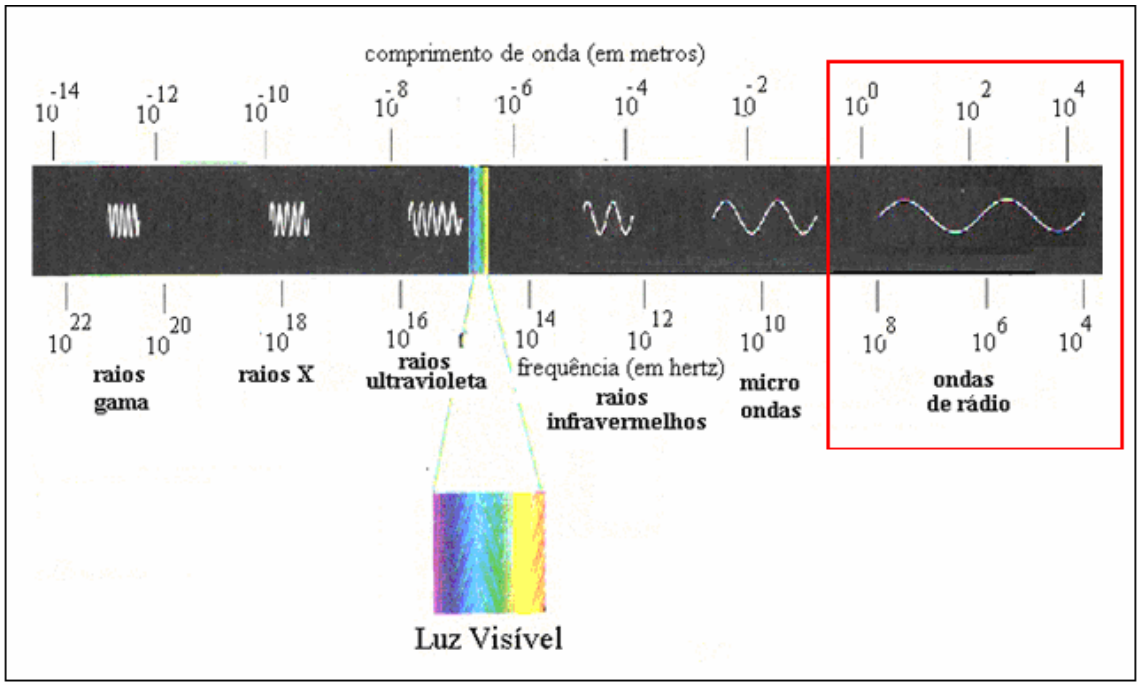


Figura 2. Espectro eletromagnético.
Fonte: EDUCAR (2008)

3.2 PADRÕES

As redes sem fio para computadores já existem há vários anos. Entretanto, por não haver quaisquer restrições, as empresas que fabricavam equipamentos para este tipo de rede, não seguiam um padrão, tornando equipamentos de marcas diferentes incompatíveis entre si.

Em meados da década de 90 os fabricantes decidiram, então, que a melhor maneira para disseminar as redes sem fio entre os usuários seria criando especificações de fabricação, possibilitando, assim, que quaisquer equipamentos conseguissem se comunicar.

Respeitada internacionalmente, a IEEE foi eleita para a criação da norma, uma vez que já havia normatizado as redes com fios. Seguindo, então, as normas já existentes, a IEEE aprovou, em 1997, a norma 802.11, específica para redes sem fio.

A norma 802.11 conta com protocolos criados com intuito de solucionar os mais diversos problemas, tais como: melhorar a qualidade de sinal, aumentar a velocidade de transmissão, ou deixar as redes sem fio mais seguras. Os principais padrões, segundo a IEEE (2008) são: 802.11a; 802.11b; 802.11g; 802.11i e 802.11n.

3.2.1 Padrão 802.11a

Com a intenção de sanar os problemas antes encontrados nos padrões 802.11 e 802.11b foi criado o padrão 802.11a, com uma velocidade maior, chegando ao máximo de 54 Mbps (de 72 a 108 Mbps por fabricantes não padronizados), podendo, também, operar em velocidade mais baixas. Trabalha numa faixa de 5GHz, que tem como vantagem poucos concorrentes, porém com menor área de alcance. Para esse padrão são permitidos 64 clientes conectados por AP.

O tipo de modulação padrão consiste de 12 canais não sobrepostos disponíveis, diferente dos 3 canais livres disponíveis nos padrões 802.11b e 802.11g, o que permite cobrir uma área maior e mais densamente povoada, em melhores condições que outros padrões.

Há, no entanto, uma desvantagem relacionada à expansão: a falta de compatibilidade com a base instalada em relação ao padrão 802.11b, pois esta utiliza faixas de freqüência diferentes.

3.2.2 Padrão 802.11b

Esse padrão, primeiro a ser definido pelo comitê, permite 11 Mbps de velocidade de transmissão máxima, podendo também comunicar-se com velocidades mais baixas como 5.5, 2 Mbps ou mesmo 1 Mbps. Todavia, por trabalhar numa banda mais baixa, pode sofrer mais interferências de outros tipos de fontes quaisquer, como por exemplo, celulares, fornos de microondas e dispositivos *Bluetooth*, entre outros, que trabalham na mesma faixa de 2,4GHz. São permitidos, no máximo, 32 clientes conectados por AP. Mesmo tendo limitações na utilização de canais, hoje é ainda o padrão mais popular no mundo e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponível, devido ao baixo custo com a banda gratuita. Na Tabela 4 apresentada abaixo é demonstrada a associação entre canal e a respectiva freqüência:

Tabela 1. Associação entre Canal e Respectiva Freqüência.

Canal	Freqüência
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Fonte: RUFINO, N. (2005)

3.2.3 Padrão 802.11g

Incorporando várias características boas dos padrões 802.11a e 802.11b, além de utilizar também modulação OFDM e velocidade de até 54 Mbps, esse padrão tem como principal vantagem sobre os outros a utilização da faixa de 5GHz por ter menor atenuação. Como desvantagem, possui incompatibilidade com dispositivos de diferentes fabricantes.

Por trabalhar na mesma faixa do padrão 802.11b (2,4 GHz), permite que equipamentos de ambos os padrões (b e g) possam interoperar no mesmo ambiente, possibilitando evolução menos traumática do parque instalado, mesmo que isso implique numa diminuição da sua taxa.

3.2.4 Padrão 802.11i

Padrão que tem por vantagem um protocolo de segurança chamado *Robust Security Network* (RSN), permitindo que os meios de comunicação sejam mais seguros que os difundidos atualmente. Criado em junho de 2004, esse padrão destaca-se pelos mecanismos de autenticação e privacidade. Também possui o protocolo *Wi-Fi Protected Access* (WPA), que foi desenhado para prover soluções mais robustas, em relação ao padrão *Wired Equivalent Privacy* (WEP).

3.2.5 Padrão 802.11n

Esse padrão também é conhecido como *World Wide Spectrum Efficiency* (WWiSE) e tem por finalidade o aumento da velocidade que varia de 100 Mbps até 500

Mbps, permitindo a distribuição de mídias e a compatibilidade retroativa com os padrões já existentes.

O padrão opera na faixa de 2,4 GHz e 5 GHz, podendo trabalhar com canais de 40 MHz e manter compatibilidade com os 20 MHz atuais. Nesse caso, as velocidades máximas oscilam em torno de 135 Mbps. Com pouca diferença dos padrões atuais, destaca-se por uma modificação de OFDM conhecida como *Multiple Input, Multiple Out-OFDM* (MIMO-OFDM) que traz maior eficiência na propagação do sinal e ampla compatibilidade reversa com demais protocolos.

3.3 ACESSO A REDES SEM FIO

Para obter acesso a uma rede sem a utilização de fios são necessários equipamentos específicos da tecnologia sem fio. Esses equipamentos são fabricados de acordo com os padrões da IEEE para que possam ser compatíveis com protocolos criptográficos, como por exemplo, WEP e WPA.

3.3.1 Ponto de Acesso - *Access Point*

Principal componente que efetua a conexão de redes com e sem fios, é ligado à rede cabeada por meio de sua conexão RJ-45, criando uma região que dá acesso sem fio a computadores com placa de rede sem fio.

Os pontos de acesso podem operar no padrão 802.11a, 11b ou 11g. Em alguns casos, o aparelho é compatível com mais de um padrão. Essa transmissão é feita por meio de um sinal com uma, duas e até por três antenas, como o exemplo nas Figuras 3 e 4.

Figura 3. Exemplo de aparelho de Ponto de Acesso com uma e duas antenas.
Fonte: TRADESYS (2008)

Figura 4. Exemplo de aparelhos de Ponto de Acesso com três antenas.
Fonte: D-LINK (2008)

Usuários acessam a internet por meio de redes residenciais ou comerciais utilizando computadores, *notebooks*, PDAs, entre outros, equipados com as placas de comunicação sem fio e um dispositivo centralizador, que é o próprio AP.

3.3.2 Cartão de rede Wi-Fi

Grande parte dos *notebooks* comercializados na atualidade inclui um adaptador de rede Wi-Fi para que se possa ter acesso a uma rede sem fio nos padrões 802.11 a/b/g. A antena tanto pode ficar embutida no *notebook*, normalmente ao lado da tela de cristal líquido, quanto em cartões PCMCIA.

3.3.3 Placa de rede PCI Wi-Fi

Não só *notebooks* podem fazer parte de uma rede sem fio. Existem placas de rede PCI Wi-Fi que atendem à necessidade de computadores *desktop*. Essas placas possuem uma chapa metálica que isolam os circuitos internos de radiofreqüência, evitando que interfiram no funcionamento do equipamento e também que sofram interferência gerada pelos circuitos do mesmo. Possuem, também, uma antena dobrável de encaixe que pode ser conectada ao dispositivo após ser instalado.

Figura 5. Placa PCI Wi-Fi
Fonte: D-LINK (2008)

3.3.4 Roteador Sem Fio

Aparelho que, ligado a um dispositivo com acesso à Internet, pode compartilhar o uso por meio de uma porta *etherne*t. É considerado um roteador de banda larga que inclui a função de *access point*. Existem, ainda, roteadores de banda larga sem fio que possuem conexões paralelas e USB, e conexão RJ45 para computadores sem placa de rede Wi-Fi.

Figura 6. Roteador sem fio
Fonte: LINKSYS (200)

4 SEGURANÇA EM REDES SEM FIO

Este capítulo aborda diversos assuntos relacionados à segurança em redes sem fio, como o funcionamento de redes sem fio, criptografia e segurança da informação, com embasamento teórico de diversos autores, especialistas nos referidos assuntos.

4.1 SEGURANÇA DA INFORMAÇÃO

Seguindo as novas tendências de mercado, muitas organizações passaram a fazer uso de infra-estruturas computacionais e comunicação para facilitar seus processos organizacionais, internos e externos.

A informação passou a ser armazenada e manipulada em segmentos eletrônicos e muitas dessas organizações passaram a se preocupar com a sua segurança.

De acordo com Cheswick, Bellovin e Rubin (2005) tendo em vista que a informação tornou-se o maior bem da humanidade, fica clara a necessidade de estabelecer normas e boas práticas para garantir seu uso de forma íntegra e confiável. Qualquer natureza de vazamento contendo dados de clientes ou conhecimentos desejados por concorrentes acarreta prejuízos imensuráveis.

A segurança da informação foi criada baseando-se no conceito de realizar métodos de proteção contra acessos não autorizados, alterações indevidas ou indisponibilidade de ativos. Esta área de pesquisa tem como objetivo proteger a informação durante seu ciclo de vida, ou seja, durante a manipulação dos dados, armazenamento, transporte e descarte, seja ela na forma impressa, escrita, eletrônica, ou até mesmo falada.

4.1.1 Pilares da Segurança

A bibliografia focada em Segurança da Informação cita, quase em sua totalidade, a utilização de três pilares que formam a base de sustentação para a segurança da informação: confidencialidade, integridade e disponibilidade.

4.1.1.1 Confidencialidade

Segundo Ferreira e Araújo (2006) a confidencialidade consiste em limitar o acesso à informação somente àqueles que estão autorizados pelo proprietário da informação.

Controles de acesso por meios de autenticação e até mesmo um protocolo de criptografia de dados implementado pode garantir um nível adequado de confidencialidade.

4.1.1.2 Integridade

A integridade tem como função primária a garantia de que a informação manipulada mantenha todas as características de origem estabelecidas pelo proprietário da informação até o destino, incluindo neste processo um controle de mudanças.

O controle de mudanças está relacionado ao não-repúdio, ou seja, o usuário que alterar uma informação não poderá negar o fato, pois existem mecanismos criptográficos que garantem sua autoria (SILVA, 2003).

4.1.1.3 Disponibilidade

O último pilar, muitas vezes não compreendido e esquecido, tem como objetivo garantir que a informação esteja sempre disponível para usuários que estejam autorizados a acessá-la.

Técnicas modernas de alta disponibilidade e redundância são aplicadas sobre este pilar para que, caso haja algum tipo de interrupção de acesso à informação, o mesmo possa ser transparentemente contornado.

Alguns autores, como Ferreira e Araújo (2006), citam outros pilares, como:

a) legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;

b) auditabilidade: todo acesso à informação deve ser registrado, possibilitando posteriormente a identificação do usuário que efetuou o acesso e também o que foi feito com a informação.

Independente da existência de outros pilares, conforme a literatura é importante ressaltar que as variações sempre norteiam os três pilares fundamentais: integridade, confidencialidade e disponibilidade.

4.2 AMEAÇAS

Possíveis, e muitas vezes desconhecidas, em certas condições podem causar impactos aos negócios organizacionais. O ativo de uma ameaça geralmente é a exploração de vulnerabilidades, culminando em perda de confidencialidade, integridade e disponibilidade.

As ameaças, segundo Ferreira e Araújo (2006), podem ser divididas conforme a Tabela 2.

Tabela 2. Ameaças à segurança da informação.

Ameaça	**Exemplos**
Naturais	Ameaças ocasionadas de fenômenos da natureza, como incêndios, enchentes, terremotos, entre outras.
Involuntárias	Ameaças inconsistentes que quase sempre são causadas pelo desconhecimento ou imprevisto: acidentes, erros, falta de energia, entre outras.
Voluntárias	Ameaças causadas propositalmente por agentes humanos, tais como hackers, invasores, ladrões, entre outras.

Fonte: Adaptado de FERREIRA, F.N.; ARAUJO, M.T (2006).

4.3 VULNERABILIDADES

Vulnerabilidade é uma condição de fragilidade de um sistema computacional, que, ao ser explorada, acaba causando um incidente de segurança. De acordo com Ferreira e Araújo (2006) são elementos passivos, falhas que só serão afetadas por agentes causadores ou condições favoráveis. Na Tabela 3 podem ser observados exemplos de vulnerabilidades.

Tabela 3. Exemplos de vulnerabilidades.

Vulnerabilidades	**Exemplos**
Físicas	Instalações fora do padrão; risco de vazamentos, incêndios; a falta de extintores, detectores de fumaça, entre outros.
Naturais	Todo ativo corre o risco de ser afetado por um desastre natural, como incêndio, enchente, terremotos entre outras.
Hardware	Falha dos recursos tecnológicos. Às vezes por desgaste ou até mesmo má utilização.
Software	Erros na instalação, má utilização e principalmente má configuração podem provocar vazamento, perda e indisponibilidade dos dados.
Mídias	Qualquer tipo de armazenamento de dados pode ser perdido ou danificado.
Comunicação	Perda de comunicação e acesso não autorizado.
Humanas	Falta de treinamento, compartilhamento indevido de informações confidenciais, erros ou omissões, greve, vandalismo, roubo, entre outras.

Fonte: Adaptado de SÊMOLA, M (2003).

4.4 MEDIDAS DE SEGURANÇA

As medidas de segurança, também conhecidas como contramedidas (*counter measures*), são elementos dentro de um sistema computacional que têm a finalidade de diminuir o risco e a fragilidade dos ativos de informação.

Segundo Sêmola (2003) as medidas de segurança podem ser classificadas, conforme a Tabela 4.

Tabela 4. Medidas de Segurança.

Medidas de Segurança	**Descrição**
Preventivas	Tem como objetivo impedir que incidentes venham a ocorrer. Visam manter a segurança imposta pela política de segurança da empresa. Palestras, treinamentos, *firewall*, antivírus e configurações adequadas de roteador e *access point* são exemplos de prevenção.
Detectáveis	Buscam identificar condições ou causadores de ameaças. Alguns exemplos são análises de riscos e câmeras de vigilância.
Corretivas	Ações voltadas à correção de estruturas tecnológicas ou humanas visando que as mesmas se adaptem a política de segurança estabelecida pela empresa.

Fonte: Adaptado de SÊMOLA, M (2003).

4.5 CRIPTOGRAFIA

Apesar do grande número de protocolos, e da aparente complexidade, devido à quantidade de informações, configurar uma rede sem fio é algo extremamente fácil. Para uma configuração simples basta ligar os cabos e começar a transmitir dados entre os equipamentos. Porém, esse procedimento não é recomendável, principalmente em grandes centros.

Uma vez que a transmissão sem fio é feita por ondas de rádios, basta possuir uma antena para capturar os dados. Sendo assim, o roubo de informações se torna algo simples, quando não se implementa qualquer tipo de política de segurança (TANENBAUM, 2003).

Apesar de existirem maneiras de restringir o acesso de pessoas não autorizadas ao ponto de acesso, tal maneira não é totalmente eficaz para garantir a segurança dos dados transmitidos, pois, apesar de não ter acesso à rede em si, uma pessoa mal intencionada pode monitorar os canais, bem como as freqüências de rádio, coletando, dessa maneira, tudo o que for transmitido de um ponto de acesso a um computador com placa Wi-Fi.

Mas, já que não há como impedir que alguém capte o sinal, pode-se fazer com que apenas o remetente original da mensagem consiga entendê-la. Para isso, usa-se a criptografia.

4.5.1 Conceito

A expressão Criptografia origina-se da junção de duas palavras gregas: *Kryptós* que significa “oculto” e *gráphien*, cuja tradução é “escrever”. Juntando-se as duas, conforme Tanenbaum (2003), forma-se “escrita secreta”.

A criptografia é de fundamental importância para a segurança das organizações na atualidade. É considerada, segundo Nakamura e Geus (2003, p. 287), “a ciência de manter as mensagens seguras”.

Os autores afirmam que a cifragem é o procedimento de embaralhar o texto original de tal forma que seu conteúdo é escondido em uma mensagem cifrada. A decifragem, por sua vez, é o processo inverso, onde o texto original é resgatado do texto cifrado.

A cifragem, também chamada de criptografia, assim como a decifragem, chamada de decriptografia, são feitas por meio do uso de algoritmos com funções

matemáticas complexas, protegendo a informação contra integridade, autenticidade, não-repúdio e sigilo (SILVA, 2003).

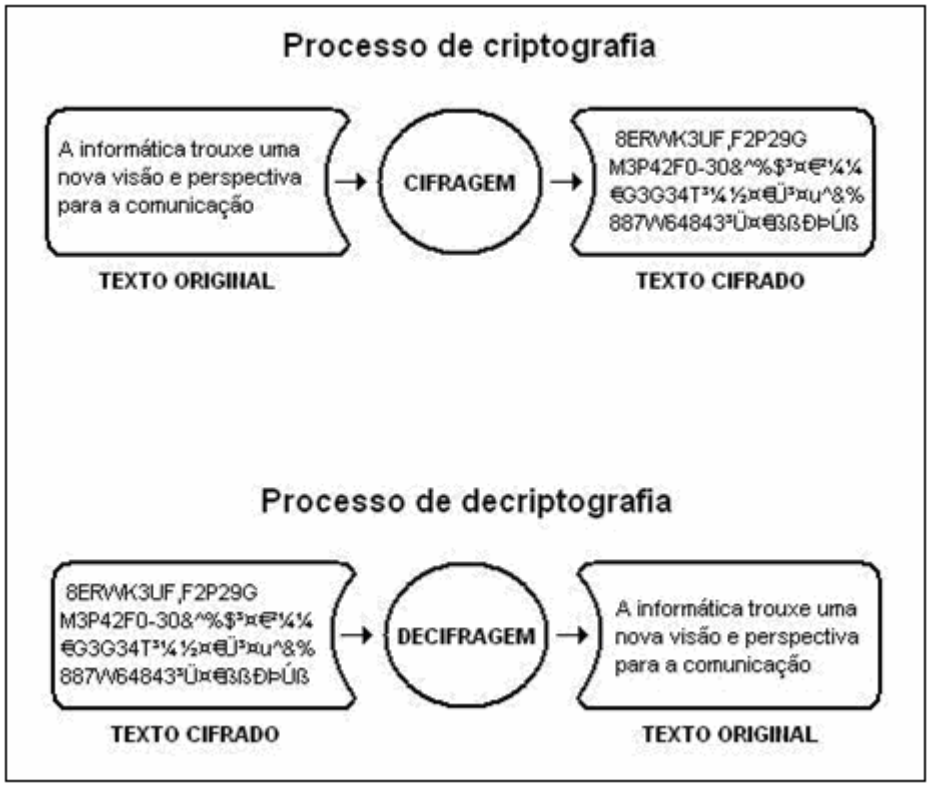


Figura 7. Processo de Criptografia e Decriptografia.
Fonte: Silva, L. (2003)

As técnicas mais conhecidas na computação utilizam o conceito de chaves criptográficas. Estas chaves, responsáveis pela cifragem e decifragem dos dados, são compostas por uma seqüência de *bits* definidas por um algoritmo. Quanto maior a quantidade de *bits* da chave, quase sempre é maior o esforço desprendido para a quebra.

Os métodos criptográficos são realizados por meio de dois grandes sistemas: criptografia simétrica, também conhecida como criptografia de chave secreta, e criptografia assimétrica, reconhecida como criptografia de chave pública (BURNETT, 2002).

4.5.2 Criptografia Simétrica e Assimétrica

A criptografia simétrica utiliza-se do conceito de chave compartilhada, mantendo uma única chave para o processo de cifragem, como para o processo de decifragem. Desta forma o segredo está guardado dentro da chave. Quem a detiver poderá cifrar ou decifrar qualquer mensagem (SILVA, 2003).

O termo chave utilizado, segundo Burnett (2002, p. 15), “vem do fato de que o número secreto que você escolhe funciona da mesma maneira que uma chave convencional”.

De forma bastante diferenciada, a criptografia de chave pública, consiste, de acordo com Burnett (2002), em utilizar um par de chaves (uma pública e outra privada) matematicamente relacionadas. Na criptografia assimétrica, uma chave é utilizada para encriptar os dados e outra para a decriptografia.

A aplicabilidade dos dois modelos de criptografia está diretamente ligada ao tipo de informação que será assegurada e principalmente ao número de pessoas e ativos que a ela podem ter acesso. É comum utilizar criptografia assimétrica quando a informação deve ser compartilhada por muitas pessoas, ao contrário da criptografia simétrica, que geralmente mantêm poucos e confiáveis envolvidos no compartilhamento.

Nakamura e Geus (2003) acrescentam, quando acordam que os algoritmos de chave simétrica, além de outros problemas como troca segura de chaves, impõem uma complexidade quanto ao gerenciamento de chaves na utilização de chaves secretas diferentes para cada tipo de comunicação.

A criptografia de chave pública, segundo os autores, resolve, além do problema de distribuição de chaves, a complexidade de gerenciamento destas. As

chaves públicas devem ficar expostas para que, quando usuários quiserem enviar dados criptografados para outros, possam utilizar a chave pública correspondente para encriptar os dados. O receptor, por sua vez, utilizará sua chave privada para o processo de decifragem. Isso funciona perfeitamente, pois no momento da geração do par de chaves, tanto a parte pública quanto a privada mantêm um relacionamento matemático, permitindo a decifragem com a chave privada quando a informação for cifrada com a parte pública (TANENBAUM, 2003).

Aparentemente, a criptografia assimétrica possui diversas vantagens com relação à simétrica. Sua utilização, contudo, é cerca de 60 a 70 vezes mais lenta que os algoritmos simétricos. Geralmente, a parte privada na criptografia assimétrica utiliza-se de um algoritmo simétrico (NAKAMURA; GEUS, 2003).

O intuito do processo de criptografia, no que tange a redes sem fio, é prover a privacidade das informações que trafegam pela rede. Os dados cifrados devem ser decifrados somente pelos elementos autorizados para fazer essa operação. A seguir são mostrados os protocolos para redes sem fio que fazem o uso de criptografia.

5 PROTOCOLOS PARA REDES SEM FIO

Transmitir informações por meio de ondas de rádio com as tecnologias existentes não é um trabalho muito difícil. A maior dificuldade está em garantir a segurança das informações que trafegam nesse meio.

Para garantir essa segurança existem os protocolos criptográficos para redes sem fio: WEP, WPA e WPA2. Esses três protocolos serão apresentados nesse capítulo.

5.1 *WIRED EQUIVALENT PRIVACY* - WEP

Em 1999, por meio do padrão 802.11, foi aprovado o *Wired Equivalent Privacy* (WEP) como primeiro protocolo de segurança para redes sem fio, objetivando oferecer as WLANs privacidade semelhante a das redes locais (TANENBAUM, 2003).

A grande maioria dos equipamentos comercializados suporta protocolo WEP, pelo menos em suas versões de 64 e 128 *bits*. Para fazer uso desse protocolo é necessário que todos os equipamentos envolvidos na comunicação o suportem. Caso contrário, não poderão ingressar à rede.

De acordo com Tanenbaum (2003) o WEP baseia-se em um algoritmo criptográfico de fluxo, chamado de *Ron's Code* 4 (RC4), para garantir privacidade das informações trafegadas. Em conjunto, o algoritmo *Cyclic Redundancy Check* (CRC-32) é utilizado para fornecer integridade quanto aos pacotes.

O autor ainda afirma que o RC4 manteve-se secreto por um período, mas acabou sendo divulgado e publicado na Internet em 1994. No WEP, esse algoritmo é utilizado para gerar um fluxo de chaves (denominado *keystream*) junto a uma operação

XOR (Ou-exclusivo) e a um texto simples (chamado *plain-text*) para formar uma mensagem cifrada.

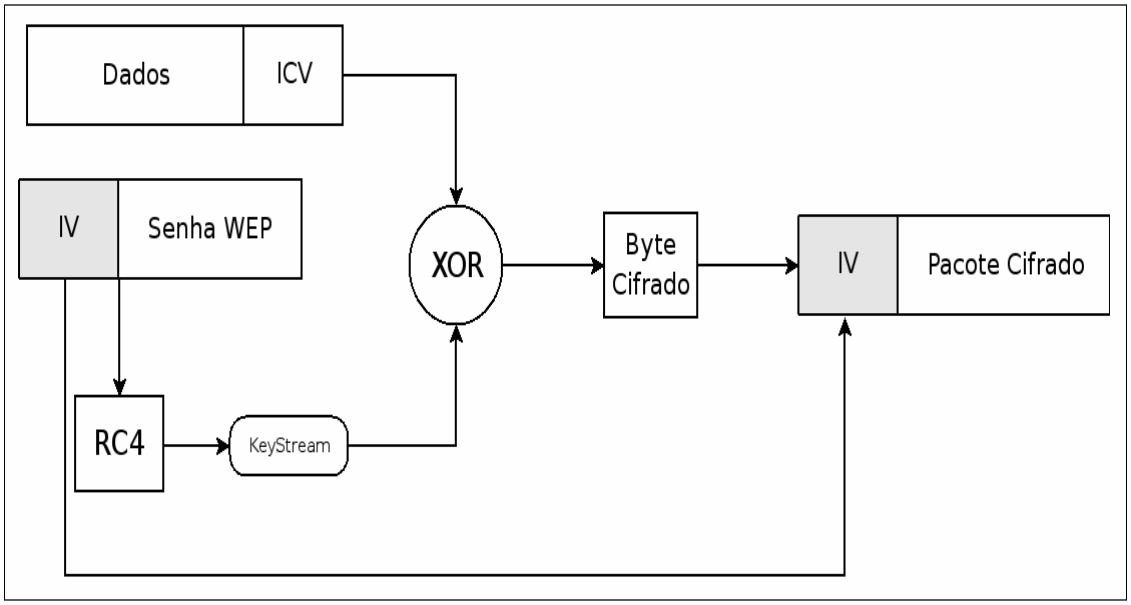


Figura 8. Encapsulamento WEP.
Fonte: Adaptado de TANEMBAUM, A. (2003)

Conforme Figura 8 apenas a mensagem e o *Integrity Check Value* (ICV) são criptografados. Todo o resto do pacote passa em texto plano pela rede sem fio. O WEP utiliza-se de um vetor de inicialização (chamado IV) com 24 *bits* de tamanho, concatenado a chave que pode ser de 40, 104 ou 232 *bits*, compartilhada entre os clientes e o ponto de acesso.

Durante a transmissão do pacote, um vetor de inicialização (IV) de 24 *bits* é selecionado randomicamente e é anexado à chave WEP para fazer uma nova chave de 64, 128 ou 256 *bits*. Nesse processo, são utilizados dois algoritmos base do RC4: *Key-Scheduling Algorithm* (KSA) e *Pseudo-Random Generation Algorithm* (PRGA) (VACCA, 2006).

5.1.1 AUTENTICAÇÃO WEP

A autenticação do protocolo WEP é feita de duas maneiras: Sistema Aberto ou Chave Compartilhada, também chamados de *Open System* e *Shared Key*.

O Sistema Aberto permite associação direta à rede sem a passagem de nenhuma senha. Para isso, basta informar a identificação (SSID) da rede sem fio. O processo de descoberta da rede e mapeamento de redes disponíveis é feito automaticamente pelos adaptadores, portanto, este processo torna-se transparente para o usuário. Logo após a associação, o ponto de acesso solicita a senha para que seja devidamente autenticado, podendo fazer uso efetivo da rede. A Figura 9 ilustra o modelo de autenticação sistema aberto.

Figura 9. Autenticação WEP Sistema Aberto
Fonte: Adaptado de INFORMAÇÃO SEGURA (2008)

Já no mecanismo de Chave Compartilhada, o ponto de acesso utiliza uma técnica de *challenge response*. O cliente envia um pedido de autenticação ao ponto de acesso que por sua vez responde com qualquer texto plano. Este texto plano é criptografado juntamente com a chave e enviada ao ponto de acesso. Se o resultado do processo de decifragem do lado do *Access Point* for o mesmo inicialmente enviado, então o cliente é associado à rede. Na Figura 10 pode ser visto o modelo de autenticação com chave compartilhada.

Figura 10. Autenticação WEP Chave compartilhada
Fonte: Adaptado de INFORMAÇÃO SEGURA (2008)

5.1.2 VULNERABILIDADES

As principais vulnerabilidades WEP descritas na literatura, por Tanembaum (2003) e Rufino (2005) e tantos outros estão relacionadas ao tamanho e reuso de chaves, autenticação fraca, gerenciamento de chaves, formato de transmissão do vetor de inicialização, entre outros.

As chaves estáticas WEP possuem tamanho de 40 *bits*, seguidos dos 24 *bits* do vetor de inicialização. Versões posteriores como WPA, criaram chaves estáticas de 104 e 232 *bits*, mantendo os 24 *bits* de IV. Em uma rede com alto volume de tráfego é normal acontecer uma repetição do vetor de inicialização e conseqüentemente a repetição de uma chave RC4. Mesmo que não haja grande volume de dados na rede, um atacante poderá por meio de técnicas de injeção de dados forçar a troca de pacotes com o ponto de acesso a fim de gerar um número elevado de IV's.

A autenticação de chave compartilhada pode ser facilmente burlada com uma escuta na rede a procura de um pacote em texto plano e seu correspondente criptografado, facilitando a identificação do fluxo de chaves para criar uma autenticação forjada, e sem senha, com o ponto de acesso.

Em 2001, Fluhrer et al apud (2001) e Nakamura e Geus (2003), publicaram um artigo abordando fraquezas no algoritmo KSA do RC4 e posteriormente sua aplicabilidade diante das chaves WEP estáticas. O ataque, conhecido como FMS (pelas iniciais de seus autores Fluhrer, Mantin e Shamir) está disponível em diversas ferramentas de auditoria de redes sem fio. Nesse ataque para descobrir a chave WEP é necessário a captura de um grande número de pacotes com IVs diferentes, ou seja, um grande número de IVs únicos.

5.2 *WI-FI PROTECT ACCESS* - WPA

A primeira versão do protocolo de criptografia WPA surgiu em 2003, por meio da união dos membros da *Wi-Fi Alliance* com membros do IEEE, com o intuito de aumentar o nível de segurança das redes sem fio tendo em vista as vulnerabilidades de conhecimento público do protocolo WEP.

De acordo com a *Wi-Fi Alliance* (2003), o WPA foi criado em meio a turbulências relacionadas às deficiências do WEP enquanto que um novo padrão, denominado 802.11i (hoje WPA2), ainda não havia sido padronizado.

O WPA, portanto, continua sendo baseado no RC4 e em alguns procedimentos encontrados na especificação do 802.11i. Melhorias aparentes surgiram tais como:

a) vetor de inicialização maior;
b) utilização de um novo código de verificação de integridade das mensagens;
c) gerenciamento de chaves;
d) modo de autenticação corporativo e pessoal (doméstico).

5.2.1 Encapsulamento WPA

O WPA faz uso do *Temporal Key Integrity Protocol* (TKIP), que é baseado no conceito de re-chaveamento ou chaves temporais, fazendo com que as elas sejam substituídas automaticamente depois de um determinado tempo de uso.

O Encapsulamenteo WPA é similar ao WEP, a grande diferença está na chave formada que servirá de base para o RC4. O resultado da chave disponibiliza combinações onde o vetor de inicialização, o endereço MAC do transmissor e a chave criptográfica são utilizados. Por sua vez, a chave resultante do algoritmo de combinação, juntamente com o vetor de inicialização, são repassados ao RC4.

5.2.2 Autenticação WPA

Existem dois tipos de autenticação no protocolo WPA, chamados WPA Pessoal e WPA Corporativo. A referência IEEE 802.11i (2004) define o modo de funcionamento destes dois modos da seguinte maneira:

a) **WPA Pessoal (WPA-PSK):** utiliza-se o conceito de chave compartilhada (*Pre-Shared Key*), variando entre 8 a 63 caracteres, funciona por meio do conhecimento da senha (chamada *passphrase*) entre o ponto de acesso e os usuários;
b) **WPA Corporativo:** toda a autenticação realizada é dependente de um servidor de autenticação. A comunicação entre o ponto de acesso e o servidor é feita com a especificação 802.1x. Neste modo de autenticação, existe outro protocolo envolvido, chamado *Extensible*

Authentication Protocol (EAP) que juntamente com o 802.1x é responsável pela autenticação externa em um servidor ou outro equipamento ativo responsável.

5.2.3 Vantagens do WPA sobre o protocolo WEP

De acordo com Sklavos e Zhang (2007), o WPA utiliza um conceito de vetor de inicialização estendido de 48 *bits*, reduzindo potencialmente a possibilidade de repetição das chaves. Aliado a isso, regras para a determinação e verificação dos IV's foram adicionados para evitar ataques de injeção de pacotes a fim de aumentar o tráfego da rede e capturar um maior número de vetores.

Outra vantagem é a melhoria no processo de autenticação de usuários, dependendo do modo de autenticação WPA, é possível fazer com que a distribuição e gerenciamento de chaves sejam dinâmicos e automáticos, sendo o protocolo responsável por todo o trabalho. Existe também a possibilidade, por meio da extensão corporativa, efetuar a autenticação utilizando servidores como *backends* de autenticação.

5.2.4 Vulnerabilidades

A principal vulnerabilidade no WPA está relacionada à utilização do método de autenticação PSK, mesmo em infra-estruturas corporativas. Segundo a *Wi-Fi Alliance* (2003), não é tão comum à existência de um servidor para fazer as autenticações, de forma que o modelo de chave compartilhada continua sendo utilizado. Um atacante poderá usufruir de ataques de dicionário por meio da captura passiva de

tráfego da rede. Pelo fato da maioria dos usuários utilizarem senhas fracas, fica fácil quebrar a senha.

No caso de senhas difíceis, o atacante ficará restrito ao tamanho do dicionário e da capacidade de combinações por segundo que o equipamento pode fazer, levando dias, meses e talvez não conseguindo quebrar, principalmente em tempo hábil.

5.3 IEEE 802.11i - WPA2

O protocolo 802.11i também conhecido como WPA2, foi ratificado em junho de 2004 pela IEEE. Criado como promessa de sanar os erros encontrados nos protocolos WEP e WPA. Sua principal melhoria em relação a sua versão anterior está relacionada ao método criptográfico utilizado, o WPA utiliza o algoritmo TKIP com o algoritmo RC4, enquanto o WPA2 utiliza a criptografia *Advanced Encryptation Standart* (AES) em conjunto com o TKIP com chave de 256 *bits*, que é considerado um método mais seguro devido ao tamanho da sua chave. A utilização da chave com 256 *bits* é padrão WPA2.

5.3.1 Algoritmo AES

O algoritmo AES foi criado a partir de uma competição promovida pela *National Institute of Standards and Technology* (NIST) dos Estados Unidos. Essa competição foi criada com o intuito de substituir o algoritmo DES.

A competição teve início em janeiro de 1997 e término no dia 2 de outubro de 2000 tendo como vencedor o algoritmo Rijndael, criado por Vincent Rijmen e Joan Daemen.

Em 2006 tornou-se um padrão efetivo já estando entre os mais populares e usados para criptografia com chave simétrica. A Figura 11 mostra uma comparação entre o algoritmo AES e outros padrões já conhecidos.

ALGORITMO	TAMANHO DA CHAVE	NO DE RODADAS	OPERAÇÕES MATEMÁTICAS
AES	128, 192 ou 256 bits	10, 12, 14	XOR, S-Boxes fixas
DES	56 bits	16	XOR, S-Boxes fixas
3DES	112 ou 168 bits	48	XOR, S-Boxes fixas
IDEA	128 bits	8	XOR, adição, multiplicação
Blowfish	Variável ate 448 bits	16	XOR, S-Boxes variáveis, adição
RC5	Variável ate 2048 bits	Variável ate 255	Adição, Subtração, XOR, rotação
CAST-128	40 ate 128 bits	16	Adição, subtração, XOR, rotação, S-Boxes fixas

Figura 11. Comparação Algoritmo AES.
Fonte: Adaptado de CARVALHO, D.B. (2000)

O AES é um algoritmo de encriptação de blocos de dados, ou seja, o algoritmo combina uma chave e um bloco de dados de 128 *bits* para gerar outro bloco de 128 *bits* completamente diferente do original.

O AES trabalha repetindo várias vezes um conjunto definido de passos que trabalha com chave secreta que opera com um número fixo de *bytes*. Uma característica interessante do AES é que o processo utilizado para encriptação dos dados é o mesmo utilizado para a desencriptação, significando que os fabricantes precisam apenas implementar o processo de encriptação não havendo a necessidade de implementar o de desencriptação (CARVALHO, 2000).

O controle de integridade e autenticação são os mesmos utilizados pelo WPA.

5.3.2 Vulnerabilidades

Mediante a pesquisa realizada poucas vulnerabilidades foram encontradas sobre o protocolo WPA2. Isso se deve ao fato de o protocolo não ser o mais utilizado, em relação aos anteriores, sendo assim menos explorado e pesquisado por invasores. As vulnerabilidades conhecidas do protocolo são:

a) **Negação de Serviço**: os mecanismos de segurança existentes até então não protegem os quadros de gerenciamento e controle, sendo assim o ataque de negação de serviço, que consiste na tentativa de deixar os recursos indisponíveis, é possível de se executar. Neste protocolo é mais comum o envio de pacotes para a desautenticação do usuário com a rede;

b) **PSK com tamanho pequeno**: não é uma vulnerabilidade propriamente dita do protocolo e sim um problema de configuração da chave pelo usuário. Chaves PSK muito pequenas são suscetíveis a ataques de dicionário. O indicado é que se utilizem chaves com mais de 20 caracteres, aumentando assim significativamente o tempo necessário para quebra da chave.

6 TRABALHOS CORRELATOS

O estudo da segurança em redes sem fio está crescendo de forma significativa nos últimos anos. A mobilidade e o baixo custo são os fatores que mais contribuem para a popularização das mesmas.

A seguir são mostrados alguns trabalhos de pesquisa relacionados à segurança nas redes sem fios:

6.1 SEGURANÇA EM REDES SEM FIO 802.11

Monografia para Conclusão de Curso de Especialização em Redes de Computadores e Comunicação de Dados, realizado em 2006, na Universidade Estadual de Londrina. O trabalho tem como objetivo apresentar os problemas contidos na segurança em redes sem fios e os esforços da comunidade em resolvê-los, oferecendo protocolos com níveis de segurança equivalente aos das redes com fio. Nesse trabalho não foi realizado nenhum tipo de teste, somente documentadas as principais falhas e algumas possíveis tentativas de minimizá-las (PAIVA, 2006).

6.2 SEGURANÇA EM REDES *WIRELESS* PADRÃO IEEE 802.11B: PROTOCOLOS WEP, WPA E ANÁLISE DE DESEMPENHO

Trabalho de Conclusão de Curso de Ciência da Computação, realizado em 2004, na Universidade da Amazônia - UNAMA. O trabalho consistiu em apresentar o funcionamento do padrão IEEE 802.11b, focando especificamente as características da segurança. Descreve os mecanismos de segurança do padrão e as fraquezas de

segurança dos protocolos WEP e WPA. São apresentadas, também, conclusões sobre experimentos práticos, medindo o fluxo da rede com a utilização dos protocolos citados. Nesse trabalho não foi realizado nenhum tipo de teste de ataque ou defesa. Foi desenvolvida uma análise de desempenho na transmissão do fluxo de dados, utilizando os protocolos WEP e WPA. (PEREIRA JUNIOR; BRABO; AMORAS, 2004).

6.3 SEGURANÇA EM REDES WI-FI

Trabalho de Conclusão de Curso de Sistemas de Informação, realizado em 2005, na Universidade Estadual de Montes Claros – UNIMONTES. O trabalho é constituído dos aspectos gerais das configurações de segurança em redes Wi-Fi. São apresentadas várias configurações, desde a localização dos aparelhos até a mais complexa configuração, ideais para se obter uma boa segurança. Nesse trabalho são documentadas as falhas que podem ser encontradas em redes Wi-Fi e como se proteger das mesmas (AGUIAR, 2005).

6.4 SEGURANÇA DA TRANSMISSÃO DE DADOS POR *BLUETOOTH* EM AMBIENTES MÓVEIS

Trabalho de Conclusão de Curso de Ciência da Computação, realizado em 2007, na Universidade do Extremo Sul Catarinense – UNESC. O Trabalho aborda a segurança como ponto principal para a utilização da tecnologia *bluetooth*. São apresentados métodos e técnicas de segurança para este tipo de ambiente móvel, utilizando o *bluetooth* como objeto de estudo para comunicação. A parte prática deste trabalho consistiu em um protótipo de *software* de prontuário eletrônico trabalhando

como cliente servidor, onde o cliente seria executado em um celular com tecnologia *bluetooth* que teria o objetivo de recolher dados dos pacientes em seus leitos hospitalares e em seguida enviá-los para um servidor, por meio da comunicação por *bluetooth* que iria armazenar esses dados num banco de dados (RODRIGUES, 2007).

7 TESTES UTILIZANDO OS PROTOCOLOS WEP, WPA E WPA2

Na pesquisa desenvolvida foi realizado um estudo teórico e prático sobre os aspectos de segurança em redes sem fio, utilizando o padrão IEEE 802.11g. Foi pesquisada a segurança nas redes sem fio e efetuados alguns testes práticos para a avaliação e validação dos protocolos criptográficos WEP, WPA e WPA2, no que tange à utilização de redes sem fio padrão 802.11.

Foram criados diferentes cenários para a coleta de informações com posterior análise, servindo de base para a conclusão e a elaboração de um documento formal e um guia de boas práticas para a utilização de redes sem fio, estas que estão cada vez mais sendo utilizadas sem as devidas preocupações relacionadas à segurança da informação.

Nessa pesquisa são mostradas as suas vulnerabilidades, bem como a maneira de se defender das mesmas. Os testes serão realizados nos ambientes implementados com cada um dos protocolos citados anteriormente, iniciando desde a menor configuração do protocolo até a mais complexa.

7.1 FERRAMENTAS E PERIFÉRICOS UTILIZADOS

Durante a validação e análise dos protocolos criptográficos WEP, WPA e WPA2, foram criados ambientes simulados para a execução dos testes. Para isso, foram utilizados os equipamentos exibidos na Figura 12, descritos na Tabela 5.

O sistema operacional utilizado no ambiente foi o *Linux Ubuntu* 8.04

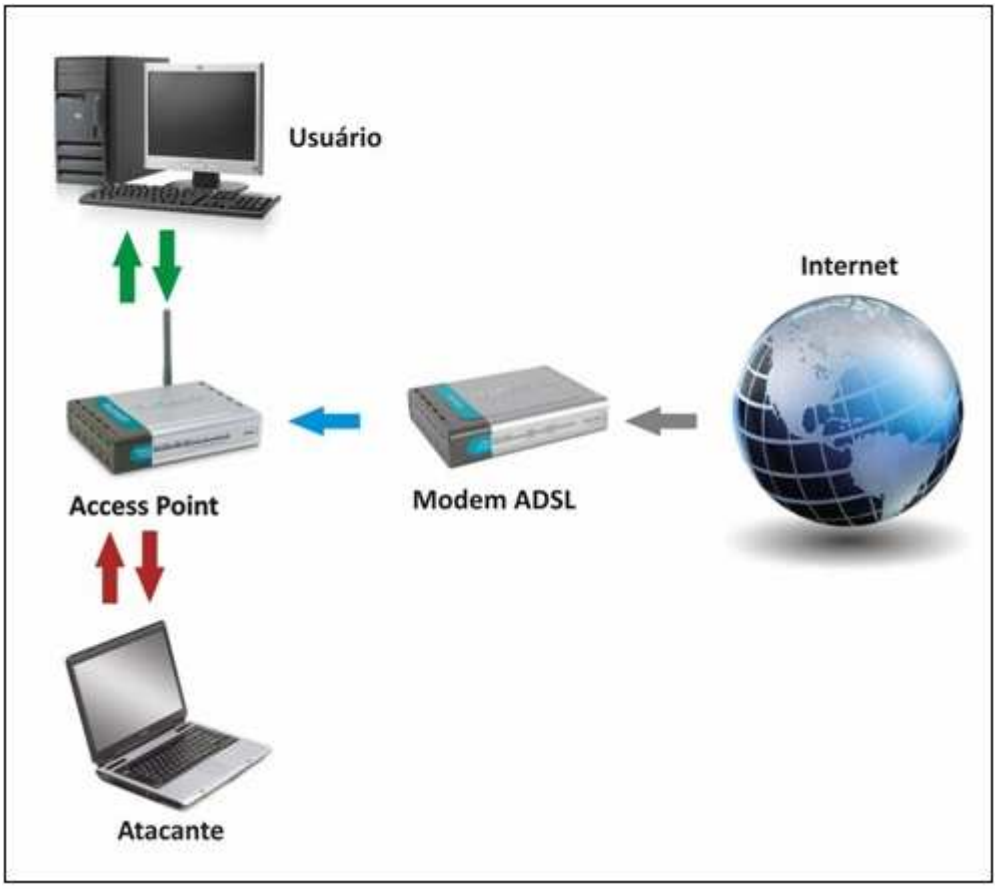


Figura 12. Ambiente utilizado nos testes realizados.

É importante ressaltar que os testes foram executados utilizando os protocolos WEP, WPA e WPA2 e o padrão 802.11g.

Tabela 5. Equipamentos e periféricos utilizados.

Equipamento	**Descrição**
D-Link DI-524	Roteador Sem Fio (*access point*)
D-Link DSL 500G	Modem ADSL
D-Link DWA-510	Placa Sem Fio PCI
D-Link DWA-110	Adaptador Sem Fio USB
Notebook Toshiba	Utilizado para efetuar os ataques.
Desktop	Utilizado como usuário de conexão com o *access point*.

O software utilizado em todos os testes foi o *Aircrack-NG* que é uma suíte com ferramentas, mundialmente reconhecida e utilizada para fins de testes sobre redes sem fio. Essa suíte é composta por vários módulos. Foram utilizados nessa pesquisa os módulos descritos na tabela 6.

A ferramenta é nativa do *Linux* e sua licença é livre, é executada por meio de comandos no terminal do *Linux*. Vale ressaltar que a ferramenta só executa os comandos com o usuário *root*[1] no *Linux*.

Tabela 6. Suíte Aircrack-NG.

Software	**Descrição**
Aircrack-NG	Responsável pela quebra das chaves.
Airmon-NG	Responsável pela definição de modo monitor nas interfaces sem fios
Airodump-NG	Responsável pela análise passiva nas redes, basicamente usado par coleta de IVs.
Aireplay-NG	Responsável pelo envio de pacotes ao *access point.* Pode ser utilizado para geração de tráfego ARP nas redes para aumentar o tráfego de pacotes e conseqüentemente diminuir o tempo necessário para a quebra.

7.2 CENÁRIOS E MÉTRICAS

Os cenários utilizados nesse trabalho compreendem algumas condições de configurações do *access point* no ambiente criado, que podem influenciar na segurança da rede sem fio. Os cenários criados foram os seguintes:

[1] O usuário *root* (também conhecido como o superusuário) tem acesso completo a todos os recursos e *softwares* do sistema.

a) **configuração padrão:** equipamento com as configurações de fábrica. Somente as informações necessárias para o seu funcionamento foram configuradas pelo assistente do equipamento (*wizard*[2]);

b) **restrição por MAC:** restrições baseadas em endereços físicos dos equipamentos sem fios que poderão ingressar na rede;

c) **presença do protocolo WEP:** existência do protocolo de criptografia WEP protegido por senha;

d) **presença do protocolo WPA:** existência do protocolo de criptografia WPA protegido por senha;

e) **presença do protocolo WPA2:** existência do protocolo de criptografia WPA2 protegido por senha.

Com base nos cenários estabelecidos é necessário estabelecer também as métricas que servirão de base para a conclusão e documentação do trabalho, as métricas são as seguintes;

a) **análise dos pacotes:** verificação do tráfego da rede em modo monitor[3] a fim de coletar dados com informações úteis aos ataques;

b) **análise dos protocolos:** implementar os protocolos citados anteriormente a fim de testar o grau de segurança dos mesmos;

c) **análise da vulnerabilidade:** em conjunto com a análise dos protocolos, tem a função de dar interpretação aos dados coletados e inferir diretamente na existência de pontos críticos na segurança no que tange ao uso da rede sem fio;

d) **análise das senhas:** quando utilizados protocolos criptográficos na rede sem fio, será analisado o tempo de quebra para senhas.

[2] Assistente de configuração do equipamento.
[3] Modo no qual o cliente não precisa estar conectado à rede, apenas captura pacotes de maneira passiva.

7.2.1 Configuração Padrão

A configuração padrão do equipamento D-Link DI-524, utilizado nos testes no decorrer do trabalho, possui um assistente, Figura 13, para configuração de algumas informações básicas para o funcionamento do equipamento. Preenchendo essas informações corretamente, o equipamento já entra em funcionamento.

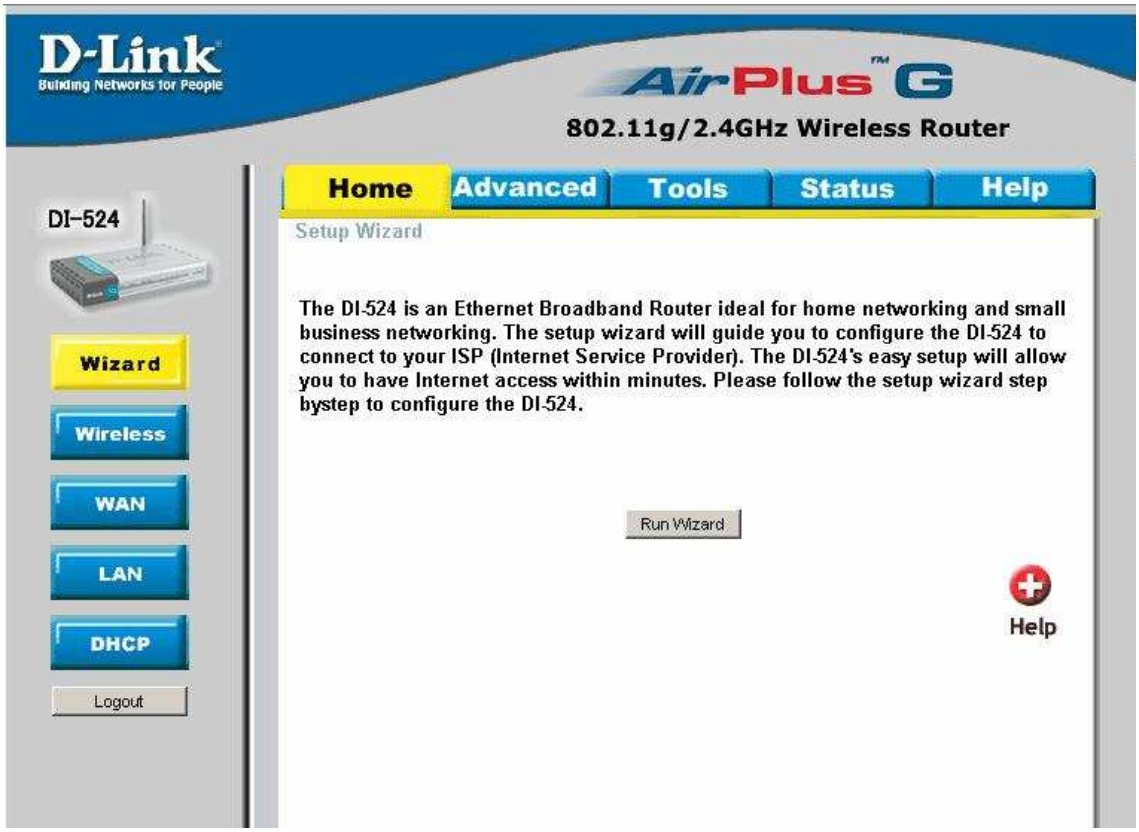


Figura 13. Tela inicial de configuração do equipamento D-Link DI-524

O problema é que a maioria dos fabricantes não alerta sobre as medidas de segurança que devem ser tomadas pelo usuário no momento da configuração dos equipamentos. Se executarmos o assistente de configuração do equipamento D-Link DI-524 no momento das configurações sem fio, a segurança (*security*) Figura 14, já vem desabilitada e o usuário que tem pouco conhecimento entenderá que não há necessidade de ser configurada.

Figura 14. Assistente de configuração da rede sem fio do equipamento D-Link DI-524

Mediante isso, conclui-se que o nível de segurança de uma rede sem fios com as configurações padrões de fábrica é extremamente baixo, estando limitado somente ao alcance do sinal, sendo que um atacante não terá dificuldade alguma para acessar a rede.

7.2.2 Restrição por MAC

Restringir o acesso por MAC significa especificar quais os endereços físicos (em nível de enlace) poderão acessar ou não o AP, tanto para a utilização de rede sem fio, quanto para a utilização de portas *Ethernet*, caso o equipamento atue como um comutador, que é o caso do equipamento em questão D-Link DI-524.

Nessa etapa do teste foi deixado o AP no estado anterior (configuração padrão), ativando, porém, o filtro por MAC, cadastrando o endereço do computador usuário. Com o computador atacante foi possível, por meio do comando *"iwlist"*, verificar quais redes estão ao alcance. O comando utilizado para escanear foi: *"iwlist scan"*, que traz as informações que podem ser observadas na Figura 15.

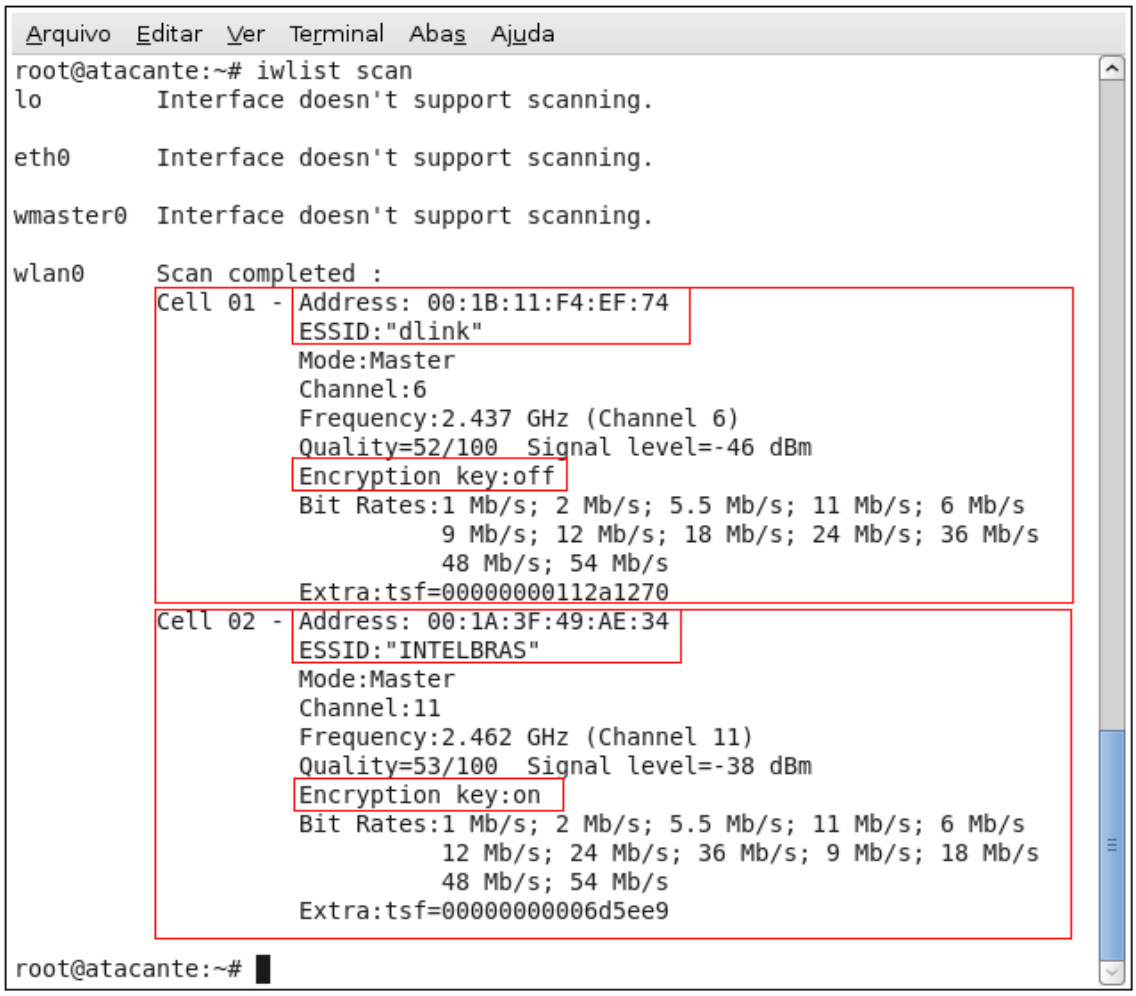


Figura 15. Saída do comando *iwlist scan*

Conforme saída do comando *"iwlist"* na Figura 15, pode-se visualizar que foram encontradas duas redes (dlink e INTELBRAS) e seus respectivos endereços MAC. Pode ser observado, também, que a rede "dlink", conforme menção anterior, não possui nenhuma encriptação (*encryption key:off*). Já a rede "INTELBRAS" a possui (*encryption key:on*).

A rede em questão é identificada como “dlink”, cujo endereço MAC é 00:1B:11:F4:EF:74. Para se ter acesso a essa rede foi necessário alterar o endereço MAC do adaptador de rede da máquina do atacante, deixando com o mesmo endereço físico do AP que foi listado. Para isso, foram executado os três comandos contidos na Figura 16. Vale ressaltar que no segundo comando deve ser colocado o endereço MAC que o adaptador de rede do atacante deve assumir.

```
1  # ifconfig wlan0 down
2  # ifconfig wlan0 hw ether 00:1B:11:F4:EF:74
3  # ifconfig wlan0 up
```

Figura 16. Comandos para alterar o endereço MAC no *Linux*.

O primeiro comando desativa a interface wlan0, que se refere à interface de rede sem fio do computador do atacante. O segundo comando altera o endereço MAC e o terceiro inicia a interface novamente.

Após a execução desses comandos, o endereço físico do adaptador do atacante já está alterado, obtendo o acesso a rede. É importante lembrar que o *access point* só aceita um endereço físico igual conectado por vez.

Utilizar restrição por MAC *address* não garante total segurança a rede, visto que nos testes efetuados foi preciso pouco tempo e alguns comandos para descobrir o MAC e cloná-lo, tendo acesso à rede sem maiores dificuldades.

Como única forma de segurança a restrição por MAC é vulnerável. Contudo, se utilizada juntamente com algum protocolo criptográfico como o WEP ou WPA, aumentará o nível da segurança da rede.

7.2.3 Presença do Protocolo WEP

O protocolo WEP tem como principal objetivo fazer uma mistura dos dados que são transmitidos pela rede sem fio, fazendo com que dispositivos, mesmo em modo monitor, não consigam enxergar a rede, nem se aproveitar de deficiências em protocolos sem criptografia. Num segundo momento, o WEP também é responsável por definir uma senha de acesso à rede.

O protocolo WEP suporta chaves de 64, 128, 152 e 256 *bits*. Os testes foram efetuados sobre chaves WEP 64 *bits* e WEP 128 *bits*, que são dois tamanhos de chaves suportadas pelos equipamentos do ambiente criado e também na grande maioria dos equipamentos disponíveis no mercado.

Conforme descrição na seção 5.1.2, o WEP possui um sério problema ao utilizar o algoritmo RC4 juntamente com o IV (vetor de inicialização), que tem como objetivo prevenir qualquer repetição de chave durante o tráfego. O vetor de inicialização, parte vital para o funcionamento do protocolo, é enviado na rede em uma área de dados não criptografada.

Muito embora as variações de WEP (64, 128, 152 e 256 *bits*) incrementem o tamanho do IV, os ataques continuam acontecendo normalmente, exigindo, entretanto, cada vez mais tráfego nas redes para que as chaves possam ser quebradas. Quanto maior o tráfego de rede, maior o número de IVs sendo transmitidos e, conseqüentemente, maior a chance de se realizar um ataque de força bruta sobre a chave relacionada.

Quebrar a criptografia WEP consiste nos seguintes passos:

a) Obter algumas informações sobre a rede;

b) iniciar interface em modo monitor;

c) capturar IVs;

d) realizar a quebra por meio de força bruta.

7.2.3.1 Quebrando WEP 64 *bits*

Inicialmente foi habilitada a criptografia WEP 64 *bits* no access point, conforme a Figura 17.

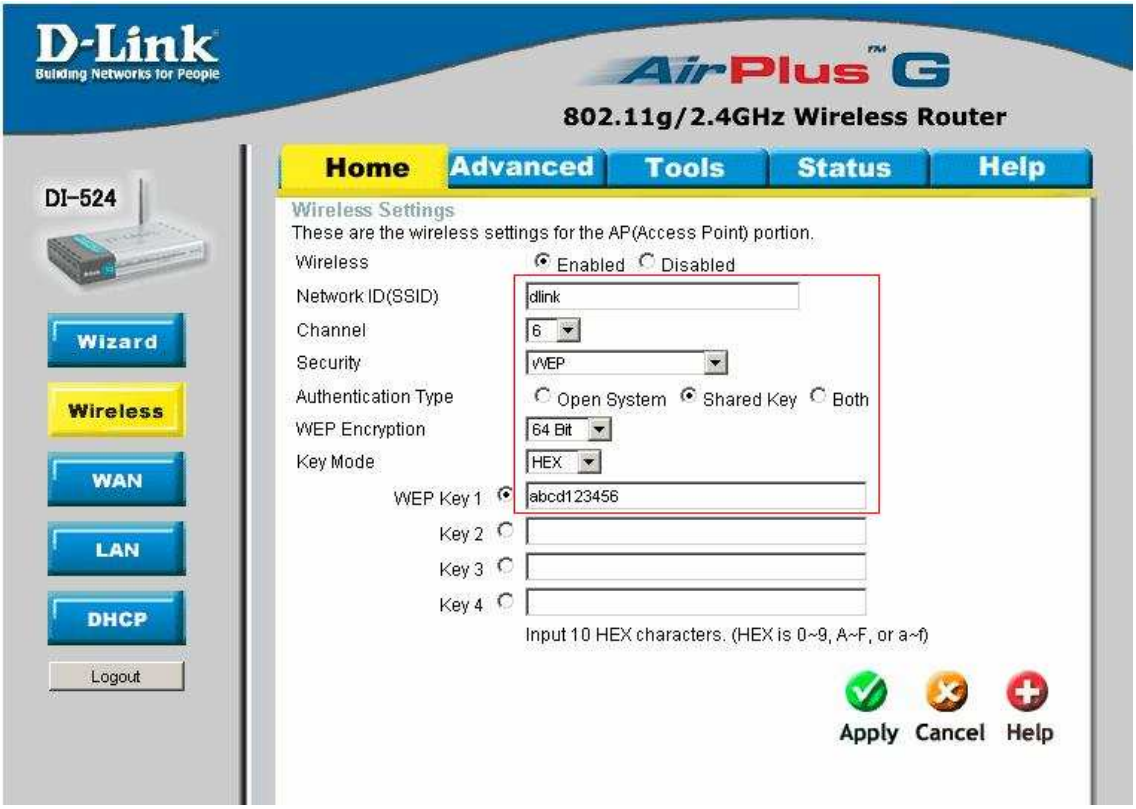


Figura 17. Criptografia WEP 64 *bits* habilitada no *access point*.

Prosseguindo com o teste foi executado o comando: "*iwlist wlan0 scan*" para se obter algumas informações básicas da rede para poder iniciar o ataque. Esse comando fez uma varredura nas redes sem fio próximas, trazendo as informações como o nome da rede, o endereço MAC, se existe ou não alguma criptografia e o canal em que a rede está transmitindo. A Figura 18 apresenta a saída do comando.

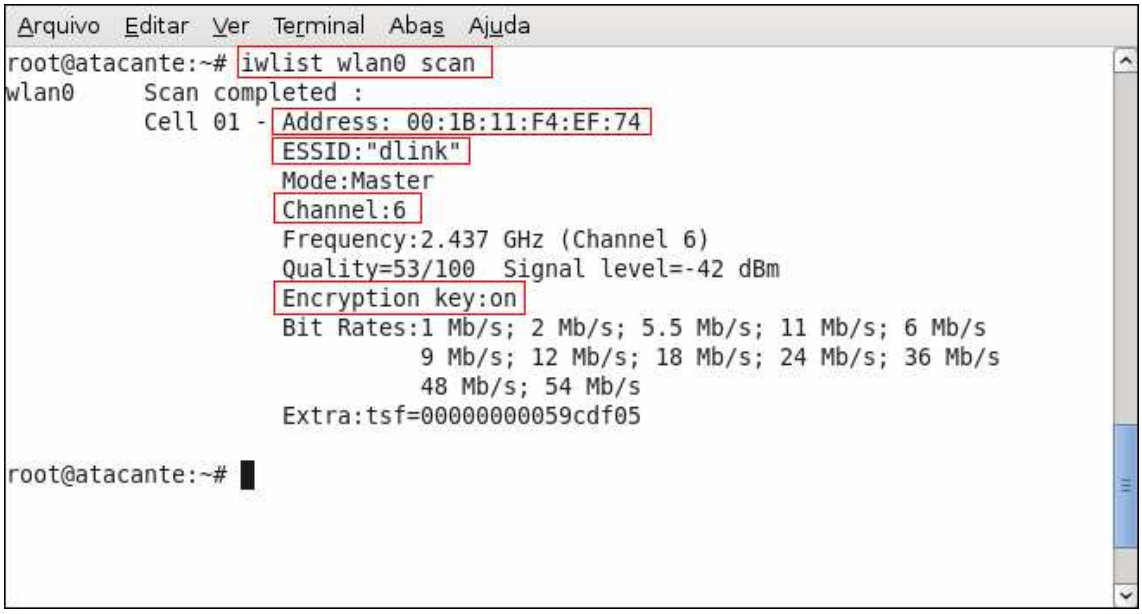


Figura 18. Varredura do comando iwlist.

Conforme a Figura 18, a rede identificada como “dlink” está com criptografia habilitada.

Nessa etapa do ataque foi colocada a interface de rede sem fio (wlan0) em modo monitor. Para tanto, foi utilizada a ferramenta *Airmon-NG* que pertence à suíte *Aircrack-NG*. Foi executado, primeiramente, o comando: “*airmon-ng stop wlan0”* para parar o modo monitor, caso o mesmo já estivesse em execução, e em seguida: “*airmon-ng start wlan0”* para iniciar a interface no modo monitor. A Figura 19 exibe os comandos que foram executados.

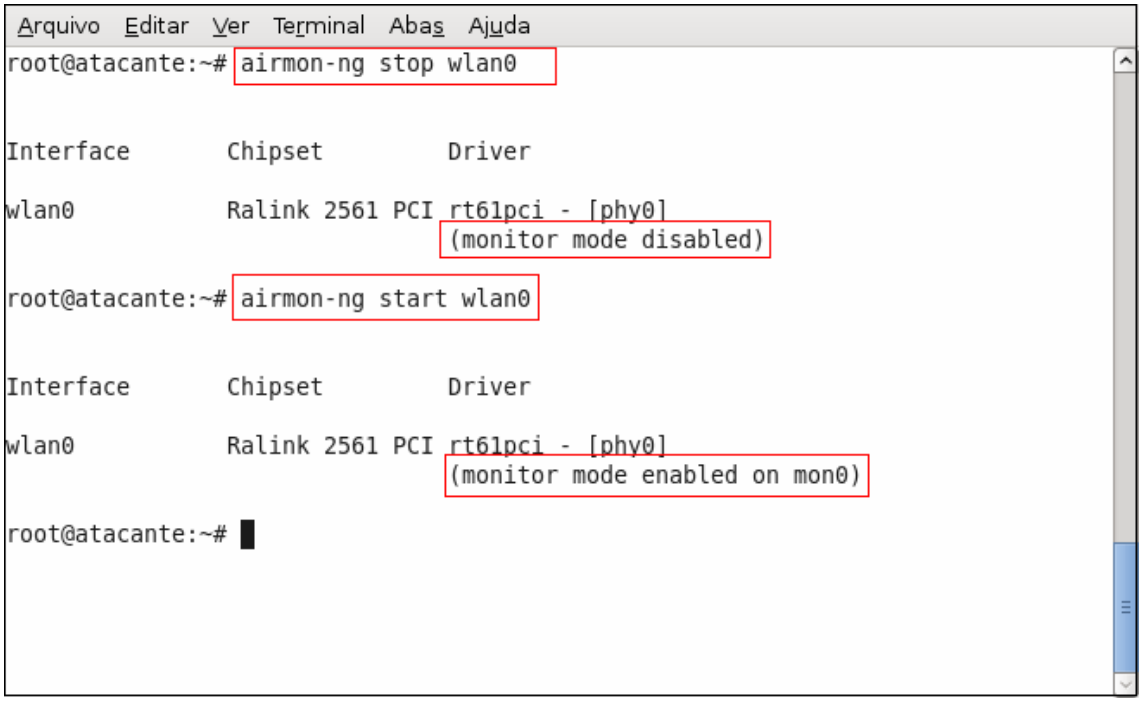


Figura 19. Configurando placa de rede como modo monitor.

Após essa etapa foi iniciada a captura de IVs do *access point*. Para capturar os IVs foi utilizado da suíte *Aicrack-NG* a ferramenta *Airodump-NG*, por meio do comando: "*airodump-ng -c 6 -w captura64 wlan0"*. Nesse comando, uma informação importante repassada foi o parâmetro (-c 6) que é o canal em que o AP está transmitindo, que foi adquirido por meio do comando "*iwlist"*. Esse parâmetro serve como filtro no comando. Caso haja mais alguma outra rede próxima, o comando irá capturar somente os IVs do canal 6 que é a rede em questão. O parâmetro "captura64" foi o nome dado ao arquivo de captura dos IVs. Na Figura 20 pode ser observada a captura dos dados por meio do *airodump-ng*.

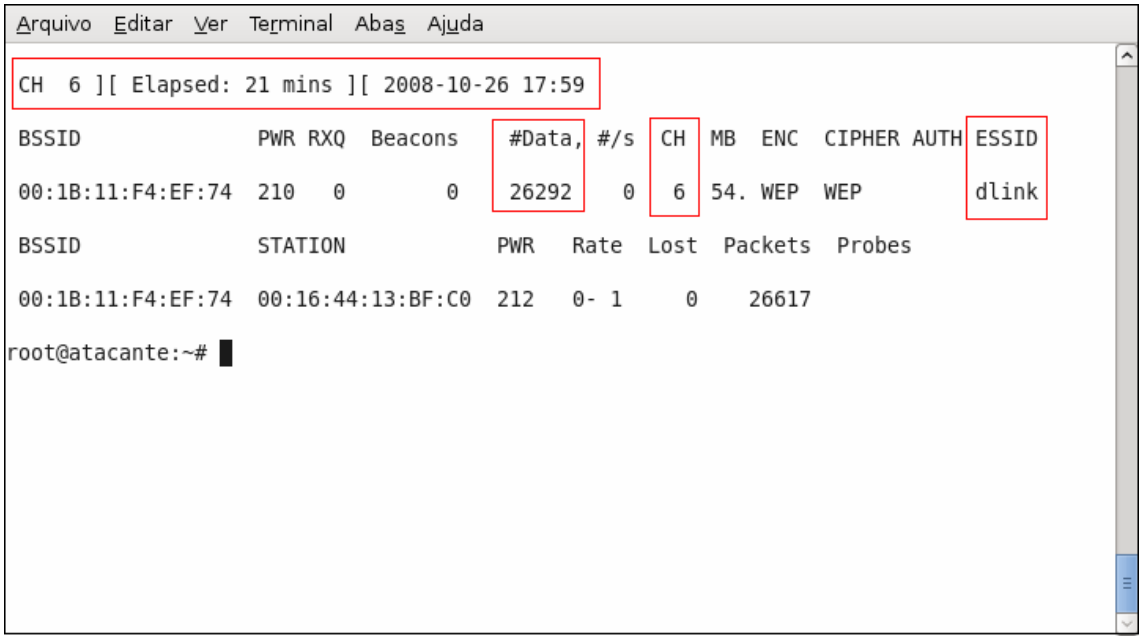


Figura 20. Airodump-ng capturando dados da rede.

Após 21 minutos, o *software* havia capturado 26.292 IVs, quantidade considerável para iniciar a quebra (recomenda em torno de 30.000 IVs para WEP 64 e 60.000 IVs para WEP 128). Após essa coleta, foi possível iniciar a quebra da chave de criptografia com a utilização do software *Aircrack-ng* por meio de força bruta.

Vale ressaltar que existem *softwares* que geram tráfego entre a rede que se deseja atacar e a máquina do atacante, a fim de minimizar o tempo de captura dos IVs e, conseqüentemente, o tempo da quebra.

Por meio do comando "*aircrack-ng ./captura64-01.cap*", foi iniciada a quebra da chave, sendo o parâmetro "captura64-01.cap" o nome do arquivo que foi salvo anteriormente com a sua respectiva extensão. A Figura 21 apresenta o *software Aircrack-NG* em execução sobre o arquivo "captura64".

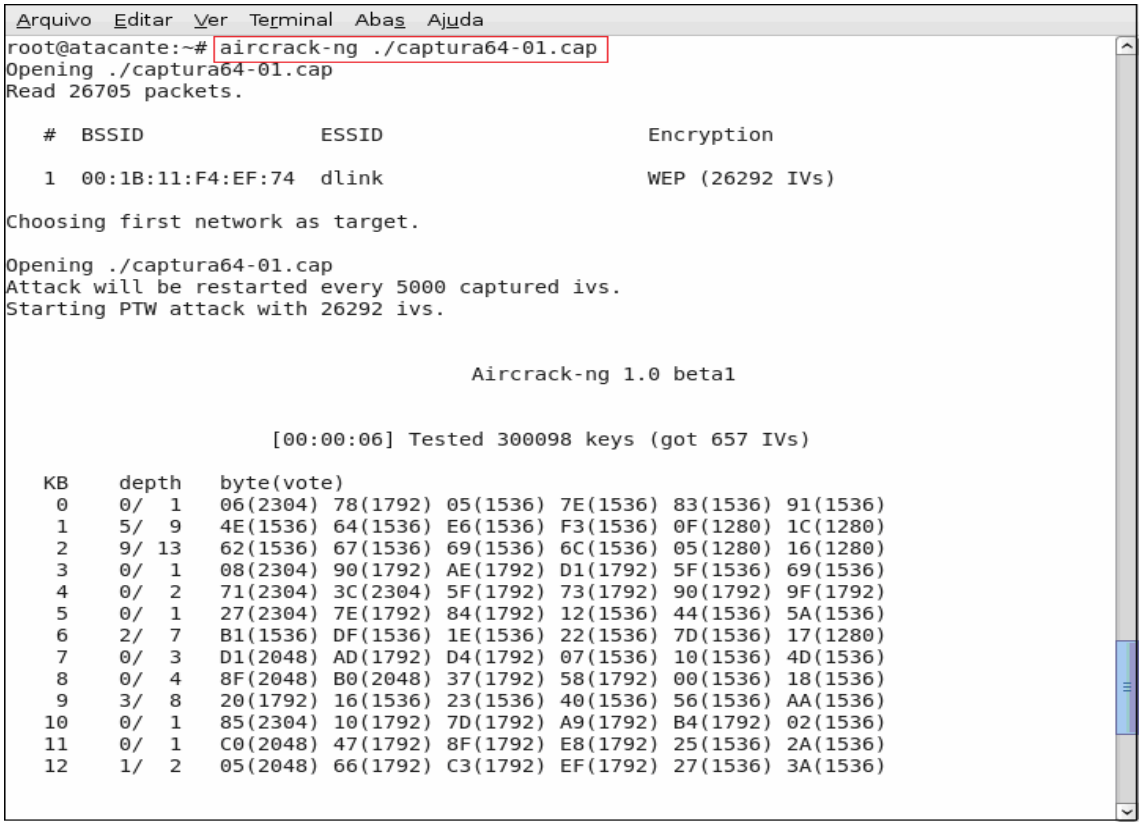


Figura 21. *Aircrack-ng* em execução.

Após 1 minuto e 11 segundos, com os 26.292 IVs capturados o *software* conseguiu quebrar a chave criptográfica WEP de 64 *bits* “ABCD123456”, testando 58.326 combinações de chaves por meio de força bruta: Figura 22. Com essa senha foi possível autenticar-se na rede e usufruir de todos os recursos sem maiores dificuldades.

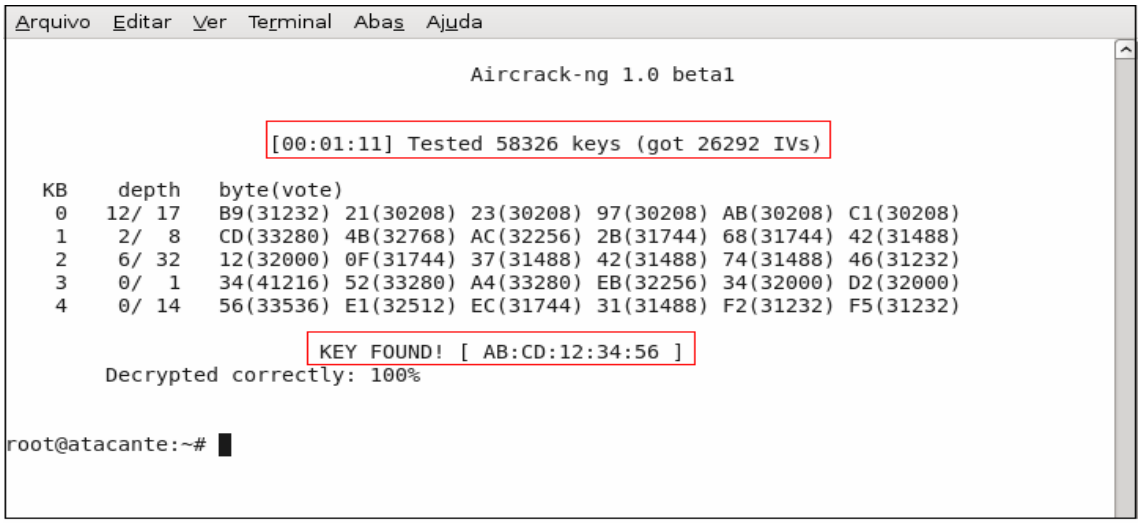


Figura 22. Criptografia WEP 64 *bits* quebrada por força bruta.

7.2.3.2 Quebrando WEP 128 *bits*

A quebra do protocolo WEP 128 *bits* foi executada seguindo as mesmas etapas da quebra do protocolo WEP 64 *bits*. Inicialmente, foram obtidos alguns dados da rede com o comando: "*iwlist wln0 scan"*, Figura 23, para poder iniciar a captura dos IVs.

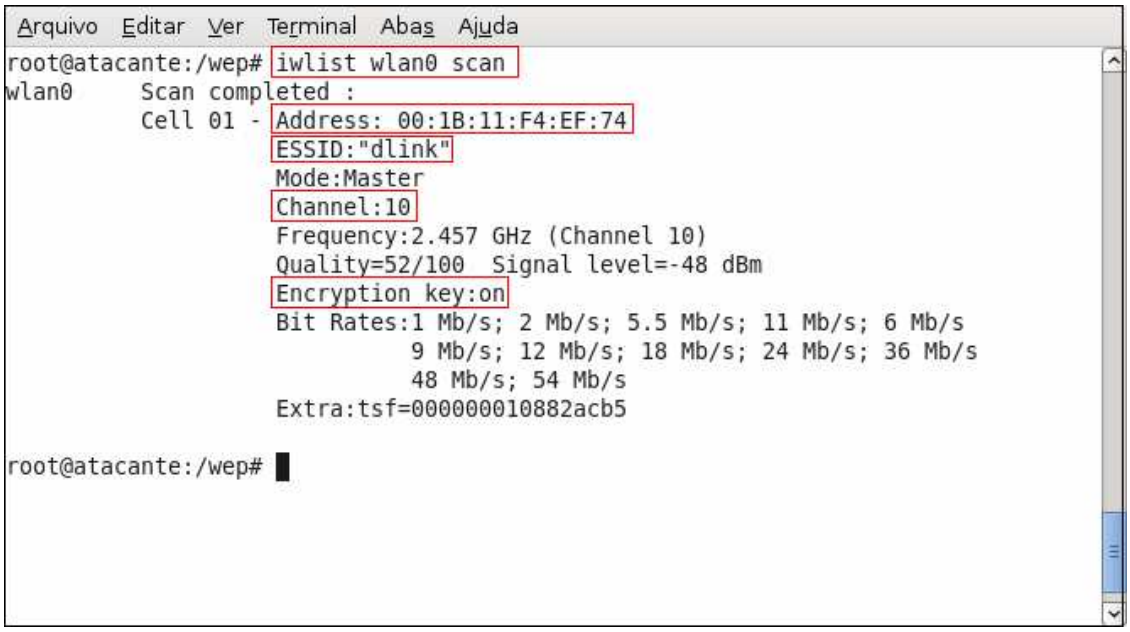


Figura 23. Saída do comando iwlist.

Conforme a Figura 23, pode-se perceber que houve uma mudança de canal. Anteriormente o sinal era transmitido pelo canal 6 e agora foi alterado para o canal 10. Essa mudança foi proposital como maneira de diferenciar a rede atual da anterior que mostra que a captura e quebra funcionam em ambos os canais. Na saída do comando pode-se perceber que existe criptografia na rede. A Figura 24 apresenta a criptografia WEP 128 que foi habilitada no *access point* para esse teste.

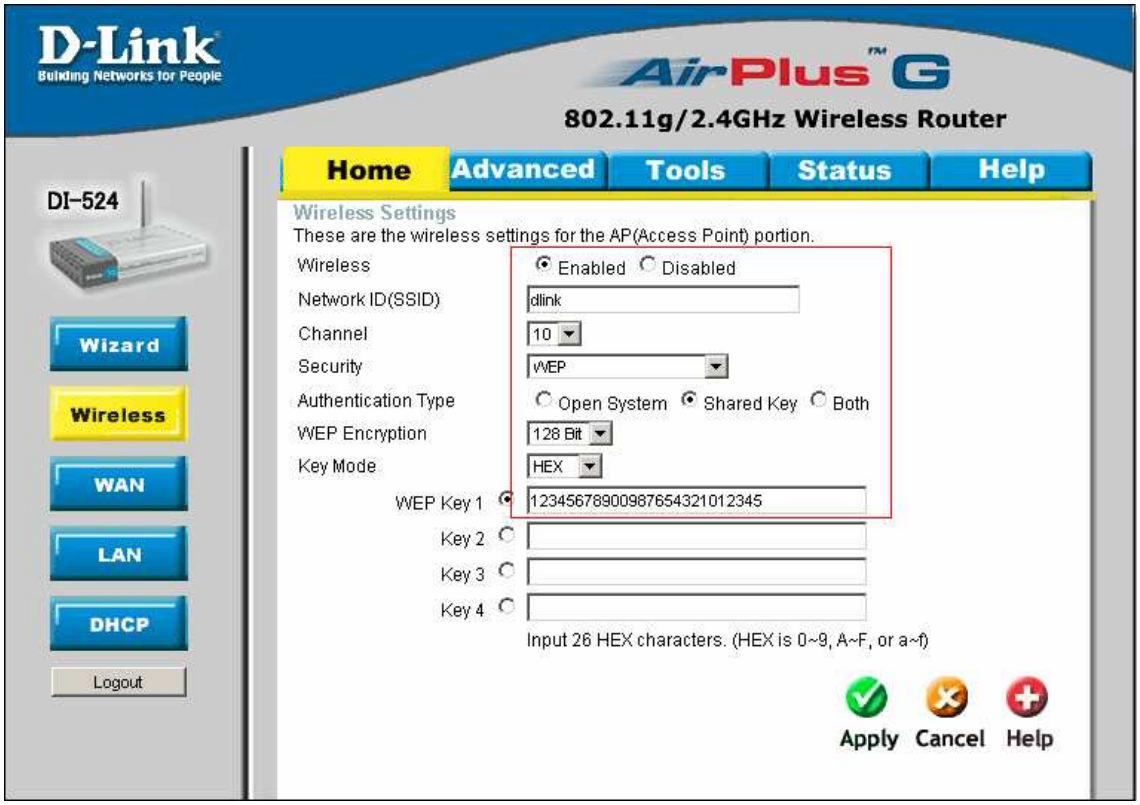


Figura 24. Criptografia WEP 128 *bits* habilitada no *access point*.

Após ter as informações necessárias sobre a rede, foi iniciada a interface sem fio em modo monitor com o comando: *"aimon-ng start wlan0"* e, em seguida, foi iniciada a captura dos IVs, sob o comando: *"airodump-ng -c 10 wep128 wlan0"*. Lembremos que a rede está transmitindo pelo canal 10 que serve como filtro para a captura. A Figura 25 demonstra a captura dos IVs na rede com criptografia WEP 128 *bits* habilitada.

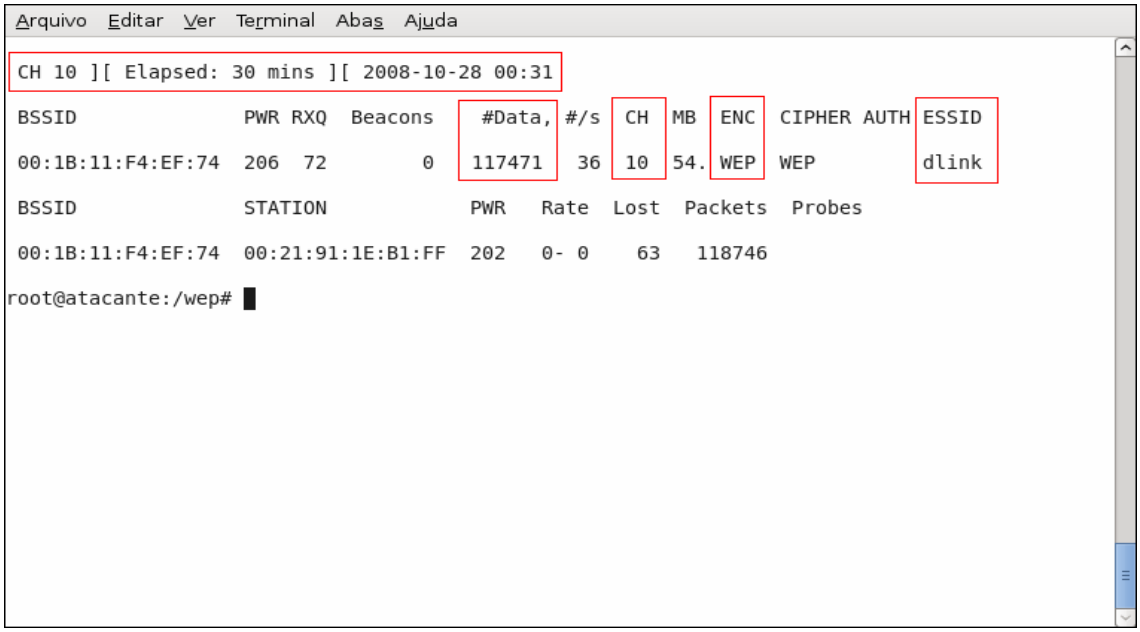


Figura 25. *Airodump-ng* capturando IVs.

Finalizando a etapa de quebra, foi executado o software *Aicrack-NG* sobre o arquivo wep128. O arquivo, contendo 117.471 IVs, foi testado por 293 chaves em 39 segundos, obtendo assim a chave “1234567890098765432101 2345” que realmente é a chave criptográfica da rede. A Figura 26 traz o processo de quebra da chave em 39 segundos.

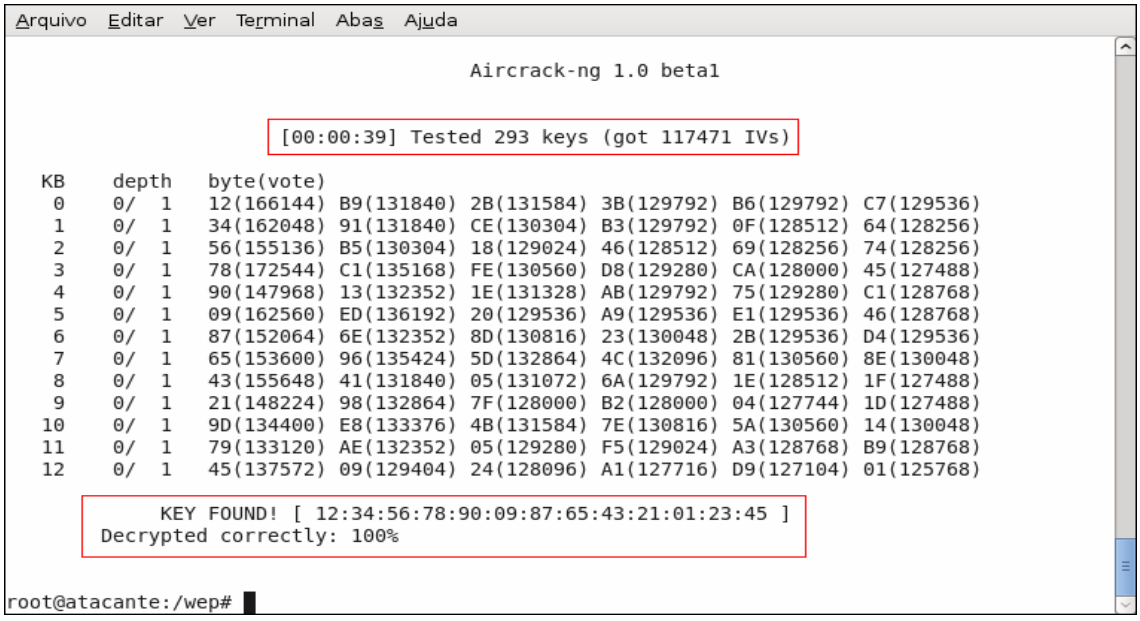


Figura 26. Criptografia WEP 128 *bits* quebrada por força bruta.

O Padrão WEP conforme comentário anterior, mostrou-se com um nível de segurança extremamente baixo, muito vulnerável a ataques, sendo que a variação do WEP 64 ou WEP 128 *bits* não garante mais segurança, pois a falha existe e o tamanho da chave só irá refletir no tempo de quebra.

Não é recomendado o uso desse padrão. Caso o equipamento utilizado não tenha outro tipo de encriptação, recomenda-se trocar a chave regularmente.

7.2.4 Presença do Protocolo WPA

Assim como o WEP, o WPA é um protocolo criptográfico, utilizado para embaralhar as informações que são transmitidas através de redes sem fio.

Entre as diversas variações do protocolo, foi testada a variação com o conceito de *Pre Shared Key (PSK).* O protocolo WPA também utiliza vetores de inicialização (IVs) na formação do pacote criptográfico.

7.2.4.1 Quebrando WPA-PSK com TKIP

O *Temporal Key Integrity Protocol* (TKIP) é um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacotes. A sua principal característica é a freqüente mudança de chaves que garante mais segurança à rede.

A Figura 27 mostra a chave criptográfica WPA-PSK com o algoritmo TKIP habilitada no AP. Além dessa alteração, foi alterado o nome da rede para “tcc” e o canal para “11” a fim de diferenciar a rede atual da anterior utilizada na quebra do protocolo WEP.

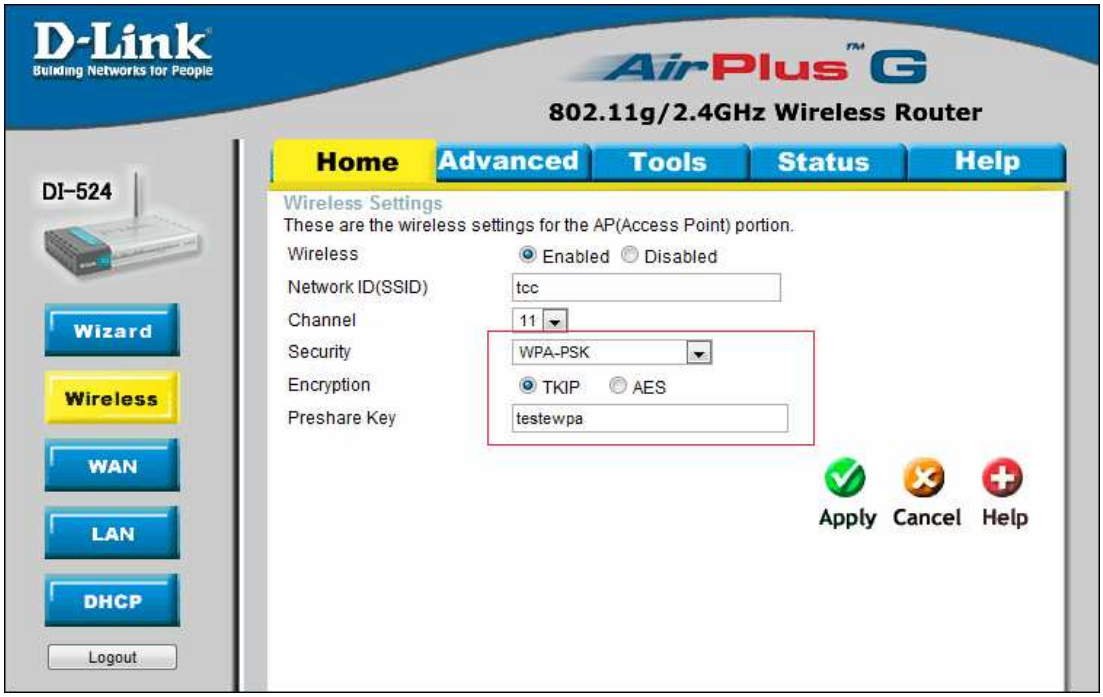


Figura 27. Chave criptográfica WPA-PSK com algoritmo TKIP habilitada no AP.

O processo de quebra de uma chave WPA é semelhante ao do WEP e consiste nos seguintes passos:

a) obter informações da rede que se deseja atacar;

b) iniciar interface em modo monitor;

c) iniciar a captura de IVs;

d) capturar a autenticação do usuário no *access point*;

e) realizar a quebra por meio de ataque de dicionário de dados.

Iniciando com o primeiro item, foi executado o comando "*iwlist wlan0 scan*" e obtida a saída exposta na Figura 28.

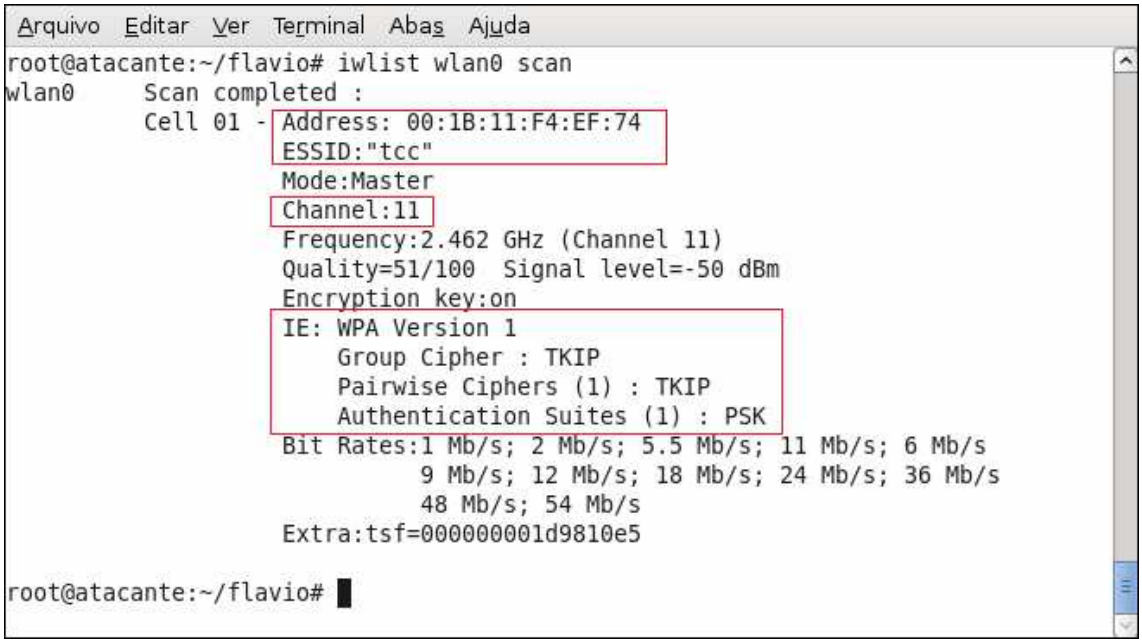


Figura 28. Saída do comando *iwlist*.

De acordo com o exposto anteriormente e por meio da Figura 28, pode ser percebido que a rede agora tem o nome “tcc” e está sendo transmitida pelo canal 11. Vemos, também, que está com encriptação WPA (versão 1), autenticação PSK e com algoritmo criptográfico TKIP.

Continuando o teste foi iniciada a interface em modo monitor por meio do *Airmon-NG*. Uma vez que a interface esteve em modo monitor, foi iniciada a captura dos IVs com o comando: “*airodump-ng –c 11 –w wpa1_tkip wlan0"*, onde o parâmetro –c se refere ao canal (11), o parâmetro “-w” ao nome do arquivo que vai conter os IVs e “wlan0” a interface de rede sem fio. A Figura 29 exibe o comando sendo executado.

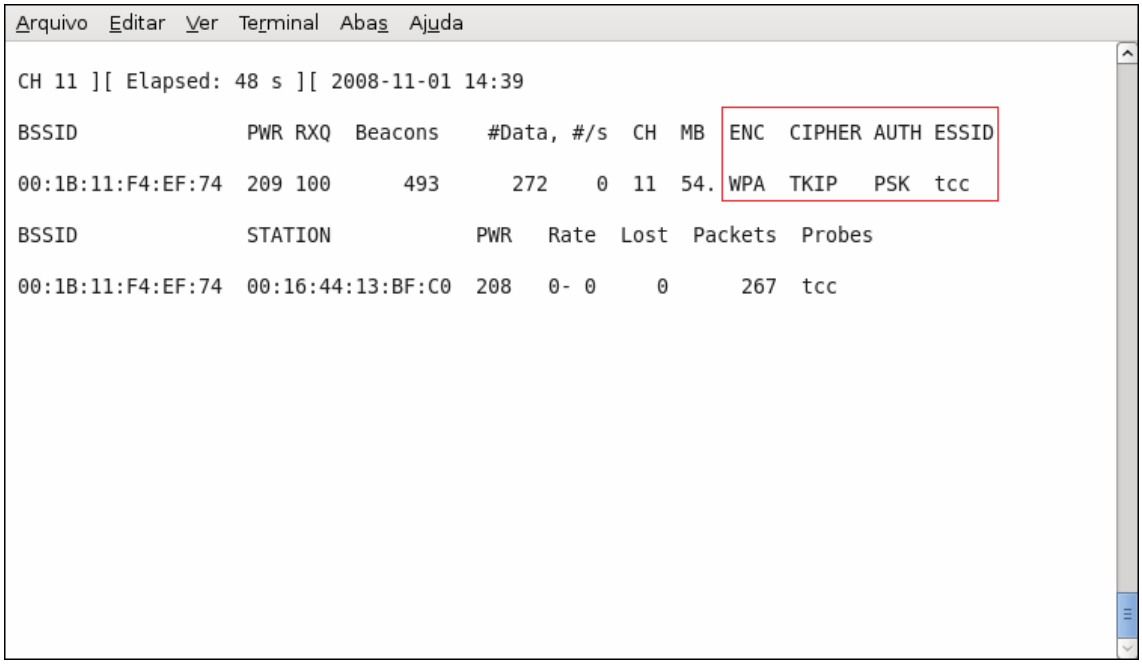


Figura 29. *Airodump-NG* iniciando captura de IVs.

A etapa seguinte do ataque consiste em capturar a autenticação do usuário no *access point*. A captura da autenticação é necessária, pois nela estão contidas informações da rede como criptografia, métodos de compressão e chaves secretas, que são indispensáveis para o *software* Aircrack-NG executar a quebra da chave.

Para isso, foi deixado o terminal atual capturando, e foi aberto outro terminal, sendo executado o comando "*aireplay-ng --deauth 1 -a 00:1B:11:F4:EF:74 -c 00:16:44:13:BF:C0 wlan0*". O primeiro parâmetro "--deauth 1" se refere ao processo de desconexão. O parâmetro "-a" se refere ao endereço MAC do *access point* e o parâmetro "-c" ao endereço MAC da máquina do usuário que está sendo atacada.

Esse comando faz com que o computador do atacante envie um pacote ao *Access Point*, simulando o processo de desconexão do usuário conectado. A Figura 30 exibe a saída do comando.

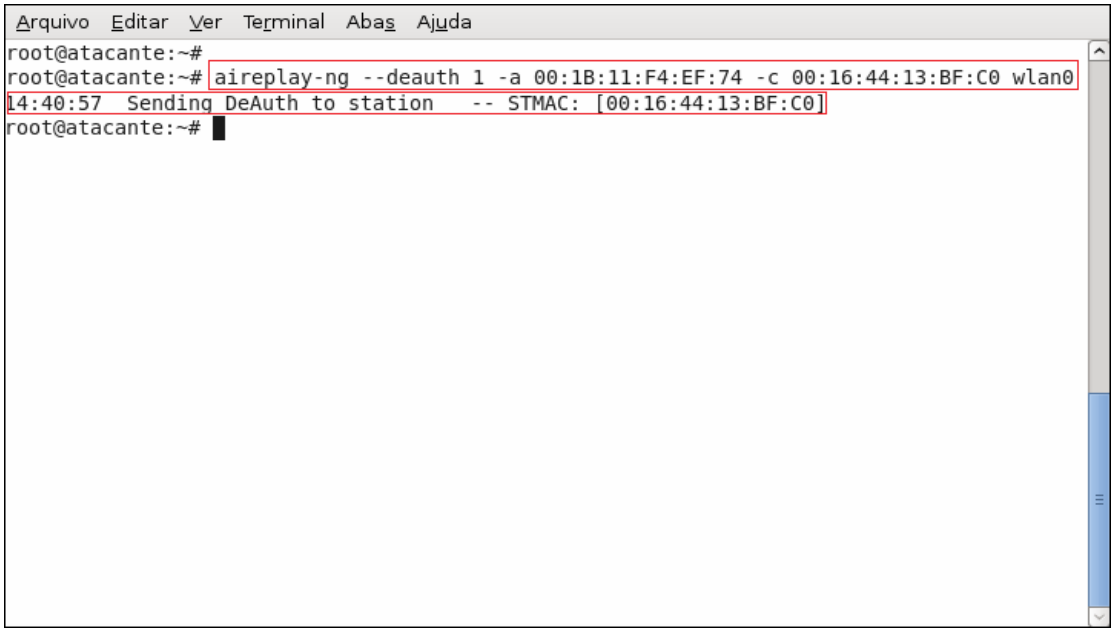


Figura 30. Envio de pacote de desconexão de rede.

Enganado pelo pacote, o *access point* faz com que o usuário se re-autentique, um processo que é executado de forma automática pela maioria dos sistemas operacionais. Com isso, o processo de autenticação será gravado pela captura que está sendo executado pelo outro terminal, conforme a Figura 31.

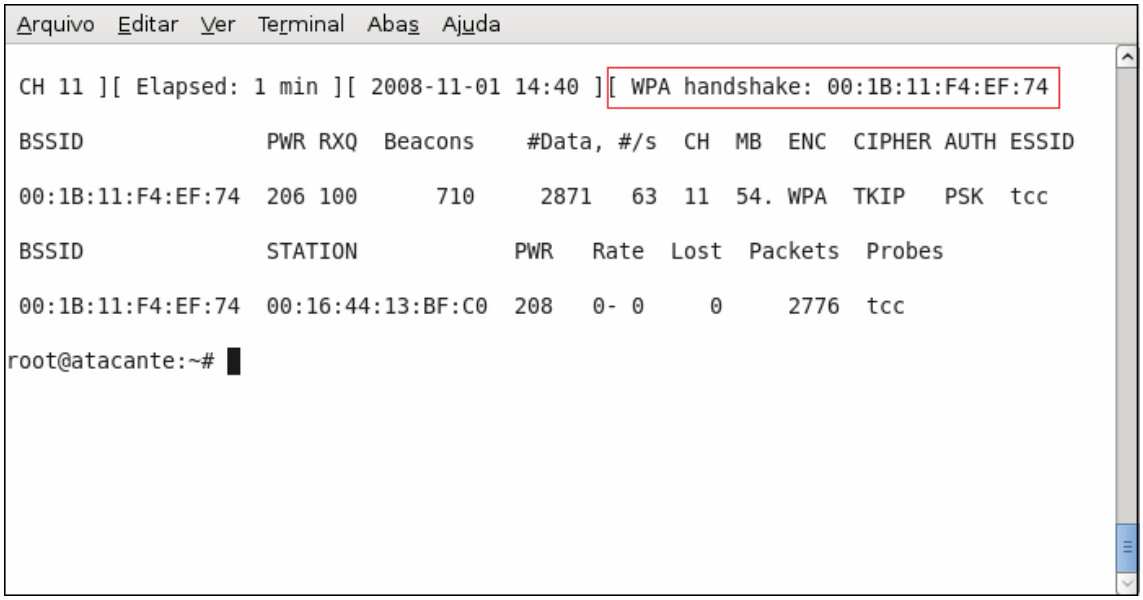


Figura 31. Autenticação no *access point*.

A indicação WPA *handshake*[4] significa que a máquina está autenticada no *access point*. Essa autenticação foi gravada no arquivo de captura dos IVs, sendo que sem gravar o processo de autenticação (*handshake*) não será possível efetuar a quebra da chave criptográfica.

Após a captura dos IVs e da autenticação foi possível iniciar a quebra da chave. Foram capturados 54.762 IVs durante 22 minutos conforme apresenta a Figura 32.

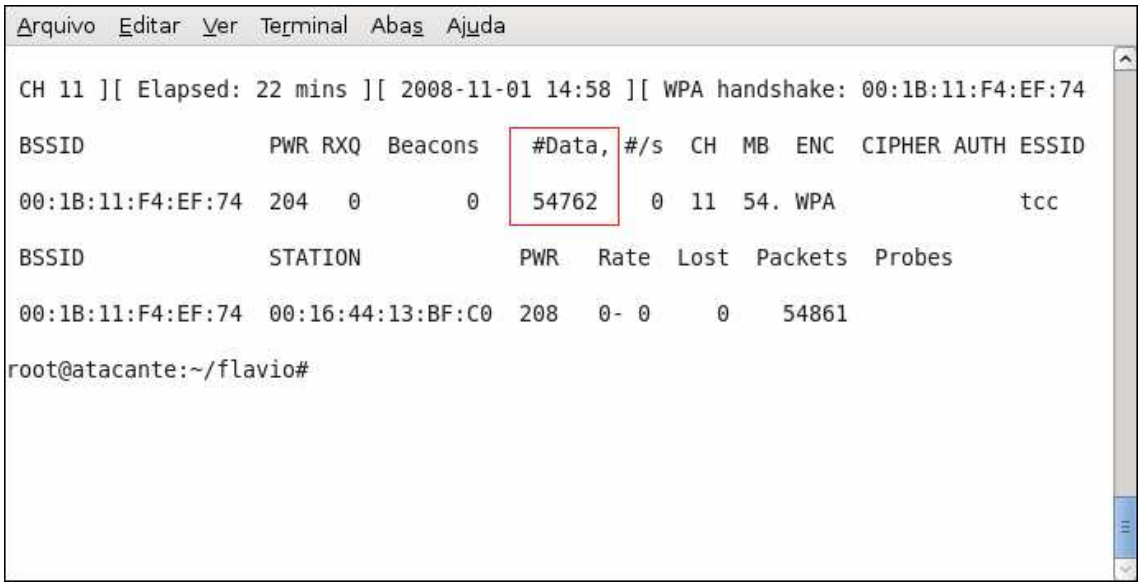


Figura 32. Captura de IVs por meio do software *airodump-ng* após 22 minutos.

Conforme o texto da sessão 5.2.1, é possível verificar que o WPA possui IVs com 48 *bits*, tornando o ataque por força bruta inviável, devido ao tempo de execução do mesmo. Desse modo, para quebrar a chave criptográfica WPA é necessário o uso de um ataque de dicionário.

O ataque de dicionário faz o uso de um arquivo de texto, conhecido também como *wordlist* com milhares ou até milhões de palavras. Assim, o *software* tenta adivinhar a chave, usando cada uma das palavras contidas no arquivo de dicionário.

[4] Protocolo de autenticação utilizado pelo protocolo WPA.

Um ataque de dicionário é geralmente mais eficiente do que um ataque de força bruta, visto que, normalmente, os usuários utilizarem senhas fracas. Alguns *softwares*, além de testarem cada palavra do arquivo, fazem combinações entre as palavras, multiplicando a quantidade de possibilidades testadas.

O passo seguinte para a quebra da chave foi executar o *Aircrack-NG* sobre o arquivo de IVs capturado pelo *Airodump-NG*. Para iniciar a quebra, foi executado o comando: "*aircrack-ng –w wordlist.lst wpa1_tkip*.cap*". O parâmetro "-w" indica o nome do arquivo de dicionário e o parâmetro "*wpa1_tkip*.cap*" indica o nome do arquivo que contém a captura.

É importante ressaltar que pode ser feita mais de uma captura, sendo efetuada a quebra desses arquivos em um único processo de quebra.

A Figura 33 exibe a chave WPA quebrada por meio de ataque de dicionário em pouco mais de 1 segundo, sendo que nesse processo o *software* testou, em média, 31 chaves por segundo.

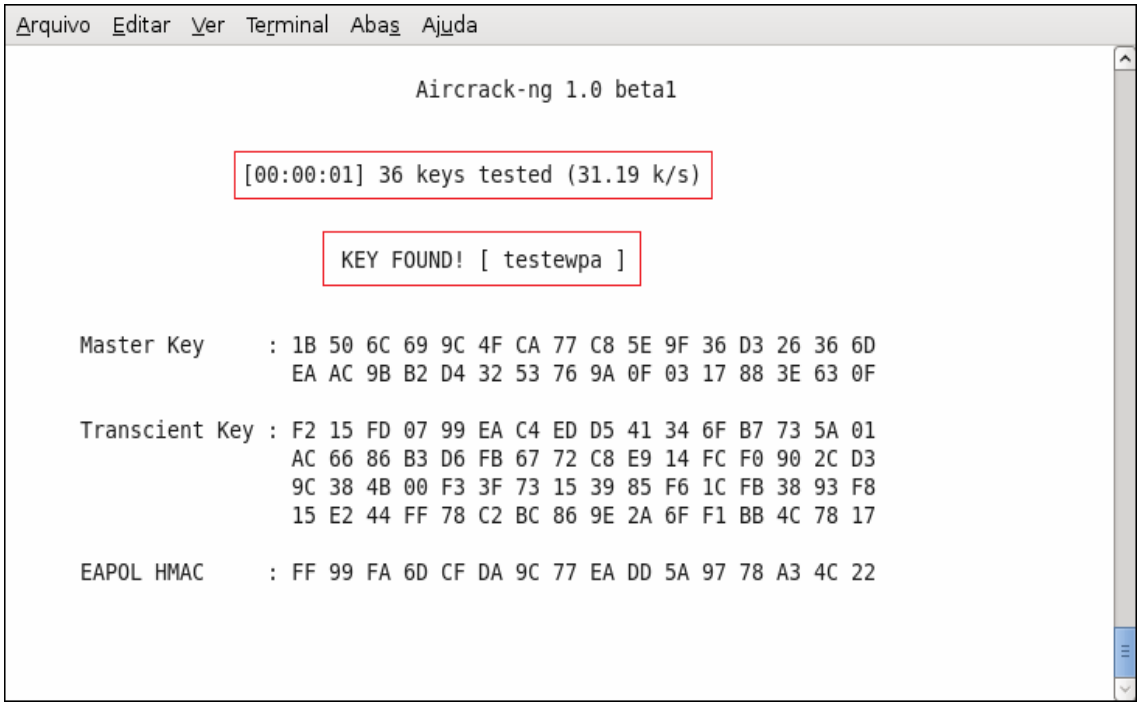


Figura 33. Processo de quebra da chave WPA.

A chave encontrada foi “testewpa” que realmente é a chave que foi configurada no *access point*. (Figura 27). Se essa chave, porém, não estivesse presente no dicionário utilizado no ataque, não seria possível a quebra da chave. Desse modo, a *wordlist* tem um papel fundamental para que se possa quebrar a criptografia WPA.

Às vezes é necessário testar com mais de um dicionário até que se quebre a chave com sucesso. A Figura 34 apresenta um processo de quebra sem sucesso.

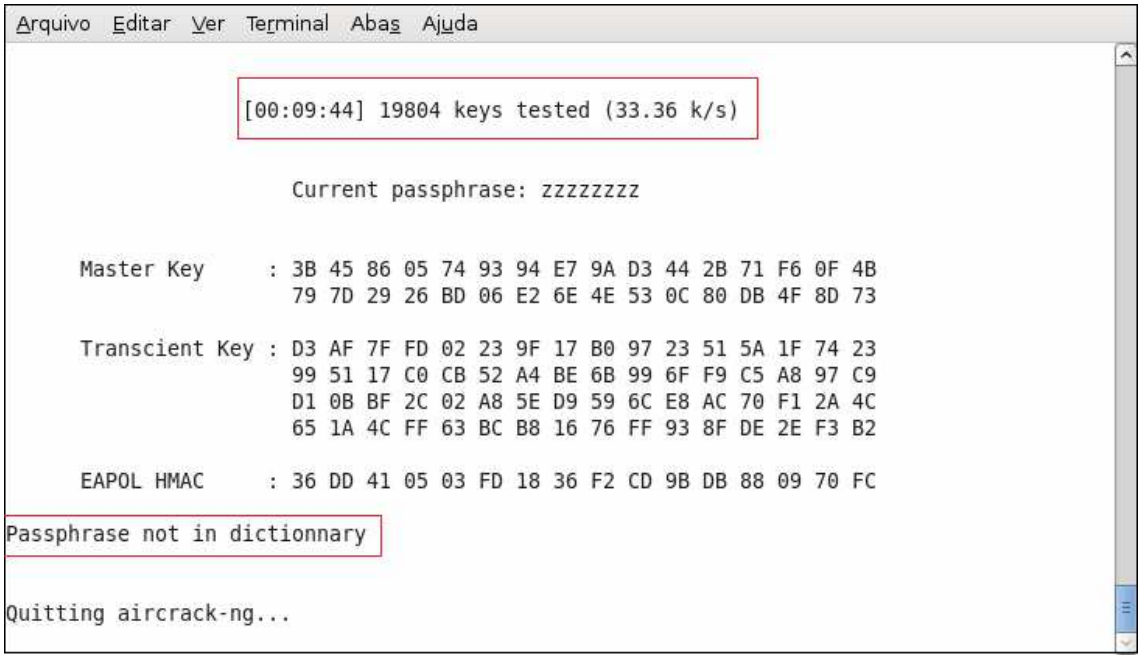


Figura 34. Quebra de chave WPA sem sucesso.

Como pode ser visto na Figura 34, testando em média 33 chaves por segundo, o *software* executou a procura por quase 10 e não obteve a chave, pois a mesma não estava contida no dicionário. Nesse caso, é necessário utilizar outro dicionário para o ataque. Muitas vezes é necessário utilizar vários dicionários até se obter a chave com sucesso.

7.2.4.2 Quebrando WPA-PSK com AES

O protocolo criptográfico *Advanced Encryption Standart* (AES) tem como fundamento dividir os dados em blocos para criptografar cada bloco separadamente. O AES, particularmente, faz uso de blocos de 128 *bits*. Em princípio, quanto maior o bloco, mais seguro o algoritmo. A chave usada para a criptografia é a mesma para todos os blocos.

Nessa parte do teste foi habilitada no AP a chave WPA-PSK como o algoritmo AES, conforme Figura 35.

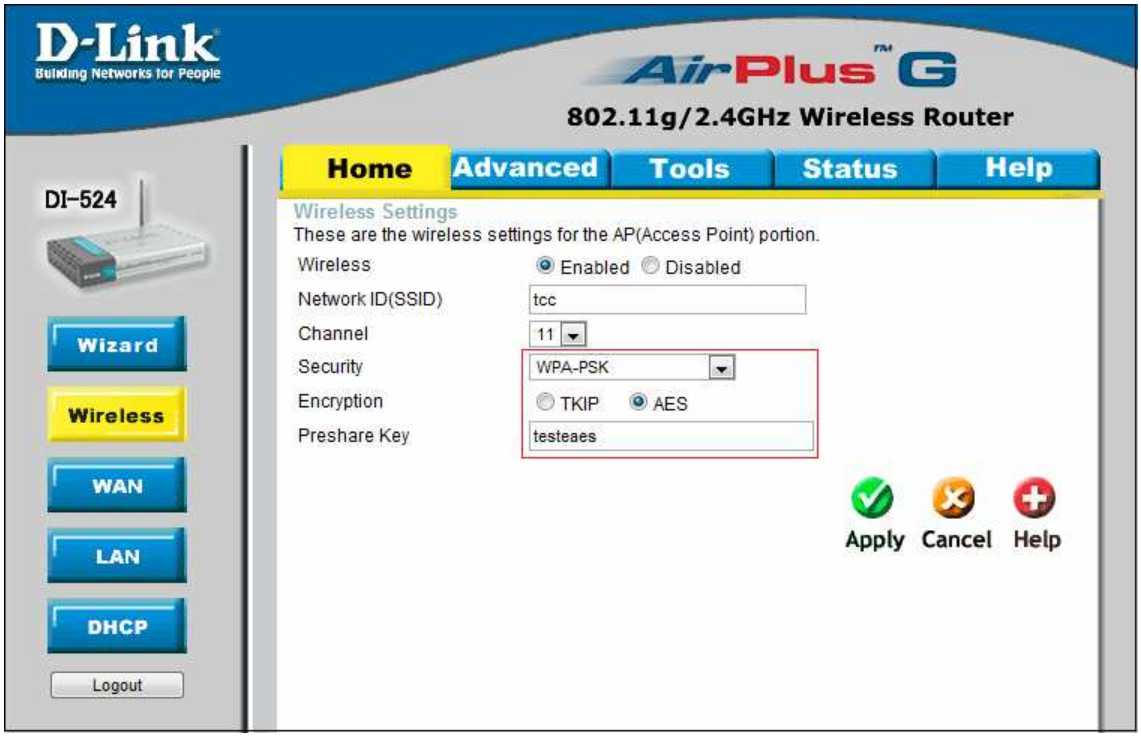


Figura 35. Segurança WPA-PSK com algoritmo AES habilitada no *access point*.

As etapas para a quebra da chave criptográfica WPA-PSK com algoritmo AES são as mesmas utilizadas na quebra do TKIP. Iniciando o ataque, foram coletadas as informações da rede, por meio do "*iwlist*".

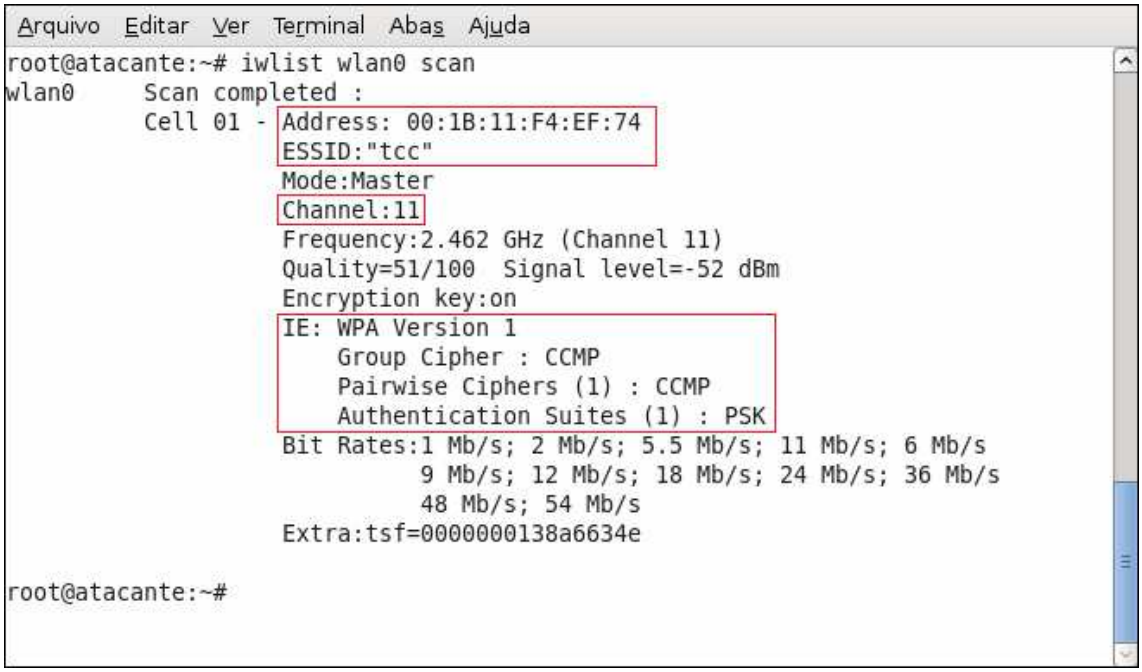


Figura 36. Informações da rede obtidas pelo comando *iwlist*.

Na Figura 36 pode ser visualizada a rede cujo nome é “tcc” com criptografia WPA (versão 1), autenticação PSK e algoritmo CCMP. O algoritmo AES também é conhecido como AES-CCMP e no *Linux* é identificado somente como CCMP.

Continuando o teste, foi colocada a interface em modo monitor e, em seguida, deu-se início à captura sob o comando “*airodump-ng -c 11 -w wpa1_aes”*.

Por se tratar de uma chave WPA, também foi necessário executar o comando de desconexão do usuário autenticado, fazendo com que ele se conectasse novamente, capturando a autenticação. A Figura 37 exibe a captura.

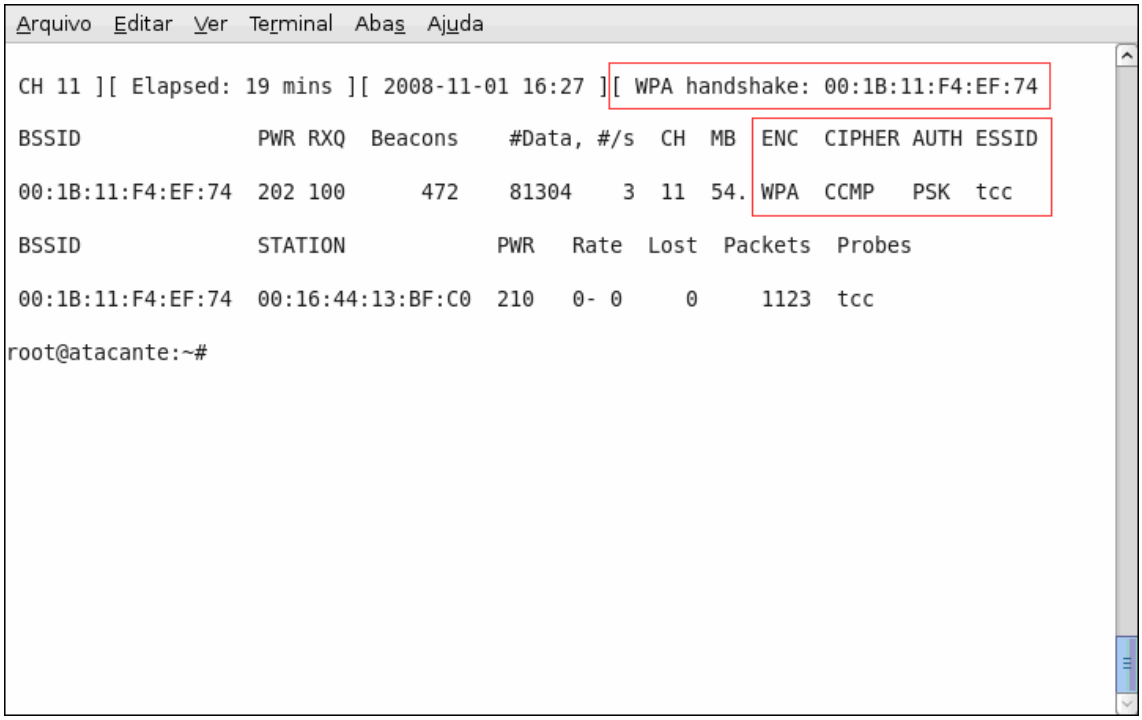


Figura 37. Captura de IVs com criptografia WPA-PSK e algoritmo AES.

A Figura 37 apresenta cerca de 81.000 IVs capturados nesse ataque. Por ser uma quantidade considerável, foi iniciada a quebra. O comando executado foi "*aircrack-ng –w wordlist.lst wpa1_aes*.cap*" que é o mesmo do outro ataque, alterando somente o nome do arquivo para *wpa1_aes*. Para esse ataque foi utilizado o mesmo dicionário do ataque ao algoritmo TKIP.

Após 8 horas e 56 minutos o *Aircrack-NG* conseguiu determinar a chave "*testeaes*" contida no *access point* e, conseqüentemente, a entrada no mesmo sem maiores dificuldades. A Figura 38 exibe a quebra sucedida.

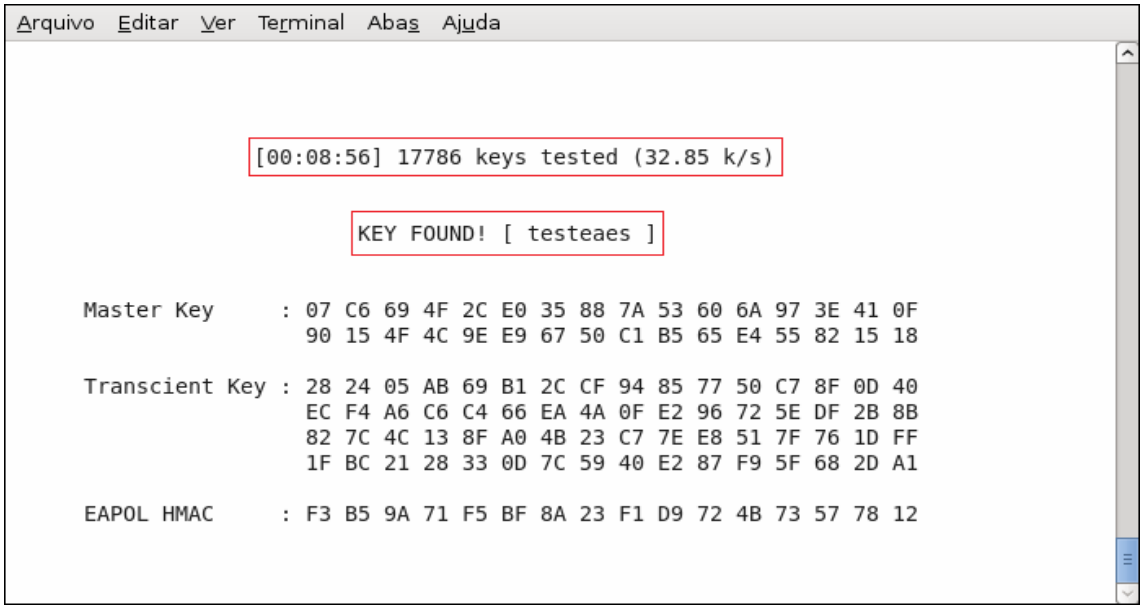


Figura 38. Chave criptográfica WPA-PSK com algoritmo AES encontrada.

Mediante os testes executados nos algoritmos TKIP e AES, verificou-se que o algoritmo AES levou uma quantidade de tempo considerável para a quebra em relação ao TKIP, sendo que o processo de captura foi o mesmo para os dois algoritmos.

O AES, se utilizado com uma chave mais elaborada, se torna mais difícil de ser quebrado. Mesmo assim, a quebra não é impossível. Ele apenas, na melhor das hipóteses, torna o ataque computacionalmente inviável, ou seja, o tempo ou o custo para que o algoritmo seja quebrado é maior que o tempo de vida ou o valor da informação criptografada respectivamente.

O dicionário de palavras tem um papel fundamental na quebra. De nada adianta capturar vários IVs da rede se não há em mãos um dicionário bem completo. É ele quem garante o sucesso da quebra. O dicionário utilizado nos testes é chamado *wordlist*, tem o tamanho de 40 *megabytes* e cerca de 6.000.000 de palavras. Foi baixado do site www.astalavista.com.br, que contém vários dicionários de várias línguas. O ideal para um atacante é fazer a concatenação de vários dicionários, obtendo um dicionário completo.

7.2.5 Presença do Protocolo WPA2

Nos testes sobre o protocolo WPA2 foi utilizada a variação WPA2-PSK com algoritmo AES. Foi configurada no *access point* a criptografia WPA2, conforme a Figura 39.

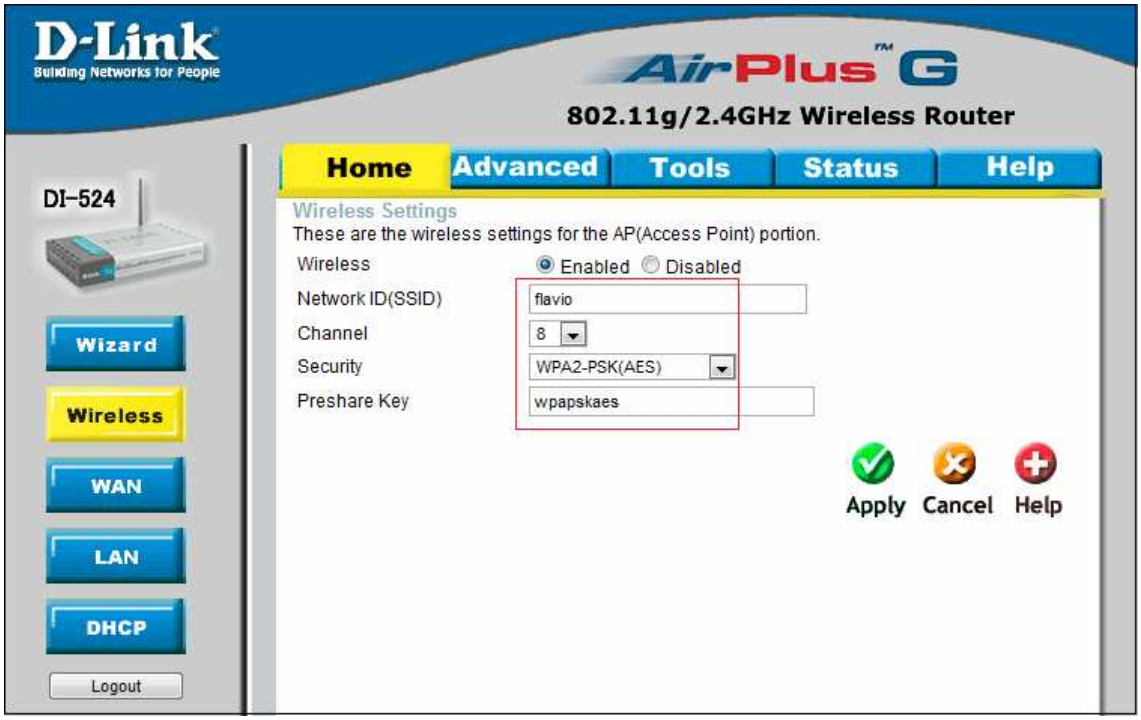


Figura 39. Segurança WPA2-PSK com algoritmo AES habilitada no *access point*.

O processo de quebra do protocolo WPA2 é idêntico ao utilizada na quebra do WPA (versão 1). Foi iniciado com a pesquisa de informações da rede por meio do *iwlist*.

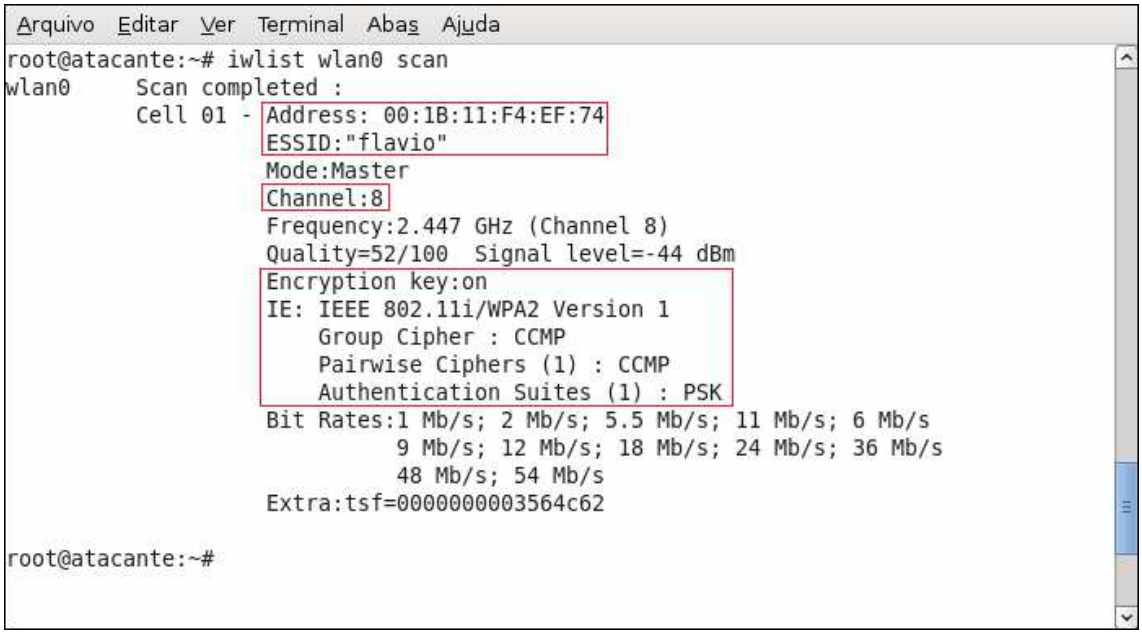


Figura 40. Saída do comando *iwlist*.

A saída do comando *iwlist* na Figura 40 exibe a chave WPA2, também conhecida como 802.11i, habilitada com autenticação PSK e algoritmo CCMP (AES).

Com essas informações foi iniciada a captura dos dados da rede sob o comando: *"airodump-ng –c 8 – w wpa2-psk wlan0"*. Vale lembrar que foram executados os mesmos procedimentos da quebra da chave WPA versão 1: pôr a interface em modo monitor antes de iniciar a captura e, durante ela, forçar a autenticação do usuário no *access point*, a fim de capturar a autenticação do mesmo por meio do *airodump-NG*.

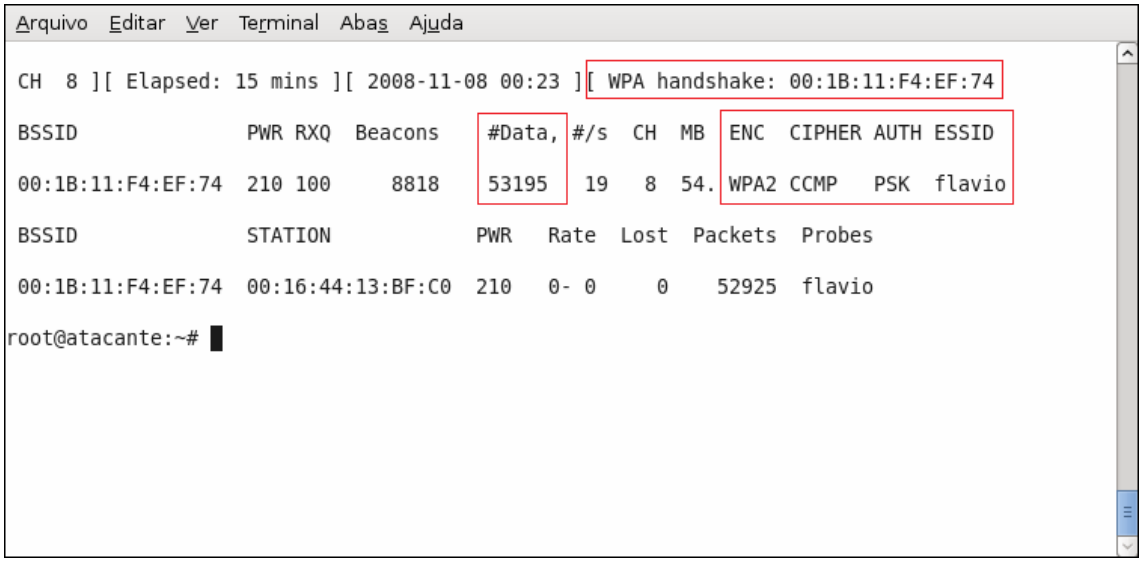


Figura 41. *Airodump-NG* capturando IVs com protocolo WPA2 habilitado.

A captura de cerca de 53.000 IVs levou 15 minutos, sendo que não foi gerado tráfego sobre essa captura. Iniciando a quebra foi executado o comando *"aicrack-ng –w wordlist.lst ./ wpa2-psk*.cap"*e, após 9 minutos e 34 segundos de execução, o *software* conseguiu determinar a chave "*wpapskaes*", que realmente é a chave que estava implementada no *access point,* exibido na Figura 39.

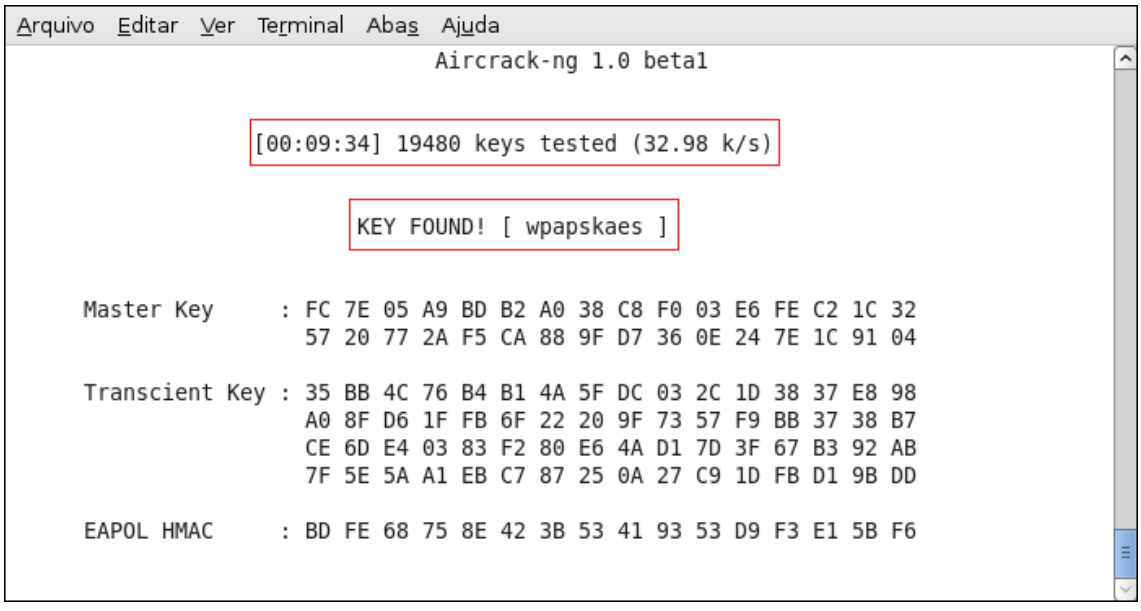


Figura 42. Quebra da chave WPA2 por meio do *Aircrack-NG*.

Mediante esse teste, conclui-se que não adianta utilizar um protocolo criptográfico robusto se a chave implementada nele não for bem elaborada. Como prova disso, foi realizado um segundo teste com uma chave bem elaborada, fazendo o uso de caracteres maiúsculos, minúsculos, caracteres especiais e números. A Figura 43 exibe a chave “TEsteSEnha23465~@#$tccfinal)(*&” configurada no *access point*.

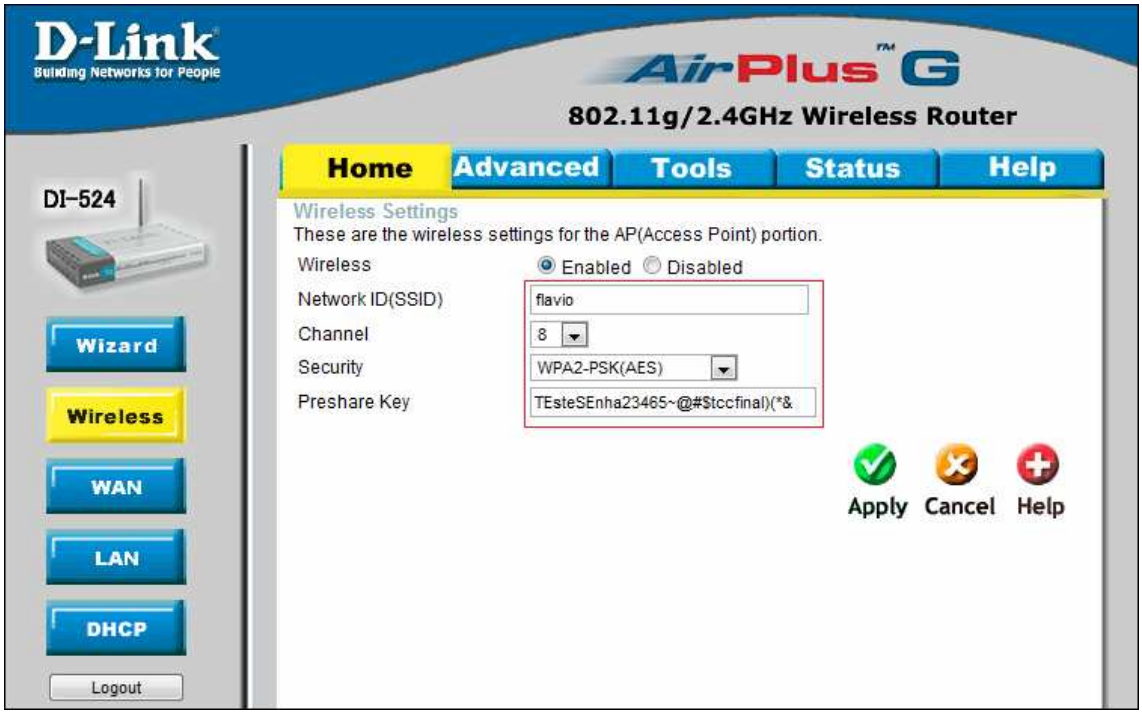


Figura 43. Segurança WPA2-PSK com algoritmo AES com chave elaborada.

Foi realizada a captura dos IVs com os mesmos passos anteriores da quebra do WPA com respectivo início da quebra da chave. O *software* executou por mais de 19 horas, testando mais de 2.340.000 combinações e não havia encontrado a chave, e o dicionário utilizado para a quebra possuía mais de 6.400.000 chaves. A Figura 44 exibe esse processo.

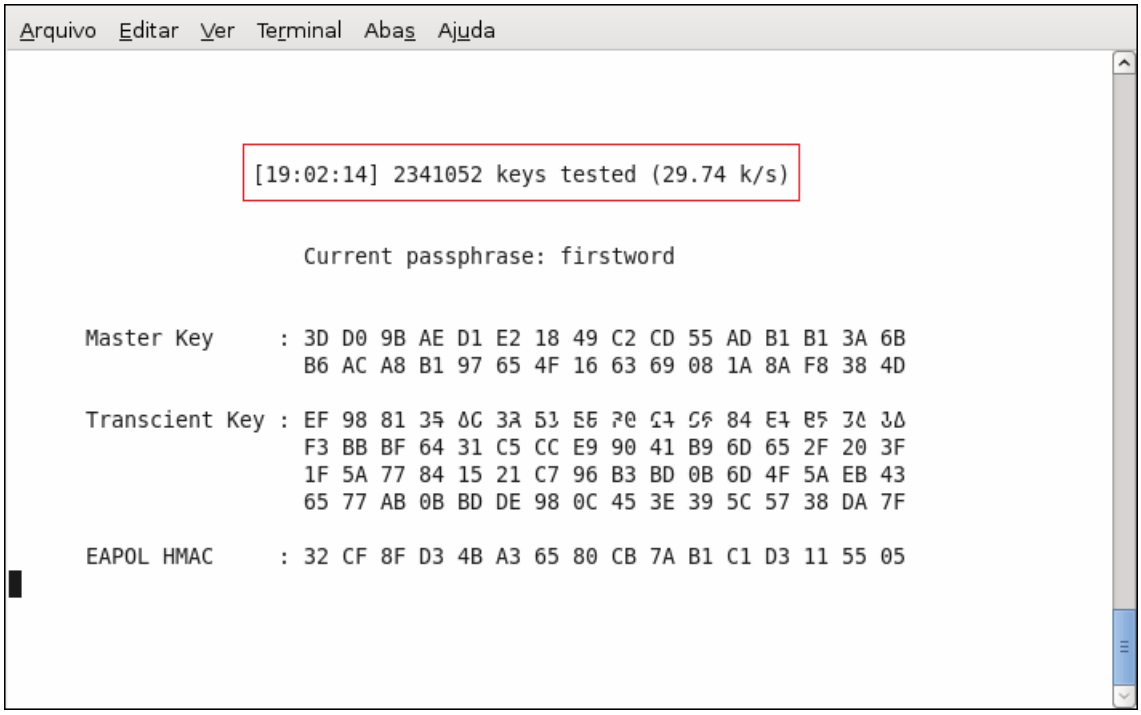


Figura 44. *Aircrack-NG* executando quebra a mais de 19 horas.

Tendo como base o segundo teste pode ser concluído que uma chave bem elaborada é uma forma de melhorar significativamente a segurança em uma rede sem fio.

7.3 RESULTADOS OBTIDOS

Com os testes realizados por meio desta pesquisa, foi possível chegar a alguns resultados a respeito da segurança em redes sem fio. Observou-se que o protocolo WEP, possui maior vulnerabilidade diante dos outros. Independente do tamanho da chave 64 ou 128 *bits* e da senha utilizada, este apresenta um nível de segurança baixo, estando restrito somente ao alcance do sinal. Assim, o uso desse protocolo criptográfico deve ser evitado sempre que possível.

No que se refere aos protocolos WPA e WPA2, foi observado que são mais seguros que o protocolo WEP, porém, ainda nem todas as vulnerabilidades foram resolvidas de forma satisfatória. As quebras efetuadas nesses protocolos durante os testes foram possíveis somente em chaves com senhas consideradas fracas, com poucos caracteres ou seqüências muito lógicas. Utilizando chaves com senhas fortes, frases com caracteres maiúsculos, minúsculos, numéricos e caracteres especiais, não foi possível efetuar a quebra em função do aumento de tempo de execução para que o *software* possa determinar a chave, podendo chegar a considerar uma estimativa de tempo acima de um ano na tentativa da quebra da chave. Essa quebra está limitada também ao dicionário de dados utilizado durante a etapa de realização do ataque, sendo que senhas consideradas fortes dificilmente estão contidas em dicionários, até podem ser descobertas, porém em um tempo não hábil.

O nível de segurança de uma rede sem fio pode ser aumentado de forma significativa, utilizando uma senha considerada forte. É importante também efetuar a troca dessa senha periodicamente. Em muitos casos a segurança de uma rede sem fio é comprometida pela configuração atribuída a esta, por falta de conhecimento dos usuários no que diz respeito à configuração dos equipamentos. Quando se trata de uma

rede corporativa onde requer um nível maior de segurança, é necessário um conhecimento maior a cerca da configuração dos dispositivos, e assim tentar garantir, um nível de segurança desejado.

CONCLUSÃO

Este trabalho demonstrou, por meio das pesquisas e testes práticos, as vulnerabilidades existentes nos protocolos WEP, WPA e WPA2, como explorá-las e como minimizar os perigos existentes na transmissão de dados em uma rede sem fio.

Prover segurança em uma rede na qual as informações trafegam pelo ar é uma tarefa extremamente difícil, sendo que os dados ficam expostos de maneira muito mais fácil de serem capturados em relação a uma rede cabeada. Garantir 100% de segurança em uma rede sem fio é totalmente impossível com os protocolos atuais, porém novos protocolos e métodos de segurança estão surgindo para sanar esses problemas. O que pode ser feito é minimizar as vulnerabilidades existentes, dificultando ao máximo os ataques.

Constantemente têm surgido novas padronizações de protocolos com o intuito de minimizar as vulnerabilidades e melhorar o desempenho dos mesmos, cabe aos usuários um melhor entendimento e atualização a cerca dos protocolos, de forma a melhorar o nível de segurança.

O presente trabalho contribui signitivamente para outras pesquisas relacionadas na área. Trabalhos futuros podem ser realizados a cerca de novos padrões seguindo a metodologia descrita nesse documento.

Por fim, este trabalho contribui deixando um capítulo, na forma de apêndice, de fácil leitura e entendimento que pode ser utilizado tanto por usuários de rede sem fio quanto para administradores para criar infra-estruturas de comunicação cada vez mais flexíveis, sem deixar de lado a segurança da informação.

REFERÊNCIAS

AGUIAR, Paulo Américo Freire. **Segurança em Redes Wi-Fi**. 2005. 79 f. Projeto Orientado de Conclusão de Curso (Bacharel em Sistemas de Informação) – Universidade Estadual de Montes Claros, Montes Claros, 2005.

Aircrack-NG Site official. Disponível em: <http://www.aircrack-ng.org/doku.php?id=aircrack-ng.pt-br> Acesso 14 de Out. de 2008.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p.

BURNETT, S. **Criptografia e segurança:** o guia oficial RSA. Tradução de Edson Furmankiewicz. Rio de Janeiro: Campus, 2002.

CARUSO, Carlos A. A. **Segurança em informática e de informações.** São Paulo: SENAC, 1999.

CARVALHO, D.B.: **Segurança de dados com criptografia:** Métodos e Algoritmos; Book Express, 2000.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 4 de Jun. 2009.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Cartilha de Segurança para internet Disponível em: <http://cartilha.cert.br/bandalarga/sec2.html >. Acesso em: 10 de Set. 2008.

CHESWICK, W.; BELLOVIN, S. M. ; RUBIN. A. D.; **Firewalls e Segurança na Internet**. 2.ed. Porto Alegre. Bokman. 2005.

COWPATTY. Disponível em: <http://wirelessdefence.org/Contents/coWPAttyMain.htm>. Acesso em: 11 de Jun. 2008.

D-LINK. DIR 635. Disponível em: <http://www.dlinkla.com/home/productos/producto.jsp?idp=928>. Acesso 29 de Abr. 2008.

D-LINK. DWA 520. Disponível em: <http://www.dlinkla.com/home/productos/producto.jsp?idp=1045>. Acesso 29 de Abr. 2008.

DECISÃO SOBRE UMA ESTRATÉGIA DE REDE SEM FIO PROTEGIDA. Disponível em: <http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx> Acesso em: 14 de Mar. 2007.

DIAS, Adilson de Souza. **Wap: wireless application protocol, a internet sem fios.** São Paulo: Ciência Moderna, 2000.

DORNAN, Andy. **Wireless communication:** o guia essencial de comunicação sem fio. Rio de Janeiro: Campus, 2001.

EDUCAR. **Saúde e Raios X**. Disponível em: <http://educar.sc.usp.br/licenciatura/2003/rx/>. Acesso em: 29 Abr. 2008.

FERREIRA, F.N.; ARAUJO, **M.T. Política de Segurança da Informação**. Rio de Janeiro, Ciência Moderna, 2006.

FLUHRER, S.,MANTIN, I; SHAMIR, A. **Weaknesses in the key scheduling algorithm of RC4**. In Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, Aug. 2001.

GIMENES, Eder Coral. **Segurança em Redes Wireless**. 2005. 58 f. Monografia. (Curso Tecnólogo em Informática com ênfase em Gestão de Negócios) - Faculdade de Tecnologia de Mauá, Mauá.

IEEE STANDARS ASSOCIATION. IEEE 802.11: **LAN/MAN Wireless LANS**. Disponível em: <http://standards.ieee.org/getieee802/802.11.html>. Acesso em: 2 jun. 2008.

IEEE STANTARS ASSOCIATION. **IEEE 802.11i**. Disponível em: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>. Acesso em: 2 Jun. 2008.

INFORMAÇÃO SEGURA. Disponível em: <http://www.infosegura.eti.br/artigos/80211.php>. Acesso em: 14 Mai. 2008.

JUNIOR, Carlos Alberto de Carvalho Vaz Pereira; BRABO, Gustavo da Silva; AMORAS, Rômulo Augusto de Sales. **Segurança em Redes Wireless Padrão 802.11b:** Protocolos WEP, WPA e Análise de Desempenho. 2004. 75 f. Monografia (Bacharel em Ciência da Computação) – Universidade da Amazônia, Belém, 2004.

KUROSE, James F; ROSS, Keith W. **Redes de Computadores e a Internet**: uma abordagem top-down. São Paulo: Editora Pearson Addison Wesley. 2005.

LINKSYS. A Division of Cisco. Disponível em: <http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1162354643512&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=4351239789B04>. Acesso: 30 de Abr. 2008.

MACHADO, Cássio Bobsin; BORN, Roger. **O impacto da tecnologia móvel na vida cotidiana**: The impact of mobile technology in daily life. Think: Caderno de Artigos e Casos Espm-rs, Porto Alegre , v. 4, n. 1 , p. 36-39, jan./jun. 2006

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

NORTHCUTT, Stephen et al. **Desvendando Segurança em Redes Sem Fio**. Rio de Janeiro: Ed. Campus, 2002.

PAIVA, Gilberto da Fonseca. **Segurança em Redes Sem Fio 802.11**. 2006. 36 f. Monografia de conclusão de curso (Especialista em Redes de Computadores e Comunicação de Dados) – Universidade Estadual de Londrina, Londrina, 2006.

RNP Rede Nacional de Pesquisa. Disponível em: <http://www.rnp.br/newsgen/9805/wireless.html> Acesso 10 de Out. de 2008.

RODRIGUES, Junior Trajano. **Segurança na Transmissão de Dados por Bluetooth em Ambientes Móveis.** 2007. 92 f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Universidade do Extremo Sul Catarinense, Criciúma, 2007.

RUFINO, Nelson Murilo de O. **Segurança em Redes Sem Fio:** aprenda e proteger suas informações em ambientes WI-FI e Bluetooth. São Paulo: Editora Novatec, 2005

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003. 156 p.

SILVA, Lino Sarlo da. **Virtual Private Network.** São Paulo: Novatec, 2003. 240 p

TANENBAUM, Andrew S. **Redes de Computadores**. São Paulo, Editora Campus, 2003. 632 p.

TEIXEIRA JUNIOR, José Helvécio. **Redes de computadores:** serviços, administração e segurança. São Paulo: Makron Books, 1999. 493 p.

TRADESYS. citrix metaframe link de radio wireless voip firewall digifort. Disponível em: <http://www.tradesys.com.br/wireless.htm>. Acesso 29 de Abr. 2008.

VACCA, John R. Guide to **Wireless Network Security**. Springer, 2006.

VERÍSSIMO, Fernando C. A. **Segurança em Redes sem fio.** 2002. 90 f. Monografia (Curso de Tópicos Especiais em Redes Integradas Faixa Larga) – Universidade Federal do Rio de Janeiro, Rio de Janeiro.

VLADIMIROV, Andrew; GAVRILENKO, Konstantin V.; MIKHAILOVSKY, Andrei A. Wi-Foo: **The Secrets of Wireless Hacking**. Indianápolis, Addison-Wesley, 2004.

WI-FI ALLIANCE. WPA: Wi-Fi Protected Access. Disponível em: <http://www.wi-fi.org/knowledge_center/wpa>. Acesso em: 30 de Abril 2008.

APÊNDICE A: DE REDES SEM FIO: GUIA DE BOAS PRÁTICAS

Após o conhecimento adquirido com o término dessa pesquisa foi possível criar um guia de boas práticas para a configuração e utilização das redes sem fios. Nesse apêndice serão abordadas boas práticas relacionadas relacionada as configurações no que tange a segurança.

1 ESCOLHA DO EQUIPAMENTO

Conforme foi mencionado no decorrer do trabalho, os APs saem de fábrica, por padrão, com as mínimas configurações de segurança. Assim, é imprescindível que certos cuidados sejam tomados.

Na escolha dos equipamentos que farão parte da rede sem fios devem ser tomados alguns cuidados. Devem ser analisados os tipos de protocolos de comunicação que são suportados pelo mesmo.

A maioria dos equipamentos existentes no mercado é compatível com os protocolos IEEE 802.11 a/b/g. Desse modo, comprar um equipamento que não suporte tais protocolos pode ocasionar problemas futuros como incompatibilidade entre os equipamentos.

Para garantir a compatibilidade entre os equipamentos, recomenda-se a aquisição de equipamentos com o certificado do *Wi-Fi Alliance*, Figura 45, órgão que certifica os padrões de comunicação em redes sem fios.

Figura 45. Modelo de selo de certificação da *Wi Fi Alliance*.
Fonte: *Wi Fi Alliance* (2008)

Apesar de não estar oficialmente homologado, o 802.11n é um padrão que começa a ser utilizado. Esse protocolo promete substituir os padrões a/b/g, pois a taxa de transferência de dados é maior. O padrão 802.11n utiliza várias antenas para a transmissão e recepção, evitando, assim, a perda de pacotes. Já existem no mercado equipamentos que se utilizam da tecnologia pré-n, a qual possui as mesmas características da futura norma, mais ainda não oficiais. A grande desvantagem desses equipamentos é o fato de não haver nenhuma garantia de compatibilidade com os equipamentos fabricados após a homologação do padrão. Testes já foram iniciados. A homologação, porém, tende a sair somente no ano de 2009.

Outro ponto a ser observado na aquisição de um equipamento são os protocolos de criptografia por ele suportados. De acordo com os vários exemplos apresentados nesse trabalho, o protocolo menos vulnerável é o WPA2. Os equipamentos mais antigos possuíam apenas WEP e WPA. A maioria dos equipamentos, no entanto, sai de fabrica hoje com o protocolo WPA2 implementado.

2 CONFIGURAÇÕES GERAIS

Após a escolha do equipamento, é aconselhável adotar algumas configurações básicas importantes para a segurança, principalmente na parte de identificação da rede.

3 SSID

A primeira preocupação nesse item é quanto ao identificador da rede (SSID). Esse identificador não deve ser um nome indutivo, que ligue a rede ao local onde ela está localizada. Em alguns casos, uma pessoa mal intencionada pode captar o sinal, porém de forma fraca. Se o nome da rede estiver referenciando o local, o possível atacante terá a opção de se aproximar para captar um sinal mais forte.

Outro item importante a ser considerado na aquisição de um AP é a opção de ativar ou não o envio do SSID por *broadcast*, ocultando o SSID da rede. Para se ter acesso à rede será necessário ter o conhecimento do nome da mesma, informando-o na configuração do dispositivo.

4 CANAL DE COMUNICAÇÃO E ALCANCE DO SINAL

Alguns modelos de *access point* possuem uma opção para diminuir o alcance do sinal do equipamento. Essa alternativa é interessante do ponto de vista de segurança, pois a diminuição na potência do sinal pode dificultar a tentativa de terceiros de identificar a rede.

Recomenda-se, então, que ao instalar um AP o responsável pela segurança defina até aonde o sinal do equipamento deve ir. Para isso, devem-se realizar alguns testes, diminuindo o sinal gradativamente até que chegue ao ponto de alcance necessário, não ultrapassando o mesmo.

5 FAIXA DE IP E DHCP

A maioria dos *access point* vem com a opção DHPC ativada. Para se obter uma maior segurança na rede é aconselhável que essa opção seja desativada. Com isso, os computadores ligados à rede estarão mais protegidos. Caso alguma pessoa não autorizada consiga acessar a rede, o atacante não terá nem o trabalho de descobrir as informações da rede, tendo assim acesso mais facilmente.

Por questões de flexibilidade e comodidade, é cada vez mais comum que a rede esteja configurada como endereçamento automático, onde da perspectiva de uma rede sem fio apresenta um risco ainda maior do ingresso não autorizado à rede. Com essa opção desativada, qualquer usuário que quiser acessar a rede deve, obrigatoriamente, ter conhecimento da faixa de IPs da rede.

Com relação ao IP, deve-se tomar cuidado, também, com a faixa de IPs utilizada na rede. A utilização de uma faixa de IPs não comum torna a rede mais segura.

Outra medida importante a ser adotada é a alteração do endereço IP do *access point*. Por padrão os APs tendem a vir com endereços como 192.168.0.1, 192.168.0.254, 10.0.0.1 ou 10.0.0.254. Uma vez que um ataque tenha sido efetuado com sucesso, e um invasor estiver na rede, esses serão os primeiros endereços testados para assumir o controle do AP. Sendo assim, a alteração do endereço padrão é uma forma inteligente para se agregar a segurança à rede.

6 PROTOCOLOS CRIPTOGRÁFICOS

A escolha do protocolo para codificar as mensagens transmitidas é, talvez, o ponto mais importante da configuração de uma rede sem fio. Conforme menção anterior, optar por não usar qualquer tipo de encriptação dos dados permite que pessoas não autorizadas tenham acesso à rede e aos dados que por ela trafegam.

No entanto, mesmo utilizando métodos de criptografia, uma rede sem fio não pode ser considerada totalmente segura. Mas, sem dúvidas, escolhendo os protocolos mais fortes, mais atuais e com menos falhas as possibilidades de roubo de dados ou acesso não autorizado diminuirão significativamente.

Entre os protocolos abordados nos capítulos anteriores, o protocolo WPA2, é sem dúvidas, o protocolo recomendado, apesar de uma grande maioria utilizar, ainda, o protocolo WEP ou WPA, devido ao não conhecimento ou a limitação do equipamento. Optar pelo WPA2 é o primeiro passo para agregar segurança na transmissão de dados em redes sem fio.

7 ESCOLHA DAS SENHAS

Na estrutura do *access point* existem dois tipos de senha. Uma para acesso às configurações do AP e outra para a criptografia. Para acessar as configurações do AP via HTTP, devemos informar o IP do equipamento seguido do usuário, geralmente admin e a senha, que costuma ser o nome do usuário. Recomenda-se que essa senha seja alterada no momento da configuração inicial, pois qualquer pessoa que a conheça poderá entrar nas configurações e alterá-las. Cada fabricante tem sua senha padrão que pode ser adquirida por qualquer pessoa por meio de manuais ou pesquisas na internet.

A outra senha é a da chave criptográfica. É relacionada ao acesso efetivo à rede sem fio. Ambos os protocolos abordados nesse trabalho funcionam com sistema de chave criptográfica. Nas configurações do AP, ao habilitar a criptografia da rede, é necessário registrar uma senha, na qual o protocolo se baseará para codificar os dados. Essa senha segue o mesmo princípio de qualquer outra. Quando maior e menos indutiva, melhor. Recomenda-se o uso de caracteres maiúsculos, minúsculos e caracteres especiais, dificultando que ela seja descoberta por meio de indução e dificultando a quebra pela força bruta.

8 RESTRIÇÃO POR MAC

Além da criptografia dos dados, existem outros métodos de agregar segurança a uma rede sem fio. A restrição por MAC *address*, por exemplo, tem como objetivo restringir o acesso à rede por meio do endereço físico do equipamento.

Uma vez que o endereço físico de uma placa de rede nunca se repete, é implementado nos *access point* a opção para cadastrar os endereços dos computadores que podem acessar a rede. Dessa forma, apenas os computadores cuja placa de rede estiver cadastrada no AP poderão acessar a rede.

9 UTILIZAÇÃO DE HOT SPOTS

Hot spots são locais públicos que disponibilizam acesso à internet por meio de redes sem fios. Geralmente são encontrados em hotéis, aeroportos, cafés, restaurantes, praças de alimentação, universidades, entre outros.

Apesar da comodidade, este ponto de acesso público pode trazer alguns problemas aos usuários, relacionados à segurança das informações que trafegam pela rede. Geralmente esses pontos de acesso não têm nenhum tipo de restrição ou criptografia implementada no AP. A única verificação feita é a de provedores de acesso à internet. Assim, os dados trafegam de maneira aberta, ficando vulneráveis a ataques.

Quando estiver acessando a internet por meio de um *hot spot*, recomenda-se não executar transações bancárias ou outros tipos de informações pessoais como e-mails e outros.