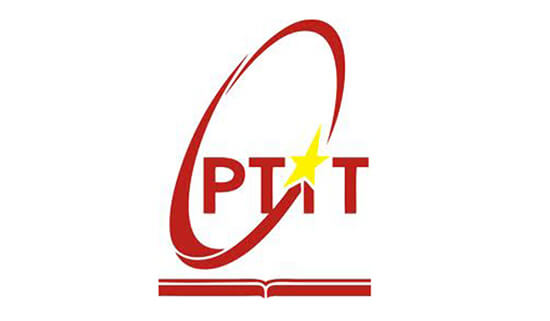
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**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 2: Máy ảo VMWare chứa lỗi, có thể tại tại: Metasploitable - Browse /Metasploitable2 at SourceForge.net

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

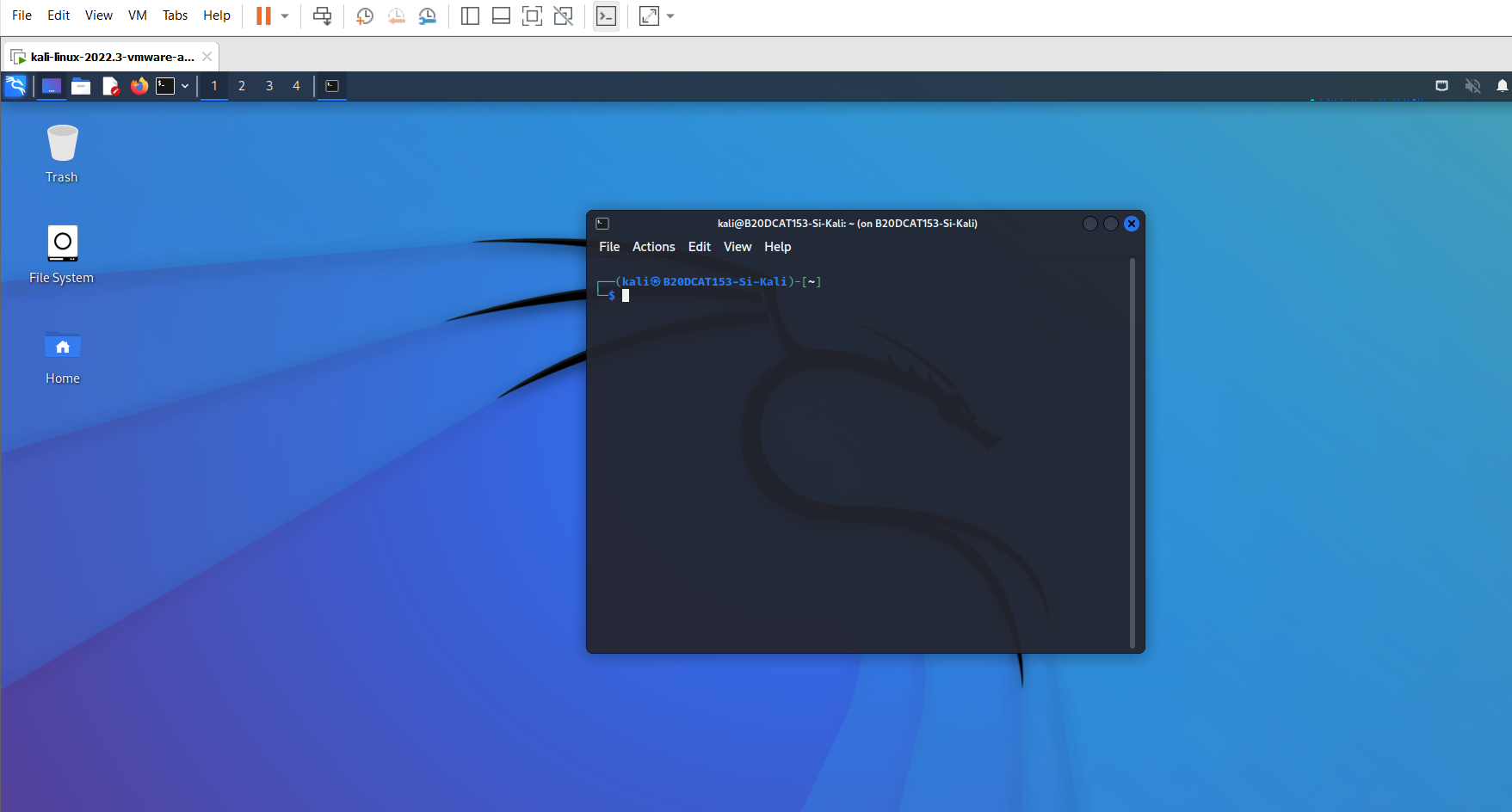
- Metasploitable là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại: <https://www.hackingarticles.in/comprehensive-guide-on-metasploitable>

* Lỗ hổng là lỗ hổng bảo mật CVE-2007-2447 trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25rc3 có thể cho phép thực thi mã từ xa. Chi tiết về lỗ hổng này có thể tìm tại: NVD - CVE-2007-2447 (nist.gov)

**III. Nội dung thực hành**

**1. Cài đặt các công cụ, nền tảng**

Cài đặt Kali Linux:



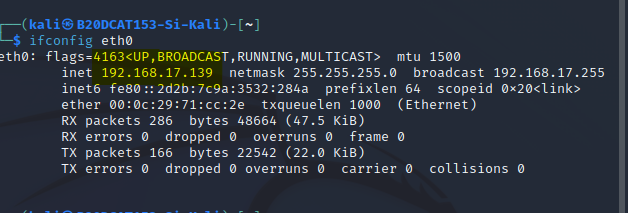
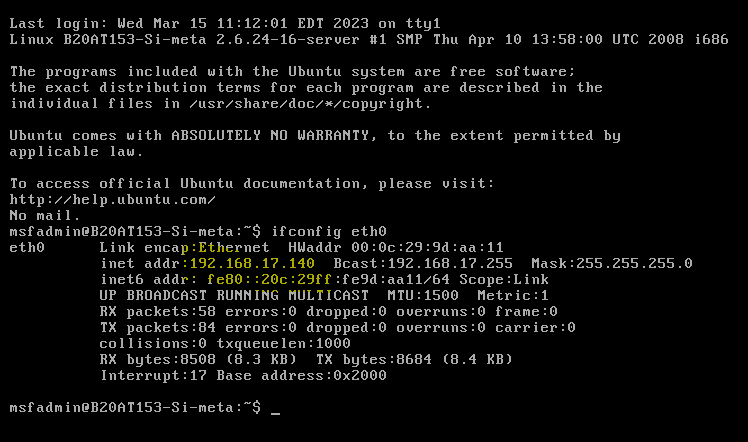
Tải và cài đặt Metasploitable2 làm máy victim:

Và tạo user mới là sidt153

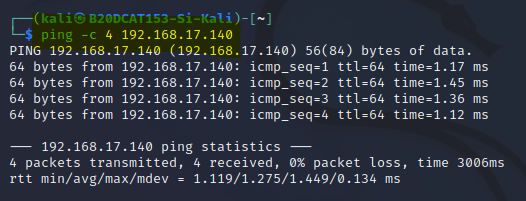


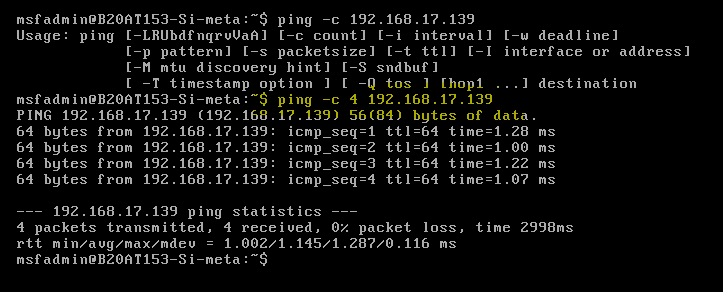
**2. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại:**

Tìm địa chỉ IP của máy victim, kali:



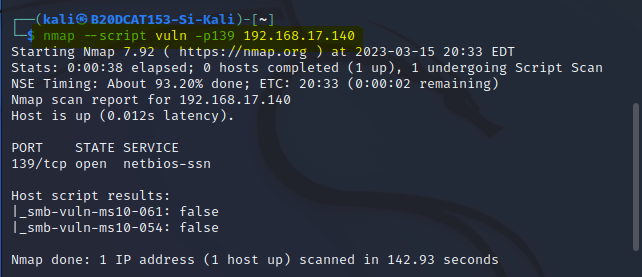
Kiểm tra kết nối mạng giữa các máy:



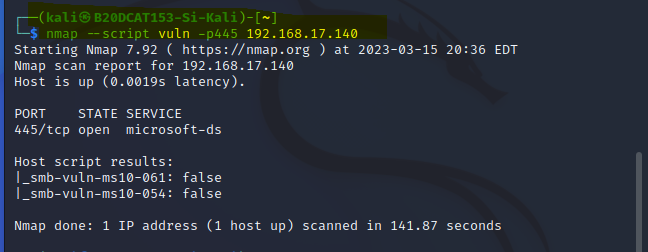


Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

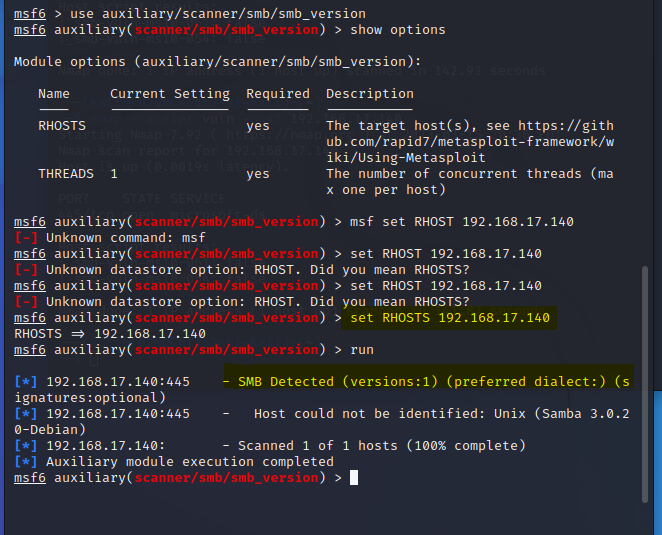
- Quét cổng dịch vụ netbios-ssn cổng 139:



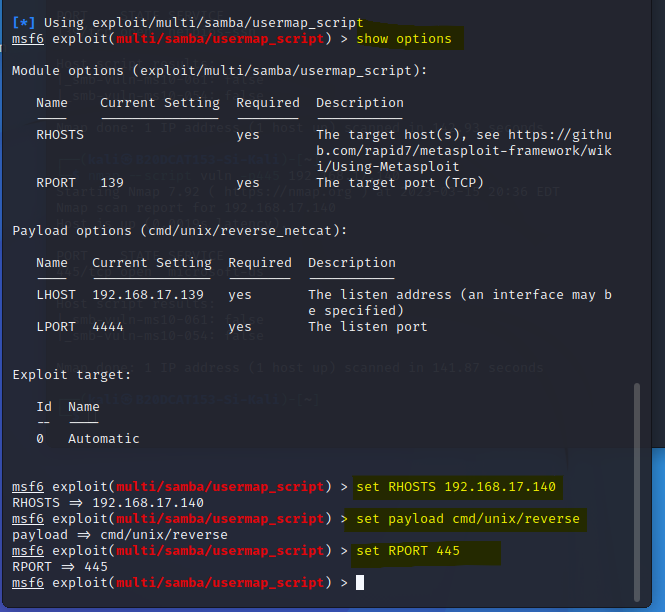
- Quét cổng dịch vụ microsoft-ds cổng 445

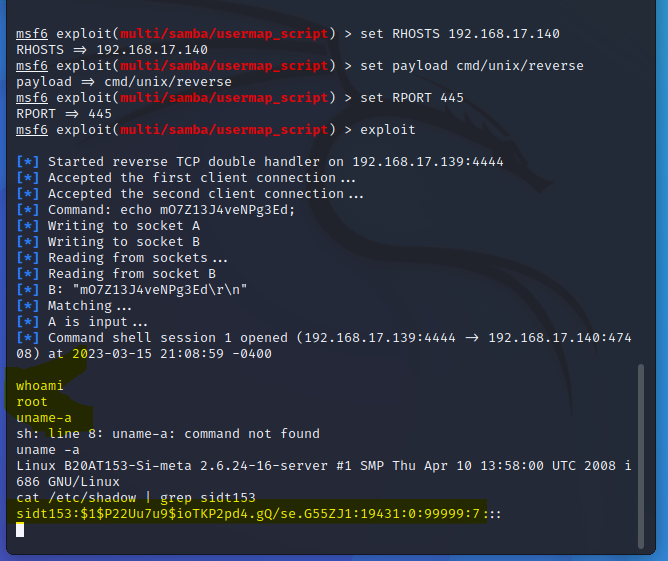


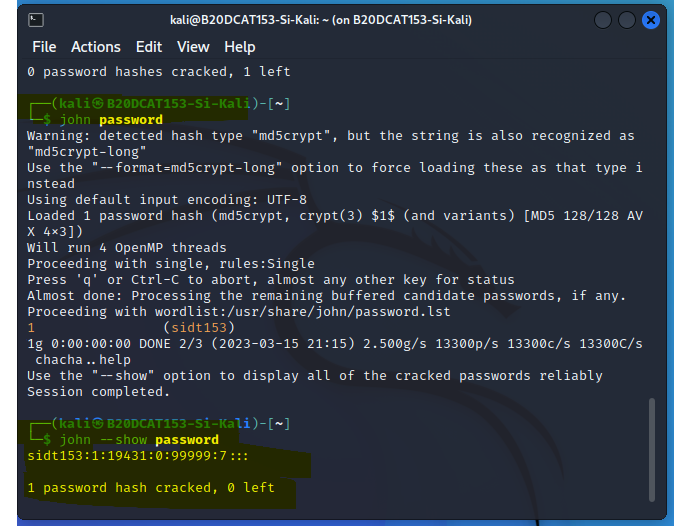
**3. Khai thác tìm phiên bản Samba đang hoạt động**



**4. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:**







Mật khẩu của sidt153 là 1