

CYBER SECURITY TECHNOLOGY

DOCUMENTATION

NAME: G.J.INDHUMATHI

CLASS: B.Sc., Information Technology

REGISTER NUMBER: CB 20S305315



DEPARTMENT OF COMPUTER SCIENCE, IT &
COMPUTER APPLICATIONS

SHRIMATI INDIRA GANDHI COLLEGE

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

TIRUCHIRAPPALLI – 620 002.



Edit with WPS Office

Nmap

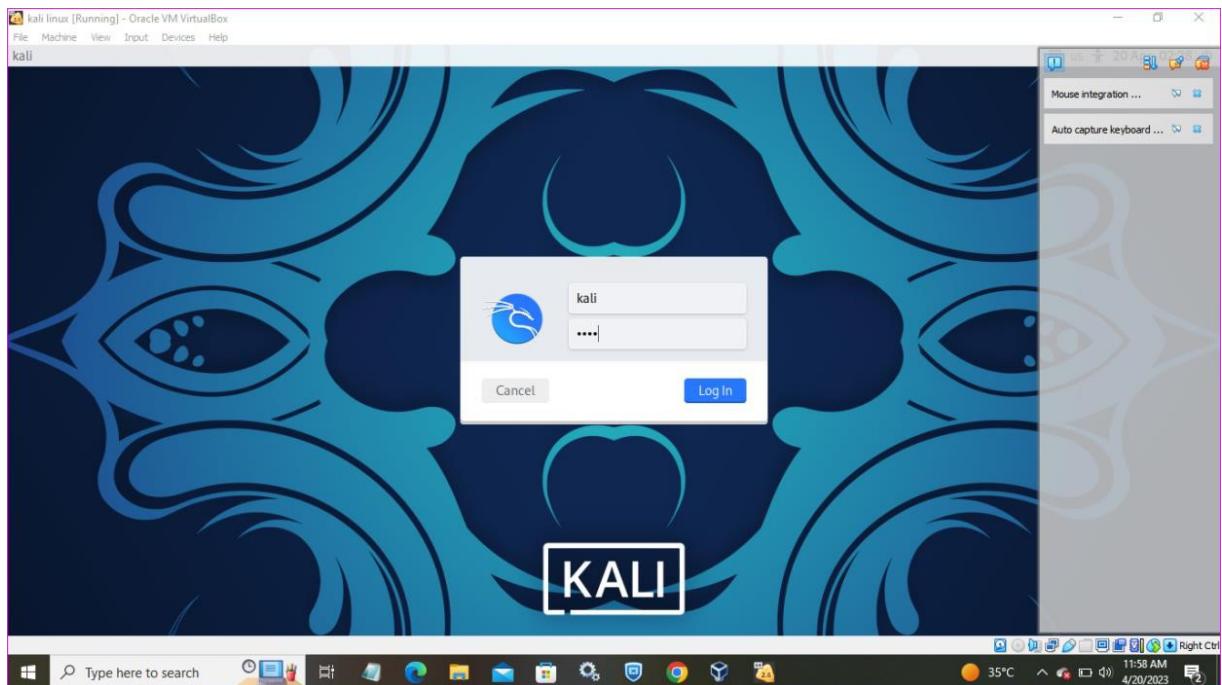
Aim:

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

Procedure:

Step 1: Start the program.

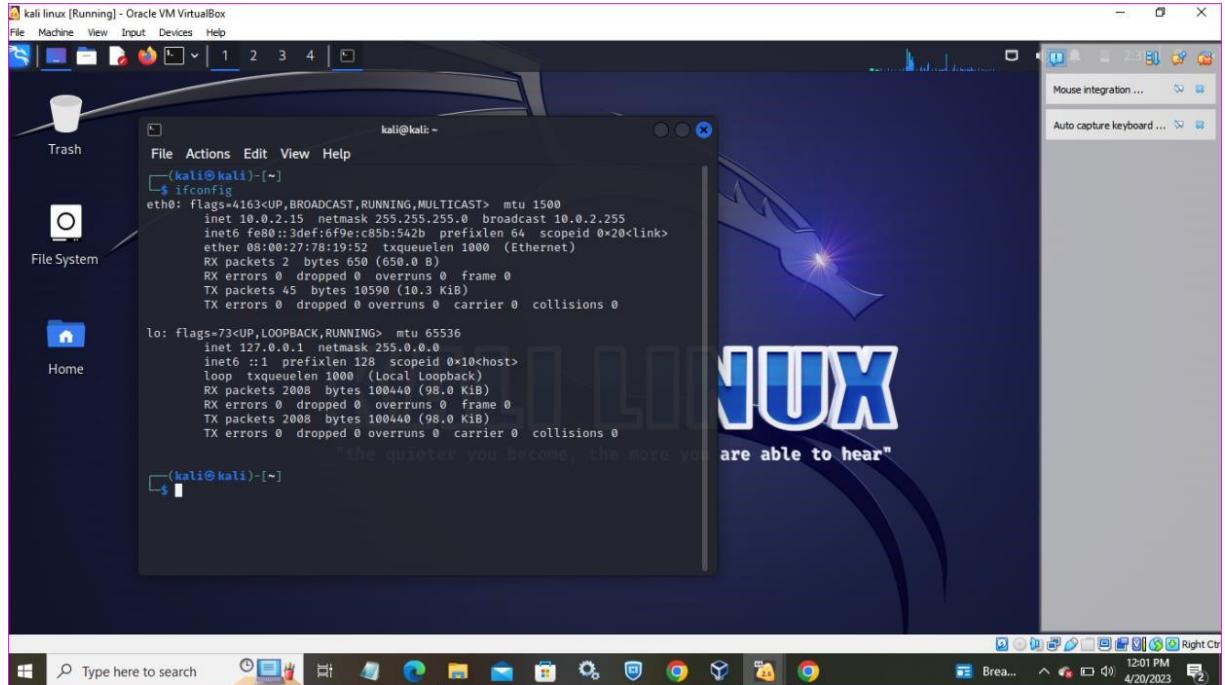
Step 2: Open kali linux using virtual box.



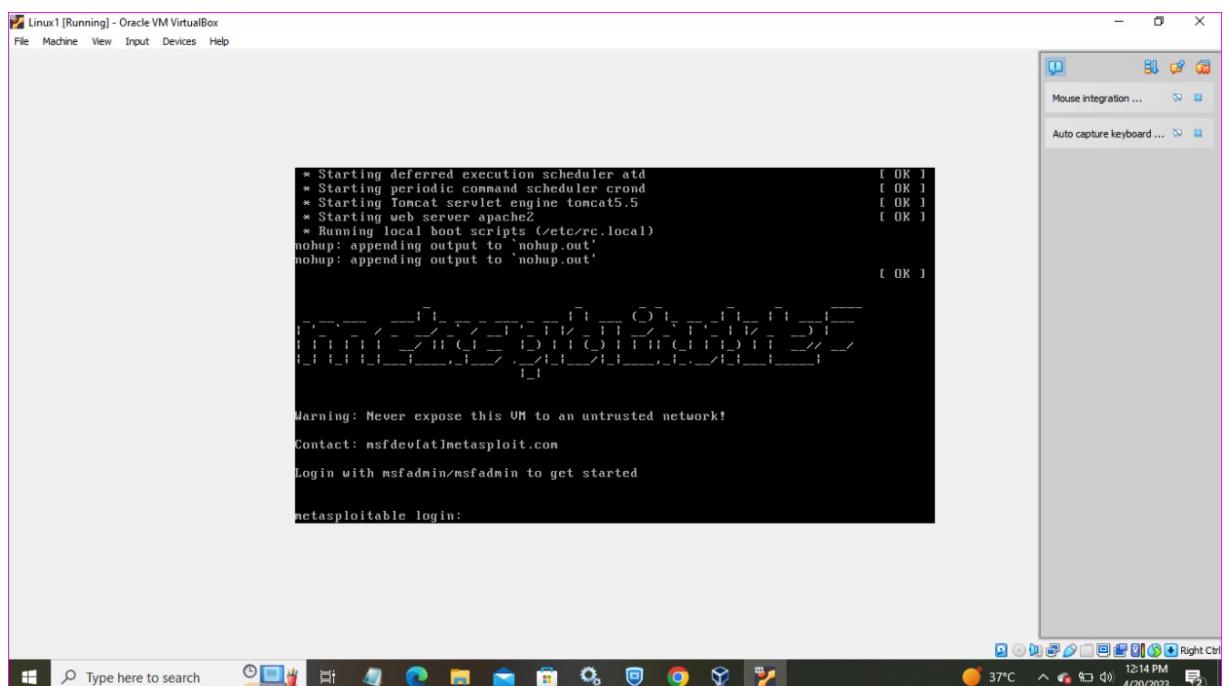
Step 3: Open kali linux terminal and add ifconfig command to find the ip address of our system.



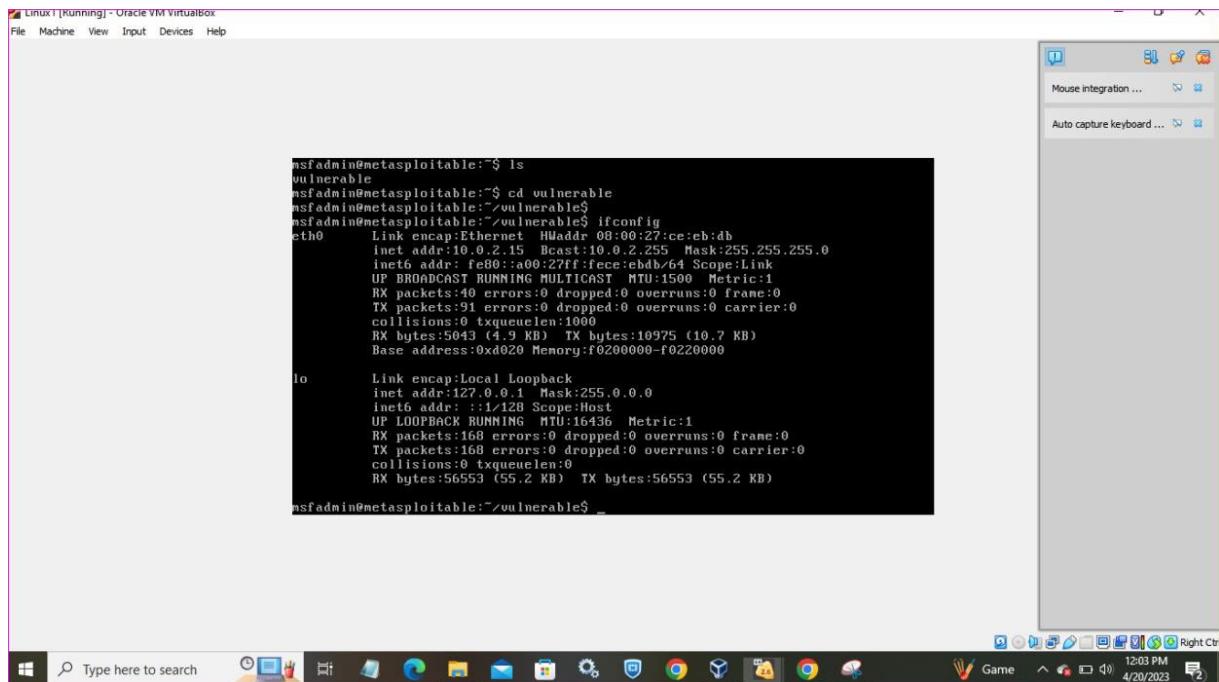
Edit with WPS Office



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

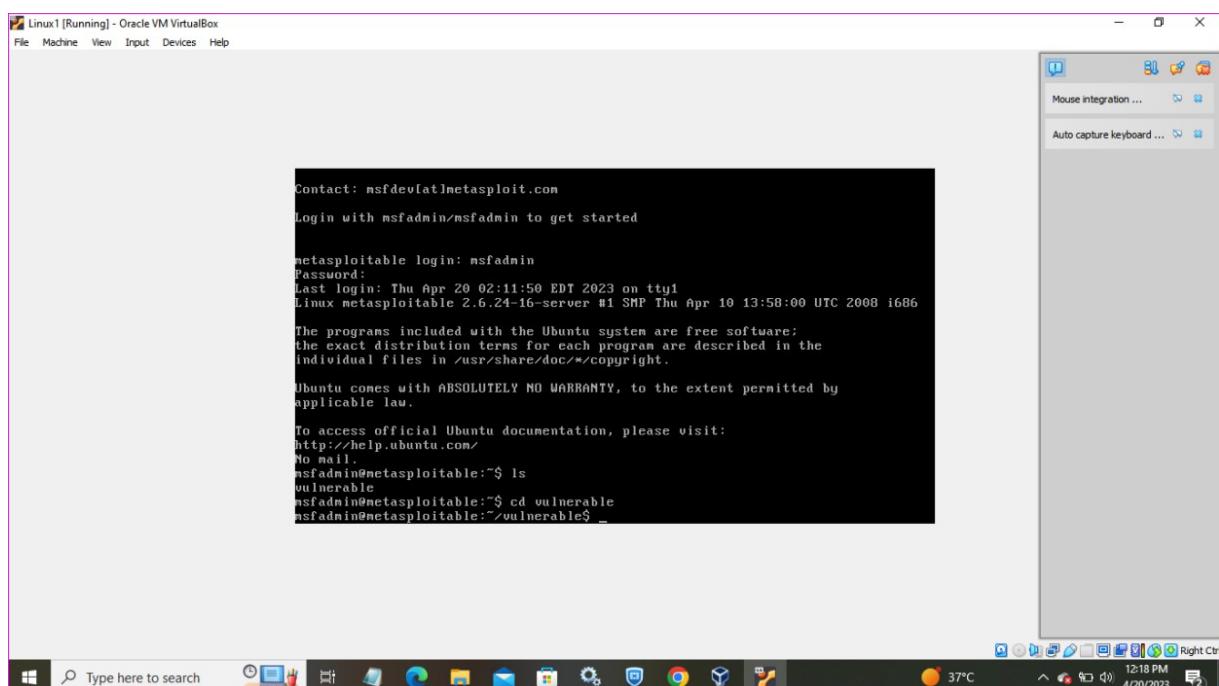


Step 5: login to metasploitable using the command msfadmin.



```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:c:e:db
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecc:eb%eth0 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:40 errors:0 dropped:0 overruns:0 frame:0
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5043 (4.9 KB) TX bytes:10975 (10.7 KB)
            Base address:0xd020 Memory:f0200000-f0220000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1%lo Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:168 errors:0 dropped:0 overruns:0 frame:0
            TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:56553 (55.2 KB) TX bytes:56553 (55.2 KB)
msfadmin@metasploitable:~/vulnerable$ ..
```

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



```
Contact: msfdevulat@metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Apr 20 02:11:50 EDT 2023 on ttys1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/**/copyright.

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

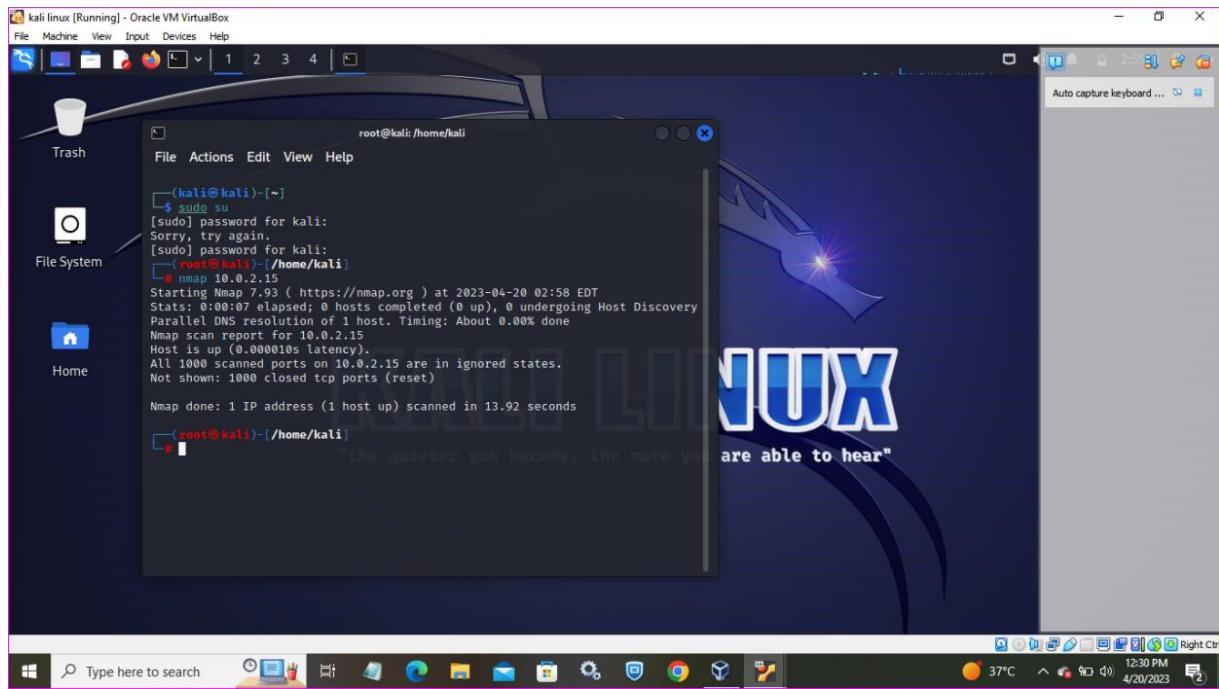
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~/vulnerable$ cd ..
msfadmin@metasploitable:~$ ..
```

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

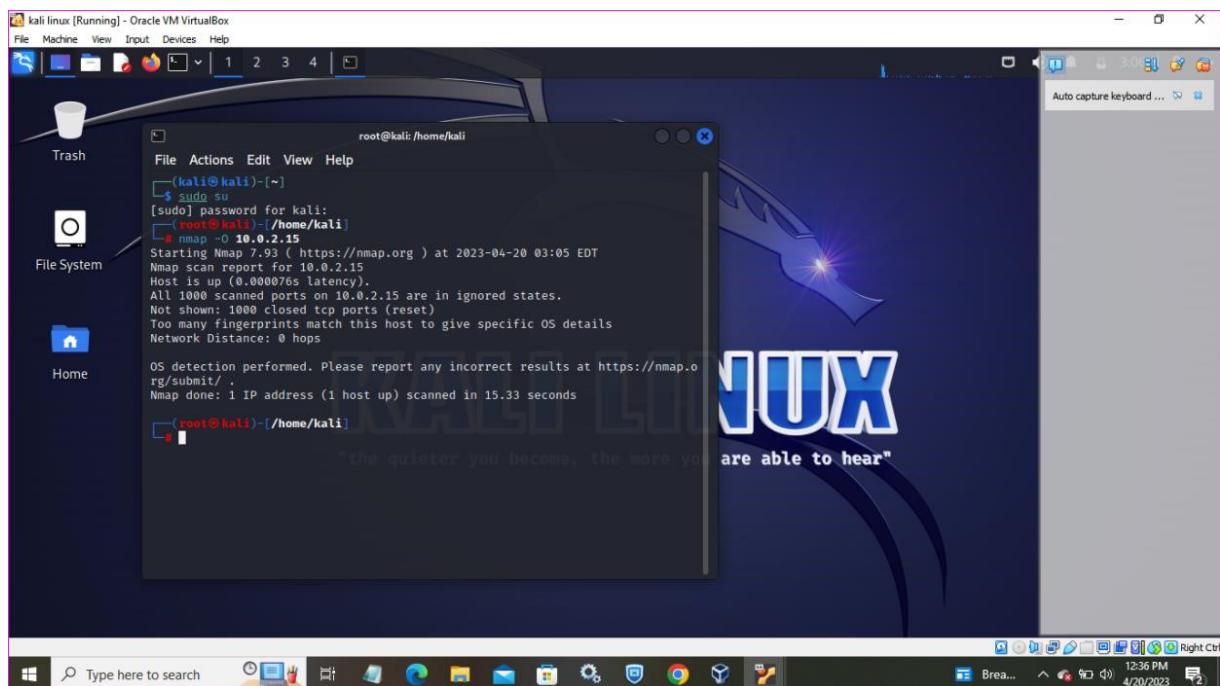
Step 8: Write nmap and IP address of Linux enter to run the command now we find the ports of another system find the vulnerabilities.



Edit with WPS Office



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



Step 10: Stop the execution.



Edit with WPS Office

Result:

Thus the vulnerabilities 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:

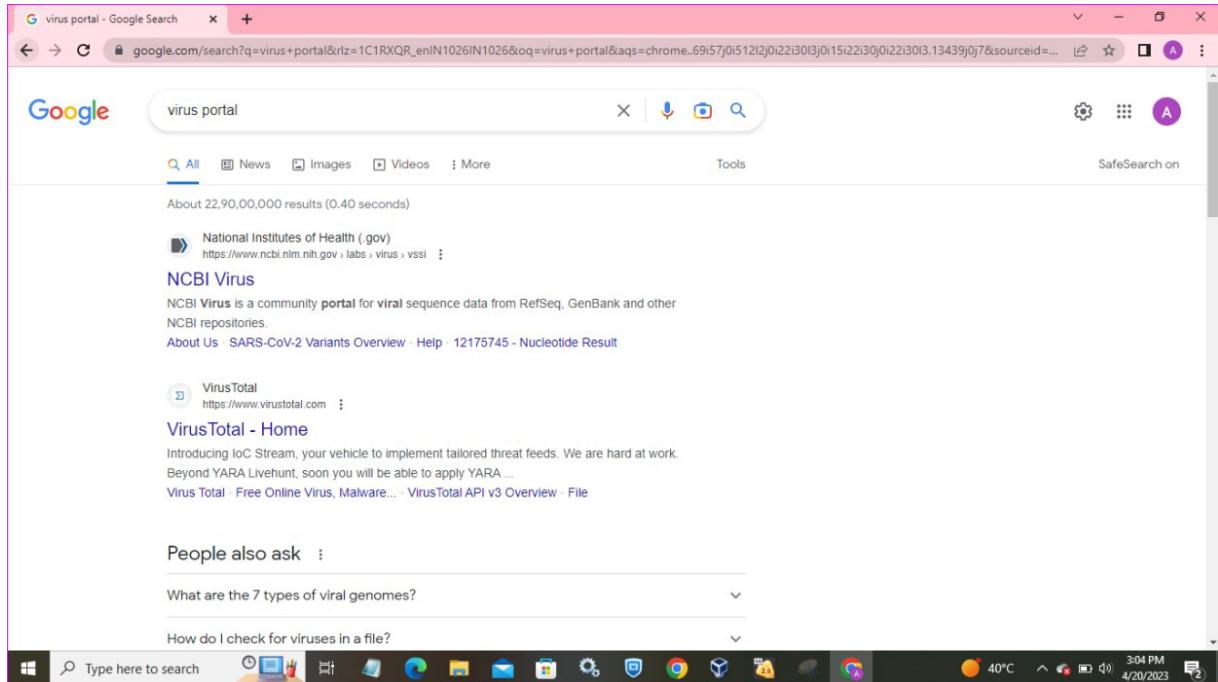


Edit with WPS Office

Step 1: Start the program.

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

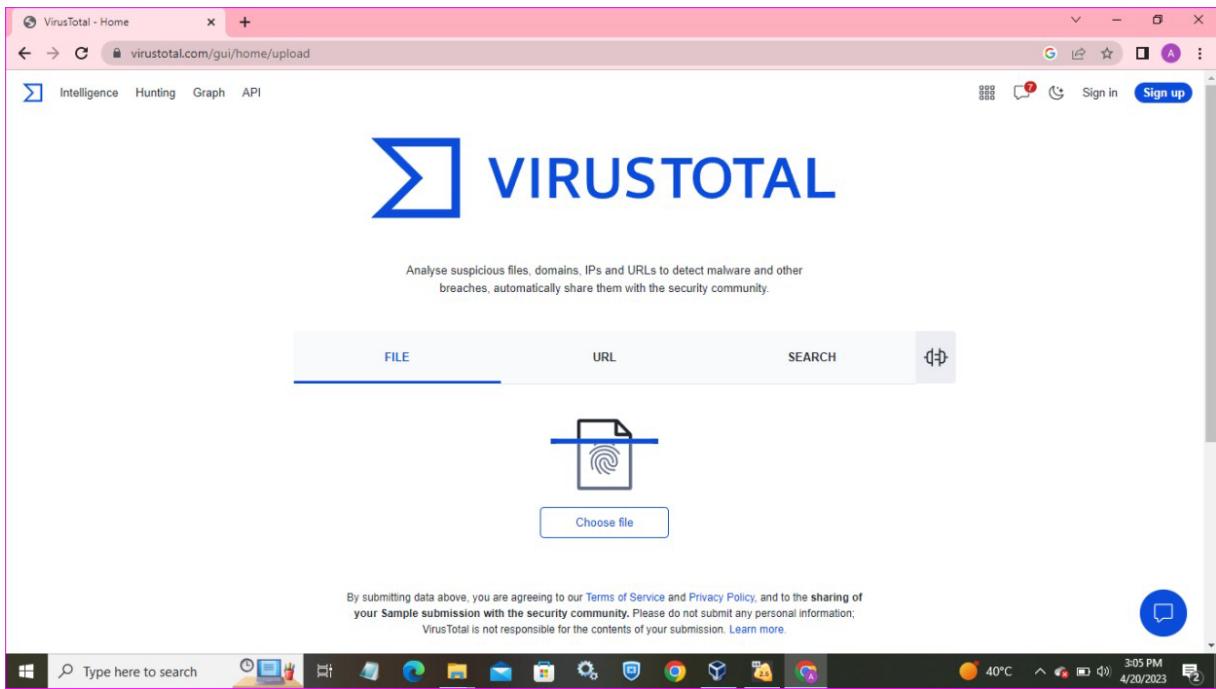
Step 3: Open the browser install Virus portal.



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



Edit with WPS Office



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

A screenshot of a web browser window showing the results for a specific file hash: '9c5011fd963c40c0f91c09febfa57c8df6402a29c250685ab34b0d0d1600dd63'. The page displays the file's metadata: 'File distributed by Microsoft' (Community Score: 0 / 58), size '18.28 KB', and date '2018-07-04 17:47:31 UTC'. Below this, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab shows a table of security vendor analysis results. The table includes columns for vendor name, detection status (Undetected for all listed), and a column for 'Do you want to automate checks?' which also shows 'Undetected' for all. The table rows are: Ad-Aware, AhnLab-V3, Antiy-AVL, Avast, AegisLab, ALYac, Arcabit, Avast-Mobile, and nsrl known-distributor.

Step 6: Stop the program.



Edit with WPS Office

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.

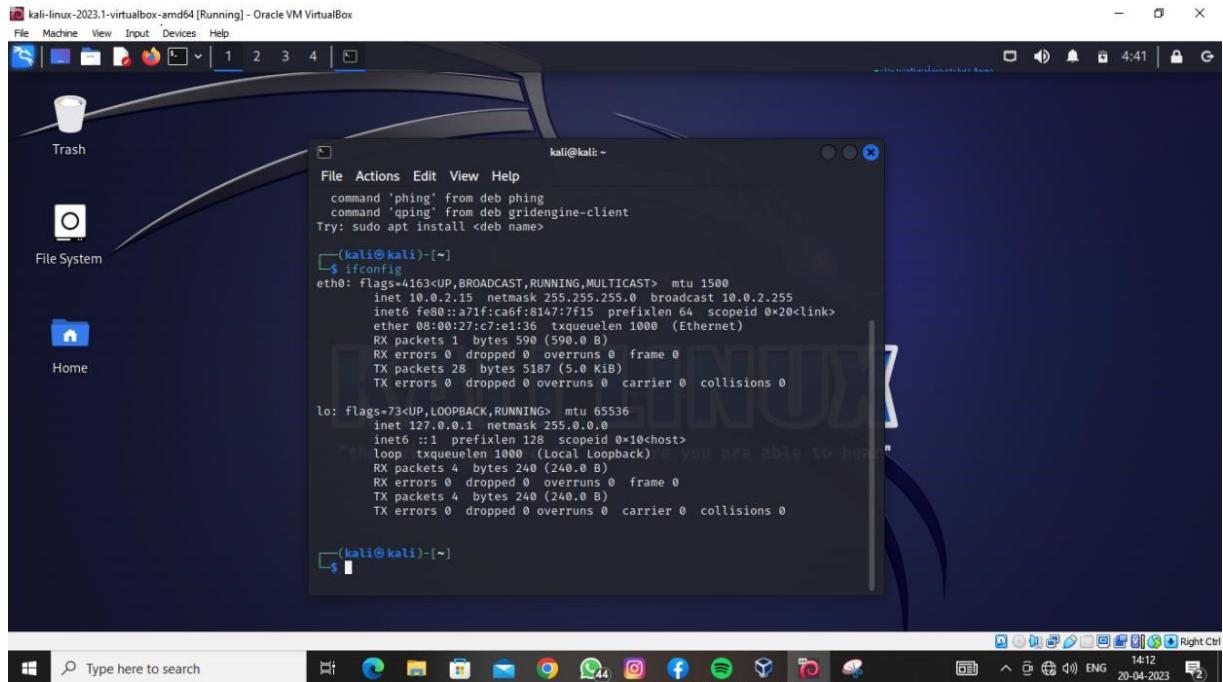


Edit with WPS Office

Procedure:

Step 1: Start the program.

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



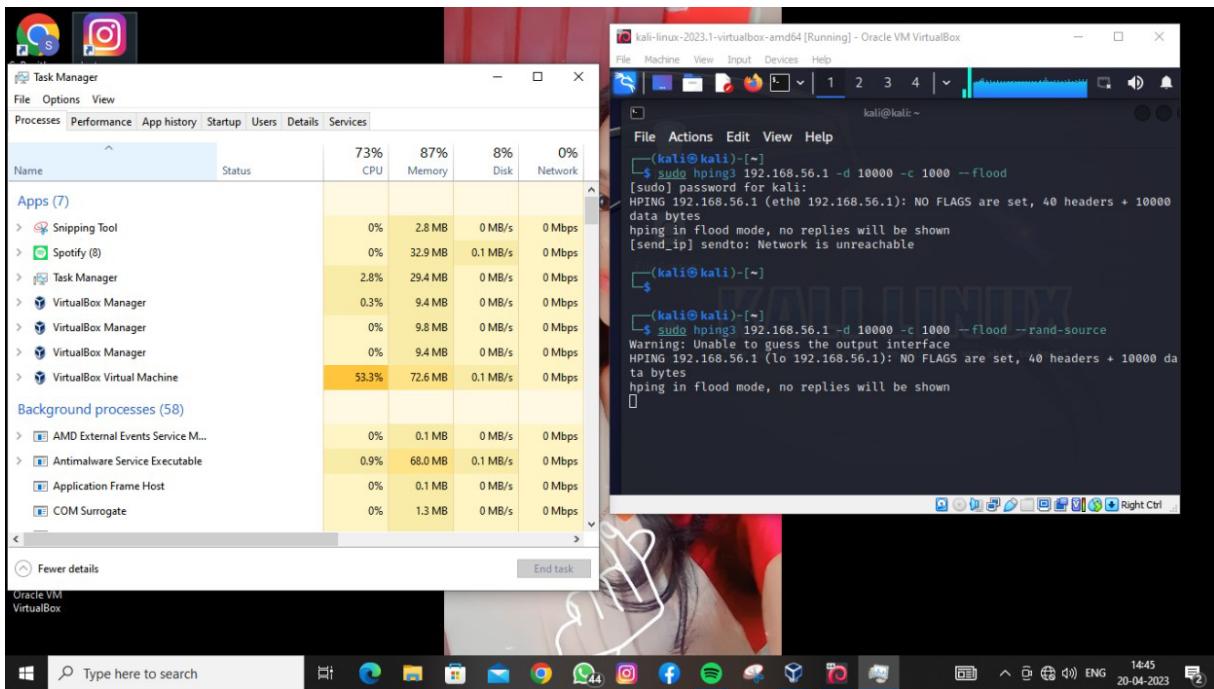
Step 3: Open windows and open command prompt and write the command ip config to find the ip address of the system.

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.



Edit with WPS Office



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



Edit with WPS Office

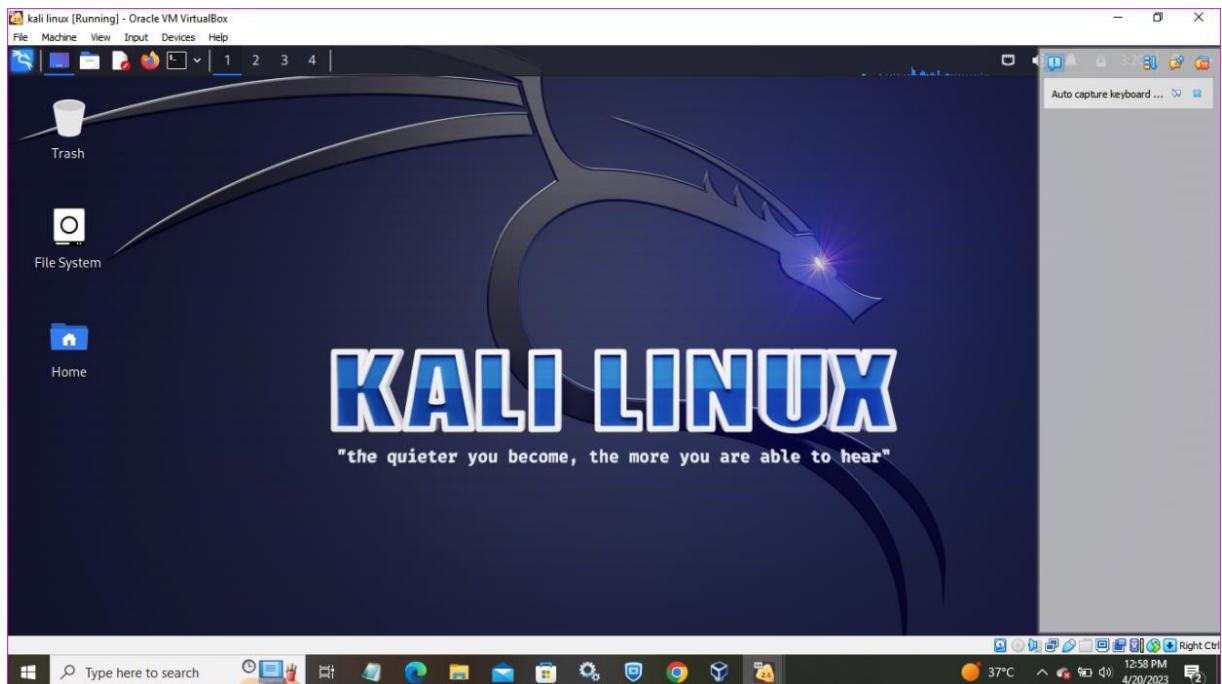
Aim:

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

Procedure:

Step 1: Start the program.

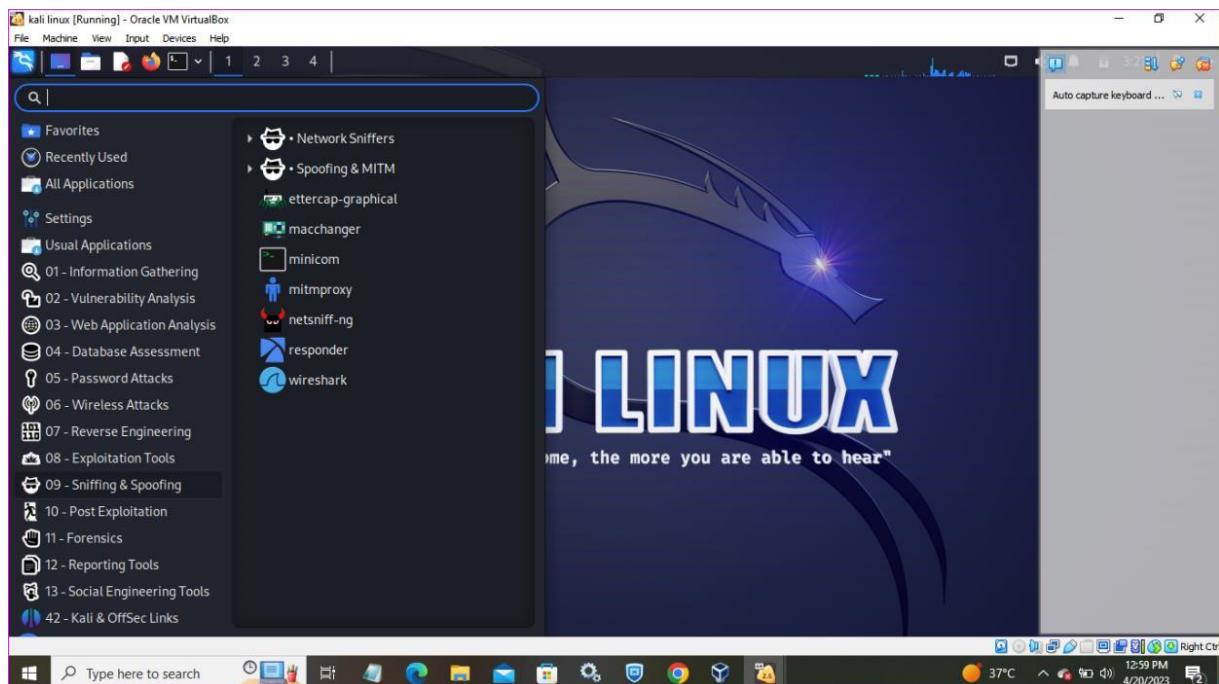
Step 2: Open kali linux.



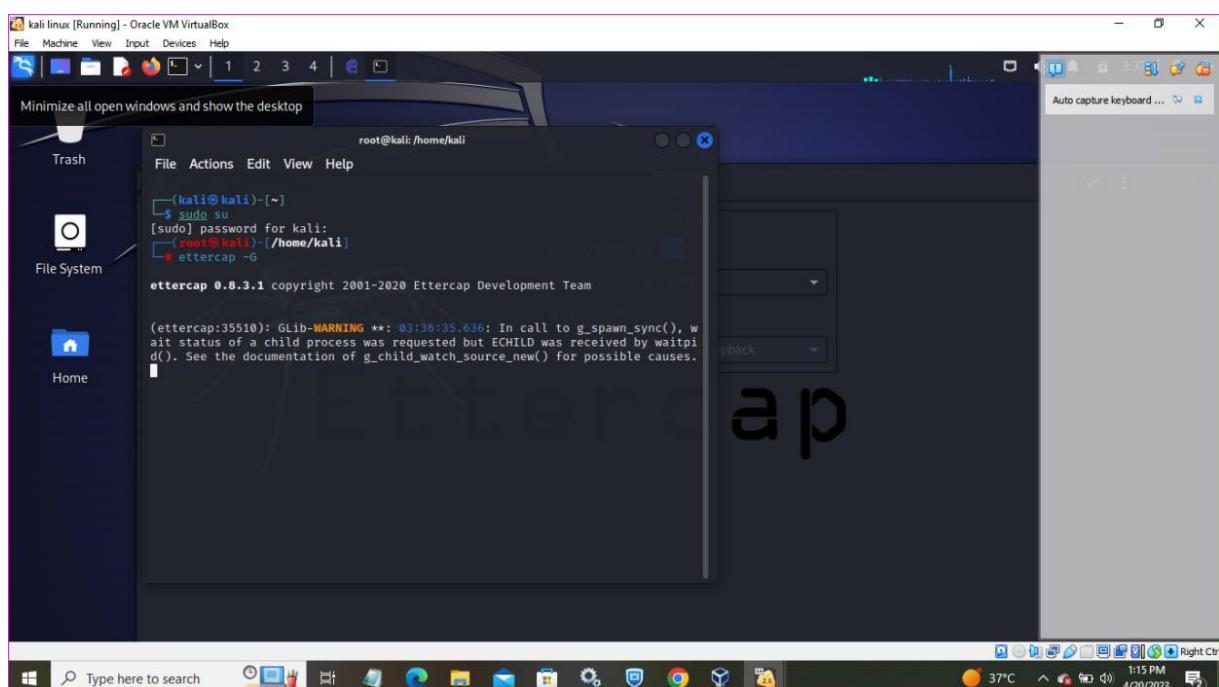
Step 3: Click the sniffing and spoofing to open the etter cap.



Edit with WPS Office



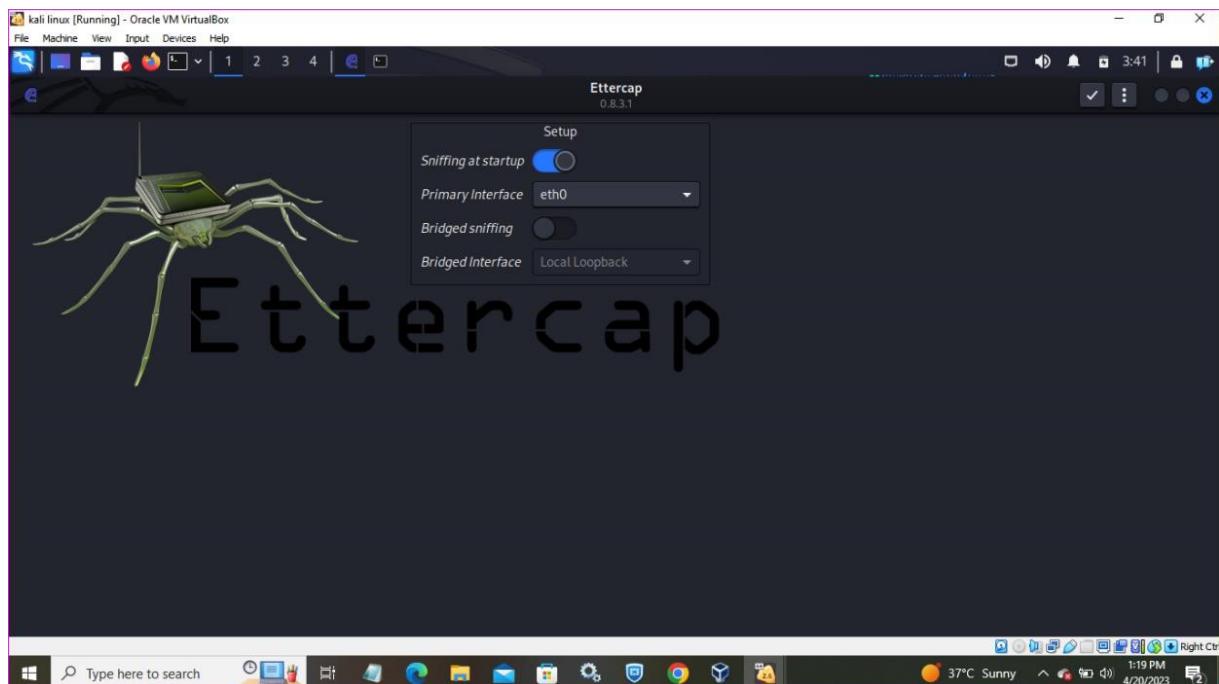
Step 4: Open the terminal and write the command sudo su for log in and write ettercap -G.



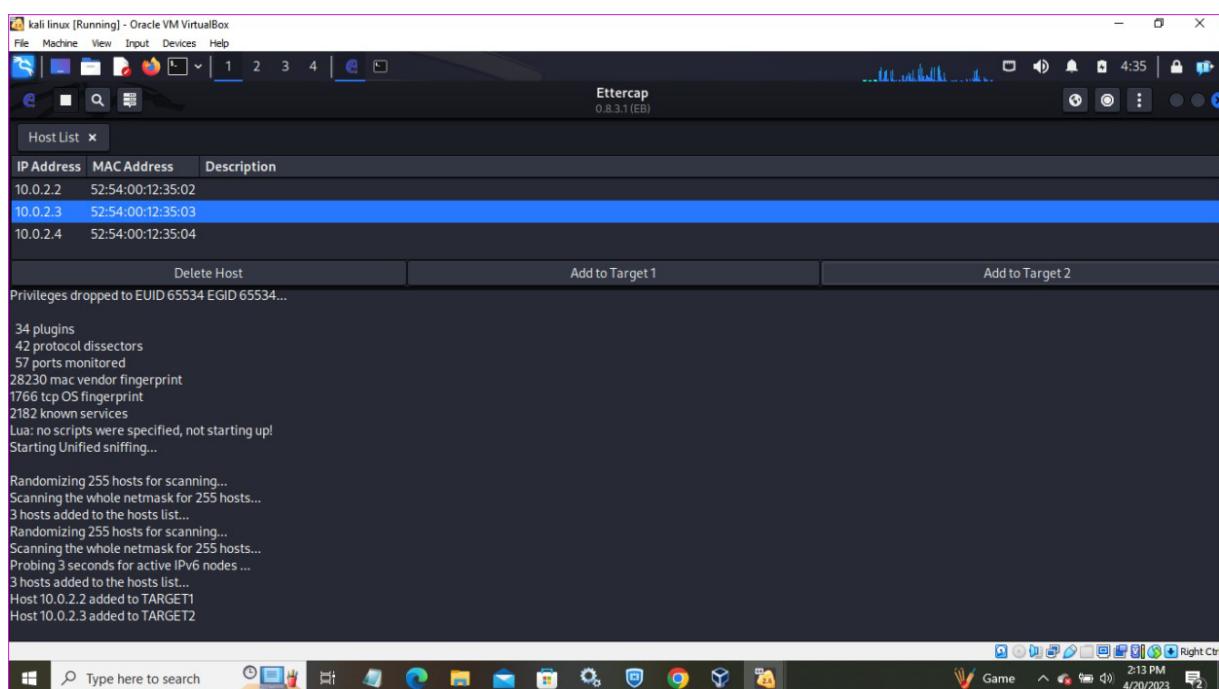
Step 5: Open Ettercap and start and setup the tool.



Edit with WPS Office



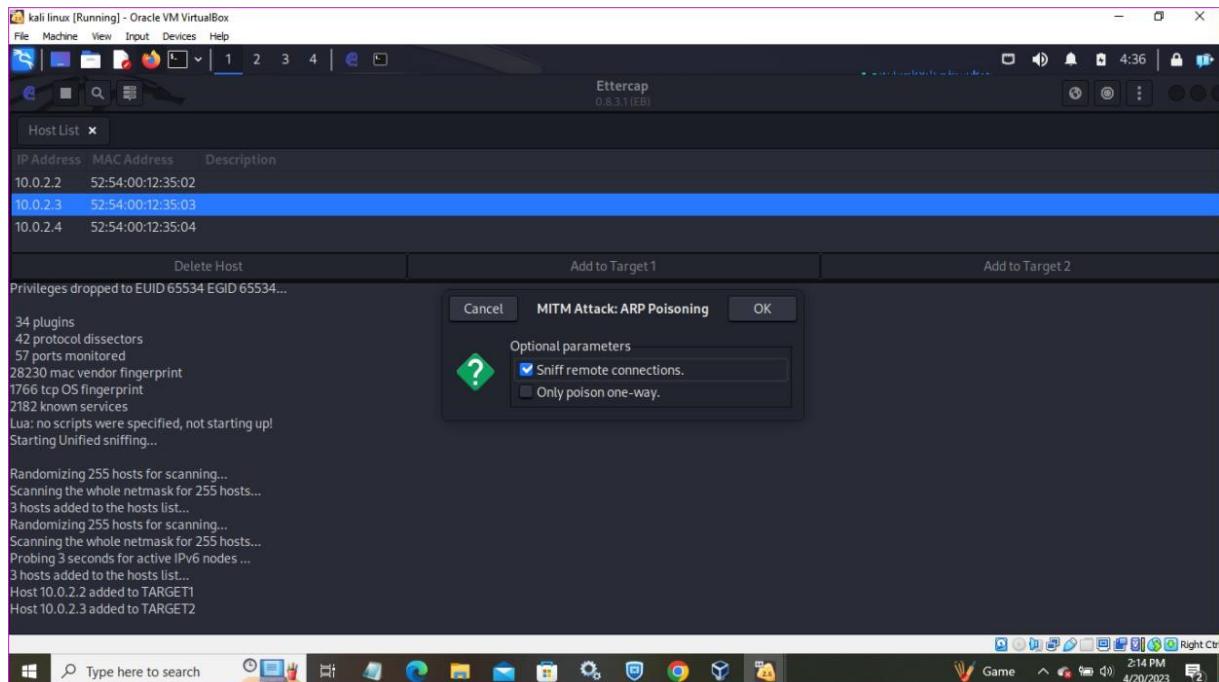
Step 6: After open the ettercap tool search the host list and fixing the target.



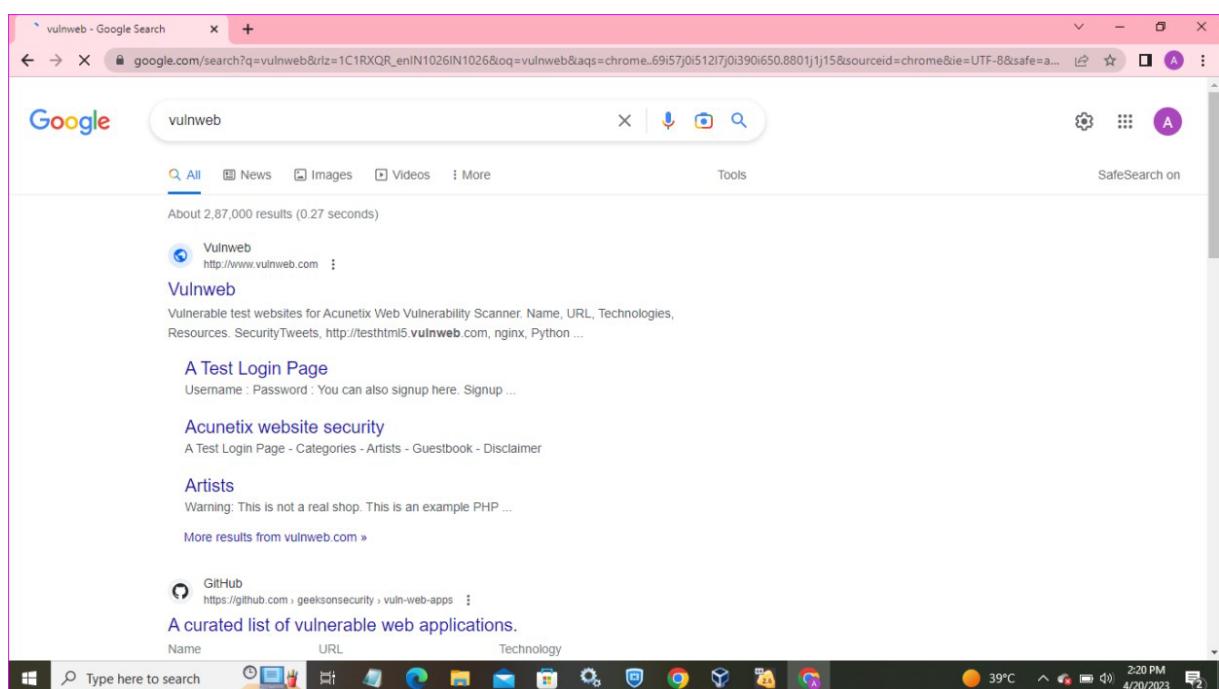
Step 7: Add ARP poisioning.



Edit with WPS Office



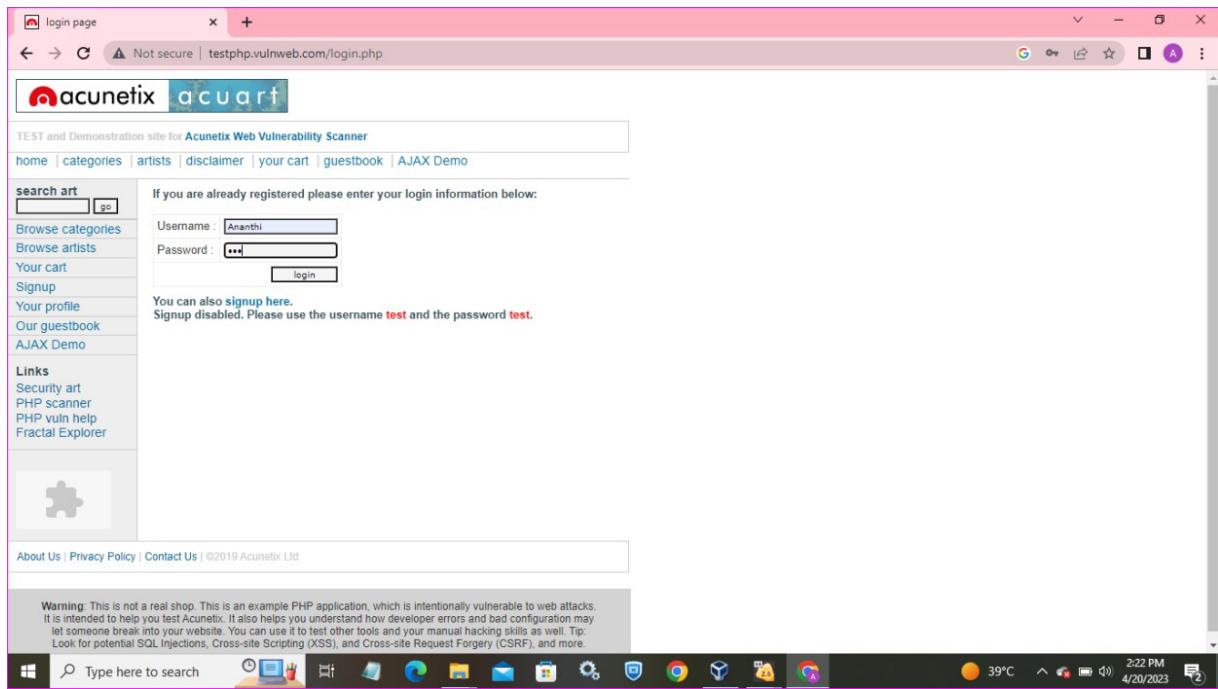
Step 8: Install the vulnweb using Google chrome.



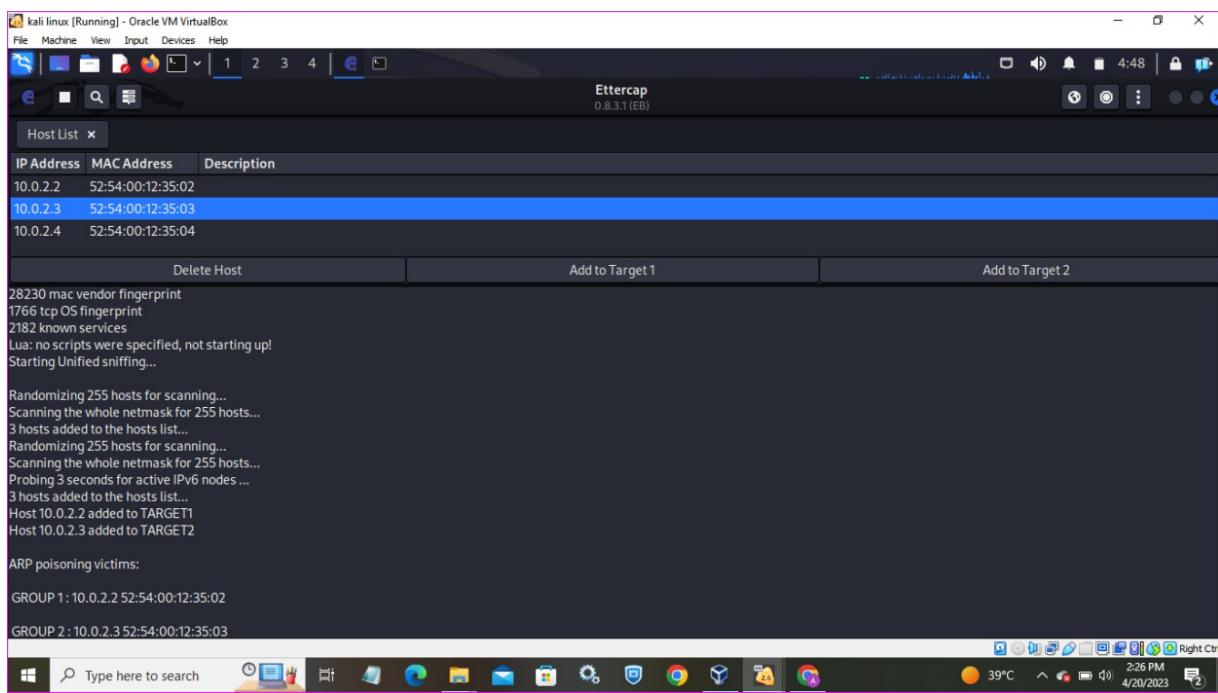
Step 9: To enter login and password.



Edit with WPS Office



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.



Edit with WPS Office

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.

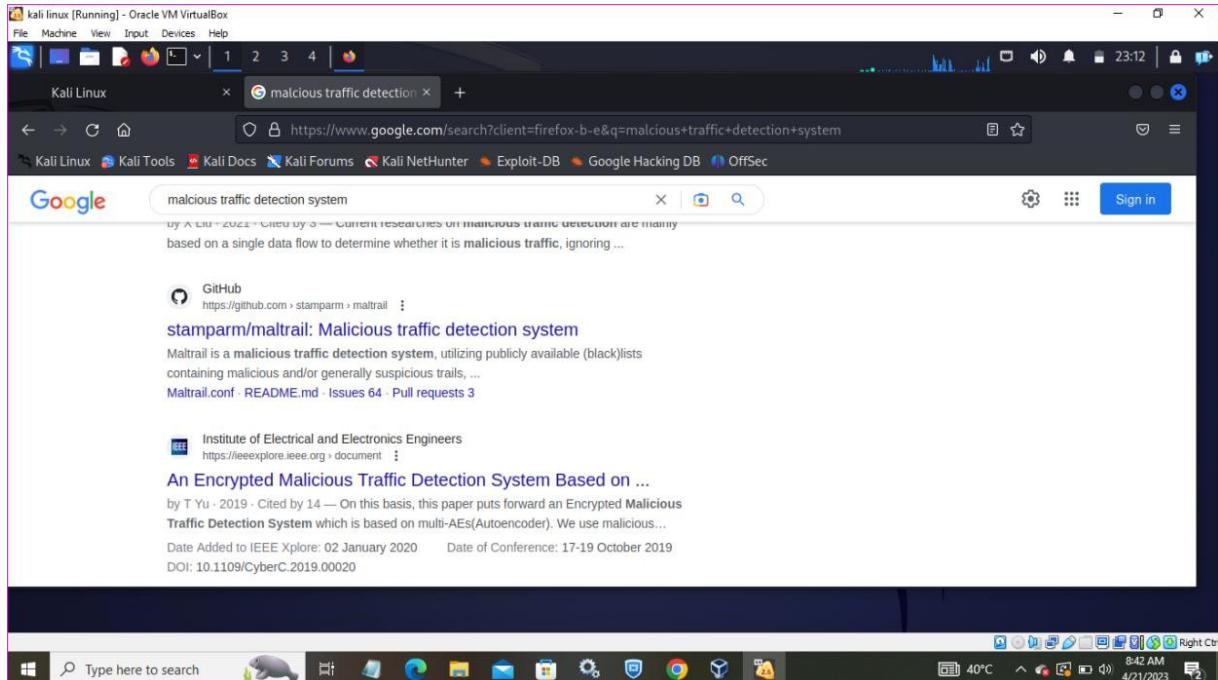
Procedure:



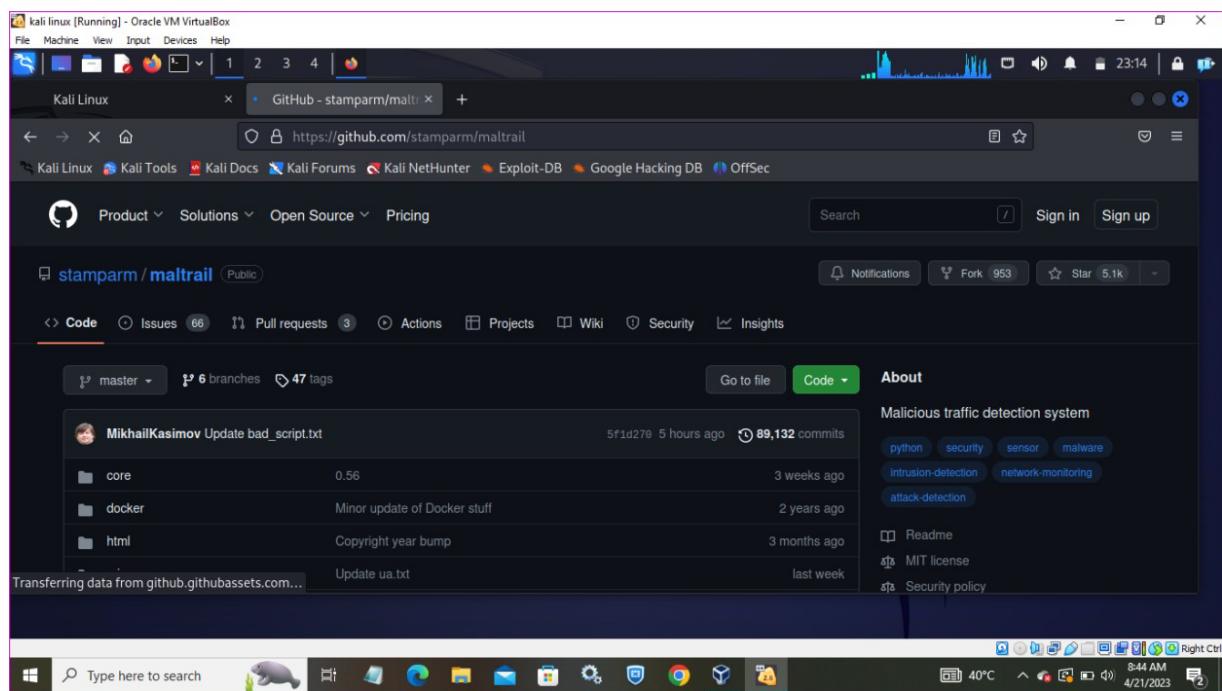
Edit with WPS Office

Step 1: Start the program.

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

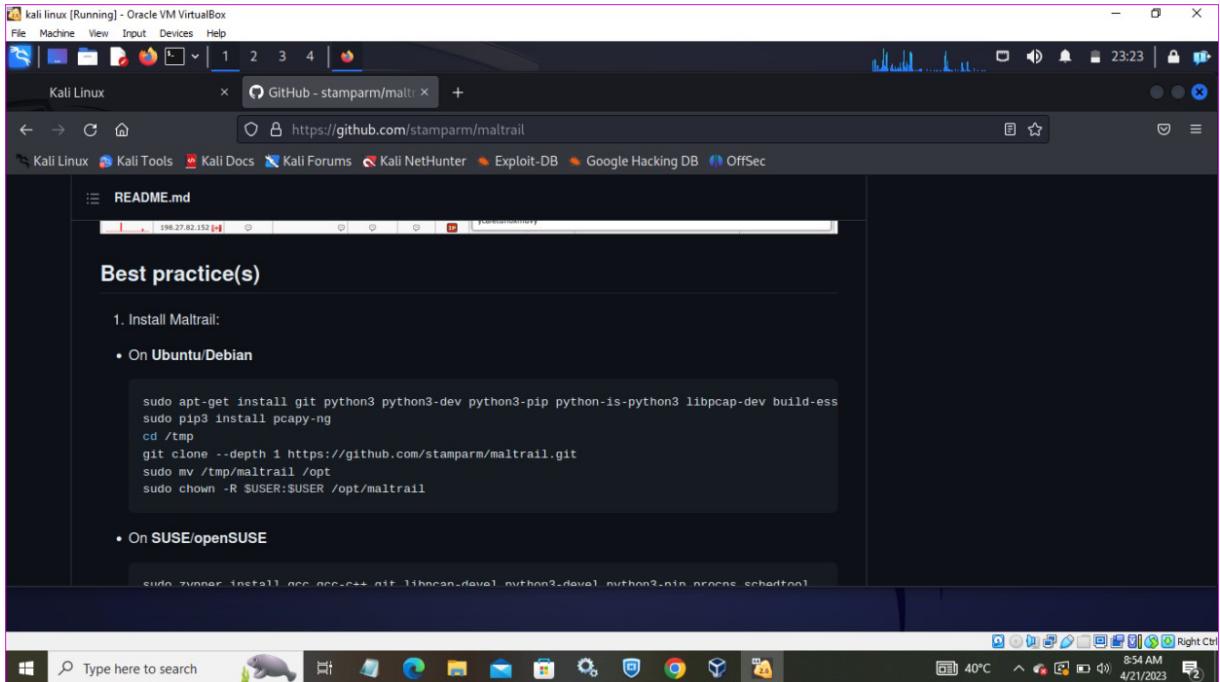


Step 3: Open Git hub.

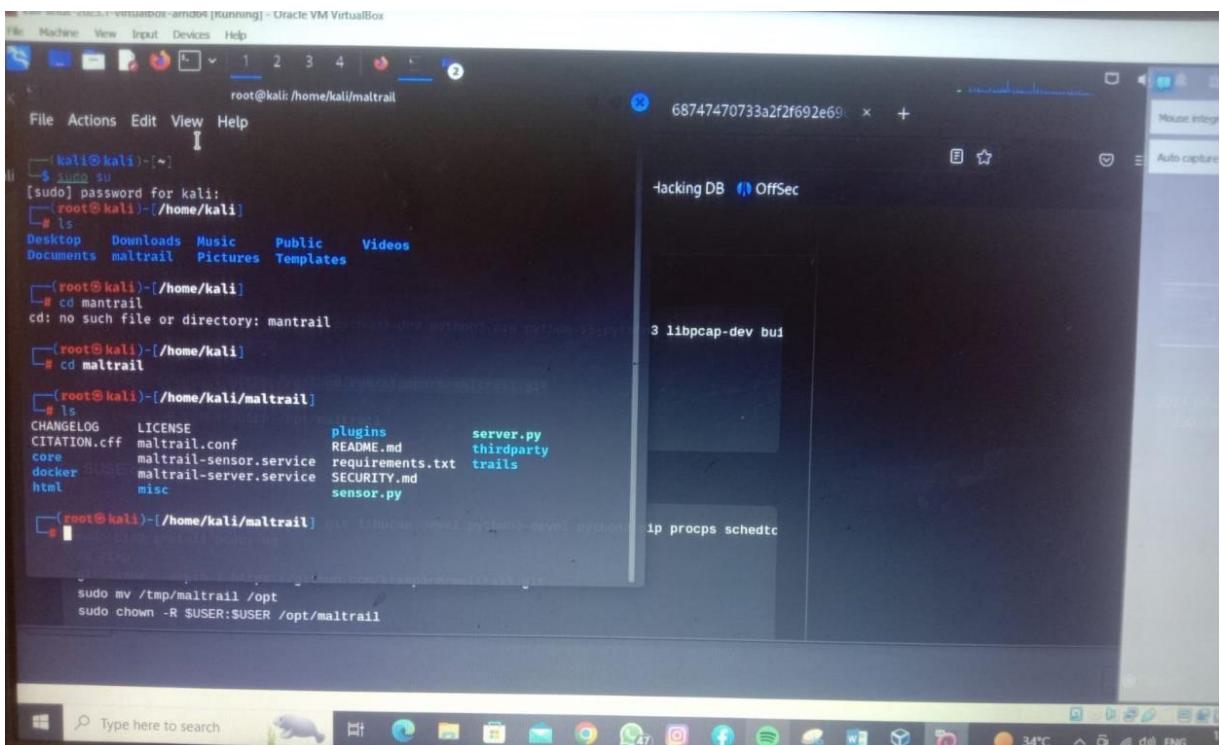


Edit with WPS Office

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.



Edit with WPS Office

Step 6: Stop the program.

Result:

The malware is detected using malicious traffic detection system.



Edit with WPS Office