BÁO CÁO BÀI THỰC HÀNH SỐ 7

PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

Họ và tên sinh viên: Nguyễn Nhật Bách

MSSV: 1050080088

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

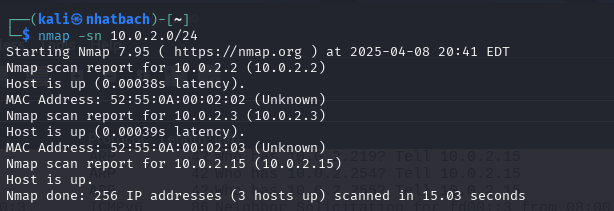
- File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

KẾT QUẢ THỰC HÀNH

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

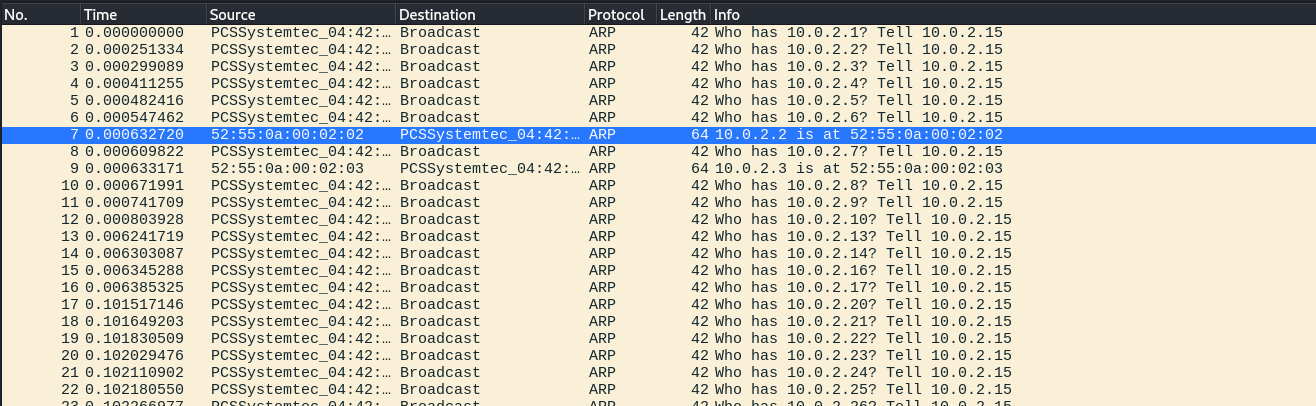
1.1. Kịch bản 1

- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm



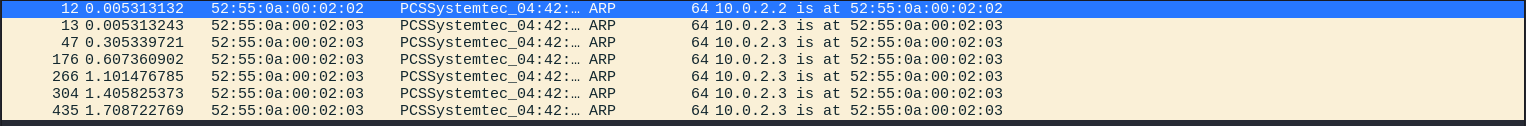
- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

Đây là **ARP Scan**, nơi attacker (10.0.2.15) gửi broadcast hỏi toàn bộ subnet để xác định IP nào đang hoạt động.





Arp.opcode == 2



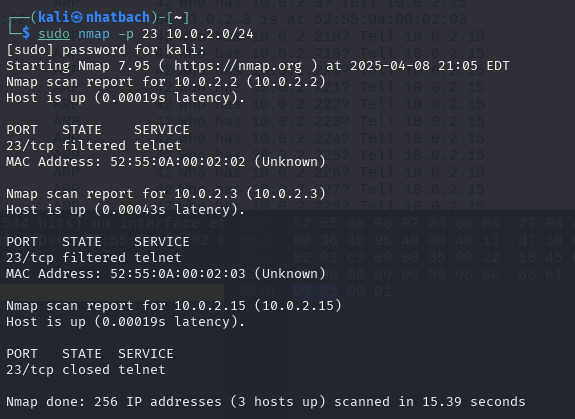
chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm

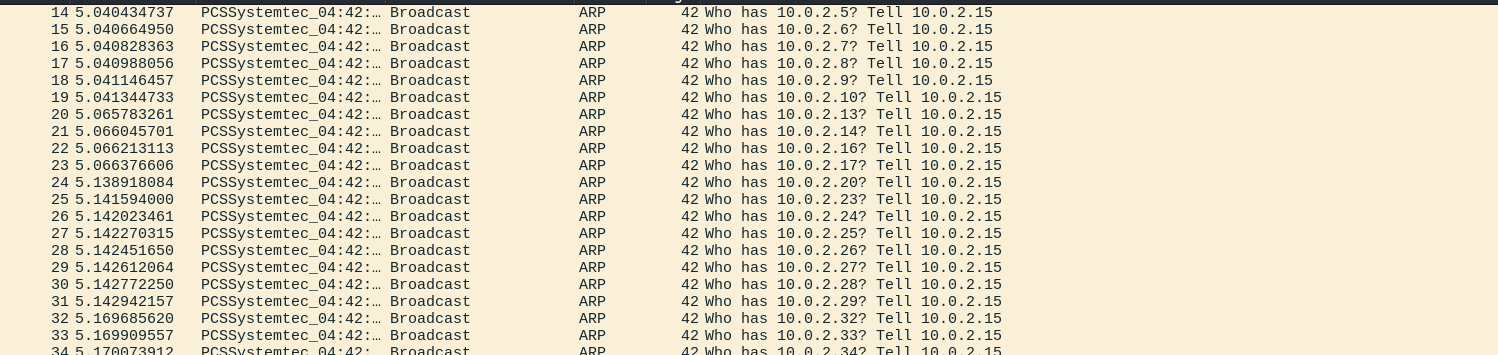
1.2. Kịch bản 2

- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm



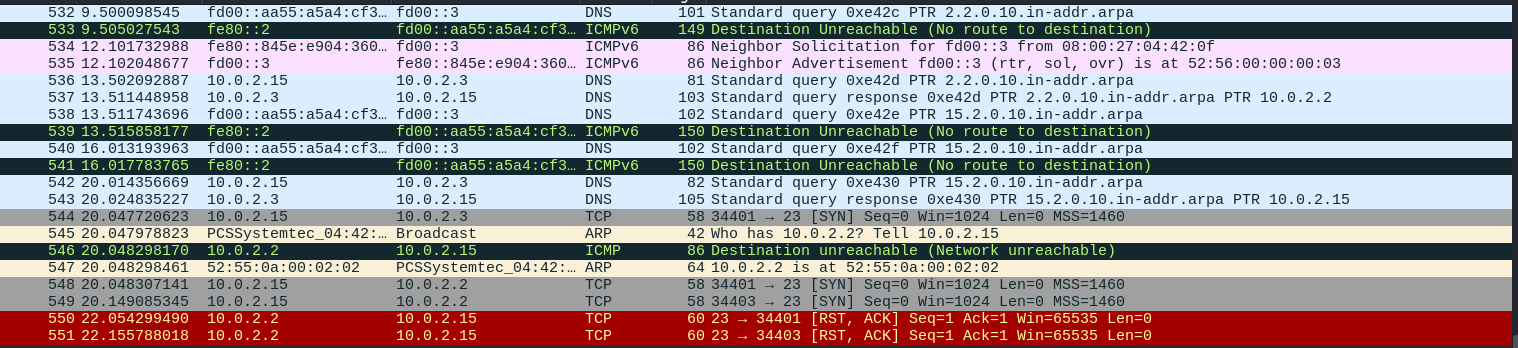
- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

các gói ARP Request gửi từ 10.0.2.15 đến toàn bộ subnet để tìm địa chỉ MAC của các IP

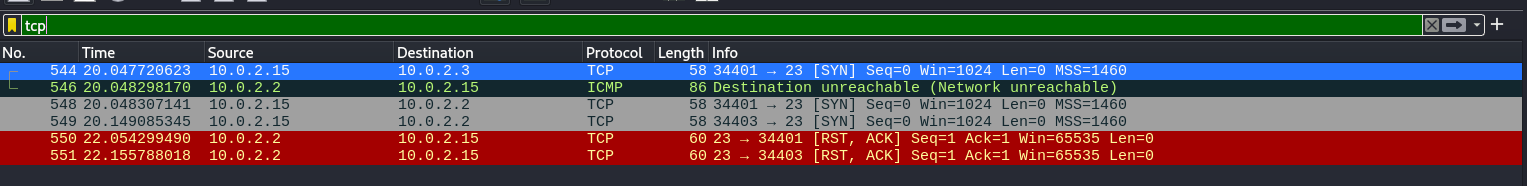


 SYN được gửi từ máy quét đến port 23.

 Đích trả lại RST → nghĩa là **cổng đóng**.



Tcp



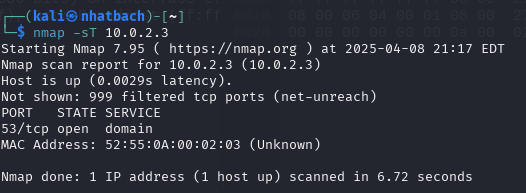
chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm

1.3. Kịch bản 3

- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

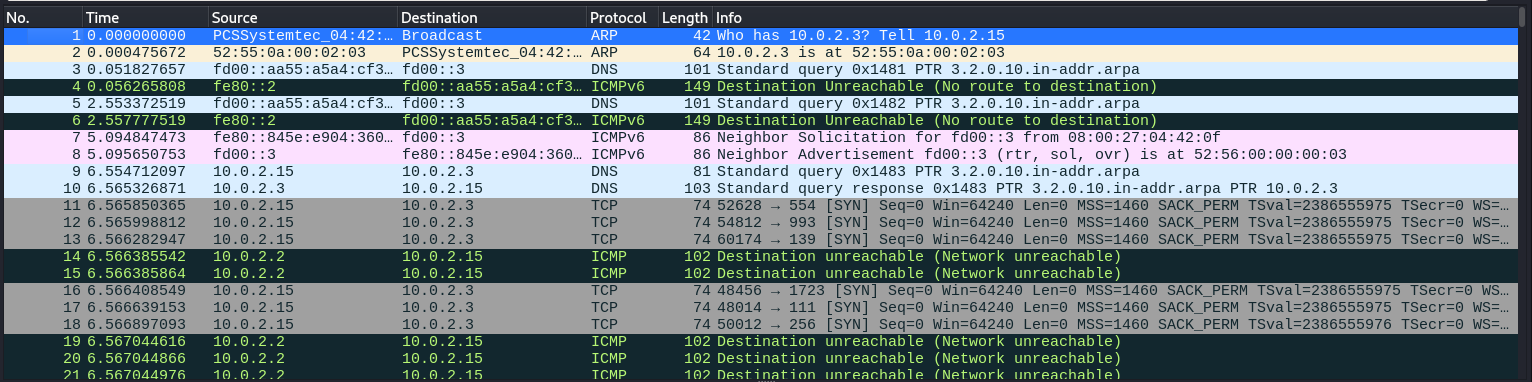


- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

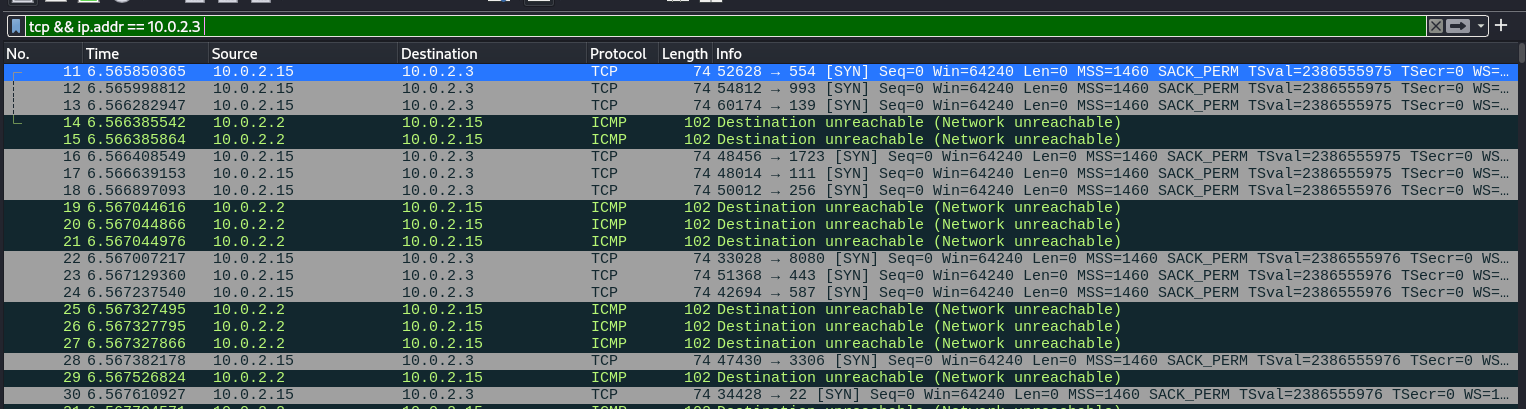
**Gói tin ARP**: Các dòng hỏi "Who has 10.0.2.x? Tell 10.0.2.15" chứng tỏ một thiết bị (10.0.2.15) đang tìm kiếm tất cả địa chỉ IP trong mạng LAN để xác định máy nào đang hoạt động. Đây là **ARP Scan**, một phương pháp phổ biến để thu thập danh sách thiết bị đang kết nối.

**Gói tin ICMP "Destination Unreachable"**: Thiết bị nguồn cố gắng giao tiếp với nhiều địa chỉ IP, nhưng nhận phản hồi "No route to destination." Đây thường là dấu hiệu của **quét thăm dò bằng ICMP**, nơi kẻ tấn công cố gắng kiểm tra xem địa chỉ nào tồn tại nhưng bị chặn truy cập.

**Gói tin TCP SYN**: Một số dòng như 10.0.2.15 → 10.0.2.2: 554 [SYN] cho thấy thiết bị 10.0.2.15 đang gửi gói tin SYN đến nhiều cổng khác nhau mà không hoàn tất kết nối ba bước (**three-way handshake**). Đây là **TCP SYN Scan**, một kỹ thuật được sử dụng để kiểm tra cổng nào đang mở mà không thiết lập kết nối đầy đủ.



tcp && ip.addr == 10.0.2.3



chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm

2. Thu thập thông tin hệ thống

- Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụngtrong lệnh này?(1 điểm)

**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

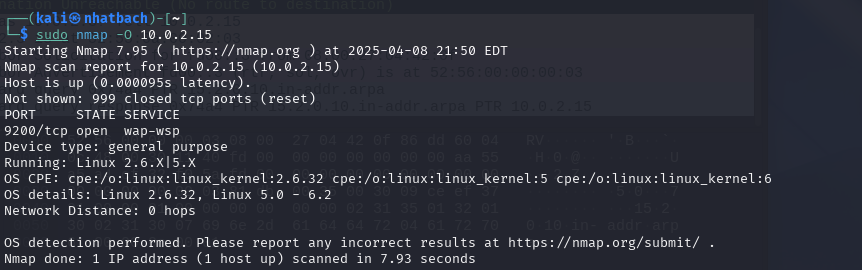
sudo nmap -O

sudo nmap -O 10.0.2.15

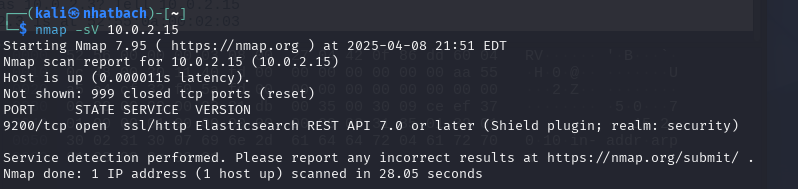
nmap -sV

nmap -sV 10.0.2.15

sudo nmap -O 10.0.2.15



nmap -sV 10.0.2.15



Thông tin hệ điều hành:

- Hình ảnh chụp kết quả của nmap: 0.25 điểm

- Nêu tên và phiên bản hệ điều hành: 0.25 điểm

Thông tin dịch vụ: 1 điểm

- Hình ảnh chụp kết quả của nmap: 0.25 điểm

- Danh sách dịch vụ: 0.75 điểm