

Task 1 – Local Network Port Scanning

Objective

Perform a reconnaissance scan on the local network to identify live hosts and open ports, analyze potential vulnerabilities, and understand the risks associated with exposed services.

Tools Used

- [Nmap](#) for port scanning
 - (Optional) Wireshark for traffic capture and deeper packet inspection
-

Local Network Info

- Local IP: 192.168.56.101
 - IP Range Used: 192.168.56.0/24
-

Commands Used

```
# TCP SYN Scan on the subnet
nmap -sS 192.168.56.0/24 -oN local_network_scan.txt

# Service version detection on the target
nmap -sV 192.168.56.1 -oN service_scan_56.1.txt

# Vulnerability detection using NSE scripts
nmap -sV --script vuln 192.168.56.1 -oN vuln_scan.txt
```

Observations

Live Hosts Detected:

- 192.168.56.1 (Services running)
- 192.168.56.100 (No open ports)
- 192.168.56.101 (Your own system, no open ports)

Open Ports on 192.168.56.1

Port	Service	Description
135	MSRPC	Microsoft RPC
139	NetBIOS-SSN	NetBIOS Session Service
445	Microsoft-DS	SMB file sharing
902	ISS RealSecure	VMware / ISS service
912	Apex Mesh	Possibly custom application port
2869	ICSLAP	Microsoft UPnP service
3306	MySQL	MySQL Database Server
6646	Unknown	Possibly custom/obscure service
8090	OpsMessaging	Web messaging / admin interface

Vulnerability & Risk Analysis




Deep Dive Table

Port	Service	Vulnerability Example	CVE ID	Risk	Recommendation
445	SMB	EternalBlue	CVE-2017-0144	Critical	Disable SMBv1, apply MS17-010 patch
139	NetBIOS	SMB Relay, NTLM Capture	CVE-2019-0708	High	Disable NetBIOS if not used
3306	MySQL	Buffer Overflow / DoS	CVE-2021-27928	Medium	Use strong auth, restrict remote access
902	VMware	Remote Code Execution	CVE-2021-21972	High	Restrict access, keep VMware updated
135	MSRPC	RPC Runtime Vulnerability	CVE-2020-0609	Medium	Patch regularly, restrict unnecessary RPC





Individual Service Analysis

Port 445 (SMB)





-  Vulnerability: EternalBlue

-  CVE: **CVE-2017-0144**
-  Summary: Remote code execution vulnerability used by WannaCry ransomware.
-  Fix: Disable SMBv1, patch with MS17-010





Port 139 (NetBIOS)

-  Vulnerability: SMB relay attacks
-  CVE: **CVE-2019-0708**
-  Summary: NetBIOS can be used to capture NTLM hashes or relay sessions.
-  Fix: Disable NetBIOS if not needed

Port 3306 (MySQL)

-  Vulnerability: Authentication bypass, buffer overflows
-  CVE: **CVE-2021-27928**
-  Summary: Buffer overflow vulnerability in MySQL that can lead to DoS or RCE.
-  Fix: Use strong passwords, bind to localhost, update MySQL

Port 902 (VMware)

-  Vulnerability: Remote Code Execution
-  CVE: **CVE-2021-21972**
-  Summary: VMware vSphere Client remote code execution flaw
-  Fix: Limit access and patch systems

Interview Questions Answered

1. What is an open port?

2. A port that actively listens for incoming network connections.

3. How does Nmap perform a TCP SYN scan?

4. Sends a SYN packet and analyzes the response. SYN-ACK means open; RST means closed.

5. What risks are associated with open ports?

6. They can expose vulnerable services, enabling unauthorized access or exploits.

7. Explain the difference between TCP and UDP scanning.

8. TCP scans use 3-way handshake. UDP is stateless, harder to detect but slower and often blocked.

9. How can open ports be secured?

10. Disable unused services, use firewalls, update software, enforce authentication.

11. **What is a firewall's role regarding ports?**

12. A firewall filters and controls access to/from specific ports.

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

14. A method to discover open ports and services on a host. Attackers use it for recon and vulnerability mapping.

15. **How does Wireshark complement port scanning?**

16. It captures network traffic, allowing deeper inspection of scan behavior and responses.





Files Included

- `local_network_scan.txt` – TCP SYN scan of the subnet
- `service_scan_56.1.txt` – Version detection scan of active host
- `vuln_scan.txt` – Vulnerability detection using NSE scripts
- *(Optional)* `wireshark_capture.pcap` – Packet capture (if used)

17 Submission Link

[Submit Task Here](#)

Bonus Additions (to stand out)

-  Included CVE research and service-specific vulnerability analysis
-  Used Nmap NSE scripts for vulnerability detection
-  Recommendations for securing exposed ports
-  Deep README with professional formatting and markdown tables

GitHub Repo Name Suggestion: `cybersecurity-task1-portscan`

Push the following to your GitHub repo:

- This `README.md`
- Your `.txt` output files from Nmap
- Any screenshots or `.pcap` files if available