# THỰC HÀNH MẠNG MÁY TÍNH

**LAB 7: PHÂN TÍCH CÁC KỸ THUẬT DO THÁM HỆ THỐNG**

Họ và tên: Trần Nguyễn Gia Long

Lớp: 10ĐH\_CNPM1

MSSV: 1050080059

Link Github: <https://github.com/Lzerotwonine/BMMMT-HT/tree/main/Lab%207>

Link video Youtube: <https://youtu.be/TjkK6e9nWhA>

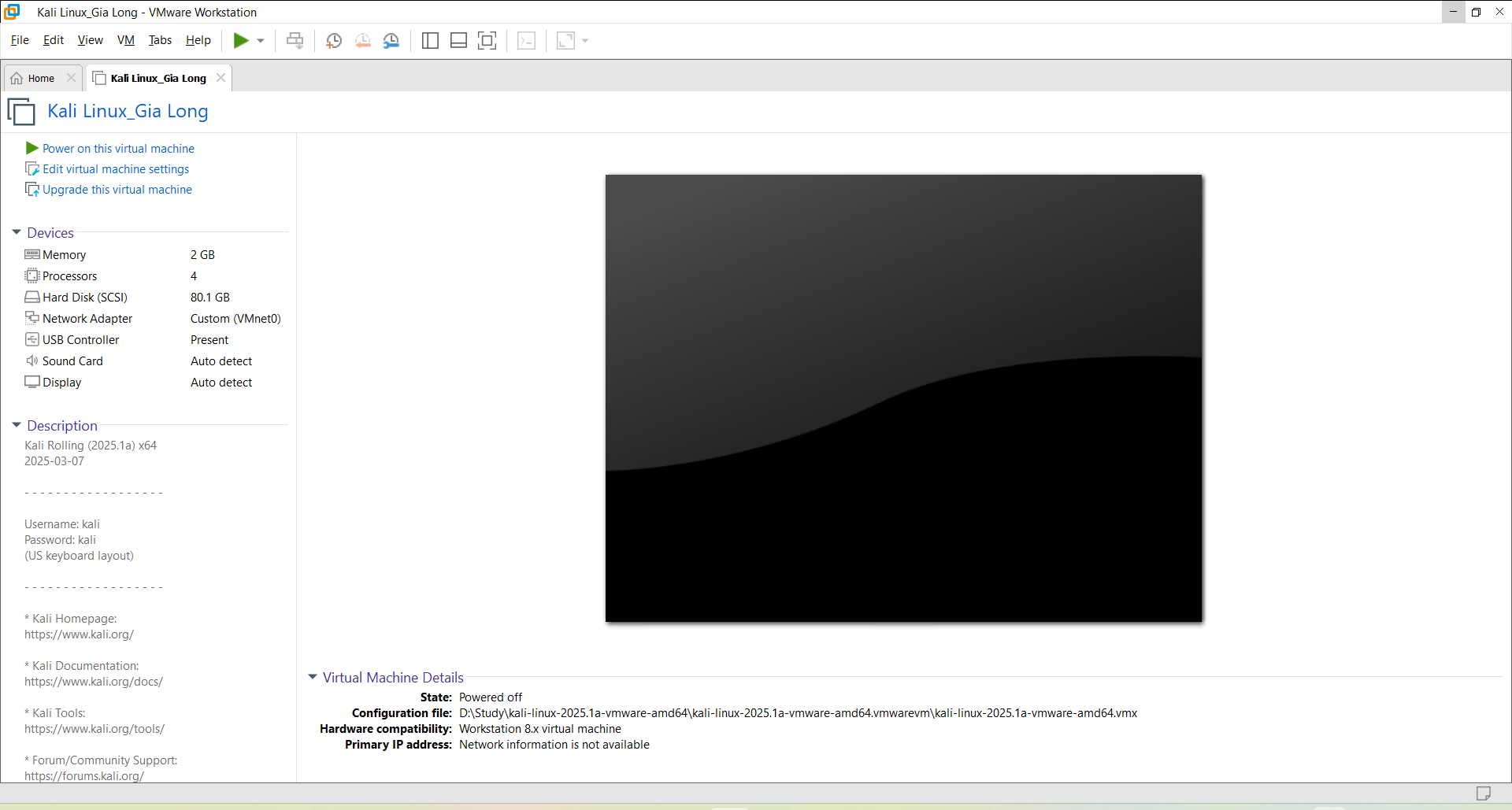
B. THỰC HÀNH

2. Luyện tập tại nhà

2.1. Quét thăm dò mạng

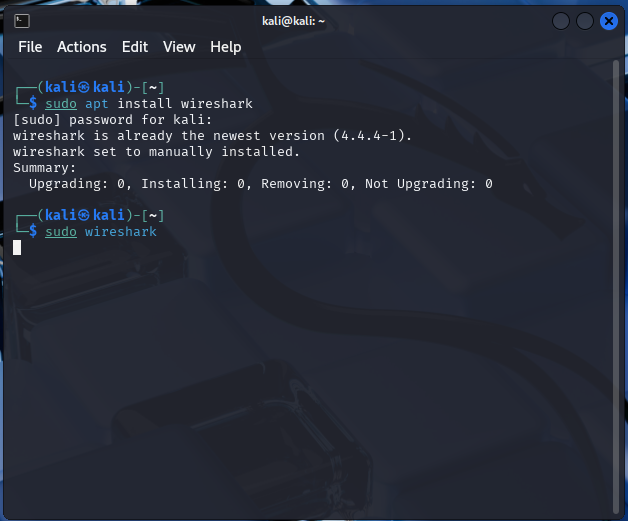
Bước 1: Truy cập máy ảo Attack:

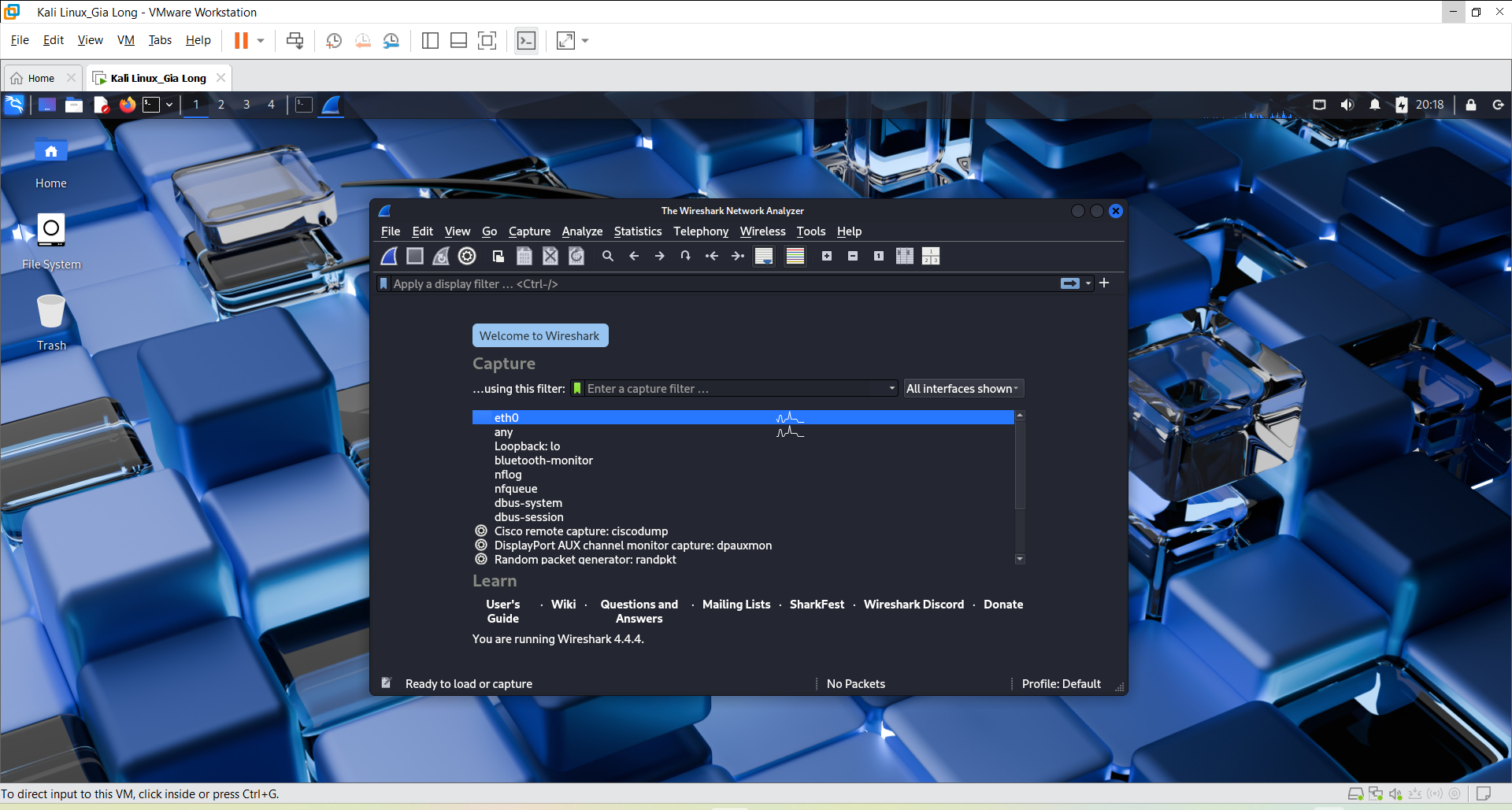
Chuẩn bị môi trường thực hành là Kali Linux.



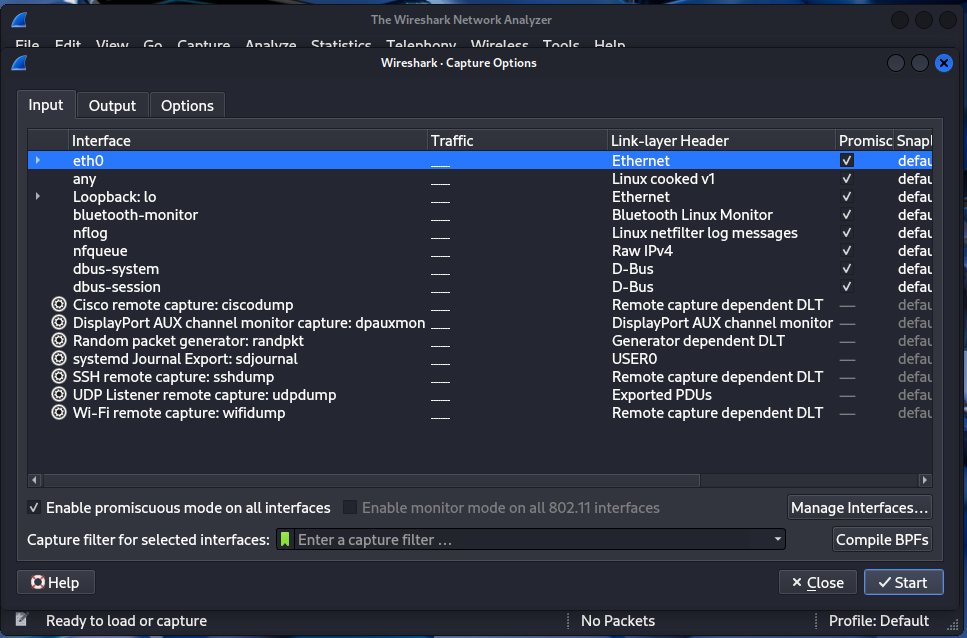
Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin

Cài đặt WireShark trên Kali Linux bằng lệnh sudo apt install wireshark. Do đã cài đặt trước nên ta bắt đầu mở wireshark.

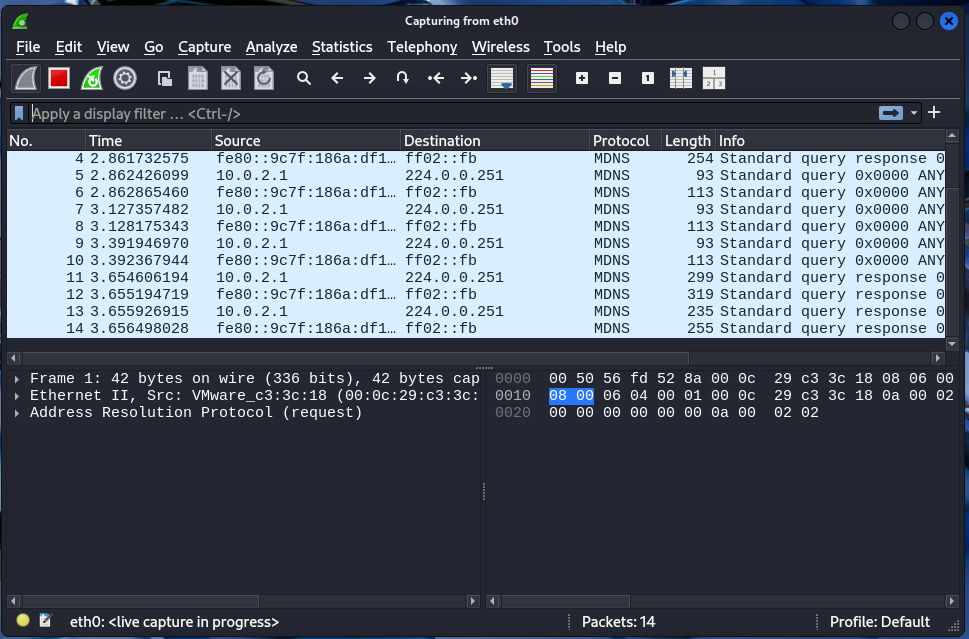




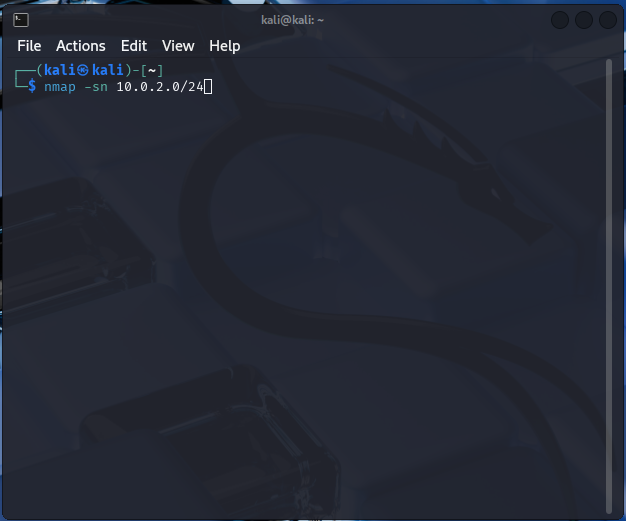
Chọn card mạng là eth0.



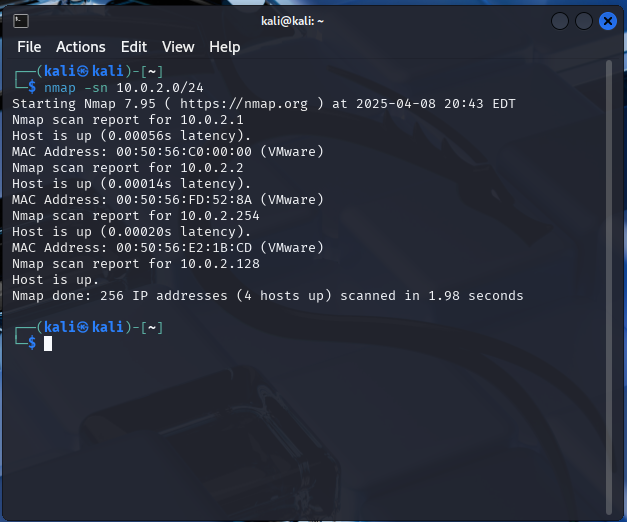
Sau đó chạy wireshark.



Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: nmap -sn 10.0.2.0/24



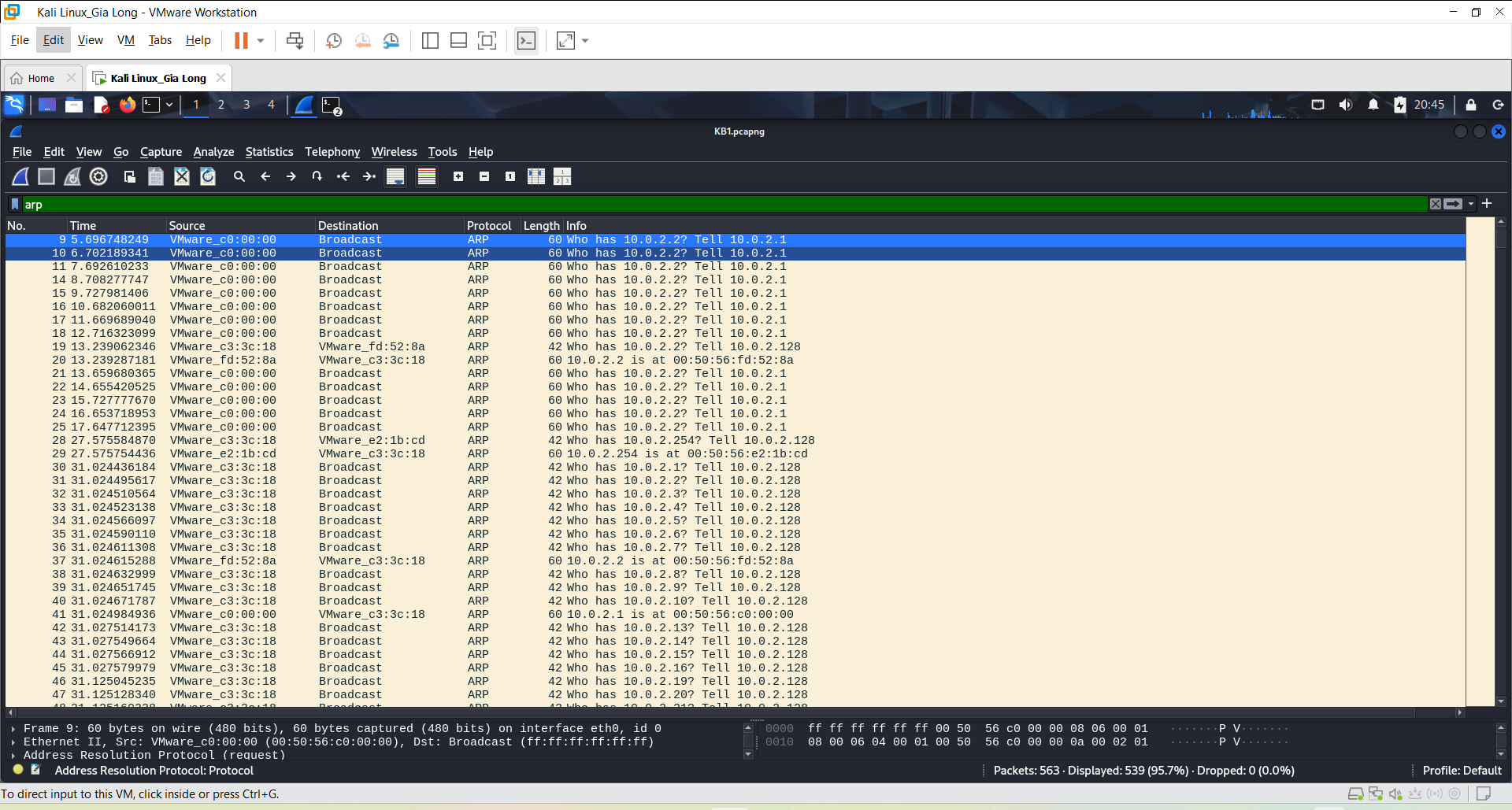
Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự như sau:



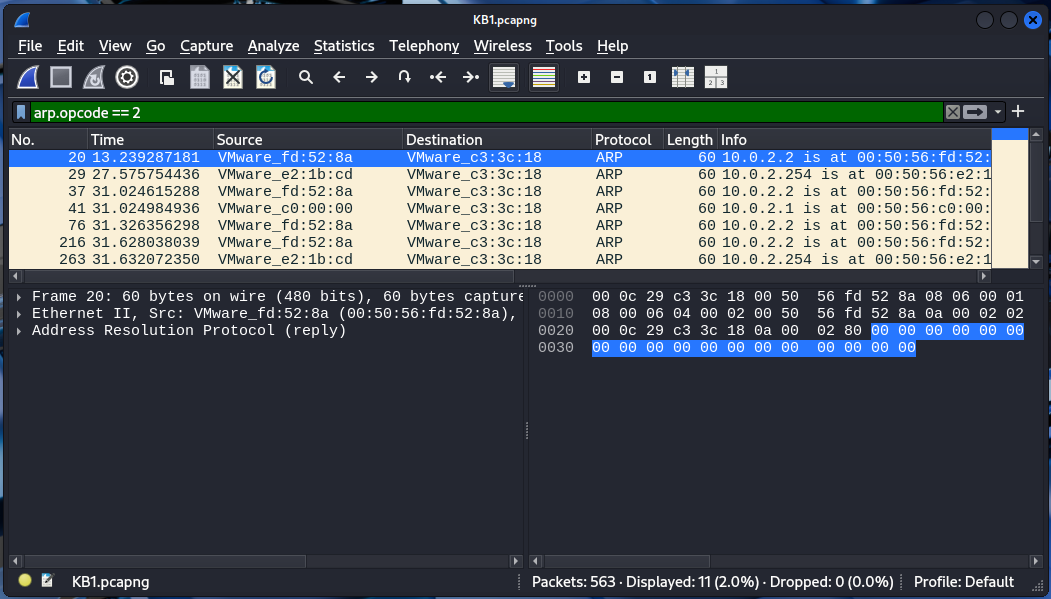
Có thể thấy ngoài địa chỉ 10.0.2.0 là địa chỉ của máy tấn công thì còn 259 nút mạng nữa đang hoạt động có địa chỉ là 10.0.2.1, 10.0.2.1 còn có 10.0.2.254 và 10.0.2.128

Bước 5: Dừng bắt gói tin trên Wireshark

Tìm kiếm Protocol theo ARP, 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 10.0.2.0/24.



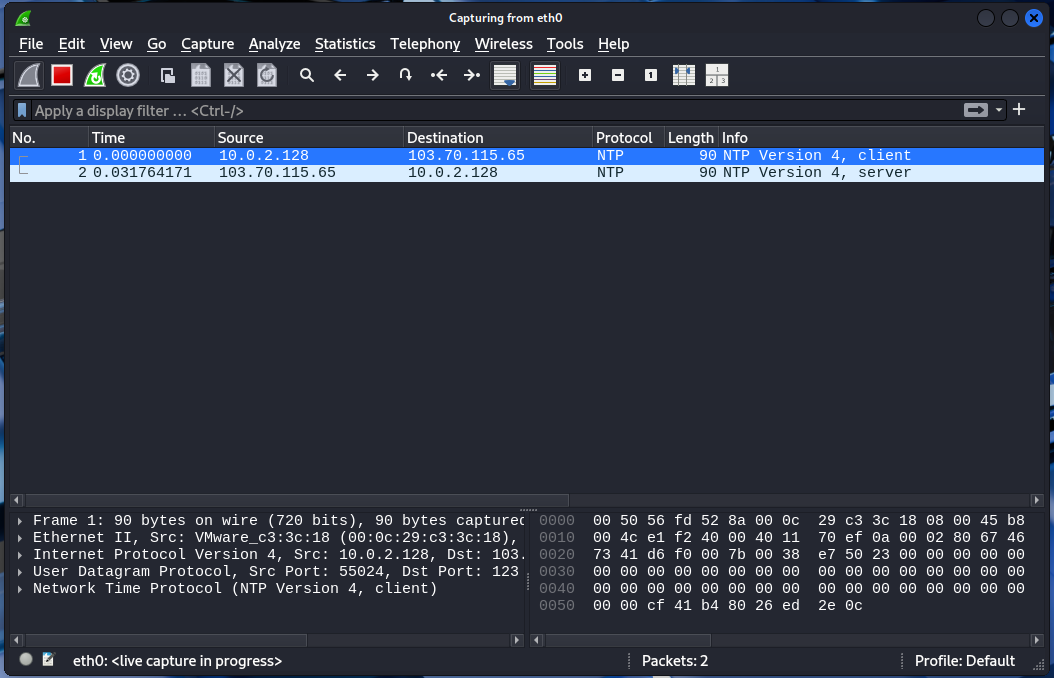
Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



2.2. Quét thăm dò dịch vụ

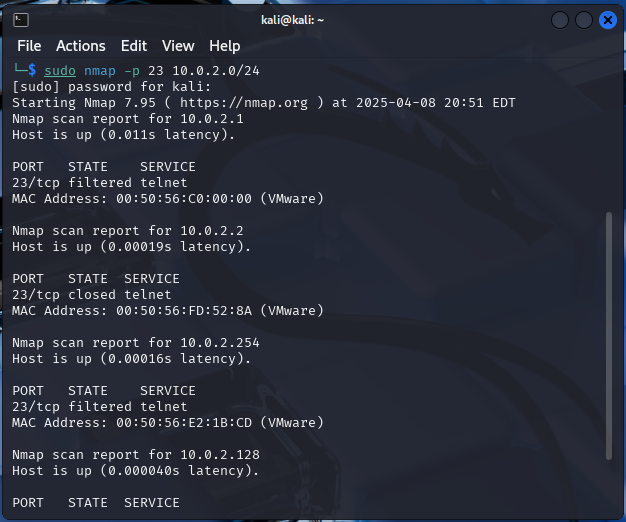
Bước 1: Truy cập máy ảo Attack

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 10.0.2.0/24

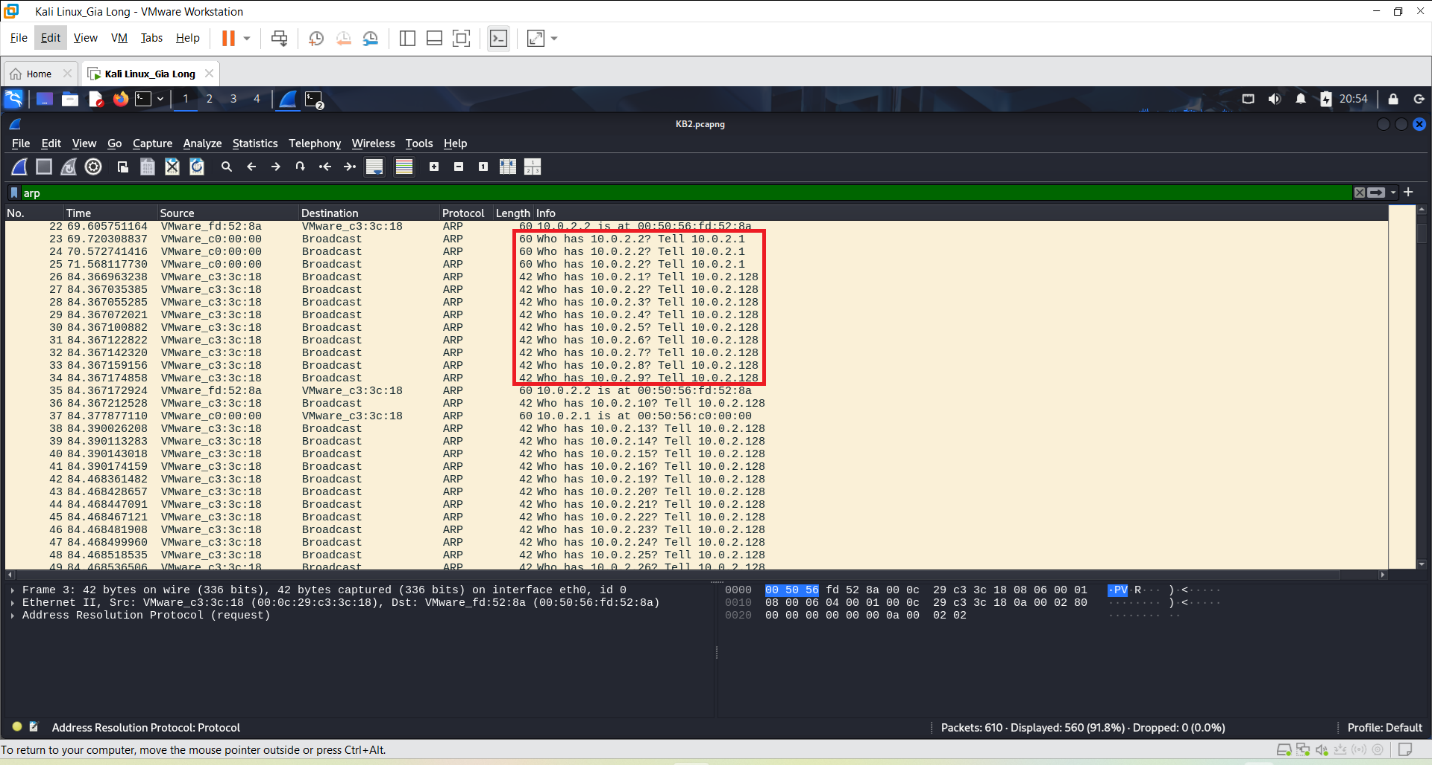
Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 10.0.2.254 có trạng thái cổng dịch vụ 23 là open.



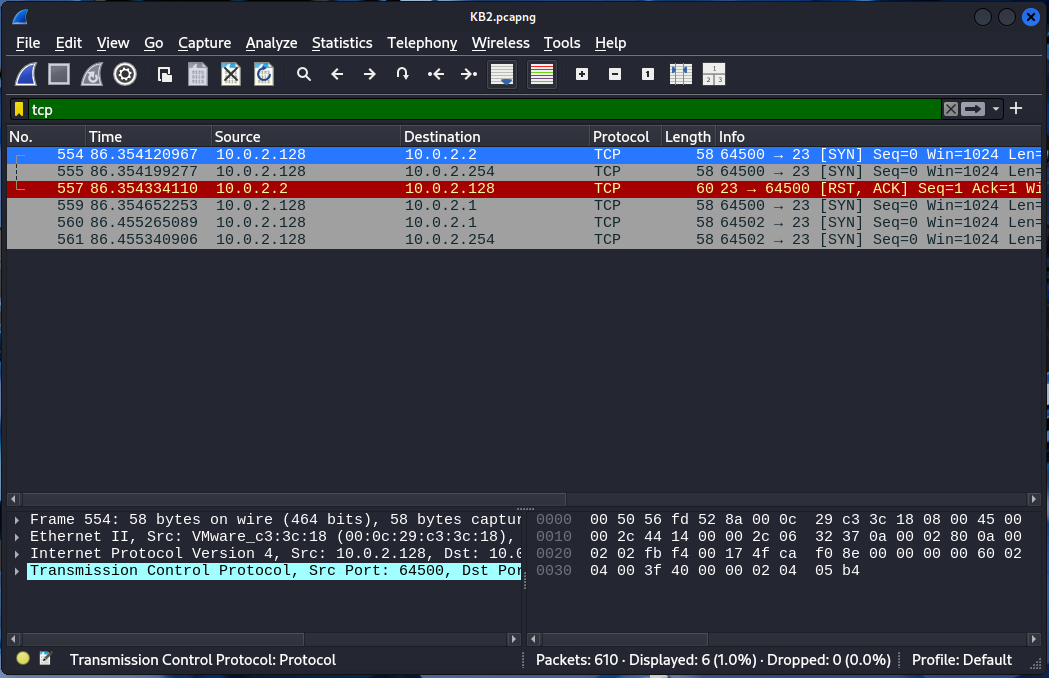
Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

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 10.0.2.0/24.



Các gói tin TCP SYN được gửi tới cổng 23 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 23 từ địa chỉ 10.0.2.2 về máy tấn công.

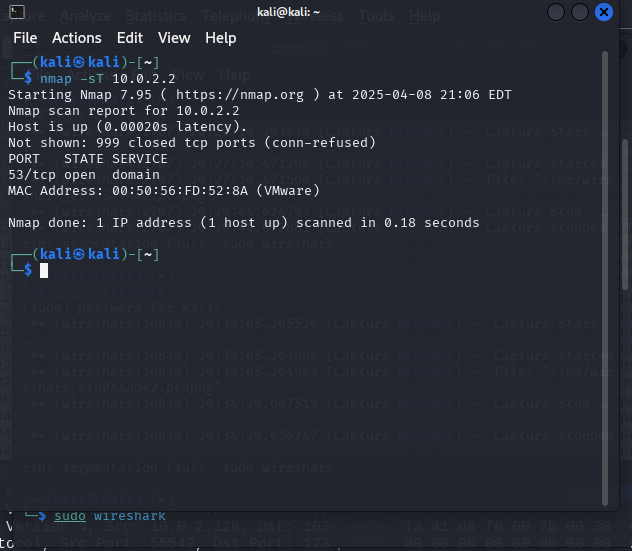
2.3. Quét cổng dịch vụ

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 10.0.2.2

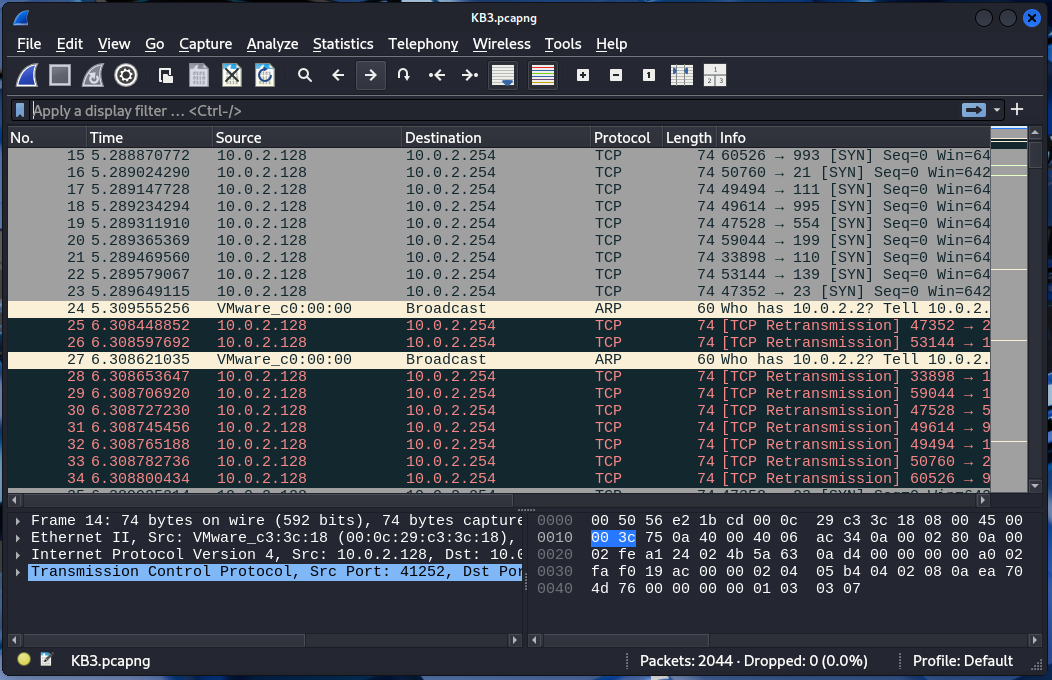
Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 53 trên máy mục tiêu 10.0.2.2 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp dịch vụ tương ứng là dns.



Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

ta thấy một lượng lớn các gói tin TCP SYN đư ợc gửi từ máy tấn công (10.0.2.128) tới máy mục tiêu là 10.0.2.254 Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



Sử dụng giá trị tcp && ip.addr == 10.0.2.128 ta lọc được các gói tin TCP.

