NMAP

namp

- stands for network mapper
- d for scanning about open ports and vulnerabilities use
- discover live hosts on a network
- detect open ports on a host
- identify services and versions running on these ports
- performs OS detection
- run vulnerability scripts (via the namp scripting engine)

Examples

```
nmap 192.168.1.1                # Scan a single IP
nmap 192.168.1.0/24             # Scan an entire subnet
nmap -p 80,443 example.com      # Scan specific ports
nmap -sV example.com            # Service version detection
nmap -O 192.168.1.1             # OS detection
nmap -A 192.168.1.1             # Aggressive scan (includes OS, version, script, traceroute)
```

Useful Options

Option	Description
`-sS`	Stealth (SYN) scan
`-sT`	TCP connect scan
`-sU`	UDP scan
`-sV`	Detect service versions
`-O`	OS detection
`-A`	Aggressive scan
`-p`	Specify ports
`-T4`	Faster execution (0-5 scale)
`-Pn`	No host discovery (treat all as online)
`--script`	Use a specific NSE script or category

`Iptables -L` → command is used to list the current rules in your system's firewall managed by the iptables. Use `-n` to show the numerical IPs and Ports (don't resolve DNS/service Names)

nmap -hh	Show the help menu
man nmap	Show the manual page to the nmap
nmap www.google.com	Scan top 1000 ports that exists on the Record
nmap -sT -sU <target>	Scan the first 1000 TCU and UDP Ports
nmap -sT –top-ports 2000 <target>	Scan the first top 2000 ports
nmap -p 80 <target>	Scan a specific port, like 80 on the example
nmap -p 80, 44, 11 <target>	Scan a specific number of ports
nmap -p 1-10 <target>	Scan range of ports
nmap -A <target>	Is a powerful and **aggressive scan** option. Which include OS detection, version detection, script scanning, traceroute. If return tcprapped: means nmap does not know the service type of the port.
nmap -iL file.txt	Scan more than one target, that exists on a text file
Nmap -sn <target>	Known as no port scan, used to perform a ping scan. That tells nmap to only discover hosts that are up without scanning for open ports. **It sends ICMP echo requests (like ping), TCP SYN packets to port 443, and sometimes ARP requests (on local networks).** **Determine which hosts are online**