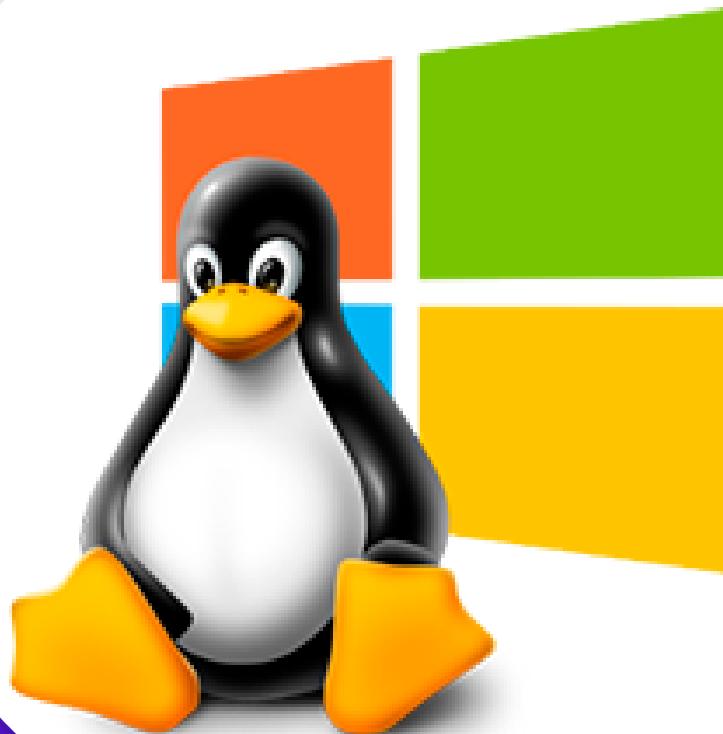


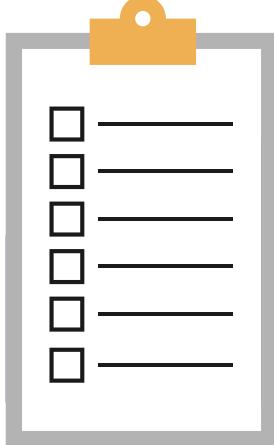
Fernando Silva

LINUX

PARA QUEM
utiliza qualquer sistema
aprender de forma rápida.



GRÁFICOS INCRÍVEIS
comandos passo a passo



SUMÁRIO

1 Sumário

3 Quem sou eu

4 Sistemas operacionais

7 Licença GPL

8 Por que servidores preferem Linux

9 Mercado de trabalho para Linux

11 Diferença entre Windows e Linux

12 Estrutura dos diretórios

13 Arquitetura do Linux

14 Distribuições e derivados

16 Interfaces gráficas

17 Como instalar o Debian

26 Como instalar o Kali

27 Sistemas de arquivos

30 Terminal, sudo e editor de texto

32 Tipos de arquivos

33 Permissões no Linux

35 Gerenciador de boot (Grub)

36 Tabela de montagem do sistema

37 Repositórios e Pacotes

42 Arquivos e Navegação no Linux

44 Contas de Usuários e Grupos

45 Análise da Rede e Acesso remoto ssh

48 Análise do sistema em geral

49 Arquivos compactados

50 Análise dos processos

51 Gerenciamento dos serviços (systemd)

52 Análise de arquivos de texto

53 Automatizando tarefas e rotinas

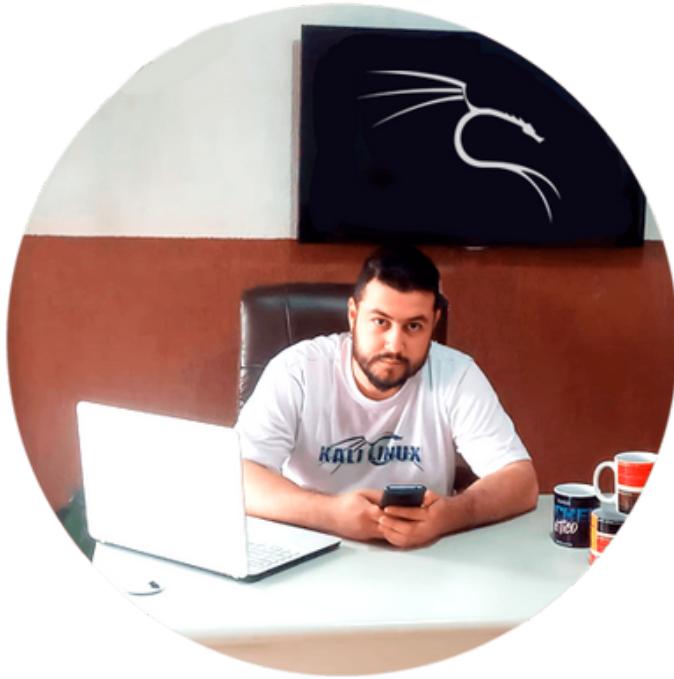
55 Corrigindo e Clonando HDs

57 Resumo rápido dos principais comandos

60 Considerações finais

61 Questões

QUEM SOU EU ?



Olá amigos, prazer sou o **Fernando Silva tenho 29 anos**, moro em SP e sou empreendedor e hacker. A primeira vez que utilizei o **Linux foi em 2011(Ubuntu)** desde então venho estudando esse sistema incrível que proporciona milhares de oportunidades no mercado de TI.

Hoje utilizo o perfil no **instagram (@linux.gnu)** para dar dicas sobre o **Linux e Hacking**, hoje esse perfil conta com mais de 50.000 seguidores, sendo um dos maiores se tratando desse segmento.

ATENÇÃO



ATENÇÃO! Este e-book é protegido por direitos autorais e qualquer forma de **distribuição ou revenda sem a autorização expressa do detentor desses direitos** é uma **VIOLAÇÃO GRAVE DA LEI**. Se você tentar distribuir ou revender este e-book sem autorização, estará sujeito a PESADAS SANÇÕES LEGAIS. **Não arrisque sofrer** as consequências devastadoras de uma **ação judicial**.

Respeite os direitos autorais e a propriedade intelectual. Não tolere a pirataria digital.



HACKER ÉTICO

PASSO A PASSO

- ✓ DOMINE O LINUX
- ✓ COMO ENCONTRAR FALHAS
- ✓ HACKEANDO DO ZERO

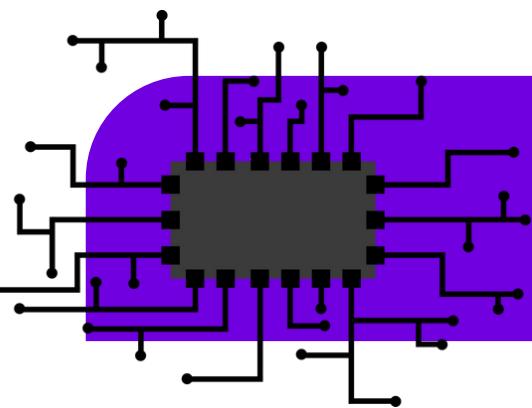
- ✓ CRIE ROBÔS HACKING
- ✓ ACESSE REDES WI-FI
- ✓ TENHA O PODER DE ATAQUE

QUERO SABER MAIS !

SISTEMAS OPERACIONAIS

Os criadores, como funcionam e suas estruturas





SISTEMAS OPERACIONAIS UM POUCO DA HISTÓRIA.

O QUE É UNIX ?

É um sistema operacional (SO) multiusuário e multitarefa projetado para flexibilidade e adaptabilidade. Desde seu lançamento em 1969, o sistema operacional Unix e suas ramificações tiveram um efeito profundo na indústria de computadores e eletrônicos, oferecendo portabilidade, estabilidade e interoperabilidade em uma **variedade infinita de dispositivos**.



**ESTRUTURA DOS
SISTEMAS OPERACIONAIS
EM GERAL.**

O QUE O UNIX FAZ ?

No coração do sistema operacional **Unix está o kernel, um programa de controle mestre** que fornece serviços para iniciar e encerrar programas. Ele também **lida com operações de baixo nível**, como alocação de memória, gerenciamento de arquivos, resposta a chamadas do sistema e agendamento de tarefas ou seja ele **gerencia os recursos de hardware e software do sistema**

Sua disponibilidade e portabilidade fizeram com que fosse amplamente adotado, **copiado e modificado por instituições** acadêmicas e negócios. Seu design influenciou autores de outros sistemas.

O Unix se tornou o **primeiro sistema operacional que poderia ser melhorado ou aprimorado por qualquer pessoa**, em parte porque foi escrito na linguagem C e abraçou muitas ideias populares.

O QUE É MINIX



É um sistema operacional **Unix-like** (semelhante ao UNIX), escrito em C e assembly, que foi desenvolvido por Andrew S. Tanenbaum em 1987 com propósitos acadêmicos, para exemplificar os conceitos de seu livro: "Sistemas Operacionais: projeto e implementação".

O QUE É LINUX ?



É o **KERNEL/Núcleo** que é utilizado por diversos eletrônicos em seus sistemas.

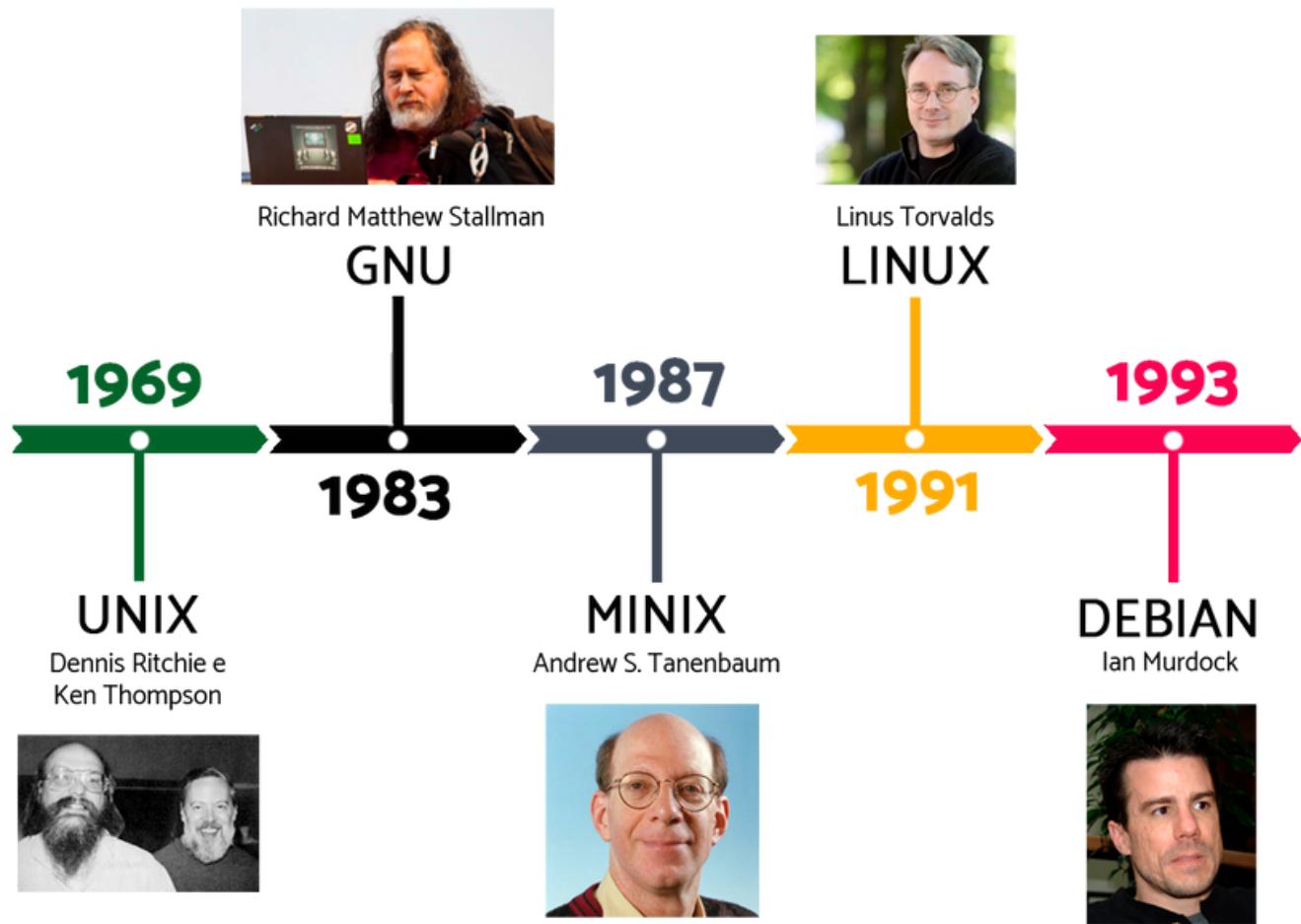
É como um **motor de um carro**, por exemplo, um motor é desenvolvido para o carro GOL, porém é possível aproveitar esse "tipo" de motor no carro POLO, basta fazer alguns ajustes.

LANÇAMENTO DO LINUX.

Em 1991 um estudante finlandês de 21 anos chamado **Linus Torvalds deu início em um projeto pessoal** com o intuito de criar um novo núcleo de sistema operacional, ele se baseou no MINIX para criar o LINUX.

Ele escreveu um programa especificamente para o hardware que estava usando e independente de um sistema operacional porque queria usar as funções de seu novo computador com um processador 80386.

O surgimento do nome LINUX é uma mistura de Linus + UNIX. Posteriormente o Kernel Linux **Integrou o projeto GNU** (1983) de Richard M. Stallman **isso resultou nos Linux de hoje em dia**.



LINUX É UTILIZADO EM ...

O kernel é embarcado em diversos dispositivos como roteadores, PABXs, receptores de televisão, Smart TVs, DVRs, e dispositivos de armazenamento em rede. Utilizam serviços providos pelo núcleo Linux para implementar as suas funcionalidades.





LICENÇA DE SOFTWARE GPL

LICENCIAMENTO

Ser open source pode ser a principal vantagem do Linux. **O Linux está disponível sob a Licença Pública Geral (GPL) GNU**. Isso significa que qualquer pessoa pode executar, estudar, compartilhar e modificar o software. O código modificado também pode ser redistribuído e até mesmo vendido, mas isso deve ser feito sob a mesma licença.

4 LIBERDADES

liberdade nº 0: A liberdade de executar o programa, para qualquer propósito

liberdade nº 1: A liberdade de estudar como o programa funciona e adaptá-lo às suas necessidades. O acesso ao código-fonte é um pré-requisito para esta liberdade.

liberdade nº 2: A liberdade de redistribuir cópias de modo que você possa ajudar ao seu próximo.

liberdade nº 3: A liberdade de aperfeiçoar o programa e liberar os seus aperfeiçoamentos, de modo que toda a comunidade beneficie deles . O acesso ao código-fonte é um pré-requisito para esta liberdade.



Idealizada por **Richard Matthew Stallman** em 1989



POR QUE SERVIDORES PREFEREM LINUX ?

- 100% dos 500 supercomputadores do mundo.
- Considerando 1 milhão dos maiores servidores do mundo, 96,3% rodam linux.
- Os 25 principais sites do mundo usam linux.
- 90% de toda a infraestrutura de nuvem opera em linux.
- 39,89% dos desenvolvedores profissionais usaram linux em 2022



Estabilidade

Não há necessidade de reiniciar o sistema em caso de atualizações e pode operar mesmo com falhas de hardware.



Eficiência

Alta performance em redes e servidores, consegue gerenciar facilmente um grande número de conexões dos usuários.



Suporte Técnico e Custos

Um dos melhores suportes, através de consultores e distribuidores comerciais.

Não precisa pagar pela licença do sistema.



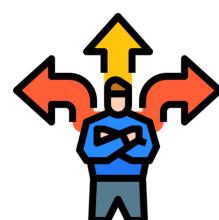
Segurança

Firewalls eficientes e robustos, permissões personalizadas facilmente, muito pouco vírus.



Multitarefa

Roda múltiplos programas simultaneamente.



Flexibilidade

Código fonte aberto, os usuários conseguem personalizá-lo.



VEJA O PORQUÊ É IMPORTANTE O CONHECIMENTO EM LINUX

MERCADO DE TRABALHO

Profissionais Linux podem trabalhar desde o suporte ao usuário, até administração de servidores, gerenciar backups, supervisionar instalações e atualizações de aplicativos, sistemas operacionais, consultoria, e desenvolvimento de software.

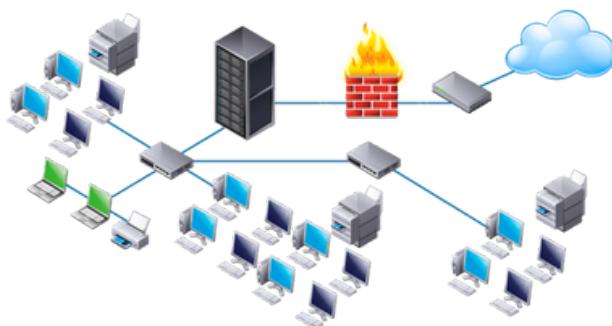
O Linux realmente está em demanda?

A resposta curta é sim! O 9º Relatório Anual de Empregos de Código Aberto da Linux Foundation Research e da edX descobriu que as habilidades em Linux eram **as segundas mais procuradas, precedidas apenas pelas habilidades em nuvem**. Esta foi de fato a primeira vez nas nove iterações deste relatório que o Linux não era a habilidade mais procurada, o que pode parecer implicar que ela está se tornando menos importante.

No entanto, quando você considera que a esmagadora maioria das **instâncias da AWS, GCP e até mesmo do Azure estão executando Linux**, fica claro que, embora a nuvem seja o tópico atual, você não pode realmente entender os fundamentos da tecnologia de nuvem sem conhecer o Linux. Qualquer pessoa que trabalhe em desenvolvimento ou arquitetura em nuvem pode dizer que precisa entrar na linha de comando do Linux com frequência, portanto, **entender como ela funciona é essencial**.

O Open Source Jobs Report também descobriu que 88% dos profissionais de tecnologia estão usando práticas de DevOps. Embora o DevOps seja um conjunto de princípios e práticas e, portanto, não exija explicitamente o conhecimento do Linux, o objetivo principal de usar o DevOps é criar e executar coisas como aplicativos que exigem um sistema operacional, e o Linux é o sistema operacional mais popular para aplicativos corporativos.

Existem inúmeros outros exemplos de como tecnologias como redes, sistemas embarcados, IoT, IA, telefones celulares, automóveis e muito mais **dependem do Linux**, mas o importante a ser lembrado é que se você espera construir uma carreira em tecnologia moderna, **você terá necessidade de possuir algum conhecimento de Linux**. Então, sim, ele realmente está em alta demanda.



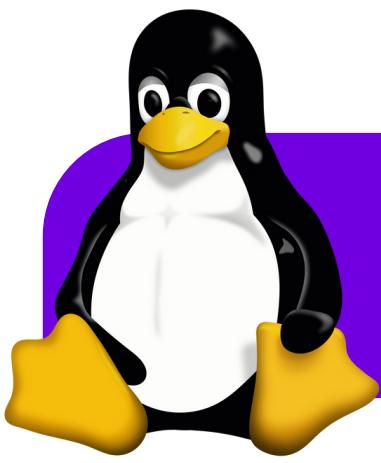
CERTIFICAÇÕES

O órgão responsável pelas certificações **Linux é o LPI** (Linux Professional Institute) e existem **4 níveis de certificações**:

- Linux Essentials
- LPIC-1: Linux Server Professional Certification
- LPIC-2: Linux Network Professional Certification
- LPIC-3: Linux Enterprise Professional Certification

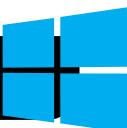


Os profissionais que **têm certificação** são **mais valorizados**.



DIFERENÇAS ENTRE WINDOWS E LINUX

WINDOWS



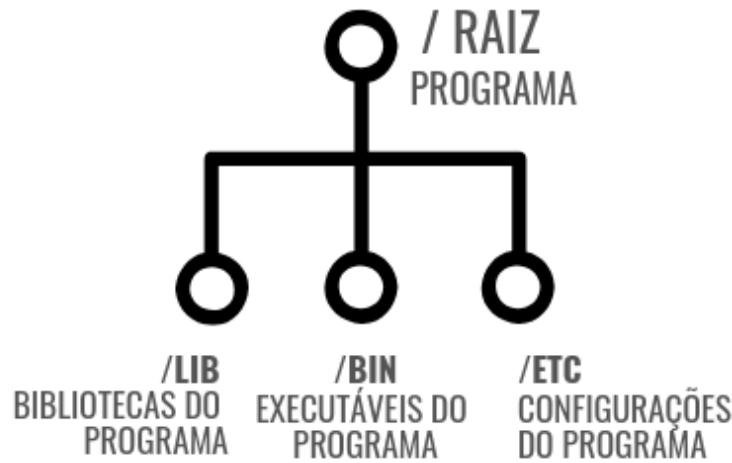
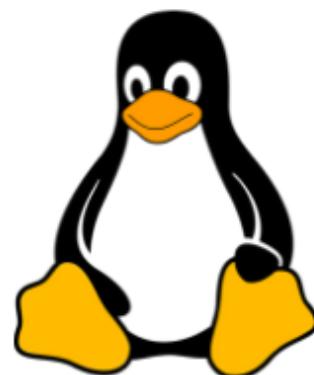
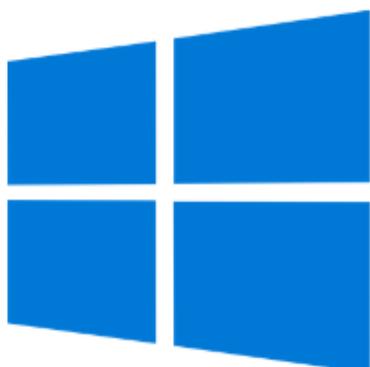
A estrutura já muito conhecida do windows funciona da seguinte maneira, as pastas **são armazenadas dentro do famoso disco C:**

Quando você instala um software é criada uma pasta dentro do disco C: com o nome do software instalado.

LINUX



A estrutura do Linux é bem diferente, os arquivos de um software **instalado são "separados"** digamos que cada parte do software fica em um diretório diferente. Cada diretório tem sua especificidade.



ESTRUTURA DOS DIRETÓRIOS





ARQUITETURA DO LINUX

EQUIPAMENTO FÍSICO

Parte física do computador como placa de memória RAM, disco



HARDWARE

KERNEL



CORAÇÃO DO SISTEMA

É basicamente o coração do sistema, no Kernel está escrita todas as instruções de gerenciamento do Sistema e do Hardware.

BIBLIOTECA DE FUNÇÕES PADRÃO

É a camada que permite o acesso a recursos através da execução de chamadas feitas por processos, como Habilitar



BIBLIOTECA

SHELL



INTERPRETA COMANDOS

interpretador de comandos, um entre os diversos tradutores entre o usuário e o sistema operacional conhecidos como shell.

PROGRAMAS UTILIZADOS

Softwares utilizados pelo usuário como browsers, editores de texto, editores de imagens etc.

Uma DISTRIBUIÇÃO Linux já vem com alguns softwares específicos instalados.



APLICAÇÕES



DISTRIBUIÇÕES E DERIVADOS

DISTROS

Uma distro é **um sistema operacional**, por exemplo Windows 10. No mundo Linux é chamado de distro (distribuição), e existem diversas distros, **cada empresa pode criar a sua própria distribuição**, como é o caso da redhat, ubuntu, open suse, etc. E ganhar dinheiro vendendo o sistema, suporte técnico, treinamento e produtos.

Uma distribuição derivada é baseada no trabalho feito em outra DISTRIBUIÇÃO, mas que tem seus próprios objetivos, identidade e audiência, e que foi criada por uma entidade independente. As distribuições derivadas modificam a "ORIGINAL" **para atingir seus próprios objetivos**.



DERIVADOS

Criados para atender uma **necessidade específica**, uma distribuição derivada já vem com ferramentas específicas para atender um determinado objetivo.

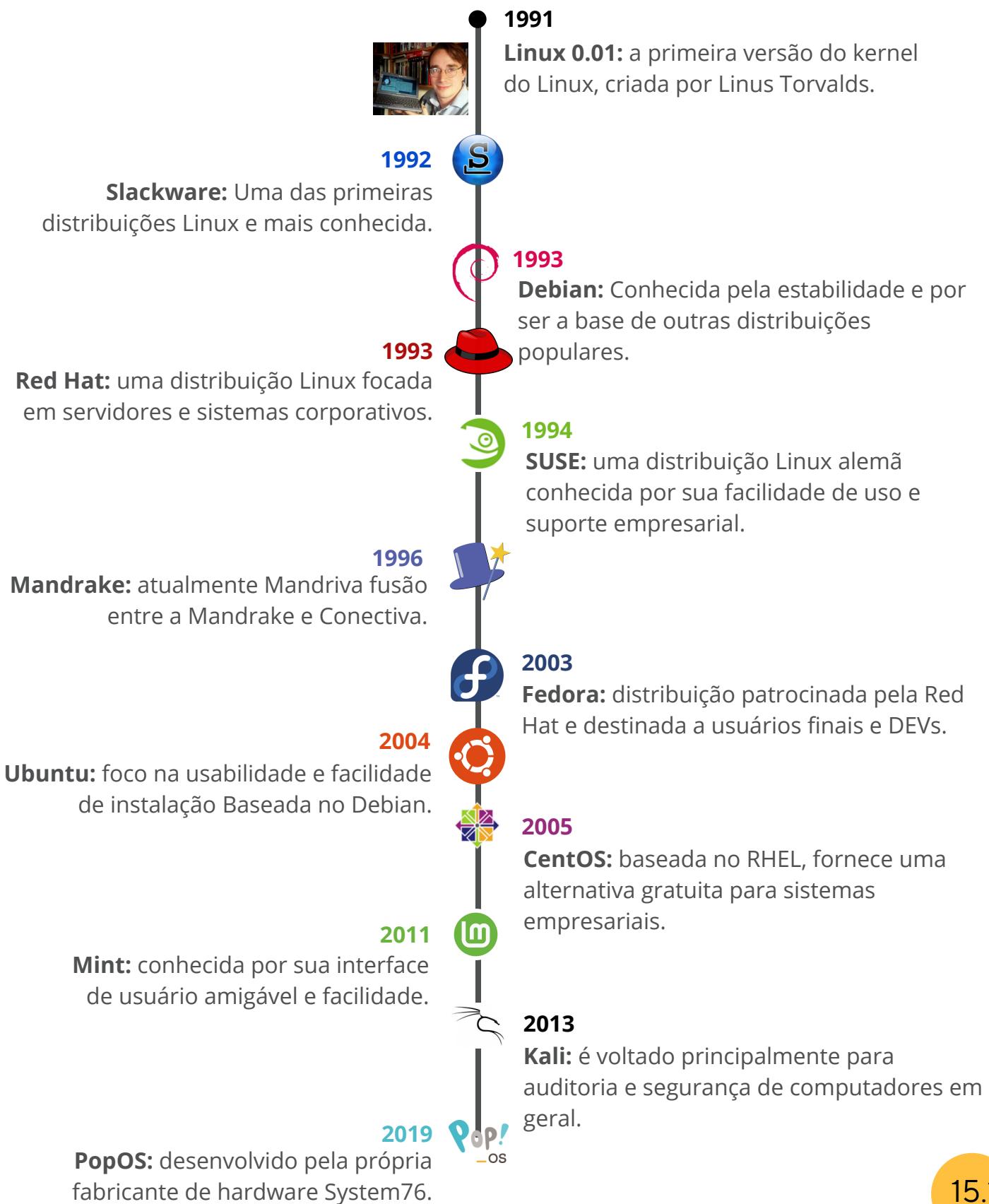
Por exemplo, o **KALI LINUX** já vem com **diversas ferramentas hacking**, assim o profissional de cibersegurança não perde tempo instalando essas ferramentas uma a uma. Todo o sistema já vem personalizado e preparado para cumprir as necessidades de um **profissional de cibersegurança**.

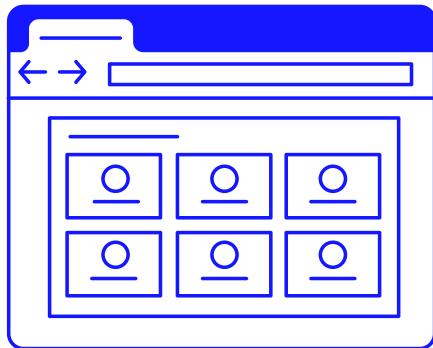
Muitas distribuições usam o Debian como base, pois o Debian está consolidado há muito tempo.



LINHA DO TEMPO

Algumas das distribuições Linux mais conhecidas e influentes.



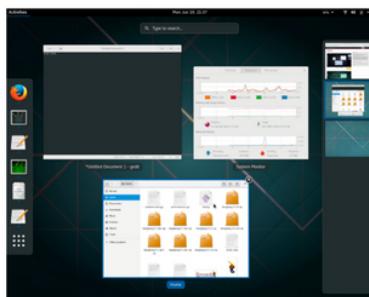


INTERFACES GRÁFICAS

INTERFACES

No Linux você pode **optar por diferentes interfaces gráficas**, cada uma com seu próprio estilo. Algumas podem ser mais leves, isso é útil quando você tem um hardware muito antigo ou “fraco”. Abaixo as interfaces mais conhecidas e seus nomes.

GNOME



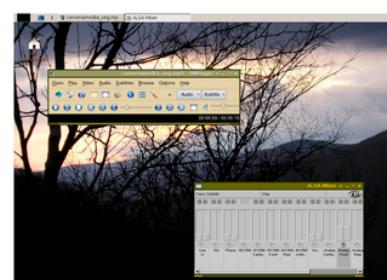
CINNAMON



XFCE



LXDE

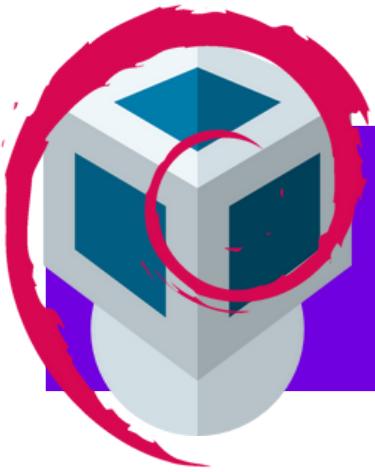


KDE PLASMA



MATE





COMO INSTALAR O DEBIAN NA VM

PASSO 1

Faça o download e instale o VirtualBox;

Faça o download da ISO do Debian;

Nesse site abaixo, você **consegue executar comandos do Linux** sem a necessidade de ter instalado, porém é limitado.

<https://bellard.org/jslinux/vm.html?>

<cpu=riscv64&url=https://bellard.org/jslinux/buildroot-riscv64.cfg&mem=256>



<https://www.virtualbox.org/wiki/Downloads>

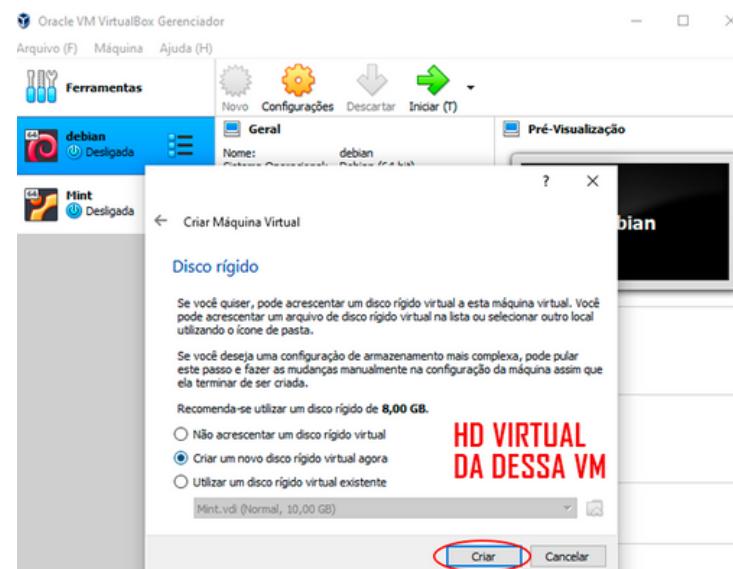
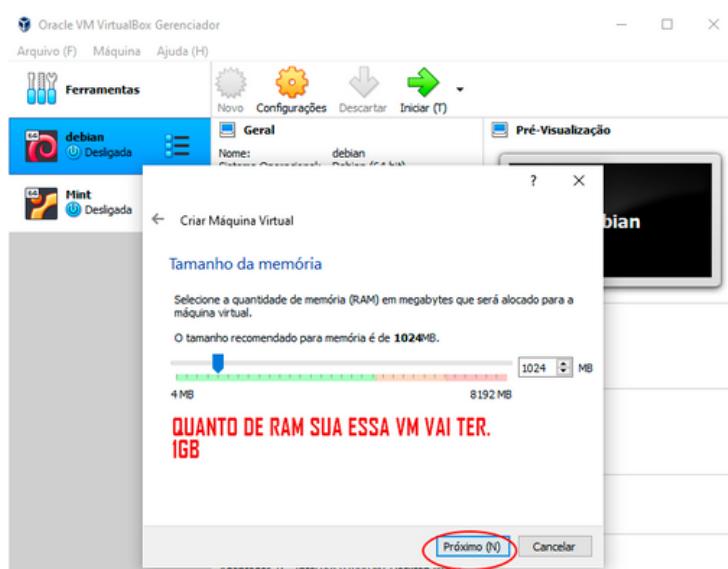
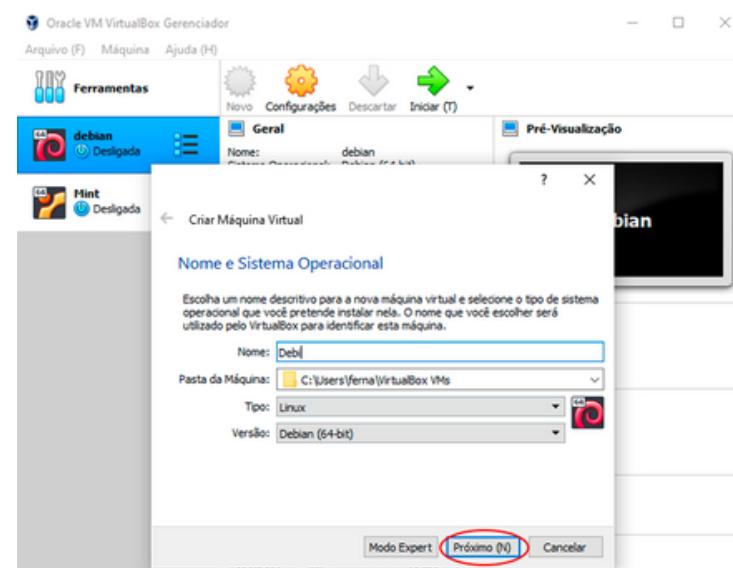
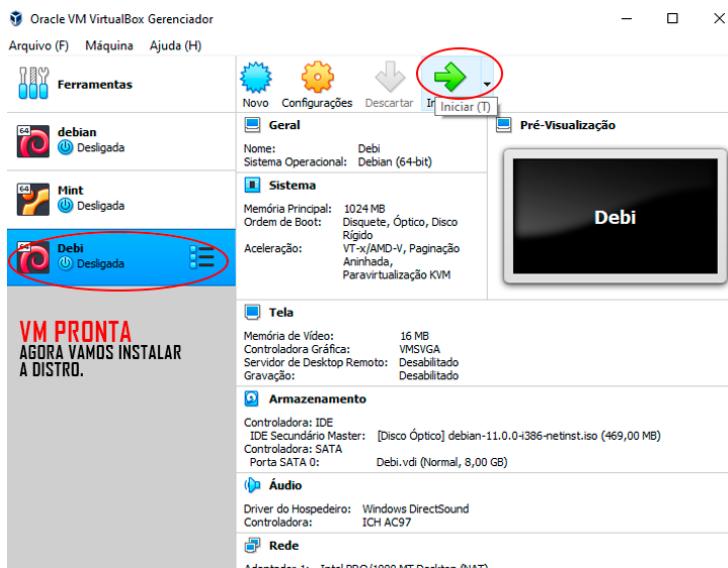


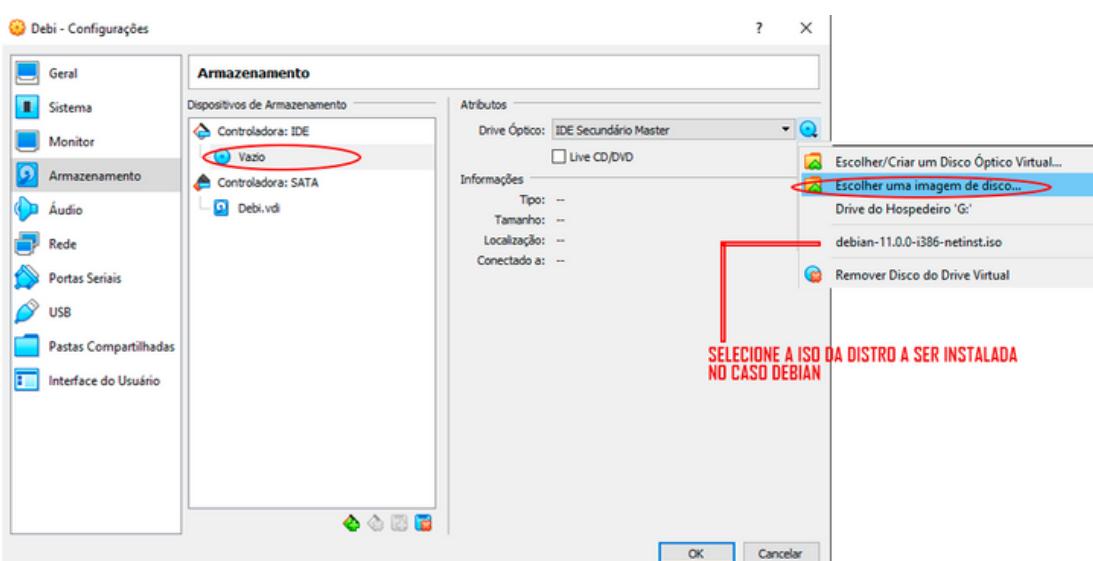
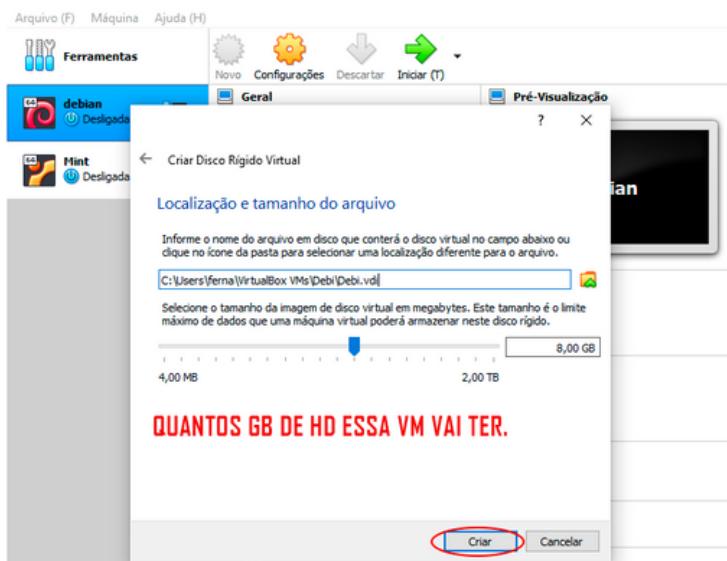
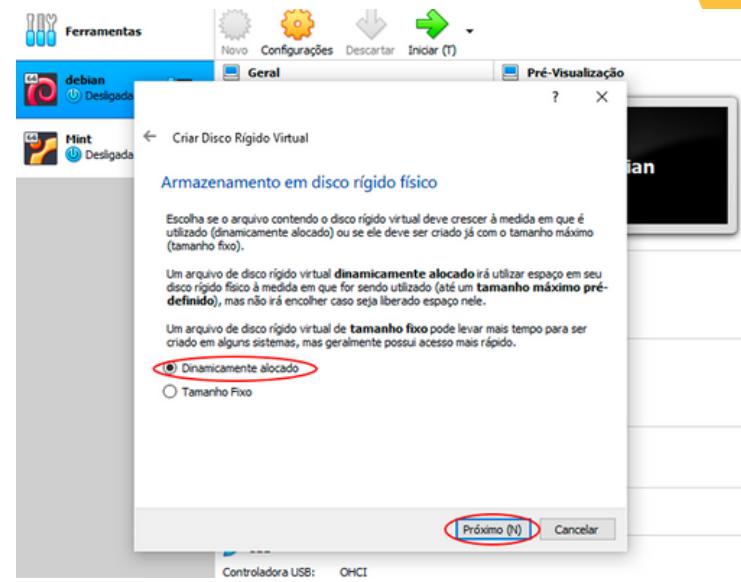
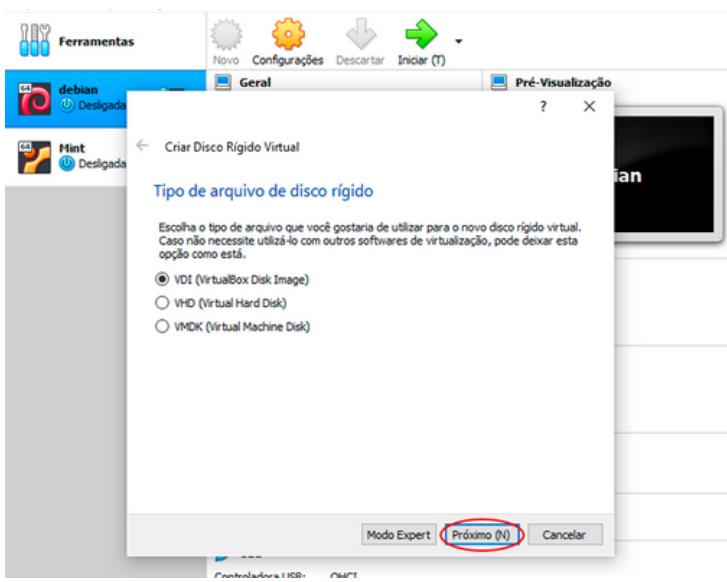
<https://cdimage.debian.org/debian-cd/current/i386/iso-cd/>

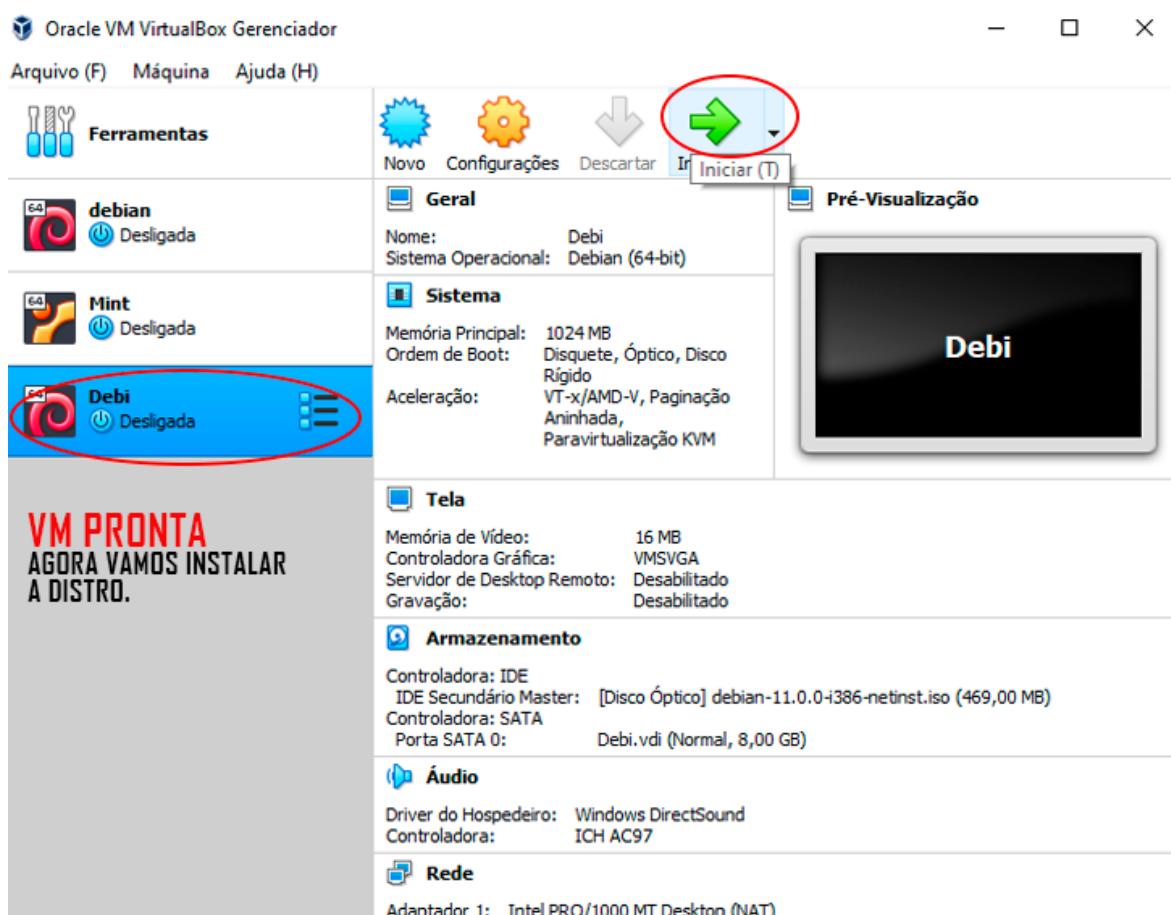
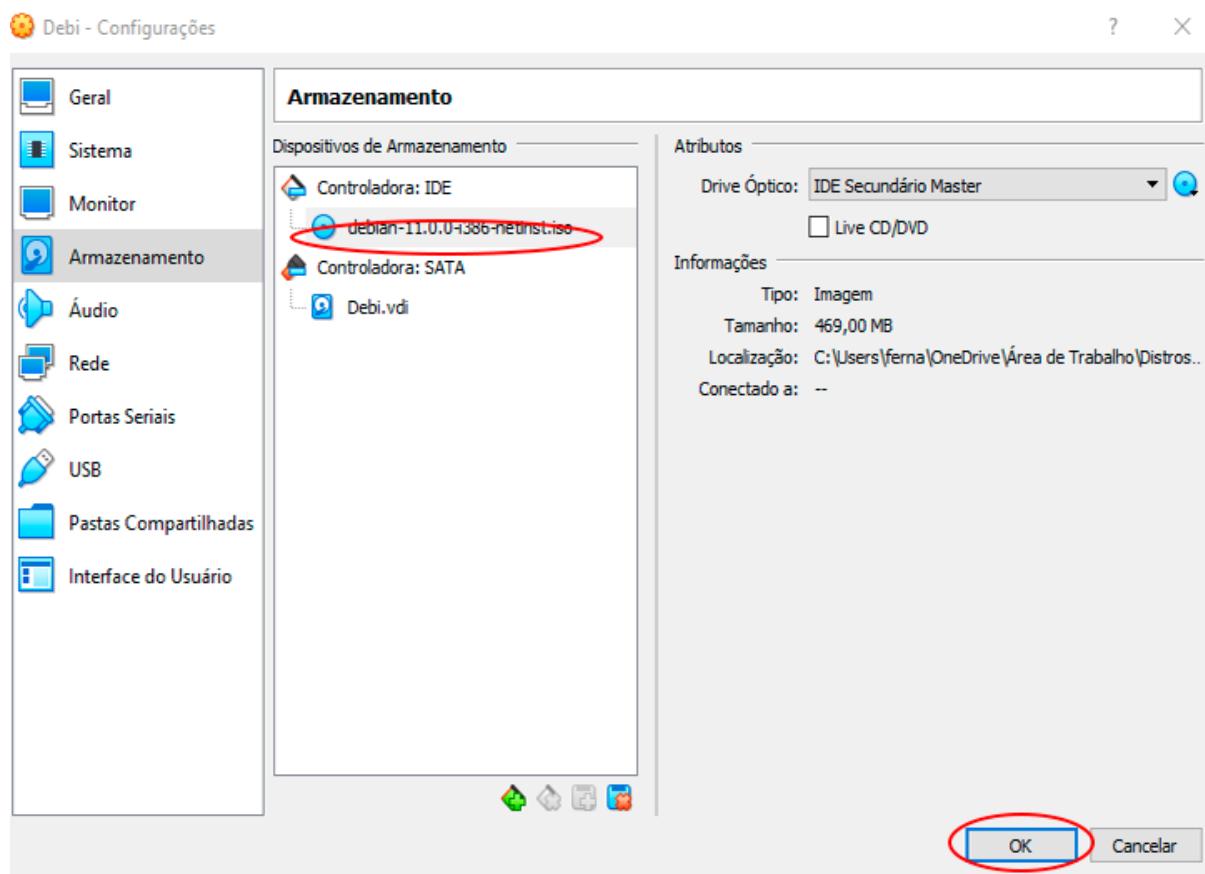
PASSO 2

Preparando a VM;

Será mostrado o passo a passo da preparação da VM, sem muita profundidade, pois o FOCO aqui não é Virtual Box. Caso você já saiba pode pular essa etapa.





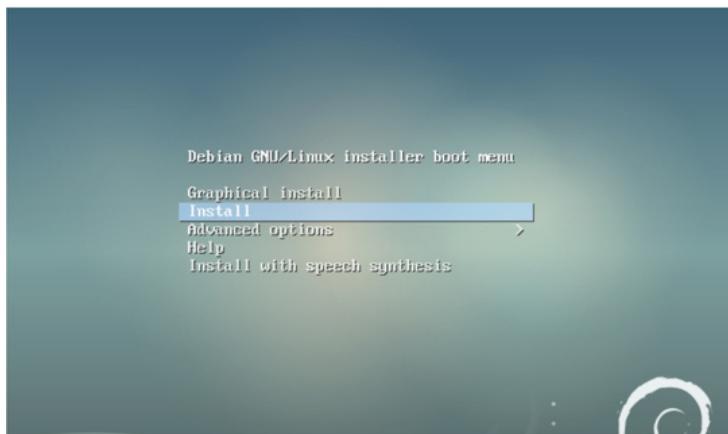


PASSO 3

Instalação do Debian.

PARTE 1

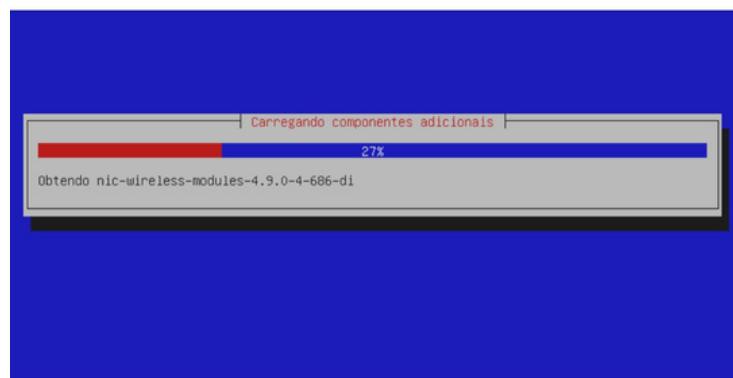
DEBIAN NA VM SEM INTERFACE GRÁFICA



Debian Servidor

PARTE 2

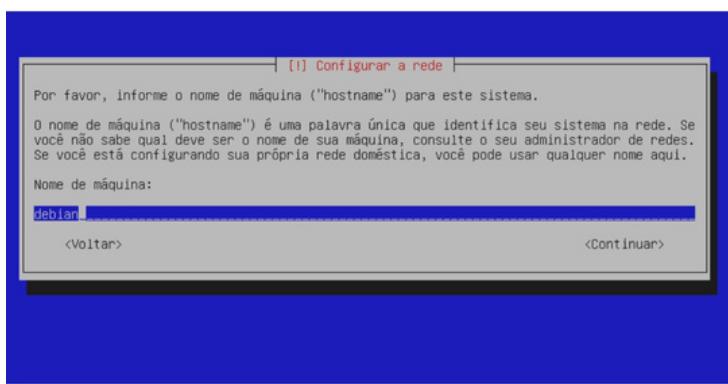
SELECIONAR PAÍS LOGO APARECERA ESSA TELA ...



Debian Servidor

PARTE 3

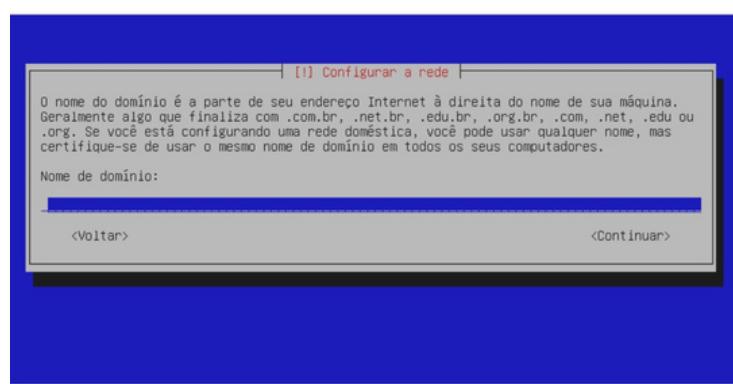
DE UM NOME PARA SUA MÁQUINA EX: PC-SALA



Debian Servidor

PARTE 4

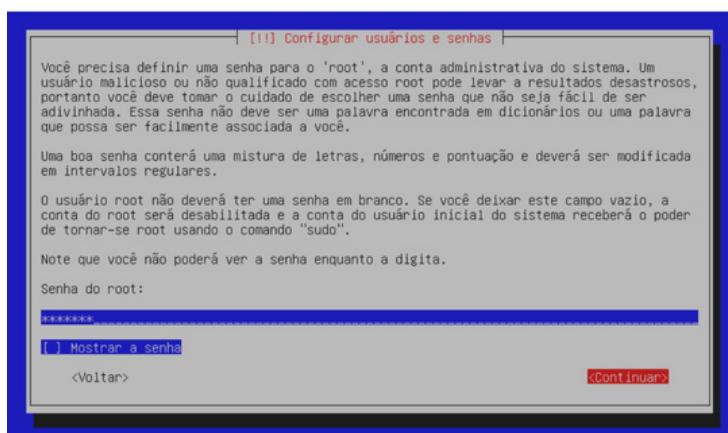
PODE DEIXAR EM BRANCO E CONTINUAR ...



Debian Servidor

PARTE 5

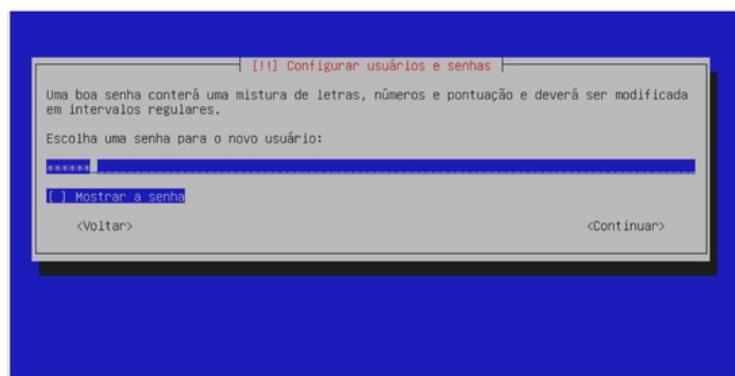
SENHA DO USUÁRIO ROOT "ANOTAR"



Debian Servidor

PARTE 6

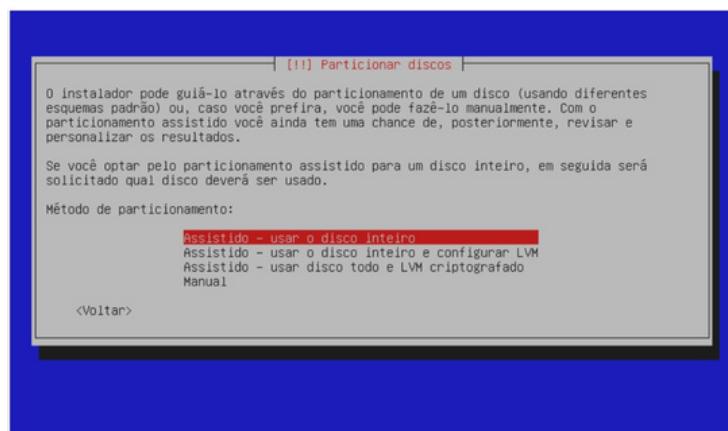
SENHA PARA USUÁRIO - DIFERENTE DA SENHA DO ROOT



Servidor Debian

PARTE 7

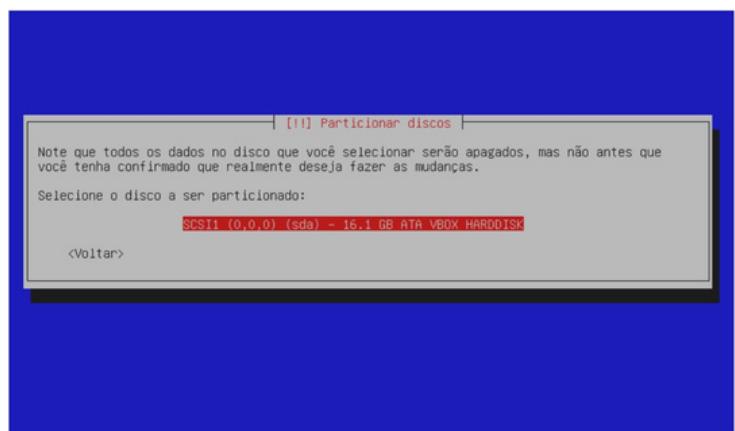
PARA INICIANTES A PRIMEIRA OPÇÃO



Servidor Debian

PARTE 8

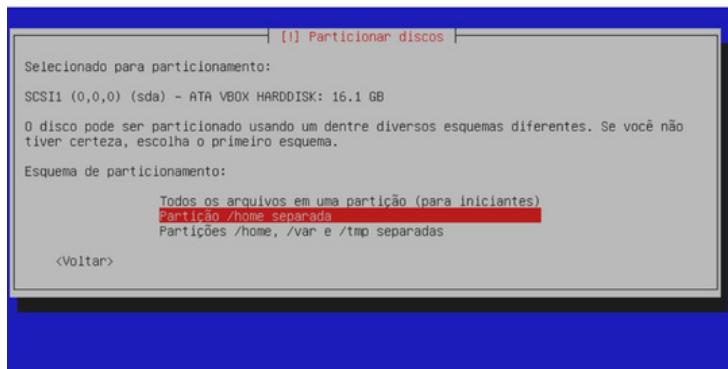
ENTER - DISCO A SER PARTICIONADO



Servidor Debian

PARTE 9

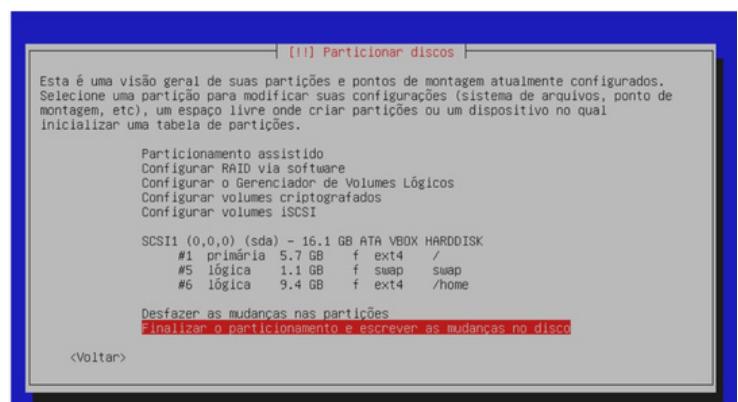
VAMOS DEIXA O DIRETÓRIO HOME SEPARADO



Servidor Debian

PARTE 10

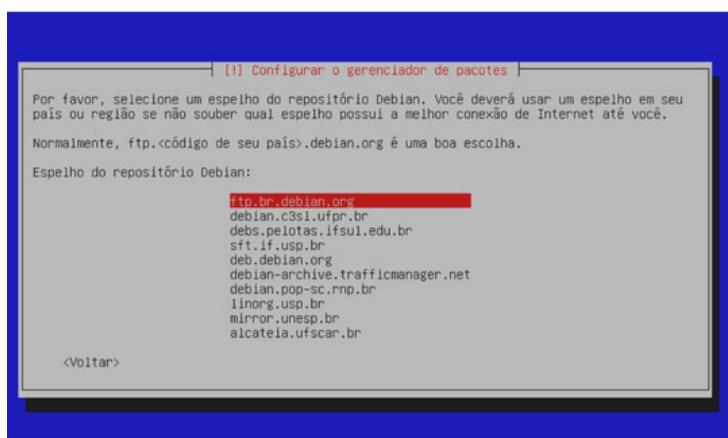
ESCREVER MUDANÇAS NO DISCO E CONFIRMAR "SIM"



Servidor Debian

PARTE 12

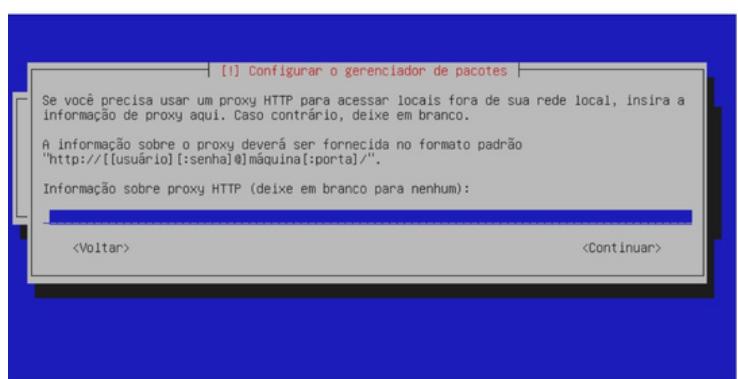
ESPELHO DO REPOSITÓRIO NORMALMENTE O PRIMEIRO "FTP.BR.DEBIAN.ORG"



Servidor Debian

PARTE 13

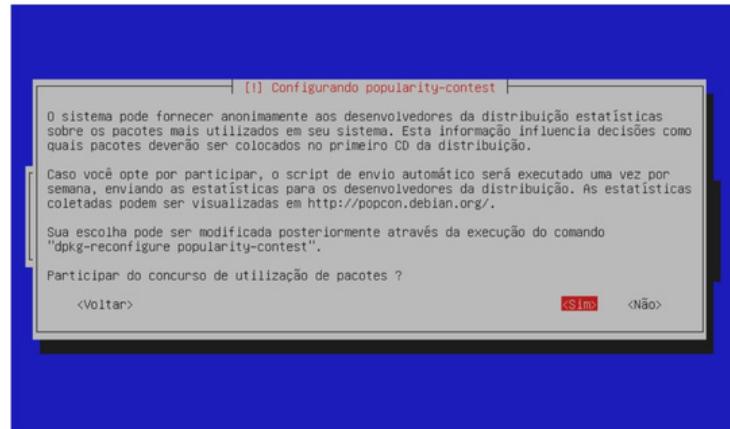
PODE DEIXAR EM BRANCO - CONTINUAR ...



Servidor Debian

PARTE 14

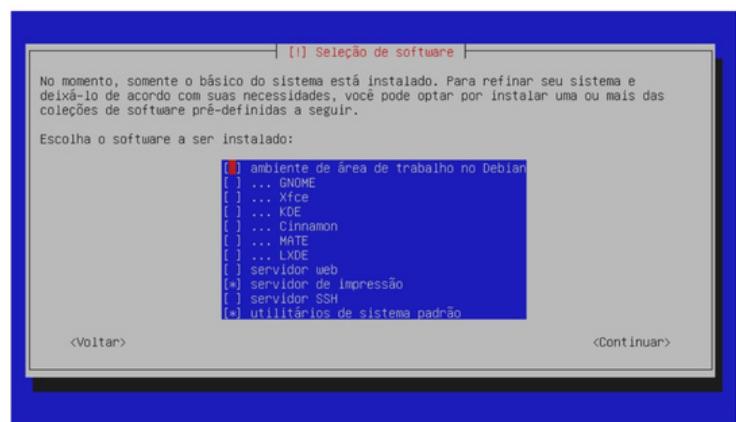
SIM PARA AJUDAR A COMUNIDADE



Servidor Debian

PARTE 15

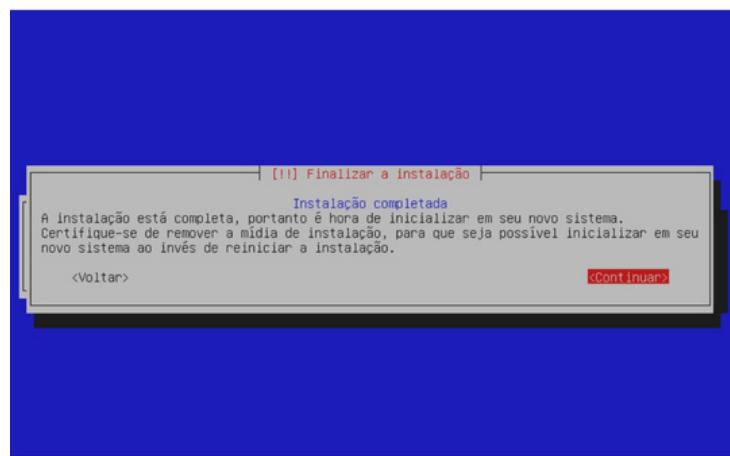
* SIGNIFICA QUE SERÁ INSTALADO - SÓ DEIXAR A ULTIMA OPÇÃO USAR TECLA ESPAÇO PARA SELECIONAR, NÃO INSTALAR MAIS NADA !



Servidor Debian

PARTE 16

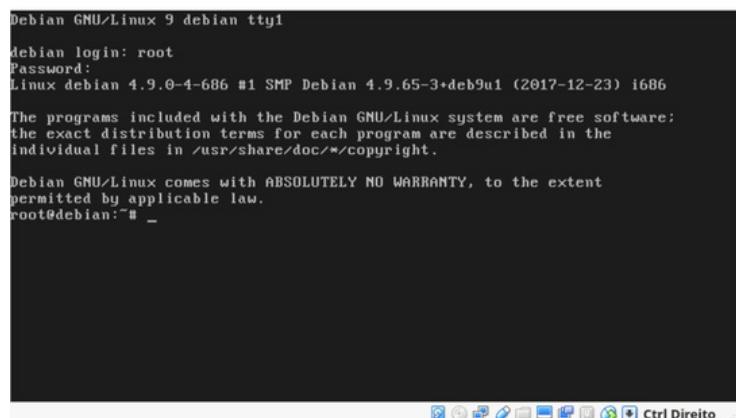
PRONTO SÓ REINICIAR - SE APARECER "INICIALIZAÇÃO DO GRUB" COLOQUE SIM



Servidor Debian

PARTE 17

LOGAR COM ROOT OU USUÁRIO CRIADO NA INSTALAÇÃO



Servidor Debian

PRONTO

Repare que na PARTE 15 você poderia ter escolhido instalar uma interface gráfica, entre elas o GNOME, Xfce, KDE, Cinnamon, MATE, LXDE.



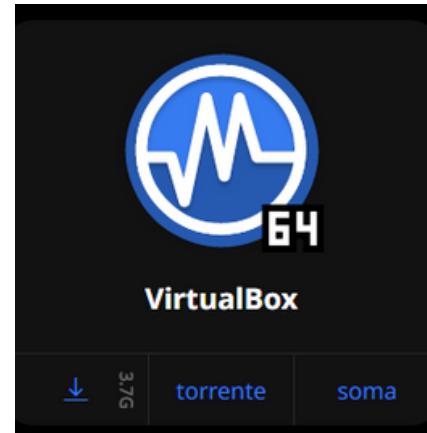
COMO INSTALAR KALI NA VM

Máquinas virtuais

- ✓ Funcionário de instantâneos
- ✓ Ambiente isolado
- ✓ Kernel Kali personalizado
- ✗ Acesso direto limitado ao hardware
- ✗ Requisitos de sistema mais altos

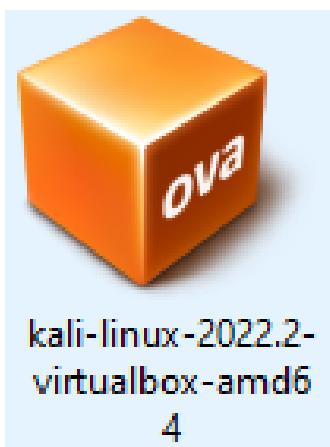
Imagens pré-criadas VMware e VirtualBox. Permitir uma instalação do Kali sem alterar o sistema operacional host com recursos adicionais, como instantâneos. Imagens Vagrant para rotação rápida também estão disponíveis.

Recommended



PARTE 1

Baixe essa imagem, basta digitar no google kali linux download



PARTE 3

Você terá esse arquivo salvo em seu computador



PARTE 4

Selecione a opção importar dentro do virtualbox.

← Importar Appliance Virtual

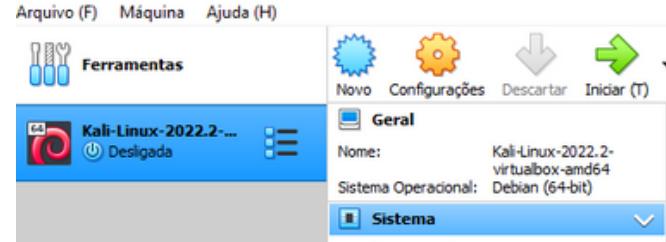
Appliance para importar

Especifique o origem de onde a appliance será importado. A origem pode ser um sistema de arquivos local para importar o arquivo OVF, ou um dos provedores de novos conhecidos para importar a VM.

Origem (O): Sistema de Arquivos Local

Selecione um arquivo de onde será importado o appliance virtual. O VirtualBox atualmente suporta importar appliances salvos no formato Open Virtualization Format (OVF). Para continuar, selecione o arquivo a importar da lista abaixo.

Arquivo (F): C:\Users\fernanda\Downloads\kali-linux-2022.2-virtualbox-amd64.ova



PARTE 5

Selecione o arquivo OVA
que você baixou e importe.

PARTE 6

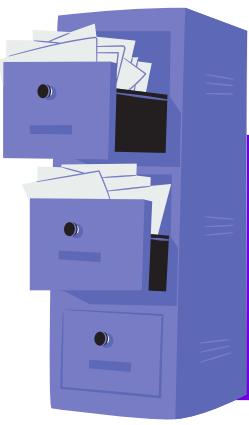
Iniciar



PRONTO

LOGIN: **kali**

SENHA: **kali**



ORGANIZAÇÃO DOS ARQUIVOS

TIPOS DE SISTEMAS

O sistema de arquivos é **como os arquivos são organizados e recuperados no disco**. Uma **partição** é um pedaço do disco (HD).



Por que usar sistemas de arquivos diferentes ?

Cada um possui as suas próprias características, como limitações, qualidade, velocidade, gerenciamento de espaço, entre outras. Isso faz diferença, por exemplo quando você gerencia um servidor com 100 Terabytes de dados armazenados.

1. Sistema de arquivos Ext, Ext2, Ext3 e Ext4

O sistema de arquivos Ext significa Extended File System . Foi desenvolvido principalmente para o MINIX OS . O sistema de arquivos Ext é uma versão mais antiga e não é mais usado devido a algumas limitações.

Ext2 é o primeiro sistema de arquivos Linux que permite gerenciar dois terabytes de dados. **O Ext3 é desenvolvido através do Ext2; é uma versão atualizada do Ext2** e contém compatibilidade com versões anteriores. A principal desvantagem do Ext3 é que ele não suporta servidores porque esse sistema de arquivos não suporta recuperação de arquivos e instantâneo de disco.

O sistema de arquivos **Ext4** é o sistema de arquivos mais rápido entre todos os sistemas de arquivos Ext, ext4 é o padrão. É uma opção muito compatível para os discos SSD (solid-state drive), e é o sistema de arquivos padrão na distribuição Linux.

2. Sistema de arquivos JFS

JFS significa Journaled File System e é desenvolvido pela IBM para AIX Unix. É uma alternativa ao sistema de arquivos Ext. Também pode ser usado no lugar do Ext4, onde a estabilidade é necessária com poucos recursos. É um sistema de arquivos útil quando a potência da CPU é limitada.

3. Sistema de Arquivos ReiserFS

ReiserFS é uma alternativa ao sistema de arquivos Ext3. Melhorou o desempenho e recursos avançados. Anteriormente, o ReiserFS era usado como o sistema de arquivos padrão no SUSE Linux, mas depois mudou algumas políticas, então o SUSE retornou ao Ext3.

4. Sistema de arquivos XFS

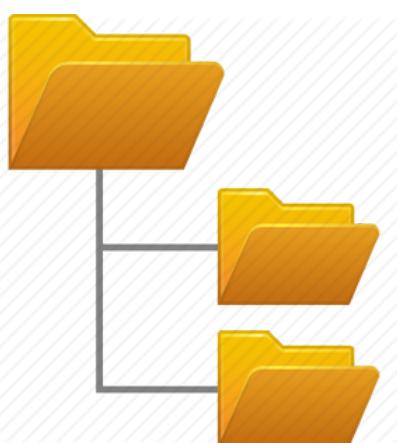
O sistema de arquivos XFS (Silicon Graphics 1994) foi considerado como JFS de alta velocidade, desenvolvido para processamento paralelo de E/S. A NASA ainda usa esse sistema de arquivos com seu **servidor de armazenamento alto** (servidor de 300+ Terabytes).

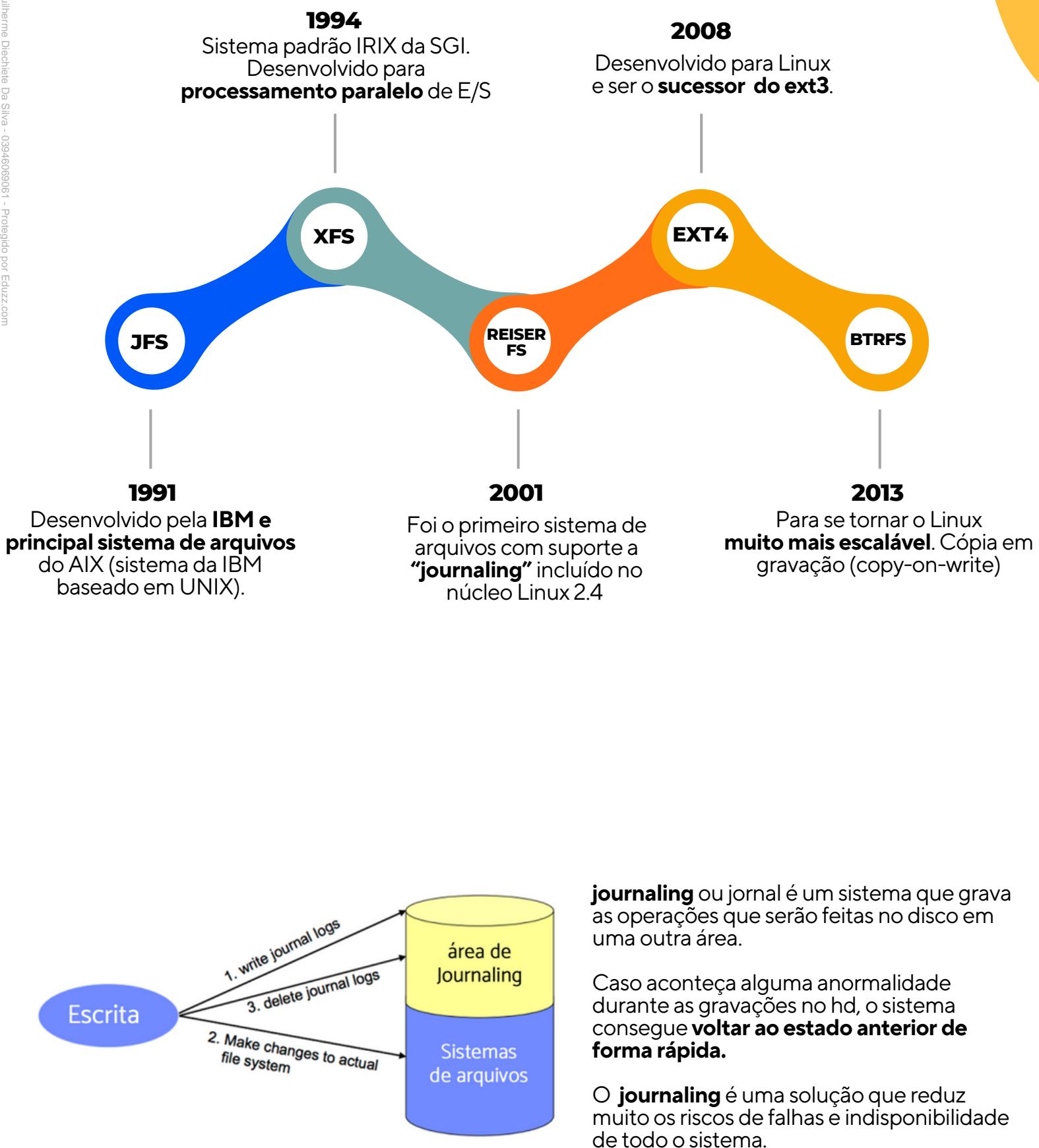
5. Sistema de Arquivos Btrfs

É um sistema de arquivos baseado no princípio **cópia em gravação** (copy-on-write). Criado pela oracle em 2007 - 2013 para tornar o Linux muito mais escalável, projetado para solucionar problemas como falta de agrupamento de discos ou volumes, snapshots e checksums.

6. Swap (Memória Virtual)

É uma partição criada dentro do disco(HD) que trabalha como memória ram quando necessário.

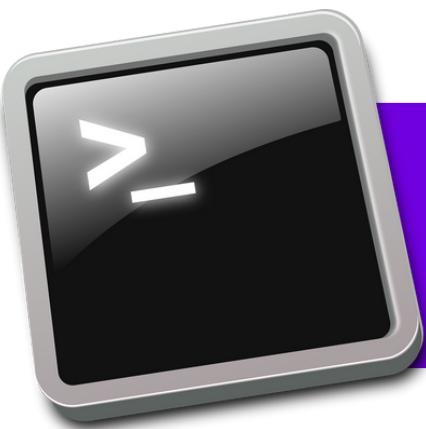




SISTEMAS LINUX

O terminal, as permissões e arquivos de
inicialização do sistema.





TERMINAL, USUÁRIOS E EDITOR DE TEXTO

TERMINAL

É um **interpretador de comandos**, o terminal permite que você instrua o computador a efetuar as operações que você deseja (como copiar um arquivo, ou iniciar a execução de um programa). Cada comando é, em geral, dado em uma linha digitada no terminal.

No Linux você tem **basicamente dois tipos** de usuários, o usuário comum que você criar e o usuário su (administrador/root) que já vem no sistema.

su: É o usuário root do sistema e possui **todos privilégios, acesso total** ao sistema, pode acessar, alterar ou deletar qualquer arquivo. Se você é iniciante só utilize esse usuário em **máquinas virtuais para estudos**, caso você delete algo não haverá prejuízo real.

comum: Limitado, sem privilégios.

Você precisa configurar uma senha para o usuário su (root/adm) do sistema, pode fazer isso com o comando abaixo.

sudo passwd: Sudo é uma **permissão de administrador** dada a um usuário comum para executar somente aquele comando, isso evita que administradores fiquem logados como su em máquinas reais, onde pode haver riscos.



\$: usuário comum (sem privilégios)

#: super usuários (**root/administrador**)

```
(kali㉿kali)-[~]
$ su
Password:
(kali㉿kali)-[/home/kali]
#
```

Os símbolos **\$** e **#** identifica os usuários.

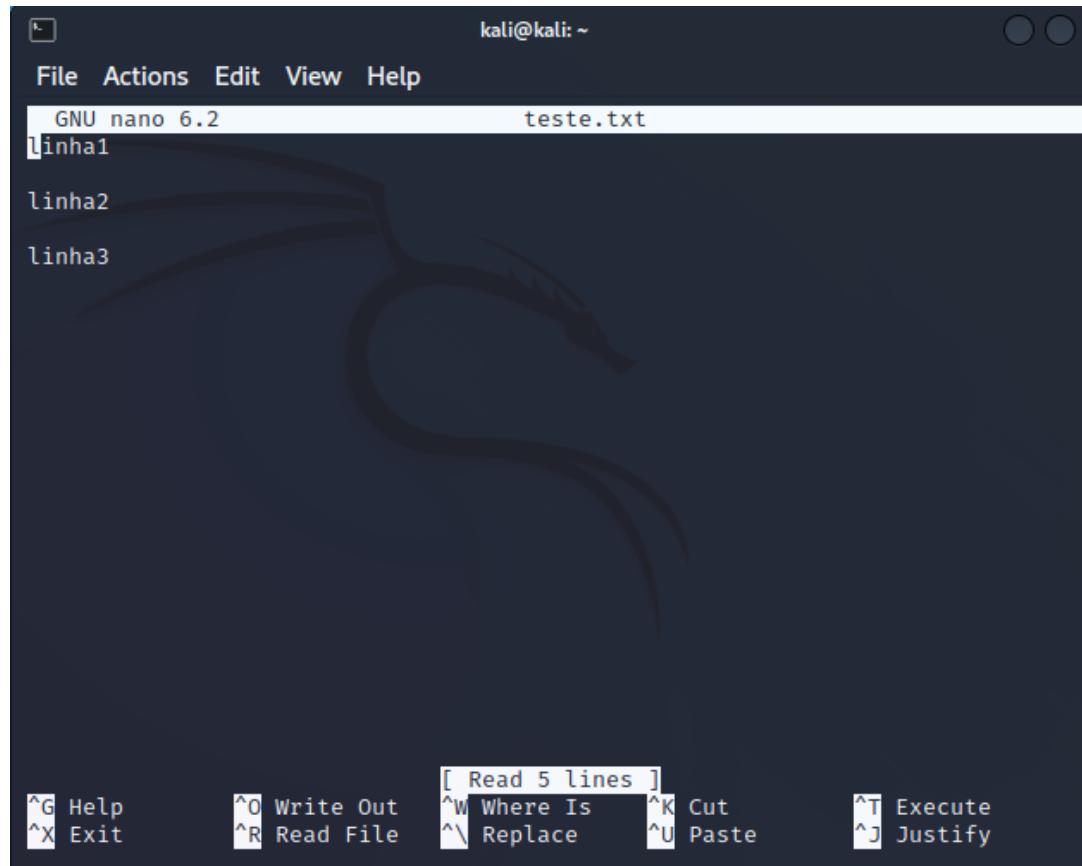
NANO

Em Linux se utiliza muito editores, porque tudo é um arquivo e as configurações são editadas nesses arquivos.

Para utilizar esse editor basta digita
nano + nome do arquivo

nano teste.txt: O arquivo teste.txt será aberto para você editar.

nano novo.txt: Cria um novo arquivo chamando novo.txt



CTRL + O: Para salvar

CTRL + X: Para sair

TIPOS DE ARQUIVOS NO LINUX

ARQUIVOS

No Linux tudo é arquivo, até os diretórios são tipos de arquivos. Um arquivo pode ser comum ou especial, na tabela abaixo mostra os tipos de arquivos e suas identificações.

- Arquivo comum
- d diretório

Os mais importantes para quem não possui conhecimento avançado

I link simbólico: Aponta para outro arquivo.

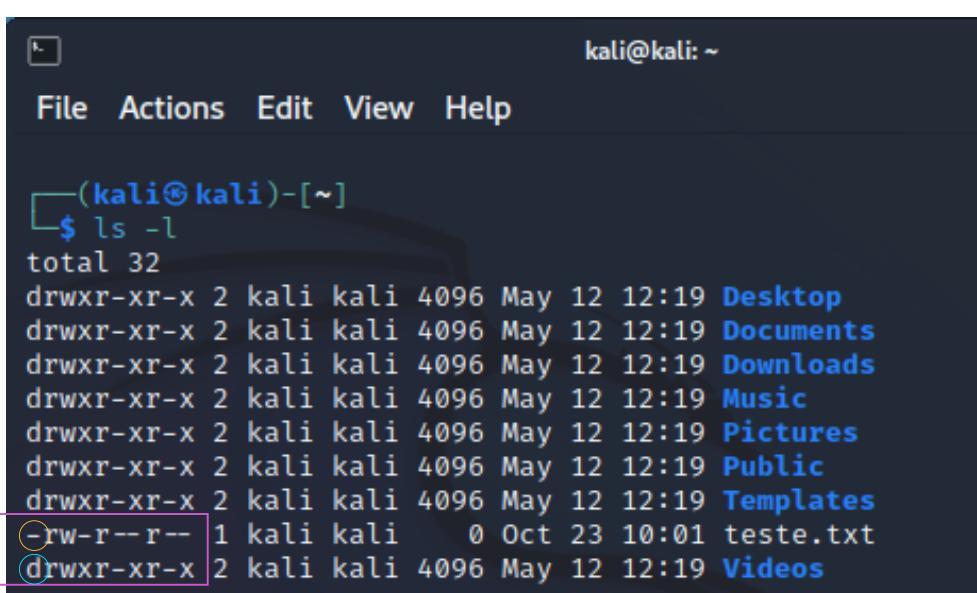
c dispositivo de caracteres: As operações de E/S são feitas de forma sequencial.

b dispositivo de blocos: Operações de E/S são feitas usando blocos de caracteres.

p pipe: Utilizado para comunicação entre processos.

s socket: Utilizado para comunicação entre processos.

veja



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ ls -l
total 32
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Desktop
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Documents
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Downloads
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Music
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Pictures
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Public
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Templates
-rw-r--r-- 1 kali kali 0 Oct 23 10:01 teste.txt
drwxr-xr-x 2 kali kali 4096 May 12 12:19 Videos
```

Arquivo comum (-)

Diretório (d)

O linux não enxerga o arquivo **como txt** porém utilizamos como forma didática.

No linux não faz diferença ter ou não a extensão **.txt**



PERMISSÕES NO LINUX

PROPRIEDADES

Cada arquivo e diretório no sistema Linux é atribuído a 3 tipos de grupos e permissões.

Um usuário é o proprietário do arquivo.

Por padrão, a pessoa que criou um arquivo se torna seu proprietário. Portanto, um usuário às vezes também é chamado de proprietário.

Um grupo de usuários pode conter vários usuários.

Todos os usuários pertencentes a um grupo terão as mesmas permissões de grupo do Linux para acessar o arquivo.

Qualquer outro usuário que tenha acesso a um arquivo.

Essa pessoa não criou o arquivo nem pertence a um grupo de usuários que poderia ser o proprietário do arquivo.

COMANDOS

chown fernando logs.txt: Altera o proprietário do arquivo para fernando.

chown fernando:grupo2 logs.txt: Altera o proprietário e o grupo.

chmod 777 teste.txt: Todas as permissões para todos os grupos.

chmod 760 teste.txt: Todas permissões para o dono do arquivo, leitura e escrita para quem está no grupo, e nenhuma permissão para outros usuários.



r: read (permissão de leitura) **4**

w: write (permissão de escrita) **2**

x: execute (permissão de execução) **1**

7 é a soma de todos,
dando assim todas
permessões

1 2 3
dono grupo outros
- rwx rwx rwx

permessões do arquivo dividido em
3 grupos (comando ls-l)

- tipo de arquivo (comum)

Grupo1 rwx: permessões do **dono**

Grupo2 rwx: permessões para usuários do **grupo**

Grupo3 rwx: permessões para **outros** usuários (qualquer um)

Todos os grupos

tem todas permessões

Permissões em valores decimais

0: --- (nenhuma permissão)

1: --x (somente execução)

2: -w- (somente escrita)

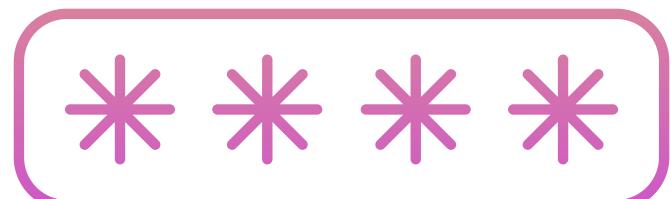
3: -wx (escrita e execução)

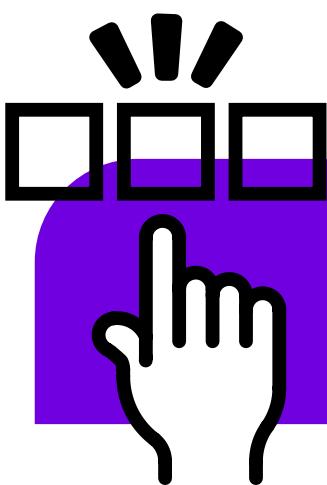
4: r-- (somente leitura)

5: r-x (leitura e execução)

6: rw- (leitura e escrita)

7: rwx (leitura, escrita e execução)





O QUE É O GRUB?

ARQUIVO

`cat /boot/grub/grub.cfg` ou `cat /boot/grub2/grub.cfg`

O GRUB é um gerenciador de boot, que pode carregar uma ampla variedade de sistemas operacionais.

Como o GRUB funciona?

Quando um computador é inicializado, a BIOS transfere o controle para o primeiro dispositivo de inicialização, que pode ser um HD, Pen drive ou qualquer outro dispositivo reconhecido pela BIOS.

O primeiro setor em um disco é chamado de **Master Boot Record (MBR)**. Esse setor tem apenas 512 bytes de comprimento e contém um pequeno pedaço de código chamado carregador de inicialização.

Por padrão, o código MBR procura a partição marcada como ativa e carrega seu setor de inicialização na memória e passa o controle para ela.

O GRUB substitui o MBR padrão por seu próprio código.



*Ordem da inicialização
BIOS => MBR => GRUB => KERNEL => Sistema Operacional*



TABELA DE MONTAGEM

ARQUIVO

`cat /etc/fstab`

É uma tabela (arquivo) que contém as instruções da montagem do próprio sistema.

O sistema vai ler essa tabela na **inicialização**, ela contém informações como:

- Dispositivo de boot (**/dev/sda1**)
- Ponto de montagem (**/**)
- Tipo do sistema de arquivos (**ext4**)
- **Opções:** ro, rw, auto, noauto, user, nouser, exec, noexec, sync, async
- **Dump:** backup ativo **1** backup não ativo **0**
- **Pass:** Ordem em qual o FSCK (Programa que verifica e repara) verifica as partições em busca de possíveis erros e correções. **1** É o dispositivo raiz **2** após o primeiro e **0** para desabilitar.

```
root@debian:~# cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options>      <dump>   <pass>
# / was on /dev/sda1 during installation
UUID=2f6ddfdf-d2c1-48c4-ba7c-7db6718402cd  /          ext4    errors=remount-ro 0       1
# swap was on /dev/sda5 during installation
UUID=b8724048-d249-40e8-a2b3-244de962ff60  none     swap    0        0        0
/dev/sr0          /media/cdrom0 udf,iso9660 user,noauto
root@debian:~#
```

A leitura dessa tabela não é algo tão fácil, não se preocupe com isso agora. No momento você só precisa saber que ela existe e que é lida na inicialização.

MÃO NO LINUX

Entendendo e operando comandos e arquivos.





REPOSITÓRIOS E PACOTES

REPOSITÓRIOS

São servidores que armazenam os pacotes, existe alguns tipos de servidores.

PACOTES

São programas, bibliotecas, papéis de parede, ícones, um pacote pode conter várias coisas. Os pacotes ficam dentro dos repositórios.

Você precisa de ferramentas para gerenciar esses pacotes (software), a que vamos utilizar agora é o APT (Advanced Packaging Tool).



O arquivo `source.list` **contém uma lista de endereços dos servidores**, que é de onde os pacotes (softwares) vêm.

Esse arquivo ficar em **`/etc/apt/sources.list`**

Esse comando exibe o que tem dentro do arquivo.
`cat /etc/apt/sources.list`

O arquivo terá esse formato:

```
deb http://deb.debian.org/debian bullseye main contrib
deb-src http://deb.debian.org/debian bullseye main
```

- **deb**: Repositório que guarda **pacotes binários**. (pré compilados).
- **deb-src**: Repositório que guarda pacotes fonte, que são os código fontes originais do programa.
- **http://deb.debian.org/debian**: Protocolo de acesso (http).
- **bullseye**: Nome da distribuição
- **main e contrib**: Tipos de servidores (repositórios).

```
# deb cdrom:[Debian GNU/Linux 9.6.0 _Stretch_ - Official amd64 NETINST 20181110-11:34]/ stretch main
#deb cdrom:[Debian GNU/Linux 9.6.0 _Stretch_ - Official amd64 NETINST 20181110-11:34]/ stretch main
deb http://ftp.it.debian.org/debian/ stretch main contrib non-free
deb-src http://ftp.it.debian.org/debian/ stretch main contrib non-free

deb http://security.debian.org/debian-security stretch/updates main contrib non-free
deb-src http://security.debian.org/debian-security stretch/updates main contrib non-free

# stretch-updates, previously known as 'volatile'
deb http://ftp.it.debian.org/debian/ stretch-updates main contrib non-free
deb-src http://ftp.it.debian.org/debian/ stretch-updates main contrib non-free
```

Ex 2

Debian strech

Tipos de repositórios

Existem alguns tipos de repositórios que são específicos, e você pode precisar deles, caso queira um software que não esteja no servidor oficial, isso acontece por exemplo, em casos de drivers específicos.

MAIN: Contém todos os pacotes que estão completamente de acordo com o Debian Free Software Guidelines, é o **repositório oficial do Debian**.

CONTRIB: Software livre que segue DFSG (Debian Free Software Guidelines) mas depende de software em non-free.

NON-FREE: Contém programas proprietários de código fechado. Todo tipo de software não livre que não segue o DFSG (Debian Free Software Guidelines)

UPDATES: Esse repositório recebe as atualizações de pacotes, com correções e melhorias.

BACKPORTS: O repositório backports oferece “pacotes backports”. O termo refere-se a um pacote de algum software recente, que foi recompilado para uma distribuição mais velha, geralmente para Stable.

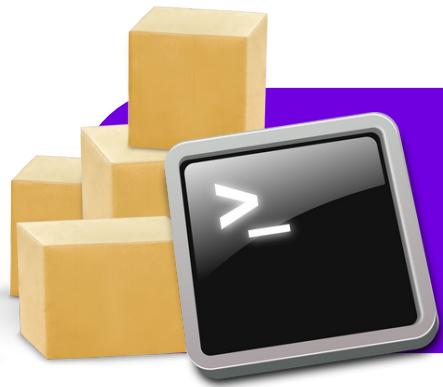
SECURITY: As atualizações de segurança não são hospedadas na rede habitual de espelhos do Debian, mas em security.debian.org.

PROPOSED-UPDATES: depois de publicada, a distribuição stable é atualizada em aproximadamente de dois em dois meses. o repositório atualizações-propostas é onde as atualizações esperadas são preparadas (sob a supervisão dos gerentes de versão estável).

DEBIAN MULTIMEDIA: Fornece pacotes para fins de edição de vídeo, imagem e codecs, entre outros.

Vamos supor que você precise adicionar um novo servidor(repositório) poi
esse outro repositório tem outros tipos de softwares que você precisa.

Então após você editar o arquivo sources.list é necessário atualizar a lista, com o comando apt update.



GERENCIAMENTO DE PACOTES

COMANDOS APT

O apt (Advanced Packaging Tool) é uma ferramenta para gerenciar pacotes.

apt update: Atualiza a lista de pacotes disponíveis.

apt upgrade: Atualiza todos os pacotes/softwares do seu sistema.

apt dist-upgrade: Atualiza a distro (sistema operacional)

apt install vim: Instalar um software chamado vim (editor).

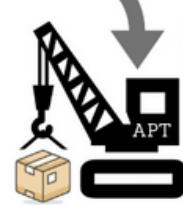
apt remove vim: Remove o pacote.

apt: autoclean: Remove os pacotes que não existem mais, e deixam “rastros”.

apt autoremove: Apaga pacotes abandonados.



GERENCIANDO REPOSITÓRIOS USANDO O APT



COMANDOS DPKG

Gerenciando pacotes com DPKG

O dpkg é o comando básico para lidar com pacotes Debian no sistema. Se você tem pacotes .deb, é com o dpkg que você instala ou analisa seu conteúdo. Mas este programa **tem apenas uma visão parcial do universo**, ele sabe o que está instalado no sistema, e o que for dado na linha de comando, mas **não sabe nada dos outros pacotes disponíveis**.

Assim, **ele vai falhar se uma dependência não for satisfeita**, um software pode depender de outro pacote para seu funcionamento completo.

Ferramentas como o apt, ao contrário, criará uma lista de dependências para instalar **tudo o mais automaticamente possível**.

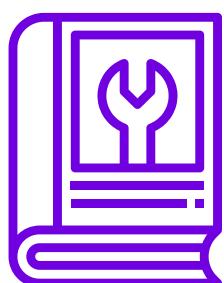
dpkg deve ser vista como uma ferramenta de sistema (nos bastidores), e apt como uma ferramenta mais próxima do usuário, que **superá as limitações das antigas**.

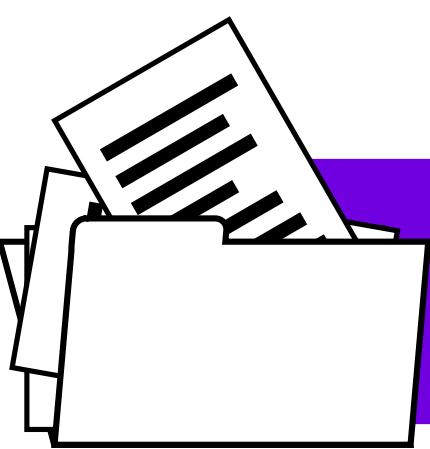
Estas ferramentas trabalham juntas, cada uma com suas particularidades, adequadas para tarefas específicas.

dpkg -i NomePacote.deb: Instalar um Pacote já baixado na máquina.
dpkg -P NomePacote.deb: Para remover completamente um pacote

dpkg -S Arquivo: Qual pacote instalou o arquivo.
dpkg -L Pacote.deb: Lista os arquivos instalados pelo pacote.

dpkg --contens Pacote.deb: Exibe o conteúdo do pacote
dpkg -l Pacote.deb: Estado do Pacote (Instalação/Problemas).





ARQUIVOS E NAVEGAÇÃO

EXIBINDO

ls: Lista os arquivos e diretórios.
ls -l: Lista os arquivos de forma detalhada.
ls -la: Lista todos os arquivos, incluindo os ocultos.

NAVEGAÇÃO

cd /home/Pasta1: Navega entre os diretórios.
cd .. : Um diretório anterior.
cd ~ : Vai para o diretório home do usuário.
pwd: Exibe na tela o diretório atual.

DIRETÓRIOS

mkdir Pasta1: Criar o diretório Pasta1

rm -r Pasta1: Deleta o diretório Pasta1 de forma recursiva.
rm -rf Pasta1: Deleta o diretório de forma recursiva e forçada

ARQUIVOS

touch teste.txt: Cria um arquivo chamado teste.txt

rm teste.txt: Deleta o arquivo teste.txt
rm -f teste.txt: Força para que o arquivo seja deletado.

cp teste.txt teste.bkp.txt: Cria uma cópia do teste.txt com o nome de teste.bkp.txt

mv descricao.txt relatorio.txt: Renomeia de descricao.txt para relatorio.txt

mv teste.txt Pasta1/arquivo.txt: Move o arquivo para outro diretório e renomeia ao mesmo tempo.





CONTAS DE USUÁRIOS E GRUPOS

ARQUIVOS

cat /etc/passwd: Exibir todos usuários do sistema.

cat /etc/group: Exibe os grupos.

COMANDOS

useradd fernando: Cria um novo usuário chamando fernando.

userdel fernando: Deleta uma conta de usuário.

passwd fernando: Define senha para o usuário.

passwd NomeUsuário: Muda a senha.

passwd -i NomeUsuário Mínimo de dias para a senha ser alterada.

passwd -l NomeUsuário: Bloqueia a conta do usuário.

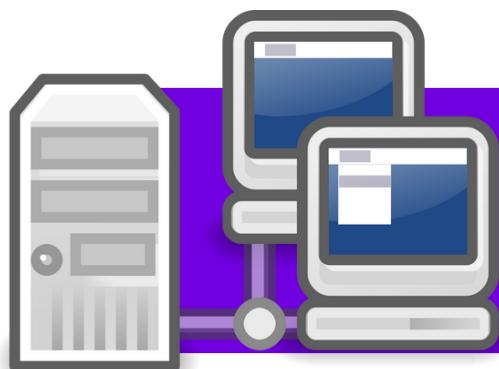
passwd -u NomeUsuário: Desbloqueia a conta de um usuário.

passwd -x NomeUsuário: Número de dias que a senha poderá ser utilizada.

groupadd alunos: Cria um novo grupo chamado alunos.

groupdel alunos: Deleta o grupo.

groupmod -n alunos profissionaisTI: Renomeia o grupo de alunos para profissionaisTI



ANÁLISE DA REDE

ARQUIVOS

cat /etc/hosts: Exibe o arquivo que possui a configuração do hostname

cat /etc/network/interfaces: Exibe o arquivo de configuração da interface de rede. No Linux é aqui que você configura a placa de rede.

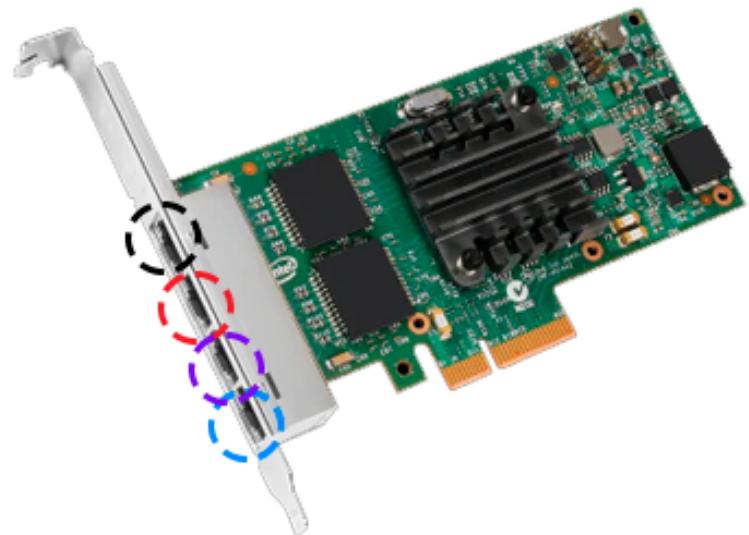
Interface **eth0**

Interface **eth1**

Interface **eth2**

Interface **eth3**

Pode ser que a nomenclatura seja **enp0s3**



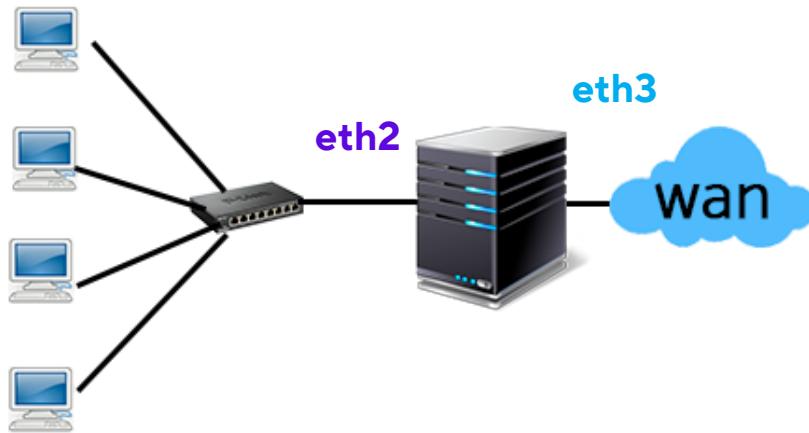
Você poderá **editar o arquivo** (`nano interfaces`) para realizar as **configurações de redes** nas interfaces específicas.

Modo estático

```
static
iface eth2 inet static
    address 192.168.1.10
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
```

Modo DHCP

```
dhcpc
auto eth2
iface eth2 inet dhcp
```



COMANDOS

ping 192.168.1.10: Verificar se um host está ativo.

hostname: Exibe qual é o nome da sua máquina na rede.

arp -a: Exibe a tabela ARP (É uma tabela que armazena os IPs e MACs de computadores que entram em contato com você).

ifconfig: Exibe o seu endereço IP e outras informações de redes.

ifconfig eth0: Status da interface de rede.

ifconfig eth0 down: Desabilitando interface de rede.

ifconfig eth0 up: Habilitando a interface de rede.

ifconfig eth0 192.168.1.15 netmask 255.255.255.0: Altera o IP da interface de rede.

iwconfig eth1: Exibe configurações da placa WI-FI

iwlist scan: Exibe as redes sem fio.

who: Mostra quem está atualmente conectado no computador

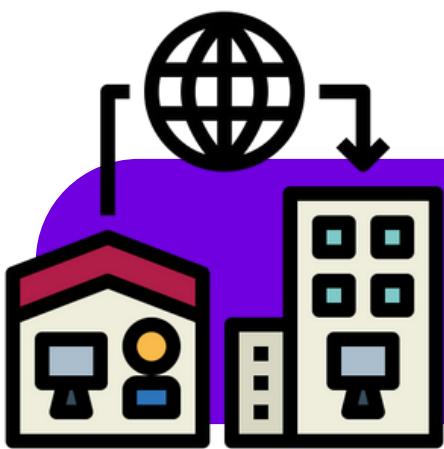
who -b: Mostra o horário do último boot do sistema

who -q: Mostra o total de usuários conectados aos terminais

route: Exibe a tabela de roteamento

host www.google.com: Descobre o endereço IP de um endereço.

wget --recursive www.NomeSite.com: Baixa um site inteiro.



ACESSO REMOTO SSH

SSH

Com o ssh você consegue fazer uma **conexão remotamente e gerenciar** os servidores remotamente.

É extremamente importante você aprender os comandos do Linux, em ambientes corporativos os servidores não possuem interface gráficas, teclados, mouses e monitores, **tudo é feito remotamente**. Porém caso queira você até consegue rodar uma interface gráfica remotamente.

Um servidor tem que ter somente o necessário para executar seu objetivo com segurança.

COMANDOS

apt install openssh-client: Instalação no client.

apt install openssh-server: Instalação no servidor.

ssh uol@192.168.0.1: Nome do usuário e endereço IP do servidor.

ssh -l root@IP-Servidor: Conectar como usuário root.



casa/trabalho
qualquer lugar, etc.



aws
site
sistema
etc.



ANÁLISE DO SISTEMA EM GERAL

COMANDOS

Comandos que exibem informações gerais do sistema.

df: Mostra o espaço livre/ocupado de cada partição

df -h: Tamanho dos arquivos e diretórios em GB

df -hT /home: Específico

df -T: Tipo de sistemas de arquivos

free: Mostra detalhes sobre a utilização da memória RAM do sistema

free -m: Mostra o resultado em Mbytes

free -t: Mostra uma linha contendo o total

uname -s: Exibe informações do Linux

uname -m: Exibe informações sobre a plataforma (x86_64).

uname -a: Exibe informações do kernel e todas outras.

lspci: Exibe o que está conectado no barramento PCI.

lsusb: Exibe o que está conectado nas saídas USB.

uptime: Há quanto tempo o sistema está ligado.

date: Data e hora do sistema.

cal: Exibe o calendário.

w: Quais usuários estão logados no sistema.

locate passwd: Lista arquivos que contenham o texto 'passwd'

compgen -c: Exibe todos os comandos do seu sistema.

reboot: Reinicia a máquina.

halt: Desliga a máquina.



ARQUIVOS COMPACTADOS

COMANDOS

O comando tar compactar e descompacta arquivos e diretórios, isso é útil para backups ou quando você precisa transferir arquivos e diretórios via ssh e precisa diminuir o tamanho do arquivo.

tar -cvzf Arquivos.tar.gz /home: Compressão do diretório home com **gz**

tar -cvjf Arquivos.tar.bz2 /home: Compressão do diretório home com **bz2**

tar -xvf Arquivos.tar.gz: Descompactado .gz

tar -xvf Arquivos.tar.bz2: Descompactado .bz2

tar -tvf Arquivos.tar.gz: Listar conteúdos do arquivo compactado .gz

tar -tvf Arquivos.tar.bz2: Listar conteúdos do arquivo compactado .bz2

OPÇÕES

c: Cria novo arquivo

z: Compressão **.gzip** + **Rápido compressão menor**

j: Compressão **.bz2** + **Demorado compressão maior**

v: Exibe o processo

f: Nome do arquivo

x: Extrair

ANÁLISE DOS PROCESSOS

COMANDOS

Processos é uma instância de um programa, em alguns casos um processo trava e você precisa matar ele ou descobrir quanto de CPU ela está consumindo.



Daemon: Um processo/programa que roda em segundo plano.



Processo zombie: Processo que terminou a execução, porém ainda se encontra na tabela de processos.

ps: Processo ativos no momento.

ps aux: Processos ativos de forma detalhada.

kill pid: Mata o processo pid (ID do processo).

killall proc: Mata todo os processos com o nome proc.

ps -u fernando: Processo de um usuário específico.

ps -aef -r: Processos que mais consomem CPU em ordem.

ps -aef -m: Processos que mais consomem memória em ordem.

pstree: Lista os processos em formato de árvore e relacionamento entre dependências.

top: Praticamente a mesma coisa que o comando ps.

top -T: Ordena processos de acordo com o tempo de execução.



GERENCIAMENTO DOS SERVIÇOS

SERVIÇOS

Serviços são programas que **rodam em segundo plano e que executam tarefas específicas**, como por exemplo o APACHE, que "transforma" a máquina em um servidor WEB, outro exemplo o SAMBA4 que "transforma" a máquina em um servidor de arquivos.

Um profissional em Linux deve usar esses serviços e comandos para **gerenciar e manter servidores e sistemas e execução** no dia a dia.

O servidor WEB está com problemas (OFF), o profissional em Linux então vai fazer uma inspeção para verificar e resolver o problema, como ?

Ele vai usar os comandos abaixo para descobrir os status dos serviços, para ativar, desativar, etc.

COMANDOS

systemctl start apache2: Inicia um serviço

systemctl stop apache2: Para um serviço

systemctl restart apache2: Reiniciar o serviço

systemctl status apache2: Estado de um serviço, ativou ou não

systemctl enable apache2: Inicia o serviço no Boot

systemctl disable apache2: Remove o serviço do Boot

ANÁLISE DE ARQUIVOS E MANIPULAÇÃO DE "TEXTO"

COMANDOS

cat sources.list: Visualiza o conteúdo de um arquivo.

cat sources.list | grep kali: Procura a palavra chave '**kali**' no arquivo. É muito importante você saber utilizar esse filtro, no linux lidamos com arquivos diariamente, **fazendo configurações editando os arquivos**, exemplo, vamos supor que você está em um arquivo de 3.000 caracteres como você encontra um determinado "argumento" porta ou IP ? **com o grep !**

```
(kali㉿kali)-[~/etc/apt]
$ cat sources.list | grep kali
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

INÍCIO >

cat teste1.txt > teste2.txt: Lê o conteúdo do teste1.txt e insere os dados no início do arquivo teste2.txt

FIM >>

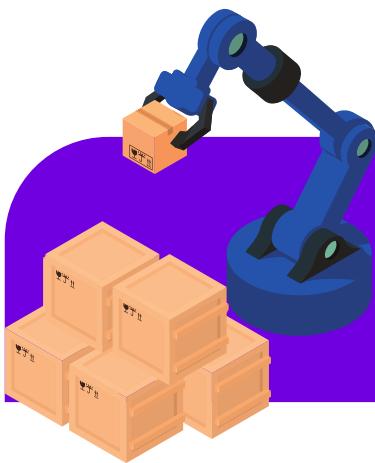
cat teste1.txt >> teste2.txt: Lê o conteúdo do arquivo teste1.txt e insere os dados no fim do arquivo teste2.txt

head -10 texto.txt: Exibe somente as 10 primeiras linhas do arquivo.

tail -10 texto.txt: Exibe somente as 10 últimas linhas.

wc texto.txt: Conta o número de linhas, palavras e bytes que o arquivo possui.

cat texto.txt | more: Quando o arquivo é muito grande pode-se utilizar o more. O more efetua uma pausa e permite que você pressione Enter ou espaço para continuar avançando (rolando) no arquivo sendo visualizado. Para sair do more pressione **q**.



AUTOMATIZANDO TAREFA E ROTINAS

AT

É possível você **agendar tarefas (at)** e **rotinas (cron)**, por exemplo um administrador precisa criar um backup toda sexta-feira às 2h através de scripts utilizando esses comandos é facilmente possível.

apt install at: Instala o at.

at now +2 min: Executa os comandos listados em 2 minutos.

at > comando 1

at > comando 2

at> comando 3

at -f comandos.txt 8:00 PM tomorrow: Agendamento para rodar os comandos dentro do arquivo comandos.txt amanhã às 8h da noite (Somente uma vez).

at -l: Verifica as tarefas agendadas.

at -r 11: Cancela a tarefa com ID 11

CRON

É uma ferramenta/tabela que permite programar a execução de comandos, diferente do at, no **cron você configura somente uma vez**.

O cron é um serviço do Linux que é **carregado durante o processo de boot** do sistema, e fica em **execução em segundo plano**.

O cron executa os comandos nas datas e horários especificados. Por exemplo, você poderia usar o cron para que o arquivo de log de um cliente fosse disponibilizado todos os dias às 21h.

Formato do arquivo cron

[minutos] [horas] [dias do mês] [mês] [dias da semana] [usuário] [comando]

Minutos: Informe números de 0 a 59

Horas: Informe números de 0 a 23

Dias do mês: Informe números de 0 a 31

Mês: Informe números de 1 a 12

Dias da semana: Informe números de 0 a 7

* Todos (todo momento)

Usuário: É o usuário que vai executar o comando (não é necessário especificá-lo se o arquivo do próprio usuário for usado)

Comando: Comando/Script que deve ser executado.

```
(kali㉿kali)-[~/etc]
└─$ cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |

# * * * * * user-name command to be executed
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6      * * 7    root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6      1 * *    root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
```

Exemplos:

[minutos] [horas] [dias do mês] [mês] [dias da semana] [comandos/script]

0 6,18 * * */bin/sh **backup.sh**

No agendamento acima ele vai rodar um **script que vai fazer um backup** de banco de dados duas vezes por dia (**às 6 da manhã e às 18h da tarde**).

O script já está criado, "é outra coisa"

0 0 ** 2 */bin/sh **backup.sh**

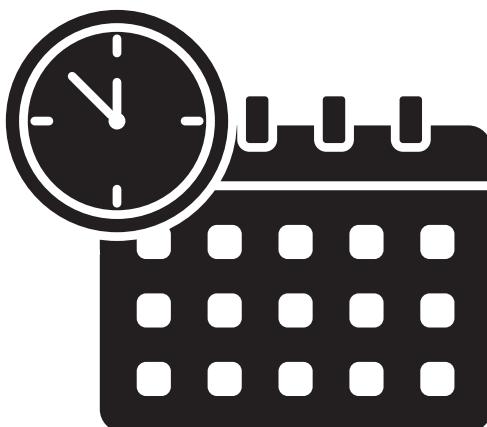
Backup de banco de dados à meia noite de toda terça-feira.

crontab -e: Serve para editar o arquivo atual do crontab, criando assim rotinas, veja que o arquivo abaixo não contém nenhuma rotina configurada.

```
GNU nano 7.2
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# Home
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
```

crontab -l: Este comando mostra o conteúdo atual do crontab.

crontab -r: Remove o arquivo atual do crontab.



cat /etc/crontab
crontab -e

RESUMO

at: Agendamento de uma única tarefa.

cron: Rotinas "coisas" que o adm precisa fazer diversas vezes na semana, mês ou dia.



SETORES DEFEITUOSOS

BAD BLOCKS

São setores do HD que **estão com algum defeito**, quando um sistema começa apresentar lentidão ou muitos travamentos pode ser bad blocks.

- **Software:** Problemas causados provavelmente por outros programas, vírus ou desligamento incorreto, bem mais chances de recuperar.
- **Hardware:** Batida, poeira, etc. Complexo e poucas chances de recuperar.

COMANDOS

fdisk -l: Visualizar as partições

badblocks -vs /dev/sda1 > badblock.txt: Identifica os setores ruins e cria um arquivo como essas identificações.

e2fsck -l badblock.txt /dev/sda1: Tenta corrigir os setores ruins em sistemas ext2, ext3 e ext4

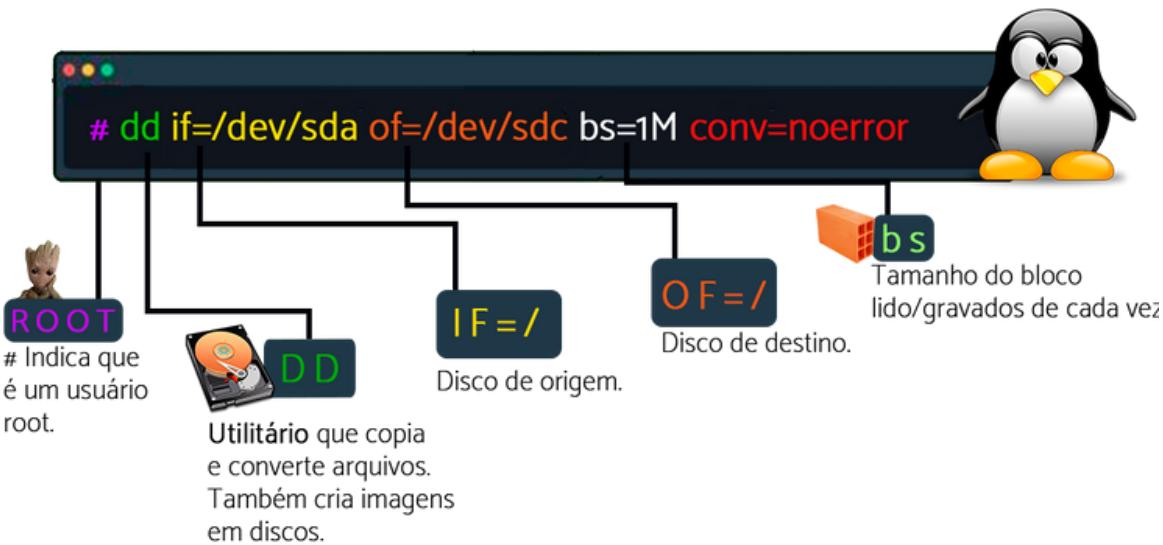
```
[root@kali] ~
# badblocks -vs /dev/sda1 > badblock2.txt
Checking blocks 0 to 82884607
Checking for bad blocks (read-only test):  0.00% done, 0:00 elapsed. (0/0/0
█ 2.99% done, 0:14 elapsed. (0/0/0 errors)
```



CLONAGEM DE DISCOS

COMANDO

dd if=/dev/sda of=/dev/sdc bs=1m: Fazendo uma clonagem de HDs com o programa dd.



O comando dd é uma ferramenta de linha. Seu objetivo principal é converter e copiar arquivos. Por outro lado, existem diversas opções interessantes para esse comando, como:

- Fazer backup e restauração de todo o disco rígido ou partição;
- Fazer backup da MBR (Master Boot Record);
- Criar arquivos para fazer imagens de inicialização. Pendrive bootável, por exemplo;
- Recuperar dados de um disco defeituoso para uma imagem ou outra mídia de armazenamento;

A opção 'noerror' permite que a ferramenta continue copiando os dados mesmo que encontre erros.

RESUMINDO O BÁSICO

Aquele resumão para salvar todo iniciante.





PRECISA APRENDER O BÁSICO MUITO RÁPIDO ?

O BÁSICO

Um resumo dos principais comandos do Linux, isso serve para você que precisa aprender pelo menos os comandos básicos de forma rápida. **Pode imprimir.**



\$: usuário comum (sem privilégios)

#: super usuários (**root**/administrador)



ls: listar

ls -l: listar detalhes



cd: navega entre os diretórios

cd ~ : ir para diretório /home

cd .. : voltar para uma diretório acima



touch: criar arquivo

> : criar arquivo

cat: exibe o conteúdo de um arquivo



mkdir: criar pastas

rm: excluir (diretórios/arquivos)

rmdir: excluir diretórios **vazios**

rm -f: força excluir

rm -rf: força excluir pastas



mv: mover ou renomear

cp: copiar arquivos ou diretórios



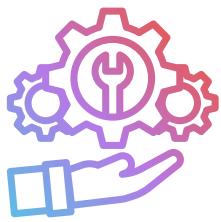
pwd: onde estou? diretório atual
clear: limpa tela do terminal



df: espaço em disco
df -h: espaço em disco com leitura legível para humanos



free: espaço de memória
free -h: espaço de memória de forma mais legível



apt-get install nomedopacote
apt-get remove nomedopacote
apt-get update: atualizar repositórios
apt-get upgrade: atualizar sistema



dpkg -i: nomedopacote.deb
dpkg -l: listar pacotes instalados



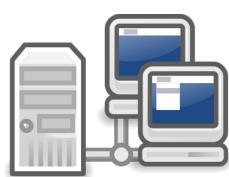
uname -a: informações do Kernel
uptime: há quanto tempo o sistema está ativo
who: quem está conectado na máquina



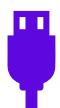
adduser: cria usuários ou grupos (-group) no sistema
userdel: remove usuário
groupdel: remove um grupo



passwd: mudar senha do usuário atual
passwd username: mudar a senha do usuário especificado



ifconfig: seu endereço IP e informações de rede
route: tabela de rotas IP
iwlist scan: exibe as redes sem fio



lspci: o que está conectado no **barramento PCI**
lsusb: o que está conectados nas **saídas USB**



tar -cvzf Arquivos.tar.gz: Compressão **gz**
tar -cvjf Arquivos.tar.bz2: Compressão **bz2**

z: Tipo gz
j: Tipo bz2



tar -xvf Arquivos.tar.gz: Descompactado **.gz**
tar -xvf Arquivos.tar.bz2: Descompactado **.bz2**

x: Extrai



ps: visualizar processos atuais do usuário
ps aux: exibe todos os processos de todos os usuários

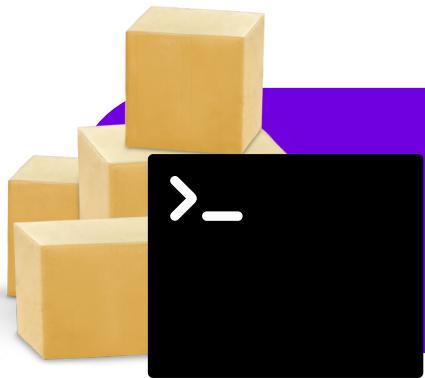


halt: desligar o computador
reboot: reiniciar o computador



systemctl start httpd.service: Inicia um serviço
systemctl stop httpd.service: Para um serviço
systemctl restart httpd.service: Reinicia um serviço

systemctl status httpd.service: Estado de um serviço
systemctl enable httpd.service: Inicia o serviço no Boot
systemctl disable httpd.service: Remove o serviço do Boot



CONSIDERAÇÕES FINAIS

E AGORA ?

Acredito que esse e-book tenha te ajudado a entender como o linux funciona e seus comandos de uma forma diferente dos materiais que tem por ai, tentei ser o mais direto possível e didático, para que você que necessita ou **deseja aprender rápido não perca tempo com detalhes** que muitas vezes não é utilizado em ambientes de trabalho ou em provas.



HACKER ÉTICO

PASSO A PASSO

- ✓ DOMINE O LINUX
- ✓ COMO ENCONTRAR FALHAS
- ✓ HACKEANDO DO ZERO

- ✓ CRIE ROBÔS HACKING
- ✓ ACESSE REDES WI-FI
- ✓ TENHA O PODER DE ATAQUE

QUERO SABER MAIS !

29

PERGUNTAS

Para você que curti testar seus conhecimentos
após um estudo.





EXERCÍCIOS 29 PERGUNTAS

SEÇÃO 1: ARQUITETURA DO SISTEMA

1) Qual é o papel do Kernel no sistema operacional Linux?

- a)** Gerenciar os recursos de hardware e software do sistema
- b)** Executar aplicativos em segundo plano
- c)** Intermediar a comunicação entre o usuário e o sistema operacional
- d)** Todos os anteriores

2) Pode se dizer que Kernel é o coração do sistema ?

- a)** Verdadeiro
- b)** Falso

3) Uma distribuição Linux é ?

- a)** Comando
- b)** Servidor
- c)** Sistema operacional
- d)** Nenhuma das anteriores

4) Uma distro derivada é um sistema operacional específico ?

- a)** Verdadeiro
- b)** Falso

5) No sistema operacional Linux você pode optar pela interface gráfica que vai utilizar ?

- a)** Verdadeiro
- b)** Falso

6) Qual é o sistema de arquivos padrão do Linux ?

- a)** NTFS
- b)** FAT32
- c)** EXT4
- d)** HFS+

7) Qual é a finalidade do GRUB ?

- a)** Gerenciar as configurações de rede do sistema
- b)** Inicializar o sistema operacional
- c)** Proteger o sistema contra malware
- d)** Configurar o ambiente de trabalho do usuário

8) O arquivo não tem fstab tem as instruções de montagem do sistema ?

- a)** Verdadeiro
- b)** Falso

SEÇÃO 2: COMANDOS GNU E UNIX

9) O terminal é um interpretador de comandos ?

- a)** Verdadeiro
- b)** Falso

10) Qual é o comando para exibir o diretório atual ?

- a)** cp
- b)** ls
- c)** cd
- d)** pwd

11) Qual é o comando para criar um diretório no Linux ?

- a)** rm
- b)** mkdir
- c)** touch
- d)** mv

12) Qual é o comando para exibir o conteúdo de um arquivo de texto ?

- a)** free
- b)** grep
- c)** cat
- d)** head

13) Qual comando exibe o espaço do disco ?

- a)** mount
- b)** free -m
- c)** tail
- d)** df-h

SEÇÃO 3: DISPOSITIVOS, SISTEMAS DE ARQUIVOS E GERENCIAMENTO DE ARMAZENAMENTO

14) Sistemas de arquivos é a forma como os arquivos são organizados no disco ?

- a)** Verdadeiro
- b)** Falso

15) Cada sistema de arquivos possui suas próprias características ?

- a)** Verdadeiro
- b)** Falso

16) Qual é o comando para listar as partições do disco rígido no Linux ?

- a)** format
- b)** fdisk
- c)** chkdsk
- d)** diskpart

17) Qual é o comando para montar uma partição do disco rígido no Linux ?

- a)** mount
- b)** umount
- c)** format
- d)** fdisk

SEÇÃO 4: ADMINISTRAÇÃO DE SISTEMA

18) Qual é o comando para listar os processos em execução no Linux ?

- a) all
- b) top
- c) kill
- d) ps

19) Qual é o comando para listar as interfaces de rede em um sistema Linux ?

- a) ipconfig
- b) ifconfig
- c) netstat
- d) ping

20) Qual é o arquivo de configuração das interfaces de rede ?

- a) /etc/fstab
- b) /etc/passwd
- c) /etc/network/interfaces
- d) /etc/iptables

21) Qual comando exibe as redes wi-fi ?

- a) who
- b) iwconfig
- c) iwlist scan
- d) route

22) No ssh faz conexão remota e gerencia servidores remotamente ?

- a)** Verdadeiro
- b)** Falso

23) O cron não permite programar tarefas repetitivas e rotineiras ?

- a)** Verdadeiro
- b)** Falso

24) O que são badblocks ?

- a)** Setores do disco bons
- b)** Software de verificação de disco
- c)** Setores do disco ruins
- d)** Arquivos do disco

25) Qual comando posso usar para clonar discos inteiros ?

- a)** ifconfig
- b)** mount
- c)** df -f
- d)** dd

SEÇÃO 5: SEGURANÇA

26) Qual é o comando para alterar a senha de um usuário no Linux ?

- a) chpasswd
- b) su
- c) passwd
- d) usermod

27) Qual é o comando para verificar o status do serviço SSH em um sistema Linux ?

- a) service ssh status
- b) systemctl status ssh
- c) netstat -an | grep 22
- d) Todos os anteriores

28) Qual o caractere é utilizado para mostrar que você está logado como root ?

- a) \$
- b) %
- c) *
- d) #

29) O usuário root possui quais permissões ?

- a) Edição
- b) Visualização mas não edição
- c) Nenhuma permissão
- d) Todas as permissões possíveis, acesso total

RESPOSTAS GABARITO

1) a
2) a
3) c
4) a
5) a
6) c
7) b
8) b
9) a
10) d

11) b
12) c
13) d
14) a
15) a
16) b
17) a
18) d
19) b
20) c

21) c
22) a
23) b
24) c
25) d
26) c
27) d
28) d
29) d



HACKER ÉTICO

PASSO A PASSO

- ✓ DOMINE O LINUX
- ✓ COMO ENCONTRAR FALHAS
- ✓ HACKEANDO DO ZERO

- ✓ CRIE ROBÔS HACKING
- ✓ ACESSE REDES WI-FI
- ✓ TENHA O PODER DE ATAQUE

QUERO SABER MAIS !