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

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;ifconfig
Monday 22 September 2025 07:05:04 PM IST
Student Name : Rahul Malatesh Sannapujar

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.196.128  netmask 255.255.255.0  broadcast 192.168.196.255
        inet6 fe80::20c:29ff:fe46:5390  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:46:53:90  txqueuelen 1000  (Ethernet)
        RX packets 137  bytes 42660 (41.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 104  bytes 42785 (41.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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.

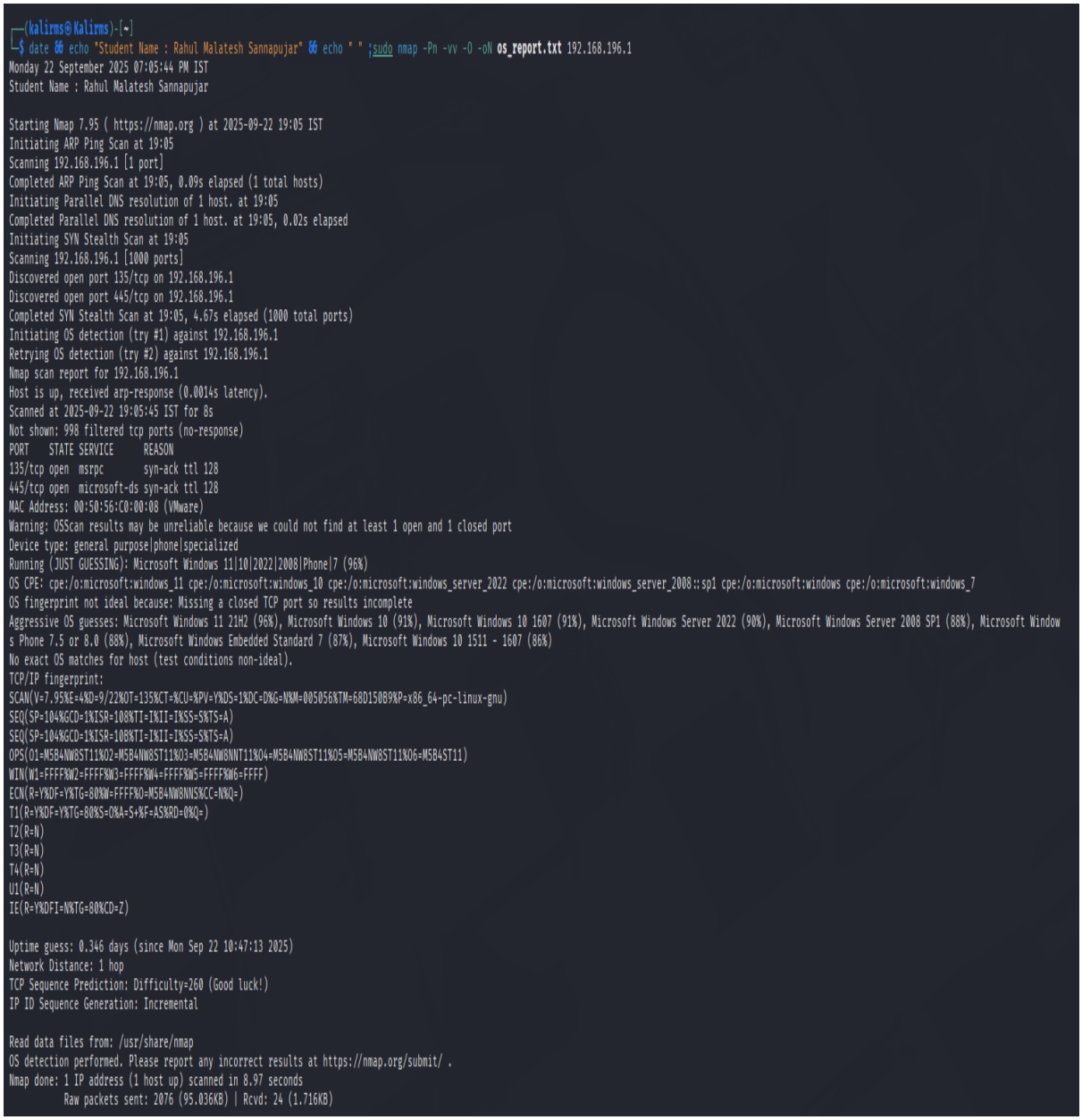
Title: Local Network Host Discovery with arp-scan

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;sudo arp-scan -l
Monday 22 September 2025 07:05:19 PM IST
Student Name : Rahul Malatesh Sannapujar

[sudo] password for kalirms:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:46:53:90, IPv4: 192.168.196.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.196.1   00:50:56:c0:00:08       VMware, Inc.
192.168.196.2   00:50:56:e0:84:a5       VMware, Inc.
192.168.196.131 00:0c:29:c5:40:69       VMware, Inc.
192.168.196.254 00:50:56:ed:06:1d       VMware, Inc.
```

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, "Rahul Malatesh Sannapujar," 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 (192.168.196.1)

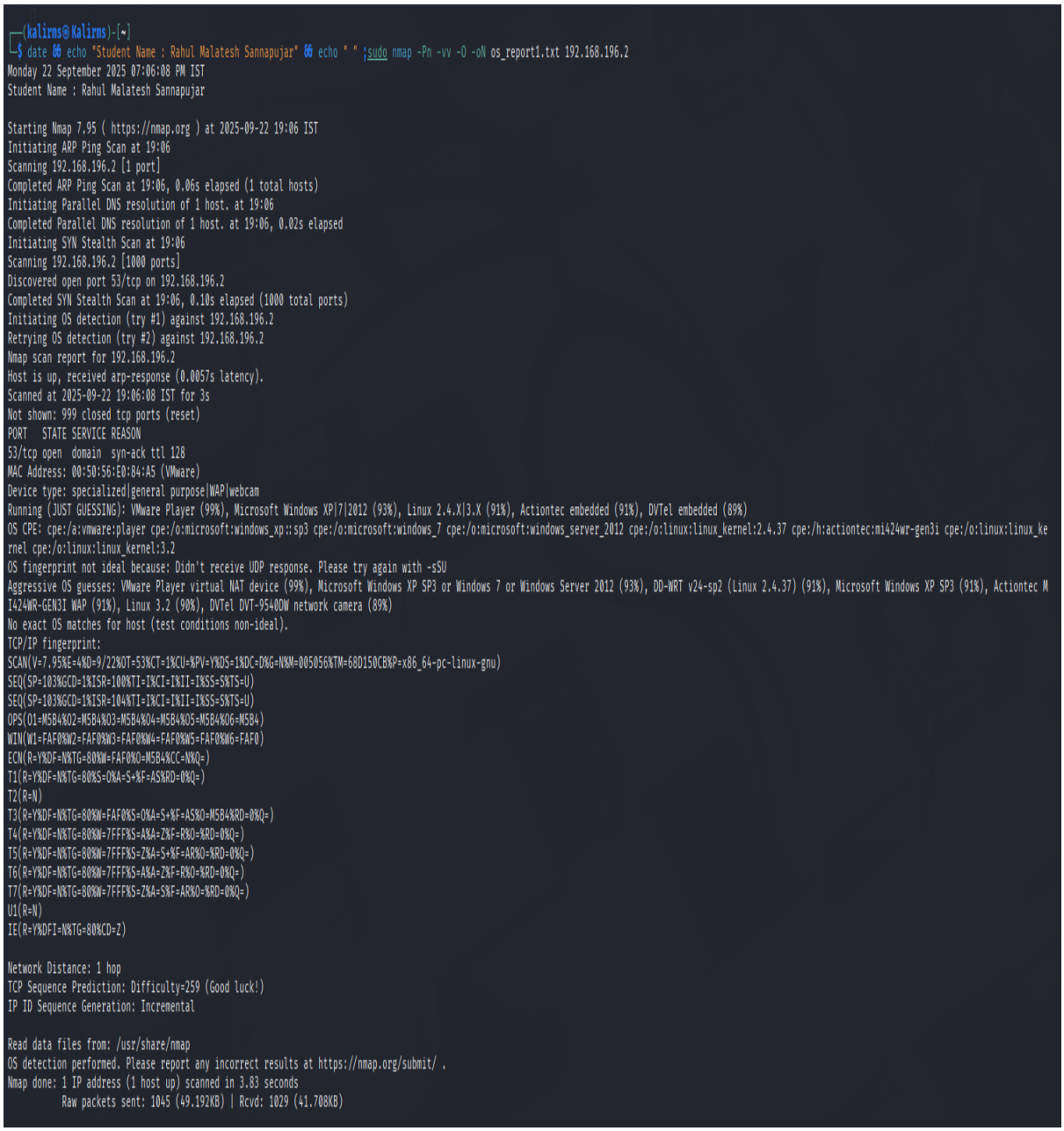


```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;sudo nmap -Pn -vv -O -oN os_report.txt 192.168.196.1
Monday 22 September 2025 07:05:44 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 19:05 IST
Initiating ARP Ping Scan at 19:05
Scanning 192.168.196.1 [1 port]
Completed ARP Ping Scan at 19:05, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:05
Completed Parallel DNS resolution of 1 host. at 19:05, 0.02s elapsed
Initiating SYN Stealth Scan at 19:05
Scanning 192.168.196.1 [1000 ports]
Discovered open port 135/tcp on 192.168.196.1
Discovered open port 445/tcp on 192.168.196.1
Completed SYN Stealth Scan at 19:05, 4.67s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.196.1
Retrying OS detection (try #2) against 192.168.196.1
Nmap scan report for 192.168.196.1
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-09-22 19:05:45 IST for 8s
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack ttl 128
445/tcp open  microsoft-ds 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|phone|specialized
Running (JUST GUESSING): Microsoft Windows 11|10|2022|2008|Phone|7 (96%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows 11 21H2 (96%), Microsoft Windows 10 (91%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2022 (90%), Microsoft Windows Server 2008 SP1 (88%), Microsoft Window
s Phone 7.5 or 8.0 (88%), Microsoft Windows Embedded Standard 7 (87%), Microsoft Windows 10 1511 - 1607 (86%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.95%E=4%D=9/22%OT=135%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=005056%TM=68D150B9%P=x86_64-pc-linux-gnu)
SEQ(SP=104%GCD=1%ISR=108%TI=I%II=I%SS=S%TS=A)
SEQ(SP=104%GCD=1%ISR=10B%TI=I%II=I%SS=S%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=Y%DFI=N%TG=80%CD=Z)

Uptime guess: 0.346 days (since Mon Sep 22 10:47:13 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (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 8.97 seconds
          Raw packets sent: 2076 (95.036KB) | Rcvd: 24 (1.716KB)
```

Description: This screenshot shows the results of an Nmap scan on the IP address 192.168.196.1. 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 (192.168.196.2)

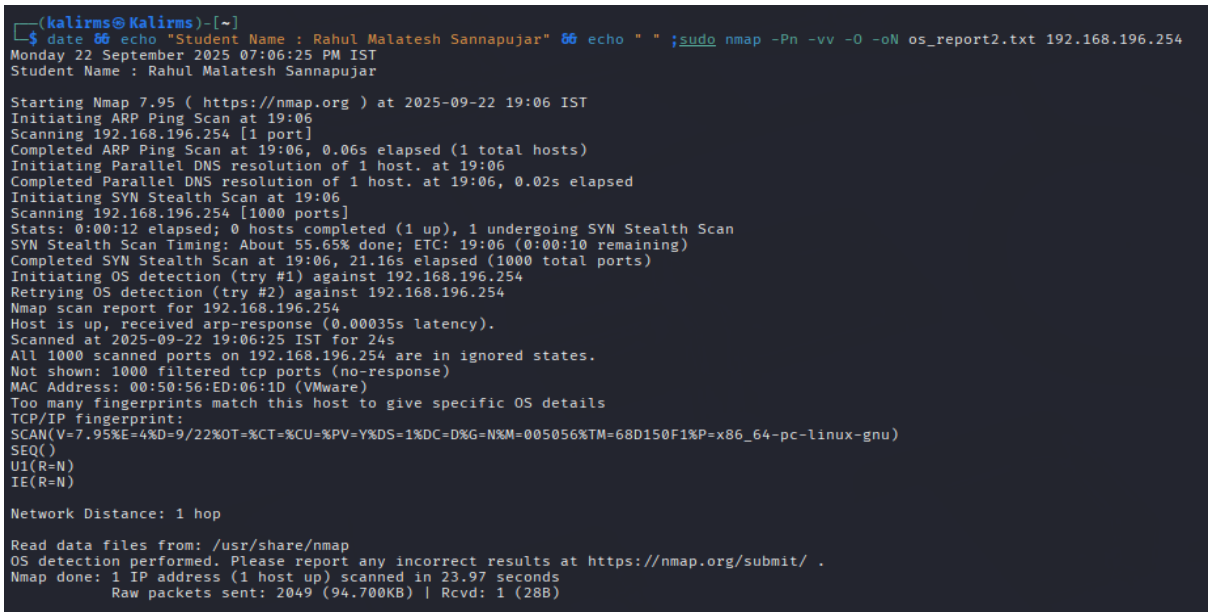


```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;sudo nmap -Pn -vv -O -oN os_report1.txt 192.168.196.2
Monday 22 September 2025 07:06:08 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 19:06 IST
Initiating ARP Ping Scan at 19:06
Scanning 192.168.196.2 [1 port]
Completed ARP Ping Scan at 19:06, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:06
Completed Parallel DNS resolution of 1 host. at 19:06, 0.02s elapsed
Initiating SYN Stealth Scan at 19:06
Scanning 192.168.196.2 [1000 ports]
Discovered open port 53/tcp on 192.168.196.2
Completed SYN Stealth Scan at 19:06, 0.10s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.196.2
Retrying OS detection (try #2) against 192.168.196.2
Nmap scan report for 192.168.196.2
Host is up, received arp-response (0.0057s latency).
Scanned at 2025-09-22 19:06:08 IST for 3s
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE REASON
53/tcp open  domain  syn-ack ttl 128
MAC Address: 00:50:56:E0:84:A5 (VMware)
Device type: specialized|general purpose|WAP|webcam
Running (JUST GUESSING): VMware Player (99%), Microsoft Windows XP|7|2012 (93%), Linux 2.4.X|3.X (91%), Actiontec embedded (91%), DVTel embedded (89%)
OS CPE: cpe:/a:vmware:player cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o:linux:linux_kernel:2.4.37 cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_ke
rnel cpe:/o:linux:linux_kernel:3.2
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec M
I424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTel DVT-9540DW network camera (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.95%E=4%D=9/22%OT=53%CT=1%CU=%PV=Y%DS=1%DC=D%G=N%M=005056%TM=68D150CB%P=x86_64-pc-linux-gnu)
SEQ(SP=103%GCD=1%ISR=100%TI=I%CI=I%II=I%SS=S%TS=U)
SEQ(SP=103%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)
WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)
ECN(R=Y%DF=N%TG=80%W=FAF0%O=M5B4%CC=N%Q=)
T1(R=Y%DF=N%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=N%TG=80%W=FAF0%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)
T4(R=Y%DF=N%TG=80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=N%TG=80%W=7FFF%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=N%TG=80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=N%TG=80%W=7FFF%S=Z%A=S%F=AR%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (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 3.83 seconds
         Raw packets sent: 1045 (49.192KB) | Rcvd: 1029 (41.708KB)
```

Description: This image shows an Nmap scan targeting 192.168.196.2. 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.

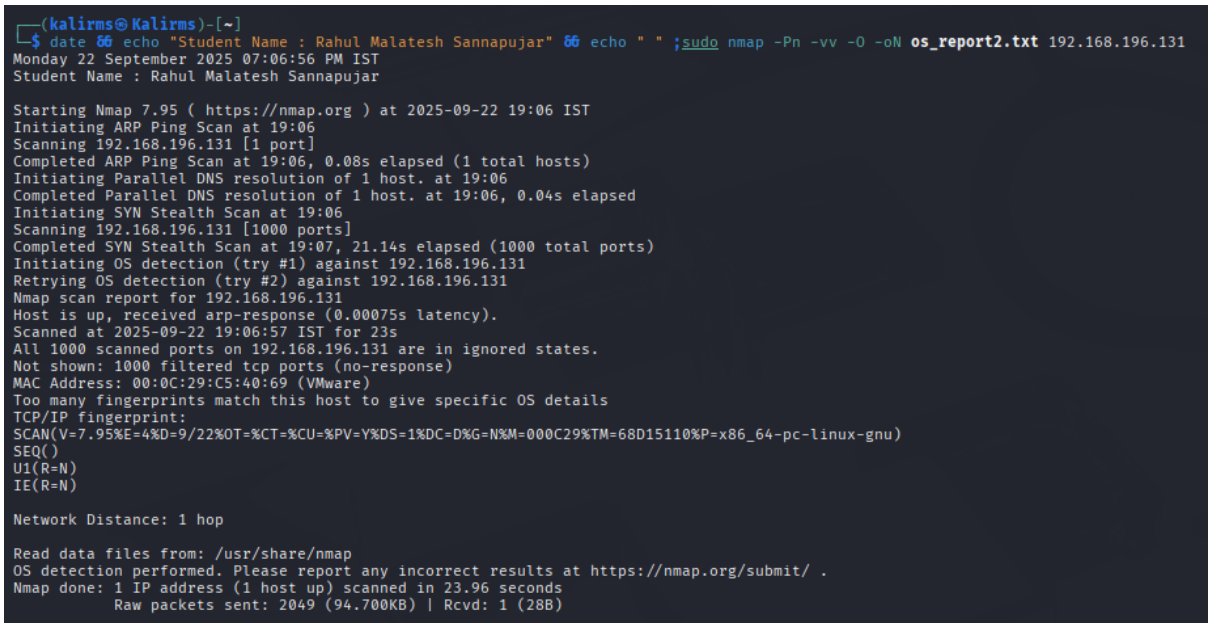
Task 1: Scan Your Local Network for Open Ports

Title: Nmap Scan of a Filtered Host (192.168.196.254)



Description: Similar to the first Nmap scan, this one targets 192.168.196.254. 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.

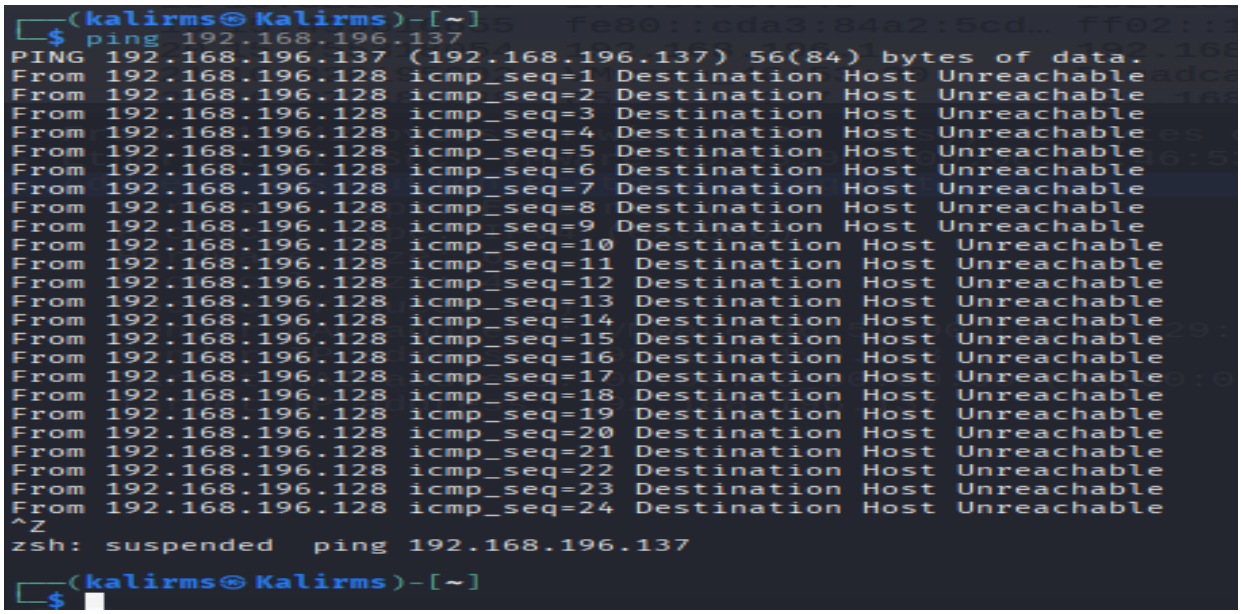
Title: Nmap Scan of a Single IP Address (192.168.196.131)



Description: This image shows the output of an Nmap scan targeting a specific IP address, 192.168.196.131. The scan, performed by "Rahul Malatesh Sannapujar" on September 22, 2025, shows that all 1000 scanned ports are filtered, meaning no response was received. The output also includes details like the MAC address, vendor (VMware), and some OS fingerprinting results, though it notes that too many fingerprints match to give a specific OS. The command used was sudo nmap -Pn -vv -O -n -oN os_report2.txt 192.168.196.131

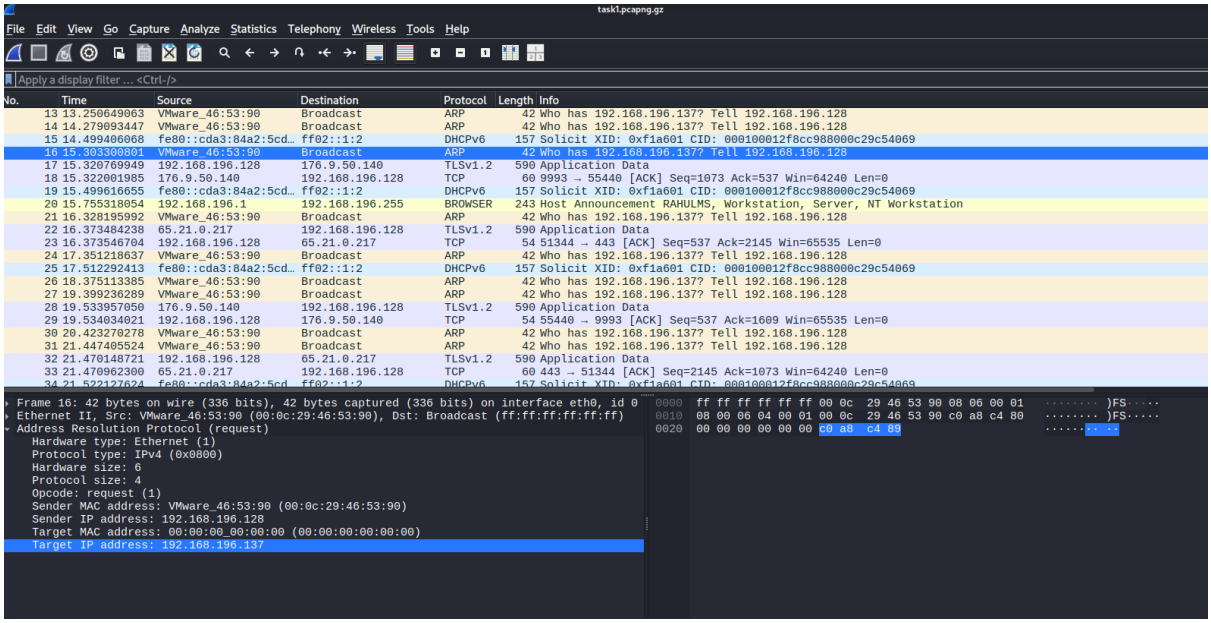
Task 1: Scan Your Local Network for Open Ports

Title: Network Connectivity Test with Ping



Description: This terminal output shows the results of a ping command to the IP address 192.168.196.137. The results consistently show "Destination Host Unreachable" from the pinging machine, 192.168.196.128, indicating that the target host is not reachable on the network. The command was manually suspended by the user with a ^Z command.

Title: Wireshark Packet Capture



Description: This image displays the Wireshark interface, showing a live packet capture on the network interface eth0. The packets shown include ARP, DHCPv6, and TCP traffic. A specific ARP packet is highlighted, showing the details of an ARP request from 192.168.196.128 to the broadcast address, targeting a host with an unknown MAC address. This demonstrates the use of Wireshark to analyze network traffic and complement port scanning.

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.