UNIVERSIDADE DO SAGRADO CORAÇÃO

ELBER CANO DA SILVA MIRANDA

ANÁLISE DA FRAGILIDADE DOS PROTOCOLOS DE SEGURANÇA EM REDE SEM FIO

BAURU
2016

ELBER CANO DA SILVA MIRANDA

ANÁLISE DA FRAGILIDADE DOS PROTOCOLOS DE SEGURANÇA EM REDE 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. Dr. Elvio Gilberto Da Silva.

BAURU
2016

Miranda, Elber Cano da Silva

M672a

Análise da fragilidade dos protocolos de segurança em rede sem fio / Elber Cano da Silva Miranda. -- 2016.

78f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

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

1. Redes de Computadores. 2. Redes sem fio. 3. Segurança de rede. 4. Kali Linux. 5. Wifi. I. Silva, Elvio Gilberto da.

ELBER CANO DA SILVA MIRANDA

ANÁLISE DA FRAGILIDADE DOS PROTOCOLOS DE SEGURANÇA EM REDE 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. Dr. Elvio Gilberto da Silva.

Banca examinadora:

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

_____
Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

Bauru, 6 de dezembro de 2016.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter abençoado todo este período, e por ter me guiado em todo o processo de elaboração deste trabalho.

Dedico todo esse esforço para minha esposa, aos meus familiares que me ajudaram e me apoiaram durante minha vida acadêmica e ao meu pai (in memoriam), meu maior exemplo.

Sou grato a todos os meus professores, em especial ao meu orientador Prof. Dr. Elvio Gilberto da Silva que me ajudou, corrigiu e me acompanhou durante toda esta pesquisa.

“ Você pode encarar um erro como uma besteira a ser esquecida, ou como um resultado que aponta uma nova direção. ” (Steve Jobs, 1998).

RESUMO

Redes Sem Fio estão sendo muito utilizadas e, com o aumento das vendas de computadores portáteis e celulares que suportam acesso à Internet, o número de usuários tende a aumentar ainda mais. Dentre os diversos padrões, destaca-se o IEEE 802.11, também conhecido como Wi-Fi. A ausência de um meio físico para a realizar a conexão entre os computadores traz diversas vantagens, como a mobilidade. Sem a necessidade cabos, qualquer dispositivo provido de uma placa de rede sem fio poderia se associar a um Ponto de Acesso, bastando apenas estar próximo dele. Para impedir usos indevidos, foram criados os protocolos de segurança que visam prover privacidade e controlar o acesso à rede. O primeiro a ser desenvolvido foi o WEP e, pouco tempo depois de sua criação, diversos estudos acusaram falhas graves em sua implementação. Surgiram então os protocolos WPA e WPA2 com o padrão 802.11i e, novamente, estudos que apontam falhas de segurança. Este projeto pretende, além de apresentar o padrão 802.11 e seus protocolos de segurança, analisar essas falhas, mostrar suas causas e apresentar resultados de testes utilizando a ferramenta Kali Linux, a fim de demonstrar na prática a possibilidade da quebra de senha e, consequentemente, uso não permitido da rede sem fio. Através da pesquisa e da análise dos testes, busca-se descobrir o que deve ser feito para impedir que usuários não autorizados se conectem à rede.

Palavras-chave: Redes de Computadores, Redes Sem Fio, IEEE 802.11, Segurança de Redes, WEP, WPA, WPA2, Kali Linux, Wi-Fi.

ABSTRACT

Wireless Networks are being widely used and, with the increase in sales of portable computers and cell phones with support to Internet access, the number of mobile users tends to increase even more. Among the various wireless standards, the IEEE 802.11, also known as Wi-Fi, stands. With the advent of wireless link to connect the computers comes many advantages, such as mobility. Without cables, any device equipped with a wireless network card is able to associate with an Access Point, just by being near it. To prevent misuse, security protocols, which are intended to provide privacy and network access control, were designed. WEP was the first to be developed and, shortly after its creation, several studies appeared accusing serious flaws in its implementation. Then the protocols WPA and WPA2 appeared within the scope of the IEEE 802.11i standard and, again, studies showing security flaws came up. This project aims at, besides presenting the 802.11 standard and its security protocols, analyzing their flaws, showing their causes and presenting results of tests using the Kali Linux tool. This work demonstrates the possibility of password cracking and misuse of the wireless network. Through research and analysis of the tests, this work tries to figure out what should be done to prevent unauthorized users from connecting to the network.

Key Words: Computers Networks, Wireless Networks, IEEE 802.11, Network Security, WEP, WPA, WPA2, Kali Linux, Wi-Fi.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADSL	Assymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
ARP	Adress Resolution Protocol
BSS	Basic Service Set
BSSID	Basic Service Set
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
D.o.S	Denial Of Service
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESA	Extended Service Area
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FHSS	Frequency-Hopping Spread Spectrum
FTAM	Transfer access and management File
FTP	File Transfer Protocol
GHz	Gigahertz
GPS	Global Position System
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute Of Electrical And Electronics Engineers
IGMP	Internet Group Message Protocol
IP	Internetworking Protocol
IPng	IP next generation
ISM	Industrial Scientific e Medical
ISO	International Standards Organization
LAN	Local Area Network

MAC	Medium Access Control
MAN	Metropolitan Area Network
Mbps	Megabits per second
MSC	Media-Specific Converters
OFDM	Orthogonal Frequency Division Multiplexing/Modulation
OSCE	Offensive Security Certified Expert
OSCP	Offensive Security Certified Professional
OSI	Open Systems Interconection
OSWP	Offensive Security Wireless Professional
PEAP	Protected Extensible Authentication Protocol
RADIUS	Authentication Dial-in User Service
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
ROM	Read Only Memory
RSN	Robust Security Network
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-fi Protected Access
WPA2	Wi-fi Protected Access2

1 INTRODUÇÃO

As redes sem fio, em particular as redes IEEE 802.11, usualmente identificadas pelo acrônimo WLAN se tornaram cada dia mais populares, sendo perceptível a conveniência de sua utilização em lugares como conferências, aeroportos, cafés e hotéis.

Outro tipo de rede sem fio é o Bluetooth, onde há uma crescente demanda de dispositivos portáteis, com suporte para essa tecnologia, quanto ao alcance dessas redes, estão aumentando a conexão, e já é possível a localização isolada desta tecnologia em alguns lugares. A utilização mais comum por usuários domésticos, é quando realizam integração de seus dispositivos portáteis, (i.e., celular com som; celular com notebook, etc.). Mediante este contexto, a praticidade e mobilidade que as redes sem fio propiciam em ambientes corporativos e também domésticos são consideráveis (RUFINO, 2007).

A primeira rede sem fio foi criada na Universidade do Havaí, em 1971, para conectar computadores nas quatro ilhas na qual se localizavam seus campi sem utilizar cabos telefônicos. As redes sem fio ingressaram no ramo da computação pessoal nos anos 80. Algumas das primeiras redes sem fio não utilizavam rádio, mas transceptores (uma combinação de transmissor e receptor) infravermelhos. Todavia tais redes nunca obtiveram sucesso porque a sua radiação não pode atravessar a maioria dos objetos físicos (ENGST; FLSIESHMAN, 2005).

Redes sem fio baseadas em ondas de rádio ganharam destaque no início dos anos 90, quando os processadores se tornaram rápidos o suficiente para gerenciar dados transmitidos e recebidos por meio de conexões de rádio. Porém, somente em 1999, o IEEE (Institute of Eletricaland Electronics Engineers) consolidou o padrão 802.11b. Em meados de 2002 o padrão 802.11a foi ratificado, superando significativamente o 802.11b em termos de velocidade. Infelizmente, devido à utilização da banda de 5 GHz, o 802.11a não é compatível com os milhões de dispositivos 802.11b atualmente em utilização, o que contribui para sua baixa aceitação. No final de 2002 surgiu o 802.11g, totalmente compatível com o 802.11b, e com mesma a velocidade do 802.11a (ENGST; FLSIESHMAN, 2005).

Redes wireless seguem os mesmos princípios que guiam todos os dispositivos sem fio. Um transceptor envia sinais através de ondas de radiação

eletromagnética, que se propagam a partir de uma antena. Esta recebe sinais nas frequências corretas e desejadas (ENGST; FLSIESHMAN, 2005).

A tecnologia de redes sem fio apresenta rapidez e facilidade em sua montagem e instalação, sem requerer conhecimento técnico específico por parte do instalador. Além disso, proporciona grande mobilidade e praticidade aos usuários. Devido a estas vantagens, as redes de computadores sem fio possuem atualmente um papel muito importante na comunicação de dados. Entretanto, o meio não-guiado por onde as informações destas redes trafegam, usando ondas de rádio, é extremamente inseguro, uma vez que os dados estão suscetíveis à escuta e a ataques diversos (GRÉGIO, 2005).

Ataques às redes sem fio, além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais estas se interconectam. Um fator determinante da segurança em redes sem fio está relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque (DUARTE, 2003).

Estas redes tornaram-se um alvo fácil para pessoas mal-intencionadas, desejosas em comprometer sistemas, pois disponibilizam inúmeros atrativos como dificuldade na identificação da origem exata do ataque, imaturidade das opções, e protocolos de segurança para esse tipo de tecnologia, facilidade em obter acesso a rede guiada através de uma conexão de rede sem fio, e principalmente, a falta de conhecimento técnico da maioria dos usuários adeptos desta nova tecnologia (DUARTE, 2003).

Desta forma, as redes sem fio têm sido exaustivamente estudadas e muitos ataques foram desenvolvidos e/ou adaptados para poderem se valer das vulnerabilidades presentes nestas redes. Além disso, elas apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio padrão 802.11 (DUARTE, 2003).

Estes problemas precisam ser solucionados para que não venham a impedir o crescimento vigoroso de sua utilização. O objetivo deste projeto é fazer um estudo detalhado da tecnologia de redes sem fio, analisando principalmente as questões de segurança. Em particular, serão estudadas as possíveis fragilidades dos protocolos existentes, analisando seus níveis de segurança, e consequentemente classificando suas fragilidades e colaborando com profissionais de segurança da informação.

A preocupação com a segurança da informação transmitida, remonta a muitos anos, e os romanos segundo relatos históricos já usavam métodos, ainda que primitivos, para resguardar as mensagens transmitidas. As redes sem fio não são tão antigas, têm apenas algumas décadas, mas muitos que as usam querem ter a certeza de que seus dados não estarão acessíveis para nenhuma pessoa indesejada.

O uso de redes sem fio (*wireless*) vem aumentando substancialmente, resultando em um impacto significante na vida das pessoas, em distâncias médias (*WIRELESS LAN*, *WLAN*) ou em curtas distâncias (*Bluetooth*), facilitando cada vez mais o dia-a-dia das pessoas, no entanto, trazem consigo novos riscos.

Essa popularização e adoção em massa, entretanto, trouxeram à tona a questão da segurança destas redes, as quais, devido a um crescimento desordenado e consequente desrespeito às normas básicas de segurança (em parte pela desinformação), têm sofrido um crescente número de ataques, gerando enormes prejuízos para as empresas (IDGNOW, 2013). Assim sendo, este trabalho visou analisar a fragilidade dos protocolos de segurança em redes sem fio, e ao mesmo tempo, colaborar com profissionais e interessados na área de segurança da informação.

2 OBJETIVOS

A seguir serão apresentados o objetivo geral e os objetivos específicos.

2.1 OBJETIVO GERAL

Analisar os níveis de segurança dos protocolos de rede sem fio e tabelar os resultados de suas fragilidades.

2.2 OBJETIVOS ESPECÍFICOS

a) Pesquisar os protocolos de segurança e criptografia;
b) analisar as vulnerabilidades de segurança destes protocolos;
c) estabelecer um comparativo entre os protocolos de segurança;
d) pesquisar o melhor SO para utilização da técnica;
e) investigar e analisar ferramentas utilizadas para invasão das redes "Wi-fi";
f) utilizar técnicas de "wardriving", em busca de redes "Wi-fi" com ou sem segurança, tentando o acesso a elas;
g) tabelar, apresentar e analisar os resultados obtidos em tais processos.

3 REVISÃO DA LITERATURA

Este capítulo apresenta os principais conceitos teóricos, necessários ao desenvolvimento do trabalho, a saber: o campo de estudos protocolos de segurança; as revisões sistemáticas de literatura e sua aplicação em redes sem fios; e por fim, outros métodos de estudos secundários.

3.1 REDES DE COMPUTADORES

Uma rede de computadores é formada por um conjunto de computadores conectados, que são capazes de trocar informações e compartilhar recursos físicos e lógicos. A rede de computadores pode ser formada por dois ou mais computadores com o objetivo de uma comunicação entre eles, podendo não só trocar dados, mas também, podem ter um compartilhamento de impressoras, mensagens através de e-mails, pastas compartilhadas entre outros. A Figura 1 exibe como pode ser formada e construída uma infraestrutura de redes (KUROSE; ROSS, 2006).

Figura 1 - Infraestrutura de redes.

Fonte: Elaborada pelo autor.

Segundo Amaral (2012), o modelo de um único computador que realiza todas as tarefas requeridas já não é mais existente, e para substituir este tipo de

arquitetura, foram implantadas as redes de computadores, a qual é formada por muitos computadores separados, interconectados por algum meio de comunicação.

A comunicação em massa de celulares e outros componentes junto, com a internet alcançaram uma necessidade de acesso rápido da informação. Antigamente as redes de computadores eram pequenas, com poucos computadores comercialmente usados em 1964 nos EUA pelas companhias aéreas. Estas soluções dependiam de um único fabricante limitando seu desenvolvimento.

Na década de 1970, fabricantes diferentes se movimentaram para padronizar e direcionar a construção de protocolos abertos, que mais tarde seriam viáveis para várias soluções. Já na década de 1980, as empresas DEC, Xerox e Intel se uniram para criar o padrão que atualmente conhecemos hoje como Ethernet (PINHEIRO, 2003 citado por AMARAL, 2012).

As redes de computadores e sua disponibilidade de enviar e receber dados permitem trafegar informações de um dispositivo a outro através de vários tipos de redes denominadas com o nome de topologia (forma e estrutura em que a rede é construída).

3.2 FUNDAMENTOS DE REDE SEM FIO 802.11

Segundo Campinhos (1999), uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos – sejam eles telefônicos, coaxiais ou ópticos – por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA.

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

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

3.2.1 Introdução

Conforme explica Tanembaum (2003), Local Area Network (LAN) é conhecida como uma rede local que é alocada em pequenas áreas físicas, permitindo o compartilhamento de vários recursos e a troca de informações de dados.

Muitas empresas, universidades e outras organizações possuem um grande número de computadores que devem permanecer conectados. Este tipo de necessidade deu a origem à rede local, a Ethernet.

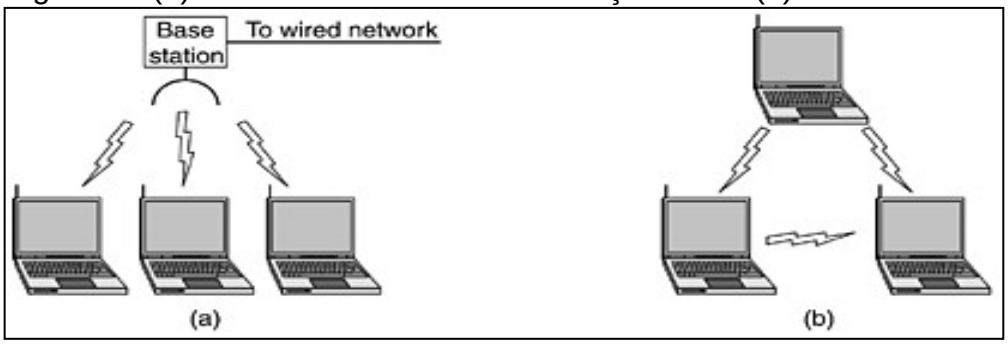
Esta origem de rede começou no primitivo Havaí, no início da década de 1970 quando o pesquisador Norman Abranson e seus colegas da University of Hawai*,* tentavam conectar usuários situados em ilhas remotas ao computador principal em Honolulu. A instalação dos seus próprios cabos sob o oceano não era realizável, e assim eles procuraram uma solução diferente. Nesta mesma época, um estudante chamado Bob Metcalfeab teve seu título de bacharel no Massachusetts Institute of Technology (M.I.T), e em seguida adquiriu o título de P.H.D. em Harvard, conhecendo o trabalho de Abramson antes de iniciar seu trabalho no Palo Alto Research Center (PARC) da Xerox e observaram um projeto físico de uma máquina em que os pesquisadores haviam projetado e montado o que futuramente seria chamado de computador pessoal (TANEMBAUM, 2003).

Ao notarem que as máquinas estavam isoladas e usando o conhecimento do trabalho realizado por Abramson e seu colega David Boggs, projetaram e implementaram a primeira rede local.

Tanembaum (2003) descreve que com o surgimento dos notebooks, muitas pessoas imaginavam entrar em seu estabelecimento e conectar o notebook à internet. Em questão disso, diversos grupos e empresas começaram a trabalhar para conseguir resultados para alcançar este objetivo, equipando o estabelecimento com transmissores e receptores de rádio de ondas curtas, permitindo a comunicação entre os receptores e os notebooks. O trabalho levou ao comércio de LANS sem fios por várias empresas. A indústria decidiu que um padrão de LAN sem fio seria necessário para sua padronização. Assim o comitê do IEEE realizou a tarefa de elaborar um padrão de LAN sem fios, recebendo o nome 118802.11 conhecido como Wi-Fi. O padrão é chamado pelo nome 802.11, e pode funcionar de dois modos:

a) Uma estação base que seria o ponto de acesso para a distribuição do sinal, chamada ponto de acesso 802.11.
b) Ausência de uma estação base, transmitindo diretamente os computadores uns para os outros. Este modo costuma ser chamado interligação de redes ad hoc. Um exemplo desse contexto seria duas ou mais pessoas juntas em uma sala não equipada com uma LAN sem fio, fazendo os computadores se comunicarem diretamente. A Figura 2 apresenta uma rede sem fio com estação base e uma rede had hoc. (TANEMBAUM, 2003).

Figura 2 - (a) Rede sem fio com um a estação base. (b) Rede ad hoc.



Fonte: Tanembaum (2010, p. 68).

3.2.2 Conceitos básicos

É utilizado um concentrador para comunicação entre estações, fazendo com que as configurações de segurança fiquem direcionadas em um só ponto, como mostra a figura 3, uma rede desse modelo é chamada de Extended Service Set (ESS). Outra vantagem desse modelo é que caso seja necessário, é possível interligar redes ethernet com redes sem fio, já que normalmente o concentrador faz o papel de gateway ou bridge (RUFINO, 2005).

3.2.2.1 Topologia de rede

Os equipamentos de rede para trocar informações entre si precisam de conexões e um meio físico para se conectarem. A forma que os equipamentos se interligam, fez com que surgisse o conceito de topologia de rede, classificando-se basicamente em: topologia em barramento, estrela ou anel (AMARAL, 2012).

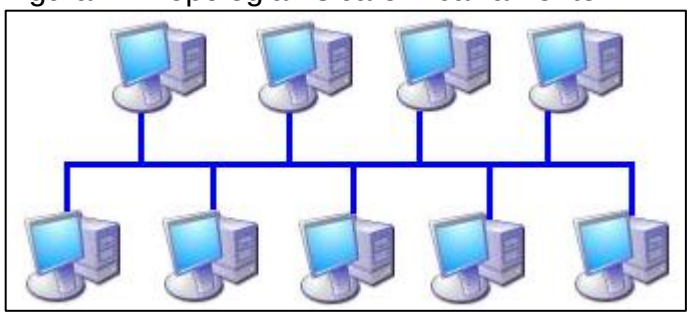
Figura 3 – Topologia de rede.

Fonte: Ribeiro (2014).

3.2.2.2 Topologia em barramento

Conforme Amaral (2012), a topologia em barramento é construída comum cabo de rede do modelo coaxial, atravessando toda a extensão da rede e interligando todos os computadores. Este meio de transmissão é utilizado nas redes LAN, atingindo taxas de transferências de até 10 Mbps por segundo (velocidade em que os dados são transferidos pela rede), e através de sua evolução foi predominada a arquitetura chamada Ethernet. Esta topologia não é mais usada pelo motivo que se algum problema ocorresse em qualquer parte desta infraestrutura, prejudicaria a rede toda, pois o cabo coaxial que interliga os computadores entre si era somente um. A Figura 4, mostra com clareza como esta topologia era ligada e se ocorresse algum problema o porquê os outros equipamentos eram prejudicados para a transferência de dados. O cabo coaxial usado parta a transferência de dados está alocado de forma horizontal ligando todos os equipamentos verticalmente.

Figura 4 - Topologia física em barramento.



Fonte: Elaborada pelo autor.

Como pode ser observado na Figura 4, o cabo é seccionado em cada local onde micro está inserido na rede, e se ocorrer algum problema de infraestrutura, todos os micros seriam afetados.

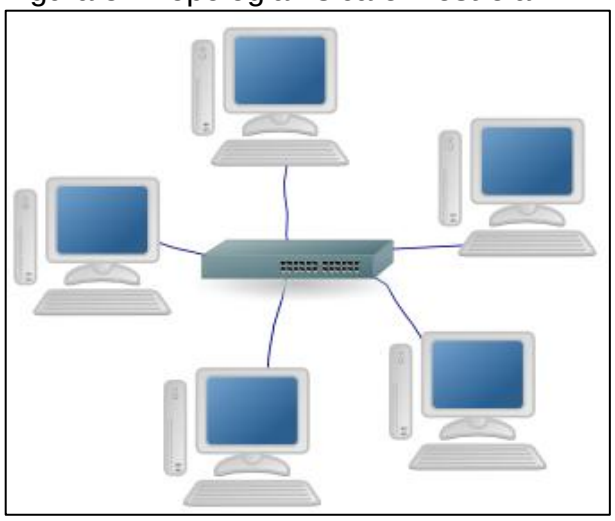
3.2.2.3 Topologia em estrela

Topologia em estrela é a evolução da topologia em barramento que atualmente é a mais utilizada em redes locais. Este nome se deve pelo fato de existir um equipamento em que conecta todos os cabos dos computadores da rede, utilizando equipamentos de distribuição chamados de hubs e switches.

O cabeamento utilizado nesta topologia evoluiu do cabo coaxial para o cabo par trançado, pois a transmissão de dados pode atingir taxas de até 10 Gbps por segundo (velocidade em que os dados são transferidos pela rede). Já para outros projetos maiores é necessário o uso de fibras óticas devido a sua confiabilidade e entrega de dados com perfeição e sem nenhuma perda.) AMARAL, 2012).

A topologia em estrela é a mais utilizada nos dias atuais, pois os computadores não são ligados através de somente um ponto horizontalmente, mas sim, através de um equipamento de distribuição concentrado que pode gerenciar os erros e apurar os resultados, dando uma nova rota de transferência de dados para os nós. A Figura 5 mostra o gerenciamento do equipamento que distribui o sinal, e faz a transferência dos dados. Caso ocorra algum tipo de perda na transmissão, o aparelho traça uma nova rota para que seja entregue a informação desejada. (AMARAL, 2012).

Figura 5 - Topologia física em estrela.



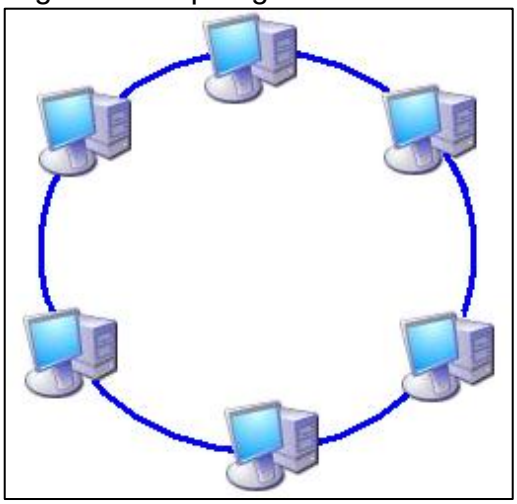
Fonte: Elaborada pelo autor.

3.2.2.4 Topologia em anel

Este tipo de topologia apresenta a ligação de vários nós da rede em círculo, formando um anel. Amaral (2012) cita que a rede cria duplos caminhos para a comunicação entre as estações interligadas. Da mesma forma que a topologia de barramento deu lugar para topologia estrela, a topologia anel também cedeu seu lugar para novas habilidades topológicas.

Esta topologia possui uma característica importante; pode ser configurada no sentido horário ou anti-horário. Como exemplo, a Figura 6, mostra uma topologia de rede ligada a uma topologia anel, que determina a distribuição dos dados. A vantagem deste tipo de rede é que se pode deixar um caminho reserva para se caso ocorra falhas durante a transferência de dados, o sistema é redirecionado ao segundo caminho já configurado para este tipo de falha. O fato de esta rede ter sido inexecutável é devido à quantidade de falhas ao seu custo.

Figura 6 - Topologia física em anel.



Fonte: Elaborada pelo autor.

Como pode ser observado na Figura 6, as redes em anel são capazes de transmitir e receber dados em configuração unidirecional.

3.3 PADRÕES ATUAIS

Segundo Rufino (2011), um grupo de trabalho formado pelo Institute of Electrical Enginners (IEEE), veio com o objetivo de definir os padrões de uso das redes sem fio. Um desses grupos foi chamado 802.11, definindo como deve ser a comunicação entre um dispositivo cliente e um concentrador, ou a comunicação entre os dois dispositivos, reunindo uma série de especificações. Este padrão é conhecido originalmente como padrão 802.11, e também conhecido como Wi-Fi, com a velocidade de transmissão no máximo 2 Mbps, e trabalhando com a banda de 2.4 GHz, contando com as principais extensões ou subpadrões descritos pela família 802.11.

3.3.1 Padrão 802.11b

Rufino (2011) ainda destaca que este padrão permite o número máximo de 32 clientes conectados e é o primeiro subpadrão, operando na frequência de 2,4 GHz e usando somente Direct Sequence Spread Spectrum (DSSS). Este padrão permite 11 Mbps de velocidade de transmissão máxima, podendo também se comunicar em velocidades mais baixas como 3, 2 ou mesmo 1 Mbps. Em 1999 foram criados e

definidos padrões bem semelhantes a redes da ethernet. Atualmente este é o padrão mais popular, e com maior base instalada, tendo limitação na utilização de canais, mas mesmo assim, o padrão disponibiliza mais produtos e ferramentas de administração e segurança disponíveis. É claro que este padrão chegou ao limite sendo desconsiderado em novas instalações e atualizações nos locais. Na Figura 7 pode ser identificada a associação do canal com a respectiva frequência.

Figura 7 - Canal e frequência

Canal	Frequência
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452

Canal	Frequência
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Fonte: Rufino (2011, p. 27).

3.3.2 Padrão 802.11a

Conforme destacado por Rufino (2011), a principal característica do padrão 802.11a é o aumento da velocidade para um máximo de 54 Mbps (108 em modo turbo), podendo operar em velocidades mais baixas. Definido após os padrões 802.11 e 802.b, e outra diferença é sua operação na faixa de 5 GHz que poucos concorrentes oferecem, porém com menor área de alcance. Seus clientes podem se conectar em até 64 clientes ao mesmo tempo, e ainda no tamanho da chave usada com WEP, em alguns casos a 256 bits tendo compatibilidade com os tamanhos menores como 64 e 128 bits.

Outra vantagem é a quantidade de canais não sobrepostos disponíveis, com o total de 12, diferente de 3 canais livres disponíveis nos padrões 802.11b e 802.11g, permitindo estender em uma área maior e muito povoada com melhores condições de outros padrões. Este padrão também adota o tipo de modulação

diferente do Direct Sequence Spread Spectrum (DSSS) usado no 802.11b, conhecido como Orthogonal Frequency Division Multiplexing/Modulation (OFDM).

Vários fabricantes investiram em equipamentos nesse padrão, e este procedimento parecido, começa a ser usado em redes novas. O problema relacionado à ampliação desse padrão é a inexistência de compatibilidade com a base instalada atual 802.11, pois este padrão utiliza faixas de frequências diferentes. RUFINO, 2011).

3.3.3 Padrão 802.11g

Este padrão pode ser implantado em vários de seus aspectos aos protocolos existentes. Responsável também por mecanismos de autenticação e privacidade, foi homologado em junho de 2004.

Rufino (2011) cita que o protocolo usado que permite meios de comunicação mais seguros que os protocolos utilizados atualmente é o Robust Security Network (RSN), estando inserido nesse padrão o protocolo Wi-fi Protected Access (WPA) projetado para prover soluções maiores de segurança relacionadas ao padrão Wired Equivalent Privacy (WEP) e Wi-fi Protected Access2 (WPA2), com a principal característica de criptografar o algoritmo Advanced Encryption Standard (AES).

3.3.4 Padrão 802.11i

O 802.11i foi ratificado a 24 de junho de 2004, a fim de fornecer uma solução de segurança das redes WiFi. Apoia-se no algoritmo de codificação Temporal Key Integrity Protocol (TKIP), e suporta igualmente o Advanced Encryption Standard (AES), tornando – se muito mais seguro.

O WiFi Alliance criou assim uma nova certificação, batizada **WPA2**, para os materiais que suportam o padrão 802.11i (computador portátil, pda, placa de rede, etc). Contrariamente ao WPA, o WPA2 permite proteger igualmente as redes sem fios em modo infraestrutura, assim como a rede em modo ad hoc (RUFINO, 2011).

3.3.5 Padrão 802.11n

Este padrão por vez é também conhecido como Word Wide Efficiency (WWiSE) tendo como objetivo principal aumentar a velocidade em uma média de 100 a 500 Mbps desejando-se obter um aumento da área de cobertura.

Nos padrões que são usados atualmente ocorrem poucas mudanças. Já outra característica deste padrão é sua compatibilidade retrocessiva com padrões vistos atualmente. Suas velocidades máximas oscilam em média de 135 Mbps no caso se trabalharem com canais de 40 MHz e mantendo a sincronia com os de 20 MHz atuais. Mesmo este padrão não sendo homologado para sua liberação no mercado, vários fabricantes se anteciparam e lançaram equipamentos com este padrão, pois a atualização definitiva é bastante simples se reduzindo a uma atualização pequena parecida com a de um firmware (sistema do roteador). O padrão 802.11n foi homologado no último trimestre de 2009. (RUFINO, 2011).

3.3.6 Padrão 802.11ac

Entre as diversas vantagens do novo padrão, a principal delas é o aumento substancial na velocidade de conexão. Segundo o especialista de produtos wireless da Cisco, Malko Saez, o novo padrão trará maior velocidade e, consequentemente, mais usuários na mesma área de cobertura, “melhorando a experiência do usuário quando navegar”. Além da velocidade, um dos grandes destaques do padrão 802.11ac é, sem dúvida, a melhora no sinal. Contudo, a melhora será maior em relação à qualidade do sinal e não necessariamente um aumento no alcance da rede. Não haverá diferença na qualidade de sinal entre uma pessoa há 30 metros de distância e outra próxima aos novos aparelhos (MACHADO, 2015).

3.4 ENDEREÇAMENTO MAC

Segundo Rufino (2005) cada dispositivo de rede utilizado tanto para redes ethernet, como para redes sem fio, deve ter um número único de identificação definido pelo fabricante e controlado pelo IEEE (Institute of Electricaland Electronics Engineers), permitindo assim, teoricamente, identificar de forma inequívoca um equipamento em relação a qualquer outro fabricado mundialmente, seja ele de

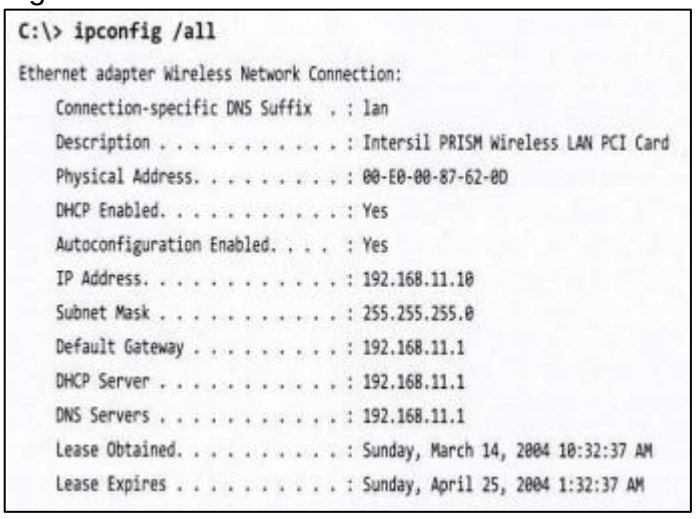
fabricantes diferentes. Mas em certos modelos de placas antigas, esse número poderia ter o mesmo número, precisando assim de um programa fornecido pelo fabricante da placa para trocar de endereço MAC único.

Pensando em que cada placa tem um número endereço, uma das maneiras disponíveis para aumentar a segurança de uma rede é o cadastramento desse endereço MAC no concentrador, restringindo assim o acesso a somente quem estiver cadastrado, essa técnica visa somente autorizar o equipamento e não só o usuário. (RUFINO, 2005).

Para melhorar a segurança utilizando o endereço MAC é necessário substituir a entrega de endereços IP via Dynamic Host Configuration Protocol (DHCP) por IP fixos, que trabalhando em conjunto dificultaria um possível ataque. alguns programas também permitem associar o endereço MAC do cliente com o endereço MAC do concentrador, permitindo assim a autenticação em um concentrador correto e não por engano, com um concentrador errado de maior potência ou de um atacante, dificultando um possível ataque. (RUFINO, 2005).

Nos sistemas operacionais como Windows XP, Windows Vista, Windows 2003, Windows 7, Windows 8 e Windows 10, pode ser usado o comando ipconfig onde a linha Phisycal address indica o endereço MAC dessa interface conforme é mostrado na Figura 8.

Figura 8 – Terminal.



Fonte: Rufino (2011).

3.5 CRIPTOGRAFIA E AUTENTICIDADE EM REDES SEM FIO.

Segundo Stallings (2008), se o envio de sinal para todas as estações possui um grande risco em redes cabeadas, em redes sem fio ganham-se uma dimensão muito maior: para ter acesso ao meio, um atacante não precisa estar presente fisicamente ou ter acesso a um equipamento da rede-alvo. Como o meio de transporte é o próprio ar, basta que um atacante esteja na área de abrangência do sinal. Os equipamentos possuem vários mecanismos de segurança, porém não habilitados na configuração original, faz com que administradores e usuários com pouca experiência em redes sem fio, coloquem os equipamentos em operação sem qualquer mudança, facilitando o ataque. Portanto, as chaves Wired Equivalent Privacy (WEP), Wi-fi Protected Access (WPA), Wi-fi Protected Access 2 (WPA2) e Service Set Identifier (SSID) devem ser modificadas de modo a não permitir identificar a rede.

Para ter uma rede sem fio aceitável, (sob a ótica da segurança), é necessário configurar recursos adicionais, como criptografia e autenticação forte, elementos esses que não fazem parte da configuração básica e que demandam tempo e trabalho para configuração e manutenção, tanto no concentrador quanto nos clientes e demais equipamentos que dessa rede façam uso (STALLINGS, 2008).

3.5.1 Wired Equivalent Privacy (WEP)

Rocha (2015) cita que o protocolo 802.11 disponibiliza possibilidades de cifração de dados. Inicialmente a sugestão para resolver este problema foi o WEP, que está totalmente difundido e presente nos produtos atuais que alocam este padrão 802.11, usando algoritmos simétricos e existindo uma chave secreta que é compartilhada com as estações de trabalho e o concentrador para cifrar e decifrar as mensagens trafegadas, seguindo os critérios para desenho do protocolo, apresentados a seguir:

a) Suficientemente forte: O algoritmo alocado deve ser adequado dependendo as necessidades do usuário
b) Auto sincronismo: Quando um equipamento abranger a área de cobertura, funcionará sem nenhuma intervenção manual.

c) Requerer poucos recursos computacionais: Equipamentos com pouco poder de processamento e pode ser implantado por software ou em hardware
d) Exportável: Pode ser passível de importação para outros países e também deve poder ser exportado dos Estados Unidos no qual em sua elaboração do padrão, para exportação de criptografia havia restrições e já hoje essas restrições estão limitadas em alguns países.

O conjunto que formará a chave usada para cifrar o tráfego da segurança WEP é composta de dois elementos básicos: uma chave estática (fixa) que é usada em todos os equipamentos da rede e um componente dinâmico (aleatório).

Rufino (2011) destaca que esta chave não é distribuída conforme o protocolo define, sendo assim mais trabalhosa, tendo que ser cadastrada manualmente em todos os equipamentos.

Após estabelecer uma conexão, a chave estática calcula uma operação matemática de geração de mais quatro novas chaves sendo escolhida uma dessas quatro para cifrar as informações percorridas na rede. Como consequência essa chave será fixa e somente irá ser trocada se a chave original estática mudar, porém essa nova chave gerada é fixa e vulnerável a ataques de dicionário de força bruta, tendo o tamanho de 40 a 104 bits, e o padrão ainda é 104, podendo ter várias implementações com valores maiores.

A tentativa de evitar esses tipos de ataques, é a adição de um segundo elemento que consiste em um conjunto de 24 bits criados por uma função pseudoaleatória que será concatenada às chaves fixas (40 ou 104), na devida ordem como 64 ou 128 bits, geralmente esse procedimento é realizado pelo roteador que distribui a informação para os elementos que estão participando da rede, entretanto os 24 bits passam em aberto pela rede pelo motivo que essa foi a forma de dar conhecimento desse valor encontrado, sendo possível que os elementos da rede estabeleçam uma comunicação criptografada. Após terem sido expostas várias vulnerabilidades do WEP, notou-se que esse protocolo sem fio é obsoleto e terrivelmente vulnerável (ROCHA, 2015)

3.5.2 WI-FI Protected Access (WPA)

De acordo com Rufino (2011), após os problemas de segurança serem divulgados para WEP, a Wi-Fi Alliance liberou o protocolo WPA e adiantou uma parte da autenticação e cifração de todo o trabalho que estava sendo feito para o fechamento do padrão 802.11i. Este protocolo deve trabalhar a maior parte a inclusão de outros elementos à infraestrutura, e em combinação com outros protocolos como o 802.11x, após várias mudanças e avanços serem colocados no mesmo. Na versão I do WPA, não está disponível suporte a conexões de rede had-hoc, portanto nessa característica de rede que não necessita o uso do roteador não há funcionamento dos mecanismos de proteção no protocolo WPA da primeira versão.

Suas duas áreas distintas executam a substituição do WEP, tendo o objetivo de garantir as informações trafegadas e sua privacidade e tratando da cifração dos dados.

Para solucionar problemas de mecanismos de criptografia existente na WEP, o WPA avançou em pontos mais vulneráveis, combinando algoritmo e chaves temporárias em ambientes que este tipo de rede pode existir como, por exemplo, (pequenos escritórios, pequenas e grandes indústrias, locais domésticos, etc.). Os protocolos para criptografar as informações podem ser usados de duas formas: um voltado para uso doméstico e pequenas redes, compartilhando uma prévia chave (Pre-sharedkey, ou WPA-PSK), identificada e conhecida como máster, que se responsabiliza pelo reconhecimento do equipamento pelo roteador, e outro apresentado como infraestrutura que exigirá a configuração de um servidor de autenticação (RADIUS), um equipamento adicional (DUARTE, 2003)

Não necessitando de equipamentos extras como servidores de autenticação, a vantagem desse método é sua simplicidade, pois não necessita de equipamentos extras. Do mesmo modo Aguiar (2005) comenta que isso ocorre no protocolo WEP, ou seja, a troca de chaves é feita manualmente, tornando o uso restrito a pequenas redes em que os participantes estão acessíveis na maior parte do tempo, dificultando também a guarda da chave. O protocolo responsável pela troca dinâmica de chaves é o Temporal Key Integrity Protocol (TKIP), uma evolução do WEP.

Segundo Rufino (2011), a troca dinâmica de chaves e a responsabilidade pela gerência de chaves temporárias, usadas pela comunicação em equipamentos é uma das novidades do WPA, o protocolo Temporal Key Integrity Protocol (TKIP), mostrando a preservação do segredo mediante a troca constante de chaves. Uma das vulnerabilidades do WEP era utilizar chaves estáticas e as partes que não são lidas atravessarem a rede em aberto (claro).

Outra correção da vulnerabilidade da WEP que foi corrigida neste protocolo e usada neste método é o aumento do vetor de inicialização, passando dos 24 para 48 bits, elevando a quantidade de combinações possíveis, tornando ataques com base na repetição de valores dos vetores praticamente inofensivos, exigindo processos fora dos padrões do mercado atual. As vantagens desta forma de troca do vetor são claras, mostrando que quanto mais rápido ocorrer essa troca menor é a chance de um atacante descobrir o valor de vetor de inicialização usado. Entrementes essa modalidade tem perdido o cansaço e várias vulnerabilidades têm aparecido explorando esse protocolo, vulnerabilidades não tão graves como o protocolo WEP (AGUIAR, 2005).

3.5.2.1 Extensible Authentication Protocol (EAP)

Esse modelo de autenticação foi definido no WPA, permite integrar soluções externas para autenticação como, por exemplo, um servidor RADIUS. O EAP utiliza o padrão 802.1x e permite vários métodos de autenticação, podendo até utilizar certificação digital.

O método de autenticação pode ser o mesmo utilizado para usuários discados, incorporando a este ambiente usuários de rede sem fio. A grande vantagem é a segurança, já que como é possível integrar outros sistemas a ele, pode-se, por exemplo, manter uma base de dados de usuários, tanto para rede cabeada como para rede sem fio (AMARAL, 2012).

3.5.3 WPA 2 ou 802.11i

Sendo a versão mais nova e segura do WPA, o WPA2, também conhecida como 802.11i, têm consigo a implementação do protocolo Counter Cipher Modewith

Block Chaining Message Authentication Code Protocol (CCMA), utilizando o algoritmo AES. Com base nas afirmações de Haines (2010), tanto o WPA quanto o WPA2, utilizam-se de chaves de 256 bits em hexadecimal, gerados pelo algoritmo Password-Based Key Derivation Functions (PBKDF2).

Isto foi proposto devido a problemas de padronização na entrada da chave, pois não era especificado se deviam estar no formato hexadecimal ou no mais comum ASCII. Outra novidade apresentada no WPA2 é a vinda do protocolo Extensible Authentication Protocol (EAP), que permite integrar soluções e de autenticação já conhecidas e testadas (RUFINO, 2011).

3.6 ANÁLISES DOS ATAQUES E VULNERABILIDADES DAS REDES SEM FIO

Nos tópicos seguintes, será apresentada uma análise sobre as principais fragilidades das redes sem fio.

3.6.1 Introdução

Segundo Ross (2009), as redes locais sem fio têm se tornado, cada vez mais, uma opção para ambientes corporativos, um dos maiores desafios do ambiente de redes sem fio é a implementação de um ambiente seguro para o tráfego das informações, vista que acessos indevidos à rede e a leitura ou alteração de dados em trânsito na mesma representam uma grande ameaça a estes ambientes.

Para cada solução de rede sem fio devemos avaliar ferramentas e topologias que atendam às necessidades da aplicação. Nenhuma rede é 100% segura e nenhuma ferramenta ou tecnologia utilizada isoladamente garante proteção completa contra-ataques e invasões.

Os principais fabricantes de equipamentos para redes locais sem fio, face às necessidades de segurança do mercado estão se antecipando aos padrões, e agregando novos mecanismos de segurança aos seus novos equipamentos. Entretanto, nem sempre, tais mecanismos são eficazes. (ROSS, 2009).

Praticamente todos os equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados durante a configuração da rede podem facilmente ser alvos de ataques à rede. O administrador deve considerar que qualquer informação pode ser útil a um hacker.

Se alguma informação de fábrica, que permita acesso ou presuma detalhes que possam ser usados em ataques, estiver disponível, certamente será utilizada em algum momento. Portanto, senhas administrativas devem ser trocadas, bem como as chaves WEP ou WPA, e o SSID deve ser modificado de modo a não permitir identificar a rede (ROSS, 2009).

Outro fator importante é o serviço SNMP que geralmente vem habilitado do fabricante do Access Point, este serviço transmite sinais em broadcast, nestes sinais estão informações importantes gerenciáveis sobre o equipamento e o trafego, a em alguns casos permite até mesmo a configuração de alguns parâmetros remotamente (ROSS, 2009)

3.6.2 Problemas de segurança física

De acordo com a ABNT (2005), onde são descritas as normas da ISO 17.799/2005 segurança física é definida como:

> As instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreira de segurança e controles de acesso apropriados. Convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p.36).

De forma mais detalhada, os perímetros de segurança são uma área delimitada por uma linha imaginária que separa de outros espaços físicos por qualquer medida preventiva, as quais dificultam o acesso não autorizado aos ativos da informação, como por exemplo, a biometria.

3.6.3 Negação de serviço (Denial of Service – DoS)

O ataque de D.o.S (Negativa de Serviço) como o nome próprio indica, procura tornar algum recurso ou serviço indisponível. Em redes sem fio estes ataques podem ser tão perturbadores quanto maior sua sofisticação.

Estes ataques podem ser disparados de qualquer lugar dentro da área de cobertura da REDE SEM FIO.

Como as redes 802.11b/g trabalham na radiofrequência de 2.4 GHz, e esta é utilizada por fornos micro-ondas, aparelhos de monitoramento de crianças, entre outro, estes produtos podem facilitar os ataques de negativa de serviço, através da inserção de ruídos a partir destes aparelhos nas redes sem fio. Entretanto, hackers podem gerar ataques mais sofisticados. Por exemplo, um atacante pode se passar por um Access point com o mesmo SSID e endereço MAC de outro Access point válido e inundar a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se re-associarem. Enviando as requisições de dissociação em períodos curtos de tempo o D.o.S é concretizado, pois os clientes não conseguem permanecer conectados por muito tempo (MORIMOTO, 2011).

3.6.4 Mapeamento do ambiente

É uma das primeiras ações realizadas pelos atacantes, pois possibilita obter o maior número de informações sobre uma determinada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de forma mais precisa e com menos riscos de ser identificados (FERREIRA, 2013).

3.6.5 Configurações

Existem várias razões para que um hacker queira acessar uma determinada rede: uma saída pura e simples para Internet, promover ataques a terceiros, interesse em informações da própria empresa, entre outras. Por outro lado, há também possíveis vulnerabilidades a que um ambiente de rede pode estar exposto, e permitir acessos não autorizados, por falta de configuração adequada (FERREIRA, 2013).

3.6.5.1 Configuração aberta

Segundo Ferreira (2013), o concentrador aceita conexão de qualquer dispositivo, portanto, basta que um hacker disponha de um equipamento com interface sem fio, e este ser compatível com o padrão utilizado no ambiente alvo. A partir do estabelecimento da conexão, o concentrador pode fornecer

automaticamente (por meio de um servidor DHCP) um endereço IP. Caso isso não ocorra, ainda assim pode-se identificar o bloco IP utilizado no ambiente e manualmente configurar sua interface. Quando não são fornecidas informações automaticamente, é possível utilizar simples escuta de trafego para obtê-las.

3.6.5.2 Configuração fechada

O mecanismo denominado “rede fechada” é aquele onde não se transmite o SSID por broadcast. O SSID é utilizado como uma senha simples, necessária no processo de autenticação. Neste caso, o cliente é solicitado a informar o SSID correto como uma das etapas do processo de autenticação. Quando um cliente legítimo percorre o processo de autenticação, ele envia o SSID em texto plano, o que possibilita sua captura e posterior utilização. Desta maneira o SSID não agrega segurança ao sistema (FERREIRA, 2013).

3.7 VULNERABILIDADES DOS PROTOCOLOS WEP E WPA

No padrão original, o protocolo WEP utiliza chave única e estática compartilhada entre todos os dispositivos de uma rede. Portanto em caso de troca da chave isso se torna impraticável em redes com muitos clientes, pois é um processo muito trabalhoso, lembrando que essa troca deverá ser feita em todos os clientes. Sendo assim, se realmente necessitar utilizar WEP em uma rede com muitos usuários, a rede ficará de alguma forma com menor segurança pois quanto maior o número de pessoas que conhecer a chave maior a probabilidade de outras pessoas descobrirem visto que os equipamentos podem ser perdidos, compartilhados ou atacados (RUFINO, 2005).

Outro problema segundo Rufino (2005), é relacionado ao uso do algoritmo RC4, pois ele recebe um byte que realiza um processamento e gera um byte também na saída, só que diferente do original, possibilitando saber quantos bytes tem a mensagem original, já que a informação terá o mesmo número de bytes que a original.

Já em relação ao vetor de inicialização (Initialization Vector – IV) a chave contém apenas 104 bits e 24 bits para o vetor de inicialização formando os 128 bits vendidos como solução pelos fabricantes. O vetor de inicialização permite variar em

24 bits a chave fixa, tornando diferente o resultado de mensagens idênticas. Mas lembre-se de que para haver comunicação cifrada a chave deve ser conhecida por ambos os lados da comunicação (RUFINO, 2005).

Com uma rede com tráfego intenso é transmitido em torno de 600 a 700 pacotes, mesmo que todos os valores sejam usados sem repetição, o mesmo valor será utilizado novamente em 7 horas, assim um atacante poderá observar passivamente o tráfego e identificar quando o mesmo valor será utilizado novamente. O protocolo pode sofrer um ataque por dicionário ou força bruta, onde o atacante testa senhas em sequência e/ou em palavras comuns, já que quando uma mensagem idêntica é cifrada com uma chave fixa, todas as vezes que uma mensagem idêntica for criptografada, terá o mesmo resultado, utilizando a equivalência entre o byte original e o byte cifrado (RUFINO, 2005).

O protocolo WPA, apesar de ser mais seguro que o WEP, apresenta algumas vulnerabilidades já documentadas e que devem ser conhecidas para minimizar seu impacto. Senhas com menos de 20 caracteres podem sofrer com os ataques de dicionários ou ataques exaustivos. Problemas com senhas de fabrica não alteradas pelos administradores de redes torna o WPA tão vulnerável quanto o WEP. (RUFINO, 2005).

Segundo Rufino (2005), mesmo com as melhorias verificadas no WPA, há vários pontos vulneráveis no processo, e independentemente do método utilizado (chaves previamente compartilhadas ou modo infraestrutura), verificam-se problemas no armazenamento das chaves, tanto nos clientes quanto nos servidores/concentradores, que podem comprometer a segurança de redes que utilizam WPA.

3.8 TÉCNICAS E FERRAMENTAS DE ATAQUE

Segundo Gimenes (2005), não existe nenhuma grande novidade nos ataques às redes sem fio. Alguns ataques não sofreram nenhuma modificação em relação aos ataques às redes cabeadas. Outros, no entanto, tiveram que sofrer algumas modificações a fim de obter melhores resultados. A seguir descrevemos algumas técnicas e ferramentas de ataque utilizadas.

3.8.1 Access Point Spoofing (Associação Maliciosa)

A associação maliciosa ocorre quando um atacante, passando-se por um Access Point, ilude outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real (DUARTE, 2003).

3.8.2 ARP Poisoning

Redireciona o tráfego para o impostor via falsificação/personificação do endereço MAC. É um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vítima. Um ataque que se utilize de ARP Poisoning pode ser disparado de uma estação da WLAN à uma estação guiada. Ou seja, este ataque não fica restrito apenas às estações sem fio (DUARTE, 2003).

3.8.3 MAC Spoofing

Os dispositivos para redes sem fio possuem a particularidade de permitir a troca do endereço físico. Com isso, atacantes mal-intencionados podem capturar um endereço MAC válido de um cliente, trocar seu próprio endereço pelo do cliente e utilizar a rede (COZER, 2006).

3.8.4 Wardriving

Wardriving é uma forma de ataque muito parecida com a anterior. Modifica-se somente a forma de como as redes sem fio são encontradas. Utilizam-se neste tipo de ataque equipamentos configurados para encontrar tantas redes sem fio quantas aquelas que estiverem dentro da área de abrangência do dispositivo de monitoramento. O objetivo deste tipo de ataque, além dos já mencionados nos ataques de vigilância é mapear todos os Access points encontrados com o auxílio de um GPS (OLIVEIRA, 2009).

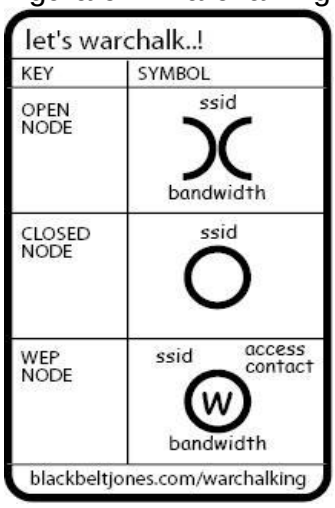
Muitas vezes apelidado de “war-driving”, este teste consiste na procura sistemática de pontos de acesso wireless piratas, eventualmente instalados por utilizadores, à revelia do departamento de informática (por exemplo, por alunos num

campus universitário). Pode também representar a tentativa sistemática de detecção de pontos de entrada desprotegidos nas redes wireless empresariais. A tecnologia atualmente existente permite realizar estas ações de uma forma (relativamente) simples e discreta, o que obrigará as organizações a ter especial cuidado na configuração dos aspectos e funcionalidades de segurança destas redes (OLIVEIRA, 2009).

3.8.5 Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas do capitulo 4.8.4, e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. Isto para que outros atacantes possam de antemão saber quais as características da rede. Alguns dos símbolos utilizados por estes atacantes podem ser observados na Figura 9. Existem grupos organizados para warchalking que utilizam símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo. Existem também grupos rivais que tentam encontrar e pichar o maior número de redes possível para ganhar mais status. Seriam como os grupos de defacers de páginas da Web, mas realizados fisicamente (DUARTE, 2003).

Figura 9 – Warchalking



Fonte: Duarte (2003).

O primeiro símbolo identifica uma rede wi-fi aberta, descrevendo seu SSID (nome da rede) e sua largura da banda.

O segundo símbolo identifica uma rede fechada, descrevendo apenas o SSID (nome da rede).

O terceiro símbolo identifica uma rede protegida pelo protocolo de criptografia WEP, junto com o SSID (nome da rede), o access contact (chave WEP utilizada) e a largura da banda (velocidade da rede).

3.8.6 Ferramentas de Ataque

Antes de analisar os ataques às redes sem fio, serão mostradas as ferramentas disponíveis tanto para a segurança quanto para o ataque nestas redes. A ideia é simplificar as explicações de cada um dos ataques e relacionar cada um destes com as ferramentas que utilizam.

3.8.6.1 Airtraf

Esta ferramenta permite coletar uma grande quantidade de informações sobre redes identificadas, tais como clientes conectados e serviços utilizados, tudo em tempo real. Além disso, “quebra” a chave do protocolo WEP no padrão 802.11b. Ela atua passivamente monitorando as transmissões.

É muito prática para coletar informações de redes sem fio, exibem detalhes úteis para a invasão, também pode ser usada por administradores que podem monitorar as atividades das quais são responsáveis (AIRTRAF, 2002).

3.8.6.2 Netstumbler

Este é a ferramenta mais conhecida de scanner para redes sem fio. Inclui muitas características como potência do sinal, SSID da rede em questão, além de suporte a GPS (Sistema de Posicionamento Global). Este programa modificou significantemente o mundo da rede sem fio. Pois, além de ser utilizado para ações maliciosas, pode ser utilizado pelo gerente da rede em questão para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição (NETSTUMBLER, 2014).

3.8.6.3 Kismet

Desenvolvido com a filosofia open source, que inclui um grande número de ferramentas e opções. Projetado como cliente e servidor, pode ter vários servidores rodando a distância de um único cliente. Além de monitorar uma gama muito grande de origens diferentes, pode armazenar os pacotes capturados em vários formatos diferentes.

Este programa gera dados relacionados à localização aproximada do dispositivo monitorado. Isto é realizado através da união das características do Kismet com um GPS. Outro ponto favorável em relação às outras ferramentas é que automaticamente salva todas as redes encontradas. Trabalhando com a biblioteca Ncurses14 e tendo várias telas e opções, disponibiliza quase todas as informações necessárias para um atacante desenvolver seus ataques. Algumas das informações que o Kismet consegue obter sobre o estado geral da sua área de abrangência são: Número de Redes sem fio detectadas, número total de pacotes capturados por Redes, ausência ou não de criptografia WEP, número de pacotes com o I.V. fraco, número de pacotes irreconhecíveis, número de pacotes descartados e tempo decorrido desde a execução do programa (RUFINO, 2005).

3.8.6.4 AirJack

Uma característica interessante desta ferramenta é a facilidade de fazer um ataque do tipo “homem no meio”, que consiste na implantação de falsos concentradores que se interpõem aos concentradores oficiais e, desta forma, passam a receber as informações transmitidas (RUFINO, 2011).

3.8.6.5 – Kali Linux

Kali Linux é uma distribuição Linux baseada no Debian que visa avançado testes de penetração e auditoria de segurança. O Kali contém várias centenas de ferramentas destinadas a várias tarefas de segurança da informação , tais como testes de penetração , Forensics e Engenharia Reversa (WEIDMAN, 2014).

Foi projetado para testes de intrusão e auditorias de segurança profissionais e atividades afins. São mais de 300 ferramentas disponíveis e que podem ser usadas

para avaliar os graus de segurança e as fraquezas que podem estar presentes (FERREIRA, 2013).

3.8.6.6 Ferramentas para quebra de chaves WEP

Existem várias ferramentas desenvolvidas para decifrar chaves WEP, com maior ou menor grau de eficiência. Geralmente aplicam uma combinação de força bruta ou ataques com dicionário.

Segundo Cozer (2006) podemos destacar:

a) Airsnort: é um programa para quebra de chaves WEP. Funciona diferentemente do WEPCrack, pois consegue quebrar qualquer chave. Isto após conseguir obter aproximadamente de três a cinco milhões de pacotes trocados.
b) WepCrack: este programa trabalha utilizando-se da vulnerabilidade encontrada no começo do ano 2001 no WEP. Na realidade este programa é um script perl e supostamente funcionaria em qualquer sistema com suporte a este tipo de script. No entanto, somente se torna inteiramente funcional em sistemas linux. Pessoas mal-intencionadas utilizam o WEPCrack para obter informações vitais à rede como o SSID para gerar posteriores ataques.
c) AirCrack: é o responsável pela quebra da senha através da análise dos pacotes capturados e pode ser usado contra WEP, WPA e WPA2. Uma vez que o Airodump (que detecta os pontos de acesso que estão ao seu alcance) tenha capturado pacotes suficientes, é possível quebrar senha WEP utilizando o AirCrack (GUIMARÃES, 2009).

3.9 ESTRATÉGIAS DE DEFESA

Nos tópicos a seguir, seguem estratégias usadas para defesas dos ataques sofridos em redes sem fio.

3.9.1 Considerações Iniciais

O uso de redes sem fio permite muito mais flexibilidade e mobilidade aos usuários, porém um fator fundamental vem sendo colocado em segundo plano na implementação dessas redes: a segurança da informação. O uso de estratégias de segurança eficazes é imprescindível, pois há a necessidade de diminuir os riscos e os acessos indevidos à rede (JUNIOR et al, 2004).

Para conseguir um nível razoável de segurança é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são fundamentais (JUNIOR et al, 2004). Neste capítulo serão apresentadas estratégias de segurança que devem ser aplicadas às redes wi-fi, tornando-as mais seguras e menos vulneráveis as inúmeras ferramentas de ataques disponíveis.

3.9.2 Configurações do concentrador

O primeiro passo para tornar a rede mais segura é desabilitar a difusão da informação de SSID (broadcast SSID), escondendo assim o nome da rede. Desta forma, apenas clientes que conhecem o nome da rede ao qual o concentrador responde poderiam estabelecer conexão. Todavia existem tipos de ataque que não necessitam conhecer o SSID, como é o caso da escuta do tráfego. Inclusive, ao realizar a escuta, é possível descobrir o SSID da rede alvo. Deve-se também modificar o nome ESSID padrão para ao menos retardar um ataque. O administrador deve escolher um nome que não revele nem o equipamento nem a empresa (MORAES, 2010).

Segundo Rufino (2005), é preciso alertar que o campo INFO é meramente documentável e permite cadastrar informações adicionais, sendo transmitido em texto não criptografado. Portanto, tanto o ESSID como o INFO devem ser usados corretamente, para dificultar ao máximo as ações de um possível atacante.

Alguns concentradores permitem alterar o endereço MAC. Esta mudança evita a identificação imediata do fabricante por parte de um atacante, pois o endereço MAC está diretamente relacionado ao seu fabricante. A maior parte dos concentradores permite configuração via HTTP e TELNET. Recomenda-se desabilitar essas opções do lado da rede sem fio, para impedir que informações

importantes (como usuário e senha) sejam interceptadas por um possível atacante. Esta ação pressupõe que a rede cabeada tenha mecanismos de proteção que possibilitem monitorar e autenticar os usuários, restringindo as configurações do concentrador somente as pessoas devidamente autorizadas (RUFINO, 2005).

Outra importante medida é fazer os concentradores ignorarem clientes que enviam SSID igual a “ANY”. Esta é uma situação que usualmente caracteriza um cliente que busca qualquer concentrador disponível. Como não é possível ter certeza de que se trata realmente de um cliente, esta situação deve ser evitada, já que um atacante pode utilizá-la para ter acesso à rede. É importante destacar que essas medidas usadas isoladamente não fornecem um bom nível de segurança, por isso devem ser combinadas com outras medidas para que se tornem devidamente eficazes (MORAES, 2010).

3.9.3 Defesa dos equipamentos clientes

Um importante mecanismo de defesa é o Publicly Secure Packet Forwarding (PSPF), que bloqueia o acesso de um cliente a outros ligados ao mesmo concentrador, evitando ataque direto de um usuário contra outro. Esta configuração equivale à de um switch, onde se define uma interface por porta. Entretanto, ao contrário do switch onde existe separação física do tráfego, este método não impede a captura dos pacotes. Desta forma, este mecanismo deve ser usado de forma combinada com outras medidas de segurança, para garantir a privacidade dos usuários (RUFINO, 2005).

3.9.4 Padrão 802.1x e RADIUS

O padrão IEEE 802.1X define métodos de autenticação, que são componentes importantes para aumentar o nível de segurança de uma rede sem fio. Um componente muito utilizado para fazer autenticação é o servidor RADIUS.

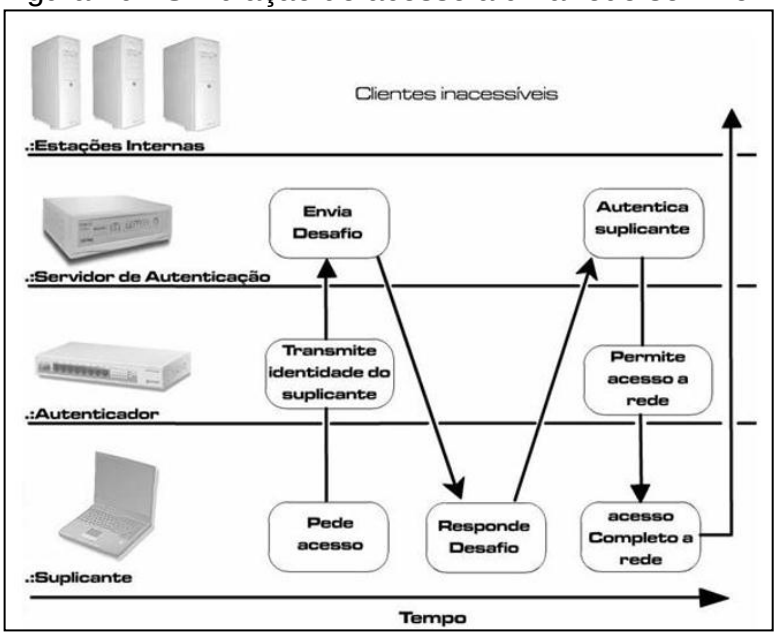
Segundo Aguiar (2005), em um processo de autenticação 802.1x existem 3 participantes:

a) O suplicante: usuário a ser autenticado.
b) Servidor de autenticação: sistema de autenticação RADIUS, que realiza a autenticação dos clientes cadastrados.

c) Autenticador: mediador na transação entre o suplicante e o servidor de autenticação. Geralmente é o AP.

De acordo com a Figura 10, o requisitante (suplicante) pede o acesso, o autenticador transmite a identidade do suplicante para o servidor de autenticação, que por sua vez envia um desafio ao suplicante. O suplicante responde o desafio e o servidor autentica o usuário para que o autenticador permita o acesso à rede (GIMENES, 2005).

Figura 10 - Simulação de acesso a uma rede sem fio.



Fonte: GIMENES (2005).

Ainda, segundo o autor, O 802.1x utiliza o protocolo EAP para gerenciar a forma como a autenticação mútua será feita na rede. Ele possibilita a escolha de um método específico de autenticação a ser utilizado, como senhas, certificados ou tokens de autenticação.

O autenticador não precisa entender o método de autenticação, ele simplesmente repassa os pacotes EAP do suplicante para o servidor de autenticação e vice-versa (AGUIAR, 2005).

3.9.5 Virtual Private Network (VPN)

Uma opção de segurança para redes sem fio são as VPN (Redes Privadas Virtuais). Segundo Junior et al. (2004), elas são túneis de criptografia entre pontos

autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações de modo seguro, entre redes corporativas ou usuários remotos. Esta técnica, também chamada de tunelamento, cria “túneis virtuais” de comunicação entre dois pontos, garantindo maior segurança no tráfego das informações transmitidas.

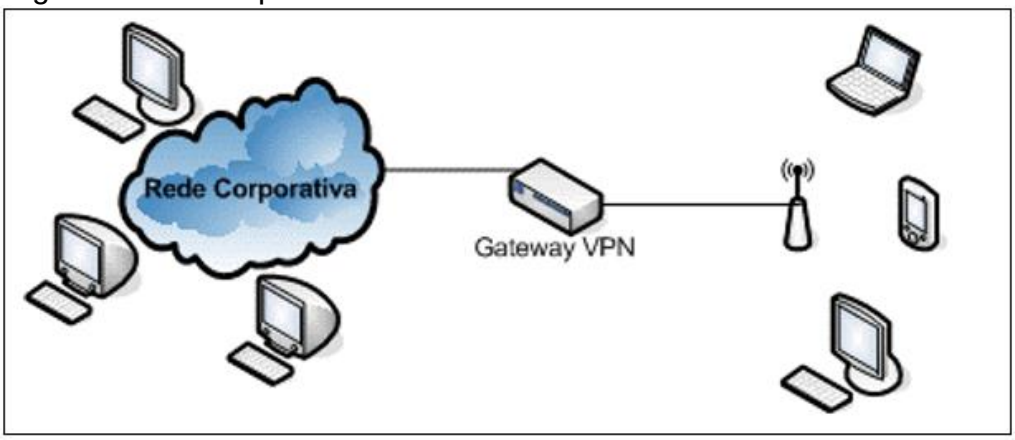
A grande maioria destas redes utiliza o protocolo IPSec para construir o canal seguro. A principal função do IPSec é fazer o roteamento das mensagens por um túnel cifrado, através da inserção de dois cabeçalhos especiais após o cabeçalho IP de cada mensagem (JUNIOR et al, 2004).

Antes do pacote ser transportado ele é criptografado, de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado viaja através da Internet até alcançar seu destino, onde é decifrado, retornando ao seu formato original (JUNIOR et al, 2004).

Além da criptografia, as VPNs oferecem a autenticação dos usuários, outro item de muita importância quando se trata de segurança no tráfego de dados. É feita uma verificação na identidade do usuário, permitindo acesso somente a clientes cadastrados (GIMENES, 2005). A Figura 11 exibe um exemplo de utilização de VPN com dispositivos wireless.

Neste exemplo os clientes conseguem fazer conexões seguras (com o IPSec) para dentro da rede corporativa, através de gateway VPN. Este gateway ainda pode ter um firewall integrado para filtrar e bloquear o tráfego.

Figura 11 – Exemplo de uma WLAN com VPN.



Fonte: Junior et al. (2004).

As VPNs podem oferecer uma opção segura para transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança (JUNIOR et al, 2004).

Todavia, a escolha por este tipo de rede deve ser muito bem analisada, pois podem ocorrer problemas de desempenho e atrasos na transmissão.

3.9.6 Firewalls

De acordo com Aguiar (2005), os firewalls são componentes fundamentais para garantir a segurança de uma rede sem fio. Através dele pode-se controlar todo o tráfego de dados que entra e sai da rede, de forma seletiva, de acordo com um conjunto de regras previamente estabelecidas em sua configuração.

O firewall também pode assumir o papel de gateway entre duas redes, podendo estas redes ser uma wi-fi e a outra LAN. Desta forma é possível isolar as duas redes, evitando que pessoas não autorizadas que possuem acesso a uma rede não tenha o mesmo privilégio em acessar à outra. Assim bloqueia-se o tráfego que ocorre do lado wi-fi para a LAN e da LAN para wi-fi (JUNIOR et al, 2004).

Além disso, um firewall é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior dos acessos às redes (JUNIOR et al, 2004).

3.9.7 Senhas descartáveis (One-time Password - OTP)

Tratando-se de mecanismos de segurança em redes sem fio, há dois pontos principais a serem protegidos: o conteúdo das informações e o acesso ao equipamento do usuário. O uso da criptografia tenta sanar o primeiro problema, mas se o atacante acessar o equipamento do usuário, a segurança provida pela criptografia tende a ser perdida (RUFINO, 2005).

Desta forma, cabe ao administrador proteger o equipamento com tecnologias de firewall, antivírus, anti-spyware e principalmente fornece mecanismos de autenticação baseados em senhas descartáveis, tokens e cartões processados (smartcards) ou fazer uso de dispositivos biométricos (RUFINO, 2005).

De acordo com o autor, as senhas descartáveis são simples e de fácil implementação. A ideia é permitir que o usuário informe uma senha diferente a cada acesso, tornando ineficiente a captura da senha pela rede, visto que será informada uma senha diferente da atual no próximo acesso.

O processo de criação das senhas descartáveis inicia-se quando o servidor envia uma informação como desafio. Este desafio é recebido pelo cliente, que o concatena com a senha secreta. Sobre este valor é aplicada uma função criptográfica, gerando a senha descartável a ser utilizada pelo cliente somente nesta seção. O servidor realiza um cálculo semelhante e verifica se o valor recebido do cliente corresponde ao calculado localmente. Se o valor recebido for válido, o cliente é autorizado a utilizar o sistema (RUFINO, 2005).

3.9.8 Certificados digitais

Segundo Aguiar (2005), os certificados digitais associam a identidade de alguém a um par de chaves eletrônicas (privada e pública) que, usadas em conjunto, fornecem a comprovação da identidade desta pessoa. É uma versão eletrônica (digital) de uma Carteira de Identidade.

Estes certificados são sempre lembrados como um dos métodos de autenticação mais seguros, principalmente quando armazenados em dispositivos processados como tokens ou cartões.

Ainda, segundo o autor, um certificado digital contém três elementos:

a) Informação de atributo: informação sobre o objeto que é certificado. No caso de uma pessoa, o seu nome, nacionalidade, etc.
b) Chave de informação pública: esta é a chave publicada na Autoridade Certificadora. O certificado atua para associar a chave pública à informação de atributo.
c) Assinatura da Autoridade Certificadora: a Autoridade assina os dois primeiros elementos, validando-os.

Entre os métodos de EAP citados nos capítulos anteriores, alguns permitem o uso de certificados digitais. O mais diretamente associado a esses recursos é o EAP_TLS, que permite autenticar o usuário em função de informações disponíveis nos certificados.

3.9.9 Token e SmartCard

Algumas formas de autenticação utilizam dispositivos físicos para armazenarem informações confidenciais como chaves privadas e senhas, na tentativa de impedir uma possível captura no computador do cliente. Como exemplos destes dispositivos podemmos citar os tokens e os smartcards. O token é um dispositivo pequeno, do tamanho de um chaveiro, que pode ser usado para armazenar IDs digitais e dados de autenticação. Para acessar o seu ID digital, basta conectar o token a uma porta USB no computador ou dispositivo móvel. O token pode incluir um teclado numérico, que permite digitar um número de identificação pessoal (PIN). A figura 12 mostra um token de autenticação. O Smartcard é um dispositivo portátil (cartão) que possui uma CPU, uma porta I/O e memória não volátil que só pode ser acessada pela CPU do cartão. Este dispositivo fornece um nível alto de segurança (AGUIAR, 2005).

Figura 12 – Token e SmartCard

Fonte: Elaborada pelo autor.

3.9.10 Detecção de ataques e monitoramento

Segundo Rufino (2005), a ação de segurança mais importante é o correto monitoramento do ambiente. Porém, o monitoramento também pode falhar em algum momento. Ao optar em qual setor devem ser aplicados os investimentos em segurança, certamente mecanismos de monitoramento devem ter prioridade, porque

eles irão detectar pontos de falha, bem como poderão analisar como um determinado ataque ocorreu ou foi bloqueado.

Um erro comum é o monitoramento apenas dos padrões utilizados no ambiente, propiciando ataques que utilizam exatamente algum padrão não existente.

3.9.10.1 – wIDS

Esta ferramenta consegue detectar não somente tipos comuns de ataques, mas também irregularidades em geral, como repetidas requisições para associação com um determinado concentrador. O wIDS está disponível para qualquer tipo de placas e chipsets, bastando a interface poder entrar em modo monitor (AGUIAR, 2005).

Para Rufino (2005), os tipos de tráfego suspeito monitorados por esta ferramenta são:

a) Análise do intervalo de tempo entre os BEACONS de cada concentrador encontrado;
b) Detecção de requisições provenientes de varredura;
c) Detecção da frequência de requisições de reassociação;
d) Detecção de grande volume de requisições de autenticação em um pequeno intervalo de tempo.

3.9.10.2 Garuda

É uma ferramenta que facilita a criação e mudança das assinaturas dos pacotes suspeitos analisados. Entretanto somente aceita placas do padrão aironet (GARUDA, 2004).

O Garuda ainda possibilita a integração com uma base de dados em MySQL. Sendo assim, as informações sobre pacotes suspeitos serão armazenadas no banco.

3.9.10.3 Kismet

Usualmente aceita como uma ferramenta para varredura e ataque, o Kismet agrega mecanismos que o tornam um grande aliado de monitoramento e detecção de ataques (COZER, 2006). Dentre as suas principais funções, destacam-se:

a) Identificação de ferramentas de ataque (Netstumbler e AirJack);

b) Detecção de tráfego irregular;

Visto que a ferramenta pode ser integrada a dispositivo GPS, o Kismet informa a localização física de um possível atacante.

3.9.10.4 Snort – Wireless

É uma tradicional ferramenta para identificar possíveis ataques baseados em assinaturas, pacotes mal formados e tráfego suspeito. Trata-se de um sistema de detecção de intruso que é capaz de fazer o registro dos pacotes e a análise do tráfego de uma rede em tempo real. Esta ferramenta consegue executar análise do protocolo e faz combinações que podem detectar uma variedade de ataques, como varredura feita por ferramentas como o NetStumbler e a presença não autorizada de um concentrador na área de abrangência da rede (RUFINO, 2005).

3.9.10.5 Honeypots e Honeynets

Honeypots são redes monitoradas com a finalidade de serem atacadas e comprometidas, para que seja possível analisar as atividades de invasão que sejam efetuadas contra as mesmas. Assim é possível compreender as técnicas utilizadas na realização de ataques a redes de computadores (GRÉGIO, 2005).

Segundo o autor supracitado, os honeypots podem ser classificados como de alta interação e baixa interação. Honeypots de alta interação são aqueles constituídos de um computador com um sistema operacional instalado, simulando um sistema de produção real. Isso permite que um invasor possa interagir totalmente com o sistema atacado e explorar as vulnerabilidades dos programas e serviços em execução neste sistema.

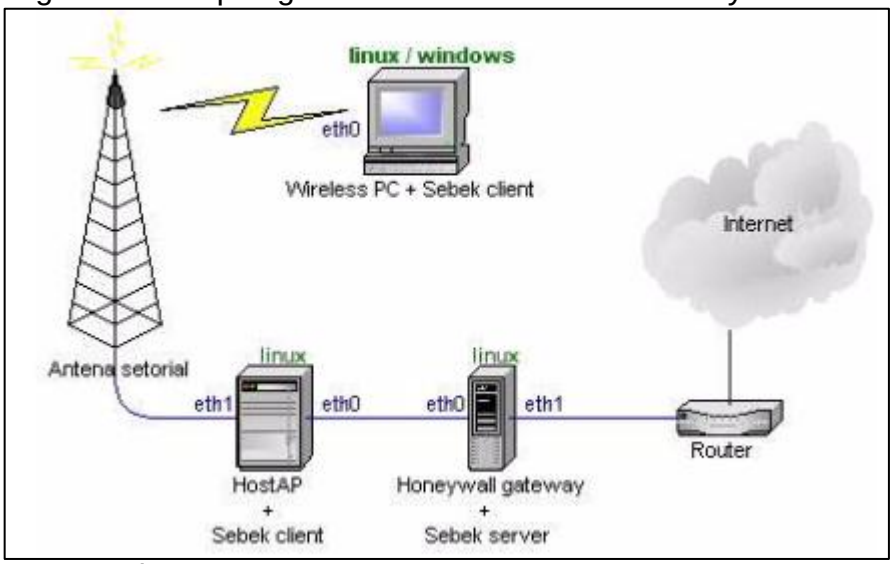
As honeynets são um tipo peculiar de honeypot de alta interação, mais complexo, consistindo de uma rede real configurada com uma quantia considerável

de ferramentas de monitoramento assim como vemos na Figura 13. A tecnologia de honeynets evoluiu, tornando a implementação e o gerenciamento mais simples pela combinação do controle e captura de dados em uma só máquina (honeywall) (GRÉGIO, 2005).

A detecção de intrusos em redes de computadores sem fio torna possível a compreensão total da metodologia utilizada por um atacante para invadir e comprometer uma rede sem fio, desde o momento em que é realizada a varredura (scanning) no concentrador de acesso – o início de um provável ataque – até tentativas de apropriação indevida do mesmo ou negativas de serviço (GRÉGIO, 2005).

Desta forma, os ataques poderão ser estudados minuciosamente para fornecer soluções que minimizem seus efeitos nocivos à utilização segura de uma rede sem fio, protegendo a integridade e confidencialidade dos dados.

Figura 13 – Topologia do modelo de wireless honeynet.



Fonte: GRÉGIO (2005).

3.9.10.6 AirMagnet

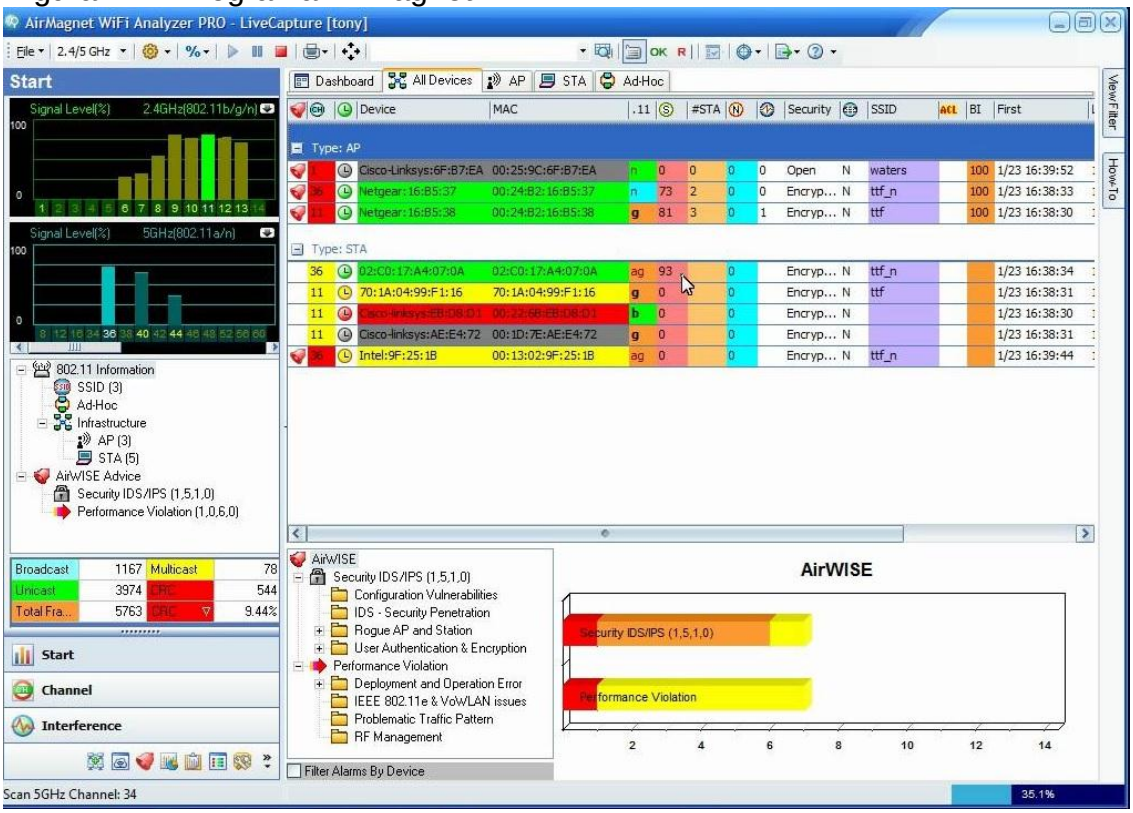
Numa rede wi-fi é possível alguém conectar um AP na rede, se passando por outro dispositivo e desta forma capturar todo o tráfego. Softwares de monitoramento de sinal como o AirMagnet permitem o reconhecimento de dispositivos estranhos conectados à rede, podendo inclusive soar alarmes quando for detectada uma irregularidade (AGUIAR, 2005).

Este software é usado para montar e monitorar redes sem fio. Ele ajuda a organizar a forma da rede e sua segurança, com base em rotinas e tarefas que auxiliam o administrador a entender o ambiente WLAN (GOLEMBIEWSKI et al., 2006).

Quando uma WLAN não é projetada de uma forma correta, as consequências para a taxa de transmissão e a conectividade podem ser desastrosas, gerando problemas de lentidão (delay) na rede. O AirMagnet oferece as ferramentas survey e coverage que dão detalhes dos pontos de acesso e adaptadores de rede wireless, avaliando suas condições de cobertura e tráfego. Também traz ferramentas que possibilitam avaliar a qualidade do sinal e identifica possíveis interferências de locais ou equipamentos desconhecidos. Ele gera um mapa de SSID's (identificadores), com informações de pontos de acesso e estações que estão dentro do alcance da rede (GOLEMBIEWSKI et al., 2006).

De acordo com o autor acima citado, o software ainda oferece arquivos de relatório, que podem ser exportados para o programa Excel, facilitando a criação de gráficos, por exemplo. Na Figura 14 observa-se a interface principal do software, onde são mostrados os campos com uma lista de SSID's, que são os identificadores dos equipamentos que se encontram no raio de cobertura dos APs. Cada campo compreende o nível de sinal, canal de operação, relação sinal ruído (S/R), se possui ou não criptografia e outras funções.

Figura 14 – Programa AirMagnet.



Fonte: Golembiewski et al. (2006).

3.9.11 AirStrike

A arquitetura da WLAN é um aspecto importante para a garantia da segurança dos usuários, do AP e da própria infraestrutura da rede cabeada. O AirStrike tem como compromisso prover segurança durante o acesso a redes sem fio através do ponto de acesso, sem comprometer, com isso, a conectividade dos usuários (AIRSTRIKE, 2007).

O AirStrike é uma solução de segurança para redes sem fio (WLAN) baseada no padrão IEEE 802.11a/b/g. Foi fundamentado no sistema operacional OpenBSD em conjunto com diversos outros softwares de código aberto sobre uma plataforma i386 (AIRSTRIKE, 2007).

Este sistema de segurança gerencia redes sem fio com segurança e confiabilidade, garantindo que somente usuários autorizados terão acesso à rede e que suas mensagens não poderão ser capturadas. Além disso, ele utiliza softwares livres para seu funcionamento, possibilitando um desenvolvimento contínuo e facilitando sua integração com os mais variados ambientes de produção (AIRSTRIKE, 2007).

De acordo com Airstrike (2007), o funcionamento do sistema está relacionado a alguns mecanismos de segurança, como:

a) Autenticação: login e senha inseridos no aplicativo cliente.
b) Autorização: firewall, que através da mudança dinâmica de suas regras permite o acesso seletivo aos recursos da rede.
c) Privacidade e Integridade: IPSec, implementação de uma VPN segura.
d) Dead Peer Detection (DPD) - detecta automaticamente o desligamento de uma estação, e reconfigura as regras de firewall.

O firewall presente no gateway de segurança permite um conjunto restrito de serviços disponíveis às estações da WLAN, dentre eles: DHCP, VPN/IPSec e autenticação. As regras são dinamicamente alteradas após a autenticação de um usuário, de modo a liberar outros serviços ao cliente autenticado. As regras do firewall restringem ao máximo a quantidade de portas abertas. Entretanto, o usuário administrador da rede AirStrike deve configurar essas regras de acordo com as necessidades do seu ambiente de rede e sua política de segurança (AIRSTRIKE, 2007).

4 METODOLOGIA

Nos tópicos a seguir, será apresentada a metodologia proposta para desenvolvimento do trabalho.

4.1 TIPO DE PESQUISA

O trabalho desenvolvido tem por finalidade, com o auxílio da pesquisa e estudo teórico (bibliográfico), explorar a infraestrutura responsável por controlar o tráfego de uma rede sem fio conectada em diversos computadores através da frequência do sinal wireless, e levantar as fragilidades dos protocolos, trazendo informações específicas dos resultados e análises desejados.

Este trabalho foi desenvolvido em três fases:

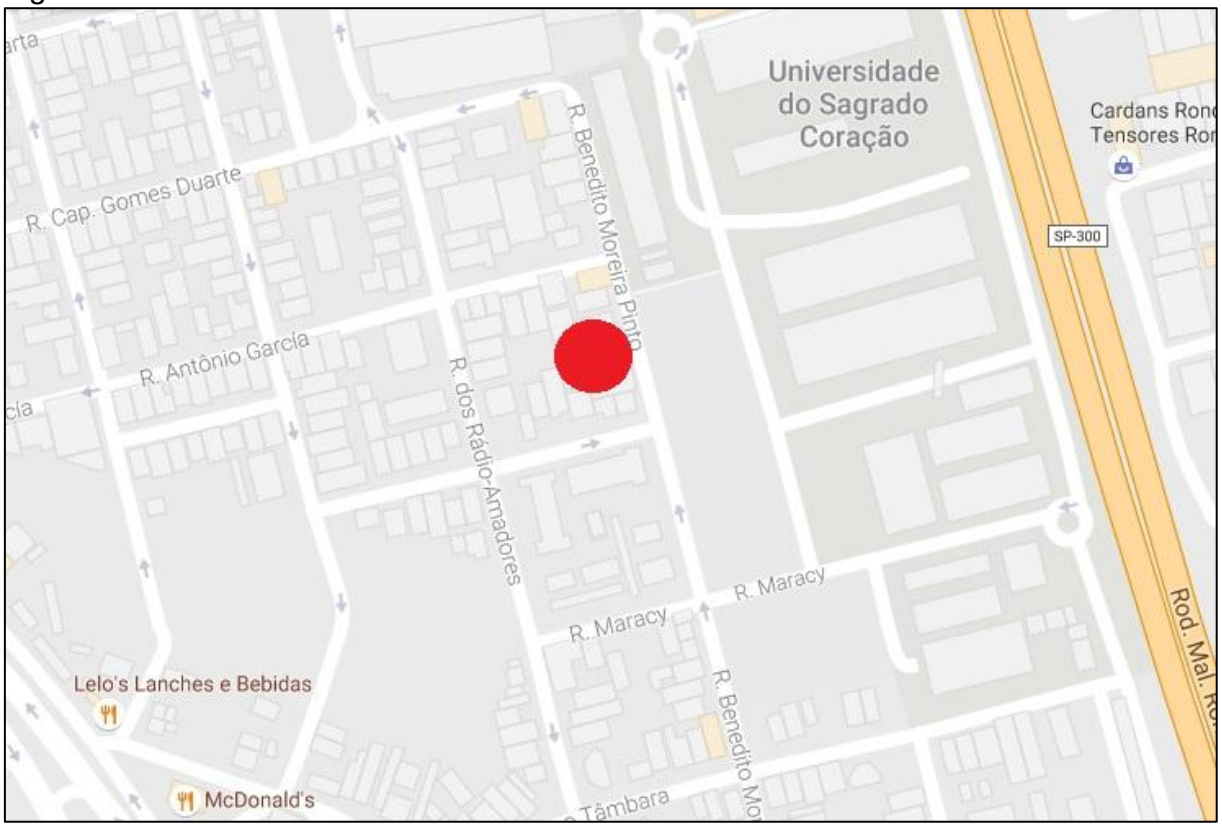
a) Estudo e pesquisa de todo o aspecto teórico envolvendo segurança da informação.
b) Aplicação e realização de uma simulação de invasão, utilizando um ambiente virtual como forma de exemplificar a teoria estudada.
c) Apresentação dos resultados obtidos com o estudo e aplicação prática da pesquisa proposta.

Na primeira fase, foi realizada uma pesquisa detalhada e levantamento de informações a respeito de segurança da informação em geral, abordando os conceitos de realizações de auditorias de segurança, focando a parte de protocolos. Também foram analisados e detalhados os procedimentos das fases e etapas, apresentando as principais ferramentas, metodologias e técnicas empregadas durante sua realização.

Na segunda fase, foi feito um estudo de caso, elaborando um ambiente de busca no local conforme destacado na Figura 15, o qual proporcionou os processos de análise. Nesse ambiente foram realizadas simulações de invasão, de rede doméstica e empresarial, onde geralmente, o usuário tem a impressão de estar conectado em uma rede segura. A região foi escolhida por se tratar de um local com muitas redes wireless, e diante da proposta do projeto, torna-se uma área ideal para os testes.

E na terceira e última fase, foram elaboradas a criação de gráficos e tabelas detalhando as análises e os resultados obtidos, bem como, as considerações finais com os estudos e pesquisas futuras em relação aos temas de fragilidade e segurança em geral na área de informática. Nos tópicos 4.2, 5 e 5.1 estão descritas as informações dos materiais utilizados e a forma como foi conduzida a pesquisa de campo e os resultados obtidos.

Figura 15 – Local de busca de rede sem fio.



Fonte: Google Maps (2016).

Foram detectadas 63 redes wireless ativas, compatíveis para a realização dos testes, sendo 21 WPA2, 21 WPA e 21 WEP.

4.2 RECURSOS

Para a realização desta pesquisa foram utilizados um notebook, marca Asus, processador I3, 3.20GHz (com 4 núcleos reais), 8 Gb de memória DDR3 de 1600 Mhz, 1 disco rígido de 500 Gb com o sistema operacional Windows 10 Pro 64 bit. No sistema operacional Windows 10, foi instalada uma máquina virtual chamada

VMware Workstation (que é um software para emulação e virtualização de máquinas) arquitetura 64 bits, com 4 Gb de memória distribuída, um disco rígido secundário de 80 Gb para a máquina virtual, e o compartilhamento dos 4 núcleos do processador I3 para o desempenho máximo da máquina virtual.

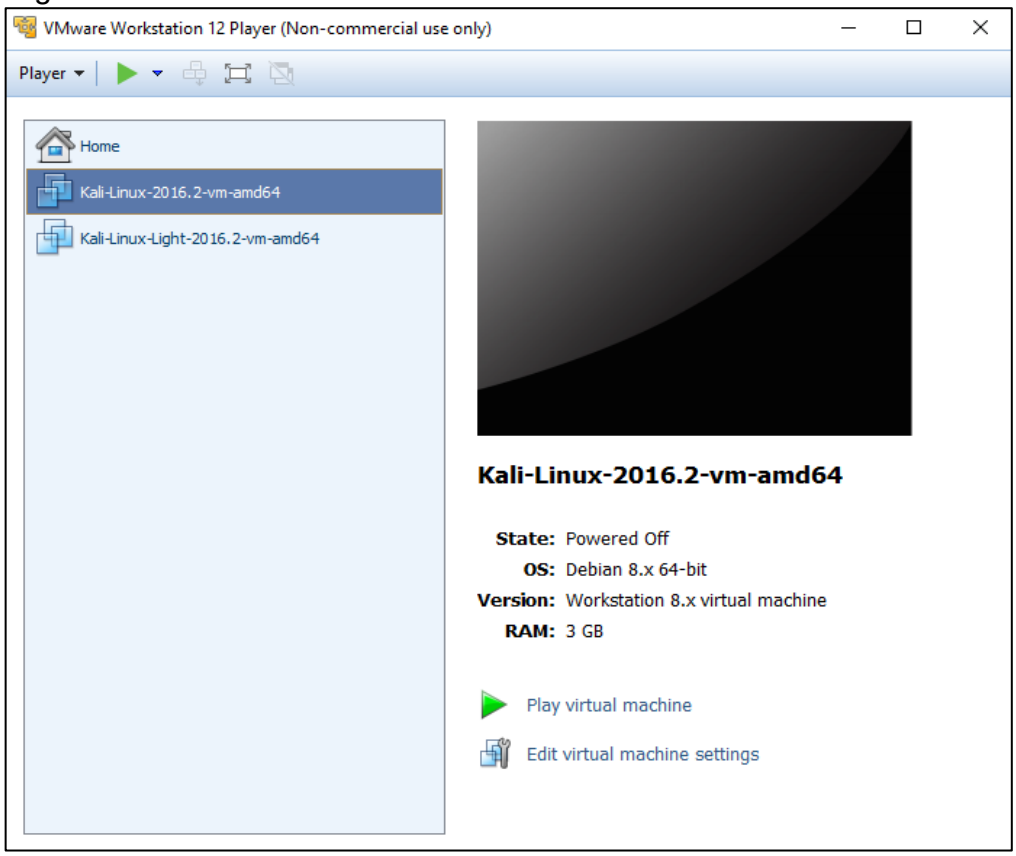
Nesta ferramenta VMware Workstation foi instalado o sistema operacional Kali Linux para a execução e o desempenho requerido. Também foi utilizado um roteador wireless TOTOLINK600 Mbps N601RT 802.11n / a / b / g / n, 2.4G a 5.0Ghz que suporta as criptografias WEP, WPA e WPA2.

Para o reconhecimento da rede sem fio e para a quebra e invasão de sua senha utilizou-se dois adaptadores USB wireless, um TP-Link, modelo TL-8188N 300 Mbps e outro D-link, modelo RTL8192cu para captura de sinais de rede.

5 RESULTADOS

Para verificar as vulnerabilidades existentes nos protocolos WEP, WPA e WPA2 da rede sem fio escolhida, foi usado o sistema operacional Windows 10 (instalado no notebook), o programa VMware (máquina virtual), e o sistema operacional Kali Linux instalado virtualmente conforme demonstra a Figura 16.

Figura 16 – Tela VMware.



Fonte: Elaborada pelo autor.

A escolha do Kali Linux para a execução desse projeto se deve pelo fato do programa além de ser gratuito, ser também um sistema completo, com várias ferramentas e suporte vasto para redes wireless.

Inicialmente, deve-se abrir o terminal e a partir dele, pode-se verificar qual o dispositivo wi-fi usado na máquina pelo o comando airmon-ng.

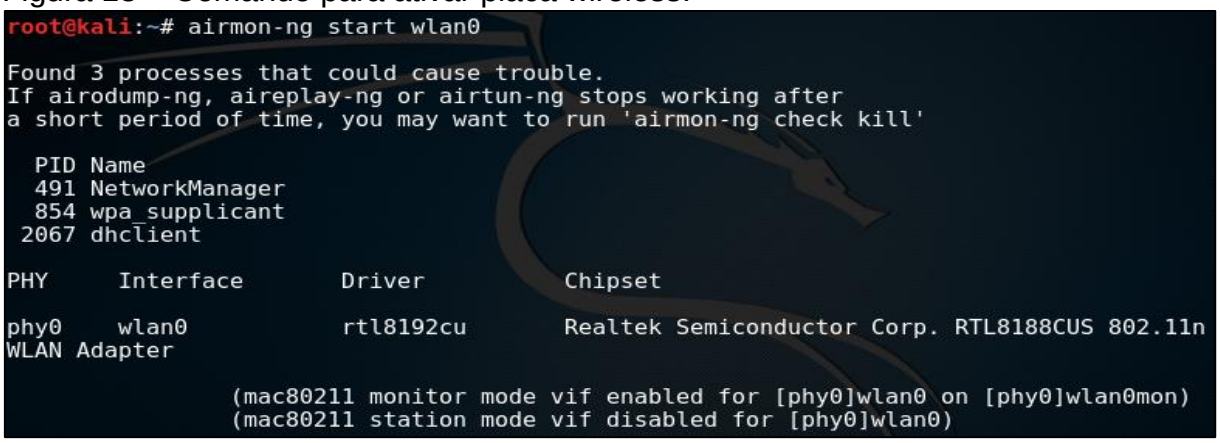
Figura 17 – Comando airmon-ng.

Fonte: Elaborada pelo autor.

Observe que o comando AIRMON-NG executado na Figura 17, já mostra a interface que o dispositivo está montado e qual o chipset e o driver usado pelo dispositivo. Um ponto muito importante para o funcionamento das diversas ferramentas de ataque é que o driver usado seja de máxima compatibilidade com o chipset, ou seja, drivers genéricos pioram o desempenho das ferramentas.

Como foi visto, usando somente o comando AIRMON-NG ele mostra informações do dispositivo. Para iniciar a placa em modo monitor tem-se de usar o comando “airmon-ng start <interface>”. A Figura 18 mostra um exemplo da tela exibida após este comando.

Figura 18 – Comando para ativar placa wireless.

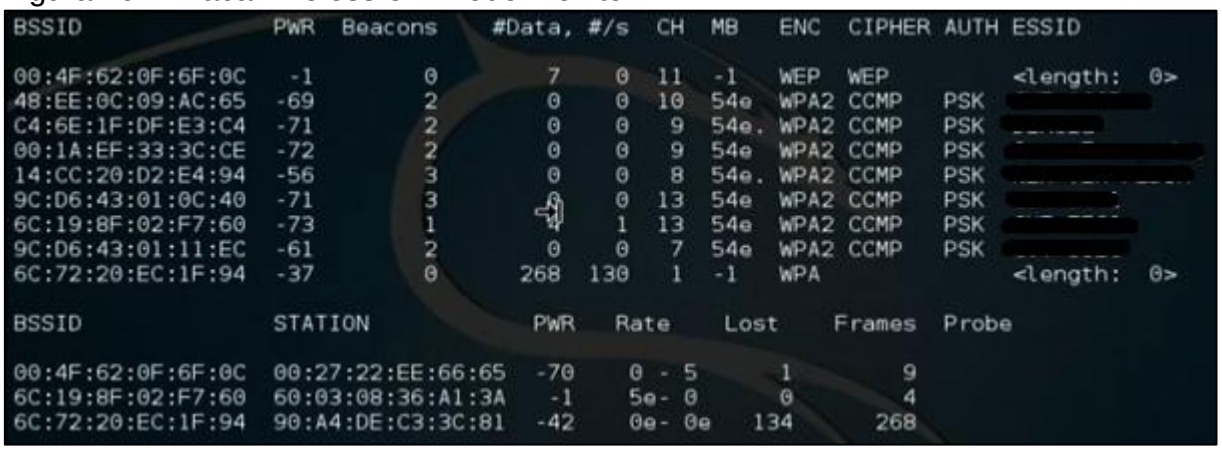


Fonte: Elaborada pelo autor.

Observa-se que são mostrados alguns processos que poderão deixar mais lento o uso da suite AIRCRACK. Para melhor funcionamento das ferramentas, é recomendado excluir estes processos. Junto com as informações dos dispositivos, consta que foi criada uma interface virtual em modo monitor denominada wlan0mon, esta interface é onde serão capturados os pacotes.

Para ver as informações das redes, deve-se executar o comando “airodump-ng wlan0mon”. A Figura 19 mostra o resultado do comando.

Figura 19 – Placa wireless em modo monitor.



Fonte: Elaborada pelo autor.

As informações obtidas com este comando são:

a) BSSID: Número MAC do dispositivo;
b) PWR: Intensidade do sinal captado pelo dispositivo wifi (quanto menor melhor);
c) Beacons: Número de pacotes beacons que o AP enviou;
d) #Data: Número de pacotes de dados capturados (se utilizar criptografia WEP, contagem de IVs), incluindo os pacotes de transmissão de dados;
e) #/s: Número de pacotes de dados por segundo capturados nos últimos 10 segundos;
f) CH: Número do canal que está sendo utilizado no momento;
g) MB: Velocidade máxima suportada pelo AP. Se MB = 11, é 802.11b e MB=54 é 802.11g/n. O ponto (após 54) indica que um preâmbulo curto é suportado. O "e" que vem a seguir o valor da velocidade MB indica se a rede tem QoS habilitado.
h) ENC: Algoritmo de criptografia que está sendo usado. OPN = sem criptografia, "WEP?" = WEP ou superior (não há dados suficientes para escolher entre WEP e WPA / WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estão presentes.
i) CIPHER: A cifra detectada. TKIP é tipicamente usado com WPA e CCMP é tipicamente usado com WPA2.
j) AUTH: O protocolo de autenticação usado.

k) ESSID: Mostra o nome da rede sem fio. O chamado "SSID", que pode estar vazia se SSID oculto é ativado. Neste caso o airodump-ng tentará recuperar o SSID a partir dos probe request e probe response. Neste caso, podemos ver que a primeira rede sem fio mostrada está oculta;

A segunda parte da Figura 19 mostra algumas informações das estações:

a) BSSID: Endereço MAC do AP que a estação está conectada;
b) STATION: Endereço MAC da estação
c) PWR: Intensidade do sinal da interface monitor até a estação mostrada;
d) Rate: Taxa da estação;
e) Lost: O número de pacotes de dados perdido durante os últimos 10 segundos da estação;
f) Packets: O número de pacotes de dados enviados pela estação;
g) Probe: ESSID do AP que a estação está conectada;

Com o AIRODUMP-NG é possível fazer vários filtros, como pelo MAC, canal, escrever os dados capturados em arquivos. Alguns destes filtros serão mostrados nos testes adiante.

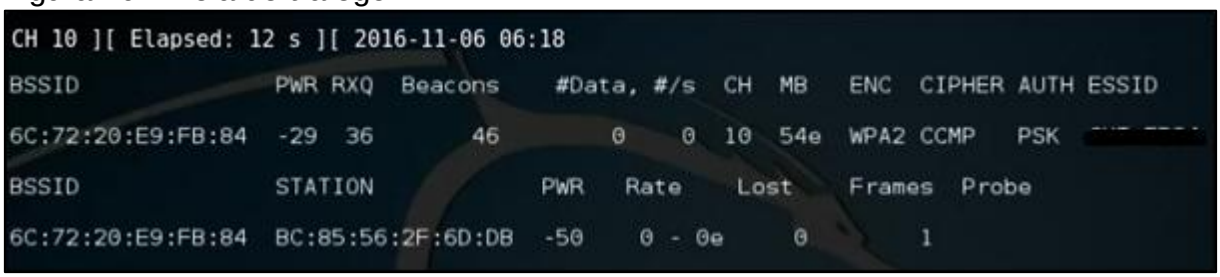
Depois de colocar a interface em modo monitor e encerrar todos os processos que podem interferir no andamento do ataque, executou-se o “airodump-ng” com a seguinte sintaxe: “airodump-ng –w GVT-TESTE -c 10 --bssid 6C:72:20:E9:FB:84 wlan0mon”.

Onde os comandos significam:

a) --bssid: Número MAC do AP alvo;
b) -c 11: Canal que o AP está usando;
c) -w: arquivo onde o programa irá escrever as informações capturadas;
d) Wlan0mon: interface utilizada para capturar as informações;

Este comando irá filtrar somente o trafego do AP destinado à realização deste trabalho. Como pode-se verificar na Figura 20 o que foi mostrado após o comando:

Figura 20 – Tela de tráfego.

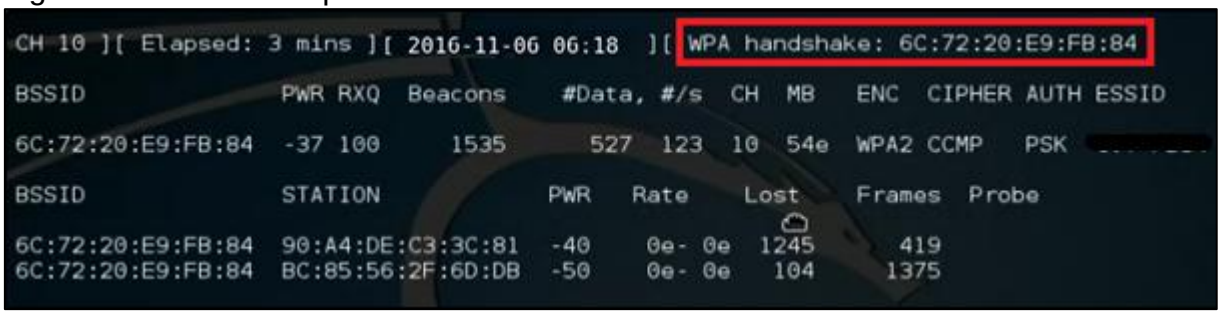


Fonte: Elaborada pelo autor.

Ao enviar uma mensagem para desautenticar a estação conectada ao AP, captura-se o handshake. A sintaxe é a seguinte: “aireplay-ng -0 10 -a 6C:72:20:E9:FB:84 -b BC:85:56:2F:6D:DB wlan0mon“

Se o AIRODUMP-NG conseguir capturar o handshake, ele irá mostrar no canto superior direito da tabela, como mostra a Figura 21.

Figura 21 – Tela de captura do handshake.



Fonte: Elaborada pelo autor.

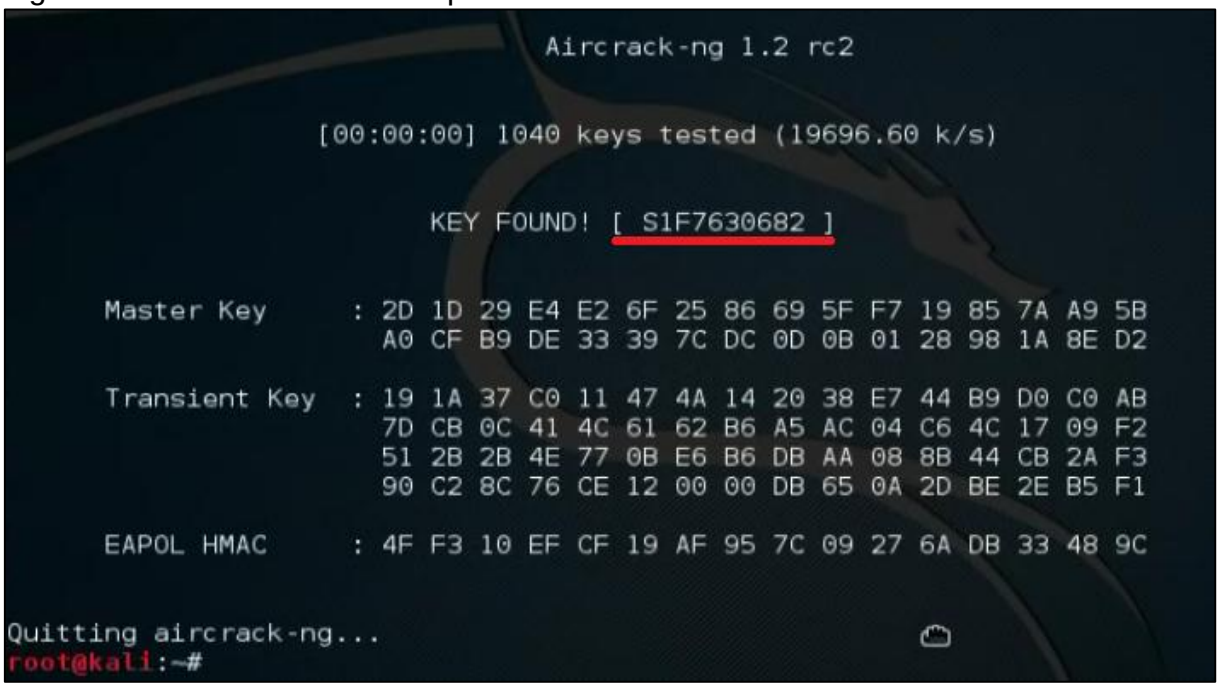
Após a captura do handshake, os dados são gravados em um arquivo, é usado um dicionário para tentarmos quebrar a senha do AP. O comando possui a seguinte sintaxe: “aircrack-ng GVT-TESTE01.cap -w dicionario.txt“.

Onde os comandos significam:

a) GVT-FB84-01.cap: arquivo contendo as informações do handshake escrito pelo airodump-ng;
b) -w: Arquivo com o dicionário usado;

Se o dicionário contiver a senha, será exibida a seguinte tela como mostra a Figura 22.

Figura 22 – Tela com a senha quebrada.



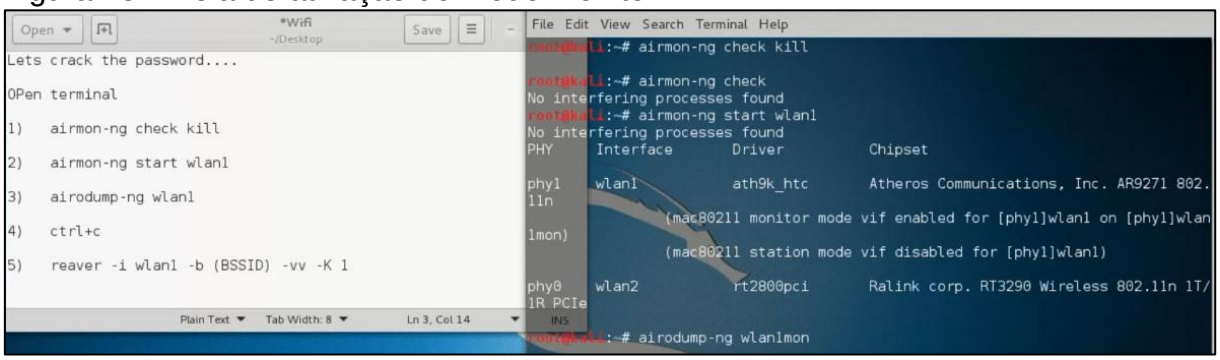
Fonte: Elaborada pelo autor.

Observe que com a ajuda do dicionário, a senha encontrada foi: “S1F7630682”.

Para alguns protocolos (em especial com WPS) foi usado o comando REAVER.

Na Figura 23 poderá ser observado a ativação da placa wireless em modo monitor através do comando: “airodump-ng wlan1mon”.

Figura 23 – Tela de ativação do modo monitor.



Fonte: Elaborada pelo autor.

A Figura 24 mostra o BSSID, o canal, a intensidade do sinal (RSSI) e o ESSID. Para começar o ataque de força bruta com o reaver, foi usado o seguinte comando: “reaver -i wlan1mon -b A4:2B:8C:62:17:AA –vv – K 1”.

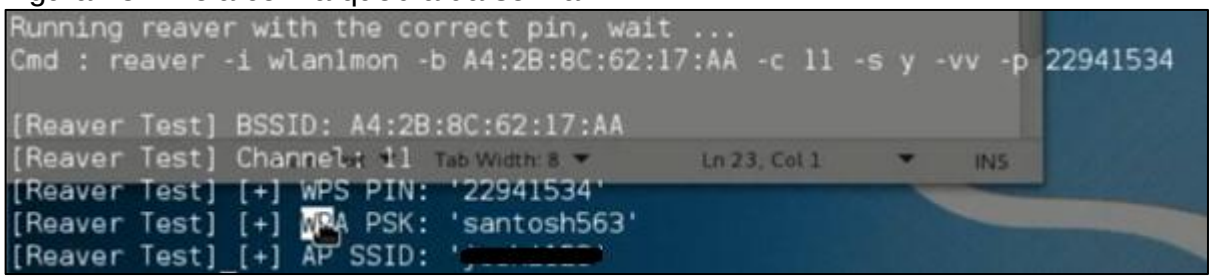
Figura 24 – Tela de monitoramento e comando de quebra.

Fonte: Elaborada pelo autor.

Existe também um parâmetro que busca em uma base de dados do programa, números PIN de dispositivos conhecidos, empregando a opção “-a”. Um comando completo para atacar o nosso AP é descrito abaixo: “reaver -i wlan1mon -b A4:2B:8C:62:17:AA -c 11 –a”.

Se o programa obtiver êxito ele irá exibir a seguinte tela conforme retrata a Figura 25.

Figura 25 – Tela com a quebra da senha.



Fonte: Elaborada pelo autor.

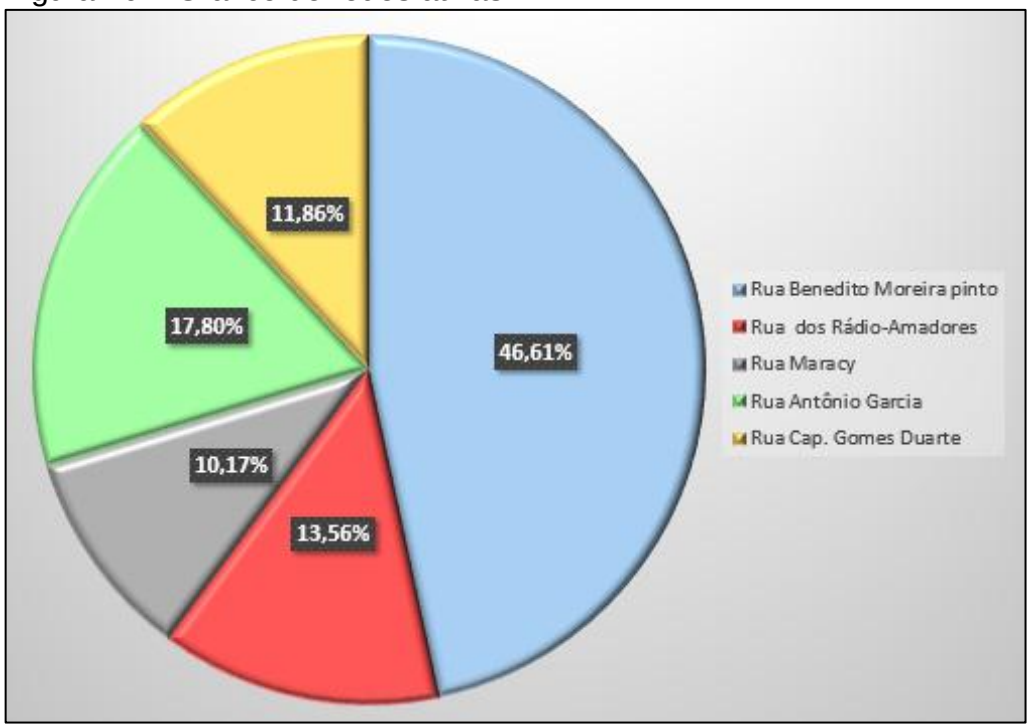
Observe que depois de quebrado o número PIN, é informada as demais configurações (ESSID e senha PSK).

5.1 ANÁLISES

Para começar a pesquisa, foi necessário um levantamento minucioso de dados com o objetivo de quantificar as redes sem fio disponíveis identificando suas formas de segurança implementada e até mesmo a ausência desses recursos.

Em um primeiro momento fez-se necessário verificar a quantidade geral de redes sem fio disponibilizadas na região descrita na Figura 15, contabilizando as redes captadas nestes trechos conforme mostrado na Figura 26, e também pode ser verificado na Tabela A em anexo na página 78.

Figura 26 – Gráfico de redes ativas.



Fonte: Elaborada pelo autor (2016).

A Figura 26 em questão traz a representação do número de hotspots encontrados e os valores relativos a estas redes, onde se pode verificar que a maior concentração de redes foi captada entre a Rua Benedito Moreira Pinto com a Rua Antônio Garcia totalizando 64,41% do total de redes encontradas, onde se conclui que vem a ser um ponto bastante susceptível a possíveis invasões e ataques que vão depender da fragilidade dos recursos de segurança que estas redes dispõem. Não diferente em termos de uso, constatou-se que alguns trechos como o caso da Rua dos Rádio-Amadores indo até a Rua Cap. Gomes Duarte também

apresentaram um valor bastante acentuado de usuários que dispõem destas redes representando um total de 25,42% justificando com esse somatório a acentuada utilização de redes sem fio.

Pode-se observar a crescente utilização das redes sem fio na região citada anteriormente, em virtude do barateamento dos equipamentos e da fácil instalação, porém alguns cuidados devem ser tomados no que tange a segurança.

Neste mapeamento, conforme ilustra a Figura 26, foram encontradas redes sem fio disponíveis, que poderiam facilmente servir de alvo de pessoas mal-intencionadas.

Com a melhoria nos equipamentos e configurações que utilizam o meio não guiado para transmitir informações, a preocupação em garantir segurança ficou ainda mais evidente, principalmente com as melhorias e aumento de tráfego que fez da internet o que é hoje. Todos os equipamentos que são implementados em um ambiente de redes wireless já dispõem de certa camada de segurança, objetivando resguardar os ativos da rede e possibilitando o impedimento de invasões, porém esta camada é muitas vezes implementada de maneira equivocada ou por falta de conhecimento técnico citado anteriormente, a fragilidade nos protocolos de criptografia utilizados nestas redes, assim são os casos do WEP e WPA.

Muito se falou nos capítulos anteriores, sobre algoritmos de criptografia, que viessem a aumentar a segurança nas redes sem fio, como é o caso mais popular da utilização do WEP. Entretanto, neste levantamento buscou-se não somente a utilização por parte do WEP como também do WPA e WPA2, onde as vulnerabilidades e fragilidades foram postas em destaque e suas seguranças colocadas em evidências.

Uma das observações a serem destacadas foram em relação ao número de protocolos WEP e WPA encontradas na região apresentada na Figura 15, onde essa quantidade representa um fator um tanto preocupante, pois, como mostra a Figura 27, muitas redes foram captadas utilizando-se destes algoritmos e revelando uma parcela não tanto segura uma vez que, a utilização do WEP já foi comprovada como sendo uma das mais inseguras.

A insegurança se deve a inúmeros fatores, porém o mais evidente e comentado em capítulos anteriores é o da fragilidade encontrada no algoritmo implementado no protocolo WEP, onde o algoritmo conhecido como RC4 revela inúmeras falhas de segurança.

A divisão da Tabela 2, representa os tipos de criptografia utilizadas nas redes captadas, ficando suas contabilizações divididas por trecho, ou seja, buscou-se o agrupamento das redes pelo algoritmo criptográfico utilizado, uma vez que um dos objetivos desta pesquisa era justamente contabilizar as redes que utilizam os mesmos. Nesta coleta é fácil perceber a enorme utilização do protocolo WEP e WPA ficando este levantamento bastante evidente no que se refere à fragilidade na segurança dessas redes, representando parcela significativa durante esta análise.

Tabela 2 – Criptografias encontradas.

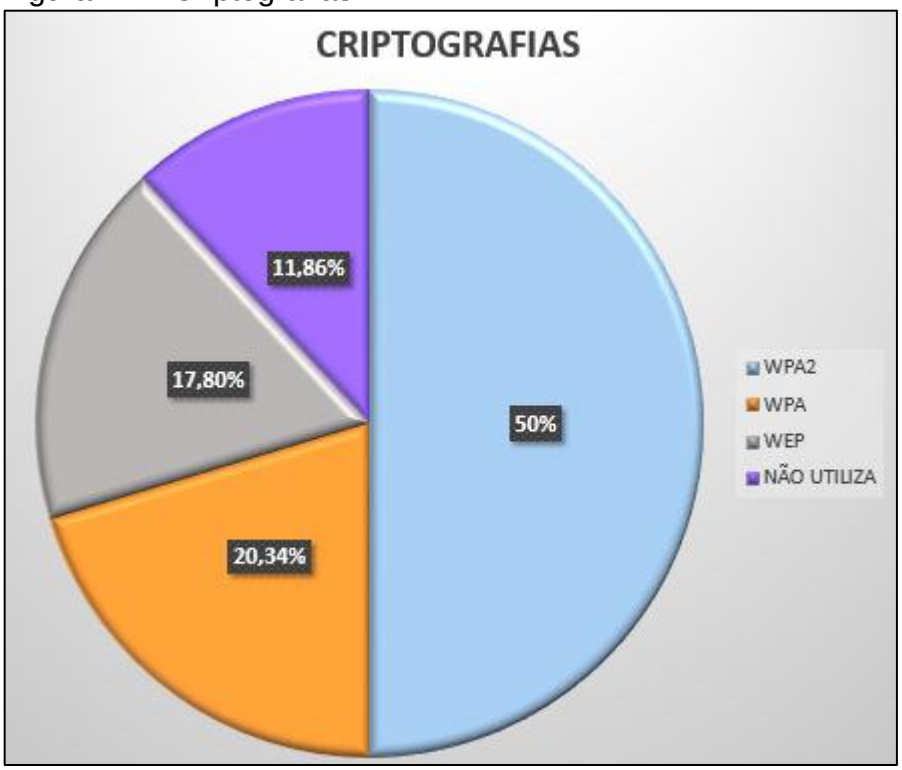
CRIPTROGRAFIAS ENCONTRADAS					
LOCAL DE BUSCA	**WPA2**	**WPA**	**WEP**	**SEM CRIPTOGRAFIA**	**TOTAL**
Rua Benedito Moreira Pinto	27	12	10	6	55
Rua dos Rádio-Amadores	9	4	2	1	16
Rua Maracy	7	2	1	2	12
Rua Antônio Garcia	9	4	5	3	21
Rua Capitão Gomes Duarte	7	2	3	2	14
TOTAL	**59**	**24**	**21**	**14**	**118**

Fonte: Elaborado pelo autor

Observando os dados, fica mais facilmente, através de uma análise relativa dos protocolos mais utilizados como mostrado na Tabela 2, buscar identificar os motivos pela escolha de determinado algoritmo por parte dos usuários.

O somatório das redes que ainda possui um algoritmo menos seguro como no caso do WEP e redes sem criptografias ainda é muito grande atualmente como mostra os dados coletados e grande parte deste resultado deve-se a considerações já levantadas anteriormente.

Figura 27 – Criptografias.



Fonte: Elaborado pelo autor (2016).

Como se pode observar na Figura 27, tem uma parcela bastante acentuada também no que se refere aos usuários que utilizam o WPA2, este sendo considerado o mais seguro entre os três, porém ainda reforçando que mesmo este valor sendo considerados alto, os usuários que utilizam os protocolos menos seguro e até mesmo os que não utilizam segurança, somam um valor de 50% do total, evidenciando uma fragilidade bastante considerável.

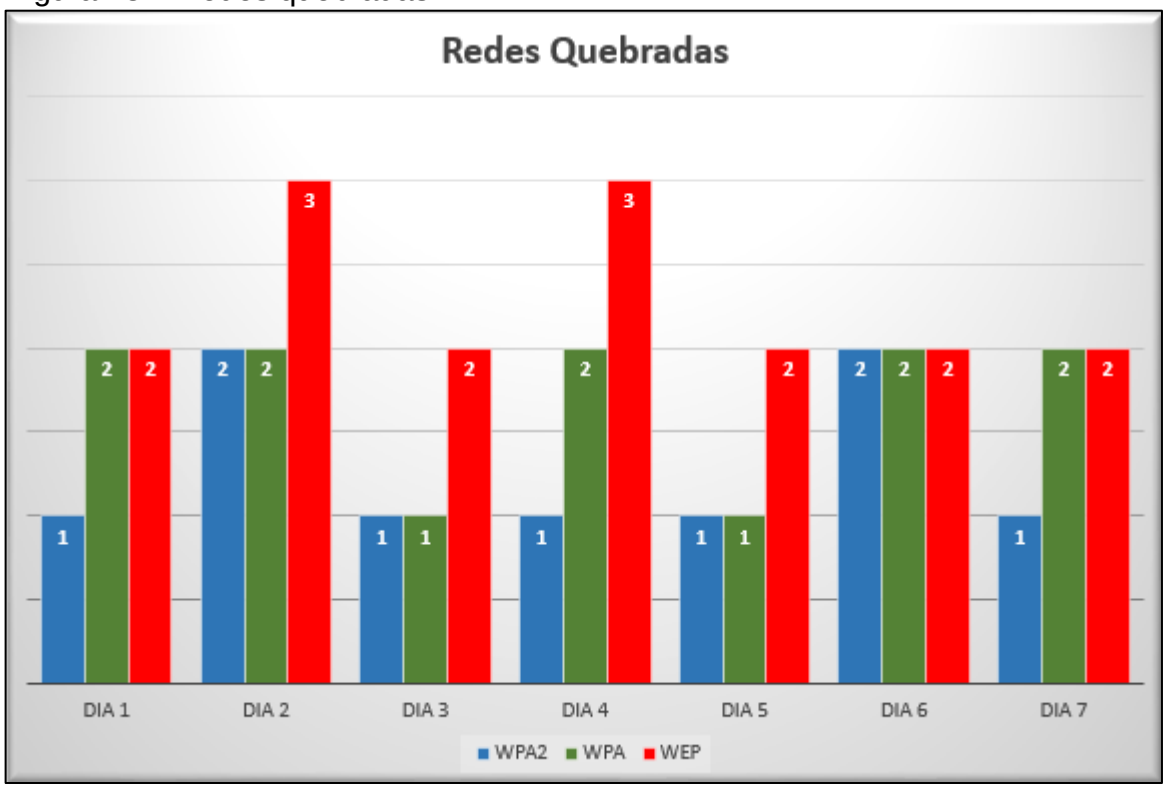
Para essa análise de fragilidade dos protocolos, durante 21 dias, foram realizadas simulações de invasões, sendo 7 dias para cada protocolo, totalizando 63 redes.

As simulações de busca e quebra, se deram por meio de regras estabelecidas mediante a testes anteriores que visavam conhecer o tempo médio de quebra:

a) Tentativa da quebra de até 3 protocolos WPA2 por dia.
b) Tentativa da quebra de até 3 protocolos WPA por dia.
c) Tentativa da quebra de até 3 protocolos WEP por dia.
d) Limite de até 30 metros do sinal.

Após os 21 dias, obteve-se o resultado conforme mostra a Figura 28.

Figura 28 – Redes quebradas.



Fonte: Elaborado pelo autor.

Conforme pode ser interpretado na Figura 27, o protocolo WEP é o mais propenso a fragilidades, pois apresentou pouca resistência aos testes. O WPA e WPA2, apesar de apresentarem algumas dificuldades de quebra, foi possível obter com sucesso o acesso as redes.

Os resultados obtidos na quebra dos protocolos são:

a) 42,85% dos protocolos WPA2 quebrados.
b) 57,14% dos protocolos WPA quebrados.
c) 76,16% dos protocolos WEP quebrados.

Com os resultados alcançados, pode se concluir que a pesquisa obteve sucesso, foi possível a quebra em 58,73% das 63 redes analisadas.

6 CONSIDERAÇÕES FINAIS

A grande facilidade de implantação de rede sem fio possibilitando a mobilidade de dispositivos fez com que crescesse o número de redes sem fio. Por conta desta procura, aumenta também a preocupação com a segurança dos dados transmitido pelo ar. A facilidade de acesso a programas capazes de invadir tornam cada vez mais necessária a utilização de ferramentas como: um bom firewall, um bom antivírus, e o SO (Sistema Operacional) sempre atualizados.

Foi mostrado nessa pesquisa como as redes sem fio são construídas, seus padrões de comunicação existentes e suas vulnerabilidades encontradas. Foram analisados os principais detalhes de uma rede sem fio, suas arquiteturas, topologias, protocolos, mostrando a forma de como deixá-la menos vulnerável aos ataques de pessoas mal-intencionadas.

As redes sem fio não foram criadas para substituir totalmente às redes cabeadas, a mobilidade e produtividade gerada pelas redes sem fio é o ponto fundamental para a superação das redes cabeadas que cresce a cada dia, tanto em ambientes residenciais como corporativos.

Percebeu-se neste estudo que as questões referentes ao padrão mais utilizado nas redes sem fio, vêm mudando porque os fabricantes estão fornecendo produtos já mais seguros, vindo como padrão o 802.11g/n/a/c. Contudo, ainda se vê muitas redes abertas totalmente vulneráveis, não sendo capaz de proporcionar uma boa segurança.

Percebeu-se também que pequenas empresas e residências não sabem nem o que é segurança, eles visam mais a parte financeira. Seus colaboradores só querem ver as redes sem fio funcionando, todos com seus notebooks conectados em rede acessando a internet e com o sorriso de realização e economia.

Foi visto que os protocolos TKIP e WPA e o WPA Enterprise são os mais recomendáveis para ambientes corporativos por utilizar o padrão 802.i, exigindo a utilização de um servidor Radius para autenticação e monitoramento de seus usuários.

Existem ajustes que melhoram substancialmente a segurança em redes wireless, que pode ser desde pequenas mudanças no protocolo de criptografia, até a utilização de redes virtuais privadas que trabalham com túneis de informação criptografados e soluções mais robustas como servidores de autenticação.

Os métodos de invasão comentados nesta pesquisa são os mais frequentemente utilizados por indivíduos maliciosos que procuram, de qualquer forma, explorar as fragilidades das redes sem fio.

Não basta apenas alertar sobre a presença de um intruso, a tecnologia deve ser capaz de prevenir e atuar em tempo real. Consequentemente muitas empresas estão optando por soluções proprietárias com garantia de disponibilidade e integridade dos dados agregando eficiência e segurança.

Se faz necessária a elaboração de políticas de segurança eficientes nas redes wireless considerando todas as particularidades e pontos fracos que levem em consideração as características do ambiente onde a rede será implantada, com diferentes utilizações para as redes wireless tendo necessidades de segurança diferentes, com políticas e procedimentos deferentes.

Assim, pode-se melhorar a segurança nas redes sem fio com acompanhamento da rede, desde a sua idealização até o momento em que a mesma está sendo trabalhada, sempre buscando novas possibilidades de melhorias para elas.

Concluiu-se que nas redes analisadas onde grande parte utilizando-se protocolos de fácil quebra, estas foram as mais sujeitas a várias formas de invasão, devido a seu algoritmo de segurança ser bastante deficitário, e o que mais surpreendeu foi que alguns pontos corporativos se utilizavam do protocolo WEP para tentar resguardar suas informações, uma vez que os protocolos WPA e WPA2 mostraram um nível de segurança bem mais elevado principalmente no que se refere ao algoritmo WPA2, em que as tentativas de quebra de segurança das redes foram demoradas e em algumas sem êxito nas redes que utilizam este protocolo.

7 TRABALHOS FUTUROS

Para trabalhos futuros propõe-se estudo referente aos tipos de criptografias utilizados em redes sem fios, mas com estudo mais aprofundado em redes corporativas e a utilização de outras ferramentas de ataques que não foram abordadas nessa monografia.

A Verificação do ambiente em que as redes sem fio operam, residências, escritórios, empresas, e analise de que modelo de segurança as mesmas utilizam. Verificar o nível de conhecimento e qualificação técnica dos indivíduos envolvidos na instalação e configuração das mesmas. Fazer a coleta em outra região da cidade a fim de fazer comparativos com dados aqui descritos. A segurança sempre será um fator de grande importância nos ambientes computacionais, a busca por uma maior qualidade da mesma deve estar sempre relacionada com profissionais capacitados e equipamento de qualidade.

Por fim sugere-se análise na segurança em outros tipos de redes, como as redes Bluetooth *WI-MAX,* as quais são semelhantes a redes Wi-Fi e também estão expostas a ataques de pessoas mal-intencionadas.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: Tecnologia da Informação - Técnicas de segurança - código de prática para a gestão da segurança da informação. [S. l.]: Associação Brasileira de Normas Técnicas, 2005, p.36.

AIRTRAF. A Wireless 802.11(b) Network Analyzer., 2002. Disponível em: <http://airtraf.sourceforge.net/>. Acesso em: 30 maio 2016.

AMARAL, A. **Redes de computadores**. Colatina: Instituto Federal do Espírito Santo, 2012.

COZER, F. L. **Segurança Redes Sem fio.** 2006. 76f. Monografia (Bacharelado em Ciência da Computação) – Faculdade de Jaguariúna, Jaguariúna, 2006.

DUARTE, L.O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** 2003. 55 f. Monografia (Bacharelado em Ciência da Computação) - UNESP / IBILCE, São José do Rio Preto, 2003.

EDNEY, J.; ARBAUGH, W. A. **Real 802.1 Security: Rede sem fio Protected.Access and 802.11i.** [S.l.]: Addison Wesley, 2003.

ENGST, A.; FLEISHMAN, G. **Kit do Iniciante em Redes Sem Fio**: o guia prático sobre redes Wi-Fi para Windows e Macintosh. 2. ed. São Paulo: Pearson Makron Books, 2005

FERREIRA, J. L. M**. Segurança em Redes sem Fio.** 2013. 67f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

FERREIRA, R. Kali Linux: o sucessor do Backtrack. 2013. Disponível em: http://www.linuxdescomplicado.com.br/2013/07/kali-linux-o-sucessor-do-backtrack.html. Acesso em: 3 jun. 2016.

FOROUZAN, B. A. **Protocolo TCP/IP**. 3. ed. São Paulo: Mcgraw-hill, 2008.

GUIMARAES, D. M. **ANÁLISE DE VULNERABILIDADES FALHAS DOS PRINCIPAIS PROTOCOLOS DE SEGURANÇA DE REDES SEM FIO PADRÃO IEEE 802.11.** 2009**.** 88f. Monografia (Bacharelado em Ciência da Computação) – Universidade Federal Fluminense, Niterói, 2009.

GARUDA. **Documentation.** 2004. Disponível em: <http://garuda.sourceforge.net/>. Acesso em: 2 maio. 2016.

GIAVAROTO, S. C. R.; SANTOS, G. R. **Backtrack Linux**: auditoria e teste de invasão em redes de computadores. Rio de Janeiro: Ciência Moderna Ltda, 2013.

GIMENES, E. C. **Segurança de Redes Wireless**. 2005. 58 f. Trabalho de Conclusão de Curso (Tecnólogo em informática com ênfase em Gestão de Negócios) – FATEC, Mauá-SP, 2005.

GOLEMBIEWSKI, H. S. D; LUCENA, V. F; SAMPAIO, R. B**. Levantamento da área de cobertura de uma rede wireless 802.11:** um estudo de caso na UNED de Manaus**.** I Congresso de Pesquisa e Inovação da Rede Norte Nordeste de Educação Tecnológica. Natal – RN, 2006, 15 p.

GRÉGIO, A.R.A. **Wireless Honeynets**: **Um Modelo de Topologia para Captura e Análise de Ataques a Redes sem Fio.** 2005, 57f. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação. Unesp. São José do Rio Preto, 2005.

IDGNOW. **Hole 196: Falha grave em redes Wi-Fi permite a espionagem de dados**. Disponível em <http://idgnow.uol.com.br/blog/plural/2011/08/22/hole-196-falha-grave-em-redes-wi-fi-permite-a-espionagem-de-dados/>. Acesso em: 9 maio. 2016.

JUNIOR, C. A. C; BRABO, G. S; AMORAS, R. A. S. **Segurança em redes wireless padrão IEEE 802.11b: Protocolos WEP, WPA e análise de desempenho**. 2004, 78f. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação. Universidade da Amazônia, Belém, PA, 2004.

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

LASTBIT Software. **LastBit Corp.**, 1997. Disponível em: <http://lastbit.com/pswcalc.asp>. Acesso em: 26 out. 2014.

MACHADO, W. L. **Simulação da camada física do protocolo IEEE 802.11AC utilizando a ferramenta MatLab.** Monografia de graduação em Engenharia de Redes – Universidade de Brasília, Brasília, 2015.

MORAES, A. F. **Redes Sem Fio - Instalação, Configuração e Segurança**. São Paulo: Editora Érica, 2010.

MORIMOTO, C. E. **Redes - guia prático**. 2. ed. Porto Alegre: GDH Press e Sul Editores, 2011.

NETSTUMBLER. Netstumbler.com 2005-2014. Disponível em: <http://www.netstumbler.com/>. Acesso em: 30 maio 2016.

OLIVEIRA, R. R. **Análise de Vulnerabilidades:** Em redes sem fio IEEE 802.11 com a prática de Wardriving apresentando a necessidade de implementação de protocolos de segurança. 2009, 62f, Monografia da Pós-Graduação em Criptografia e Segurança de Redes – Universidade Federal Fluminense, Niterói, 2009.

RIBEIRO, D. **Como funciona um roteador e saiba quais os tipos existentes**. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/05/como-funciona-um-roteador-e-saiba-quais-os-tipos-existentes.html>. Acesso em: 27 de maio de 2016.

ROSS, J. **O livro do wireless**: um guia definitivo para wi-fi Redes Sem Fio. 2. ed. São Paulo: Altas Books, 2009.

RUFINO, N. M. O. **Segurança em redes sem fio**: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. São Paulo: Novatec, 2005.

_____. **Segurança em redes sem fio**: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 2. ed. São Paulo: Novatec, 2007.

_____. **Segurança em redes sem fio**: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 3. ed. São Paulo: Novatec, 2011.

STALLINGS, W. **Criptografia e Segurança de Redes.** São Paulo: Pearson Prentice Hall, 2008.

TACIO, P. **Endereço Mac**. Disponível em: <http://www.mundodoshackers.com.br/o-que-e-um-endereco-mac >. Acesso em: 4 de abr. 2016.

TANENBAUM, A. S. **Redes de computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003.

WEIDMAN, G. Testes de invasão. São Paulo: Novatec, 2014.

ANEXOS

Tabela A

Tabela 1 – Redes sem fio captadas.

LOCAL DE BUSCA	QUANTIDADE DE HOTSPOT CAPTADOS	
	FA	**FR**
Rua Benedito Moreira Pinto	55	46,61
Rua dos Rádio-Amadores	16	13,56
Rua Maracy	12	10,17
Rua Antônio Garcia	21	17,80
Rua Capitão Gomes Duarte	14	11,86
TOTAL	118	100,00

Fonte: Elaborada pelo autor.

Nota: FA - Frequência Absoluta e FR - Frequência Relativa