BÁO CÁO BÀI THỰC HÀNH SỐ 7

# PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

***Họ và tên sinh viên: Huỳnh Tuấn Kiệt***

***MSSV: 1050082069***

**KẾT QUẢ THỰC HÀNH**

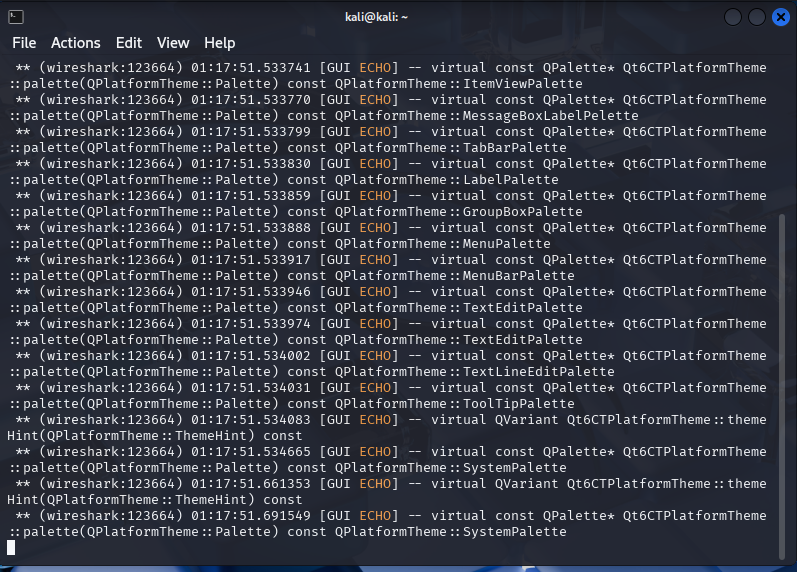
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**

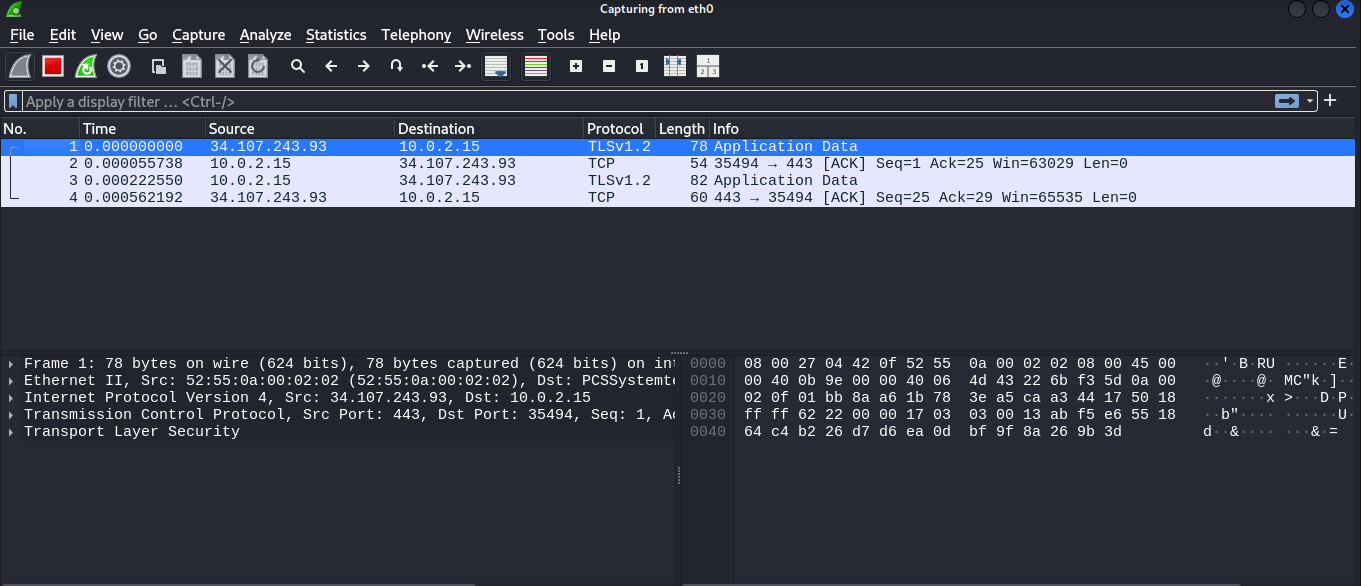
**Quét thăm dò mạng**

- Bước 1: Truy cập máy ảo Attack

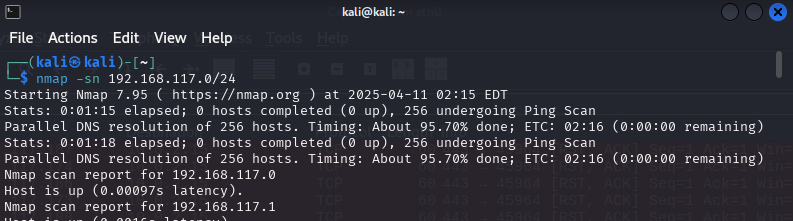


- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

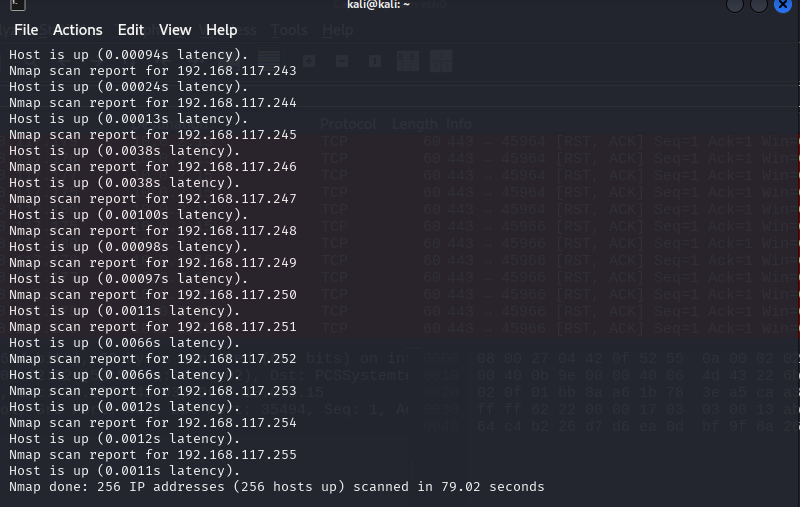




- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: nmap –sn 192.168.117.0/24



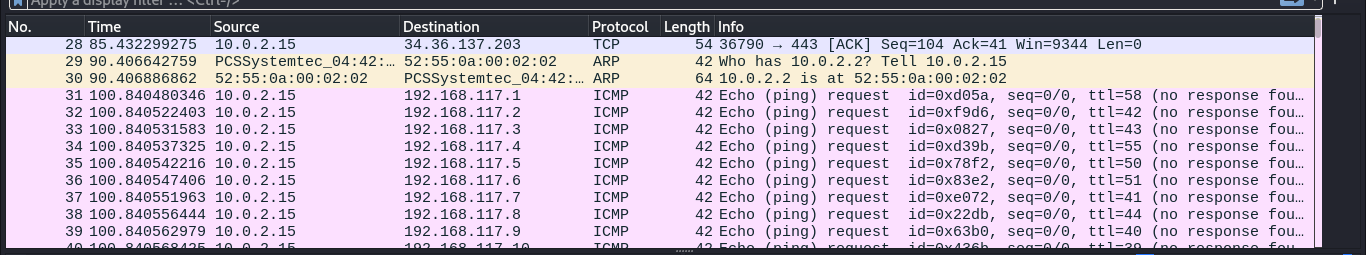
- Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:



- Bước 5: Dừng bắt gói tin trên

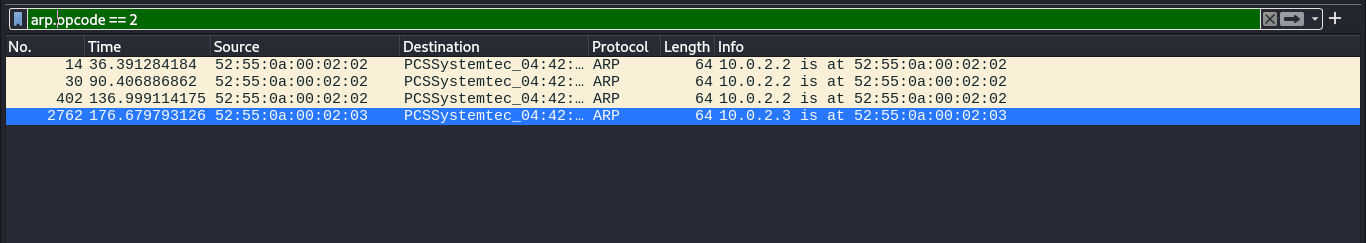
Wireshark Phân tích lưu lượng:

- 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 192.168.117.0/24



- 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.



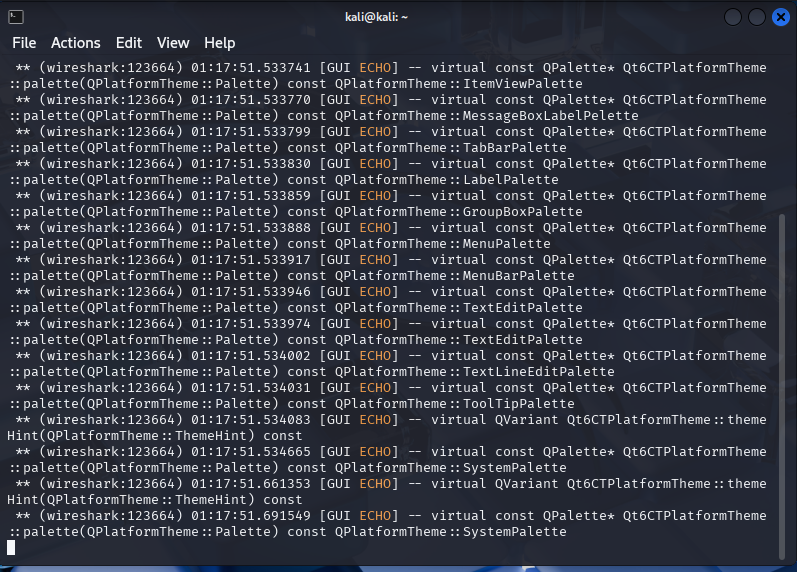
**Quét thăm dò dịch vụ**

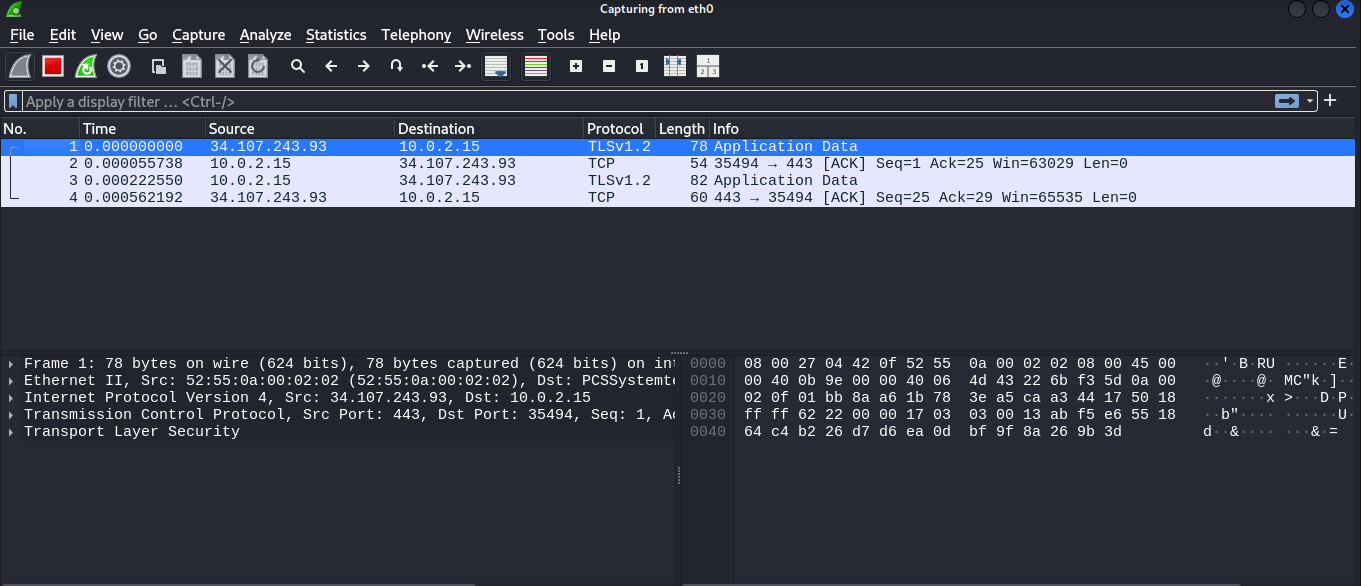
Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

- Bước 1: Truy cập máy ảo Attack

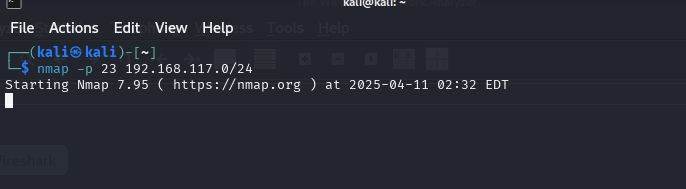


- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

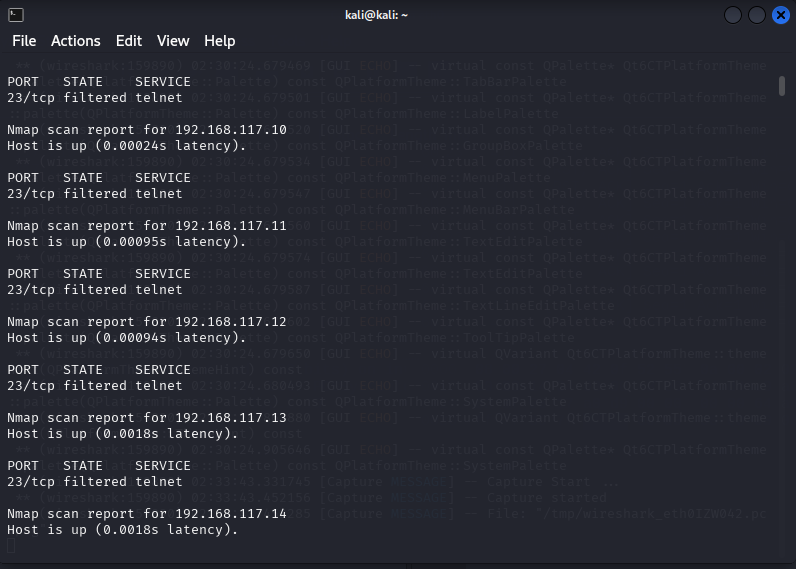




- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: sudo nmap -p 23 192.168.117.0/24



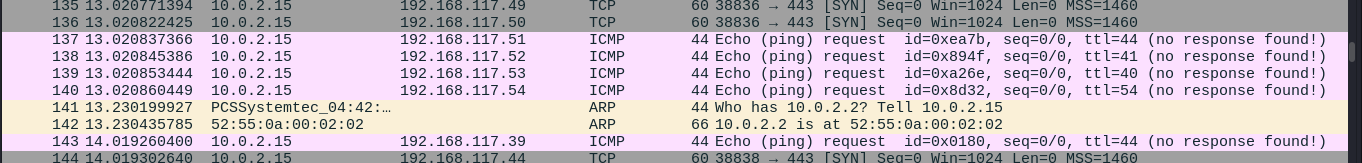
- Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.



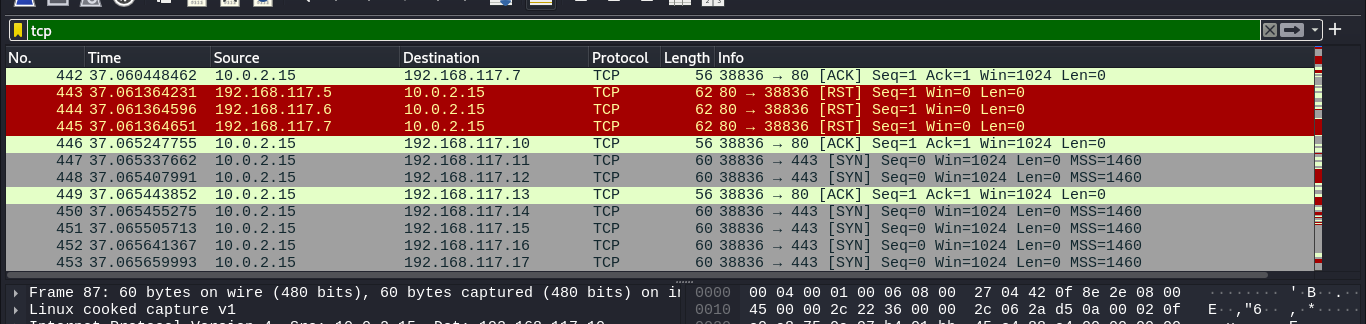
- Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng: 5

- 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 192.168.117.0/24.



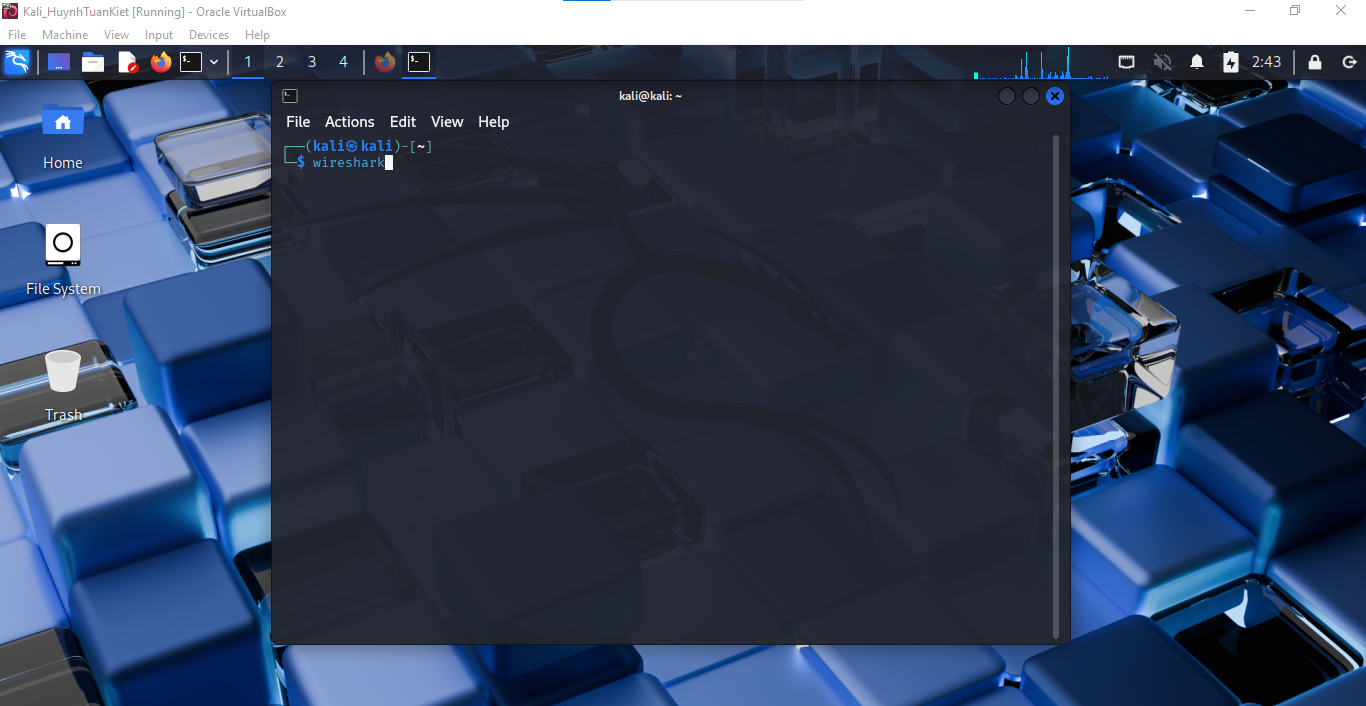
- Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 23 của các máy đang hoạt động.



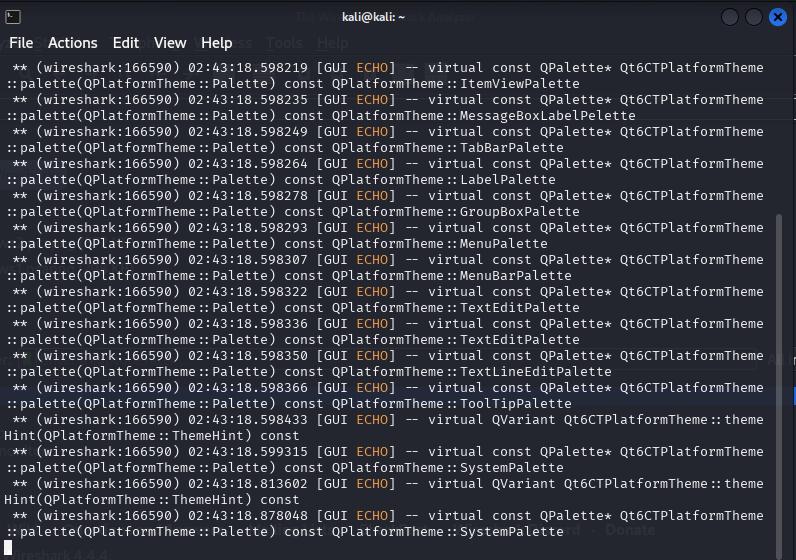
Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

**Quét cổng dịch vụ**

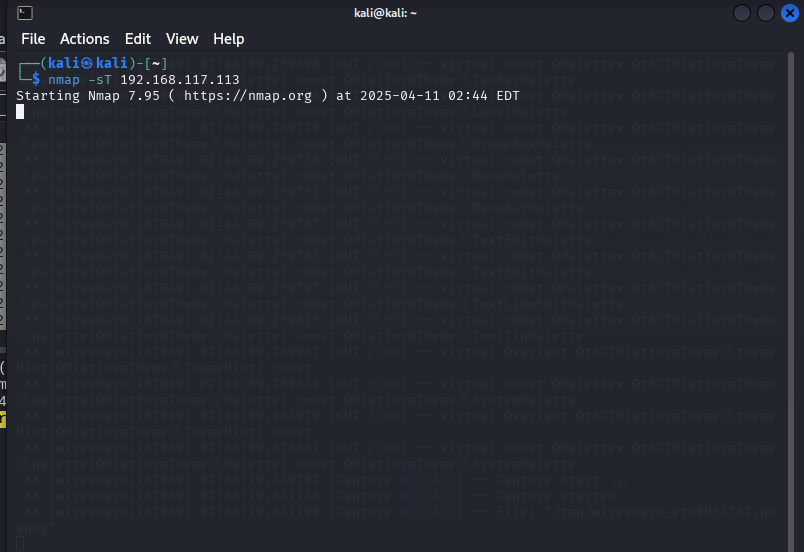
- Bước 1: Truy cập máy ảo Attack



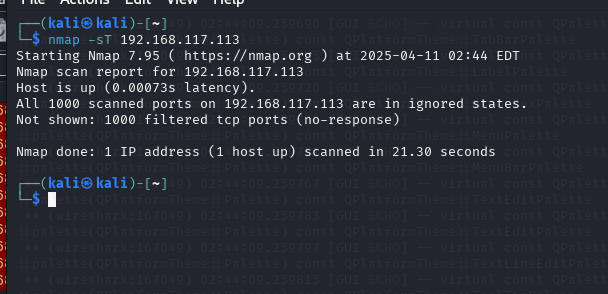
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.



- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: nmap -sT 192.168.117.13



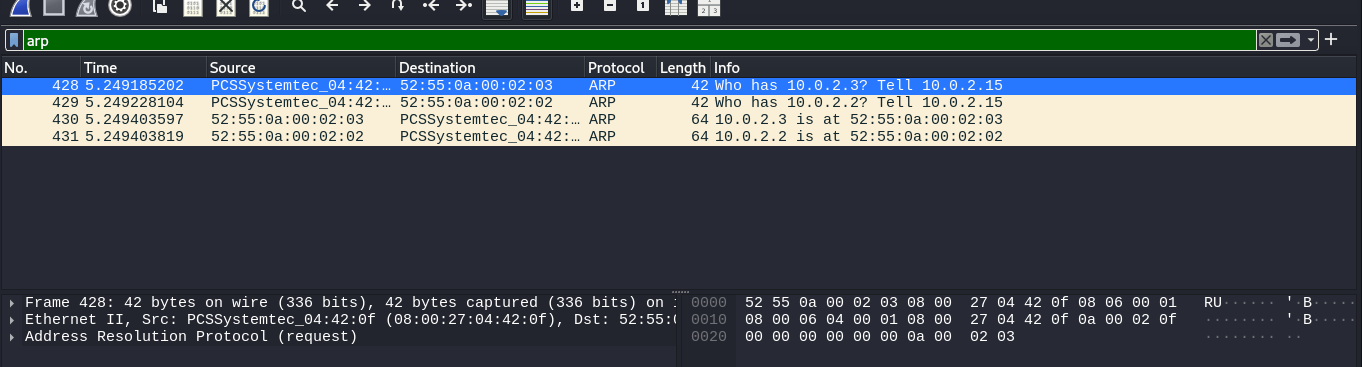
- Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 22, 23, 53 trên máy mục tiêu 192.168.117.13 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

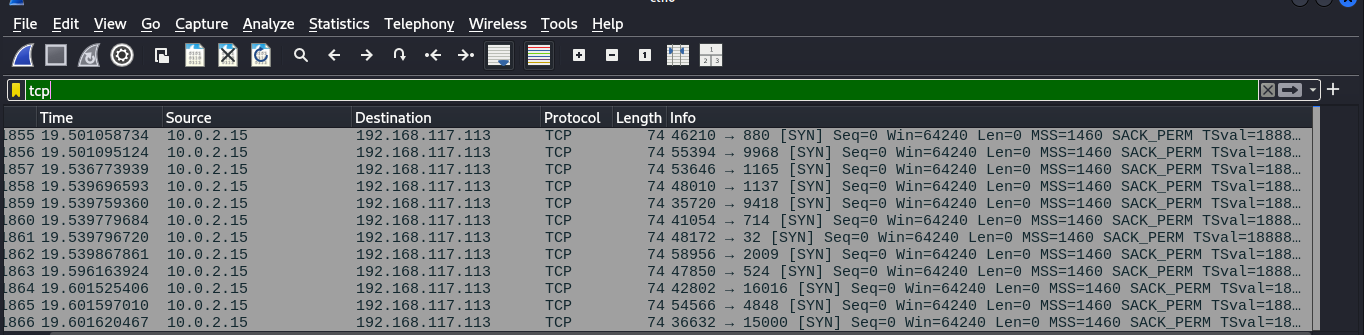


- Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

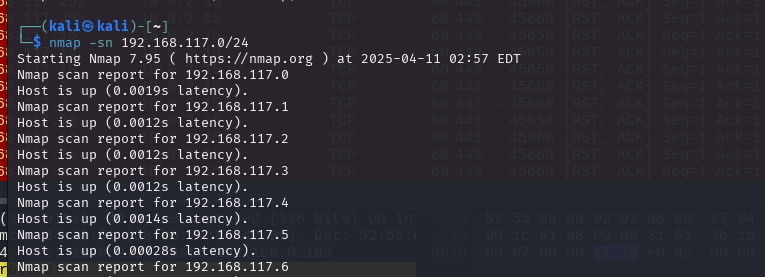
- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói 7 tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.13. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.

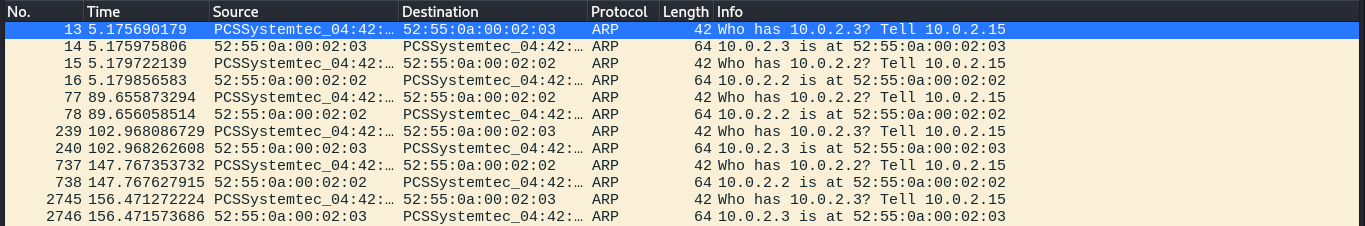




- Sử dụng giá trị tcp && ip.addr == 192.168.117.13 ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 12, 16, 17 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin 30) để hủy kết nối này.

* 1. **Kịch bản 1**
     + Ảnh chụp kết quả thực hiện của nmap: **0.5 điểm**

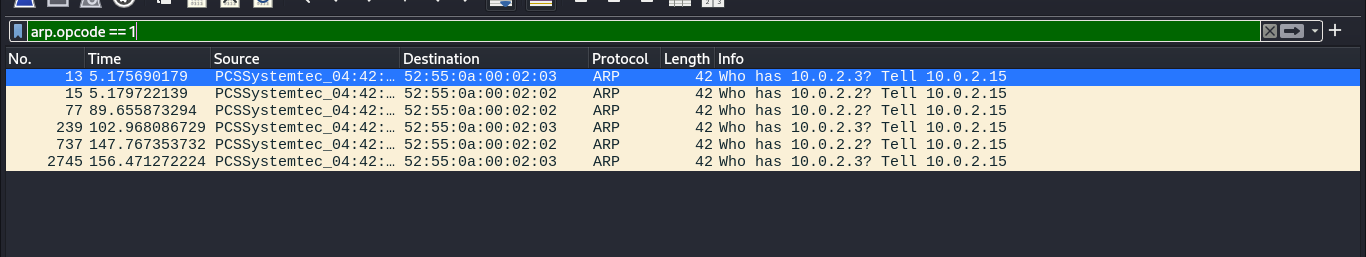


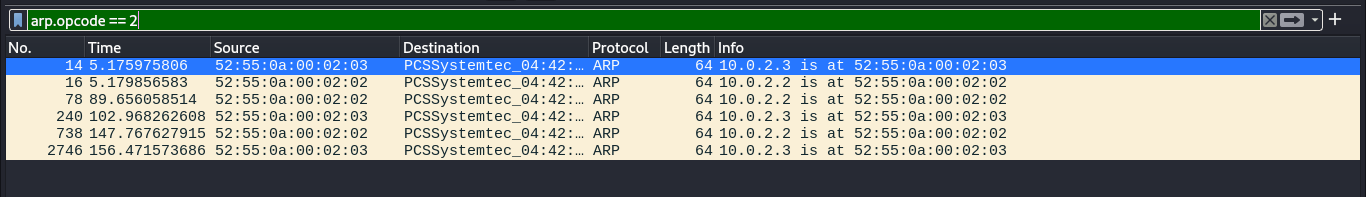


* + - Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: **1 điểm**

Kỹ thuật quét: ARP Ping Scan

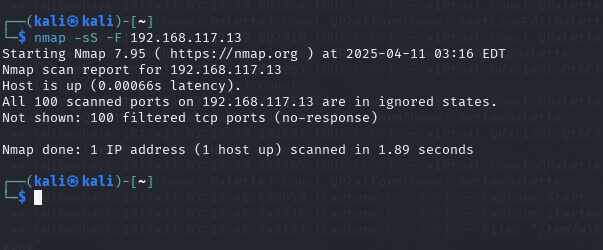
Dấu hiệu: Các gói tin ARP Request được gửi từ máy bạn đến nhiều IP, và ARP Reply trả về từ các IP đang hoạt động.





# Kịch bản 2

* + - Ảnh chụp kết quả thực hiện của nmap: **0.5 điểm**



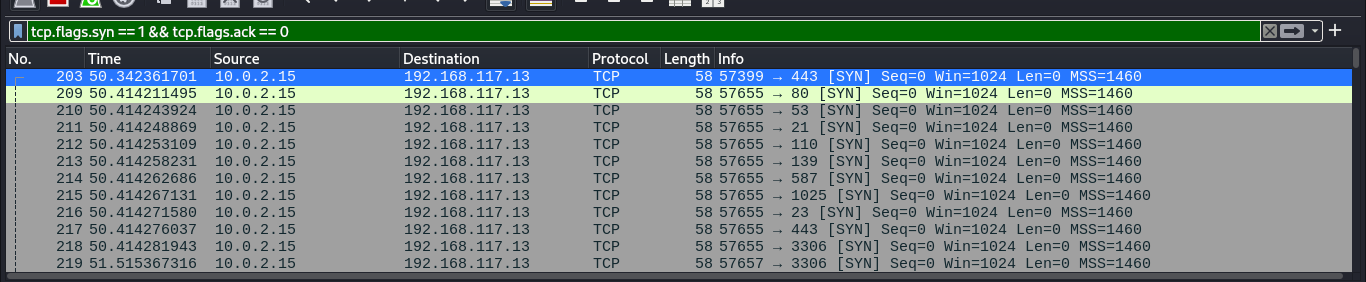
* + - Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: **1 điểm**

Kỹ thuật quét: TCP SYN Scan

Dấu hiệu:

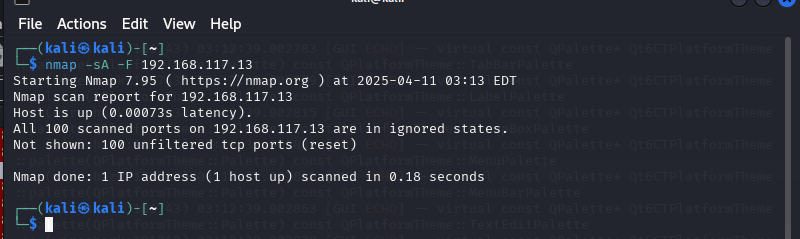
Máy do thám gửi gói SYN

Máy mục tiêu phản hồi bằng SYN/ACK nếu cổng mở



# Kịch bản 3

* + - Ảnh chụp kết quả thực hiện của nmap: **0.5 điểm**



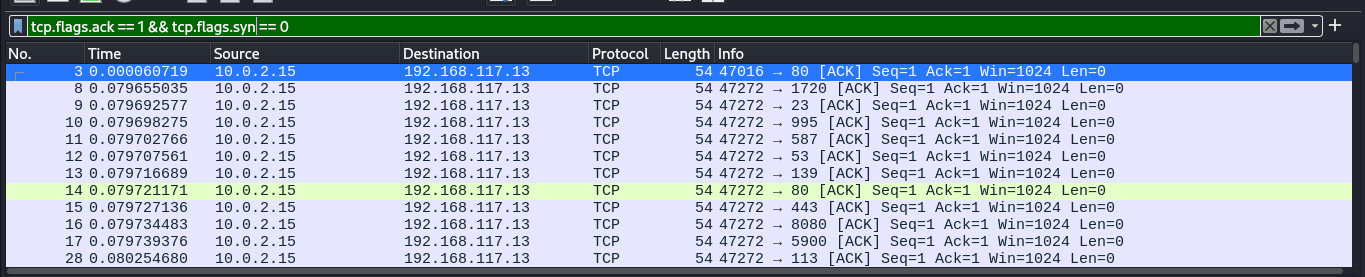
* + - Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: **1 điểm**

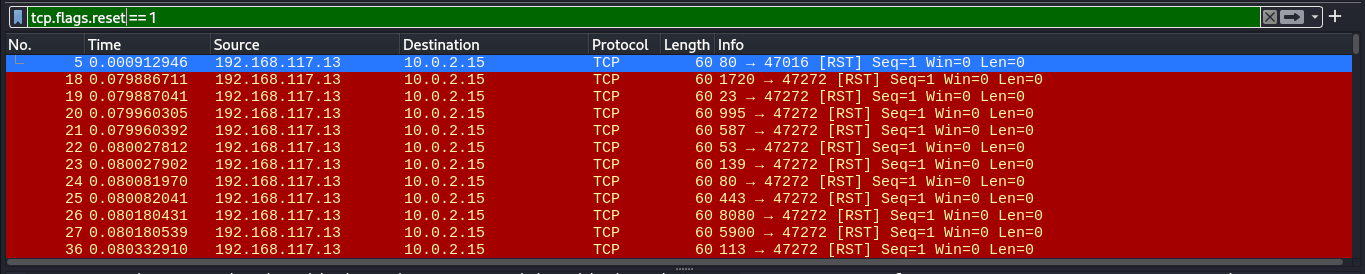
Kỹ thuật quét: TCP ACK Scan

Dấu hiệu:

Gửi các gói ACK tới các cổng khác nhau

Nhận được TCP RST từ các cổng nghĩa là cổng đang lọc



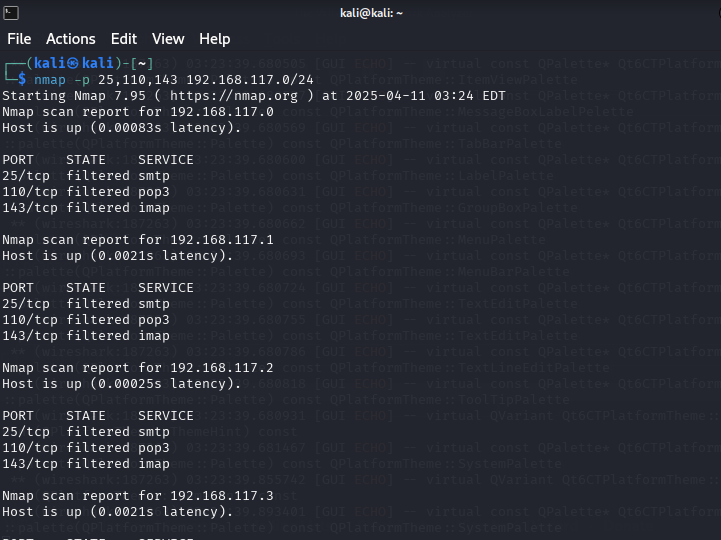


# Thu thập thông tin hệ thống

* 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)**

**Lệnh quét thăm dò tìm kiếm máy chủ email:**

**nmap -p 25,110,143 192.168.117.0/24**

****

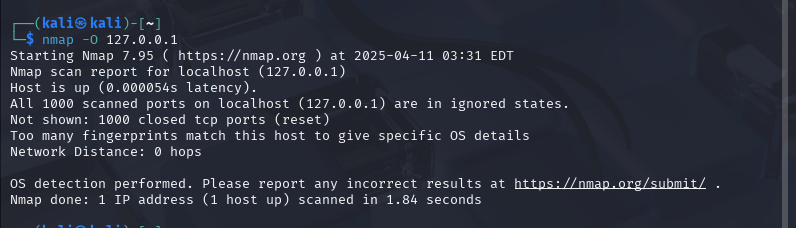
|  |  |
| --- | --- |
| nmap | Công cụ quét mạng và cổng phổ biến, dùng để dò quét các máy chủ trong mạng. |

|  |  |
| --- | --- |
| -p 25,110,143 | Chỉ định quét các cổng phổ biến của máy chủ email:  • Cổng 25: SMTP – dùng để gửi email  • Cổng 110: POP3 – dùng để nhận email theo kiểu tải về  • Cổng 143: IMAP – dùng để nhận email theo kiểu giữ lại trên server |

|  |  |
| --- | --- |
| 192.168.117.0/24 | Mạng nội bộ cần quét (24-bit subnet), tức là quét tất cả các địa chỉ IP từ 192.168.117.1 đến 192.168.117.254 |

# Thông tin hệ điều hành:

* Hình ảnh chụp kết quả của nmap: 0.25 điểm



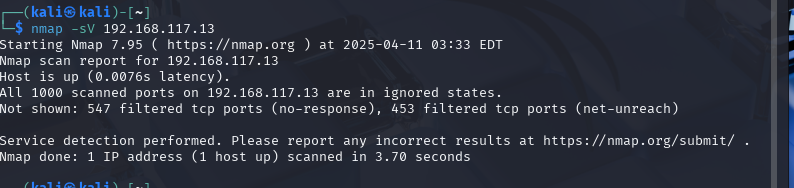
* Nêu tên và phiên bản hệ điều hành: 0.25 điểm

Kali Linux

2025.1a

# 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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)** |
|  |  |  |
|  |  |  |