



# Parul University

FACULTY OF ENGINEERING AND TECHNOLOGY

BACHELOR OF TECHNOLOGY

INFORMATION TECHNOLOGY  
DEPARTMENT

CYBER SECURITY LABORATORY  
(203105327)

VI SEMESTER

**Lab Manual**

## CERTIFICATE

This is to certify that Mr./Ms **Hemil Chovatiya** with enrollment no. **200303108003** has successfully completed his/her laboratory experiments in the **Cyber Security Laboratory (203105327)** from the department of **Information Technology** during the academic year **2022-23**.



Date of Submission: 03/03/2023

Staff In-charge: \_\_\_\_\_

Head of Department: \_\_\_\_\_

## TABLE OF CONTENT

Sr. No.	Practical Name	Page No.		Date of Performance	Date of Submission	Sign	Marks Out of 10
		Start	End				
1	Implementation to gather information from any pc connected to the Lan using whois, port scanners, network Scanning, Angry IP.	4	8	14 <sup>th</sup> -NOV-2022	21-Nov-2022		
2	Experiments with open source firewall/proxy packages like iptables, squid.	9	12	28-Nov-2022	05-Dec-2022		
3	Implementation of Steganography	13	16	5-DEC-2022	12-Dec-2023		
4	Implementation of MITM attack Using Wireshark /network sniffers.	17	20	19 <sup>th</sup> -DEC-2022	26-Dec-2023		
5	Implementation of windows Security using firewalls and other tools.	21	22	2 <sup>nd</sup> -JAN-2023	09-Jan-2023		
6	Implementation to identify web vulnerabilities, using owasp	23	29	23 <sup>rd</sup> -JAN-2023	30-Jan-2023		
7	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report	30	32	6 <sup>th</sup> -FEB-2023	13-Feb-2023		
8	Implementation of OS hardening and RAM dump analysis to collect the Artifacts and other Information.	33	36	13 <sup>th</sup> -FEB-2023	20-Feb-2023		
9	Implementation of Mobile Audit and generate the report of the existing Artifacts	37	40	20 <sup>th</sup> -FEB-2023	27-Feb-2023		
10	Implementation of Cyber Forensics tools for Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery.	41	43	27 <sup>th</sup> -FEB-2023	03-Feb-2023		

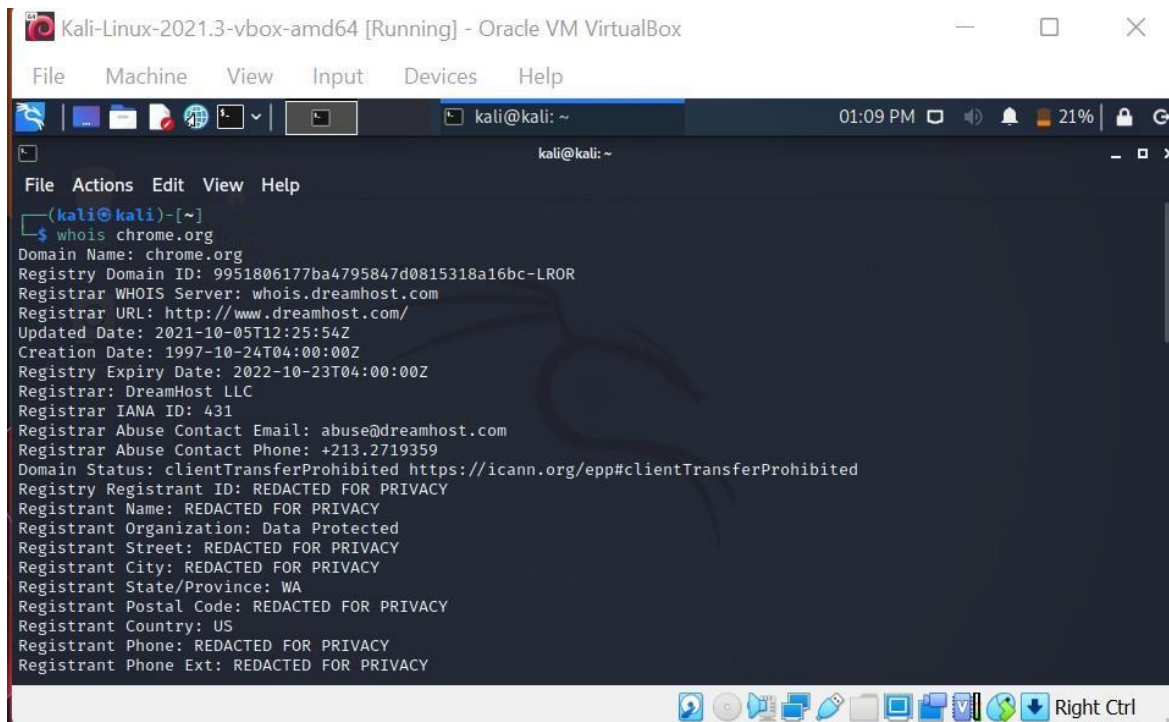
## PRACTICAL - 01

**AIM :-** Implementation to gather information from any pc connected to the Lan using whois, port scanners, network scanning, Angry Ip scanners etc.

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

- 1) After downloading create a new folder and name it as you want.
- 2) Extract it in new folder.
- 3) Open command prompt.
- 4) Cd and the path of the file.
- 5) Next run this command (whois and domain name)

### Using kali linux :-

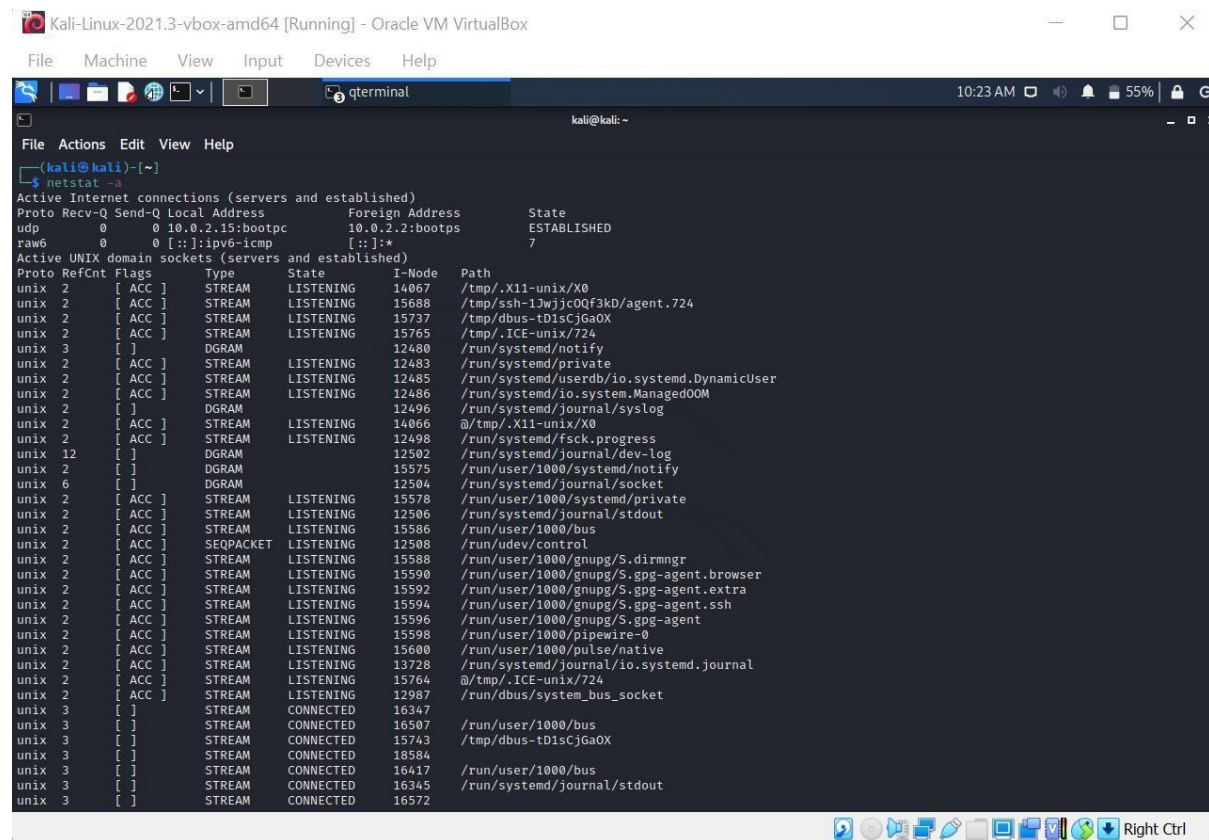


```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
01:09 PM 21%
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ whois chrome.org
Domain Name: chrome.org
Registry Domain ID: 9951806177ba4795847d0815318a16bc-LROR
Registrar WHOIS Server: whois.dreamhost.com
Registrar URL: http://www.dreamhost.com/
Updated Date: 2021-10-05T12:25:54Z
Creation Date: 1997-10-24T04:00:00Z
Registry Expiry Date: 2022-10-23T04:00:00Z
Registrar: DreamHost LLC
Registrar IANA ID: 431
Registrar Abuse Contact Email: abuse@dreamhost.com
Registrar Abuse Contact Phone: +213.2719359
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Data Protected
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: WA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
```

## Port scanners :-

The Windows command prompt utility netstat allows you to scan your computer to learn whether it has any programs or services listening for incoming connections over the Internet. In most cases, legitimate programs such as anti-virus update services cause your computer to listen for incoming connections.

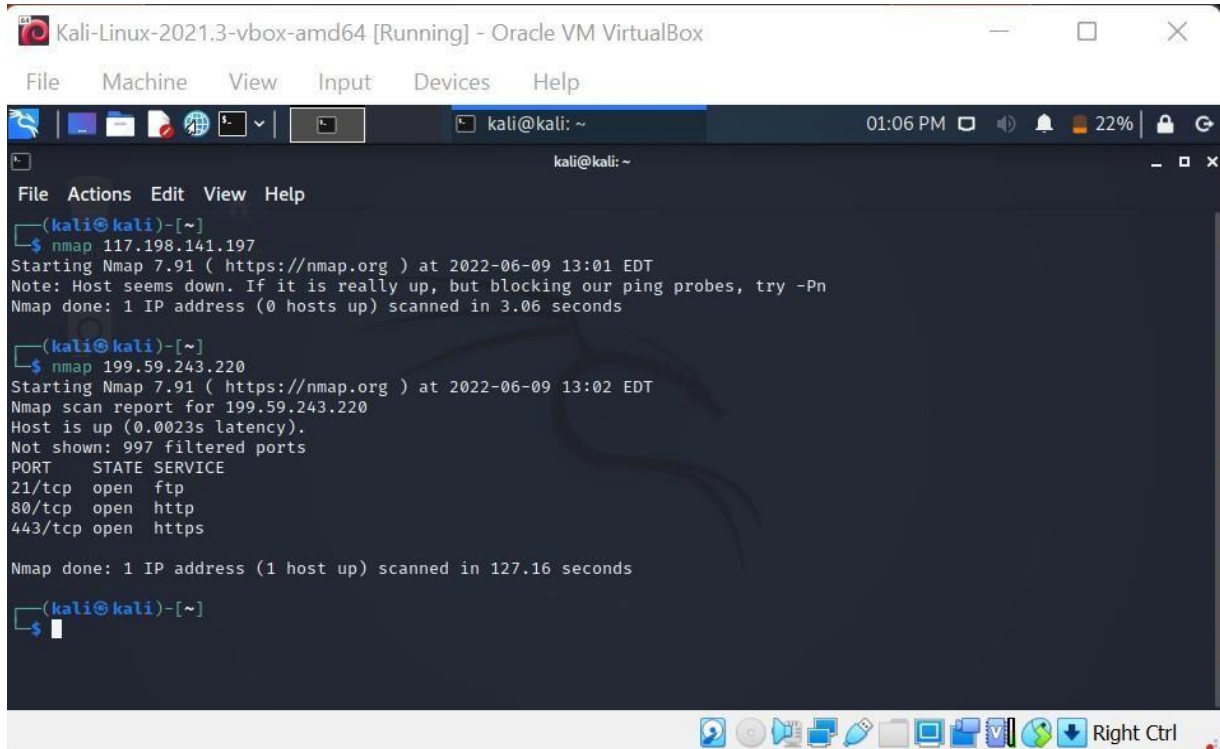
- 1) Open command prompt.
- 2) And then type this command netstat -a
- 3) The computer displays a list of all open tcp and udp ports.



```

(kali@kali)-[~]
└─$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 10.0.2.15:bootpc       10.0.2.2:bootps        ESTABLISHED
raw        0      0 0.0.0.0:icmp            0.0.0.0:*               7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State           I-Node      Path
unix  2      [ ACC ] STREAM   LISTENING     14067       /tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM   LISTENING     15688       /tmp/ssh-1jwjic0Qf3kD/agent.724
unix  2      [ ACC ] STREAM   LISTENING     15737       /tmp/dbus-tD1sCjGaOX
unix  2      [ ACC ] STREAM   LISTENING     15765       /tmp/.ICE-unix/724
unix  3      [ ]     DGRAM                12480       /run/systemd/notify
unix  2      [ ACC ] STREAM   LISTENING     12483       /run/systemd/private
unix  2      [ ACC ] STREAM   LISTENING     12485       /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ] STREAM   LISTENING     12486       /run/systemd/io.system.ManagedOOM
unix  2      [ ]     DGRAM                12496       /run/systemd/journal/syslog
unix  2      [ ACC ] STREAM   LISTENING     14066       @/tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM   LISTENING     12498       /run/systemd/fsck.progress
unix  12     [ ]     DGRAM                12502       /run/systemd/journal/dev-log
unix  2      [ ]     DGRAM                15575       /run/user/1000/systemd/notify
unix  6      [ ]     DGRAM                12504       /run/systemd/journal/socket
unix  2      [ ACC ] STREAM   LISTENING     15578       /run/user/1000/systemd/private
unix  2      [ ACC ] STREAM   LISTENING     12506       /run/systemd/journal/stdout
unix  2      [ ACC ] STREAM   LISTENING     15586       /run/user/1000/bus
unix  2      [ ACC ] SEQPACKET LISTENING     12508       /run/udev/control
unix  2      [ ACC ] STREAM   LISTENING     15588       /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ] STREAM   LISTENING     15590       /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ] STREAM   LISTENING     15592       /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ] STREAM   LISTENING     15594       /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ] STREAM   LISTENING     15596       /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ] STREAM   LISTENING     15598       /run/user/1000/pipewire-0
unix  2      [ ACC ] STREAM   LISTENING     15600       /run/user/1000/pulse/native
unix  2      [ ACC ] STREAM   LISTENING     13728       /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ] STREAM   LISTENING     15764       @/tmp/.ICE-unix/724
unix  2      [ ACC ] STREAM   LISTENING     12987       /run/dbus/system_bus_socket
unix  3      [ ]     STREAM   CONNECTED     16507       /run/user/1000/bus
unix  3      [ ]     STREAM   CONNECTED     15743       /tmp/dbus-tD1sCjGaOX
unix  3      [ ]     STREAM   CONNECTED     18584
unix  3      [ ]     STREAM   CONNECTED     16417       /run/user/1000/bus
unix  3      [ ]     STREAM   CONNECTED     16345       /run/systemd/journal/stdout
unix  3      [ ]     STREAM   CONNECTED     16572
  
```

- 4) Look for any port number that displays the word "LISTENING" under the "State" column. Your computer is listening for incoming connection requests over these port numbers. Look the port numbers up using an online list to determine the programs and services associated with those ports.
- 5) We can scan the port through the Nmap also.



```
Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
01:06 PM 22%
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap 117.198.141.197
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-09 13:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds

(kali@kali)-[~]
$ nmap 199.59.243.220
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-09 13:02 EDT
Nmap scan report for 199.59.243.220
Host is up (0.0023s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 127.16 seconds

(kali@kali)-[~]
$
```

### How to Scan for Any Device IP Address on a Network With Tools :-

1. [IP Address Tracker](#)
2. [Angry IP Scanner](#)
3. [IP Scanner](#)
4. [IP Address Manager](#)
5. [Engineer's Toolset](#)
6. [Network Performance Monitor](#)
7. [User Device Tracker](#)

**Angry IP Scanners :-** Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports.

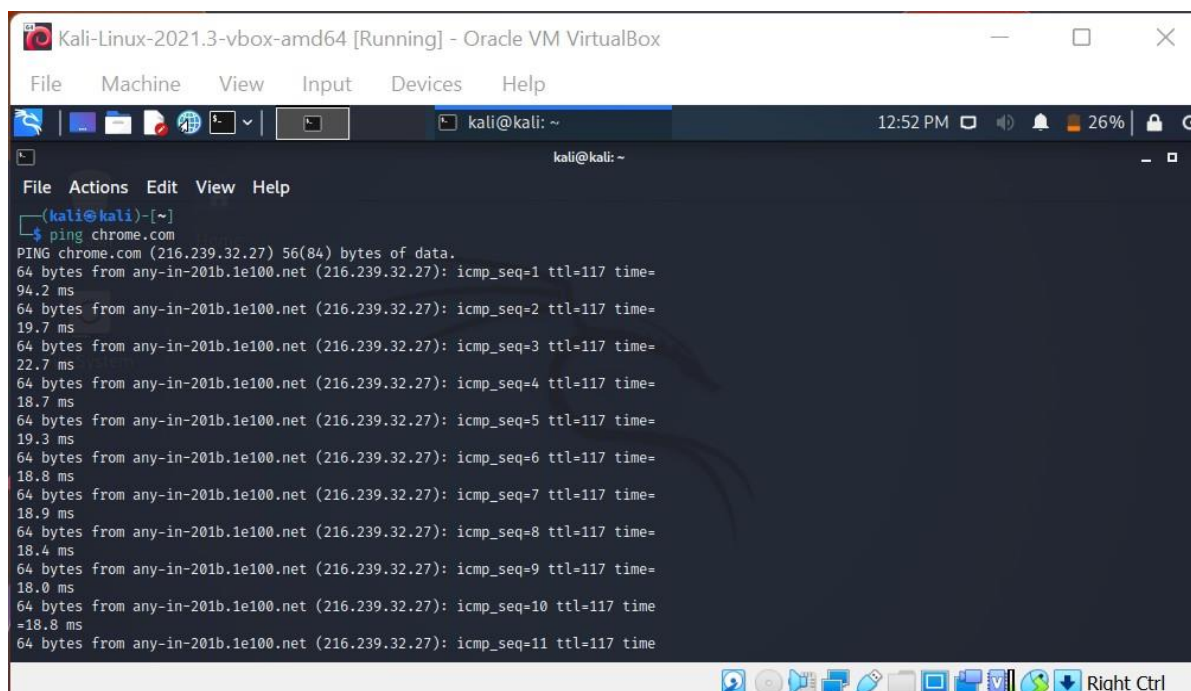
- 1) After the installation we have to run it we will get this pop up
- 2) Now it open like below the figure.



## PING SCANNING:

Ping scans are **internet control message protocol (ICMP) requests** and send out an automated blast of several ICMP requests to different servers to bait responses. IT administrators may use this technique to troubleshoot, or disable the ping scan by using a firewall — which makes it impossible for attackers to find the network through pings.

## OUTPUT:

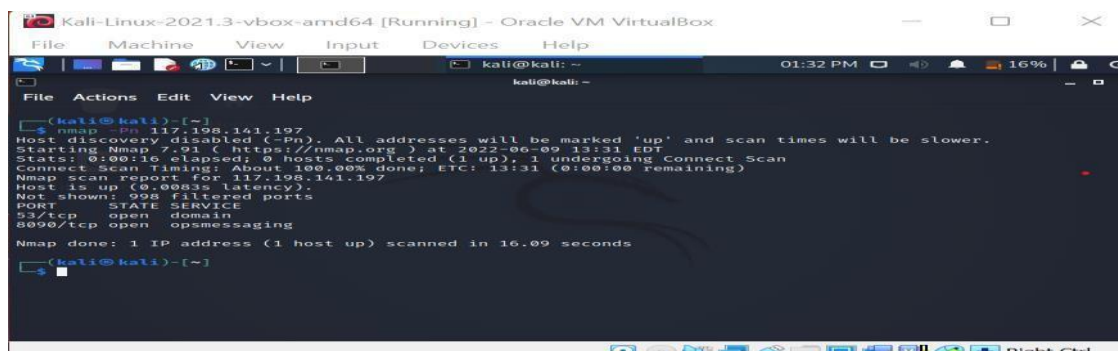


```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ping chrome.com
PING chrome.com (216.239.32.27) 56(84) bytes of data:
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=1 ttl=117 time=94.2 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=2 ttl=117 time=19.7 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=3 ttl=117 time=22.7 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=4 ttl=117 time=18.7 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=5 ttl=117 time=19.3 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=6 ttl=117 time=18.8 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=7 ttl=117 time=18.9 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=8 ttl=117 time=18.4 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=9 ttl=117 time=18.0 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=10 ttl=117 time=18.8 ms
64 bytes from any-in-201b.1e100.net (216.239.32.27): icmp_seq=11 ttl=117 time=

```

## HOST:



```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -Pn 117.198.141.197
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-09 13:31 EDT
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 100.00% done; ETC: 13:31 (0:00:00 remaining)
Nmap scan report for 117.198.141.197
Host is up (0.0082s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
8090/tcp  open  opsmessaging
Nmap done: 1 IP address (1 host up) scanned in 16.09 seconds
(kali@kali)-[~]
$

```





## **PRACTICAL - 2**

**AIM :-** Experiments with open source firewall/proxy packages like iptables, squid etc.

### **About iptables**

iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action.

### **Policy Chain Default Behavior**

We need to decide what you want the default behavior of the three chains to be.

To see what your policy chains are currently configured to do with unmatched traffic, run the iptables -L | grep policy command.

### **Types of Chains**

iptables uses three different chains: input, forward, and output.

**Input** – This chain is used to control the behaviour for incoming connections. For example, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.

**Forward** – This chain is used for incoming connections that aren't actually being delivered locally. Think of a router – data is always being sent to it but rarely actually destined for the router itself; the data is just forwarded to its target. Unless you're doing some kind of routing, NATing, or something else on your system that requires forwarding, you won't even use this chain.

**Output** – This chain is used for outgoing connections. For example, if you try to ping howtogeek.com, iptables will check its output chain to see what the rules are regarding ping and howtogeek.com before making a decision to allow or deny the connection attempt.

### **For Flush the Commands:-**

Sudo iptables -F

**Accept** – Allow the connection.



```
Kali-Linux-2021.3-vbox-amd64 [Running] - Ora...
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

(root@kali)-[/home/kali]
# iptables -L -v
iptables v1.8.7 (nf_tables)

(root@kali)-[/home/kali]
# ping 5.5.5.5
PING 5.5.5.5 (5.5.5.5) 56(84) bytes of data.
■
```

```
(root@kali)-[~]
# iptables -A INPUT -s 8.8.8.8 -j ACCEPT

(root@kali)-[~]
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=199 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=74.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=72.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=71.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=70.0 ms
^C
— 8.8.8.8 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 69.950/97.287/198.831/50.791 ms

(root@kali)-[~]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
5 420 ACCEPT all -- any any dns.google anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
```



**Drop** – Drop the connection, act like it never happened. This is best if you don't want the source to realize your system exists.

```
(root@kali)-[~]
# iptables -A INPUT -s 8.8.8.8 -j DROP

(root@kali)-[~]
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
-- 8.8.8.8 ping statistics --
3 packets transmitted, 0 received, 100% packet loss, time 2039ms

(root@kali)-[~]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
    3  252 DROP       all  --  any    any    dns.google     anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
```

**Reject** – Don't allow the connection, but send back an error. This is best if you don't want a particular source to connect to your system, but you want them to know that your firewall blocked them.

```
(root@kali)-[~]
# iptables -A INPUT -s 8.8.8.8 -j REJECT

(root@kali)-[~]
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
-- 8.8.8.8 ping statistics --
3 packets transmitted, 0 received, 100% packet loss, time 2053ms

(root@kali)-[~]
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
    3  252 REJECT     all  --  any    any    dns.google     anywhere             reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
```



### **Squid: Optimising Web Delivery**

---

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. Squid has extensive access controls and makes a great server accelerator. It runs on most available operating systems, including Windows and is licensed under the GNU GPL.

### **Making the most of your Internet Connection**

---

Squid is used by hundreds of Internet Providers world-wide to provide their users with the best possible web access. Squid optimizes the data flow between client and server to improve performance and caches frequently-used content to save bandwidth. Squid can also route content requests to servers in a wide variety of ways to build cache server hierarchies which optimize network throughput.



## **PRACTICAL - 3**

### **AIM :-** Implementation of Steganography.

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data in the form of image,

### **Hiding text inside of image:- STEPS :-**

- 1) Open image
- 2) Select the path and copy it and open the command prompt and paste the path with the help of cd command.

(or)

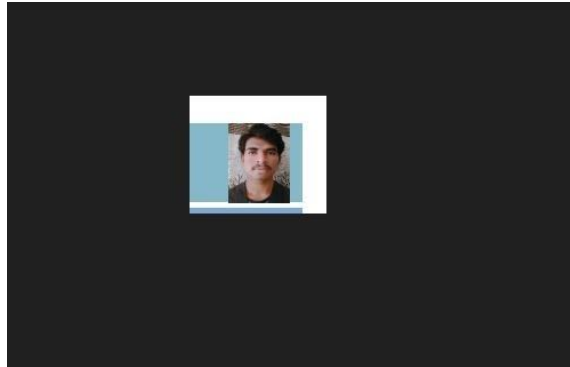
In the path selection write cmd

- 3) Enter the command for hiding the message inside the image  
Echo "TEXT MESSAGE" >> IMAGE NAME

**EXAMPLE :-** echo "Bhagav 200303124205 " >> testing.png

```
Command Prompt
D:\>"C:\Users\bharg\Downloads\m.png">echo "Bhargav 200303124205" >>testing.png
D:\>|
```

- 4) THEN OPEN THE IMAGE WITH NOTEPAD IN THE LAST WE WILL FIND THE MESSAGE



### **Hiding zip file inside image:-**

- 1) Choose the zip file and one file
- 2) Enter the command  
Copy /b image name + zip file name and new image name

**Example:-** copy /b test.png + Node-Mcu-Jammer.zip testing.png

```
Command Prompt
D:\>"C:\Users\bharg\Downloads\m.png">echo "Bhargav 200303124205" >>testing.png
D:\>"C:\Users\bharg\Downloads\m.png">copy /b test.png + Node-Mcu-Jammer.zip testing.png
D:\>|
```

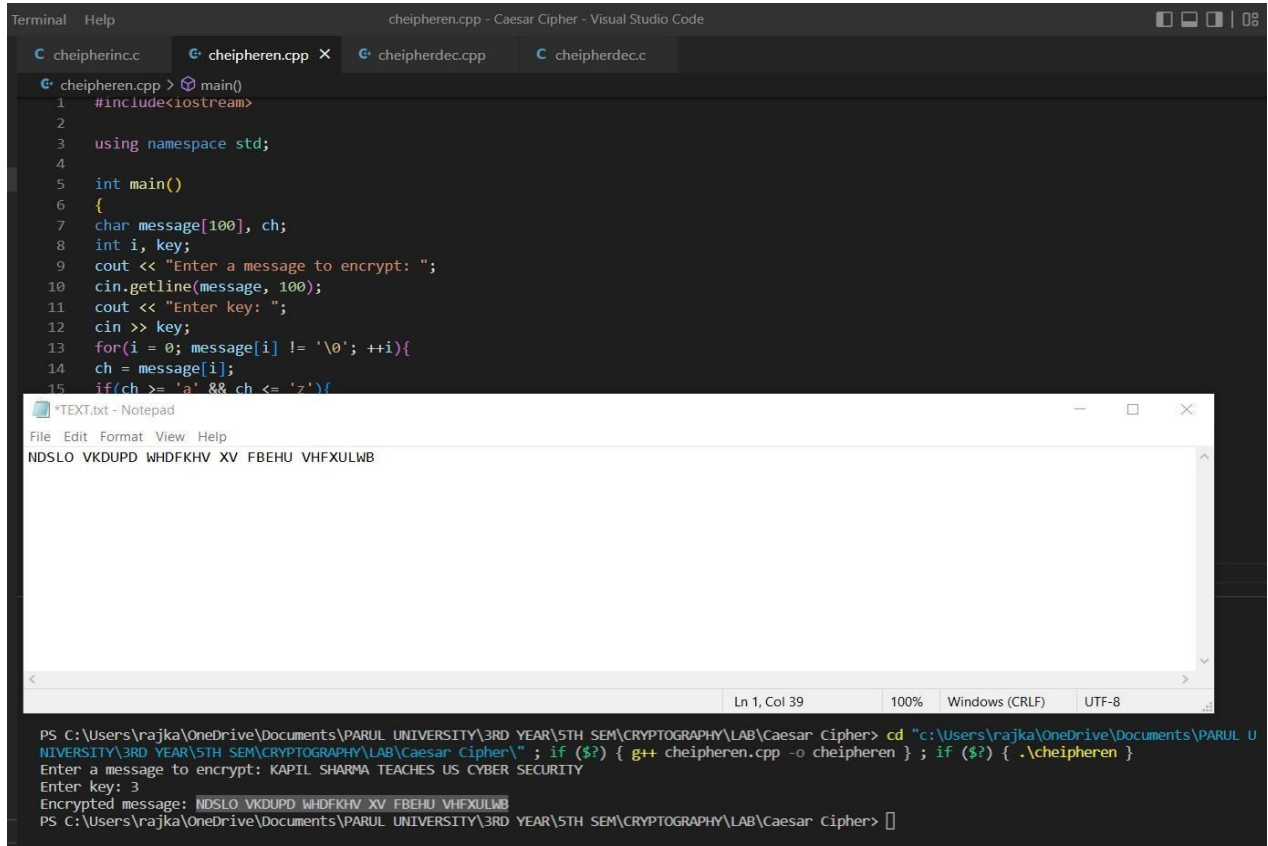
- 3) Rename the new image extension as .zip

### **Hiding encrypted text file inside image :-**

- 1) Choose image



- 2) Run the code and change it to an plain text to cipher text to others can not able to read them



```

cheipheren.cpp - Caesar Cipher - Visual Studio Code
cheipherenc.c  cheipheren.cpp x cheipherdec.cpp  cheipherdec.c
cheipheren.cpp > main()
1 #include<iostream>
2
3 using namespace std;
4
5 int main()
6 {
7     char message[100], ch;
8     int i, key;
9     cout << "Enter a message to encrypt: ";
10    cin.getline(message, 100);
11    cout << "Enter key: ";
12    cin >> key;
13    for(i = 0; message[i] != '\0'; ++i){
14        ch = message[i];
15        if(ch >= 'a' && ch <= 'z'){

```

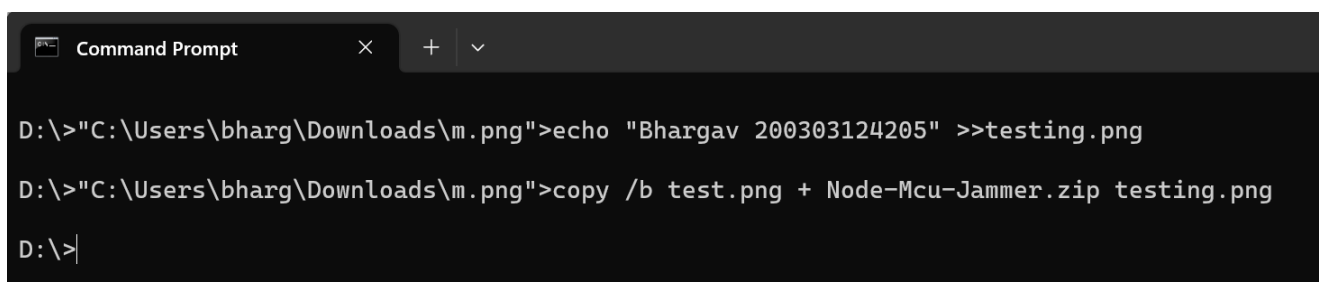
```

PS C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CRYPTOGRAPHY\LAB\Caesar Cipher> cd "c:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CRYPTOGRAPHY\LAB\Caesar Cipher\" ; if ($?) { g++ cheipheren.cpp -o cheipheren } ; if ($?) { .\cheipheren }
Enter a message to encrypt: KAPIL SHARMA TEACHES US CYBER SECURITY
Enter key: 3
Encrypted message: NDSLO VKDUPD WHDFKHV XV FBEHU VHFJULWB
PS C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CRYPTOGRAPHY\LAB\Caesar Cipher>

```

- 3) After that the encrypted message paste it in a new text file and name it as we want
- 4) Enter the command shown bellow  
Copy /b image name + file name new image name

**EXAMPLE:-** copy /b test.png + text.txt testing.png

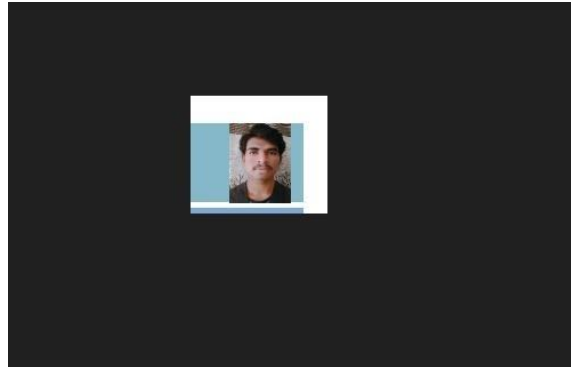


```

Command Prompt
D:\>"C:\Users\bharg\Downloads\m.png">echo "Bhargav 200303124205" >>testing.png
D:\>"C:\Users\bharg\Downloads\m.png">copy /b test.png + Node-Mcu-Jammer.zip testing.png
D:\>

```

- 5) Open the message with the note pad scroll it down there we can find our encrypted text as shown in the image



- 6) After the message Is found encrypted then make it decrypt using the program.

```
C cheipherinc.c  C cheipheren.cpp  C cheipherdec.cpp  C cheipherdec.c X
C cheipherdec.c > main()
1  #include<stdio.h>
2
3  int main()
4  {
5  char message[100], ch;
6  int i, key;
7  printf("Enter a message to decrypt: ");
8  gets(message);
9  printf("Enter key: ");
10 scanf("%d", &key);
11
12 for(i = 0; message[i] != '\0'; ++i){
13 ch = message[i];
14 if(ch >= 'a' && ch <= 'z'){
15 ch = ch - key;
16 if(ch < 'a'){
17 ch = ch + 'z' - 'a' + 1;
18 }
19 message[i] = ch;
20 }
21 else if(ch >= 'A' && ch <= 'Z'){
22 ch = ch - key;
23 if(ch < 'A'){
24 ch = ch + 'Z' - 'A' + 1;
25 }
26 }
27 }
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

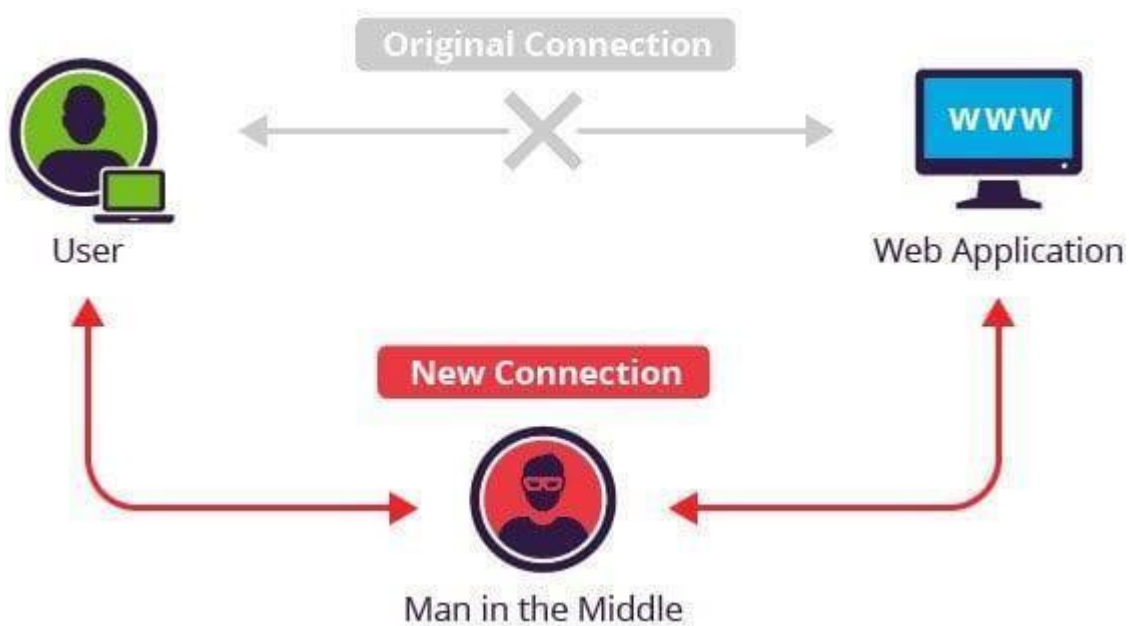
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell <https://aka.ms/pscore6>



## **PRACTICAL – 4**

### **AIM :- Implementation of MITM attack using Wireshark /network sniffers.**

**Man – in – the – middle – attack :-** is a very common type of cyber attack which involves eavesdropping on a network connection. The attackers usually insert themselves between a conversation, usually occurring among a web server and an application. Hackers can have various end goals for launching this attack, they may either silently observe data packets or impersonate a user and modify the data they send or receive.



### **Implementation of Wireshark :-**

We'll need a client machine as well whose network traffic we will spoof and sniff to get cleartext submission of passwords from certain vulnerable websites.

The IP address of the client machine used over LAN for this demo is: 192.168.1.44

And the Attacker IP is: 192.168.1.1



### Steps :-

- Open terminal and ping the target machine to verify the IP address you are using and to add it to your arp table
- Type arp in the terminal command line to see your arp table
- For security purposes, IP forwarding is by default disabled in modern Linux systems. For temporarily enabling it, type : echo 1 > /proc/sys/net/ipv4/ip\_forward
- For ARP poisoning, the command syntax is: arpspoof -i interface -t target -r host

A basic setup is complete and victim network traffic will now pass through the attacker machine. To listen to these packets, we will use Wireshark .

### Implementation of wireshark :- Steps :-

- Open up a new terminal and type wireshark. Go to the interface which is capturing all the data flow (here eth0) and start the capture.
- Filter out packets according to what you are looking for. For the purpose of this demo, the user is logging in to a vulnerable website DVWA which uses HTTP instead of the secure version HTTPS. Filter protocol as http and search for required data.

No.	Time	Source	Destination	Protocol	Length	Info
27	3.018434822	192.168.1.44	34.217.87.81	HTTP	537	GET /dvwa/vulnerabilities/brute/?username=pablo&password=cocaine&login=...
40	3.287583239	34.217.87.81	192.168.1.44	HTTP	407	HTTP/1.1 200 OK (text/html)
346	70.099436430	192.168.1.44	34.217.87.81	HTTP	581	GET /dvwa/vulnerabilities/brute/?username=pablo&password=letmein&login=...
355	70.354802397	34.217.87.81	192.168.1.44	HTTP	1892	HTTP/1.1 200 OK (text/html)
360	70.368923992	192.168.1.44	34.217.87.81	HTTP	509	GET /dvwa/hackable/users/pablo.jpg HTTP/1.1
367	70.625162397	34.217.87.81	192.168.1.44	HTTP	1864	HTTP/1.1 200 OK (JPEG JFIF image)
454	79.279781982	192.168.1.44	34.217.87.81	HTTP	537	GET /dvwa/vulnerabilities/brute/ HTTP/1.1
458	79.288494380	192.168.1.44	34.217.87.81	HTTP	537	GET /dvwa/vulnerabilities/brute/ HTTP/1.1
466	79.547272589	34.217.87.81	192.168.1.44	HTTP	1831	HTTP/1.1 200 OK (text/html)
477	79.558745717	34.217.87.81	192.168.1.44	HTTP	1831	HTTP/1.1 200 OK (text/html)

Frame 346: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits) on interface 0  
 Ethernet II, Src: Micro-St\_8d:10:9c (d8:cb:8a:8d:10:9c), Dst: Micro-St\_8d:1b:7b (d8:cb:8a:8d:1b:7b)  
 Internet Protocol Version 4, Src: 192.168.1.44, Dst: 34.217.87.81

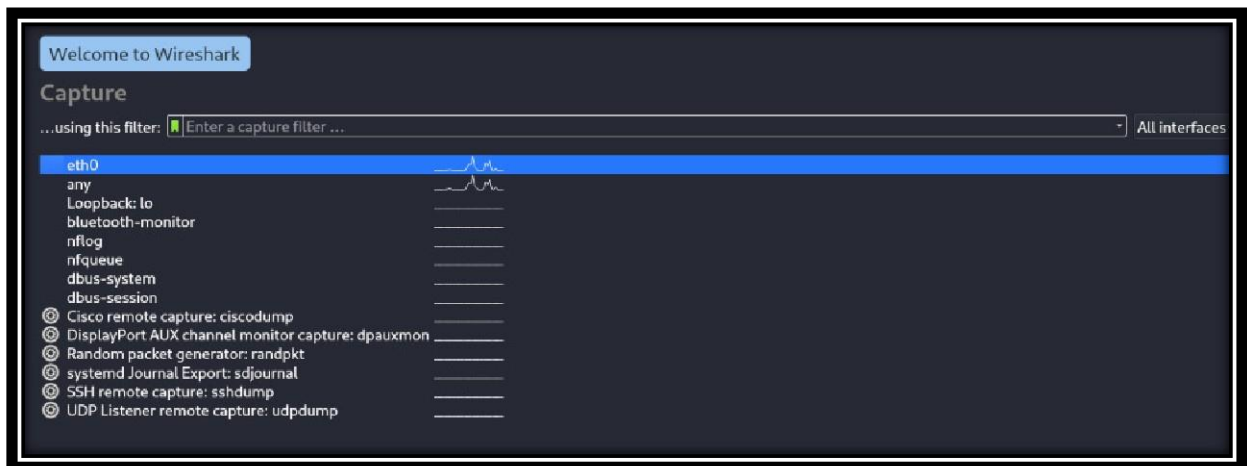
- Right click on the packet and follow TCP stream to open up the data contained within. We can clearly obtain the login credentials of the user, that is the username and password.



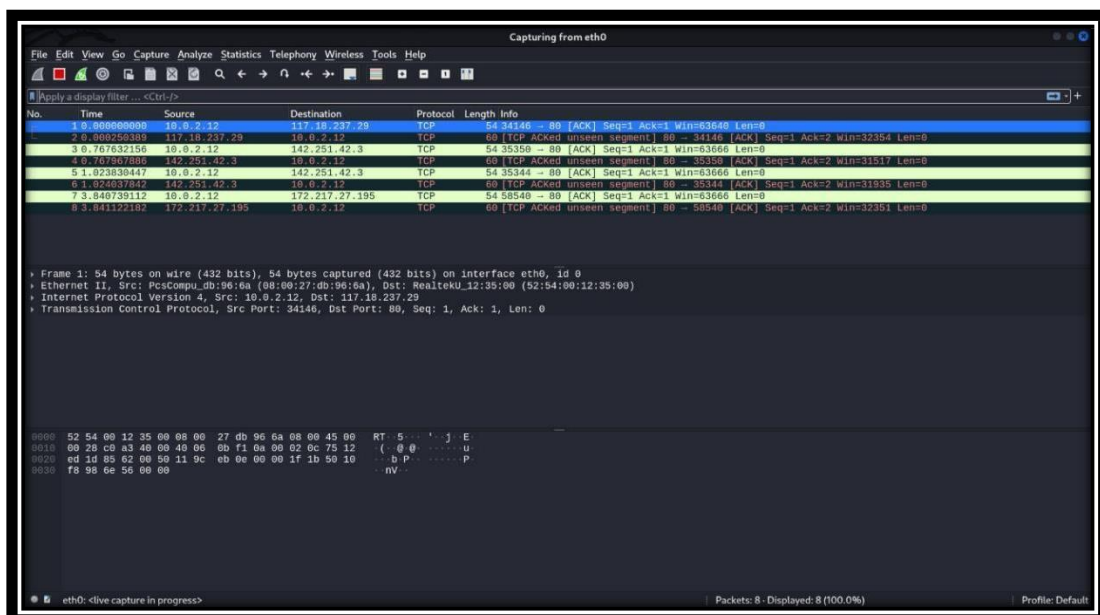
## IMPLEMENTATION OF STEPS:

### STEP-01:

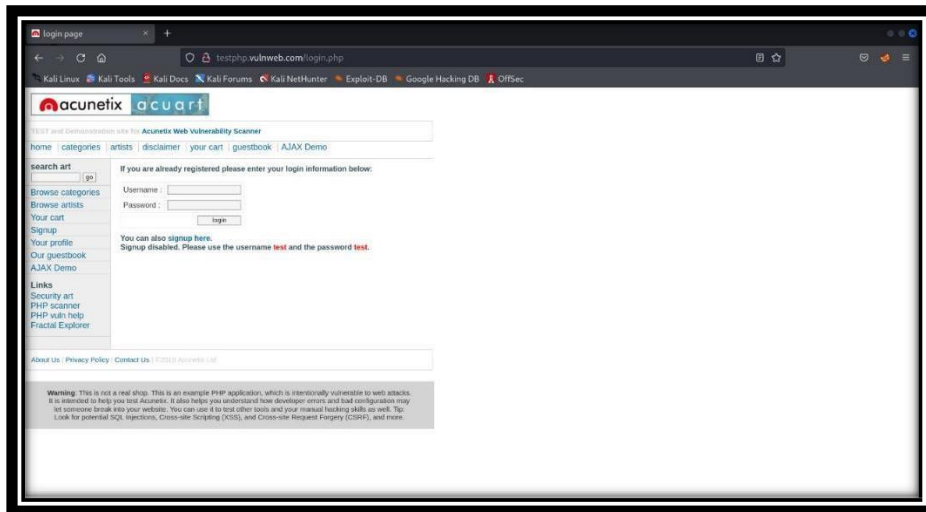
```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~[~]  
# sudo wireshark  
** (wireshark:1312) 12:39:29.623141 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



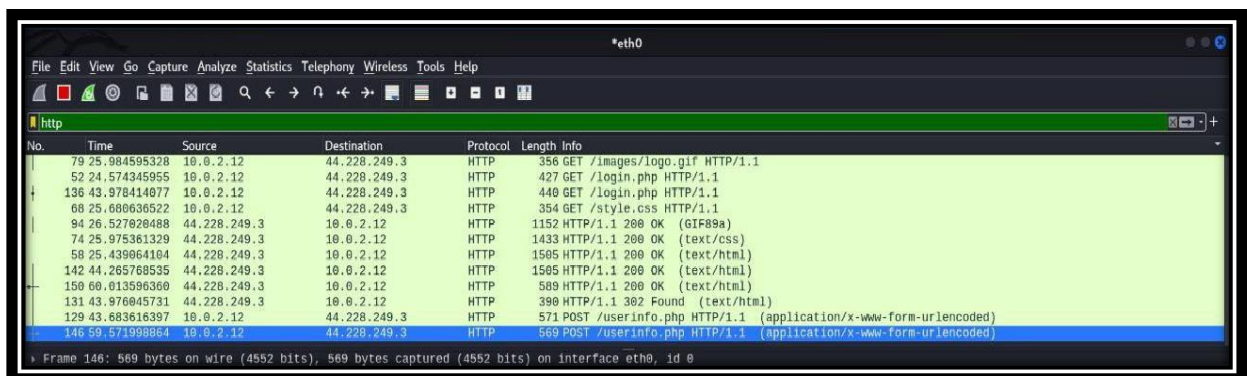
### STEP-02:



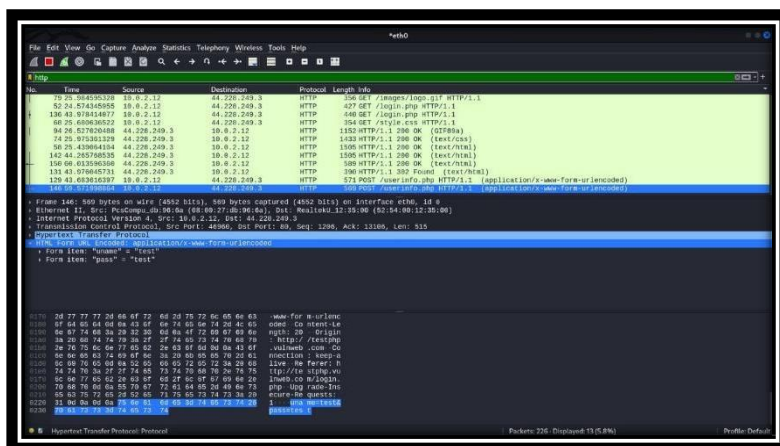
### STEP-03:



### STEP-04:



### STEP-05:







## PRACTICAL – 5

### **AIM :- Implementation of windows security using firewalls and other tools**

Windows Defender Firewall helps prevent hackers and malicious software from gaining access to your PC through the internet or a network. Your organization might require you to turn it on before you can access their network resources from your device.

#### **To turn on Windows Defender Firewall:**

Go to Start and open Control Panel.

Select System and Security > Windows Defender Firewall.

Choose Turn Windows Firewall on or off.

Select Turn on Windows Firewall for domain, private, and public network settings.





Customize Settings

← → ↕ ↑ > Control Panel > System and Security > Windows Defender Firewall > Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

Public network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☐ Turn off Windows Defender Firewall (not recommended)

**List Of The Best Free Firewall :-**

1)SolarWinds Network Firewall Security Management

2)ManageEngine Firewall Analyzer

3)System Mechanic Ultimate Defense

4)Norton

5)LifeLock

6)ZoneAlarm

7)Comodo

Firewall

8)TinyWall

9)Netdefender

10)Glasswire

11)PeerBlock

12) AVS Firewall

13) OpenDNS Home

14)Privatefirewall



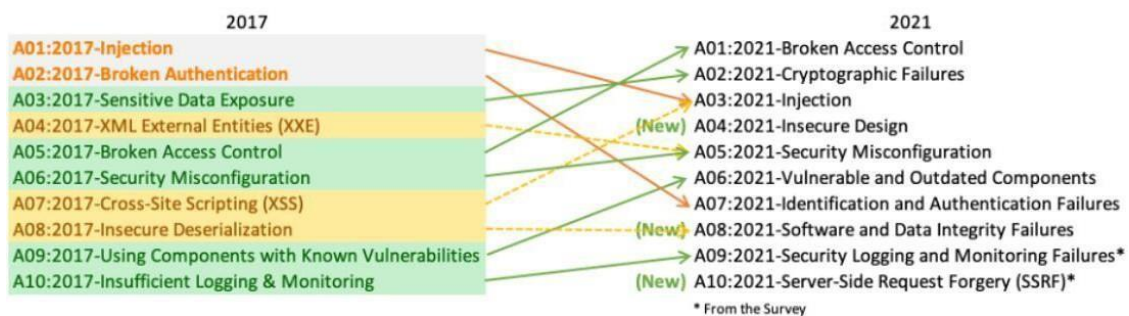
## **PRACTICAL – 6**

**AIM :-** Implementation to identify web vulnerabilities, using owasp project.

### **What is OWASP?**

- OWASP is Open Web Application Security Project
- It is a team of web researcher's which monitors the vulnerability's.
- It works to improve the security of the software.
- It sort out top 10 vulnerability's.

### **TOP 10 vulnerability's in OWASP 2021**



### **A01:2021 BROKEN ACCESS CONTROL**

- 94% application's are tested for some form of broken access control.
- Access control means the person outside the organization does not have the access for data or control for the application.
- Failure of access control leads to information disclosure
- Bypassing access control by modifying the parameters in URL is one of the way for BROKEN ACCESS CONTROL.
- Permitting viewing or editing someone else's account, by providing its unique identifier it is other way.

### **A02:2021 CRYPTOGRAPHIC FAILURE**



- Sensitive Data Exposure, which is more of a broad symptom rather than a root cause, the focus is on failures related to cryptography.
- Failure of cryptography it leads to loss of sensitive information.
- It happens when we may used old or weak cryptographic algorithm.
- It may happens because of re-used or weak crypto keys.
- Are initialization vectors ignored, reused, or not generated sufficiently secure for the cryptographic mode of operation, it is also one of the possibilities for cryptographic failure.

### **A03:2021 INJECTION**

- It is the third highest common vulnerability in an web application.
- Most common Injections are SQL, OS command, Object Relational Mapping etc.
- User-supplied data is not validated, filtered, or sanitized by the application.
- Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

### **A04:2021 INSECURE DESIGN**

- It is referred as risks related to design and architectural flaws.
- An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.
- We differentiate between design flaws and implementation defects for a reason.
- A secure design can still have implementation defects leading to vulnerabilities that may be exploited.

### **A05:2021 SECURITY MISCONFIGURATIONS**

- 90% of the applications were tested for some type of misconfigurations.
- It mostly happens when there is a disturbances in the system functionalities.
- Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services.
- Unnecessary features are enabled or installed.



- The server does not send security headers or directives, or they are not set to secure values.

#### **A06:2021 Vulnerable and Outdated Components**

- Vulnerable Components are a known issue that we struggle to test and assess risk
- It may happen when we don't know the version we use (both client and server side) or when we use old versions, where it will be more vulnerable.
- If you don't update the software like windows versions or BIOS updates.
- If software developers do not test the compatibility of updated, upgraded, or patched libraries.

#### **A07:2021 Identification and Authentication Failures**

- Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks.
- It happens due to CRYPTOGRAPHIC FAILURE too.
- Has missing values for authentication.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".

#### **A08:2021 SOFTWARE AND DATA INTEGRITY FAILURE**

- Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations.
- many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application.
- Attackers could potentially upload their own updates to be distributed and run on all installations.

#### **A09:2021 SECURITY LOGGING AND MONITORING FAILURE**

- this category is to help detect, escalate, and respond to active breaches.
- Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time.

- Logins are not stored, if stored also they have stored locally which leads to this vulnerability.
- Logs of applications and APIs are not monitored for suspicious activity.

### **A10:2021 SERVER SIDE REQUEST FORGERY(SSRF)**

- When a client send a request then the server then the server send the acknowledgement of the request.
- Here the request has been modified by the attacker so they can access the data in the server.
- SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL.
- As modern web applications provide end-users with convenient features, fetching a URL becomes a common scenario. As a result, the incidence of SSRF is increasing.
- Developers can prevent SSRF by implementing some or all the following defense in depth controls.

### **How to use OWASP ZAP:**

Install tool form <https://www.zaproxy.org/> and start with attack on a testing website to see the security checks:

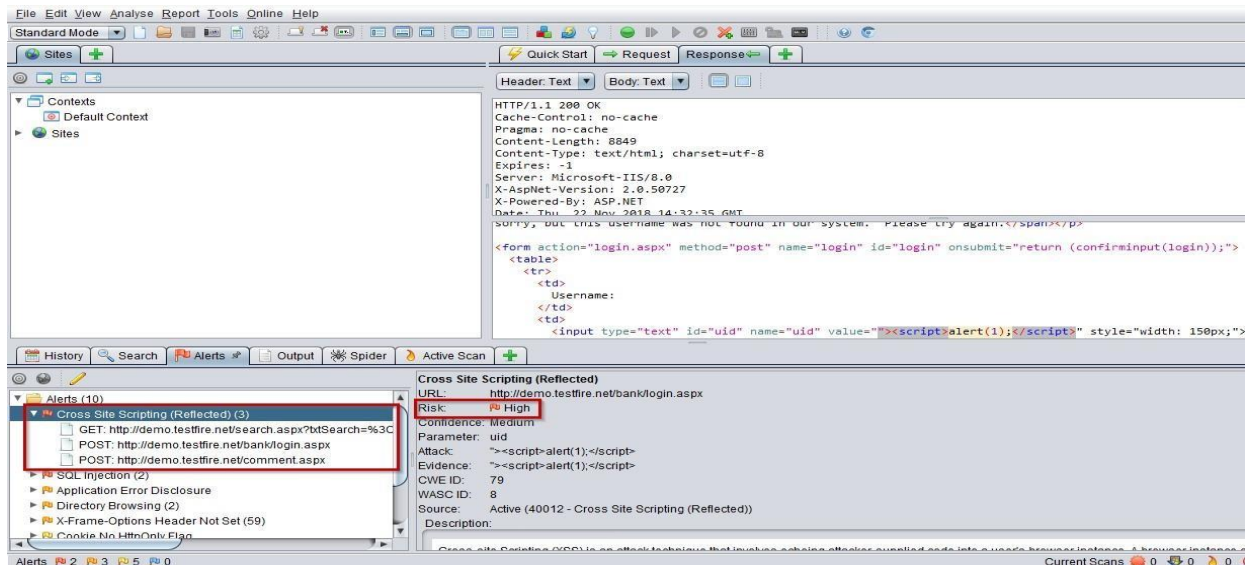


Response after attacking on a website are mentioned below and the good thing about OWASP ZAP it shows the URL in the response that where are the issues.



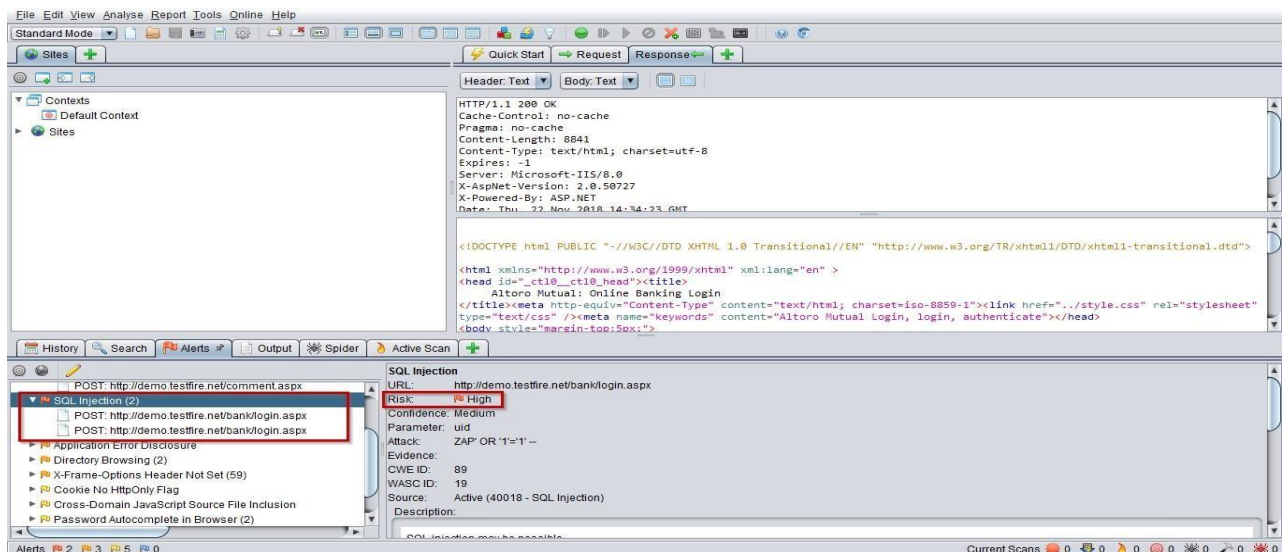
## Cross-Site scripting :

Vulnerabilities that exists in cross-site scripting



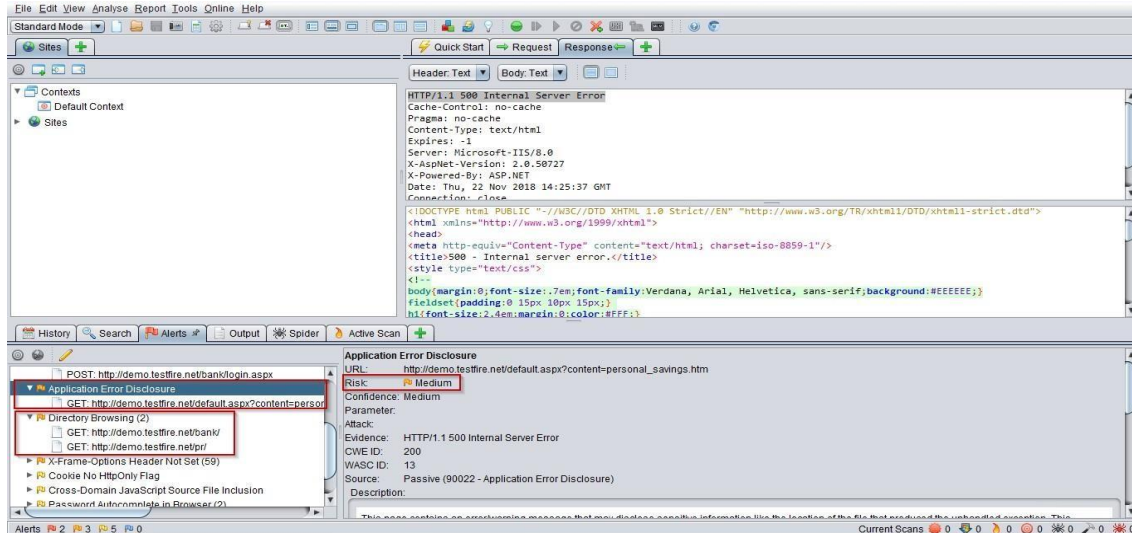
## SQL Injection :

Vulnerabilities that exists in SQL injection



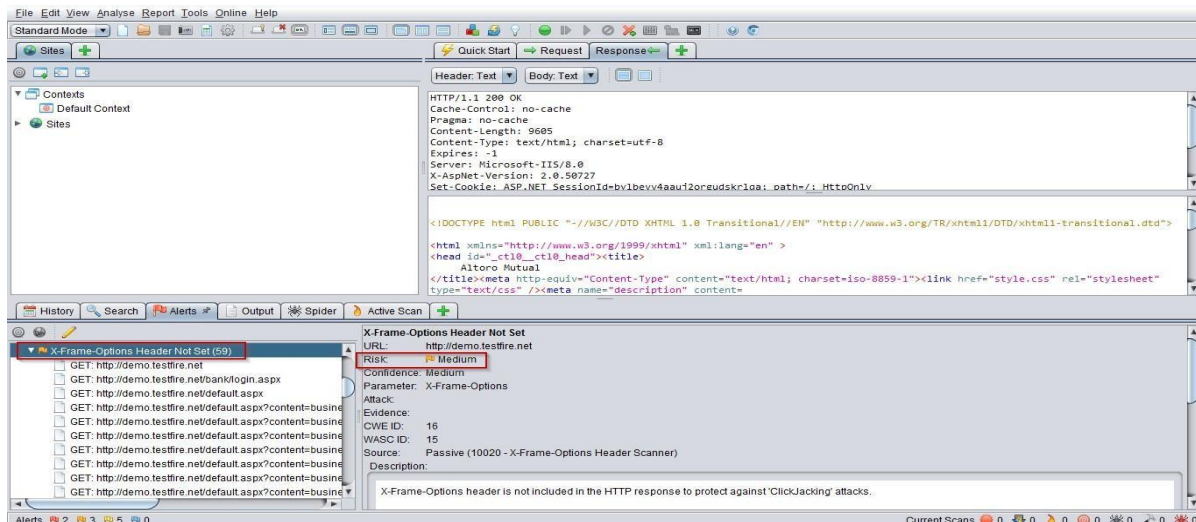
## Application Error Disclosure and Directory Browsing :

### Vulnerabilities that exists in Application Error Disclosure and Directory Browsing

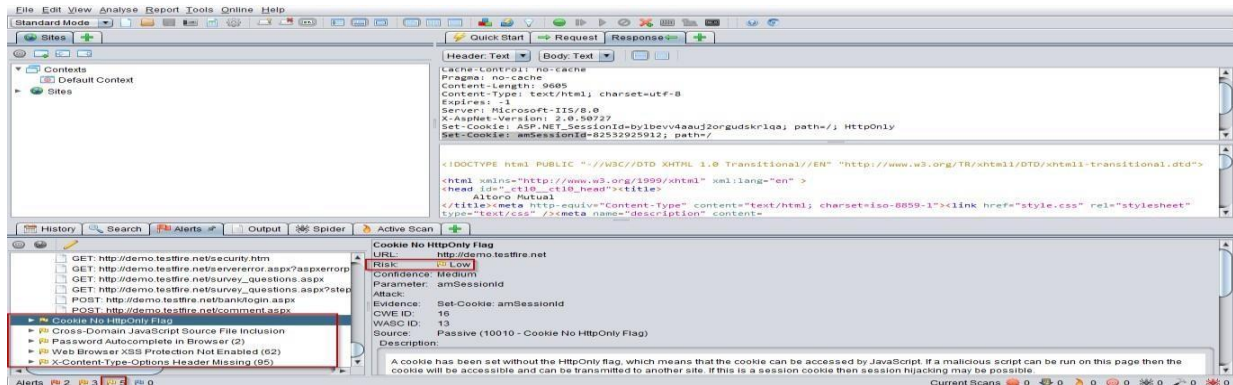


### X-Frame options header not set :

### Vulnerabilities that exists when X-Frame options headers are not set



Here we can see some Low Risks area:





## **PRACTICAL – 7**

**AIM :-** Implementation of it audit, malware analysis and vulnerability assessment and generate the report.

### **What is an it audit ?**

An it audit (**Information Technology**) audit is the examination and evaluation of an organization's information technology infrastructure, applications, data use and management, policies, procedures and operational processes against recognized standards or established policies.

### **What is vulnerability ?**

- A vulnerability is an exploitable gap in the security of your website, application, or network. It takes root from a bug and may result in a hack.
- A vulnerability may occur due to a misconfigured security patch, a gap in input validation, weak passwords, outdated software, or infected plugins among other things.
- If a vulnerability is exploited it can give the hacker privileged access. They can steal data, hijack your devices, or deny service. Either way, it ends in you losing business time, money, reputation, and reliability.

### **What is vulnerability assessment ?**

- A vulnerability assessment is a process of identifying, categorizing, and reporting security vulnerabilities that exist in your website, application, network, or devices. Usually, it is an automated procedure involving different types of vulnerability scanners.
- It helps your detect security risks like SQL injection, cross-site scripting, outdated security patches, broken access control, among other common vulnerabilities and exposures (CVEs).
- A vulnerability assessment tool is designed to test for the CVEs enlisted in security enhancement projects like OWASP top 10, and SANS top 25.
- However, the scope of vulnerability assessment is not limited to these enlistments.

### **What is the process of vulnerability assessment?**

Vulnerability assessment has a four-step process:



**Step 1.** The scope of the vulnerability assessment is determined by identifying the sensitive data storage areas, the systems running on a network, internet-facing assets, and devices.

**Step 2.** An automated vulnerability scanner is engaged to root out all the potential vulnerabilities in the systems within the scope of the assessment.

**Step 3.** A vulnerability assessment report is prepared with analytical information on the vulnerabilities found – the severity and risk score of the vulnerabilities, the possible ways to remove those issues, etc.

**Step 4.** The testee organization has to segregate the false positives from genuine issues, then fix the issues to strengthen their security.

### **What is a Vulnerability Assessment Report?**

A vulnerability assessment report is a document that records all the vulnerabilities found in your systems during a [vulnerability scan](#). The report provides you with a list of the vulnerabilities indexed by severity along with suggestions for fixing the vulnerabilities.

The vulnerability assessment report is basically the result of the vulnerability scan, and it is what helps you understand the security posture of your organization, and build a strategy for vulnerability management. Let us learn more about its importance.

### **Why is a vulnerability assessment report important?**

The primary goal of vulnerability assessment is to give the target organization a clear idea about the security loopholes present in their systems. The vulnerability assessment report is the medium of this information. The following are some specific advantages of a vulnerability scanning report.

**Efficient vulnerability management :-** The vulnerability report categorizes the vulnerabilities according to the risk posed by each of them. It helps a company prioritize the remediation of critical vulnerabilities. They can allocate the resources where it is needed the most, and thus get the most out of the process.

**Compliance management :-** The vulnerability assessment report helps a company identify the areas of security they have to spend on in order to gain compliance with relevant regulations.



**Building trust :-** A vulnerability report confirms how secure a company is. It helps them build trust among the customers.

**Reduce insurance premiums :-** A lot of companies insure their websites against cyber attacks. The insurance premiums are significantly less for companies that conduct regular vulnerability scans and have a positive report.

**Remediation of vulnerabilities :-** The vulnerability assessment report comes with suggestions on how to fix certain vulnerabilities. These suggestions work as guidelines for developers trying to fix the issues.

### **What are the components of a vulnerability assessment report?**

A vulnerability scan report is usually divided into 3 parts. An executive summary, the details of the vulnerabilities, and the details of the scan. Let us understand the significance of each segment.

**The executive summary :-** As the name would suggest, the executive summary is meant to create a high-level understanding of the vulnerability situation of an organization. This part talks about the vulnerabilities, their CVSS scores, the impact they could have on the business, and how much risk they pose to the system they're in.

**The details of vulnerabilities :-** This is the part where each of the detected vulnerabilities is explained with technical details along with suggestions for fixing them. This is the most important part of the vulnerability report from a developer's perspective because this part allows them to plan the remediation.

**Details of the scan :-** Vulnerability assessments involve hundreds of test cases. All these tests have to be documented in the report. This part tells you what tests were conducted, their categories, whether they were manually done or automated .





## **PRACTICAL – 8**

**AIM :-** Implementation of os hardening and ram dump analysis to collect the artifacts and other information.

However, what is really important to understand is that whatever works is always in the memory and whatever happens is always in the memory.

It is, therefore, fantastic to learn how to perform memory dumps in order to follow the incident response activities and also how to extract the information from the memory, so that we are able to get a little bit more insight about what was, or is, working in the operating system at that moment.

We are going to first learn how to perform a memory dump of the whole operating system's memory. Then, we are going to learn how to perform memory dumps of the system process and how to analyze both ways.

A memory dump is the process of taking all information content in RAM and writing it to a storage drive.

Developers commonly use memory dumps to gather diagnostic information at the time of a crash to help them troubleshoot issues and learn more about the event.

### **memory dump of the full operating system :- Steps :-**

1) Let's first perform the memory dump of the full operating system. For that, I am going to use the tool Dumpit. It is a tool developed by Matthieu Suiche.

### **Link to download dumpit tool :-**

<https://down10.software/download-dumpit/download/>

2)open cmd in administrator mode

3)go to the directory which we had downloaded the file as shown in the image

4) then click yes to start extracting of raw image.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>"C:\Users\91910\Downloads\CS>DumpIt.exe
'"C:\Users\91910\Downloads\CS>DumpIt.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>"C:\Users\91910\Downloads\CS.docx">DumpIt.exe

C:\Windows\system32>"C:\Users\91910\Downloads\CS.docx">DumpIt.exe

C:\Windows\system32>_
```

```
Administrator: Command Prompt
C:\WINDOWS\system32>CD C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CYBERSECURITY\LAB\EXPERIMENT 8\SOFTWARE
C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CYBERSECURITY\LAB\EXPERIMENT 8\SOFTWARE>LS
'LS' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CYBERSECURITY\LAB\EXPERIMENT 8\SOFTWARE>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\rajka\OneDrive\Documents\PARUL UNIVERSITY\3RD YEAR\5TH SEM\CYBERSECURITY\LAB\EXPERIMENT 8\SOFTWARE>DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      24423432192 bytes ( 23292 Mb)
Free space size:         69894062080 bytes ( 66656 Mb)
```

### memory dump of the process :-

- 1) open task manager
- 2) choose any one process as I had choosed windows explorer
- 3) right click on the process then create dump file
- 4) then the process will start executing and then it will start creating a dump file

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Status	71% CPU	39% Memory	1% Disk	0% Network
<b>Apps (5)</b>					
> Google Chrome (15)		0.1%	470.3 MB	0.1 MB/s	0 Mbps
> Microsoft Edge (10)		0.1%	287.1 MB	0 MB/s	0 Mbps
> Microsoft Word		0%	82.3 MB	0 MB/s	0 Mbps
> Task Manager		0.1%	25.8 MB	0 MB/s	0 Mbps
> Windows Explorer		1.0%	200.1 MB	0 MB/s	0 Mbps
<b>Background processes (86)</b>					
Adobe IPC Broker (32 bit)			1.3 MB	0 MB/s	0 Mbps
Antimalware Service Executable			0.5 MB	0 MB/s	0 Mbps
AppHelperCap.exe			2.1 MB	0 MB/s	0 Mbps
Application Frame Host			0.6 MB	0 MB/s	0 Mbps
Casting protocol connection list...			0.6 MB	0 MB/s	0 Mbps
CCXProcess (32 bit)			0.3 MB	0 MB/s	0 Mbps

Expand  
Restart  
End task  
Resource values  
Provide feedback  
Debug  
Create dump file  
Go to details  
Open file location  
Search online  
Properties

### To see more about the process :-

- 1) open task manager
- 2) choose any task which is running I had choosed Microsoft edge
- 3) Right click on the task then click on the go to details as shown in the image

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Status	70% CPU	41% Memory	2% Disk	0% Network
<b>Apps (5)</b>					
> Google Chrome (14)		0.2%	457.1 MB	0 MB/s	0 Mbps
> Microsoft Edge (10)		0%	294.0 MB	0 MB/s	0 Mbps
> Microsoft Word		0%	93.8 MB	0 MB/s	0 Mbps
> Task Manager		1.0%	34.7 MB	0 MB/s	0 Mbps
> Windows Explorer		0.2%	151.6 MB	0 MB/s	0 Mbps
<b>Background processes (86)</b>					
Adobe IPC Broker (32 bit)		0%	1.3 MB	0 MB/s	0 Mbps
Antimalware Service Executable		5.2%	162.1 MB	0 MB/s	0 Mbps
AppHelperCap.exe		0%	2.1 MB	0 MB/s	0 Mbps
Application Frame Host		0%	11.7 MB	0 MB/s	0 Mbps
Casting protocol connection list...		0%	1.6 MB	0 MB/s	0 Mbps
CCXProcess (32 bit)		0%	0.3 MB	0 MB/s	0 Mbps

Expand  
End task  
Resource values  
Provide feedback  
Debug  
Create dump file  
Go to details  
Open file location  
Search online  
Properties

Fewer details End task



Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (ac...	UAC virtualizati...
svchost.exe	12992	Running	SYSTEM	00	924 K	Not allowed
svchost.exe	12716	Running	rajka	00	2,160 K	Disabled
svchost.exe	13020	Running	rajka	00	3,696 K	Disabled
svchost.exe	10960	Running	SYSTEM	00	1,932 K	Not allowed
svchost.exe	8464	Running	SYSTEM	00	1,488 K	Not allowed
svchost.exe	12680	Running	LOCAL SER...	00	824 K	Not allowed
svchost.exe	12456	Running	SYSTEM	00	908 K	Not allowed
SysInfoCap.exe	2412	Running	SYSTEM	00	3,048 K	Not allowed
System	4	Running	SYSTEM	00	20 K	
System Idle Process	0	Running	SYSTEM	67	8 K	
System interrupts	-	Running	SYSTEM	01	0 K	
SystemSettings.exe	10024	Suspended	rajka	00	0 K	Disabled
taskhostw.exe	11196	Running	rajka	00	3,492 K	Disabled
taskhostw.exe	11148	Running	rajka	00	820 K	Disabled
Taskmgr.exe	11792	Running	rajka	00	32,468 K	Not allowed
TextInputHost.exe	7024	Running	rajka	00	10,532 K	Disabled
TouchpointAnalyticsC...	2640	Running	SYSTEM	00	26,492 K	Not allowed
unsecapp.exe	5112	Running	SYSTEM	00	1,100 K	Not allowed
UserOOBEBroker.exe	2664	Running	rajka	00	908 K	Disabled
wininit.exe	952	Running	SYSTEM	00	1,004 K	Not allowed
winlogon.exe	13220	Running	SYSTEM	00	1,296 K	Not allowed
WINWORD.EXE	11404	Running	rajka	00	96,072 K	Disabled
WmiPrvSE.exe	6008	Running	SYSTEM	00	1,744 K	Not allowed

⏮ Fewer details

End task



## **PRACTICAL – 9**

**AIM :-** Implementation of mobile audit and generate the report of the existing artifacts.

### **Why mobile app security audit ?**

A single Data Breach can ruin your customer's trust in your company forever.

Any successful cybersecurity breach can crumble your entire company and destroy your market reputation.

Hackers are interested in information such as email addresses, phone numbers, account numbers, etc. If a hacker can access this information through your Mobile App (which is the case mostly), it invariably becomes a hot target.

A good security audit can help simulate real-life attacks that your Mobile App may face. It eventually improves the security and integrity of your app.

### **Who is Mobile Audit for ?**

Mobile Audit focuses not only in the security testing and defensive use cases, the goal of the project is to become a complete homologation for Android APKs, which includes:

**Static Analysis (SAST) :-** It will perform a full decompilation of the APK and extract all the possible information of it. It reports the different vulnerabilities and findings in the source code grouped by different categories. Also, it has full support on finding triage (change status and criticality).

**Malware Analysis :-** finds dangerous permissions and suspicious code.

**Best Practices of Secure Android Coding :-** tells developers in which parts of the code they are coding securely and where they are not.

### **It is aimed to different user profiles :-**

- Developers
- System Administrators
- Security Engineers

**In each of the scans, it would have the following information :-**



- Application Info
- Security Info
- Components
- SAST Findings
- Best Practices Implemented
- Virus Total Info
- Certificate Info
- Strings
- Databases
- Files

Mobile Audit

HomeFindingsCreateOthers

BACKREFRESH

Scan

Description: V2.2


Created by: monica

Status: Finding vulnerabilities

40%

DELETEEXPORT

Application info

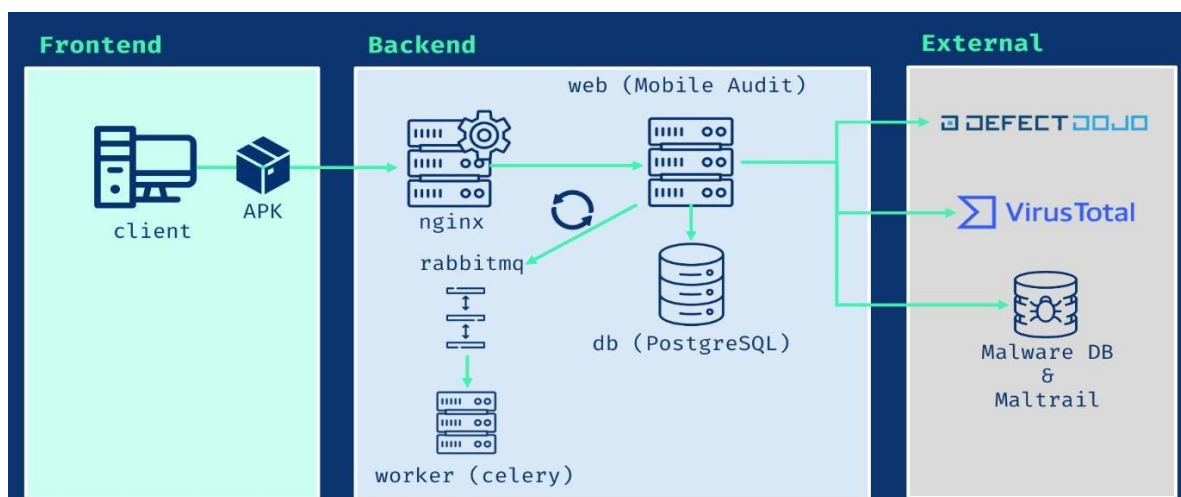
Icon	
App name	InsecureBankv2
Package	com.android.insecurebankv2
Version name	1.0
Version code	1
Min version	15
Max version	None
Target version	22
Effective version	22
File size	3462429
md5	5ee4829c65640f9c936ac861d1650ffc



Mobile Audit				
sha256				b18af
ssdeep				98304
Harmless				2
Malicious				1
Antivirus				
Antivirus	Version	Category	Result	
Avast	1.3.0.9899	failure	None	
Elastic	4.0.17	type-unsupported	None	
ClamAV	0.103.1.0	undetected	None	
CMC	2.10.2019.1	undetected	None	
CAT-QuickHeal	14.00	malicious	Android.Obfus.GEN41318	

## Main features

- ✓ Uses Docker for easy deployment in multiplatform environment
- ✓ Extract all information of the APK





- ☒ Analyze all the source code searching for weaknesses
- ☒ All findings are categorized and follows CWE standards
- ☒ Also highlight the Best Practices in Secure Android Implementation in the APK
- ☒ The findings can be edited and the false positives can be triaged and deleted
- ☒ All scan results can be exported to PDF
- ☒ User authentication and user management
- ☒ API v1 with Swagger and ReDoc
- ☒ TLS
- ☒ Dynamic page reload (WIP)
- ☐ Export to Markdown
- ☐ Export to CSV
- ☐ LDAP integration



## **PRACTICAL – 10**

**AIM :-** Implementation of cyber forensics tools for disk imaging, data acquisition, data extraction and data analysis and recovery.

### **Disk imaging :-**

**Disk imaging as defined by Jim Bates, Technical Director of Computer Forensics Ltd, refers to :-**

“An image of the whole disk was copied. This was regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image.”

Disk imaging is also one of the approaches for backup except that backup only copies the active file. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and file slack.

### **Data acquisition :-**

Data acquisition is the process of sampling signals that measure real-world physical conditions and converting the resulting samples into digital numeric values that can be manipulated by a computer. Data acquisition systems, abbreviated by the acronyms *DAS*, *DAQ*, or *DAU*, typically convert analog waveforms into digital values for processing.

**The components of data acquisition systems include :-**

- Sensors, to convert physical parameters to electrical signals.
- Signal conditioning circuitry, to convert sensor signals into a form that can be converted to digital values.
- Analog-to-digital converters, to convert conditioned sensor signals to digital values.

### **Data extraction :-**

Data extraction is the process of collecting or retrieving disparate types of data from a variety of sources, many of which may be poorly organized or completely unstructured. [Data](#)



extraction makes it possible to consolidate, process, and refine data so that it can be stored in a centralized location in order to be transformed. These locations may be on-site, cloud-based, or a hybrid of the two.

Data extraction is the first step in both ETL (extract, transform, load) and ELT (extract, load, transform) processes. ETL/ELT are themselves part of a complete data integration strategy.

### **Data Extraction and ETL :-**

To put the importance of data extraction in context, it's helpful to briefly consider the ETL process as a whole. In essence, ETL allows companies and organizations to

- 1) consolidate data from different sources into a centralized location and
- 2) assimilate different types of data into a common format.

### **There are three steps in the ETL process :-**

**Extraction :-** Data is taken from one or more sources or systems. The extraction locates and identifies relevant data, then prepares it for processing or transformation. Extraction allows many different kinds of data to be combined and ultimately mined for business intelligence.

**Transformation :-** Once the data has been successfully extracted, it is ready to be refined. During the transformation phase, data is sorted, organized, and cleansed. For example, duplicate entries will be deleted, missing values removed or enriched, and audits will be performed to produce data that is reliable, consistent, and usable.

**Loading :-** The transformed, high quality data is then delivered to a single, unified target location for storage and analysis.

### **Data analysis :-**

Data analysis is a process of inspecting, cleansing, transforming, and modelling data with the goal of discovering useful information, informing conclusions, and supporting decision- making.

Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, and is used in different business, science, and social science domains.

In today's business world, data analysis plays a role in making decisions more scientific and helping businesses operate more effectively.



### **Data recovery :-**

In computing, data recovery is a process of salvaging deleted, inaccessible, lost, corrupted, damaged, or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a usual way.

The data is most often salvaged from storage media such as internal or external hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices. Recovery may be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

Data recovery can be a very simple or technical challenge. This is why there are specific software companies specialized in this field.