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:

B22DCAT018 – Nguyễn Hoàng Anh

Giảng viên hướng dẫn: ThS. Ninh Thị Thu Trang

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. TÌM HIỂU LÝ THUYẾT

1.1 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 lổng 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.

1.2 Tìm hiểu lý thuyết

1.2.1 Lý thuyết về các công cụ nmap/zenmap, nessus, Metasploit framework.

a) Công cụ nmap

Nmap (Network Mapper) được Gordon Lyon giới thiệu lần đầu vào năm 1997, là một công cụ quét, theo dõi và đánh giá bảo mật hàng đầu, ban đầu nmap chỉ phát triển trên hệ điều hành linux, về sau có cả phiên bản dành cho các hệ điều hành khác như Windows, Mac OS,... đặc biệt nmap có một phiên bản GUI tên là Zenmap. Nmap có thể thực hiện quét trên một IP, dải IP, domain hay là cả một danh sách. Ví dụ: thekalitools.com, thekalitools.com/24, 192.168.0.1; 10.0.0-255.1-254;...

b) Công cụ nessus

Nessus là một 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. Theo cuộc khảo sát năm 2009 bởi sectools.org, Nessus là công cụ quét lỗ hổng bảo mật nổi tiếng nhất thế giới.

Nessus cho phép quét các loại lỗ hổng như cho phép kiểm soát từ xa hoặc truy cập dữ liệu nhạy cảm trên hệ thống, cấu hình sai, sử dụng mật khẩu mặc định, mật khẩu dễ đoán, 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, hoặc tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại,....

Nessus bao gồm hai phần chính:

- Nessusd - dịch vụ luôn chạy của Nessus - thực hiện quét
- Nessus client - chương trình con - điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng.

Các phiên bản sau của Nessus (4 và mới hơn) sử dụng một máy chủ web cung cấp cùng tính năng giống như Nessus client. Thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn ngữ tấn công dạng kịch bản Nessus - Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng.

c) Công cụ metasploit

Metasploit framework là một công cụ rất mạnh mẽ có thể được sử dụng để thăm dò các lỗ hổng hệ thống trên mạng và máy chủ. Bởi vì nó có mã nguồn mở, nó có thể dễ dàng tùy chỉnh và sử dụng với hầu hết các hệ điều hành. Metasploit chứa trên 1677 chương trình khai thác lỗ hổng trên 25 nền tảng, như Cisco, Java, Python, PHP, Android và các nền tảng khác. Với Metasploit, người kiểm thử xâm nhập có thể sử dụng chương trình tấn công có sẵn hoặc tùy chỉnh và thực thi vào một mạng để thăm dò các điểm yếu. Một khi các lỗ hổng được xác định và ghi lại, thông tin có thể được sử dụng để giải quyết các điểm yếu hệ thống và ưu tiên các giải pháp.

1.2.2 Lý thuyết về một số lỗ hổng, một số cổng dịch vụ quét được

Lỗ hổng bảo mật là những lỗi phần mềm, lỗi trong đặc điểm kỹ thuật và thiết kế, nhưng đa số là lỗi trong lập trình. Bất kỳ gói phần mềm lớn nào cũng có hàng ngàn lỗi. Đây là những lỗ hổng nằm ủ mình trong hệ thống phần mềm của chúng ta, đợi đến khi được kích hoạt hoặc bị phát hiện. Khi đó, chúng có thể được dùng để tấn công các hệ thống.

Các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo nên sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép truy cập bất hợp pháp vào hệ thống. Các lỗ hổng bảo mật có thể nằm ngay các dịch vụ cung cấp như web, mail, ftp,… Ngoài ra các chương trình ứng dụng hay dùng cũng chứa các lỗ hổng.

Có nhiều nguyên nhân gây ra lỗ hổng bảo mật: do lỗi của bản thân hệ thống, hoặc do người quản trị hệ thống không hiểu sâu sắc các dịch vụ cung cấp hoặc do người dùng sử dụng có ý thức bảo mật kem click vào các đường link hoặc tải về các ứng dụng độc hại.

Lỗ hổng bảo mật có mức độ ảnh hưởng khác nhau. Có những lỗ hổng chỉ ảnh hưởng đến chất lượng dịch vụ cung cấp nhưng cũng có những lỗ hổng ảnh hưởng tới cả hệ thống hoặc làm ngưng trệ dịch vụ. Một số cổng dịch vụ quét được lỗ hổng như: SSH, FTP, SMTP, HTTP, HTTPS, DNS, SNMP, MySQL,…

* Lỗ hổng nessus quét được trên máy windows 7:

Lỗ hổng MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check). Đây là lỗ hổng trong cơ chế phân giải DNS của Windows có thể cho phép kẻ tấn công thực thi mã từ xa nếu người dùng truy cập vào một máy chủ DNS độc hại. Nó cho phép RCE (Remote Code Execution), rất nguy hiểm nếu bị khai thác thành công. Giải pháp là cập nhật bản vá Microsoft MS11-030 (mã CVE: CVE-2011-0035).

Lỗ hổng Unsupported Windows OS (remote). Hệ điều hành Windows được phát hiện không còn được Microsoft hỗ trợ (ví dụ: Windows XP, Windows 7 cũ...). Hiện nay không còn bản vá bảo mật nên cực kỳ dễ bị khai thác thông qua các lỗ hổng đã biết. Giải pháp là nâng cấp lên phiên bản Windows được hỗ trợ như Windows 10, 11 hoặc Windows Server 2019+.

Lỗ hổng MS17-010: Eternal Blue. Đây là lỗ hổng nghiêm trọng trong giao thức SMBv1 của Windows, được sử dụng trong vụ tấn công WannaCry ransomware. Nó Cho phép thực thi mã từ xa mà không cần xác thực, lan truyền nhanh qua mạng. Giải pháp là cập nhật bản vá MS17-010 hoặc vô hiệu hóa SMBv1 nếu không cần thiết.

Lỗ hổng MS16-047: Windows CSRSS Elevation of Privilege. Đây là lỗ hổng trong CSRSS (Client/Server Runtime Subsystem) cho phép người dùng cục bộ leo thang đặc quyền. Khiến cho kẻ tấn công có thể chiếm quyền quản trị hệ thống từ tài khoản có quyền thấp. Giải pháp là áp dụng bản vá bảo mật MS16-047 từ Microsoft.

1.2.3 Lý thuyết về lỗ hổng mà Metasploit framework khai thác được (lỗ hổng ms17-010)

Lỗ hổng MS17-010 là một lỗ hổng bảo mật trong giao thức SMBv1 (Server Message Block version 1), được phát hiện và công bố bởi Microsoft vào tháng 3 năm 2017. Đây là một lỗ hổng đặc biệt nguy hiểm vì nó cho phép tin tặc thực hiện tấn công từ xa trên các hệ thống chạy hệ điều hành Windows.

Tác hại của lỗ hổng này rất nghiêm trọng. Nó cho phép tin tặc thực hiện tấn công kiểu "Remote Code Execution" (RCE), có nghĩa là tin tặc có thể thực thi mã từ xa trên hệ thống mục tiêu mà không cần tài khoản người dùng hợp lệ. Điều này có thể dẫn đến việc kiểm soát hoàn toàn hệ thống, đánh cắp dữ liệu, triển khai phần mềm độc hại, hoặc thậm chí tấn công các hệ thống khác trong mạng nội bộ.

Lỗ hổng MS17-010 tồn tại trong các phiên bản của hệ điều hành Windows từ Windows 7 đến Windows Server 2016.

Để khắc phục lỗ hổng này, Microsoft đã phát hành các bản vá bảo mật. Đối với người dùng và quản trị viên hệ thống, việc cập nhật hệ thống với các bản vá bảo mật mới nhất từ Microsoft là cách hiệu quả nhất để ngăn chặn việc tận dụng lỗ hổng này. Ngoài ra, có thể tắt giao thức SMBv1 hoặc triển khai các biện pháp kiểm soát truy cập bổ sung để giảm thiểu rủi ro từ lỗ hổng MS17-010.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

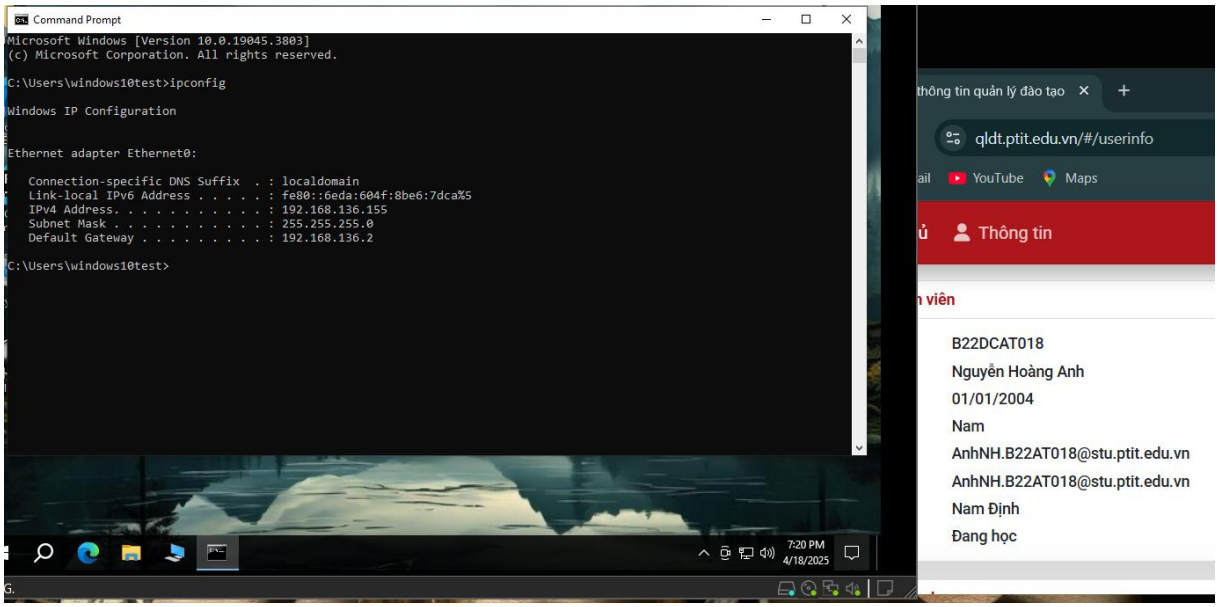
2.1 Chuẩn bị môi trường

Phần mềm ảo hoá VMWARE

Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework.

2.2 Các bước thực hiện

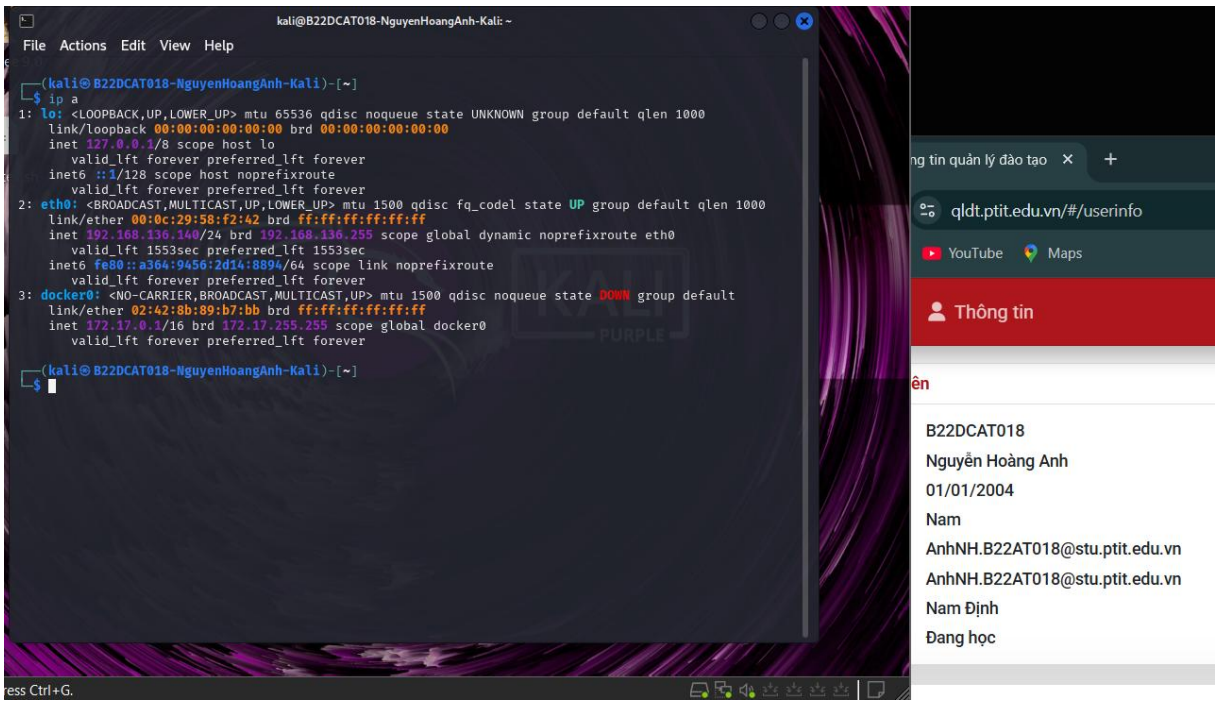
Máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows.



Hình 1 - máy nạn nhân

➔ Máy windows có ip: 192.168.136.155

Máy của người tấn công là máy tính kali:

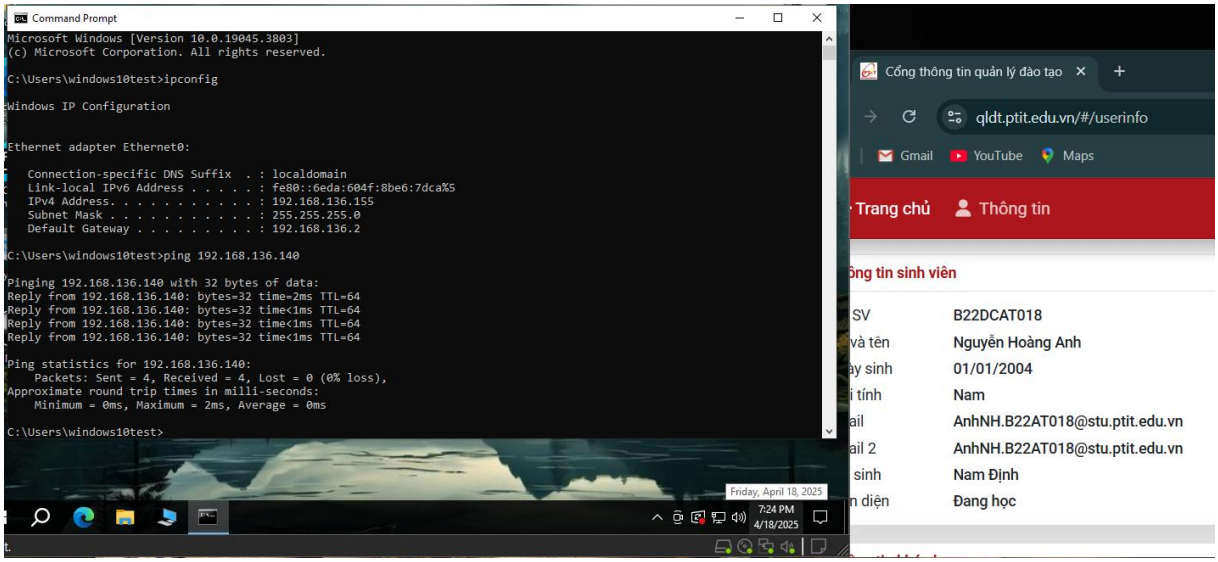


Hình 2 - máy tấn công

➔ Máy kali có ip: 192.168.136.140

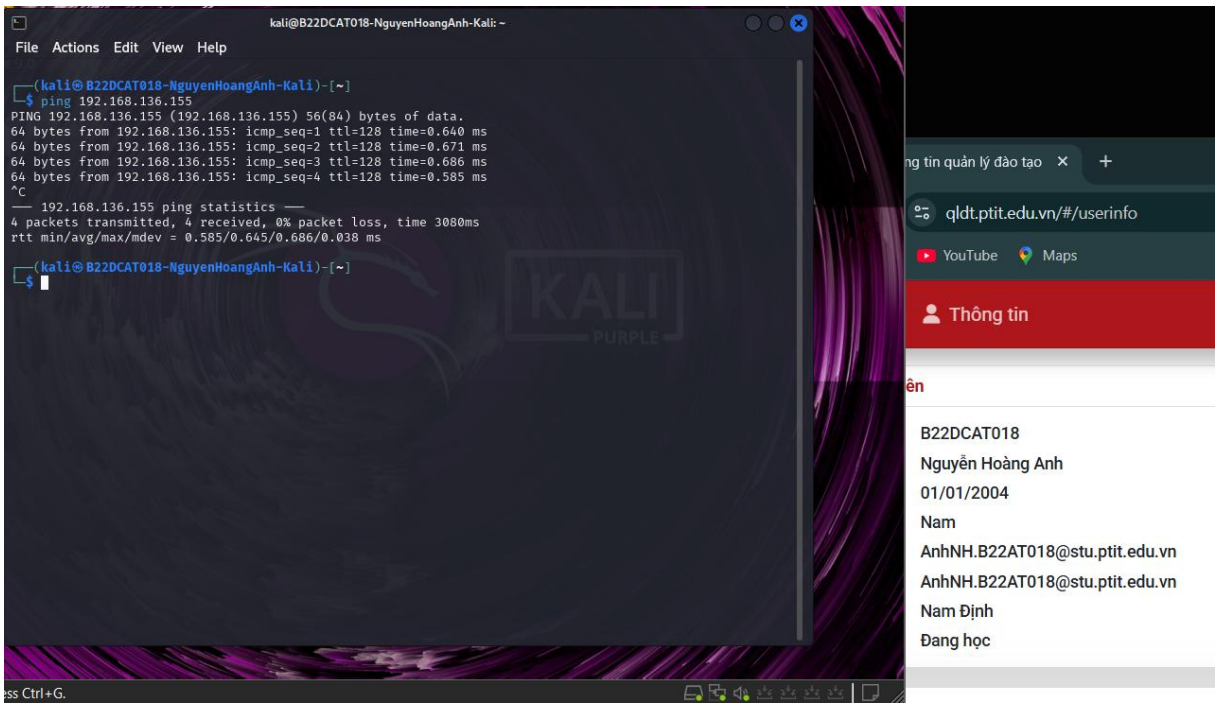
Kiểm tra sự thông nhau

Ping từ máy windows đến máy kali:



Hình 3 - ping từ máy windows đến máy kali

Ping từ máy kali đến máy windows 10:



Hình 4 - ping từ máy kali đến máy windows

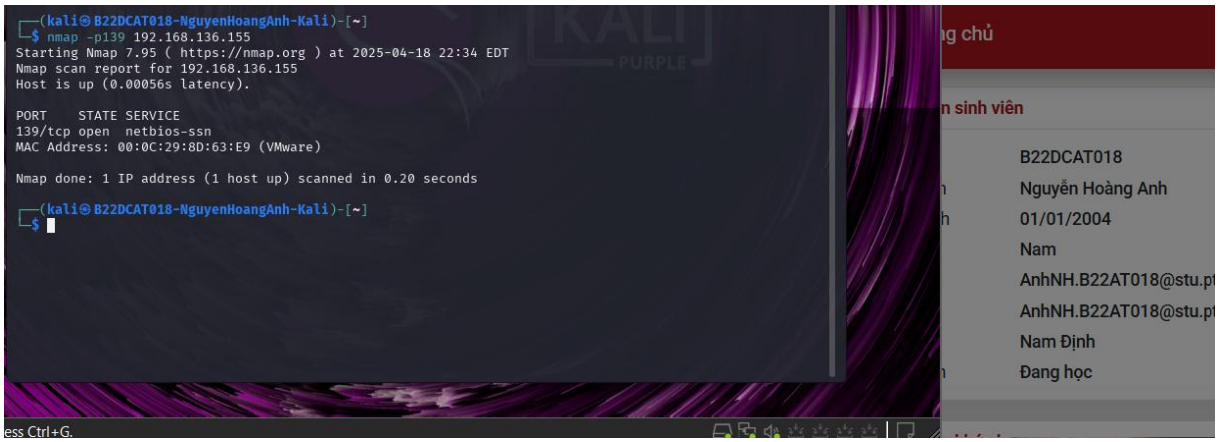
2.2.1 Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng).

Quét bằng nmap:

Hình 5 - quét bằng nmap

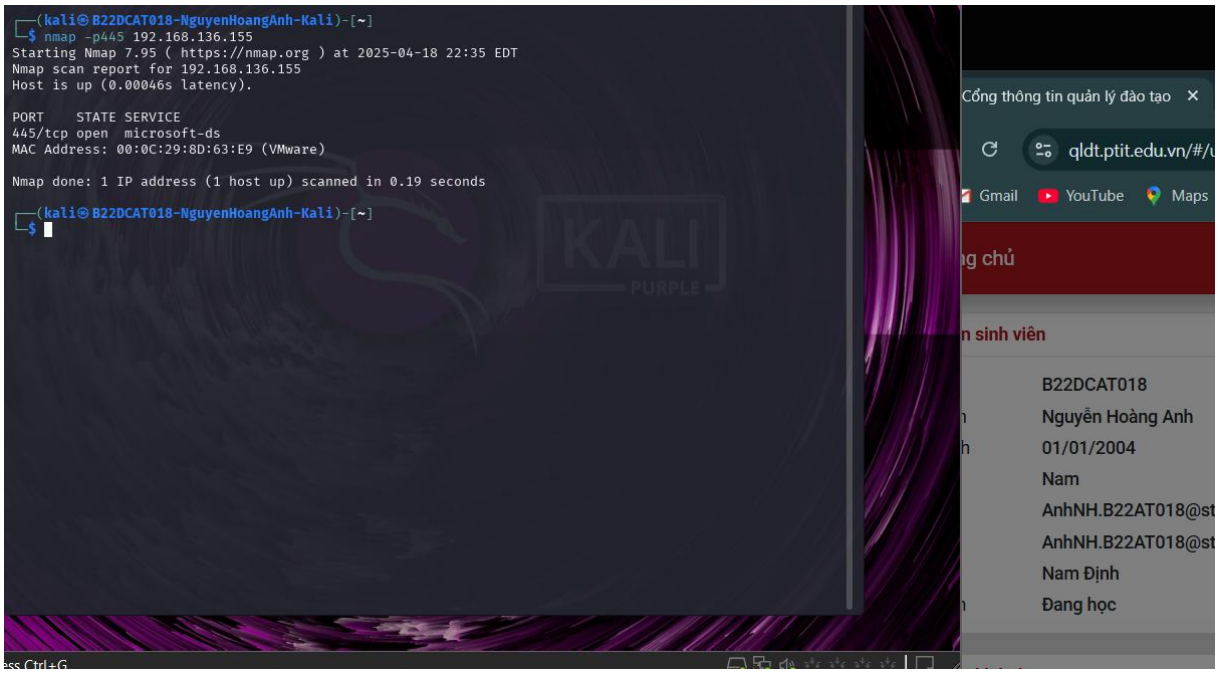
➔ Kết quả trả về là các cổng đang mở trên máy windows

Quét cổng dịch vụ netbios-ssn (cổng 139)



Hình 6 - quét cổng dịch vụ netbios-ssn

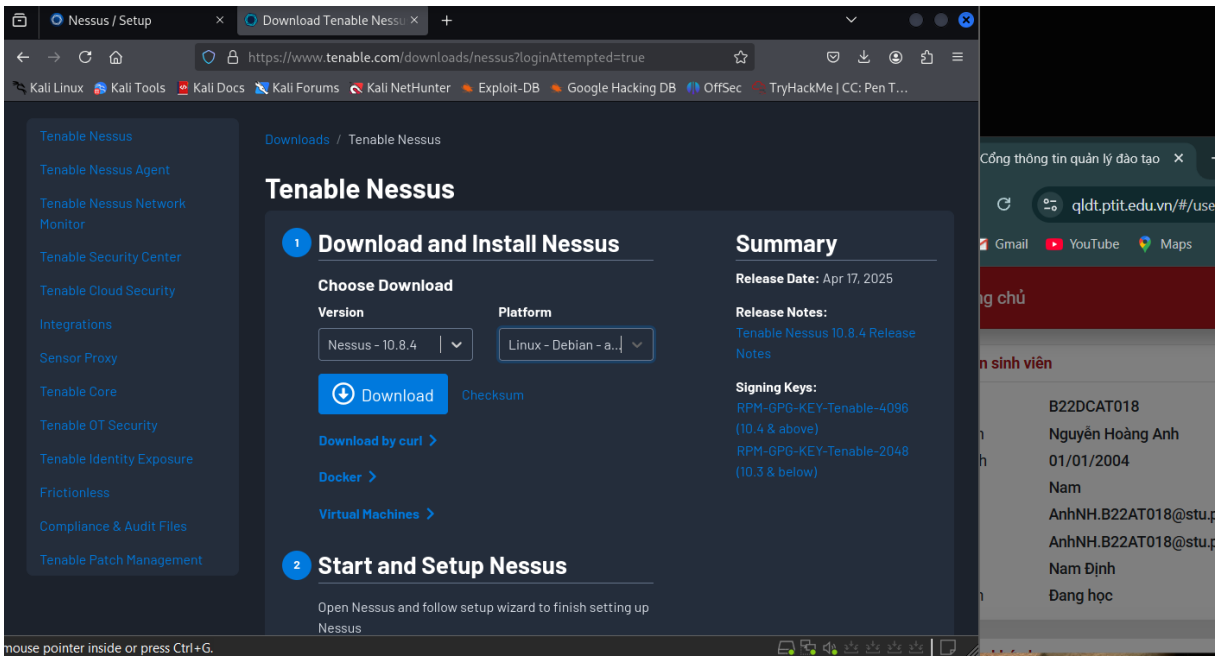
Quét cổng dịch vụ microsoft-ds (cổng 445)



Hình 7 - quét cổng dịch vụ microsoft-ds

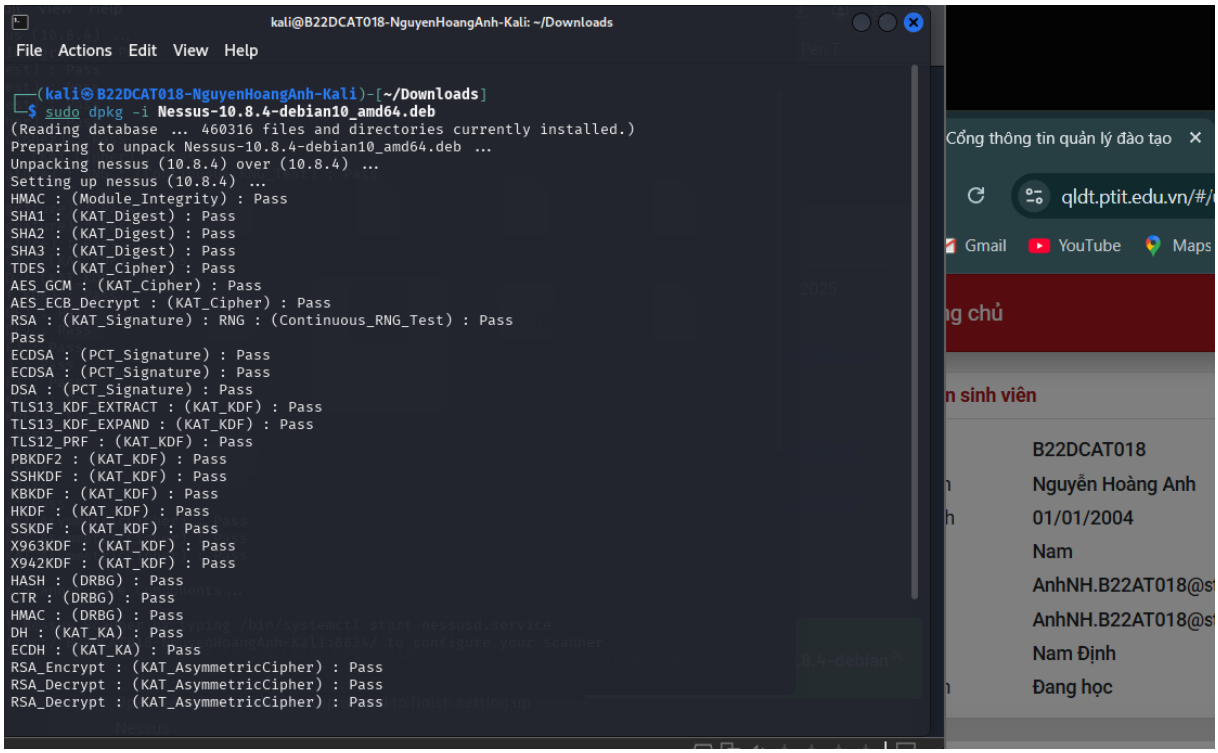
2.2.2 Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).

Tải nessus về do máy kali không có sẵn



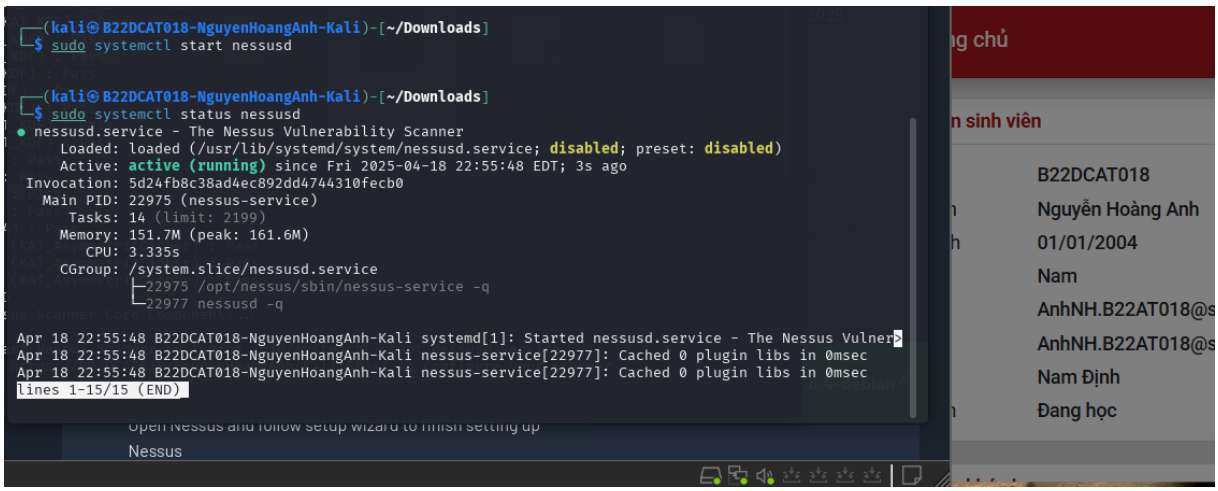
Hình 8 - tải nessus tại trang chủ tenable

Chạy lệnh để cài đặt nessus



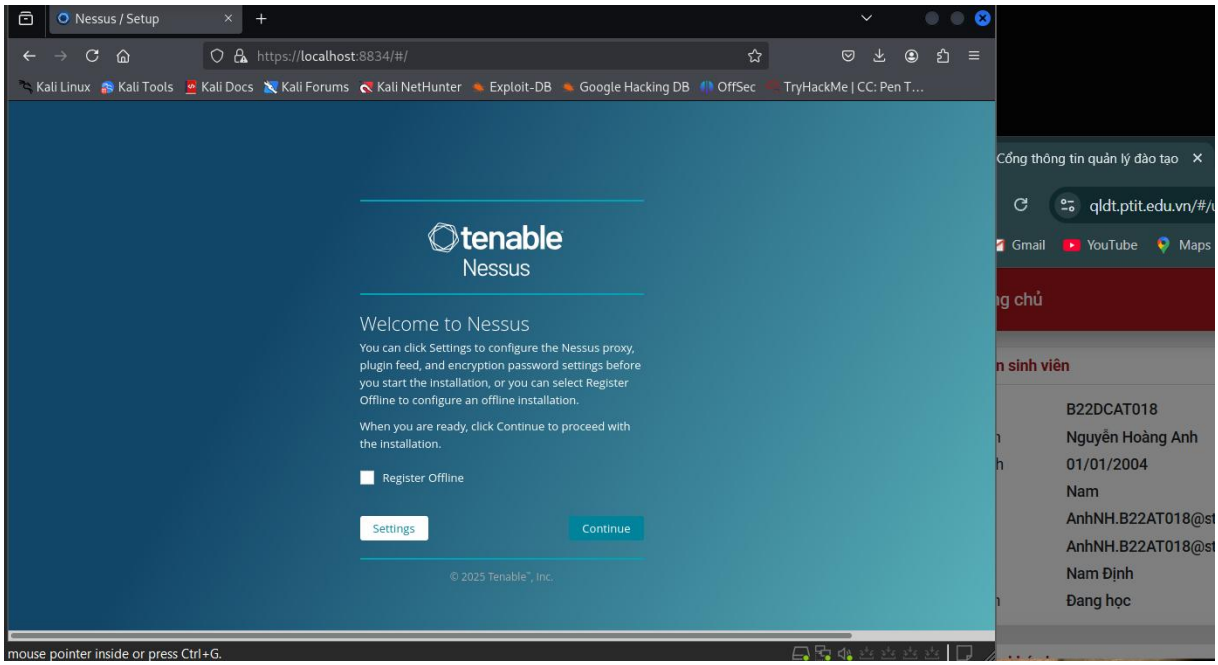
Hình 9 - cài đặt nessus

Khởi động dịch vụ nessus và kiểm tra trạng thái (running)



Hình 10 - khởi động và kiểm tra trạng thái nessus

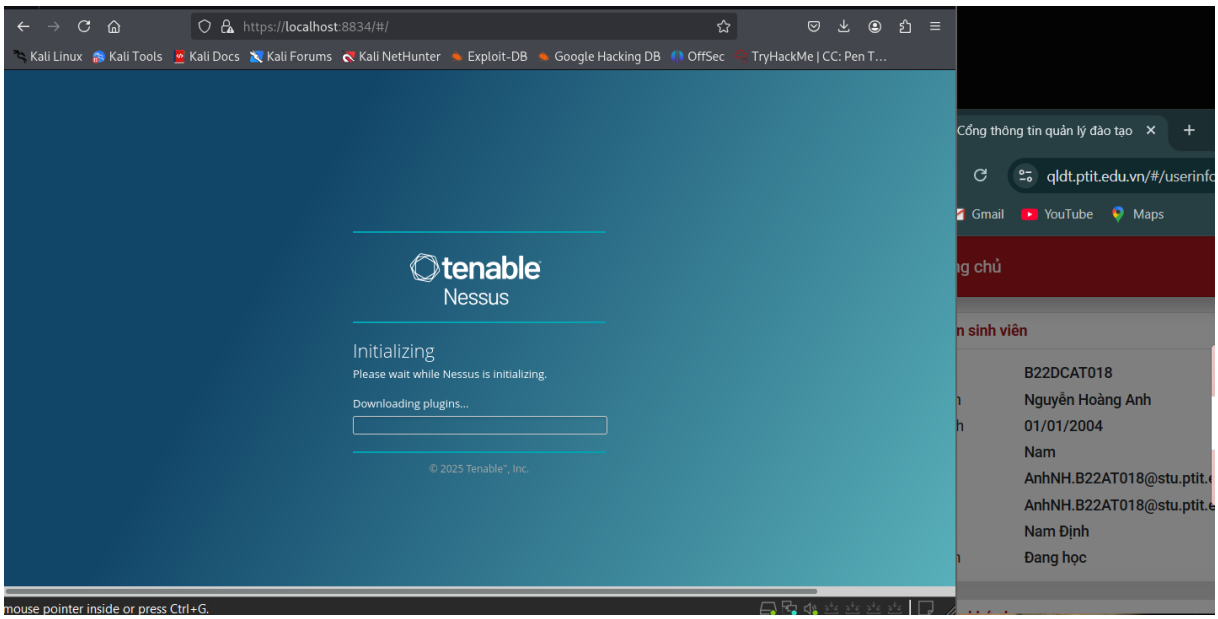
Vào trình duyệt và vào địa chỉ: *https://localhost:8834/* để truy cập giao diện nessus



Hình 11 - truy cập giao diện nessus

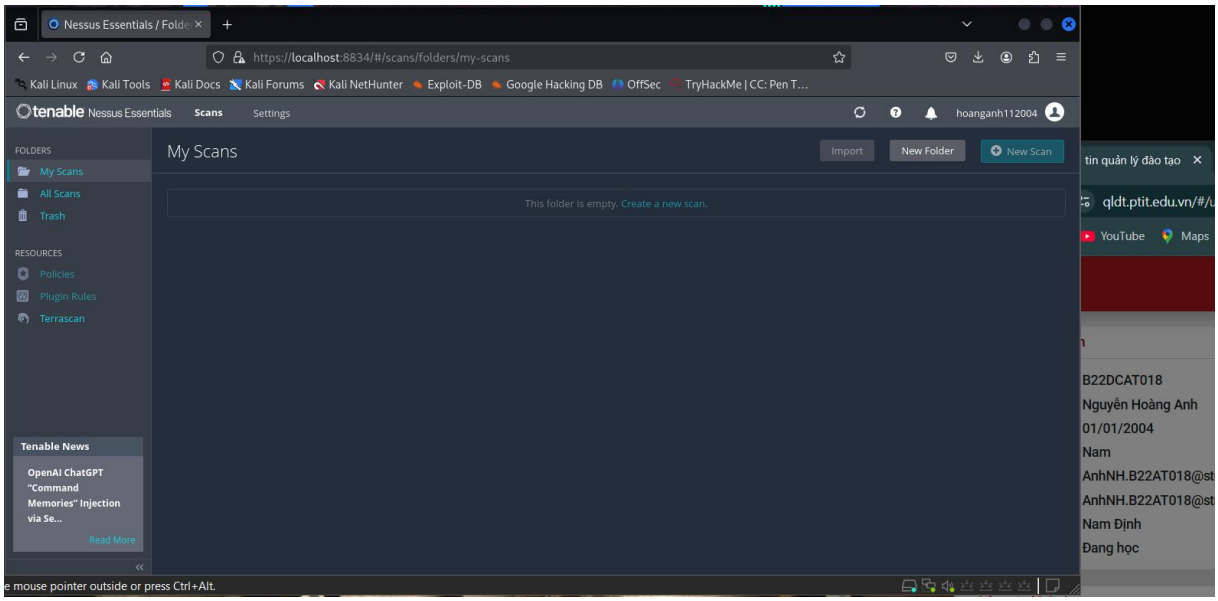
Chọn “continue” → chọn bản “ nessus essentials” (bản miễn phí) → nhập thông tin để tạo tài khoản và tải xuống plugins

Giao diện khi tải plugins:



Hình 12 - tải plugins

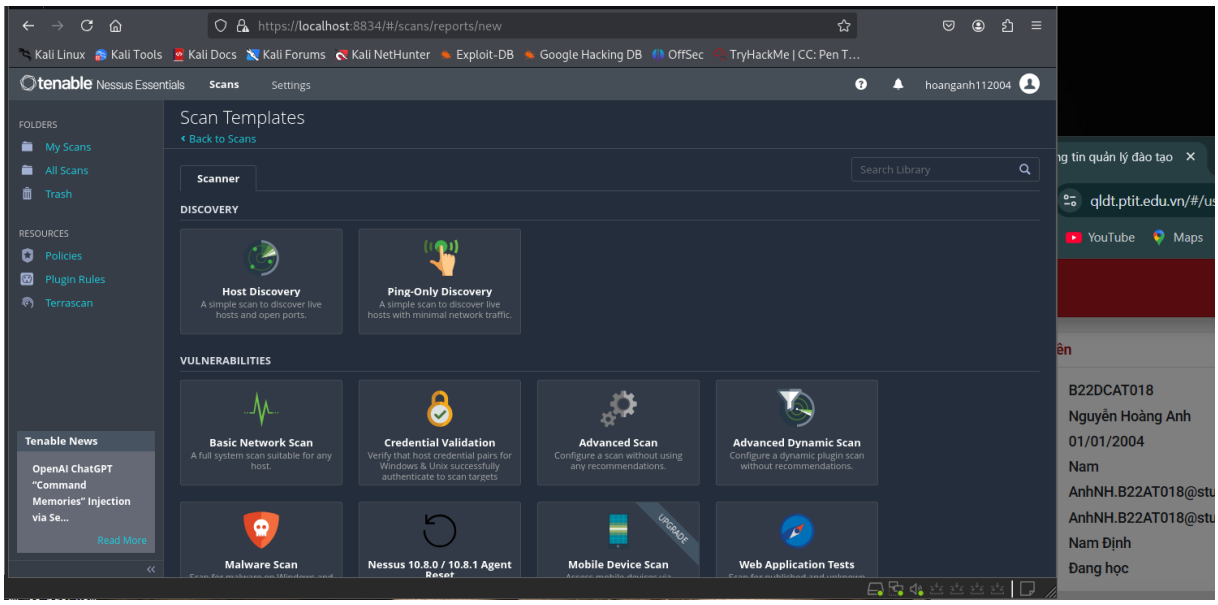
Giao diện browser nessus



Hình 13 - giao diện browser nessus

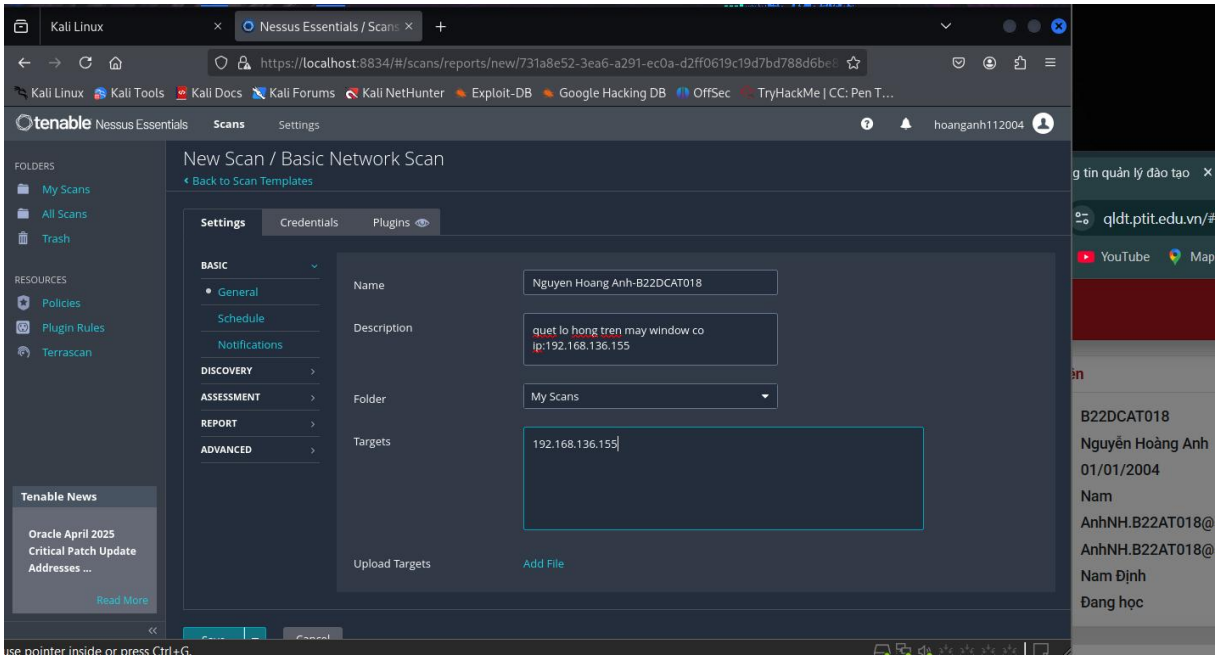
* Quét lỗ hổng sử dụng nessus:

Chọn “New Scan”:



Hình 14 - giao diện new scan

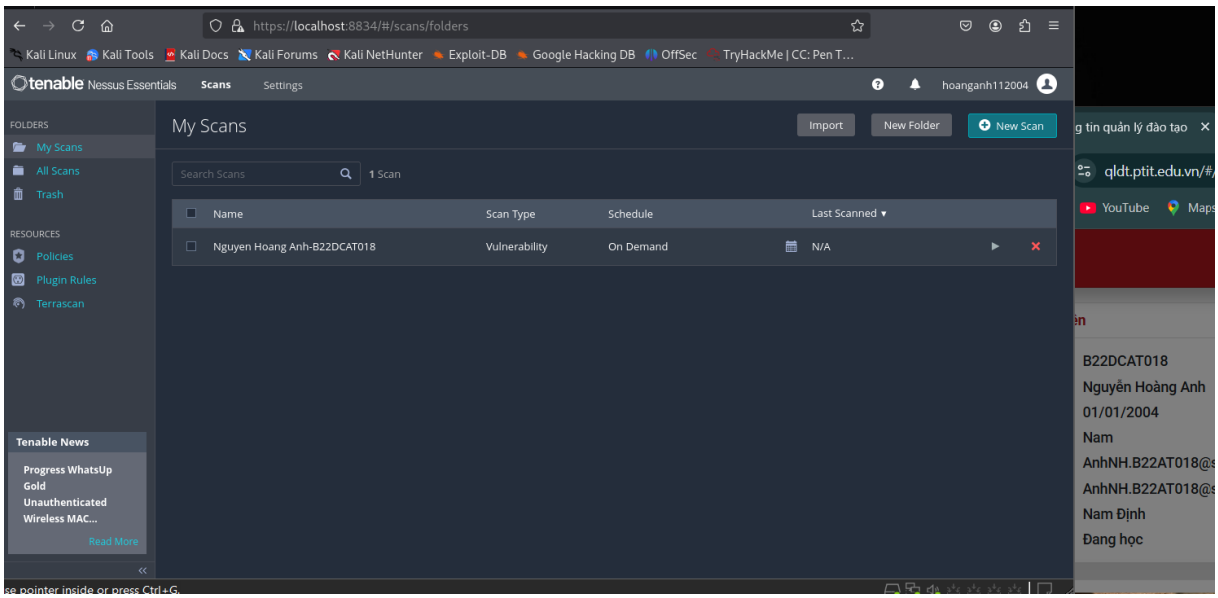
Chọn “basic network scan” và nhập các thông số



Hình 15 - giao diện basic network scan

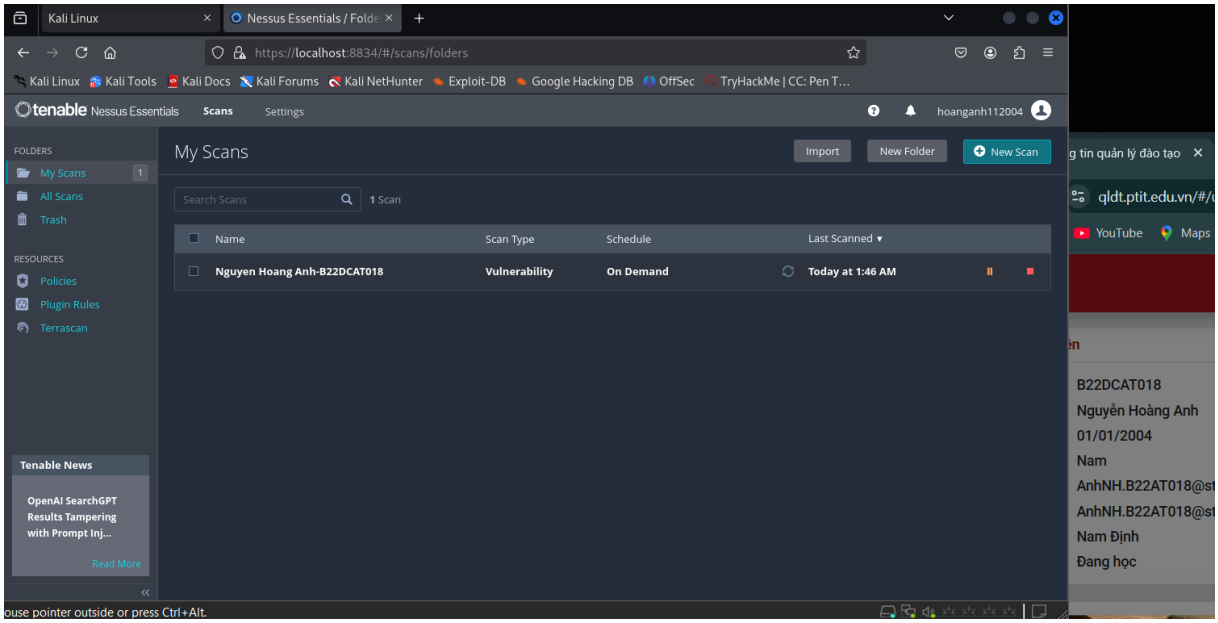
Sau khi đã nhập xong thông số, chọn “save” để lưu scan

Ở phần “my scan” sẽ xuất hiện scan vừa lưu, chọn và ấn “launch” để quét



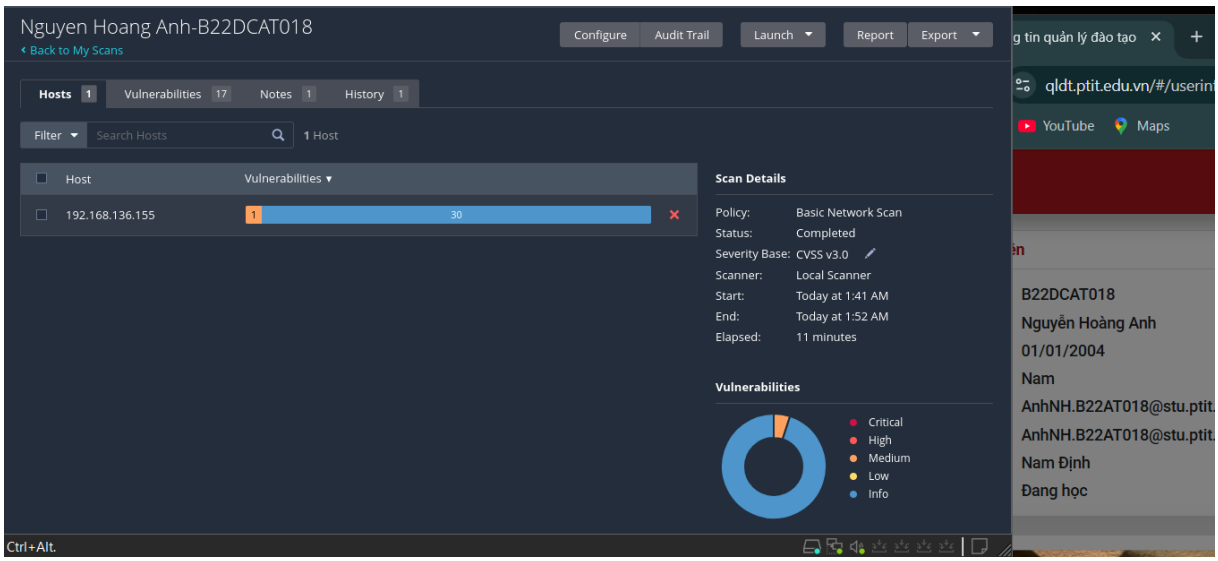
Hình 16 - scan được lưu lại

Quá trình quét



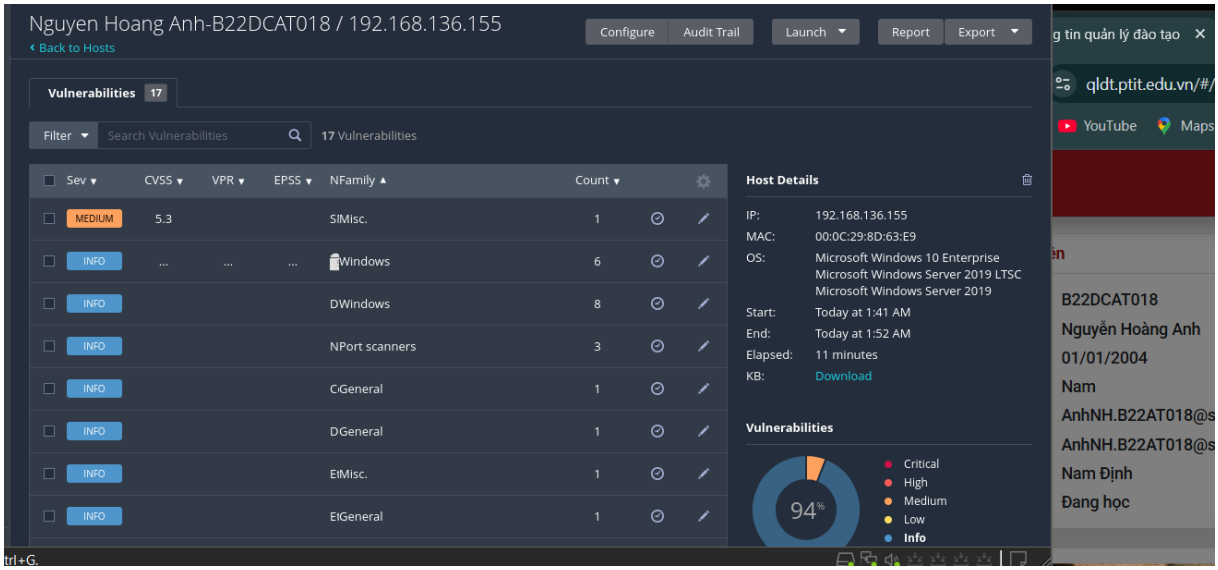
Hình 17 - quá trình quét

Kết quả sau khi quét xong



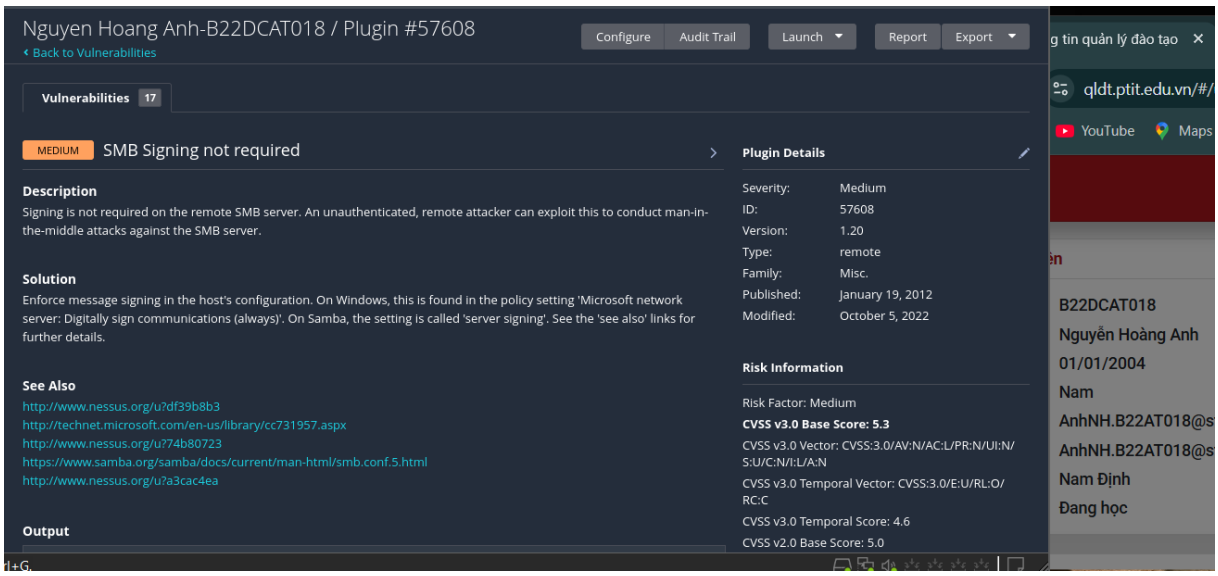
Hình 18 - kết quả

Chi tiết các lỗ hổng quét được



Hình 19 - các lỗ hổng quét được

Chọn vào 1 lỗ hổng để xem chi tiết về mô tả, cách khắc phục, các vấn đề liên quan

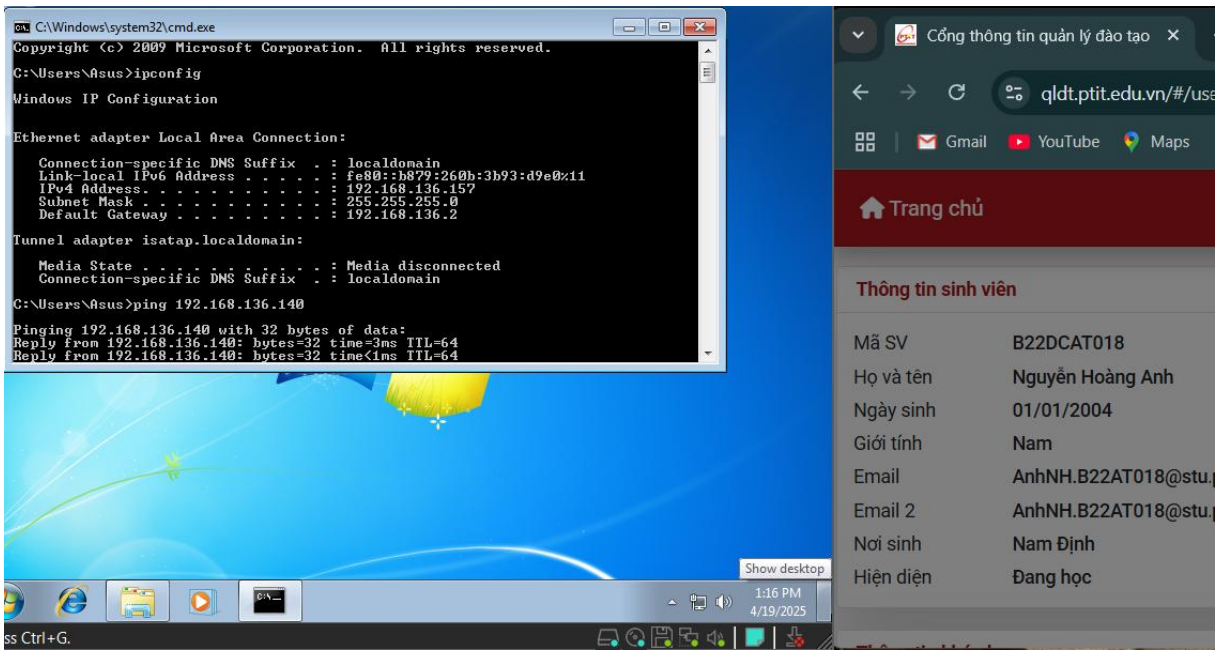


Hình 20 - chi tiết của một lỗ hổng

2.2.3 Sử dụng Metasploit framework khai thác lỗ hổng (ít nhất khai thác thành công 1 lỗ hổng trên máy nạn nhân).

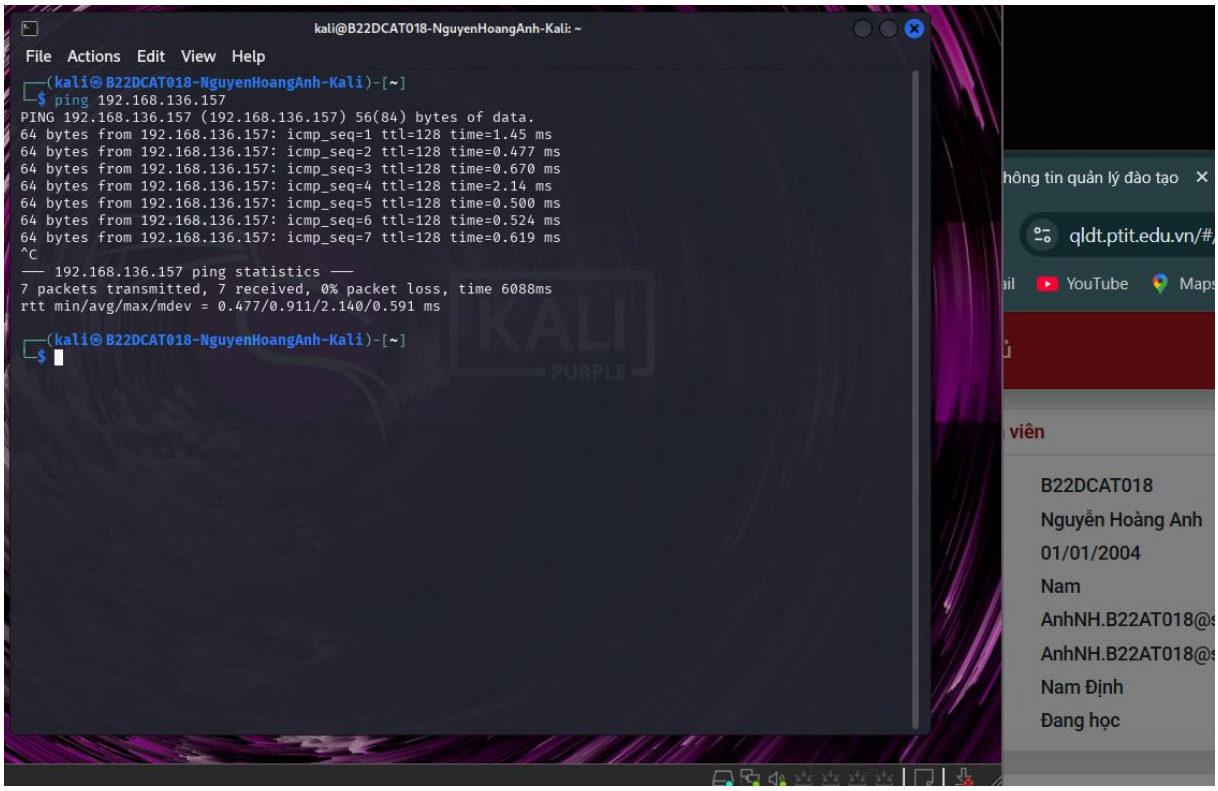
Vì máy windows 10 đã được fix lỗ hổng nên ở phần này em sử dụng máy nạn nhân là máy windows 7

Sử dụng máy nạn nhân là máy windows 7 có ip: 192.168.136.157



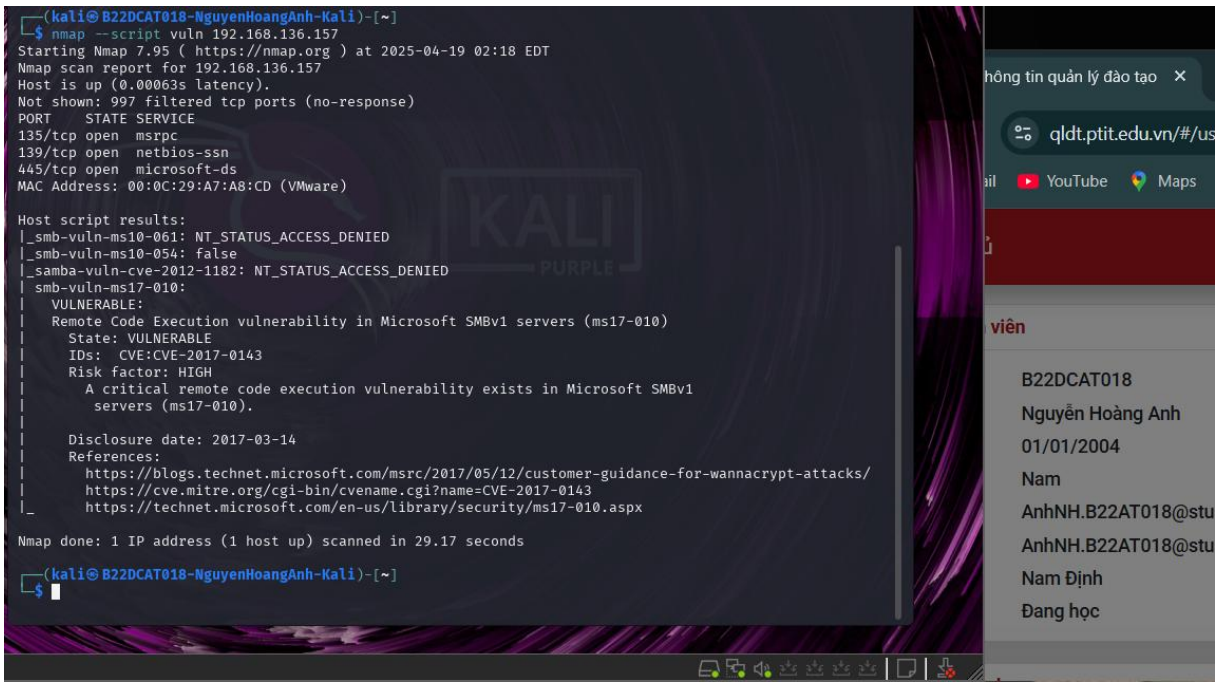
Hình 21 - máy windows 7

ping từ máy kali đến máy windows 7



Hình 22 - ping từ máy kali đến máy windows 7

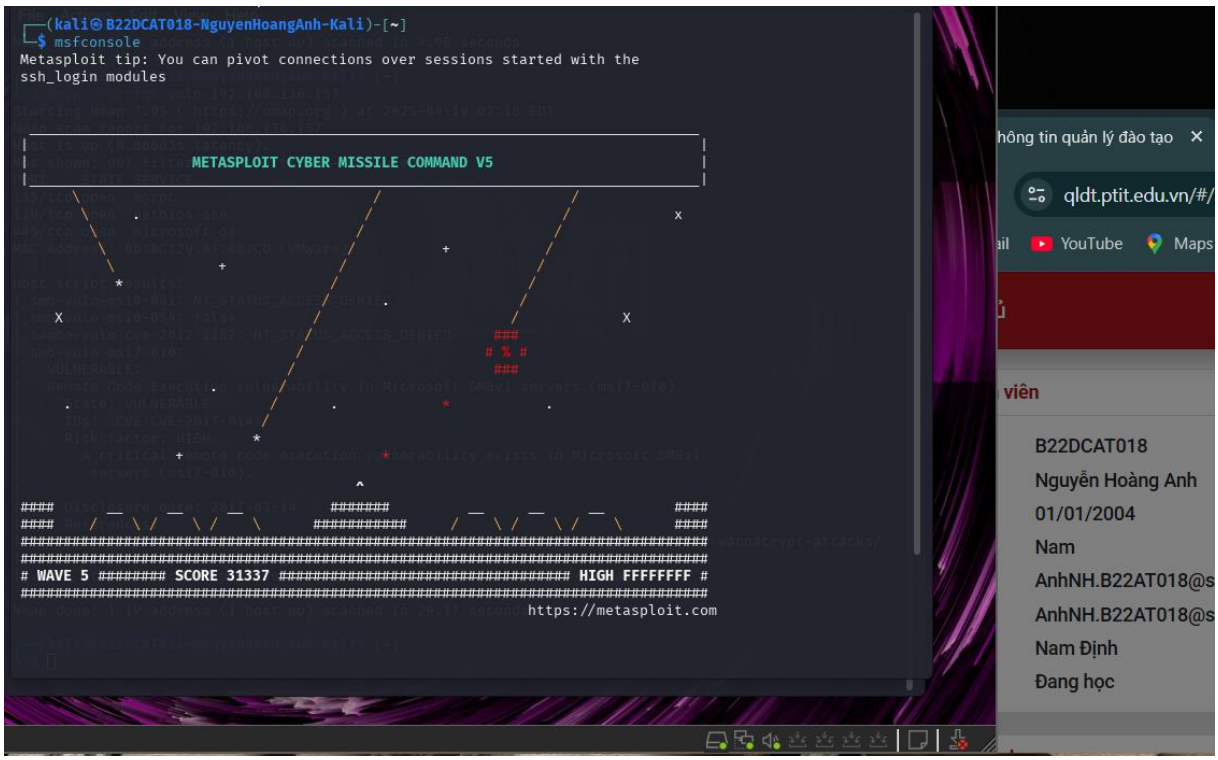
Sử dụng nmap để quét máy windows 7



Hình 23 - quét windows 7 bằng nmap

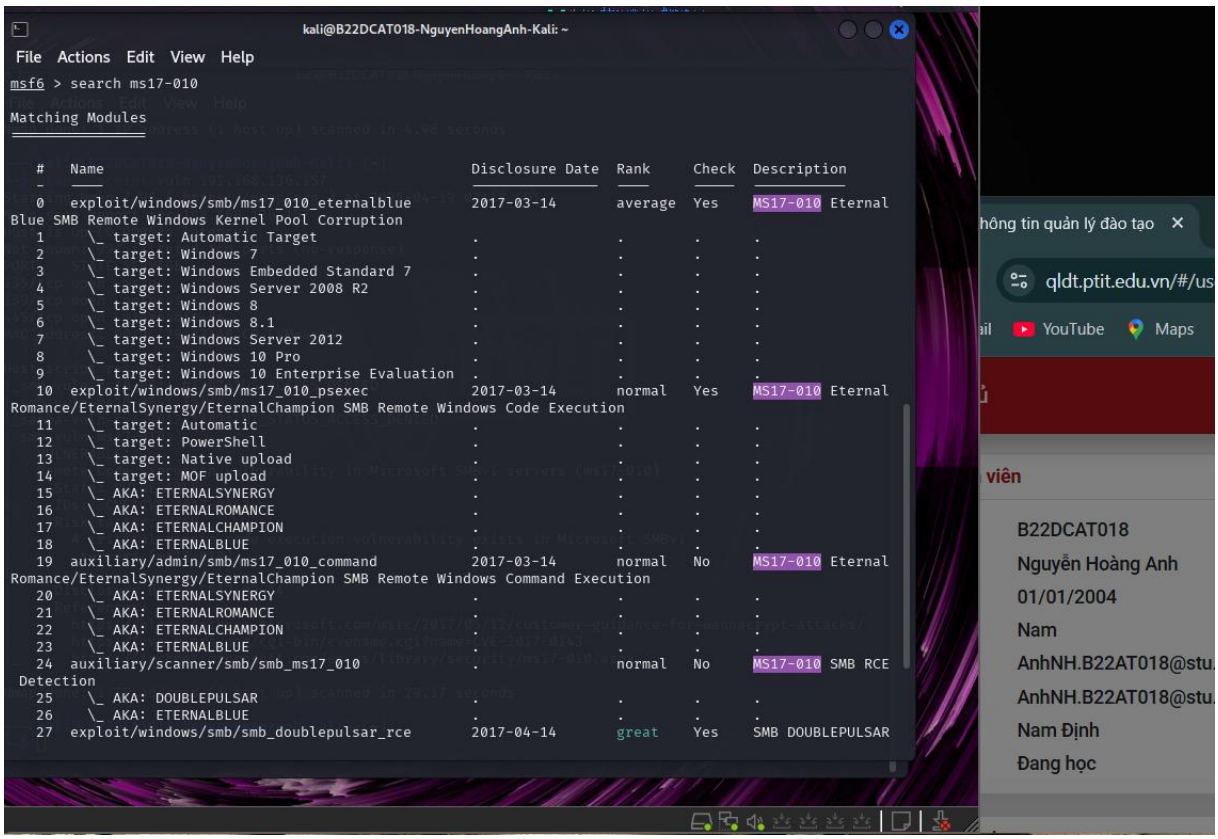
➔ Nhận thấy có thể khai thác lỗ hổng ms17-010

Khởi động metasploit trên máy kali với lệnh: *msfconsole*



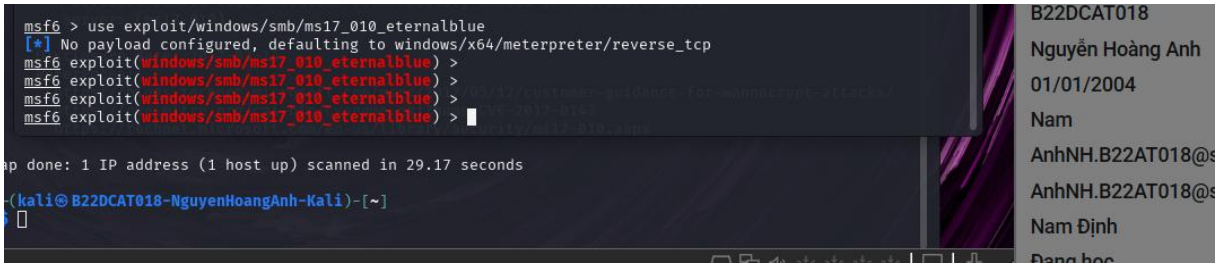
Hình 24 - khởi động metasploit

Sử dụng: *search <tên lỗ hổng>* để tìm kiếm tên chính xác của module tấn công



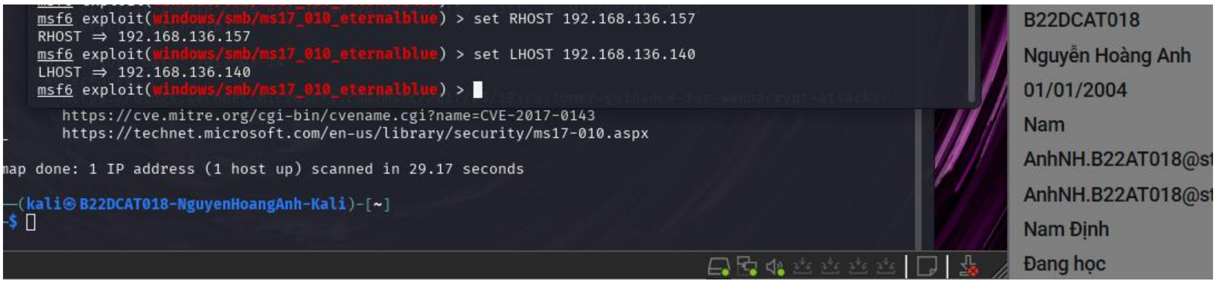
Hình 25 - tìm kiếm module tấn công

Lựa chọn sử dụng: *use <tên module>*



Hình 26 - lựa chọn lỗ hổng

Thiết lập các thông số tấn công cho mo-dun đã chọn:
Set RHOST <IP máy nạn nhân>
Set LHOST <IP máy tấn công>



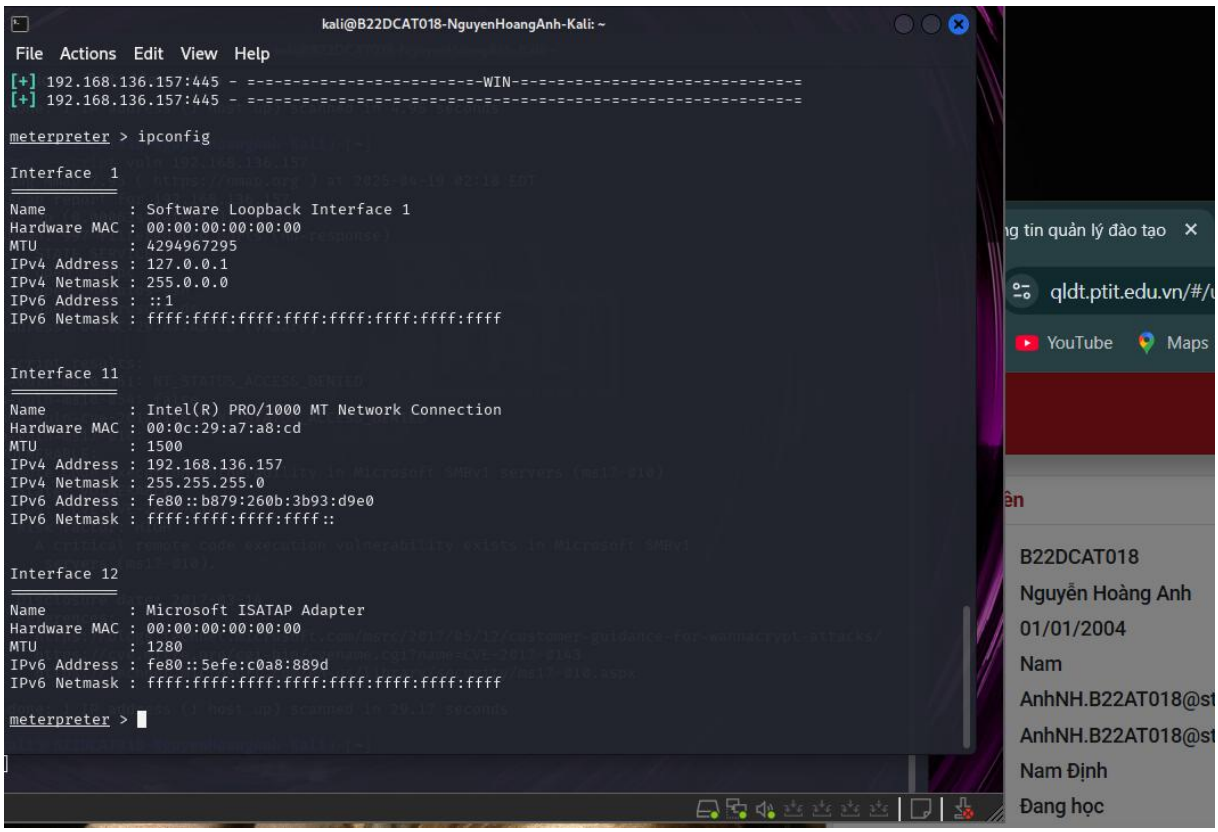
Hình 27 - thiết lập các thông số

Sau khi thiết lập xong, tấn công bằng lệnh: *exploit*

Hình 28 - thực hiện tấn công

➔ Kết quả: xâm nhập thành công vào máy windows 7

Sử dụng lệnh *ipconfig* để xem ip máy windows 7



Hình 29 - kiểm tra ip máy windows 7 vừa xâm nhập

Lệnh *sysinfo* để xem thông tin máy

Hình 30 - kiểm tra thông tin máy windows 7 vừa xâm nhập

TÀI LIỆU THAM KHẢO

1. Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
2. Tài liệu CEH, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
3. Lab 14 của CSSIA CompTIA Security+® Supported Labs