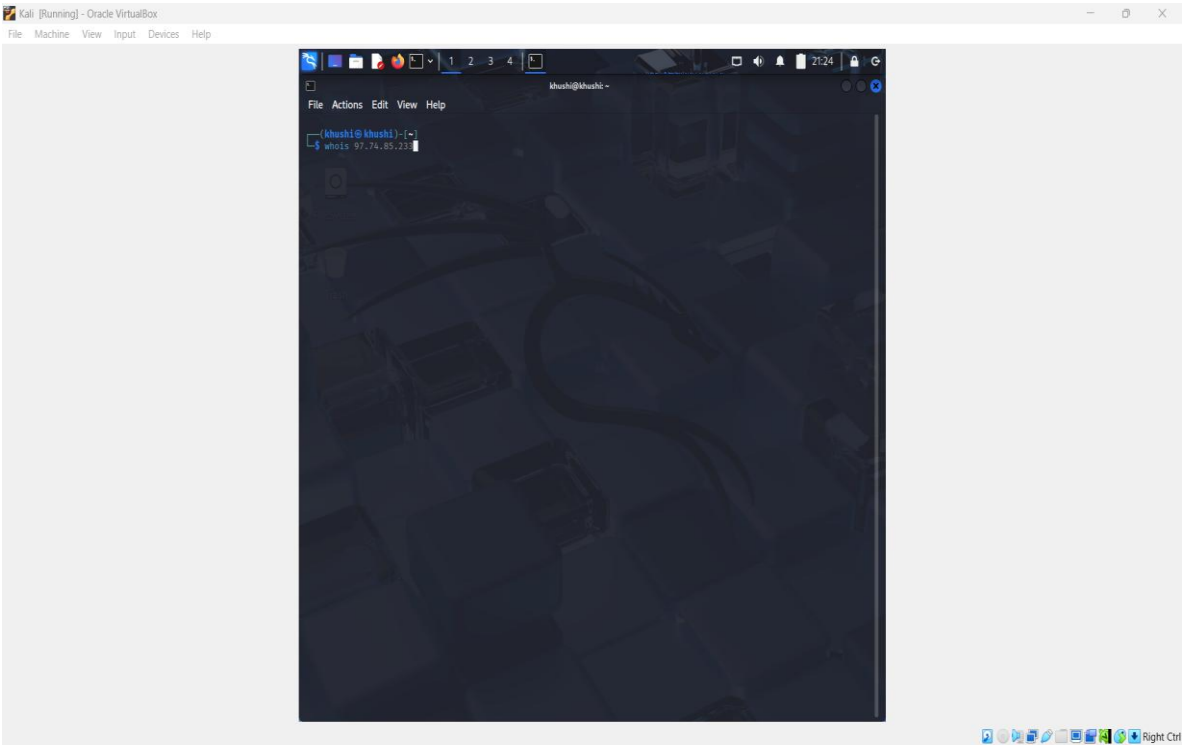
Practical-2

AIM:

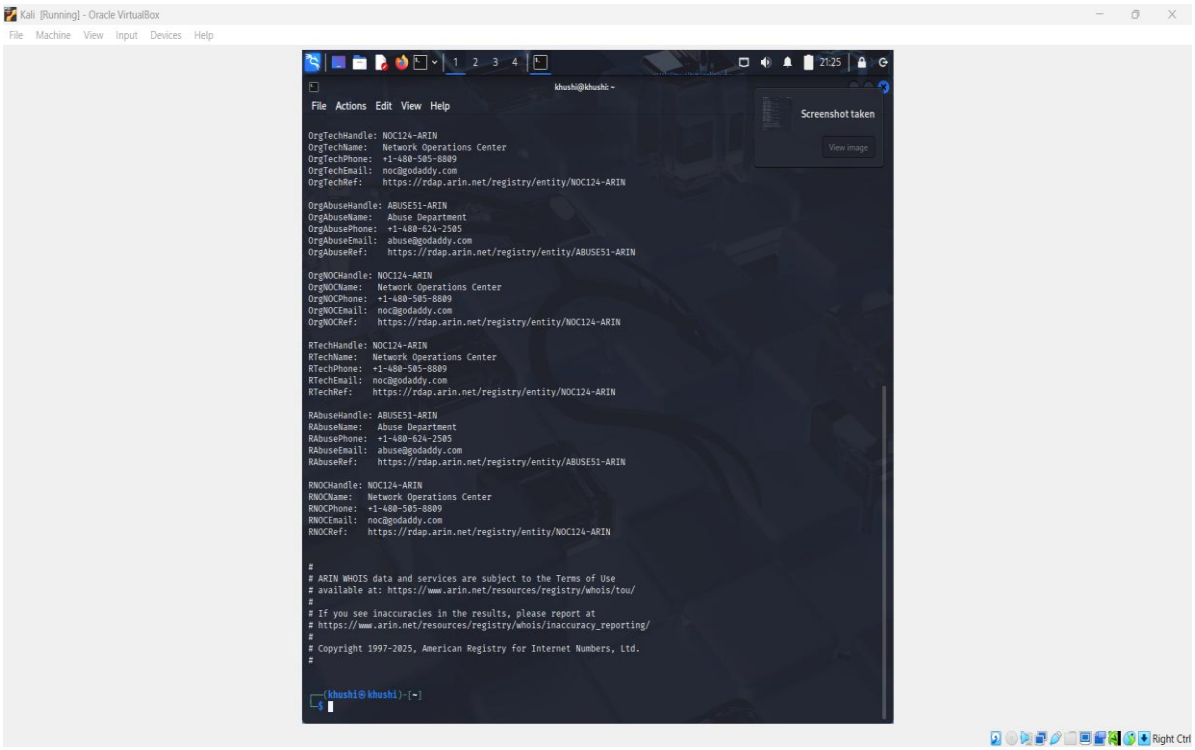
Perform passive reconnaissance on the target web application/server using tools like Whois, nslookup, dig, host, dnsrecon, dnsenum, theHarvester, and DNSDumpster to collect domain and infrastructure details without active interaction.

STEPS with screenshots:

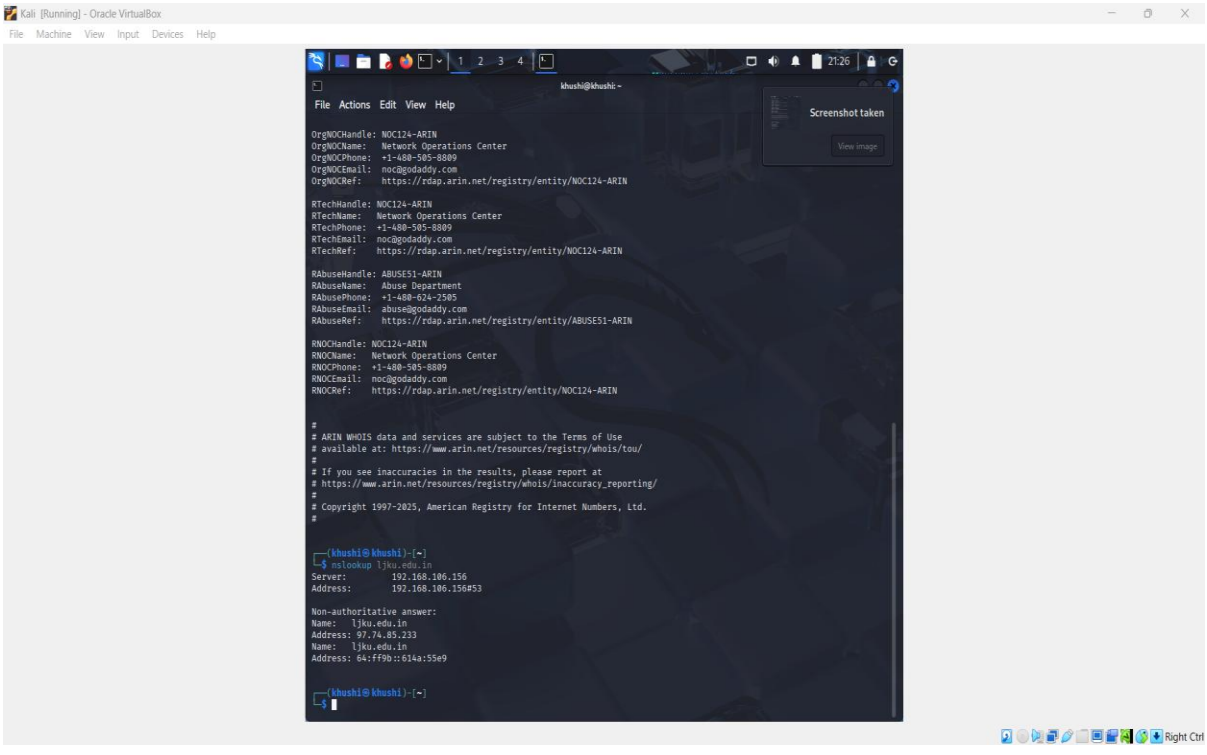
1) Whois



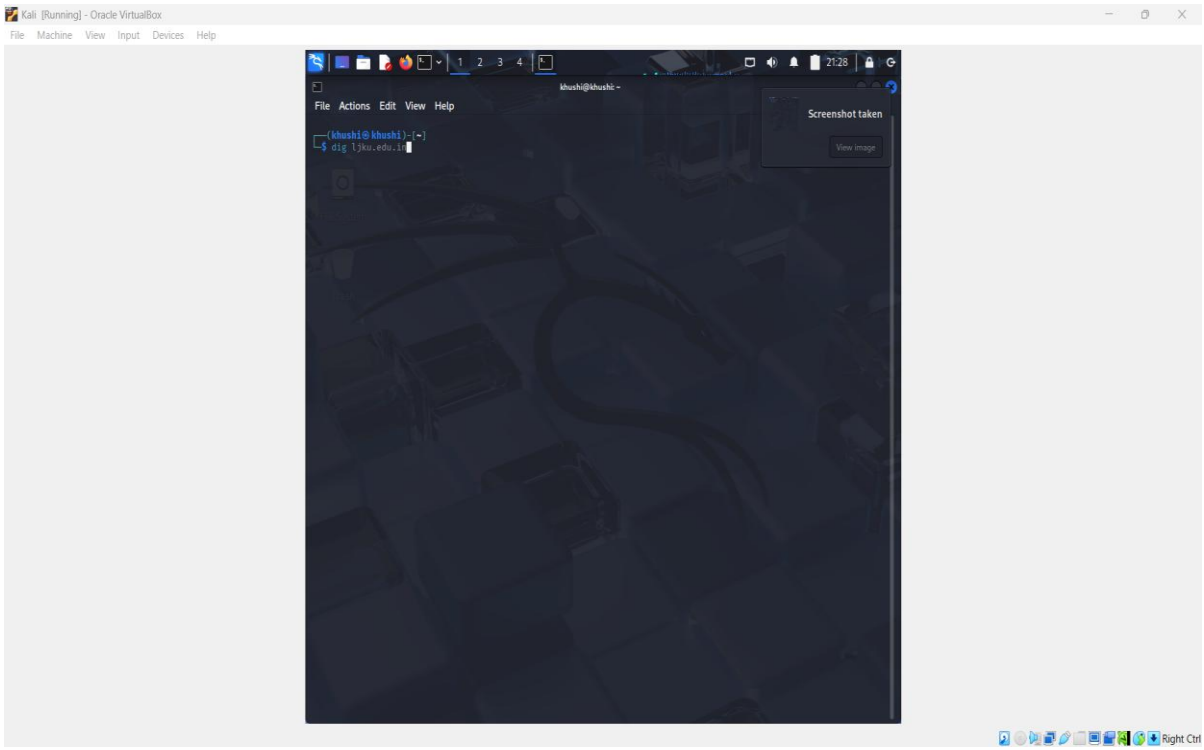
Output of Whois Commad:



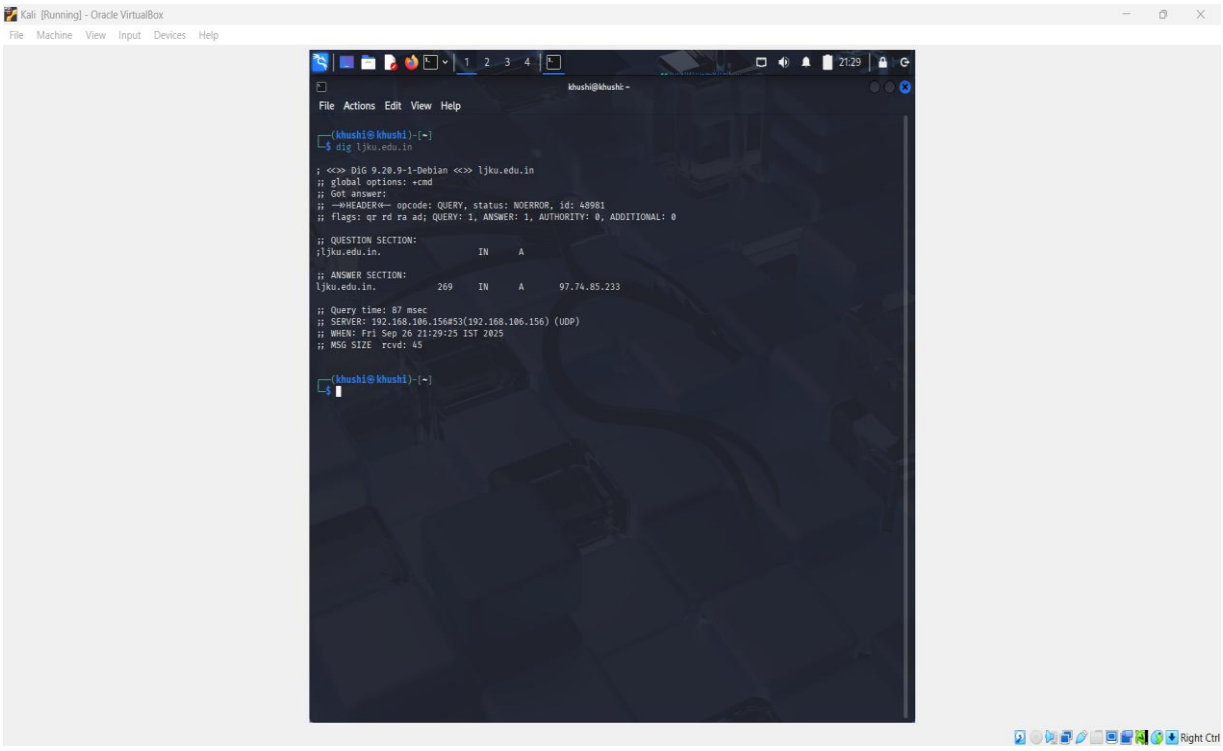
2) Nslookup With Output:



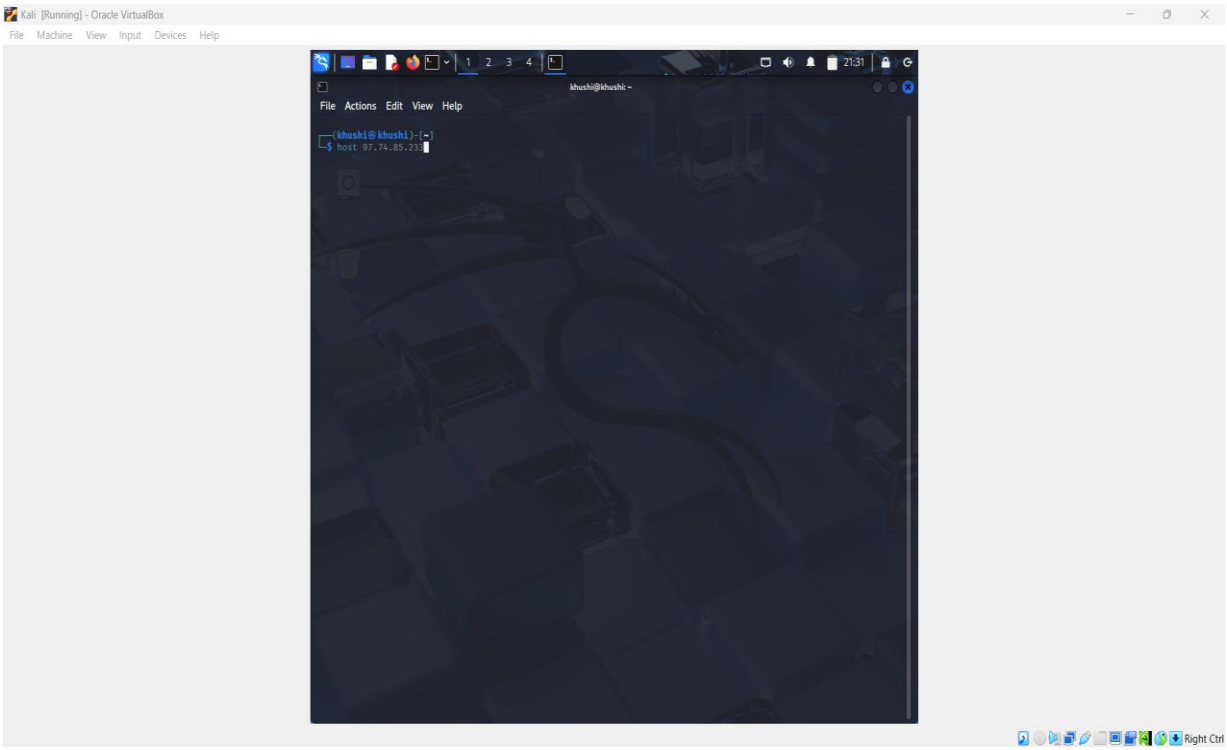
3) Dig:



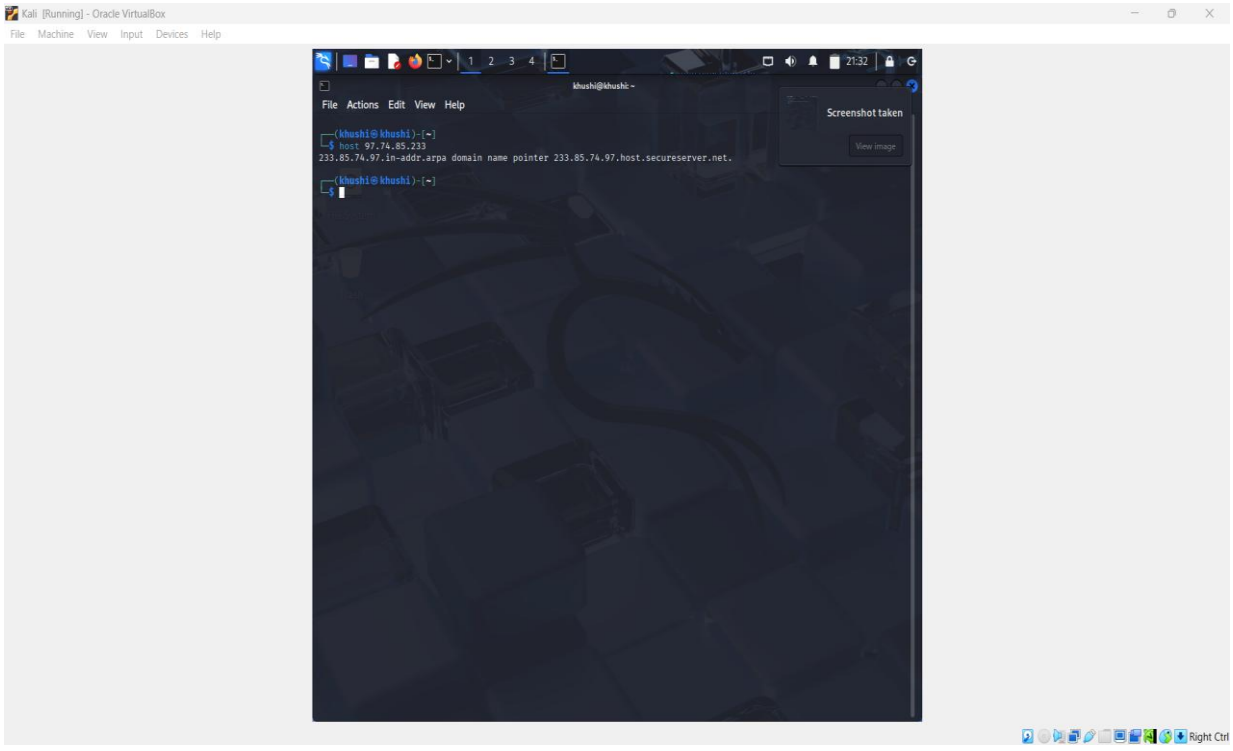
Dig Command Output:



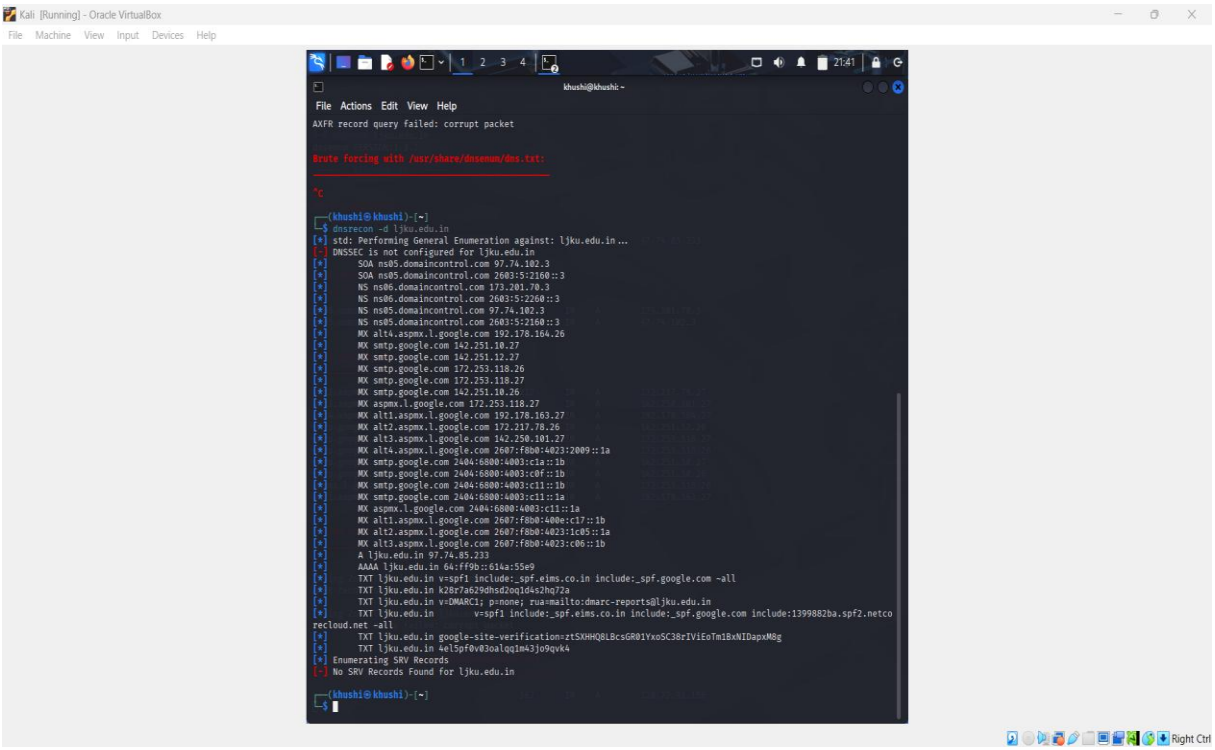
4) Host **:**



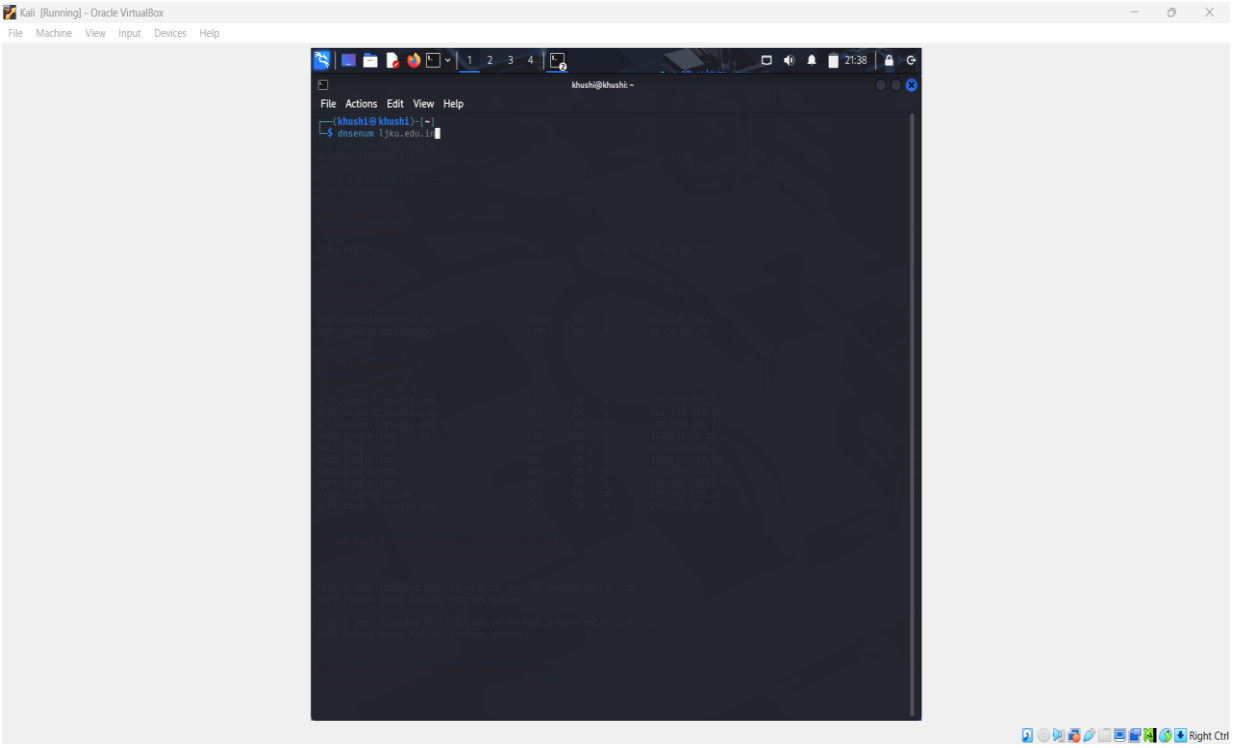
Host Command Output :



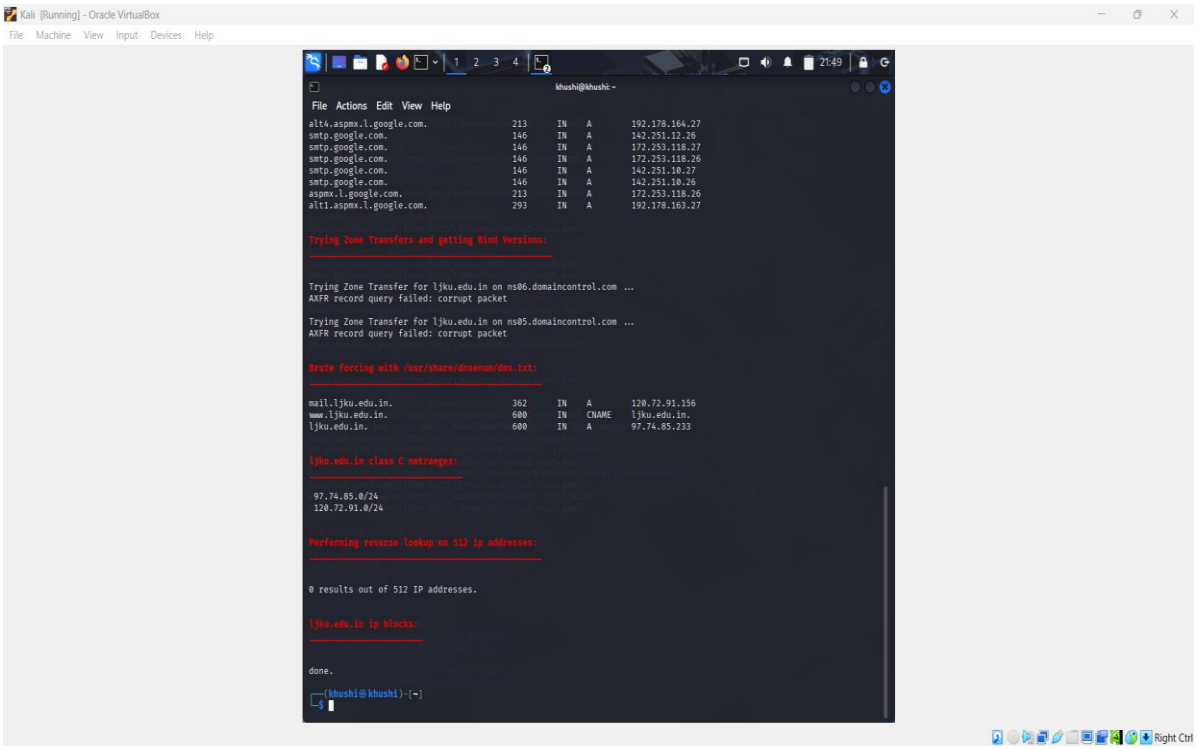
5) Dnsrecon with Output :



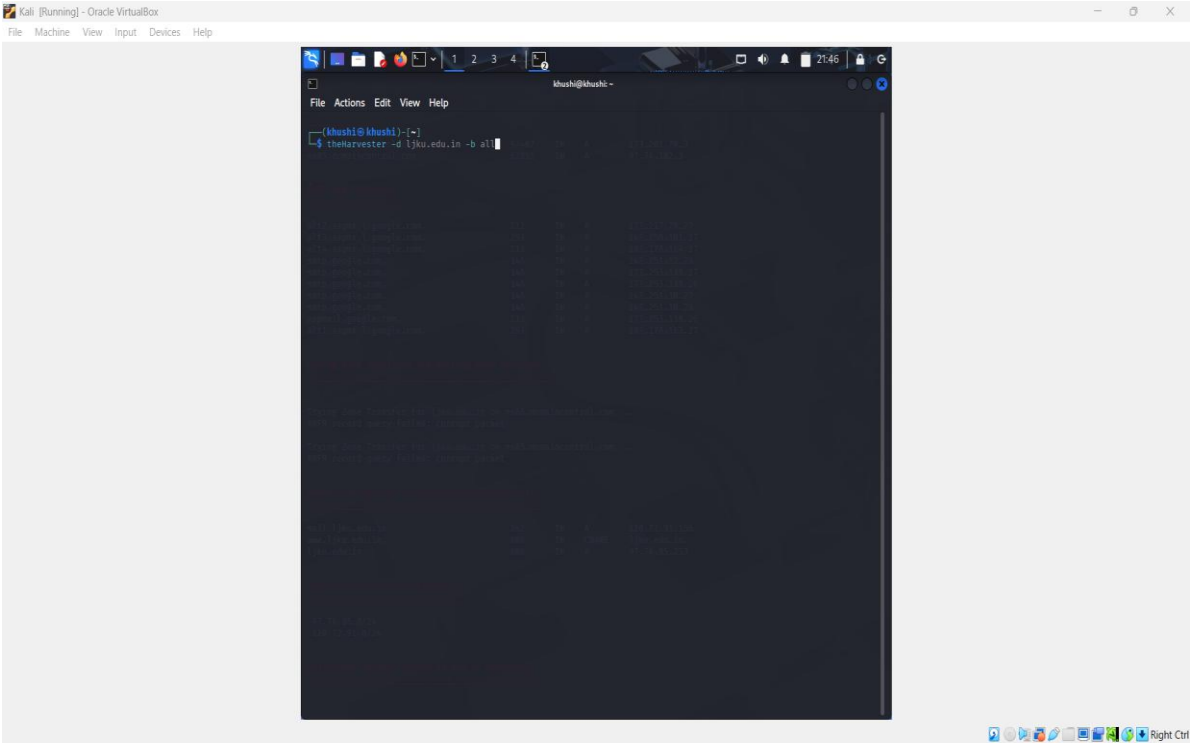
6) Dnsenum :



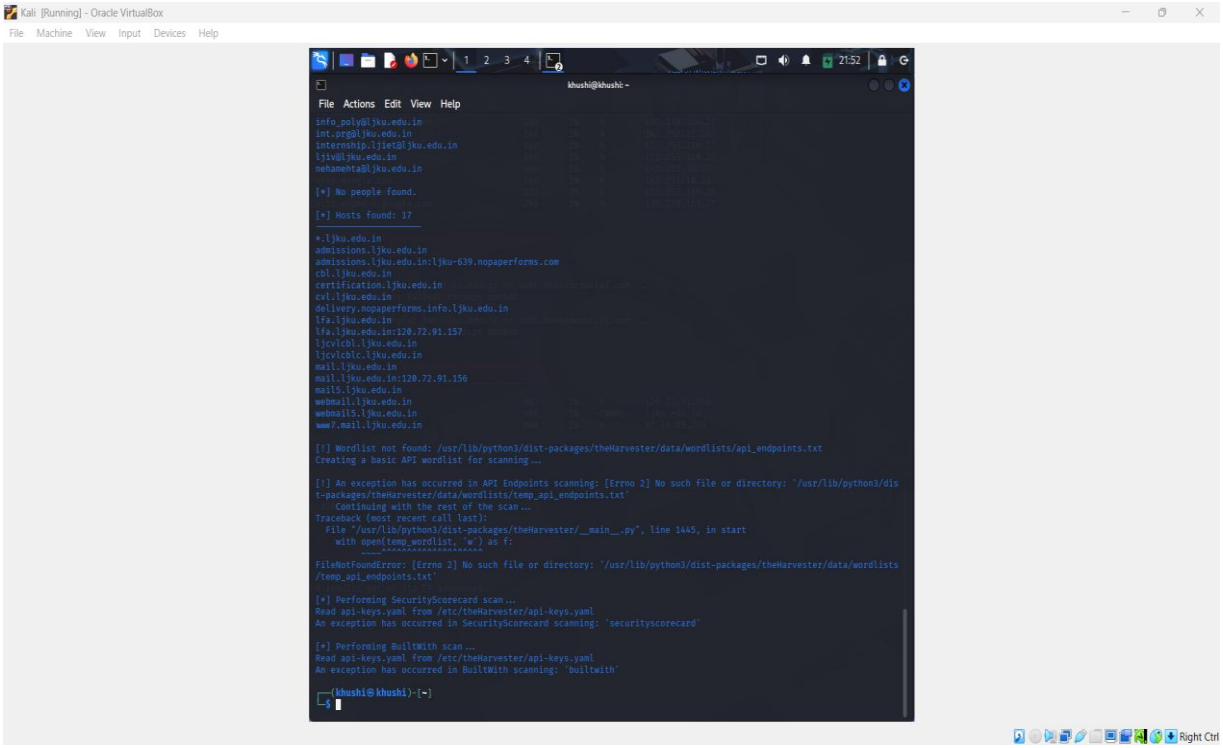
Dnsenum Command Output :



7) theHarvester:



theHarvester Command Output :



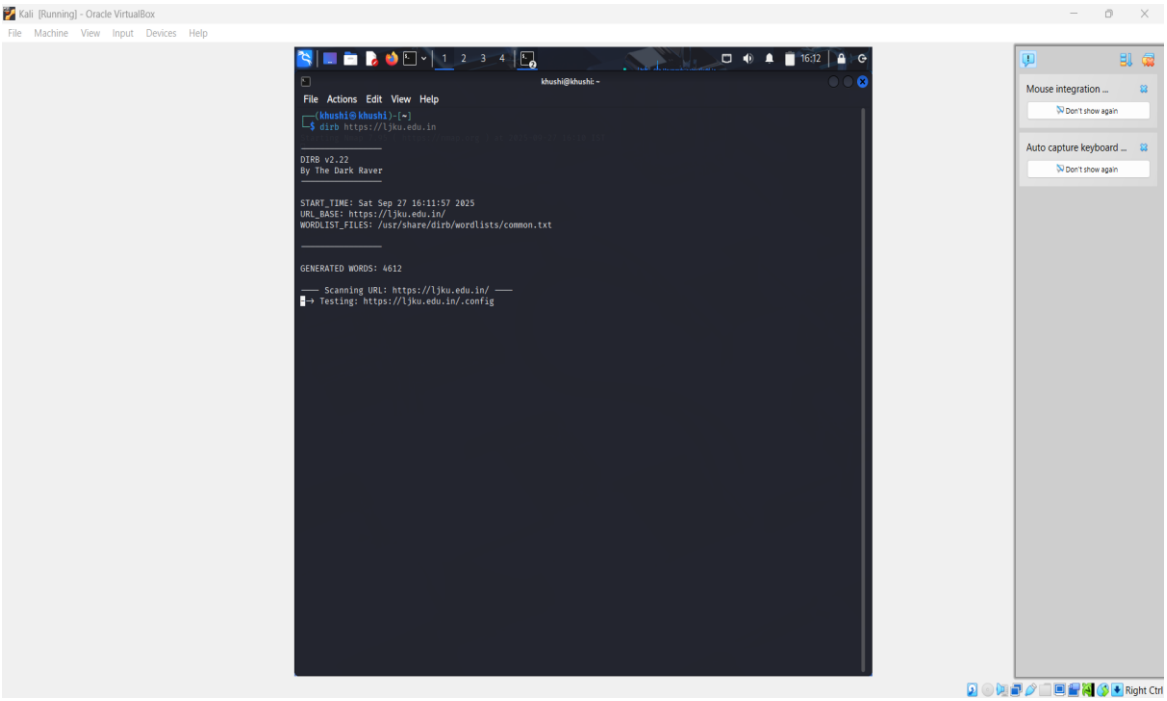
Practical-3

AIM:

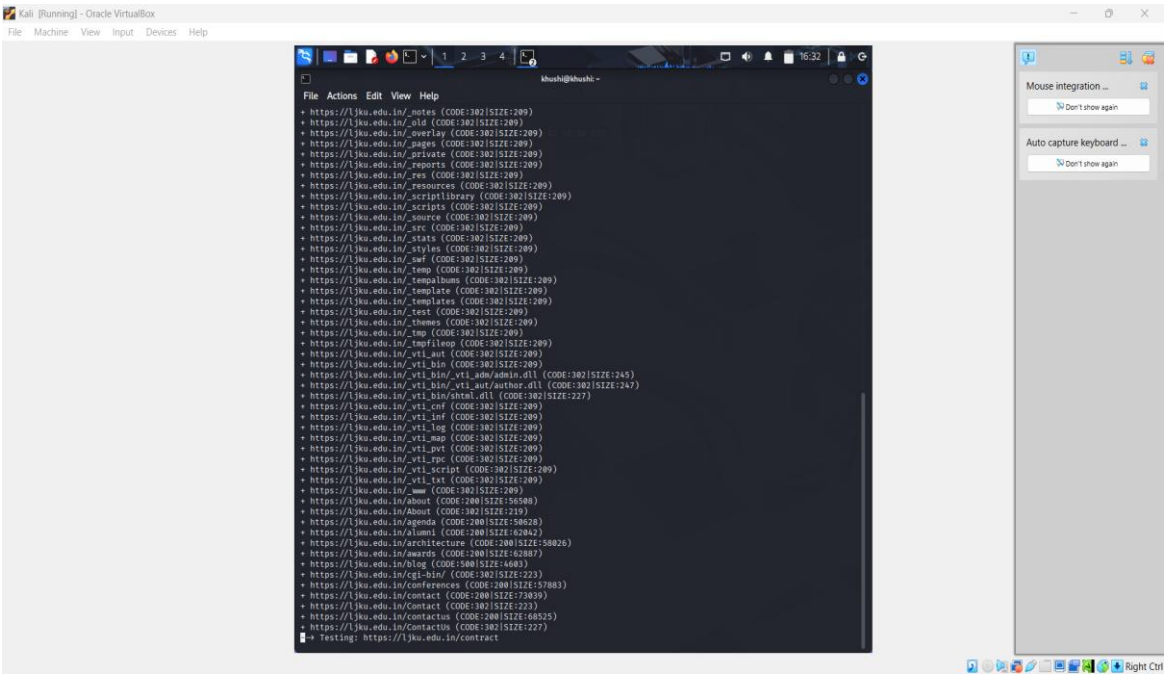
Conduct active reconnaissance on the target web application/server using tools such as dirb, ping, traceroute, netdiscover, sublist3r, amass, wget, and curl to identify directories, subdomains, network structure, and live hosts.

STEPS with screenshots:

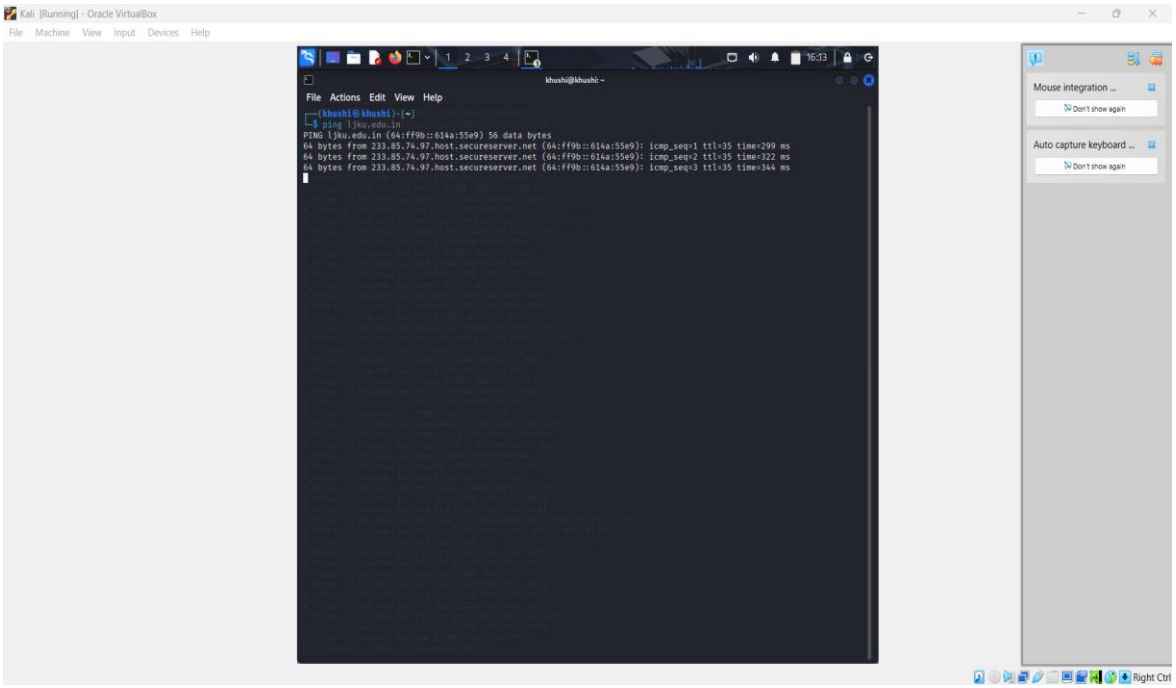
1) dirb:



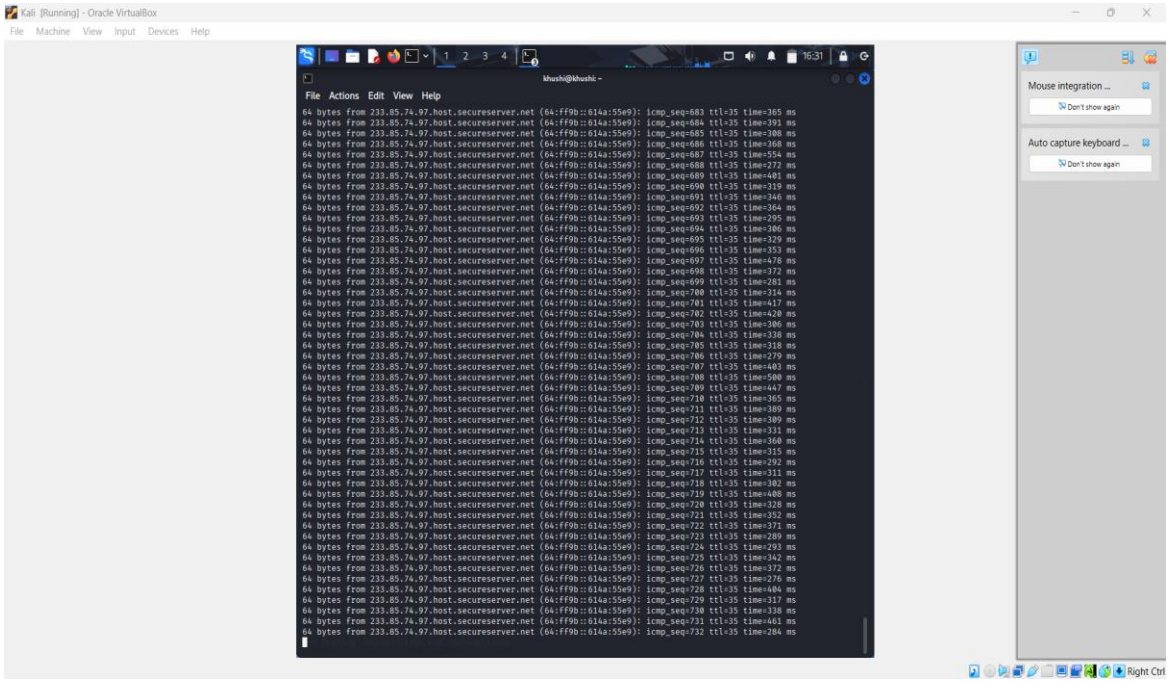
Dirb Command Output :



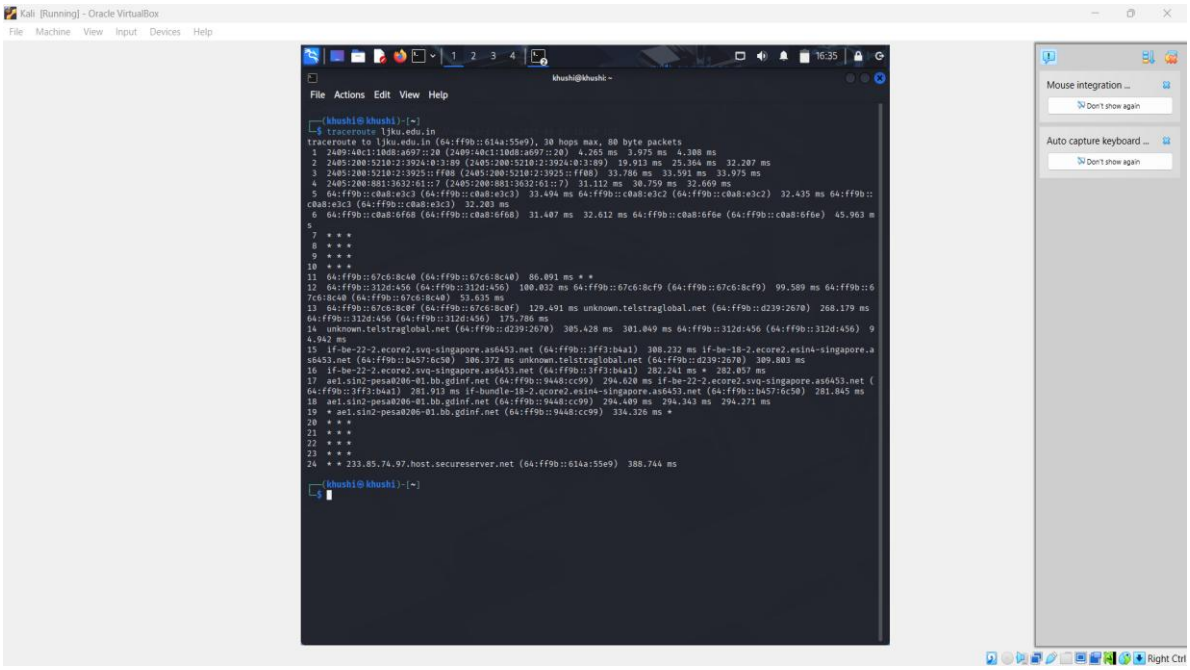
2) ping:



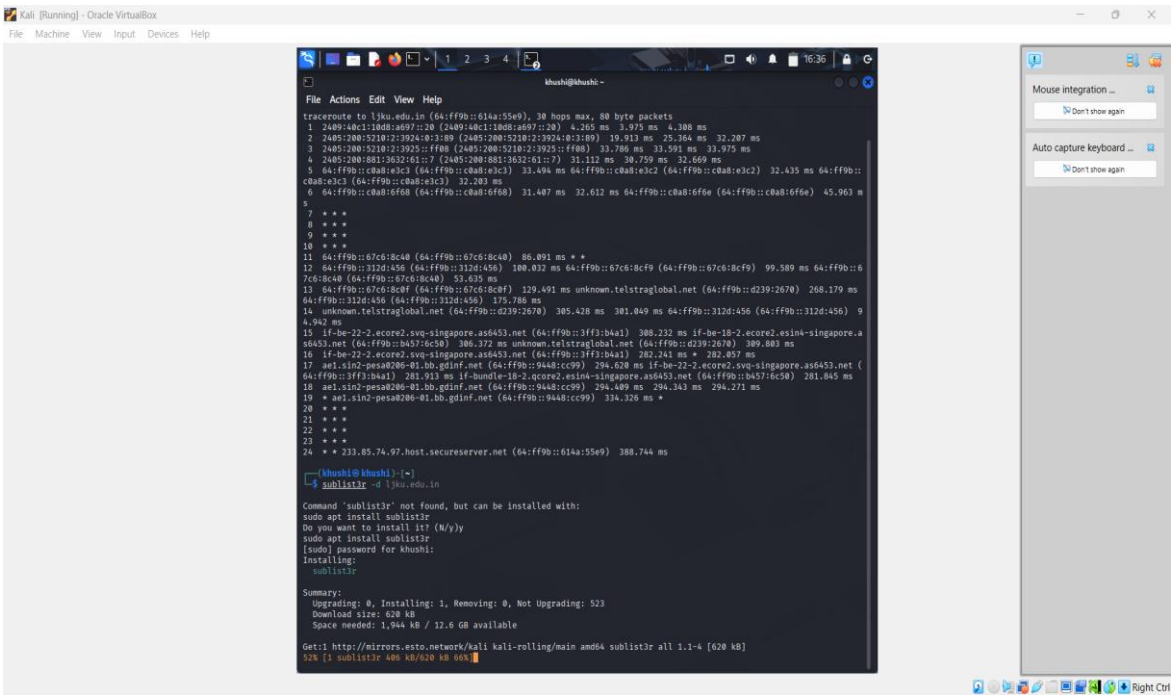
Pig Command Output :



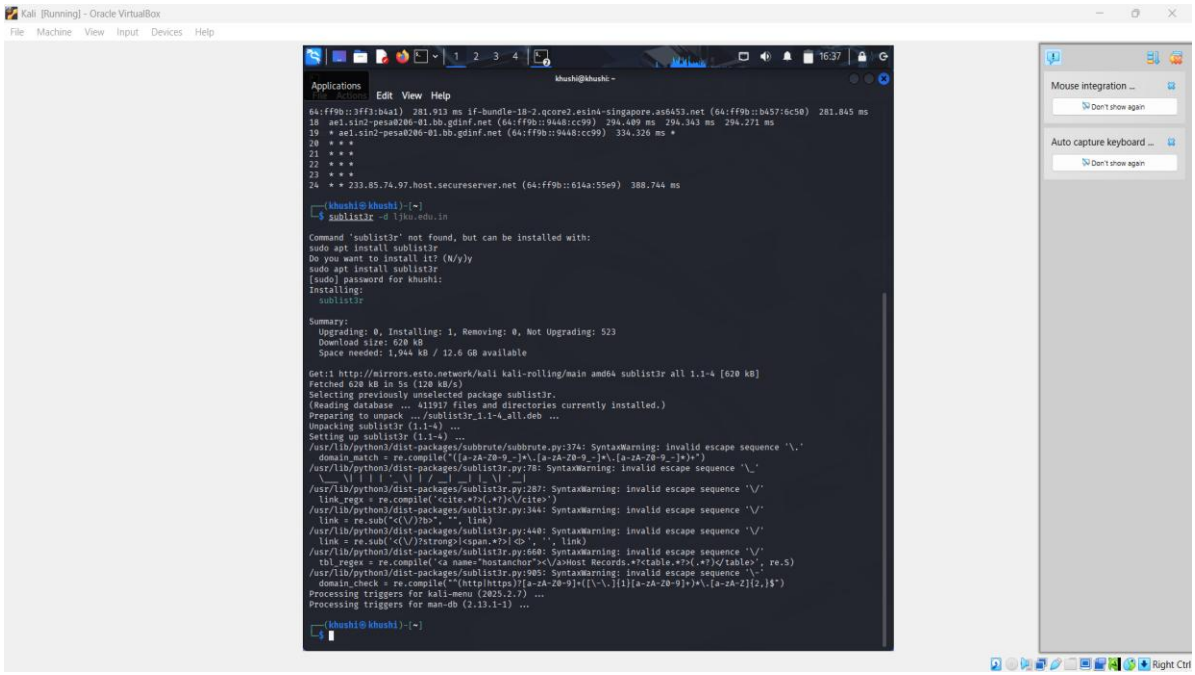
3) traceroute Command With Output :



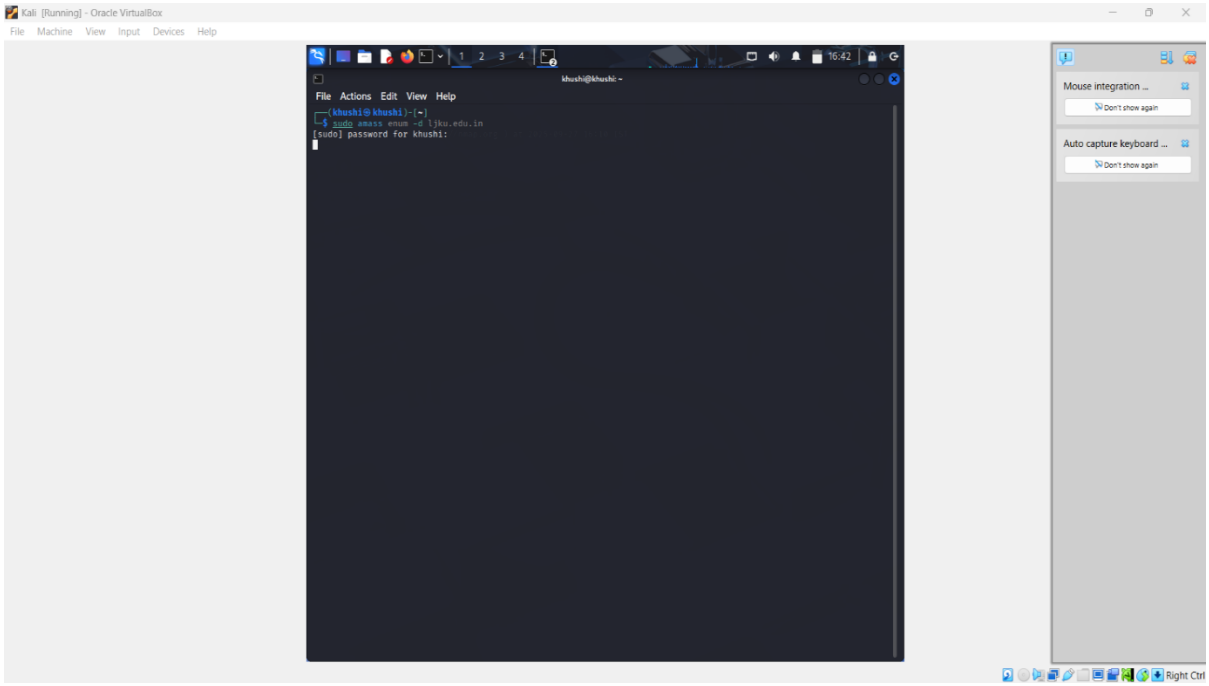
4) sublist3r :



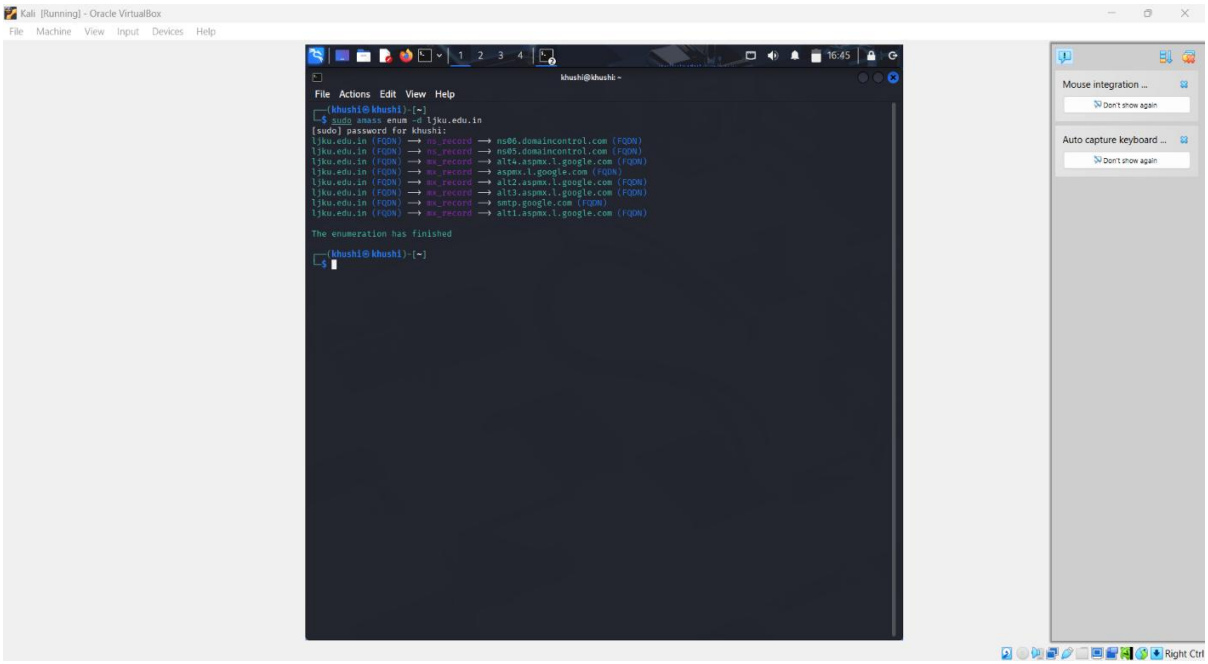
sublist3r Command Output:



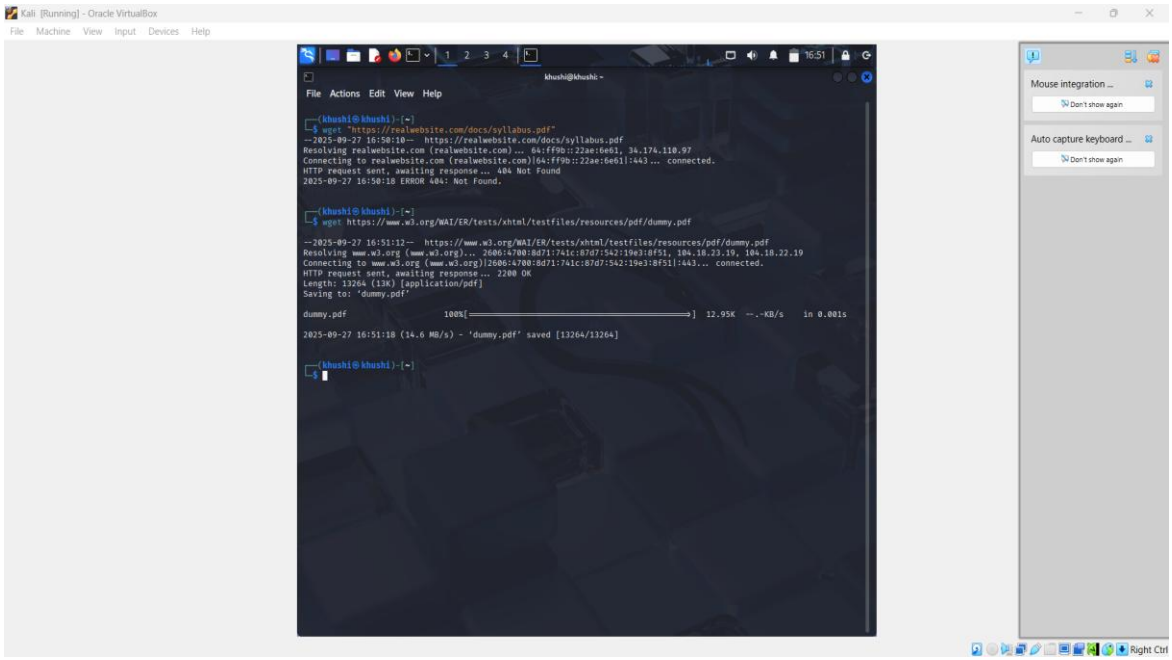
5) amass:



Amass Command Output :



6) Wget Command with Output:



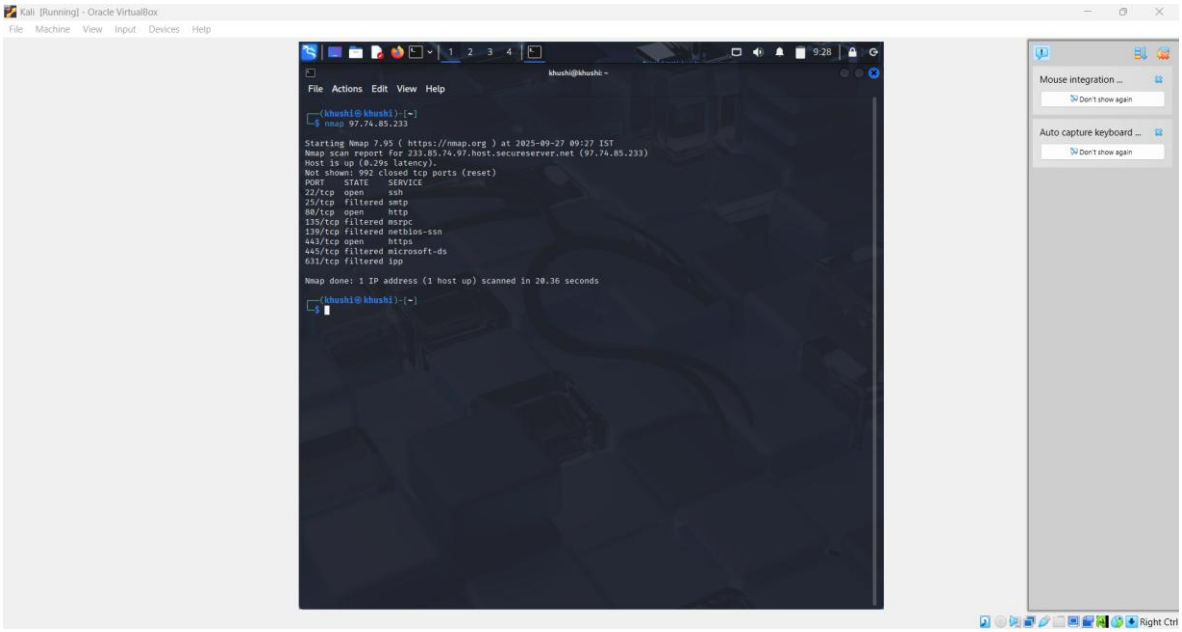
Practical-5

AIM:

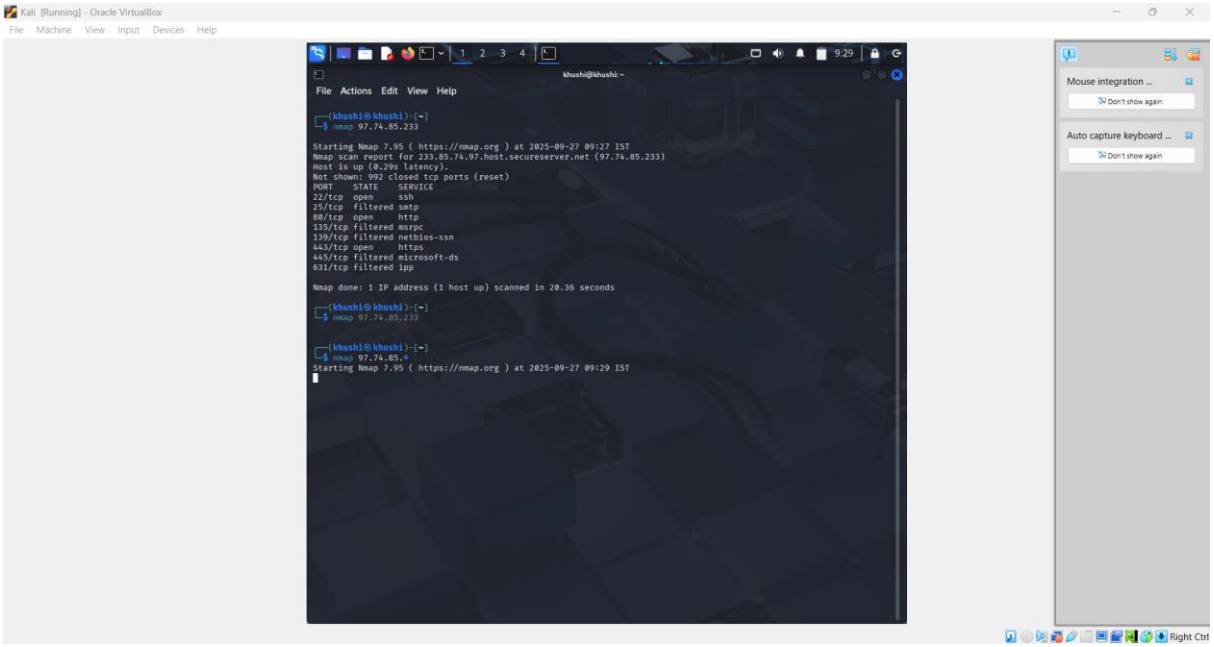
Execute a detailed Nmap scan to perform host discovery, detect open ports, determine operating systems, identify running services, and assess potential vulnerabilities on the target IP.

STEPS with screenshots:

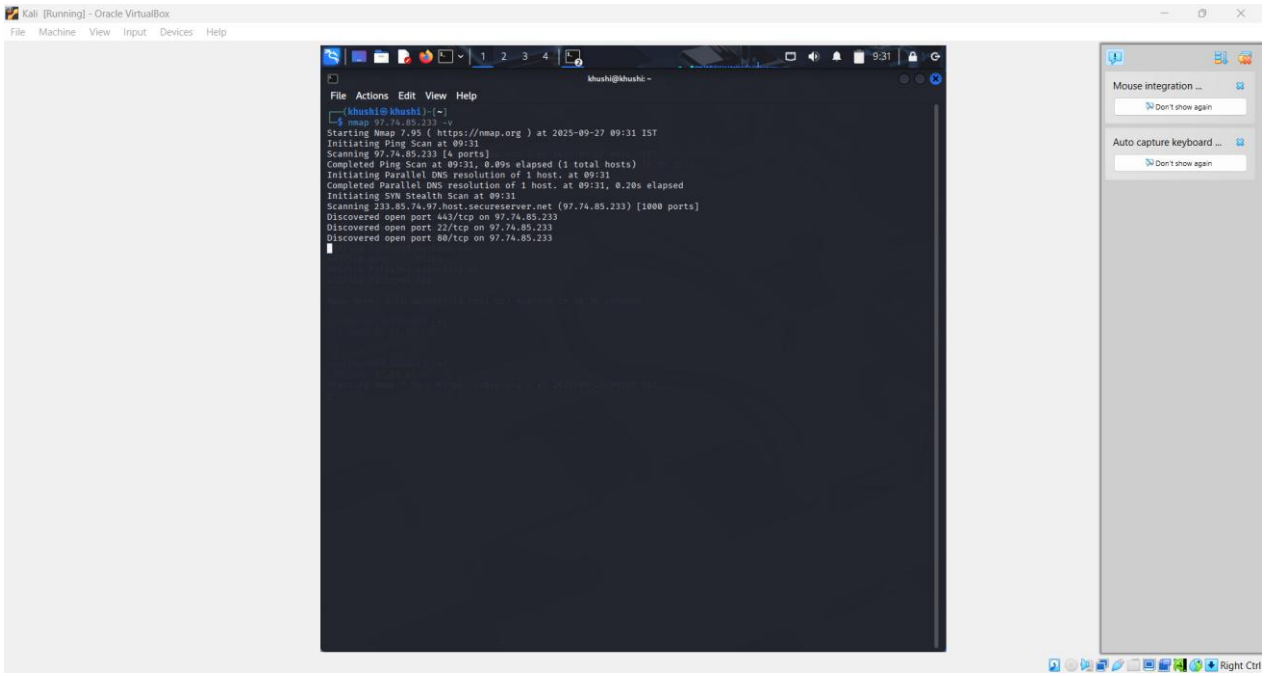
1) **Nmap :** Check if host is active and scan 1000 ports With Output



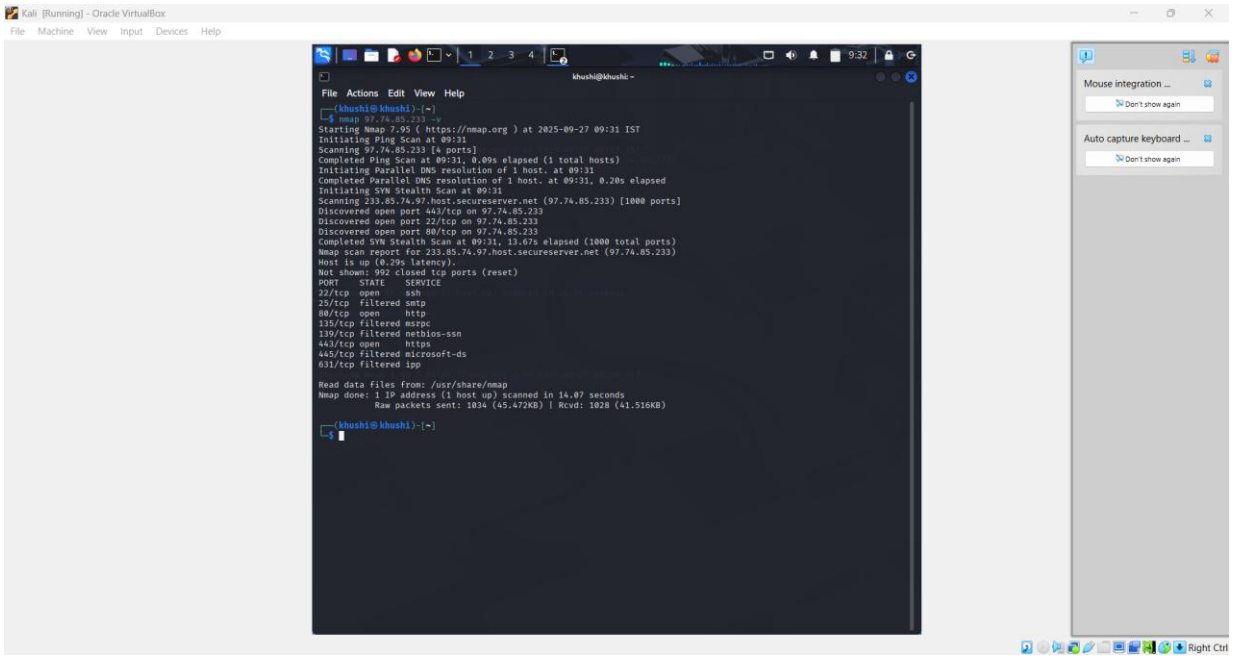
2) nmap x.x.x.*: Search for number of hosts in network.



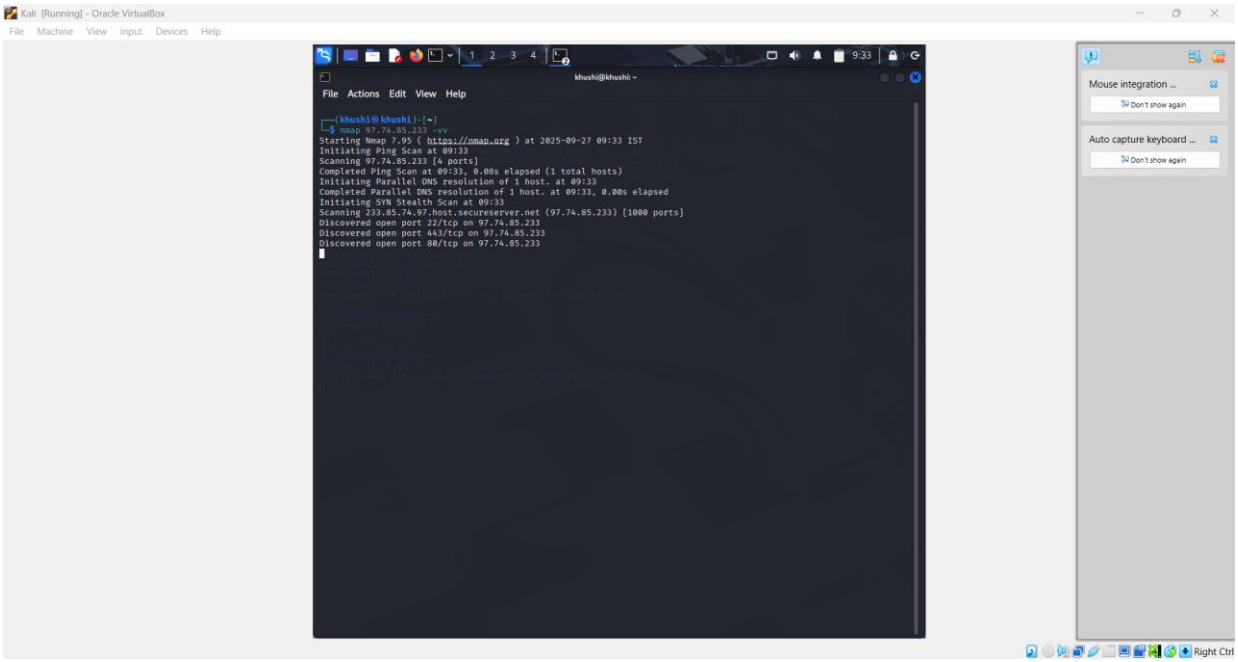
3) nmap -v <target>: Verbose scan, provides more details.



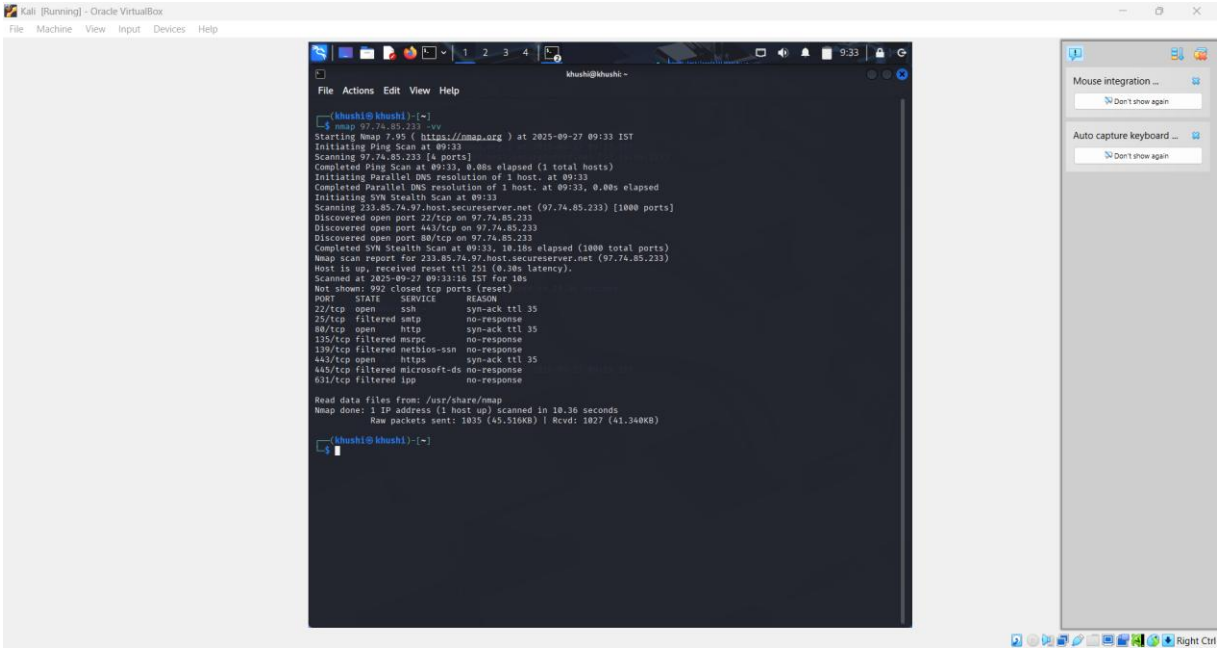
nmap -v <target> Command Output :



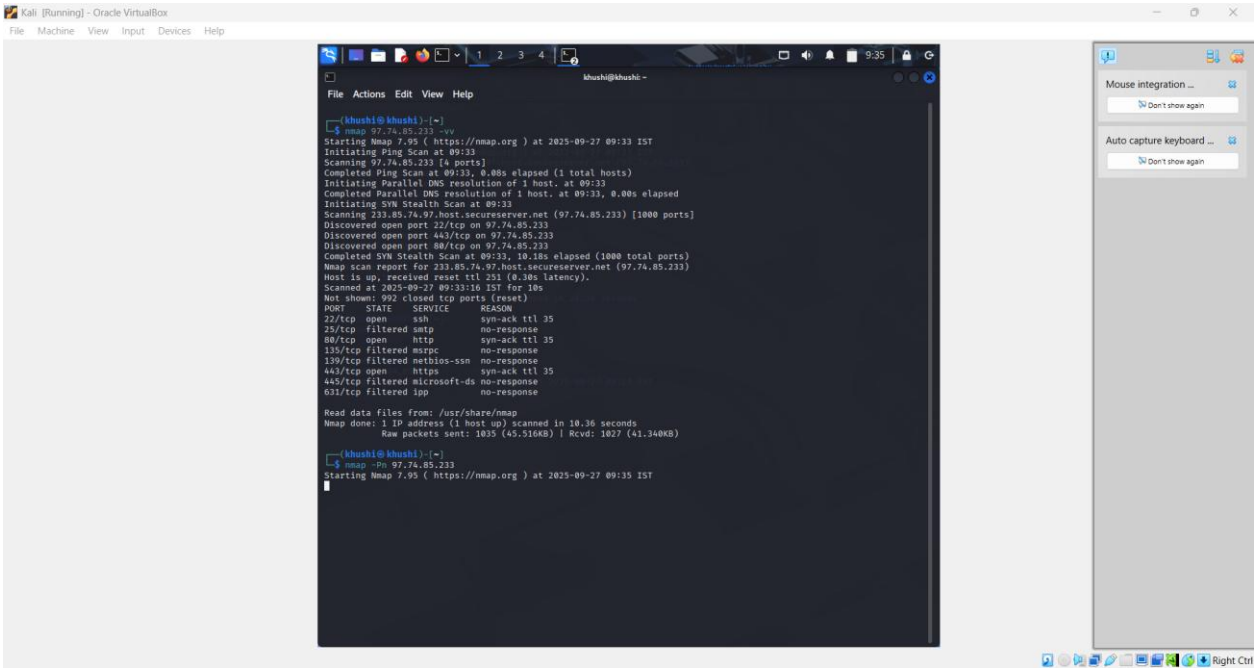
4) nmap -vv <target>: Very verbose scan, even more details.



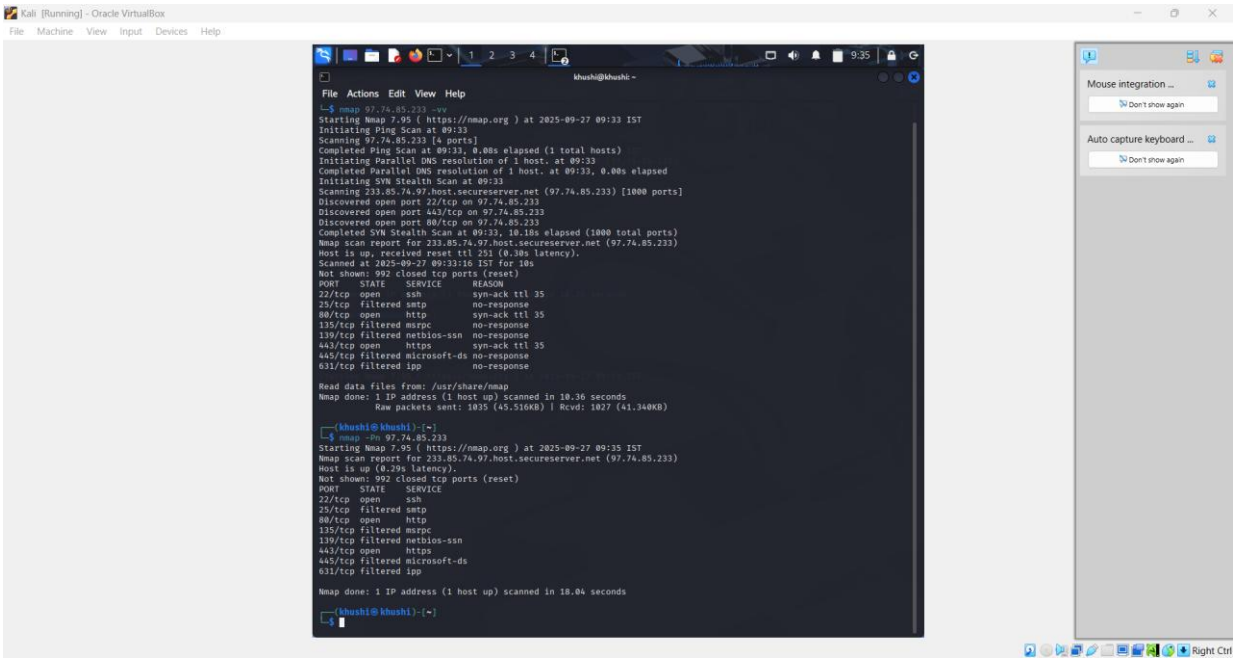
nmap -vv <target> command Output :



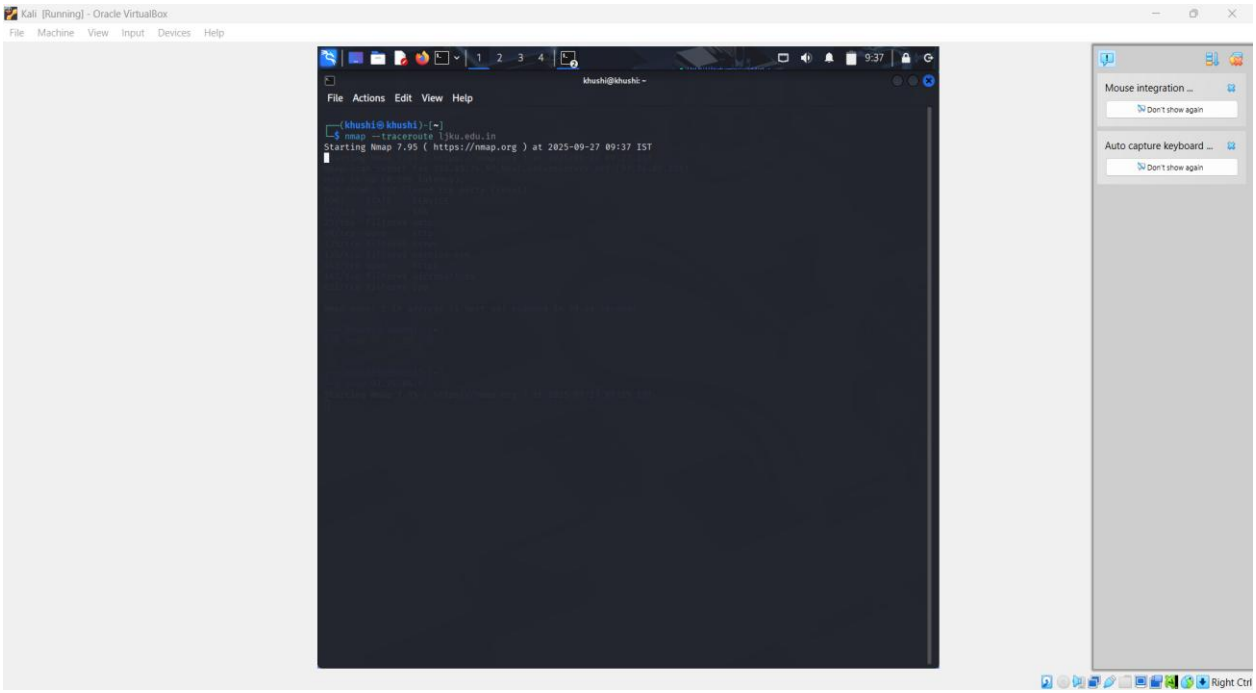
5) nmap -Pn <target> : Treat host as online, skip host discovery.



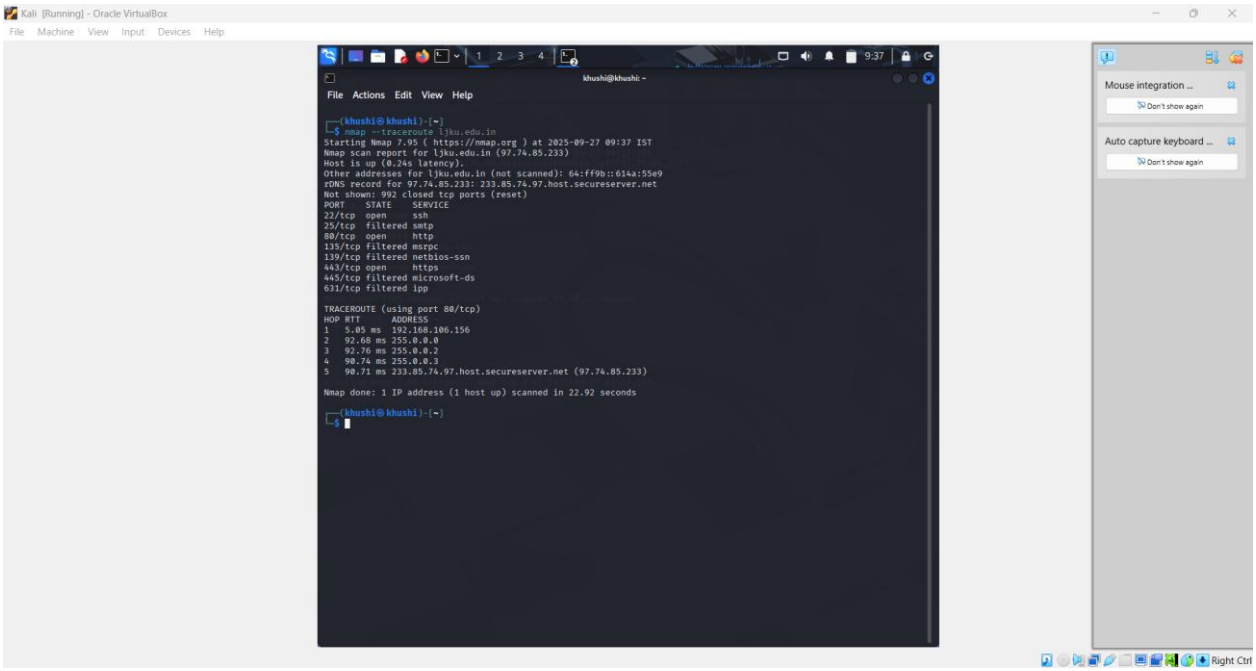
nmap -Pn <target> Command Output :



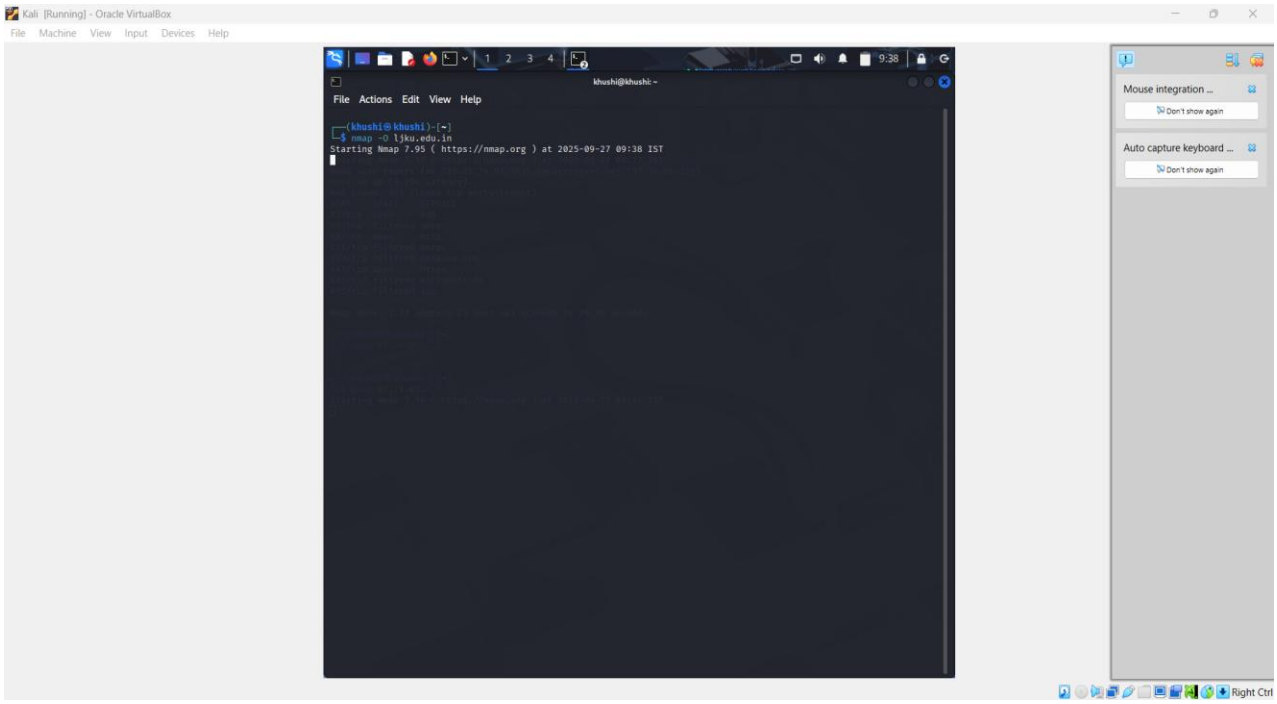
6) nmap --traceroute <target>: Perform traceroute after the scan.



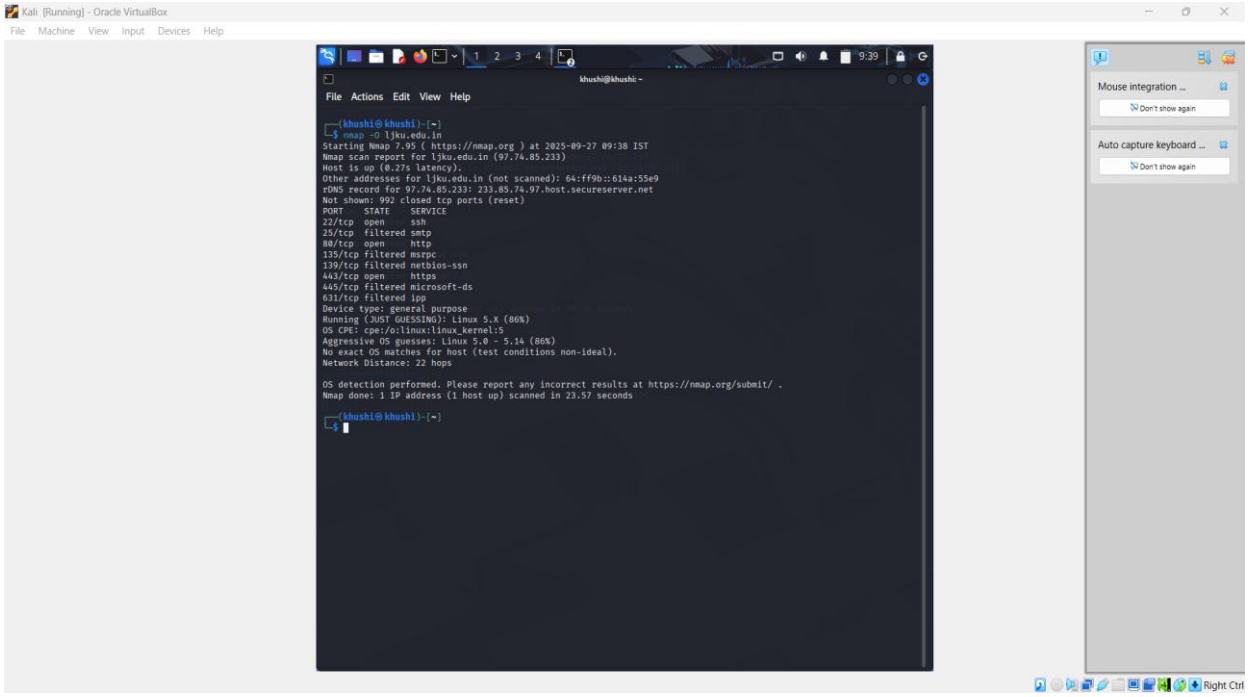
nmap --traceroute <target> Command Output :



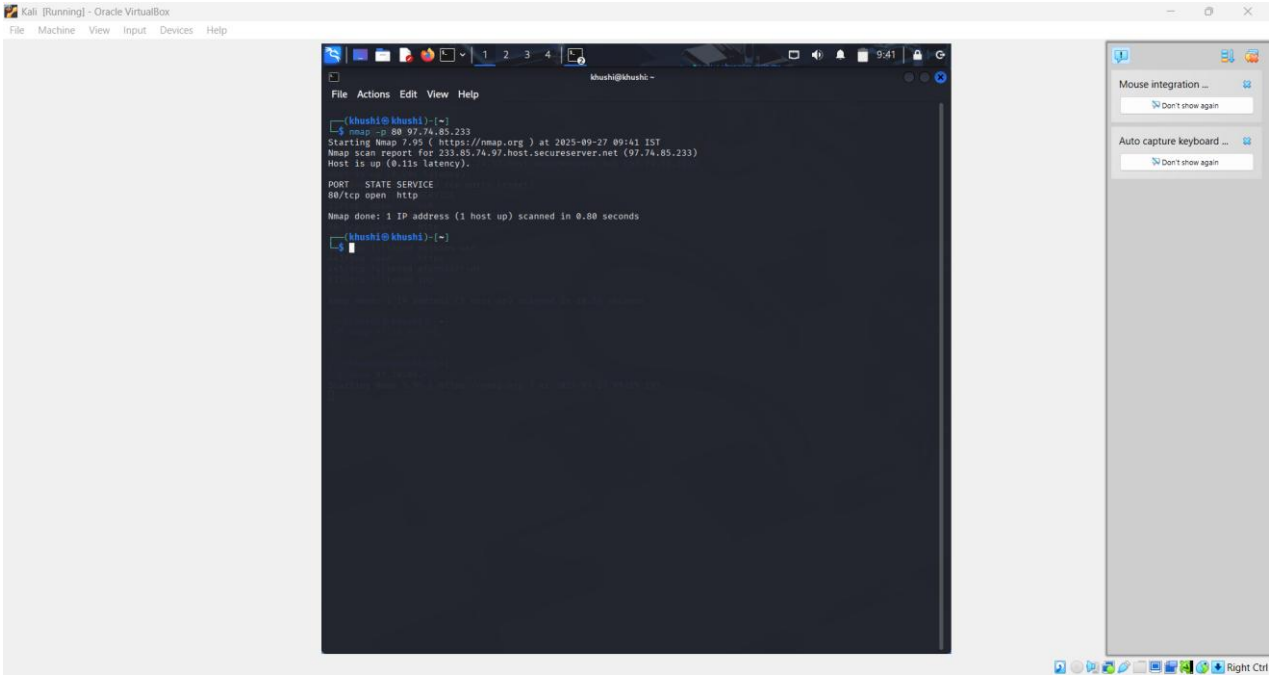
7) nmap -O <target> : OS detection scan.



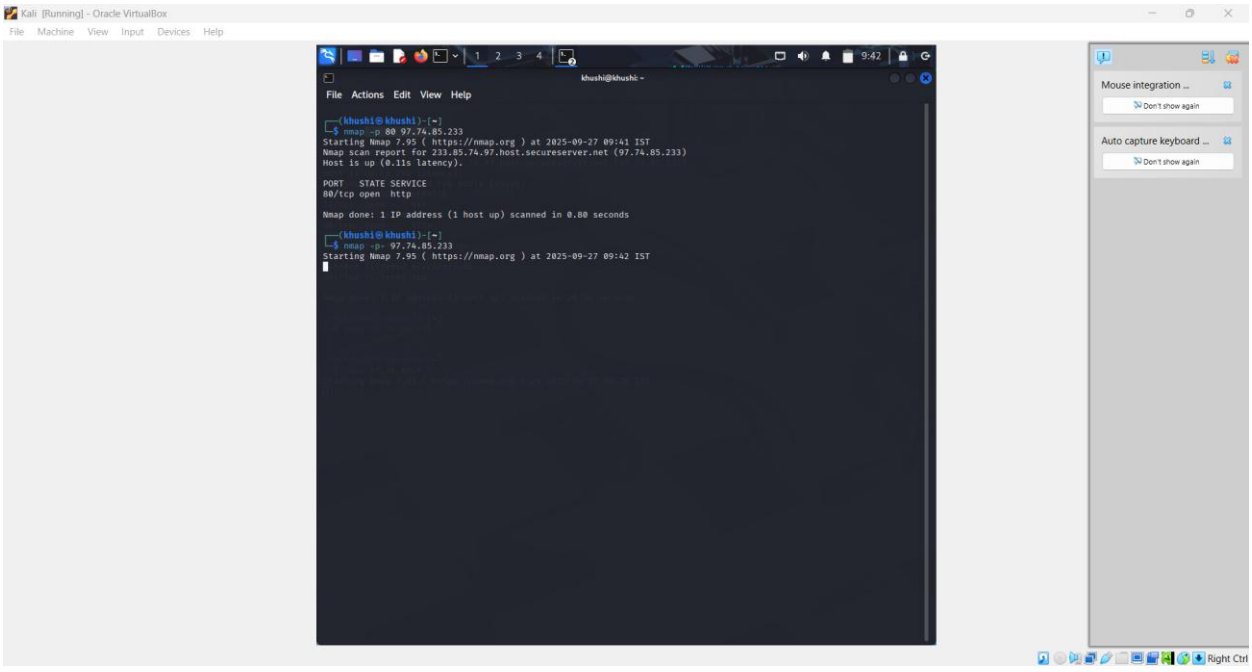
nmap -O <target> Command Output :



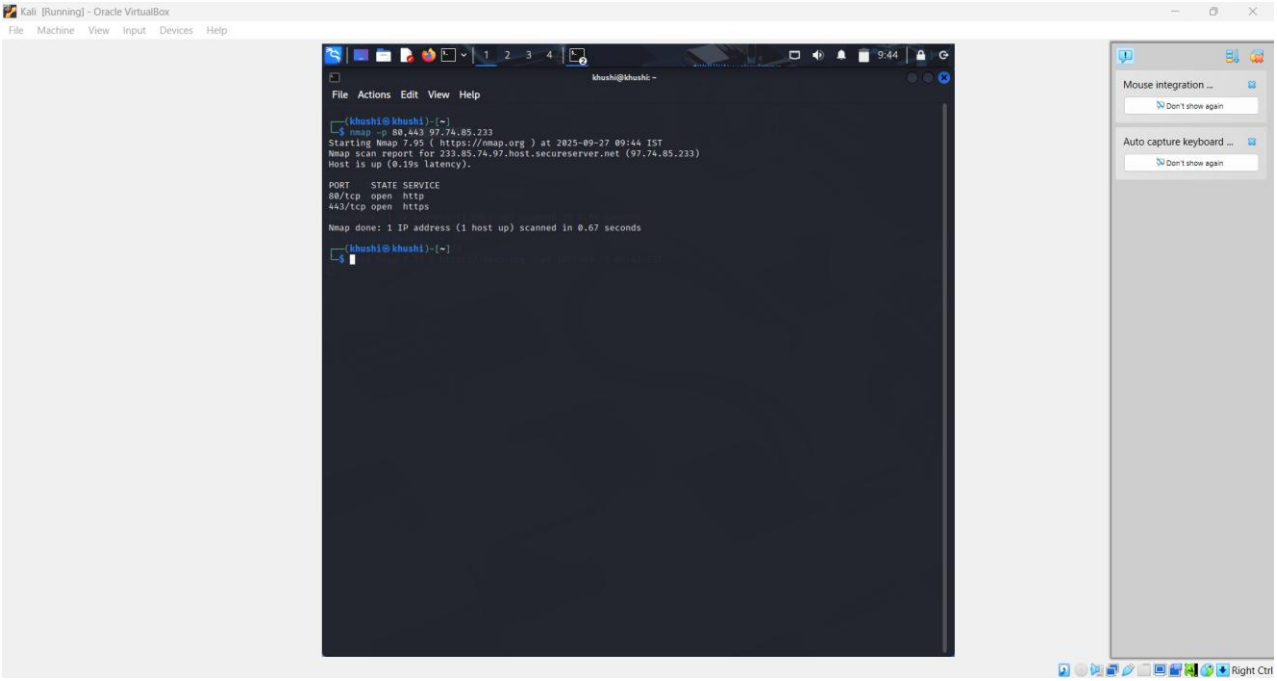
8) nmap -p <port> <target> With Output : Scan specific port(s).



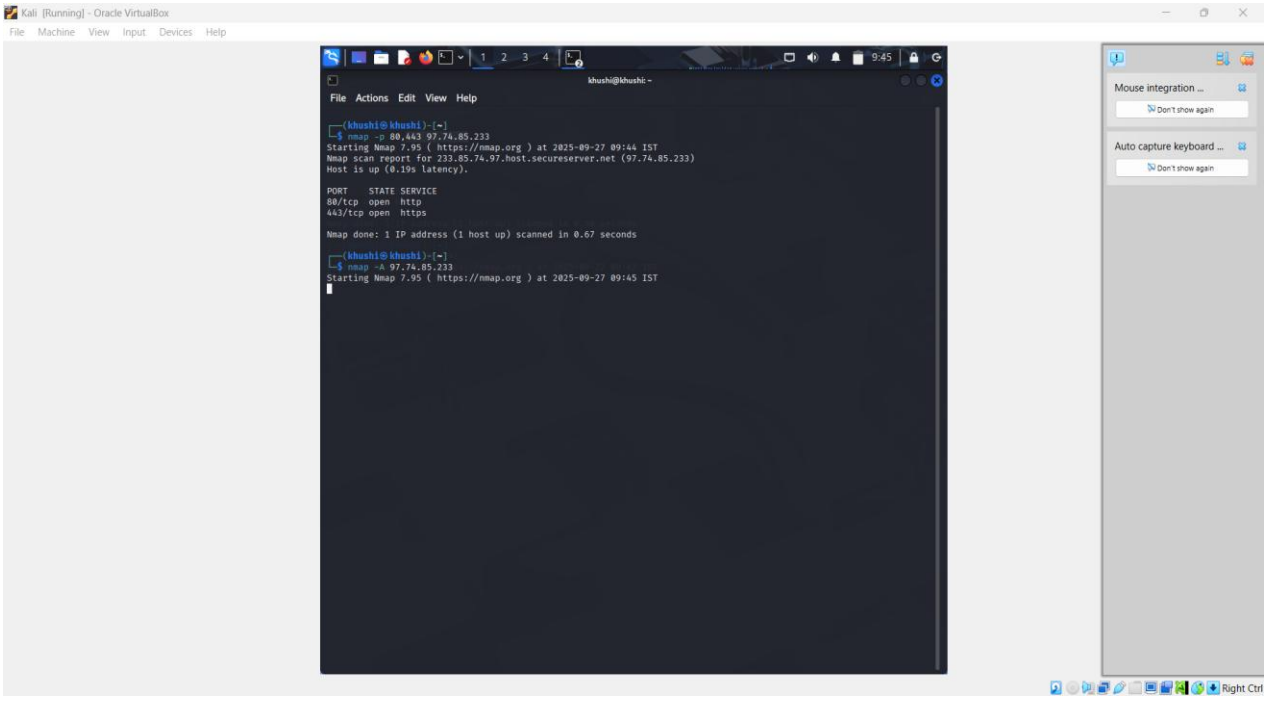
9) nmap -p- <target> : Scan all ports (0-65535).



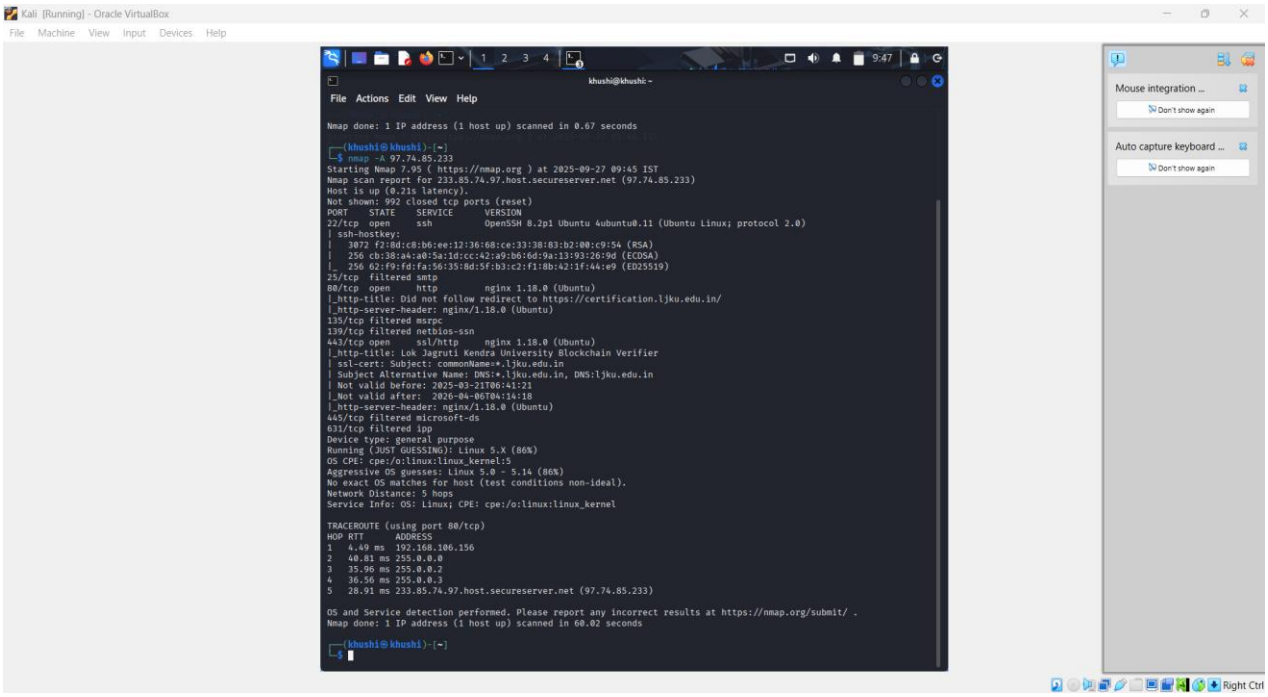
10) nmap -p 80,443 <target> With Output : Scan specific ports (e.g., 80, 443).



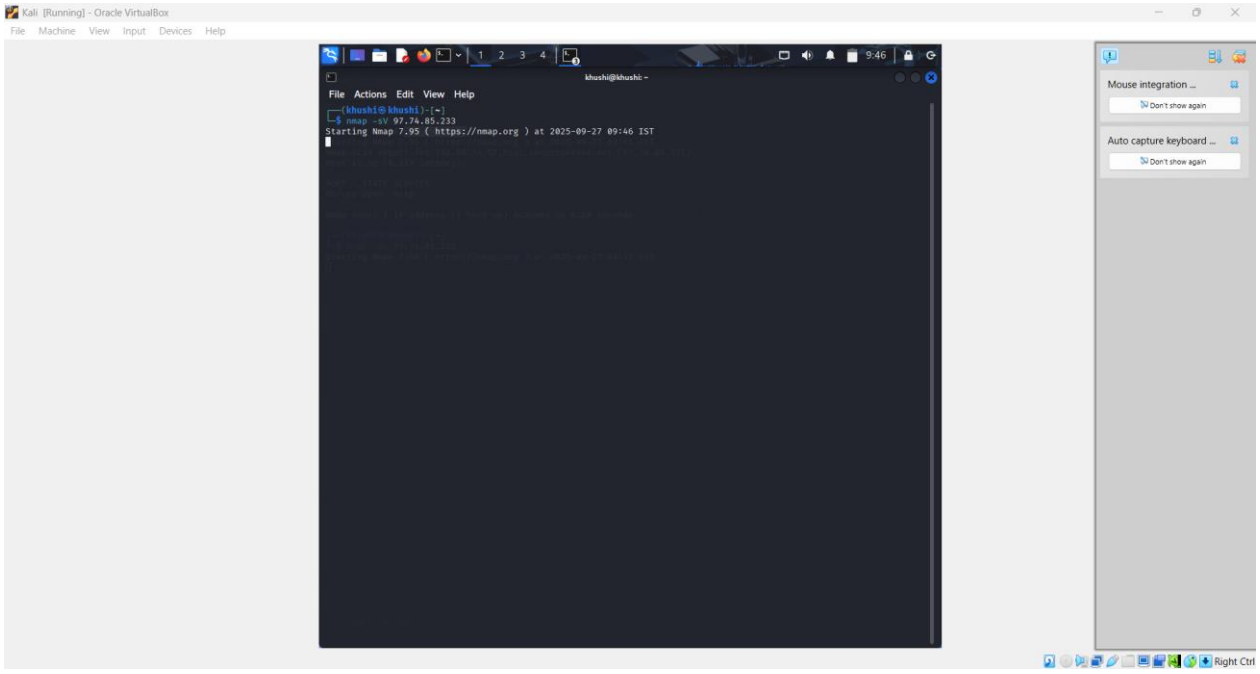
11) nmap -A <target>: Comprehensive scan (OS detection, version detection, script scanning, and traceroute).



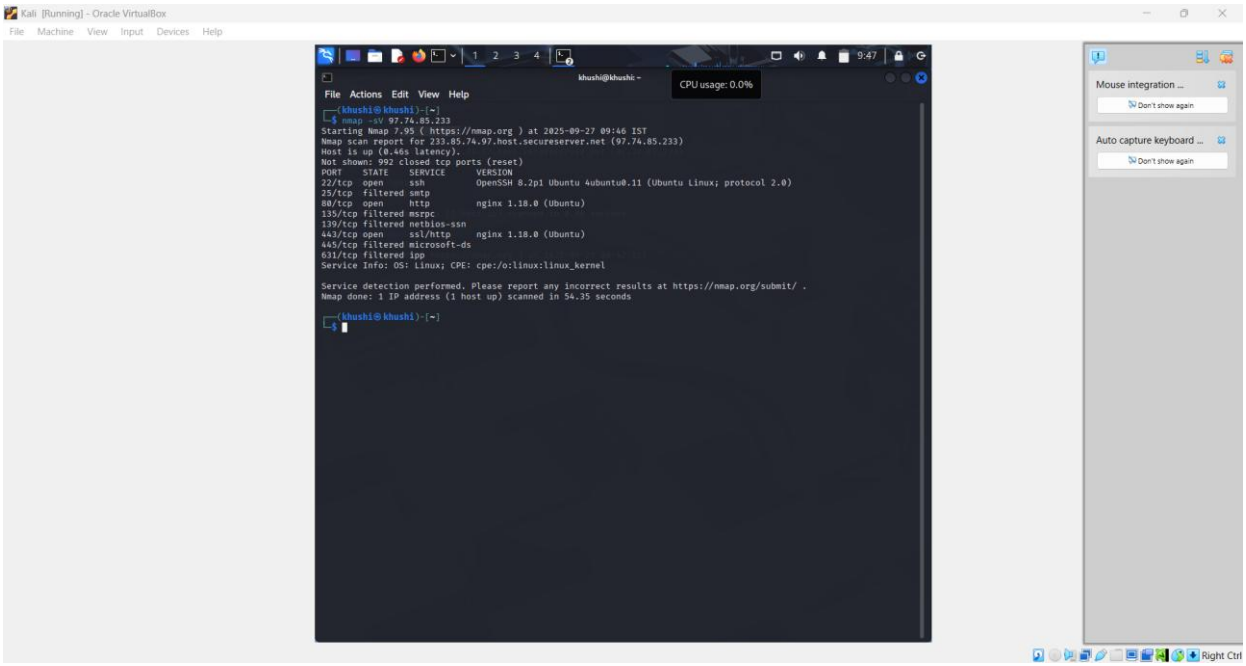
nmap -A <target> Command Output :



12) nmap -sV <target> : Version detection scan.



nmap -sV <target> Command Output :



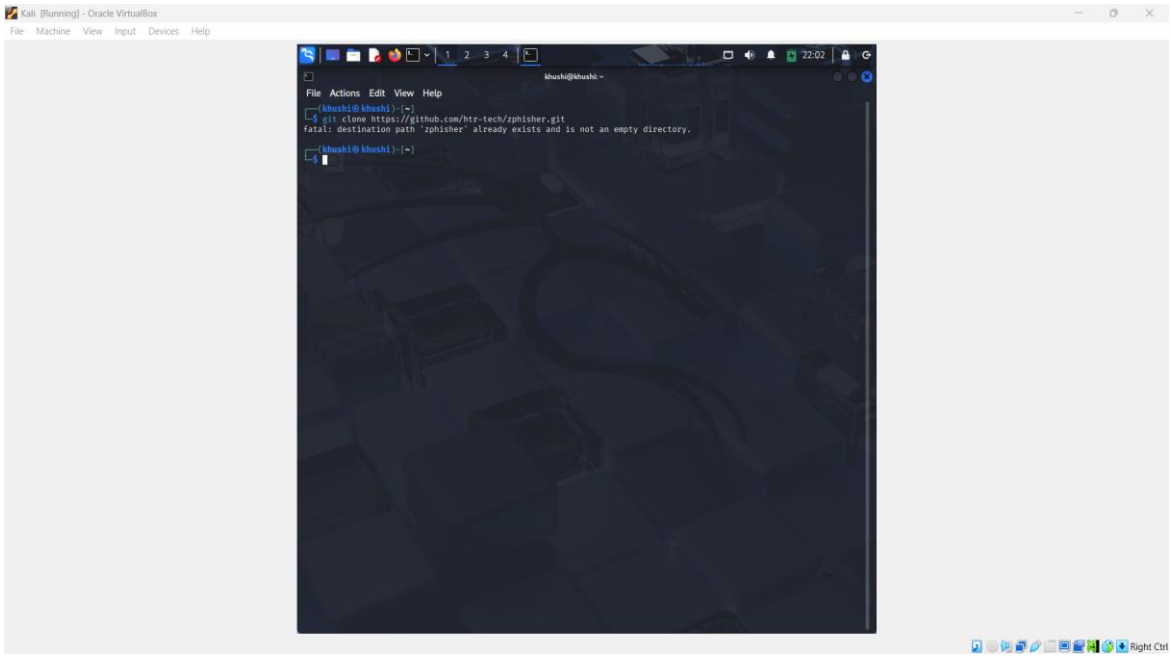
Practical-6

AIM:

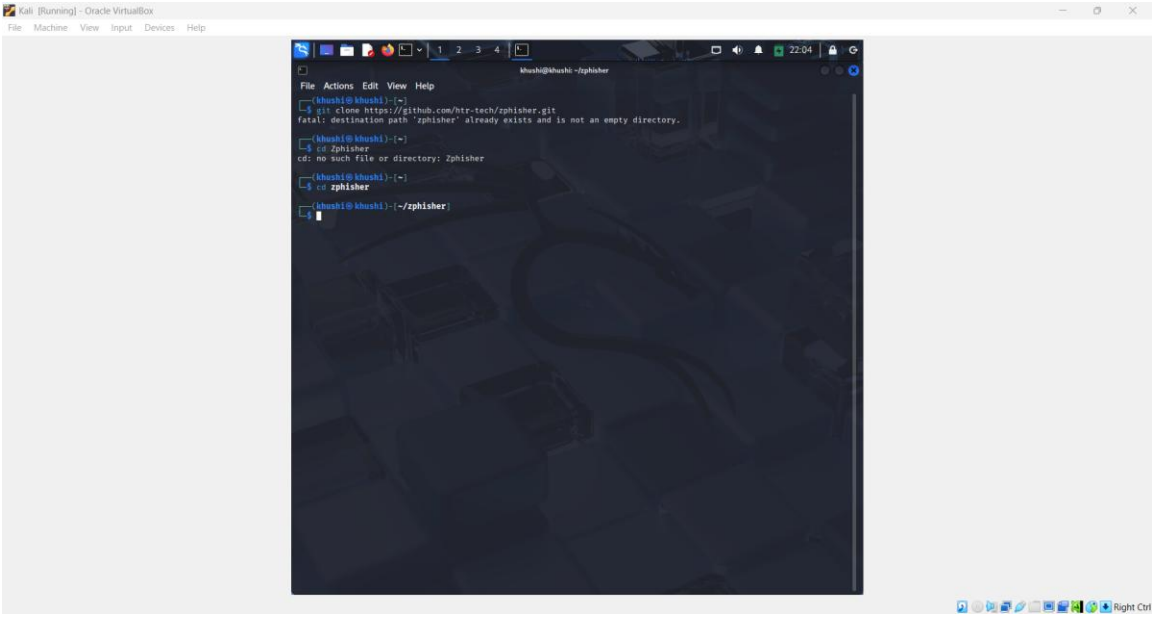
Demonstrate credential harvesting through social engineering by creating phishing pages using Zphisher, showing how attackers can exploit user trust on social media platforms.

STEPS with screenshots:

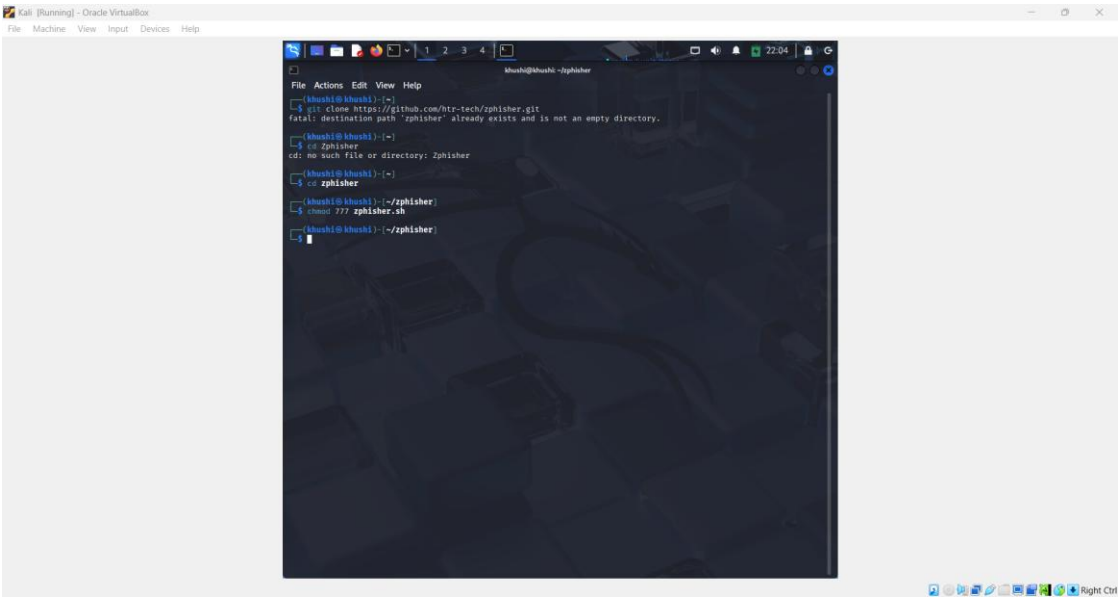
1) Git clone though add zphiser:



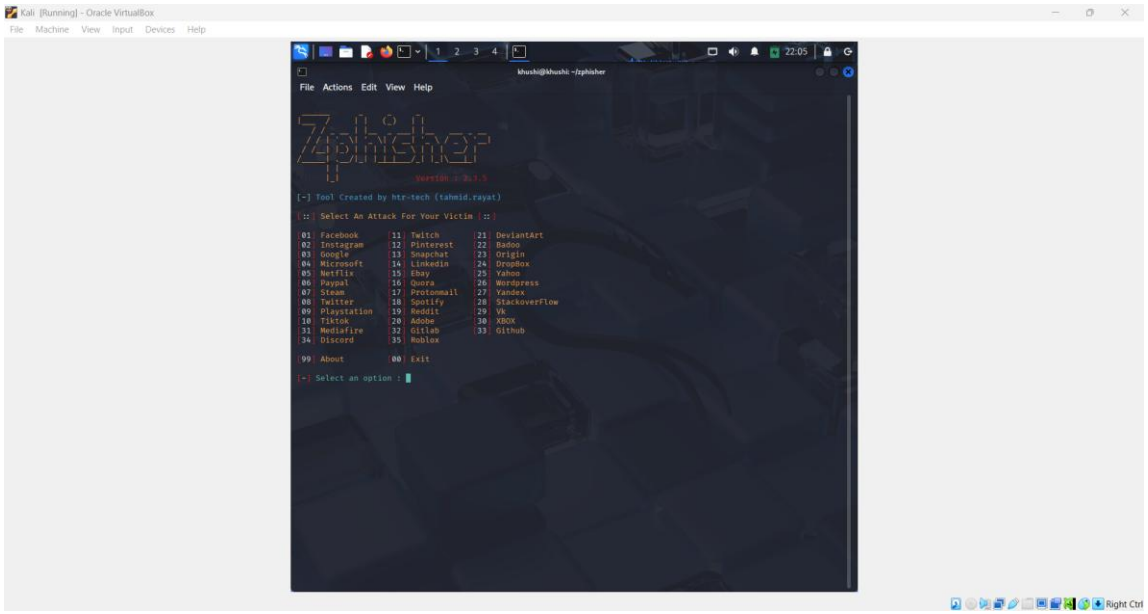
2) Redirect zphisher:



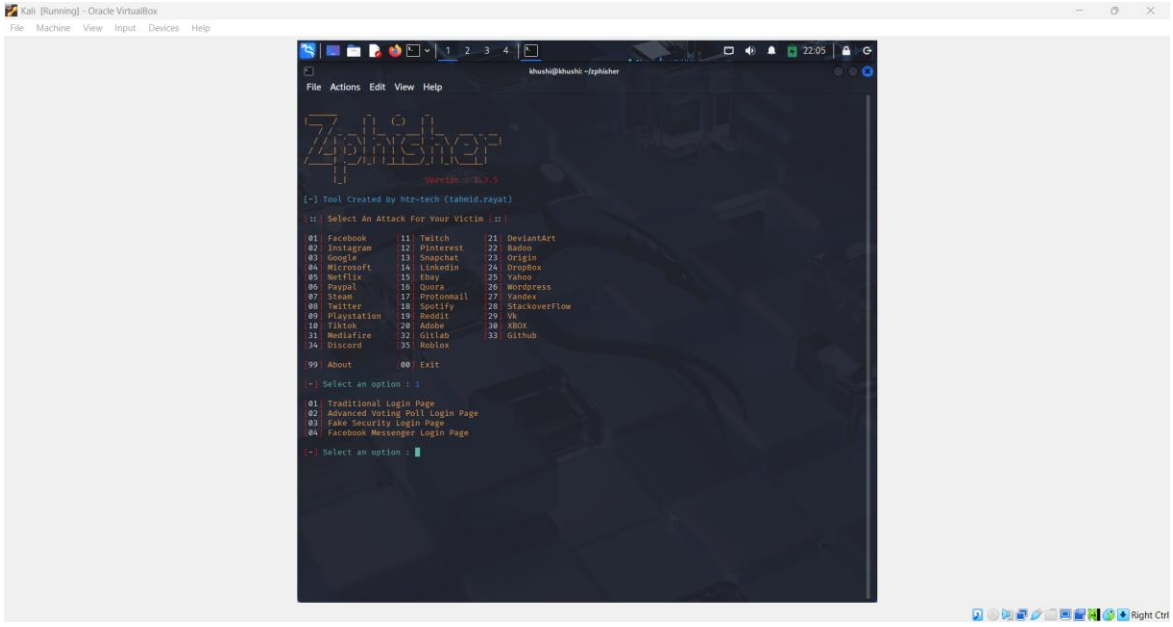
3) Chmod 777 zphisher.sh:



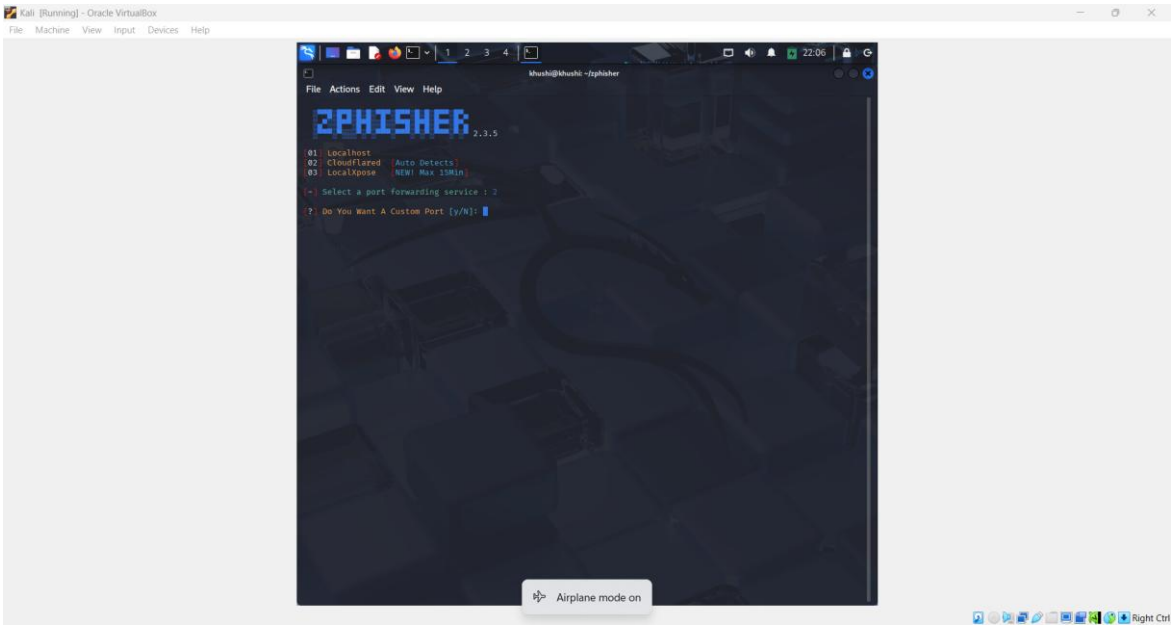
4) Select option :



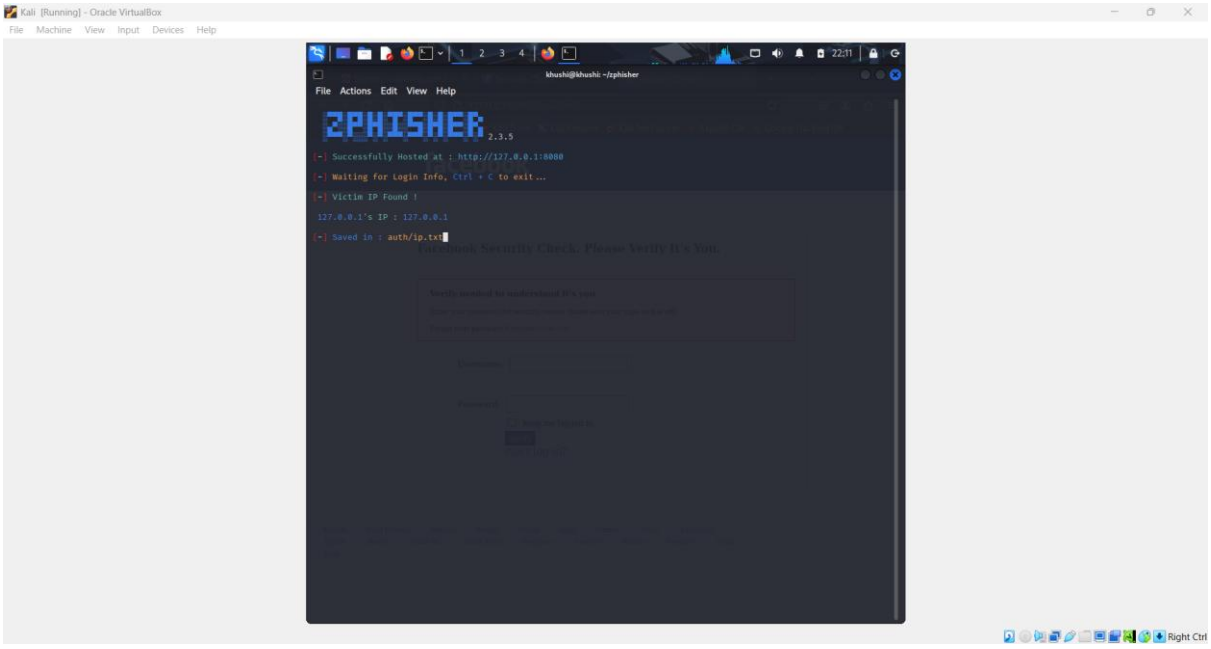
5) Select Option 1:



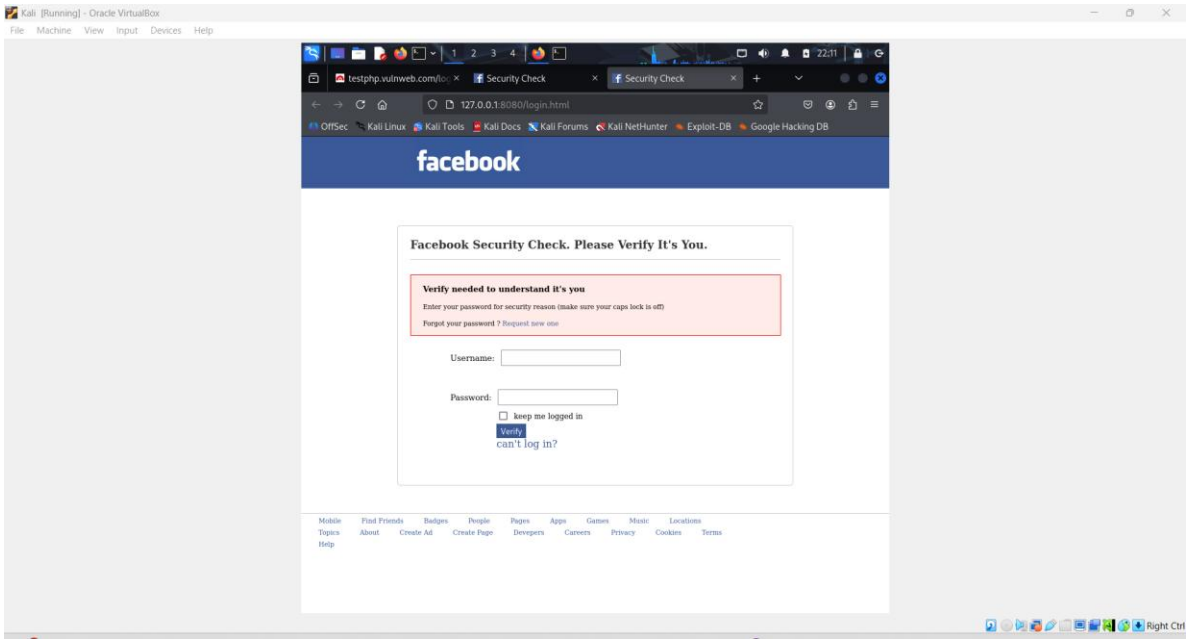
6) Select a Custom Port:



6) Start a zphisher:



7) Open a Facebook Login page:



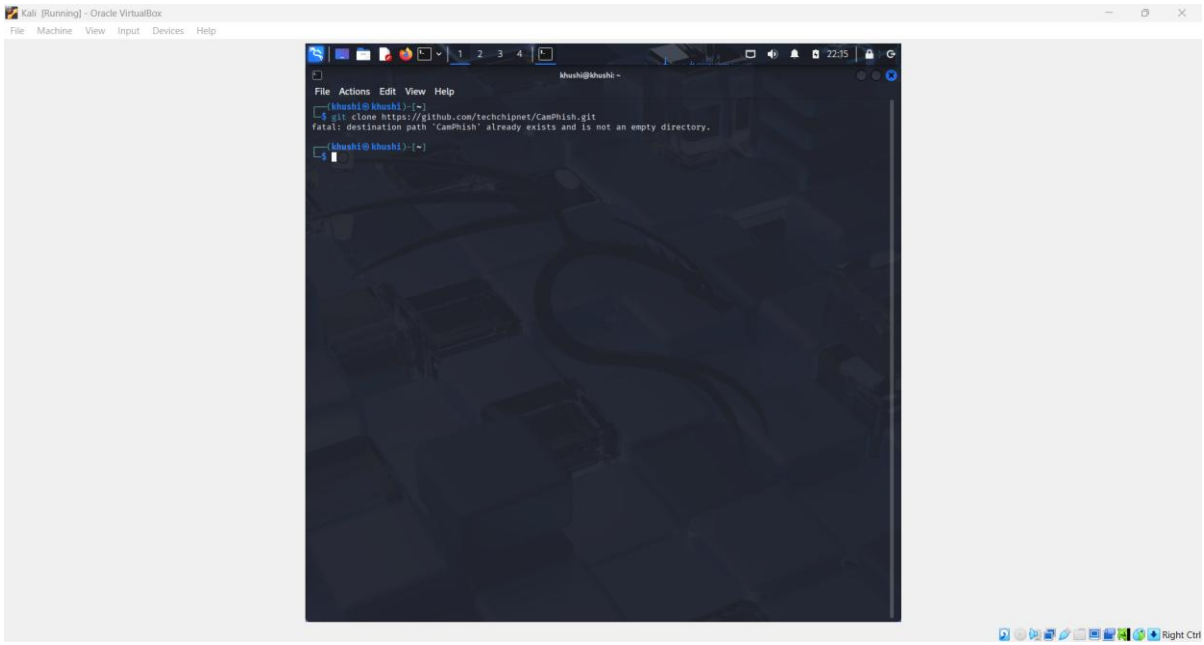
Practical-7

AIM:

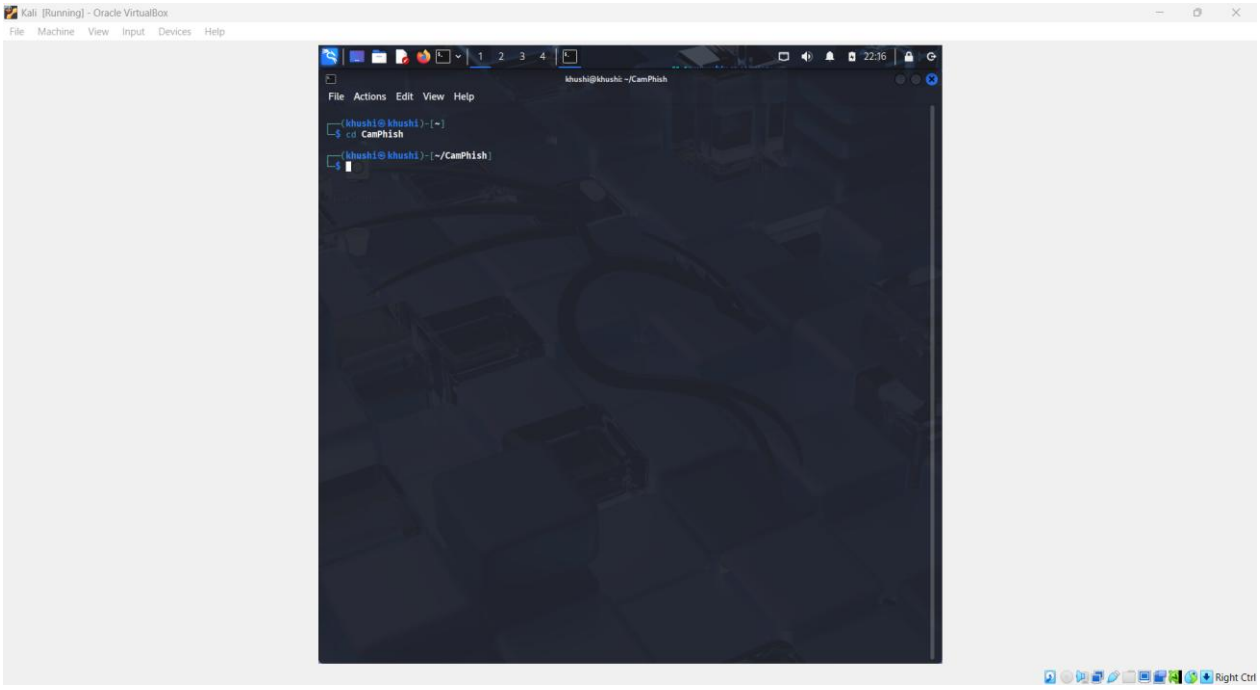
Simulate unauthorized access to a target device's camera using CamPhish through social engineering techniques to understand risks associated with malicious camera exploitation.

STEPS with screenshots:

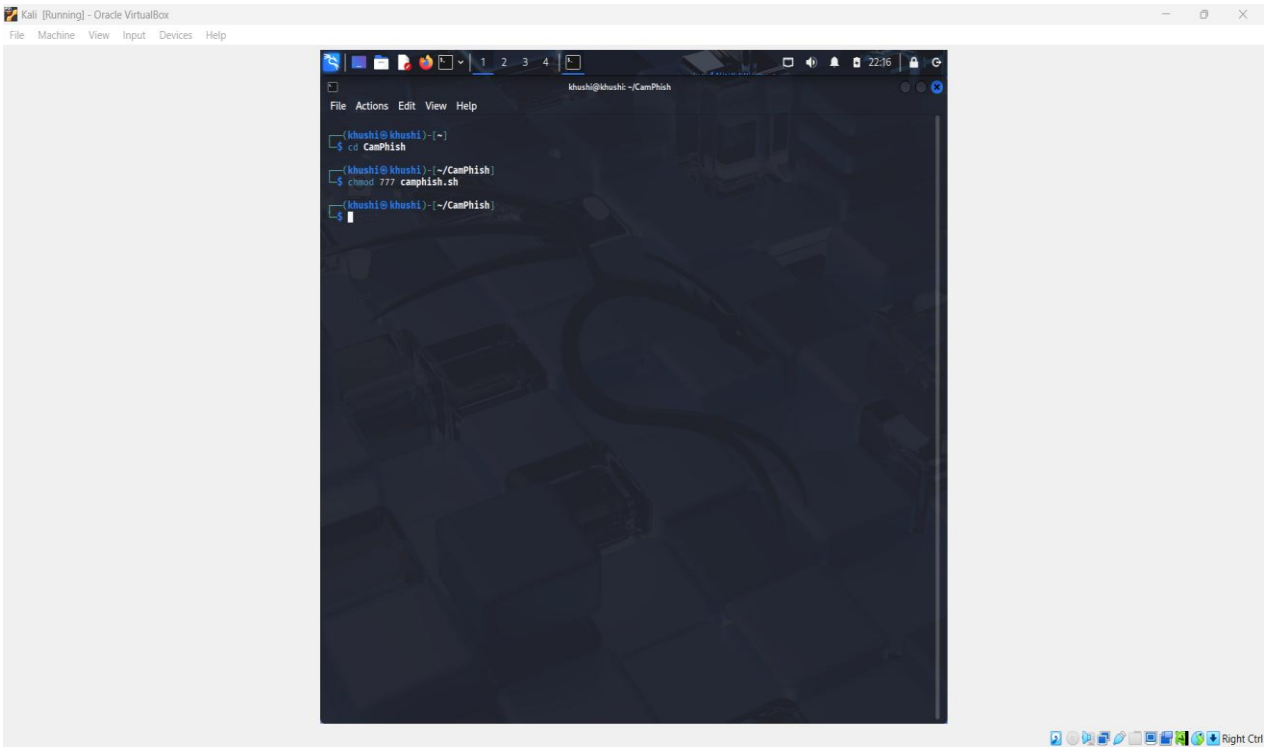
1) Git clone though add CamPhish:



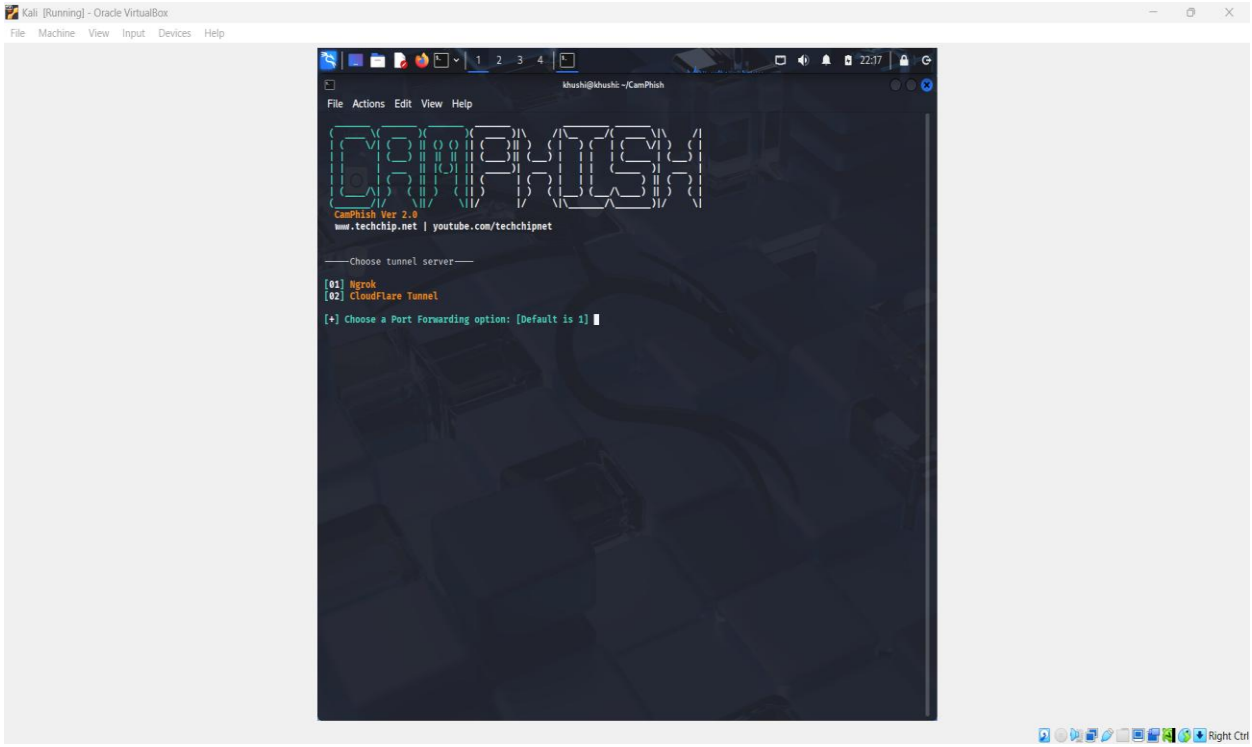
2) Redirect CamPhish:



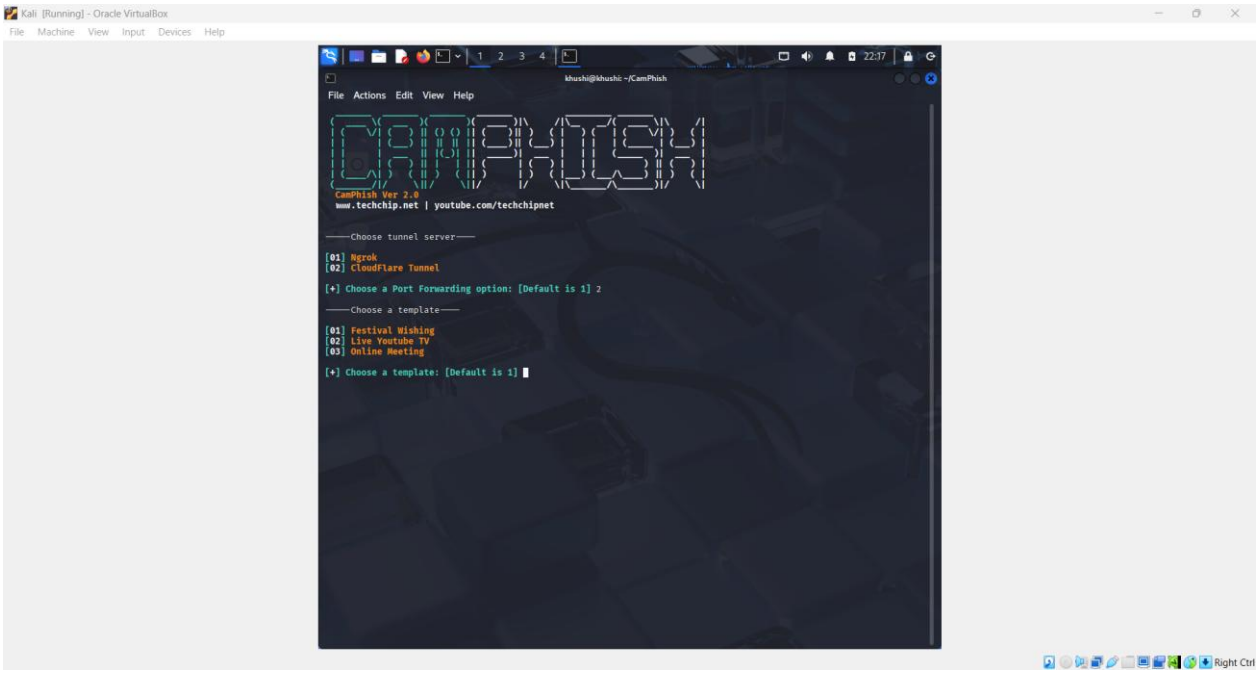
3) chmod 777 camphish.sh:



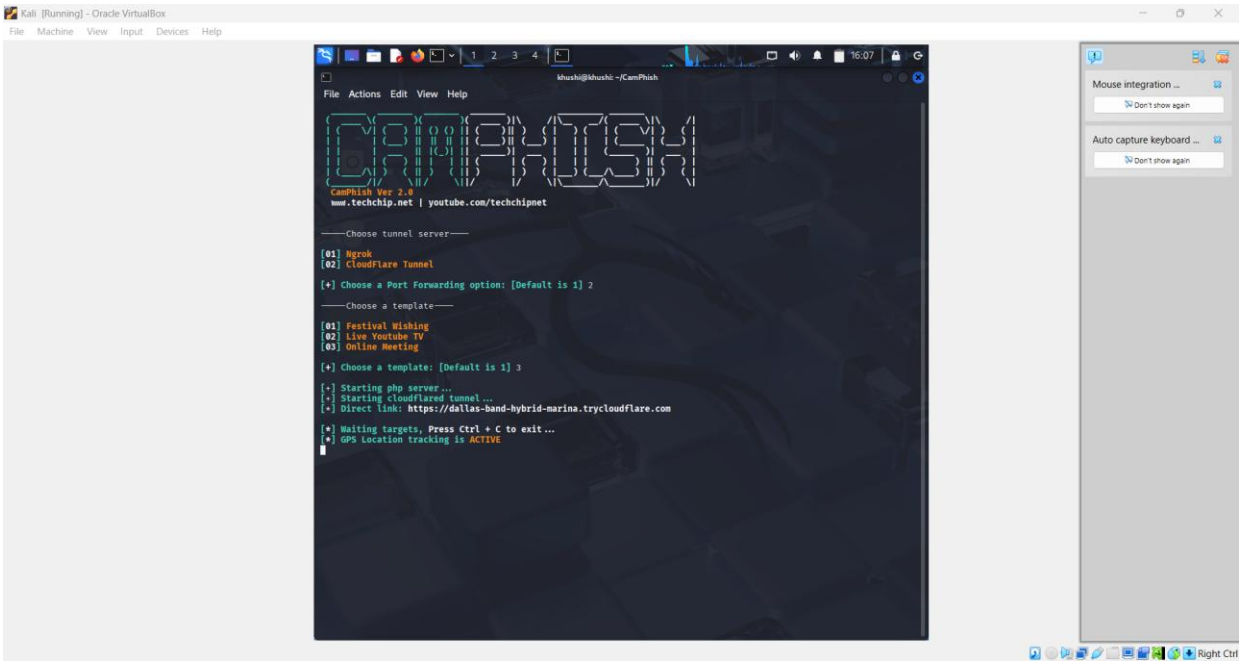
4) Select a Option:



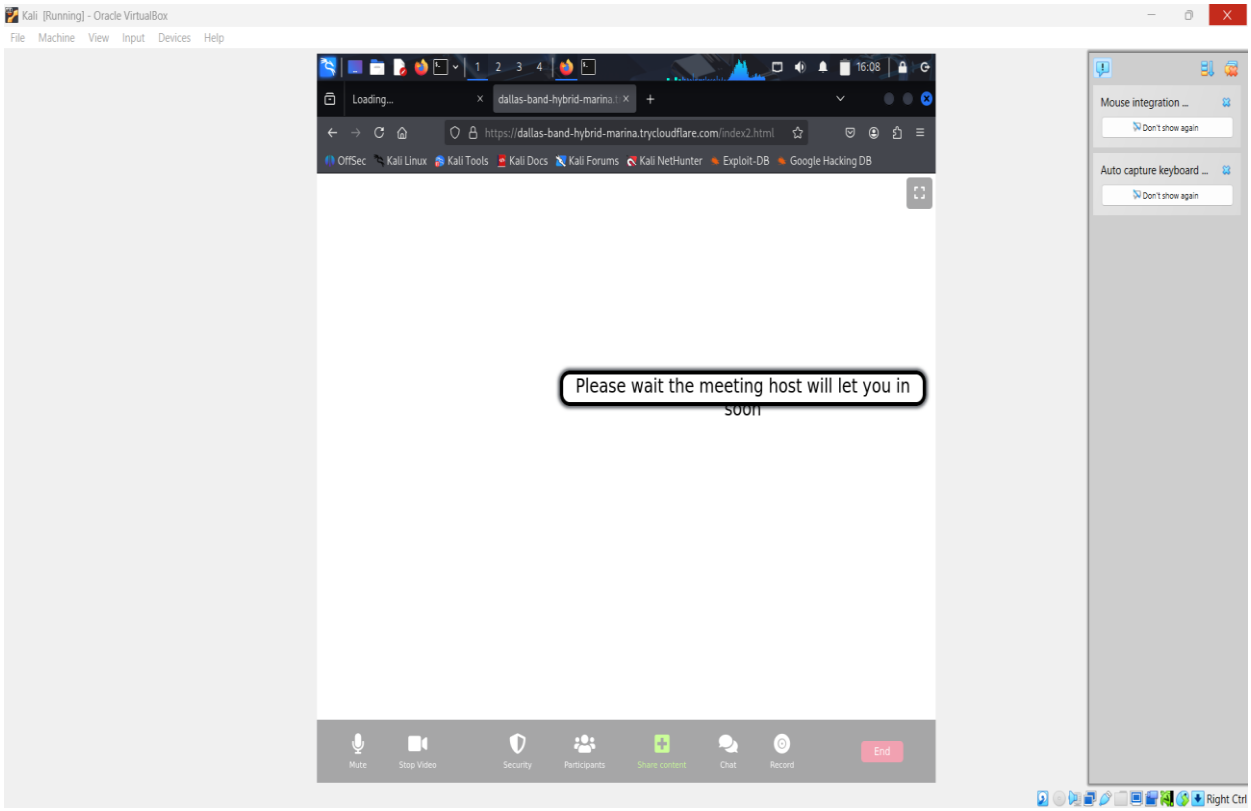
5) Select a Option :



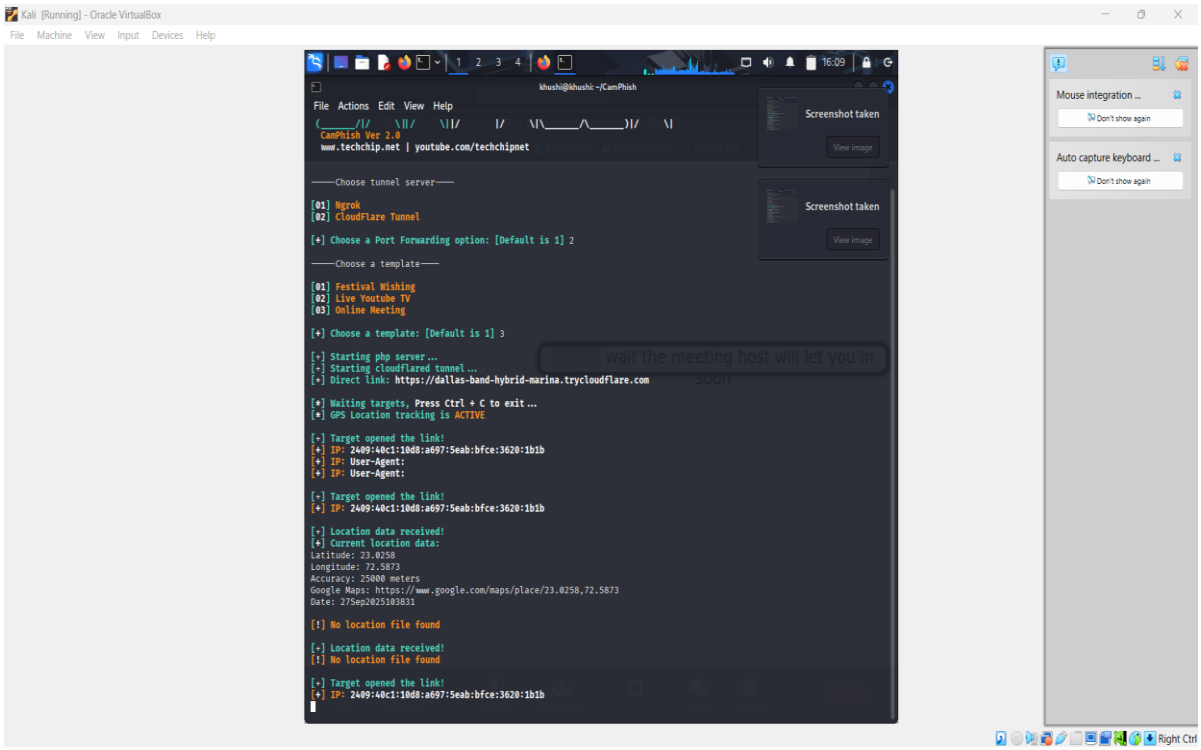
6) Started a Attack:



7) Click a Link Now start a attack:



8) Start a Camera access :



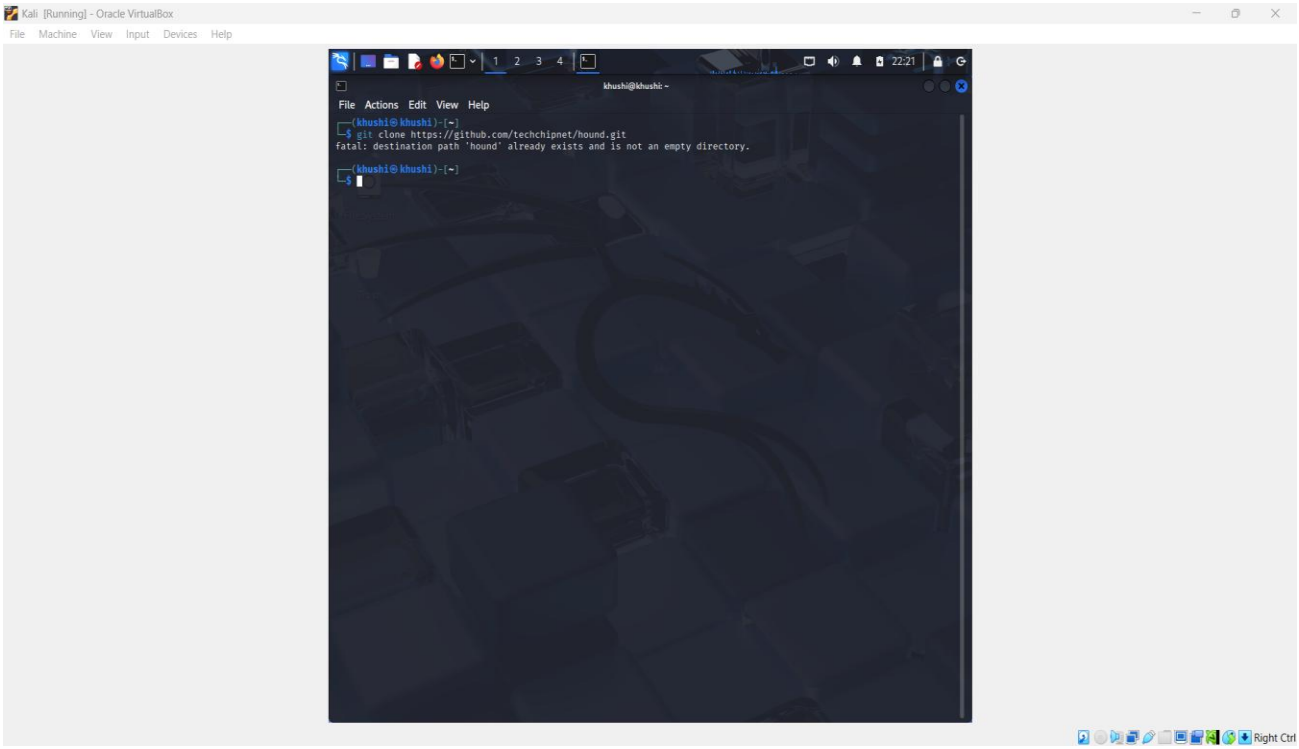
Practical-8

AIM:

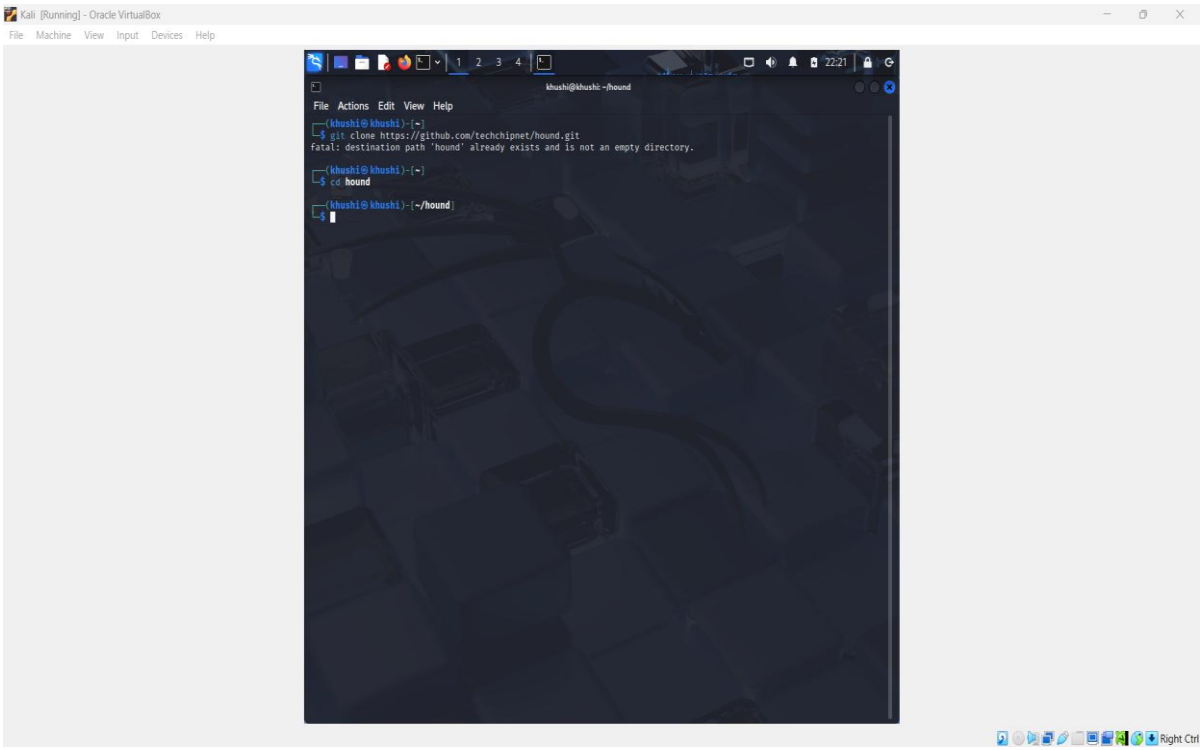
Identify and track the precise geographical location of a target device or individual using the Hound tool to demonstrate location-based information gathering.

STEPS with screenshots:

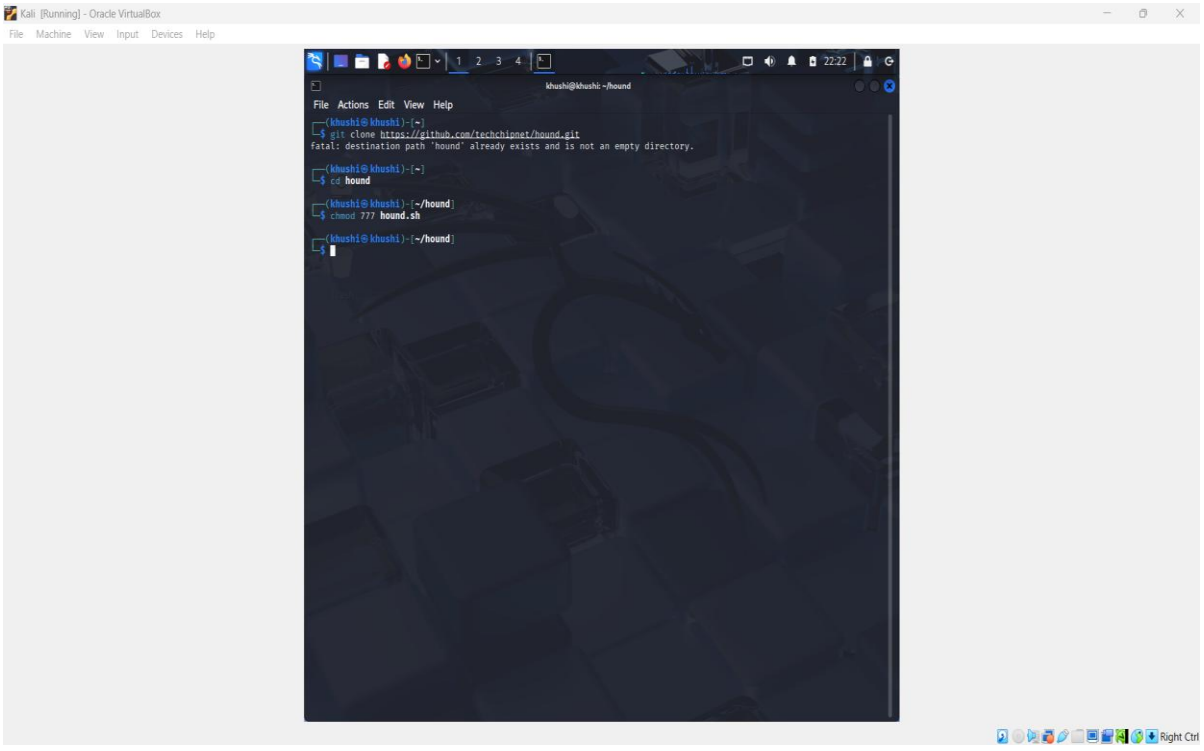
1) Git clone though add Hound:



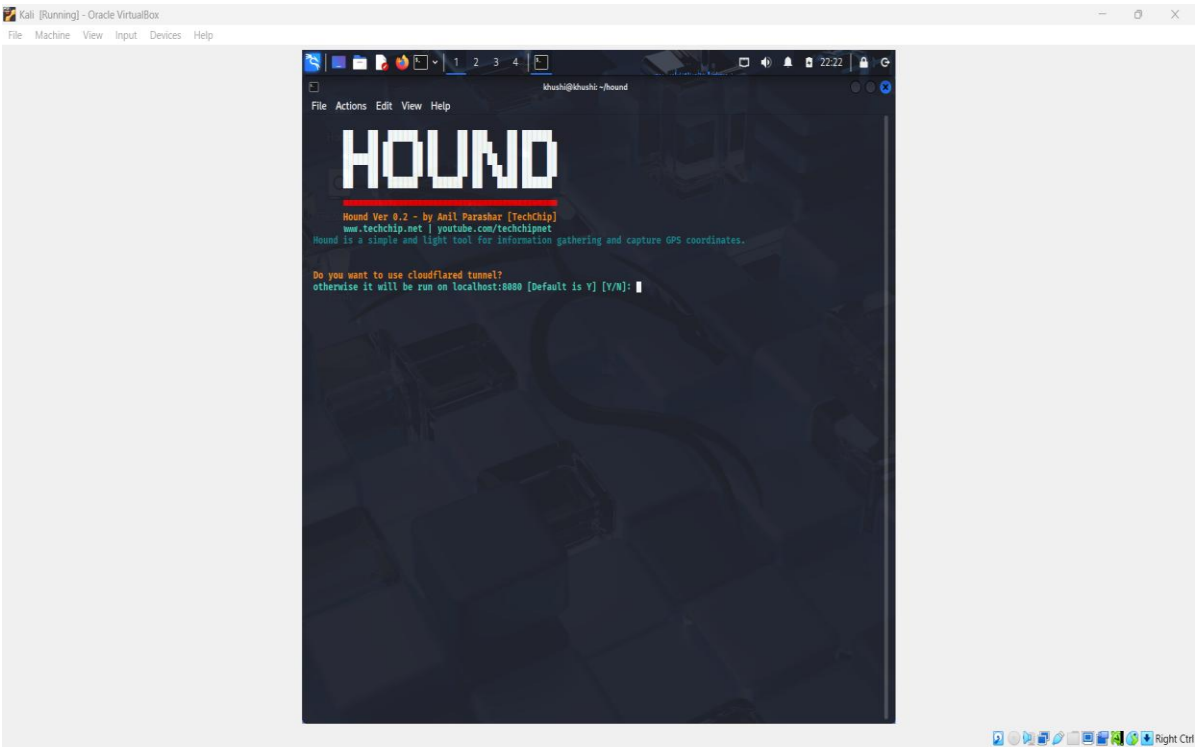
2) Redirect Hound:



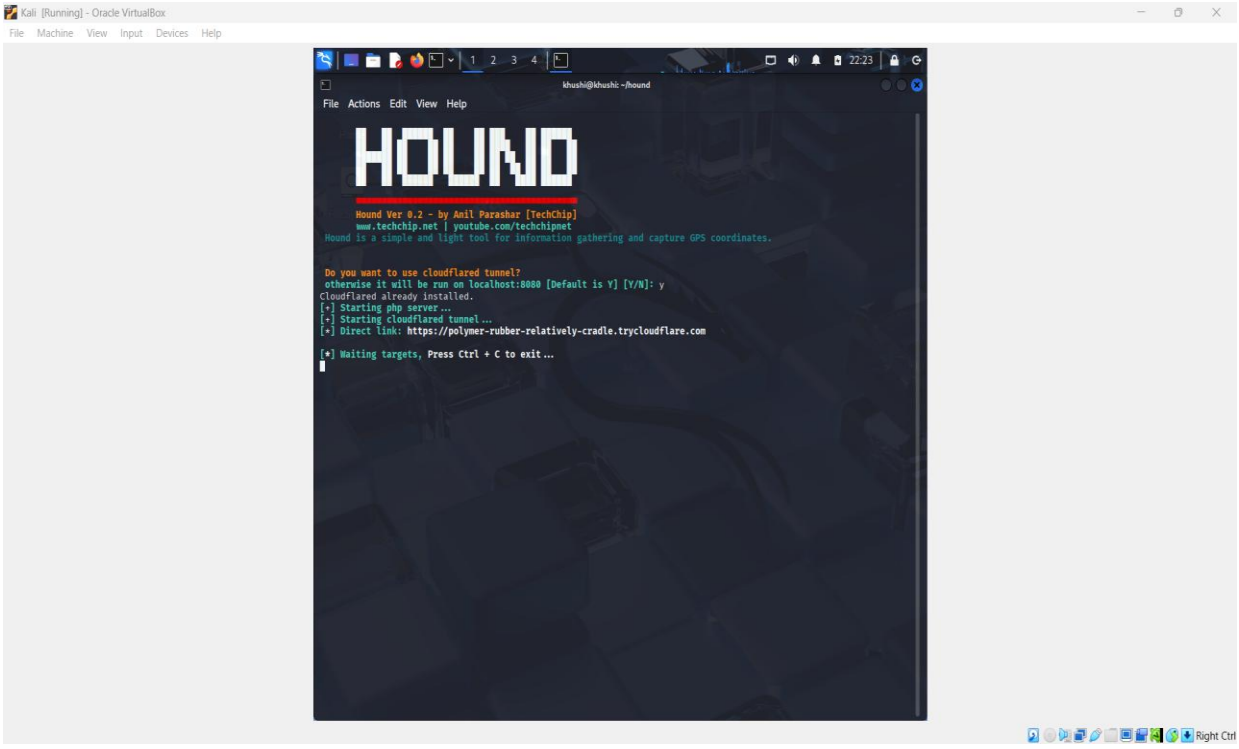
3) Chmod 777 hound.sh:



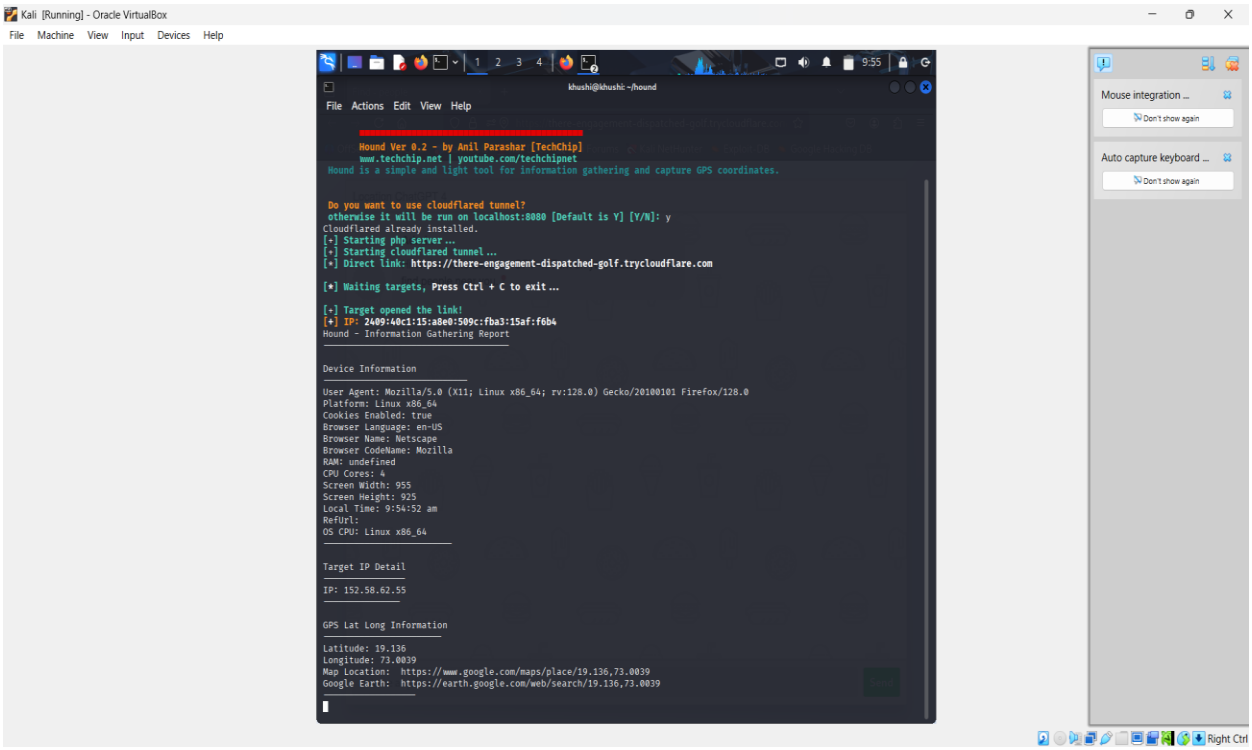
4) Select yes:



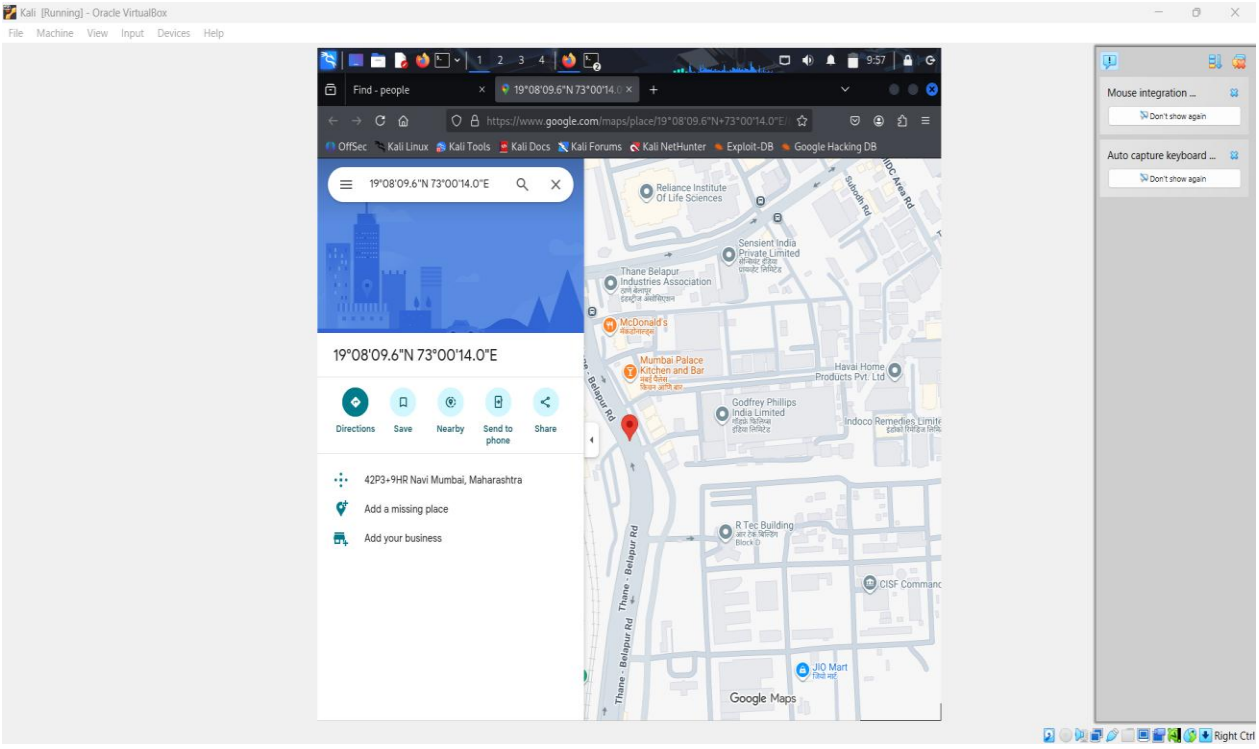
5) Start a attack:



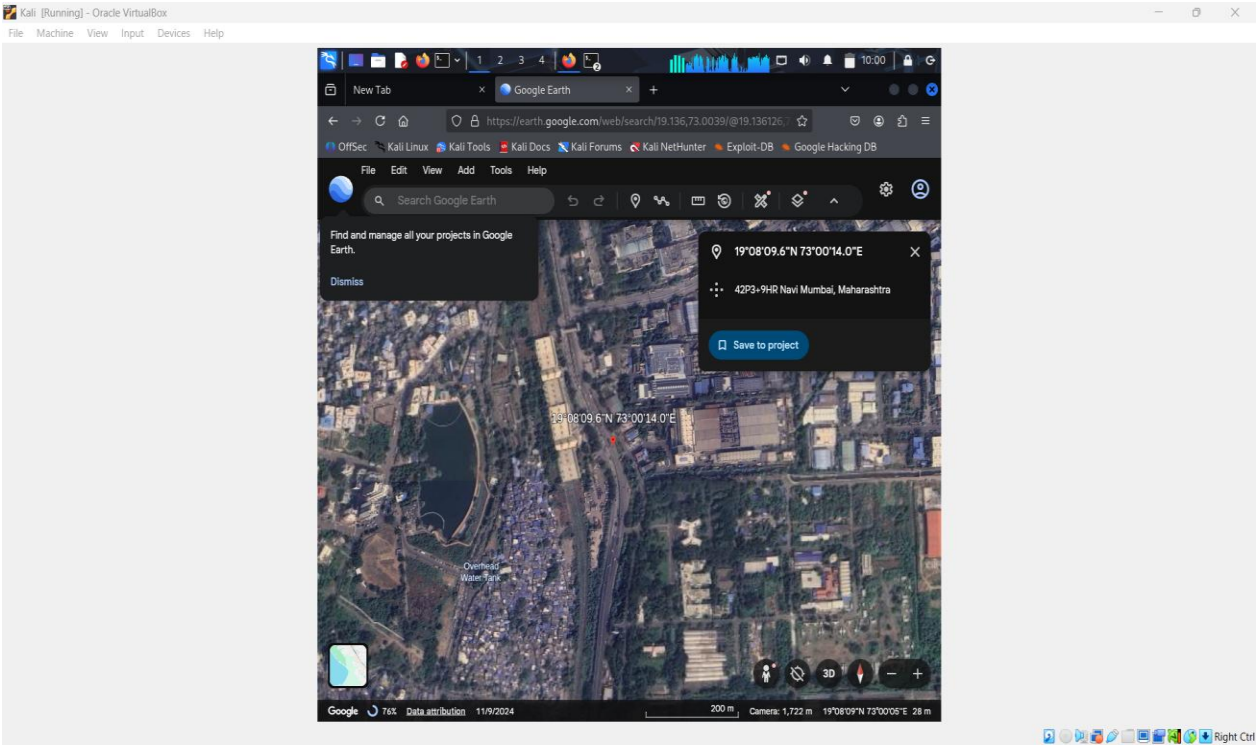
6) Start a attack:



07) Location Find:



08) Location Find:



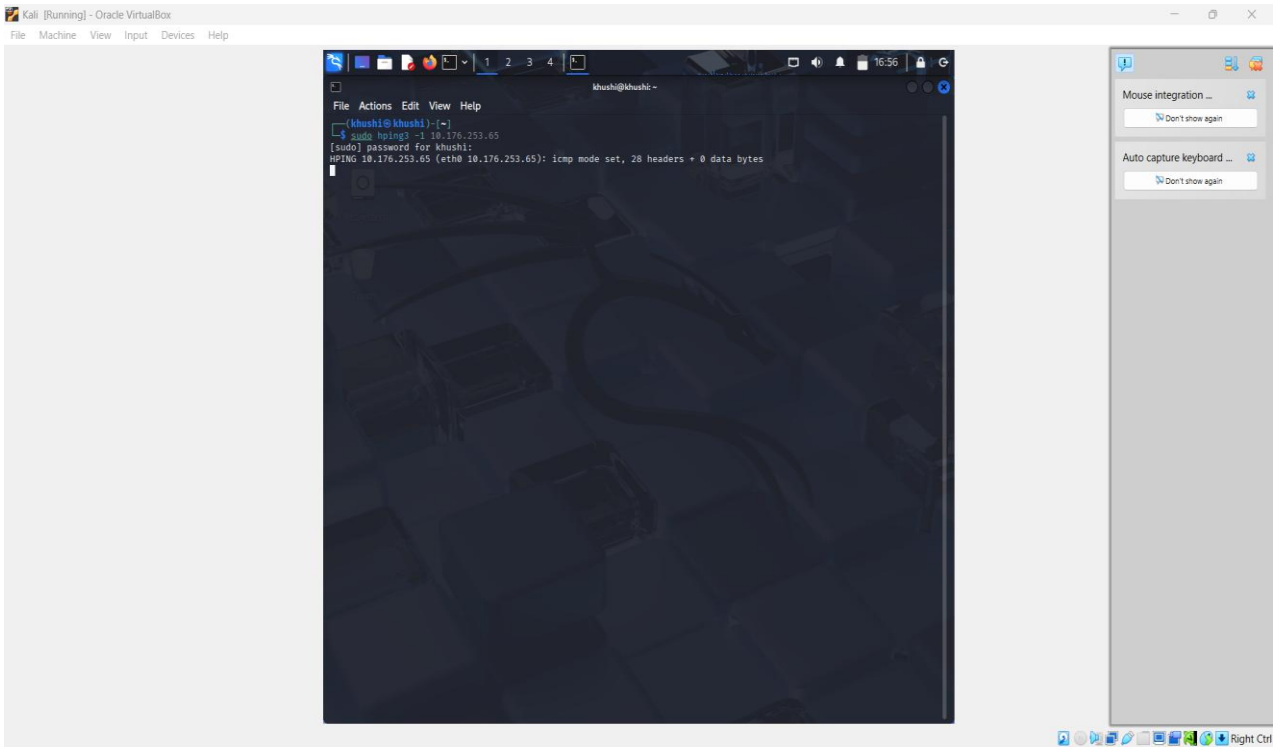
Practical-9

AIM:

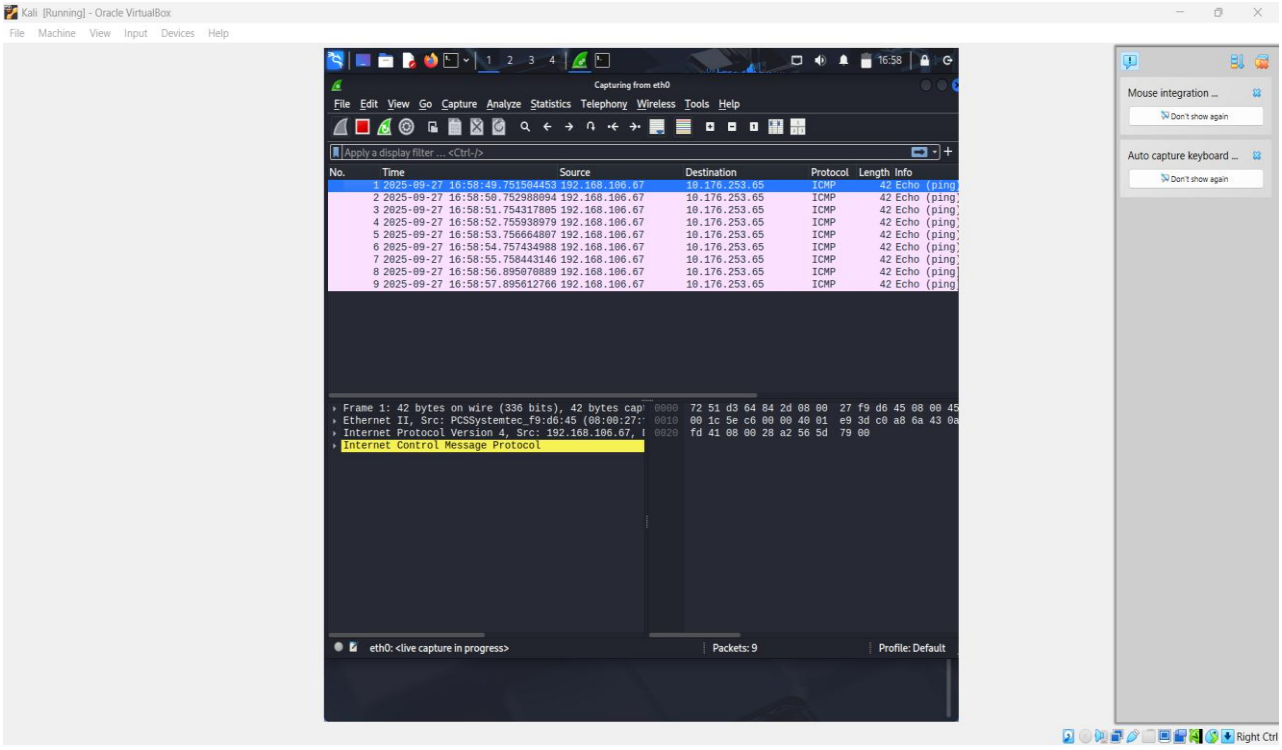
Simulate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks against a controlled target using hping3 to analyze the impact of traffic-based disruption attacks.

STEPS with screenshots:

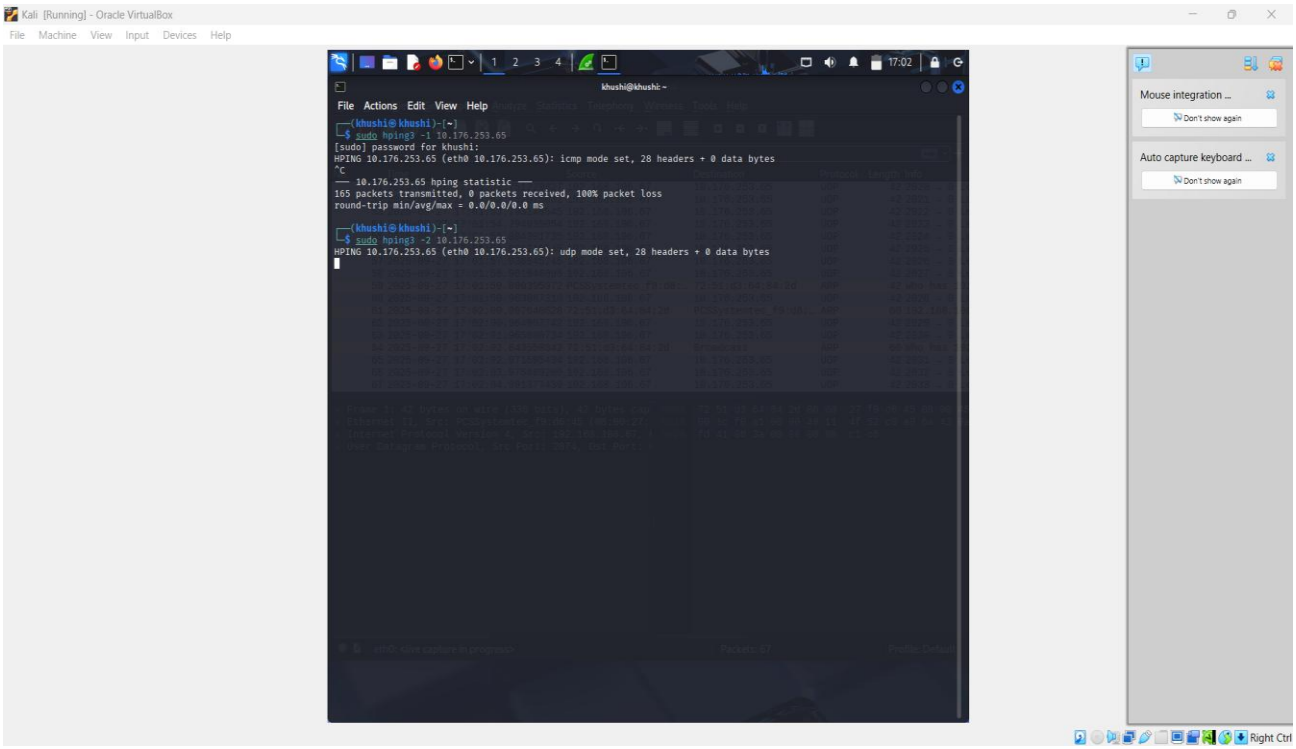
1) sudo hping3 -1 10.176.253.65(ICMP mode (like ping))



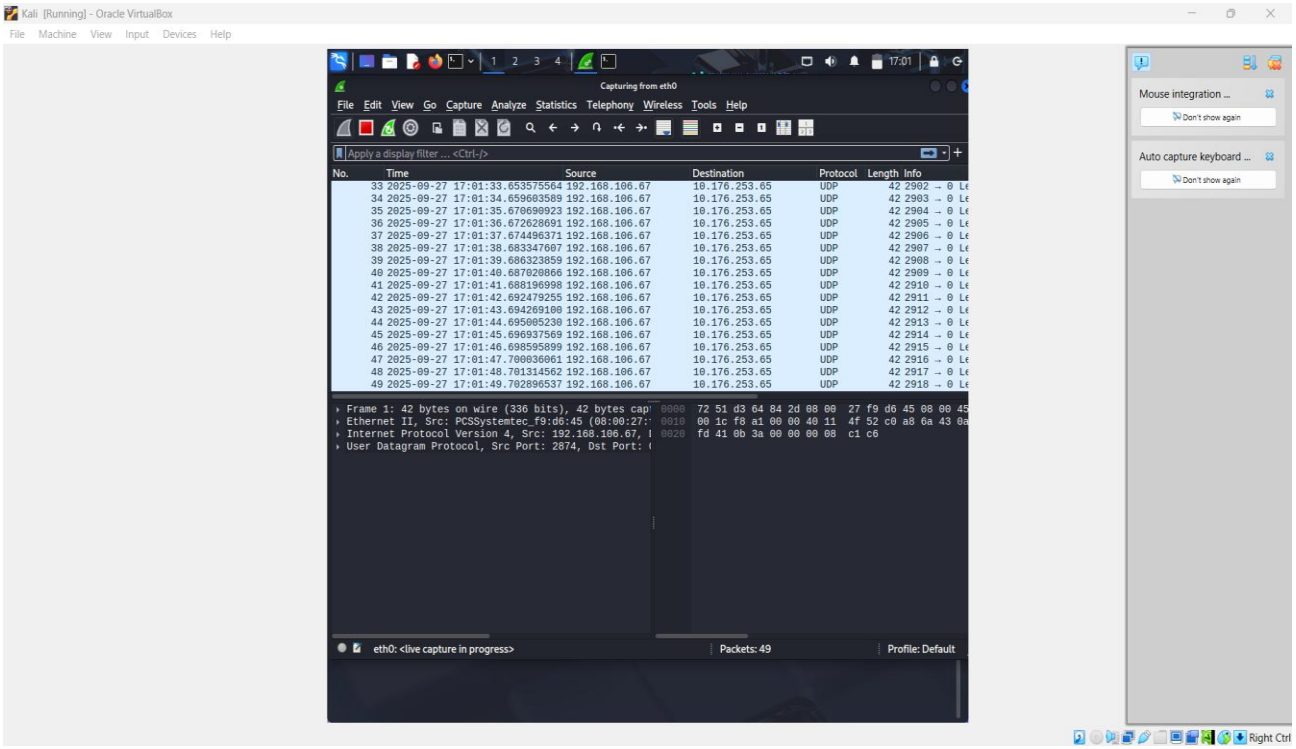
Output On Wireshark:



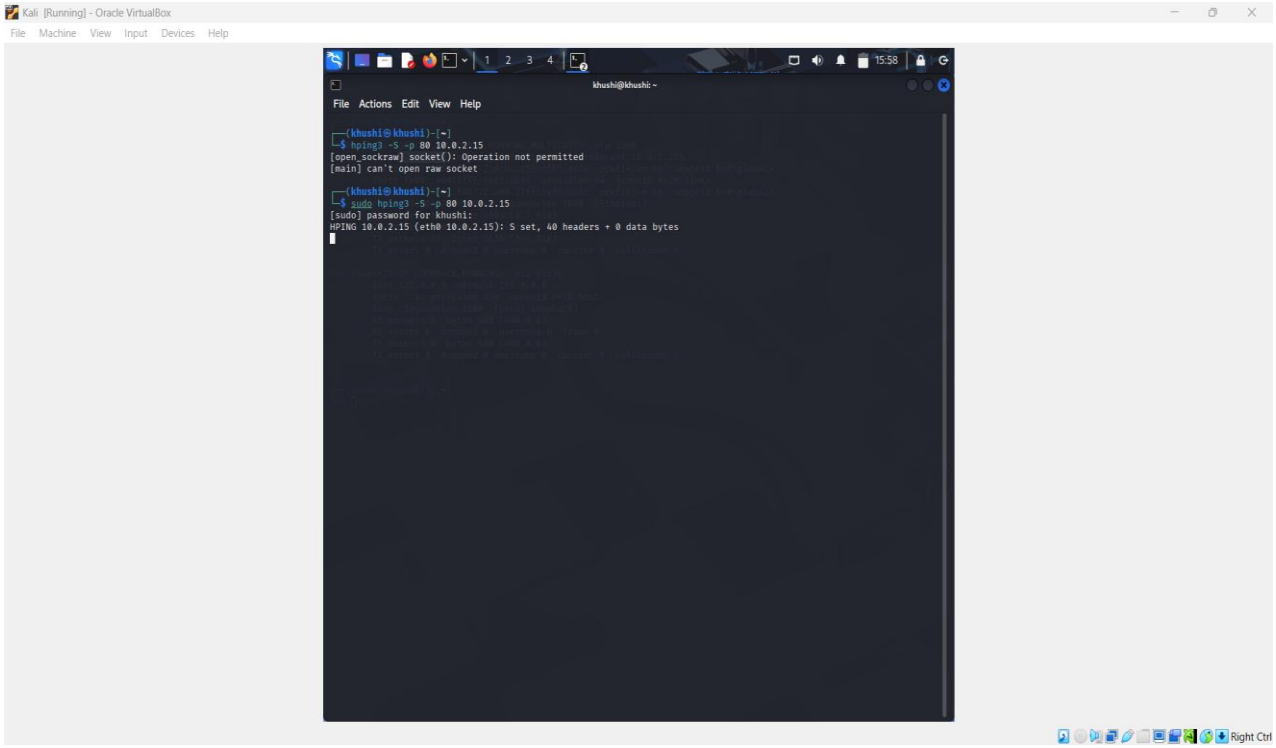
2) sudo hping3 -2 10.176.253.65(+UDP mode):



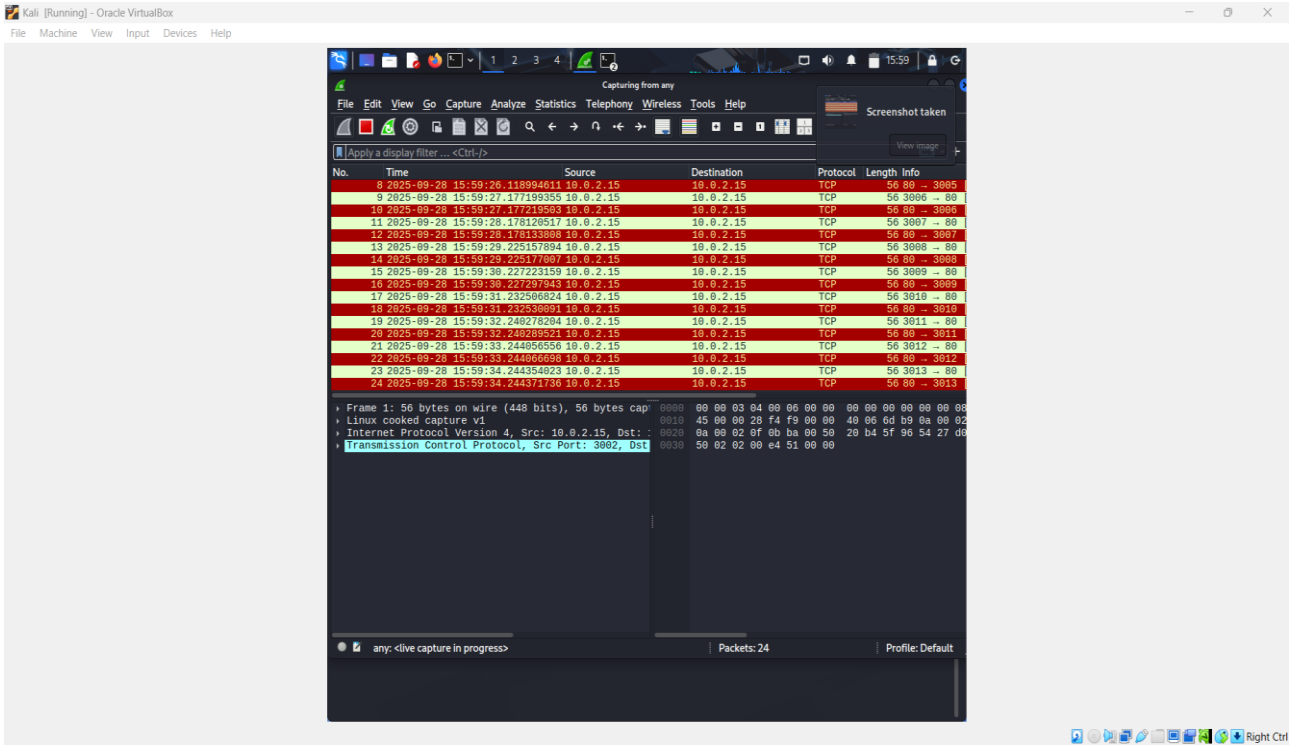
Output On Wireshark:



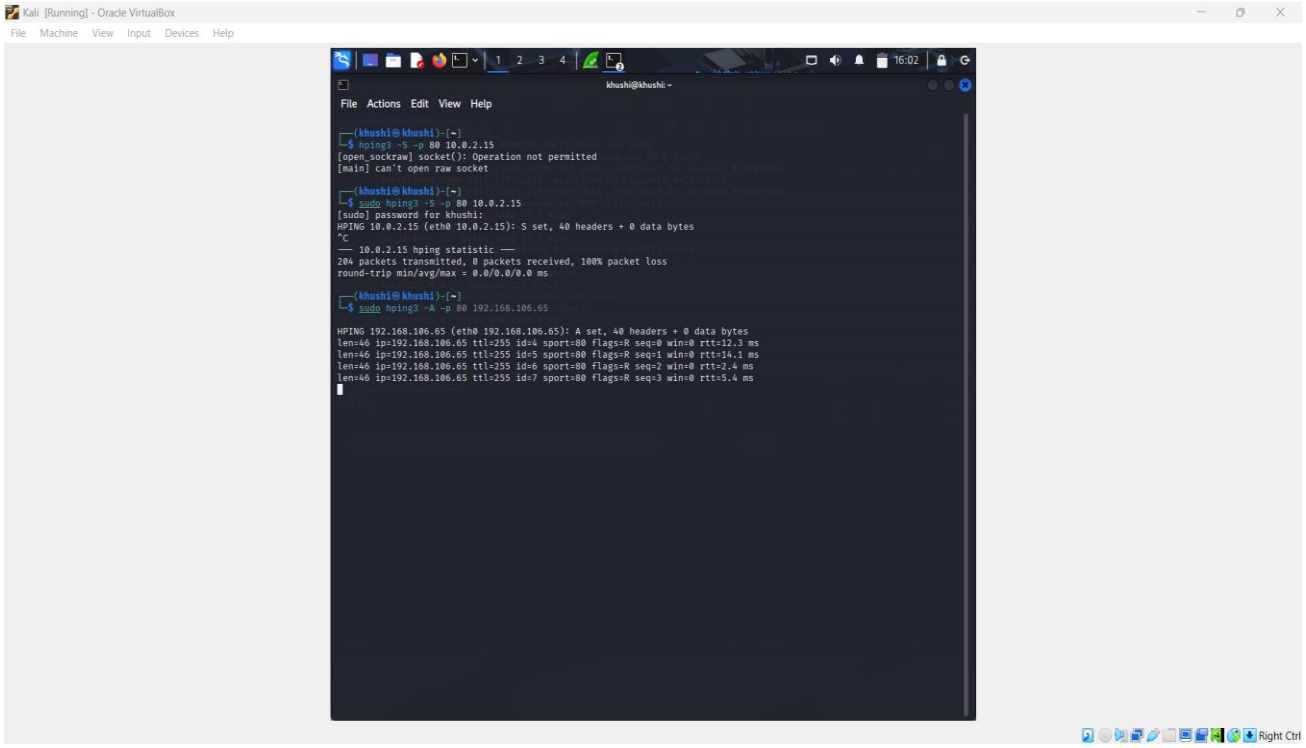
3) hping3 -S -p 80 192.168.1.1 (TCP SYN flag (scan)):



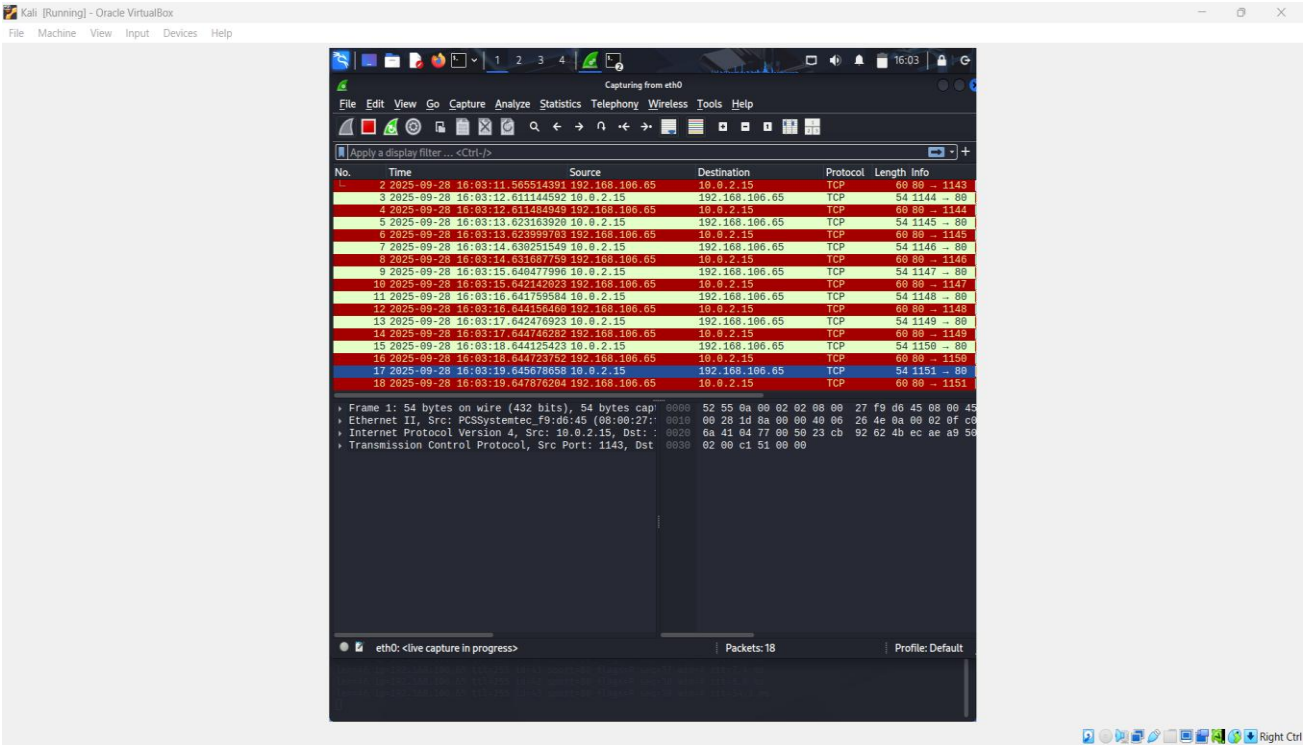
Output on WireShark:



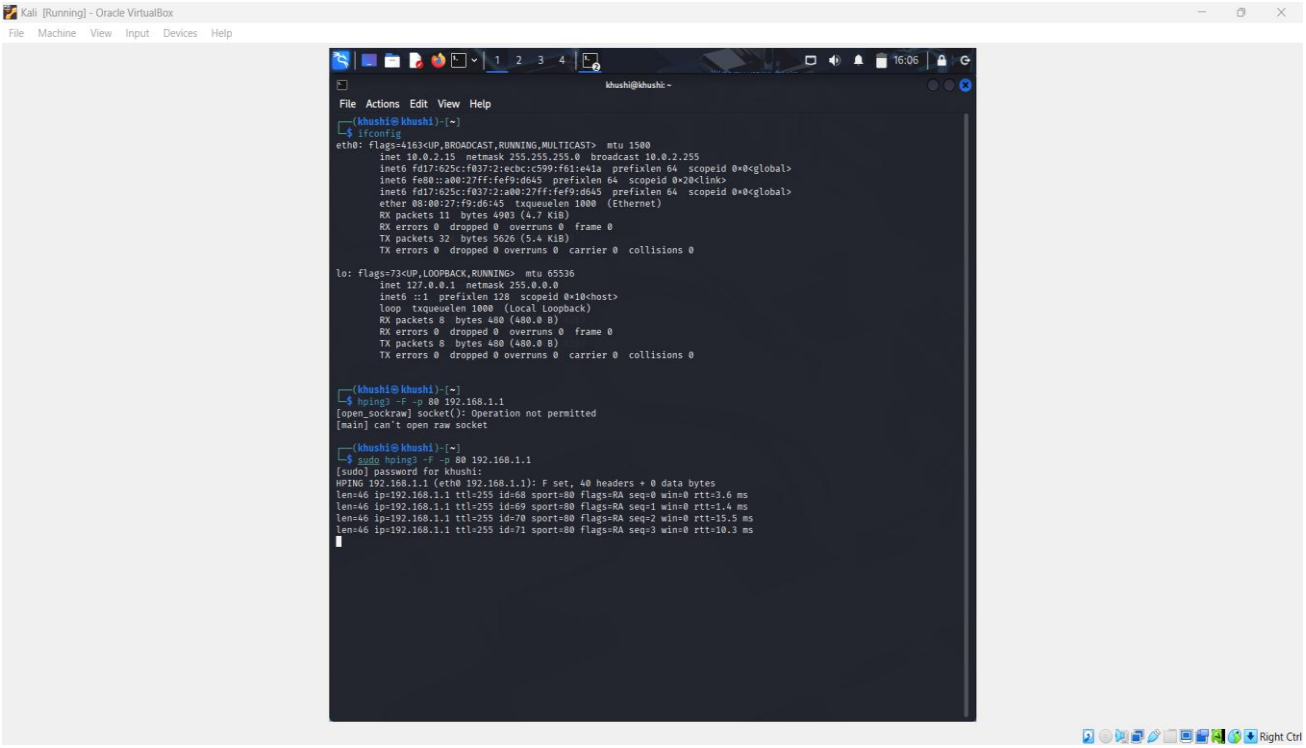
4) hping3 -A -p 80 192.168.1.1(TCP ACK flag (firewall testing)):



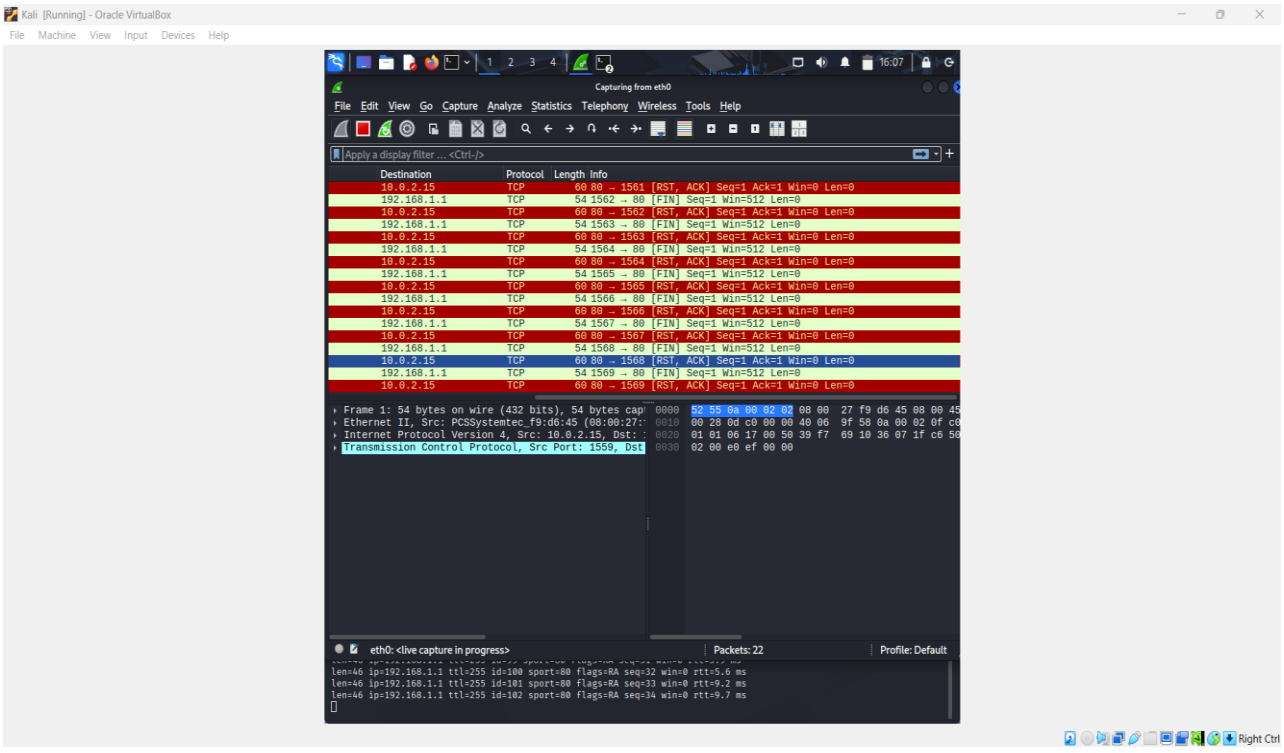
Output on WireShark:



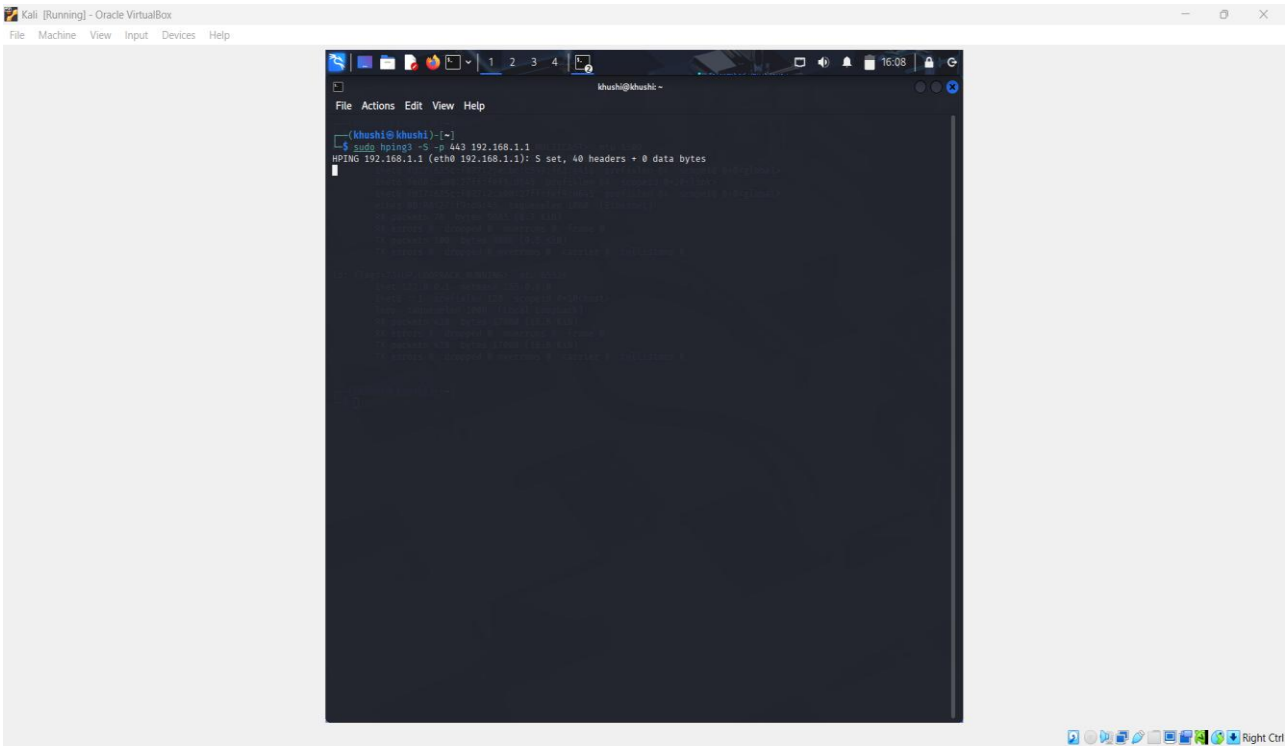
5) hping3 -F -p 80 192.168.1.1(TCP FIN flag):



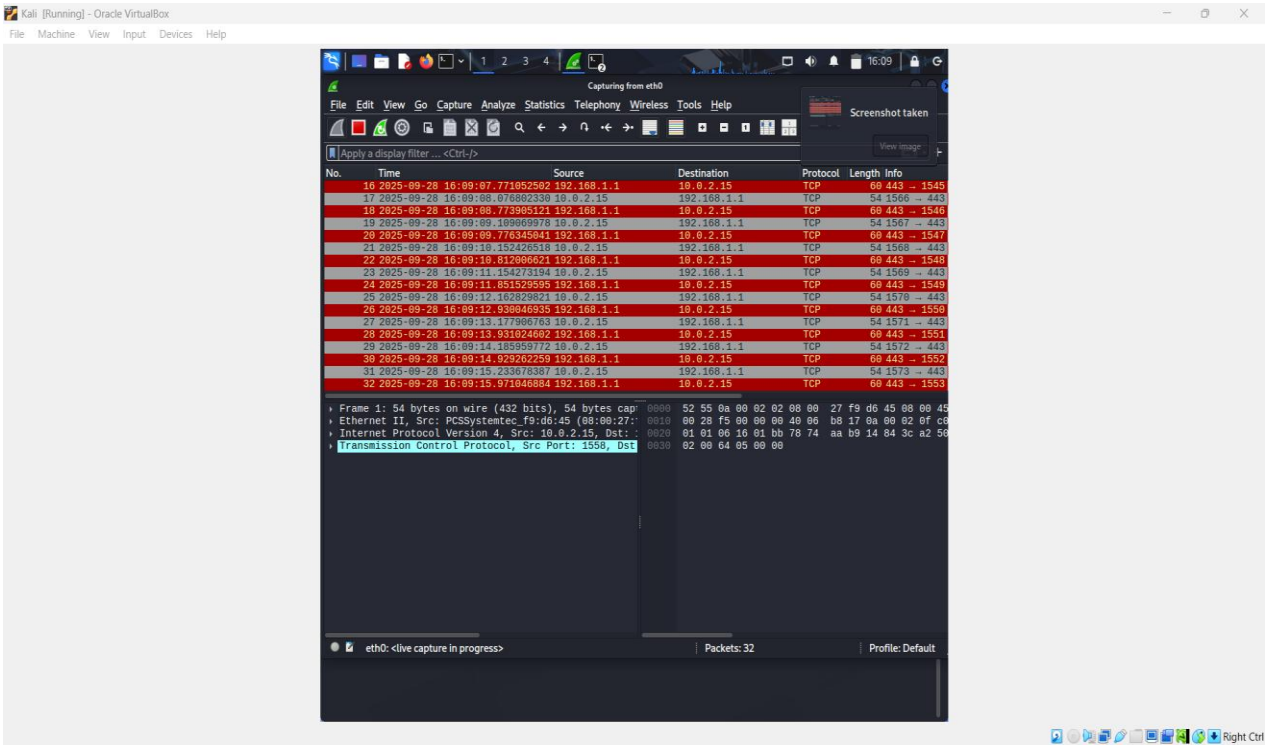
Output on WireShark:



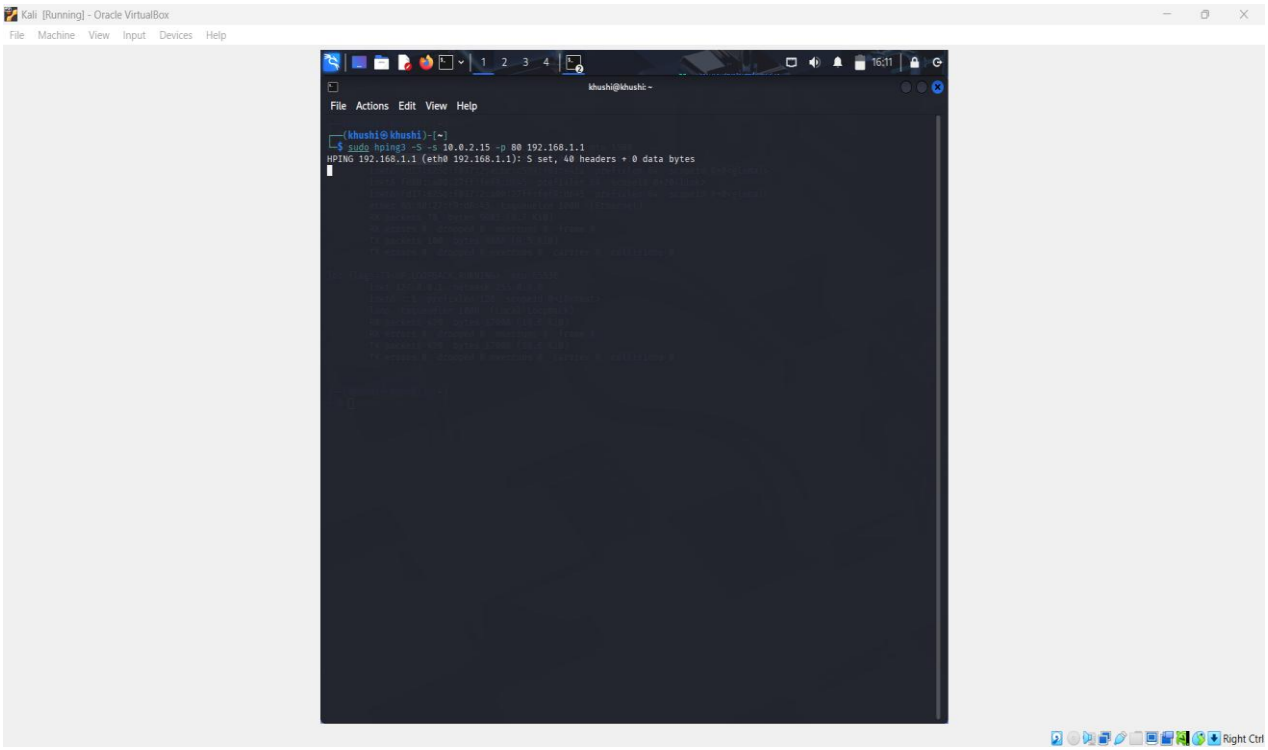
6) hping3 -S -p 443 192.168.1.1(Destination port):



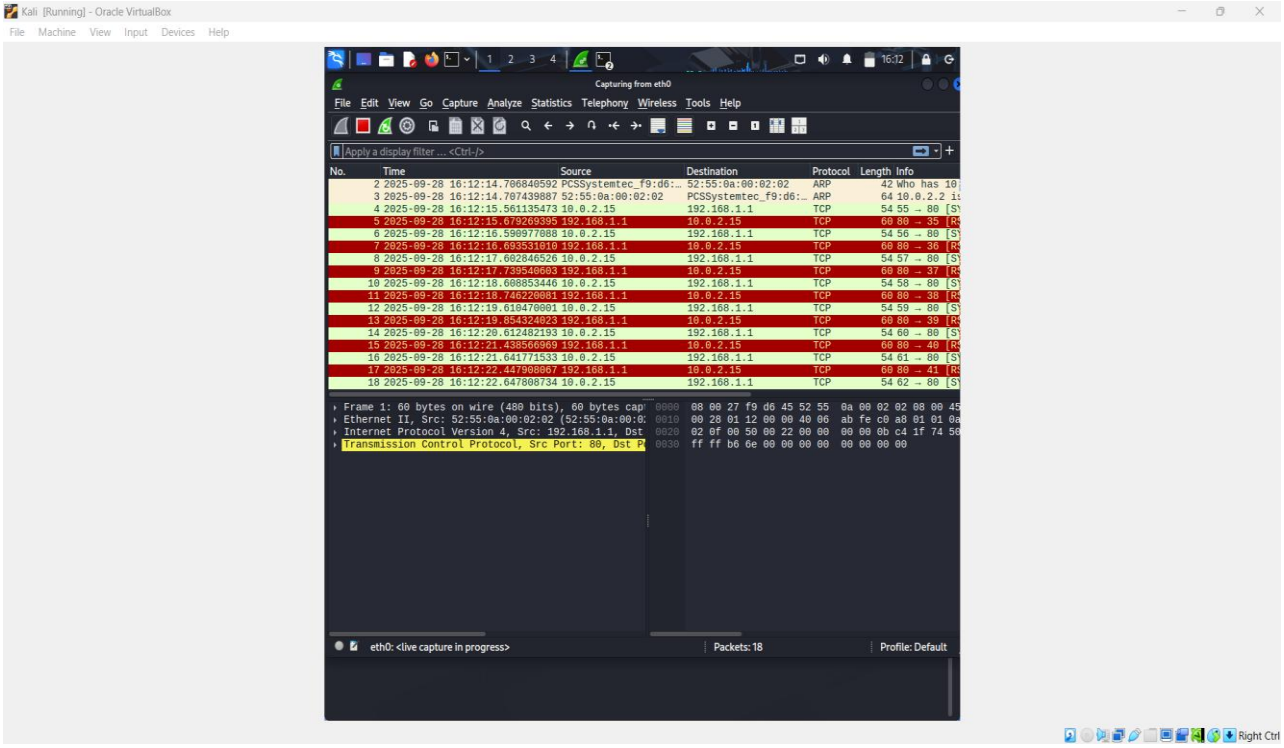
Output on WireShark:



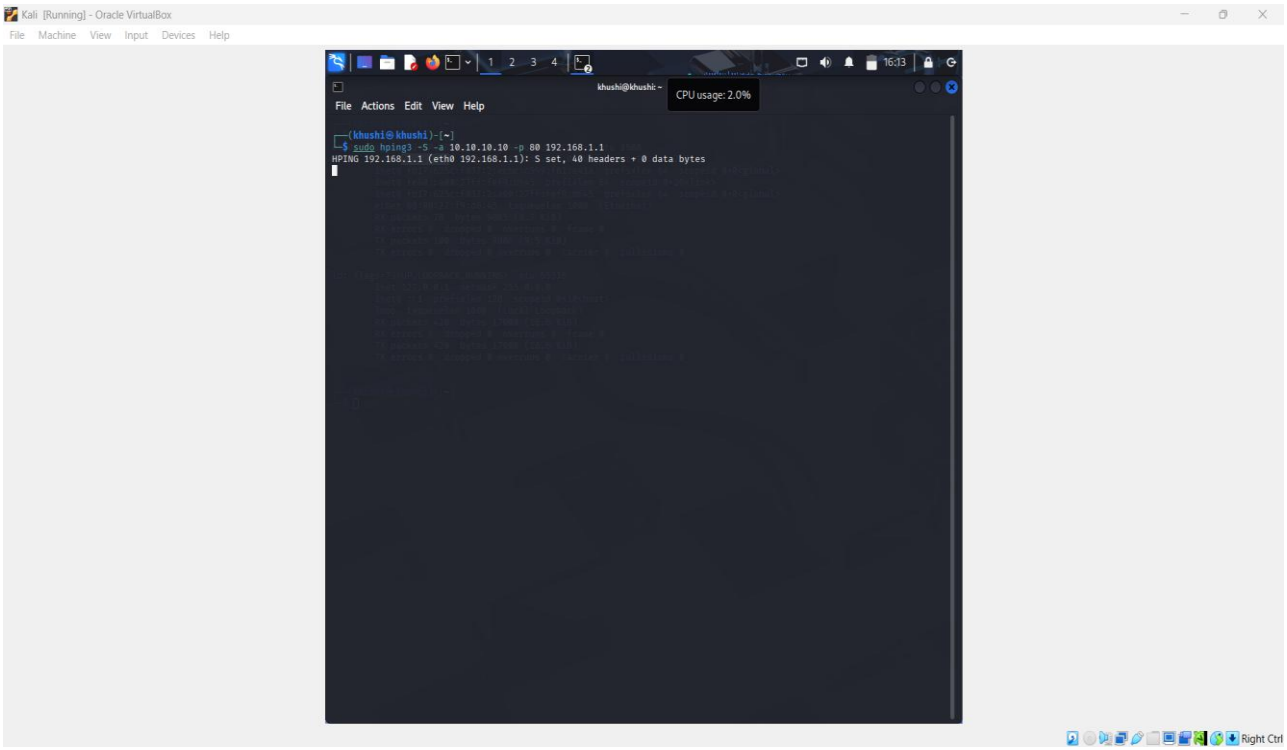
7) hping3 -S -s 12345 -p 80 192.168.1.1(Source port):



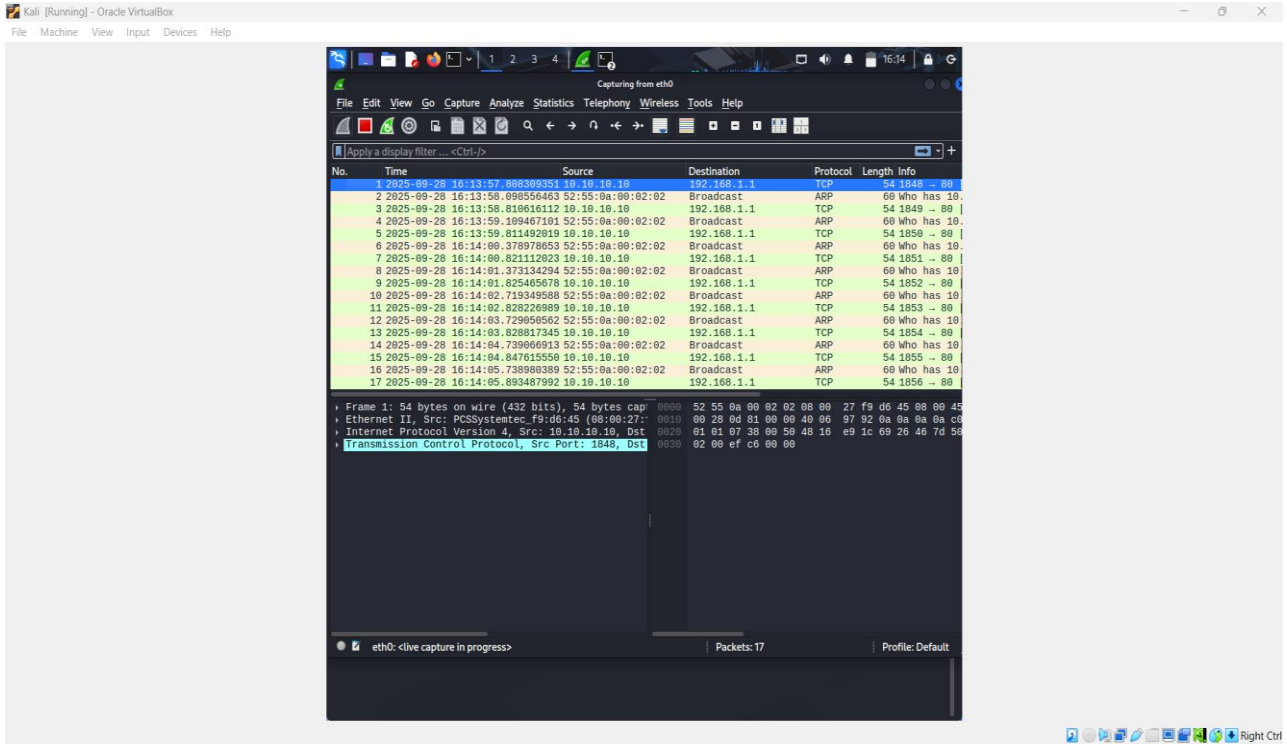
Output On WireShark:



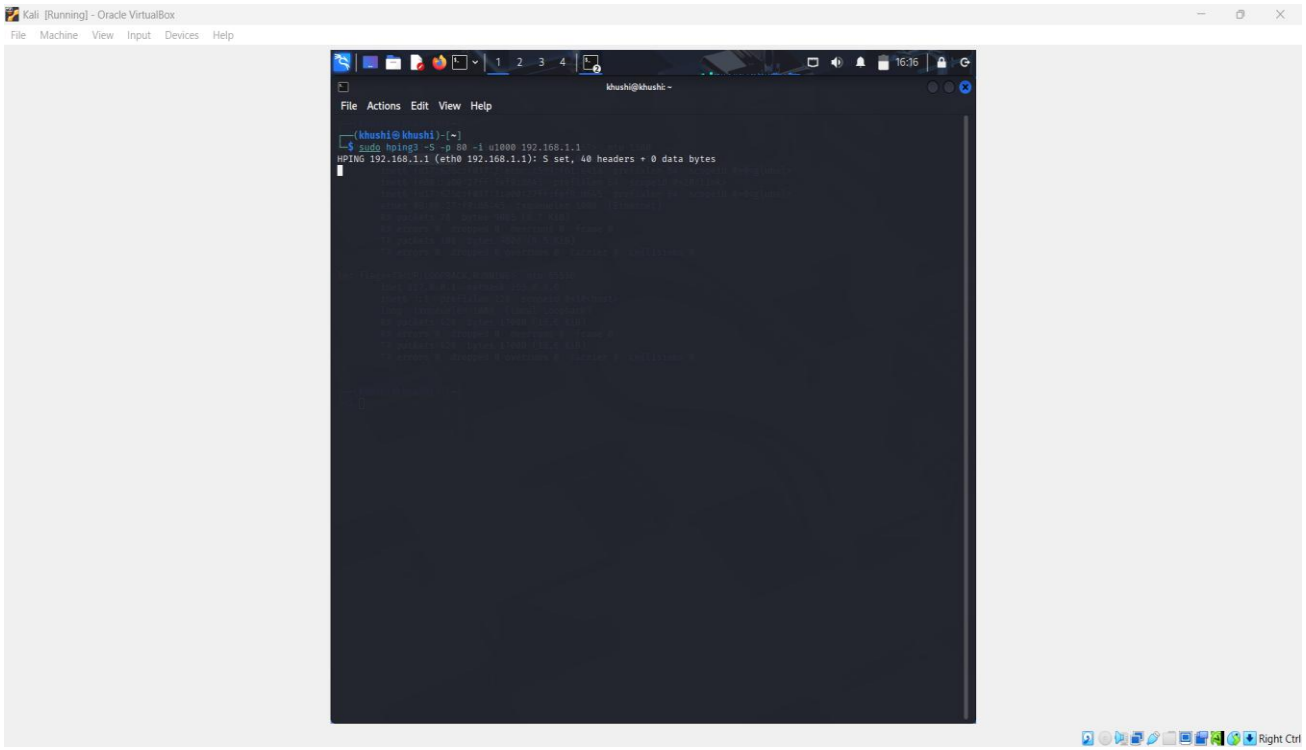
8) hping3 -S -a 10.10.10.10 -p 80 192.168.1.1(Spoof source IP):



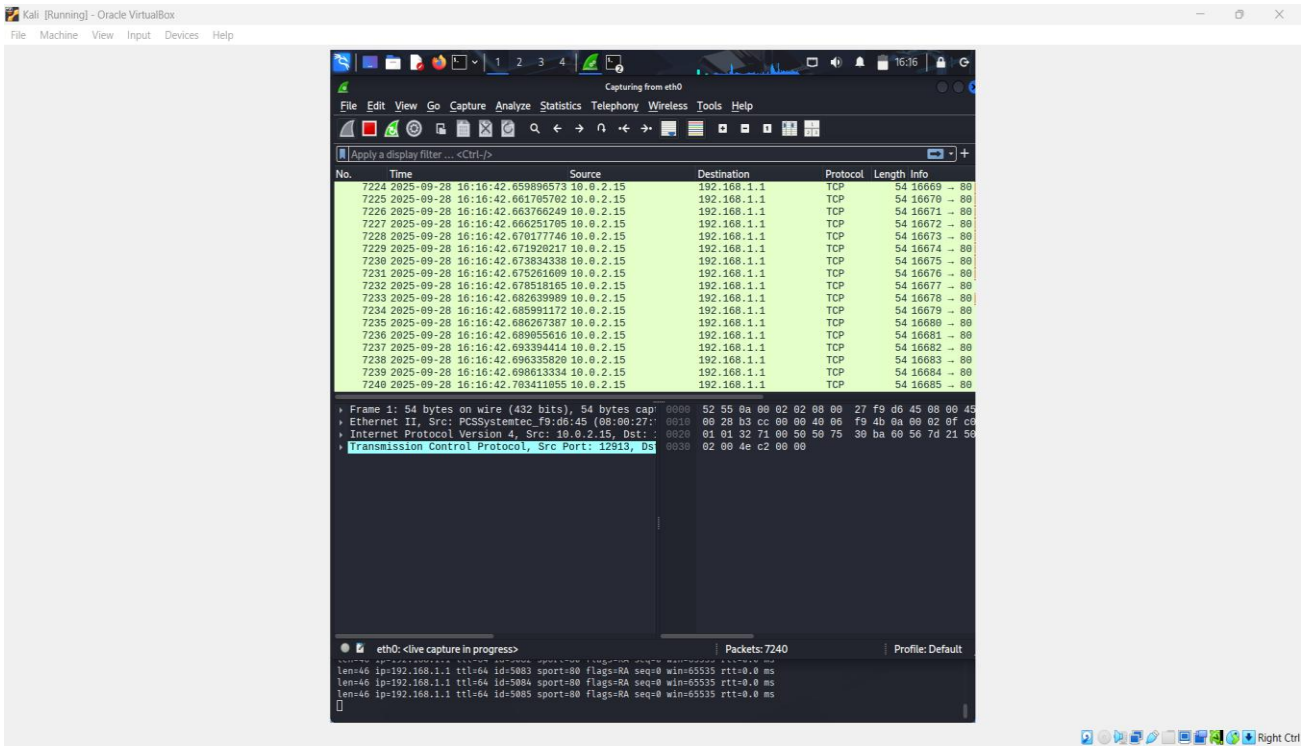
Output on WireShark :



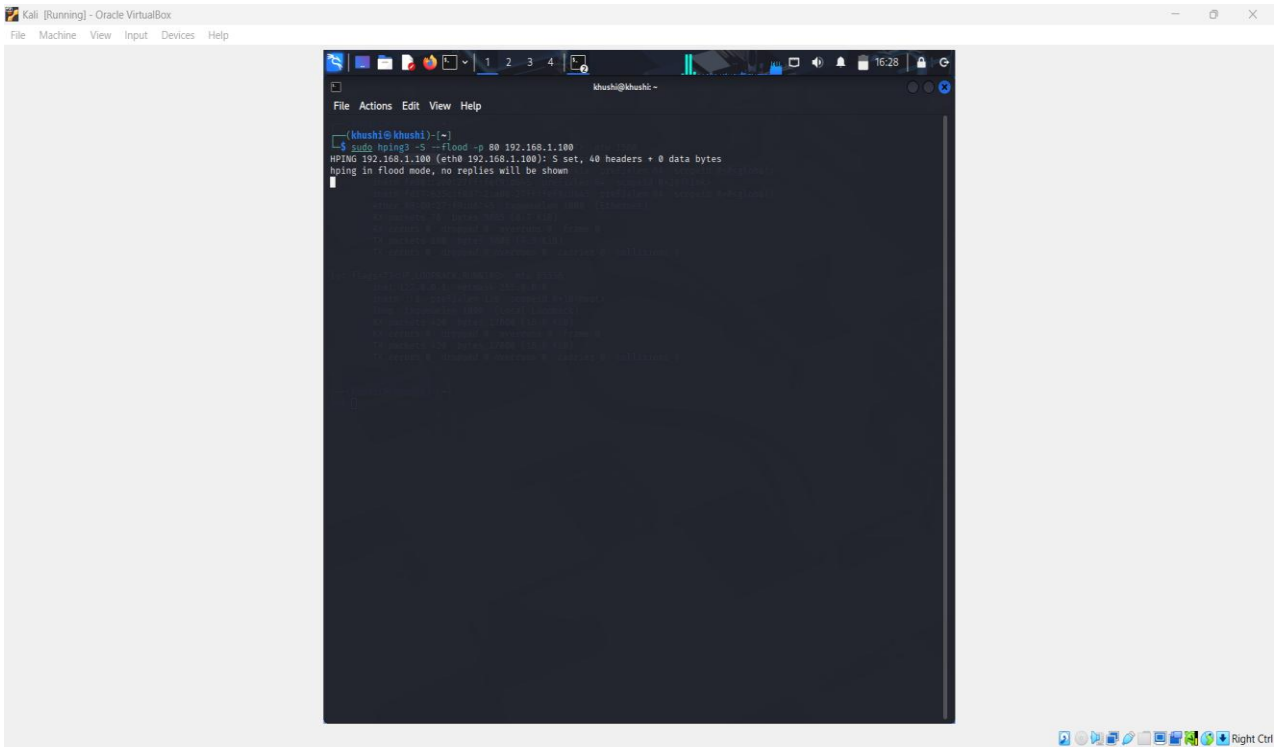
9) hping3 -S -p 80 -i u1000 192.168.1.1(Send packet every 1000µs (1ms)):



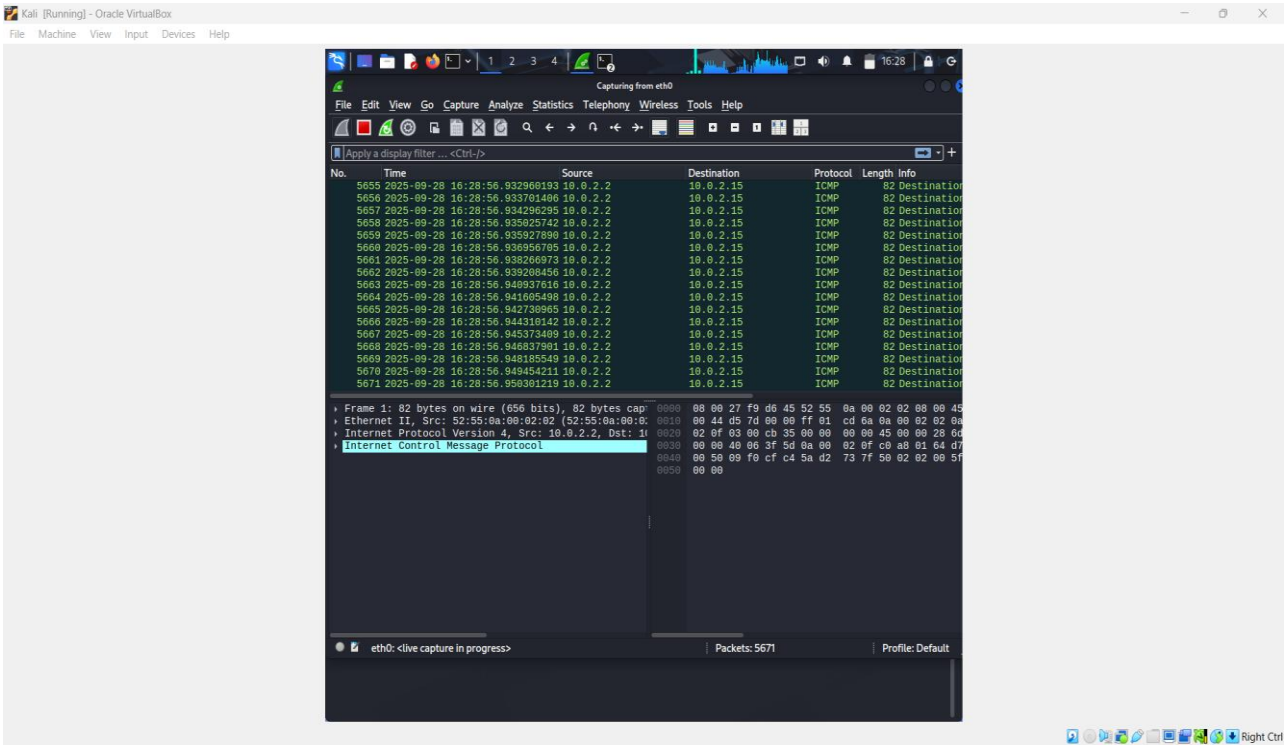
Output on WireShark:



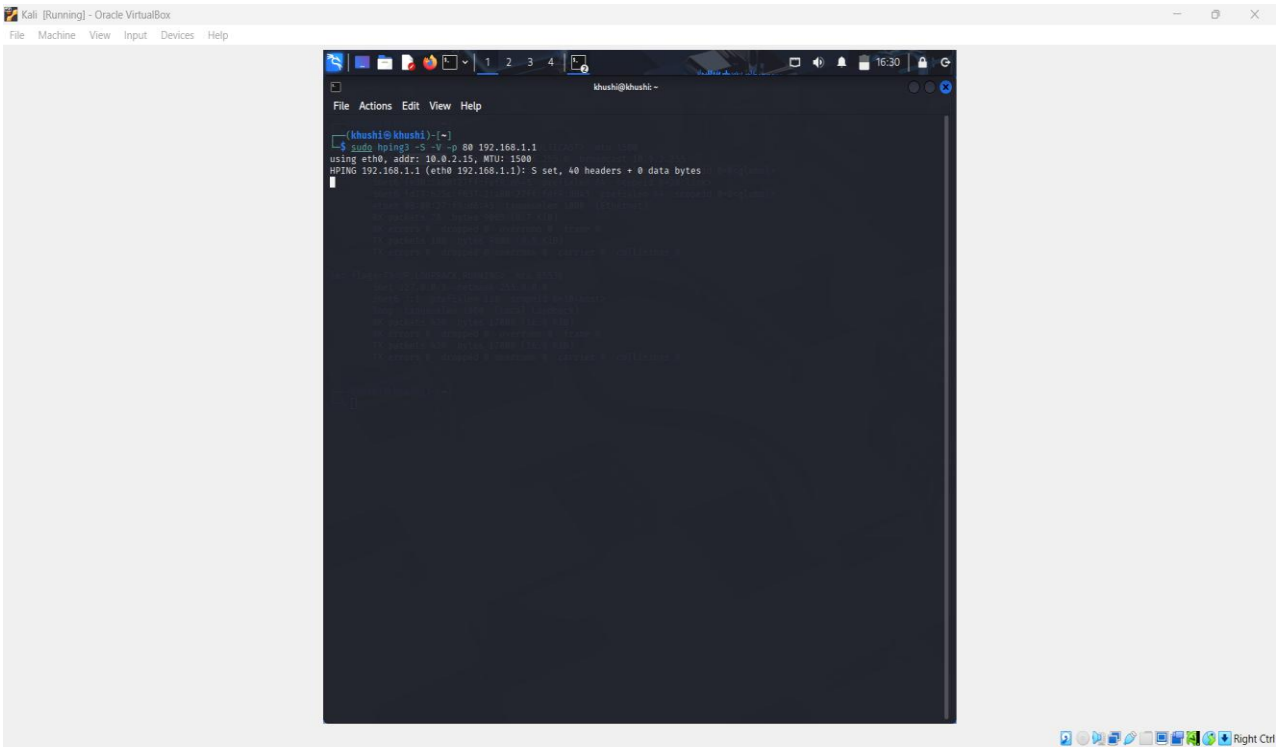
10) hping3 -S --flood -p 80 192.168.1.100(Flood mode (DoS simulation)):



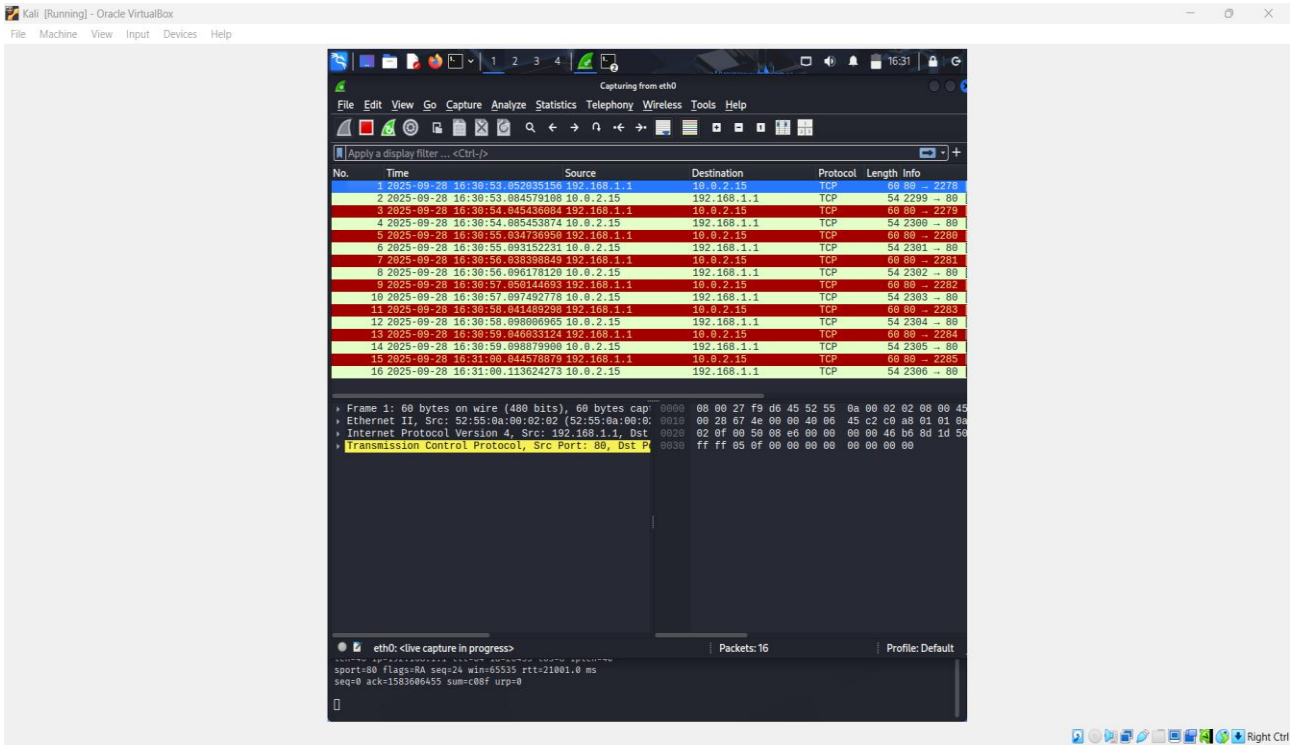
Output on WireShark:



11) hping3 -S -V -p 80 192.168.1.1(Verbose output):



Output On WireShark:



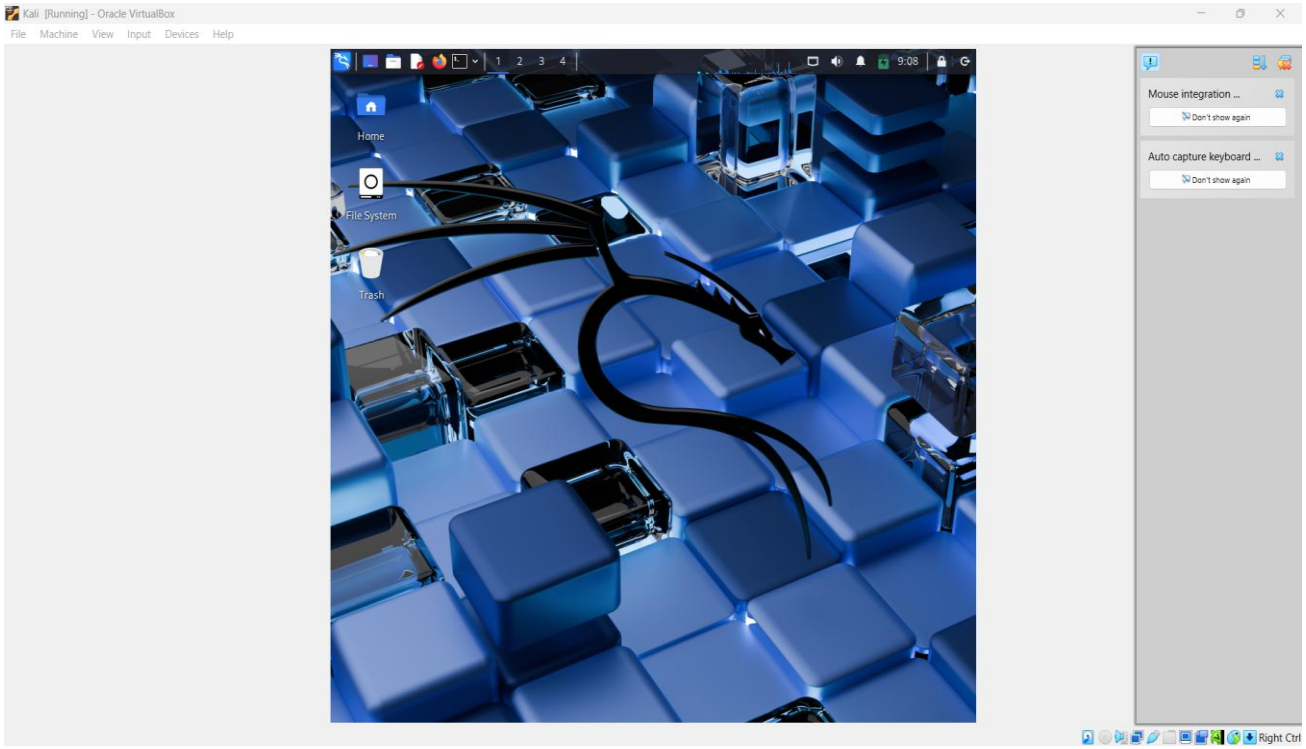
Practical-10

AIM:

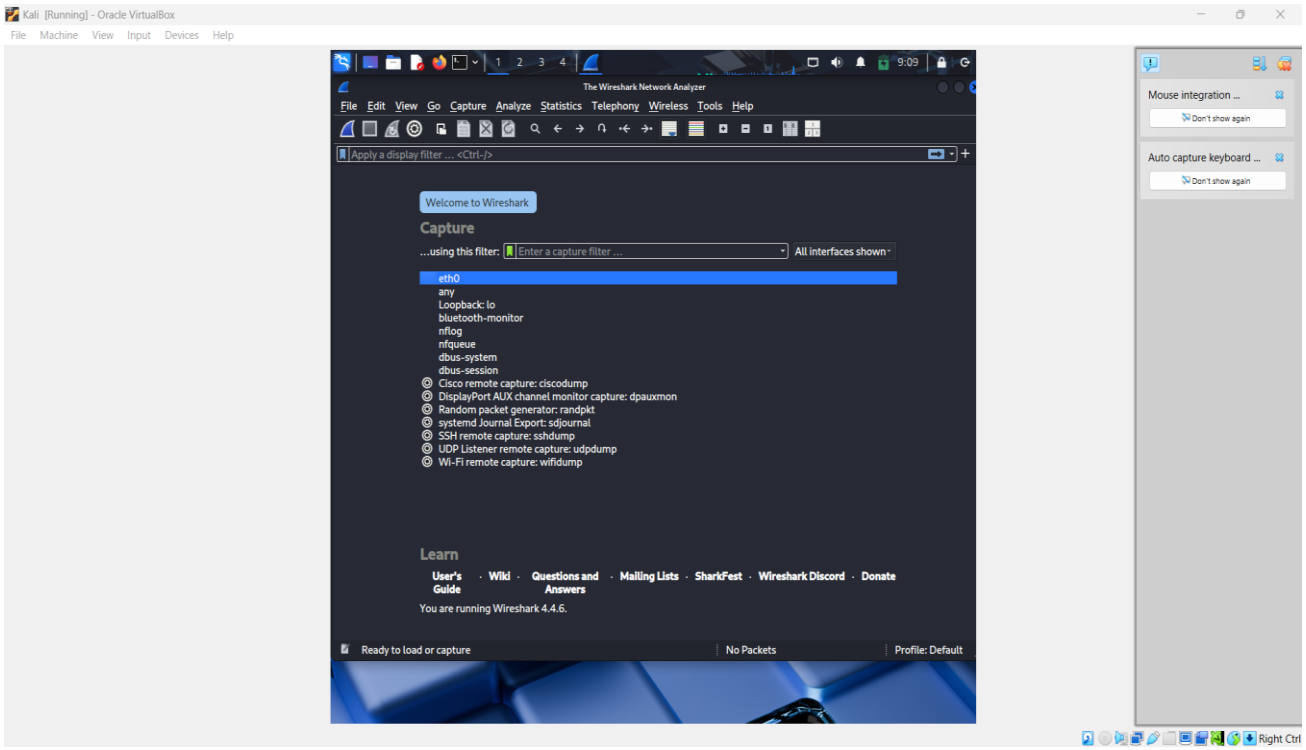
Capture and analyze HTTP traffic using Wireshark to identify plaintext credentials and sensitive information. Apply various display filters to uncover hidden data exchanged between client and server.

STEPS with screenshots:

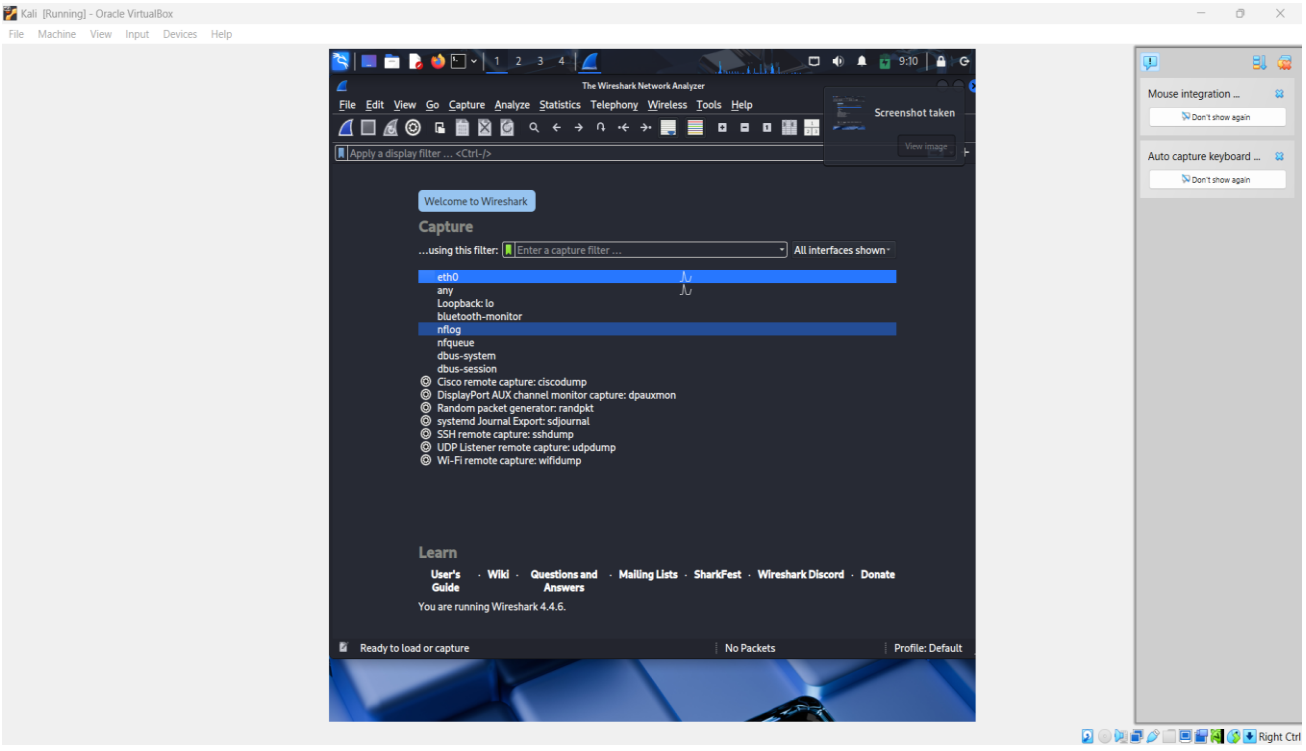
1) Start a Kali Linux:

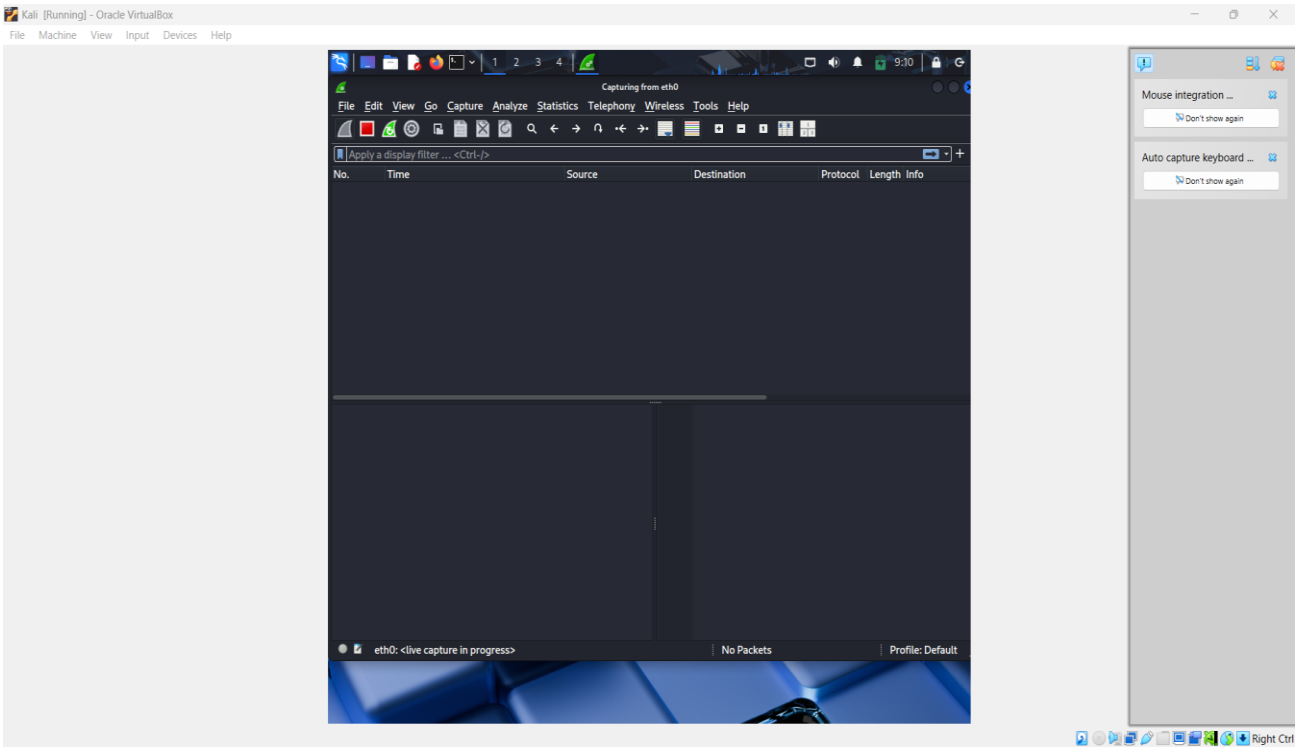


2) Start a WireShark:

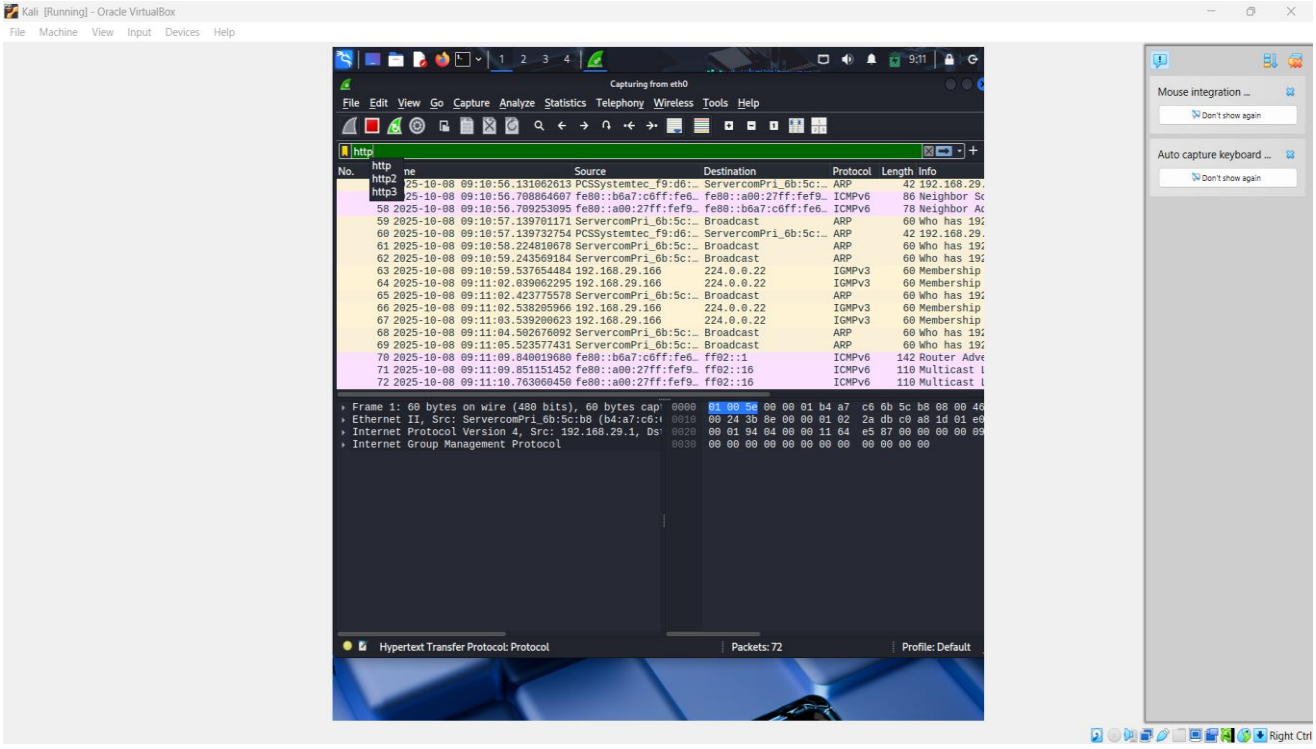

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.6.
Ready to load or capture
No Packets
Profile: Default
Mouse integration ...
Don't show again
Auto capture keyboard ...
Don't show again
Right Ctrl

3) Add a etho:

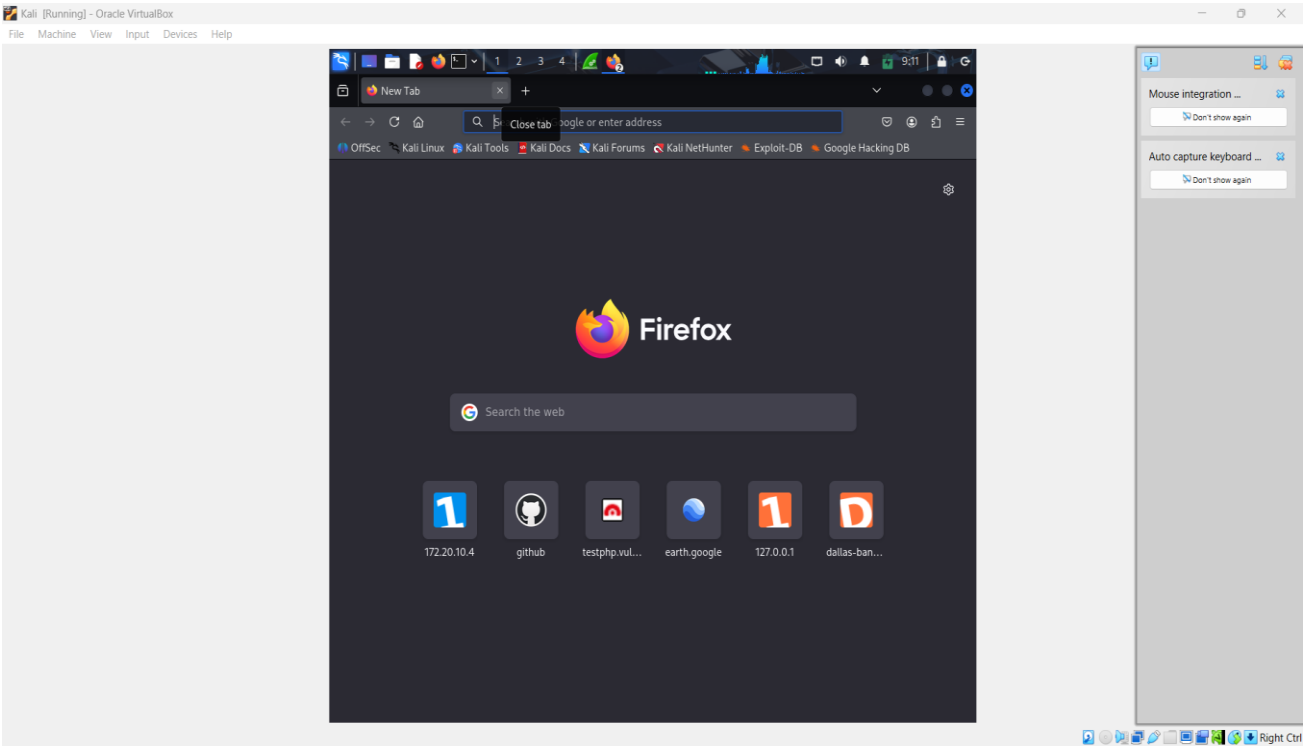

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screenshot taken
View image
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.6.
Ready to load or capture
No Packets
Profile: Default
Mouse integration ...
Don't show again
Auto capture keyboard ...
Don't show again
Right Ctrl



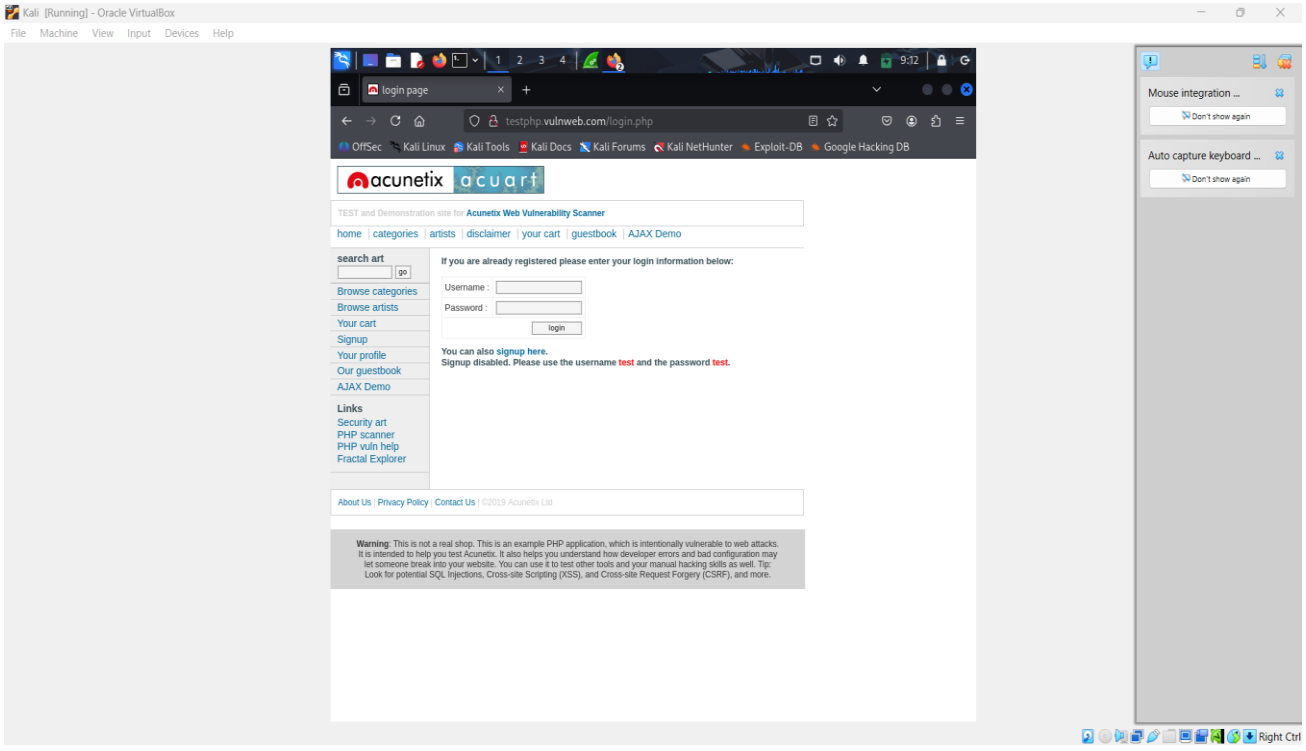
4) Filter by http:



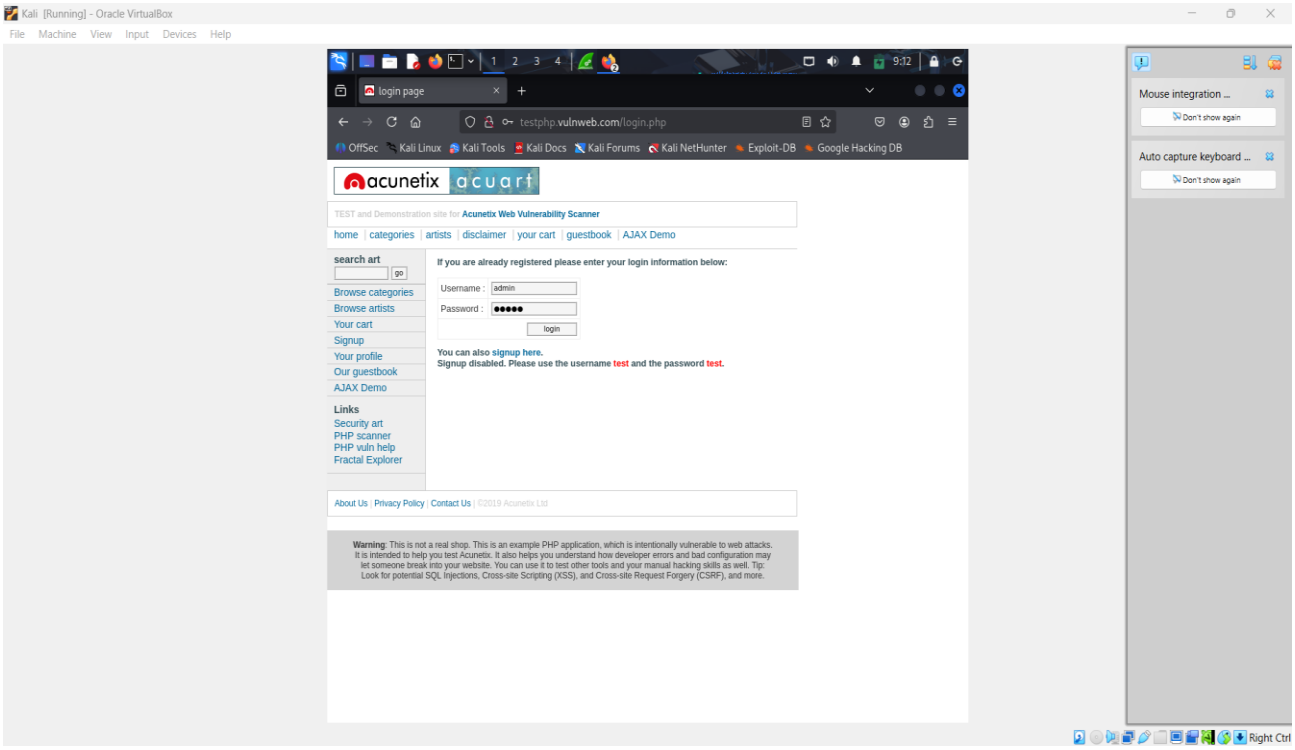
5) Start a FireFox :



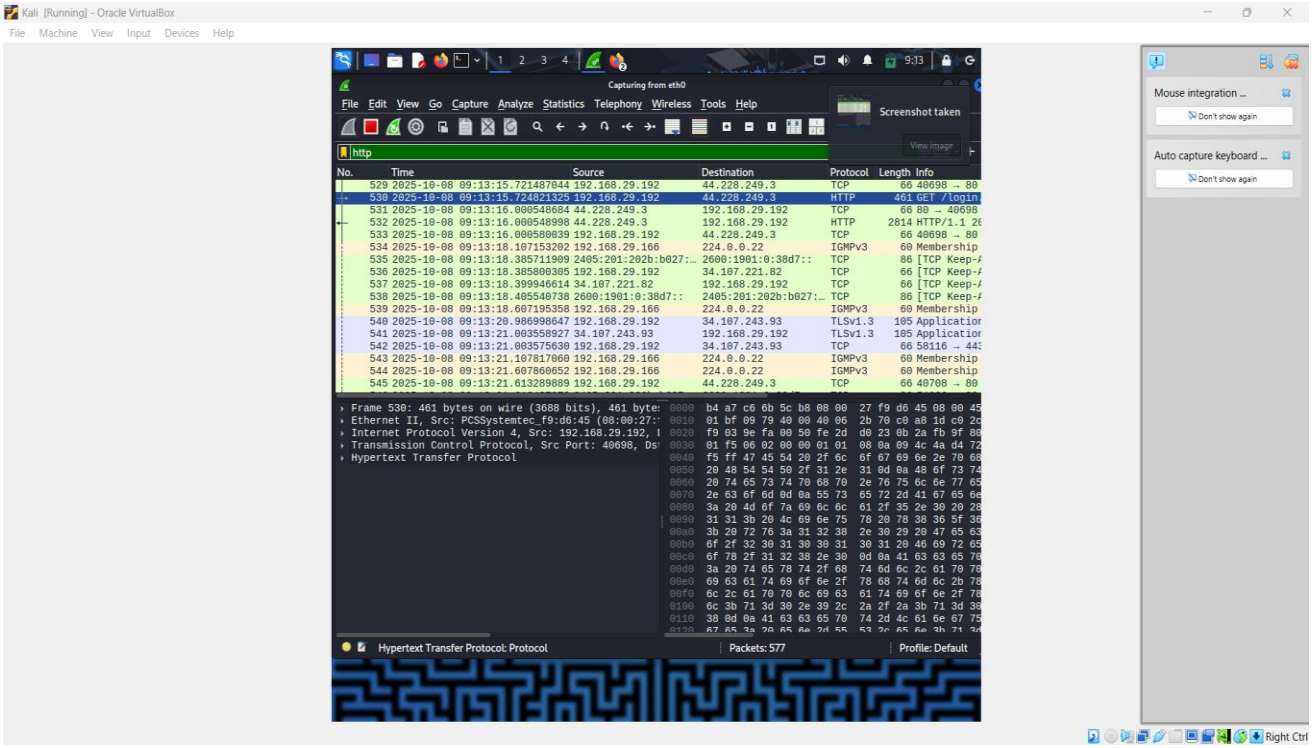
6) Start any Website :



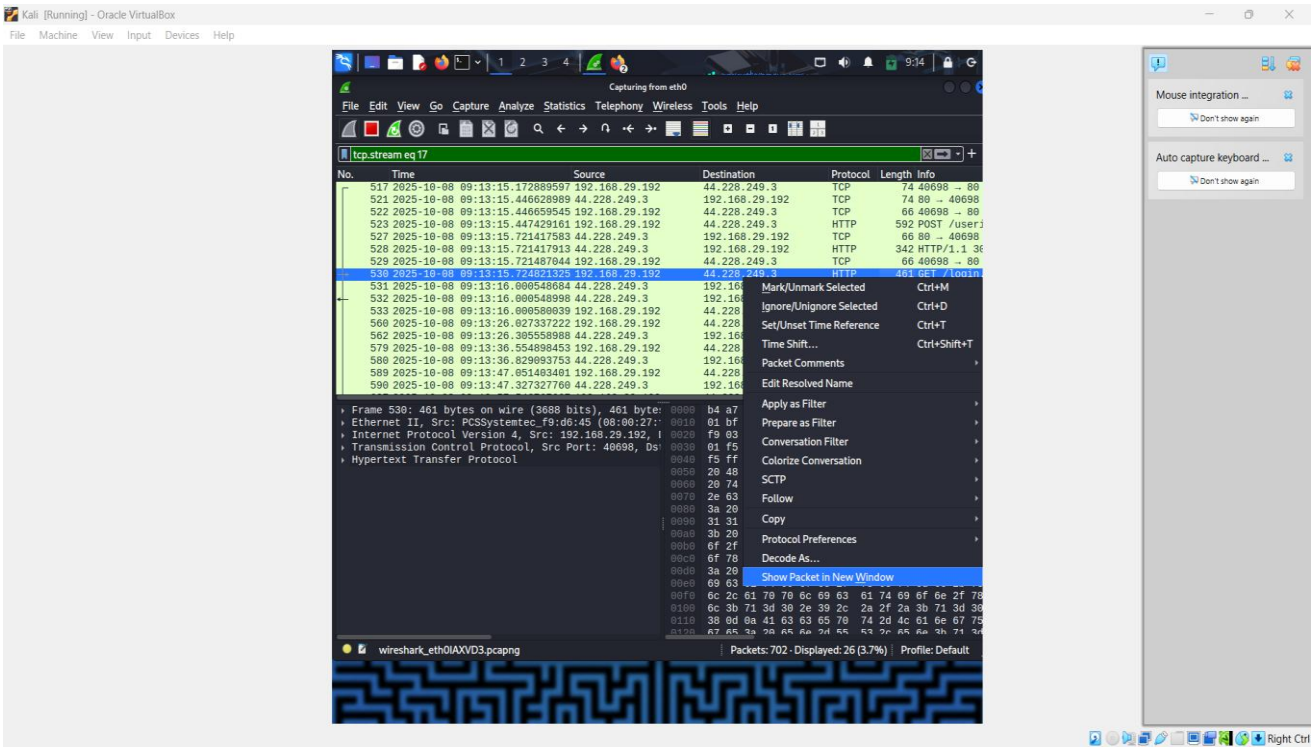
7) Add username and password :



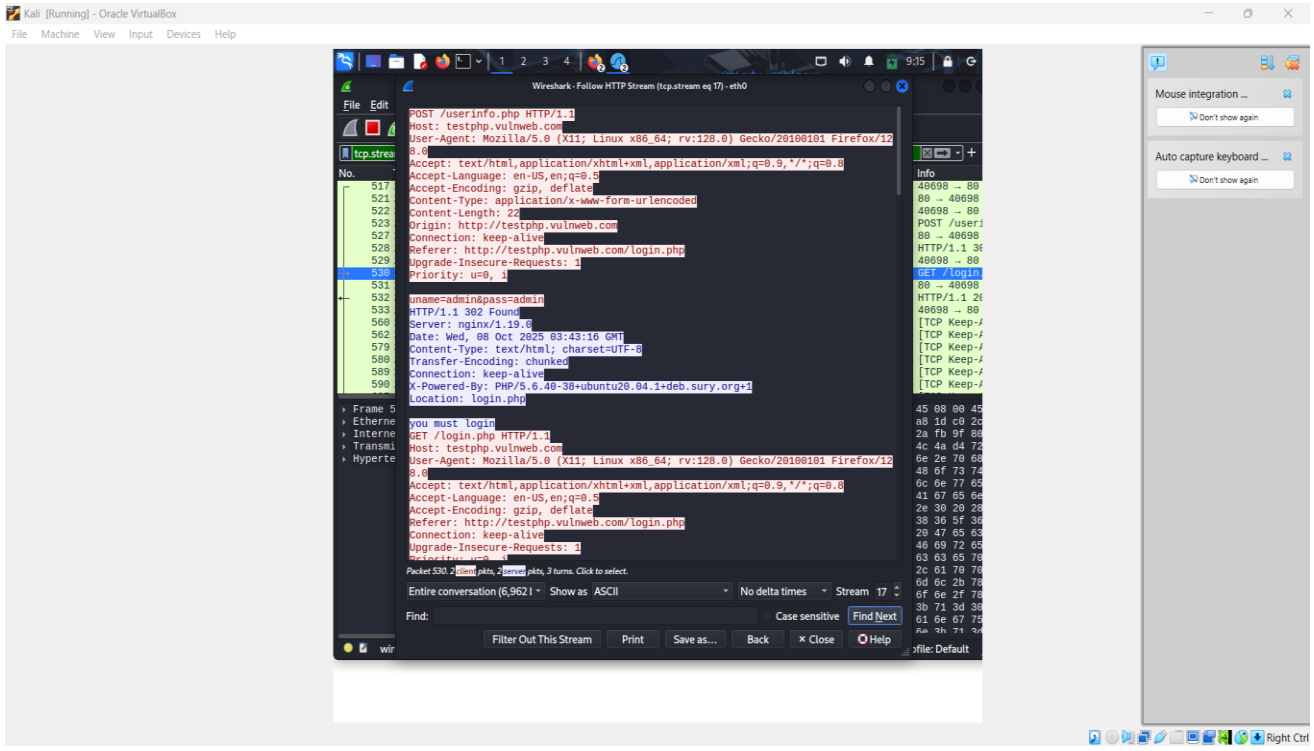
8) Check a wireshark :



9) Right click and Click a Follow and http Stream :



10)View Information:



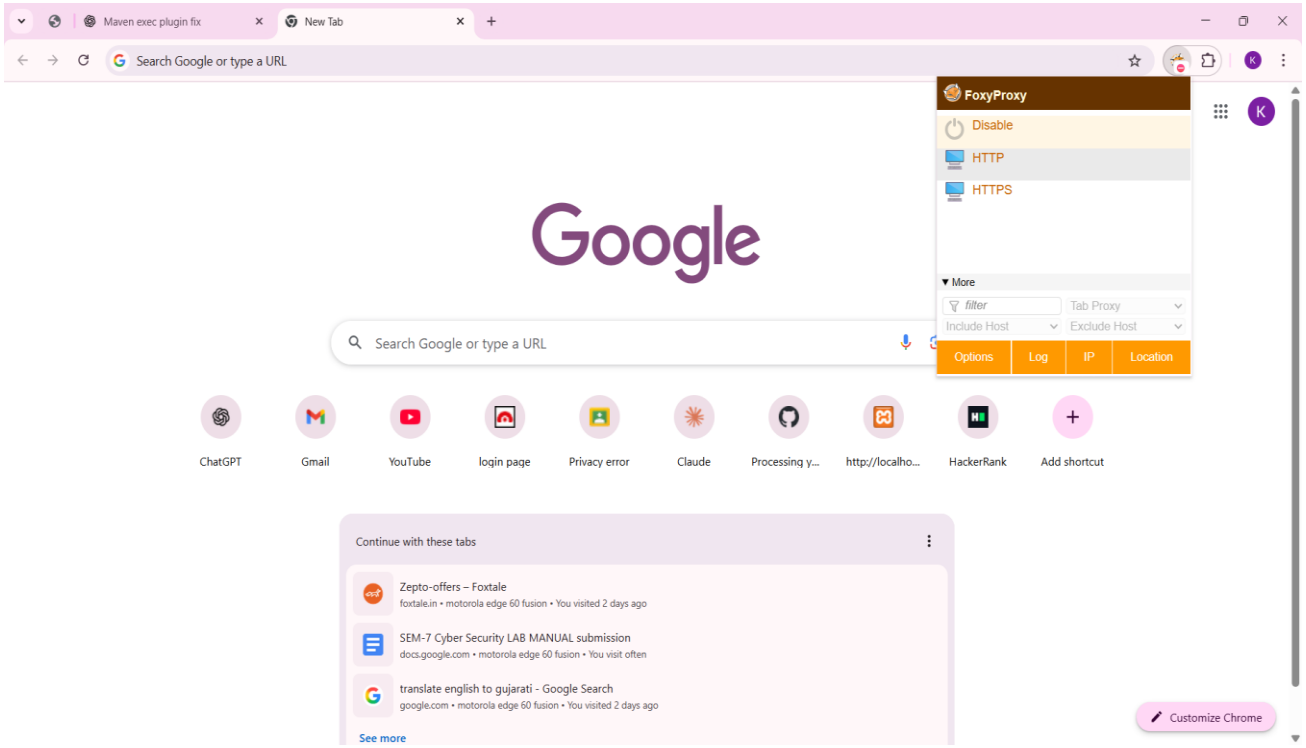
Practical-11

AIM:

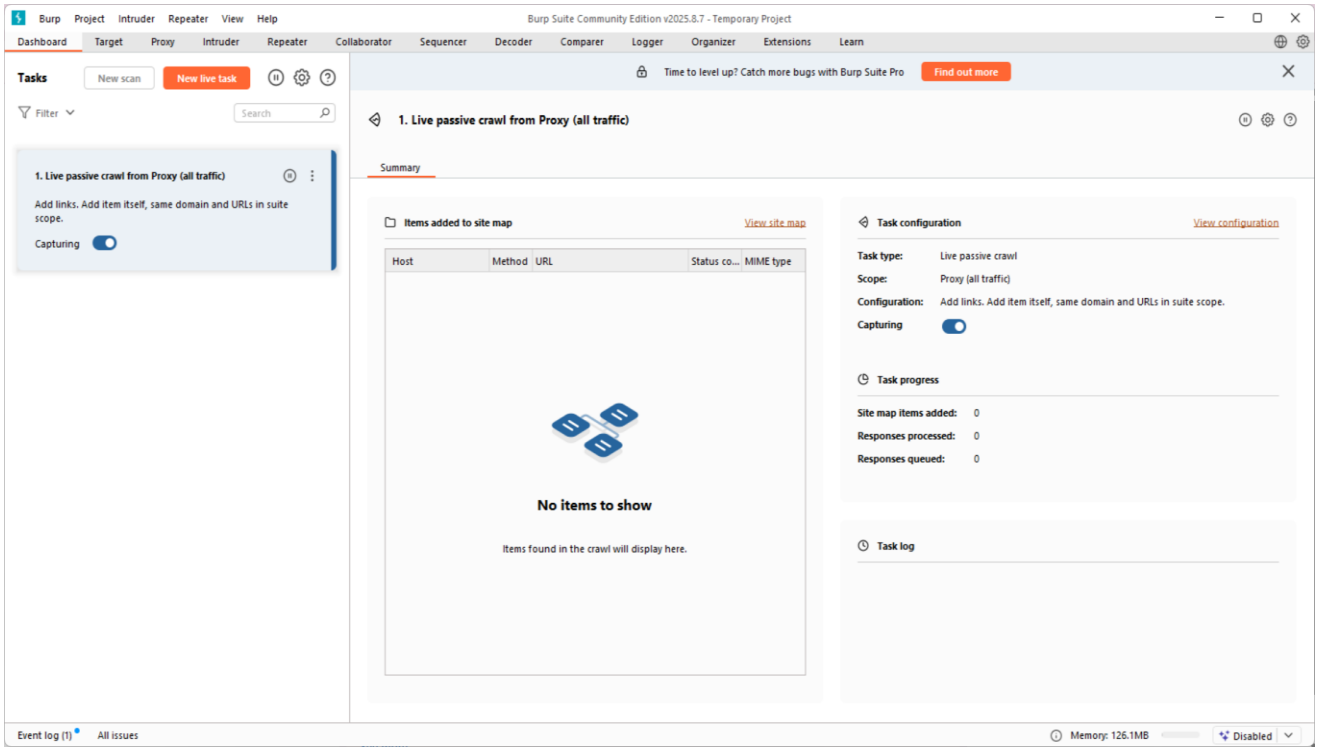
Intercept network traffic using Burp Suite and FoxyProxy to manipulate captured requests. Perform a dictionary attack through the Intruder module to demonstrate credential brute forcing.

STEPS with screenshots:

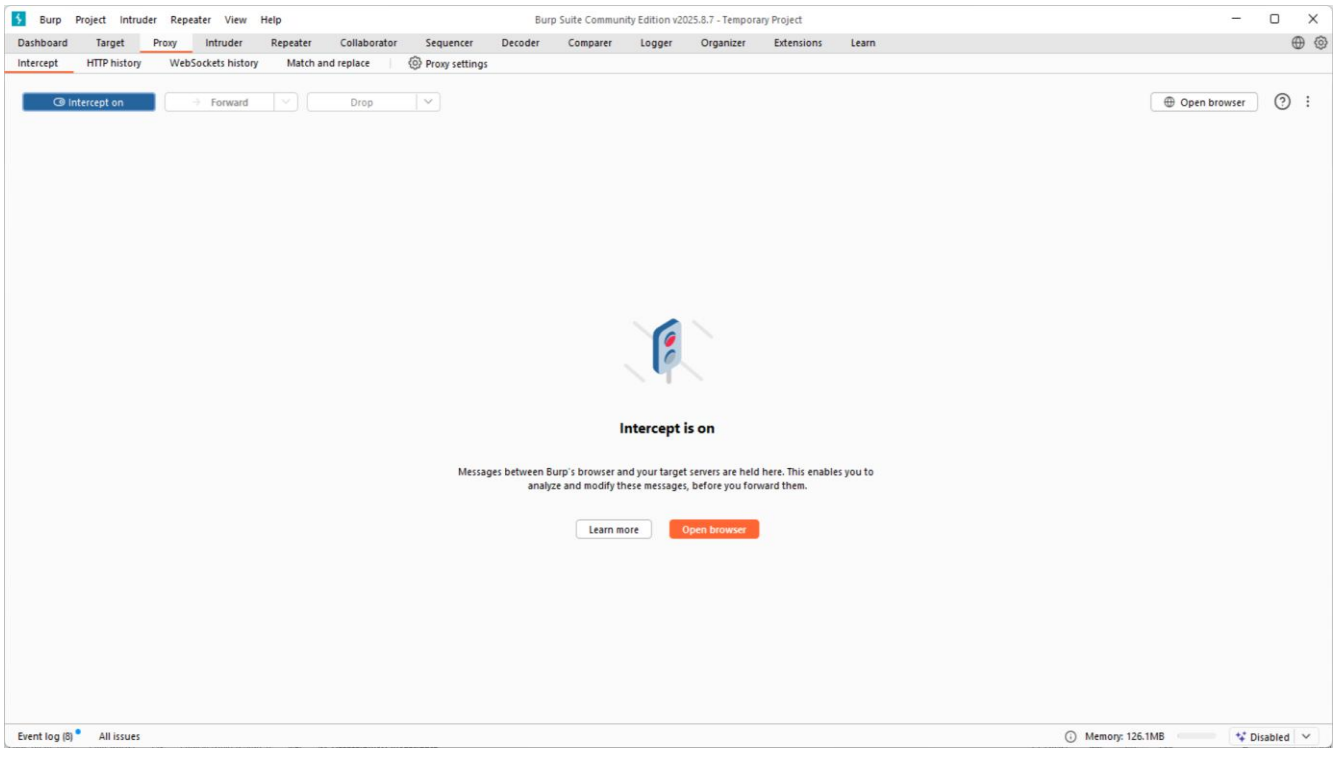
1) Start a forxy Proxy :



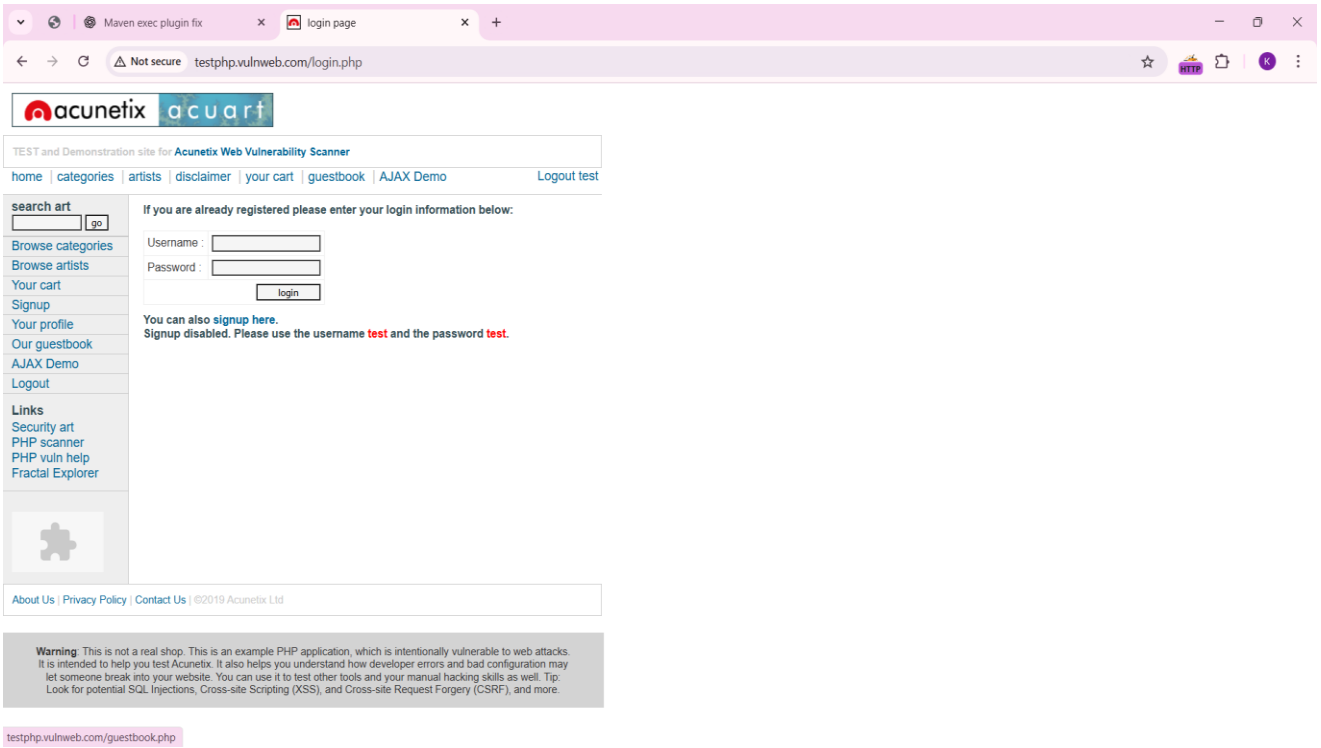
2) Start a brute suite :



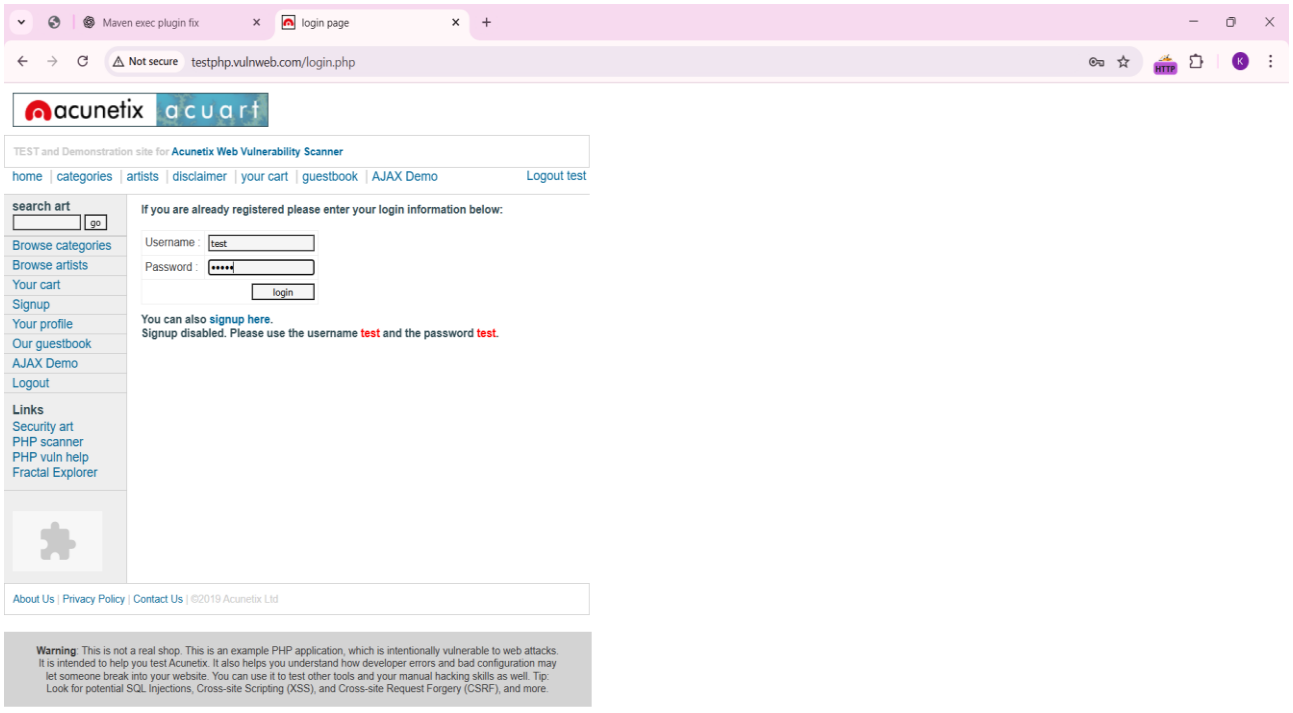
3) Turn on Intercept :



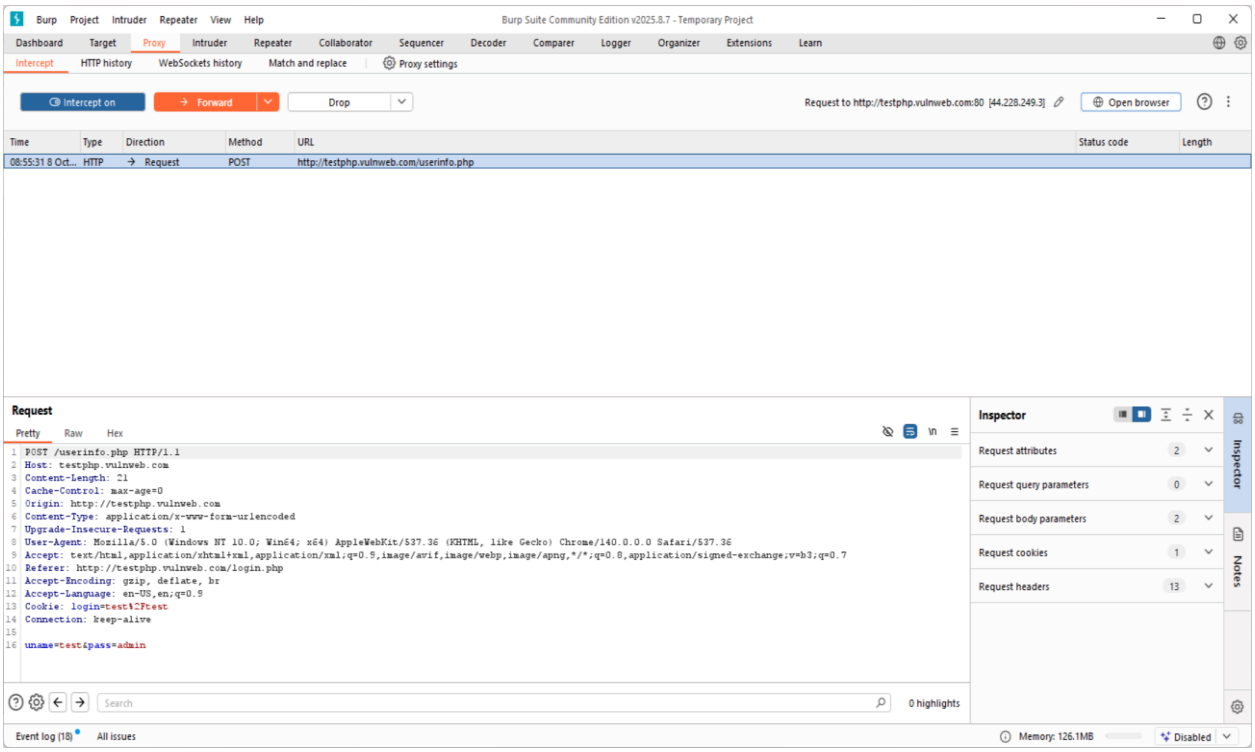
4) Select a any website :



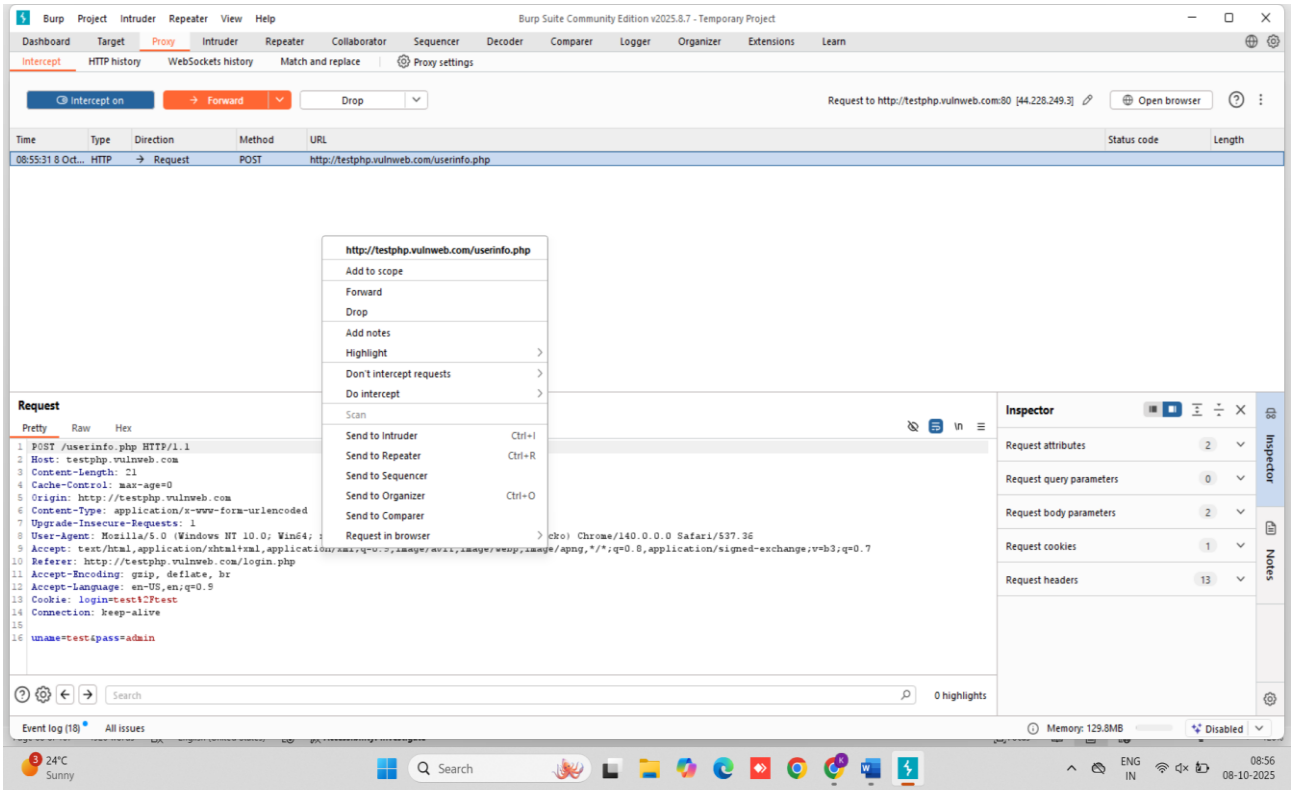
5) Enter username and password :



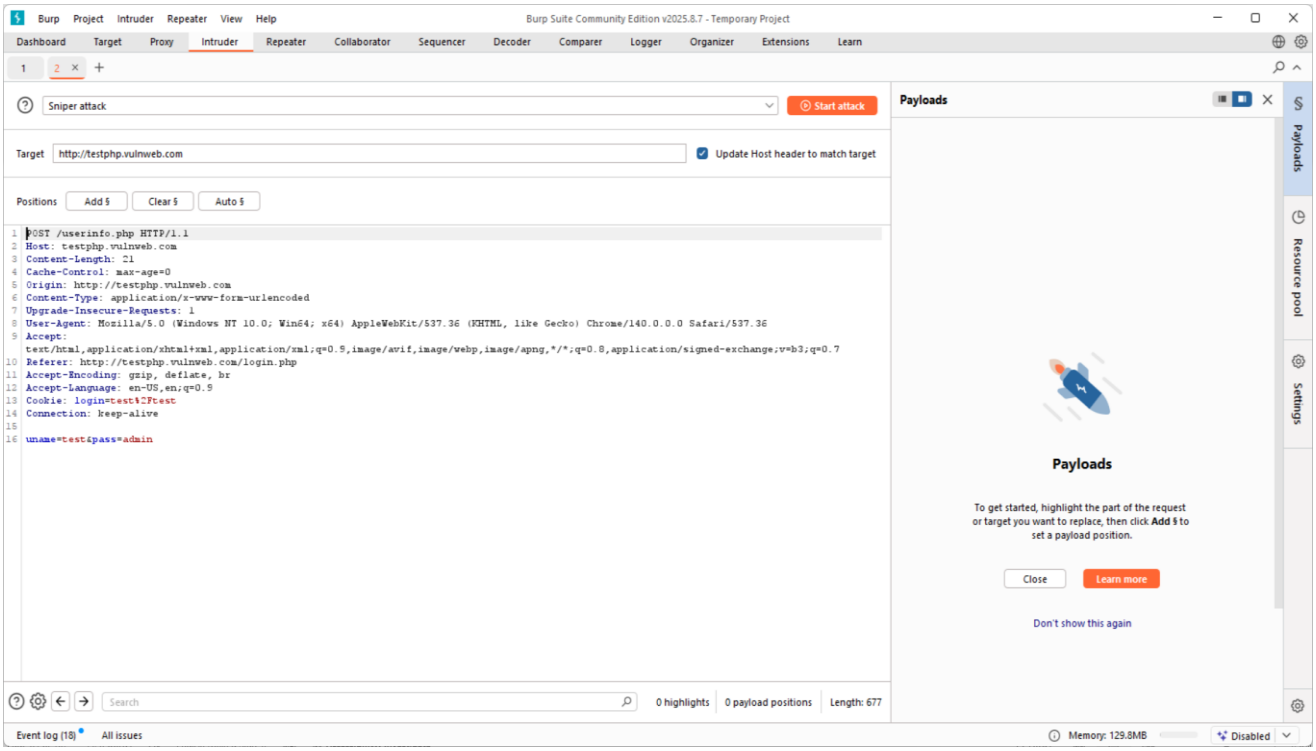
6) Chack a brup suite request:



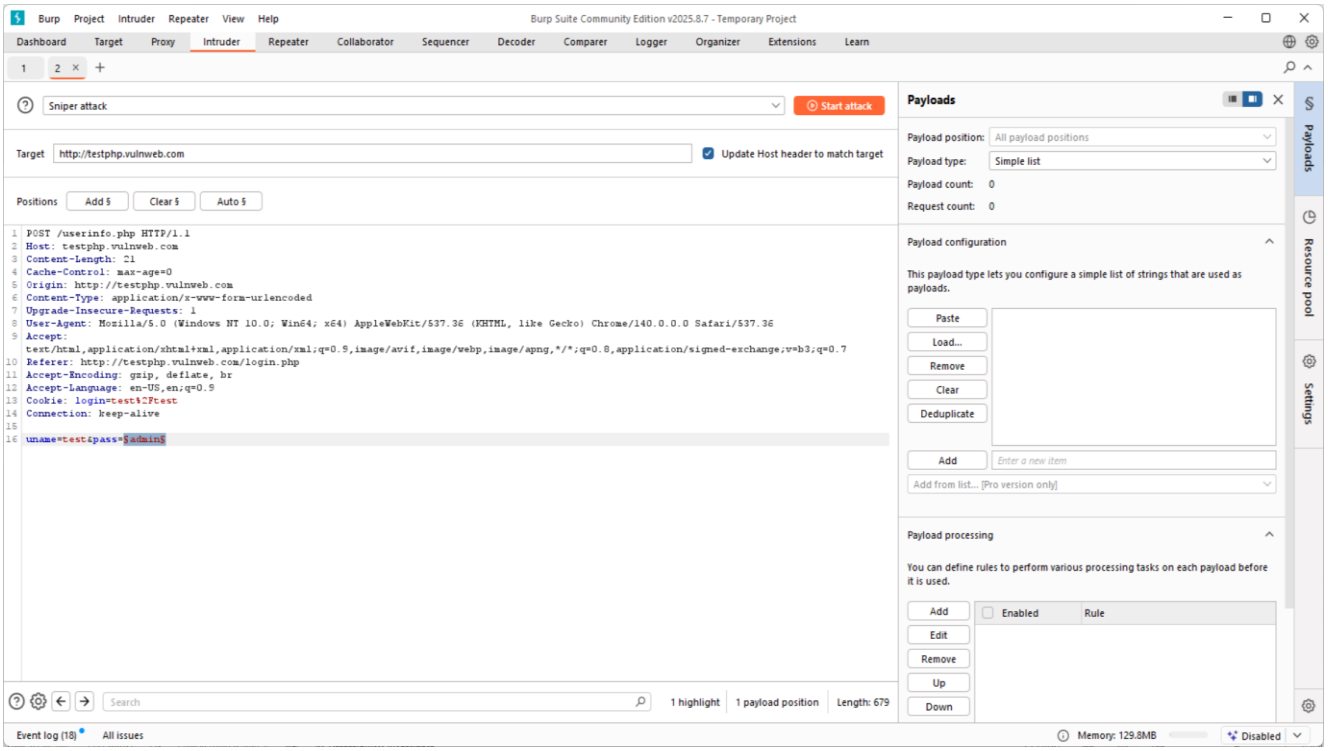
7) Right click and add intruder:



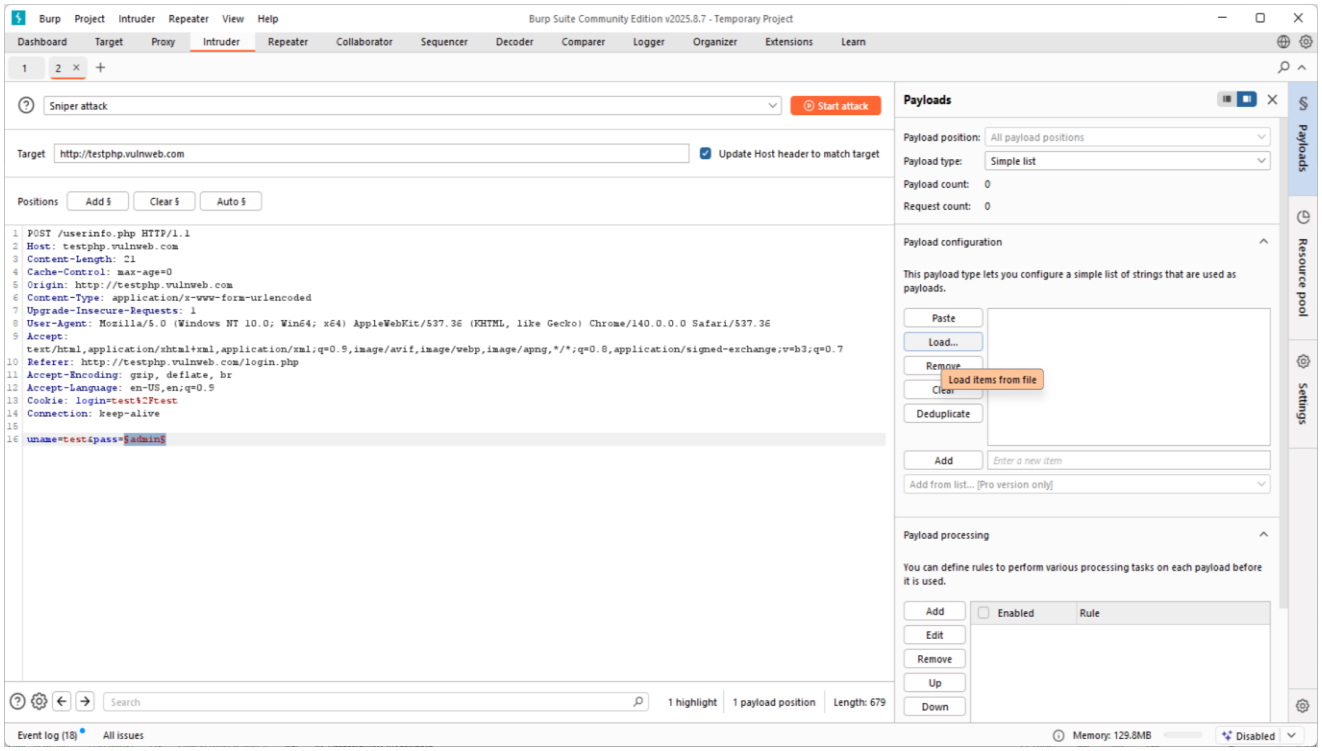
8) Chack a intruder page :



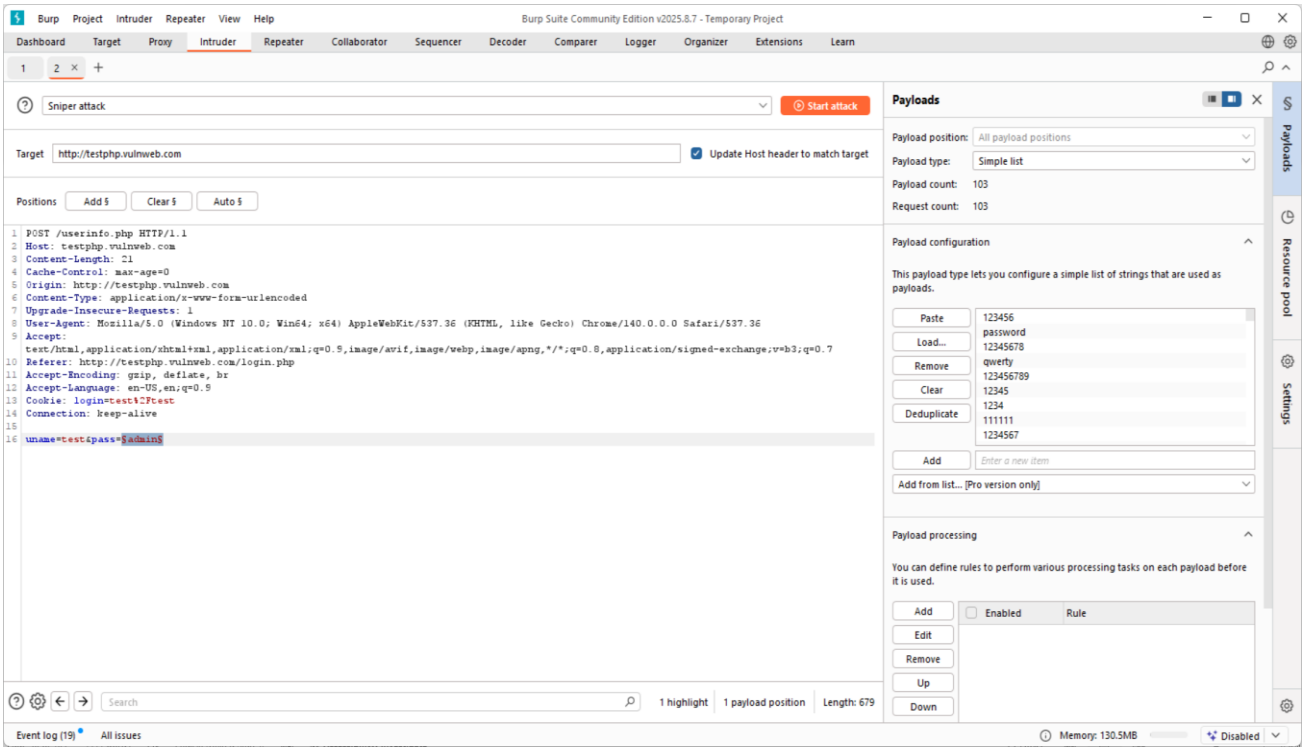
9) Assign to $ sign :



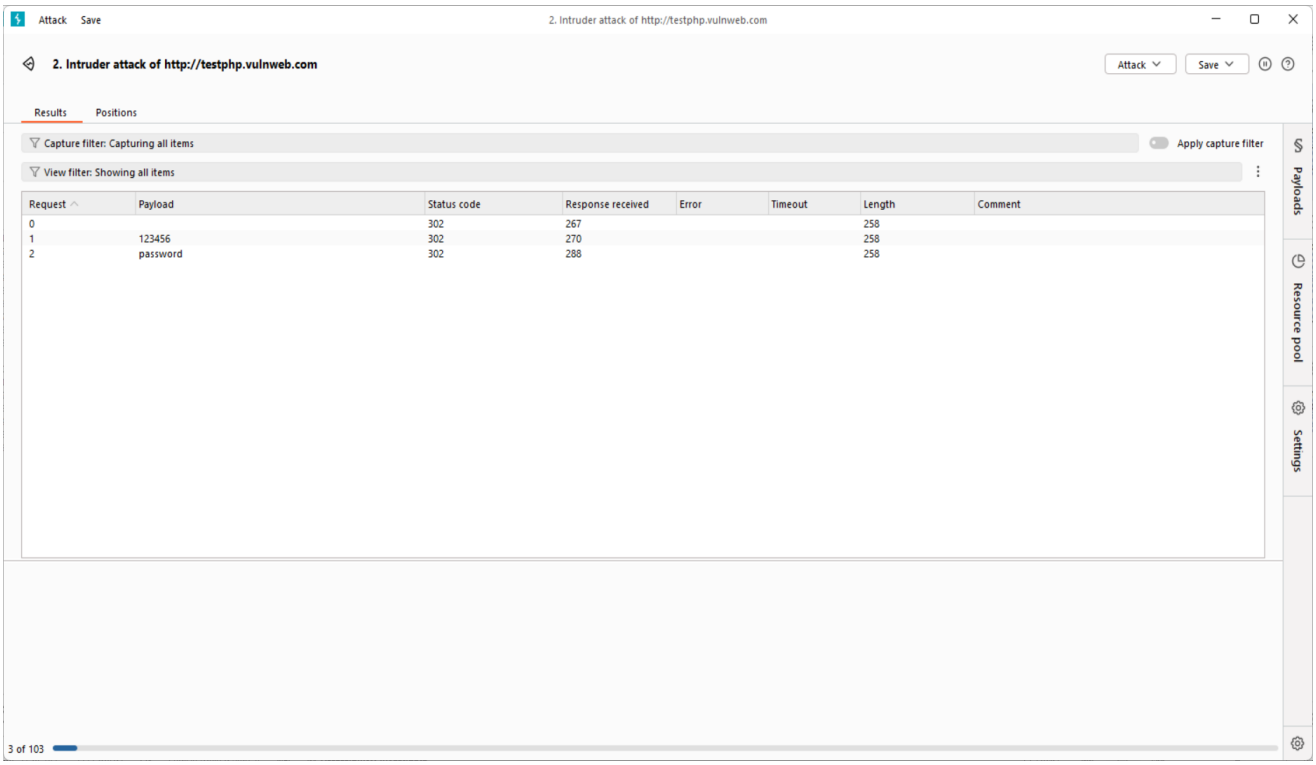
10)Load a Password file :



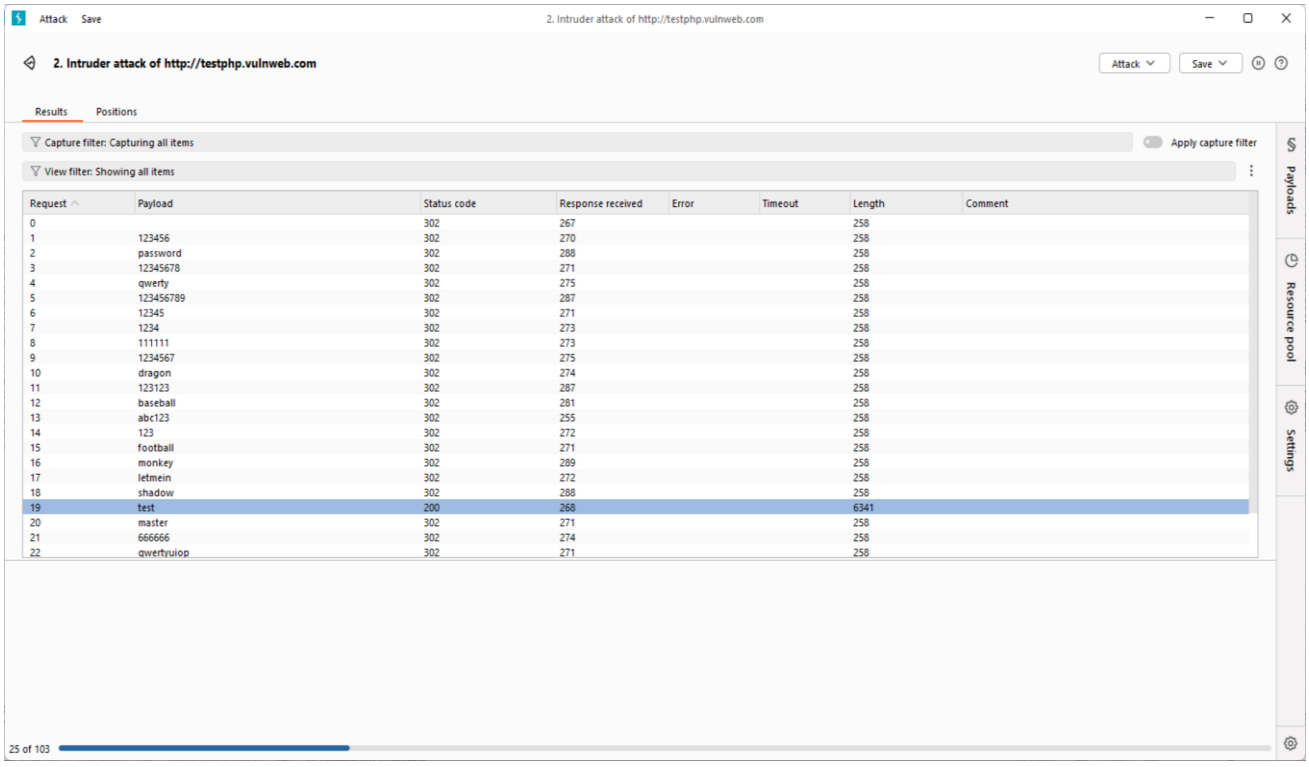
11)Now Start Attack :



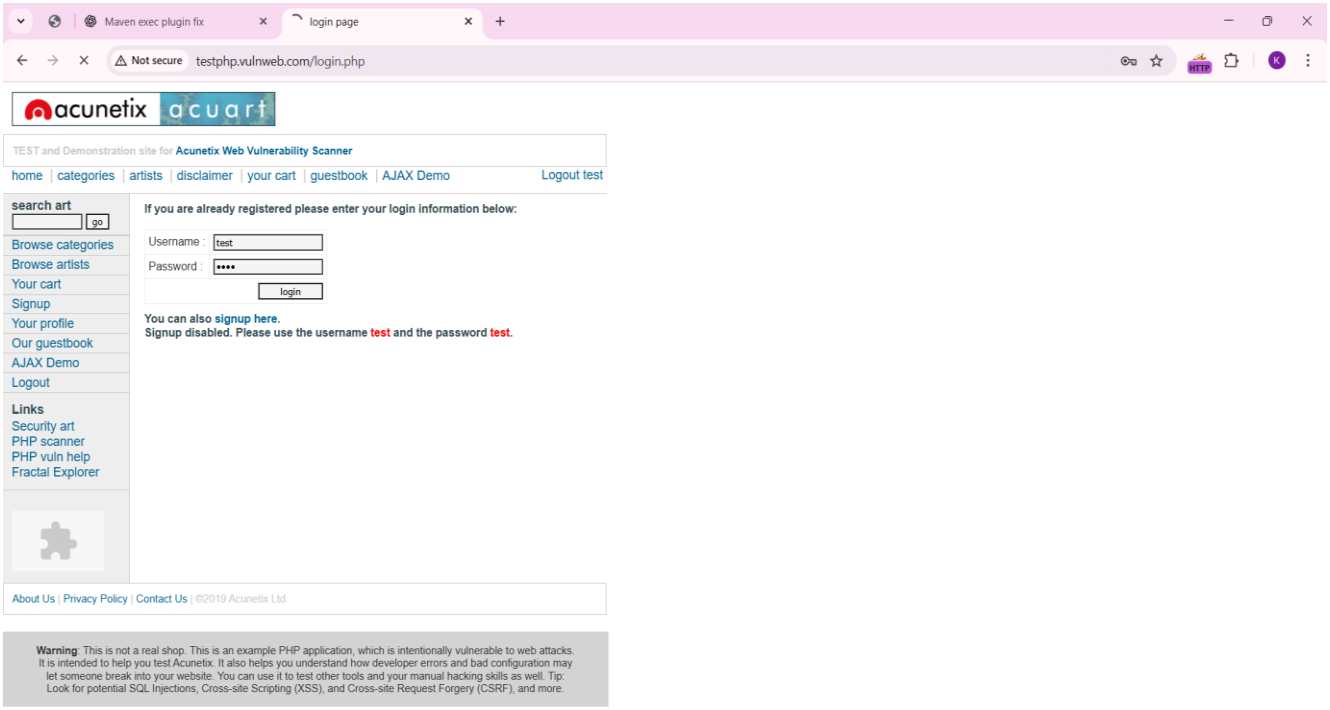
12)Started attack :



13)Password is creaked:



14)Relogin with password :



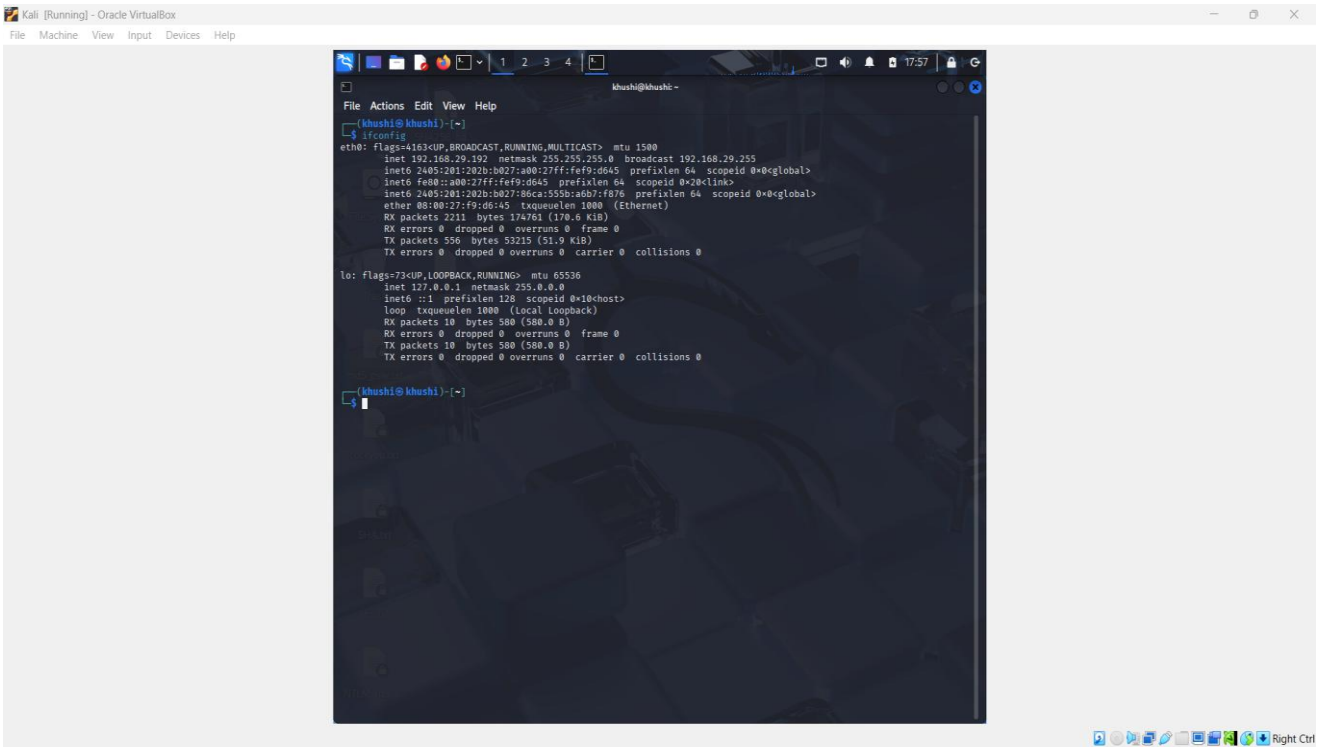
Practical-12

AIM:

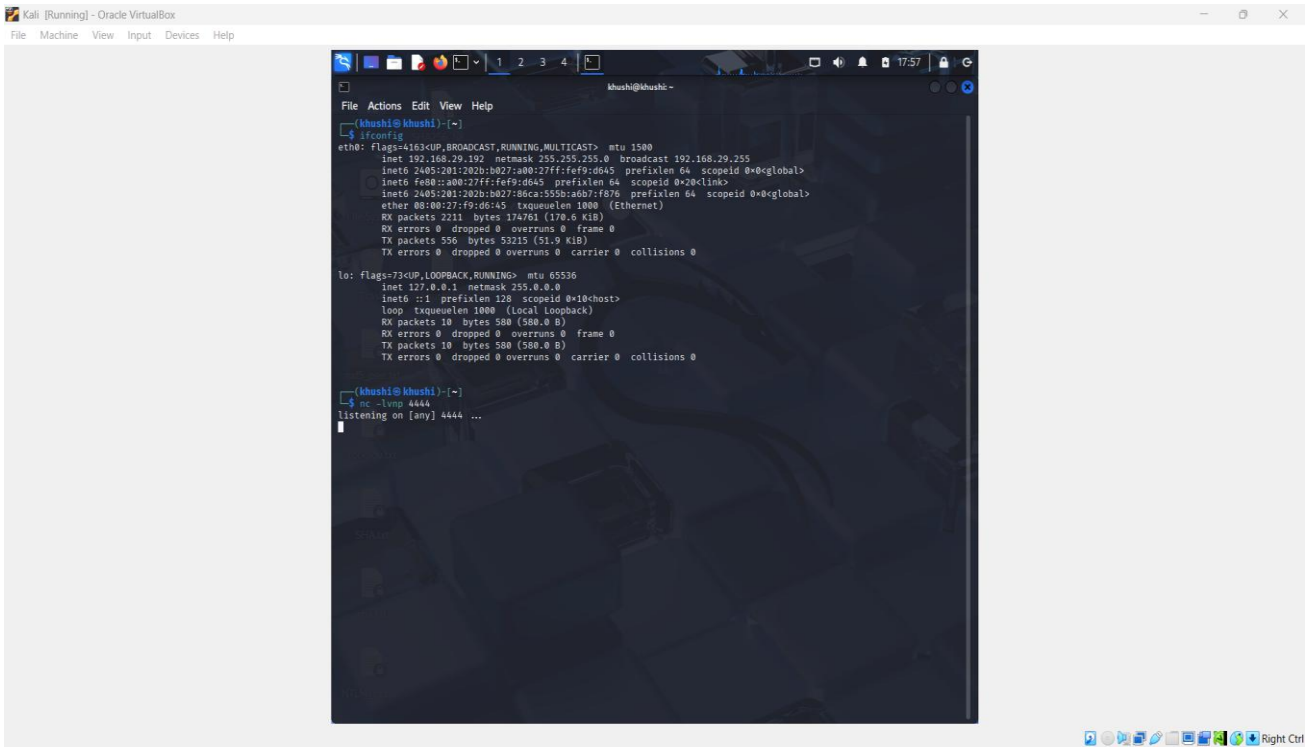
Use Netcat to simulate a reverse shell connection, demonstrating how attackers can gain unauthorized remote access to a victim system through network exploitation.

STEPS with screenshots:

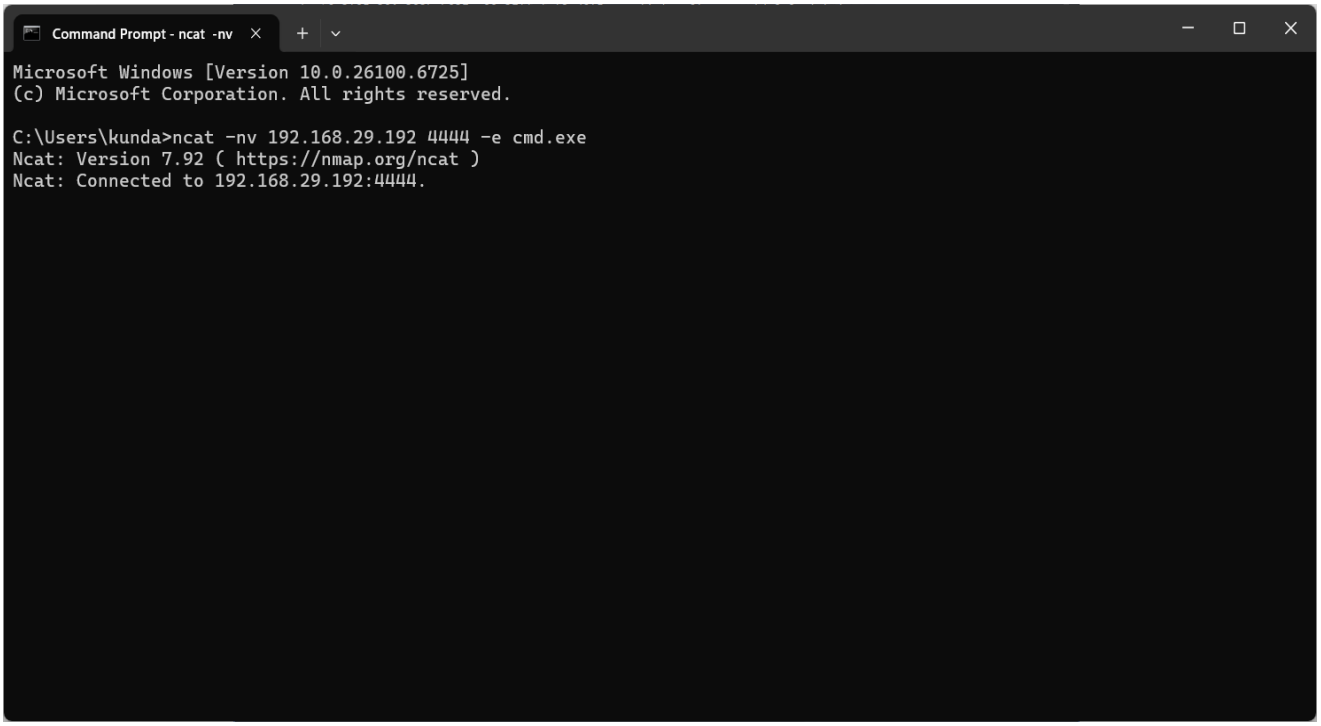
1) Find IP Address:



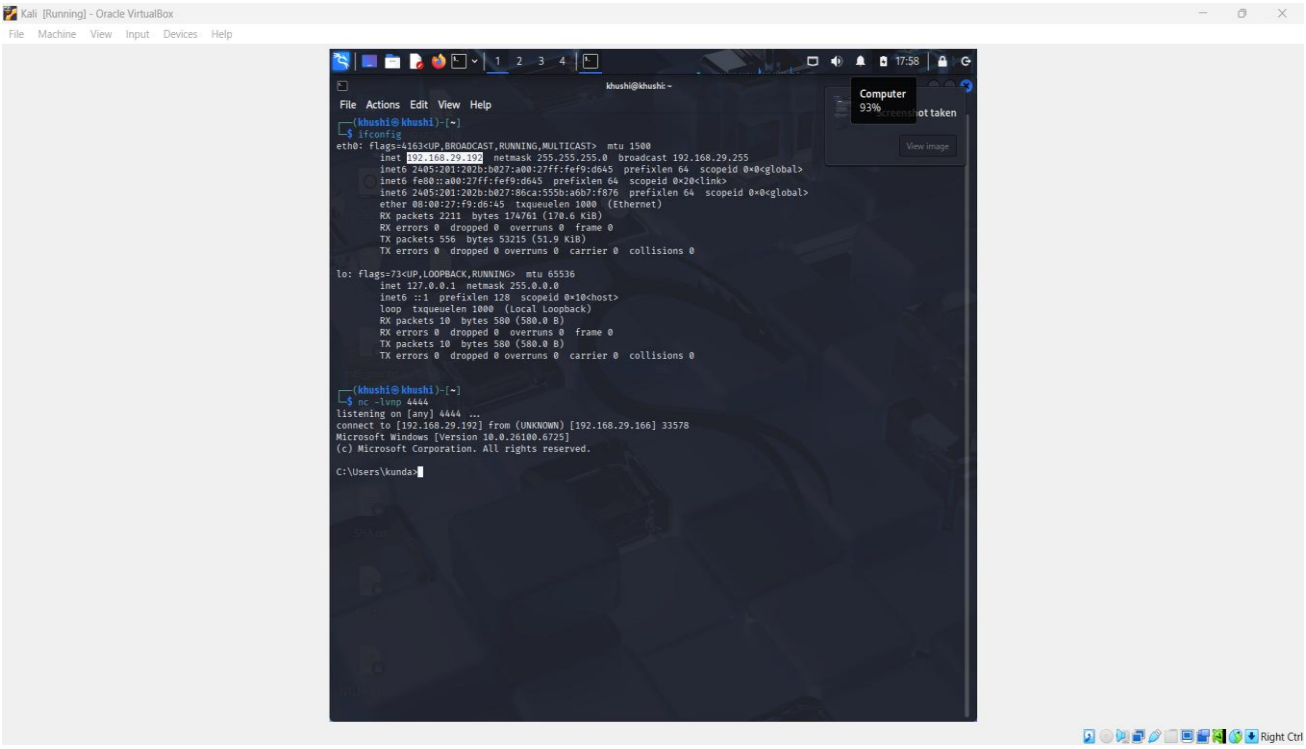
2) Nc -lvnp 4444:



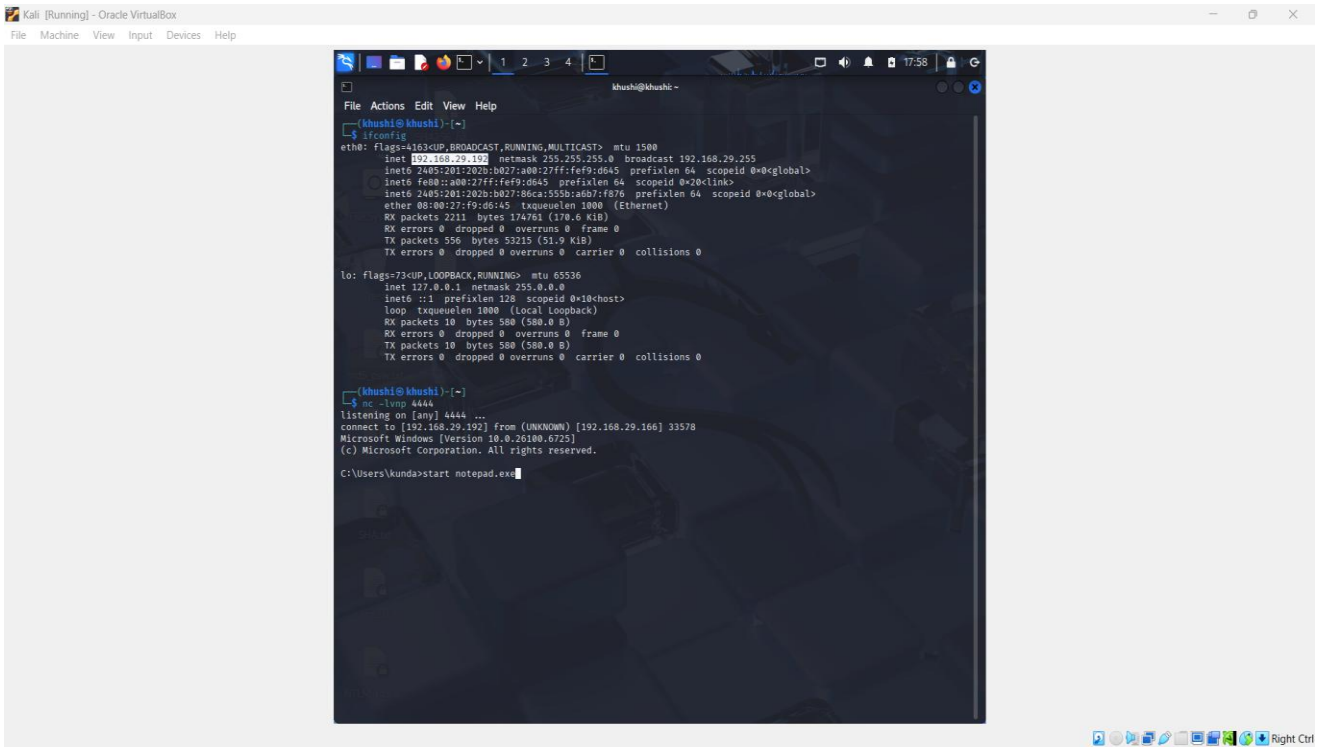
3) Window Cmp :



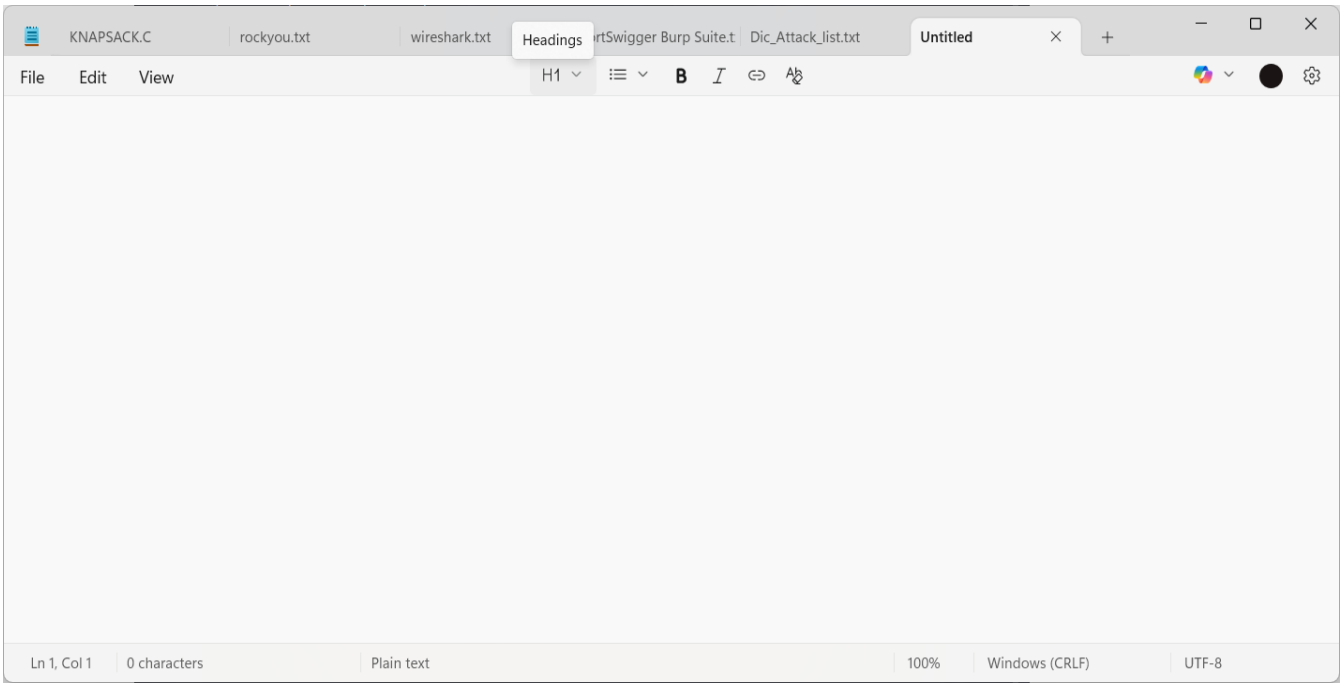
4) Connection done:



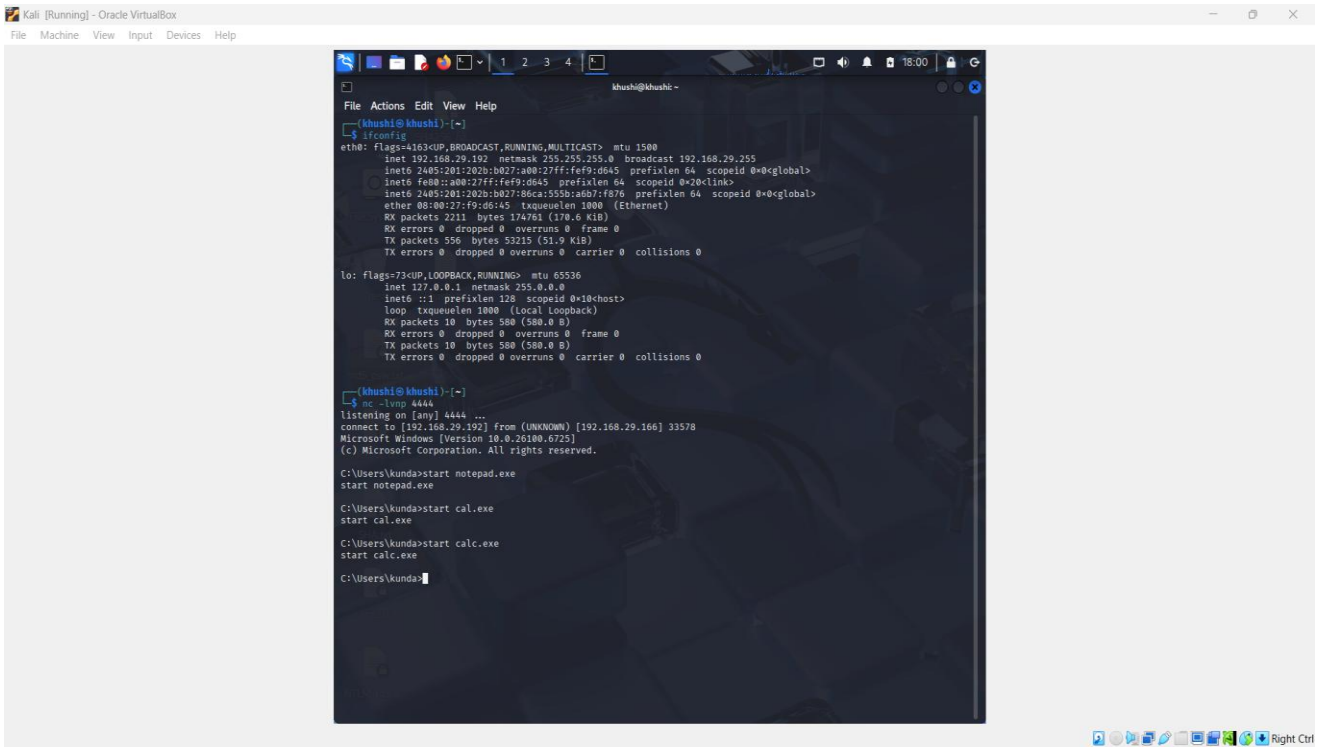
5) Start notepad :



6) Notepad :



7) Start calc:



8) Cal:

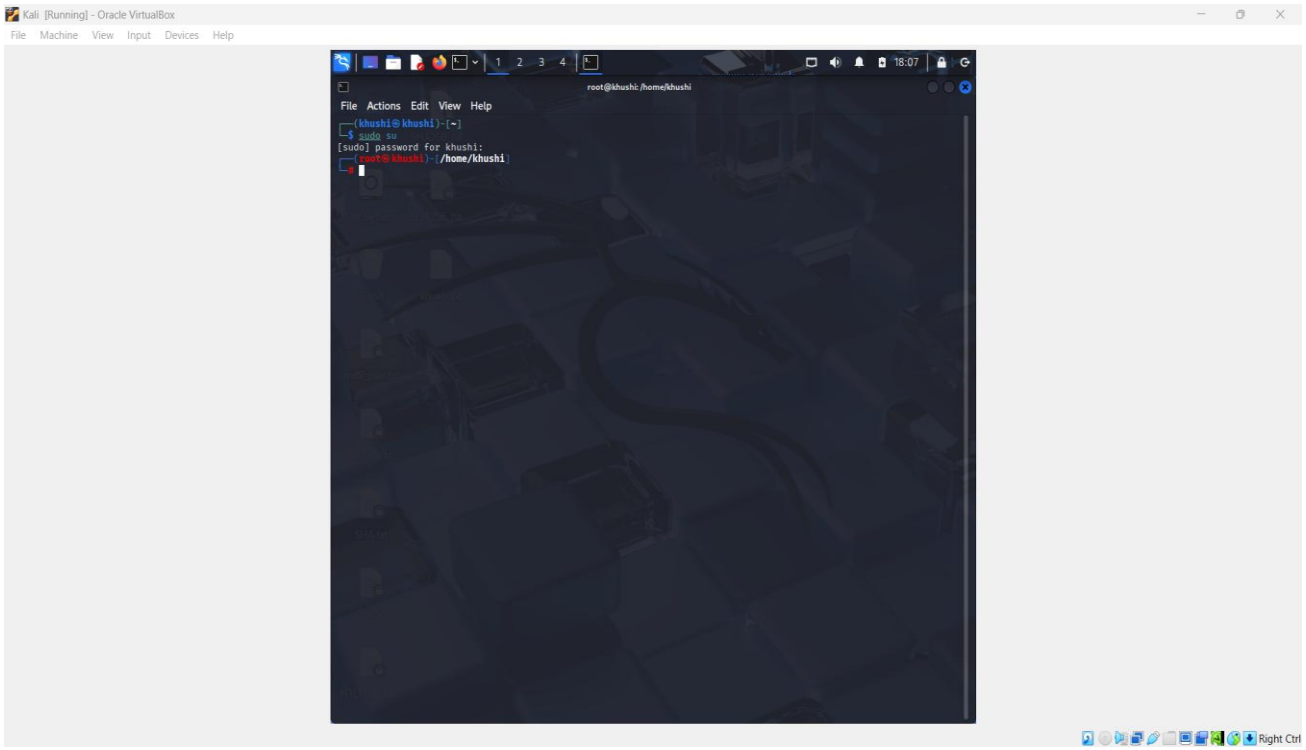
Practical-13

AIM:

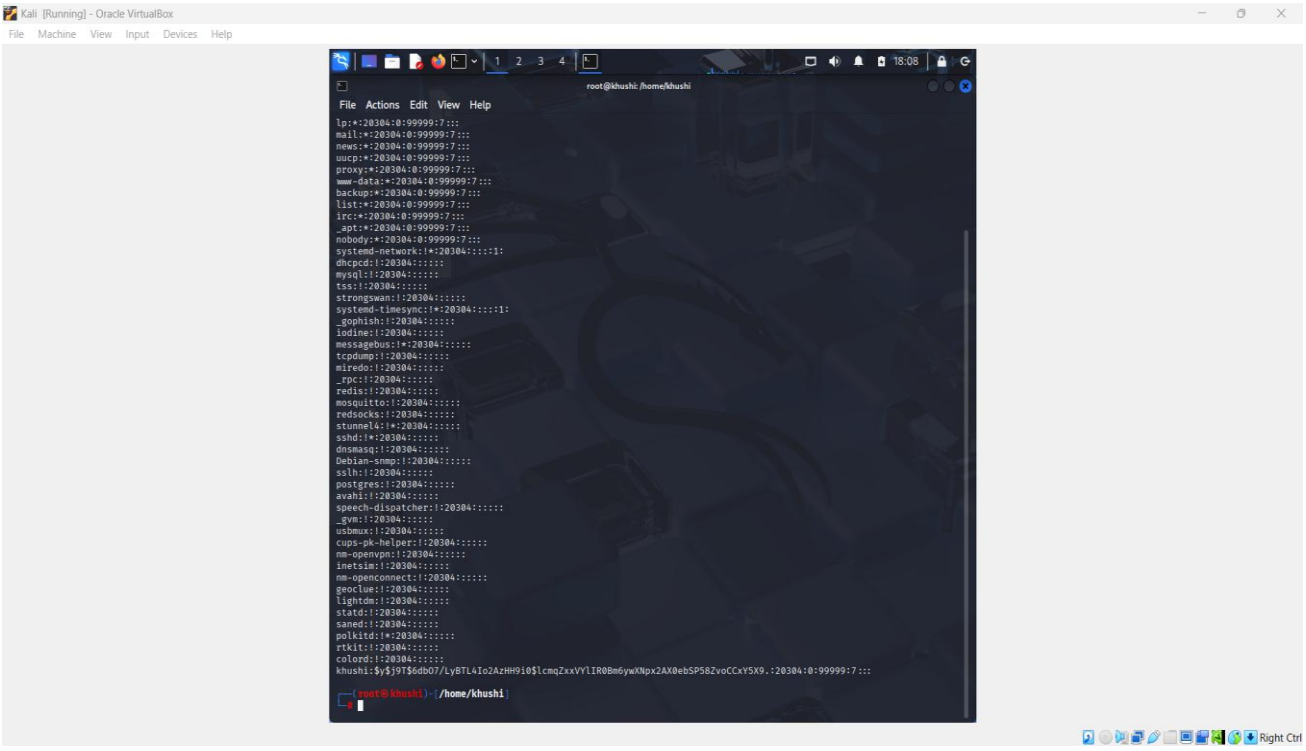
Perform password cracking on hashed credentials using John the Ripper to demonstrate how weak or exposed passwords can be compromised through offline attacks.

STEPS with screenshots:

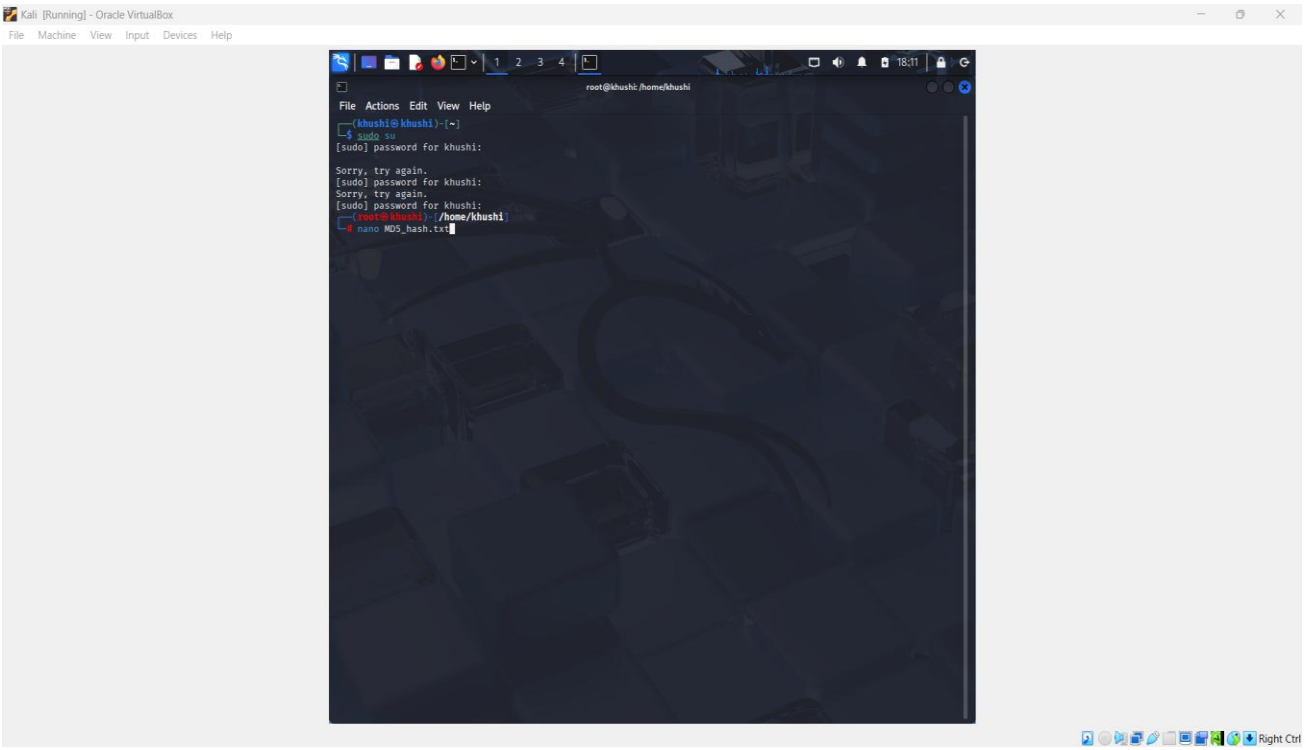
1) Start a root node :



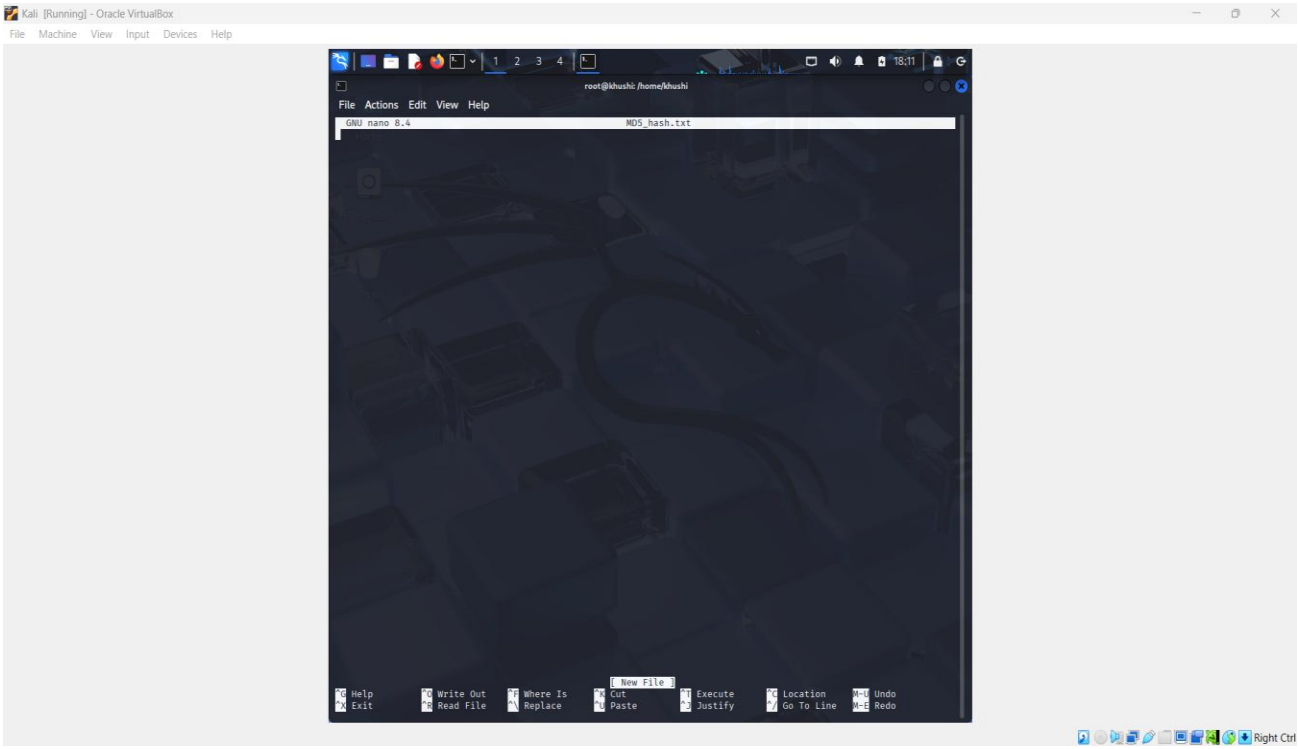
2) Find a kali linux password :



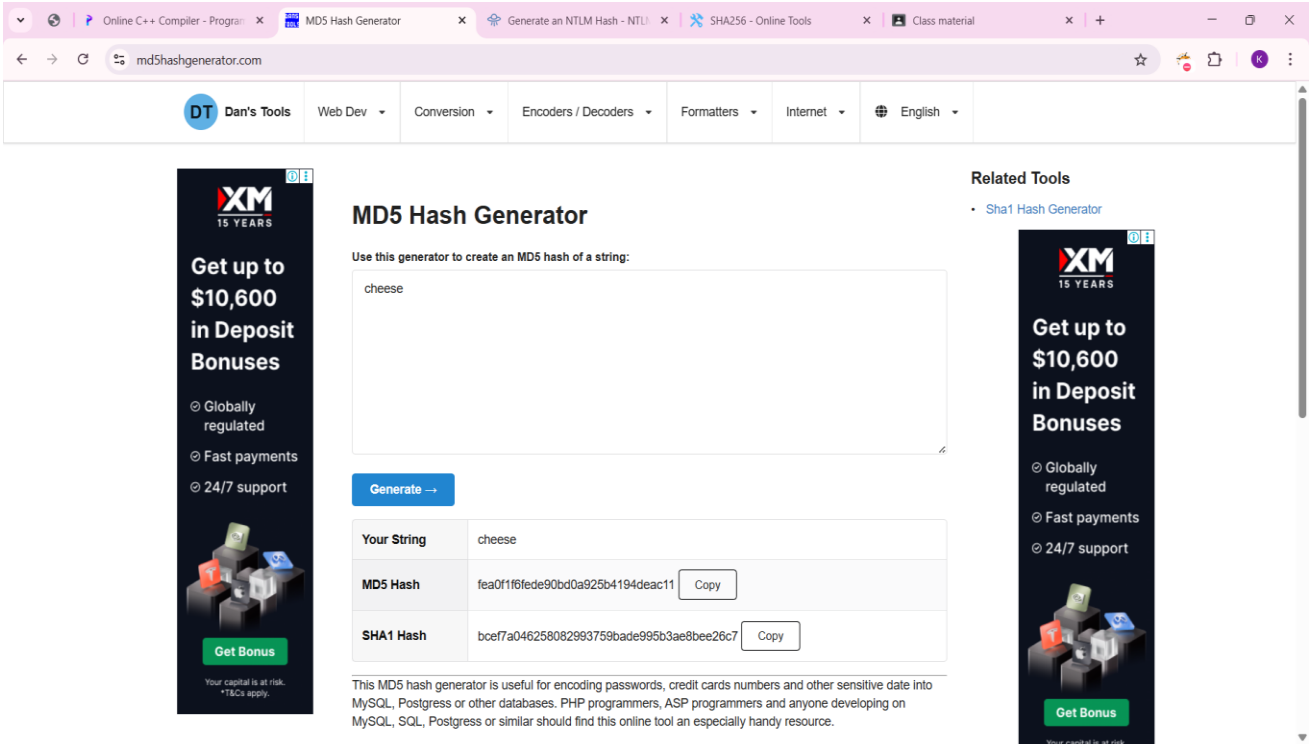
3) Create a MD5_hash.txt file:



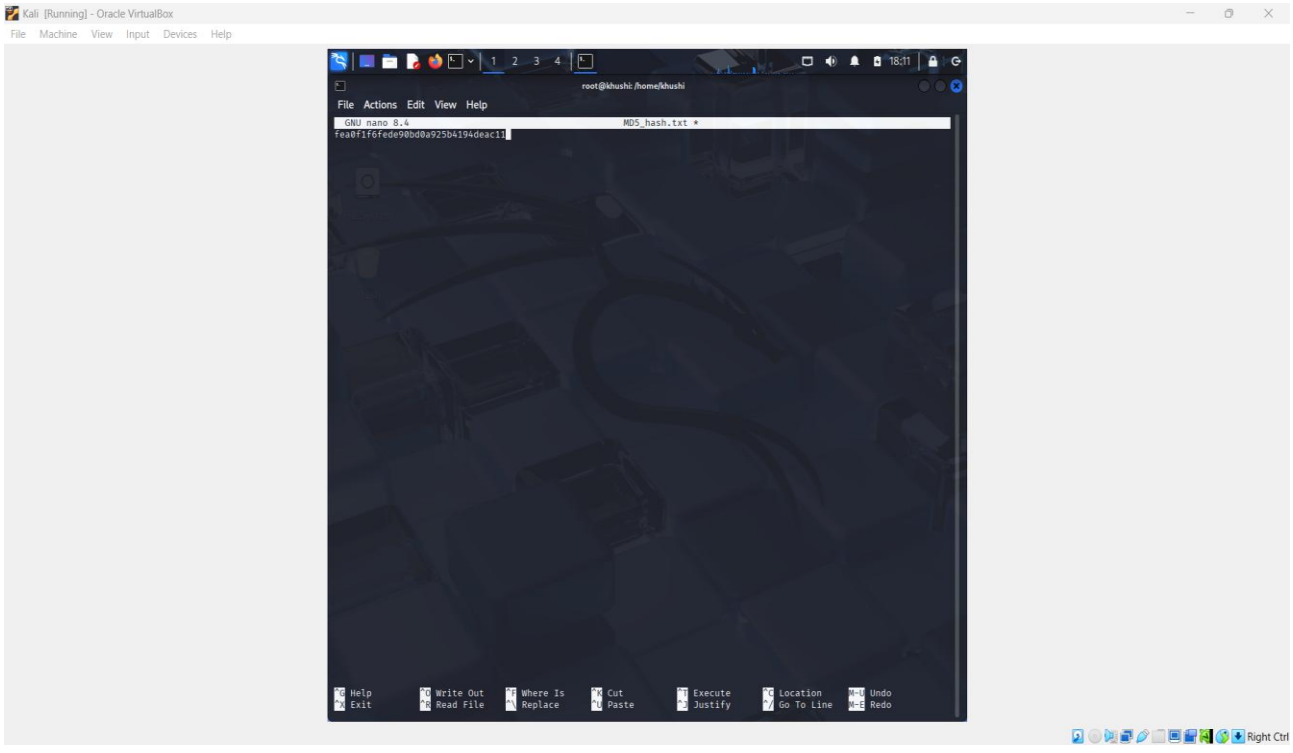
4) Write a hashing password and save and exit:



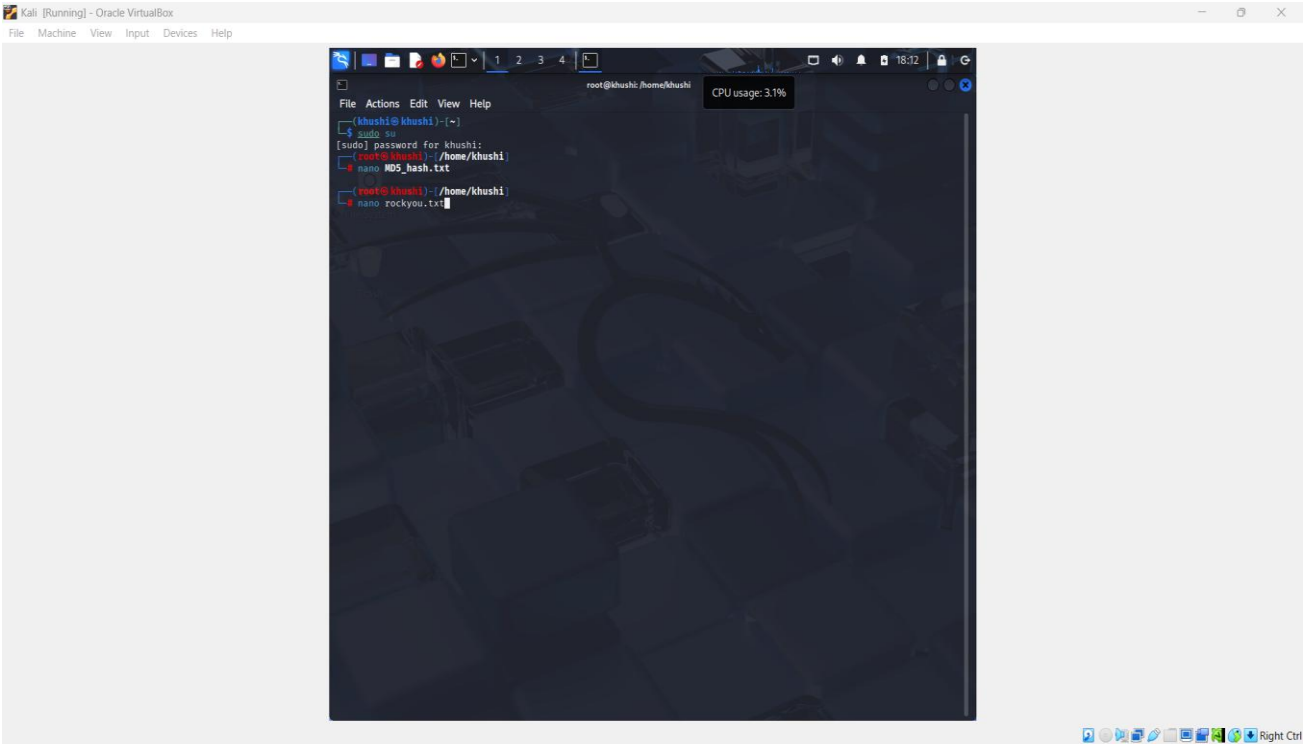
5) MD5 Hash Generator:



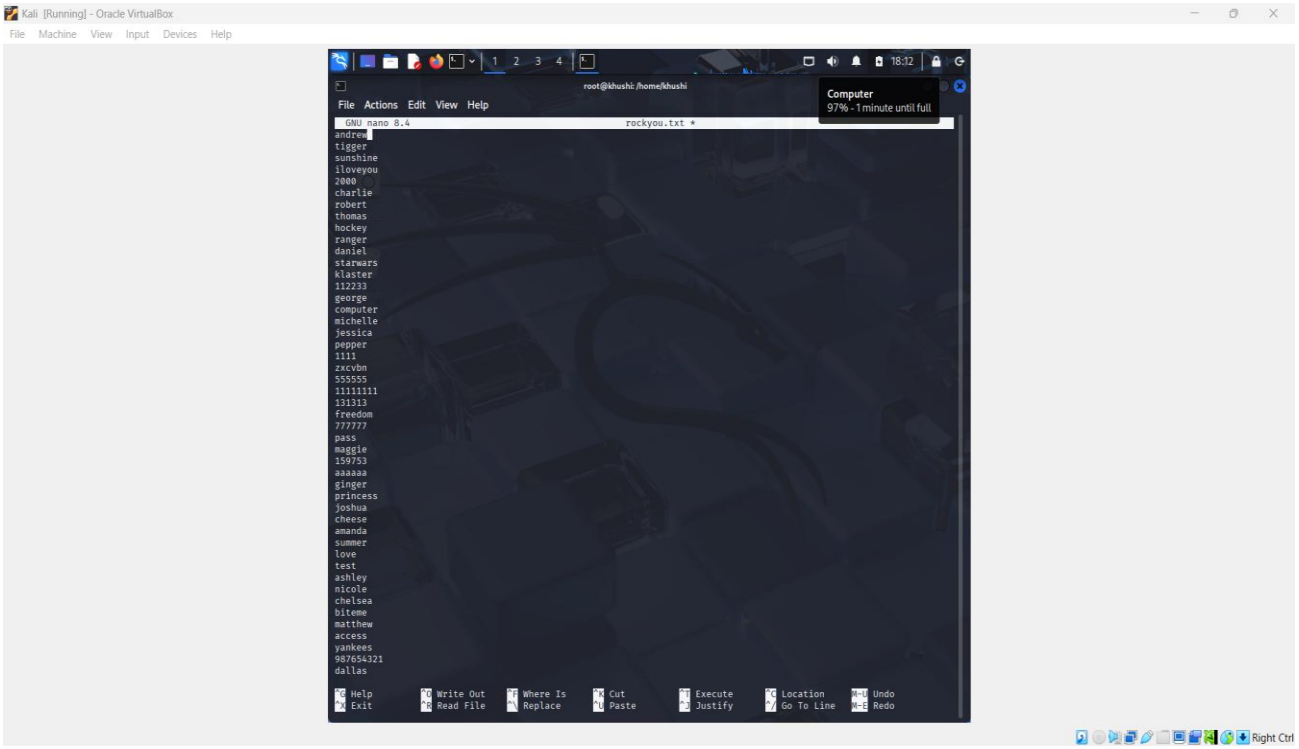
6) Save hash Password in file:

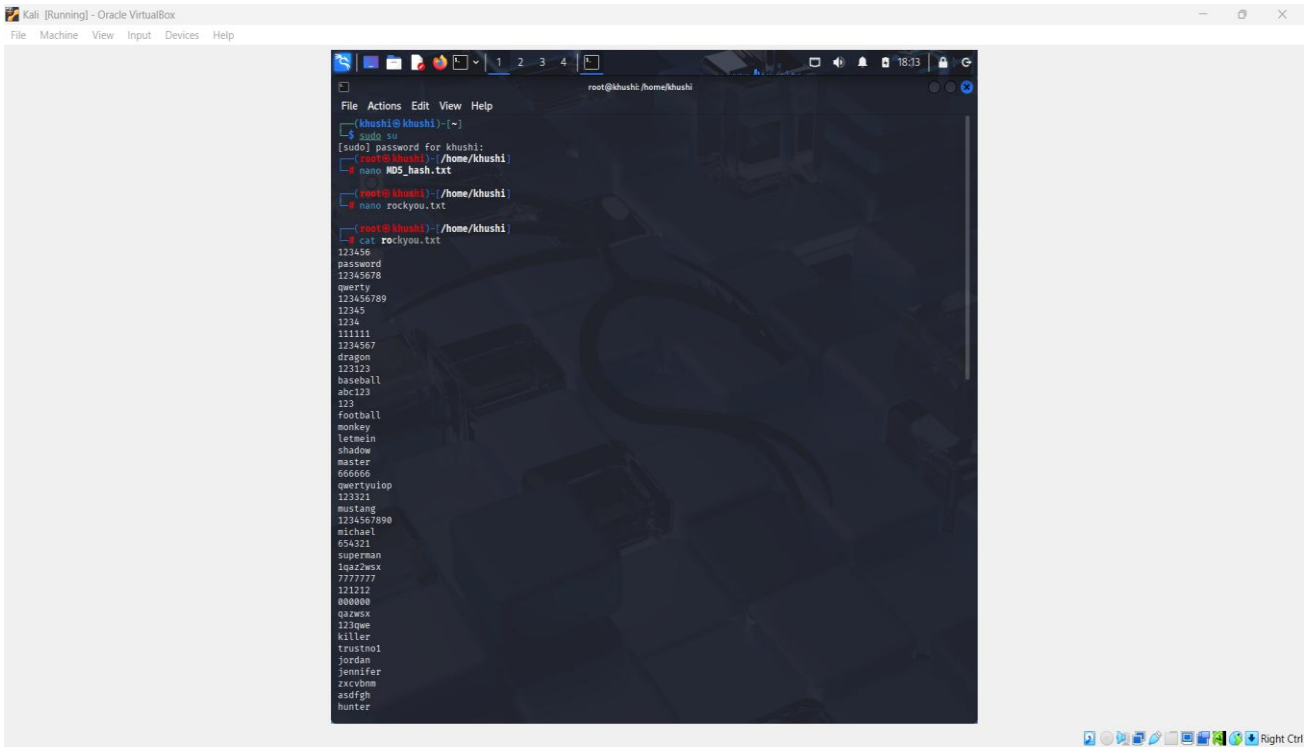


7) Create a List of Password:

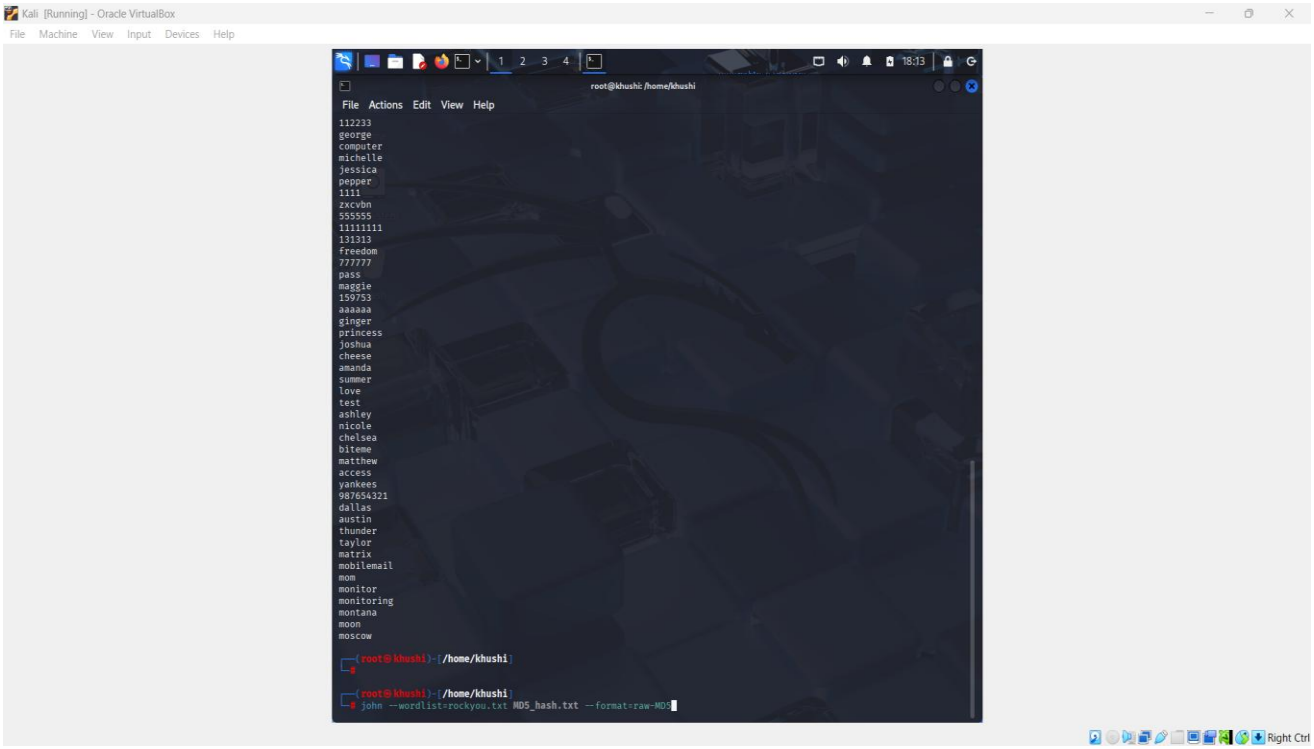


8) Save a List of Password :

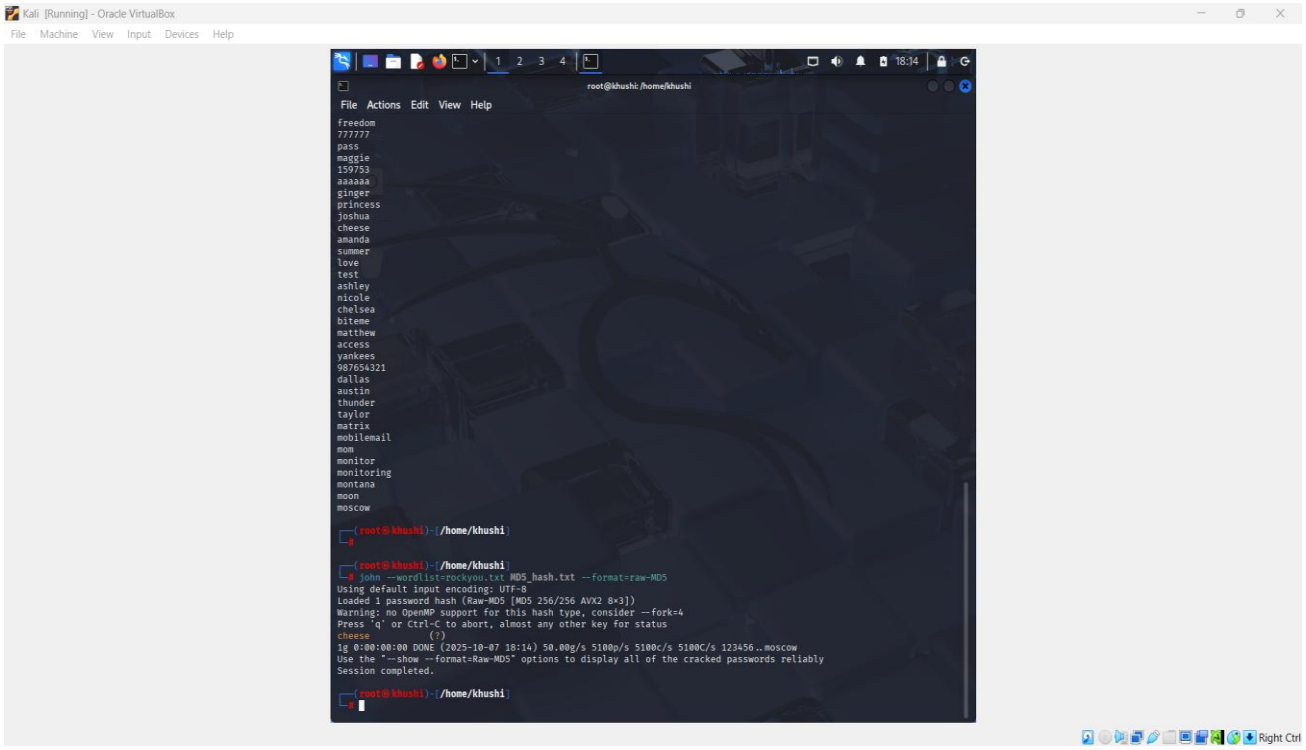




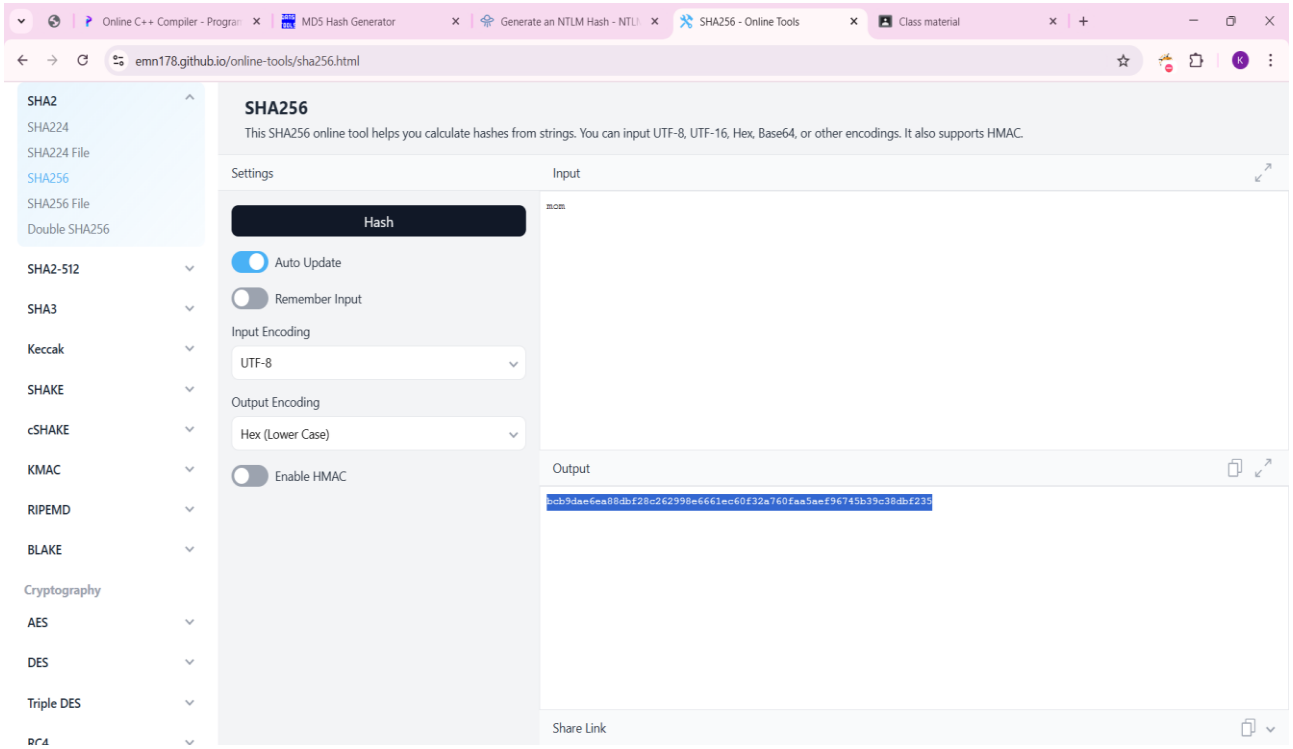
9) Crack password:



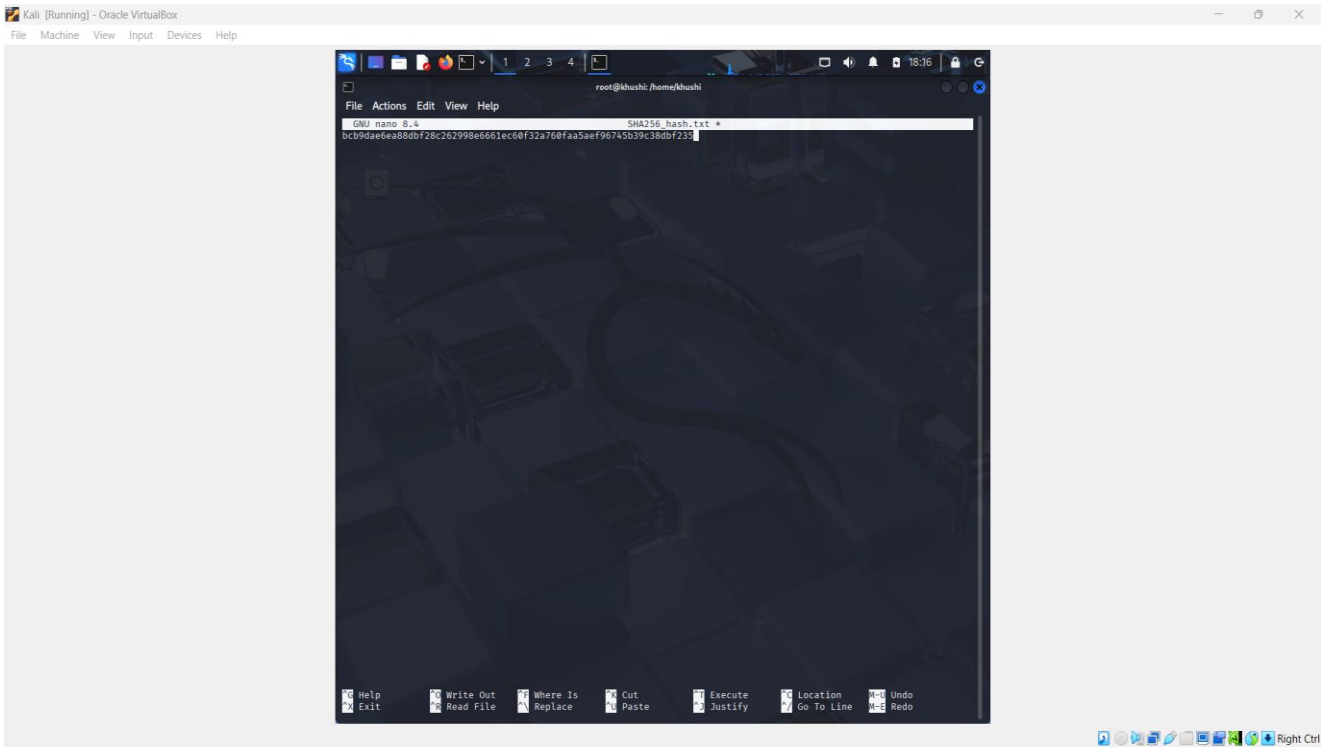
10) Password is Cracked :

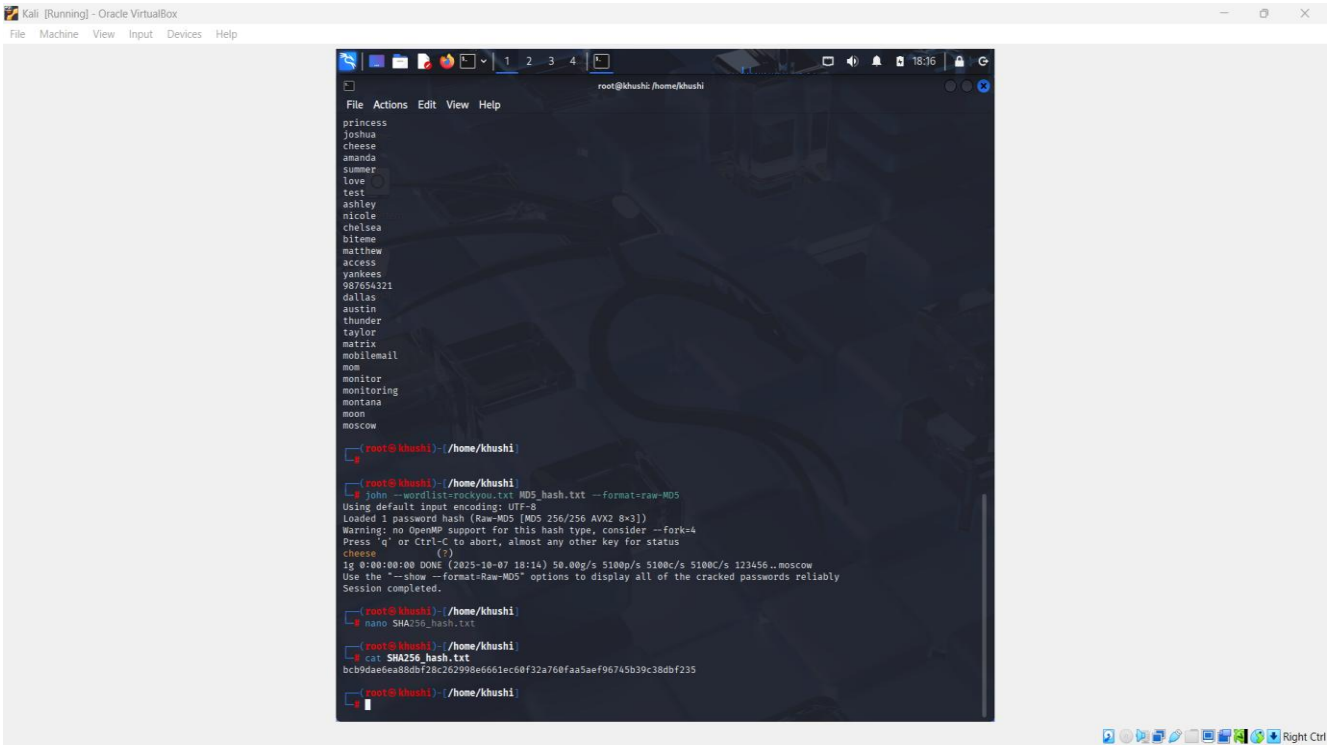


11) SHA256 Converter :

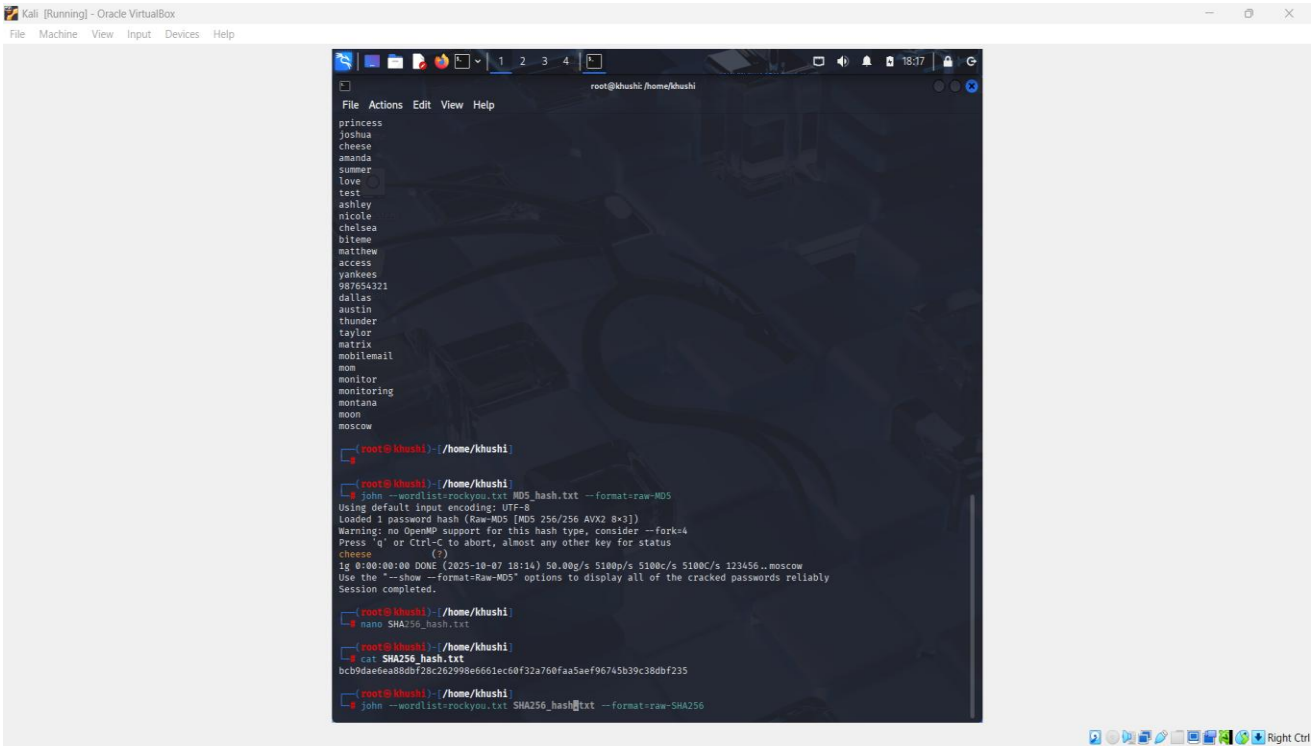


12)Create a SHA256_hash.txt file:

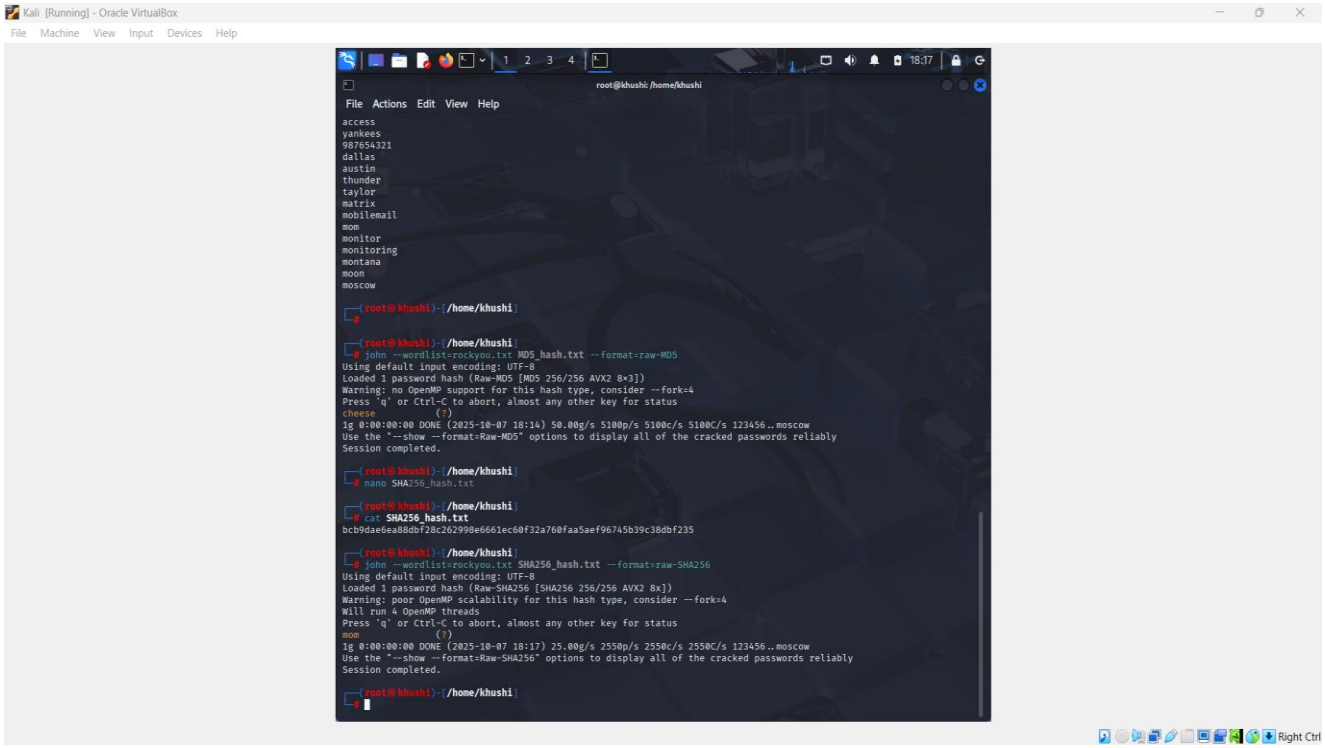




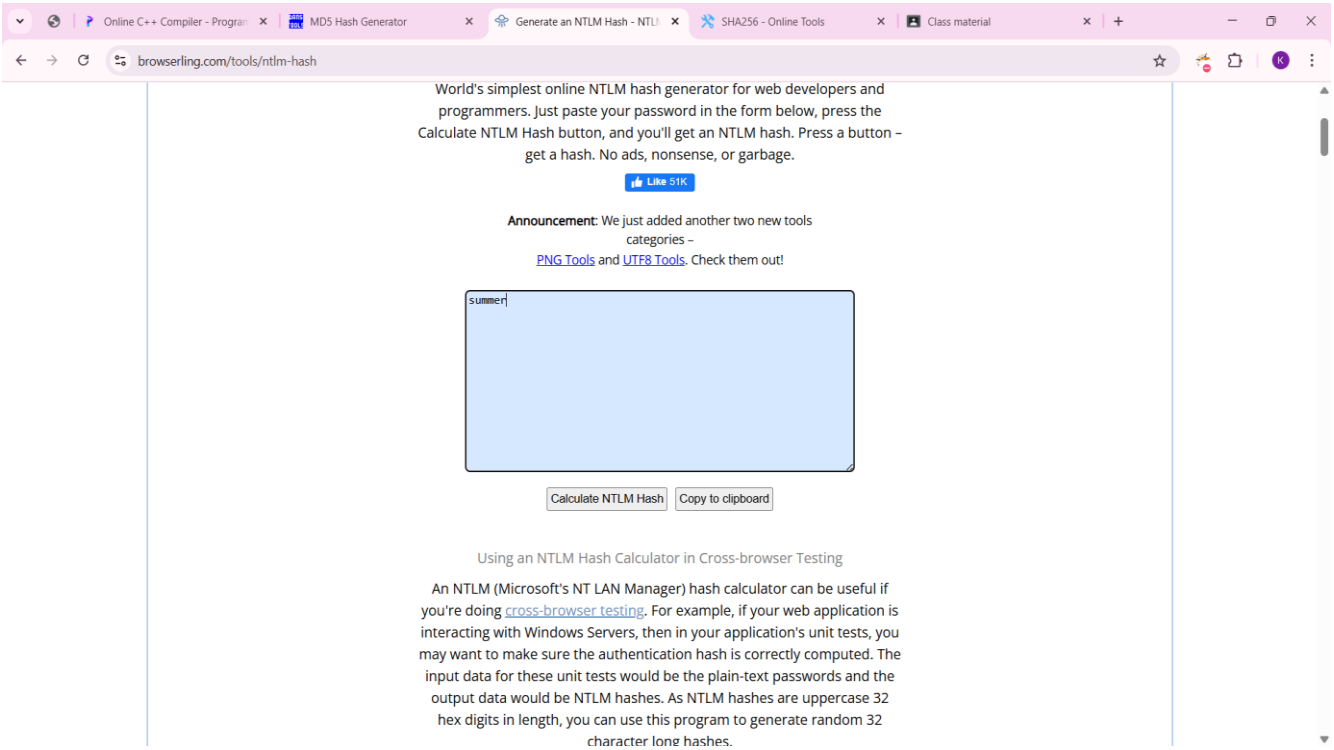
13)Crack password:

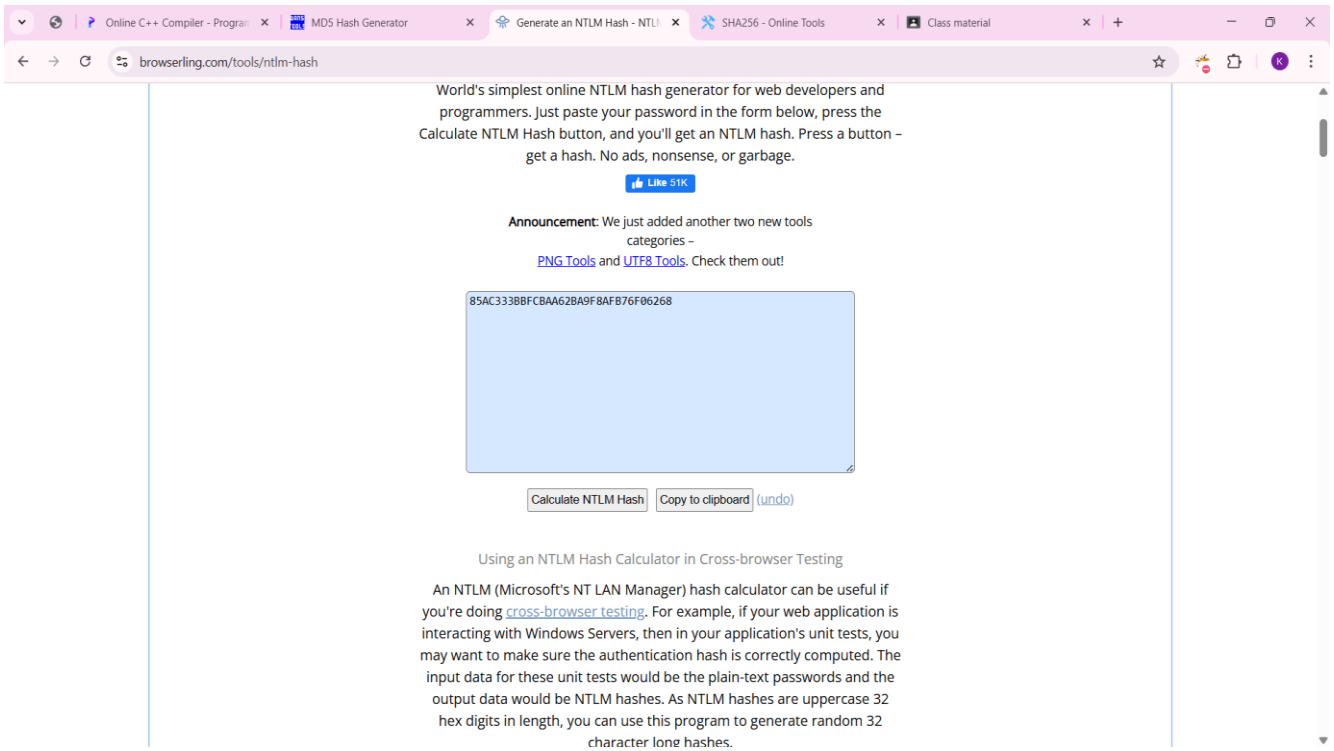


14)Password is Cracked :

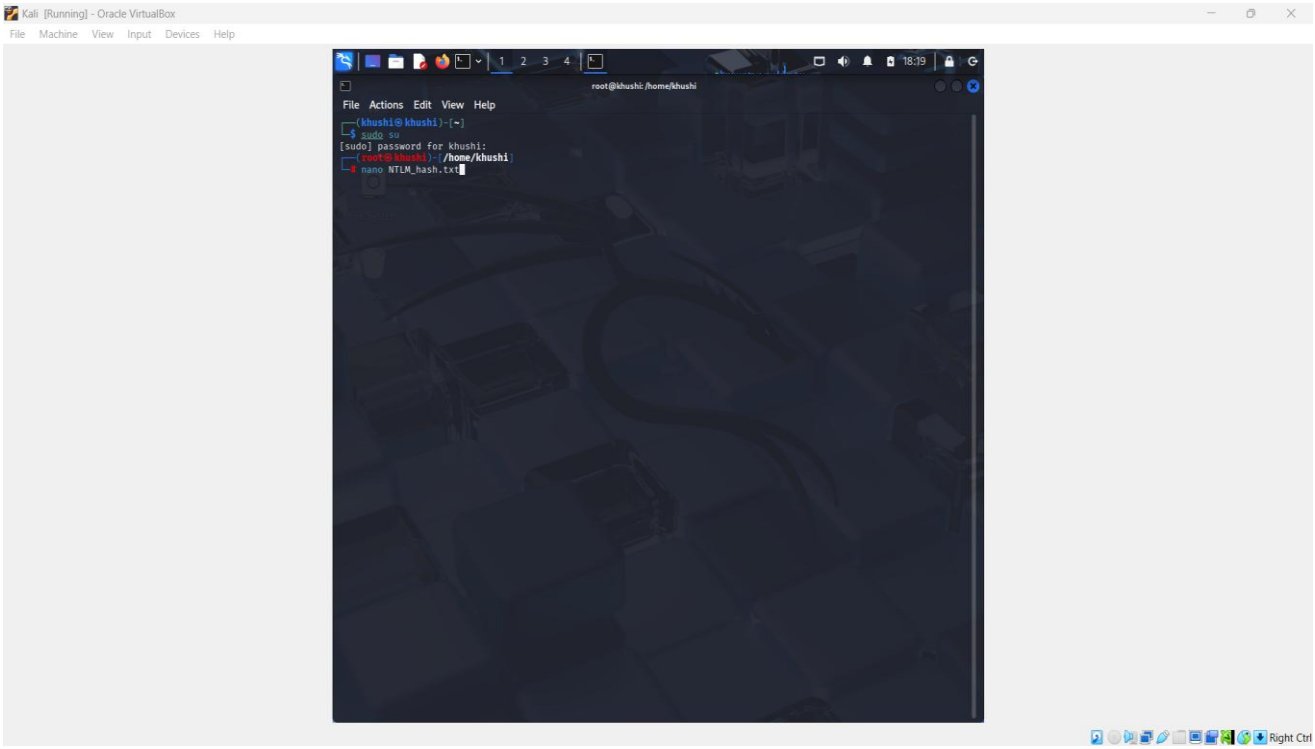


15)NTLM Hash Converter :

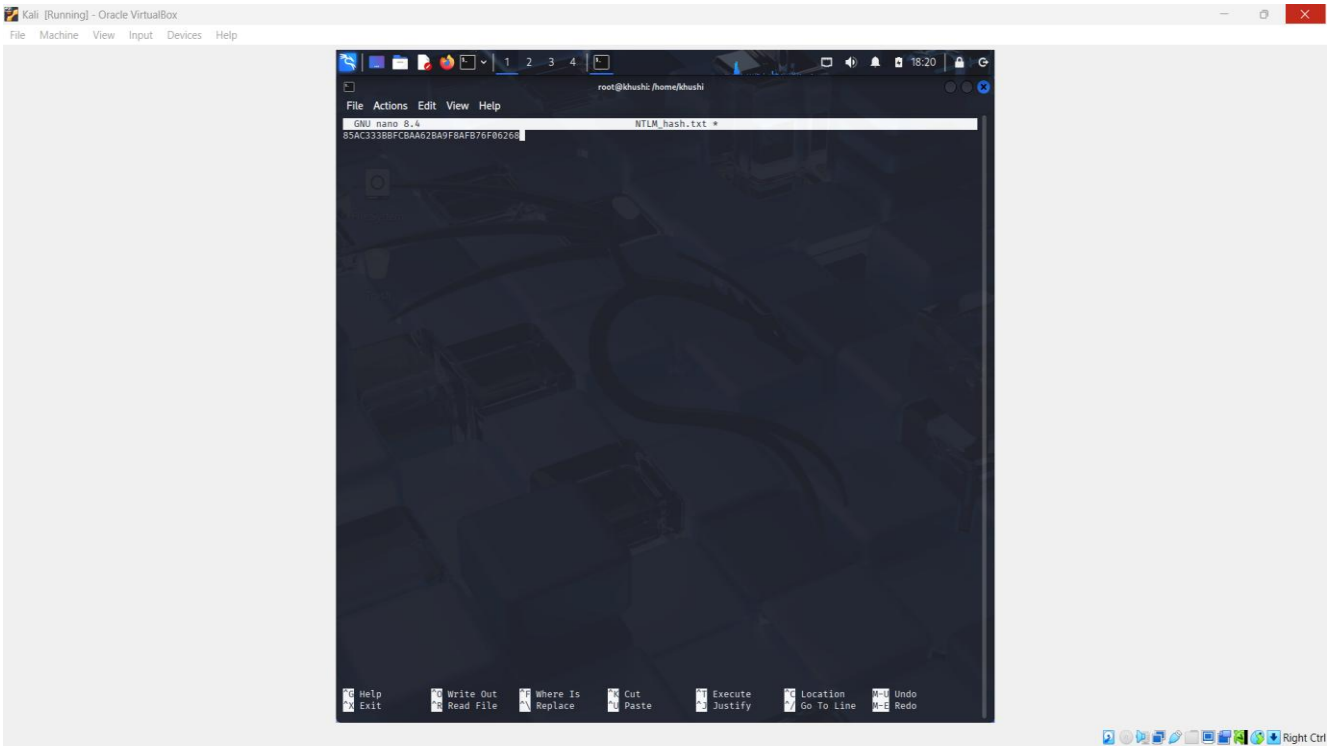




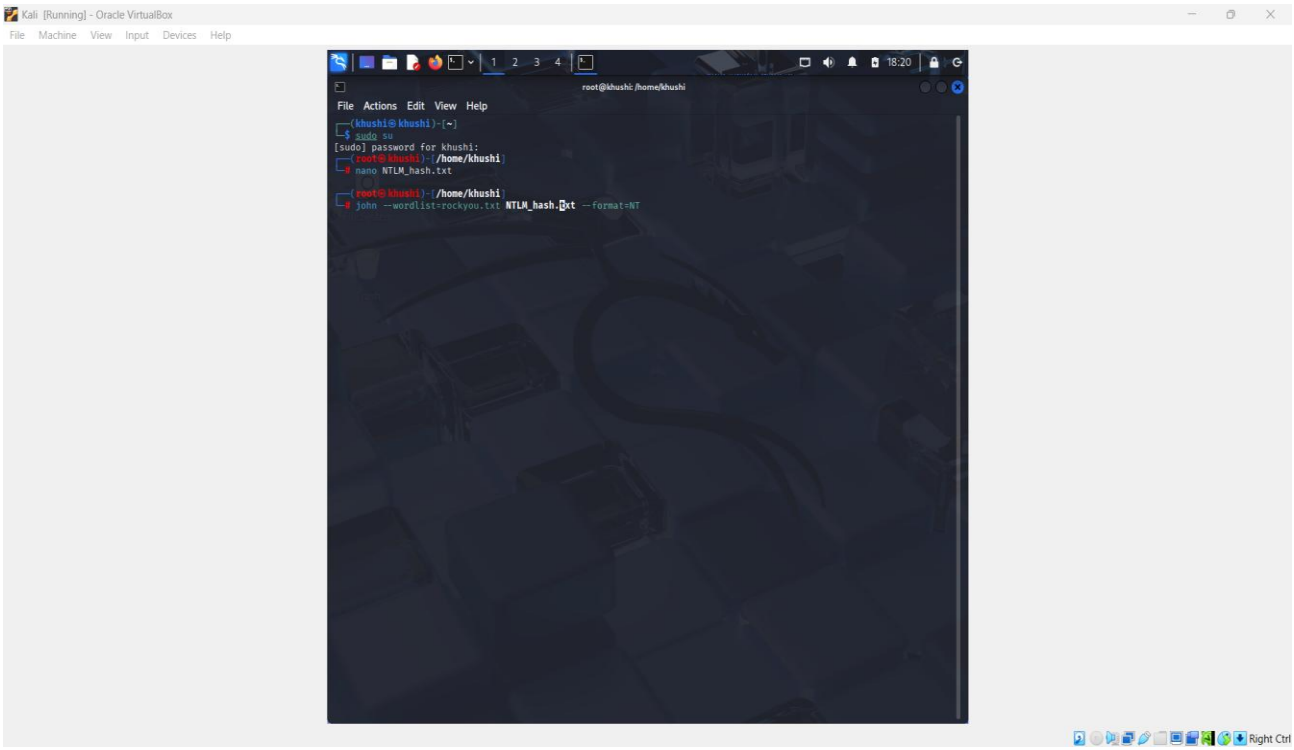
16) Create NTML_hash.txt file:



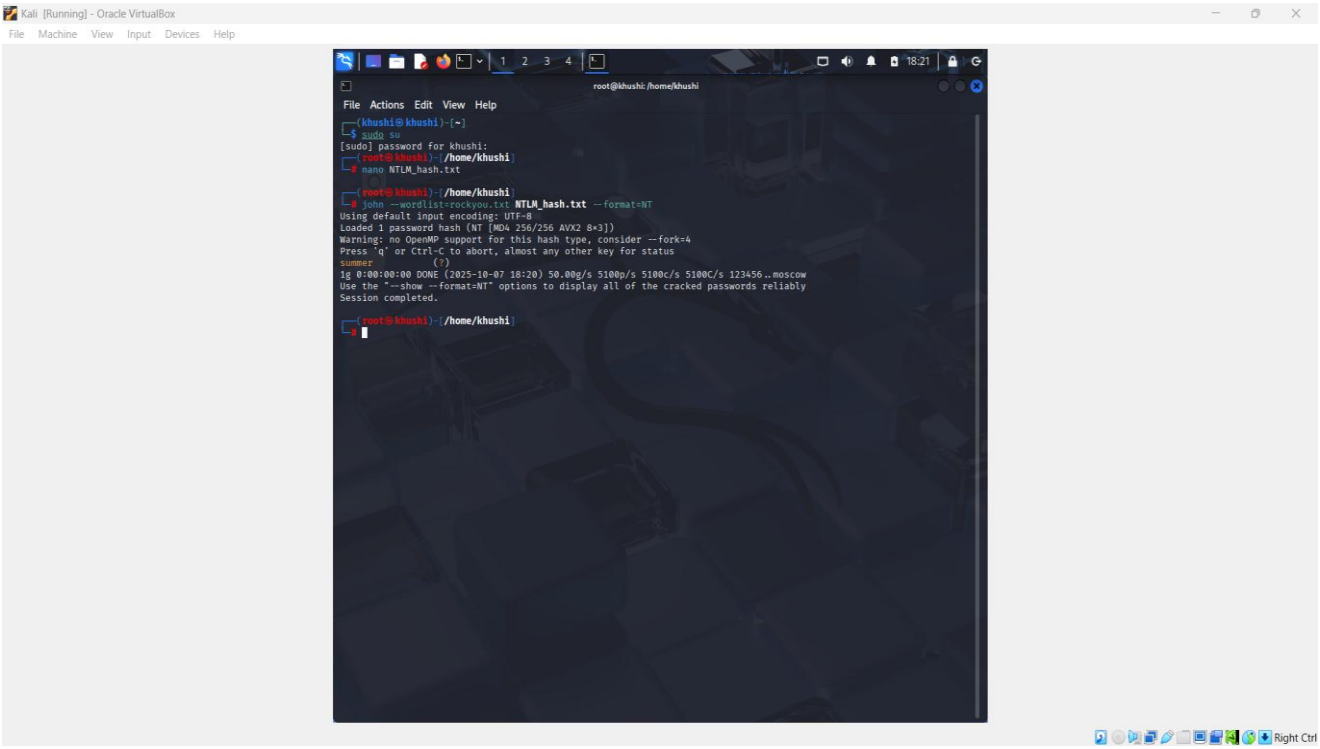
17)Enter a value:



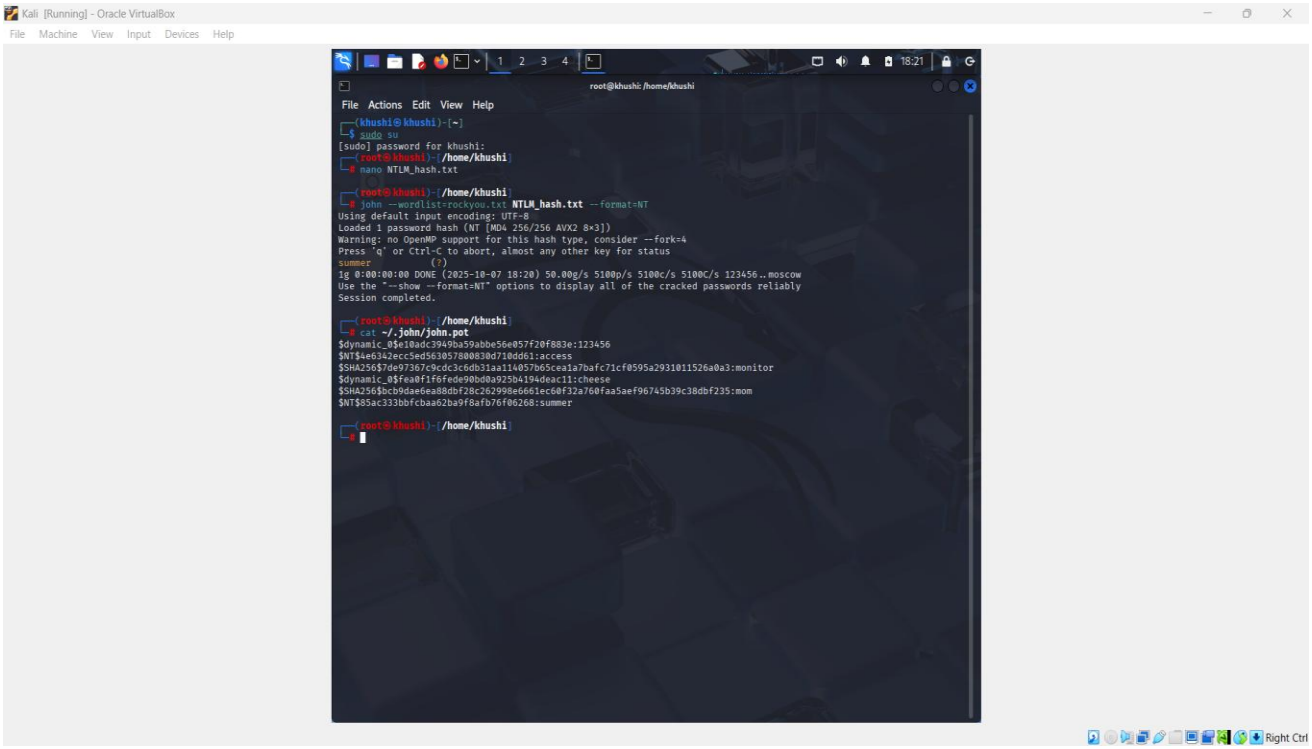
18)Crack password:



19) Password is Cracked :



20)Show all Crack password :



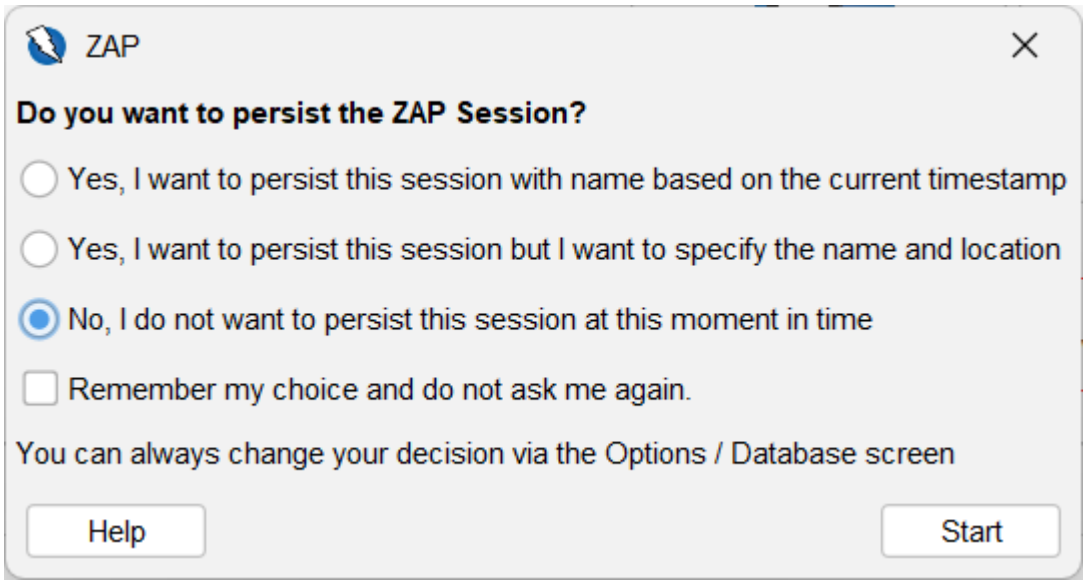
Practical-14

AIM:

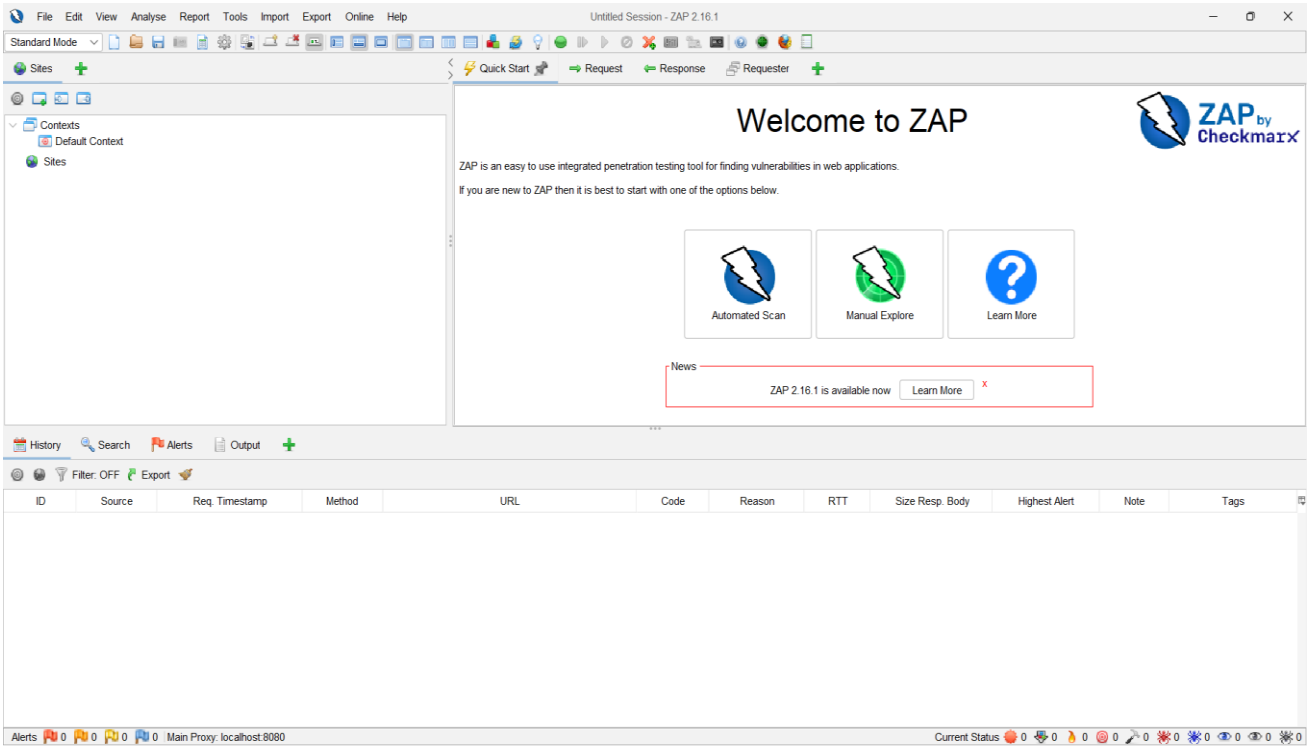
Explore automated web-application security by configuring policies, performing spidering, and detecting vulnerabilities to understand real-world attack surfaces.

STEPS with screenshots:

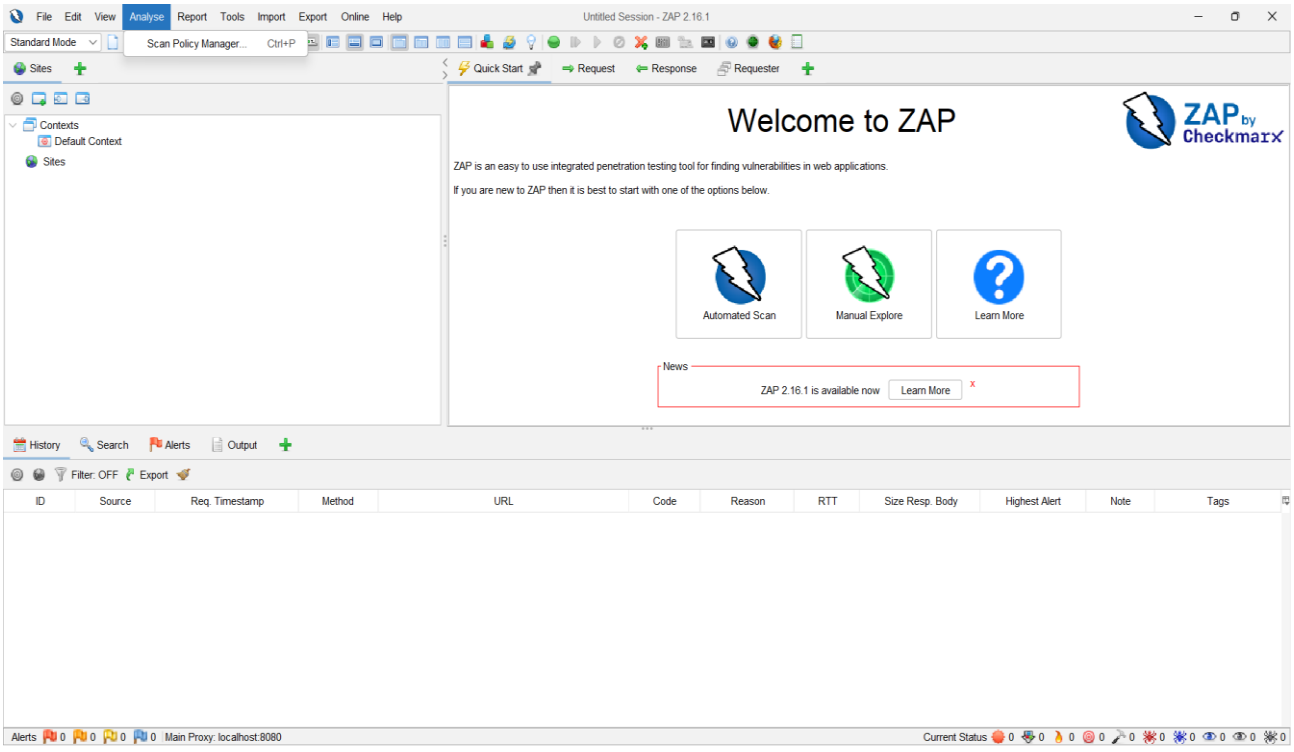
1) Start a Zap Proxy:



2) Start a Main Page :

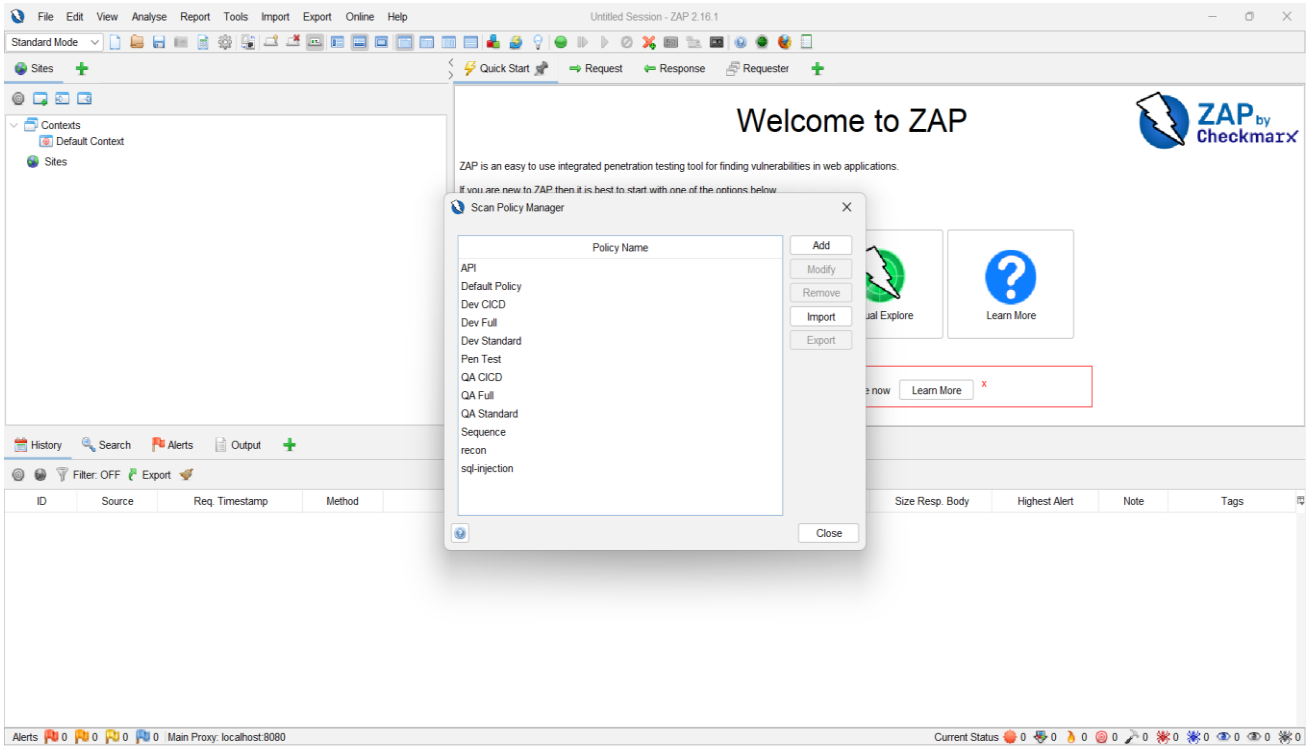


3) Open a Scan Policy Manager:

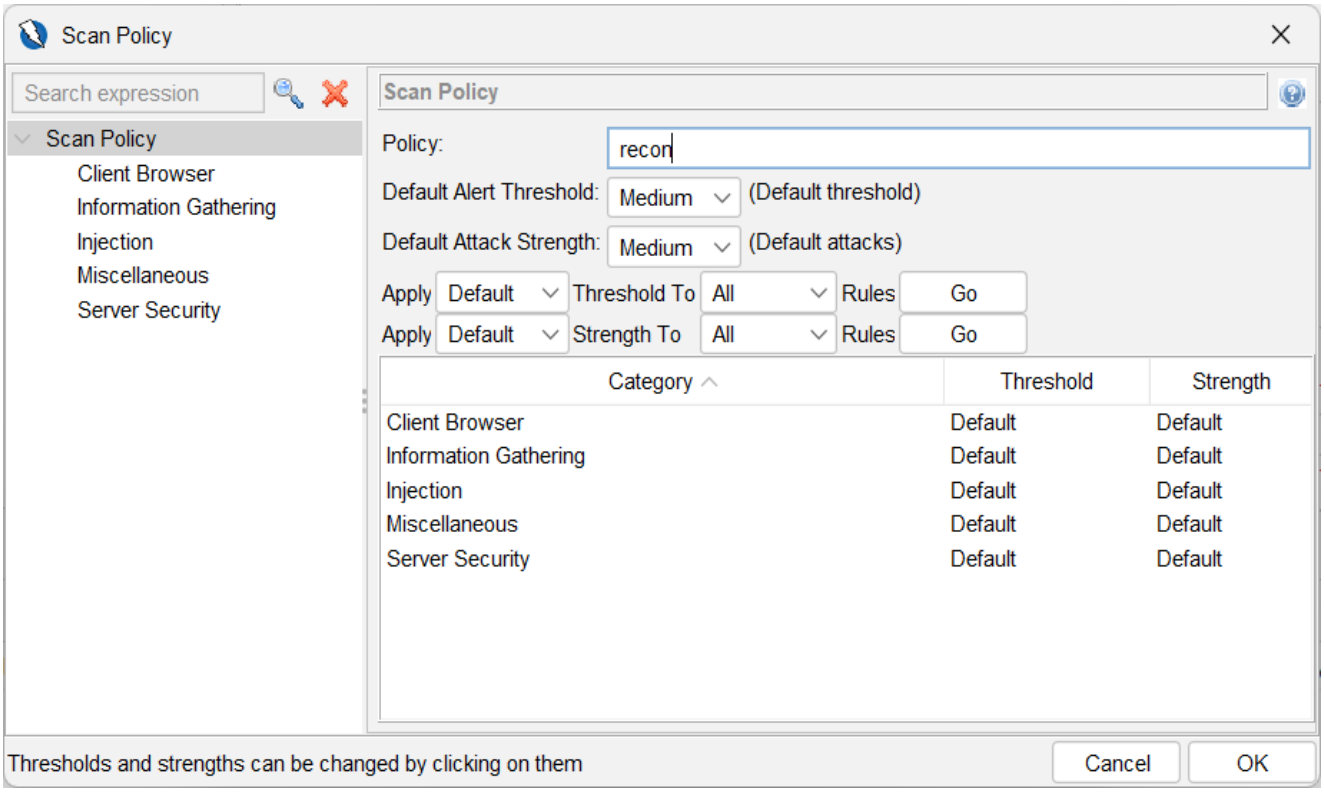


4) Open it :

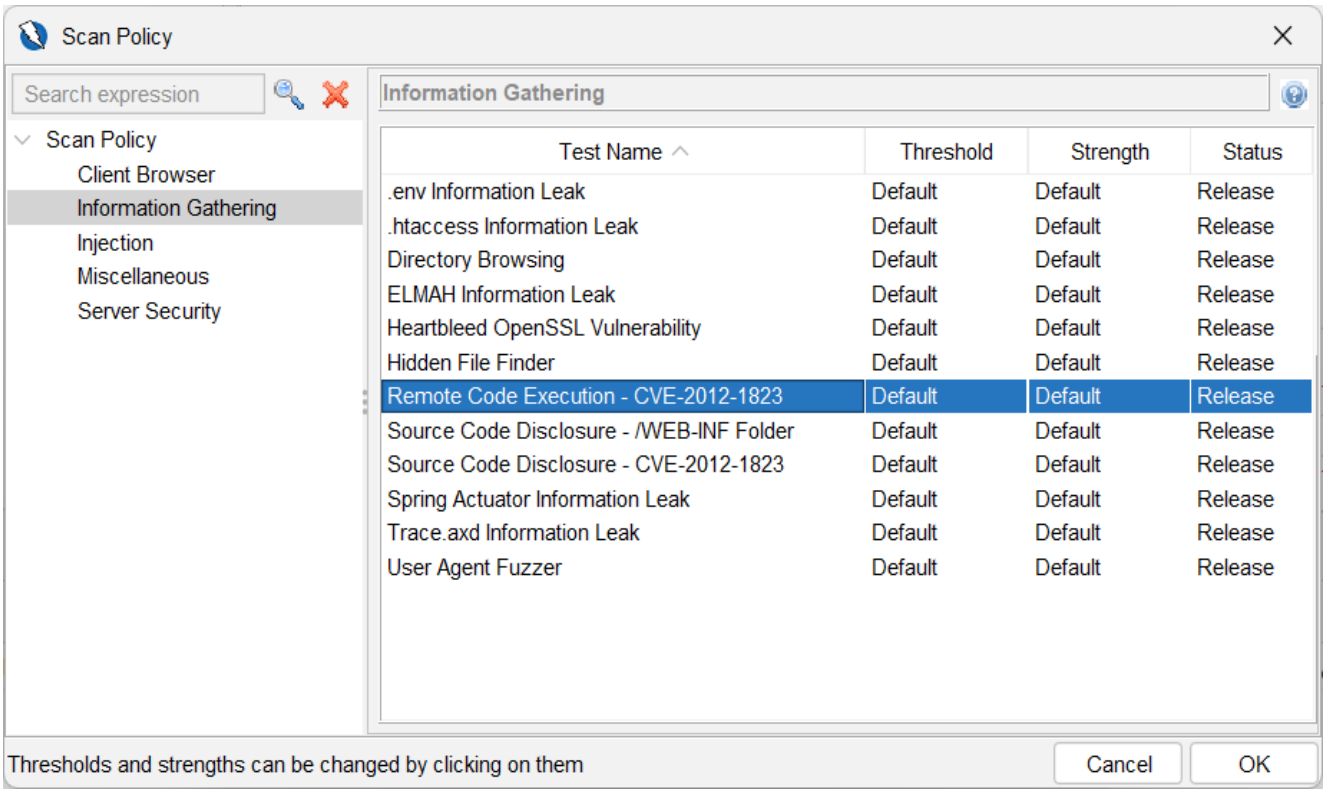
5) Remove all Policy :



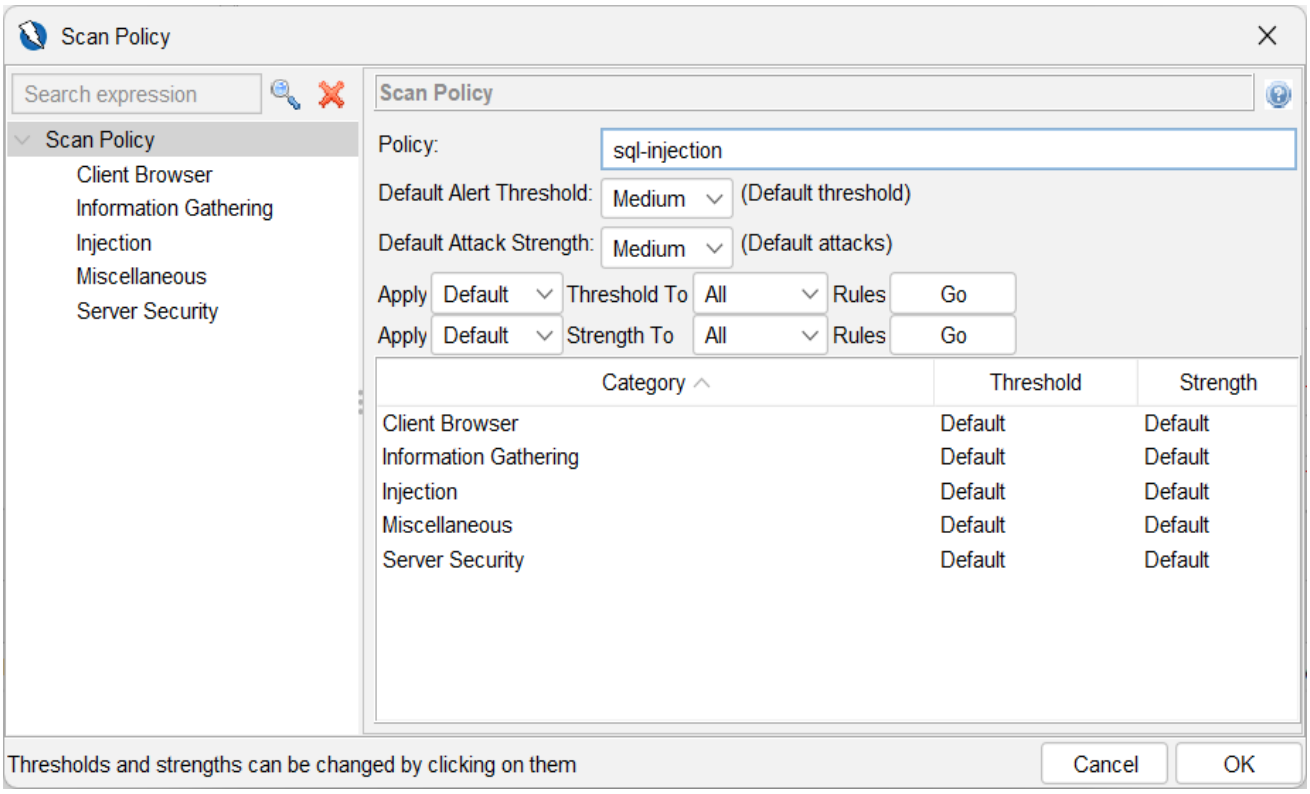
6) Add new Policy :



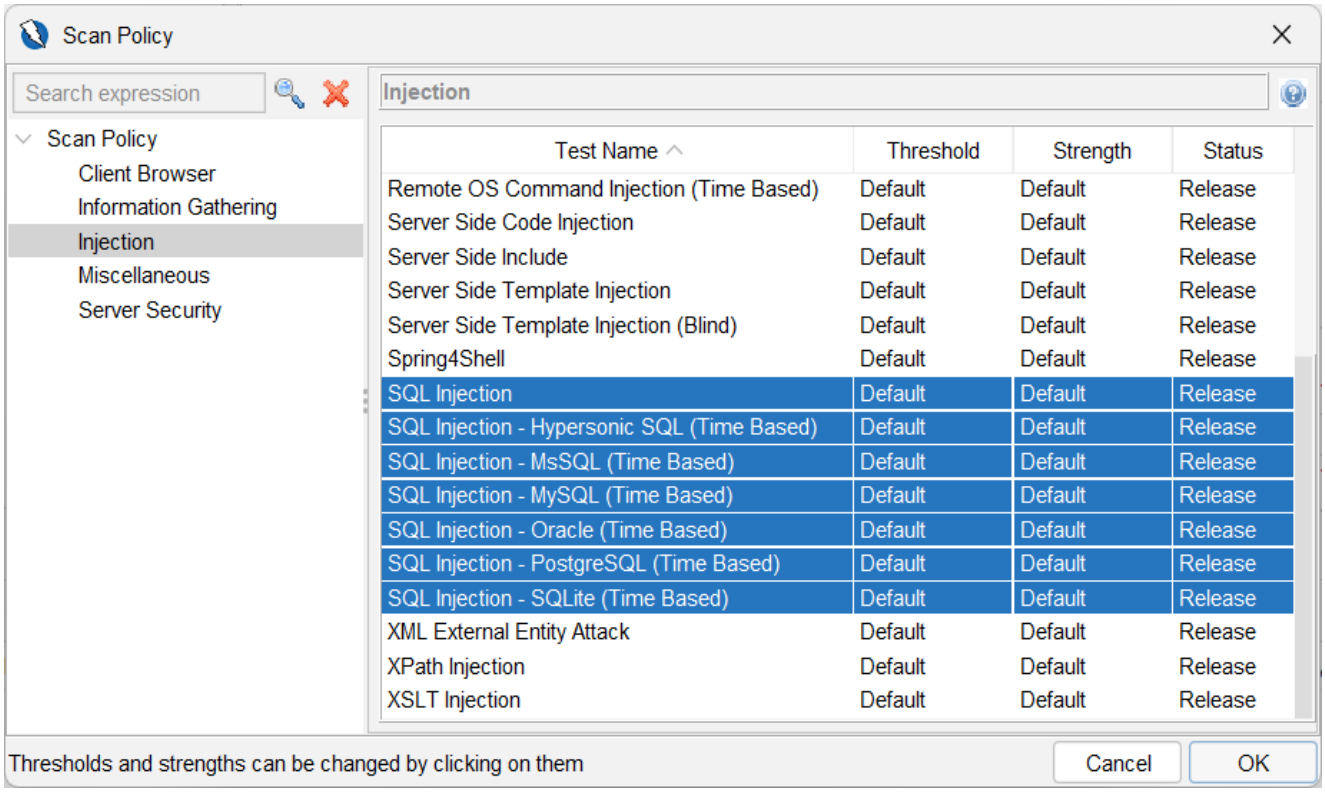
7) Add a information Gathering :



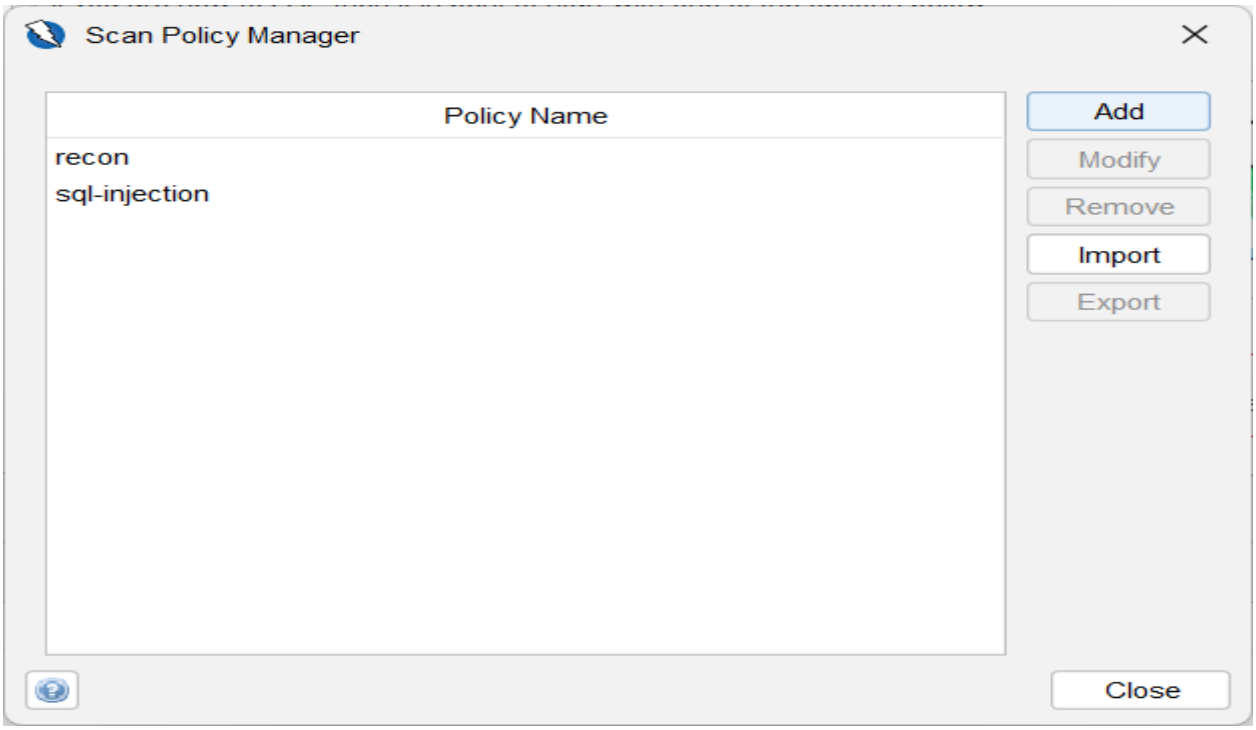
8) Add a sql-injection policy :



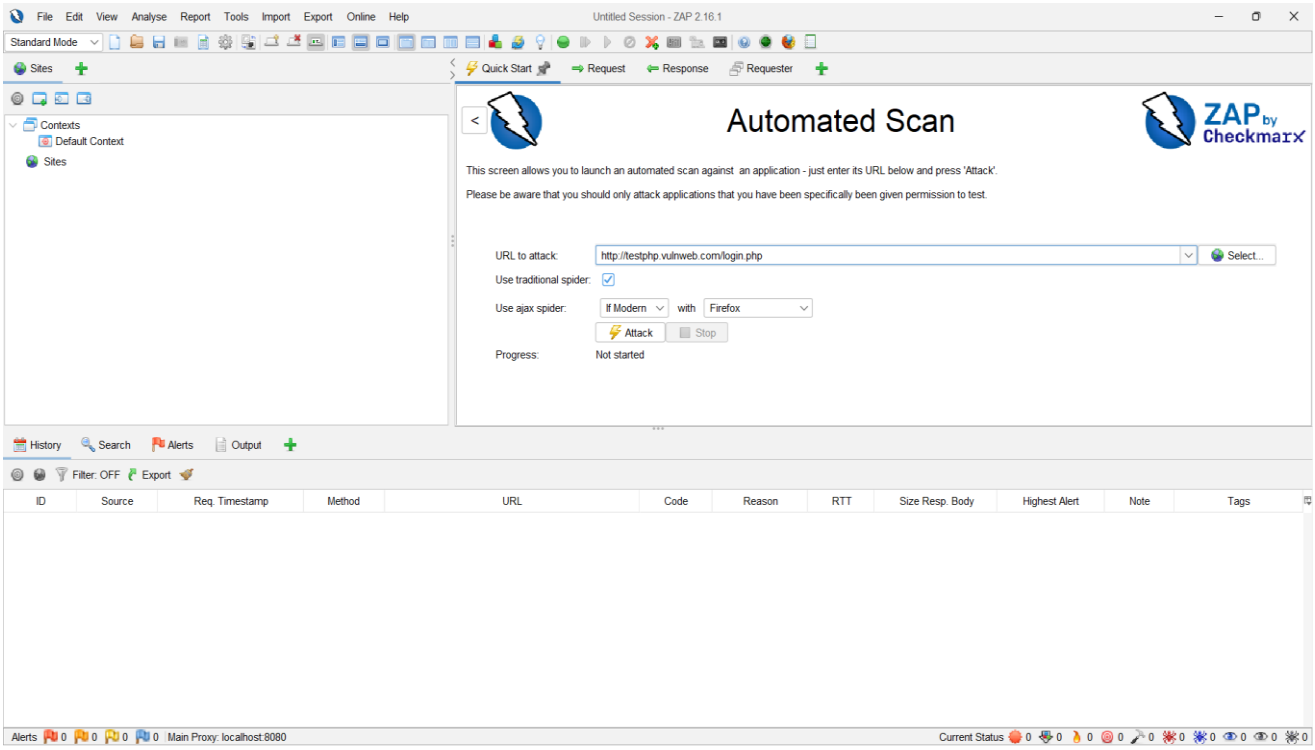
9) Add sql-injection policy :



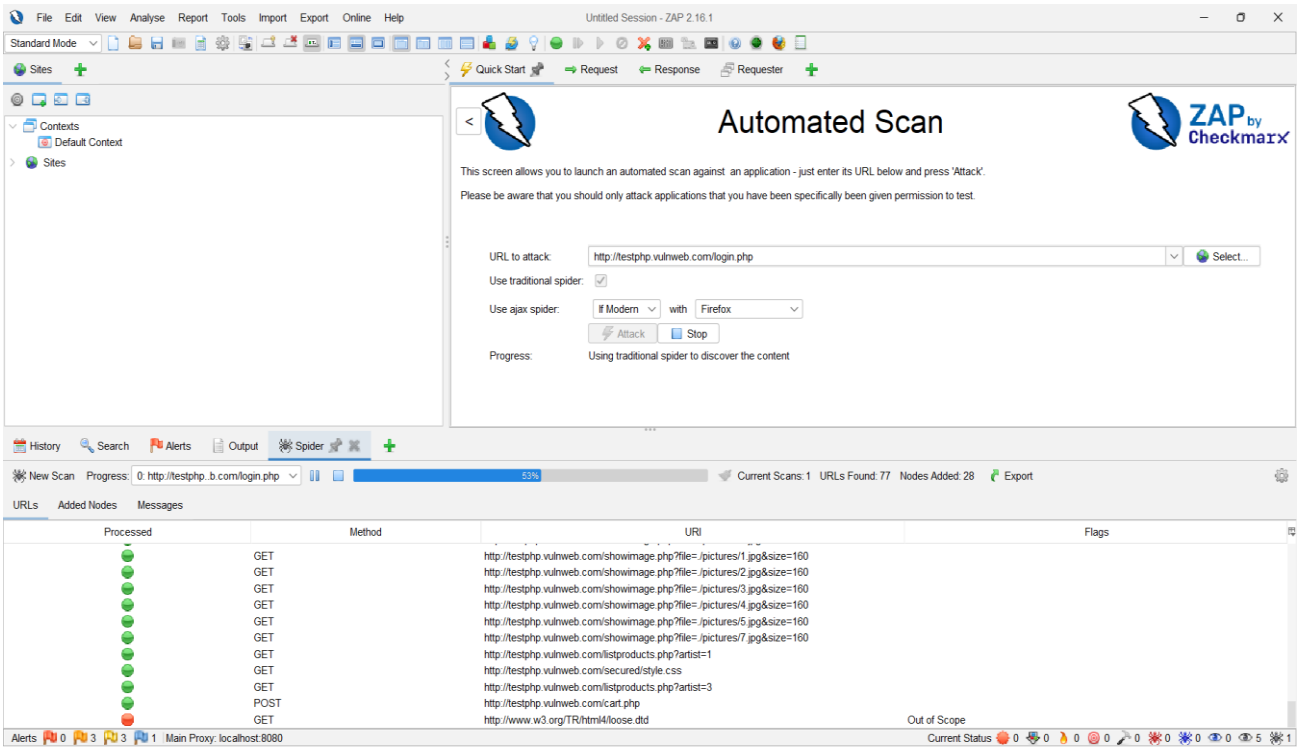
10) Policy Manager :



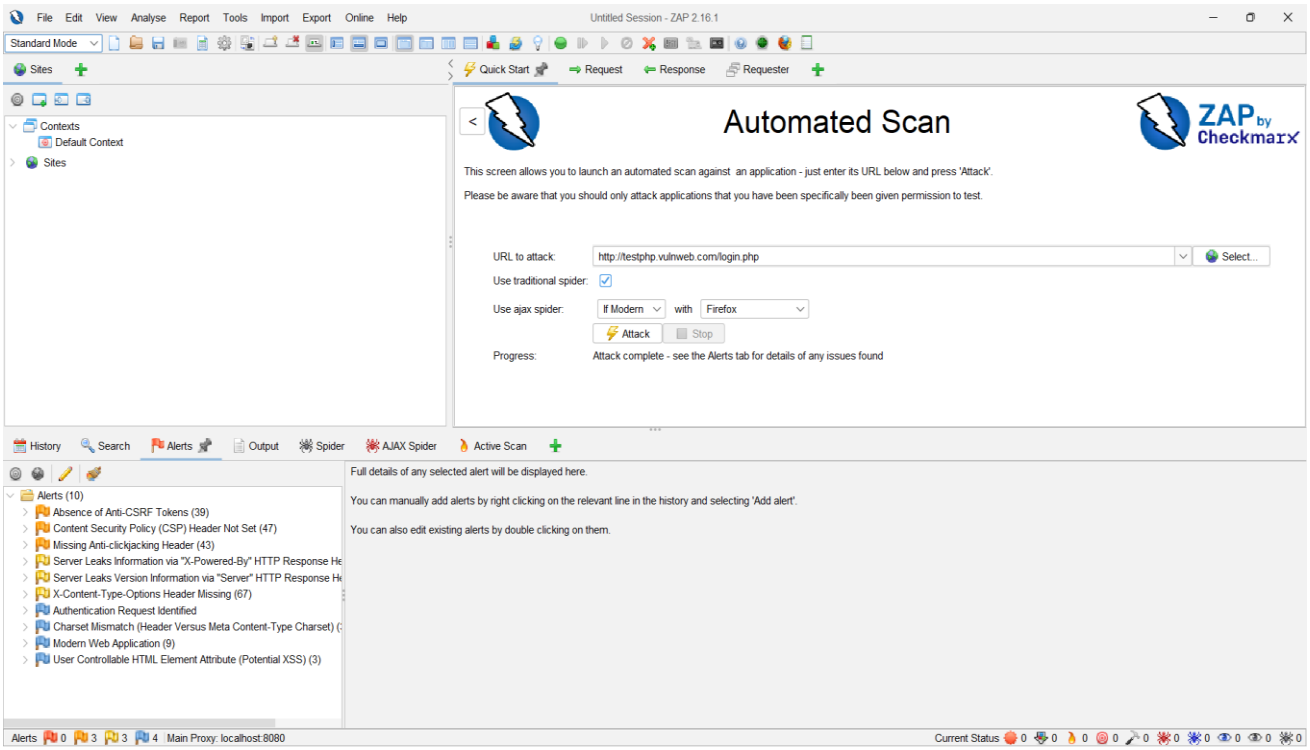
11)Enter a URL :



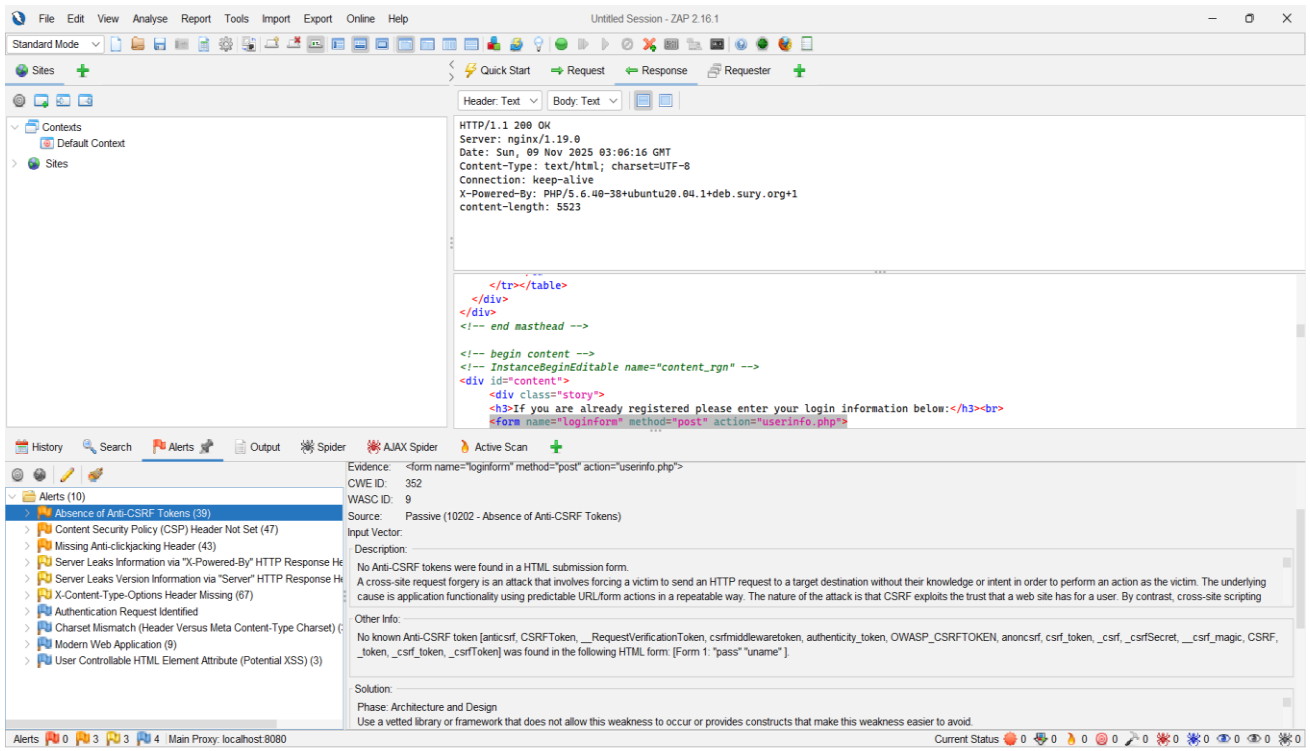
12)Start a Attack :



13) Complete a Attack :



14) Observe a Attack :



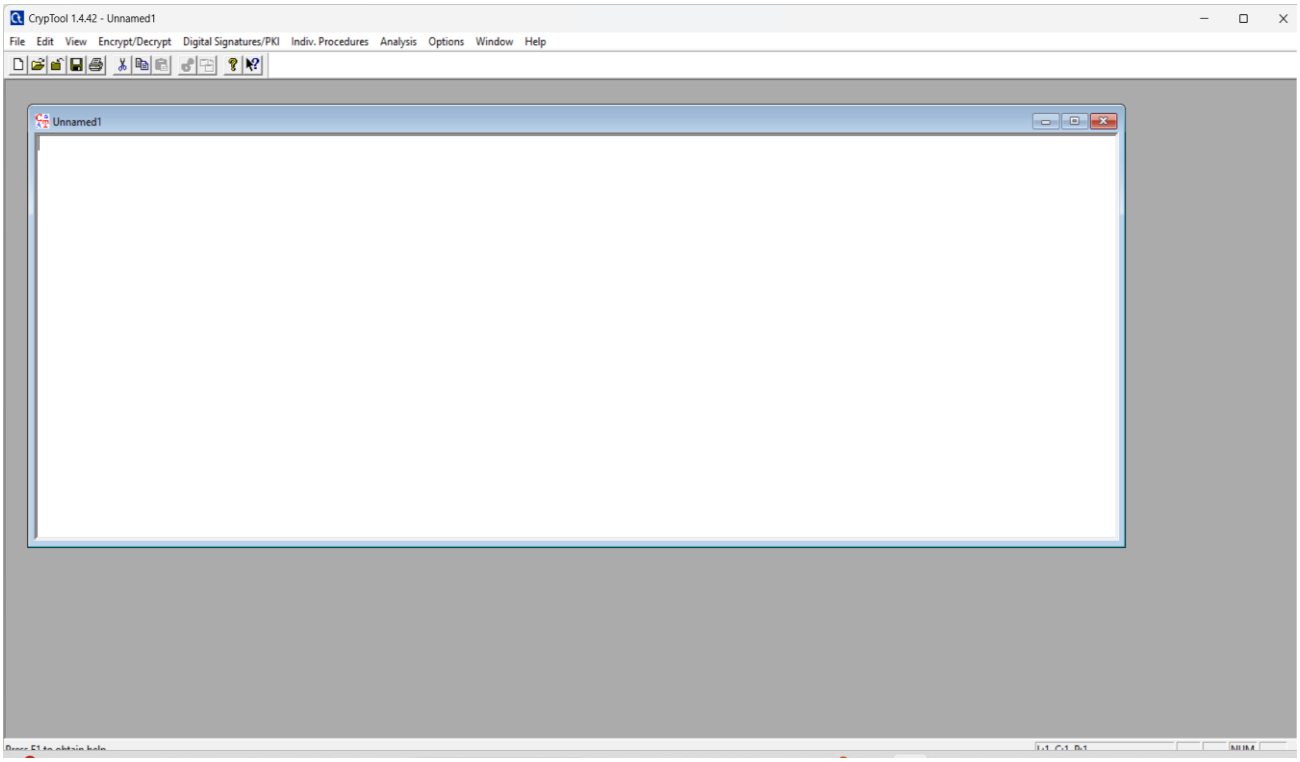
Practical-15

AIM:

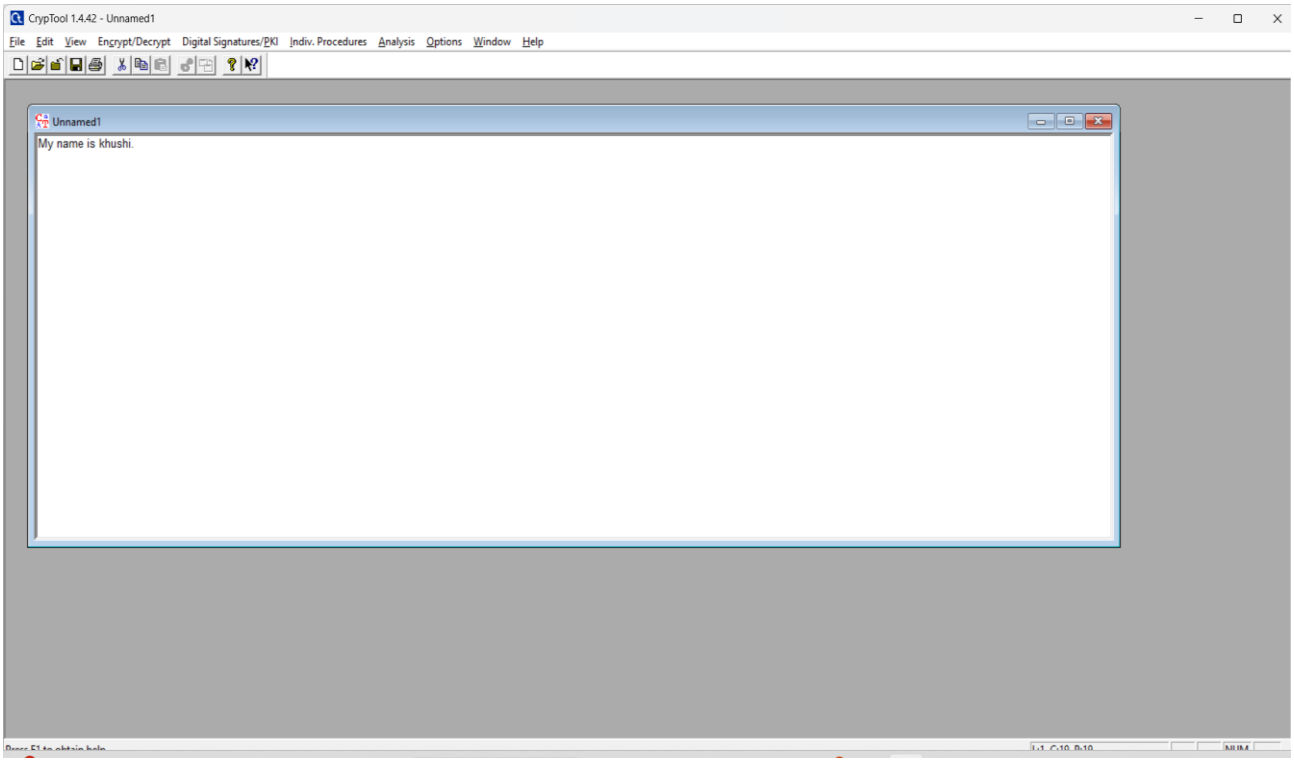
Investigate classical symmetric ciphers: Caesar, Substitution, and Playfair using CrypTool to understand encryption logic, key dependency, and susceptibility to cryptanalytic attacks

STEPS with screenshots:

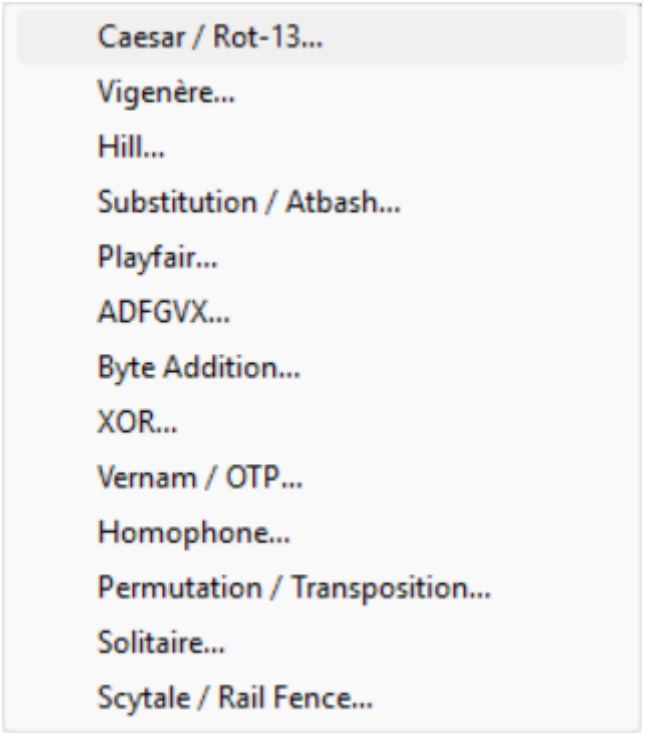
1) Start a CrypTool and New file open :



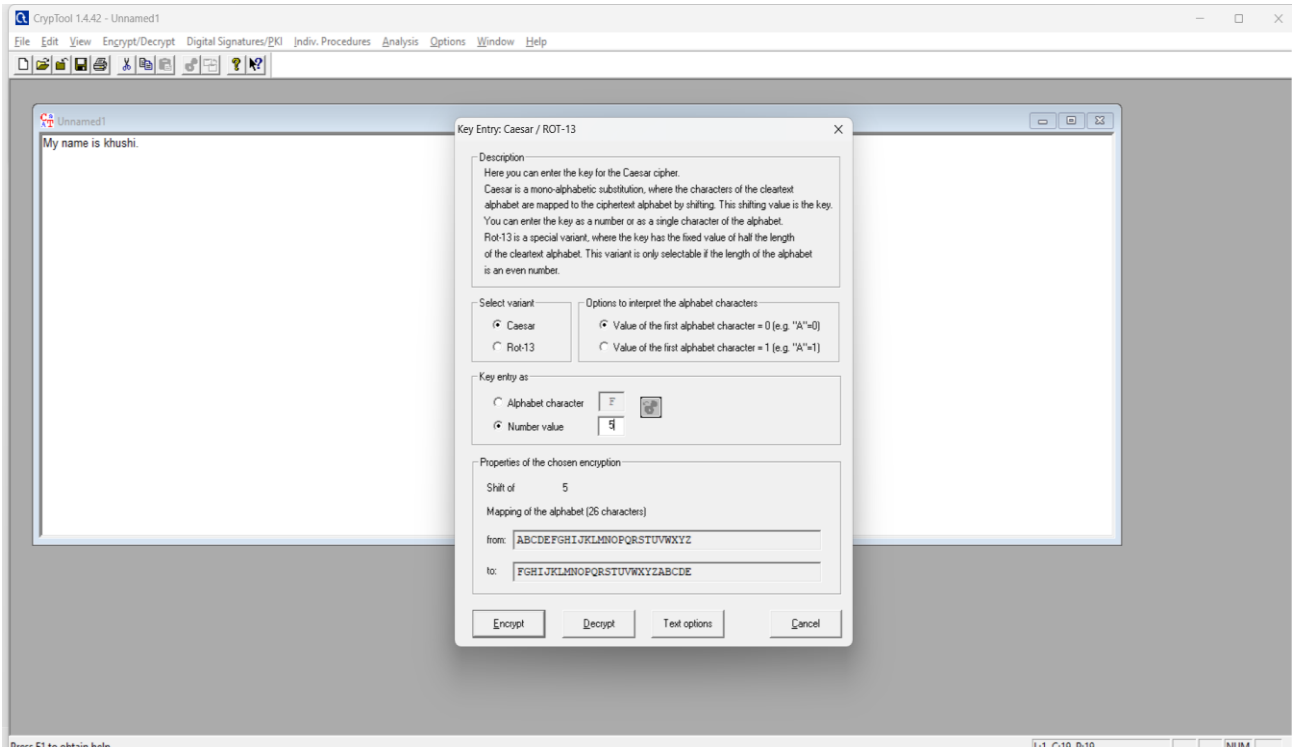
2) Add a contain in file :(Secrete message):



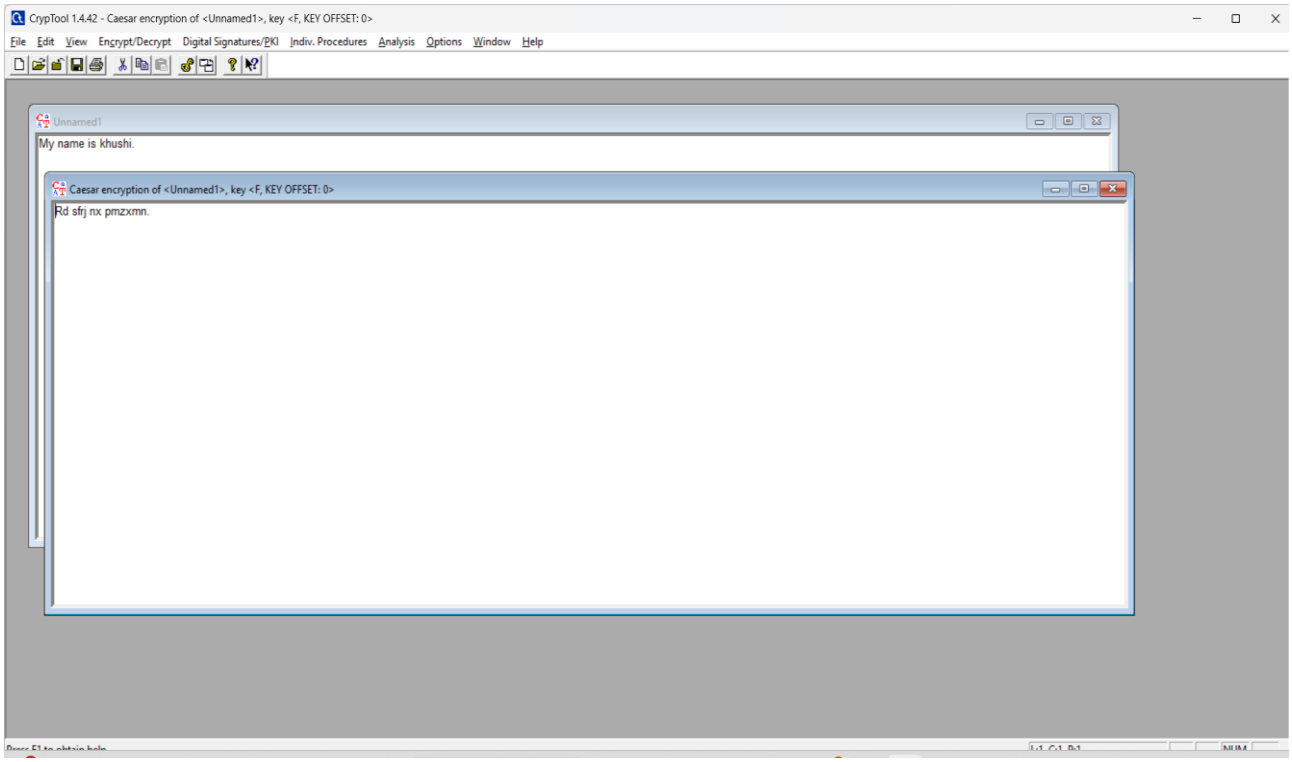
3) Select a Caesar:



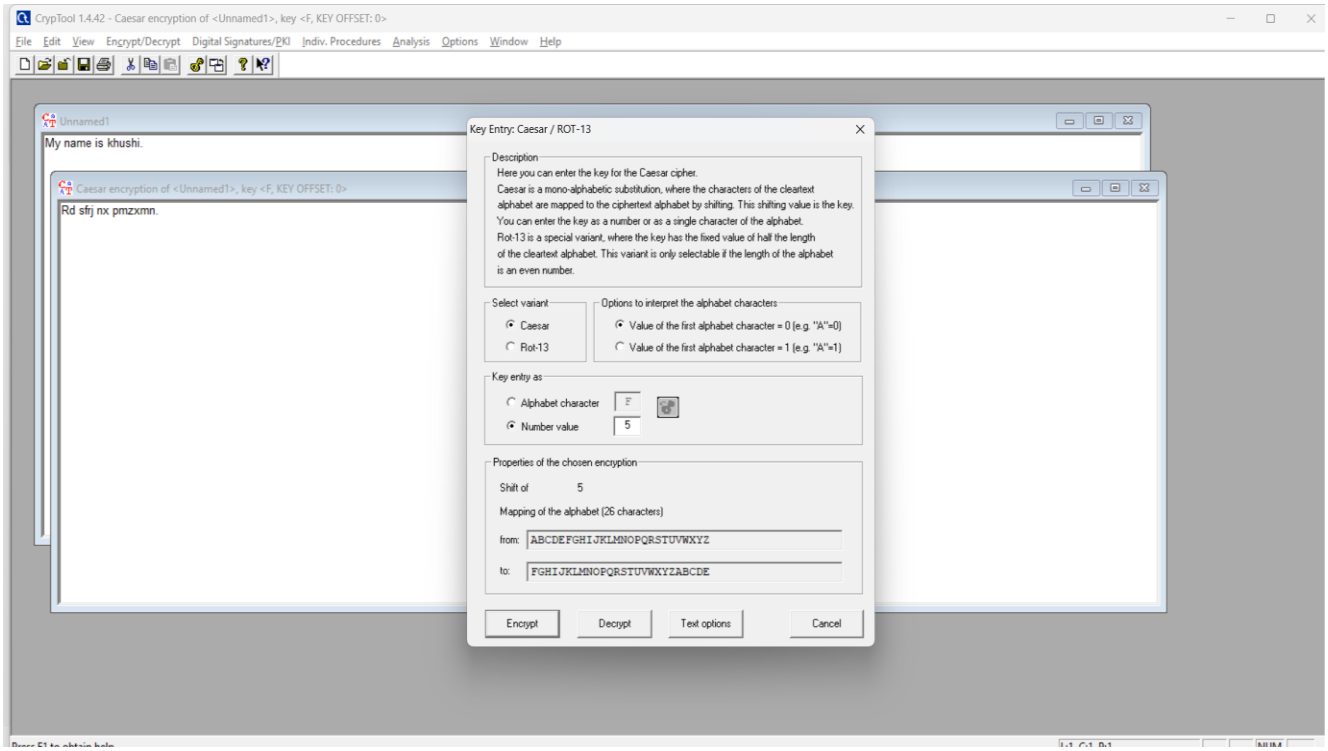
4) Enter a Number value :



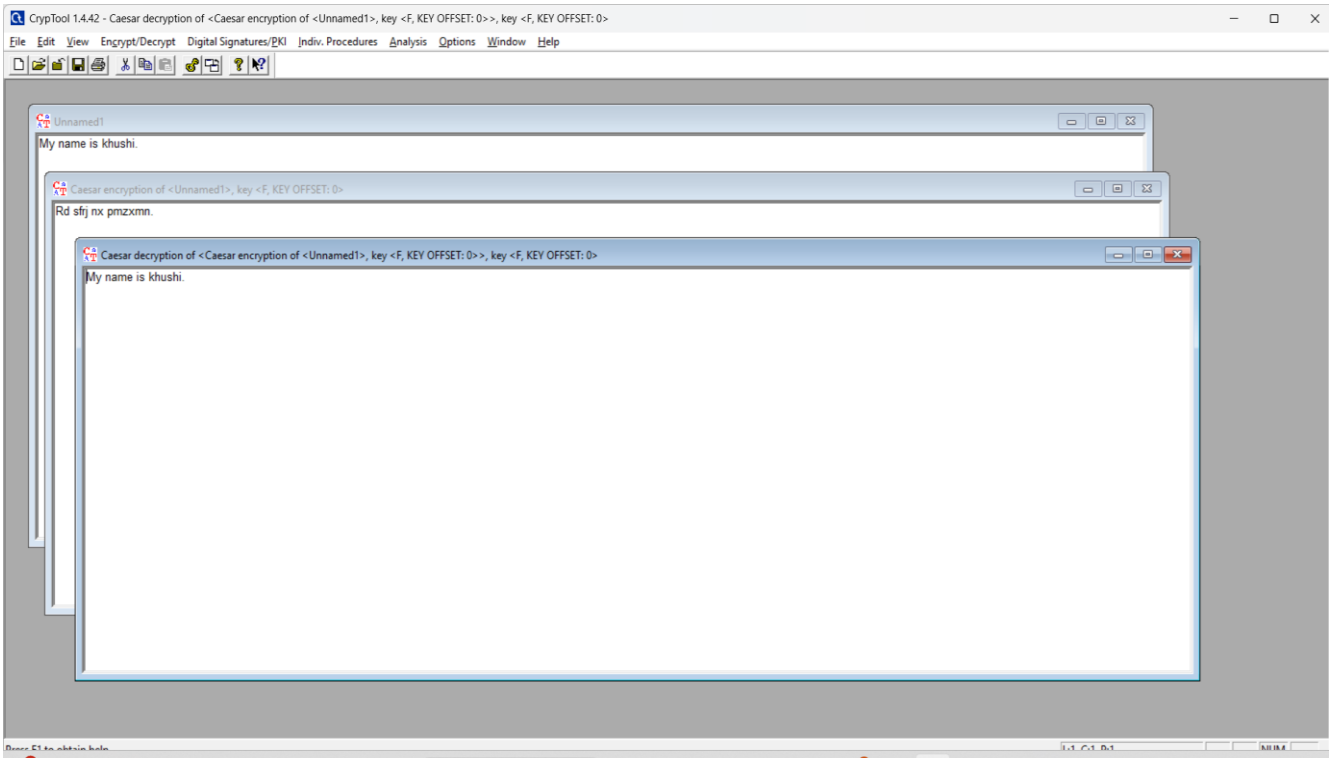
5) Encrypt a Message :



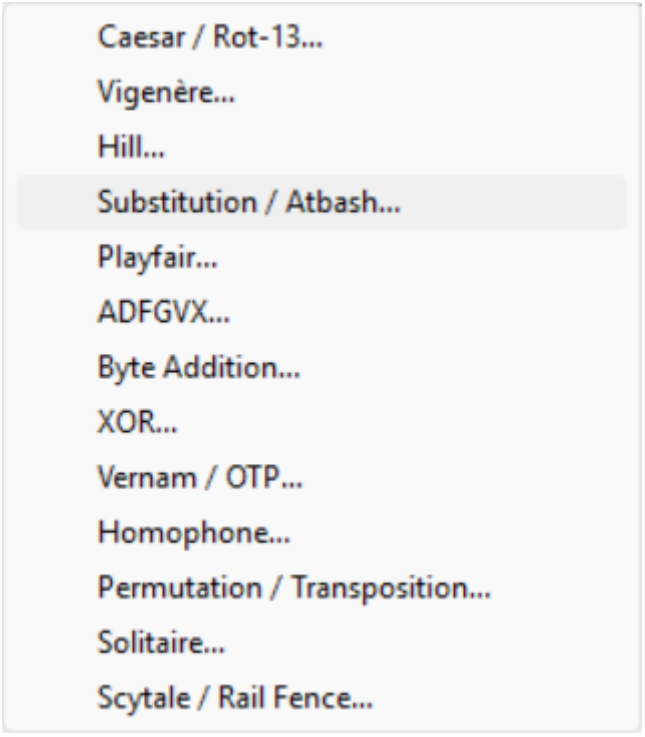
6) Input a number value :



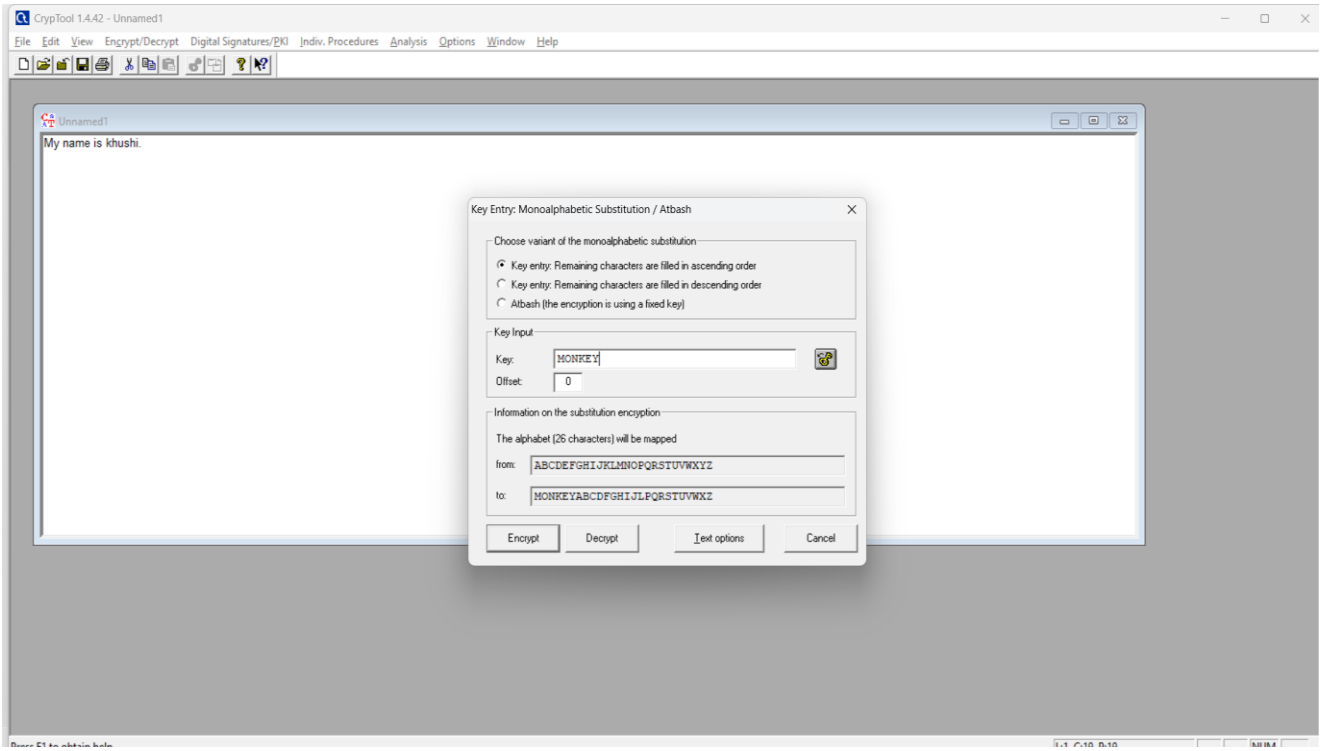
7) Decrypt a Message :



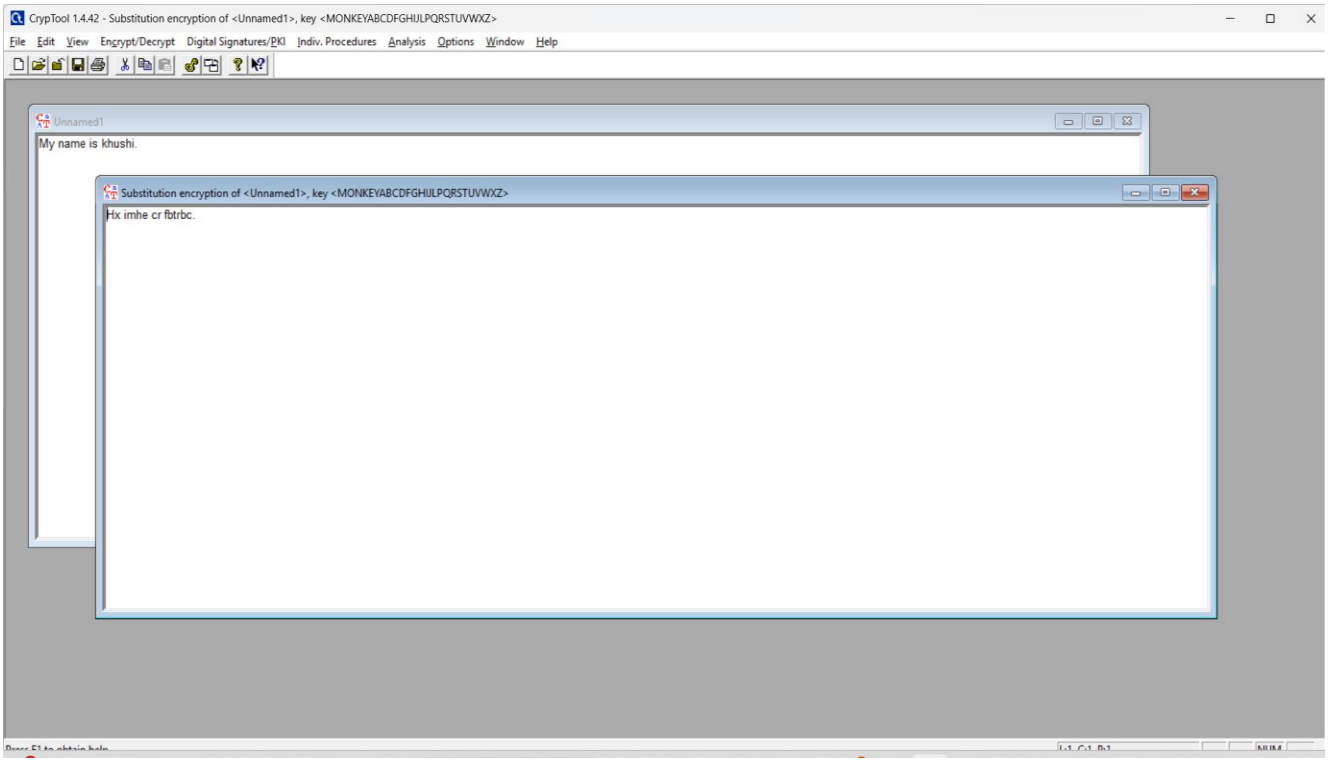
8) Substitution :



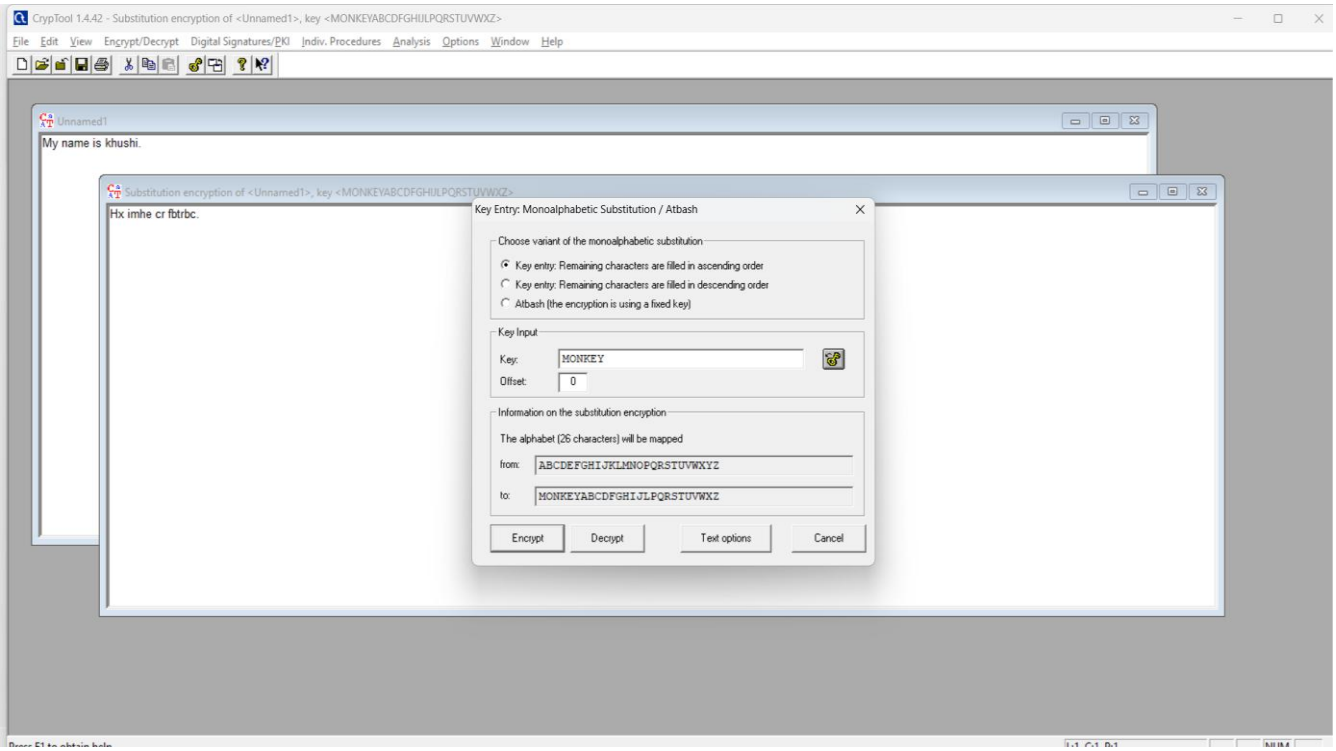
9) Enter a key :



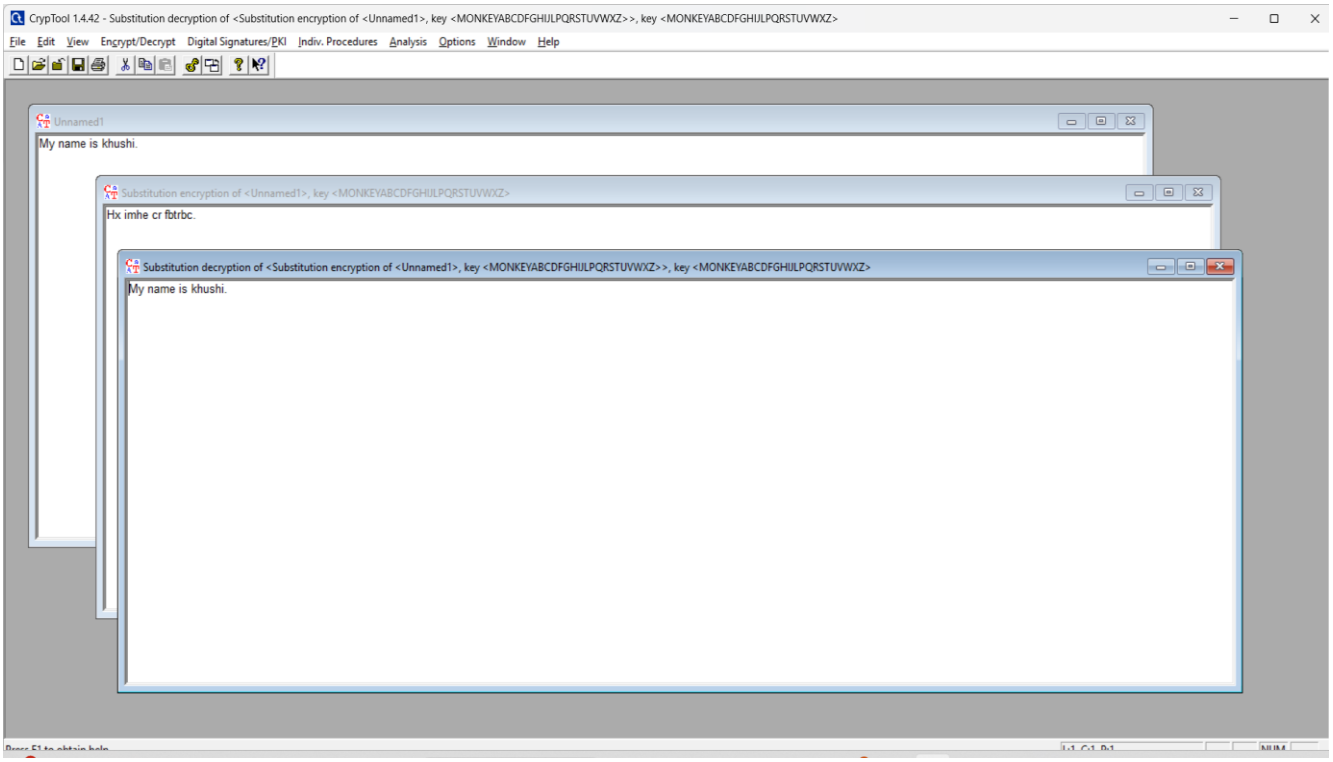
10) Encrypt a message :



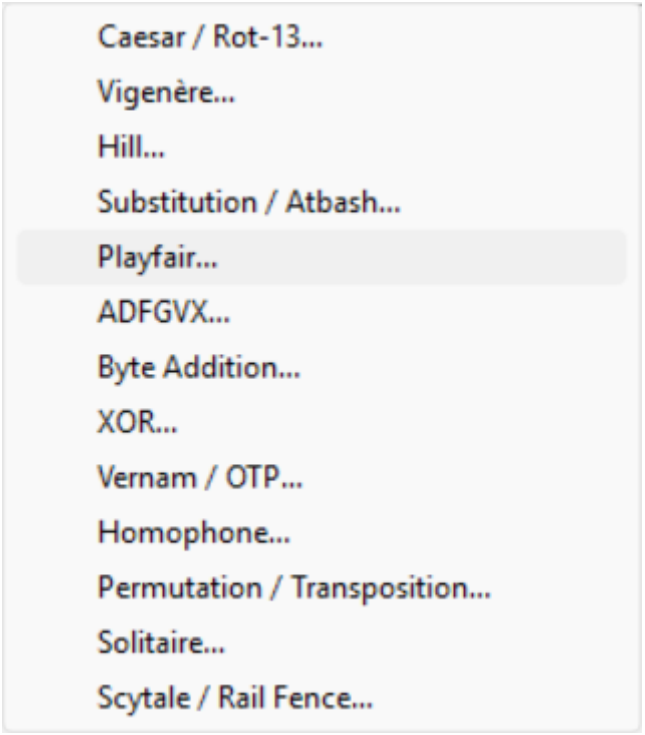
11) How to decrypt message (Input a key):



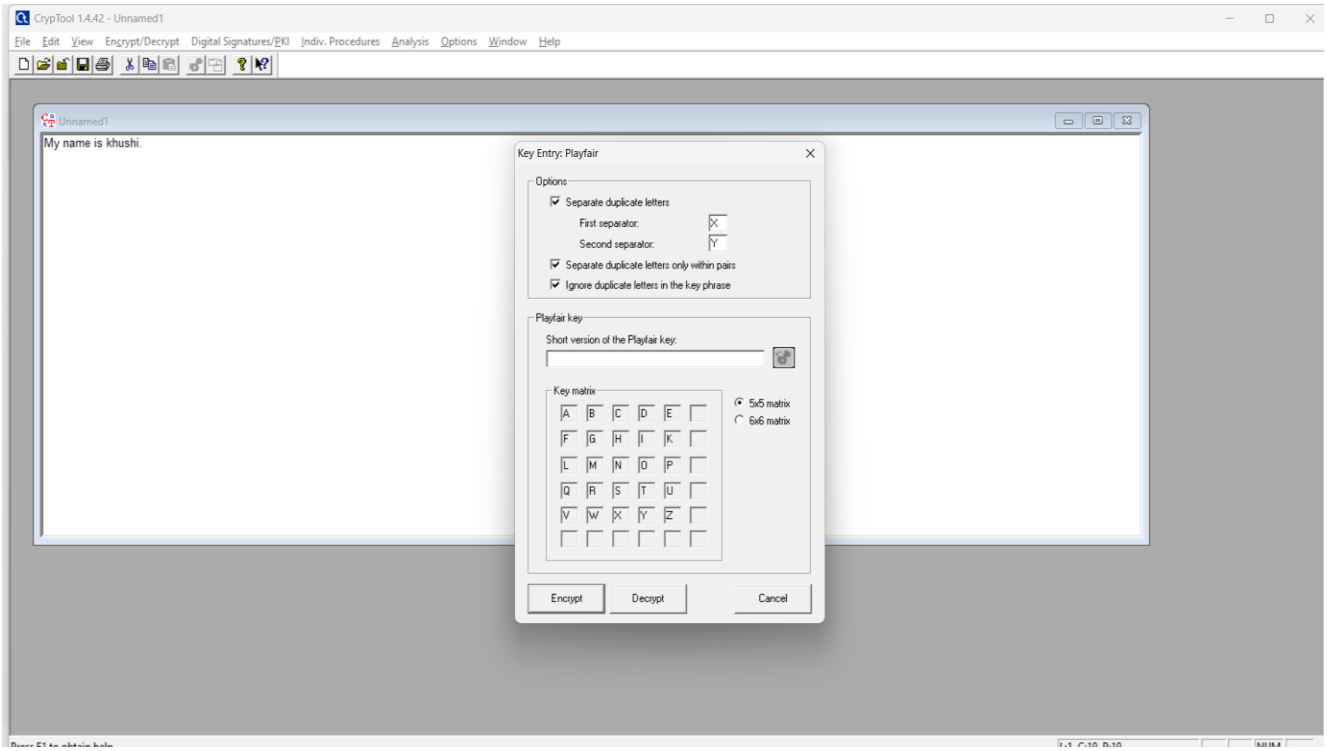
12)Decrypt a message :



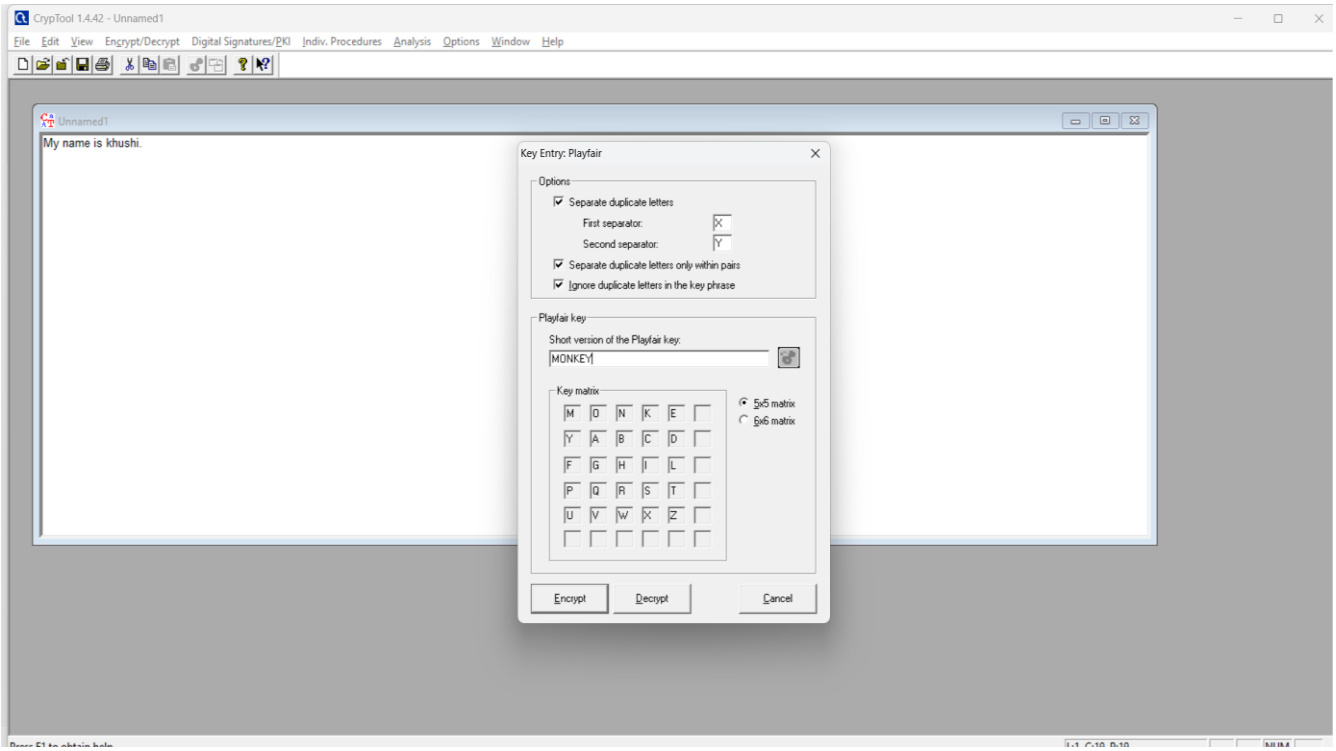
13)Playfair :



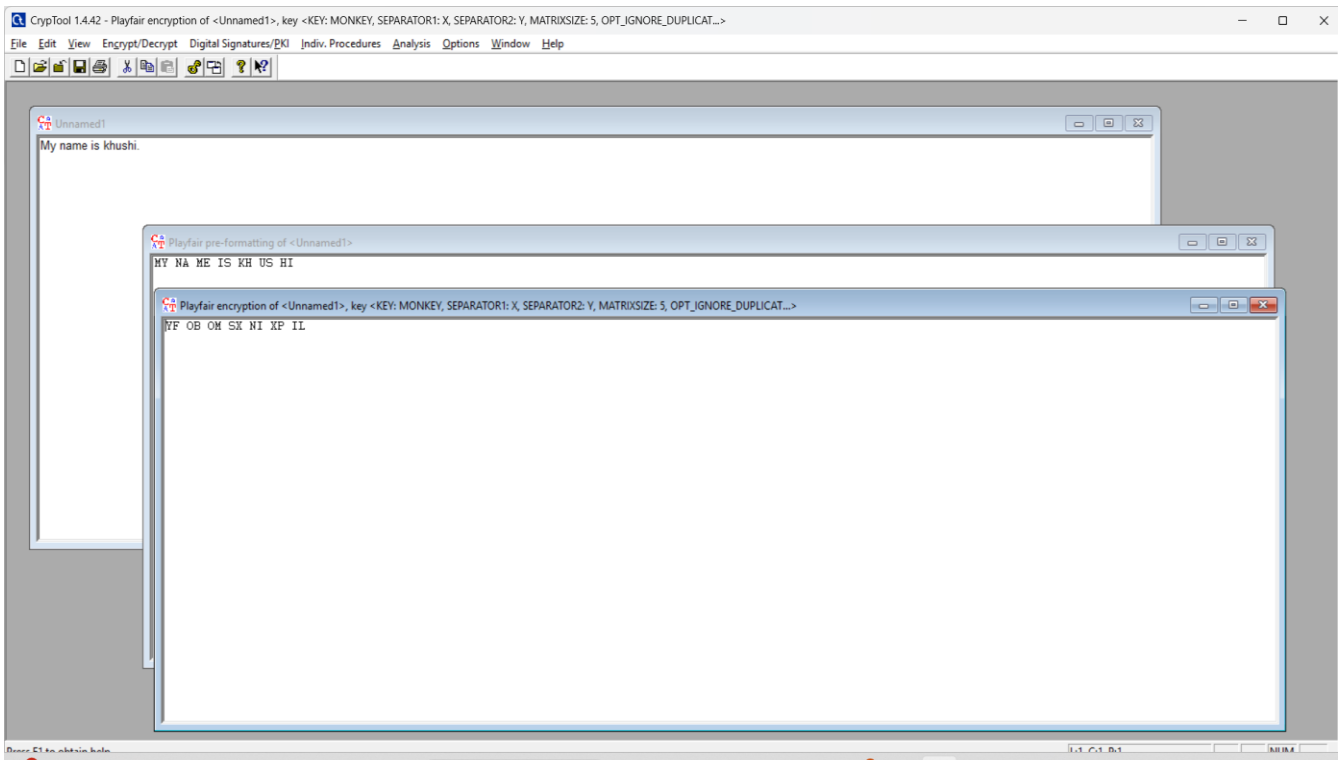
14) Enter a key :



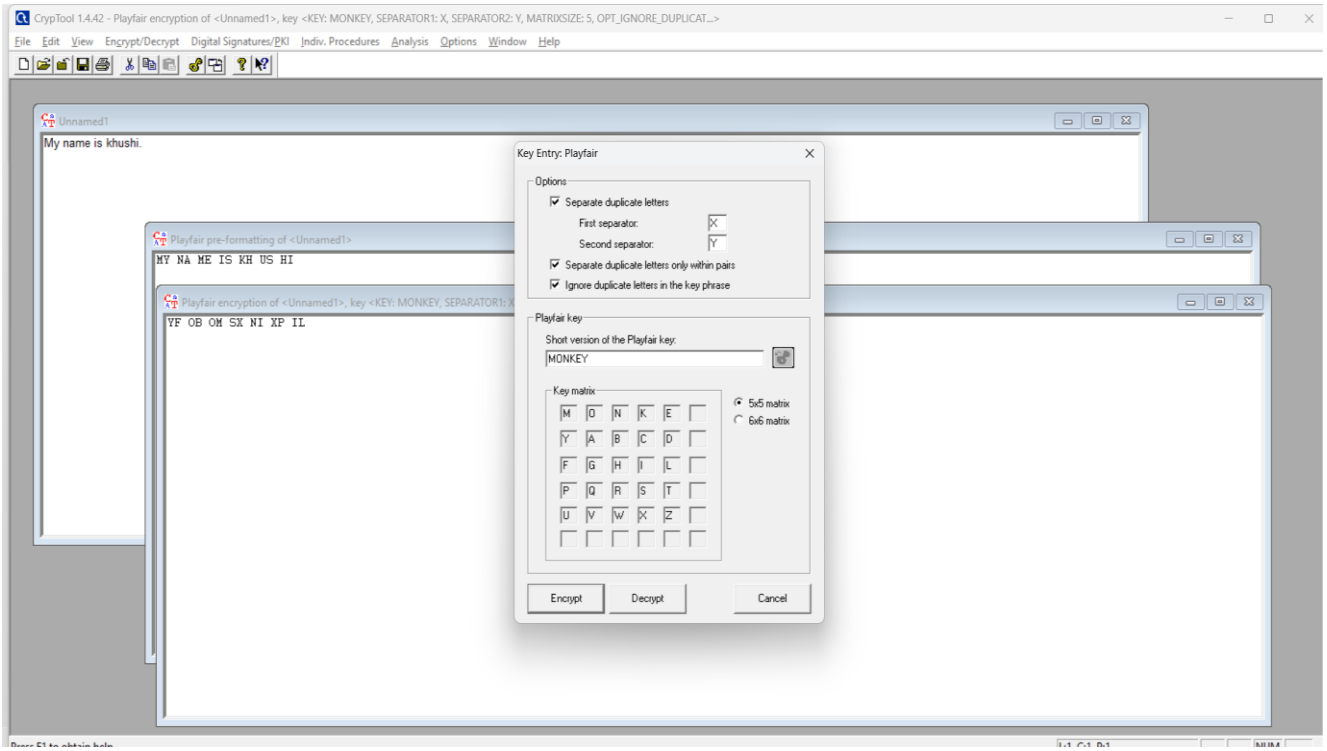
15) Encrypt button click :



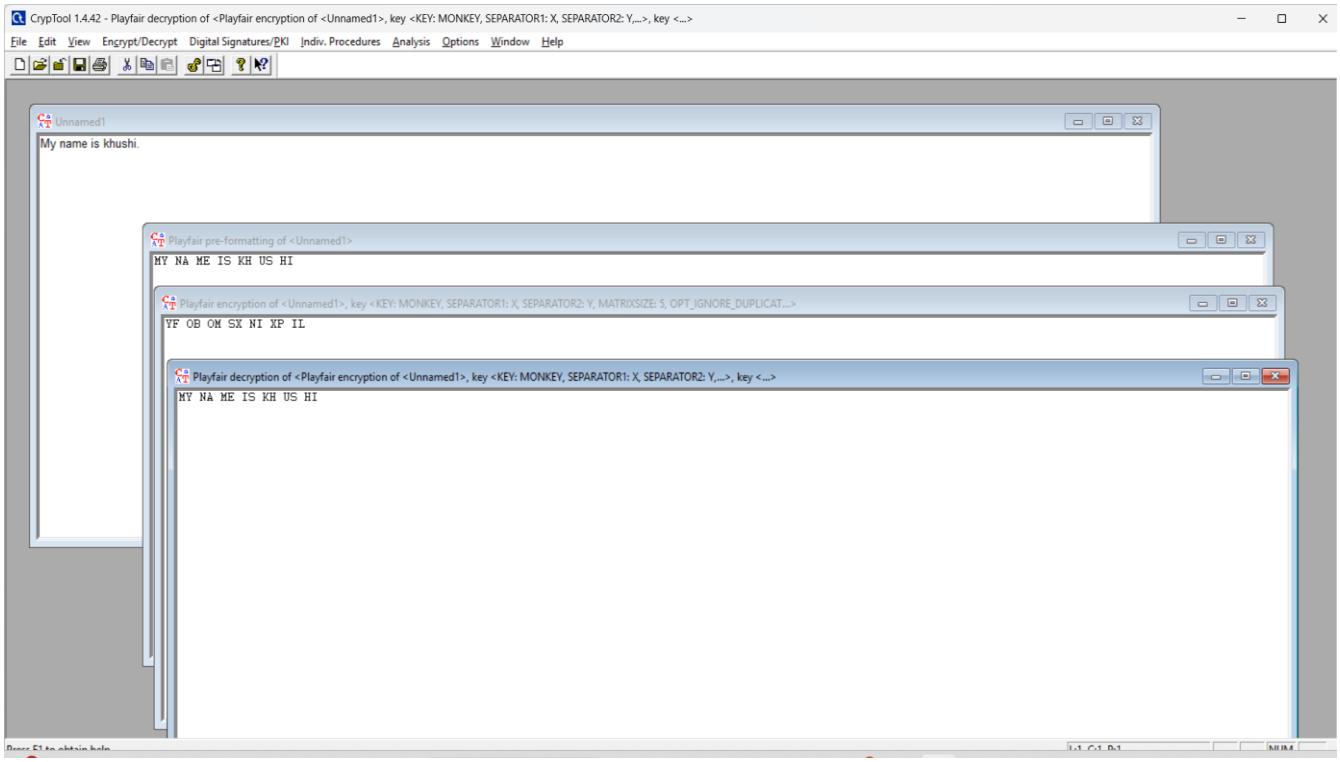
16) Encrypt a message :



17) Click a Decrypt button:



18) Decrypt a message :



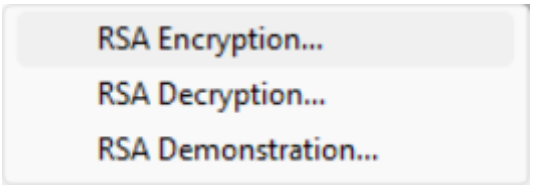
Practical-16

AIM:

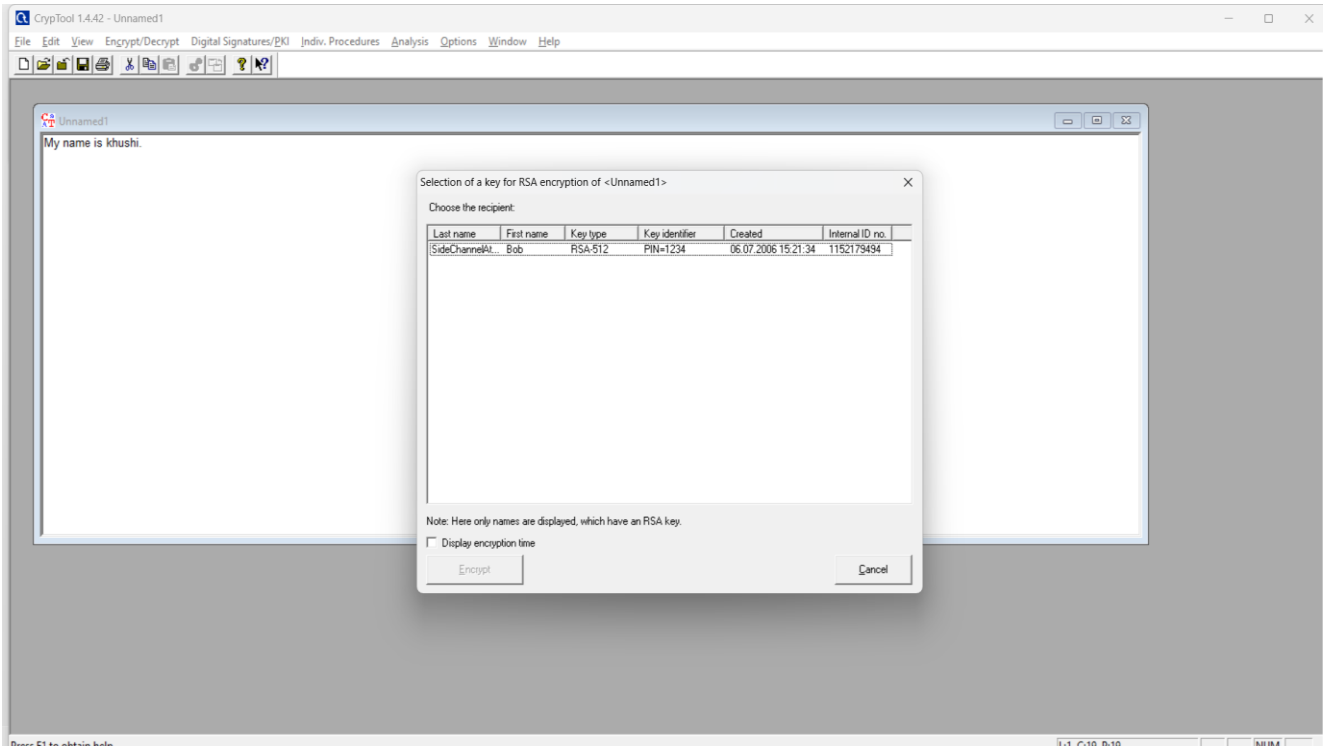
Implement RSA and digital signatures in CrypTool to analyze key-pair generation, secure message encryption, and authentication through integrity verification mechanisms.

STEPS with screenshots:

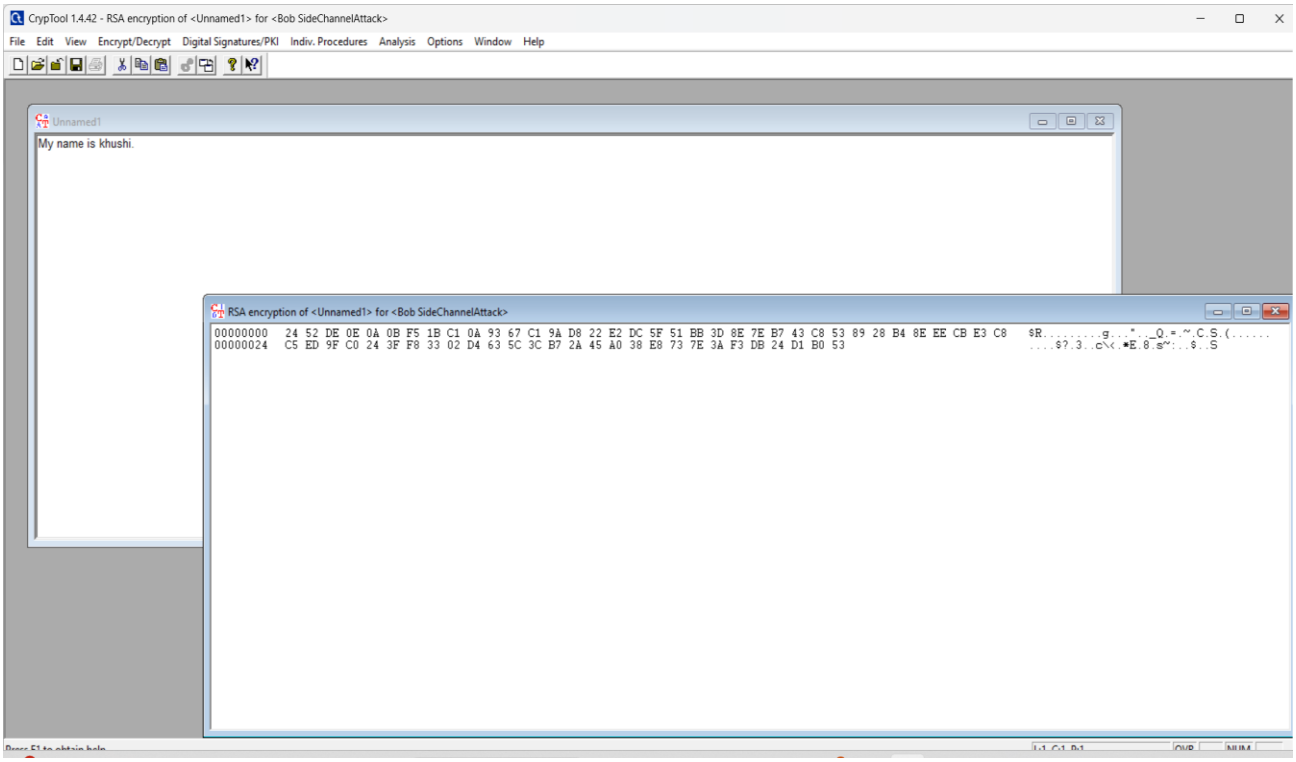
1) Select a RSA Encryption:



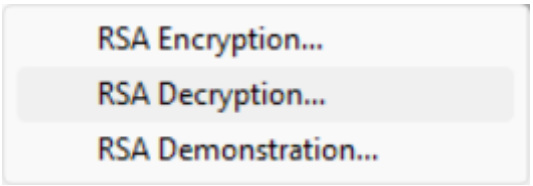
2) Select a recipient: (Encrypt button click):



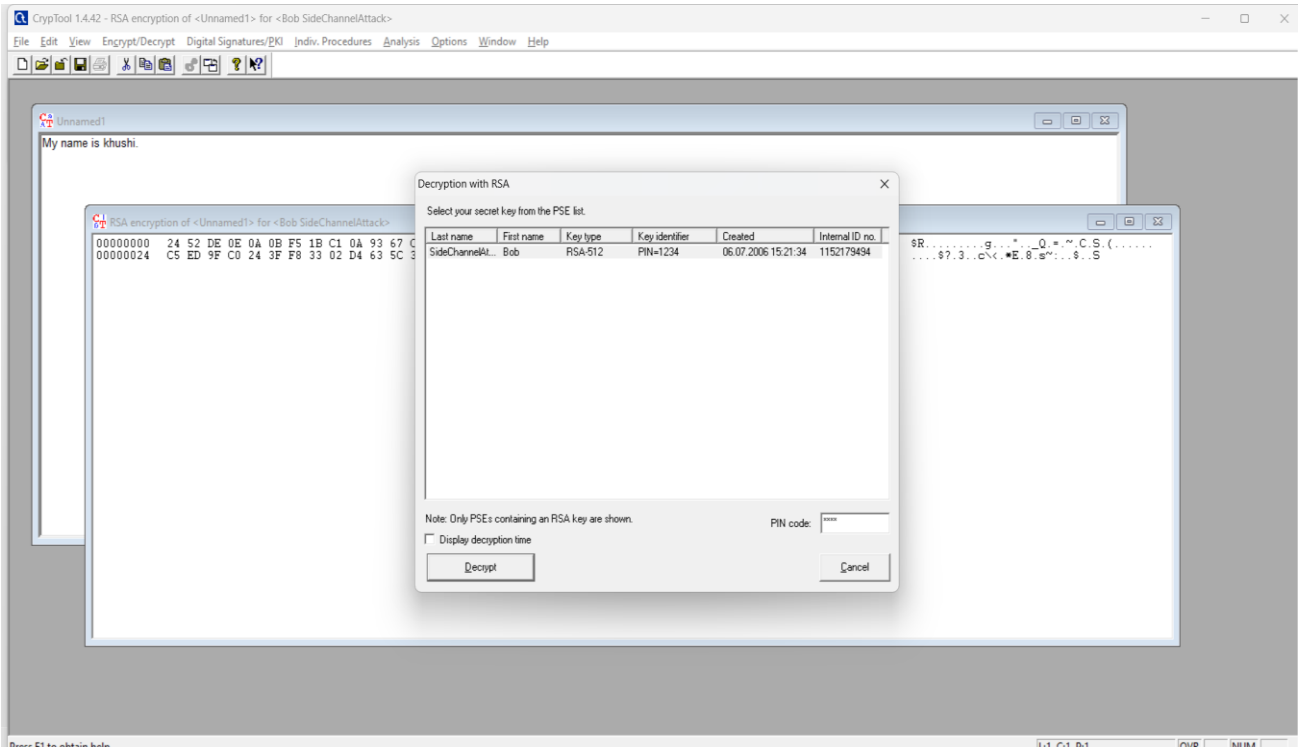
3) Encrypt a message :



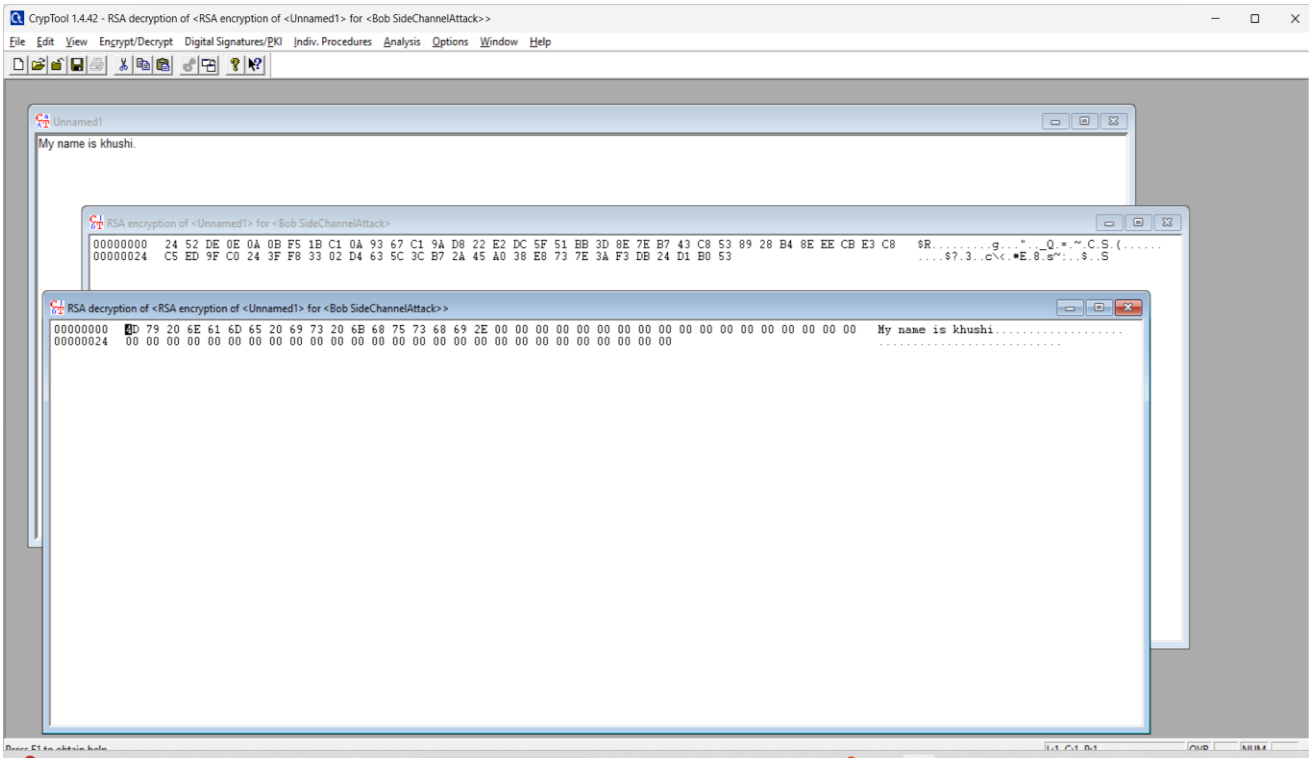
4) Decryption :



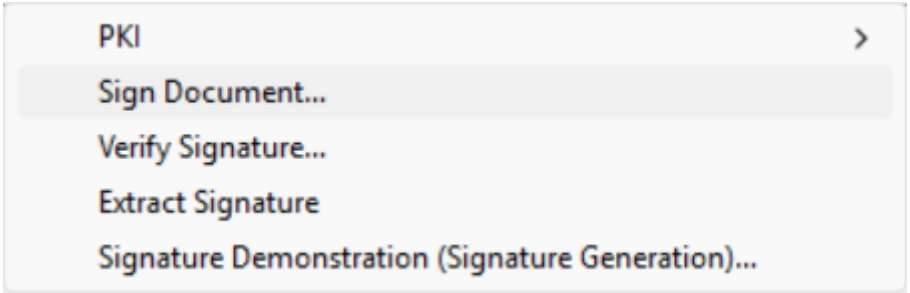
5) Decryption (Enter a pincode and click a Decrypt button):



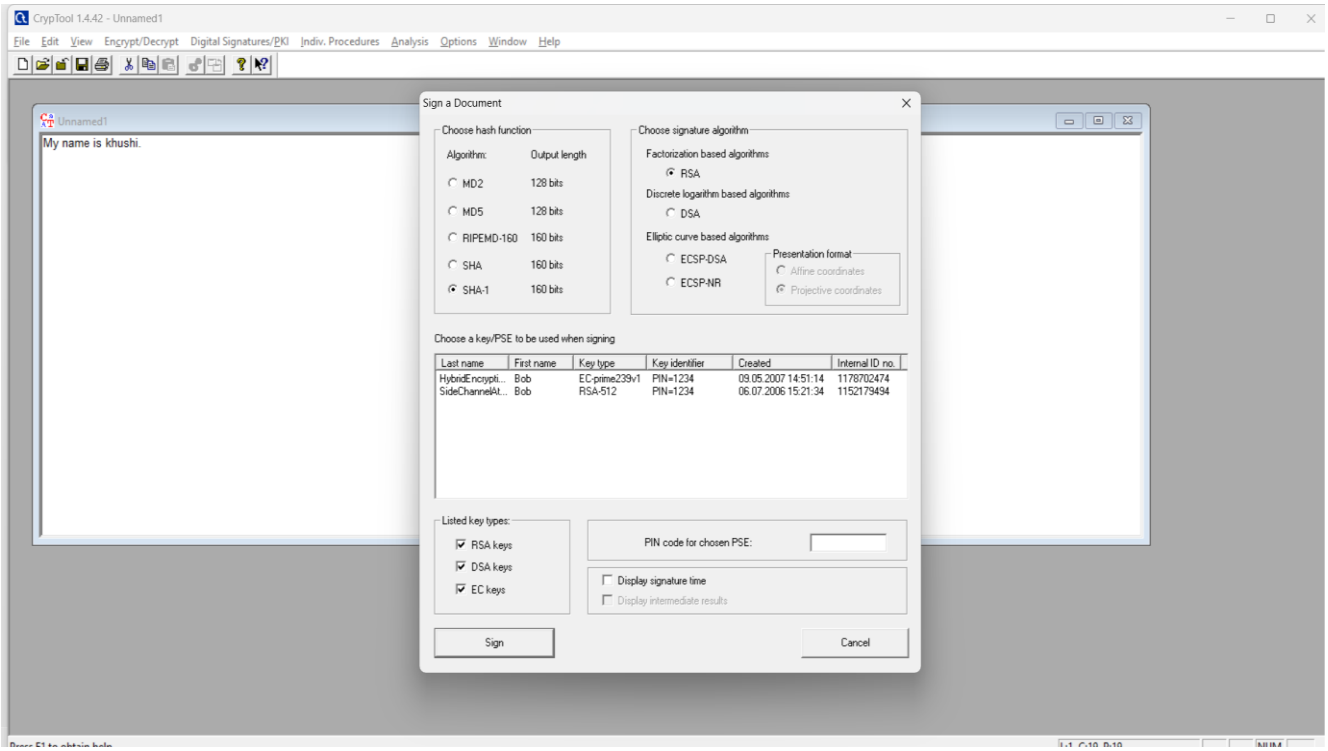
6) Decrypt a message :



7) Sign Document :

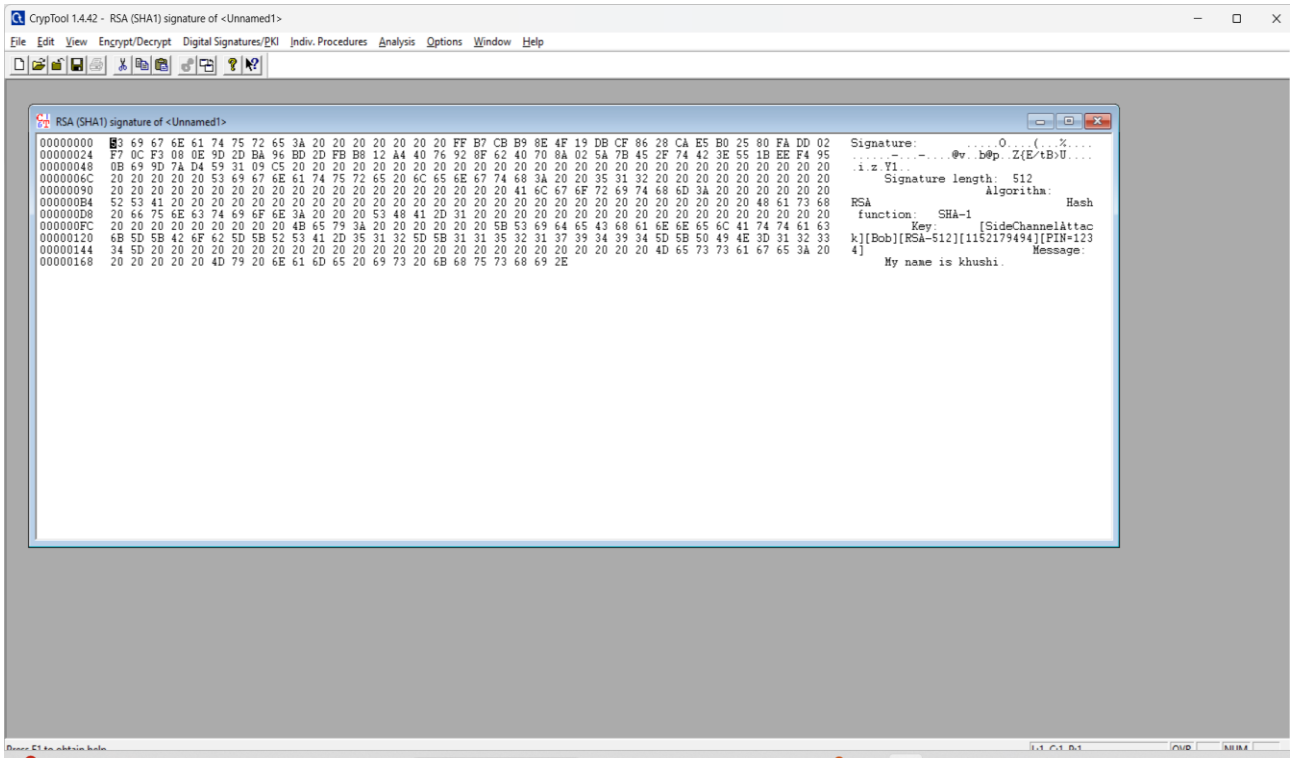


8) RSA Sign a Document :



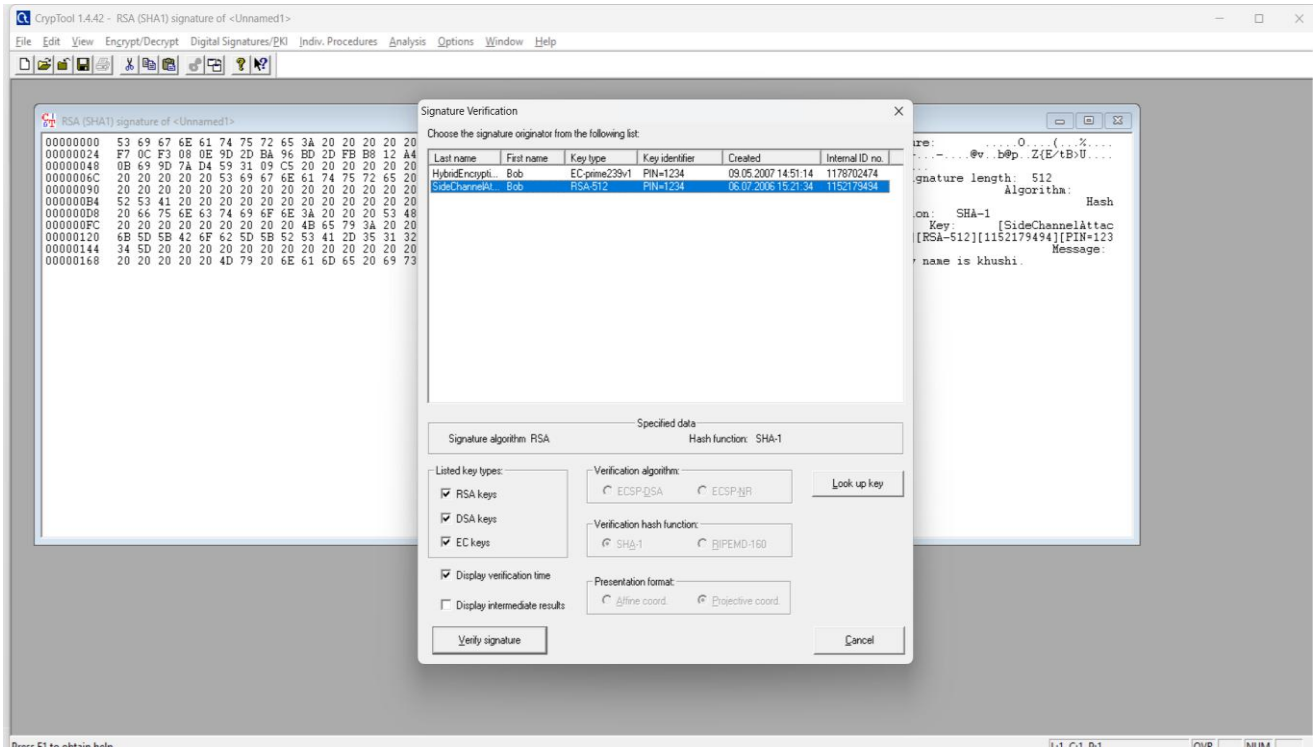
9) Enter a pincode (click a sign button):

10) Digital signature :

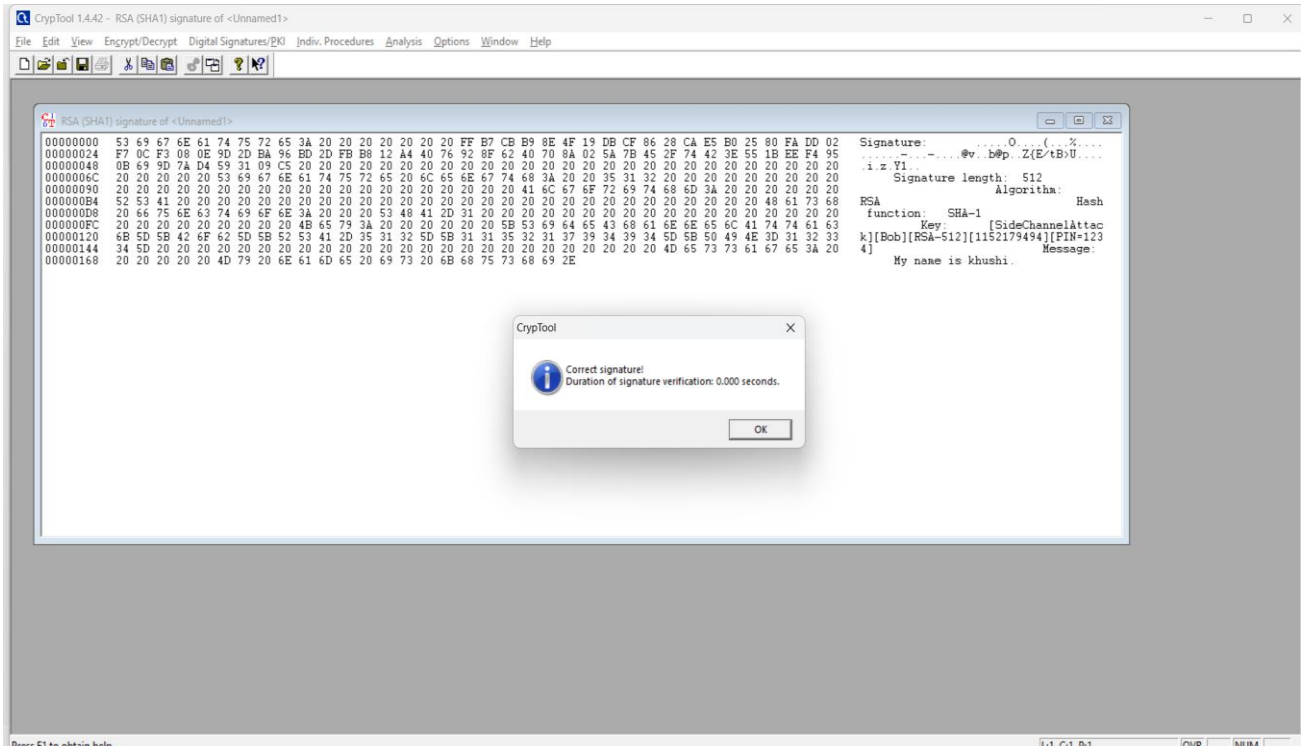


11)Verify Signature:

12)Select a algorithm and verify signature :

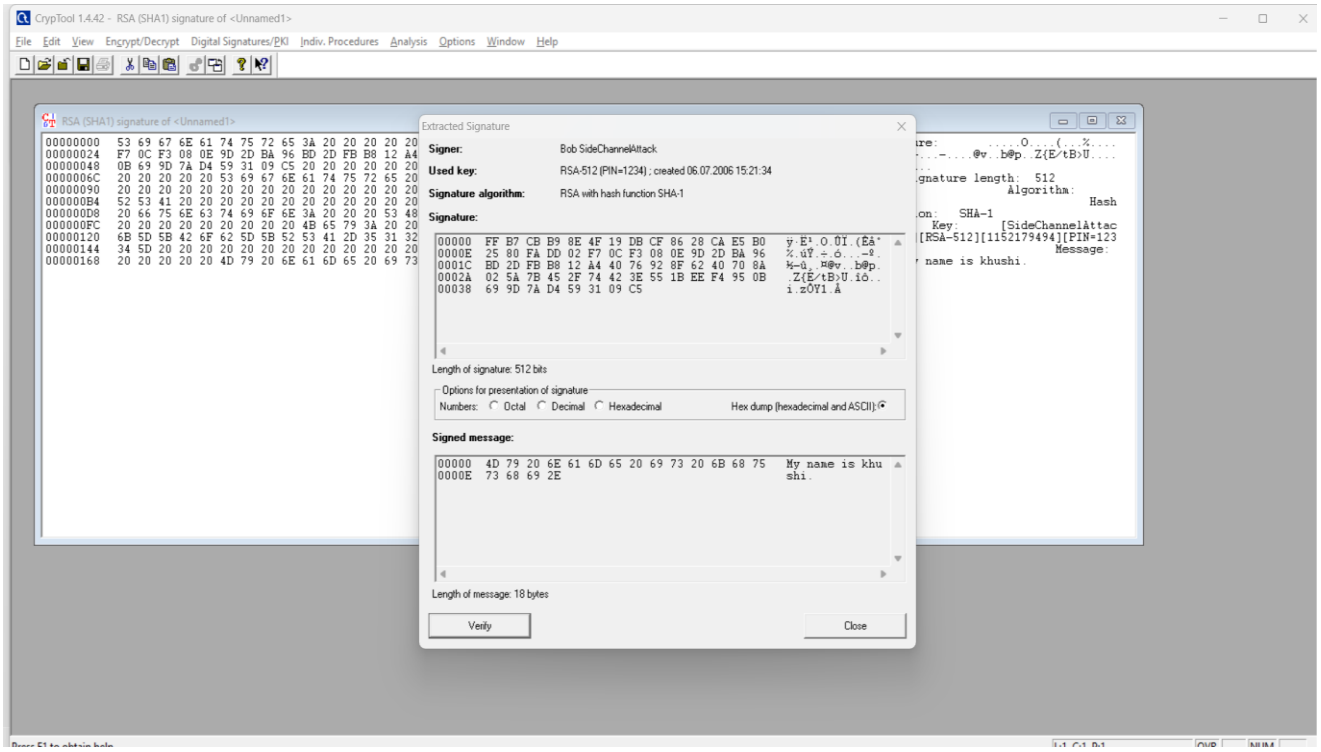


13)Verification Time :

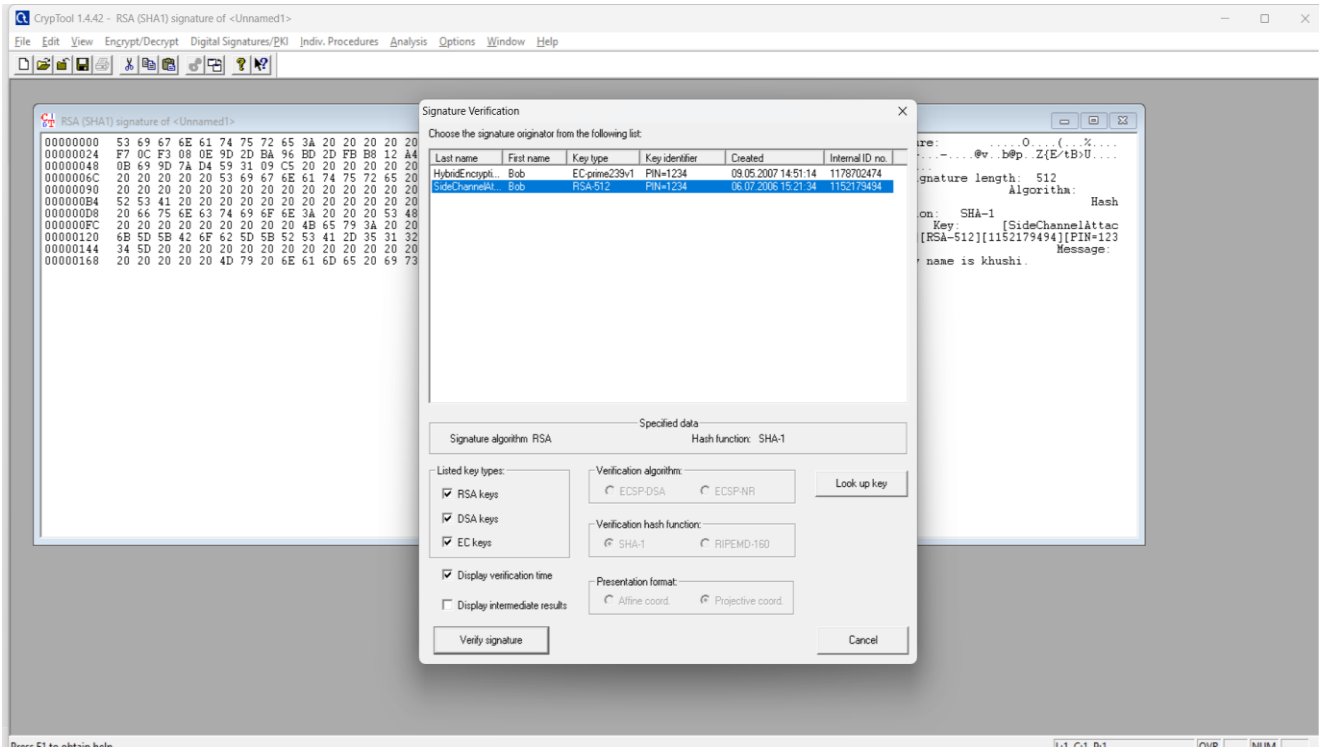


14) Extract Signature :

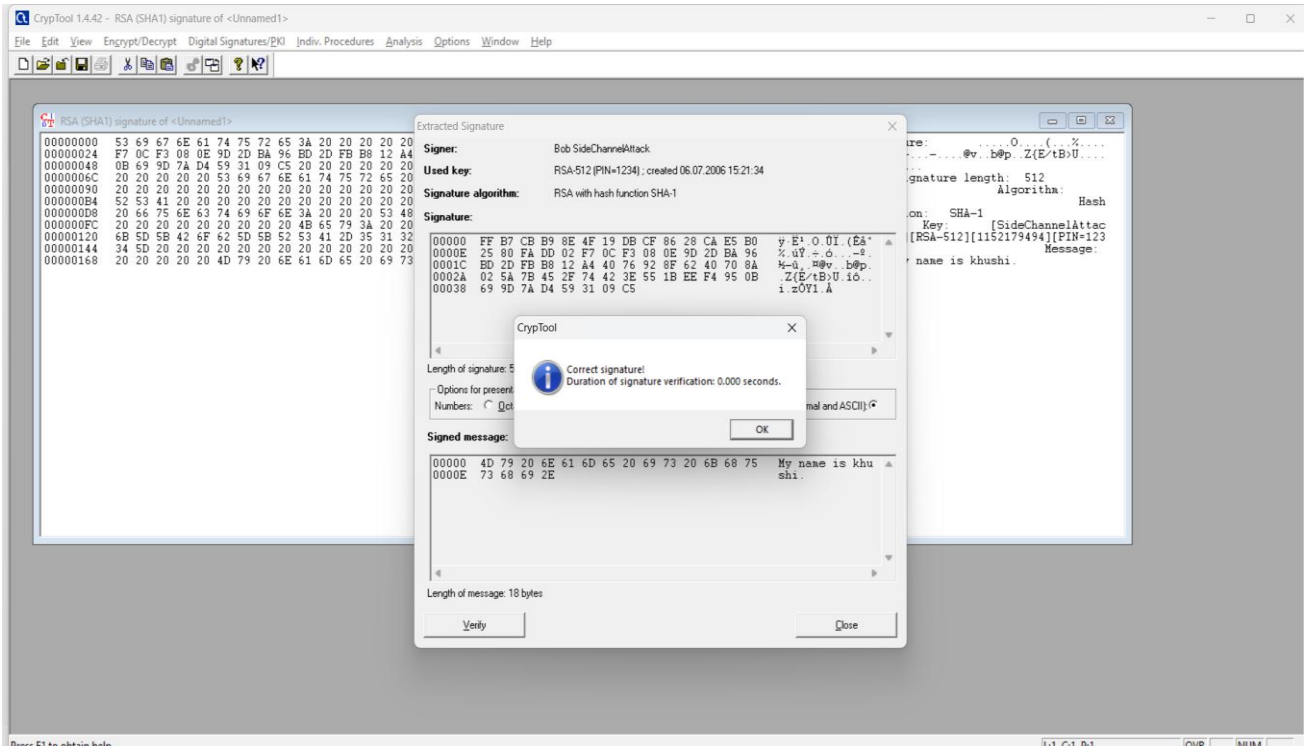
15)verify a key :



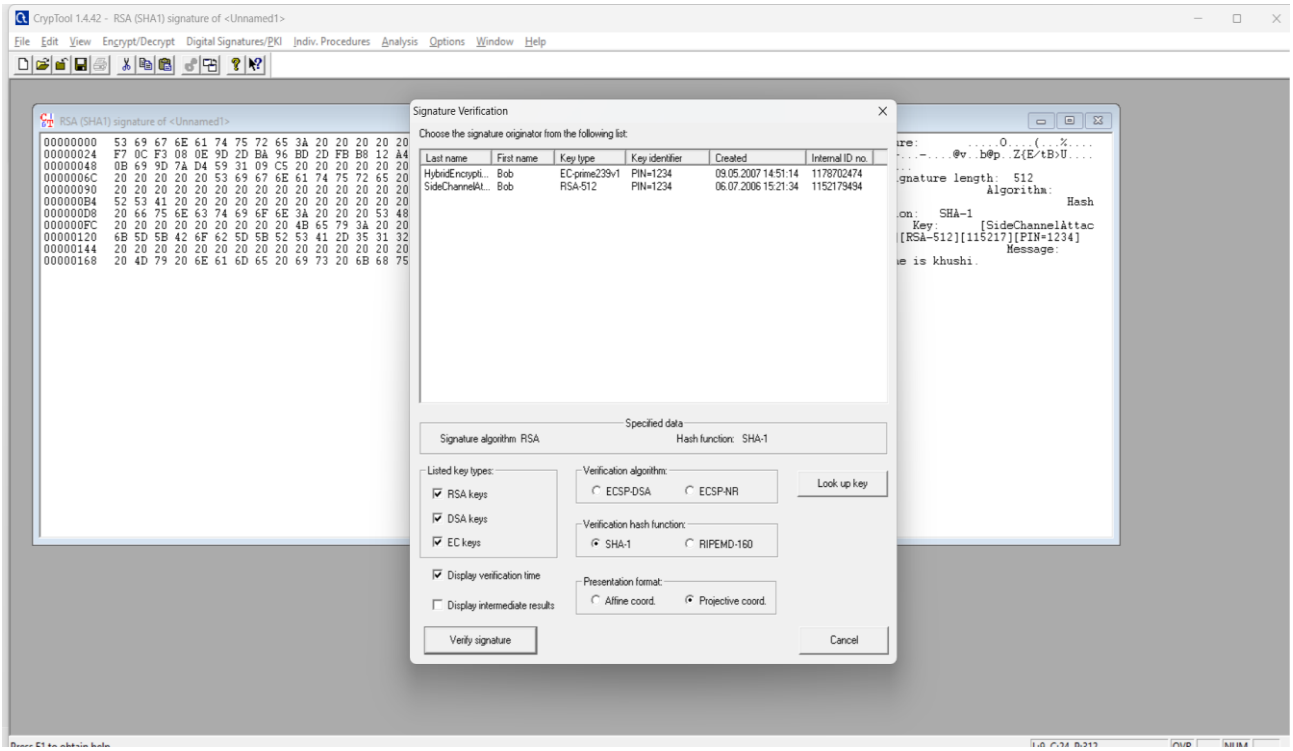
16) select a algorithm and verify :



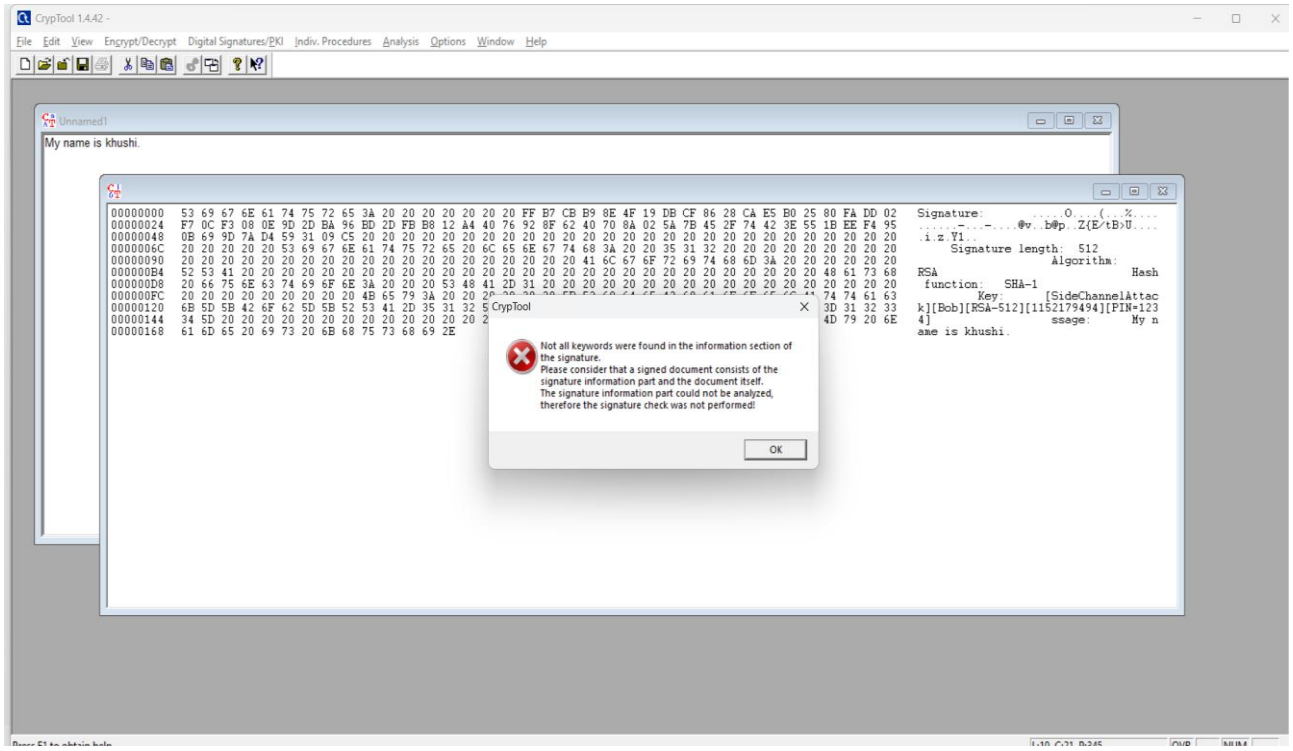
17)Verification time :



18)Select algorithm and verify (change a file contain):



19)Not Found digital signature :



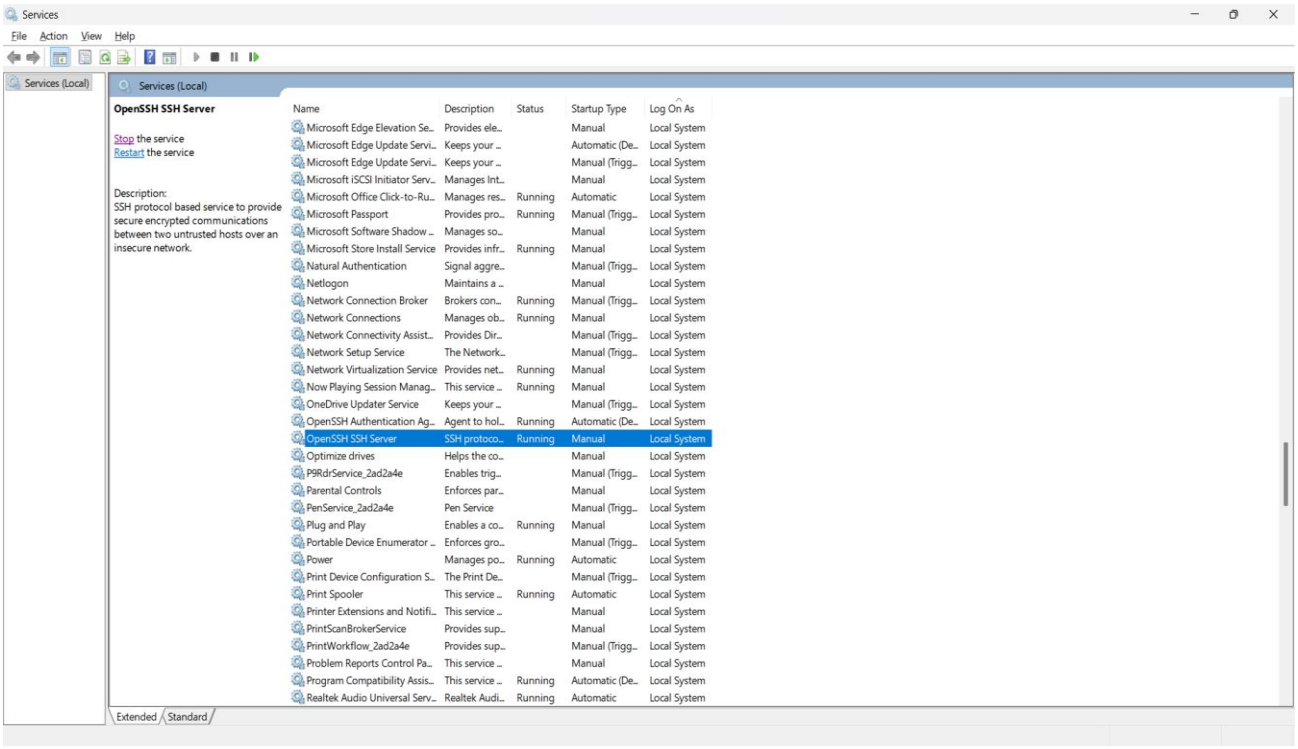
Practical-17

AIM:

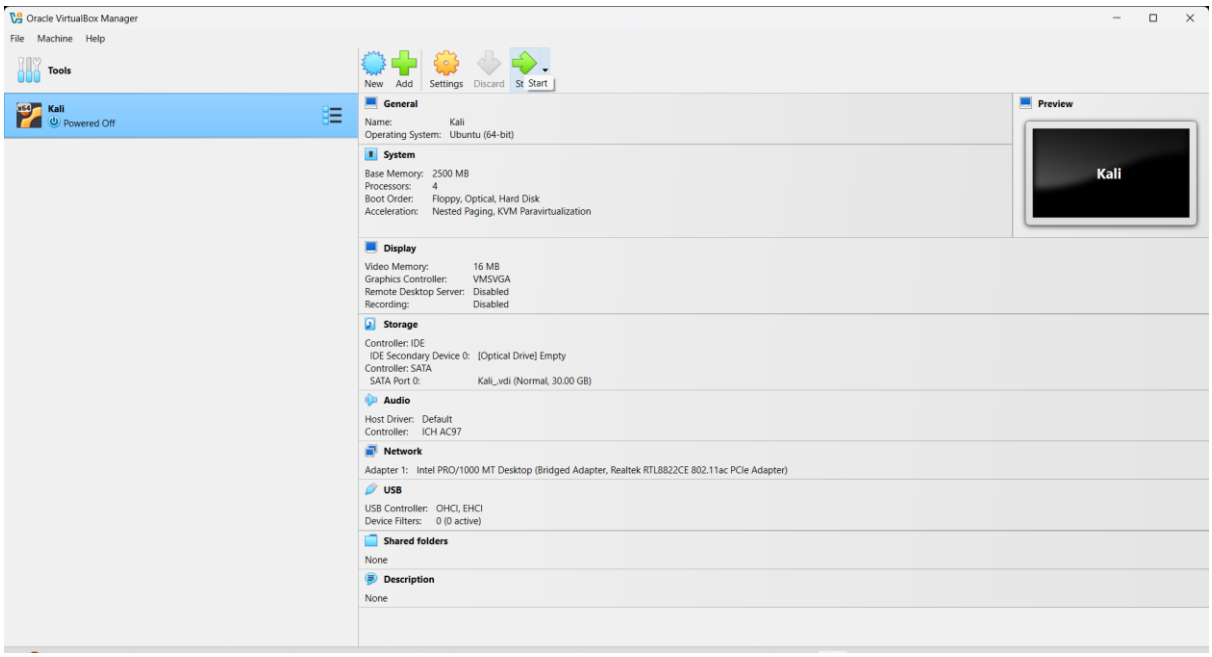
Demonstrate SSH brute-force exploitation using Hydra to understand authentication weaknesses, credential security, and preventive mitigation strategies.

STEPS with screenshots:

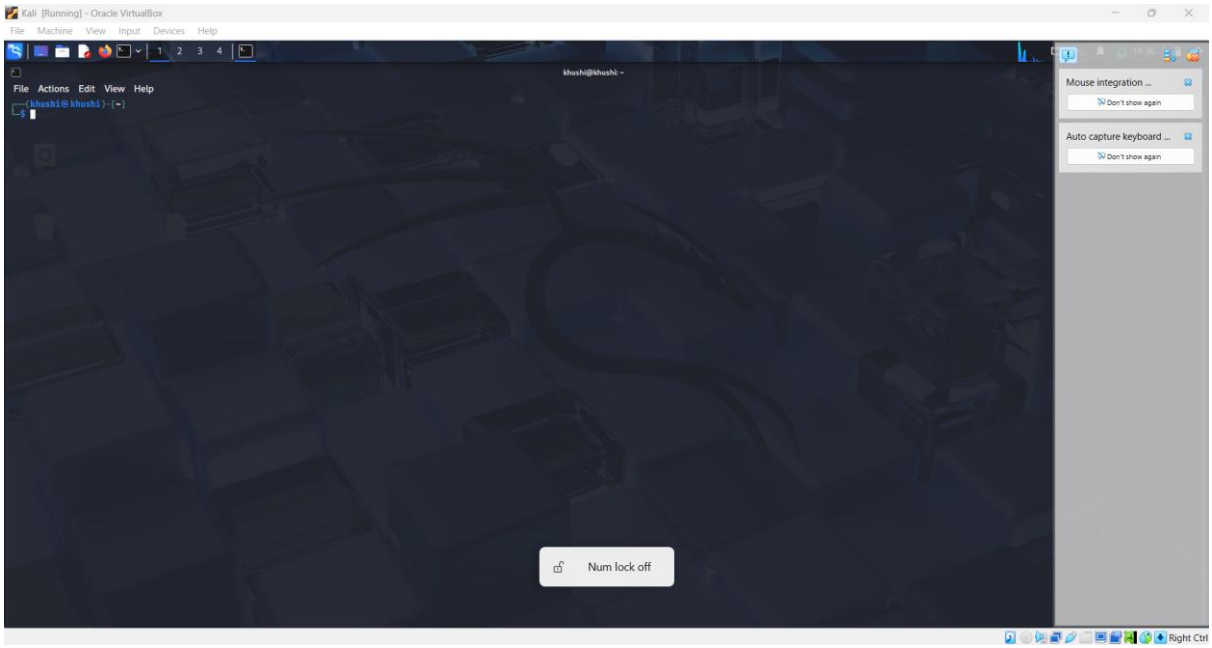
1) Start a SSH Server:



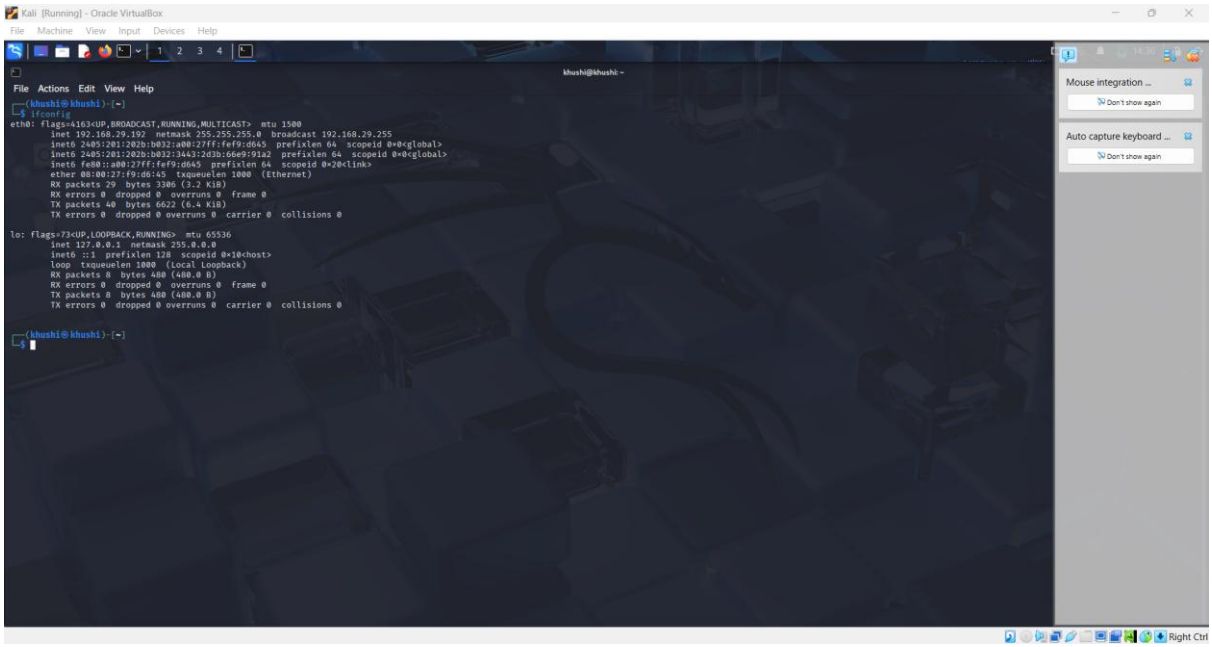
2) Start a kali :



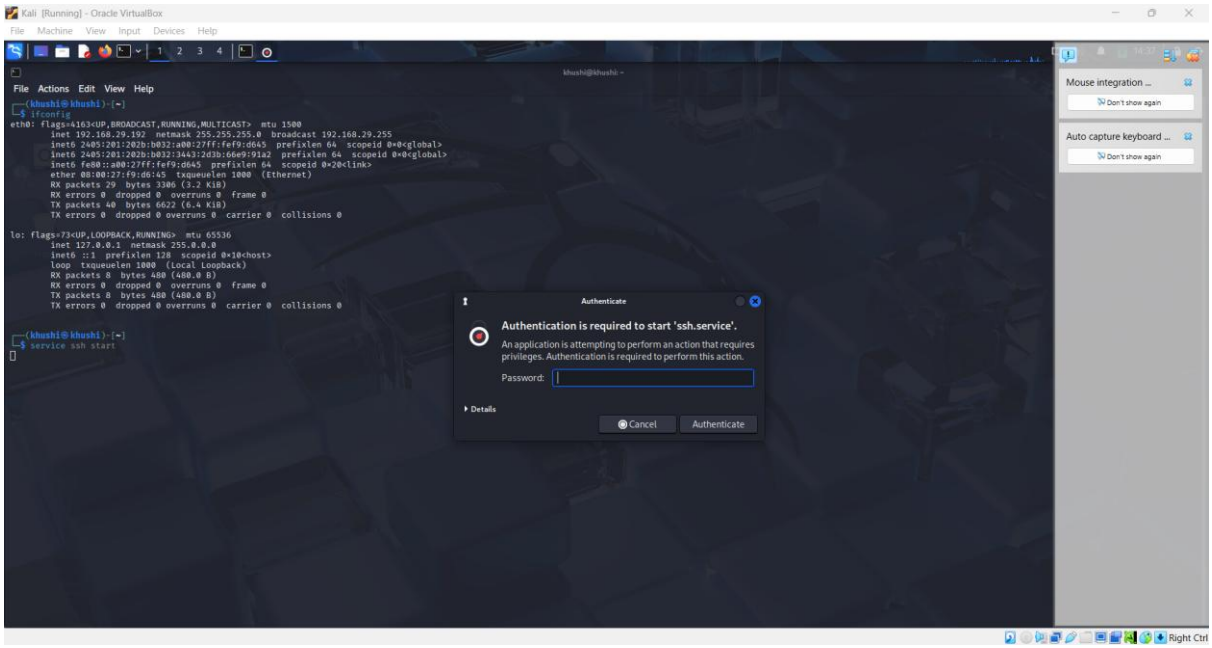
3) Start a Terminal :



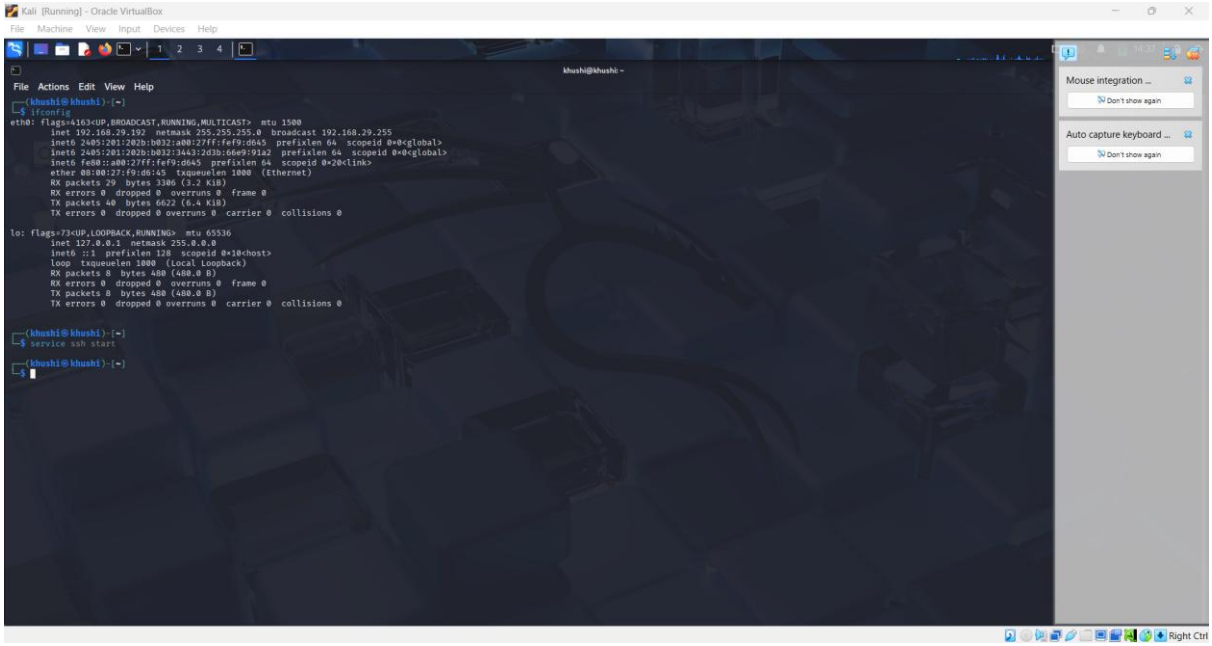
4) Find Ip Address :



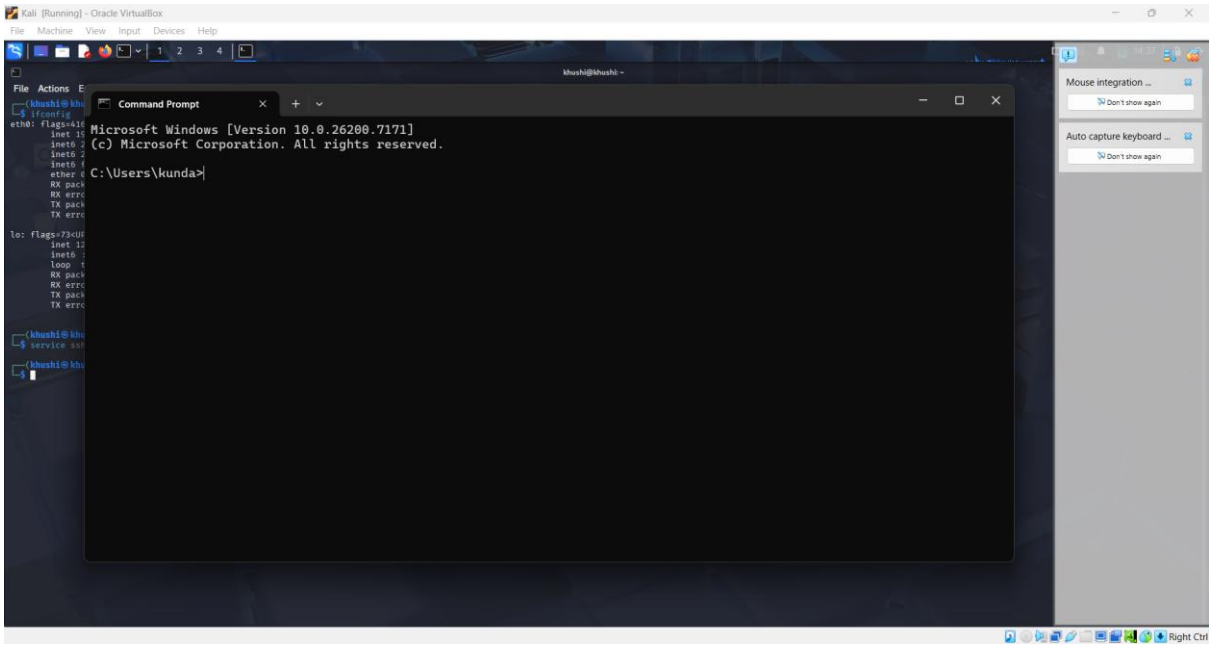
5) Service SSH Start :



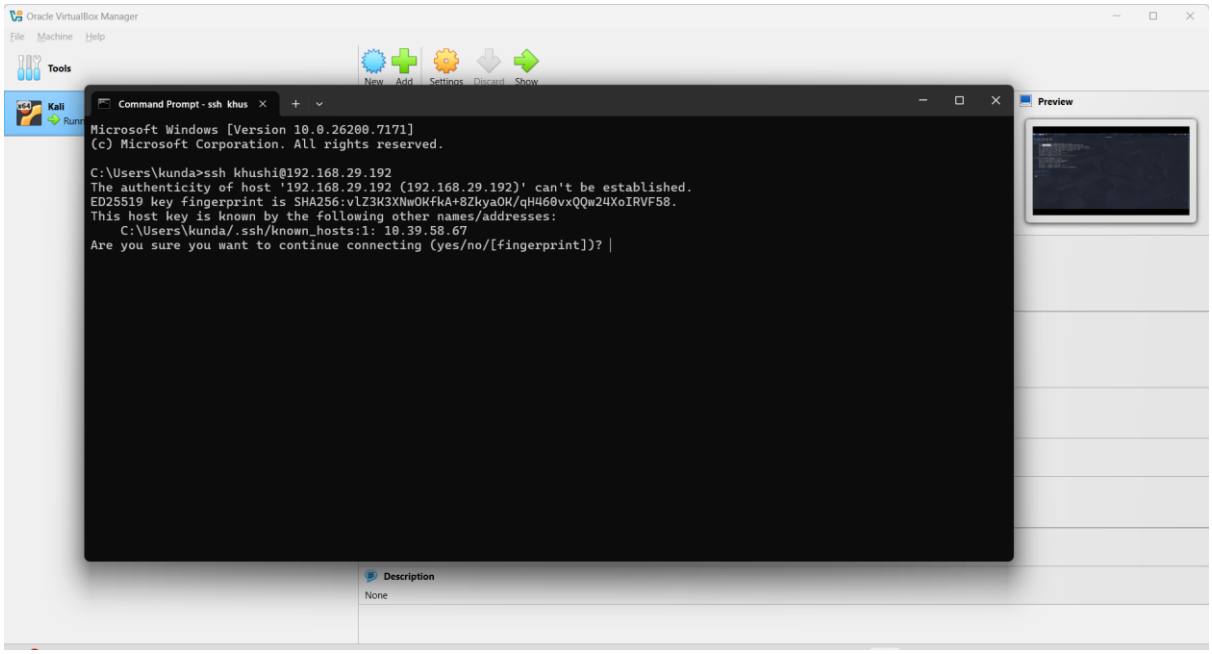
6) Server is started :



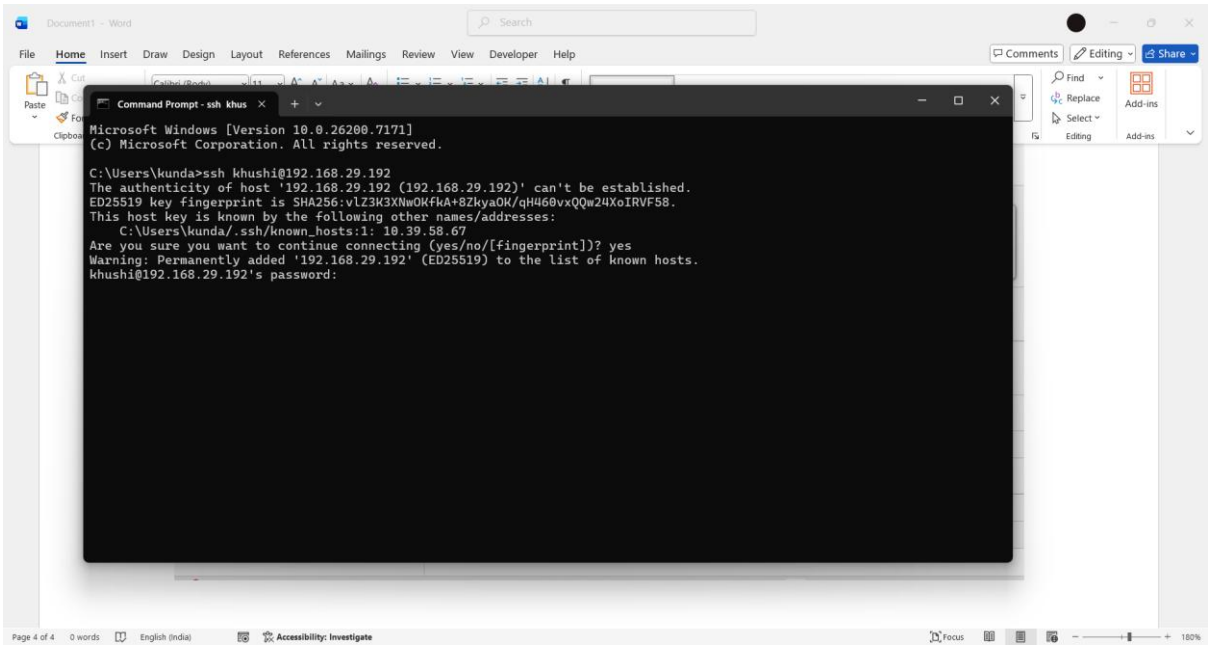
7) Open a Windows CMD:



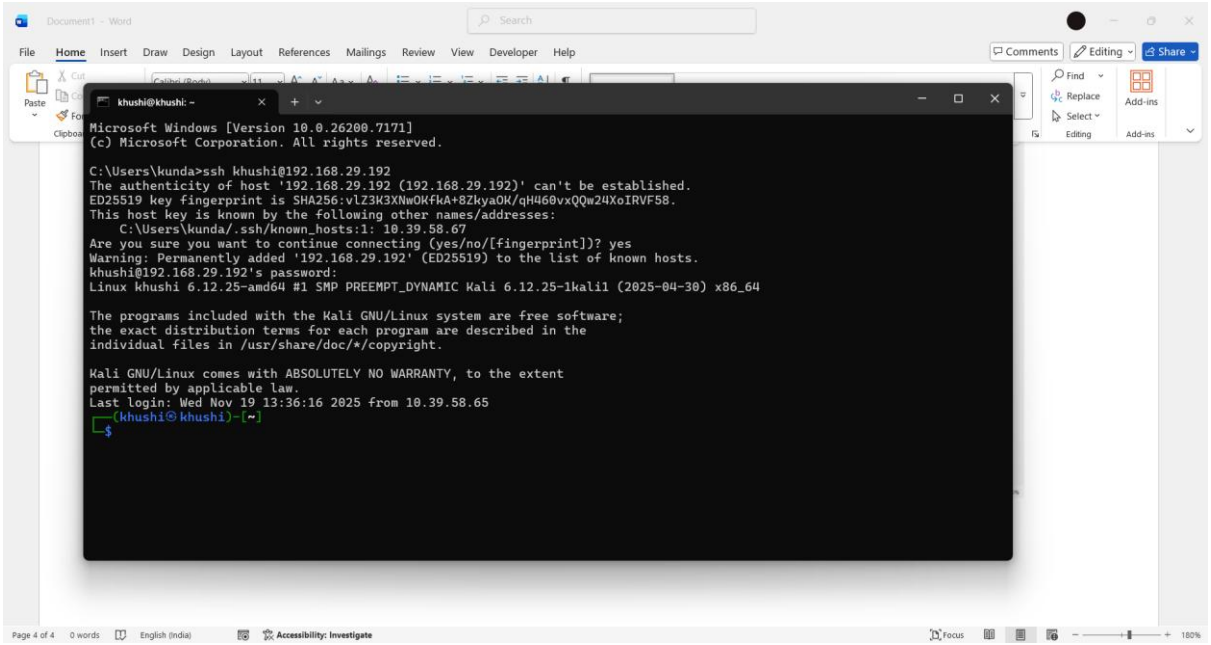
8) Run SSH khushi@Ip of kali:



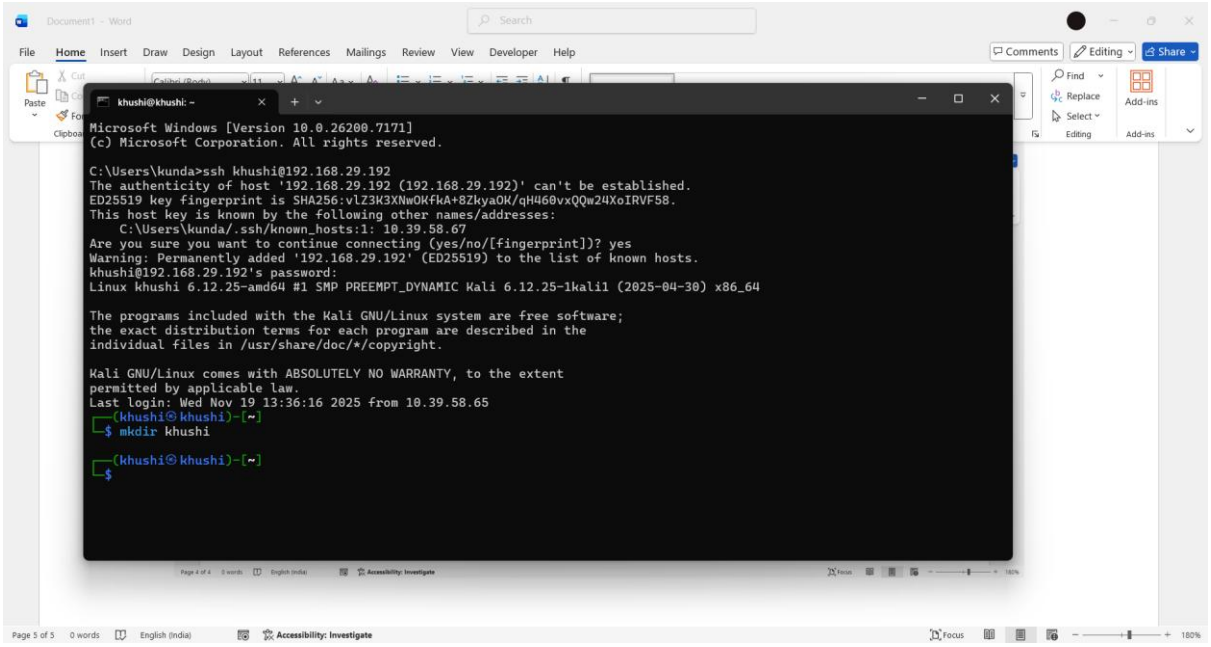
9) Enter a Kali Password :



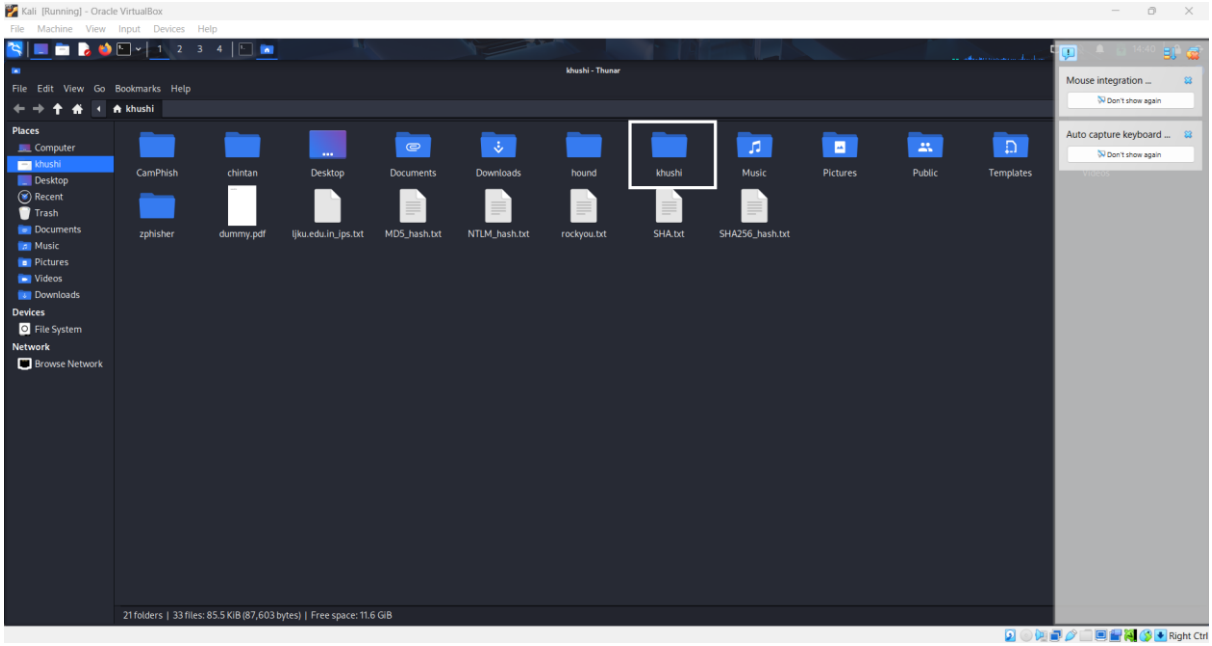
10) Start acess of Kali :



11) Create a directory :



12) Show make a Directory :



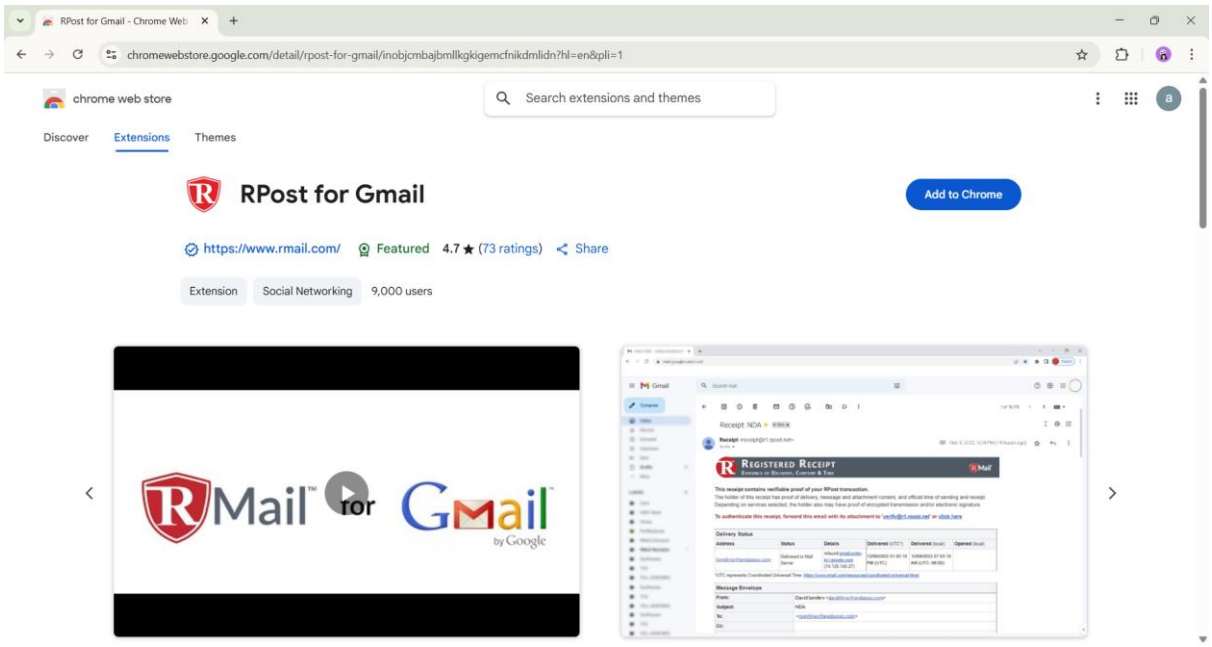
Practical-18

AIM:

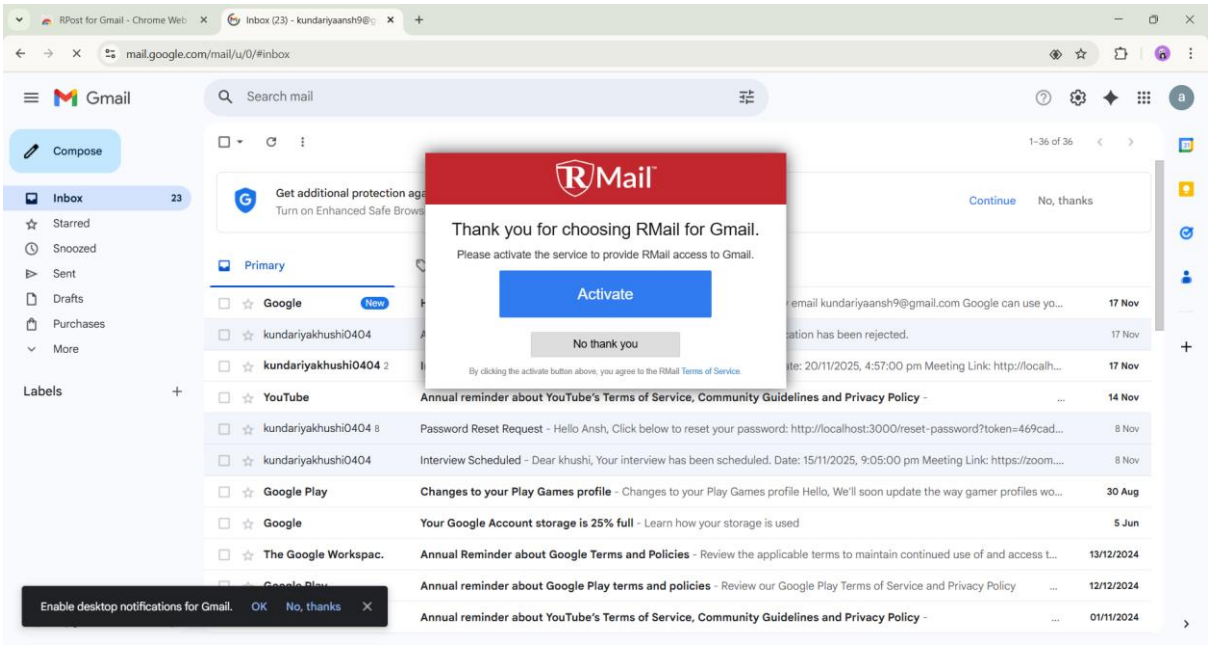
Configure encrypted and digitally signed communication using RMail to understand secure email workflows, confidentiality assurance, and sender authenticity validation.

STEPS with screenshots:

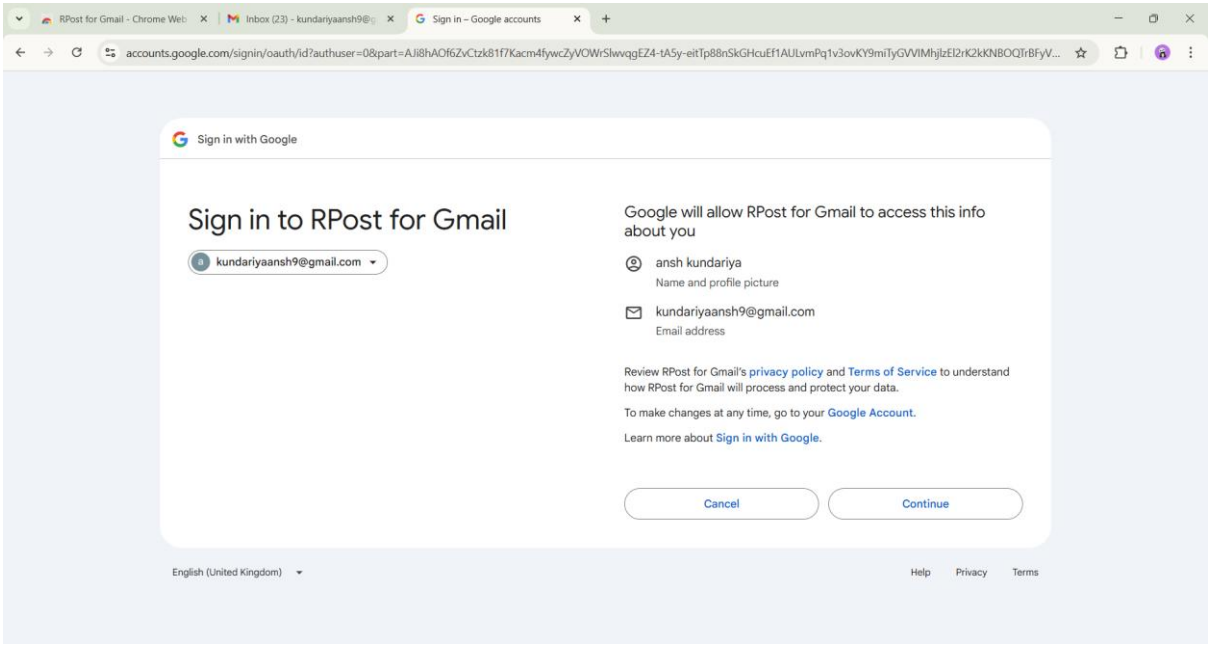
1) Add a Extension :

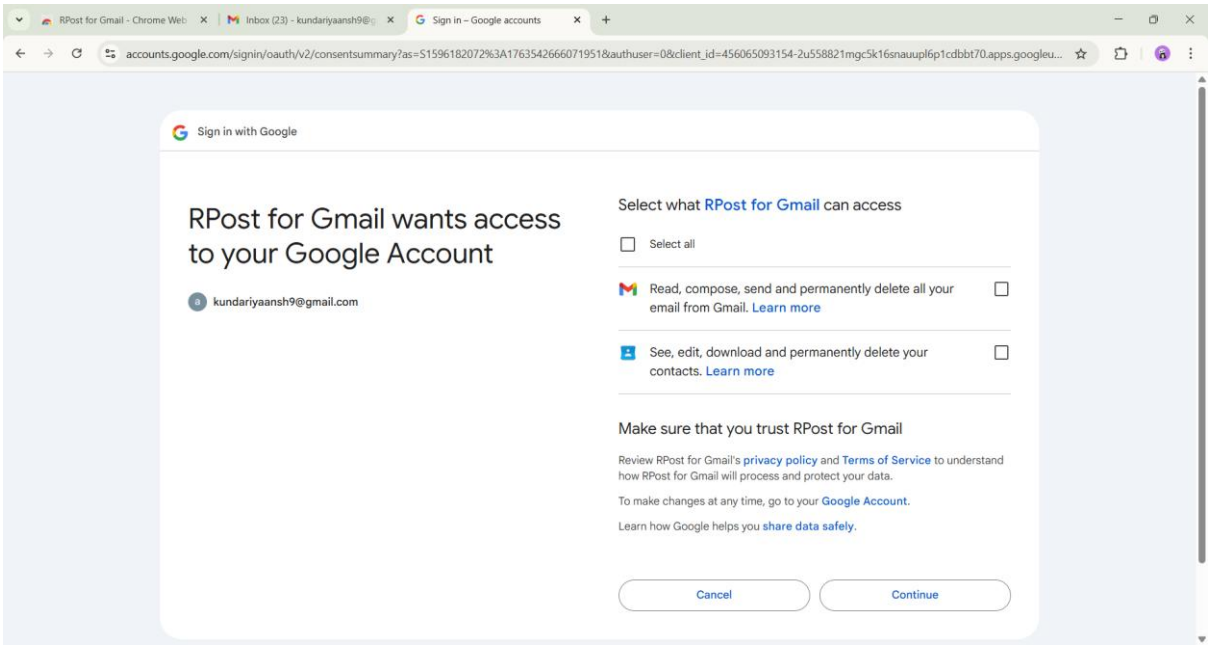


2) Active a Rmail:

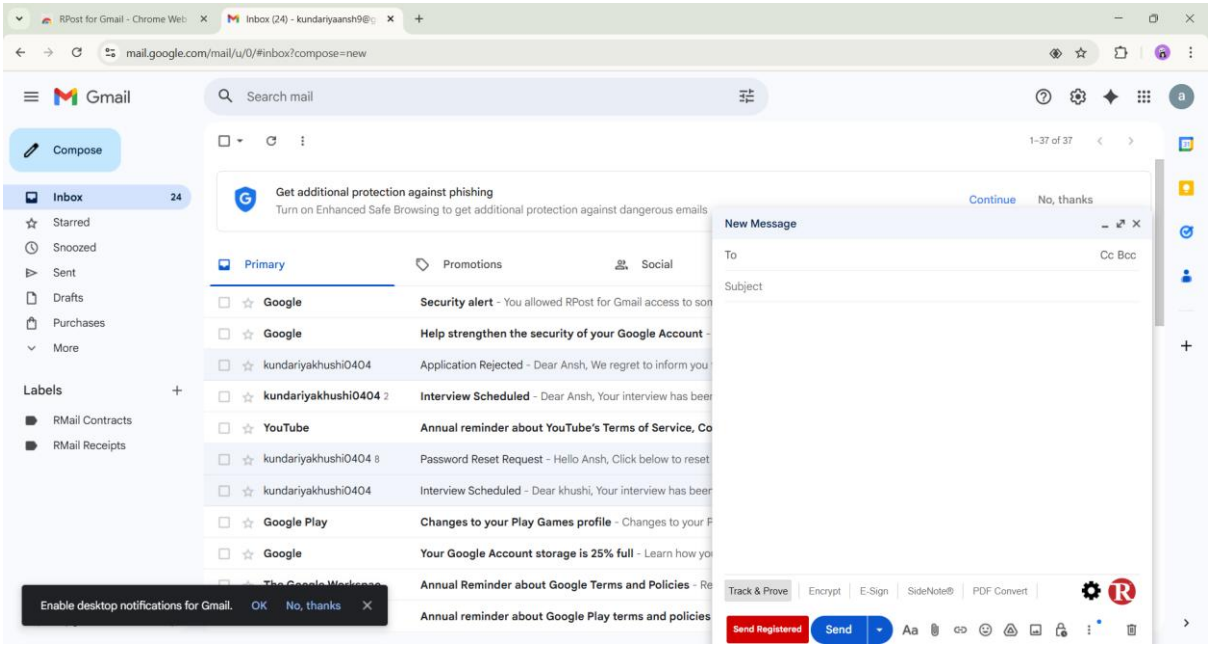


3) Authentication :

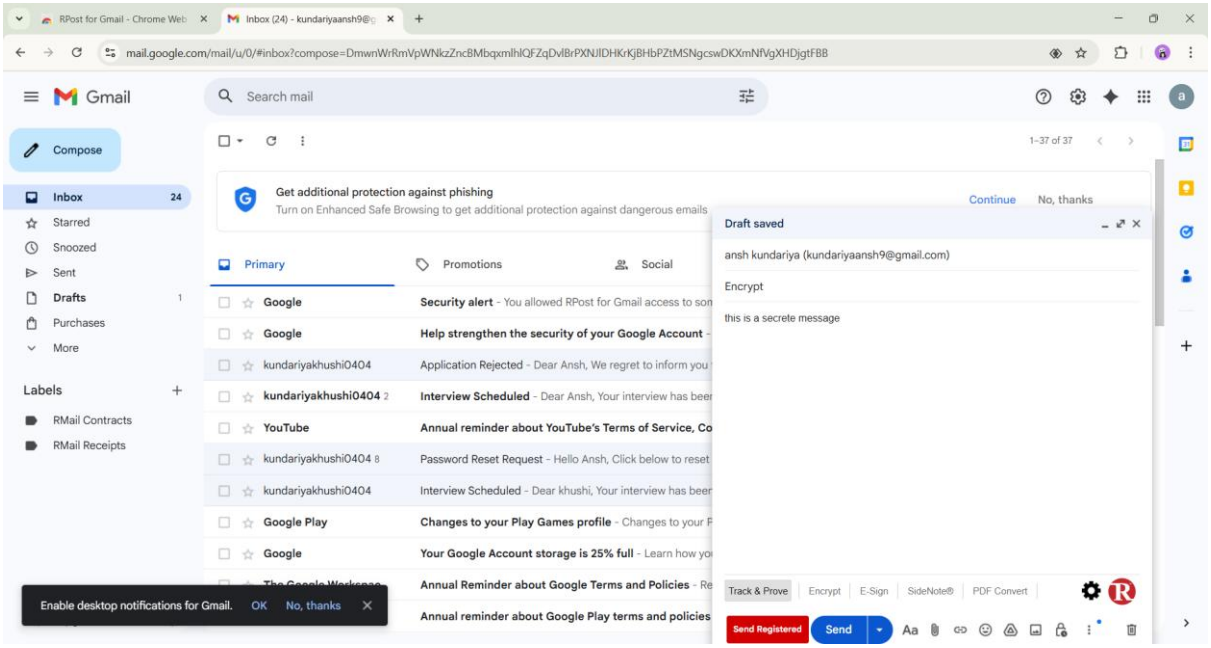




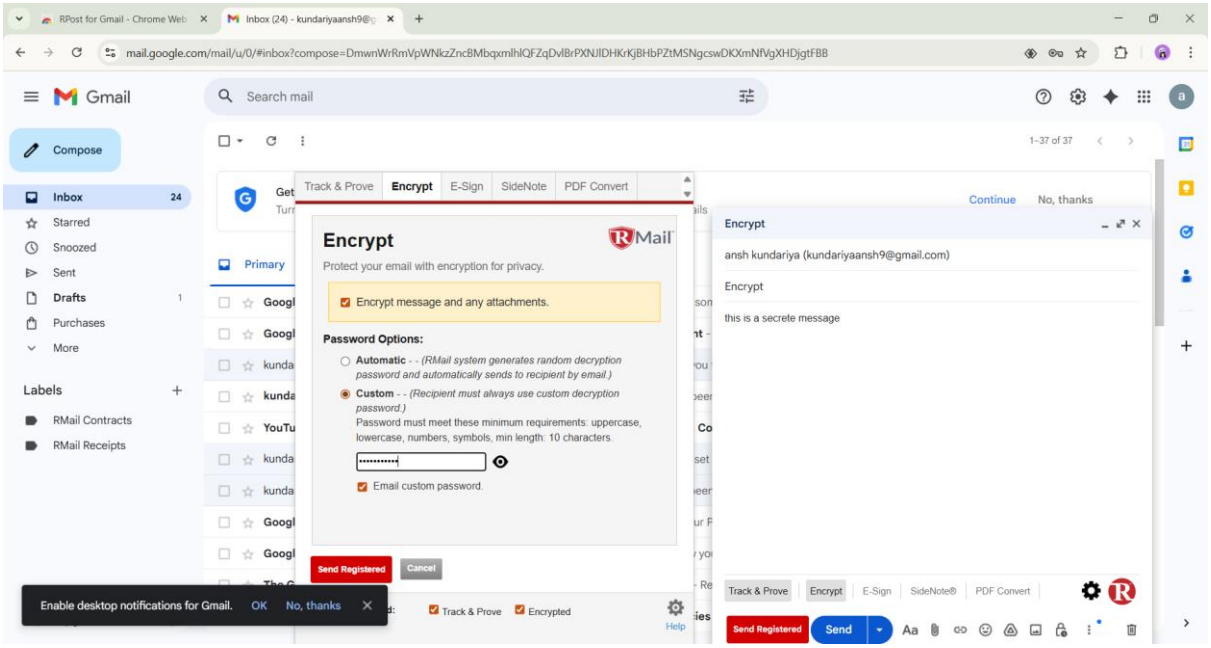
4) Open a Compose :



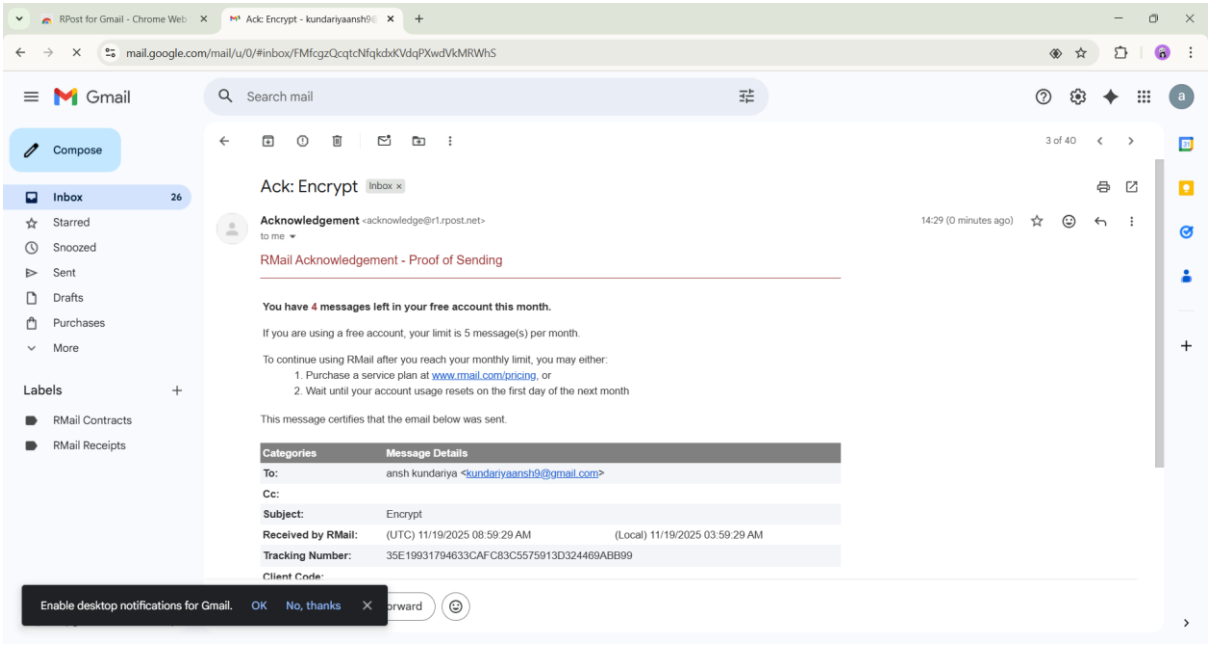
5) Mail Message :



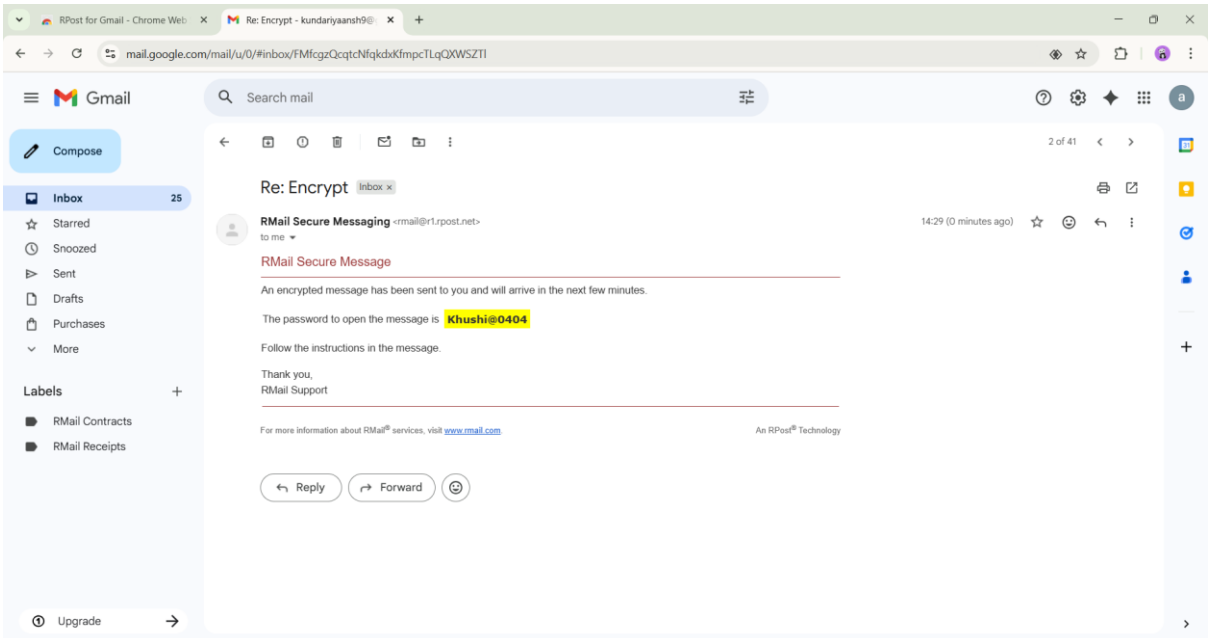
6) Click a Encrypt Button :



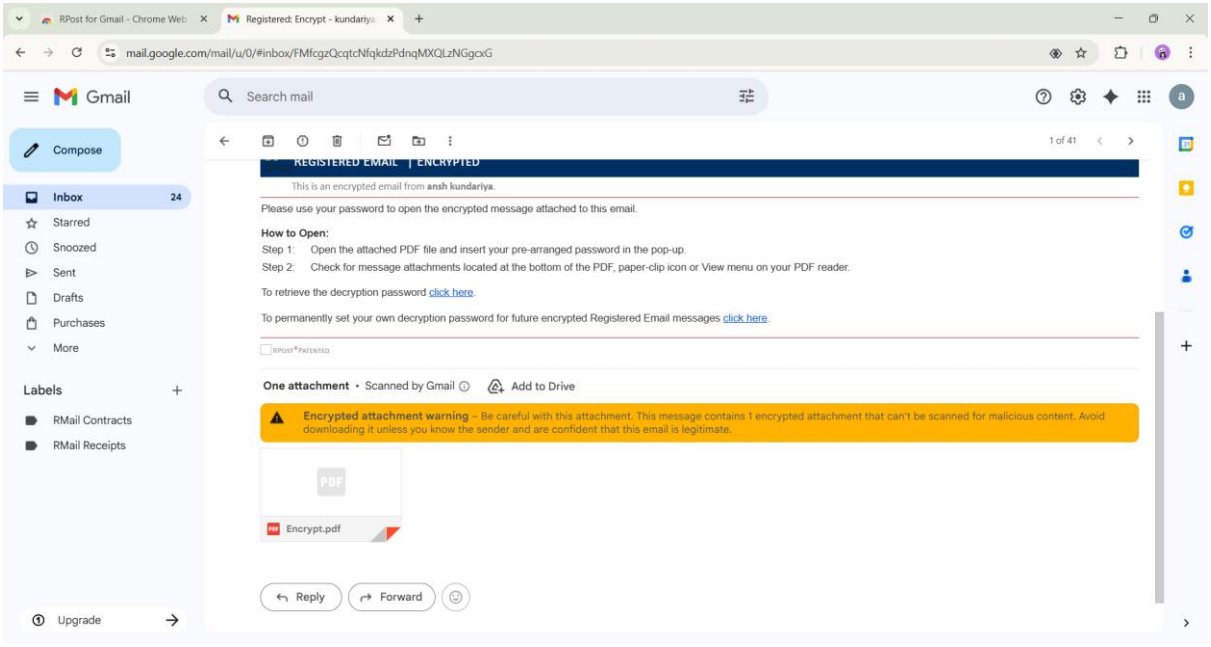
7) Security Mail:



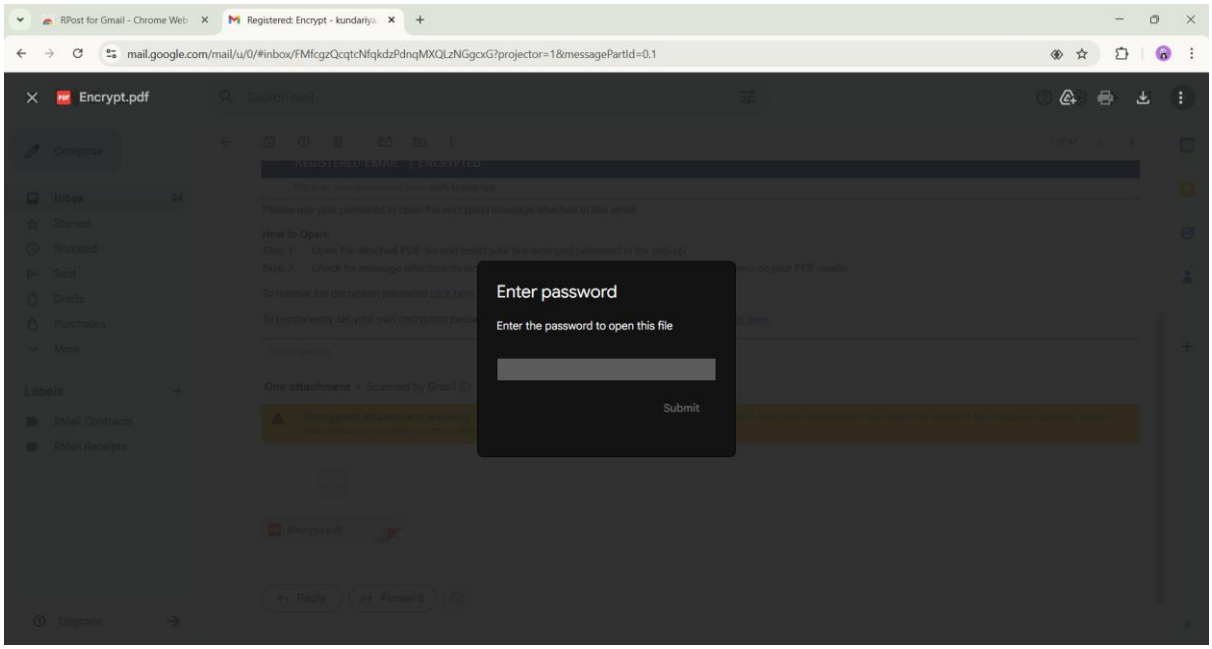
8) Password Mail :



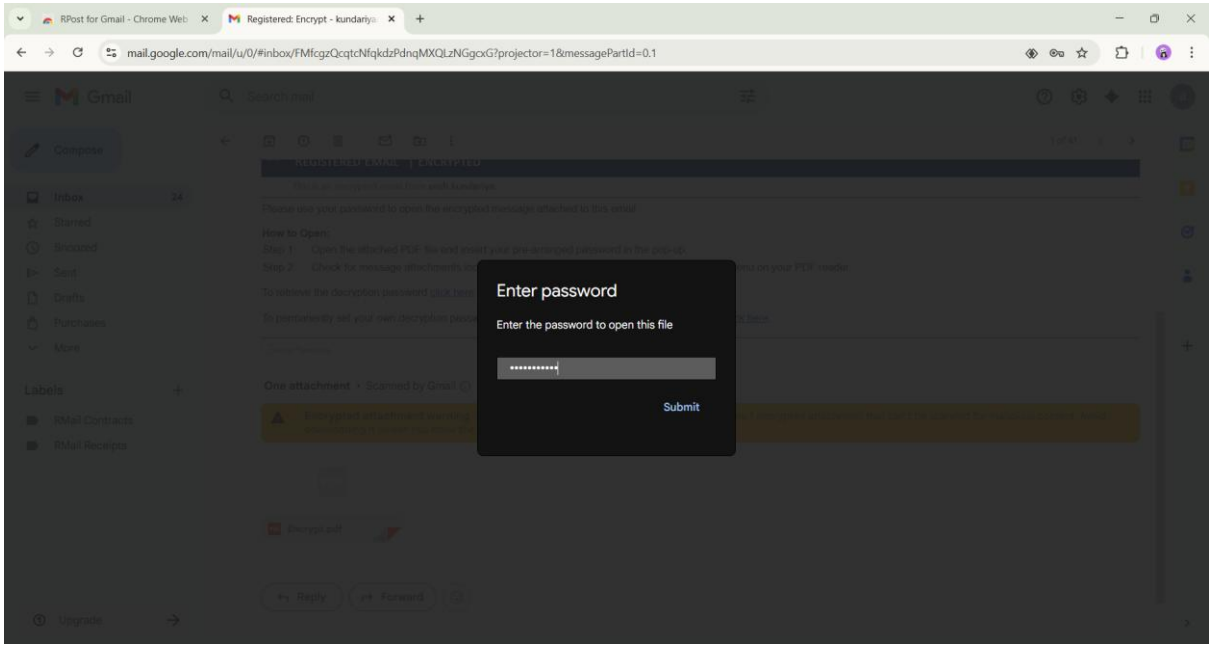
9) Encrypt file mail:



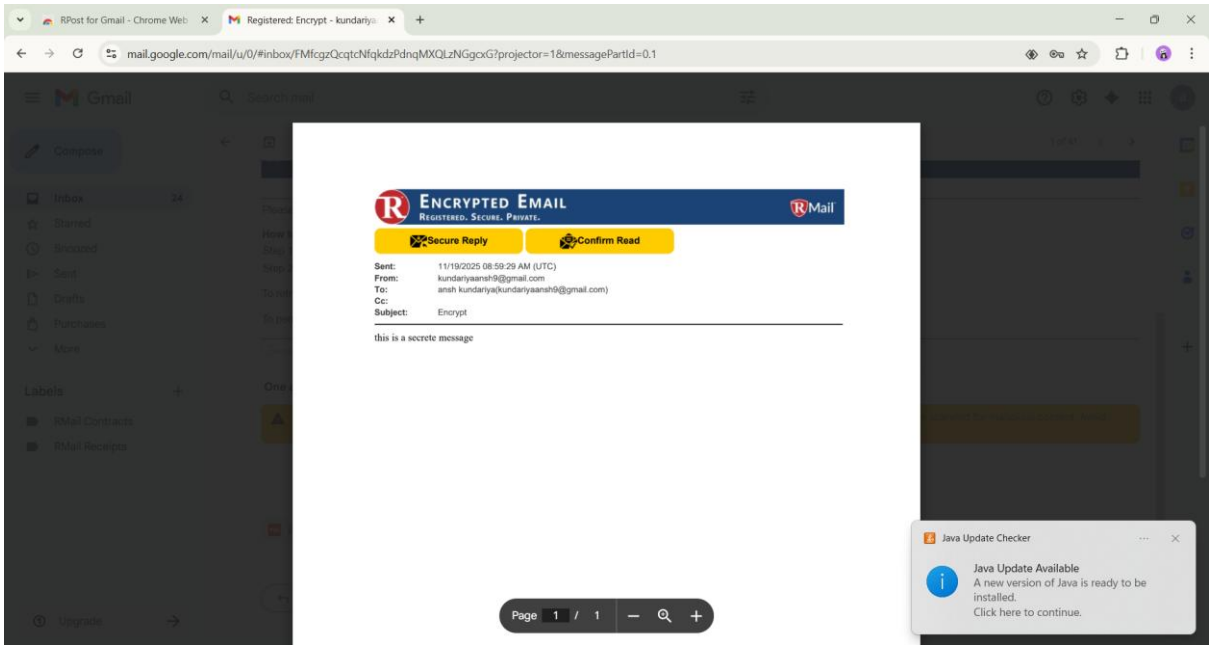
10)Enter A password :



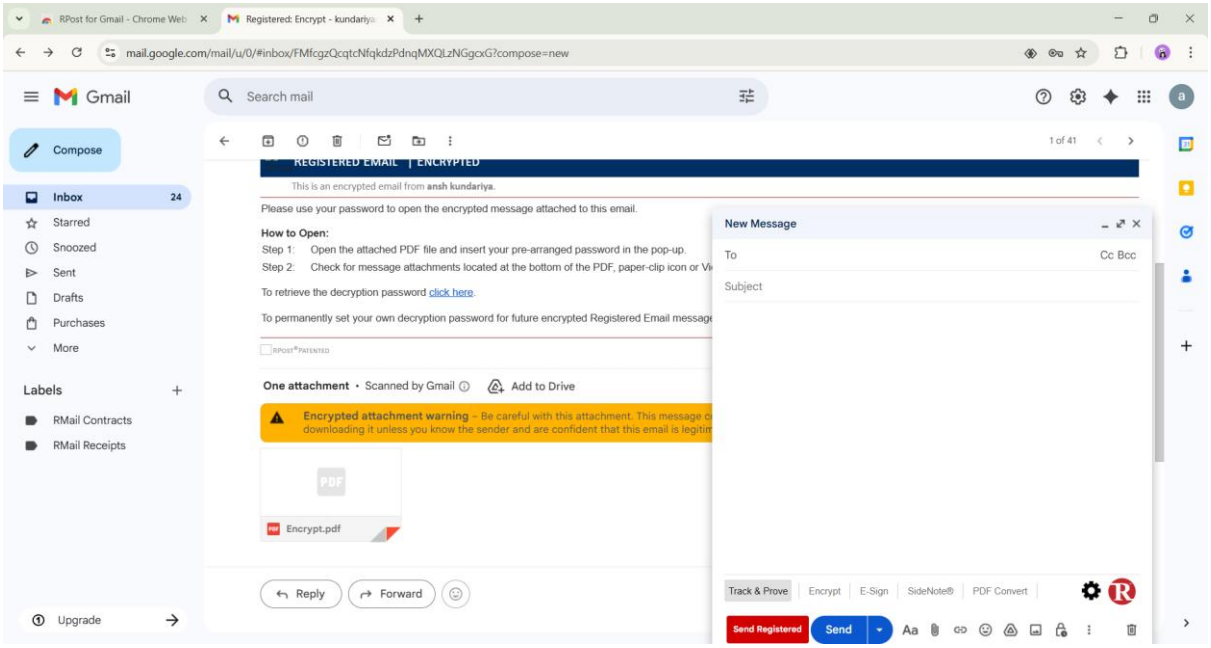
11)Submit a password :



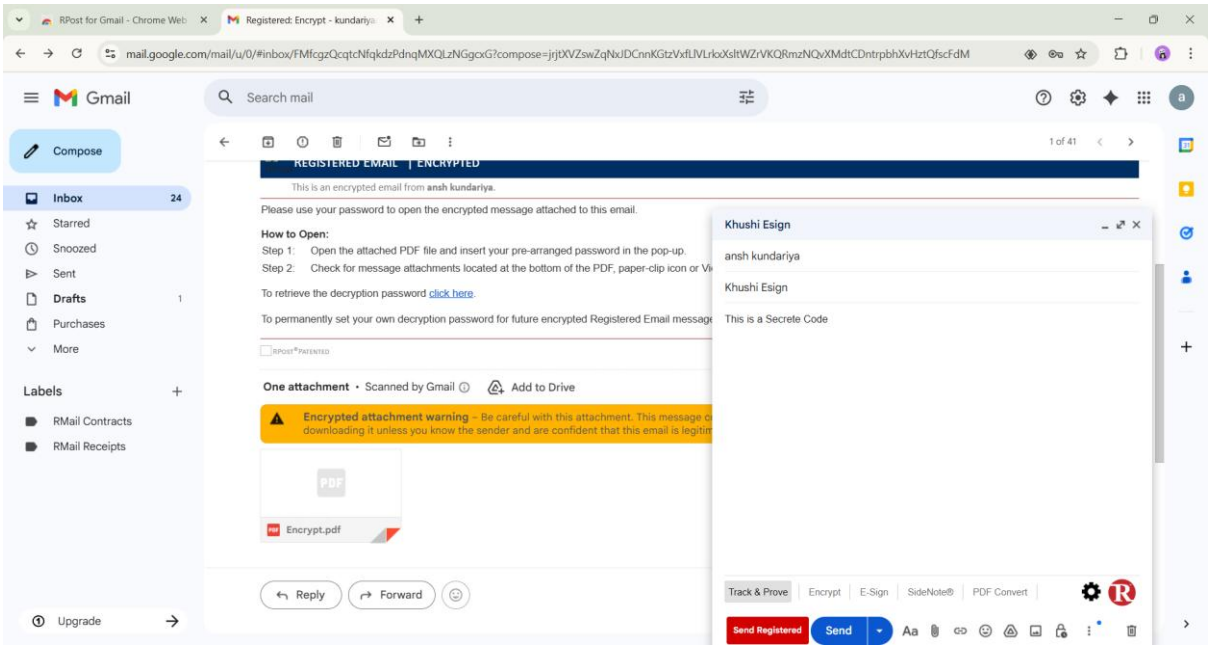
12) File is Open :



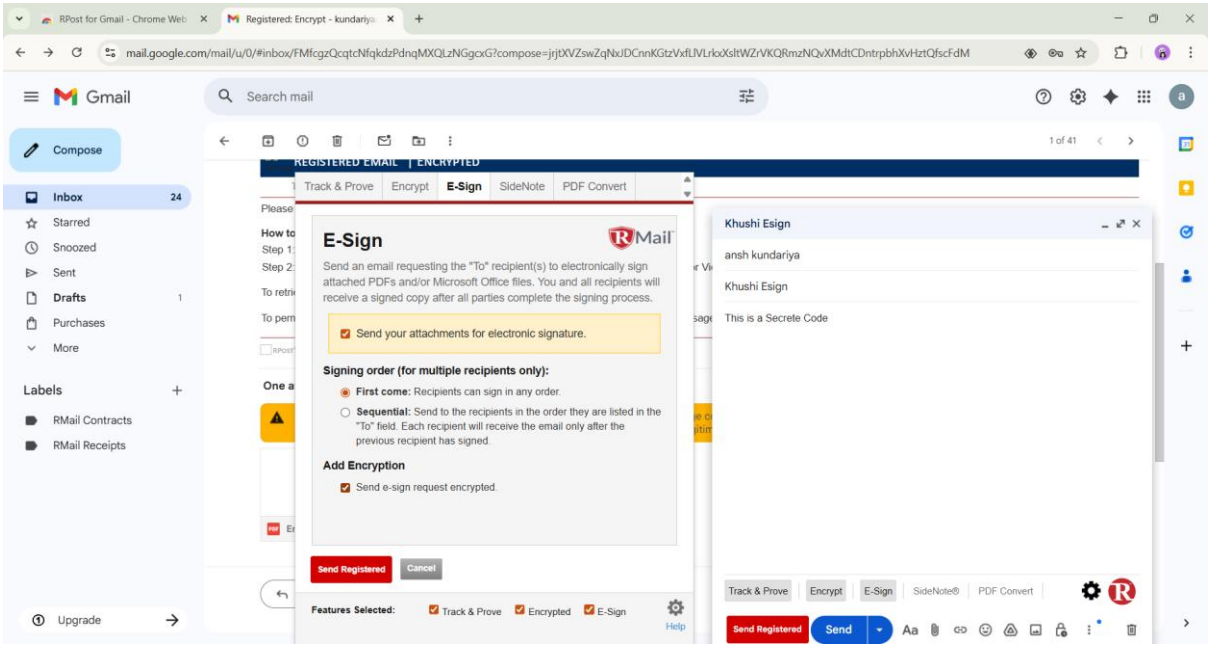
13) Open a Compose :



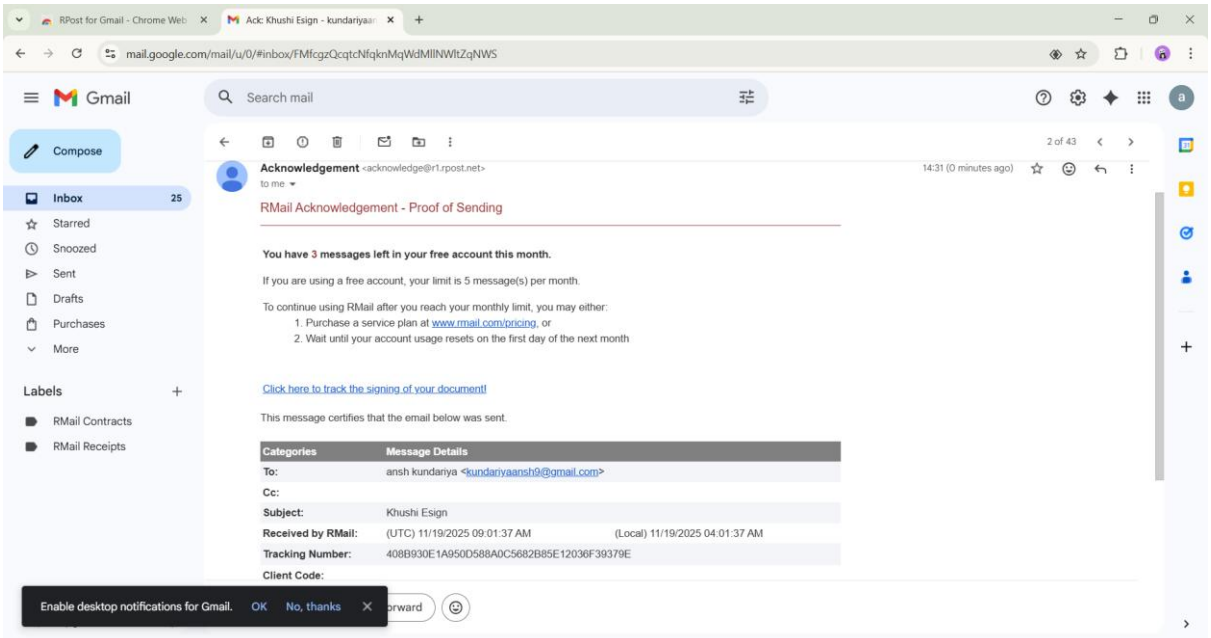
14)Write a E-sign Mail :



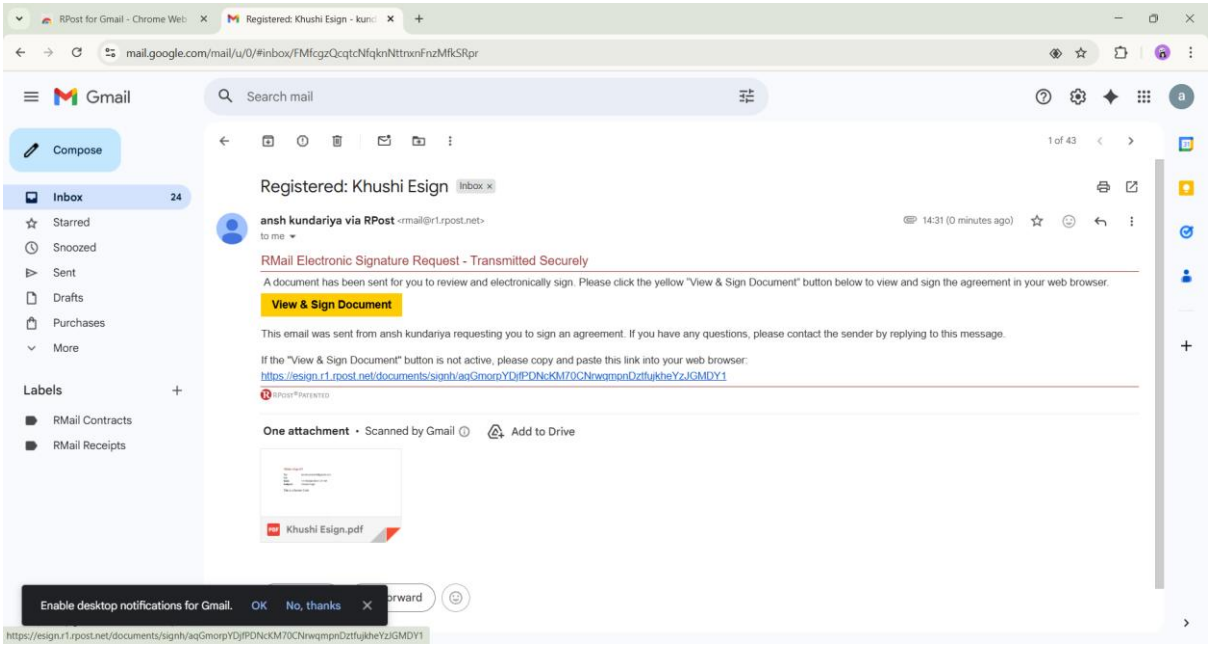
15)Click a Send Button :



16) Security Mail:



17)E-sign Mail :



18)E-sign mail Pdf :