**MỤC LỤC**

[**1. Cài đặt môi trường** 1](#_Toc133429139)

[**2. Luyện tập** 4](#_Toc133429140)

[**2.1 Quét thăm dò mạng** 4](#_Toc133429141)

[**2.2 Quét thăm dò dịch vụ** 8](#_Toc133429142)

[**2.3 Quét cổng dịch vụ** 13](#_Toc133429143)

[**3. Yêu cầu** 16](#_Toc133429144)

[**3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap** 16](#_Toc133429145)

[3.1.1. Kịch bản 1 16](#_Toc133429146)

[3.1.2. Kịch bản 2 19](#_Toc133429147)

[3.1.3. Kịch bản 3 22](#_Toc133429148)

[**3.2. Thu thập thông tin hệ thống** 25](#_Toc133429149)

[**3.3. Tìm kiếm thông tin về các lỗ hổng** 30](#_Toc133429150)

BÁO CÁO BÀI THỰC HÀNH SỐ 1

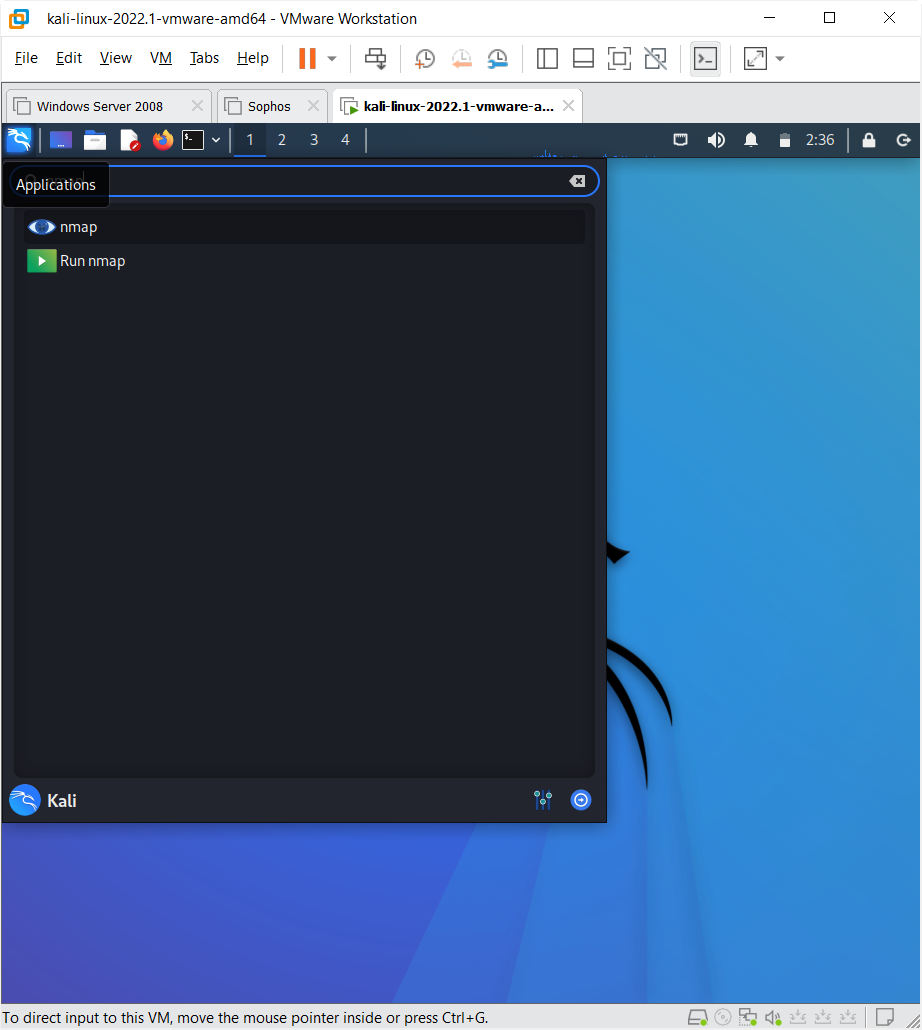
**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

Họ và tên sinh viên: Lê Thị Bảo Yến

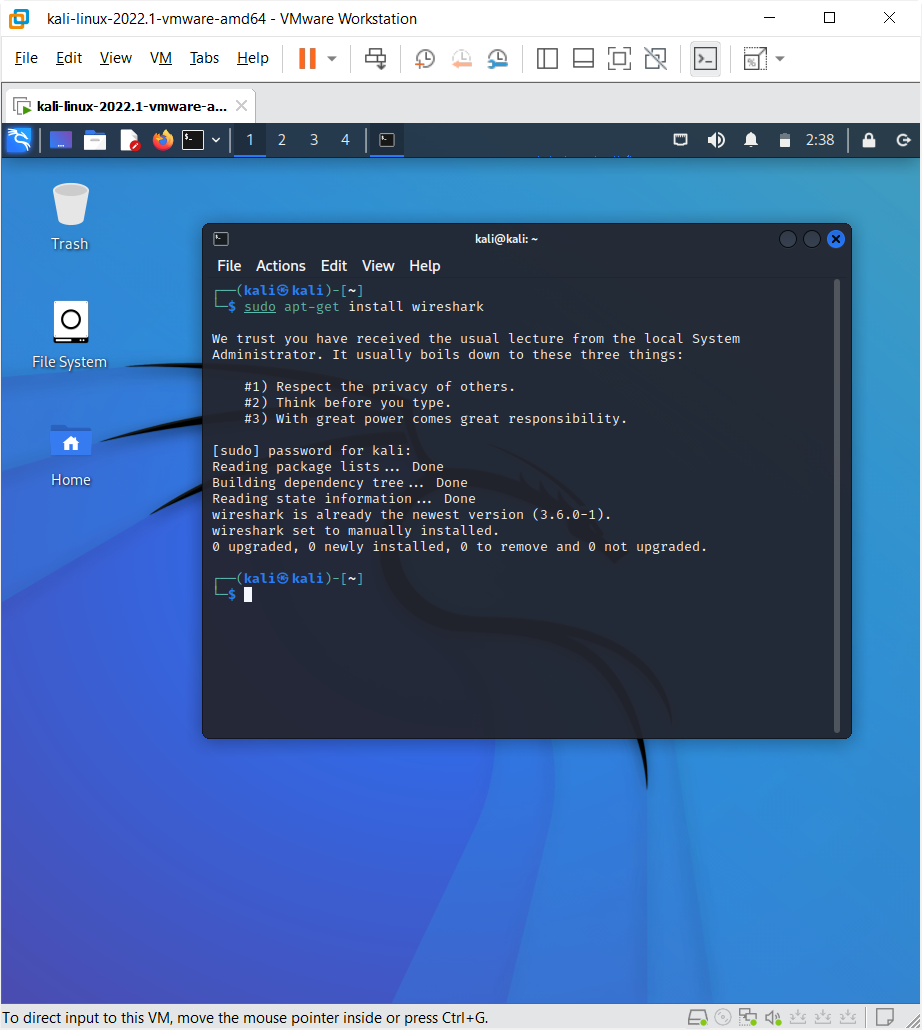
MSSV: 0850080057

# **1. Cài đặt môi trường**

**B1**: Cài đặt môi trường Kali-Linux trên máy ảo Vmware WorkStation Pro 16 để thực hiện.

**B2:** Sau khi cài đặt KaLi trên VMware thì nó đã có sẵn nmap mà không cần cài đặt.

**B3**: Cài đặt Wireshark.



Giao diện WireShark



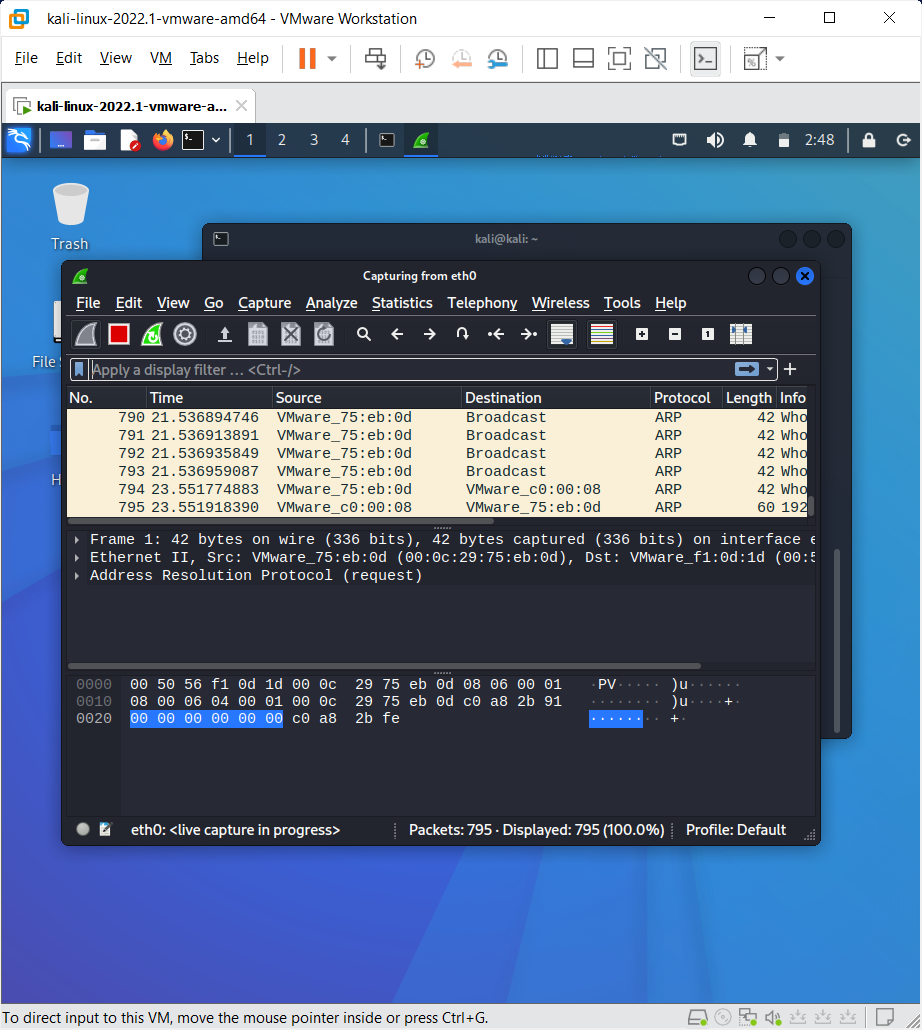
**2. Luyện tập**

**2.1 Quét thăm dò mạng**

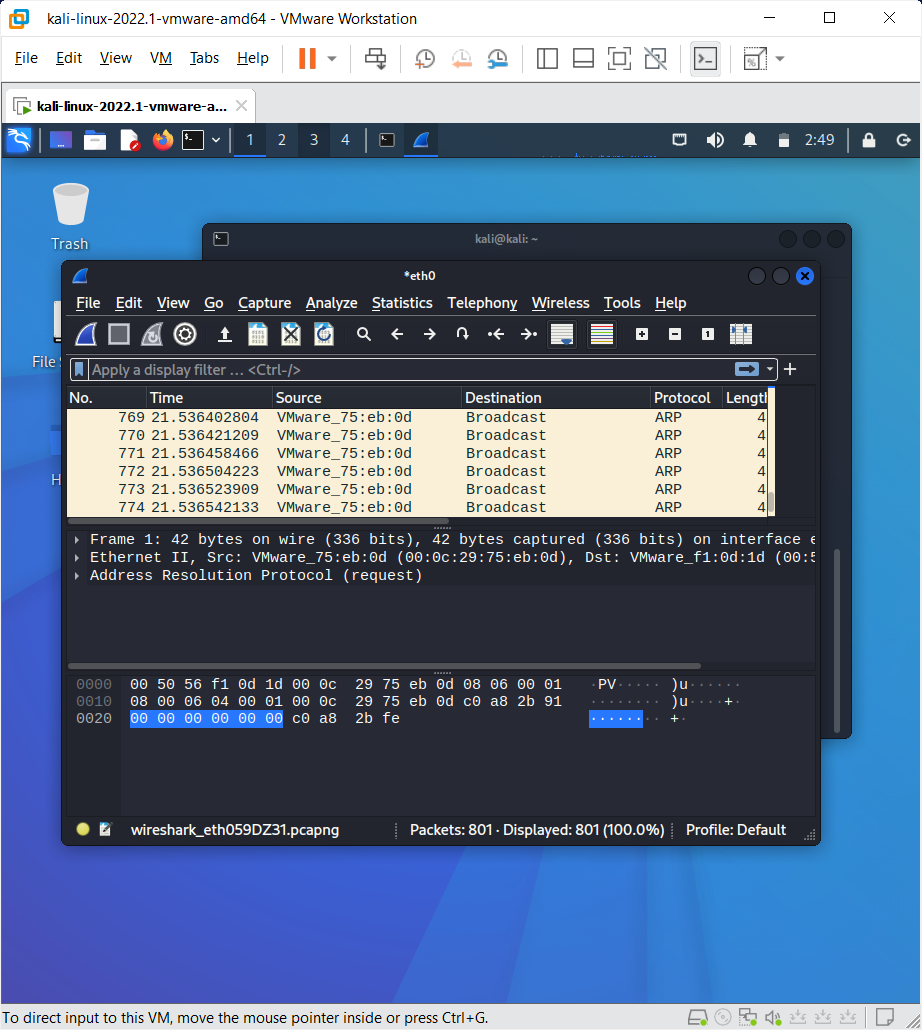
Sử dụng Nmap để quét mạng với lệnh: **nmap –sn 192.168.43.0/24**



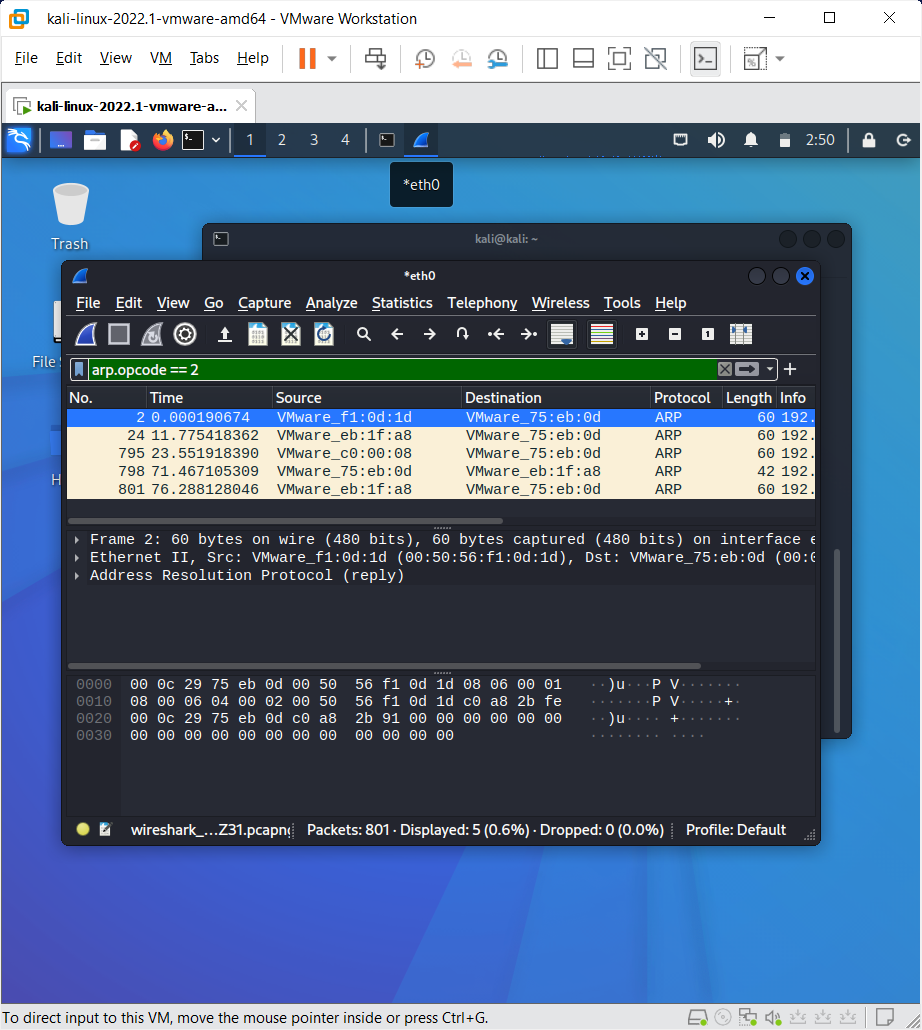
Sau khi quét mạng và chạy trên WireShark



**B5**: Dừng bắt gói tin trên wireshark và phân tích lưu lượng



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.

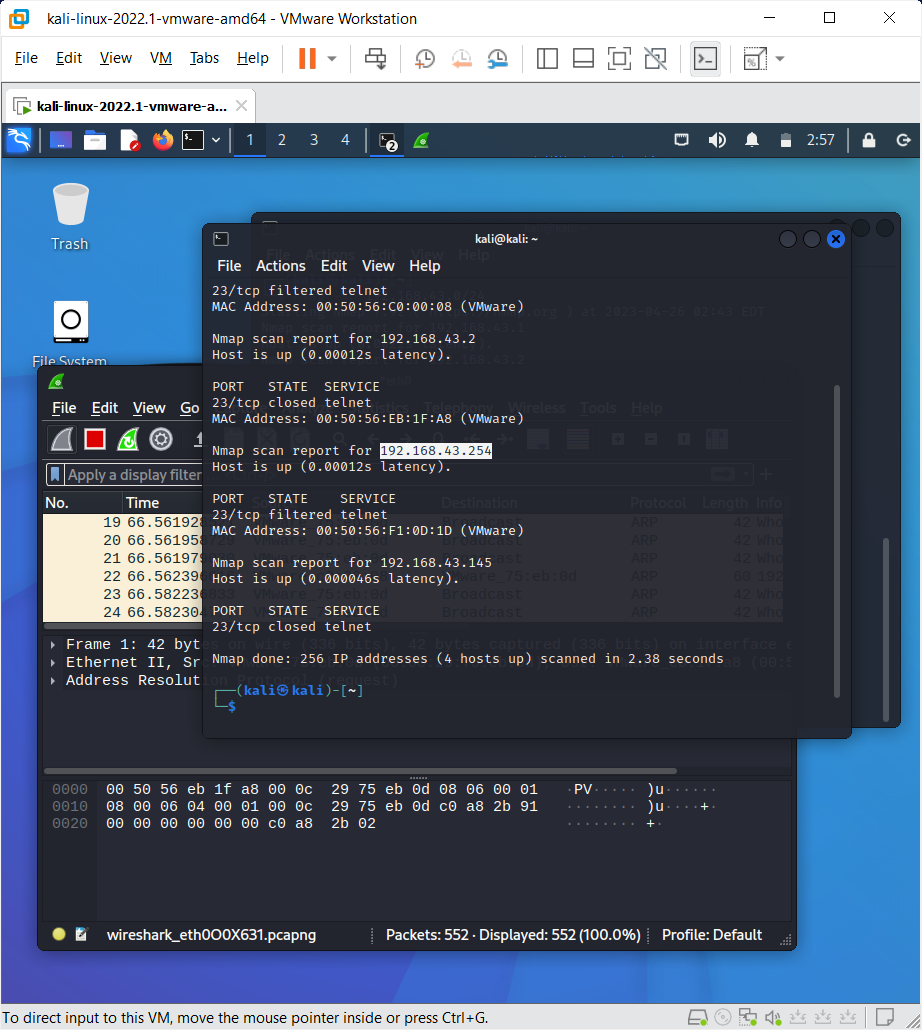


**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

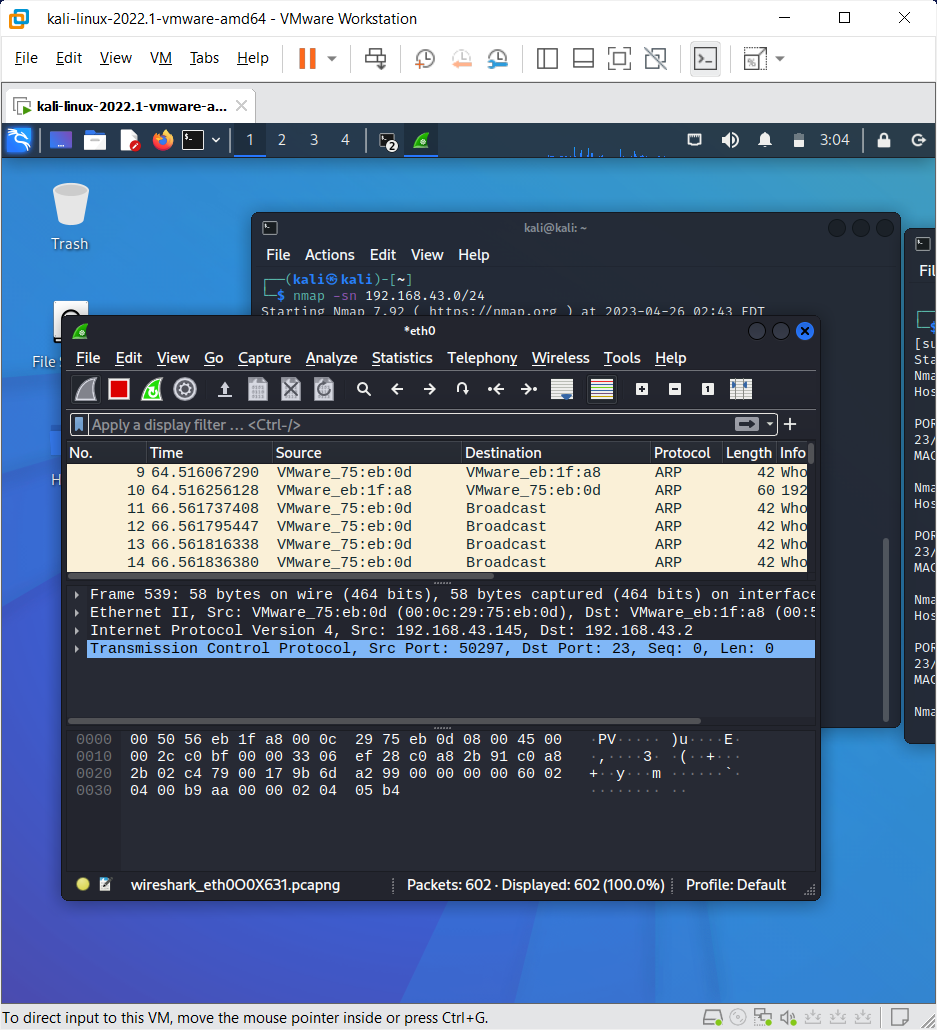
**2.2 Quét thăm dò dịch vụ**

**Bước 1:** Mở terminal và chạy Wireshark, sau đó mở terminal thứ 2 để chạy câu lệnh sau:

**sudo nmap -p 23 192.168.43.0/24**

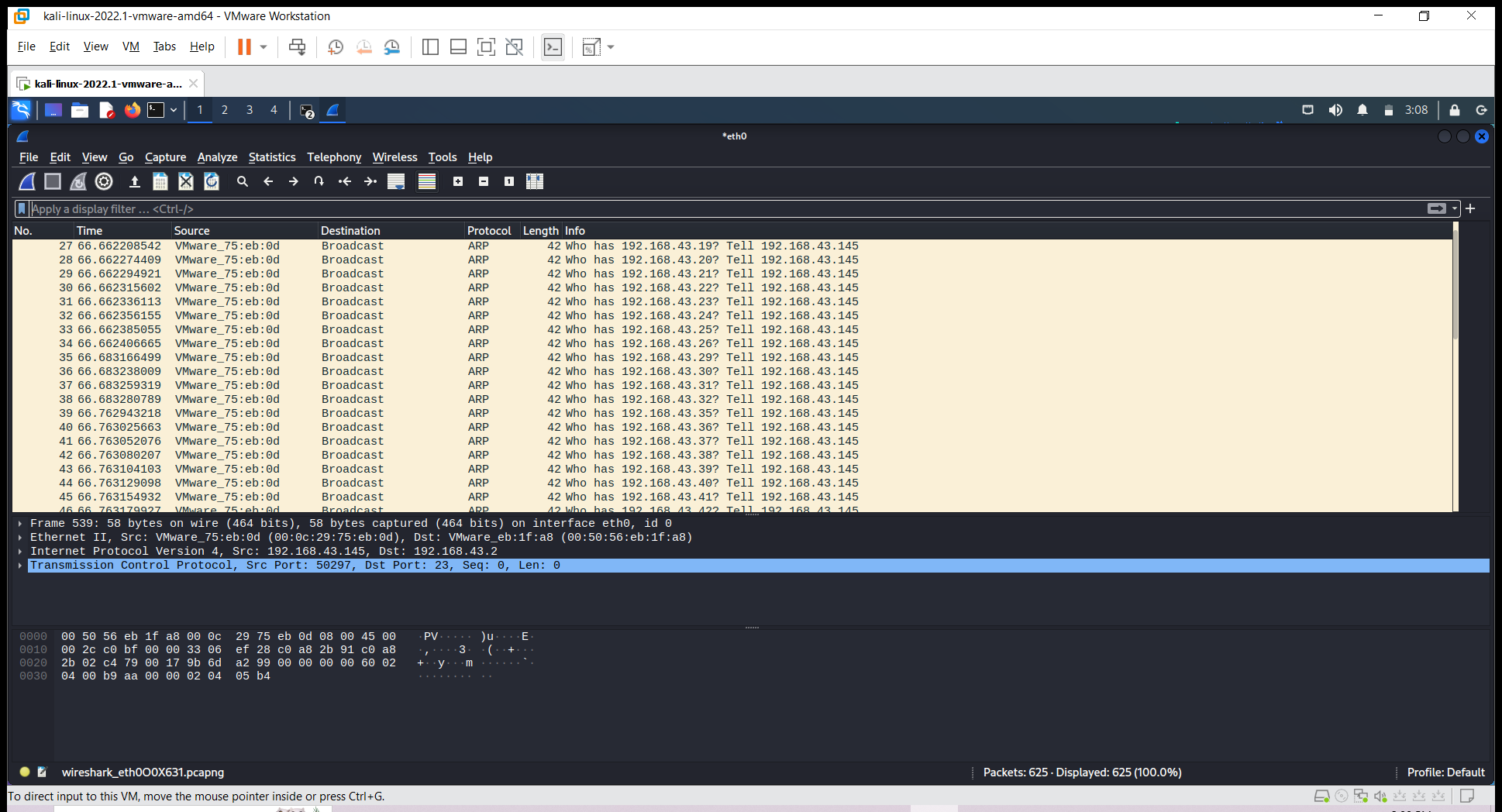


**B2:** Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.43.254 và 192.168.43.2 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

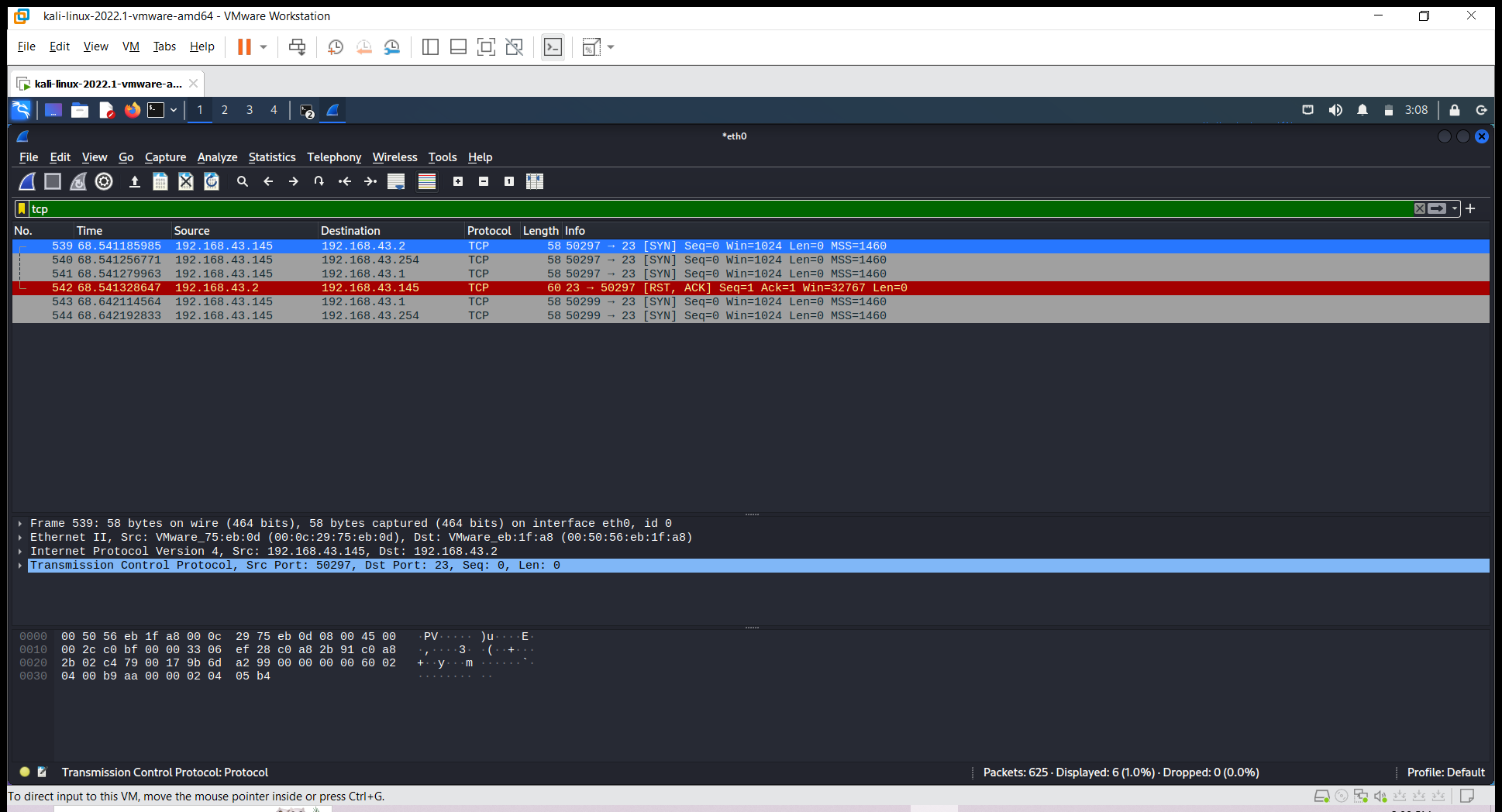


**B3**: Dừng bắt gói tin và phân tích lưu lượng

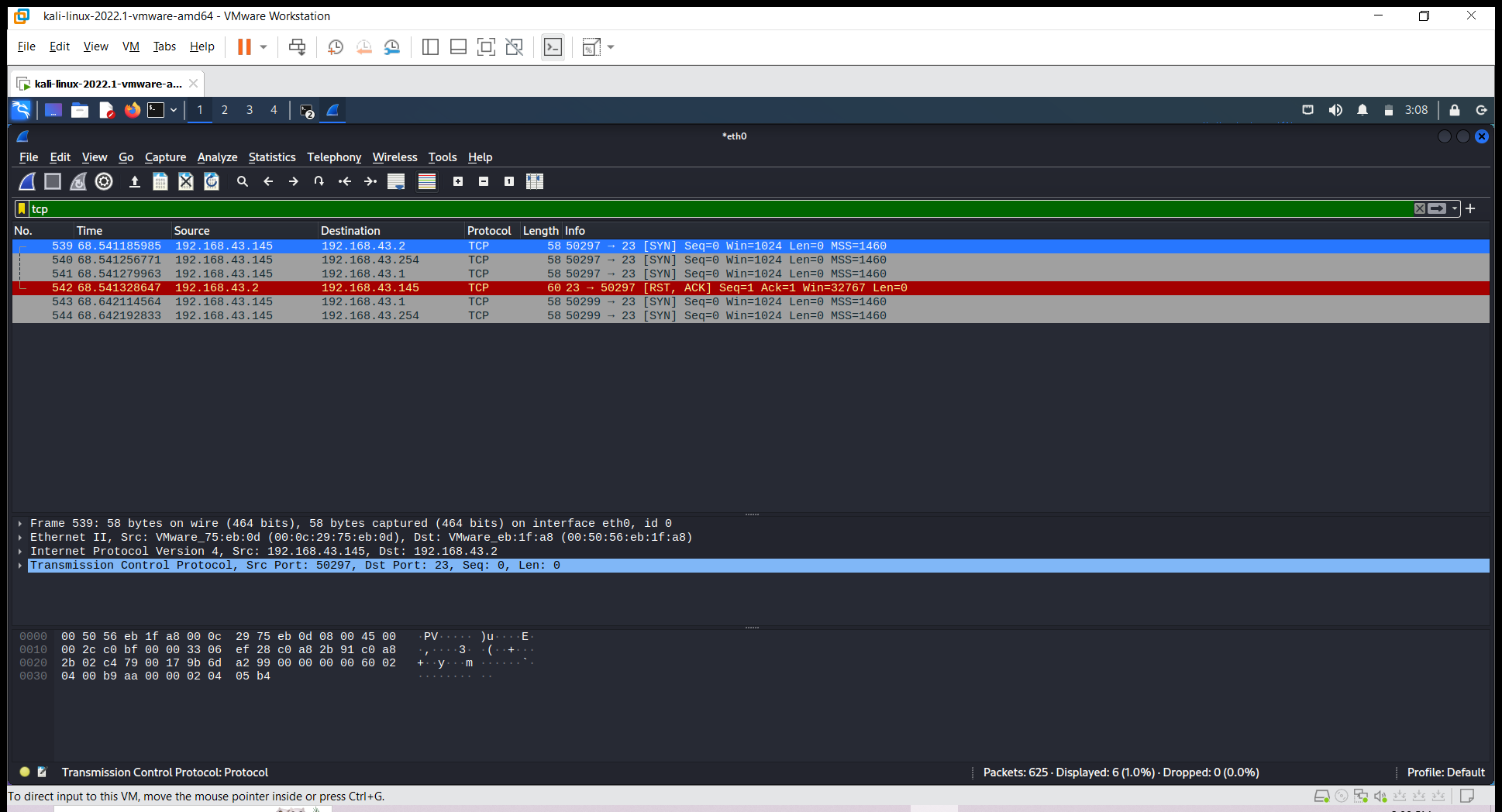
Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.43.0/24.



Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 23 của các máy đang hoạt động.



Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.43.145 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.43.2 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet).



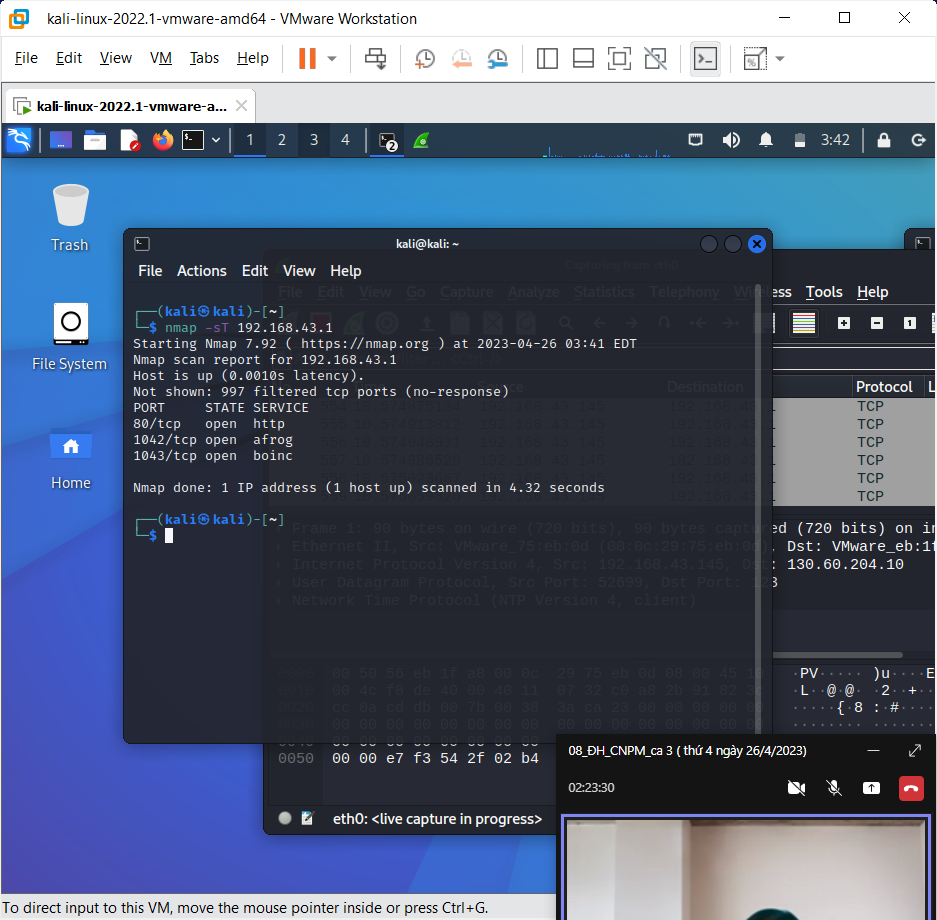
Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

## **2.3 Quét cổng dịch vụ**

B1: Mở terminal và chạy wireshark, sau đó mở terminal thứ 2 để chạy câu lệnh sau:

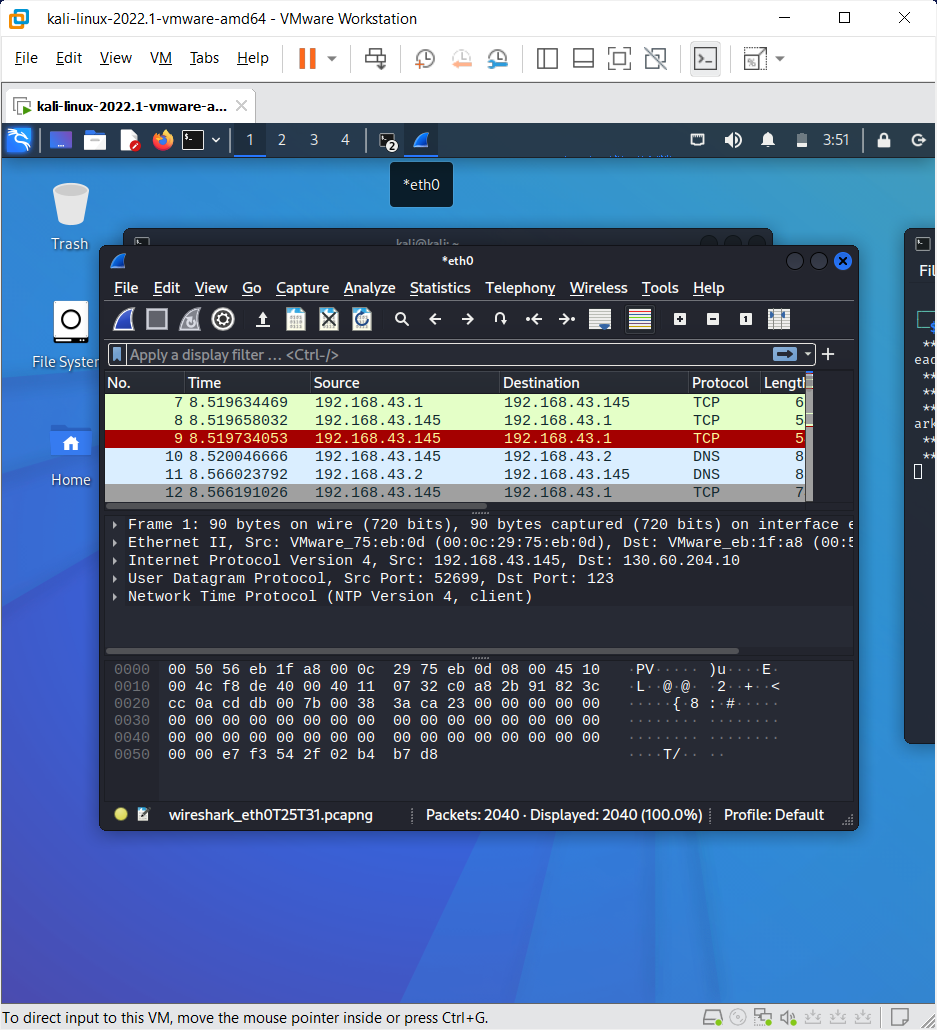
**nmap -sT 192.168.43.1**

B2: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 80, 1042, 1043 trên máy mục tiêu 192.168.43.1 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

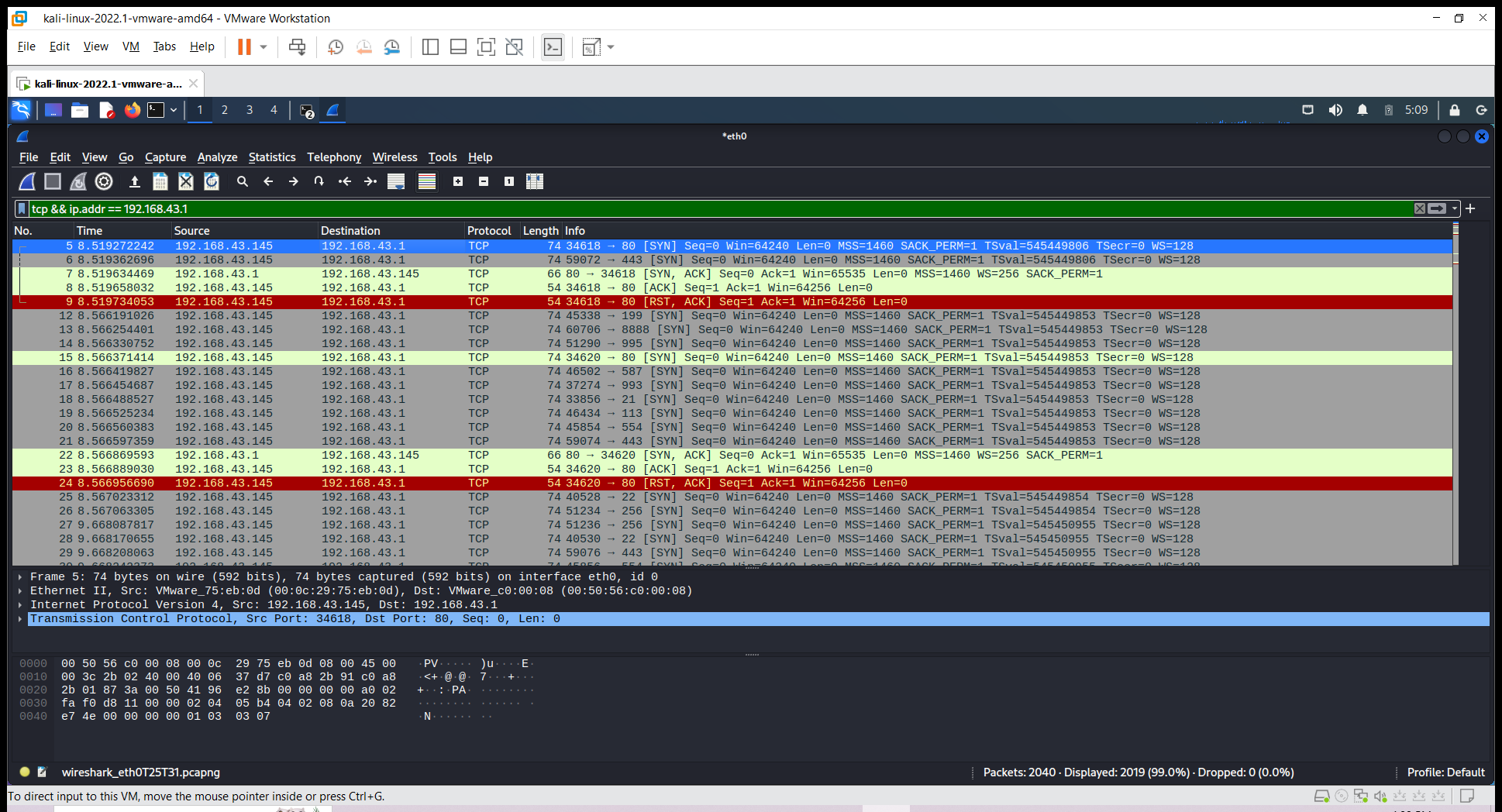


B3: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng: Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.43.1 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói tin TCP SYN được gửi từ máy tấn công (192.168.43.145) tới máy mục tiêu là 192.168.43.1. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



Sử dụng giá trị **tcp && ip.addr == 192.168.43.1** ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 5 đã được thiết lập (các gói tin 6, 7, 8 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST (gói tin 9) để hủy kết nối này.



Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 15, 22. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan.

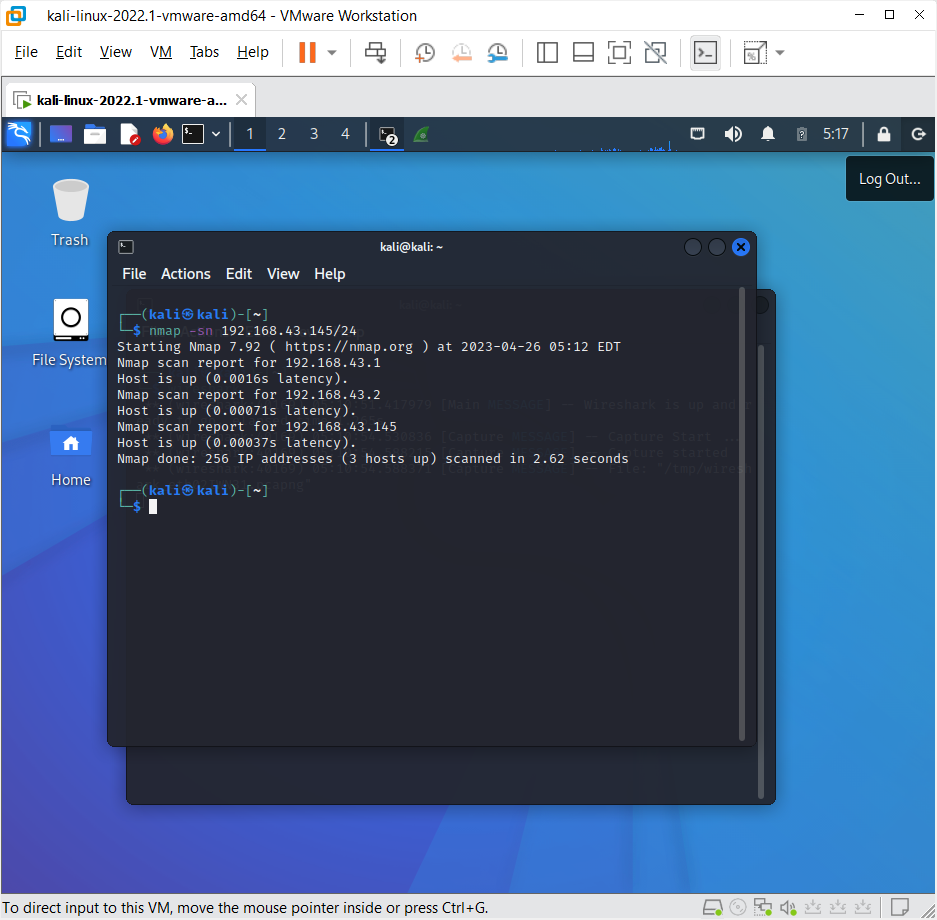
Danh sách các cổng ứng dụng trên máy mục tiêu có thiết lập kết nối với máy do thám trùng khớp với kết quả trả về của lệnh quét nmap trên máy do thám.

# **3. Yêu cầu**

## **3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**

### **3.1.1. Kịch bản 1**

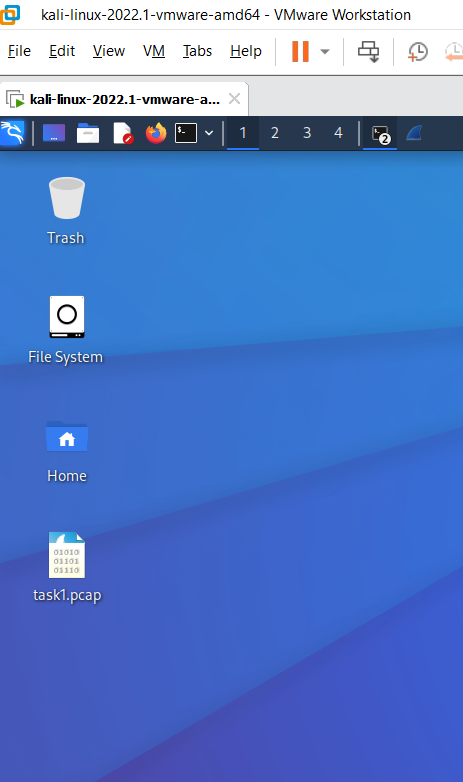
Thực hiện lệnh quét **nmap –sn 192.168.43.145/24** trên máy do thám



Kết quả:

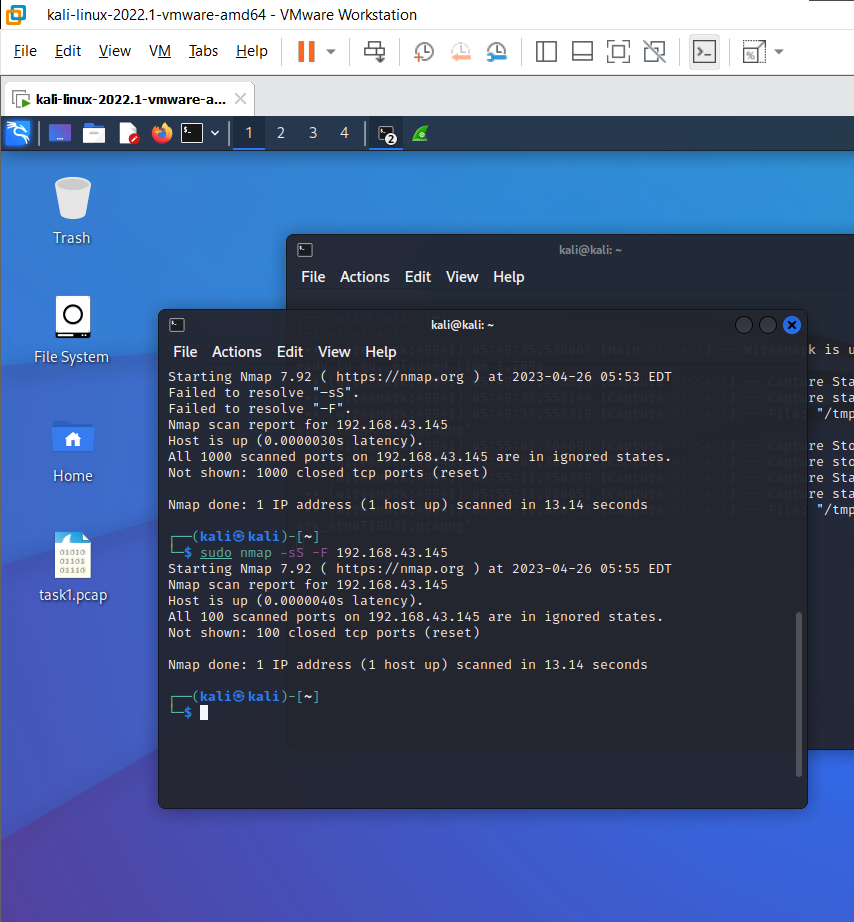


Kỹ thuật quét được sử dụng là “**Ping Scan**”.

Lưu lại.

## 3.1.2. Kịch bản 2

Thực hiện lệnh quét **sudo** **nmap –sS –F 192.168.43.145**

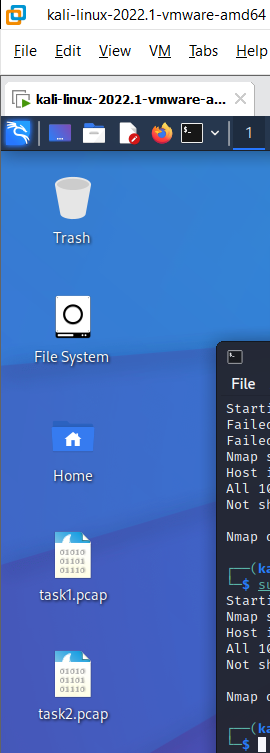


Kết quả:



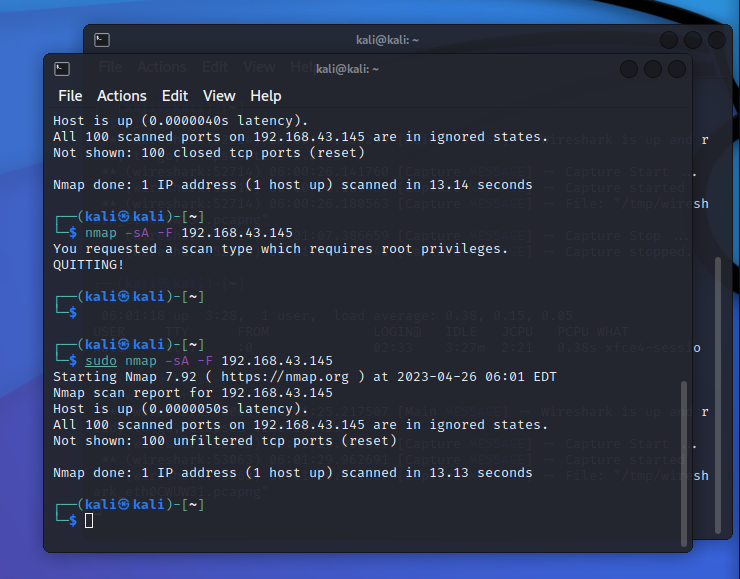
Kỹ thuật quét được sử dụng là “**TCP SYN Scan**”.

Lưu file

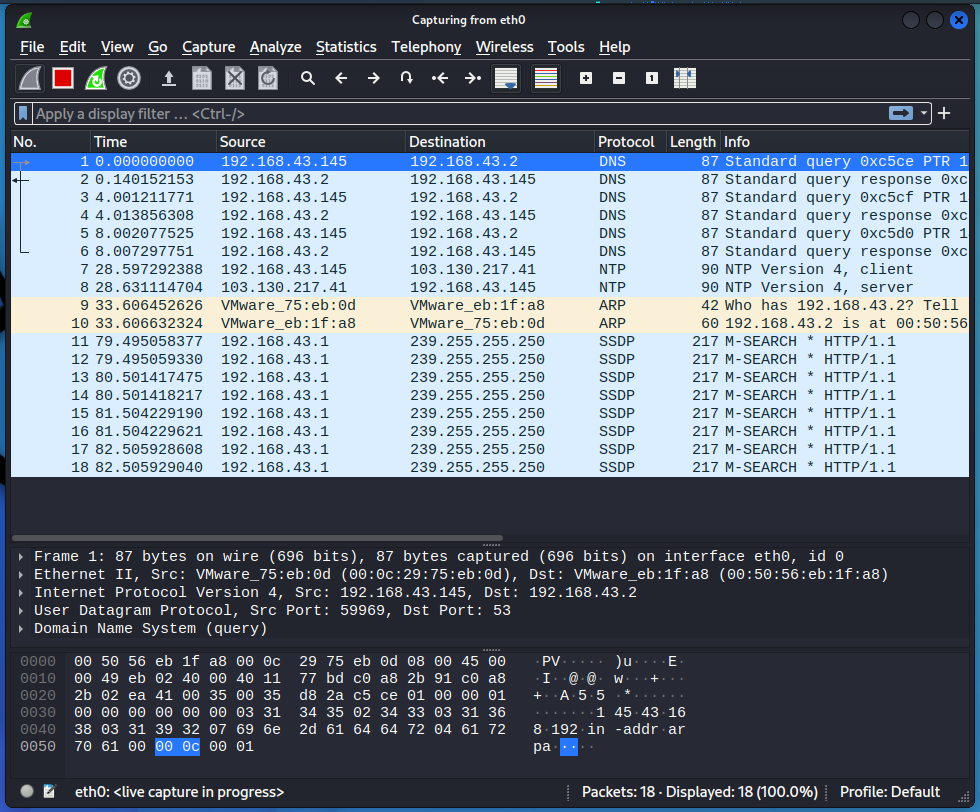


### **3.1.3. Kịch bản 3**

Thực hiện lệnh quét **sudo** **nmap –sA –F 192.168.43.145**

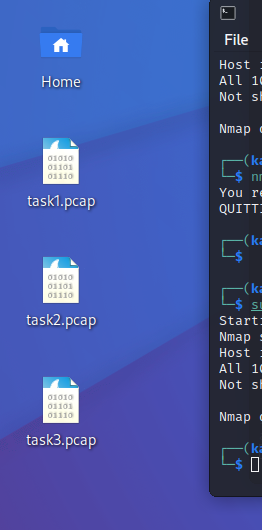


Kết quả:



Kỹ thuật quét được sử dụng là “**TCP ACK Scan**”.

Lưu file



## **3.2. Thu thập thông tin hệ thống**

Để xác định nút mạng trong mạng 192.168.100.0 /24 cung cấp dịch vụ email, sử dụng lệnh

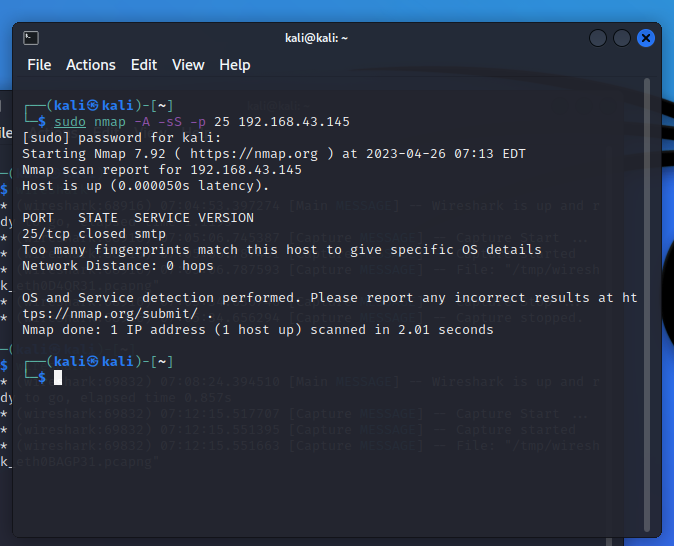
**nmap -p 25 --open 192.168.100.0/24**

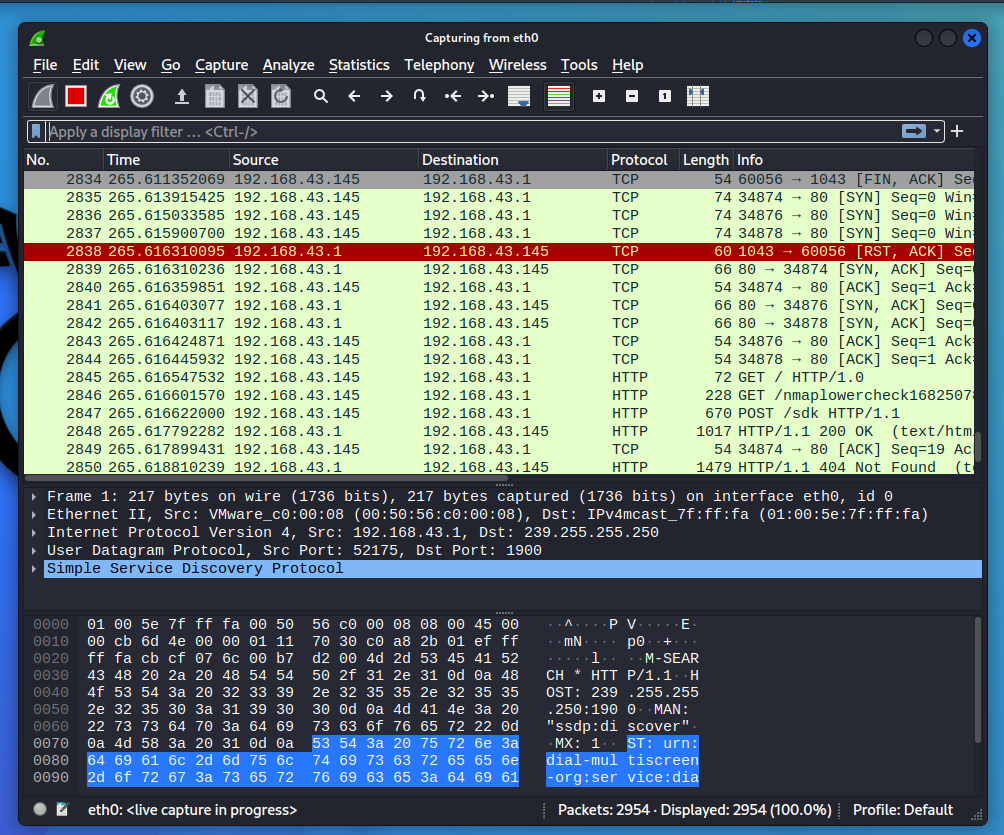
Lệnh này sẽ quét các cổng 25 (SMTP) trên các địa chỉ IP trong phạm vi mạng 192.168.100.0/24 và chỉ liệt kê các địa chỉ IP có cổng 25 đang mở. Trong đó:

* Cổng 25 (SMTP) là cổng chuẩn để cung cấp dịch vụ email trên máy chủ.
* “nmap” là tên của phần mềm quét mạng.
* “--open” là chỉ hiển thị những máy chủ có cổng 25 đang mở.
* “192.168.100.0/24”: Địa chỉ IP đại diện cho dải mạng cần quét.

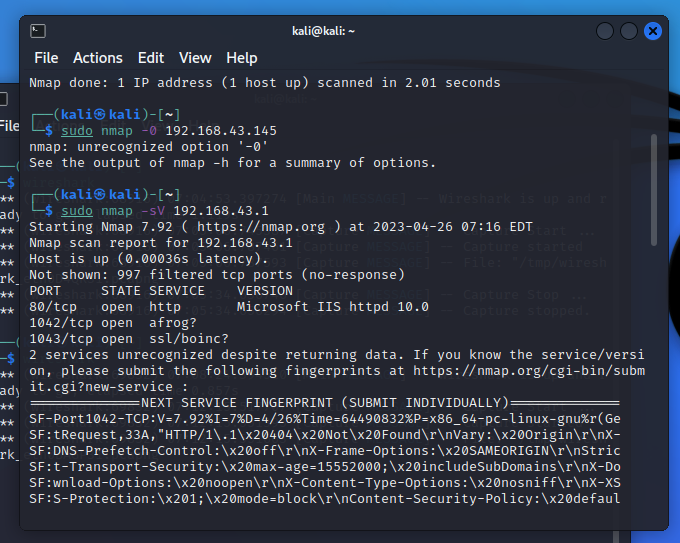


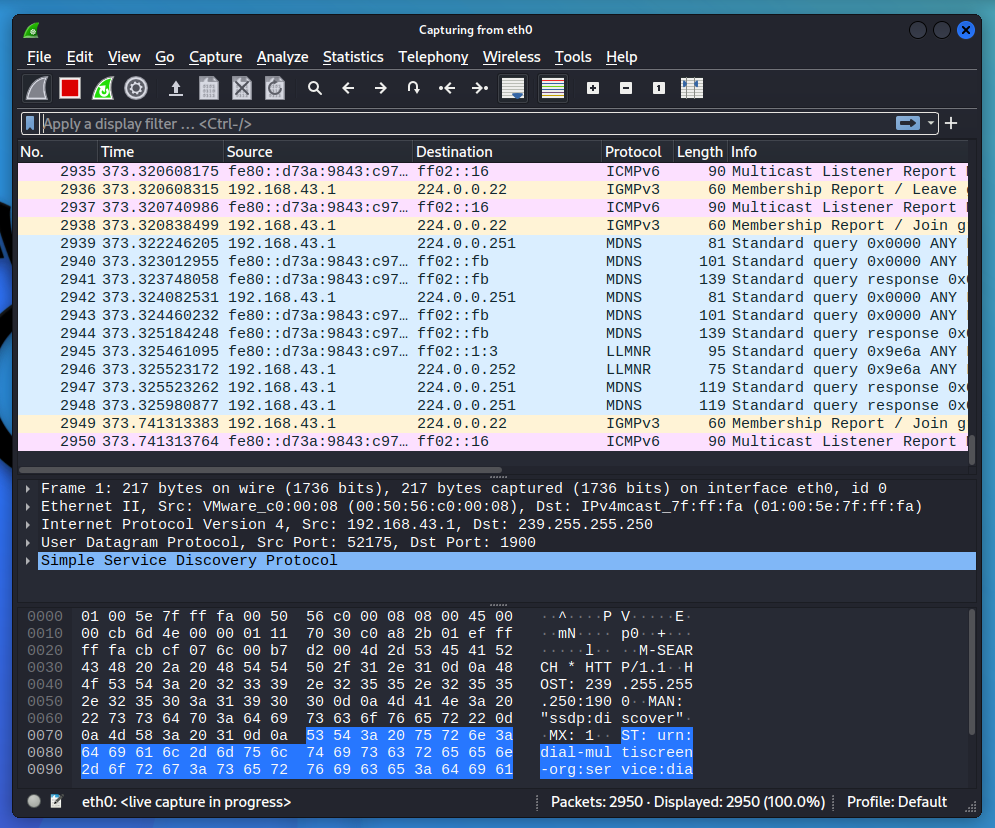
Hình ảnh kết quả thông tin hệ điều hành





Kết quả thông tin dịch vụ





Danh sách dịch vụ

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | http | 80/tcp | Microsoft IIS httpd 10.0 |
| 2 | afrog? | 1042/tcp |  |
| 3 | ssl/boinc? | 1043/tcp |  |

## 3.3. Tìm kiếm thông tin về các lỗ hổng

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm,  phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| Microsoft Exchange Server | CVE-2021-26855 | Lỗ hổng cho phép tấn công từ xa để truy cập trái phép vào các tài khoản và dữ liệu. |