GROUP PROJECT

by Adriana Afandi

Submission date: 16-Jan-2024 04:01PM (UTC+0800)
Submission ID: 2271786077
File name: CIPHER_02A_FINAL_PROJECT.pdf (36.3M)
Word count: 4755
Character count: 24017

DATA NETWORK & SECURITY

BCN2023

PROJECT

LECTURER'S NAME: ABDULLAH BIN MAT SAFRI		
DATE OF SUBMISSION: 16 JANUARY 2024		
SECTION: 02A		
NAME	**MATRIC ID**	**STUDENT PHOTO**
MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI	CB21012	
NURUL ADRIANA BINTI MOHAMMAD AFANDI	CB21045	
TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH	CB21039	
WARSENA A/P EH CHUOI	CB21056	

TABLE OF CONTENTS

CONCEPT

Our 10-week project, which accounts for 25% of our assessment, aims to improve online system security. We divided our four-person group into two teams: the Blue Team and the Red Team.

Blue Team's Job: Establishing Strong Defences

The Blue Team, made up of two members, began by connecting three computers. Two PCs use distinct operating systems: Windows and Linux. We updated and installed the newest security patches to ensure optimal protection. On Windows, we configured a web service and enabled networking options. The Linux machine received all of the essential networking tools.

Our goal as the Blue Team was to protect against possible attacks. We investigated and implemented online defence techniques on both computers. We chronicled the entire process, including the first steps and ultimate defence setup.

Red Team Role: Testing the defences.

The remaining two members comprised the Red Team. Our task was to simulate hacking (in a responsible manner) and test our ability to gain access to computers. We evaluated various attack strategies and tools for Windows and Linux. We thoroughly documented our results and meticulously planned our attacks. We did not intend to inflict harm, only to test the defences. We executed five simulated attacks on Windows and three on Linux systems. We provided step-by-step explanations of each attack, including accompanying photos.

Learning and Improving Together:

The Blue Team then took over, demonstrating how they resisted our simulated onslaught. They had plans in place to prevent attacks and defend their systems. We chronicled their defences and gained valuable insights from their approach.

Throughout our project, we made a point of mentioning where we acquired our information. This allows others to check and learn more as needed. We communicated extensively as a group to ensure everyone understood the situation and resolved any issues.

Our goal was to understand and develop our systems while being responsible and ethical. This project is our effort to make online places safer for everyone.

COMPUTER AND NETWORK SERVICES PREPARATION

In preparation for the targeted attack, we have categorized the tools into two separate categories according to the platforms they are compatible with: Windows and Linux. Zphisher, Ettercap, Kage, Slowloris, Cain, and Abel are the tools that are used in the Windows environment. Meanwhile, Storm Breaker, Hping3, and SARA are available for the Linux platform. Below are the explanations for each tool on Windows and Linux.

RED TEAM

WINDOWS

TOOLS	EXPLANATION
Zphisher	❖ Zphisher is a phishing application that automatically generates phishing websites across multiple internet platforms. ❖ A form of social engineering where hackers trick users into revealing personal data including usernames and passwords.
Ettercap	❖ Ettercap is used to carry out Man-in-the-Middle (MitM) attacks. ❖ It has the ability to record, capture, and examine conversations between two network users.
Kage	❖ Kage makes the process of designing graphical user interfaces (GUIs) for different penetration testing tools easier. ❖ It aims to simplify user interaction with many tools

	via a single interface.
Slowloris	❖ A Slowloris attack is a particular kind of Denial of Service (DoS) attack that may be carried out with the use of the tool Slowloris. ❖ It functions by establishing and maintaining many connections to the target web server.
Cain and Abel	❖ Cain and Abel is a Microsoft Windows password recovery programme. ❖ It can retrieve a variety of password formats by employing strategies like brute-force and dictionary attacks.

LINUX

TOOLS	EXPLANATION
SARA	❖ SARA is a security testing tool intended to assist security experts in locating and evaluating computer system vulnerabilities.
Storm Breaker	❖ Storm Breaker is a tool that targets flaws in people rather than in technological systems. ❖ The main purpose of it is to locate the victim, including their GPS coordinates.
Hping3	❖ Hping3 may be used for creating packets, scanning networks, and testing firewalls.

BLUE TEAM

WINDOWS

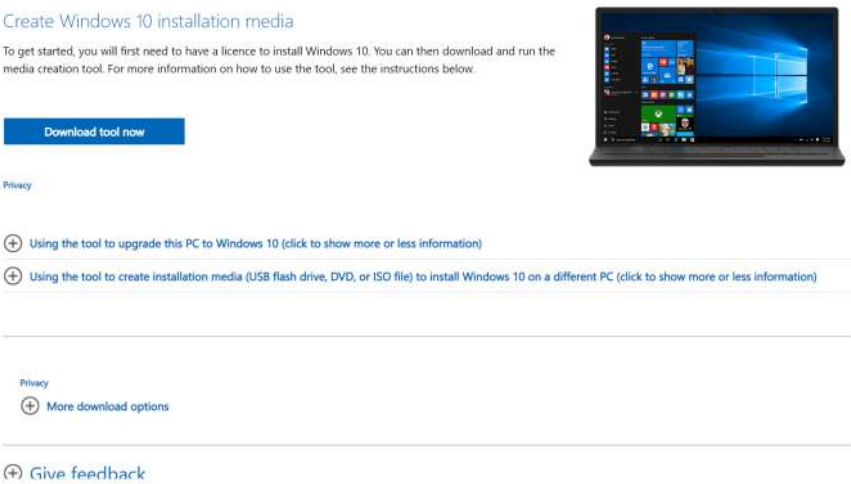
TOOLS	EXPLANATION
AVG Antivirus	❖ AVG is an antivirus program that defends your computer against viruses, malware, and other internet threats. ❖ It contains features like real-time scanning, email protection, and secure web browsing.
Avast Antivirus	❖ Avast is another antivirus product that protects against viruses, malware, and other cyber dangers. ❖ It has capabilities including real-time scanning, behaviour analysis, and a range of scanning methods.
Windows Defender Firewall	❖ Windows Defender is a built-in antivirus and malware protection solution for Windows operating systems. ❖ In addition to antivirus protection, Windows Defender has a firewall that monitors and controls incoming and outgoing network traffic.

LINUX

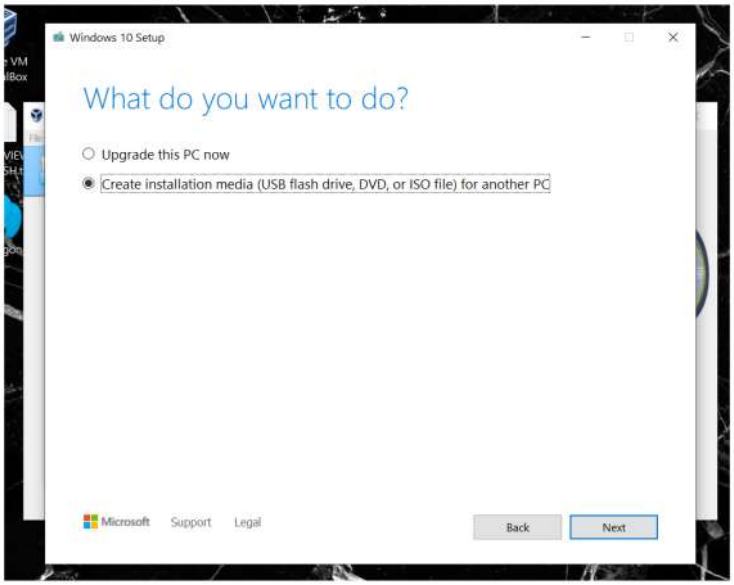
TOOLS	EXPLANATION
Antivirus ClamAV	❖ ClamAV is an open-source antivirus engine designed to detect a variety of harmful malware. ❖ It is commonly used on Linux-based systems and may be connected with email servers to detect viruses in attachments.
Eset nod 32 Firewall	❖ Eset NOD32 is an antivirus software that protects against viruses, worms, and other forms of malware. ❖ It also has a firewall component for monitoring and controlling network traffic.
XDP-Firewall	❖ A stateless firewall that hooks to the Linux kernel's XDP hook using (e)BPF for rapid packet processing. ❖ This firewall is intended to read filtering rules and filter incoming packets based on a configuration file stored on a disc.

SETTING UP WINDOWS

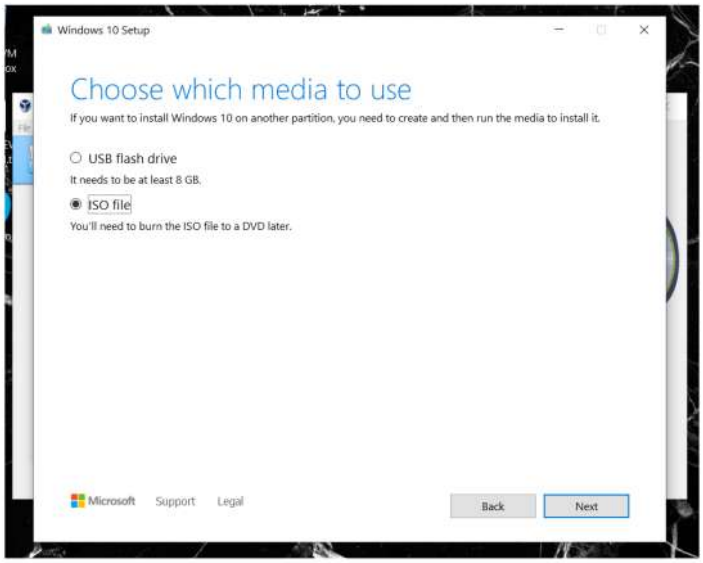
Step 1: Download Windows 10 ISO tool through this link
https://www.microsoft.com/en-au/softwaredownload/windows10



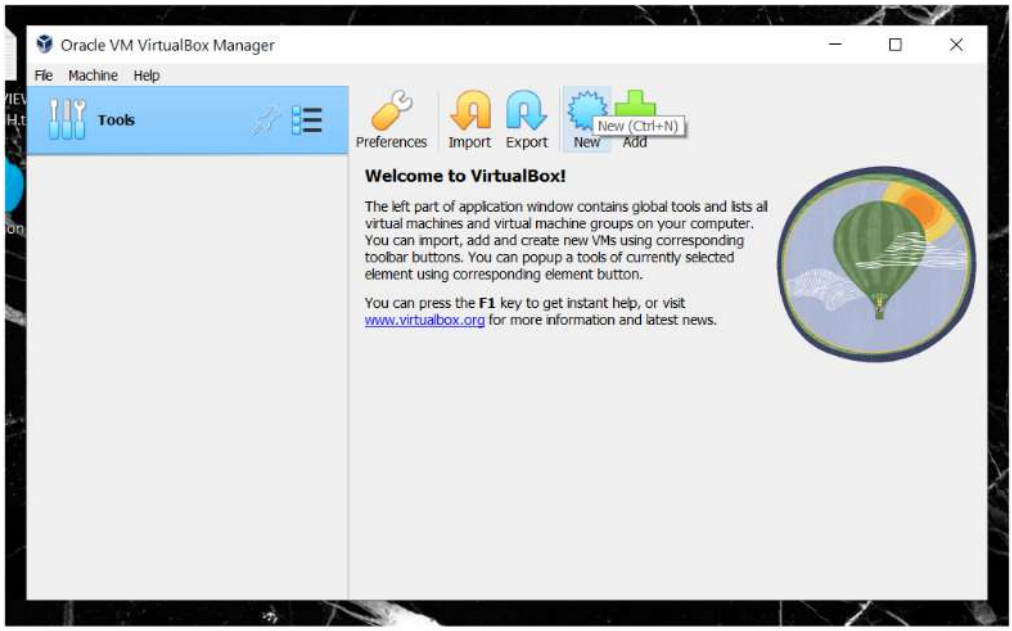
Step 2: After installation, launch the exe file and select "Create installation media for another PC" and go to the next step.



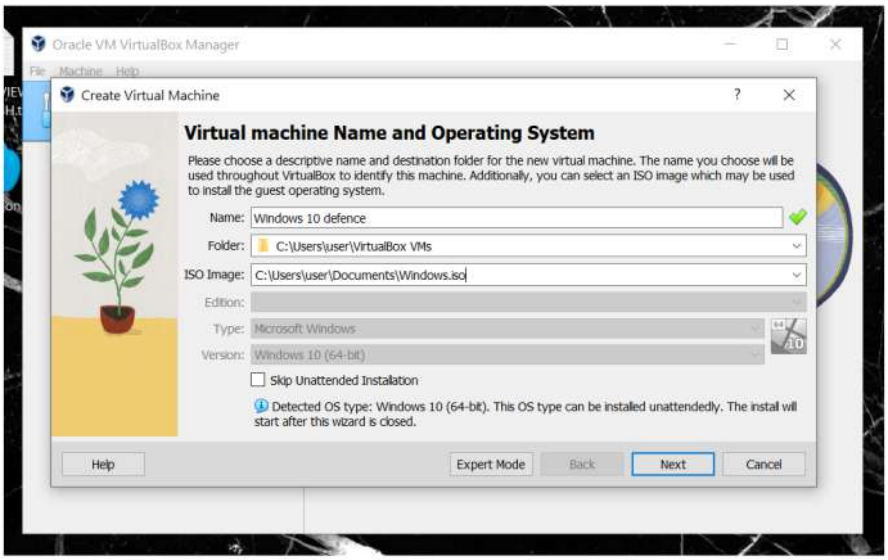
Step 3: To select the media to utilise, select an ISO file and proceed with the next step.



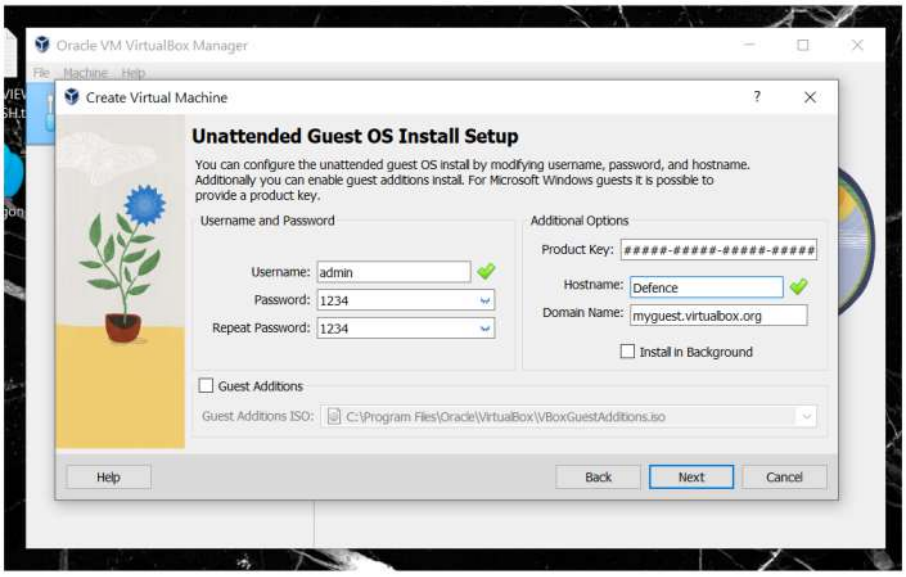
Setting up VirtualBox for Windows
Step 1: Run the VM VirtualBox and click new.



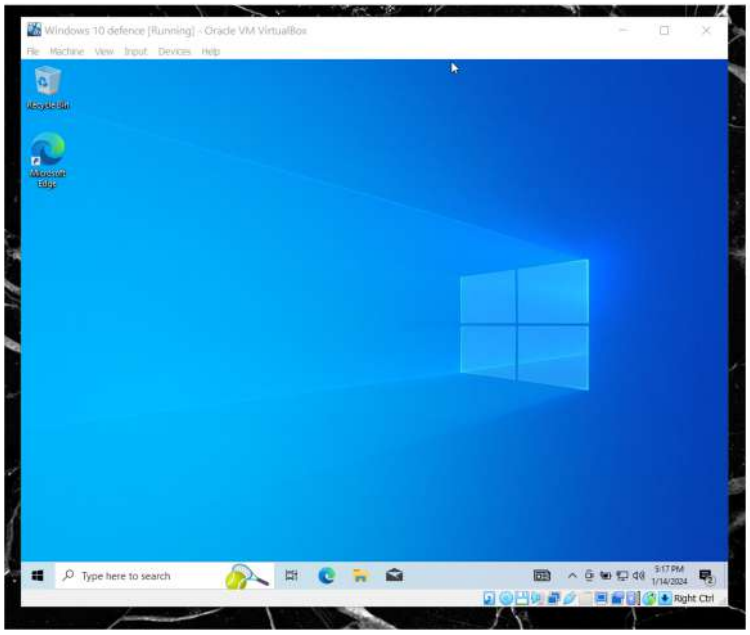
Step 2: To save the folder, enter the name "Defence Windows 10".
Select the previously saved Windows.iso from the download file and proceed to the next step.



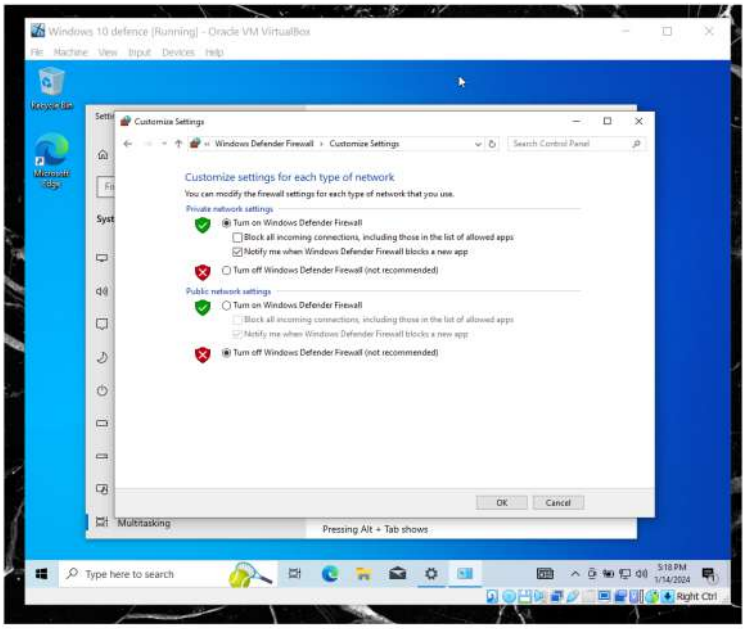
Step 3: To proceed, enter the admin username, repeat the password (1234), and click Next.



Step 4: After the setup has been completed, users can now run Windows using the virtualbox.



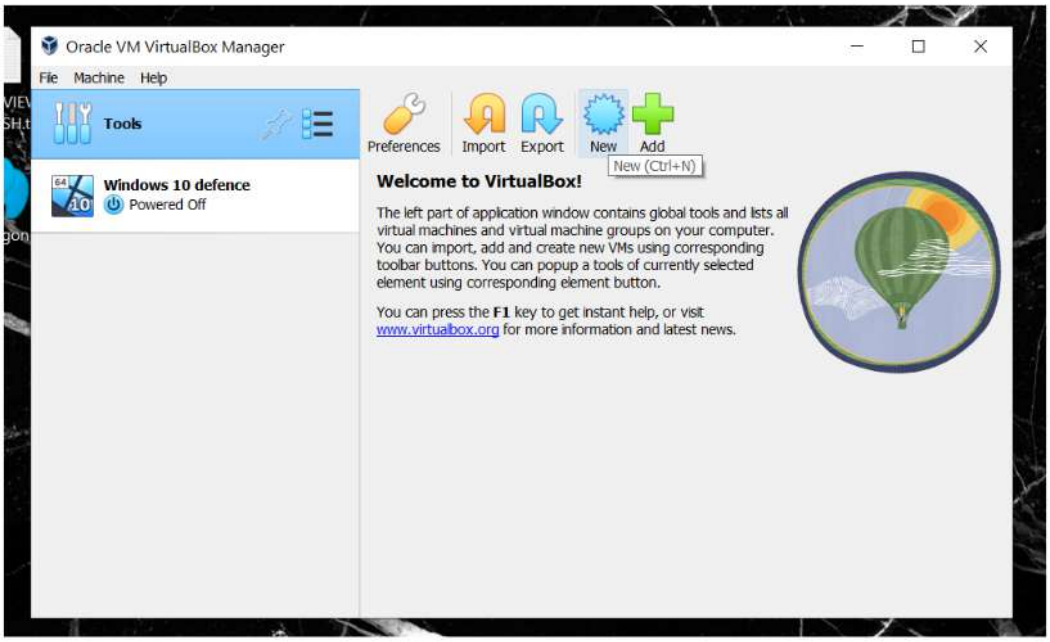
Step 5: To initiate the attack, turn off Windows Defender Wirefall.



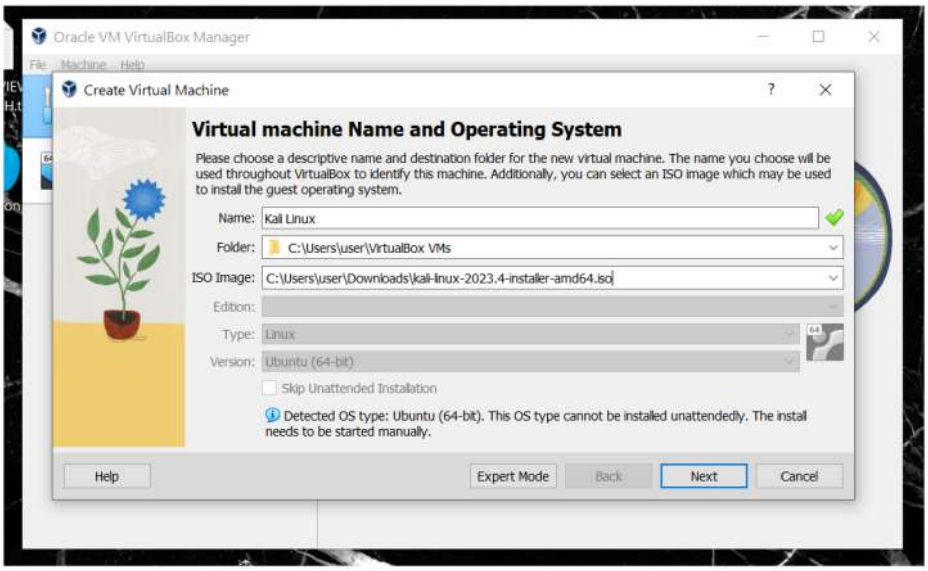
SETTING UP KALI LINUX

Step 1: Open https://www.kali.org/get-kali/#kali-installer-images Select the 64-bit installer and click to start the download.

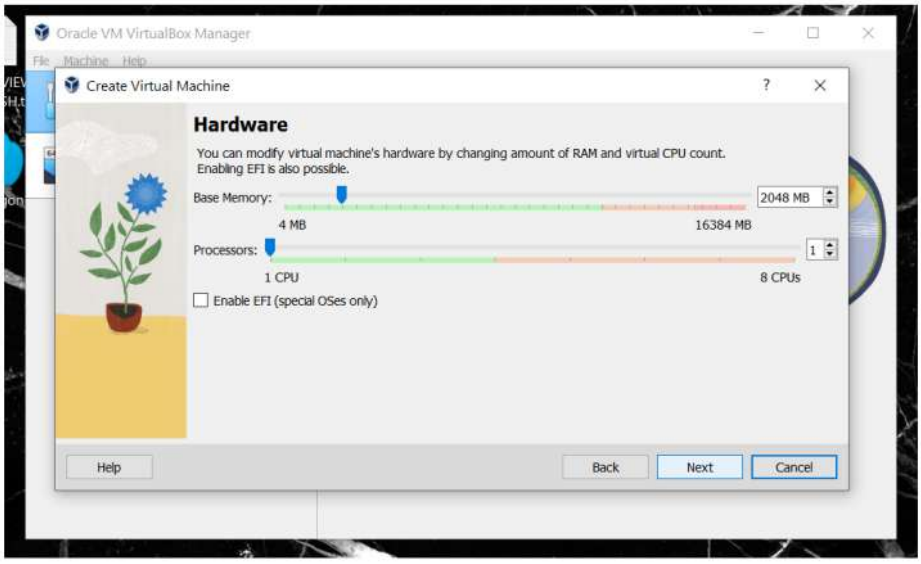
Setting up VirtualBox for Kali Linux
Step 1: Run the VM VirtualBox and click new.



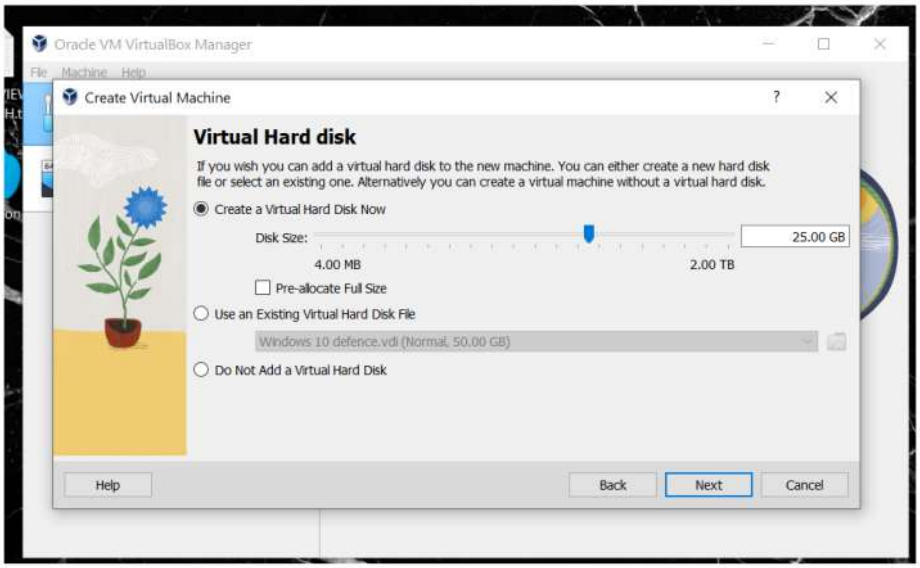
Step 2: To save a folder on Kali Linux, provide its name then, select the iso image (kali-linux-2023.4-installer-amd64.iso) saved in the download file and proceed by clicking the next button.



Step 3: Modify the virtual machine's hardware based on the device specifications, then click Next.

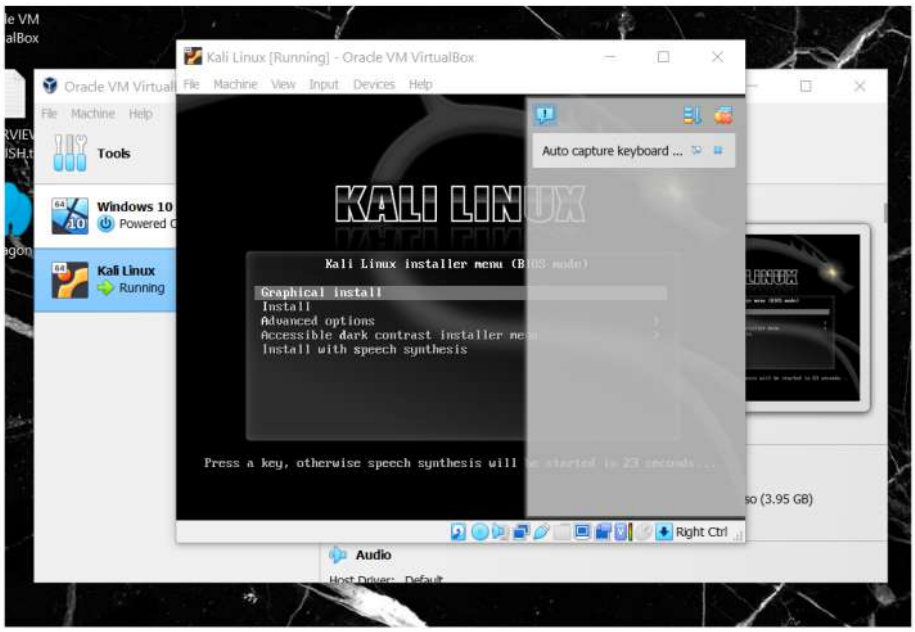


Step 4: To add a virtual hard disc or create a new one, click Next.



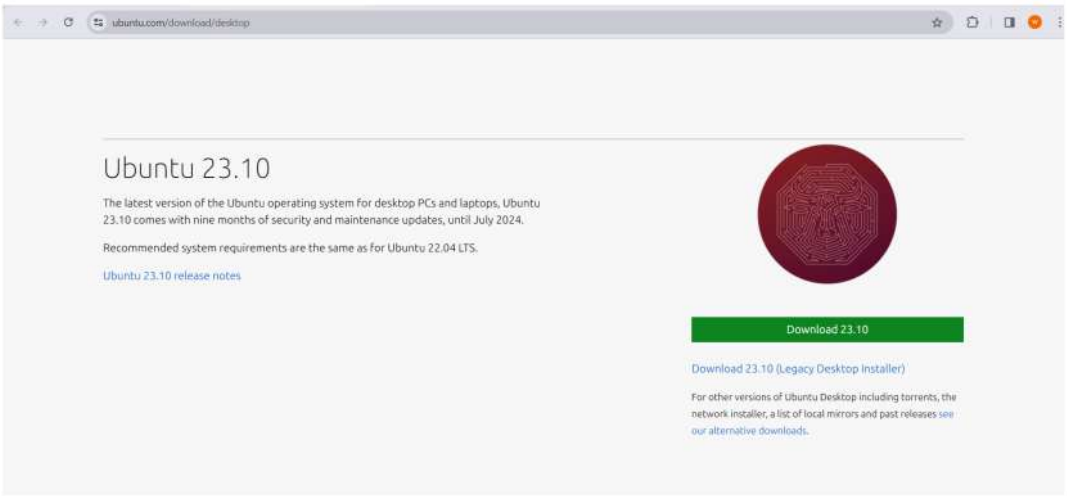
Step 5: The setup has been successfully completed.

Step 6: After the setup has been completed, users can now run Kali Linux using the virtualbox.



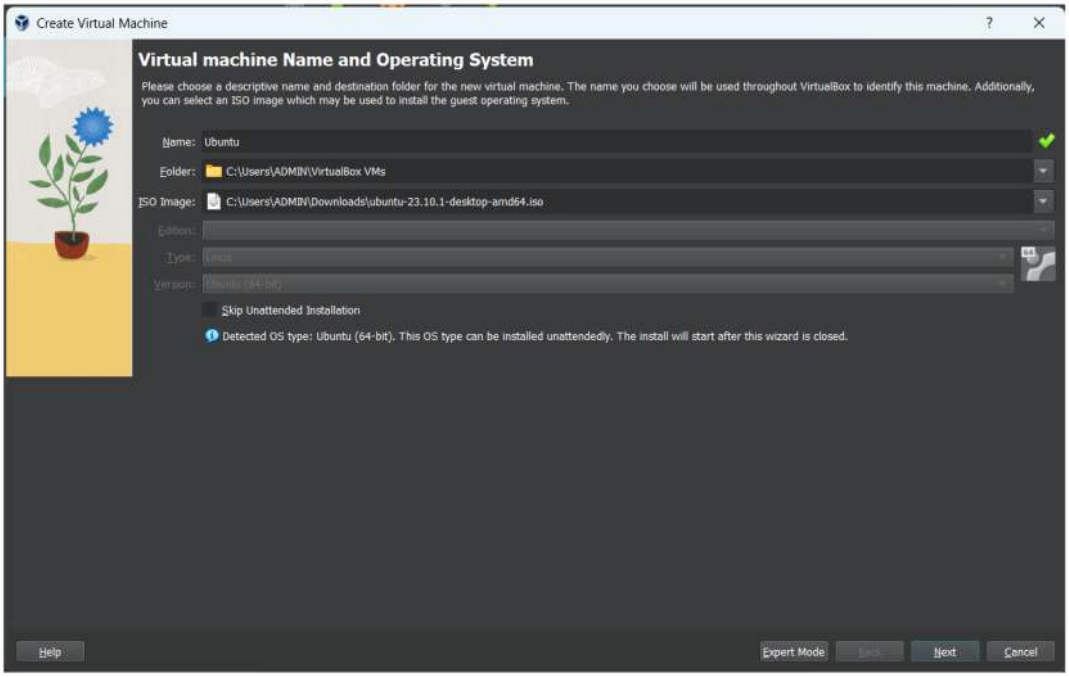
SETTING UP UBUNTU

Step 1: Download Ubuntu 23.0 through this link https://ubuntu.com/download/desktop

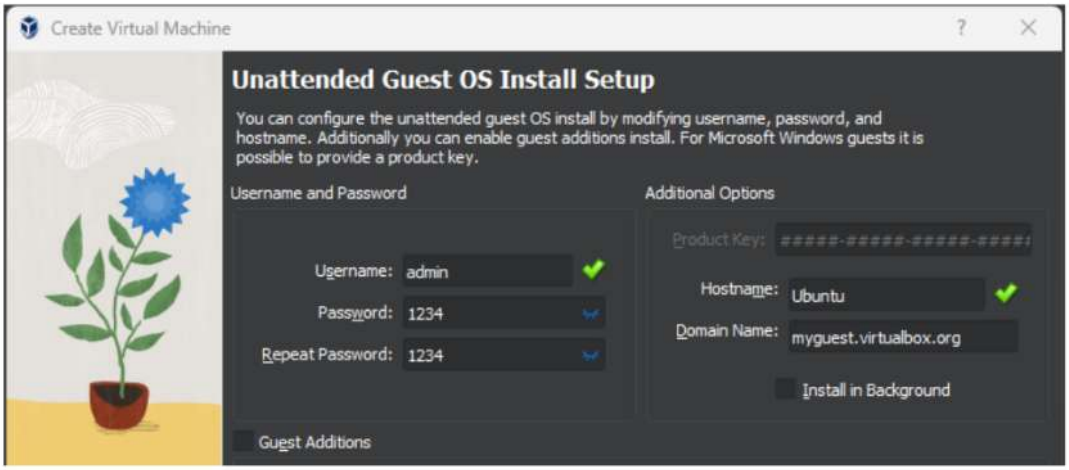


Step 2: Run the Oracle Virtual Box and click the "New" icon.

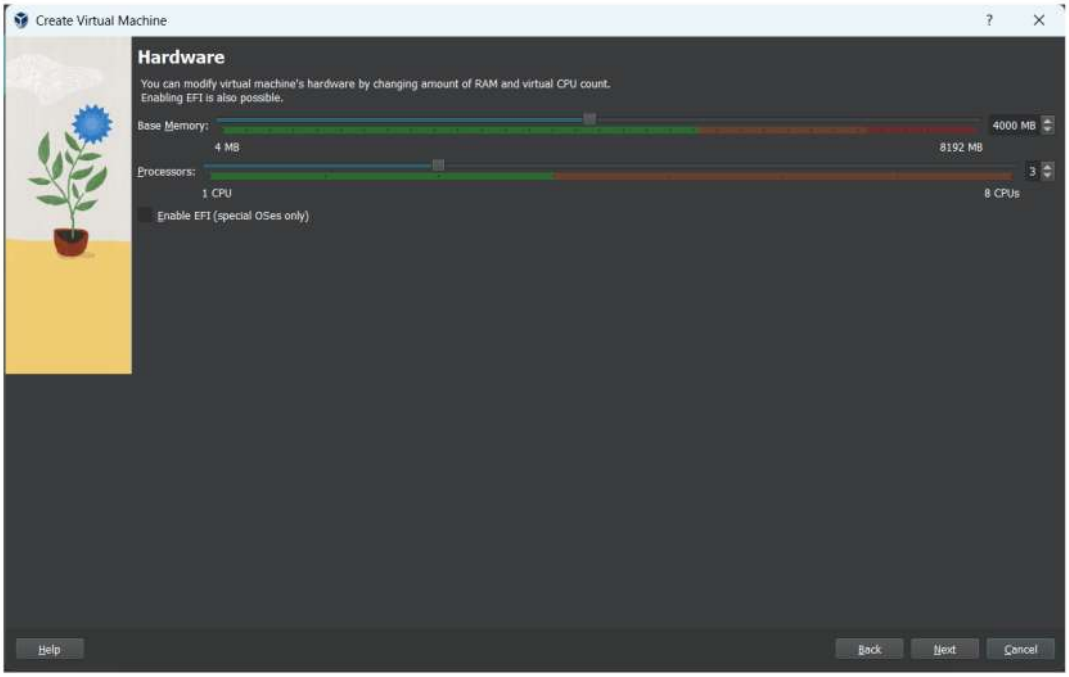
Step 3: Enter the "Ubuntu" at the Name field. Then choose the ISO image from the download file. Then, click "Next".



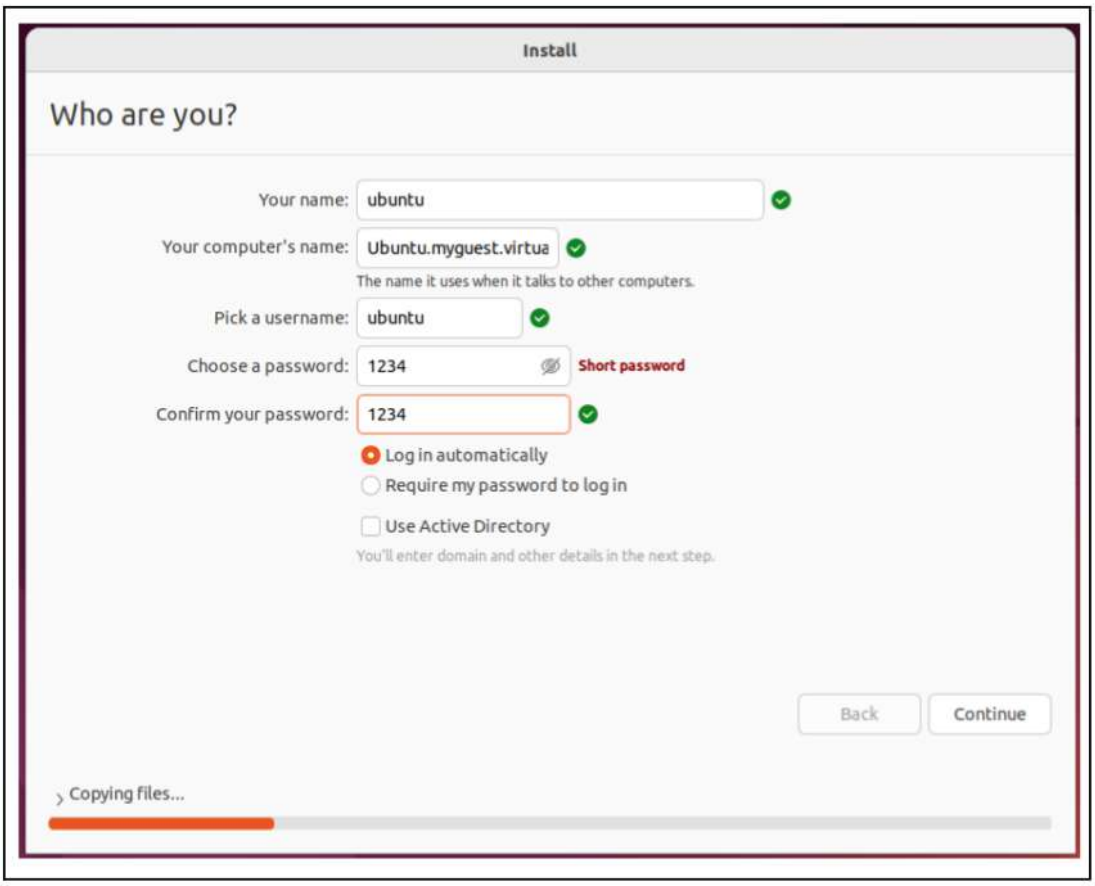
Step 4: Enter the username and password. Then, click "Next".



Step 5: Update the "Base Memory" and "Processors". After that, click the "Next" button.



Step 6: Enter a username and confirm a password same as Step 4. Then click the "Continue" button to allow the users to access Ubuntu.


Install
Who are you?
Your name:
ubuntu
Your computer's name:
Ubuntu.myguest.virtua
The name it uses when it talks to other computers.
Pick a username:
ubuntu
Choose a password:
1234
Short password
Confirm your password:
1234
Log in automatically
Require my password to log in
Use Active Directory
You'll enter domain and other details in the next step.
Back
Continue
Copying files...

ATTACK

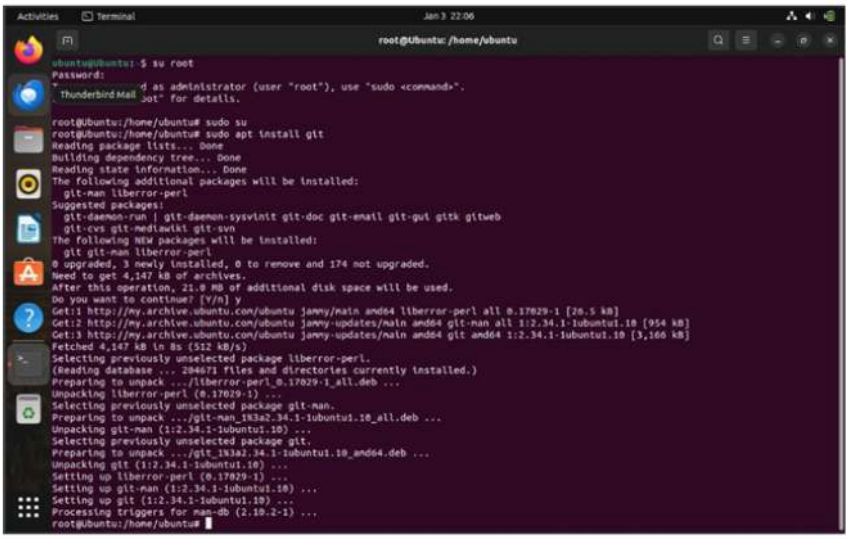
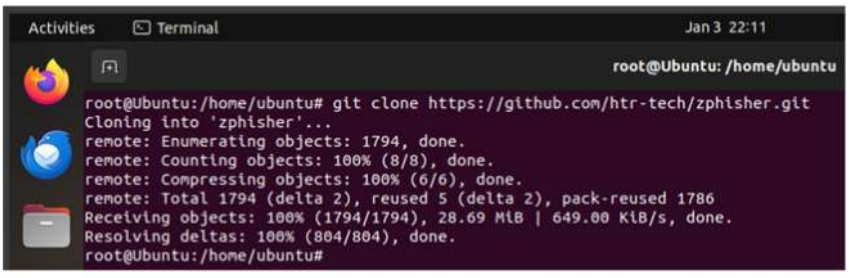
TOOLS

WINDOWS	LINUX
1. Zphisher 2. Ettercap 3. Kage 4. Slowloris 5. Cain and Abel	1. SARA 2. Storm Breaker 3. Hping3

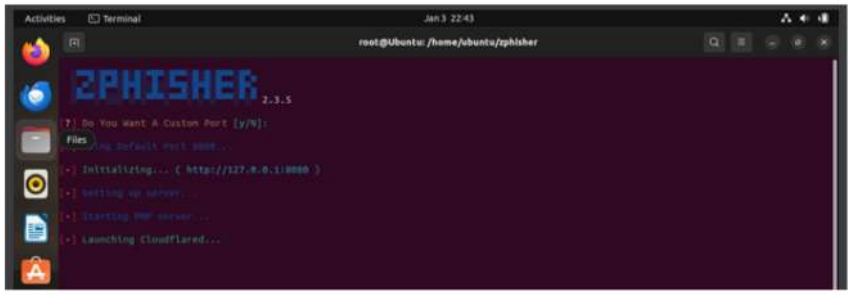
PLANNING

WINDOWS

1. Zphisher (Instagram Phishing)

Step 1: Execute the command *sudo apt install git* to install the Git package on Ubuntu.

Step 2: Utilize the "git clone" command to fetch the Zphisher tool from its GitHub repository, specifically designed for phishing purposes.

Step 3: Develop a deceptive login page mimicking Instagram for phishing purposes.

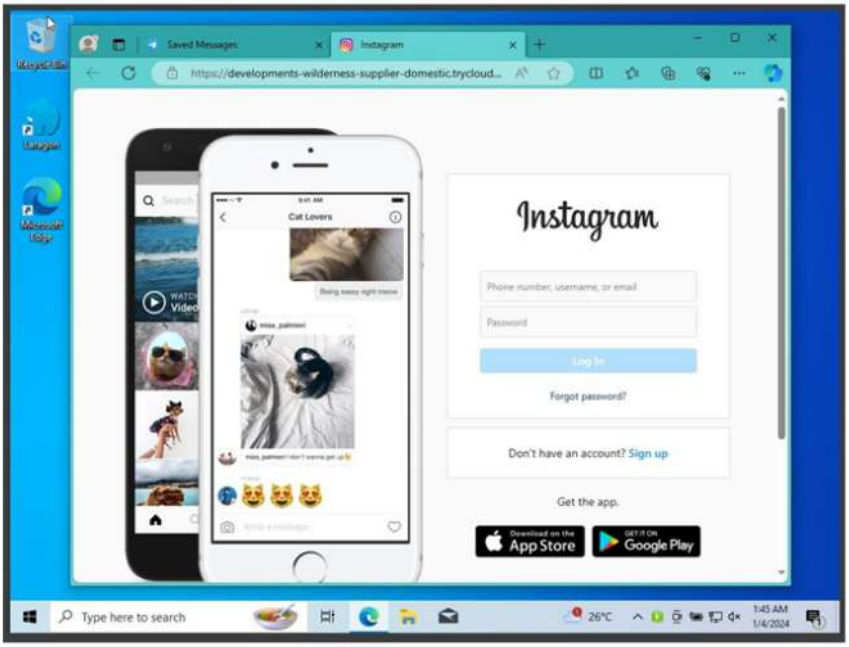
Step 4: Specify the port configuration for the phishing setup.



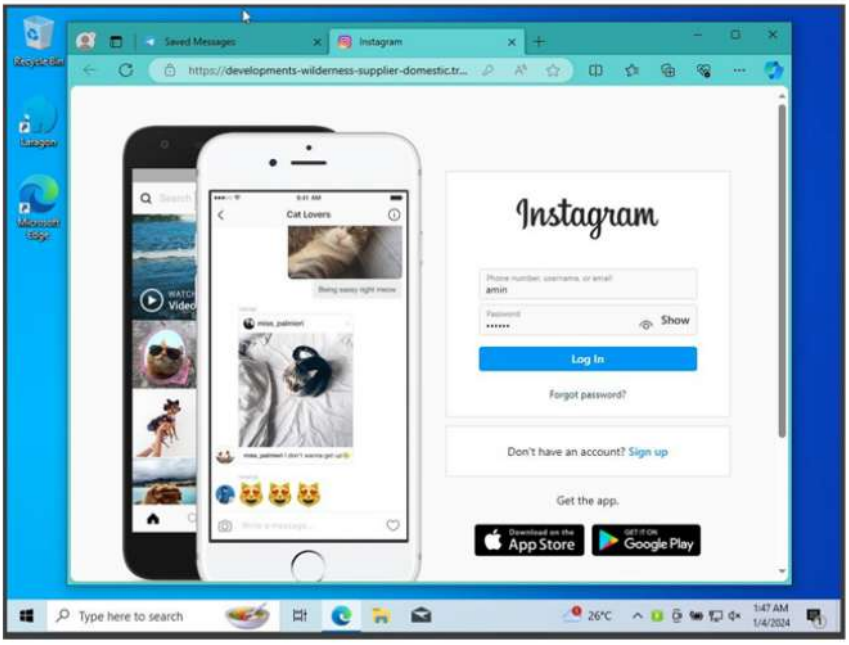
Step 5: The first URL for the phishing Instagram page has been generated.

Step 6: Upon clicking the following link: https://developments-wilderness-supplier-domestic.trycloudflare.com/login.ht

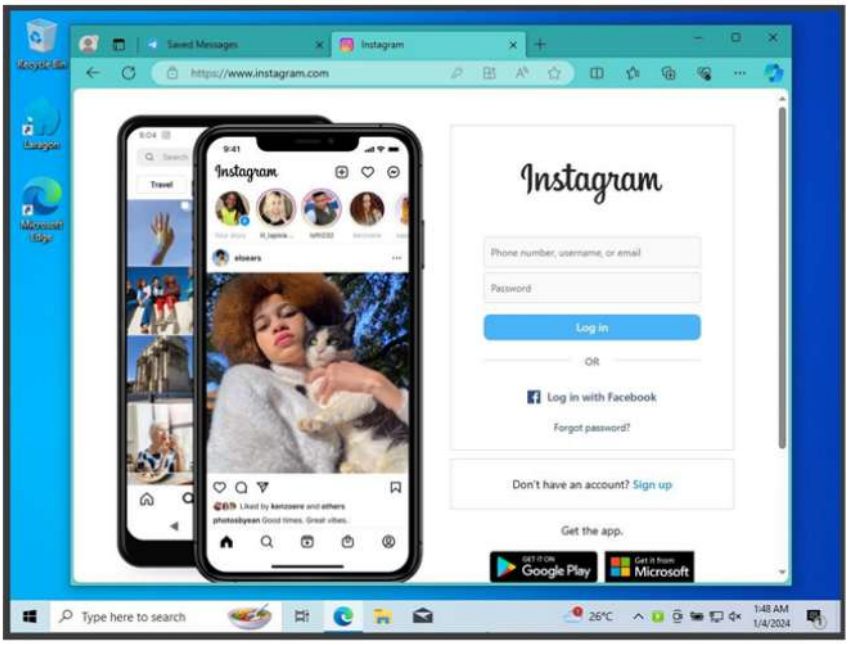
ml, users will be redirected to the phishing Instagram login page.



Step 7: Users are prompted to input their login credentials, including username and password, and subsequently click the login button.



Step 8: Upon clicking the login button on the phishing page, the user will be redirected to the authentic Instagram login page.



Step 9: While the user logs in on the phishing Instagram page from a Windows 10 machine, the entered credentials are saved in the "auth/ip.txt" file on the attacker's Ubuntu machine.

2. Ettercap

Step 1: Install Ettercap on Kali Linux by executing the command: *sudo apt install ettercap-graphical*.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ettercap-graphical
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
ettercap-graphical is already the newest version (1:0.8.3.1-11).
ettercap-graphical set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 764 not upgraded.
```

Step 2: After the installation is finished, go to the Ettercap directory by typing *cd /etc/ettercap*.

Step 3: Display all folders in the Ettercap directory by typing *ls*.

Step 4: Subsequently, open the file named *etter.conf* using the command *nano etter.conf*. In this file, modify the *ec_uid* and *ec_gid* lines to have the value 0.

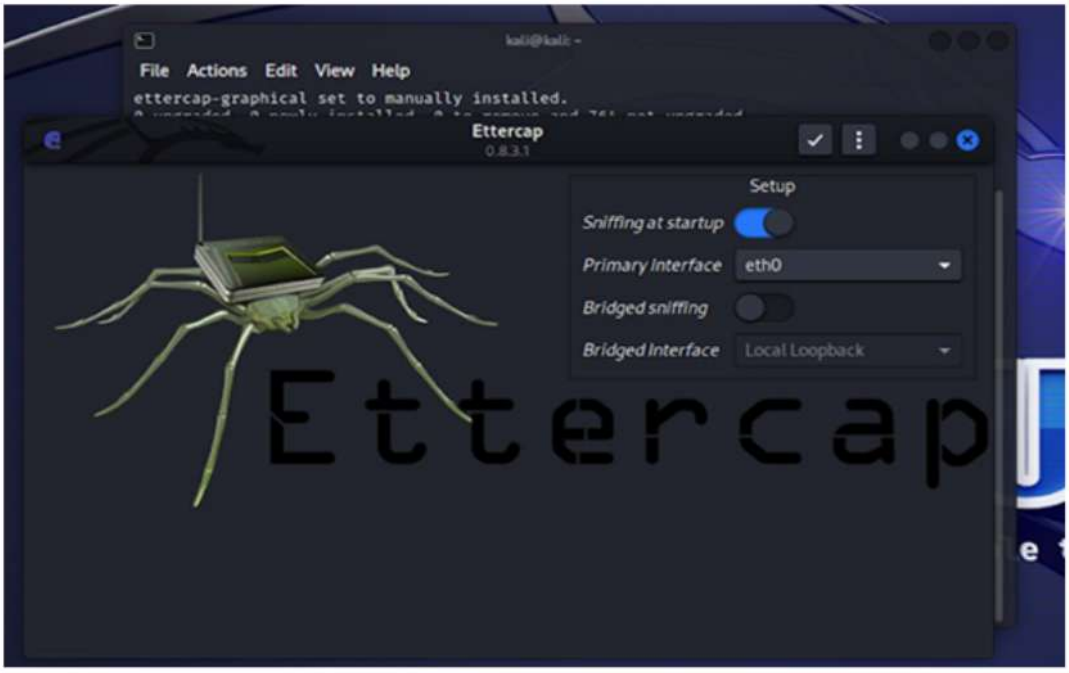
Step 5: Save the changes to the settings.

```
┌──(kali㉿kali)-[~]
└─$ cd /etc/ettercap

┌──(kali㉿kali)-[/etc/ettercap]
└─$ ls
etter.conf  etter.dns  etter.mdns  etter.nbns

┌──(kali㉿kali)-[/etc/ettercap]
└─$ sudo nano etter.conf
```

Step 6: Once the configuration is done, initiate Ettercap by using the command *sudo ettercap-G*.

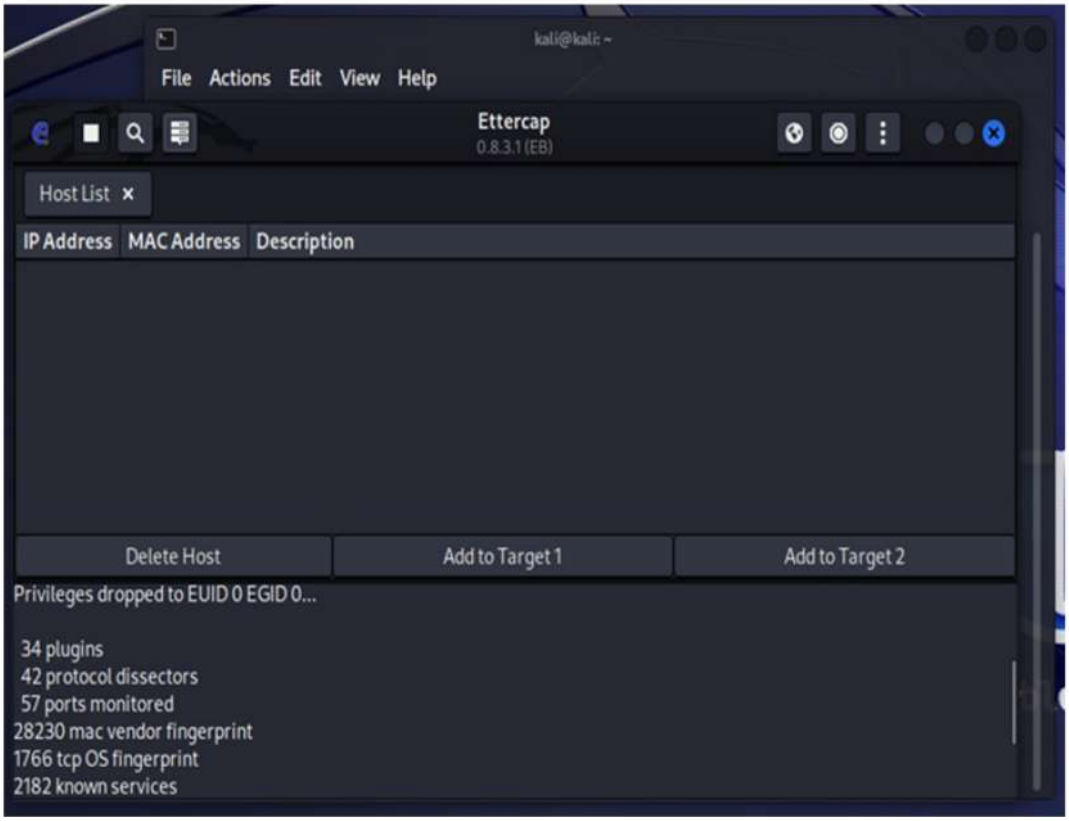
```
┌──(kali㉿kali)-[~]
└─$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team


(ettercap:4721): GLib-WARNING **: 09:46:02.095: In call to g_spawn_sync(), wait status o
f a child process was requested but ECHILD was received by waitpid(). See the documentat
ion of g_child_watch_source_new() for possible causes.
```

Step 7: Select the primary interface as eth0 and click the Accept button to proceed.

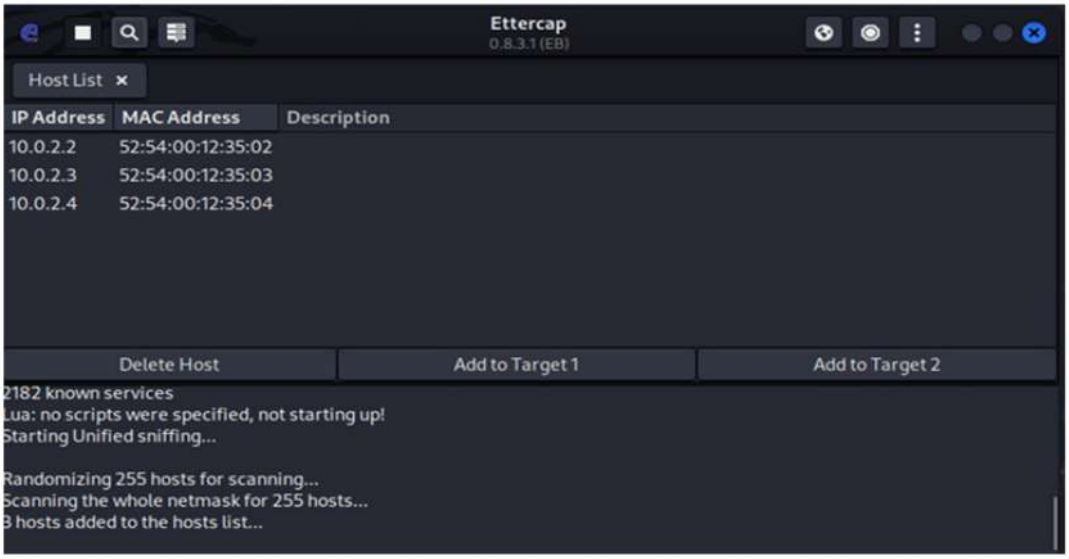


Step 8: Access the host list panel by clicking on the host list icon, which is the fourth button from the left.

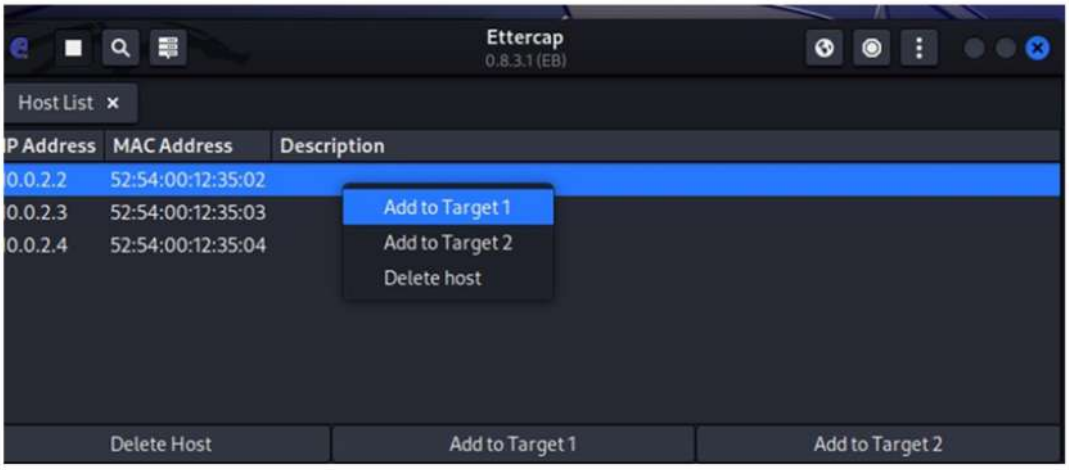
Step 9: Perform a host scan by clicking on the Scan for Hosts button, located as the third button from the left.

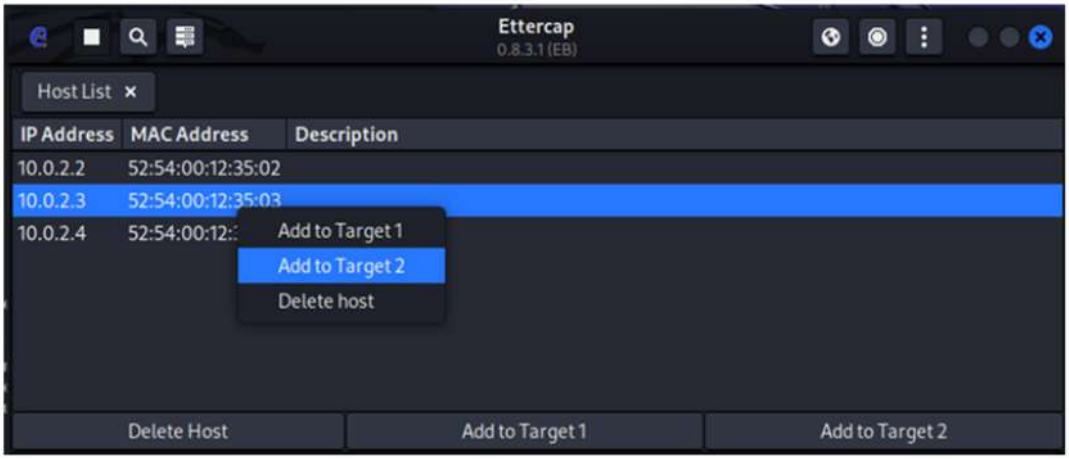


Step 10: Confirm that the host lists are now visible on the screen.



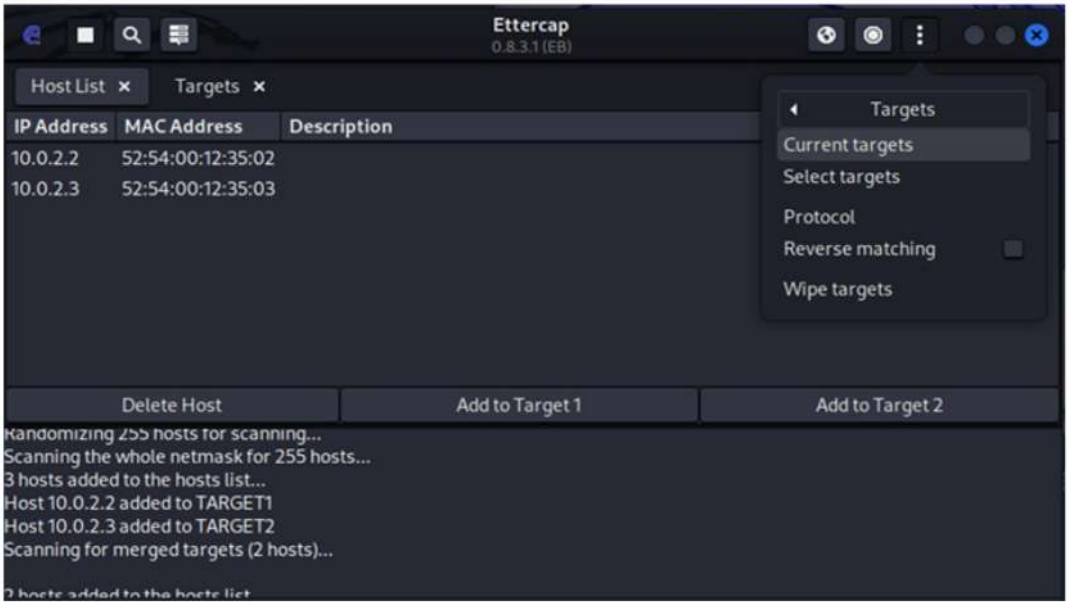
Step 11: Choose the IP addresses from the host lists and assign them as Target 1 and Target 2.

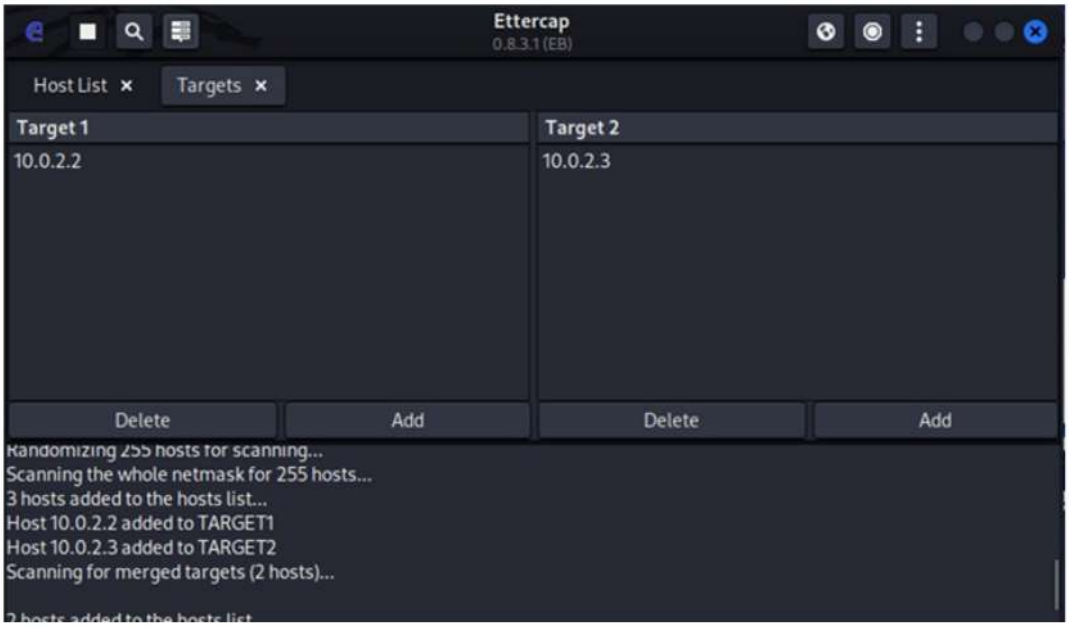




Step 12: Once the targets are selected, open the Targets panel to review the chosen IP addresses.

Step 13: Navigate to the Ettercap menu, select Targets, and then choose Current Target.





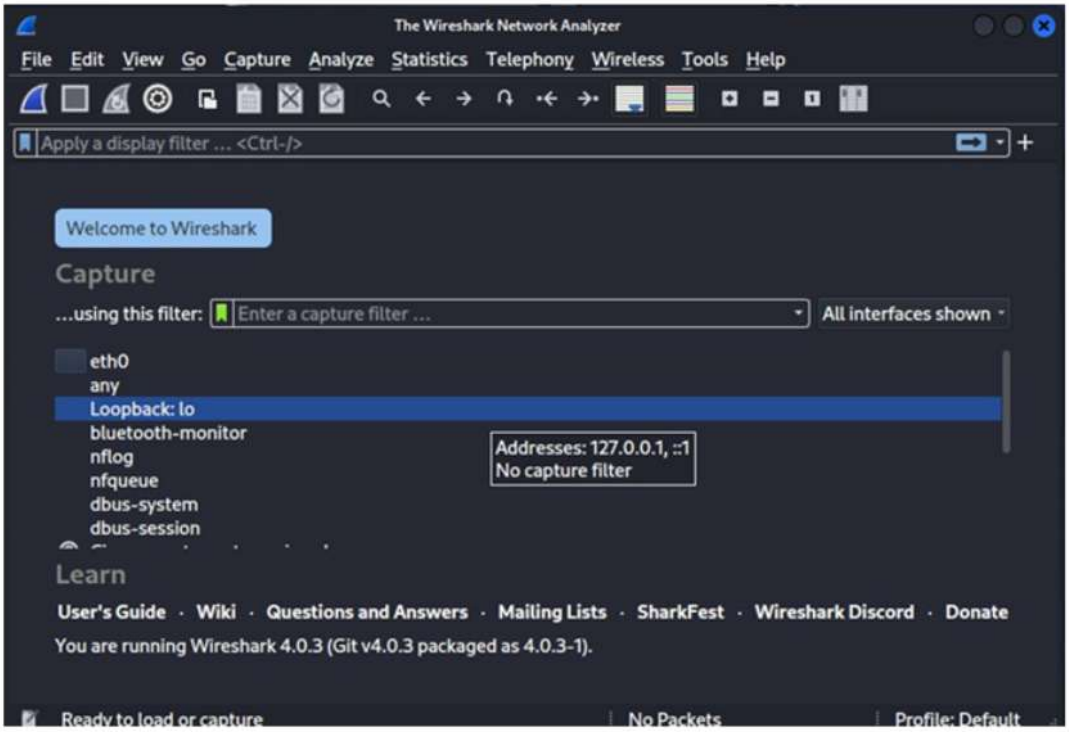
Step 14: Open a new terminal and check the value of ip_forward by typing

cat /proc/sys/net/ipv4/ip_forward.

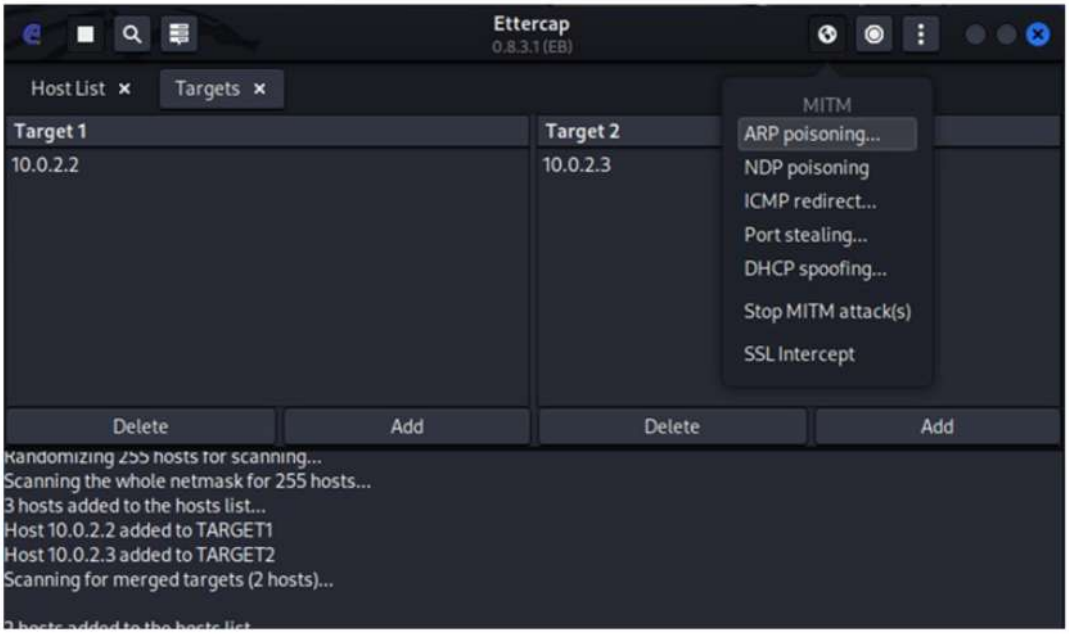
Step 15: Open a new terminal and set the ip_forward value to 1 by entering the command *echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward*.

Step 16: If prompted, provide your password. Following that, initiate Wireshark by executing the command *wireshark &*.

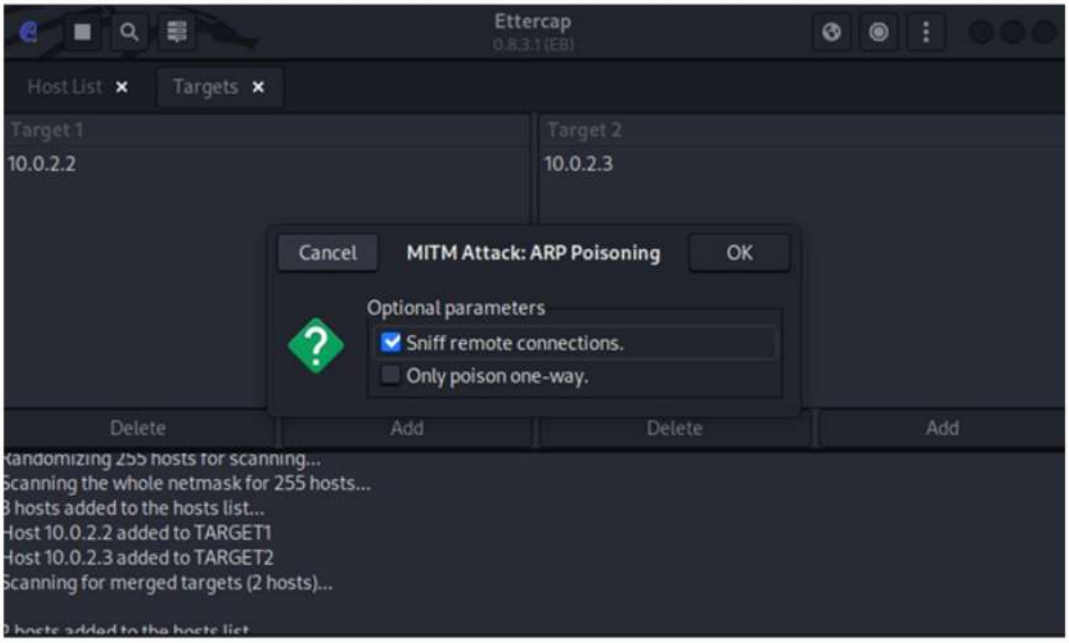
Step 17: Once Wireshark is open, choose the eth0 network interface to capture the network traffic.



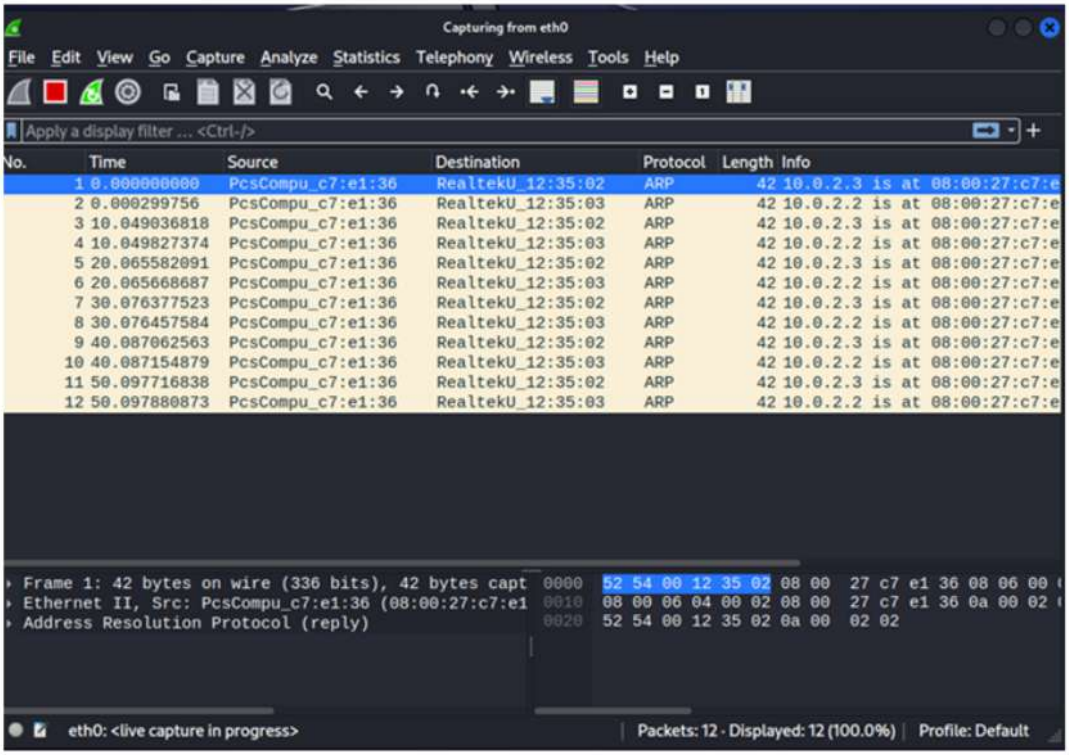
Step 18: Go to the MITM (Man-in-the-Middle) button, located as the third button from the right, and click on ARP Poisoning.



Step 19: Select "Sniff remote connections" and click OK to commence ARP poisoning in the network.

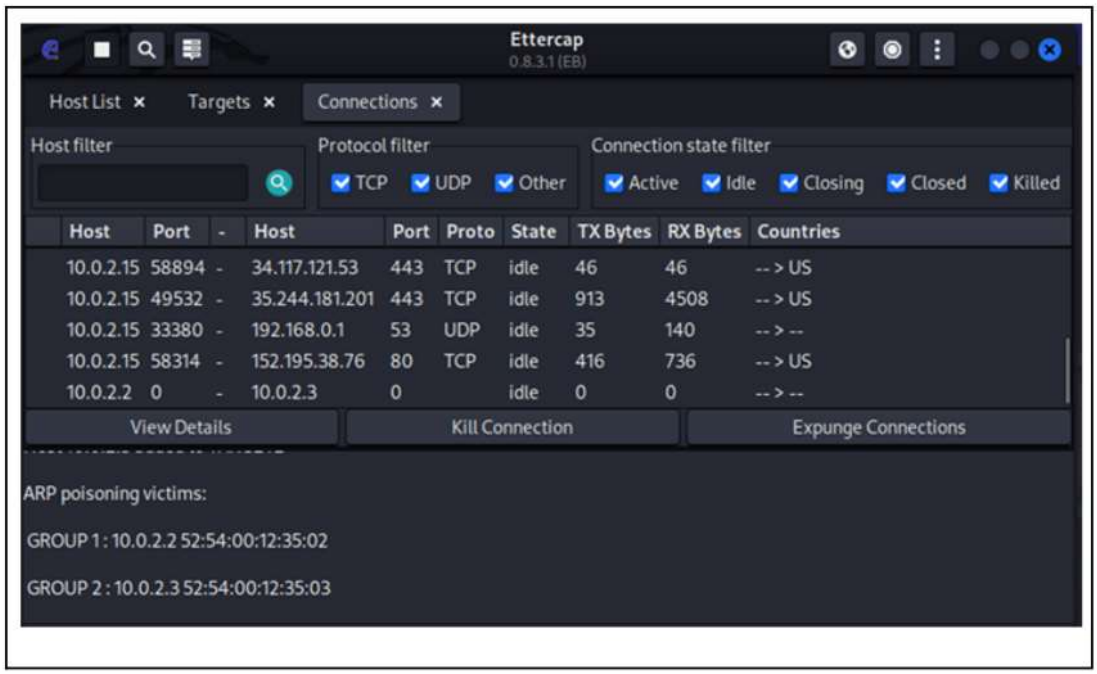


Step 20: As ARP poisoning commences, multiple ARP messages are broadcasted to the network, leading to confusion among various IP addresses.



Step 21: Examine the target's active connections by opening the connection.

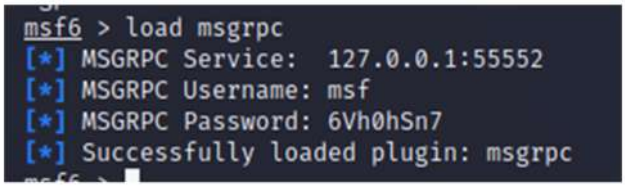
Step 22: Click on the connection and observe the sent information on the left and the received information on the right, provided the packets are not encrypted.

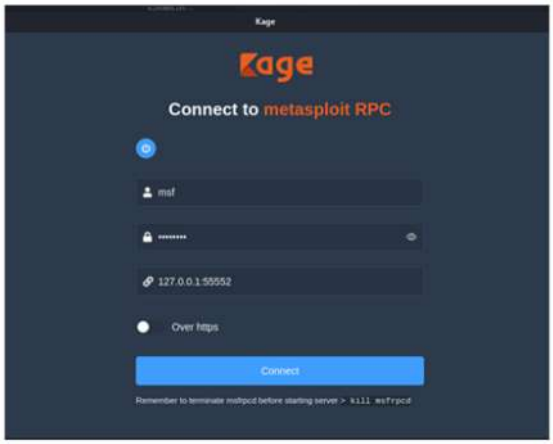

Ettercap
0.8.3.1 (EB)
Host List ×
Targets ×
Connections ×
Host filter
Protocol filter
TCP
UDP
Other
Connection state filter
Active
Idle
Closing
Closed
Killed
Host Port - Host Port Proto State TX Bytes RX Bytes Countries
10.0.2.15 58894 - 34.117.121.53 443 TCP idle 46 46 -- > US
10.0.2.15 49532 - 35.244.181.201 443 TCP idle 913 4508 -- > US
10.0.2.15 33380 - 192.168.0.1 53 UDP idle 35 140 -- > --
10.0.2.15 58314 - 152.195.38.76 80 TCP idle 416 736 -- > US
10.0.2.2 0 - 10.0.2.3 0 idle 0 0 -- > --
View Details
Kill Connection
Expunge Connections
ARP poisoning victims:
GROUP 1 : 10.0.2.2 52:54:00:12:35:02
GROUP 2 : 10.0.2.3 52:54:00:12:35:03

3. Kage

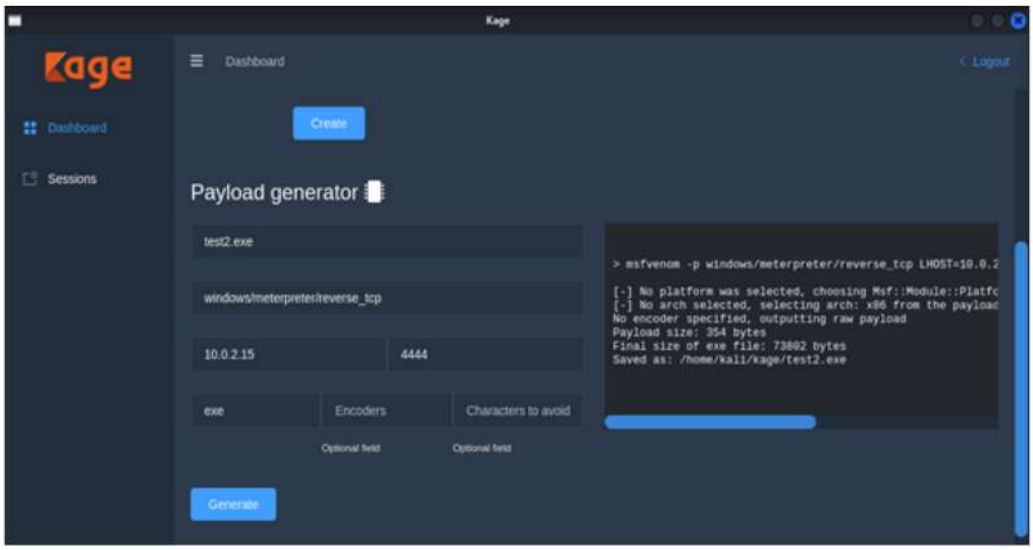
Step 1: Install Ettercap on Kali Linux by executing the command: *sudo apt install ettercap-graphical*.

Step 2: Execute *msgrpc* to obtain the username and password required for logging into Kage.

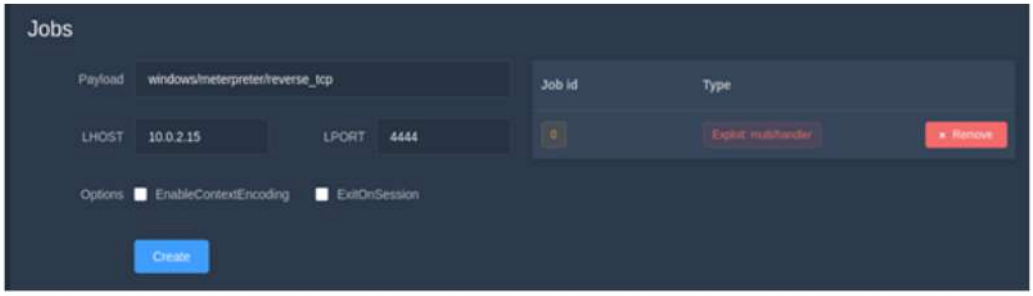




Step 3: After logging in, proceed to create a new botnet through the payload generator. Here, we'll craft the test2.exe botnet for our use.



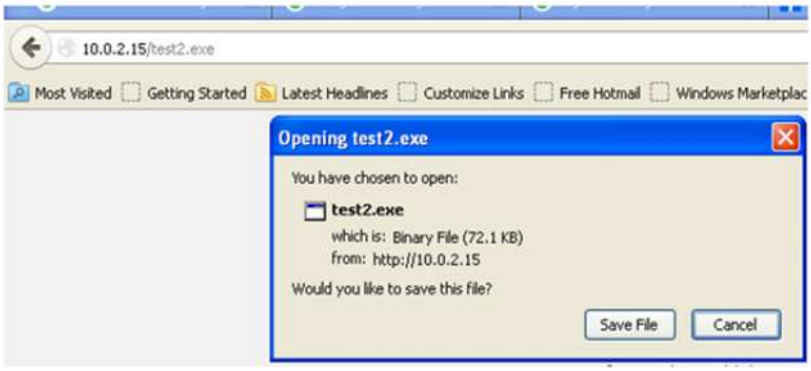
Step 4: Furthermore, navigate to the Jobs section in Kage to configure the payload, lhost, and lport for exploitation.



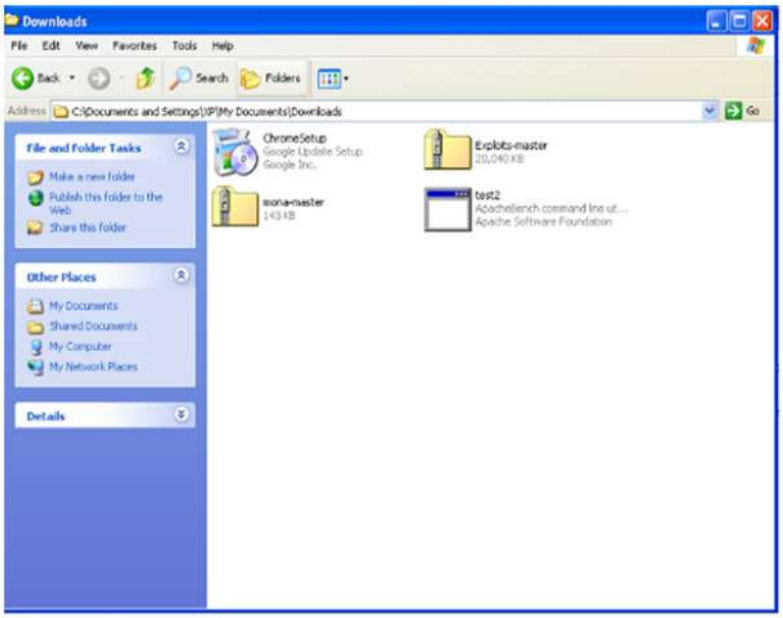
Step 5: Subsequently, initiate the Apache service after transferring the botnet to HTML. This action allows the victim to establish a connection with the attacker's botnet.

```
┌──(kali㉿kali)-[~]
└─$ sudo mv /home/kali/kage/test2.exe /var/www/html/

┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
```

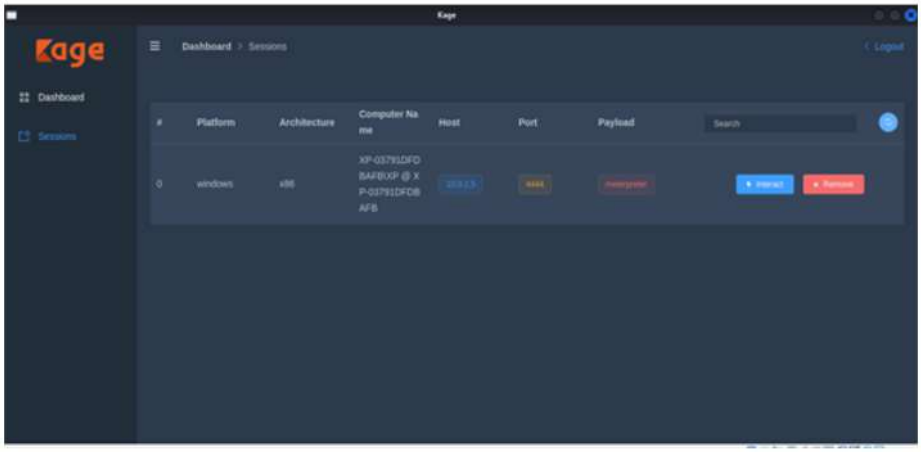
Step 6: Download the file onto the Windows XP system using the attacker's IP address.



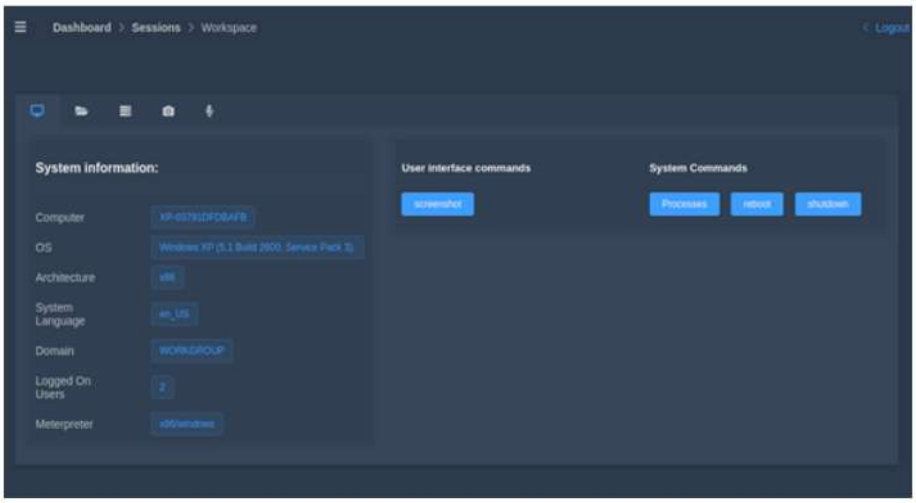
Step 7: You can now inspect the contents of the file and execute it as needed.



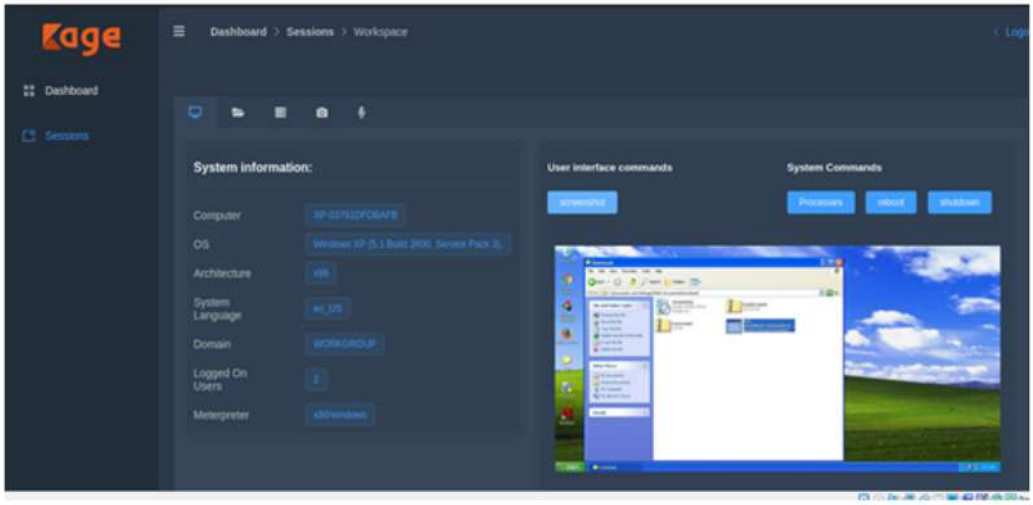
Step 8: Upon establishing a connection with the victim, a new platform will be visible in the session area upon returning to Kage. To actively engage with the victim, proceed by pressing the interact button.



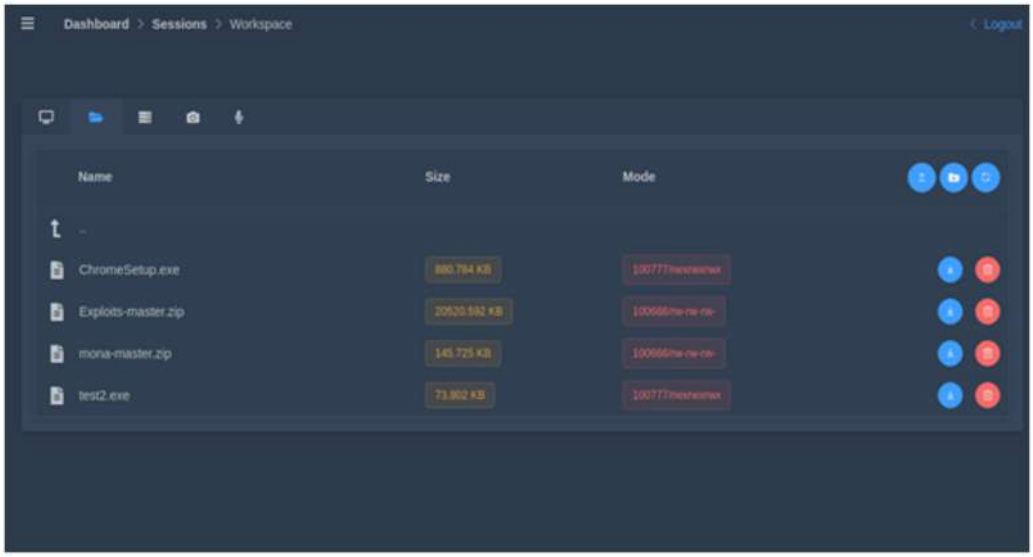
Step 9: At this stage, you can examine the victim's system data on the left and execute commands on the right.



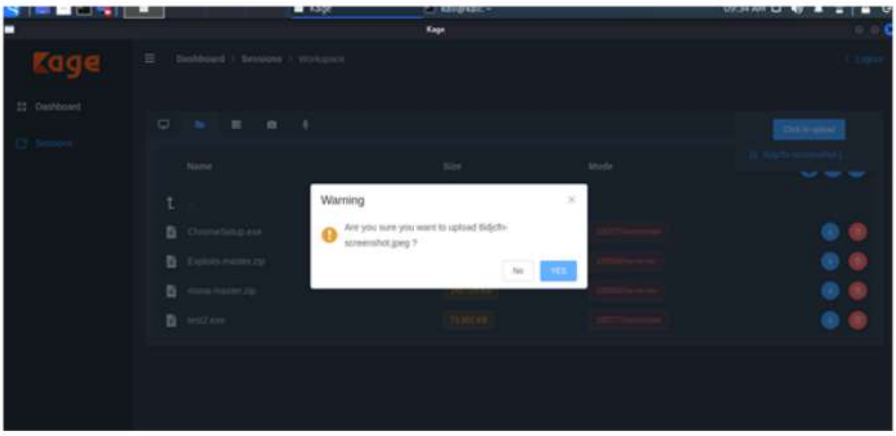
Step 10: Utilizing the "snapshot" command, we have the capability to capture a screenshot of the entire victim's user interface.

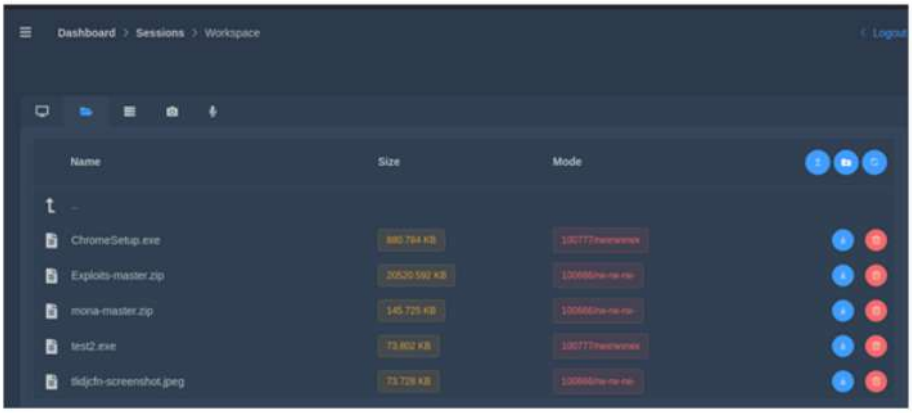


Step 11: Navigate to the second folder resembling a logo to access the file management feature. In this section, you can view all files present in the entire location of the botnet.



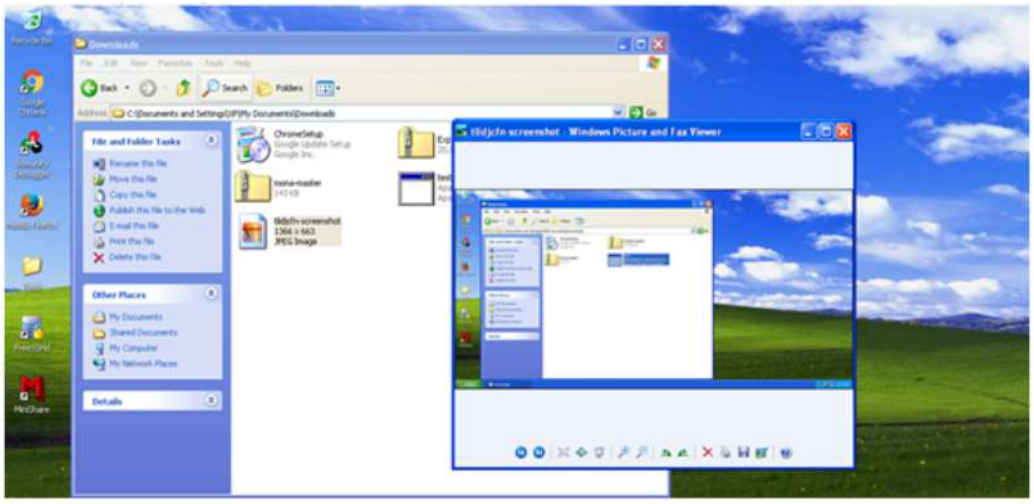
Step 12: You can now submit the screenshot we just captured. Additionally, it's evident that Kage has successfully uploaded the screenshot to the designated folder.





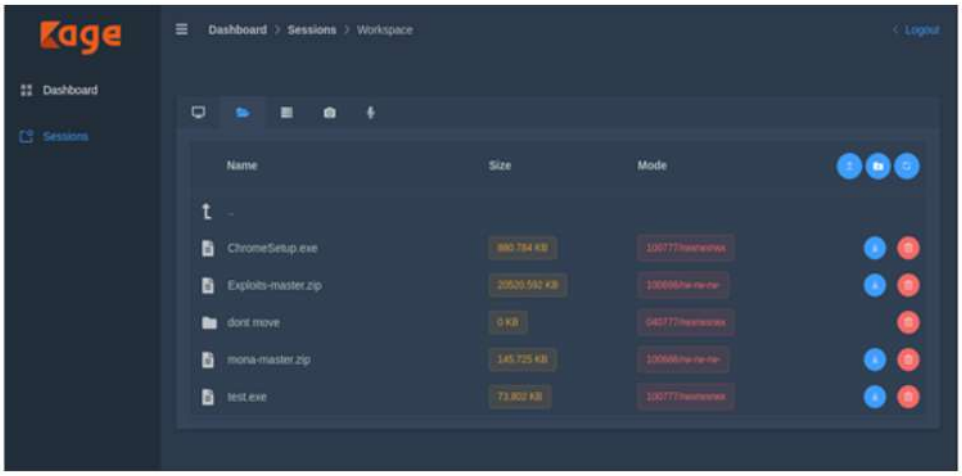
Step 13: After the initial attempt, check the results on Windows XP, confirming the successful relocation of the screenshot to a new location.

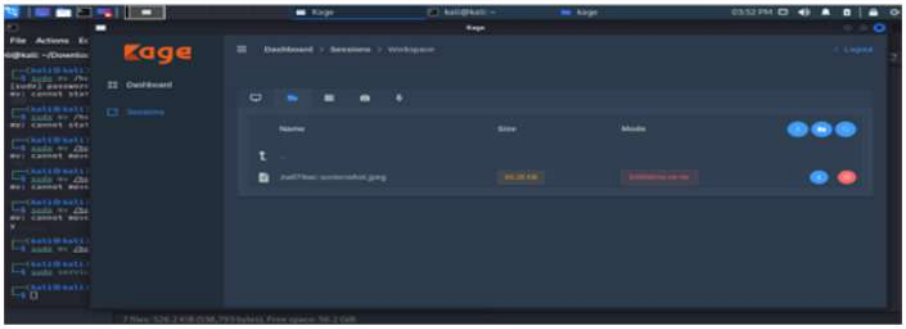
Step 14: Verify that the content of the screenshot within the new location corresponds to the one captured by Kage.



Step 15: Delete the previous botnet file and create a new one named test.exe to establish a connection as before.

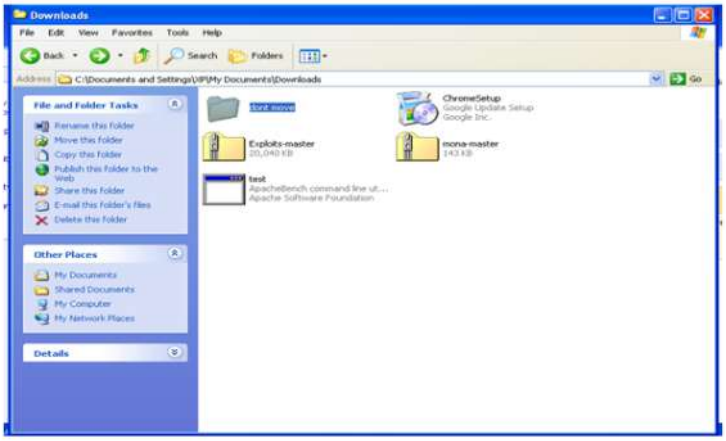
Step 16: Use Kage to create a *don't move* folder and paste another screenshot inside it.

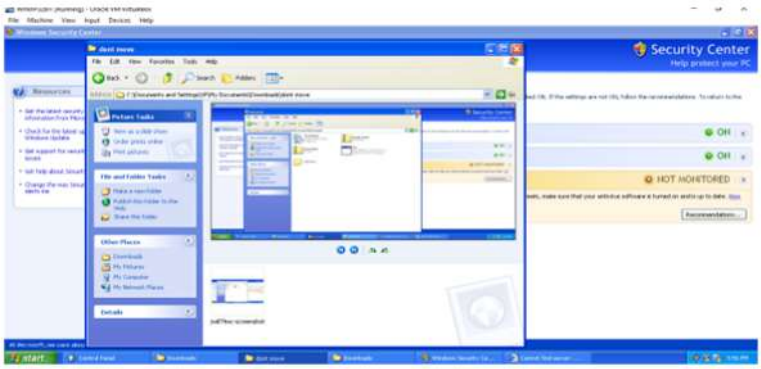




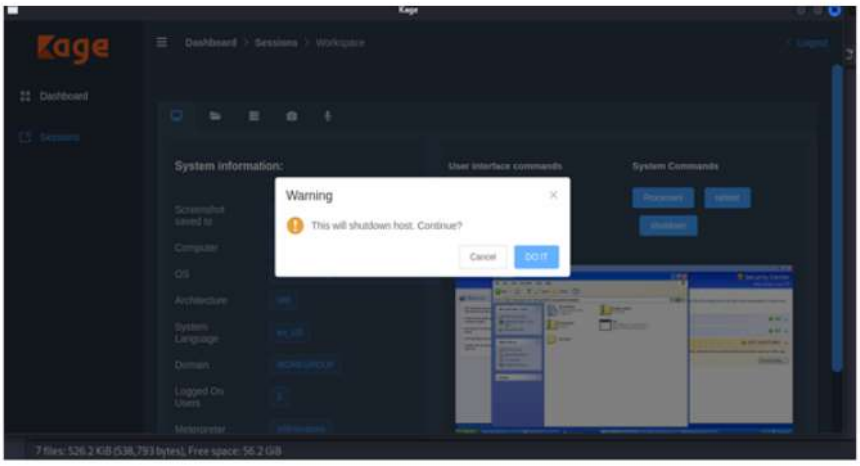
Step 17: Confirm the presence of the "don't move" file in the victim folder.

Step 18: Observe the snapshot provided by the attacker upon accessing the folder, demonstrating the successful execution of the second trial.

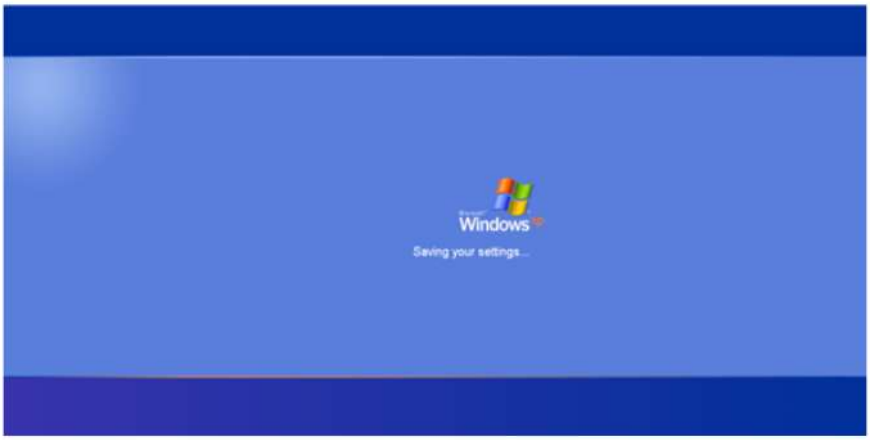




Step 19: Additionally, perform a shutdown command test to assess whether the machine responds by shutting down as expected.



Step 20: As a result, both the victim's (Windows XP) and the attacker's machines were successfully shut down in response to the test.

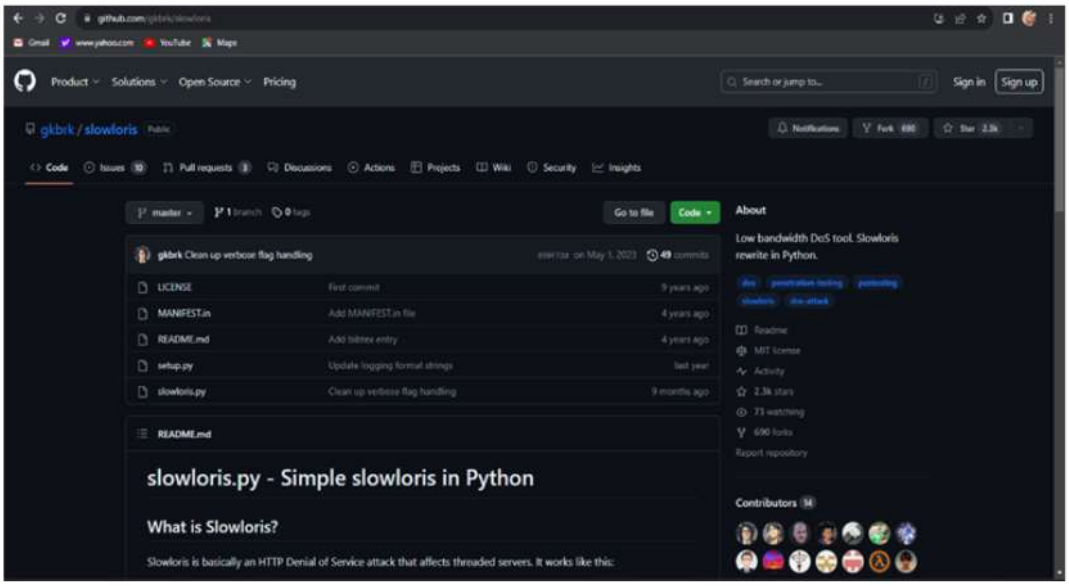


As a result, we can observe that Kage is useful for conducting botnets on a variety of operating systems, including Windows XP. It shows how Kage may use it to view the victim's system information, take a screenshot of the victim's current screen, create a folder and file within the victim's folder, and shut down the victim's PC.

4. Slowloris

Step 1: Open your web browser and navigate to the Slowloris GitHub repository using the following link: *https://github.com/gkbrk/slowloris*.

Step 2: Press the green Code button and copy the HTTPS link from the provided options.

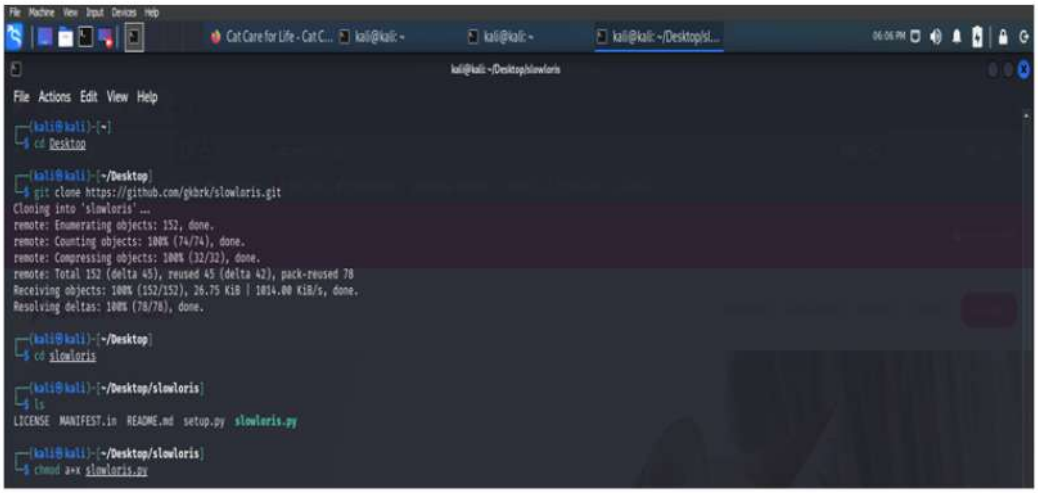


Step 3: Launch the Kali Linux terminal and enter the command *cd Desktop* to navigate to the desktop directory.

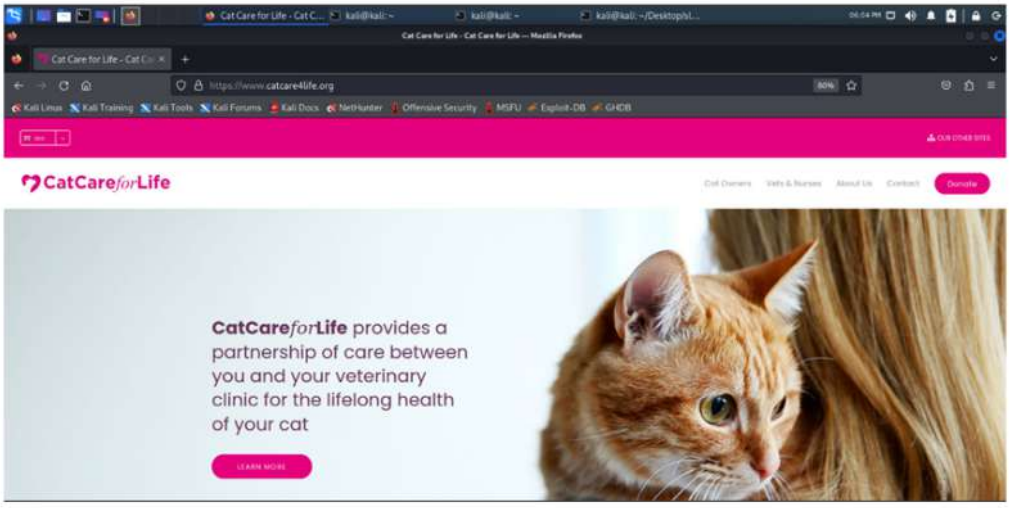
Step 4: Enter the command *git clone*, followed by pasting the previously copied link.

Step 5: Issue the command *cd slowloris* to enter the Slowloris directory. Subsequently, utilize the *ls* command to view the contents of files in the Slowloris directory.

Step 6: Next, input *chmod a+x slowloris.py* to grant execution permission to the slowloris.py file for all users.

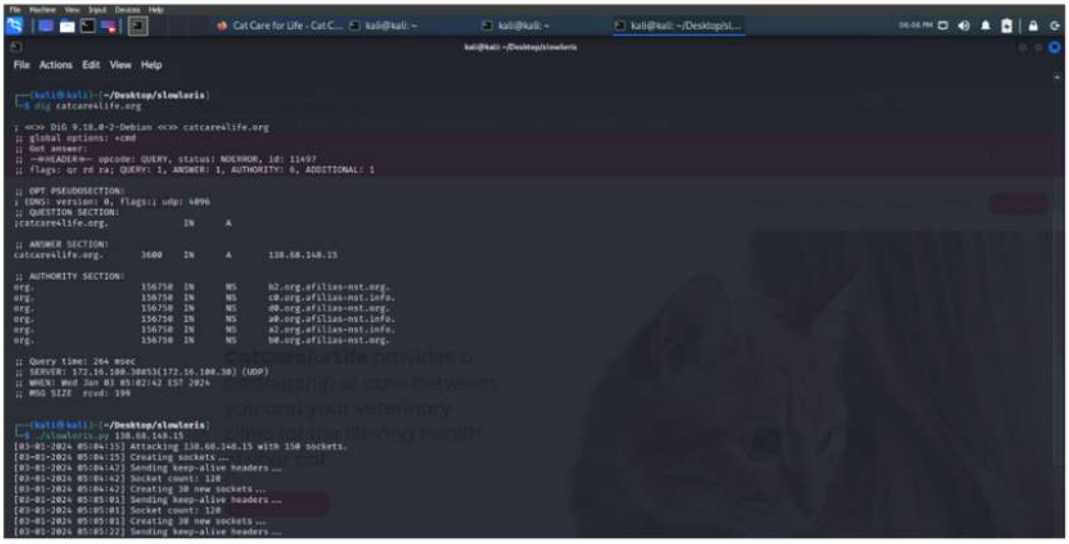


Step 7: catcare4life.org is the website we want to attack.

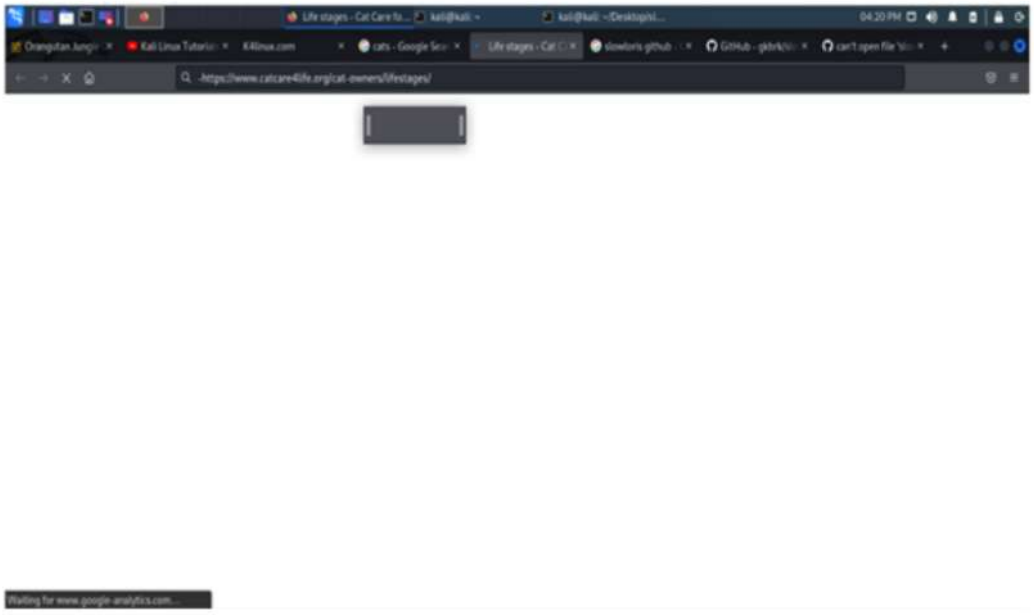


Step 8: Enter "dig catcare4life.org" in the terminal to discover its IP address.

Step 9: Now, execute *./slowloris.py 138.68.148.15*, where 138.68.148.15 is the IP address of the target website to initiate the attack.

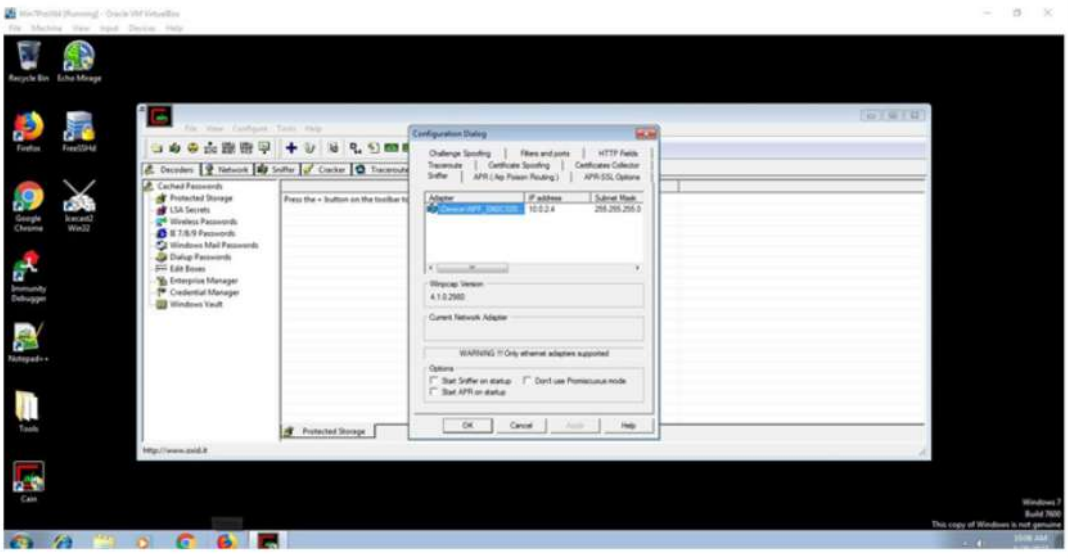


Step 10: Step 9: Confirm the success of the attack by attempting to access the website again. If the site remains unreachable, it indicates that the attack was successful in temporarily taking down catcare4life.org.

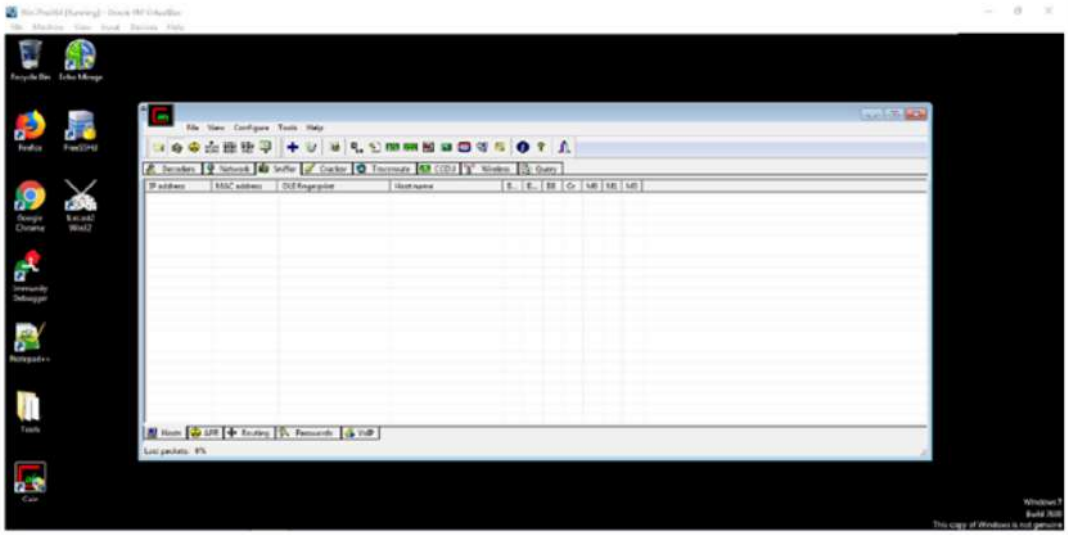


5. Cain and Abel

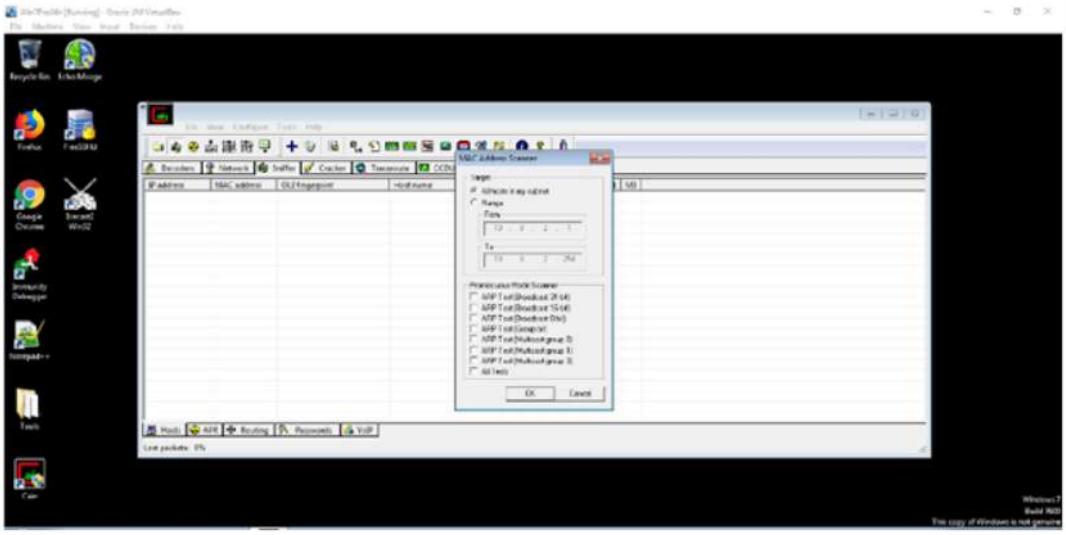
Step 1: Install the LOIC software on your PC's Windows.

Step 2: As soon as it launched, the network setup was established and the wireless network interface was selected. Then, click the Sniffer and Hosts buttons.


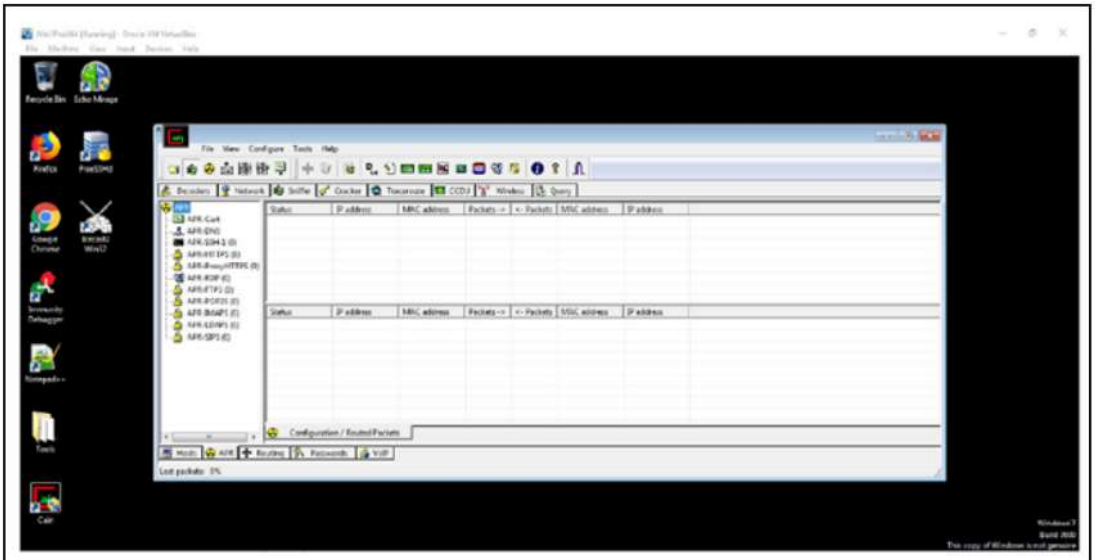
Step 3: Click on the plus sign symbol.



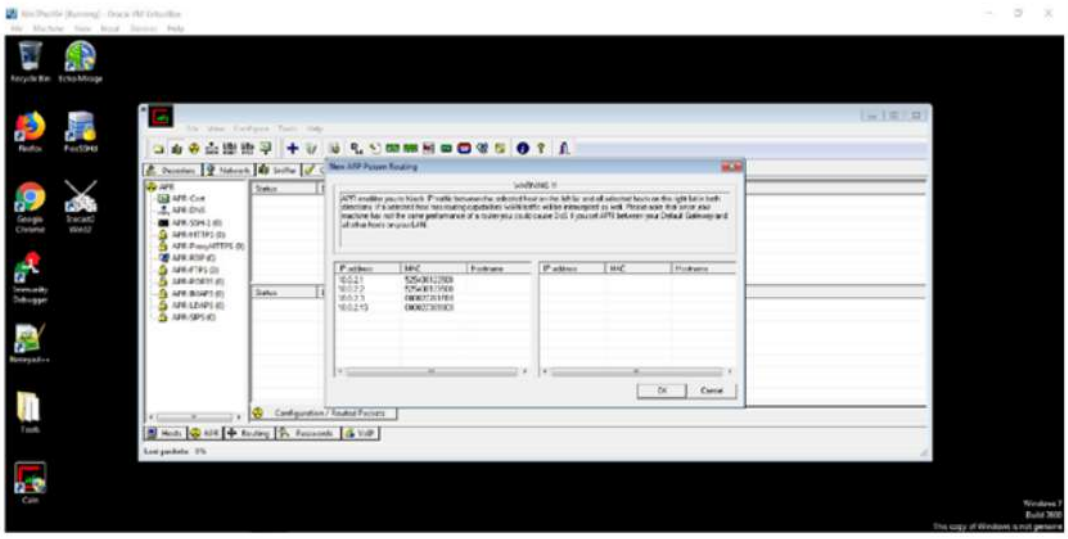
Step 4: Subsequently, click the OK button to verify that all settings are in their default positions and that our network's IP address has been accurately acquired.



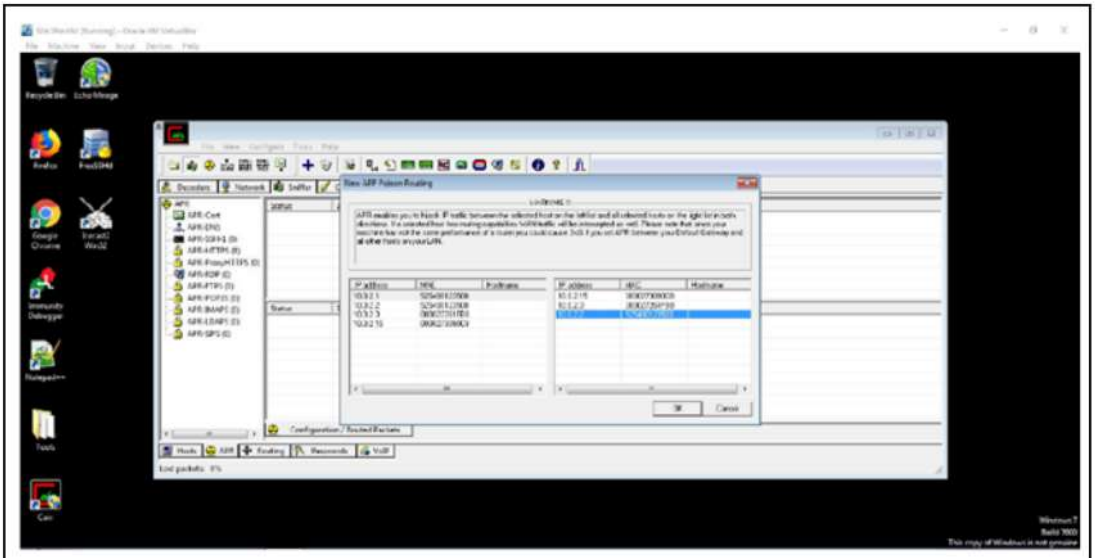
Step 5: Select APR from the list of tabs below.



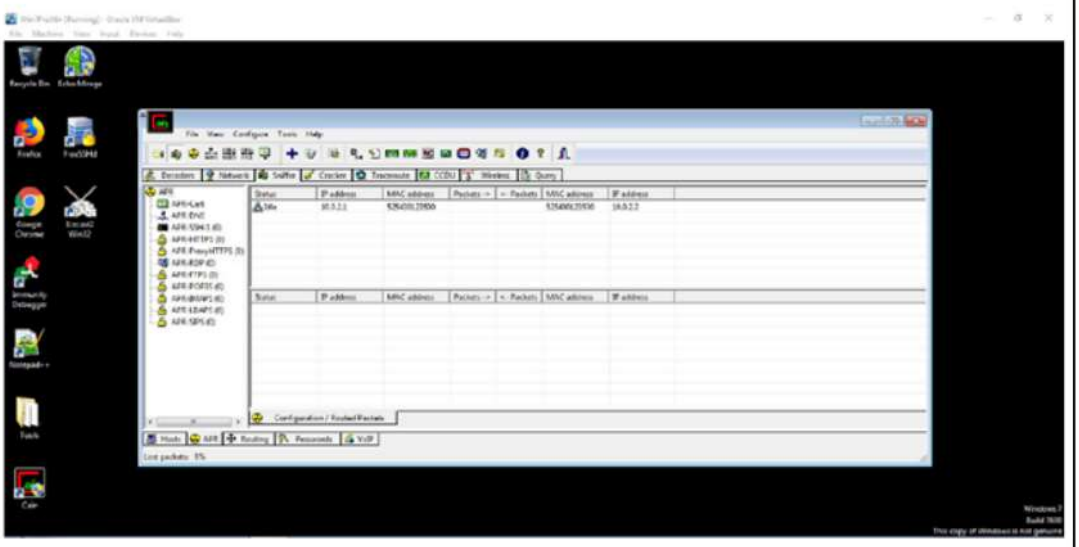
Step 6: Within the upper section of the two spaces to the right of the tree view, click on the plus symbol.



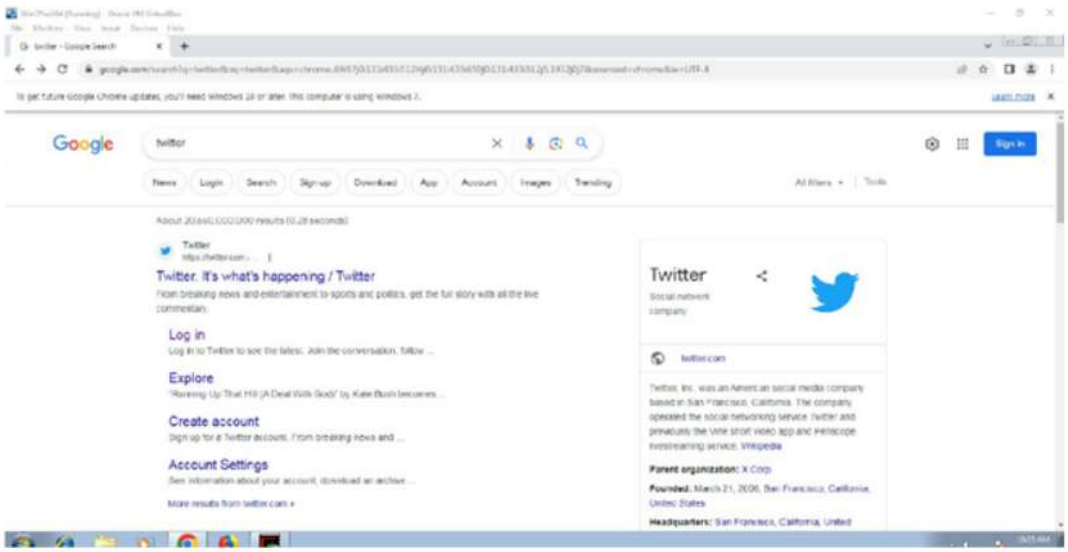
Step 7: Identify every IP and MAC combination available. Select the victim's IP address and MAC on the right side, and designate the network's actual gateway as the victim gateway on the left.



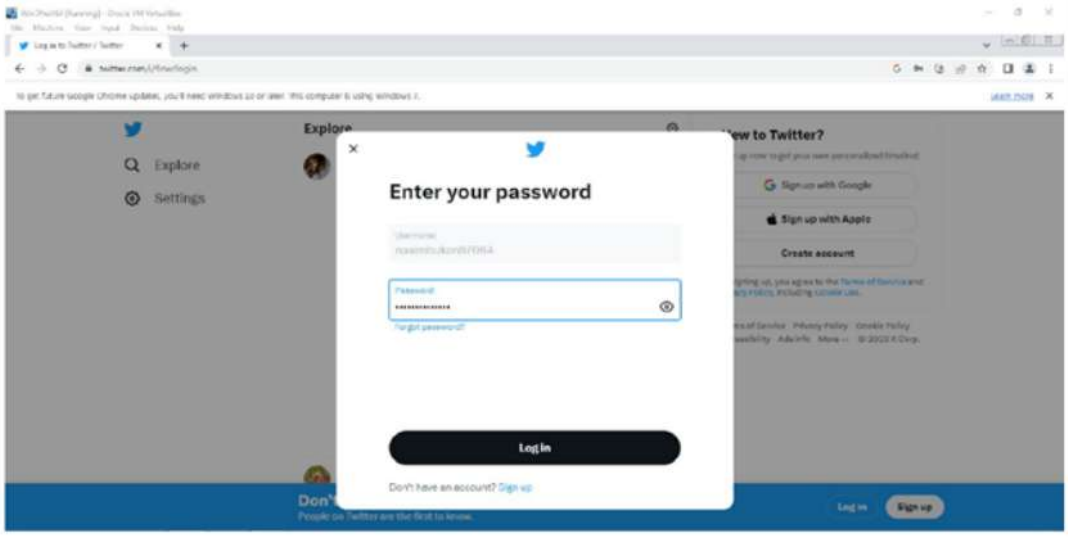
Step 8: Click the third button to initiate the ARP Poisoning.



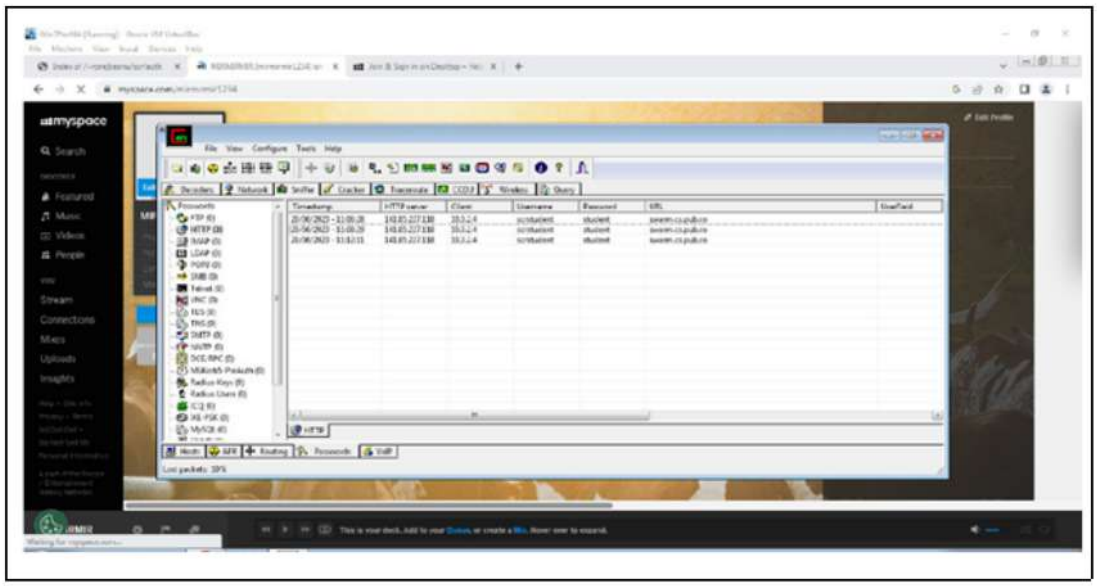
Step 9: Subsequently, we opt to use a Twitter website to gather the email address and password, accessing it while the chain is active.



Step 10: For safety purposes, we are creating a new account to target. Proceed by entering the password.

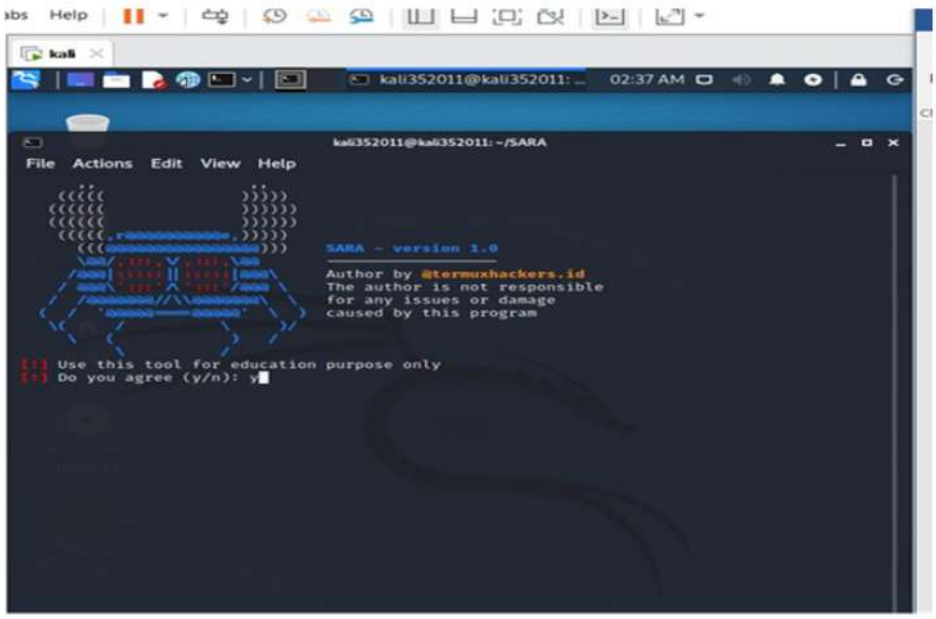


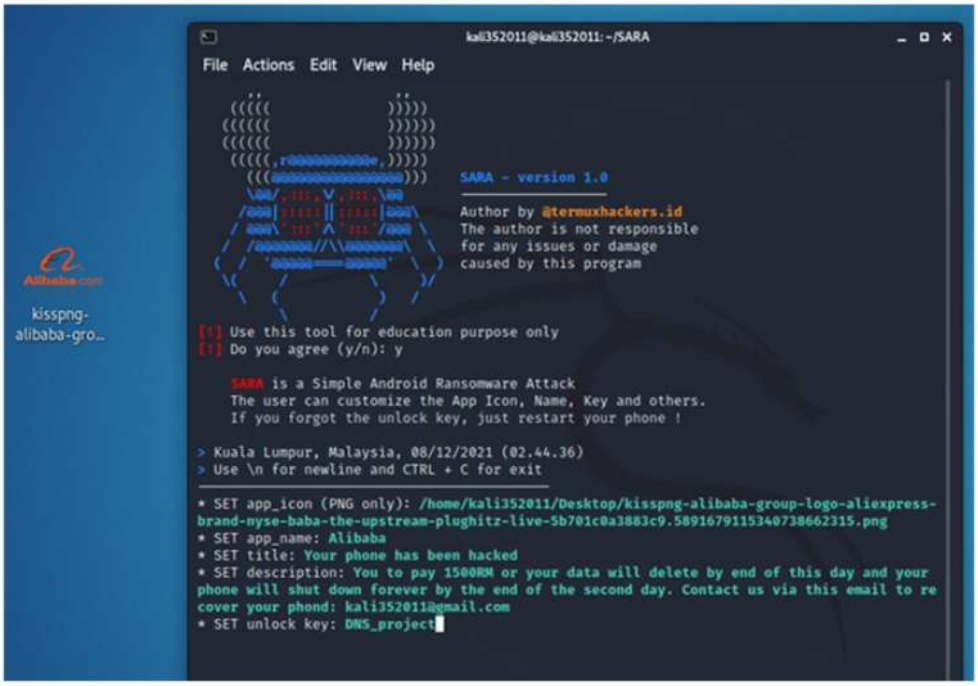
Step 11: Lastly, you can notice that the username and password are now showing up in Cain under the Password lower tab (HTTP protocol), on the sniffer tab. The results are being recorded in Cain.


myspace
Search
Featured
Music
Videos
People
Stream
Connections
Mixes
Uploads
Insights

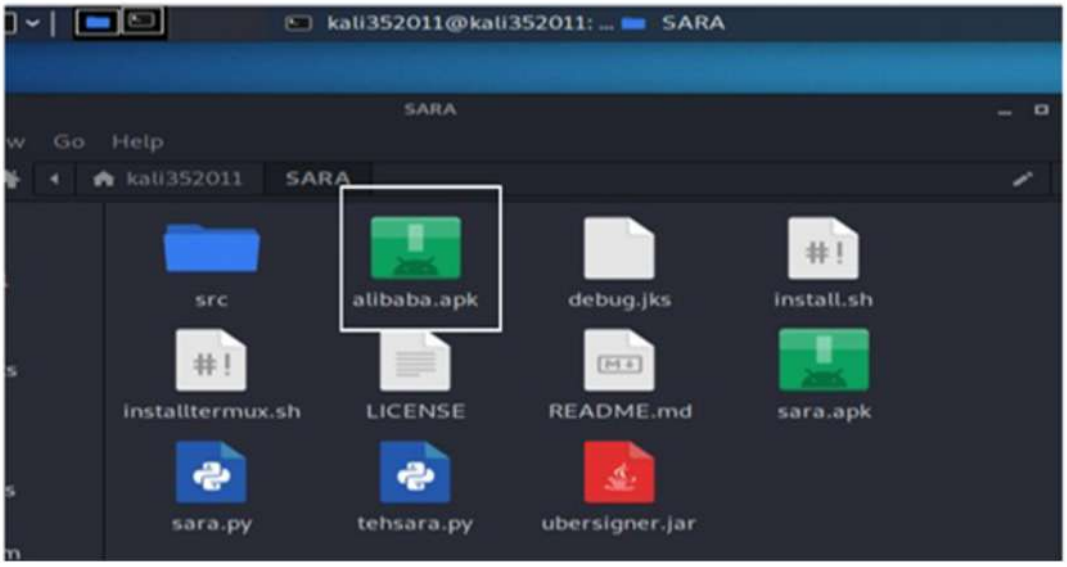
LINUX

1. SARA

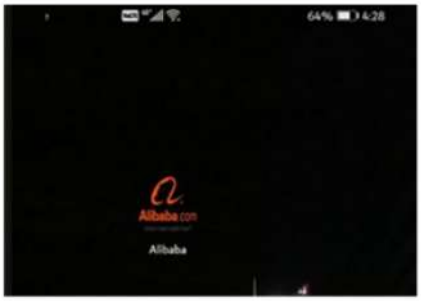
Step 1: Run the command *python3 sara.py* to initiate the SARA utility. Respond to the prompt by typing *y*.

Step 2: Upload the PNG of the app's logo to the SARA tool. Enter the unlock key, specify the name of the new app, and provide a threatening message for the victim.

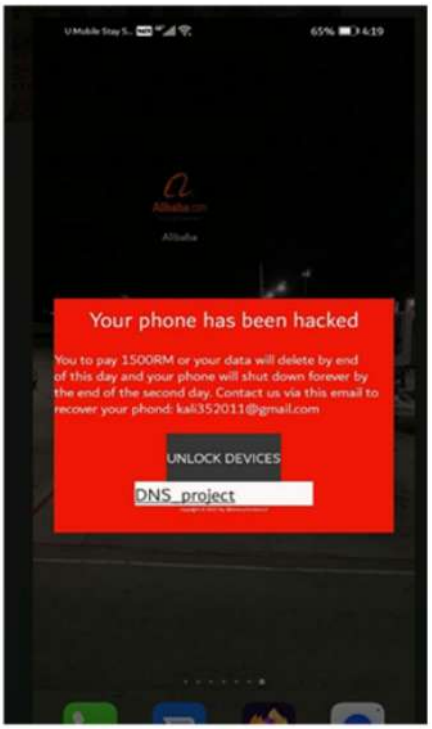


Step 3: The newly generated program is now ready to be handed to the victim.



Step 4: The new software has been successfully sent to the victim. Upon launching, the software will display a message, rendering all phone functionalities inaccessible.

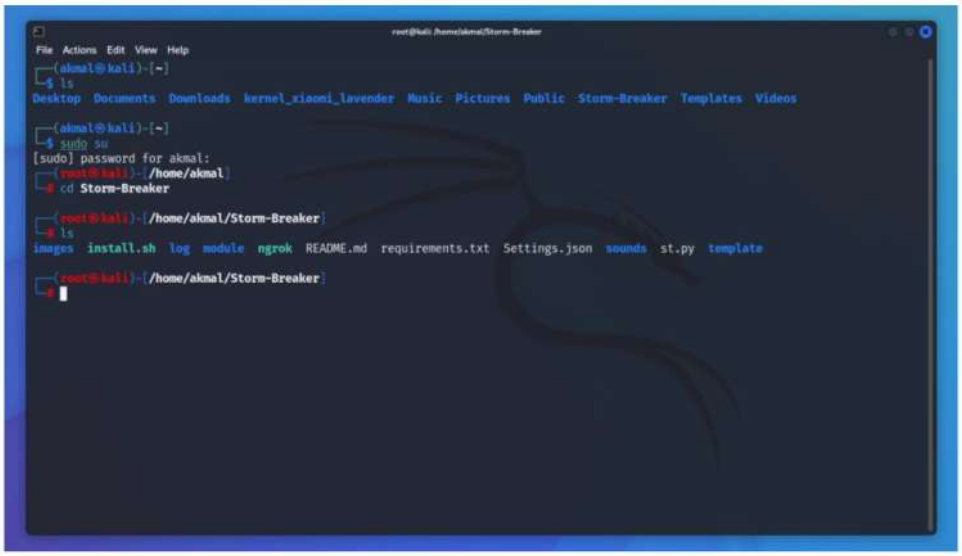




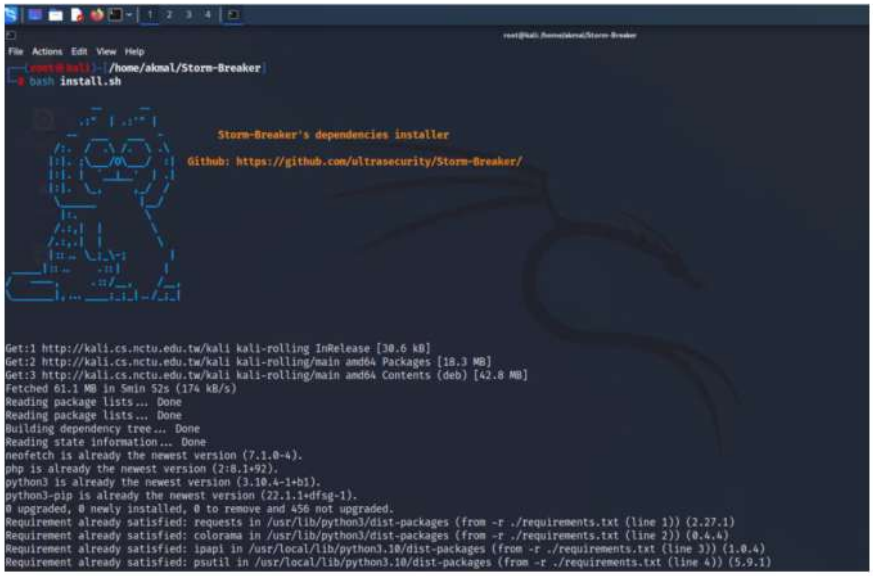
2. Storm Breaker

Step 1: Write *cd Storm-Breaker* to redirect into Storm Breaker directory.

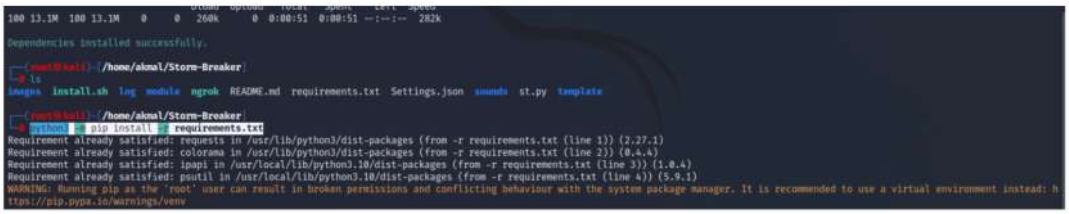
Step 2: Run *ls* command to view all files in the directory.



Step 3: Run *bash.install.sh* to install the required files to run the attack.



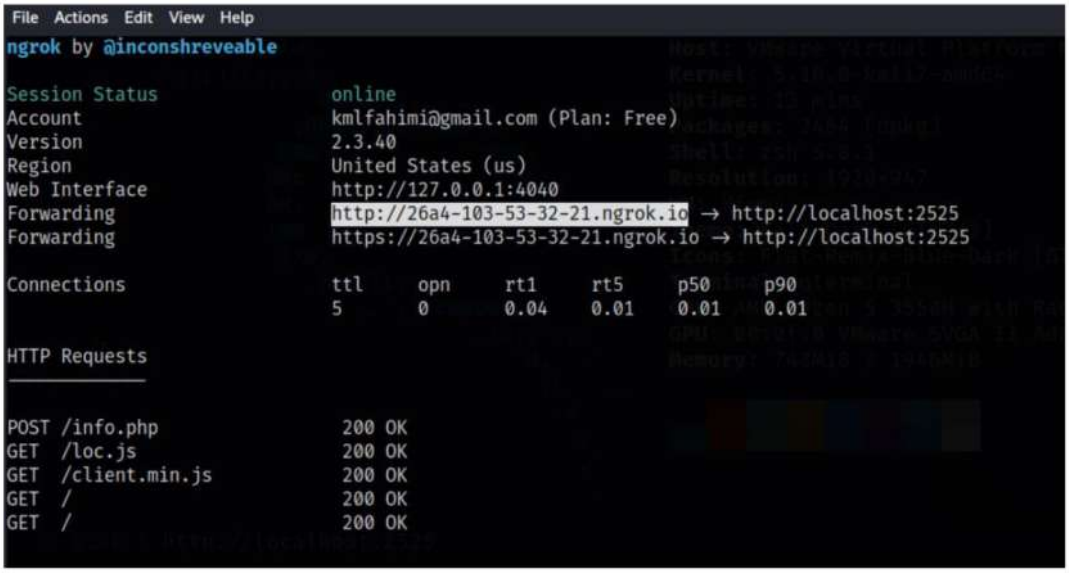
Step 4: To give executable permission to the StormBreaker python file, run the *python3 -m pip install -r requirements.txt* command.



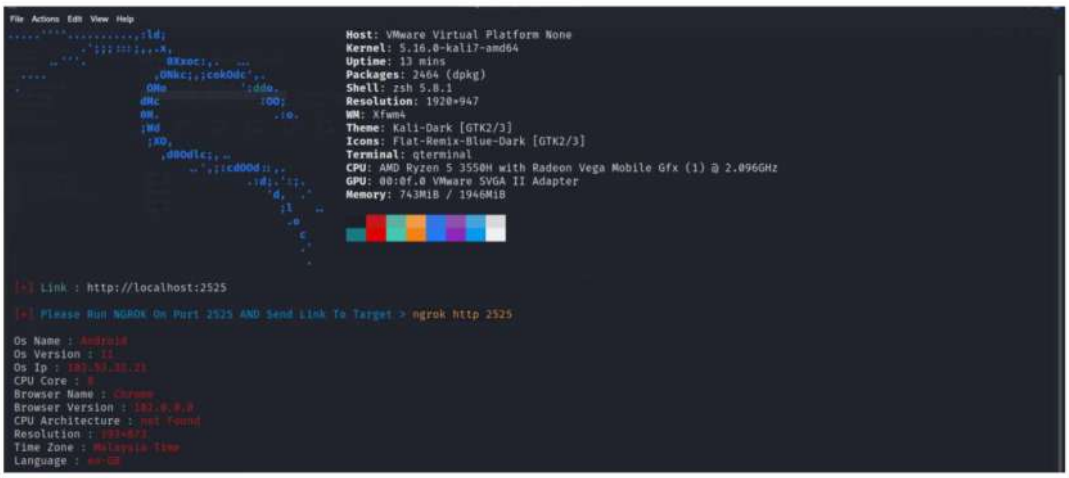
Step 5: Next, write a command *python3 st.py* to run the tool to start the attack.

Step 6: Run Option 1 which is Get Location [SMARTPHONES] to get the target location. The tool will ask to run the *ngrok* to generate two links. One link is sent to the target and the other one to the local host.

Step 7: Run *ngrok http 2897* to generate the link and send to the target.

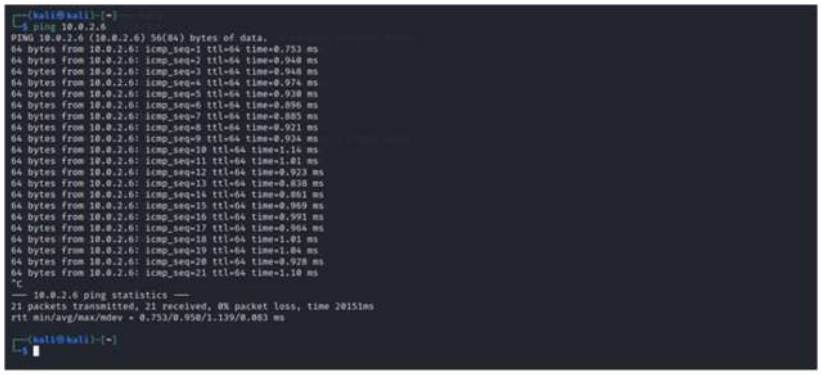
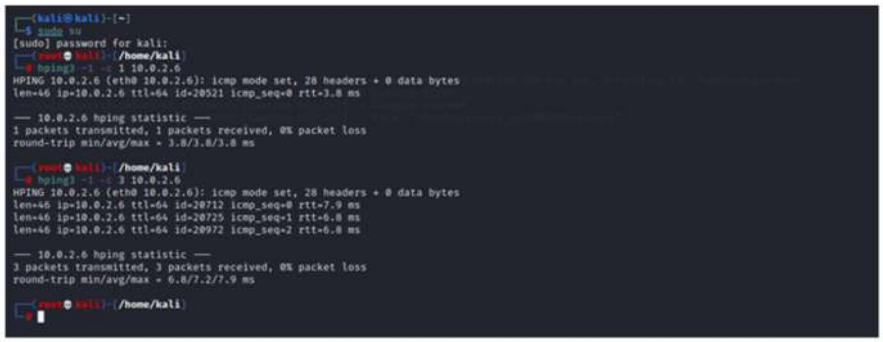


Step 8: Target location was revealed and run *N* to continue the second attack.



Step 9: Run Options 3 and 4 which are accessing the webcam and microphone of the target. The tool will ask to run the *ngrok* to generate two links. One link is sent to the target and the other one to the local host.

3. Hping3

Step 1: Ping the victim's IP Address which is 10.0.2.6 to make sure the packet can be sent to the intended recipient.

Step 2: Write the command *hping3 –1 –c 3 10.0.2.6* to transmit a packet to the victim and the reply must be received.

Step 3: Then, run the command *hping3 –1 - -flood 10.0.2.6* to start the flooding on the victim.


DEFENSE

TOOLS

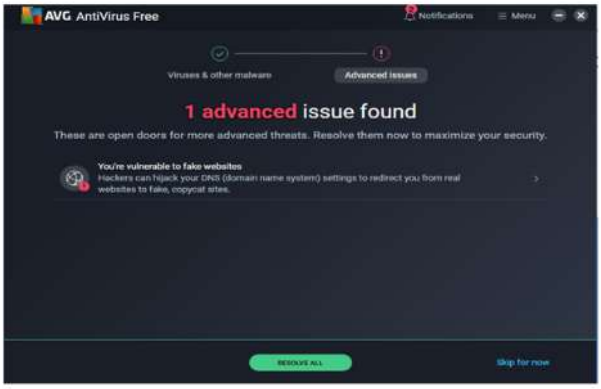
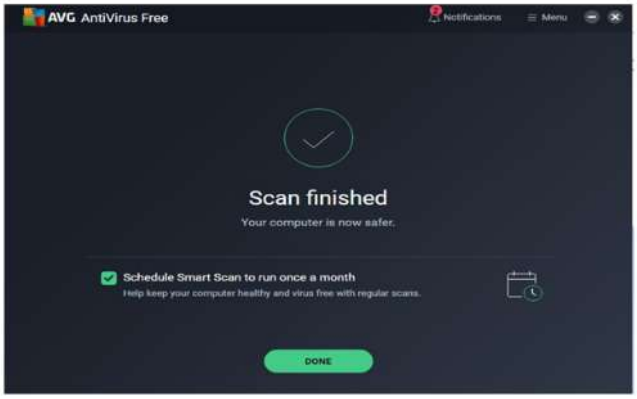
WINDOWS	LINUX
1. AVG Antivirus 2. Avast Antivirus 3. Windows Defender Firewall (for Kage) 4. Windows Defender Firewall (for Slowloris) 5. Windows Defender Firewall (for Cain and Abel)	1. Antivirus ClamAV 2. Eset nod 32 Firewall 3. XDP-Firewall

PLANNING

WINDOWS

1. AVG Antivirus

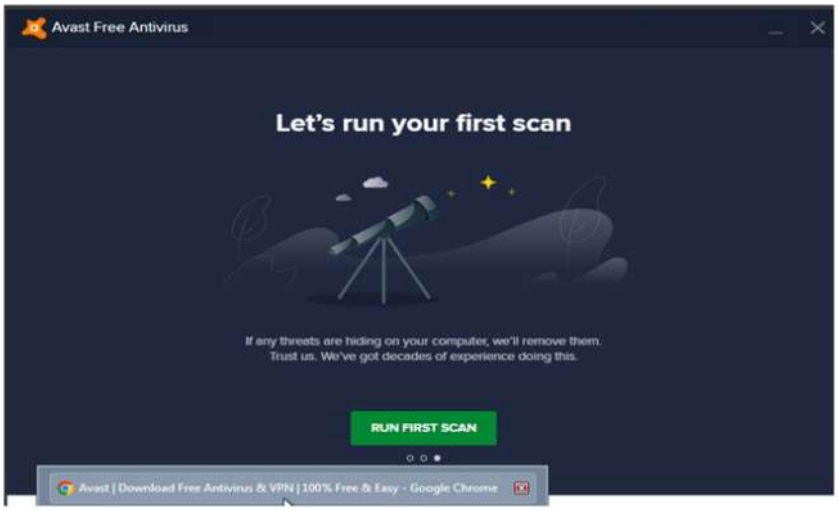
   Defending against Phishing by using AVG Antivirus

Step 1: Install a third-party firewall. We have already fortified our defense using AVG antivirus, capable of detecting whether the victim machine has been attacked or not. In this instance, AVG antivirus detected an issue on the victim machine.

Step 2: Upon completing the scan, AVG antivirus will automatically remove the detected threat from the network.


2. Avast Antivirus

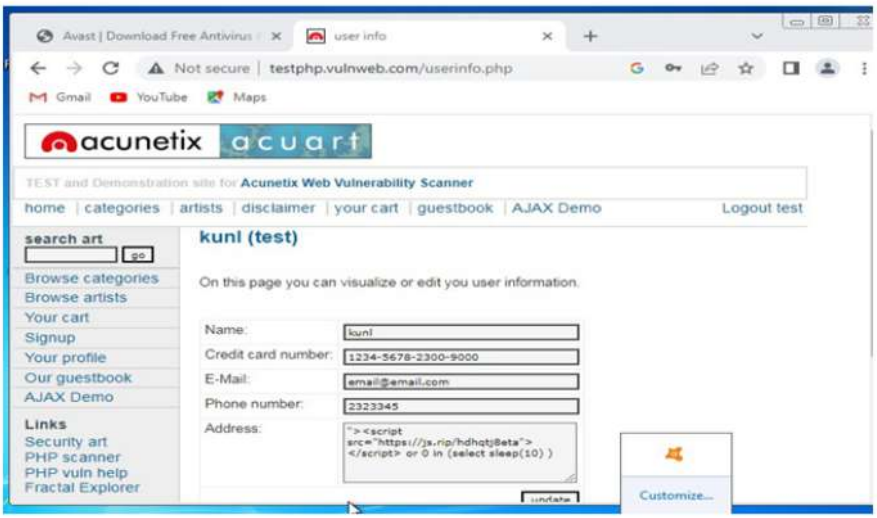
Defending against Ettercap by using Avast Antivirus

Step 1: To defend against potential Ettercap attacks, we've opted for Avast antivirus, relying on its advanced features and real-time scanning capabilities to create a robust barrier.

Step 2: Following the scan, we are assessing Avast antivirus's ability to detect any potential connection between the victim's machine and the attacker's, specifically evaluating its capacity to identify the exploit.


Step 3: Go to this link: *http://www.testphp.vulnweb.com/login.php* then enter the username and password, then click login on the Windows machine.

Step 4: If Ettercap attempts to launch an attack on the victim while Avast Antivirus is active, the antivirus can effectively thwart Ettercap's efforts to capture the data.

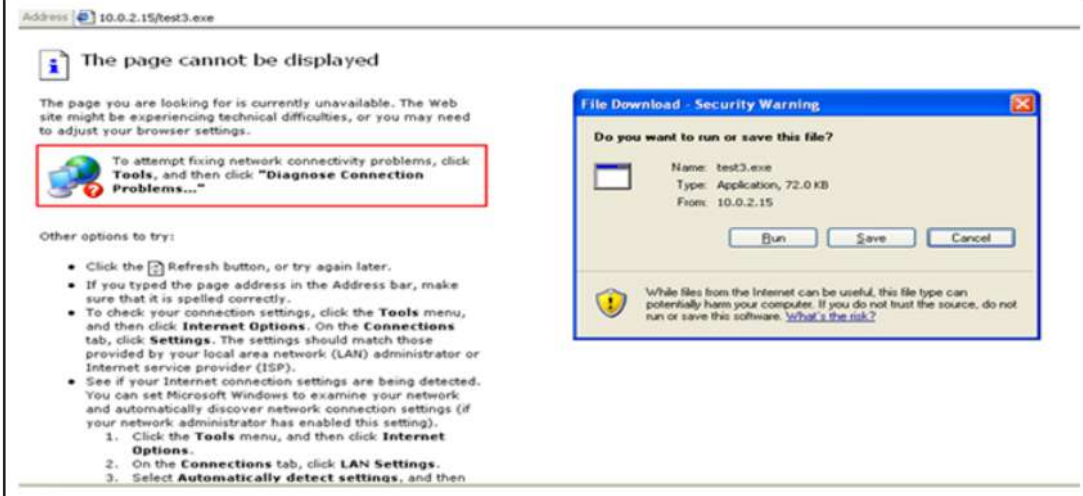


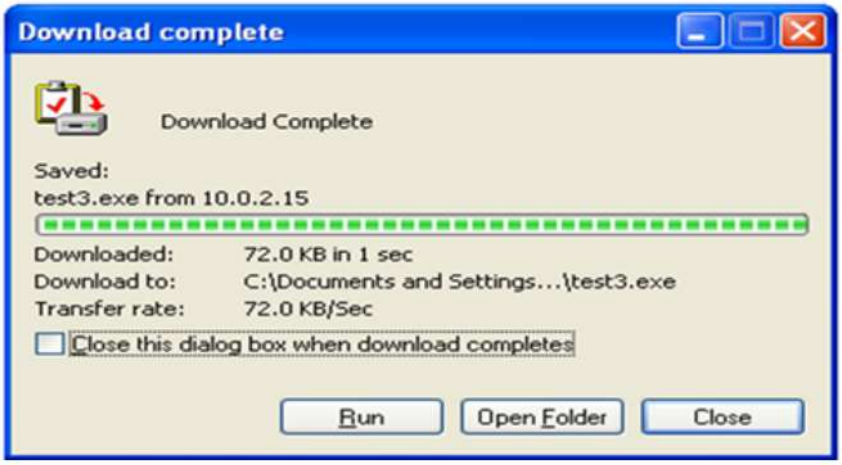
3. Windows Defender Firewall

Defending against Kage by using Windows Defender Firewall

Step 1: We decided to test the effectiveness of the initial Kage defense simulation. To begin, we accessed the security center on Windows XP and opened the firewall.

Step 2: In an attempt to retrieve the botnet file from the attacker, we ran the process again. Surprisingly, even with the firewall open, the file was still able to be downloaded.

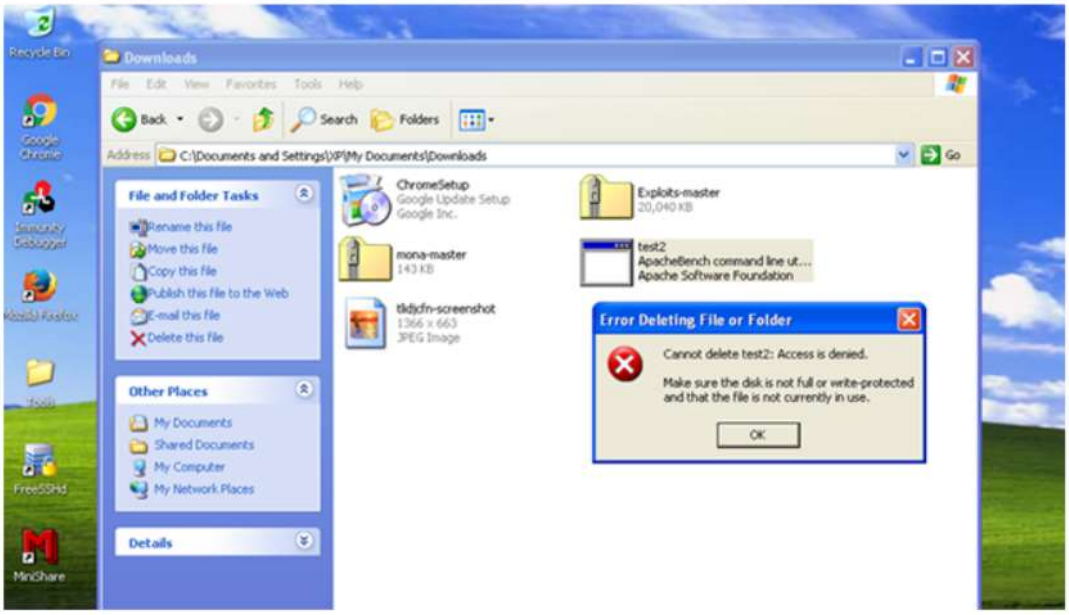




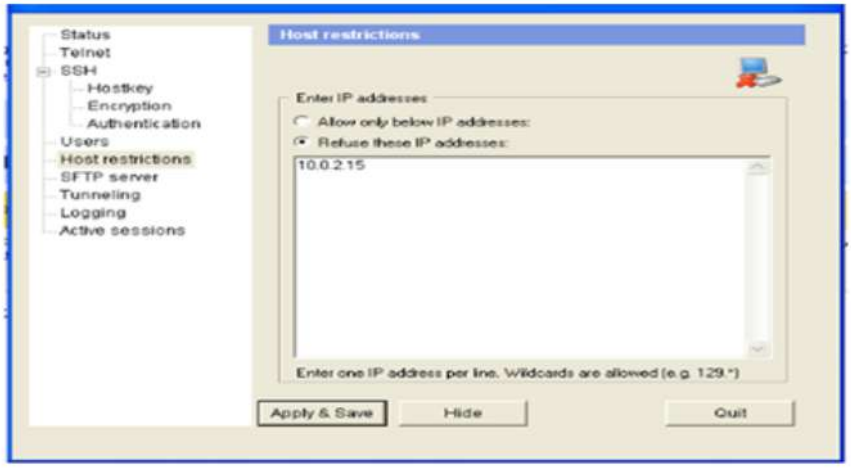
Step 3: Upon starting the botnet software, it also presents the Kage interface.

The test shows that the Windows XP firewall cannot stop software downloads, likely due to its weakness against botnet malware. This implies that Windows XP's firewall is not very effective in protecting against botnet attacks.

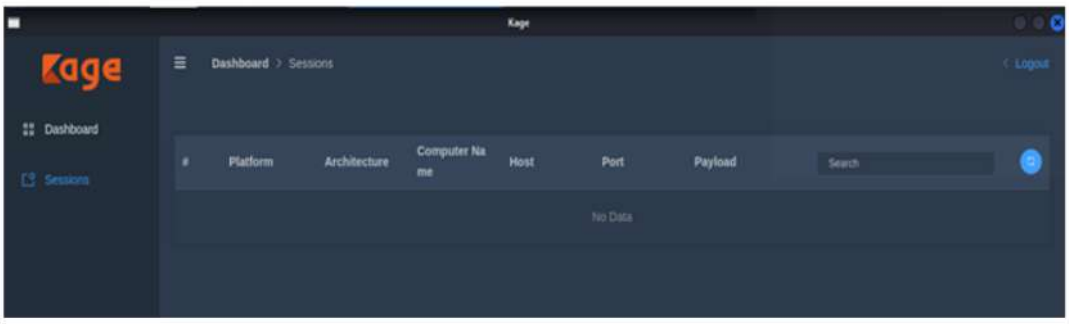
Consequently, despite identifying the file as part of the attacker's botnet, we are unable to eliminate it.



Step 4: Given our knowledge of the attacker's IP address, we can use host limitation to block their IP address, effectively putting a stop to the botnet's activities.

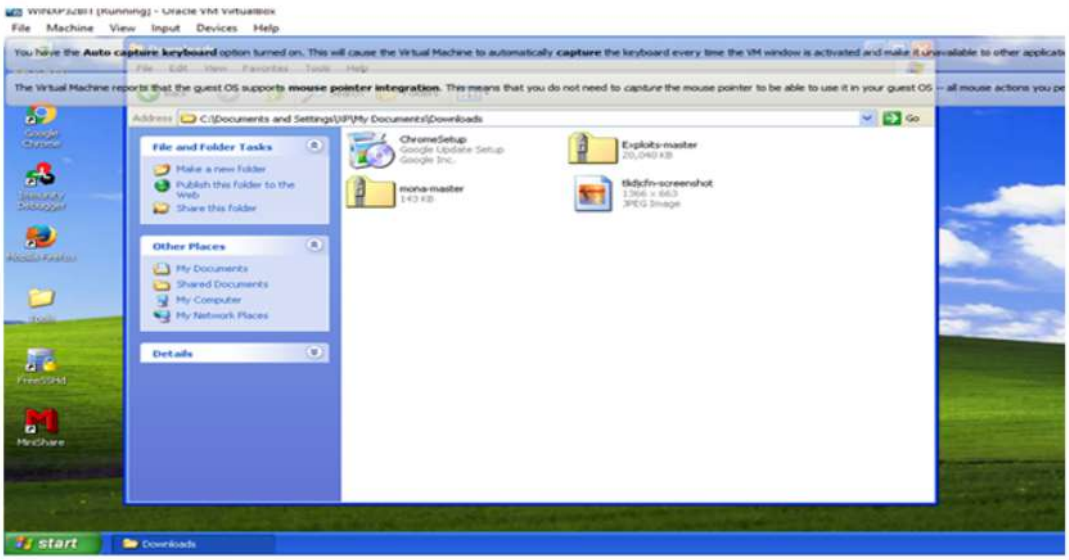


Step 5: We can notice that the platform is no longer present in Kage.



Step 6: We can see that the session has concluded, thanks to the meterpreter.

Step 7: Following this, we can successfully remove the entire botnet program from the computer.



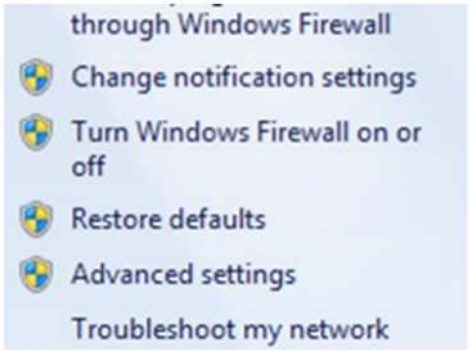
This outcome demonstrates that limiting the attacker's IP address is the best strategy to terminate the botnet malware.

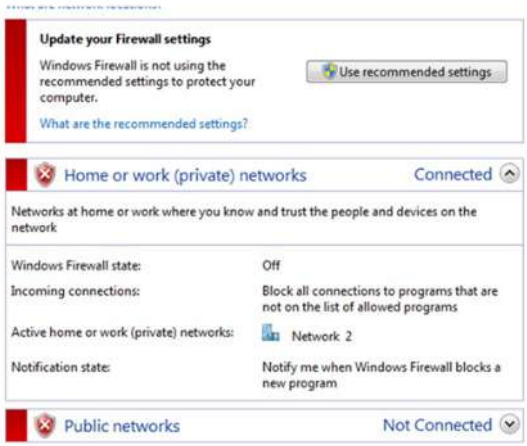
4. Windows Defender Firewall

Defending against Slowloris by using Windows Defender Firewall

Step 1: Commence by opening the Control Panel from the Windows tab.

Step 2: Subsequently, select *System and Security*.

Step 3: In the System and Security. It will provide us with a Windows firewall.

Step 4: Within the firewall settings, locate the option to turn the firewall on or off and click on it.

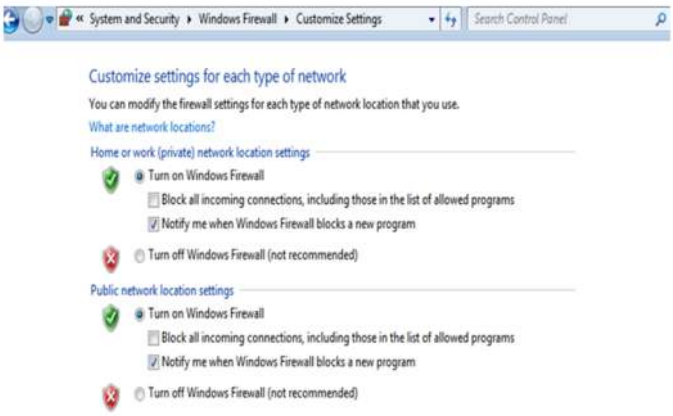
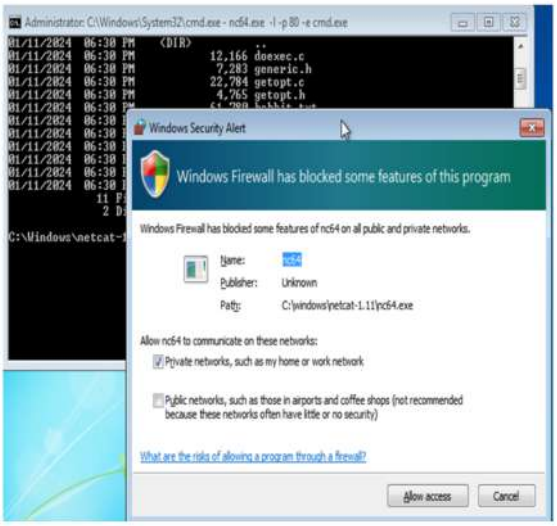


Step 5: Observe that the color on the page remains red, indicating that the firewall is still turned off.

Step 6: On this page, we should tick the options on the firewall and click *Okay* to make the system do what we desire.

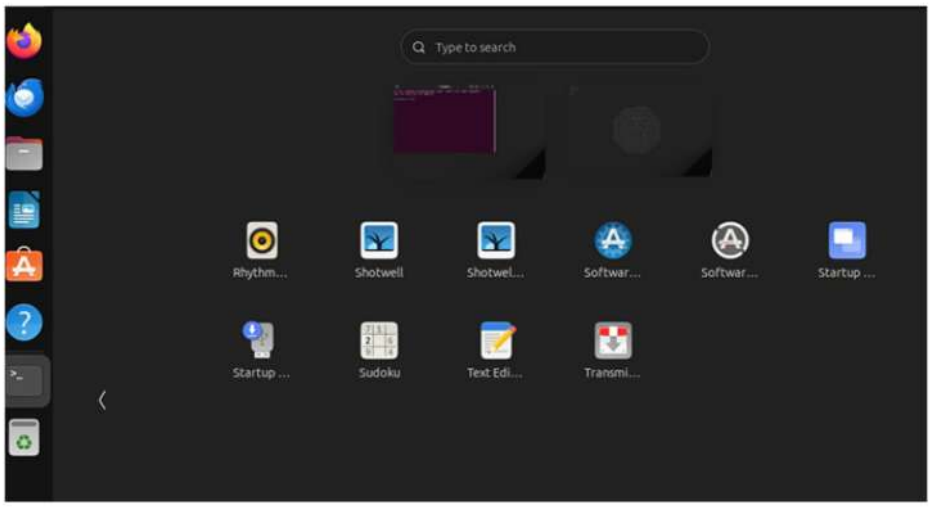
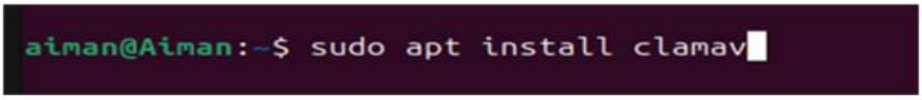
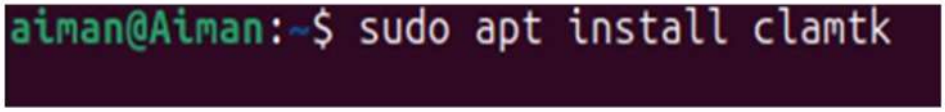
5. Windows Defender Firewall

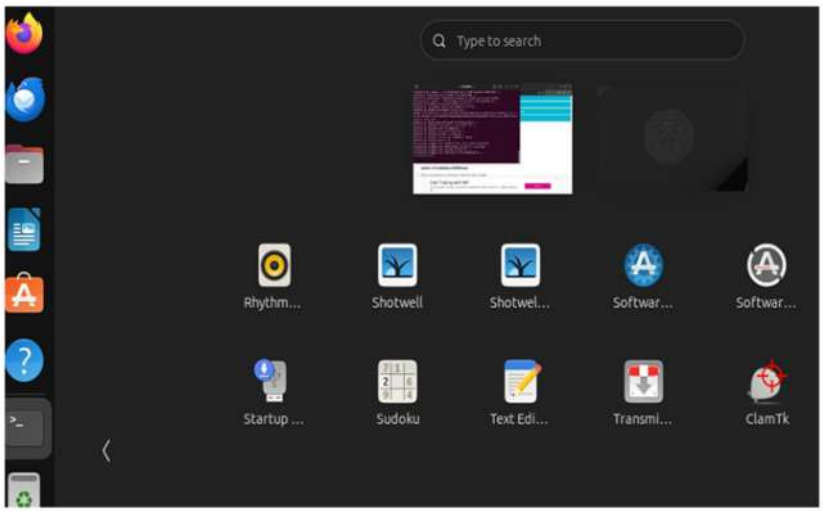
Defending against Cain and Abel by using Windows Defender Firewall

Step 1: Turning on Windows Firewall in Windows entails configuring rules to regulate the traffic coming into and going out of our network.

Step 2: To stop an intruder from accessing Windows, the Windows firewall generates security alerts.


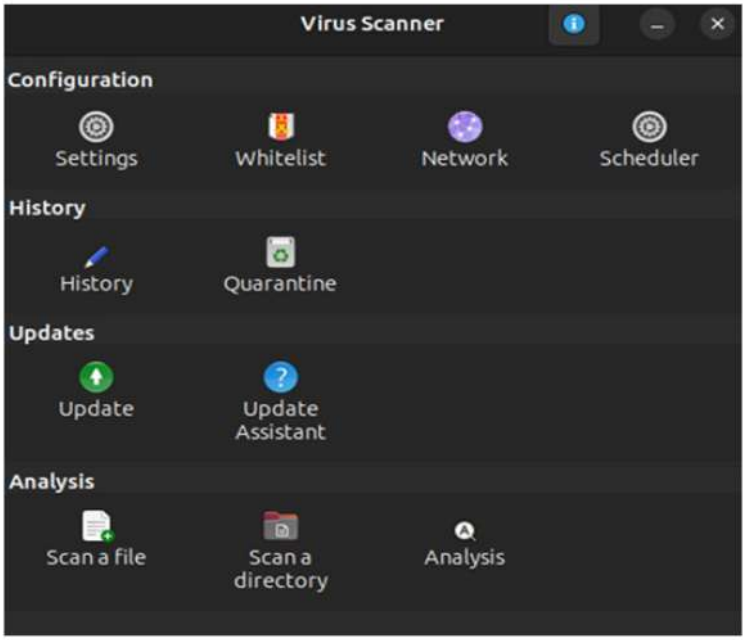
LINUX

1. Antivirus ClamAV

Step 1: Ubuntu Linux does not come with antivirus software by default.

Step 2: Install ClamAV on your Ubuntu machine by entering the following command in the terminal: *apt install clamav*

Step 3: For Ubuntu Desktop users who want a graphical front end, they can install ClamTk by entering the following command: *apt install clamtk*

Step 4: ClamTK has been successfully installed on your desktop.



Step 5: Explore the features of the ClamAV antivirus.



Step 6: To check the ClamAV version, run the following command:

```
aiman@Aiman:~$ clamscan --version
ClamAV 1.0.4/27151/Thu Jan 11 17:41:16 2024
```

Step 7: Once the installation is finished, run the freshclam command to update the virus signature database. To do so, stop the Freshclam service by entering the following command: *systemctl stop clamav-freshclam.service*

```
aiman@Aiman:~$ systemctl stop clamav-freshclam.service
aiman@Aiman:~$
```

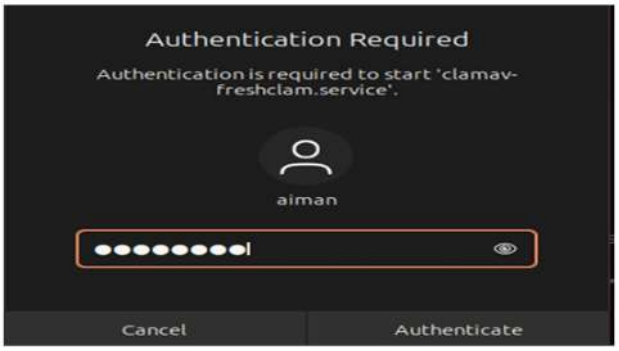
Step 8: Proceed to update the database by running the following command: *sudo freshclam*

```
aiman@Aiman:~$ sudo freshclam
[sudo] password for aiman:
ClamAV update process started a
```

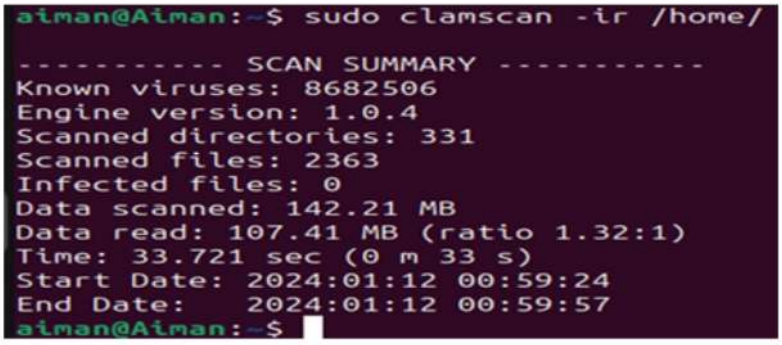
Step 9: Restart the freshclam and enter the following command: *systemctl start clamav-freshclam.service*

```
aiman@Aiman:~$ systemctl start clamav-freshclam.service
```

Step 10: Enter your password for authentication

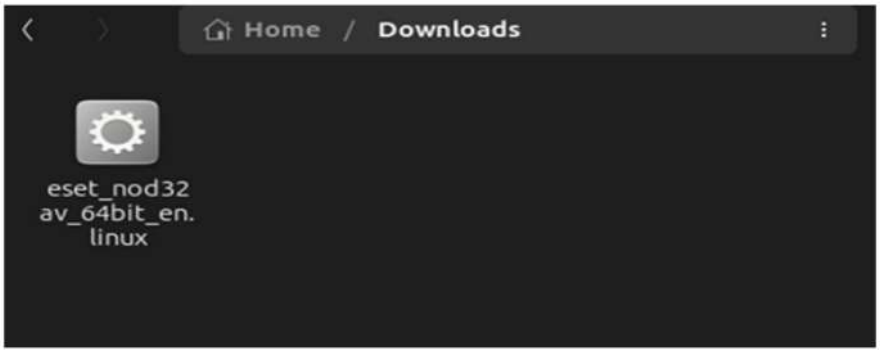


Step 11: ClamAV is capable of detecting viruses, Trojans, and other forms of malware. Scanning files for viruses is done with clamscan command, enter the following command: *sudo clamscan -ir /home/*



2. Eset nod 32 Firewall

Step 1: Download the 64-bit version of the nod32 Firewall for Ubuntu.

Step 2: Open the downloaded file in the designated folder.

Step 3: Open the file in the terminal.

Step 4: Execute the file using the following command: *Chmod +x eset_nod32av_64bit_en.linux*

```
aiman@Aiman:~/Downloads$ chmod +x eset_nod32av_64bit_en.linux
aiman@Aiman:~/Downloads$ ls
eset_nod32av_64bit_en.linux
```

Step 5: Enter the file by using the following command:

./ eset_nod32av_64bit_en.linux

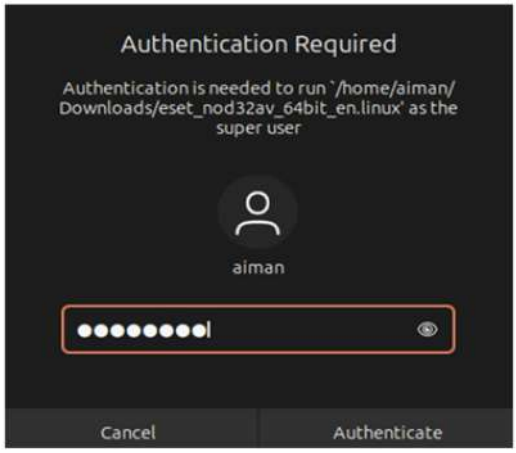
```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

Step 6: If there is an error like this, install the missing package, libc6:i386, and enter the following command:

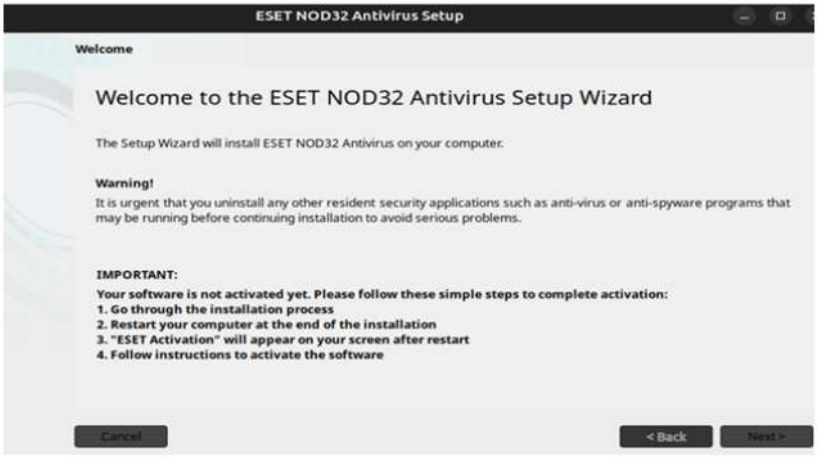
Sudo dpkg –add-architecture i386; sudo apt-get install

```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
error[277b0000]: Please install the following files or packages: libc6:i386, /li
b/ld-linux.so.2
aiman@Aiman:~/Downloads$ sudo dpkg --add-architecture i386; sudo apt-get install
 libc6:i386
```

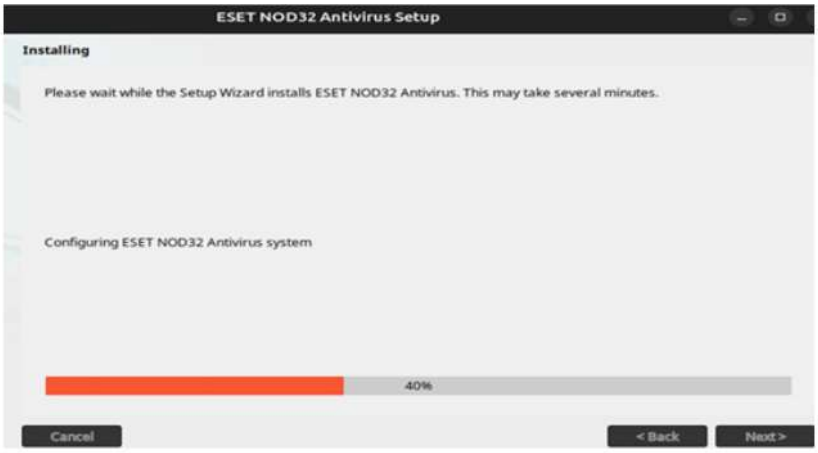
Step 8: Enter your password to grant authentication.



Step 9: In the antivirus setup, click Next.

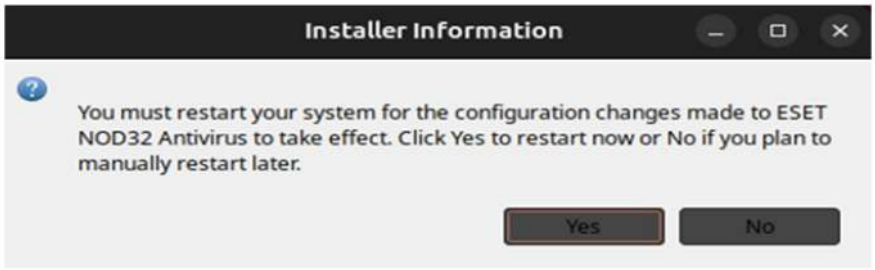


Step 10: Accept all the requirements and then click Install.



Step 11: Once the installation is complete, click Finish.

Step 12: Restart your system to apply the changes and activate the antivirus.



Step 13 : The antivirus has been installed and usable in your ubuntu desktop.

3. XDP-Firewall

Step 1: Install dependencies using the following command:
sudo apt install -y libconfig-dev llvm clang libelf-dev build-essential

```
aiman@Aiman:~$ sudo apt install -y libconfig-dev llvm clang libelf-dev build-ess
ential
```

Step 2: Install dependencies for building LibXDP and LibBPF. Use the following command: *sudo apt install -y libpcap-dev m4 gcc-multilib*

```
aiman@Aiman:~$ sudo apt install -y libpcap-dev m4 gcc-multilib
```

Step 3: You need tools for your kernel. Since we need BPFTool, use the following command to install it: *sudo apt install -y linux-tools-$(uname -r)*

```
aiman@Aiman:~$ sudo apt install -y linux-tools-$(uname -r)
```

Step 4: To install git in your Ubuntu, run the following command: *Apt install git*

```
aiman@Aiman:~$ apt install git
```

Step 5: To clone the repository via Git. Use the recursive flag to download LibBPF sub-module using the following command:
git clone --recursive https://github.com/gamemann/XDP-Firewall.git

```
aiman@Aiman:~$ git clone --recursive https://github.com/gamemann/XDP-Firewall.gi
t
```

Step 6: Change the directory to the repository using the following command:
cd XDP-Firewall

```
aiman@Aiman:~$ cd XDP-Firewall
```

Step 7: To install make use the following command: *sudo apt install make.*

Step 8: Build XDP-Tools and install LibXDP & LibBPF to /usr/include using the following command: *make libxdp*

```
aiman@Aiman:~/XDP-Firewall$ make libxdp
```

Step 9: Build the main project and install as root via Sudo using the following command: *make && sudo make install*

```
aiman@Aiman:~/XDP-Firewall$ sudo make && sudo make install
```

TASK DISTRIBUTION

Task	Person in Charge
Blue Team concepts and activities preparation	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012) 2. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045)
Red Team concepts and activities preparation	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039) 2. WARSENA A/P EH CHUOI (CB21056)
Computer and network services preparation	1. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045) 2. WARSENA A/P EH CHUOI (CB21056)
Identify tools for attack	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039)
Identify tools for defend	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012)
Set up computer and network services (Blue Team)	1. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045)
Setup attack tools (Red Team)	1. WARSENA A/P EH CHUOI (CB21056)
Perform attack tools (Red Team)	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039)
Plan mitigation and perform countermeasures based on each of the attacks (Blue Team)	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012)

REFERENCES

Firch, J. (2020, September 27). What Is A Red Team VS A Blue Team In Cyber Security? PurpleSec. https://purplesec.us/red-team-vs-blue-team-cyber-security/

Top 10 Kali Linux Tools For Hacking. (2020, July 11). GeeksforGeeks. https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/

17 free cybersecurity tools you should know about. (n.d.). WhatIs.com. https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about

Saxena, A. (2023, March 11). Top 15 Cybersecurity tools You Must Know in 2023. Sprinto. https://sprinto.com/blog/best-cybersecurity-tools/

Top 25 Linux Security Tools to Boost Cyber Defense. (2023, May 23). https://www.stationx.net/linux-security-tools/

AVG 2019 | FREE Antivirus & TuneUp for PC, Mac, Android. (n.d.). AVG.com. https://www.avg.com/en-ww/homepage#pc

What is Windows Defender Firewall? (n.d.). Www.computerhope.com. https://www.computerhope.com/jargon/w/windows-defender-firewall.htm

GROUP PROJECT

ORIGINALITY REPORT

8%	4%	0%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universiti Malaysia Pahang Student Paper	4%
2	Submitted to Anderson University Student Paper	1%
3	Submitted to Sheffield Hallam University Student Paper	<1%
4	quieora.ink Internet Source	<1%
5	Submitted to Champlain College Student Paper	<1%
6	Submitted to Study Group Australia Student Paper	<1%
7	Submitted to University of Teesside Student Paper	<1%
8	Submitted to CTI Education Group Student Paper	<1%
9	www.hillsoft.com Internet Source	<1%

10	Submitted to Henley College Coventry, Coventry Student Paper	<1%
11	kupdf.net Internet Source	<1%
12	linux.org Internet Source	<1%
13	buildmedia.readthedocs.org Internet Source	<1%
14	www.precidia.com Internet Source	<1%
15	forums.kali.org Internet Source	<1%
16	uap.unnes.ac.id Internet Source	<1%
17	www.malekal.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

DATA NETWORK & SECURITY

BCN2023

PROJECT

LECTURER'S NAME: ABDULLAH BIN MAT SAFRI		
DATE OF SUBMISSION: 16 JANUARY 2024		
SECTION: 02A		
NAME	**MATRIC ID**	**STUDENT PHOTO**
MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI	CB21012	
NURUL ADRIANA BINTI MOHAMMAD AFANDI	CB21045	
TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH	CB21039	
WARSENA A/P EH CHUOI	CB21056	

TABLE OF CONTENTS

CONCEPT

Our 10-week project, which accounts for 25% of our assessment, aims to improve online system security. We divided our four-person group into two teams: the Blue Team and the Red Team.

Blue Team's Job: Establishing Strong Defences

The Blue Team, made up of two members, began by connecting three computers. Two PCs use distinct operating systems: Windows and Linux. We updated and installed the newest security patches to ensure optimal protection. On Windows, we configured a web service and enabled networking options. The Linux machine received all of the essential networking tools.

Our goal as the Blue Team was to protect against possible attacks. We investigated and implemented online defence techniques on both computers. We chronicled the entire process, including the first steps and ultimate defence setup.

Red Team Role: Testing the defences.

The remaining two members comprised the Red Team. Our task was to simulate hacking (in a responsible manner) and test our ability to gain access to computers. We evaluated various attack strategies and tools for Windows and Linux. We thoroughly documented our results and meticulously planned our attacks. We did not intend to inflict harm, only to test the defences. We executed five simulated attacks on Windows and three on Linux systems. We provided step-by-step explanations of each attack, including accompanying photos.

Learning and Improving Together:

The Blue Team then took over, demonstrating how they resisted our simulated onslaught. They had plans in place to prevent attacks and defend their systems. We chronicled their defences and gained valuable insights from their approach.

Throughout our project, we made a point of mentioning where we acquired our information. This allows others to check and learn more as needed. We communicated extensively as a group to ensure everyone understood the situation and resolved any issues.

Our goal was to understand and develop our systems while being responsible and ethical. This project is our effort to make online places safer for everyone.

COMPUTER AND NETWORK SERVICES PREPARATION

In preparation for the targeted attack, we have categorized the tools into two separate categories according to the platforms they are compatible with: Windows and Linux. Zphisher, Ettercap, Kage, Slowloris, Cain, and Abel are the tools that are used in the Windows environment. Meanwhile, Storm Breaker, Hping3, and SARA are available for the Linux platform. Below are the explanations for each tool on Windows and Linux.

RED TEAM

WINDOWS

TOOLS	EXPLANATION
Zphisher	❖ Zphisher is a phishing application that automatically generates phishing websites across multiple internet platforms. ❖ A form of social engineering where hackers trick users into revealing personal data including usernames and passwords.
Ettercap	❖ Ettercap is used to carry out Man-in-the-Middle (MitM) attacks. ❖ It has the ability to record, capture, and examine conversations between two network users.
Kage	❖ Kage makes the process of designing graphical user interfaces (GUIs) for different penetration testing tools easier. ❖ It aims to simplify user interaction with many tools

	via a single interface.
Slowloris	❖ A Slowloris attack is a particular kind of Denial of Service (DoS) attack that may be carried out with the use of the tool Slowloris. ❖ It functions by establishing and maintaining many connections to the target web server.
Cain and Abel	❖ Cain and Abel is a Microsoft Windows password recovery programme. ❖ It can retrieve a variety of password formats by employing strategies like brute-force and dictionary attacks.

LINUX

TOOLS	EXPLANATION
SARA	❖ SARA is a security testing tool intended to assist security experts in locating and evaluating computer system vulnerabilities.
Storm Breaker	❖ Storm Breaker is a tool that targets flaws in people rather than in technological systems. ❖ The main purpose of it is to locate the victim, including their GPS coordinates.
Hping3	❖ Hping3 may be used for creating packets, scanning networks, and testing firewalls.

BLUE TEAM

WINDOWS

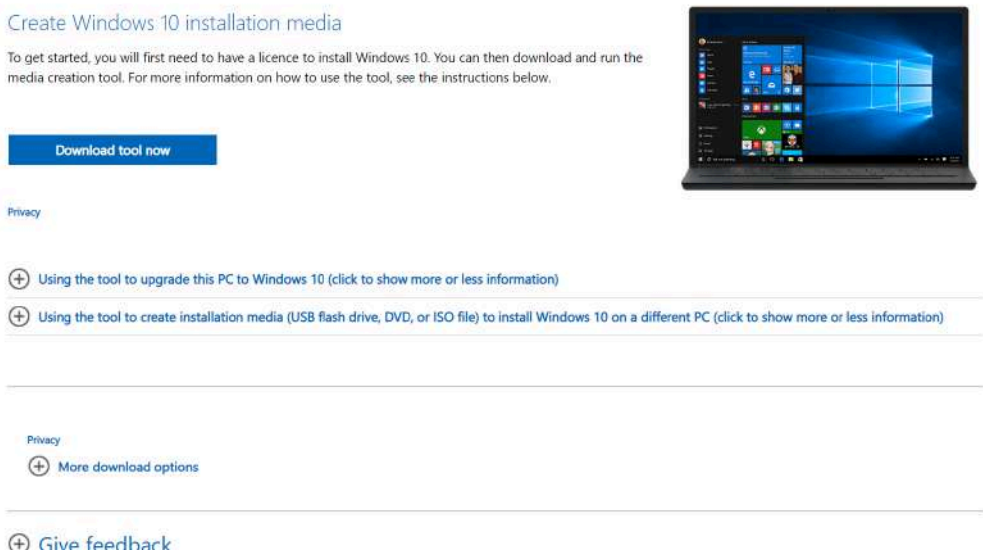
TOOLS	EXPLANATION
AVG Antivirus	❖ AVG is an antivirus program that defends your computer against viruses, malware, and other internet threats. ❖ It contains features like real-time scanning, email protection, and secure web browsing.
Avast Antivirus	❖ Avast is another antivirus product that protects against viruses, malware, and other cyber dangers. ❖ It has capabilities including real-time scanning, behaviour analysis, and a range of scanning methods.
Windows Defender Firewall	❖ Windows Defender is a built-in antivirus and malware protection solution for Windows operating systems. ❖ In addition to antivirus protection, Windows Defender has a firewall that monitors and controls incoming and outgoing network traffic.

LINUX

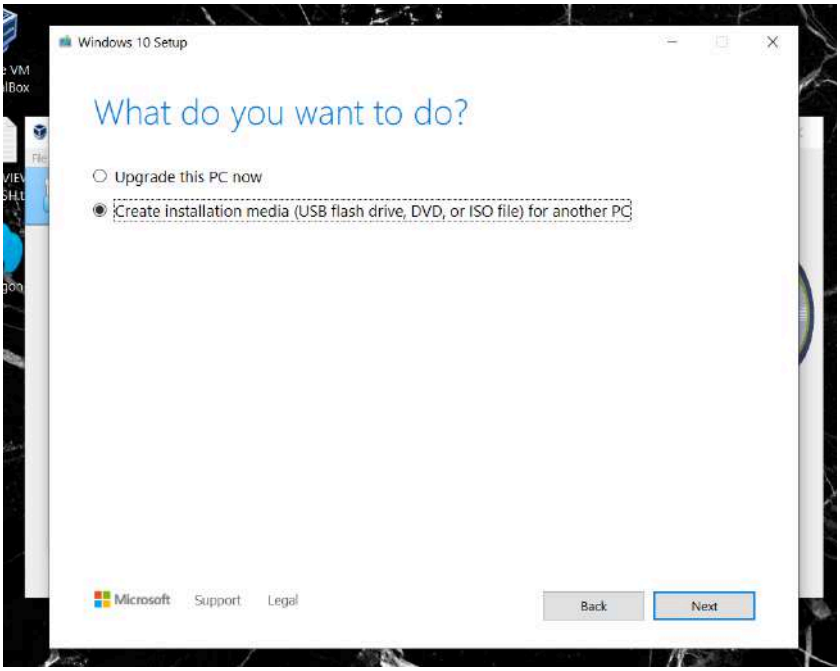
TOOLS	EXPLANATION
Antivirus ClamAV	❖ ClamAV is an open-source antivirus engine designed to detect a variety of harmful malware. ❖ It is commonly used on Linux-based systems and may be connected with email servers to detect viruses in attachments.
Eset nod 32 Firewall	❖ Eset NOD32 is an antivirus software that protects against viruses, worms, and other forms of malware. ❖ It also has a firewall component for monitoring and controlling network traffic.
XDP-Firewall	❖ A stateless firewall that hooks to the Linux kernel's XDP hook using (e)BPF for rapid packet processing. ❖ This firewall is intended to read filtering rules and filter incoming packets based on a configuration file stored on a disc.

SETTING UP WINDOWS

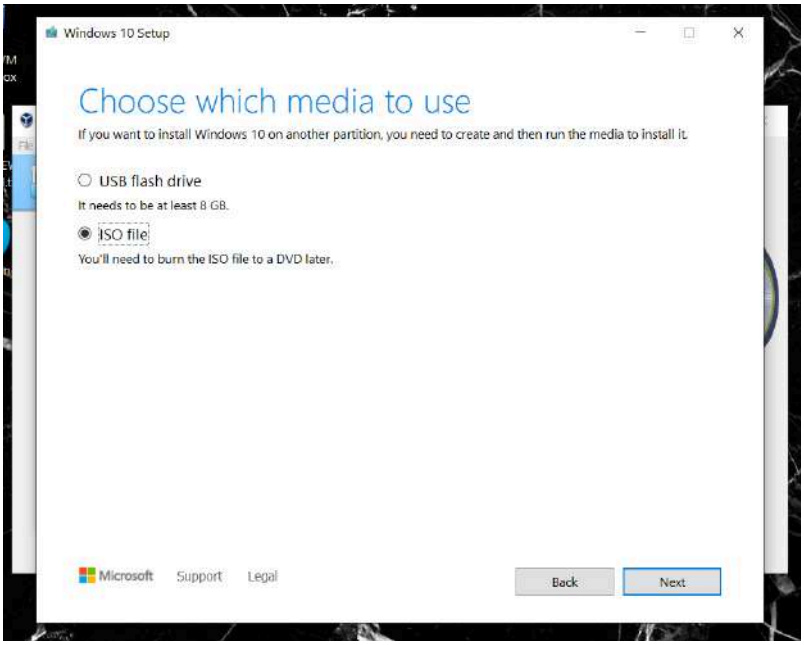
Step 1: Download Windows 10 ISO tool through this link https://www.microsoft.com/en-au/softwaredownload/windows10



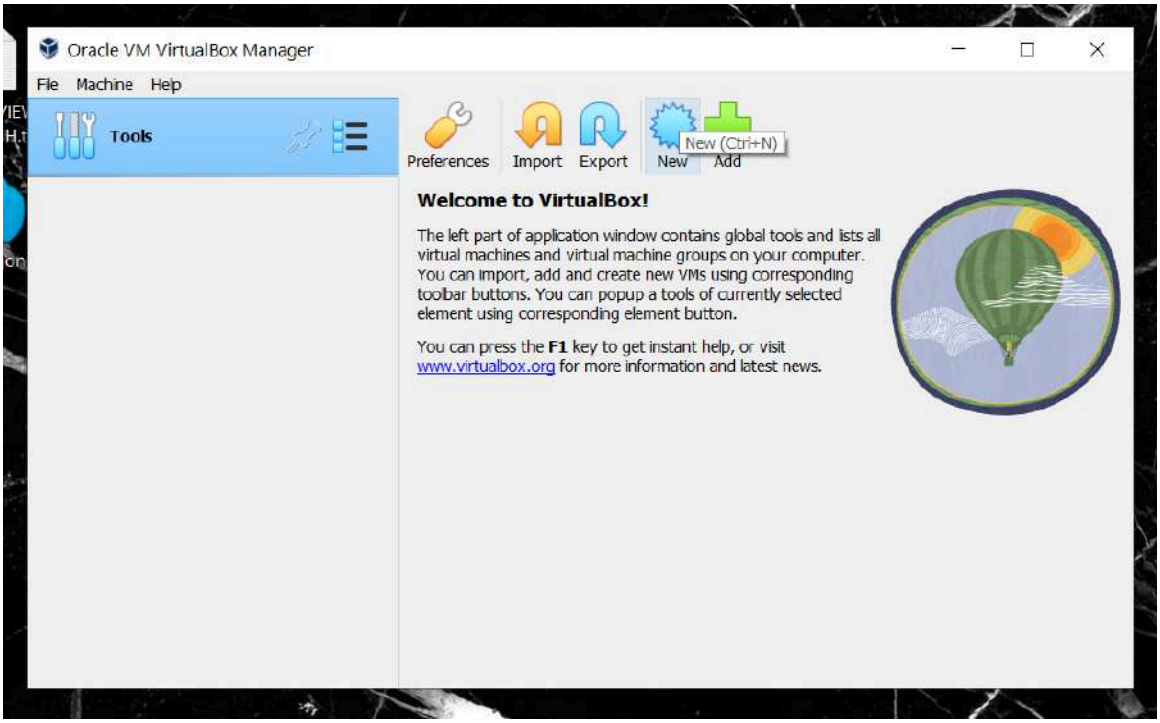
Step 2: After installation, launch the exe file and select "Create installation media for another PC" and go to the next step.



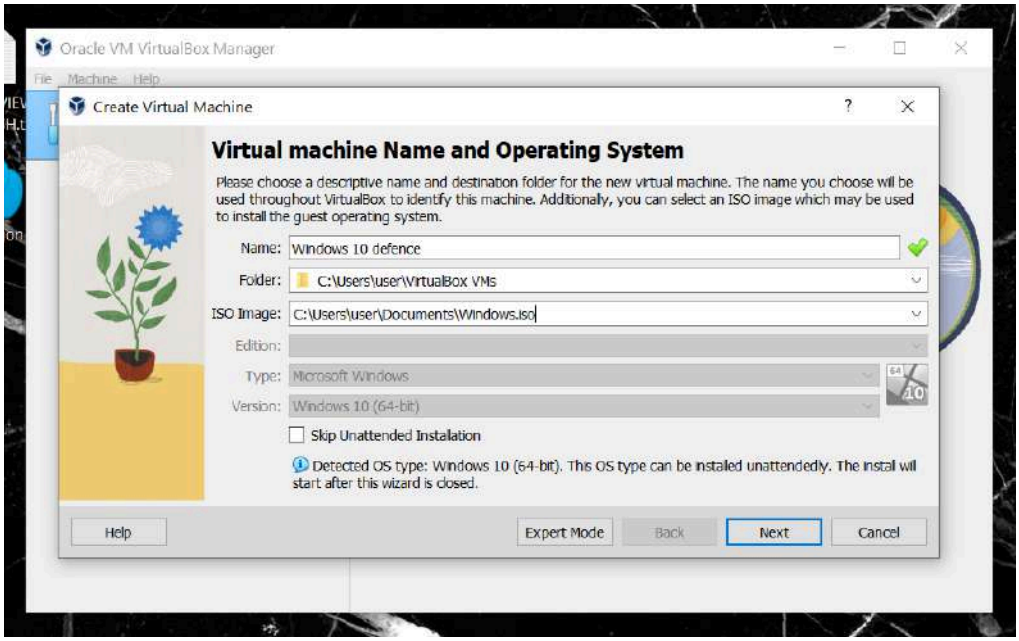
Step 3: To select the media to utilise, select an ISO file and proceed with the next step.



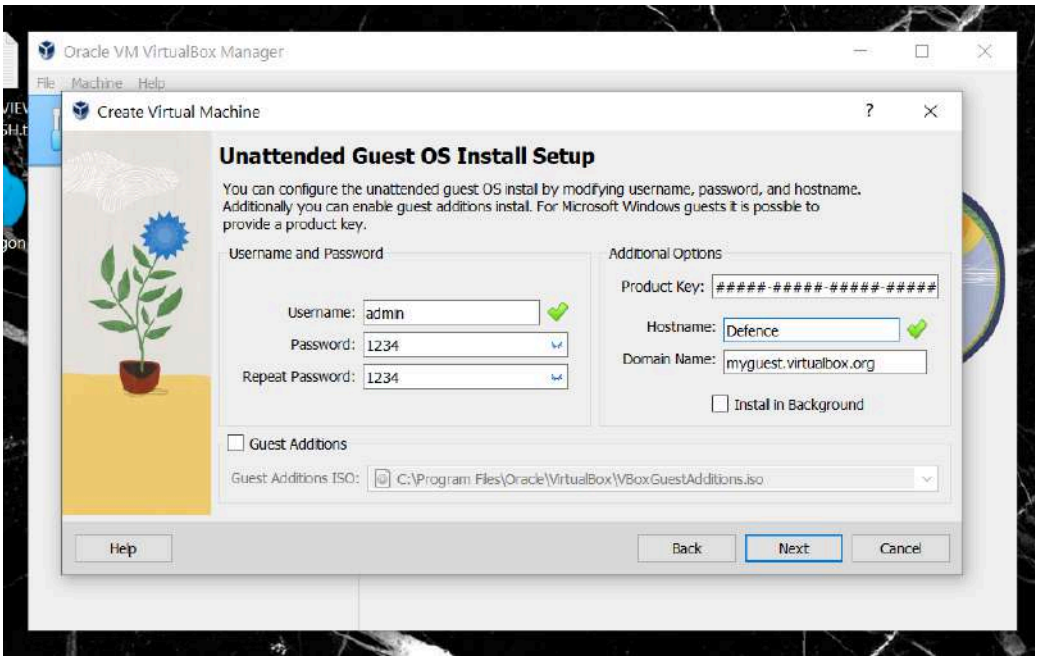
Setting up VirtualBox for Windows
Step 1: Run the VM VirtualBox and click new.



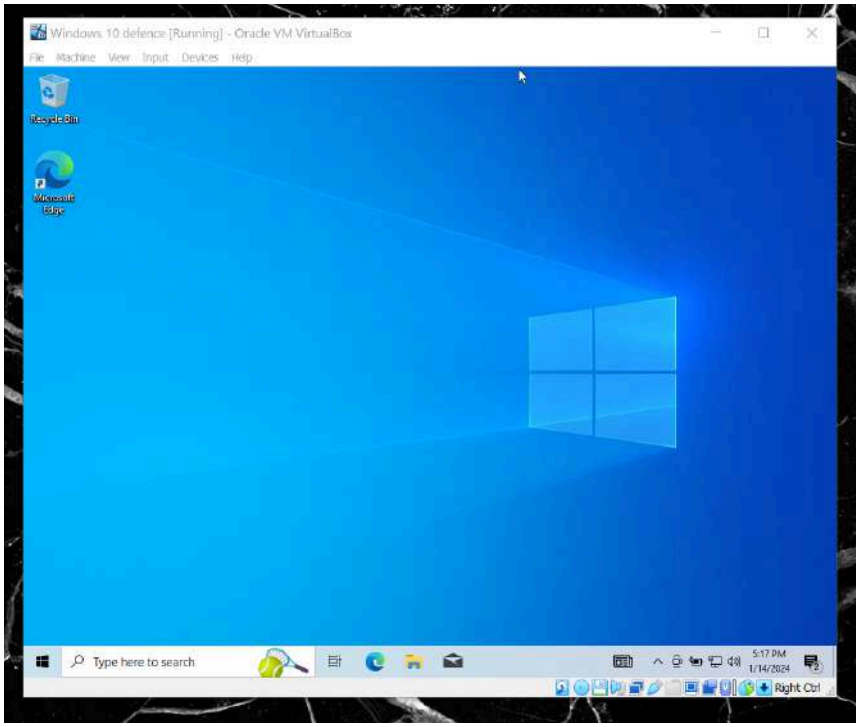
Step 2: To save the folder, enter the name "Defence Windows 10".
Select the previously saved Windows.iso from the download file and proceed to the next step.



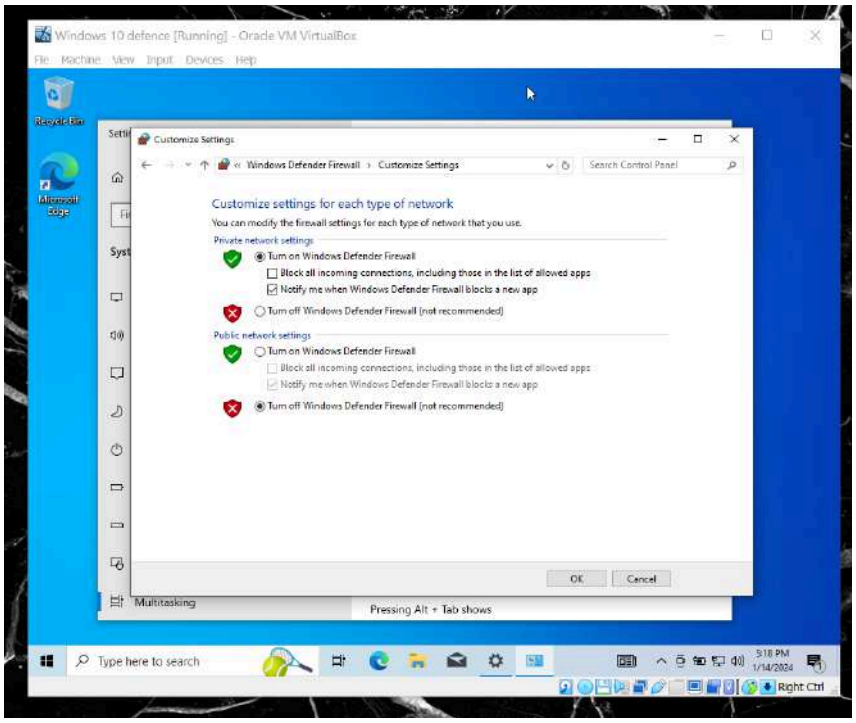
Step 3: To proceed, enter the admin username, repeat the password (1234), and click Next.



Step 4: After the setup has been completed, users can now run Windows using the virtualbox.



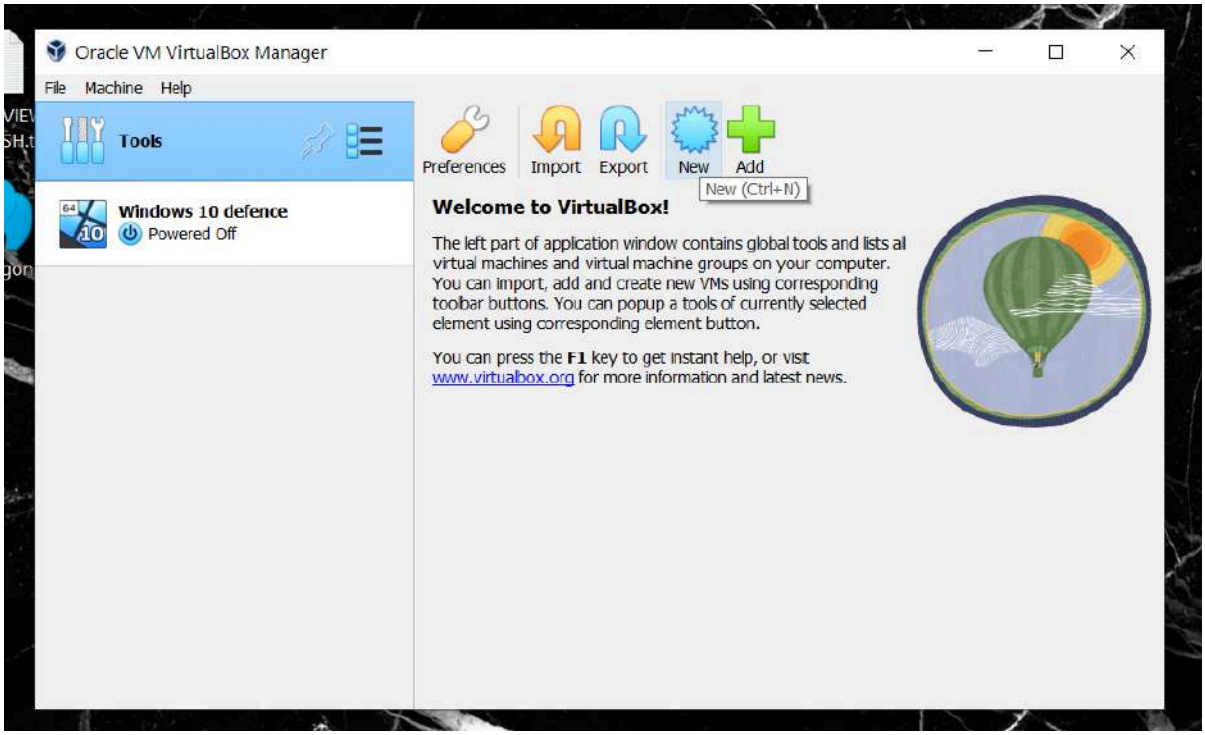
Step 5: To initiate the attack, turn off Windows Defender Wirefall.



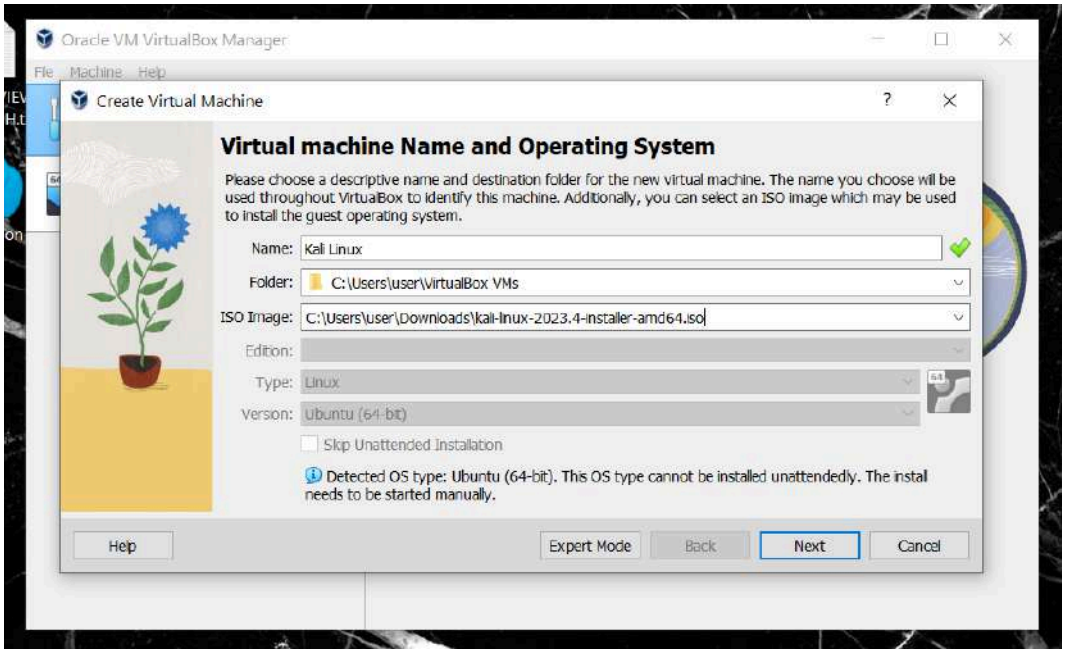
SETTING UP KALI LINUX

Step 1: Open https://www.kali.org/get-kali/#kali-installer-images Select the 64-bit installer and click to start the download.

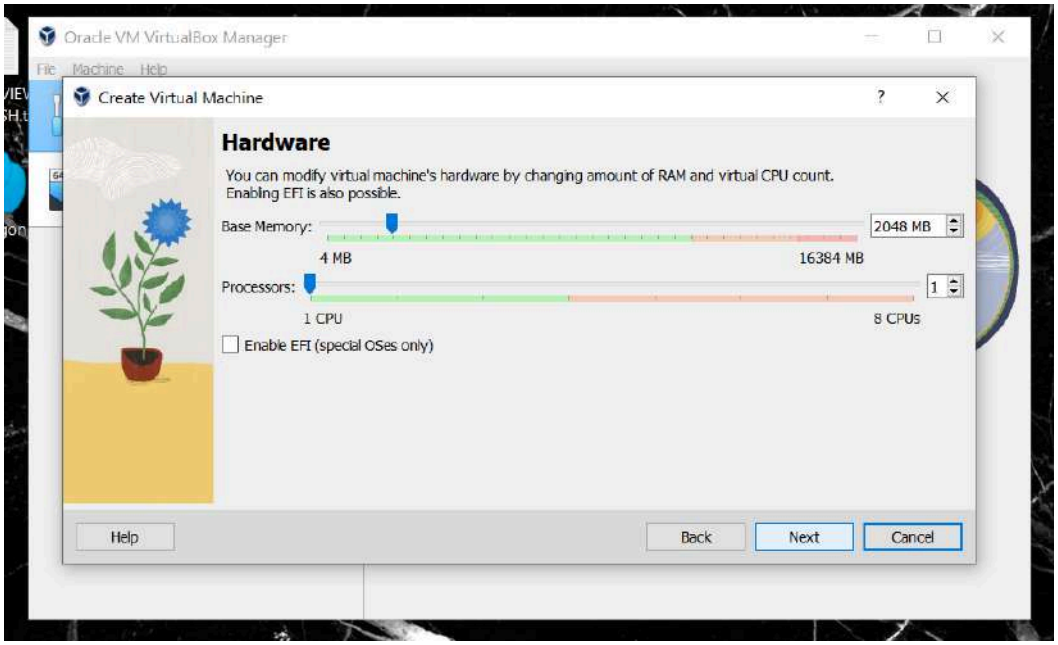
Setting up VirtualBox for Kali Linux
Step 1: Run the VM VirtualBox and click new.



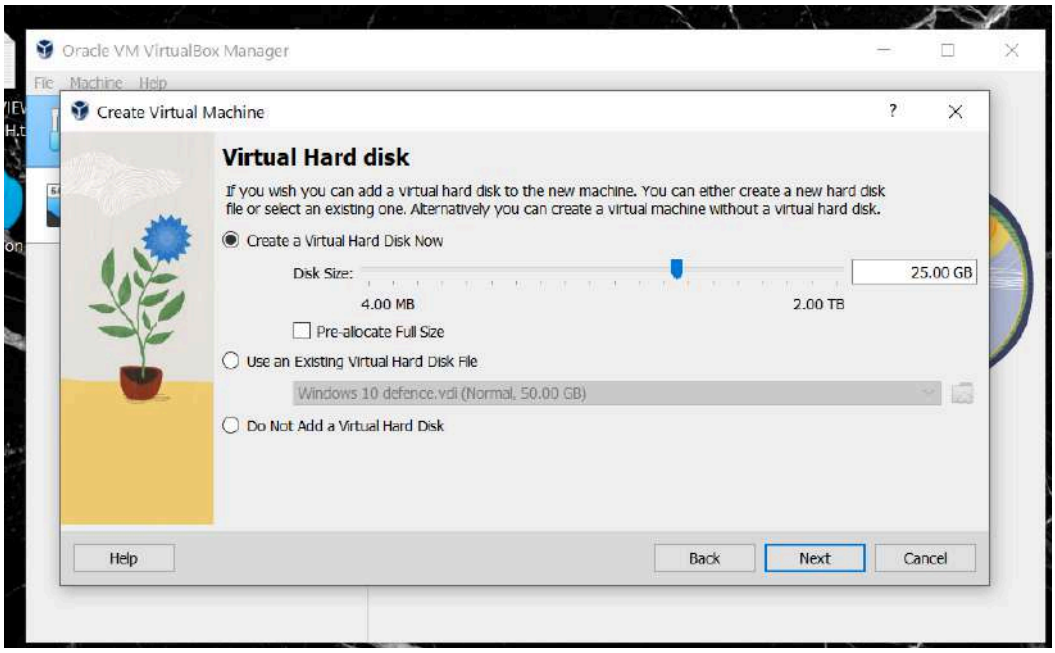
Step 2: To save a folder on Kali Linux, provide its name then, select the iso image (kali-linux-2023.4-installer-amd64.iso) saved in the download file and proceed by clicking the next button.



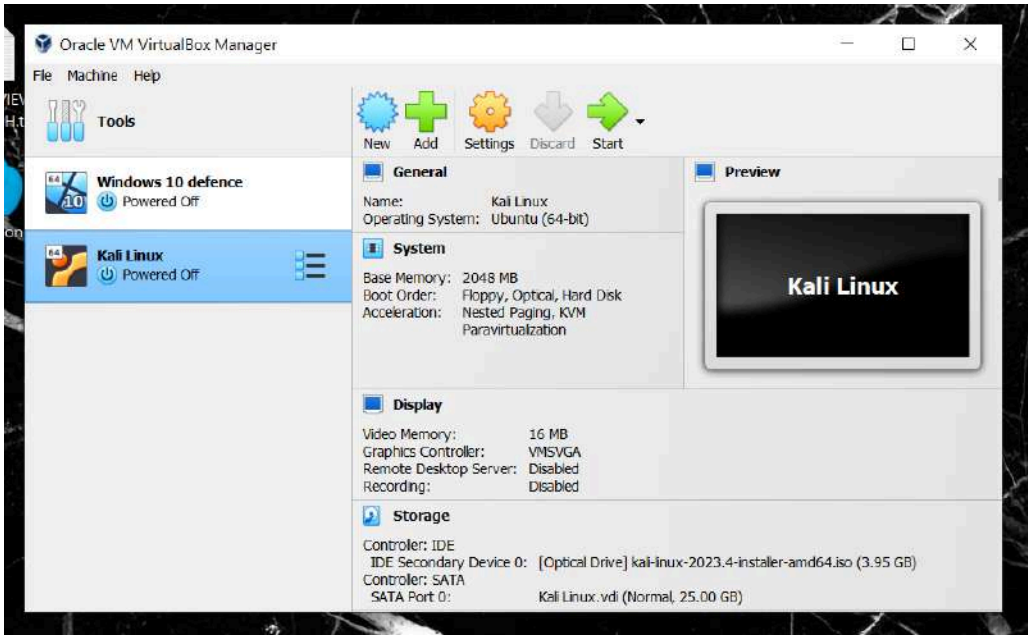
Step 3: Modify the virtual machine's hardware based on the device specifications, then click Next.



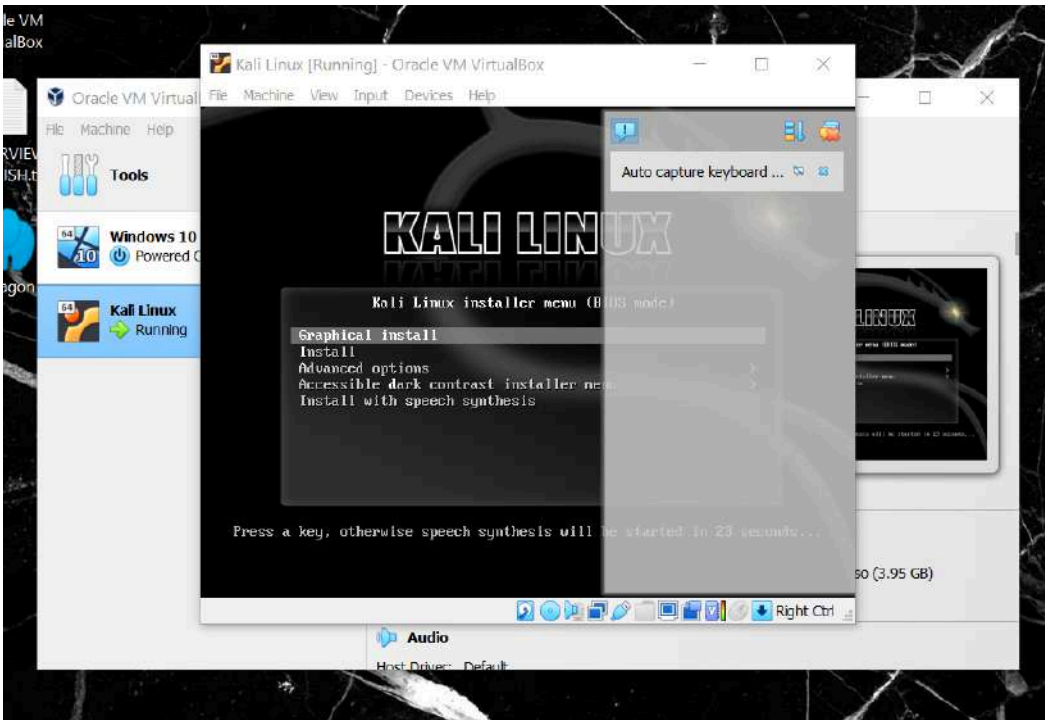
Step 4: To add a virtual hard disc or create a new one, click Next.



Step 5: The setup has been successfully completed.

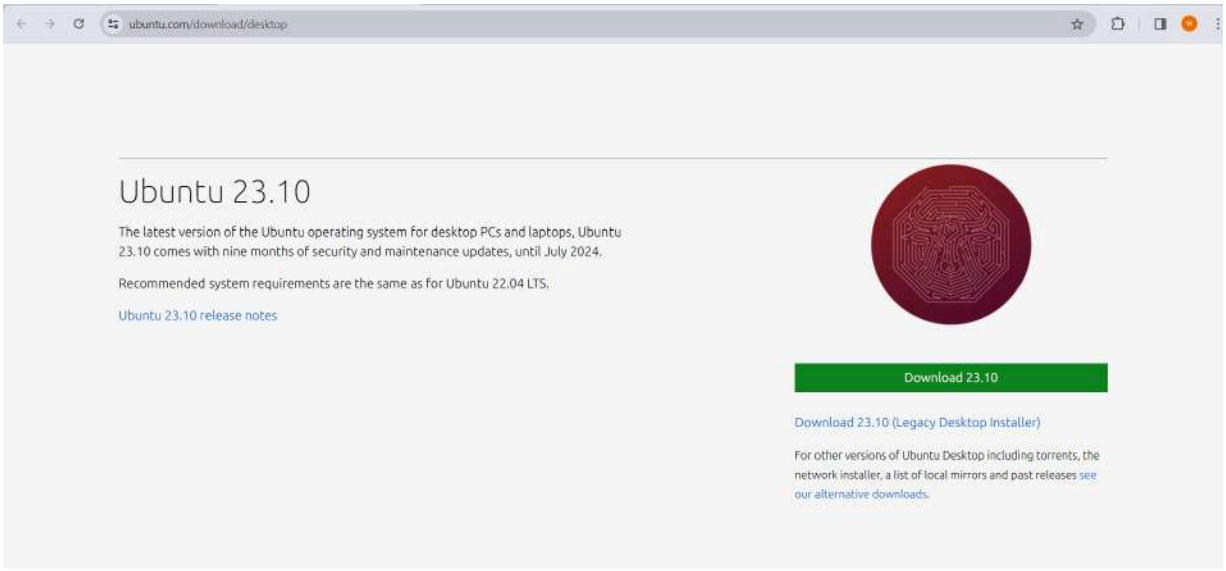


Step 6: After the setup has been completed, users can now run Kali Linux using the virtualbox.



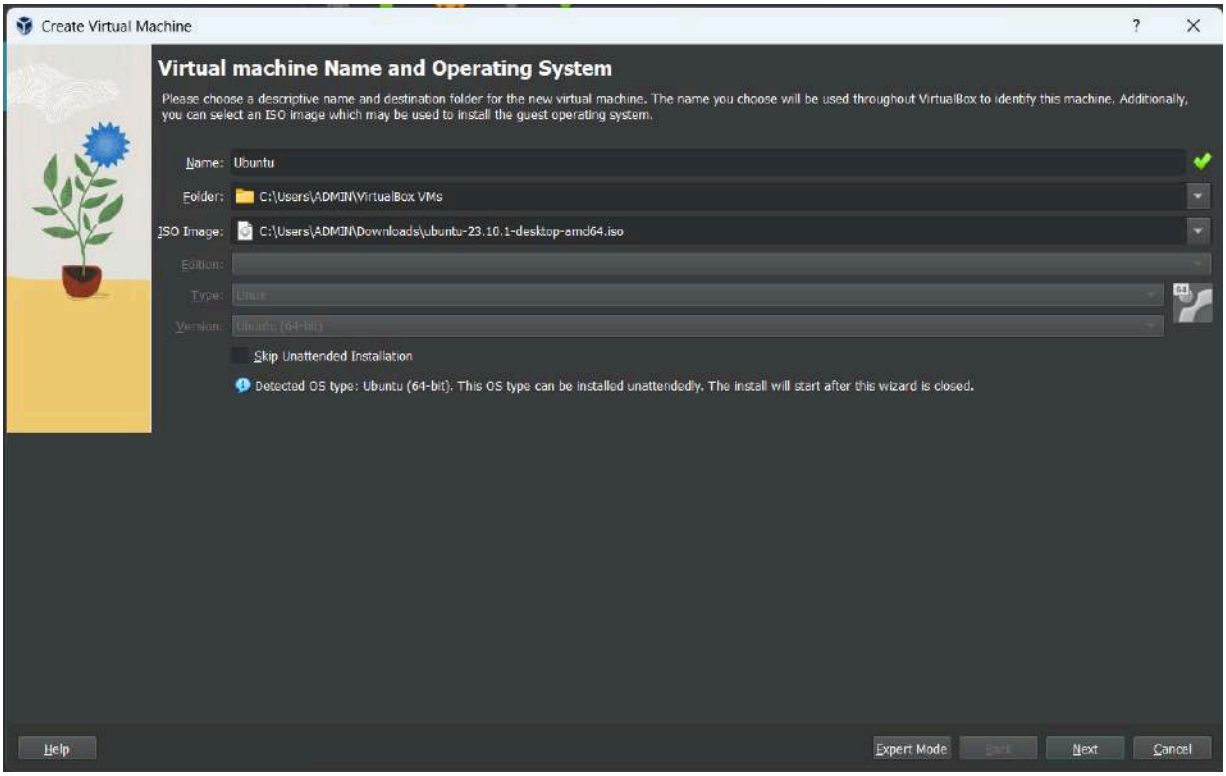
SETTING UP UBUNTU

Step 1: Download Ubuntu 23.0 through this link https://ubuntu.com/download/desktop

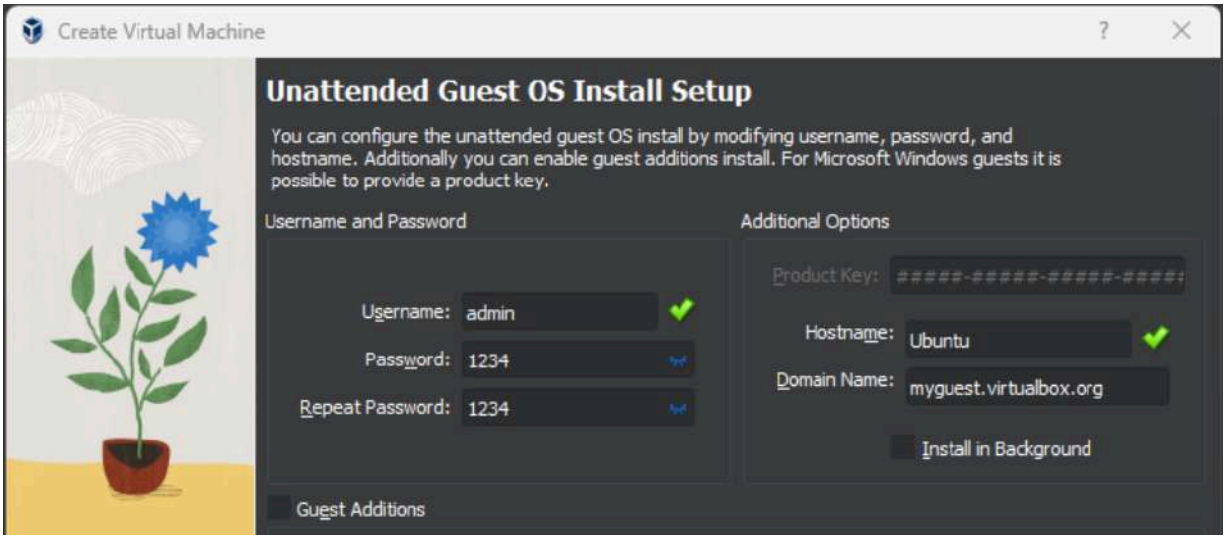


Step 2: Run the Oracle Virtual Box and click the "New" icon.

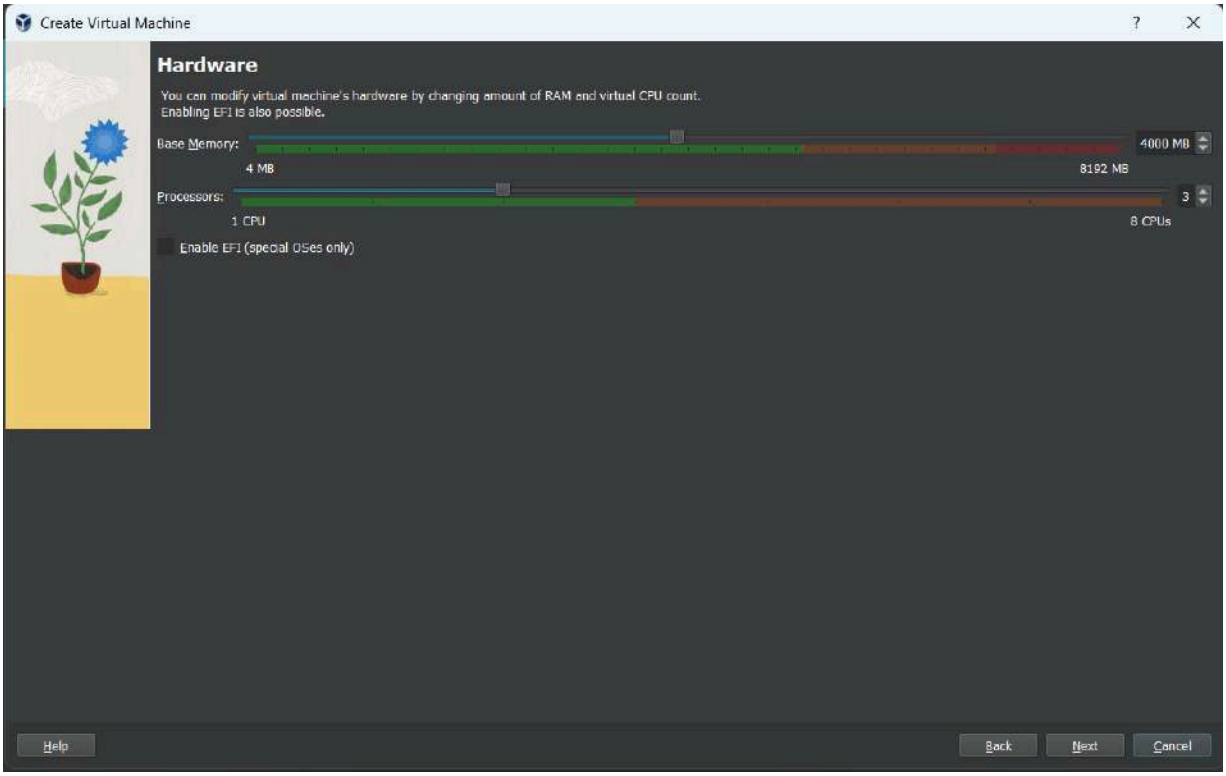
Step 3: Enter the "Ubuntu" at the Name field. Then choose the ISO image from the download file. Then, click "Next".



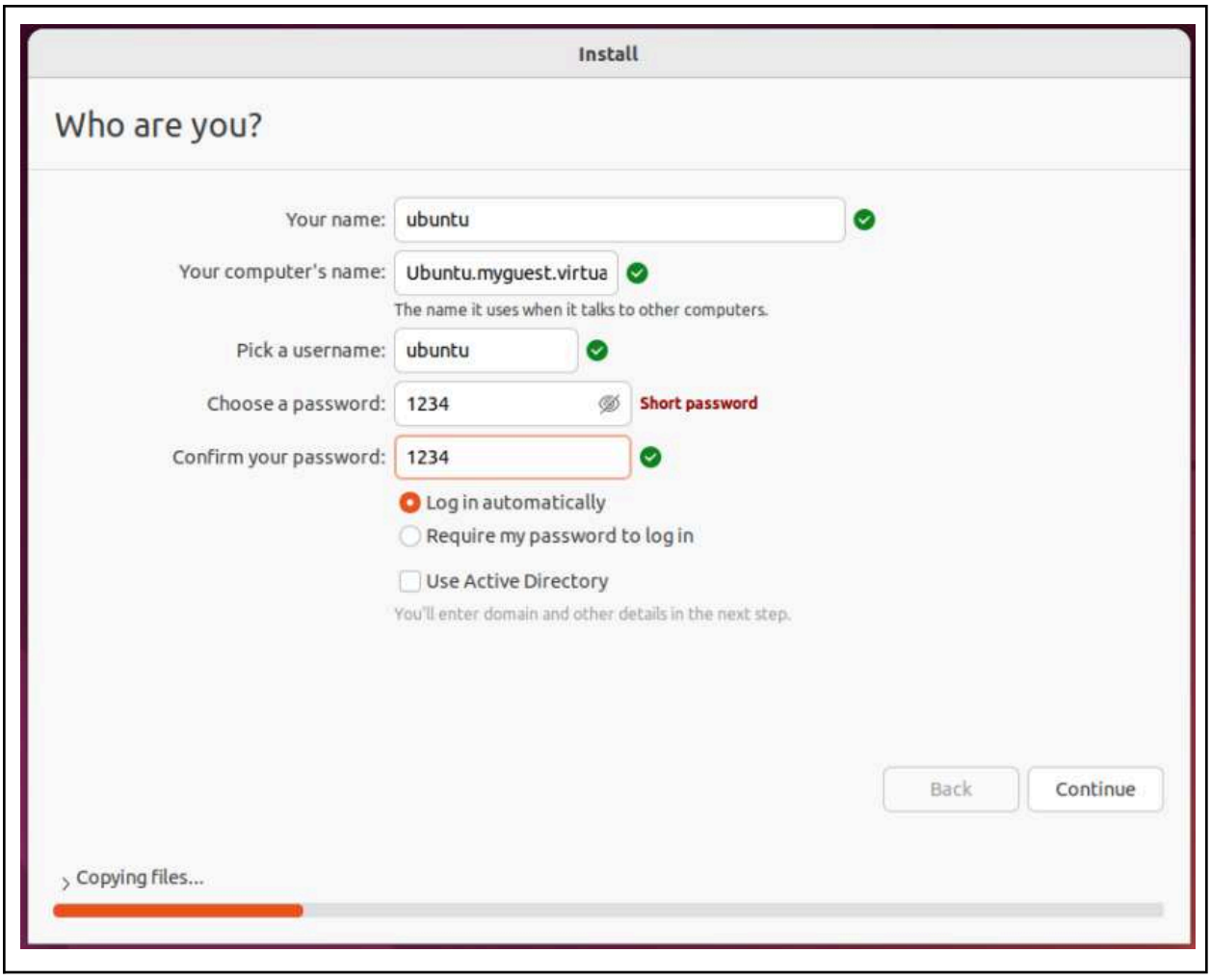
Step 4: Enter the username and password. Then, click "Next".



Step 5: Update the "Base Memory" and "Processors". After that, click the "Next" button.



Step 6: Enter a username and confirm a password same as Step 4. Then click the "Continue" button to allow the users to access Ubuntu.


Install
Who are you?
Your name:
ubuntu
Your computer's name:
Ubuntu.myguest.virtua
The name it uses when it talks to other computers.
Pick a username:
ubuntu
Choose a password:
1234
Short password
Confirm your password:
1234
Log in automatically
Require my password to log in
Use Active Directory
You'll enter domain and other details in the next step.
Back
Continue
Copying files...

ATTACK

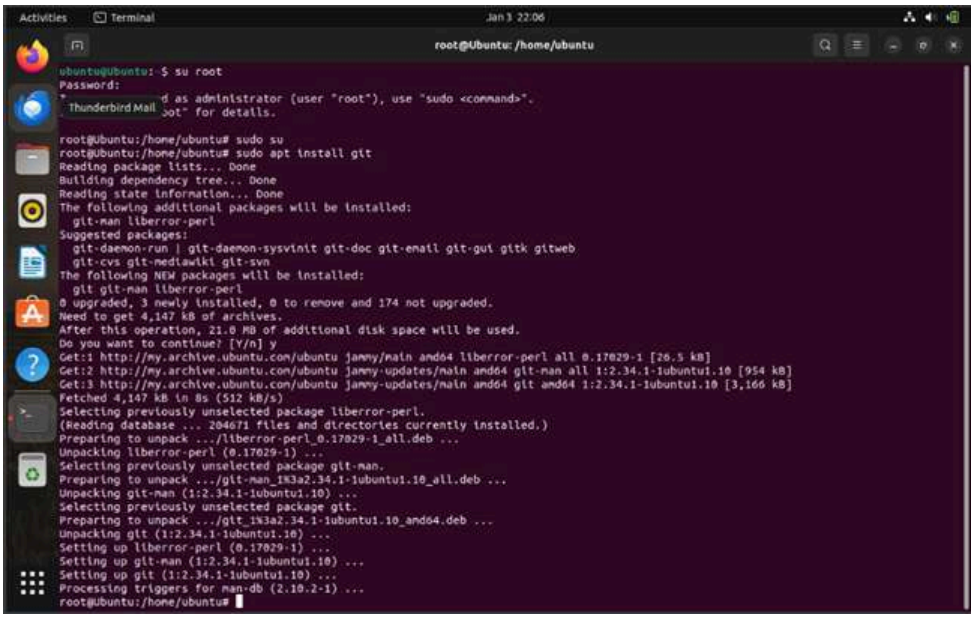
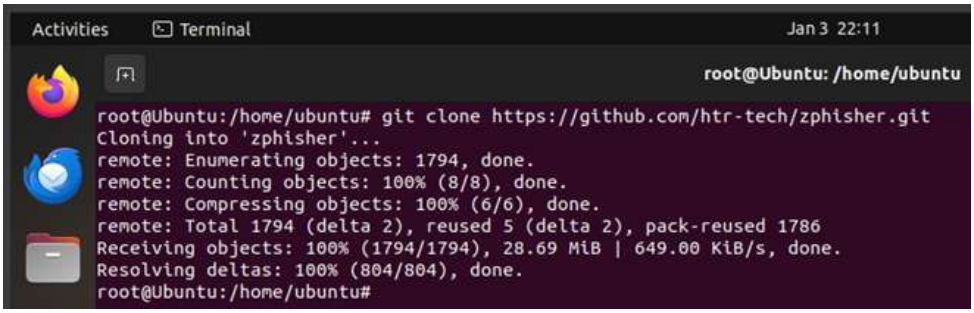
TOOLS

WINDOWS	LINUX
1. Zphisher 2. Ettercap 3. Kage 4. Slowloris 5. Cain and Abel	1. SARA 2. Storm Breaker 3. Hping3

PLANNING

WINDOWS

1. Zphisher (Instagram Phishing)

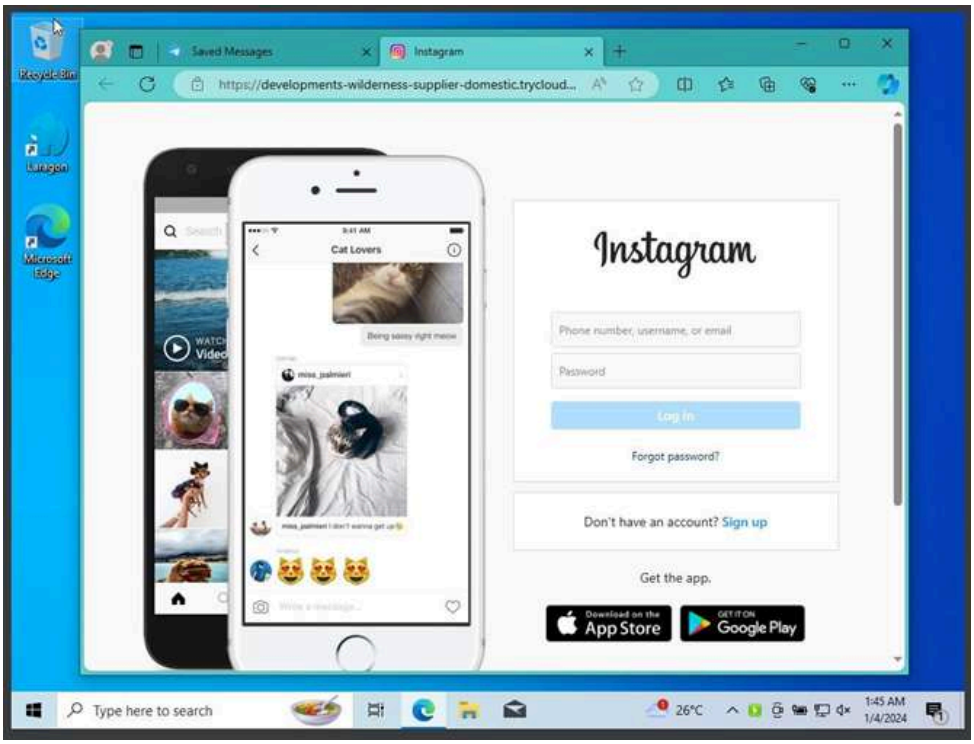
Step 1: Execute the command *sudo apt install git* to install the Git package on Ubuntu.

Step 2: Utilize the "git clone" command to fetch the Zphisher tool from its GitHub repository, specifically designed for phishing purposes.

Step 3: Develop a deceptive login page mimicking Instagram for phishing purposes.

Step 4: Specify the port configuration for the phishing setup.

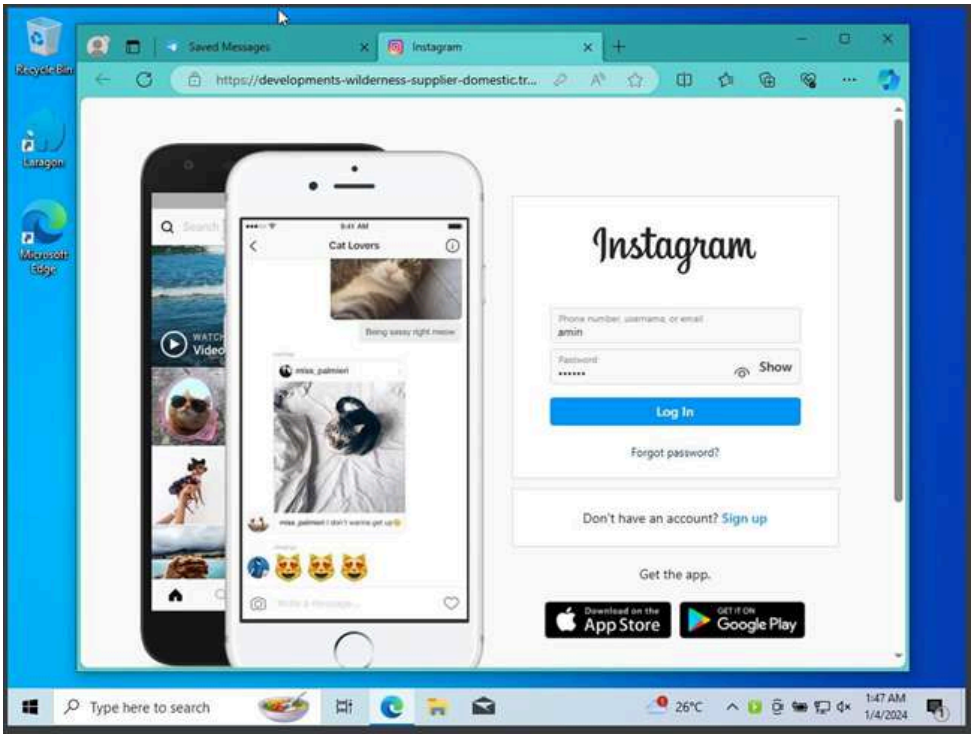
Step 5: The first URL for the phishing Instagram page has been generated.

Step 6: Upon clicking the following link: https://developments-wilderness-supplier-domestic.trycloudflare.com/login.ht

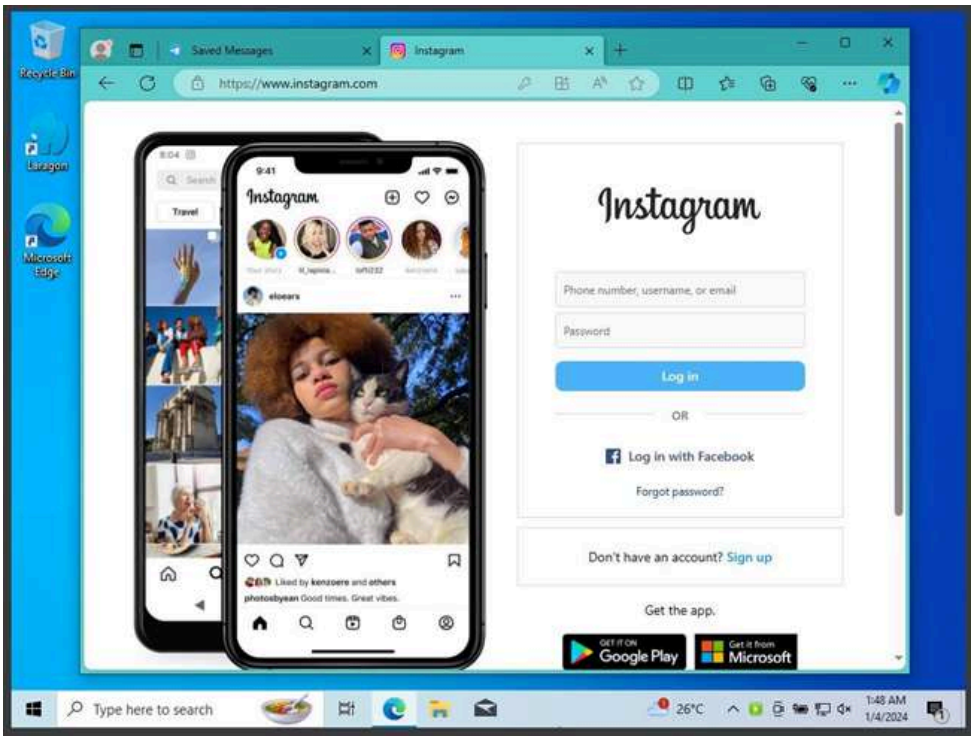
ml, users will be redirected to the phishing Instagram login page.



Step 7: Users are prompted to input their login credentials, including username and password, and subsequently click the login button.



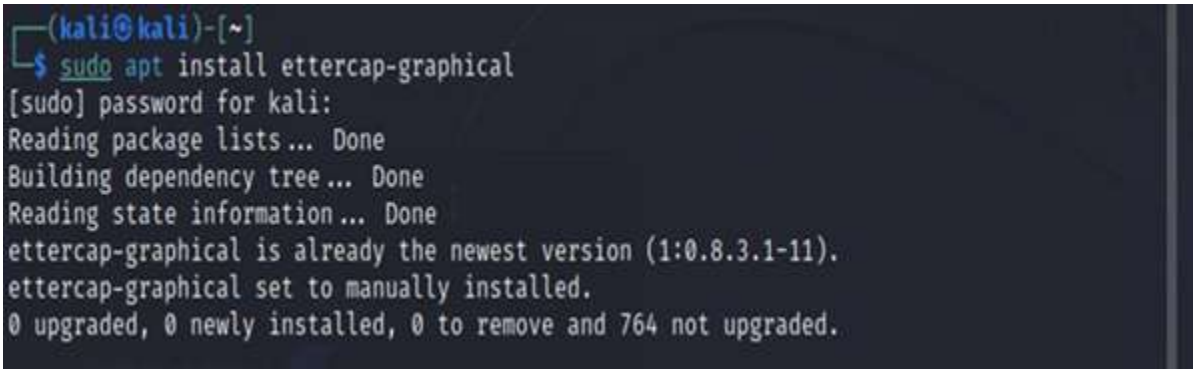
Step 8: Upon clicking the login button on the phishing page, the user will be redirected to the authentic Instagram login page.



Step 9: While the user logs in on the phishing Instagram page from a Windows 10 machine, the entered credentials are saved in the "auth/ip.txt" file on the attacker's Ubuntu machine.

2. Ettercap

Step 1: Install Ettercap on Kali Linux by executing the command: *sudo apt install ettercap-graphical*.



Step 2: After the installation is finished, go to the Ettercap directory by typing *cd /etc/ettercap*.

Step 3: Display all folders in the Ettercap directory by typing *ls*.

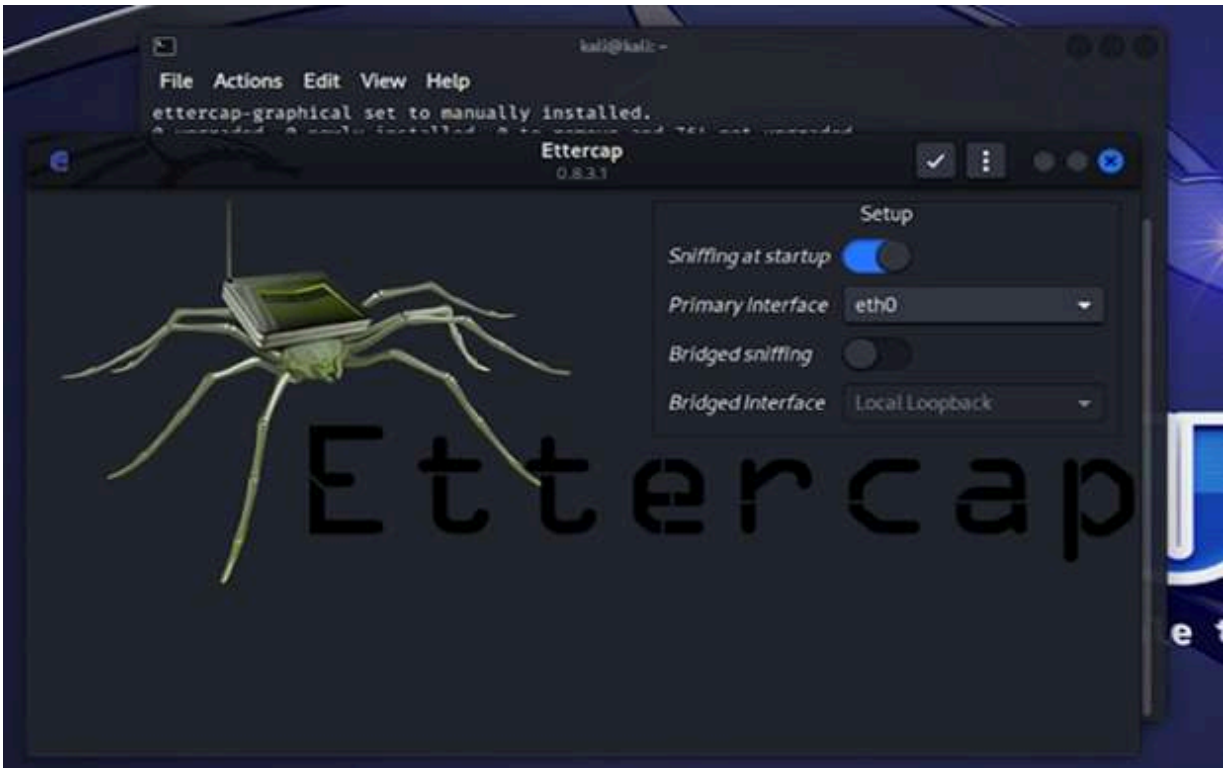
Step 4: Subsequently, open the file named *etter.conf* using the command *nano etter.conf*. In this file, modify the *ec_uid* and *ec_gid* lines to have the value 0.

Step 5: Save the changes to the settings.

Step 6: Once the configuration is done, initiate Ettercap by using the command *sudo ettercap-G*.

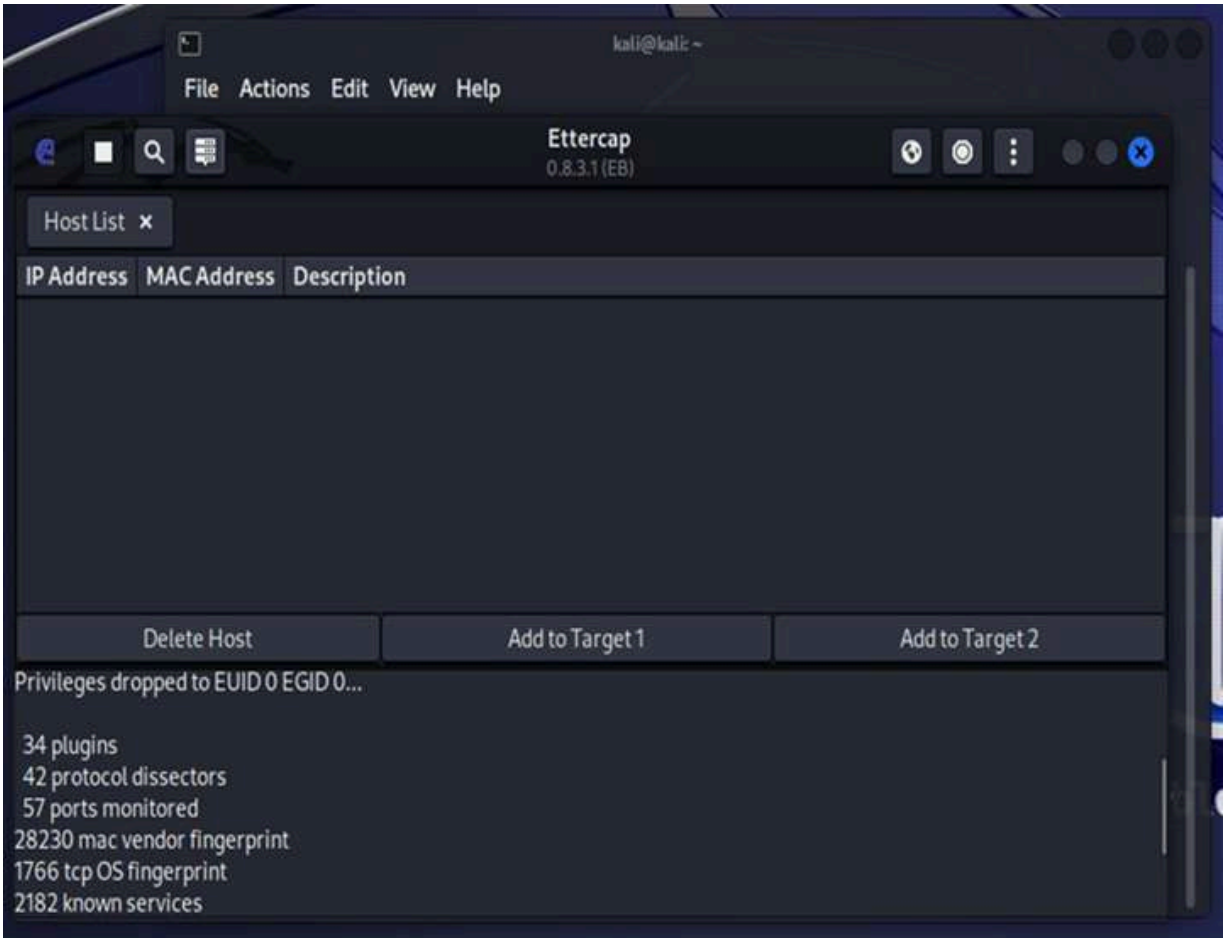
```
┌──(kali㉿kali)-[~]
└─$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team


(ettercap:4721): GLib-WARNING **: 09:46:02.095: In call to g_spawn_sync(), wait status o
f a child process was requested but ECHILD was received by waitpid(). See the documentat
ion of g_child_watch_source_new() for possible causes.
```

Step 7: Select the primary interface as eth0 and click the Accept button to proceed.

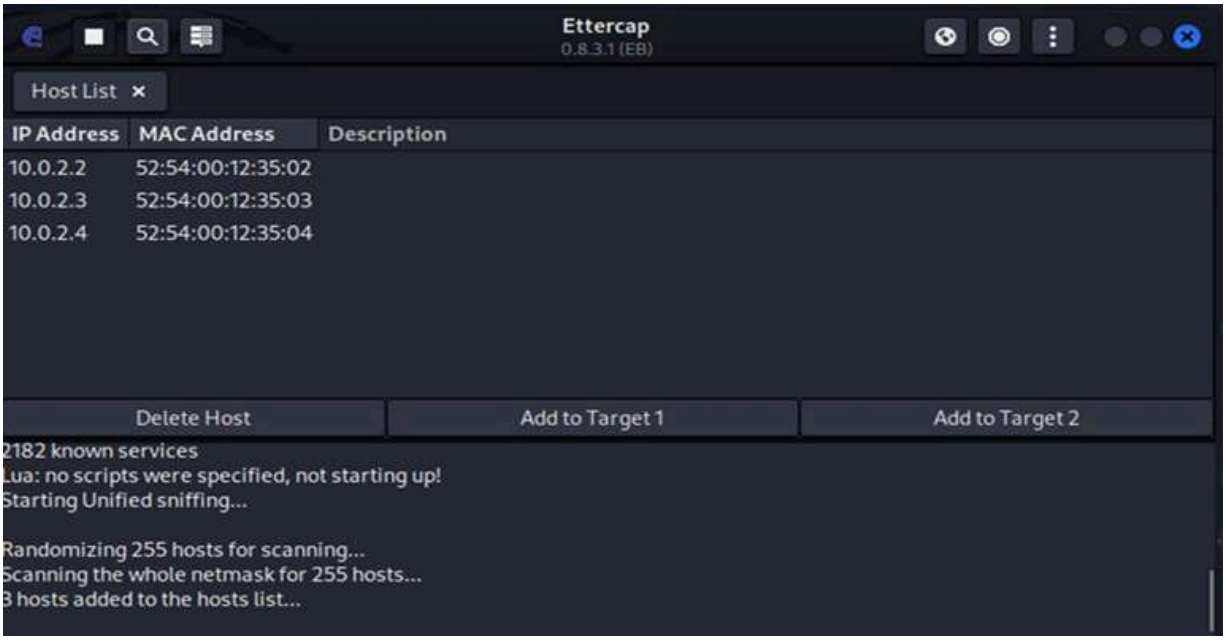


Step 8: Access the host list panel by clicking on the host list icon, which is the fourth button from the left.

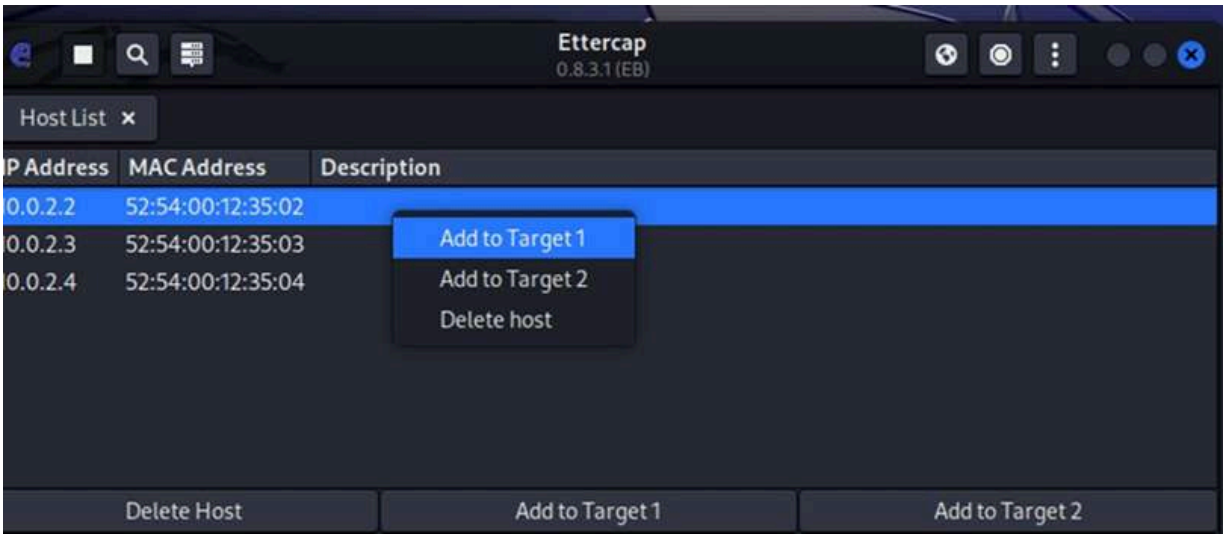
Step 9: Perform a host scan by clicking on the Scan for Hosts button, located as the third button from the left.

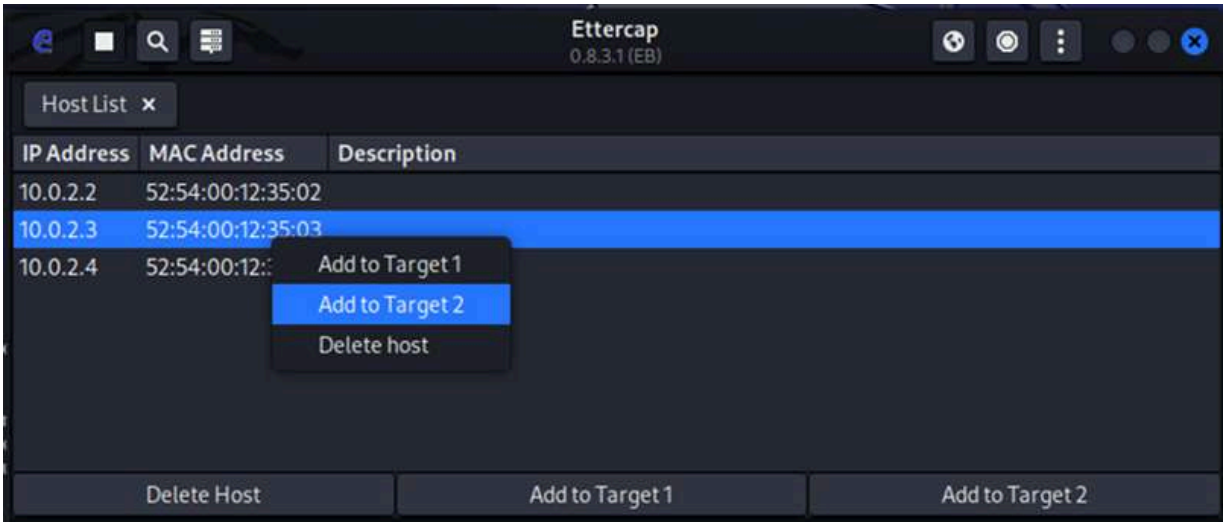


Step 10: Confirm that the host lists are now visible on the screen.



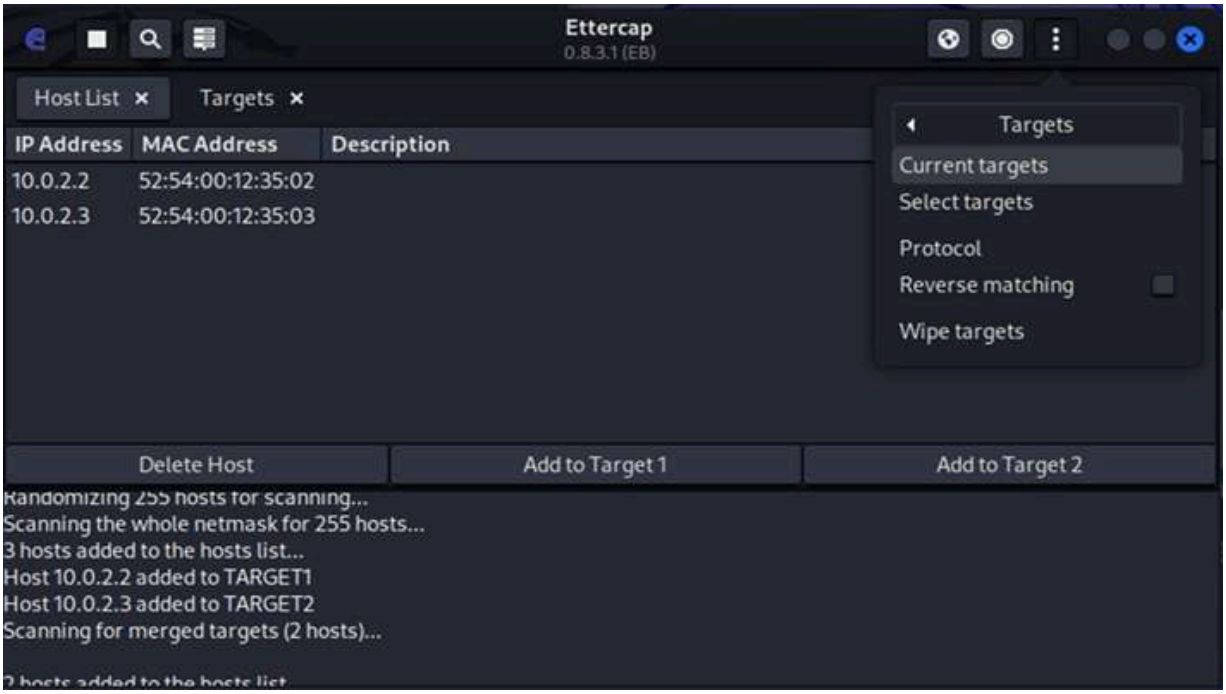
Step 11: Choose the IP addresses from the host lists and assign them as Target 1 and Target 2.

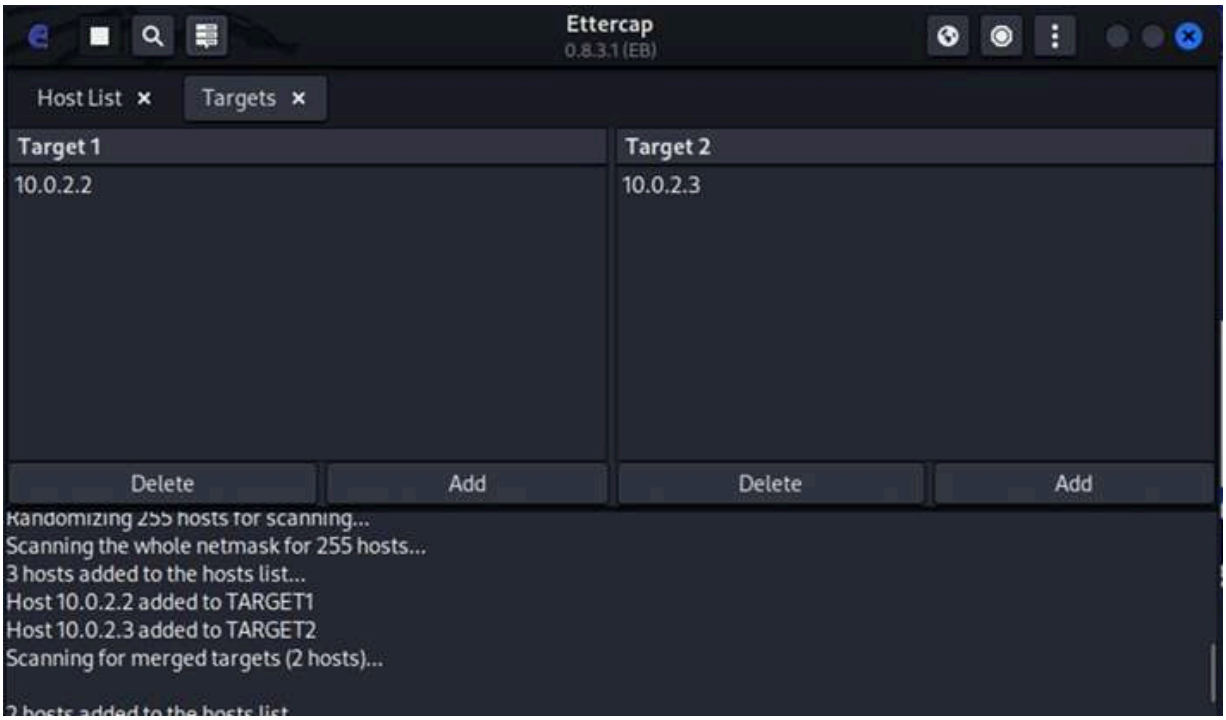




Step 12: Once the targets are selected, open the Targets panel to review the chosen IP addresses.

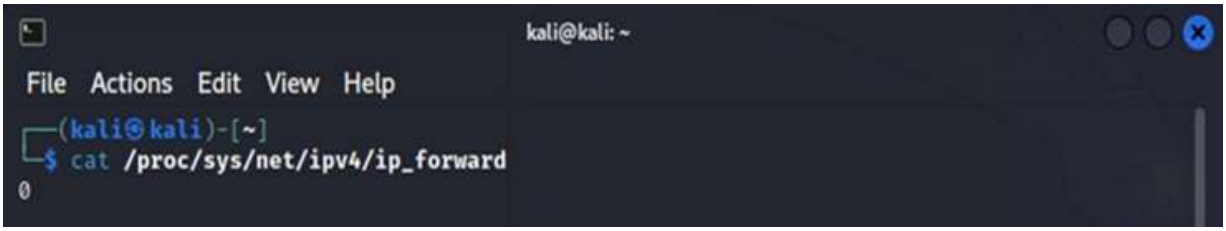
Step 13: Navigate to the Ettercap menu, select Targets, and then choose Current Target.





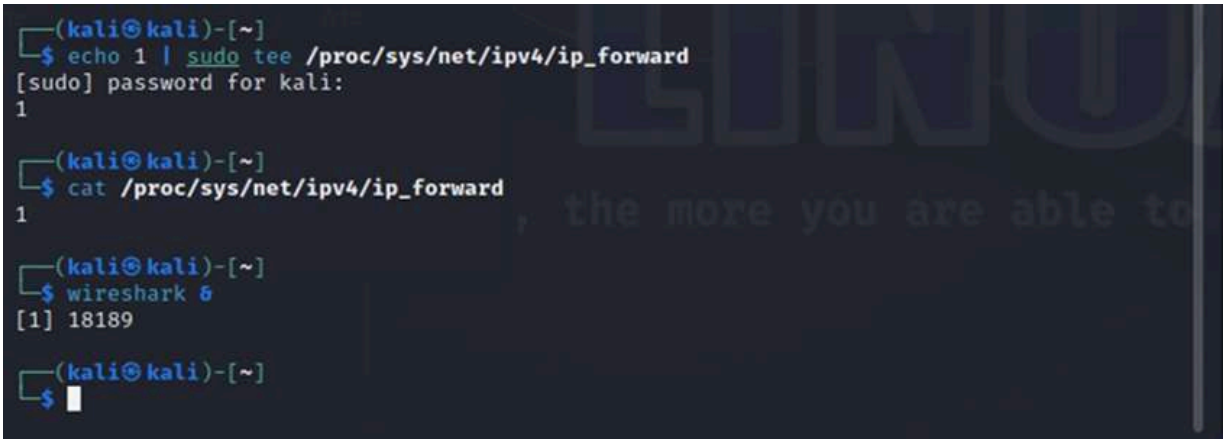
Step 14: Open a new terminal and check the value of ip_forward by typing

cat /proc/sys/net/ipv4/ip_forward.

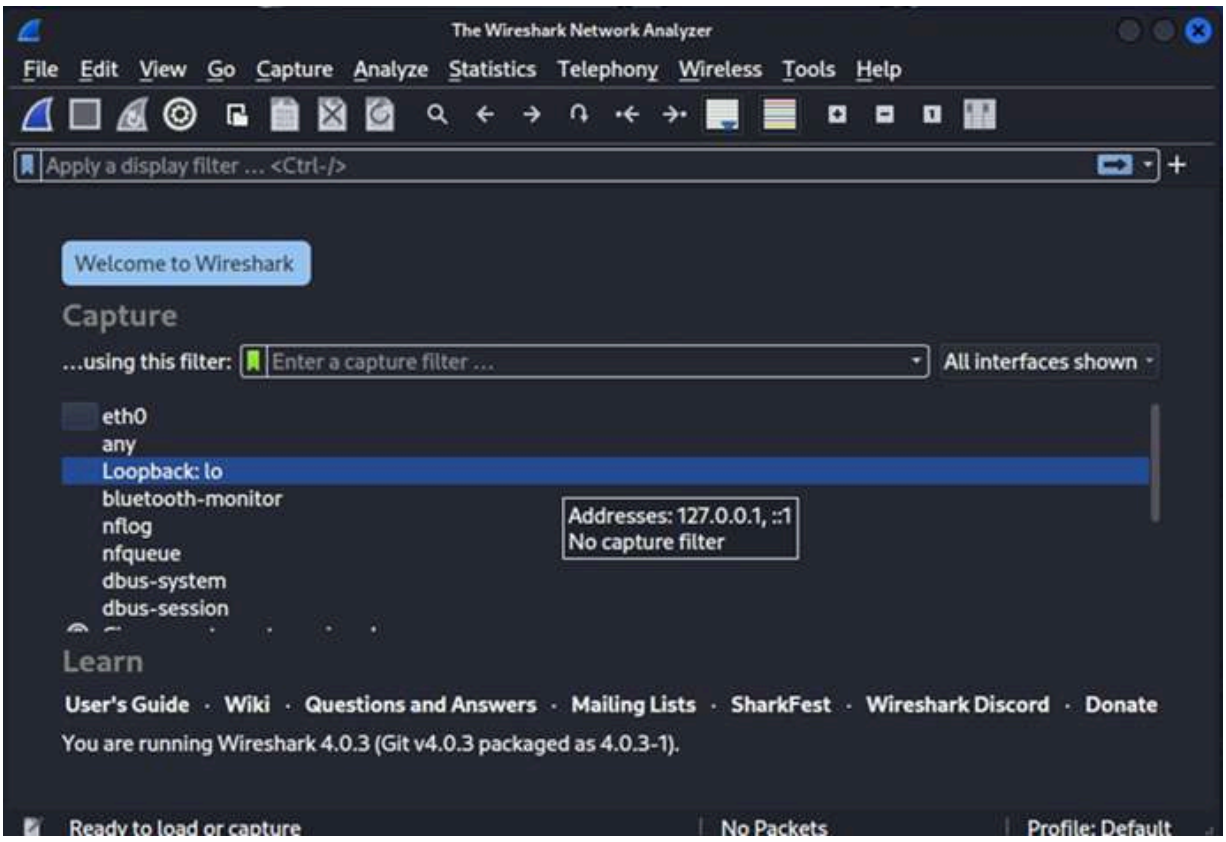


Step 15: Open a new terminal and set the ip_forward value to 1 by entering the command *echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward*.

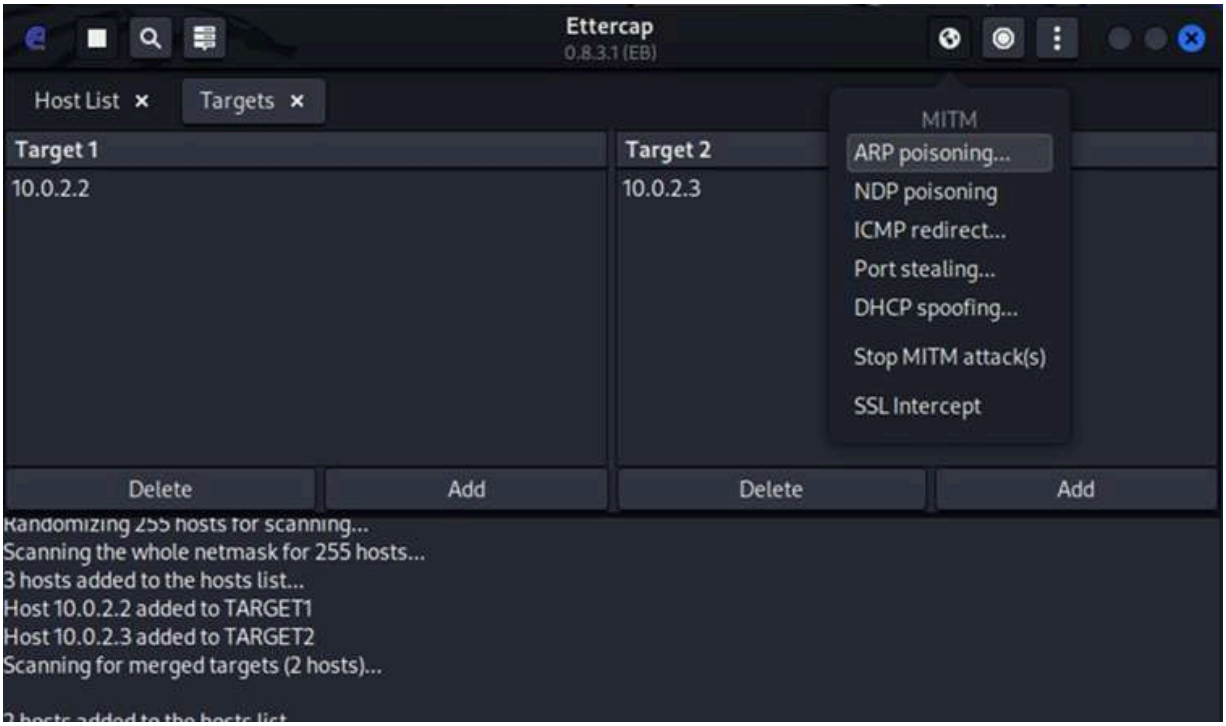
Step 16: If prompted, provide your password. Following that, initiate Wireshark by executing the command *wireshark &*.



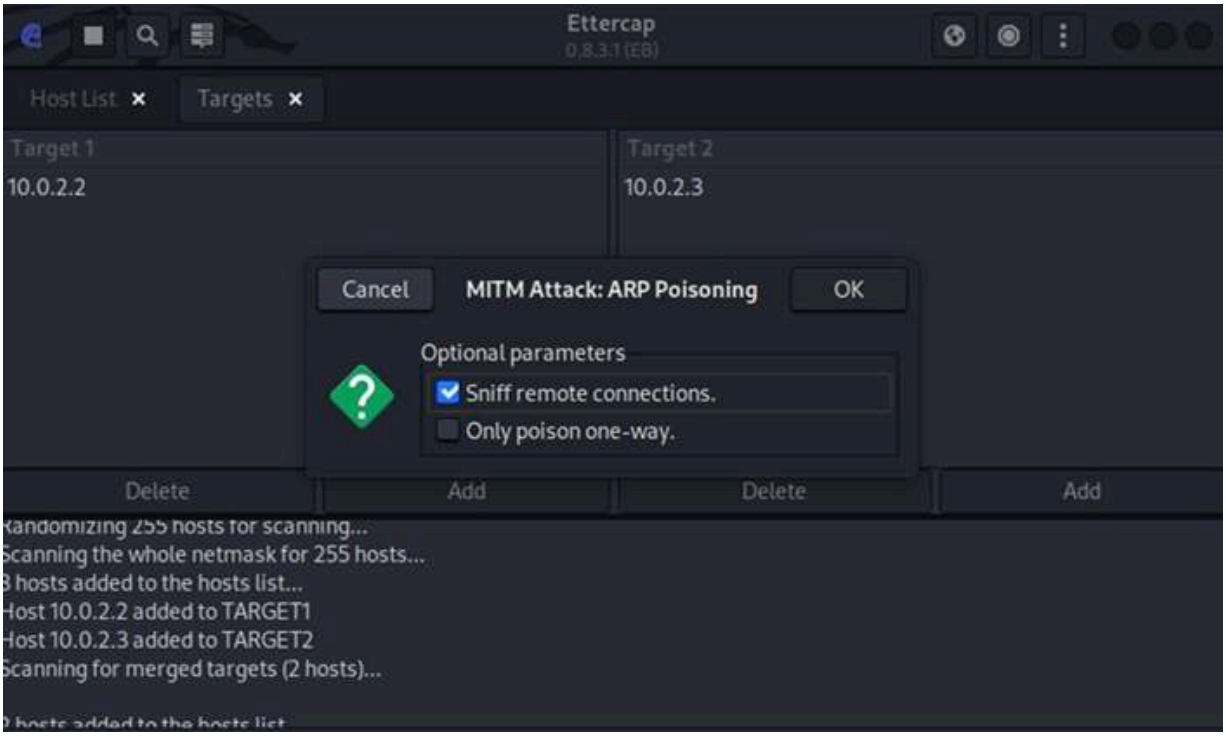
Step 17: Once Wireshark is open, choose the eth0 network interface to capture the network traffic.



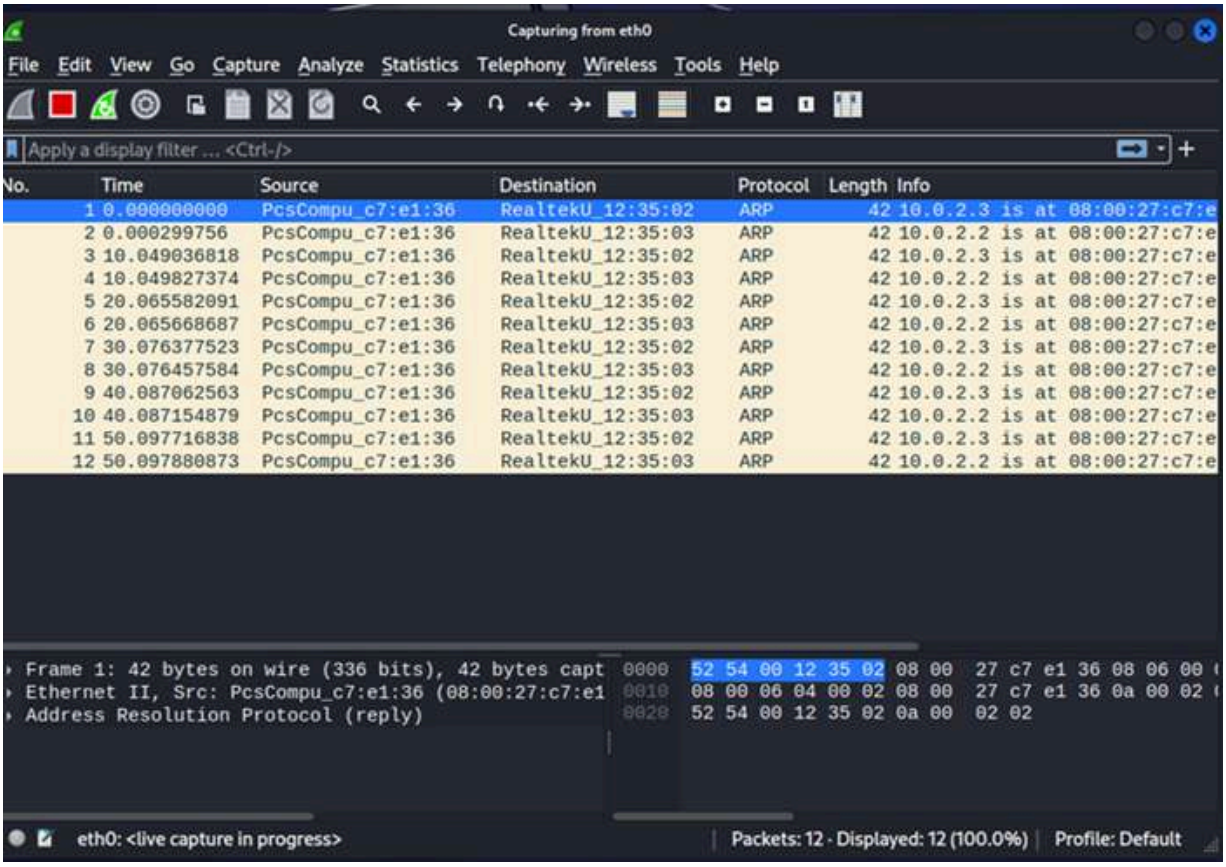
Step 18: Go to the MITM (Man-in-the-Middle) button, located as the third button from the right, and click on ARP Poisoning.



Step 19: Select "Sniff remote connections" and click OK to commence ARP poisoning in the network.

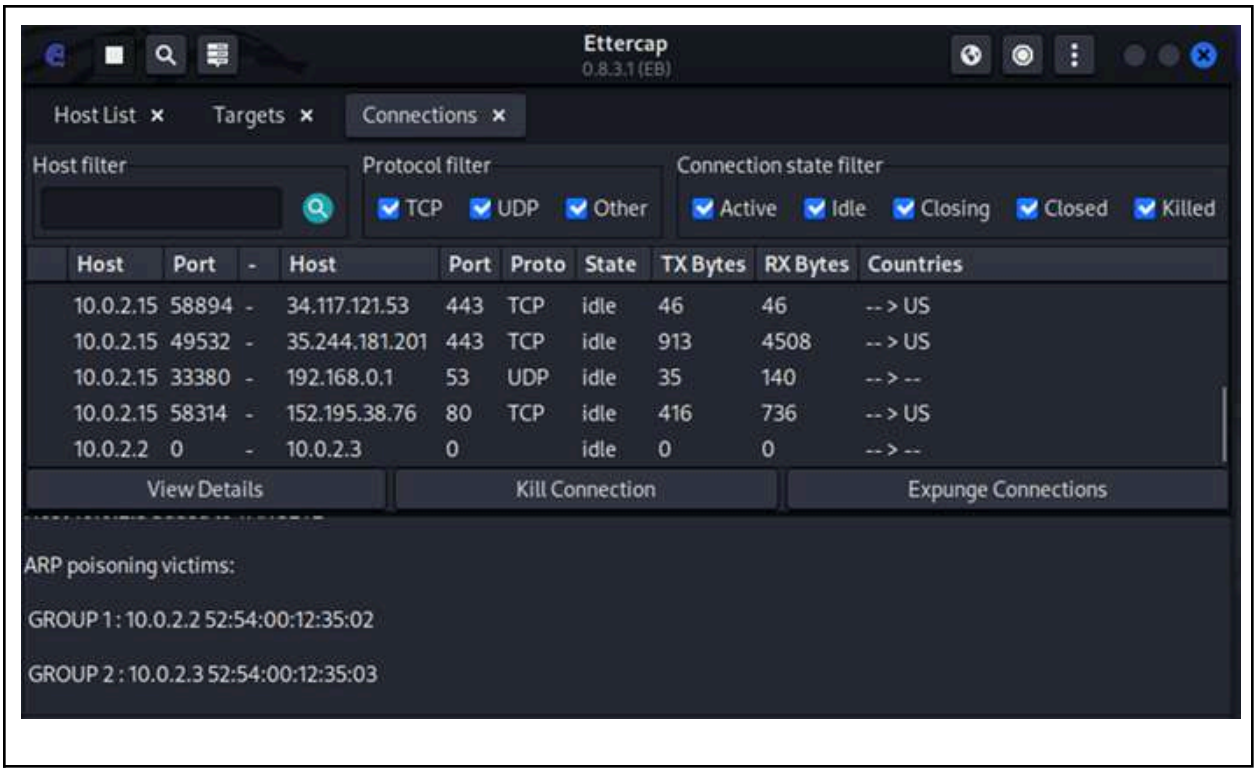


Step 20: As ARP poisoning commences, multiple ARP messages are broadcasted to the network, leading to confusion among various IP addresses.



Step 21: Examine the target's active connections by opening the connection.

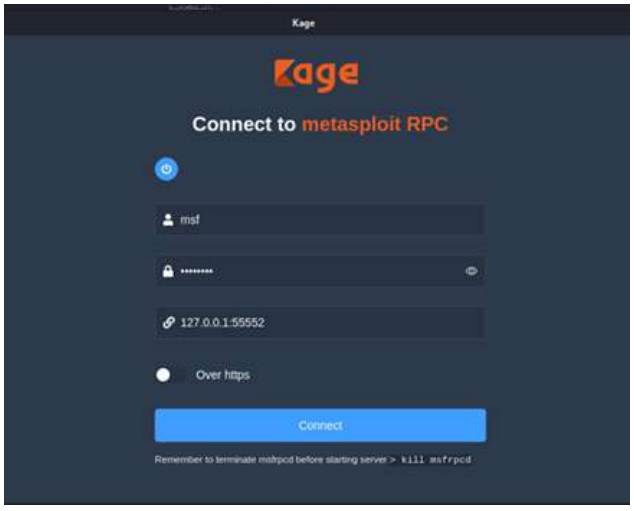
Step 22: Click on the connection and observe the sent information on the left and the received information on the right, provided the packets are not encrypted.


Ettercap
0.8.3.1 (EB)
Host List ×
Targets ×
Connections ×
Host filter
Protocol filter
TCP
UDP
Other
Connection state filter
Active
Idle
Closing
Closed
Killed
Host Port - Host Port Proto State TX Bytes RX Bytes Countries
10.0.2.15 58894 - 34.117.121.53 443 TCP idle 46 46 --> US
10.0.2.15 49532 - 35.244.181.201 443 TCP idle 913 4508 --> US
10.0.2.15 33380 - 192.168.0.1 53 UDP idle 35 140 --> --
10.0.2.15 58314 - 152.195.38.76 80 TCP idle 416 736 --> US
10.0.2.2 0 - 10.0.2.3 0 idle 0 0 --> --
View Details
Kill Connection
Expunge Connections
ARP poisoning victims:
GROUP 1 : 10.0.2.2 52:54:00:12:35:02
GROUP 2 : 10.0.2.3 52:54:00:12:35:03

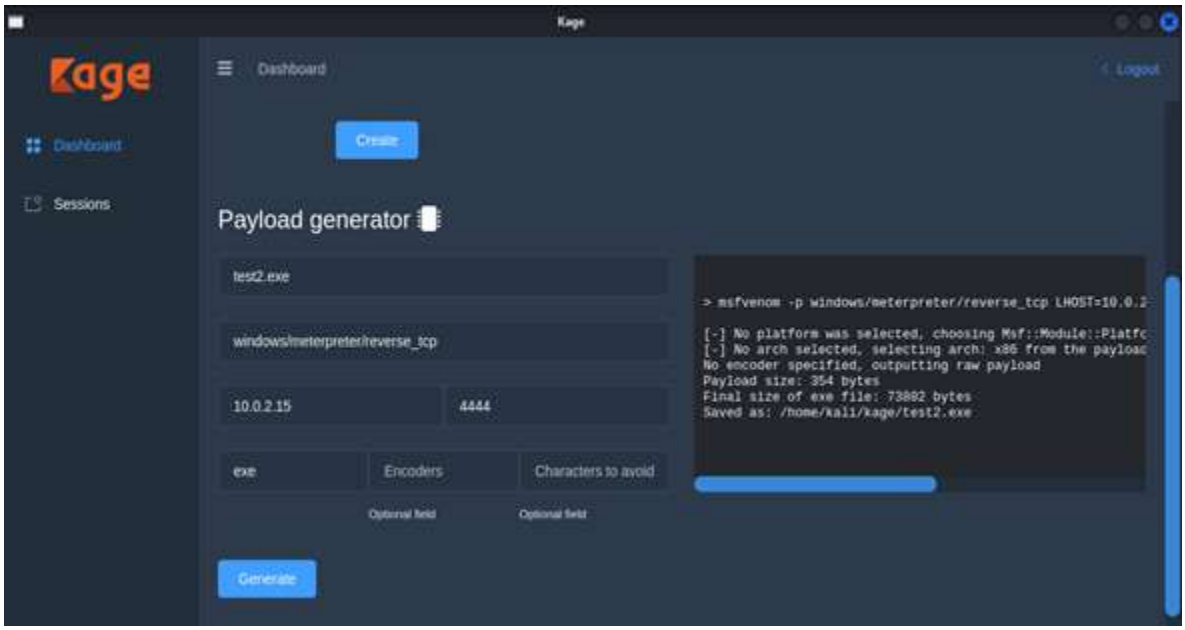
3. Kage

Step 1: Install Ettercap on Kali Linux by executing the command: *sudo apt install ettercap-graphical*.

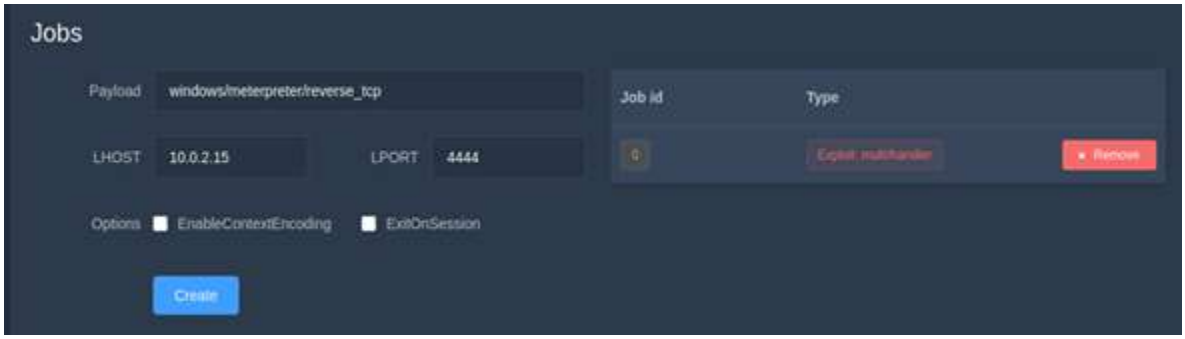
Step 2: Execute *msgrpc* to obtain the username and password required for logging into Kage.



Step 3: After logging in, proceed to create a new botnet through the payload generator. Here, we'll craft the test2.exe botnet for our use.



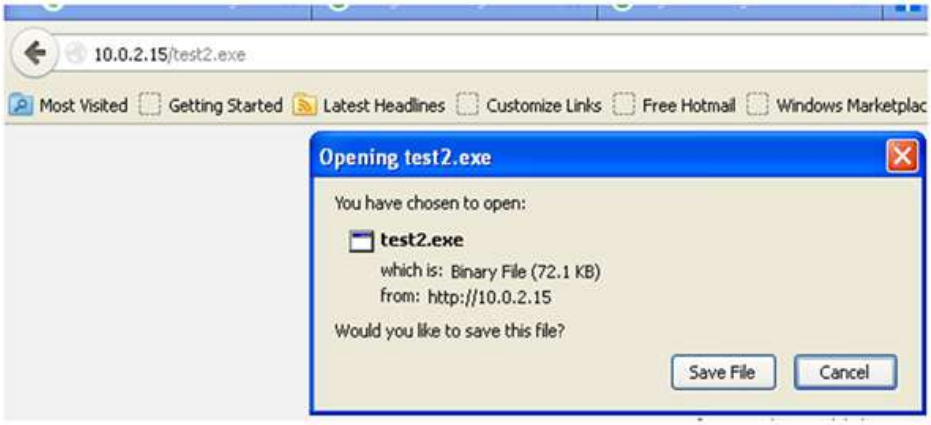
Step 4: Furthermore, navigate to the Jobs section in Kage to configure the payload, lhost, and lport for exploitation.



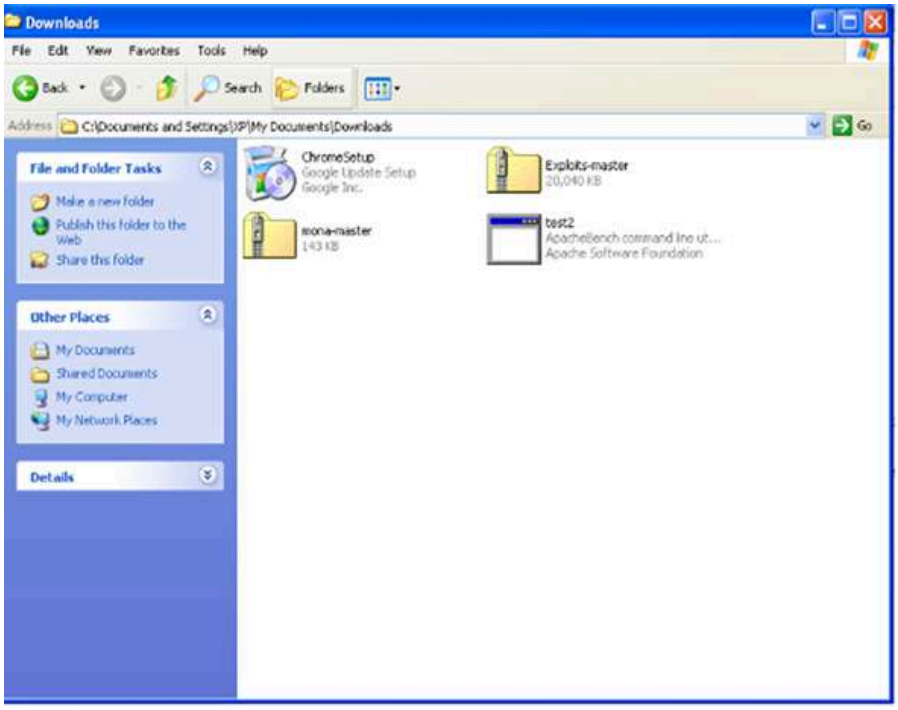
Step 5: Subsequently, initiate the Apache service after transferring the botnet to HTML. This action allows the victim to establish a connection with the attacker's botnet.

```
┌──(kali㉿kali)-[~]
└─$ sudo mv /home/kali/kage/test2.exe /var/www/html/

┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
```

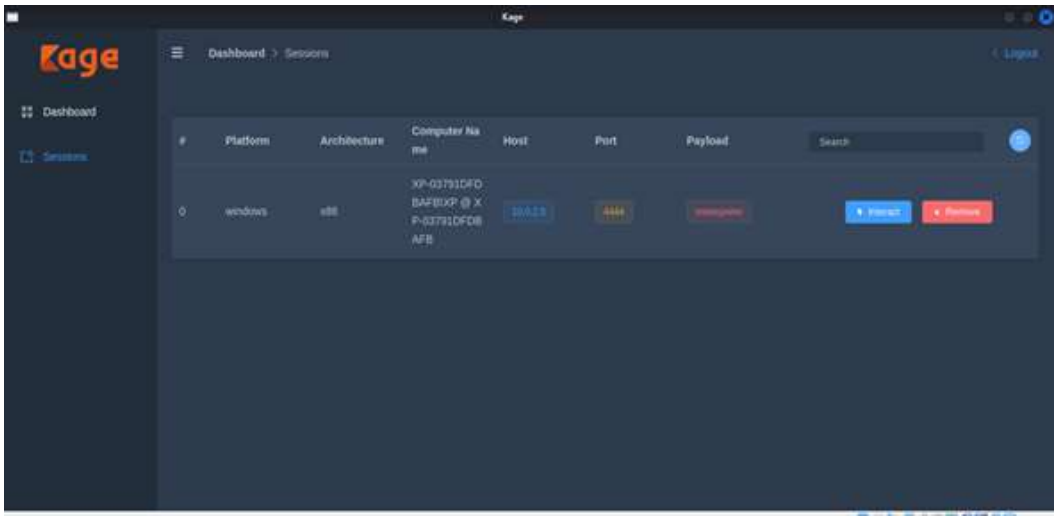
Step 6: Download the file onto the Windows XP system using the attacker's IP address.



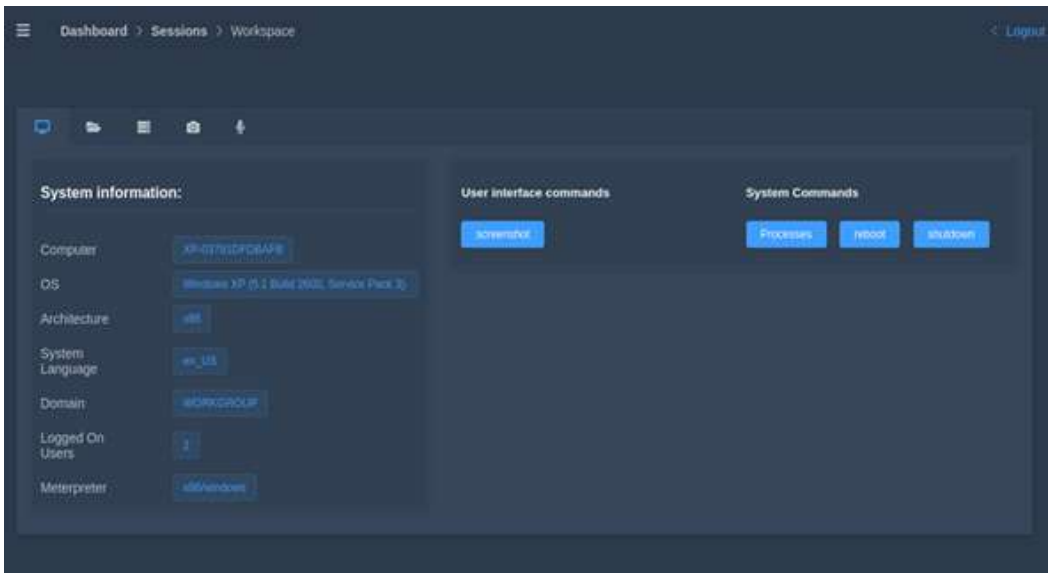
Step 7: You can now inspect the contents of the file and execute it as needed.



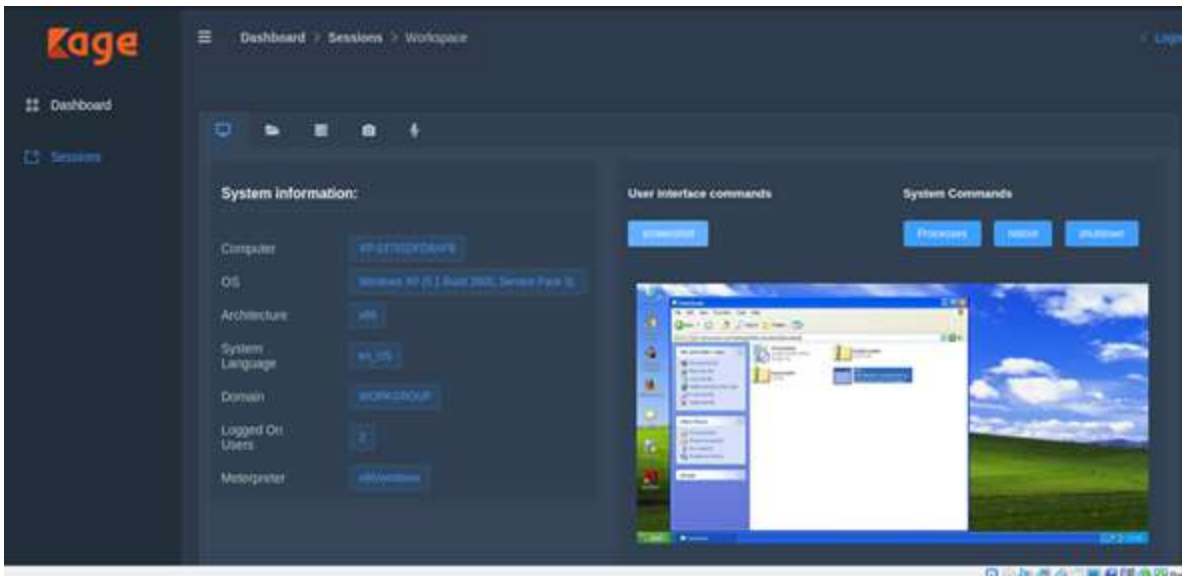
Step 8: Upon establishing a connection with the victim, a new platform will be visible in the session area upon returning to Kage. To actively engage with the victim, proceed by pressing the interact button.



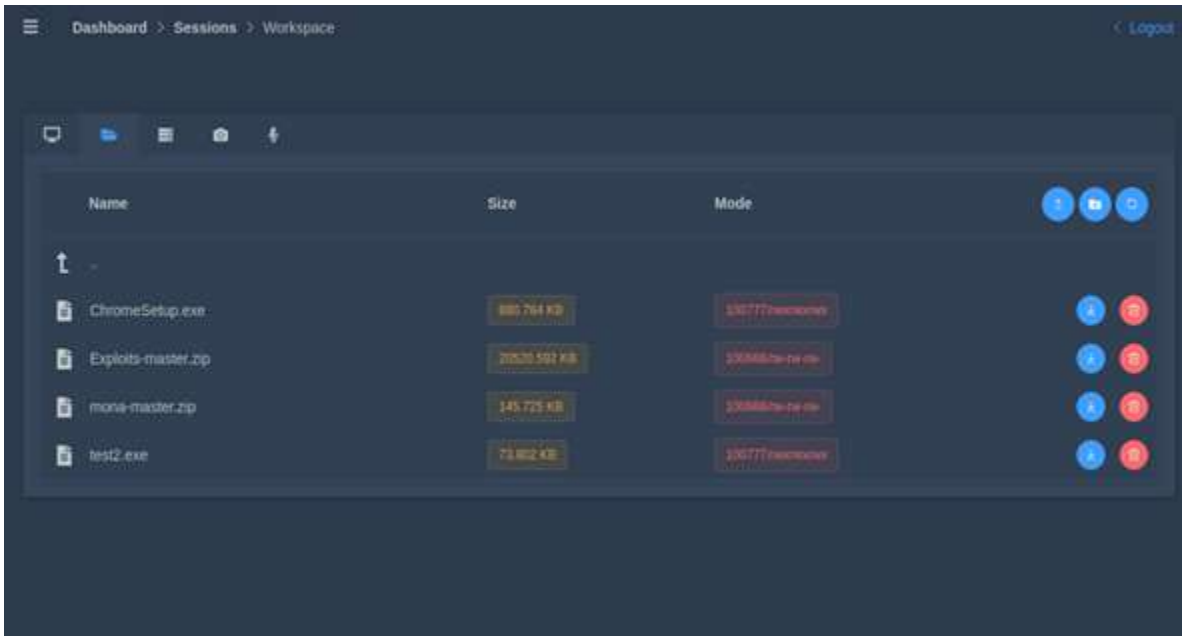
Step 9: At this stage, you can examine the victim's system data on the left and execute commands on the right.



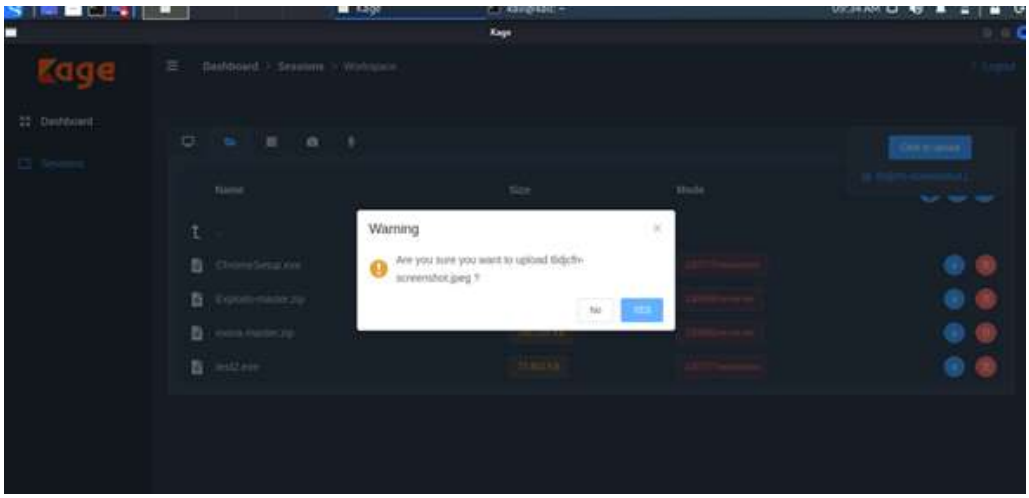
Step 10: Utilizing the "snapshot" command, we have the capability to capture a screenshot of the entire victim's user interface.

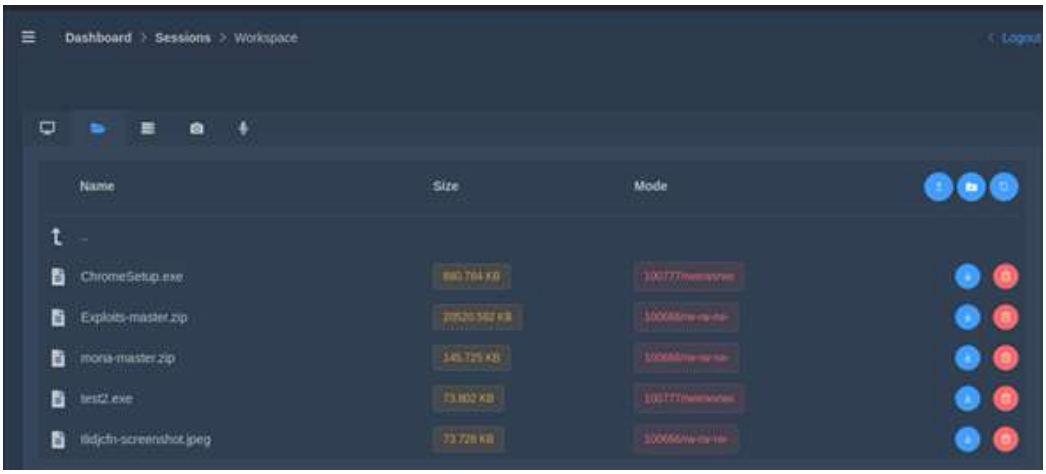


Step 11: Navigate to the second folder resembling a logo to access the file management feature. In this section, you can view all files present in the entire location of the botnet.



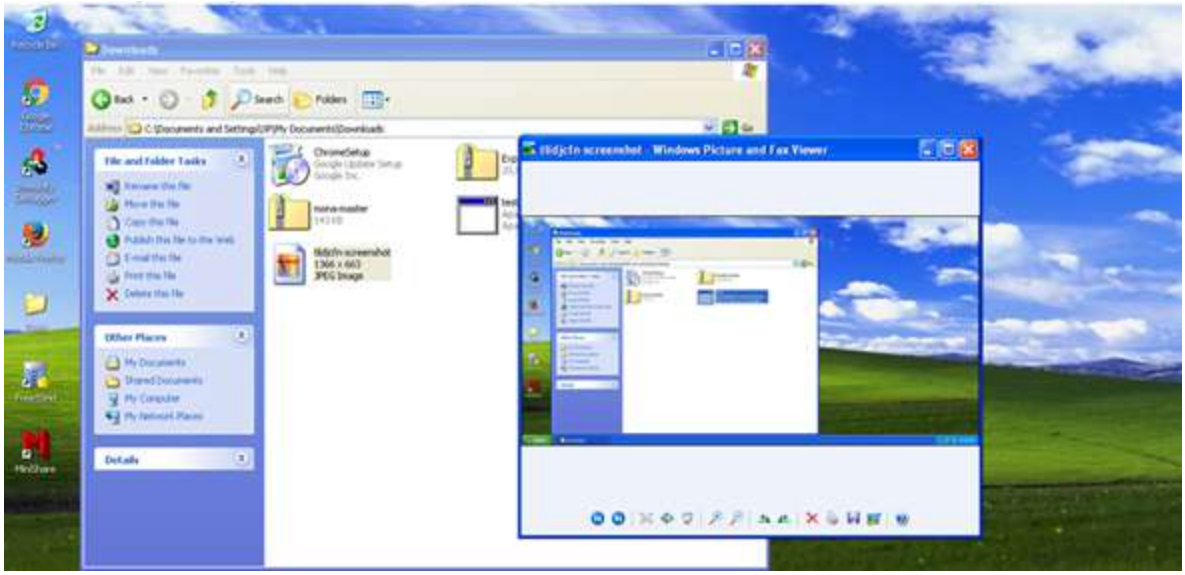
Step 12: You can now submit the screenshot we just captured. Additionally, it's evident that Kage has successfully uploaded the screenshot to the designated folder.





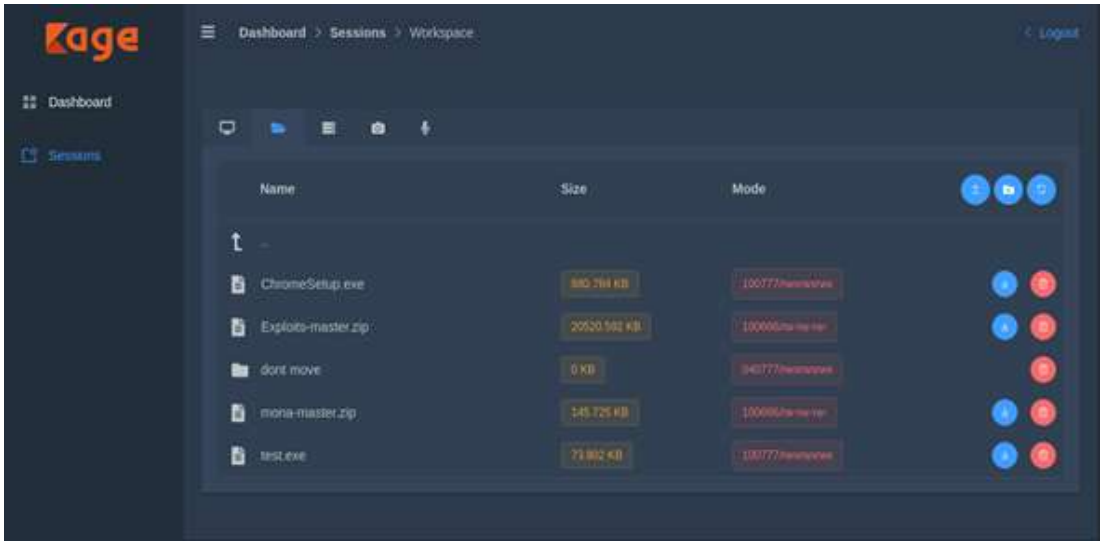
Step 13: After the initial attempt, check the results on Windows XP, confirming the successful relocation of the screenshot to a new location.

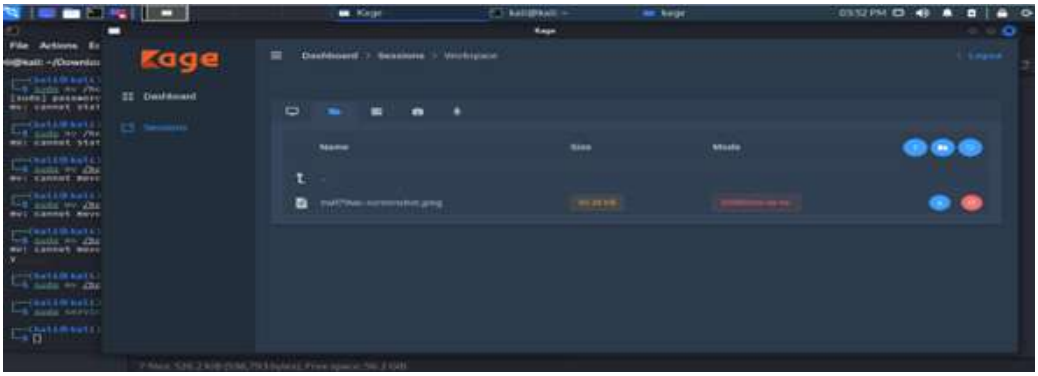
Step 14: Verify that the content of the screenshot within the new location corresponds to the one captured by Kage.



Step 15: Delete the previous botnet file and create a new one named test.exe to establish a connection as before.

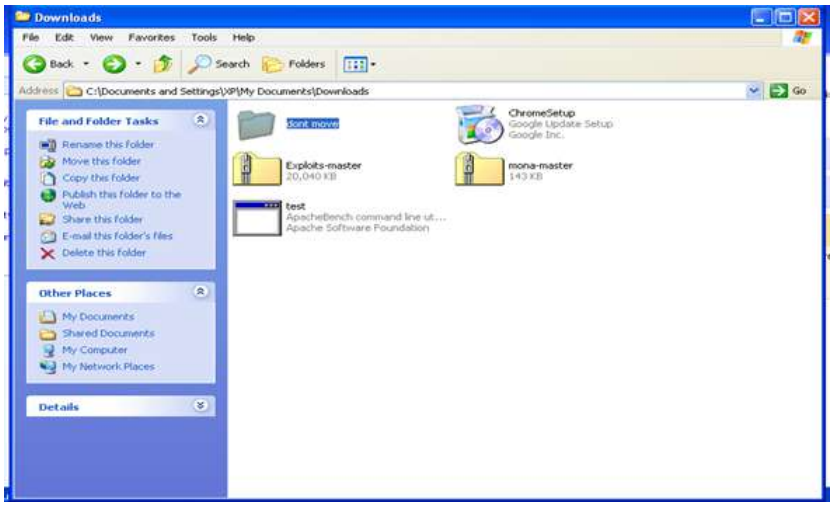
Step 16: Use Kage to create a *don't move* folder and paste another screenshot inside it.

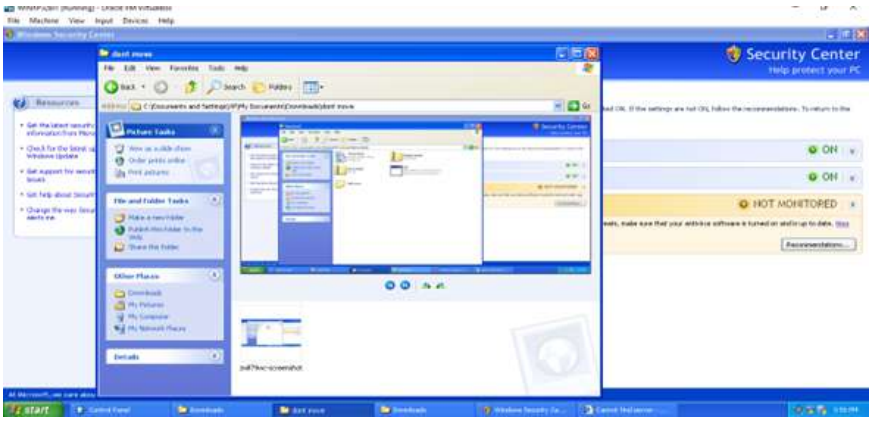




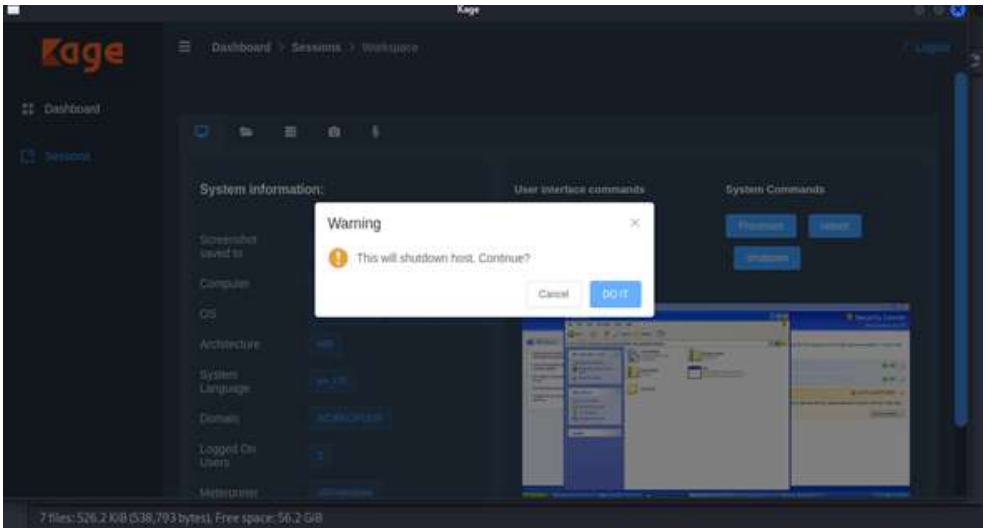
Step 17: Confirm the presence of the "don't move" file in the victim folder.

Step 18: Observe the snapshot provided by the attacker upon accessing the folder, demonstrating the successful execution of the second trial.

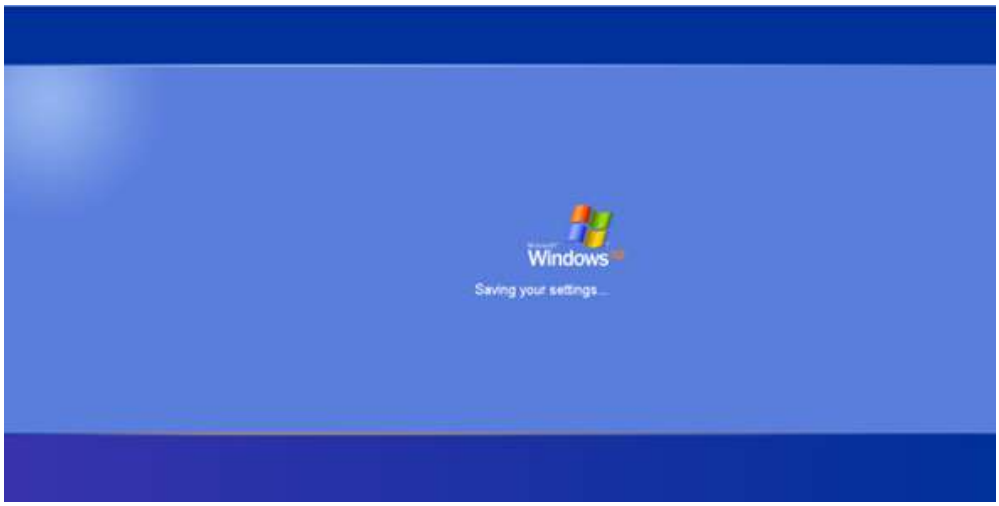




Step 19: Additionally, perform a shutdown command test to assess whether the machine responds by shutting down as expected.



Step 20: As a result, both the victim's (Windows XP) and the attacker's machines were successfully shut down in response to the test.

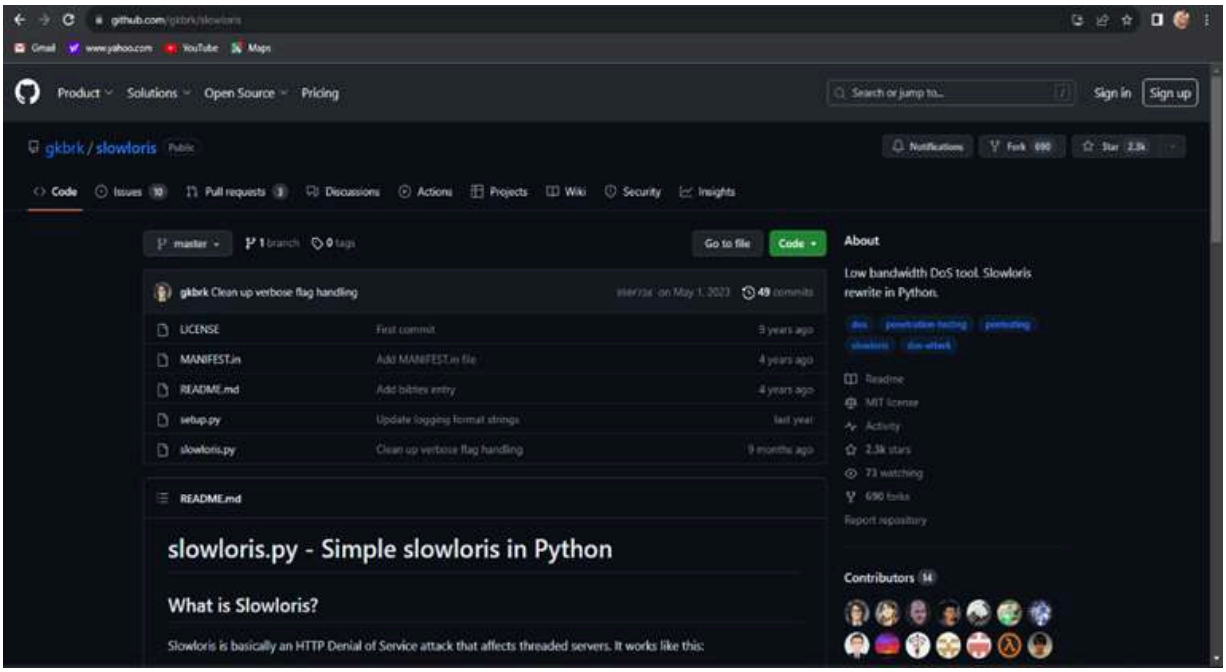


As a result, we can observe that Kage is useful for conducting botnets on a variety of operating systems, including Windows XP. It shows how Kage may use it to view the victim's system information, take a screenshot of the victim's current screen, create a folder and file within the victim's folder, and shut down the victim's PC.

4. Slowloris

Step 1: Open your web browser and navigate to the Slowloris GitHub repository using the following link: *https://github.com/gkbrk/slowloris*.

Step 2: Press the green Code button and copy the HTTPS link from the provided options.

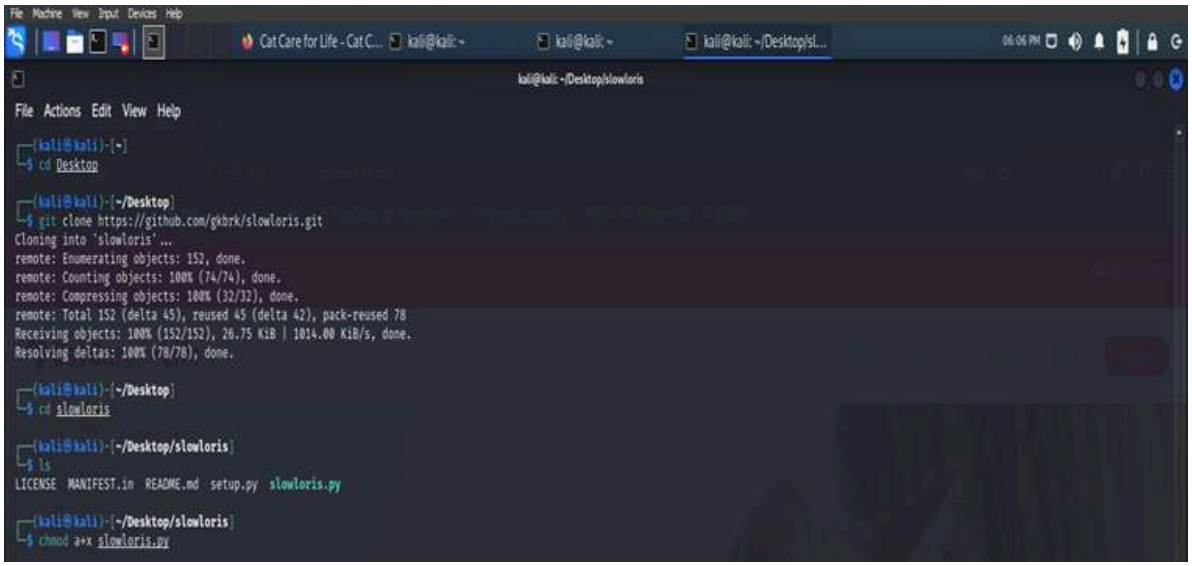


Step 3: Launch the Kali Linux terminal and enter the command *cd Desktop* to navigate to the desktop directory.

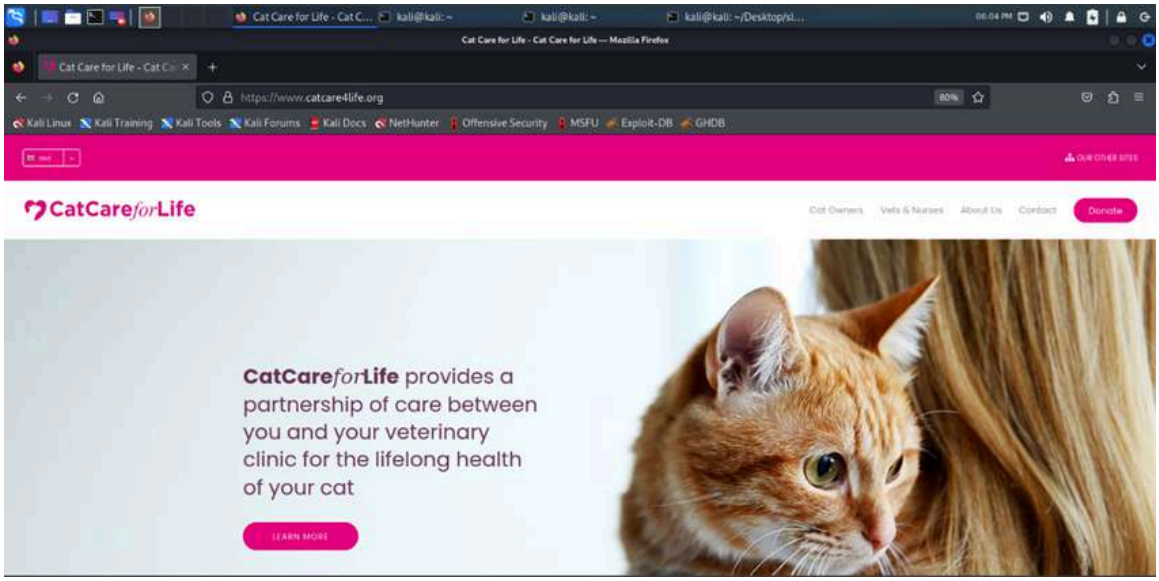
Step 4: Enter the command *git clone*, followed by pasting the previously copied link.

Step 5: Issue the command *cd slowloris* to enter the Slowloris directory. Subsequently, utilize the *ls* command to view the contents of files in the Slowloris directory.

Step 6: Next, input *chmod a+x slowloris.py* to grant execution permission to the slowloris.py file for all users.

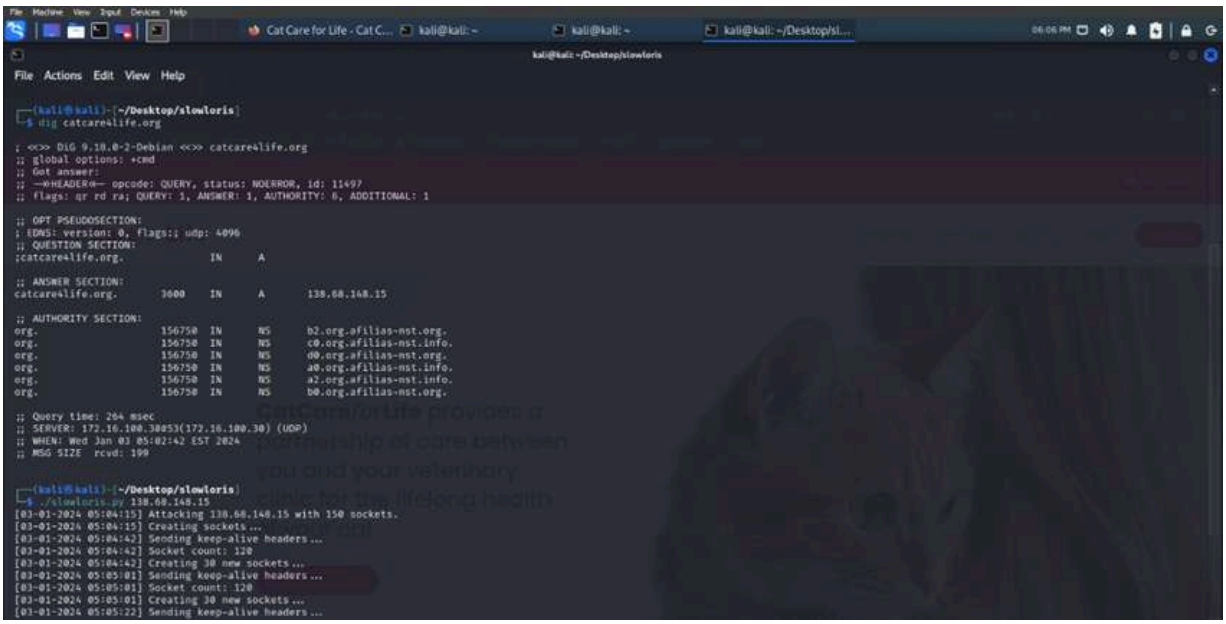


Step 7: catcare4life.org is the website we want to attack.

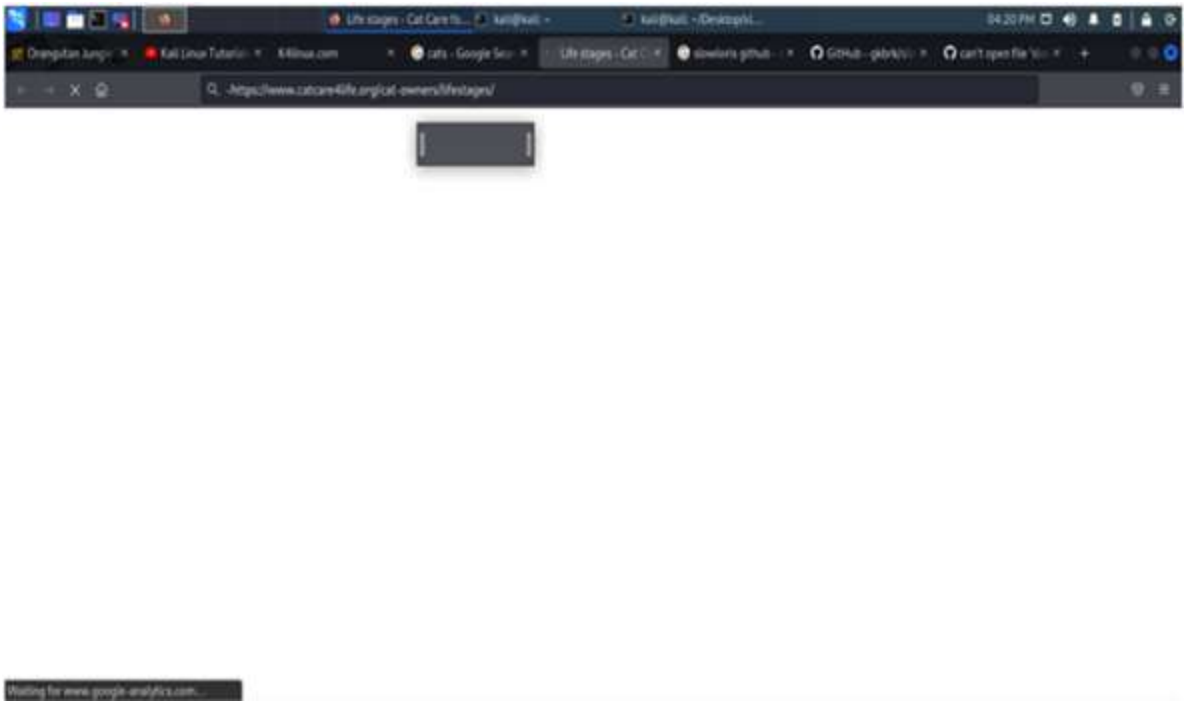


Step 8: Enter "dig catcare4life.org" in the terminal to discover its IP address.

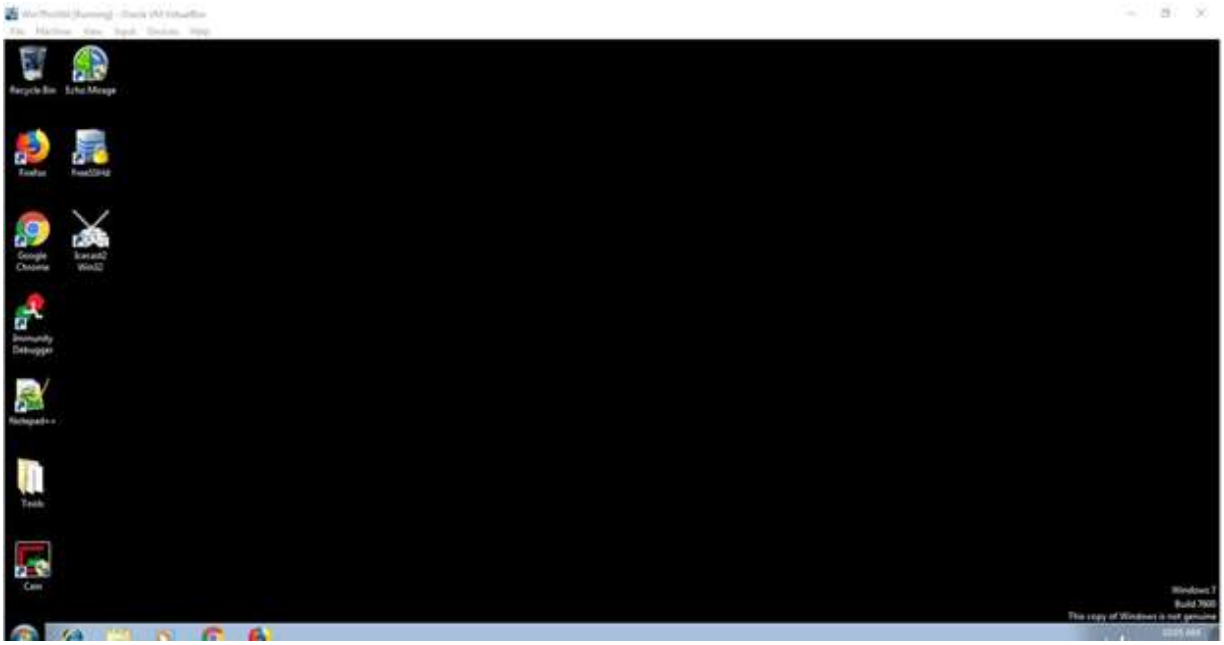
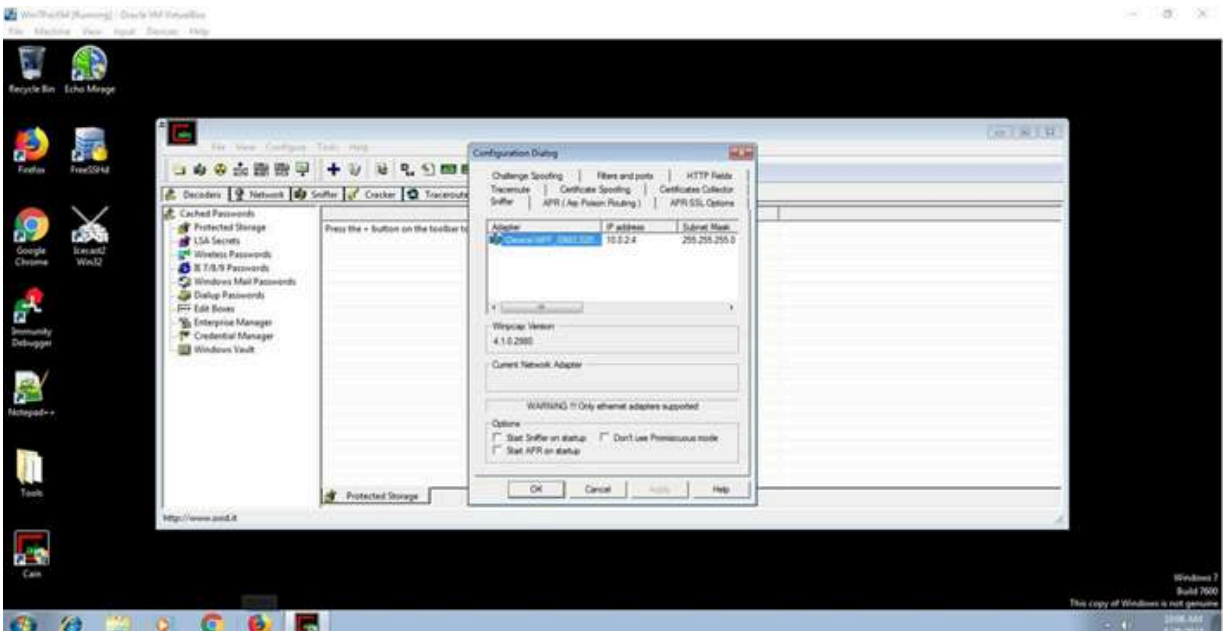
Step 9: Now, execute *./slowloris.py 138.68.148.15*, where 138.68.148.15 is the IP address of the target website to initiate the attack.



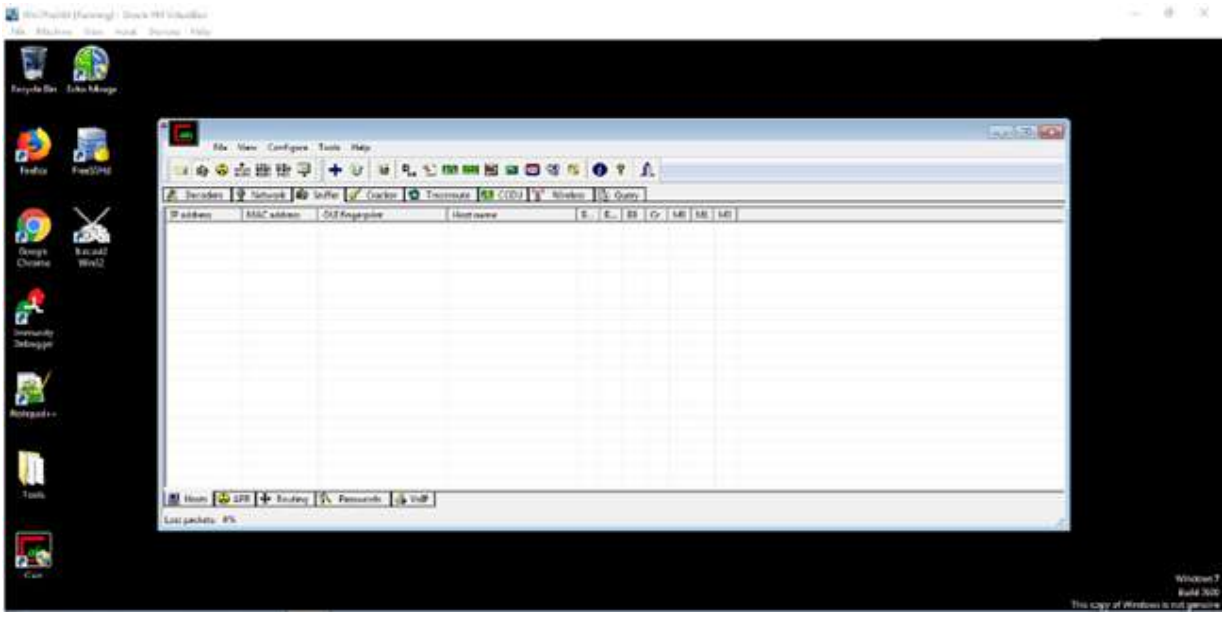
Step 10: Step 9: Confirm the success of the attack by attempting to access the website again. If the site remains unreachable, it indicates that the attack was successful in temporarily taking down catcare4life.org.



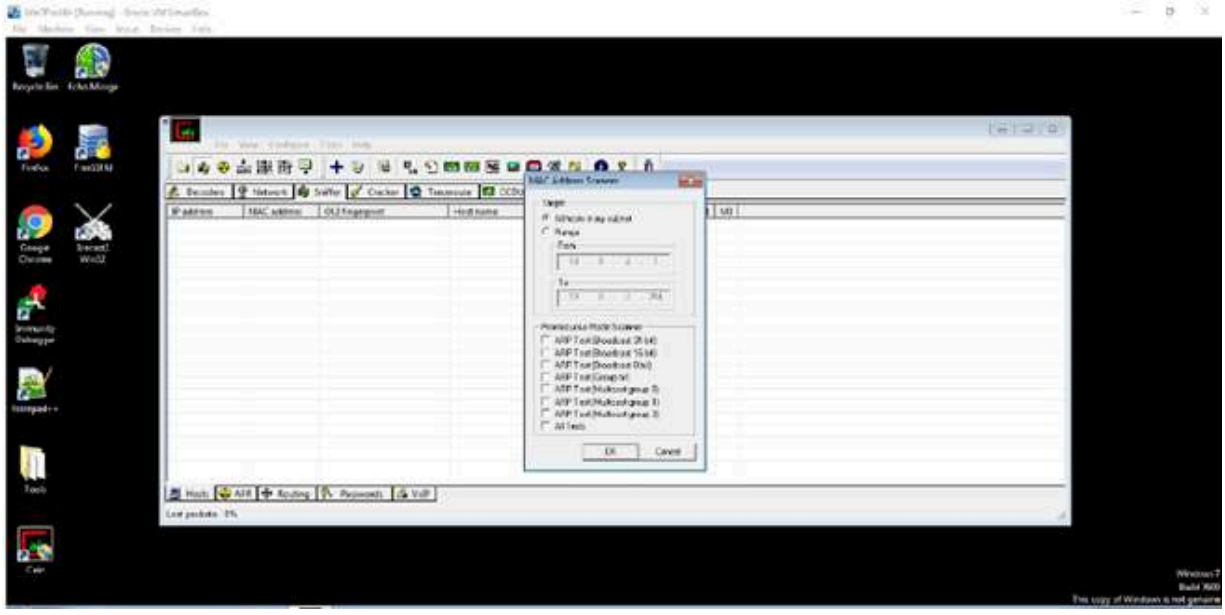
5. Cain and Abel

Step 1: Install the LOIC software on your PC's Windows.

Step 2: As soon as it launched, the network setup was established and the wireless network interface was selected. Then, click the Sniffer and Hosts buttons.


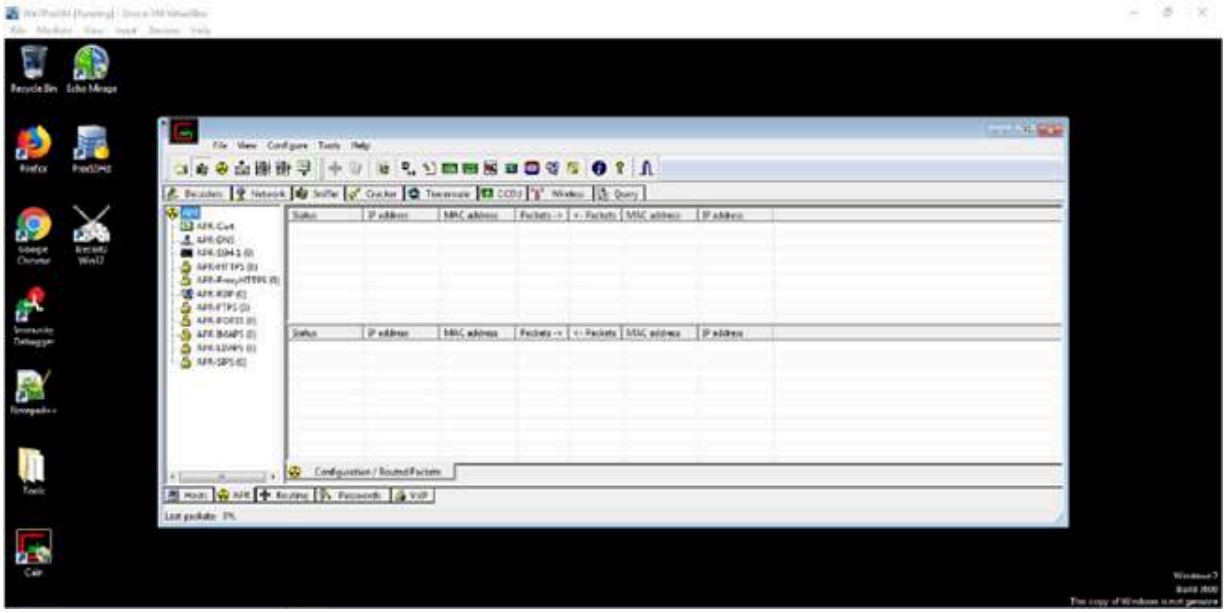
Step 3: Click on the plus sign symbol.



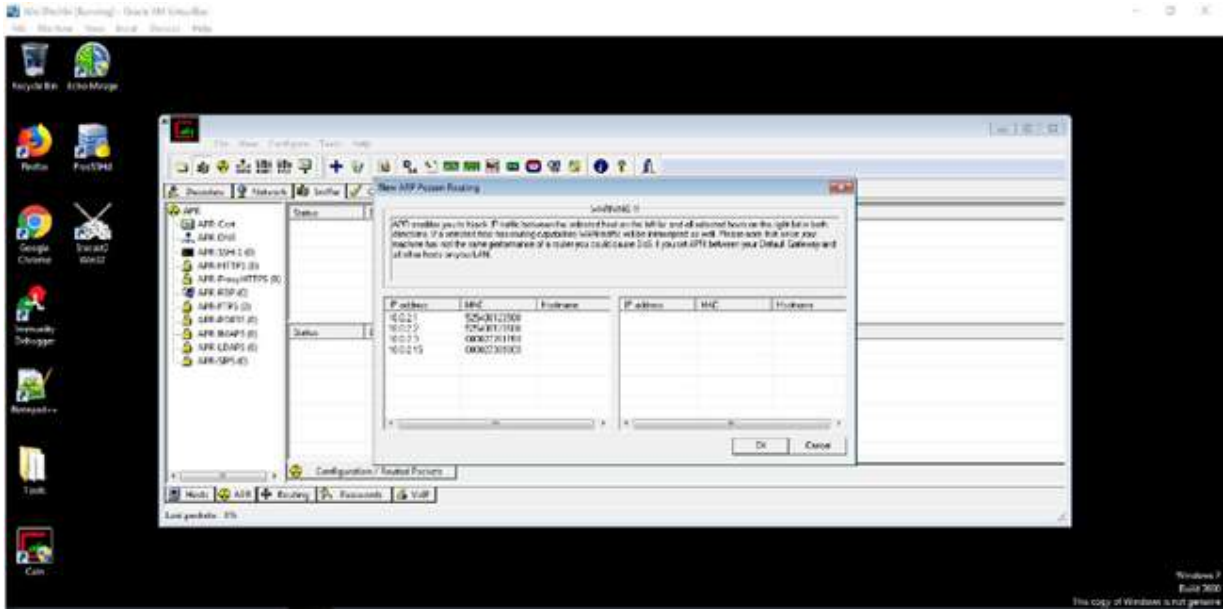
Step 4: Subsequently, click the OK button to verify that all settings are in their default positions and that our network's IP address has been accurately acquired.



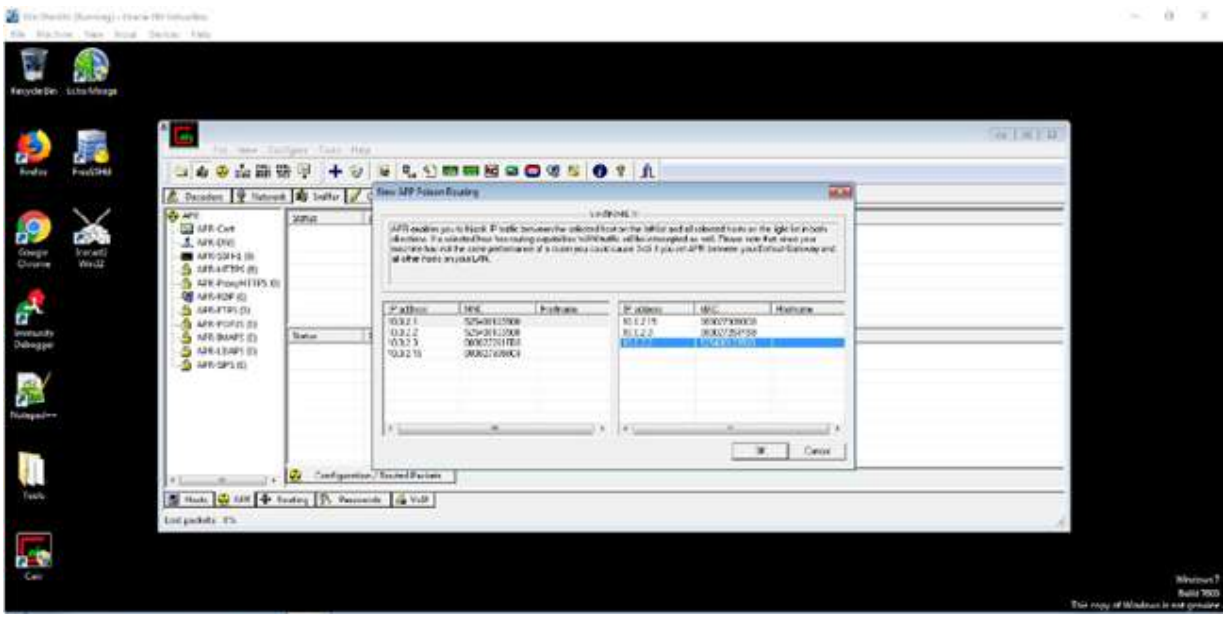
Step 5: Select APR from the list of tabs below.



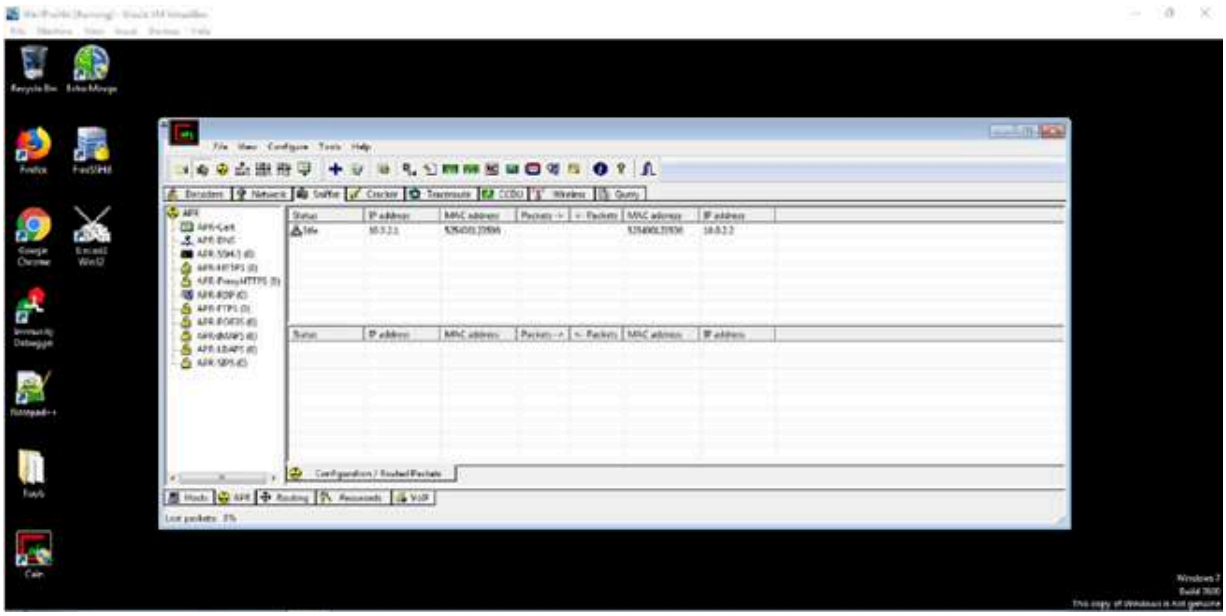
Step 6: Within the upper section of the two spaces to the right of the tree view, click on the plus symbol.



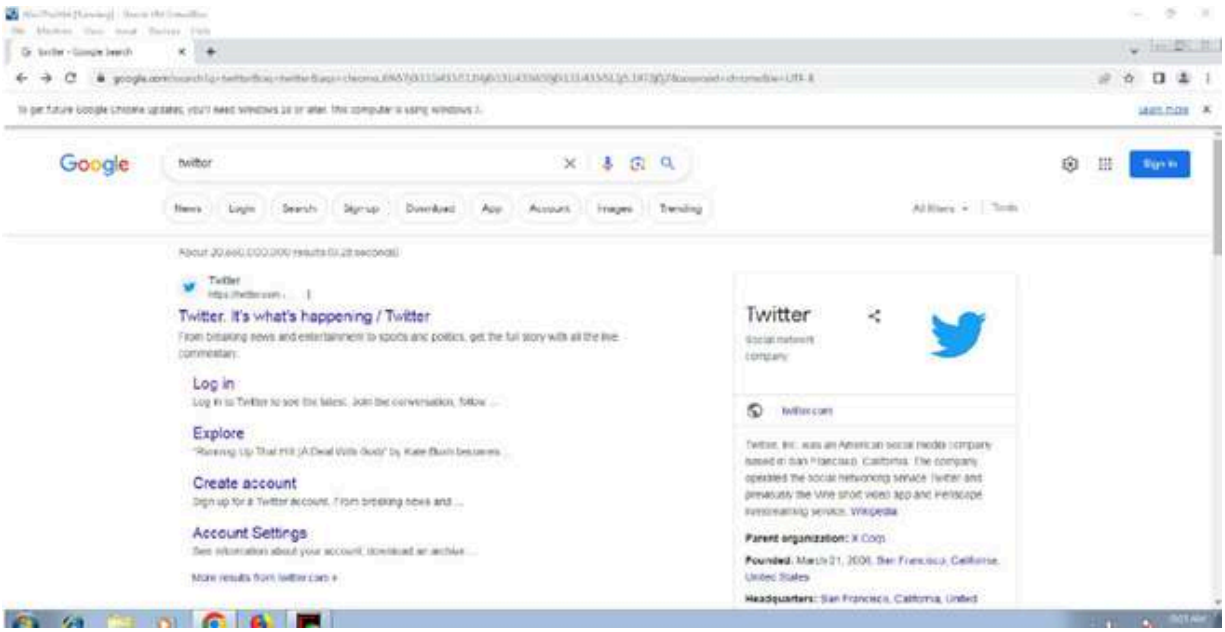
Step 7: Identify every IP and MAC combination available. Select the victim's IP address and MAC on the right side, and designate the network's actual gateway as the victim gateway on the left.



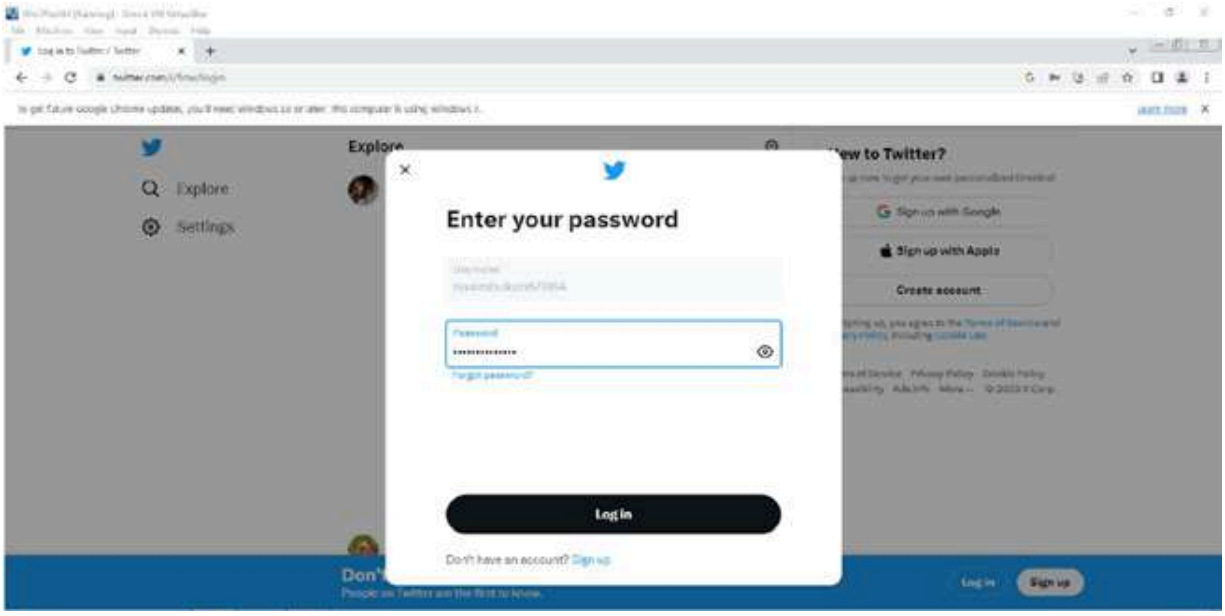
Step 8: Click the third button to initiate the ARP Poisoning.



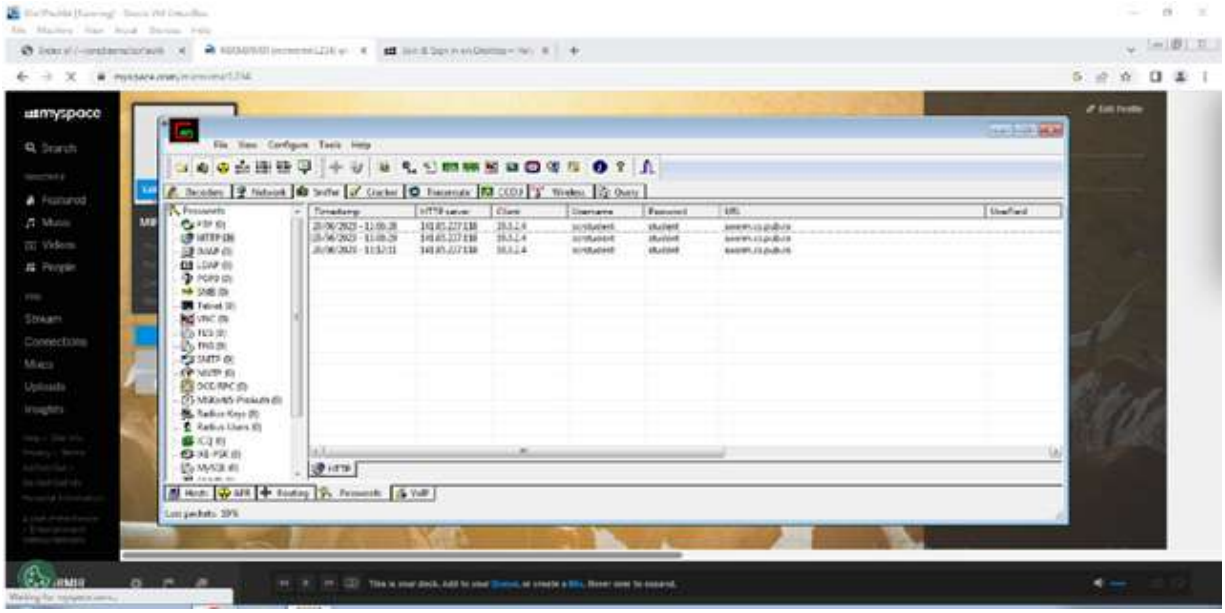
Step 9: Subsequently, we opt to use a Twitter website to gather the email address and password, accessing it while the chain is active.



Step 10: For safety purposes, we are creating a new account to target. Proceed by entering the password.

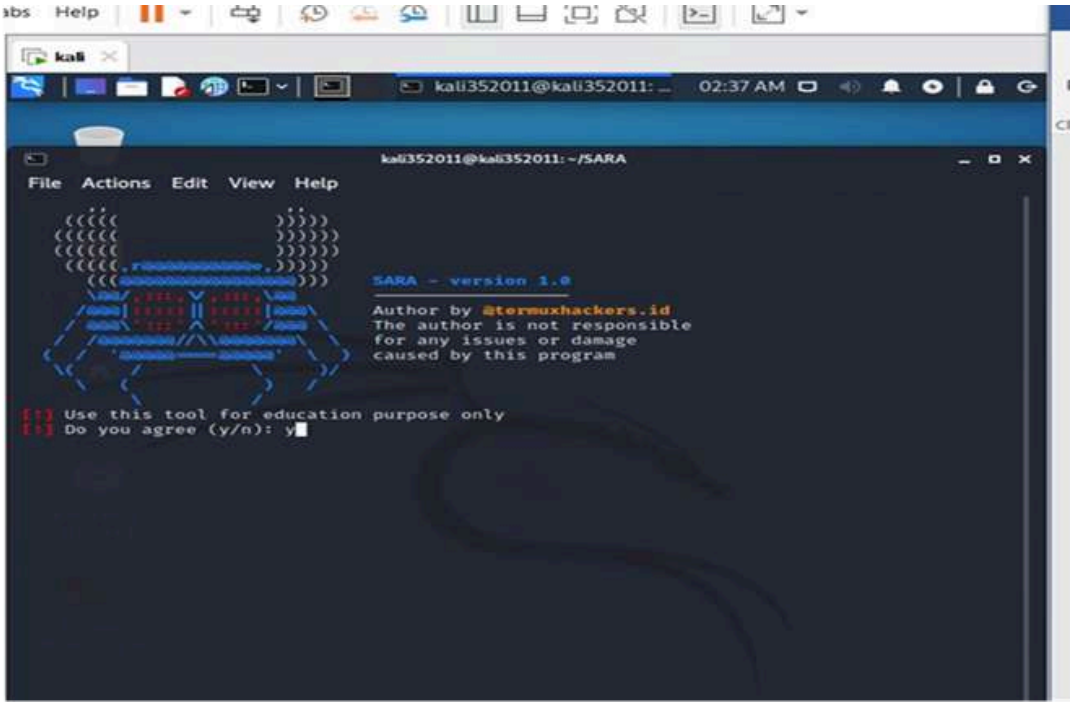


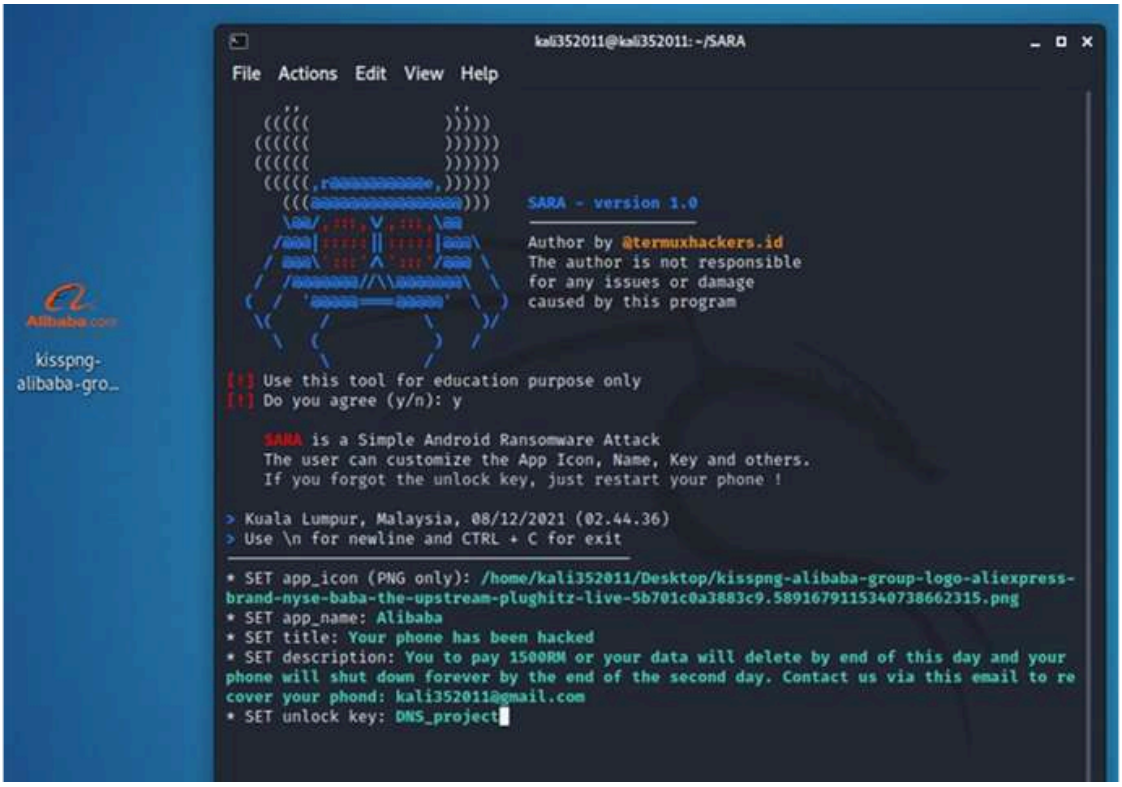
Step 11: Lastly, you can notice that the username and password are now showing up in Cain under the Password lower tab (HTTP protocol), on the sniffer tab. The results are being recorded in Cain.


myspace
Search
Featured
Music
Videos
People
Stream
Connections
Mixes
Uploads
Insights
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CO2
Wireless
Query
Passwords
Timestamp
HTTP server
Client
Username
Password
URL
ShowPanel
HTTP
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 39%

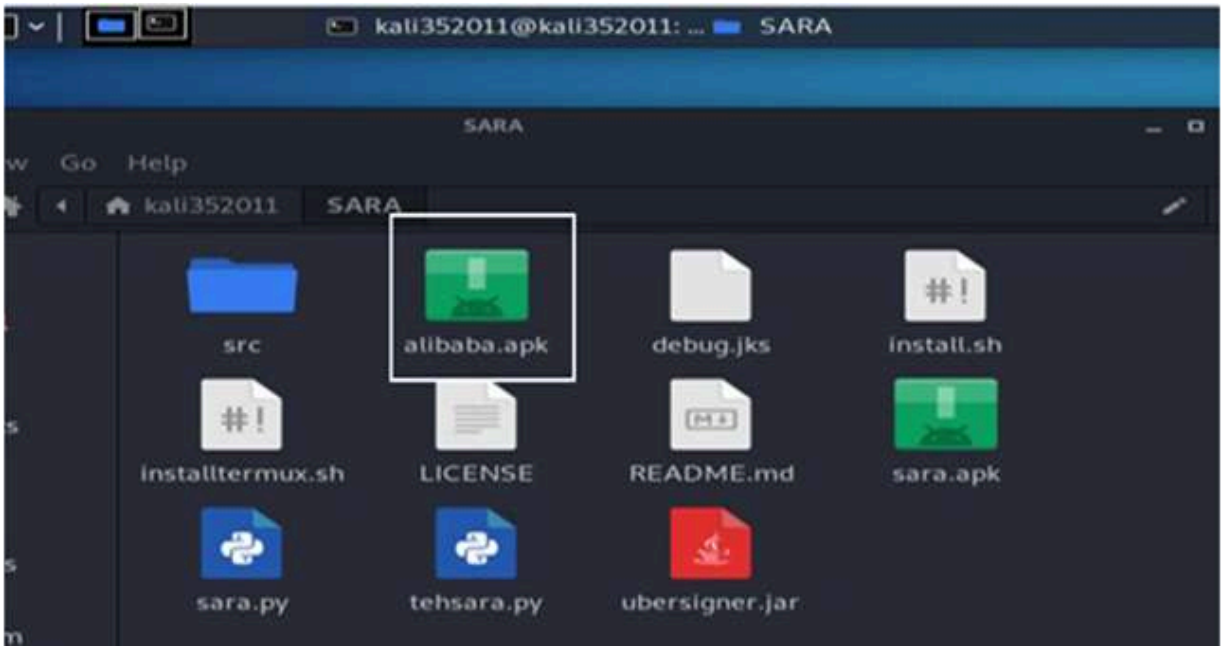
LINUX

1. SARA

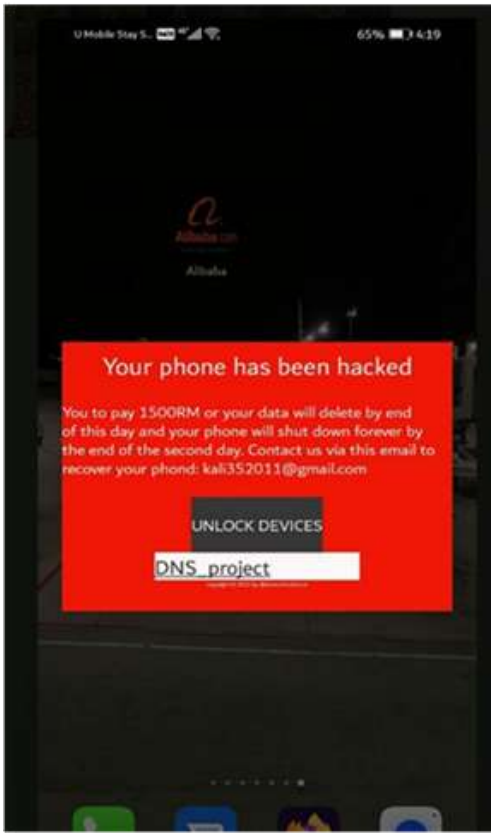
Step 1: Run the command *python3 sara.py* to initiate the SARA utility. Respond to the prompt by typing *y*.

Step 2: Upload the PNG of the app's logo to the SARA tool. Enter the unlock key, specify the name of the new app, and provide a threatening message for the victim.



Step 3: The newly generated program is now ready to be handed to the victim.



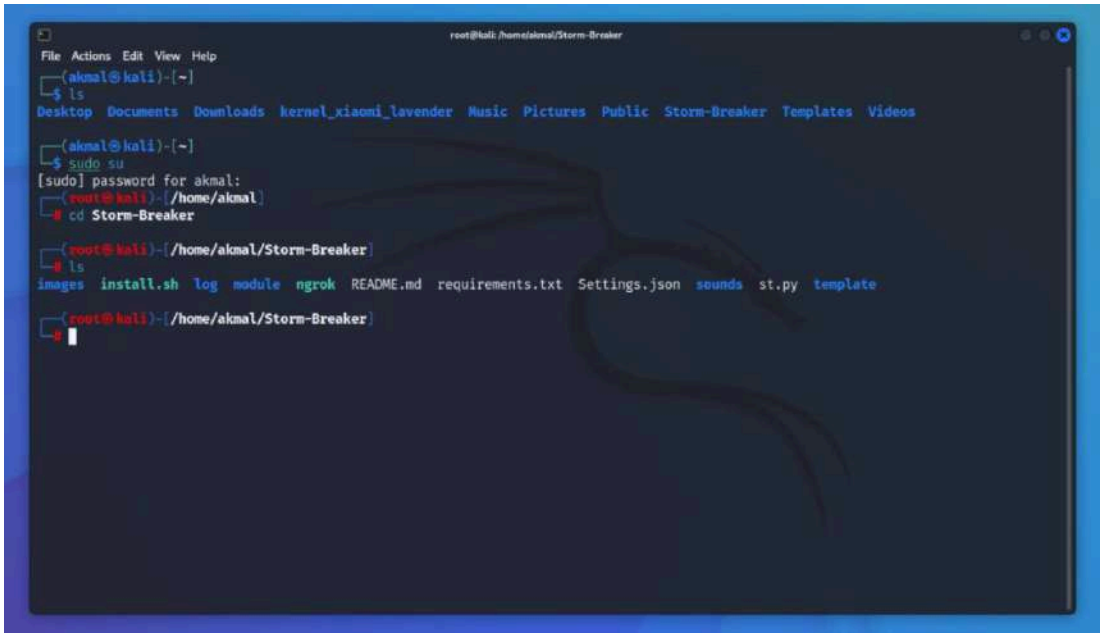
Step 4: The new software has been successfully sent to the victim. Upon launching, the software will display a message, rendering all phone functionalities inaccessible.



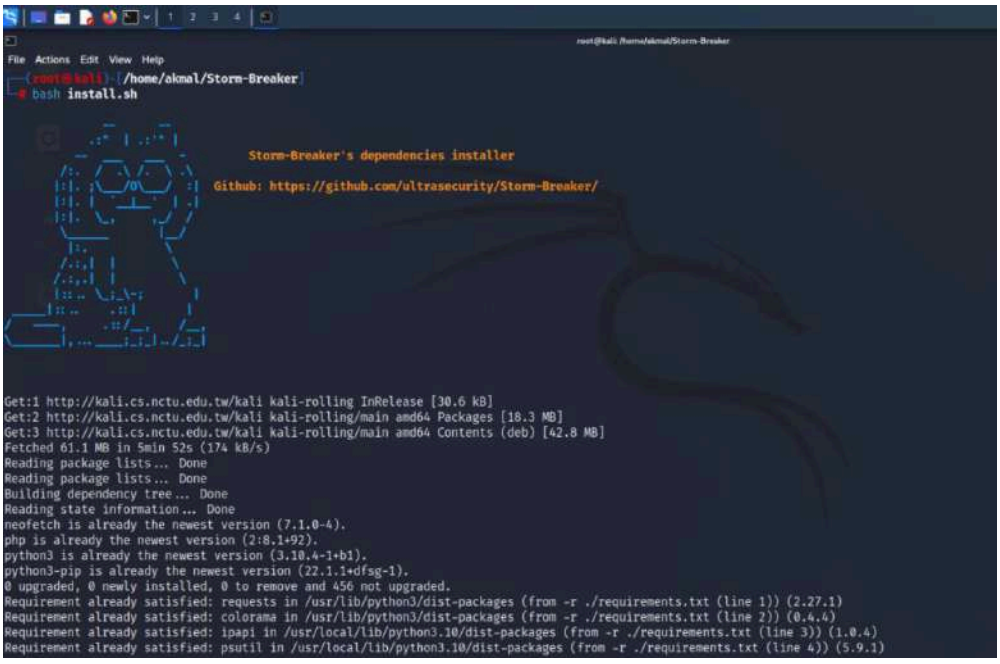
2. Storm Breaker

Step 1: Write *cd Storm-Breaker* to redirect into Storm Breaker directory.

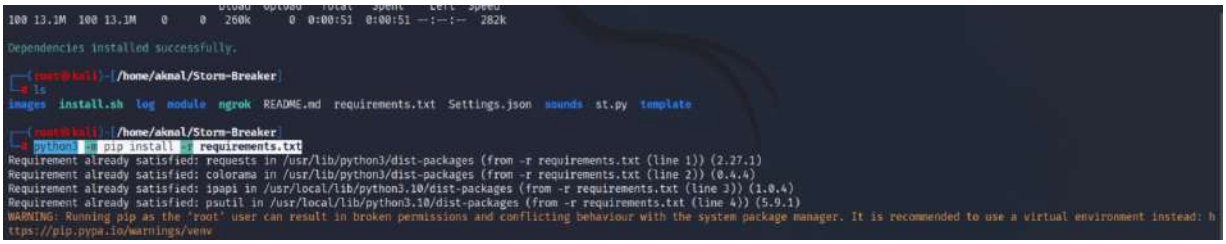
Step 2: Run *ls* command to view all files in the directory.



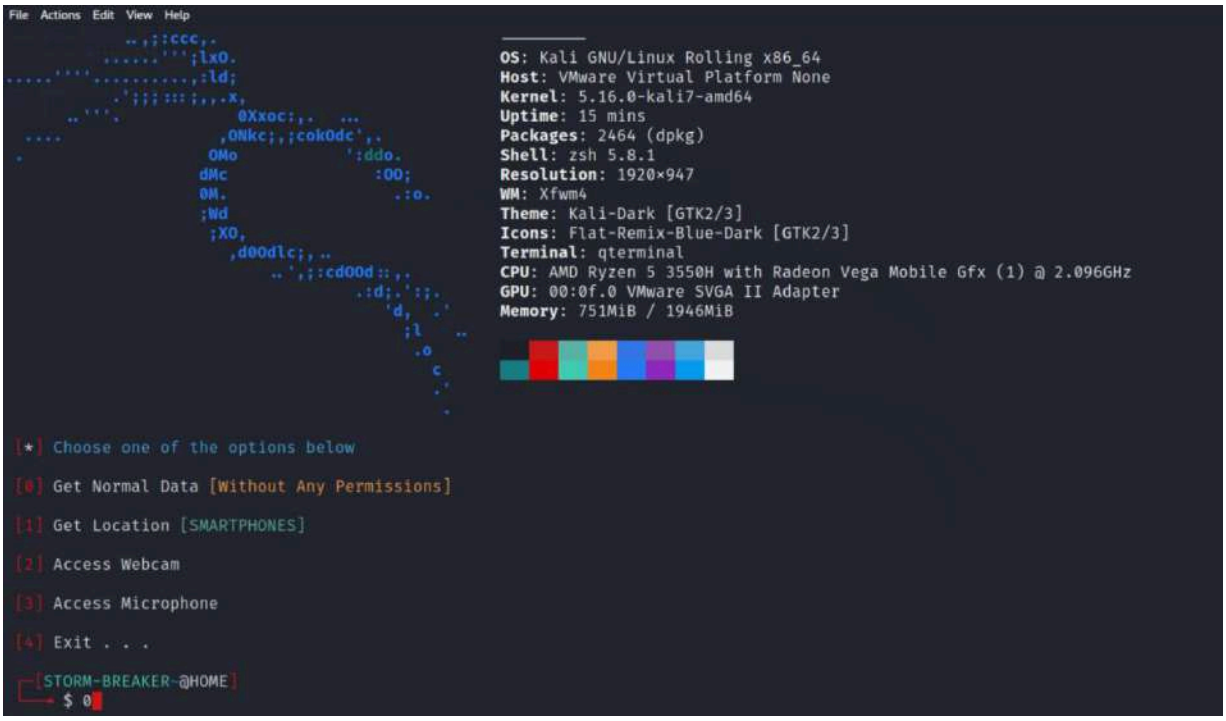
Step 3: Run *bash.install.sh* to install the required files to run the attack.



Step 4: To give executable permission to the StormBreaker python file, run the *python3 -m pip install -r requirements.txt* command.

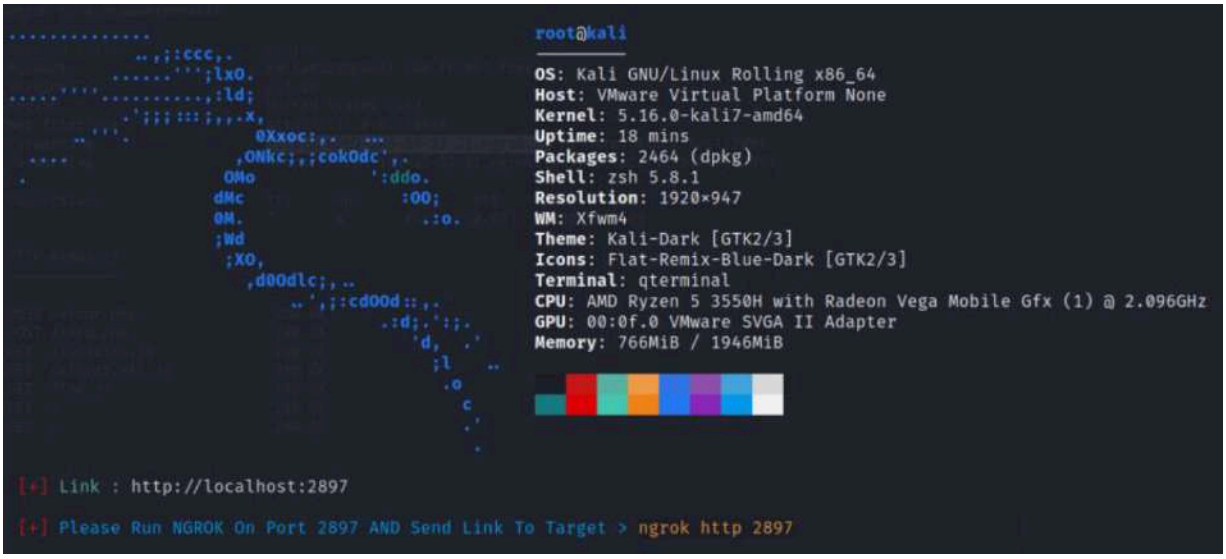


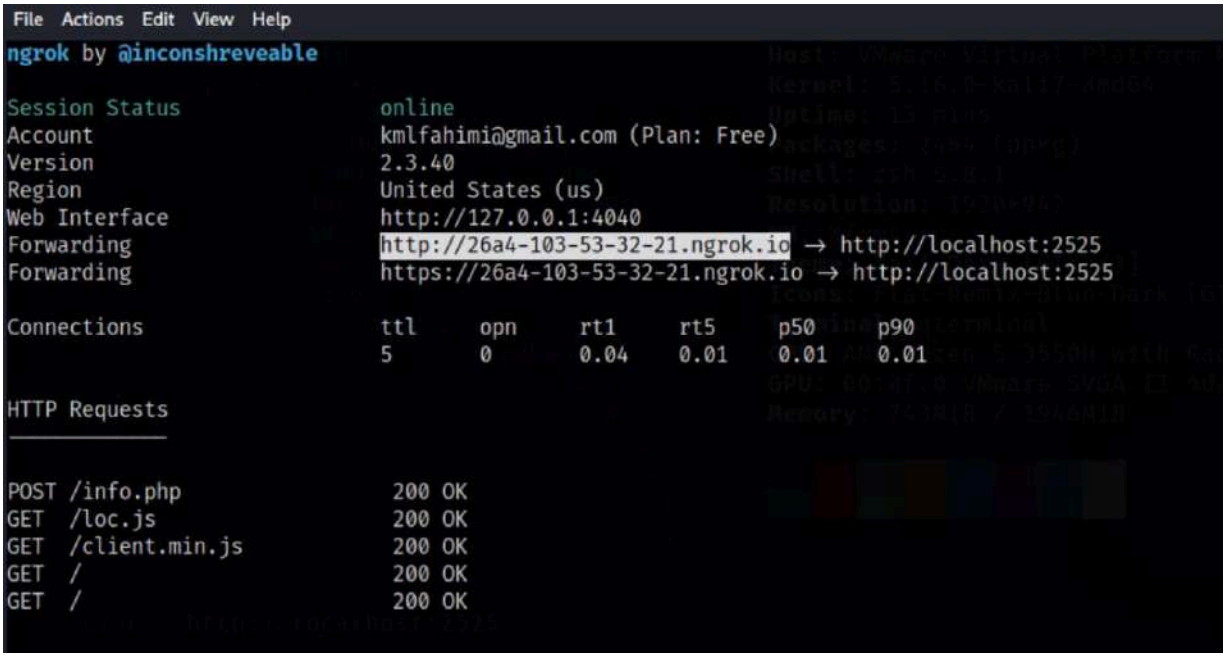
Step 5: Next, write a command *python3 st.py* to run the tool to start the attack.



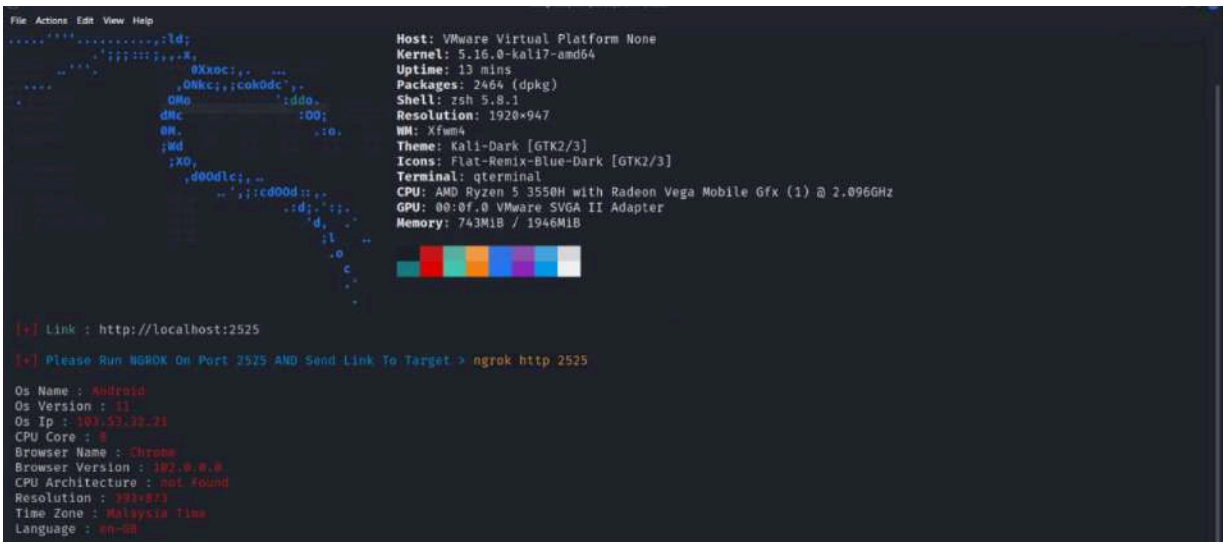
Step 6: Run Option 1 which is Get Location [SMARTPHONES] to get the target location. The tool will ask to run the *ngrok* to generate two links. One link is sent to the target and the other one to the local host.

Step 7: Run *ngrok http 2897* to generate the link and send to the target.





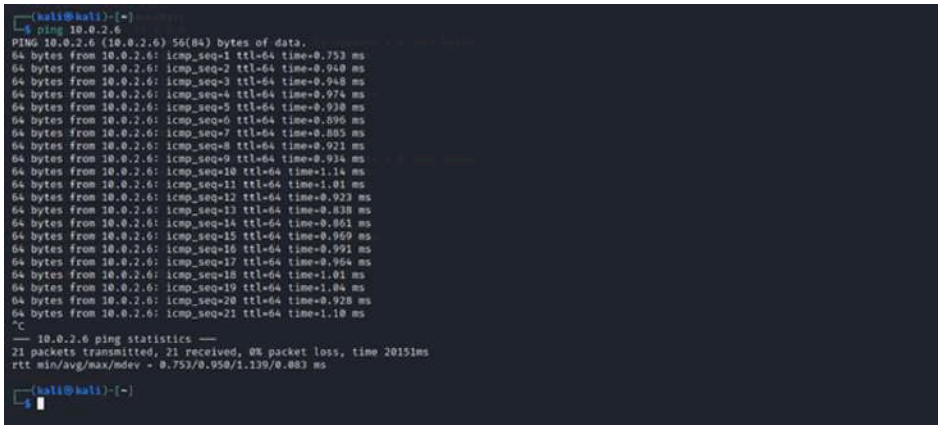
Step 8: Target location was revealed and run *N* to continue the second attack.



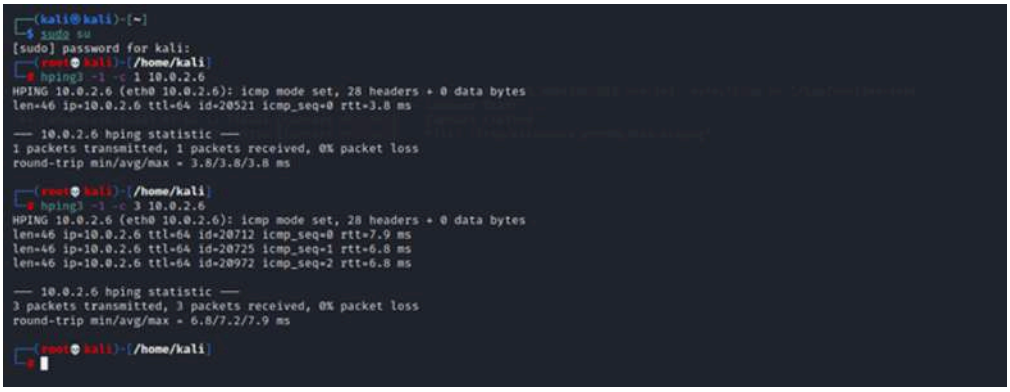
Step 9: Run Options 3 and 4 which are accessing the webcam and microphone of the target. The tool will ask to run the *ngrok* to generate two links. One link is sent to the target and the other one to the local host.

3. Hping3

Step 1: Ping the victim's IP Address which is 10.0.2.6 to make sure the packet can be sent to the intended recipient.



Step 2: Write the command *hping3 –1 –c 3 10.0.2.6* to transmit a packet to the victim and the reply must be received.



Step 3: Then, run the command *hping3 –1 - -flood 10.0.2.6* to start the flooding on the victim.

DEFENSE

TOOLS

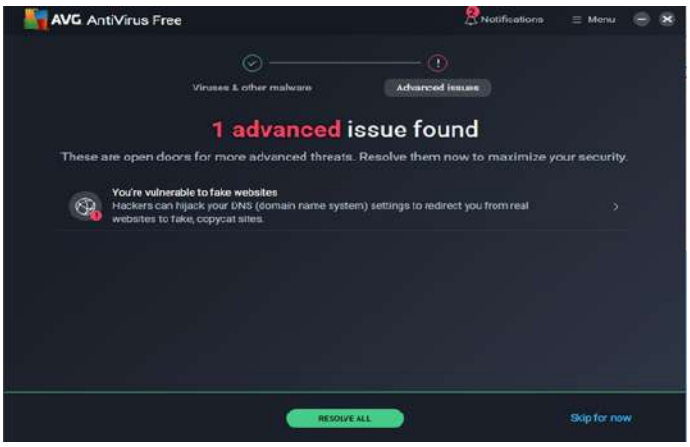
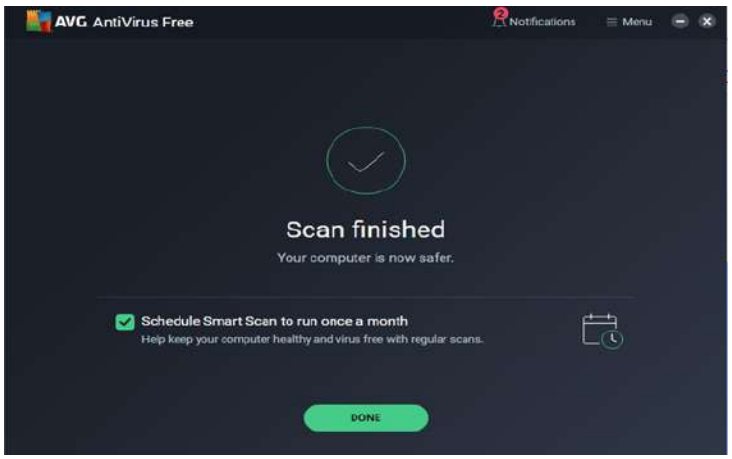
WINDOWS	LINUX
1. AVG Antivirus 2. Avast Antivirus 3. Windows Defender Firewall (for Kage) 4. Windows Defender Firewall (for Slowloris) 5. Windows Defender Firewall (for Cain and Abel)	1. Antivirus ClamAV 2. Eset nod 32 Firewall 3. XDP-Firewall

PLANNING

WINDOWS

1. AVG Antivirus

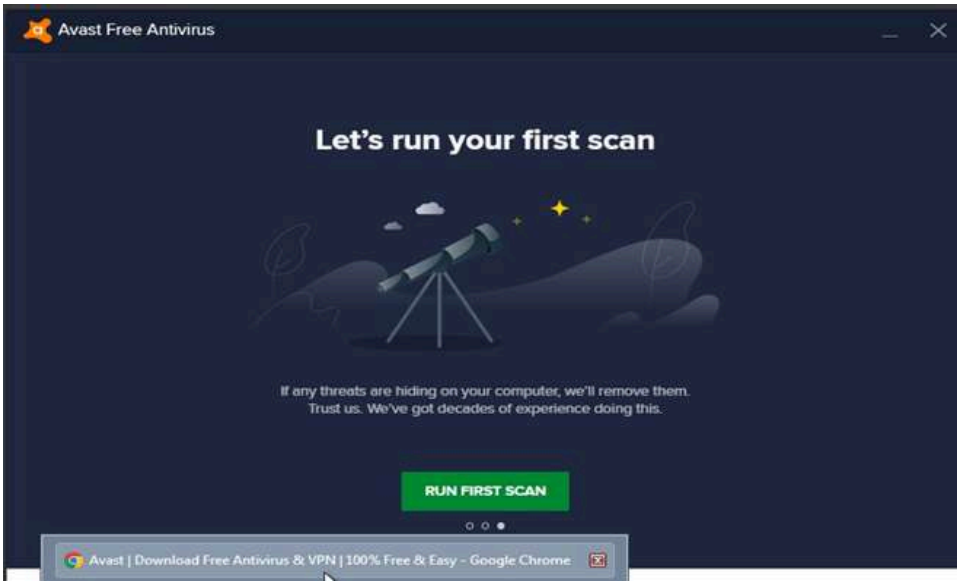
   Defending against Phishing by using AVG Antivirus

Step 1: Install a third-party firewall. We have already fortified our defense using AVG antivirus, capable of detecting whether the victim machine has been attacked or not. In this instance, AVG antivirus detected an issue on the victim machine.

Step 2: Upon completing the scan, AVG antivirus will automatically remove the detected threat from the network.


2. Avast Antivirus

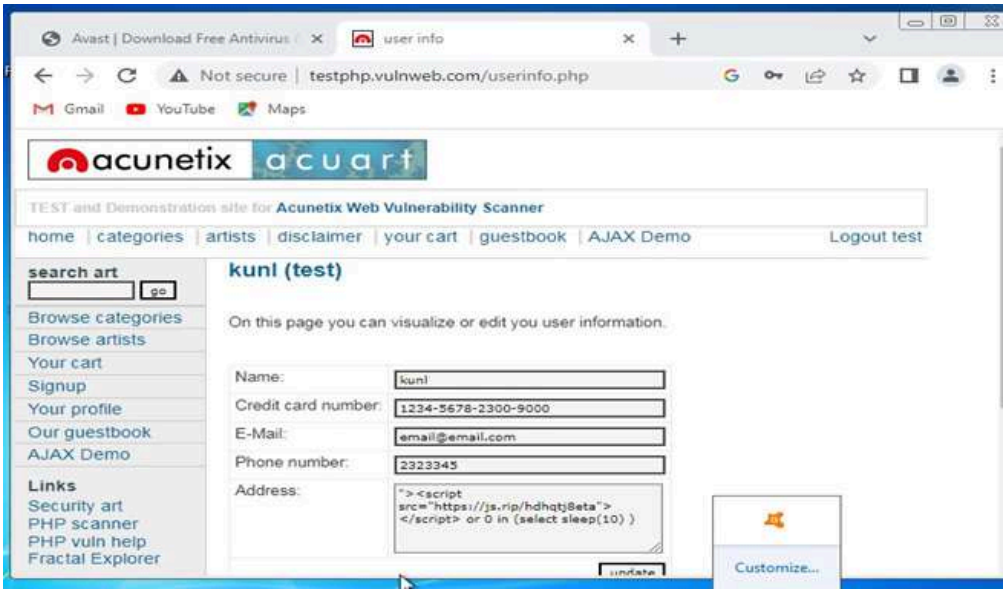
Defending against Ettercap by using Avast Antivirus

Step 1: To defend against potential Ettercap attacks, we've opted for Avast antivirus, relying on its advanced features and real-time scanning capabilities to create a robust barrier.

Step 2: Following the scan, we are assessing Avast antivirus's ability to detect any potential connection between the victim's machine and the attacker's, specifically evaluating its capacity to identify the exploit.


Step 3: Go to this link: *http://www.testphp.vulnweb.com/login.php* then enter the username and password, then click login on the Windows machine.

Step 4: If Ettercap attempts to launch an attack on the victim while Avast Antivirus is active, the antivirus can effectively thwart Ettercap's efforts to capture the data.

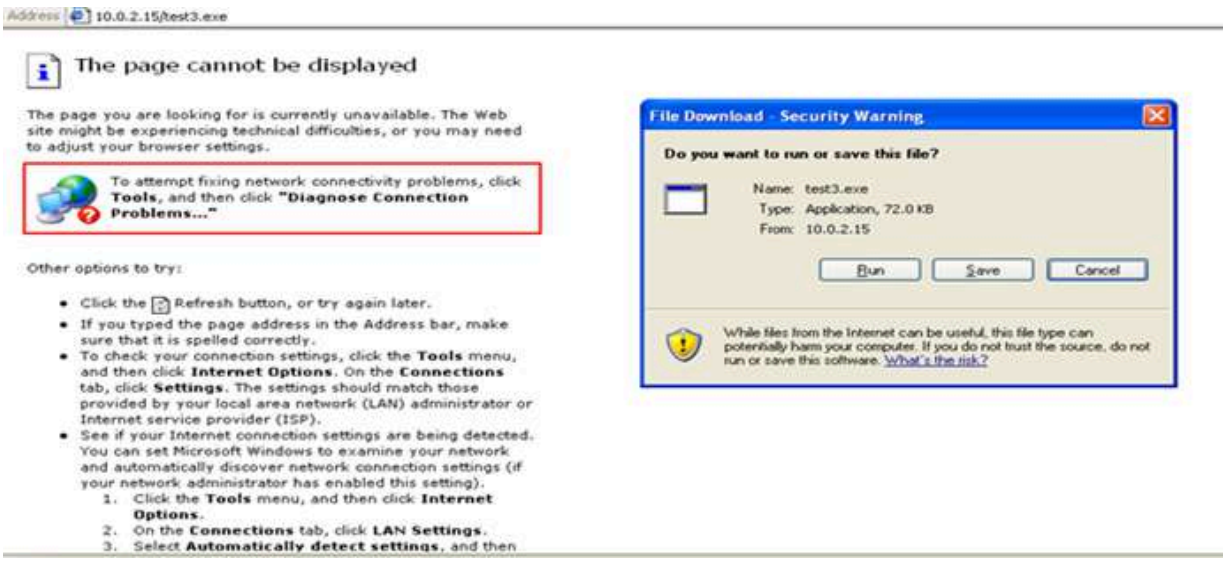


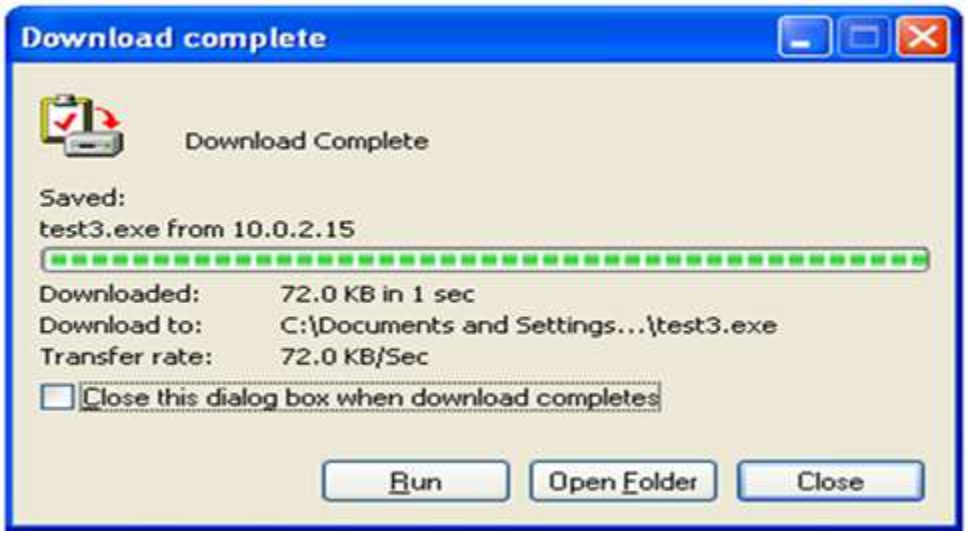
3. Windows Defender Firewall

Defending against Kage by using Windows Defender Firewall

Step 1: We decided to test the effectiveness of the initial Kage defense simulation. To begin, we accessed the security center on Windows XP and opened the firewall.

Step 2: In an attempt to retrieve the botnet file from the attacker, we ran the process again. Surprisingly, even with the firewall open, the file was still able to be downloaded.

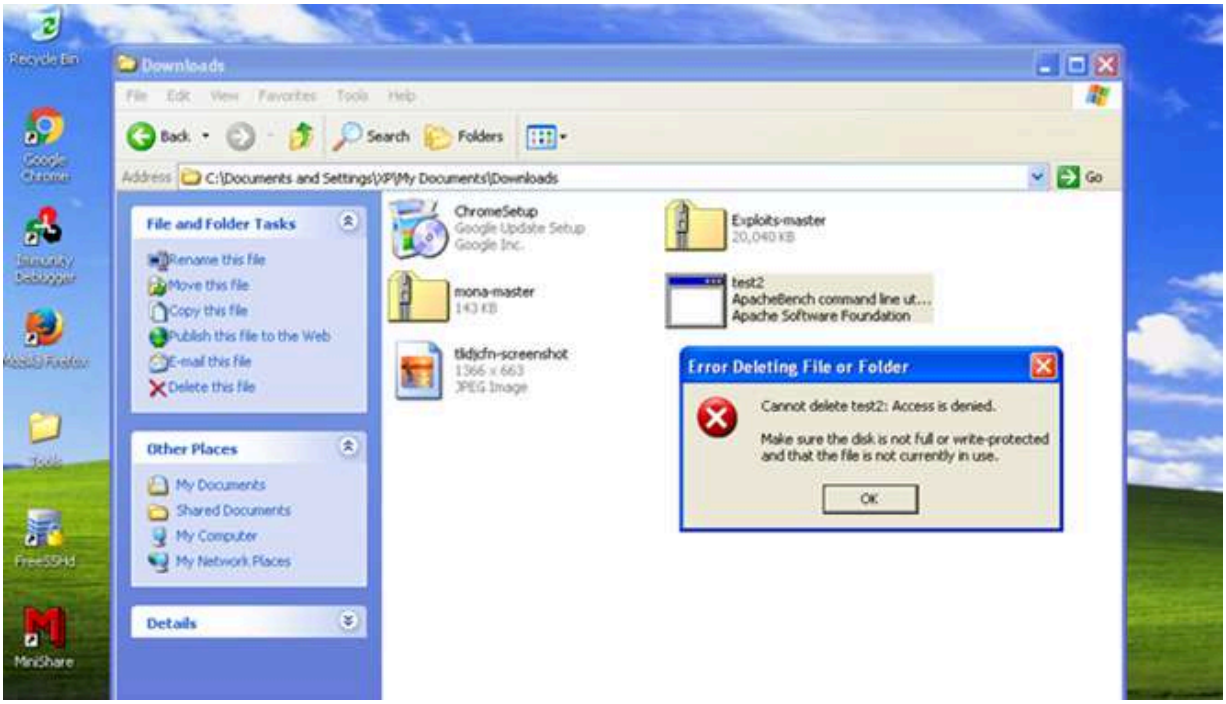




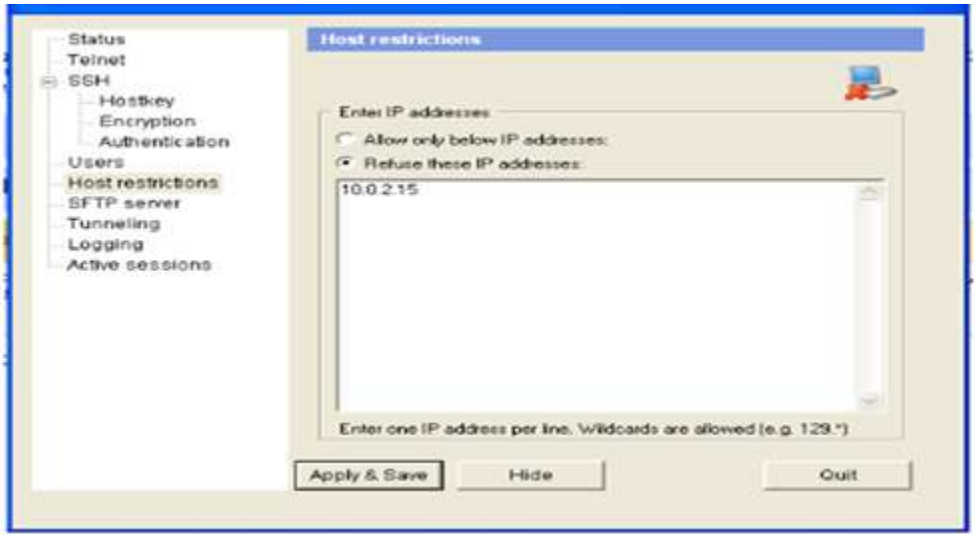
Step 3: Upon starting the botnet software, it also presents the Kage interface.

The test shows that the Windows XP firewall cannot stop software downloads, likely due to its weakness against botnet malware. This implies that Windows XP's firewall is not very effective in protecting against botnet attacks.

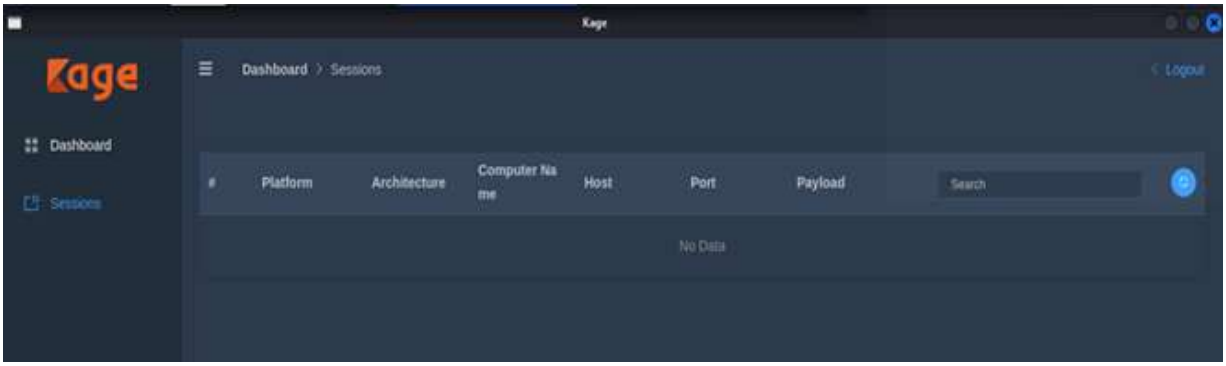
Consequently, despite identifying the file as part of the attacker's botnet, we are unable to eliminate it.



Step 4: Given our knowledge of the attacker's IP address, we can use host limitation to block their IP address, effectively putting a stop to the botnet's activities.

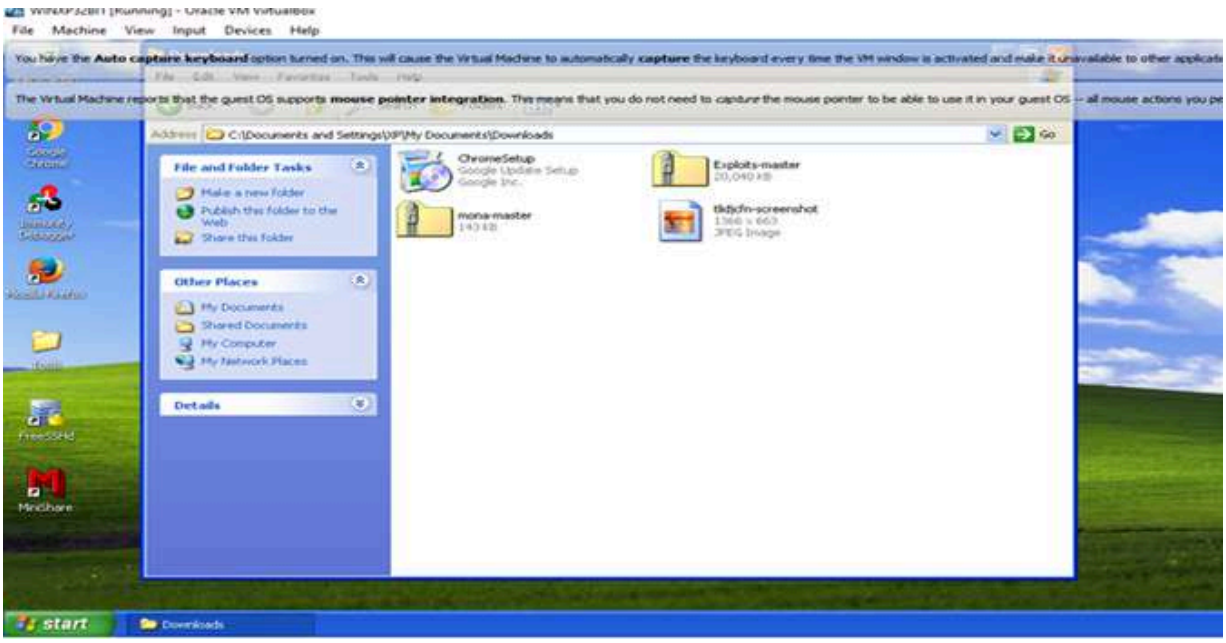


Step 5: We can notice that the platform is no longer present in Kage.



Step 6: We can see that the session has concluded, thanks to the meterpreter.

Step 7: Following this, we can successfully remove the entire botnet program from the computer.



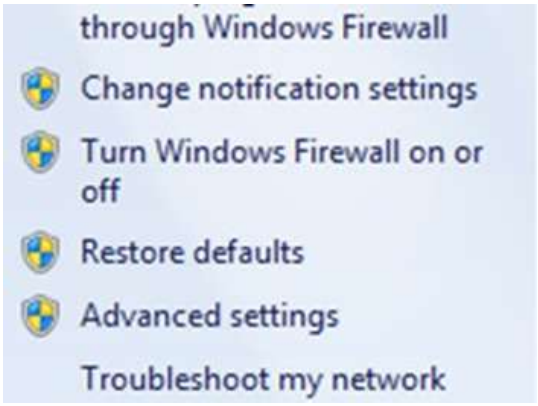
This outcome demonstrates that limiting the attacker's IP address is the best strategy to terminate the botnet malware.

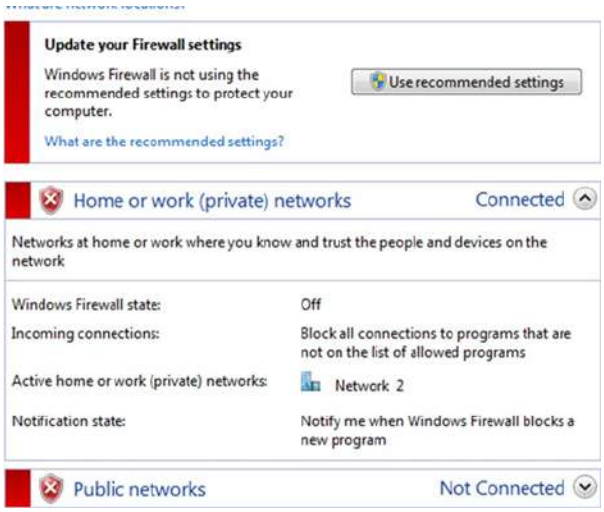
4. Windows Defender Firewall

Defending against Slowloris by using Windows Defender Firewall

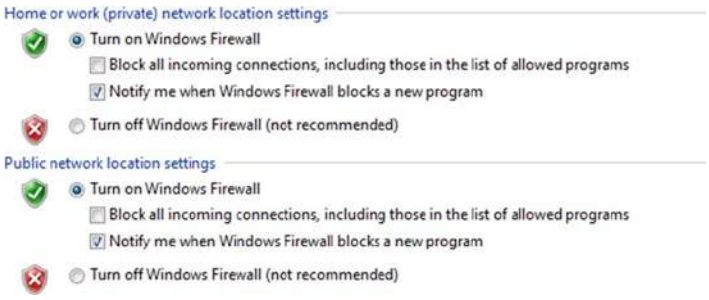
Step 1: Commence by opening the Control Panel from the Windows tab.

Step 2: Subsequently, select *System and Security*.

Step 3: In the System and Security. It will provide us with a Windows firewall.

Step 4: Within the firewall settings, locate the option to turn the firewall on or off and click on it.



Step 5: Observe that the color on the page remains red, indicating that the firewall is still turned off.

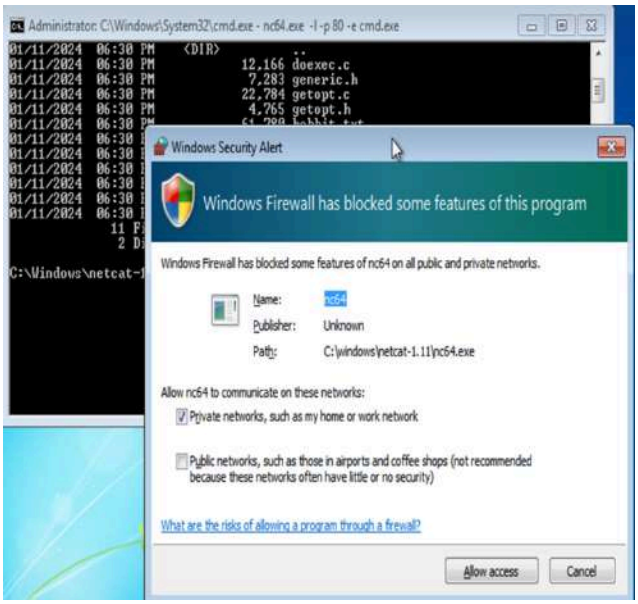


Step 6: On this page, we should tick the options on the firewall and click *Okay* to make the system do what we desire.

5. Windows Defender Firewall

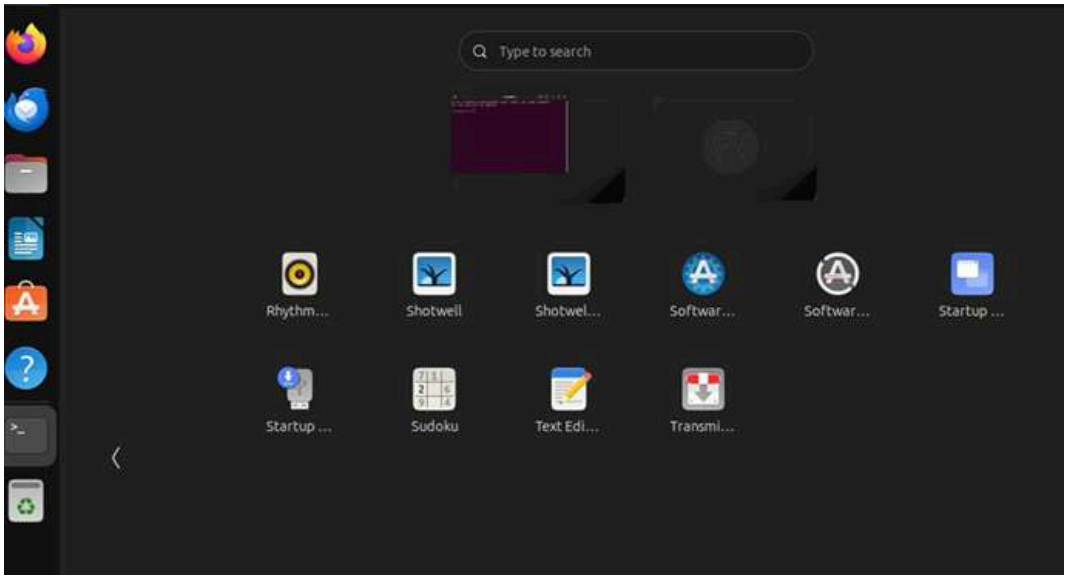
Defending against Cain and Abel by using Windows Defender Firewall

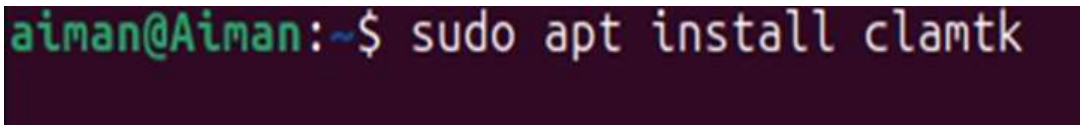
Step 1: Turning on Windows Firewall in Windows entails configuring rules to regulate the traffic coming into and going out of our network.

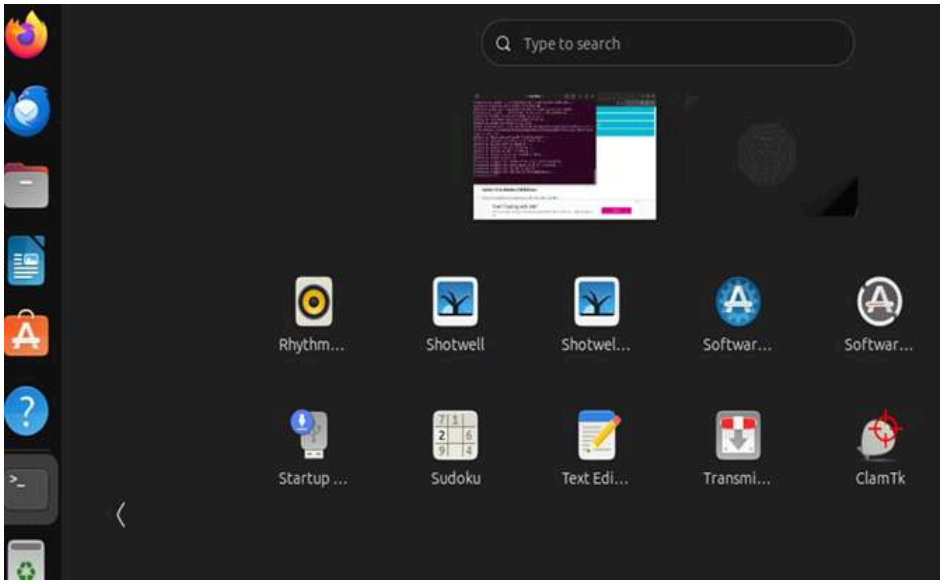
Step 2: To stop an intruder from accessing Windows, the Windows firewall generates security alerts.


LINUX

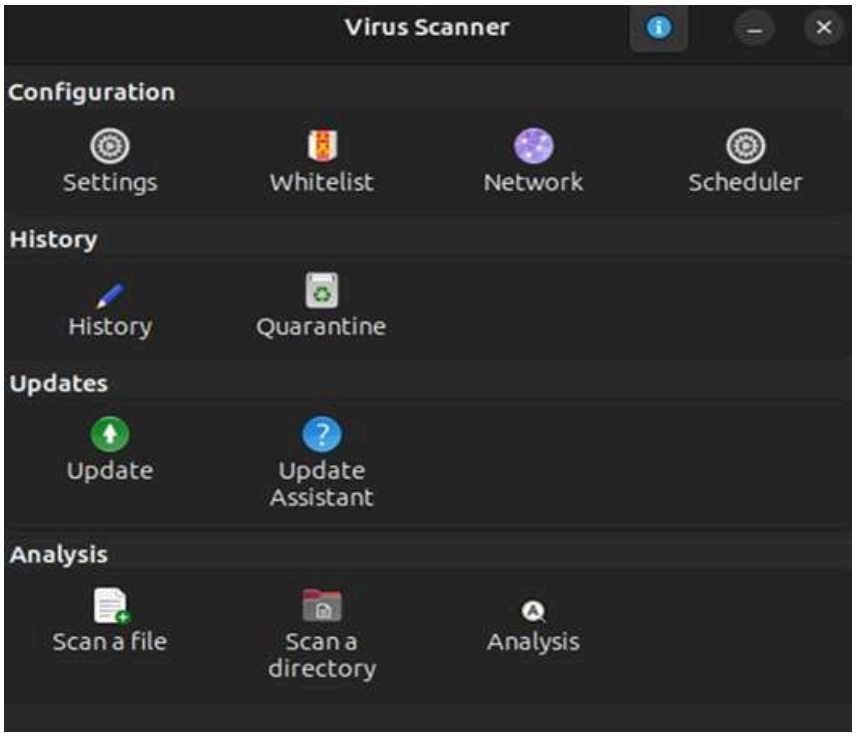
1. Antivirus ClamAV

Step 1: Ubuntu Linux does not come with antivirus software by default.

Step 2: Install ClamAV on your Ubuntu machine by entering the following command in the terminal: *apt install clamav*

Step 3: For Ubuntu Desktop users who want a graphical front end, they can install ClamTk by entering the following command: *apt install clamtk*

Step 4: ClamTK has been successfully installed on your desktop.



Step 5: Explore the features of the ClamAV antivirus.



Step 6: To check the ClamAV version, run the following command:

```
aiman@Aiman:~$ clamscan --version
ClamAV 1.0.4/27151/Thu Jan 11 17:41:16 2024
```

Step 7: Once the installation is finished, run the freshclam command to update the virus signature database. To do so, stop the Freshclam service by entering the following command: *systemctl stop clamav-freshclam.service*

```
aiman@Aiman:~$ systemctl stop clamav-freshclam.service
aiman@Aiman:~$
```

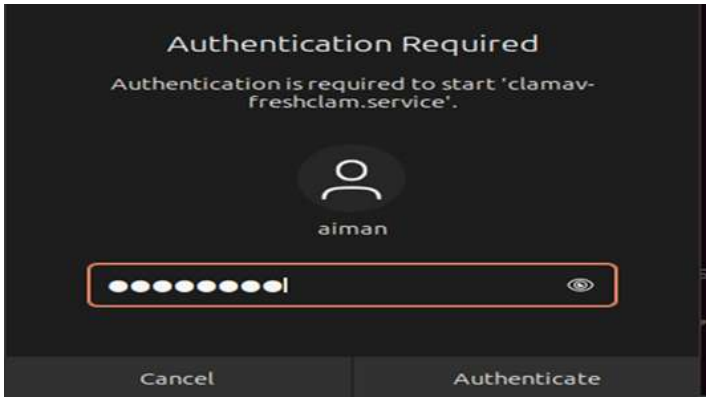
Step 8: Proceed to update the database by running the following command: *sudo freshclam*

```
aiman@Aiman:~$ sudo freshclam
[sudo] password for aiman:
ClamAV update process started a
```

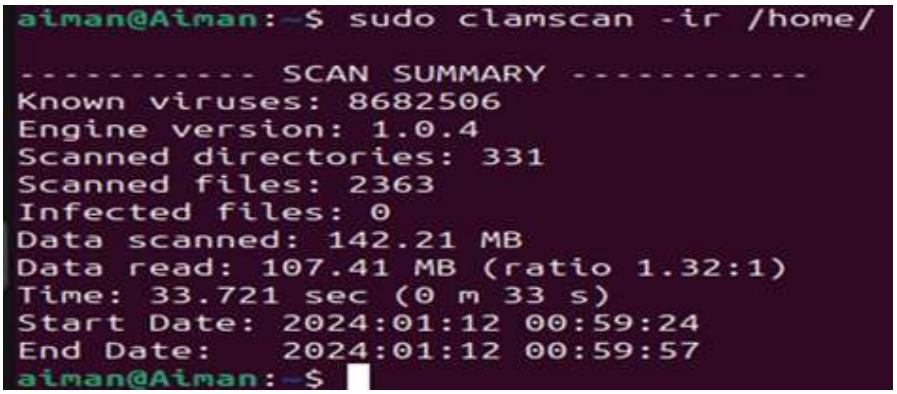
Step 9: Restart the freshclam and enter the following command: *systemctl start clamav-freshclam.service*

```
aiman@Aiman:~$ systemctl start clamav-freshclam.service
```

Step 10: Enter your password for authentication

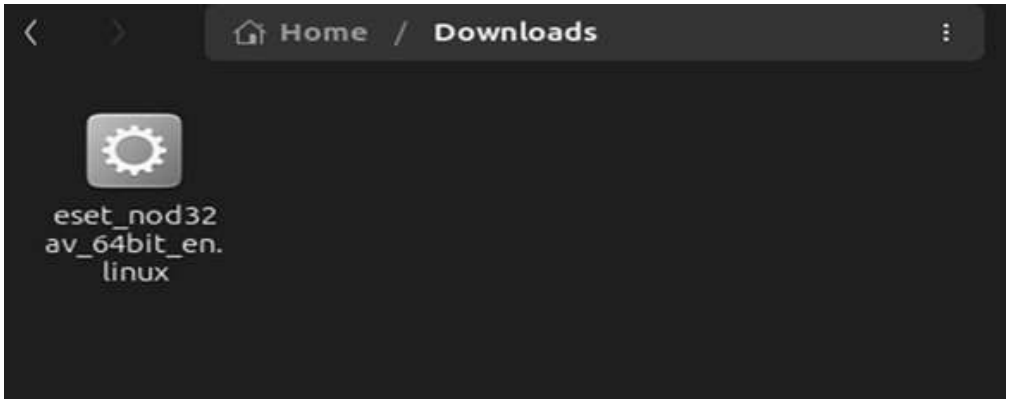


Step 11: ClamAV is capable of detecting viruses, Trojans, and other forms of malware. Scanning files for viruses is done with clamscan command, enter the following command: *sudo clamscan -ir /home/*



2. Eset nod 32 Firewall

Step 1: Download the 64-bit version of the nod32 Firewall for Ubuntu.

Step 2: Open the downloaded file in the designated folder.

Step 3: Open the file in the terminal.

Step 4: Execute the file using the following command: *Chmod +x eset_nod32av_64bit_en.linux*

```
aiman@Aiman:~/Downloads$ chmod +x eset_nod32av_64bit_en.linux
aiman@Aiman:~/Downloads$ ls
eset_nod32av_64bit_en.linux
```

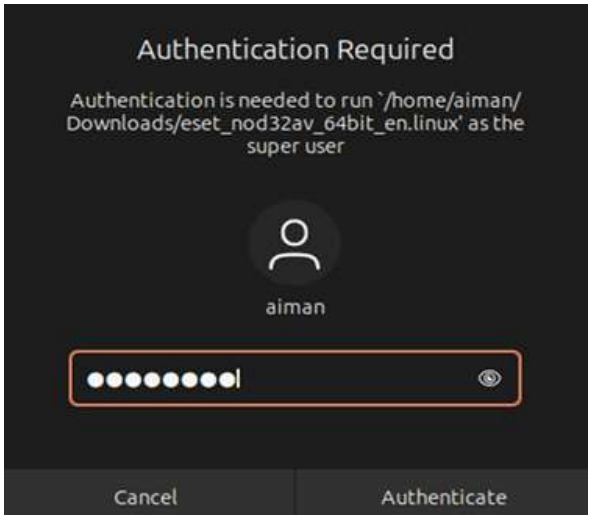
Step 5: Enter the file by using the following command:
./ eset_nod32av_64bit_en.linux

```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

Step 6: If there is an error like this, install the missing package, libc6:i386, and enter the following command:
Sudo dpkg –add-architecture i386; sudo apt-get install

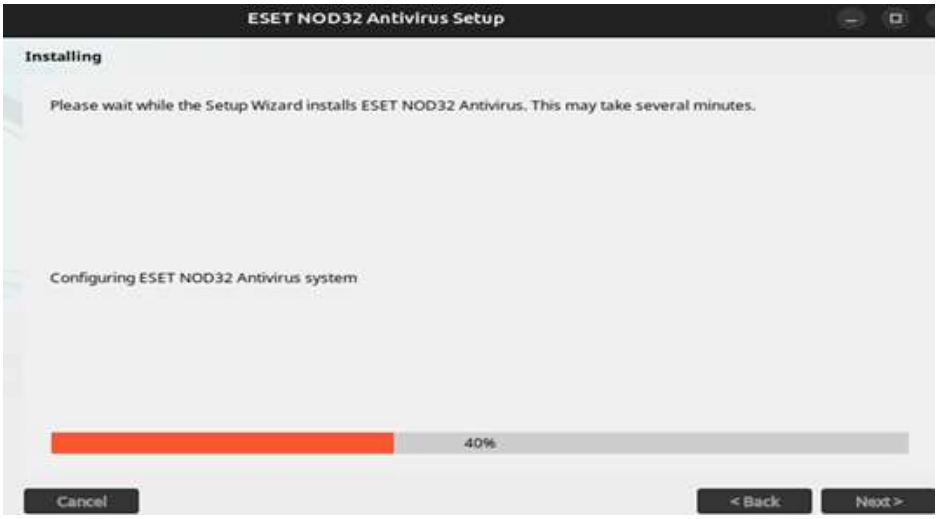
```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
error[277b0000]: Please install the following files or packages: libc6:i386, /li
b/ld-linux.so.2
aiman@Aiman:~/Downloads$ sudo dpkg --add-architecture i386; sudo apt-get install
 libc6:i386
```

Step 8: Enter your password to grant authentication.



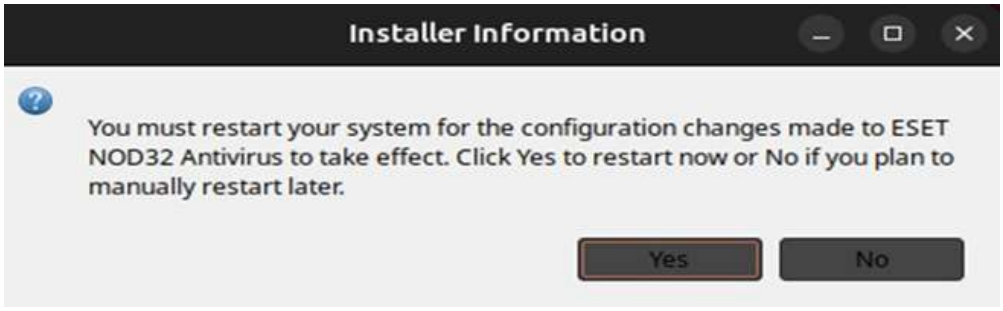
Step 9: In the antivirus setup, click Next.

Step 10: Accept all the requirements and then click Install.



Step 11: Once the installation is complete, click Finish.

Step 12: Restart your system to apply the changes and activate the antivirus.



Step 13 : The antivirus has been installed and usable in your ubuntu desktop.

3. XDP-Firewall

Step 1: Install dependencies using the following command:
sudo apt install -y libconfig-dev llvm clang libelf-dev build-essential

```
aiman@Aiman:~$ sudo apt install -y libconfig-dev llvm clang libelf-dev build-ess
ential
```

Step 2: Install dependencies for building LibXDP and LibBPF. Use the following command: *sudo apt install -y libpcap-dev m4 gcc-multilib*

```
aiman@Aiman:~$ sudo apt install -y libpcap-dev m4 gcc-multilib
```

Step 3: You need tools for your kernel. Since we need BPFTool, use the following command to install it: *sudo apt install -y linux-tools-$(uname -r)*

```
aiman@Aiman:~$ sudo apt install -y linux-tools-$(uname -r)
```

Step 4: To install git in your Ubuntu, run the following command: *Apt install git*

```
aiman@Aiman:~$ apt install git
```

Step 5: To clone the repository via Git. Use the recursive flag to download LibBPF sub-module using the following command:
git clone --recursive https://github.com/gamemann/XDP-Firewall.git

```
aiman@Aiman:~$ git clone --recursive https://github.com/gamemann/XDP-Firewall.gi
t
```

Step 6: Change the directory to the repository using the following command: *cd XDP-Firewall*

```
aiman@Aiman:~$ cd XDP-Firewall
```

Step 7: To install make use the following command: *sudo apt install make*.

Step 8: Build XDP-Tools and install LibXDP & LibBPF to /usr/include using the following command: *make libxdp*

```
aiman@Aiman:~/XDP-Firewall$ make libxdp
```

Step 9: Build the main project and install as root via Sudo using the following command: *make && sudo make install*

```
aiman@Aiman:~/XDP-Firewall$ sudo make && sudo make install
```

TASK DISTRIBUTION

Task	Person in Charge
Blue Team concepts and activities preparation	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012) 2. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045)
Red Team concepts and activities preparation	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039) 2. WARSENA A/P EH CHUOI (CB21056)
Computer and network services preparation	1. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045) 2. WARSENA A/P EH CHUOI (CB21056)
Identify tools for attack	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039)
Identify tools for defend	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012)
Set up computer and network services (Blue Team)	1. NURUL ADRIANA BINTI MOHAMMAD AFANDI (CB21045)
Setup attack tools (Red Team)	1. WARSENA A/P EH CHUOI (CB21056)
Perform attack tools (Red Team)	1. TENGKU FARISHA ELLIANA BINTI TENGKU HAMZAH (CB21039)
Plan mitigation and perform countermeasures based on each of the attacks (Blue Team)	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012)

REFERENCES

Firch, J. (2020, September 27). What Is A Red Team VS A Blue Team In Cyber Security? PurpleSec. https://purplesec.us/red-team-vs-blue-team-cyber-security/

Top 10 Kali Linux Tools For Hacking. (2020, July 11). GeeksforGeeks. https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/

17 free cybersecurity tools you should know about. (n.d.). WhatIs.com. https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about

Saxena, A. (2023, March 11). Top 15 Cybersecurity tools You Must Know in 2023. Sprinto. https://sprinto.com/blog/best-cybersecurity-tools/

Top 25 Linux Security Tools to Boost Cyber Defense. (2023, May 23). https://www.stationx.net/linux-security-tools/

AVG 2019 | FREE Antivirus & TuneUp for PC, Mac, Android. (n.d.). AVG.com. https://www.avg.com/en-ww/homepage#pc

What is Windows Defender Firewall? (n.d.). Www.computerhope.com. https://www.computerhope.com/jargon/w/windows-defender-firewall.htm