KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Cryptographic attack using Hashcat

Aim:

To use "Hashcat" to perform cryptographic attack.

Procedure:

Step-1: First, make sure hashcat is installed. Else, install it with the command:

```
sudo pacman -S hashcat
```

Step-2: Next, check if required drivers are installed for hashcat using the command "hashcat -I"

Step-3: If you get the warning that there are no compatible drivers, install OpenCL drivers for the processor in your device and make sure to install the "pocl" drivers as well using the following command:

```
sudo pacman –S opencl-intel pocl
```

Step-4: Now, try hashcat-I again. It won't show any errors.

Step-5: We need rockyou.txt for our dictionary. We can get it from the url:

"https://tinyurl.com/rockyougit"

Extract it using the command "gunzip rockyou.txt.gz"

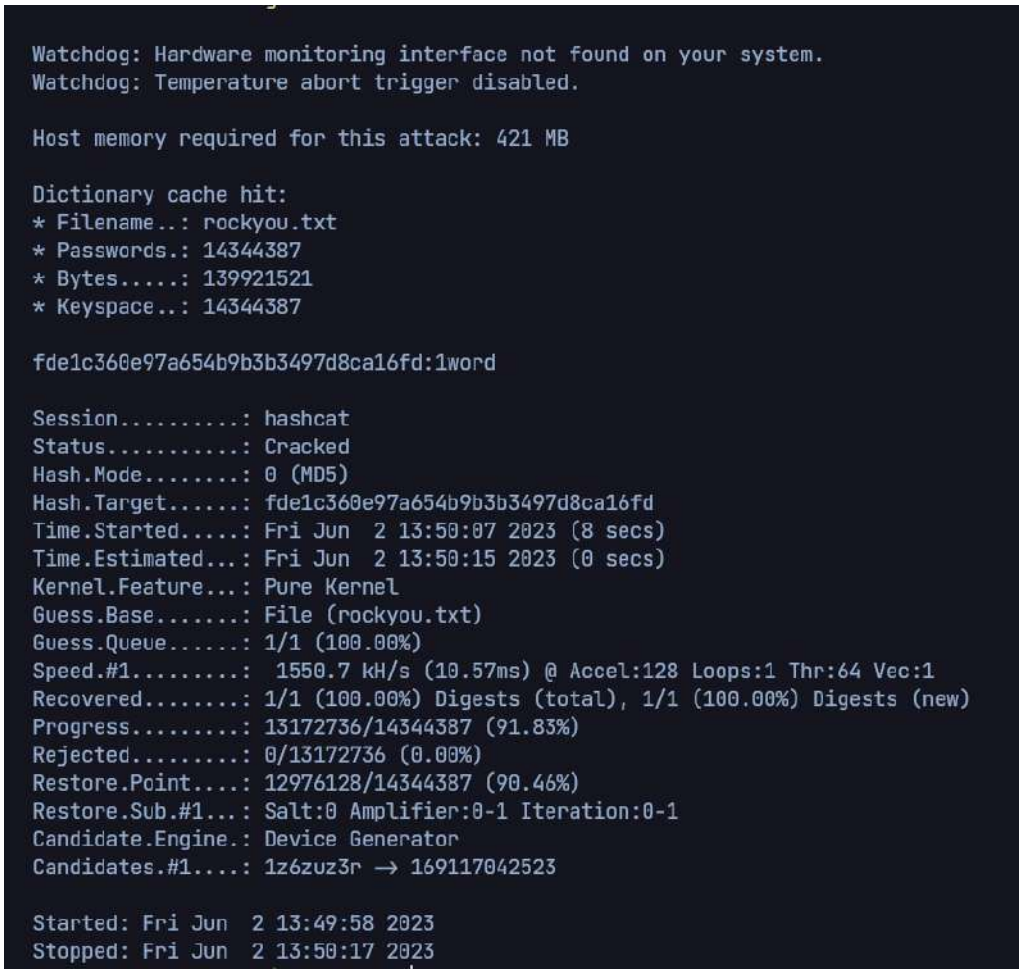
Step-6: For generating the hash, you can visit any online hash generator to generate MD5 hashes, or you can do it in command line using

"echo –n word | md5sum". The word "word" can be replaced by any word you wish. Copy this hash to a new file called hashes.txt.

Step-7: Now, run the following command to crack the hashes. This will be using only a single hash to crack the program.

```
hashcat -a 0 -m 0 fde1c360e97a654b9b3b3497d8ca16fd rockyou.txt
```

Output Screenshot:



Result:

Successfully cracked a hash using hashcat by performing cryptographic attack.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No	**:**	99220040586
Name	**:**	K.V. Hitesh Kumar Chowdary
Class	**:**	Cyber 2
Ex.No/Name	**:**	Working Lab Setup of Virtual Box, Kali Linux, and Metasploitable

Aim:

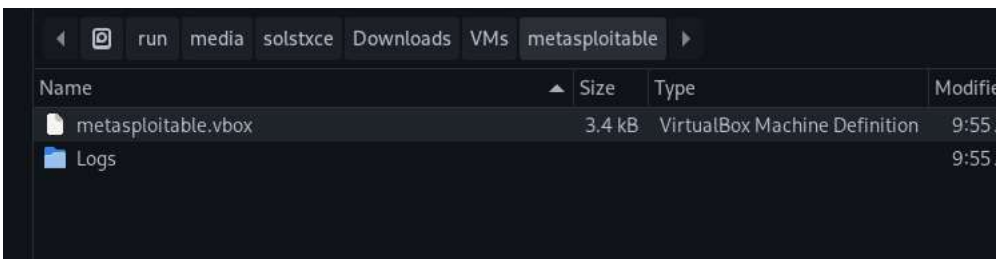
Installation and setup of Oracle Virtual Box, Kali Linux and Metasploitable Virtual Machine

Procedure:

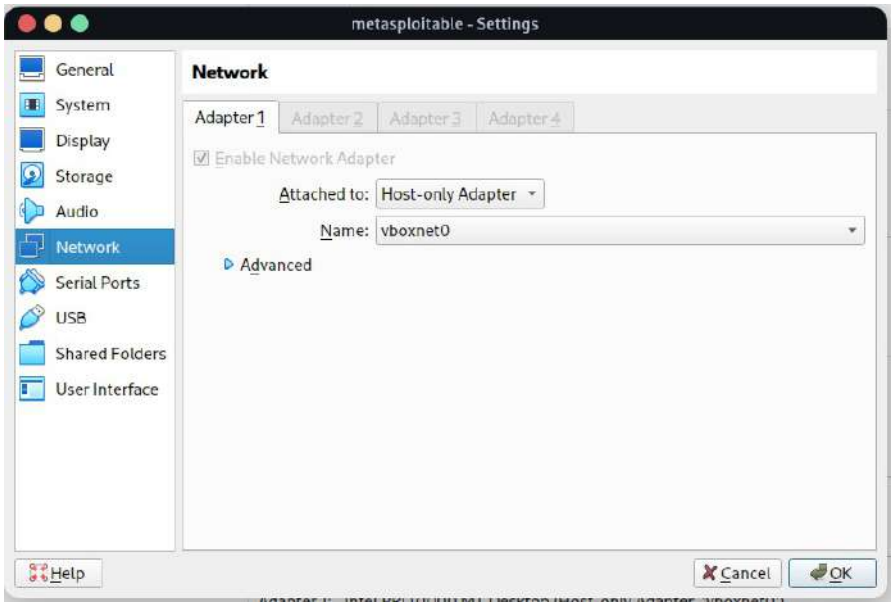
Step-1: First download virrtual box using the default package manager along with its required drivers and packages. For pacman, it is: "sudo pacman –S virtualbox virtualbox-host-dkms"

Step-2: Now open virtualbox and then create a virtual machine by clicking the add button at the top.

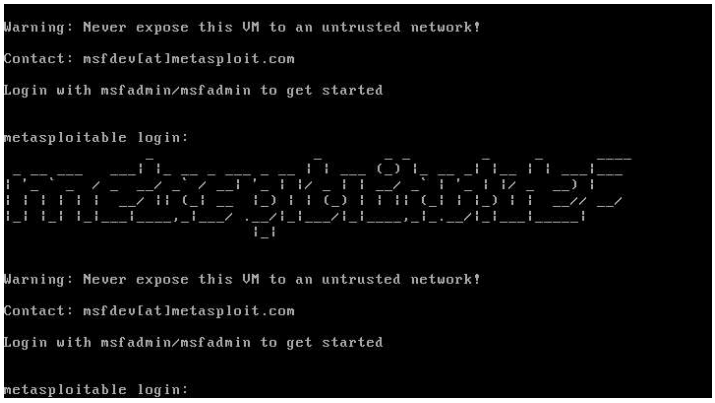
Step-3: Now go to metasploitable website and download the latest available file. Extract it. Now back in virtual box, select the metasploitable.vbox file.



Step-4: After that, click the settings icon and in the network tab, change the network adapter to host-only.



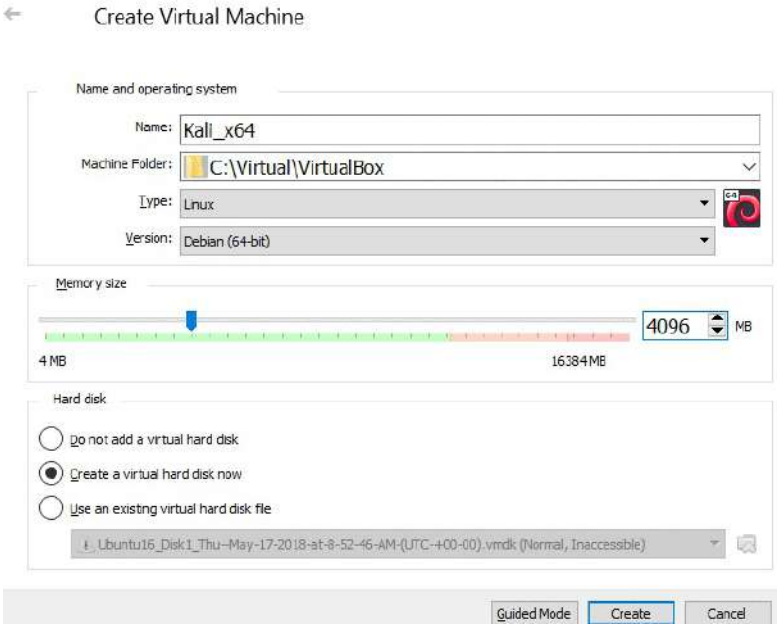
Step-5: After that, start the virtual machine. Now you have successfully started the metasploitable virtual machine.



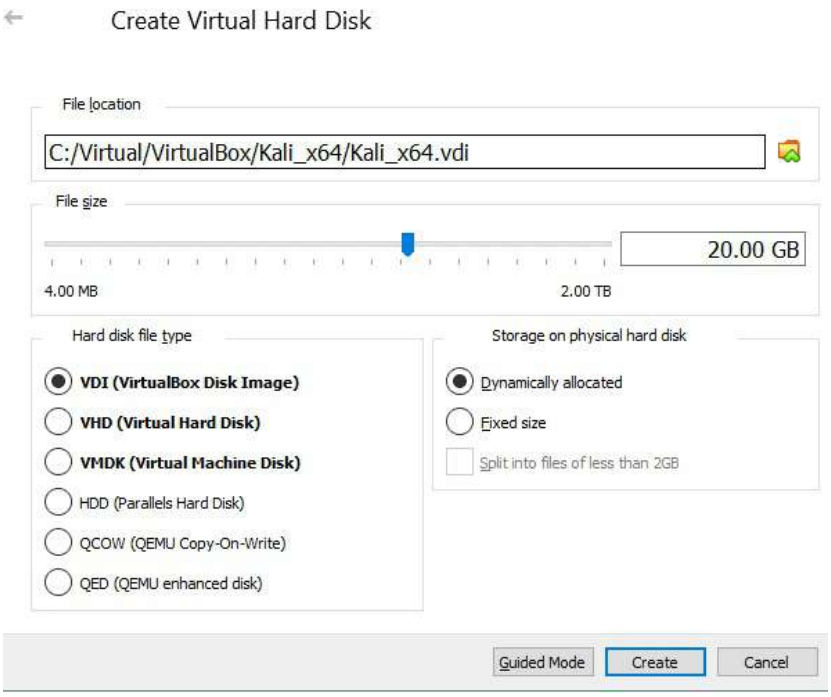
Step-6: Now we will install Kali Linux. Download the latest iso from the website.

Image Name	Download	Size	Version	SHA256Sum
Kali Linux 64-Bit	HTTP | Torrent	3.2G	2019.2	67574ee0039eaf4043a237e7c4b0eb432ca07ebf9c7b2dd0667a83bc3900b2cf
Kali Linux 32-Bit	HTTP | Torrent	3.2G	2019.2	1e03023bbd81fdec9c49717219c2c48f62da3f99009df1bbe73f158eef246282
Kali Linux LXDE 64-Bit	HTTP | Torrent	3.0G	2019.2	cd0d7fc95275de49b40108838f8fca2984d5cbec9472f54656dc351d09edc8dc
Kali Linux MATE 64-Bit	HTTP | Torrent	3.1G	2019.2	f81ca6a35bcd61678f1a84dc8949023b11c7434d80f35bc2ac8d6f08dfd93bad
Kali Linux Light armhf	HTTP | Torrent	741M	2019.2	0f3ad59fc2fed868cb3ddeab38c7968a190e54e655c50b9561f847e9d17e7963
Kali Linux KDE 64-Bit	HTTP | Torrent	3.5G	2019.2	b794d360923c1f2c73f607835d8506cbfe3c4746c20e009ac21aa37b47c32749f

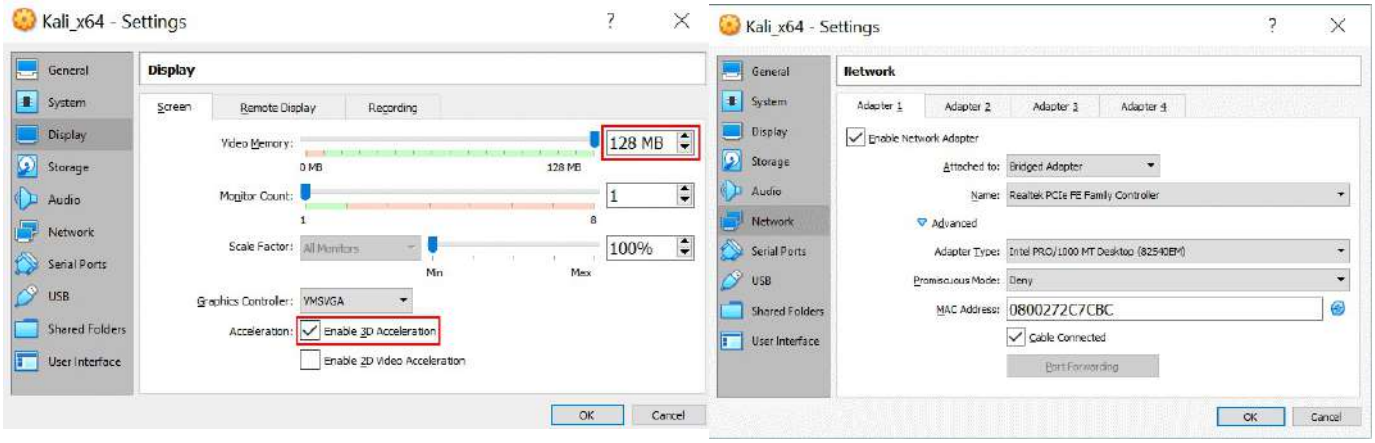
Step-7: Now click the new buton and then choose the type as debian x64 and give it atleast 4GB RAM to ensure smooth working.



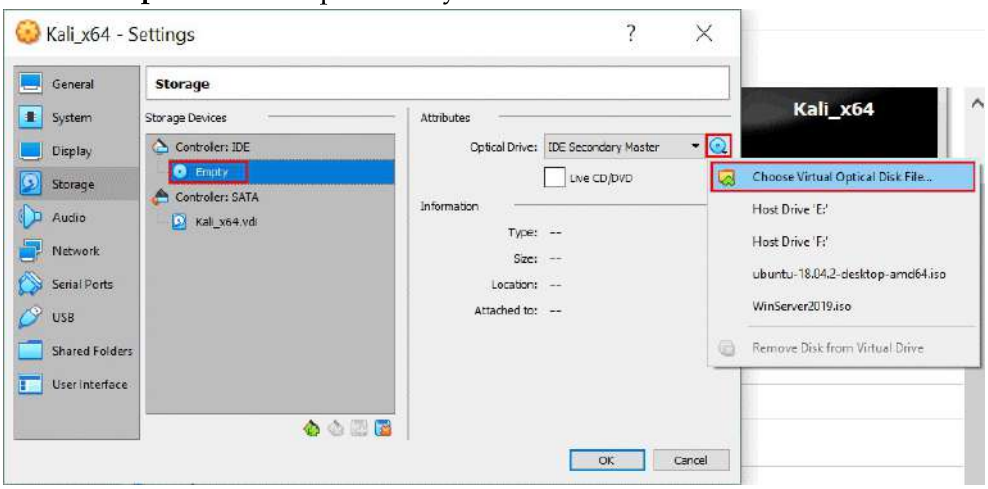
Step-8: Create a VDI and give it atleast 20GB



Step-8: Change the following settings in that.

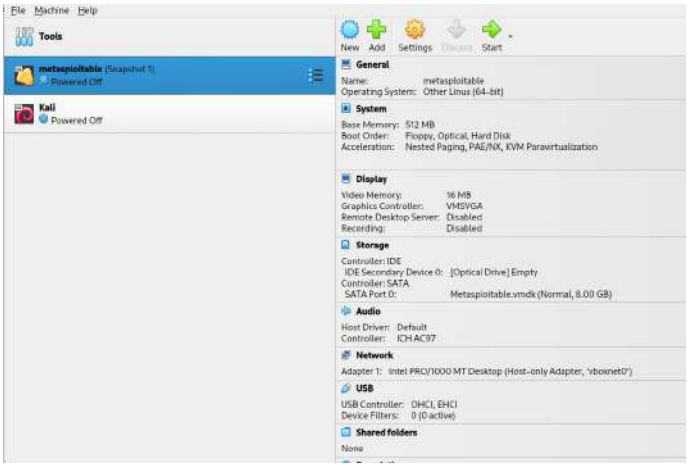


Step-9: Load the previously downloaded kali ISO here.



Step-10: Now, click ok and start the kali virtual machine. After that, go according to the installation steps and install the kali linux.

Output Screenshot:



Result:

Thus, Oracle Virtual Box, Kali Linux and Metasploitable virtual boxes were setup properly.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Vulnerability analysis using Legion

Aim:

To perform vulnerability analysis on a web server with "Legion"

Procedure:

Step-1: Install Legion package on your machine. This is a package that only installs in Linux. Here, we are installing with docker, so that we can reduce issues.

To install docker, use the command "sudo pacman –S docker"

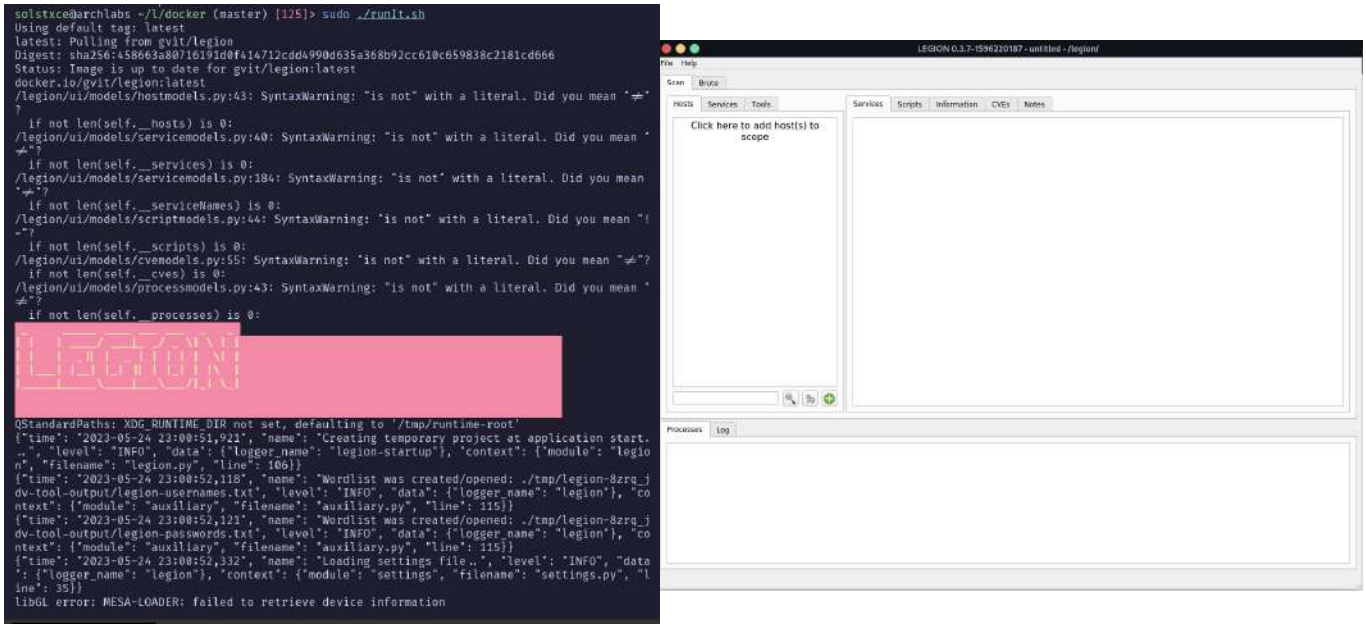
Step-2: Next to start the dockerd process, use the command "sudo systemctl start dockerd" or just type "sudo dockerd" in another terminal instance.

```
solstxce@archlabs ~/l/docker (master)> sudo dockerd
[sudo] password for solstxce:
INFO[2023-05-25T09:30:40.465945993+05:30] Starting up
INFO[2023-05-25T09:30:40.467135512+05:30] containerd not running, starting managed containerd
INFO[2023-05-25T09:30:40.469105417+05:30] started new containerd process                addre
ss=/var/run/docker/containerd/containerd.sock module=libcontainerd pid=92121
INFO[2023-05-25T09:30:40.572686948+05:30] starting containerd                           revis
ion=1677a17964311325ed1c31e2c0a3589ce6d5c30d.m version=v1.7.1
INFO[2023-05-25T09:30:40.594546901+05:30] loading plugin "io.containerd.snapshotter.v1.aufs".
..  type=io.containerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597096490+05:30] skip loading plugin "io.containerd.snapshotter.v1.a
ufs" ...  error="aufs is not supported (modprobe aufs failed: exit status 1 \"modprobe: FATAL:
 Module aufs not found in directory /lib/modules/6.3.2-arch1-1\\n\"): skip plugin" type=io.co
ntainerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597129799+05:30] loading plugin "io.containerd.snapshotter.v1.btrfs"
...  type=io.containerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597326583+05:30] skip loading plugin "io.containerd.snapshotter.v1.b
trfs" ...  error="path /var/lib/docker/containerd/daemon/io.containerd.snapshotter.v1.btrfs (e
xt4) must be a btrfs filesystem to be used with the btrfs snapshotter: skip plugin" type=io.c
ontainerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597343840+05:30] loading plugin "io.containerd.content.v1.content"..
.  type=io.containerd.content.v1
INFO[2023-05-25T09:30:40.597362524+05:30] loading plugin "io.containerd.snapshotter.v1.native
" ...  type=io.containerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597393575+05:30] loading plugin "io.containerd.snapshotter.v1.overla
yfs" ...  type=io.containerd.snapshotter.v1
INFO[2023-05-25T09:30:40.597686396+05:30] loading plugin "io.containerd.snapshotter.v1.devmap
per" ...  type=io.containerd.snapshotter.v1
WARN[2023-05-25T09:30:40.597705267+05:30] failed to load plugin io.containerd.snapshotter.v1.
```

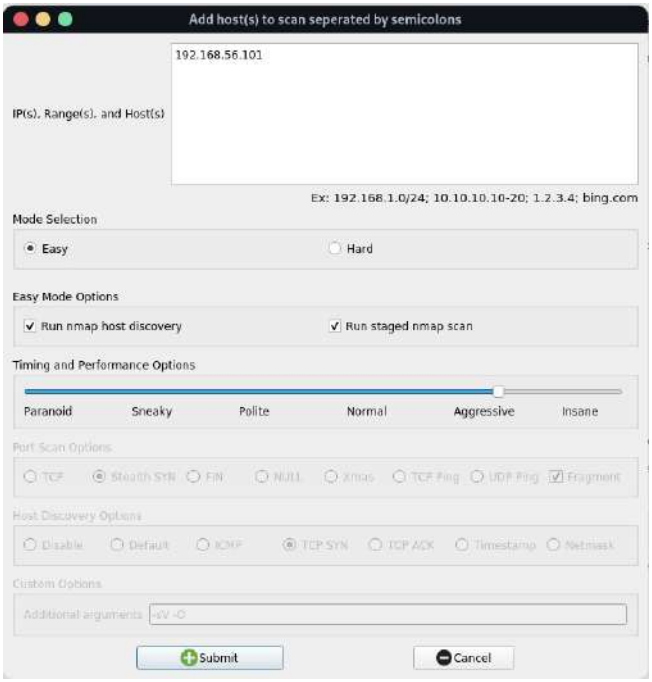
Step-3: Give appropriate permissions using the following commands:

```
sudo usermod -aG docker $USER

sudo chmod 666 /var/run/docker.sock

sudo xhost +local:docker
```

Step-4: Open “Legion” app with the script in the docker folder.

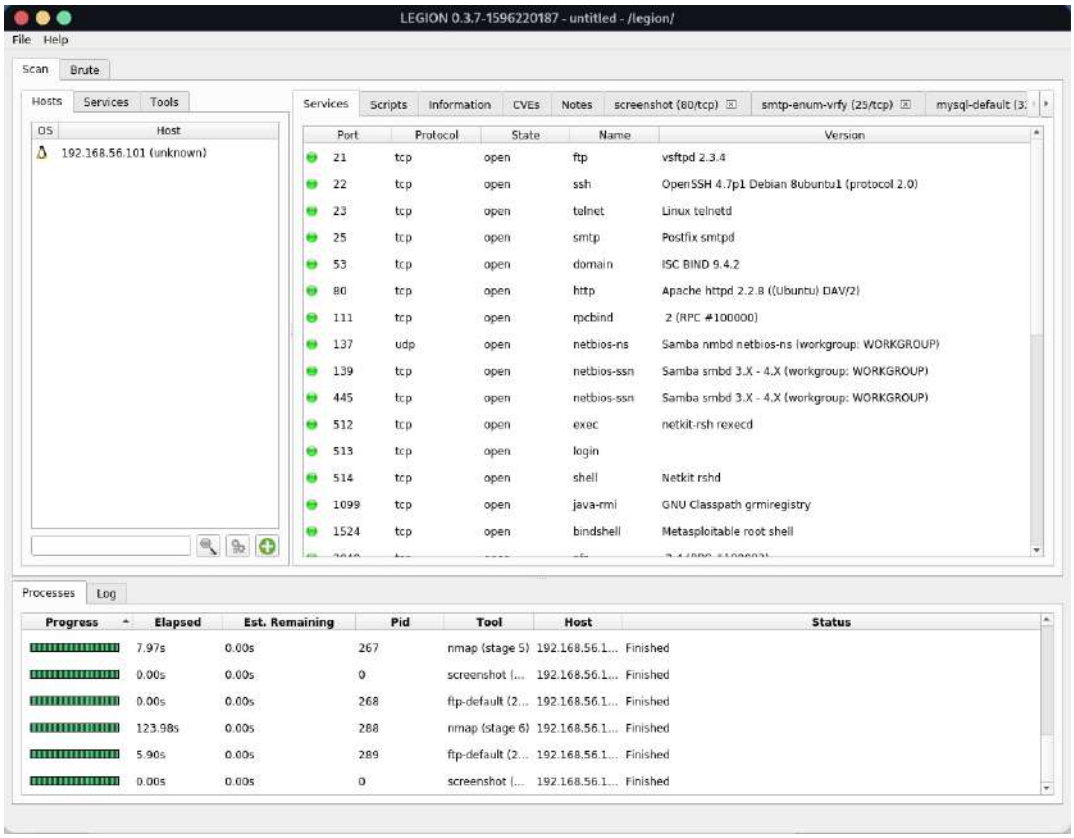


Step-5: Click on the “Hosts” panel at left side. Then in the hosts section, type in the address of the website or the IP address which you want to perform a scan on. Here, we are using “metasploitable” virtual machine as the testing machine.



Step-6: Click the submit button and wait for the scan to finish. Later you will get a list of all the services and vulnerabilities which are present in the web server.

Output Screenshot:



Result:

Thus, all the information about target machine like services and vulnerabilities were found using the "Legion" tool.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Exploring network vulnerabilities using nikto tool

---

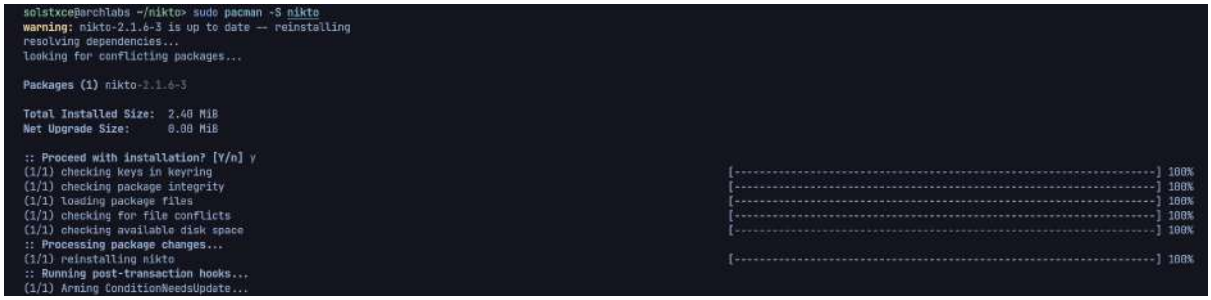
Aim:

To find out the vulnerabilities in the web server using the nikto tool

Procedure:

Step-1: First, install the nikto tool using the default package manager

```
sudo pacman -S nikto
```



Step-2: Now, launch the metasploitable virtual machine and login

Step-3: Now get the IP address of the virtual machine.

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a0:88:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fea0:88b8/64 scope link
       valid_lft forever preferred_lft forever
```

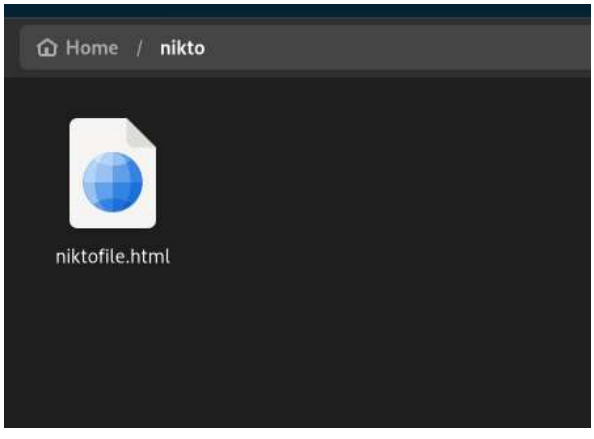
Step-4: Now use the nikto tool along with this IP address to find vulnerabilities in the machine.

```
sudo nikto -h http://192.168.56.101 -Format html -output ~/niktofile
```

Step-5: Now,wait for the scan to finish.

```
solstxce@archLabs ~/nikto [2]> sudo nikto -h http://192.168.56.101 -Format html -output ~/niktofile
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2023-05-26 15:39:40 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following a
ves for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
```

Step-6: After that, you will get the output in the file called niktofile which will be created in the home directory.Open it with any browser to see the output.



Output Screenshot:

192.168.56.101 / 192.168.56.101 port 80	
Target IP	192.168.56.101
Target hostname	192.168.56.101
Target Port	80
HTTP Server	Apache/2.2.8 (Ubuntu) DAV/2
Site Link (Name)	http://192.168.56.101:80/
Site Link (IP)	http://192.168.56.101:80/

URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
Test Links	http://192.168.56.101:80/ http://192.168.56.101:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://192.168.56.101:80/ http://192.168.56.101:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://192.168.56.101:80/ http://192.168.56.101:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://192.168.56.101:80/ http://192.168.56.101:80/
OSVDB Entries	OSVDB-0
URI	/index
HTTP Method	GET
Description	Uncommon header 'tcn' found, with contents: list
Test Links	http://192.168.56.101:80/index http://192.168.56.101:80/index
OSVDB Entries	OSVDB-0
URI	/index
HTTP Method	GET

Result:

Thus, using niktotool all the vulnerabilities in the remote web server were found and it was output to a HTML file.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Vulnerability analysis using nmap

Aim:

To find the vulnerabilities in the web server using nmap.

Procedure:

Step-1: Install nmap using the default package manager

```
sudo pacman –S nmap
```

```
solstxce@archlabs ~ [SIGINT]> sudo pacman -S nmap
[sudo] password for solstxce:
warning: nmap-7.93-1 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Packages (1) nmap-7.93-1

Total Download Size:    5.53 MiB
Total Installed Size:  24.24 MiB
Net Upgrade Size:       0.00 MiB

:: Proceed with installation? [Y/n] y
:: Retrieving packages...
```

Step-2: Now, start the metasploitable virtual machine and login and get its IP address.

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a0:88:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fea0:88b8/64 scope link
       valid_lft forever preferred_lft forever
```

Step-3: Use the command nmap –sn to get the information about the target machine's MAC address.

```
solstxce@archlabs ~ [1]> sudo nmap -sn 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 16:40 IST
Nmap scan report for 192.168.56.101
Host is up (0.00031s latency).
MAC Address: 08:00:27:A0:88:B8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Step-4: Now, use the command "nmap –sV –p 20-500 –T4 vv "

```
solstxce@archlabs ~ [1]> nmap -sV -p 20-500 -T4 -vv 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 17:22 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 17:22
Scanning 192.168.56.101 [2 ports]
Completed Ping Scan at 17:22, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:22
Completed Parallel DNS resolution of 1 host. at 17:22, 0.08s elapsed
Initiating Connect Scan at 17:22
Scanning 192.168.56.101 [481 ports]
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Completed Connect Scan at 17:22, 0.05s elapsed (481 total ports)
Initiating Service scan at 17:22
Scanning 9 services on 192.168.56.101
Completed Service scan at 17:22, 11.01s elapsed (9 services on 1 host)
NSE: Script scanning 192.168.56.101.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 17:22
Completed NSE at 17:22, 0.16s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:22
Completed NSE at 17:22, 0.03s elapsed
Nmap scan report for 192.168.56.101
Host is up, received syn-ack (0.00045s latency).
Scanned at 2023-05-26 17:22:48 IST for 11s
Not shown: 472 closed tcp ports (conn-refused)
PORT    STATE SERVICE     REASON  VERSION
21/tcp  open  ftp         syn-ack vsftpd 2.3.4
22/tcp  open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      syn-ack Linux telnetd
25/tcp  open  smtp        syn-ack Postfix smtpd
53/tcp  open  domain      syn-ack ISC BIND 9.4.2
80/tcp  open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Step-5: Now, use the following command to find the ftp-anon exploit.

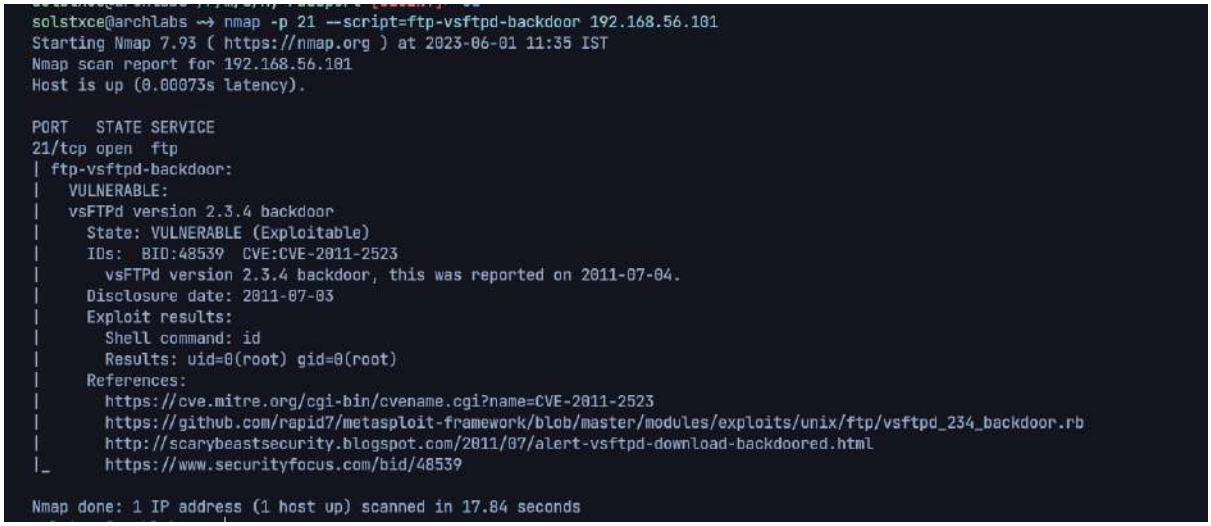
```
nmap -p 21 --script=ftp-anon
```

```
solstxce@archlabs ~> nmap -p 21 --script=ftp-anon 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 17:24 IST
Nmap scan report for 192.168.56.101
Host is up (0.00044s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Step-6: Now, check for the vsftpd-backdoor

```
nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.56.101
```

Output Screenshot:



Result:

By using nmap, we were able to successfully check for multiple vulnerabilities in the remote web server, in this case a metasploitable virtual machine.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Hash data by using Quickhash-GUI tool

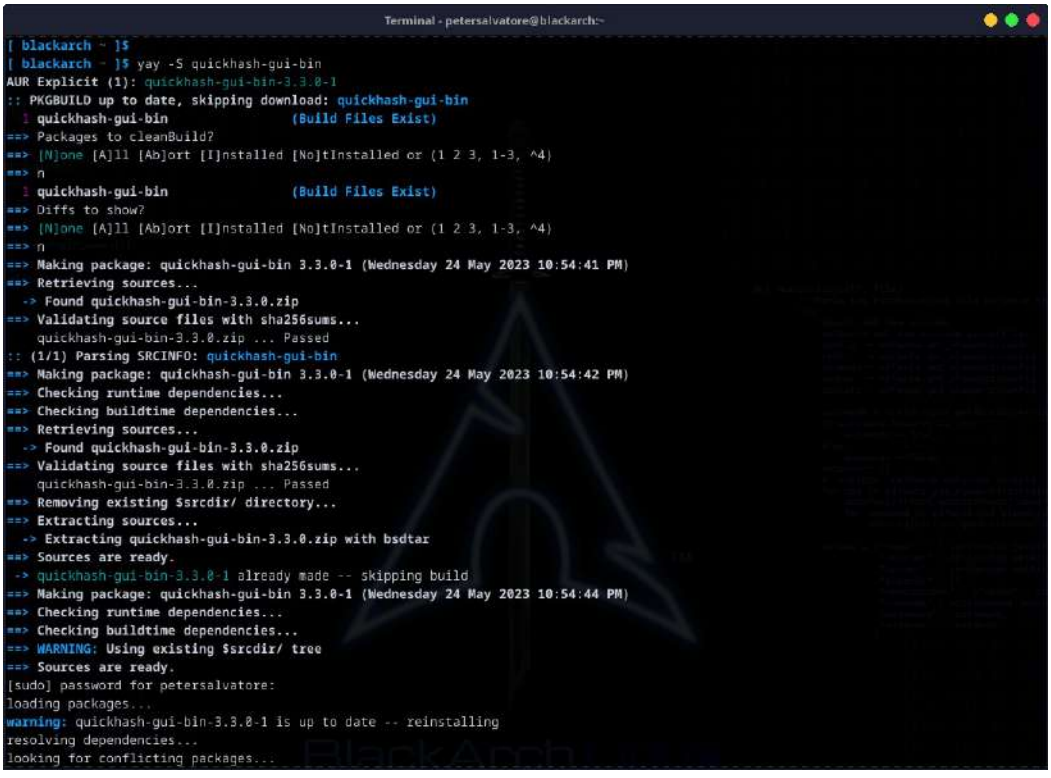
Aim:

To hash data by using Quick-hash-GUI tool.

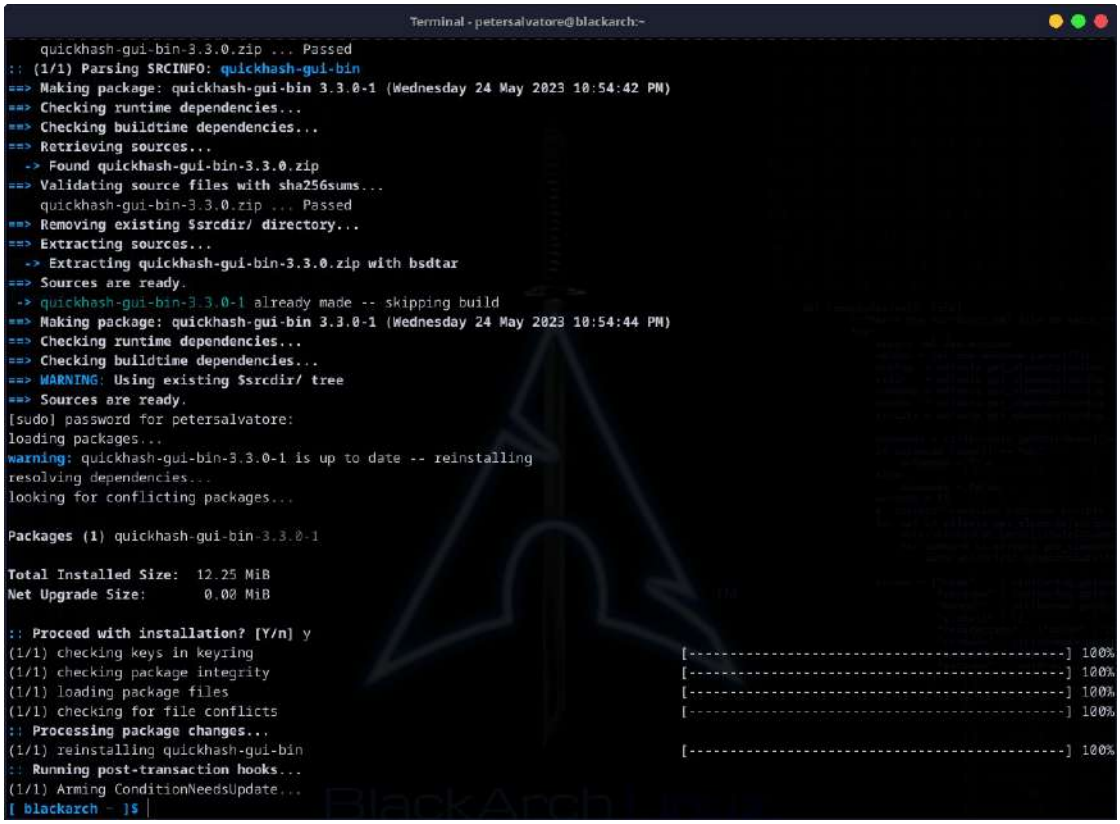
Procedure:

Step 1: To install Quick Hash-GUI for linux using the command

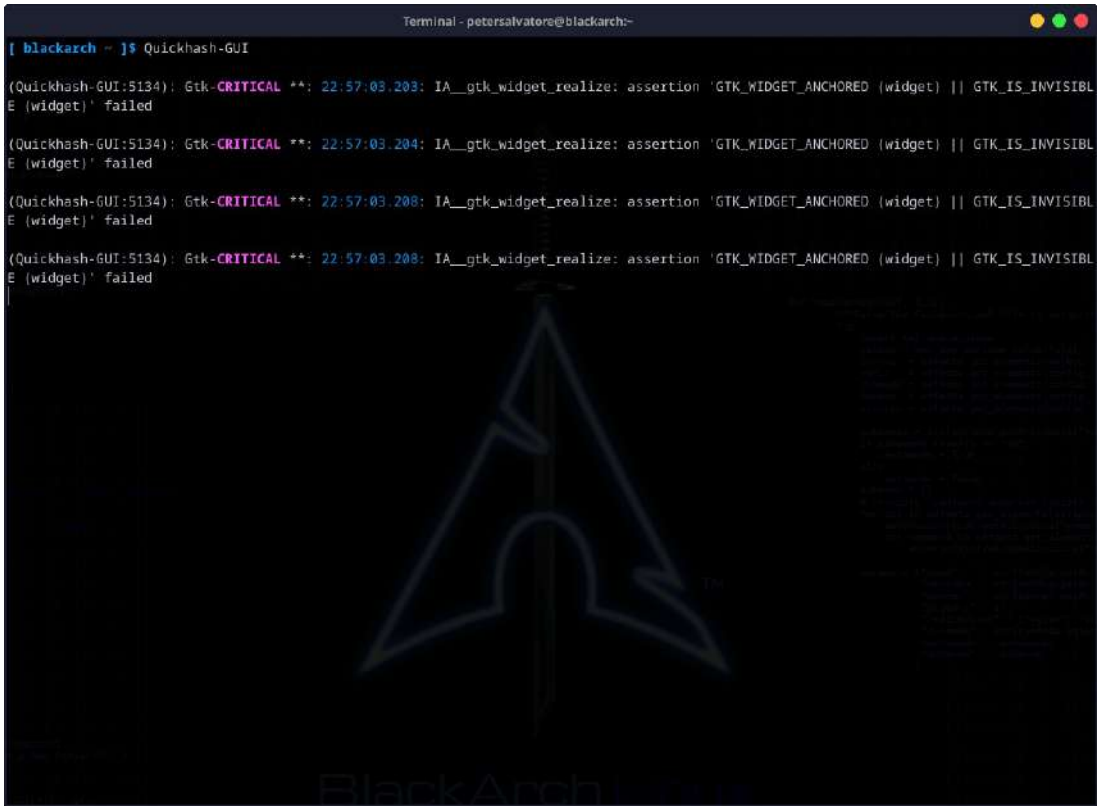
```
yay –S quickhash-gui-bin
```



Step 2: To complete the installation process type yes command



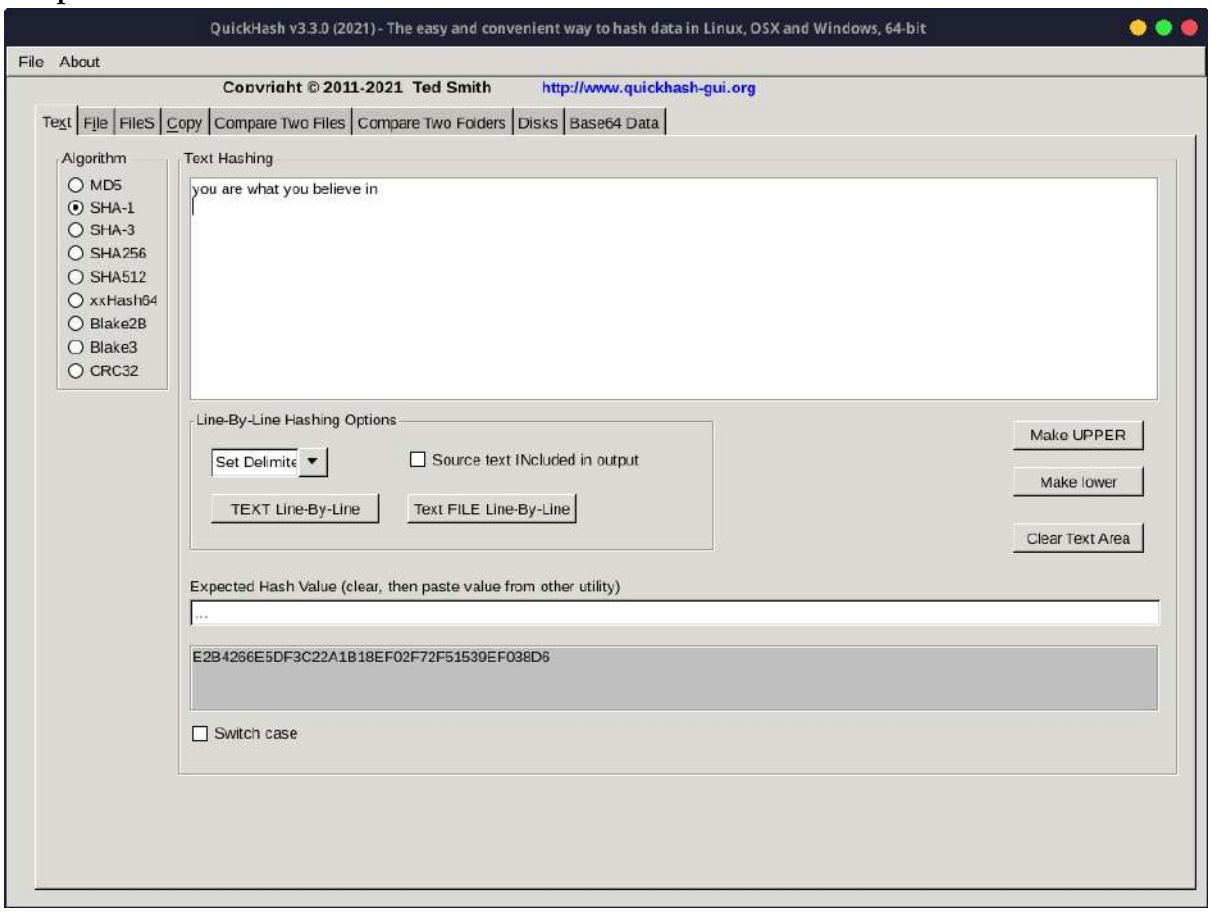
Step 3: Open the Quick hash GUI for hashing the data



Step 4: Select any algorithm and type or paste text in the hashing panel and get a hash value at the bottom.

Step 5: Here we select: SHA-1 algorithm. After that, try it with SHA-256 algorithm and SHA-512 algorithm.

Output:



Result:

Learned hashing text data with two different algorithms using the Quick Hash-GUI tool Successfully.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Hide and Unhide sensitive Information using Steghide.

Aim:

To Hide and Unhide sensitive data using Steghide.

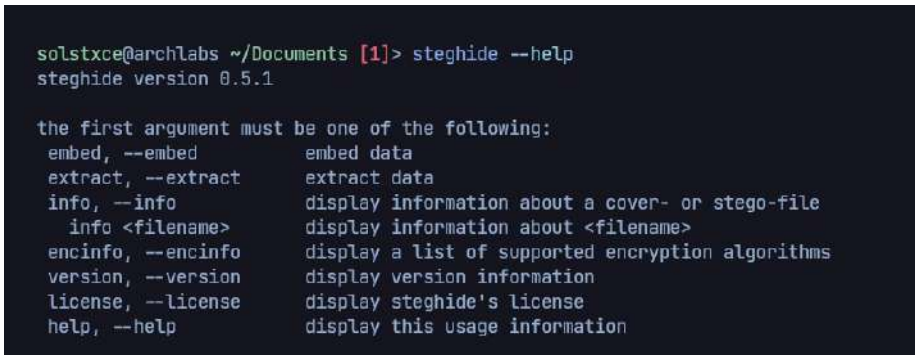
Procedure:

Step-1: Open Terminal and make sure steghide is installed.

Step-2: Change the working directory to in which the images are there. In this case, they are in Documents. So change using "cd Documents" command.

Step-3: Create a text file with content in it and download an image file. Here, the example text file is "secret.txt"and image is "image.jpg"

Step-4: Type steghide or steghide -h to show all the option of steghide.



Step-5: Now type the command**: steghide embed -cf image.jpg -ef secret.txt** to embed the text File into the image file with a password.

Step-6: Now, Enter a Passphrase/password. Then re-enter the same passphrase to confirm and hit enter. Now you'll get an output on terminal.

```
solstxce@archlabs ~/Documents> steghide embed -cf image.jpg -ef secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "image.jpg"... done
solstxce@archlabs ~/Documents>
```

Step-7: To extract the data, you can use the command **"steghide extract -sf image.jpg".** The content can be verified by seeing the content of "secret.txt"

```
solstxce@archlabs ~/Documents> steghide extract -sf image.jpg
Enter passphrase:
the file "secret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.txt".
solstxce@archlabs ~/Documents>
```

Output:

Content of "secret.txt" file after successfully unhiding:

```
solstxce@archlabs ~/Documents> cat secret.txt
hello world!
solstxce@archlabs ~/Documents>
```

Result:

Thus, the steghide is used to Hide and Unhide sensitive data successfully.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Encryption and Decryption process using VeraCrypt

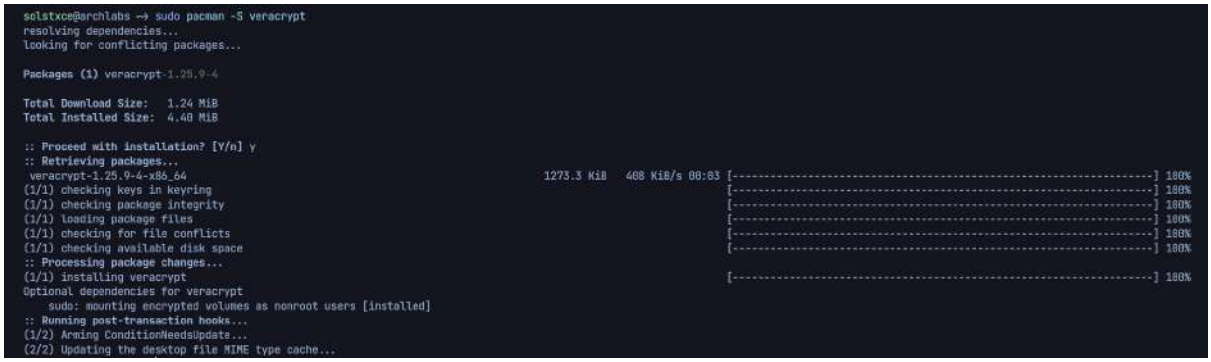
---

Aim:

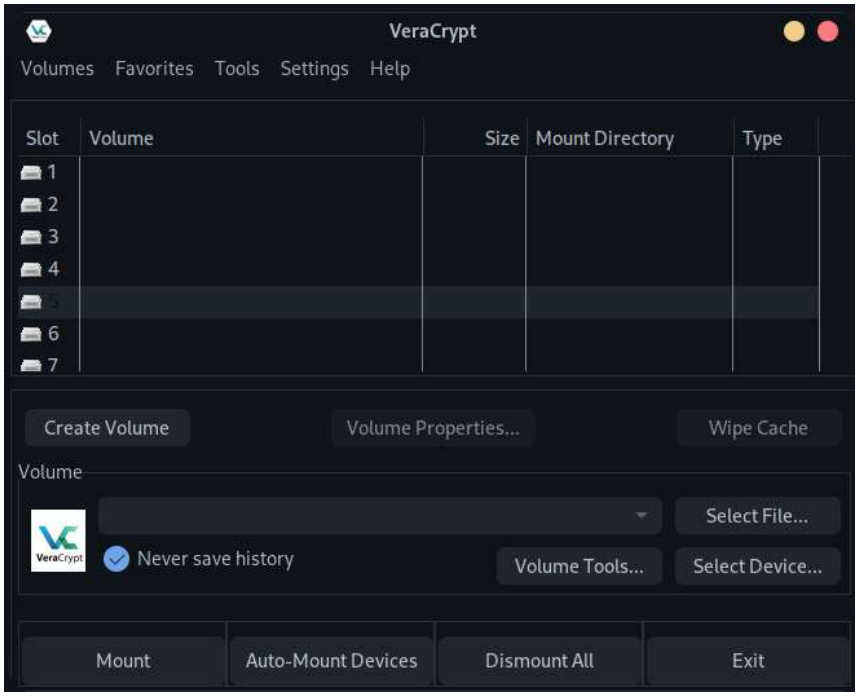
To analyze the Encryption/Decryption process using Vera Crypt tool

Procedure:

Step-1: Install Veracrypt using the default package manager (here it is pacman)



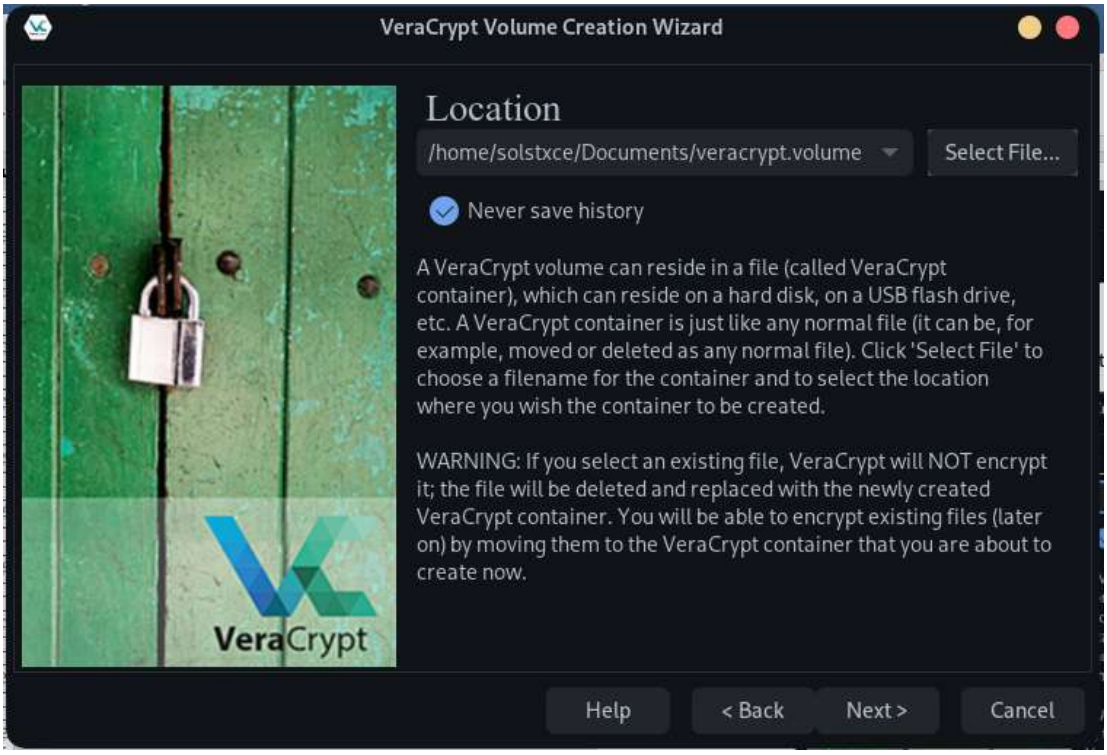
Step-2: After installation of VeraCrypt, now we start encryption of the drive. Choose any drive to create volume. Here we chose volume 5 as example.



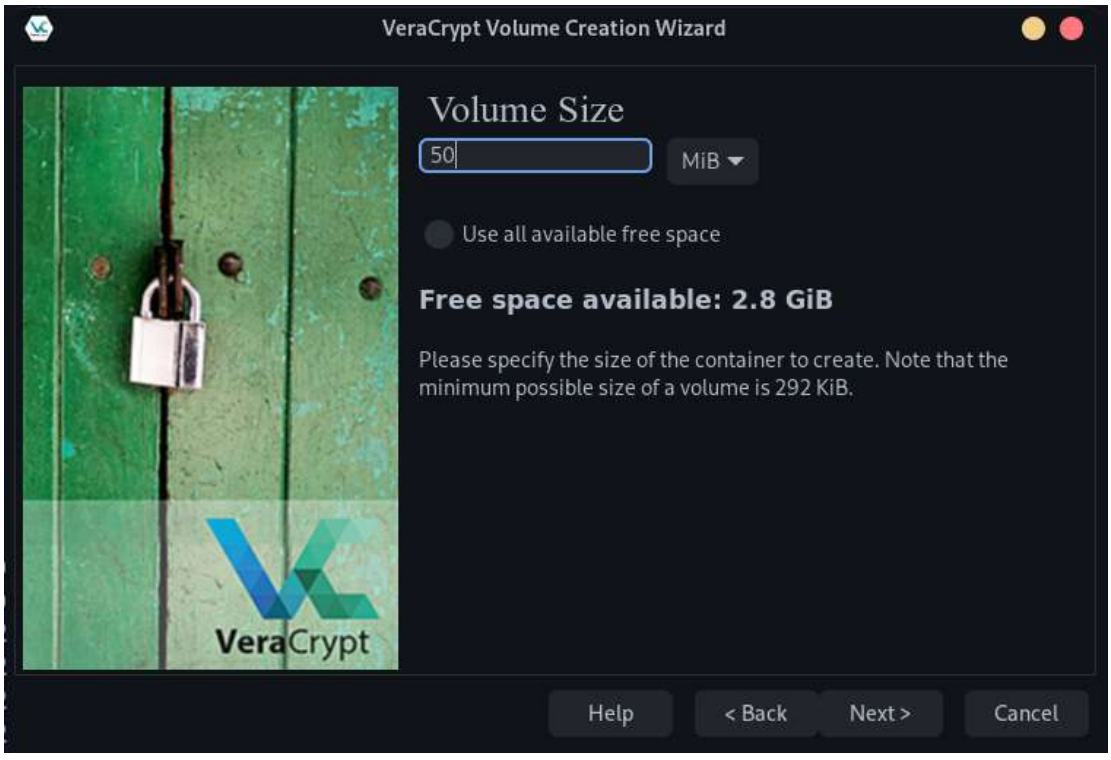
Step-3: Now we create the volume using the create volume feature. Click on Create Volume Button.

Step-4: Click "Next" button 2 times until it asks for location. Now click "Select File".

Step-5: Create a new file and choose it.

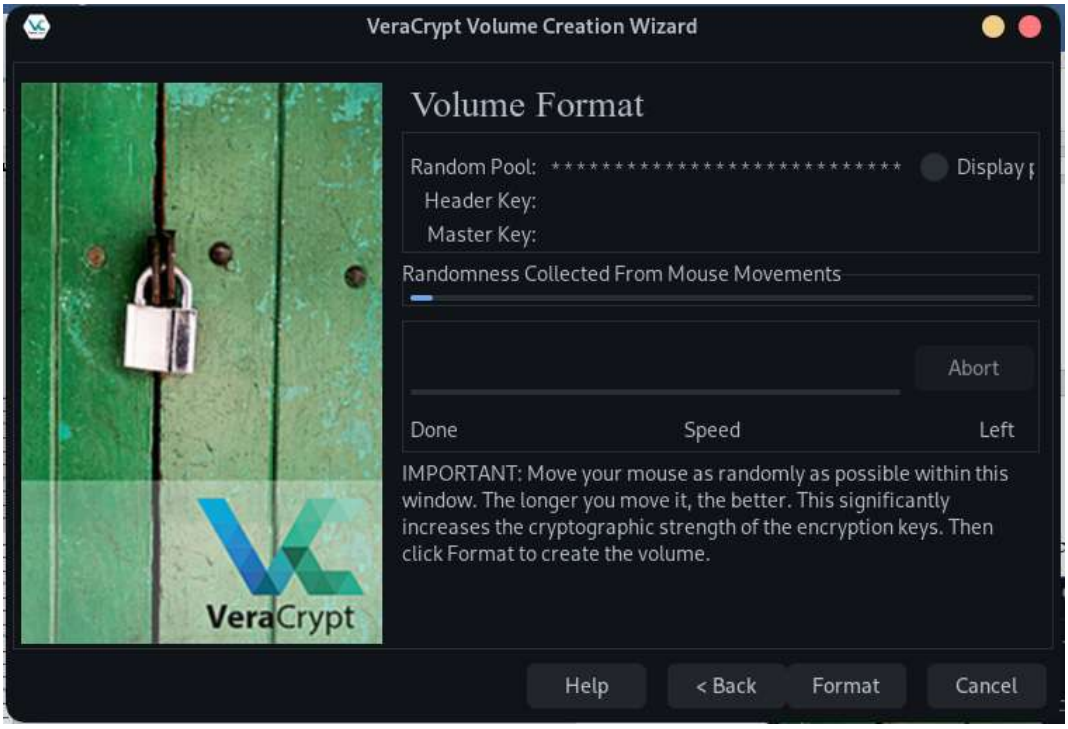


Step-6: Click "Next" until it asks for volume size. Here you can enter any size for volume.

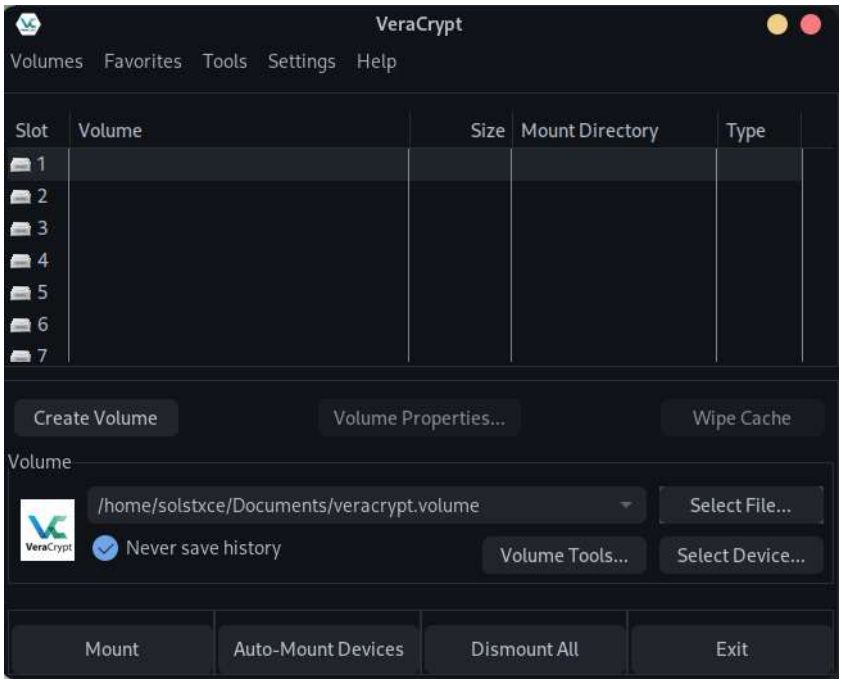


Step-7: Click “Next”. Choose a strong password with atleast 20 characters.

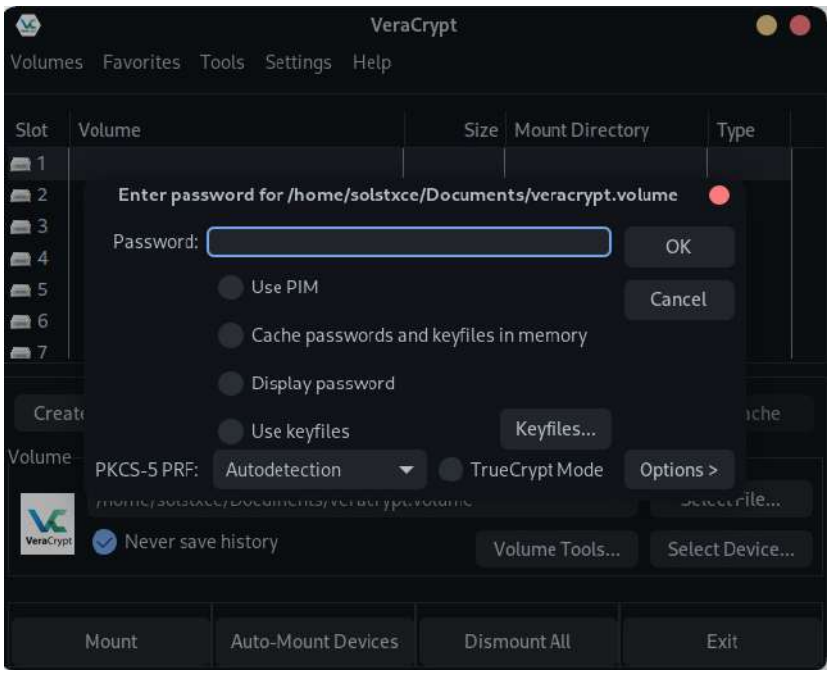
Step-8: Click “Next” until it asks for randomness. Now move the mouse over the app window for a few seconds. The more you move, the better the security. Then, click “Format” Button. Next click exit button after the volume is created.



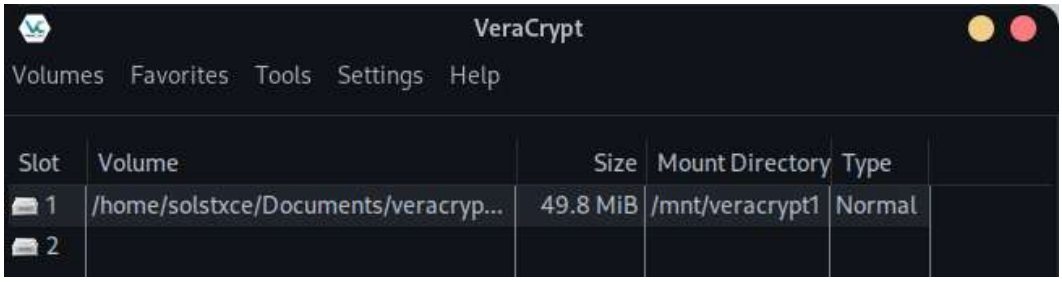
Step-9: After the volume was created and encrypted, you can now load it using the "Select File" button. Select the file from the opened window and click okay.



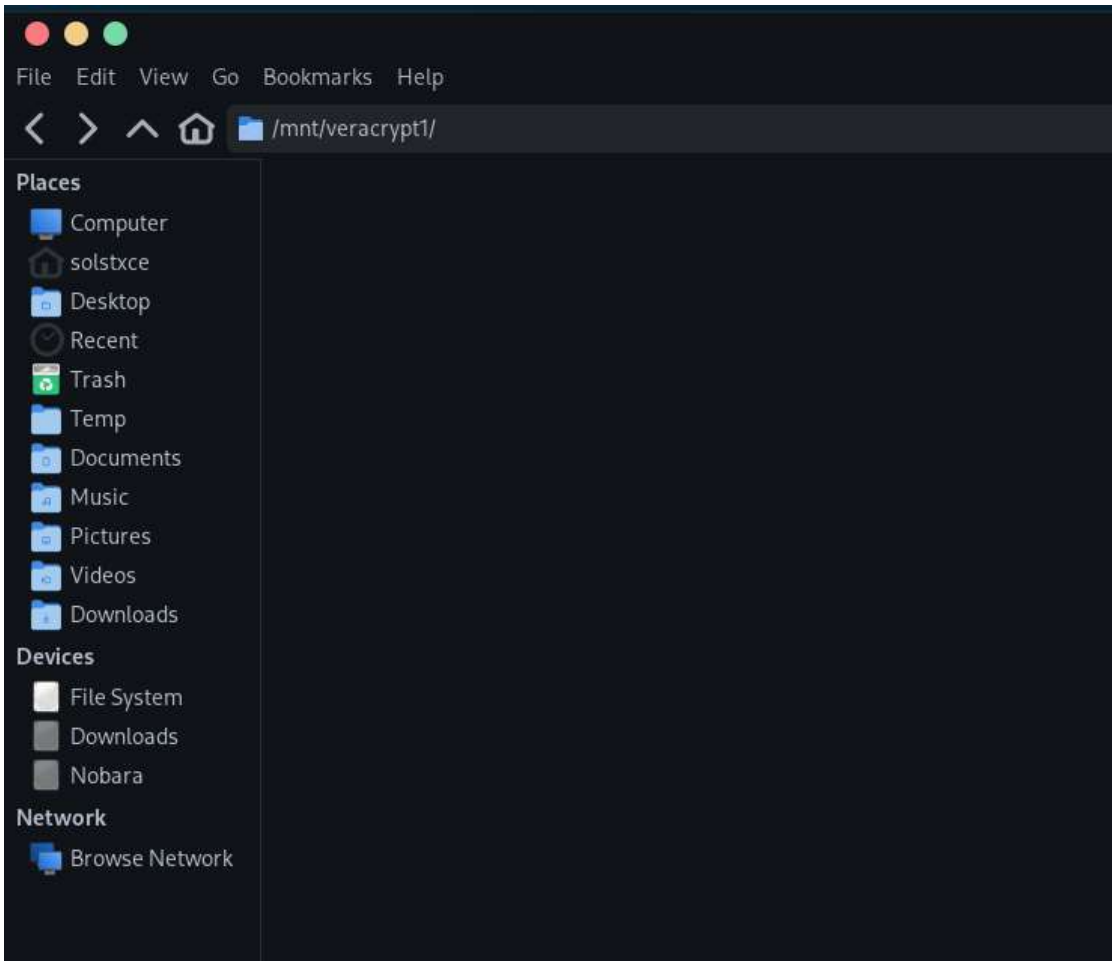
Step-10: Click the "Mount" button and enter the password you used earlier. Now the disk will be mounted.



Step-11: After it is mounted, you can access its location by going to the folder in "Mount Directory" column.



Output: The encrypted directory is successfully decrypted and mounted.



Result: A volume is created, encrypted and decrypted using VeraCrypt successfully.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : To check the vulnerabilities in network using Wireshark.

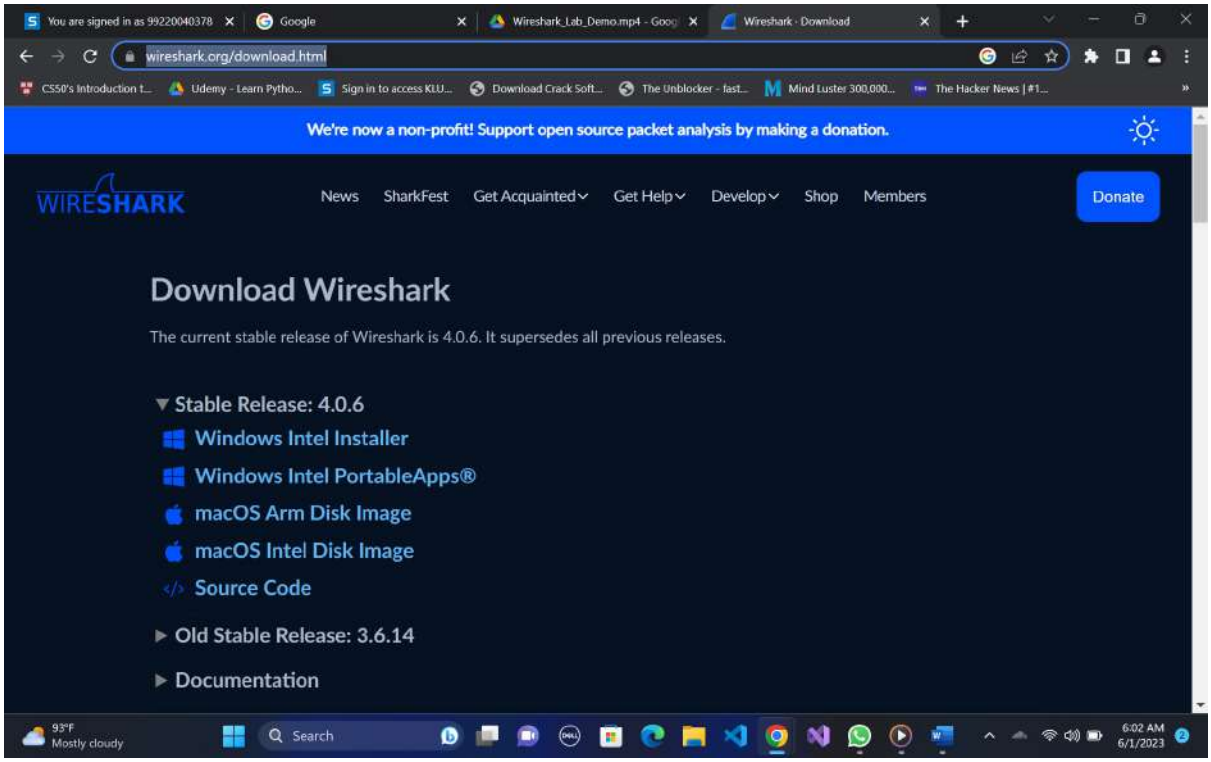
Aim:

To check the vulnerabilities in networks using Wireshark

Procedure:

Step-1: First download/install the Wireshark from

https://www.wireshark.org/download.html



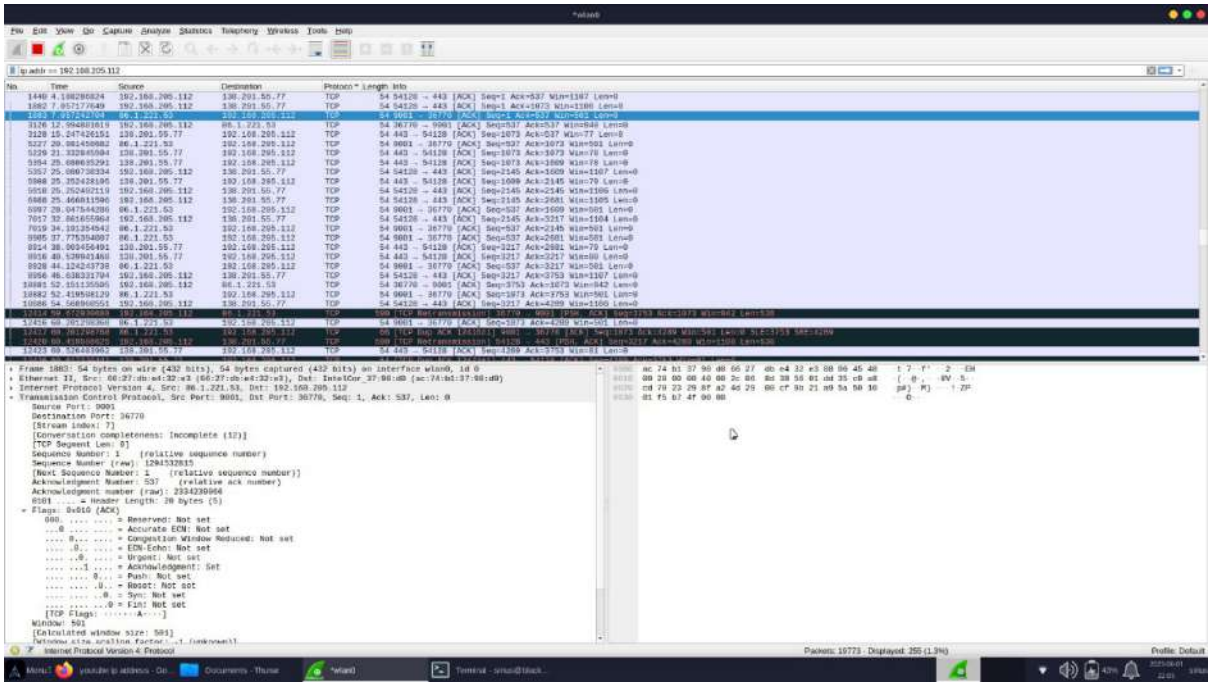
Step-2: Now open the Wireshark and check whether any networks available or not.

Step-3: Start capturing the networks with ip addresses and then after capturing continue capturing without saving.

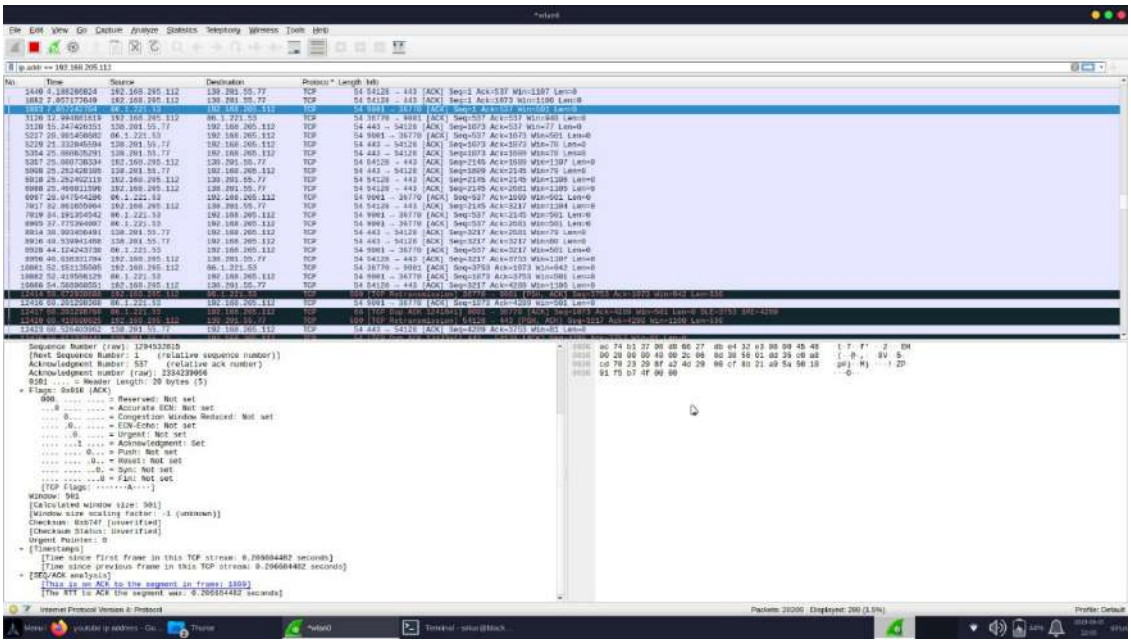
Step-4: Open the 3 way hand shake website in the goggle chrome to understand the TCP and enter the pakcets.

Step-5: Search the destination and protocol with “ip.addr==192.168.225.112”.

You will get the specified details of the network.



Output Screenshot:



Result:

Network vulnerabilities using Wireshark was successfully detected.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : Network Vulnerability using Wireshark

Aim:

To test network vulnerability using Wireshark

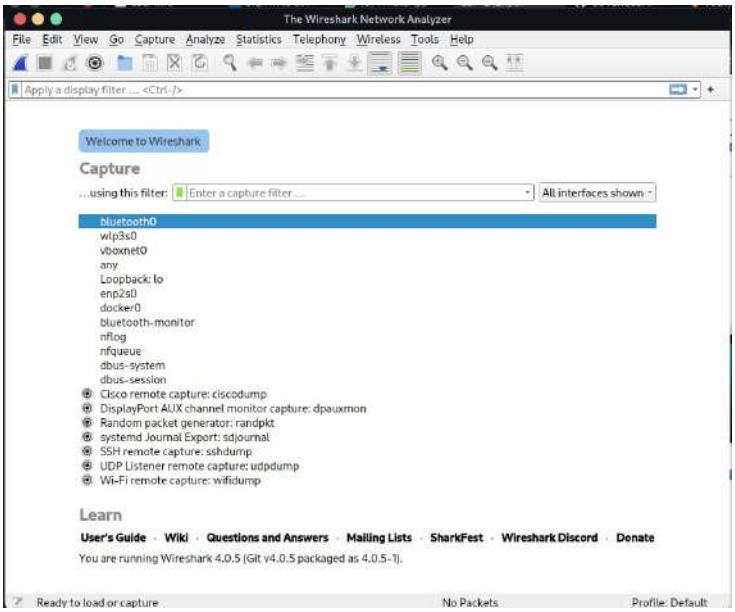
Procedure:

Step-1: Install wireshark using the command: "sudo pacman –S wireshark-qt"

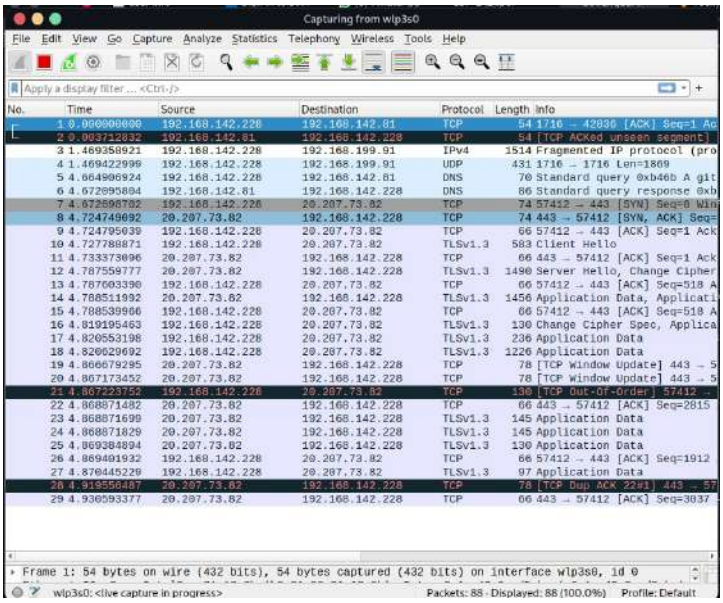
Step-2: Now, open add the user to the wireshark group with command

```
sudo usermod -aG wireshark $USER
```

Step-3: Now open wireshark.



Step-4: Choose the device wlp3s0 as it is the Wi-Fi source for this machine. In other devices it might be labeled as Wi-fi or wlan0. Now wireshark will start capturing packets.

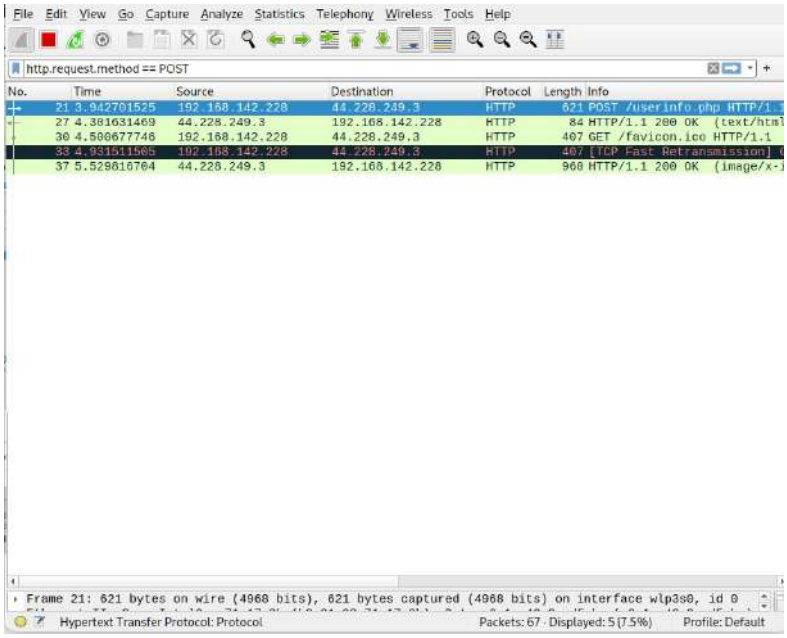


Step-5: Now visit any vulnerable website. For this test case, we will be using the website "testphp.vulnweb.com/login.php" and login with the default credentials.

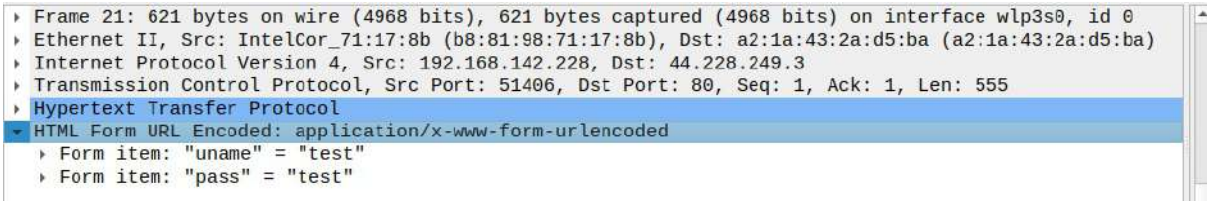
Step-6: Now go back to wireshark and click the red stop button to stop capturing the packets. After that, click the filter bar to filter out the requests.

Step-7: In that, type 'http.request.method === "POST" ' to filter out the POST requests as credentials are usually sent to the website using that method

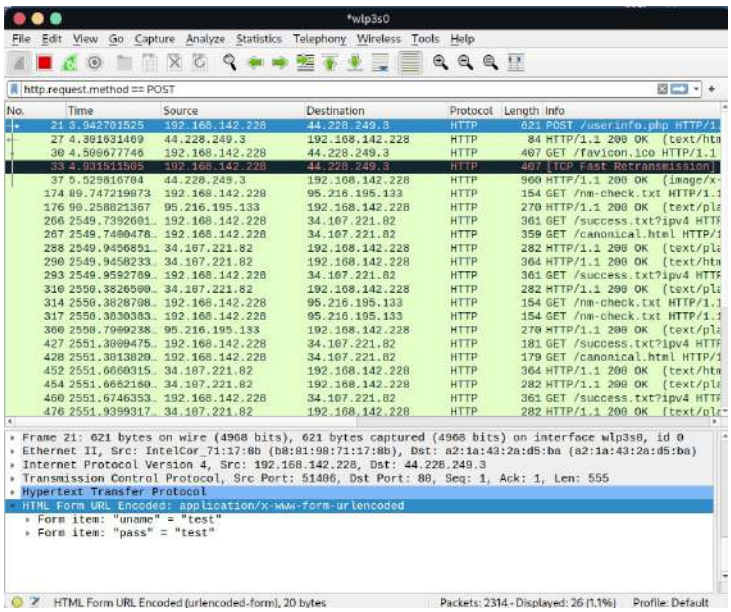
Step-8: Click the one with /userinfo.php. A new panel will open up. At the bottom of that, there will be a button with "application/x-www-form-urlencoded"



Step-9: Now, you'll be able to see the password and username which was entered in the vulnerable website.



Output Screenshot:



Result:

Network vulnerabilities using Wireshark was successfully detected and credentials were successfully found using network sniffing.

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
School of computing
Department of computer science and engineering

213CSE1302 – Information Security Fundamentals

Register No : 99220040586

Name : K.V. Hitesh Kumar Chowdary

Class : Cyber 2

Ex.No/Name : To understand the working of zenmap tool.

Procedure:

Step-1: Install the nmap into your computer you need to get the installer from below link

https://zenmap.org/download.html

Step-2: Complete the installation process

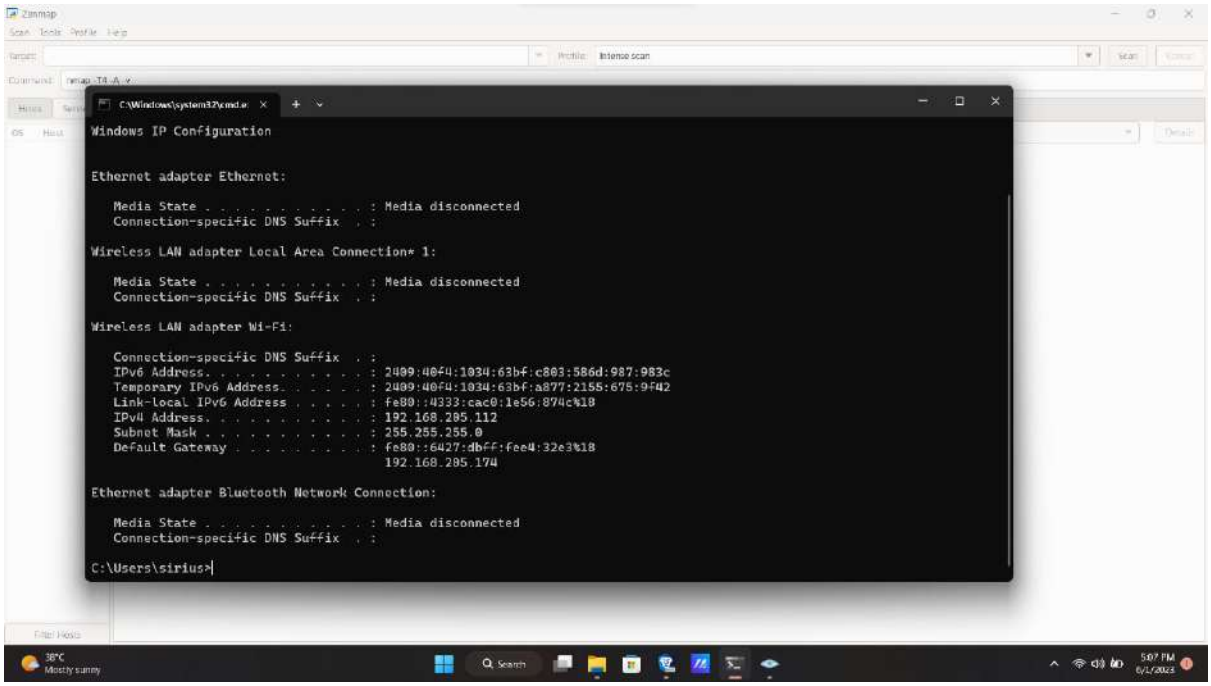
Step-3: Open command prompt and find your device ip address

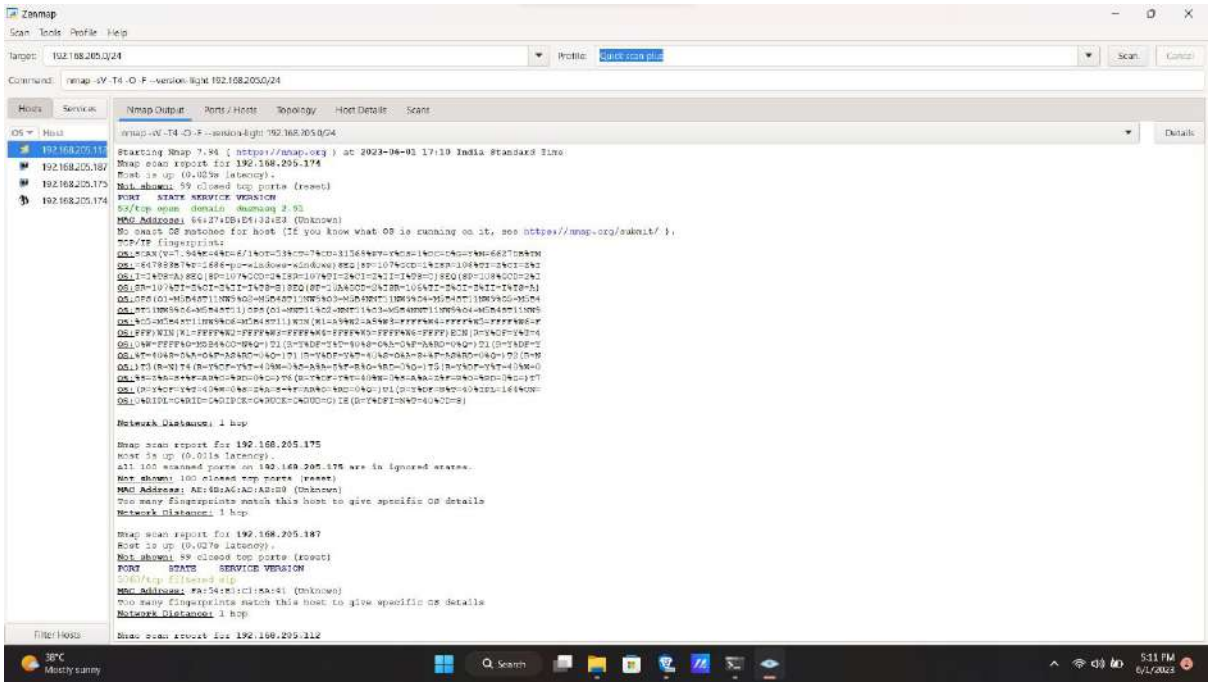
Check your net address and open the zenmap

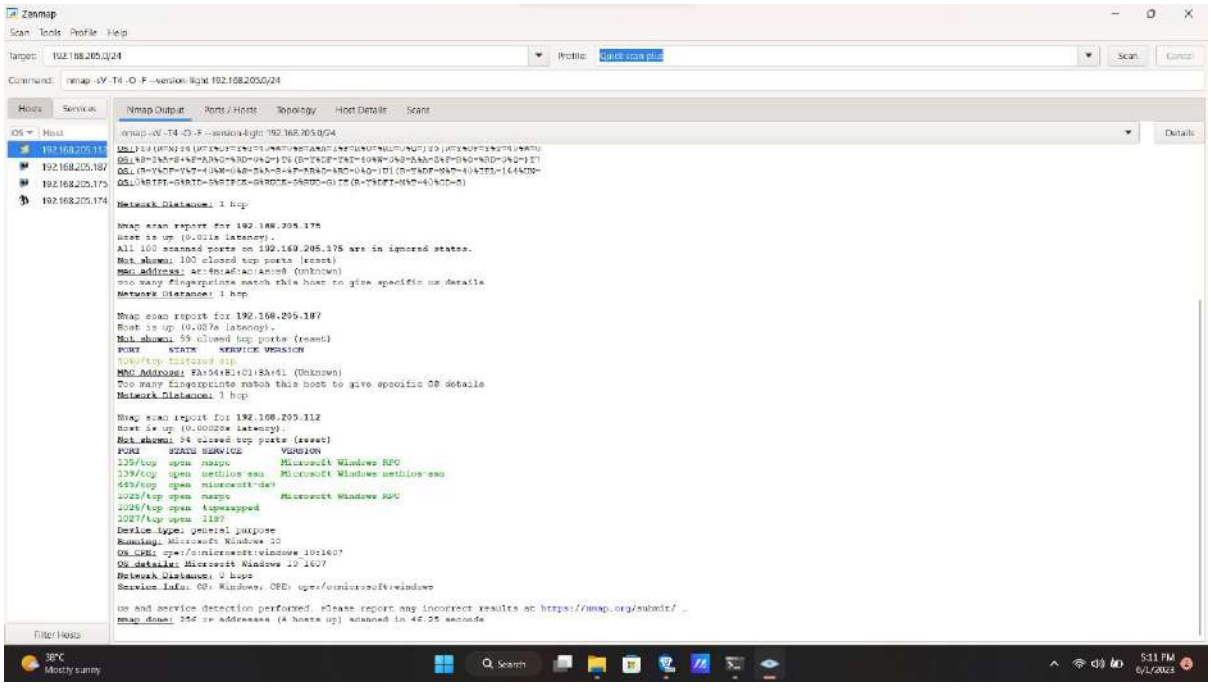
Step-4: enter your ip address and select host

Step-5: It will shows the mac address and ip address and types of port.

Output Screenshots:







Result:

Zenmap is installed successfully