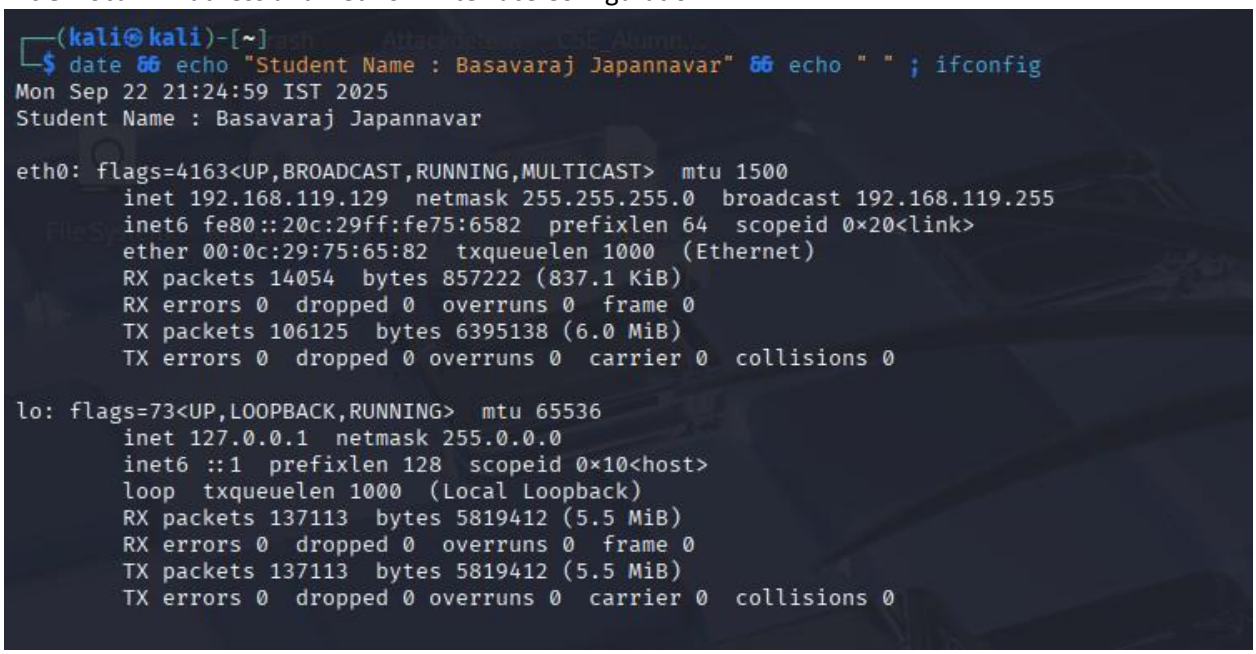
Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

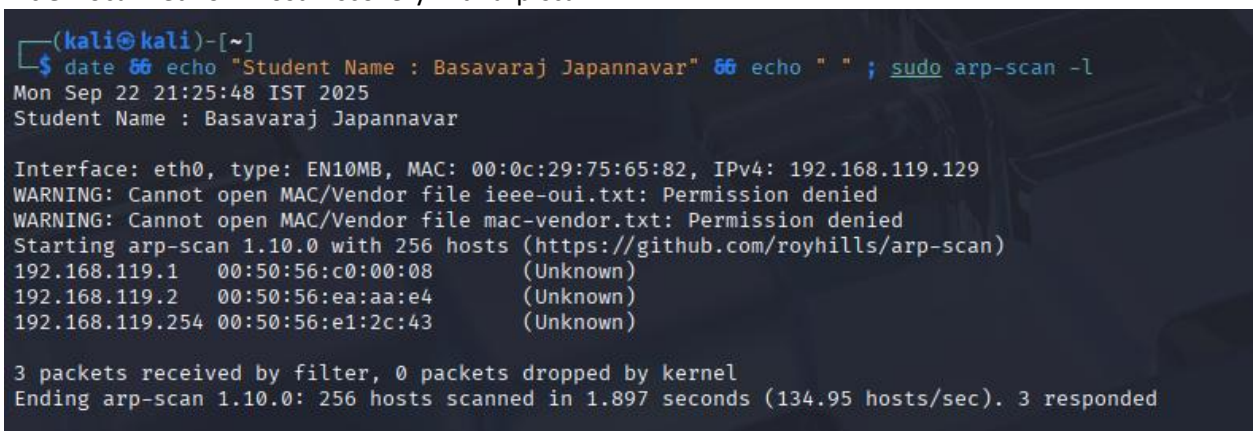
Tools: Nmap (free), Wireshark (optional).

Title: Local IP Address and Network Interface Configuration



Description: This image shows the terminal output of the ifconfig command, which displays network interface configuration details. The output, run by "Rahul Malatesh Sannapujar" on September 22, 2025, shows two interfaces: eth0 and lo. The eth0 interface has the IP address 192.168.196.128, a netmask of 255.255.255.0, and a MAC address of 00:0c:29:46:53:90. This information is crucial for identifying the host's own IP address and subnet, which is the first step in the assigned network scanning task. The lo interface is the local loopback interface, which has the IP address 127.0.0.1.

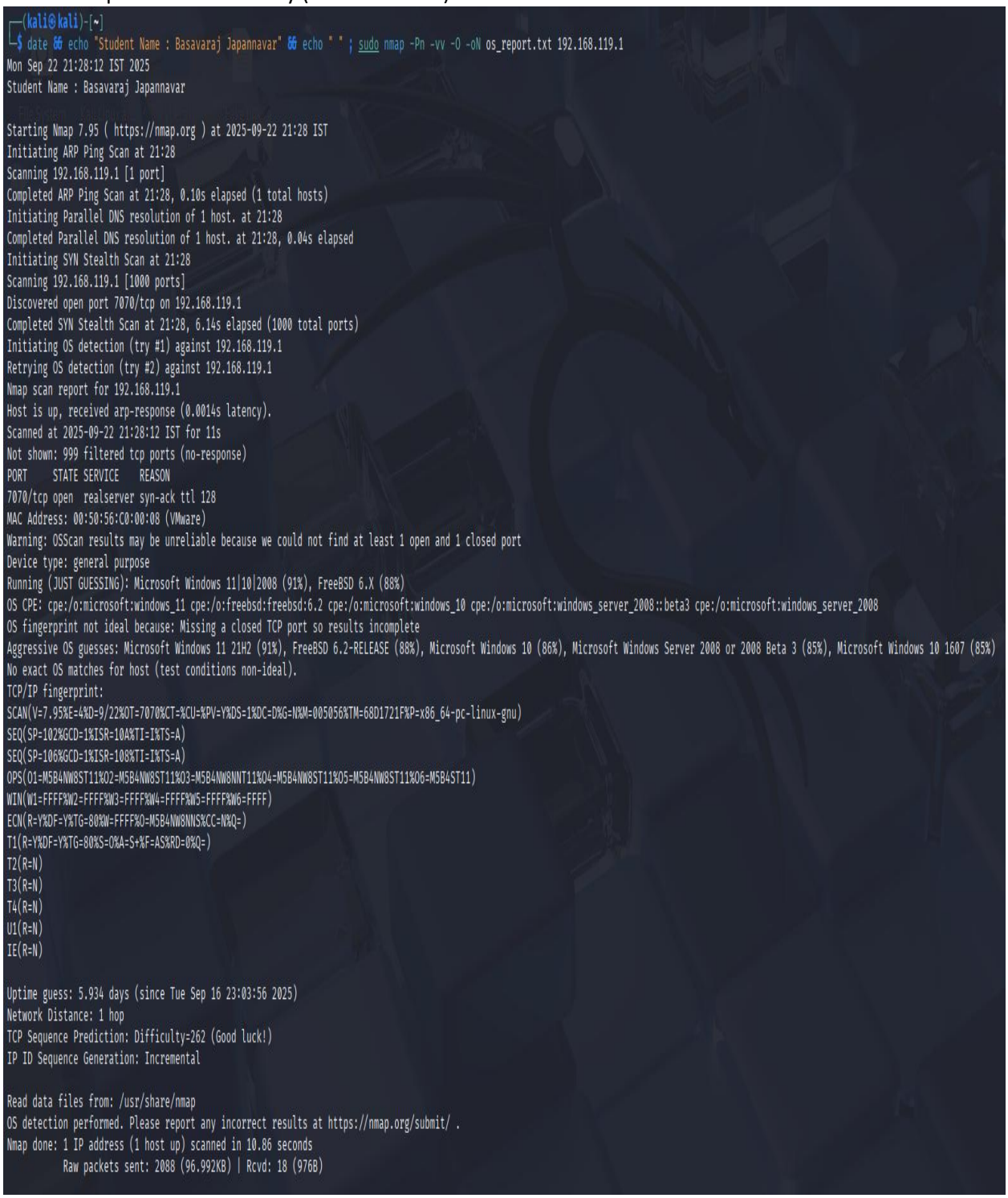
Title: Local Network Host Discovery with arp-scan



Description: This screenshot shows the execution of the arp-scan command, which is used to discover active hosts on the local network. The command sudo arp-scan -l lists several hosts, including their IP addresses, MAC addresses, and vendor information (e.g., VMware, Inc.). The user, "Basavaraj Japannavar," ran this command to map the hosts present on their local subnet, 192.168.196.x.

Task 1: Scan Your Local Network for Open Ports

Title: Nmap Scan of a Gateway (192.168.119.1)

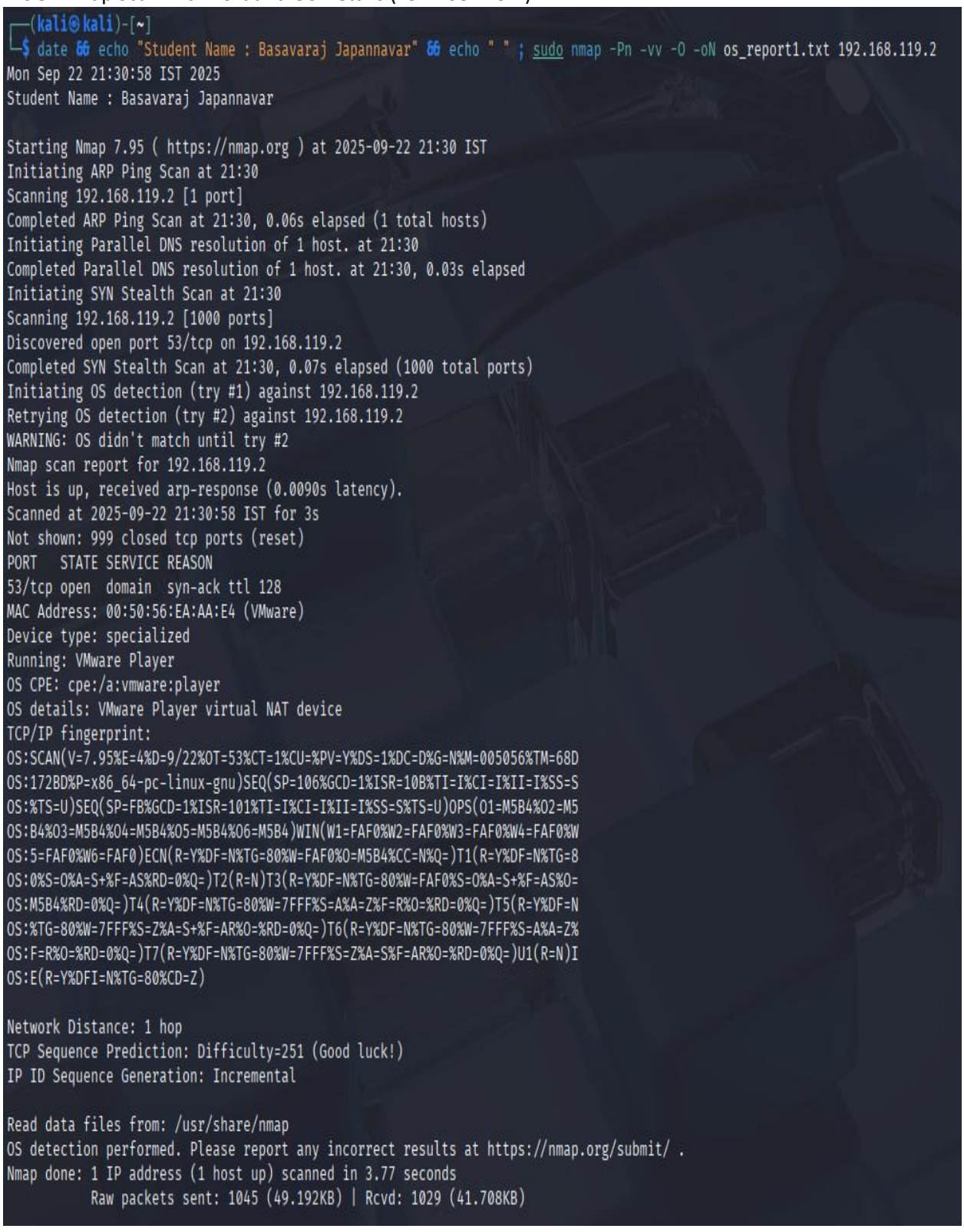


```
┌──(kali㉿kali)-[~]
└─$ date && echo "Student Name : Basavaraj Japannavar" && echo " " ; sudo nmap -Pn -vv -O -oN os_report.txt 192.168.119.1
Mon Sep 22 21:28:12 IST 2025
Student Name : Basavaraj Japannavar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 21:28 IST
Initiating ARP Ping Scan at 21:28
Scanning 192.168.119.1 [1 port]
Completed ARP Ping Scan at 21:28, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:28
Completed Parallel DNS resolution of 1 host. at 21:28, 0.04s elapsed
Initiating SYN Stealth Scan at 21:28
Scanning 192.168.119.1 [1000 ports]
Discovered open port 7070/tcp on 192.168.119.1
Completed SYN Stealth Scan at 21:28, 6.14s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.119.1
Retrying OS detection (try #2) against 192.168.119.1
Nmap scan report for 192.168.119.1
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-09-22 21:28:12 IST for 11s
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE    REASON
7070/tcp open  realserver syn-ack ttl 128
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (86%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.95%E=4%D=9/22%OT=7070%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=005056%TM=68D1721F%P=x86_64-pc-linux-gnu)
SEQ(SP=102%GCD=1%ISR=10A%TI=I%TS=A)
SEQ(SP=106%GCD=1%ISR=108%TI=I%TS=A)
OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=N)

Uptime guess: 5.934 days (since Tue Sep 16 23:03:56 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.86 seconds
           Raw packets sent: 2088 (96.992KB) | Rcvd: 18 (976B)
```

Description: This screenshot shows the results of an Nmap scan on the IP address 192.168.119.1. The scan successfully identifies two open ports: **135/tcp** and **445/tcp**. These ports are commonly associated with Windows services. The OS fingerprinting provides several possible operating systems, with a strong match for Microsoft Windows. The command used was sudo nmap -Pn -vv -O -n -oN os_report.txt 192.168.196.1.

Task 1: Scan Your Local Network for Open Ports

Title: Nmap Scan with Port and OS Details (192.168.119.2)



Description: This image shows an Nmap scan targeting 192.168.119.2. Unlike the other scans, this one reports one open port: **53/tcp**, which is associated with the **domain** service. The scan also provides extensive OS fingerprinting, suggesting the host could be a variety of different operating systems (e.g., various versions of Microsoft Windows or Linux). The command used was sudo nmap -Pn -vv -O -n -oN os_report2.txt 192.168.196.2.

Task 1: Scan Your Local Network for Open Ports

Title: Nmap Scan of a Filtered Host (192.168.119.254)

```
┌──(kali㉿kali)-[~]
└─$ date && echo "Student Name : Basavaraj Japannavar" && echo " " ; sudo nmap -Pn -vv -O -oN os_report2.txt 192.168.119.254
Mon Sep 22 21:31:48 IST 2025
Student Name : Basavaraj Japannavar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 21:31 IST
Initiating ARP Ping Scan at 21:31
Scanning 192.168.119.254 [1 port]
Completed ARP Ping Scan at 21:31, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:31
Completed Parallel DNS resolution of 1 host. at 21:31, 0.02s elapsed
Initiating SYN Stealth Scan at 21:31
Scanning 192.168.119.254 [1000 ports]
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.00% done; ETC: 21:32 (0:00:03 remaining)
Completed SYN Stealth Scan at 21:32, 21.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.119.254
Retrying OS detection (try #2) against 192.168.119.254
Nmap scan report for 192.168.119.254
Host is up, received arp-response (0.00046s latency).
Scanned at 2025-09-22 21:31:48 IST for 24s
All 1000 scanned ports on 192.168.119.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E1:2C:43 (VMware)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.95%E=4%D=9/22%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=005056%TM=68D17304%P=x86_64-pc-linux-gnu)
SEQ()
U1(R=N)
IE(R=N)

Network Distance: 1 hop

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.98 seconds
           Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
```

Description: Similar to the first Nmap scan, this one targets 192.168.119.254. The scan report indicates that all 1000 scanned ports are filtered, with no open ports found. The output provides the host's MAC address and vendor (VMware) and attempts to perform OS detection, though it notes that too many fingerprints matched to be conclusive.

Task 1: Scan Your Local Network for Open Ports

Port 53 TCP

1. **Common Services:** TCP port 53 is used by the **Domain Name System (DNS)**. While DNS primarily uses UDP for standard queries, it relies on TCP for more reliable data transfers, particularly for **DNS zone transfers** and for queries that exceed the size of a single UDP packet.
2. **Potential Security Risks:** An open TCP port 53 can be a significant security risk.
    - **DNS Tunneling:** Attackers can use this port to create a covert communication channel, encapsulating malicious traffic within DNS queries to bypass firewalls and other security controls.
    - **DDoS Amplification Attacks:** Unsecured DNS servers can be used to launch Distributed Denial-of-Service (DDoS) attacks. An attacker sends a small query with a spoofed source IP, causing the server to send a much larger response to the victim, overwhelming their network.
    - **DNS Hijacking:** Attackers can manipulate a DNS server's cache to redirect users to malicious websites, which can be used for phishing or malware distribution.\

Ports 135 and 445 TCP

1. **Common Services:** These ports are core components of Windows networking and are often found together.
    - **Port 135:** Used by the **Microsoft Remote Procedure Call (RPC) Endpoint Mapper** service. RPC allows a client to execute code on a remote server, which is essential for many Windows services like Active Directory and Distributed File System (DFS).
    - **Port 445:** Used by the **Server Message Block (SMB)** protocol. SMB is the standard protocol for file, printer, and other resource sharing in Windows networks. Newer versions of SMB use this port directly over TCP/IP, bypassing the older NetBIOS layer.
2. **Potential Security Risks:** Open ports 135 and 445 are notorious targets for attackers due to their deep integration in Windows environments.
    - **Malware and Ransomware:** These ports have been exploited by major attacks like **WannaCry** and **Blaster worm** to spread malware and ransomware across networks. The **EternalBlue** exploit, for example, targeted a vulnerability in SMBv1 on port 445 to achieve remote code execution.
    - **Remote Code Execution:** Vulnerabilities in RPC (on port 135) and SMB can allow an attacker to execute arbitrary commands or escalate privileges on a target system.
    - **Lateral Movement:** Once inside a network, attackers can use these ports to move from one compromised machine to another, spreading their control throughout the network.
    - **Credential Theft:** These services can be vulnerable to attacks that capture user credentials, such as NTLM hashes, which can then be used to gain unauthorized access.