Essential Nmap Commands for Cybersecurity Learners

https://www.linkedin.com/in/halilbaris/

Basic Scan

nmap <target>

Scan Specific Ports

```
nmap -p <port1,port2,...> <target>
```

Aggressive Scan and Stealth

nmap -A <target>

nmap -S <spoofed ip> <other options>

nmap --source-port <port no> <other options>

OS Detection

nmap -O <target>

Service Version Detection

nmap -sV <target>

https://www.linkedin.com/in/halilbaris/

Scan a Range of IPs

nmap <start-ip>-<end-ip>

Scan Subnet

nmap <network>/CIDR

Stealth Scan (SYN Scan)

```
nmap -sS <target>
```

https://www.linkedin.com/in/halilbaris/

UDP - TCP Scan

nmap -sU <target>
nmap -sT <target>