**LAB 1**

**Bài thực hành phục vụ cho nghiên cứu và học tập, không phục**

**vụ cho mục đích phá hoại và bất hợp pháp !**

**THIẾT LẬP MÔI TRƯỜNG THỰC HÀNH - TÌM HIỂU KALI LINUX - SỬ DỤNG MỘT**

**SỐ CÔNG CỤ KHAI THÁC CÁC LỖ HỔNG BẢO MẬT**

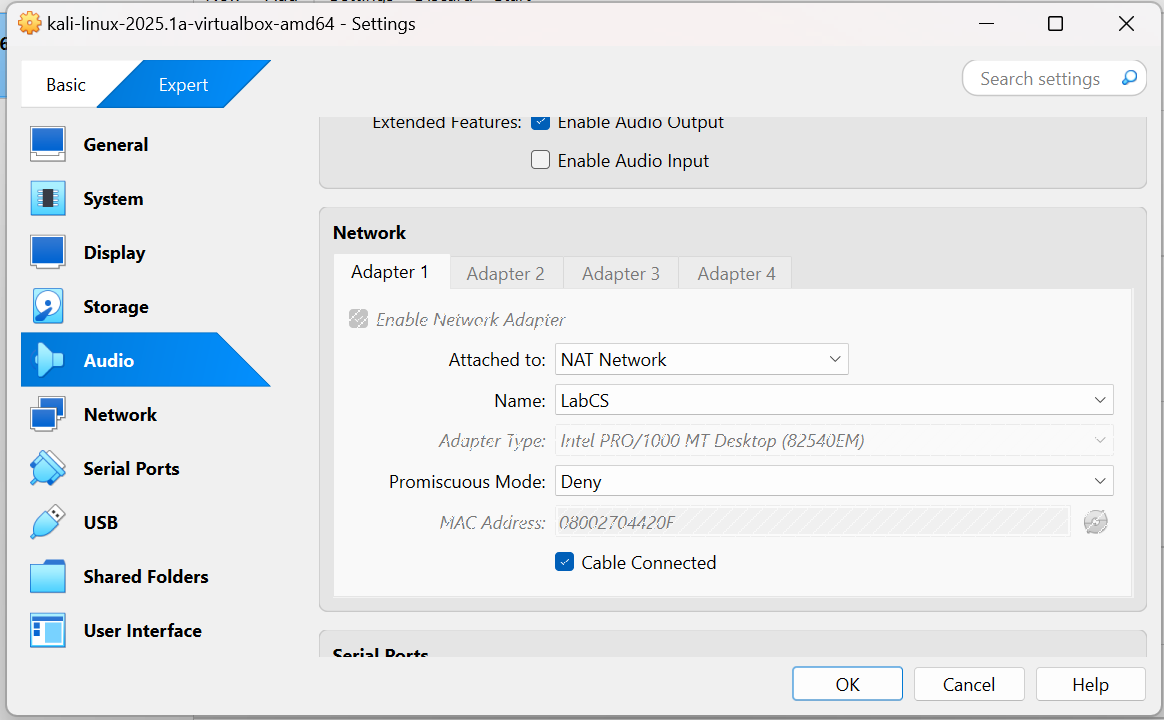
**Họ và tên :** Nguyễn Hoàng Khang

**Lớp :** 10\_ĐH\_CNPM3

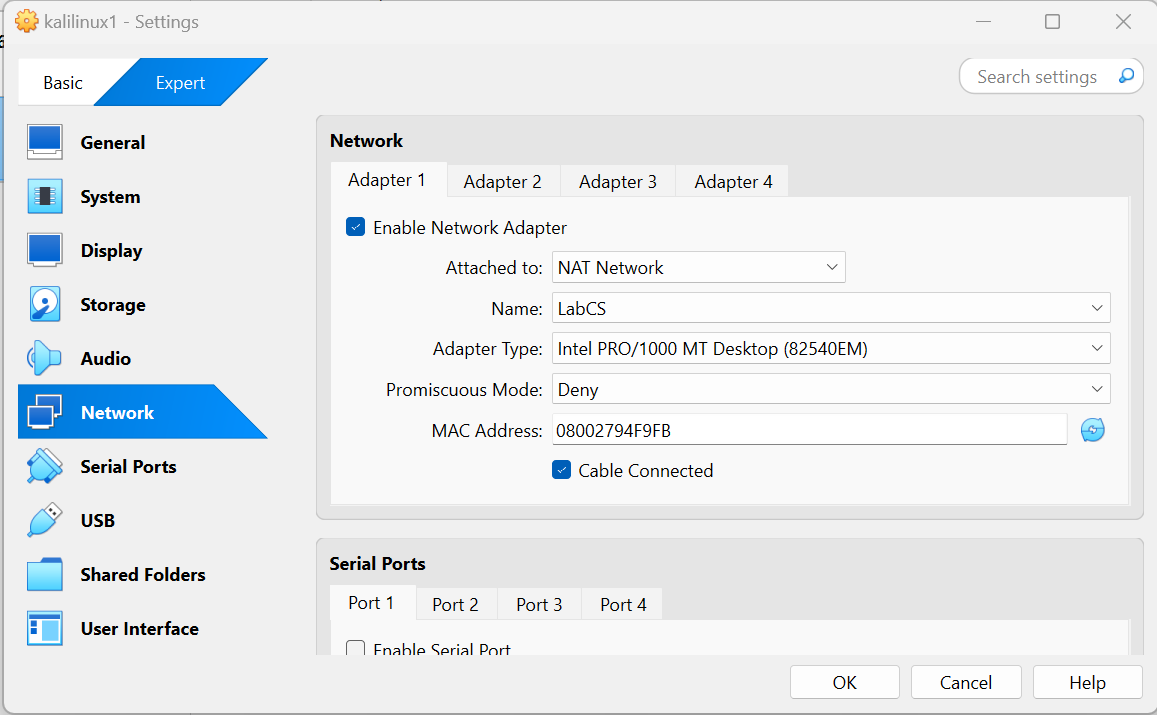
**Mssv:** 1050080287

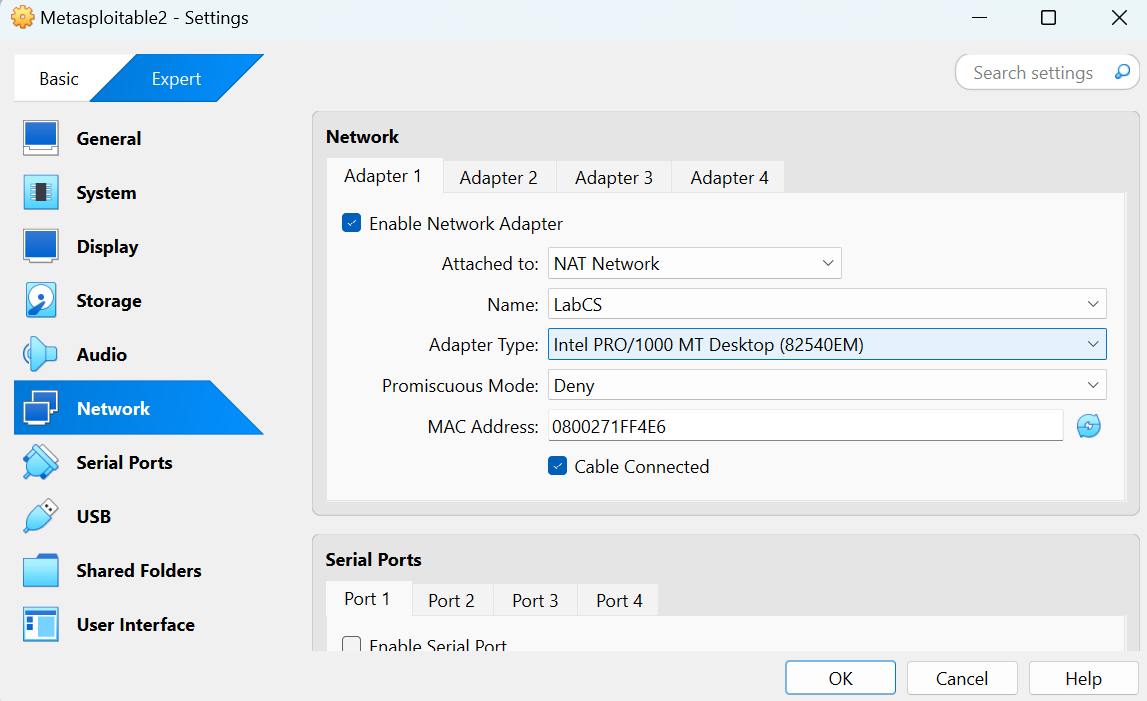
**Câu 1: Thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân**

1.1. Tạo 1 NAT network có tên “labcs” trên VirtualBox

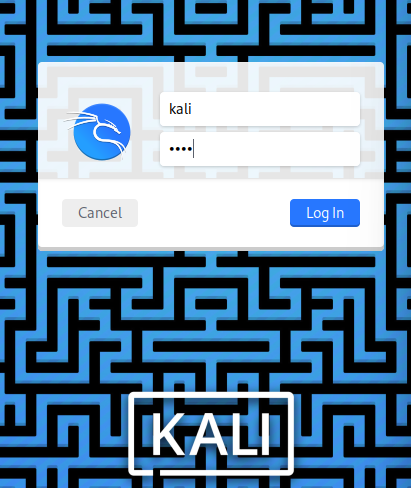


1.2. Tạo 2 máy ảo KaliLinux và Metasploitable 2, sử dụng các file máy ảo được cung cấp. Sau đó cấu hình mạng cho 2 máy ảo vào NAT network “labcs”





1.3. Khởi động máy ảo và đăng nhập vào KaliLinux sử dụng username/password là kali/kali (chụp hình minh hoạ)





**Câu 2: Sử dụng các công cụ trên KaliLinux**

**2.1. Truy cập vào địa chỉ https://tools.kali.org/tools-listing [3] tìm hiểu Nmap, trả lời các câu hỏi sau:**

+Chức năng chính của Nmap là gì?

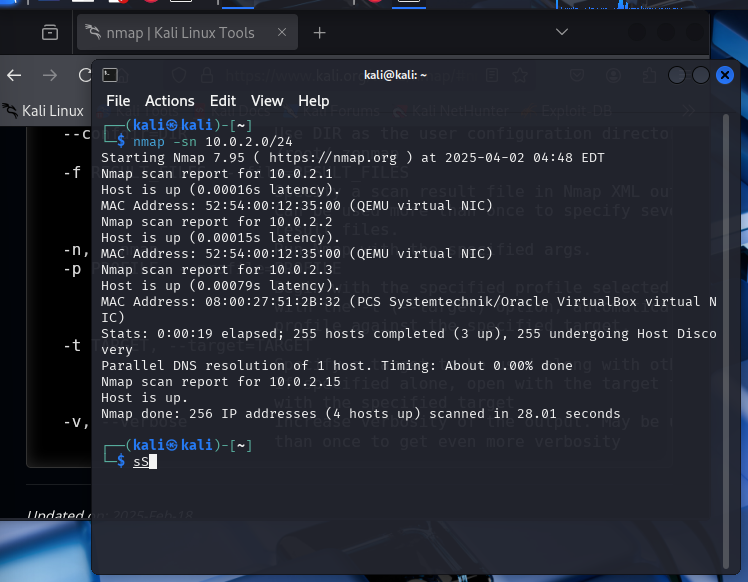
Trả lời: Nmap (“NetworkMapper”) là một tiện ích (giấy phép) mã nguồn mở và miễn phí để

khám phá mạng và kiểm tra bảo mật. Nhiều hệ thống và quản trị viên mạng cũng thấy nó hữu ích cho các tác vụ như kiểm kê mạng, quản lý lịch nâng cấp dịch vụ và theo dõi máy chủ lưu trữ hoặc thời gian hoạt động của dịch vụ.

+Liệt kê một số tham số trọng của Nmap.

Trả lời: Chúng ta có nhiều tham số trên nmap ví dụ như:

∙ -sn: ping tất cả host có trong nhánh mạng – tắt quét cổng.



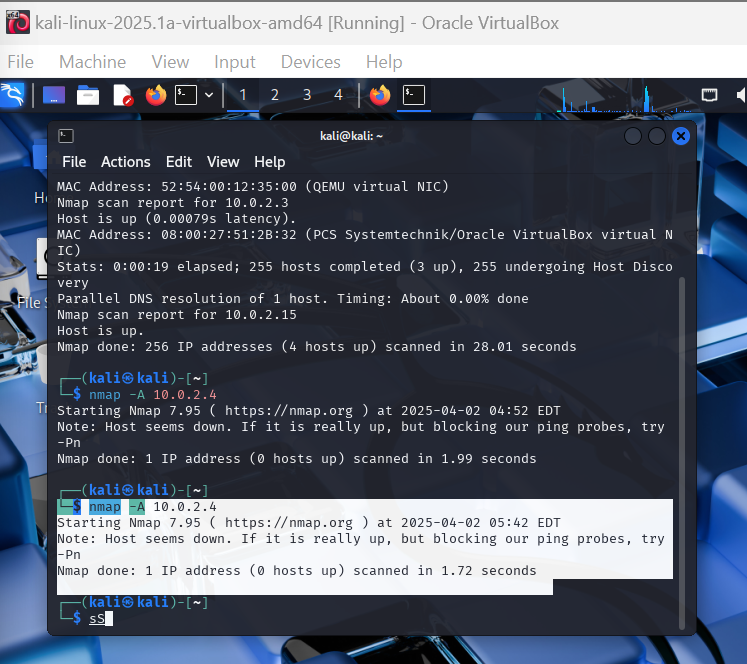
∙ -A: quét tất cả những thông tin trên máy mục tiêu.

∙ -6: Bật quét Ipv6.

∙ -V: In số phiên bản.

**2.2. Sử dụng Nmap để tìm tất cả thông tin về hệ điều hành, các dịch vụ được cài đặt trên máy ảo Metasploitable 2 (chụp hình minh hoạ).**

* Lệnh dùng nmap để tìm tất cả thông tin về hệ điều hành, các dịch vụ được cài đặt trên máy ảo Metasploitable 2: nmap –A 10.0.2.4. Thông báo:



**Lỗi rồi thầy ơi fix ko được ☺**