UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE COMPUTAÇÃO
CURSO DE CIÊNCIA DA COMPUTAÇÃO

VITOR LONGO

ANÁLISE DE SEGURANÇA NA REDE DOMÉSTICA UTILIZANDO-SE DE SOFTWARES IDENTIFICADORES DE VULNERABILIDADES

TRABALHO DE CONCLUSÃO DE CURSO

MEDIANEIRA

2017

VITOR LONGO

ANÁLISE DE SEGURANÇA NA REDE DOMÉSTICA UTILIZANDO-SE DE SOFTWARES IDENTIFICADORES DE VULNERABILIDADES

Trabalho de Conclusão de Curso apresentado ao Departamento Acadêmico de Computação da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Bacharel em Computação".

Orientador: Prof. Dr. Neylor Michel

MEDIANEIRA

2017

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Graduação e Educação Profissional
Coordenação do Curso de Ciência da Computação

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TERMO DE APROVAÇÃO

ANÁLISE DE SEGURANÇA NA REDE DOMÉSTICA UTILIZANDO-SE DE SOFTWARES IDENTIFICADORES DE VULNERABILIDADES

Por

VITOR LONGO

Este Trabalho de Conclusão de Curso foi apresentado às 13:00 do dia 21 de novembro de 2017 como requisito parcial para a obtenção do título de Bacharel no Curso de Ciência da Computação, da Universidade Tecnológica Federal do Paraná, Câmpus Medianeira. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Nelson Miguel Betzek
UTFPR - Câmpus Medianeira

Prof. Hamiton Pereira da Silva
UTFPR - Câmpus Medianeira

Prof. Dr. Neylor Michel
UTFPR - Câmpus Medianeira

A folha de aprovação assinada encontra-se na Coordenação do Curso.

RESUMO

LONGO, Vitor. ANÁLISE DE SEGURANÇA NA REDE DOMÉSTICA UTILIZANDO-SE DE SOFTWARES IDENTIFICADORES DE VULNERABILIDADES. 40 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2017.

Com o avanço tecnológico na atual sociedade, se conectar a rede global de Internet está se tornando uma atividade muito comum entre as pessoas. Considerando este cenário, a maioria dos usuários conectados não tem conhecimento dos riscos a que podem estar expostos, acessando locais que não garantem a segurança de suas informações. Portanto este trabalho tem a finalidade de avaliar quão eficiente é a segurança contida em uma rede pessoal doméstica, se apenas as seguranças pré-definidas nos diferentes roteadores empregados neste trabalho são suficientes e quais são suas vulnerabilidades, gerando assim um relatório com o objetivo de trazer uma noção dos riscos que o usuário de uma rede doméstica está correndo e o que ele pode fazer para prevenir se.

A metodologia dos testes foi baseada e adaptada do Penetration Testing Execition Standardard, a execução e avaliação do nível da gravidade das vulnerabilidades contidas nas redes domésticas segue o padrão Common Vulnerability Scoring System contida na ferramenta Nexpose.

Palavras-chave: prevenção, riscos, teste de invasão

ABSTRACT

LONGO, Vitor. SECURITY ANALYSIS IN THE HOME NETWORK USING SOFTWARE VULNERABILITY IDENTIFIERS). 40 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2017.

With the tremendous technological breakthrough in our current society, connecting to the global Internet network is becoming a very common activity among people. Considering this scenario, most connected users are not aware of the risks they may be running, accessing locations that do not guarantee the security of their information. Therefore, this work has the purpose of evaluating how efficient is the security contained in a personal home network, if only the pre-defined security in the different routers used in this work are sufficient and what are their vulnerabilities, thus generating a report with the objective of bringing a notion of the risks that the home network user is running and what he can do to prevent himself.

The testing methodology will be based on and adapted from the Penetration Testing Execition Standardard, the implementation and assessment of the level of vulnerability contained in the home networks will follow the Common Vulnerability Scoring System contained in the Nexpose tool.

Keywords: prevention, risks, invasion test

LISTA DE FIGURAS

LISTA DE SIGLAS

ALG	Application Layer Gateway
ARP	Address Resolution Protocol
CIFS	Common Internet File System
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DoS	Denial of Service
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPSEC	IP Security Protocol
L2TP	Protocolo de Tunelamento de Camada 2
LAN	Local Área Network
MAC	Media Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
PFD	Portable Document Format
PPTP	Point-to-Point Tunneling Protocol
PTES	Penetration Testing Execution Standard
SMB	Server Message Block
SPI	State Packet Inspection
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WEB	World Wide Web

TERMINOLOGIA

Termo	Descrição
Botnet	É um conjunto de programas conectados à Internet que comunicam-se entre si com a finalidade de executar tarefas.
Datagrama	É uma entidade de dados completa, um nome genérico para uma mensagem enviada sem conexão e sem confirmação.
Ethernet	Consiste em uma arquitetura cabeada de interconexão para redes locais.
Framework	É uma abstração que une códigos comuns entre vários projetos de software provendo uma funcionalidade genérica.
Gateway	É uma máquina destinada a algum tipo de aplicação, geralmente interligando redes ou trabalhando junto com outra aplicação.
Handshake	Pode ser entendido como aperto de mão, o processo pelo qual duas máquinas afirmam uma a outra que a reconheceu e está pronta para iniciar a comunicação.
Host	É qualquer máquina ou computador conectado a uma rede, que possa oferecer informações.
LAN	Do inglês Local Área Network. Geralmente refere se a redes de computadores restritas a um certo local específico.
Malware	Destinado a infiltrar-se em um sistema de computador de forma ilícita.
Metadata	É dados que fornecem informações sobre outros dados.
Software	É uma sequência de instruções interpretadas e com o objetivo de executar tarefas especificas.
Scanning	Um processo em que sonda uma rede alvo com intenção de revelar informações úteis.
Testes de Penetração	É um processo de simulação de ataques maliciosos reais, visando encontrar e remover vulnerabilidades.

SUMÁRIO

1 INTRODUÇÃO

Devido ao grande número de informações expostas no mundo tecnológico, a criminalidade tem insistido em atuar crescentemente nos delitos virtuais, onde gradativamente se cria o hábito de salvar dados em formatos digitais e armazená-los online. Deste modo tornou-se mais que necessário ter confiabilidade e garantia de segurança quando ocorre a manipulação dessas importantes informações, obtendo assim, uma ação preventiva contra roubos e perda de dados pessoais, fotos, senhas e informações bancárias.

O custo para prevenir-se antes da ameaça, deve ser menor que o custo de uma perca, caso a ameaça o atingir. Com a existência dos riscos, ameaças e a facilidade em se conectar na rede global de Internet, é encontrado uma grande quantidade de métodos, informações e softwares de segurança para prevenir-se desses problemas. O *firewall* contido no roteador, na qual conecta a rede doméstica na rede de internet, existe com o escopo de filtrar algumas dessas ameaças.

Neste trabalho foi estudado o quão eficiente é a segurança contida em uma rede pessoal doméstica, se apenas as seguranças pré-definidas nos diferentes roteadores empregados neste trabalho são suficientes e quais são suas vulnerabilidades, foram realizados testes com o auxílio de softwares e *frameworks* que identificam as falhas que possam estar presentes em uma rede a partir de uma vulnerabilidade nela exposta e que detectam a fragilidade do tal. Com isso foi gerado um relatório com o objetivo de identificar os riscos que o usuário de uma rede doméstica está exposto e o que se pode fazer para prevenir. Tendo em vista que é muito simples para estar conectados na rede global de internet sem a necessidade de ter algum conhecimento sobre os riscos expostos.

1.1 OBJETIVOS GERAIS

Analisar a segurança, vulnerabilidade e riscos em uma topologia de rede doméstica, com o auxílio de softwares e *frameworks* que identificam as falhas que possam estar presentes em uma rede a partir de uma vulnerabilidade nela exposta e que detectam a fragilidade do tal, trazendo um relatório geral ao usuário e prevenções que ele pode tomar.

1.2 OBJETIVOS ESPECÍFICOS

Este trabalho inicialmente será composto pelos seguintes passos:

- Compreender a estrutura básica de uma rede doméstica;
- Estudar a metodologia de testes e análises que possam ser executados para a finalidade deste trabalho;
- Estudar o funcionamento das ferramentas presentes no Kali Linux, do Nexpose, Nmap e Metasploit;
- Analisar os resultados da análise sobre as vulnerabilidades e falhas na rede e/ou dispositivos;
- Apresentar um relatório geral sobre os riscos, vulnerabilidades, soluções para as falhas encontradas e prevenções que os usuários podem adotar.

1.3 JUSTIFICATIVA

Segundo a Symantec (2016) mais de meio bilhão de registros de informações pessoais foram roubados ou perdidos em 2015. Considerando essa e outras informações como os inúmeros ataques, invasões de privacidades, roubos de dados, mal intencionadas com o intuito de burlar sistemas, o roteador é o principal equipamento que faz a conexão entre à rede residencial com a rede global de internet, com isso será analisado a segurança, vulnerabilidade

e riscos em uma topologia de rede doméstica, com o auxílio de softwares e *frameworks*, com a metodologia dos testes baseada e adaptada do *Penetration Testing Execution Standard*(PTES)) e a avaliação do nível da gravidade das vulnerabilidades contidas nas redes domésticas seguirá o padrão *Common Vulnerability Scoring System*(CVSS) contida na ferramenta Nexpose.

Tudo isso com o propósito de diminuir os riscos, trazendo assim prevenções e uma maior tranquilidade ao usuário. Vendo que atualmente é muito simples para qualquer pessoa estar conectado na rede global de Internet sem a necessidade de ter algum conhecimento sobre os riscos que pode estar correndo. Este trabalho vem com o intuito de analisar a segurança em uma rede residencial, acarretando uma interessante análise aos usuários.

2 REFERENCIAL TEÓRICO

Este capítulo destina-se a apresentação do estado da arte, redes domésticas e a importância da segurança; Também será dada uma breve introdução sobre algumas ferramentas que serão usadas no trabalho.

2.1 REDES DOMÉSTICAS

Em Tanenbaum (1996) é lembrado que em 1977 o presidente da *Digital Equipment Corporation*, Ken Olsen, a segunda maior fornecedora de computadores de todo o mundo, foi questionado sobre o porquê sua empresa não estava seguindo a tendência do mercado de computadores pessoais. Olsen respondeu que não existia nenhuma razão para qualquer individuo possuir um computador em casa. Ou seja, a história mostrou o contrário, e a empresa de Olsen já não existe mais.

O uso doméstico de computadores era restrito à processamento de textos e jogos, só que nos últimos anos esse quadro mudou radicalmente. Segundo a CGI (2015), 51% dos domicílios brasileiros possuem conexão com à Internet.

Mesmo que a rede doméstica seja pequena e não consiste em ser alvo principal de usuários maliciosos, existe a necessidade de atenção na sua segurança, pois a presença de arquivos confidenciais também é grande e em ambientes residenciais tem a propensão de permanecer conectado na Internet por um longo período de tempo (CECíLIO, 2000).

Segundo Almeida (2009) os componentes básicos para uma rede doméstica consistem em:

- **Modem** - estabelece a ligação autenticada entre a rede interna com o provedor de Internet contratado;
- **Roteador** - consiste em permitir as comunicações da rede doméstica com o provedor, através do mecanismo de traduções de endereços;

- **Switch** - disponibiliza interfaces *Ethernet* para a ligação de equipamentos cabeados a partir da rede interna;
- **Acesso Wi-Fi** – possibilita a criação de uma rede sem fio com mecanismos de proteção para dispositivos móveis;
- **Servidor DHCP** – é a gestão na qual configura todos os equipamentos que solicitam a conectividade na rede.

Na Figura 1 apresenta-se a interligação dos componentes presentes em uma rede residencial.

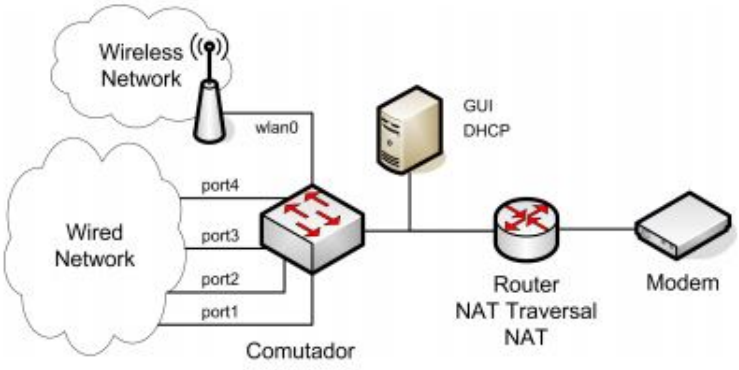

Figura 1 – Componentes básicos de uma rede doméstica.
Fonte: Almeida (2009)

Com o grande avanço na tecnologia, atualmente encontram-se todos esses componentes em apenas um equipamento, como apresentado na Figura 2. Além de conter configurações de segurança pré-definidas como a do *firewall*, onde o usuário pode escolher as opções de segurança que preferir.

Por serem apenas de uso residencial, os equipamentos tendem a ser de baixo custo, gerando dúvida ao usuário quanto à segurança da conexão.

Na próxima seção será descrito mais detalhado sobre o roteador.

2.2 ROTEADORES

O roteador ONT ZHONE 2426, do ano de 2012, é um dispositivo de conexão com especificação *Dual* 802.11b/g/n WiFi, cabeada, um *switch* com 4 portas, porta USB e suporte

Figura 2 – Roteador TP-Link TD-W8961N.
Fonte: TP-Link (2017)

para fibra óptica. É um dos modelos fornecidos no plano de internet da empresa Copel Telecom. Vem com regras de segurança no *firewall* já configuradas, não sendo possível edita-las pelo login do usuário.

Figura 3 – Roteador ONT ZHONE 2426.
Fonte: Multicominc (2017)

O roteador TP-LINK TL-WR741ND, do ano de 2010, é um dispositivo de conexão de rede cabeada e *wireless* integrado com um roteador de compartilhamento de Internet e um *switch* com 4 portas. É muito usado em redes domésticas devido ao seu preço bem acessível. Suas configurações de segurança do *firewall* que podem ser habilitadas são:

- **SPI Firewall** - a Inspeção do Estado do Pacote (do inglês, *State Packet Inspection* (SPI)) ajuda a evitar ataques de hackers rastreando estados por sessão estabelecida (aplicações rodando tempo real na rede). Valida o tráfego avaliando a sessão criada e seu respectivo protocolo;
- **Virtual Private Network (VPN)** - possui as opções *Point-to-Point Tunneling Protocol*(PPTP), (L2TP) e *IP Security Protocol* (IPSEC) *Passthrough*, na qual permitem ou não os caminhos de tunelamento que passam pelo roteador;
- **Gateway da Camada de Aplicação (do inglês, *Application Layer Gateway* (ALG)** - permite fazer o controle entre cliente e servidos dos protocolos *File Transfer Protocol* (FTP), *Trivial File Transfer Protocol* (TFTP), entre outros;
- **DoS** - através desta opção é possível proteger o roteador de ataques do tipo DoS, como os diferentes tipos de ataque de inundações;
- **Proteção Address Resolution Protocol (ARP)** - é útil para o controle do acesso em nível de endereços dos computadores na rede local. Só permitirá o tráfego dos pacotes com base no *Media Access Control* (MAC) e IP vinculados.

O Roteador EDIMAX EW-7209APg, do ano de 2007, é um dispositivo de conexão com especificação IEEE 802.11g / b 2.4GHz de rede cabeada e *wireless* integrado com um roteador de compartilhamento de Internet, possui função repetidor e tem um *switch* com 5 portas. Suas configurações de segurança do *firewall* que podem ser habilitadas são:

- **Filtro de Portas, IP e MAC** - é uma tabela criada para restringir pacotes da rede local para a Internet através do *gateway*;
- **Redirecionamento de Portas** - permite o redirecionamento automático de serviços de rede comuns a uma máquina específica através do firewall *Network Address Translation* (NAT);
- **Script Pessoal** - está opção permite a execução de script manual.

2.3 IMPORTÂNCIA DA SEGURANÇA

No decorrer dos anos, acaba-se tendo uma preocupação maior com os problemas de segurança na área de tecnologia, como pode-se destacar alguns casos ocorridos em páginas World Wide Web(WEB)) de várias organizações como o Yahoo, Exército dos Estados Unidos, a NASA e o New York Times na quais foram invadidas e modificadas por crackers

Figura 4 – Roteador TP-LINK TL-WR741ND e EDIMAX EW-7209APg.
Fonte: Autoria própria.

(TANENBAUM, 1996).

O termo mais usado pra quem realiza um ataque em um sistema de computadores é hacker, porém em sua definição original, hacker usa seu conhecimento para invadir sistemas e mostrar sua habilidade, mas não com o intuito de causar danos, diferentemente dos denominados crackers, que invadem os sistemas com a finalidade de causar prejuízos e roubar informações, geralmente obtendo algum lucro com isso.

A segurança da informação é a proteção dos sistemas de informação contra usuários não autorizados, intrusões e a modificação não autorizada de dados ou informações, armazenadas, em processamento ou em trânsito, a fim de prevenir, identificar e armazenar as possíveis ameaças a seu desenvolvimento (ABNT, 2005; TIPTON; KRAUSE, 2007; DIAS, 2000).

É evidente a necessidade de um maior cuidado ao manipular informações nesse atual mundo globalizado devido aos riscos que se encontram nele, conforme Abnt (2005), Tipton e Krause (2007), Dias (2000), a confidencialidade, integridade e disponibilidade são os princípios básicos para garantir a segurança das informações:

- **Confidencialidade** - a informação acessada apenas por pessoas autorizadas, garantindo assim a identificação e autenticação das partes envolvidas;
- **Disponibilidade** - a disponibilidade da informação ou sistema de computador quando a mesma for necessária;

- **Integridade** - a originalidade da informação no exato momento de seu armazenamento, ou seja, a proteção dos dados contra modificações intencionais ou acidentais não autorizadas.

Sêmola (2002), Rezende e Abreu (2003), defendem que para uma informação seja considerada segura, deve se respeitar os seguintes pontos:

- **Autenticidade** - garante que a informação ou o usuário da mesma é autêntico, ou seja, de uma origem comprovada e validada;
- **Não repúdio** - não é possível negar uma operação sobre os dados que foram criados, modificados, recebidos e/ou enviados;
- **Legalidade** - garante a legalidade via judicial da informação, onde todas as partes ligadas estão de acordo com as cláusulas contratuais definidas inicialmente ou a legislação nacional ou internacional vigente;
- **Privacidade** - diferente de confidencialidade, pois uma informação pode ser definida como confidencial, mas não privada. É a disponibilidade de um usuário realizar ações em um sistema, sem que seja identificado.

Fica claro que com a manipulação de dados particulares é necessário ter uma maior atenção. A seguinte subseção irá descrever as definições de ameaças, riscos e ataques a sistemas de informações.

2.3.1 Definição de Ameaça

Devido à pouca segurança, seja ela, pela falta de conhecimento ou pela inteligência de intrusos, o usuário se encontra exposto a várias ameaças. Segundo Shirey (2000), ameaça é um possível perigo que poderia explorar uma vulnerabilidade causando prejuízos, e também classifica os diferentes tipos das ameaças, dentre elas as voluntárias, isto é, as intencionais, denominando os praticantes como hackers, ladrões, espiões e disseminadores de malwares.

Segundo Cisco (2014) na Figura 5 é possível observar a evolução ocorrida nas formas de ataque no decorrer dos anos e que atualmente as formas de ataques mais sofisticados lideram o cenário.

Muitos sites foram derrubados por ataques de negação de serviço (do inglês, *Denial of Service*(DoS)), no qual consiste em que o cracker inunda o site ou aplicação através de envio de um grande número de pacotes ou conexão, tornando-o impossibilitado de responder solicitações

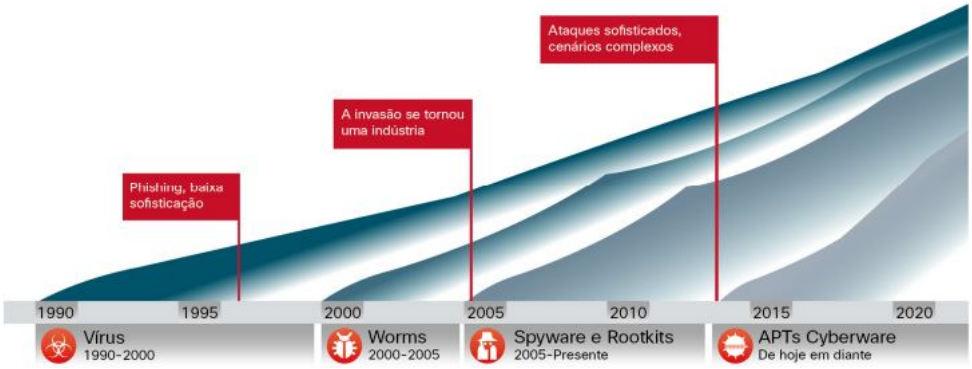

Figura 5 – Evolução das formas de invasões.

Fonte: Cisco (2014)

legais.

Um ataque DoS distribuído (do inglês *Distributed Denial of Service* (DDoS)) ocorre como na Figura 6. O atacante controla vários pontos que sobrecarregam o alvo. Os ataques DDos potencializam vários botnets para as inundações, que consiste num grupo de dispositivos sequestrados na Internet, cada um deles injetado com *malwares*, tendo como objetivo obedecer as ordens do atacante principal, sendo assim muito difíceis de detectar e prevenir do que um ataque DoS (KUROSE; ROSS, 2009).

Desta maneira, os aparelhos conectados em uma rede doméstica com pouca segurança, podem estar sendo parte de um ”exército”com propósitos maliciosos e sem que o usuário tenha conhecimento do fato.

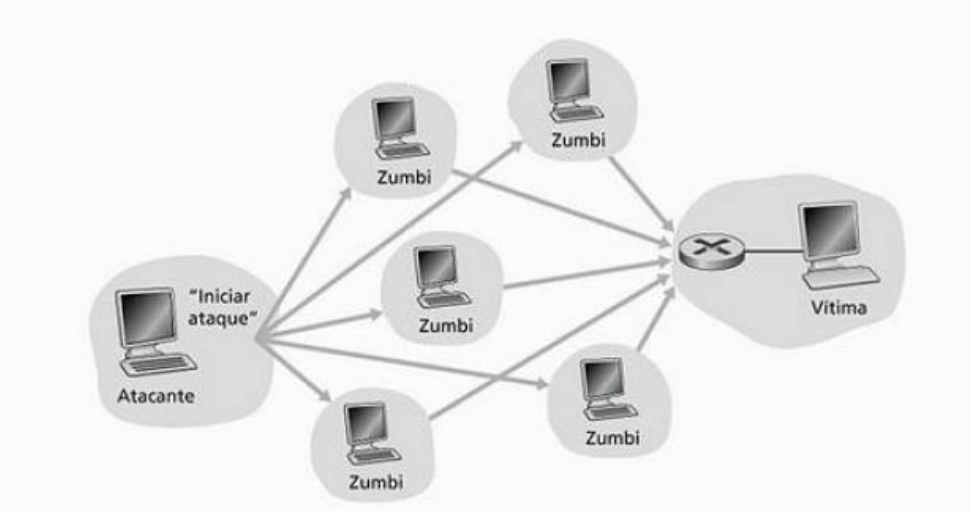

Figura 6 – Um ataque DDoS.

Fonte: Kurose e Ross (2009)

Ainda em 2015, segundo a Symantec (2016), foram ocorridos inúmeras invasões registradas. Ocorreram violações com mais de 10 milhões de identidades expostas, uma crescente de 36% sobre novos *malwares* identificados na rede comparado com 2015 e no final de 2015 ocorreu uma das maiores violações já relatadas, mais de 110 milhões de dados pessoais foram expostos.

Na próxima seção será descrito uma visão geral sobre o funcionamento do *firewall*.

2.4 FIREWALL E IDS

Segundo Tanenbaum (1996), *firewall* é uma forma de segurança adaptada da era medieval, onde se cavava um poço fundo ao redor do castelo, obrigando todos a passar por uma única ponte de entrada e saída, desta maneira podendo ter guardas nela para fazer revistas. Na prática em redes isso se equivale a todo o fluxo de pacotes ocorridos a passar por uma ponte eletrônica, neste caso a ponte é o *firewall*. Na Figura 7 pode ser visto um *firewall* com dois filtros e um *gateway* de aplicação. O filtro de pacotes da *Local Área Network* (LAN) interna verificará os envios, o externo verificará os recebidos. Os pacotes que passam pelo primeiro obstáculo vão ser submetidos a mais uma verificação no *gateway* de aplicação. A importância dos dois filtros de pacotes em diferentes LANs tem como objetivo assegurar que nenhum pacote fique sem passar no *gateway* de aplicação, já que não há outro caminho.

A arquitetura de um *firewall* deve ser desenvolvida de acordo com as necessidades e políticas do usuário. Sendo assim não existe um tipo especifico de configuração e arquitetura de *firewall* na qual que servirá para todos.

Conforme Kurose e Ross (2009), um *firewall* é o trabalho conjunto de um hardware e um software, que isola a rede interna da internet em geral, controla os pacotes, e permite um administrador gerenciar o fluxo de tráfego. Kurose e Ross (2009) também classifica um *firewall* em 3 categorias:

- **Filtros de pacotes tradicionais** - normalmente uma topologia de internet tanto corporativa ou doméstica tem um roteador de borda que conecta sua rede interna com a Internet externa, isto é, a rede pública, como mostra na Figura 8.

  Portanto todo o tráfego que entra e sai dessa rede interna, passa por esse roteador e nele ocorre a filtragem de pacotes pelo *firewall*. Na filtragem, é determinado se cada datagrama que está sozinho deve passar ou ficar, conforme as decisões que geralmente são baseadas

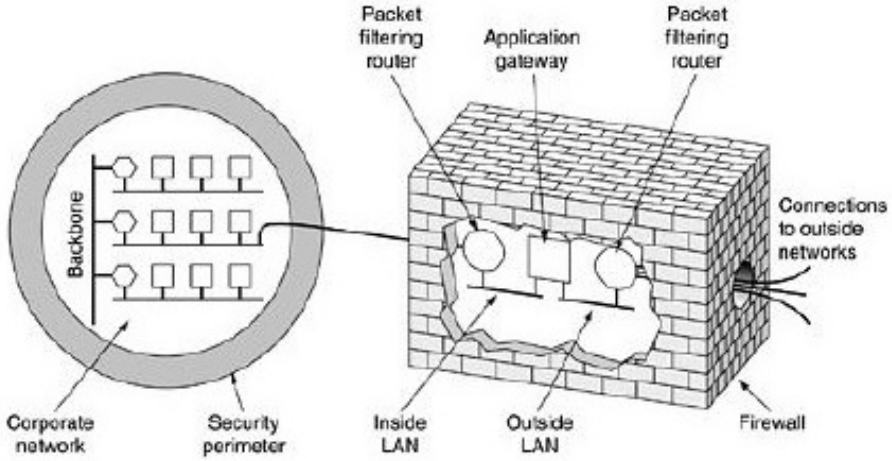

Figura 7 – Estrutura de um firewall com dois fitros e um gateway de aplicação.
Fonte: Tanenbaum (1996)

em endereço *Internet Protocol* (IP) de origem e destino, tipo de protocolo, tipo de porta de origem e de destino e regras diferentes para cada datagrama que entram e saem da rede, onde um administrador de rede gera com base nas politicas da organização;

- **Filtro de estado** - em um filtro de pacote tradicional, as decisões são feitas em cada pacote isolado. Com base nesse conhecimento, os filtros de estado rastreiam conexões *Transmission Control Protocol* (TCP) e tomam as decisões necessárias. Por exemplo, caso um usuário da rede interna solicita navegar em um site Web externo e o servidor Web externo devolve os pacotes, normalmente esses pacotes passariam sem problemas pelo *firewall* na volta, pois alguém o solicitou. Na ocorrência da rede interna receber um pacote defeituoso com a intenção de prejudicar ou causar algum dano, o filtro de estado verifica se existe alguma solicitação desse pacote em andamento, caso não existir, rejeita-o;
- **Gateway de aplicação** - para conseguir um nível mais refinado de segurança, o *firewall* tem que combinar os filtros de pacotes com *gateways* de aplicação. O *gateway* funciona como servidor específico de aplicação, podendo ter um ou mais, cada um com um controle particular próprio de restrições, como podemos observar na Figura 9. Ainda assim os *gateways* têm suas desvantagens, pois deve se ter um para cada aplicação, tornando se o serviço custoso, além de que vários usuários e aplicações usam o mesmo *gateway* ao mesmo tempo, gerando uma preocupação quanto ao seu desempenho.

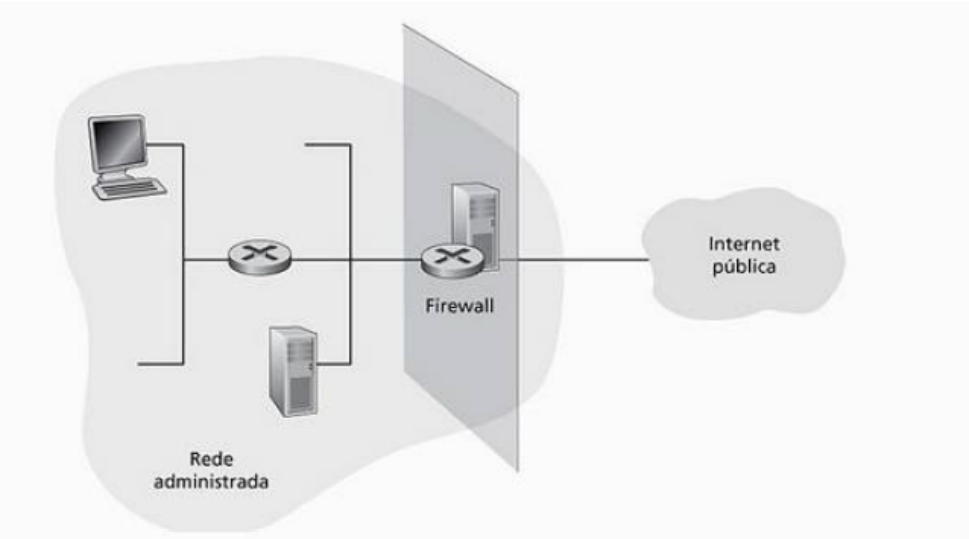

Figura 8 – Posição do firewall entre a rede interna e a rede externa.
Fonte: Kurose e Ross (2009)

Nakamura e Geus (2007) cita outra importante funcionalidade dentro do conceito de *firewall*, os *proxies*, que são softwares que atuam como *gateway* entre as redes. Com essa tecnologia não é possível o usuário interno se conectar diretamente com um servidor externo, garantindo maior segurança para a rede interna.

O funcionamento dos *proxies* é basicamente onde o cliente faz a conexão e seguidamente é autenticado pelo *firewall*. Após esta etapa, o cliente envia sua requisição ao *proxy* que retransmite para o servidor de destino. Já a resposta do servidor externo também é incidida pelo *proxy*. Tudo isso como forma de segurança entre o cliente e o servidor, na prevenção de roubos de informações como possíveis danos entre os dados recebidos na conexão.

Um sistema que gera alerta quando monitora sistemas mal intencionados é chamado de sistema de detecção de intrusos (do inglês, *Intrusion Detection System* (IDS)). Uma IDS pode ser usada para detectar vários tipos de ameaças, como mapeamento de rede, escaneamento de portas, ataques de inundação de banda larga, vulnerabilidade do sistema operacional, vulnerabilidade de aplicações e vírus (KUROSE; ROSS, 2009).

Já Laureano (2005) cita que o IDS tem como principal função detectar e informar quando alguém está tentando invadir um sistema ou se algum usuário autêntico está fazendo mau uso do mesmo.

Uma IDS pode ser instalada em diversas localidades na topologia da rede, já que cada posição pode significar uma configuração de proteção em específico como podem ser visto na Figura 10.

Na sua execução o IDS pode também encontrar alguns problemas, como os *scannings*

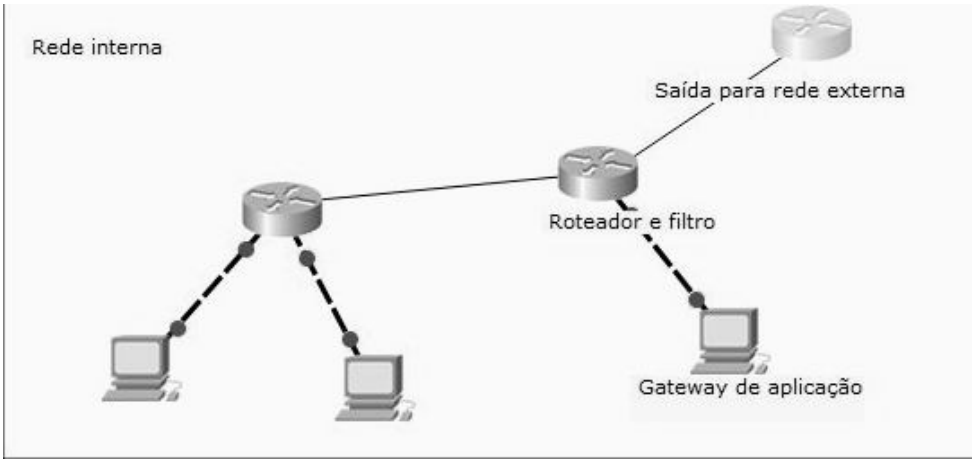

Figura 9 – Topologia com gateway atuando em conjunto com o firewall.
Fonte: Autoria Própria

frequente de intrusos na rede, quantidade grande de pacotes a serem analisados, IP *Spoofing* que impossibilita a descoberta de novos tipos e da origem dos ataques(NAKAMURA; GEUS, 2007).

Na próxima seção, será retratado o *framework*, que consiste em avaliar a segurança em diversas áreas da tecnologia.

2.5 MODELAGEM DE ANÁLISE E TESTE

Segundo Weidman (2014), antes de começar qualquer análise ou teste, é necessário saber o motivo e razão pelo qual será executado. Pois geralmente o cliente que contrata esses testes para sua empresa ou aplicação, desejam obter apenas vulnerabilidades e falhas, não deixando claro para o testador o motivo, uma vez que esses testes são bem intrusivos. Para mais, também será necessário determinar os hosts e endereços de IP que vão fazer parte do escopo para serem efetuados os testes e análises.

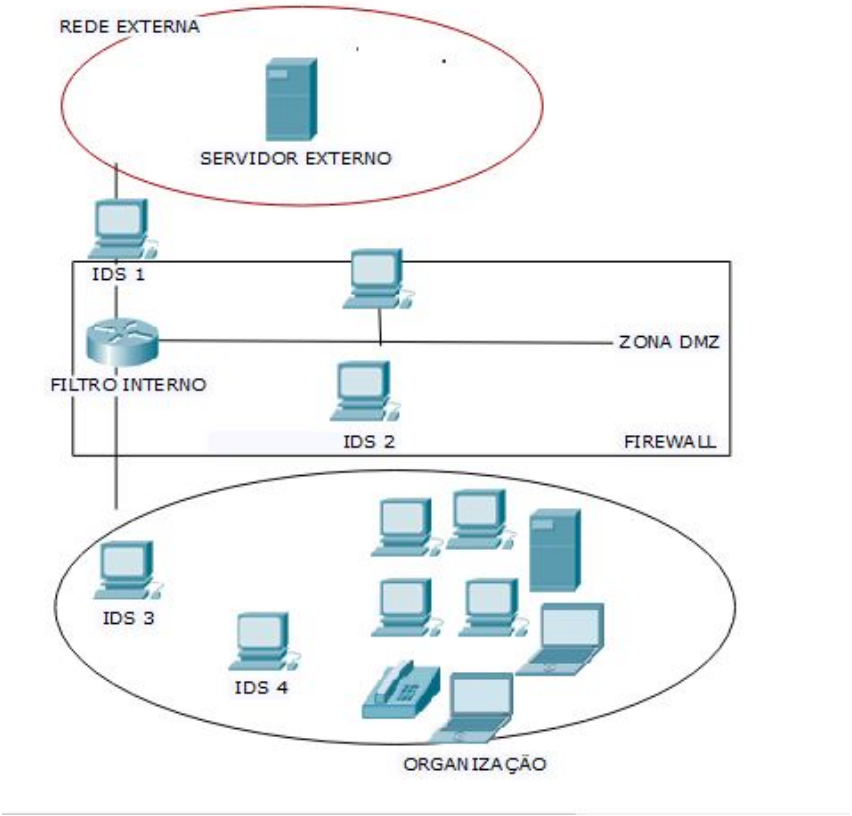

Figura 10 – Topologia com diversos IDSs.

Fonte: Autoria Própria

2.5.1 Coleta de Informação

Na fase de coleta, o objetivo é conseguir o máximo de informação sobre o alvo que será testado, pois a partir dessas informações, será definido o melhor escopo sobre o planejamento dos testes. A coleta de informação apresenta-se de três formas segundo Pentest (2017):

- **Passiva** – na coleta passiva, o testador não deve de maneira alguma ter algum contato com o alvo, deve apenas se utilizar informações armazenadas em repositórios públicos ou de terceiros. Portanto não se tem garantia nenhuma que as informações obtidas estarão corretas;
- **Semi-Passiva** – nesta etapa é permitido o contato com o alvo, porém o tráfego gerado deve ser algo similar com o de um usuário comum, sem despertar algum tipo de atenção. Nesta fase são analisados apenas os metadados presentes em arquivos;
- **Ativa** – a coleta ativa busca mapear toda a estrutura e topologia do alvo, procurando por arquivos, servidores, serviços ocultos e vulnerabilidades. Nesta fase é aplicada

ferramentas que geralmente serão bloqueadas pela rede.

Na próxima subseção será descrito a etapa de análise de vulnerabilidade.

2.5.2 Análise de Vulnerabilidade

Na análise de vulnerabilidade, o PTES descreve de duas maneiras, a fase passiva e a fase ativa:

- **Passiva** – baseia-se na interpretação das metadatas coletados. Pois um arquivo pode conter em sua metadata informações padrões como nome do autor, data de criação e entre outros, mas muitos arquivos permitem customizar essas informações, tendo como exemplo, caminhos para servidores ocultos ou endereço de IP externo. Outra Maneira é conectar a uma rede dados e a partir disso, coletar pacotes para análise (PENTEST, 2017);
- **Ativa** – segue o caminho contrário da passiva, dado que a análise envolve iteração direta com o alvo testado, sendo que está iteração pode ser manual ou automatizada. Na análise automatizada ocorrem tarefas repetitivas, que é o caso do *port scanner*, no qual tem a finalidade de percorrer todas as portas de um host buscando encontrar alguma aberta para conexão (PENTEST, 2017);

  Existem diferentes tipos de *scanners*, os*port scanner*, que normalmente são os primeiros à serem executados pelo testador, pois estes fazem uma varredura geral sobre quais portas estão disponíveis. Este tipo de *scanner* utiliza protocolos baseados no IP como TCP, *User Datagram Protocol*(UDP) e *Internet Control Message Protocol*(ICMP), ambos com a finalidade de encontrar portas abertas para conexão (PENTEST, 2017).

2.5.3 Exploração, Pós-Exploração e Relatório

Na fase de exploração o testador aciona *exploits* com a finalidade de comprometer seu alvo. Deve se executar um *exploit* apenas quando se tem a garantia de que ele será bem sucedido, por isso antes que qualquer tipo de ataque é importante considerar todos os possíveis

mecanismos de segurança ativos no sistema, ou seja, executar *exploits* em massa não é garantia de sucesso e muito menos recomendado (KENNEDY et al., 2011).

Na pós-exploração espera-se que o testador tenha já algum tipo de acesso ao alvo. O objetivo é atacar sistemas específicos, identificando partes críticas e informações que deveriam ser protegidas pela organização. O testador deve também determinar e identificar quais são os ataques que podem comprometer as propriedades intelectuais da organização.

No relatório descreve se quais vulnerabilidades foram descobertas, de que modo foram exploradas e como se pode corrigir as falhas detectadas. As informações produzidas durante a realização dos testes são de suma importância para que os responsáveis pela segurança da organização consigam impedir problemas futuros (KENNEDY et al., 2011).

2.6 METASPLOIT

Metasploit é um *framework* completo para automatizar tarefas rotineiras e até mesmo complexas na área de segurança. Foi criada por H. D. Moore em 2003, pois ele percebeu que perdia muito tempo validando e verificando códigos de *exploits* públicos na empresa de segurança onde trabalhava. Então, H. D. Moore criou sua primeira versão do Metasploit, baseada em Perl, uma estrutura flexível e sustentável para o desenvolvimento de *exploits*. Esta ferramenta tem como objetivo criar um meio de pesquisa para explorar vulnerabilidades, permitindo analisar erros ou falhas que levam a uma brecha na segurança. A partir da descoberta de vulnerabilidades, é feito um estudo para determinar qual o grau da ameaça. Em 2003, o Metasploit foi reescrito por um time de desenvolvimento, desta vez vem na linguagem Ruby. Já em 2009 foi adquirida pela Rapid7, uma empresada muito conceituada na área de detecção de vulnerabilidades, na qual continua aperfeiçoando o *framework* (KENNEDY et al., 2011).

Na Figura 11 observa-se a tela de comandos do Metasploit no sistema operacional Kali Linux.

Na próxima seção, será descrito a ferramenta NMap, seus meios de escaneamento e o Nexpose.

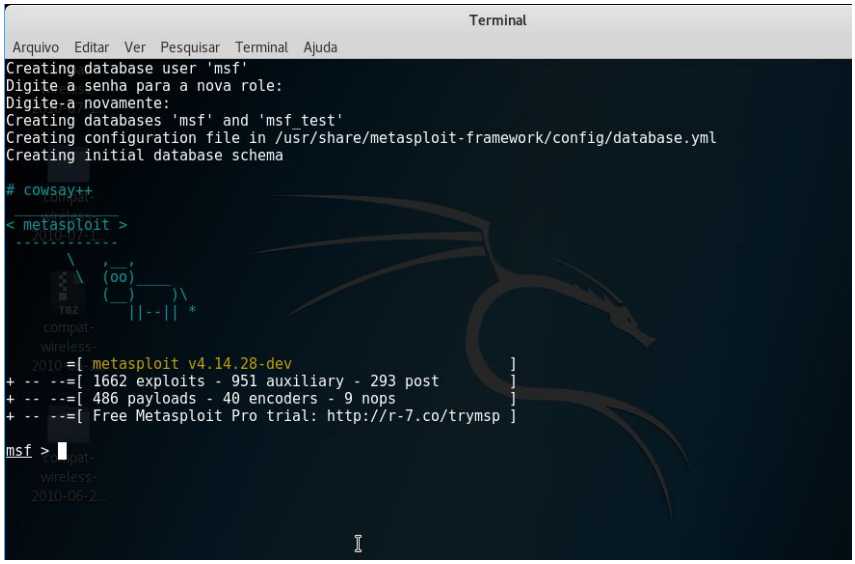

Figura 11 – Tela de comando do Metasploit.

Fonte: Autoria própria

2.7 NMAP E NEXPOSE

Nmap vem do inglês, *Network Mapper*, uma ferramenta de rede com código aberto para exploração e auditoria de segurança. Foi desenvolvida por Gordon Lyon, com o objetivo de escanear rapidamente redes amplas, porem funciona muito bem para estruturas menores e até mesmos hosts únicos. O Nmap utiliza pacotes IP em estado bruto, de maneira inovadora para determinar quais *hosts* estão disponíveis na rede, quais seus serviços, quais seus sistemas operacionais e outras características. Embora o Nmap seja normalmente utilizado para auditorias de segurança, é também muito usado por administradores de sistema para procurar por falhas (NMAP.ORG, 2017).

O Nmap possui o TCP *connect* e o *Synchronise scan*, também conhecido como *Stealth Scan*, que em português seria escâner direto, ambos como forma básica de escaneamento. Esses dois métodos são baseados no protocolo TCP, porem o TCP *connect* faz uma chamada de sistema para iniciar uma conexão com o dispositivo alvo. Se obtiver sucesso é considerado ativo, caso contrário é um elemento inativo (NMAP.ORG, 2017).

O Stealth Scan não mantem a conexão ativa, ele utiliza o processo *handshake* triplo do protocolo TCP, que envolve a troca de 3 pacotes para sincroniza-los e estabelecer a conexão. Esse tipo de escâner consegue impedir o seu aparecimento em logs de aplicações, mas ainda assim, pode ser detectado por mecanismo de detecção de intrusão, os conhecidos

IDS (NMAP.ORG, 2017).

O Nexpose é uma ferramenta desenvolvida pela empresa Rapid7 com a finalidade de escanear vulnerabilidades na rede e em hosts ativos. Além disso divide os resultados em categorias de acordo com o risco encontrado. Essa ferramenta também pode ser integrada perfeitamente com o Metasploit, já que ela se limita em explorar alguns tipos de vulnerabilidades. Além do escaneamento, ela também apresenta correções efetivas para as falhas encontradas, já que gera relatórios com uma grande opção de modelos do resultado obtido (RAPID7, 2017).

Na próxima e última seção deste capítulo, será retratado a ferramenta Kali Linux, que consiste em avaliar a segurança em diversas áreas da tecnologia.

2.8 KALI LINUX

O Kali Linux é um projeto de código aberto baseado no Debian Linux 7.0 que é mantido e financiado pela Offensive Security, uma empresa treinamento de segurança de informação de classe mundial e serviços de teste de penetração presentes em muitas corporações de grande importância global. Kali Linux é a reconstrução completa do antecessor Backtrack.

Nesta sua ultima versão é contida mais de 300 ferramentas e teste de penetração categorizada em grupos mais utilizados por testadores que avaliam a segurança de sistemas de informação. A sua instalação é muito simples, não se diferenciando de instalações dos sistemas operacionais mais conhecidos. Além de instalar diretamente no disco rígido do computador, o Kali Linux pode ser executado diretamente pelo live de um dispositivo removível ou também à partir de uma máquina virtual (BROAD; BINDNER, 2014; KALI, 2017).

Na Figura 12 observamos o terminal do Kali Linux executando uma aplicação scanner de vulnerabilidade em um servidor.

No próximo capítulo será abordado os materiais e métodos detalhado do trabalho.

Figura 12 – Terminal do Kali Linux.

Fonte: Broad e Bindner (2014)

3 MATERIAL E MÉTODOS

Neste capítulo são apresentadas as ferramentas e tecnologias empregadas na realização deste trabalho, bem como a metodologia utilizada para analisar as vulnerabilidades de uma rede doméstica.

3.1 MATERIAL

Para os testes foram necessário a utilização de alguns materiais, como hardwares e softwares, que são descritos a seguir:

3.1.1 Hardware

- Roteador ONT ZHONE 2426;
- Roteador TP-LINK TL-WR741ND;
- Roteador EDIMAX EW-7209APg;
- Smarthpone com sistema operacional Android;
- Notebook - Com 6 gigabytes de memória RAM, processador Intel Core i5 1.80 GHz e sistema operacional Microsoft Windows 10.

3.1.2 Software

Os softwares necessários para a realização deste trabalho são:

- **Oracle VM VirtualBox** - ferramenta da Oracle de virtualização multiplataformas. Permite estender a capacidade do computador para executar vários sistemas operacionais ao mesmo tempo. Neste trabalho foi utilizado está ferramenta com o intuito de permitir a execução do Kali Linux;
- **Metasploit** - Metasploit é um *framework* completo para automatizar tarefas rotineiras e até mesmo complexas na área de segurança;
- **Kali Linux** - é uma distribuição Linux baseada no Debian, voltada para testes de penetração e auditoria de segurança. Neste trabalho será utilizada para executar os testes e descobrir as vulnerabilidades existentes;
- **Nexpose** - uma ferramenta da empresa Rapid7, com o objetivo de escanear vulnerabilidades numa rede de Internet;
- **Nmap** - do inglês *Network Mapper*, é uma ferramenta gratuita e de código aberto para análise do tráfego de rede. Determina a quantidade de *hosts* na rede, aplicações, serviços e portas abertas que estão presentes. No trabalho será usado em uma varredura e *hosts* que se encontram na rede.

3.2 MÉTODOS

As metodologia, análises e testes de segurança da rede doméstica foram baseada e adaptada do PTES, a avaliação do nível da gravidade das vulnerabilidades contidas nas redes domésticas seguirá o padrão CVSS contida na ferramenta Nexpose e constituídas pelas seguintes etapas:

- **Etapa 1** - Inicialmente foi decidido quais os *hosts* que serão analisados e as suas respectivas topologias. Foi usado como base na Seção 2.5 como metodologia, que geralmente é usada em testes de penetração para aplicações corporativas. No caso deste trabalho foi modificada e adaptada para o uso em redes domésticas. Para coleta de informações mais detalhadas foi usada à coleta ativa descrito Seção 2.5 e utilizado a ferramenta Nmap *scanner*. Com a conclusão desta etapa, foi gerado um arquivo com

as informações dos *hosts* ativos, endereços de ips, versão do sistema operacional, portas abertas e os serviços executados em cada *host* pertencente à topologia da rede doméstica. Para melhor organização, foi feito 3 grupos de topologias para os testes:

- Grupo 1 - máquina virtual para fazer os testes com o Oracle VM VirtualBox contendo o Kali Linux, um notebook, um *smartphone*, ambos conectados via *wireless* e o Roteador ONT ZHONE 2426;
- Grupo 2 - máquina virtual para fazer os testes com o Oracle VM VirtualBox contendo o Kali Linux, um notebook, um *smartphone*, ambos conectados via *wireless* e o Roteador TP-LINK TL-WR741ND;
- Grupo 3 - máquina virtual para fazer os testes com o Oracle VM VirtualBox contendo o Kali Linux, um notebook, um *smartphone*, ambos conectados via *wireless* e o Roteador EDIMAX EW-7209APg.

Podemos observar na Figura 13 a topologia da rede doméstica analisada.

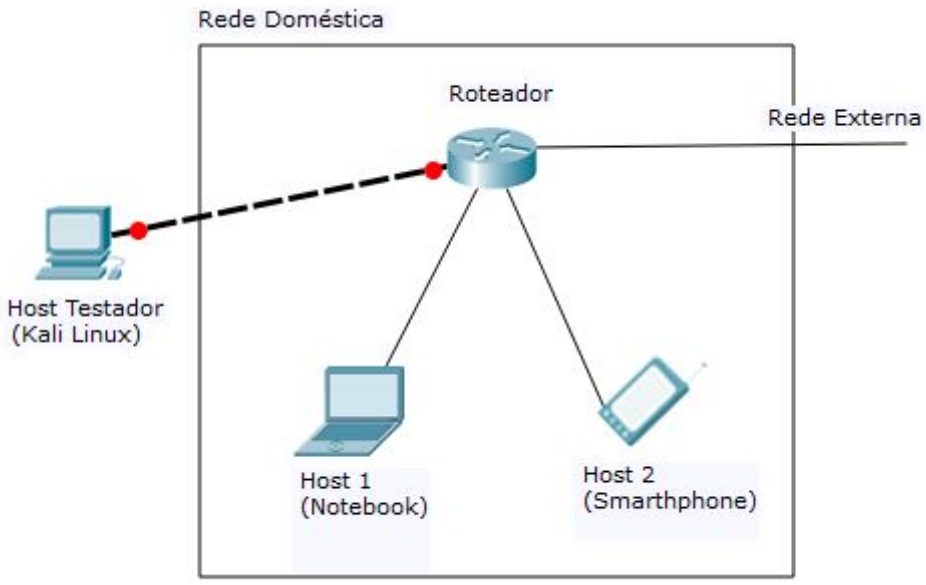

Figura 13 – Topologia da rede doméstica analisada.
Fonte: Autoria Própria

- **Etapa 2** - com as informações adquiridas na etapa 1, foi modelado e explorado as vulnerabilidades com base na fase ativa descrito na Seção 2.5, com a finalidade de encontrar falhas nos *hosts* ativos da rede, neste caso foi usado o Nexpose;
- **Etapa 3** - nesta fase foram executados *exploits* do Metasploit *framework* no Kali Linux, porém apenas são falhas específicas, portanto eles foram escolhidos de acordo com os tipos de vulnerabilidade que foram encontradas em etapas anteriores;

- **Etapa 4** - com os testes feito nas etapas anteriores, é possível até o momento ter uma visão geral de como funciona a rede doméstica, quais seus *hosts* ativos, suas portas abertas, suas vulnerabilidades e quais topologias com o roteador específico possuem mais falhas. A partir disso e através dos resultados obtidos pelo Nexpose, já é possível saber quais as vulnerabilidades mais comuns e as que trazem mais riscos através de gráficos. Também já e notório saber quais dos roteadores contém menos vulnerabilidades. Sendo assim, avançar para a etapa 5, a última etapa, na qual é criada um relatório geral;
- **Etapa 5** - com todas as informações anteriores já obtidas, foi gerado um relatório técnico com o intuito de mostrar as vulnerabilidades da rede, os riscos que elas trazem e se os diferentes roteadores usados trouxeram alguma diferença no resultado da análise, tudo isso de uma forma fácil de entender, esperando-se levar uma visão geral das análises e riscos para pessoas que não possuem conhecimento na área. Além dessas informações, foram listadas dicas e prevenções onde o usuário poderá seguir, a fim de proteger seus dados e interesses quando conectado à rede.

Na próxima seção será demonstrado os resultados obtidos no trabalho.

4 RESULTADOS OBTIDOS

Antes de dar inicio nos testes, foram definidos as topologias e o escopo a ser usado como base. Neste capítulo é descrito a coleta de informações, análise de vulnerabilidades e relatório.

4.0.1 Coleta de Informações

Na fase da coleta de informações utilizaram-se as ferramentas Nmap *scanner* para se obter as dados da rede doméstica. Como o escopo e topologia já foram definidos inicialmente, algumas informações coletadas já são de conhecimento na análise.

O Nmap *scanner* foi executada a partir de uma máquina virtual conectada a rede via *Ethernet*(rede cabeada), contendo o sistema operacional Kali Linux e executada pela Oracle VM VirtualBox, com o objetivo de obter informações sobre os dispositivos e serviços ativos na rede. O comando utilizado foi o seguinte:

1 nmap -sS -O -sV -oN ScannerRedeDomestica.txt 192.168..**

A flag nmap é o comando inicial do *scanner*, o –sS indica que o tipo a ser executado é *Stealth Scan*, devido as suas vantagens, que foram descritos na Seção 2.7. O –O tenta identificar o sistema operacional dos dispositivos conectados durante a análise. O -sV busca uma maior eficácia nos resultados. Já o comando –oN ScannerRedeDomestica.txt faz a ferramenta criar um arquivo de texto com o nome ScannerRedeDomestica contendo os resultados obtidos. Já no final, é identificado os endereços a serem escaneados, onde nesse caso foram os IP entre 192.168.0.1 e 192.168.255.254.

Foram encontrados 3 endereços de Ip ativos em cada um dos testes nos diferentes tipos de roteadores conectados a rede, seus respectivos sistemas operacionais e suas portas abertas. A Figura 14 mostra os resultados gerado para o *host* de endereço 192.168.1.14, utilizando roteador ONT ZHONE 2426.

```
Nmap scan report for 192.168.1.14
Host is up, received arp-response (0.0016s latency).
Scanned at 2017-10-18 13:56:08 -02 for 75s
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT    STATE SERVICE      REASON          VERSION
135/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 0C:84:DC:D3:FA:DF (Hon Hai Precision Ind.)
Microsoft Windows 10 build 10586 - 14393
TCP/IP fingerprint:
Uptime guess: 0.510 days (since Wed Oct 18 01:42:30 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: VITORLONGO; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figura 14 – Resultado obtido através da ferramenta Nmap.

Fonte: Autoria prória.

Os resultados obtidos com o Nmap teve o êxito de conseguir uma alta noção de como é a infraestrutura da rede analisada, identificando assim roteadores e dispositivos na rede através de seu sistema operacional. O Nmap mostrou uma visão geral da estrutura física da rede e uma noção de tipos de vulnerabilidades através das portas abertas e os serviços executados. Como neste caso só identifica a topologia e informações dos dispositivos conectados, os resultados obtidos nos diferentes grupos de testes foram os mesmos.

4.0.2 Análise de Vulnerabilidades

Com as informações adquiridas anteriormente, iniciou-se a fase de análise de vulnerabilidades. As análises foram divididas em três grupos e cada um com três dispositivos ativos. O primeiro grupo com o modelo de roteador ONT ZHONE 2426, o segundo com o modelo de roteador TP-LINK TL-WR741ND e outro com o modelo EDIMAX EW-7209APg.

Para classificar o grau de ameaça de cada vulnerabilidade, o Nexpose utiliza o CVSS, que tem a capacidade de calcular pontuações para elas. Este modelo é mantido pela *National Institute of Standards and Technology* (NIST), com a finalidade de manter um padrão para essa classificação.

A pontuação se baseia na complexidade de acesso, autenticação requerida e o impacto causado caso a vulnerabilidade for explorada, tendo assim um ranking analisado pela maior pontuação, automaticamente a mais critica é a com maior prioridade de remediação

(WEIDMAN, 2014). As vulnerabilidades podem ser também categorizadas como críticas, severas e moderadas. As criticas necessita de remediação imediata, pois tem um risco maior, já as severas merecem uma atenção necessária, sem tanto risco e as moderadas devem também ser removidas, porém sua demanda não é tão urgente e seus riscos são quase nulos.

No grupo 1 e grupo 2 foram obtidos o resultado de 9 vulnerabilidades e com apenas uma considerada crítica. No caso do grupo 1, as 8 vulnerabilidades restantes ficaram divididas entre severas e moderadas, como pode ser observado na Figura 15.

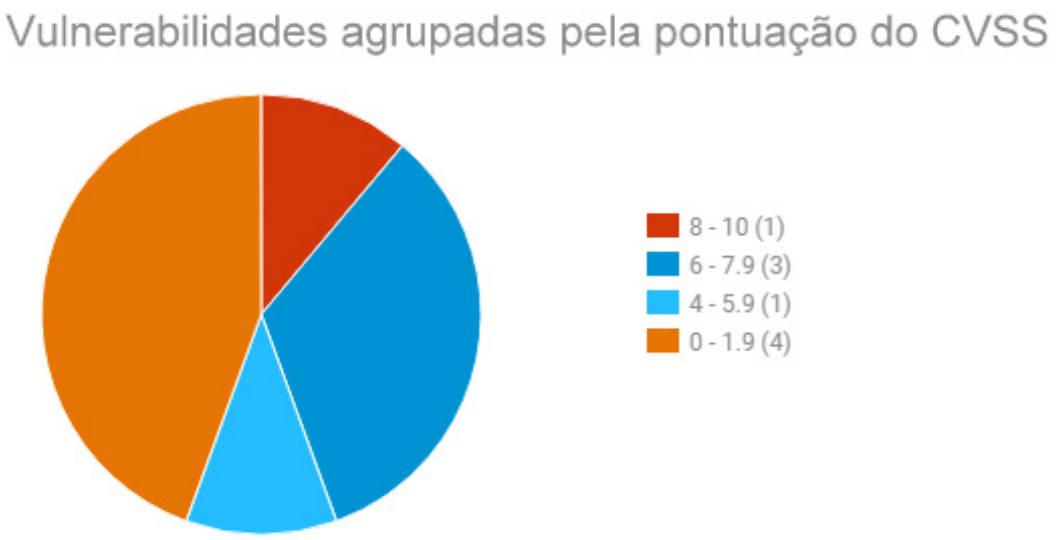

Figura 15 – Vulnerabilidades do grupo 1 agrupadas pela pontuação do CVSS.
Fonte: Relatório criado pela ferramenta Nexpose.

Na Figura 16 referente ao grupo 2, houve 2 ocorrências das vulnerabilidades, a cifs-smb-signature-disabled e cifs-smb-signature-not-required, tornando-as vulnerabilidades mais comuns. Houve 4 instâncias de vulnerabilidade na categoria *Common Internet File System* (CIFS), tornando-a a categoria de vulnerabilidade mais comum.

O grupo 3 foi o que menos apresentou vulnerabilidades encontradas, entretanto manteve o mesmo número de vulnerabilidades críticas e consideradas moderadas, a alteração foi nas categorizadas severas, onde no caso do grupo 3 foi menor, como observado na Figura 17.

Na Figura 18 referente ao grupo 3, houve 2 ocorrências das vulnerabilidades cifs-smb-signature-disabled, cifs-smb-signature-not-required e genérico-icmp-timestamp, tornando-os as vulnerabilidades mais comuns. Houve 4 instâncias de vulnerabilidade na categoria CIFS, tornando-a a categoria mais comum de vulnerabilidade.

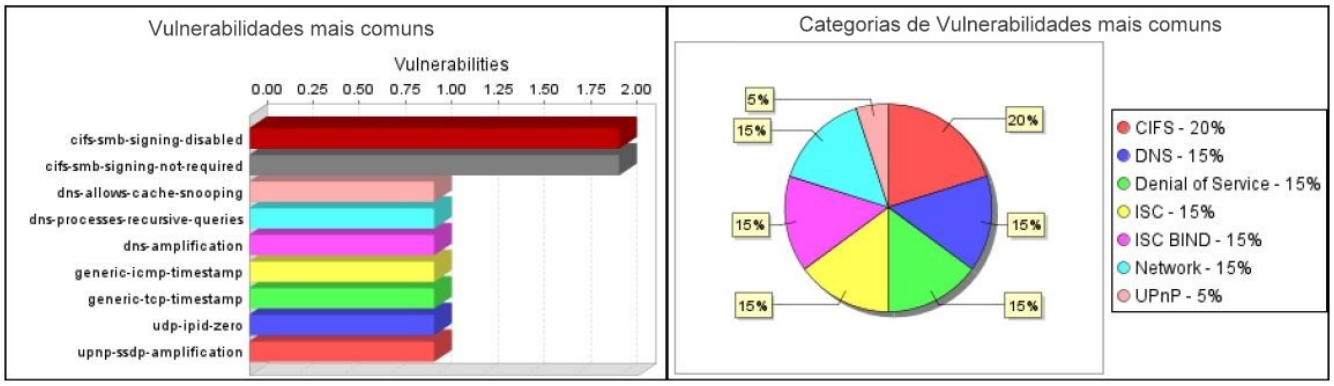

Figura 16 – Vulnerabilidades em comum referente ao grupo 2.

Fonte: Relatório criado pela ferramenta Nexpose.

4.1 EXPLORAÇÃO

Na etapa de exploração, não se teve exito na tarefa usando o Metasploit no Kali Linux, não obtendo solução para o tal. Porém a Rapid7 disponibiliza possíveis soluções para as vulnerabilidades encontradas. No caso do DNS-server-allows-cache-snooping, é mostrado que um invasor pode fazer consultas não recursivas a um servidor de DNS, procurando registros potencialmente já resolvidos por este servidor de DNS para outros clientes. Dependendo da resposta, um invasor pode usar essas informações para potencializar outros ataques.

Para o generic-icmp-timestamp, mostra que as informações de datas e horas de ações do sistema estão disponíveis e em anexo já deixa o site com os passos para desativar está opção que traz as respostas quando solicitado.

Já para o cifs-smb-signature-disabled e o smb-signing-not-required, é mostrado que o sistema não possui assinatura *Server Message Block*(SMB), não garantindo assim a autenticidade destes pacotes. O Nexpose deixa o *link* de um site contendo as soluções para a assinatura do SMB.

Para mais detalhes e soluções para outras vulnerabilidades, se encontra no *link* https://goo.gl/dZWGYq (2017).

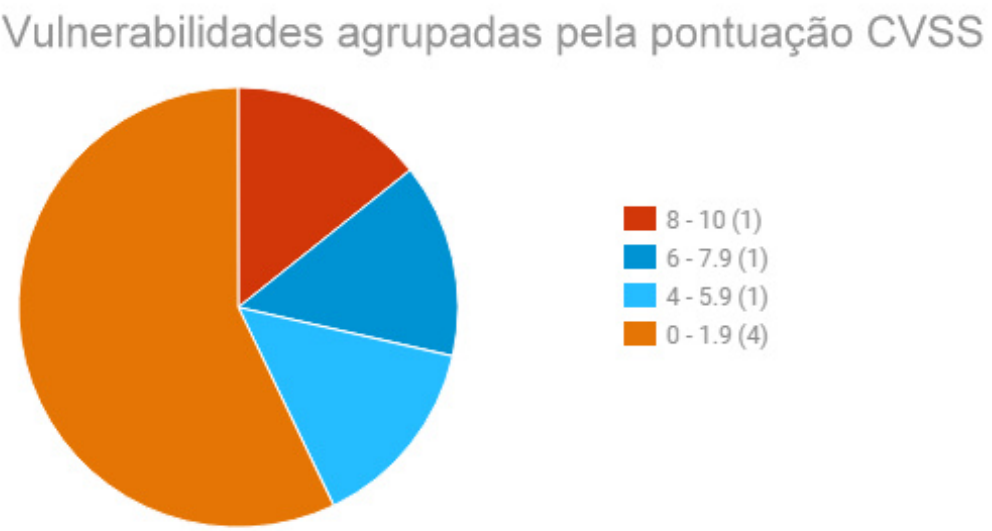

Figura 17 – Vulnerabilidades do grupo 3 agrupadas pela pontuação do CVSS.

Fonte: Relatório criado pela ferramenta Nexpose.

4.2 RELATÓRIO

Para apresentar todos os resultados, potenciais falhas e seus detalhes, foi gerado um documento em *Portable Document Format*(PFD) no qual foi armazenado e disponível para visualização no *link* https://goo.gl/dZWGYq (2017). Entretanto, a fim de não apenas trazer os riscos, no relatório disponível é demonstrado informações relativas às falhas e o que pode ser feito para corrigi-las. Lembrando que as informações estão de forma intuitiva, por meio de

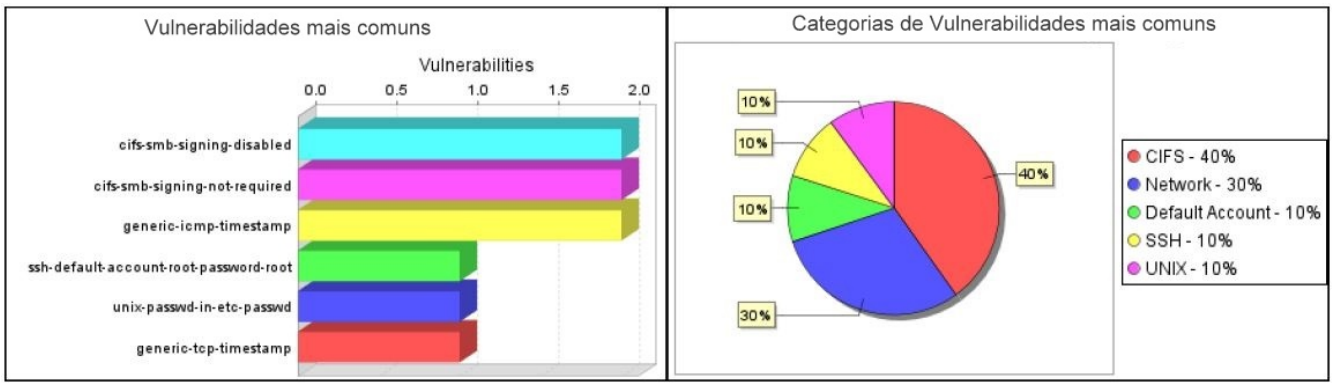

Figura 18 – Vulnerabilidades em comum referente ao grupo 3.

Fonte: Relatório criado pela ferramenta Nexpose.

gráficos, permitindo que pessoas leigas na área tenham um panorama da situação de segurança que a rede oferece, que possui também os números de vulnerabilidades, classificação de acordo com a severidade de cada, quais as mais comuns, as que oferecem mais riscos, identificando os *hosts* ativos, com seus nomes, endereços de IPs, sistemas operacionais e demais informações.

No próximo capítulo será descrito a conclusão final do estudo e sugestões de trabalhos futuros.

5 CONCLUSÕES E TRABALHOS FUTUROS

Nesta seção serão apresentadas as conclusões, bem como possíveis trabalhos futuros com a finalidade de uma melhor avaliação da segurança em redes domésticas.

5.1 CONCLUSÕES

O objetivo principal deste trabalho foi avaliar a segurança de um usuário leigo em sua rede pessoal doméstica através de vulnerabilidades encontradas, analisando os riscos que poderia estar exposto. Com os resultados obtidos utilizando o Nexpose, foi identificado um número muito abaixo do esperado de falhas e com a maioria sem riscos críticos. Uma rede doméstica básica possui sim seus riscos, porém os resultados obtidos neste estudo não seria o grande problema, ou seja, não é o foco da principal preocupação de segurança do usuário.

Por ter sido feito uma análise nas camadas de segurança da rede física, demonstrou-se que os maiores riscos não são na estrutura da rede doméstica. A partir dos resultados obtidos e já como sugestão de trabalho futuro, seria analisar a camada de aplicação, onde o próprio usuário permite os acessos não autorizados de forma indireta e/ou intencional.

Para os tipos de explorações, não foi possível encontrar *exploits* no Metasploit para as vulnerabilidades encontradas, mas foi possível obter referências de soluções para as falhas.

As informações detalhadas das falhas encontradas, resultados e suas soluções, foram disponibilizadas num arquivo em PDF armazenado em https://goo.gl/dZWGYq (2017).

O foco do trabalho foi determinar se os mecanismos de segurança presentes na rede doméstica básica são capazes de garantir a segurança de seus usuários. Analisando o baixo número de vulnerabilidades e seus baixos riscos com as topologias testadas, determina que o nível de segurança para os testes e análises feitas, foi satisfatório.

Quanto aos roteadores testados nas topologias, comprovou que o modelo EDIMAX EW-7209APg, o mais antigo, possuiu menos vulnerabilidades.

5.2 TRABALHOS FUTUROS

Para trabalhos futuros existem uma grande demanda de outras análises e testes que possam obter resultados interessantes. Usar um IDS na própria rede doméstica e mante-lá ativada por vários dias, poderia trazer uma ideia dos tipos de pacotes maliciosos que trafegam na rede.

Um novo estudo que poderia trazer uma noção melhor dos riscos de uma rede doméstica básica, e já com os resultados obtidos deste trabalho, seria fazer uma pesquisa sobre quais tipos de serviços (conta bancária, aplicações que pedem dados pessoais, tipos de armazenamento de dados e etc) o usuário acessa de sua rede. Com isso poderia avaliar-se outros riscos e em conjunto com este trabalho, gerar um relatório mais completo.

Outro estudo seria realizar os mesmos testes de vulnerabilidades usado neste trabalho, em conjunto com outros métodos de avaliação de segurança a serem pesquisados, para outros roteadores, com o intuito de gerar um comparativos de segurança entre diferentes modelos.

REFERÊNCIAS

ABNT. **Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação**. Rio de Janeiro: [s.n.], 2005.

ALMEIDA, J. F. P. de. **Redes Domésticas Seguras**. Dissertação (Mestrado Integrado em Engenharia Electrotécnica e de Computadores) — Faculdade de Engenharia da Universidade do Porto, 2009.

BROAD, J.; BINDNER, A. **Hacking with Kali: Practical penetration testing techniques.** [S.l.]: Steve Elliot, 2014. ISBN 9780124077492.

CECíLIO, E. L. **Acesso Residencial em Banda Larga**. Dissertação (Tese de Mestrado em Informática) — Universidade Federal do Rio de janeiro, 2000.

CGI, C. G. D. I. N. B. . **TIC DOMICÍLIOS 2015 - PESQUISA SOBRE O USO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NOS DOMICÍLIOS BRASILEIROS**. 2015. 1-424 p. Disponível em: <http://cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2015/>. Acesso em: 16 de abril de 2017.

CISCO. **Como lidar com a sequência de ataque completa: antes, durante e depois de um ataque. É hora de ter um novo modelo de segurança**. 2014. 1-8 p.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000. ISBN 8573231319.

HTTPS://GOO.GL/DZWGYQ. **Relatório do resultado do Tcc: Análise de segurança na rede doméstica utilizando-se de softwares identificadores de vulnerabilidades**. 2017. Disponível em: <https://goo.gl/dZWGYq>. Acesso em: 29 de outubro de 2017.

KALI. **What is Kali?** 2017. Disponível em: <https://www.kali.org/>. Acesso em: 20 de maio de 2017.

KENNEDY, D.; O'GORMAN, J.; KEARNS, D. **Metasploit: The Penetration Tester's Guide**. [S.l.]: No Starch Press, Inc, 2011. ISBN 9781593272883.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e A Internet - Uma Abordagem Top-Down**. São Paulo: Pearson Education - Br, 2009. ISBN 9788581436777.

LAUREANO, M. A. P. **Gestão de Segurança da Informação**. 2005. 1-132 p. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 10 de março de 2017.

MULTICOMINC. **Roteador ONT ZHONE 2426**. 2017.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec editora Ltda, 2007. ISBN 9788575221365.

NMAP.ORG. **Nmap Network Scanning**. 2017. Disponível em: <https://nmap.org/>. Acesso em: 11 de julho de 2017.

PENTEST. **Penetration Testing Execition Standard**. 2017. Disponível em: <http://www.pentest-standard.org/index.php>. Acesso em: 24 de julho de 2017.

RAPID7. **Nexpose: Your on-prem vulnerability scanner**. 2017. Disponível em: <https://www.rapid7.com/products/nexpose/>. Acesso em: 18 de agosto de 2017.

REZENDE, D. A.; ABREU, A. F. de. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas S.A, 2003.

SHIREY, R. **RFC 2828 – Internet Security Glossary. The Internet Society**. 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt?number=2828>. Acesso em: 14 de abril de 2017.

SêMOLA, M. **Gestão da Segurança da Informação – Uma visão Executiva**. [S.l.]: Campus, 2002. ISBN 9788535271782.

SYMANTEC. **Internet Security Threat Report**. 2016. 1-81 p. Disponível em: <https://www.symantec.com/security-center/threat-report>. Acesso em: 25 de março de 2017.

TANENBAUM, A. S. **Computer Networks**. [s.n.], 1996. 349–351 p. ISSN 13891286. ISBN 0130661023. Disponível em: <http://www.ietf.org/rfc/rfc169.txt>.

TIPTON, H. F.; KRAUSE, M. **Information Security Management Handbook, Sixth Edition**. [s.n.], 2007. 3280 p. ISBN 1420090925. Disponível em: <http://www.amazon.com/Information-Security-Management-Handbook-Sixth/dp/1420090925>.

TP-LINK. **Roteador TD-W8961N**. 2017. Disponível em: <http://www.tp-link.com.br/products/details/cat-15_TD-W8961N.html>. Acesso em: 16 de maio de 2017.

WEIDMAN, G. **Penetration testing: A Hands-On Introduction to Hacking**. San Francisco, CA: No Starch Press, Inc, 2014. ISBN 9781593275648.