Câu lệnh tải nmap: $sudo apt-get install nmap



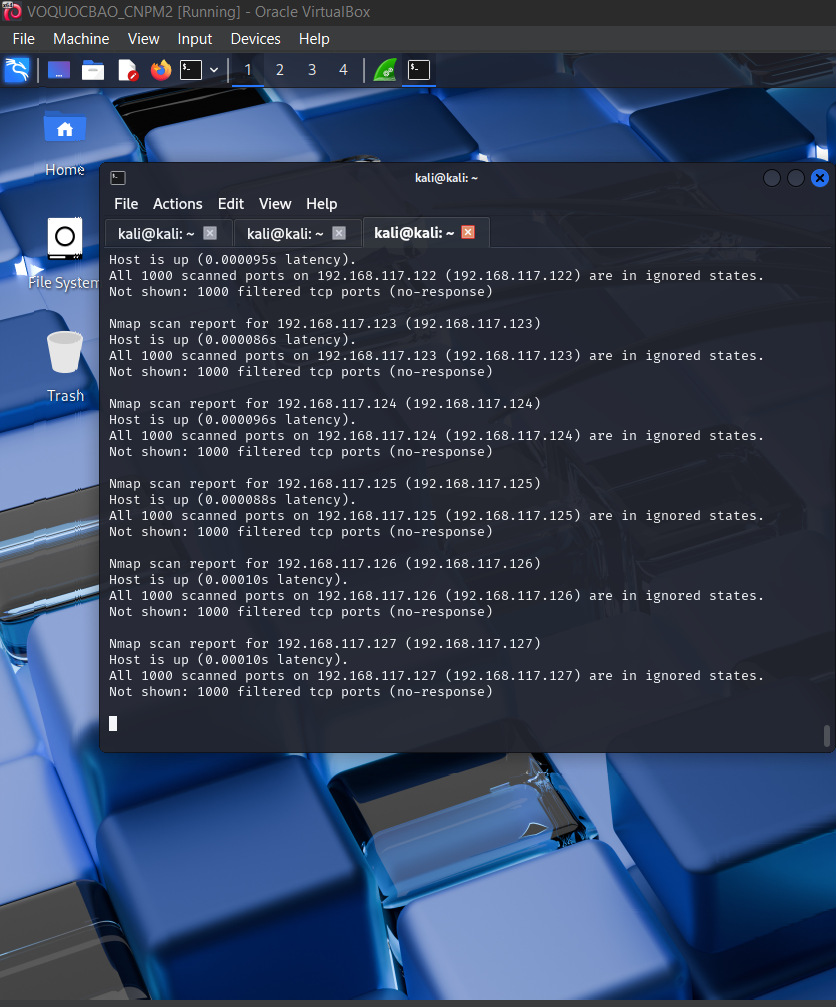
Kịch bản 1:

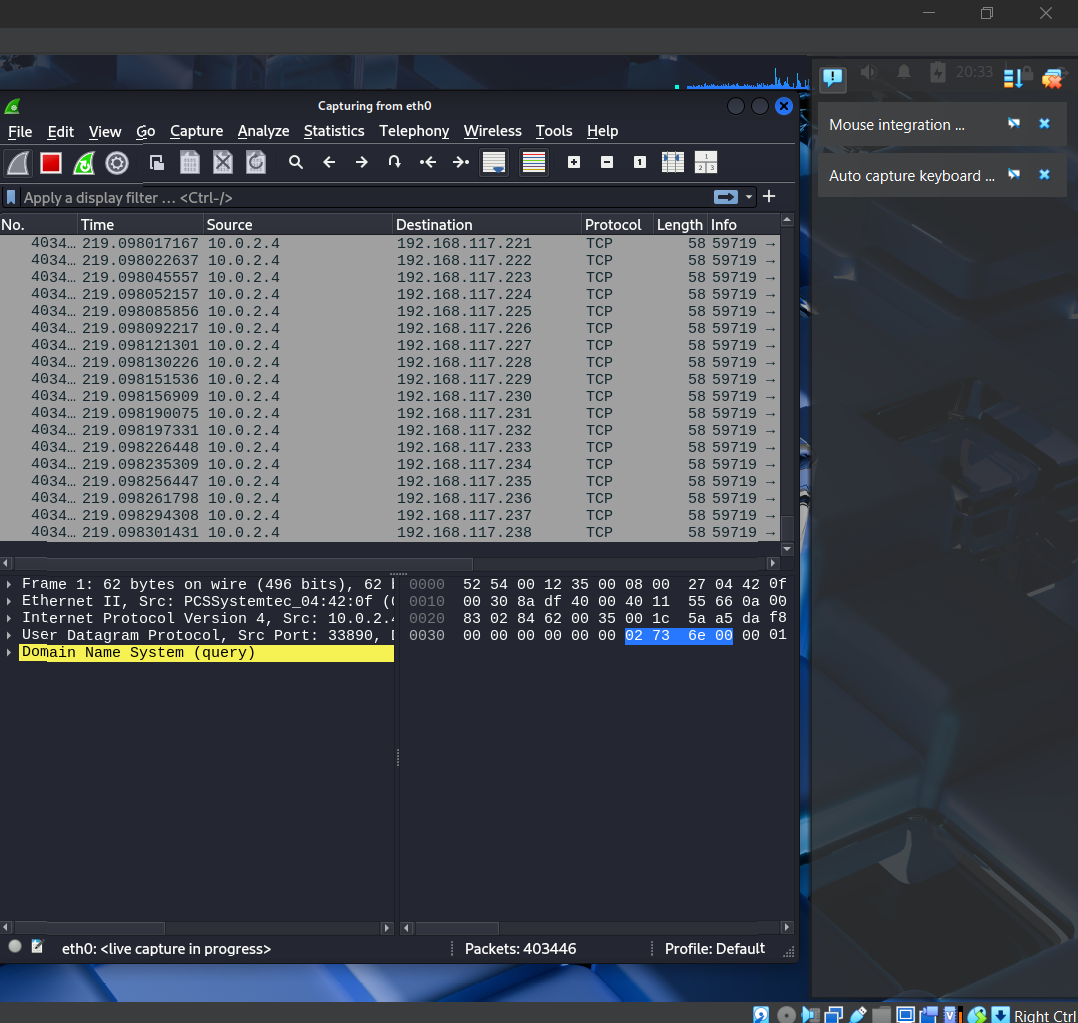
**Quét thăm dò mạng**

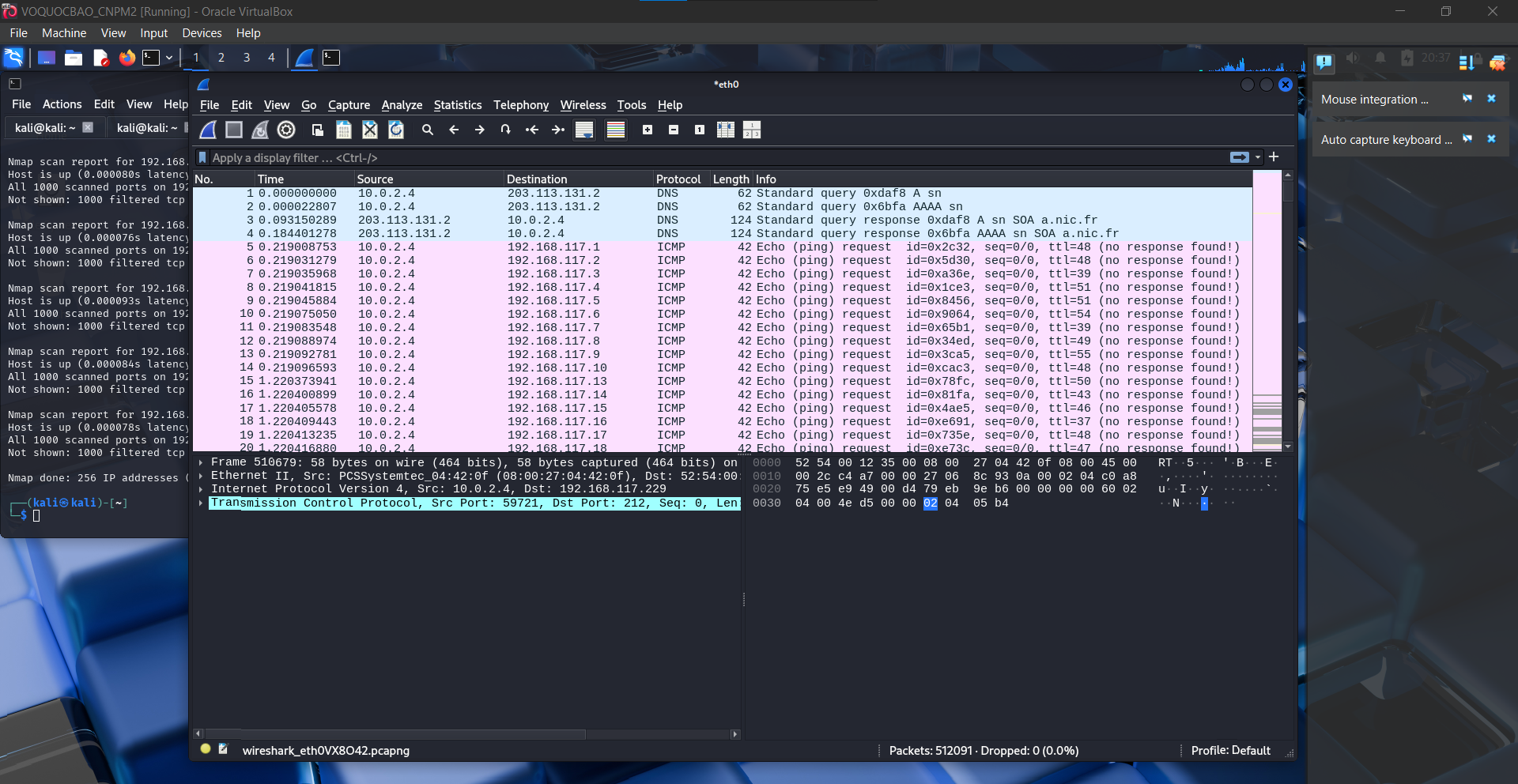
Mở 1 terminal để bật wireshark

Mở thêm 1 termianl để ghi lệnh dưới:

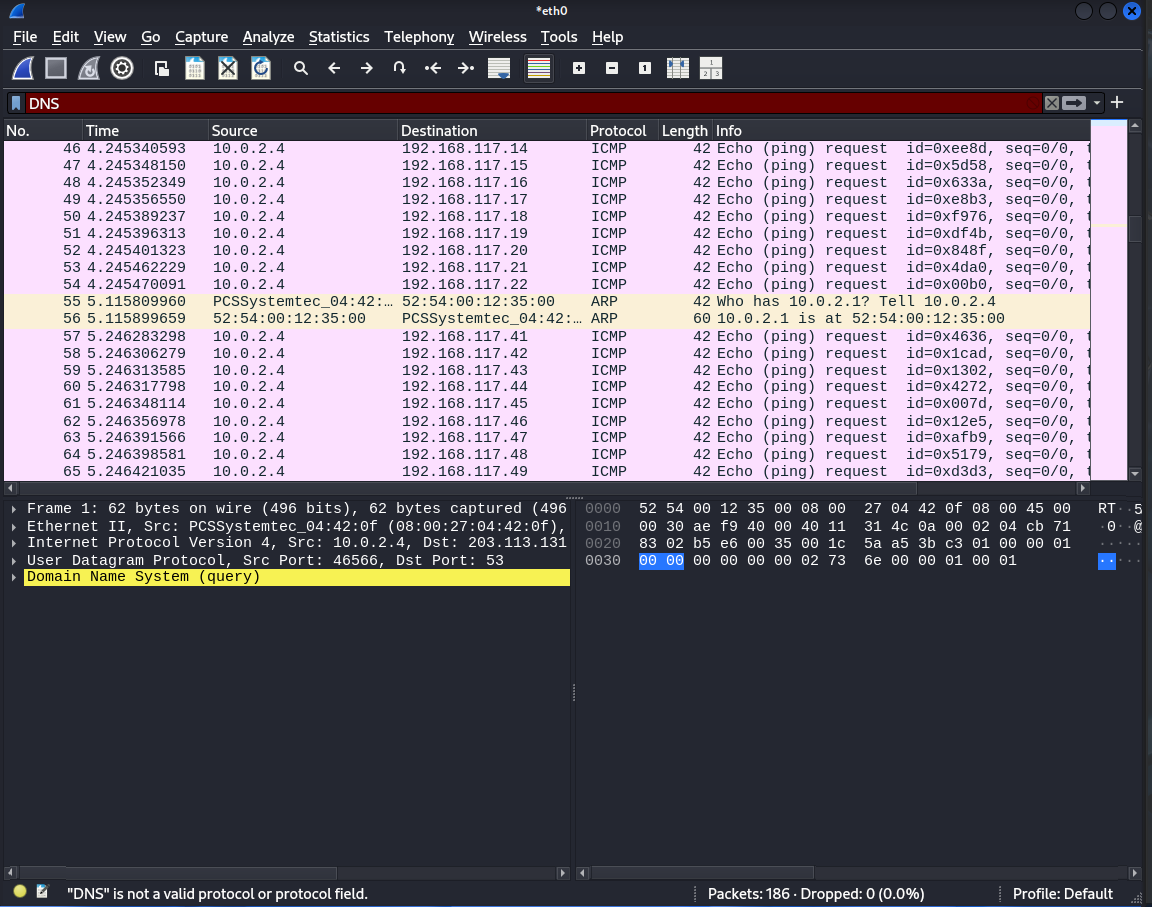
nmap sn 192.168.117.0/24







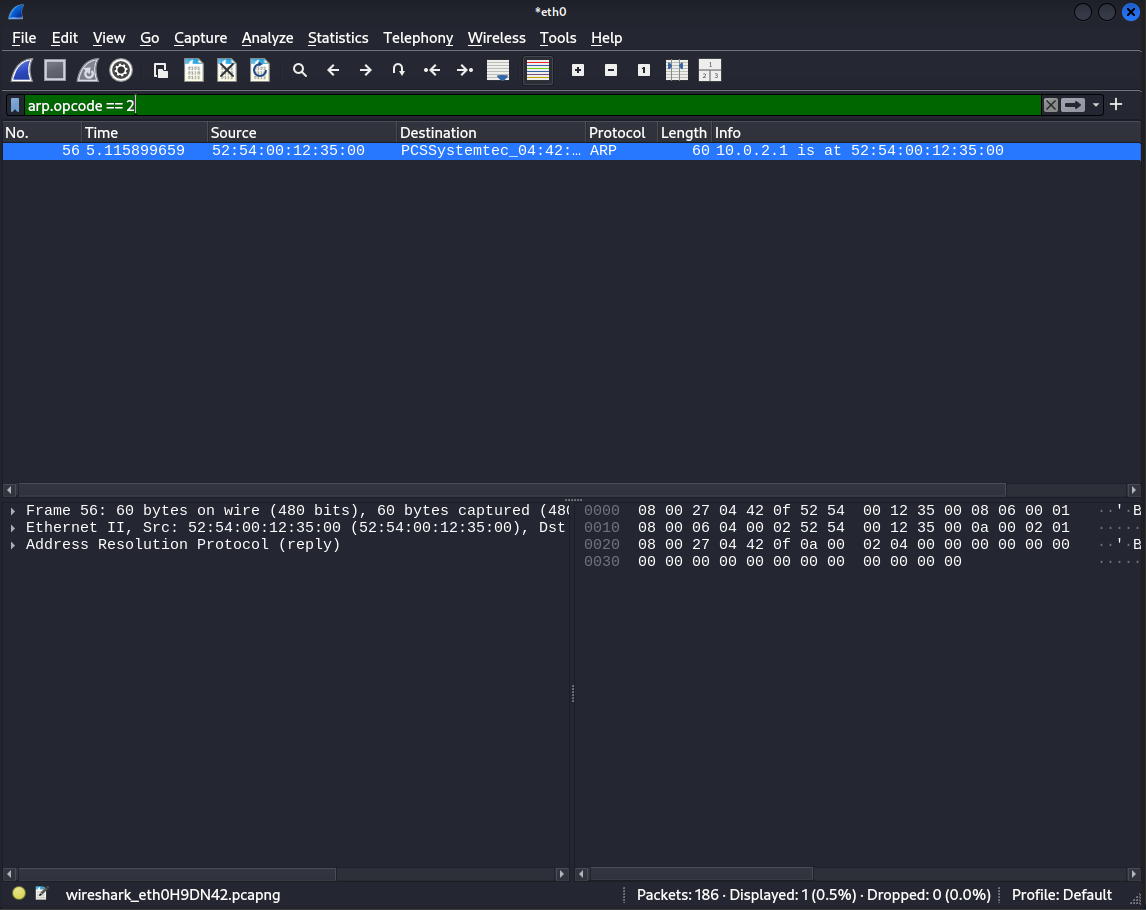
Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính

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 luận:

* Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

Kịch bản 2:

**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.

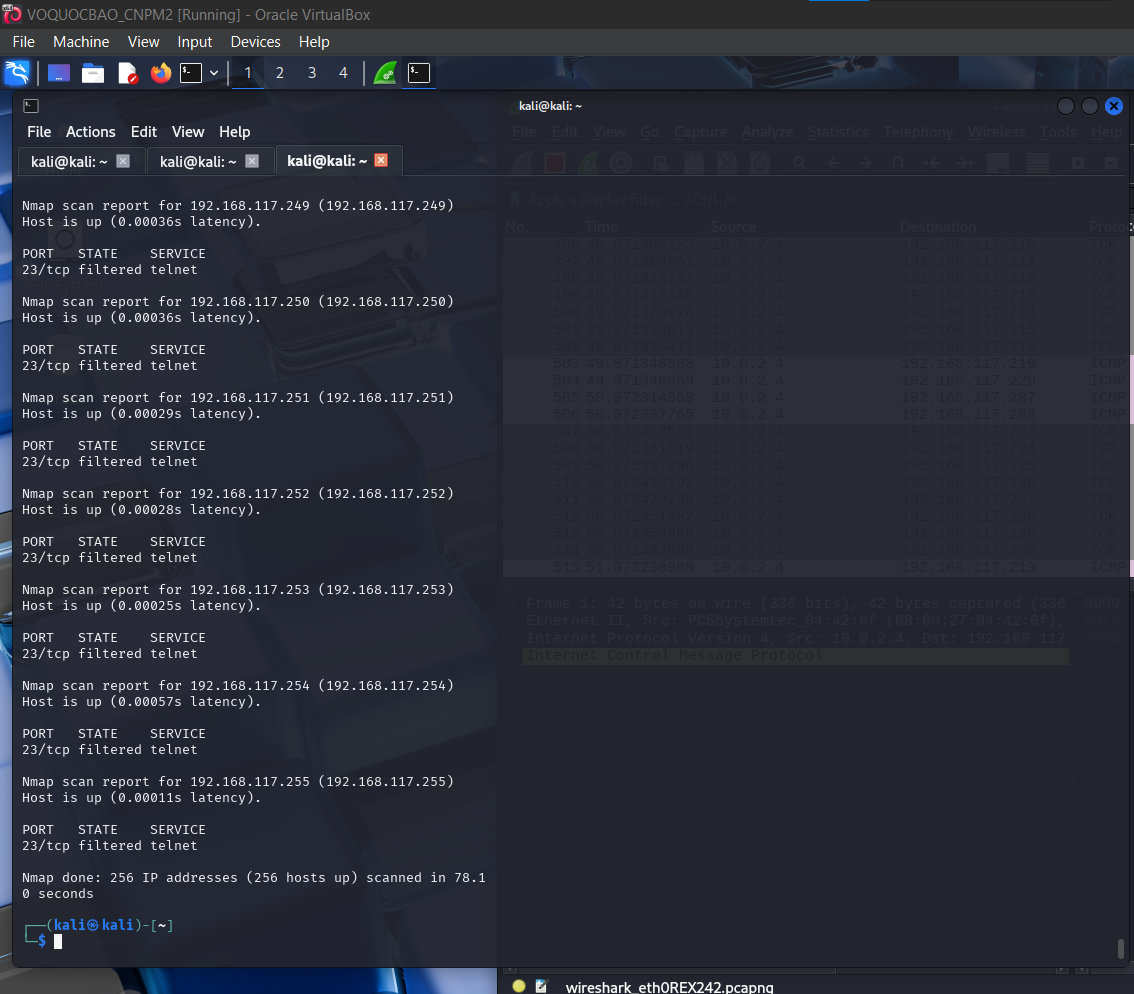
- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

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.

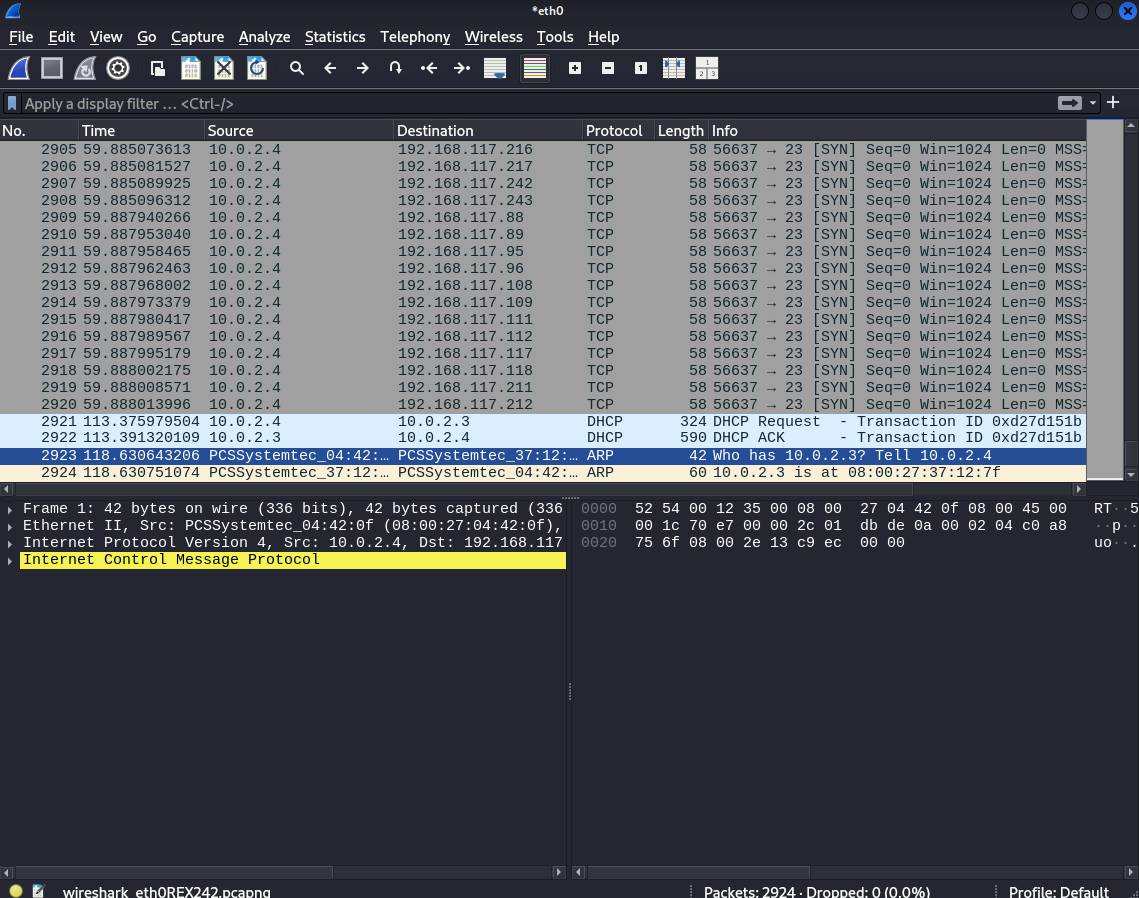


Bước 5: Dừng bắt gói tin trên Wireshark

Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể

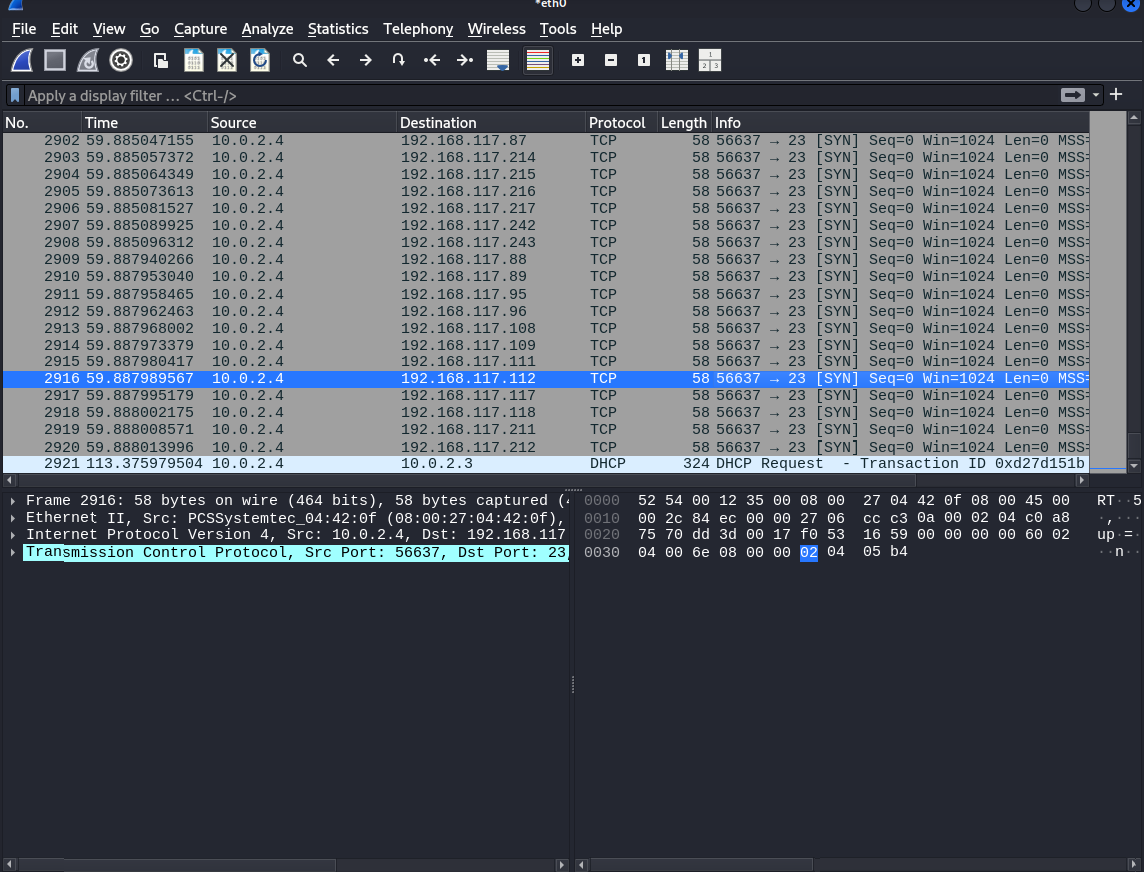
thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC

của các máy tính trong mạng 192.168.117.0/24.

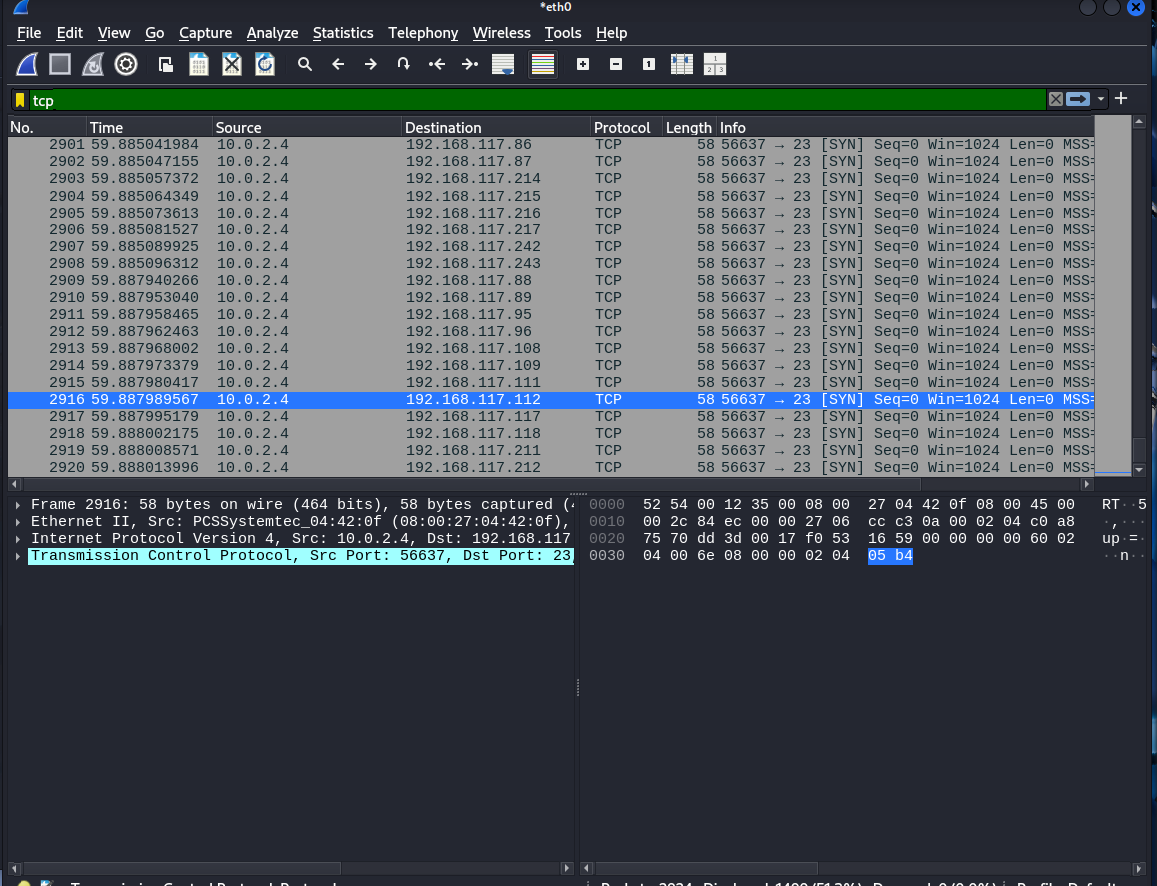


Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP

SYN được gửi tới cổng 23 của các máy đang hoạt động.



Nhập giá trị tcp vào bộ lọc.



* Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

Kịch bản 3:

Quét cổng dịch vụ

- Bước 1: Truy cập máy ảo Attack

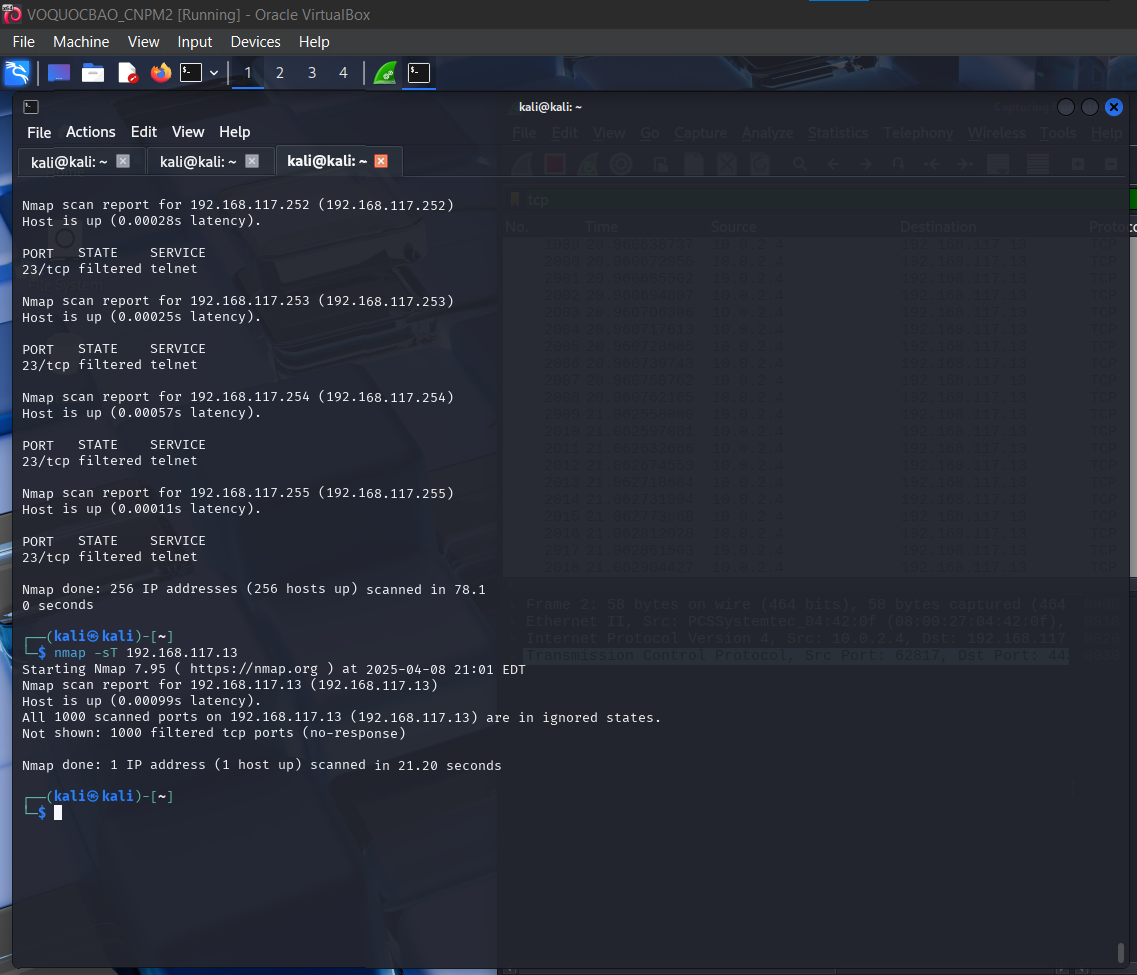
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

- 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 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.



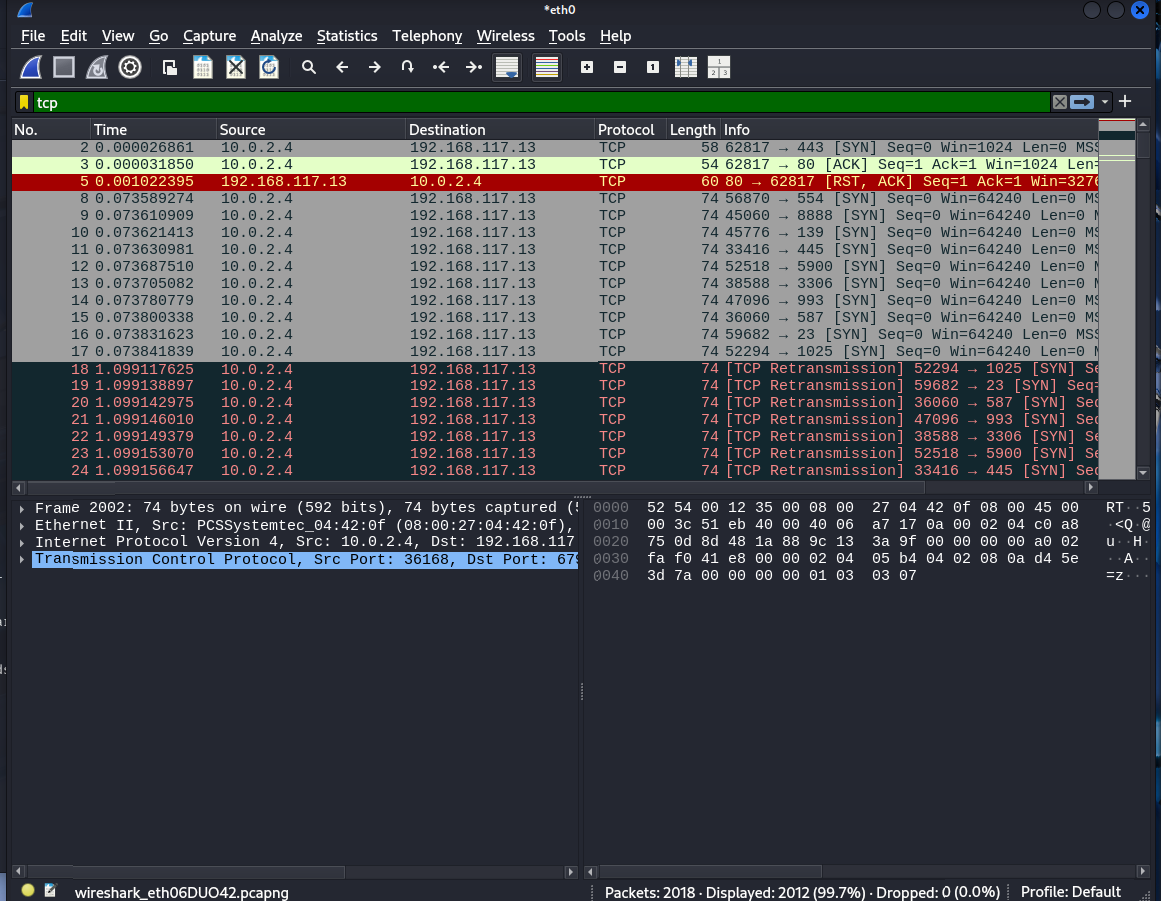
Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

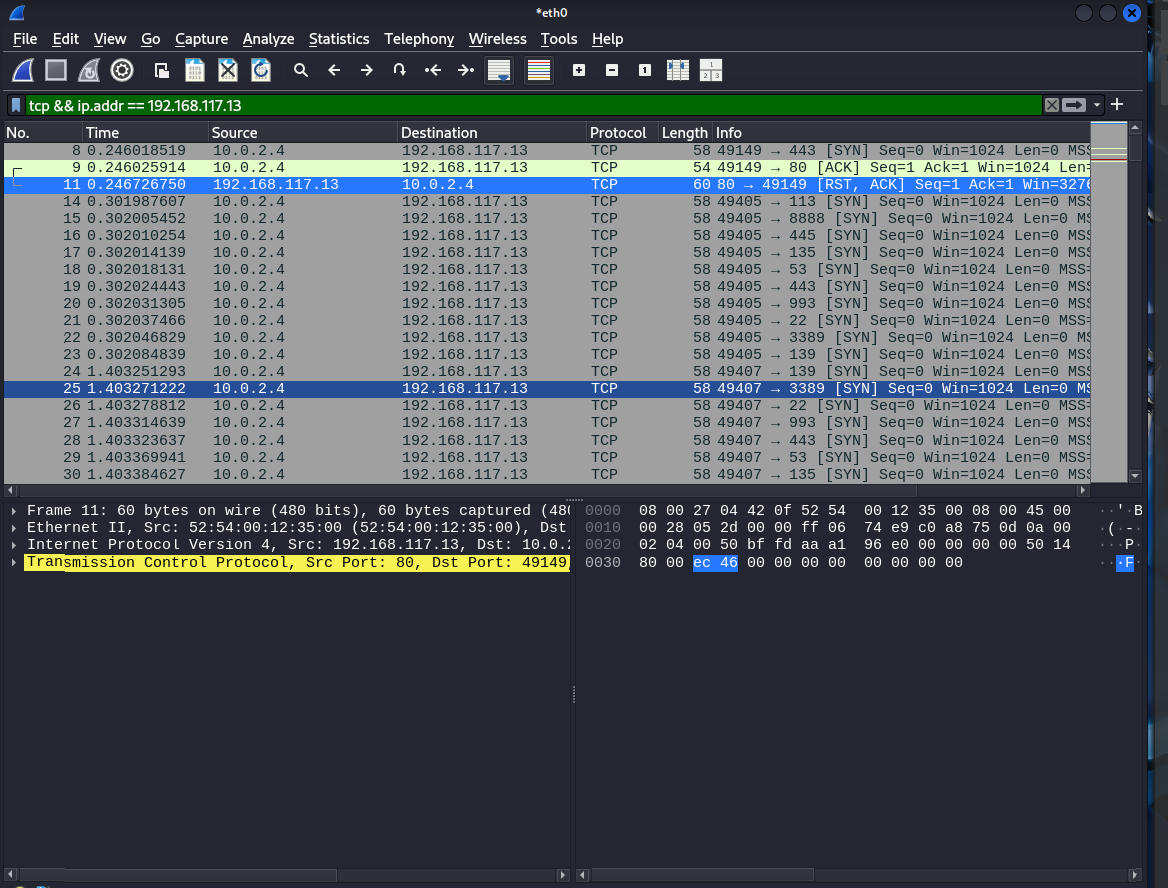
- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra

máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói 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.

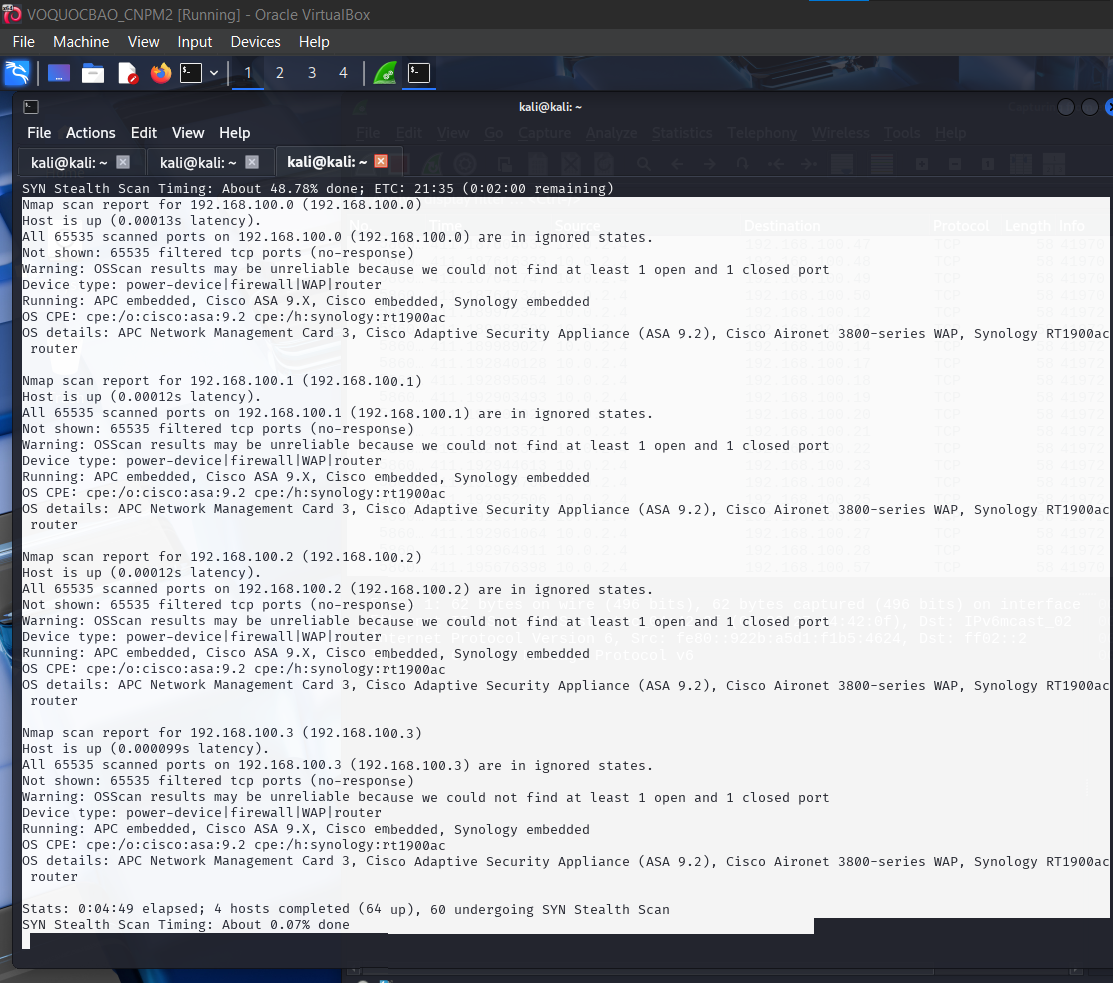


Sử dụng giá trị tcp && ip.addr == 192.168.117.13 ta lọc được các gói tin TCP



Thu thập thông tin hệ thống

Dùng lệnh: sudo nmap –sS –sV –O -p- 192.168.100.0/24



Các lỗ hỏng

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| Telnet (Generic) | CVE-2020-10188 | Lỗ hổng buffer overflow trong telnet client có thể bị khai thác để thực thi mã độc từ xa. |
| Telnet (Windows 10 client) | CVE-2019-1253 | Remote Code Execution do xử lý đầu vào sai khi dùng telnet client. |
| Telnet (Unix/Linux Telnet Daemon) | CVE-2011-4862 | Lỗ hổng DoS qua lệnh đặc biệt trong Telnet, ảnh hưởng đến dịch vụ. |