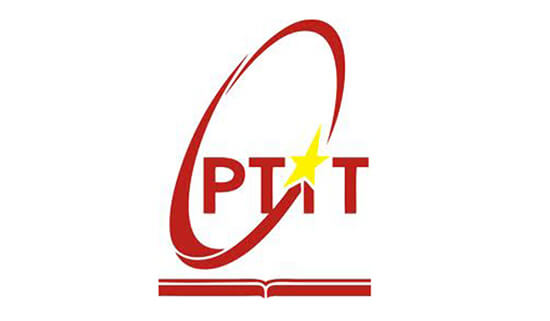
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn: AN TOÀN HỆ ĐIỀU HÀNH

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

Họ và tên sinh viên:

Đỗ Tiến Sĩ

Mã số sinh viên:

B20DCAT153

Họ và tên giảng viên:

PGS.TS. Hoàng Xuân Dậu

Hà Nội 3/2023 (tháng/năm)

**I. Mục đích**

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

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

**II. Chuẩn bị**

1. Các phần mềm, công cụ cần có

- Kali Linux

- Metasploit

- Metasploitable: Máy ảo VMWare chứa lỗi, có thể tại tại:

o Metasploitable - Browse /Metasploitable2 at SourceForge.net

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

Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại:

<https://www.hackingarticles.in/comprehensive-guide-on-metasploitable>

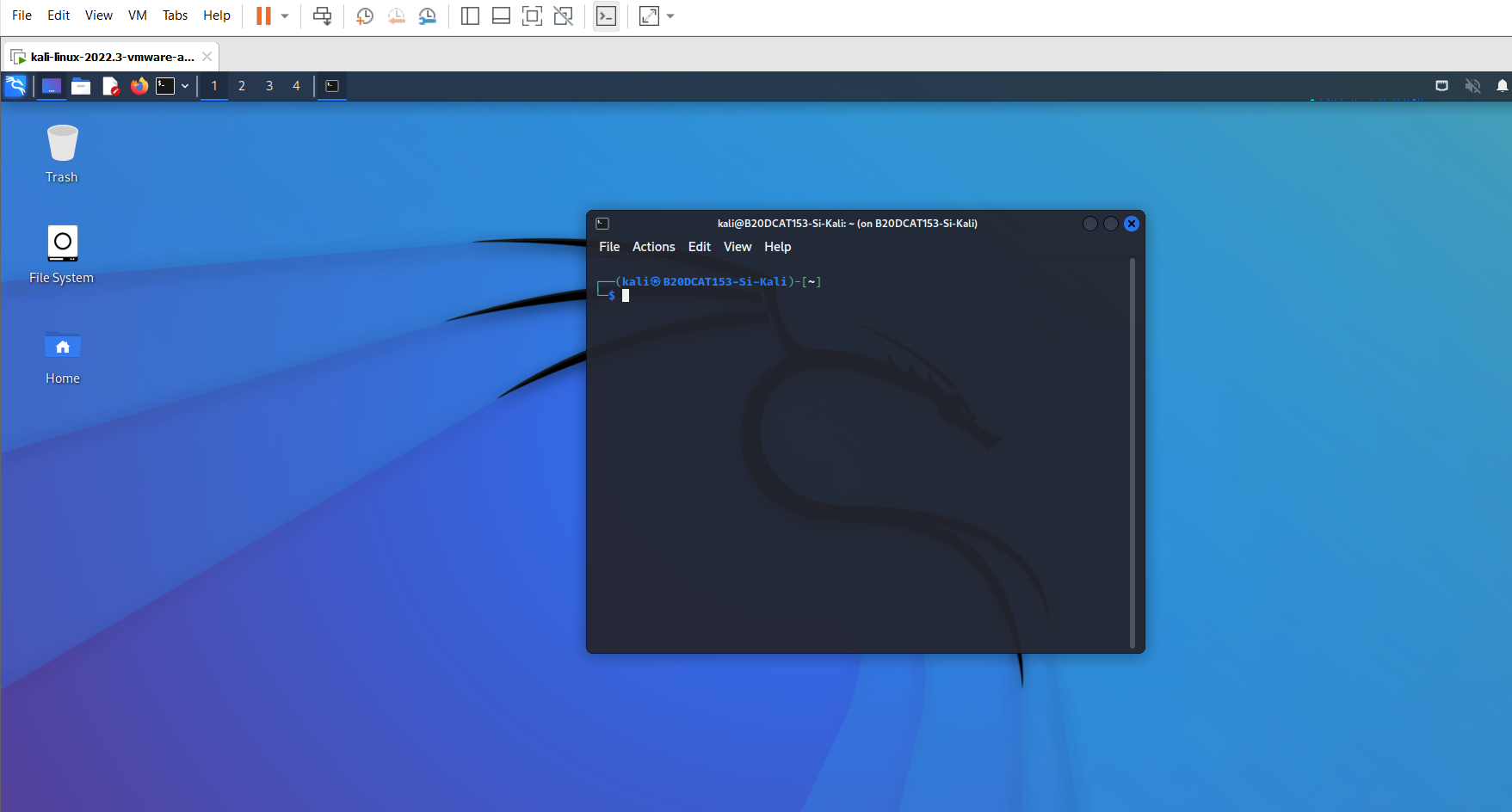
Bài thực hành này tìm hiểu về các lỗ hổng bảo mật nguy hiểm trên một số dịch vụ của hệ điều hành và cách khai thác: - Lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI chạy trên cổng 8080, cho phép khai thác và kiểm soát hệ thống. Đọc thêm tại https://www.infosecmatter.com/metasploit-modulelibrary/?mm=exploit/multi/misc/java\_rmi\_server -

- 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 hệthống. Đọc thêm tại https://www.infosecmatter.com/metasploit-modulelibrary/?mm=exploit/multi/http/tomcat\_mgr\_upload

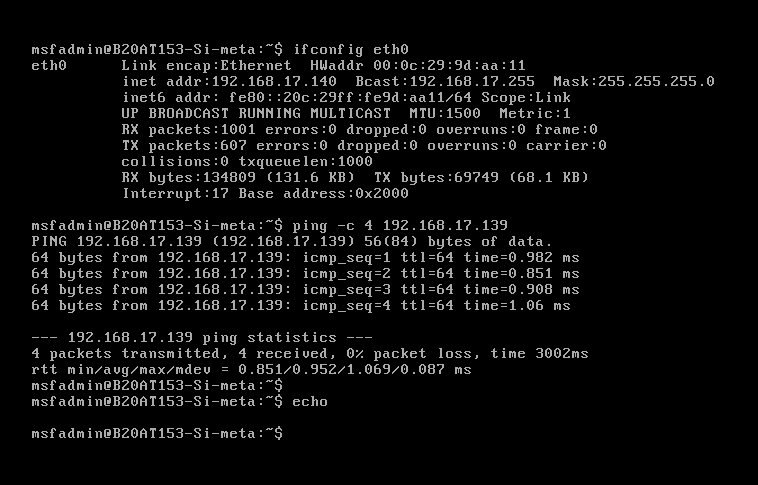
**III. Nội dung thực hành**

**1. Cài đặt các công cụ, nền tảng**

Cài đặt Kali Linux:

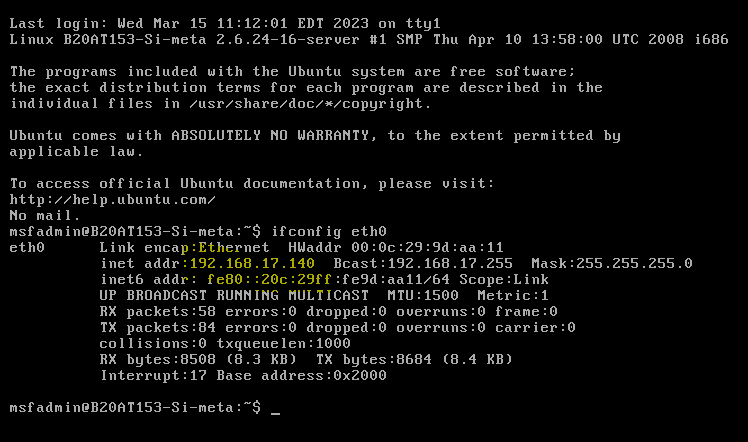


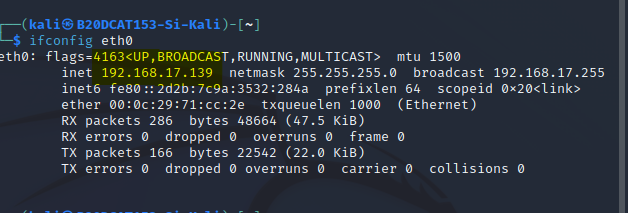
Tải và cài đặt Metasploitable2 làm máy victim:



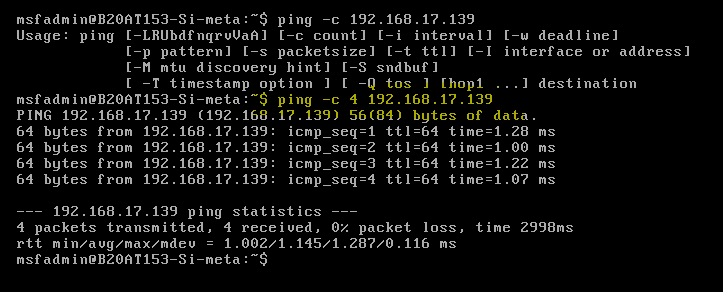
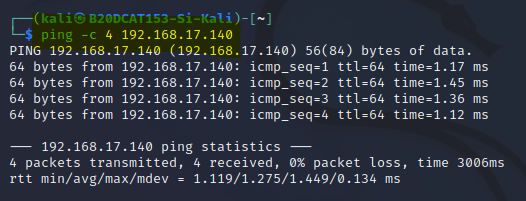
**2. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại:**

Tìm địa chỉ IP của máy victim, kali:

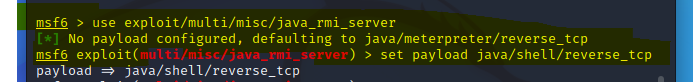


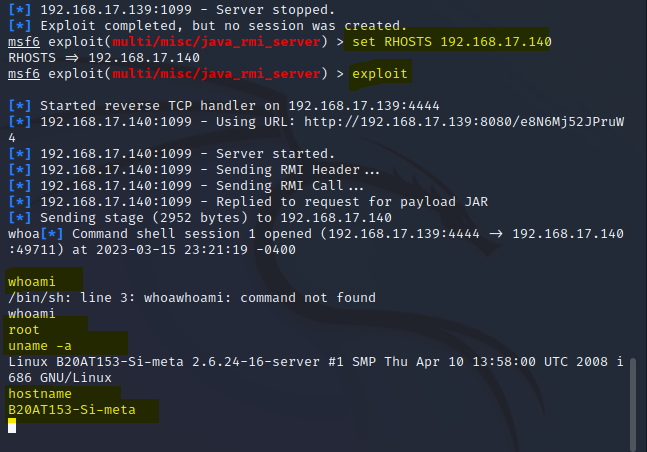


Kiểm tra kết nối mạng giữa các máy:



**3. Khai thác lỗ hổng sự dụng cấu hình ngầm định trong dịch vụ Java RMI**





**4. Khai thác lỗi trên Apache Tomcat**

