UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

EDUARDO SANTANA DA SILVA NETO

PESQUISA E ANÁLISE DOS PROTOCOLOS DE SEGURANÇA NAS IMPLEMENTAÇÕES DE REDES UTILIZANDO O PADRÃO IEEE 802.11

MONOGRAFIA

CURITIBA
2011

EDUARDO SANTANA DA SILVA NETO

PESQUISA E ANÁLISE DOS PROTOCOLOS DE SEGURANÇA NAS IMPLEMENTAÇÕES DE REDES UTILIZANDO O PADRÃO IEEE 802.11

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná Orientador: Prof. Msc Fabiano Scriptore de Carvalho

CURITIBA
2011

RESUMO

SILVA NETO, Eduardo S. **Pesquisa e Análise dos Protocolos de Segurança nas implementações de redes utilizando o padrão IEEE 802.11.** 2011.56f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

Este trabalho tem como tema central a segurança em redes sem fio. Estipular métodos de segurança em uma rede sem fio comparando os protocolos de segurança WEP, WPA e WPA2 é o objetivo principal deste trabalho. A pesquisa é de natureza aplicada, e explicativa quanto a seu propósito, utilizando apoio bibliográfico e de uma pesquisa de campo para coleta de informações sobre os pontos de acesso de uma organização de grande porte. A partir dessa coleta juntamente com o apoio bibliográfico se espera estipular critérios para se configurar uma rede sem fio, sendo possível aplicar esses critérios em qualquer ponto de acesso existente ou que será configurado.

Palavras chave: Segurança. IEEE. WEP. WPA. WPA2

ABSTRACT

SILVA NETO, Eduardo S. **Pesquisa e Análise dos Protocolos de Segurança nas implementações de redes utilizando o padrão IEEE 802.11.** 2011.56f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

This paper has its main subject the safety in wireless network. Stipulate the safety methods in a wireless network, comparing the protocols WEP, WPA e WPA2 is the focus of this paper. The research is applied and explanatory, as its purpose, using bibliographic support and a field research to collect information about the points of access in a great company. From this collect, along with the bibliographic support, we expect to define the criteria to configure a wireless network, making possible to apply these criteria in every point of access existent or those which will be configured.

Key Words: Security. IEEE. WEP. WPA. WPA2

LISTA DE FIGURAS

LISTA DE SIGLAS

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryptation Standart
CRC:	Cyclic Redudancy Checks
CSMA/CA	Carrier Sense Multiple Access/Colision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Colision Detection
CTS	Clear to Send
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol – Tunneled Transport Layer Security
FCC	Federal Communications Commision
FHSS	Frequency Hopping Spread Sprectrum
GTK	Group Temporal Key
HTTP	Hyper Text Transfer Protocol
ICV:	Integrity Check Valuer
IEEE	Institute of Electrical and Eletronics Engineers
IP	Internet Protocol
ISM	Industrial Scientific and Medical.
ISO	International Standards Organization
IV	Vetor de Inicialização
LDAP	Ligthweight Directory Access Protocol
LLC	Logical Link Control
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
OFDM	Othogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PCF	Point Coordination Function
PEAP	Protected Extensible Authentication Protocol
PSK	Pre Shared Key
PTK	Pairwise Transient Key
Radius	Remote Authentication Dial-in User Service
RTS	Request to Send
SSID	Service Set IDentifier
TTAK	Temporal and Transmitter Address Key
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

WPA2	Wi-Fi Protected Access2
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo será tradado o Tema, Delimitação da Pesquisa, Problemas e Premissas, o Objetivo Geral, os Objetivos Específicos, Justificativa, Procedimentos Metodológicos, Embasamento Teórico e a Estrutura deste trabalho.

1.1 TEMA

Durante muitos anos, o principal meio de transmissão utilizado para interconectar dispositivos por meio de uma rede de computadores era o cabo metálico. Com a evolução das tecnologias e a utilização de padrões como o IEEE 802.11, foi possível a interligação de dispositivos por meio de redes sem fio. Atualmente, o padrão 802.11 permite que os administradores de redes possam configurar uma ou mais redes sem fio dentro de uma organização (Tanembaum, 2003).

A vantagem destas redes em comparação com as redes que utilizam cabos metálicos é a mobilidade. Com uma rede cabeada, o usuário deve utilizar a estrutura já existente, e só poderá se conectar a rede onde existir uma tomada de conexão física que possibilitará o seu acesso a Rede de Computadores. Quando houver a necessidade de mudança física do local de trabalho do usuário, deverá ser feito uma nova tomada para que ele consiga acessar a rede. Com a utilização de uma rede sem fio, o usuário pode se mover dentro da organização sem que o mesmo perca o acesso a rede de computadores (Ozorio, 2010).

As WLANs (*Wireless Local Area Network),* como são chamadas as redes sem fio locais, permitem que os usuários utilizem uma estrutura de redes por meios dos chamados Pontos de Acesso (*Access Points*), que fazem a interligação entre os dispositivos que utilizam a rede sem fio com a Rede de Computadores da organização (Silva, 2010).

É possível interligar estas Redes sem Fio para que os usuários possam ter acesso com a *Internet* ou outros sistemas remotos. Essa tecnologia vem crescendo

a cada dia, e é muito utilizado por empresas, aeroportos e em ambiente doméstico (Silva, 2010).

Essa mobilidade oferecida pelas redes sem fio junto com a facilidade de instalação que a mesma vem proporcionando (em alguns equipamentos só é necessário ligar o mesmo que a rede sem fio já estará funcional), são os principais fatores para esse grande avanço da tecnologia (Alecrim, 2008). Essa preocupação em ter a rede sem fio funcionando acaba fazendo algumas pessoas esquecerem um detalhe muito importante nas redes sem fio: a segurança.

A cada dia que passa o ataque as redes sem fio vêm aumentando. Sem a necessidade uma conexão física (cabo), o invasor só precisa conseguir o acesso ao meio para capturar as informações que deseja. Nas redes sem fio os dados da rede se propagam pelo ar, e assim podem ser interceptados por qualquer pessoa que esteja ao alcance do sinal sem fio e conectado a rede (Ozorio, 2007).

Por isso as redes sem fio vêm se tornando alvo constante de ataques, podendo comprometer dados pessoais e empresariais. Com isso é necessário que seja lembrado três aspectos básicos de segurança: Confidencialidade, Integridade e Disponibilidade (Ozorio, 2007).

- ✓ Confidencialidade: é garantir que somente as pessoas conectadas na rede poderão acessar a mesma. Verificando sua identidade através da sua identidade do cliente e a autenticidade da máquina (Campos, 2008).
- ✓ Integridade: garantir que os dados transmitidos não sejam modificados durante a transmissão (Campos, 2008).
- ✓ Disponibilidade: garantir não apenas o funcionamento da rede sem fio, mais de todos os equipamentos que envolvem a rede, como por exemplo, um servidor de *e-mail*. O invasor pode invadir a rede visando deixar este servidor fora de operação. Assim com a garantia que a rede sem fio esta protegida você acaba protegendo o resto da sua rede (Campos, 2008).

Este trabalho aborda algumas formas de se implementar segurança em uma rede sem fio, dificultando o acesso de um invasor e garantindo a confidencialidade, integridade e disponibilidade dos dados de uma rede corporativa ou doméstica. Os seguintes aspectos serão considerados: redes de computadores, redes sem fio, o padrão 802.11 e suas variantes (a, b, g e n), e os protocolos de segurança utilizado nas redes sem fio. Será realizada uma pesquisa de campo buscando as vulnerabilidades e as configurações mais comuns dos equipamentos.

1.1.1 Delimitação de Pesquisa

Para um bom entendimento dessa pesquisa, será mostrado primeiramente o que é uma Rede de Computadores, como ela funciona e suas principais características. Em seguida serão abordados os conceitos de redes sem fio, seu surgimento, suas aplicações e os seus padrões de funcionamento.

Referente às tecnologias de segurança, o foco do estudo será os protocolos de segurança Wi-Fi, não sendo tratadas outras tecnologias como *firewall* e antivírus.

Esta pesquisa será feita em uma organização de grande porte, onde tem atualmente vários Pontos de Acessos de Redes sem Fio.

1.2 PROBLEMA E PREMISSAS

Atualmente as Redes sem Fio estão se tornando itens importantes, tanto no ambiente empresarial quanto nas casas das pessoas. O baixo custo dos equipamentos e a sua facilidade de instalação aliada à mobilidade que essa tecnologia possui são os principais fatores para tal importância.

Como as Redes sem Fio estão sendo utilizadas por muitos usuários, um fator importante que deve ser considerado é a segurança. Muitos usuários não têm conhecimento para saber que um Ponto de Acesso configurado de forma errada pode deixar uma porta aberta para que outros usuários acessem a sua rede interna, possibilitando a utilização da sua largura de banda no acesso à *Internet*, ou até mesmo acessar os arquivos da sua rede local.

Quando o assunto é Redes de Computadores, segurança é um termo muito complexo, mais muito importante devido à tecnologia fazer parte da vida de todos nós hoje em dia. Para planejar uma rede segura, primeiramente precisa-se definir e perceber a importância dos dados em uma rede (COMER, 2007).

Após essa noção é possível começar a definir uma política de segurança para uma rede, podendo se utilizar de diversas ferramentas como antivírus, *firewall*, e outras ferramentas disponíveis.

Em Redes sem Fio, a segurança é tratada um pouco diferente, pois a preocupação principal é permitir o uso da rede sem fio e dos serviços da rede em geral a computadores que façam parte da rede local. O sinal de uma rede sem fio está disponível a todas as pessoas que estejam ao alcance do sinal, por isso é necessários ter o seu equipamento configurado corretamente.

Apoiado nessa preocupação, o foco principal dessa pesquisa visa ajudar a solucionar o seguinte problema:

Como estipular métodos de segurança em redes sem fio?

Visando resolver o problema, a ideia dessa pesquisa é mostrar os diferentes tipos de protocolos de segurança que podem ser utilizados, aliado a técnicas que podem dificultar o acesso de um invasor a sua rede sem fio, e conseqüentemente as informações disponíveis dentro da rede.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Analisar os protocolos de segurança utilizados nas Redes sem Fio, verificando as suas características e diferenciando os melhores protocolos a serem utilizados;

1.3.2 Objetivos Específicos

- Definir o padrão IEEE 802.11 e suas variantes (a, b, g, n), bem como analisar o controle de acesso ao meio e o formato do quadro;
- Analisar as faixas de espectro utilizadas nas Redes sem Fio que utilizam o padrão 802.11;
- Discriminar segurança além da tecnologia;

- Fazer uma pesquisa de campo utilizando uma antena de maior potência para estudar a forma que os usuários estão configurando os Pontos de Acesso das Redes sem Fio, em uma organização de grande porte;
- Analisar a segurança que está sendo utilizada nesta organização de grande porte, permitindo verificar os possíveis pontos de falhas na segurança.

1.4 JUSTIFICATIVA

Com o barateamento dos equipamentos de Redes sem Fio, e a utilização de um padrão aberto, que é o IEEE 802.11, as Redes sem Fio estão cada vez mais sendo utilizadas, tanto por usuários domésticos quanto nos ambientes empresariais. Na maioria das vezes por desconhecimento das falhas de segurança dos protocolos utilizados nos Pontos de Acessos das Redes sem Fio, os usuários estão implementando suas redes com pouca ou nenhuma segurança. Sem saber que estão vulneráveis, estes usuários utilizam por anos suas redes, até que um problema maior possa acontecer. Para evitar estes problemas, este trabalho tem o foco na segurança das Redes sem Fio: qual o protocolo de segurança mais apropriado, quais as configurações que não devem ser feitas, como deixar mais segura às redes utilizadas pelos usuários. Para isso, será feito uma pesquisa de campo em uma organização de grande porte indicando as falhas de configurações reais, que estão sendo utilizadas. Com isto, poderá se verificar os métodos de segurança utilizado nesses pontos de acesso. A escolha do protocolo de segurança utilizado será mostrado e comparado a fragilidade ou segurança de cada um.

As informações obtidas poderão ser utilizadas para melhorar a segurança nos pontos de acesso desta organização e em outros pontos de acesso, seja de um usuário doméstico ou de uma empresa.

> Desenvolver uma política de segurança de rede pode ser complexo porque uma política nacional exige que a organização relacione a segurança de rede e computadores ao comportamento humano e avalie o valor das informações (COMER, 2007, p.548).

1.5 PROCEDIMENTOS METODOLÓGICOS

Verificando os critérios de pesquisa proposto por Gil (2010), a pesquisa é de natureza aplicada. Já quanto aos seus objetivos gerais e propostos é uma pesquisa explicativa. E por fim será uma pesquisa de campo para análise dos pontos de acesso sem fio de uma organização. Nesta análise serão coletados alguns dados como nome do ponto de acesso, protocolo de segurança utilizado, canal utilizado e a freqüência que se encontra a rede. Para realizar essa avaliação serão utilizados os *softwares* Kismet e Gerix.

Para analisar a segurança dos pontos de acesso, será utilizado o Backtrack 5, que é uma distribuição Linux Debian voltado para segurança. Esta ferramenta permite a análise de vários aspectos na segurança de Redes sem Fio.

1.6 EMBASAMENTO TEÓRICO

Com a intenção de mostrar os conceitos sobre Redes de Computadores destacam-se os trabalho bibliográficos de Santos (2008), Comer (2007) e Tanembaum (2003). Para a explicação teórica sobre redes sem fio 802.11, topologias de redes sem fio, seus padrões e faixas de frequência, além de Comer (2007) e Tanembaum (2003) será utilizada a contribuição bibliográfica de Forouzan (2004), Rappaport (2009), Rufino (2005), Pereira (2009) e Saade et al (2008).

Referente à segurança e protocolos de autenticação a pesquisa foi baseada no material de Ozorio (2007), Rufino (2005), Sartorato et al (2008) e Peixoto (2010).

Referente ao tema segurança além da tecnologia será utilizado o material de Campos (2008) e material da ISSO 27000.

E para finalizar o embasamento teórico atendendo ao objetivo específico de analisar os pontos de acesso de uma organização de grande porte, além das bibliografias citadas acima, haverá como já dito no item 1.5 (Procedimentos Metodológicos) uma pesquisa de campo, que pretende mostrar por meio dos resultados obtidos a importância da segurança em uma rede sem fio, protegendo conseqüentemente o resto da rede e seus computadores.

1.7 ESTRUTURA

O trabalho esta organizado em seis capítulos.

O capítulo 1 deste trabalho apresenta a Introdução, falando do tema, delimitação da pesquisa, problemas e premissas, objetivos, justificativa, procedimentos metodológicos, embasamento teórico e a estrutura descrita aqui.

O capítulo 2 concentra na fundamentação teórica da pesquisa.

No capítulo 2.1 apresenta uma breve introdução às redes de computadores, modelo OSI, TCP/IP e sua importância nos dias de hoje.

O capítulo 2.2 mostra a fundamentação teórica das redes sem fio, falando sobre 802.11 e suas variantes, freqüência e canais que as redes sem fio utilizam.

O capítulo 2.3 irá tratar exclusivamente sobre Segurança em redes sem fio, falando dos protocolos de autenticação WEP, WPA, WPA2, mostrando a evolução destes protocolos.

O capítulo 3 é a parte da pesquisa de campo que foi realizada, serão mostrados os resultados da análise feita nos pontos de acesso de uma organização de grande porte..

O capitulo 4 contém a conclusão do trabalho e sugestões de trabalhos futuros.

2 REFERENCIAIS TEÓRICOS

Neste capítulo será descrito o Referencial Teórico do trabalho, que contém os seguintes assuntos: Redes de Computadores, o Modelo de Referência OSI, o modelo de Referência TCP/IP, o Padrão IEEE 802.11, Topologias do IEEE 802.11, o IEEE 802.11 e suas variantes (a, b, g, n), o Formato do Quadro, Faixas de Espectro e os Protocolos de autenticação do IEEE 802.11 (WEP, WPA e WPA2).

2.1 REDES DE COMPUTADORES

Segundo Tanembaum (2003), pode-se conceituar o termo rede de computadores, como um conjunto de computadores e outros dispositivos utilizando uma tecnologia que permite a troca de informações compartilhando o mesmo meio físico e lógico As Redes de Computadores podem ser utilizadas para diversos serviços, tanto para empresas quanto para indivíduos. Nas empresas as redes são utilizadas para compartilhar arquivos, impressoras e informações coorporativas, e para as pessoas servem como fonte de informação, pesquisa e diversão (Tanembaum, 2003).

No inicio das redes de computadores cada fabricante possuía sua própria forma de trabalho e sua linha de desenvolvimento tecnológico. Desse modo uma placa do fabricante Y só pode ser conectada por meio físico (fio) a outra placa do mesmo fabricante. Se uma das placas apresentasse problemas e não sendo possível a substituição por outra placa do mesmo fabricante, seria necessário trocar as duas placas, isso causava transtornos e gastos elevados (Tanembaum, 2003).

2.1.1 O Modelo de Referência OSI

Visando resolver este problema de interoperabilidade, a interconectividade, a portabilidade e a escalabilidade entre tecnologias e produtos de diferentes fabricantes, foi criado pela ISO (*International Standards Organization*) no ano de 1970 o modelo de referência OSI (*Open Systems Interconnection*), que seria utilizado como padrão para troca de informações entre e dentro das redes (Tanembaum, 2003). Esse modelo possui sete camadas (figura 1), as camadas em ordem crescente são: física, enlace de dados, transporte, rede, sessão, apresentação e aplicação. Segue uma breve descrição das sete camadas.

Figura 1 - Modelo de Referência OSI
Fonte: Rodrigues, 2009

Camada Física: A camada física cuida das características físicas, elétricas, funcionais e procedimentos para ativar, manter e desativar conexões entre duas partes. Ela está ligada diretamente à transmissão de bits primários (bit 0 e bit 1) por um canal de comunicação (Santos, 2008).

Camada de Enlace: Providencia maneiras funcionais e procedimentos para estabelecimento, manutenção e liberação de enlace de dados entre as entidades da rede. Os objetivos são providenciar a transmissão de dados para a camada de rede e detectar, e possivelmente corrigir, erros que possam ocorrer no meio físico (Santos, 2008).

Camada de Rede: A principal função da camada de rede é controlar a operação de rede. Ela estabelece uma conexão lógica entre dois pontos, cuidando do tráfego e roteamentos dos dados da rede (Tanembaum, 2003).

Camada de Transporte: A principal função da camada de transporte é receber dados da camada de sessão, dividi-los em pacotes menores caso haja necessidade, transmitir os mesmos para a camada de rede e garantir que todos os pacotes sejam entregues (Santos, 2008).

Camada de Sessão: A camada de sessão gerencia as atividades das camadas inferiores. Permite que usuários de diferentes máquinas estabeleçam comunicação entre si. A camada sessão cuida de vários serviços, como por exemplo, qual maquina deve transmitir em cada momento, controle de troca de dados e sincronização entre as duas máquinas (Santos, 2008).

Camada de Apresentação: A camada de apresentação é responsável pela conversão dos dados para uma forma que eles sejam entendidos por todos os sistemas envolvidos na comunicação, resolvendo assim problemas de sintaxe entre os sistemas. Também realiza compressão, descompressão, criptografia e descriptografia (Tanembaum, 2003).

Camada de Aplicação: Na camada de aplicação se encontrada os serviços utilizados pelos usuários, como transferência de arquivos, e-mail, gerenciamento de redes e outras facilidades. Um protocolo amplamente utilizado na camada de aplicação é o HTTP (*HyperText Transfer Protocol*) que constitui a base para o WWW (*Word Wide Web)*. Quando acessamos uma pagina na Web, o nome desta pagina é enviada ao servidor utilizando o protocolo HTTP. Depois o servidor transmite a página novamente (Santos, 2008).

2.1.2 O Modelo de Referência TCP/IP

O modelo TCP/IP surgiu para atender as necessidades de conexão da ARPANET, que era uma rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos, e pouco a pouco universidades e repartições publicas foram sendo conectadas a esta rede através de linha telefônica dedicada. Após a

criação das redes de rádio e satélite começaram a surgir problemas com a arquitetura existente, por isso foi necessário a criação de um novo modelo de referência, esse modelo tinha como principal objetivo conectar várias redes de maneira uniforme (Tanembaum, 2003).

O Modelo TCP/IP foi projetado sem que se conhecessem as camadas do modelo OSI, e não foi criado para se tornar um modelo de referência padrão, mas sim para atender as necessidades do Departamento de Defesa dos Estados Unidos, que queria que suas conexões permanecessem intactas enquanto as máquinas de origem e destino estivessem funcionando, mesmo que algumas máquinas ou linhas intermediárias estivessem inoperantes por um tempo (Tanembaum, 2003)

O TCP/IP é composto por quatro camadas (figura 2), a camada de Host, a camada de Inter-Rede, a camada de Transporte e a camada de Aplicação. Segue abaixo a descrição das funcionalidades principais das quatro camadas.

Figura 2 - Modelo de Referência TCP/IP
Fonte: Rodrigues, 2009

Camada de Acesso à Rede: O Modelo de Referência TCP/IP não especifica muito bem o que ocorre nesta camada, apenas fala que o host deve se conectar a rede utilizando algum protocolo que seja possível enviar pacotes IP (*Internet Protocol*), este protocolo não é definido e varia de *host* para *host* e de rede para rede (Tanembaum, 2003)

Camada de *Internet* (Inter-Rede): A função da camada de *Internet* ou inter-rede é garantir que um *host* consiga enviar pacotes em qualquer rede e garantir que

esses pacotes trafegarão independentemente até o destino, esse destino pode ser uma rede diferente. Estes pacotes podem chegar fora de ordem, daí cabe as camadas superiores reorganizá-los caso a entrega necessite ser em ordem. A camada de inter-redes define um formato de pacote padrão e um protocolo denominado IP, entregando esses pacotes aonde for necessário, dando atenção para parte de roteamento, visando evitar congestionamento. A camada inter-redes do TCP/IP é muito semelhante à camada de rede do modelo OSI (Tanembaum, 2003).

Camada de Transporte: A camada de transporte do modelo TCP/IP tem a mesma função que a camada de transporte do modelo OSI, garantir a entrega dos pacotes enviados, garantindo que os *hosts* de origem e destino mantenham uma conversação. Dois protocolos fim a fim foram definidos nesta camada. O primeiro deles é o TCP (Transmission Control Protocol – Protocolo de Controle de Transmissão), é um protocolo orientado a conexão que permite a entrega sem erros de um pacote enviado pela origem até o destino. O TCP fragmenta os pacotes em mensagens secretas e encaminha cada mensagem para a camada de inter-redes. Chegando ao destino o TCP monta essas mensagens e envia uma confirmação de entrega para a origem (Comer, 2007).

O Segundo protocolo é o UDP (User Datagram Protocol) é um padrão TCP/IP, este protocolo é utilizado para transporte rápido entre host TCP/IP. Porém o UDP não garante entrega e nem verificação de dados, ele simplesmente encaminha o pacote para o destino, e o destinatário nunca saberá se o pacote chegou corretamente. Esse serviço do UDP é chamado de sem conexão. (Comer, 2007)

Camada de Aplicação: O modelo TCP/IP não possui as camadas de apresentação e de sessão, pois não houve necessidade destas camadas. Assim acima da camada de transporte encontramos a camada de aplicação, responsável pela execução dos serviços utilizados pelos usuários como transferência de arquivos, e-mail e terminal virtual, também conhecido como telnet (Tanenbaum, 2003)

2.2 O PADRÃO IEEE 802.11

Os avanços nas telecomunicações nos últimos anos vêem possibilitando o surgimento de várias tecnologias que estão facilitando a vida do ser humano seja ela no trabalho ou em sua casa. Uma dessas tecnologias que está facilitando as pessoas é a rede sem fio, que deixou de ser usada apenas em comunicações de longa distância e passou a ser utilizada em redes locais (Comer, 2007)

Acreditando nas redes sem fio um órgão denominado IEEE (*Institute of Electrical and Eletronics Engineers)* criou um grupo com a intenção de padronizar as redes sem fio. E esse padrão foi nomeado como Padrão IEEE 802.11. Esse padrão foi ratificado pela IEEE no ano de 1997, apesar do projeto de padronização ter iniciado no de ano de 1990, ele só ratificado sete anos depois devido à baixa taxa de transferência de dados inicialmente oferecida pelas redes sem fio, na faixa de kbit/s. Assim que a taxa de transferência começou a chegar à faixa de megabit/s, as redes sem fio começaram a ser vista como uma tecnologia promissora e passaram a receber investimento para criação de equipamentos que possibilitassem a comunicação sem fio entre computadores (Tanembaum, 2003).

O IEEE 802.11 foca nas duas primeiras camadas do modelo OSI (figura 3), camada física e a camada de enlace de dados.

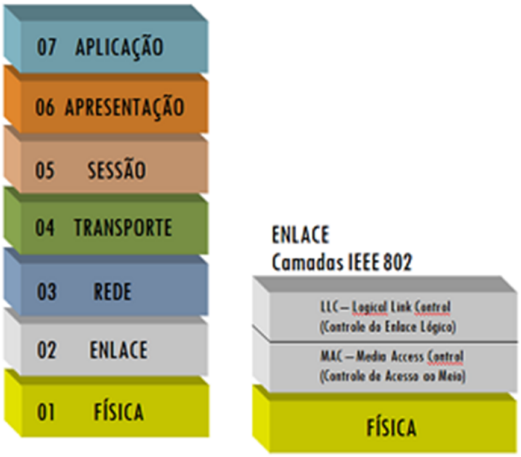

Figura 3 - Relação das camadas OSI e camadas do padrão IEEE 802.11

Fonte: Barbosa, 2010

A camada física é responsável pela transmissão do quadro por um canal de comunicação. O IEEE 802.11 definiu quatro técnicas de transmissão para as redes sem fio, com a finalidade de melhor adequar um sinal antes de transmiti-lo ao meio (Rufino, 2005). Essas técnicas são:

Infravermelho: Esta técnica utiliza raios de transmissão próximos à luz visível. Como o raio infravermelho não ultrapassa paredes, ela é utilizada apenas em ambientes fechados, operando em 1 Mbps ou 2 Mbps (Forouzan, 2004)

As comunicações infravermelhas podem ser realizadas de duas maneiras, por reflexão (difusão) ou linha direta. Na primeira, a comunicação é realizada através de um ponto de reflexão, não podendo haver nenhum obstáculo entre o pronto de reflexão e as estações sem fio. Na comunicação direta os raios infravermelhos são diretamente transmitidos do emissor para o receptor, sem a necessidade de um intermediário, um exemplo dessa comunicação é a transferência de arquivos entre computadores portáteis (Forouzan, 2004).

FHSS: O FHSS (*Frequency Hopping Spread Spectrum*) é uma técnica que utiliza como meio de transmissão o rádio de alcance limitado, operando na banda ISM (*Industrial Scientific and Medical*) de 2.4 GHz. A banda de frequência é dividida em 79 canais com frequência de 1 MHz de largura cada, gerando um sequência pseudo-randômica. O FHSS é insensível a interferências de rádio e tem como ponto negativo a baixa largura de banda (Rufino, 2005).

DSSS: O DSSS (*Direct Sequence Spread Spectrum*) também ultiza radiofrequência como meio de transmissão e opera na banda de 2.4 GHz. Segundo o padrão 802.11, o DSSS usa uma sequência de 11 bits para difundir os dados antes de iniciar a transmissão. Cada bit transmitido é modulado por esta sequência. Este processo espalha a energia de radio–frequência em torno de uma banda de faixa larga que pode ser necessária para transmitir o dado. O receptor concentra o sinal de radio–frequência recebido para recuperar o dado original (Rufino, 2005).

OFDM: O OFDM **(***Othogonal Frequency Division Multiplexing*) é um modo de transmissão mais eficiente, utilizado não somente em redes sem fio, mais também em redes cabeadas, como ADSL (*Asymmetric Digital Subscriber Line*), cujas características de modulação de sinal e isolamento de interferências podem ser bem aproveitadas. As maiorias dos padrões atuais de redes sem fio utilizam esse modo

de transmissão, devido a capacidade que o OFDM tem de identificar ruídos e interferências (Rufino, 2005).

Na segunda camada utilizada pelo IEEE 802.11, a camada de enlace de dados é divida em duas subcamadas, a subcamada MAC (*Media Access Control*) e a subcamada LLC (*Logical Link Control*).

Subcamada MAC: No IEEE 802.11 a subcamada MAC tem como principal função determinar como o canal é alocado, isto é, determinar quem será o próximo a transmitir devendo ser compatível como a *Ethernet*. A rede *Ethernet* utiliza o CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*), para realizar esta função. No IEEE 802.11 não é possível utilizar o CSMA/CD, pois a maioria dos rádios é halduplex, isso significa que eles não podem transmitir e ouvir ao mesmo tempo em uma única frequência. Assim o IEEE 802.11 não utiliza o CSMA/CD, e sim o CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) uma variante do CSMA/CD. Na resolução desses problemas, a subcamada MAC emprega dois modos de acesso ao meio: um chamado DCF (*Distributed Coordination Function* – função de coordenação distribuída) e o outro chamado PCF (*Point Coordination Function* – função de coordenação de ponto) (Forouzan, 2004)

O modo de operação DCF utiliza o CSMA/CA, fazendo a detecção de canal físico e canal virtual. Na detecção de canal físico quando uma estação quer transmitir, primeiramente ela escuta o canal e se estiver livre a transmissão é feita. Na detecção de canal virtual, primeiramente o transmissor envia um pequeno pacote denominado RTS (Request to send), esse endereço contém os endereços de origem e destino, além do tempo estimado para a transmissão. Se o canal estiver livre o receptor responde com outro pacote denominado CTS (Clear to send) (Forouzan, 2004).

No modo PCF existe um ponto de acesso para controle de quem pode transmitir, por existir esse ponto de acesso, nesse modo não ocorre colisão. O funcionamento básico do PCF esta na difusão periódica pelo ponto de acesso de um quadro de baliza que contém parâmetros do sistema, como sequências de saltos, tempos de parada e sincronização do *clock* (Forouzan, 2004)

Subcamada LLC: A função da subcamada LLC é ocultar diferenças entre as variações do 802 e torna-la indistinguível na camada de rede. Esta subcamada fornece três opções de serviço: serviço de datagrama não confiável, serviço de

datagrama com confirmação e serviço confiável orientado a conexões (Forouzan, 2004).

2.2.1 Topologias IEEE 802.11

O padrão IEEE 802.11 especifica duas topologias para as redes sem, a primeira denominada AD-HOC e a segunda infraestruturada.

2.2.1.1 Topologia AD-HOC

Na topologia AD-HOC, também conhecida como ponto a ponto nenhum Ponto de Acesso é utilizado, a comunicação é feita entre os clientes (figura 4). Deve ser utilizada raramente e em situações temporárias, como por exemplo, em uma reunião onde se precisa realizar troca de arquivos (Pereira, 2009).

Figura 4 - Topologia de rede AD-HOC
Fonte: Kotviski, 2009

2.2.1.2 Topologia Infraestruturada

A topologia infraestruturada é a mais utilizada atualmente. Nesta topologia existe obrigatoriamente um Ponto de Acesso que é responsável por gerenciar a conexão, deste modo não há conexão direta entre os clientes, pois tudo passa pelo Access Point (figura 5). (Pereira, 2009).

Figura 5 - Topologia de rede Infraestruturada
Fonte: Alecrim, 2008

2.2.2 Variantes do IEEE 802.11.

O padrão IEEE 802.11 possui várias variantes (a, b, g, n), cada uma com diferentes especificações para dispositivos de redes sem fio, incluindo frequência de operação, compatibilidade de equipamentos com os outros padrões, taxas de transmissão, etc. No presente trabalho, variante será denominada como padrão, pelo fato deste último ser usado por vários autores.

802.11b: No ano de 1999, o padrão IEEE 802.11 recebeu uma atualização, denominada de 802.11b. A principal novidade dessa atualização era a possibilidade de realizar transmissões nas seguintes velocidades: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps. O intervalo de frequência utilizado pelo 802.11b é o mesmo do 802.11 original (entre 2,4 GHz e 2,4835 GHz). Uma limitação do 802.11b é referente ao método de transmissão que fica restrito ao DSSS, pois o FHSS não atende as normas estabelecidas pela FCC (*Federal Communications Commission*), já que o 802.11b realiza transmissões com velocidades acima de 2Mb (Rufino, 2005).

Sua área de cobertura pode chegar a 400 metros em lugares abertos e 50 metros em lugares fechados, como escritórios e bares por exemplo. Vale lembrar que a cobertura de transmissão pode sofrer influência de vários fatores, como interferência de outros objetos que trabalham na mesma frequência e que podem impedir a propagação do sinal (Rappaport, 2009)

O padrão 802.11b foi o primeiro a ser adota em grande escala, sendo um dos grandes responsáveis pelo enorme crescimento das redes sem fio.

802.11a: O padrão 802.11a foi disponibilizado no final do ano de 1999, um pouco depois da primeira atualização, o 802.11b. A sua principal característica é pode trabalhar com as seguintes taxas de transmissão de dados: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps. Possui um alcance geográfico de transmissão de 50 metros, e tem como grande diferença dos outros padrões a sua taxa de frequência que é de 5 Ghz.

A grande vantagem de se trabalhar com essa taxa de frequência é a baixa interferência existente, pois essa taxa é pouco usada atualmente. Mais há também o lado negativo, pois a frequência de 5 Ghz não é regulamentada por alguns países, e ainda pode causar dificuldades de comunicação que utilizam o padrão 802.11 original e o padrão 802.11b (Saade et al, 2008).

Uma aspecto importante do 802.11a é que ele não utiliza o DSSS ou o FHSS, para realizar a transmissão ele utiliza uma técnica conhecida como OFDM. Nesse método de transmissão a informação é dividida em vários pequenos conjuntos de dados que são transmitidos em diferentes frequências. Apesar das vantagens citada o padrão 802.11a não chegou a ser tão popular como o 802.11b (Rufino, 2005).

802.11g: O padrão 802.11g, foi disponibilizado no ano de 2003, é considerado um sucessor do padrão 802.11b, por ser totalmente compatível com o mesmo. Assim um roteador, por exemplo, que opera no padrão 802.11g pode se comunicar com o outro que opera no padrão 802.11b, ficando a taxa de transmissão de dados limitada pelo que é suportada no padrão 802.11b (Saade et al, 2008).

A principal vantagem do padrão 802.11g é taxa de transmissão de dados que pode chegar até 54 Mbps assim como o padrão 802.11a. Mais diferentemente do 802.11a o padrão 802.11g opera com frequências na taxa de 2,4 Ghz e possui um alcance geográfico de 400 metros em lugares aberto e 50 metros em ambientes fechado, igual o 802.11b. A técnica de transmissão utilizada por este padrão é a

OFDM, mais quando há comunicação com dispositivos 802.11b é utilizada a técnica de transmissão DSSS (Rappaport, 2009).

802.11n: O padrão 802.11n é o sucessor do 802.11g, foi aprovado no ano de 2004 pela IEEE com a intenção de aumentar as taxas de transferências. A principal característica desse padrão é a utilização do MIMO (*Multiple-Input Multiple-Output),* com o MIMO é capaz de se aumentar a velocidade da taxa de transferência através da combinação de várias vias de transmissão. Com isso, por exemplo, é possível usar três ou mais emissores e receptores em uma rede. Um exemplo dessa estrutura é: um Ponto de Acesso com três antenas (três vias de transmissão) e uma placa de rede sem fio, por exemplo, com a mesma quantidade de receptores (Rufino, 2005).

Com essa característica o 802.11n é capaz de transmitir dados em uma taxa de 300 Mbps, e na teoria pode chegar até 600 Mbps. Outra característica do 802.11n é trabalhar nas frequências 2.4 Ghz e 5 Ghz tornando esse padrão compatível com seus antecessores. Sua técnica de transmissão padrão é a OFDM, mais com o uso do MIMO é chamado também de MIMO-OFDM, e sua área de cobertura pode chegar a 400 metros (Rufino, 2005).

2.2.3 Formato do Quadro no IEEE 802.11

O padrão IEEE 802.11 tem definido três classes de quadros, que são dados, controle e gerenciamento. Cada um desses quadros possui um cabeçalho com alguns campos usados na subcamada MAC e outros pela camada física que trata mais sobre modulação que não será tratado neste trabalho (Tanembaum, 2003).

O formato do quadro é mostrado na figura 6, esse quadro possui nove campos separados da seguinte forma (Tanembaum, 2003)

Controle de Quadro: Este campo é dividido em onze subcampos, que são os seguintes.

- **Versão de protocolo** (permite a operação de duas versões de protocolo).
- **Tipo** (dados, controle e gerenciamento).

- **Subtipo** (RTS ou CTS, por exemplo).
- Os bits **Para DS** e **De DS** indicam se o quadro esta indo ou vindo do sistema de distribuição entre células (por exemplo, Ethernet).
- O bit **MF** significa que haverá mais fragmentos.
- O bit **Repeti**r indica uma retransmissão de um quadro enviado anteriormente.
- O bit **Gerenciamento de energia** e usado pela estação base para deixar o receptor em estado de espera ou retira-lo do estado de espera.
- O bit **Mais** indica que o transmissor tem quadros adicionais para o receptor.
- O bit **W** especifica que o corpo de quadro foi criptografado com o algoritmo WEP (*Wired Equivalent Privacy* - Privacidade Equivalente quando fisicamente conectado).
- Por último, o bit **O** informa ao receptor que uma sequência de quadros com esse bit tem de ser processada em ordem.

Duração: É o segundo campo do quadro de dados, esse campo informa por quanto tempo o quadro de sua confirmação ocupará o canal.

Quatro campos de endereço: Contém os endereços de origem e destino do quadro, e os endereços de origem e destino do ponto de acesso.

Sequência: Este campo permite que os fragmentos sejam numerados. Há 16 bits disponíveis para isso, 12 bits identificam o quadro e os 4 restantes identificam os fragmentos.

Dados: Contém a carga útil de 2312 bytes.

Total de verificação: Campo que vem em seguida do campo de dados.

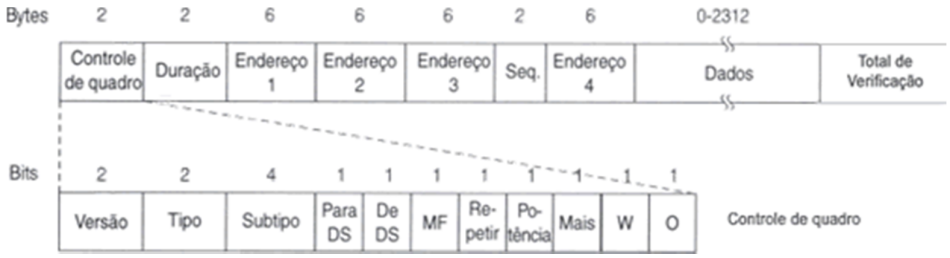

Figura 6 - Quadro de dados do IEEE 802.11

Fonte: Tanembaum, (2003)

Os quadros de gerenciamento têm um funcionamento similar ao quadro de dados, a diferença nesse quadro é no campo de endereço, que tem um endereço a menos no ponto de acesso, pois os quadros de gerenciamento estão restritos a uma única célula (Tanembaum, 2003)

Os quadros de controle são menores ainda, possuindo apenas um ou dois endereços, e não possui nenhum campo de dados e nenhum campo de sequência. A principal informação deste quadro esta no campo subtipo, em geral um RTS, CTS ou ACK (Tanembaum, 2003).

2.2.4 Faixas de Espectro do Padrão IEEE 802.11.

Os padrões IEEE 802.11 utilizam duas faixas de espectro de uso não licenciado, ou de uso ISM (*Industrial, Scientific and Medical*), como o nome já diz, são faixas reservadas para uso industrial, científico e médico. A primeira é denominada S-ISM, e inclui frequências em torno de 2,4 Ghz, utilizadas tanto pelos dispositivos do padrão IEEE 802.11b quanto pelos dispositivos do padrão IEEE 802.11g. A segunda inclui freqüências em torno de 5,7 GHz, utilizadas pelo padrão IEEE 802.11a e pelo padrão IEEE 802.11n. Os valores de freqüências de cada faixa, respectivamente, variam ligeiramente de país para país nos dois casos (Saade et al., 2008).

Um dos grandes problemas encontrados nos dispositivos dos padrões IEEE 802.11b e IEEE 802.11g é a interferência, pois existem vários equipamentos que também operam na faixa de freqüência de 2,4 GHz como, por exemplo, alguns fornos de microondas, aparelhos de telefone sem fio, Bluetooth (Rufino, 2005; Saade et al., 2008).

Para reduzir os problemas de interferências, os 83,5 MHz disponíveis na banda foram divididos em 14 canais (padrão europeu) de aproximadamente 5 MHz de largura cada. Porém, destes 14 canais, apenas nos canais 1, 6 e 11 não ocorre sobreposição, ou seja, nos canais 1, 6 e 11 podem ser realizadas transmissões

simultâneas sem a ocorrência de interferências, como sugere a figura 7 abaixo (Saade et al., 2008).

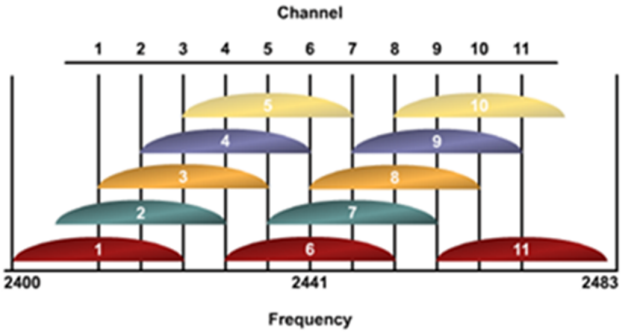

Figura 7 - Divisão de banda S-ISM em canais

Fonte: Peixoto, 2011.

Os dispositivos que utilizam a segunda faixa de freqüência não estão sujeitos a muita interferência devido ao baixo número de dispositivos que utilizam esta faixa. Esta faixa possui um alcance de sinal menor se comparando as outras frequências, o que pode se tornar um problema em ambientes amplos, ou uma vantagem quando não se deseja que o sinal atinja áreas maiores que o necessário para o funcionamento dos equipamentos de rede (Rufino, 2005).

2.3 PROTOCOLOS DE SEGURANÇA E AUTENTICAÇÃO.

A segurança é um dos principais fatores para utilização das redes sem fio nos dias de hoje. Nas redes sem fio os dados transmitidos ficam disponíveis para qualquer pessoa que estiver no alcance do sinal. Para permitir acesso apenas a pessoas autorizadas na rede e garantir a confidencialidade, disponibilidade e integridade dos dados disponíveis, se faz necessário à utilização de métodos criptográficos de segurança (Ozorio, 2007).

2.3.1 WEP (Wired Equivalent Privacy).

Com a finalidade de oferecer a criptografia dos dados e autenticação nas redes sem fio, o IEEE sugeriu no ano de 1999 o protocolo WEP que possui especificações para a camada de enlace de dados, e que hoje em dia já esta disponível em todos os produtos do padrão IEEE. O WEP é um protocolo que utiliza algoritmos simétricos, isso quer dizer que para cifrar e decifrar os dados uma chave é compartilhada entre as estações de trabalho e o concentrador (Rufino, 2005).

Referente ao seu funcionamento, a segurança do WEP é composta por uma chave estática que deve ser igual em todos os dispositivos da rede e um componente dinâmico, que juntos irão formar uma chave para cifrar o tráfego.

A distribuição desta chave deverá ser realizada manualmente em cada dispositivo (Rufino, 2005).

Esta chave configurada será fixa e pode ser alterada somente se a chave estática original for trocada. A tecnologia utilizada de cifração possui dois padrões: 40 e 104 bits, que combinados com uma sequência de 24 bits, denominada IV (Vetor de inicialização), se tornam 64 bits e 128 bits (Figura 8). O padrão de 64 bits é suportado por toda interface Wi-Fi (*Wireless Fidelity*), enquanto o padrão de 128 bits é o mais seguro, porém não é suportado em todos os dispositivos (Ozorio, 2007).

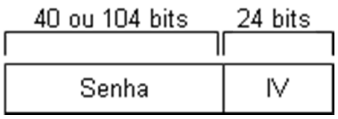

Figura 8 - Senha WEP + IV

Fonte: Sartorato et al, 2008

Para manter a confidencialidade, integridade e disponibilidade dos dados o WEP adiciona as chaves de 64 bits e 128 bits o ICV (*Integrity Check Value*) aos dados utilizando o CRC-32 (*Cyclic Redundancy Checks*) e depois realiza a criptografia utilizando o algoritmo RC4, desenvolvido por Ron Rivest. Desse modo é criada uma sequência de bits pseudoaleatória através de operações XOR (OU Exclusivo) (Figura 9). O IV é enviado sem criptografia, para o receptor realizar o

processo inverso. Ao ser enviado o ótimo byte o receptor aumenta uma unidade no IV para impedir uma repetição (Sartorato et al, 2008)

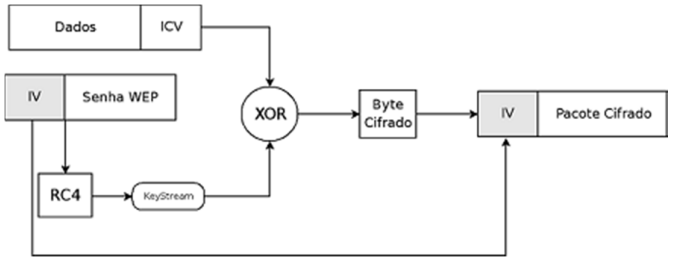

Figura 9 - Funcionamento WEP
Fonte: Sartorato et al, 2008.

O CRC-32 é um recurso do protocolo WEP, que tem como função realizar a detecção de erros. Ele realiza cálculos sobre os dados transmitidos e gera o relatório ICV e os envia junto com a mensagem para receptor. Ao receber esta mensagem o receptor realiza os mesmos cálculos e compara o CRC recebido com o cálculo CRC realizado ao receber a mensagem. Se os resultados forem iguais, o receptor identifica que a mensagem não foi modificada ou corrompida durante o trajeto (Ozorio, 2007).

Nas redes sem fio podem ser usados dois tipos de autenticação: Aberto (*Open System Authentication*), no modo aberto a autenticação é feita sem criptografia. E com uma chave pré-compartilhada, nesse método é utilizado criptografia. (Sartorato et al, 2008)

No acesso aberto (figura 10), os APs da rede mandam *broadcast* para os clientes Wi-Fi. O *broadcast* contém informações importantes da rede, como o canal e o SSID (*Service Set Identifier*). Nesse método o protocolo WEP está desabilitado e o envio de SSID ativo. (Sartorato et al, 2008)

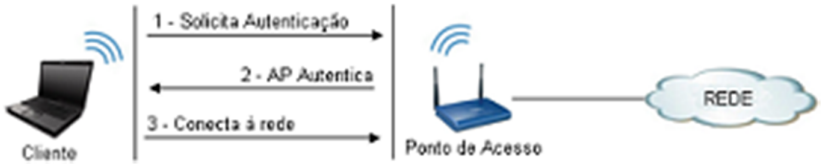

Figura 10 - Autenticação Aberta, sem criptografia
Fonte: Sartorato et al, 2008

No modo que utiliza criptografia (figura 11), o cliente sem fio necessita solicitar a autenticação e depois fornecer a chave pré-compartilhada que foi configurada no AP para poder obter acesso à rede. (Sartorato et al, 2008)

Figura 11 - Autenticação Criptografada
Fonte: Sartorato et al, 2008

O WEP é um protocolo que perdeu credibilidade nos últimos anos, muitos especialistas o consideram um protocolo muito vulnerável e aconselham aqueles que utilizam este protocolo a trocar a senha de autenticação do mesmo periodicamente visando diminuir os riscos (Ozorio, 2007).

O fato do WEP possui uma chave única e estática pode gerar grandes problemas em redes de maior porte, se for necessário trocar a chave no Access Point, também será necessário trocar a chave em cada estação de trabalho que utilize a rede sem fio, gerando assim um processo trabalhoso (Rufino, 2005).

Outra falha do WEP está na variação da chave. A chave utilizada é mesma para todos os dispositivos da rede, e através do IV que o algoritmo RC4 realiza a variação dessa chave. Como o IV possui 24 bits, esse valor é considerado pequeno e o numero de variações disponíveis é de 16.777.216 (Ozorio, 2007). Como o IV varia de pacote para pacote, o IV certamente começará a repetir os valores, devido à quantidade de tráfego que temos em uma rede nos dias de hoje, abrindo caminho

para o atacante capturar dados e descobrir a senha de autenticação a rede sem fio (Sartarato et al, 2008).

Outro problema questionado do WEP esta na maneira que sua chave é armazenada no cliente (figura 12). O protocolo não define nenhum método de criptografia na guarda da chave, esta é armazenada de forma legível, tornando assim um ambiente que utilize o protocolo WEP vulnerável (Rufino, 2005).

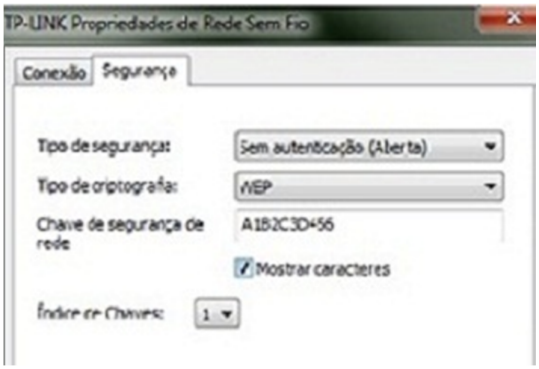

Figura 12 - Chave WEP salva no cliente

Fonte: O Autor.

2.3.2 WPA (Wi-Fi Protected Access)

Devido aos problemas de segurança divulgados do protocolo WEP, a Wi-Fi Aliance disponibilizou no ano de 2003 um novo protocolo denominando WPA. Várias modificações e avanços foram adicionados a este protocolo, principalmente na parte de autenticação e variação das chaves (Rufino, 2005).

O WPA utiliza na sua criptografia o algoritmo RC4, com uma chave de 128 bits, IV de 48 bits e a principal diferença esta com a inclusão do algoritmo (ou protocolo como descrevem alguns autores) denominado TKIP (*Temporal Key Integrity Protocol*), esse protocolo trabalha com o conceito de chave dinâmica, assim, essa chave é usada por um período, e depois de usada uma nova chave dinâmica é gerada, podendo assim cada pacote ser encriptado com uma chave diferente. No TKIP uma chave base de 128 bits denominada TK (*Temporal Key*) é utilizada e combinada com o endereço MAC do transmissor acaba gerando outra

chave chamada TTAK (*Temporal and Transmitter Address Key*), também conhecida como chave da “primeira fase”. Na “segunda fase” a chave TTAK é combinada com o IV do RC4 para gerar diferentes chaves para cada pacote. O TKIP faz cada estação possuir uma chave diferente da outra para se comunicar com o AP, pois as chaves são geradas com o endereço MAC de cada estação (Ozorio, 2007).

Para garantir a integridade dos dados é usado o CRC, assim que o pacote chega o destino o CRC faz cálculos necessários, se esses cálculos tiverem valores diferentes do CRC original o pacote é descartado.

No WPA a autenticação se tornou obrigatória, e possui dois métodos: a primeira denominada Pessoal, onde é usada uma chave compartilhada (WPA-*Pre Shared Key* ou WPA-PSK) entre o ponto de acesso e os clientes da rede sem fio. A segunda é denominada Corporativo, onde se utiliza um servidor de autenticação, por exemplo, um servidor RADIUS (*Remote Authentication Dial-In User Service*), LDAP (*Lightweight Directory Access Protocol*). Esse método utiliza um protocolo de comunicação 802.1x entre o Ponto de Acesso e o servidor de autenticação em conjunto com algum tipo de EAP (*Extensible Authentication Protocol*) (Rufino, 2005, Sartarato, 2008)

O EAP é um protocolo que permite várias técnicas de autenticação, é definido pela RFC 3478 e pode ser em redes sem fio e em redes 802.3. Os padrões EAP mais usados em redes sem fio são os seguintes: EAP-MD5, EAP-TLS (EAP-*Transport Layer Security*), EAP-TTLS (EAP-*Tunneled Transport Layer Security*) e PEAP (*Protected Extensible Authentication Protocol*). Os métodos de autenticação EAP podem ser: certificados digitais, biometria, usuário/senha e muitos outros. A figura 12 mostra um exemplo de autenticação EAP com protocolo WPA (Sartarato, 2008)

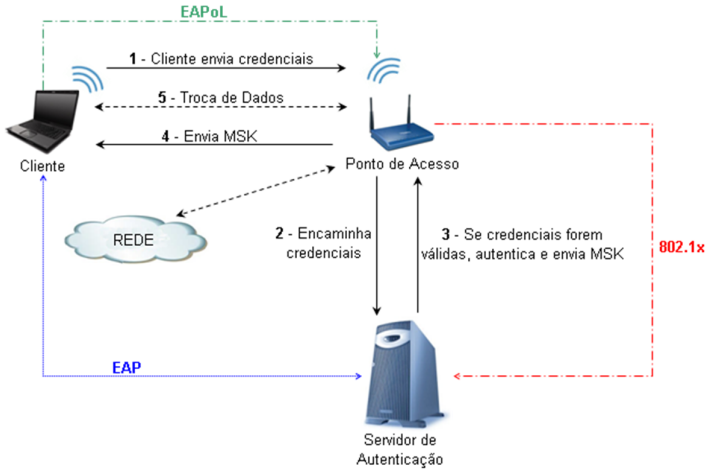

Figura 13 - Autenticação WPA, 802.1x EAP

Fonte: Sartorato, 2008

Para garantir a integridade dos dados o WPA utiliza um algoritmo denominado Michael juntamente com o ICV, que também é utilizado pelo WEP. O algoritmo Michael possui a facilidade de utilizar sua própria chave de integridade. São utilizados para garantir a integridade os endereços MAC de destino e origem e o Data Integrity Key produzindo assim o (MIC) *Message Integrity Check,* adicionando mais 8 bytes aos 4 bytes utilizados pelo CRC-32 totalizando assim 12 bytes para integridade (Figura 13) (Sartorato et al, 2008)

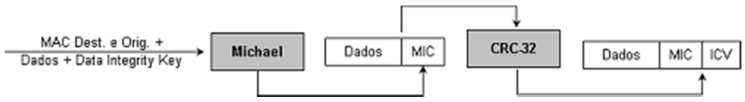

Figura 14 - Integridade WPA

Fonte: Sartorato, 2008

Mesmo com todos os avanços que o protocolo WPA possui, ele está sujeito a ataques. Como ocorre no protocolo WEP, o WPA poderá sofrer ataques de força bruta ou dicionário, nesse ataque o invasor tenta descobrir a senha com palavras comuns ou até mesmo em sequências alfanuméricas. Esse ataque ocorre geralmente em senhas que tenham menos de 20 caracteres e em equipamentos que

possuem configurações pré-estabelecidas pelos fabricantes, cuja senha tem de 8 a 10 caracteres e que não são reconfigurados (Rufino, 2005).

2.3.3 WPA2.

O protocolo WPA eliminou diversos problemas do seu antecessor, o WEP. Entretanto no ano 2004 a IEEE liberou o protocolo WPA2 ou 802.11i como alguns chamam, com a promessa de ser a solução definitiva de segurança para as redes sem fio (Sartorato et al, 2008).

A principal evolução no protocolo WPA2 esta na criptografia, enquanto o WPA utiliza o protocolo em conjunto com o algoritmo RC4, o WPA2 utiliza o TKIP com um algoritmo mais poderoso denominado AES (*Advanced Encyptation Standart).* O algoritmo AES oferece a possibilidade de se trabalhar com chaves de 128 bits, 192 bits e 256 bits. A chave de 256 bits é padrão no WPA2. Como possui uma criptografia forte, foi necessário à implementação de um novo hardware para se trabalhar com esta criptografia, por isso o WPA2 possui um co-processador para realizar os cálculos criptográficos do AES (Ozorio, 2007).

O AES é um cifrador em blocos que criptografa blocos de 16 bits, e repete várias vezes um conjunto definido de regras que trabalha com chave secreta e que opera com um número fixo de bits (Sartorato et al, 2008) O AES é reversível, o procedimento utilizado para criptografar os dados, é utilizado para decriptografá-los. O AES, assim como o WEP, trabalha com operações de XOR entre os blocos e a chave, organiza o bloco em uma matriz e realiza trocas circulares em cada linha e promove uma mistura entre as colunas da matriz. Para controle de integridade e autenticação, o WPA2 trabalha da mesma maneira que o protocolo WPA (Sartorato et al, 2008).

Segue abaixo (figura 14) uma comparação mostrando a evolução da segurança nas redes sem fio, comparativo entre os protocolos WEP e WPA2.

Ponto fraco do WEP	Como o ponto fraco é abordado pelo WPA2
O IV (vetor de inicialização) é muito pequeno	No CCMP do AES, o IV foi substituído por um campo de Número do pacote e duplicou em tamanho, para 48 bits.
Integridade dos dados fraca	O cálculo da soma de verificação criptografada pelo WEP foi substituído pelo algoritmo CBC-MAC do AES, que foi criado para fornecer uma integridade dos dados forte. O algoritmo CBC-MAC calcula um valor de 128 bits, e o WPA2 usa os 64 bits de ordem superior como um MIC (código de integridade da mensagem). O WPA2 criptografa o MIC com a criptografia do modo de contador do AES.
Usa a chave mestra em vez de uma chave derivada	Como o WPA e o protocolo TKIP (Temporal Key Integrity Protocol), o CCPM do AES usa um conjunto de chaves temporais derivadas de uma chave mestra e de outros valores. A chave mestra é derivada do processo de autenticação do 802.1X do EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) ou do PEAP (Protected EAP).
Sem rechaveamento	O CCMP do AES faz o rechaveamento automaticamente para derivar novos conjuntos de chaves temporais.
Sem proteção contra reexecução	O CCMP do AES usa um campo de Número do pacote como contador para fornecer proteção contra reexecução.

Figura 15 - Evolução da segurança em redes sem fio – comparativo WEP e WPA2

Figura 15: Fonte: Sartorato et al, 2008

O protocolo WPA2 não possui nenhuma vulnerabilidade reconhecida sobre a sua senha de autenticação. No ano de 2010 o pesquisador Md Sohail Ahmad da AirTight, encontrou uma vulnerabilidade chamada de Hole 196, essa vulnerabilidade permite que um usuário mal intencionado conectado a rede sem fio possa ter acesso ao tráfego que esta sendo gerado por outro usuário conectado a mesma rede (Peixoto, 2010)

O protocolo WPA2 utiliza duas chaves, a primeira chave é a PTK (*Pairwise Transient Key)*, que é única para cada cliente e que é utilizada para a proteção do tráfego entre o cliente e o ponto de acesso, e uma segunda chave denominada GTK (*Group Temporal Key)*, utilizada para cifrar o tráfego para todos os clientes na rede. A vulnerabilidade encontrada esta na segunda chave, a GTK (Peixoto, 2010)

O utilizador que pretende aceder ao tráfego dos outros utilizadores tem “apenas” de enviar um pacote falsificado, usando a chave GTK. De acordo com o descrito no protocolo, esta chave GTK não tem a capacidade de detectar pacotes falsificados, ao contrário da chave PTK, o que leva a que o cliente atacado não tenha a capacidade de detectar que está a sofrer um ataque. Com o envio destes pacotes o atacante consegue “routear” todo o tráfego de uma rede para si e posteriormente proceder à analise do mesmo, funcionando basicamente como um sniffer (Peixoto, 2010).

Mais esta vulnerabilidade é limitada, pois para realizá-la o atacante necessita estar conectado ao ponto de acesso.

Atualmente o protocolo WPA2 é considerado o mais seguro, pois possui uma forte criptografia e não possui nenhuma fragilidade conhecida referente à quebra de sua chave de autenticação.

2.4 SEGURANÇA ALÉM DA TECNOLOGIA.

Quando o termo segurança é tratado em redes de computadores, seja ela sem fio ou cabeada, geralmente a primeira coisa que se pensa é qual a tecnologia, protocolo ou quais políticas deve – se usar para a rede se tornar segura. A tecnologia é um fator de extrema importância na segurança nos dias de hoje, mais há outros fatores que são tão importantes quanto à tecnologia e as vezes acabam sendo esquecidos por profissionais de TI (Tecnologia da Informação) e por usuários domésticos. Estes fatores são os seguintes: Segurança Física, Processos em TI e Seres Humanos (Comer, 2007).

A segurança física visa proteger os ativos de informação que sustentam os negócios da organização. Nos dias de hoje a segurança física esta distribuída em equipamentos móveis, como em smartphones, notebook, impressoras, estações de trabalho e etc. A segurança física deve proteger todos estes dispositivos das vulnerabilidades físicas que cada um pode possuir. As vulnerabilidades são classificadas como (ISO 27000):

- Naturais: enchentes, tempestades, altas temperaturas, alta umidade entre outras.
- Sistemas de Apoio: queda de energia, queda de um link.
- Humanas: explosão, invasão, sabotagem.
- Eventos Políticos: ataque terrorista, greves, espionagem.

Visando evitar os problemas citados acima, devemos considerar algumas políticas de segurança, como:

- Controle de entrada física.

- Instalação e proteção de equipamentos.
- Proteção contra ameaças externas naturais.
- Controle de acesso de pessoas externas
- Proteção de áreas críticas.

Os processos de TI é o controle sobre hardware, rede, métodos de transmissão, compartilhamento, segurança na I*nternet* entre outros. Para melhor organização dessas atividades, é recomendado que processos sejam criados, funções atribuídas e que procedimentos sejam planejados, homologados e publicados (ISO 27000).

Se forem necessários serviços de terceiros, os mesmos precisam ser regulados e gerenciados. Necessidades de sistemas devem ser planejadas de acordo com a necessidade do negócio, passando por aprovação, testes e homologação antes de entrar em operação. Uma política de backup deve ser criada e gerenciada, pois nunca sabemos o que pode ocorrer com arquivos e documentos. Regras na troca de informações são de extrema importância, como procedimentos de mensagens eletrônicas (ISO 27000).

E pra finalizar a existência de registro de auditoria, log de sistemas, log de operação tanto do administrador quanto do usuário, sincronização do horário das estações de trabalho, ajudam a solucionar possíveis problemas com a segurança da informação (Campos, 2008).

As pessoas são consideradas o elemento principal na segurança da informação. As pessoas sempre estão envolvidas nos incidentes que ocorrem na segurança da informação, podem estar no lado vulnerável, ou lado das ameaças, ou seja, explorando as vulnerabilidades. Os seres humanos estão sujeitos a ataques de engenharia social. A engenharia social é capaz de mudar o comportamento de um ser humano, quando o objetivo é obter acesso a informações e sistemas não autorizados (Campos, 2008).

Para tentar evitar esse tipo de ataque, algumas políticas podem ser aplicadas antes do contrato pessoal, durante o contrato pessoal e depois do contrato pessoal.

Antes do contrato pessoal: a seleção, atribuição de função e a assinatura de termos e condições de trabalho.

Durantes a vigência do contrato: treinamentos, responsabilidades da gerência ou direção com a disciplina.

Após o encerramento do contrato: devolução de ativos e cancelamento dos direitos de acesso.

Essas três áreas definidas acima, aliada a tecnologia, possibilitam a existências dos princípios básicos de segurança em uma rede, esses princípios são: Confidencialidade, Integridade e Disponibilidade (Campos, 2008).

3. PROCEDIMENTOS EXPERIMENTAIS

Neste capítulo será descrito os procedimentos experimentais realizados para análise e estudo das redes sem fio de uma organização de grande porte, visando comparar os protocolos de segurança dos pontos de acesso.

3.1 Análises das redes sem fio em uma organização de grande porte.

Em busca de comparar os protocolos de segurança e outros métodos de segurança utilizados nas redes sem fio, foi realizada uma análise dos pontos de acesso em uma organização de grande porte. Com esta análise podemos verificar como as pessoas e profissionais de TI se preocupam com a configuração do seu ponto de acesso e consequentemente com os dados da sua rede e o uso da *Internet*.

Para execução desta análise utilizamos um notebook com uma distribuição Linux Debian, denominada Backtrack versão 5. Esta distribuição Linux é voltada para a parte de segurança e é bastante utilizada por profissionais de segurança da informação para avaliar riscos que uma rede sem fio ou cabeada pode possuir. Será utilizado juntamente ao notebook um adaptador sem fio externo com uma antena para maior alcance de sinal, essa antena proporciona um alcance de 9dbi.

Para busca das redes sem fio que estiverem ao alcance do sinal utilizamos o *software* que já esta disponível na distribuição Backtracjk 5, esse *software* é denominado Gerix. Com este *software* é possível verificar o SSID da rede sem fio, o canal que a rede esta utilizando e o protocolo de segurança utilizado pela rede.. Para utilizar este *software* é necessário possuir uma placa de rede que trabalhe em modo monitor e que seja suportada pelo Backtrack 5, no endereço http://www.backtrack-linux.org/wiki.index.php/wireless_drivers é possível encontrar os drivers de redes sem fio suportados pelo BackTrack 5.

Além do Gerix, utilizamos outro *software* disponível no Backtrack 5, este *software* é denominado Kismet, uma ferramenta muito útil para se utilizar nas redes sem fio. Pode ser usado como um analisador de redes e seus pacotes capturados

podem ser analisados em outros programas como o Wireshark. E também podemos utilizar o Kismet para checar redes vizinhas, o Kismet fornece o endereço MAC do ponto de acesso e dos possíveis clientes conectados. Assim como o Gerix, para utilizar o Kismet é necessário possuir uma placa rede que trabalhe no modo monitor.

3.1.1 Redes sem fio encontradas

Na busca realizada de redes sem fio dentro da organização de grande porte, através do *software* Gerix, foi encontrado ao todo um total de 22 redes sem fio (Figuras 16 e 17). Dessas 22 redes encontradas, 1 estava configurada com o protocolo de segurança WEP, 4 estavam configuradas com o protocolo de segurança WPA, 9 estavam configuradas com o protocolo de segurança WPA2 e 8 redes sem fio estavam sem nenhum protocolo de segurança configurada, ou seja, não havia necessidade de senha para a conexão.

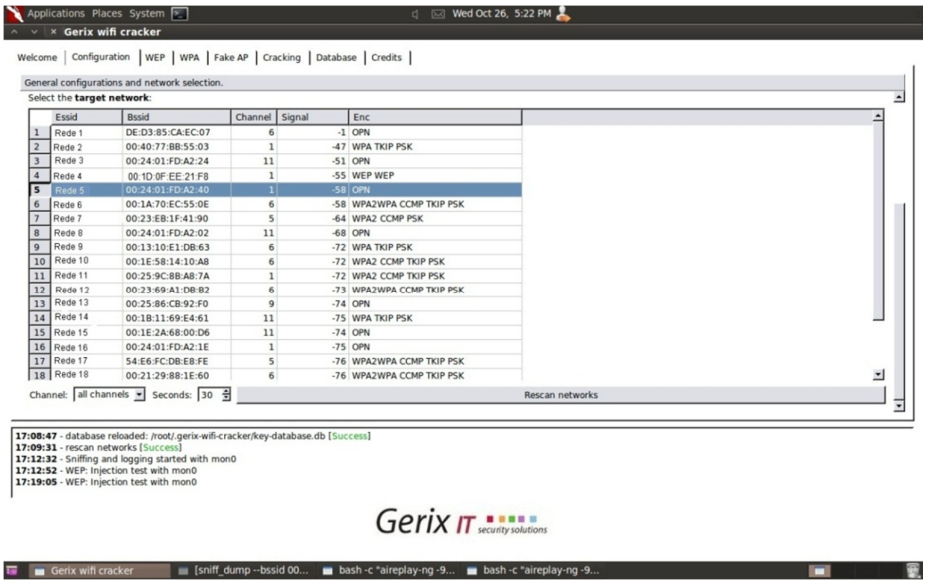

Figura 16 - Análise redes sem fio com Gerix parte 1

Fonte: O Autor

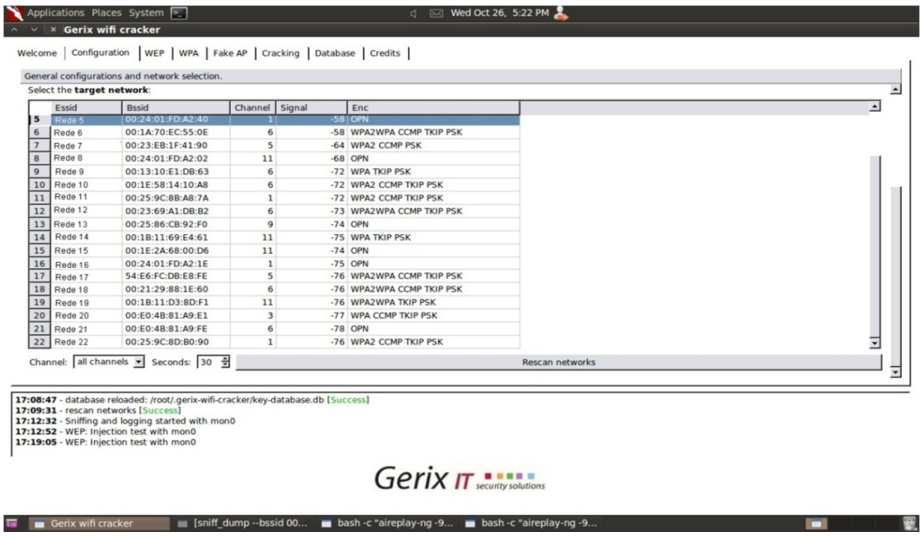

Figura 17 - Análise redes sem fio com Gerix parte 2

Fonte: O Autor

Outra informação muito importante que o *software* Gerix nos fornece, é o canal que cada ponto de acesso esta utilizando:

- 7 pontos de acesso estão configurados com o canal 6
- 6 pontos de acesso estão configurado com o canal 1
- 5 pontos de acesso estão configurados com o canal 11
- 2 pontos de acesso estão configurado com o canal 5
- 1 ponto de acesso está configurado com o canal 9
- 1 ponto de acesso está configurado com o canal 3

Uma modificação pode ser realizada nos pontos de acesso que estão utilizando os canais 3, 5 e 9. Esses pontos podem ser configurados com os canais 1, 6 ou 11, pois nestes canais não ocorrem sobreposição, ou seja, podem ser transmitidos dados simultaneamente sem interferência.

3.1.2 Rede sem fio abertas

Na análise realizada, foram encontradas 8 redes sem fio sem nenhum protocolo de autenticação configurado, uma falha de segurança muito grande, pois qualquer pessoa, seja ela mal intencionada ou não pode ser conectar a esta rede e utilizar a banda da *Internet* ou tentar acesso a informações da rede.

Na tentativa de associação com os pontos de acesso encontrados, utilizamos o gerenciador de redes e conexão do Backtrack 5. Conseguimos associação e navegação na *Internet* em 6 pontos de acesso, outros 2 pontos de acesso não foram mostrados pelo gerenciador de redes e conexão do BackTrack 5 e em uma rede foi necessário um pouco mais de trabalho para se realizar a associação, pois esta não tinha protocolo de segurança configurados, mais possuía habilitado o filtro de endereço MAC e o DHCP desabilitado.

Essas duas opções são consideradas maneiras de se aumentar a segurança do Ponto de Acesso, com o filtro de endereço MAC é necessário cadastrar no Ponto de Acesso, o endereço MAC da placa de rede sem fio de um notebook, celular, ou qualquer outro dispositivo que tenha uma placa de rede sem fio para que se tenha permissão para se associar ao ponto de acesso, e com o DHCP desabilitado é necessário configurar na placa de rede um endereço IP que faça parte da rede do Ponto de Acesso.

Mesmo como estes dois métodos adicionais de defesa, conseguimos realização com este ponto de acesso. Para isto utilizamos o *software* Kismet para descobrir o endereço MAC e um endereço IP de algum cliente que estivesse conectado a este ponto de acesso. O endereço MAC do cliente que utilizamos é o 44:A7:CF:35:42:61, e o endereço IP é o 172.17..4.173, máscara de rede 255.255.255.0 e o gateway(o IP do Ponto de Acesso) 172.17.1.1.

Para alterar o endereço MAC da placa de rede sem fio utilizamos os seguintes comandos:

#ifconfig wlan0 down

#ifconfig wlan hw ether 44:A7:CF:35:42:61

#ifconfig wlan0 up

E para configurar o endereço IP usamos o seguinte comando

#ifconfig wlan0 172.17.4.173 netmask 255.255.255.0 gw 172.17.1.1

Com estas configurações conseguimos nos associar ao ponto de acesso e navegar na *Internet*. Desse modo podemos ver que o filtro de MAC e o DHCP desabilitado são métodos de segurança que podem ser facilmente burlados com a ajuda de programas como o Kismet que foi utilizado nesta pesquisa.

3.1.3 Redes sem fio com o protocolo de segurança WEP.

Na análise que realizamos, conforme mostrado no Gerix, encontramos apenas um ponto de acesso configurado com o protocolo de segurança WEP.

Visando mostrar as vulnerabilidades do protocolo de segurança WEP, foi realizada uma tentativa de descoberta da senha para se associar a este pronto de acesso. Para isto utilizamos a distribuição Backtrack 5 e as ferramentas disponíveis., estas ferramentas são as seguintes: airodump-ng, aireplay-ng e o aircrack-ng.

O airodump-ng tem como principal finalidade capturar os IVs dos pacotes WEP, esses pacotes são capturados e salvos em um arquivo de log e são utilizados posteriormente pelo aircrack-ng para a descoberta da chave que o pacote WEP utilizava.

O aireplay-ng pode ser utilizado para realizar uma autenticação falsa, para desautenticar um cliente do ponto de acesso fazendo o mesmo realizar a autenticação de novo e assim é possível capturar a nova requisição ARP realizada pelo cliente e pacotes ACK recebidos.

Agora serão mostrados os comandos utilizados para realizar a descoberta da senha WEP deste ponto de acesso e assim realizar a associação.

Primeiramente é necessário estar com a placa de rede sem fio no modo monitor, para isso utilizamos o seguinte comando (Figura 18).

 # airmon-ng start wlan0.

Figura 18 - Ativar modo monitor na placa de rede sem fio

Fonte: O Autor

Agora vamos listar todas as redes WEP disponíveis ao nosso alcance e possíveis clientes associados ao ponto de acesso através do airodump-ng (Figura 19).

 # airodump-ng –encrypt wep mon0.

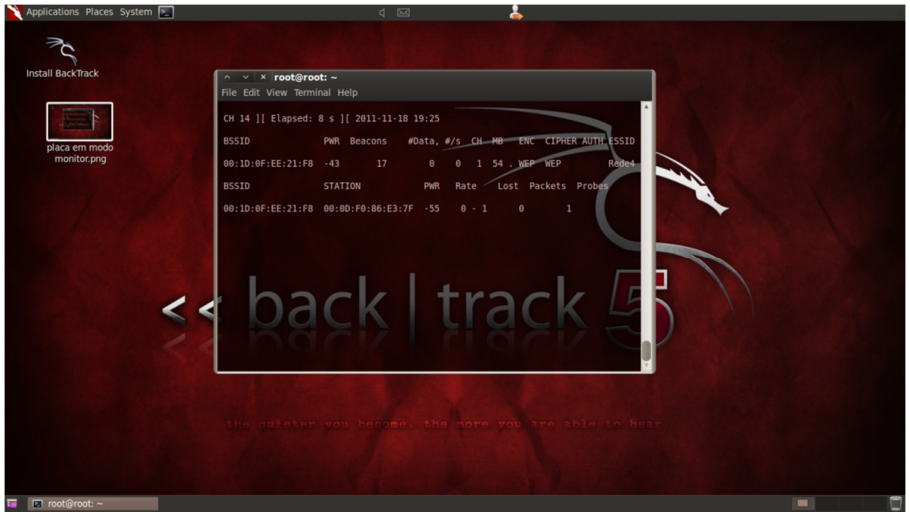

Figura 19 - Redes WEP disponíveis

Fonte: O Autor

Como é possível notar na imagem acima, foi listado um ponto de acesso com o protocolo WEP, esse ponto de acesso possui o SSID Rede4, endereço MAC 00:1D:0F:EE:21:F8, utiliza o canal 1 e possui um cliente associado no momento, o endereço MAC deste cliente é 00:0D:F0:86:E3:7F.

Após coletar estas informações do ponto de acesso e do cliente, vamos salvar em um arquivo todo o tráfego que o cliente gerar na rede, esse será utilizado posteriormente pelo aircrack-ng para tentativa de descoberta da senha WEP do ponto de acesso. Para isso utilizamos o seguinte comando.

 # airodump-ng –bssid 00:1D:0F:EE:21:F8 –c 1 –w Rede4 mon0

Onde o bssid é o endereço MAC do ponto de acesso, -c 1 é o canal que o ponto de acesso utiliza e –w Rede4 é o arquivo de log que estamos salvando no diretório atual (Figura 20).

Figura 20 - Salvando pacotes que passam pelo ponto de acesso

Fonte: O Autor.

Podemos observar na figura acima que esta passando tráfego neste ponto de acesso, onde esta # Data, mostrando a quantidade de tráfego gerada pelo ponto de acesso.

O próximo passo é forçar o cliente a realizar a desautenticação do ponto de acesso, para isto vamos utilizar o aireplay-ng (Figura 21)

 # aireplay-ng –deauth 1 –a 00:1D:0F:EE:21:F8 –c 00:0D:F0:86:E3:7F mon0

Onde –a é o endereço MAC do ponto de acesso e –c é o endereço MAC do cliente.

Este comando faz com que o notebook que estamos utilizando envie um pacote falseado ao ponto de acesso, simulando o processo de desconexão do cliente especificado. Enganada pelo pacote, o ponto de acesso desconecta o cliente, fazendo o cliente realizar a autenticação novamente, essa autenticação geralmente é realizada automaticamente pelos sistemas operacionais. Com isso o processo de autenticação será gravado no arquivo de captura que foi iniciado anteriormente.

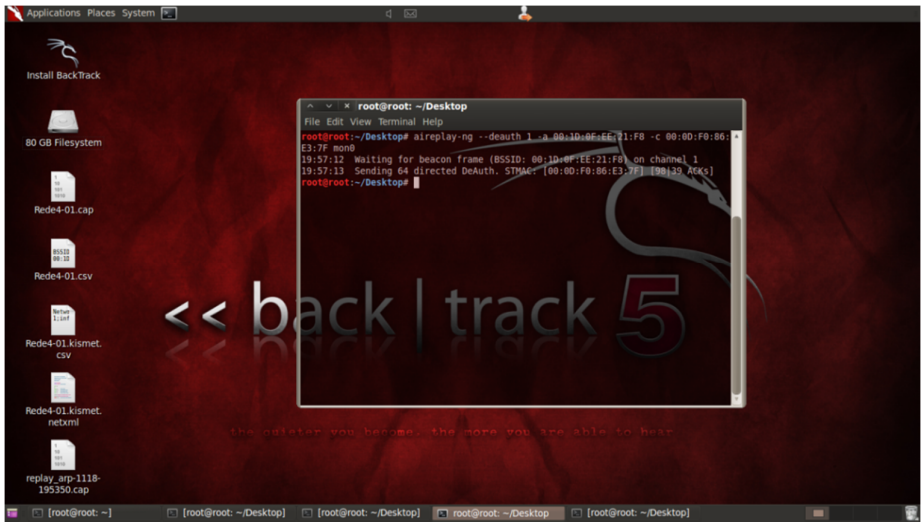

Figura 21 - Desautenticação do cliente e captura do processo de autenticação
Fonte: O Autor

Com a captura dos pacotes e do processo de autenticação, vamos utilizar o aricrack-ng para tentativa de descoberta de senha do ponto de acesso, para isso utilizamos o seguinte comando (Figura 22)

 # aircrack-ng –b 00:1D:0F:EE:21:F8 Rede4-01.cap

Onde –b é o endereço MAC do ponto de acesso e Rede4-01.cap é o arquivo onde esta armazenado os pacotes capturados e o processo de autenticação.

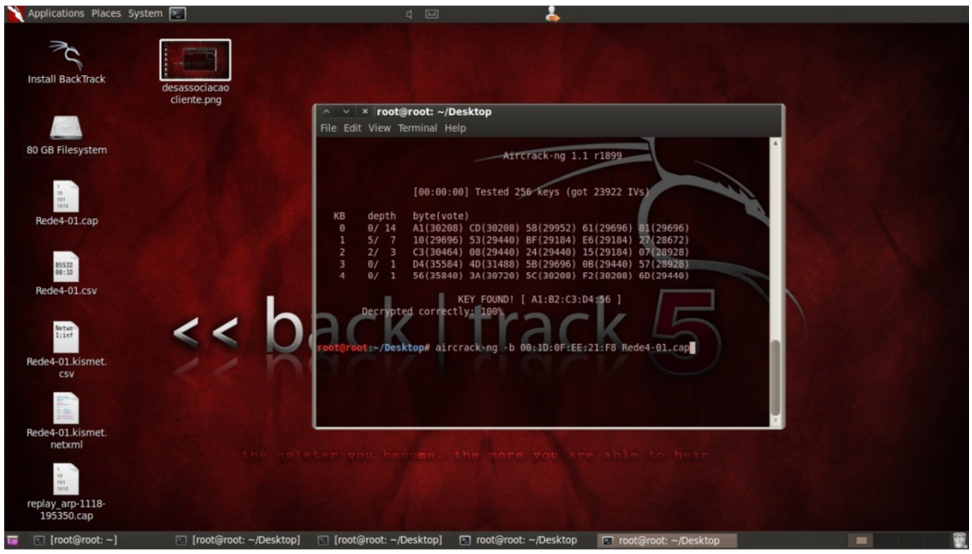

Figura 22 - Descoberta da senha feita pelo aircrack-ng
Fonte: O Autor.

Como mostrado na figura acima, o aircrack-ng obteve sucesso na descoberta da senha do ponto de acesso, a senha é a1b2c3d456, com essa senha realizamos a associação e navegamos na *Internet*.

Assim podemos observar que o protocolo WEP possui uma segurança muito frágil, essa fragilidade se deve ao vetor de inicialização do WEP ser muito pequeno, 24 bits, e não possui criptografia. Como esse vetor de inicialização é muito pequeno ele acaba se repetindo devido à alta quantidade de tráfego que temos nos dias de hoje. Com a captura desses pacotes e do processo de autenticação, é descoberta a senha de uma rede WEP.

3.1.4 Redes sem fio com o protocolo de segurança WPA.

Na análise realizada das redes sem fio de uma organização de grande porte, através do *software* Gerix, foram encontradas ao todo 4 prontos de acesso configurados com o protocolo de segurança WPA.

O WPA abandonou o uso dos vetores de inicialização e do uso da chave fixa, que eram os dois grandes pontos fracos do WEP. No lugar disso, passou a ser

usado o sistema TKIP onde a chave de encriptação é trocada periodicamente e a chave definida na configuração da rede é usada apenas para fazer a conexão inicial.

Combinando o uso do TKIP com outras melhorias, o WPA se tornou um sistema relativamente seguro, que não possui brechas óbvias de segurança. Mesmo com essas melhorias é ainda possível quebrar chaves fáceis ou com poucos caracteres usando através de ataques de força bruta, mas chaves com 20 caracteres ou mais são inviáveis de se quebrar, devido ao enorme tempo que seria necessário para testar todas as combinações possíveis. Para se realizar um ataque de força bruta é necessário possuir um dicionário ou uma *wordlist* como algumas pessoas chamam. Estes dicionários podem ser encontrados facilmente na *Internet,* podem ser encontrados dicionários por países, que contém as palavras e combinações alfanuméricas mais utilizadas num determinado país, há também dicionário por linguagem e o dicionário mundial que contém milhões de palavras.

Não foi realizada tentativa de força bruta nos pontos de acesso que foram encontrados porque não havia tráfego sendo gerado no momento que foi realizada as análises. Com a finalidade de mostrar como funciona uma tentativa de descoberta de senha WPA através da força bruta, foi simulada uma rede sem fio configurada com o protocolo WPA e criado um dicionário em formato texto que contém diversas palavras, entre elas a senha que foi utilizada para configurar o WPA no ponto de acesso.

O processo é semelhante com o do WEP e utiliza as mesmas ferramentas, o airodump-ng, o aireplay-ng e o aircrack-ng. Abaixo segue os comandos utilizados.

airmon-ng start wlan0 – Ativar o modo monitor na placa de rede sem fio

airodump-ng mon0 – para mostrar todas as redes disponíveis e clientes associados.

airodump-ng –w teste –c 6 mon0 – para capturar os pacotes de todas as redes que utilizam o canal 6 e salvá–los em um arquivo de log denominado teste.

aireplay-ng –deauth 1 –a (endereço MAC do ponto de acesso) –c (endereço MAC do cliente) – para desautenticar o cliente e obrigar a realizar a autenticação novamente, assim é possível capturar o pacote de autenticação e salvar no arquivo de log criado acima

aircrack-ng (SSID) –w password.lst teste-01.cap – onde password.lst é o dicionário que utilizamos e teste-01.cap é o arquivo de log com os pacotes capturados

O teste é feito de modo *offline*, usando os pacotes de autenticação capturados para simular o processo de autenticação usando cada uma das palavras que estão no dicionário.

O protocolo WPA é o mínimo de configuração de segurança que se deve ter em uma rede sem fio, com senhas de 20 caracteres configuradas. Com essa configuração o a força bruta se torna um ataque inviável devido ao tempo que iria demorar para descobrir a senha WPA.

3.1.4 Redes sem fio encontradas WPA2.

Mesmo o protocolo WPA não possuindo falhas de segurança se configurado corretamente, a IEEE resolveu disponibilizar o protocolo de segurança WPA2. Esse protocolo foi lançado para fortalecer ainda mais a segurança nas redes sem fio, sendo considerado atualmente o protocolo mais seguro, não possuindo vulnerabilidade conhecida atualmente referente a questão da chave de segurança.

Desse modo o protocolo WPA2 é o mais seguro nos dias de hoje e recomendado para configuração de autenticação nos pontos de acesso, pois possui um forte sistema de criptografia devido ao AES. Este protocolo é suportado em todos os equipamentos atualmente.

4. CONCLUSÂO

O referencial teórico descrito neste trabalho aliado a pesquisa de campo realizada em uma organização de grande porte, nos proporcionou analisar a segurança disponível para as redes sem fio e verificar as vulnerabilidades dos protocolos disponíveis atualmente.

De acordo a análise realizada foi possível verificar que quando é realizada a configuração do protocolo de segurança nos pontos de acessos, os usuários e administradores de redes estão adotando os protocolos WPA e WPA2, que são atualmente os protocolos mais seguros, o protocolo WPA pode sofrer ataques de força bruta, mais se estiver configurado com uma senha forte como, por exemplo, uma senha de 20 caracteres ou mais acaba tornando um possível ataque inviável em virtude do tempo que demoraria. O protocolo WPA2 não possui nenhum ataque conhecido atualmente, por isto é considerado o protocolo de redes sem fio mais seguro e é o protocolo recomendado para se configurar nos pontos de acesso nos dias de hoje.

O protocolo WEP não esta sendo muito utilizado na configuração dos pontos de acesso devido as suas vulnerabilidades conhecidas. Na análise realizada encontramos uma rede sem fio configurada com este protocolo e conseguimos mostrar as vulnerabilidades deste protocolo descobrindo a senha de acesso à rede sem fio que estava configurada no ponto de acesso.

Encontramos também pontos de acesso que não possuíam nenhum protocolo de segurança configurado, isto é uma grande falha de segurança, pois pode permitir qualquer pessoa utilizar a conexão da *Internet* e dependendo da configuração interna da rede pode ser possível acesso a servidores e dados importantes.

Outro fator importante a se destacar, são as frequências configuradas para os pontos de acesso. A maioria dos equipamentos são configurados de fábrica para utilizarem o canal 6, alguns administradores de rede e usuários domésticos, esses mais por desconhecimento, acabam não alterando a configuração do canal, causando assim interferência entre os pontos de acesso devido ao grande número de equipamentos que estão utilizando a mesma frequência, por isto é recomendado fazer uma verificação da ocupação dos canais pelos pontos de acesso ao alcance,

isto é possível atualmente na maioria dos equipamentos, após esta verificação é recomendada a utilização dos canais 1, 6 e 11.

Estima-se que com as inovações tecnológicas e com a pesquisa de vulnerabilidades que *hackers* fazem nos dias de hoje, podem futuramente ser descobertas novas vulnerabilidades nos protocolos WPA e WPA2. E também com o avanço da tecnologia pode surgir um novo protocolo de segurança para as redes sem fio e um aumento na utilização de pontos de acesso na faixa de frequência de 5Ghz ficando assim como sugestão de trabalhos futuros uma nova análise de novas vulnerabilidades e novos protocolos em segurança de redes sem fio.

REFERÊNCIAS

ALECRIM Emerson. **Tecnologia Wi-Fi (IEEE 802.11).** 2008. Disponível em: http://www.infowester.com/wifi.php > Acessado em 22/06/2011 às 19h04min.

BARBOSA Anderson. **Padrão IEEE 802. 2010.** Disponível em: http://desmontacia.wordpress.com/2010/09/29/padro-ieee-802 > Acessado 22/06/2011.

CAMPOS André**. Auditoria em Tecnologia da Informação,** 2008. Disponível em: http://www.slideshare.net/NLDT/auditoria-em-segurana-da-informao-andre-campos > Acessado em 17/10/2011

COMER Douglas E. **Redes de Computadores e internet** 4ª ed. Porto Alegre, Bookman, 2007.

FOROUZAN A. Behrouz. **Comunicação de Dados e Redes de Computadores**. 3ª ed. Porto Alegre, Bookman, 2004.

GIL Antonio C. **Como elaborar projetos de pesquisa**. 5ª ed. São Paulo: Atlas, 2010.

ISO 27000. **Grupo de segurança da Informação: Uma Abordagem Profissional**. Disponível em: http://www.iso27000.com.br/index.php?Option=com_content&view=article&id=65:segingprof&catid=34:seginfartgeral&Itemid=53 > Acessado em 17/10/2011

KOTVISKI André. **O que são redes Ad – Hoc.** 2009. Disponível em: http://www.tecmundo.com.br/2792-o-que-sao-redes-ad-hoc-.html > Acessado em 21/10/2011.

OZORIO Cesar Wellington. **ANÁLISE COMPARATIVA ENTRE OS PROTOCOLOS DE SEGURANÇA WEP, WPA E WPA2,** 2007. Disponível em: http://bibdig.poliseducacional.com.br/document/?view=47 > Acessado em 21/06/2011

PEIXOTO Martins Aureliano. **Wireless Sem Colisões**, 2011. Disponível em http://aurelianomartins.wordpress.com/2011/04/21/wireless-%E2%80%9Csem-colisoes%E2%80%9D/ > Acessado em 15/10/2011

PEIXOTO Martins Aureliano. **Detalhes e Webinar sobre a vulnerabilidade Hole 196 do WPA2,** 2010. Disponível em http://aurelianomartins.wordpress.com/2010/08/03/detalhes-e-webinar-sobre-a-vulnerabilidade-hole196-do-wpa2/ > Acessado em 22/10/2011

PEREIRA H. B. **Segurança em redes wireless 802.11 infraestruturadas**. 2009. Disponível em: <http://www.ginux.ufla.br/files/artigo-HelioPereira.pdf>. Acesso em: 20/10/2011.

RAPPAPORT Theodore S. **Comunicação Sem Fio, Princípios e Práticas.** 2ª ed. São Paulo, Pearson, 2009.

RODRIGUES Paulo Henrique. **Quadro Comparativo Camadas ISO-OSI e TCP/IP**, UNIP/SP, 2009. Disponível em: http://paulohrodrigues.blogspot.com/2009/09/tabelas-iso-osi-e-tcpip.html

RUFINO Nelson M. de Oliveira. **Segurança em Redes sem fio.** São Paulo, Novatec, 2005.

SAADE D. M.; et al. **Multihop MAC: desvendando o padrão 802.11s**. Capítulo 1 do livro texto Minicursos SBRC 2008 do 26º simpósio brasileiro de redes de computadores. Niterói, 2008. Disponível em: <http://www.ic.uff.br/~celio/papers/minicurso-sbrc08.pdf>. Acesso em: 13/10/2011

SANTOS Pinheiro M. José. **OSI: Um modelo de Referência**, 2008. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_osi_um_modelo_de_referencia.php

SARTORATO Flavio Malfati. et al. **Análise de Protocolo de Enlace IEEE 802.11,** 2008. Disponível em: http://www.infosegura.eti.br/artigos/80211.php > Acesso em 15/10/2011

SILVA, Leandro Rodrigues **Segurança em Redes Sem Fio (Wireless**), PUC/PR, 2010. Disponível em http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Leandro%20Rodrigues%20Silva%20-%20Artigo.pdf > Acessado em 22/06/2011