UNIVERSIDADE SAGRADO CORAÇÃO

KLEBER BELTRAMI DO AMARAL

VULNERABILIDADE NO PROTOCOLO DE SEGURANÇA WEP E POLÍTICAS DE PROTEÇÃO PARA REDES SEM FIO

BAURU
2012

KLEBER BELTRAMI DO AMARAL

VULNERABILIDADE NO PROTOCOLO DE SEGURANÇA WEP E POLÍTICAS DE PROTEÇÃO PARA REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título de Bacharel em Ciência da Computação, sob orientação do Prof. Ms.Wiliam Carlos Galvão.

BAURU
2012

Amaral, Kleber Beltrami do

A485v

Vulnerabilidade no protocolo de segurança wep e políticas de proteção para redes sem fio / Kleber Beltrami do Amaral -- 2012.

45f. : il.

Orientador: Prof. Ms. Wiliam Carlos Galvão.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Sagrado Coração - Bauru - SP

1. Wireless. 2. Tecnologia. 3. Falhas. 4. Segurança. I. Galvão, Wiliam Carlos. II. Título.

KLEBER BELTRAMI DO AMARAL

VULNERABILIDADE NO PROTOCOLO DE SEGURANÇA WEP E POLÍTICAS DE PROTEÇÃO PARA REDES SEM FIO.

Trabalho de conclusão de curso apresentado à Universidade Sagrado Coração, para a obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof.Me. Wiliam Carlos Galvão.

Profº Esp. Henrique Pachioni Martins

Universidade Sagrado Coração

Profº. Dr. Élvio Gilberto da Silva

Universidade Sagrado Coração

Profº. Ms. Wiliam Carlos Galvão

Universidade Sagrado Coração

Bauru, 22 de Junho de 2012.

LISTAS DE FIGURAS

SUMÁRIO

AGRADECIMENTOS

Agradeço aos meus pais, que sempre fizeram o possível para que eu me tornasse quem sou e que me ajudaram com os objetivos que consegui até agora.

Aos meus amigos com quem ri, briguei, aprendi e ajudei durante esses anos convivendo juntos.

Aos professores sempre dispostos a ensinar e ajudar para que este momento fosse possível.

Ao meu orientador Prof. Ms. Wiliam Carlos Galvão, pela disposição, vontade e atenção.

“Deus nos fez perfeitos e não escolhe os capacitados,

capacita os escolhidos.”

Albert Einstein

RESUMO

O crescimento das redes wireless nos dias de hoje está claro, a facilidade e mobilidade que esta gerou caíram nas graças de todos, tanto as redes domésticas quanto as empresariais estão utilizando esta tecnologia em suas redes de computadores. Mas é necessário ficar atento as falhas e vulnerabilidades que surgem junto a ela, vários métodos são utilizados por *hackers* para invadir e roubar dados, e para que isso seja evitado, devem-se tomar precauções e utilizar o que a tecnologia nos oferece para manter a segurança intacta. Através de captação de sinais de redes sem fio, pessoas com conhecimento podem utilizar ferramentas especificas para fraudar a segurança e obter acesso a esta rede privada, correndo o risco de copiar dados importantes e causar prejuízos as empresas e pessoas. Sendo assim, existe a necessidade de implementar regras ou políticas de segurança para que isso não ocorra.

Palavras Chave: Wireless. Tecnologia. Falhas. Segurança.

ABSTRACT

The increase of wireless networks today are obvious, the facility and mobility that is generated fell into the graces of everyone, both the corporate and personal networks are using this technology in their computers. But is necessary that you be alert of the weaknesses and vulnerabilities that come with it, several methods are used by hackers to break into and steal data, and to prevent it, you should take precautions and use what technology offers us to keep security intact. By capturing signals of wireless networks, people with knowledge can use specific tools to cheat security and gain access to private network, at the risk of copying important data and cause damage to companies and people, there is a need to implement security rules to prevent this from happening.

Keywords: Wireless. Technology. Failures. Security.

1 INTRODUÇÃO

As redes baseadas em *Wireless* combinam conectividade e mobilidade, pôr parte de seus usuários, assim como simplicidade em sua configuração. Nos últimos sete anos esse tipo de rede tem crescido e tem ganhado popularidade nos diversos setores, principalmente no que diz respeito às WLAN (*Wireless Local Area Network*) (MENEZES, 2004).

A Rede *Wireless* (sem fio) foi criado para a transmissão de dados sem a necessidade de redes cabeadas, proporcionando praticidade e conveniência aos usuários. Segundo Moher e Haykin (2008), os dispositivos *Wireless* estão em toda parte. Telefones celulares são itens de consumo muito comuns. Além disso, há uma tendência em substituir o cabeamento das redes Ethernet por redes *Wireless*. A introdução desses serviços aumentou a mobilidade e a área de serviço de muitas das aplicações existentes, criando numerosas aplicações (não previstas). A tecnologia *Wireless* é uma área em franco crescimento nas redes públicas e tem se destacado nos sistemas de comunicações privados/dedicados (MOHER e HAYKIN, 2008).

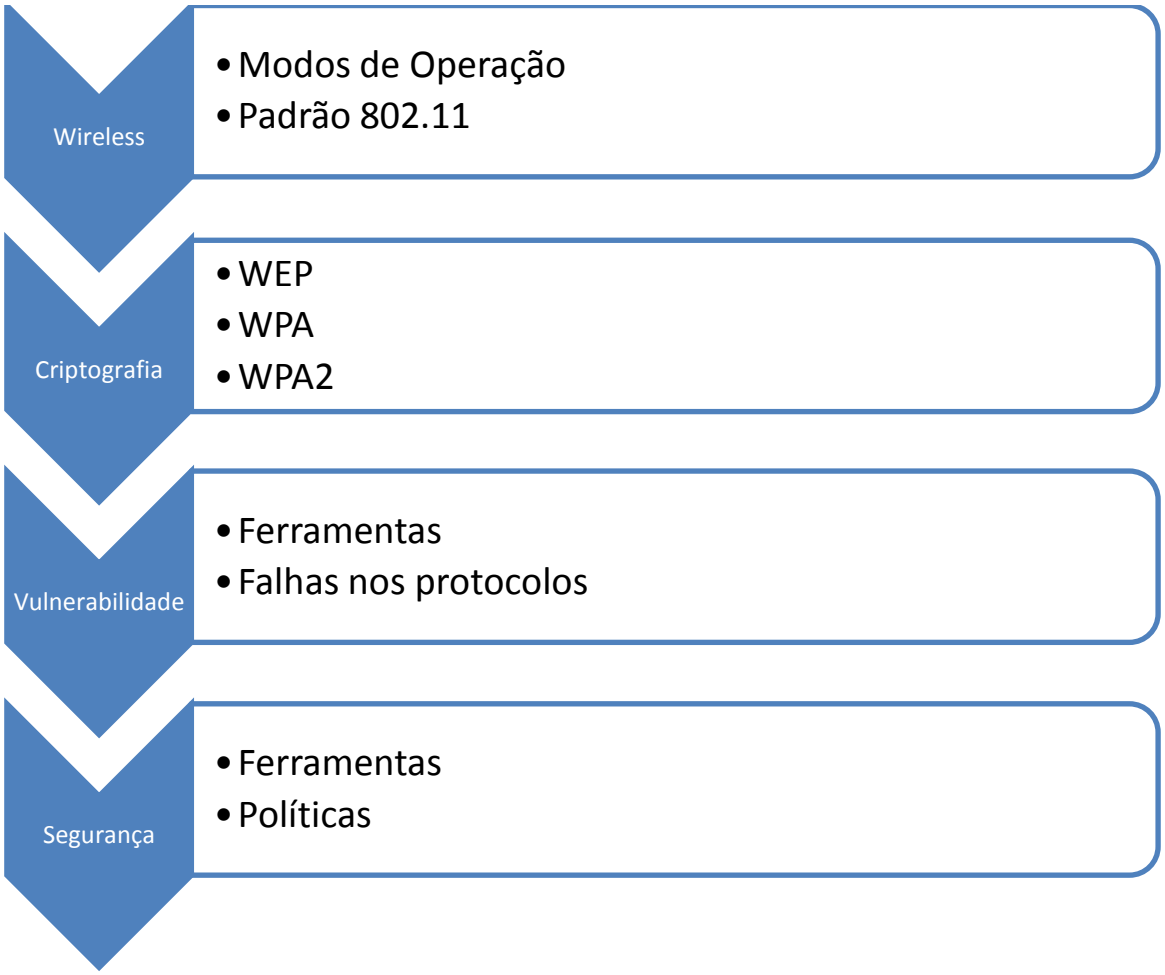
Surgiu a necessidade de se criar uma segurança para que dados pessoais e sigilosos pudessem ser transmitidos sem correr o risco de serem vistos por outras pessoas, foram criados então, os protocolos de segurança para redes sem fio que tem como função utilizar algoritmos de criptografia para que os dados não possam ser visualizados (MORAZ, 2006).

Com todo o aumento na utilização das redes sem fio, *hackers* começaram a procurar métodos para que esses protocolos de segurança fossem fraudados e assim as informações dos usuários pudessem ser acessadas e utilizadas para proveito próprio (MORAZ, 2006).

Foi abordada toda a criação do sistema *Wireless* incluindo seu desenvolvimento, suas mudanças com o tempo, a topologia e os padrões criados, para melhorarem seu funcionamento. Também serão citadas, as criptografias utilizadas para segurança, além de ferramentas especificas para este fim, como o

firewall e o IDS (Sistema para Identificação de Intrusos) e finalmente algumas ferramentas utilizadas para que se possa tentar quebrar a segurança de uma rede sem fio.

Finalmente, o intuito é demonstrar como é necessária a utilização de políticas de segurança para evitar que as redes sejam invadidas e para isso serão simuladas invasões em uma rede onde a segurança da sua chave é mínima, abaixo temos de forma resumida uma lista que demonstra os principais conteúdos abordados.



1.1 JUSTIFICATIVA

Sistemas Wireless surgiram para facilitar a vida das pessoas. A praticidade com que se pode ser utilizado na criação de uma rede foi o que chamou tanto a atenção de todos. Mas é necessário também que se demonstrem as falhas existentes nas redes sem fio, criptografia falha, senhas mal elaboradas, e outros fatores podem comprometer a segurança da rede, colocando em risco a privacidade das informações que trafegam por ela.

Este trabalho busca contribuir para que as vulnerabilidades e falhas existentes em uma rede sem fio possam ser eliminadas garantindo uma maior confiabilidade e segurança destas redes. Isso foi feito através da demonstração das falhas em meios de encriptação e senhas de baixo nível de segurança, além de citar alguns métodos que podem ser utilizados através de políticas e práticas de segurança e medidas simples para que possam ser reparados, mantendo a privacidade de sua rede contra ataques e invasões.

2 OBJETIVOS

2.1 Objetivo Geral

Realizar testes de invasões em redes sem fio para verificar as vulnerabilidades e obter a senha utilizada, além de desenvolver uma lista com políticas de segurança para prevenir esses problemas.

2.2 Objetivos Específicos

- Capturar as possíveis redes sem fio existentes.
- Simular ataques a rede sem fio.
- Analisar as vulnerabilidades encontradas.
- Obter a chave já desencriptada.
- Definir políticas de segurança para redes sem fio através das falhas identificadas.

3 WIRELESS

Segundo Ross (2008), a tecnologia hoje chegou a um grau de disseminação na sociedade que faz com que esteja presente em todas as áreas do trabalho e também até nas áreas do entretenimento. Esse aumento fez com que as pessoas queiram se conectar nas redes a todo o momento.

Em muitas situações é impossível ou muito custoso montar uma estrutura de conexão utilizando cabeamento normal. É ai que entra a conexão de wireless (Figura 1). As redes sem fio correspondem a infraestruturas que dão acesso a conexão de computadores entre si ou a uma rede, utilizando tecnologias de comunicação que dispensam a utilização de cabos (ROSS, 2008).

Para Jardim (2007), a *Wi-Fi* é o nome usado para demonstrar um conjunto de padrões Wireless desenvolvido pelo comitê 802.11 do IEEE (*Institute of Eletrical and Eletronic Engineers*). A tecnologia tornou-se a de mais rápida adoção no mundo computacional nos últimos quatro anos. E é dividida em três principais padrões: 802.11b, 802.11a e 802.11g.

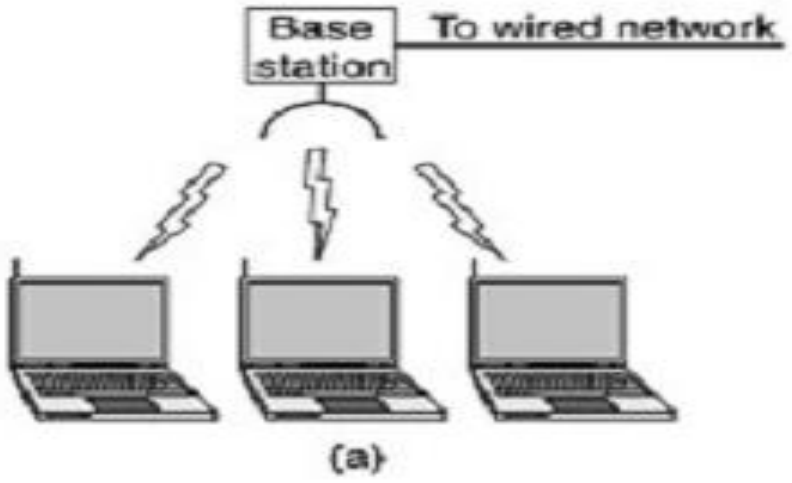


Figura 1: Wireless (rede sem fio)
Fonte: Tanenbaum (2003).

3.1 Modos de Operação

Nos modos de operação, um SSID (*Service Set Identifier*), é conhecido como “Nome da rede sem fio” e identifica a rede sem fio. O SSID é um parâmetro configurado no Ponto de Acesso, para o modo infraestrutura, ou para um cliente sem fio em todos os modos. O SSID é frequentimente anunciado pelo AP ou pela estação usando um MAC 802.11 conhecido como *beacon frame* (quadro de anúncio). Entretanto, algumas implementações de segurança dizem para não mostrar o SSID em redes privadas e com o acesso restrito. Quando utilizado o modo ponto-a-ponto (*Ad-Hoc*), um dispositivo conectado a rede *Wi-Fi* se comunica diretamente com outro(s) dispositivo(s) (JARDIM, 2007).

3.1.1 Ad-Hoc

Quando se trata de redes *ad-hoc*, são redes que não tem infraestrutura. A conexão é feita diretamente entre os usuários, as máquinas sem fio agrupam-se em uma topologia de malha para formarem um conjunto básico de serviços independentes (Figura 2). A responsabilidade pela organização e controle nessas redes é distribuída entre as próprias máquinas, que funcionam como roteadores capazes de encaminhar, de forma comunitária, os quadros que vem das máquinas vizinhas (CHAVES, 2010).

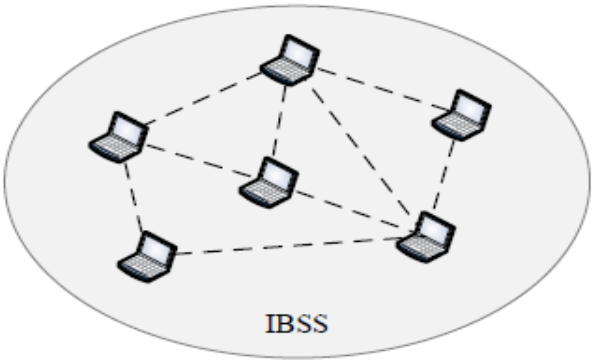


Figura 2: Rede sem fio Ad-hoc
CHAVES (2010).

3.1.2 Infraestrutura

De acordo com Jardim (2007), a comunicação no modo infraestrutura utiliza um dispositivo centralizador (semelhante ao tradicional *hub* na rede cabeada). Assim, para que os dispositivos se comuniquem, é preciso se comunicar a um controlador ou ponto central. Esse controlador recebe o nome *de Acces Point*, ou simplesmente ponto de acesso (Figura 3). O modo infraestrutura utiliza o conceito de BSA (*Basic Service Area*) que mostra a área na qual os dispositivos móveis podem trocar dados. A área que é abrangida por um Ponto de Acesso é chamada BSS (*Basic Service Set*). Cada BSS possui um identificador (SSID).

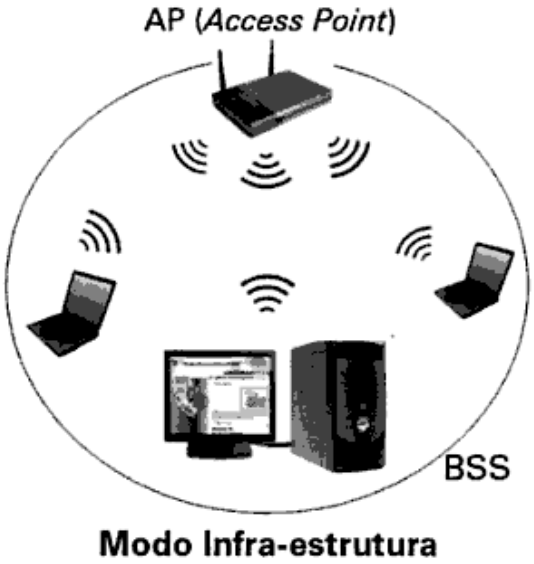


Figura 3:Modelo de Infraestrutura
JARDIM (2007).

3.2 Padrão 802.11

Juntamente com o surgimento dos *notebooks*, as pessoas sonhavam com o dia em que entrariam em um escritório e seu *notebook* se conectaria a Internet. Em decorrência disso, muitos grupos começaram a pesquisar para descobrir maneiras de alcançar esse objetivo. A abordagem mais prática é colocar tanto no escritório

quanto nos *notebooks,* transmissores e receptores de rádio de ondas curtas para permitir a comunicação entre eles. Esse método levou rapidamente à comercialização de LANs sem fios por várias empresas (TANENBAUM, 2003).

Tanenbaum (2003) ainda afirma que o problema era encontrar transmissores e receptores que fossem compatíveis. Essa proliferação de padrões significava que um computador equipado com um rádio da marca X não funcionaria em uma sala equipada com uma estação base da marca Y. Finalmente, a indústria decidiu que um padrão de LAN sem fio poderia ser uma boa idéia, e assim o comitê do IEEE que padronizou as LANs sem fios recebeu a tarefa de elaborar um padrão de LANs sem fios. O padrão recebeu o nome 118802.11. Um apelido comum para ele é *Wi-Fi*. Trata-se de um padrão importante e que merece respeito, e assim vamos chamá-lo por seu nome correto, 802.11.

3.2.1 Padrão 802.11b

Este padrão funciona na faixa de 2,4GHz, conhecida como ISM (*Industrial Scientific and Medical*). Utiliza as técnicas DSSS (*Direct Sequency Spread Spectrum*). Como trabalha numa banda mais baixa esse padrão corre mais riscos de sofrer interferências provocadas por outros tipos quaisquer de fontes, como por exemplo, celulares, fornos de microondas, telefones sem fio, etc, pois estes trabalham na mesma faixa de 2,4GHz. Para atingir taxas de 5,5Mbps e 11Mbps é utilizado em conjunto, a técnica CCK (*Complementary Code Keying*). Este padrão utiliza modulação DBPSK (*Differential Binary Phase Shift Keying*) para taxas de 1Mbps e DQPSK (*Differential Quadrature Phase Shift Keying*) para taxas de 2, 5,5 e 11Mbps (SANTOS, 2008).

3.2.2 Padrão 802.11g

Sobre este sub-padrão, Santos (2008) afirma ser o mais recente e que está no mercado a pouco tempo. Tenta reunir as principais vantagens do 802.11a e b. Trabalha na mesma faixa do padrão 802.11b. Por ter menor atenuação, pode trabalhar na mesma faixa do padrão mais antigo, 802.11b, e assim pode interoperar com as bases já instaladas com maior facilidade apesar de diminuir suas taxas. O uso da multiplexação por divisão de freqüência ortogonal, também conhecido como OFDM (*orthogonal frequency-division multiplexing*) permite que sejam atingidas taxas de até 54Mbps, pois ele divide os bits em diversos *streams* (fluxo de mídia) de taxas menores podendo transmitir os dados por sub-canais paralelos (SANTOS, 2008).

3.2.3 Padrão 802.11a

Surgiu depois da criação dos padrões 802.11 e 802.11b com a expectativa de resolver os problemas existentes nestes. O padrão 802.11a tem como principal característica o aumento da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), mas podendo operar em velocidades mais baixas. Outra diferença é a operação na faixa de 5 GHz, uma faixa com poucos concorrentes, porém com menor área de alcance (RUFINO, 2005).

Tem a disposição também aumento na quantidade de clientes conectados (64) e ainda no tamanho da chave usada com WEP, chegando a alguns casos a 256 bits (mas possui compatibilidade com os tamanhos menores, como 64 e 128 bits). Por fim, utiliza muito o tipo de modulação OFDM, diferentemente do DSSS usado no 802.11b.

Outra vantagem deste padrão consiste na quantidade de canais não sobrepostos disponíveis, um total de 12, diferentemente 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 (RUFINO, 2005).

Ainda segundo Rufino (2005) existem novos padrões que estão surgindo, como o 802.11n, também conhecido como WWiSE (*World Wide Spectrum Efficiency*). Este é um padrão em desenvolvimento, cujo foco principal é o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM, conhecida como MIMO-OFDM (*Multiple Input, Multiple Out-OFDM*). Outra Característica deste padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 Mhz, também, manter compatibilidade com os 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135 Mbps.

A Figura 4 mostra a evolução dos padrões 802.11 desde sua criação até os dias atuais.

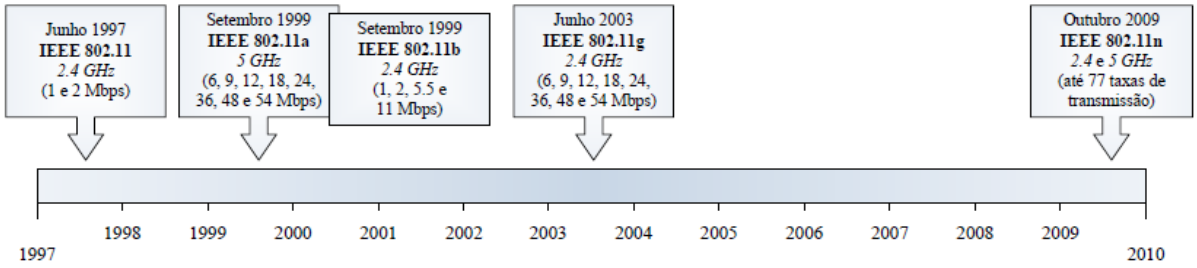


Figura 4: Evolução do padrão 802.11 ao longo dos anos
Fonte: CHAVES (2010) apud MCCANN (2010)

3.3 Criptografia

Santos (2008) diz que a criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida somente pelo seu destinatário (detentor da “chave secreta”). O que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

3.3.1 WEP

O protocolo WEP (Wired Equivalent Privacy) foi criado com o intuito de garantir a privacidade da comunicação entre os clientes e os pontos de acesso. Foi levado em consideração o custo para implementar o protocolo no *hardware*. A base de funcionamento do WEP é a utilização do algoritmo criptográfico RC4 com chaves de 40 bits para cifrar os pacotes trocados entre o ponto de acesso e o cliente, de uma forma que a informação não possa ser recebida por outro cliente qualquer que não tenha a chave criptográfica. Para evitar que o pacote seja alterado antes de chegar ao destino, o WEP utiliza uma função detectora de erros chamada CRC-32. Ao fazer o *checksum* (código usado para verificar a integridade de dados transmitidos através de um canal com ruídos ou armazenados em algum meio por algum tempo) do pacote, utiliza-se esta função para gerar um outro identificador chamado ICV (*Integrity Check Value*) que é conferido no destino do pacote. Como uma primeira tentativa de fornecer segurança para as comunicações sem fio, o WEP foi bem vindo e é largamente utilizado até hoje (BARBOZA, 2008).

Todavia, as falhas de segurança fizeram com que o WEP perdesse a credibilidade para ser usado em redes sem fio onde os requisitos de segurança fossem exigentes. Seu modo de operação é vulnerável, uma vez que utiliza sempre a mesma chave na comunicação, portanto acaba facilitando na captura de alguns pacotes e análise dos mesmos para a descoberta da chave da rede (ANTONIO, 2008).

3.3.2 WPA

Desenvolvido pela *Wi-Fi Alliance*, o grupo que tem os direitos da marca Wi-Fi e é responsável por certificar todos os dispositivos compatíveis com este padrão, WPA é um esforço para tentar suprimir as falhas de segurança encontradas no WEP. Ele foi criado tendo base o modelo IEEE 802.11i, já incluindo a maioria desta especificação. Sua versão mais recente, WPA2 (WPA versão 2), é 100% compatível

com o 802.11i. WPA é compatível com todos os adaptadores de rede sem fio, porém requer atualização dos pontos de acesso mais antigos (BARBOZA, 2008).

Para implementar o WPA, Barboza (2008) reitera que pode ser necessário atualizar o *firmware* tanto do ponto de acesso quanto dos adaptadores Wi-Fi. Este padrão foi desenvolvido para a utilização em conjunto com um servidor de autenticação IEEE 802.1x, também chamado de servidor AAA (*Authentication, Authorization and Accounting*), porém pode ser usado no modo chave pré-compartilhada, onde todos os dispositivos Wi-Fi usam a mesma palavra-chave para o acesso. Dentre os diversos avanços do WPA em relação ao WEP, destacamos o TKIP (*Temporal Key Integrity Protocol*).

Este protocolo foi elaborado com o intuito de ser o mais compatível possível com o WEP, de maneira que não fosse necessária a troca dos dispositivos de rede Wi-Fi. Portanto ele continua a utilizar o RC4, usado no WEP e comprovadamente inseguro nos padrões de hoje. O que o torna mais seguro do que o WEP, dentre outros atributos, é a checagem de integridade da mensagem e redistribuição de chaves. No WEP, é possível alterar o conteúdo de um pacote cujo conteúdo seja conhecido, mesmo sem decifrá-lo. Isto não acontece com o TKIP, pois sua verificação de integridade de mensagens cobre este caso. A redistribuição de chaves faz com que um atacante tenha menos dados decifrados com uma mesma chave para tentar algum tipo de ataque, pois a chave de cifragem usada por um dispositivo móvel é trocada periodicamente (BARBOZA, 2008).

3.3.3 WPA2

Esse protocolo foi autenticado pelo IEEE em 2004, ficando como um produto disponível por meio da *Wi-fi Alliance.* A diferença entre o WPA2 e o WPA é sua criptografia utilizada. O WPA utiliza o TKIP com o RC4, já o WPA2 utiliza o AES (*Advanced Encryption Standard*) em conjunto com o TKIP com chave de 256 bits, que é um método de criptografia muito mais poderoso. O AES permite a utilização de chaves de 128, 192 e 256 bits, que juntas formam assim uma ferramenta poderosa de criptografia. A chave de 256 bits no WPA2 é padrão. A utilização do AES necessita de um novo *hardware*, que seja capaz de fazer todo o processo

criptográfico, pois em dispositivos mais recentes é necessário existir um co-processador para realizar os cálculos da criptografia (AGUIAR, 2005).

3.4 Ferramentas de Segurança

Para prover segurança no acesso a uma rede, diversos modelos de segurança podem ser aplicados em diversos níveis. Cada um possui vantagens e desvantagens que são convenientes ou não para situações específicas (BARBOZA, 2008).

3.4.1 Firewall

Firewalls são os mecanismos de controle de acesso que deixam uma rede segura verificando acessos indesejáveis na rede. De maneira simplificada, um firewall é um roteador ou conjunto de roteadores que é instalado no ponto onde a rede privada é conectada à rede pública. Os computadores na rede privada não estão abertos ao mundo “externo”. Qualquer tentativa maliciosa para acessá-los exigiria passar pelo *firewall*. Portanto, um firewall age como um buffer entre uma rede privada e uma rede pública como a Internet (Figura 5). Em outras palavras, um *firewall* protege uma rede do acesso não-confiável (PARIHAR, et al, 2002).

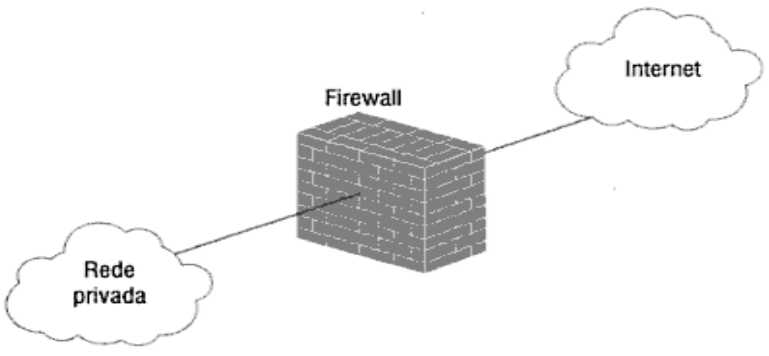


Figura 5: Disposição tradicional de um sistema firewall
Fonte: PARIHAR, et al (2002)

3.4.2 Filtragem de Endereços MAC

A filtragem de endereços MAC (*Media Access Control*) pode ser uma boa alternativa para a segurança de redes Wireless, Forouzan (2008) diz que os endereços MAC e IP (*Internet Protocol*) possuem dois tipos de identificadores diferentes: Precisamos dos dois protocolos porque uma rede física, como a E*thernet*, geralmente utiliza dois ou mais protocolos diferentes de camada de rede ao mesmo tempo, tal como o IP e o IPX (Novell). Do mesmo modo, um pacote como o IP pode trafegar por diferentes redes físicas, por exemplo, *Ethernet* e *Token Ring*. Isso significa que o processo de entrega de um pacote para um cliente ou roteador requer dois níveis de endereçamento: IP e MAC. Precisamos ser capazes de mapear um endereço IP a partir do endereço MAC correspondente.

3.4.3 Detecção de Intrusos

Segundo Compagno (2005), os IDS (*Intrusion Detection System*) surgiram há aproximadamente 20 anos e vários modelos foram propostos desde então. De forma simplificada, os sistemas de detecção de intrusão podem ser considerados evolução, ou mesmo automatização, da auditoria inicialmente praticada em sistemas de computação que visava encontrar eventos que não se enquadravam em atividades normais. No principio, as informações analisadas provinham de registros de atividades (*logs*) de sistemas, principalmente sistemas operacionais. Quando eventos de atividade anormal eram identificados, tinham suas características registradas em três categorias de informação:

- Autoria ou contabilidade: o que causou a brecha de segurança;
- Levantamento de danos: o que foi executado para gerar o dano;
- Recuperação de danos: passos necessários para recuperar os danos.

Em geral, os sistemas de detecção de intrusão são formados por três componentes básicos listados a seguir e representados na figura 6:

- Fonte de informação, que fornece registro de eventos;
- Mecanismo de análise, que monitora a ocorrência de ataques;

- Mecanismo de resposta, que gera reações baseadas em resultados obtidos no mecanismo de análise.

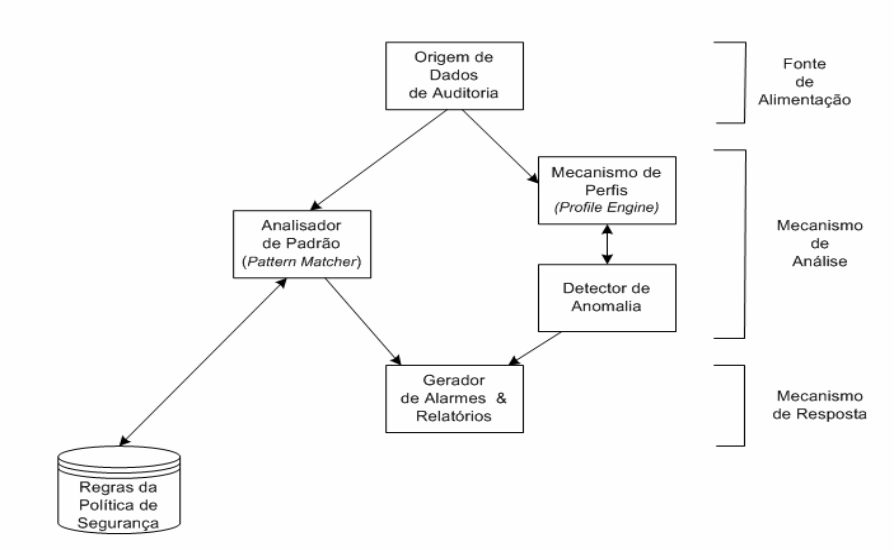


Figura 6: Arquitetura típica de um sistema de detectação de intrusos
Fonte: COMPAGNO (2005)

3.4.4 Certificação Digital

Basicamente é um método de criptografia que permite que se identifique corretamente qualquer pessoa física ou entidade jurídica; permitindo que se tenha certeza de que uma pessoa ou uma entidade é realmente quem diz ser. O Certificado Digital é um documento eletrônico, “assinado” digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo, servidor) a uma chave pública. Um certificado digital contém os dados de seu titular, tais como nome, e-mail, CPF, chave pública, nome e assinatura da autoridade certificadora que o emitiu. Desta maneira busca dar a quem o recebe a certeza da identidade de quem o enviou. Isso garante que qualquer conteúdo eletrônico que tenha sido assinado digitalmente por determinada pessoa ou entidade tenha garantida a autenticidade de origem (CARUSO e STEFFEN, 1999).

Para Caruso e Steffen (1999), a finalidade do certificado digital é fazer com que cada pacote de dados que trafegue pela Internet, em qualquer de suas formas (transações, voz, documentos eletrônicos ou quaisquer outras informações), se

transforme em um documento autenticado e com “firma reconhecida”, a exemplo do que ocorre no mundo real. Em termos humanos, é a célula de identidade das informações e dos processos.

3.4.5 Desativação do DHCP

É importante manter o DHCP (*Dynamic Host Configuration Protocol*) desativado, pois, quando um usuário se conecta à rede, não precisa fornecer credenciais para obter uma concessão. Um usuário não autenticado pode, portanto, obter uma concessão para que qualquer cliente DHCP sempre que um servidor DHCP estiver disponível para fornecer uma concessão. Quaisquer valores de opção que o servidor DHCP forneça com a concessão, como endereços IP de servidor WINS (*Windows Internet Name Service*) ou DNS (*Domain Name System*), estarão disponíveis para o usuário não autenticado. Se o cliente DHCP for identificado como membro de uma classe de usuário ou classe fornecedor, as opções associadas à classe também estarão disponíveis (MICROSOFT, 2008).

3.4.6 Filtragem de Pacotes TCP/IP

Segundo Comer (2007), um filtro de pacote opera examinando campos no cabeçalho de cada pacote. O filtro pode ser configurado para especificar quais campos do cabeçalho examinar e como interpretar os valores. Para o TCP/IP (*Transmission Control Protocol/Internet Protocol*), as especificações do filtro de pacotes geralmente incluem um tipo de quadro de 0800 (para o IP), um endereço de fonte IP ou um endereço de destino (ou ambos), um tipo de datagrama e um número de porta de protocolo. Por exemplo, um filtro de pacotes pode permitir o tráfego TCP de qualquer endereço IP para a porta 80 em um endereço de IP particular. A habilidade de permitir pacotes seletivamente para um serviço particular significa que o gerenciador pode permitir o tráfego para um serviço, enquanto bloqueia o tráfego

para outros (por exemplo, permitindo o tráfego Web enquanto bloqueia o tráfego para serviços como o *e-mail*).

3.5 Ferramentas de invasão

As redes Wireless e os pontos de acesso *(Access points*) são os alvos para se realizar o *War-Driving* (ação de procurar redes *wireless* enquanto está em movimento em um veículo ou mesmo a pé, utilizando dispositivos móveis*)*. O *War-Driving* pode ser utilizado como uma configuração simples de um *notebook* ou uma placa sem fio. Hoje em dia, é uma configuração mais moderna, que pode usar tipos de antenas poderosas, placas sem fio e dispositivos de computação do tamanho da palma da mão, incluindo os populares iPAQ e Palm. É usado o termo "*War-Driving*" livremente no âmbito da metodologia de invasão e principalmente porque você não precisa estar dirigindo. Pode estar andando por um parque tecnológico, pelo centro da cidade ou simplesmente pelos corredores do seu próprio prédio com seu *notebook*, se estiver fazendo uma auditoria interna (KURTZ, 2003).

3.5.1 AiroPeek NX

Uma das ferramentas de monitoração e análise 802.11 é o AiroPeek NX, segundo Kurtz (2003), esta ferramenta oferece suporte para placas 802.11b Lucent e Cisco, além de algumas das placas 802.11 mais recentes. O AiroPeek NX foi criado principalmente para o diagnóstico e a análise de redes sem fio, mas também possui algumas opções de segurança amigáveis.

Kurtz (2003), ainda afirma que o AiroPeek NX tem suporte para varredura de canais em um intervalo definido pelo usuário, além de decifração de tráfego no alto, com uma chave WEP fornecida. A filtragem do AiroPeek NX também é muito fácil de configurar, e você pode salvar combinações de filtro em arquivos de modelo. Isso lhe dará a capacidade de alternar rapidamente entre grupos de filtros que podem ser

usados para descoberta de rede e outros grupos que você pode usar para análise minuciosa. O AiroPeek NX também oferece um modo de exibição de nós útil, que agrupa estações detectadas por seu endereço MAC e também mostra endereços IP e protocolos observados para cada um. O modo de exibição de mapa de pares (Peer Map) apresenta uma matriz de todos os hosts descobertos na rede por suas conexões entre si. Isso pode facilitar bastante a visualização dos relacionamentos entro ponto de acesso e cliente.

3.5.2 AirSnort

Para Kurtz (2003), a ferramenta AirSnort é uma coleção de *scripts* e programas derivados da pesquisa realizada por Tim Newsham, da universidade de Maryland, e da Universidade da Califórnia em Berkeley. Essa com certeza é a ferramenta Linux mais popular e mais conhecida no setor, usada especificamente para decifração de pacotes sem fio. Originalmente, ela era a ferramenta da linha de comandos baseada no Linux que simplesmente capturava pacotes sem fio 802.11b e tentava decifrar os pacotes por meio da falha do vetor de inicialização. Desde então, ela evoluiu para incluir uma GUI (*Graphical User Interface*), permitindo a configuração rápida do canal a varrer e a capacidade de especificar a força da chave WEP.

3.5.3 Kismet

Esta ferramenta funciona como um detector de rede sem fio 802.11, *sniffer* (monitora o tráfego da rede), e sistema de detectação e intrusão. O Kismet funcionará com qualquer placa Wireless que suporta modo de monitoramento, e pode encontrar os padrões 802.11b, 802.11a, 802.11g e tráfego 802.11n. Ele também é composto de uma arquitetura de *plugins* que permitem adicionais 802.11 e protocolos a serem decodificados. Ele identifica redes passivamente por recolher pacotes, o que lhe permite detectar de redes ocultas (KISMET, 2009).

3.5.4 Aircrack-ng

Aircrack-ng é um pacote de ferramentas que permite recuperar senhas de redes WEP (*Wired Equivalent Privacy*), WPA e WPA2-PSK, ou seja, aquelas que se conectam sem fio. O funcionamento do programa é muito simples: os pacotes que circulam pela rede analisada são capturados e, já obtidos, se fazem ataques de recuperação convencionais, como a força bruta, o uso de um dicionário de chaves mais populares, etc. O tempo que demora Aircrack-ng em recuperar uma senha varia conforme ao tipo de senha utilizada e ao potencial de *hardware* do usuário. Contudo, na maioria dos casos, o processo é muito rápido e eficaz (AIRCRACK-NG.ORG, 2009).

Juntamente com o Aircrack, são utilizadas outras de suas ferramentas complementares para que se consiga encontrar a chave Wireless, entre elas estão: airdecap-ng (descriptografa arquivos capturados com criptografia WEP ou WPA com a chave conhecida); airmon-ng (coloca placas diferentes em modo monitor); aireplay-ng (injeção de pacotes); airodump-ng (coloca tráfego do ar em um “arquivo .cap” e mostra informação das redes), a figura 7 demonstra que a chave foi encontrada após todos os passos (AIRCRACK-NG.ORG, 2009).

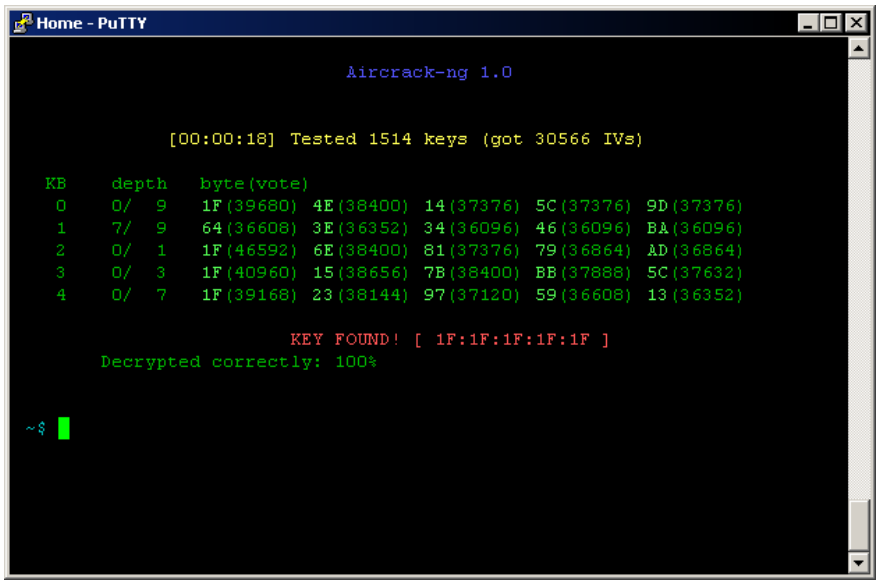


Figura 7: Desencriptação pelo aircrack-ng
Fonte: AIRCRACK-NR.ORG (2009)

3.5.5 Linux

Do ponto de vista geral, o Linux é simplesmente um sistema operacional. Esta definição não está errada, mas também não está completa. Na verdade, o Linux é parte de um todo, mais precisamente, é um kernel de código-fonte aberto, que foi e é desenvolvido ao longo do tempo graças à colaboração voluntária de desenvolvedores de várias partes do mundo.

Para Alecrim (2011), o Kernel pode ser entendido como o núcleo do sistema operacional, isto é, como a parte essencial deste. Cabe ao kernel fazer o intermédio entre o hardware e os programas executados pelo computador. Isso significa que a junção do kernel mais os softwares que tornam o computador usável (drivers, protocolos de comunicação, entre outros), de acordo com a sua aplicação, é que formam o sistema operacional em si.

Perceba que o kernel não é, necessariamente, um software manipulável pelo usuário. Ou seja, não se trata de algo tão simples a ponto de poder ser instalado e, logo em seguida, estar pronto para uso, como um programa de edição de textos, por exemplo. O kernel é uma base complexa, que serve de estrutura para o sistema, atuando por de trás. Assim, o usuário sequer precisa saber de sua existência para poder utilizar o computador (ALECRIM, 2011).

3.5.6 Máquina Virtual

Máquinas virtuais são “computadores virtuais” que rodam dentro do computador “físico”. A máquina virtual é criada por um programa que é instalado, como qualquer outro. Nesse programa, pode-se criar um disco rígido virtual e também executar um sistema a partir deste disco, sem a necessidade de reparticionar o disco “físico” verdadeiro. A máquina virtual alocará, durante a execução, uma quantidade definida de memória RAM, podendo essa também ser alterada (ALTIERES, 2009).

3.6 Políticas de Segurança

As Políticas de Segurança da Informação são um conjunto de normas e diretrizes que procuram melhorar a utilização de todo o ambiente da tecnologia da informação. É composta por regras que todos devem respeitar, assim, assegurando que no descumprimento, penalizações serão aplicadas (GUIMARAES, LINS e OLIVEIRA, 2006).

Em redes de computadores, a política de segurança visa controlar o tráfego da rede e de sua utilização, descreve o que é permitido e o que é proibido nesta infraestrutura ou em um sistema. Identifica os recursos e as possíveis ameaças desta rede. Define usos e responsabilidades e detalha os planos de ação destinados a situações que ocorram violações. Portanto, a política deve ser utilizada de maneira estratégica estabelecendo limites na rede. Basicamente existem dois modelos de política de segurança: a proibitiva, onde tudo que não é expressamente permitido é proibido e a permissiva, onde tudo que não é expressamente proibido é permitido (GUIMARAES, LINS e OLIVEIRA, 2006).

4 METODOLOGIA

Foram realizadas pesquisas bibliográficas em livros na área de computação, internet, monografias e artigos científicos, após estas, foram descritos os conteúdos e tomado o assunto. Este trabalho visa verificar possíveis vulnerabilidades em redes sem fio, explorar essas falhas para invadir uma rede da qual não se tem acesso. Então foi criada uma lista de procedimentos, também conhecidos como políticas de segurança para manter a rede mais segura e tentar ao máximo evitar futuras invasões.

Logo após foram feitos testes de detectação, captura de endereço MAC do roteador, captura de pacotes e armazenamento de uma rede sem fio doméstica para verificar o funcionamento e o reconhecimento do *hardware*, os testes foram feitos com um notebook rodando uma maquina virtual (Vmware) na qual foi instalado Linux Debbi e a ferramenta Aircrack-ng, juntamente com um receptor wireless USB com opção para modo de monitoramento.

O intuito foi utilizar a ferramenta Aircrack-ng para encontrar redes e seus respectivos endereços MAC, para isso são utilizadas as extensões airmon-ng para ativar o modo monitoramento de seu receptor e o airodump-ng, que usa os endereços encontrados para se capturar pacotes da rede e estes pacotes serão gravados em um arquivo .cap, após isto, será utilizada a extensão aireplay-ng com a função de fazer a associação entre o roteador wireless e o receptor para habilitar a captura dos pacotes. Após capturar um número elevado de pacotes, se ativa a extensão aircrack-ng juntamente com o arquivo .cap gerado, estes farão juntos o reconhecimento e descriptografia da chave da rede.

Após a realização de todos os procedimentos antes citados e receber como resultado a falha existente na rede, é iniciado à fase final do trabalho, onde será criada a lista de políticas de segurança a partir do que foi visto no decorrer dos testes na rede, juntamente com pesquisas em livros, artigos e na internet, gerando regras para que esta seja uma rede consistente e mais confiável possível.

5 RESULTADOS

Diante dos estudos bibliográficos e dos testes realizados, foram obtidos os resultados sobre as vulnerabilidades dos seguintes protocolos:

WEP

Foi o primeiro protocolo criado, por isso, apresenta muitas vulnerabilidades por causa da utilização do algoritmo criptográfico RC4 com chaves de 64 bits (40 reais) e 128 bits (104 reais) para cifrar os pacotes trocados entre o ponto de acesso e o cliente. Todos os clientes usam a mesma chave criptográfica, aumentando assim o volume de dados para um atacante realizar ataques sobre a mesma chave. Portanto, se torna mais fácil a desencriptação da sua chave de segurança, sendo quebrada com programas maliciosos e sem a necessidade de bibliotecas de caracteres ou outros recursos como no caso dos outros protocolos. Nos testes realizados foi possível descriptografar a chave utilizando o aircrack-ng.

Na Figura 8, foi possível ver que a rede foi encontrada através do modo de monitoramento do receptor wireless e a utilização do comando airodump-ng.

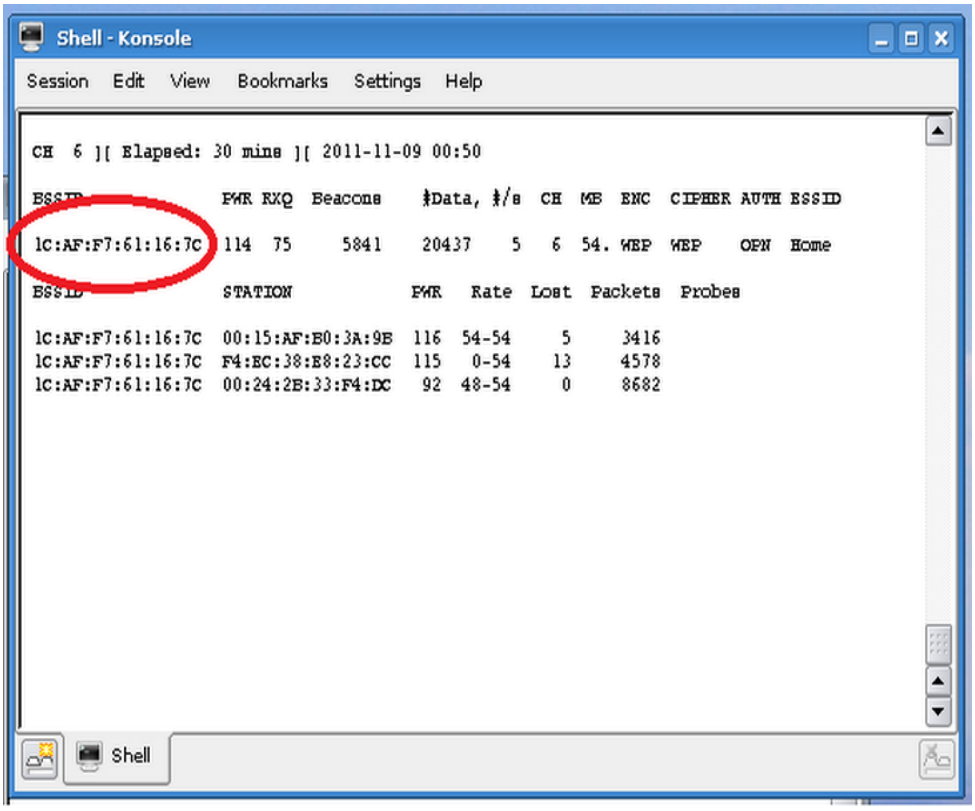


Figura 8: Rede encontrada através do receptor em modo monitoramento

Na Figura 9, foi visto que utilizando o comando aireplay-ng foi possível conseguir a autenticação entre o roteador e o receptor, e utilizando o mesmo comando para começa a injetar e ler pacotes da rede.

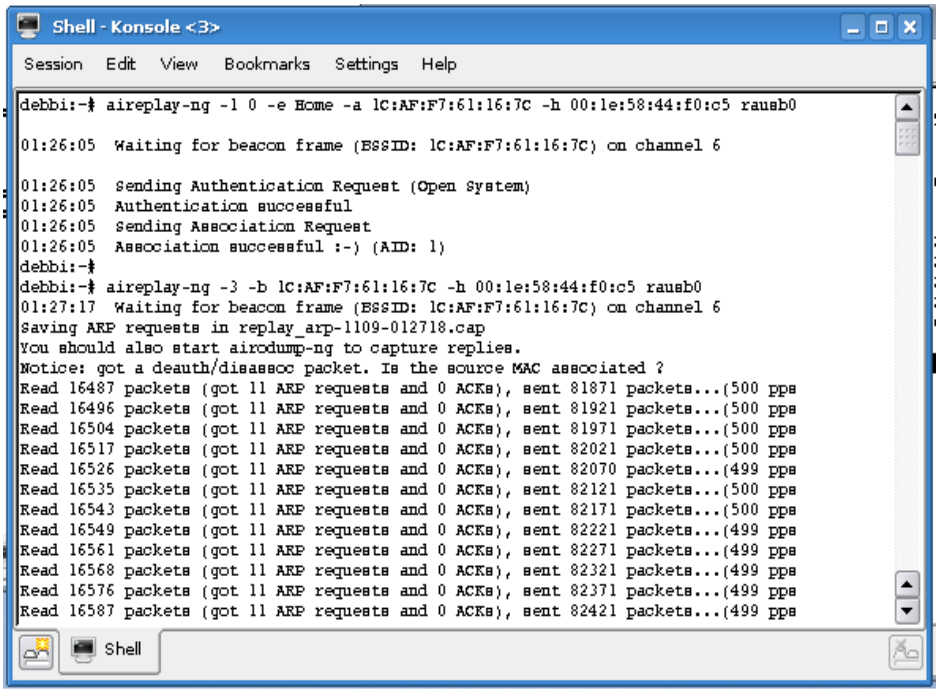


Figura 9: Autenticação e captura de pacotes

A Figura 10 mostra o comando aircrack-ng em funcionamento e a descoberta da chave da rede.

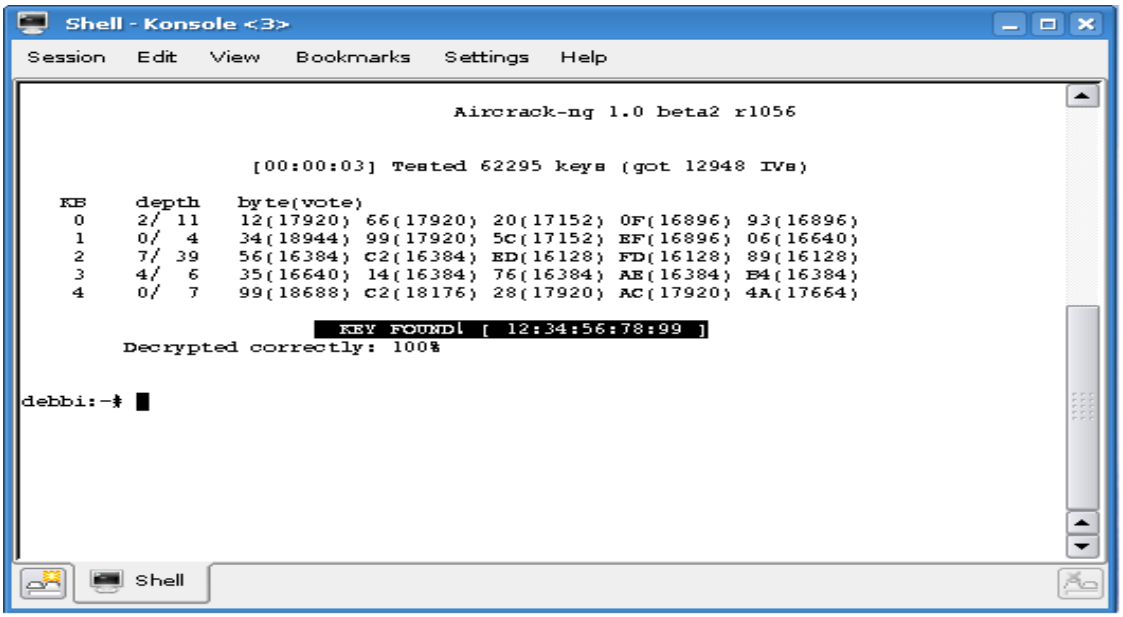


Figura 10: Chave encontrada

Diferente da WEP, este protocolo utilizada o TKIP (Protocolo de integridade de chaves temporárias), onde enquanto o WEP tem sua criptografia RC4 estática e utiliza sempre à mesma chave, este protocolo gera chaves temporárias dinamicamente, portanto, para a quebra seria necessário utilizar listas de caracteres para se tentar obter a chave.

Justamente por utilizar uma criptografia dinâmica, nos testes de invasão realizados para quebra de chaves dos protocolos, não foi possível obter a chave do WPA.

Portanto é recomendável que usuários de redes sem fio adotem políticas de segurança, para que suas informações não fiquem expostas a pessoas mal-intencionadas.

Lista com Políticas e Práticas de Segurança recomendadas:

- Definição de quem está autorizado a instalar novos APs (pontos de acesso) no local;
- Definição de quem está autorizado a utilizar a rede sem fio;
- Prever ações no caso de roubo de algum dos equipamentos da rede sem fio;
- Definir qual o tipo de informações poderão transitar na rede;
- Colocar os APs em um segmento de rede próprio e utilizar um firewall entre esse segmento e o resto da infraestrutura;
- Utilizar uma ferramenta de detectação de intrusos;
- Definir uma criptografia e mecanismos de autenticação na rede;
- Alterar o SSID (nome da rede) que vem padrão de fábrica dos APs;
- Entre os protocolos como o HTTP, SNMP, Telnet, etc. Desabilitar os que não estiverem sendo utilizados;
- Desabilitar o broadcast (transmissão) de SSID pelo AP;
- Utilizar o recurso de filtragem por endereço MAC;
- Fazer atualizações do *firmware* do AP sempre que disponível;

➢ Senhas:

- Comprimento mínimo de 8 caracteres;
- Formada por letras, números e caracteres especiais;
- Não ser criada a partir de dados pessoais, tais como nomes de membros da família, números de telefone, placas de carros, números de documentos e datas;
- Não ser baseada em preferências pessoais (time para o qual torce, escritor, ator ou cantor favorito, nomes de livros, filmes ou músicas, etc.);
- Palavras diferentes das que estão presentes em dicionários (de português ou de outros idiomas).

6 CONSIDERAÇÕES FINAIS

Neste trabalho, foi demonstrado que se pode utilizar a partir das vulnerabilidades no protocolo WEP de segurança das redes sem fio, a invasão nesta rede se aproveitando de algumas falhas cruciais que consequentemente possibilitaram a captura e obtenção das senhas, permitindo assim o acesso indevido às redes de testes citadas.

Foram abordadas também ferramentas e métodos como habilitar a filtragem de endereço MAC, desabilitar a transmissão do nome da rede e outros, que se tornaram importantes aliados contra ataques em redes sem fio.

Nesse contexto, esse estudo possibilitou a escolha e formulação de políticas de segurança, podendo citar pontos e modelos que devem ser obedecidos e assim não tornem um possível ataque as redes sem fio algo fácil de ser realizado, como exemplos pode-se citar o uso de *firewalls*, reconhecimento de endereço MAC, senha com alto nível de dificuldade (utilizando letras maiúsculas e minúsculas juntamente com números e caracteres especiais), podendo também usar de preferência como protocolo de segurança o WPA ou WPA2 que são mais seguros que o WEP, pois utilizam um algoritmo de criptografia mais complexo e não utilizam chave estática.

Portanto, é válido afirmar a importância do estudo constante para criar segurança às redes sem fio, já que o mesmo é feito para que estas sejam violadas por pessoas que estejam mal intencionadas buscando assim falhas ou vulnerabilidade.

REFERÊNCIAS

AGUIAR, P.A. F. **Segurança em Redes WI-FI.** Montes Claros, MG. Universidade Estadual de Montes Claros, 2005, 79p. Monografia defendida para obtenção do grau de Bacharel em Sistemas de Informação.

AIRCRACK-NG. **Description.** 2009. Disponível na Internet: <http://www.aircrack-ng.org/>. Acessado em: 11/05/2011.

ALECRIM, E. **O que é Linux e qual sua história**. 2011. Disponível na Internet: <http://www.infowester.com/historia_linux.php> Acessado em: 25/06/2012.

ALTIERES, R. **Saiba o que são máquinas virtuais e como elas ajudam na segurança do PC**. 2009. Disponível na Internet: < http://g1.globo.com/Noticias/Tecnologia/0,,MUL1252543-6174,00-SAIBA+O+QUE+SAO+MAQUINAS+VIRTUAIS+E+COMO+ELAS+AJUDAM+NA+SEGURANCA+DO+PC.html> Acessado em: 25/06/2012.

ANTONIO, J. **Informática Para Concursos.** 4ª ed.: Nacional. Ed: Campus, 2008. 768p.

BARBOZA, D. H. **Acesso Seguro à Redes Móveis IP**. Campinas, SP. Universidade Estadual de Campinas, 2008, 82p. Dissertação apresentada para obtenção de grau de mestre em Engenharia Elétrica.

CARLOS, A. A. C. ; STEFFEN, F. **Segurança em Informática e de Informações**. 2ª ed.: Nacional. Ed: Senac, 1999. 367p.

CHAVES. L. J. **Um Mecanismo Cognitivo para Adaptação Automática da Taxa de Transmissão em Redes IEEE 802.11**. Campinas, SP. Universal Estadual, 2010, 115p. Dissertação apresentada para obtenção de grau de mestre em Ciência da Computação.

COMER, E. D. **Redes de Computadores e Internet.** 1ª ed. Nacional. Ed: Bookman. 2007. 632p.

COMPAGNO, R. **Geração Automáticas de Políticas para Detecção de Intrusões Baseadas em Evidências de Ataque**. Campinas, SP. Universidade Estadual de Campinas, 2005, 121p. Monografia defendida para obtenção do grau de mestre em computação na área de redes de computadores.

CORRÊA JÚNIOR, M. A. C. **Evolução da Segurança em Redes Sem Fio**.Recife, PE. Universidade Federal de Pernambuco, 2008, 77p. Monografia defendida para obtenção do grau em Ciência da Computação.

FOROUZAN, A. B. **Comunicação de Dados e Redes de Computadores**. 4ª ed. Nacional. Ed: Mcgraw-Hill Brasil, 2008. 1168p.

GUIMARAES, A. G. ; LINS, R. D. ; OLIVEIRA, R. C. **Segurança em Redes Privadas Virtuais – VPNs**. 1ª ed. Nacional. Ed: Brasport, 2006. 232p.

JARDIM, F. M. **Treinamento Avançado em Redes Wireless**. 1ª ed.: São Paulo. Ed: Digerati Books, 2007. 128p.

KISMET. **Documentation.** 2009. Disponível na Internet: <http://www.kismetwireless.net/>. Acessado em: 11/05/2011.

KURTZ, G. **Hackers Expostos:** Segredos e Soluções para a Segurança de Redes. 4ª ed. Ed: Makron Books, 2003. 510p.

MENEZES, R. S. **IEEE 802.11 – Wireless.** 2004. Disponível na Internet: <http://www.gta.ufrj.br/grad/98_2/rodrigo/trabalho.html>. Acessado em: 11/05/2011.

MICROSOFT. **Informações de Segurança do DHCP.** Disponivel na Internet: <http://technet.microsoft.com/pt-br/library/cc780347(WS.10).aspx>. Acessado em: 01/06/2011

MOHER, M. ; HAYKIN, S. **Sistemas Modernos de Comunicação Wireless**. 1ª ed. Ed: Bookman, 2008. 580p.

MORAZ, E. **Treinamento Profissional Anti-Hacker**. 1ª ed.: Nacional. Ed: Digerati Editorial, 2006. 128p.

NELSON, M. **Segurança em Redes Sem Fio.** 2003.Disponível na Internet: <ftp://ftp.registro.br/pub/gts/gts0103/nelson-murilo-wireless-gts2003.pdf>. Acessado em: 19/04/2011.

PARIHAR, M. , et al. **TCP/IP:** A Bíblia. 1ª ed. Nacional. Ed: Campus, 2002. 664p.

PEREIRA, H. B. **Segurança em Redes Wireless 802.11 Infra-estruturadas**. Lavras, MG. Universidade Federal de Lavras, 16p. Trabalho para conclusão de especialização em administração de redes Linux.

ROSS, J. **Rede de Computadores**. 1ª ed. Nacional. Ed: Antenna Edições Técnicas, 2008. 148p.

RUFINO, N.M.O. **Segurança em Redes sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**.** São Paulo, SP. Ed: Novatec, 2005. 224p.

SANTOS, A. **Quem Mexeu no Meu Sistema?**. 1ª ed. Nacional. Ed: Brasport, 2008. 212p.

SANTOS, T. C. **Análise de Desempenho de Transmissão de Vídeo em Redes IEEE 802.11 visando a Estruturação de Canais de Retorno para TV Digital**. Campinas, SP. Universidade Estadual de Campinas, 2008, 91p. Monografia defendida para obtenção do grau de mestre em Engenharia Elétrica.

TANENBAUM, A. S. **Rede de Computadores**. 4ª ed. Nacional. Ed: Campus, 2003. 955p.

APENDICE A

Segurança para Evitar Ataques as Redes Sem Fio

Kleber B. Amaral[1], Wiliam C. Galvão[1], Henrique P. Martins[1], Élvio G. Silva[1]

[1]Centro de Ciências Exatas e Aplicadas – Universidade Sagrado Coração (USC)

Bauru, SP – Brasil

Abstract. *The increase of wireless networks today are obvious, the facility and mobility that is generated fell into the graces of everyone, both the corporate and home networks are using this technology in their computer networks. But is necessary that you be alert of the weaknesses and vulnerabilities that come with it, several methods are used by hackers to break into and steal data, and to prevent it, you should take precautions and use what technology offers us to keep security intact. By capturing signals of wireless networks, people with knowledge can use specific tools to cheat security and gain access to private network, at the risk of copying important data and cause damage to companies and people, there is a need to implement rules security to prevent this from happening.*

Resumo. *O crescimento das redes wireless nos dias de hoje estão claras, a facilidade e mobilidade que está gerou caíram nas graças de todos, tanto as redes domésticas quanto as empresariais estão utilizando está tecnologia em suas redes de computadores. Mas é necessário ficar atento as fraquezas e vulnerabilidades que surgem junto a ela, vários métodos são utilizados por hackers para invadir e roubar dados, e para que isso seja evitado, devem-se tomar precauções e utilizar o que a tecnologia nos oferece para manter a segurança intacta. Através de captação de sinais de redes sem fio, pessoas com conhecimento podem utilizar ferramentas especificas para burlar a segurança e obter acesso a está rede privada, correndo o risco de copiar dados importantes e causar prejuízos a empresas e pessoas, existe a necessidade de implementar regras de segurança para que isso não ocorra.*

1. Introdução

A tecnologia hoje atingiu um grau de disseminação na sociedade que faz com que esteja presente em todas as áreas do trabalho e também ate nas áreas do entretenimento. Esse crescimento fez com que as pessoas precisem se conectar em redes em qualquer lugar a qualquer hora. O princípio de funcionamento do Wireless se baseia na transmissão de dados através da camada atmosférica utilizando a propagação das ondas eletromagnéticas com caminho entre o transmissor e o receptor (ROSS, 2008).

As redes baseadas em *Wireless* combinam conectividade e mobilidade, pôr parte de seus usuários, assim como simplicidade em sua configuração. Nos últimos sete anos esse tipo de rede tem crescido e tem ganhado popularidade nos diversos setores, principalmente no que diz respeito as WLAN (*Wireless Local Area Network*) (MENEZES, 2004).

Com o intuito de garantir a privacidade da comunicação entre os clientes e os pontos de acesso foi desenvolvido o protocolo WEP. A base de funcionamento do WEP é a utilização do algoritmo criptográfico RC4 com chaves de 40 bits para cifrar os pacotes trocados entre o ponto de acesso e o cliente, de maneira que a informação não pudesse ser recebida por outro cliente qualquer que não tivesse a chave criptográfica (BARBOZA, 2008).

A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida somente pelo seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade (SANTOS, 2008).

O algoritmo RC4 utilizado no WEP mostrou-se fraco, podendo ser quebrado facilmente com o hardware disponível hoje. A sua função de detecção de erros é linear, tornando possível adulterar pacotes cifrados sem saber a chave RC4. Além disso, existem outras características que comprometem a segurança: todos os clientes usam a mesma chave criptográfica, aumentando assim o volume de dados para um atacante realizar ataques sobre a mesma chave. Finalmente, diversas ferramentas conseguem quebrar a segurança de uma rede WEP em cerca de minutos, explorando as falhas de segurança que o protocolo apresenta (BARBOZA, 2008).

O objetivo é realizar testes de invasões em redes sem fio e obter a senha utilizada, para isso serão feitas as invasões em cima de falhas no algoritmo de criptografia dos protocolos utilizados.

Primeiramente serão capturadas e analisadas as possíveis redes sem fio existentes, após isto, analisar as vulnerabilidades encontradas.

Após está primeira fase, juntamente com ferramentas próprias, como o *aircrack-ng*, poderemos obter o acesso na rede, simulando ataques onde serão lidos e gravados pacotes de dados para se conseguir a chave da mesma.

2. Revisão Bibliográfica

Quase na mesma época em que surgiram os *notebooks*, muitas pessoas sonhavam com o dia em que entrariam em um escritório e magicamente seu *notebook* se conectaria a Internet. Em conseqüência disso, diversos grupos começaram a trabalhar para descobrir maneiras de alcançar esse objetivo. A abordagem mais prática é equipar o escritório e os *notebooks* com transmissores e receptores de rádio de ondas curtas para permitir a comunicação entre eles. Esse trabalho levou rapidamente à comercialização de LANs sem fios por várias empresas (TANENBAUM, 2003).

O problema era encontrar duas delas que fossem compatíveis. Essa proliferação de padrões significava que um computador equipado com um rádio da marca X não funcionaria em uma sala equipada com uma estação base da marca Y. Finalmente, a indústria decidiu que um padrão de LAN sem fio poderia ser uma boa idéia, e assim o comitê do IEEE que padronizou as LANs sem fios recebeu a tarefa de elaborar um padrão de LANs sem fios. O padrão recebeu o nome 118802.11. Um apelido comum para ele é *Wi-Fi*. Trata-se de um padrão importante e que merece respeito, e assim vamos chamá-lo por seu nome correto, 802.11 (TANENBAUM, 2003).

A partir deste padrão se criou os modelos mais utilizados hoje, o padrão b, a e g, e segundo Rufino (2005), existem novos padrões que estão surgindo, como o 802.11n, também conhecido como WWiSE (*World Wide Spectrum Efficiency*), este é um padrão em desenvolvimento, cujo foco principal é o aumento da velocidade (cerca de 100 a 500 Mbps), a figura 4 demonstra a evolução dos padrões. Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM (*Orthogonal Frequency-Division Multiplexing*), conhecida como MIMO-OFDM (*Multiple Input, Multiple Out-OFDM*). Outra Característica deste padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 Mhz, também, manter compatibilidade com os 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135 Mbps.

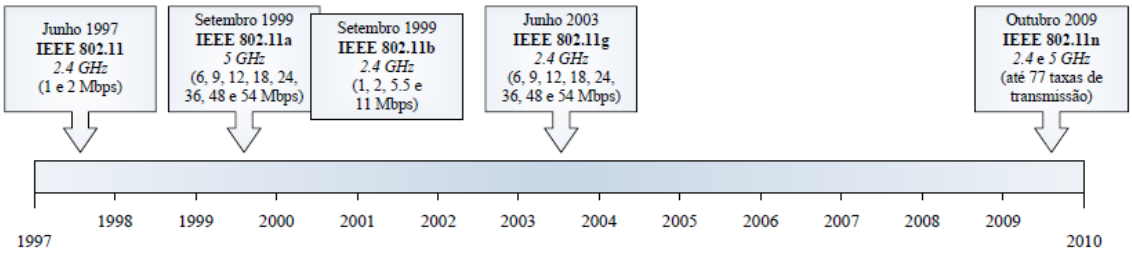


Figura 4 : Evolução do padrão 802.11 ao longo dos anos

Fonte: CHAVES (2010) apud MCCANN (2010)

Surgiu então a necessidade da criação de protocolos de segurança para esses padrões, Moraz (2006) explica que o primeiro protocolo a ser implementado para criptografar os pacotes de dados transitados em uma rede wireless foi o WEP (Wireless Equivalence Privacy). O WEP utiliza um algoritmo de criptografia de chave simétrica (RC4), entre 40 e 104 bits. Na verdade, as chaves enviadas acabam sendo de 64 e 128 bits, por possuírem 24 bits adicionais referentes ao vetor de inicialização do protocolo WEP. Ou seja, as chaves passam a ser de 40+24 bits e 104+24 bits, conhecidos respectivamente como 64 e 128 bits, ou WEP e WEP2.

O algoritmo RC4 utilizado pelo WEP determina uma alteração periódica de parte da chave (24 bits), dificultando a quebra desta por algum programa que possa agir como um sniffer. Todavia, essa troca possui um tempo de vida máximo, ou seja, em determinado instante, após algumas horas, essa chave se repete. Esse é o principal ponto fraco do protocolo WEP (MONAZ, 2006).

Por isso foi necessária a criação de outro protocolo, daí surgiu o WPA, Barboza (2008) diz que dentre os diversos avanços do WPA em relação ao WEP, destacamos o TKIP (*Temporal Key Integrity Protocol*). Este protocolo foi elaborado com o intuito de ser o mais compatível possível com o WEP, de maneira que não fosse necessária a troca dos dispositivos de rede Wi-Fi. Portanto ele continua a utilizar o RC4, usado no WEP e comprovadamente inseguro nos padrões de hoje. O que o torna mais seguro do que o WEP, dentre outros atributos, é a checagem de integridade da mensagem e redistribuição de chaves. No WEP, é possível alterar o conteúdo de um pacote cujo conteúdo fosse conhecido, mesmo sem decifrá-lo. Isto não acontece com o TKIP, pois sua verificação de integridade de mensagens cobre este caso. A redistribuição de chaves faz com que um atacante tenha menos dados decifrados com uma mesma chave para tentar algum tipo de ataque, pois a chave de cifragem usada por um dispositivo móvel é trocada periodicamente.

3. Metodologia

Foram realizadas pesquisas bibliográficas em livros na área de computação e na internet, após estas, foram descritos os conteúdos e tomado o assunto. Por fim, foram feitos testes em redes sem fio para se ter certeza do funcionamento, os testes foram feitos com um notebook rodando uma maquina virtual (Vmware) na qual foi instalado Linux Debbi e a ferramenta Aircrack-ng, juntamente com um receptor wireless USB com opção para modo de monitoramento.

O intuito é utilizar a ferramenta Aircrack-ng para encontrar redes e seus respectivos endereços MAC, para isso são utilizadas as extensões airmon-ng para ativar o modo monitoramento de seu receptor e o airodump-ng, que usa os endereços encontrados para se capturar pacotes da rede e estes pacotes serão gravados em um arquivo .cap, após isto, será utilizada a extensão aireplay-ng com a função de fazer a associação entre o roteador wireless e o receptor para habilitar a captura dos pacotes. Após capturar um número elevado de pacotes, se ativa a extensão aircrack-ng juntamente com o arquivo .cap gerado, estes farão juntos o reconhecimento e descriptografia da chave da rede.

4. Resultados

Diante dos estudos bibliográficos e dos testes realizados, foram obtidos os resultados sobre as vulnerabilidades dos seguintes protocolos:

WEP

Foi o primeiro protocolo criado, por isso, apresenta muitas vulnerabilidades por causa da utilização do algoritmo criptográfico RC4 com chaves de 64 bits (40 reais) e 128 bits (104 reais) para cifrar os pacotes trocados entre o ponto de acesso e o cliente. Todos os clientes usam a mesma chave criptográfica, aumentando assim o volume de dados para um atacante realizar ataques sobre a mesma chave. Portanto, se torna mais fácil a desencriptação da sua chave de segurança, sendo quebrada com programas maliciosos e sem a necessidade de bibliotecas de caracteres ou outros recursos como no caso dos outros protocolos. Nos testes realizados foi possível descriptografar a chave utilizando o aircrack-ng.

Na Figura 1, podemos ver que a rede foi encontrada através do modo de monitoramento do receptor wireless e a utilização do comando airodump-ng.

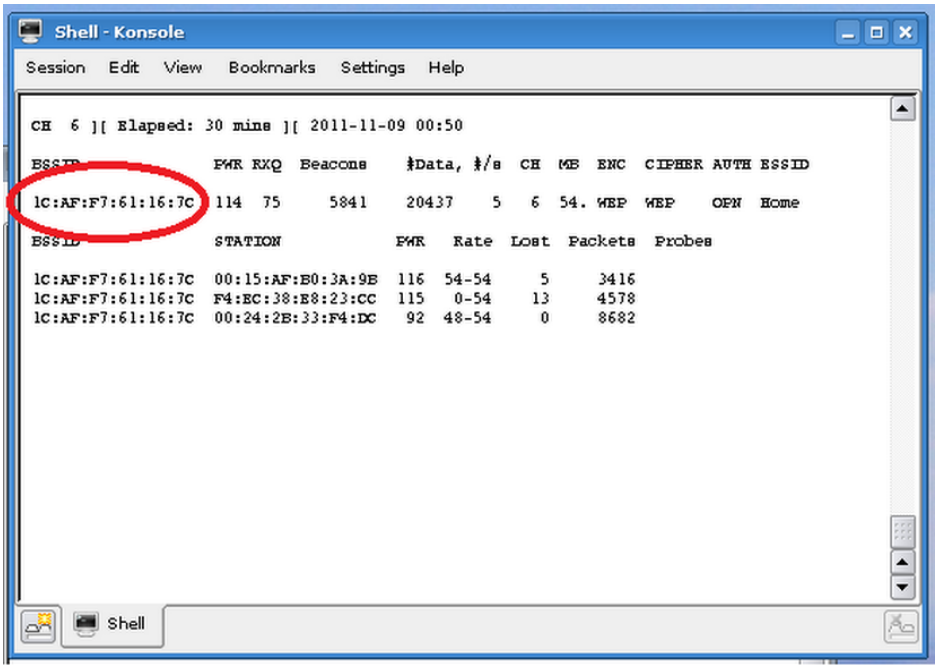


Figura 1. Rede encontrada através do receptor em modo monitoramento

Na Figura 2, pode ser visto que utilizando o comando aireplay-ng foi possível conseguir a autenticação entre o roteador e o receptor, e utilizando o mesmo comando se começa a injetar e ler pacotes da rede.

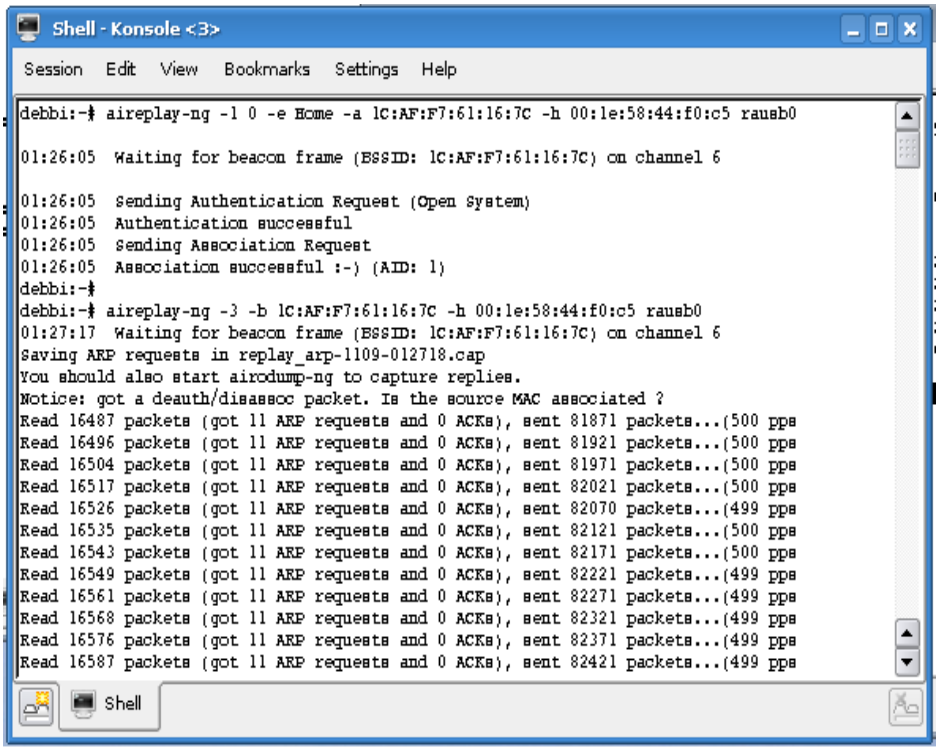


Figura 2. Autenticação e captura de pacotes

A Figura 3 mostra o comando aircrack-ng em funcionamento e a descoberta da chave da rede.

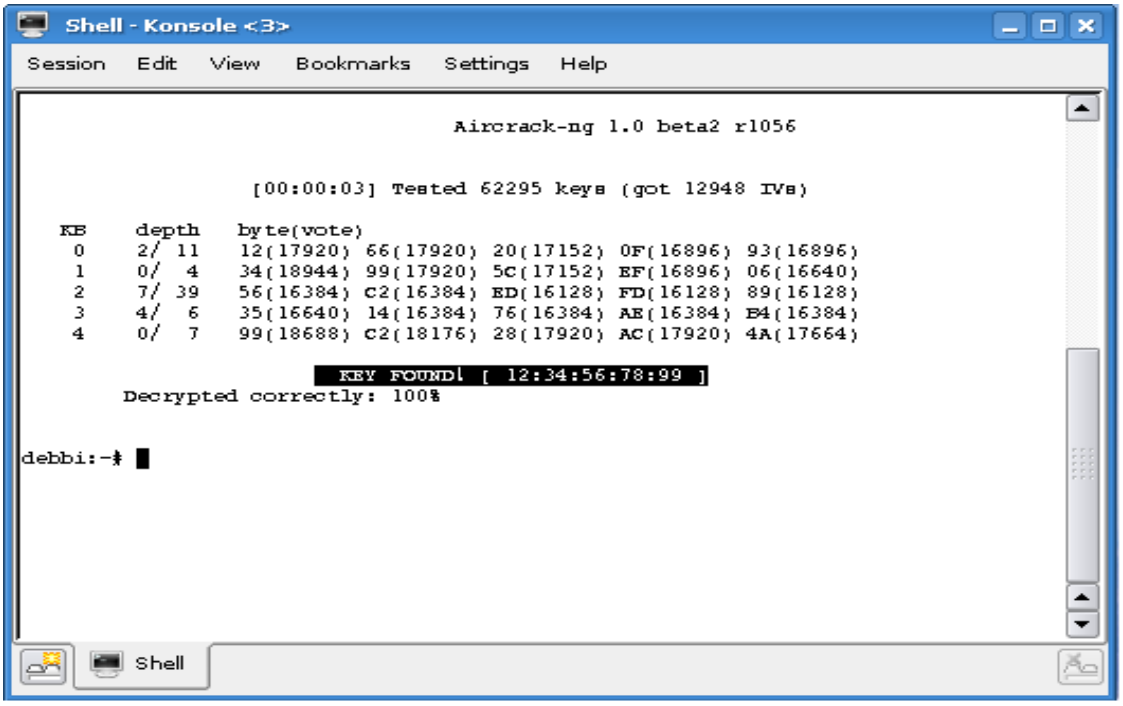


Figura 3. Chave encontrada

Diferente da WEP, este protocolo utilizada o TKIP (Protocolo de integridade de chaves temporárias), onde enquanto o WEP tem sua criptografia RC4 estática e utiliza sempre à mesma chave, este protocolo gera chaves temporárias dinamicamente, portanto, para a quebra seria necessário utilizar listas de caracteres para se tentar obter a chave.

Justamente por utilizar uma criptografia dinâmica, nos testes de invasão realizados para quebra de chaves dos protocolos, não foi possível obter a chave do WPA.

5. Considerações Finais

Neste trabalho, foi demonstrado que existem vulnerabilidades em alguns protocolos de seguranças das redes sem fio, com o propósito de que possam ocorrer melhorias para o futuro.

É importante a formulação de uma política de segurança, onde sejam citados pontos e regras que devem ser obedecidos e assim não tornem um possível ataque algo fácil de realizar, é importante a cada dia estudos para criar seguranças às redes sem fio, já que estudos para que estas sejam violadas são freqüentes por pessoas que estejam mal intencionadas.

Referências

BARBOZA, D. H. Acesso Seguro à Redes Móveis IP. Campinas, SP. Universidade Estadual de Campinas, 2008, 82p. Dissertação apresentada para obtenção de grau de mestre em Engenharia Elétrica.

CHAVES. L. J. Um Mecanismo Cognitivo para Adaptação Automática da Taxa de Transmissão em Redes IEEE 802.11. Campinas, SP. Universal Estadual, 2010, 115p. Dissertação apresentada para obtenção de grau de mestre em Ciência da Computação.

MENEZES, R. S. IEEE 802.11 – Wireless. 2004. Disponível na Internet: <http://www.gta.ufrj.br/grad/98_2/rodrigo/trabalho.html>. Acessado em: 11/05/2011.

MONAZ, E. Treinamento Profissional Anti-hacker. 1ª ed. Nacional. Ed: Digerati Editorial, 2006. 128p.

ROSS, J. Rede de Computadores. 1ª ed. Nacional. Ed: Antenna Edições Técnicas, 2008. 148p.

RUFINO, N.M.O. Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**.** São Paulo, SP. Ed: Novatec, 2005. 224p.

SANTOS, A. Quem Mexeu no Meu Sistema?. 1ª ed. Nacional. Ed: Brasport, 2008. 212p.

TANENBAUM, A. S. Rede de Computadores. 4ª ed. Nacional. Ed: Campus, 2003. 955p.