Day 1

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, Wireshark

Nmap: **Network Mapper**

Nmap, short for Network Mapper, is a free and open-source tool used for network discovery and security auditing. It's primarily used to identify hosts, services, and open ports on a network by sending packets and analyzing the responses. Nmap can also detect operating systems and identify potential security vulnerabilities.

Wireshark:

Wireshark is a free and open-source network protocol analyzer primarily used for capturing and analyzing network traffic in real-time. It allows users to inspect data at the packet level, making it a valuable tool for troubleshooting, security analysis, and network protocol development.

Step1: Open kali linux terminal.

Step2: Check the network ip address of that system (Command= ip a).

Step3: Check the devices that are connected to that network using Nmap tool

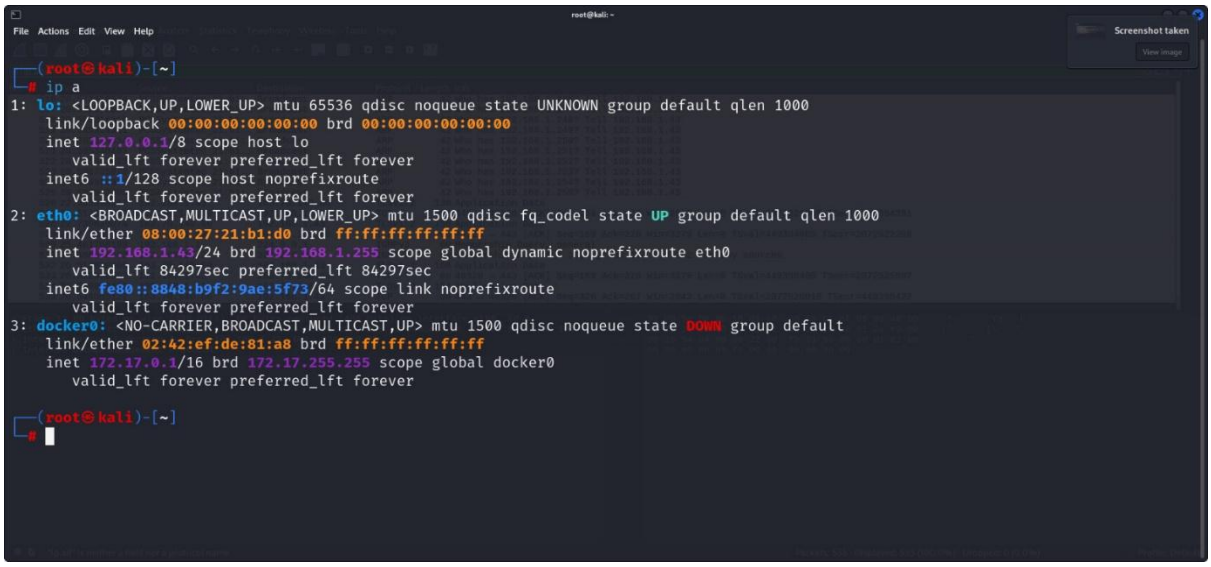
(Command = nmap -sS 192.168.1.0/24).

Step4: Check what are all the ports that are opened in that devices.

Step5: Capture the network flow and analyse with the wireshark tool.

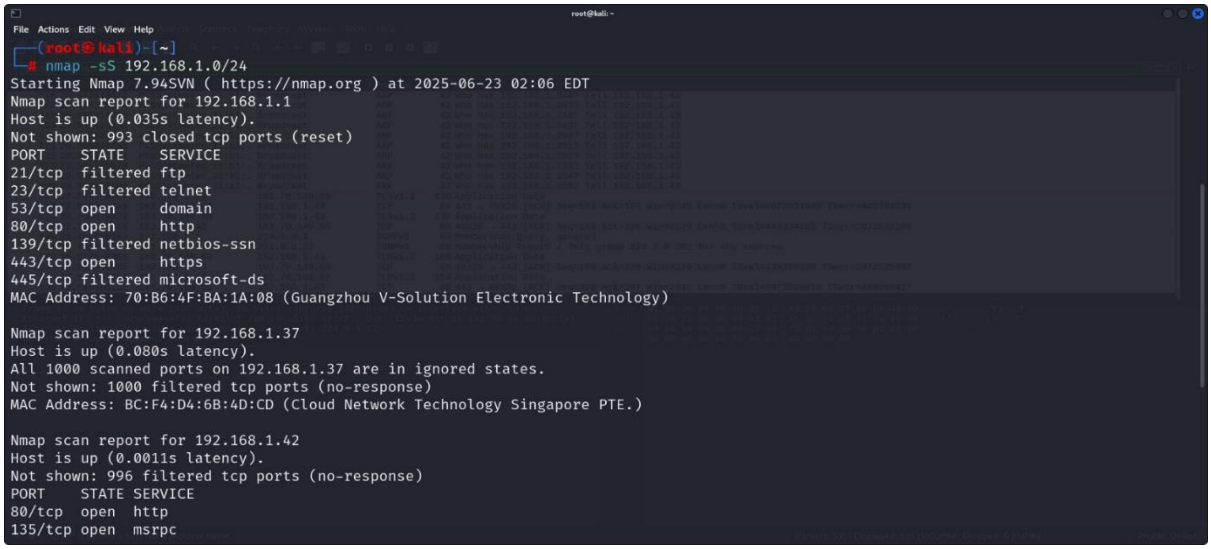
IP address of network = 192.168.1.0/24

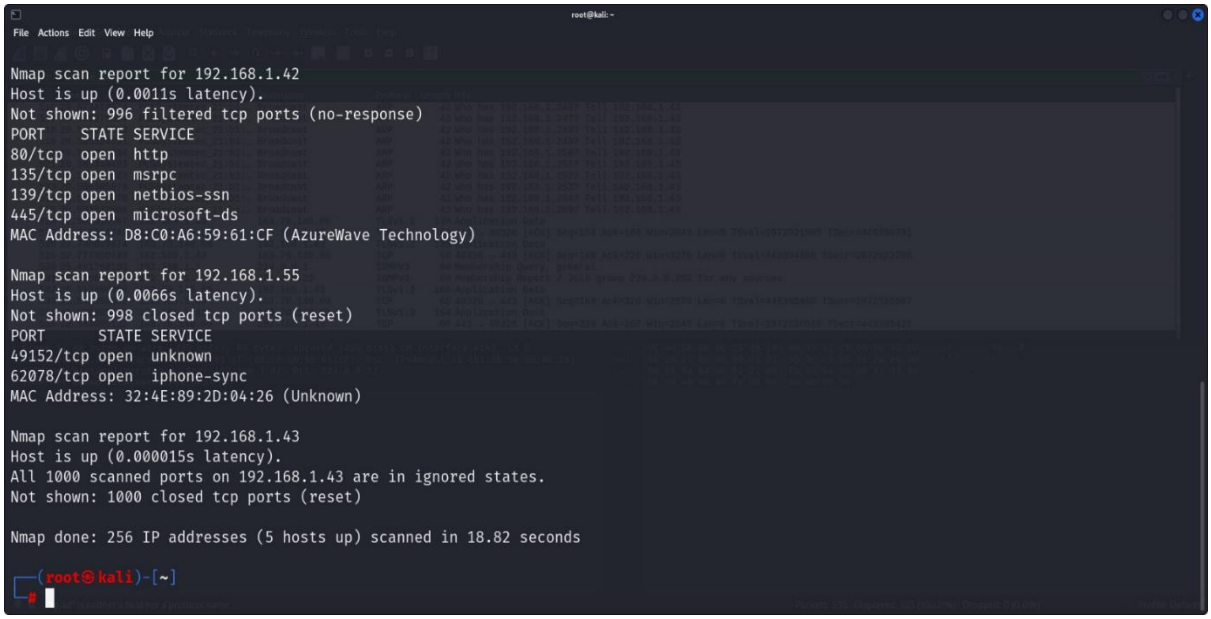
IP addrss of system =192.168.1.43



Systems that are connected to that network 192.168.1.0/24 and Open ports

Systems ip addresses		**Open ports**
192.168.1.1	---------	**21,23,53,80,139,443,445**
192.168.1.37	---------	**all are filtered (No open ports)**
192.168.1.42	---------	**80,135,139,445**
192.168.1.43	---------	**49152,62078**
192.168.1.55	----------	**No open ports**





Port numbers and services that are running on that port

Port number	Service
21	File Transfer Protocol
23	Telnet
53	Domain Name System
80	Hypertext Transfer Protocol
139	NetBIOS Session Service
443	Hypertext Transfer Protocol Secure
445	Server Message Block
49152	Windows Remote Procedure Call
62078	----------

Potential Security risks from open ports:

File Transfer protocol (21): Port 21 is primarily used by the File Transfer Protocol (FTP) for establishing control connections between a client and a server. This port handles the initial communication, including commands and responses, necessary for managing file transfers. While the control connection is established on port 21, the actual data transfer, like uploading or downloading files, often occurs on different ports, sometimes port 20 or dynamically assigned ports.

Open port 21, commonly used by FTP, poses several security risks due to its inherent vulnerability to unencrypted communication and potential for exploitation. Attackers can exploit these vulnerabilities to gain unauthorized access, steal credentials, and potentially compromise the entire system.

Telnet (23): Port 23 is primarily associated with the Telnet protocol. Telnet is a network protocol that enables remote access to devices and servers, allowing users to interact with them as if they were directly connected to a local console. Telnet uses port 23 by default for communication.

An open Telnet port (port 23) presents significant security risks due to its use of unencrypted communication, making it vulnerable to eavesdropping and unauthorized access. Attackers can exploit this to steal sensitive information like usernames and passwords transmitted during Telnet sessions.

Domain Name System (53): Port 53 is primarily used by the Domain Name System (DNS) service. DNS uses port 53 to translate human-readable domain names (like google.com) into numerical IP addresses that computers use to locate resources on the internet. This process is essential for web browsing, email, and other internet activities.

An open port 53, used by DNS (Domain Name System), can expose a network to several security risks. These include DDoS attacks, DNS spoofing, and DNS hijacking, all of which can disrupt service, redirect users to malicious sites, or expose sensitive information.

Hypertext Transfer Protocol (80): Port 80 is the default port used for HTTP (Hypertext Transfer Protocol) web traffic. It's the standard port that web browsers and servers use to communicate when a user accesses a website using the "http://" protocol.

Open port 80, commonly used for HTTP traffic, presents several security risks due to its unencrypted nature. These risks include the potential for man-in-the-middle attacks, where attackers can intercept and read sensitive data like login credentials and personal information. Additionally, the lack of authentication and data integrity mechanisms in HTTP makes it susceptible to various exploits.

NetBIOS Session Service (139): Port 139 is primarily associated with the NetBIOS Session Service, which is a legacy protocol used for file and printer sharing in Windows networks. It enables communication between devices on a local network, allowing them to ac-cess shared resources like files and printers

Open port 139, associated with NetBIOS over TCP, poses significant security risks, particularly in Windows environments, due to its use in file and printer sharing. Attackers can exploit vulnerabilities in SMB (Server Message Block) protocols running on this port to gain unauthorized access to sensitive data, potentially leading to ransomware attacks, data breaches, and espionage.

Hypertext Transfer Protocol Secure (443): Port 443 is primarily used for HTTPS (Hypertext Transfer Protocol Secure) traffic, which is the secure version of HTTP used for encrypted communication between web browsers and servers. It ensures that data transmitted over the internet, like your login credentials or payment informa-tion, is encrypted and protected from potential eavesdropping.

While Port 443, commonly used for HTTPS, is generally considered secure due to encryption, it is not entirely immune to security risks. Open port 443 can still be vulnerable to attacks like Man-in-the-Middle (MITM) attacks, DDoS attacks, and attacks exploiting vulnerabilities in SSL/TLS protocols. Additionally, misconfigurations or outdated software using port 443 can expose vulnerabilities.

Server Message Block (445): Port 445 is primarily used by the Server Message Block (SMB) protocol in Windows networks for file and printer sharing, as well as for Active Directory operations. It allows devices on a network to access shared resources like files and printers. While SMB over port 445 is common on local networks, it can also be used for remote access, making it a potential security risk if not properly managed.

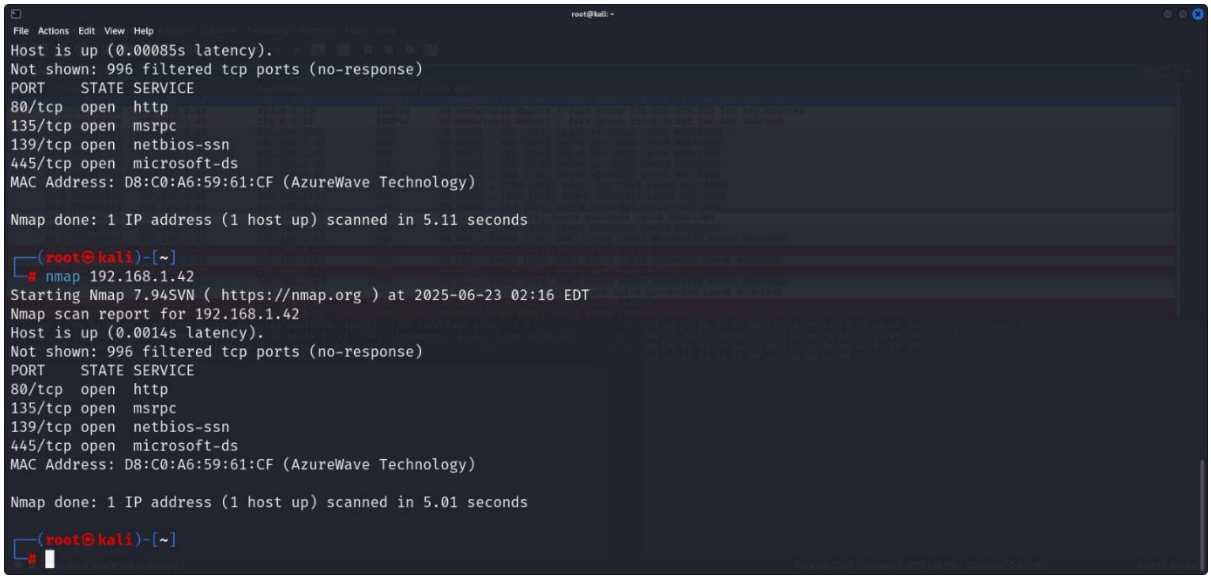
An open port 445 poses a significant security risk because it's associated with the Server Message Block(SMB) Protocol, which is used for file and printer sharing in Windows. Attackers can exploit vulnerabilities in older versions of SMB to gain unauthorized access to systems, potentially leading to malware infections, ransomware attacks, or data breaches.

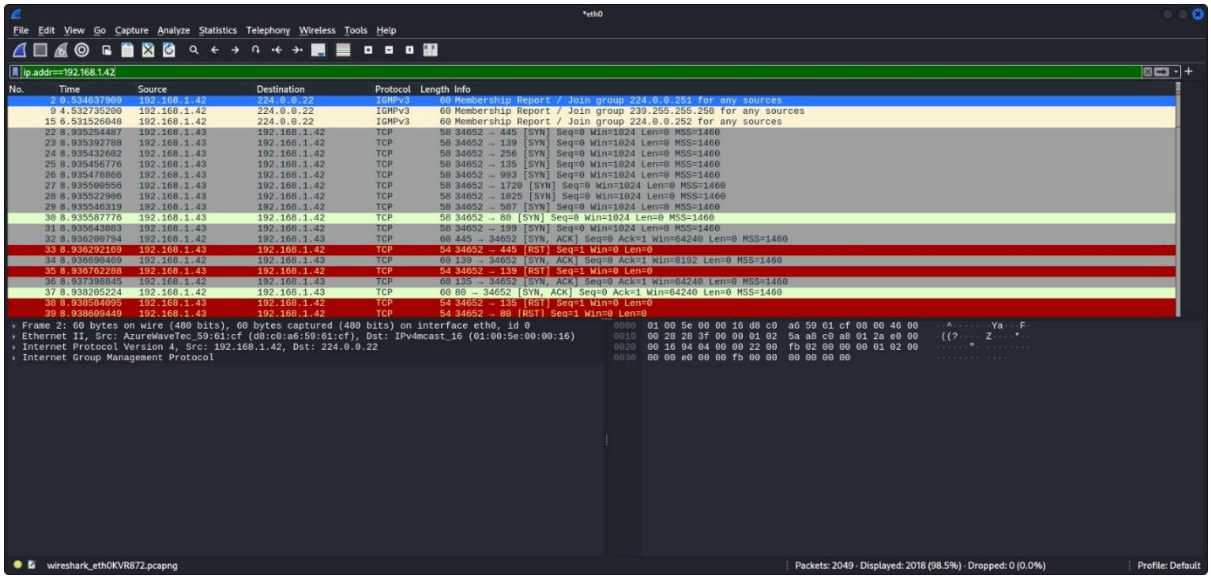
Windows Remote Procedure Call (49152): Port 49152, part of the dynamic or private port range (49152-65535), is commonly used by Windows RPC (Remote Procedure Call) services for communication. Specifically, it's used when a Windows service, like those involved in WMI or DCOM, negotiates a connection through port 135 and then communicates over a dynamically assigned port. These dynamic ports are not assigned or registered by IANA and are used for ephemeral, or temporary, connections.

Open port 49152, belonging to the dynamic and private port range (49152-65535), can pose security risks, primarily because it's often associated with Windows Remote Procedure Call (RPC) and can be exploited for lateral movement, enumeration, and privilege escalation. While not inherently dangerous, its use by vulnerable services or improper configuration can create entry points for attackers.

Packet capture with Wireshark

IP address 192.168.1.42





Nmap scan on 192.168.1.43 system it shows what are all the ports that are opened on the system.The scan will be captured by wireshark that show the information about the attacking system and the target sysem.
