**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

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

**Họ và tên sinh viên:** Bùi Kim Ngân

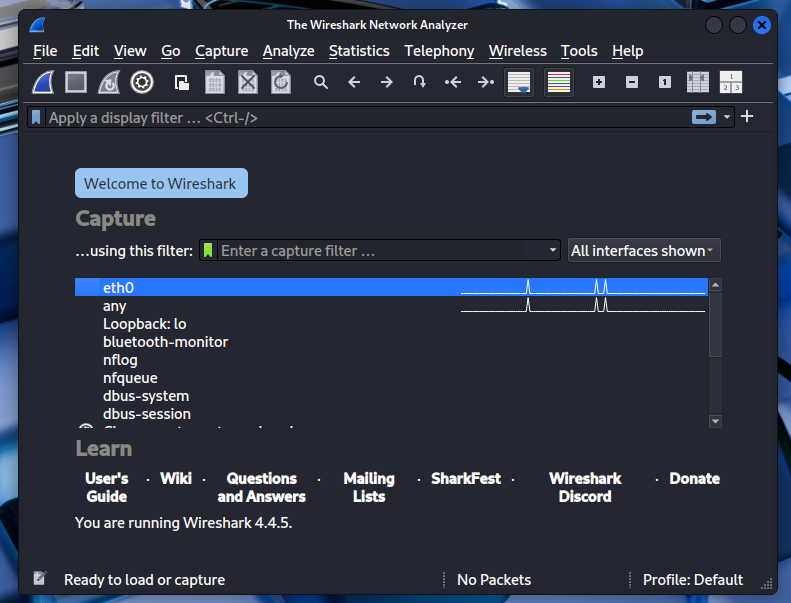
**MSSV: 1050080277**

**Lớp: 10\_ĐH\_CNPM3**

**2.1. Quét thăm dò mạng**

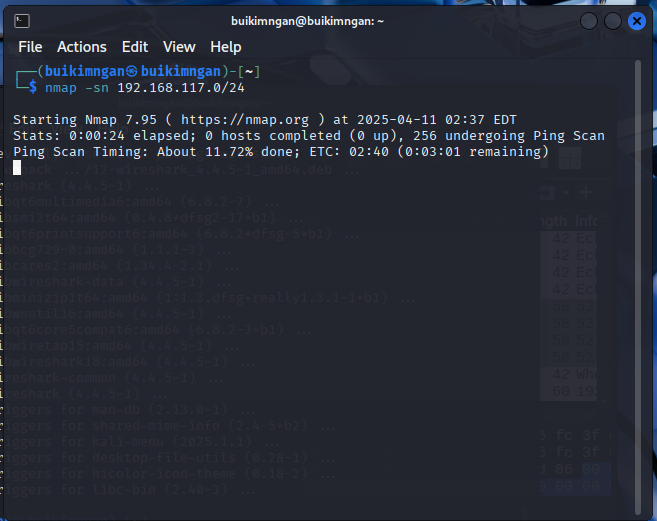
- **Bước 1:** Truy cập máy ảo Attack

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

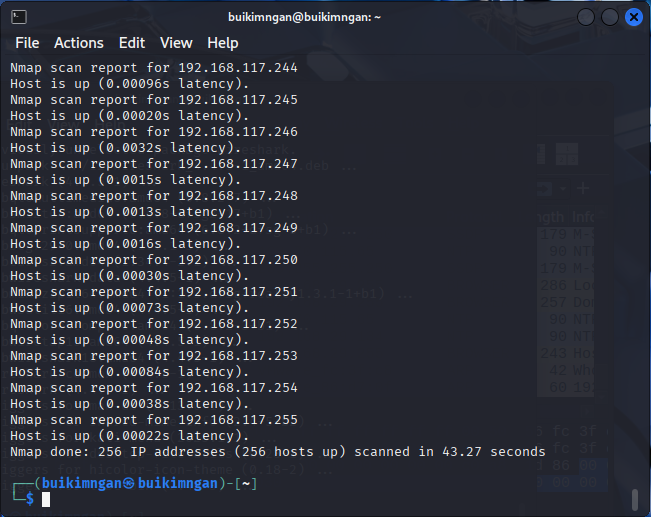


**Bước 3:** Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

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:

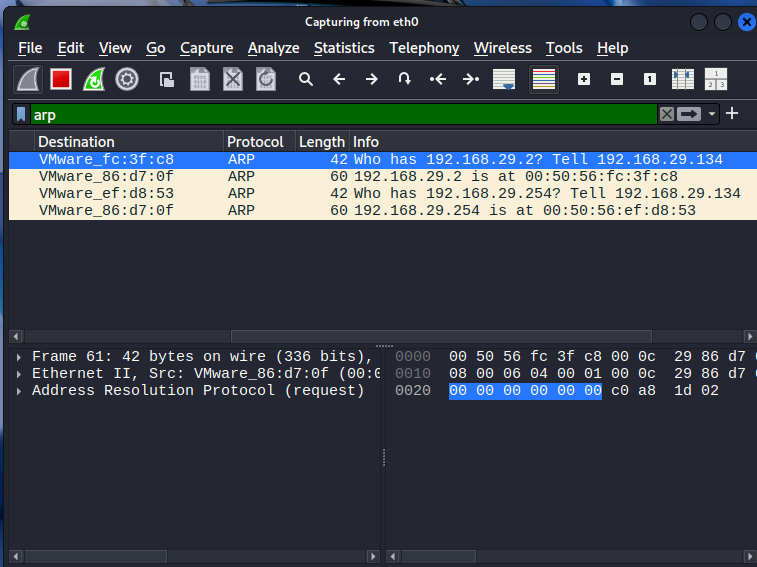


Có thể thấy ngoài địa chỉ 192.168.117.255 là địa chỉ của máy tấn công thì còn các nút mạng nữa đang hoạt động

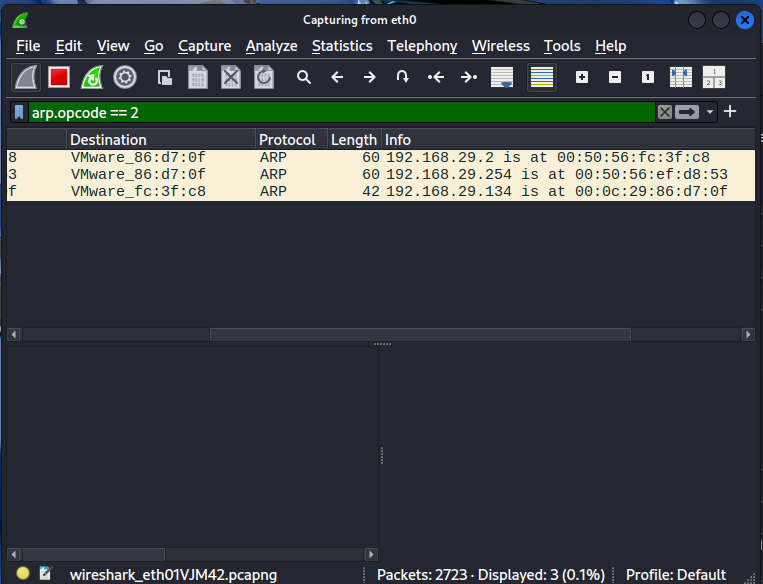
- **Bước 5:** Dừng bắt gói tin trên Wireshark

**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.



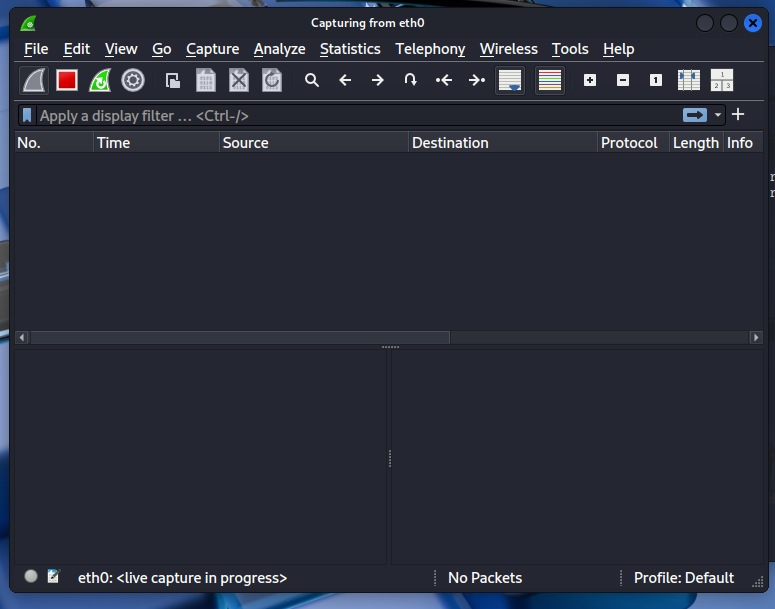
**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

**2.2. 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).

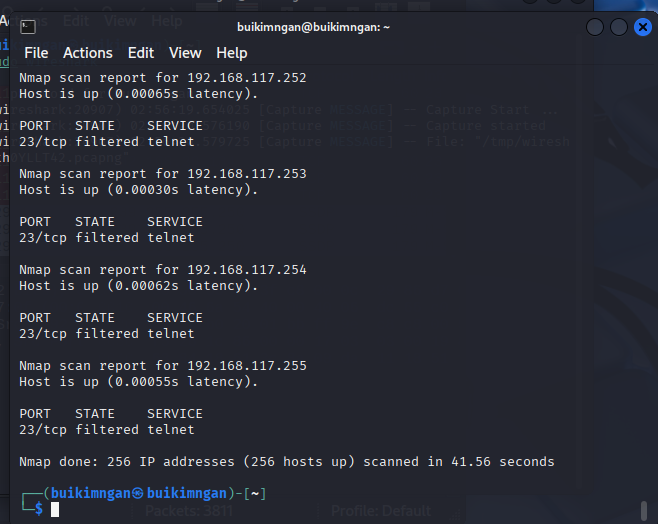
- **Bước 1:** Truy cập máy ảo Attack

- **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:

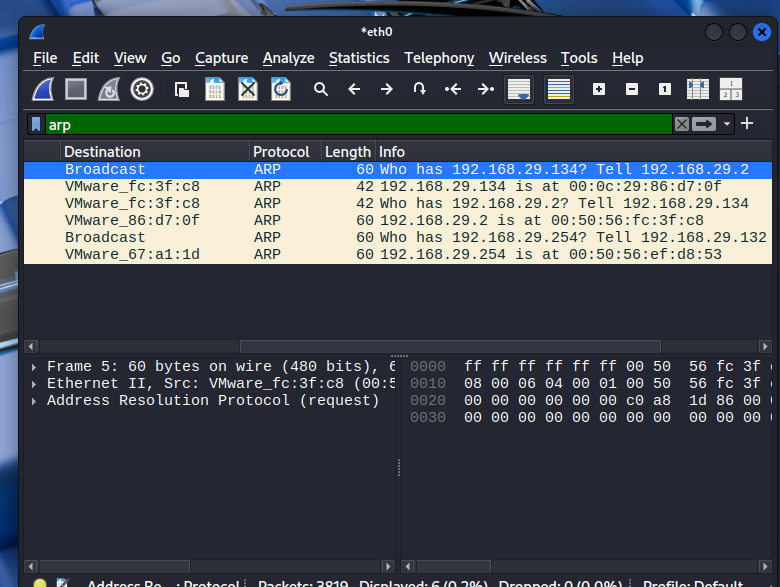
**sudo nmap -p 23 192.168.117.0/24**



Phân tích lưu lượng:

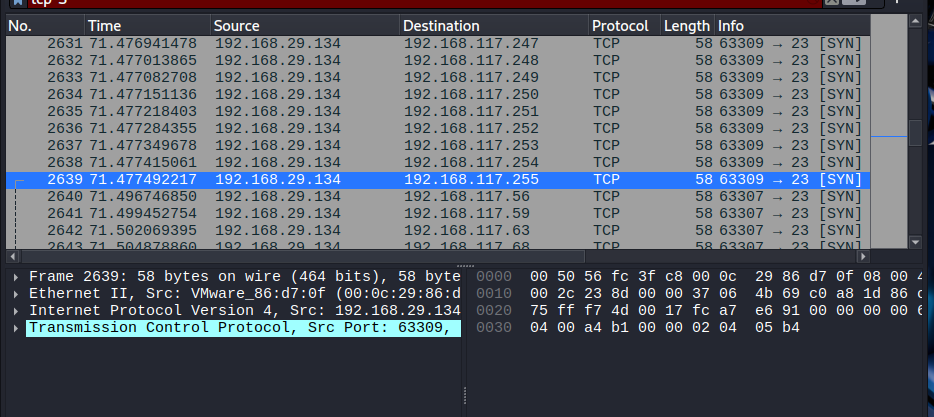
- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể

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 23 của các máy đang hoạt động.



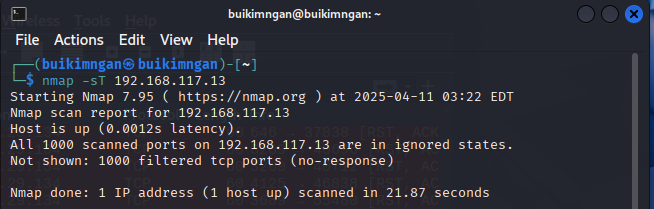
**2.3. Quét cổng dịch vụ**

- **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**

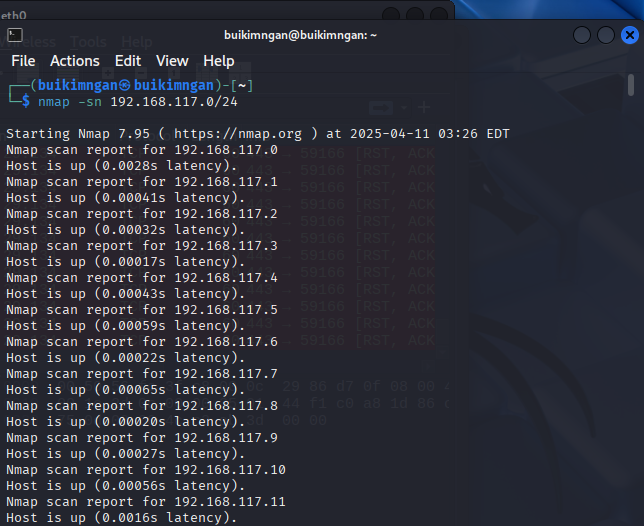


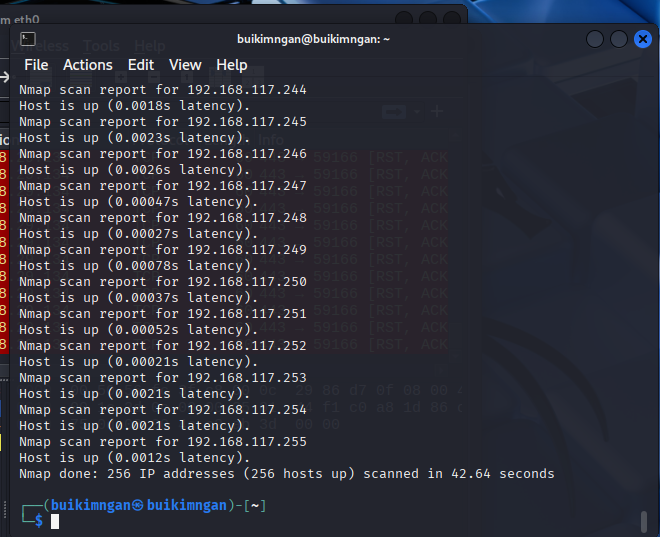
**3. Yêu cầu thực hành trên lớp**

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

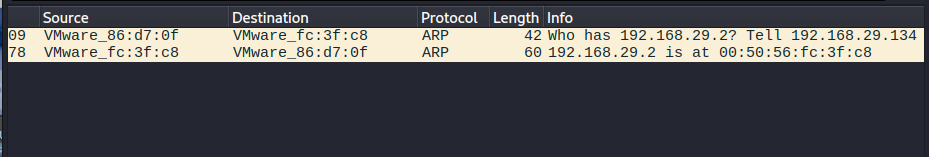
**3.1.1. Kịch bản 1**

Thực hiện lệnh quét **nmap –sn 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**.



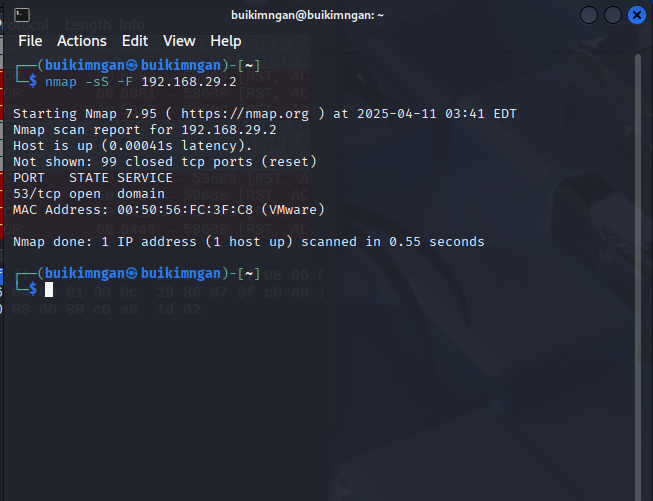


Phân tích trên máy do thám (Wireshark)



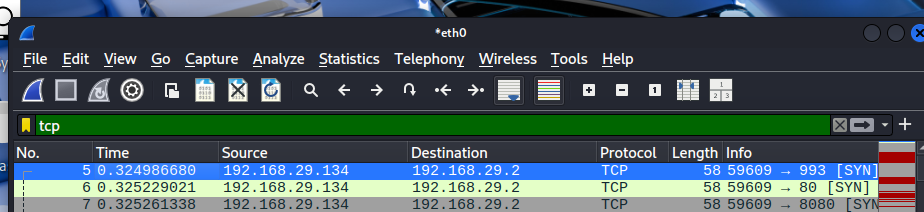
ARP Scan là kỹ thuật quét chủ yếu được dùng trong mạng LAN để phát hiện các host đang hoạt động, thông qua việc gửi các **ARP Request** đến từng IP trong mạng. Nếu host đó tồn tại, nó sẽ phản hồi bằng **ARP Reply**.

Kịch bản 2:

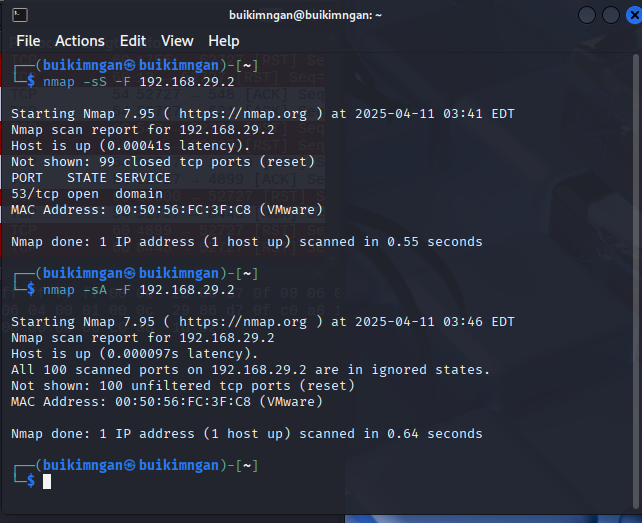


**TCP SYN Scan (Half-open scan)**

Đây là một kỹ thuật quét phổ biến và stealthy (ẩn mình), vì nó không hoàn tất quá trình bắt tay TCP, do đó tránh được nhiều hệ thống phát hiện xâm nhập (IDS).



Kịch bản 3:



**Kỹ thuật được sử dụng:**  
- TCP ACK Scan

