BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Nguyễn Thanh Trường***

***MSSV: 1050080082***

***Yêu cầu kết quả thực hành:***

**KẾT QUẢ THỰC HÀNH**

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

*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*

Thực hiện lệnh quét **nmap –sn Dia\_chi\_mang/Mat\_na** trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là **task1.pcap**.

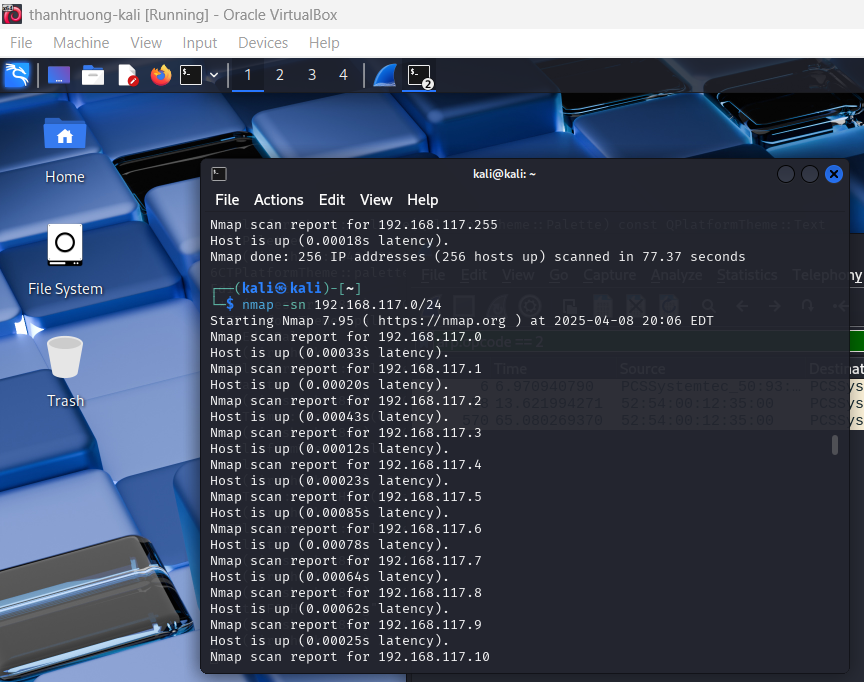
**Quét thăm dò mạng**

- **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:

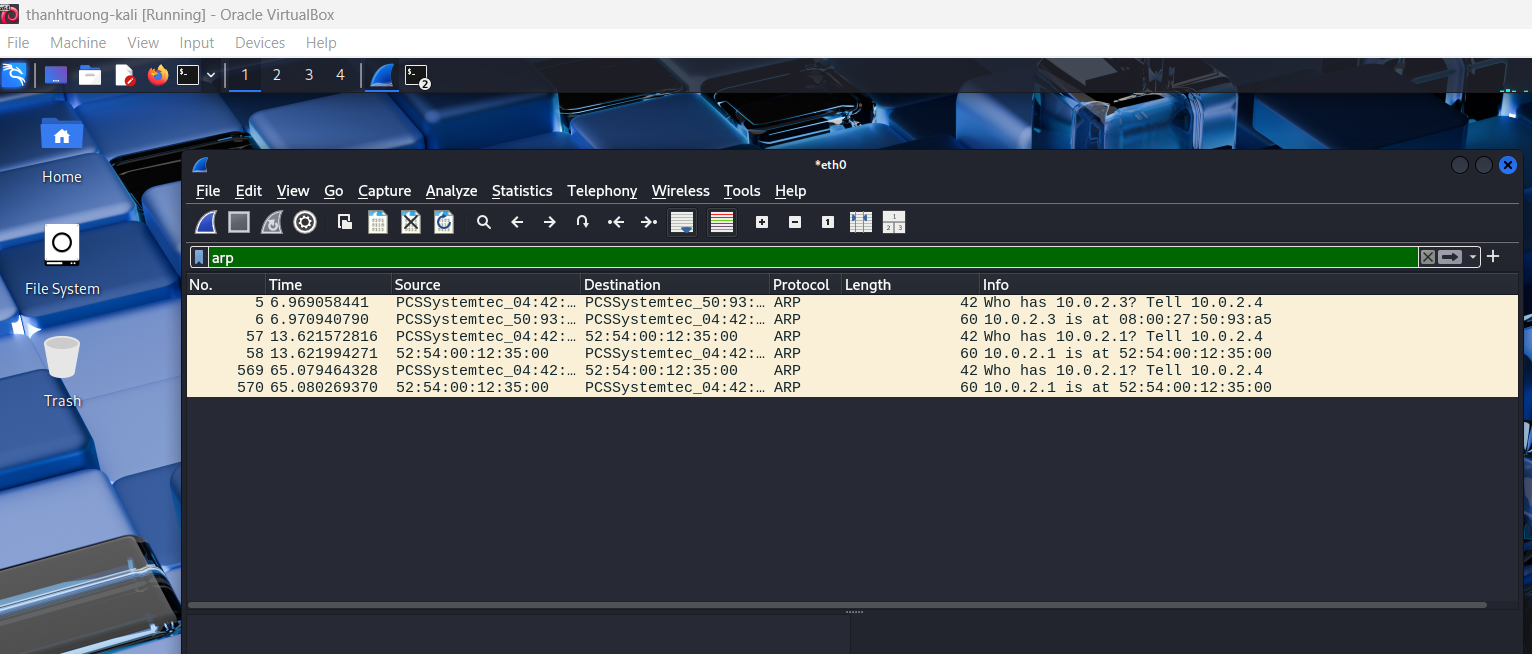


Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.1, 192.168.117.2 và 192.168.117.3,.....

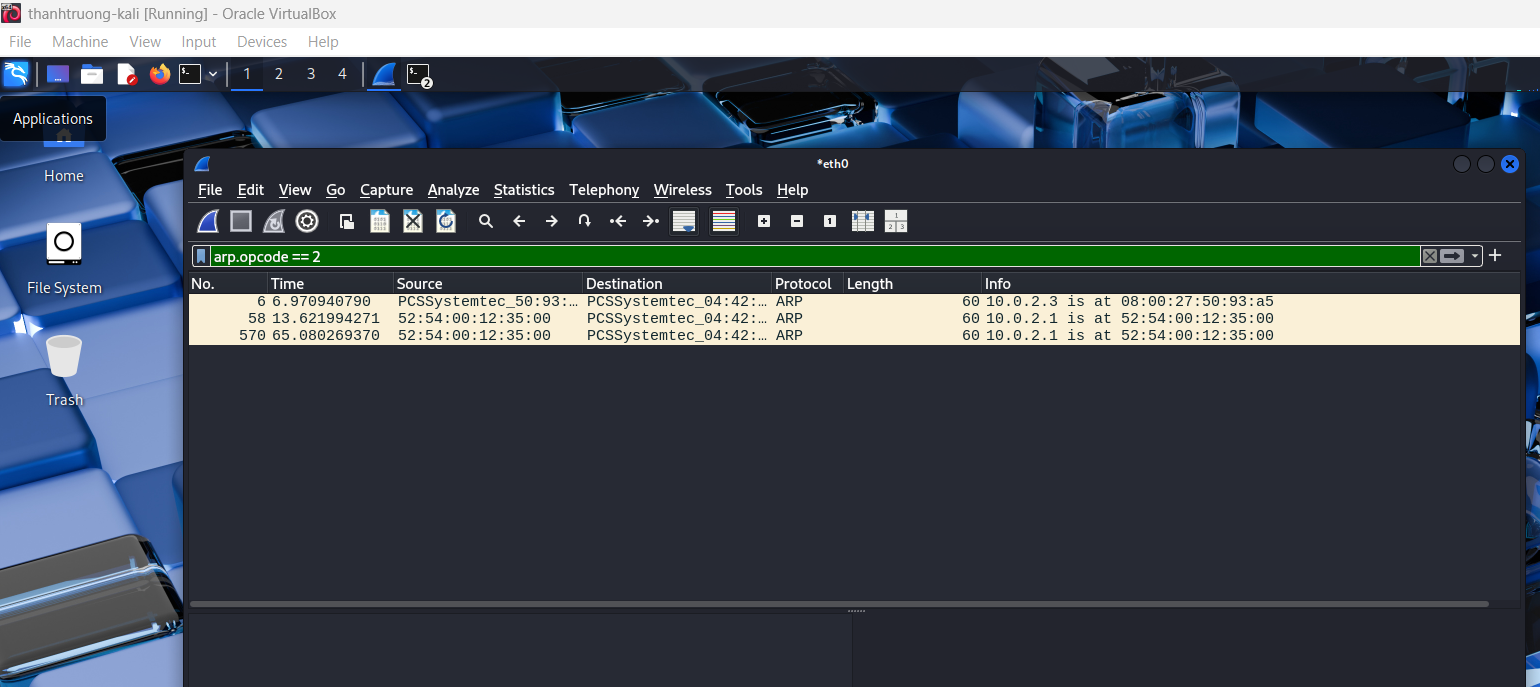
**Bước 5:** Dừng bắt gói tin trên Wireshark

**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.



**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.

**Quét thăm dò dịch vụ**

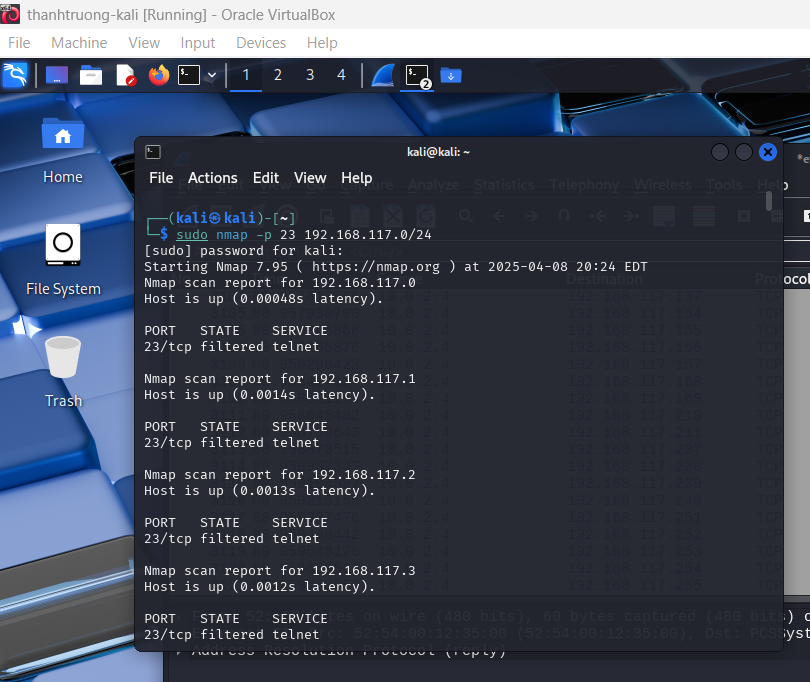
Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

- **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**

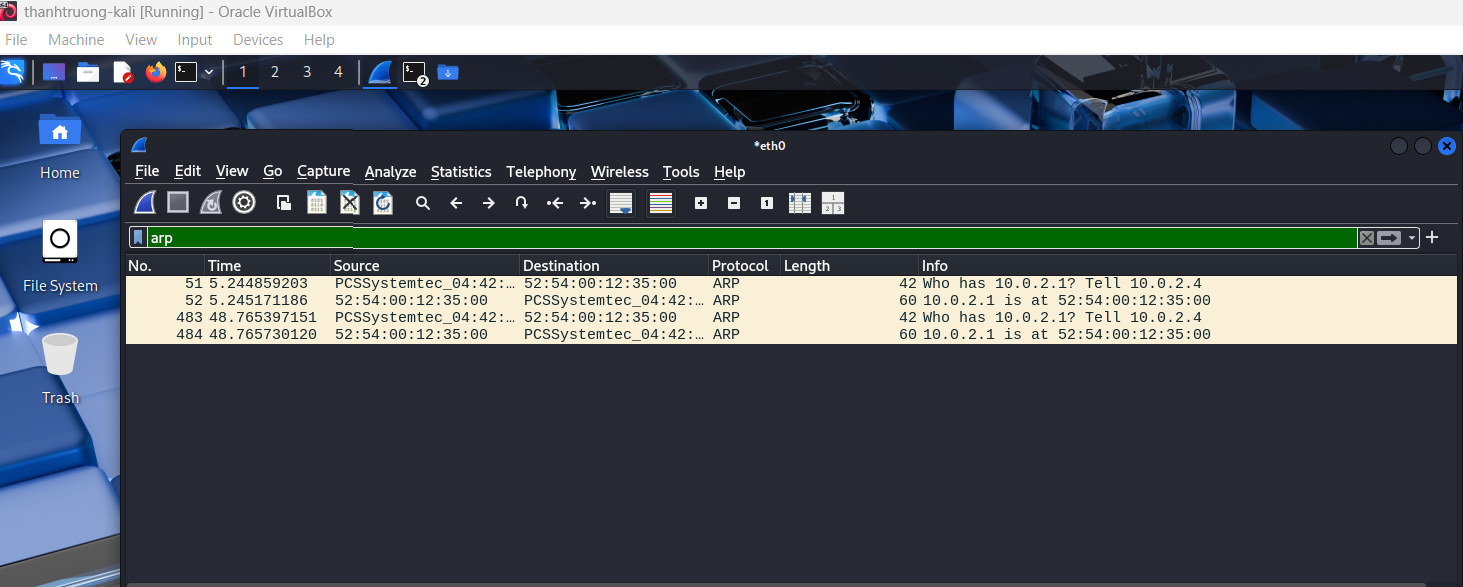
- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.1 và 192.168.117.2,... có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.



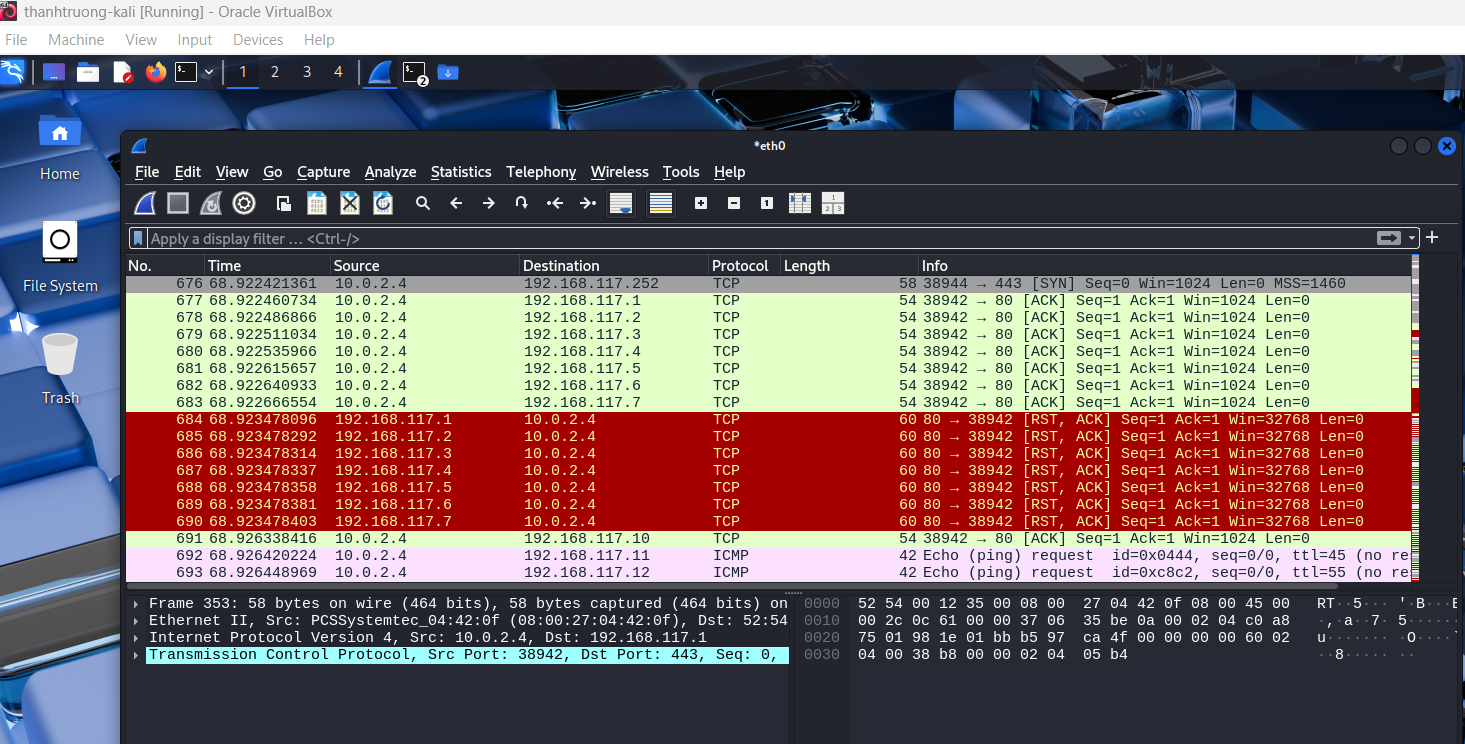
- **Bước 5:** Dừng bắt gói tin trên Wireshark

**Phân tích lưu lượng:**

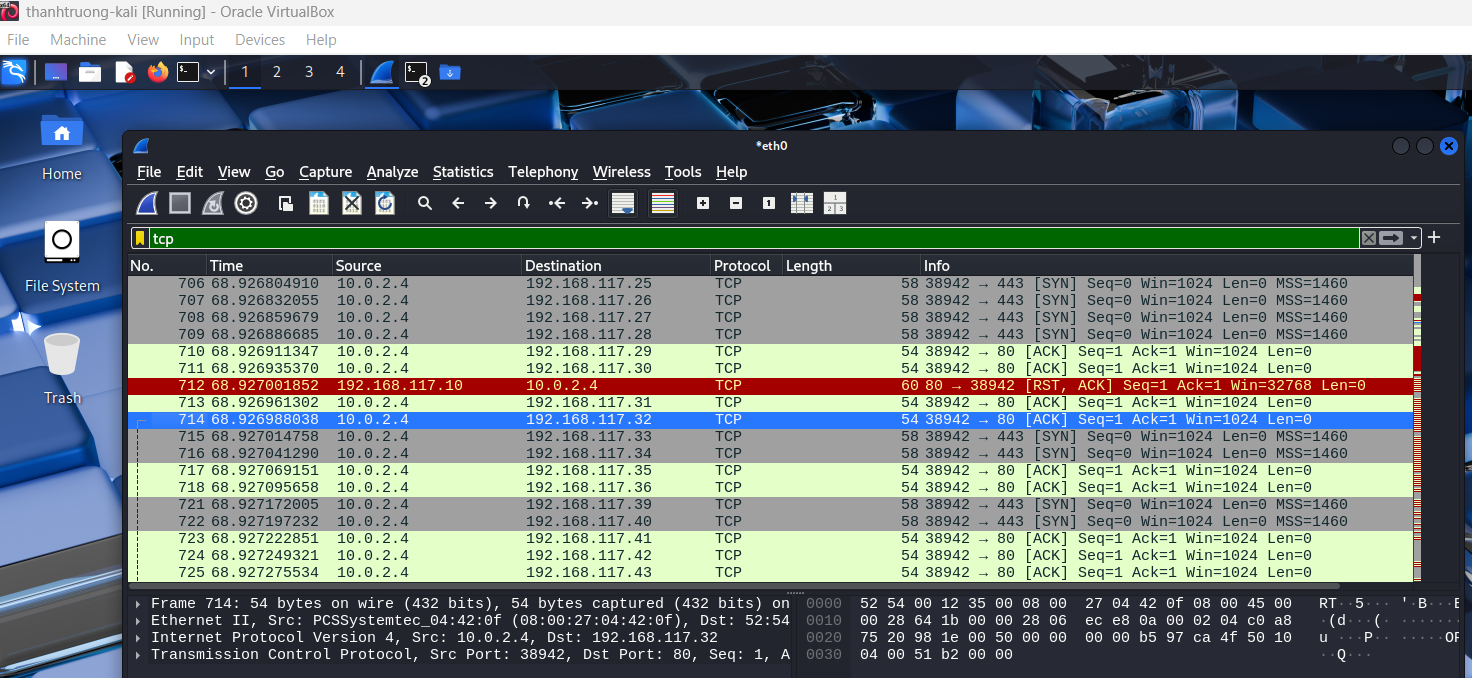
- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.117.0/24.



- Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 80 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 80 từ địa chỉ 192.168.117.10 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 Telnet)



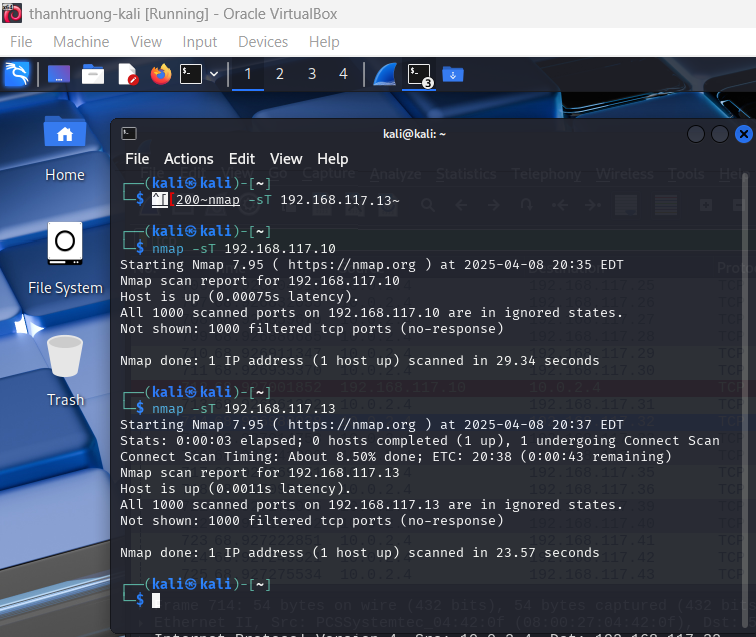
**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

**2.3. Quét cổng dịch vụ**

- **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 không có cổng dịch vụ nào trên máy mục tiêu 192.168.117.13 có trạng thái open.****

* 1. **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

*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*

Thực hiện lệnh quét **nmap –sS –F Địa\_chỉ\_IP\_máy\_mục\_tiêu** trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là **task2.pcap**.

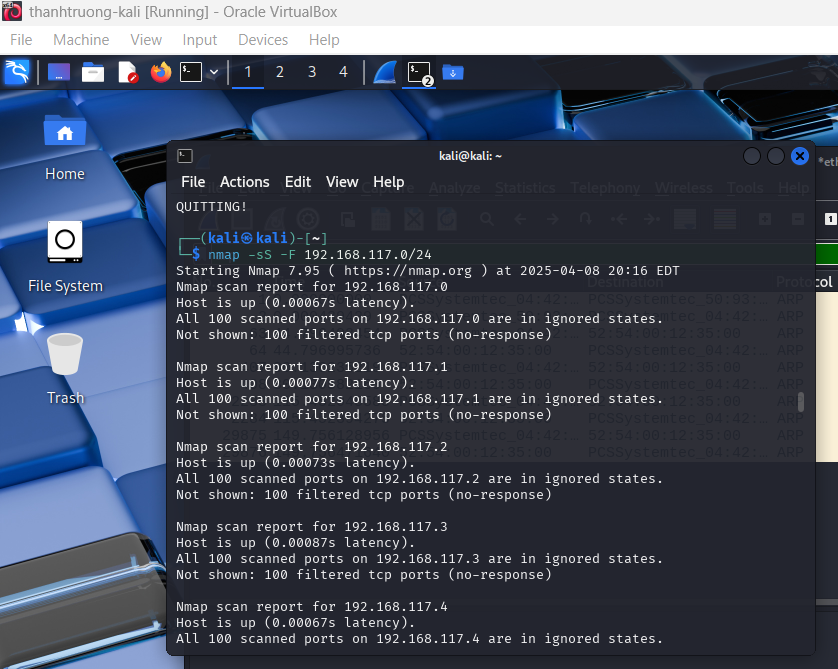
**Quét thăm dò mạng**

- **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 –sS -F 192.168.117.0/24

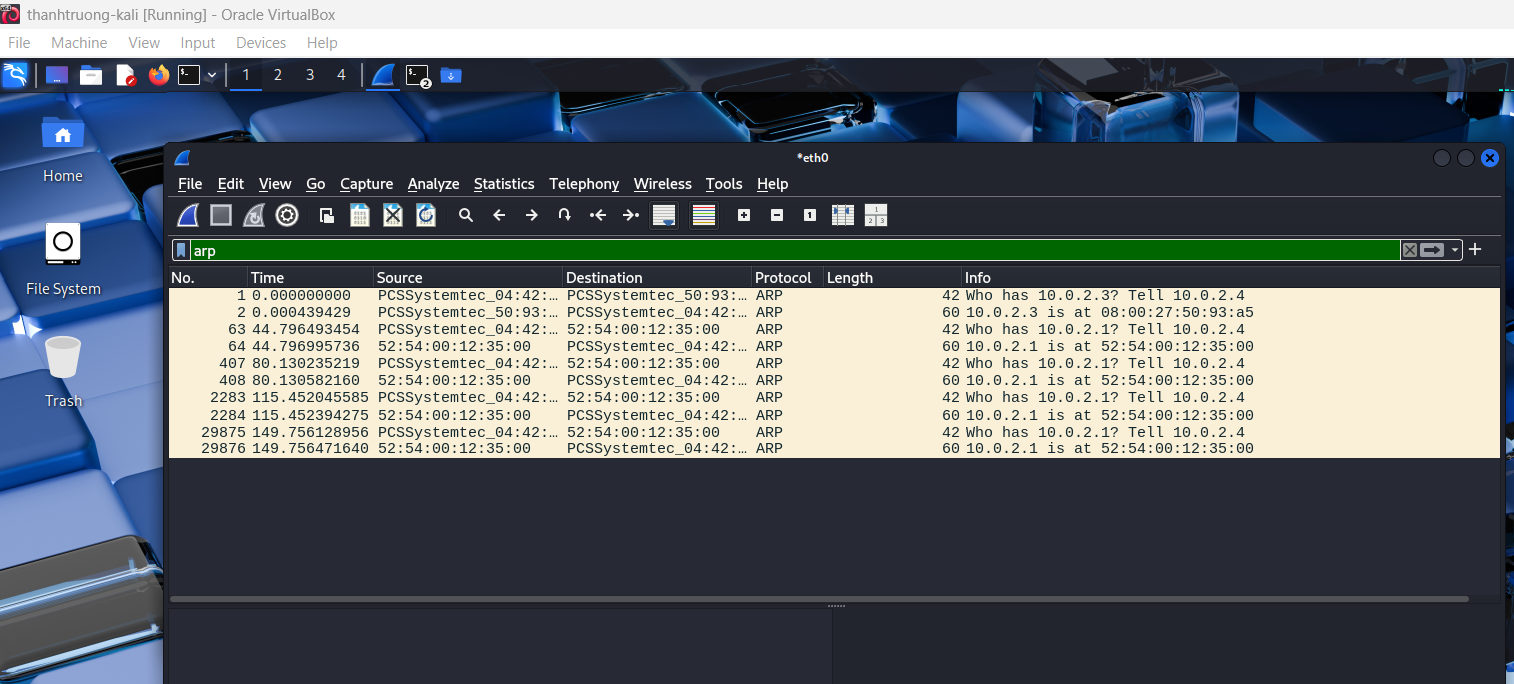
- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:



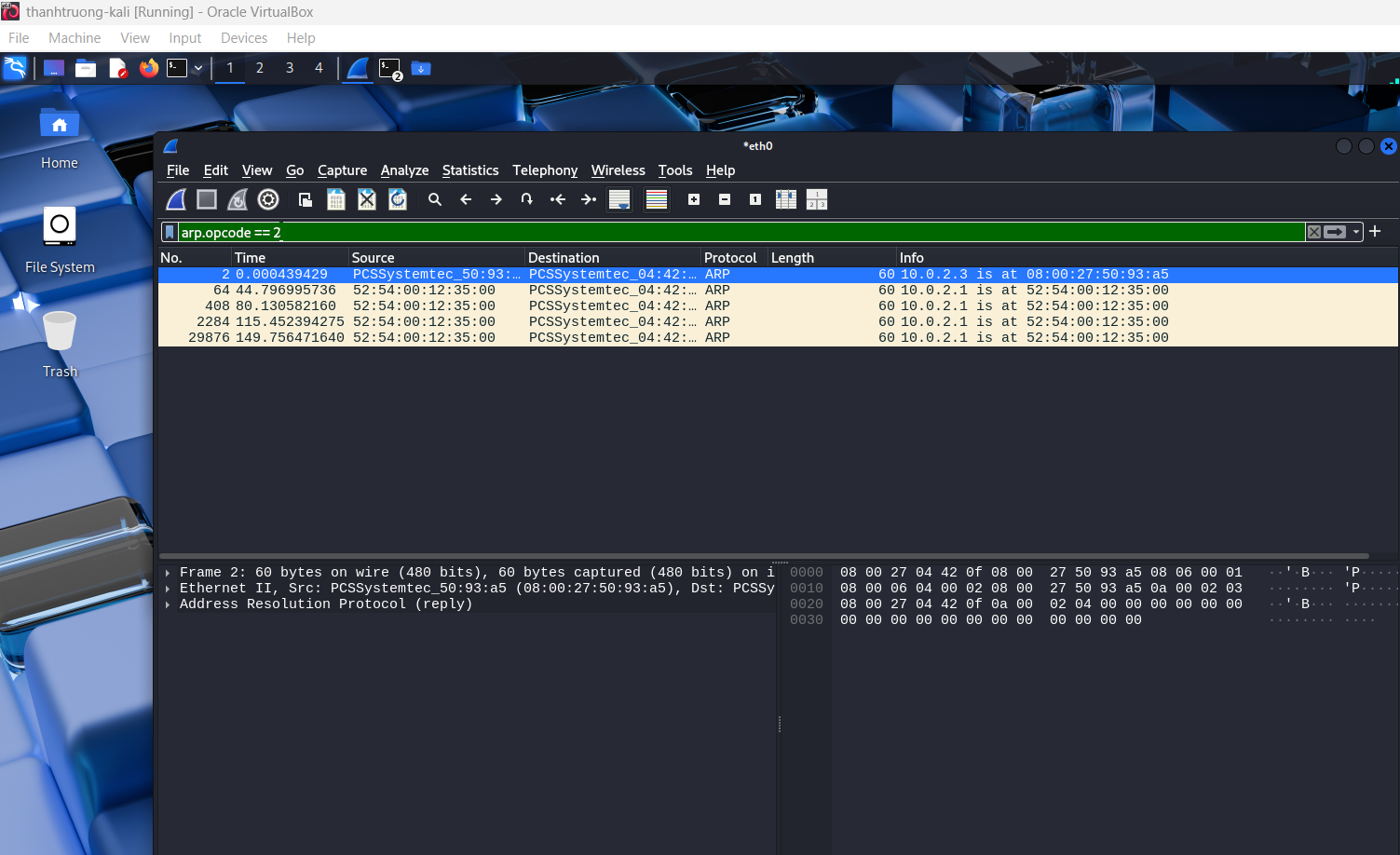
**Bước 5:** Dừng bắt gói tin trên Wireshark

**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.



**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.

* 1. **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

*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*

Thực hiện lệnh quét **nmap –sA –F Địa\_chỉ\_IP\_máy\_mục\_tiêu** trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là **task3.pcap**.

**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 –sA -F 192.168.117.0/24

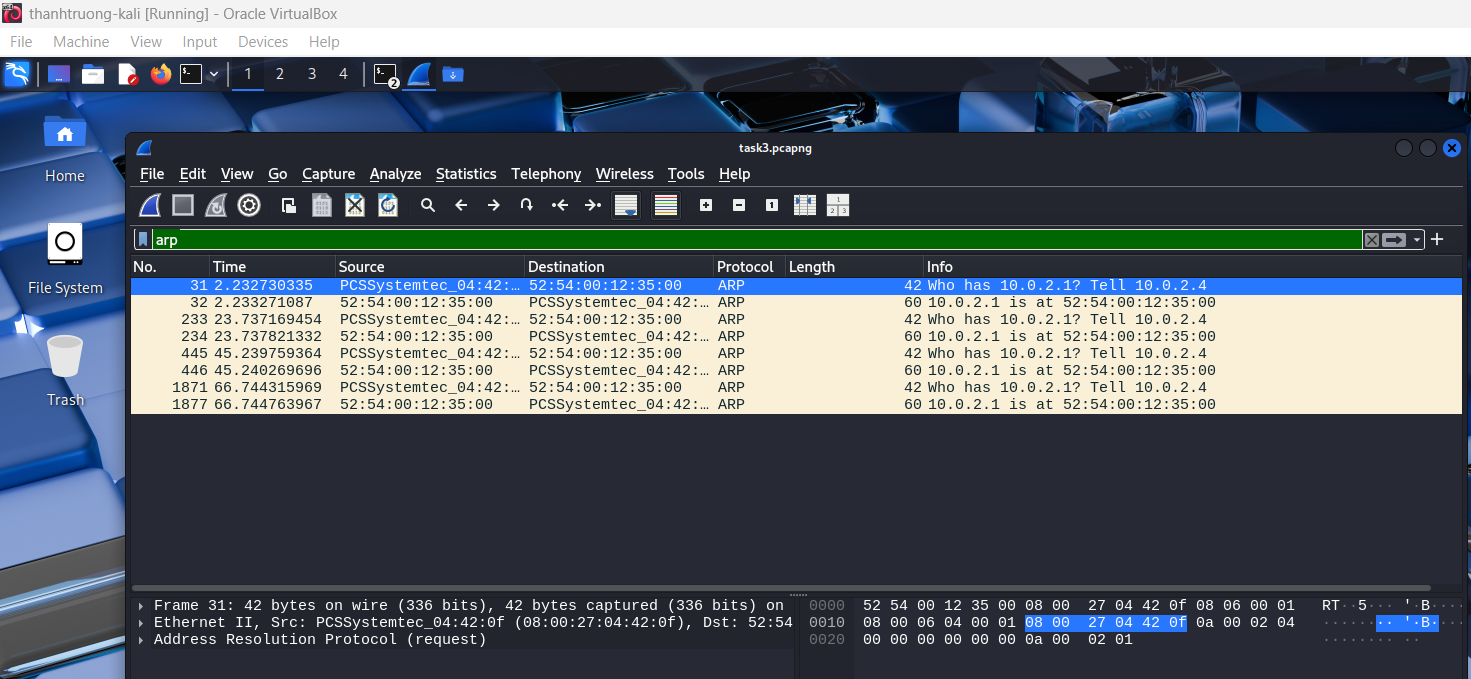
- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:



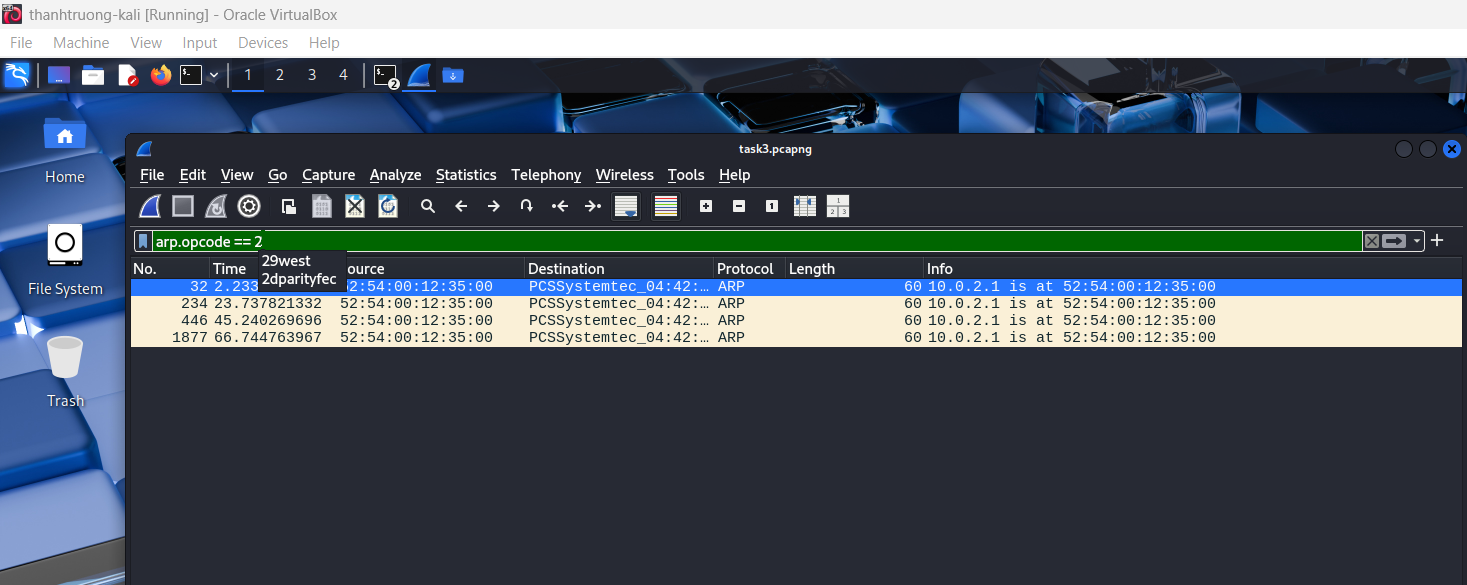
- **Bước 5:** Dừng bắt gói tin trên Wireshark

**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



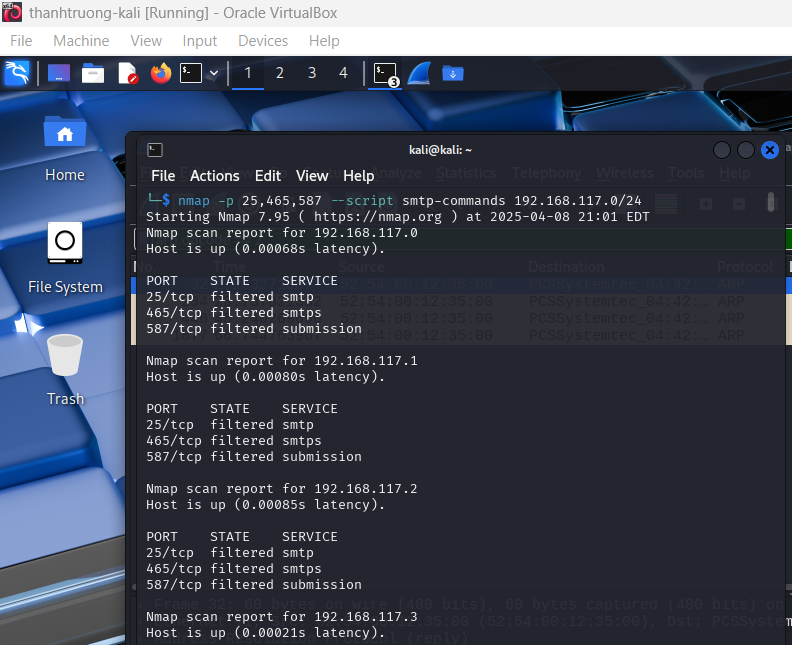
- Trên cửa sổ của Wireshark, sử dụng giá trị **arp.opcode == 2** cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



**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.

1. **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 là:  
   **nmap -p 25,465,587 --script smtp-commands <IP>**
* Trong đó:
  + nmap: Công cụ dùng để quét mạng và tìm kiếm dịch vụ.
  + -p 25,465,587:
    - Quét các cổng thường được dùng bởi máy chủ email:
    - • 25: SMTP
    - • 465: SMTPS (SMTP over SSL)
    - • 587: SMTP (gửi mail có xác thực)
  + --script smtp-commands: Sử dụng script Nmap để gửi lệnh SMTP và phân tích phản hồi, giúp xác định chức năng dịch vụ email và kiểm tra các lệnh được hỗ trợ (như HELO, EHLO, VRFY, MAIL FROM, RCPT TO...)
  + <IP>: Địa chỉ IP của máy chủ cần quét.

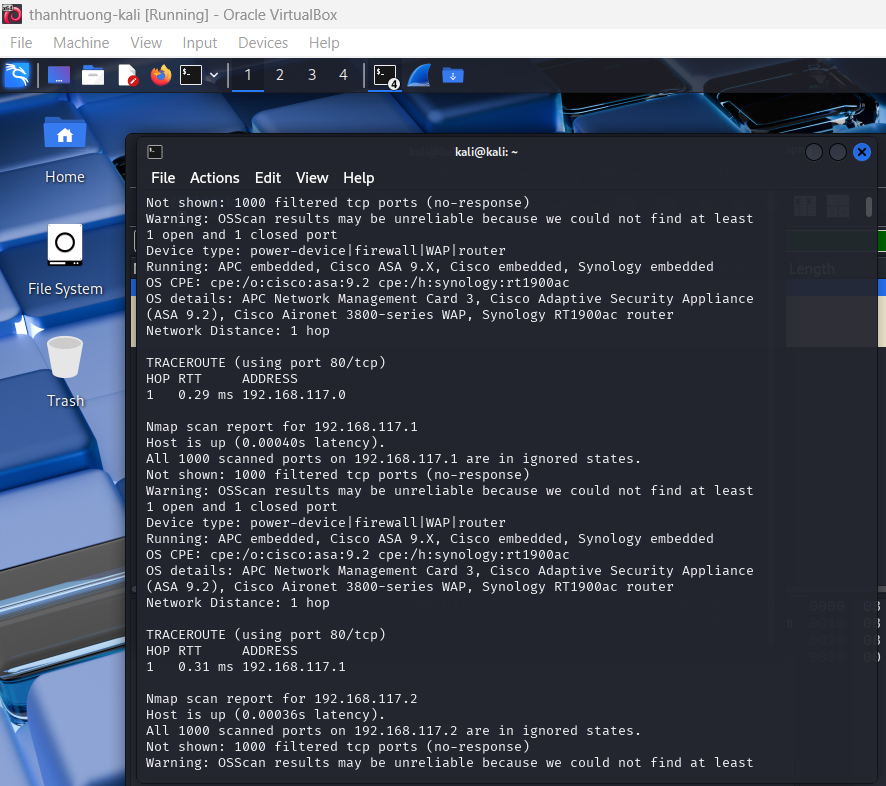


Lệnh quét thông tin hệ điều hành và dịch vụ: **nmap -A <IP>**

**Thông tin hệ điều hành:**

Tên và phiên bản hệ điều hành:

Có thể là Cisco ASA 9.X, hoặc Synology RT1900ac, hoặc hệ điều hành nhúng của APC/Cisco/Synology.



**Thông tin dịch vụ: 1 điểm**



* Không tìm thấy dịch vụ nào

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)** |
| --- | --- | --- |
| | Cisco Adaptive Security Appliance (ASA) 9.2 | | --- |  |  | | --- | | CVE-2020-3452 | Lỗ hổng cho phép truy cập thư mục tùy ý (directory traversal) qua Web Services interface. Tin tặc có thể đọc file cấu hình nhạy cảm trên thiết bị. |
| Synology RT1900ac Router | CVE-2022-43931 | Lỗ hổng thực thi mã từ xa (RCE) trong Synology VPN Plus Server cho phép kẻ tấn công thực thi mã độc mà không cần xác thực. |