Báo cáo bài thực hành số 2

Môn học

An toàn Hệ điều hành

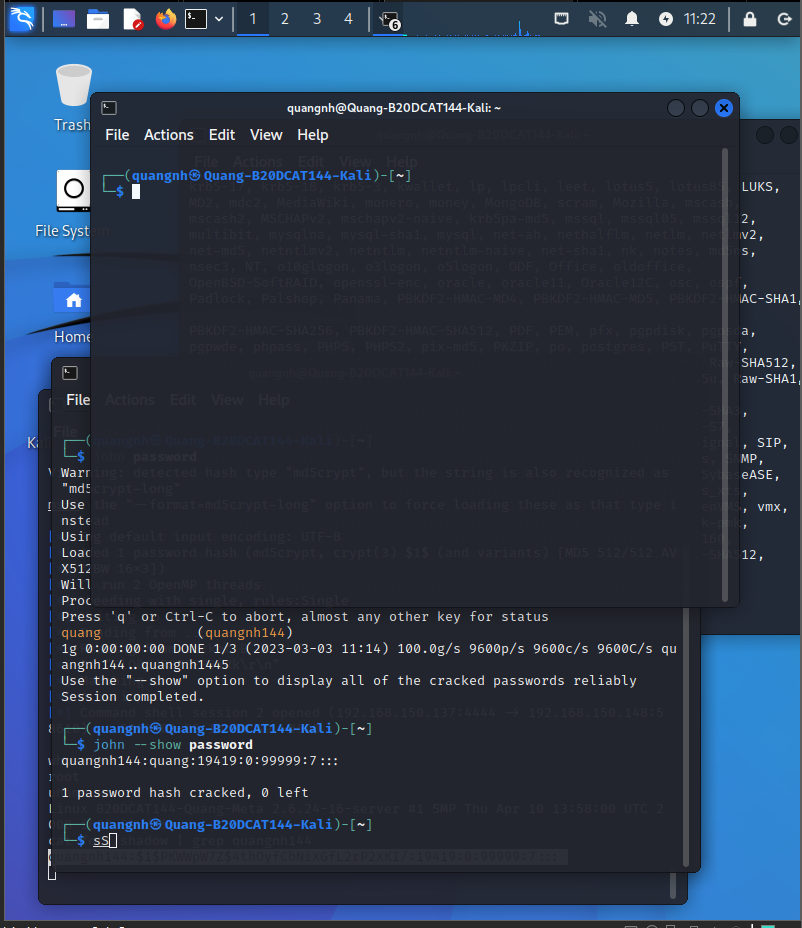
Giảng viên : Hoàng Xuân Dậu Họ tên : Nguyễn Huy Quang Mã SV: B20DCAT1144

# Mục đích:

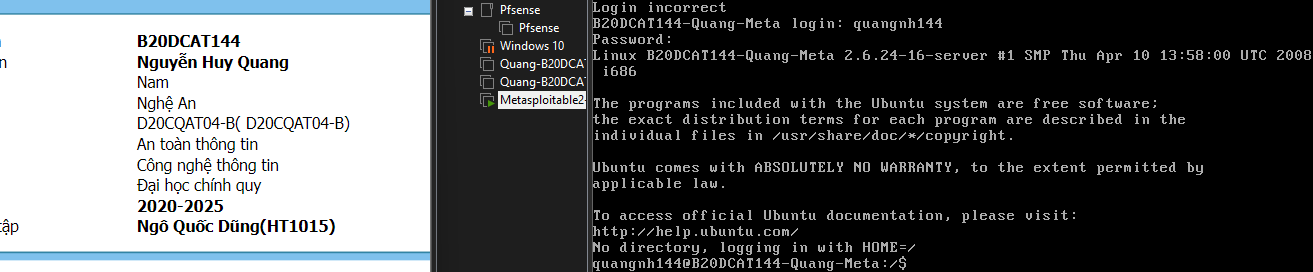
* + Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
  + Luyện thành thạo kỹ năng thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

# Thực hành:

* + Cài đặt các công cụ, nền tảng:
    - Cài đặt Kali Linux

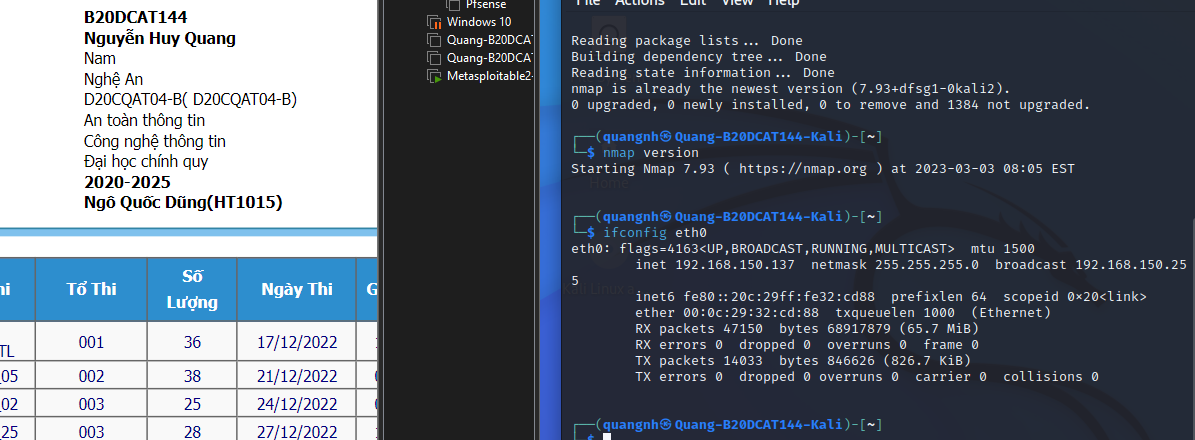


* + - Cài đặt Metasploitable2 làm máy victim

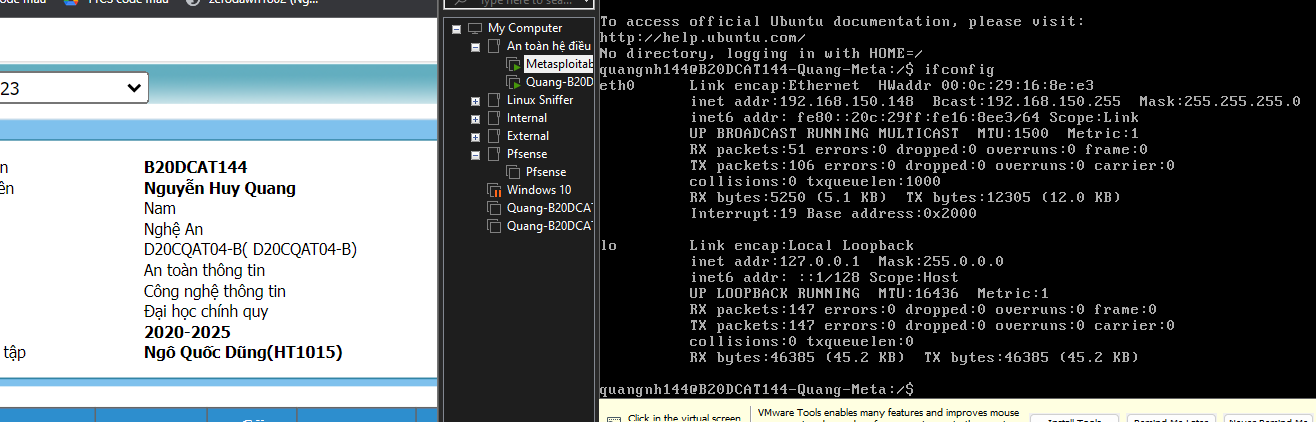


* + Tìm địa chỉ IP máy victim, kali :

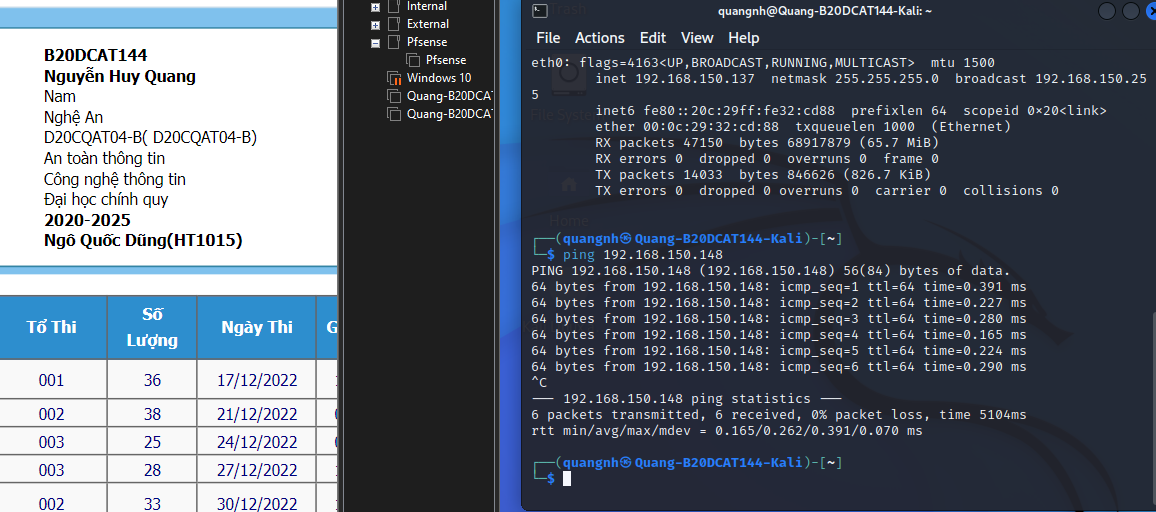
+ IP máy kali :



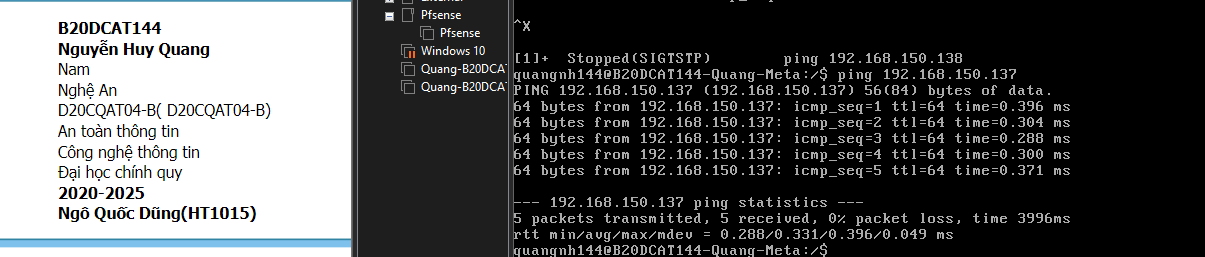
* + - IP máy victim :



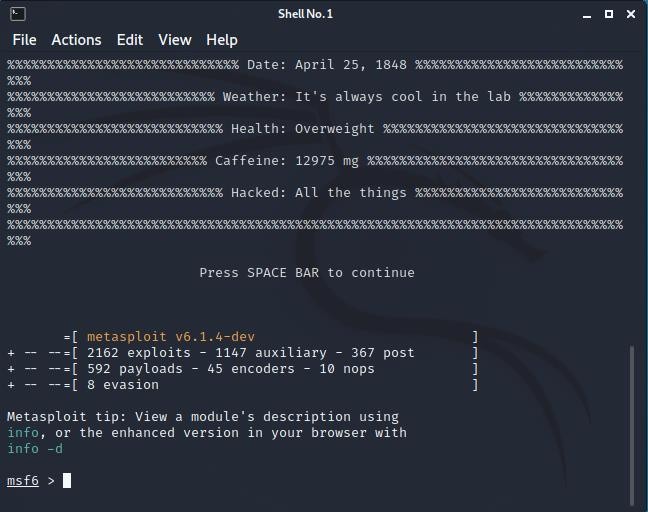
* + Kiểm tra kết nối giữa các máy :
    - Từ máy Kali ping tới máy victim

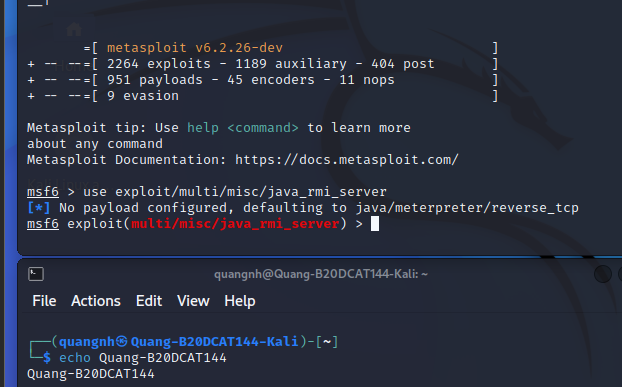


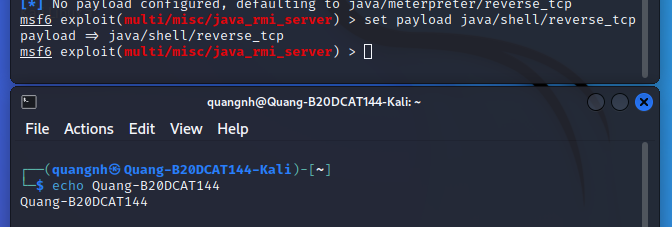
* + - Từ máy victim ping tới máy Kali



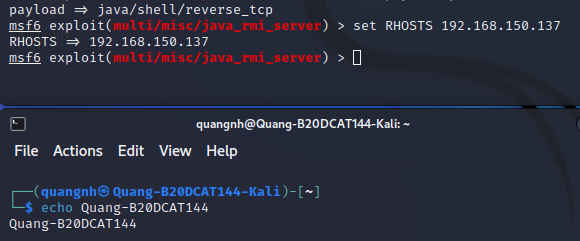
* + Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI
    - Khởi động Metasploit



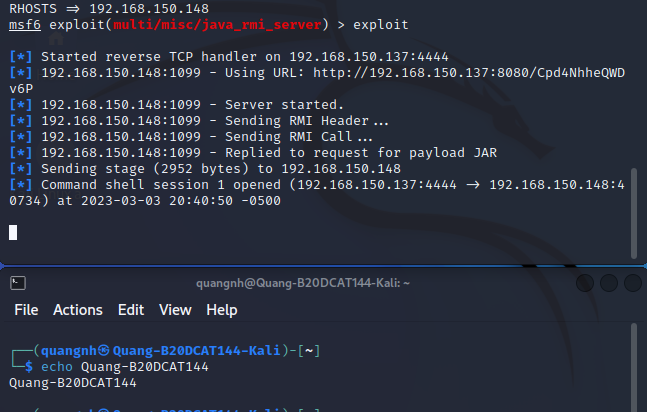
* + - Khai báo sử dụng mô đun tấn công 
    - Chọn payload cho thực thi (mở shell)

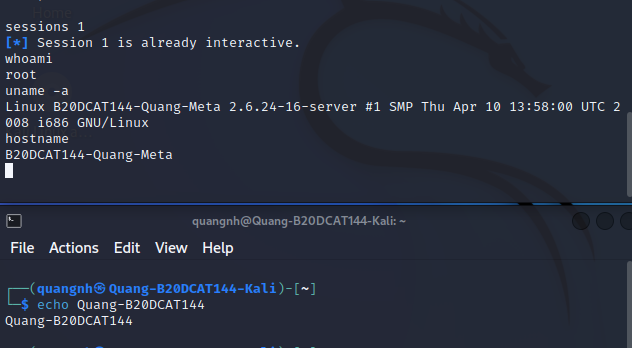


* + - Đặt địa chỉ IP máy victim



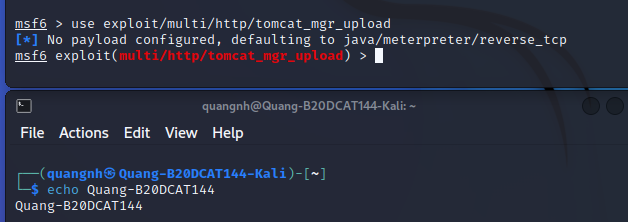
* + - Thực thi tấn công



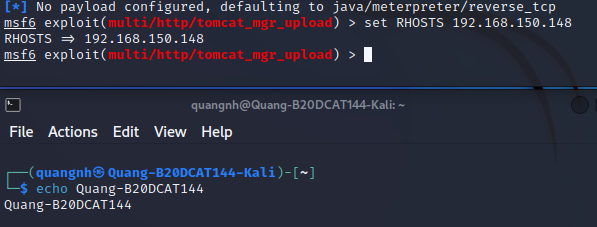


* + Khai thác lỗi trên Apache Tomcat

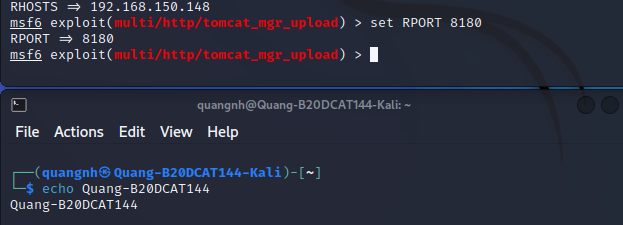
* + - Khai báo sử dụng mô đun tấn công



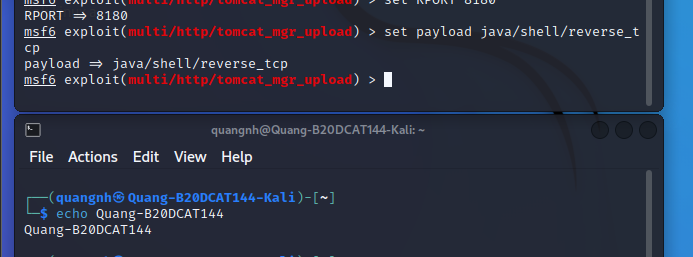
* + - Đặt địa chỉ IP máy victim



* + - Đặt 445 là cổng truy cập máy victim



* + - Chọn payload cho thực thi (mở shell)



* + - Thực thi tấn công

