FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA

Curso Técnico em Informática

Parecer SEC/CEED 007/2016

Rua Dr. Flores 396 - Centro - POA/RS

BRENDA ANDERSEN DE LIMA

SEGURANÇA NO GNU/LINUX

Medidas básicas para obtê-la

Porto Alegre

2020

BRENDA ANDERSEN DE LIMA1

SEGURANÇA NO GNU/LINUX

Medidas básicas para obtê-la

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Técnico em Informática da Faculdade de Tecnologia Alcides Maya.

Orientador: Prof. Me. João Padilha Moreira2

Porto Alegre

2020

1 Aluno do curso técnico em informática – e-mail: brenda_andersen@protonmail.com

2 Professor orientador João Padilha Moreira – e-mail: joao_moreira@alcidesmaya.edu.br

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
FTP	File Transfer Protocol
GNU	GNU's Not Unix
NBR	Normas Brasileiras de Regulação
RCP	Remote copy
SSH	Secure Shell
SO	Sistema Operacional

SUMÁRIO

RESUMO

A segurança da informação torna-se essencial a medida que o valor da informação aumenta. Tal importância existe tanto no meio profissional quanto no pessoal e é independente do sistema operacional utilizado. Os riscos são grandes e vão além da possibilidade do roubo dessas informações. A partir desses fatos, serão apresentadas alternativas de como realizar a aplicação introdutória da segurança no sistema operacional GNU/Linux. Com o intuito de auxiliar um iniciante na área de segurança a proteger suas informações e/ou a proteger a utilização do seu computador a fim de evitar problemas futuros. Esta é uma pesquisa aplicada, optou-se pela utilização da pesquisa documental e bibliográfica. Além de uma abordagem qualitativa a fim de obter os resultados. Por sua vez, esses são compostos por uma breve exposição de alguns softwares de segurança, tais como antivírus, antirootkits, firewall, e ferramenta de backup, além da instalação desses e de dicas para evitar a interferência do fator humano na efetivação da segurança. Concluiu-se que tendo cuidados com a engenharia social e instalando softwares de segurança confiáveis, pode-se obter a proteção básica para o seu sistema. Sendo assim, como o trabalho é puramente introdutório, deve-se partir dele para um futuro aprofundamento na área, como conhecer outros softwares e/ou hardwares de segurança, assim como entender a fundo os conceitos a respeito da segurança da informação, detalhes sobre cibersegurança e assim por diante.

Palavras-Chave: Segurança da informação; Segurança em TI; GNU/Linux.

1. INTRODUÇÃO

O mundo está conectado. O que precisamos agora é garantir que exista segurança nessa conexão. A partir da Red Hat (2011), tomar medidas apropriadas antes de se conectar a uma rede não confiável, como a Internet, é um meio efetivo de impedir tentativas de intrusão. Ainda de acordo com essa fonte, notamos o motivo do surgimento da necessidade da proteção das informações: a segurança da informação tem evoluído ao longo dos anos devido à crescente dependência em redes públicas para não expor informações pessoais, financeiras e outras informações restritas.

Pode-se ver, que tais medidas são importantes, visto que os ataques cibernéticos (CAVALCANTE, 2013) “tem tido um crescimento exponencial, seja pelo aumento do número de usuários da rede, pelas falhas de segurança desta ou por inabilidade ou negligência no seu uso”.

Sendo assim, notamos que a segurança é importante, mas também há a necessidade dessa no sistema operacional GNU/Linux, pois como disse Orloff (2008) “é muito pouco provável que um sistema GNU/Linux configurado por um novato completo seja mais seguro do que um sistema Windows configurado por um especialista altamente qualificado.”

1.1 Definição do Tema ou Problema

Como um estudante que está iniciando suas pesquisas sobre segurança deve proteger as suas informações no sistema operacional GNU/Linux?

Proteger nossas informações é algo fundamental. Segundo a Red Hat (2011), a necessidade da segurança da informação é decorrente de vários fatores, tais como os casos Mitnick e Vladimir Levin, os quais causaram grandes mudanças na forma como as organizações lidavam com a informação, incluindo sua transmissão e exposição. É dito ainda que, a partir da expansão da internet, necessitou-se aprimorar cada vez mais a proteção da informação. Por isso e pelo fato de que todo SO é vulnerável a falhas, apesar de “existirem

poucos vírus para GNU/Linux em relação ao Windows“ (SANTOS, 2016), esse tema é de suma importância.

1.2 Delimitações do Trabalho

O intuito da pesquisa é tanto orientar estudantes que pretendem aplicar segurança no seu ambiente GNU/Linux pela primeira vez quanto mostrar sua importância àqueles que negligenciam a mesma. Sendo assim, esse tema será abordado de forma puramente introdutória, visto o quão extensa é a área da segurança da informação e suas variadas aplicações no GNU/Linux, as quais mudam com maior agilidade ao decorrer do tempo.

1.3 Objetivos

Os objetivos dividem-se em geral e específicos.

1.3.1 Objetivo Geral

Reconhecer as alternativas básicas de segurança no sistema operacional GNU/Linux a fim de propor a compreensão introdutória de segurança para conter as ameaças à informação que julgamos valorosa.

1.3.2 Objetivos Específicos

1. Auxiliar no estudo introdutório de um estudante a respeito de segurança de informação;
2. Identificar as principais ameaças à informação;
3. Compreender o quão importante é a proteção da informação;

1.4 Justificativa

Proteger os nossos dados é e será essencial. Visto que, de acordo com Marciano e Lima-Marques (2006) […] este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes [...].

Com isso, pode-se afirmar que essa importância tende a aumentar mais ainda. Consequentemente, além da imensa satisfação que é aprender sobre segurança da informação, auxiliar outros iniciantes na área da segurança de forma prática é a base para evitar problemas com essa e possibilitar um futuro empenho por parte do estudante nesse ramo. Sendo assim, esse é o tema escolhido para o trabalho de conclusão de curso.

2. METODOLOGIA

Este trabalho segue um enfoque metodológico de natureza qualitativa, o qual (RICHARDSON, 1999) se caracteriza por empregar a quantificação, tanto nas modalidades de coleta de informação, quanto no tratamento dos dados, mediante procedimentos estatísticos.

A fim de atender os objetivos dessa pesquisa, optou-se pela pequisa documental, essa, segundo Aires (2015, p. 46), tem como característica a redução de dados que ocorre constantemente ao longo de toda a investigação, sendo que estes dados podem ser reduzidos e transformados, quantitativa ou qualitativamente, de forma diferente. Para complementar esse tipo de pesquisa, recorreu-se pela pesquisa bibliografia, a qual segundo Gil (2002, p. 44), “ […] é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos”, visto que (TUMELERO, 2019) a pesquisa documental tem objetivos específicos e pode ser um rico complemento à pesquisa bibliográfica.

A coleta dos dados foi realizada principalmente a partir das informações propostas pelos autores Jeffrey Orloff, a comunidade do viva o linux, Marcos A. Simplício e o Guia de Segurança da Red Hat Enterprise Linux. Além do livro segurança dos sistemas de informação (SILVA et al., 2003), que contribuiu para esse trabalho.

3. REFERENCIAL TEÓRICO

3.1 Segurança da informação

Antes de falar sobre a aplicação da segurança no sistema operacional GNU/Linux, é preciso explicar ideias básicas sobre a segurança da informação, a qual será feita com o intuito de mostrar a importância da proteção da informação e o que seria essa.

Logo, fica a questão: afinal, o que é segurança da informação? A priori, a segurança da informação é:

> uma disciplina composta por medidas administrativas, tecnológicas e físicas adotadas com o intuito de preservar os princípios da informação que é considerada importante para um indivíduo ou uma organização, durante todo seu ciclo de vida: criação, manipulação, armazenamento, transporte e descarte (MARCONDES, 2016).

Também pode ser definida como “uma área do conhecimento dedicada à proteção da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade” (SÊMOLA, 2003 apud CARMO, 2013).

Notamos que a segurança da informação é basicamente a condição para a existência da própria informação, mas o que seria a informação? De acordo com a norma NBR ISO/IEC 17799 (Associação Brasileira de Normas Técnicas, 2005, p. 9), “é um ativo que, como qualquer outro ativo importante é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegido.”

A partir disso, é importante frisar que a principal preocupação da segurança da informação “é proteger as informações da empresa contra acessos não autorizados de qualquer tipo” (CAMARGO, 2017).

3.1.1 Política de segurança de TI

A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a

autenticidade e o não repúdio3 – garante que a pessoa não negue ter assinado ou criado a informação, ou seja, permite provar quem fez o quê, quando e onde. Essas medidas de segurança podem ser classificadas, em função da maneira como abordam as ameaças, em duas grandes categorias: prevenção e proteção (SILVA et al., 2003).

Figura 01 – Componentes da Segurança da Informação

Fonte: Manuel (2008).4

Segundo a norma NBR ISO/IEC 17799, o objetivo geral da segurança da informação é:

> a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (Associação Brasileira de Normas Técnicas, 2005, p. 9)

Em contraponto, a partir da Alerta Security (2018) a segurança em TI é focada em manter a segurança dos sistemas operacionais e da infraestrutura de TI da empresa. Dentro desse raciocínio, os três pilares da segurança em TI são:

- **Confidencialidade:** garantia de que qualquer informação armazenada em um sistema de computação ou transmitida via rede, seja revelada somente a usuários autorizados.

3 Seu sinônimo é irretratabilidade, em algumas fontes esse aparece como parte dos pilares da segurança da informação.

4 Disponível em: http://b.link/commons. Acesso em: 14 maio 2020.

- **Integridade:** capacidade de verificar a consistência da informação contida nos dados impedindo que seja alterada de forma imperceptível.
- **Disponibilidade:** garantia de que usuários legítimos não sejam impedidos indevidamente de acessar as informações e os recursos do sistema. É um serviço essencialmente extra criptográfico e o mais arquitetural dentre os serviços básicos da segurança.

Referenciados como CID, são esses os principais objetivos da segurança em TI. Há autores que adicionam outros pilares, – tais como autenticidade, conformidade e irretratabilidade – mas esses são considerados os principais. Sendo assim, a preservação desses atributos é o dever de todas as organizações, visto que, sem a confidencialidade, a integridade e a disponibilidade da informação, a mesma perderá a sua relevância, pois de acordo com Mitnick e Simon (2003, p. 31): assim como as peças de um quebra-cabeça, cada informação parece irrelevante sozinha. Porém, quando as peças são juntadas, uma figura aparece.

3.1.2 A importância da segurança

Ao contrário da crença popular, todo sistema é vulnerável a falhas de segurança (CAVALIERI, [201-?] apud SANTOS, 2016). Falhas essas que aumentam cada vez mais devido ao gigantesco avanço tecnológico e, consequentemente, o fato de que tudo está imerso na rede. Por isso, notamos que há dois cenários, o pré-internet e o pós-internet. No primeiro existem as redes privadas, soluções proprietárias e recursos individualizados (acesso controlado, mas custo elevado) com poucos computadores (SIMPLÍCIO, 2018). No segundo existe, a partir de Simplício (2018), “o compartilhamento de recursos (economia de escala) e adoção de padrões abertos de comunicação”. Com isso, o sigilo das informações tornou-se indispensável em todos os lugares, principalmente em ambientes profissionais, os quais lidam diariamente com as informações pessoais dos clientes e funcionários.

3.1.3 As ameaças à segurança

Com base no senso comum, as principais ameaças à segurança são os malwares. Apesar dessa não ser a principal – fato que será explicado adiante – o que seria um malware? De acordo com Alecrim (2017) “uma combinação das palavras malicious e software que significa programa malicioso”. Portanto, malware é a forma como nos referimos a um software malicioso, visto que ele “pode ser dividido em vários grupos, como: um vírus, um worm, um spyware, cavalos de troia, rootkits e assim por diante” (ALECRIM, 2017). Sendo assim, precisamos fazer uma observação importante: todo vírus é um malware, mas nem todo malware é vírus.

A fim de demonstrar a importância dita na seção anterior, alguns exemplos de ameaças mais comuns à segurança:

- Rootkit: a partir da Kaspersky (2013), o rootkit age a fim de esconder as atividades de um cracker das ferramentas de monitoramento embutidas no SO e dos sensores de antivírus. Esses são utilizados cada vez mais como forma de ocultar a atividade de cavalos de Troia.
- DdoS: pertencente a categoria de origem de ataque “zombies”, são sistemas informáticos infectados com programas específicos, de controle remoto, que são utilizados por terceiros para realizar ataques coordenados contra um alvo; o exemplo mais conhecido são os DDoS, ou ataques distribuídos de negação de serviços, em que grandes números de sistemas atacam simultaneamente um alvo com o objetivo de estrangular a sua ligação à Internet (SILVA et al., 2003).
- Spyware: de acordo com Caldas (2018), esse malware tem como objetivo obter informação confidencial através da internet para propósitos maliciosos. Essas informações voltam para o remetente através de diversos canais, utilizando protocolos comuns da rede, como HTTP, FTP, E-mail ou IRC. Com as informações em mãos, o criminoso pode até mesmo se passar pela pessoa para cometer crimes e obter outras informações.

- Phishing: é caracterizado por tentativas de adquirir informações sigilosas, tais como senhas e números de cartão de crédito, através da engenharia social: fingindo ser uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial, como um correio ou uma mensagem instantânea (POZZEBOM, 2015).

Então, apesar dos poucos exemplos, é notório que os riscos são grandes. Mas ainda precisamos comentar sobre outra principal ameaça: o fator humano. A utilização da engenharia social é a melhor forma encontrada pelos crackers5 para obter informações confidenciais. Esses podem obter tais informações simplesmente conversando com o seu "alvo" ou através das redes sociais desse e dos seus familiares. Prestes (2018) apresenta medidas para diminuir os riscos da interferência desse fator nas empresas, são elas: controlar todos os canais de transmissão de informações, analisar o tráfego e orientar os funcionários sobre as regras de segurança da informação. Mitnick e Simon ainda aconselham:

> Todo sistema externo de computadores que é usado para a conexão com a rede corporativa deve ter software antivírus, software que o proteja do Cavalo de Tróia e um firewall pessoal (hardware ou software). Os arquivos de definições do antivírus ou do Cavalo de Tróia precisam ser atualizados pelo menos uma vez por semana. (2003, p. 260)

Porém, como devemos lidar com o fator humano fora das empresas? Essa questão será abordada novamente na próxima seção.

3.1.3.1 O fator humano

Serão descritas várias iniciativas para combater os temíveis malwares e para instaurar a segurança básica no seu sistema. Porém, nada disso irá adianta se não for levado em consideração a principal "aliada" dos crackers: a engenharia social6. O fator humano, como dito em uma seção acima, é o

---

5 São hackers mal intencionados (CARMO, 2013).

6 É uma ciência que estuda o comportamento humano para identificar métodos que induzam determinadas pessoas, consideradas alvos, a compartilharem informações sigilosas, sejam elas de cunho pessoal ou profissional (NASCIMENTO, 2018).

principal meio utilizado pelos crackers para obter informações sigilosas. De acordo com Zanichelli e Martimiano:

> Apenas a combinação de um antivírus com um firewall não garante a proteção de um ambiente computacional, é preciso muito mais. É preciso principalmente treinar e conscientizar as pessoas [...]. (2010)

A fim de deixar claro a importância desse problema, algumas táticas utilizadas por engenheiros sociais de acordo com Nascimento (2018):

- Pessoalmente: é considerada uma abordagem pouco comum, visto a atuação necessária pelo engenheiro – como fingir ser um conhecido ou inventar um personagem – para persuadir a vítima
- Telefone: é considerada uma abordagem difundida entre os engenheiros sociais. Esses normalmente simulam uma empresa de telefonia, fingindo precisar das informações pessoais da vítima para a atualizar seu cadastro.
- Observação: nesse tipo de tática, o engenheiro social aproveita um dado momento onde as vítimas estão falando sobre assuntos de cunho pessoal ou profissional a fim de obter informações sigilosas dessas.
- Lixo: pode-se obter diversas informações confidenciais a partir do lixo de uma pessoa ou de uma empresa. Esses podem ser números de telefones, endereços, nomes, datas e até mesmo senhas das vítimas.
- Internet: esse método pode ter sucesso de várias formas: através de e-mails falsos, chats e mensageiros eletrônicos (através destes é muito fácil o engenheiro social se passar por outra pessoa), spywares e, por último, através das redes sociais. O engenheiro social pode conseguir diversas informações sobre alguém a partir da rede social da pessoa através de postagens da vítima ou informações do perfil dessa.

A partir de Sêmola:

> Muitas pessoas pensam que segurança da informação se resume à compra de equipamentos e sistemas caros, como firewalls, sistemas de detecção de intrusos ou antivírus. [...] Mas nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconsequente. (2003 p. 9)

Sendo assim, muitas vezes, a perda da informação é relativa ao fator humano, ou seja, não adianta ter um antivírus caro, um firewall bem configurado, informações salvas devidamente e assim por diante se você, por exemplo, guardar as suas senhas escritas em um papel ao lado do seu computador.

4. DESCRIÇÃO DA SOLUÇÃO

4.1 Protegendo o Sistema Operacional

Antes de apresentarmos softwares de segurança, vejamos os princípios gerais da segurança da informação, os quais fornecem uma visão de boas práticas de segurança a partir da Red Hat (2011):

- não utilize softwares antigos. Procure versões recentes de navegadores, editores de texto, sistemas operacionais e assim por diante.
- minimize a quantidade de software instalado e serviços de execução.
- se possível, execute cada serviço de rede em um sistema separado para minimizar o risco de um serviço comprometido sendo utilizado para comprometer outros serviços.
- reveja o sistema e logs de aplicativos diariamente. Por padrão, os logs de sistema relevante a segurança são gravados em /var/log/secure e /var/log/audit/audit.log. Nota: o envio de logs ao servidor de log dedicado ajuda a prevenir atacantes de modificar com facilidade logs locais para evitar a detecção.
- nunca autentique-se como usuário root, a menos que absolutamente necessário. Recomenda-se que os administradores usem o sudo para executar comandos como root quando requerido. Os usuários capazes de executar o sudo são especificados em /etc/sudoers. Use o utilitário visudo para editar o /etc/sudoers.

4.1.1 Proteção contra Malware

Malwares são programas desenvolvidos com o intuito de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações (CALDAS, 2016). A partir desse conceito importante, vejamos uma observação que Orloff destaca acerca desse assunto:

> Para o malware espalhar-se entre sistemas e para causar danos, o programa ou arquivo precisa ser executado. O GNU/Linux foi projetado de forma que os usuários não estejam executando sob a conta root (administrador); portanto, os programas e arquivos não têm a capacidade de executarem sem permissão explícita. Sem a habilidade de executar programa neste estado de login, o malware não consegue instalar-se ou propagar-se através de um sistema GNU/Linux devido às permissões do usuário. O recurso de segurança de permissões do usuário está integrado no GNU/Linux e é uma ferramentas mais efetivas contra a propagação do malware. (2008)

É notável, pois, que embora alguns aspectos do malware sejam irrelevantes para o desktop GNU/Linux, existem outros motivos pelos quais precisamos nos preocupar com ele. Sendo assim, é necessário executar varreduras ativamente a fim de verificar se há algum malware.

Após esse conselho, vejamos algumas dicas básicas para proteger nossas informações. Primordialmente, é necessário garantir a frequente atualização do seu SO.

4.1.1.1 Antivírus

Certamente o melhor antivírus é o usuário. Não obstante, proteção nunca é demais desde que não seja exagerada – um exemplo de exagero perigoso é o uso de mais de um antivírus, ação que gera conflito entre os dois e, consequentemente, problemas ao usuário. Sendo assim, como exemplo de antivírus, será utilizado o ClamAV. Esse é um mecanismo antivírus de código aberto para detecção de Trojans, malwares e outras ameaças (BRITO, [2019?]).

Características do ClamAV: está em constante desenvolvimento; Scanner de interface de linha de comando; digitalização por e-mail; suporta uma variedade de arquivos, como arquivos PDF, Office e zip (ANDERSON, 2019). Para instalá-lo através de linha de comando (BRITO, [2019?]):

Ubuntu e derivados:

```
$ sudo apt-get install clamav-daemon
```

Red Hat e derivados:

```
$ sudo yum install clamav
```

CentOS e derivados:

```
$ sudo yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd
```

OpenSuse e derivados:

```
$ sudo zypper install clamav
```

Para obter mais informações quanto à instalação ou contribuir com o manual do usuário e as perguntas frequentes, acesse o mesmo através do GitHub7.

4.1.1.1.1 Outras Recomendações de Antivírus

Visto que não há uma melhor opção de antivírus genérica, foram escolhidas algumas outras opções para que você possa verificar qual antivírus se aplica melhor aos seus interesses (ANDERSON, 2019):

1. Comodo;

---

7 Disponível em: https://github.com/Cisco-Talos/clamav-faq/tree/master/manual/UserManual/Installation-Unix. Acesso em: 14 maio 2020.

2. ESET NOD32 Antivírus;
3. Bitdefender;
4. Avast Core Security.

4.1.1.1.2 Atualize suas definições de vírus

Como qualquer antivírus, sua eficácia depende da frequência com que você atualiza sua definição de vírus. Então, continuando com o mesmo exemplo de antivírus anterior, atualize o ClamAV com o seguinte comando (BRITO, [2019?]):

```
1. freshclam
```

Em seguida, escaneie um diretório (note que a opção -r é para fazer o programa pesquisar recursivamente):

```
2. clamscan -r /home/nome-do-usuario
```

Caso o ClamAV encontre um arquivo infectado, remova-o usando esse comando:

```
3. clamscan --infected --remove --recursive /home/nome-do-usuario
```

Caso o processo acima tenha que ser feito frequentemente, substitua-o pela inicialização do daemon do ClamAV para que ele possa procurar por ameaças constantemente:

```
4. /etc/init.d/clamav-daemon start
5. /etc/init.d/clamav-freshclam start
```

4.1.1.2 Proteção contra rootkits

Tendo surgido no GNU/Linux, “o método rootkit é um conjunto de ferramentas que possibilita que um cracker tenha acesso à conta root (de administrador) em seu computador” (ORLOFF, 2008), ao mesmo tempo que ocultam a sua presença.

Para lutar contra rootkits e outras possíveis explorações, Orloff (2008) recomenda instalar e utilizar o rkhunter e, para uma proteção mais abrangente, o chkrootkit, visto o enorme problema proporcionado por esse malware. Para instalar o rkhunter em qualquer distribuição, abra o terminal e execute os comandos abaixo:

Primeiro vamos entrar no diretório temporário:

```
1. cd /tmp
```

Faça o download do pacote disponibilizado no site oficial do projeto:

```
2. wget -c https://sourceforge.net/projects/rkhunter/files/rkhunter/1.4.6/rkhunter-1.4.6.tar.gz
```

Extraia o conteúdo baixado:

```
3. sudo tar -xvf rkhunter-1.4.6.tar.gz
4. sudo cd rkhunter-1.4.6
5. sudo ./installer.sh --layout default --install
```

Atualize a base do rkhunter através deste processo de instalação, execute:

```
6. sudo /usr/local/bin/rkhunter --update
7. sudo /usr/local/bin/rkhunter --propupd
```

Para instalar e em seguida executar o chkrootkit:

1. sudo apt install chkrootkit
2. sudo chkrootkit

E pronto, você estará um pouco mais seguro dos cibercriminosos que tentarem permanecer no seu sistema (muitas vezes esse malware se esconde por meses ou até anos no mesmo sistema sem a percepção do usuário) para fins maliciosos – como para produzir bitcoins (moeda digital), enviar spam, participar de ataques DDoS e assim por diante.

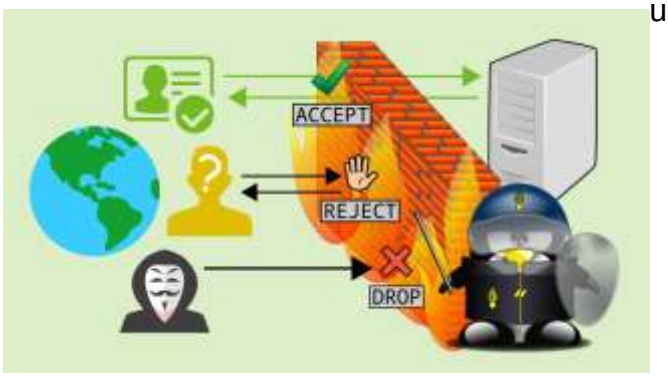
4.1.1.3 Firewall

Antes de tudo, o objetivo do mesmo é aplicar política da segurança a um determinado ponto de rede (CARMO, 2013). Ou ainda, simplesmente bloquear o tráfego de dados indesejados e liberar acessos autorizados. Mas o que é um firewall? Vejamos o conceito dado: “É um sistema ou grupo de sistemas que aplicam políticas de controle de acesso entre duas redes” (CAVINATO, 2015). Ou seja, um firewall é algo abstrato. Alecrim (2013) define o firewall como:

> É uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

A partir disso, um firewall, analogicamente, atua como um porteiro: impede a entrada de pessoas não autorizadas. Além de impedir malwares de utilizarem determinadas portas para se instalar em um computador sem o usuário saber, um programa que envia dados sigilosos para a internet, entre outros.

Figura 02 – Representação de um firewall



Fonte: Linux Kamarada Project (2019)8

O IPTables é uma ferramenta usada para configurar o subsistema de processamento de pacotes presente nas distribuições Linux, o Netfilter (DELFINO, [201-?]), ou ainda: é uma estrutura de tabela genérica para a definição de conjuntos de regras.

Para o funcionamento correto do firewall é preciso estabelecer políticas, as ditas regras (rules). A partir disso, precisamos entender a principal função do iptables, a qual é analisar o tráfego de rede recebido pelo computador, ou seja, essa ferramenta inspeciona todos os pacotes, verifica o enquadramento de cada um em relação às regras e aplica uma determinada ação. O processamento dos pacotes é feito pelo iptables a partir de uma estrutura que contém suas tabelas – tables – e cadeias – chains (DELFINO, [2018?]).

A fim de adentrar o funcionamento de um firewall será introduzido alguns conceitos a respeito. Sendo assim, dentro da estrutura do iptables há cinco tabelas. Tabelas são locais utilizados para armazenar as cadeias9 e regras do nosso firewall. Dessa forma, as tabelas e as cadeias nelas inseridas determinarão os pacotes onde as regras serão aplicadas. De acordo com Dorneles (2019), as tabelas do IPTables são:

1. Filter: é a tabela padrão. Regras responsáveis por determinar tudo o que entra e sai da máquina local. Frequentemente utilizada em Firewall de host. Dentro dessa camada existem três cadeias: INPUT, OUTPUT e FORWARD.

---

8 Disponível em: http://b.link/firewall. Acesso em: 14 maio 2020.

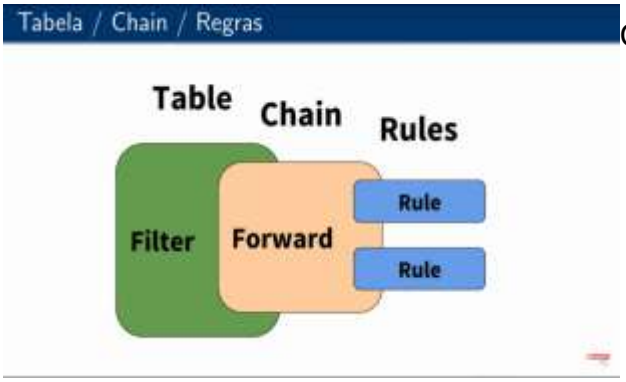
9 Local onde definimos as regras para o firewall, ou seja, uma chain é composta por um conjunto de regras.

2. NAT (Network Address Translation): como a própria origem do acrônimo nos diz, realiza a tradução dos endereços que passam pelo roteador onde ela age. Utilizada para dados que geram outra conexão, como mascarar a Internet e redirecionar requisições. Frequentemente utilizada para firewall de rede. Suas três cadeias são: PREROUTING, POSTROUTING e OUTPUT.
3. Mangle: utilizada para fazer QoS. Especifica as ações especiais que devem ser aplicadas no tráfego que passa pelas cadeias. No caso, tais ações ocorrem anteriormente às cadeias das tabelas filter e NAT. Aqui existem cinco cadeias, as quais correspondem às cadeias das outras camadas do iptables: PREROUTING, POSTROUTING, INPUT, OUTPUT e FORWARD.
4. Raw: de acordo com Victor, essa tabela é utlizada principalmente para a configuração de isenções de rastreamento de conexões em combinação com o alvo NOTRACK. Ela registra os ganchos netfilter com maior prioridade e é chamada pelo ip_conntrack, ou quaisquer outras tabelas IP. Residem as cadeias PREROUTING e OUTPUT.
5. Security: a partir do professor Fábio (2014), essa tabela é utilizada para regras de rede MAC (Mandatory Acess Control).

Cada chain possui uma política padrão que vai determinar que tipo de regras você irá criar na chain (DORNELES, 2019). As principais cadeias são:

- ACCEPT: cria-se regras de liberação de pacotes.
- REJECT: barra um pacote silenciosamente. Nenhuma resposta é devolvida ao remetente.
- DROP: barra um pacote e devolve uma mensagem de erro ao remetente informando que o pacote foi barrado.
- LOG: cria um log diferente à regra, em /*var*/log/messages. Usar antes de outras ações.

Figura 03 – Organização do IPTables



Fonte: Dorneles (2019)

4.1.1.3.1 Tipos de firewall

Apesar do firewall, como foi dito anteriormente, apenas bloquear o tráfego de dados indesejados e liberar os acessos autorizados, esse trabalho pode ser feito de diversas maneiras. Pois, como afirmou Alecrim:

> O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. (2013)

Por essa razão, precisamos, novamente, verificar a melhor opção, a qual irá cumprir todos os nossos interesses. Podemos encontrar tipos de firewall, são eles:

1. **Filtragem de pacotes** (packet filtering): A partir da definição de Pizzolato (2018), esse tipo de firewall consiste basicamente em uma lista de regras criadas pelo desenvolvedor, que o firewall analisa. Se as informações são compatíveis, então aquele usuário é autorizado. Caso contrário, é negado. São dois os tipos de filtragem de pacotes:

- **Estático**: os dados são analisados com base nas regras, independentemente da ligação que cada pacote tem com o outro. É uma boa solução, embora possa ocorrer o bloqueio de algumas respostas necessárias devido a conflitos que podem ser criados, já que as regras são estáticas.

- **Dinâmico**: surgiu para corrigir as limitações dos filtros estáticos. Ele permite a criação de regras que se adaptem ao cenário, possibilitando que os pacotes trafeguem quando necessário e apenas durante o período determinado, corrigindo esse gargalo dos pacotes estáticos. É dividido, ainda, em Firewall de aplicação – ou proxy de serviços – e Inspeção de Estados.

4.1.1.3.2 Instalação do firewall

Utilizar um firewall integrado ao seu sistema operacional é essencial para a segurança do mesmo. De acordo com Reis (2019), a maioria das distribuições já possuem uma tabela de regras e filtros de tráfego (o IPTables). Utilizaremos como exemplo o UFW, o qual é um acrônimo para Uncomplicated Firewall. Esse é uma solução de código aberto construída em Python e distribuída sob licença GNU (General Public License). Sendo uma versão descomplicada do IPTables, o projeto UFW visa proporcionar facilidades ao usuário iniciante (DELFINO, [201-?]). Esse último ainda possui uma interface gráfica, o GUFW.

Para verificar se o UFW está instalado e ativo em sua distribuição, execute (adicione numbered após a palavra status caso queira ver o número da regra):

```
$ sudo ufw status
```

Caso esteja instalado, mas não ativo, então execute:

```
$ sudo ufw enable
```

Caso não esteja instalado, execute10 (Debian e derivados):

```
$ sudo apt-get install ufw gufw
```

10 Ou ainda instale pelo site.

Como foi dito anteriormente, é preciso configurar o firewall criando regras para bloquear acessos indevidos de entrada e de saída. Porém, caso você não queira configurá-lo, apenas ative as configurações que existem por padrão. Em contraponto, caso queira saber mais sobre como configurá-lo e utilizá-lo por linha de comando, saiba mais aqui (RODRIGUES, 2020). E saiba que, mesmo sendo simples de utilizar, esse é um firewall poderoso.

Figura 04 – Interface do GUFW

Fonte: gufw.org (2020)11

4.1.1.3.3 Criando regras

O firewall trabalha com dois tipos de regras: de entrada (exterior – como a Internet – para o seu computador) e de saída (origem na rede local com destino ao exterior). Para permitir acesso a um serviço, você precisará de informações sobre esse, como o nome oficial, o protocolo e o número da porta que esse serviço utiliza. Para verificar essas informações você pode procurá-las na internet ou utilizar esse comando, o qual abrirá um arquivo com essas informações – os serviços disponíveis, seus números de portas e seus respectivos protocolos12 (REIS, 2013):

11 Disponível em: gufw.org. Acesso em: 14 maio 2020.

12 Para sair do arquivo, basta digitar ‘q’.

```
$ less /etc/services
```

Sintaxe geral para permitir a entrada de um serviço:

```
$  sudo ufw allow porta/protocolo(opcional)
```

Sintaxe geral para negar um serviço:

```
$ sudo ufw deny porta/protocolo(opcional)
```

Como exemplo, caso queira habilitar o tráfego na porta tcp 22 (ssh):

```
$ sudo ufw allow 22/tcp
```

Para apagar uma regra, você pode utilizar o nome dessa ou, de forma mais simples, o número dela (utilize o comando status numbered mostrado anteriormente para verificar o número da regra):

```
$ sudo ufw delete 1
```

Da mesma forma, caso queira negar todo o tráfego na porta tcp 22 (ssh):

```
$ sudo ufw deny 22/tcp
```

Caso queira negar saída para web13:

```
$ sudo ufw deny out 80
```

4.1.1.3.4 Outras opções de ferramentas

13 Note que para criar alguma regra de saída é necessário especificar com ‘out’, mas isso não é necessário especificar quando se trata de alguma regra de entrada.

Assim como antivírus, ferramentas de backup, VPN's14 e outras medidas para implementação de segurança, não há fórmula mágica que nos diga qual é a melhor ferramenta que devemos investir (tanto tempo quanto dinheiro). Por essa razão, outros exemplos de ferramentas:

1. IPTables;15
2. NFTables;
3. pfSense;
4. Firewalld.

4.1.1.3.5 Limitações do firewall

A importância do firewall é notável. Porém, isso não significa que esse é imune à falhas. Tendo isso em vista, é preciso frisar as limitações existentes nesse. Pode-se destacar (ALECRIM, 2013):

- As regras devem ser constantemente verificadas a fim de não prejudicar o funcionamento de serviços recentemente instalados e o desempenho do computador;
- Verificar se esses novos serviços ou protocolos estão devidamente tratados por proxies já implementados;
- O firewall pode não identificar uma atividade maliciosa ocorrida através do descuido do usuário – como o caso de o usuário enviar suas informações pessoais para um site falso que foi enviado a ele por uma mensagem de e-mail;
- Crackers experientes podem tentar descobrir ou explorar brechas de segurança existentes no firewall;

14 A VPN (Virtual Private Network) é uma rede privada construída sobre a infraestrutura de uma rede pública, normalmente a Internet.

15 O IPTables é a base para as outras ferramentas (DORNELES, 2019).

- Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma conexão 3G o firewall não conseguirá interferir.

4.1.2 Backup

Até agora foi falado sobre a proteção das suas informações. Porém, do que adianta proteger nossos dados se, por falta de um backup, esses acabarem sendo perdidos? Por isso, esse processo é a base de todos os outros, apesar ser um dos últimos comentados.

Por definição, “backup é uma forma de proteger nossos dados pessoais e profissionais” (DELFINO, [201-?]). Esse pode ser realizado em mídia física (CD, pendrive e Blu-ray) ou na nuvem (Google Drive, Dropbox e SkyDrive).

Como exemplo, utilizaremos a ferramenta Rsync, a qual é utilizada para realizar operações de backup de arquivos e diretórios em ambientes UNIX/Linux e vem previamente instalada em quase todas as distribuições do GNU/Linux.

Com o Rsync podemos criar rotinas de backup incrementais para salvar os arquivos localmente ou em servidor remoto. O Rsync, por ser baseado no antigo rcp, herdou as propriedades de criptografia do protocolo SSH16, o que torna sua transmissão de informações mais segura que o FTP (PAULA, 2003). Sendo assim, esse, por padrão, utiliza o protocolo SSH. Uma observação sobre o SSH: ele responde na porta17 22, consequentemente, é necessário configurá-la no firewall a fim de ter mais segurança (REIS, 2016). Dessa maneira, é necessário que a máquina que irá receber as informações tenha o SSH funcionando. Pode-se instalar o OpenSSH server – conjunto de ferramentas livres e de código aberto, usadas para fornecer segurança e

16 É um protocolo para a troca segura de dados entre dois computadores em uma rede não confiável.

17 As portas são interfaces de conexão utilizadas por aplicações para estabelecer uma conexão com o servidor.

encriptar a comunicação entre computadores numa rede (DELFINO, [201-?]) – com o seguinte comando:

```
$ sudo apt-get install openssh-server
```

Para verificar se o Rsync está instalado, execute:

```
$ whereis rsync
```

Caso a ferramenta não esteja incluída na sua distribuição e, consequentemente, não apareça o diretório dessa quando o comando anterior for executado, digite o seguinte comando para a instalação:

Nas distribuições baseadas em Red Hat:

```
$ sudo yum install rsync
```

Nas distribuições baseadas em Debian:

```
$ sudo apt-get install rsync
```

Sintaxe geral do Rsync:

```
$ rsync [opções] origem destino
```

Como existem diversas opções, acesse as páginas de manual ou ajuda do utilitário com **man rsync** ou **rsync –help** para conferi-las18.

4.1.2.1 Outras opções de ferramentas

18 Mais informações sobre como utilizar o Rsync: sincronizacao de arquivos no linux rsync e transferindo arquivos com o rsync.

Pode-se, ainda, verificar essas outras eficientes ferramentas para obter a melhor opção para você:

- fwbackups;
- mondo rescue;
- déjà dup;
- kbackup.

4.1.3 Medidas para evitar problemas com o fator humano

Como foi dito antes, o fator humano é um dos grandes problema para a segurança da informação. Por isso, apresentaremos algumas medidas que podemos tomar a fim de evitar a interferência desse fator. Medidas que, apesar de extremamente simples, às vezes, por um descuido ou por realmente pensar que não é nada demais, colocam tudo a perder.

1. Cuidado com dispositivos emprestados e com mídias removíveis: computadores de empresas, de escolas e celulares de conhecidos são exemplos de dispositivos que não devemos salvar cadastros, senhas e assim por diante. Assim como “certificar-se de que esses dispositivos criptografem as informações, protegendo, consequentemente, as informações armazenadas caso ocorra alguma invasão ou roubo” (OLIVEIRA, [20--?]).

2. Utilize senhas complexas: (OLIVEIRA, [20--?]) deve-se utilizar tanto letras minúsculas quanto maiúsculas nas senhas, assim como números e caracteres especiais. Porém, antes de tudo, deve-se lembrar da senha, então, caso necessário, anote-a em um papel e guarde-o em um local seguro, longe do computador e de uma forma que apenas você entenda.

3. Encerre suas sessões após o uso: ao acessar seu e-mail, sua conta em uma loja online, Facebook ou qualquer outra rede social, clique em Logout, Logoff, Sair, Desconectar ou equivalente para sair (ALECRIM, 2019).

4. Cuidado com downloads: a partir de Alecrim (2019), caso você utilize programas de compartilhamento ou baixa arquivos em sites especializados em downloads, verifique a extensão e o tamanho do arquivo. Cibercriminosos

normalmente utilizam arquivos de vídeos, músicas, aplicativos e afins para enganar o usuário. Por fim, sempre examine o arquivo baixado com um antivírus.

5. Evite o uso de softwares piratas: softwares piratas quase sempre têm malwares e por isso eles são gratuitos. Esses ainda “não contam com as atualizações de segurança que o desenvolvedor disponibiliza para as cópias originais” (ALECRIM, 2019). Então, muito cuidado ao fazer o download de jogos, sistemas operacionais, editores de imagens e afins caso esses sejam piratas.

6. Cuidado com e-mails e SMS’s falsos: qualquer SMS com título ou remetente duvidoso ou desconhecido deve ser evitado. Coisas que, por exemplo, dizem que você tem uma dívida ou que suas informações precisam ser atualizadas trata-se, muito provavelmente, de um phishing, ou seja, de uma mensagem falsa, portanto, ignore-a (ALECRIM, 2019).

7. Cuidado ao fazer compras pela internet: (ALECRIM, 2019) apesar da simplicidade que é comprar o que você precisa sem sair de casa, faça-o apenas em sites confiáveis que sejam de comércio eletrônico e com boa reputação.

8. Cuidado ao fazer cadastros online: (ALECRIM, 2019) muitas vezes exigir cadastro no site para utilizar o conteúdo desse é apenas uma técnica para obter informações como seu e-mail ou número de telefone para inserir esses em listas de spam ou marketing. Então, antes de tudo, veja se você realmente precisa desses serviços e se o endereço desse tem registro de alguma atividade legítima.

9. Use verificação em duas etapas: a partir de Alecrim (2019) há mais chances de impossibilitar o uso das suas informações por terceiros caso você utilize verificação em duas etapas. A partir do uso dessa, você receberá uma mensagem através de aplicativos como Google Autenticador e Microsoft Authenticator. Esses são as mais confiáveis, sendo assim, é aconselhável que as utilize ao invés das mensagens por SMS.

10. Evite utilizar redes Wi-Fi públicas: redes Wi-Fi sem senha. Muitas delas são meios de obter informações sobre os dispositivos conectados a ela ou direcionar o usuário para sites falsos. Por isso, dê preferência a redes de empresas conhecidas (ALECRIM, 2019).

Prestando atenção nesses passos básicos podemos evitar problemas enormes no futuro, pois o roubo de informação ocorre, na maior parte das vezes, a partir desses simples descuidos.

5. CONSIDERAÇÕES FINAIS

Tratou-se, pois, de termos básicos a respeito de segurança em TI e da aplicação dessa no sistema operacional GNU/Linux. O intuito desse trabalho foi auxiliar um iniciante na área de segurança a proteger os suas informações a fim de evitar problemas futuros. Além de criar a possibilidade de implicar a entrada de novos integrantes no ramo de segurança da informação ou ao menos incentivar o início de um longo estudo a respeito desse tema.

Porém, como dito anteriormente, as limitações existentes nesse trabalho são notáveis, pode-se destacar, entre elas: a instabilidade da segurança, os assuntos quase infinitos dentro da área de segurança da informação, a falta da abordagem da criptografia e da proteção do grub para a implementação da segurança.

A instabilidade da segurança existe porque, como dito na justificativa, o alto valor dessas implica novos ataques e esses implicam mais segurança. Por isso, a mudança nessa existe de forma natural. Relativo aos assuntos quase infinitos dessa área, apenas alguns desses são abordados e de forma puramente introdutória. Tanto a criptografia quanto a proteção do grub são essenciais para a proteção do nosso sistema. Não obstante, como o intuito do trabalho é falar sobre práticas básicas para obtenção da segurança e a fim não prolongar muito o trabalho, optou-se por não abordar esse tópico, mas faz-se necessário frisar, em última análise, que isso reduz a segurança necessária.

Por fim, deve-se constar que há uma longa estrada pela qual se deve passar a fim de compreender o tema, devido a abrangência do mesmo. Nesse sentido, devemos partir desse trabalho com algumas respostas e com novas perguntas.

6. CRONOGRAMA

Coloque as principais atividades que serão realizadas, e as datas em que tais eventos acontecerão (trata-se de uma estimativa de tempo para a realização do projeto).

Figura 02 - O cronograma deve ser adequado às necessidades do trabalho.

Atividades	**Projeto Final**							
	Projeto 1				**Projeto 2**			
	1ª sem	2ª sem	3ª sem	4ª sem	1ª sem	2ª sem	3ª sem	4ª sem
Escolha do assunto do projeto	x							
Elaboração da estrutura do projeto	x	x						
Seleção e leitura das obras para elaboração do projeto		x	x					
Elaboração dos objetivos, delimitação do tema, definição do problema, etc.		x		x				
Elaboração da pesquisa bibliográfica e documental do projeto			x	x				
Coleta de dados		x	x					
Tratamento dos dados			x	x				
Revisão final do texto e elaboração da introdução e conclusão							x	
Data limite de entrega do Projeto de Estágio								x

Fonte: o autor

ATENÇÃO:

Este cronograma está adaptado para o primeiro semestre. Caso seja utilizado para o segundo semestre, fazer as adequações necessárias. Verifique com o seu Orientador a adequação do cronograma.

7. REFERÊNCIAS BIBLIOGRÁFICAS

AIRES, Luísa. Paradigma qualitativo e práticas de investigação educacional. Lisboa: Universidade Aberta, 2015.

ALECRIM, Emerson. Dicas de segurança na internet. 2019. Disponível em: https://www.infowester.com/dicaseguranca.php. Acesso em: 05 maio 2020.

ALECRIM, Emerson. Malwares: o que são e como agem. 2017. Disponível em: https://www.infowester.com/malwares.php. Acesso em: 24 abr. 2020.

ALECRIM, Emerson. O que é firewall? - Conceito, tipos e arquiteturas. 2013. Disponível em: https://www.infowester.com/firewall.php. Acesso em: 28 abr. 2020.

ANDERSON, Sophie. 7 melhores (REALMENTE GRÁTIS) Antivirus para Linux em 2020. Disponível em: http://b.link/antivirusgratis. Acesso em: 28 abr. 2020.

ARNTZ, Pieter. How to protect your computer from malicious cryptomining. 2018. Disponível em: http://b.link/protect-your-computer. Acesso em: 3 maio 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 17799: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro, p. 9. 2005.

BRITO, Edivaldo. Como instalar o ClamAV no Linux e usá-lo corretamente. 2019. Disponível em: https://www.edivaldobrito.com.br/clamav-no-linux/. Acesso em: 25 abr. 2020.

CALDAS, Daniel Mendes. ANÁLISE E EXTRAÇÃO DE CARACTERÍSTICAS ESTRUTURAIS E COMPORTAMENTAIS PARA PERFIS DE MALWARE. 2016. 105 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Universidade de Brasília, Df, 2016.

CARVALHO, Italo Rezende Ferreira de. SEGURANÇA DA INFORMAÇÃO: um instrumento para avaliação do plano de continuidade do negócio aplicado em uma organização pública. 2020. 76 f. TCC (Graduação) - Curso de Ciências da Computação, Universidade Federal de Lavras, Lavras, 2011.

CAVALCANTE, Waldek Fachinelli. Crimes cibernéticos. 2013. Disponível em: https://jus.com.br/artigos/25743/crimes-ciberneticos. Acesso em: 29 abr. 2020.

CAMARGO, Renata. Dicas de segurança da informação na hora de escolher um Software de Orçamento. Disponível em: http://b.link/ciberseguranca-e-si. Acesso em: 06 maio 2020.

CARMO, Jonathan Souza do. A SEGURANÇA DA INFORMAÇÃO NA REDE BANCÁRIA NO MUNICÍPIO DE ROLIM DE MOURA / RO1. 2013. 41 f. TCC (Graduação) - Curso de Administração, Universidade Federal de Rondônia, Porto Velho, 2020.

CAVINATO, Marcos Vinicius. Firewall. Disponível em:http://b.link/firewall-introducao. Acesso em: 28 abr. 2020.

DELFINO, Pedro. Tabelas do iptables: Entenda a lógica do Firewall do Linux. Disponível em: http://b.link/iptables. Acesso em: 25 abr. 2020.

DELFINO, Pedro. OPENSSH: COMO UTILIZAR PARA CRIAR UM SERVIDOR SSH NO LINUX COM DIVERSAS CAMADAS DE SEGURANÇA. Disponível em: https://e-tinet.com/linux/openssh/. Acesso em: 28 abr. 2020.

DORNELES, Ademir. Laboratórios de Serviços de Rede - Linux Debian 10 | Videoaula 06 – Firewall. Disponível em: http://b.link/lab-firewall. Acesso em: 25 abr. 2020.

GIL, A. C.; 2002. Métodos e Técnicas de Pesquisa Social. 6. ed. São Paulo: Atlas.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. Ciência da Informação, [s.l.], v. 35, n. 3, p. 89-98, dez. 2006. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0100-19652006000300009.

MARCONDES, José. Conceito de segurança da informação organizacional. Disponível em: http://b.link/seguranca. Acesso em: 10 abr. 2020.

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar. São Paulo: Pearson Education, 2003. Disponível em: http://b.link/arte-de-enganar. Acesso em: 16 abr. 2020.

NASCIMENTO, Felipe. Segurança da Informação e Engenharia Social: a relevância do fator humano. 2018. Disponível em: http://b.link/engenharia-social. Acesso em: 4 maio 2020.

ORLOFF, Jeffrey. Protegendo o Desktop do Linux: uma seleção de ferramentas fáceis de usar para manter seus sistemas seguros. Uma seleção de ferramentas fáceis de usar para manter seus sistemas seguros. 2008. Disponível em: http://b.link/ibm-guide. Acesso em: 23 abr. 2020.

OLIVEIRA, Wallison. Segurança da Informação: 9 dicas para se proteger. Disponível em: http://b.link/seguranca-informacao. Acesso em: 05 maio 2020.

O que são Rootkits e como Enfrentá-los. **Kaspersky**. Disponível em: http://b.link/rootkits. Acesso em: 30 abr. 2020.

O que é um firewall?. **Cisco**. Disponível em: http://b.link/o-que-e-firewall. Acesso em: 28 abr. 2020.

PAULA, Fábio. Transferindo arquivos com o rsync. Disponível em: http://b.link/rsync. Acesso em: 28 abr. 2020.

PIZZOLATO, Rafael. Quais os tipos de Firewall e suas diferenças?. 2018. Disponível em: https://blog.starti.com.br/tipos-de-firewall/. Acesso em: 28 abr. 2020.

POZZEBOM, Rafaela. Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit. 2015. Disponível em: http://b.link/diferenca-malwares. Acesso em: 23 abr. 2020.

PRESTES, Vladimir. Indústria e segurança da informação: as principais ameaças de 2018. 2018. Disponível em: http://b.link/ameacas. Acesso em: 26 abr. 2020.

RED HAT. Red Hat enterprise linux 6.8: security guide. [S.l.], 2011. Disponível em: http://b.link/security-guide. Acesso em: 24 abr. 2020.

RICHARDSON, Roberto Jarry. Pesquisa social: métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

RODRIGUES, Diego. Firewall com UFW. 2020. Disponível em: http://b.link/ufw. Acesso em: 25 abr. 2020.

REIS, Fábio. rsync - Cópia, Sincronização e Backup de arquivos no Linux. 2016. Disponível em: https://www.youtube.com/watch?v=djtMHTA_aBA. Acesso em: 29 abr. 2020.

REIS, Fábio. Configurar Firewall UFW no Ubuntu Linux – parte 1 . 2013. Disponível em: http://b.link/ufw-ubuntu. Acesso em: 06 maio 2020.

REIS, Fábio. Firewall iptables no Linux – Parte 01: Noções Básicas. 2019. Disponível em: http://b.link/iptables-firewall. Acesso em: 06 maio 2020.

SANTOS, Andre H. O.. GNU/Linux é 100% Seguro? 2016. Disponível em: https://www.vivaolinux.com.br/artigo/GNULinux-e-100-Seguro/. Acesso em: 24 abr. 2020.

VOCÊ sabe quais as diferenças entre segurança da informação e segurança em TI?. **Alerta Security**. 27 ago 2018. Disponível em: http://b.link/seguranca-informacao-e-seguranca-ti. Acesso em: 17 maio 2020.

SILVA, Pedro Tavares et al. Segurança dos sistemas de informação. Lisboa: Centro Atântico Pt, 2003.

SIMPLÍCIO, Marcos. Segurança da Informação - Aula 01 – Introdução. Disponível em: http://b.link/seguranca-inform. Acesso em: 29 abr. 2020.

SÊMOLA, M. 2003: Gestão da Segurança da Informação. 1. Ed. Rio de Janeiro: Campus, 2003.

VISÃO Geral do Sistema GNU. **GNU**. 29 abr. 2019. Disponível em: https://www.gnu.org/gnu/gnu-history.pt-br.html. Acesso em: 06 maio 2020.

ZANICHELLI, Anderson de Souza; MARTIMIANO, Luciana Andréia Fondazzi. Definição de uma Política de Segurança para um Ambiente de Desenvolvimento Distribuído de Software. 2010. 10 f. TCC (Graduação) - Curso de Ciências da Computação, Universidade Estadual de Maringá, Maringá, 2020.

4. APÊNDICE A - NOME DO APÊNDICE

Para que os apêndices apareçam no sumário automático - Digite APÊNDICE A – TÍTULO DO MESMO - Vá até a janela de Estilo- selecione – Título 1 e centralize (por ser um elemento pós-textual, não possui numeração e deve ser centralizada, os espaços já estão definidos conforme as normas da ABNT).

Elemento opcional; é o texto ou o documento elaborado pelo próprio autor, com a finalidade de complementar seu trabalho.

5. ANEXO A - NOME DO ANEXO

Para que os apêndices apareçam no sumário automático - Digite ANEXO A – TÍTULO DO MESMO - Vá até a janela de Estilo- selecione – Título 1 e centralize (por ser um elemento pós-textual, não possui numeração e deve ser centralizada, os espaços já estão definidos conforme as normas da ABNT).

Elementos opcionais que se destinam à inclusão de materiais não elaborados pelo próprio autor, como: cópias de artigos, manuais, folders, balancetes, etc. e que não precisam estar em conformidade com o modelo.

FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA
Curso Técnico em Informática

Parecer SEC/CEED 007/2016
Rua Dr. Flores 396 - Centro - POA/RS

Ficha de Autorização para publicação no Site da Escola ou Repositório Eletrônico Escolar

Nome do estagiário (a): Brenda Andersen de Lima.

Autorizo a publicação deste projeto no repositório eletrônico escolar em:
<http://raam.alcidesmaya.com.br/index.php/projetos/issue/view/9>

_____

Nome Aluno