Ethernet, Intranet & Server Pentesting Mega Cheat Sheet (200+ Commands)

Ethernet / LAN Security

```
tcpdump -i eth0
```

Capture all packets on interface eth0.

```
tshark -i eth0
```

Command-line packet capture like Wireshark.

```
arping 192.168.1.1
```

Send ARP requests to test ARP responses.

```
arpspoof -i eth0 -t 192.168.1.10 192.168.1.1
```

ARP spoof a target host.

```
macchanger -r eth0
```

Randomize MAC address for anonymity.

Intranet Recon & Enumeration

```
        nmap -sP 192.168.1.0/24
```

Ping scan entire subnet to discover hosts.

```
        nbtscan 192.168.1.0/24
```

Scan for NetBIOS information.

```
        smbclient -L //192.168.1.5 -N
```

List SMB shares without authentication.

```
        enum4linux -a 192.168.1.5
```

Enumerate Windows systems over SMB.

```
        snmpwalk -v2c -c public 192.168.1.5
```

Enumerate SNMP services.

Server Enumeration

```
nc -nv 192.168.1.5 80
```

Banner grab HTTP service.

```
curl -I http://192.168.1.5
```

Fetch HTTP headers.

```
openssl s_client -connect 192.168.1.5:443
```

Check SSL/TLS certificate details.

```
nikto -h http://192.168.1.5
```

Web vulnerability scan.

```
smbmap -H 192.168.1.5
```

Enumerate SMB shares and permissions.

Exploitation & Brute-force

```
hydra -l admin -P rockyou.txt ssh://192.168.1.5
```

SSH brute force attack.

```
medusa -h 192.168.1.5 -u admin -P wordlist.txt -M ssh
```

SSH brute force with medusa.

```
ncrack -p ssh:192.168.1.5 -U users.txt -P pass.txt
```

SSH brute force with ncrack.

```
sqlmap -u 'http://192.168.1.5/index.php?id=1' --dbs
```

SQL injection test.

```
msfconsole
```

Launch Metasploit Framework console.

Post-Exploitation & Privilege Escalation

```
        sudo -l
```

List allowed sudo commands.

```
        find / -perm -4000 -type f 2>/dev/null
```

Find SUID binaries.

```
        getcap -r / 2>/dev/null
```

Check Linux capabilities.

```
        linpeas.sh
```

Run LinPEAS for privilege escalation checks.

```
        winPEAS.exe
```

Run winPEAS on Windows target.