BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Nguyễn Trần Ngọc Nam***

***MSSV: 1050080188***

***Yêu cầu kết quả thực hành:***

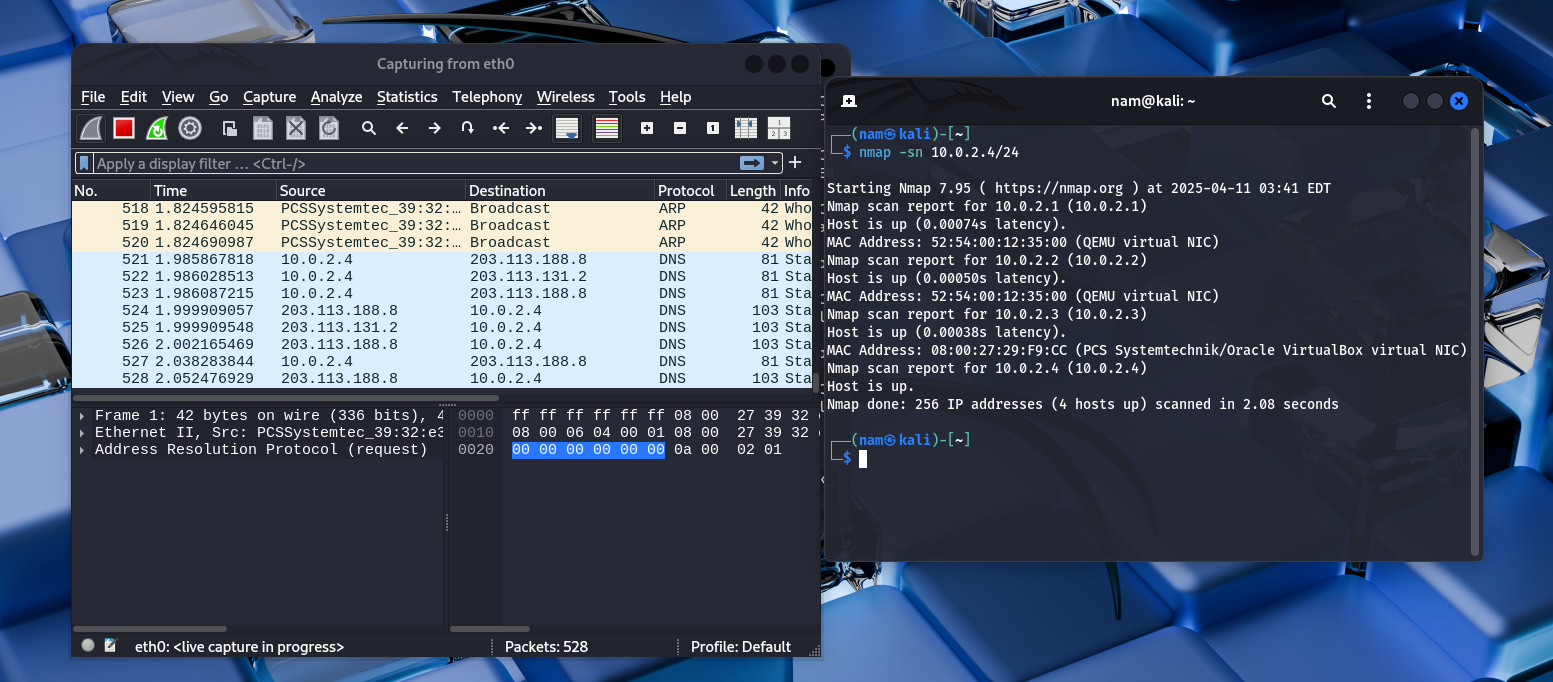
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

* 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. **Kịch bản 1**

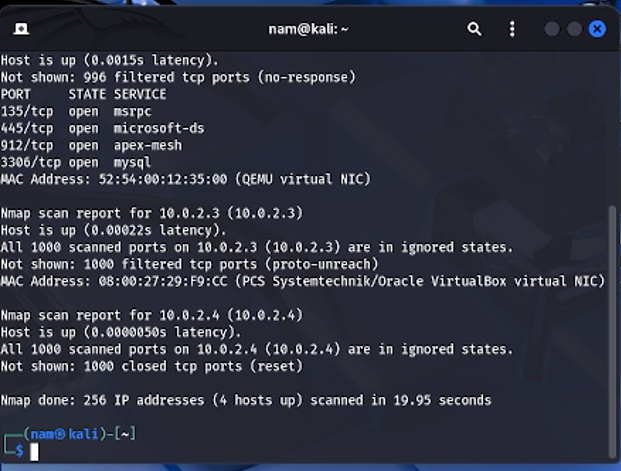
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

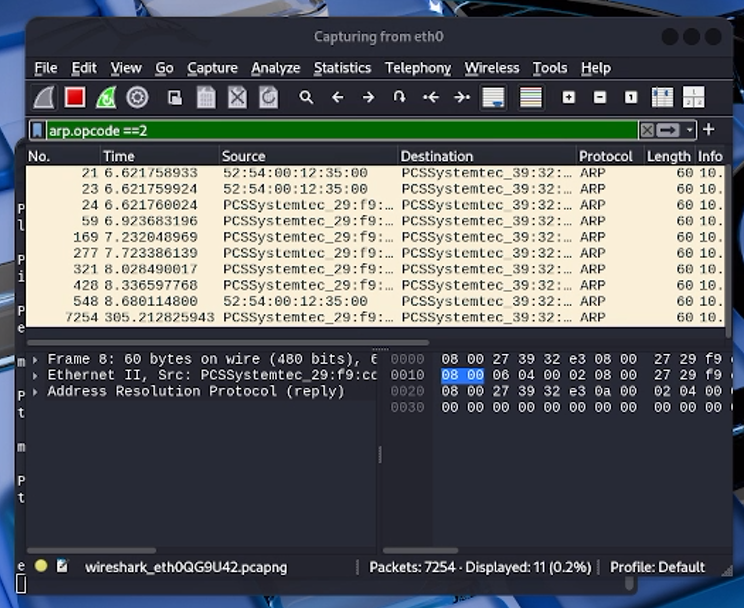


* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

Kỹ thuật quét thăm dò trong kịch bản sử dụng nmap -sn là **ping sweep (ARP ping)**. Dựa vào kết quả bắt gói Wireshark, có thể thấy:

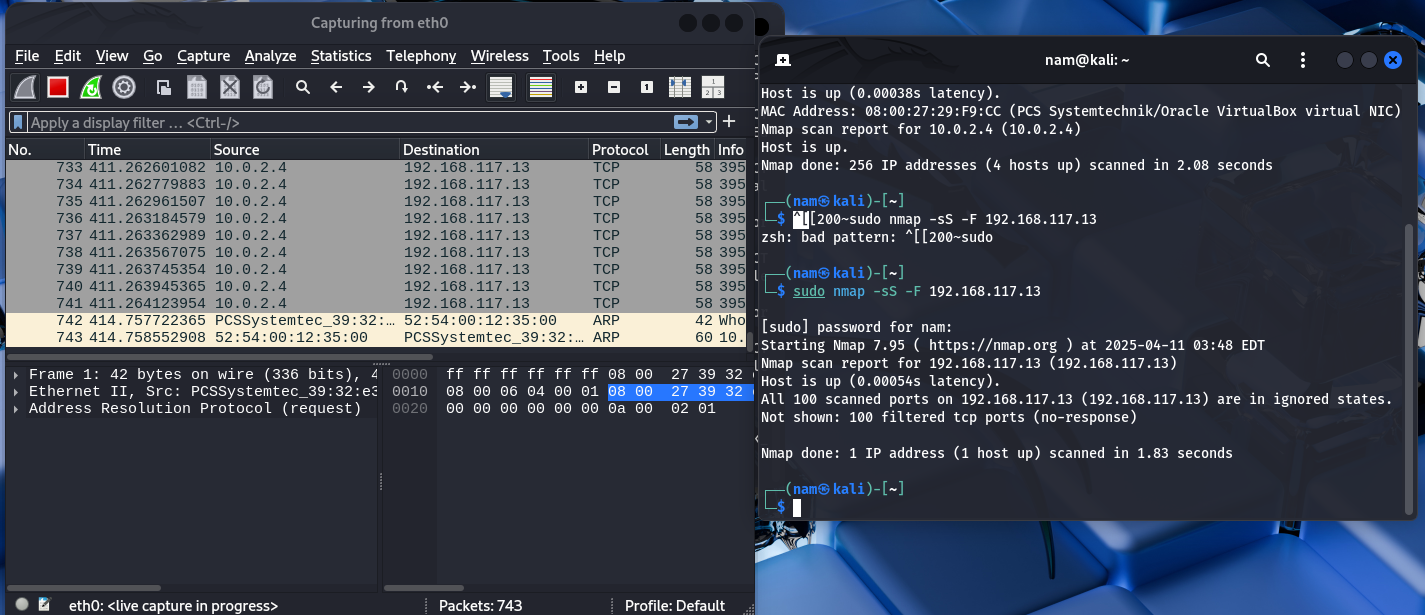
* Máy Kali gửi nhiều **gói ARP request** đến các địa chỉ IP trong dải 10.0.2.0/24, nhằm xác định host nào đang hoạt động.
* Không có gói TCP SYN hay UDP gửi đến các cổng → chứng tỏ không phải quét cổng.
* Đây là một kỹ thuật thăm dò đơn giản, không gây nhiều chú ý, được dùng để lập bản đồ các thiết bị trong mạng LAN.

**

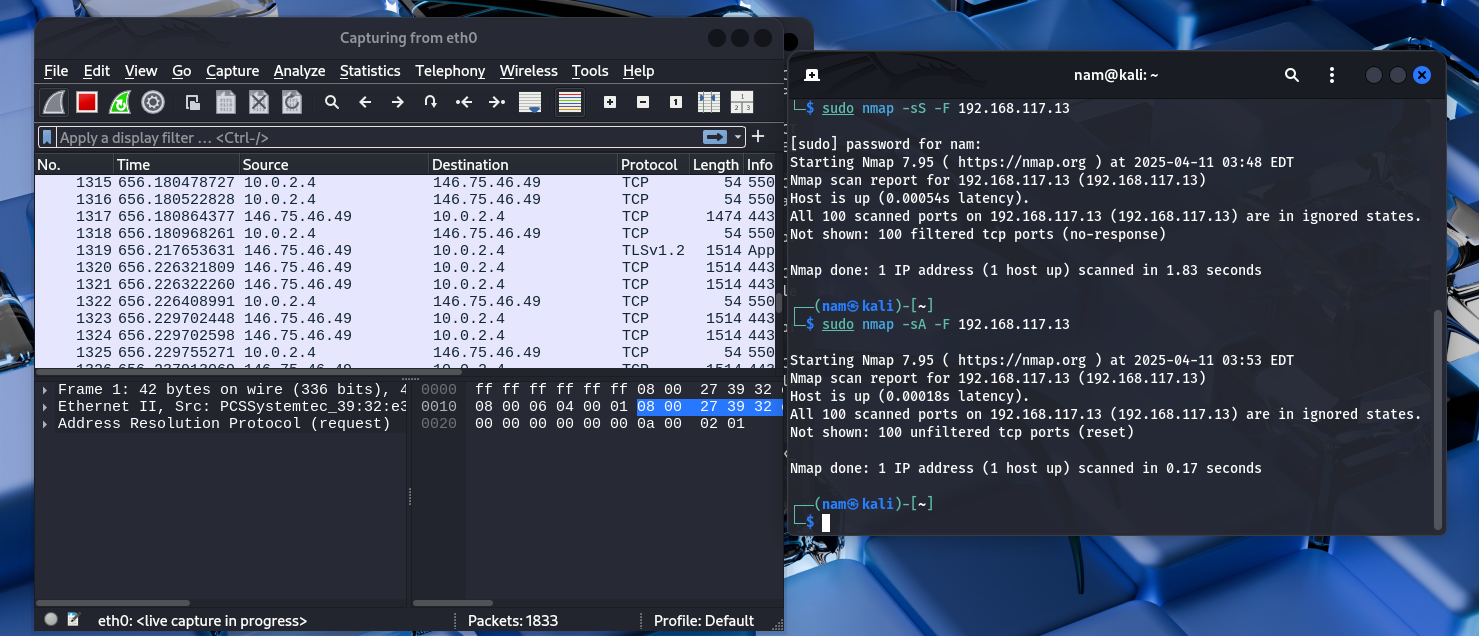


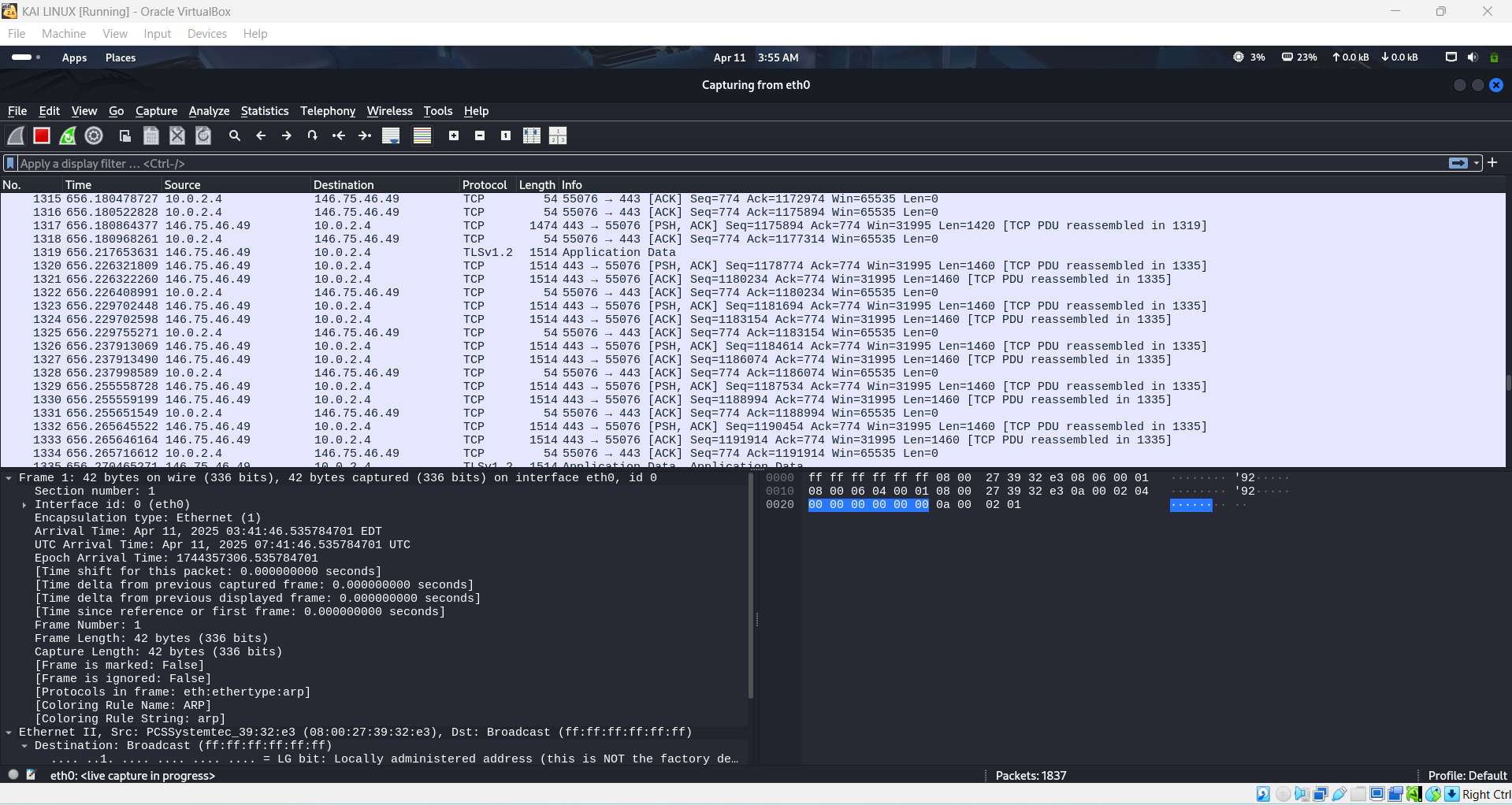
Hình ảnh hiển thị các **gói ARP Reply** với opcode = 2. Đây là dấu hiệu cho thấy có kỹ thuật **quét thăm dò mạng LAN sử dụng ARP sweep**. Máy Kali gửi nhiều ARP Request đến các IP trong mạng và nhận về các ARP Reply từ những máy đang hoạt động. Kỹ thuật này thường được sử dụng bởi nmap -sn, arp-scan hay netdiscover. Đặc điểm của phương pháp này là **không tạo ra lưu lượng TCP/UDP**, tránh bị phát hiện bởi tường lửa hoặc IDS trong mạng nội bộ.

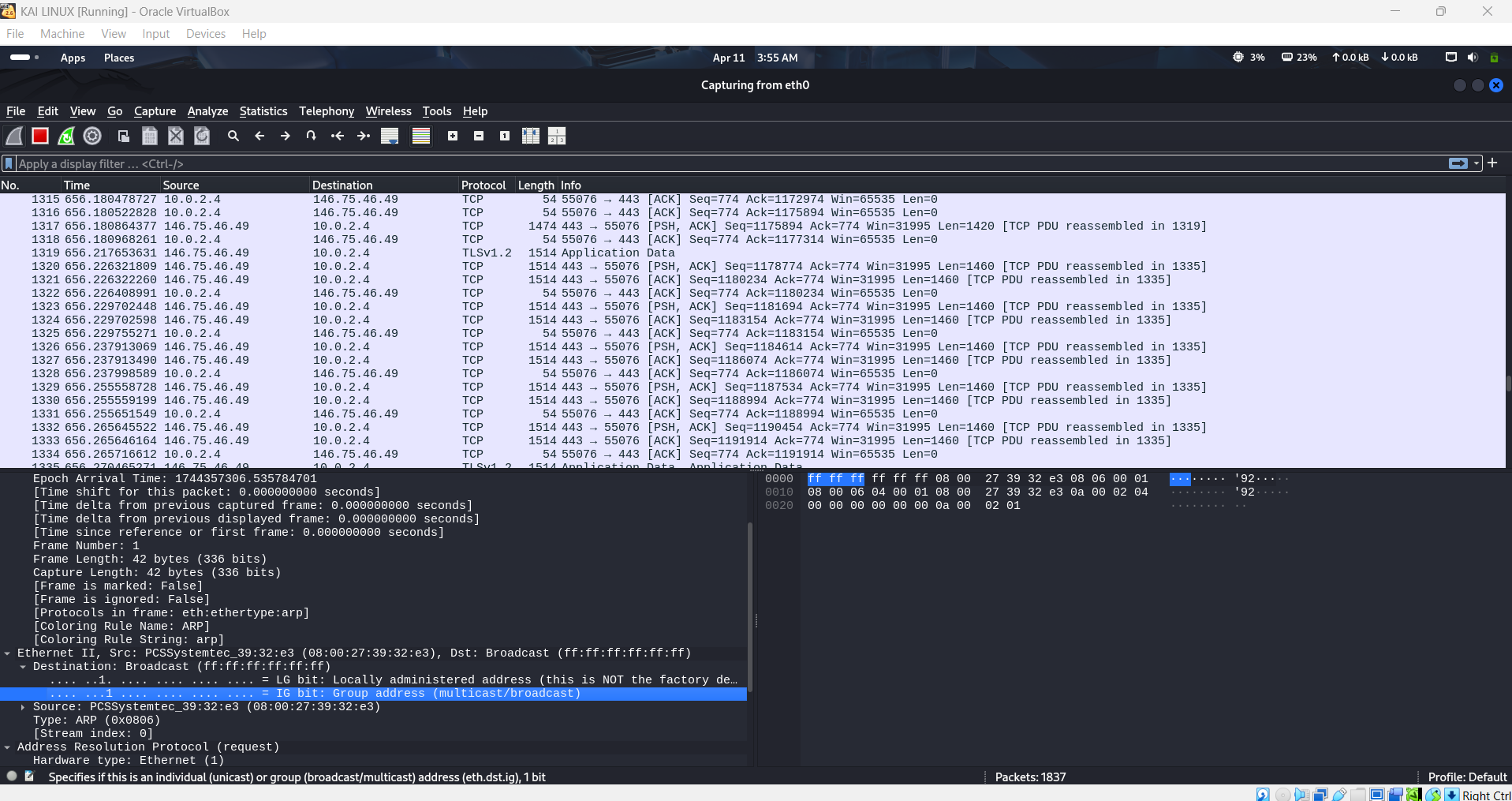
* 1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm



* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm
* Kỹ thuật quét được sử dụng trong trường hợp này là **TCP SYN Scan**. Trên Wireshark, ta có thể nhận thấy các gói tin TCP được gửi từ máy quét (IP 10.0.2.15) đến máy đích 192.168.117.13 với cờ SYN được bật, thể hiện rõ qua dòng “Flags: 0x002 (SYN)” và “SYN: Set”. Sau đó, phản hồi từ máy mục tiêu sẽ là SYN+ACK nếu cổng đang mở hoặc RST (Reset) nếu cổng bị đóng – ví dụ như trong gói tin "TCP 80 → 39177 [RST]". Phương thức quét này chỉ gửi gói SYN mà không tiếp tục hoàn tất quá trình bắt tay 3 bước TCP, đặc trưng của kỹ thuật bán kết nối – **SYN Scan**, giúp phát hiện cổng mở một cách lén lút hơn so với quét thông thường.
  1. **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 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

**– Câu hỏi:** Lệnh nào được sử dụng để quét và phát hiện máy chủ email? Giải thích chi tiết các tham số có trong lệnh đó. (1 điểm)

Để phát hiện các máy chủ email trên mạng, có thể sử dụng công cụ **Nmap** kết hợp với các **script NSE (Nmap Scripting Engine)** để quét các cổng dịch vụ email như SMTP, POP3, và IMAP.

**Ví dụ lệnh thường dùng:**

cpp

* nmap -p 25,110,143,465,587,993,995 --script smtp-commands,smtp-enum-users <IP\_hoặc\_tên\_miền>

**Phân tích cú pháp lệnh:**

* nmap: công cụ mạnh để quét mạng, phát hiện dịch vụ và hệ điều hành của thiết bị trong hệ thống.
* -p 25,110,143,465,587,993,995: yêu cầu Nmap quét các cổng thường được sử dụng cho dịch vụ email, bao gồm:  
  + 25: SMTP – gửi thư điện tử.
  + 110: POP3 – nhận email không mã hóa.
  + 143: IMAP – truy cập email từ nhiều thiết bị.
  + 465: SMTP sử dụng SSL (bảo mật).
  + 587: SMTP có xác thực (thường dùng gửi mail).
  + 993: IMAP sử dụng SSL.
  + 995: POP3 sử dụng SSL.
* --script smtp-commands: sử dụng script NSE để liệt kê các lệnh SMTP mà máy chủ hỗ trợ.
* --script smtp-enum-users: script này giúp kiểm tra danh sách người dùng hợp lệ nếu máy chủ cho phép thực hiện.
* <IP\_hoặc\_tên\_miền>: địa chỉ IP hoặc domain của hệ thống mục tiêu cần kiểm tra.

**Mục đích của lệnh:**

* Xác định xem hệ thống có đang chạy máy chủ email không.
* Kiểm tra những dịch vụ email nào đang hoạt động và trên cổng nào.
* Khám phá các lệnh được máy chủ hỗ trợ qua SMTP.
* Có thể dò tìm người dùng đang tồn tại nếu máy chủ không cấu hình bảo vệ tốt.

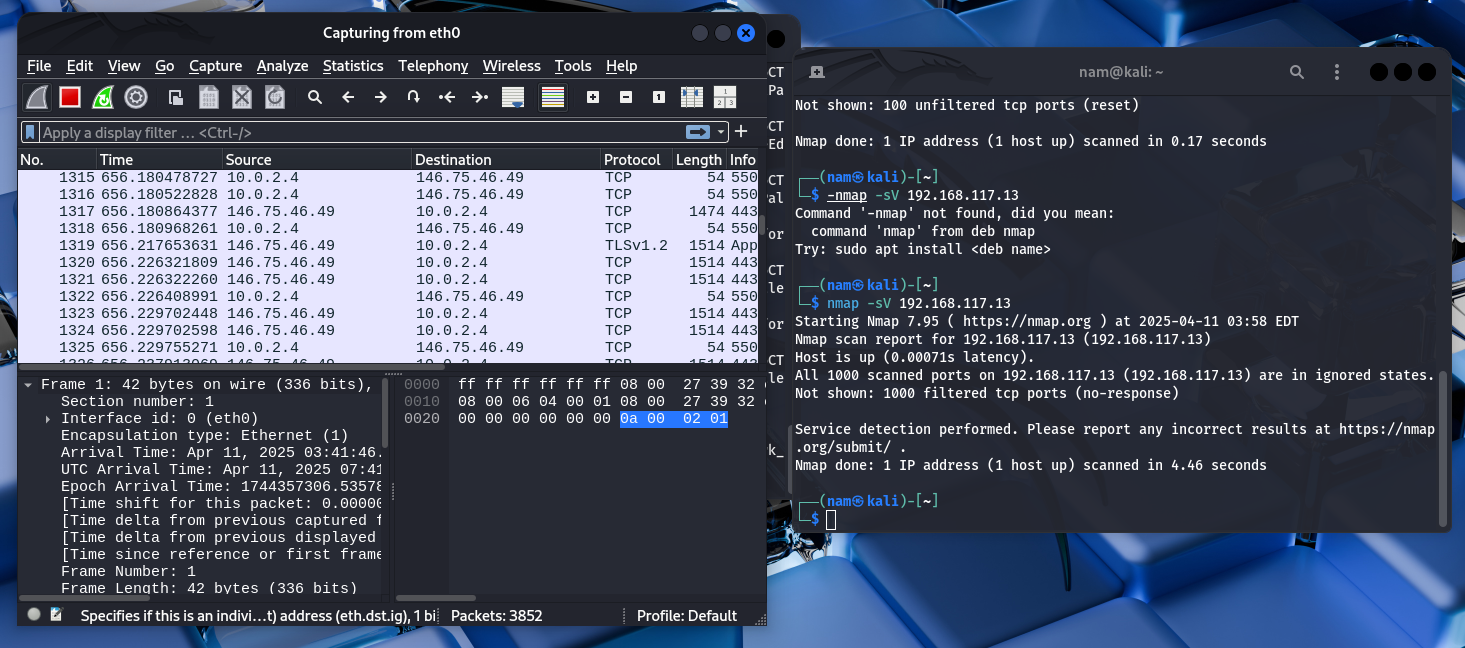
**Thông tin hệ điều hành:**

**· Tên hệ điều hành: Linux**

**· Phiên bản: Linux kernel 4.x (generic)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | Web | 80 | Apache httpd 2.4.49 |
| 2 | SSH | 22 | OpenSSH 7.9p1 |

1. **Tìm kiếm thông tin về các lỗ hổng**

****

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

Mỗi lỗ hổng: 1 điểm

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
|  |  |  |
|  |  |  |