CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNOLÓGICA EM
REDES DE COMPUTADORES

THAISE CRISTINA DA SILVA

WELLINGTON MARCOLINO DA SILVA JUNIOR

# ESTUDO DE FERRAMENTAS EM ANÁLISE DE SEGURANÇA EM REDES

RECIFE/2020

THAISE CRISTINA DA SILVA

WELLINGTON MARCOLINO DA SILVA JUNIOR

# ESTUDO DE FERRAMENTAS EM ANÁLISE DE SEGURANÇA EM REDES

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de computadores.

Professor Orientador: Adilson Silva

RECIFE/2020

S586e

Silva, Thaise Cristina da

Estudo de ferramentas em análise de segurança e redes. / Thaise Cristina da Silva; Wellington Marcolino da Silva Junior. - Recife : O Autor, 2018.

25 p.

Orientador(a): Adilson Silva

Trabalho De Conclusão De Curso (Graduação) Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2020.

1. Segurança. 2. Redes. 3. Sistemas. 4. Ferramentas. Centro Universitário Brasileiro - UNIBRA. II. Título

CDU: 004.7

THAISE CRISTINA DA SILVA

WELLINGTON MARCOLINO DA SILVA JUNIOR

# ESTUDO DE FERRAMENTAS EM ANÁLISE DE SEGURANÇA EM REDES

Artigo aprovado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

---

Prof.° MSc. Adilson da Silva

Professor Orientador

---

Prof.° MSc. Renan Costa Alencar

Professor Examinador

---

Prof.° Esp. Alberto Luiz Veigas

Professor Examinador

Recife. __/__/____

NOTA: _____

*Dedicamos esse trabalho a nossa família, amigos, mestres e profissionais de T.I*

## AGRADECIEMENTOS

Gostaríamos de agradecer pelo apoio dos amigos e familiares nesse projeto, por acreditar que seria capaz e dar total apoio aos envolvidos. Agradecemos também aos nossos professores e mestres que colaboraram com nossa evolução e entendimento sobre o projeto e pesquisa.

*“Quando a educação não é libertadora, o sonho do oprimido é ser o opressor.”*

*(Paulo Freire)*

## SUMÁRIO



## LISTA DE FIGURAS

## LISTA DE SIGLAS

| | |
|---|---|
| **ASCII** | Código Padrão Americano para o Intercâmbio de Informação. |
| **TI** | Tecnologia da Informação. |
| **NASA** | Administração Nacional da Aeronáutica e Espaço. |
| **PenTest** | Teste de Penetração |
| **TTL** | Time To Live (Tempo de vida) |

# ESTUDO DE FERRAMENTAS EM ANÁLISE DE SEGURANÇA EM REDES

Thaise Cristina da Silva

Wellington Marcolino Da Silva Junior

Adilson Silva[1]

**Resumo:** O estudo tem o objetivo de apresentar a importância de algumas ferramentas de segurança e suas aplicabilidades. Será apresentado o desenvolvimento e primeiros passos da segurança nas redes de computadores. A partir de uma análise bibliográfica mostrará a importância e o impacto da obtenção de sistemas de segurança e técnicas para evitar e minimizar danos com ataques e atividades maliciosas. Terá como objetivo mostrar algumas técnicas de invasão que cresceram nos últimos anos e como isso pode ser danoso aos grupos públicos e privados. Assim, pretende justificar os investimentos na área de segurança e esclarecerá o quão é importante a manutenção efetiva nessas áreas dentro das corporações.

**Palavras-Chave:** Segurança. Redes. Sistemas. Ferramentas.

---

[1] Professor da UNIBRA. MSc. Adilson da Silva Orientador. E-mail para contato:adilsondasilva.professor@gmail.com

## 1 INTRODUÇÃO

Em decorrência do grande avanço tecnológico nas últimas décadas, foi possível compreender a importância de obter uma infraestrutura de segurança firme dentro das corporações. Há três pilares quando se fala em segurança: integridade, disponibilidade e confidencialidade, termos que tornaram-se indispensáveis nos negócios e organizações, pois elas dependem constantemente de informações para a realização de seus processos diários. Por esse motivo, será apresentado nesse documento ferramentas com intuito de proteger e assegurar que os principais pilares da segurança não sejam violados e acarretem problemas para os computadores e usuários, principalmente aos ambientes corporativos (BRASIL ESCOLA, UOL, 2016).

Nas áreas que serão descritas no projeto haverá a introdução da história da segurança, os primeiros passos da mesma e desenvolvimento no mundo. Citando marcos históricos e exemplos de funcionando em suas práticas. Em seguida irá discorrer sobre uma das principais ferramentas de segurança em rede: o firewall. Com suas ferramentas internas, explicará o funcionando de alguma das principais funções, como: Filtro de pacotes, filtragem de dados IP, NAT e Proxy de aplicação.

Adentrará em casos de vulnerabilidades em redes, que são espécies de brechas, fraquezas que são encontradas nos sistemas ou em infraestruturas de rede. Seguirá explicando os ataques em rede, negação de serviço e como empresas podem implementar políticas de segurança para evitar vulnerabilidades na rede.

Por fim, a abordagem do tema Pentest. Uma técnica nova no mercado que tem o objetivo de ajudar a encontrar e tratar falhas e brechas nos sistemas, com ações planejadas e organizadas para que tais falhas sejam estudadas e consertadas. O estudo segue explicando os tipos de PENtest e benefícios do mesmo para os grupos coorporativos.

## 2 **DELINEAMENTO METODOLÓGICO**

Para realização deste projeto, será abordada uma pesquisa bibliográfica, analisada e constituída a partir de artigos, livros e materiais disponibilizados na internet, com suas devidas citações. Dessa forma, visa compreender, interpretar e analisar tais dados e informações através de teorias e recursos disponibilizados

Na primeira parte é descrito a história da segurança e seus primeiros passos nas redes de computadores, discutindo o desenvolvimento da mesma no âmbito computacional.

Na segunda parte será descrito sobre a ferramenta de Firewall, aparelho que é constituído por hardware e software. Será apresentado sua história e irá explicar sobre uma das ferramentas mais importantes na proteção de rede atualmente

Também descreverá sobre as vulnerabilidades, que geralmente são descritas como brechas, riscos que podem ser explorados nas tentativas de ataque. Aplicação de golpes, roubo de informações de empresas e pessoas, isso e muito mais é possível quando sistemas estão vulneráveis (Rafael Pizzolato, CMO na Starti, 2019).

Por fim, é explicado sobre um novo método de analises de vulnerabilidades, o PENtest. Uma série de testes que tem como objetivo, descobrir, mapear e expor todas as possíveis vulnerabilidades de uma rede. Definição feita a partir do livro “*PENtest* em redes sem fio”, de Daniel Moreno. Será examinado e apresentado que técnica de *PENtest* não é apenas um scaneamento de vulnerabilidades e portas. *PENtest* faz uso de *softwares* e ferramentas que buscam identificar tipos de informações que podem ser obtidas indevidamente através daquelas falhas.

## 3. SEGURANÇA DE REDES DE COMPUTADORES

Com o surgimento das redes e com a evolução da internet a segurança de redes vem sendo cada vez mais abordada, e para demonstrar essa evolução, será apresentado uma cronologia histórica das redes ao longo do tempo e suas evoluções, os anos 60 foi marcado pelo surgimento do conceito de redes de computadores, avanços na comunicação via satélite, o surgimento do primeiro padrão universal para permitir a troca de dados entre máquinas fabricadas por diferentes empresas, a criação da primeira rede de computadores, a ARPANET, e a conexão dos primeiros computadores nesta rede *(Macedo et.al*. *2018)*.

Segundo *Macedo et.al*(*2018)* O conceito de computadores se deu em meados dos anos 1962 em *Massachussets Institute of Technology* pelo cientista da computação e psicólogo Joseph Carl Robnett Licklider ele descreveu o conceito como uma rede intergaláctica, onde cada indivíduo do globo estaria interconectado e poderia acessar programas e dados em qualquer sítio, indepedente da sua localização, um ano após o satélite SYNCOM (*SYNchronous COMmunication satellite*), ou satélite de comunicação síncrona, foi lançado pela agência espacial NASA(*National Aeronautics and Space Administration*), ainda em 1963, um comitê formado por membros da indústria e do governo criou o padrão ASCI, que consistiu no primeiro padrão universal para codificação de caracteres produzido para computadores e em 1968, o maior supercomputador do seu tempo foi construído pela NASA, o ILLIAC e por último a criação da ARPANET que consisti na primeira rede de computadores totalmente funcional de larga escala. (*Macedo et.al, 2018*).

Nos anos 70 os principais eventos consistiram no surgimento do UNIX, na crescente adição de nós na ARPANET e nos aprimoramentos dos protocolos e das interfaces de conexão, nessa década vários acontecimentos ocorreram, no final de 1971 a ARPANET já possuia dezenove computadores na rede, em 1972 o primeiro programa para enviar mensagens por meio de um correio eletrônico sob a ARPANET desenvolvido por Ray Tomlinson na empresa BBN, nessa década uma

série de avanços onde vale destacar o artigo publicado por Bob Kahn e Vint Cerf “*A Protocol for Packet Network Interconnection*” apresentando o protocolo TCP (*Transmission Control Protocol).* (*Macedo et.al, 2018*).

Nos anos 80 os avanços nas redes de computadores foram crescendo e os computadores pessoais se proliferando, o surgimento da *WEB* e as interconexões de redes, um dos maiores problemas existente nessa epóca consistia na forma como as pessoas identificavam os computadores nas redes, foi onde um pouco depois os pesquisadores JonPostel, Paul Mockapetris e Craig Partridge desenvolveram o serviço DNS (*Domain Name System*) para controlar esse problema Por meio deste serviço, cada endereço IP era associado com um nome, facilitando a interação entre pessoas e os computadores na rede. Em 1984, o DSN foi introduzido na Internet, dando origem aos domínios .gov, .edu, .org, .com e .mil. Em 1985, a Internet possuía dois mil computadores conectados. Ainda nos anos 80, outros pontos bastantes importantes como o surgimento do protocolo SNMP (*Simple Network Management Protocol*) onde permitiu identificar se um dispositivo estava conectado à rede e as condições de operação do mesmo, e para fechar os anos 80 foi criada a WWW(*World Wide Web*) ou WEB por Tim Berners-Lee físico suíço do CERN (*Conseil Européen pourl la Recherche Nucléaire*) gerando um impacto positivo na evolução da internet. (*Macedo et.al, 2018*).

Anos 90, formalmente foi desativada a arpanet, um crescimento absurdo nos últimos anos em relação a rede, onde cresceu de quatro para cerca de de trezentos mil hosts e vários países já se conectavam a internet, e com toda essa evoução começaram a surgir relatos de eventos contra a segurança da informação. Anos 2000, foi conhecido como a bolha da internet, Esse fenômeno ocasionou um crescimento dos valores das ações das novas empresas ligadas ao ramo da tecnologia da informação e comunicação operando com base na Internet, nessa década sérios ataques contra usuários na internet porém em 2017 quatro bilhões cento e cinquenta e sete milhões de pessoas, ou

seja, 54,4% das pessoas no planeta estavam conectadas a internet. (*Macedo et.al, 2018*).

E com o passar dos anos e com essas grandes evoluções foi mais nítida a preocupação com o termo “Segurança” tendo em vista as vulnerabilidades das máquinas conectadas a uma gradiosa rede que é a internet. Segundo a ISO(*International Standardization Organization* – Organização Internacional para Padronização), no contexto da computação, vulnerabilidade refere-se a qualquer fraqueza, ou falha, que possa ser explorada para violar um sistema ou as informações que nele contém, ao conectar o computador a rede o mesmo fica sujeito a vários tipos de ameaças e dentre elas vale destacar:

• Furto de dados e Interceptação de tráfego: corresponde à obtenção de forma não autorizada a informações pessoais (entre outros dados sigilosos), através da interceptação de tráfego da rede não criptografado ou, ainda, através da exploração de vulnerabilidades conhecidas existentes em computador pessoal (seja em um serviço, software aplicativo ou sistema operacional). (*Macedo et.al, 2018*)

• Uso indevido de recursos: um atacante (quem efetua um ataque) obtém acesso a um computador e de posse deste dispositivo pode utilizá-lo de forma maliciosa, obtendo arquivos, enviando spans, gerando ataque a outros computadores e ocultando sua identidade original. (*Macedo et.al, 2018*)

• Varredura: corresponde ao processo de vasculhar uma rede de computadores com o propósito de identificar outros dispositivos que compõe esta rede, suas configurações, serviços, sistema operacional que utilizam, entre outros. A varredura compõe uma parte inicial de um ataque quanto ao mapeamento de uma determinada rede, para que de posse desta informação, possa direcionar alvos de ataques. (*Macedo et.al, 2018*)

• Exploração de vulnerabilidades: consiste em explorar possíveis falhas existentes em softwares aplicativos, plug-ins, serviços ou no próprio sistema operacional instalado. Ao explorar uma vulnerabilidade e

obter acesso ao computador, um atacante pode disparar ataques, coletar dados indevidamente, além de poder propagar códigos maliciosos em geral. Dispositivos de rede como roteadores, também podem ser invadidos, reconfigurados e direcionar usuários a sites fraudulentos. (*Macedo et.al, 2018*)

• Ataque de negação de serviço e de força bruta: na primeira modalidade de ataque o atacante utiliza uma rede de computadores para poder enviar uma grande quantidade de dados para um computador destino, a fim de que o mesmo possa parar ou ser incapaz de continuar respondendo. Já no ataque de força bruta a ideia é automatizar o processo de descobrimento de senhas fracas (softwares podem realizar tal trabalho através de uma wordlist) que podem ter sido utilizadas pelo administrador do sistema (na autenticação), com o propósito de identificá-las e obter acesso. Entre outros ataques [...](*Macedo et.al, 2018*).

Como já foi falado sobre ameças, será abordado um pouco sobre prevenção e como se deve ter uma política de segurança bem estruturada para que esses ataques não venham a acontecer, a palavra política da segurança conforme Macedo *et.al*, (2018), diz que corresponde a um conjunto de regras que especificam o que pode e o que não pode ser feito, geralmente aplicada a uma rede local de computadores (principalmente em uma rede corporativa – ambiente de trabalho), bem como as penalidades as quais estão sujeitos os usuários que dela não cumprem. Algumas políticas de segurança pode ser indispensavéis tanto para rede local ou corporativa e são elas (*Macedo et.al, 2018*):

- definição de cronogramas de backup;
- estabelecimento de regras para o uso de senhas e credenciais de acesso;
- controle de acesso aos espaços físicos;
- definição de diretrizes para o acesso à informação de diferentes profissionais e times, estabelecendo graus de acessibilidade;
- criação de planos de contingência e de gerenciamento de riscos;
- definição das políticas de atualização de softwares

Todas essas políticas mencionadas ajudam a ter menos problemas com segurança e deixam o ambiente mais seguro, também falaremos um pouco sobre os princípios da segurança que são essenciais para qualquer ambiente sendo ele corporativo ou não, eles são definidos como; Confidencialidade, Integridade e Disponibilidade (*Macedo et.al, 2018*).

- Confidencialidade – Como o nome já fala, é tudo aquilo que garanta o sigilo das informações que você tem acesso.
- Integridade – É garantir que as informações não sejam modificadas ou alteradas.
- Disponibilidade – É ter acesso as informações sempre que desejar de forma segura e estruturada. (Docusign, n.d.).

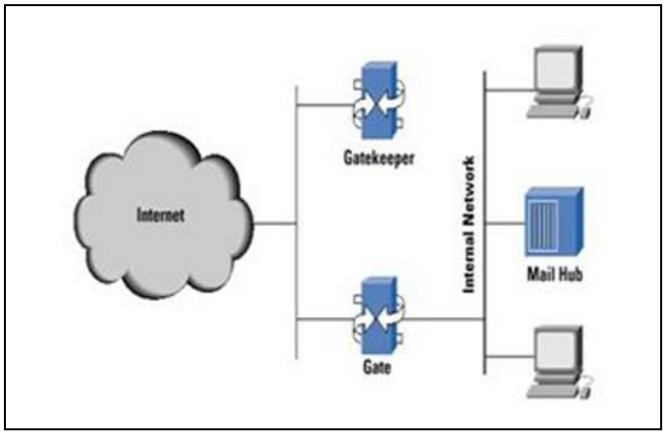
## 4. FIREWALL

O *Firewall* é um termo bastante utilizado no mercado de segurança, é um dos componentes mais lembrados dentro de uma arquitetura de segurança. Começou a ser usado no final da década de 80. Nessa época haviam roteadores que separavam pequenas redes, dessa forma, era bastante conveniente a instalação de aplicações e gerenciamento de recursos nas redes, quando tais aplicações apresentavam algum problema de congestionamento na rede, as demais dos segmentos não eram afetadas. Os primeiros *Firewalls* de fato, apareceram no início dos anos 90, esses trabalhavam a segurança de redes (OSTEC, 2018)

Inicialmente as aplicações não eram complexas, lidando com conjuntos de regras básicos, como: Usuário da rede X pode acessar a rede Y, ou usuário da rede Z não pode acessar a rede Y. Eram ferramentas efetivas, porém bastante limitadas. Já a segunda geração foi um pouco mais desenvolvida, pois usavam filtros de pacotes e aplicativos, os famosos "*proxys".* Além disso, traziam interfaces gráficas para o gerenciamento das regras. Eram conhecidos como "*Bastion Host" (1).* (Erika Hoyer, 2020)

Desenvolvido pelo de *Network Systems* da *Digital Equipament Corporation,* O DEC *Firewall* foi o primeiro de sua geração. Configurado e instalado para uma grande empresa química da costa leste americana, no dia 13 de junho de 1991. Durante meses o Marcus Ranum, colaborador da DEC, criou proxies de segurança e desenvolveu muito do código do *Firewall.* Esse *Firewall* foi criado e nomeado de DEC SEAL. Ele era composto de um elemento externo chamado *Gatekeeper,* de um gateway de filtragem e um dispositivo interno chamado *Mail Hub.* Apresentação do modelo mencionado a seguir, em figura 1(Erika Hoyer, 2013):

**Figura 1** - Representação do DEC SEAL




**Fonte:** GTA – UFR (2013)

Após longas alterações em suas funcionalidades, Check Point lançou seu produto chamado: "*Firewall*-1", em 1994. Introduzindo uma interface amigável para o mundo da segurança na internet. Os equipamentos antes do *Firewall*-1 precisavam de edição de arquivos *ASCII* [(2)] com editores *ASCII*. Então foi introduzido ícones, cores, mouse e um ambiente gráfico X11, para interface de configurações dos administradores, assim seria possível simplificar a instalação e administração do *Firewall*. Por esse motivo a Check Point tornou-se líder de mercado nesse seguimento de segurança com o *Firewall-1* e ocupou em dezembro de 2003 cerca de 48% do Market-share desse segmento. (Erika Hoyer, 2013)

## 4.1 Filtro de Pacotes

Filtros de pacotes são tipicamente formados por um conjunto de regras que descrevem uma determinada condição a ser avaliada e na ocorrência desta, uma ação, também descrita para cada regra, deve ser efetuada. Afirmação feita pelo André Luís Fávero e Raul Fernando Weber [3]. Na maioria dos filtros a verificação acontece conforme o ordenamento das regras, caso tal condição seja satisfatória, as demais regras subsequentes serão ignoradas. Mas se nenhuma regra obtiver suas condições satisfeitas, irá ser aplicado sobre o pacote uma política de segurança default (André Luís Weber, 2005).

Mesmo sendo uma tecnologia muito usada em grande escala e bem estabelecida no mercado, os filtros não realizam qualquer tipo de verificação semântica das regras que o administrador define. Por esse motivo, muitas regras podem ser escritas de forma errônea, o que pode acabar alterando uma política realmente implementada pelo filtro (André Luís Weber, 2005)

### 4.1.1 Filtragem de dados IP

Avaliando as informações no cabeçalho de um pacote toda vez que um chega ao *Firewall,* é dessa forma que é decido ou não se é permitido a sua passagem, assim funcionam os filtros de pacotes (Pedro Meirelles, 2013)

Sendo permitido a passagem do pacote, ele seguirá seu caminho normalmente. Entretanto, nenhum pacote passa por firewall ou roteador sem sofrer algumas modificações. Antes de um pacote seguir seu caminho o roteador ou firewall reduz o valor da TTL *(Time-To-Live)* no cabeçalho em pelo menos 1. Caso o TTL, que o emissor deverá ter configurado como 128, atingir a marca de 0, o pacote será automaticamente descartado, assim será evitado um looping infinito de um pacote no meio. Podem ser criadas regras de filtragem que verificam os seguintes campos de um pacote:

IP de origem: Seria um endereço de IP que o pacote lista como seu emissor.

IP de destino: Endereço de IP para onde o pacote será enviado.

ID de protocolo IP: Um cabeçalho IP pode ser seguido por vários cabeçalhos de protocolos. Cada um dos protocolos tem seu próprio ID de protocolo IP.

Número de portas TCP ou UDP: Número da porta indicando que tipo de serviço o pacote será destinado.

Flag de fragmentação: Pacotes podem ser quebrados em pacotes menores para serem alocados em redes que apenas suportam pacotes pequenos.

Ajuste de opções do IP: Funções opcionais no TCP/IP que podem ser especificadas nesse campo. Essas opções são destinadas apenas para diagnósticos (Pedro Meirelles, 2013).

### 4.2 NAT (*Network Address Translation*)

Conversão de endereço de rede (NAT) foi projetada para conservar o endereço IP. Essa técnica permite que as redes IP privadas que podem usar endereços de IP não registrados, possam se conectar à internet. A NAT funciona em roteadores, que costuma conectar duas redes entre si e converte endereços privados na rede interna em endereços legais, isso tudo acontece antes que os pacotes sejam encaminhados para outra rede. Oura característica desse recurso é que a NAT pode ser configurada para anunciar para o mundo apenas um endereço para toda a rede, acionando segurança adicional ao ocultar o fato de que a rede interna está por trás do endereço, de modo geral, a NAT disponibiliza funções duplas de segurança e conservação de endereços e é aplicada em ambientes de acesso remoto (Cisco, 2014)

Com o surgimento e crescimento das redes privadas com a internet partilhada, surgiu também o problema de como os computadores que pertencem a essa rede privada poderiam receber as respostas aos seus pedidos realizados para fora da sua rede. Tratando-se de uma rede privada, os números de IP interno da rede não podiam ser passados para a internet pois não existem e o computador que recebeu os números de IP não saberia para onde enviar a resposta. A solução para esse problema foi fazer um mapeamento baseado no IP interno e na porta local do computador. Assim, o NAT gera um número de 16 bits, e então esse número é escrito na porta de origem (Thiago Veiga em WordPresss, 2008)

Existem vários programas que permitem compartilhar uma conexão usando NAT, uma delas é o Internet *Conection Sharing do* Windows, porém existem proxys com recursos parecidos, por exemplo o Wingate. A vantagem destes sobre os proxys manuais se dá pelo fato de a conexão ser quase inteiramente transparente. Todos os computadores poderão ser configurados para acessar diretamente a Internet, usando o servidor NAT como gateway, dispensando assim a configuração manual do proxy em cada programa separado (Guia Hardware, 2005).

As vantagens do NAT são geradas por pedidos dos computadores de dentro da rede privada, apenas. Assim, um pacote que chega ao router vindo de fora e que não tenha sido gerado em resposta a um pedido de rede, não irá encontrar nenhuma entrada no NAT e o pacote será descartado automaticamente, não sendo entregue a computador algum da rede. Assim, impossibilitará a entrada de conexões indesejadas e o NAT acabará funcionando como um firewall nada rede (The TCP/IP Guide, 2012)

### 4.3 Proxy de Aplicação

O Proxy é um servidor que irá receber as requisições de um usuário na rede e a passará para frente, alterando o remetente da mensagem com o objetivo de enviar dados de forma anônima ou filtros o conteúdo (CanalTech, 2012)

De forma mais clara, imagine que um usuário (A) é conectado a um servidor proxy (B) e faz uma pesquisa no Google, que em seu funcionamento normal irá utilizar um algoritmo de busca usando o perfil do usuário base. O resultado que será retornado não será direcionado diretamente ao usuário (A), mas sim ao servidor (P) que logo após irá encaminhar para o usuário (U).

Para um bom funcionamento de um Firewall é preciso que haja um bom serviço de Proxy de aplicação, muitas vezes conhecido como *Application Gateway,* pode ser entendido como uma versão elaborada de filtragem dos pacotes. Uma filtragem de pacotes é capaz de verificar dados em níveis mais baixos de um pacote de IP, como por exemplo um endereço de IP ou um número de porta, já o proxy de aplicação é capaz de verificar uma parte de dados de aplicação inteira de um pacote de IP. (Pedro Meirelles, 2013)

Um bom exemplo é um proxy de aplicação FTP [(3)], que é capaz de analisar pacotes de FTP por determinados nomes de arquivos e bloquear os pedidos se for necessário. De forma mais clara, um computador da rede interna mandará um pedido particular para a internet para o firewall, o proxy de aplicação dentro do firewall irá pegar esse pedido, inspeciona o pacote inteiro, de acordo com as regras configuradas pelo admin do firewall, e então segue gerando novamente um pedido para a internet inteira antes mesmo de enviar para o servidor de destino (Pedro Meirelles, 2013).

Um proxy costuma manter duas conexões separadas: A primeira é entre o computador da rede interna com o firewall e a outra é do firewall com o servidor de internet (TecMundo, 2008).

Proxys de aplicação oferecem várias vantagens:

- O Proxy de aplicação pode verificar uma porção inteira da aplicação do pacote. Essa verificação acontece quando a solicitação é enviada e quando o pacote de resposta do servidor de internet volta.

- O Proxy de aplicação compreende o protocolo de aplicação, podendo ciar um registro bem mais detalhado do que foi enviado pelo firewall, pois os registros de filtragens de pacotes apenas sabem das informações do cabeçalho dos pacotes.

- Computadores da rede interna e o servidor de internet nunca terão uma conexão real entre os mesmos. O firewall cria todos os pacotes que são enviados entre eles, assim, ataques e condições ilegais nos pacotes nunca irão alcançar o computador da rede interna.

- Um Proxy de aplicação é capaz de inspecionar tráfegos na rede que usam múltiplas conexões. A filtragem dos pacotes não identifica que conexões separadas da mesma aplicação estão juntas.

Infelizmente, proxies de aplicação possuem desvantagens:

- Proxy por aplicação: Um serviço de proxy de aplicação necessita entender o protocolo de aplicação que será usado. Então, o firewall deve ter um específico proxy de aplicação para cada aplicação. Muitos firewalls dão suporte para várias aplicações, como: FTP e HTTP, mas diferente disso, normalmente o proxy de aplicação não se encaixa.

- Requerimento de configuração de proxy: Em alguns proxys de aplicação, o computador da rede interna deverá saber que ele está conectado ao proxy de aplicação, e não ao servidor de internet. Se o computador da rede interna pode usar o proxy sem nenhuma configuração especial, será chamado de proxy de aplicação transparente (Pedro Meirelles, 2013)

## 5. VULNERABILIDADES

Vulnerabilidade: característica para definir alguma coisa ou alguém que é vulnerável, frágil, delicado. Um termo utilizado para representar a fraqueza de um indivíduo ou de algo (Starti, 2020).

Dentro de Segurança da Informação, as vulnerabilidades são vistas como riscos, brechas que podem ser exploradas por criminosos nas tentativas de ataques cibernéticos. Tendo como finalidade aplicar golpes, roubar informações de uma empresa ou pessoa (Starti, 2020).

Uma série de ataques cibernéticos a empresas e governos no Brasil e exterior tornou público o poder de impacto econômico é o desse tipo de atividade, tanto do ponto de vista privado quanto público (Wagner Aparecido, 2013).

Logo na introdução, o Livro Verde (Brasil, 2010), apresenta a segurança cibernética como o grande desafio do século XXI. Essa ideia expõe uma preocupação do Brasil e seu alinhamento com as tendências internacionais em relação ao espaço na rede. A segurança cibernética é colocada como a característica do novo paradigma mundial, pois a tecnologia em constante desenvolvimento torna-se inseparável de todos os aspectos da sociedade moderna, direta ou indiretamente. Dessa forma, são expostas ainda as principais perspectivas que irão consolidar esse cenário em 2020:

- Revolução de Infraestrutura;

- Mundo sempre conectado;

- Explosão de dados;

Vulnerabilidades fazem parte do ponto inicial na estratégia de um ataque online, cibernético. Um criminoso ao realizar seu ataque, fará uso de quatro pilares: objetivo, estratégia, inteligência e o alvo. O objetivo será roubar dados e/ou informações (Alctel, 2020).

Antes de tratar das principais causas de vulnerabilidade é preciso entender o que compromete a segurança de rede e também entender a diferença entre vulnerabilidade, ameaça e riscos:

- Vulnerabilidades: geralmente apresentam falhas no sistema. Independentemente da origem da falha, se comprometer o sistema de dados ou a infraestrutura de TI é uma vulnerabilidade;

- Ameaça: se entende como uma possibilidade de um agente, que pode ser interno ou externo, explorar propositalmente ou acidentalmente as falhas que um sistema pode apresentar, entendendo-se que ameaças externas são mais difíceis de controlar;

- Riscos: São basicamente consequências pelas quais a empresa estará sujeita a passar, caso falhas sejam exploradas por ameaças (Alctel, 2020).

Existem algumas fontes de vulnerabilidades e as principais delas são: erro de desenvolvimento, tanto no desenvolvimento de um banco de dados quanto no planejamento da estrutura de TI. Má gestão de Software, isso inclui barreiras de segurança como firewalls, antivírus e AntiSpam [(4)], mal configuradas, assim como a falta de Updates nesses softwares. Falha humana, uma das causas mais abrangentes de todas, podendo ir de uma simples execução indevida de programa malicioso até a exclusão de arquivos importantes. Falta de um plano de recuperação, essa questão seria uma espécie de “bote salva-vidas” das empresas para muitos casos não previstos virtualmente, como o roubo de equipamentos e comprometimento do fornecimento de energia elétrica e internet.

---

*[(4)] AntiSpam: Para impedir não só mensagens não solicitadas, mas também prevenir alguns danos como vírus, foi desenvolvido ferramentas de AntiSpam. Um recurso que serve para filtrar os E-mails e evitar que os usuários estejam expostos aos riscos ligados a utilização do recurso < OSTEC, Segurança digital de resultados>.*

## 5.1 ATAQUES EM REDE

Visando diferentes alvos e usando variadas técnicas muitos ataques costumam acontecer na internet com diversos objetivos. Qualquer dispositivo pode ser alvo de um ataque, basta estar conectado e que seja acessível via internet. E qualquer computador que tenha acesso à internet também poderá participar de um ataque (CERT.BR 2017)

Existem vários motivos que ocasionam os atacantes propagarem os ataques na internet. E estão entre uma simples diversão até a realização de ações criminosas (CERT. 2017):

- Demonstração de poder: tem a finalidade de mostrar a uma empresa ou grupo que a mesma pode ser invadida ou ter seus serviços suspensos, em seguida, o atacante poderá usar da chantagem para que o ataque não aconteça novamente.

- Prestígio: Vangloriar-se, diante de outros atacantes, por ter conseguido invadir um sistema ou empresa. Disputar com outros atacantes quem consegue o maior número de ataques.

- Motivações Financeiras: Para a aplicação de golpes, alguns atacantes tentam coletar e utilizar informações confidenciais.

- Motivações ideológicas: Atacantes também divulgam mensagens de apoio ou contrárias a uma determinada ideologia, em muitos casos bloqueiam ou forçam o divulgamento de conteúdos sensíveis ou plataformas que contrariam de suas opiniões.

- Motivos comerciais: Atacam computadores ou sites de empresas concorrentes, tentando impedir o acesso dos clientes e comprometer reputação de uma determinada empresa (CERT. 2017).

### 5.1.1 NEGAÇÃO DE SERVIÇO

Um exemplo bem conhecido é o DoS ou DDoS. Um ataque de negação de serviço. Técnica que um atacante irá utilizar um computador para remover do ar a operação de um serviço, um computador ou até mesmo uma rede que está conectada à internet, esse é o DoS. Já o DDoS será quando de forma coordenada e distribuída e ataque acontecer. Assim, um conjunto de computadores será utilizado no ataque, recebesse o nome de negação de serviço distribuído (CERT.BR 2017).

O principal objetivo desses ataques não são invadir ou roubar informações, mas de usar recursos e promover uma instabilidade ao sistema atacado. Todos os usuários que dependem do serviço são prejudicados com a indisponibilidade do serviço e não conseguem realizar suas operações. Em muitos casos que já foram registrados anteriormente, os alvos ficaram impossibilitados de prover seus serviços durante o tempo em que estavam sendo atacados, mas depois, voltaram a funcionar normalmente, sem vazamento de informações ou comprometimento dos sistemas (CERT.BR 2017).

São diversos os meios para realização dos ataques, como:

- A partir do envio de uma grande quantidade de requisições para um serviço, assim, consumindo todos os recursos necessários para seu funcionamento, e isso impede que novas requisições sejam atendidas.

- Gerando um grande tráfego de dados para a rede, ocupando toda ou quase toda banda da rede disponível, fazendo com que seja impossível o acesso de serviços ou computadores da rede.

- A partir da exploração das vulnerabilidades que existem em programas, fazendo com que um determinado serviço fique indisponível (CERT.BR 2017).

## 5.2 EVITANDO VULNERABILIDADES NA REDE

Nenhuma empresa ou usuário irá desejar ter seus dados capturados de informa ilegal por conta de vulnerabilidades na rede. Porém, ataques são uma realidade bem comum no meio cibernético e que afetam grupos e empresas de forma ainda mais grave, pois além de prejuízos como produtividade e lucros, existe também o risco de encarar as consequências de quebras dos contratos (HDStore, 2018).

No ano de 2018, uma empresa chamada “Nayana”, representante de hospedagem que fica situada na Coréia do Sul, foi vítima de ataque. Nesse crime, mais de 150 servidores foram invadidos por conta de falhas na segurança. Os atacantes acessaram dados dos clientes e ainda tiveram controle dos equipamentos. Por conta disso, aproximadamente 3,4 mil usuários sofreram, em sua maioria, companhias de pequeno e médio porte (HDStore, 2018).

A seguir, será possível observar alguns protocolos para melhorar a segurança na rede e tentar evitar o roube de dados (HDStore, 2018):

- Ativação de senhas de acessos: Uma implementação de senhas internas será sempre uma medida importante e necessária para rastrear melhor os possíveis acessos ou roubos de senhas dentro de um ambiente empresarial. Sabendo exatamente quem acessou setores ou arquivos, as informações ficarão bem mais protegidas, assegurando respaldos em casos de acusações indevidas de roubo de dados.

- Realização efetiva de backups diários: Com a realização de backups dos arquivos, será menos danoso para a empresa caso aconteça erros das plataformas ou ataques ao sistema caucionados por ransomware, por exemplo. Pois os dados estarão guardados em outro local, e poderão ser recuperados assim que necessário.

- Automatização de bloqueios de conteúdo na rede: Diversos sites possuem conteúdo malicioso, são criados com intenção de espalhar vírus ou roubar dados para uso de cibercriminosos. Para que tais prejuízos possam ser evitados, é preciso instalar programas de segurança na rede, como um bom antivírus. Além disso, pode ser

mencionado também o uso e manutenção de um bom Firewall, para que o filtro de conteúdo e tráfego seja monitorado e tratado constantemente.

- Atualizações dos sistemas operacionais: Toda vez que sistemas operacionais são atualizados, várias falhas da versão anterior são corrigidas, por isso, a atualização efetiva dos sistemas operacionais e programas dos equipamentos é sempre tarefa fundamental para qualquer empresa e usuário (HDStore, 2018).

Além dessas formas de proteção, não pode ser esquecida a “Engenharia Social”. É basicamente um termo usado para descrever um método de ataque que faz uso da persuasão. Uma técnica que faz uso da ingenuidade ou confiança de um usuário, assim visa obter informações que podem ser utilizadas para ter um acesso não autorizado aos sistemas e informações dos grupos empresariais (Terra, 2020).

## 6. Pentest

Vem da abreviação de *Penetration Test* (Literal, Teste de Penetração) mas também é conhecido como Teste de Intrusão, por fazer a detecção minuciosa com técnicas utilizadas por hackers éticos. Esses testes de intrusão visam encontrar possíveis vulnerabilidades em um sistema, servidor ou em uma estrutura de rede. Além disso, o PENtest usa ferramentas específicas para realizar a intrusão que mostram quais dados e informações corporativas podem ser roubadas por meio de tal ação (OSTEC, 2020).

De forma geral, é uma grande quantidade de testes metodológicos que tem o objetivo de mapear, descobrir e expor todas as possíveis vulnerabilidades de uma rede. É importante destacar que o objetivo do PENtest não é obter acesso não autorizado a um sistema ou servidores, tem a finalidade de a partir das falhas encontradas, aplicar os devidos mecanismos de segurança para aquele sistema monitorado.

A técnica de Pentest não é definida apenas como um scaneamento das portas ou simples vulnerabilidades, vai bem além disso. Faz-se uso de software e ferramentas, conhecidas como: *pentest tools,* para identificar as vulnerabilidades existentes, tentando entender que tipo de informação pode ser capturada com aquela falha encontrada (Profissional Hacker, 2019).

Os profissionais que atuam nessa área são chamados de “PenTester”, também pode ser chamado de “Auditor PenTester” ou “*Ethical Hacker”.* É um profissional que detém um elevado nível de conhecimento em sistemas operacionais e redes de computadores e em decorrência disso, utiliza técnicas, ferramentas e programas para realizar as suas análises. É bastante comum que esses profissionais possuam um certificado internacional em Ethical Hacking. Certificação essa que dá credibilidade ao profissional e comprova que de fato, o mesmo atua de maneira profissional e dentro de princípios éticos (4infra, 2020).

## 6.1 Tipos de PenTest

Existem diversos tipos e classificações para as análises do PENtest, irá depender muito da fonte da informação e da empresa que presta o serviço. Esses são alguns tipos e subclassificações que citam os seguintes termos (OSTEC, 2020):

- Quantidade de informações que o grupo de PenTester possui antes de dar início aos testes.

- Origem do teste, interna ou externa, que se dá pela simulação do ataque de fora da rede ou internamente.

- A divulgação ou não, das realizações dos testes pelos funcionários internos da empresa.

Existem algumas formas de realização dos testes de intrusão, cada um deles terá uma eficiência diferenciada. Destacam-se a White Box, Black Box e a Grey Box (OSTEC, 2020):

White Box: Conhecido como o teste mais completo, pois inicia por uma análise integral, que verifica e avalia toda a infraestrutura de uma rede. Tudo é possível pois ao iniciar esse teste, o hacker ético irá possuir conhecimento de todas as informações essenciais da empresa.

Black Box: Esse é um pouco diferente do primeiro mencionado, funcionando praticamente às cegas. Pois o hacker não irá possuir grande parte das informações disponíveis sobre a empresa. É o mais próximo de seguir os padrões de ataques externos.

Grey Box: É definido como a mistura dos dois tipos mencionados anteriormente. Esse tipo de teste já obtém certas informações para realizar a intrusão. Porém, a quantidade de informações é pequena e não pode ser comparada a quantidade de dados que são disponibilizados em um teste de White Box.

## 6.2 Benefícios do PenTest

Podem ser citados alguns benefícios, sendo os principais:

- Ajudar empresas a testarem a capacidade e eficiência de sua segurança em rede.

- Encontrar fragilidades dentro dos sistemas de segurança antes que cibercriminosos as encontre.

- Permite que muitas empresas adotem novas posturas em relação à segurança da informação, dar suporte e acreditar nos possíveis investimentos na área.

- Garantir e cuidar da reputação de um grupo empresarial, os testes mostram o comprometimento em assegurar a continuidade do negócio e mantêm uma relação justa e efetiva com a segurança na rede (OSTEC, 2020).

## 7. Conclusões

Com o objetivo de melhorar o entendimento, o projeto mencionou alguns pontos da segurança em rede e é entendido que a aplicação de mecanismos e ferramentas protetoras dentro das redes de computadores se faz necessário. A aplicação de um firewall irá melhorar a segurança da rede com suas configurações de tráfegos e análise, bloqueios e restrições. Com políticas de segurança é possível entender e desenvolver diariamente atividades que auxiliam a existência das vulnerabilidades. Com técnicas de estudo e monitoramento como o PENtest é possível investir ainda mais para manter a segurança dos grupos empresarias.

O PENtest é um tema relativamente novo no mercado, e mais acima foi possível falar sobre a técnica e de algumas características. Deve ser lembrado a importância do tema e possível assunto com conteúdo satisfatório para um projeto futuro, dado a importância do mesmo para a análise de vulnerabilidades dentro dos sistemas de redes e computadores.

Em um mundo na qual os negócios acreditam cada vez mais na internet e em suas redes de computadores, empresas podem confiar cada vez mais nos processos de segurança da rede e dos sistemas, visto que diariamente vem sendo comprovada a eficiência da segurança da informação, as empresas podem enfrentar ameaças de erros, invasões e infecções por vírus, por isso se faz tão importante proteger a rede.

Um outro motivo para investir na segurança de rede são os patrimônios físicos de uma empresa, podendo evitar danos físicos causados por malwares e vírus.

Por fim, garantir uma boa infraestrutura de segurança na rede e nos sistemas, garante e mostra o comprometimento do negócio para com seus clientes internos e externos. Assim, é garantido a longevidade na vida das empresas e gastos indesejáveis com processos judiciais por motivos de vazamento dos dados de usuários

## Referências


Cristina D. A. Ciferri, Ricardo Ciferri, Sônia França, Firewall – Brasil, Disponível em < https://www.cin.ufpe.br/~flash/resultados/eventos/workshopais972/firewall/artigo.html > Acessado em 18/05/2020.

Segurança em rede IP – Alexandre Fernandez Marques. Brasil, Abril 2001 Disponível em: < http://servicosderedes.com.br/wpcontent/uploads/2015/04/segurança_redes_ip.pdf > Acessado em 20/05/2020.

Mateus Micael Coutinho, Robson Nunes dos Santos, Vitor Henrique, Eliane Cristina, Eliney Sabino, Narumi Abe – Estudo de caso: Principais pilares da segurança da informação nas organizações. Brasil, 2017. Disponível em: <http://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf > Acessado em 21/05/2020

Vulnerabilidades em rede – CERT. Brasil, 2016. Disponível em: < https://cartilha.cert.br/ataques/ > Acessado em 18/05/2020

Vulnerabilidades em rede – HDStore. Brasil, 2018. Blog.

< https://blog.hdstore.com.br/o-que-fazer-para-evitar-vulnerabilidade-na-rede/ > Acessado em 25/05/2020.

Júlio César, Segurança na rede – InfoSec. Brasil, 2019. Disponível em: < https://www.infosec.com.br/seguranca-de-rede/ > Acessado em 19/05/2020.

Segurança da Informação, conceitos e mecanismos. – Oficina Net. Brasil, 2008. Disponível em: < https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos > Acessado em 01/06/2020.

André Redin Cella, Apresentação de um firewall em ambiente público com a ferramenta Sophos –. TCC, 2018. Disponível em: < http://repositorio.faculdadeam.edu.br/xmlui/bitstream/handle/123456789/315/TCC_SI_ANDRÉ_REDIN_CELLA_AMF_2018.pdf?sequence=1&isAllowed=y > Acessado em 02/06/2020.

José Luiz Zem, O Impacto do Serviço de NAT e Firewall no atendimento de requições Web. Congresso de pesquisa. UNIMEP, 2011. Disponível em: < https://www.cisco.com/c/pt_br/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html > Acessado em 05/06/2020.

Daniel Moreno , PenTest em redes sem Fio. Brasil, 2016. Disponível em:
<https://books.google.com.br/books?hl=pt-BR&lr=&id=tcm_CwAAQBAJ&oi=fnd&pg=PA16&dq=Pentest&ots=c1iR1QRekK&sig=Martyys303nhEK4wcCIVygHQPml#v=onepage&q&f=false > Acessado em 10/06/2020.