Name: Gauri Khatate

Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap (free)

Step by Step procedure

1.Install Nmap from official website.

2.Find your local IP range (e.g., 192.168.1.0/24).

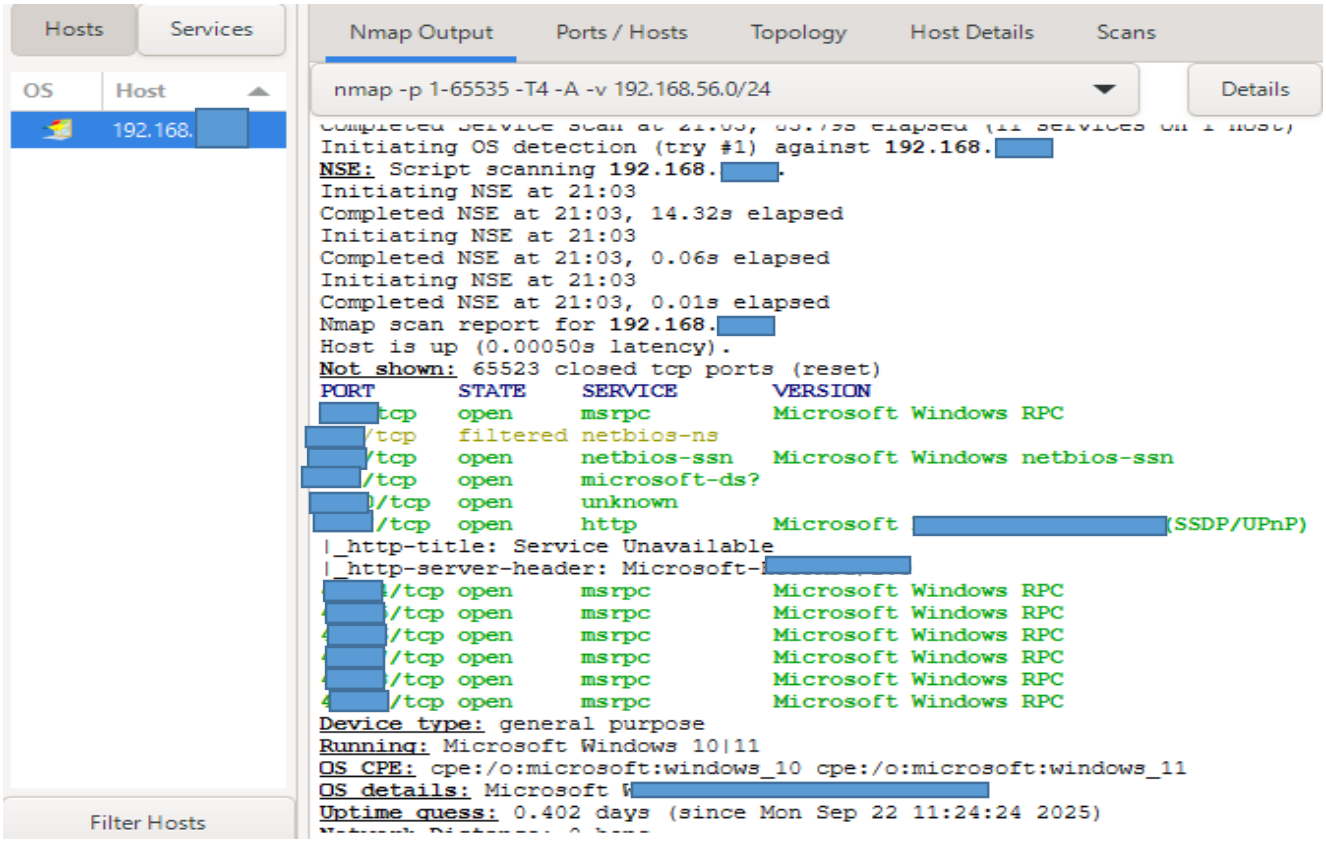
3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

4.Note down IP addresses and open ports found.

How to reproduce (brief)

1. Install Nmap/Zenmap (from nmap.org).
2. Identify your network range: ipconfig / ifconfig.
3. Run nmap -sS -sV -O <target> or use Zenmap “Intense scan”.
4. Save outputs and take screenshots.

Final result:



Interview Questions:

1. What is an open port?
An open port is like an entry door on a computer or server that's actively listening for connections. It allows services (like HTTP on 80, SSH on 22) to communicate over the network. But if unnecessary ports are left open, they can become entry points for attackers.

---

2. How does Nmap perform a TCP SYN scan?
In a SYN scan, Nmap sends only the initial SYN packet of the TCP handshake.

- If it gets **SYN-ACK**, the port is open.
- If it gets **RST**, the port is closed.
- If there's no reply, it's filtered (like blocked by a firewall).
  This method is fast and stealthier because it doesn't complete the handshake.

---

3. What risks are associated with open ports?
Open ports can expose services to attacks such as brute-force login attempts, unpatched service exploits, malware spreading, or unauthorized data access. Basically, every unnecessary open port increases the attack surface.

---

4. Explain the difference between TCP and UDP scanning.
TCP scanning involves connection attempts (handshake based), so results are more reliable.
UDP scanning is connectionless — slower and harder because many services don't respond unless probed correctly, but it helps discover services like DNS or SNMP that run on UDP.

---

5. How can open ports be secured?
By:

- Closing unused ports and disabling unnecessary services
- Using firewalls to restrict access
- Enabling authentication and encryption for required services
- Regular patching to fix service vulnerabilities

---

6. What is a firewall's role regarding ports?
A firewall acts like a security guard. It decides which ports are allowed or blocked based on rules, preventing unauthorized access while letting legitimate traffic through.

---

7. What is a port scan and why do attackers perform it?
A port scan is a way to map which ports are open on a system. Attackers use it for reconnaissance — to identify potential entry points, running services, and possible vulnerabilities.

---

8. How does Wireshark complement port scanning?
Nmap tells you which ports are open, but Wireshark shows you the actual traffic going in and out. With Wireshark, you can capture and analyze packets to understand protocols, detect anomalies, or confirm what services are really doing behind those ports.

Key Concepts:

Port scanning

A technique that probes a host to see which network ports are **open**, **closed**, or **filtered**.
Why it matters: it maps available services (attack surface) so defenders can secure them and attackers can find entry points.
Quick tip: always have permission before scanning someone else's network.

TCP SYN scan

A common, fast "half-open" TCP scan where the scanner sends a **SYN** packet and observes the reply: **SYN-ACK = open**, **RST = closed**, no reply = filtered.
Why it matters: it's efficient and stealthier than completing full handshakes, so it's widely used for initial reconnaissance.

IP ranges (CIDR)

A way to describe a block of IP addresses. Example: 192.168.56.0/24 means addresses 192.168.56.0–192.168.56.255. The /24 shows how many bits are fixed for the network.
Why it matters: scans target ranges, and correct CIDR selection defines scope of reconnaissance.

Network reconnaissance

The process of discovering hosts, services, and topology on a network (using tools like nmap, arp, ping, traceroute).
Why it matters: it builds an inventory of assets and informs where security controls are needed— used by both defenders (to harden systems) and attackers (to find weaknesses).

Open ports

Ports on a host where a service is actively listening for connections (e.g., 22 for SSH, 80 for HTTP).
Why it matters: each open port equals a potential entry point — if the service is vulnerable or misconfigured, it can be exploited.

Network security basics

Core practices to protect networks: minimize open services, apply patches, use firewalls and access controls, enable strong authentication and encryption, and monitor/log traffic.
Why it matters: these basics reduce the attack surface and make exploitation harder and detection easier.
