Lê Nguyễn Hà My

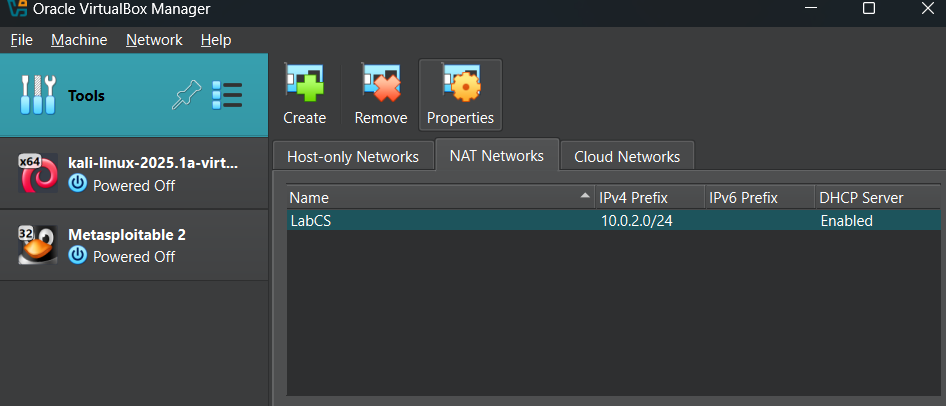
1050080185

LAB 1 TH

THIẾT LẬP MÔI TRƯỜNG THỰC HÀNH - TÌM HIỂU KALI LINUX - SỬ DỤNG MỘT SỐ CÔNG CỤ KHAI THÁC CÁC LỖ HỔNG BẢO MẬT

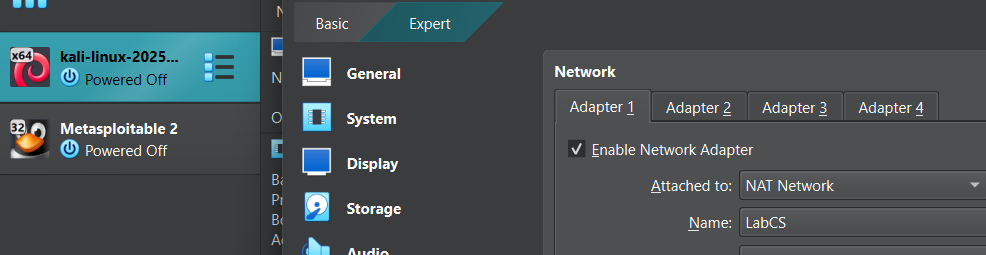
Câu 1: Thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân

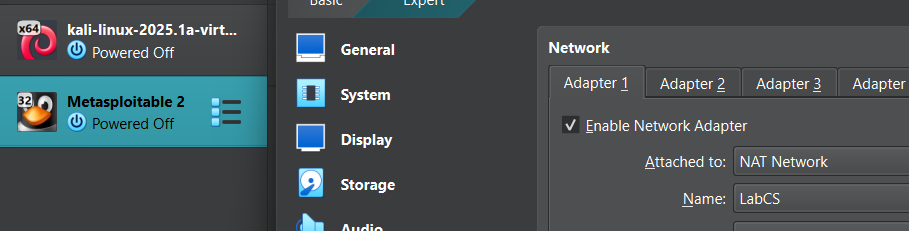
* 1. Tạo 1 NAT network có tên “labcs” trên VirtualBox



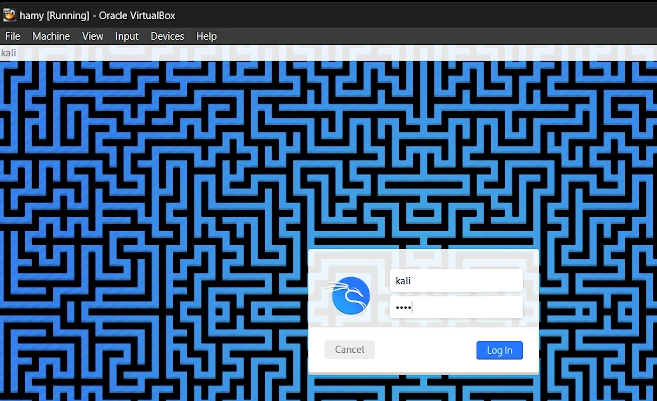
1.2 Tạo 2 máy ảo Kali Linux và Metasploitable 2, sử dụng các file máy ảo được cung cấp.

Sau đó cấu hình mạng cho 2 máy ảo vào NAT network “labcs”





1.3. Khởi động máy ảo và đăng nhập vào Kali Linux sử dụng username/password là kali/kali



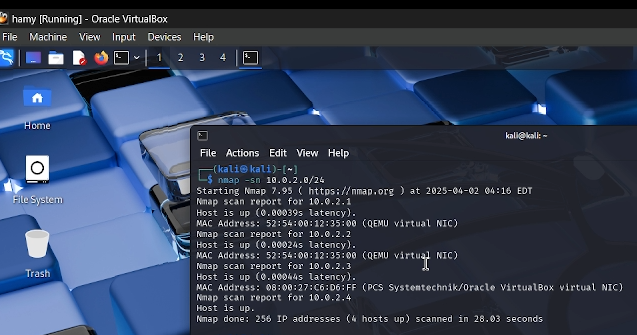
Câu 2: Sử dụng các công cụ trên Kali Linux

+Chức năng chính của Nmap là gì?

Nmap (**Network Mapper**) là một công cụ mã nguồn mở dùng để quét mạng và kiểm tra bảo mật. Các chức năng chính của Nmap gồm:  
✅ **Quét mạng**: Phát hiện các thiết bị đang hoạt động trong mạng.  
✅ **Xác định cổng mở**: Kiểm tra các cổng TCP/UDP đang mở trên hệ thống.  
✅ **Phát hiện dịch vụ (Service Detection)**: Xác định các dịch vụ đang chạy trên cổng.  
✅ **Xác định hệ điều hành (OS Detection)**: Nhận diện hệ điều hành của máy đích.  
✅ **Phát hiện lỗ hổng bảo mật**: Kiểm tra và phát hiện các lỗ hổng tiềm ẩn.

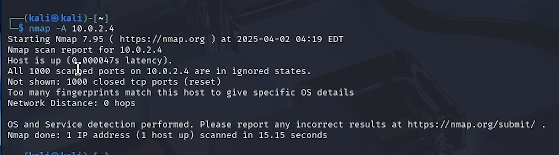
+Liệt kê một số tham số trọng của Nmap.

**-sS (SYN Scan)**: Quét nhanh bằng cách gửi gói SYN (Stealth Scan).  
🔸 **-sT (TCP Connect Scan)**: Quét cổng bằng cách thiết lập kết nối TCP đầy đủ.  
🔸 **-sU (UDP Scan)**: Quét các cổng UDP.  
🔸 **-p <cổng>**: Chỉ định cổng cần quét (ví dụ -p 80,443,8080).  
🔸 **-O**: Phát hiện hệ điều hành của máy đích.  
🔸 **-A**: Quét nâng cao (bao gồm phát hiện OS, dịch vụ, traceroute).  
🔸 **-T<0-5>**: Điều chỉnh tốc độ quét (T0 rất chậm, T5 rất nhanh).  
🔸 **-Pn**: Bỏ qua kiểm tra ping, quét ngay cả khi máy chủ không phản hồi ICMP.  
🔸 **-oN, -oX, -oG**: Xuất kết quả ra file (.txt, .xml, .grep).



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

- 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:



2.3. Tìm hiểu dịch vụ cài đặt trên cổng 21 của Metasploitable 2 có những lỗ hổng bảo mật gì?

Dịch vụ chạy trên cổng 21: vsftpd 2.3.4 (FTP Server)

📌 Lỗ hổng chính:

* Backdoor (CVE-2011-2523): Cho phép hacker mở shell root bằng cách đăng nhập với username chứa :).
* Khi khai thác thành công, máy chủ sẽ mở cổng 6200 cho phép thực thi lệnh từ xa.

📌 Cách khai thác:

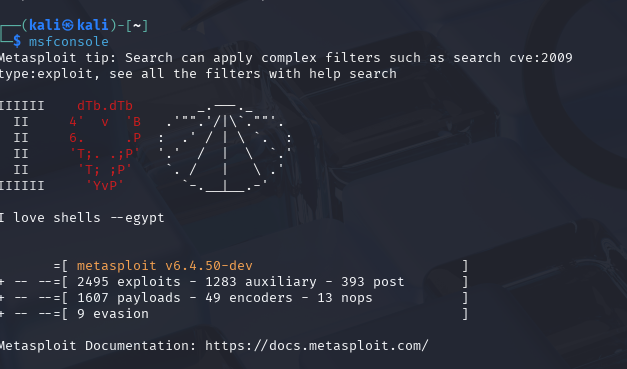
* Dùng Metasploit với module exploit/unix/ftp/vsftpd\_234\_backdoor để chiếm quyền điều khiển.

📌 Cách khắc phục:

* Nâng cấp FTP server lên phiên bản mới hơn.
* Vô hiệu hóa FTP, sử dụng SFTP hoặc SCP thay thế.
* Giới hạn quyền truy cập, chỉ cho phép IP đáng tin cậy.

2.4. Sử dụng công cụ Metasploit khai thác lỗ hổng trên và chiếm root shell của máy ảo Metasploitable 2 (chụp hình minh hoạ).

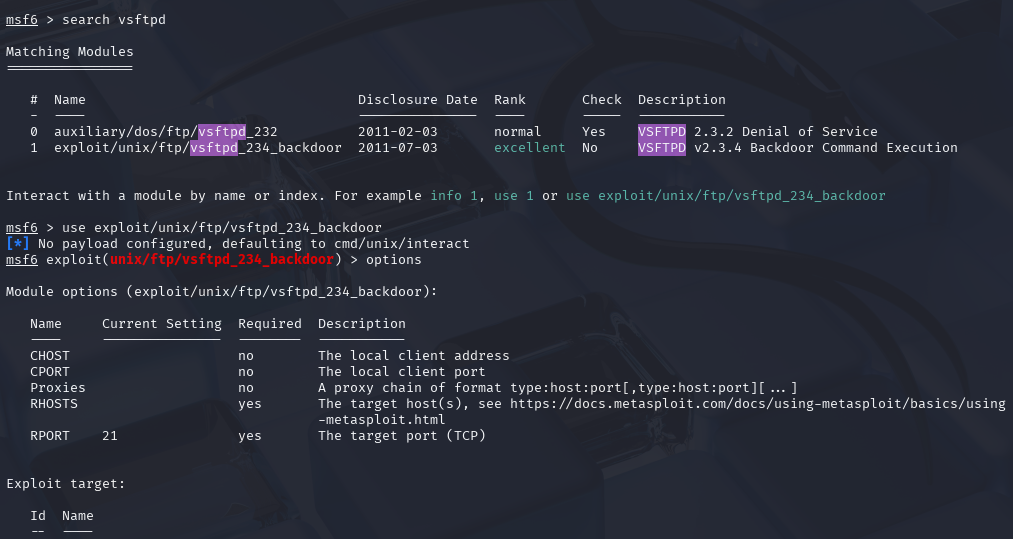
- Sử dụng lệnh msfconsole để chạy lên mã nhận lệnh của công cụ Metasploit:



-Lệnh tìm mô đun nào đó có sẵn trên công cụ này để khai thác lỗ hổng bảo mật trên phần mềm vfstpd ta có thể dùng lệnh: search vsftpd

- Sau đó ta gõ lệnh use kèm theo tên công cụ để sử dụng hoặc là số thứ tự của nó.

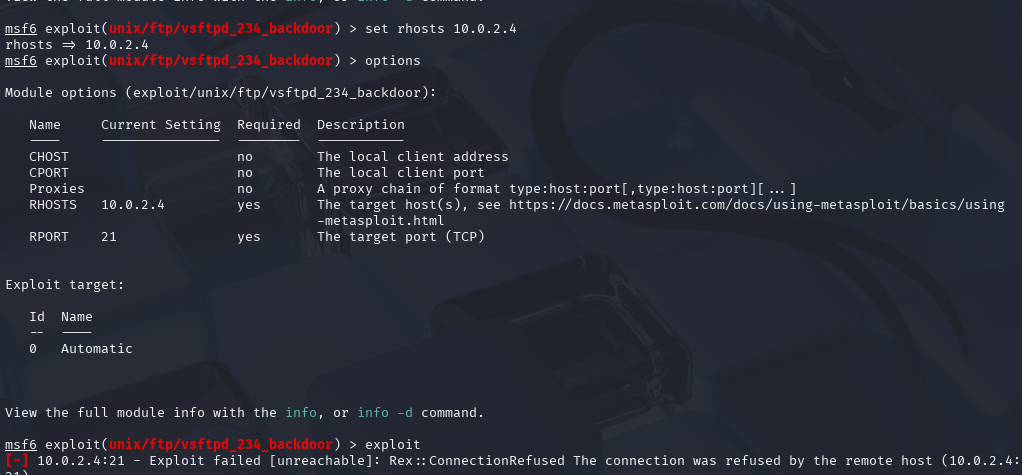
- Tiếp theo ta gõ lệnh options để xem các tham số cần thiết.



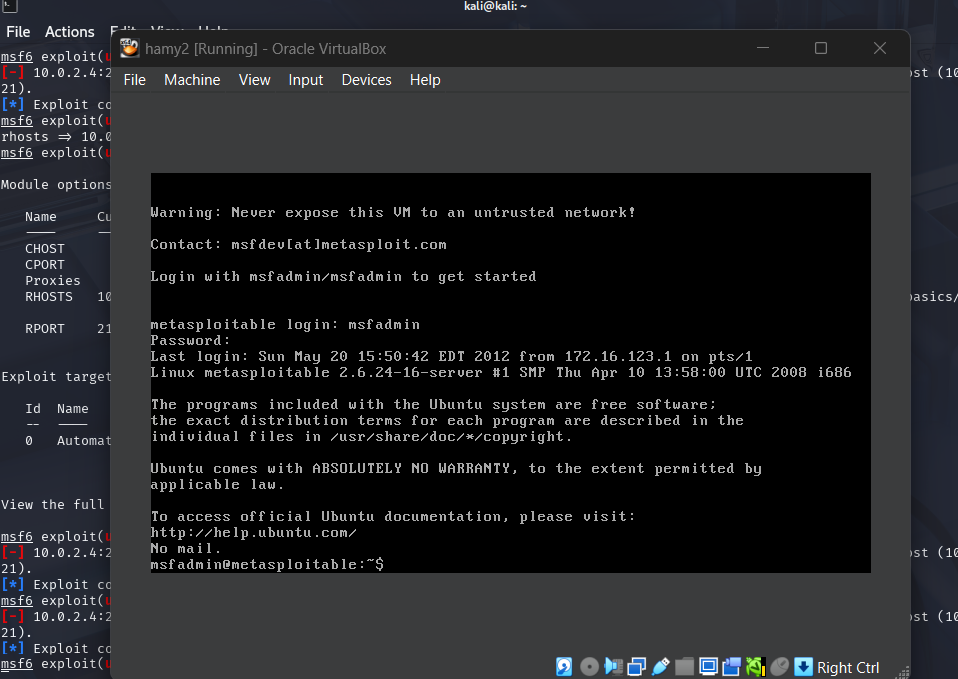
-Ở đây do dịch vụ mục tiêu ở cổng mặc nhiên 21 đã được tạo sẵn, ta chỉ cần nhập vào địa chỉ của máy mục tiêu ta gõ lệnh: set rhost 10.0.2.4.

- Ta gõ lệnh options để xem lại các tham số.

- Tiếp theo ta gõ lệnh exploit để khai thác.

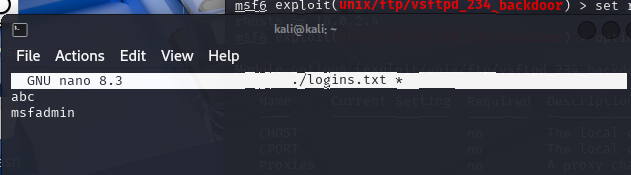


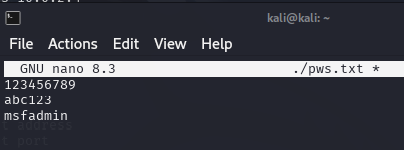
-Ta đã chiếm được shell của máy mục tiêu và thử gõ các lệnh để thực hiện trên máy mục tiêu như các lệnh: whoami, pwd, touch abc.txt



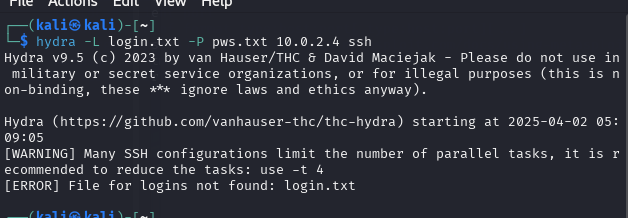
2.5. Sử dụng công cụ Hydra để tấn công dò mật khẩu dịch vụ SSH trên máy ảo Metasploitable2

- Đầu tiên ta tạo hai file là logins.txt và file pws.txt sau đó nhập các mật tên đăng nhập và mật khẩu có thể có của dịch vụ ssh trên máy ảo Metasploitable 2 với lệnh nano:





-Tiếp theo ta dùng lệnh hydra –L logins.txt –P pws.txt 10.0.2.4 ssh để tấn công dò mậtkhẩu dịch vụ SSH trên máy ảo Metasploitable 2 và ta tìm được login:msfadmin và password:msfadmin:



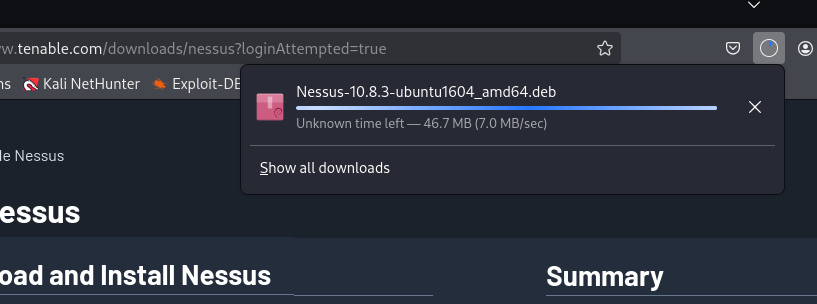
- Chúng ta có thể nối kết vào bằng các sử dụng ssh: ssh msfadmin@10.0.2.4 và gõ

password msfadmin để nối kết vào máy mục tiêu:

Câu 3: Sử dụng Nessus để tìm lỗ hổng bảo mật

3.1. Tải và cài đặt công cụ Nessus (https://www.tenable.com/downloads/nessus) vào máy ảo Kali

- Ta tải về công cụ cụ Nessus (https://www.tenable.com/downloads/nessus) vào máy ảo Kali



3.2. Khởi động và truy cập vào dịch vụ Nessus (https://localhost:8834), đăng ký activation code. Sau đăng ký thành công, thực viện quét tìm các lỗ hổng bảo mật trên Metasploitable 2.

Có bao nhiêu lỗ hổng bảo mật (low/medium/high) được tìm thấy (chụp hình minh hoạ)?