

1. Nmap

Nmap (Network Mapper) is a **free and open-source** network scanning tool used by network administrators, ethical hackers, and cybersecurity professionals to:

- Discover hosts and services on a network
- Scan open ports
- Detect operating systems and versions
- Map the network

Nmap supports many types of scans, such as:

- TCP SYN scan (`-sS`)
- TCP connect scan (`-sT`)
- UDP scan (`-sU`)
- OS detection (`-O`)
- Version detection (`-sV`)

It's fast, flexible, and scriptable using NSE (Nmap Scripting Engine) for advanced scans.

2. Local IP Address and Network Ranges

A **local IP address** identifies a device within your private LAN (Local Area Network). These usually follow private IP ranges such as:

- `192.168.x.x`
- `10.x.x.x`
- `172.16.x.x – 172.31.x.x`

A **CIDR notation** like `/24` in `192.168.1.0/24` means scanning the IP range `192.168.1.0` to `192.168.1.255`. This covers **256 addresses**, which is common for a home or small office network.

Understanding this allows you to:

- Identify your subnet
- Target the correct IP range for scanning
- Avoid scanning devices outside your network (which could be illegal or unethical)

3. TCP SYN Scan (**nmap -sS**)

This is a **stealthy and fast** way to scan for open TCP ports:

- Sends a TCP SYN packet (used to initiate a connection)
- Waits for SYN-ACK (response from open ports)
- If received, the port is open; if RST (reset), the port is closed

Because the full TCP handshake isn't completed, this scan is harder to detect and log, which makes it ideal for ethical hacking or security assessments.

4. Common Services and Ports

Here's a table of **frequently found ports and services**:

Port	Protocol	Service	Description
21	TCP	FTP	File transfer
22	TCP	SSH	Secure remote login
23	TCP	Telnet	Unencrypted remote login
25	TCP	SMTP	Email sending
53	TCP/UDP	DNS	Domain Name System
80	TCP	HTTP	Web traffic
443	TCP	HTTPS	Secure web traffic
3306	TCP	MySQL	Database

5. Security Risks of Open Ports

Open ports can be **vulnerabilities** if:

- Services running on them are outdated
- Misconfigured (e.g., public admin panels)
- Unnecessary (e.g., test servers left running)


Risks include:

- **Unauthorized access**
- **Data leakage**
- **Malware infections**
- **Remote code execution**

1. What is an open port?

An open port is a network port on a device (e.g., computer, router, server) that is actively accepting connections. Each port corresponds to a specific service or application, like a web server, email server, or database.

- Example: If port 80 is open, it usually indicates that an HTTP server is running and ready to handle web requests.
- Open ports are necessary for communication, but each open port increases the attack surface—especially if the service behind it is outdated or misconfigured.

 Key point: Open ports are not inherently dangerous, but they need to be properly managed and monitored.

2. How does Nmap perform a TCP SYN scan?

A TCP SYN scan (`nmap -sS`) is one of Nmap's fastest and stealthiest scanning techniques. It works by sending a SYN (synchronize) packet to a port, simulating the beginning of a TCP handshake.

- If the port is open, it responds with a SYN-ACK (acknowledge).
- If it is closed, it sends a RST (reset).
- If it's filtered (e.g., blocked by a firewall), no response or an ICMP error is returned.

Unlike a full connection, this scan does not complete the 3-way TCP handshake—making it harder to detect by the target system's logging tools.

🧠 **Key point:** SYN scan is fast, stealthy, and ideal for reconnaissance.

3. What risks are associated with open ports?

Open ports can pose several **security risks**:

- **Unauthorized Access:** If remote access services like SSH (port 22) or RDP (port 3389) are open and poorly secured, attackers might exploit them.
- **Exploits and Vulnerabilities:** Services running on open ports may contain vulnerabilities that can be exploited (e.g., buffer overflows, remote code execution).
- **Information Leakage:** Some services expose sensitive data (e.g., banners or version info) that help attackers during reconnaissance.
- **Botnets and Malware:** Malware may use open ports to communicate with command-and-control servers.

🧠 **Key point:** Every unnecessary open port increases your **attack surface**.

4. Explain the difference between TCP and UDP scanning.

Feature	TCP Scanning	UDP Scanning
Protocol Type	Connection-oriented	Connectionless
Response Expected	SYN-ACK / RST	Often no response (silent)
Detection	Easier to detect (logs exist)	Harder to detect, but more unreliable
Use Cases	Web, SSH, FTP, RDP	DNS, SNMP, DHCP


Tools

`nmap -sS (SYN), -sT`
(Connect)

`nmap -sU`

UDP scans are more difficult because:

- No response \neq closed (could be filtered)
- Firewalls often block or throttle UDP packets

 **Key point:** TCP scans are more reliable; UDP scans are harder to interpret and stealthier.

5. How can open ports be secured?

To secure open ports:

1. **Close Unused Ports:** Only keep ports open if absolutely necessary.
2. **Use Firewalls:** Filter traffic by port, IP, or service.
3. **Enable Authentication:** Protect services (e.g., SSH) with strong passwords or keys.
4. **Patch Services:** Regularly update services and operating systems to patch vulnerabilities.
5. **Use Network Segmentation:** Limit access to critical services based on zones.
6. **Port Knocking / VPN:** Hide ports until a secret sequence or VPN access is used.

 **Key point:** Security isn't just about blocking—it's about **control, visibility, and monitoring**.

6. What is a firewall's role regarding ports?

A **firewall** is a network security system that monitors and controls **incoming and outgoing traffic** based on predefined rules.

Regarding ports, firewalls:

- **Allow or deny traffic** to specific ports (e.g., block port 23 for Telnet)
- **Filter packets** based on IP, protocol, and application

- **Detect anomalies** like port scanning or brute-force attempts
- **Log access attempts** to help in auditing and forensics

Firewalls can be:

- **Host-based** (e.g., Windows Defender Firewall)
- **Network-based** (e.g., routers, UTM devices)

 **Key point:** Firewalls act as the **gatekeepers** of your network traffic.


7. What is a port scan and why do attackers perform it?

A **port scan** is a technique used to identify **open, closed, or filtered ports** on a target system.

Attackers perform port scans to:

- **Discover services** running on the target
- **Fingerprint OS or software versions**
- **Identify weaknesses** (e.g., outdated services)
- **Map the network** for further exploitation

Legitimate users (e.g., sysadmins or ethical hackers) use port scans for **inventory and risk assessment**, while attackers use it for **reconnaissance** before launching attacks.

 **Key point:** Port scanning is like **knocking on all doors** of a building to see which ones are open.

8. How does Wireshark complement port scanning?

Wireshark is a **packet analyzer** that captures and displays the actual data traveling over a network.

In the context of port scanning:

- It lets you **observe raw packets** sent by Nmap (e.g., SYN packets)
- You can **verify scan behavior** (SYN-ACK, RST responses)
- It helps you detect **anomalies** like firewalls dropping packets

- You can **understand protocols in-depth**, down to header fields and flags

Together with Nmap:

- Nmap scans and maps the network
- Wireshark **monitors and analyzes the traffic generated by those scans**

 **Key point:** Wireshark helps you see **what's actually happening** on the wire during a scan.