BÁO CÁO BÀI THỰC HÀNH SỐ 1

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

***Họ và tên sinh viên: Đồng Văn Tuấn Đạt***

***MSSV: 0850080015***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng HoTenSV\_MSSV\_Lab01.zip

* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

**KẾT QUẢ THỰC HÀNH**

**Cài đặt môi trường**

truy cập vào trang chủ của Kali Linux: <https://www.kali.org/get-kali/>

em tải lại kali linux từ máy bạn nên bỏ qua bước tải



công cụ hỗ trợ giả lập hệ điều hành em sài Vmware 17 Pro



File này là một file đã được cấu hình hết tất cả để phù hợp cho VMware, bạn chỉ cần mở VMware và thêm vào.

Vào VMware 🡪 File 🡪 Open.

Chọn vào nơi cài file Kali Linux và chọn vào file có đuôi là .vmx. Bấm Open là file đã được mở, thầy và các bạn chỉ cần chờ ít phút, sau đó cài đặt tài khoản và mật khẩu, tài khoản và mật khẩu đều là kali.

Phần mềm nmap đã được tích hợp sẵn ở trên máy ảo Kali Linux nên thầy sẽ không cần cài đặt mà có thể sử dụng luôn.

Các bạn mở cmd chạy lệnh

Để có thể cài đặt wireshark trên máy kali, ta dùng lệnh **sudo apt-get install wireshark**

Và nhập mk là kali là chạy được và các mở wireshark ra chạy

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

- Bước 1: Truy cập máy ảo Kali Linux.

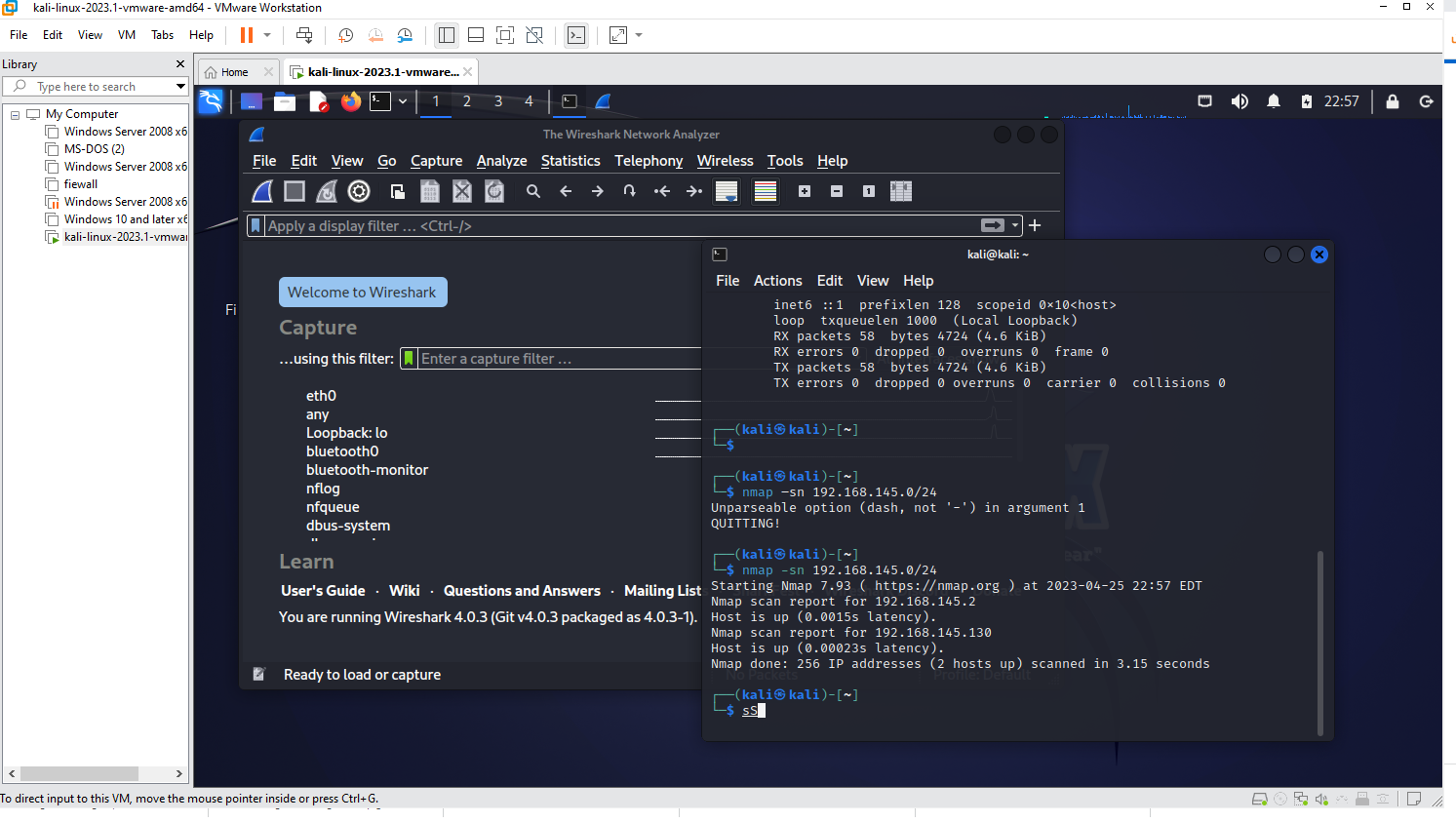
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

 để lấy ip

Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự

như sau:



Có thể thấy ngoài địa chỉ 192.168.145.0 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang

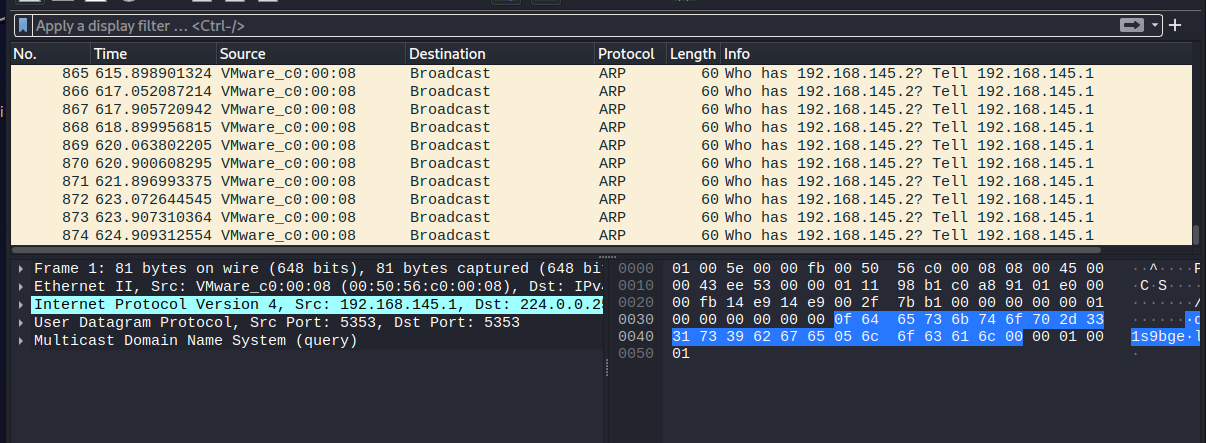
hoạt động có địa chỉ là 192.168. 145.2 và192.168. 145.130

Bước 5: Dừng bắt gói tin trên Wireshark

Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn

công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính

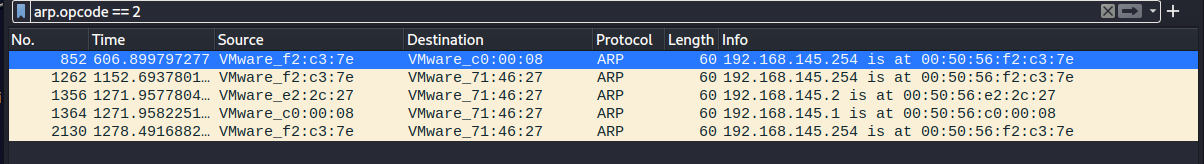
trong mạng 192.168.145.0 /24



Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy

các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong

kết quả quét mạng bằng công cụ nmap.

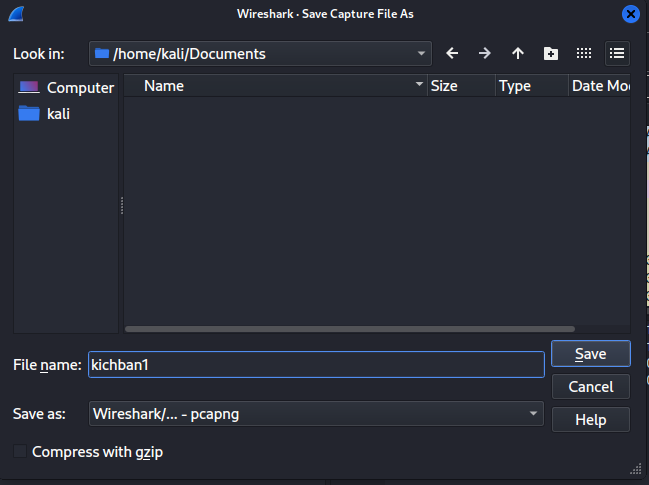


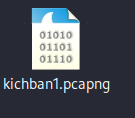
Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để

phát hiện các nút mạng đang hoạt động trong mạng.

buoc 6:

Lưu lại file lưu lượng trên máy do thám với tên là kichban1.pcap





* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* *Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*
* *Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm
  1. **Kịch bản 2**

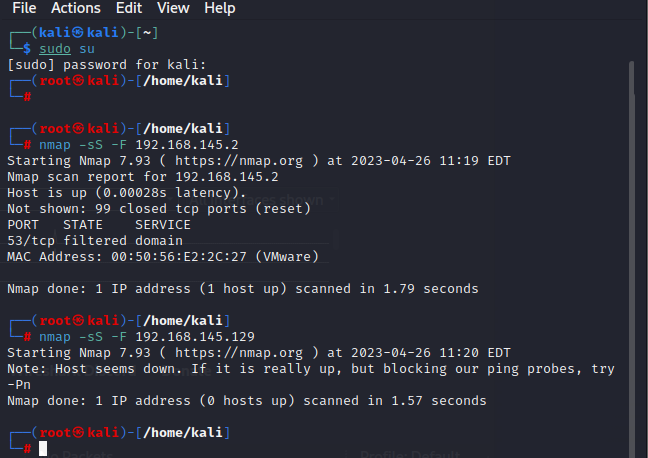
- Bước 1: Truy cập máy ảo Kali linux

- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: sudo su để đăng nhập với quyền root, sau đó sài lệnh

nmap –sS –F Địa\_chỉ\_IP\_máy\_mục\_tiêu

192.168. 145.2



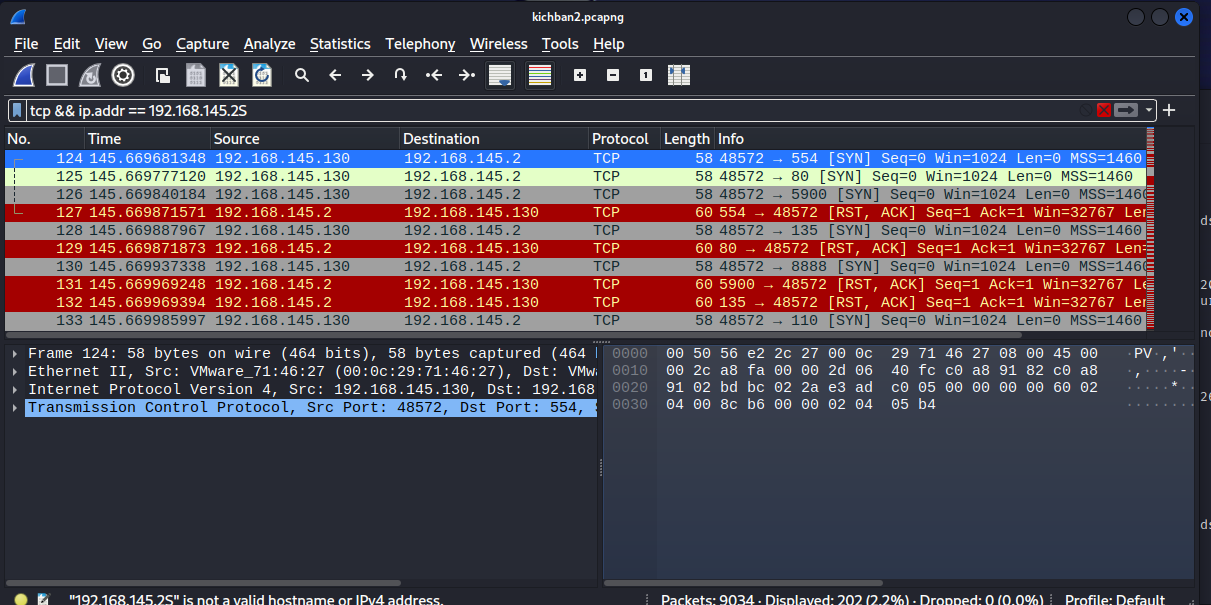
- Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.145.2có trạng thái cổng dịch vụ là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Domain.

Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.145.2.

Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 53 của các máy đang hoạt động.



Sử dụng giá trị tcp && ip.addr == 192.168.145.2.ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 124 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 53 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ

Domain).

Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

Bước 6: Lưu tập tin với file kichban2.pcapng



* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

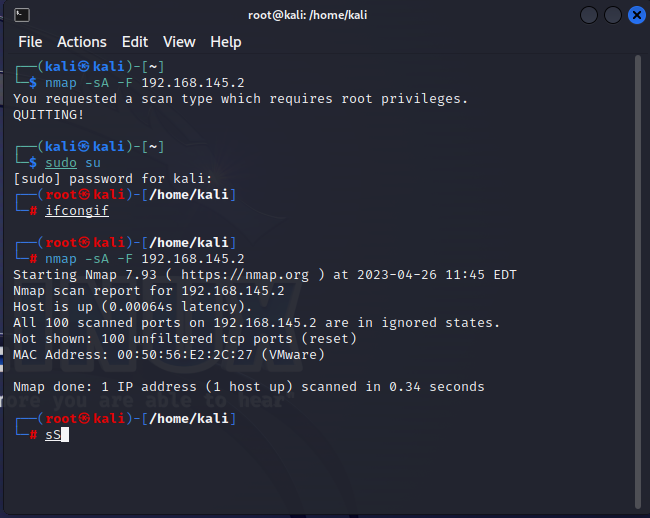
* 1. **Kịch bản 3**

- Bước 1: Truy cập máy ảo Attack

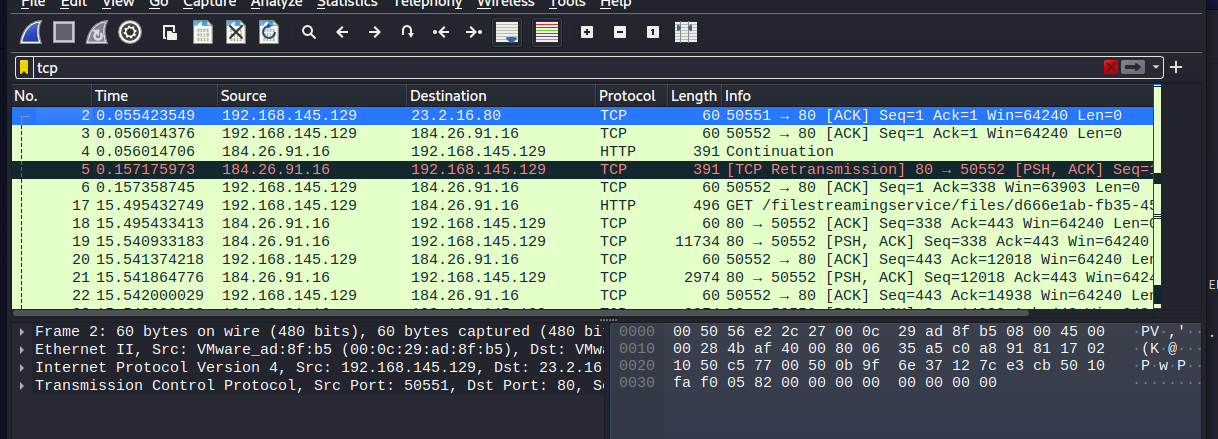
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: **nmap -sA -F 192.168.145.2**

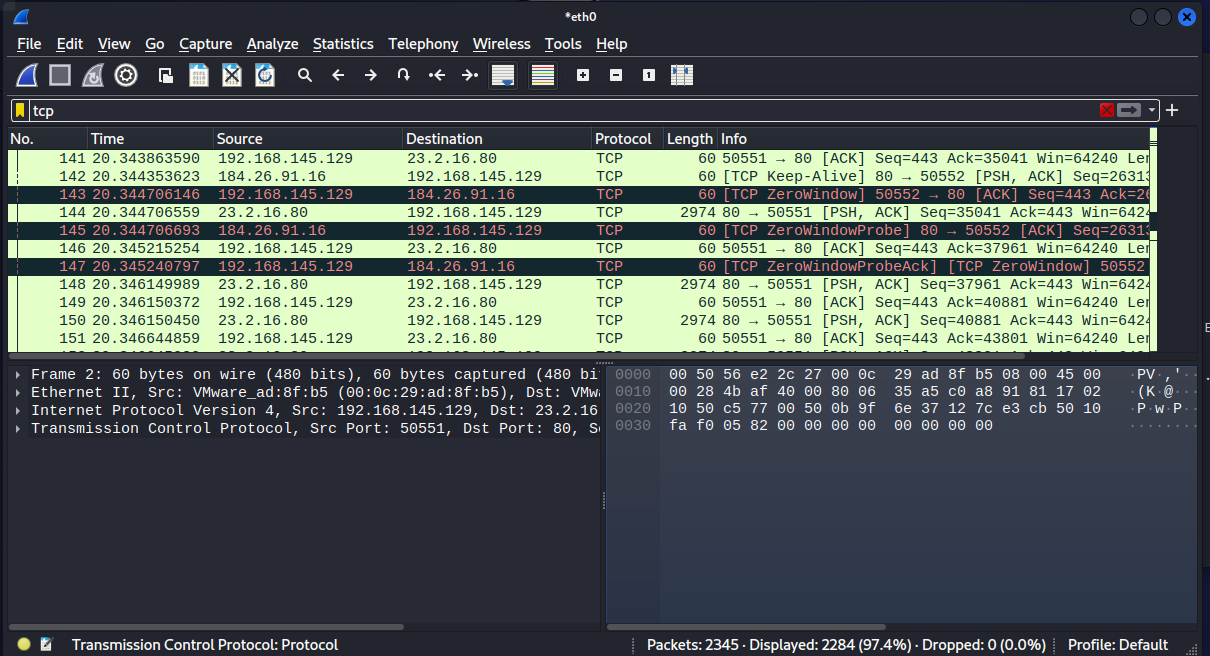
- Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy tất cả 100 cổng được quét trên địa chỉ IP **192.168.145.2**đang trong trạng thái bị bỏ qua (ignored), có nghĩa là không có máy chủ hoặc dịch vụ nào phản hồi trên các cổng này. Tuy nhiên, kết quả quét cũng cho thấy địa chỉ MAC của máy tính đích được quét là 00:0C:29:00:AF:57, cho thấy máy tính đó là một máy ảo VMware. Vì vậy, máy tính của bạn không bị gì cả, nhưng không có bất kỳ dịch vụ hoặc máy chủ nào phản hồi trên các cổng được quét.



- Bước 5: dừng bắt gói tin wireshark và kiểm tra.

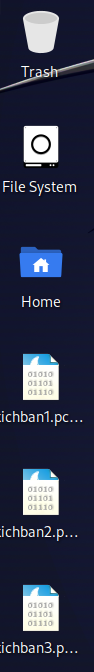


Sử dụng giá trị tcp && ip.addr == **192.168.145.2** ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 53, 143, 443 được quét ở kịch bản 2 vẫn chạy.



Kết quả: Lệnh nmap –sA –F 192.168.145.2 trong nmap được sử dụng để quét mạng bằng phương thức ACK. Tùy chọn -F chỉ quét các cổng phổ biến nhất. Khi sử dụng tùy chọn này, nmap sẽ gửi một yêu cầu ACK tới các cổng mạng đích và chờ đợi phản hồi. Nếu phản hồi ACK được trả về, nó cho biết rằng cổng đó có thể đang mở hoặc bị chặn bởi tường lửa. Nếu không có phản hồi, nó cho biết rằng cổng đó bị đóng. Việc sử dụng ACK quét có thể giúp người dùng phát hiện các cổng bị chặn bởi tường lửa hoặc các thiết bị bảo mật.

Bước 6: lưu file với tên kichban3.pcapng.



* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

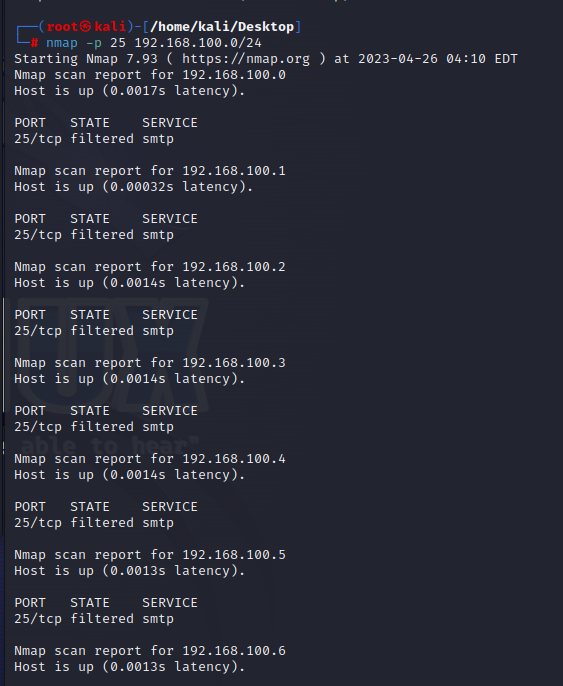
*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

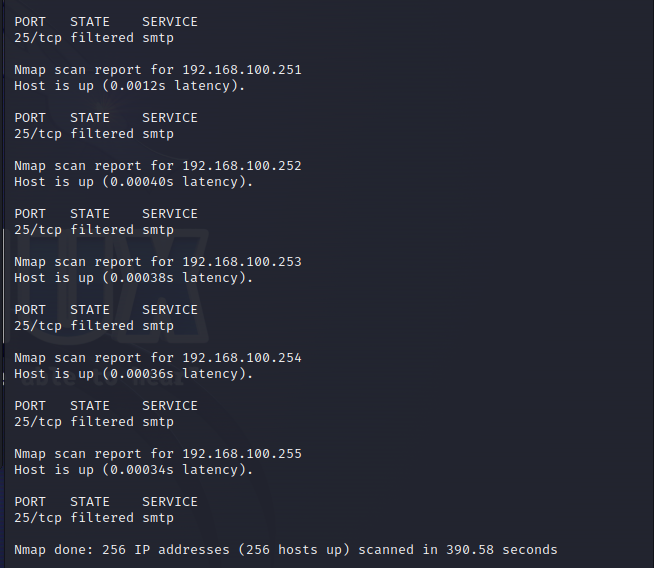
*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

1. **Thu thập thông tin hệ thống**

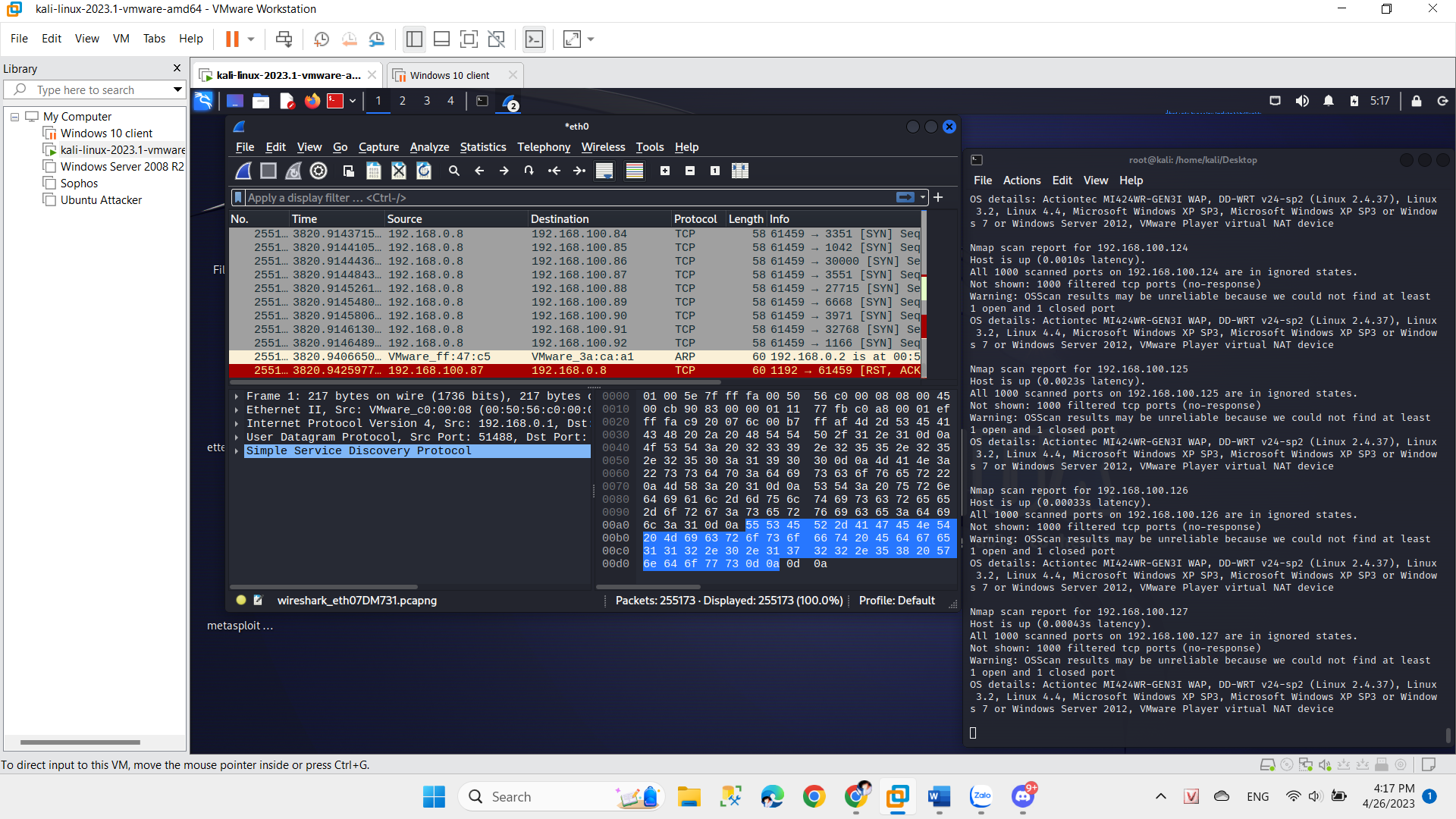
Bước 1: mở wireshar và thực hiện bắt gói tin.

Bước 2: mở nmap và thực hiện lệnh nmap -p 25 192.168.100.0/24 để xác định nút mạng trong mạng 192.168.100.0/24 cung cấp dịch vụ email.

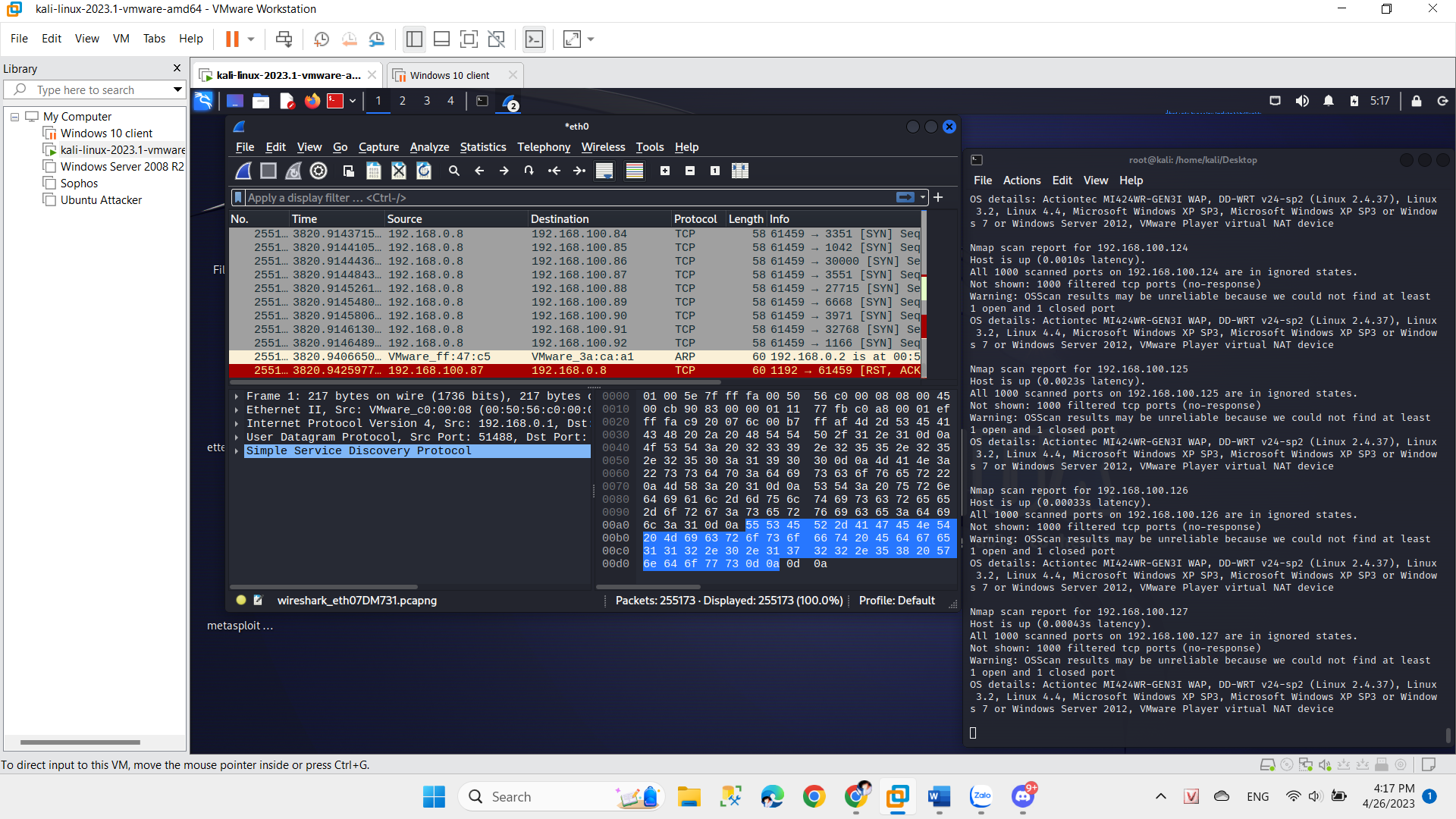




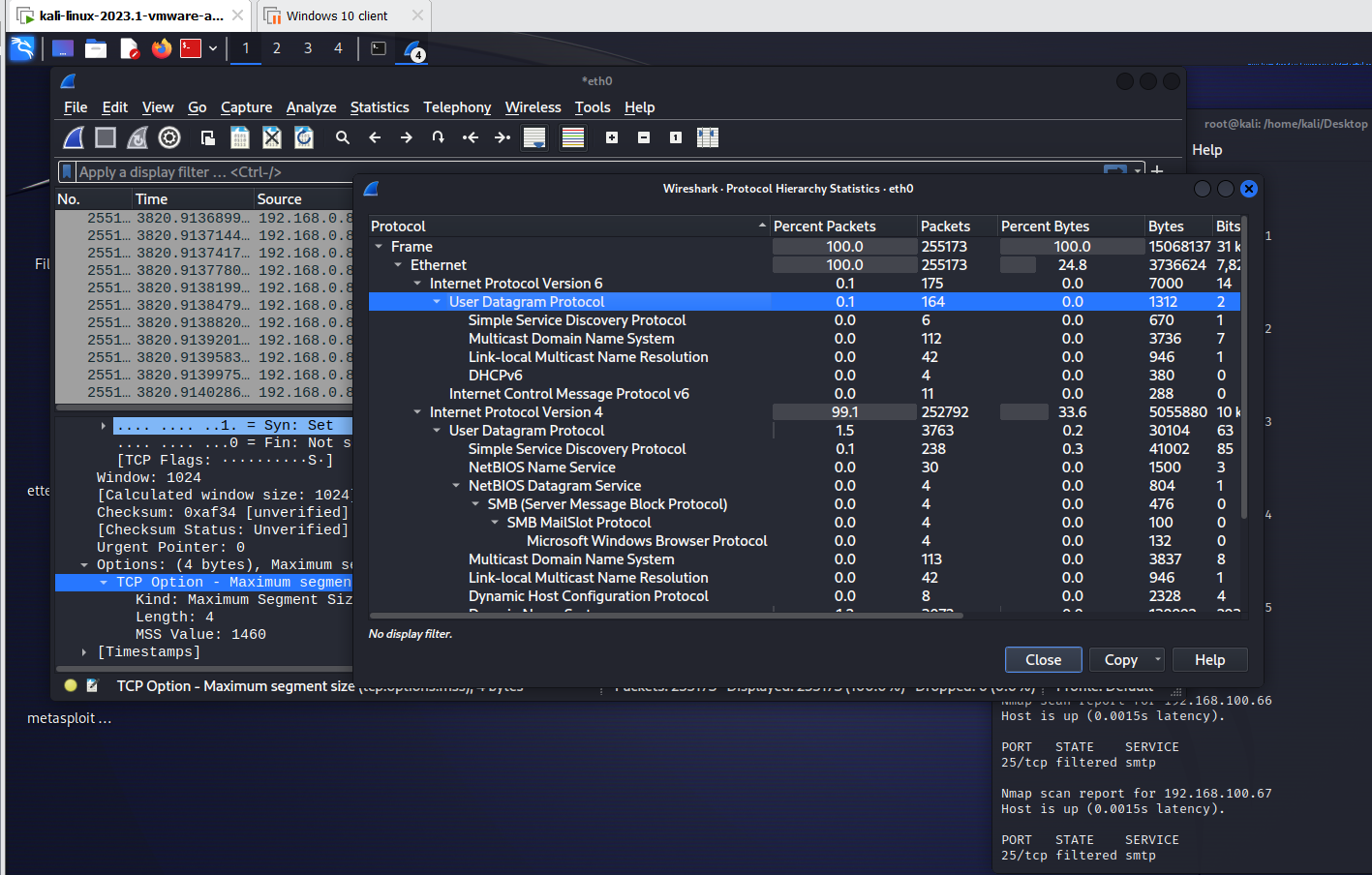
Bước 3: dùng lệnh nmap -sV -O 192.168.100.0/24 để quét, thu thập thông tin về hệ điều hành và các dịch vụ trên nút mạng 192.169.100.0

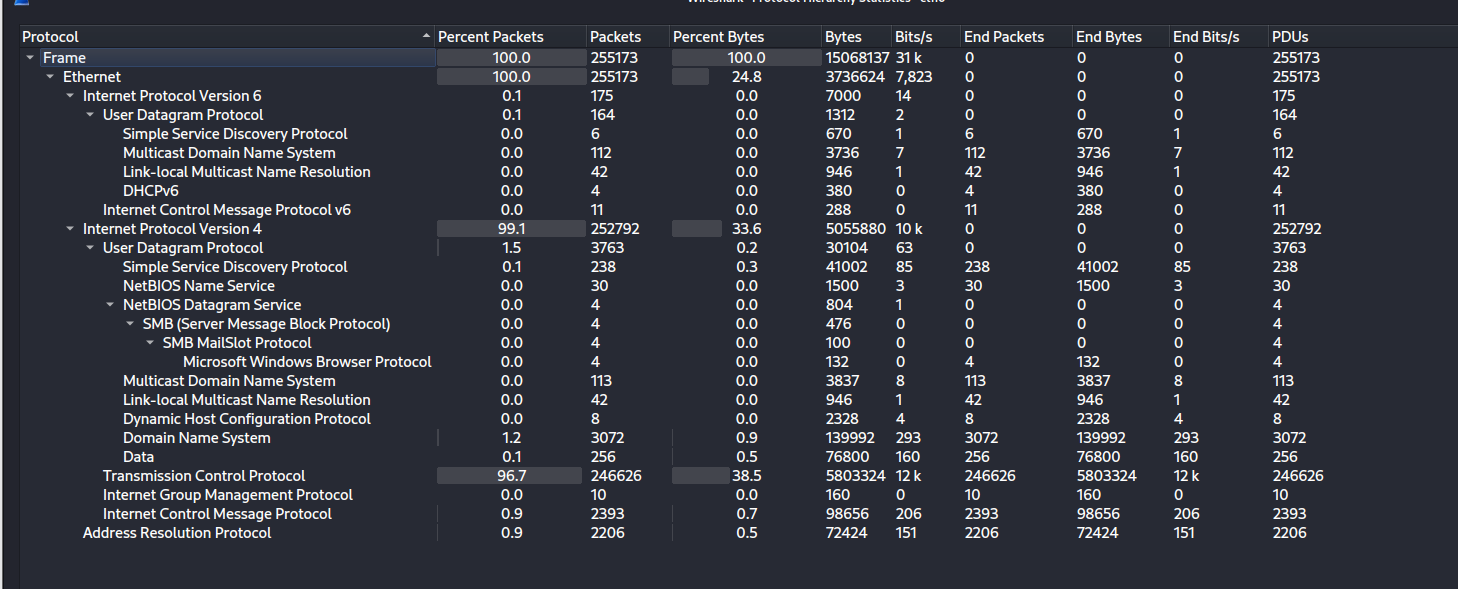


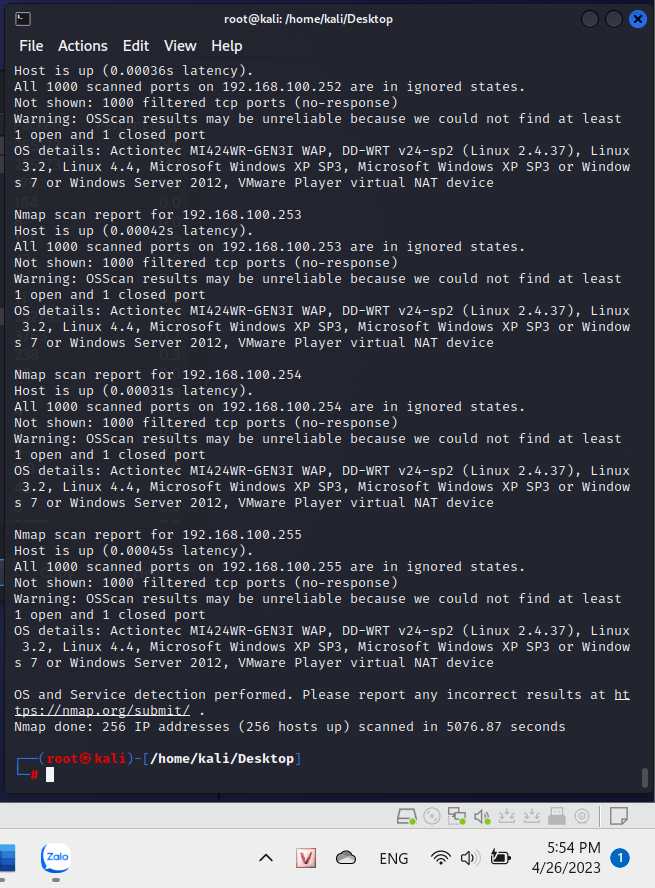
Bước 4: dừng bắt gói tin.



Trên thanh công cụ, chọn "Statistics" và chọn "Protocol Hierarchy".

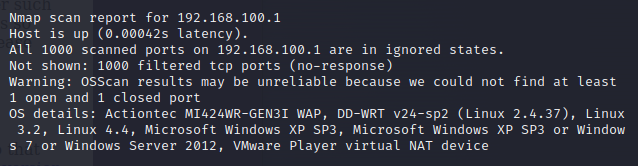






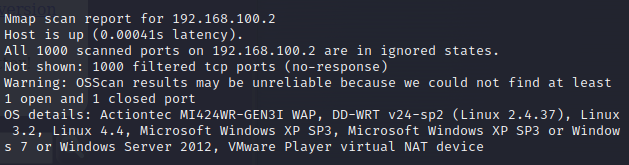
-Các hệ điều hành có thể có của địa chỉ thứ 1 là:

+ Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.



-Các hệ điều hành có thể có của địa chỉ thứ 2 là:

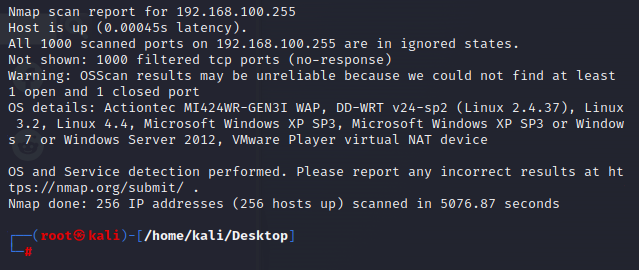
+ ctiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.

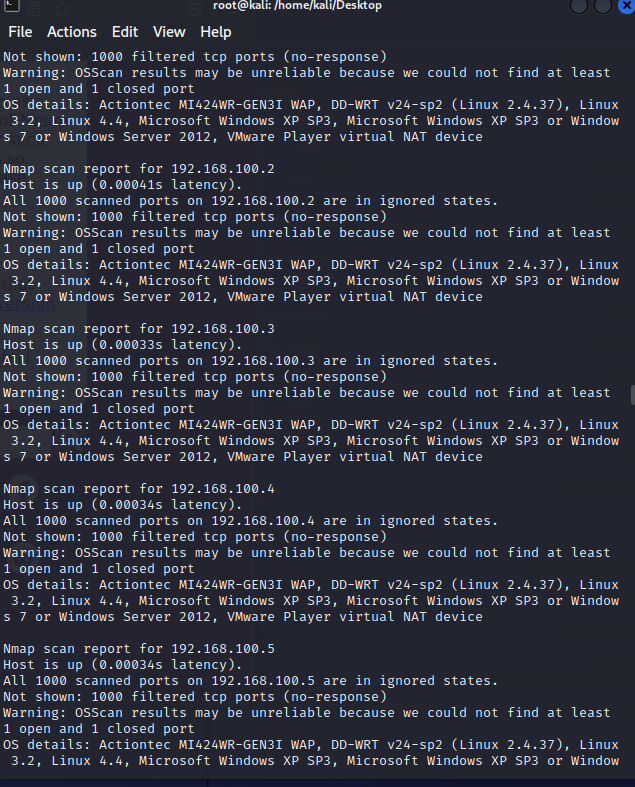


+…

-Các hệ điều hành có thể có của địa chỉ thứ 255 là:

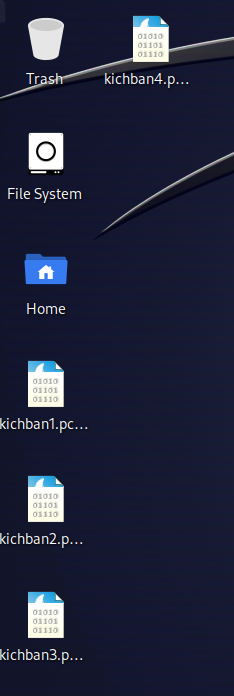
+ Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.





Dịch vụ được chạy trên từng port này hiển thị ở phần Not shown và tất cả port đều chạy trên dịch vụ tcp.

Lưu lại file lưu lượng trên máy do thám với tên là kichban4.pcap



* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

**Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Nêu tên và phiên bản hệ điều hành: 0.25 điểm

**Thông tin dịch vụ: 1 điểm**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Tìm kiếm thông tin về các lỗ hổng**

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

Mỗi lỗ hổng: 1 điểm

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
|  |  |  |
|  |  |  |