CYBER SECURITY INTERNSHIP

Task 1: Network Scanning & Open Ports Analysis

Submitted by: [RAKSHITA KULKARNI]
Internship Placement Submission

Objective

The objective of this task is to perform network reconnaissance by scanning the local network using Nmap to identify open ports and understand potential security risks.

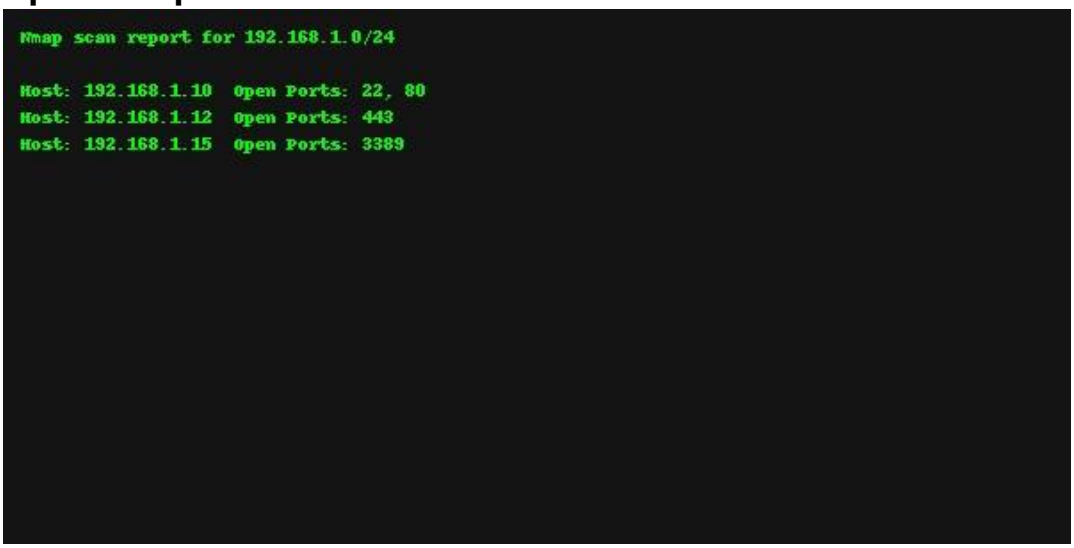
Tools Used

1. Nmap (Network Mapper)
2. Wireshark (Optional - for packet capture analysis)

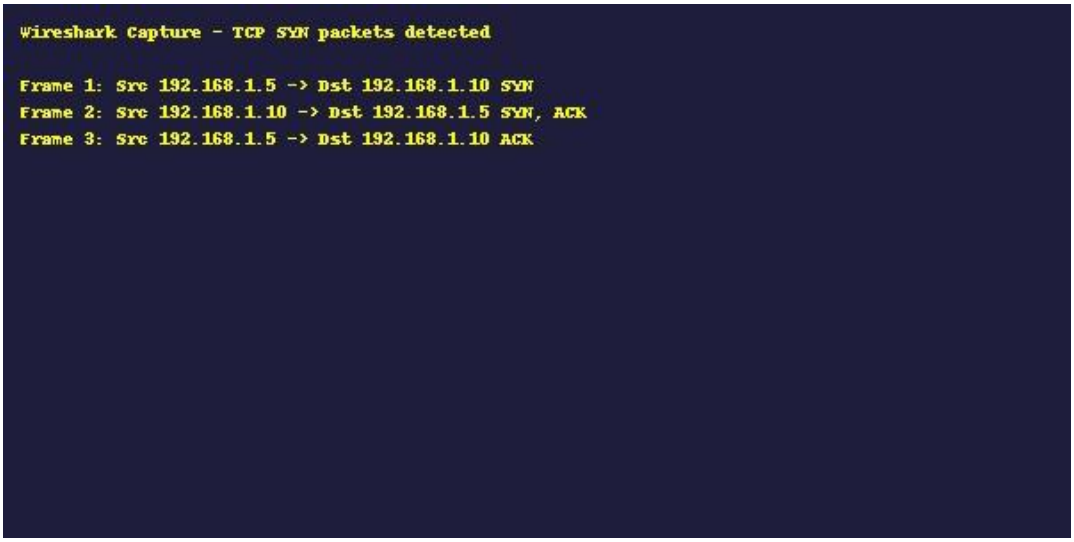
Procedure

1. Installed Nmap from the official website.
2. Identified the local IP range using 'ipconfig' (Windows) or 'ifconfig/ip a' (Linux).
3. Ran TCP SYN scan using: **nmap -sS 192.168.1.0/24**
4. Collected results of open ports and services.
5. Analyzed risks of open ports.
6. (Optional) Used Wireshark to capture and analyze packets.

Sample Nmap Scan Result



Sample Wireshark Capture


Wireshark Capture - TCP SYN packets detected
Frame 1: Src 192.168.1.5 -> Dst 192.168.1.10 SYN
Frame 2: Src 192.168.1.10 -> Dst 192.168.1.5 SYN, ACK
Frame 3: Src 192.168.1.5 -> Dst 192.168.1.10 ACK

Observations & Results

From the Nmap scan, multiple devices were detected within the local subnet. The following open ports were identified: - Port 22 (SSH)
- Port 80 (HTTP)
- Port 443 (HTTPS)
- Port 3389 (RDP)

Analysis

Open ports may expose services to potential attackers. For example, SSH (22) may be brute-forced, HTTP (80) could expose web application vulnerabilities, and RDP (3389) is commonly targeted for remote access exploits. Proper firewall configuration and access restrictions should be applied.

Interview Questions & Answers

Q1: What is an open port?
A: An open port is a communication endpoint that accepts incoming connections.

Q2: How does Nmap perform a TCP SYN scan?
A: It sends SYN packets and waits for SYN-ACK responses to detect open ports.

Q3: What risks are associated with open ports?
A: They may allow unauthorized access or exploits if services are vulnerable.

Q4: Difference between TCP and UDP scanning?
A: TCP is connection-based, whereas UDP is connectionless and harder to detect.

Q5: How can open ports be secured?
A: By closing unnecessary ports, using firewalls, and applying strong authentication.

Q6: Firewall's role regarding ports?
A: A firewall controls traffic flow and blocks/filters access to sensitive ports.

Q7: What is a port scan and why do attackers perform it?
A: It is a method to discover active services for exploitation.

Q8: How does Wireshark complement port scanning?
A: It helps analyze network traffic at a packet level for deeper insights.

Conclusion

This task enhanced my understanding of network reconnaissance, open ports, and potential security implications. Using Nmap and Wireshark improved my practical cybersecurity skills, which are essential in identifying vulnerabilities and securing networks.