CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA

DE MINAS GERAIS - CAMPUS TIMÓTEO

Curso de Engenharia da Computação

Vinícius Cardoso Quintão

SEGURANÇA EM REDES SEM FIO EM PEQUENAS EMPRESAS UTILIZANDO PROGRAMAS GRATUITOS PARA OS ATAQUES DE NEGAÇÃO DE SERVIÇO

Timóteo - MG

2019

Vinícius Cardoso Quintão

SEGURANÇA EM REDES SEM FIO EM PEQUENAS EMPRESAS UTILIZANDO PROGRAMAS GRATUITOS PARA OS ATAQUES DE NEGAÇÃO DE SERVIÇO

Monografia apresentada ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, como requisito para obtenção do título de Bacharel em Engenharia de Computação

Orientador: Maurílio Alves Martins da Costa.

Timóteo – MG

2019

Vinícius Cardoso Quintão

Segurança em Redes Sem Fio em Pequenas Empresas Utilizando Programas Gratuitos para os Ataques de Negação de Serviço

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, campus Timóteo, como requisito parcial para obtenção do título de Engenheiro de Computação.

Trabalho aprovado. Timóteo, 09 de agosto de 2019:

Prof. Dr. Maurilio Alves Martins da Costa
Orientador

Prof. Me. Deisymar Botega Tavares
Professor Convidado

Prof. Me. Adilson Mendes Ricardo
Professor Convidado

Timóteo
2019

Resumo

As redes sem fio, devido ao custo de projeto, facilidade de instalação e mobilidade vem sendo utilizada em ambientes domésticos e corporativos. O trabalho visa as pequenas organizações, que não tem orçamento para investir em equipamentos robustos, consultorias e ferramentas para tratar os incidentes. Um dos ataques que mais afetam as redes sem fio é o de negação de serviço, que utilizam vulnerabilidades do protocolo de transporte TCP e UDP para esgotar os recursos dos equipamentos de rede deixando-os indisponíveis para novas conexões. Foi proposto um procedimento operacional utilizando as ferramentas gratuitas Zabbix e FastNetMon em um ambiente de teste. Esses programas são responsáveis pela notificação e mitigação dos ataques, respectivamente. Para testar as ferramentas foram feitos testes banda utilizando os protocolos TCP e UDP, onde no primeiro foi configurado banda acima de 40 megas e 40 conexões, e no segundo foi configurado banda acima de 90 megas. Com estes parâmetros foi possível detectar ataques de negação de serviço do tipo TCP SYN Flood e UDP Flood, verificando o aumento de latência, banda, processamento e perda de pacote. Assim o zabbix e o fastnetmon foram configurados para notificar e mitigar qualquer anomalia nestas variáveis gastando em média 63 segundos para TCP SYN Flood e 72 segundos par a UDP Flood. Com isso percebemos que é possível ajudar os pequenos empresários a aumentarem o nível de segurança contra ataques de negação de serviço em redes sem fio utilizando as ferramentas gratuitas aplicadas no processo operacional.

Palavras-chave: Redes sem fio, Negação de serviço, Zabbix, Fastnetmon, Monitoramento, Pequenas organizações, Notificação, Mitigação, UDP e TCP.

Abstract

Wireless networks, due to their design cost, ease of installation and mobility, have been used in both home and corporate environments. The work is aimed at small organizations, which have no budget to invest in robust equipment, consulting and tools to handle incidents. One of the most damaging attacks on wireless networks is denial of service, which uses TCP and UDP transport protocol vulnerabilities to deplete network equipment resources and make them unavailable for new connections. An operational procedure has been proposed using the free Zabbix and FastNetMon tools in a test environment. These programs are responsible for notification and mitigation of attacks, respectively. To test the tools bandwidth tests were performed using the TCP and UDP protocols, where in the first band was configured above 40 megs and 40 connections, and in the second band was configured above 90 megs. With these parameters it was possible to detect TCP SYN Flood and UDP Flood denial of service attacks, verifying increased latency, bandwidth, processing and packet loss. Thus zabbix and fastnetmon were configured to notify and mitigate any anomaly in these variables spending on average 63 seconds for TCP SYN Flood and 72 seconds for UDP Flood. From this we realize that it is possible to help small business owners to increase the level of security against denial of service attacks on wireless networks by using the free tools applied in the operational process.

Keywords: Wireless Networks, Denial of Service, Zabbix, Fastnetmon, Monitoring, Small Organizations, Notification, Mitigation, UDP and TCP.

LISTA DE FIGURAS

LISTA DE SIGLAS

ACK – Acknowledge

AES – Advanced Encryption Standard

AP – Access Point

CEFET – Centro Federal de Educação Tecnológica

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CPF – Cadastro de Pessoa Física

CPU – Central Processing Unit

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

DES - Data Encryption Standard

DFIR – Diffused Infra-Red

DNS – Domain Name Service

DoS – Denial of Service

DSSS – Direct Sequence Spread Spectrum

EAP – Extensible Authentication Protocol

FHSS – Frequency Hopping Spread Spectrum

GPS – Global Positioning System

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Security

IEEE – Institute of Eletrical and Eletronic Engineers

ISM – Industrial Scientific Medical

MAC – Media Access Control

NAT – Network Address Translation

NIST – National Institute of Standards and Technologies

OFDM – Orthogonal Frequency Division Multiplexing

OTP –On-time password

PDU –Protocol Data Unit

PFS – Perfect Forward Secrecy

PSK –Pre-Shared Key

PSPF –Publicly Secure Packet Forwarding

QoS – Quality of Service

ROI –Return On Investment

RSN – Robust Security Network

SSID – Service Set Identifier

SSL – Secure Sockets Layer

SYN – Synchronize

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TKIP –Temporal Key Integrity Protocol

UDP – User Datagram Protocol

WEP –Wired Equivalent Privacy

WPA –Wi-Fi Protected Access

Sumário

1. INTRODUÇÃO

As redes de computadores estão presentes na vida da sociedade há muito tempo. De acordo com Torres “[...] as redes não são uma tecnologia nova. Elas existem desde a época dos primeiros computadores [...]” (TORRES, 2011, p. 5). Surgiu com objetivo de suprir a necessidade de transmitir e receber informações de diferentes pessoas que podem estar em lugares diferentes de forma rápida. A partir disso, pode-se dizer que uma rede de computadores “[...]é um conjunto de computadores autônomos interconectados por uma única tecnologia.” (TANENBAUM, 2003, p.18). Tal interconexão pode ser cabeada ou sem fio.

O objeto de estudo deste trabalho são as redes sem fio ou wireless, este tipo de rede utiliza o ar como forma de transmissão dos dados utilizando equipamentos de radiofrequência ou infravermelho. Moraes (2010) relata que “nos últimos 15 anos temos observado um crescimento exponencial da utilização de tecnologias baseadas em redes sem fio, computadores móveis, telefones celulares, acesso à Internet por redes 3G e smartphones”. (MORAES, 2010, p.15). De acordo com Rufino (2011), tal crescimento é baseado na sua mobilidade e praticidade. Além do baixo custo de instalação e manutenção, na escalabilidade e, no mais importante, a não necessidade da estrutura de cabeamento. Porém existe uma vulnerabilidade em relação a este tipo de rede: a utilização do ar como forma de propagação, que de acordo com Moreno (2016) juntamente com a escolha de criptografia e escolha de senha deixa as informações vulneráveis a ataques caso não tenha sido feita uma análise do ambiente em que a rede será inserida, da configuração e da instalação segura da rede, dentre outros fatores. Com isso, alguém poderá acessar, analisar, alterar ou destruir as informações, caso não estejam totalmente seguras.

A rede sem fio é um sonho que se tornou realidade para o espião: dados gratuitos sem qualquer trabalho. Por essa razão, não é preciso dizer que a segurança é ainda mais importante para sistemas sem fios que para sistemas fisicamente conectados. (TANENBAUM, 2003, p. 185).

Para manter a segurança da informação é necessário reduzir as vulnerabilidades da rede sem fio. Tais vulnerabilidades ocorrem da seguinte maneira: a rede possui uma falha, o invasor tem acesso ou conhecimento dessa falha e com isso ele explora essa falha, alterando assim a garantia das informações. De acordo com Moraes (2010), essa garantia é baseada em três pilares que formam a segurança da informação, a saber:

- Integridade: é o que garante que a informação não sofreu alterações durante sua transmissão ou armazenamento, sem a autorização do proprietário;
- Confidencialidade: é a proteção que garante que os dados não foram acessados por pessoas não autorizadas;
- Disponibilidade: são mecanismos que vão evitar que o sistema fique indisponível.

Pretende-se neste trabalho realizar testes em um ambiente controlado para ataques de negação de serviço, onde é avaliado o protocolo de comunicação e o tempo de notificação e mitigação incidentes.

1.1 Pergunta de Pesquisa

Com este projeto pretende-se investigar formas de reduzir as vulnerabilidades das redes sem fio favorecendo os pequenos empresários que fazem uso de tais redes, já que em comparação com as redes cabeadas, elas reduzem os gastos e espaço físico. Pretende-se também desenvolver um servidor de monitoramento e segurança com programas open source para auxiliar na notificação e mitigação dos ataques de negação de serviço. Ou seja, como auxiliar as pequenas organizações a identificar e solucionar ataques de negação de serviço com programas gratuitos?

1.2 Objetivo Geral

Este trabalho tem como objetivo geral desenvolver um procedimento operacional para incrementar o nível de **segurança** das redes sem fio para evitar os

ataques de negação de serviço em pequenas empresas utilizando somente programas gratuitos.

1.2.1 Objetivos Específicos

Identificar os principais problemas relacionados à segurança da informação em pequenas empresas;

Identificar equipamentos e programas gratuitos que ajudem na identificação e mitigação de ataques nas redes sem fio;

Desenvolver um processo operacional que notifique e mitigue ataques de negação de serviço em redes sem fio;

Realizar testes de tempo de notificação e mitigação dos ataques.

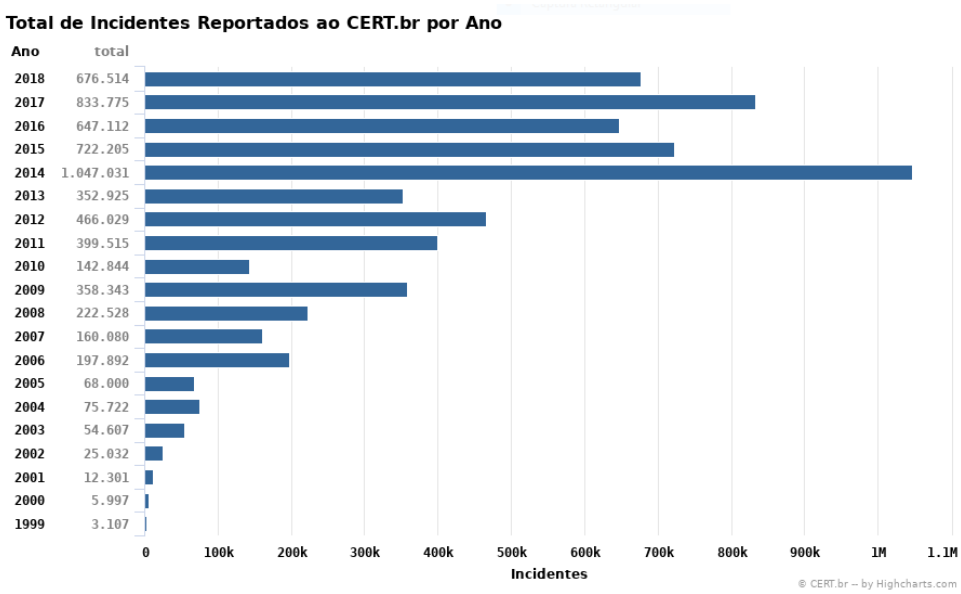
1.3 Justificativa

As informações são o bem mais precioso que uma organização possui, e mantê-las seguras é primordial para que possam alcançar suas metas. Com isso, muitas delas não aderem a uma rede sem fio devido à falta de segurança que ela proporciona.

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira. Mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

De acordo com o CERT.br (Figura 1), pode-se perceber que até o ano de 2018, o número de incidentes cresceu muito em relação aos outros anos, isso mostra que as ameaças relacionadas aos problemas de segurança estão aumentando cada vez mais. A partir disso, percebe-se que a segurança ainda tem que ser implantada e melhorada nas redes de computadores. Mesmo que em alguns anos o número de incidentes tenha caído, ainda é um número muito grande e que deve ser reduzido.

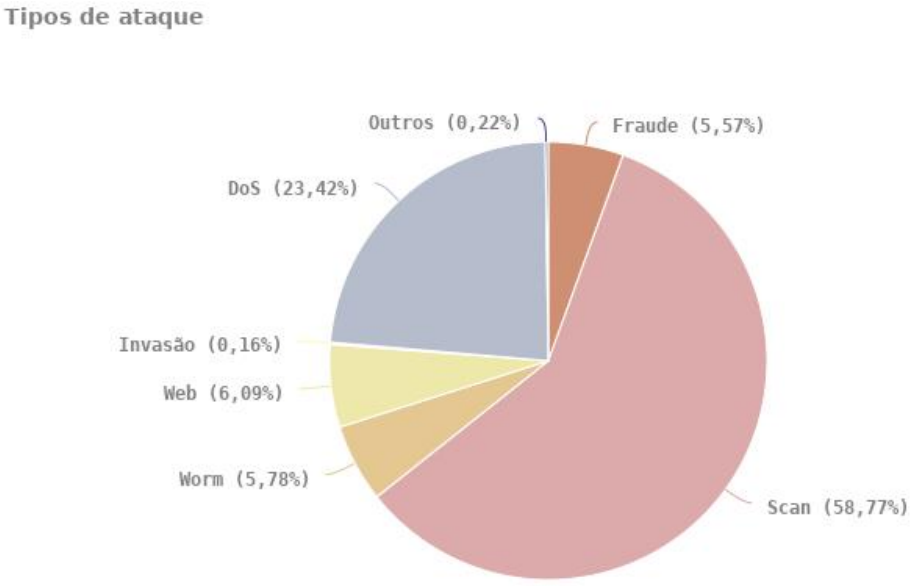
Figura 1 – Total de Ataques Reportados de 1999 até 2018



Fonte: Cert.br, acessado em 2019

Observando outro gráfico do CERT.br (Figura 2), é possível ver que 23,42% dos incidentes reportados são ataques de negação de serviço.

Figura 2 Tipos de ataques reportados de Janeiro a Dezembro de 2018



Fonte: Cert.br, 2019

Baseado no Relatório de Segurança da TI para PME 2018 da Untangle, empresa responsável pelo fornecimento de soluções de segurança de rede para pequenas e médias empresas (SMBs) em todo o mundo, em pesquisa com 350 PMEs 48% haviam restrições orçamentárias, 37% tem tempo limitado para pesquisar e entender novas ameaças e 34% estavam com falta de mão de obra para monitorar e gerenciar a segurança, conforme o gráfico abaixo:

1.4 Apresentação de Trabalho

Este trabalho, que visa a identificação e mitigação de ataques de negação de serviço em redes sem fio, será dividido da seguinte maneira:

No capítulo 2 é mostrado o Estado da Arte.

Nos capítulos 3, 4, 5 é apresentada a revisão de literatura sendo que:

No capítulo 3, o assunto são as redes sem fio, já que é necessário conhecê-la para poder aplicar de maneira correta e eficiente os métodos de segurança;

No capítulo 4, o tema é a segurança da informação que será utilizada junto com os métodos e técnicas de segurança visando reduzir as falhas;

No capítulo 5 ocorre a união dos capítulos 3 e 4, formando assim a segurança em redes sem fio, onde é mais detalhado os conceitos, técnicas, procedimentos e métodos de segurança utilizados para reduzir as vulnerabilidades de uma rede sem fio.

No capítulo 6 é apresentada a metodologia de pesquisa.

No capítulo 7 é discorrido sobre os resultados.

Por fim, no capítulo 8 é apresentada as considerações finais.

2. ESTADO DA ARTE

O tema segurança de redes é um assunto muito extenso e complexo e vem sendo estudado de formas diversas para identificar, prevenir e mitigar ataques. Santos (2015), aborda um estudo de caso com o objetivo de realizar uma análise na segurança de redes sem fio no laboratório de engenharia de redes e comunicação para os incidentes de quebra de criptografia, ataques testes foram realizados aos protocolos WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPA2, como resultado o mesmo indicou a utilização de servidor radius para controle de acesso e utilização de roteadores com funções de QoS (Quality of Service), Nat (Network Address Translation) e lista de controle de acesso como proposta para auxiliar e controlar acessos indevidos ao laboratório.

Os ataques de negação de serviço vêm sendo abordados de diversas formas, utilizando sistemas de detecção de intrusos, firewall; sendo que na maioria dos estudos são utilizadas ferramentas e sistemas gratuitos. Cruz (2013), baseia sua solução utilizando firewall OpenBSD e o sistema de detecção e prevenção de intrusão SNORT para mitigar ataques de negação de serviço utilizando técnicas de detecção, prevenção e intrusão. A ferramenta utilizada para simular o ataque foi o Slowloris HTTP (HyperText Transfer Protocol) DoS (Denial of Service) que mantêm conexões abertas por meio de solicitações HTTP parciais a um servidor deixando sua página web indisponível, enquanto a CPU (Central Processing Unit) e memória permanecem normais. Como resultado, o SNORT conseguiu identificar os ataques através de análises de tráfego das interfaces rede, assim quando houvesse várias conexões ao servidor em um espaço curto de tempo será emitido uma notificação de incidente ao administrador de rede para que faça uma análise e mitigue o ataque.

Enquanto Cruz, Ramos, Vasconcelos e Torres (2013), simula um ataque de negação de serviço utilizando uma máquina Windows como cliente e um servidor debian, Kali Linux. Foram usadas as ferramentas Nmap, Nessus, WhireShark, T50 e Slowloris para descobrir vulnerabilidades, fazer a leitura de pacotes nas interfaces de rede e realizar ataques de negação de serviço, respectivamente. Como resultado, o

mesmo percebeu a falha nos servidores e indicou a utilização de sistemas de detecção de intrusos para defender a rede.

Para Vilela, Shinoda, Ferreira, Oliveira, Nascimento e Araújo (2013), é necessário construir uma base de dados para ajudar os sistemas de detecção de intrusos nas redes sem fio com diversos protocolos de criptografia. Para isso, foi construído dois ambientes de teste sem fio, um com menos equipamentos simulando uma rede doméstica, enquanto no outro havia uma estrutura mais complexa e com mais hosts. Diante disso, foram feitas análises diante do comportamento da rede utilizando os softwares WhireShark e Tshark para monitorar e processar os dados, e a ferramenta Aircrack para realizar os ataques de negação de serviço. Como conclusão, conseguiram identificar o comportamento da rede diante de tráfegos normais e anômalos, ajudando assim em testes de negação de serviço em ambientes de teste.

Enquanto Pinheiro (2014), utiliza uma propriedade do protocolo HTTPS, o PFS (Perfect Forward Secrecy), e o handshake TLS/SSL (Secure Sockets Layer) em ataques de negação de serviço, onde ambos vão gerar novas conexões a cada requisição feita no servidor. O Forward Secrecy utiliza uma chave diferente para cada conexão e o TLS (Transport Layer Security) mantém a integridades dos pacotes através de requisições ao serviço. Com isso, muitos ataques utilizam destas características para gerar diversas conexões até que os recursos do servidor se esgotem. Como conclusão, foi verificado que utilizando o PFS e sem handshake TLS/SSL deixavam o servidor indisponível mais rápido e este valor aumentava de acordo com número de threads utilizadas pelo servidor durante o processo.

3. REDES SEM FIO

Tudo começou em 1888 quando o físico alemão, Heinrich Rudolf Hertz, produziu a primeira onda de rádio. Depois de alguns anos de estudos, mais especificamente em 1894, suas ondas de rádio se tornaram uma forma de comunicação, ajudando no desenvolvimento do rádio, televisão e radar.

Quem fez com que as ondas de rádio de Heinrich pudessem ser transmitidas pelo ar foi um inventor italiano chamado Guglielmo Marconi Marchese, de acordo com Castilho, Antonio e Lamparelli (2014), ele evoluiu as ondas de rádio, ampliando-as, para que pudessem percorrer longas distâncias. Bordim citado por Castilho, Antonio e Lamparelli (2014, p. 5) afirma que “Desde a descoberta das ondas de rádio buscou-se utilizar suas propriedades para a transmissão de dados, permitindo mobilidade e conexões entre localidades remotas”.

Por conseguir transmitir mensagens de forma rápida e por longas distâncias, fizeram com que as ondas de rádio se tornassem uma ferramenta útil durante a segunda guerra mundial, onde o exército americano a usava para enviar os planos de batalha, ou seja, era o meio de comunicação entre as tropas terrestres, marítimas e aéreas, enviando instruções de batalha.

Após a guerra, no ano de 1971, as redes sem fio, segundo Engst e Fleishman (2005, p.11), iniciaram-se de um projeto que ligou as universidades do Havaí que conectavam os computadores de quatro ilhas utilizando a primeira rede local sem fio, chamada de ALOHAnet. Elas entraram para o uso da computação pessoal em 1980, quando começou a se tornar necessário a comunicação e o compartilhamento de informações entre computadores.

As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade em 1991, quando foram criadas tecnologias que permitiram aos computadores suportar tal aplicação. Como estavam sendo criadas diversas redes por diversas pessoas, isso acabou gerando incompatibilidade de comunicação entre elas, devido a isso, de acordo com Augusto e Jara (2011), no meio da década de 90 as atenções

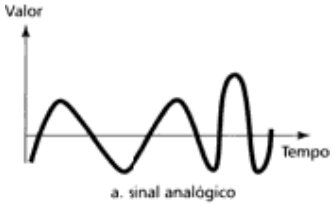
se voltaram para o novo modelo do IEEE (Instituto de Engenheiros e Eletricistas Eletrônicos / Institute of Eletrical and Eletronic Engineers), o 802.11, que padroniza todos equipamentos de rede sem fio.

3.1 Transmissão

Os sinais podem ser:

- Analógicos: possuem infinitos valores em um certo intervalo de tempo, ou seja, possuem valores contínuos. Como mostra a figura 3.

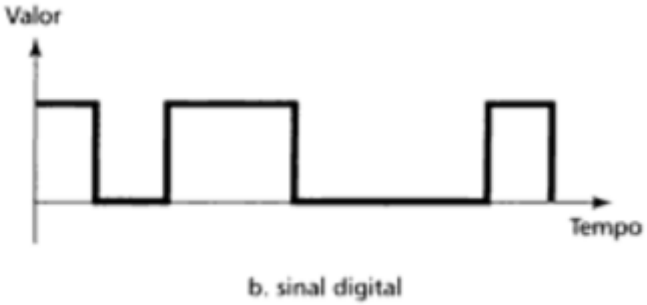
Figura 3 Exemplo de sinal analógico



Fonte: Forouzan, 2011

- Digitais: é definido por um número limitado e definido de valores, normalmente 0’s e 1’s. Um exemplo na figura 4.

Figura 4 Exemplo de sinal digital



Fonte: Forouzan, 2011

- Periódicos: quando completam um padrão dentro de um intervalo de tempo mensurável e repete este padrão nos períodos de tempo subsequentes;
- Não Periódicos: quando evoluem no tempo sem exibir um padrão ou completam um ciclo.

De acordo com Forouzan (2011), as redes em geral têm como finalidade a transmissão de dados, esta transmissão ocorre com a conversão dos dados em sinais. Em comunicação de dados, é utilizado frequentemente sinais analógicos periódicos e sinais digitais não periódicos.

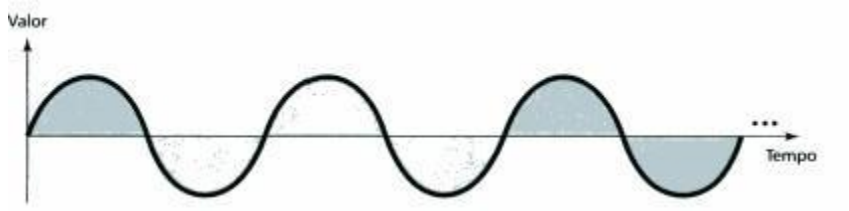
3.1.1 Sinais Analógicos

Os sinais analógicos são formados por uma soma discreta, possivelmente infinita, de múltiplas ondas senoidais. A onda senoidal representa o sinal analógico periódico de maior importância na comunicação de dados. A figura 5 representa uma onda senoidal, que segue a seguinte equação:

$$s\ t = Asen(2\pi ft + \emptyset) \quad (1)$$

Onda s é o valor instantâneo do sinal, A é a amplitude de pico, f é a frequência e ø a fase da onda.

Figura 5 Exemplo de onda senoidal

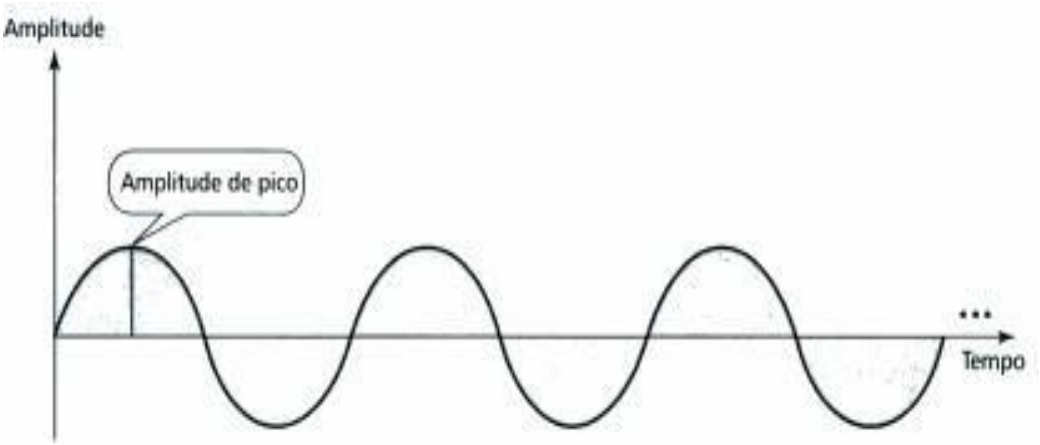


Fonte: Forouzan, 2011

Tais variáveis são explicadas abaixo:

Amplitude de pico: Como mostrado na figura 6, a amplitude representa o valor de intensidade mais alta, proporcionalmente à energia transportada pelo sinal. Em comunicação de dados a medida é em volts.

Figura 6 Exemplo mostrando a amplitude em uma onda



Fonte: Forouzan, 2011

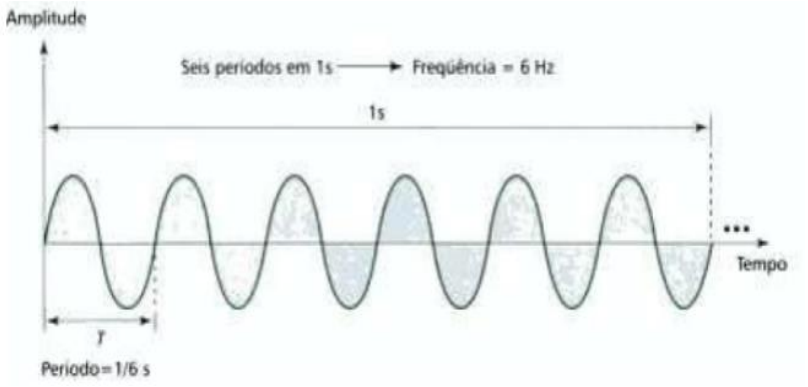
Frequência e Período: o período é o intervalo de tempo que uma onda gasta para completar um ciclo, por ser uma variável temporal, sua medida é em segundos. Já a frequência é a quantidade de períodos ou ciclos num intervalo de tempo igual a 1 segundo, sua medida é expressa em hertz (Hz). O período é o inverso da frequência. As fórmulas que os representam são:

$$f = {}^{1}/_{T} \quad (2)$$

Ou:

$$T = {}^{1}/_{\mathrm{f}} \quad (3)$$

Figura 7 Exemplo de frequência e período em uma onda

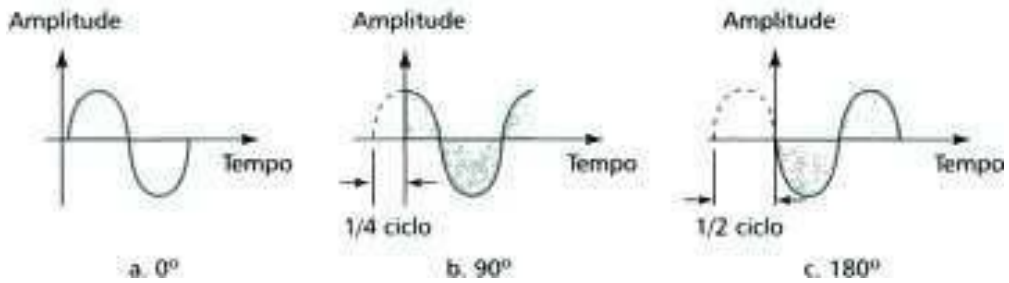


Fonte: Forouzan, 2011

A frequência pode ser utilizada como uma taxa de variação genérica de um sinal em relação ao tempo. Se as variações são curtas no tempo isso quer dizer que o sinal possui frequência alta, se as variações ocorrem em grandes intervalos de tempo, a frequência do sinal será baixa.

Fase: o termo fase informa a posição da forma de onda com relação ao marco zero do tempo. A fase mostra o quanto um sinal está deslocado na origem em relação ao eixo do tempo, ela indica o status do primeiro ciclo. Como mostra a figura 8.

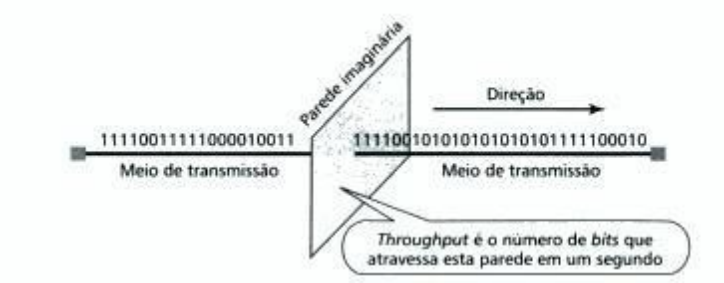
Figura 8 Diferentes fases em uma onda



Fonte: Forouzan, 2011

Throughput: é uma medida da velocidade com que os dados passam por um determinado ponto na rede, ou seja, o número de bits que cruzam um determinado ponto. Pode-se ver este processo na figura 9.

Figura 9 O que é o throughput



Fonte: Forouzan, 2011

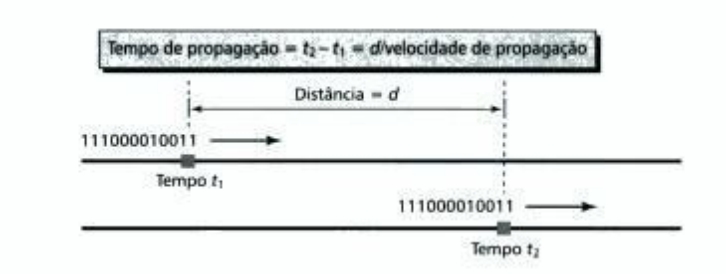
Velocidade de Propagação: é uma medida da distância que um sinal ou bit pode viajar em um meio durante o tempo de 1 segundo;

Tempo de Propagação: é uma medida utilizada para mostrar o tempo necessário para que um sinal ou um bit viaje de um ponto especifico no meio de transmissão até outro ponto. Esta medida é calculada através da divisão entre a distância percorrida pela velocidade de propagação do sinal, ou seja:

$$Tempo\ de\ propagação = distância/velocidade\ de\ propagação \quad (4)$$

Percebe-se isto na figura 10.

Figura 10 Como é feito o cálculo do tempo de propagação



Fonte: Forouzan, 2011

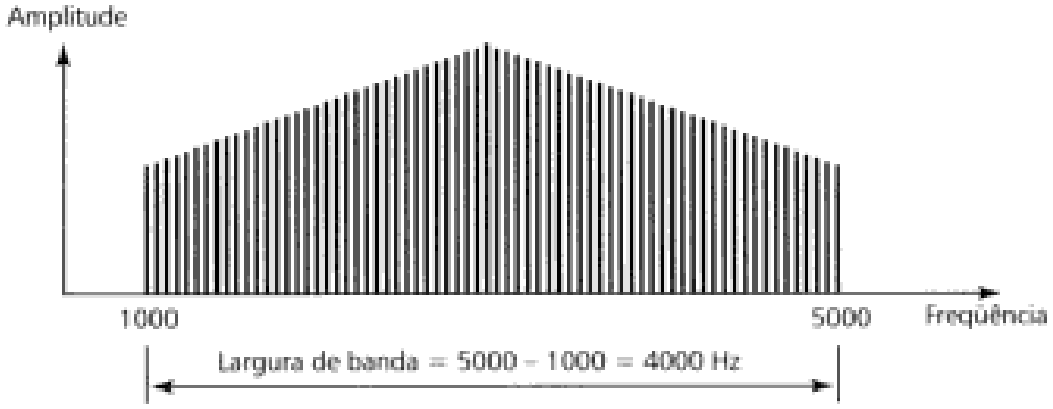
Comprimento de Onda: é uma característica do final que une o período ou a frequência de uma onda com a velocidade de propagação do meio. O comprimento de onda é a distância que um sinal simples pode viajar durante um período do sinal. Utiliza-se a seguinte fórmula:

$$\lambda = c \cdot f \quad (5)$$

Onde o comprimento de onda é a letra grega λ, a velocidade de propagação é a letra c, e a frequência é a letra f.

Largura de banda ou bandwidth: é a faixa de frequência passante em um meio, ela é calculada pela diferença entre o maior e a menor frequências que o meio pode transmitir. Como na figura 11.

Figura 11 Como é calculado a largura de banda



Fonte: Forouzan, 2011

3.2 Perdas na transmissão

Os sinais trafegam por meios de transmissão, como os meios de transmissão são imperfeitos acabam gerando uma perda de sinal, de acordo com Forouzan (2011, p. 81 - 84) tal perda pode acontecer devido a três causas: atenuação, distorção ou ruído.

- Atenuação: é a perda de energia, onde o sinal que trafega por um meio de transmissão perde parte de sua energia devido à resistência que o meio possui;
- Distorção: quando sinal muda de forma. Ela pode ocorrer quando um sinal composto, isto é, um sinal que é a junção de diversas ondas senoidais simples, elas se modificam durante a passagem pelo meio, sabendo que cada uma das ondas possui velocidades de propagação diferentes. Sendo assim cada uma das ondas terá um retardo diferente. Com isso haverá uma alteração na fase da onda do sinal composto;
- Ruído: podem ser de diferentes tipos como: térmicos, induzidos, entre outros. Ele causa dano ao sinal, dificultando e alterando a transmissão dos dados.

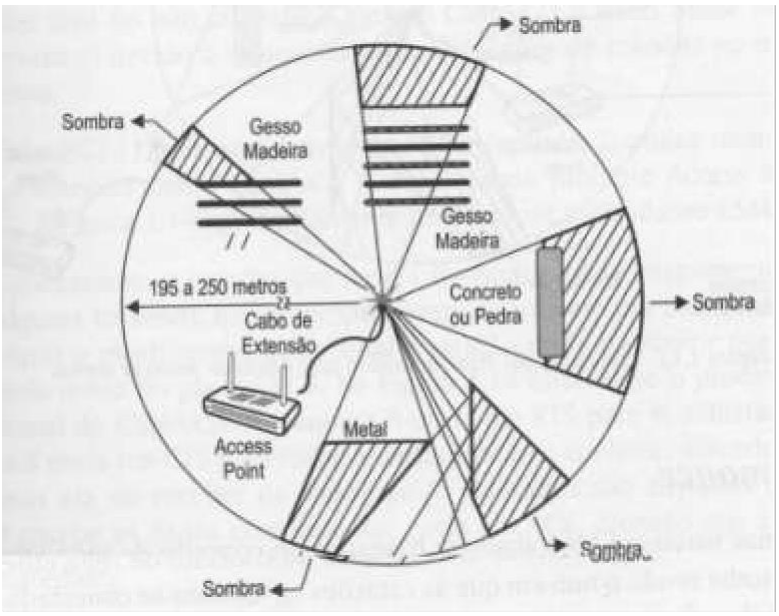
3.3 - Alcance e Propagação

De acordo com Moraes (2010), nas redes sem fio o alcance dos sinais é diretamente ligado com a potência de transmissão, a sensibilidade do receptor e o caminho por onde a onda se propaga. O tipo do material utilizado na construção, paredes e pessoas podem afetar na propagação do sinal e no alcance. Os ruídos e a utilização de antenas inadequadas também influenciam na transmissão. Quando o sinal fica fraco em um local, a placa de rede wireless reduz o sinal para uma velocidade menor.

Também de acordo com Moraes (2010), a propagação está diretamente ligada a frequência do sinal, potência de transmissão, o tipo e orientação das antenas, os sinais refletivos e o tipo de construção.

Na figura 12, tem-se diversos materiais como: metal, gessos e pedra; cada elemento exerce uma influência no alcance da rede sem fio, as áreas que deixam de ser alcançada por causa de algum material tem o nome de sombra.

Figura 12 - Influência de materiais no alcance da rede sem fio



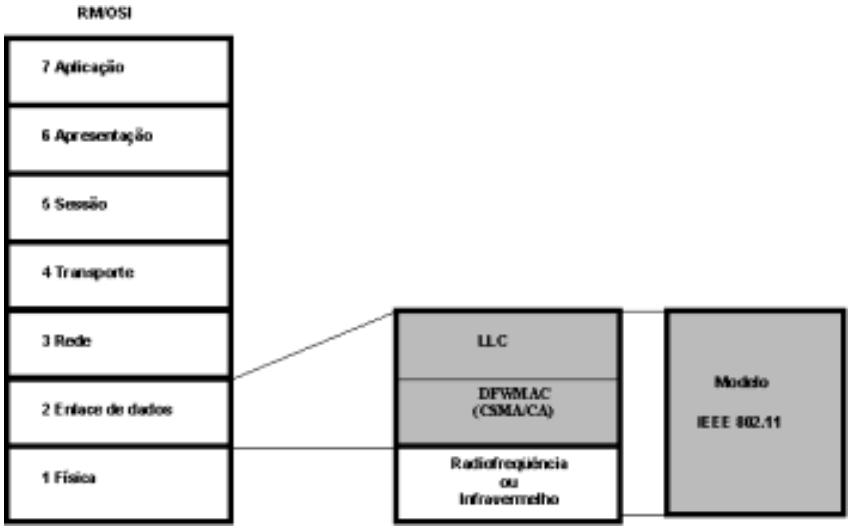
Fonte: Moraes, 2010

3.4 Padrão 802.11

Segundo Torres (2011), “um dos grandes problemas da comunicação sem fio é a falta de padronização entre os fabricantes” (TORRES, 2011, p.261), isso causava a incompatibilidade entre os equipamentos fabricados, pois eles não conseguiam se comunicar. Com isso, o IEEE criou o padrão 802.11.

Também de acordo com Torres (2011), o modelo de camadas OSI para uma rede que está no padrão 802.11 é exemplificado na figura 13.

Figura 13 – Modelo de camadas OSI para redes no padrão 802.11



Fonte: Garcia, sd

Com está padronização os equipamentos de diferentes marcas e fabricantes poderiam ser utilizados juntas sem nenhum problema de comunicação.

3.4.1 CSMA/CA

O padrão 802.11 utiliza uma forma de transmissão chamada CSMA/CA (Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão ou Carrier Sense Multiple Acess with Collision Avoidance) que de acordo com Torres (2011) trabalha da seguinte maneira:

Na primeira transmissão, o transmissor escuta o canal para verificar se está desocupado. Se nenhuma transmissão estiver sendo efetuada, ele inicia a primeira transmissão. Após a primeira transmissão ter ocorrido, cada máquina é configurada para transmitir um determinado período de tempo. Assim, não há colisões, já que cada máquina possui uma hora certa de transmitir. Se a rede ficar ociosa, isto é, se passar o tempo de todas as maquinas transmitirem e nenhuma quiser transmitir, então o canal para de ser usado e a rede volta ao estado anterior ao da primeira transmissão, isto é, a alocação de tempo de transmissão de cada máquina só é definida após a primeira transmissão ter sido efetuada.” (TORRES, 2011, p. 262)

Com isso, percebe-se que somente ocorre colisão nesta arquitetura durante a primeira transmissão, quando duas ou mais máquinas verificam que o canal está livre e tentam transmitir ao mesmo tempo, diferentemente do CSMA/CD que é utilizado em redes cabeadas onde sempre poderá existir uma colisão quando o canal estiver disponível.

Uma vantagem deste tipo de transmissão é a fragmentação que de acordo com Moraes (2010), permite que o CSMA/CA quebre grandes quadros em porções menores facilitando a retransmissão dos quadros caso ocorra algum erro durante o envio e recepção dos mesmos.

Este padrão utiliza várias frequências para realizar a transmissão de dados que variam dentro da faixa de 2.4 GHz. Para realizar tais transmissões de acordo com Torres (2011), o padrão 802.11 define transmissões por rádio que utilizam as técnicas FHSS, DSSS ou OFDM e para transmissões infravermelhas é utilizado a técnica DFIR (Diffused Infra-Red) que não será estudada por não entrar no objeto de estudo do trabalho. Tais técnicas são baseadas no Spread Spectrum.

3.4.2 Spread Spectrum

A técnica foi desenvolvida primeiramente para uso militar com o objetivo de distribuir o sinal por toda a faixa de frequência de maneira uniforme. De acordo com Rufino, o spread spectrum consome mais banda, mas oferece maior segurança, está

menos sujeito a ruídos e interferências, já que neste caso um ruído em uma certa frequência afetará somente a transmissão nessa frequência, e não a faixa inteira (RUFINO, 2011). Com isso, o sinal só é retransmitido quando se fizer uso da frequência que estiver com ruído.

O primeiro padrão que utilizou o Spread Spectrum foi o FHSS (Espectro de Difusão em Frequência Variável ou Frequency Hopping Spread Spectrum), que utiliza diversas frequências de forma aleatória, durante intervalos de tempo com isso o canal que estava sendo usado também será alterado aleatoriamente. A partir disso para conseguir realizar a transmissão e recepção dos dados será necessário que os dispositivos que estão na rede saibam a sequência dos canais utilizados. As vantagens desta técnica estão no aumento da segurança, que de acordo com Torres (2011), “mesmo que um hacker tenha uma antena multifrequencial na região, se ele não souber a sequência de transmissão dos canais, ele não conseguirá captar os dados que estão sendo transmitidos na rede” (Torres, 2011, p. 263) e na redução dos conflitos em um ambiente onde possua mais de uma rede utilizando o FHSS. Isso se deve ao fato de que as chances de existir um conflito entre elas, de acordo com Torres (2011), será de 1:79 (1.26%) já que existem 79 canais, sem contar que tal conflito só irá durar 100 milissegundos.

Como o FHSS utiliza muitas mudanças de canal, ele acaba se tornando muito lento, com isso ocorreu a criação de uma nova técnica o DSSS (Espectro de Difusão em Sequência Direta ou Direct Sequence Spread Spectrum).

A diferença do DSSS em relação ao FHSS está na forma de trocar os canais de frequência, sendo que no DSSS não ocorre de forma aleatória e sim de forma sequencial. Ambas tecnologias são incompatíveis, com isso uma antena com DSSS não consegue se comunicar com uma antena FHSS.

Como os canais são escolhidos de forma sequencial, a segurança adquirida pelo FHSS acabou se perdendo, sendo necessário somente uma antena DSSS para capturar os dados. Porém o que se perde de segurança, se ganha de desempenho, e

segundo Moraes (2010) essa tecnologia é muito eficiente, apresentando pouco overhead, isto é, não realiza processamento em excesso, é mais veloz do que o FHSS para uma mesma distância.

Por último, tem-se o OFDM (Multiplexação Ortogonal por Divisão de Frequência ou Orthogonal Frequency Division Multiplexing) que de acordo com Moraes (2010), é uma técnica de transmissão mais eficiente do que as demais, pode ser utilizada em redes sem fio e cabeadas. De acordo com Rufino (2011), a maioria dos padrões atuais de redes sem fio utiliza esta forma de transmissão, devido a sua capacidade de identificar interferências e ruídos, realizando uma troca ou isolamento de uma faixa de frequência que esteja sendo afetada por alguma forma de perda de sinal, interferência ou ruído. Além disso, existem diversas vantagens, como cita Moraes (2010):

- Se adapta rapidamente às más condições de transmissão, como a interferência sem a necessidade de uma equalização do sinal complexa;
- Baixa sensibilidade a erros de sincronismo de sinal;
- Não necessita de filtros dos subcanais.

Como dito antes, é muito resistente a interferência de sinal tanto em banda larga como entre os canais.

3.5 Família 802.11

O padrão 802.11 é o nome dado para padrões de operações em tecnologia de redes sem fio que foram desenvolvidos pelo IEEE. Como Moraes (2010) mostra o padrão 802.11 foi evoluindo, com isso acabou se dividindo em partes específicas para determinado tipo de serviço. Tal divisão ocorreu da seguinte forma:

- 802.11b: utiliza a faixa de 2.4 GHz e com DSSS pode trabalhar com taxas de até 11Mbps. Este tipo de padrão, 802.11b, baseia-se na comunicação multiponto, onde o access point se comunica com uma antena onidirecional com um ou mais clientes da rede sem fio. Este padrão aceita no máximo 32 pessoas conectadas à rede. De acordo com

Rufino, este é “[...]o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis”. (RUFINO, 2011, p.27);

- 802.11a: foi aprovado junto com o 802.11b, mas veio para corrigir problemas presentes nas duas versões anteriores. Pode-se utilizá-lo em faixas de até 54 Mbps. Utiliza a técnica OFDM que é mais eficiente que o DSSS, aumentando assim a velocidade para 54 Mbps. O que interfere nessa velocidade é a utilização da faixa de frequência de 5 GHz, uma faixa com poucos concorrentes, mas com menor área de alcance. Houve também o aumento na quantidade de clientes conectados, no máximo 64 pessoas, a utilização da chave WEPi, que aumentou razoavelmente a segurança;
- 802.11g: opera na faixa de frequência de 2,4 GHz, é compatível com os equipamentos dos padrões b e g, ou seja, eles poderão ser utilizados em um mesmo ambiente de rede. Este padrão foi baseado no 802.11a, porém com uma faixa de frequência de 2,4 GHz, com isso o 802.11g incorpora as características do padrão a, ou seja, utiliza o OFDM e mantém a velocidade de 54 Mbps;
- 802.11i: de acordo com Rufino (2011), este padrão é baseado em mecanismos de autenticação e privacidade. O principal protocolo usado neste padrão é o Segurança de Rede Robusta ou Robust Security Network (RSN), ele implica mais segurança. Também neste padrão, tem-se o protocolo WPA (Acesso protegido de Wi-Fi ou Wi-Fi Protected Access), que foi desenvolvido para corrigir as limitações do protocolo WEP (Wired Equivalent Privacy), além do WPA2, que utiliza o algoritmo de criptografia Advanced Encryption Standard (AES), todos os métodos citados acima serão mais detalhados no capítulo 5. Percebe-se então que este padrão veio para incrementar a segurança das redes sem fio;
- 802.11n: seus principais objetivos são o aumento da velocidade de transmissão que varia de 100 a 500 Mbps e o aumento do alcance. De acordo com Moraes (2010), o que mudou neste padrão foi a utilização

de uma variação do OFDM conhecida como Múltiplas Entradas Múltiplas Saídas ou Multiple Input Multiple Output OFDM (MIMO-OFDM), que combina entrada e saídas múltiplas, que multiplica a capacidade de transmissão de diferentes sinais de mais de múltiplas antenas e usa o OFDM, que divide um canal de rádio em um grande número de sub-canais espaçados para proporcionar comunicações mais confiáveis a altas velocidades. Este padrão também é compatível com os padrões mais antigos. Na figura 14 tem-se um quadro comparativo dos principais padrões do 802.11.

Figura 14 – Comparação dos principais padrões do 802.11

Padrão	Freqüência	Throughput bruto/real	Compatível com o 802.11b	Ano em que se tornou real	Tendência à adoção
802.11b	2,4 GHz	11Mbps /5Mbps	Sim	1999	Diminuindo em computadores, avançando na eletrônica mais barata
802.11a	5 GHz	54Mbps/ 25Mbps	Não	2002	Empresas adotando lentamente, sem consumidores
802.11g	2,4 GHz	54Mbps/ 25Mbps	Sim	2003	Avançando em todos os lugares

Fonte: Jara, Augusto, 2011

3.5.1 Topologia das redes sem fio

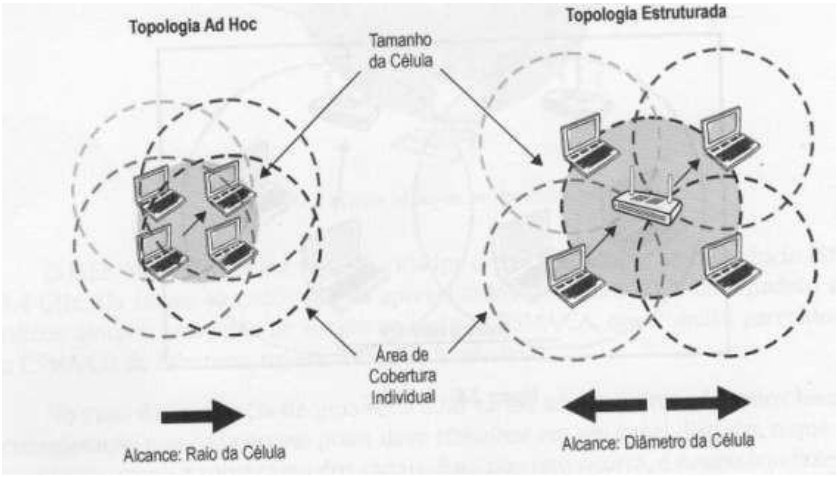
Na arquitetura 802.11, as redes sem fio podem funcionar de duas maneiras utilizando a topologia estruturada ou topologia ad hoc. Estas topologias mostram como é a organização de uma rede sem fio.

Na topologia estruturada, os computadores ou estações, são controlados por um access point, com isso, a rede é fixa, depende da posição do access point para

determinar o alcance. Percebe- se que neste caso o access point centraliza tudo para ele e de acordo com Moraes, “Nessa arquitetura a rede possui uma topologia fixa definida pelo posicionamento do access point, que neste caso é o responsável por alocar os recursos, além de gerenciar o consumo de energia das estações” (MORAES, 2010, p.45).

Enquanto na topologia ad hoc, as estações são dispositivos móveis que ficam conectados entre si, formando assim a rede. Também de acordo com Moraes, percebe-se que “neste caso não existe uma topologia definida, uma vez que os participantes podem se mover, alterando a topologia da rede” (MORAES, 2010, p.46). Com isso, não existe a centralização, tudo fica dividido entre as estações, portanto o gerenciamento de recursos e energia estabelecidos na rede serão feitos por todas as estações. Na figura 15, pode-se perceber a diferença entre as duas topologias, principalmente a presença do access point, o alcance de todo o conjunto de estações, chamado de célula, e a área de cobertura individual.

Figura 15 – Diferença entre as topologias estruturada e ad hoc



Fonte: Moraes, 2010

3.6 Dispositivos Usados

Para montar uma rede sem fio são necessários a utilização de diversos dispositivos que auxiliarão na elaboração da rede. Quando todos os equipamentos estão juntos, conectados e configurados da maneira correta, qualquer equipamento que possui uma placa de rede sem fio poderá utilizá-la. Hoje diversos equipamentos utilizam este tipo de rede como: smartphones, impressoras, notebooks, tablets, smart tv's, entre diversos outros aparelhos.

3.6.1 Placa de Rede sem Fio

De acordo com Moraes (2010), "são os adaptadores utilizados nas estações, os quais possuem barramento PCI, PCMCIA e USB, podendo ser instalados tanto em notebooks como em computadores desktop" (MORAES, 2010, p.35). Já os outros aparelhos já vêm com está placa instalada de fábrica, ou compra-se um adaptador. Na figura 16, tem-se uma placa wireless da 3Com e o adaptador de redes sem fio.

Figura 16 – Placa de rede sem fio

Fonte: Moraes, 2010

3.6.2 Concentrador

Concentrador ou access point ou ponto de acesso, de acordo com Moraes (2010) é responsável pelo gerenciamento das conexões entre os usuários e a rede,

podendo também servir como o ponto de conexão entre a rede sem fio e a rede cabeada.

De acordo com Wrightson (2014), os pontos de acesso mudaram muito desde que chegaram ao mercado, como por exemplo, o tamanho, funcionalidade, largura de banda e alcance. Para ele também as duas melhores mudanças do ponto de vista de um invasor são: o tamanho físico e o conjunto de recursos. Como esses novos pontos de acesso são mais compactos e com muitos recursos ajudam na construção de um cenário de ataque muito mais fácil com relativamente pouco risco.

Para as redes domésticas, pode-se utilizar pontos de acesso das marcas, Intelbras, TP-LINK, Linksys, Mikrotik, NetGear, entre outras marcas. A figura 17 mostra um roteador da Linksys, o WRT54G.

Figura 17 – Exemplo de concentrador

Fonte: Wrightson, 2014

Já para ambientes corporativos podem ser usadas as marcas Cisco, Mikrotik e Aruba, pois elas estão no mercado a mais tempo e possuem recursos que atraem a confiança dos consumidores, alguns destes recursos segundo Wrightson (2014) são:

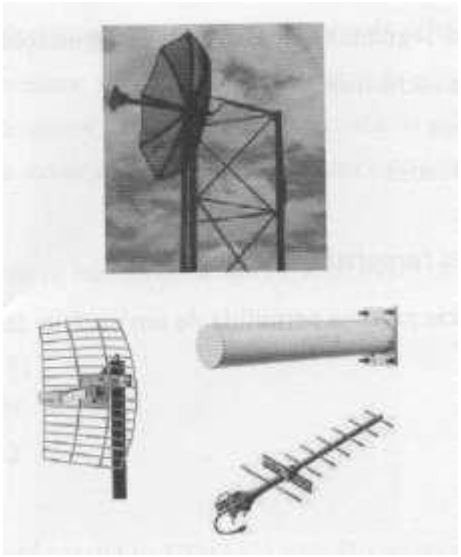
- Construção mais robusta;
- Sistemas baseados em controlador, isto é, de operação mais leves.
- Sistemas de gerenciamento de software;
- Opções de suporte ao fornecedor.

3.6.3 Antenas

As antenas irradiam os sinais da rede sem fio, seu principal objetivo é que elas aumentam o alcance do envio e recebimento de dados. De acordo com Wrightson (2014), elas são muito importantes no ponto de vista da segurança, devido ao fato de que com uma boa antena, pode- se captar sinais de tecnologias sem fio a alguns quilômetros de distância da fonte.

As antenas podem ser internas ou externas, dos tipos direcional e omnidirecional. Onde as antenas direcionais ou yagi, transmitem o sinal em uma única posição. A figura 18, mostra alguns exemplos de antenas direcionais.

Figura 18 – Antenas Direcionais



Fonte: Moraes, 2010

Já as omnidirecionais, propagam ao longo do eixo em um ângulo de 360 graus. Na figura 19, tem-se exemplos de antenas omnidirecionais.

Figura 19 – Antenas Omnidirecionais

Fonte: Moraes, 2010

3.7 Tipos de Redes Sem Fio

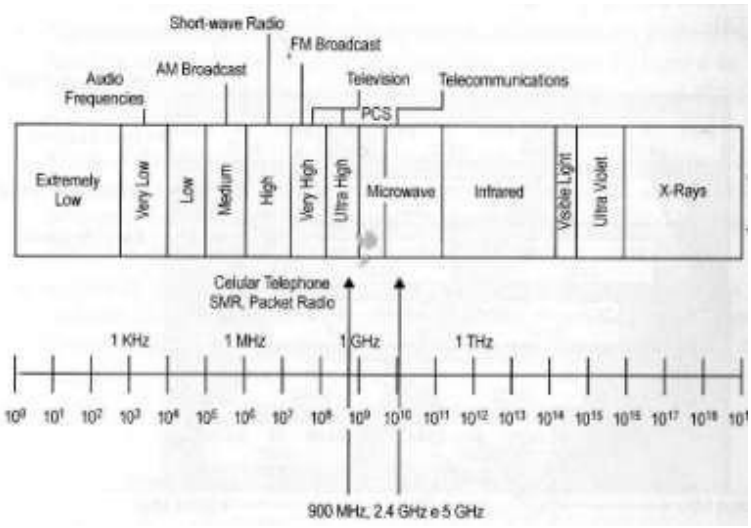
De acordo com Moraes (2010), as redes sem fio podem ser subdivididas em três tipos:

- Baseadas em infravermelho;
- Baseadas em radiofrequência, que são o objeto de estudo deste trabalho, ou seja, o Wi-fi, e também incluem o bluetooth;
- Baseadas em laser.

Destaca-se aqui as redes baseadas em radiofrequência por ser objeto de estudo deste trabalho. A radiofrequência é um tipo de rede sem fio que utiliza micro-ondas para realizar a transmissão do sinal através do ar, normalmente as suas faixas de frequência são conhecidas como ISM (Industrial Scientific Medical), são faixas abertas já que não é necessário de autorização para transmitir sinais nessas frequências.

O ISM padronizou em grande parte dos países três faixas de frequência, são elas: 900 MHz, 2.4 GHz e 5 GHz. As primeiras redes sem fio criadas utilizavam a faixa de 900MHz, porém como está faixa de frequência é muito utilizada por outros equipamentos e aplicações, o que acaba gerando muita interferência. Devido a isso, ocorreu uma mudança e atualmente as redes sem fio utilizam as faixas de frequência de 2.4 GHz. Na figura 20, pode-se observar o ISM dentro do espectro de frequências.

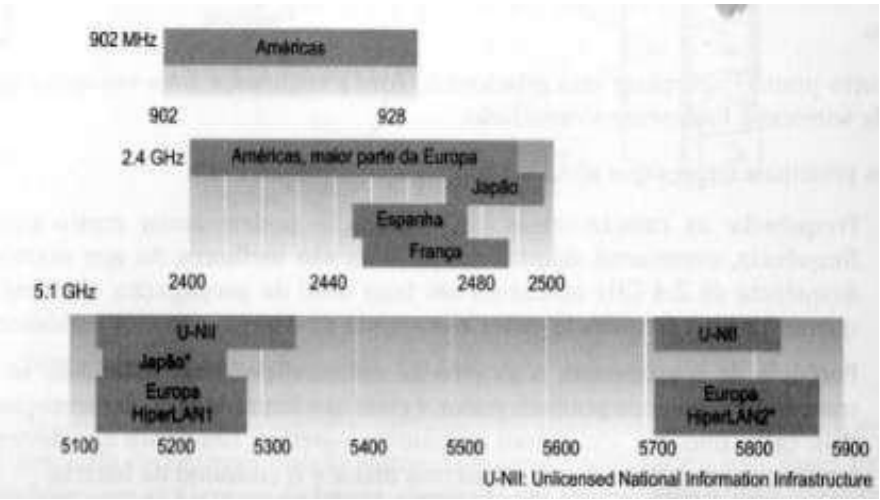
Figura 20 – ISM no espectro de frequência



Fonte: Moraes, 2010

A partir da figura 21, pode-se perceber que no Brasil a faixa de frequência utilizada para as redes sem fio é a de 2.4 GHz.

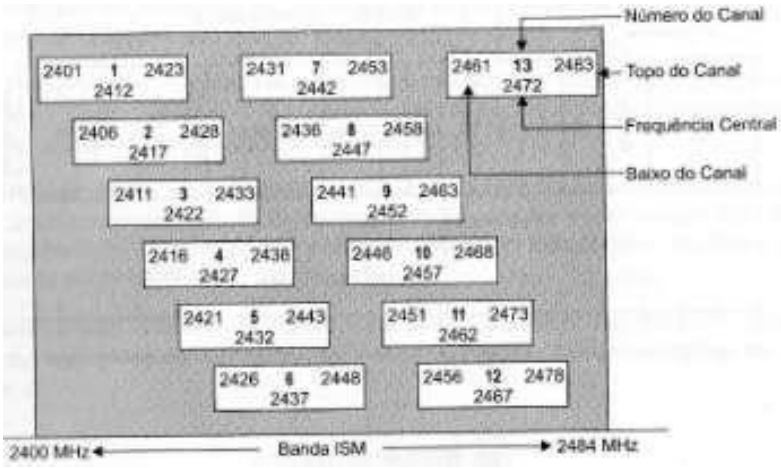
Figura 21 – Faixa de frequência usada nos continentes



Fonte: Moraes, 2010

Para as redes sem fio, existem 13 canais liberados para transmissão, mas em alguns países como no Brasil, existem somente 11. Em cada canal, pode-se encontrar canais específicos para uma certa organização ou para determinado tipo de equipamento. Na figura 22, pode-se visualizar estes canais.

Figura 22 – Divisão dos canais no Brasil

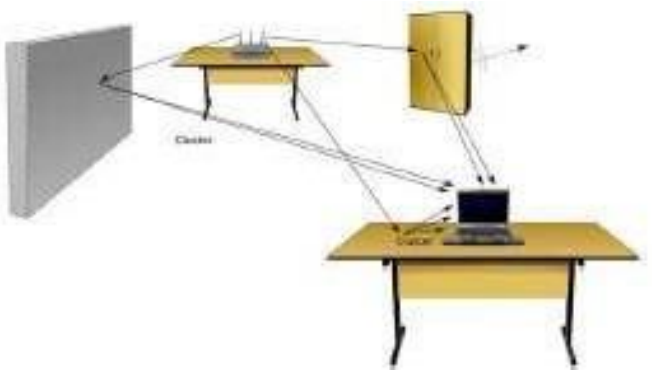


Fonte: Moraes, 2010

O ar possui vantagens em comparação a outros meios de transmissão, a principal delas está na dificuldade para interrupção, porém as ondas transmitidas podem sofrer alguns efeitos que podem afetar esta transmissão, de acordo com Moraes (2010) são eles:

- Frequência: as características de propagação variam muito com a frequência, onde em determinada faixa de frequência pode ocorrer interrupções, ou influenciar no nível de propagação. Quanto maior a frequência, maior o consumo de energia e menor o alcance;
- Potência de transmissão: o alcance pode aumentar se for transmitido com uma potência maior. Quanto maior a potência, maior é o consumo da bateria;
- Antenas: a posição, o tipo e a orientação delas influenciam bastante na transmissão, o mau posicionamento ou uso incorreto de um determinado tipo de antena pode causar problemas nas redes sem fio;
- Tipo de construção: dependendo do material utilizado no ambiente físico em que a rede será inserida pode dificultar ou até mesmo anular a propagação do sinal, como exemplo temos o ferro que em excesso e com outros metais podem afetar diretamente no alcance da rede sem fio, sendo assim necessário, a instalação de mais pontos de acesso;
- Sinais refletidos: o sinal pode ir em diversas direções, com isso haverá diversos caminhos entre o transmissor e o receptor, este evento é chamado de multipath. Com isso, haverá um enfraquecimento do sinal com a sua própria interferência. Na figura 23, pode-se ver tal evento.

Figura 23 – Sinais Refletidos



Fonte: Bof, 2010

- Fontes de interferência: quando há outros dispositivos utilizando a mesma faixa de frequência da rede sem fio, eles poderão interferir na transmissão de sinais da rede sem fio. Em um ambiente doméstico tem-se os telefones sem fio e o aparelho de micro-ondas que trabalham na mesma frequência das redes sem fio.

3.8 Vantagens e Desvantagens das Redes sem fio

As redes sem fio são muitos úteis em todos os tipos de ambiente, principalmente em locais em que uma rede cabeada é impossível de ser feita, como em prédios tombados e outros. De acordo com Moraes (2010), isso se deve ao fato delas oferecerem uma série de vantagens como: mobilidade, fácil e rápida instalação, escalabilidade, redução de custo na instalação e na compra de equipamentos.

Porém, tem-se alguns problemas em relação à segurança já que utiliza o ar como meio de transmissão, problemas de interferência, caso neste mesmo ambiente exista outros aparelhos que utilizem a mesma faixa de frequência e também pode haver problemas no gerenciamento caso não tenha o controle de acesso suficiente para manter a rede intacta e operante.

4. SEGURANÇA DA INFORMAÇÃO

A palavra segurança significa de acordo com o dicionário Aurélio, “estado, qualidade ou condição de seguro. Condição daquele ou daquilo em que se pode confiar. Certeza, firmeza, convicção.” (AURÉLIO, 2005). Ainda mais específico, de acordo com Howard citado por Moraes (2010), pode-se perceber que a segurança de computadores se baseia em prevenir ataques que tenham como objetivos uso ou acesso não autorizado de computadores e redes.

Ou ainda mais específico, de acordo com British Standards Institute citado por Moraes (2010), a segurança da informação tem como objetivo a garantia de continuidade do negócio e minimizar o dano causado, prevenindo e minimizando o impacto de incidentes de segurança.

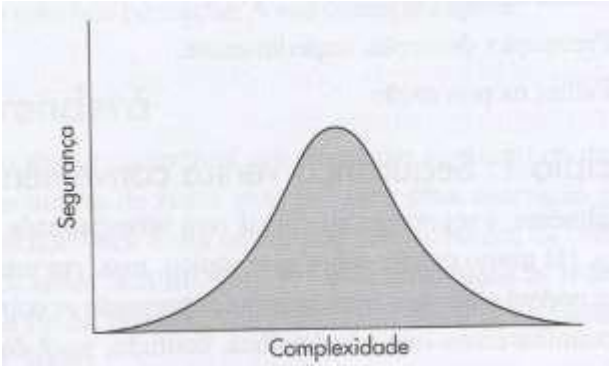
4.1 Princípios para análise de segurança

De acordo com Wrightson (2014), existem 11 princípios que são utilizados para análise de segurança, independente da tecnologia. Tais princípios seguem abaixo de forma detalhada.

4.1.1 Segurança versus conveniência

Este princípio mostra que quando se quer mais segurança, mais inconveniência terá. Por isso, Wrightson (2014) criou um paradoxo que ele gosta de chamar de curva de sino da segurança versus conveniência, a qual mostra que à medida que se aumenta o fator inconveniência, aumenta-se a segurança, mas a partir de um certo momento, a inconveniência tem efeito contrário sobre a segurança como pode-se perceber na figura 24.

Figura 24 – Curva de segurança x Complexidade



Fonte: Wrightson, 2014

4.1.2 É impossível eliminar todos os riscos

A definição de risco de acordo com dicionário Aurélio, “perigo ou possibilidade de perigo.” (AURÉLIO, 2005).

É impossível eliminar todo o risco de qualquer tecnologia, isto é, para cada processo há um certo risco, mesmo sendo minúsculo. O risco está presente em tudo, desde o que é feito até as decisões tomadas. Observe a figura 25 para ver um exemplo de um risco que se corre ao atravessar uma rua.

Figura 25 – Riscos que corremos a atravessar a rua

	Descrição
Risco	Ser atropelado por um carro
Controle de mitigação	Olhar para os dois lados antes de atravessar a rua (É fácil ver que o controle de mitigação da travessia da rua é adequado. Mas ele elimina todos os riscos da travessia?)
Outros riscos	Superfície escorregadia (cair e se machucar) Motorista distraído Tiros vindos de um automóvel Queda de avião

Fonte: Wrightson, 2014

Com isso, percebe-se que a análise de risco nem sempre é a seleção do caminho de menor risco, mas sim a tomada de uma decisão embasada que melhor atenda à empresa ou à pessoa.

4.1.3 Regras para o cálculo de risco e controles de mitigação

De acordo com Wrightson (2014), o risco pode ser calculado da seguinte forma:

$$Risco = consequência\ x\ probabilidade \quad (6)$$

Analisando cada termo desta equação tem-se que:

- Consequência: é o impacto sentido quando uma vulnerabilidade é explorada, pode ser expressa em termos numéricos, quantitativos ou em termos mais subjetivos, qualitativos
- Probabilidade: é a possibilidade de uma vulnerabilidade ser explorada.

Com isso, é calculado o nível de risco associado a uma determinada vulnerabilidade.

Voltando ao exemplo da figura 25, pode-se perceber que é melhor se preocupar com motoristas do que com queda de aviões ao atravessar uma rua, já que um tem uma probabilidade muita alta de acontecer e outro é muito raro de acontecer.

Figura 26 – Probabilidade de risco

Vulnerabilidade	Queda de avião
Impacto	10 (morte)
Probabilidade	0,000001 (uma em cada 1.000.000 de pessoas morre devido a quedas de aviões todo ano nos Estados Unidos)
Nível de risco	0,00001 (10 × 0,000001)
Vulnerabilidade	Motorista distraído
Impacto	10 (morte)
Probabilidade	0,001 (uma em cada 1.000 pessoas morre devido a motoristas "distraídos" todo ano nos Estados Unidos)
Nível de risco	0,01

Fonte: Wrightson, 2014

4.1.4 Nem todos os riscos devem ser mitigados

Este princípio se baseia em analisar quais os riscos valem a pena serem mitigados, voltando ao exemplo do avião, com alguns milhões de dólares poderia ser construída uma casa que absorvesse ao impacto da queda de um avião, porém a possibilidade disso acontecer é muito baixa e não valeria a pena pagar milhões em uma coisa que às vezes pode nem acontecer.

Quando se tem que gerir um risco deve-se ser analisada quatro situações, aceitar, evitar transferir ou mitigar o risco. Para isso é necessário ter senso crítico para pensar no melhor custo benefício onde os custos não são tão altos e a rede se mantenha segura. Na figura 27, pode-se ver a definição entre evitar, transferir e mitigar.

Figura 27 – Diferença entre evitar, transferir e mitigar

Evitar	Suponhamos que o regulamento só se aplicasse a empresas operando no Texas. Se sua empresa pudesse prosperar sem fazer negócios no Texas, então, você conseguiria evitar o risco.
Transferir	Talvez você possa transferir o risco para terceiros. Se pudesse terceirizar a parte de seus negócios abordada pelo regulamento e permitir que terceiros se preocupassem com ela, então, teria transferido o risco.
Mitigar	Se em vez de evitar, transferir ou aceitar o risco, você decidisse implementar controles para aderir ao regulamento. Assim, mitigaria de maneira eficaz o risco de pagar uma multa por sua causa.

Fonte: Wrightson, 2014

4.1.5 Segurança não é apenas manter os criminosos do lado de fora

Este princípio mostra que não se deve preocupar somente com fatores externos, sendo que a maioria dos ataques vem de falhas internas, de quem utiliza a rede, principalmente com o uso de engenharia social, tema que será detalhado mais à frente. Portanto, deve existir a preocupação de se manter os criminosos do lado de fora e de conscientizar as pessoas para evitar um ataque que possa acontecer por falhas externas.

4.1.6 Cálculo do retorno sobre o investimento não funciona para segurança

No caso da segurança o cálculo do retorno sobre investimento ou ROI (Return On Investment) não funciona, por que a segurança não se trata de um processo empresarial de geração de receitas. Isto é, o dinheiro e recurso gasto em segurança são para evitar que se perca uma maior quantia de dinheiro ou de recursos, correndo o risco de ter sua imagem, reputação manchados por um longo prazo, o que nem chega perto do valor dedicado para garantir a segurança das informações.

4.1.7 Defesa em profundidade

A defesa em profundidade defende a seguinte afirmação: “a verdadeira segurança não vem de um controle de mitigação de risco; em vez disso, vem da implementação de muitas soluções sinérgicas.” (Wrightson, 2014).

4.1.8 Privilégio mínimo

Privilégio mínimo é um princípio usado para aumentar a segurança, este princípio significa dar aos usuários os direitos mínimos para que eles possam realizar as atividades, dando privilégios adicionais somente quando necessário.

4.1.9 Tríade CID

A tríade CID é um modelo utilizado pela indústria para proteção de sistemas. Sua sigla significa confidencialidade, integridade e disponibilidade, isto é, os pilares da segurança da informação.

Confidencialidade: somente quem tiver direito de acesso a visualização dos dados poderá vê-lo e impede a exibição sem autorização de informações sigilosas;

Integridade: é a proteção que garante que os dados não foram acessados por pessoas desautorizadas;

Disponibilidade: garante que a informação esteja sempre disponível quando necessário, realizando técnicas que evitem a interrupção do serviço e da produtividade.

4.1.10 Prevenção, detecção, impedimentos

Seguindo o princípio da defesa em profundidade, é sempre bom implementar vários tipos de controle de segurança sempre que possível. Esses controles se enquadram em pelo menos uma das categorias abaixo.

- Prevenção: se preocupar em deter uma atividade antes que ela ocorra. Exemplos: um firewall, barras em janelas, fechaduras em portas;
- Detecção: mostra ou revela certas atividades. Exemplo: câmeras ativadas por movimento e um sistema de detecção de intrusos;
- Impedimentos: são usados para impedir que alguém faça coisas que não devem e que prejudicam a segurança. Eles são de dois tipos: físicos ou lógicos. Exemplo: a cerca elétrica impediria que pulasse por que senão a pessoa poderia ser eletrocutada, enquanto as câmeras de segurança agem como um impedimento lógico, já que elas podem ser utilizadas para provar o procedimento inadequado do criminoso.

Os controles de segurança podem estar em mais de uma das categorias citadas acima, como por exemplo: as câmeras tanto detectam quanto potencialmente impedem a atividade criminosa.

4.1.11 Falhas de prevenção

Dentro da segurança é fato que toda medida preventiva possivelmente poderá falhar, mas isso não quer dizer que será burlada, mas que é possível que aconteça. Por isso, deve-se investir em uma forte estratégia de defesa em profundidade que use bem técnicas de impedimentos e métodos de detecção.

4.2 Política de Segurança

A política de segurança ajuda no controle interno de uma organização, minimizando as falhas criadas por pessoas envolvidas. De acordo com Moraes (2010), as suas diretrizes são baseadas em:

- Riscos ao patrimônio, risco de roubo e de fraude;
- Acesso de usuários aos sistemas;
- O uso de canais de comunicação;
- Sistemas redundantes e tolerantes a falhas;
- Garantia de integridade de software.

Seus principais objetivos são: informar o que deve ser protegido, mostrar quem é o responsável pela proteção e funcionar como referência para resolver conflitos e problemas.

4.3 Plano de Segurança

São usadas por organizações que desejam criar de forma embasada segurança para suas informações. Para conseguir fazer um plano de segurança, de acordo com Moraes (2010), é necessário seguir alguns passos essenciais, são eles:

- Análise dos riscos de uma determinada organização está sujeita;
- Com o levantamento dos riscos, deve-se tomar uma decisão de nível gerencial na organização sobre quais as ações serão tomadas, isto é, se o risco será ignorado, aceito, minimizado ou se a corporação vai querer passar pelo risco;
- Quando ocorre a análise dos riscos, planeja-se as ações que serão tomadas, levantando as perdas tangíveis e intangíveis, ou seja, levar em conta os recursos, imagem e reputação da organização;
- Com base no que pode ser afetado com determinado risco levanta-se as possíveis maneiras de resolvê-lo.

4.3.1 Análise e Gerenciamento de Riscos

A análise e o gerenciamento de riscos têm como objetivo a identificação de perdas e impactos causados por uma falha de confidencialidade ou roubo das informações da empresa. Os riscos podem ser relacionados à distribuição de dados de importância crítica para a empresa e à perda de integridade das informações.

A avaliação e tomada de decisões permitem a identificação dos riscos envolvidos em um sistema, isto é, análise de risco. De acordo com Moraes (2010), ela pode ser feita de duas maneiras, fazendo uma análise quantitativa ou qualitativa, levando em conta fatores como as ameaças, vulnerabilidades e os recursos envolvidos.

4.3.2 Análise quantitativa

Segundo Moraes (2010), a análise quantitativa é ligada com a questão financeira e estima os custos gastos com as ameaças e com a proteção. Também é ligada à medição dos custos de uma perda, que é uma medida difícil de estimar já que é muito complexo pois são envolvidos valores tangíveis e intangíveis, gastando assim muito tempo, e quando estão prontos podem ser que não sejam mais válidos pois o ambiente operacional da empresa já mudou.

4.3.3 Análise qualitativa

Análise qualitativa estima-se somente a perda, esquecendo análises probabilísticas e segundo Moraes (2010), está se tornando mais popular do que a análise quantitativa, pois é feita de forma mais objetiva e rápida. Esta análise trabalha com ameaças, vulnerabilidades e mecanismos de controle.

4.3.4 Ameaças

As ameaças são mais perigosas e as que acontecem com maior frequência em uma análise. De acordo com Moraes (2010), elas podem ser:

- Intencionais: são causadas de forma intencional e podem ser causadas por um agente interno ou externo;
- Relacionadas aos equipamentos: um equipamento pode apresentar falhas de software ou hardware, devido a um defeito ou por bugs;
- Relativas a um evento natural: neste caso os equipamentos ou instalações físicas podem estar sujeitos a uma ameaça natural como fogo, inundação e quedas de energia;
- Não intencionais: acontecem devido a ignorância, sendo que a maior parte dos danos causados no sistema surgem sem intenção e não por ações maliciosas.

4.3.5 Vulnerabilidades

As vulnerabilidades mostram o quanto um sistema é suscetível a um ataque, onde a ameaça é a intenção concreta de explorar uma determinada vulnerabilidade. Segundo Moraes (2010), as vulnerabilidades são divididas em:

- Físicas: no caso a estrutura física do local o deixa exposto, podendo ser facilmente invadido;
- Naturais: quando fatores como fogo, terremoto, perda de energia pode danificar algo útil na empresa, como por exemplo os computadores que com estes fatores podem facilmente serem danificados e com isso perde-se os dados;
- Hardware e Software: falhas de no hardware e no software podem comprometer toda a segurança de um sistema, onde por exemplo uma falha de hardware pode deixar o sistema utilizável, enquanto um bug no software pode abrir brechas ou portas no sistema, deixando-o fácil de ser invadido;
- Mídia: os materiais como disco, material impresso, podem ser facilmente roubados, destruídos ou danificados;
- Emanação: é o tipo de vulnerabilidade estudada neste trabalho, onde os equipamentos eletrônicos emitem radiações elétricas ou eletromagnéticas, onde esses sinais podem ser capturados e decifrados, possuindo assim as informações do sistema ou de algum outro conteúdo;
- Comunicação: durante a transmissão de uma mensagem ela pode ser interceptada, desviada ou alteradas. As linhas de comunicação podem ser escutadas ou interrompidas;
- Humanas: é o fator que representa a maior vulnerabilidade, a segurança do sistema é mais fácil de gerenciar, enquanto as pessoas podem cometer erros que comprometam o sistema.

4.3.6 Controles

Os controles são os mecanismos que tem como objetivo a minimização de ameaças, de acordo com Moraes (2010), esses mecanismos podem ser:

- Efetivo: controle para diminuir a probabilidade de ocorrer uma ameaça;
- Preventivo: tem como objetivo a prevenção de vulnerabilidades para minimizar o sucesso das tentativas de ataque;
- Corretivo: reduzir os efeitos das ameaças;
- Detectivo: tem como finalidade a descoberta de ataques e possui mecanismos para gerenciar a correção;
- Recuperação: realizam a restauração para um quadro normal da empresa após um ataque.

4.4 Tipos de Invasores

Existem diversos tipos de invasores, cada um com um objetivo e forma própria de atacar. Eles têm uma coisa em comum, querem invadir sistemas e isso ameaça as informações dos usuários. De acordo com Caraça e Penna (2009), eles podem ser divididos em:

- Hacker: grande facilidade de análise, assimilação, compreensão e sabem que nenhum sistema é completamente livre de falhas e gostam de testá-las já que sabem como procurar utilizando técnicas próprias e variadas;
- Cracker: são como os hackers, porém eles destroem o que encontram, agem para prejudicar financeiramente alguém ou em benefício próprio;
- Phreaker: são especializados em telefonia, gostam de informações que são úteis para pessoas más intencionadas.

Além disso, eles podem ser divididos em grupos mais genéricos. De acordo com Broad e Bindner (2014), eles podem ser classificados em:

- Red Team ou equipe vermelha: simula um adversário em potencial baseados em suas metodologias e técnicas. Normalmente eles atacam empresas usando os meios de natureza técnica, social e física, com o objetivo de testar as proteções da empresa ou dos sistemas de informação;
- Hacking ético: é o profissional que ataca um determinado sistema com ordem do proprietário, com o objetivo de encontrar falhas de segurança;
- White hat ou chapéu branco: é uma gíria para um hacker ético que se especializou em metodologias para melhoria da segurança dos sistemas;
- Black hat ou chapéu preto: este termo é usado para identificar indivíduos que usam técnicas para invadir um sistema sem a permissão do proprietário, ou seja, agem de forma ilegal;
- Grey hat ou chapéu cinza: são especialistas que ficam no limite entre os white hats e os black hats. Eles tentam passar pela segurança de um sistema sem permissão para informar aos administradores as vulnerabilidades do sistema.

4.5 Modelo de Referência de Segurança

Este tipo de modelo tem como objetivo, definir uma arquitetura de rede confiável e que esteja ligada a uma política de segurança. De acordo com Moraes (2010), um modelo é constituído dos seguintes componentes:

- Equipamentos de rede. Exemplo: pontos de acesso, gateways, roteadores, entre outros;
- Sistemas de autenticação. Exemplo: assinatura digital, sistemas biométricos e certificação digital;
- Sistemas de segurança. Exemplo: sistemas de criptografia e firewalls;
- Sistemas de auditoria;

Precisa ter um log, isto é, precisa ter as informações e mensagens trocadas no sistema.

Para criar um modelo mais seguro é necessário conhecer e entender os serviços de segurança que o sistema implementa. Estes serviços são divididos em:

- Integridade;
- Autenticidade;
- Confidencialidade;
- Não repúdio;
- Disponibilidade;
- Controle de Acesso;
- Auditoria.

4.5.1 Integridade

Como dito na seção 4.1.9, a integridade é a proteção que garante que os dados não foram acessados por pessoas desautorizadas. Seu maior objetivo é proteger as informações para que elas não sejam intencionalmente ou acidentalmente alteradas sem a devida autorização. Por fazer parte da tríade CID, a integridade sempre é alvo de ameaças, necessitando de mecanismos que a protejam como as funções de hashing.

- Ameaças à integridade

Qualquer ação que implique na alteração dos dados ou programas, normalmente os hackers, usuários sem autorização e programas maliciosos são as principais ameaças. Porém, de acordo com Moraes (2010), existem três controles de segurança que ajudam a manter a integridade das informações, são eles:

- Rotation of duties, ou troca de equipe: se baseia na troca constante de pessoas em cargos chave, com isso pode-se evitar a fraude no sistema,

além disso existirá uma equipe de backup que entra em ação caso perca-se profissional;

- Need to know ou o que os usuários precisam saber: é um conceito que já foi muito usado por militares e hoje as empresas o utilizam. Este conceito se baseia em permitir acesso ao usuário somente nos programas ou informações que ele necessita para executar uma determinada tarefa;
- Separation of duties ou divisão de responsabilidade: tem como objetivo a garantia de que do início ao fim de um processo duas ou mais pessoas tenham o controle ou responsabilidade dele, fazendo assim que todo o controle não esteja na mão de uma única pessoa.

- Funções de hashing

Hashing é uma técnica usada para verificar e garantir que a integridade dos dados se manteve. É uma função matemática, que utiliza o cálculo dos dados que estão sendo armazenados ou transmitidos em um meio de comunicação. Segundo Moraes (2010), o hashing funciona da seguinte maneira:

- Quando se transmite uma mensagem, calcula-se o seu hashing e em seguida o envia junto com a mensagem;
- Quando a mensagem chegar ao seu destino, refaz-se o cálculo e compara-se o novo hashing calculado com o que foi recebido;
- Se houver alteração no valor, houve alteração da mensagem;
- Se não a mensagem está intacta.

De acordo com Moraes (2010), os principais algoritmos de hashing são:

- SHA-1 (Secure Hash Algorith): é calculado em uma mensagem que pode ser de qualquer tamanho, depois disso gera-se um resultado de 512 bits. Ele é usado junto com algoritmos de criptografia (serão abordados no capítulo 5) como o DES, AES e o Triple DES;

- MD5: este algoritmo processa a entrada em blocos de mensagens de 512 bits e gera um hash de 128 bits, neste caso pode haver colisões.

4.5.2 Confidencialidade

A confidencialidade se baseia em proteger a informação, sistemas e processos de pessoas que não possuem o acesso autorizado. Como a informação não pode ser disponibilizada a quem não tem acesso, pode-se dizer então que a confidencialidade também é um mecanismo que garante a privacidade dos dados.

De acordo com Moraes (2010), as ameaças mais comuns a confidencialidade são: Hackers: podem tentar descobrir os dados de usuários autorizados para conseguirem acesso e comprometer a confidencialidade, além disso eles podem criar portas de acesso ou backdoor para que outros usuários não autorizados possam ter acesso ao sistema:

- Downloads não autorizados: isso ocorre quando as informações são movidas de um lugar seguro para ambientes vulneráveis, sendo assim não é possível garantir a confidencialidade;
- Redes: esta ameaça quer mostrar que os dados devem ser criptografados para evitar que os dados sejam comprometidos durante a transmissão;
- Vírus e Trojans: esses arquivos maliciosos podem buscar por informações confidenciais, podendo copiá-los para uma máquina externa;
- Engenharia social: neste caso o indivíduo tenta se passar por uma pessoa confiável e simplesmente tenta obter informações dos usuários do sistema.

A confidencialidade pode ser mantida quando ocorre a criptografia dos dados, restrição de acesso, classificação dos dados e com processos de segurança.

4.5.3 Autenticidade e Controle de Acesso

A autenticidade e o controle de acesso são interligados para se obter um nível de segurança no controle de acesso, segundo Moraes (2010), é necessário que ocorra o processo a seguir:

- Identificação: identificar o usuário, programa ou processo. Para assim acontecer a autenticação, ou seja, a identificação é um pré-requisito da autenticação;
- Autenticação: Com usuário já identificado no sistema, deve-se oferecer uma forma de comprovar de que é ela mesma que está tentando obter o acesso. Essas formas de acesso podem ser senha, frase secreta, certificado, um cartão, uma chave criptográfica ou até mesmo uma leitura biométrica;
- Autorização: Após o usuário obter a identificação e ser autenticado, o sistema verifica os privilégios e autoriza o acesso obedecendo aos princípios de integridade.

4.5.4 Disponibilidade

A disponibilidade é a garantia de que o sistema sempre estará disponível quando o usuário precisar. Suas principais ameaças estão relacionadas a ataques de negação de serviço e causas naturais, como incêndio, enchente, entre outros.

De acordo com Moraes (2010), os ataques de negação de serviço derrubam servidores, fazendo assim com que as informações fiquem indisponíveis. Eles derrubam o servidor quando realizam muitas requisições até chegar em um ponto que o servidor não pode suportar derrubando assim o serviço oferecido por tal servidor, sobrecarregando também os recursos e links de comunicação.

Desastres naturais não tem como se evitar, porém os ataques a servidores, podem ser evitados com a utilização de equipamentos, aplicativos e servidores

redundantes, que entram em ação quando o principal falhar, isto é, o sistema de backup.

4.5.5 Não Repúdio

O não repúdio é um serviço de segurança que possui mecanismos para que o remetente da mensagem não possa negar no futuro que foi ele quem enviou a mensagem.

4.5.6 Auditoria

Segundo Moraes (2010), a auditoria é um serviço de rede que implica na criação de registros (logs), que registram as ações que ocorreram na rede, são utilizadas para verificar no futuro se ocorreu alguma irregularidade, por parte de pessoas autorizadas e não autorizadas.

Com o detalhamento de cada serviço, percebe-se que todos eles são importantes, porém dependendo do ambiente em o sistema está inserido alguns serviços podem ser mais úteis e importantes.

5. SEGURANÇA EM REDE SEM FIO

A segurança em redes sem fio é um fator primordial, e quanto mais cedo possível for realizado um plano de segurança mais segura ela estará, deve-se em uma organização tratar da segurança desde a criação do mapa da rede e sua instalação. O motivo disso acontecer de acordo com Moraes (2010), é o fato de que “o wireless também expande o perímetro da rede da empresa. O que antes era um ambiente de rede controlada, centralizado e cabeado acaba se tornando um desafio de segurança[...]”.

5.1 Criptografia

De acordo com Moraes (2010), a “criptografia é a ciência que utiliza algoritmos matemáticos para criptografar/encriptar (cripto = esconder) dados (texto claro) numa forma aparentemente não legível (texto cifrado) e recuperá-los (descriptografá-los)” (MORAES, 2010, p.123).

Para entender todo este mecanismo é necessário saber alguns conceitos básicos:

- Encriptação: é transformar um dado legível, escrito de forma clara em forma ilegível;
- Decriptação: é o contrário da encriptação, transforma o texto ilegível em legível novamente;
- Texto claro: mensagem que será enviada, caso ela seja interceptada durante a transmissão, poderá ser lida facilmente pelo invasor;
- Texto cifrado: é a mensagem que será enviada, porém ela passou por um processo de encriptação, dificultando, no caso de interceptação de um invasor, a leitura da mensagem transmitida.

Muitos invasores utilizam as técnicas de criptoanálise, isto é, estudam os métodos, algoritmos e dispositivos que são usados para quebrar a segurança dos sistemas criptográficos, para poderem descobrir o método de decriptografia e assim

ler o texto claro. Por isso, devem sempre existir métodos novos que realizam criptografias mais difíceis de serem quebradas.

Segundo Moraes (2010), a criptografia é usada em redes sem fio para: garantir que a mensagem enviada é autêntica, manter a integridade, garantir a confidencialidade da mensagem, garantir que a mensagem não foi alterada durante a transmissão e provar o envio.

Durante a transmissão de dados, as informações reservadas e sigilosas e que não podem ser interceptadas, devem ser criptografadas, para isso, de acordo com Moraes (2010), pode-se utilizar três técnicas, são elas:

Sistema de chave secreta: neste caso o transmissor e o receptor sabem a chave secreta, isso é, sabem os meios de encriptação e decriptação. É um modelo seguro enquanto a chave utilizada for considerada secreta.

Sistema de chave pública: usa uma chave pública onde ambas as partes a conhecem e uma chave privada usada para encriptar os dados. Com isso o transmissor e o receptor devem ter um par de chaves, uma pública e uma privada. Veja o seguinte exemplo: João quer enviar uma mensagem para Maria, para isso ela tem que saber a chave pública de João, pois somente ela será capaz de descriptografar a mensagem enviada com a chave privada de João.

As chaves de criptografia são usadas no processo de encriptação e decriptação dos dados e são chamadas de chaves porque utilizam informações secretas. Elas são usadas junto com o algoritmo de criptografia para criar o texto cifrado, normalmente a chave é um número primo e seus atributos são:

- Tamanho: o número de bits que a chave irá possuir;
- Espaço: utilização de coleções matemáticas que tenham o mesmo tamanho da chave.

5.1.1 Tipos de Criptografia

As criptografias podem ser divididas de acordo com o tipo e a quantidade de chave que possuem, os dois tipos são os simétricos e os assimétricos.

- Criptografia Simétrica

De acordo com Moraes (2010), na criptografia simétrica o receptor e o transmissor da mensagem devem possuir a mesma chave. Os algoritmos utilizados são rápidos, porém é necessário a utilização de um canal seguro para enviar a chave secreta, pois se alguém descobrir a chave secreta conseguirá ler as mensagens transmitidas. A figura 28, mostra como funciona uma criptografia simétrica.

Figura 28 – Funcionamento da criptografia simétrica

Fonte: Moraes, 2010

De acordo com Moraes (2010), os algoritmos utilizados para reforçar a segurança nas chaves simétricas são:

- DES e 3DES: DES significa (Data Encryption Standard), foi desenvolvido nos anos 70 pelo NIST (National Institute of Standards and Technologies) e a IBM. Sua chave tem o tamanho de 56 bits. Já o 3DES é o mesmo algoritmo, porém aplicado três vezes com três chaves diferentes de 168 bits ou duas chaves diferentes de 112 bits. Como o processo é bem simples é executado mais rápido;

- AES: também criado pelo NIST, utilizando um padrão de alto nível de criptografia, surgiu em concurso realizado pelo NIST e tem como objetivo substituir o DES e o 3DES. Seus pré-requisitos são: ter o algoritmo publicamente definido, usar cifra simétrica com método de encriptação por bloco, possui escalabilidade, pode ser usado em hardware e software e foi baseado nos termos da ANSI. Para a criação foram analisadas as questões de segurança, eficiência, simplicidade e licenciamento. O algoritmo utiliza com um bloco fixo de 128 bits e uma chave que pode variar de 128, 192 ou 256 bits;
- RC4: trabalha com uma cifra baseada em fluxo (40 bits de chave + 24 bits do vetor de inicialização). Possui somente uma chave que é usada para encriptar e decriptar.

O modelo de encriptação por bloco, significa que durante a encriptação um bloco inteiro de texto legível será transformado em texto cifrado. Já na encriptação por fluxo, é definido por uma operação binária e cada bit de texto legível é transformado em um bit de texto cifrado.

- Criptografia Assimétrica

As criptografias assimétricas utilizam duas chaves, uma secreta e uma pública, onde uma das chaves será usada para encriptar e a outra para decriptar os dados. Pode ser chamada de criptografia pública, onde as chaves públicas devem ser colocadas em um ambiente seguro e autenticado. De acordo com Moraes (2010), uma das suas principais características é o fato de utilizar funções matemáticas unidirecionais, ou seja, não é possível chegar ao valor inicial caso seja feita a engenharia reversa. Na figura 29, pode-se ver como funciona a criptografia assimétrica.

Figura 29 –Funcionamento da criptografia assimétrica

Fonte: Moraes, 2010

Pode ser utilizado os seguintes algoritmos:

- RSA: é um algoritmo considerado seguro, caso seja feita fatorações difíceis de quebrar. As chaves pública e privada são números primos muito grandes, o que acaba o deixando mais lento, por isso não é viável a utilização em grandes quantidades de dados;
- Diffie-Hellman: este algoritmo é baseado no uso de chaves logarítmicas e de acordo com Moraes, “é utilizado pelos algoritmos de chave pública para a troca de uma chave pública compartilhada por meio de um canal público (não seguro) de comunicação” (MORAES, 2010, p.136).

Na figura 30, estão descritas as principais diferenças entre a criptografia assimétrica e simétrica.

Figura 30 – Diferenças entre a criptografia simétrica e assimétrica

Atributo	Simétricos	Assimétricos
Número de chave	Única chave compartilhada pelas partes	Par de chaves em cada lado
Tipo de chave	Secreta	Uma pública e uma secreta em cada lac
Proteção das chaves	Distribuição indevida e modificação	Distribuição para a chave privada e modificação para a chave pública
Velocidade	Processo rápido	Processo lento
Tamanho da chave	Fixo*	Variável
Uso típico	Criptografia de grande quantidade de informações	Distribuição de chaves e assinaturas

* Existem alguns algoritmos simétricos com tamanho de chave variável, como o RC2, RC5 e Blowfish.

Fonte: Moraes, 2010

- Criptoanálise

Como já foi explicado anteriormente, a criptoanálise é um estudo de técnicas para burlar códigos criptográficos. Para ser considerado seguro um algoritmo criptográfico tem que ser feito de uma maneira que seja impossível descobrir a chave e encontrar o texto legível a partir do texto cifrado.

Para aumentar a segurança, de acordo com Moraes (2010), é aconselhável que os sistemas de criptografia façam:

- Controle do texto legível. Exemplo: apagar arquivos temporários;
- Evitar utilizar algoritmos de criptografia proprietários;
- Não fazer backup da chave criptográfica.

As criptografias podem ser quebradas de duas formas, realizando criptoanálise ou por força bruta, que se baseia em buscas exaustivas da chave, onde são testadas combinações para encontrar a chave criptográfica.

5.2 Criptografia em Redes Sem Fio

Neste tópico serão tratados os mecanismos e algoritmos de segurança utilizados em redes sem fio que foram baseados no estudo de criptografia.

5.2.1 Wired Equivalent Privacy (WEP)

O Wired Equivalent Privacy (WEP) surgiu com o intuito de prover o mesmo nível de confiança que uma rede cabeada possui. Segundo Moraes (2010), seus objetivos são:

- Fornecer confiança aos dados com um algoritmo de criptografia de chave secreta;
- Ser eficiente principalmente no processamento via software;
- Ter uma técnica de criptografia que fosse usada em todos os países.

Com isso foi criado o RC4, um algoritmo de criptografia. Este algoritmo com uma única chave encripta e decripta os dados do PDU (Protocol Data Unit). A cada transmissão o texto legível passa em um XOR que possui um fluxo aleatório baseado na chave de criptografia para produzir o texto cifrado. O contrário é feito para realizar a decriptação.

De acordo com Moraes (2010), o algoritmo funciona da seguinte maneira:

- A chave secreta é distribuída para as estações que estão transmitindo e recebendo de forma segura;
- A estação que estiver transmitindo uma chave criptográfica de 40 bits será concatenada com o vetor de inicialização (24 bits) produzindo assim a semente;
- A semente vai gerar um fluxo de dados randômicos;
- Depois o fluxo de dados randômicos entra na XOR com o texto legível e gera o texto cifrado;

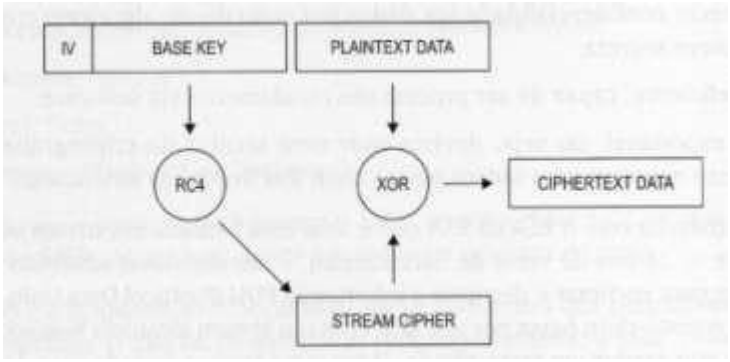
- Ocorrendo isso o texto cifrado é concatenado com o vetor de inicialização e é transmitido.

Para receber a mensagem o processo é reverso, ocorrendo da seguinte forma:

- Leitura do vetor de inicialização que vem junto com a mensagem;
- Concatena com a chave de criptografia para gerar a semente;
- Com isso, o receptor pode gerar o mesmo fluxo de dados randômicos que foi utilizado na transmissão;
- Depois disso é feita a operação XOR entre o fluxo randômico e o texto cifrado, obtendo assim o texto claro;
- Ainda existe a proteção de CRC que faz a verificação de erros durante a transmissão.

Na figura 31, pode-se observar o algoritmo do WEP em funcionamento.

Figura 31 – Funcionamento do WEP



Fonte: Moraes, 2010

Provou-se que o WEP não é um método seguro devido a algumas vulnerabilidades que ele apresenta. De acordo com Rufino (2011), existem três problemas de vulnerabilidades no WEP, são eles:

- Compartilhamento de chave: diz que deve existir uma chave conhecida pelo transmissor e o receptor, porém não indica e nem sugere como a

chave deve ser distribuída. Então um problema é a distribuição das chaves de criptografia;

- Uso do algoritmo RC4: ao usar uma técnica de equivalência numérica, o algoritmo recebe um byte que realiza um processamento e gera como saída também um byte, só que diferente do original. Com isso pode-se identificar quantos bytes tem a mensagem original;
- Vetor de inicialização: o tamanho do vetor de inicialização é muito pequeno, 40 bits, sendo que já existe algoritmos que utilizam 128 bits. Neste caso, se uma mensagem é cifrada com uma chave fixa, toda vez que uma mensagem idêntica é criptografada, terá o mesmo resultado, com isso um invasor poderia ir montando a chave de criptografia a partir das igualdades entre o byte original e o cifrado.

5.2.2 Wi-fi Protected Access (WPA)

O WPA foi criado em 2003 com o intuito de superar as vulnerabilidades do WEP. A primeira versão somente adicionou o TKIP (Temporal Key Integrity Protocol) ao WEP, já que o TKIP ajuda a fornecer um melhor método de gerenciamento de chaves, criando uma chave temporal de 128 bits que é repassada para todas as estações e o access point.

O TKIP age unindo o endereço MAC da estação com a chave temporal, tendo assim 16 octetos adicionados ao vetor de inicialização, produzindo assim a chave de criptografia. Para reduzir a vulnerabilidade do vetor de inicialização, a chave temporal é trocada a cada 10.000 pacotes. De acordo com Moraes (2010), o WPA pode ser dividido em dois tipos, são eles:

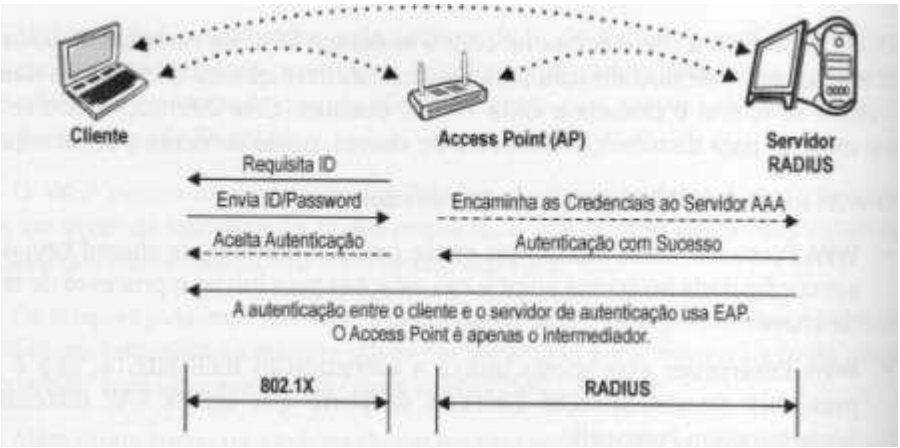
- WPA-PSK (Pre-Shared Key) ou WPA- Personal: é atribuído uma única chave que será compartilhada entre todas as estações associadas a rede sem fio. O método de criação e distribuição de chave do WPA-PSK é o mesmo do WEP, porém neste caso a chave terá 256 bits;

- WPA-Enterprise: é difícil de configurar, requerendo mais servidores para autenticar os usuários da rede, porém é mais fácil de gerenciar em empresas maiores e possui uma camada extra de segurança. No processo de autenticação é utilizado o IEEE 802.1x que é um protocolo baseado na porta EAP (Extensible Authentication Protocol).
- Padrão 802.1x

Padrão 802.1x é um padrão utilizado em redes sem fio e em redes cabeadas, baseia-se no EAP, é um conjunto de mecanismos de autenticação.

De acordo com Moraes (2010), quem realiza a autenticação é um servidor central, baseado no protocolo RADIUS. Em redes sem fio é usado para realizar a troca dinâmica de chaves. Na figura 32, é apresentado como ocorre o processo de autenticação de uma estação na rede com EAP, que utiliza duas fases.

Figura 32 – Autenticação com RADIUS



Fonte: Moraes, 2010

- Vulnerabilidades do WPA

De acordo com Rufino (2011), as WPA são mais seguras que o WEP, porém ainda apresentam vulnerabilidades, entre elas está:

O uso de senhas pequenas ou de fácil adivinhação: este caso retrata o uso de programas que utilizam a força bruta para descobrir a senha. Então, senhas com menos de 20 caracteres estão suscetíveis a este tipo de ataque. O que acontece é que os fabricantes colocam senhas pequenas pensando que o gerente de redes irá alterá-la quando colocar o dispositivo para funcionar, porém muitos não fazem isso, tornando o equipamento mais vulnerável do que as redes WEP;

Ataques ao TKIP: é um problema parecido com o que acontecia com o vetor de inicialização do WEP, chamado de “chopchop”, onde o objetivo não é descobrir a chave de criptografia do WPA e sim de decifrar um tráfego previamente capturado.

5.2.3 WPA2

O WPA2 foi lançado em 2004, veio para atingir um alto nível de proteção aos dados, para que somente pessoas autorizadas tenham acesso à rede. O WPA2 está dentro do padrão 802.11i e utiliza a última versão do AES, de acordo com Moraes, “esse algoritmo é certificado no mais alto nível de segurança pelo governo dos Estados Unidos com o FIPS 140-2” (MORAES, 2010, p.158). O método inovou na forma de autenticação, criando dois modos diferentes de realizá-la, são eles:

- Personal Mode: é uma solução para redes domésticas e para redes de pequenas empresas, onde é necessário uma pre-shared key para conseguir realizar a autenticação;
- Enterprise Mode: é a mesma utilizada no WPA- Enterprise, baseada no padrão 802.1x com servidores de autenticação RADIUS.

Na figura 33, é possível ver as diferenças entre as versões do WPA.

Figura 33 – Diferenças entre o WPA e o WPA2

	MODO	WPA	WPA2
Personal Mode	Autenticação	Pre Shared Key	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES
Enterprise Mode	Autenticação	IEEE 802.1X/EAP	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES

Fonte: Moraes, 2010

- Vulnerabilidades do WPA2

De acordo com Moraes (2010), este algoritmo, WPA2, utilizando o AES, é a solução mais segura que existe, devido ao AES que é um algoritmo de criptografia por enquanto inviolável, sendo necessário milhares de anos para poder quebrar a chave de 256 bits do AES. Porém tem algumas fraquezas:

- A pre-shared key é suscetível a ataques de força bruta, principalmente quando a frase secreta é de baixa complexidade.

5.3 Ameaças e Riscos

As redes sem fio são cercadas de vulnerabilidades, portanto nesta seção serão abordados os principais riscos e ameaças.

5.3.1 Segurança Física

De acordo com Rufino (2011), muitas vezes a segurança lógica é supervalorizada e os administradores acabam esquecendo do espaço físico em que a rede será inserida. A parte física é um fator importante devido a área de alcance que uma rede sem fio possui. Onde deve ser pensado a posição dos componentes de rede para não facilitar o acesso não autorizado e outros tipos de ataque. Deve-se analisar o padrão para verificar qual o alcance da rede, se será 802.11b, 802.11a ou 802.11g,

e a potência dependendo da área de cobertura e qualidade do sinal. Deve-se também escolher uma antena que se encaixe nas características da rede.

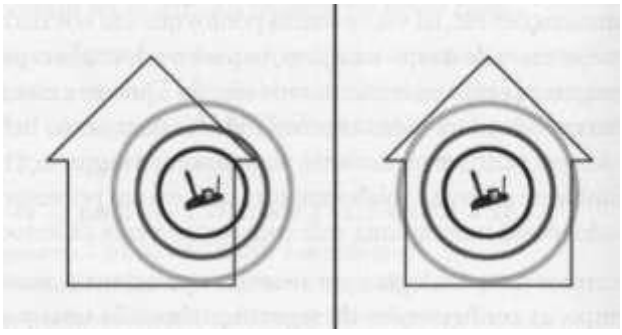
5.3.2 Configuração de Fábrica

São desenvolvidos cada vez mais aparelhos com novos e melhores mecanismos de segurança, porém muitas vezes este equipamento vem com uma configuração padronizada pela fábrica. Está configuração padrão envolve senhas de acesso e endereço IP. De acordo com Rufino (2011), muitos administradores de redes inexperientes não trocam estas configurações, dando condições para que um invasor as utilize para obter acesso a rede, identificando todas as configurações podendo até mesmo modificá-las. Outras configurações que devem ser alteradas são: as chaves WEP, WPA, WPA2 e o SSID.

5.3.3 Envio e recepção de sinal

Sabe-se que o sinal da antena de um access point é enviado em várias direções, portanto a localização do roteador influencia muito na qualidade e na segurança da rede. De acordo com Rufino (2011), quanto mais ao centro do local em que a rede for instalada estiver o access point, evitará que o sinal se irradie para fora, deixando assim brechas para que um atacante possa invadir a rede. Na figura 34, mostra tal problema.

Figura 34 - Colocar o access point ao centro do ambiente físico



Fonte: Rufino, 2011

5.3.4 Mapeamento do Ambiente

O mapeamento do ambiente é um procedimento que visa a obtenção do maior número de informações sobre uma rede, permitindo saber de detalhes que facilitam o lançamento de ataques precisos e com menos chance de ser identificado. Por isso, os invasores fazem primeiramente um mapa do ambiente da rede que eles querem atacar.

- Mapeamento específico para redes sem fio.

Em redes sem fio o mapeamento é uma forma de identificar as redes sem fio que estão próximas, isso é feito com comandos ou programas específicos. No ambiente Linux, é possível a partir do comando: iwlist, com a opção scan. No Windows, existe um programa padrão que é possível detectar as redes sem fio.

Para Rufino (2011), somente as redes que os access points permitem difusão de nomes das redes são detectadas por esses programas ou comandos. Para redes fechadas são necessárias ferramentas específicas para o sistema operacional e o tipo de rede.

5.3.5 Captura de Tráfego

Como foi dito no capítulo 4, as ondas de radiofrequência se propagam pelo ar e caso as informações não estejam criptografadas, é possível ter acesso ao tráfego e ao conteúdo das informações que ali transitam. Para isso, um invasor só precisa estar na mesma área de cobertura do sinal a ser capturado, usando um computador, notebook ou smartphone com uma ferramenta de captura de tráfego.

5.3.6 Equipamentos sem fio em ambientes cabeados

Muitos aparelhos saem de fábrica com configurações cabeadas e sem fio, e quando se está em um ambiente composto somente por rede cabeada o administrador não encontra razões para realizar um monitoramento de rede sem fio. Então caso um aparelho desses ative (acidentalmente) o modo sem fio poderia ser uma maneira de

fácil acesso para um invasor. De acordo com Rufino (2011), uma forma de fazer isso é um invasor conectar à rede cabeada da empresa que ele deseja invadir e com isso ele pode fornecer um acesso a um segundo invasor externo somente habilitando a placa Wi-fi para o modo Ad-hoc e permitir o roteamento com a rede cabeada.

5.4 Formas de ataque

Os invasores utilizam diversas técnicas para se aproveitarem das vulnerabilidades do sistema, com isso podem burlar a segurança e ter acesso a informações sigilosas. De acordo com Caraça e Penna, as principais são:

5.4.1 Spoofing

De acordo com Oliveira citado por Caraça e Penna (2009), o spoofing é uma técnica contra a autenticidade em que uma pessoa externa se passa por uma pessoa ou um computador. Para isso acontecer o invasor convence alguém de ser algo ou alguém que ele não é, assim ele conseguirá ter livre acesso ao sistema.

5.4.2 DNS Spoofing

O DNS é o servidor onde ficam armazenados os nomes dos sites, que são convertidos para seus respectivos IP’s. Quando este tipo de ataque ocorre, o servidor de DNS é destruído para que as máquinas do invasor passem a ser confiáveis. Com o controle do servidor de DNS, o invasor pode alterar os registros, podendo alterar o endereço IP de uma máquina invasora por um de uma máquina confiável.

5.4.3 Sniffers

Sniffers é um software que controla o tráfego na rede, podendo capturar decodificar e analisar o conteúdo dos pacotes enviados. Este programa pode ser usado para realizar manutenção na rede pelos administradores do sistema, mas também é usado por invasores que querem ter acesso aos dados de login dos usuários.

5.4.4 Ataque do tipo negação de serviço

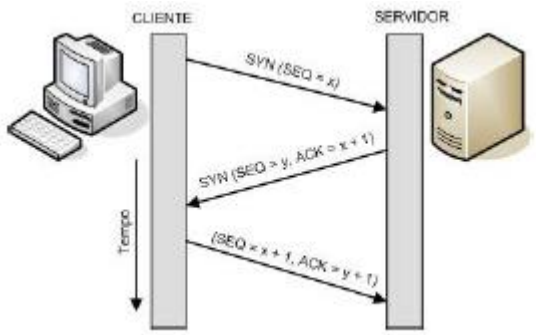
De acordo com Cruz (2013), o ataque de negação de serviço consiste em aproveitar de alguma vulnerabilidade para impedir que usuários legítimos tenham acesso a um determinado serviço ou equipamento, ou seja, são todo tipo de ataque que ferem o princípio da disponibilidade.

Segundo Pinheiro (2014), há diversas formas de executar um ataque de negação de serviço, os principais são:

- TCP SYN Flooding

TCP SYN Flooding - Quando um cliente inicia uma conexão TCP com um servidor, ele primeiramente envia uma mensagem SYN para este servidor. O servidor, por sua vez, responde a esta mensagem com outra do tipo SYN-ACK. O cliente, então, completa o handshake respondendo uma mensagem ACK. A partir daí a conexão entre o cliente e o servidor está aberta e dados podem ser trocados entre eles. O ataque surge no estado em que o servidor está esperando a última mensagem ACK do cliente para finalizar o handshake. Depois disso, o servidor separa uma porção de memória para guardar as informações desta conexão quase-aberta. A memória é liberada quando o servidor receber o ACK do cliente ou até a conexão expirar. Realizando esse processo inúmeras vezes em pouco tempo, o servidor não tem como estabelecer novas conexões, e assim, não consegue prover seus serviços.

Figura 35 - Estabelecimento da conexão TCP



Fonte: Cruz, 2013

- UDP Flooding

O UDP Flooding consiste no envio de vários pacotes UDP para a vítima, consumindo assim toda a largura de banda disponível. Fazendo com que o servidor ou a rede não tenha largura de banda disponível para iniciar novas conexões com usuários legítimos.

- Rudy

O Rudy é um ataque difícil de ser detectado, pois gera um volume muito baixo de tráfego. Seu objetivo é explorar vulnerabilidade no protocolo HTTP quando há a utilização do método POST para requisitar mensagens. Nesse tipo de ataque, são enviados apenas 1 byte de dados por pacote em intervalos aleatórios de tempo, sem deixar que ocorra timeout na conexão, fazendo com que o servidor não consiga mais receber novas conexões por conta das centenas de conexões abertas.

- Slowloris

Slowloris também é um ataque difícil de ser detectado, pois gera um volume de tráfego baixo. Explorando vulnerabilidades no protocolo HTTP, fazendo com que toda requisição HTTP seja enviada sem a sequência de fim de linha, fazendo com que o servidor deixe a conexão aberta e aloque recursos que estão esperando pela

sequência de término. Durante o ataque, são feitas diversas conexões deste tipo e em pouco tempo um usuário legítimo estará impedido de usar o serviço.

De acordo com Cruz (2013), algumas medidas podem ser tomadas para evitar os ataques de negação de serviço, são elas:

- Atualizar sempre o firmware dos equipamentos, juntamente com os patches de segurança;
- Desativar os serviços de rede que não utilizados;
- Implementação de filtros nos roteadores;
- Monitorar a rede ou o sistema, estabelecendo uma base para definir o que uma atividade normal na rede para poder detectar variações incomuns.

Para Pinheiro (2014, os ataques podem ser divididos pelas fraquezas que exploram, sendo elas:

- Ataques semânticos, utilizam de vulnerabilidades de algum protocolo ou aplicação para consumir os recursos. Exemplos deste tipo: TCP SYN;
- Ataques de força bruta ou inundação, deixam serviços e redes indisponíveis através de um grande volume de tráfego ou de requisições válidas. Exemplo: UDP Flooding.

Neste trabalho são tratados os seguintes tipos, TCP SYN e UDP Flooding, pois se aplicam a redes sem fio, enquanto os outros exemplos são usados em servidores e serviços.

5.4.5 Ataque do tipo DDoS

O ataque do tipo DDoS é muito parecido com o tipo DoS, porém no DDoS a máquina a ser sobrecarrega é escolhida a partir de alguma vulnerabilidade encontrada pelo invasor que coloca diversos agentes, máquinas zumbis, para dispararem

diversas requisições se transformando em diversos ataques do tipo DoS ao mesmo tempo.

5.4.6 Exploits

Exploits são programas que abusam das vulnerabilidades encontradas em programas ou sistemas para conseguir acesso ao root ou ao usuário administrador.

5.4.7 Vírus

Os vírus são arquivos infectados, utilizados por invasores de maneira maliciosa infectando outros arquivos em outros programas. Essa infecção começa quando o arquivo é executado, assim ele danifica tudo por onde ele passa, como exemplo tem-se os Worms que fazem exatamente isso.

Os vírus podem ter diversos tipos, mas os principais são os cavalos de troia ou trojans, são vírus inteligentes que são manipulados da forma que o invasor queira. Este tipo de vírus pode ter controle do computador, podendo realizar tarefas simples como mexer o mouse e usar o IP da máquina para realizar outros ataques.

Os cavalos de Tróia podem ser divididos nos seguintes tipos:

Utilização da porta TCP e UDP para invadir: normalmente são utilizados em servidores, possui dois arquivos, um no computador atacado e um no computador do invasor, que poderá controlar o servidor;

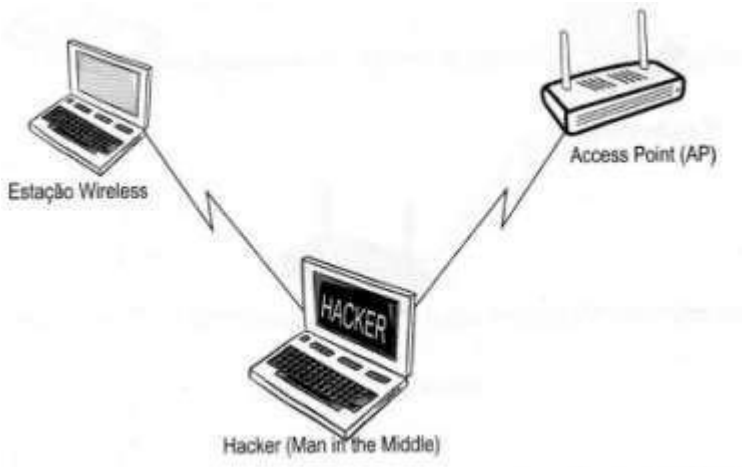
- Trojans de informação: são trojans que se acomodam na máquina invadida e com isso pode capturar informações sigilosas como: senhas, login, CPF e outros. Ele pega a informação e envia por e-mail ao invasor;
- Trojans de ponte: com esse trojan o invasor pode utilizar o IP da máquina invadida para realizar outros ataques;

- Rootkits: ocorrem nos sistemas Linux e Unix, age substituindo arquivos executáveis por outros infectados, conseguindo assim acesso ao invasor, que por causa dos arquivos terá seu log salvo.

5.4.8 Man in the middle

Man in the middle ou homem no meio, é um tipo de ataque em que o invasor intercepta os dados para conseguir acesso as informações de conexões entre o access point e as estações, podendo inclusive controlar os dados que trafegam nesse meio. De forma resumida o invasor age como se fosse um proxy onde ele pode interceptar e alterar as mensagens que passam por ele. A figura 36, representa a forma de ataque man in the middle.

Figura 36 – Forma de ataque man in the middle



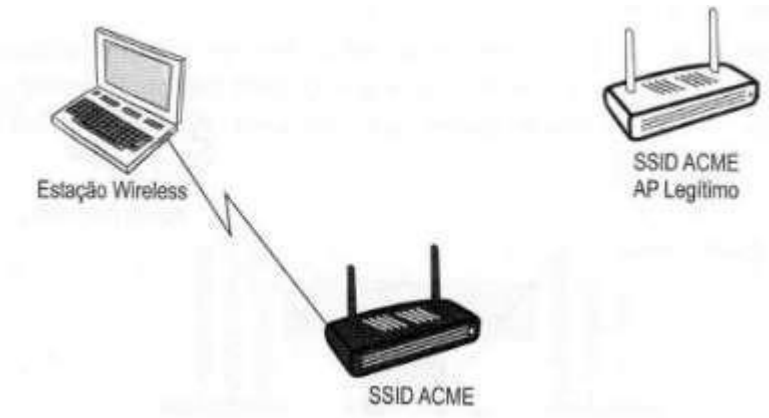
Fonte: Moraes, 2010

5.4.9 Evil Twinks

É um ataque muito parecido com o man in the middle porém neste caso o invasor se encontra entre o usuário e o access point, se tornando assim um access point falso, porém o usuário acha que ele é o verdadeiro. Dessa forma, ele pode conseguir dados do usuário, veja o exemplo: o invasor pode criar uma página em

HTML e pedir para que o usuário insira seu login e senha. A figura 37, mostra como ocorre o Evil Twinks.

Figura 37 – Como ocorre o ataque Evil Twinks



Fonte: Moraes, 2010

5.4.10 War Driving

Nesta forma de invasão, os invasores saem pelas ruas com laptops e com programas sniffers e uma antena para mapear as conexões de rede sem fio. Com isso, ele consegue identificar pontos de acesso vulneráveis onde ele poderá realizar um scanning de tráfego, isso é, poderá capturar os pacotes enviados dentro da rede.

5.4.11 Engenharia Social

Engenharia social também é uma técnica utilizada para obter informações de uma organização, através do poder de persuasão do invasor para enganar e convencer as pessoas de que o engenheiro social é alguém que na verdade ele não é.

5.5 Técnicas e ferramentas de ataques

As vulnerabilidades citadas na seção anterior podem ser exploradas a partir de técnicas e programas que serão explicados nesta seção. De acordo com Rufino (2011), as ferramentas e técnicas são bem específicas para cada modelo de placa de rede, padrão.

5.5.1 Airtraf

Ferramenta que permite coletar informações sobre as redes identificadas, como por exemplo: quantas pessoas estão conectadas nela, quais serviços ela utiliza, entre outros. De acordo com Rufino (2011), este programa é suportado pelas placas de rede: Orinoco/Proxim, Prism2/Hostap ou Aeronet/Cisco. Se a placa é suportada pelo programa, então o programa irá executar uma varredura para identificar as redes disponíveis.

Com a análise feita, é necessário escolher o access point que será monitorado.

Com isso percebe-se que esta ferramenta é muito útil para coletar informações como endereço IP da rede e endereços MAC dos clientes, além de ser útil para invasores é muito útil para administradores que desejam monitorar a rede da qual ele é responsável.

5.5.2 Airsnort

Segundo Rufino (2011), esta é a ferramenta mais antiga, por isso ela atinge somente uma pequena quantidade de placas de rede, são elas: Orinoco/Proxim, Prisms2 e Atheros. Esta ferramenta apresenta uma característica que o diferencia dos outros, o fato de que mesmo a placa não seja suportada diretamente, pode-se colocá-la manualmente em modo monitor e escolher o item Other na opção Driver Type.

Suas principais funcionalidades são:

- Quebra de chave WEP no meio da captura do tráfego;

- Identificação das redes e informações, no caso podem ser vistos somente o SSID e o endereço MAC;
- Se uma rede utiliza ou não o padrão WEP;
- Pode-se varrer todos os canais de uma só vez ou então pode-se varrer somente o canal que for necessário.

5.5.3 BSD Air Tools

BSD Air Tools é um conjunto de ferramentas cujo os objetivos são o monitoramento do tráfego da rede e a captura de pacotes para quebrar o protocolo WEP. A sua desvantagem é o nível alto de restrição, podendo ser utilizado somente por máquinas que operam no padrão 802.11b e que possuam placas de rede Prism2 ou Orinoco. Sua principal funcionalidade é quebrar chaves WEP.

5.5.4 Netstumbler

Ferramenta com o objetivo de mapear e identificar as redes sem fio no sistema operacional Windows. De acordo com Rufino (2011), sua maior vantagem é que ela utiliza os padrões mais novos do mercado, desde que estejam no padrão 802.11 /a/b/g. Reconhece um número maior de placas de rede. Com ela é possível identificar o nome da rede, endereço MAC, nível do sinal e outras.

Sua desvantagem é que não captura o tráfego e nem quebra a chave WEP, ela é uma ferramenta somente para levantamento de informações, e por sinal, os faz muito bem.

5.5.5 Kismet

Ferramenta sempre atualizada e em crescimento, ela pode ser usada para realizar mapeamento de redes, podendo identificar redes estruturadas e Ad-hoc além de muitas outras coisas como: SSID, nível de sinal, canal utilizado, endereço MAC dos usuários entre outras informações. A ferreamente pode também realizar a captura de tráfego, onde tudo que ele captura é armazenado em um arquivo dump ou então pode ser visto em tempo real pelo atacante.

5.5.6 Fake AP

Fake AP é uma ferramenta que coloca o atacante entre o cliente e access point, assim o atacante se passará pelo access point podendo capturar senhas e conseguir informações que trafegam naquela transmissão.

Suas desvantagens são: precisa de uma interface para usar no modo de gerência, podendo permitir outro tipo de estrutura como o Ad-hoc. Também precisa de uma relação com os access points originais para que depois de capturar a informação desejada possa redirecionar o tráfego para eles.

5.5.7 Air Jack

Ferramenta que faz o invasor se passar como o access point para conseguir informações dos usuários da rede. Sua maior vantagem é a capacidade que tem de fazer o ataque homem no meio com HTTPS com um certificado falso, que é necessário que o usuário aceite.

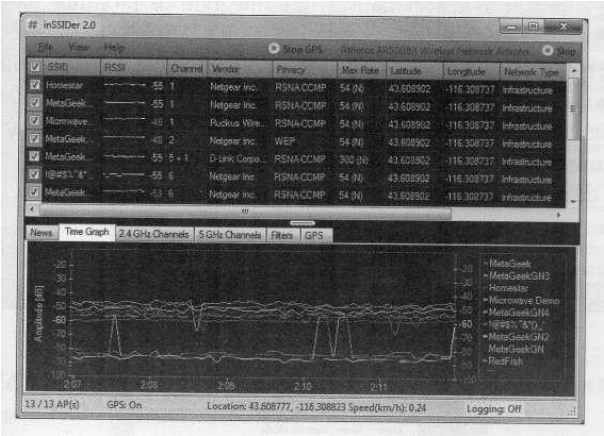
5.5.8 Air Snarf

Air Snarf também é uma ferramenta que atrai os usuários para um falso access point, só que neste caso é com serviços de telefonia, assim que o usuário acessar o access point falso os dados são encaminhados para um HTTP e DNS falso, com isso o invasor conseguirá a partir do acesso no celular o usuário, senhas, contatos, entre outras informações pessoais.

5.5.9 inSSIDer

Permissão de visualizar redes, canais e mecanismos de segurança que uma rede sem fio possui, junto com uma interface gráfica que ajuda no monitoramento, distribuição de canais, potências, entre outros. Consegue identificar o padrão 802.11n, está disponível para Windows e Linux. Na figura 38, é possível ver uma tela do programa em execução.

Figura 38 – Tela do programa inSSIDer



Fonte: Rufino, 2011

5.5.10 Kali Linux

De acordo com Broad e Bindner (2014), o Kali Linux é um sistema operacional com distribuição Debian 7.0, voltado para testes de segurança criado pela Offensive Security. O SO possui diversas ferramentas, utilizadas para fazer avaliações de segurança em sistemas e em redes.

5.6 Ferramentas e Técnicas de Defesa

Para conseguir defender a rede sem fio dos ataques é necessário a combinação de várias técnicas de defesa. Entre elas tem-se:

5.6.1 Monitoramento de Rede

De acordo com Benício (2015), “gerenciamento de redes pode ser definido como coordenação, controle de atividade e monitoramento de recursos, assegurando na medida do possível, confiabilidade, segurança e alta disponibilidade.” O monitoramento faz parte desse processo, ajudando na coleta, diagnóstico e notificação de informações sobre equipamentos e serviços da rede. Segundo Bueno (2012), seu funcionamento é baseado no funcionamento agente e gerente, sendo o

gerente o computador que possui o software de gerenciamento de rede e o agente é onde temos a base com dados a serem consultados pelo gerente.

Ainda segundo Bueno (2012), o monitoramento pode ser dividido em dois tipos local e remoto. O monitoramento local há uma parte do software instalado no dispositivo gerenciado que executa tarefas e rotinas. Para o monitoramento remoto, o equipamento gerente faz consultas periódicas ao dispositivo gerenciado que retornará as respostas, assim sempre haverá uma requisição e sua respectiva resposta.

5.6.1.1 Protocolo SNMP

Segundo Filho (2014), o SNMP (Simple Network Management Protocol) é um protocolo utilizado para unificar e padronizar informações de gerência. Muito utilizado no monitoramento remoto para fazer a comunicação das MIB's (Management Information Base) entre o gerente e o agente.

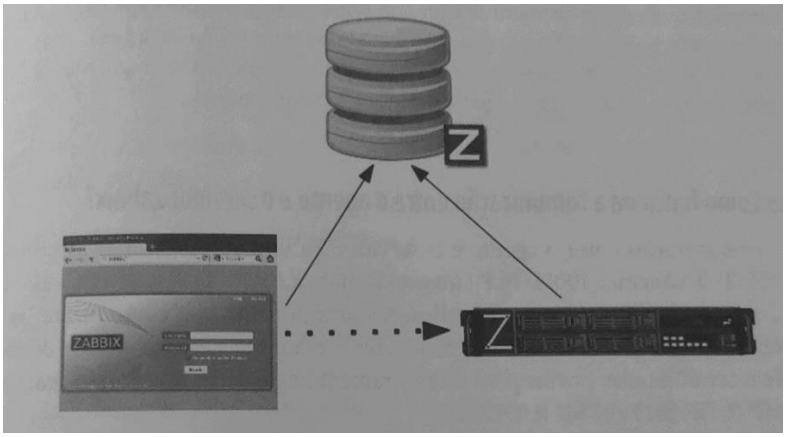
De acordo com Benício (2015), a troca de informações são feitas via UDP (User Datagram Procol) nas portas 161 (requisições) e 162 (traps). Sendo executadas através de três operações (Stalling, 2005):

- GET: permite que o gerente recupere o valor dos objetos no agente;
- SET: permite que o gerente defina o valor dos objetos no agente;
- NOTIFY (TRAP): permite que um agente envie notificações não solicitadas à estação de gerenciamento sobre os eventos importantes.

5.6.1.2 Zabbix

Zabbix é uma ferramenta de monitoramento, gratuita e multi plataforma. De acordo com Horst, Pires e Déo (2015) o Zabbix utiliza um sistema de gerenciamento de banco de dados para armazenar dados e configurações, os módulos de coleta e sincronismo de dados foram desenvolvidos em C e sua interface web é baseada em php.

Figura 39 - Comunicação entre servidor Zabbix, Banco de Dados e Interface Web



Fonte: Horst, Pires e Déo, 2015

Suas principais funcionalidades de acordo com Horst, Pires e Déo (2015) são:

- Compatibilidade com diversos sistemas, aplicações e servidores;
- Monitoramento com ou sem o uso de agentes;
- Suporte ao protocolo SNMP;
- Autenticação Segura de Usuário;
- Permissões Flexíveis;
- Auditoria;
- Envio de notificações via e-mail, sms, slack, entre outros;
- Suporte a scripts.

Segundo Horst, Pires e Déo (2015), a comunicação entre o agente e o servidor zabbix podem variar de acordo com o item que está sendo coletado, quando é normal ou passivo o servidor conecta a um agente que repassa os dados; quando é ativo o fluxo inverte e o agente se conecta ao servidor. Toda essa comunicação é feita através de prta TCP.

A forma de organização do zabbix é dividida em: template, host, itens e triggers. De acordo com Horst, Pires e Déo (2015):

- template é um modelo de regras de coleta, alertas e representações gráficas de todos elementos monitorados;
- item é onde é feita a indicação de um dado a ser coletado;
- trigger ou gatilho é a utilização dos itens para informar que uma determinada condição foi alcançada, gerando assim uma notificação.
- host é parâmetro que vai unificar os itens, triggers a um determinado equipamento ou aplicação.

O zabbix possui integração com o protocolo SNMP, para isso é necessário instalar o pacote snmp-mibs-downloader no servidor, onde será possível fazer a coleta das variáveis da MIBS através do comando snmpget e snmpwalk, que fará a interação com os valores das variáveis no momento da execução.

5.6.1.3 FastNetMon

De acordo com Doubladez (2018), o FastNetMon é um analisador de tráfego lançado recentemente e com capacidade para detectar ataques de negação de serviço com suporte a ferramentas de controle de fluxo como: NetFlow, IPFIX e sFLOW.

Ele pode detectar tráfego malicioso na rede e bloquear imediatamente o IP auxiliando na mitigação dos ataques através do flow. Tem compatibilidade com os principais equipamentos de rede como Cisco, Juniper, A10 Networks, Extreme, Brocade e MikroTik.

5.6.2 Configurações do access point

De acordo com Rufino (2011), o access point é o principal dispositivo em que a segurança deve ser implementada, pois se algum invasor conseguir acessá-lo, poderá colocar toda a rede em risco.

Quando consegue-se proteger o access point, a rede será protegida de ataques que objetivam o acesso não autorizado e a negação de serviço.

- Desabilitar a difusão do envio do SSID

Desabilitar a difusão do envio do SSID é a primeira configuração que deve ser feita, quando se faz isso, os invasores encontram dificuldades para encontrar o nome da rede, dificultando assim ataques maliciosos que precisam reconhecer o nome da rede para serem executados, de acordo com Rufino (2011), este processo é chamado de segurança por obscuridade, isto é, mantém a segurança escondendo informações.

Segundo Rufino (2011), ela gera segurança em alguns tipos de ataque, mas em outros ataques como a escuta de tráfego é ineficaz pois o invasor conseguirá o SSID pelos: beacons, por um concentrador ativo, quando é realizada a busca por um concentrador e em requisições de associação e de reassociação.

- Modificar o SSID padrão

Modificar o SSID padrão é considerado também uma segurança por obscuridade, na qual é necessário alterar o SSID padrão do concentrador, o que ajudará pelo menos a retardar o ataque do invasor, e neste tempo o administrador pode perceber que está sendo atacado, podendo assim detectar o invasor e tomar as medidas necessárias para retomar a segurança.

De acordo com Rufino (2011), em alguns casos os administradores não trocam o SSID padrão, assim os invasores podem descobrir o modelo do concentrador e com isso podem ter acesso ao SSID da rede. Por isso, é necessário realizar a mudança, para dificultar ainda mais o ataque planejado por um invasor.

- Substituir o endereço MAC

O IEEE definiu que todo equipamento deve ter um número único, este número é chamado de MAC e é utilizado para encontrar um aparelho, independentemente de sua marca ou modelo.

Para saber o endereço MAC em sistemas operacionais Windows utiliza-se o seguinte comando, no prompt de comando:

C:\ >ipconfig /all

Nos sistemas operacionais Unix utiliza-se:

ifcongif –a

A troca do endereço MAC evita a identificação da configuração padrão de fábrica, que normalmente a primeira a ser testada pelos invasores.

- Desabilitar configurações via Web

Os roteadores podem ser configurados por uma página da internet, é uma prática muito utilizada para as redes cabeadas que são preparadas para este tipo de acesso, através de mecanismos que monitoram e autenticam os usuários. Porém nas redes sem fio é melhor desabilitar esta opção, pois assim seria evitado que o usuário e a senha fossem interceptados por um invasor.

- Não reconhecer usuários que possuam SSID igual a ANY

Quando um usuário possui este SSID significa que ele está querendo acesso em qualquer access point disponível na rede sem fio. Este tipo de SSID é muito usado por invasores que estão explorando uma rede qualquer.

- Usar o roteador em modo ponte

Esta solução baseia-se em remover o endereço IP, o que impede o acesso remoto ao equipamento. De acordo com Rufino (2011), é muito usada em ambientes de rede em que não se pode utilizar recursos que possam bloquear o acesso ao roteador ou que a rede sem fio seja usada como acesso casual para realizar mudanças na configuração. É usado nos casos nos quais não é necessário fazer constantes alterações de configuração e quando não há filtros de acesso, assim no

modo ponte, como não há o endereço IP, dificulta a captura de informações como usuário e senha.

5.6.3 Defender os equipamentos do usuário

Este tipo de defesa se baseia em prevenir acesso não autorizado as configurações de segurança da rede e evitar que durante a transmissão os dados sejam capturados. Então para isso é utilizado o Publicly Secure Packet Forwarding (PSPF), que evita um ataque direto entre clientes que estejam usando o mesmo roteador. Esta técnica previne ataques diretos, porém não evita a interceptação dos pacotes de dados, portanto, deve ser utilizado junto com outras técnicas.

5.6.4 Utilizar criptografia

A criptografia protege os dados que trafegam na rede, porém se o invasor obter acesso ao equipamento do usuário, ele pode conseguir quebrar a criptografia e desta forma pode descriptografar os dados que são transmitidos. Para evitar isso pode-se proteger o equipamento com firewalls, anti-spyware e antivírus, ou inserir mecanismos de autenticação que utilizam senhas descartáveis, cartões processados e tokens.

As senhas descartáveis ou On-time password (OTP), é muito simples e fácil de implementar, esta técnica baseia-se na utilização de uma senha diferente a cada acesso. Assim fica quase impossível capturar a senha pela rede.

A cada sessão, uma senha é usada para autenticar o usuário, logo após a realização da autenticação, ela é descartada. Para fazer isso são usados softwares, um deles é opie password, onde é inserida a senha mestre e com ela gera-se as outras senhas usando OTP, que é dividido em opie info, que exibe o desafio atual para determinado usuário e o opie key, que gera as chaves OTP.

As senhas que utilizam os métodos de autenticação do EAP, podem utilizar cartões processados. Segundo Rufino (2011), para que ocorra o armazenamento é necessário que a senha de acesso à chave originalmente esteja no arquivo de

configuração, e seria necessário o acesso a essa chave pelo servidor RADIUS. Porém se esta ficar armazenada nos computadores, ela fica suscetível a ataques, para evitar que isto aconteça, a senha é armazenada em cartões processados ou tokens.

5.6.5 Ferramentas de defesa

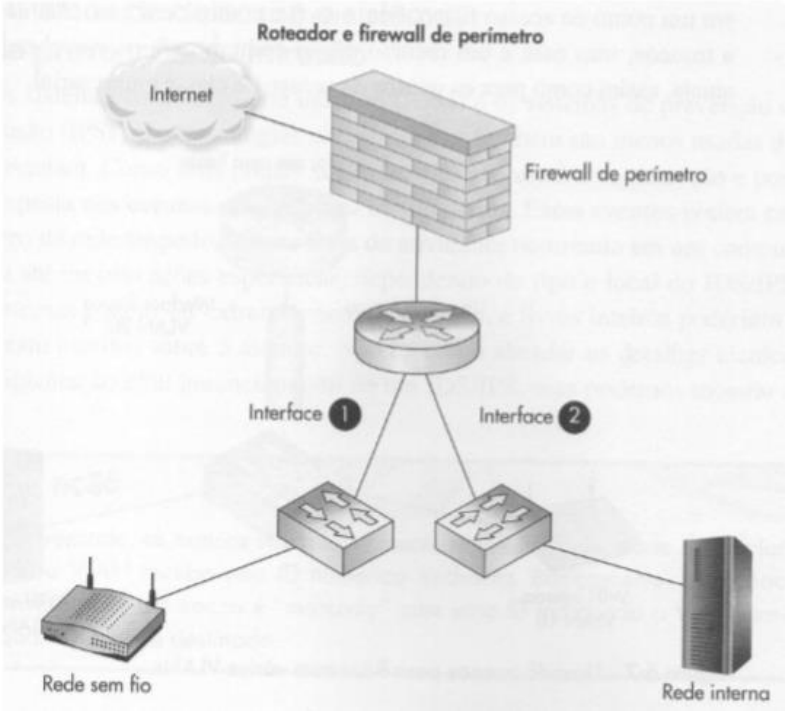
As ferramentas de defesa auxiliam o administrador a monitorar a rede, controlar o tráfego de informações, proteger os dados, fazer filtros de acesso e detectar ataques. Algumas serão detalhadas a seguir.

5.6.5.1 Firewall

Firewall ou parede de fogo é uma camada de proteção que tem como objetivo o bloqueio de acesso as informações, porém esta parede não impede que os dados transitem, deixa eles fluírem.

De acordo com Wrightson (2014), o firewall é um componente importante para manter a rede segura, porém em muitos projetos de rede sem fio ele não é incorporado. Na figura 40, mostra o funcionamento básico de um firewall para realizar a segmentação entre a rede sem fio e a rede interna. As duas interfaces fazem com que não exista tráfego entre a rede sem fio e a rede interna, assim incrementará a segurança já que ambos só terão acesso à internet. É muito usado quando se tem duas redes sem fio e uma não pode ter acesso aos dados da outra.

Figura 40 – Funcionamento básico de um firewall



Fonte: Wrightson, 2014

5.6.5.2 Honeypots

Os honeypots são sistemas usados para atrair um possível invasor mostrando as vulnerabilidades da rede ou alguma outra informação específica que o interesse. Assim eles são utilizados como prova de que tem alguém tentando invadir a rede. Pode-se utilizá-los também para tentar encontrar o invasor.

5.6.5.3 wIDS

De acordo com Rufino (2011), “o wIDS consegue detectar não somente tipos de ataques, mas também anomalias e procedimentos suspeitos” (RUFINO, 2011, p.188). Esta ferramenta é compatível com diversas placas e chipsets. Além de ter a opção de agir como um honeypots.

- Ela monitora os tráfegos dos seguintes tipos:

- Requisições vindas da varredura;
- Frequência de requisições de reassociação;
- Análise da sequência numérica dos pacotes 802.11;
- Detecta grande volume de requisições de autenticação por um determinado intervalo de tempo.

- Garuda

Ferramenta que objetiva criar e mudar assinatura de pacotes suspeitos já analisados. Tem problema de incompatibilidade, já que só pode ser usado nas placas Aironet. Ele pode ser ativado por algum serviço ou pode ser ativado a partir de alertas que chegam diretamente no console. Ele pode usar uma base de dados do MySQL, onde as informações de pacotes suspeitos serão salvas no banco de dados no MySQL.

5.6.5.4 AirIDS

Programa que faz análise de tráfego suspeito na rede sem fio, porém, diferente das outras, ela só é compatível com as placas prism2, aironet e com o sistema operacional Linux. Para executá-lo, basta executar o programa e colocar um arquivo de assinaturas na mesma página. É mais fácil de rodar, porém é incompatível com a maioria das placas e sistemas operacionais atuais.

5.6.5.5 Kismet

Kismet é uma ferramenta usada no monitoramento e detecção de ataques. Os ataques são detectados a partir da identificação de ferramentas de ataques como Netslumber, AirJack e outras, de tráfego incomum na rede. Como pode ser integrado a um GPS, ele consegue detectar a localização física do invasor.

5.6.5.6 Beholder

Beholder é um programa que veio para corrigir algumas vulnerabilidades de outras ferramentas de detecção de ataque. Suas principais características são: utiliza código aberto com novas formas de detectar ataques, uso de expressão regular para alertar sobre os SSID's que trafegam na rede, consegue detectar Karma e ferramentas parecidas, entre outras.

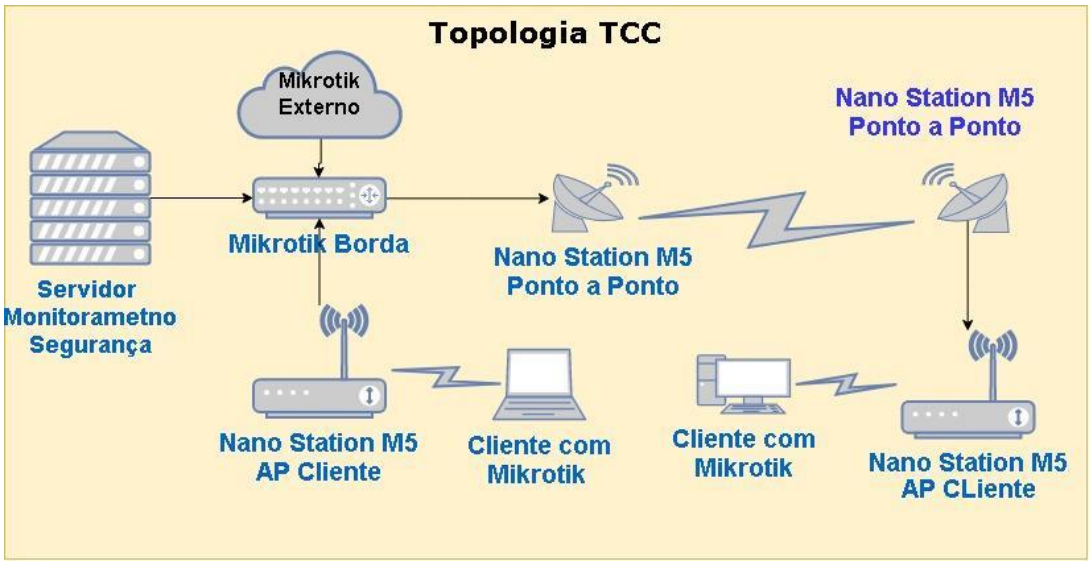
Pode ser usado para monitorar vários ambientes de rede sem fio, podendo alertar no console ou no serviço alguma ação suspeita.

6. METODOLOGIA

De acordo com Starosky (2009), a pesquisa do trabalho é de natureza aplicada já que os resultados são baseados em um ambiente de teste prático, com abordagem quantitativa onde os dados são coletados, analisados e classificados para identificar um possível ataque ou não; e pode ser classificada como uma pesquisa com objetivo exploratório na qual é necessário descrever ferramentas para solucionar o problema.

Para fazer a validação dos testes foi montado um ambiente sem acesso à internet, com um servidor Ubuntu virtualizado, três roteadores Mikrotik 750G e quatro rádios Ubiquiti Nano Station M5. Os equipamentos foram dispostos conforme figura 41 abaixo:

Figura 41 - Disposição dos equipamentos



Fonte: Próprio autor, 2019

6.1 Ambiente de teste

Foi criado um servidor Ubuntu versão 18.04.2 virtualizado pelo programa Virtual Box e a máquina possui as seguintes configurações: 4 GB de memória ram e 40 GB de HD. Os valores foram escolhidos devido à baixa quantidade de hosts no ambiente

teste, já que este número interfere na capacidade de processamento, armazenamento e memória do servidor, resumindo o número de hosts e o consumo de recursos são diretamente proporcionais.

Para este ambiente houve a seguinte segmentação de rede conforme abaixo:

- 192.168.28.0/24 - Gerência do Servidor;
- 192.168.20.0/30 - Gerência AP Cliente 1, onde há uma NanoStation M5 como AP para cliente;
- 192.168.21.0/29 - Gerência de equipamentos Cliente 2, existe um ponto a ponto de rádio antes do AP;
- 200.200.200.0/30 - Rede de Uplink, é considerada a rede válida entregue pelo provedor ou operadora de internet ao cliente;
- 10.10.10.0/29 e 10.10.100.0/29 - Rede de cliente 1 e cliente 2, respectivamente. Estão configuradas como DHCP na borda e entregue pelos AP's aos clientes. Somente nestas redes é possível haver comunicação com uma rede externa, ou seja, funciona como IP válido. Isto é possível devido a criação de duas rotas estáticas apontando para o IP do roteador Externo. Ou seja, os equipamentos que não pertencem a rede só vão conhecer as redes acima, simulando o ambiente de Internet.

6.2 Ferramentas

Foram instaladas as seguintes ferramentas no servidor: Zabbix 4.2.5 e FastNetMon que podem ser baixadas gratuitamente através dos links abaixo, respectivamente:

- https://www.zabbix.com/download
- https://fastnetmon.com/install/

6.2.1 Zabbix

No Zabbix foi adicionado os templates de Mikrotik, Ubiquiti, Smokeping, SNMP e Lembrete.

- Os templates de Mikrotik e Ubiquiti foram configurados para exibir o uso de CPU, memória e tráfego das interfaces no sentido de download e upload. Com estes dados foi criado um gatilho que é acionado quando há um comportamento anormal na rede, isto é, quando acontece um aumento repentino de banda, CPU e memória. Para ser considerado um incidente, foi utilizado uma média de cálculo destes valores e caso o valor das últimas 10 coletas de dados for maior do que a média é gerado uma notificação na dashboard do Zabbix avisando de um possível ataque de negação de serviço;
- O template SNMP é o básico para que o Zabbix consiga coletar e verificar os dados;
- Template Smokeping é baseado no protocolo ICMP e faz uma comunicação via ping entre o servidor e os hosts da rede. Podendo coletar os valores de latência e perda de pacotes entre os hosts. Quando há um nível de 70¨% de perdas e uma latência acima de 100ms uma trigger é acionada avisando de um possível ataque;
- Template Lembrete é um conjunto de variáveis sobre o servidor do Zabbix, onde foi usado o item de tempo do servidor para gerar um gatilho que é acionado todo dia quatro de cada mês, onde é gerado um incidente informativo lembrando ao administrador de rede que deve alterar as senhas, portas e acesso padrão dos equipamentos e desabilitar serviços inutilizados. E a cada seis meses é gerado um gatilho avisando sobre uma possível atualização de firmware. Tais lembretes ajudam a reduzir vulnerabilidades e aumentar o nível de segurança da rede para os ataques de negação de serviço e força bruta;

- Template Tentativa Log possui uma variável que busca nos logs dos equipamentos as tentativas de login, tal filtro é feito a partir de expressão regular. Caso tenha mais de 20 tentativas de acesso um gatilho é acionado gerando um incidente de possível ataque de força bruta.

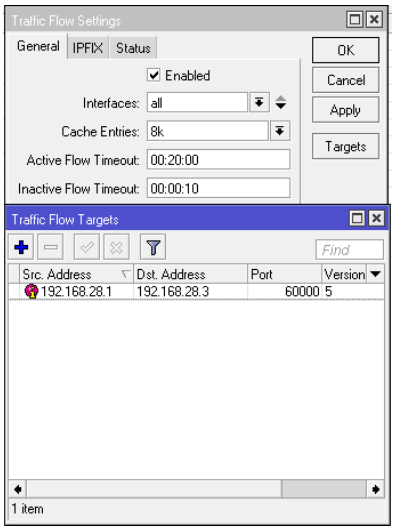
6.2.2 FastNetMon

No FastNetMon as redes 10.10.10.0/29 e 10.10.100.0/29 foram adicionadas a lista de monitoramento enquanto as outras foram adicionadas a um White List, que funciona como uma exceção, não sendo monitorados pela ferramenta. O software realiza a comunicação de dados via Flow entre o servidor e o equipamento de borda da rede. Com isso, os dados são analisados a partir de duas variáveis, pacotes por segundo e largura de banda. Caso ocorra um valor acima de 200 pps e 10 mbps nas interfaces dos endereços IP monitorados haverá um bloqueio de 100 segundos do endereço IP de destino, fazendo com que o resto da rede continue disponível. Lembrando que estes valores são para a capacidade de banda e os equipamentos utilizados no ambiente de teste.

6.3 Integração FastNetMon, Mikrotik e Zabbix

Para poder realizar a integração do Zabbix com o FastNetMon utiliza o Flow, com isso é um requisito para o funcionamento da ferramenta. Os roteadores Mikrotik possuem uma opção chamada Traffic Flow.

Figura 42- Traffic Flow Mikrotik



Fonte: Próprio autor, 2019

Com esta função habilitada o roteador Mikrotik consegue conversar com a ferramenta de mitigação. Quando um IP monitorado atinge alguma das restrições de ataque o FastNetMon o classifica como ban, quando isso acontece o servidor acessa o roteador via ssh e adiciona uma rota estática apontando o endereço para null, fazendo com que a conexão seja encerrada. Após os 100 segundos configurados o IP é classificado como unban e a rota é removida.

No processo de envio da rota para o Mikrotik, um pacote do zabbix chamado zabbix sender, é utilizado para passar duas variáveis ao zabbix, o contador de ataques e o IP que está sendo afetado, conforme o script abaixo (Figura 43).

Figura 43- Script FastNetMon - Mikrotik e FastNetMon-Zabbix

```
#!/bin/bash

#  $1 client_ip_as_string
#  $2 data_direction
#  $3 pps_as_string
#  $4 action (ban or unban)
if [ "$4" = "ban" ]; then
        #cat | mail -s "FastNetMon Guard: IP $1 blocked because $2 attack with power $3 pps";
        #ban
        cat | echo "$1" >> /var/log/ataques
        zabbix_sender -z 192.168.28.3 -s "Zabbix server" -k attack_counter -o $(wc -l </var/log/ataq
ues)
        zabbix_sender -z 192.168.28.3 -s "Zabbix server" -k attack_ip -o $1
        zabbix_sender -z 192.168.28.3 -s "Zabbix server" -k stat -o $4
        ssh vinicius@192.168.28.1 -p33 "ip route add type=blackhole dst-address=$1/32];quit"
        exit 0
fi

if [ "$4" = "unban" ]; then
        #unban
        sed -i "/^$1$/d" /var/log/ataques
        zabbix_sender -z 192.168.28.3 -s "Zabbix server" -k attack_counter -o $(wc -l </var/log/ataq
ues)
        zabbix_sender -z 192.168.28.3 -s "Zabbix server" -k stat -o $4
        # Unban actions if used
        ssh vinicius@192.168.28.1 -p33 "ip route remove [find type=blackhole dst-address=$1/32];quit
"
        exit 0
fi
~
~
```

Fonte: Próprio autor, 2019

6.4 Testes

Os testes serão feitos utilizando uma Mikrotik 750g externa a rede, utilizando o IP 200.200.200.1. Este roteador possui conectividade com a borda e com os clientes finais. A comunicação com os clientes finais é devido a uma rota estática na borda da rede que aponta os blocos para o IP 200.200.200.1, simulando uma rede válida.

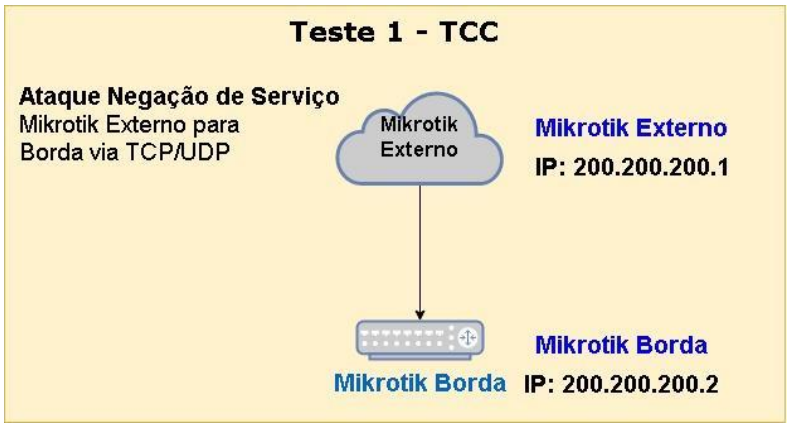
Os testes serão realizados com o bandwidth teste, uma ferramenta dos roteadores Mikrotik, na qual é possível realizar testes de banda TCP e UDP, variando o tamanho dos pacotes UDP e quantidade de conexões TCP.

Diante de todas essas características serão executados quatro testes de validação do funcionamento das ferramentas do servidor em mitigar e notificar possíveis ataques de negação de serviço e força bruta.

- Primeiro Teste é de uma rede externa até a borda, mostrando que se a borda sofrer um ataque, ele não é mitigado pelo FastNetMon, mas é notificado pelo Zabbix, sendo assim o administrador de rede tem que resolver a situação;
- Segundo Teste é de uma rede externa até o cliente final via protocolos TCP e UDP;
- Terceiro Teste é do cliente final até a rede externa via protocolos TCP e UDP;
- Quarto Teste é colocar o valor do gatilho de lembrete de acordo com a data.

O primeiro teste tem como objetivo mostrar que a borda da rede não pode ser mitigada e que deve ser notificado o mais rápido possível para que o administrador tome alguma decisão. É possível observar na figura 44 o que ocorre no teste 1.

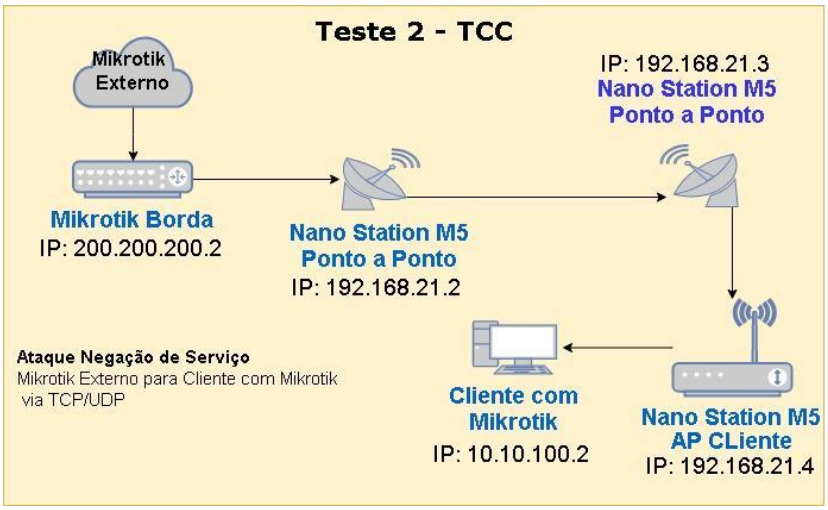
Figura 44 - Teste 1



Fonte: Próprio autor, 2019

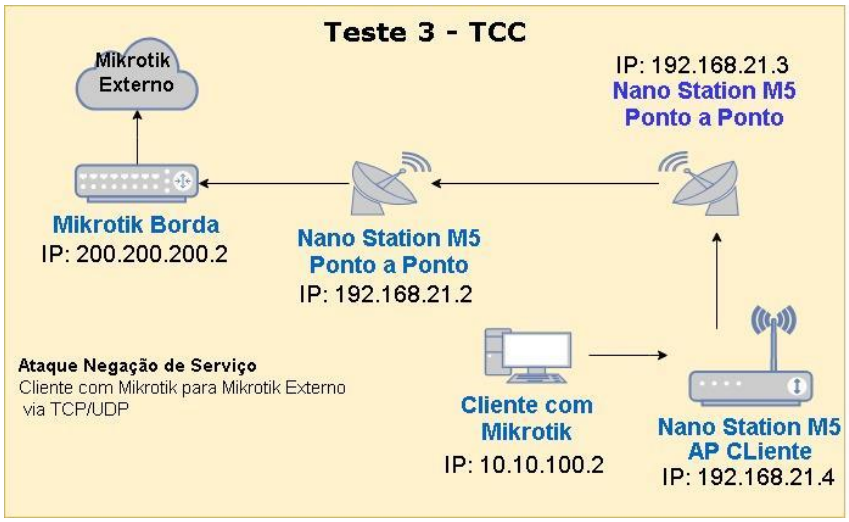
Do segundo ao terceiro teste, o objetivo é notificar e mitigar um possível ataque de negação de serviço com características de pacotes por segundo e largura de banda nos sentidos de download e upload (Tx/Rx). Para ilustrar o segundo e o terceiro teste tem-se, respectivamente, as figuras 45 e 46.

Figura 45 - Teste 2



Fonte: Próprio autor, 2019

Figura 46 - Teste 3



Fonte: Próprio autor, 2019

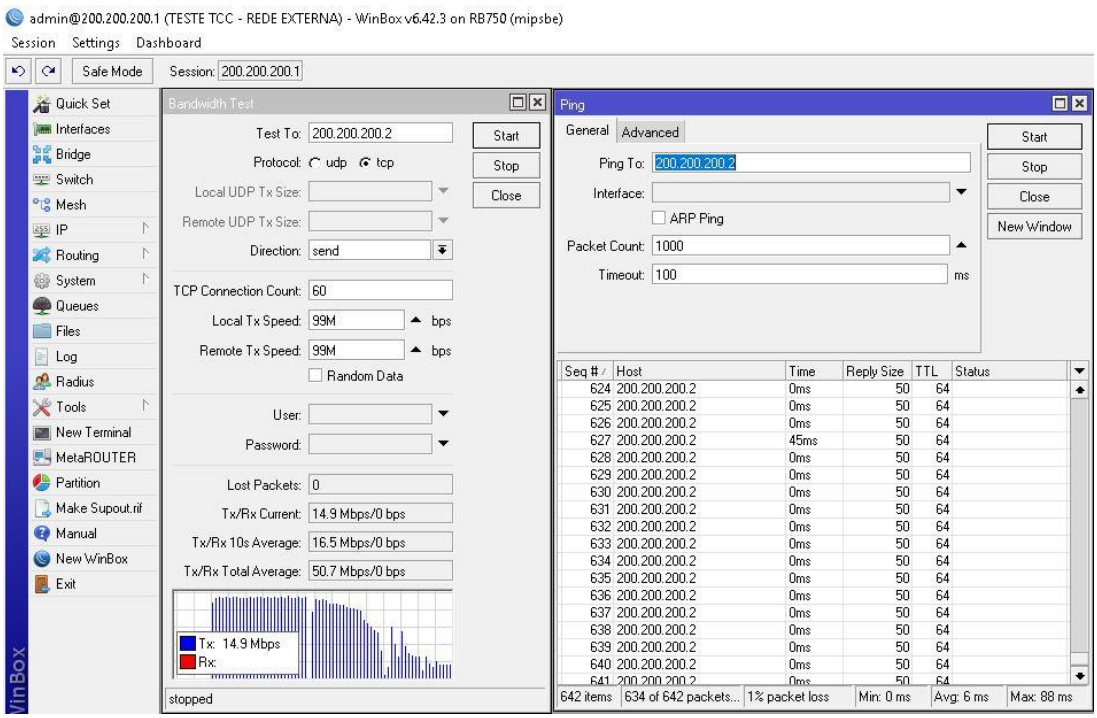
O quarto teste vem ajudar a notificar possíveis vulnerabilidades na rede. Ajudando a incrementar o nível de segurança.

6.5 Análise de Dados

Nos testes realizados foram identificados ataques de negação de serviço dos tipos UDP Flood e TCP Syn. Segue os resultados dos testes.

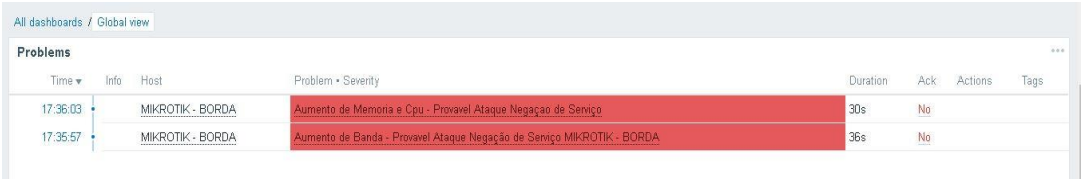
- Teste 1 Protocolo TCP

Figura 47 -Tipo do teste, consumo e latência durante o teste TCP Rede Externa para Borda



Fonte: Próprio autor, 2019

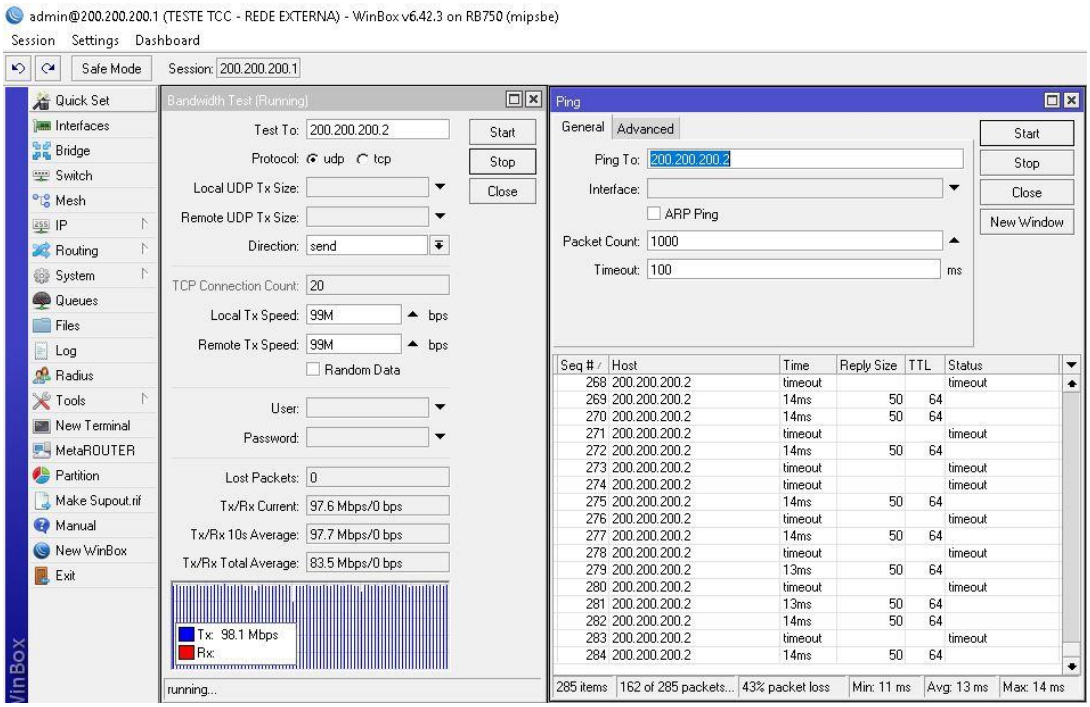
Figura 48 - Incidentes Zabbix durante teste TCP da Rede Externa para Borda



Fonte: Próprio autor, 2019

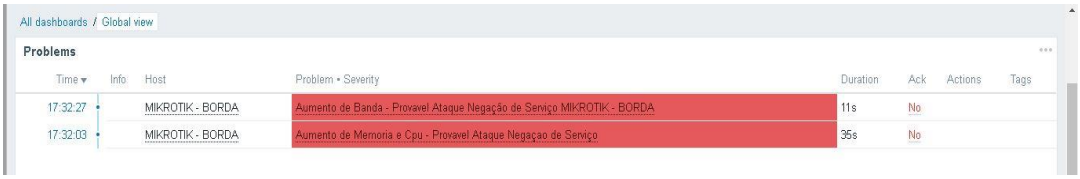
- Teste 1 Protocolo UDP

Figura 49- Tipo do teste, consumo e latência durante o teste UDP Rede Externa para Borda



Fonte: Próprio autor, 2019

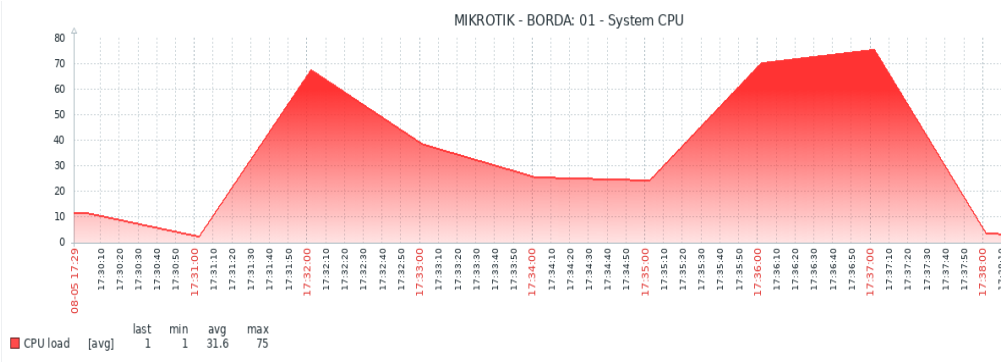
Figura 50- Incidentes Zabbix durante teste UDP da Rede Externa para Cliente



Fonte: Próprio autor, 2019

No teste 1 não é possível mensurar o tempo, pois é necessário a participação do administrador para resolver a situação. Mas foi possível observar que a CPU no horário dos testes chegou à 75% devido ao consumo total de recursos, já que os testes feitos foram baseados na capacidade total da interface física que é 100M.

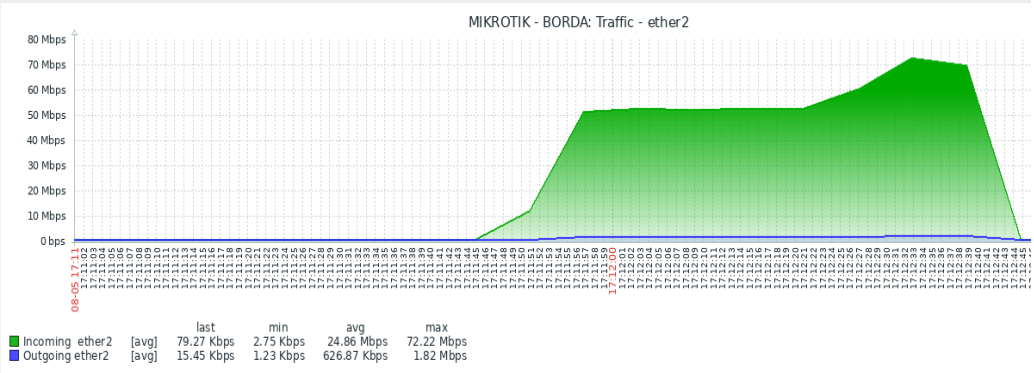
Figura 51 - Consumo Mikrotik Borda durante teste da Rede Externa para Borda



Fonte: Próprio autor, 2019

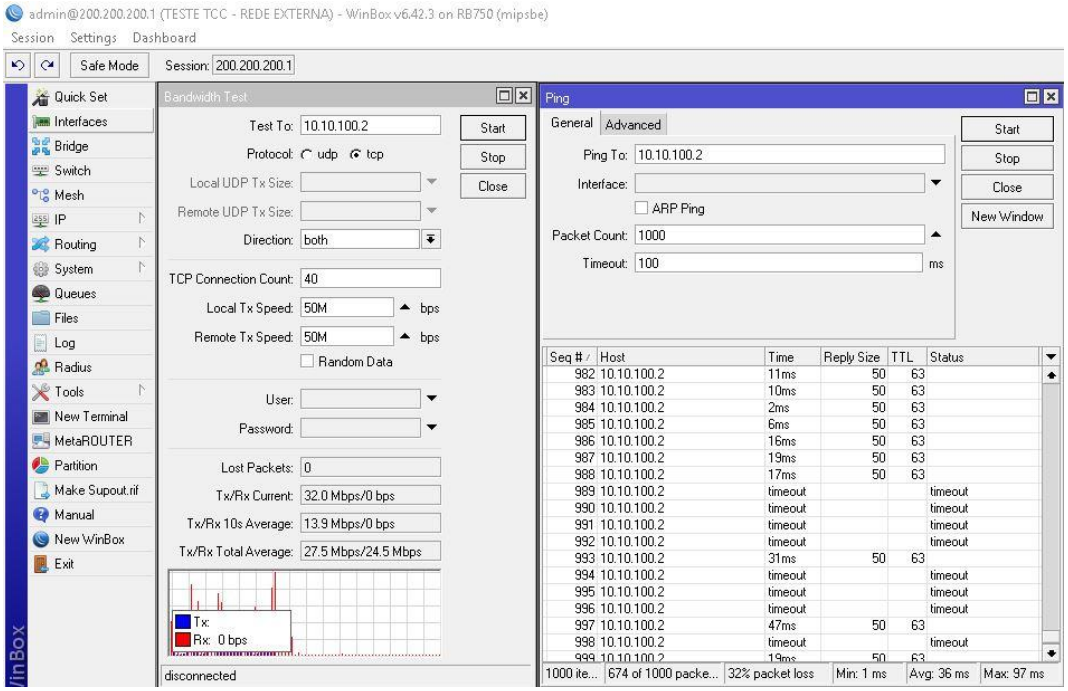
- Teste 2 Protocolo TCP

Figura 52- Consumo de banda na interface de Uplink do Mikrotik de Borda



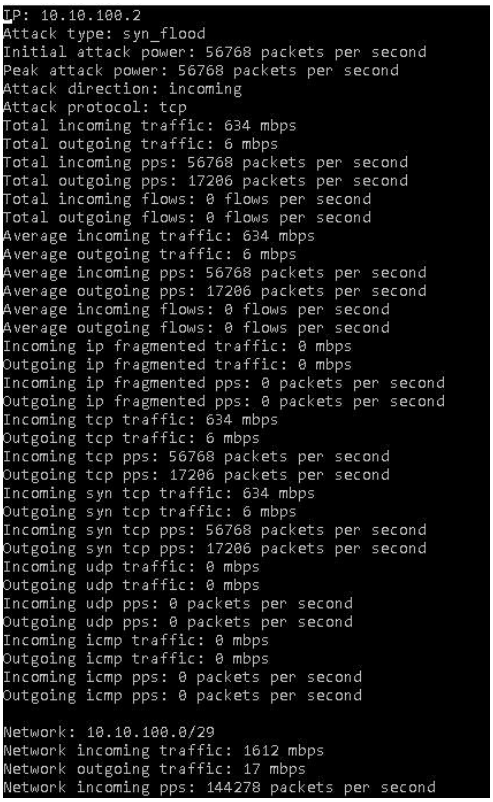
Fonte: Próprio autor, 2019

Figura 53- Tipo do teste, consumo e latência durante o teste TCP da Borda para o Cliente



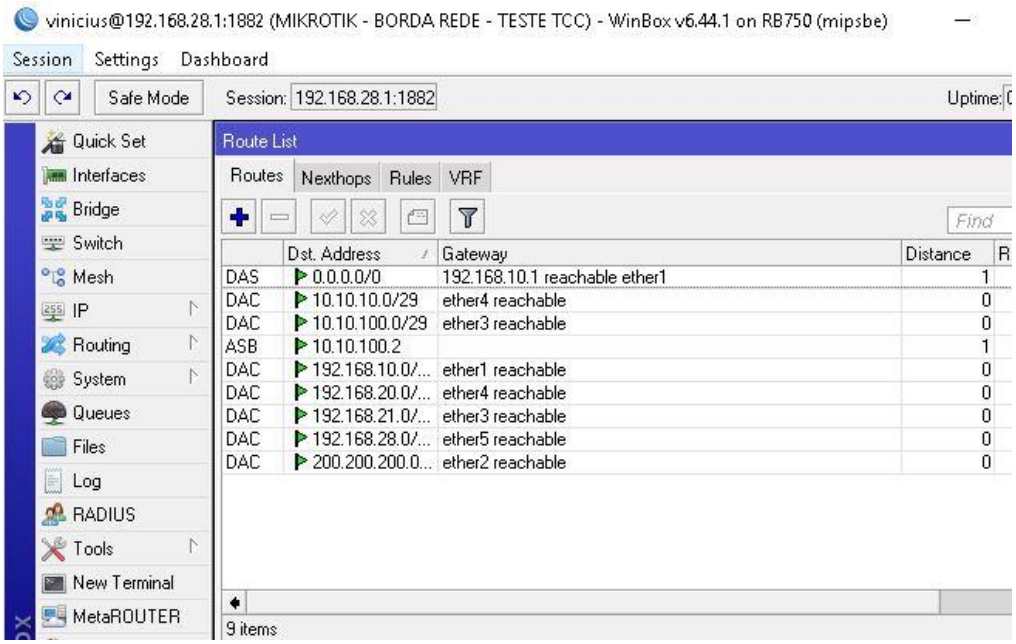
Fonte: Próprio autor, 2019

Figura 54- Log FastNetMon do ataque TCP da Rede Externa para O Cliente



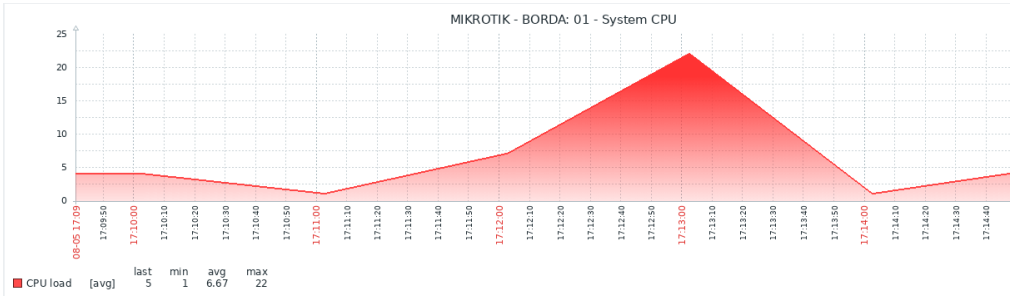
Fonte: Próprio autor, 2019

Figura 55 - Rota Estática Bloqueando o IP



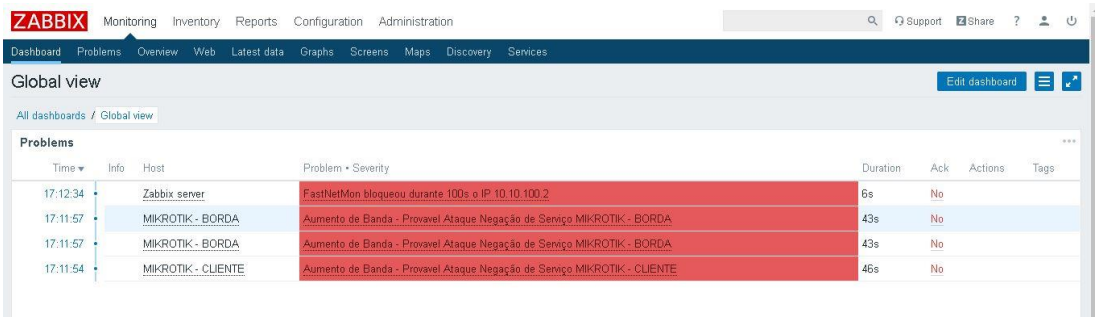
Fonte: Próprio autor, 2019

Figura 56 - CPU Mikrotik Borda durante o teste TCP da Rede Externa para Cliente



Fonte: Próprio autor, 2019

Figura 57 - Incidentes Zabbix durante teste TCP da Rede Externa para Cliente

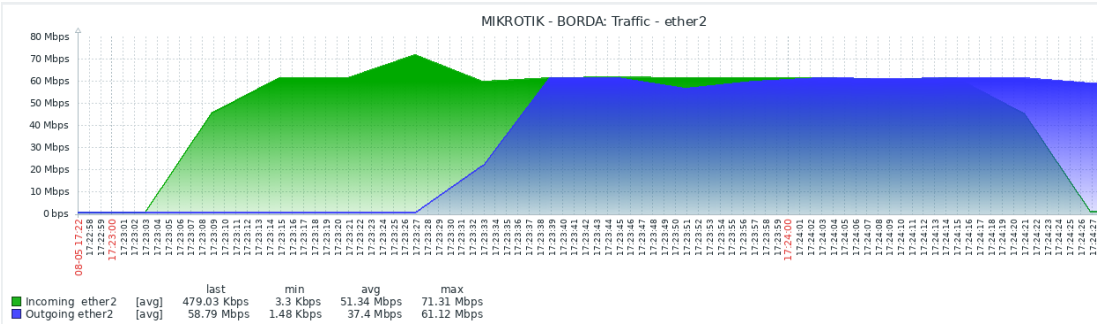


Fonte: Próprio autor, 2019

Percebe-se através dos gráficos que a CPU durante este teste chegou a 22% e foram gastos desde o início até a mitigação do ataque 60s.

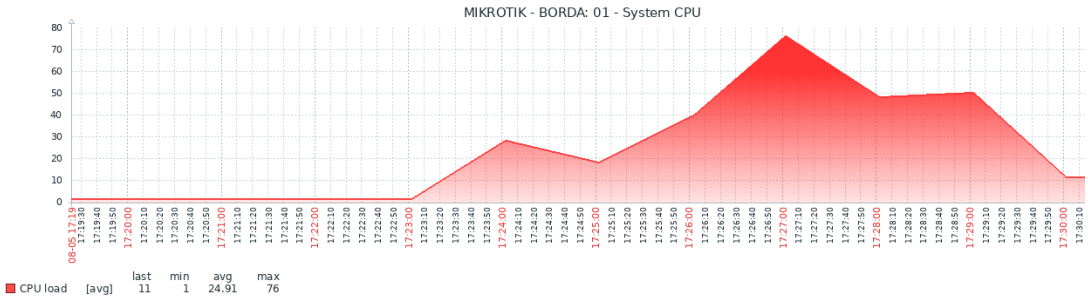
- Teste 2 Protocolo UDP

Figura 58 - Consumo de banda na interface de Uplink do Mikrotik de Borda



Fonte: Próprio autor, 2019

Figura 59 - CPU Mikrotik Borda durante o teste UDP da Rede Externa para Cliente



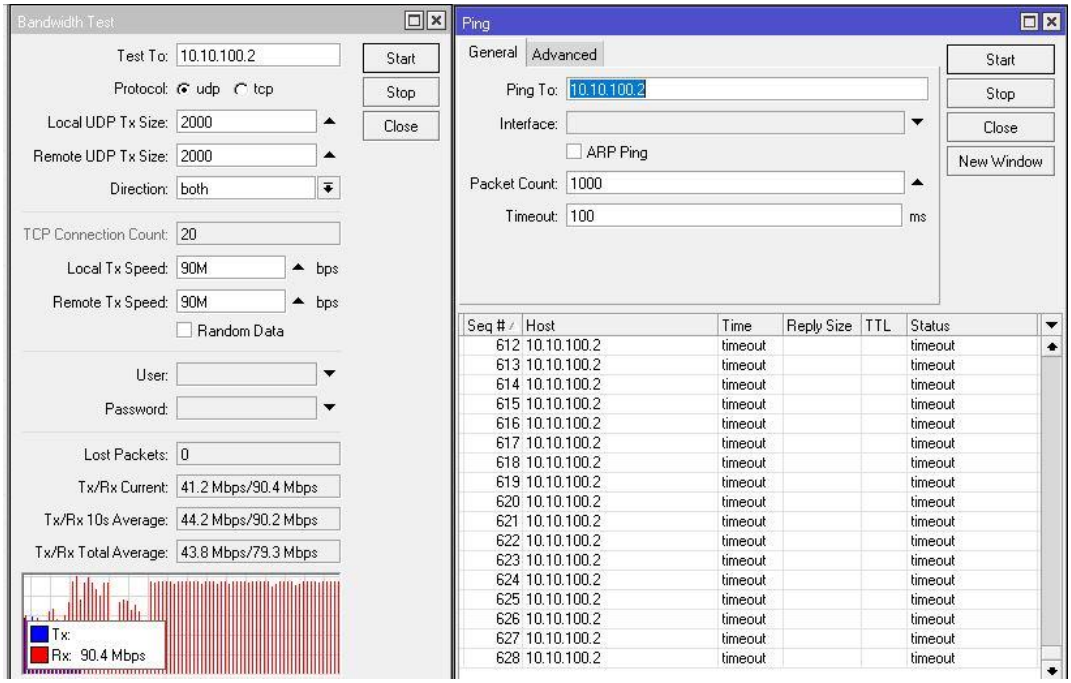
Fonte: Próprio autor, 2019

Figura 60 - Log FastNetMon do ataque UDP da Rede Externa para o Cliente

```
IP: 10.10.100.2
Attack type: udp_flood
Initial attack power: 430061 packets per second
Peak attack power: 430061 packets per second
Attack direction: outgoing
Attack protocol: udp
Total incoming traffic: 5 mbps
Total outgoing traffic: 6561 mbps
Total incoming pps: 1331 packets per second
Total outgoing pps: 430061 packets per second
Total incoming flows: 0 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 5 mbps
Average outgoing traffic: 6561 mbps
Average incoming pps: 1331 packets per second
Average outgoing pps: 430061 packets per second
Average incoming flows: 0 flows per second
Average outgoing flows: 0 flows per second
Incoming ip fragmented traffic: 0 mbps
Outgoing ip fragmented traffic: 0 mbps
Incoming ip fragmented pps: 0 packets per second
Outgoing ip fragmented pps: 0 packets per second
Incoming tcp traffic: 0 mbps
Outgoing tcp traffic: 0 mbps
Incoming tcp pps: 0 packets per second
Outgoing tcp pps: 0 packets per second
Incoming syn tcp traffic: 0 mbps
Outgoing syn tcp traffic: 0 mbps
Incoming syn tcp pps: 0 packets per second
Outgoing syn tcp pps: 0 packets per second
Incoming udp traffic: 5 mbps
Outgoing udp traffic: 6561 mbps
Incoming udp pps: 1331 packets per second
Outgoing udp pps: 430061 packets per second
Incoming icmp traffic: 0 mbps
Outgoing icmp traffic: 0 mbps
Incoming icmp pps: 0 packets per second
Outgoing icmp pps: 0 packets per second
```

Fonte: Próprio autor, 2019

Figura 61 - Tipo do teste, consumo e latência durante o teste UDP da Borda para o Cliente

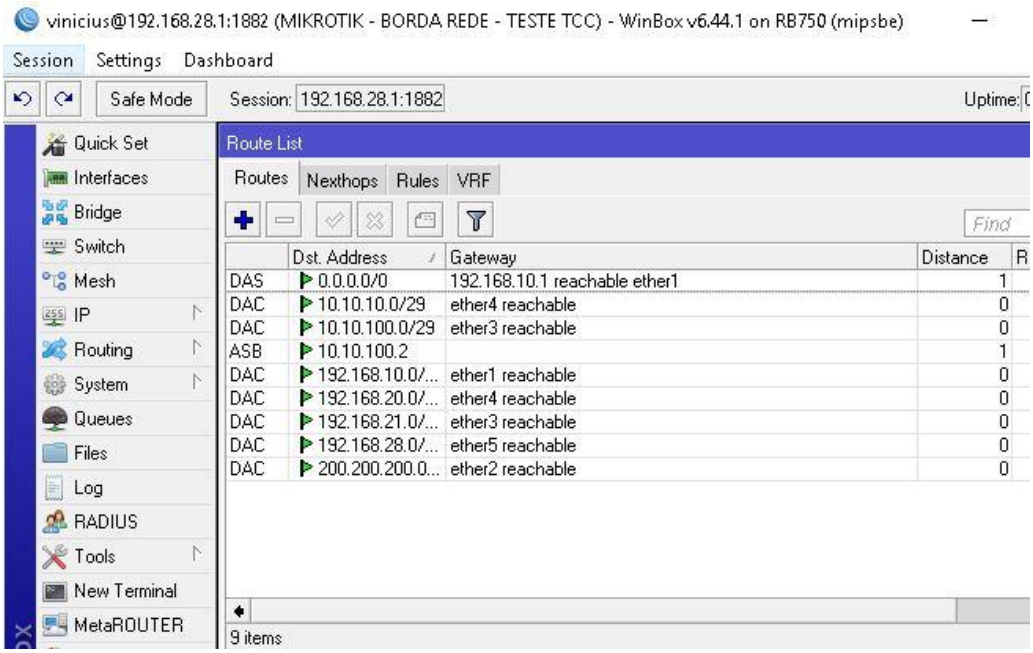


Fonte: Próprio autor, 2019

Figura 62- Incidentes Zabbix durante teste UDP da Rede Externa para Cliente

Fonte: Próprio autor, 2019

Figura 63 - Rota Estática Bloqueando o IP

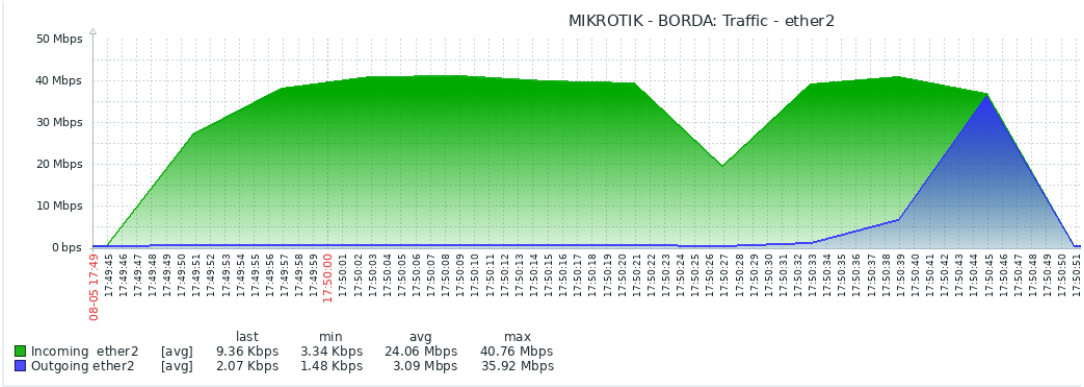


Fonte: Próprio autor, 2019

Para este foram gastos 84s desde o início até a mitigação do ataque, a CPU chegou a um pico de 76%. Houve uma situação durante este teste pois estava sendo realizado um teste em outro equipamento no sentido contrário, o que provavelmente ocasionou o pico de CPU. Mas conforme o log do FastNetMon ocorreu um ataque de UDP Flood neste momento.

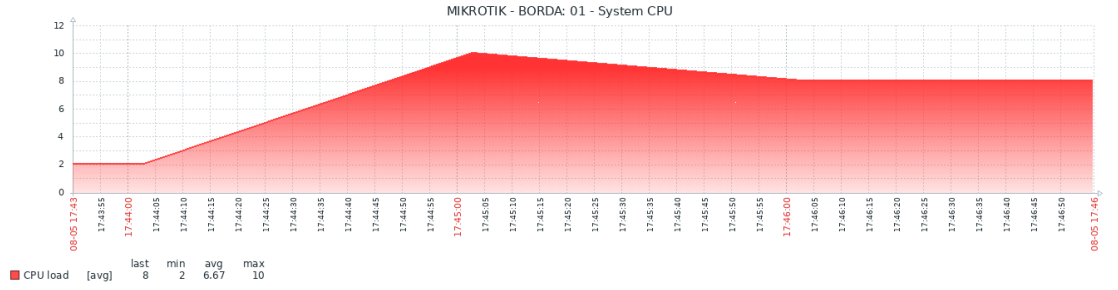
- Teste 3 Protocolo TCP

Figura 64 - Consumo de banda na interface de Uplink do Mikrotik de Borda



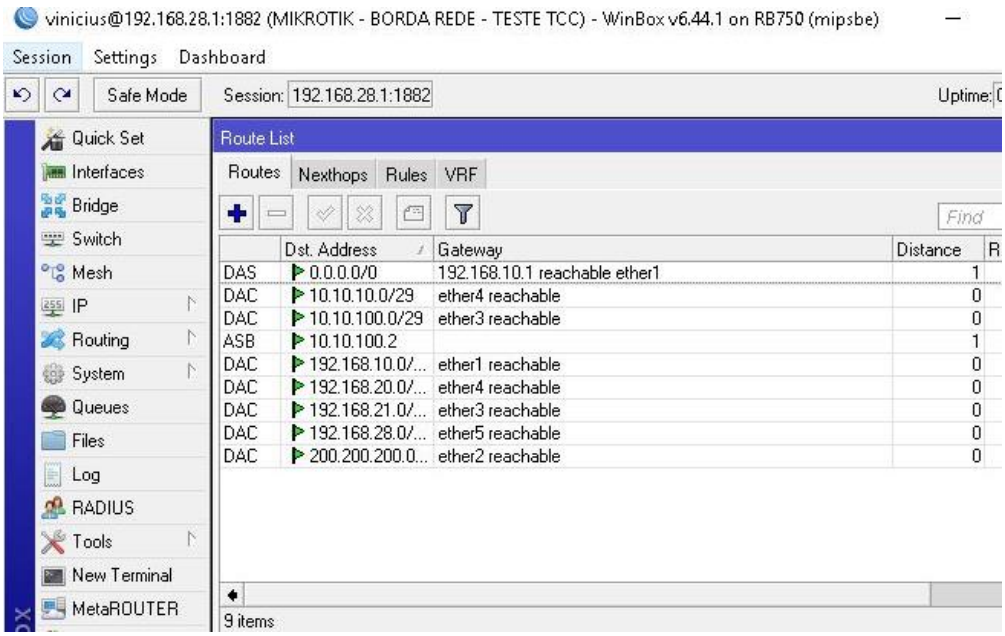
Fonte: Próprio autor, 2019

Figura 65 - CPU Mikrotik Borda durante o teste TCP do Cliente para Rede Externa



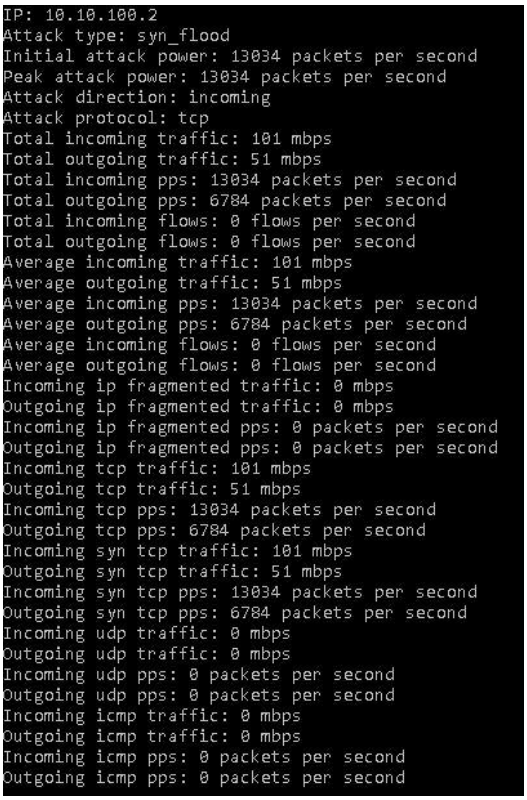
Fonte: Próprio autor, 2019

Figura 66 - Rota Estática Bloqueando o IP



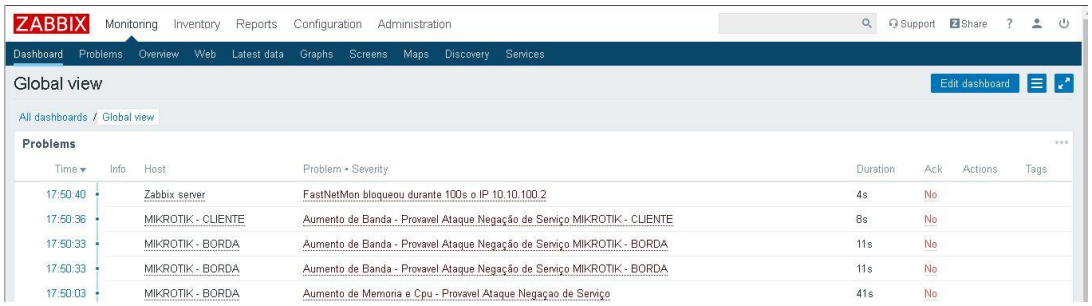
Fonte: Próprio autor, 2019

Figura 67- Log FastNetMon do ataque TCP do Cliente para Rede Externa



Fonte: Próprio autor, 2019

Figura 68 - Incidentes Zabbix durante teste TCP do Cliente para Rede Externa



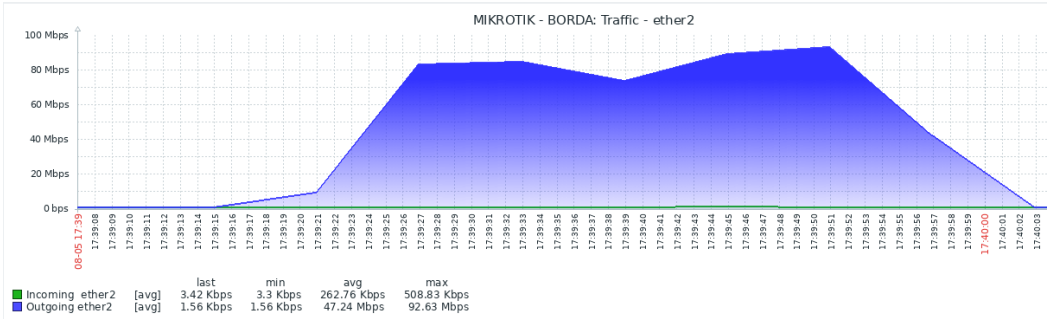
Fonte: Próprio autor, 2019

Neste teste foram gastos 66s do começo do ataque até a mitigação. A CPU chegou a 10% e uma situação é no sentido de saído teste a banda demorou para

subir, podendo ser devido a quantidade alta de processamento do equipamento Mikrotik no cliente final.

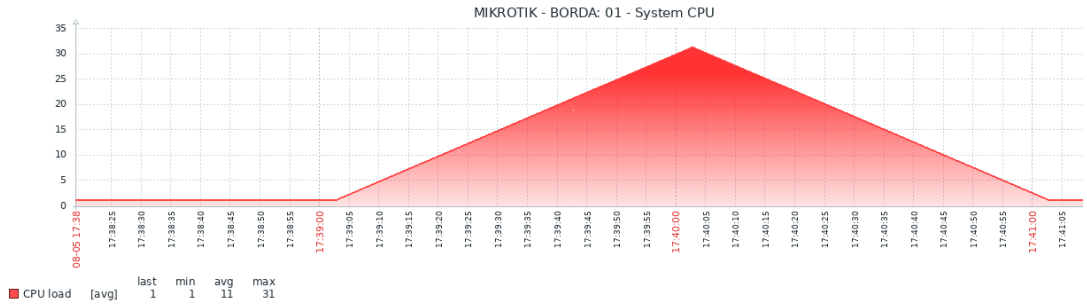
- Teste 3 Protocolo UDP

Figura 69 - Consumo de banda na interface de Uplink do Mikrotik de Borda



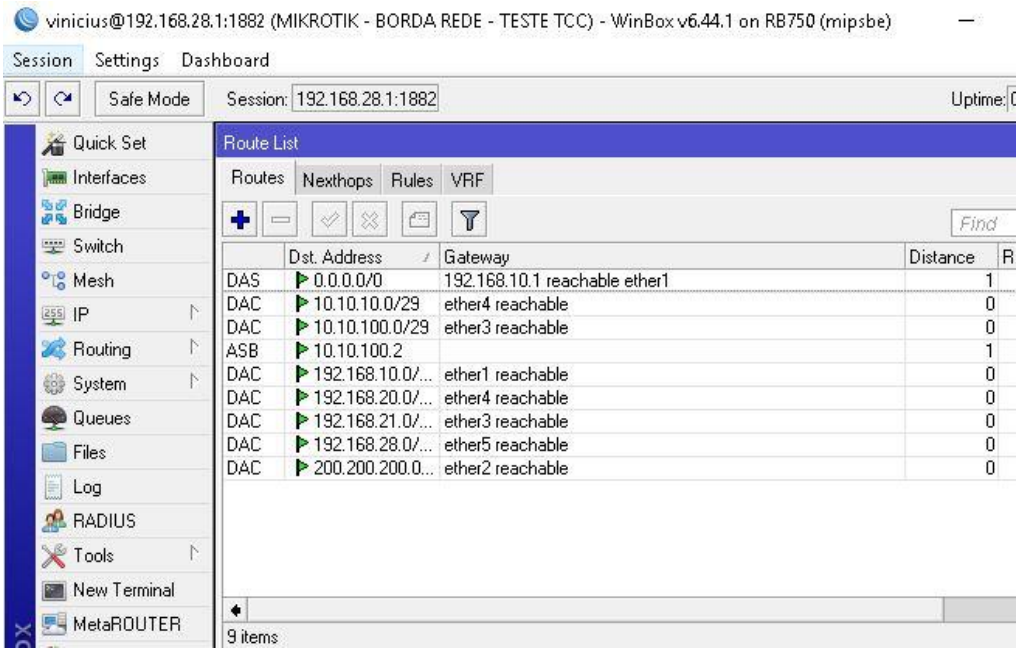
Fonte: Próprio autor, 2019

Figura 70 - CPU Mikrotik Borda durante o teste UDP do Cliente para Rede Externa



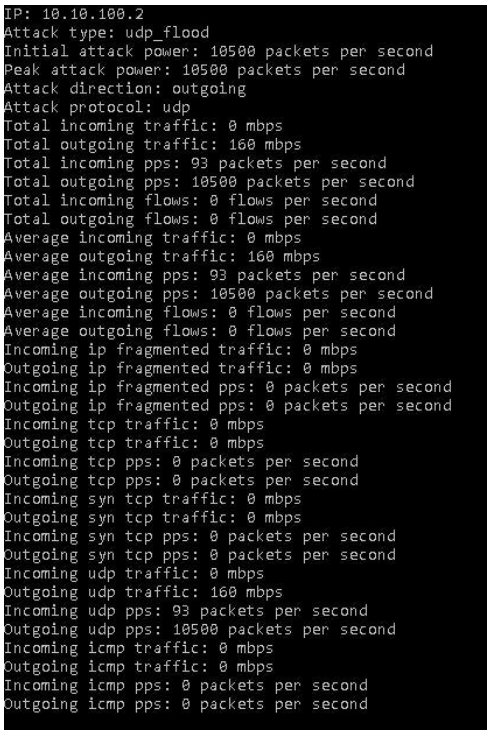
Fonte: Próprio autor, 2019

Figura 71 - Rota Estática Bloqueando o IP



Fonte: Próprio autor, 2019

Figura 72 - Log FastNetMon do ataque UDP do Cliente para Rede Externa



Fonte: Próprio autor, 2019

Figura 73 - Incidentes Zabbix durante teste UDP do Cliente para Rede Externa

Fonte: Próprio autor, 2019

Durante a execução do teste a CPU chegou a um pico de 31% e demorou 60s desde começo até o final do teste. No caso do teste três, do cliente para rede externa, não foi possível coletar a figura com o tipo de teste por que a conexão com o equipamento caia, devido a mitigação do ataque pelo FastNetMon, mas pelo log do ataque é possível identificar.

- Teste 4

Figura 74- Função Lembrete de Vulnerabilidades

Time		Severity	Recovery time	Status	Info	Host	Problem
2019-08-03 14:27:00		Information	2019-08-03 21:00:14	RESOLVED		Zabbix server	Lembrete: Desativar serviços desnecessários, Atualizar Firmware dos Equipamentos Atualizados, Alterar Porta Padrões

Fonte: Próprio autor, 2019

No dia 03/08/2019 a trigger foi ativa exibindo a mensagem de Lembrete: “Desativar serviços desnecessários, Atualizar Firmware dos Equipamentos Atualizados, Alterar Porta Padrão”.

7. RESULTADOS

Percebe-se que todos testes foram validados para os ataques de negação de serviço do tipo UDP Flood e Syn Flood, onde o tempo médio gasto para o zabbix identificar e o fastnetmon mitigar foi de 72 segundos para os ataques de UDP Flood e de 63 segundos para os ataques de TCP Syn Flood, conforme a média de valores dos incidentes do zabbix nos testes, com os parâmetros configurados no teste. Para um ataque de negação de serviços, o tempo de notificação e mitigação são considerados bons já que com este tempo os serviços e clientes ficam pouco tempo indisponíveis, chegando a ser imperceptível.

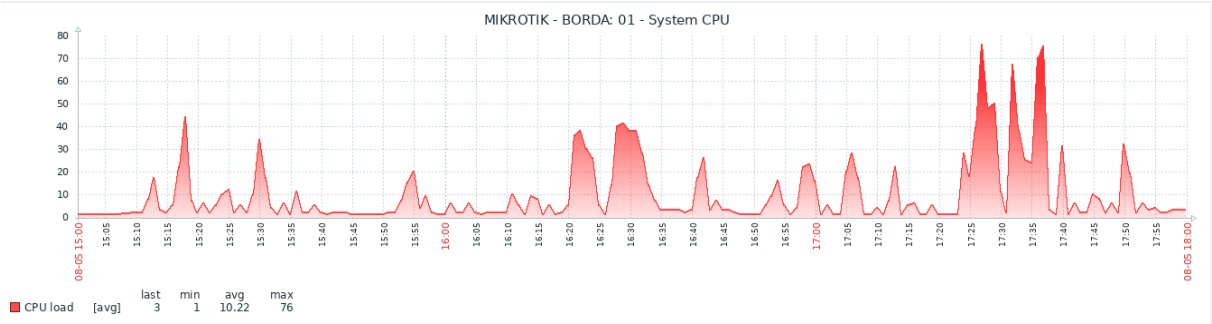
Tabela 1- Tempo de Notificação e Mitigação dos Ataques nos testes

Teste/Ataque	UDP Flood	TCP SYN Flood
TESTE 1	Indisponível	Indisponível
TESTE 2	84s	60s
TESTE 3	60s	66s

Fonte: Próprio autor, 2019

Nota-se que durante os testes via UDP, o processamento dos roteadores são maiores que os do TCP sendo causado devido à dificuldade do equipamento em suportar vários pacotes mais simples que ocupavam toda a largura de banda. Enquanto o protocolo TCP somente envia as requisições SYN, utilizando pouco volume de banda. No gráfico (Figura 75) abaixo podemos ver o processamento durante o período do teste TCP e UDP do teste.

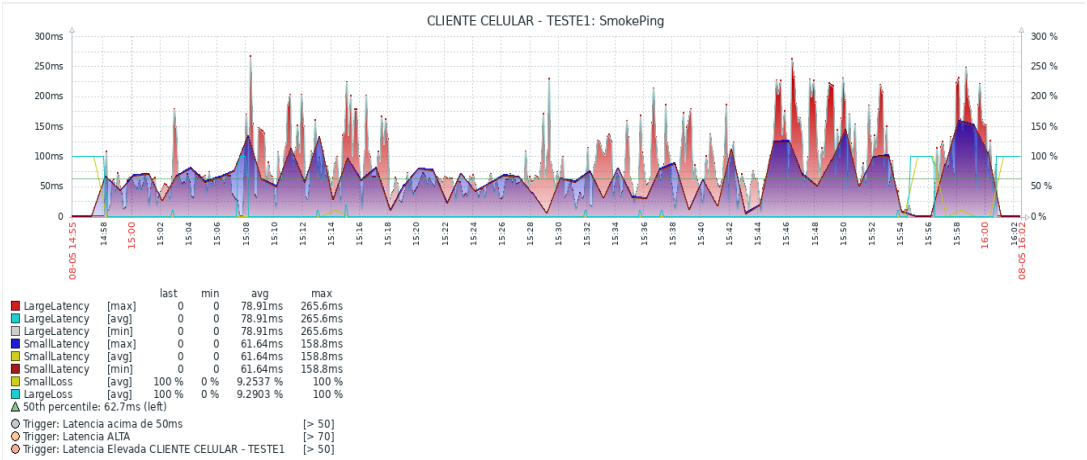
Figura 75- CPU do Mikrotik de Borda durante o intervalo total dos testes



Fonte: Próprio autor, 2019

Durante os testes também foi analisado o cliente 1 que em nenhum dos testes foi alvo dos ataques, sofreu com pequenas intermitências e picos de latência durante os ataques TCP, que elevavam a CPU do roteador, causando assim perda de pacote e latência alta, conforme a imagem abaixo (Figura 76).

Figura 76- Smokeping Cliente 1 durante o período de testes

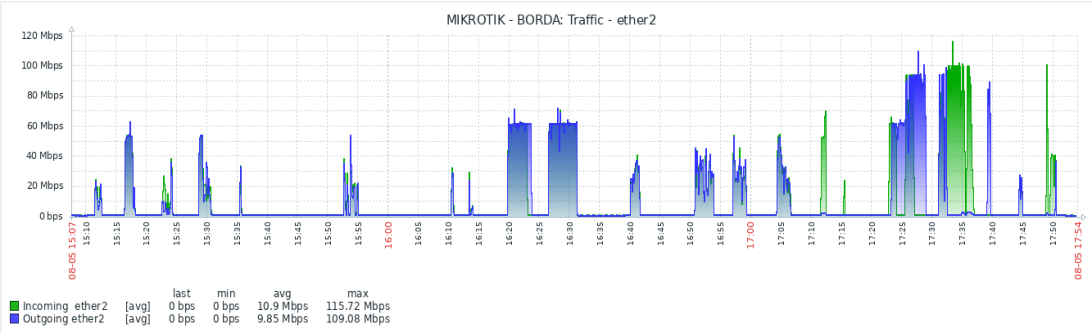


Fonte: Próprio autor, 2019

Nota-se também que a utilização de banda durante os testes UDP são mais constantes, por serem pacotes mais simples e consumirem menos memória, enquanto durante os testes TCP, com 40 conexões, a banda varia devido ao processamento da

rb e capacidade dos rádios Ubiquiti Nano Station M5, conforme a figura abaixo (Figura 77).

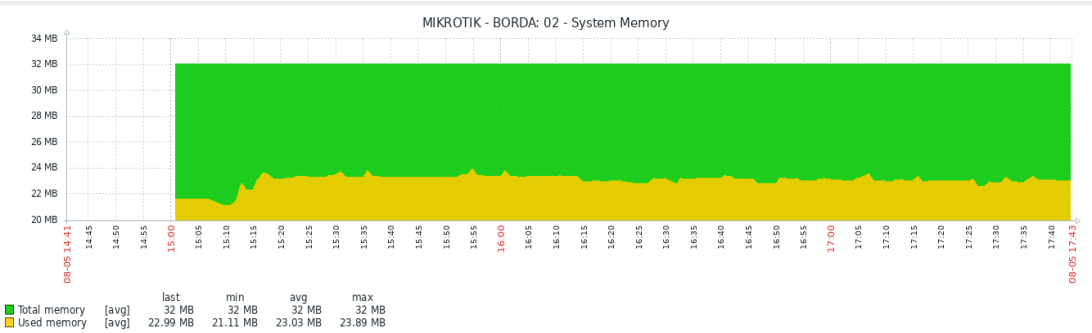
Figura 77- Consumo da Interface de UPLINK durante o período de testes



Fonte: Próprio autor, 2019

A memória do Mikrotik não sofreu grandes alterações, devido a limitação de equipamentos no ambiente de testes, e devido a memória ser mais usada para armazenamento de logs e arquivos.

Figura 78- Memória do Mikrotik de Borda durante o período de testes

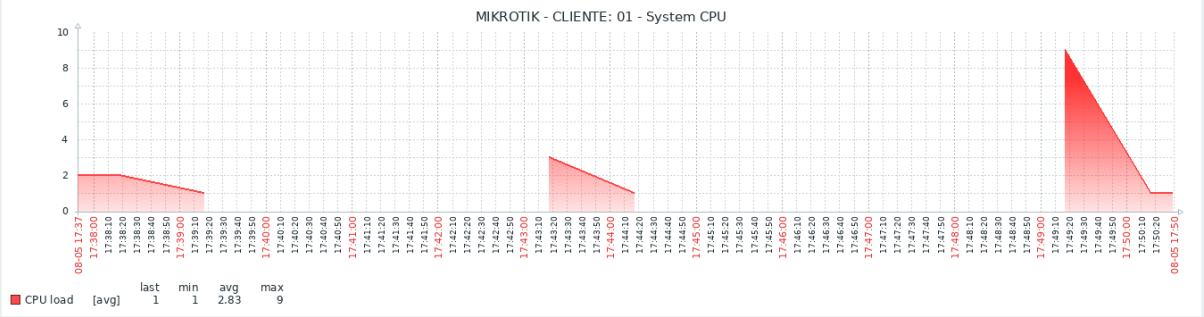


Fonte: Próprio autor, 2019

Ao analisar os gráficos do Mikrotik final devido a falha de coleta não foi possível utilizá-los já que os enlaces estavam sendo saturados devido ao ataque, sendo assim a comunicação do zabbix do cliente foi interrompida. Percebe-se nas figuras abaixo

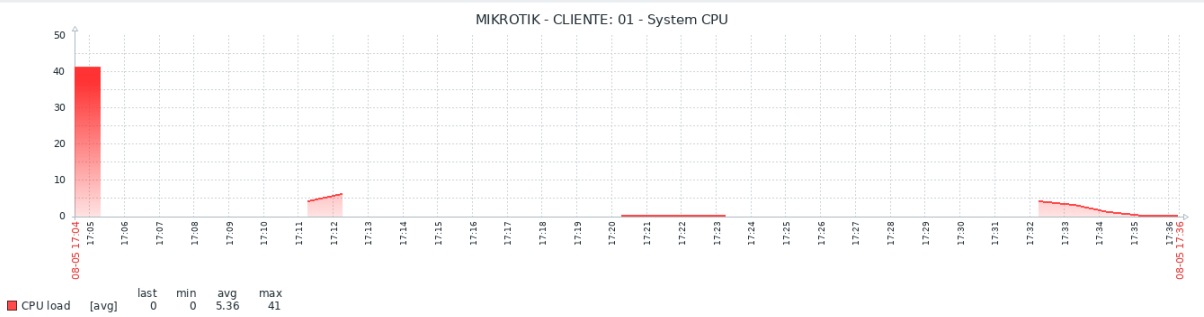
que, ao executar o ataque a comunicação foi interrompida devido à falta de recursos dos equipamentos usados na comunicação do cliente.

Figura 79 - CPU do Mikrotik Cliente durante os ataques do Cliente para Rede Externa



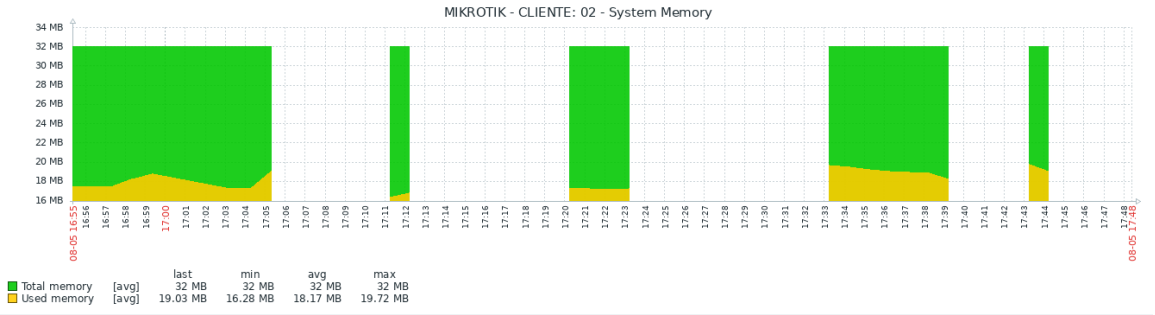
Fonte: Próprio autor, 2019

Figura 80 - CPU do Mikrotik Cliente durante os ataques da Rede Externa para o Cliente



Fonte: Próprio autor, 2019

Figura 81 - Memoria do Mikrotik Cliente durante todo o período de testes



Fonte: Próprio autor, 2019

8. CONSIDERAÇÕES FINAIS

De acordo com a Untangle(2018), boa parte das pequenas e médias empresas não tem condições financeiras de manter a segurança da informação devido ao custo elevado de ferramentas, serviços e profissionais. Diante disso, conclui-se a necessidade de desenvolver um procedimento operacional que com o auxílio de ferramentas gratuitas auxiliam os administradores de rede desses tipos de organizações a notificarem e mitigarem ataques de negação de serviço. Com tais ferramentas é a empresa tem mais orçamento para investir no hardware da rede.

Devido aos equipamentos terem suporte a aplicações de NetFlow, suporte SNMP e acesso via ssh, identificou-se a necessidade de investir um pouco mais em roteadores e rádios que tenham a capacidade de reconhecerem as principais aplicações disponíveis no mercado, já que são necessários para a comunicação de informações e de trafego entre o servidor de monitoramento e os equipamentos de rede.

Em vista dos resultados apresentados nos testes do procedimento operacional, percebe-se que utilizando o sistema de monitoramento Zabbix e a ferramenta de análise de trafego FastNetMon foi possível notificar e mitigar ataques de negação de serviço em redes sem fio, com um tempo de resposta médio de 62 segundos para o UDP Flood e 73 segundos para o TCP Syn Flood.

Analisando a configuração dos gatilhos do Zabbix e dos parâmetros do FastNetMon, conclui-se que para os ataques de negação de serviço do tipo UDP Flood e TCP Syn Flood as variáveis que sofrem mais variações são o aumento da largura de banda, uso da cpu e perda de pacote.

Os testes também mostraram que as redes sem fio têm suas limitações, sendo necessário a utilização de ferramentas externas para auxiliar os administradores de rede. Neste caso poderia ter sido utilizado uma análise do comportamento da rede para gerar testes mais precisos e otimizar as configuração das ferramentas para evitar que aconteça os falsos positivos, pois nem sempre uma latência alta ou perda de

pacote elevada resultam em um ataque de negação de serviço, pode ser o cliente distante do equipamento wireless, ou então uma degradação de sinal do enlace utilizado para atender um access point.

Mas mesmo com todas as limitações, o objetivo do trabalho foi alcançado, onde os testes foram notificados e mitigados utilizando o procedimento operacional em conjunto com as ferramentas gratuitas em ambientes de redes sem fio contra ataques de negação de serviço.

8.1 Propostas de trabalhos futuros

Este trabalho abre porta para diversas outras situações, já que o Zabbix é uma ferramenta com muitos recursos que podem auxiliar em outros trabalhos como:

- Testar com redes cabeadas;
- Testar com equipamentos mais robustos;
- Testar com outras ferramentas como T50, ferramenta brasileira que realiza ataques;
- Fazer em um ambiente mais realístico com mais hosts e se possível sem utilizar hosts virtualizados;
- Fazer comunicação das ferramentas como slack, telegram e whatsapp. Sendo assim as notificações chegariam mais rápido ao administrador de rede;
- Testar para ataques de força bruta e quebra de criptografia, já que o zabbix consegue ler os arquivos de log e através rsyslog seria possível fazer uma análise dos logs dos equipamentos para gerar incidentes de tentativa de log;
- Testar para as vulnerabilidades de rede, tentar usar o zabbix para notificar equipamentos que estão com configuração padrão na rede e atualização de firmwares.

REFERÊNCIAS BIBLIOGRÁFICAS

Benício, Washington Ernando Pereira. **Monitoramento e Gerenciamento de Redes Utilizando Zabbix**. 2015. 71 f. Monografia (Tecnólogo) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, São Paulo. Disponível em: <http://zabbixbrasil.org/files/Monitoramento_e_Gerenciamento_de_Redes_Utilizando_Zabbix.pdf>. Acesso em: 05 ago. 2019.

Bueno, Edimilson Moreira. **Monitoramento de Redes de Computadores com Uso de Ferramentas de Software Livre**. 2012. 72 f. Monografia - Universidade Tecnológica Federal do Paraná, Curitiba. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1842/1/CT_CESOL_I_2012_05.pdf>. Acesso em: 05 ago. 2019.

CRUZ, Gleyson Luiz S. **Sistema de Detecção de Intrusão Utilizando Open BSD e SNORT: Mitigando Ataques de Negação de Serviço**. 2013 Monografia (Pós-Graduação) – Centro Universitário de Brasília, Brasília. Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/235/8147/1/51106308.pdf>. Acesso em: 06 ago. 2019.

Pinheiro, Marco Antônio Marques. **Viabilidade de Ataque de Negação de Serviço explorando Perfect Forward Secrecy no SSL/TLS.** 2014. 32 f. Monografia (Graduação) - Universidade de Brasília, Brasília. Disponível em: <http://www.bdm.unb.br/bitstream/10483/11151/1/2014_MarcoAntonioMarquesPinheiro.pdf>. Acesso em: 04 ago. 2019.

Cruz, L. G. A., Ramos, P. D. O., Vasconcelos, S. N. D. & Torres, C. T. 2013. **Estudo de caso de Ataques de Negação de Serviço (DDoS)**. Faculdade de Tecnologia de Bauru, São Paulo. Disponível em: <http://www.fatecbauru.edu.br/ojs/index.php/CET/article/view/197/164>. Acesso em: 05 ago. 2019.

Vilela, D. W. F. L., Shinoda, A. A., Oliveira, E. T. F., Oliveira, R., Nascimento, V. & Araújo, N. **Construção de Bases de Dados para Auxiliar a Avaliação de Sistemas de Detecção de Intrusos em uma Rede IEEE 802.11 com Criptografia WEP, WPA e WPA2 Habilitada**. 2013. 10º Encontro Anual de Computação. Disponível em: <https://www.enacomp.com.br/2013/anais/pdf/19.pdf>. Acesso em: 05 ago. 2019.

WRIGHTSON, **Tyler. Segurança de Redes Sem Fio: Guia do Iniciante**. Porto Alegre: Bookman, 2014.

TORRES, Gabriel. **Redes de Computadores Curso Completo**. AxelBooks, 2011.

BOF, Edson. **Segurança em Redes Wireless**. 2010. Monografia, Curso de Pós-Graduação - Faculdade do Centro Leste, Serra. Disponível em: <http://br.monografias.com/trabalhos-pdf/seguranca-redes-wireless/seguranca-redes-wireless.pdf>.Acesso em: 01 out. 2014.

BROAD, James; BINDNER, Andrew. **Hacking com Kali Linux: Técnicas práticas para testes de invasão**. São Paulo: Novatec, 2014.

CARAÇA, Francislaine Vanessa; PENNA, Roberta Galacine. **Segurança em redes sem fio: Desafios, Vulnerabilidades e Soluções**. São José dos Campos – SP, 2009.

ENGST, Adam; FLEISHMAN, Glenn. **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.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. Porto Alegre: Bookman, 3. ed, 2006.

GARCIA, Luis Guilherme Uzeda. **REDES 802.11 (Camada de Enlace): Redes locais sem fio que atendem ao ao padrão IEEE 802.11**. Disponível em: < http://www.gta.ufrj.br/grad/01_2/802-mac/R802_11-2.htm>. Acesso em: 25 nov. 2014.

HORST, A. S.; Pires, A. S.; DÉO, A. L. B. **De A a ZABBIX**. São Paulo: Novatec, 2015.

MINIAURÉLIO. 6ª edição revista e atualizada do Minidicionário Aurélio da Língua Portuguesa 5ª impressão. Curitiba, agosto de 2005.

MORAES, Alexandre Fernandes de. **Redes Sem Fio: Instalação, Configuração e Segurança**. São Paulo: Érica, 2010.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. São Paulo: Novatec, 3. ed, 2011.

STAROSKY, Ana Francisca. **Panorama dos Trabalhos de Conclusão de Graduação em Enfermagem da Universidade do Vale do Itajaí - Biguaçu no período de 2003 a 2009-1.** 2009. Conclusão de Curso - Universidade do Vale Itajaí, Biguaçu. Disponível em: <http://siaibib01.univali.br/pdf/Ana%20Francisca%20Starosky.pdf> Acesso em 04 ago. 2019.

TANENBAUM, Andrew Stuart. **Redes de Computadores**. Pearson, 4. ed, 2003.

TEIXEIRA, Iêda Paula de Farias; SILVA, Maria das Graças Maciel. **Segurança em Redes sem Fio**.2012. Conclusão de Curso – Instituto de Computação, Alagoas. Disponível em:<http://www.ufal.edu.br/unidadeacademica/ic/graduacao/sistemas-de-informacao/arquivos-monografias/arquivos-2012/seguranca-em-redes-sem-fio>.Acesso em: 01 out. 2014.

SANTOS, Pedro Paulo Martins dos. **Análise de Segurança em Redes sem Fio e Proposta de Solução para o Laboratório da Engenharia de Redes de Comunicação**. 2015. Conclusão de Curso – Universidade de Brasília, Brasília. Disponível em: < http://bdm.unb.br/bitstream/10483/15505/1/2015_PedroPauloMartinsDosSantos_tcc.pdf>. Acesso em: 05 ago. 2019.

.FILHO, Huber Bernal. **Simple Network Management Procol (SNMP)**. 2 ed. Disponivel em: <https://www.teleco.com.br/tutoriais/tutorialsnmp/default.asp>. Acesso em: 04 ago. 2019.