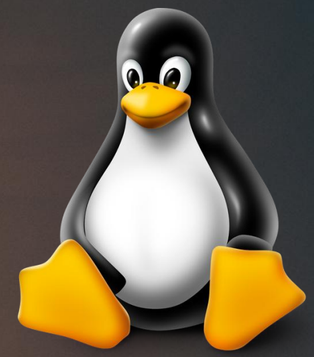
BASETI



LINUX

For Cybersecurity

MARÇO - 2025

treinamento.basetic.com.br

Sobre a BaseTI

A Base TI é uma empresa líder em soluções de tecnologia da informação especializada em cibersegurança e treinamentos avançados. Com sede em Brasília e atuação em todo o território nacional, oferece serviços de proteção digital abrangentes, incluindo avaliação de vulnerabilidades, implementação de soluções de segurança, monitoramento 24/7 e conformidade regulatória. Seus treinamentos Linux cobrem desde níveis básicos até avançados, com preparação para certificações internacionais.

CEO

Especialista em segurança cibernética, atuando com a orquestração de tecnologias gerando valor para os clientes e parceiros. Profissional experiente e com certificações como CEH, Comptia Pentest+, EHF da Exin e LPI.

Módulos

Iniciando com Linux

Aprendendo a estrutura do Linux, desde a instalação e o Sistema de arquivos, comandos básicos, encontrando arquivos, gerenciar serviços e encontrar instalar e remover programas.

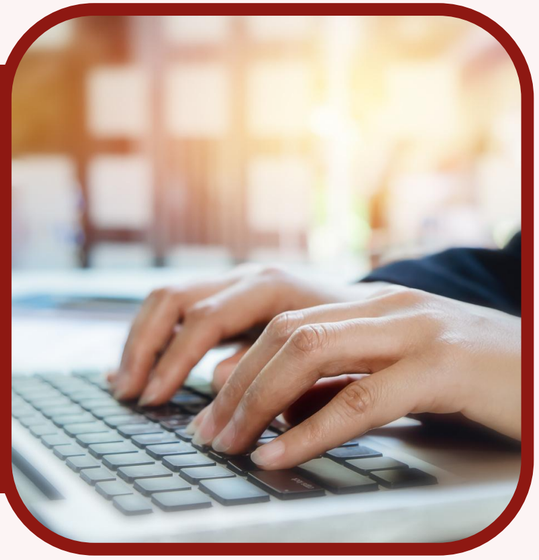
Linha de Comando

Aprender sobre o ambiente do shell, piping e redirecionamento, procurando textos, editando arquivos, gerenciando processos, monitorando arquivos e comandos, baixando arquivos.

Customizando o Shell

Trabalhando com o Shell, utilizando alias, customização persistente.

Módulos



Ferramentas

Aprender a conectar em portas TCP/UDP, trabalhar com netcat para administração e transferência de arquivos, cenários de bind e reverse shell. Trabalhar com Socat. Utilizar o Wireshark.

PowerShell e Powercat

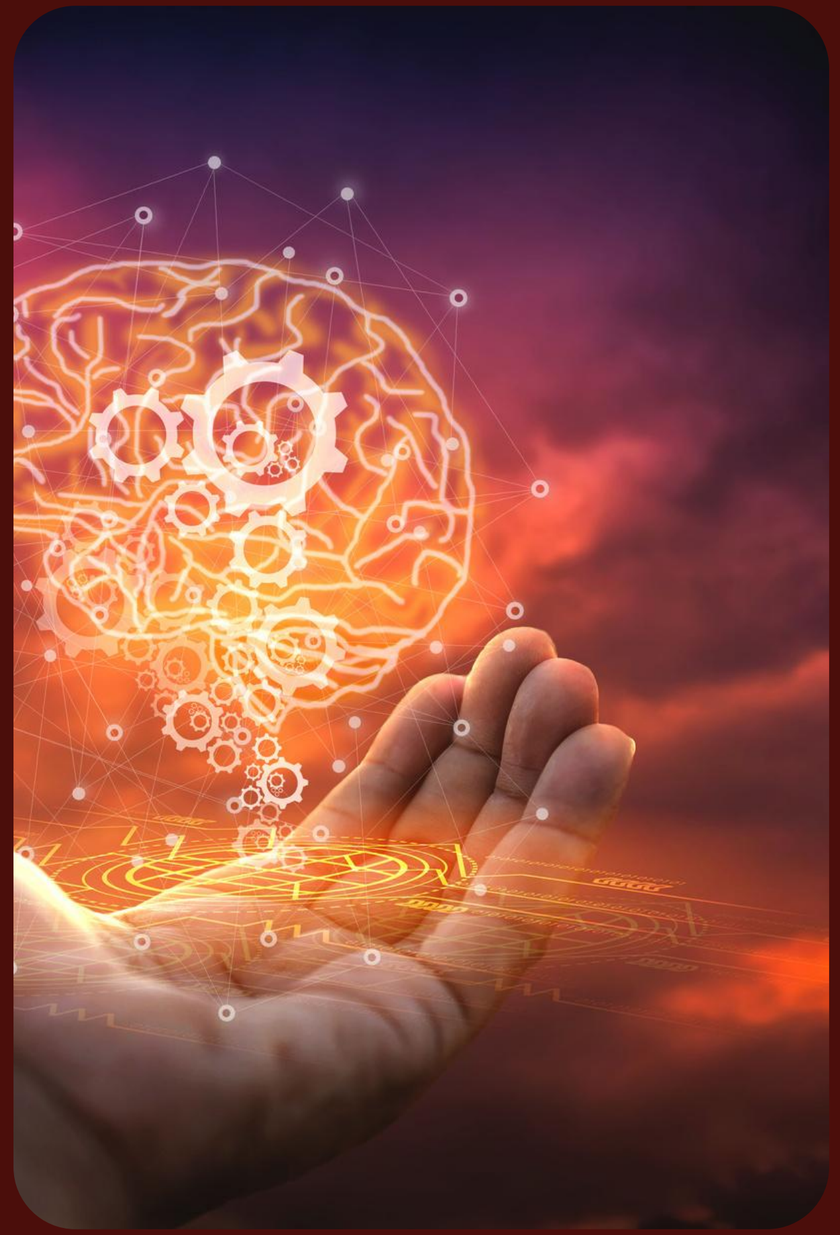
Aprender a trabalhar com o PowerShell e Powercat – transferir arquivos, reverse e bind shells.

Shell Scripting

Utilizar shell scripting, aprender sobre variáveis, argumentos, estruturas condicionais e funções. Exemplos práticos.

Módulo 0

ATUAR COM CYBERSECURITY



Analista de Segurança

Na função de Analista de Segurança (júnior) você será um especialista em Triagem. Monitorando os logs de eventos e alertas. Responsabilidades:

- Monitorar e investigar os alertas (SOC 24 X 7)
- Configurar e gerenciar as ferramentas de segurança (Linux)
- Desenvolver e implementar assinaturas básicas de IDS
- Participar de grupos de trabalho e reuniões do SOC
- Criar tickets e escalar os incidentes de segurança para o Nível 2 e o líder da equipe.

Qualificações

- 0-2 anos de experiência com Operações de Segurança
- Conhecimento básico de Redes
- Sistemas Operacionais (**Linux** e Windows)
- Aplicações Web (Protocolos)
- Habilidades de script/programação são um diferencial
- Docker

SOC

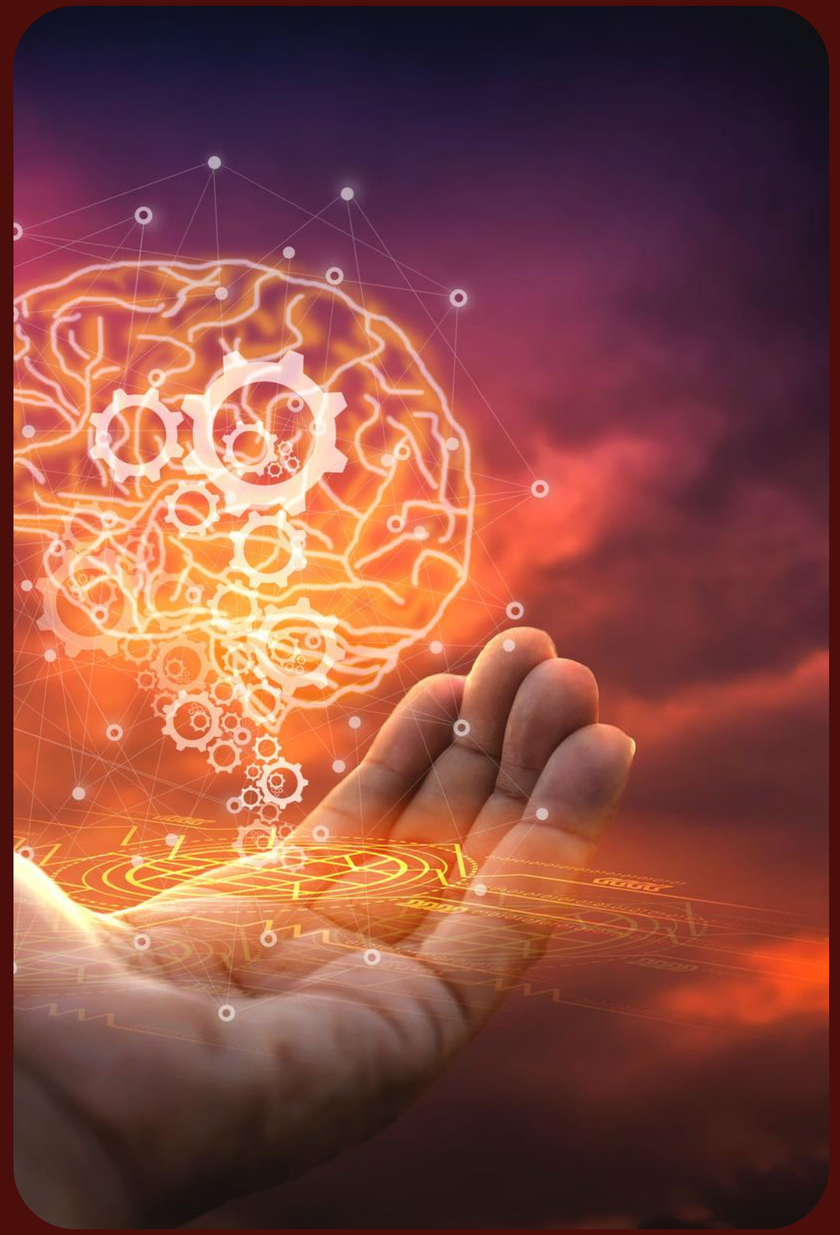

ANALISTA DE SEGURANÇA JUN IOR
(TIER 1)
TRIAGEM
Monitora logs e eventos de tráfego de redes
Trabalha nos tickets e fecha os alertas
Realiza investigações básicas e mitigações
ANALISTA DE SEGURANÇA DE OPERAÇÕES
(TIER 2)
INCIDENT RESPONDER
Foca em investigações, análises e remediações mais profundas.
Threat Hunting
Monitora e resolve alertas mais complexos
ANALISTA DE SEGURANÇA DE OPERAÇÕES
(TIER 3)
THREAT HUNTER
Trabalha em investigações mais avançadas
Executa busca avançada de ameaças e pesquisa de adversários
Realiza análise reversa de malware

Objetivo

A idéia aqui é desenvolver suas capacidades com Linux para, conforme exposto, configurar e gerenciar ferramentas de segurança, desenvolver assinaturas básicas de IDS e iniciar na construção de conhecimento para criar scripts para automação e resolução de problemas. Outro objetivo é desenvolver a capacidade de resolver problemas do dia-a-dia.

Módulo 1

INICIANDO COM O LINUX



Linux

Saber utilizar o Linux é um diferencial significativo para profissionais de Cybersecurity. Ele não apenas fornece as ferramentas e o ambiente necessários para realizar tarefas de segurança eficazes, mas também oferece uma compreensão profunda dos sistemas que muitas vezes são alvos de ataque.

Para atuar em Cybersecurity é altamente recomendável investir tempo no aprendizado e na prática com sistemas Linux, explorando suas capacidades de segurança e desenvolvendo habilidades em administração de sistemas Linux.

As principais ferramentas livres são baseadas em sistemas operacionais usando Linux como o Kali Linux, Parrot dentre outros.

1.1 Instalação do Linux

Qual distribuição Linux utilizar? Darei 3 opções:

- Debian 12
- **Ubuntu Server LTS**
- **Kali Linux**

Virtualizadores:

- **VirtualBox** - Recomendado
- VMWare Workstation

Instalação do Linux

- Entender sobre a instalação!
- Planejamento inicial – Qual finalidade desse novo sistema?
- Recursos computacionais – memória, disco, CPU´s
- VM pronta para Download – Problema de Espaço em Disco.

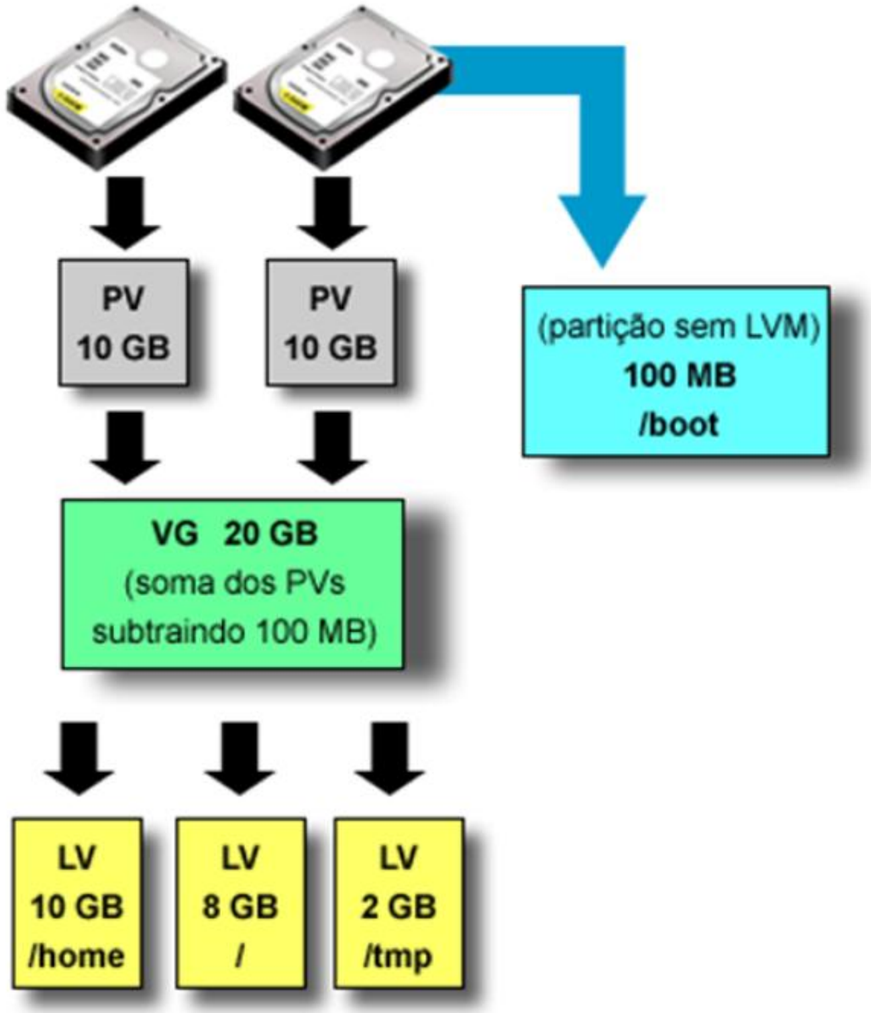
- https://drive.google.com/file/d/1pSBYQtMjfbEt6nTl_mQtYWRC1glMj02n/view?usp=sharing

1.2 Utilizando LVM

LVM é a sigla para Logical Volume Manager ou Gerenciador de Volume Lógico.

- Physical Volume – PV – Volume Físico
- Volume Group – VG
- Logical Volume

LVM



Disco de 40 GB

/ - 3 GB

Swapp – 2 GB

/tmp – 256 MB

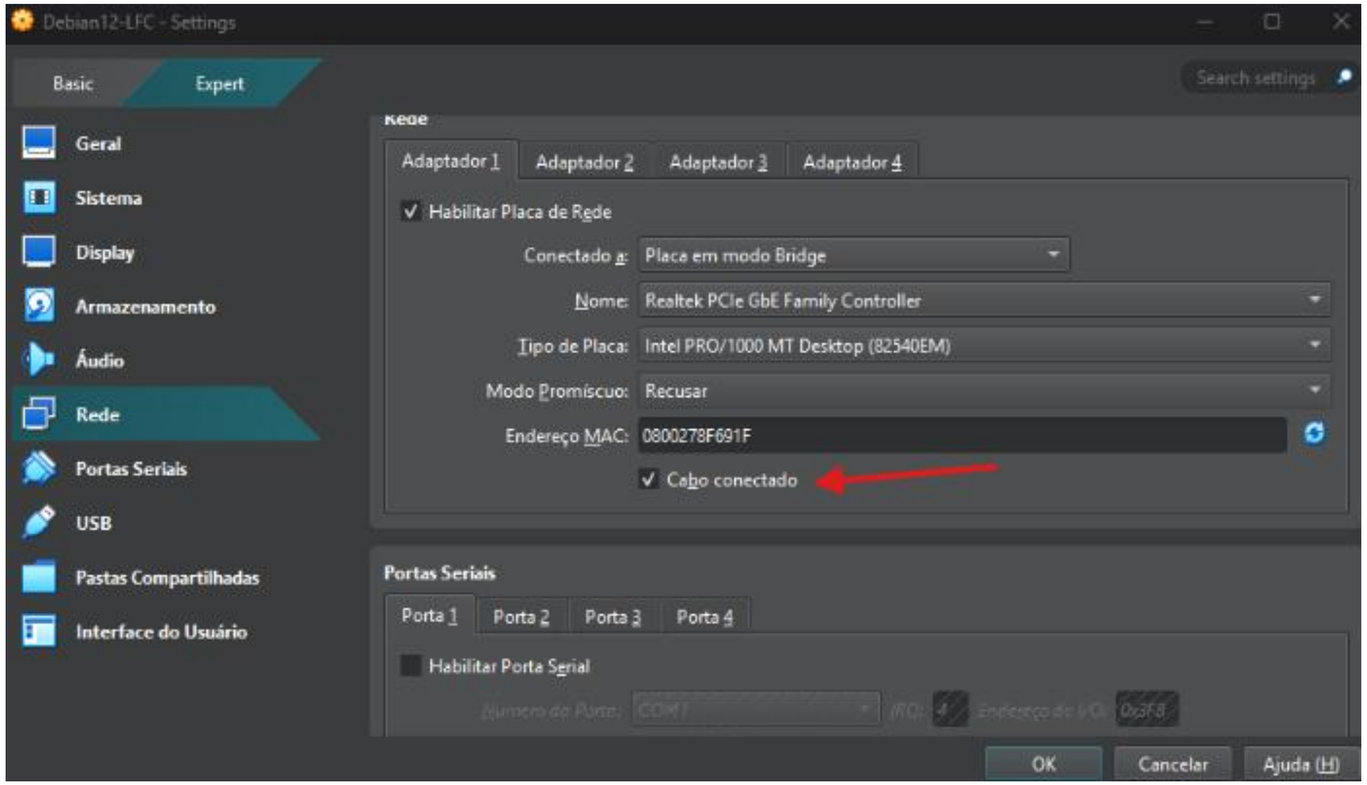
/home – 25 GB

/usr – 8 GB

/var – Restante do Disco

1.3 Atividades Pós-Instalação

Ligar a rede da VM



Configurar a Rede

- Verificar o nome da sua interface:

 # ip a s

- Editar o arquivo /etc/network/interfaces

 # nano /etc/network/interfaces

auto enp0s3

iface enp0s3 inet dhcp

Configurar a Rede

- Solicitar para buscar IP automaticamente:

 # dhclient –v enp0s3

- Verificar o IP:

 # ip -4 –br a

Configurar Repositórios

- Editar o arquivo /etc/apt/sources.list:

 # nano /etc/apt/sources.list

deb http://debian.org/debian bookworm main contrib non-free

deb-src http://debian.org/debian bookworm main contrib non-free

- Atualizar a relação de pacotes:

 # apt update

Instalar Programas

- Instalar o editor vim:

 # apt install -y vim

- Instalar o SSH Server

 # apt install –y openssh-server

- Verificar se a porta 22 abriu:

 # ss -nat | grep :22

Completar Repositórios

- Editar o arquivo /etc/apt/sources.list:

 # vim /etc/apt/sources.list

 # Repositórios oficiais do Debian 12

deb http://deb.debian.org/debian bookworm main contrib non-free

deb-src http://deb.debian.org/debian bookworm main contrib non-free

 # Repositórios de Segurança

deb http://deb.debian.org/debian-security/ bookworm-security main contrib non-free

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

 # Repositórios de Atualizações

deb http://deb.debian.org/debian bookworm-updates main contrib non-free

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

 # Backports

deb http://deb.debian.org/debian bookworm-backports main contrib non-free

deb-src http://deb.debian.org/debian bookworm-backports main contrib non-free

Configurar o vim

- Editar o arquivo /etc/vim/vimrc

 # vim /etc/vim/vimrc +$

set cursorline

set cursorcolumn

set number

Descrição das opções

- **vimrc**: Arquivo de parametrização do vim
- **cursorline**: Exibe uma linha onde o cursor estiver posicionado
- **cursorcolumn**: Exibe uma coluna onde o cursor estiver posicionado
- **number**: Exibe o número das linhas.

1.4 Usuário root e usuário comum

- Usuário comum ($)
- Usuário root (#)
- Usuário de sistema

```
root@hunter:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
```

1.5 Sistema de Arquivos

- Árvore invertida
- FHS
  - Uma estrutura de diretórios padronizada mantém o sistema organizado e sempre previsível a orientar onde cada informação ou comando está. O intuito é organizar o sistema afim de conseguir compatibilidade entre as numerosas distribuições Linux.

FHS

/

Diretório raiz

/bin

Comandos essenciais, qualquer usuário pode executar

/sbin

Comandos essenciais, apenas o root pode executar

/etc

Arquivos de configuração

/home

Diretório pessoal dos usuários

/var

Arquivos de tamanho variável (logs)

/usr

Hierarquia secundária do /, Programas de uso geral

Sistema de Arquivos

- Instalar o tree

 # apt install tree

 # tree –L 1 /

```
root@hunter:/usr/local/share# tree -L 1 /
/
├── bin -> usr/bin
├── boot
├── dev
├── etc
├── home
├── initrd.img -> boot/initrd.img-6.1.0-22-amd64
├── initrd.img.old -> boot/initrd.img-6.1.0-22-amd64
├── lib -> usr/lib
├── lib64 -> usr/lib64
├── lost+found
├── media
├── mnt
├── opt
├── proc
├── root
├── run
├── sbin -> usr/sbin
├── srv
├── sys
├── tmp
├── usr
├── var
├── vmlinuz -> boot/vmlinuz-6.1.0-22-amd64
└── vmlinuz.old -> boot/vmlinuz-6.1.0-22-amd64

21 directories, 4 files
root@hunter:/usr/local/share#
```

1.6 Comandos Básicos

Iremos aprender comandos básicos mas importantes até para o desenvolvimento do curso, como:

- man
- apropos
- ls
- cd
- pwd
- pushd
- popd
- mkdir e rmdir
- rm

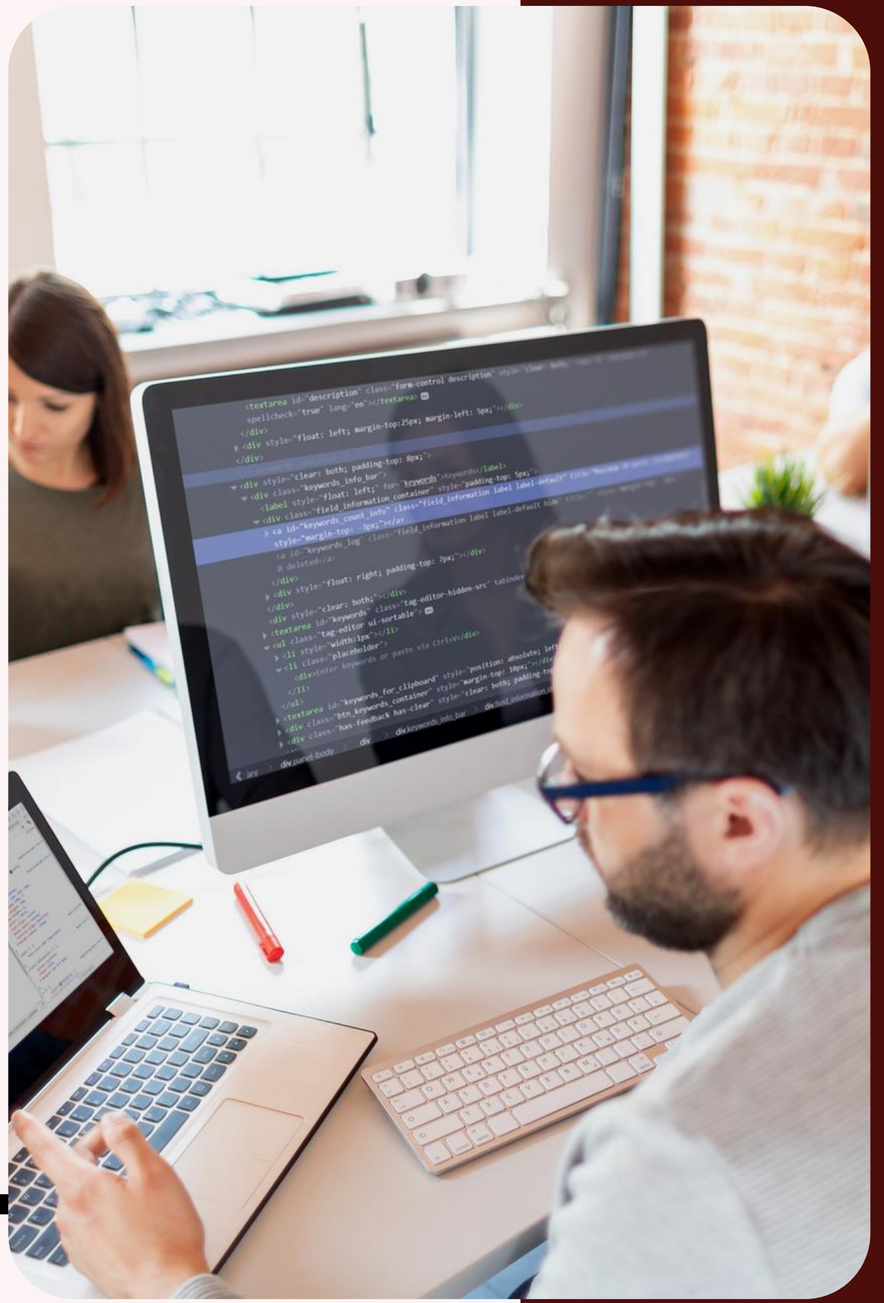
man

- Páginas de manual

 # man sort

 # man –k passwd

 # man 5 passwd

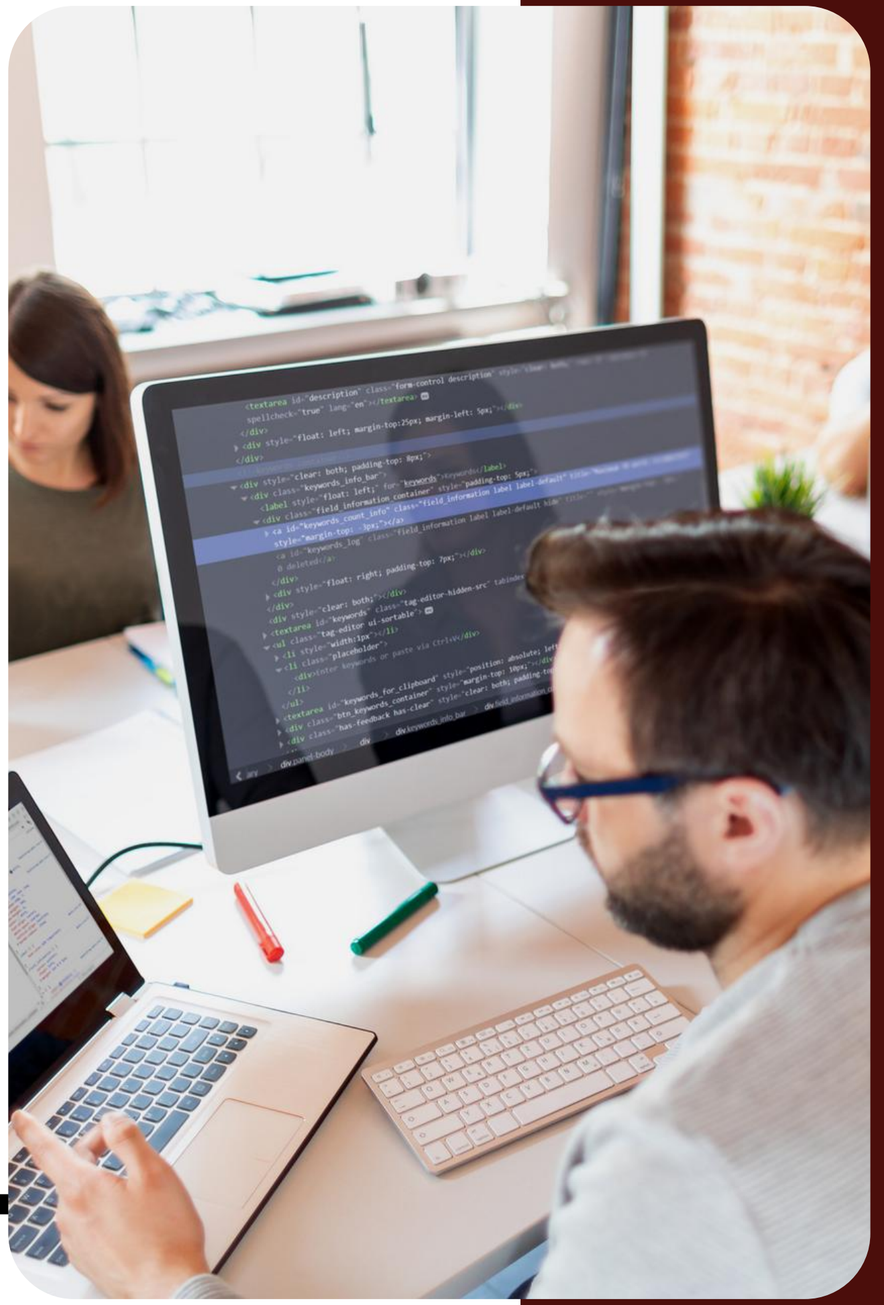


apropos

- Pesquisar a lista de descrições de páginas de manual

 # apropos partition

 # apropos disk usage



Listando arquivos

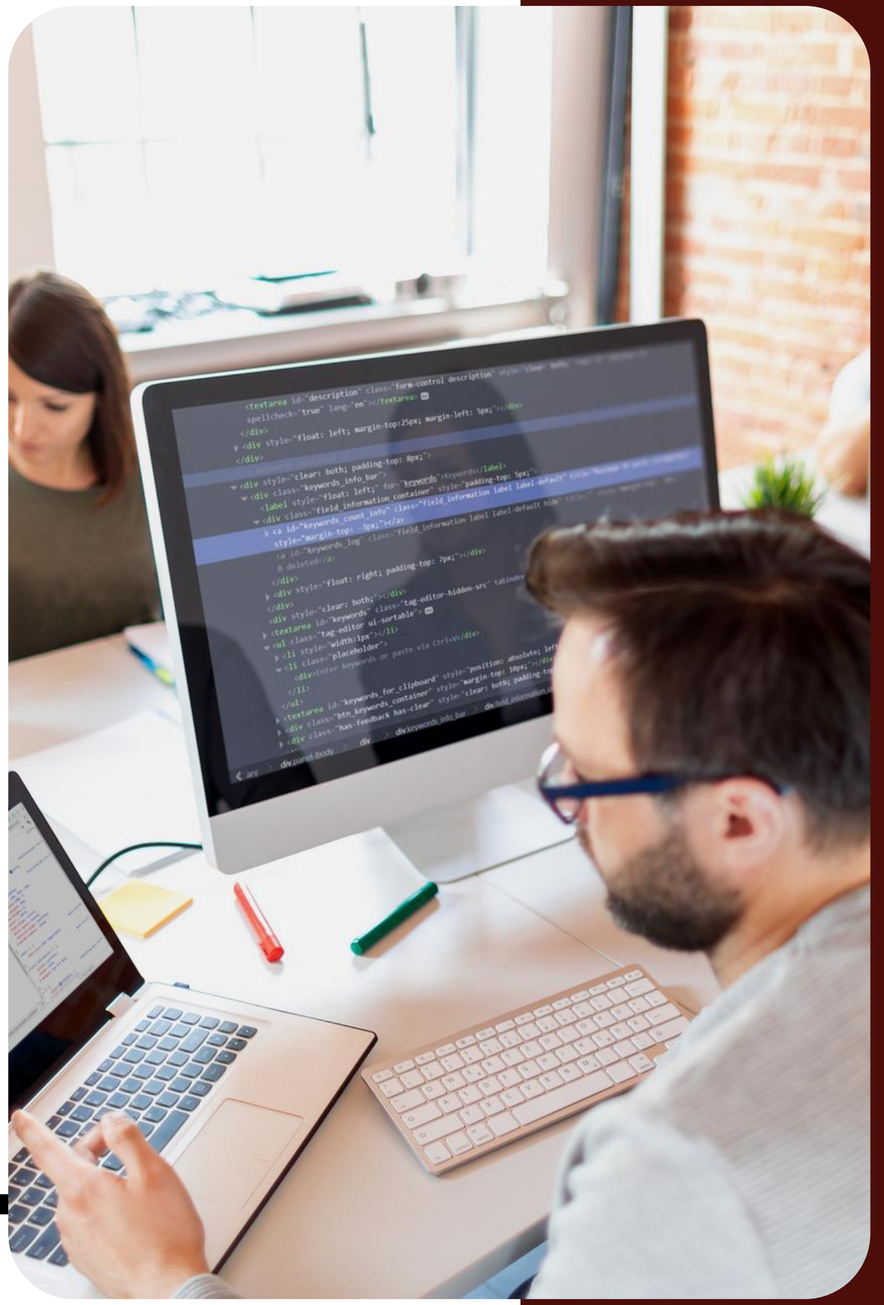
- Exibe na telas os arquivos de um diretório

 # ls

 # ls /etc/.conf*

 # ls –a1 /etc/.conf*

 # ls –ltrh /etc



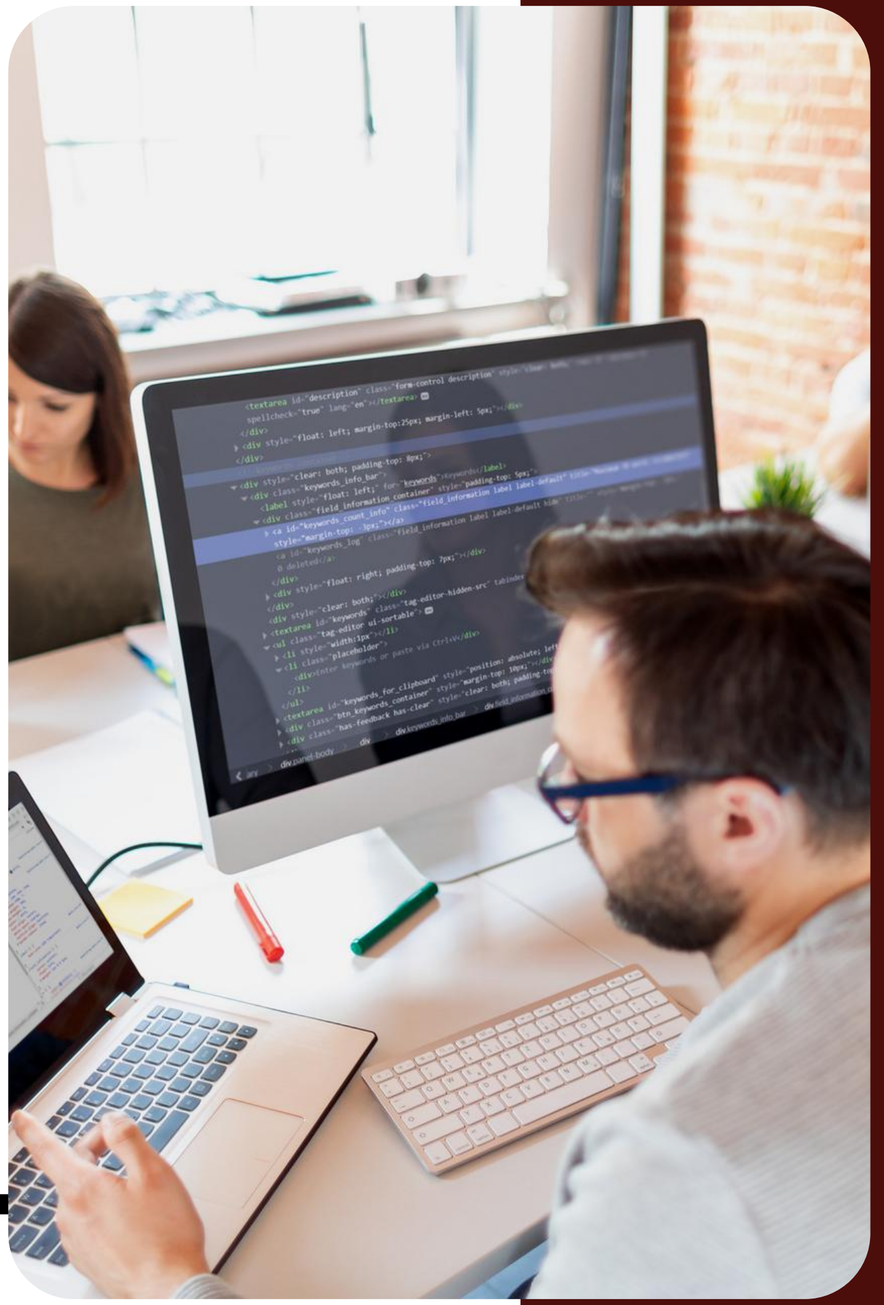
Navegando no Sistema

- Todos os arquivos são filhos do diretório raiz

 # cd /usr/local/share

 # pwd

$ pushd /var/log
/var/log ~
/var/log $ pushd /etc
/etc /var/log ~
/etc $ popd
/var/log ~
/var/log $ popd
~
~ $



Criando diretórios

- Utilizar o comando mkdir (make Directory)

 # mkdir web

 # cd web

 # mkdir modulo teste

 # ls

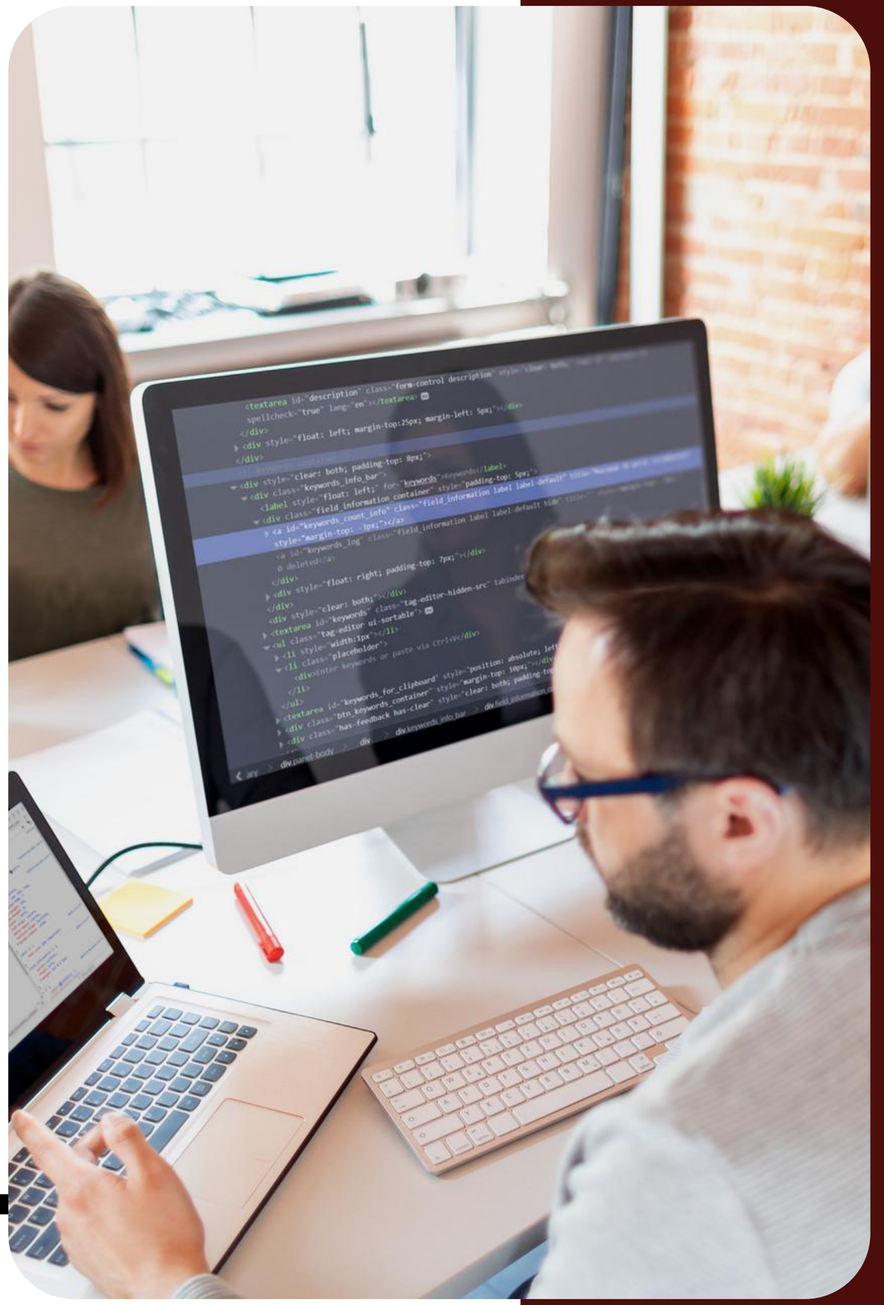
 # rm -rf modulo/ teste/

 # mkdir "modulo teste“

 # cd modulo\ teste/

 # mkdir -p reports/{vul_altas,vul_medias,vul_baixas}

 # ls -1 reports



1.7 Procurando Arquivos

Três dos comandos mais comuns do Linux usados para localizar arquivos no Linux incluem:

- find
- locate
- which

Esses utilitários têm similaridades, mas funcionam e retornam dados de maneiras diferentes e, portanto, podem ser usados em circunstâncias diferentes.

find

- Principal comando de localização de arquivos no Linux.
- Critérios comuns:
  - -type
  - -name
  - -iname
  - -user
  - -perm
  - -size

Exemplos

 # find /home -iname aluno

 # find / -iname SERVICES

 # find /var -size +10M -exec ls -lh {} \;

 # find / -regex '^/etc/p[a-z]$'*

 # find / -regex '^[/a-z_][cC]+[Oo]*[nN]+[fF]+[iI]*[gG]+$'*

- Um comando bem interessante , que usamos na parte de Red Team, é procurar por arquivos com o SUID BIT habilitado. Vamos entender melhor quando vermos permissões de arquivos.

 # find / -type f \(-perm -4000 -o -perm -2000 \) > suid_sgid_files.txt

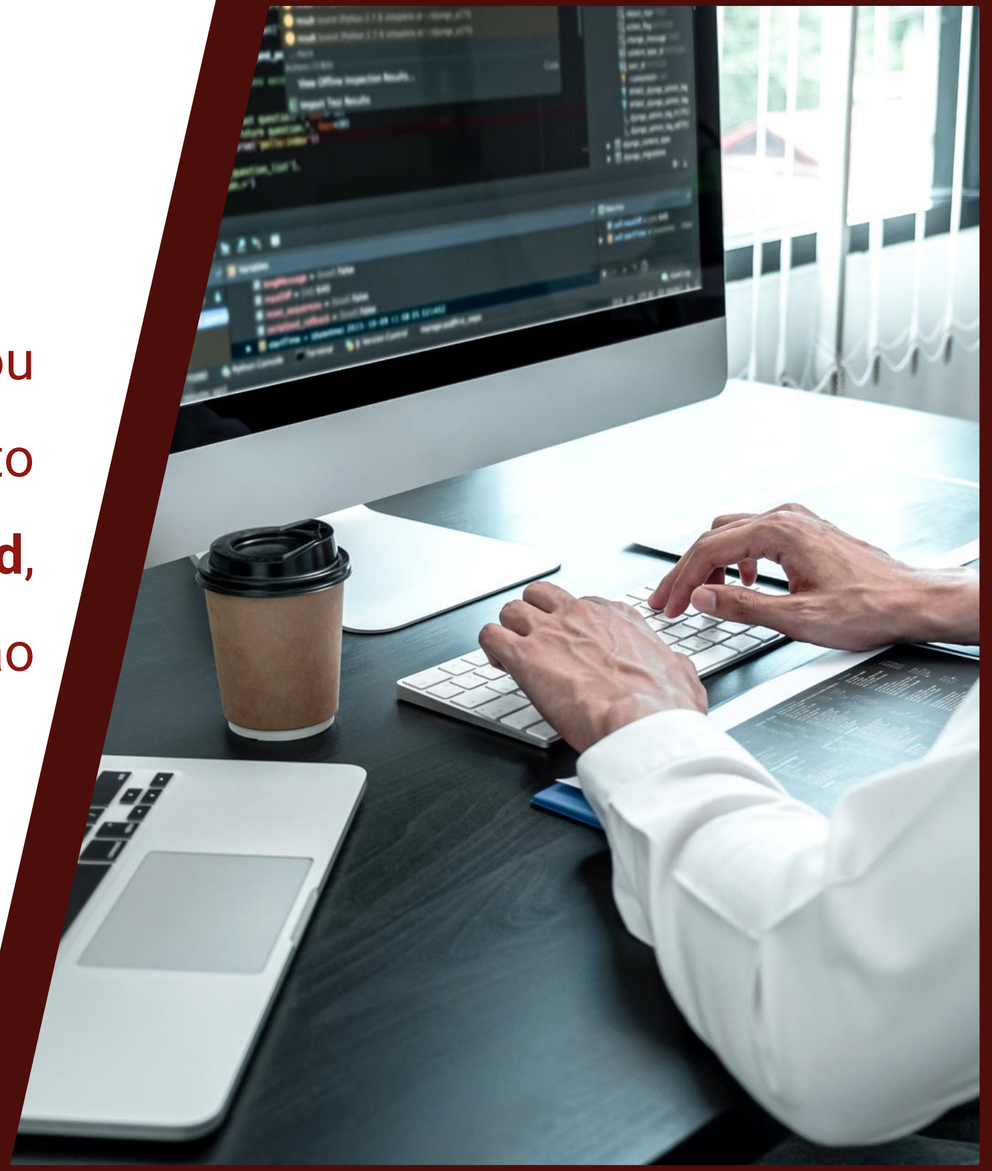
locate

- Sua utilização é simples, todo caminho do arquivo ou diretório contendo a expressão fornecida como argumento será mostrado. A busca é mais rápida em relação ao **find**, pois ele realiza a busca em seu banco dedados e não diretamente no disco.

 # apt install –y locate

 # updatedb

 # locate sysadmin



which

- O comando which localiza o executável de um arquivo, informa o diretório onde ele está.

 # which ls

 # apt install iptables

 # which iptables

 # whereis iptables

1.8 Gerenciando Serviços no Linux

- SysvInit - runlevels

- Systemd – Paralelismo de scripts
  - Estado de Serviços

 # systemctl status ssh

Listando Units com systemctl

- Listando o estado de todas as units para verificar o startup de um sistema:

 # systemctl

- Listando o estado de apenas units de serviços

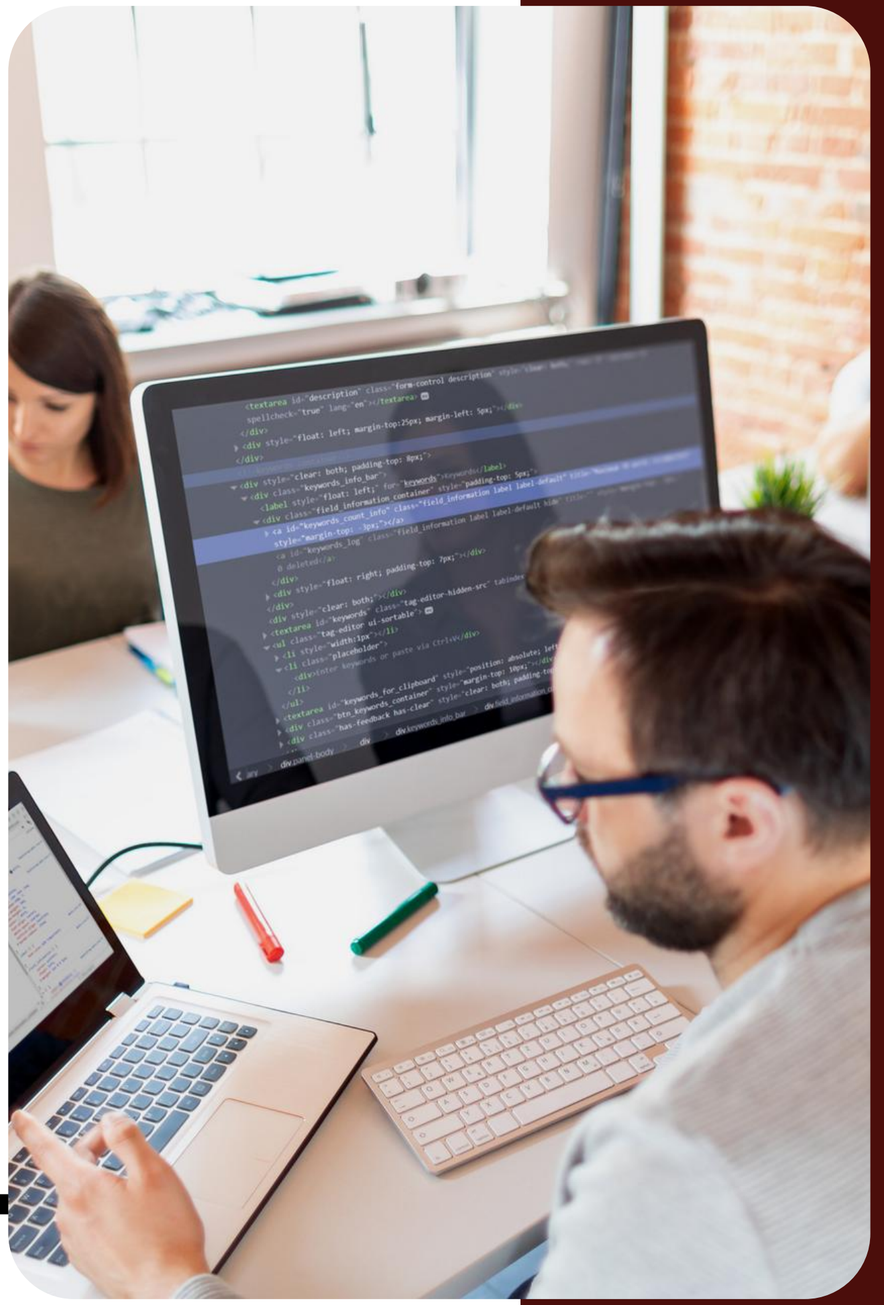
 # systemctl --type=service

- Investigando uma unit

 # systemctl --type=service

- Investigando uma unit com saída completa

 # systemctl status ssh -l



Iniciando e parando daemons

 # systemctl status ssh

 # ps –up 3019

 # systemctl stop ssh

 # systemctl status ssh

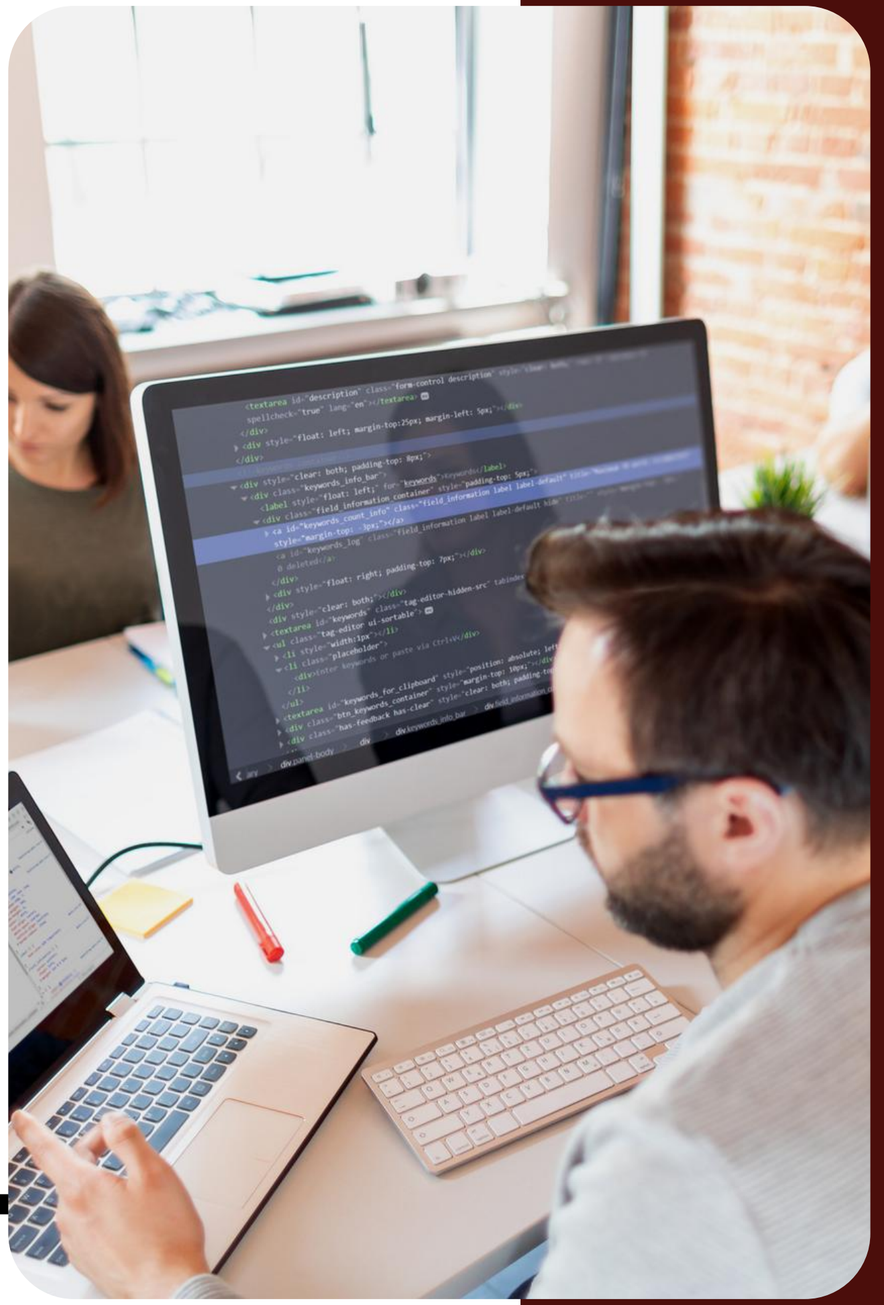
 # systemctl start ssh

 # systemctl status ssh

 # systemctl restart ssh

 # systemctl reload ssh

 # systemctl status ssh



Habilitando o serviço

 # systemctl status ssh

 # systemctl disable ssh

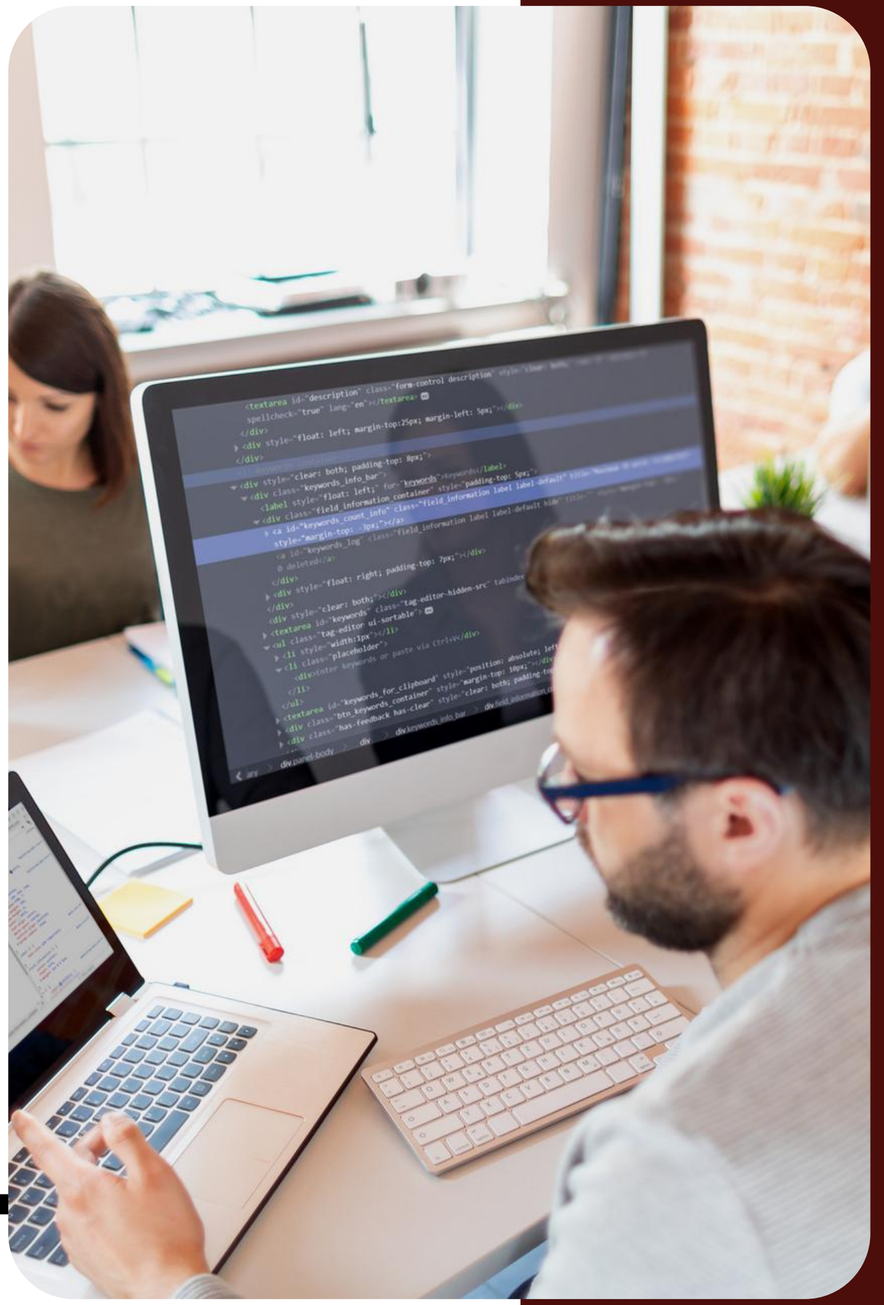
 # systemctl status ssh

 # systemctl enable ssh

 # systemctl is-enabled ssh

Magia:

 # systemctl enable --now sshd.service



Journald

Responsável pela coleta e armazenamento dos logs gerados pelo sistema e por suas aplicações.

Consultar logs do kernel:

 # journalctl –k

Exibir os logs somente dos serviços de rede:

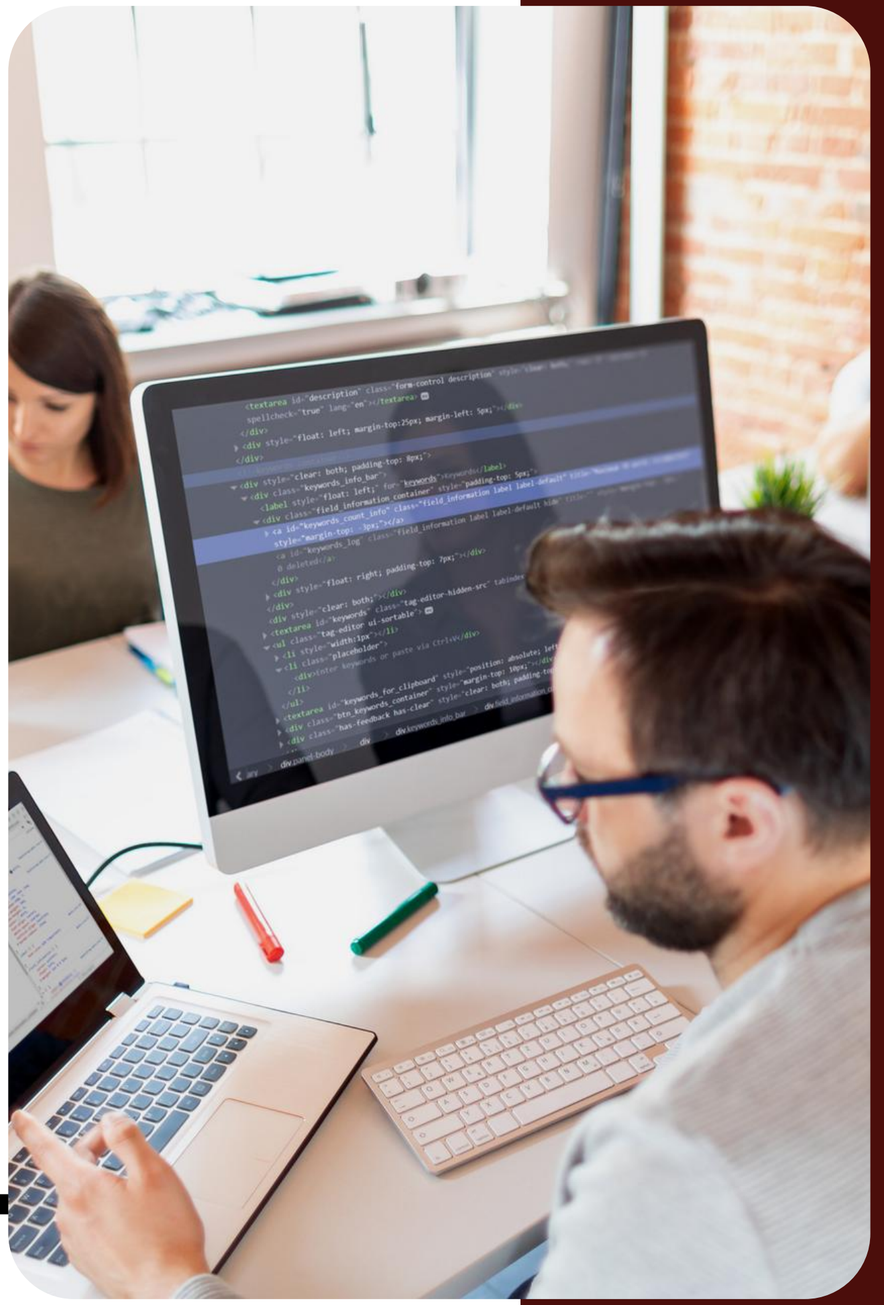
 # journalctl -u network.service

Exibir logs recentes em tempo real:

 # journalctl –f

Exibir os logs filtrando por nível de severidade:

 # journalctl -u ssh.service -p err



1.9 Encontrando, instalando e removendo tools

- A imagem de um sistema Linux, por exemplo do Kali Linux contém as ferramentas mais comuns usadas no campo de testes de penetração (PenTest).

- Exploraremos o APT (Advanced Package Tool)

- Programa de gerenciamento de pacotes do Debian e derivados como: Ubuntu e Kali Linux.

apt update / upgrade

- Atualizar a lista de pacotes disponíveis

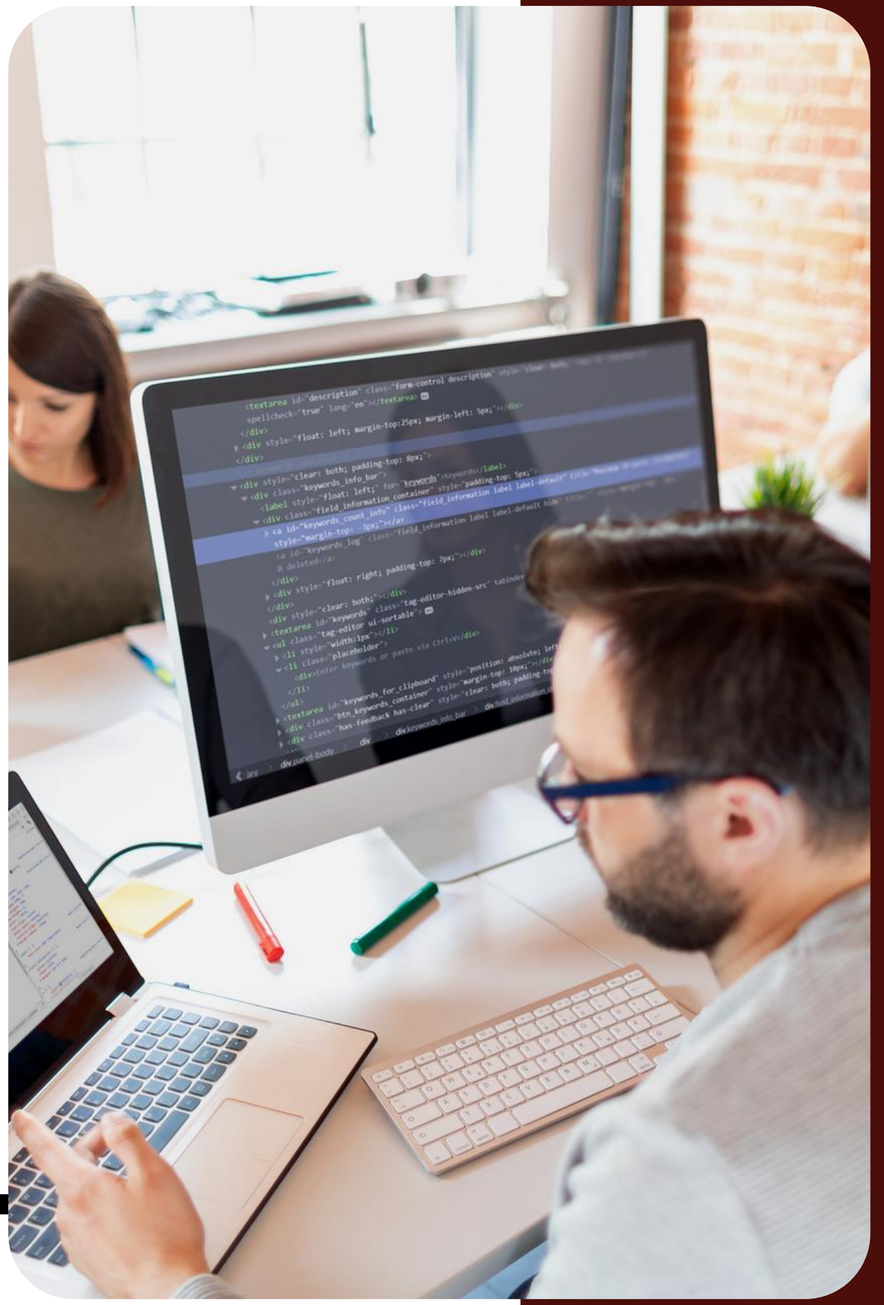
 # apt update

- Atualizar os pacotes instalados

 # apt upgrade

- Atualizar um único pacote

 # apt upgrade vim



apt-cache / apt-show

- O comando apt-cache search exibe muitas das informações armazenadas no banco de dados de pacotes em cache interno. Procura na descrição do pacote

- *# apt-cache search pure-ftpd*

- Confirmando que a descrição do pacote resource-agentes contém a palavra “pure-ftpd”

 # apt show resource-agents

 # apt show pure-ftpd

apt install

- O comando apt install pode ser usado para adicionar um pacote ao sistema com apt install seguido pelo nome do pacote

 # apt install tcpdump

- Procurando e instalando um pacote

 # apt search cmatrix

 # apt install –y cmatrix

apt remove --purge

- Remove completamente os pacotes do Linux. Depende como você remove, pequenos arquivos de configuração podem ficar para trás.

- 1. Removendo por partes

 # apt remove tcpdump

 # apt purge tcpdump

- 2. Removendo de uma vez

 # apt remove --purge tcpdump

- 3. Remover de uma vez

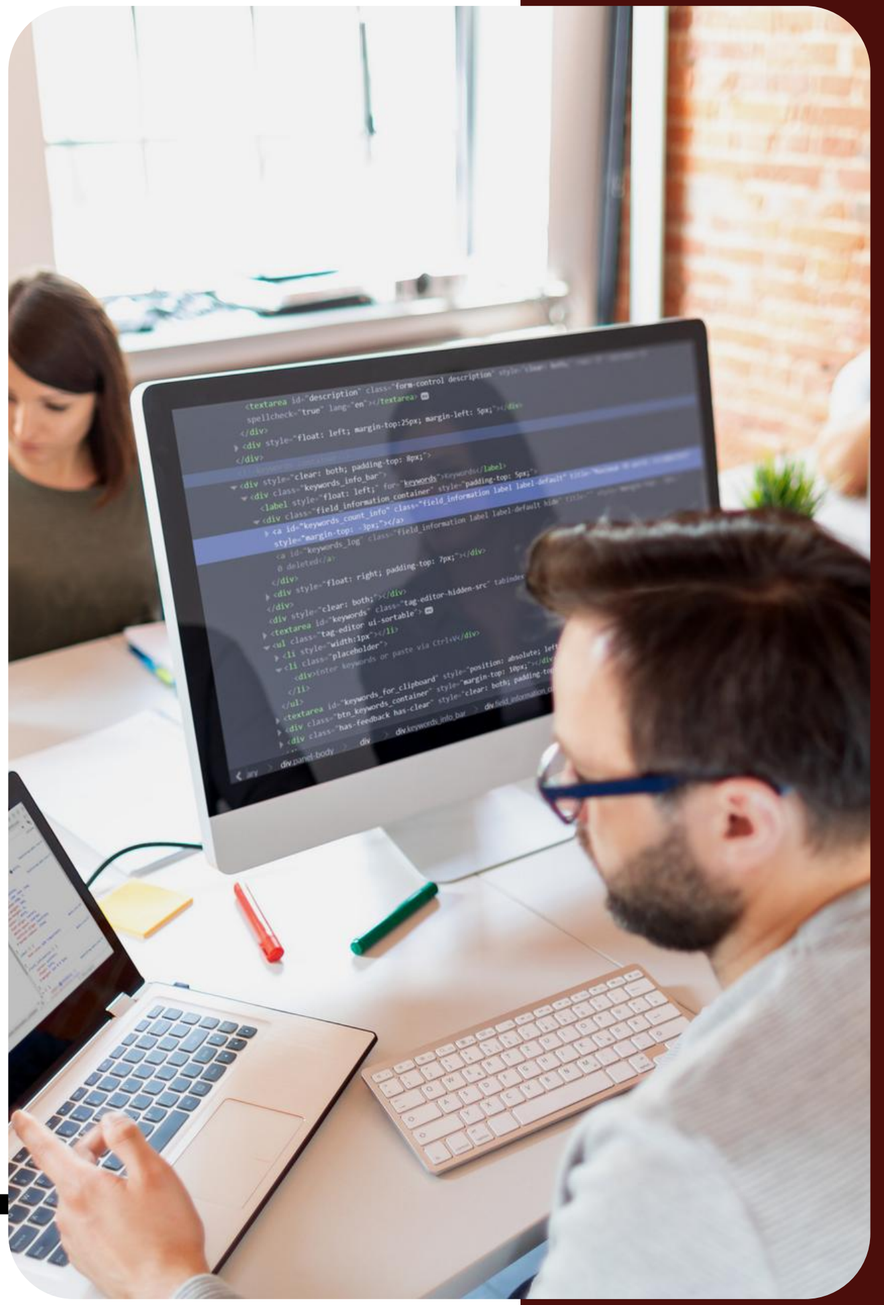
 # apt purge tcpdump

dpkg

- dpkg é a ferramenta principal usada para instalar um pacote, direta ou indiretamente por meio do APT. Também é a ferramenta preferida para usar ao operar offline, pois não requer uma conexão com a Internet.

- Observe que o dpkg não instalará nenhuma dependência que o pacote possa exigir. Para instalar um pacote com o dpkg, forneça a opção -i ou --install e o caminho para o arquivo do pacote .deb.

- Isso pressupõe que o arquivo .deb do pacote a ser instalado tenha sido baixado anteriormente ou obtido de alguma outra forma.



Exemplos uso do dpkg

- Baixar o pacote cmatrix

 # apt download cmatrix

- Realizar a instalação com o dpkg

 # dpkg -i cmatrix_2.0-3_amd64.deb

- Verificar pelos pacotes instalados no sistema

 # dpkg –l

- Verificar se o pacote tcp

 # dpkg –l | grep tcpdump

- Lista os arquivos instalados pelo pacote

 # dpkg –L cmatrix

OBRIGADO

Março - 2025

treinamento.basetic.com.br