Ex1. Perform an Experiment for port scanning with nmap

Aim of the Experiment:

-To understand what a **network port** is, how to use **Nmap** to scan for open ports on a machine, and to distinguish between **ethical** and **unethical** uses of port scanning with real-world examples.

What is a Port?

Imagine a Computer as a Hotel:

- A **hotel** has many **rooms**.
- Each **room** serves a different purpose (e.g., dining, sleeping, storage).
- A **computer** is like a **hotel**, and **ports** are its **rooms**.

Definition:

-A **port** is a **communication endpoint** on a computer where data is received and sent. Each port is associated with a specific service or application.

Port Numbers:

- Ports are numbered from **0 to 65535**.
- Common Port Numbers:

Port Number	Protocol	Use
20, 21	FTP	File transfer
22	SSH	Secure remote login
23	Telnet	Unsecure remote login
25	SMTP	Sending email
53	DNS	Resolving domain names
80	HTTP	Web browsing
443	HTTPS	Secure web browsing
3306	MySQL	Database

Example:

- When you open **https://www.google.com**, your browser connects to **port 443** on Google's servers because it's using **HTTPS**.

What is Port Scanning?

-Port scanning is like checking which **doors (ports)** are open on a building (computer) to see which services are active. It helps in:

- Identifying vulnerabilities
- Auditing networks
- Ethical hacking

What is Nmap?

- **Nmap** = **Network Mapper**
- It's a powerful command-line tool used to:
    - Discover live hosts on a network
    - Identify open ports and services
    - Detect the operating system
    - Perform security audits

Tools Required:

Tool	Description
Nmap	Port scanner
Target Machine	Localhost / VM (Ubuntu, Windows, etc.)
OS	Kali Linux / Ubuntu / Windows
Network Setup	LAN or Virtual Network (do **not** scan public IPs without permission)

Types of Port States (Nmap output):

Port State	Meaning
Open	Service is listening (can connect)
Closed	No service is listening (but port exists)
Filtered	Port blocked by firewall
Unfiltered	Port accessible, but no info
**Open	Filtered**
**Closed	Filtered**

Nmap Command Reference Guide with Detailed Explanations

1. Basic Scanning Commands

Command	Description	Example	Detailed Explanation
nmap <IP>	Basic scan	nmap 192.168.1.1	Performs a default scan (TCP SYN on 1000 common ports) on the target IP. Useful for identifying open ports on a host.
nmap <domain>	Scan domain	nmap google.com	Resolves the domain to its IP address and scans it for open ports. Useful for scanning websites or remote servers.
nmap <subnet>/24	Subnet scan	nmap 192.168.1.0/24	Scans all 256 hosts in the subnet for live hosts and open ports. Excellent for discovering devices in a local network.

2. Port Scanning Options

Command	Description	Example	Detailed Explanation
-p <port>	Scan specific port	nmap -p 22 192.168.1.1	Checks if a specific port (e.g., SSH on port 22) is open on the target. Good for auditing known services.
-p-	Scan all ports	nmap -p- 192.168.1.1	Scans all 65535 TCP ports on the target. Useful for thorough investigations.
-F	Fast scan	nmap -F 192.168.1.1	Scans only the top 100 most common ports. Fast but may miss uncommon services.
-r	Ordered scan	nmap -r 192.168.1.1	Disables randomization of port scan order. Useful when predictable behavior is required.
--top-ports <n>	Scan top N ports	nmap --top-ports 20 192.168.1.1	Scans the top N ports most commonly used across the Internet. Faster than a full scan.

3. Scan Techniques

Command	Technique	Example	Detailed Explanation
-sS	SYN scan (Stealth Scan)	nmap -sS 192.168.1.1	Sends SYN packets and waits for a response. If a SYN-ACK is received, the port is open. If RST is received, the port is closed. It doesn't complete the handshake, making it stealthy and hard to detect. Requires root/admin privileges.
-sT	TCP Connect Scan	nmap -sT 192.168.1.1	Uses the OS's network API to complete a full TCP handshake. It's noisier than SYN scan but doesn't require root.

			Useful when user has limited privileges.
-sU	UDP Scan	nmap -sU 192.168.1.1	Sends empty UDP packets to specified ports. If ICMP Port Unreachable is returned, port is closed. If no response, port may be open or filtered. Slower than TCP due to lack of response feedback. Ideal for scanning services like DNS, SNMP, and TFTP.
-sN	Null Scan	nmap -sN 192.168.1.1	Sends packets with no TCP flags. Relies on target's TCP stack to identify open ports. Some systems respond with RST for closed ports and nothing for open ones. Effective against basic firewall filtering.
-sX	Xmas Scan	nmap -sX 192.168.1.1	Sends packets with FIN, URG, and PSH flags set, resembling a Christmas tree (all lights on). Useful for bypassing certain firewall rules and detecting open ports based on how target responds.
-sF	FIN Scan	nmap -sF 192.168.1.1	Sends TCP packets with only the FIN flag set. Open ports often ignore the packet while closed ports respond with RST. Used to evade firewalls that block SYN packets.

4. Service & Version Detection

Command	Description	Example	Detailed Explanation
-sV	Service version detection	nmap -sV 192.168.1.1	Queries open ports to detect service versions (e.g., Apache 2.4.29). Important for vulnerability assessment.
--version-intensity <0-9>	Adjust detection depth	nmap --version-intensity 5	Controls how aggressively Nmap probes ports. Lower values are faster but less accurate.

5. OS Detection

Command	Description	Example	Detailed Explanation
-O	Operating System detection	nmap -O 192.168.1.1	Uses TCP/IP stack fingerprinting to identify the OS of the target host.
--osscan-guess	Aggressive OS guessing	nmap -O --osscan-guess	Attempts to guess the OS even when certainty is low. Useful in mixed environments.

6. Aggressive Scan

Command	Description	Example	Detailed Explanation
-A	Aggressive scan	nmap -A 192.168.1.1	Combines OS detection, version detection, script scanning, and traceroute. Ideal for full reconnaissance.

7. Script Scanning (NSE)

Command	Description	Example	Detailed Explanation
-sC	Default scripts	nmap -sC 192.168.1.1	Runs a set of scripts for common vulnerabilities and info gathering.
--script <script>	Specific script	nmap --script http-title	Executes a single script, like retrieving the title of a web page.
--script vuln	Vulnerability scripts	nmap --script vuln 192.168.1.1	Runs multiple vulnerability detection scripts. Very useful for pentesting.

8. Timing & Performance

Command	Description	Example	Detailed Explanation
-T<0-5>	Timing template	nmap -T4 192.168.1.1	Controls scan speed. T0 = slowest/stealthy, T5 = fastest/loudest.
--min-rate <n>	Set min packet rate	nmap --min-rate 1000	Ensures Nmap sends at least N packets per second. Useful for fast scans.
--max-retries <n>	Retry limit	nmap --max-retries 2	Sets how many times Nmap retries a probe before giving up.

9. Output Options

Command	Description	Example	Detailed Explanation
-oN <file>	Normal output	nmap -oN scan.txt	Human-readable output written to a file.
-oX <file>	XML output	nmap -oX scan.xml	XML format for parsing and automation.
-oG <file>	Grepable output	nmap -oG scan.grep	Easy to filter using grep/awk. Useful for scripting.
-oA <prefix>	All formats	nmap -oA myscan	Creates .nmap, .xml, and .grep files with given prefix.

10. Host Discovery

Command	Description	Example	Detailed Explanation
-sn	Ping scan	nmap -sn 192.168.1.0/24	Finds which hosts are up without scanning ports.
-Pn	No ping	nmap -Pn 192.168.1.1	Skips host discovery; assumes target is online.
-PS	TCP SYN ping	nmap -PS80,443 192.168.1.1	Sends SYN packets to specified ports to discover live hosts.

-PA	TCP ACK ping	nmap -PA80,443	Sends ACK packets to detect hosts that allow incoming traffic.
-PU	UDP ping	nmap -PU53	Sends UDP packets to test if host responds.

11. Firewall/IDS Evasion

Command	Description	Example	Detailed Explanation
-f	Fragment packets	nmap -f 192.168.1.1	Breaks up packets to evade simple firewall rules.
--source-port <port>	Set source port	nmap --source-port 53	Tricks firewalls into thinking traffic is DNS or another trusted service.
-D RND:10	Decoy scan	nmap -D RND:10 192.168.1.1	Sends fake scans from random IPs to mask real source.
--data-length <n>	Pad packets	nmap --data-length 50	Adds junk data to packets to obscure signature.

Full Command Example:

nmap -sS -p 80 --source-port 53 192.168.1.1

Explanation of Each Part:

Part	Meaning
nmap	Start the Nmap tool
-sS	Use TCP SYN scan (stealthy)
-p 80	Scan port 80 (HTTP)
--source-port 53	Set **source port** to 53 (DNS)
192.168.1.1	Target IP address

Use Case:

Some firewalls **trust traffic from port 53** (used by DNS), so attackers or pentesters may use this trick to **bypass basic filters** or **evade intrusion detection systems (IDS)**.

Important Notes:

- Only works if you run the scan with **root privileges** (use sudo)
  Example:

```
sudo nmap -sS -p 80 --source-port 53 192.168.1.1
```

- This technique is for **ethical testing only** and should be used in **authorized environments**.

Full Command Example:

1. --data-length <n>

Adds extra random data to each packet to obfuscate scans.

```
sudo nmap -sS -p 80 --data-length 50 192.168.1.1
```

Use Case:

This adds **50 bytes of random data** to each packet to **evade signature-based IDS/IPS** systems by making the packets look different from standard Nmap scans.

2. -f (Fragment Packets)

Splits packets into tiny pieces (fragments) to bypass simple firewalls or intrusion detection systems.

```
sudo nmap -sS -p 80 -f 192.168.1.1
```

Use Case:

Some **packet filters can't reassemble fragmented packets**, so this may help bypass those filters. It's a stealthy technique used in penetration testing.

3. -D (Decoy Scanning)

Spoofs multiple IP addresses to confuse the target about your real IP**.**

```
sudo nmap -sS -p 80 -D RND:10 192.168.1.1
```

Use Case:

This tells Nmap to generate **10 random decoy IPs**, so the target sees many incoming scans and **can't easily tell which is real**.

Example: Useful for **bypassing logging or honeypots** during red team operations.

Combine Multiple Evasion Techniques:

sudo nmap -sS -p 80 --source-port 53 --data-length 100 -f -D RND:5 192.168.1.1

This:

- Uses **DNS port 53** as the source port
- Adds **100 bytes of random data**
- **Fragments** packets
- Spoofs **5 decoys**
- Targets **port 80** (HTTP)

⚠️ **Ethical Reminder:**

These techniques should only be used on systems you have **permission** to test, like:

- Internal networks
- Training environments (e.g., Hack The Box, TryHackMe)
- Client-approved penetration tests

12. Scanning Multiple Targets

Command	Description	Example	Detailed Explanation
nmap 192.168.1.1-10	IP range	nmap 192.168.1.1-254	Scans a range of IP addresses in sequence.
nmap -iL list.txt	Input from file	nmap -iL ips.txt	Loads a list of target IPs from a text file.
nmap -iR 5	Random IPs	nmap -iR 5	Scans randomly chosen IP addresses. Useful for testing.
nmap --exclude <ip>	Exclude hosts	nmap --exclude 192.168.1.5	Skips scanning specific IPs.

13. Real-World Use Cases

Use Case	Example Command	Explanation
Network Inventory	nmap -sn 192.168.0.0/24	Lists all live hosts in the subnet.
Find Open Web Servers	nmap -p 80,443 -sV 192.168.1.0/24	Detects live websites and service versions.
Detect Vulnerabilities	nmap --script vuln 192.168.1.1	Checks for known CVEs on open ports.
Audit SSH Security	nmap --script ssh* -p 22 192.168.1.1	Runs all SSH-related scripts.
Check Database Exposure	nmap -p 3306 --script mysql* 192.168.1.1	Detects exposed MySQL services.
Identify IoT Devices	nmap -O -sV 192.168.1.1	Matches services and OS to known IoT fingerprints.
Firewall Evasion (lab only)	nmap -f or nmap -D RND:10	Tests firewall bypass methods.

14. Advanced Script Scanning

Command	Description	Example	Use Case
--script-help <script>	Show script description	nmap --script-help http-title	Get help for a specific NSE script
--script-args <args>	Pass arguments to NSE script	nmap --script http-brute --script-args userdb=users.txt,passdb=pass.txt	Run brute-force attack with custom credentials
--script-args-file <file>	Load NSE args from a file	nmap --script-args-file args.txt	Reuse custom script inputs from file

15. Authentication and Safe Mode

Command	Description	Example	Use Case
--script-trace	Show all packets sent by scripts	nmap --script-trace -sC 192.168.1.1	Debug how scripts interact with hosts
--privileged	Force privileged scan	nmap --privileged -sS	Force use of raw sockets in restricted shells
--unprivileged	Force unprivileged scan mode	nmap --unprivileged -sT	Simulate behavior of a non-root user

16. Performance and Parallelism

Command	Description	Example	Use Case
--min-parallelism <num>	Set minimum parallel probes	nmap --min-parallelism 10 192.168.1.1	Speed up scans on fast networks
--max-parallelism <num>	Set maximum parallel probes	nmap --max-parallelism 100 192.168.1.1	Avoid overwhelming network/host
--scan-delay <time>	Set delay between probes	nmap --scan-delay 1s 192.168.1.1	Evade rate-limiting firewalls

17. IPv6 Scanning

Command	Description	Example	Use Case
nmap -6 <IPv6>	Scan IPv6 address	nmap -6 2001:db8::1	Scan modern networks using IPv6

18. NSE Categories (Script Groups)

Category	Description	Example
auth	Authentication checks	nmap --script auth 192.168.1.1
vuln	Known vulnerabilities	nmap --script vuln 192.168.1.1
default	Default scripts	nmap -sC 192.168.1.1
discovery	Network and host discovery	nmap --script discovery 192.168.1.1
malware	Malware scanning	nmap --script malware 192.168.1.1
brute	Brute-force attacks	nmap --script brute 192.168.1.1
exploit	Exploit known vulnerabilities	nmap --script exploit 192.168.1.1

To view available scripts in a category:

nmap --script-help <category>

19. Save and Resume Scans

Command	Description	Example	Use Case
--resume <file>	Resume an interrupted scan	nmap --resume myscan.log	Continue a long scan without restarting
--datadir <path>	Use custom Nmap data directory	nmap --datadir /opt/nmap	Load scripts/fingerprints from custom path

20. NSE Update and Integration

Command	Description	Example	Use Case
--script-updatedb	Update local script DB	sudo nmap --script-updatedb	After adding or modifying scripts
-oX	XML output	nmap -oX result.xml	Use results in other tools like Metasploit

Extra Tips

- View help: nmap --help
- Read the manual: man nmap
- List scripts: ls /usr/share/nmap/scripts/
- Practice on safe targets like scanme.nmap.org

Note: Nmap now supports over **1000+ NSE scripts**, powerful evasion methods, and performance options for both beginners and experts.

21. Advanced Output Options

Command	Description	Example	Use Case
--append-output	Append to output file	nmap -oN scan.txt --append-output	Continue logging into the same file across scans
--webxml	Create XML for web viewer	nmap -oX scan.xml --webxml	Format designed for web browsers
--reason	Show port state reasons	nmap --reason 192.168.1.1	Explains why a port is open/closed
--open	Only show open ports	nmap --open 192.168.1.1	Cleaner results by hiding closed/filtered ports

--iflist	List network interfaces	nmap --iflist	Shows available interfaces/IPs (debugging)
--stylesheet <file>	Attach XSLT to XML	nmap -oX scan.xml --stylesheet style.xsl	Beautify XML output in browsers

22. Advanced Host Discovery

Command	Description	Example	Use Case
--traceroute	Trace route to target	nmap --traceroute 192.168.1.1	Identify intermediate hops
--dns-servers <servers>	Use specific DNS	nmap --dns-servers 1.1.1.1,8.8.8.8	Override system DNS
--system-dns	Use system-configured DNS	nmap --system-dns	Fall back to system DNS if others fail
--resolve-all	Resolve all hostnames	nmap --resolve-all google.com	Find all DNS IPs for a domain

23. Packet Crafting & Customization

Command	Description	Example	Use Case
--ttl <value>	Set packet TTL	nmap --ttl 10 192.168.1.1	Test hop filters or TTL behavior
--badsum	Send bad checksum	nmap --badsum 192.168.1.1	IDS/IPS testing, packets should be dropped
--mtu <size>	Fragment packets	nmap --mtu 24 192.168.1.1	Obfuscate scan to evade firewalls

24. Target Specification Enhancements

Command	Description	Example	Use Case
--exclude-file <file>	Exclude targets via file	nmap -iL targets.txt --exclude-file skip.txt	Fine control over target lists
-sL <range>	List targets only	nmap -sL 192.168.1.0/24	Preview scan scope (no packets sent)
-iL <file>	Load IPs from file	nmap -iL myips.txt	Batch scanning from saved list

25. Debugging and Troubleshooting

Command	Description	Example	Use Case
-d, -d2 to -d9	Debug output	nmap -d3 192.168.1.1	See detailed scan logic and flow
--packet-trace	Trace packets	nmap --packet-trace	Show each packet sent/received
--reason	Show port reasons	nmap --reason	Know why port status is assigned

26. Performance & Reliability Tuning

Command	Description	Example	Use Case
--host-timeout <time>	Max time per host	nmap --host-timeout 5m	Stop slow scans from stalling full scan
--max-scan-delay <time>	Cap delay between probes	nmap --max-scan-delay 100ms	Improve efficiency
--max-rtt-timeout <time>	Max round-trip wait	nmap --max-rtt-timeout 1s	Ensure timely port response cutoff
--initial-rtt-timeout <time>	Set initial RTT	nmap --initial-rtt-timeout 200ms	Tweak scan speed in fast/slow networks

27. Nmap GUI (Zenmap)

Command	Description	Example	Use Case
zenmap	Launch GUI interface	zenmap	Graphical version of Nmap (if installed)
Save profiles	Create custom scan profiles	—	For repeated scans (e.g., daily web audit)

Zenmap is a graphical front-end for Nmap with features like scan history, topology maps, and result comparison. Use it if you prefer visual tools.

28. Ndiff (Compare Nmap Outputs)

Command	Description	Example	Use Case
ndiff file1.xml file2.xml	Compare two Nmap scans	ndiff before.xml after.xml	Spot changes between scans (added/removed hosts/services)

29. NSE Performance Flags (Advanced)

Command	Description	Example	Use Case
--script-timeout <time>	Set NSE script timeout	--script-timeout 20s	Avoid long-running scripts in large scans
--script-trace	Show NSE script packet traces	--script-trace	For debugging or transparency
--script-updatedb	Update NSE script DB	sudo nmap --script-updatedb	After adding new custom scripts

Full Command Example:

nmap --script vuln --script-timeout 20s 192.168.1.1

Explanation of Each Part:

Part	Meaning
nmap	Starts the Nmap tool

--script vuln	Runs vulnerability detection scripts
--script-timeout 20s	Limits each script to run for max **20 seconds**
192.168.1.1	Target IP address

Use Case:

You're scanning a server for known vulnerabilities, but you don't want the scan to hang because of slow scripts. So you **limit each script to 20 seconds** — anything slower gets skipped.

Tips:

- You can use 10s, 30s, 1m, etc.
- Combine with other options like -sV or -A if needed.

30. Custom NSE Script Usage

If you write your own NSE script (e.g., myscan.nse), use:

nmap --script ./myscan.nse <target>

Write custom scripts using Lua. This is powerful for building:

- Malware detectors
- Custom brute-force checks
- Exploit attempts for known vulnerabilities

31. Location and Resource Paths

Command	Description	Example
nmap --datadir <path>	Custom data path	nmap --datadir /opt/nmap
nmap --script-updatedb	Update script cache	sudo nmap --script-updatedb
ls /usr/share/nmap/scripts/	View installed scripts	For script discovery

32. Combine with Other Tools

- **With Metasploit**: Use -oX XML output in Metasploit (db_import).
- **With Wireshark**: Use --packet-trace or tcpdump alongside Nmap.
- **With cron jobs**: Automate regular scans with logging.

Conclusion

You've now documented **32 categories of Nmap functionality**, including:

- Basic and advanced scans
- Script engine (NSE)
- Firewall evasion
- Performance tuning
- Comparison and automation

1. NSE – Nmap Scripting Engine

What is it?

NSE (Nmap Scripting Engine) allows Nmap to **run special scripts** that can check for vulnerabilities, brute-force login pages, scan web pages, etc. These scripts are written in **Lua** language and give **extra power** to your scans.

How to use?

```
nmap --script vuln 192.168.1.1
```

This runs scripts from the **vuln category** to check for known security weaknesses.

Real-world examples:

Goal	Command
Check for common web flaws	nmap --script http-vuln* <IP>
Brute-force SSH passwords	nmap --script ssh-brute -p 22 <IP>
Get HTTP titles	nmap --script http-title <IP>

2. Scripts (used with NSE)

Scripts are small programs that:

- Detect CVEs (vulnerabilities)
- Test server configurations
- Gather data (titles, banners, DNS info, etc.)

You can list available scripts:

```
ls /usr/share/nmap/scripts/
```

Example:

nmap --script http-title 192.168.1.1

It fetches the title of any web page hosted on the IP (like "Welcome to Apache").

3. Zenmap – GUI for Nmap

What is it?

Zenmap is the **Graphical User Interface (GUI)** version of Nmap. It makes Nmap easier for beginners by:

- Letting you select scan types from dropdowns
- Showing results in color-coded views
- Saving scan profiles and comparing results

How to use?

If installed:

zenmap

Or install it:

sudo apt install zenmap

You can:

- Run the same scans as terminal
- See scan topology
- Save your frequent scans (profiles)

4. Output Options

Nmap can save its results in different formats so you don't lose them.

Option	Use	Example	Description
-oN scan.txt	Normal	nmap -oN scan.txt 192.168.1.1	Saves output as text
-oX scan.xml	XML	nmap -oX scan.xml	Saves in XML (for automation)
-oG scan.grep	Grepable	nmap -oG scan.grep	Easy to filter using grep
-oA allformats	All formats	nmap -oA myscan	Saves .nmap, .xml, and .grep

Next Steps After Mastering Nmap

1. Learn **Wireshark** for packet analysis
2. Master **Nmap Scripting Engine (NSE)** scripting (Lua-based)
3. Move into **Vulnerability Scanning** with tools like **Nessus**, **OpenVAS**
4. Practice on labs like **TryHackMe**, **Hack The Box**
5. Get certified: **CEH**, **OSCP**, or **CompTIA Security+**
6. Combine Nmap with **Metasploit Framework**
7. Scan and secure cloud systems (AWS, Azure, GCP)

Observations:

Command	Purpose	Your Observation

Real-Time Scenarios (Examples):

Legal Scenario:

-A security team scans their company's internal servers to find open ports for maintenance — **with permission**.

Illegal Scenario:

-A hacker scans a bank's website without permission and uses open ports to exploit a server — **without permission**, violates the **IT Act 66C/66D** in India.

Legal vs Illegal Use of Port Scanning:

Action	Legal	Illegal	Example
Scan your own PC/server	✅	❌	Test open services on localhost
Scan a public IP without asking	❌	✅	Scanning Netflix.com
Scan a friend's PC with permission	✅	❌	Lab practice
Scan government servers	❌	✅	Against the law

Additional Tips for Better Understanding:

- Use nmap localhost to safely test on your own machine.
- Use nmap -F for a **fast scan** (top 100 ports).
- Use nmap -O to detect the **OS** of the target (in aggressive mode).
- Always **log your scans** with on filename.txt.

Precautions and Ethics:

- **Never** scan unknown IPs without written permission.
- Respect **cyber laws** and **digital ethics**.
- Use tools only in labs, sandboxes, or for **certified penetration testing**.
- Educate others on legal/illegal boundaries of scanning.

What Can I Do If I Know Port Scanning Well?

- - Learn vulnerability assessment and penetration testing (VAPT)
- - Practice ethical hacking using platforms like Hack The Box, TryHackMe
- - Get certified (e.g., CEH, CompTIA Security+, OSCP)
- - Learn advanced tools like Wireshark, Nessus, Metasploit
- - Join bug bounty programs (HackerOne, Bugcrowd)

Result:

This experiment taught:

- The **concept of ports and services**
- **Nmap** usage at various levels (basic to advanced)
- The importance of **ethical hacking**
- Differences between **safe/unsafe**, **legal/illegal** scanning

Port scanning is a powerful tool — but with great power comes great responsibility!

Viva Questions:

1. What is a network port?
2. How does Nmap work?
3. What is the difference between TCP and UDP scanning?
4. What do you mean by "filtered" port?
5. What are ethical issues in port scanning?
6. What Indian law punishes illegal hacking or scanning?
7. Why do attackers use Nmap?
8. How can organizations protect their open ports?

1. What is Nmap?

Answer:
Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It can detect live hosts, open ports, services, and vulnerabilities.

2. What is the default scan type used by Nmap?

Answer:
Nmap uses a **TCP SYN scan (-sS)** by default if run with root privileges.

3. What are the different types of scans in Nmap?

Answer:

- -sS: SYN scan (stealthy)
- -sT: TCP connect scan (less stealthy)
- -sU: UDP scan
- -sN, -sF, -sX: Null, FIN, Xmas scans (firewall evasion)
- -A: Aggressive scan

4. What does the -p- option do in Nmap?

Answer:
It tells Nmap to scan **all 65,535 TCP ports**, not just the common ones.

5. How do you scan a specific port or port range?

Answer:

nmap -p 22 192.168.1.1 # Specific port

nmap -p 20-80 192.168.1.1 # Range of ports

6. What is the Nmap Scripting Engine (NSE)?

Answer:
NSE allows Nmap to run **scripts written in Lua** for vulnerability detection, brute-force attacks, malware scans, etc. It makes Nmap very powerful for security testing.

7. How can you detect the operating system of a host using Nmap?

Answer:

nmap -O <target>

This enables OS detection by analyzing TCP/IP stack responses.

8. What is Zenmap?

Answer:
Zenmap is the **GUI (Graphical User Interface)** for Nmap. It allows users to run scans without typing commands and view results in graphical formats.

9. What is the use of --script-timeout in Nmap?

Answer:
It sets a **maximum time limit** for each NSE script. For example:

nmap --script vuln --script-timeout 30s 192.168.1.1

10. How can you discover live hosts in a network?

Answer:

nmap -sn 192.168.1.0/24

This sends ping probes to detect which hosts are online.

11. How do you use Nmap for vulnerability scanning?

Answer:

nmap --script vuln 192.168.1.1

This runs multiple vulnerability detection scripts on the target.

12. How can Nmap evade firewalls and IDS?

Answer:

- Fragment packets: -f
- Use decoys: -D RND:10
- Change source port: --source-port 53
- Use timing: -T0 to -T5

13. What are the different output options in Nmap?

Answer:

- -oN: Normal output (e.g., -oN output.txt)
- -oX: XML output (used for scripts or tools)
- -oG: Grepable output (used in scripting)
- -oA: All formats (output.nmap, .xml, .grep)

14. How to resume a paused or incomplete Nmap scan?

Answer:

nmap --resume scan.log

Only works if the original scan was saved using --log-errors.

15. What is a Null scan, and when is it used?

Answer:
Null scan (-sN) sends TCP packets with **no flags set**. It's used to bypass **stateless firewalls** or confuse intrusion detection systems (IDS).

16. Bonus Tips for Viva:

- Be ready to **explain one full command with all options**. Example:

nmap -A -p 22,80,443 --script vuln -oN result.txt 192.168.1.1

- Know how to scan a subnet:

nmap 192.168.1.0/24

- Be clear on **TCP vs UDP scan** differences.
- Be confident explaining **scripts** (vuln, default, brute, etc.).