INTRODUCTION TO NMAP

- Nmap (Network Mapper) is a free, open-source tool used for network discovery and security auditing.
- Below is a list of commonly used Nmap commands and what they do.

All Nmap Commands and Explanations :--

1. Host Discovery:

```
nmap -sn 192.168.1.0/24
```

-> Scans the subnet and shows live hosts.

2. Port Scanning:

```
nmap -p 22,80,443 192.168.1.1
```

-> Scans only specific ports.

```
nmap -p- 192.168.1.1
```

-> Scans all 65535 ports.

3. Service Detection:

```
nmap -sV 192.168.1.1
```

-> Detects the service and version running on ports.

4. OS Detection:

```
nmap -O 192.168.1.1
```

-> Tries to guess the target operating system.

5. Aggressive Scan:

```
nmap -A 192.168.1.1
```

-> Performs OS detection, version detection, script scanning, and traceroute.

6. Stealth/Advanced Scans:

```
nmap -sS 192.168.1.1 -> SYN scan (stealthy)
nmap -sT 192.168.1.1 -> TCP connect scan
nmap -sU 192.168.1.1 -> UDP scan
nmap -sX 192.168.1.1 -> Xmas scan (used to evade firewalls)
```

7. Scan Multiple Targets:

```
nmap 192.168.1.1 192.168.1.2
nmap 192.168.1.0/24
nmap -iL list.txt
# -> Scans targets listed in a file.
```

8. NSE Scripts (Nmap Scripting Engine):

```
nmap --script vuln 192.168.1.1
# -> Scans for vulnerabilities.
```

```
nmap --script ftp-anon 192.168.1.1
# -> Checks for anonymous FTP access.
```

```
nmap --script http-enum 192.168.1.1
# -> Enumerates directories on HTTP services.
```

9. Output Options:

```
nmap -oN scan.txt 192.168.1.1
# -> Normal output to a file.
```

```
nmap -oX scan.xml 192.168.1.1
# -> XML output.
```

```
nmap -oA allformats 192.168.1.1
# -> Saves output in all formats.
```

10. Timing Options:

```
nmap -T1 to -T5
# -> Adjusts scan speed (T1=slow, T5=fastest).
```

11. Firewall Bypass Techniques:

```
nmap -f 192.168.1.1
# -> Fragment packets to bypass firewall.
```

```
nmap --source-port 53 192.168.1.1
# -> Spoof port as DNS.
```

```
nmap --data-length 50 192.168.1.1
# -> Adds extra payload to bypass filters.
```

Recommended Learning Path (7 Days):

- Day 1: Introduction + Installation (Linux/Kali/WSL)
- Day 2: Host Discovery + Port Scanning
- Day 3: OS & Service Detection
- Day 4: NSE Scripting Basics
- Day 5: Firewall Bypass Techniques
- Day 6: Output Formatting + Automation
- Day 7: Real-world Practice (HackTheBox, TryHackMe)

SOURCE: chatgpt.com , wikipedia.com , youtube.com