|  |  |
| --- | --- |
| Logo  Description automatically generated | THỰC HÀNH LAP 07  CÁC LỆNH CƠ BẢN CỦA Metasploit |

Họ và tên Sinh viên: Nguyễn Công Cường

Mã Sinh viên: 102200013

Nhóm học phần: 20Nh10

# Truy cập từ xa đến Kali Linux

A computer screen shot of a black screen

Description automatically generated

# 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