ENUMERAÇÃO PADRÃO → REDES

→ primeiro scan: descoberta de portas

```
nmap [ip_address]
```

→ portas descobertas: descoberta de serviços e versão

```
nmap -p[ports_discovered] [-A/-sV + -O] [ip_address]
```

TIPO DE COMANDO → COMANDO

SCAN TYPE OPTIONS	NMAP COMMAND
TCP SYN SCAN	nmap -sS [ip_address]
TCP CONNECT SCAN	nmap -sT [ip_address]
TCP ACK SCAN	nmap -sA [ip_address]
TCP FIN SCAN	nmap -Sf [ip_address]
TCP NULL SCAN	nmap -sN [ip_address]
TCP XMAS SCAN	nmap -sX [ip_address]
TCP PING SCAN	nmap -Sp [ip_address]
UDP SCAN	nmap -sU [ip_address]

DISCOVERY TYPE OPTIONS	NMAP COMMAND
TCP SYN PING DISC SCAN	nmap -PS [ip_address]
TCP ACK PING DISC SCAN	nmap -PA [ip_address]
IP PROTOCOL PING DISC SCAN	nmap -PO [ip_address]
ICMP ECHO DISC SCAN	nmap -PE [ip_address]
ICMP DISC TIMESTAMP	nmap -PP [ip_address]
ICMP ADDRESS MAP DISC	nmap -PM [ip_address]
ARP DISC SCAN	nmap -PR [ip_address]
UDP PING DISC SCAN	nmap -PU [ip_address]
TRACEROUTE	nmap --traceroute [ip_address]

HOST DISCOVERY	NMAP COMMAND

LIST ONLY	nmap -sl [ip_address]
NO PORT SCANNING	nmap -sn [ip_address]
DISABLE DNS RES	nmap -n [ip_adddress]

PORT SCANNING	NMAP COMMAND
ALL PORTS	nmap -p- [ip_address]
SPECIFIC PORT	nmap -p [port1,port2…] [ip_address
PORT RANGE	nmap -p [ini_port-final_port] [ip_address]
SEQUENTIAL PORTS	nmap -r [ip_address]

VERSION DETECTION	NMAP COMMAND
NORMAL DETECTION	nmap -sV [ip_address]
OS DETECTION	nmap -O [ip_address]
ALL DETECTION	nmap -A [ip_address]
INTENSITY	nmap --version-intensity [0-9] [ip_address]

FIREWALL / IDS EVASION	NMAP COMMAND
MASK ORIGIN PORT	nmap --source-port [port] [ip_address]
FAKE CHECKSUM	nmap --badsum [ip_address]
PACKET FRAG FOR HARD DETECT	nmap -mtu [mtu_value] [ip_address]
PACKET FRAG	nmap -f [ip_address]
NO PING (good against windows)	nmap -Pn [ip_address]

TIMING SCAN OPTIONS	NMAP COMMAND
SLOWEST SCAN	nmap -T 0 [ip_address]
TRICKY SCAN, AVOID IDS	nmap -T 1 [ip_address]
TIMELY SCAN	nmap -T 2 [ip_address]

DEFAULT SCAN	nmap -T 3 [ip_address]
AGGRESSIVE SCAN	nmap -T 4 [ip_address]
VERY AGGRESSIVE SCAN	nmap -T 5 [ip_address]