HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 3.3
RÀ QUÉT VÀ KHAI THÁC LỖ HỔNG

Sinh viên thực hiện: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SIEM	Security Information and Event Management	Giải pháp giám sát, phát hiện và phản ứng nhanh với mối đe dọa.
DNS	Domain Name System	Giao thức tên miền
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
IIS	Internet Information Services	Dịch cụ Web Server chính của Microsoft
WAS	Windows Process Activation Service	Dịch vụ hỗ trợ cho IIS

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. Mục đích

- Hiểu được các mối đe dọa và lỗ hổng
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ hổng như: nmap/ zenmap, Nessus, Metasploit framework
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/ zenmap, Nessus, Metasploit framework.

II. Tìm hiểu lý thuyết

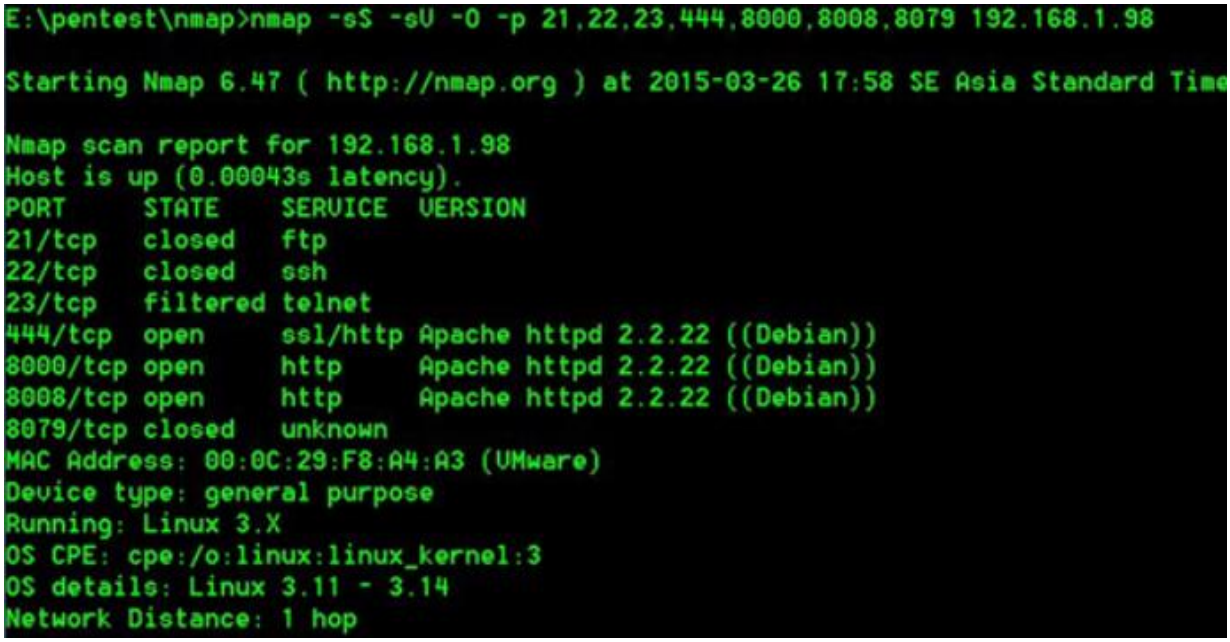
1. Nmap

Nmap là một ứng dụng đa nền tảng ban đầu chạy trên hệ điều hành Linux và đã được phát triển trên các hệ điều hành khác như Windows và Linux. Nmap là công cụ quét mạng mạnh mẽ và dùng để phát hiện ra lỗ hổng trong mạng, port, từ đó giúp IT có thể khắc phục được sự cố mạng nhanh hơn.

Cách thức hoạt động: Nmap sử dụng các IP trên các gói tin theo những cách đặc biết khác nhau để có thể xác định các host trên một hệ thống mạng để rồi từ đó xác định xem những services đang chạy trên hệ thống đó, hệ điều hành đang chạy, bộ lọc các gói tin cũng như tường lửa đang sử dụng gì.

Tính năng của nmap:

- Phát hiện lỗ hổng bảo mật
- Khai thác lỗ hổng bảo mật
- Phát hiện ra backdoor
- Quét mạng network
- Quét các máy chủ và các cổng trên máy chủ trên hệ thống
- Xác định hệ điều hành, service, firewall đang sử dụng.
- Cung cấp thông tin về loại thiết bị, tên DNS, địa chỉ MAC
- Thực thi các đoạn script NSE hoặc Lua với các đối tượng được kiểm thử



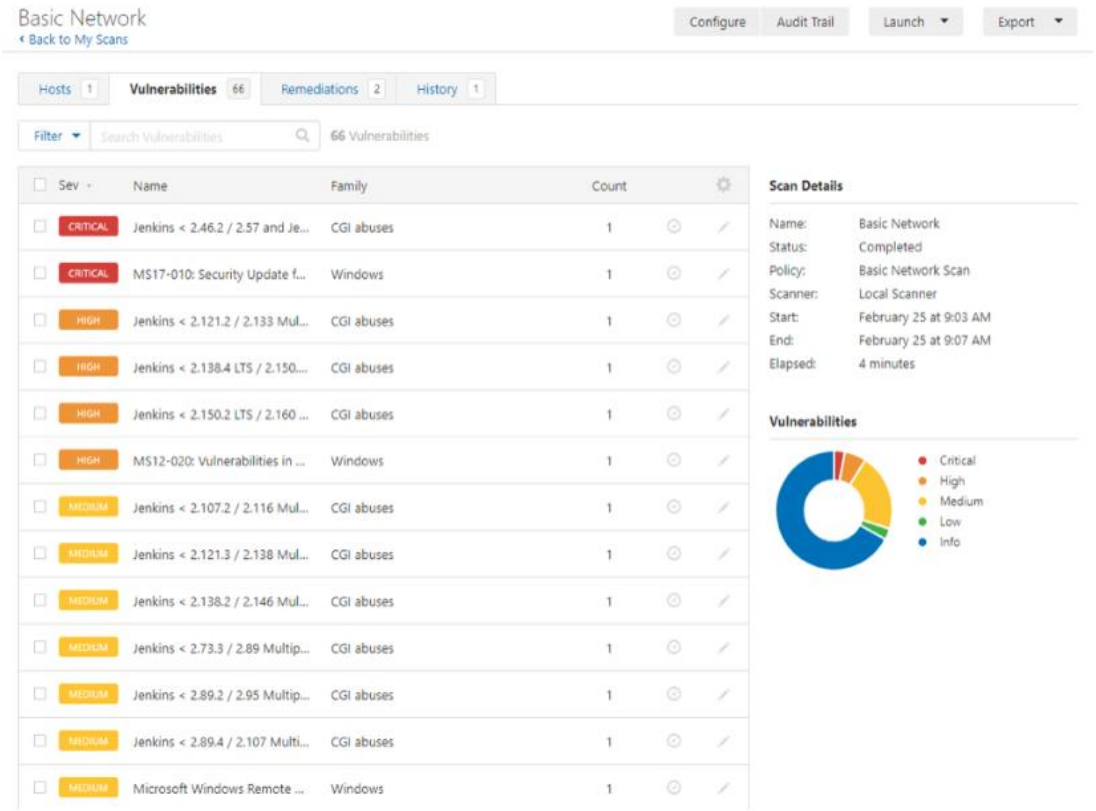
Hình ảnh 1: Cách thức hoạt động của Nmap

2. Nessus

Nessus là công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại.

Nessus cho phép quét các loại lỗ hổng:

- Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống
- Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,..)
- Mật khẩu mặc định, một vài mật khẩu thường được sử dụng và mật khẩu trống trên các tài khoản hệ thống.
- Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển.
- Tấn công từ chối dịch vụ bằng gói tin độc hại
- Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS)



Hình ảnh 2 : Giao diện của Nessus.

3. Metasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service.

Tính năng của Metasploit:

- Quét cổng để xác định các dịch vụ đang hoạt động trên server.
- Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.
- Thử nghiệm khai thác các lỗ hổng đã được xác định.

Hình ảnh 3: Cách thức hoạt động của Metasploit.

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

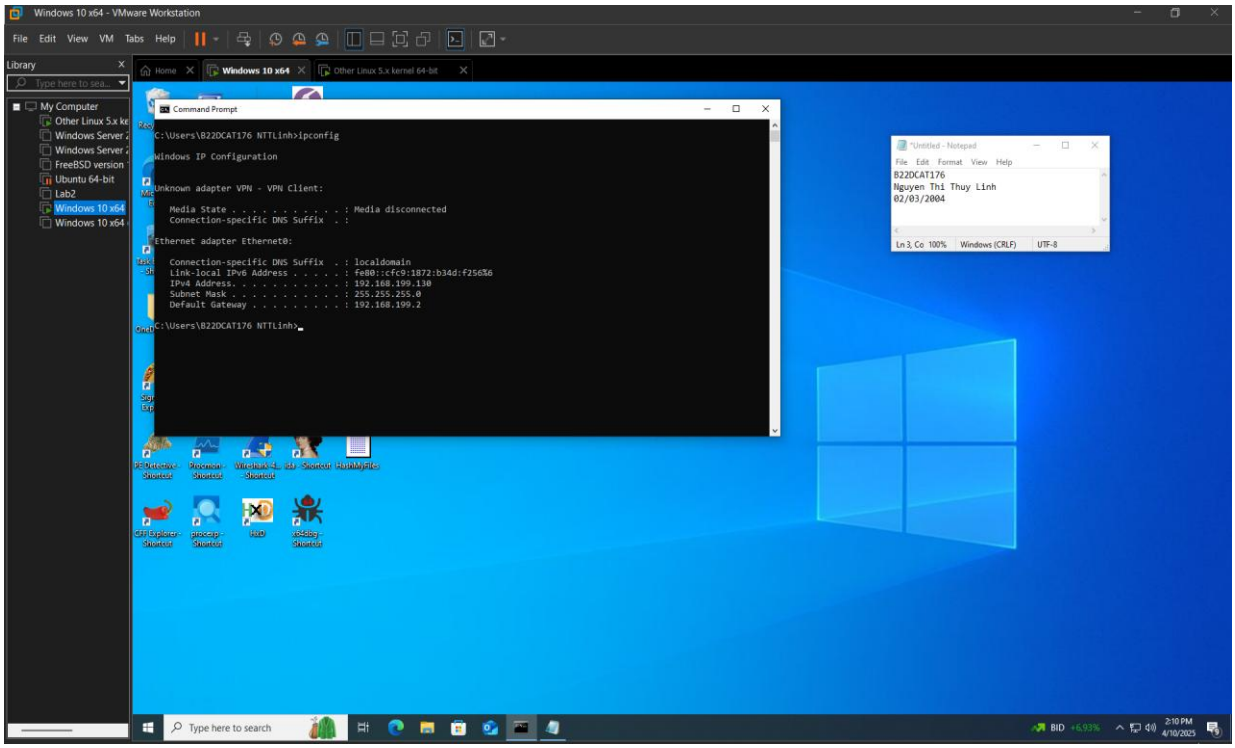
I. Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa
- Cài đặt các công cụ nmap/zenmap, Nessus, Metasploit framework

II. Các bước thực hiện

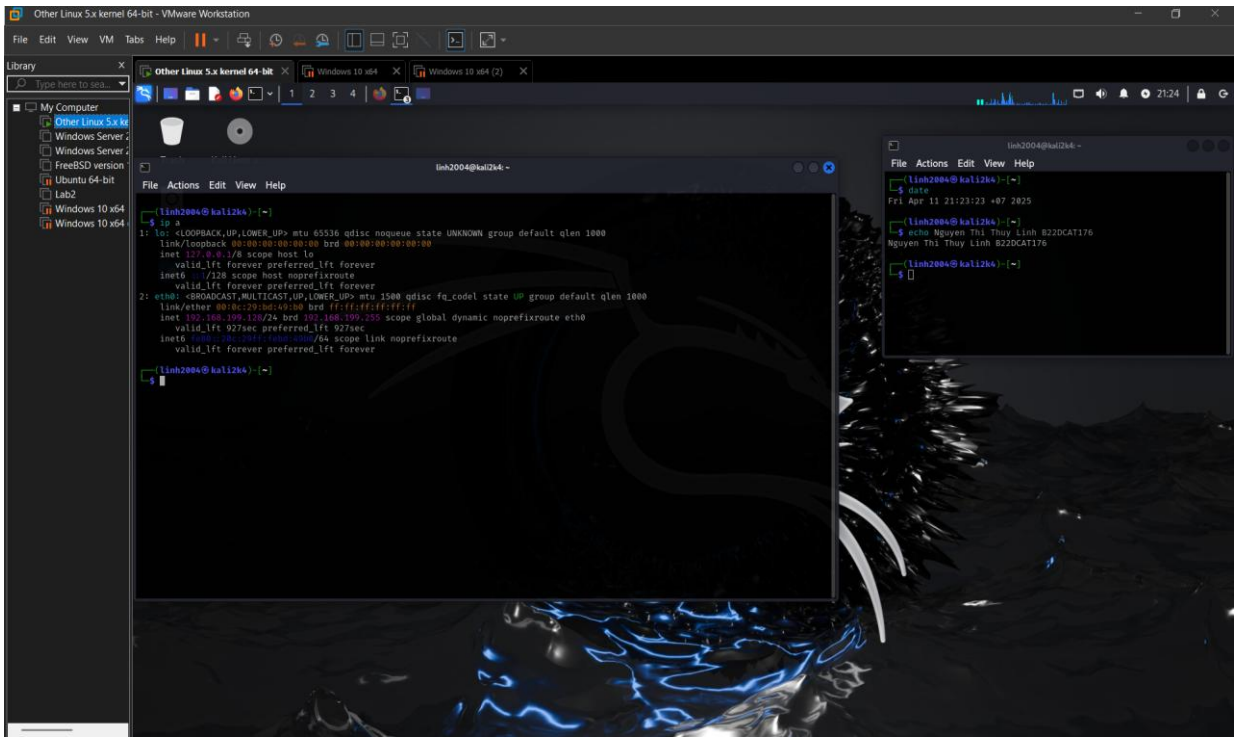
2.1. Sử dụng nmap/zenmap để quét các cổng dịch vụ

IP náy Windows:



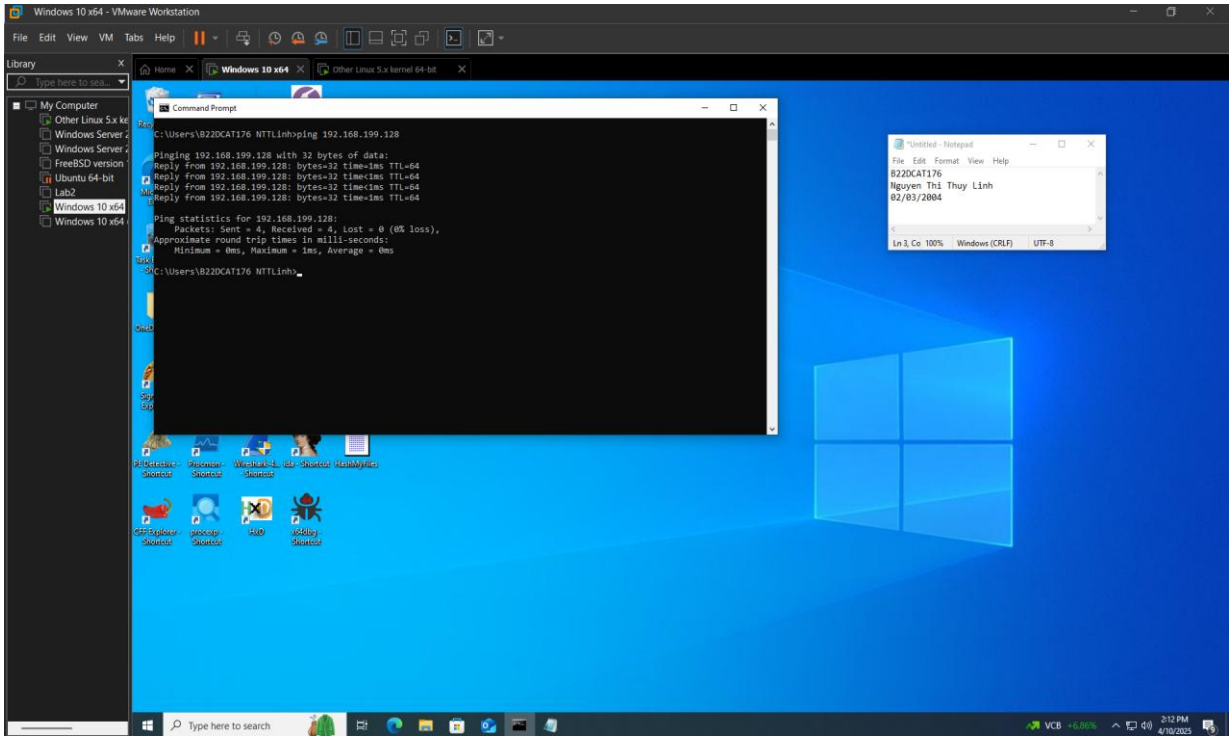
Hình ảnh 4: IP của máy Windows

IP máy Kali:

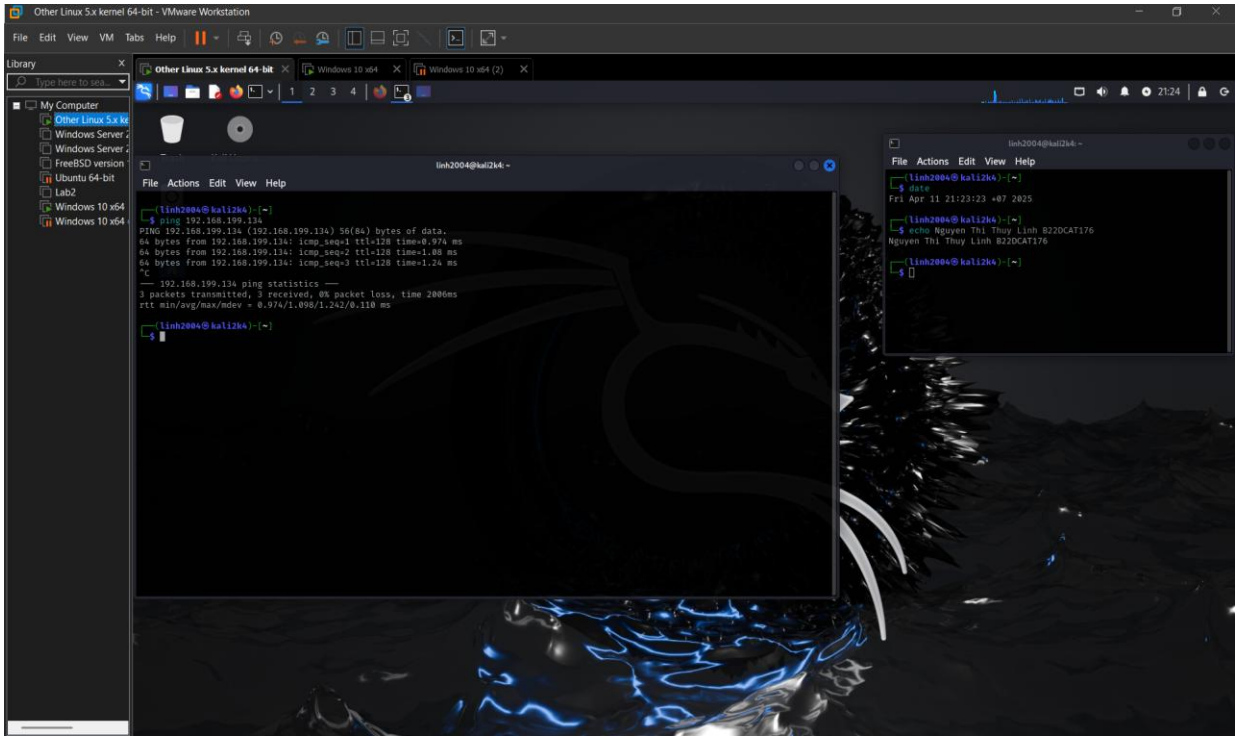


Hình ảnh 5: IP máy Kali.

Thực hiện ping giữa 2 máy:



Hình ảnh 6: Ping từ máy Windows.

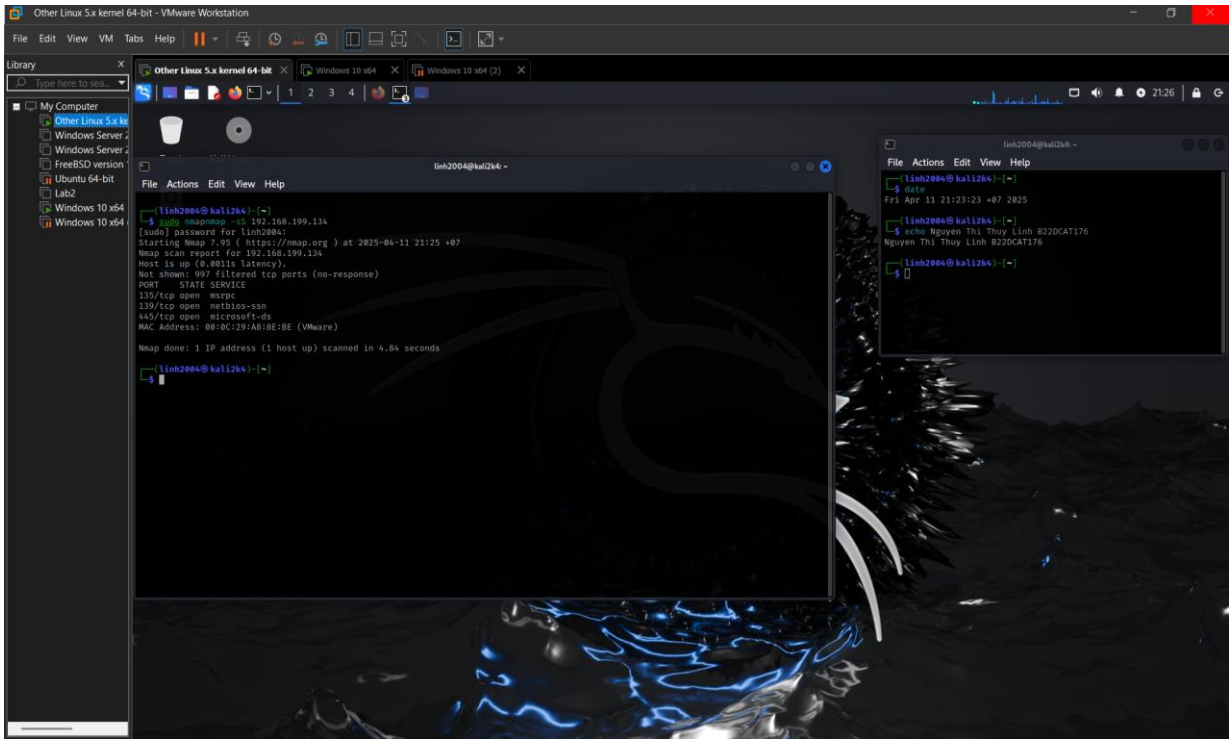


Hình ảnh 7: Ping IP từ máy Kali Linxux.

2.2. Sử dụng nmap/ zenmap để quét các cổng dịch vụ giao thức trên Windows 7 (thay đổi máy nhưng vẫn giữ nguyên IP)

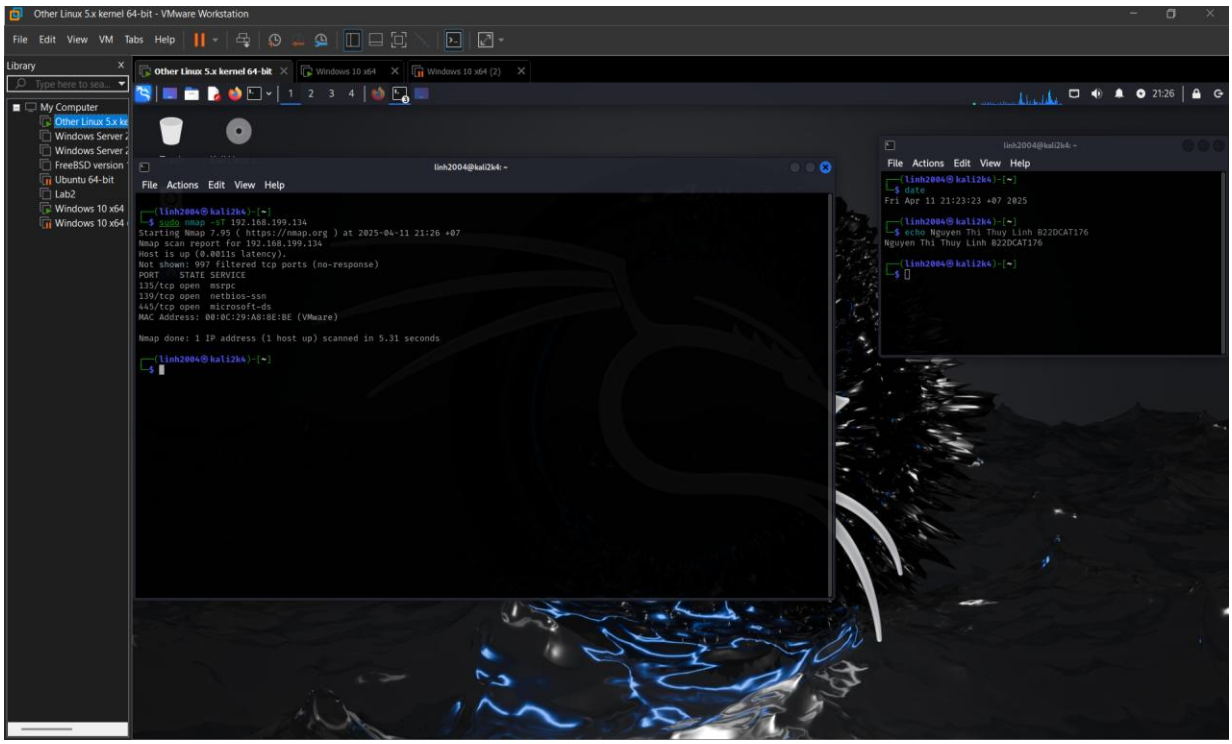
-*Dịch vụ TCP SYN scan*: nmap gửi một gói tin tới port mục tiêu của Windows Server. Nếu nhận được ACK_SYN thì port đó đang ở trạng thái open,nmap sẽ gửi gói tin RST

để đóng kết nối thay vì gửi ACK để hoàn tất quá trình bắt tay 3 bước (vì thế kỹ thuật này được gọi là half open scan). Nếu nhận được RST thì port đó ở trạng thái close. Nếu sau 1 lần gửi mà không nhận được trả lời hoặc nhận được ICMP type 3 thì port ở trạng thái đã bị firewall chặn.



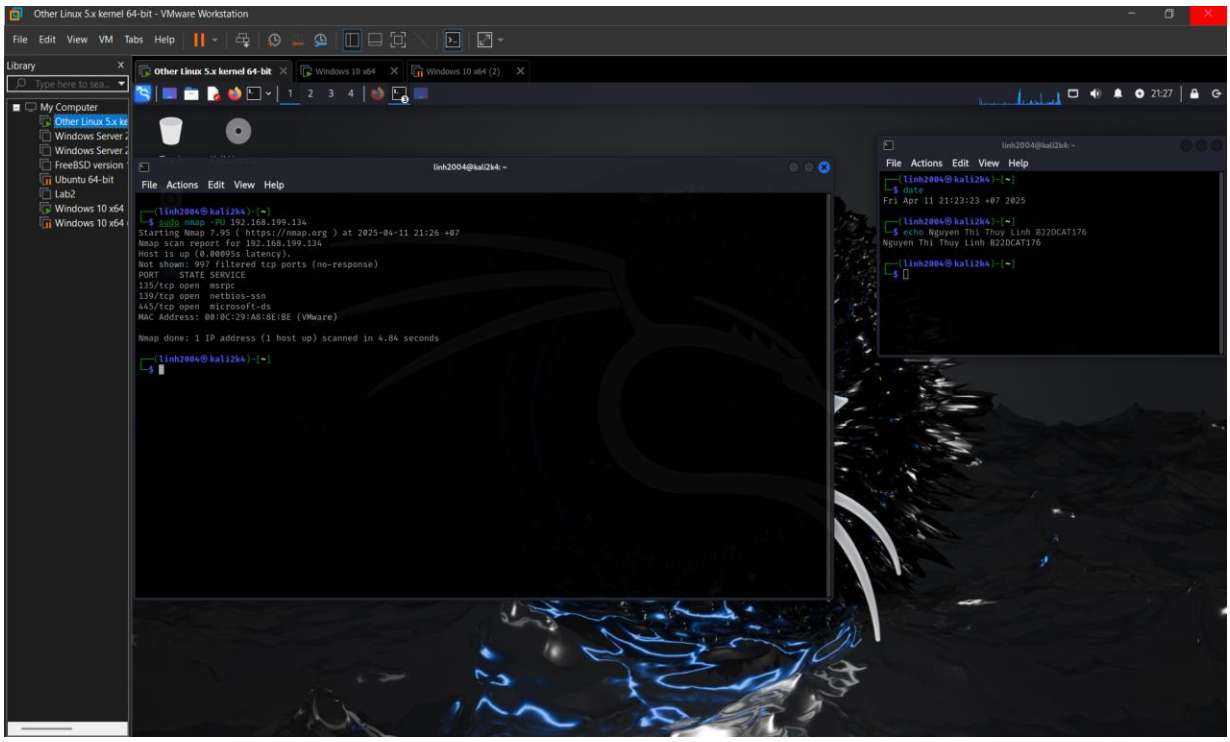
Hình ảnh 8: Quét cổng bằng TCP SYN.

- *Dịch vụ TCP connect scan*: Kỹ thuật này cho kết quả tương đương nhưu TCP SYN scan, nếu nhận được ACK_SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước. TCP connect scan được dùng khi user không có quyền truy cập raw packet để thực hiện SYN scan. TCP connect scan sử dụng TCP stack của hệ điều hành để tạo ra 1 kết nối bình thường với mục tiêu, do thực hiện 1 kết nối đầy đủ nên kỹ thuật này dễ bị phát hiện bởi hệ thống log của mục tiêu do đó SYN scan thường được sử dụng nhiều hơn để tránh bị phát hiện.



Hình ảnh 9: Quét cổng bằng TCP Connect Scan.

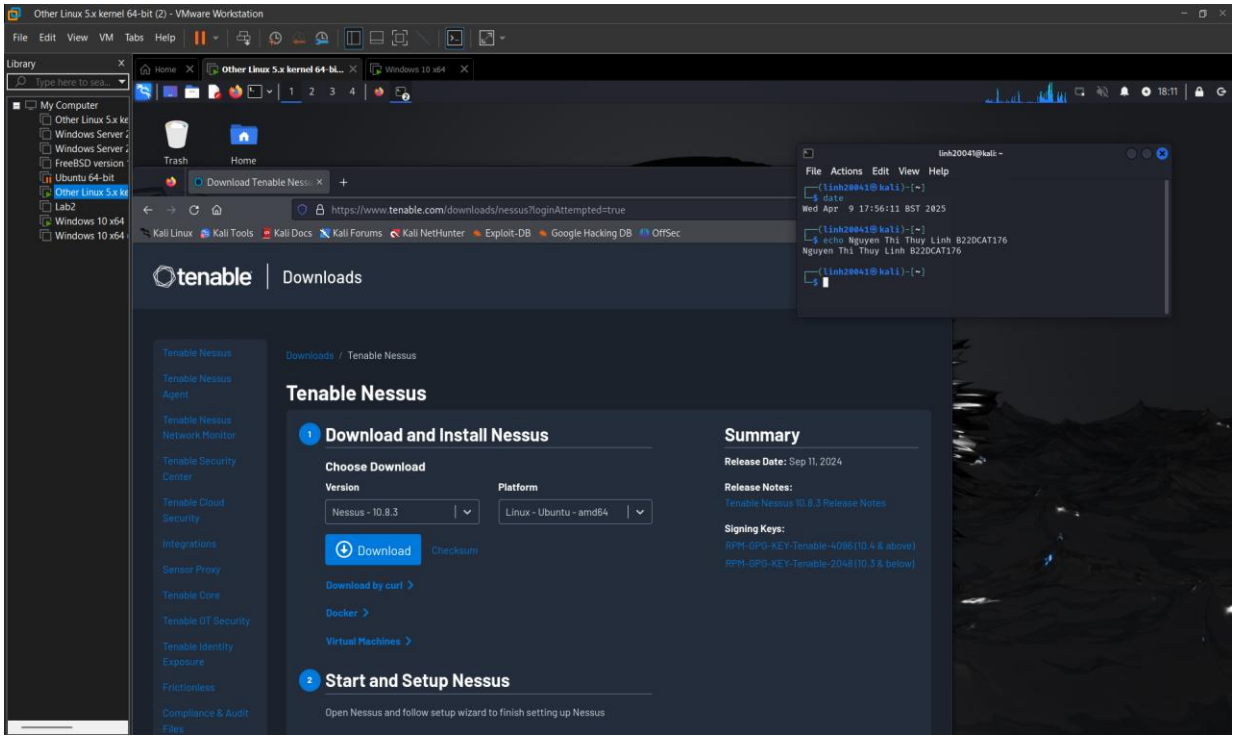
- *Dịch vụ UDP scan*: nmap sử dụng gói tin UDP tới 1 port của mục tiêu nếu nhận được gói tin *ICMP port unreachable error* (type 3, code 3) thì port đó ở trạng thái close. Nếu nahanj được *ICMP unreachable error* (type 3, codes 1,2,9,10,6 hoặc 13) thì port đó ở trạng thái filtered. Nếu không nhận được gì thì port ở trạng thái open hoặc filtered. Nếu nhận được gói tin UDP thì poet đó ở trạng thái open.



Hình ảnh 10: Quét cổng bằng UDP Scan.

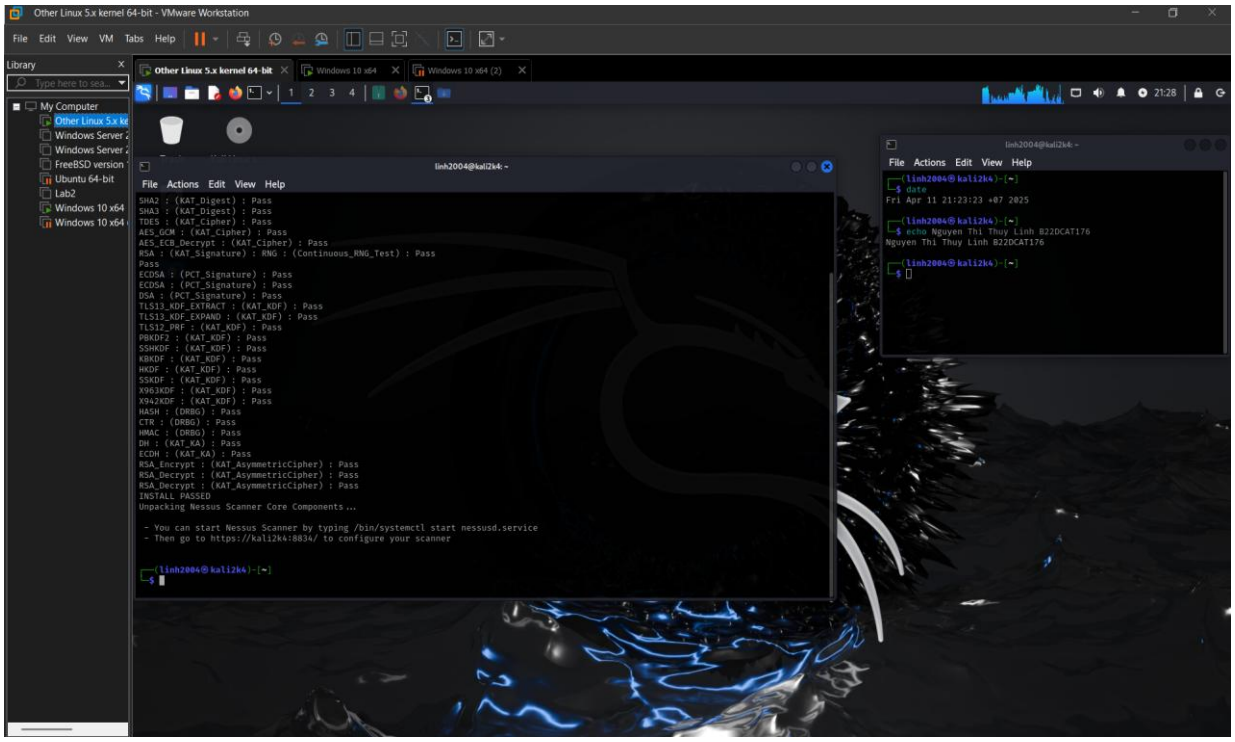
2.3. Sử dụng Nessus để quét các lỗ hổng trên máy Windows 7

Tiến hành download Nessus trên Kali.



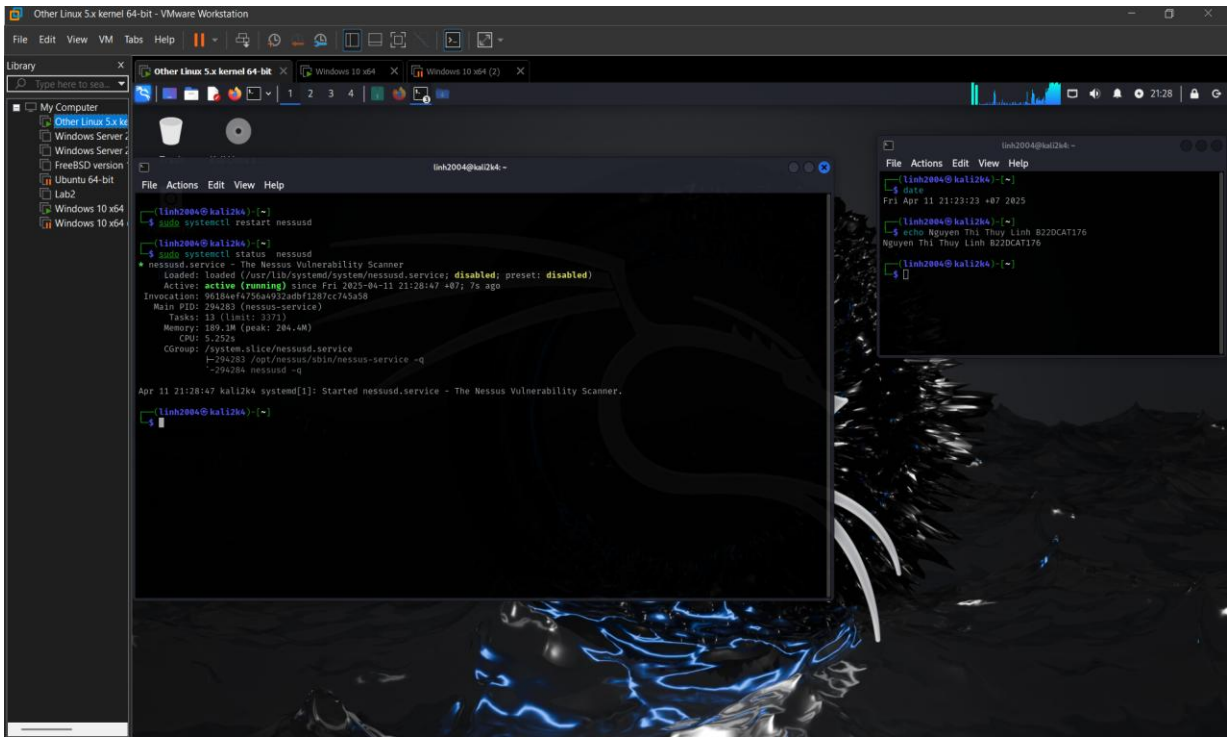
Hình ảnh 11: Download

Cấu hình Nessus:



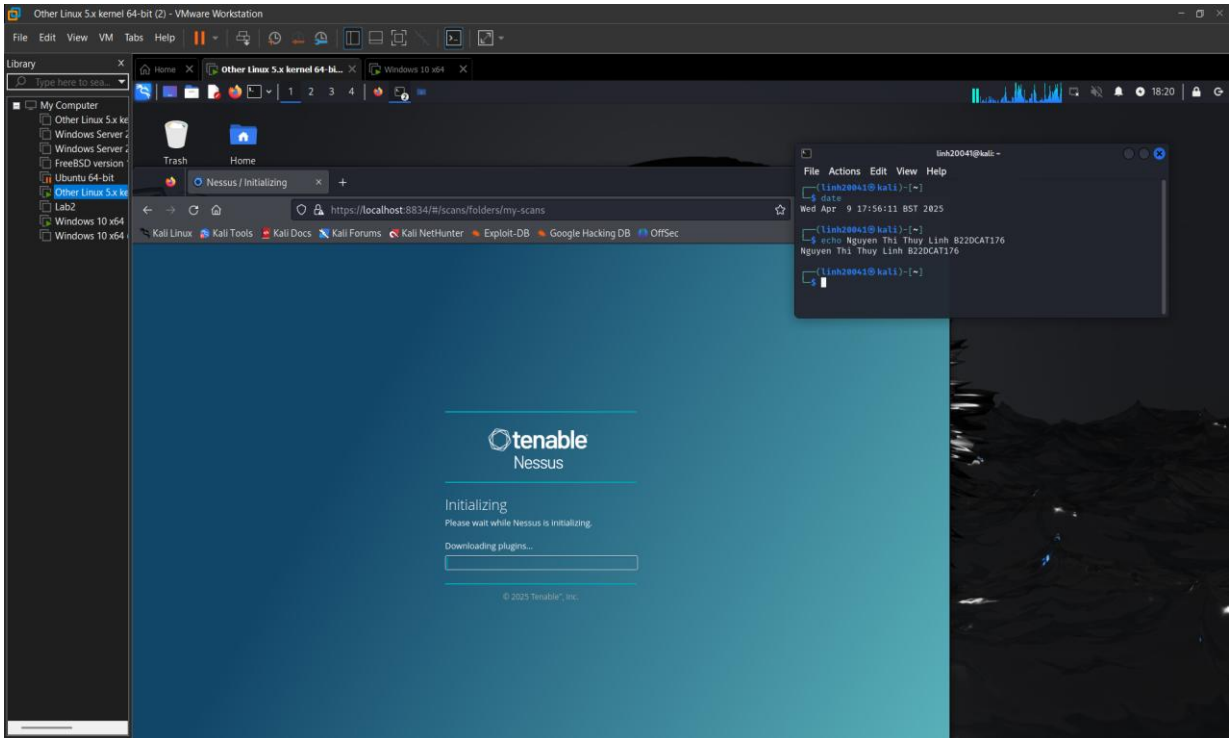
Hình ảnh 12: Cài đặt Nessus.

-Khởi động dịch vụ Nessus.



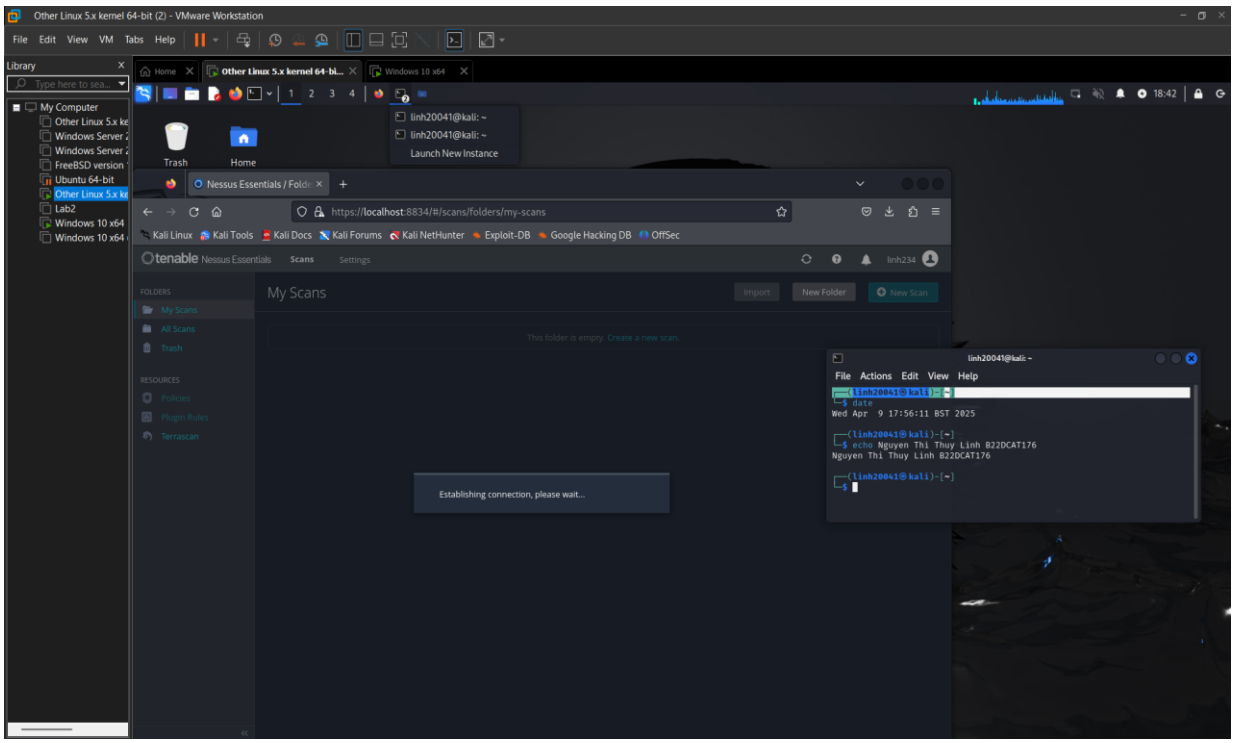
Hình ảnh 13: Khởi động Nessus.

Tạo tài khoản Nessus.



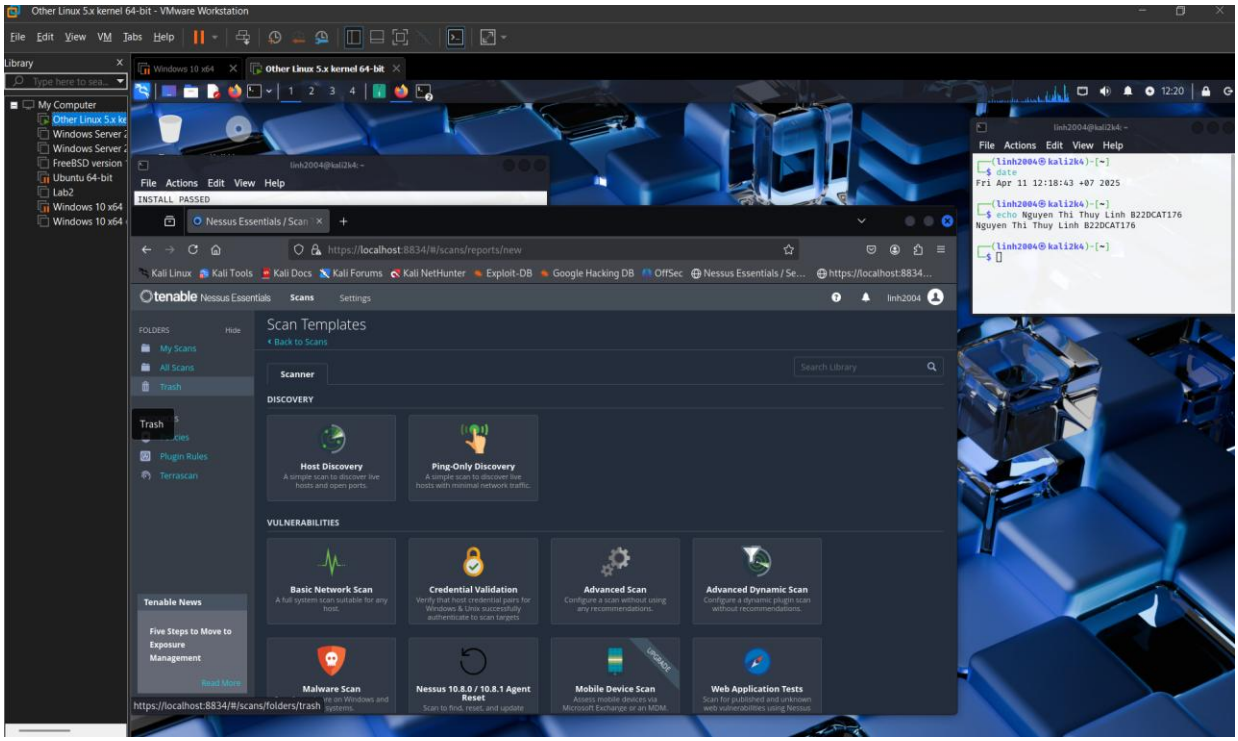
Hình ảnh 14: Tạo tài khoản Nessus.

-Tiến hành đăng nhập Nessus.



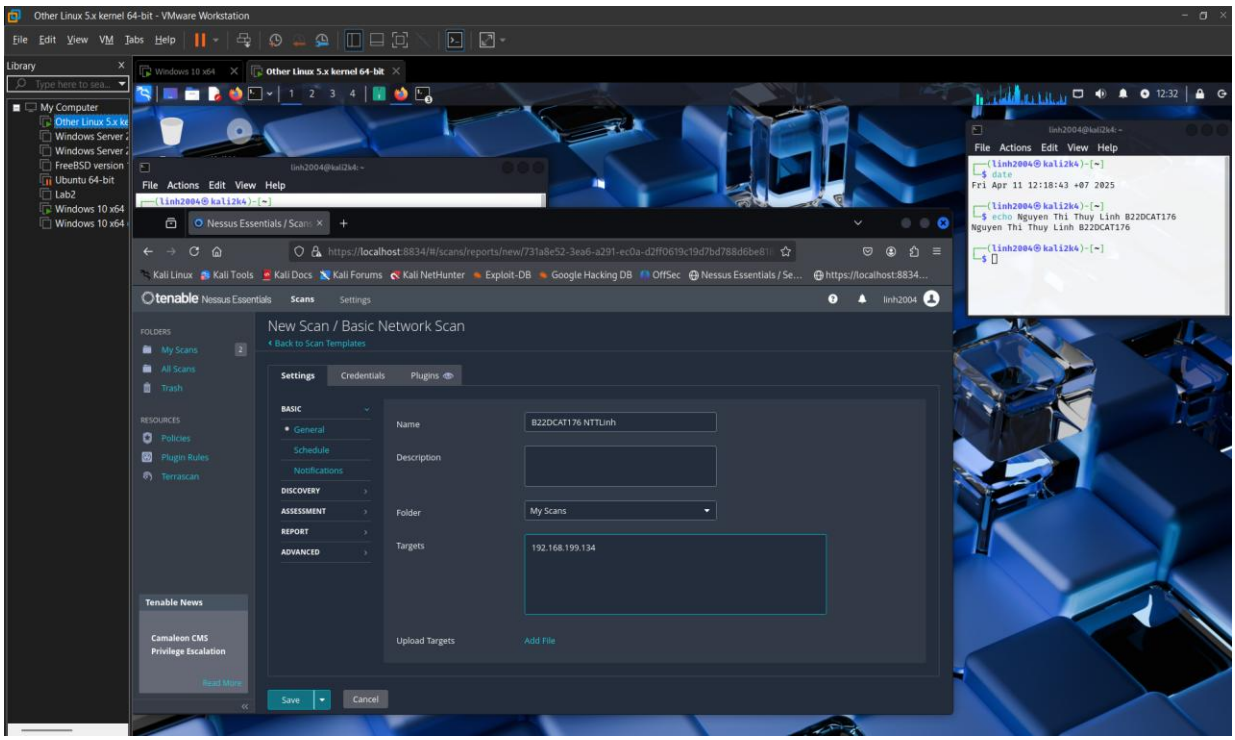
Hình ảnh 15: Đăng nhập Nessus.

-Chọn *New Scan*.



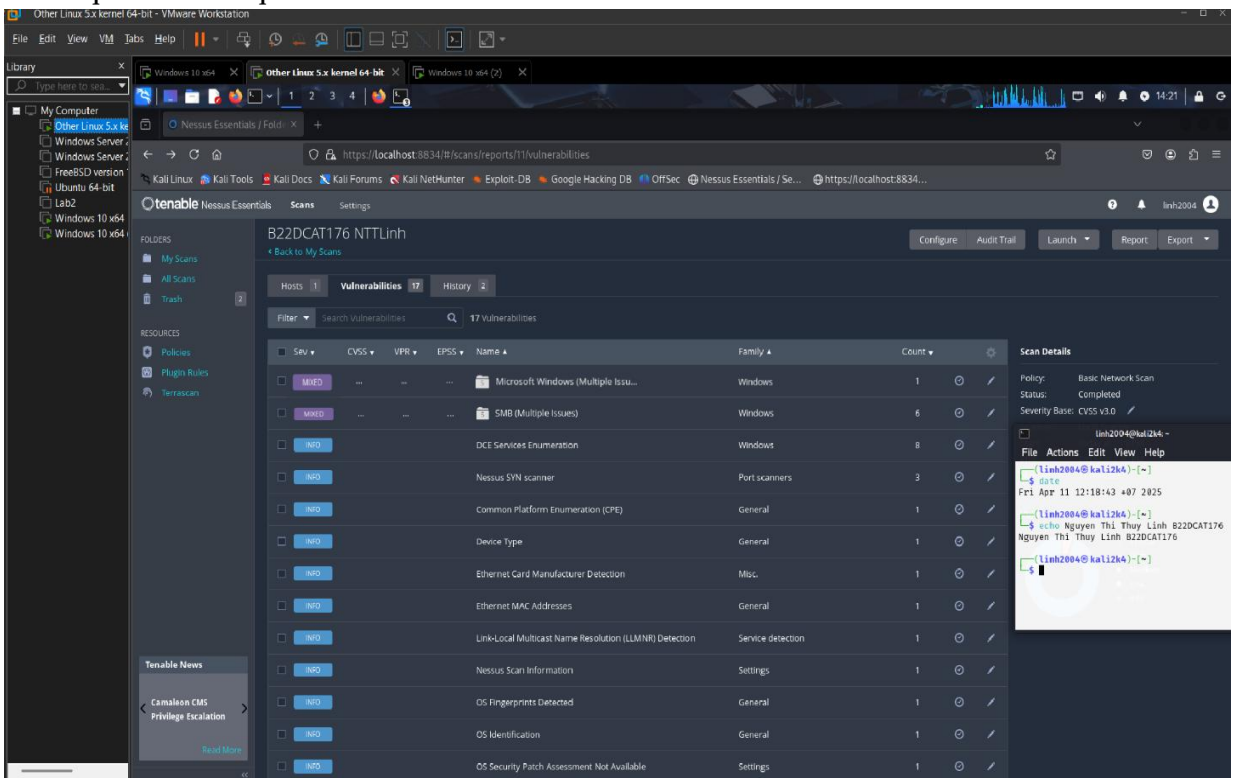
Hình ảnh 16: Chọn New Scan.

- Chọn Basic Network Scan và thêm tên và IP của máy cần quét.



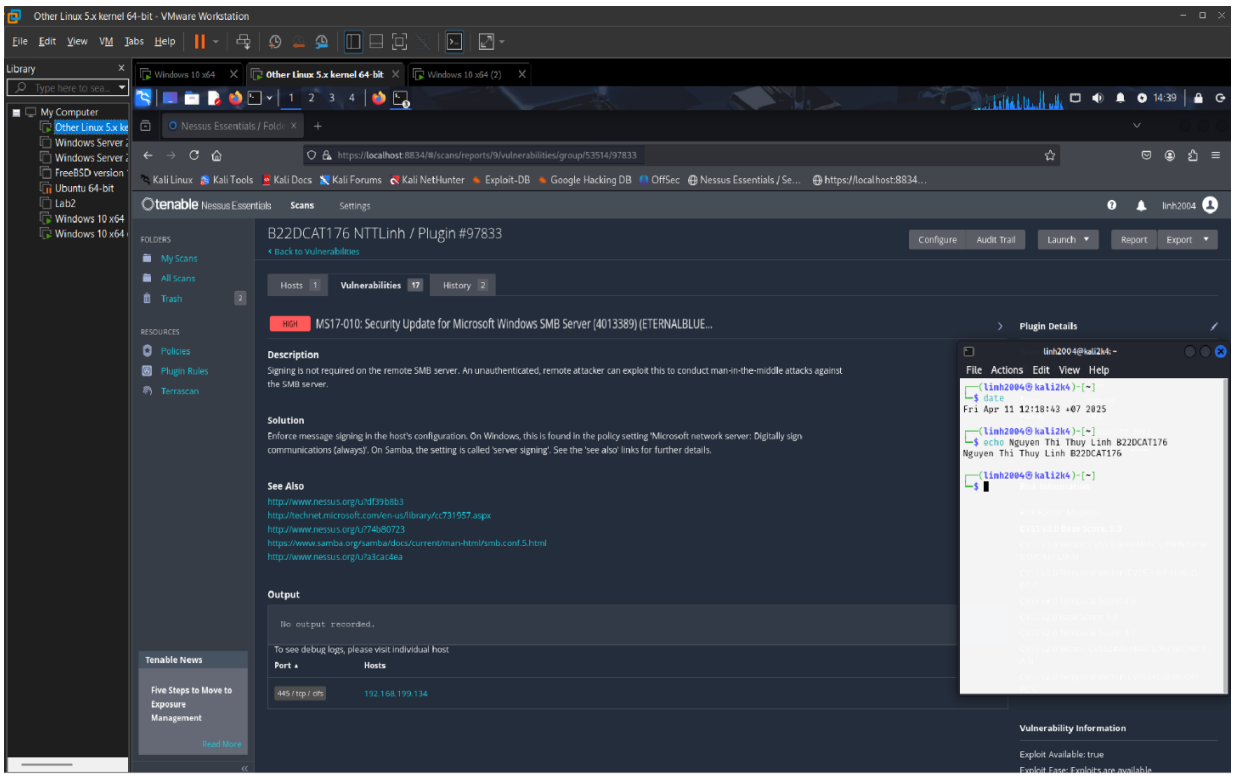
Hình ảnh 17: Chọn Basic Network Scan.

- Kết quả sau khi quét.



Hình 18: Kết quả sau khi quét.

-Thấy có lỗ hổng mức độ High với id là #97833.



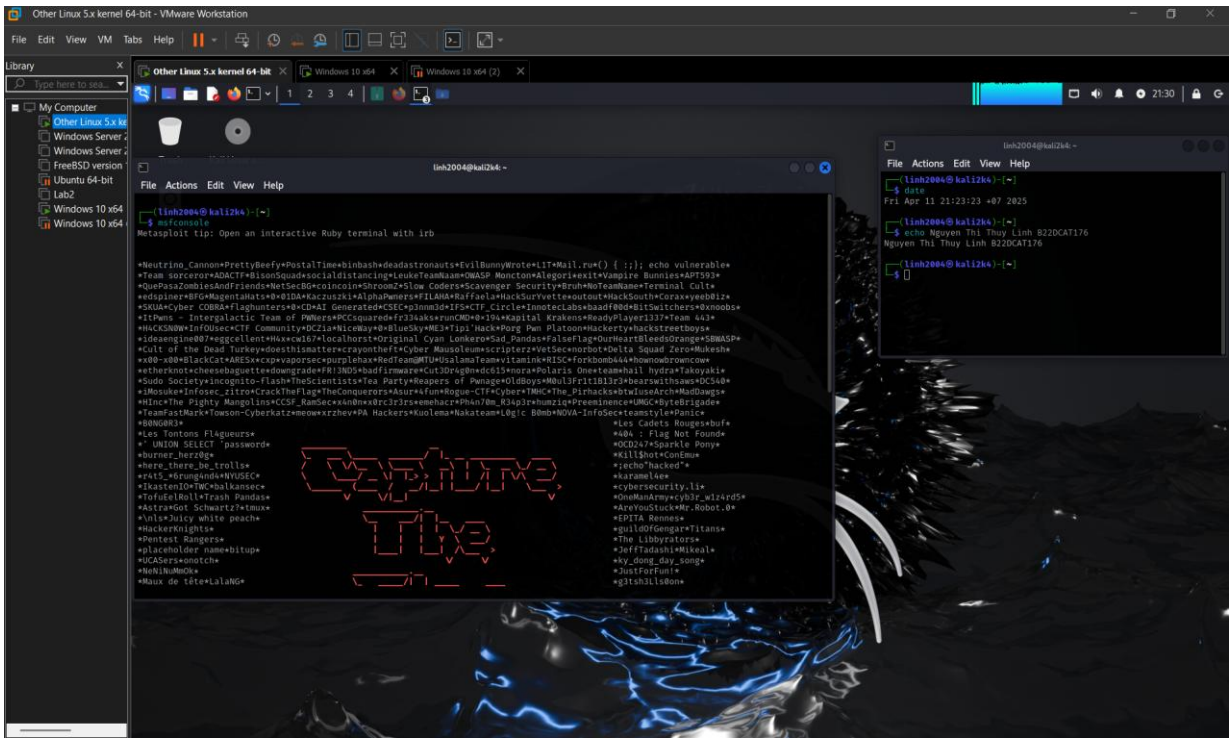
Hình ảnh 19: Thông tin về lỗ hổng.

2.4 Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7

Như phần trước, ta đã quét và nhận thấy có lỗ hổng *MS17-010*, ở mục này chúng ta sẽ khai thác lỗ hổng này. Đây chính là lỗ hổng *Eternal Blue* nổi tiếng được sử dụng trong cuộc tấn công quy mô lớn của *WannaCry* năm 2017.

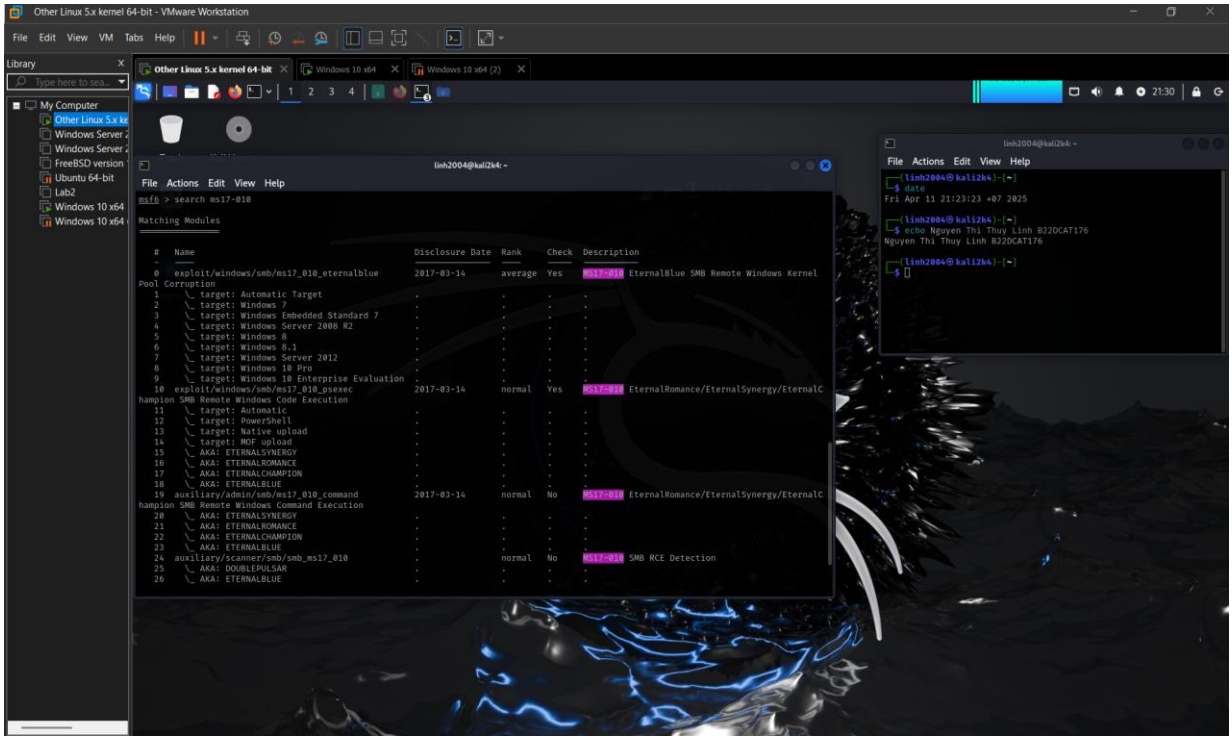
Lỗ hổng *EternalBlue*, có mã *CVE-2017-0144*, là một lỗ hổng bảo mật nghiêm trọng được phát hiện trên giao thức SMB (*Server Message Block*) của Microsoft Windows. Lỗ hổng này cho phép kẻ tấn công thực hiện tấn công từ xa và lây nhiễm malware một cách tự động mà không cần xác thực.

Trên Kali, mở terminal và chạy lệnh *msfconsole*



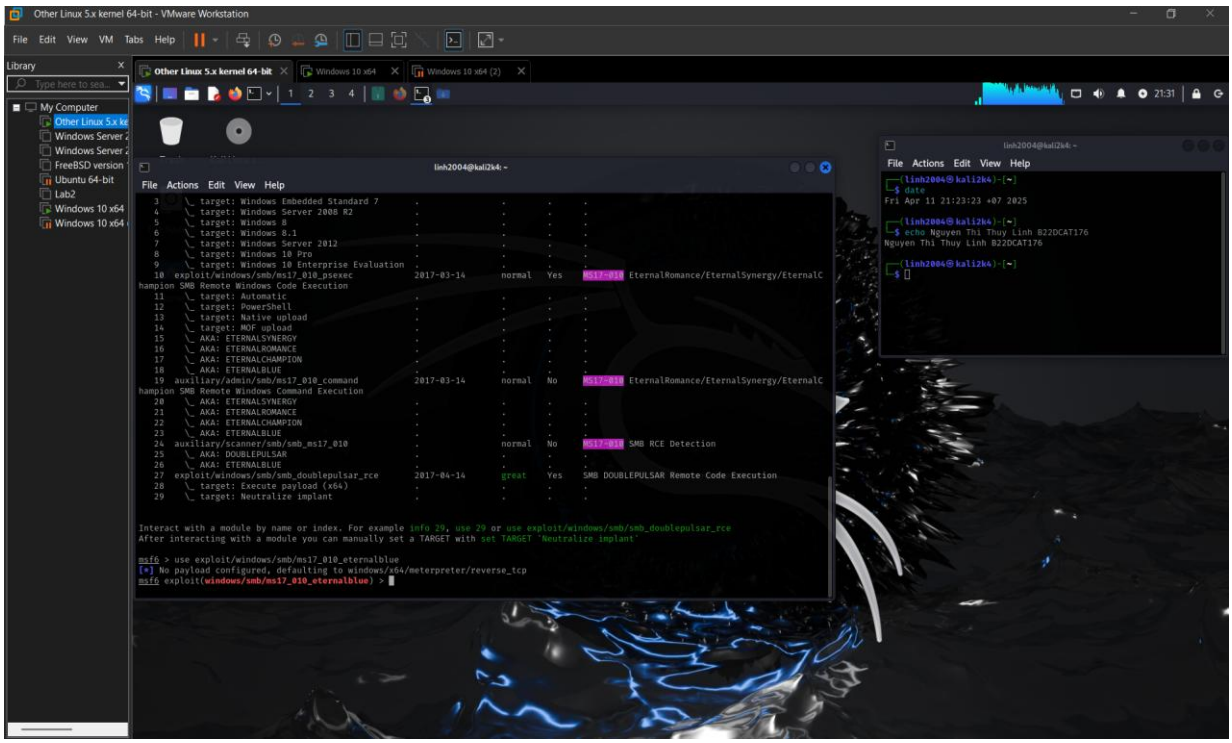
Hình ảnh 20: Khởi chạy Metasploit.

Chạy lệnh *search ms17-010*



Hình ảnh 21: Chạy lệnh search ms17-010

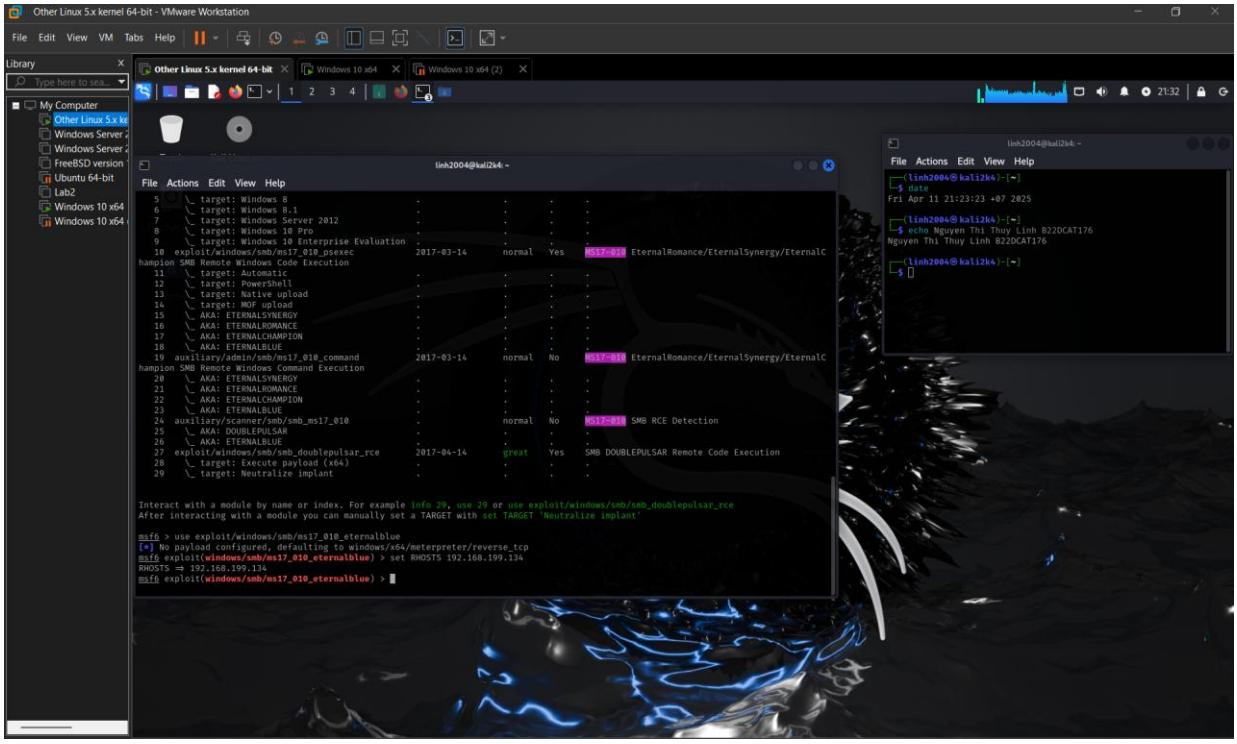
- Chọn module bằng lệnh *use exploit/windows/smb/ms17_010_eternalblue*



Hình ảnh 22: use exploit/windows/smb/ms17_010_eternalblue

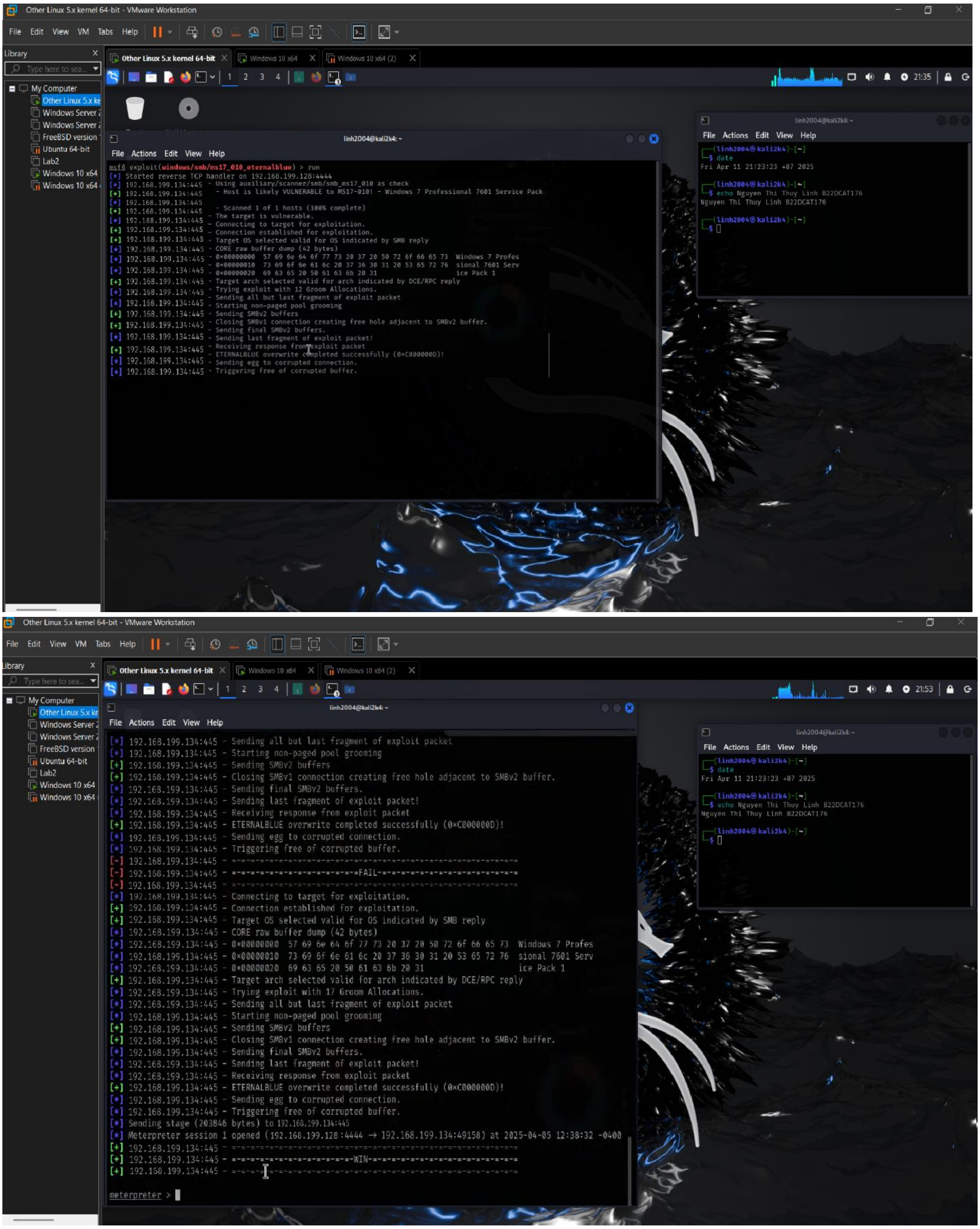
- Thiết lập lại địa chỉ IP máy mục tiêu:

set RHOSTS 192.168.199.134



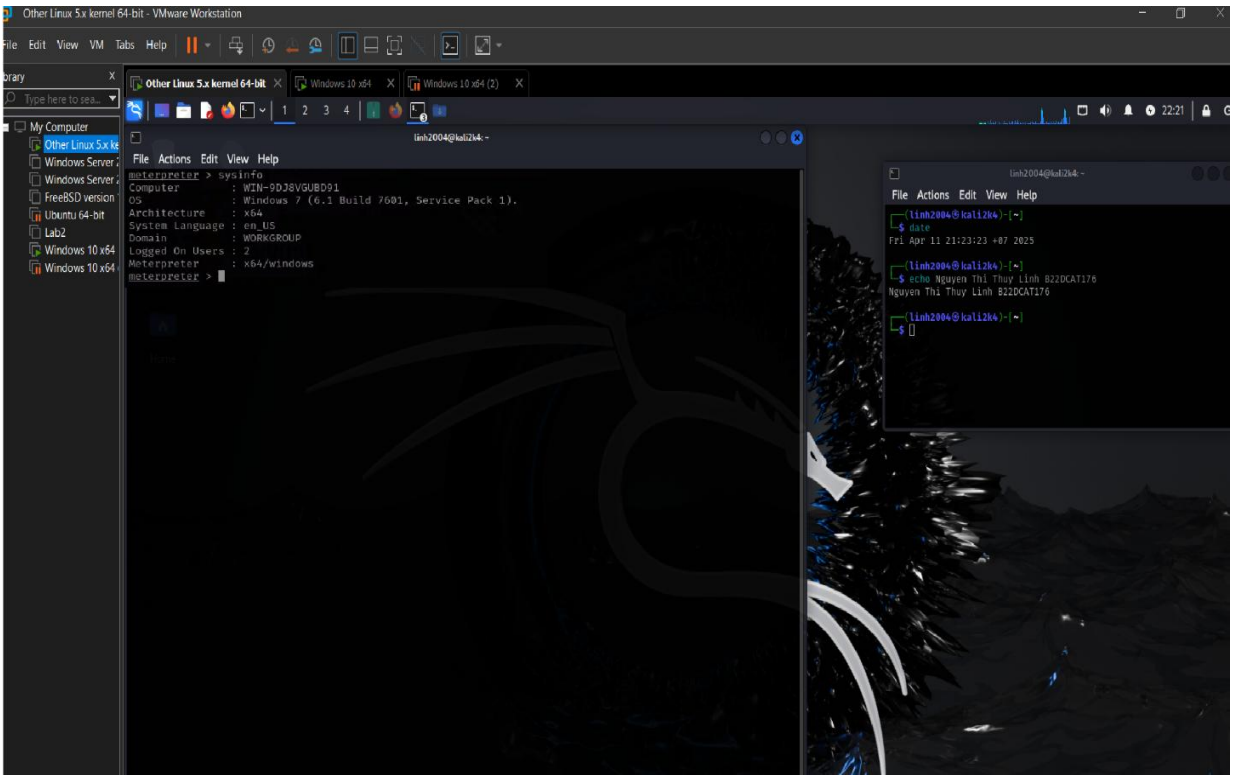
Hình ảnh 23: set RHOSTS 192.168.199.134

Thực hiện lệnh run để bắt đầu khai thác.



Hình ảnh 24: Thực hiện khai thác.

Khai thác thành công. Sử dụng lệnh sysinfo để kiểm tra thông tin máy mục tiêu.



Hình ảnh 25: Thông tin của máy mục tiêu.

3. Kết quả đạt được

- Sử dụng được nmap để rà quét các cổng dịch vụ
- Sử dụng được nessus để quét các lỗ hổng của máy tính.
- Sử dụng Metasploit để khai thác một trong những lỗ hổng đã tìm được.

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.

[3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.