nmap ip\_to\_scan Normal scan :

nmap ip1 ip2 Multiple Ips

nmap ip-254 [eg : nmap 192.168.1.1-254 ] Scan a Range

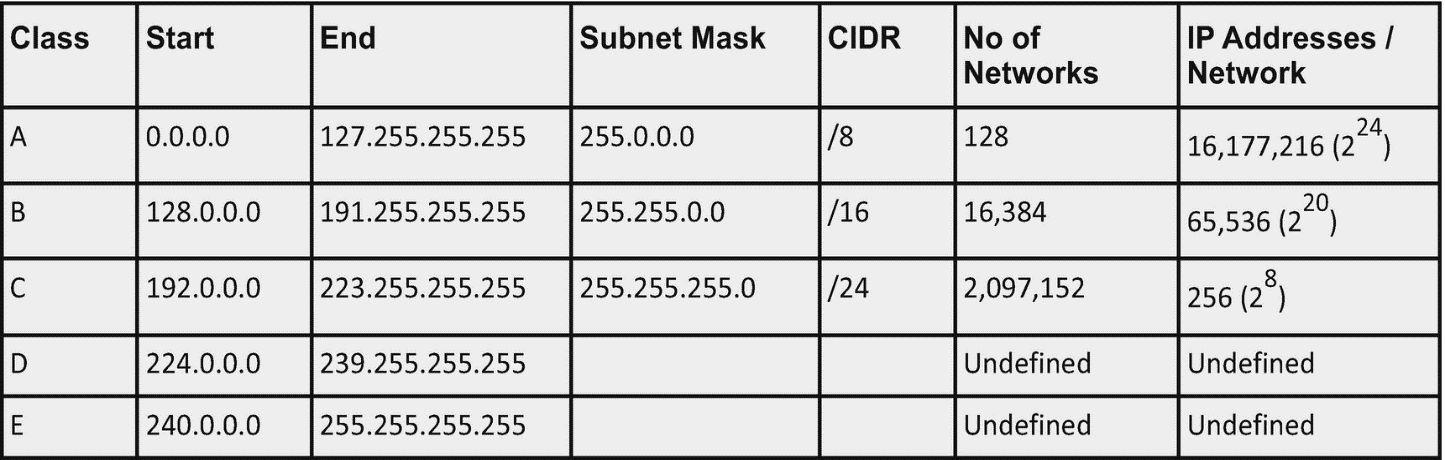
nmap -**iL** targets.txt 🡪 Scans targets from a **List**

nmap -**iR** 100 🡪 Scan 100 **Random** hosts

nmap –**exclude** 192.168.1.1 🡪 Exclude listed hosts

nmap 192.168.1.0/24 🡪 Scan using CIDR notation

\*CIDR – Classless Inter Domain Routing



Scan Techniques ::

-**sS** 🡪 TCP syn port scan ( **S**tealth Scan ) 🡪 nmap <ip-address> -sS

-**sT** 🡪 TCP connec**T** port scan 🡪 nmap <ip-address> -sT

-**sU** 🡪 **U**DP port scan

**-sA 🡪** TCP **A**CK port scan

-s**W** 🡪 TCP **W**indows port scan

-s**M** 🡪 TCP **M**aimon port scan

*HOST Discovery :::::::*

-sn Disable Port Scanning.Host Discovery Only

-**P**n Disable Host Discovery.**Port Scan** only.

**-n** 🡪 nmap ip -n 🡪 Never do DNS resolution

PORT Specification :::::::

**-p** nmap ip **-p** 21 🡪 Port scan for port specified

**-p** nmap ip **-p** 21-100 🡪 Port scan a range

**-p-** nmap ip **-p- 🡪** Port Scan all ports

**-p**  nmap ip **-p** http,https 🡪 Port scan from service name

-**F** nmap ip **-F 🡪 Fast** port scan (100 ports)

**--top-ports** nmap ip --top-ports 300 🡪 Port scan top 300 ports

SERVICE & Version Detection :::::::

Switch Example Description

-**sV** nmap ip -sV Attempts to determine the version

of the service running on port

**-sV –version-intensity**

Eg:

**nmap ip -sV –version-intensity 8** 🡪 Intensity level 0 – 9 . Higher the number higher possibility of correctness

**-A** nmap ip -A 🡪 **Aggressive** scan : Enable OS detection ,version detection ,

Script scanning and traceroute

**TIMING AND PERFORMANCE :::::::::::**

-T0 nmap ip -T0 Paranoid (0) Intruson Detection System evasion

-T1 nmap ip -T1 Sneaky (1) Intrusion Detection System evasion

-T2 -----

-T3 -🡪 Default

-T4 🡪 Fastest

**NSE Scripts :::::::::**

-sC 🡪 nmap ip -sC 🡪 Scan with default NSE scripts.

--script 🡪nmap ip script=https,banner 🡪Scan with 2 scripts

--script 🡪nmap ip script “non-intrusive” 🡪Scan Default but remove instrusive scripts

Nmap –script whois\* domain.com 🡪 Whois query

Nmap -p80 –script http-unsafe-output-escaping <url> 🡪 Detect XSS

Nmap -p80- --script http-sql-injection <url> 🡪 Check for SQL injections

**FIREWALL / IDS Evasion and Spoofind**

-f 🡪 nmap ip -f 🡪Requested Scan use tiny fragmented IP packets making it

Harder for packet filters

-D 🡪 nmap -D decoy-ip-1, decoy-ip-2, OWN-ip , decoy-ip-4 Remote-Host-ip

🡪 Remote Host Ip Is the Ip to be scanned

-S 🡪 nmap -S www.microsoft.com www.fb.com 🡪 Scan Fb from Microsoft

--data-length 🡪

nmap --data-length 200 <ip>

🡪 Appends random data to sent packets

‘’’’’’sometimes we may such errors



-Pn is “no Ping” . Used when the Ping is Blocked by the other comp.

::::::::::::::::OUTPUT

-**oN**  nmap ip -oN output.txt normal o/p to output.txt

**-oX** nmap ip -oX xml.file **xml o/p**

**-oG** nmap -oG grep.file **grepable** o/p

-v verbose mode

-vv more verbose

-d debug level

-dd increased debugging level

--reason display reason a port is in a particular state

--open only show open ports

--packet-trace shows all packets send and received

--iflist 🡪 nmap –iflist 🡪 shows host interfaces and routes like ifconfig

--resume 🡪 nmap –resume results.file 🡪 Resume a scan