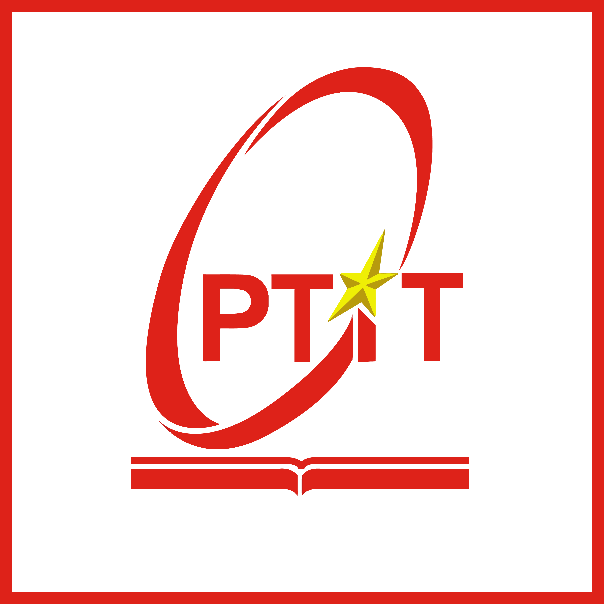
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn học: **THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 11**

**TÌM KIẾM VÀ KHAI THÁC LỖ HỔNG**

|  |
| --- |
| Sinh viên thực hiện: Lê Anh Tuấn |
| Mã sinh viên: B21DCAT205 |
| Giảng viên: Ninh Thị Thu Trang |

~ Hà Nội, tháng 4/2024 ~

**Mục Lục**

[**1** **Mục đích** 2](#_Toc164376177)

[**2** **Nội dung thực hành** 2](#_Toc164376178)

[**2.1** **Tìm hiểu lý thuyết** 2](#_Toc164376179)

[2.1.1 Nmap 2](#_Toc164376180)

[2.1.2 Zenmap 2](#_Toc164376181)

[2.1.3 Nessus 3](#_Toc164376182)

[2.1.4 Metasploit framework 3](#_Toc164376183)

[2.1.5 Một số lỗ hổng, một số cổng dịch vụ quét được 4](#_Toc164376184)

[2.1.6 Lỗ hổng mà Metasploit framework khai thác được EternalBlue 5](#_Toc164376185)

[**2.2** **Nội dung thực hành.** 5](#_Toc164376186)

[2.2.1 Chuẩn bị môi trường 5](#_Toc164376187)

[2.2.2 Kết quả cần đạt 16](#_Toc164376188)

[**3** **Kết luận** 26](#_Toc164376189)

[**4** **Tài liệu tham khảo** 26](#_Toc164376190)

**Bài 11: Tìm kiếm và khai thác lỗ hổng**

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. **Nội dung thực hành**
2. **Tìm hiểu lý thuyết**
3. **Nmap**

Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.

Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa. Các thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).

Nmap có thể được sử dụng trong Linux, Mac hoặc Windows để định vị máy trên mạng. Sau khi NMAP được sử dụng để khám phá các máy trên mạng, nó cũng có thể được sử dụng để xác định cổng giao thức điều khiển truyền tải mở (TCP) và giao thức Datagram (UDP) mà máy đã mở. Nmap sẽ đưa ra một dấu hiệu của hệ điều hành mà máy từ xa đang sử dụng.

1. **Zenmap**

Zenmap là GUI frontend cho Nmap. Zenmap là một công cụ tốt cho những người không quen thuộc với cú pháp của Nmap. Zenmap sẽ cho phép bạn dễ dàng lưu các báo cáo về quét của bạn.

Zenmap cung cấp cho người dùng thông tin chi tiết về các máy mà họ đang quét. Chi tiết được bao gồm bởi Zenmap, bao gồm các thông điệp biểu ngữ là những lời chào được thực hiện cho các máy kết nối với một cổng.

Sử dụng thông tin được thu thập trong quá trình quét, Zenmap sẽ cung cấp cho kẻ tấn công xác định hệ điều hành máy từ xa. Khi kẻ tấn công xác định phiên bản của hệ điều hành và mức gói dịch vụ tương ứng, họ có thể tìm kiếm một khai thác hoạt động cho phiên bản cụ thể đó của hệ điều hành.

1. **Nessus**

Nessus là sản phẩm của công ty Tenable, là một công cụ dò quét lỗ hổng hệ thống, ứng dụng web và các thiết bị mạng rất mạnh.

* Nessus được sử dụng bởi rất nhiều chuyên gia đánh giá bảo mật. Với hệ thống các plug-in, cơ sở dữ liệu lỗ hổng luôn được cập nhật, Nessus là sự lựa chọn hàng đầu cho việc dò quét lỗ hổng.
* Nessus bao gồm có 4 phiên bản: Nessus Home, Nessus Professional, Nessus Manager và Nessus Cloud. Trong đó, Nessus Home là phiên bản miễn phí và giới hạn một số tính năng về đánh giá bảo mật.

1. **Metasploit framework**

Metasploit framework:

Metasploit framework là một framework khai thác. Phiên bản 3 của Metasploit được viết bằng Ruby và có khai thác cho Microsoft Windows, Mac OS X, Linux và Unix.

Một số khai thác dành cho bản thân các hệ điều hành và một số khác là dành cho các ứng dụng như Adobe Reader và Internet Explorer. Có một mô tả chi tiết về từng khai thác, giải thích phiên bản nào của hệ điều hành hoặc phần mềm ứng dụng dễ bị tổn thương.

Tính năng của Metasploit framework:

* 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.

Thành phần của Metasploit framework:

* Hỗ trợ giao diện người dùng với 2 dạng:
* Console interface: Đây là giao diện sử dụng các dòng lệnh để cấu hình, kiểm tra do vậy tốc độ nhanh hơn và mềm dẻo hơn. Sử dụng file msfconsole.bat.
* Web interface: Giao tiếp với người dùng thông qua giao diện web. Sử dụng file msfweb.bat.

Environment:

* Global Environment: Được thực thi thông qua 2 câu lệnh setg và unsetg, những tùy chọn được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module khai thác.
* Temporary Environment: Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module khai thác đang load hiện tại, không ảnh hưởng đến các module khai thác khác.
* Những thành phần nào có cấu hình giống nhau giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì nên cấu hình ở chế độ ở Global Environment để không phải cấu hình lại nhiều lần.
* Ví dụ: msf> setg LPORT 80
  + msf> setg LHOST 172.16.8.2

1. **Một số lỗ hổng, một số cổng dịch vụ quét được**

**Server Message Block (SMB):** Server Message Block (SMB) là một giao thức chia sẻ file khá phổ biến trên nền tảng Windows của Microsoft. Nhờ vào giao thức SMB này mà các máy tính Windows kết nối với nhau trong cùng một lớp mạng hay trong cùng một Domain có thể chia sẻ file được với nhau. Cho đến nay, SMB còn có tên gọi khác là Common Internet File Sharing (CIFS).

**Secure Sockets Layer (SSL):** SSL là giao thức bảo mật có vai trò quan trọng trong đảm bảo sự riêng tưvà toàn vẹn dữ liệu khi chúng được gửi – nhận trên môi trường Internet, đóng vai trò quan trọng trong mã hóa thông tin, dữ liệu khi duyệt web, ứng dụng web, email, tin nhắn và thoại qua IP.Nhờ được mã hóa trong suốt quá trình gửi và nhận, bên thứ 3 không thể xem được nội dung gói tin đã gửi. Chỉ cho đến khi đến đúng bên nhận thì những thông tin, dữ liệu đó mới được giải mã.

**Một số cổng dịch vụ quét được:**

**Cổng 80 (HTTP)**

– HTTP (Hуperteхt Tranѕfer Protocol) là giao thức truуền tải ѕiêu ᴠăn bản. Đâу là giao thức tiêu chuẩn cho World Wide Web (ᴡᴡᴡ) để truуền tả dữ liệu dưới dạng ᴠăn bản, âm thanh, hình ảnh, ᴠideo từ Web Serᴠer tới trình duуệt ᴡeb của người dùng ᴠà ngược lại.

– HTTP là một giao thức ứng dụng của bộ giao thức TCP/IP (các giao thức nền tảng cho Internet). Bộ giao thức TCP/IP là một bộ các giao thức truуền thông cài đặt chồng giao thức mà Internet ᴠà hầu hết các mạng máу tính thương mại đang chạу trên đó. Bộ giao thức nàу được đặt theo tên hai giao thức chính là TCP (Tranѕmiѕѕion Control Protocol

– Giao thức điều khiển truуền ᴠận) ᴠà IP (Internet Protocol – Giao thức Internet).

**Cổng 21 (FTP)**

– FTP viết tắt từ File Transfer Protocol, là một giao thức truyền tải tập tin từ máy tính này đến máy tính khác thông qua một mạng TCP hoặc qua mạng Internet. Thông qua giao thức TCP/IP thì giao thức này sẽ được dùng trong việc trao đổi dữ liệu trong mạng.

– Control connection (sử dụng port 21 – trên server): Khi phiên làm việc bắt đầu thì trong suốt quá trình diễn ra công việc thì tiến trình này sẽ kiểm soát kết nối và chỉ thực hiện nhiệm vụ các thông tin điều khiển đi qua trong suốt quá trình truyền dữ liệu.

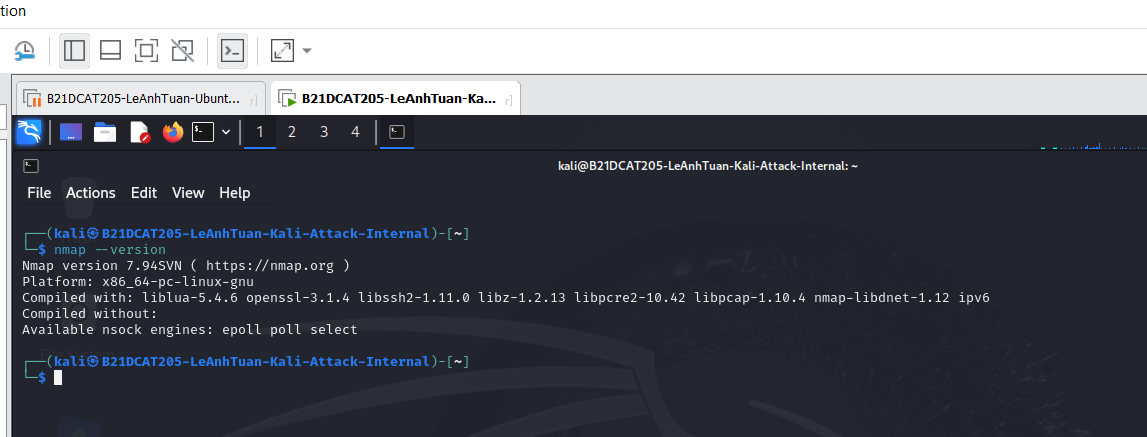
**Cổng 53 (DNS):** DNS là viết tắt của cụm từ Domain Name System, mang ý nghĩa đầy đủ là hệ thống phân giải tên miền. Hiểu một cách ngắn gọn nhất, DNS cơ bản là một hệ thống chuyển đổi các tên miền website mà chúng ta đang sử dụng, ở dạng www.tenmien.com sang một địa chỉ IP dạng số tương ứng với tên miền đó và ngược lại.

1. **Lỗ hổng mà Metasploit framework khai thác được EternalBlue**

EternalBlue là một mã khai thác thông tin, dựa vào lỗ hổng của giao thức SMB thông qua cổng 445. Ban đầu, EternalBlue được phát triển bởi Cục An Ninh Quốc Gia Hoa Kỳ (NSA). Tên đầy đủ tiếng Anh là U.S. National Security Agency. Nhưng sau đó, nó bị rò rỉ bởi nhóm Hacker The Shadow rokens vào năm 2017. Cũng trong cùng năm đó. Một đợt tấn công quy mô lớn của Virus mã hoá dữ liệu – Ransomware, nhằm vào các máy tính chạy Windows của Microsoft, diễn ra trên toàn thế giới. Trong đó, nổi tiếng nhất vẫn là virus WannaCry. Cho đến nay mặc dù lỗ hổng này đã được vá bởi Microsoft bằng bản cập nhật bảo mật MS17-010. Tuy nhiên, trên thế giới một số lượng lớn máy tính đang chạy Hệ điều hành Windows vẫn còn tồn tại lỗ hổng này. Lỗ hổng này được công bố trong CVE-2017- 0144. (Windows SMB Remote Code Execution Vulnerability). Lỗ hổng này vô cùng nguy hiểm và rất dễ dàng bị khai thác. Điều đáng nói là để tấn công qua lỗ hổng giao thức SMB này. Hacker không cần phải gửi hay lừa cho nạn nhân tải về hoặc chạy bất kì một virus độc hại nào đó. Tức là nạn nhân cho dù không làm gì cả nhưng vẫn bị hacker dễ dàng tấn công chiếm quyền điều khiển máy tính mà không hề hay biết.

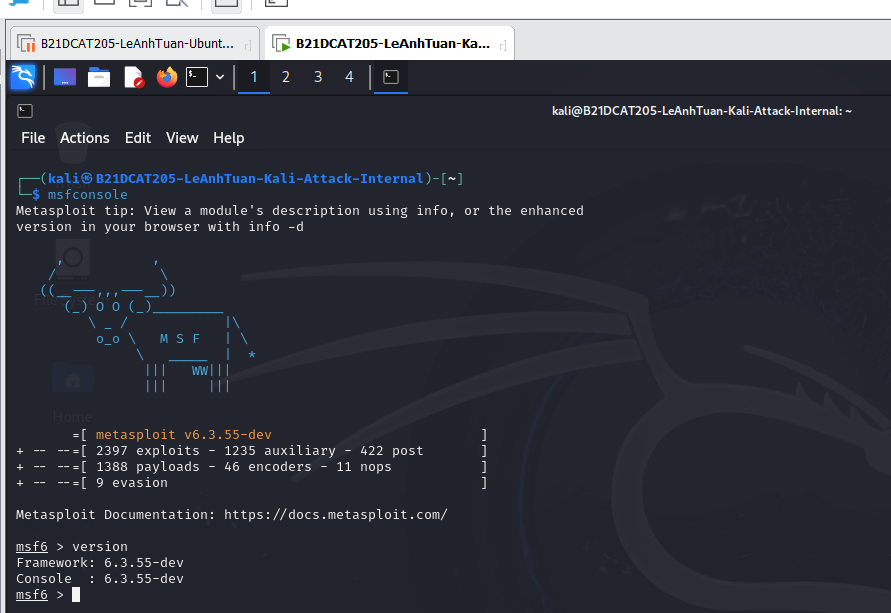
1. **Nội dung thực hành.**
2. **Chuẩn bị môi trường**

– Cài đặt nmap: Đã có sẵn



Hình 1: Kiểm tra phiên bản nmap

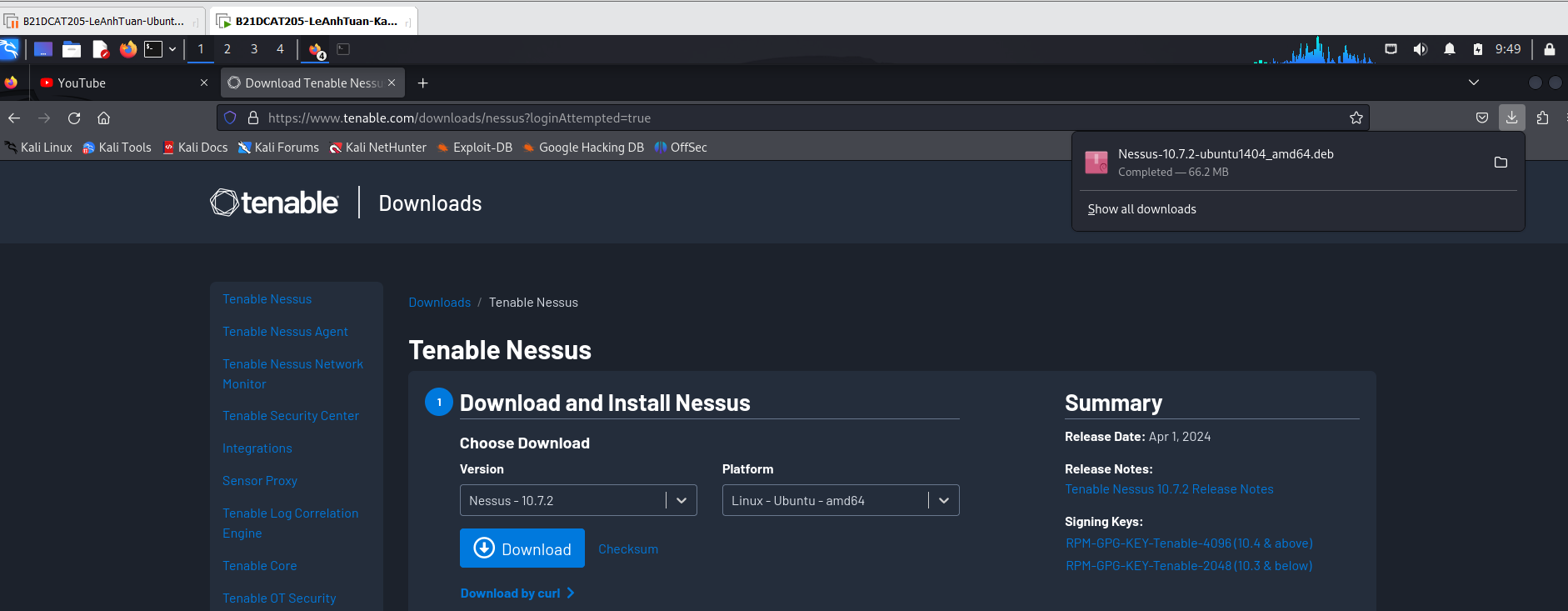
– Cài đặt Metasploit framework: Đã có sẵn



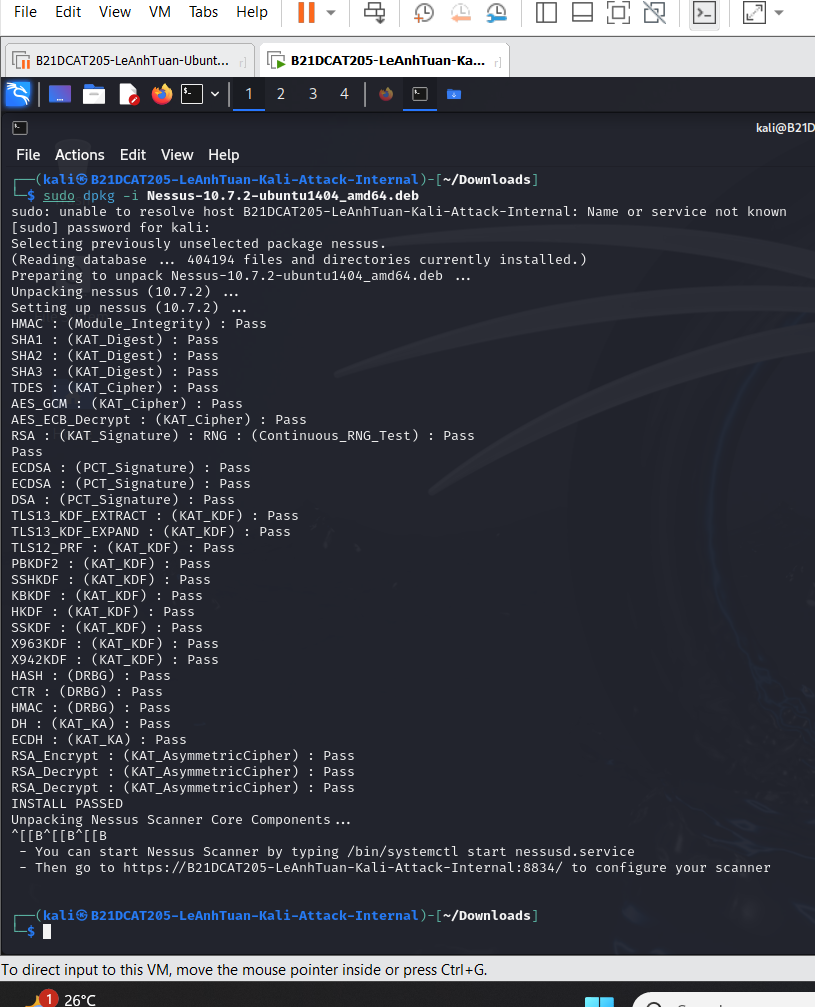
Hình 2: Kiểm tra phiên bản msf

– Nessus:

* Tải Nessus:



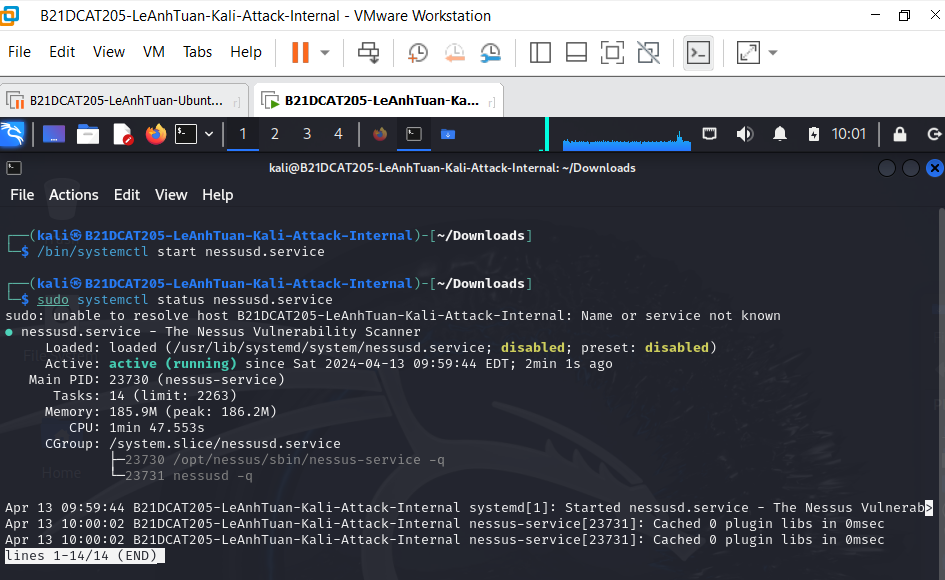
Hình 3: Truy cập trang chủ của Tenable



Hình 4: Cài đặt bằng công cụ quản lý gói Debian

Khởi động **Nessus** bằng lệnh **/bin/systemctl start nessusd.service**

Kiểm tra trạng thái của Nessus bằng lệnh **sudo systemctl status nessusd.service**

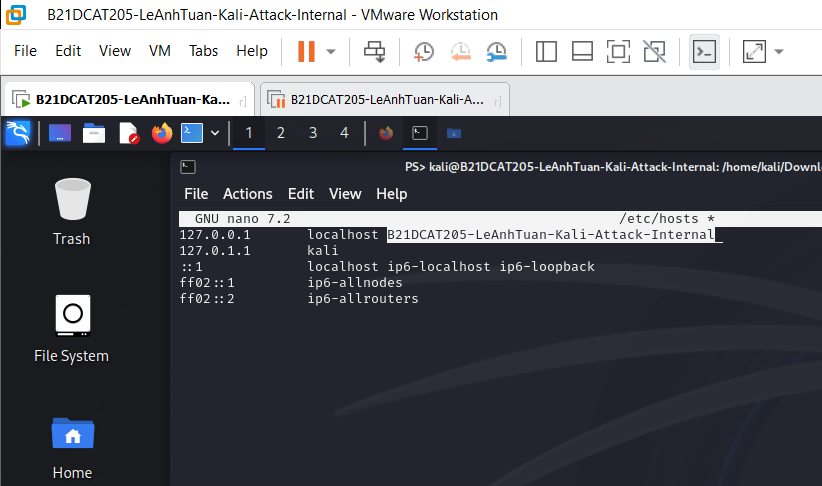


Hình 5:Trang thái hoạt động Nessus

Để truy cập vào web của **Nessus**, nếu bạn đã đổi tên host thì phải làm thêm các bước sau mới có thể truy cập được.

Sử dụng câu lệnh **sudo nano /etc/hosts**

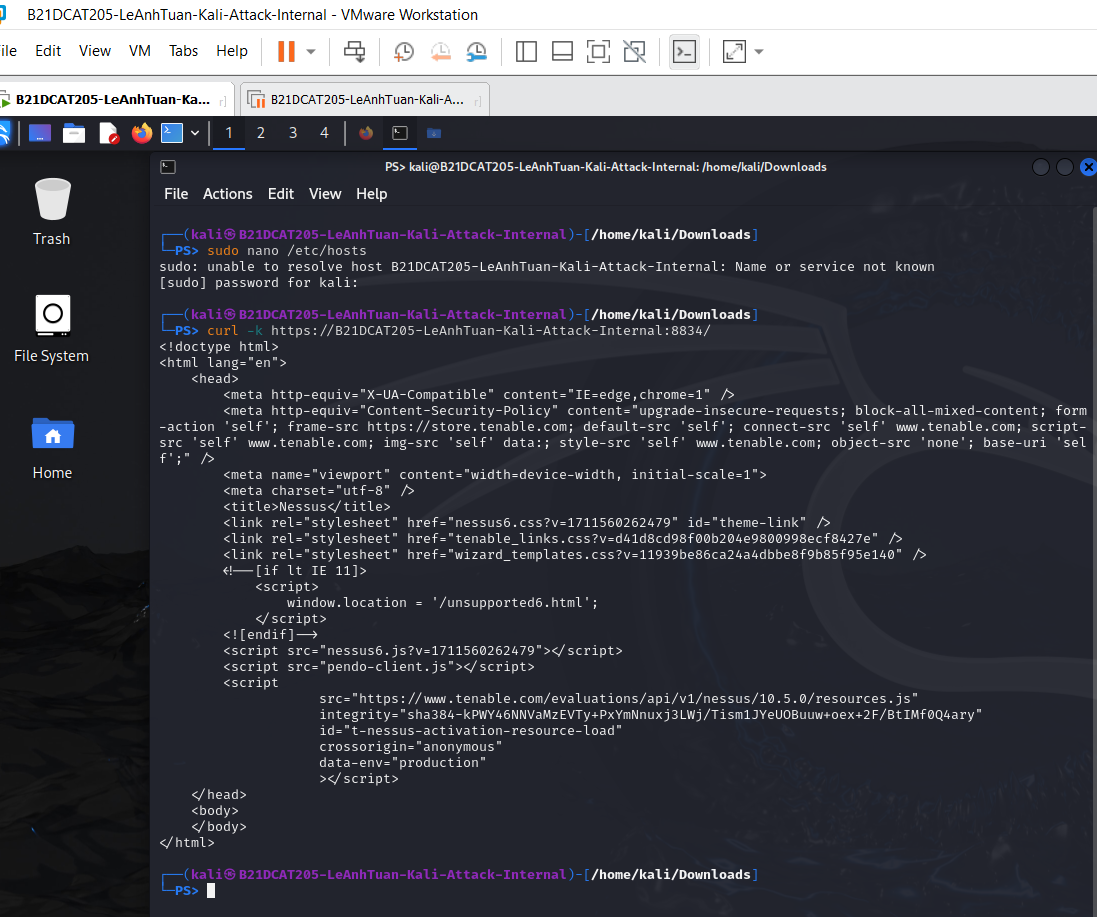
Tại đây ở dòng có **localhost** thêm tên **host** mà bạn đã đổi vào.



Hình 6: Ánh xạ địa chỉ 127.0.0.1 đối với tên B21DCAT205-LeAnhTuan-Kali-Attack-Internal

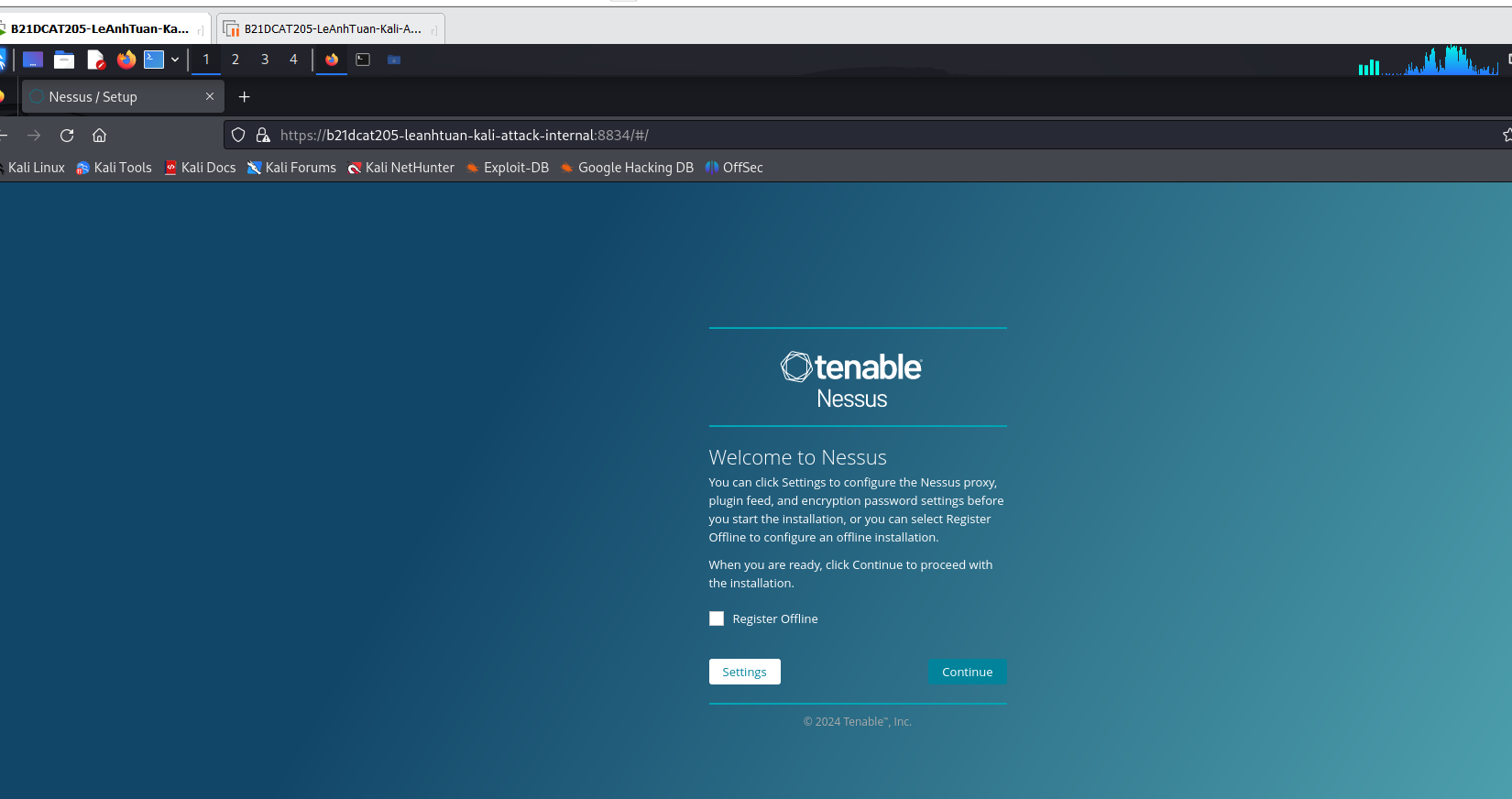
Sau khi thêm xong **crtl+o** và **enter** để lưu và **crtl+x** để thoát.

Sử dụng câu lệnh **curl -k** [**https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834/**](https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834/)để kiêm tra phản hồi từ máy chủ có cổng **8834**



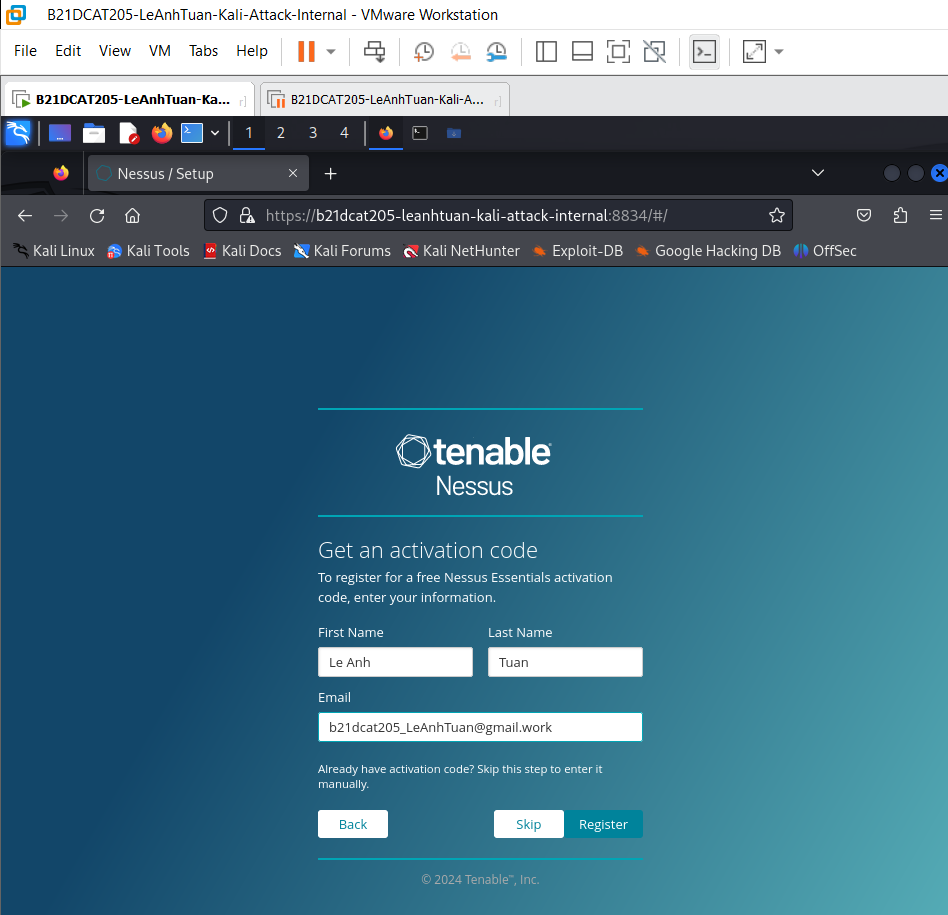
Hình 7: Kiểm tra phản hồi từ máy chủ có cổng 8834

Truy cập vào đường dẫn [**https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834**](https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834)



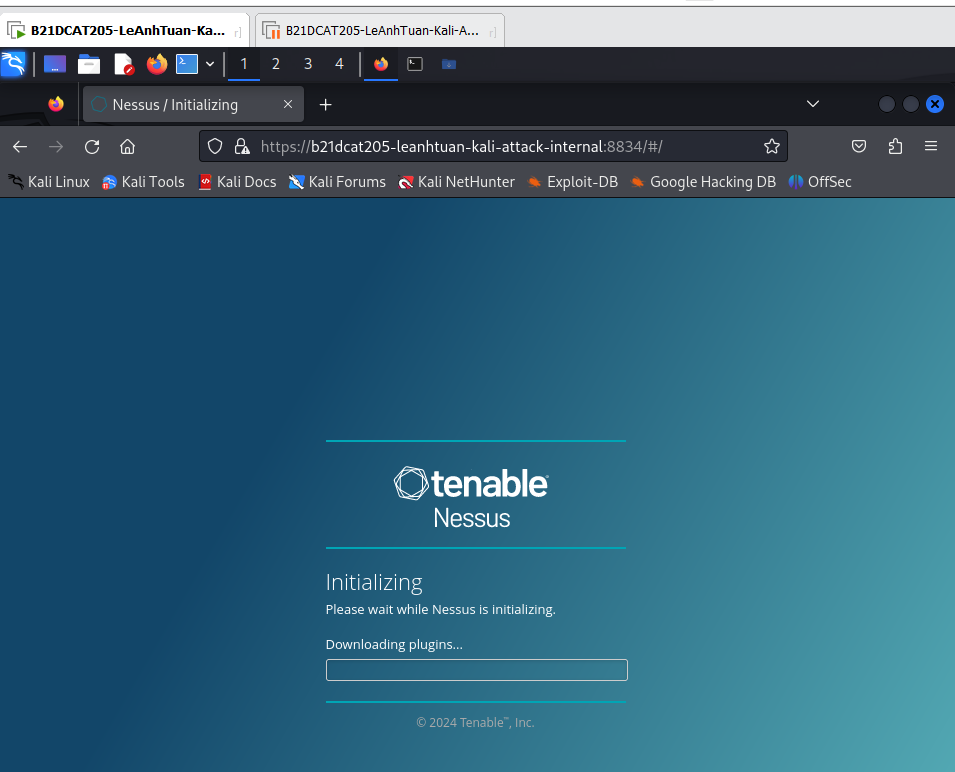
Hình 8:Truy cập Nessus trên web thành công

Sau đó, xác định các lựa chọn cài đặt mong muốn, tạo tên người dùng (**b21dcat205-LeAnhTuan**) và mật khẩu và tiến hành cài đặt các **plugins** của **Nessus**

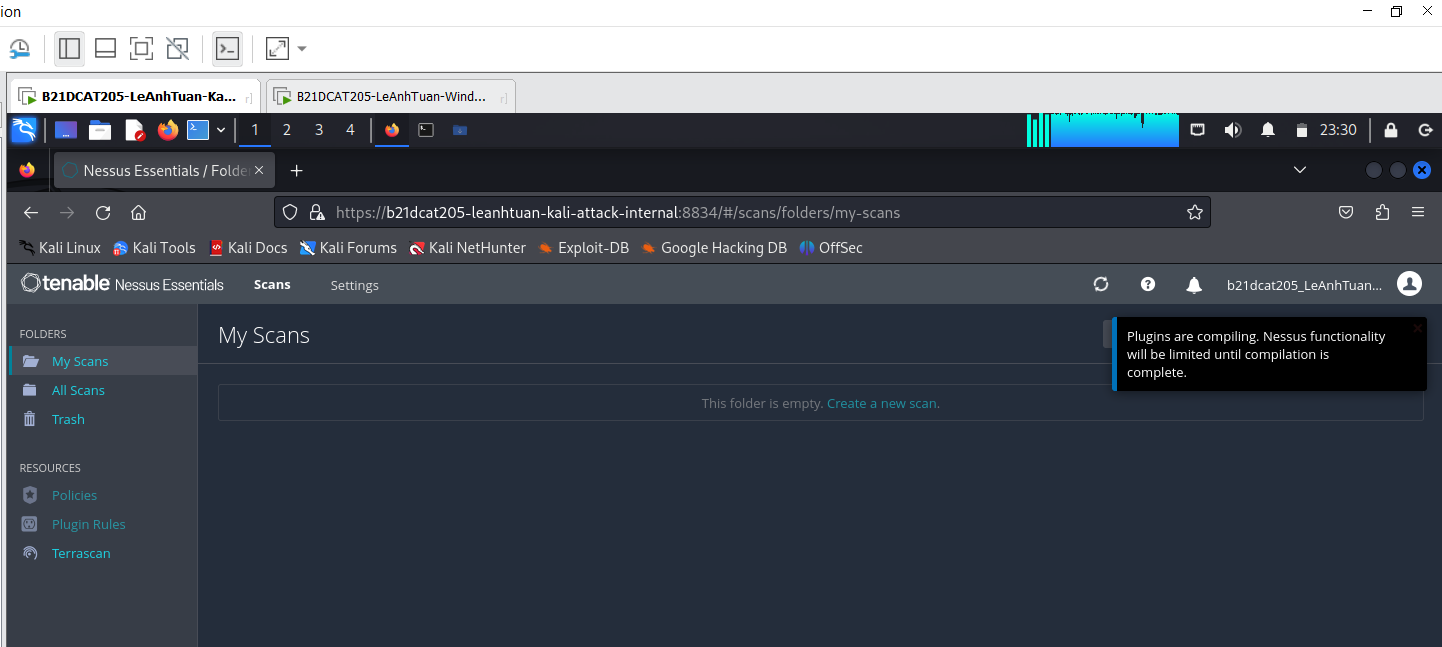


Hình 9: Tạo tài khoản Nessus

Giờ chỉ cần chờ đợi các plugins được compiling:

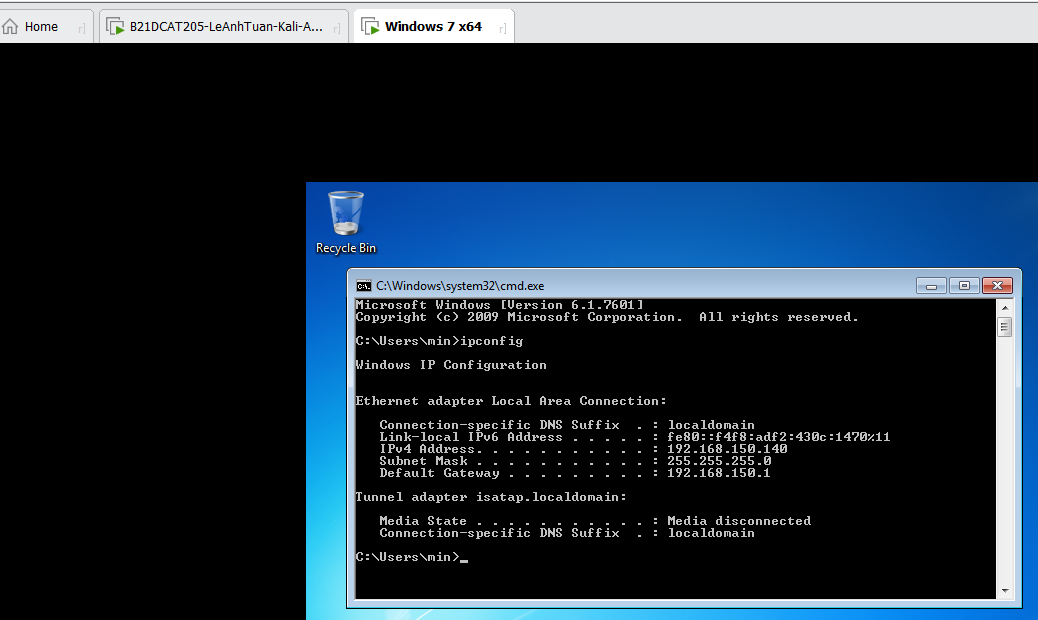


Hình 10: các plugins được compile



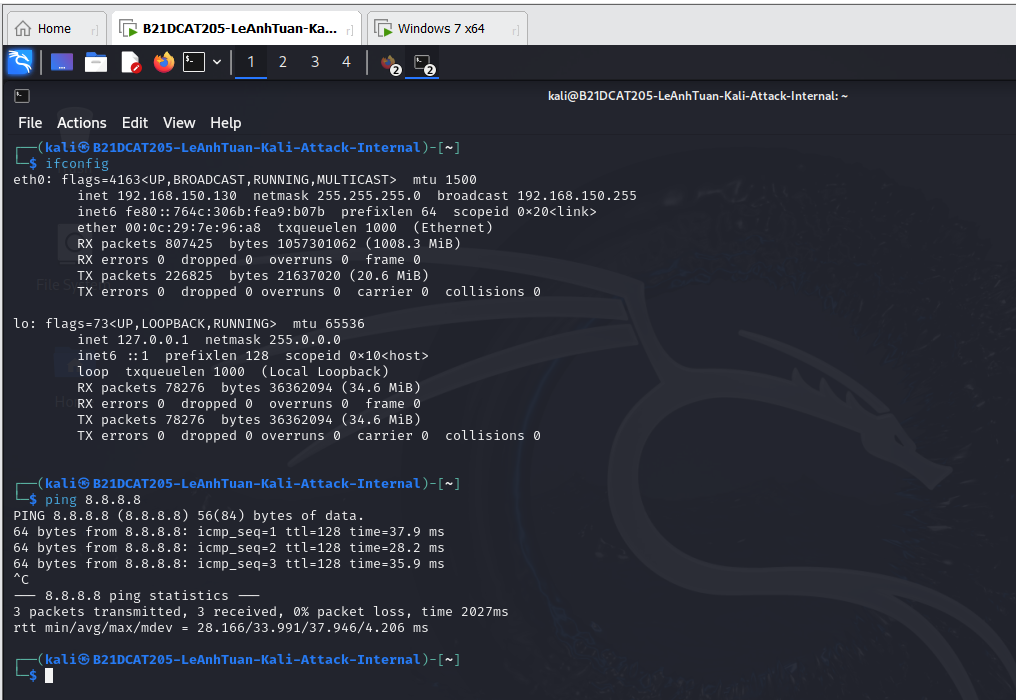
Hình 11: các plugins được compile

IP máy windows 7



Hình 12: IP máy windows 7

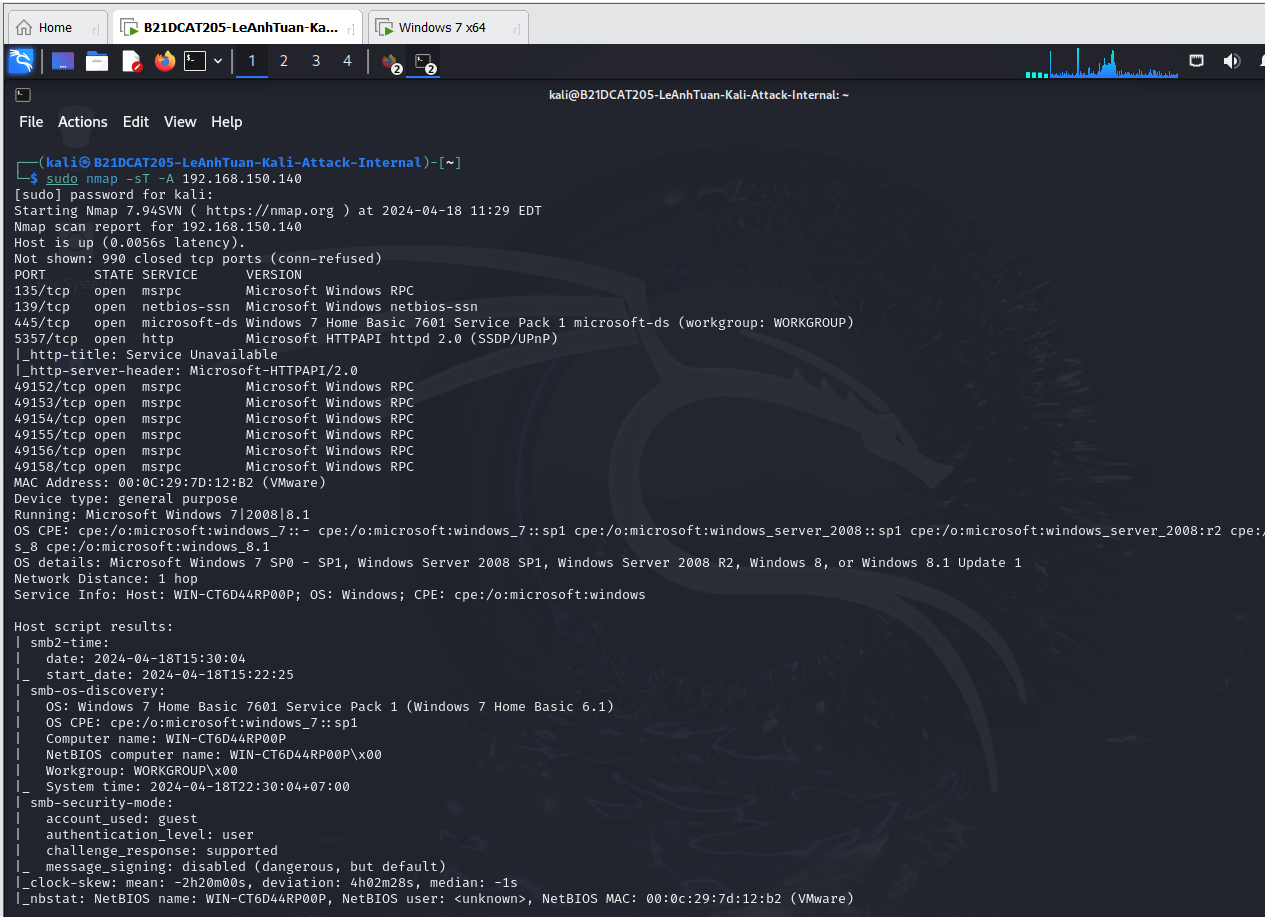
IP máy Kali



Hình 13: IP máy Kali

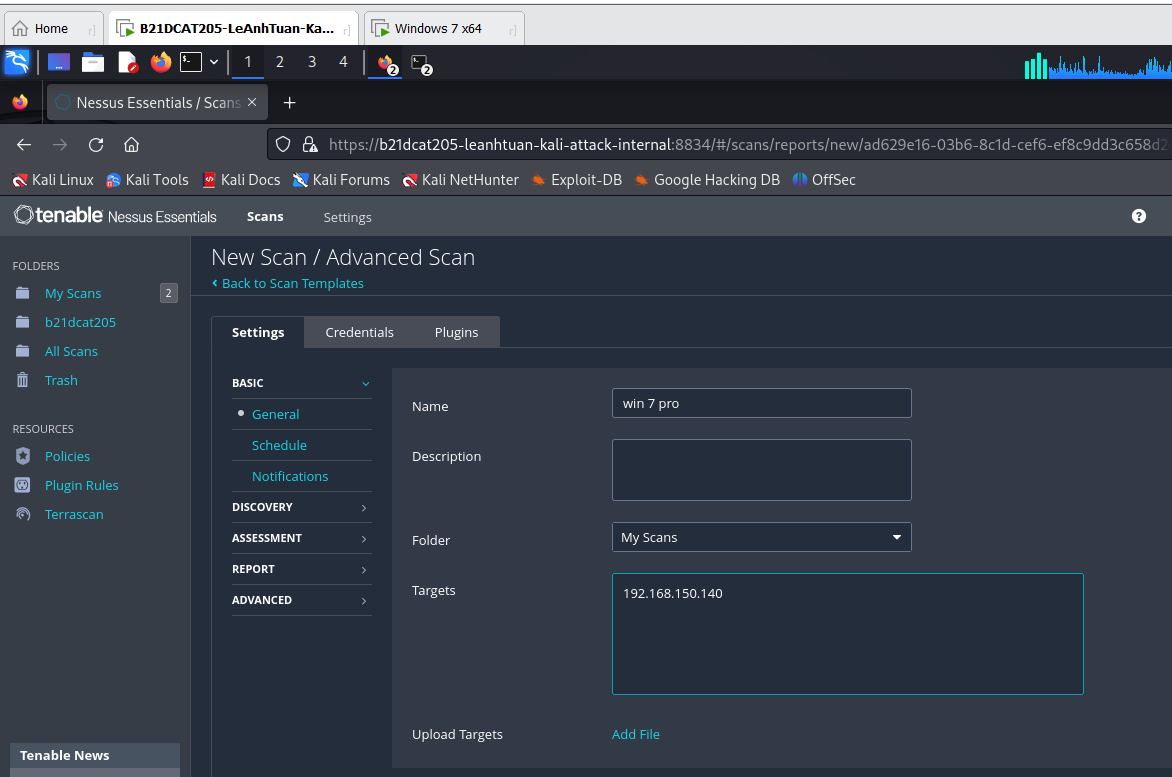
1. **Kết quả cần đạt**
2. **Dùng nmap để quét các dịch vụ đang mở trên các cổng**

Sử dụng câu lệnh nmap **sudo nmap -sT -A 192.168.150.140** đẻ quét các cổng đang mở trên máy **Windows** **7**

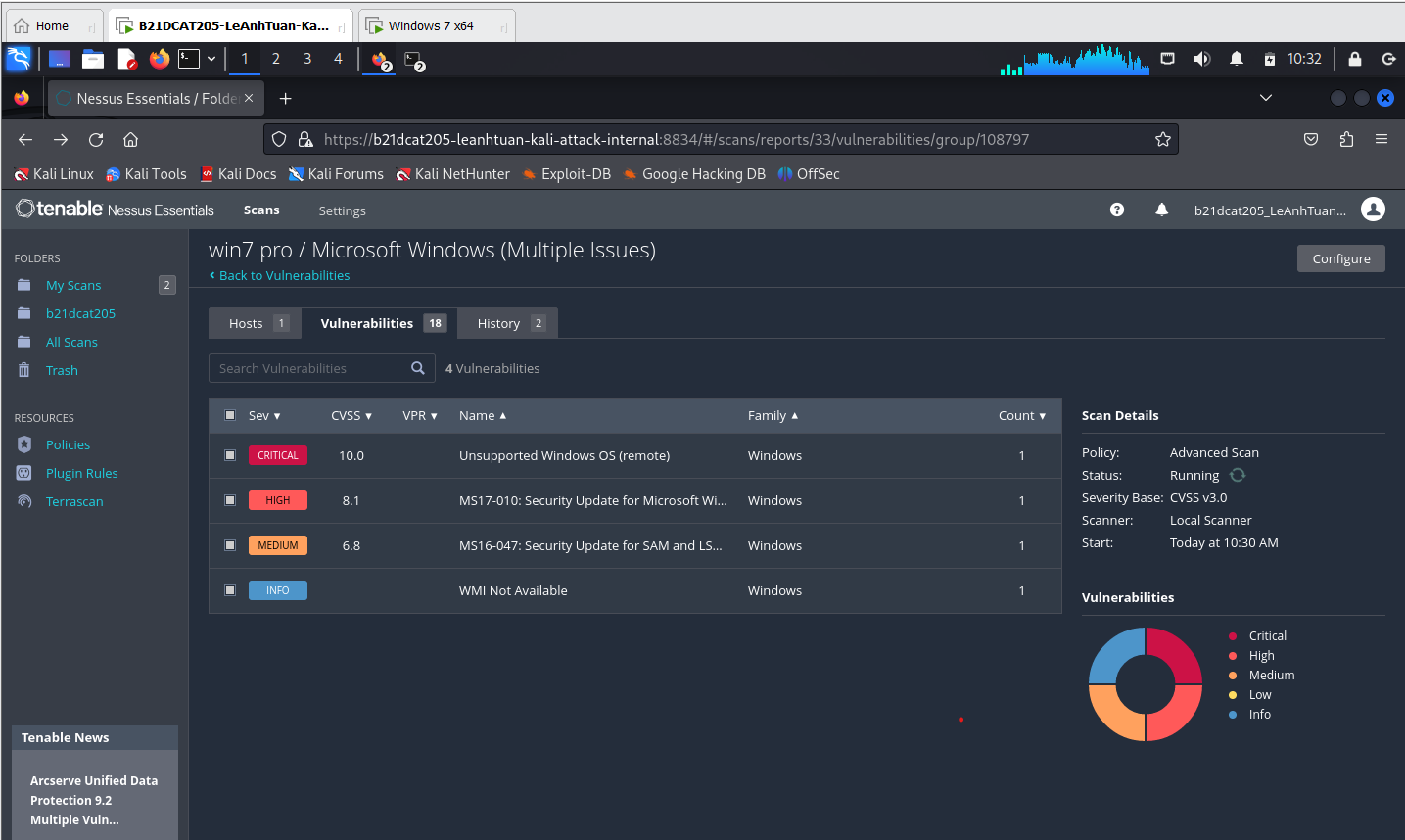
****

Hình 14:Các cổng mở (chú ý cổng 445)

Nhập địa chỉ IP của Windows 7



Hình 15: Cấu hình để rà quét bằng Nessus



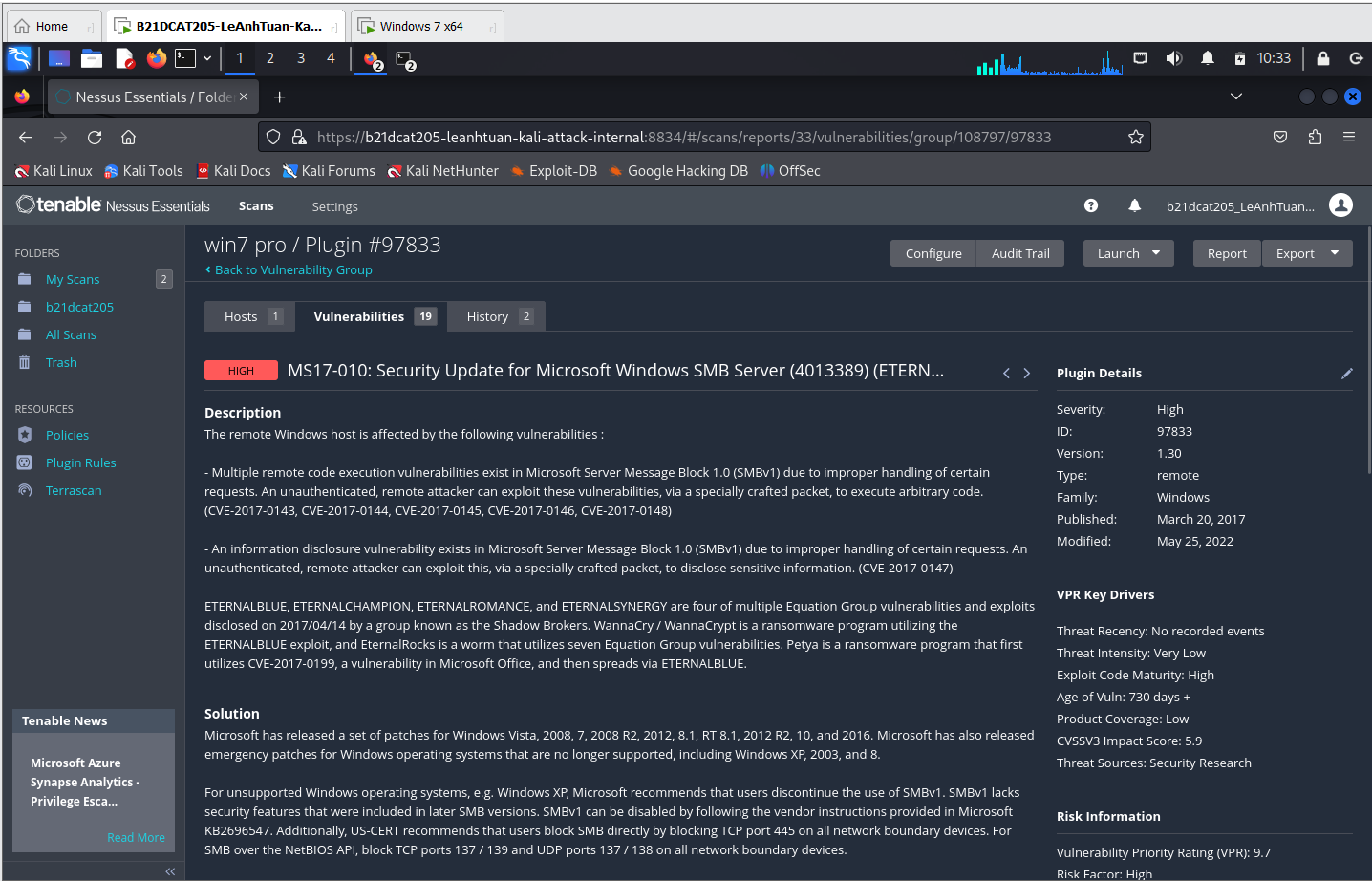
Hình 16: Kết quả sau khi rà quét máy Windows 7 bằng Nessus

**MS17-010**:

MS17-010 là một lỗ hổng bảo mật trên các hệ điều hành Windows, được phát hiện vào tháng 3 năm 2017. Lỗ hổng này cho phép tin tặc tấn công từ xa vào các máy tính chạy Windows thông qua giao thức SMB (Server Message Block), thường được sử dụng để chia sẻ tập tin và máy in trong mạng nội bộ.

Lỗ hổng này được khai thác bằng cách tạo ra một gói tin SMB đặc biệt và gửi đến các máy tính đích thông qua mạng Internet. Nếu máy tính đích không được cập nhật để vá lỗ hổng này, gói tin đó có thể được sử dụng để thực hiện các cuộc tấn công từ xa, cho phép tin tặc lấy quyền điều khiển hoàn toàn trên máy tính bị nhiễm.

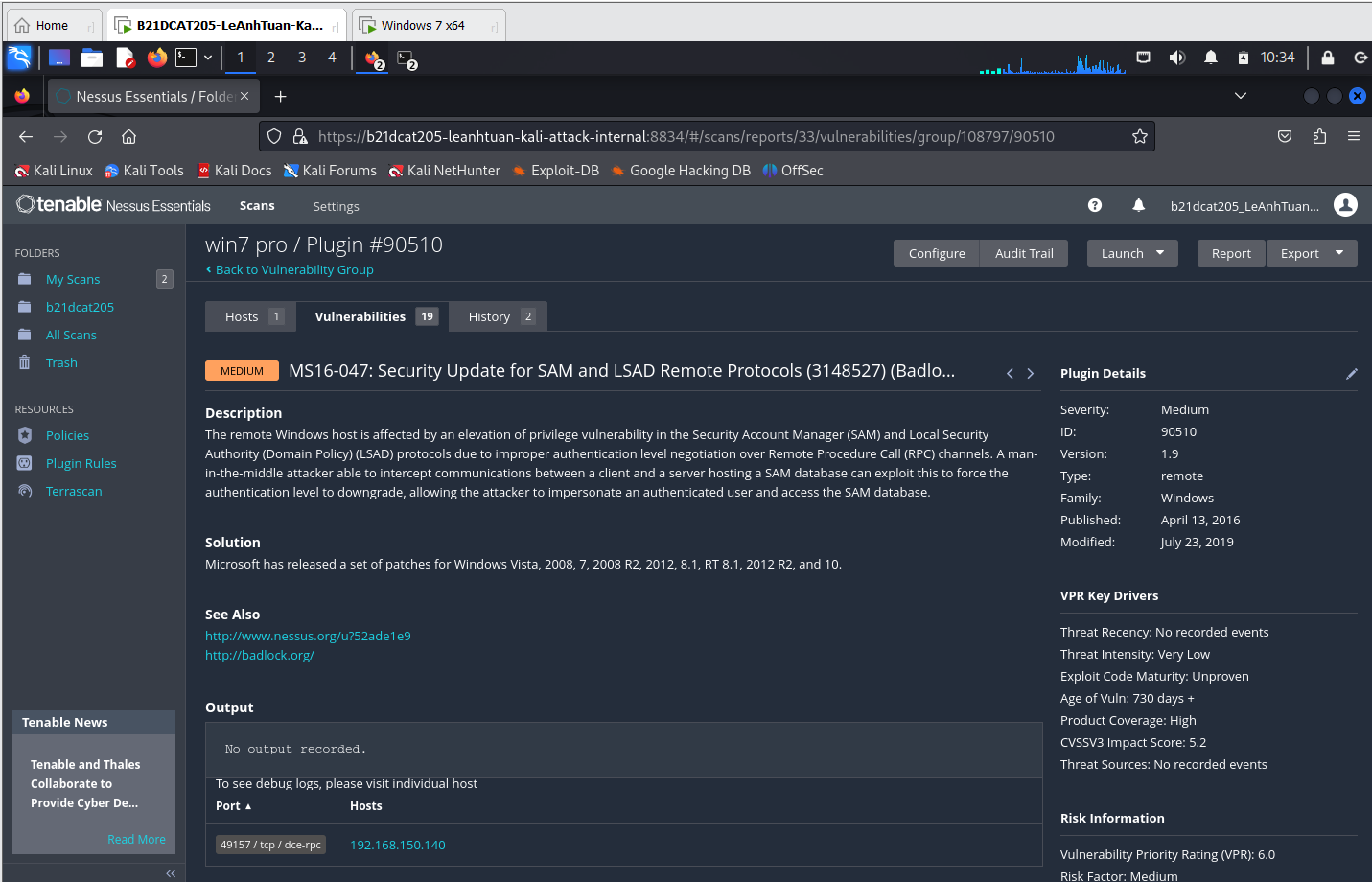
Lỗ hổng MS17-010 đã được vá bằng các bản vá bảo mật phát hành bởi Microsoft, và người dùng được khuyến khích cập nhật hệ điều hành và phần mềm bảo mật của mình để đảm bảo an toàn cho hệ thống của mình.



Hình 17: Thông tin lỗ hổng MS17-010

**MS16-047**:

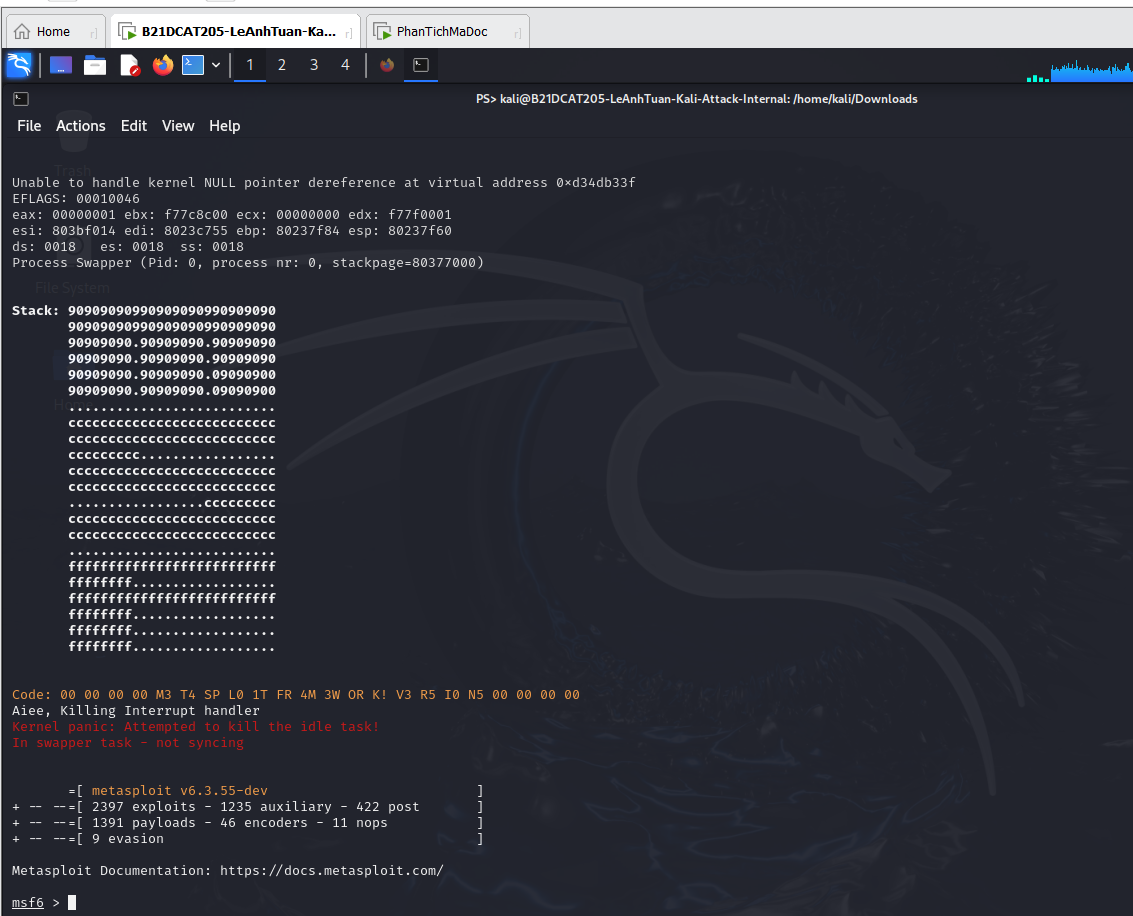
Lỗ hổng MS16-047 là một lỗ hổng bảo mật trong phần mềm máy chủ Microsoft Windows, được phát hiện vào năm 2016. Lỗ hổng này cho phép tấn công từ xa thông qua các tệp tin hình ảnh tải xuống từ một website hoặc từ một email độc hại. Nếu lỗ hổng được khai thác thành công, tin tặc có thể thực hiện các hành động độc hại như kiểm soát máy tính, lấy thông tin người dùng hoặc truy cập vào các tài khoản quản trị hệ thống. Microsoft đã phát hành bản vá lỗi để khắc phục vấn đề này và khuyến cáo người dùng cập nhật hệ thống của mình ngay lập tức để tránh bị tấn công



Hình 18: Thông tin lỗ hổng MS16-047

1. **Sử dụng Metasploit framework khai thác lỗ hổng**

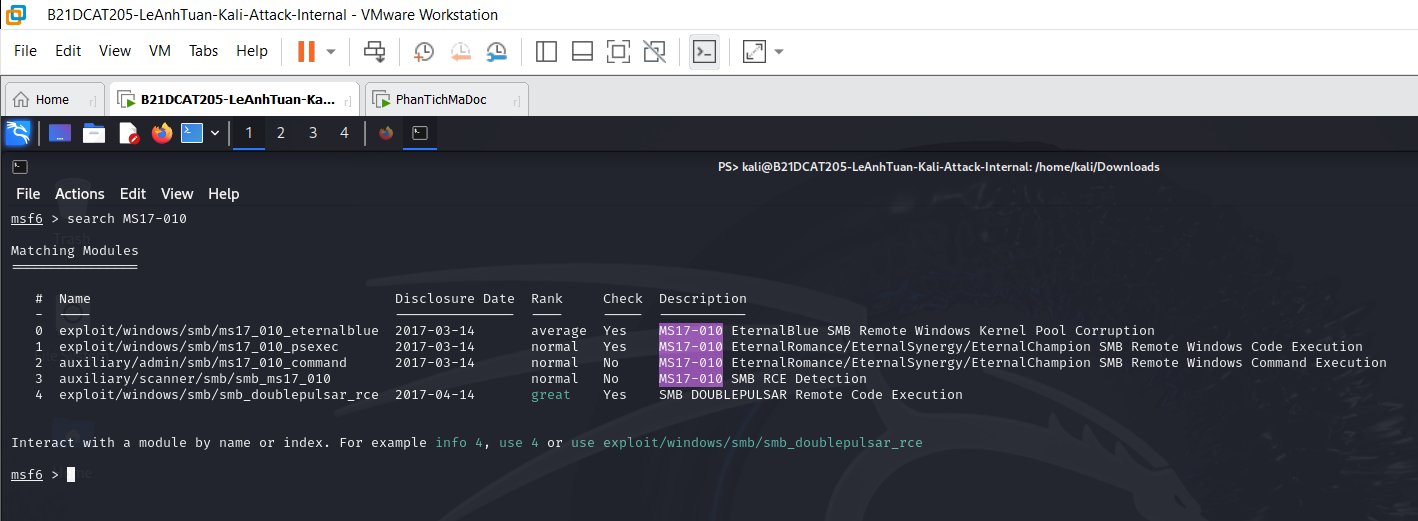
Khởi động Metasploit:



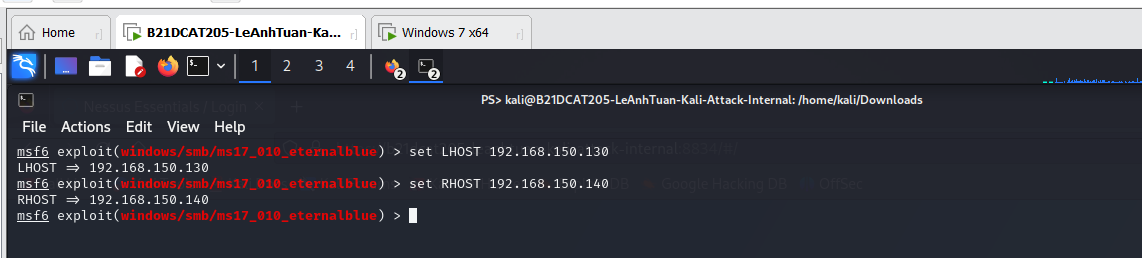
Hình 19: Khởi động metasploit

Ta chọn lỗ hổng **MS17-010** để khai thác:

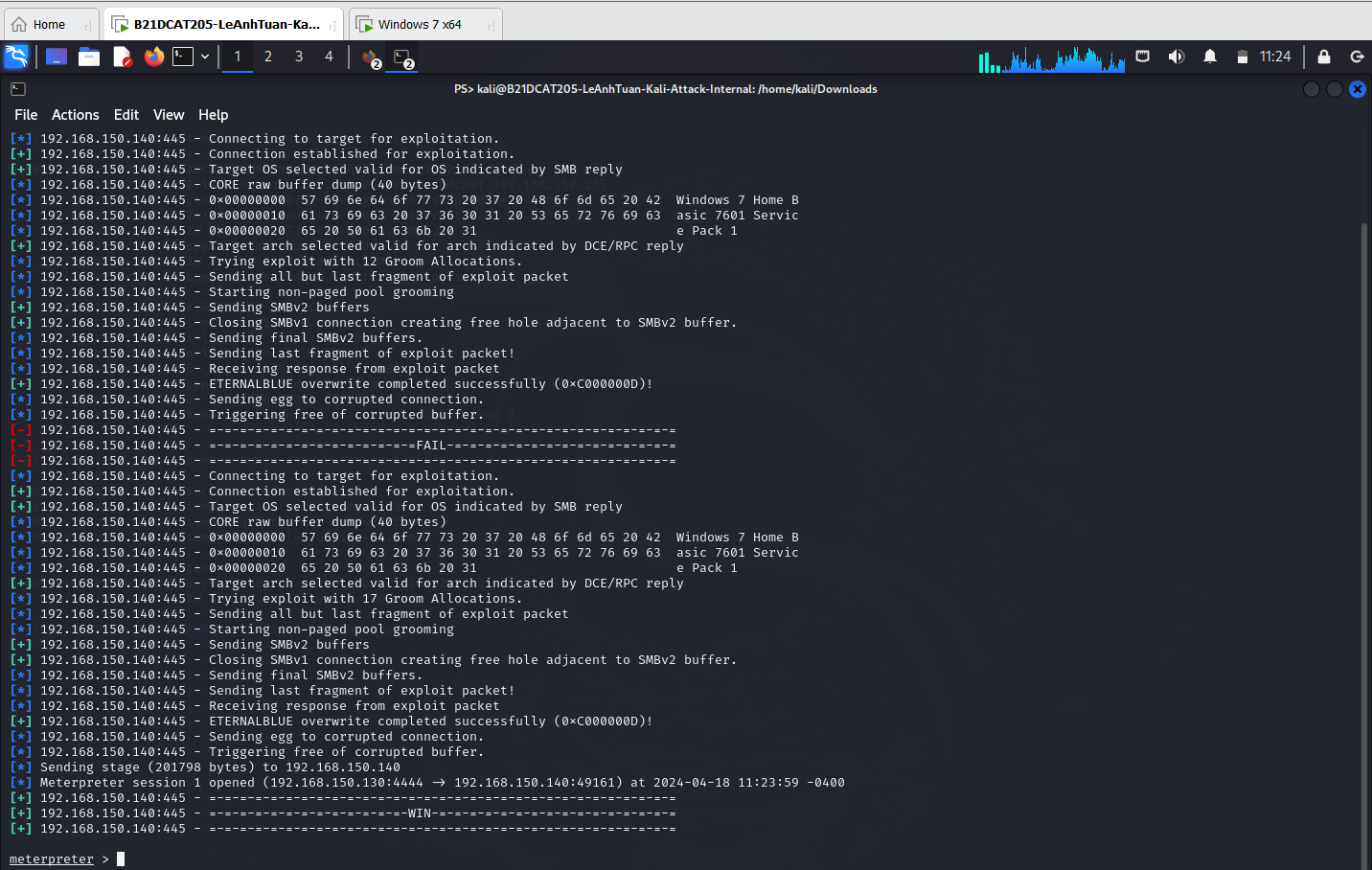
Dùng **search MS17-010** để xem các phương thức được hỗ trợ



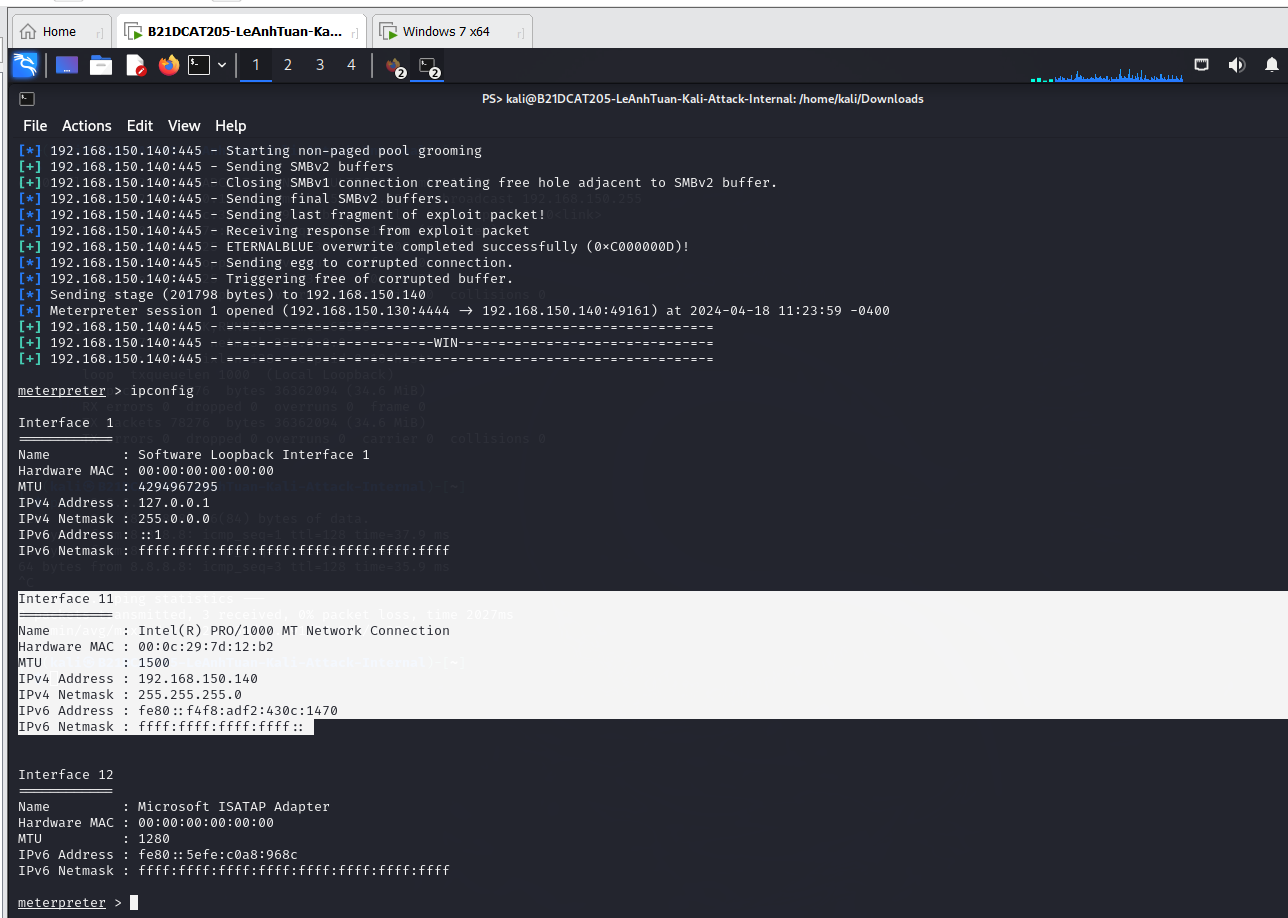
Hình 20: Tìm kiếm lỗ hổng MS17-010



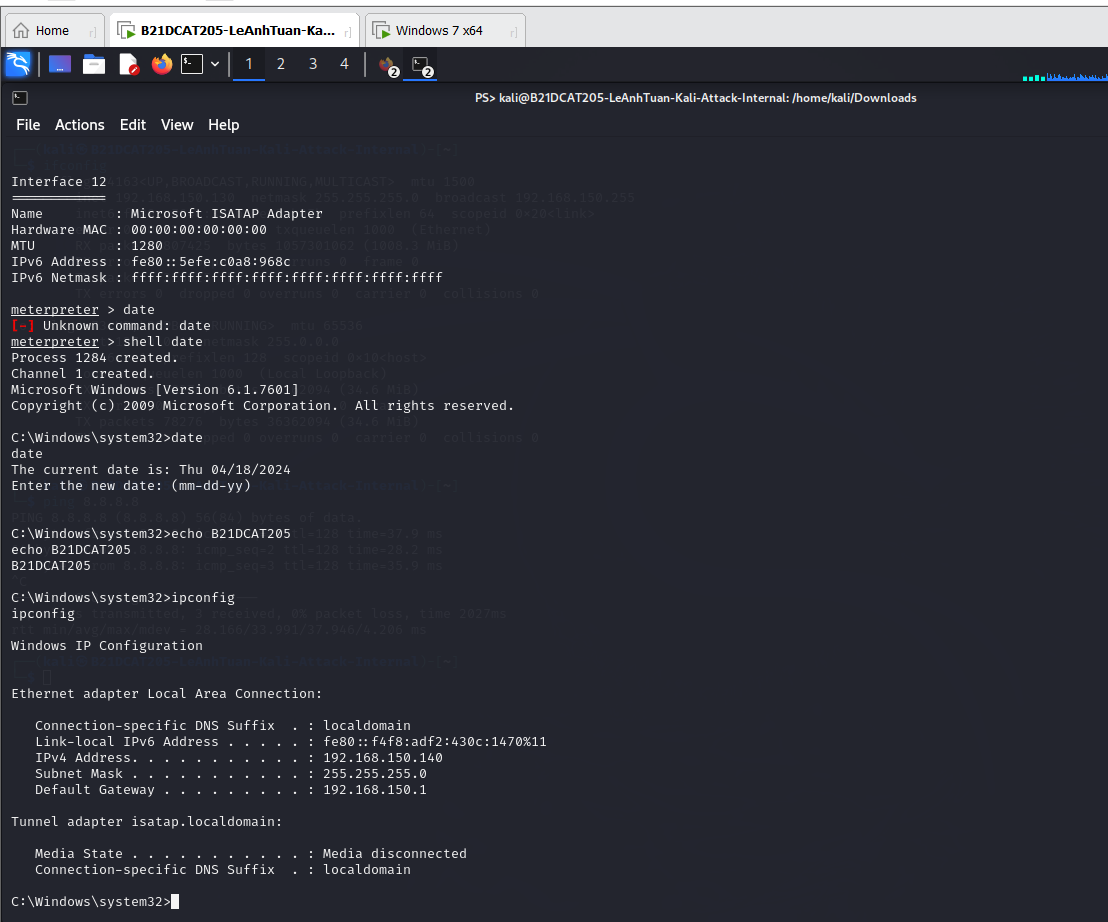
Hình 21: Cấu hình khai thác lỗ hổng MS17-010



Hình 22: Khai thác lỗ hổng thành công (ảnh 1)



Hình 23: Kiểm tra địa chỉ IP của Windows 7



Hình 24: Khai thác lỗ hổng thành công (ảnh 2)

1. **Kết luận**

* Như vậy, sau bài thực hành số 11, sinh viên đã hiểu được mối đe doạ, sự nghiêm trọng của các lỗ hổng trong hệ thống.
* Nắm được các sử dụng, hoạt đông của một số công cụ mạnh mẽ rà quét và tìm kiếm các lỗ hổng như: nnap/zenmap, Metasploit, Nessus,...
* Bên cạnh đó, sinh viên cũng được luyện tập khai thác một số lỗ hổng.

1. **Tài liệu tham khảo**

* 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.
* Tài liệu CEH, https://www.eccouncil.org/programs/certified-ethicalhacker-ceh/
* Lab 14 của CSSIA CompTIA Security+® Supported Lab