BÁO CÁO BÀI THỰC HÀNH SỐ 7

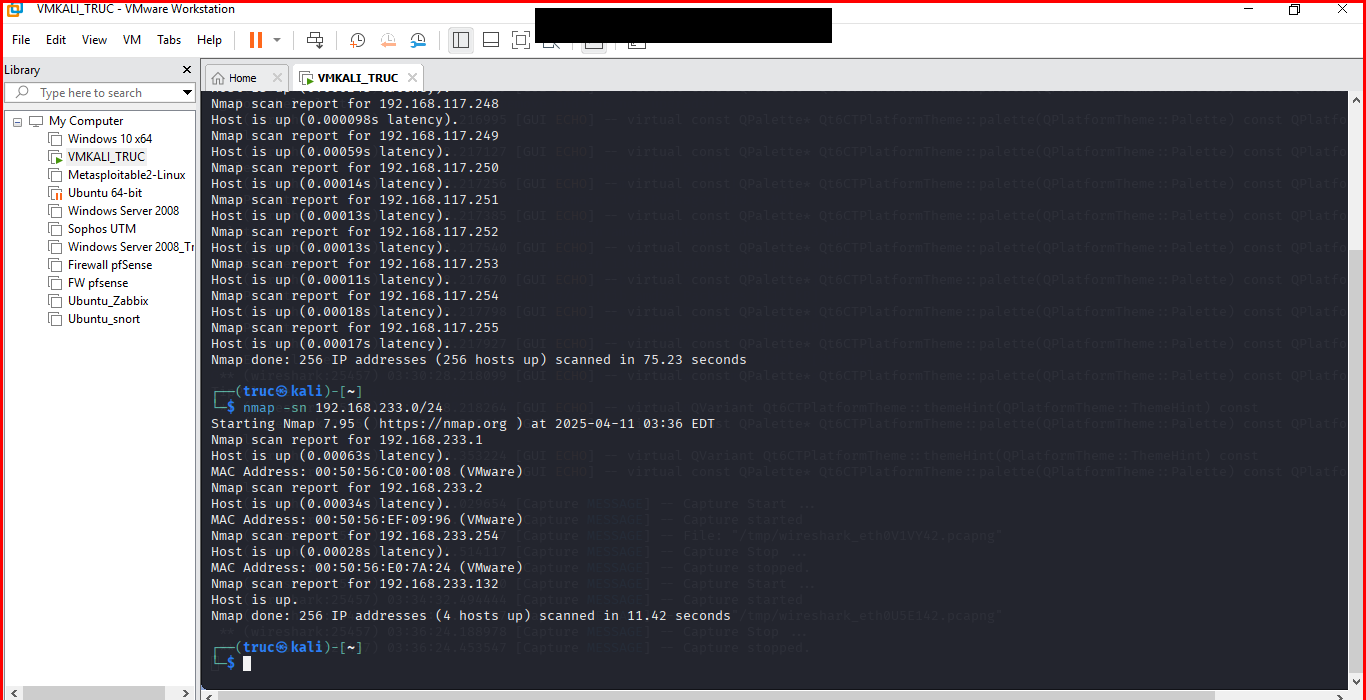
**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

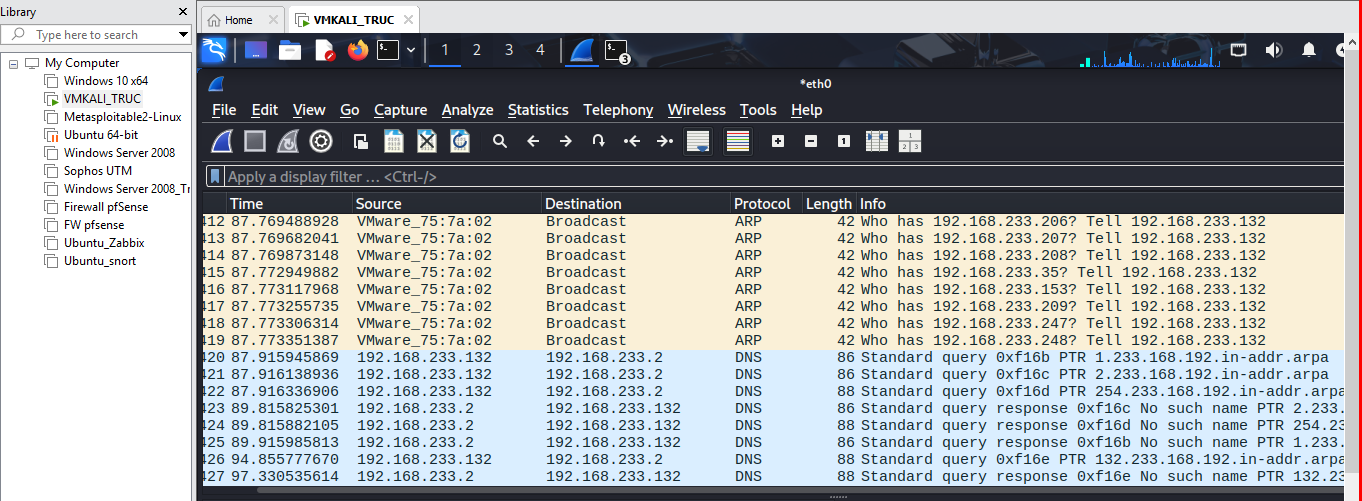
***Họ và tên sinh viên: Nguyễn Thanh Trúc***

***MSSV: 1050070048***

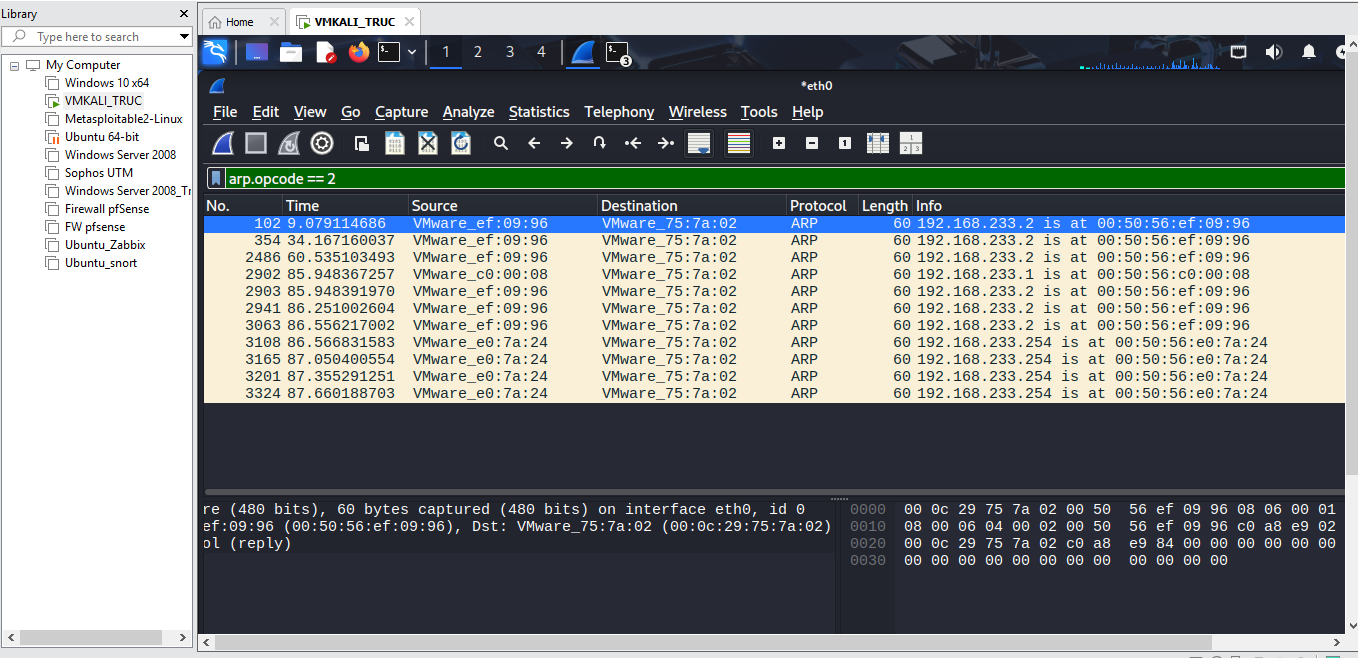
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

* Ảnh chụp kết quả thực hiện của nmap:
* 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





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.



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).

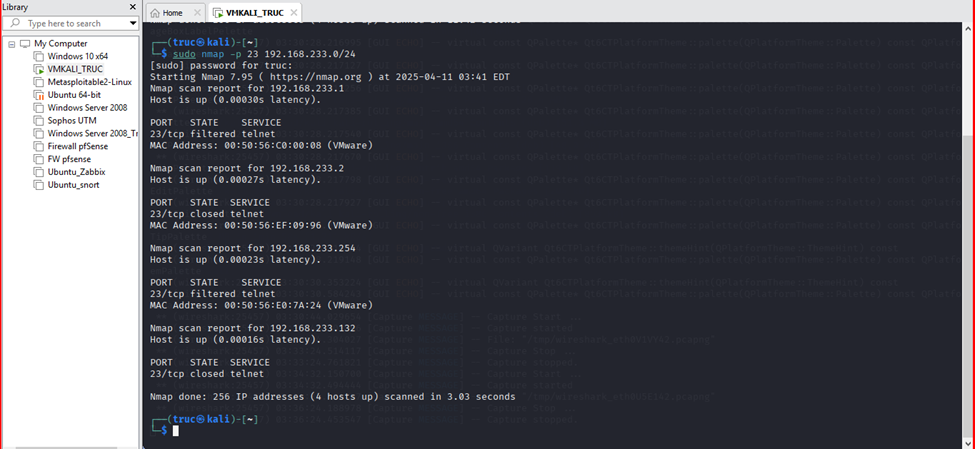
- Bước 1: Truy cập máy ảo Attack

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

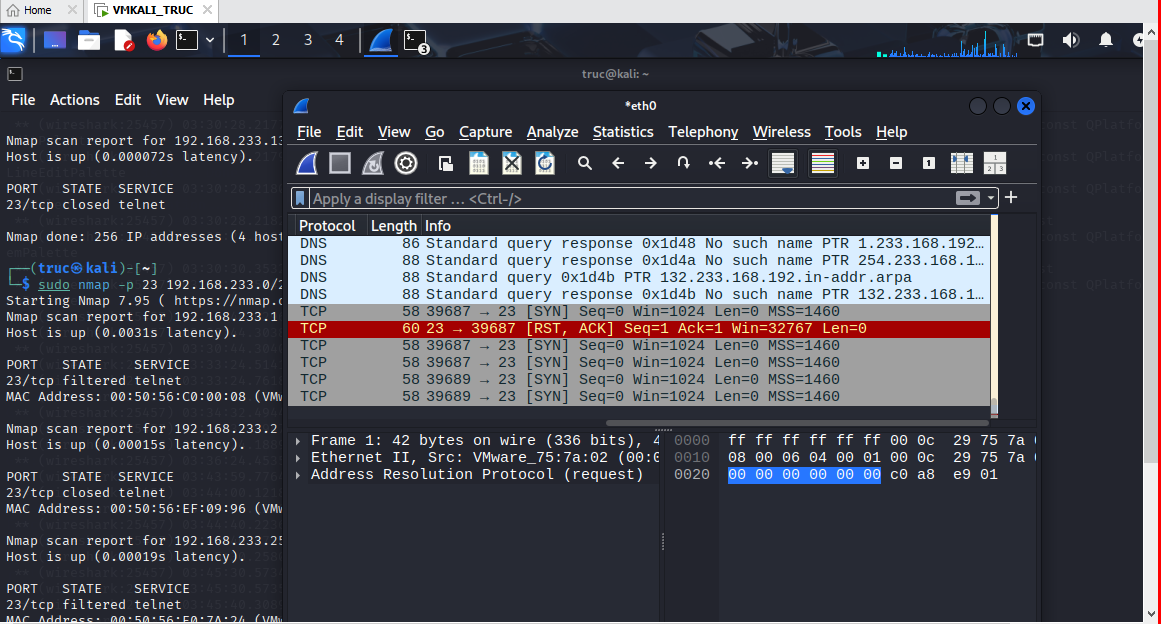
- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

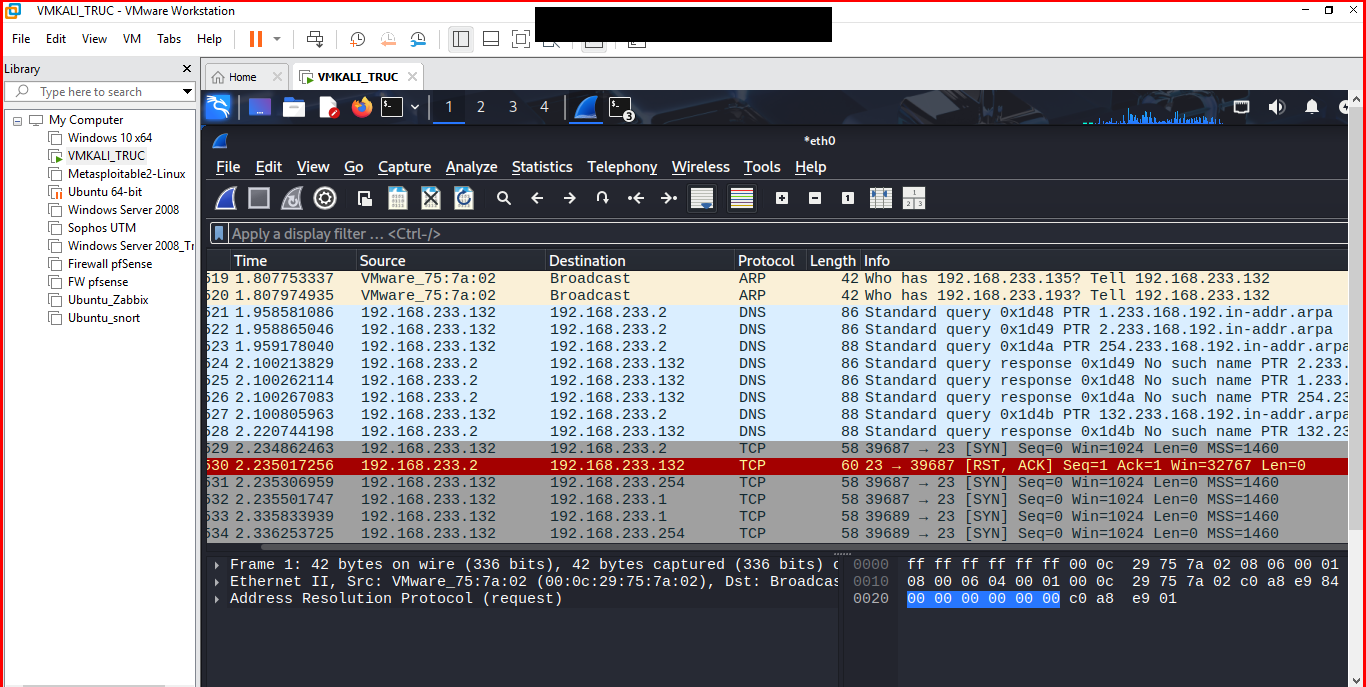
sudo nmap -p 23 192.168.233.0/24

- Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.



Bước 5: Dừng bắt gói tin trên Wireshark





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 192.168.233.132

- 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 192.168.233.132 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.