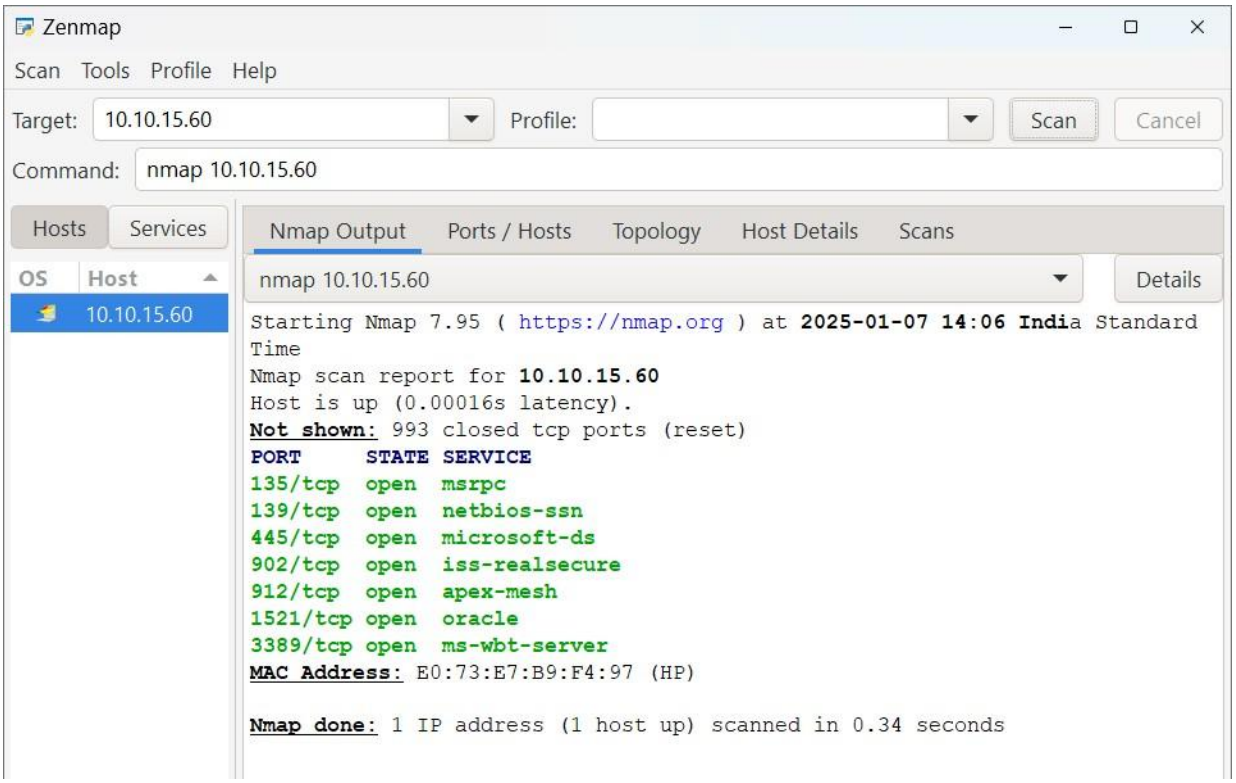
PRACTICAL 1

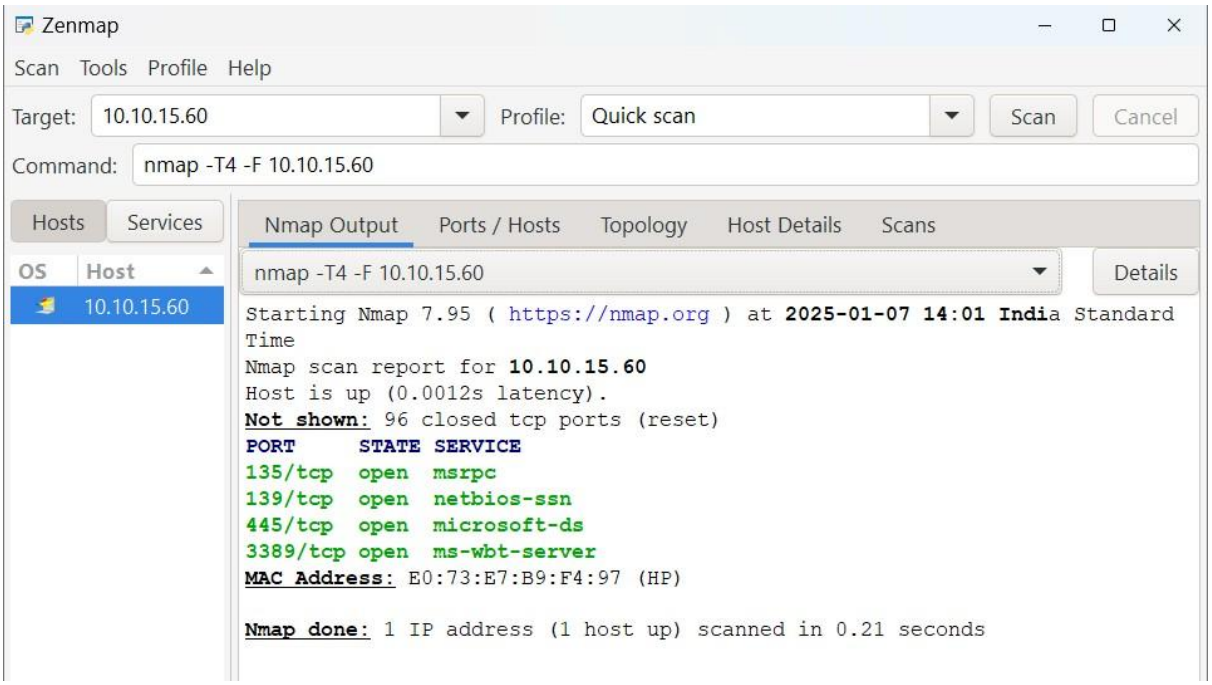
AIM: Network scanning and reconnaissance using Nmap and other tools to identify open ports, operating systems and potential vulnerabilities.

- Target IP: 10.10.15.60
- Nmap: Scan the Open ports.
- Command: nmap 10.10.15.60



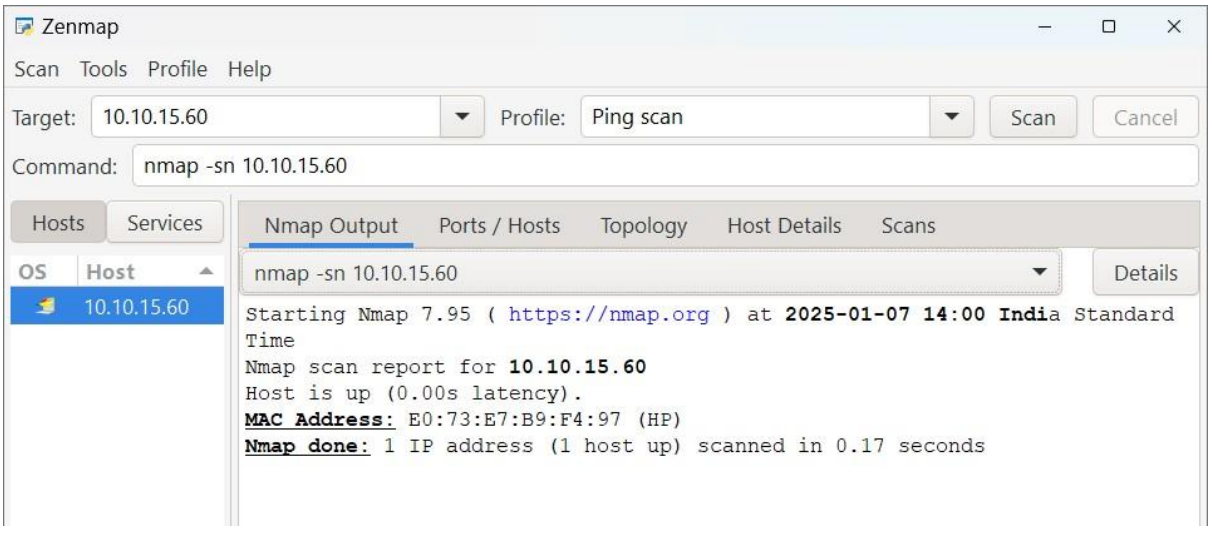
- Quick scan :

Command : nmap -T4 -F 10.10.15.60



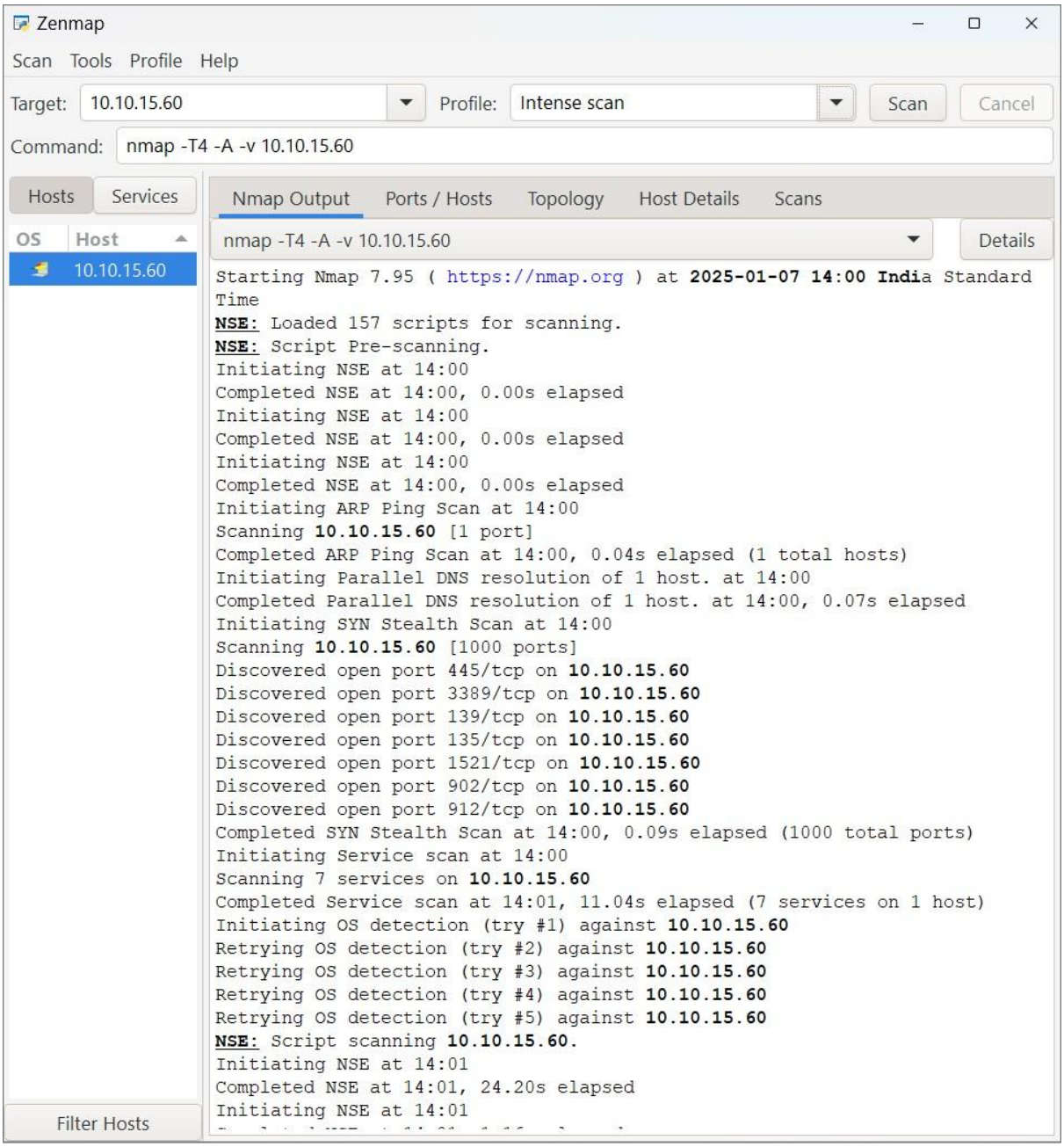
- Ping scan :

Command : nmap -sn 10.10.15.60



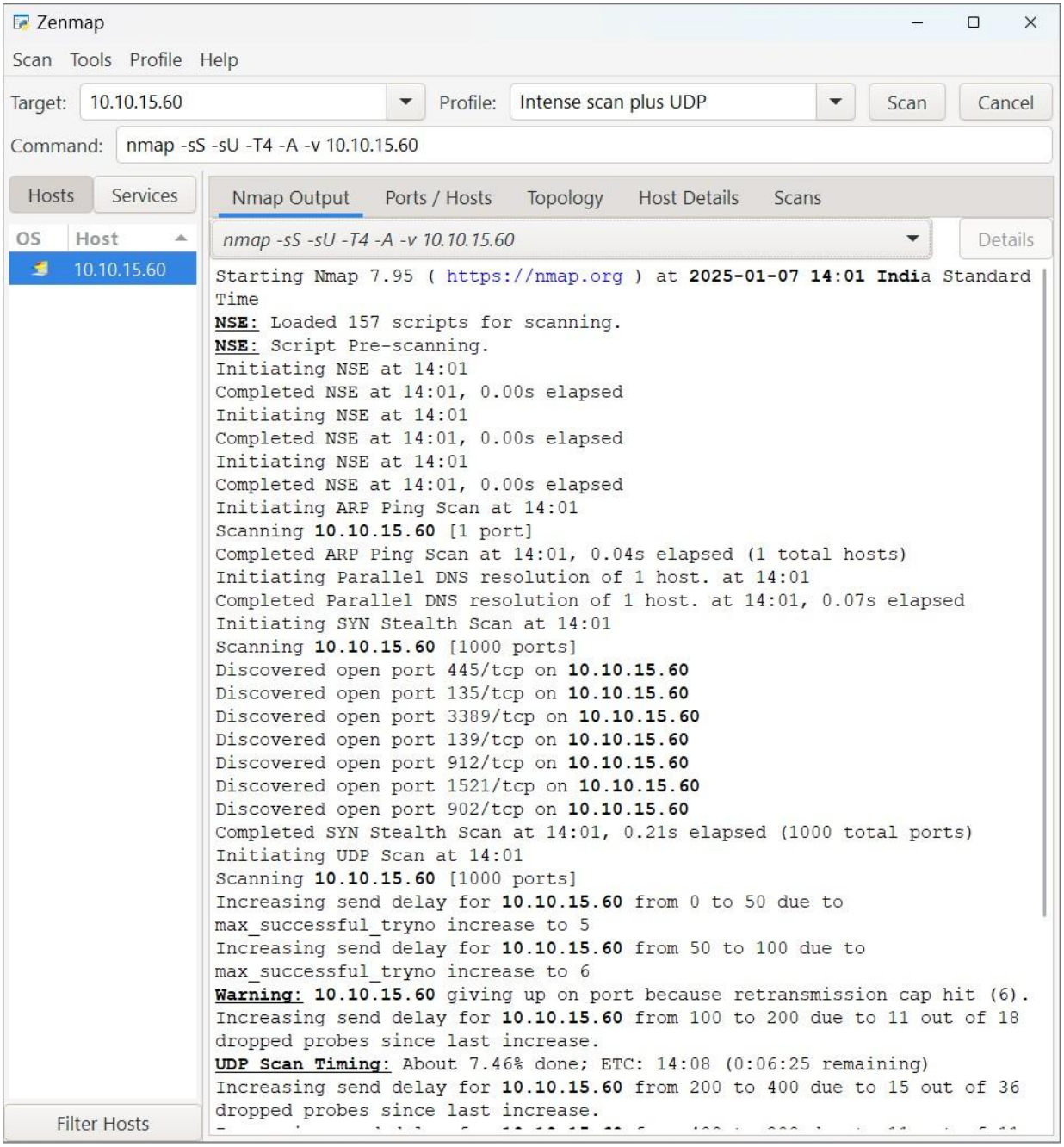
- Intense scan :

Command : nmap -T4 -A -v 10.10.15.60



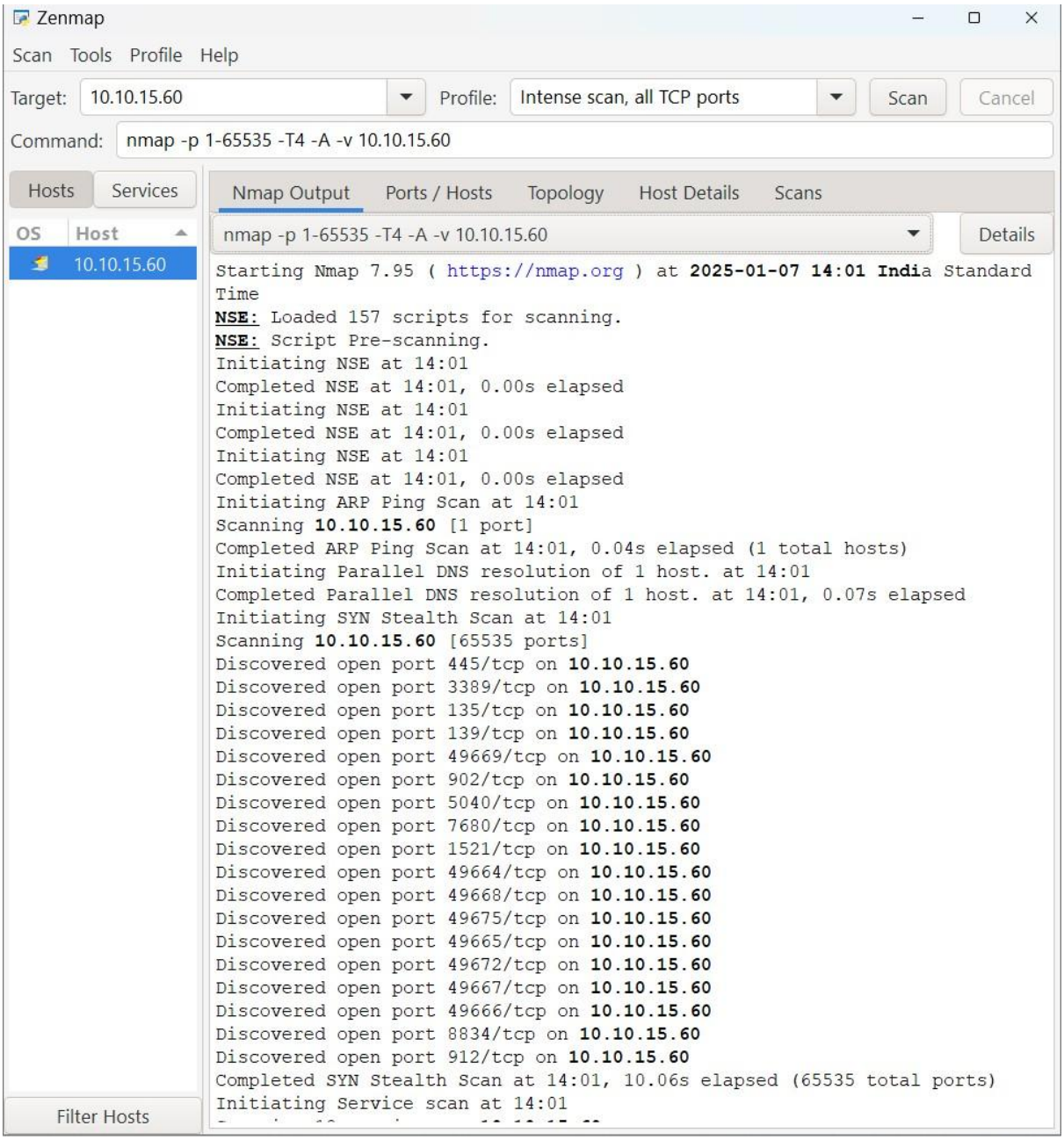
- UDP scan :

Command : nmap -sS -sU -T4 -A -v 10.10.15.60



- TCP scan :

Command : nmap -p 1-65535 -T4 -A -v 10.10.15.60



Output:

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
3389	tcp	open	ms-wbt-server	
902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1521	tcp	open	oracle-tns	Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
5040	tcp	open		
7680	tcp	open	pando-pub	
8834	tcp	open	nessus-xmlrpc	
49664	tcp	open	msrpc	Microsoft Windows RPC
49665	tcp	open	msrpc	Microsoft Windows RPC
49666	tcp	open	msrpc	Microsoft Windows RPC
49667	tcp	open	msrpc	Microsoft Windows RPC
49668	tcp	open	msrpc	Microsoft Windows RPC
49669	tcp	open	msrpc	Microsoft Windows RPC
49672	tcp	open	msrpc	Microsoft Windows RPC
49675	tcp	open	oracle	Oracle Database
80	udp	open|filtered	http	
123	udp	open|filtered	ntp	
137	udp	open	netbios-ns	Microsoft Windows Mobile netbios-ns
138	udp	open|filtered	netbios-dgm	
500	udp	open|filtered	isakmp	
1484	udp	open|filtered	confluent	
1900	udp	open|filtered	upnp	
2148	udp	open|filtered	veritas-ucl	
3389	udp	open|filtered	ms-wbt-server	

.

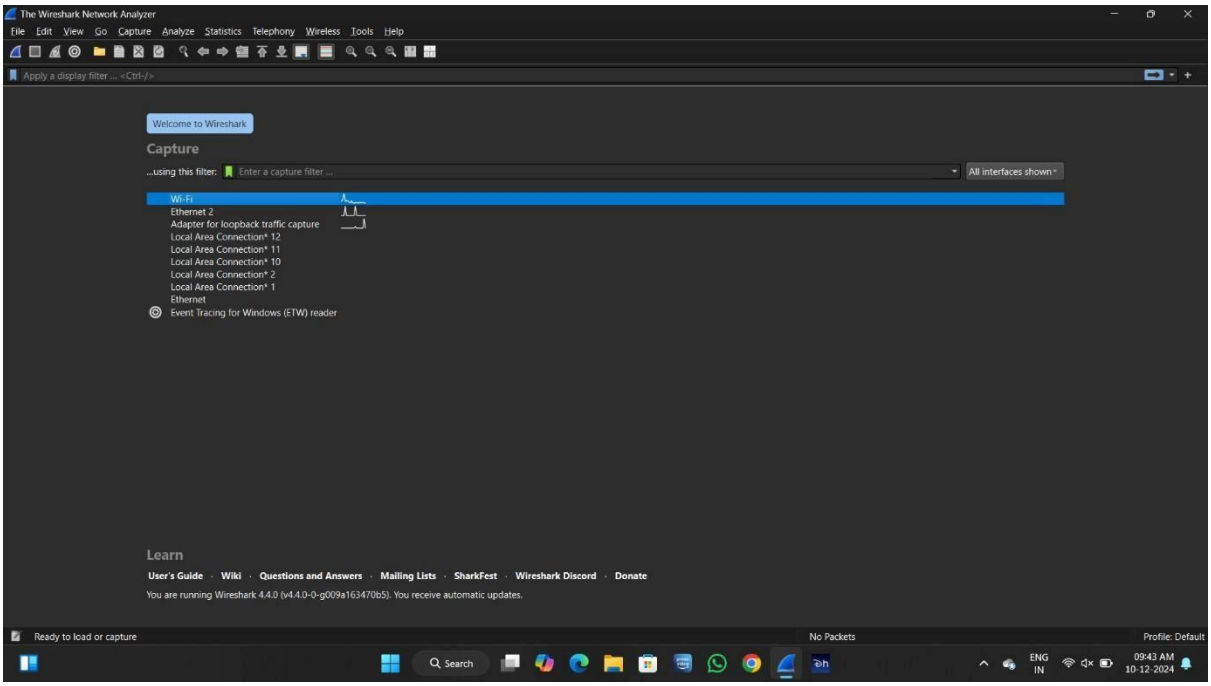
Conclusion:

Network scanning and reconnaissance are critical components of the cybersecurity lifecycle, enabling both defenders and ethical hackers to assess the security posture of systems before malicious actors can exploit them. Tools like Nmap provide powerful capabilities to identify open ports, running services, and even operating systems, offering a comprehensive view of the target environment.

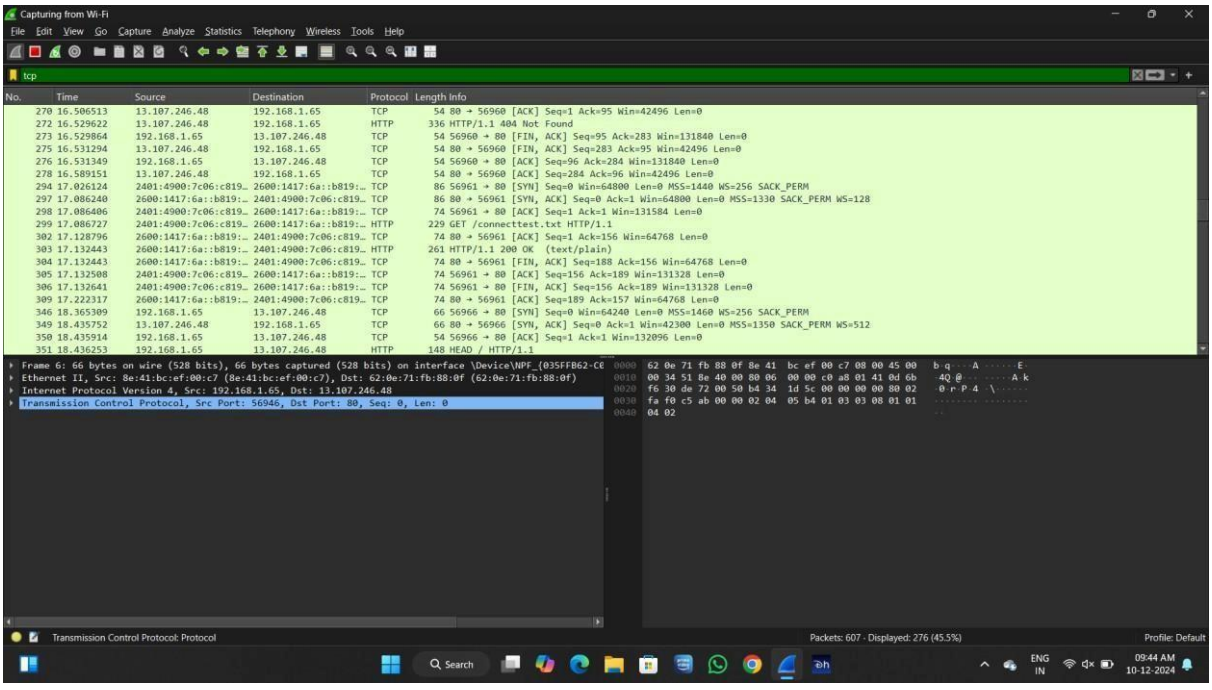
PRACTICAL 2

AIM: Find tcp, dns, http and http website login id & password using wireshark.

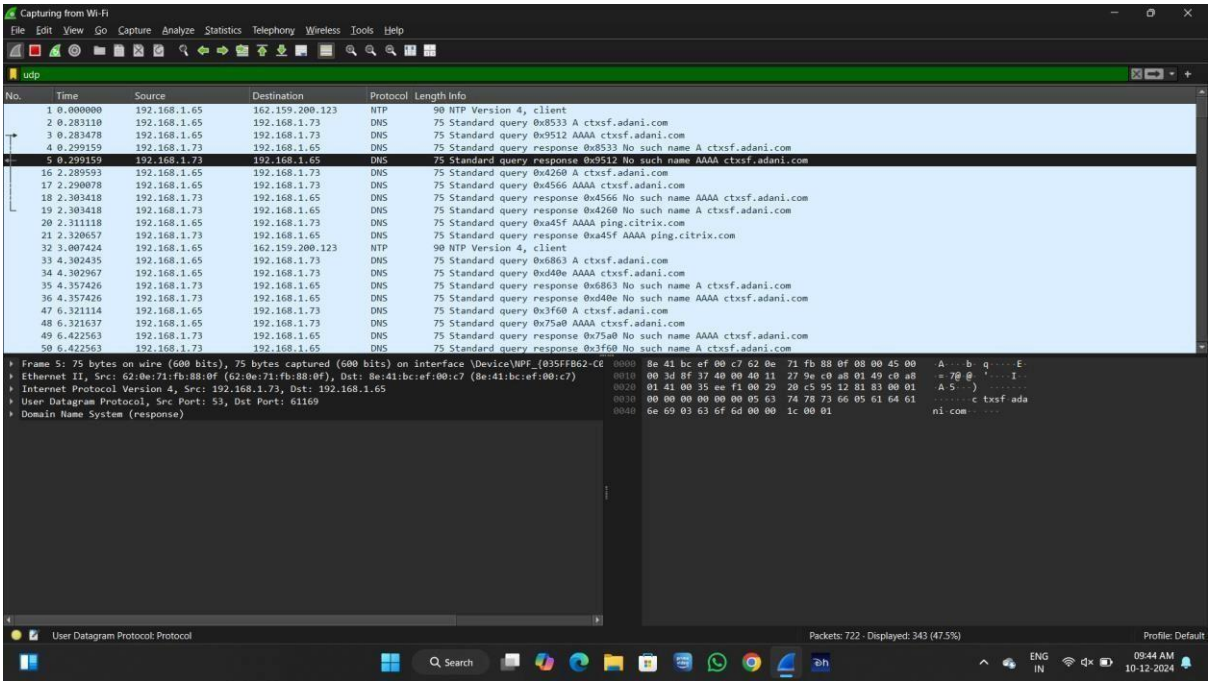
Step 1 : open wireshark and connet with wifi



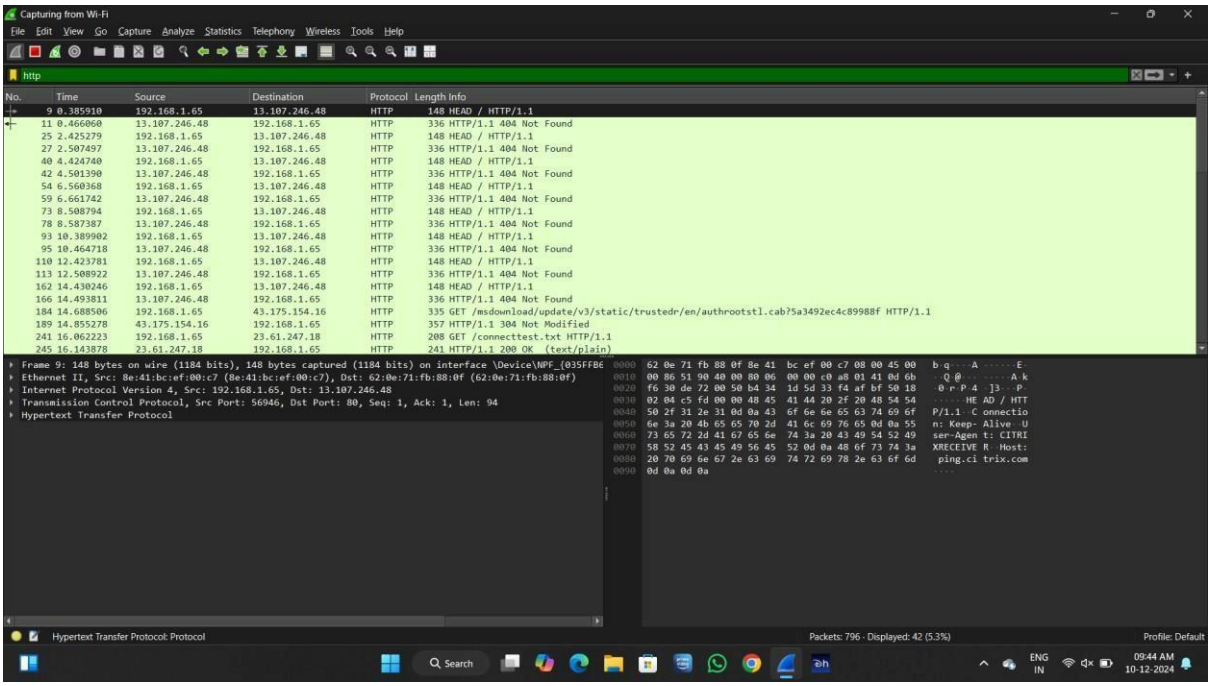
Step 2 : find TCP package



Step 3 : find DNS package

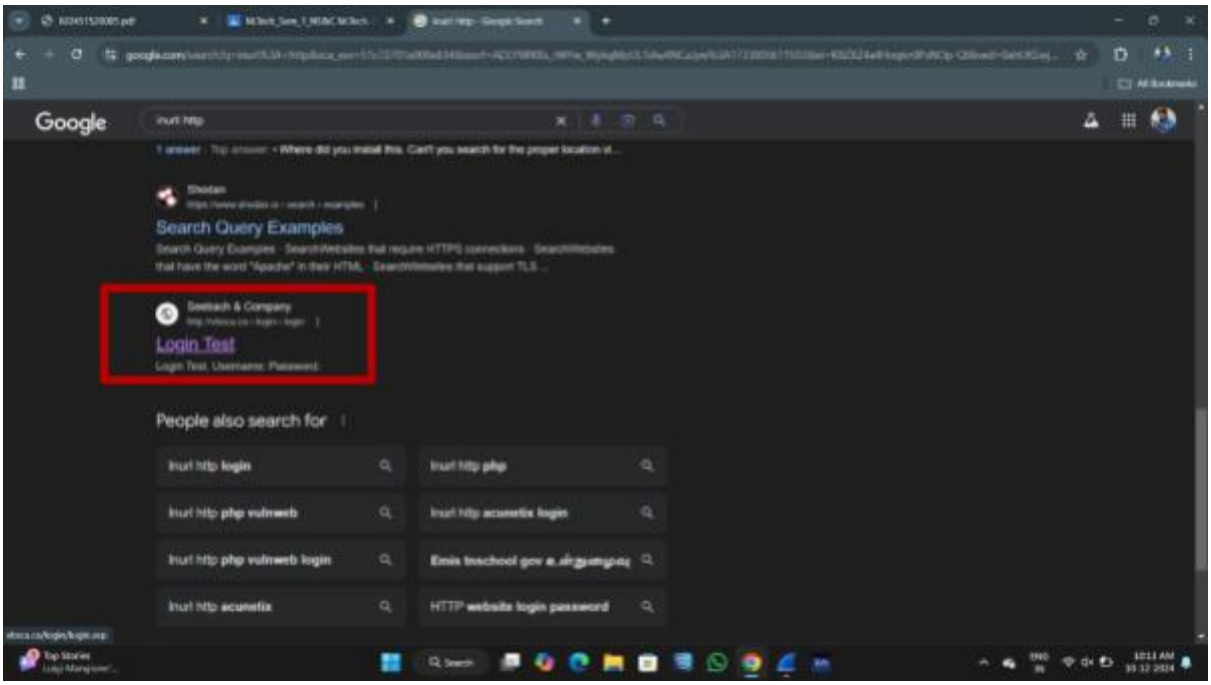


Step 4 : find HTTP package

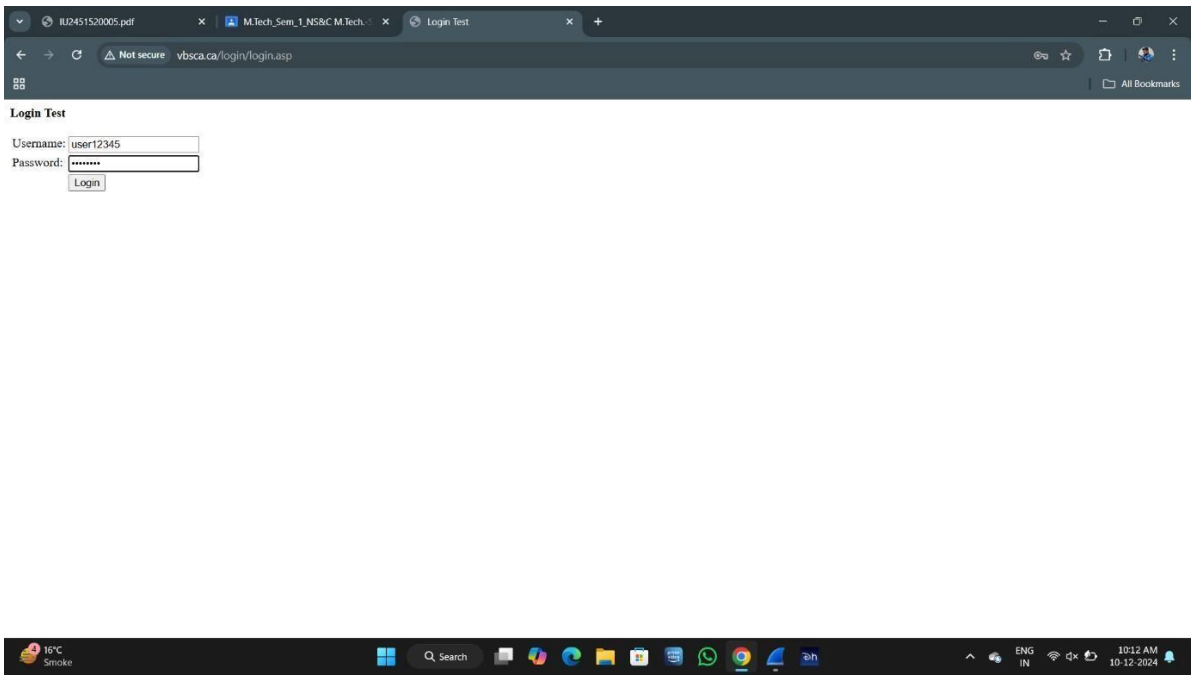


FIND ID PASSWORD

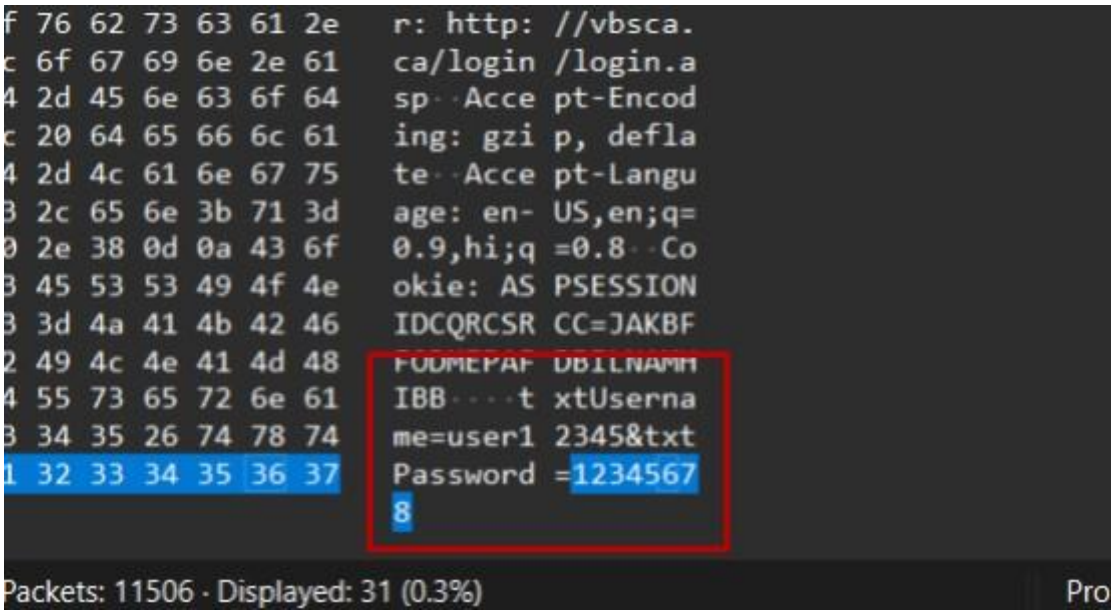
Step 1 : find any HTTP website on browser



Step 2 : login user ID and PASSWORD



Step 3 : open wireshark and search http in search and find ID & PASSWORD



Conclusion:

Wireshark is a powerful packet-sniffing tool that allows users to analyze network traffic in real-time. By capturing and inspecting packets, it is possible to identify various protocols such as TCP, DNS, and HTTP, revealing important network activities and potentially sensitive data.

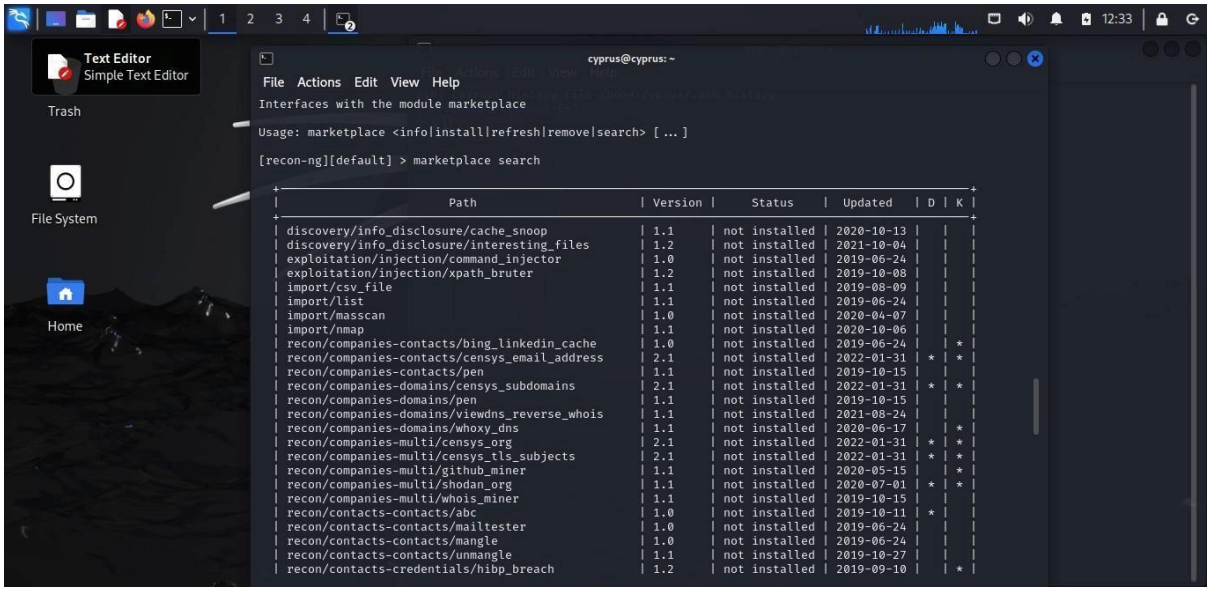
During analysis, HTTP traffic can sometimes expose login IDs and passwords, especially if the website does not use encryption (i.e., not using HTTPS). This highlights a critical vulnerability: unencrypted traffic can be easily intercepted and exploited by attackers. Through TCP and DNS analysis, Wireshark also provides deeper insight into session behaviors, host communications, and domain lookups, aiding in identifying suspicious or unauthorized connections.

PRACTICAL 3

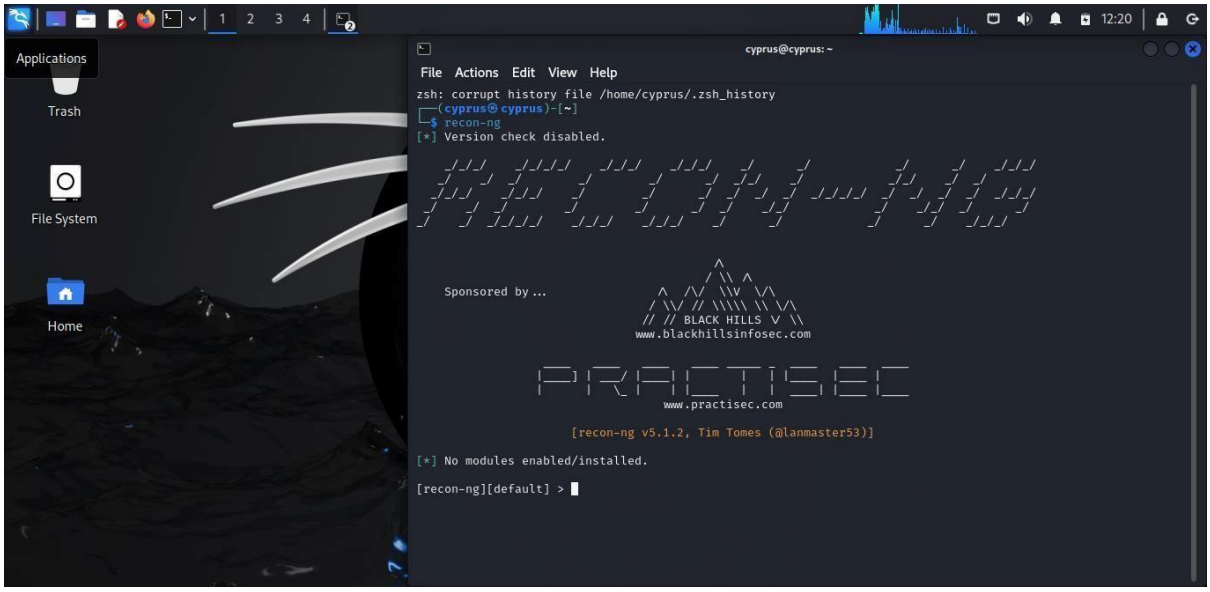
AIM: To automate and enhance the information-gathering process using Recon-ng.

Definition: Recon-ng is a Python-based web reconnaissance framework for automating OSINT tasks. It provides modules for gathering information like domains, contacts, and IPs, integrating APIs, and visualizing data. It is widely used in cybersecurity for penetration testing and intelligence gathering.

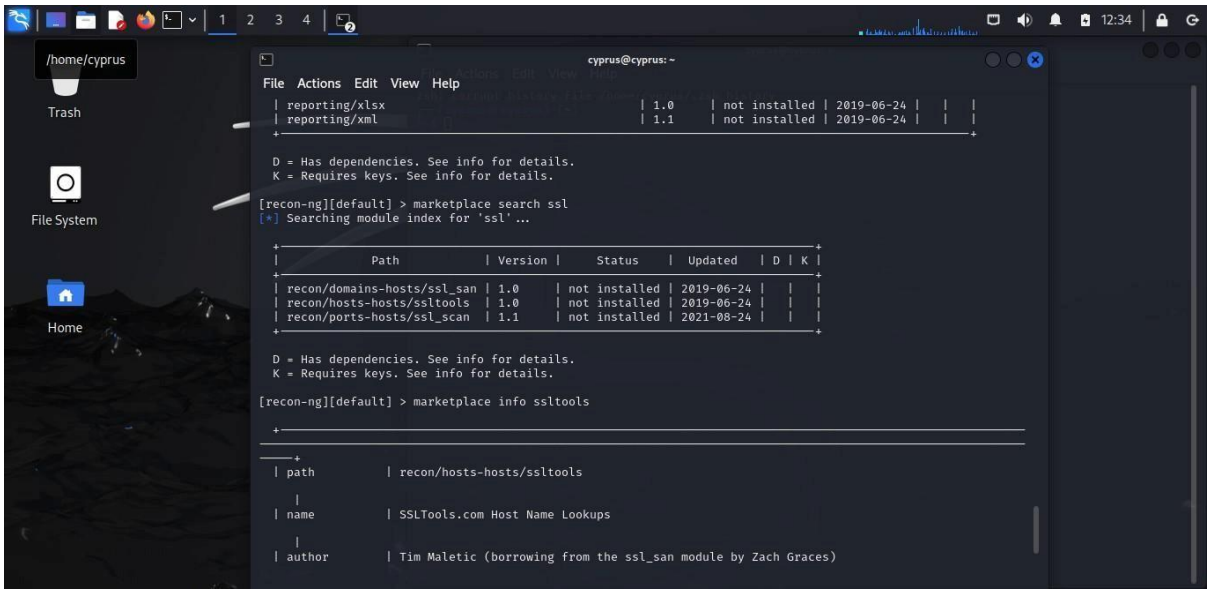
step 1: open RECON_NG



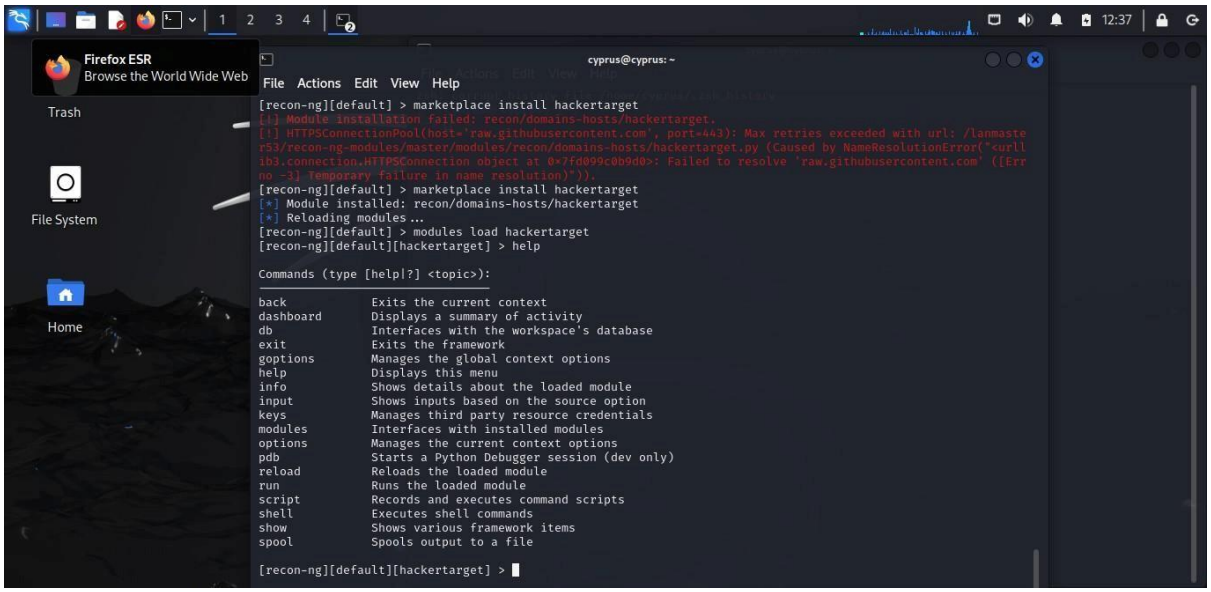
step 2 : search market places for module installation or to select which module you want to choose



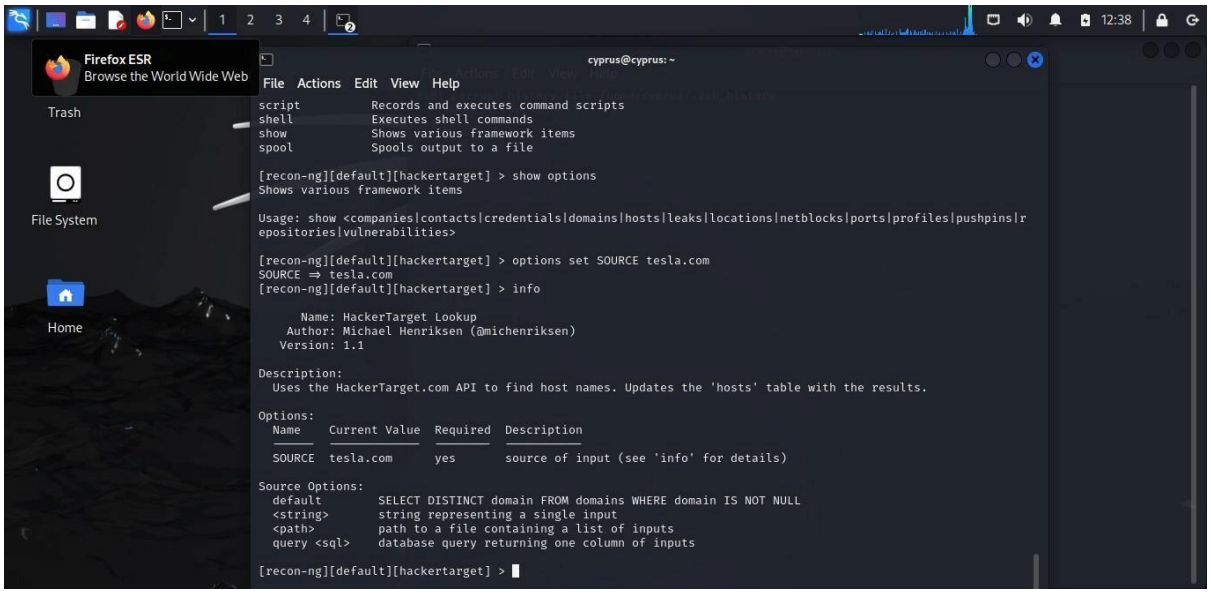
step 3 : search module for SSL



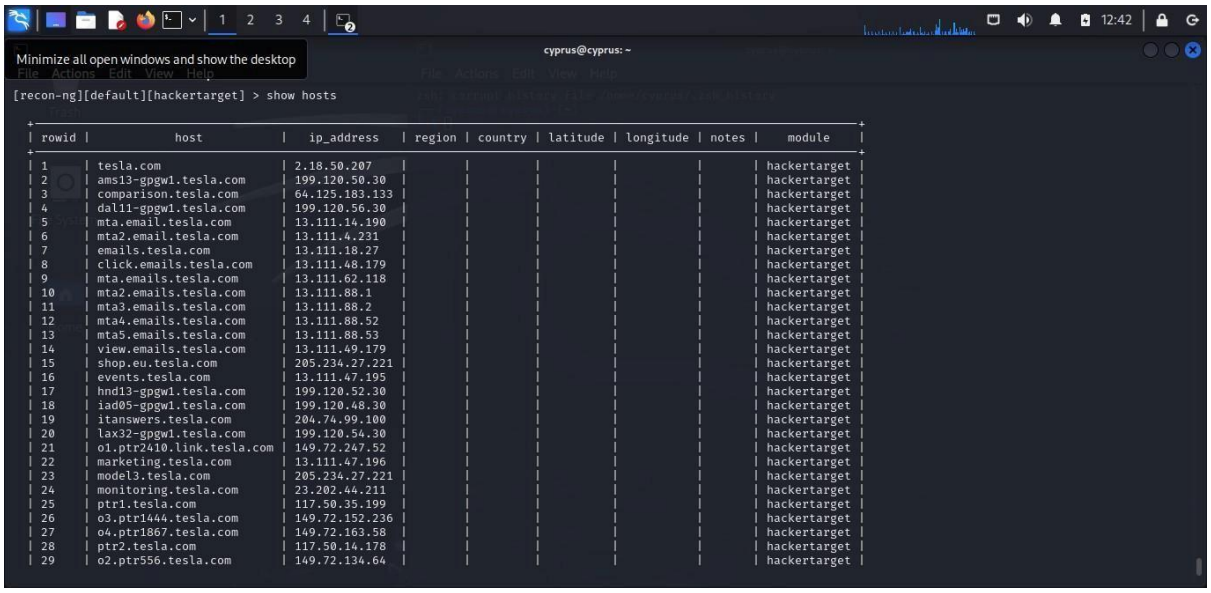
step 4 : install marketplace hackertarget



step 5: set the source of tesla.com



step 6: show the all host name of tesla.com



Conclusion:

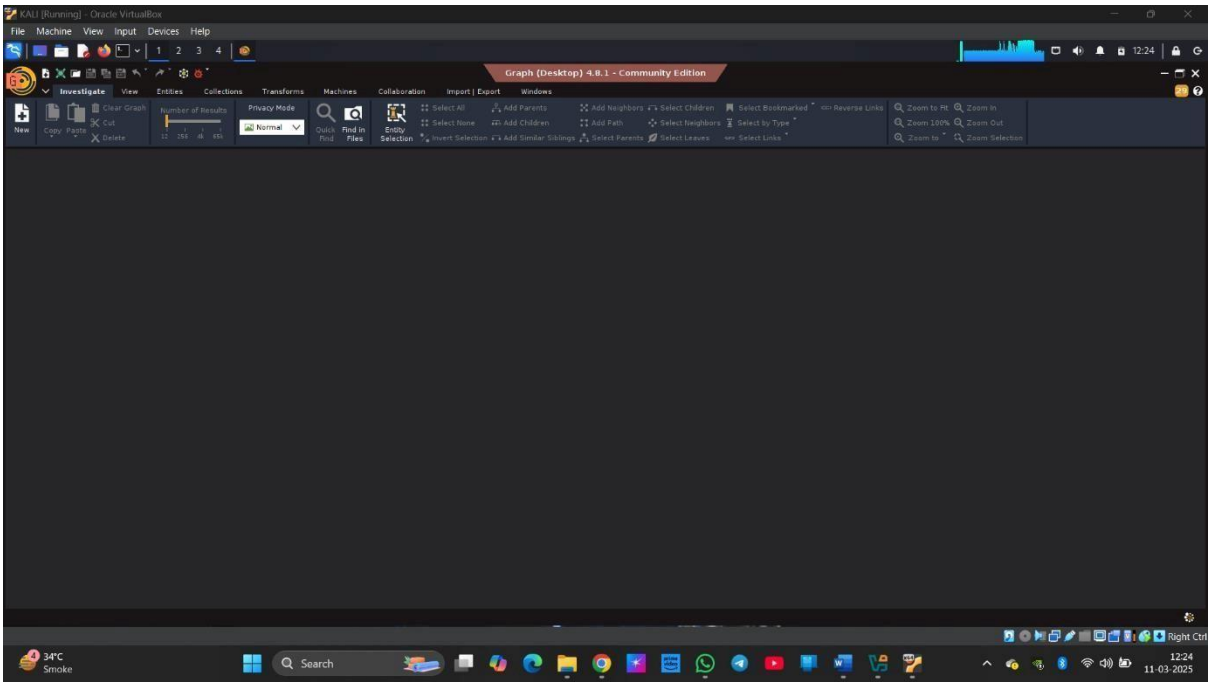
Recon-ng is a robust and modular open-source reconnaissance tool designed to automate and enhance the information-gathering process during cybersecurity assessments. Its powerful framework integrates seamlessly with various APIs and data sources, allowing security professionals to quickly collect and correlate valuable intelligence such as domain names, IP addresses, WHOIS information, and social media data.

PRACTICAL 4

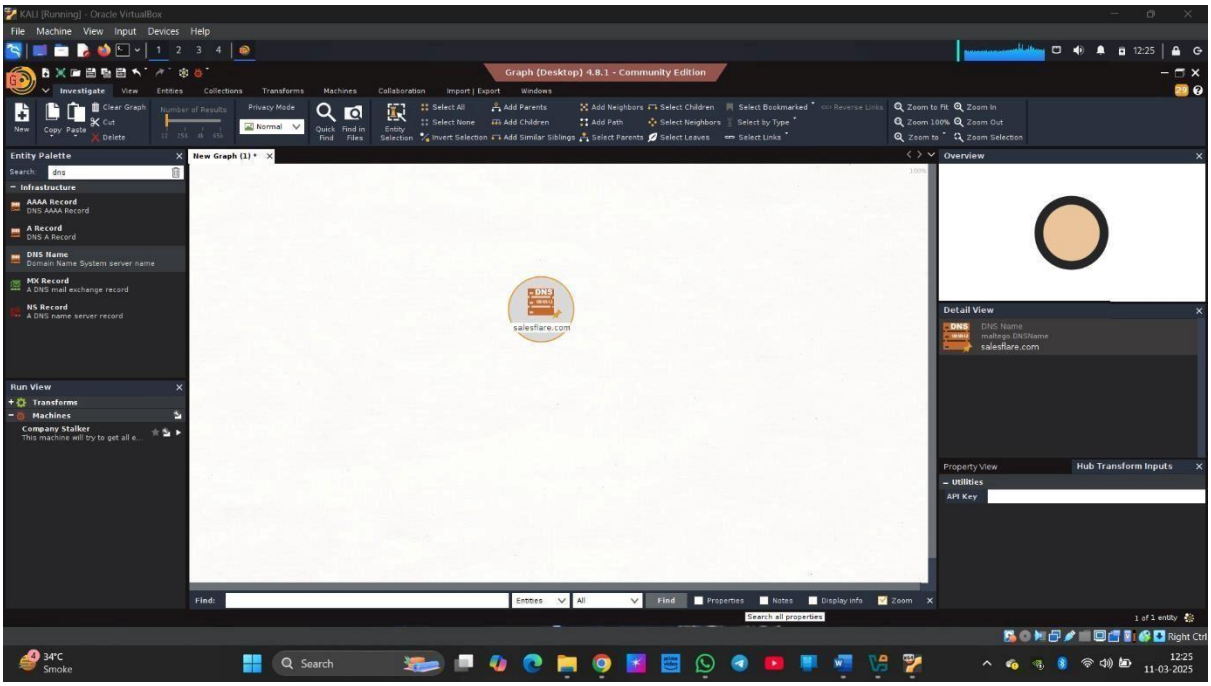
AIM: To automate and enhance the information-gathering process using Maltego, enabling graphical visualization of relationships.

Definition: Maltego is an open-source intelligence (OSINT) and forensics tool that helps in data gathering and link analysis. It is widely used for cyber investigations to map relationships between entities such as people, organizations, and online resources.

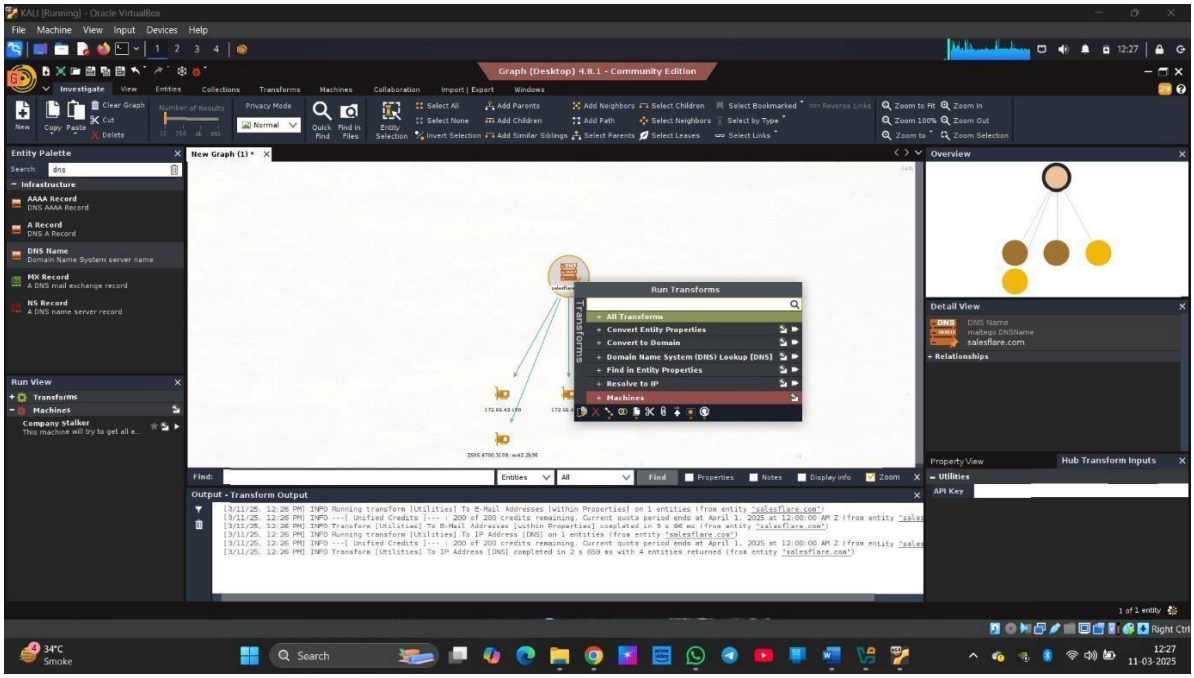
Step 1: open maltigo in kali

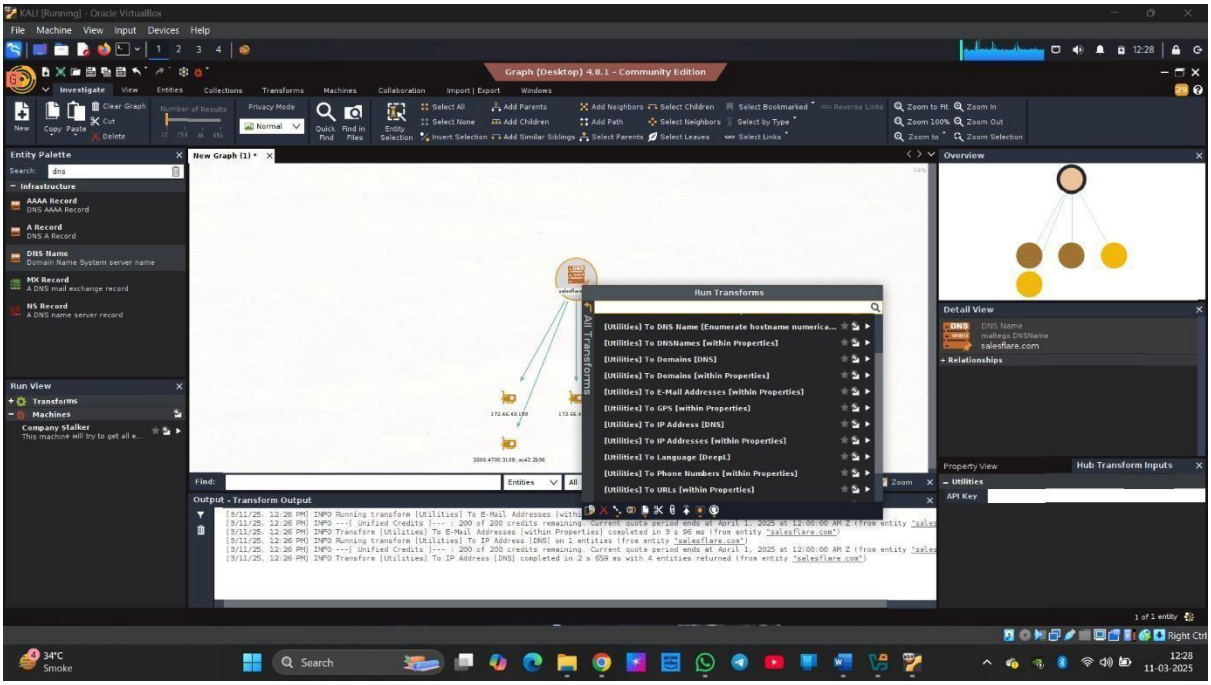


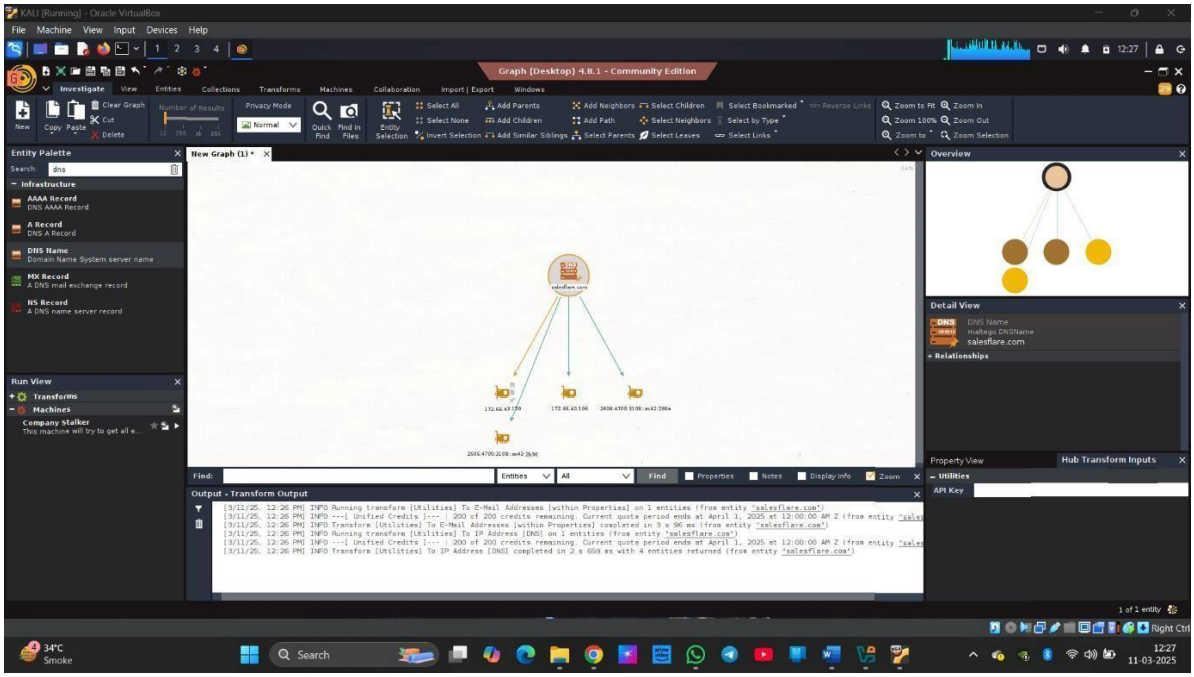
Step 2: enter the domain name for gathering information.



Step 3: right click on that domain and click on all transform and select find IP address







Conclusion:

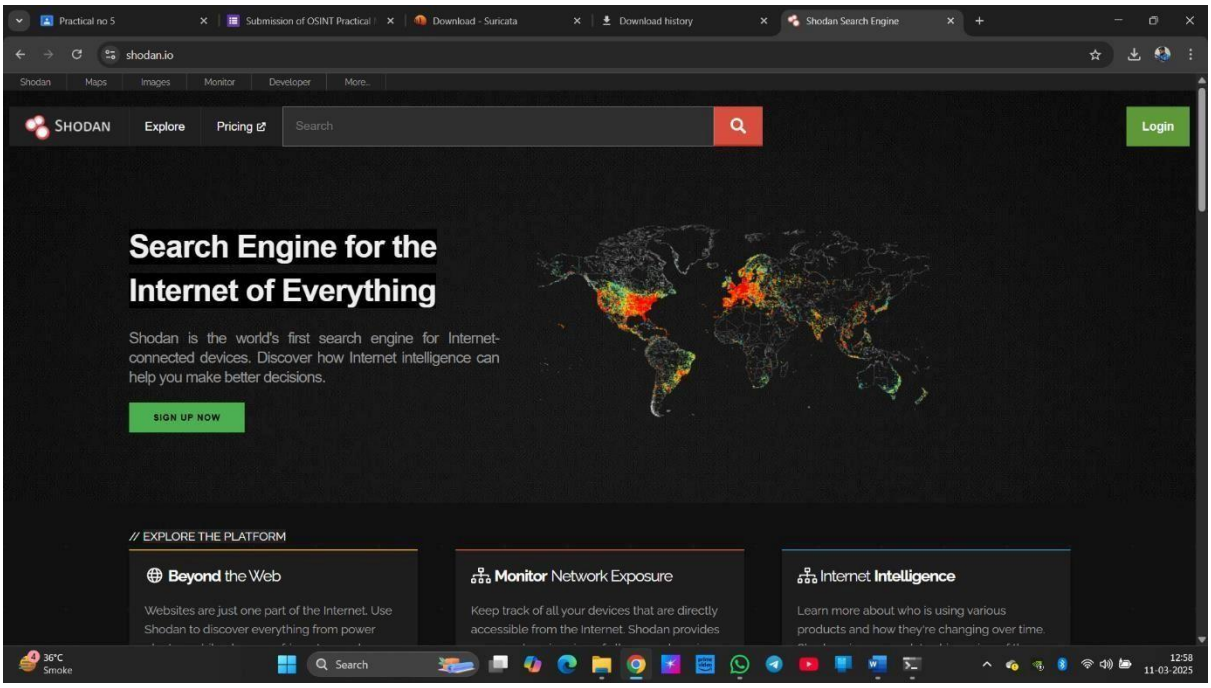
Maltego is a powerful intelligence-gathering and analysis tool that automates data collection and provides graphical visualization of relationships between entities such as people, domains, IP addresses, social media profiles, and infrastructure components. By leveraging open-source intelligence (OSINT) and a wide range of transforms, Maltego enables investigators to uncover hidden connections and gain deep insights into target environments.

PRACTICAL 5

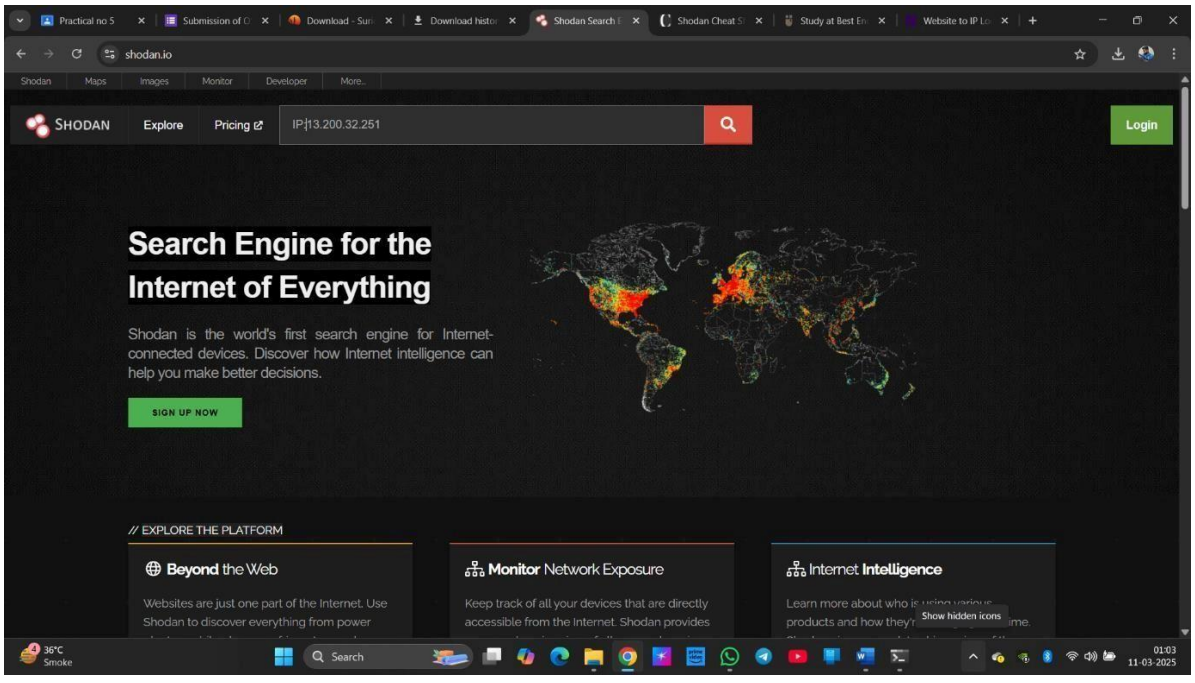
AIM: To identify and analyze internet-exposed devices and vulnerabilities through automated information gathering using the Shodan search engine.

Definition: Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

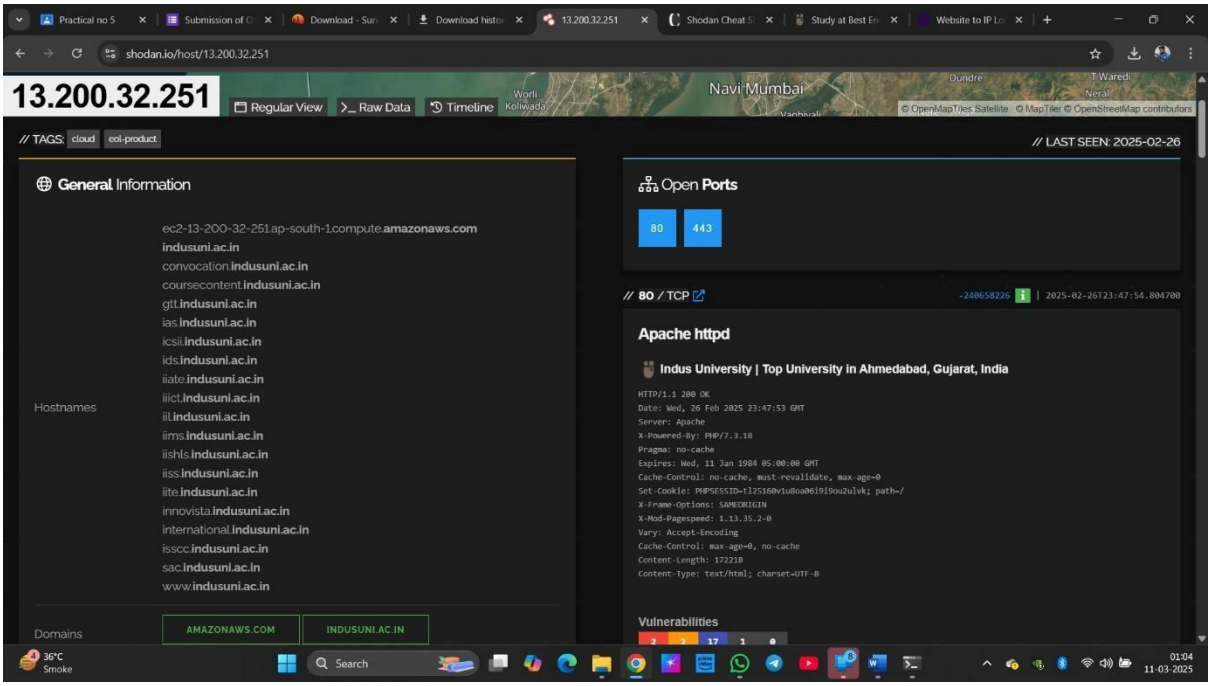
Step 1: open SHODAN

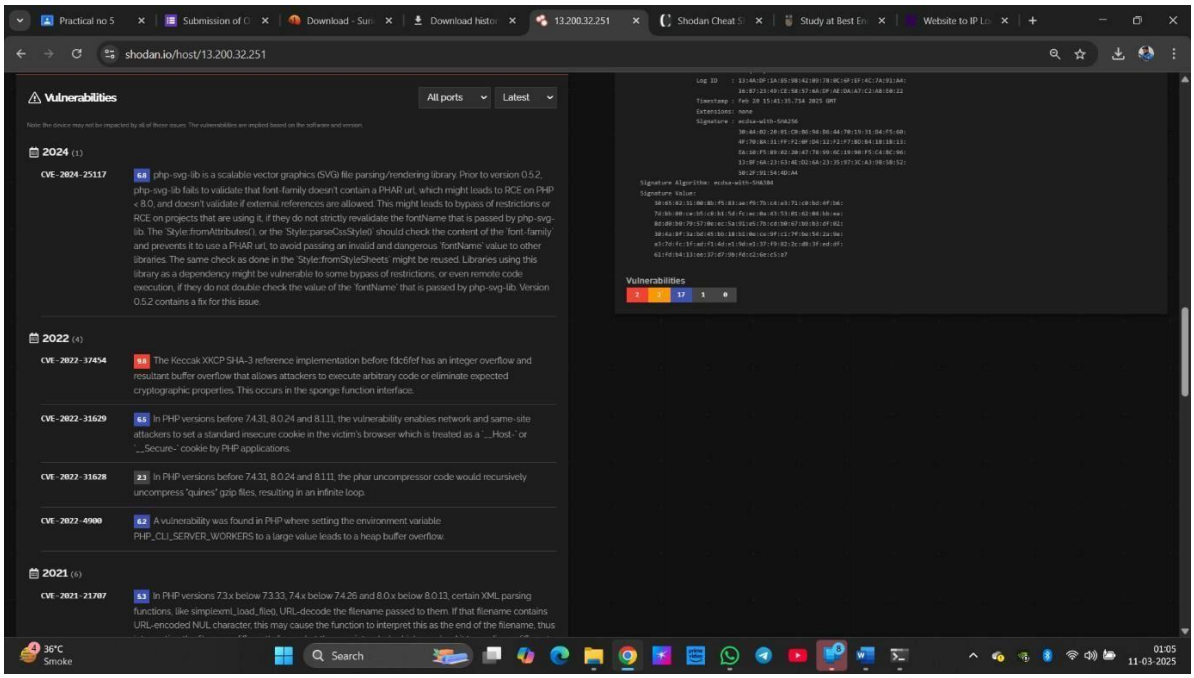


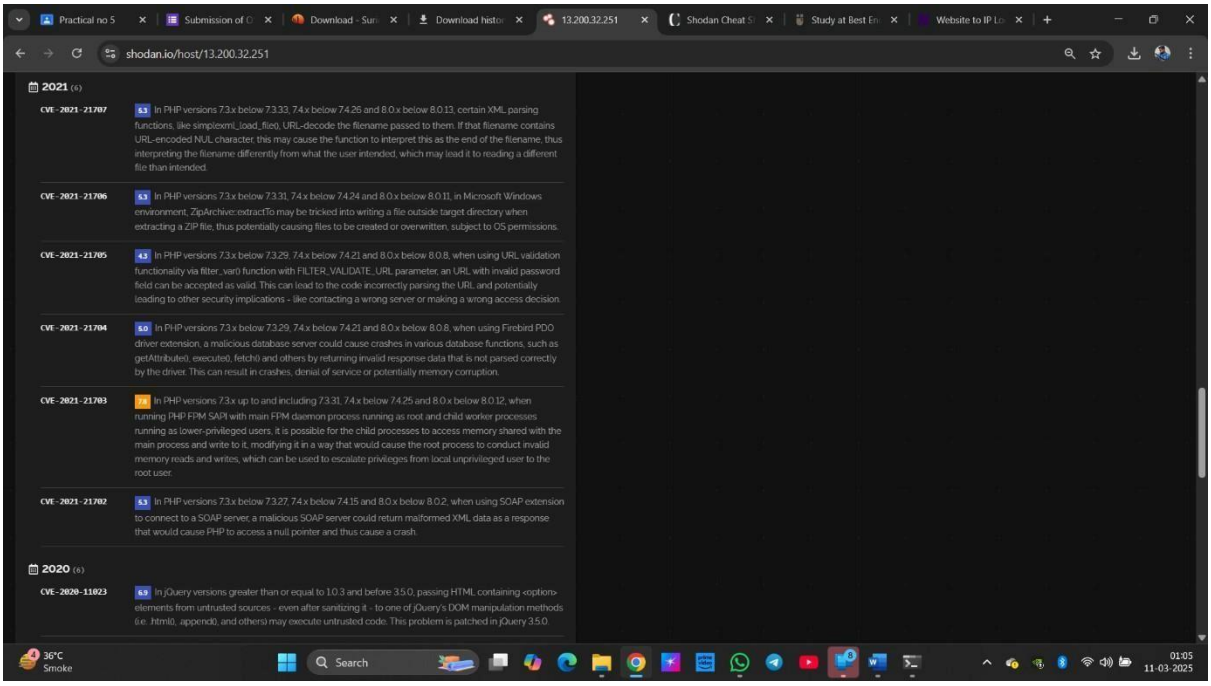
Step 2: enter IP address of the target system

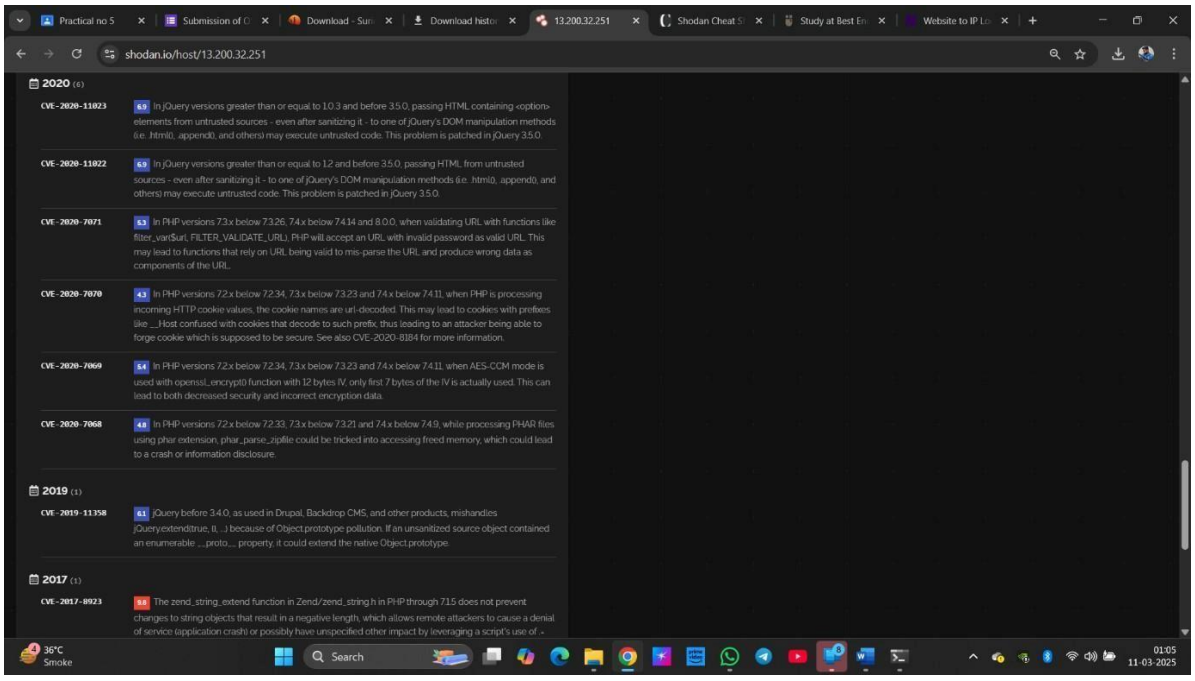


Step 3: get the information and vulnerability of target domain.









Conclusion:

Shodan is a specialized search engine designed to identify and analyze internet-exposed devices and their associated vulnerabilities through automated information gathering. Unlike traditional search engines, Shodan indexes data from IoT devices, servers, webcams, industrial control systems, and more—revealing what is accessible over the internet.

PRACTICAL 6

AIM: Intrusion detection and prevention, including setting up and configuring Suricata or other IDS/IPS systems and analyzing logs and alerts.

Definition: Maltego is an open-source intelligence (OSINT) and forensics tool that helps in data gathering and link analysis. It is widely used for cyber investigations to map relationships between entities such as people, organizations, and online resources.

Step 1: Install Suricata.

Command: sudo apt update && sudo apt install suricata Step

2: Verify Installation

Command: suricata --build-info Step

3: Configure Suricata

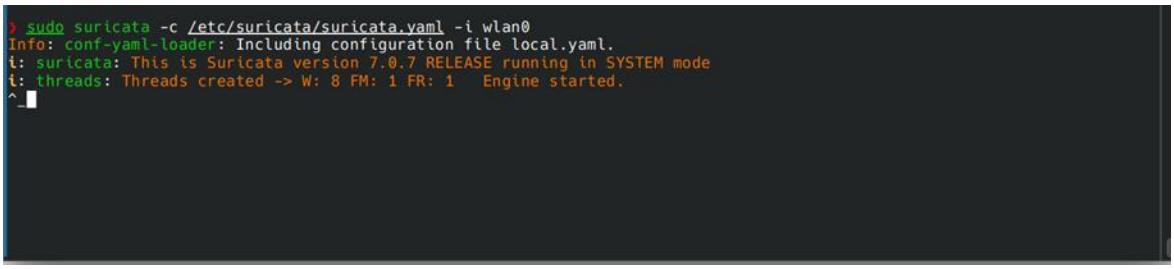
Command: sudo nano /etc/suricata/suricata.yaml Ensure the network interface is correct:

af-packet:

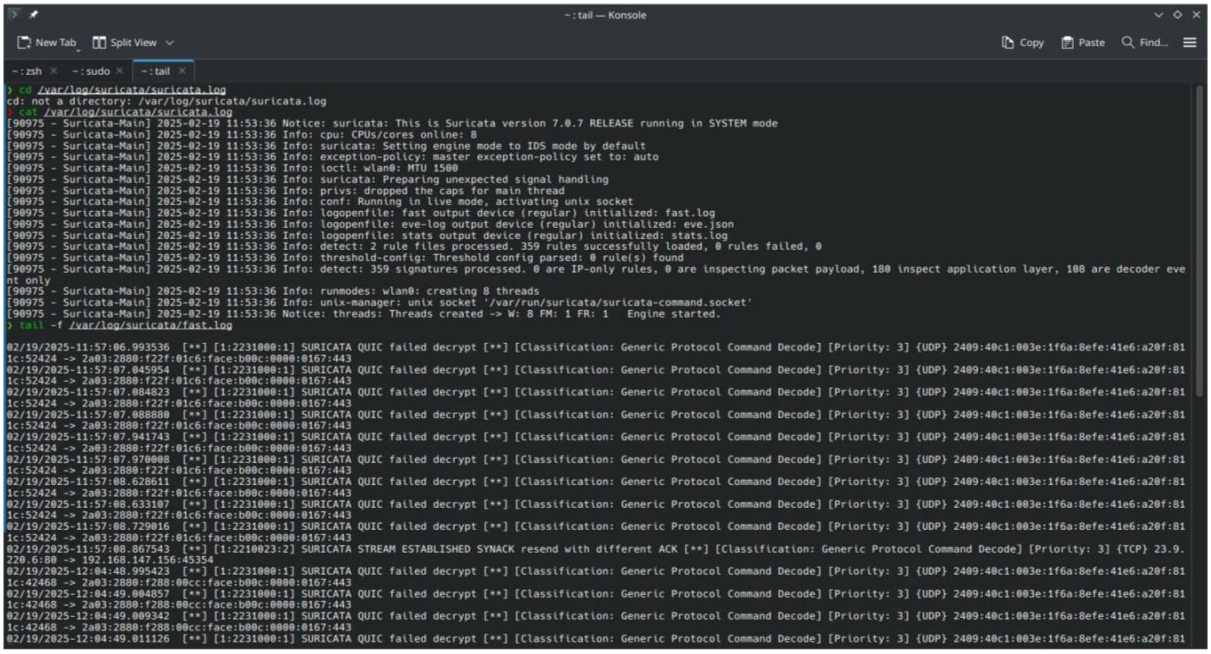
interface: eth0 # Change this to your active network interface

Step 4: Run suricata in IDS mode.

Command: sudo suricata -c /etc/suricata/suricata.yaml -i eth0



To view log alert: nano /var/log/suricata/fast.log



Conclusion:

Intrusion Detection and Prevention Systems (IDS/IPS) play a vital role in modern network security by monitoring, detecting, and responding to malicious activity in real time. Tools like Suricata offer advanced capabilities, including deep packet inspection, protocol analysis, and real-time alerting, making them essential for defending against a wide range of threats.

PRACTICAL 7

AIM: Configure S/MIME and sow email-authentication

To configure S/MIME for email authentication in Kali Linux, the process involves installing the necessary tools, obtaining a digital certificate, and setting up an email client that supports S/MIME (like Thunderbird).

Steps to Configure S/MIME on Kali Linux:

1. Install Thunderbird on Kali Linux

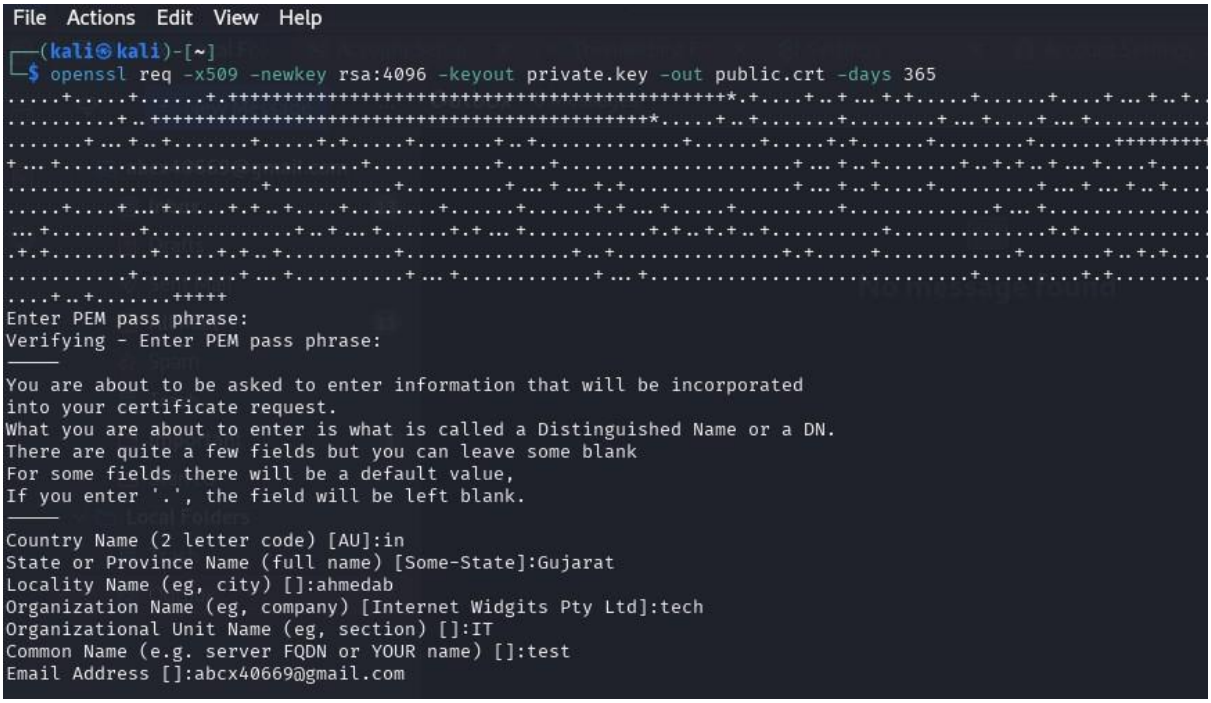
First, ensure that Thunderbird is installed on your Kali Linux system, as it is one of the most common email clients that supports S/MIME.

Command :sudo apt install thunderbird

2. Obtain a Digital Certificate

You need a digital certificate (public/private key pair) to sign and encrypt emails. You can obtain a certificate from a Certificate Authority (CA), or you can create your own self-signed certificate.

- For a self-signed certificate (for personal use): You can generate one using OpenSSL:
- Command : openssl req -x509 -newkey rsa:4096 -keyout private.key -out public.crt -days 365



3. Install the Certificate in Thunderbird

- For a personal certificate:

1. Open Thunderbird.

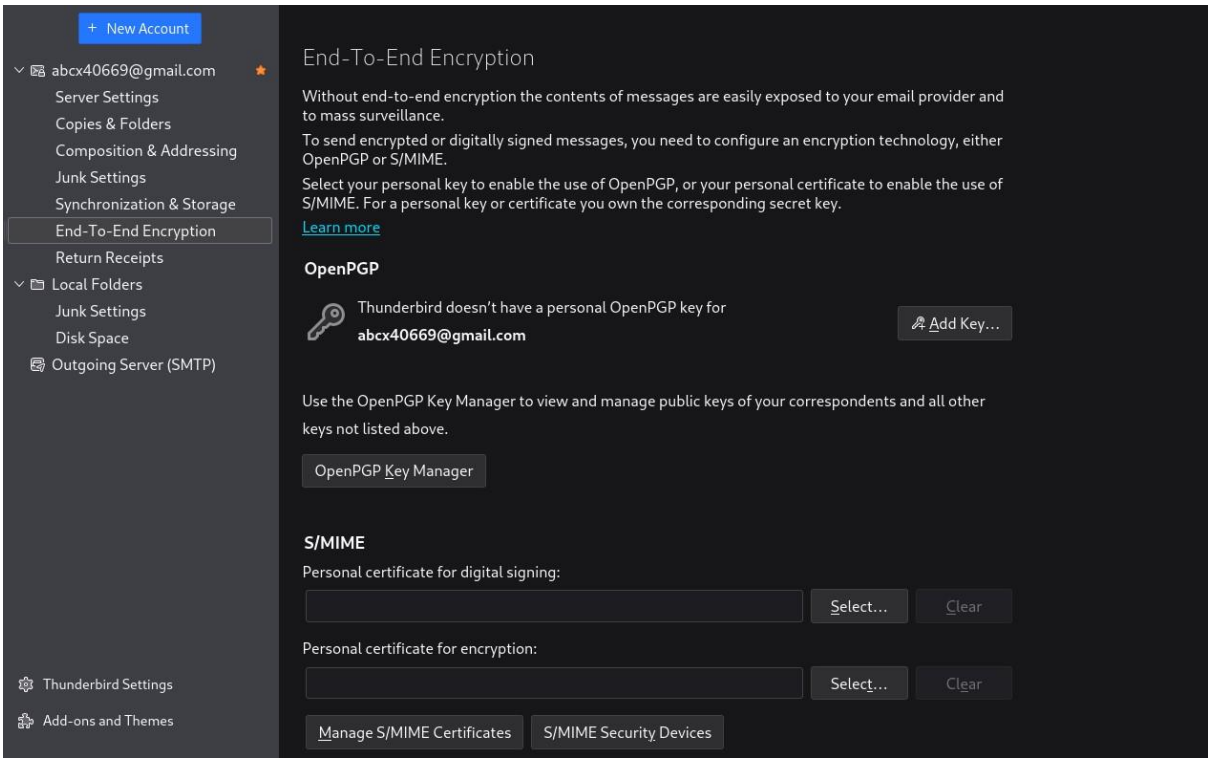
2. Go to Preferences > Account Settings.

3. Select your email account from the list.

4. Under End-to-End Encryption, click Choose... next to Digital Signing Certificate and Encryption Certificate.

5. Browse to where your certificate (e.g., public.crt) is stored and import it.

6. After importing, select the appropriate certificate for signing and encryption.



- For a certificate from a CA:If you've received the certificate as a .pfx or .p12 file from your CA, import it by navigating to Preferences > Privacy & Security in Thunderbird and selecting View Certificates > Import.
- Then, use this certificate for signing and encryption.

4. Configure Thunderbird for S/MIME Signing and Encryption

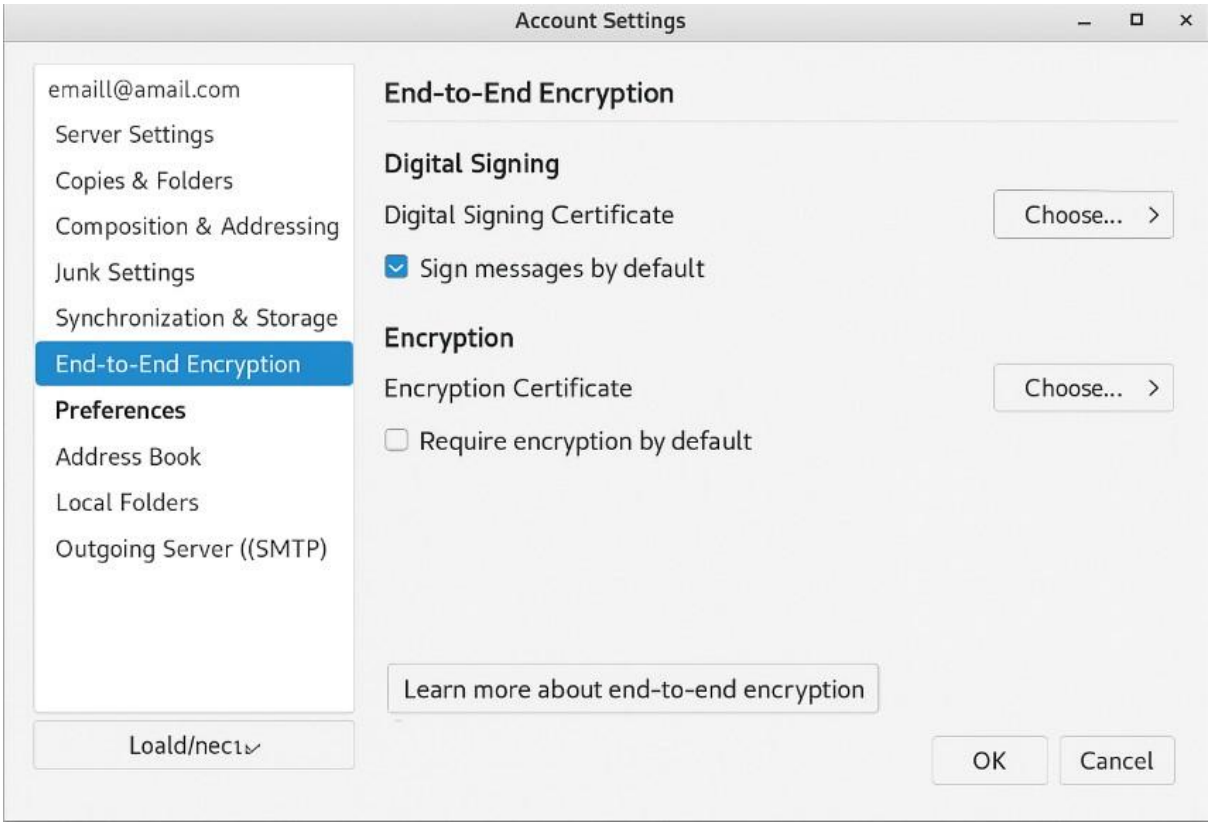
After installing your certificate, you need to configure Thunderbird to sign and encrypt your emails.

1. Go to Account Settings > End-to-End Encryption.

2. In the Digital Signing Certificate and Encryption Certificate sections, select your installed certificate.

3. Enable the option to Sign messages by default if you want all outgoing emails to be signed automatically.

4. Enable the option to Encrypt messages by default if you want to encrypt all outgoing messages (this requires the recipient's public key).

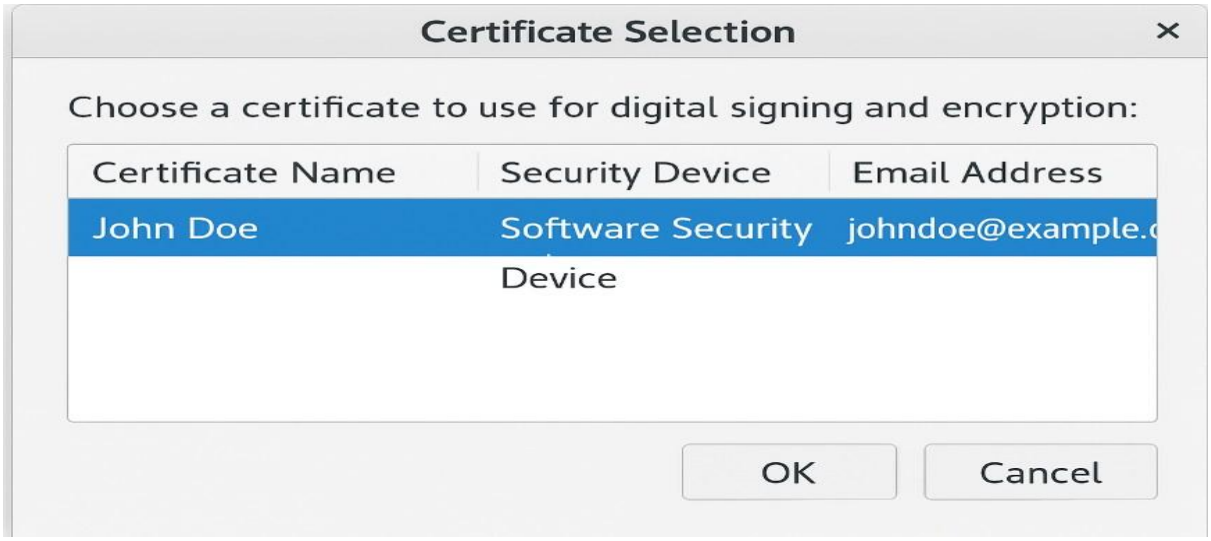


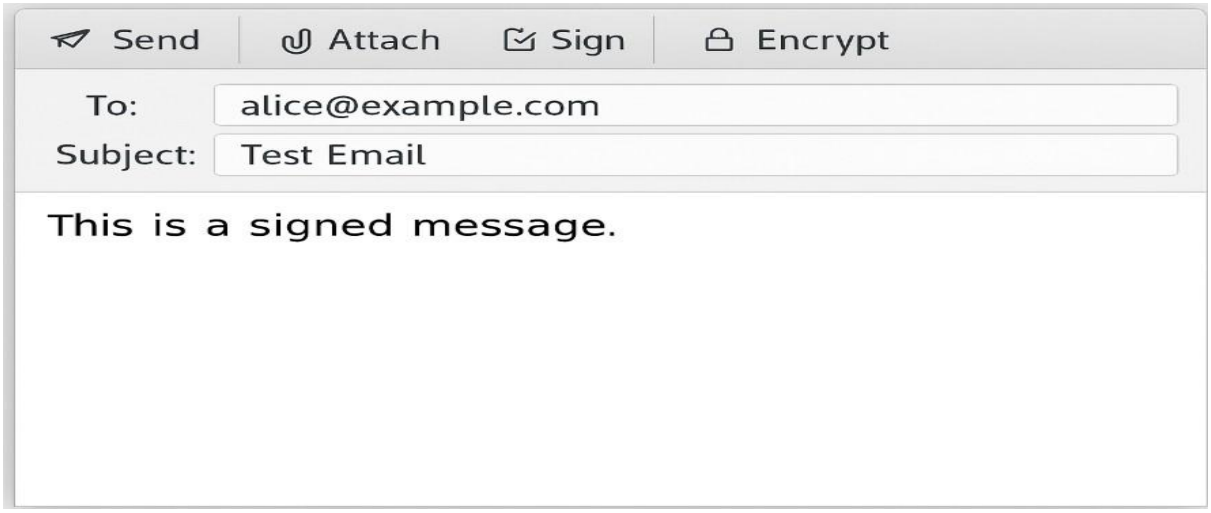
5. Sending Signed and Encrypted Emails

- To send a signed email:

When composing an email, you'll see a Sign option in the toolbar. If it's not selected, tick it to sign the email.

- To send an encrypted email:





○ You must have the recipient's public key certificate to send an encrypted email. You can obtain this by asking the recipient to send you a signed email, which will allow you to store their public key.

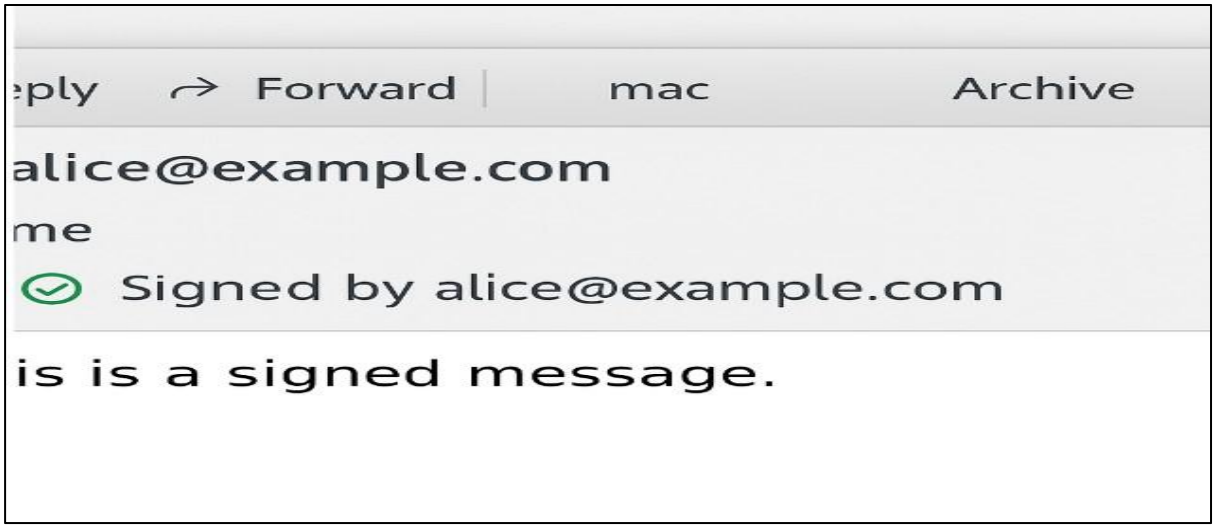
○ When composing the email, click the Encrypt button (or select the encryption option in the toolbar).

6. Verifying Email Authentication

When you receive a signed email:

● Thunderbird will show an icon indicating whether the email is signed and the signature is valid.

● If the email is encrypted, you will need the corresponding private key to decrypt it.



Conclusion:

By following these steps, you will have successfully set up S/MIME on Kali Linux using Thunderbird to send signed and encrypted emails. Remember, both the sender and recipient need valid certificates to send encrypted emails.

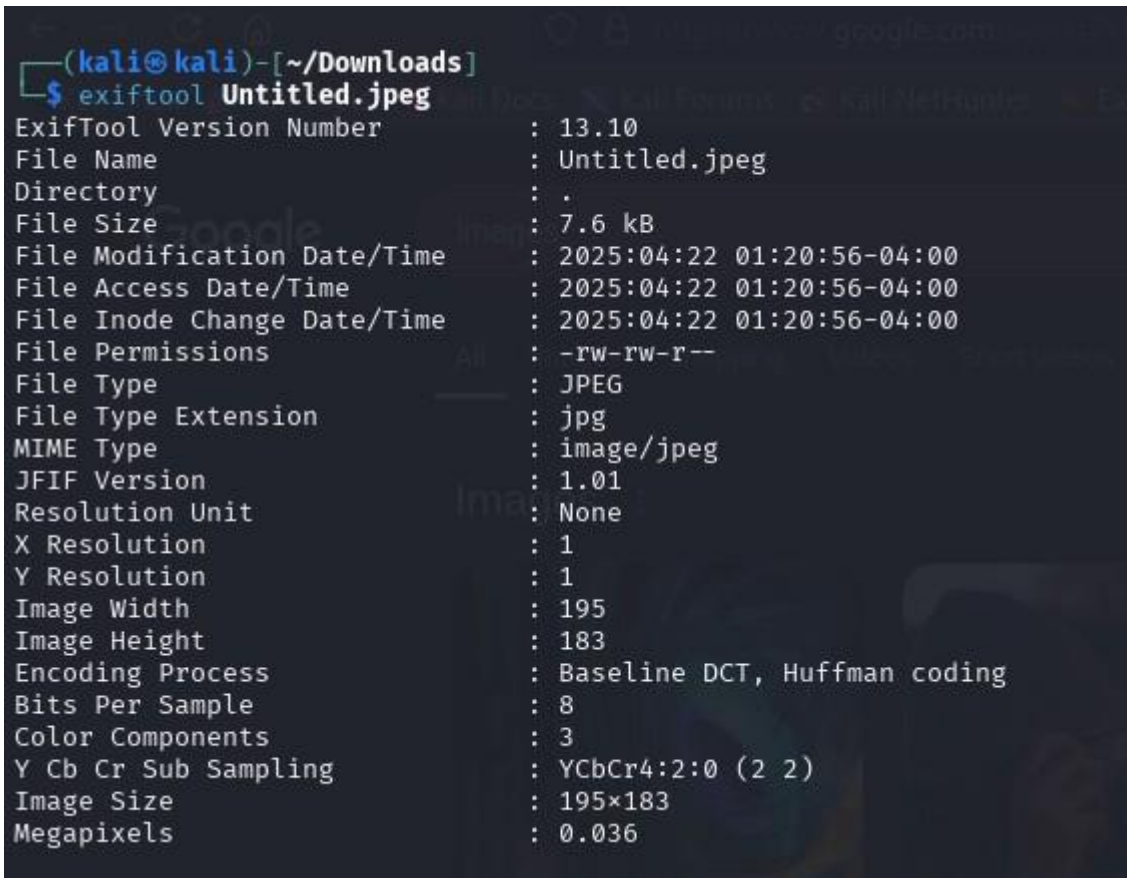
PRACTICAL 8

AIM: To extract and analyze metadata from various file types (image, document, and video) using metadata analysis tools such as and , and to understand the significance of metadata in digital forensics and information security.

Metadata Analysis Tools by File Type

1.Images , Videos & Other

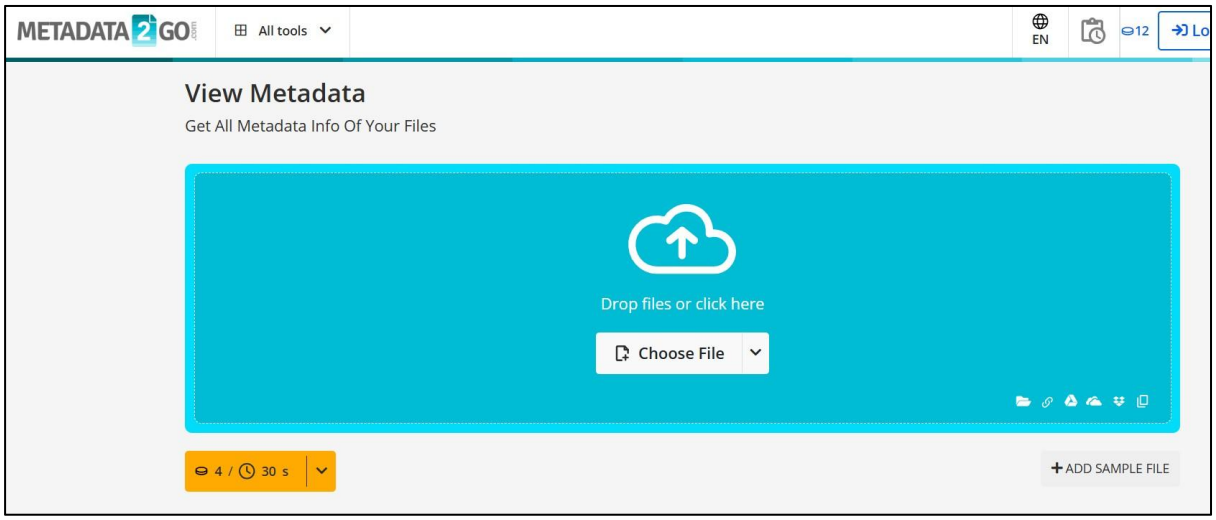
ExifTool: A powerful command-line utility that reads, writes, and edits metadata for a wide range of file formats, including images. It supports metadata types like EXIF, IPTC, and XMP Command : exiftool image.jpg



2.Documents (e.g., PDFs, Word Files)

ExifTool: Also supports metadata extraction from various document formats.

Metadata2Go: Supports document files, enabling you to upload and analyze metadata from PDFs, Word documents, and more.



checksum	fddf0a2036635598be92c8c0045e1bd5
file_name	practical-1.pdf
file_size	481 kB
file_type	PDF
file_type_extension	pdf
mime_type	application/pdf
pdf_version	1.7
linearized	No
page_count	7
language	en

tagged_pdf	Yes
xmp_toolkit	3.1-701
producer	Microsoft® Word 2019
creator	CYBER
creator_tool	Microsoft® Word 2019
create_date	2025:03:11 16:57:15+05:30
modify_date	2025:03:11 16:57:15+05:30
document_id	uuid:C16B5BC4-AEA7-40A3-9983-761CEA1B7A20
instance_id	uuid:C16B5BC4-AEA7-40A3-9983-761CEA1B7A20
author	CYBER
category	application

Conclusion:

Metadata analysis is a critical component of digital forensics and information security, providing valuable contextual information about files—such as creation dates, authorship, geolocation data, device information, and modification history. By extracting and analyzing metadata from various file types, including images, documents, and videos, investigators can uncover hidden insights that are often invisible in the file content itself.

PRACTICAL 9

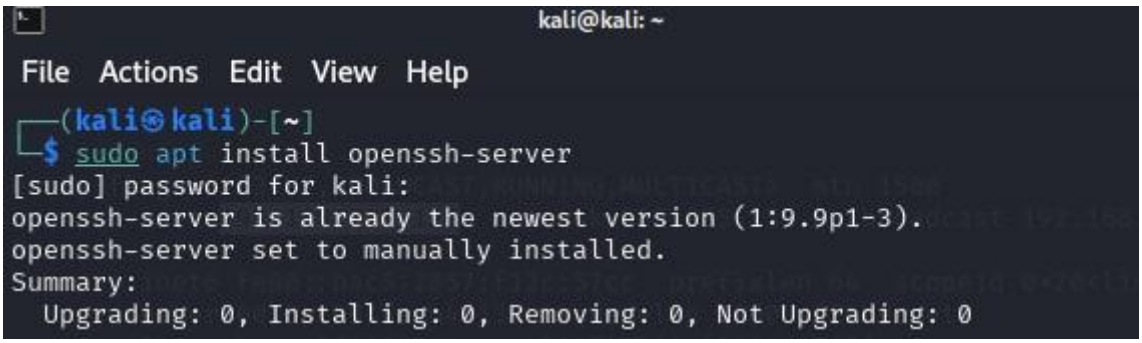
AIM: To configure SSH (Secure Shell) for secure remote communication between systems and to verify the configuration by securely sending and receiving a file over the SSH connection using the configured parameters.

Definition : SSH (Secure Shell) is a protocol that provides a secure channel over an unsecured network by using encryption for remote login, command execution, and file transfer between two networked devices.

Step 1: Install SSH (if not already installed)

Command : sudo apt update

sudo apt install openssh-server



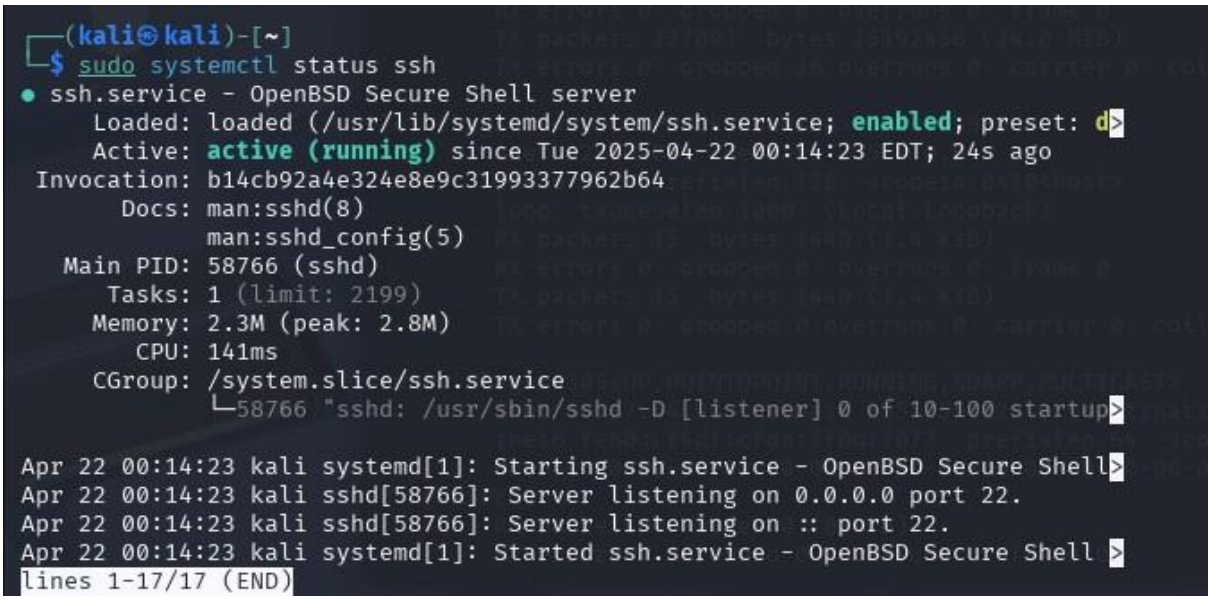
Step 2: Start and Enable SSH Service

Command : sudo systemctl start ssh

sudo systemctl enable ssh

Step 3:Check SSH Status

Command : sudo systemctl status ssh



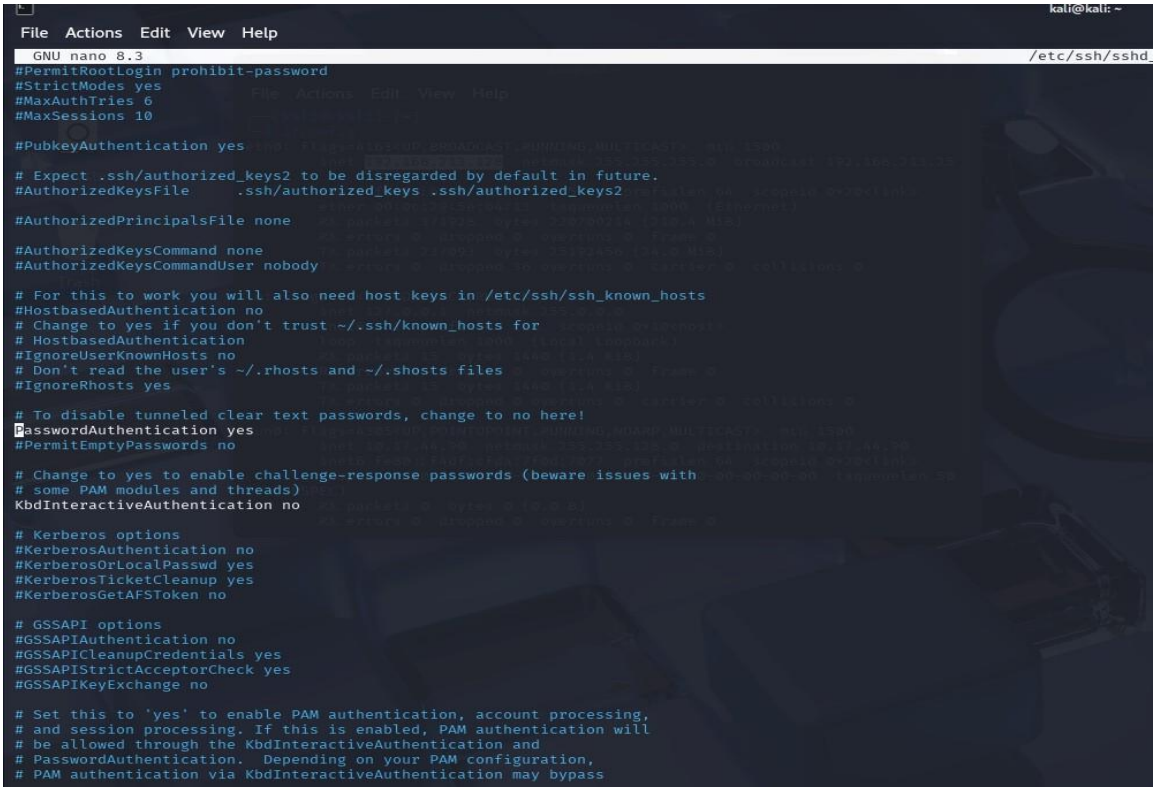
Step 4: Configure SSH (optional but recommended)

Command : sudo nano /etc/ssh/sshd_config

Edit in File : Port 22

PermitRootLogin no , PasswordAuthentication yes

PermitEmptyPasswords no



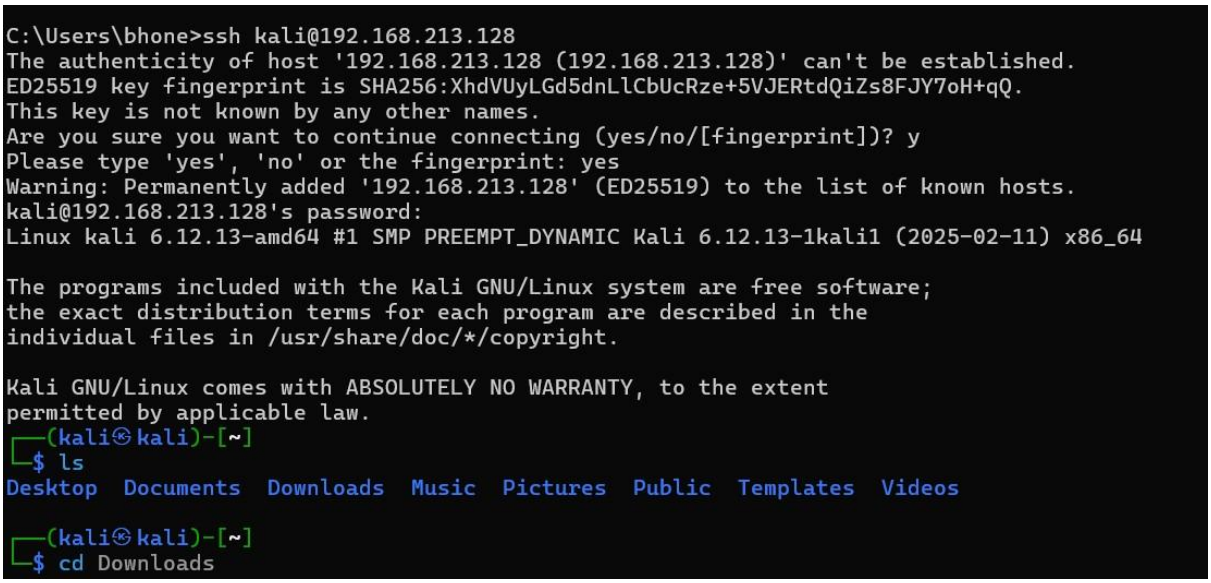
Step 5 : Then restart the SSH service to apply changes:

Command :sudo systemctl restart ssh

Step 6 :Test SSH Connection

From System A, connect to System B: Access kali machine in windows

Command :ssh kali@192.168.213.128



Step 7: Receive a File from Remote to Local

Copy a file from the remote system to your local machine:

Conclusion:

Configuring SSH (Secure Shell) is a fundamental step in ensuring secure remote communication between systems. SSH provides encrypted channels that protect data in transit from eavesdropping, tampering, and unauthorized access, making it a critical component in system administration and network security.

PRACTICAL 10

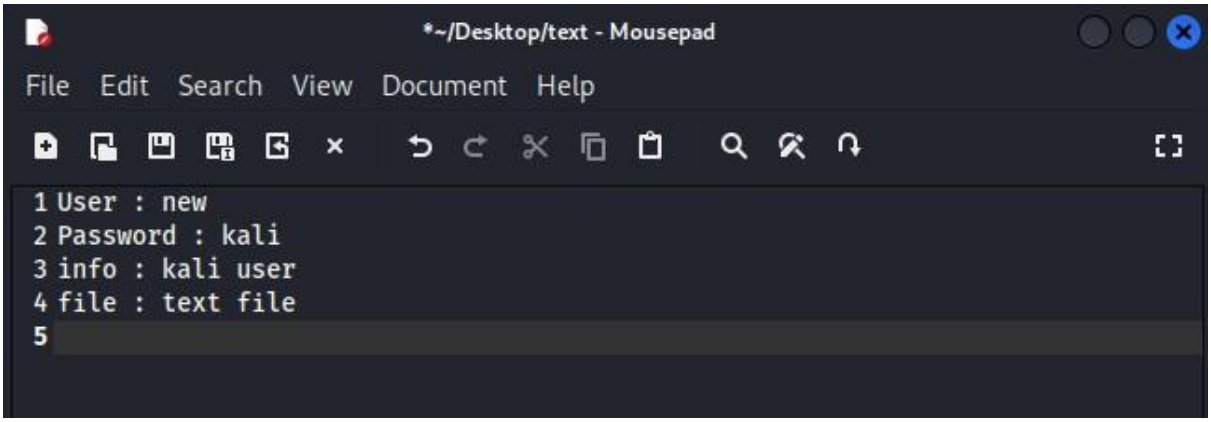
AIM: To implement encryption and decryption with OpenSSL.

Definition: OpenSSL is a powerful command-line tool that facilitates encryption and decryption using various cryptographic algorithms.

Symmetric Encryption (Password-Based)

Symmetric encryption uses the same password for both encryption and decryption.

Step 1: Create text file



Step 2: Encrypting a File

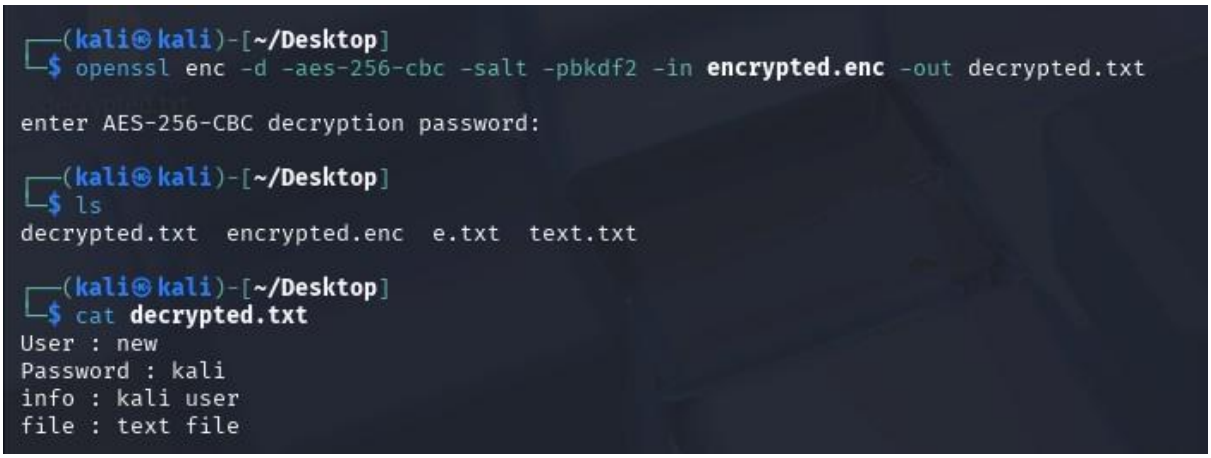
Command : openssl enc -aes-256-cbc -salt -pbkdf2 -in text.txt -out encrypted.enc

Explanation:

- enc: Specifies the encryption command.
- -aes-256-cbc: Uses the AES algorithm with a 256-bit key in CBC mode.
- -salt: Adds a random salt to strengthen encryption.
- -pbkdf2: Applies the PBKDF2 key derivation function for enhanced security.
- -in plaintext.txt: Specifies the input file to encrypt.
- -out encrypted.enc: Specifies the output encrypted file.

Step 3: Decrypting a File

Command : openssl enc -d -aes-256-cbc -salt -pbkdf2 -in encrypted.enc -out decrypted.txt



Explanation:

- -d: Indicates decryption mode.
- Other parameters mirror those used during encryption.

Conclusion: Successfully perform encryption and decryption using open ssl

Conclusion:

Implementing encryption and decryption using OpenSSL is a practical and essential step in understanding how data confidentiality and integrity are maintained in secure communication. OpenSSL provides a powerful set of tools and libraries that support a wide range of cryptographic functions, including symmetric and asymmetric encryption, hashing, and digital certificates.