|  |  |
| --- | --- |
| Logo  Description automatically generated | THỰC HÀNH  CÁC LỆNH CƠ BẢN CỦA Metasploit |

Họ và tên Sinh viên: Mã Sinh viên:

Nhóm học phần:

[1. Giới thiệu 2](#_Toc144382410)

[1.1. Các bước chính sử dụng Metasploit framework 2](#_Toc144382411)

[1.1.1 Chọn module exploit: 2](#_Toc144382412)

[1.1.2 Thiết lập các tham số cho module exploit đã chọn: 2](#_Toc144382413)

[1.1.3 Lựa chọn payload 2](#_Toc144382414)

[1.1.4 Thực thi khai thác lỗ hổng (exploit) 2](#_Toc144382415)

[1.2. Các tham số của metasploit 3](#_Toc144382416)

[1.3. Giới thiệu payload meterpreter 3](#_Toc144382417)

[1.4. Hệ thống mạng thực hành 5](#_Toc144382418)

[2. Truy cập từ xa đến Kali Linux 5](#_Toc144382419)

[3. Sử dụng các lệnh metasploit cơ bản 7](#_Toc144382420)

[3.1. Khởi động Metasploit: 7](#_Toc144382421)

[3.2. Xem tất cả các tùy chọn: 7](#_Toc144382422)

[3.3. Xem thông tin database của metasploit 8](#_Toc144382423)

[3.4. show: Shows every module within Metasploit. 8](#_Toc144382424)

[3.5. use : Select a module 8](#_Toc144382425)

[3.6. help: Returns a list and small description of all available commands. 9](#_Toc144382426)

[3.7. check: (Not supported by all exploit) check option that will check to see if a target is vulnerable 9](#_Toc144382427)

[3.8. targets: Within the context of an exploit module show targets returns which targets are supported. 9](#_Toc144382428)

[3.9. back: Once you have finished working with a particular module use the back command to move out of the current context. 9](#_Toc144382429)

[3.10. info: Provides detailed information about a particular module including all options, targets, and other information. 9](#_Toc144382430)

[3.11. connect : Netcat-like command built into the msfconsole. 9](#_Toc144382431)

[3.12. edit: Edit the current module in Vim 9](#_Toc144382432)

[3.13. irb: Opens a live ruby interpreter shell 9](#_Toc144382433)

[3.14. jobs: Provides the ability to list and terminate background jobs 10](#_Toc144382434)

[3.15. kill: Kill any running jobs. 10](#_Toc144382435)

[3.16. load: Loads a plugin from Metasploit’s plugin directory 10](#_Toc144382436)

[3.17. loadpath: Load a third-part module tree 10](#_Toc144382437)

[3.18. unload: Unloads a previously loaded plugin and removes any extended commands 10](#_Toc144382438)

[3.19. resource: Runs resource files that can be loaded through msfconsole 10](#_Toc144382439)

[3.20. sessions: Allows to list, interact with, and kill spawned sessions 10](#_Toc144382440)

[3.21. set: Set framework options and parameters for the current module 10](#_Toc144382441)

[3.22. unset: Removes a parameter previously configured with set. (unset all removes all assigned variables) 10](#_Toc144382442)

[3.23. setg: Set a global variables within msfconsole. The current environment can be saved with save command 10](#_Toc144382443)

[3.24. Sử dụng một số lệnh HĐH trongmetasploit 11](#_Toc144382444)

[3.25. exit: Exit msfconsole 11](#_Toc144382445)

[3.26. Xem nội dung thư mục /usr/share/metasploit-framework 11](#_Toc144382446)

# 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.*

## Các bước chính sử dụng Metasploit framework

### Chọn module exploit:

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

* **show exploits:** Xem các module exploit mà framework có hỗ trợ
* **use exploit\_name:** Chọn module exploit
* **info exploit\_name**: Xem thông tin về module exploit

### Thiết lập các tham số cho module exploit đã chọn:

* **show options:** Xác định những options nào cần cấu hình
* **set**: Cấu hình cho những option của module đó
* **show advanceds**: Xem các advanced options của một số module

### Lựa chọn payload

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính victim được điều khiển từ xa.

* **show payloads:** Liệt kê ra những payload của module exploit hiện tại
* **info payload\_name:** Xem thông tin chi tiết về payload đó
* **set PAYLOAD payload\_name:** Xác định payload module name.Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó
* **show advanced:** Xem những advanced option của payload đó.

### Thực thi khai thác lỗ hổng (exploit)

* **exploit:** Lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác.

## Các tham số của metasploit

* LHOST: Địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì dùng IP Public, hoặc DDNS của No-IP.com)
* RHOST, RHOSTS: Địa chỉ IP của máy Vicitm (Nếu tấn công ngoài Internet thì dùng IP Public, RHOST có thể là URL Website)
* LPORT: Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)
* RPORT: Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho người dùng)
* PAYLOAD: Có cấu trúc như sau (tên hệ điều hành/kiểu hệ thống/kiểu tấn công/giao thức tấn công)
* Tên hệ điều hành: android hay windows
* Kiểu hệ thống: x86 hay x64 (Có thể bỏ qua)
* Kiểu tấn công: meterpreter hay shell
* Giao thức: reverse\_tcp; reverse\_tcp\_dns; reverse\_https

Ví dụ: *windows/meterpreter/reverse\_tcp\_dns*

## Giới thiệu payload meterpreter

Meterpreter cung cấp một tập lệnh để khai thác trên các remote computer:

* **Fs:** Cho phép upload và download files từ các remote machine
* **Net:** Cho phép xem thông tin mạng của remote machine như IP, route table
* **Process:** Cho phép tạo các processes mới trên remote machine
* **Sys:** Cho phép xem thông tin hệ thống của remote machine

Sử dụng câu lệnh:

* *use -m module1,module2,module3 [ -p path ] [ -d ]*: Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process.
* *loadlib -f library [ -t target ] [ -lde ]*: Câu lệnh cho phép load các thư viện của remote machines.
* *read channel\_id [length]*: Lệnh read cho phép xem dữ liêu của remote machine trên channel đang kết nối.
* *write channel\_id*: Lệnh write cho phép ghi dữ liệu lên remote machine.
* *close channel\_id*: Đóng channel mà đã kết nối với remote computer.
* *interact channel\_id*: Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.
* *initcrypt cipher [parameters]*: Mã hoá dữ liệu được gửi giữa host và remote machine.

**Sử dụng module Fs:** Cho phép upload và download files từ các remote machine.

* *cd directory:* Giống lệnh cd
* *getcwd:*Cho biết thư mục đang làm việc hiện tại
* *ls [filter\_string]*: liệt kê các thư mục và tập tin
* upload src1 [src2 ...] dst: Upload file
* download src1 [src2 ...] dst: Download file

Sử dụng module Net:

* ipconfig
* *route:* Xem bảng định tuyến của remote machine.
* portfwd [ -arv ] [ -L laddr ] [ -l lport ] [ -h RHOST ] [ -p RPORT ] [ -P ]: Cho phép tạo port forward giữa host và remote machine.

Sử dụng module Process:

* *execute -f file [ -a args ] [ -Hc ]*: Câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu
* *kill pid1 pid2 pid3*: Huỷ những process đang chạy trên máy remote machine
* *ps*: Liệt kê những process của remote machine.

Sử dụng module Sys:

* *getuid*: Cho biết username hiện tại của remote machine
* *sysinfo*: Cho biết thông tin về tên máy tính, hệ điều hành.

Nhóm lệnh thao tác trên mục tiêu :

* cat <file> : Xuất nội dung file ra terminal.
* cd <folder> : Chuyển thư mục thực thi.
* edit <file> : Chỉnh sửa nội dung một file.
* getwd và pwd : Hiển thị thực thi hiện hành.
* ls [folder] : Xuất ra danh sách các file và thự mục.
* mkdir <folder> : Tạo thư mục mới.
* cp <file1> <file2> : Sao chép file đến địa chỉ mới và đổi tên (nếu có).
* mv <file1> <file2> : Di chuyển file đến địa chỉ mới và đổi tên (nếu có).
* rm <file> : Xóa file.
* rmdir <folder> : Xóa thư mục rỗng.
* search <name> : Tìm kiếm file hoặc thư mục.

Nhóm lệnh thao tác trên Local:

* getlwd và lpwd cho biết địa chỉ thư mục đang thực hiện.
* lcd để di chuyển thư mục thực thi hiện hành.

Nhóm lệnh chung:

* upload <file> : Tải lên một tập tin từ local lên mục tiêu.
* download <file> : Tải xuống một tập tin từ remote về local.

## Hệ thống mạng thực hành

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>@itfdut.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: itfdut.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.

# Sử dụng các lệnh metasploit cơ bản

## Khởi động Metasploit:

user@vmkali:~$ cd

user@vmkali:~$ sudo msfconsole

[-] \*\*\*rting the Metasploit Framework console...|

[-] \* WARNING: No database support: No database YAML file

[-] \*\*\*

IIIIII    dTb.dTb        \_.---.\_

  II     4'  v  'B   .'"".'/|\`.""'.

  II     6.     .P  :  .' / | \ `.  :

  II     'T;. .;P'  '.'  /  |  \  `.'

  II      'T; ;P'    `. /   |   \ .'

IIIIII     'YvP'       `-.\_\_|\_\_.-'

I love shells --egypt

       =[ metasploit v5.0.2-dev                           ]

+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post       ]

+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]

+ -- --=[ 2 evasion                                       ]

+ -- --=[ \*\* This is Metasploit 5 development branch \*\*   ]

msf6 >

## Xem tất cả các tùy chọn:

msf6 > help search

msf6 > search cve:2021 type:exploit

msf6 > search cve:2021 type:exploit platform:-linux

* Tìm exploit cho lỗ hổng Microsoft’s Security Bulletin MS13-069

msf6 > search MS13-069

* Tìm theo số CVE ID

msf6 > search cve:2013-3660

* Tìm tất cả CVE ID thuộc năm nào đó

msf6 > search cve:2022

msf6 > search cve:2023

* search: Regular-expression based search functionality (naming convention for Metasploit modules uses underscores versus hyphens).

msf6 > search struts

msf6 > search name:struts

* platform: Search to modules that affect a specific platform.

msf6 > search platform:android

* author: Search for modules by a specific author.

msf6 > search author:rapid7

msf6 > search type:exploit name:struts cve:2017

## Xem thông tin database của metasploit

msf6 > db\_status

## show: Shows every module within Metasploit.

* Xem tất cả các exploit có trong database của Metasploit

msf6 > show exploits

* auxiliary: Display a list of all of the available auxiliary modules.

msf6 > show auxiliary

* payloads: show payloads will display all of the different payloads available.

msf6 > show payloads

* show encoders: Display a listing of the encoders that are available within MSF.

msf6 > show encoders

## use : Select a module

* Chọn sử dụng exploit *ms17\_010\_eternalblue*

msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show info

## help: Returns a list and small description of all available commands.

msf6 > help

## check: (Not supported by all exploit) check option that will check to see if a target is vulnerable

msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > check

[\*] www.XYZXYZ.org:8080 The target is not exploitable.

## targets: Within the context of an exploit module show targets returns which targets are supported.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show targets

## back: Once you have finished working with a particular module use the back command to move out of the current context.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > back

msf6 >

## info: Provides detailed information about a particular module including all options, targets, and other information.

* Xem thông tin về exploit cụ thể. Thông tin bao gồm tác giả, các tham số, giới thiệu và các trang web thông tin về exploit đó.

msf6 > info exploit/windows/browser/ms13\_069\_caret

* Provides detailed information about a particular module including all options, targets, and other information.

msf6 > info exploit/windows/browser/ms13\_069\_caret

## connect : Netcat-like command built into the msfconsole.

msf6 > connect 192.168.1.10 80

## edit: Edit the current module in Vim

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > edit

[!] LocalEditor or $VISUAL/$EDITOR should be set. Falling back on vim.

[\*] Launching vim /opt/metasploit-framework/embedded/framework/modules/exploits/windows/smb/ms17\_010\_eternalblue.rb

## irb: Opens a live ruby interpreter shell

msf6 > irb

[\*] Starting IRB shell...

>> puts "Test!"

Test!

## jobs: Provides the ability to list and terminate background jobs

msf6 > jobs -h

## kill: Kill any running jobs.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > kill 0

## load: Loads a plugin from Metasploit’s plugin directory

msf6 > load

## loadpath: Load a third-part module tree

msf6 > loadpath /home/andrea/modules

## unload: Unloads a previously loaded plugin and removes any extended commands

msf6 > unload pcap\_log

## resource: Runs resource files that can be loaded through msfconsole

msf6 > resource

## sessions: Allows to list, interact with, and kill spawned sessions

msf6 > sessions -h

## set: Set framework options and parameters for the current module

msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOST 192.168.1.110

RHOST => 192.168.1.10

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

## unset: Removes a parameter previously configured with set. (unset all removes all assigned variables)

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOST 192.168.1.110

RHOST => 192.168.1.10

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > unset RHOST

Unsetting RHOST...

## setg: Set a global variables within msfconsole. The current environment can be saved with save command

msf6 > setg LHOST 192.168.1.10

LHOST => 192.168.1.10

msf6 > setg RHOSTS 192.168.1.110/24

RHOSTS => 192.168.1.110/24

msf6 > save

Saved configuration to: /home/andrea/.msf4/config

## Sử dụng một số lệnh HĐH trongmetasploit

msf6 > pwd

msf6 > hostname

msf6 > ifconfig

msf6 > ping 8.8.8.8

msf6 > ping 192.168.1.110

msf6 > sudo nmap 192.168.1.110

…

## exit: Exit msfconsole

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > exit

user@vmkali:~$

## Xem nội dung thư mục /usr/share/metasploit-framework

user@vmkali:~$ ls /usr/share/metasploit-framework/

app            Gemfile                       msfconsole       msfrpcd    Rakefile         scripts

config         Gemfile.lock                  msfd             msfupdate  ruby             tools

data           lib                           msfdb            msfvenom   script-exploit   vendor

db             metasploit-framework.gemspec  msf-json-rpc.ru  msf-ws.ru  script-password

documentation  modules                       msfrpc           plugins    script-recon

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/

auxiliary  encoders  evasion  exploits  nops  payloads  post

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/exploits/

aix      apple\_ios  bsdi    example.rb  freebsd  irix   mainframe  netware  qnx      unix

android  bsd        dialup  firefox     hpux     linux  multi      osx      solaris  windows

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/payloads/

singles  stagers  stages

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/auxiliary/

admin    bnat    cloud    docx  example.rb  fuzzers  parser  scanner  sniffer  sqli  vsploit

analyze  client  crawler  dos   fileformat  gather   pdf     server   spoof    voip

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/encoders/

cmd  generic  mipsbe  mipsle  php  ppc  ruby  sparc  x64  x86

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/exploits/windows/

antivirus   browser     firewall  iis      local  motorola  novell    proxy  smtp    unicenter

arkeia      dcerpc      ftp       imap     lotus  mssql     nuuo      rdp    ssh     vnc

backdoor    email       games     isapi    lpd    mysql     oracle    scada  ssl     vpn

backupexec  emc         http      ldap     misc   nfs       pop3      sip    telnet  winrm

brightstor  fileformat  ibm       license  mmsp   nntp      postgres  smb    tftp    wins

user@vmkali:~$ ls /usr/share/metasploit-framework/modules/exploits/windows/smb/

eternalblue\_doublepulsar.rb   ms06\_040\_netapi.rb                     ms17\_010\_eternalblue\_win8.py

generic\_smb\_dll\_injection.rb  ms06\_066\_nwapi.rb                      ms17\_010\_psexec.rb

group\_policy\_startup.rb       ms06\_066\_nwwks.rb                      netidentity\_xtierrpcpipe.rb

ipass\_pipe\_exec.rb            ms06\_070\_wkssvc.rb                     psexec\_psh.rb

ms03\_049\_netapi.rb            ms07\_029\_msdns\_zonename.rb             psexec.rb

ms04\_007\_killbill.rb          ms08\_067\_netapi.rb                     smb\_delivery.rb

ms04\_011\_lsass.rb             ms09\_050\_smb2\_negotiate\_func\_index.rb  smb\_relay.rb

ms04\_031\_netdde.rb            ms10\_046\_shortcut\_icon\_dllloader.rb    timbuktu\_plughntcommand\_bof.rb

ms05\_039\_pnp.rb               ms10\_061\_spoolss.rb                    webexec.rb

ms06\_025\_rasmans\_reg.rb       ms15\_020\_shortcut\_icon\_dllloader.rb

ms06\_025\_rras.rb              ms17\_010\_eternalblue.rb

user@vmkali:~$

user@vmkali:~$ msfconsole --version

user@vmkali:~$ ruby --version

user@vmkali:~$ lsb\_release -a

user@vmkali:~$ bundle –version

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