

Task 1: Network Port Scanning using Nmap

Nmap Scan Summary

Target IP: 192.168.56.1

Command Used: `nmap -sS -oN scan_results.txt 192.168.56.1`

Date of Scan: August 4, 2025

Scan Duration: ~1.08 seconds

Host Status: Up

Open Ports and Services

Port	State	Service	Description
135	open	msrpc	Microsoft RPC endpoint mapper. Used for DCOM services.
139	open	netbios-ssn	NetBIOS Session Service; used for file/printer sharing.
445	open	microsoft-ds	SMB (Server Message Block) over TCP.
2179	open	vmrdp	Microsoft RemoteFX (for VM remote desktop).
7070	open	realserver	RealAudio streaming protocol.
9999	open	abyss	Often used by Abyss Web Server (or seen in backdoors).

Security Risk Assessment

135, 139, 445	High	Commonly exploited Windows ports (e.g., SMB vulnerabilities).
2179	Medium	Used for VM RDP; risk of brute force attacks.
7070	Low/Medium	Might expose internal streaming services.
9999	High	Often used by backdoors; verify the service.

Interview Questions

1. What is an open port?

An open port is a network port that is accepting incoming connections. It indicates that a service is listening for data on that port.

2. How does Nmap perform a TCP SYN scan?

Nmap sends a TCP packet with the SYN flag. If it receives SYN-ACK, the port is open. Nmap then resets the connection, making the scan stealthy.

3. What risks are associated with open ports?

Open ports can expose vulnerable services, allowing attackers to exploit them for unauthorized access,

malware injection, or denial of service.

4. Explain the difference between TCP and UDP scanning.

TCP scans are reliable and confirm open ports via handshakes. UDP scans are less reliable due to filtering but can bypass some firewalls.

5. How can open ports be secured?

By disabling unused services, configuring firewalls, patching software, and using intrusion detection systems.

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

Firewalls regulate access to ports by filtering traffic based on rules, preventing unauthorized access.

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

A port scan discovers open ports/services. Attackers use it to map systems and find vulnerable services.

8. How does Wireshark complement port scanning?

Wireshark inspects network packets in detail, helping detect traffic on open ports and unusual activities.

Conclusion & Learnings

This task helped me understand the fundamentals of port scanning, service exposure, and potential risks.

Tools like Nmap and Wireshark are crucial for cyber defense and system auditing.