CYBER SECURITY TECHNOLOGY

DOCUMENTATION

NAME: G.J.INDHUMATHI

CLASS: B.Sc., Information Technology

REGISTER NUMBER: CB 20S305315

DEPARTMENTOF COMPUTER SCIENCE, IT &
COMPUTER APPLICATIONS

SHRIMATI INDIRA GANDHI COLLEGE

(Nationally Accredited at “A” Grade (3rd Cycle) by NAAC)

TIRUCHIRAPPALLI – 620 002.

Nmap

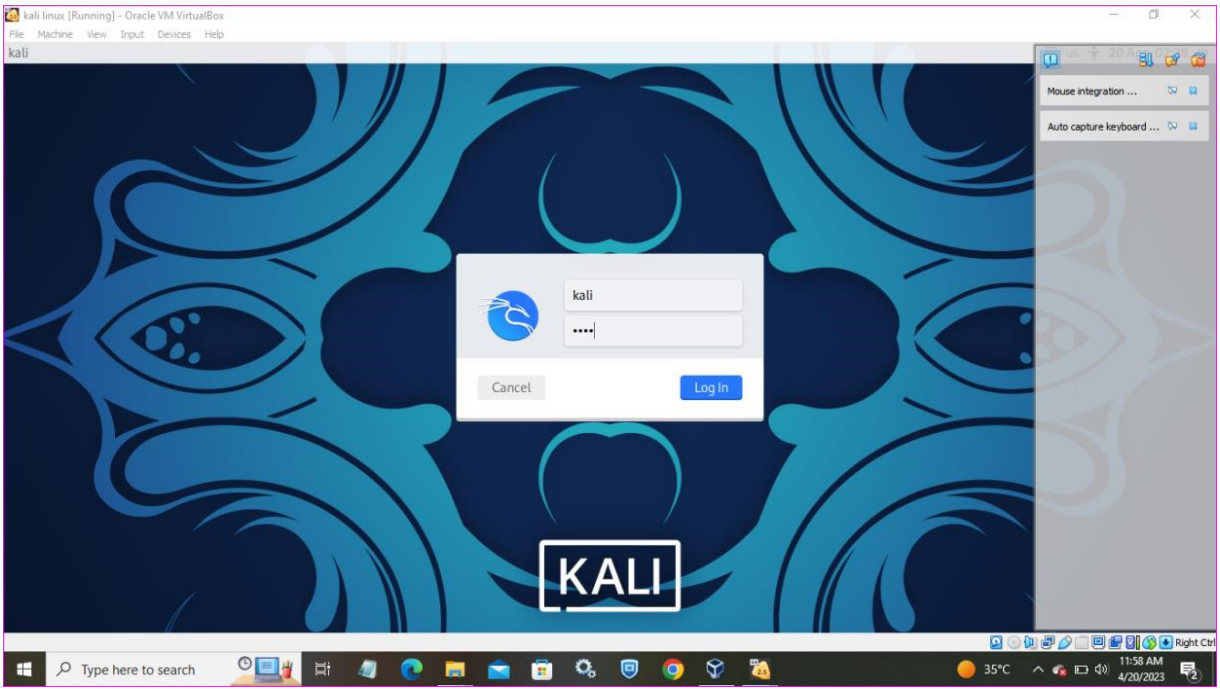
Aim:

To create cyber security program for scanning the web vulnerabilities using Nmap tool.

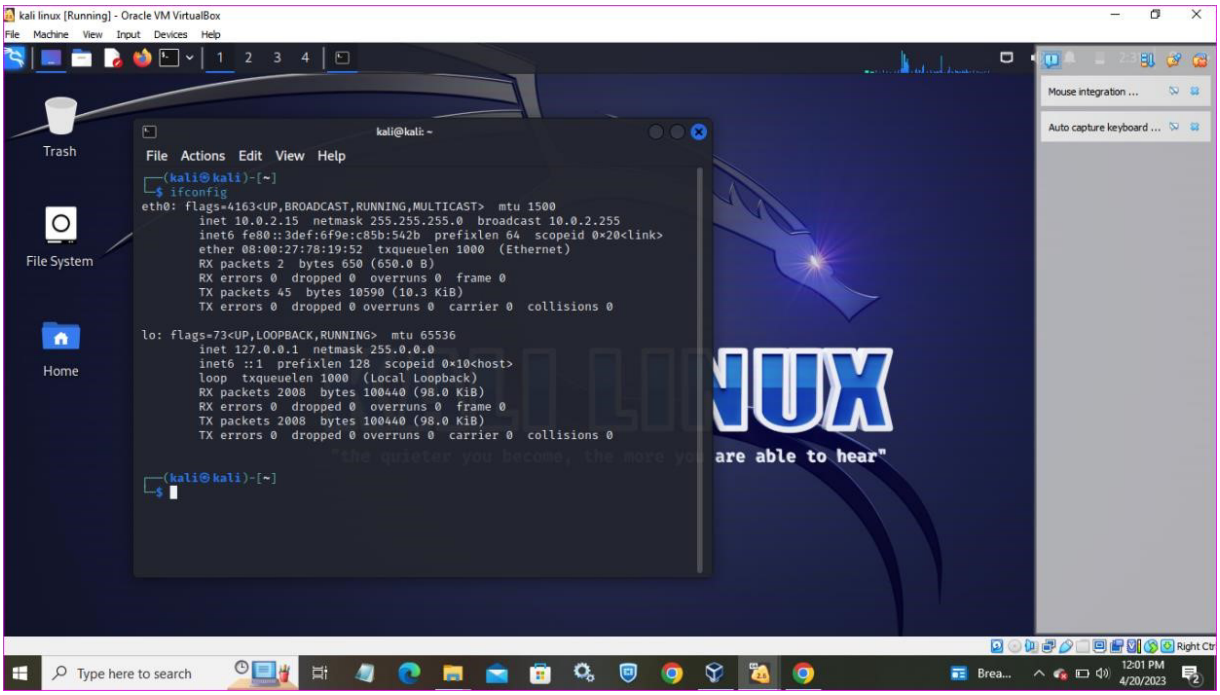
Procedure:

Step 1: Start the program.

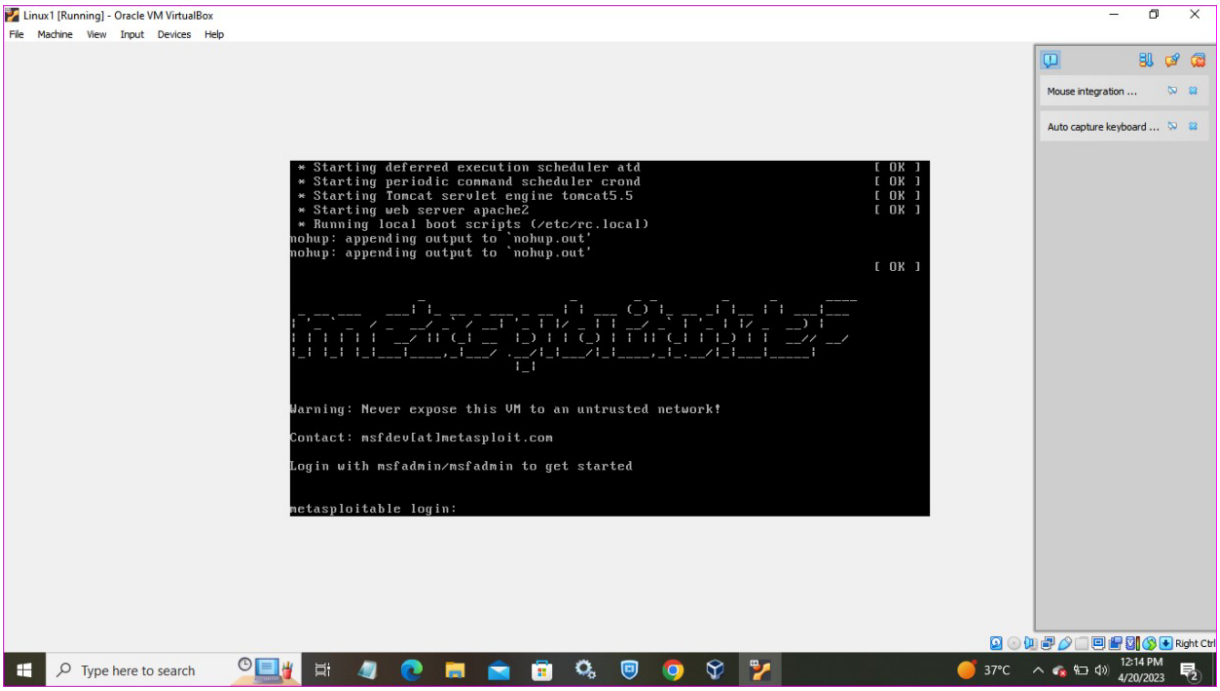
Step 2: Open kali linux using virtual box.



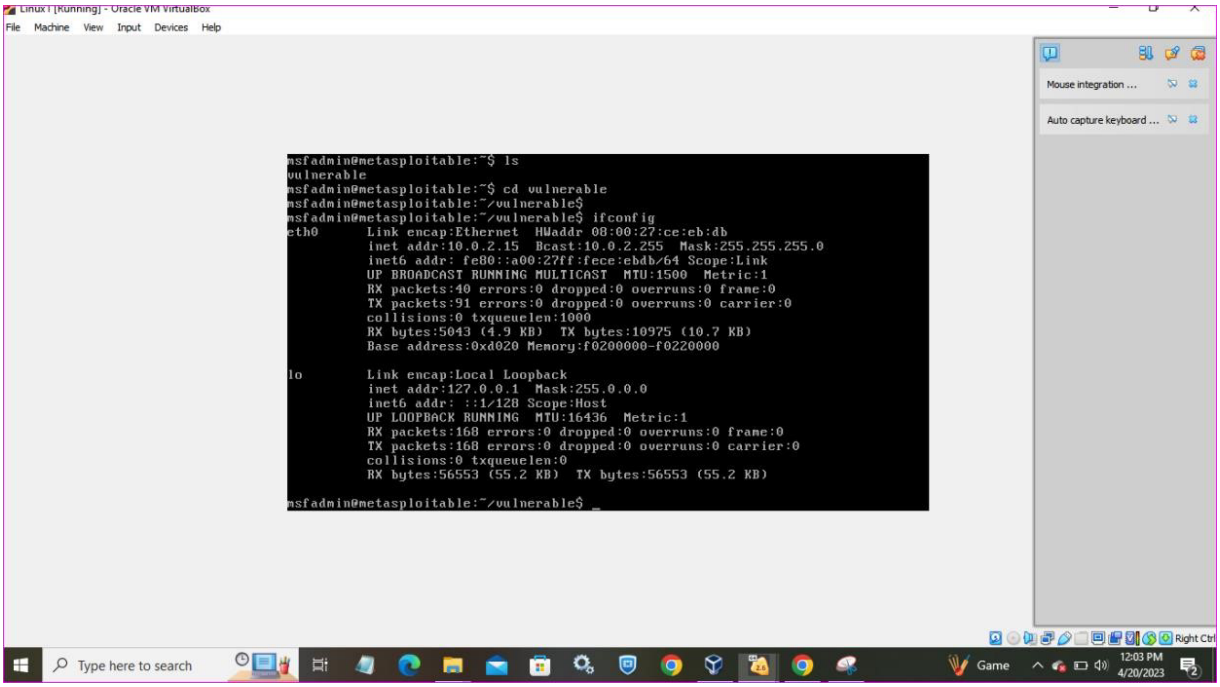
Step 3: Open kali linux terminal and add ifconfig command to find the ip address of our system.



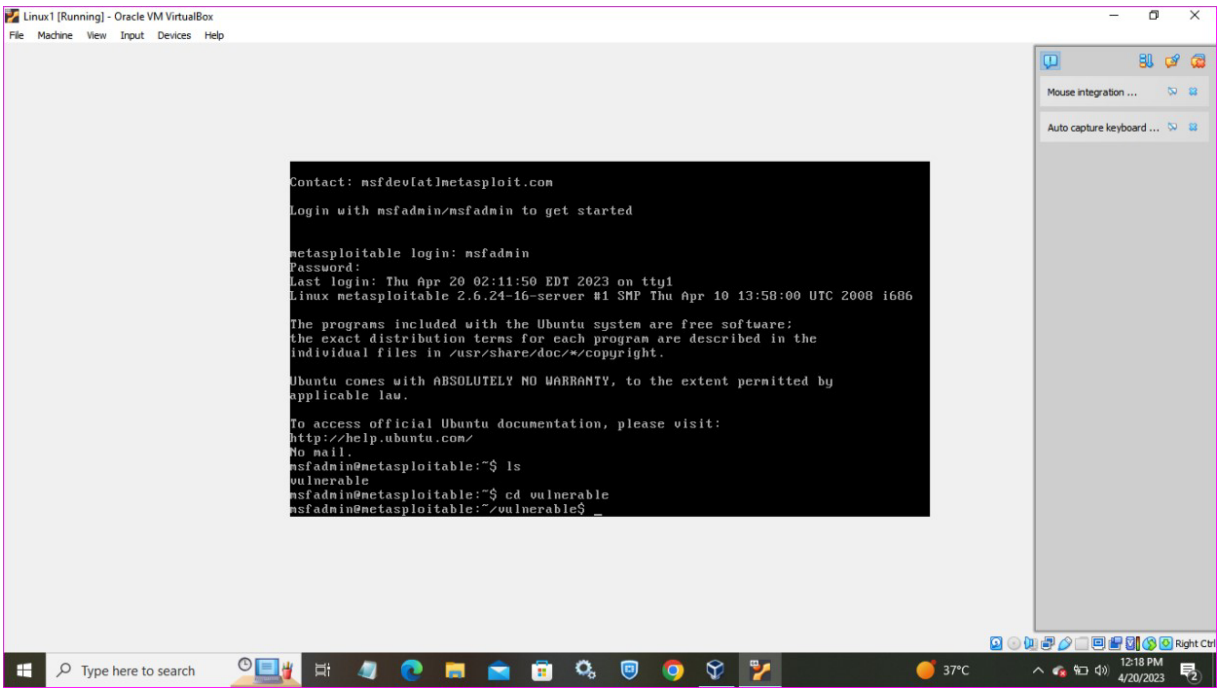
Step 4: Install metasploitable reaname as Linux in our pc.



Step 5: login to metasploitable using the command msfadmin.

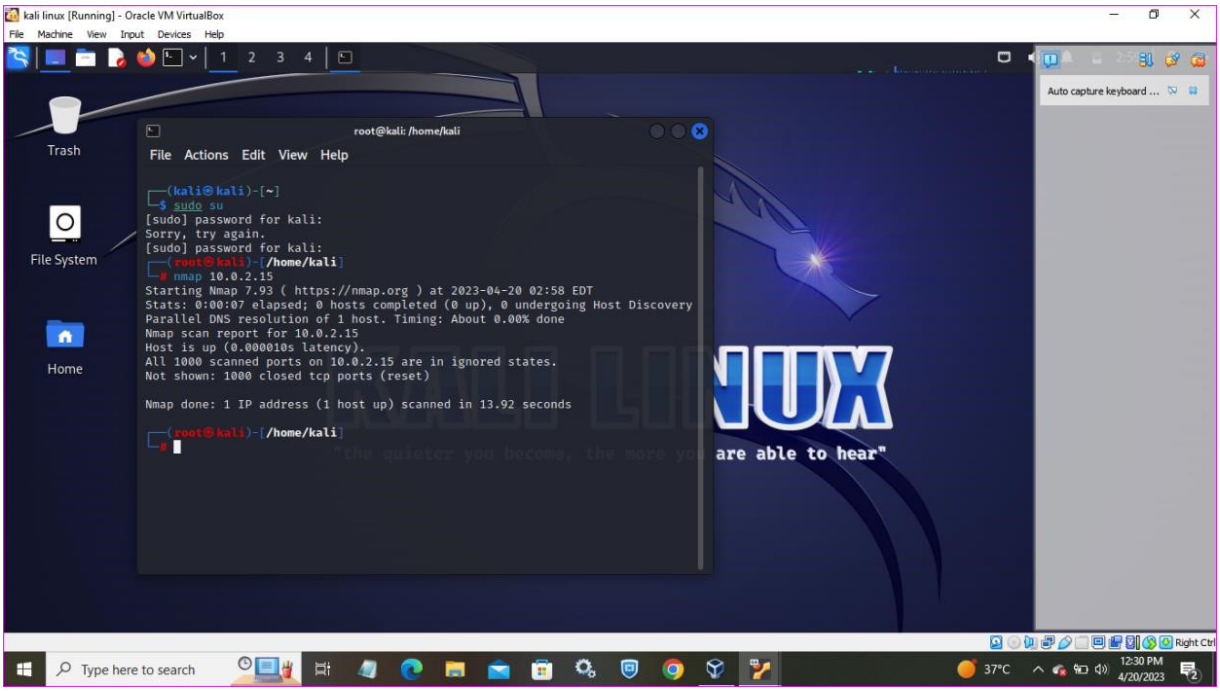


Step 6: Insert the ls and cd command for the list and change directory.

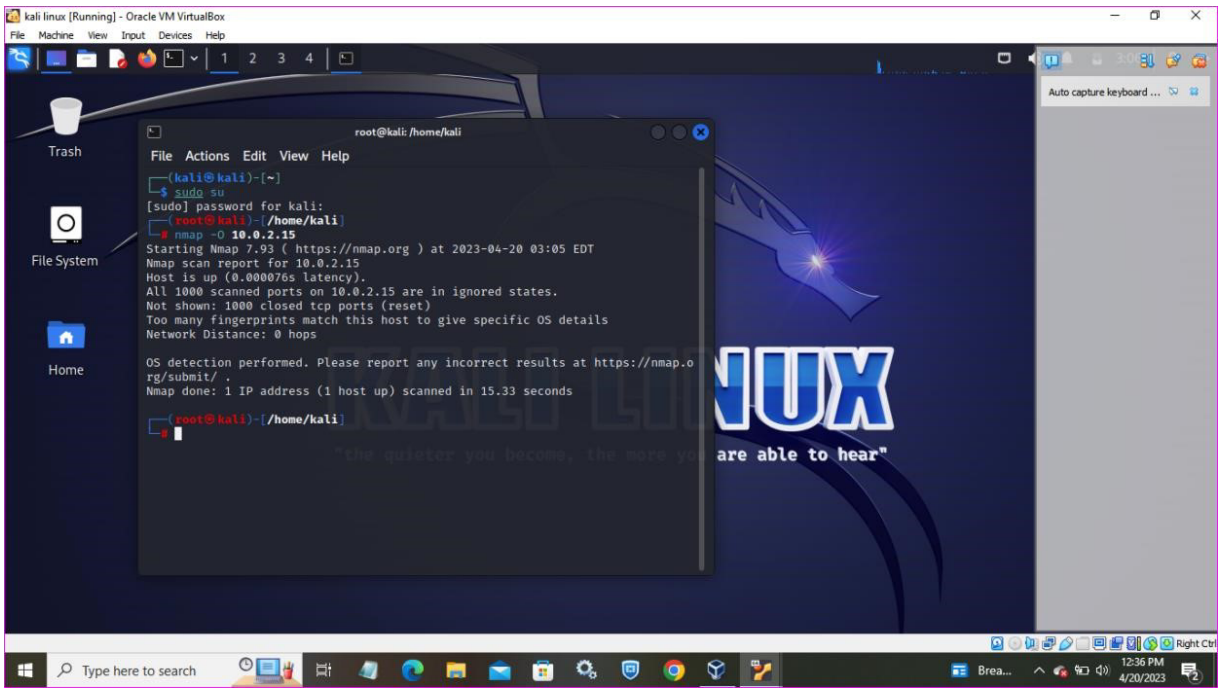


Step 7: Open kali linux terminal enter with sudo su command.

Step 8: Write nmap and IP address of Linux enter to run the command now we find the ports of another system find the vulnerabilities.



Step 9: Write another command nmap -O IP address of linux to find the operating systems for scan vulnerabilities.



Step 10: Stop the execution.

Result:

Thus the vulnerabitlities was scanned using the nmap tool.

Wire Shark

Aim:

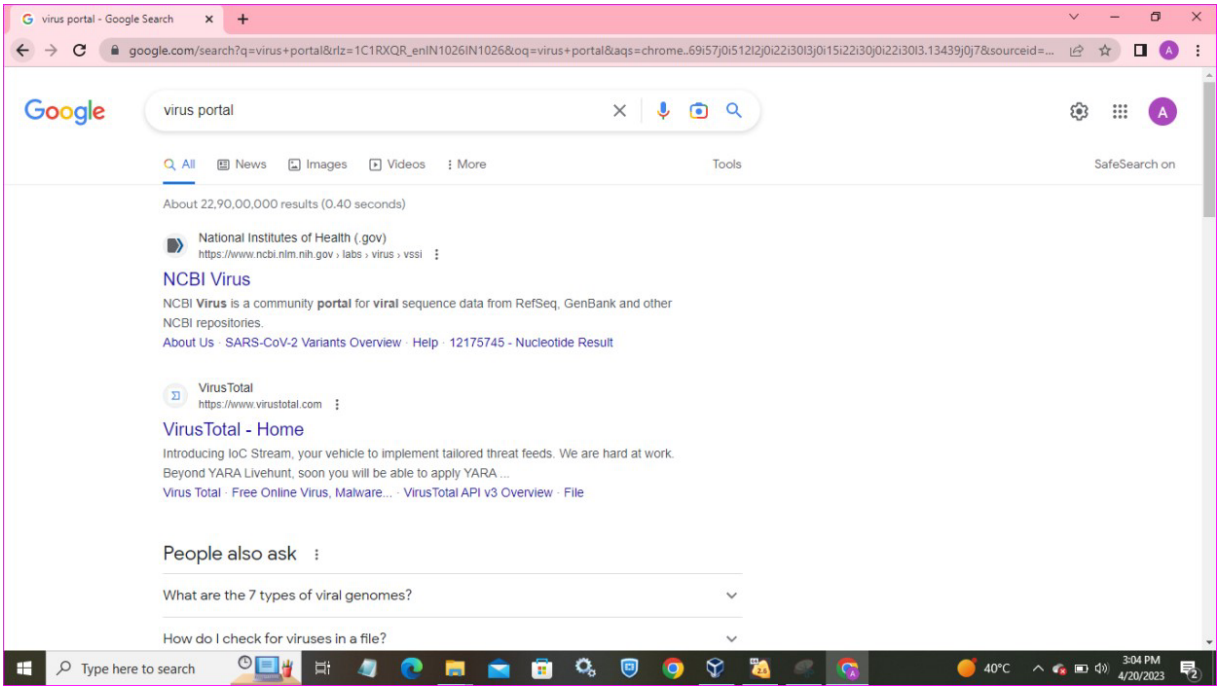
To write cyber security program for analyze the packets with help of the wire shark tool.

Procedure:

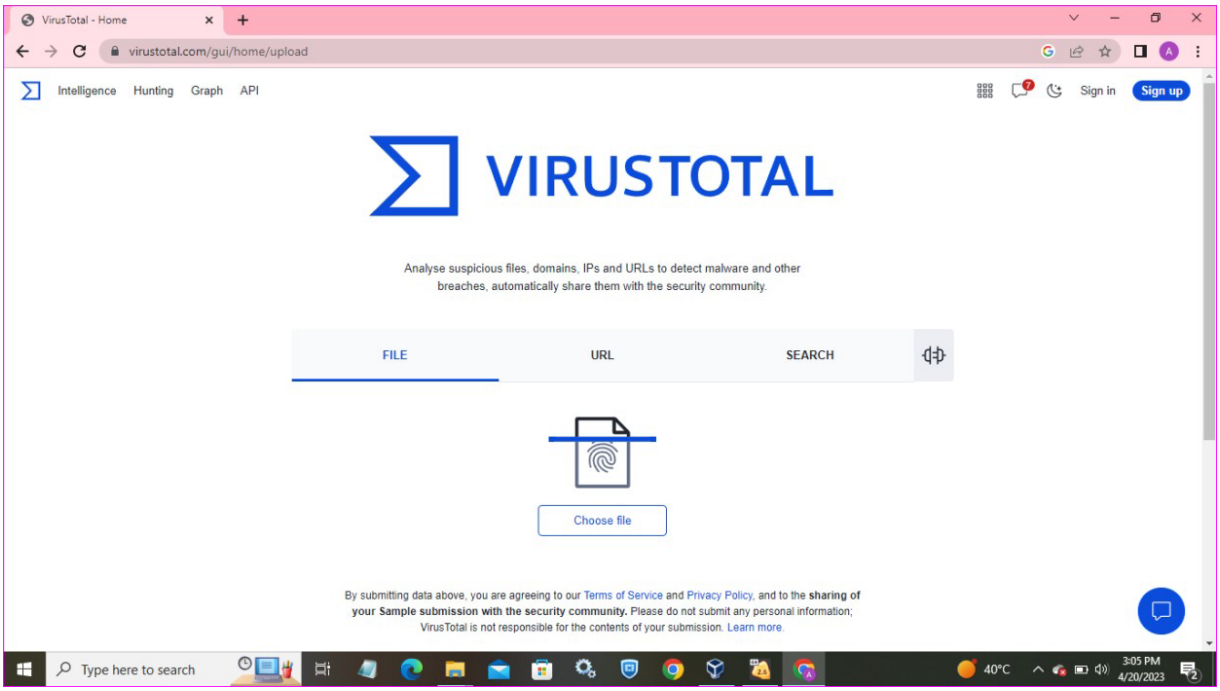
Step 1: Start the program.

Step 2: Install wire shark it contain all the information about the packet. Create as file.

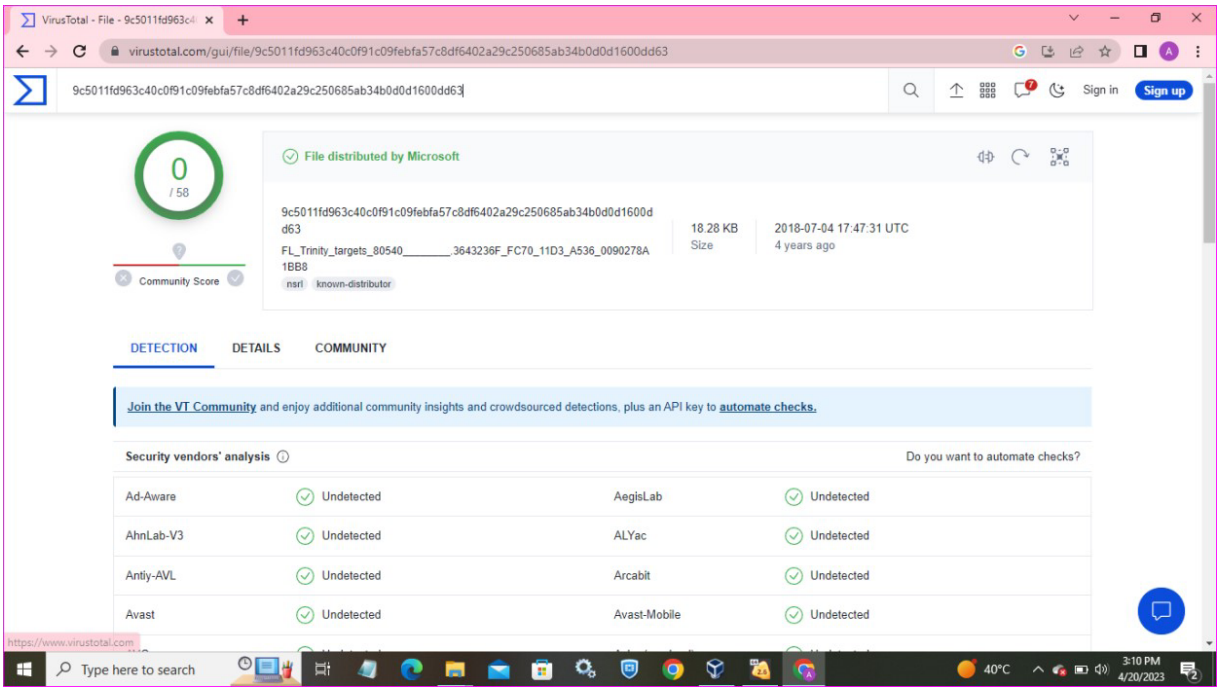
Step 3: Open the browser install Virus portal.



Step 4: Open the Virus portal and choose a file from our folders.



Step 5: Virus portal detect the malwares of chose file.



Step 6: Stop the program.

Result:

Thus the cyber security program was processed and the packets were analyzed with help of wire shark tool.

Dos attack

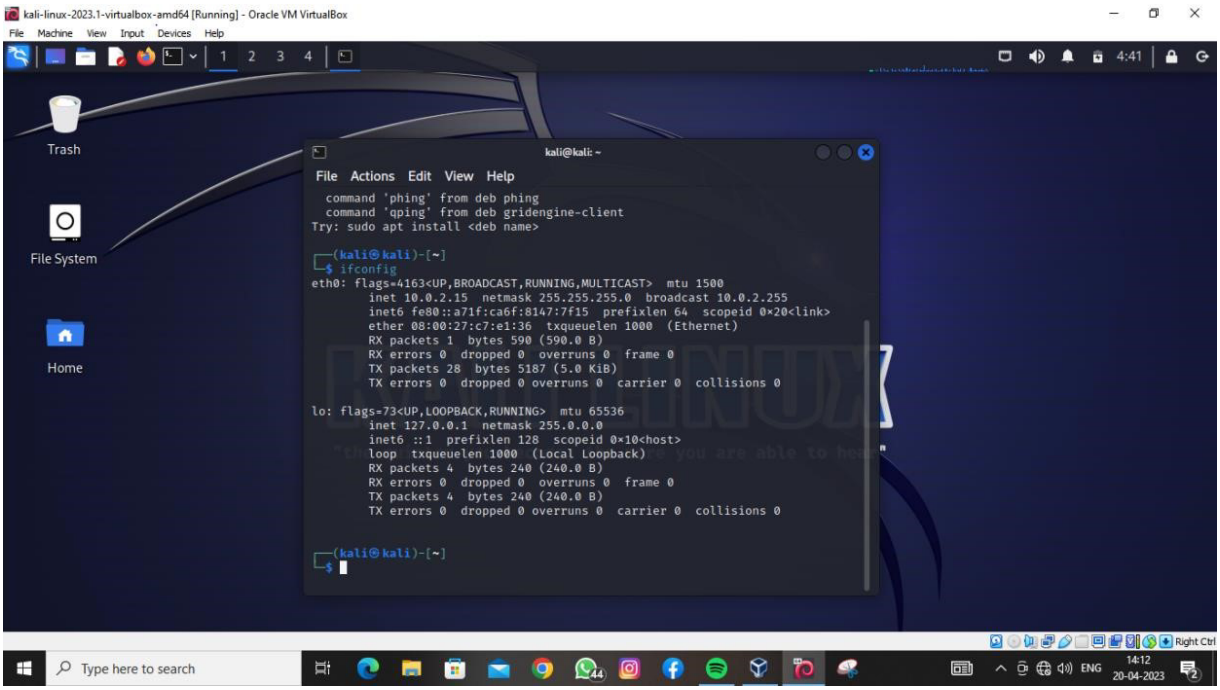
Aim:

To attack the server without access the internet using the tool iping.

Procedure:

Step 1: Start the program.

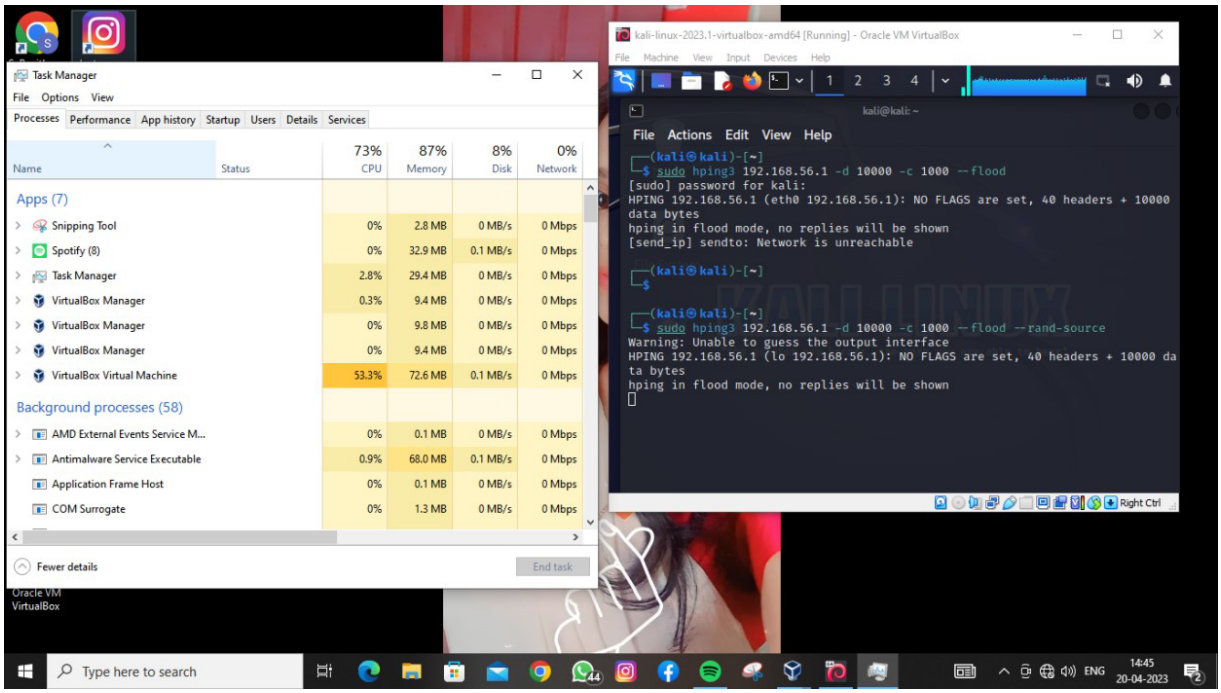
Step 2: Open kali linux terminal write if config command to find the ip address.



Step 3: Open windows and open command prompt and write the command ip config to find the ip address of the system.

Step 4: Switch to kali linux and open terminal write the command sudo hping3 ip address of target system –d 10000 –c 1000 it crash our target system few seconds and cancel the process.

Step 5: Again go to terminal write command sudo hping3 ip of target system –d 10000 –c 1000 --flood it also crash our system few seconds.



Step 6: check usage of the CPU.

Step 7: Stop the process.

Result:

Thus the server was attacked using iping tool without using internet.

MITM Attack

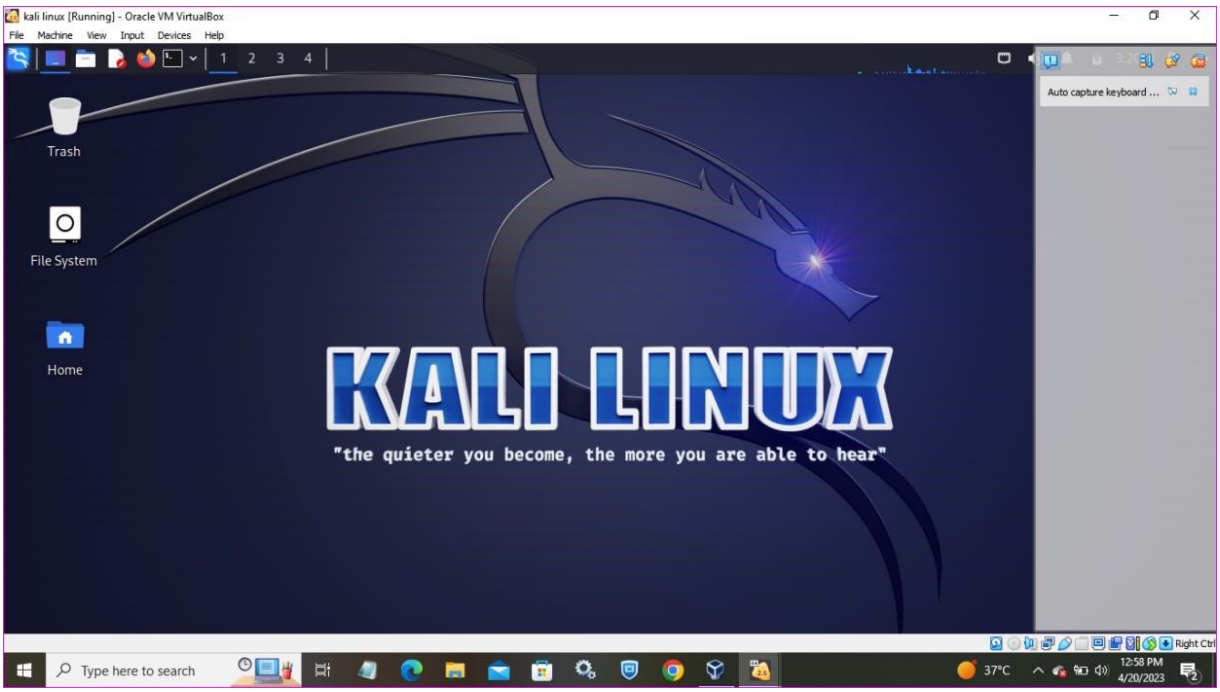
Aim:

To sniff the user login using ARP poisioning and the ettercap tool.

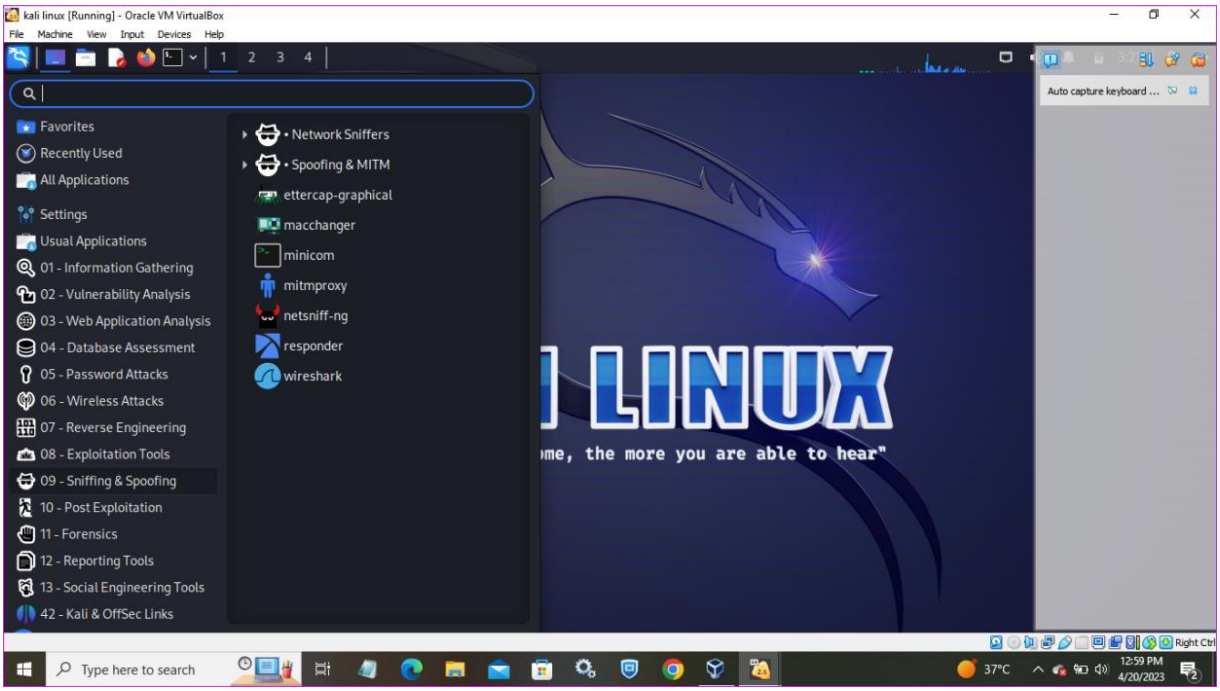
Procedure:

Step 1: Start the program.

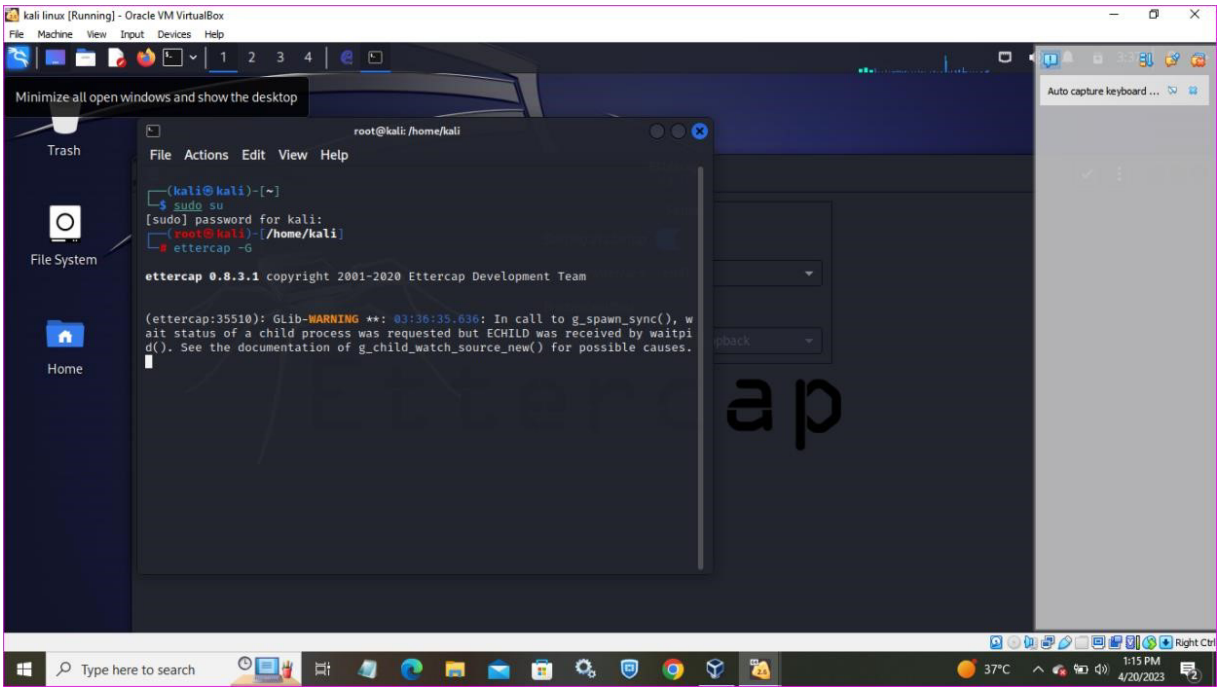
Step 2: Open kali linux.



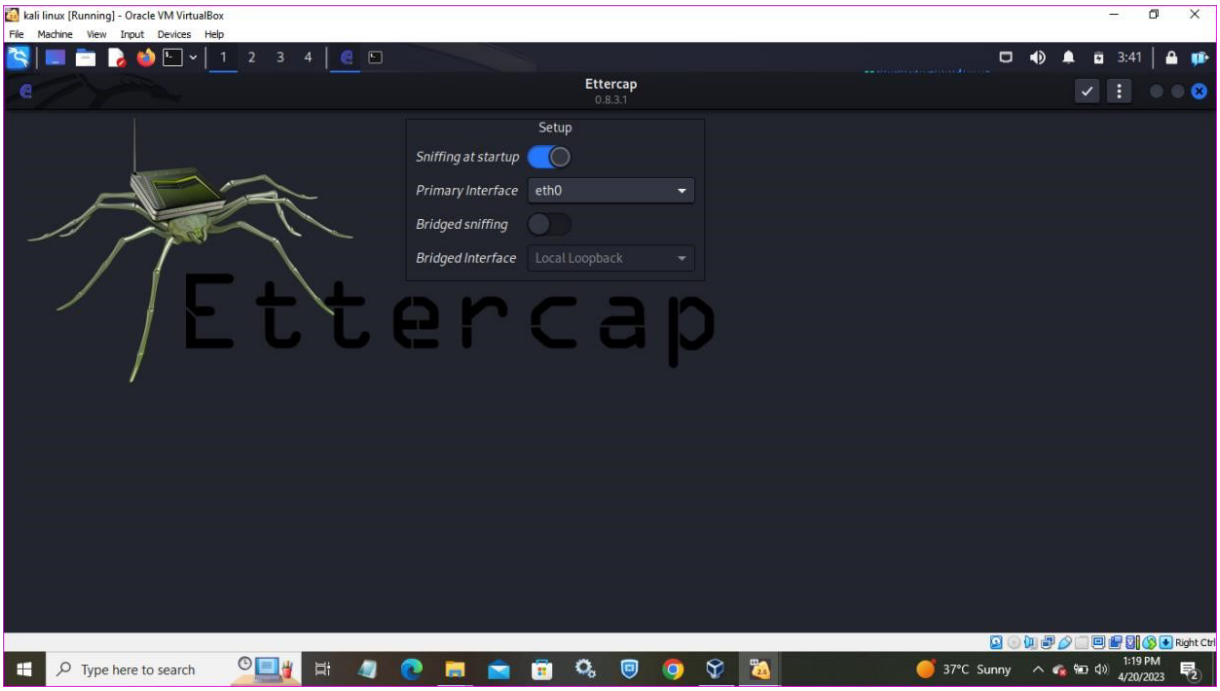
Step 3: Click the sniffing and spoofing to open the etter cap.



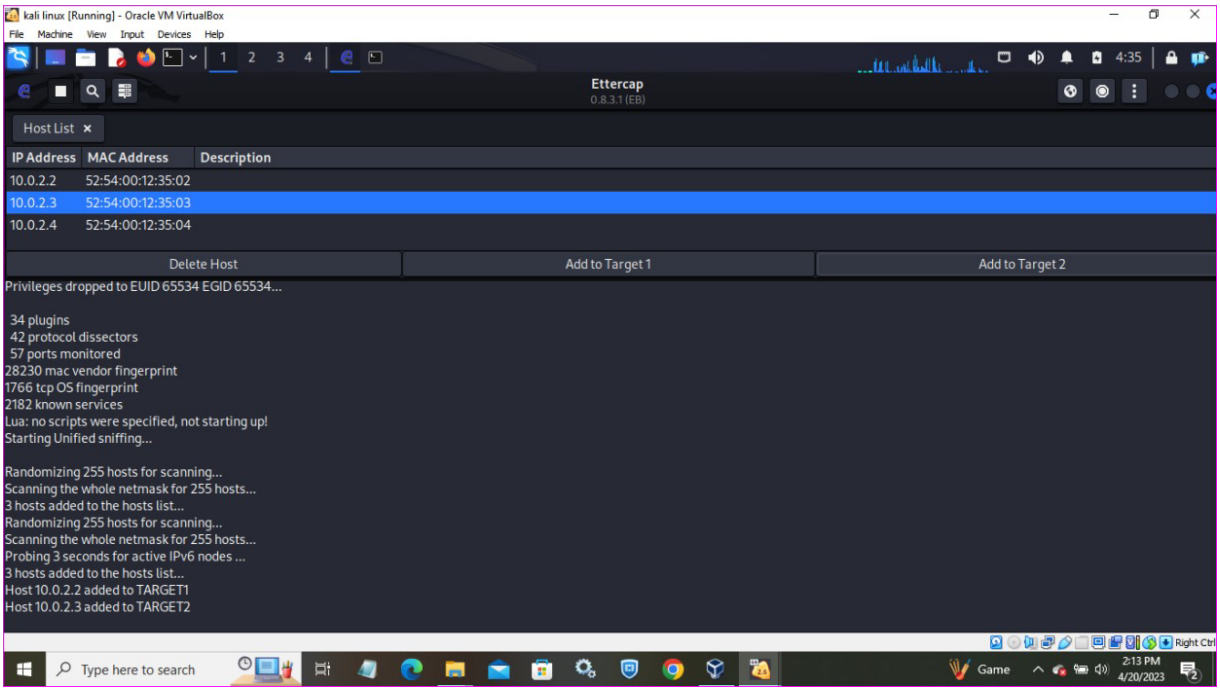
Step 4: Open the terminal and write the command sudo su for log in and write ettercap –G.



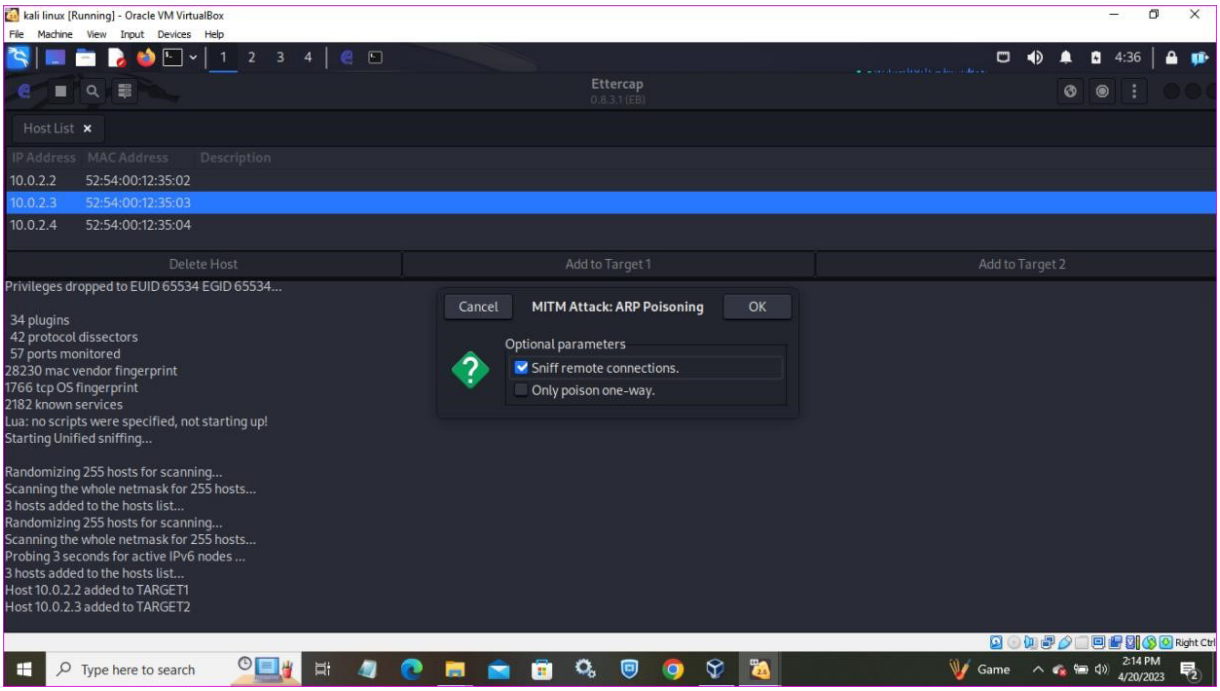
Step 5: Open Ettercap and start and setup the tool.



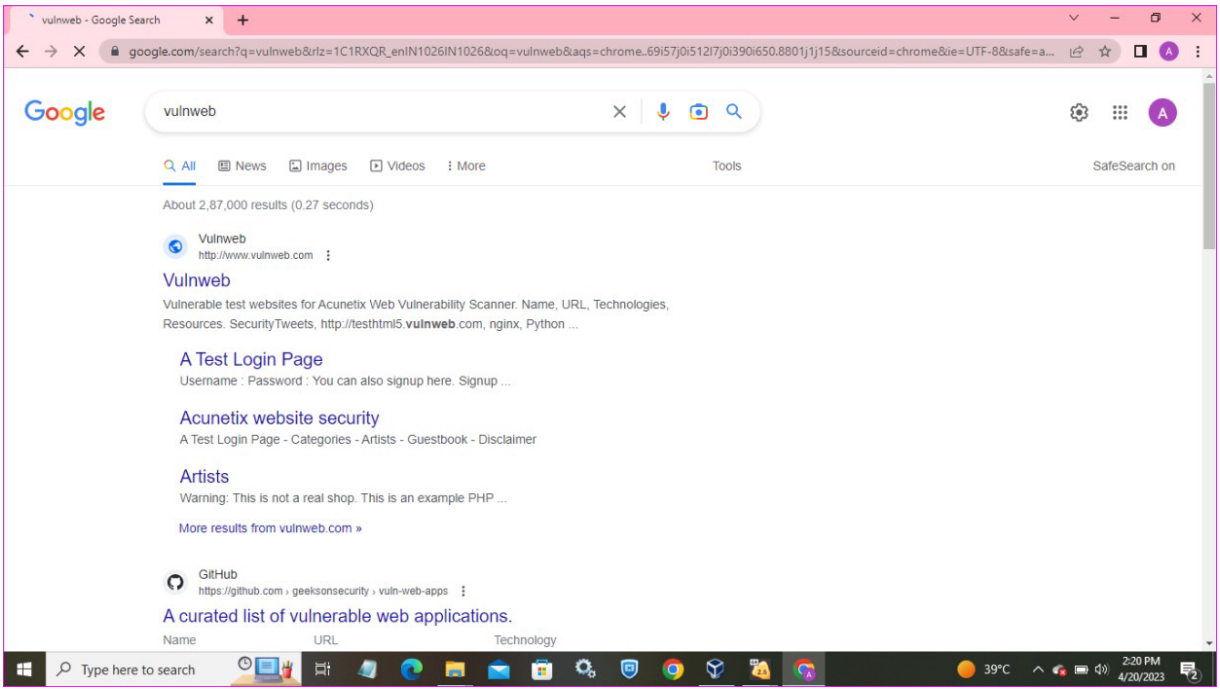
Step 6: After open the ettercap tool search the host list and fixing the target.



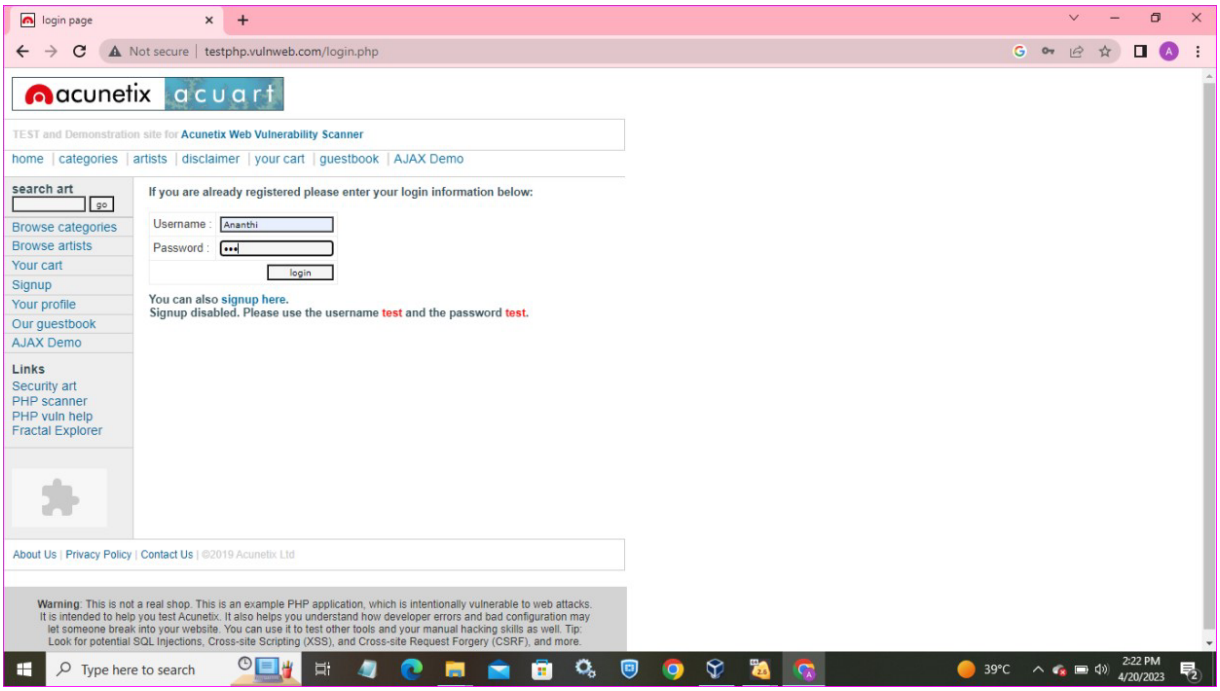
Step 7: Add ARP poisioning.



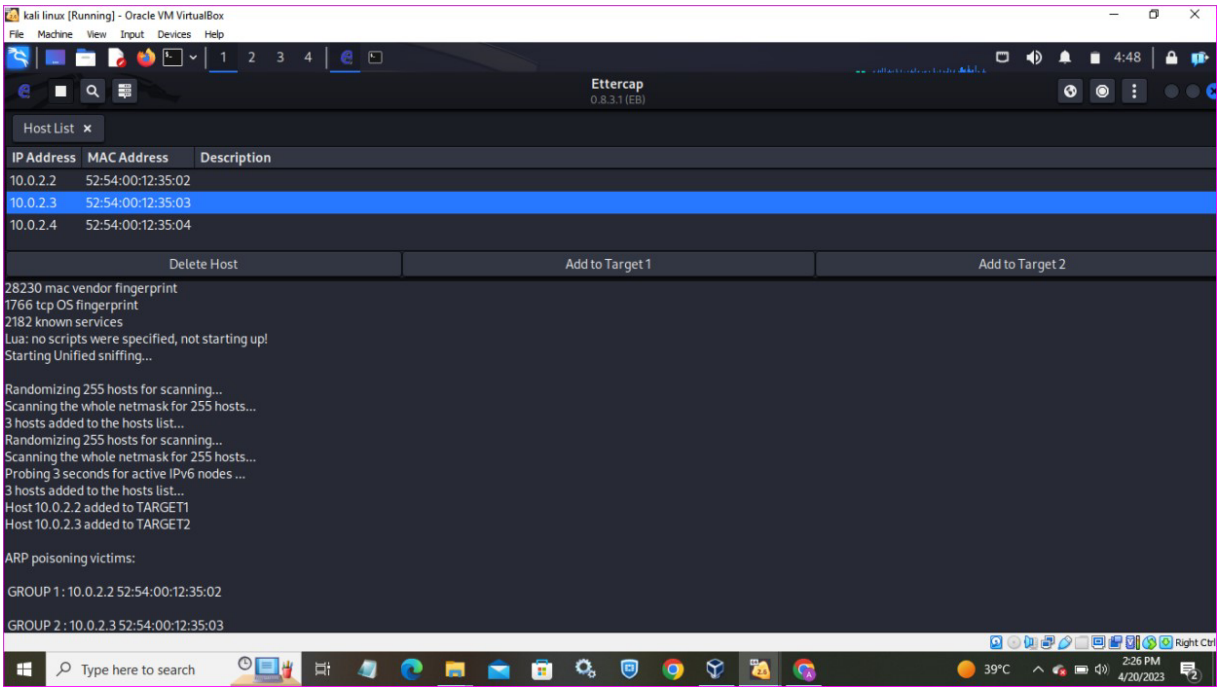
Step 8: Install the vulnweb using Google chrome.



Step 9: To enter login and password.



Step 10: Switch to ettercap tool now the ettercap find the user name and password which is used in vulnweb.



Step 11: Stop the program.

Result:

Thus the user id and password was sniffed using the tool ettercap.

Maltrail

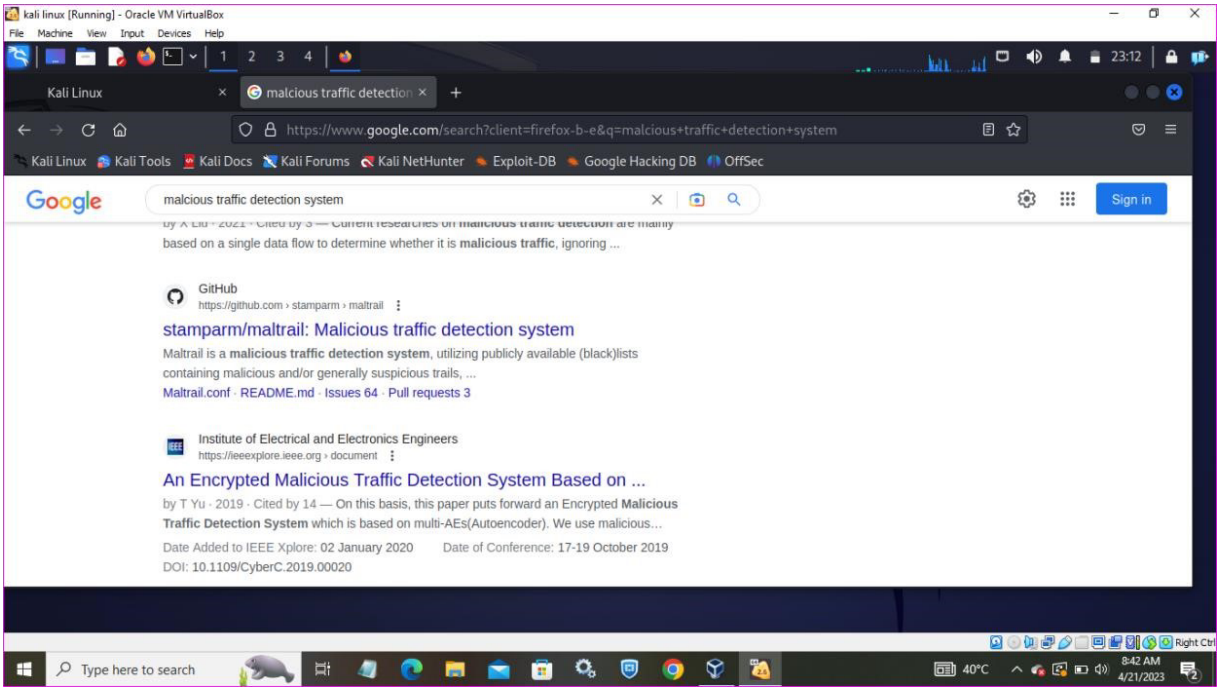
Aim:

To find the malware using the malicious traffic detection system.

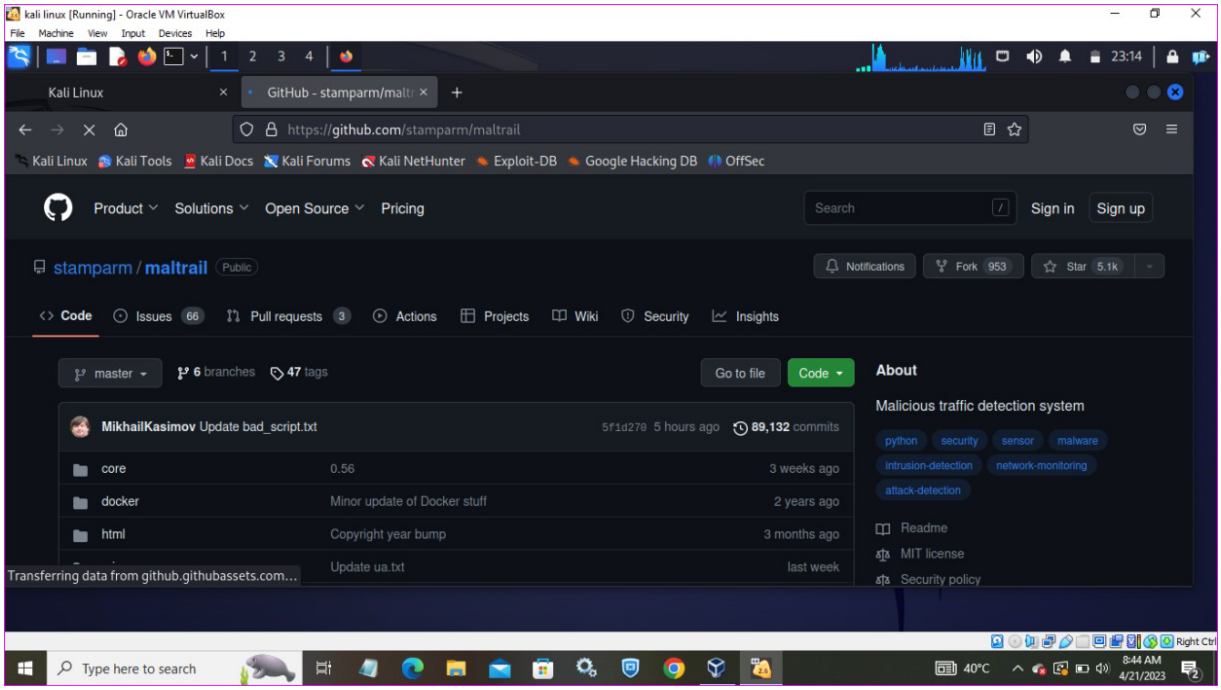
Procedure:

Step 1:Start the program.

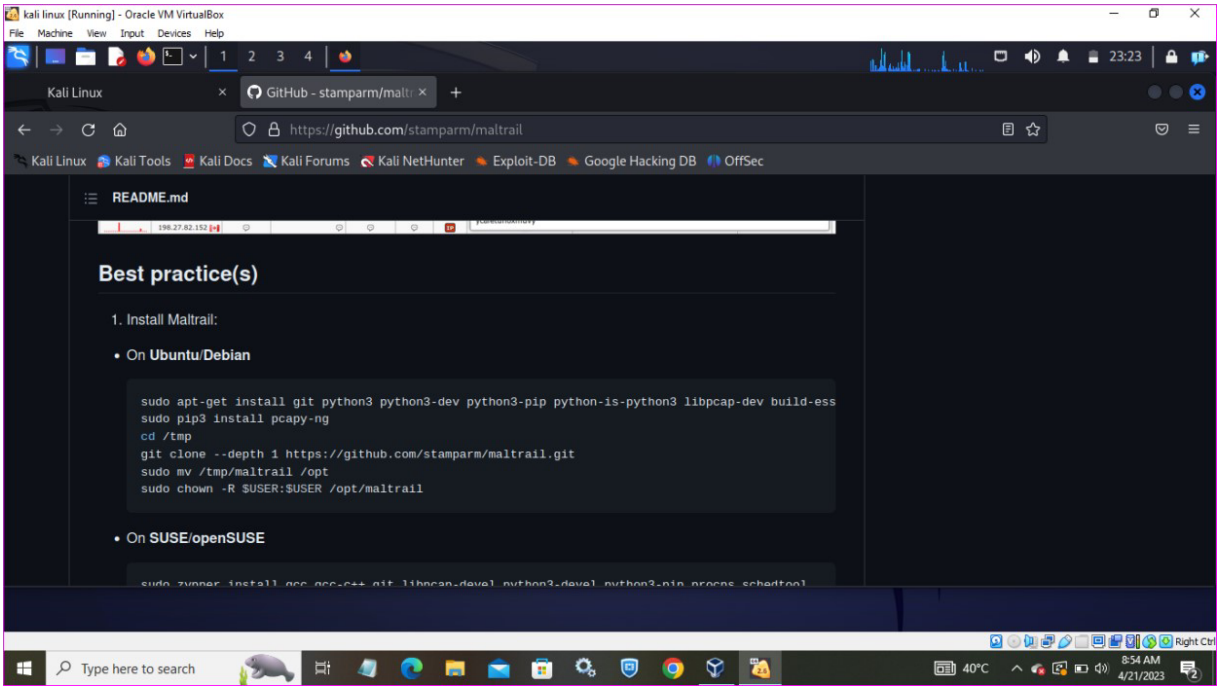
Step 2: Install Mantrail using fire fox browser in kali linux.



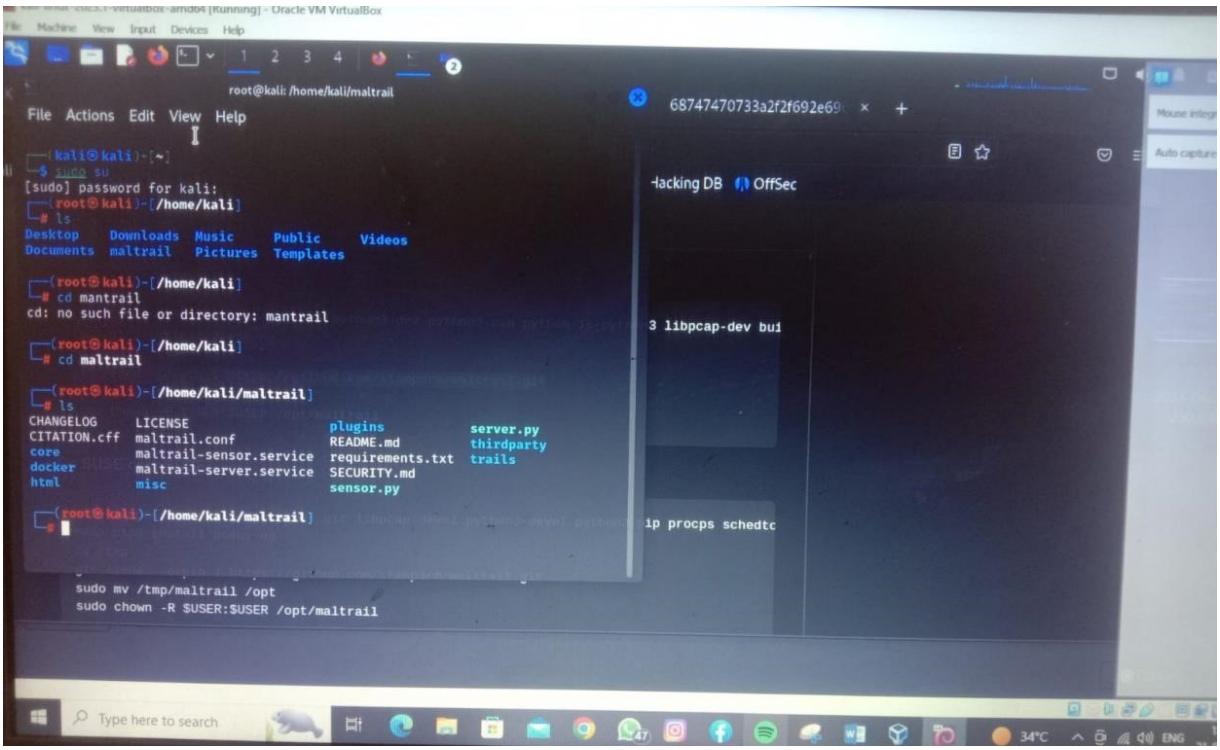
Step 3: Open Git hub.



Step 4: Open the terminal and type the command in the git hub for installation of maltrail.



Step 5: To finding the malware using this command in the terminal.



Step 6: Stop the program.

Result:

The malware is detected using malicious traffic detection system.