Cyber Security Internship

Title: Task 1: Scan Your Local Network for Open Ports

Name: Rithika Swami

Date: June 2025

Objective

Learn to discover open ports and understand network exposure using Nmap and Wireshark.

Tools Used

- Nmap (for scanning open ports)
- Wireshark (for packet capture)

Nmap Scan Results

- Installed Nmap from the official website.
- Identified the IP range using ipconfig (192.168.1.0/24).
- Ran the command: nmap -T4 -A 192.168.1.0/24 and nmap -sS 192.168.1.0/24
- Noted down IP addresses and open ports found.
- Analyzed the services associated with the open ports.
- Identified potential security risks and recommended mitigations.
- Exported results for record and review.
- Results: [NMAP HTML]

Devices Detected

IP	OS / Details	Open Ports
192.168.1.1	Linux (HP ProCurve MSM422)	*(Device is a WAP)*
192.168.1.38	Unknown (All ports closed)	No open ports
192.168.1.41	Windows 10 (21H2)	135, 139, 445, 2179, 2869, 5357

- The Windows host (192.168.1.41) has open ports (135, 139, 445) which are associated with services like RPC and NetBIOS that have known exploits.
- The access point exposes its OS information (Linux), making it a potential target for attacks.

common services:

1. **Port 135 (Windows RPC)**

What it is: Enables remote procedure calls (Windows services communication).
Security Concern: Frequently targeted by malware (e.g., MSRPC exploits) because it allows remote code execution if misconfigured.

2. **Port 139 (NetBIOS Session Service)**

What it is: Enables file and printer sharing over a local network.
Security Concern: Commonly scanned for identifying file shares and extracting sensitive information.

3. **Port 445 (Microsoft-DS / SMB)**

What it is: Enables access to files, printer sharing, and IPC (Windows).
Security Concern: Frequently used for ransomware attacks (e.g., WannaCry) and exploits like EternalBlue.

4. **Port 2179 (Windows RDP Session Service)**

What it is: Enables remote connections via RDP for Hyper-V Virtual Machines.
Security Concern: Brute-force attacks and unauthorized access if exposed to untrusted networks.

5. **Port 2869 (Windows HTTP Services)**

What it is: Enables UPnP device detection over HTTP for service configuration.
Security Concern: UPnP can be leveraged for unauthorized access or internal network attacks if not configured securely.

6. **Port 5357 (Windows HTTP Services)**

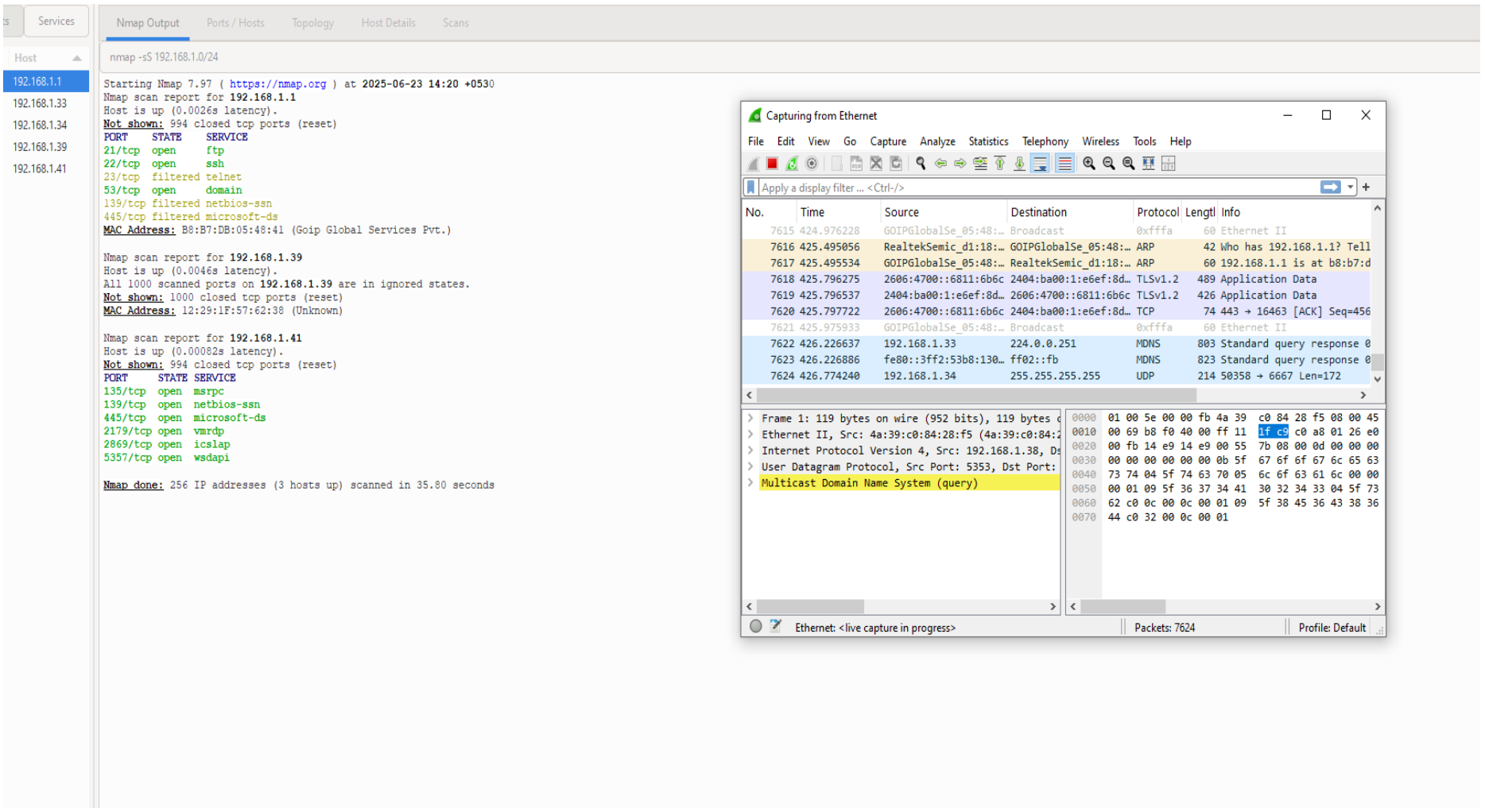
What it is: Enables service discovery and access over the Windows HTTP services.
Security Concern: Could expose device information for reconnaissance attacks.

In addition to scanning, I used **Wireshark** to observe network traffic generated by the Nmap scans.

Methodology:

- Started a Wireshark capture on the active network interface.
- Ran the **Nmap SYN scan** (nmap -sS 192.168.1.0/24) while capturing traffic.

- Analyzed the captured packets to observe the SYN and SYN-ACK exchanges between the scanner and target hosts.



- Verified that the **SYN scan** sends a SYN packet to initiate the handshake.
- Confirmed that open ports responded with a **SYN-ACK**, and closed ports responded with a **RST** packet.
- Observed the scanner terminating connections promptly after receiving SYN-ACK, making it stealthier than a full connect scan.

Final Conclusion:

In this task, I learned how to use Nmap and Wireshark for network reconnaissance.
The Nmap scans identified open ports and services across the network, highlighting common services and potential security concerns.
The Wireshark captures offered deep insight into the TCP handshake process.