**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

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

**Họ và tên sinh viên: Trương Đan Huy**

**MSSV: 1050080100**

**Yêu cầu kết quả thực hành:**

**Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07**

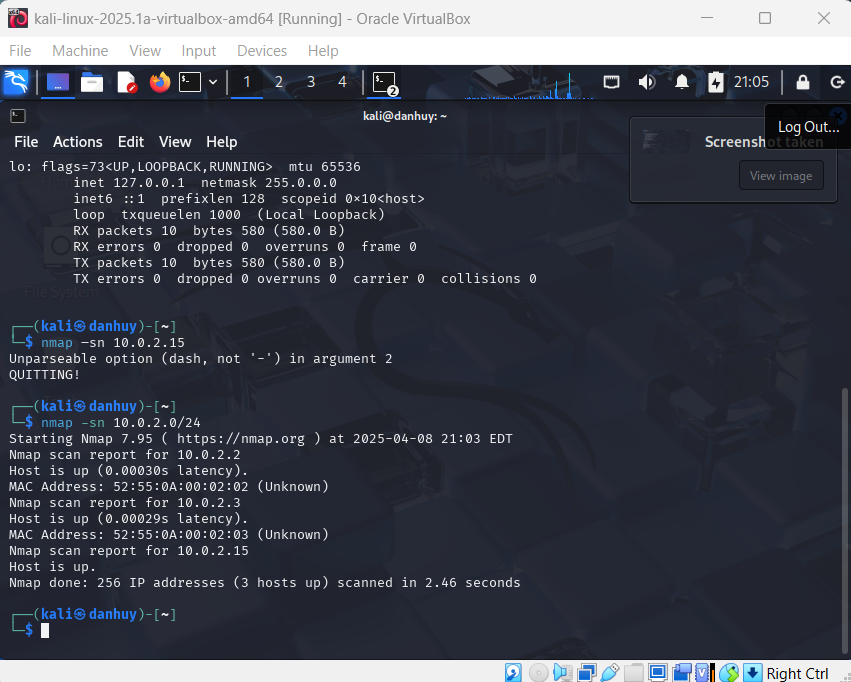
**- Báo cáo kết quả thực hành**

**- File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.**

**KẾT QUẢ THỰC HÀNH**

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

**1.1 Kịch bản 1**



Lệnh đã dùng:

nmap -sn 10.0.2.0/24

**Kết quả:**

* Phát hiện 3 host đang hoạt động trên mạng con 10.0.2.0/24, gồm các địa chỉ:
  + 10.0.2.2
  + 10.0.2.3
  + 10.0.2.15

**1 Phân tích đặc điểm lưu lượng:**

Lệnh nmap -sn thực hiện ping scan, đây là một dạng quét thăm dò để xác định máy nào đang bật mà không quét cổng.

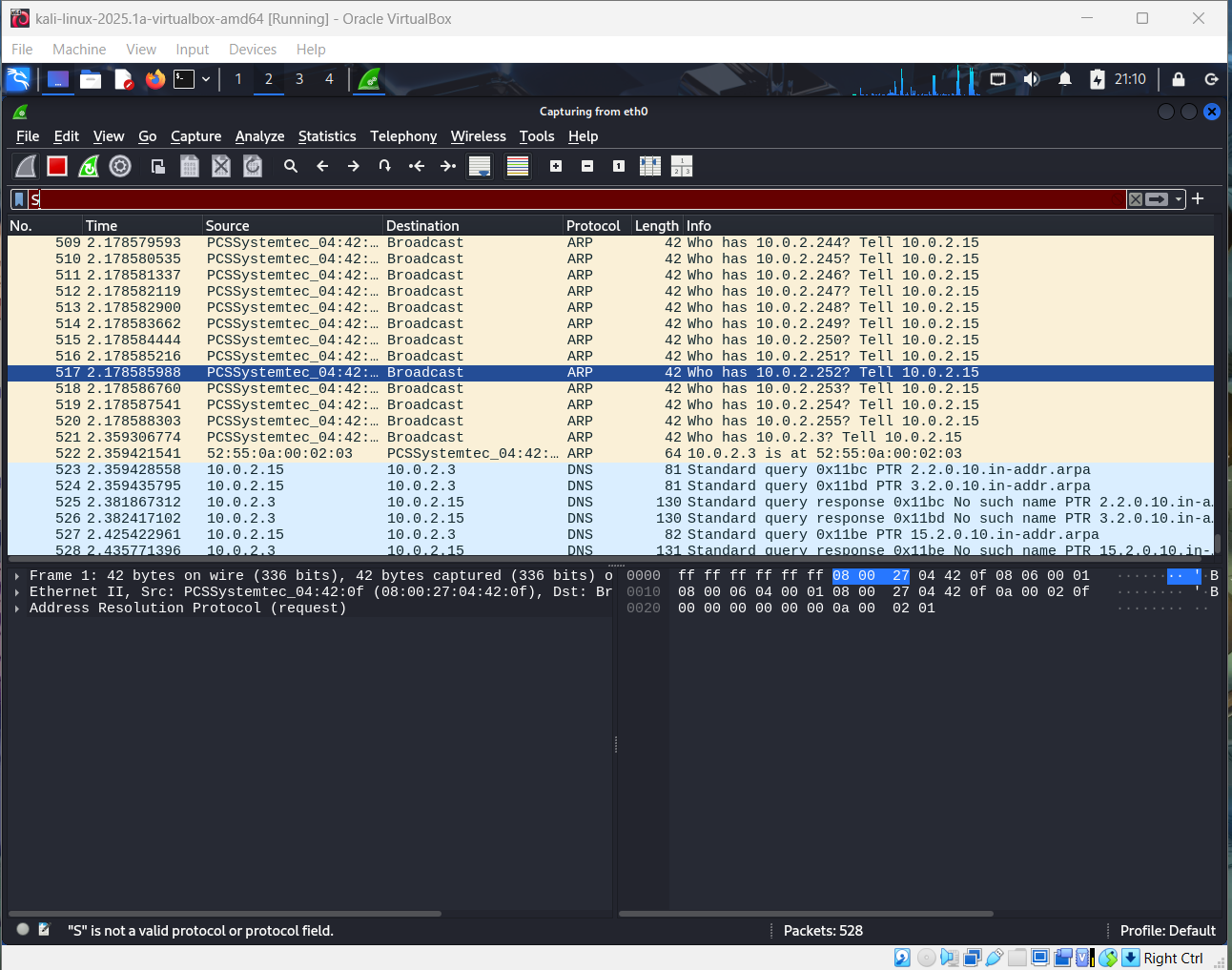
**2 Quét toàn bộ dải mạng con (/24)**

Lệnh nmap -sn 10.0.2.0/24 cho thấy việc quét toàn bộ 256 địa chỉ IP trong mạng 10.0.2.0/24, tương ứng subnet mask 255.255.255.0.

**3. Sử dụng địa chỉ MAC để xác định host**

Nmap trả về thông tin địa chỉ MAC nếu tìm được thiết bị → cho thấy nó dùng ARP (trong mạng LAN) để kiểm tra host còn sống.

**1.2 kịch bản 2**



**Đặc điểm 1: Sử dụng giao thức ARP để tìm host**

Khi nmap quét trong mạng LAN, nó sử dụng **ARP Request** để tìm ra thiết bị nào đang hoạt động.

Điều này cho thấy Kali Linux đang gửi **gói ARP broadcast** để hỏi "ai sở hữu địa chỉ IP 10.0.2.x?"

**Đặc điểm 2: Dải IP bị quét tuần tự theo subnet**

Nmap quét theo dải từ 10.0.2.1 đến 10.0.2.255

Các dòng trong ảnh thể hiện:

Đây là hành vi đặc trưng của kỹ thuật **ping sweep qua ARP** → cho thấy nmap đang dò toàn bộ lớp mạng /24.

**Đặc điểm 3: Không có gói TCP/UDP – chỉ là ARP**

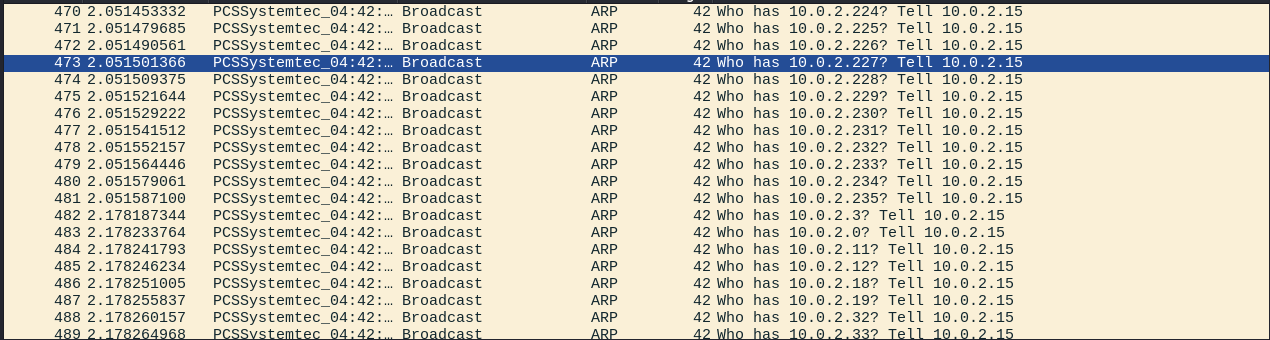
Kỹ thuật này không dùng đến port scan, chỉ xác định host đang "bật".

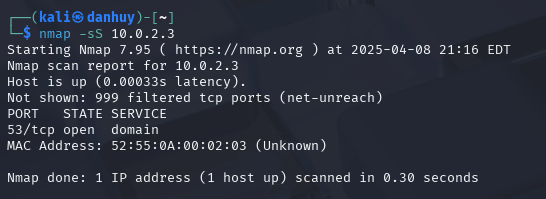
**Minh chứng trong ảnh**:

* Tất cả các gói bắt được là **ARP** hoặc **DNS**
* Không có gói TCP/UDP SYN hoặc ICMP

Đây là kỹ thuật **host discovery** không xâm nhập sâu → minh chứng rõ là nmap -sn quét thăm dò đơn giản.

**1.3 kich bản 3**





**Đặc điểm 1: Giao thức TCP với cờ SYN được gửi đi**

Kỹ thuật -sS gửi **gói TCP với cờ SYN** đến các cổng → nếu nhận SYN-ACK, host đang mở cổng.

Đặc trưng của kỹ thuật **TCP SYN Scan** (quét nửa mở).

**Đặc điểm 2: Không hoàn tất bắt tay TCP (không có ACK)**

Nmap -sS chỉ gửi SYN, nếu nhận SYN-ACK, nó không gửi ACK → không thiết lập kết nối hoàn toàn.

Cho thấy kiểu quét **nửa mở**, đặc trưng của -sS.

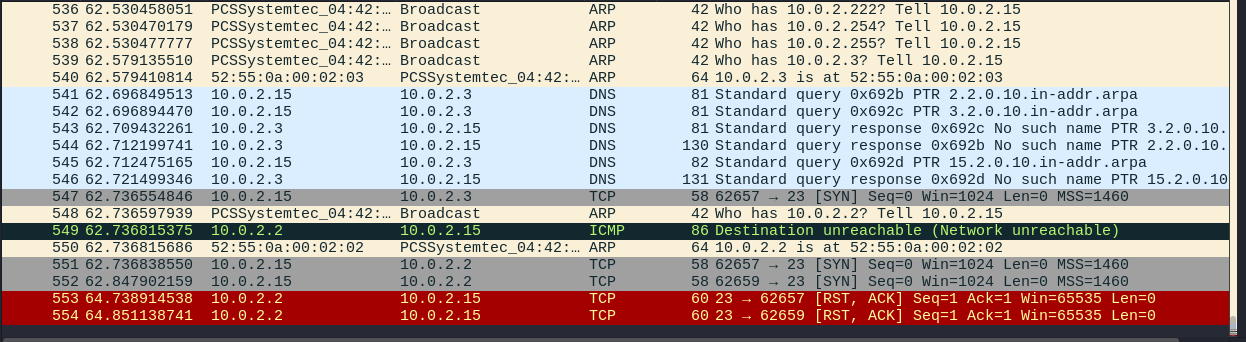
**Đặc điểm 3: Có thể thấy trạng thái các cổng (open/closed)**

Ảnh nmap đầu ra sẽ hiển thị:

* Cổng mở (open)
* Cổng đóng (closed)
* Cổng được lọc (filtered)

Đây là đặc điểm của **port scanning** chứ không chỉ là host discovery như -sn.

**Bài 2:** **Thu thập thông tin hệ thống**



**Các lệnh thực hiện:**

nmap -p 25,110,143,465,587,993,995 -sV

nmap -p 25,110,143,465,587,993,995 -sV 10.0.2.15

sudo nmap -O

sudo nmap -O 10.0.2.15

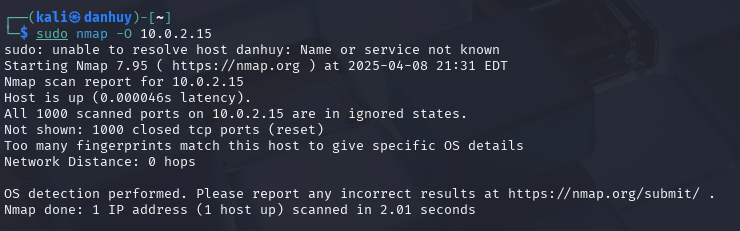
nmap -sV

nmap -sV 10.0.2.15

**2. Quét hệ điều hành**

sudo nmap -O 10.0.2.15

em chạy lệnh này rồi mà máy không phản hồi



**3. Quét phát hiện dịch vụ**

nmap -sV 10.0.2.15

**Giải thích:**

* -sV: bật tính năng dò phiên bản dịch vụ đang chạy trên các cổng mở.

