**Task 1 intern**

1.Install Nmap from official website.

2.Find your local IP range (e.g., 192.168.1.0/24).

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

4.Note down IP addresses and open ports found.

5.Optionally analyze packet capture with Wireshark.

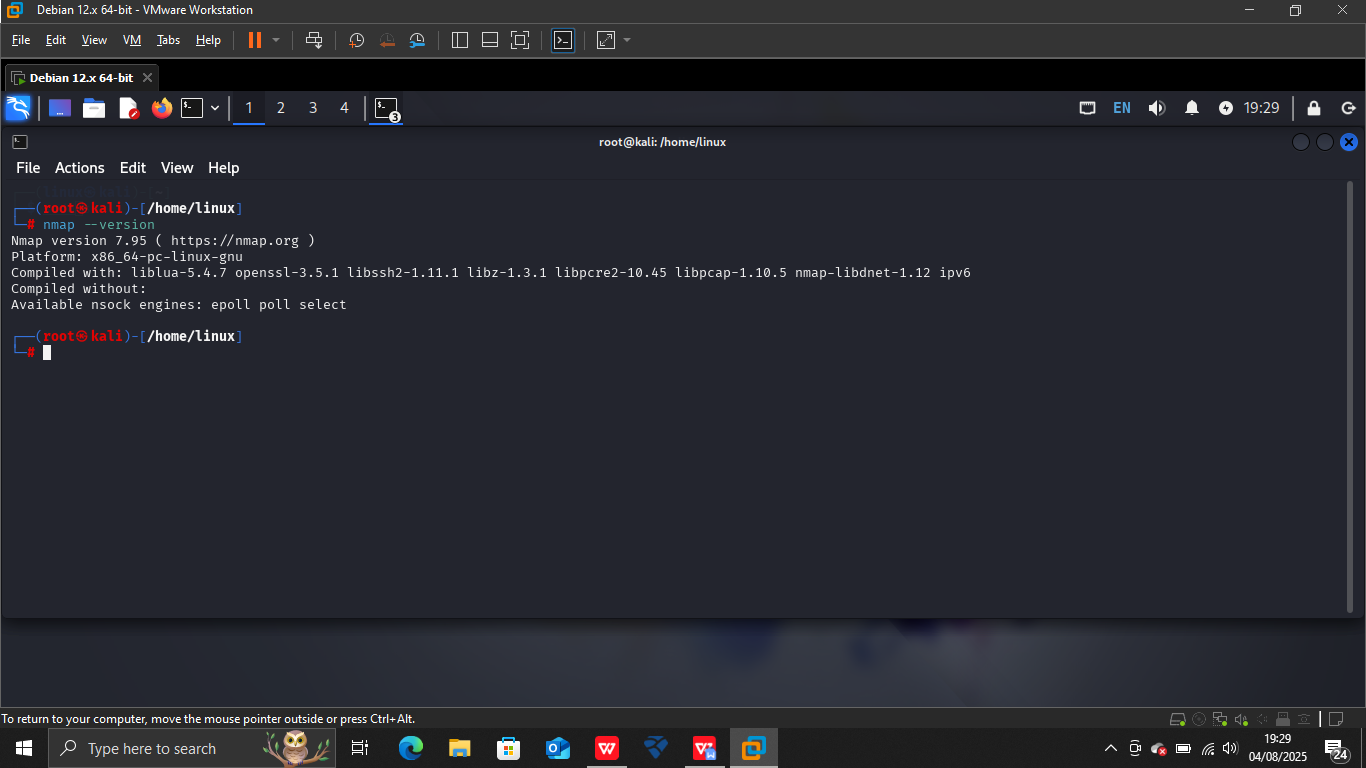
6.Research common services running on those ports.

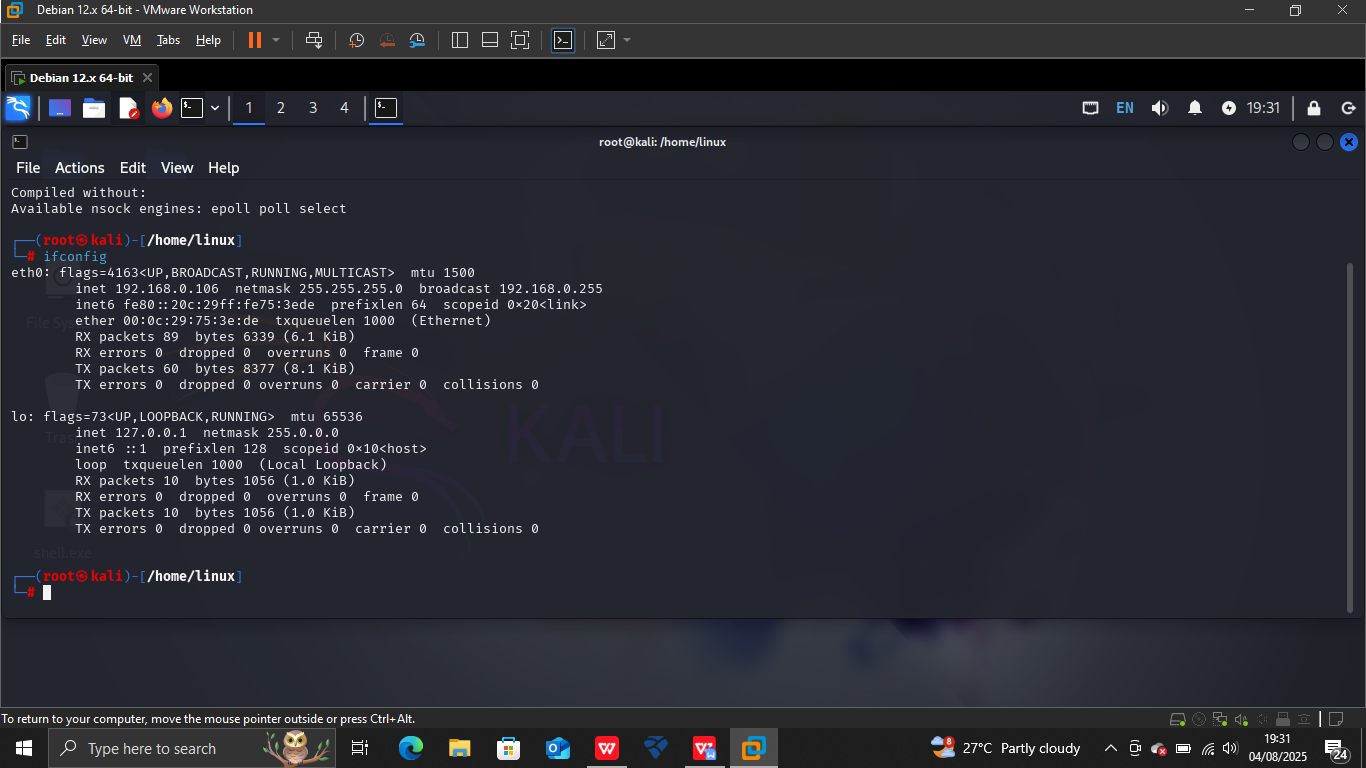
7.Identify potential security risks from open ports.

8.Save scan results as a text or HTML file.

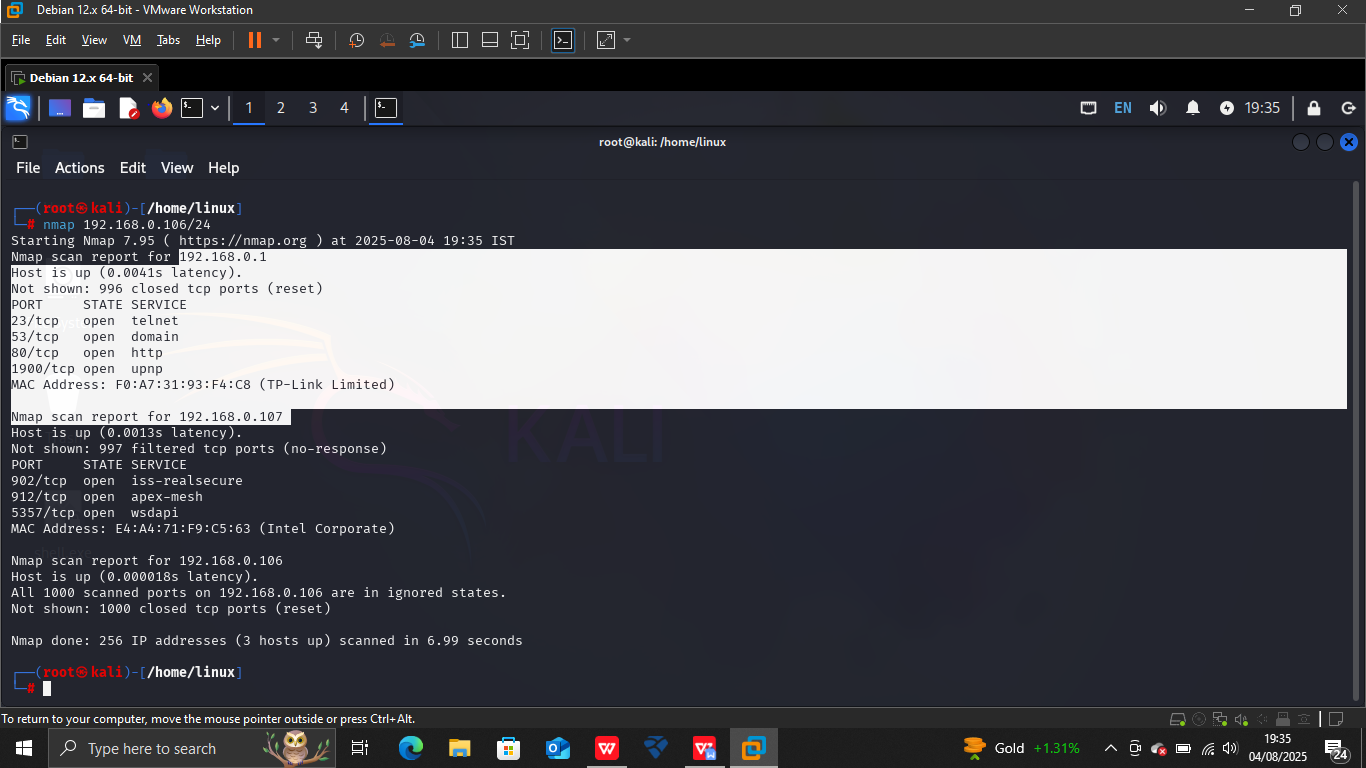
**Nmap I have the version 7.95 in kali**

Local IP range





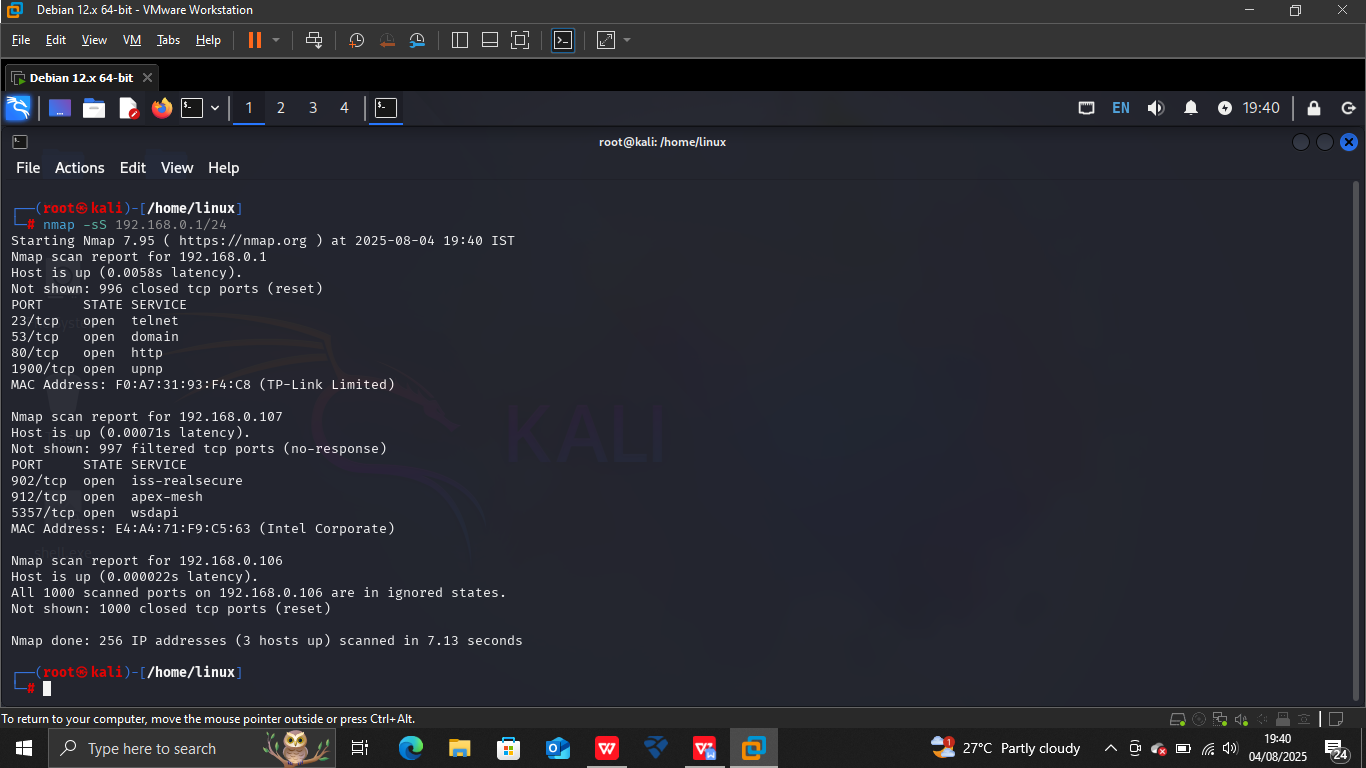
2.**Scanning the ip range 192.168.0.106/24**



Here 192.168.0.1 and 192.168.0.107 are the active ip’s

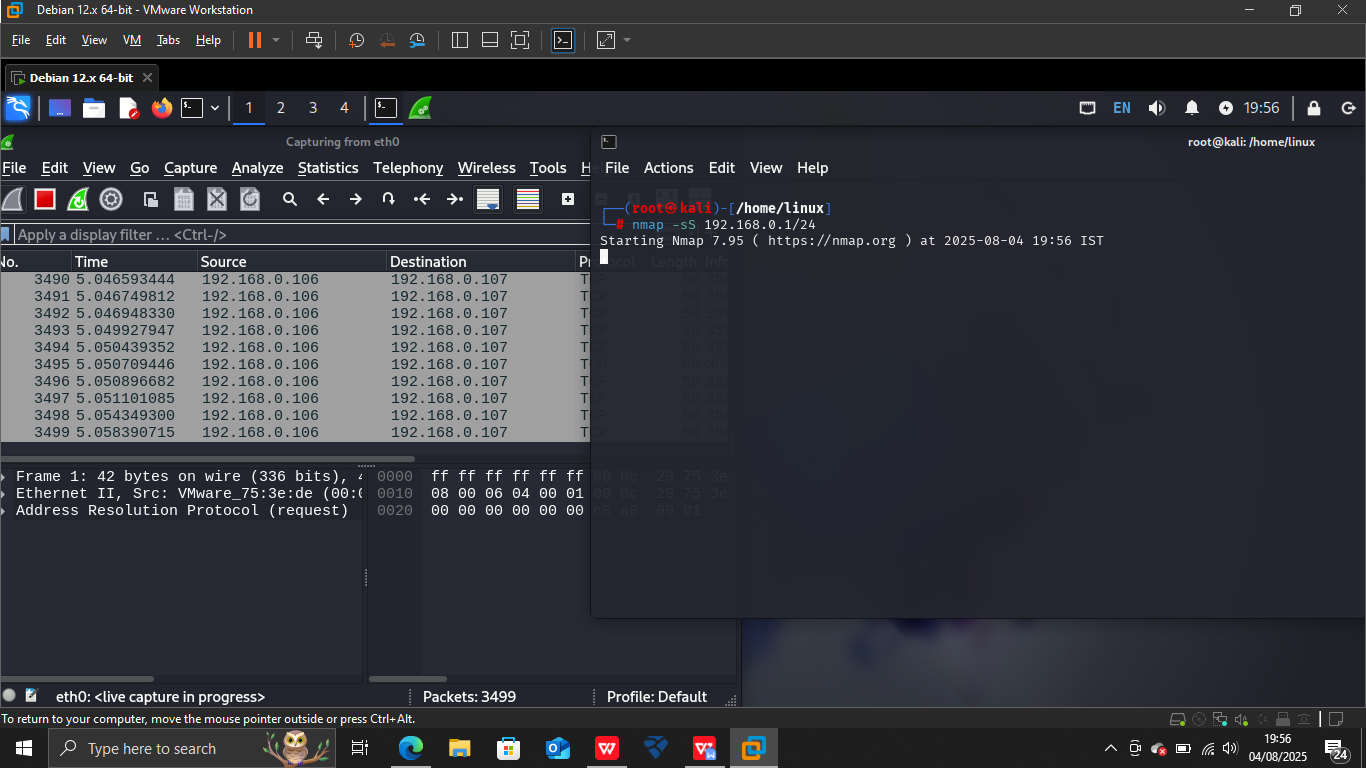
1. **Nmap scan for TCP SYN scan on ip range**

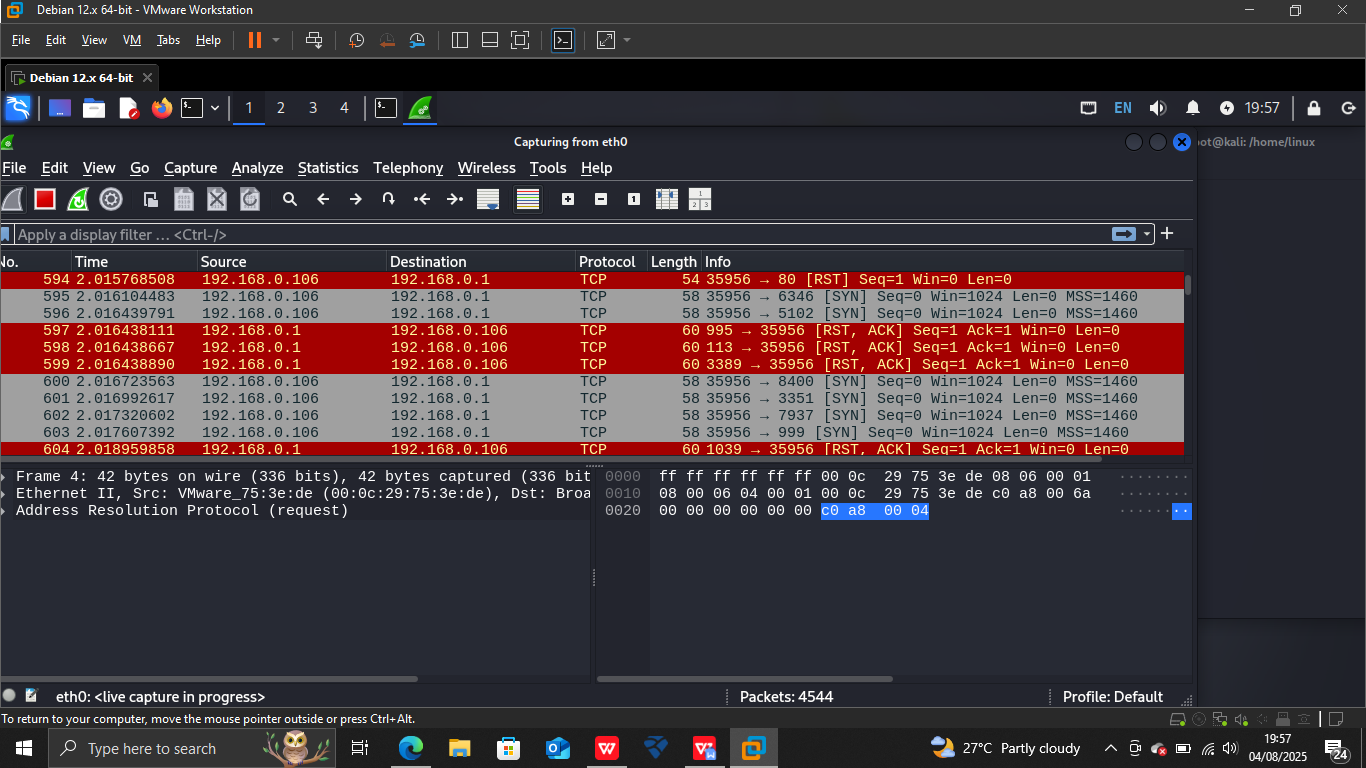
Nmap -sS 192.168.0.1/24



1. **Ports and services running on**
2. 23/tcp telnet my router
3. 53/tcp domain use for the DNS server
4. 80/tcp http
5. 1900/tcp upnp
6. 902/tcp iss-realsecure Windows machine
7. 912/tcp apex-mesh
8. 5357/tcp wsdapi

**5 . Analysing packets with the wireshark**

****

****

1. **Open ports and services running on that ports**
2. **This is router ip**

Found the open ports 23 telnet on ip 192.168.0.1

**What is Telnet?**

Telnet is an application protocol or older network protocol that Telnet enables the remote access to another machine with the use of telnet client, to connect to and execute commands on a remote machine that's hosting a telnet server.

Found the open ports 1900 servive upnp

**What is upnp**

The Simple Service Discovery Protocol (SSDP) operates over UDP port 1900 to enable automatic discovery of UPnP devices within a local network. Devices broadcast NOTIFY messages and respond to M-SEARCH requests to advertise or discover services.

1. **Windows ip**

Found port 902 open iss-realsecure

While it is true most communication occurs over HTTP and HTTPS, TCP ports 3998 and 3999 are also used for communication between SiteProtector and the RealSecure Sensors.

Another port open 912 apex-mesh

Port assigned to the APEX (Application Exchange Core) protocol. It is an XML-based protocol designed for sending instant messages based on the Blocks Extensible Exchange Protocol (BEEP).

1. **Potential risks from the open ports**

**1. 23/tcp — Telnet**

Service: Telnet (Unencrypted Remote Access)

Risk Level: Critical

Risk: Sends credentials and data in plain text; easily exploited for credential sniffing, brute-force, or remote code execution.

Recommendation: Disable Telnet; replace with SSH (22/tcp).

**2. 53/tcp — Domain (DNS)**

Service: DNS

Risk Level: Moderate to High

Risk: Can be abused for DNS zone transfers, which expose internal network details. Also vulnerable to DNS amplification attacks.

Recommendation: Allow TCP/53 only if needed (e.g., authoritative DNS server); disable zone transfers or restrict them to trusted IPs.

**3. 80/tcp — HTTP**

Service: HTTP (Unencrypted Web Traffic)

Risk Level: Moderate

Risk: Data and credentials transmitted in cleartext. Potential for web server exploits, directory traversal, XSS, SQL injection, etc.

Recommendation: Use HTTPS (443) instead and keep web apps patched.

**4. 1900/tcp — UPnP (Unusual on TCP)**

Service: Universal Plug and Play (usually UDP)

Risk Level: High

Risk: UPnP allows automatic port forwarding, which can be abused by malware. Exposing it externally can lead to network compromise.

Recommendation: UPnP should never be exposed to the internet. Disable or firewall it.

**5. 902/tcp — VMware Server / ISS RealSecure**

Service: Used by VMware for remote management and file transfers between host/guest

Risk Level: Moderate to High

Risk: If exposed, can allow remote access to virtual machines or the hypervisor. Historically targeted by attackers.

Recommendation: Restrict access to trusted IPs; use firewalls; keep VMware products up to date.

**6. 912/tcp — Apex Mesh (Custom/Unknown)**

Service: Often associated with Apex One or custom applications

Risk Level: Unknown to Moderate

Risk: Unknown services can be weak points if not updated or configured securely.

Recommendation: Identify what is using this port; if unnecessary, close it.

**7. 5357/tcp — WSDAPI (Web Services for Devices)**

Service: Used by Windows for network printer discovery and device communication

Risk Level: Moderate

Risk: Can reveal device info to attackers; historically had info disclosure and privilege escalation bugs.

Recommendation: Block externally; allow only on local networks if needed.