BÁO CÁO BÀI THỰC HÀNH SỐ 7

PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

Họ và tên sinh viên: Lê Vũ Anh Kiệt

MSSV: 1050080056

Yêu cầu kết quả thực hành:

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

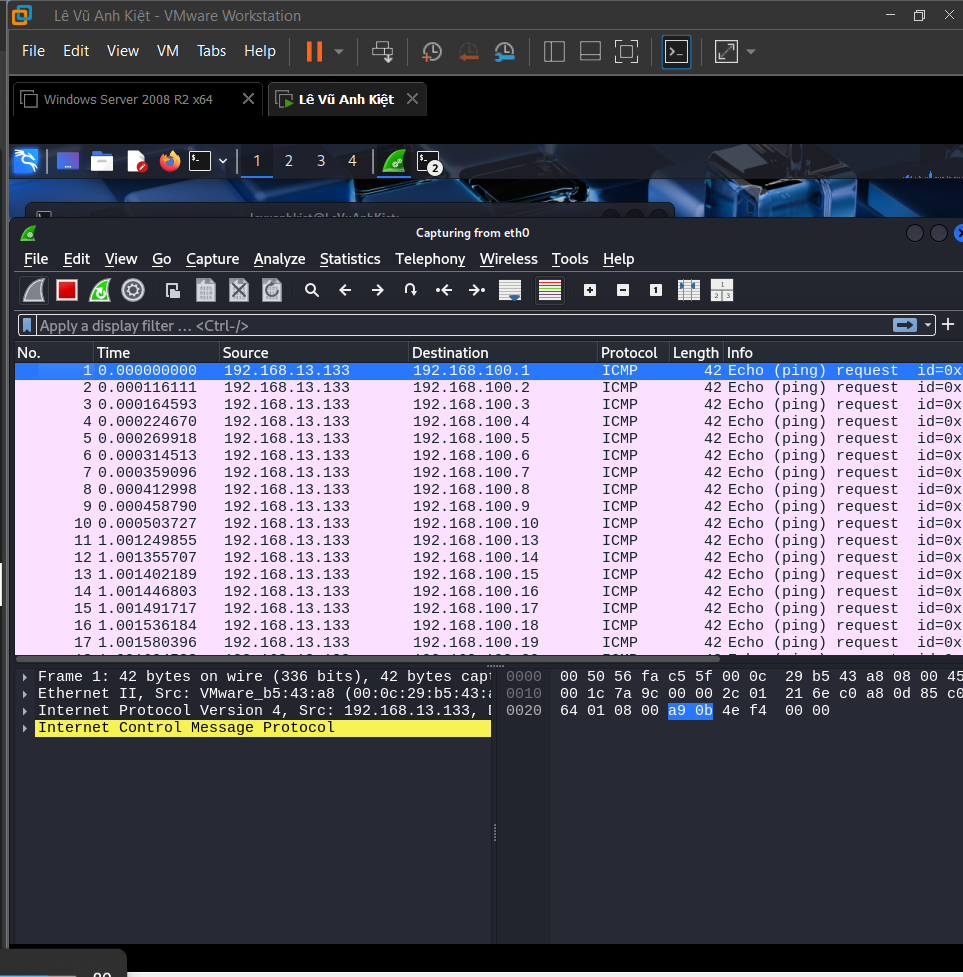
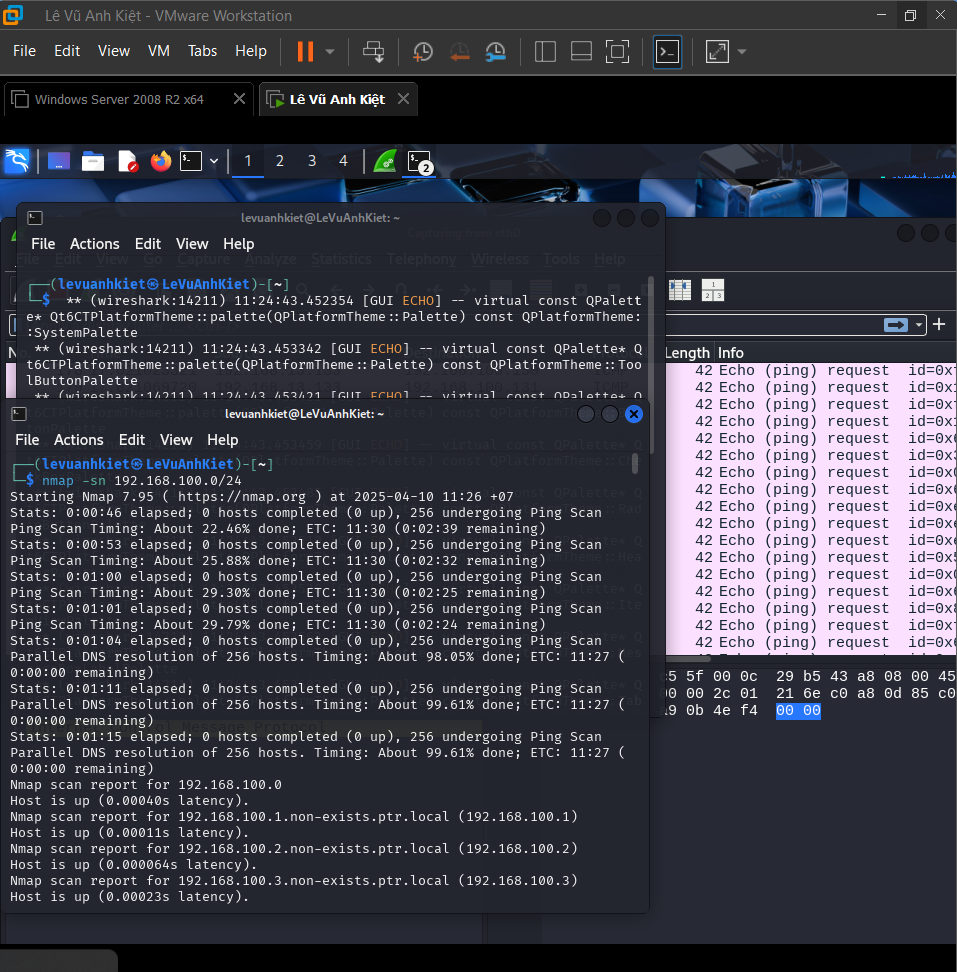
- Báo cáo kết quả thực hành

- 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

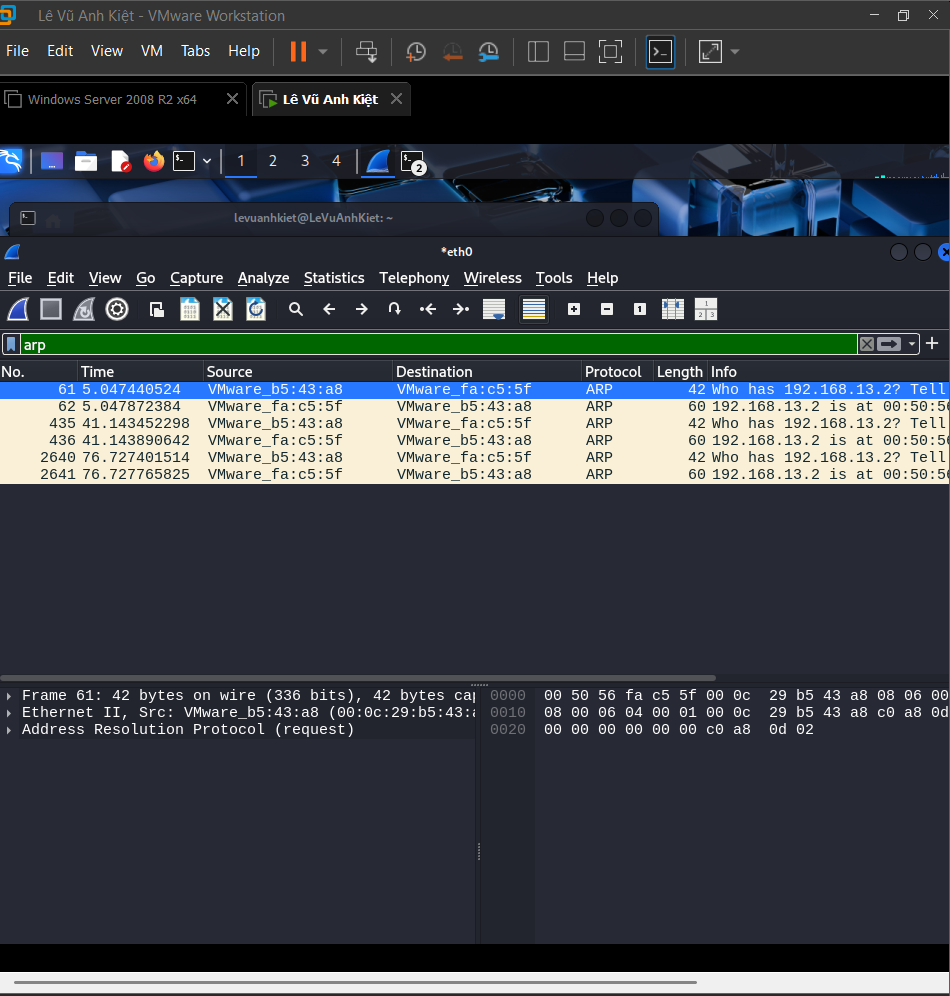
- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

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

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

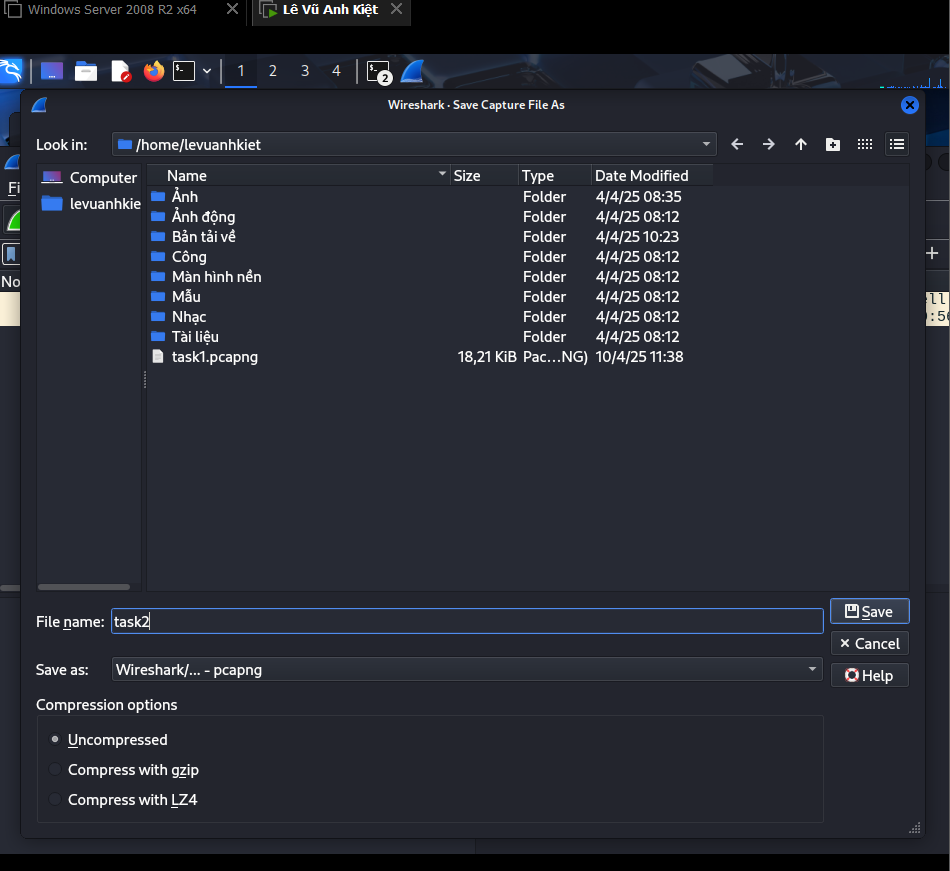
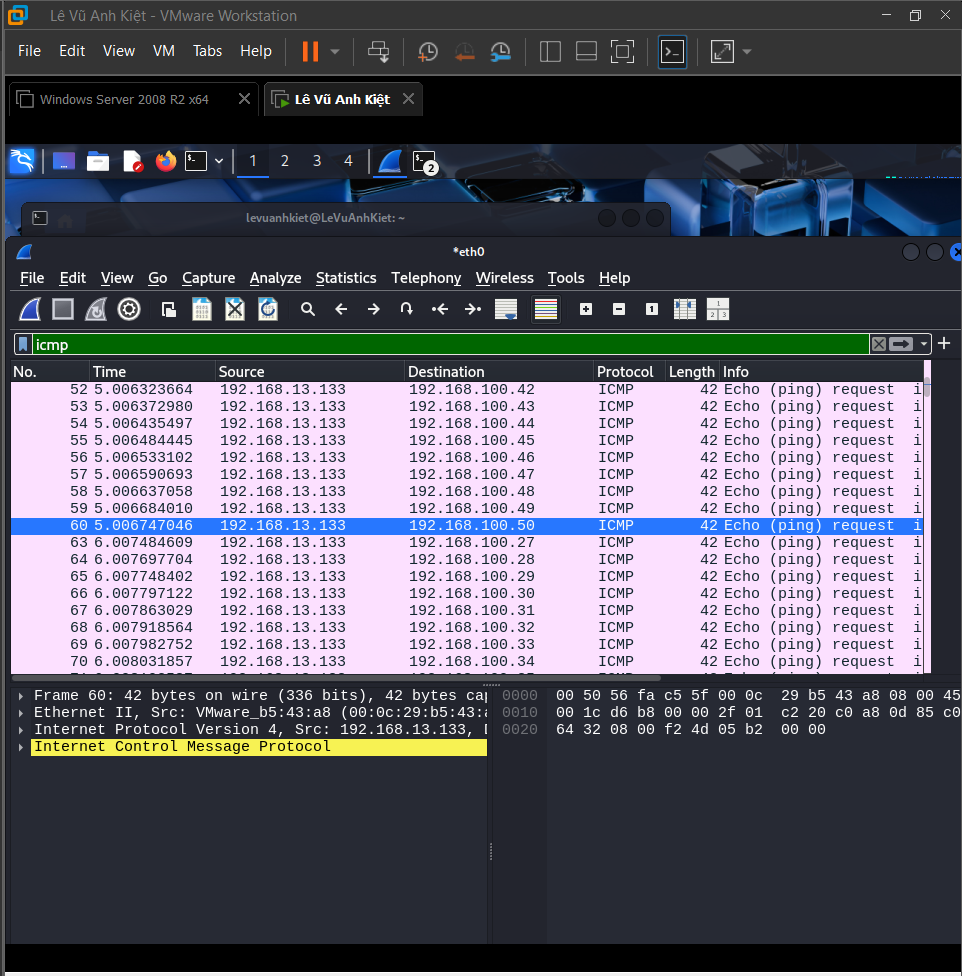
+ Kỹ thuật quét than dò ARP Ping Scan

thấy các gói tin ARP Request và ARP Reply, thì Nmap đã sử dụng **ARP Ping Scan** (vì đây là mạng nội bộ).



+ Kỹ thuật quét ICMP Ping Scan

thấy các gói tin ICMP Echo Request và ICMP Echo Reply, thì kỹ thuật là **ICMP Ping Scan** (thường dùng cho mạng bên ngoài)

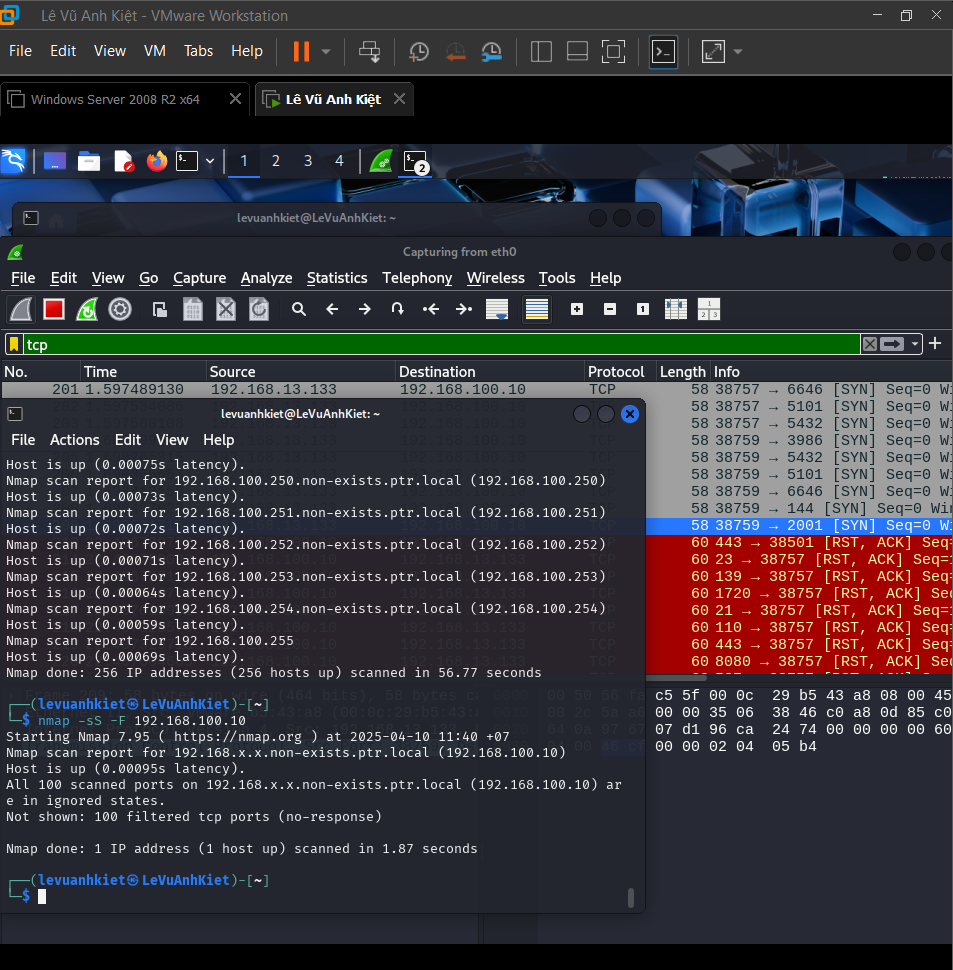


Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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

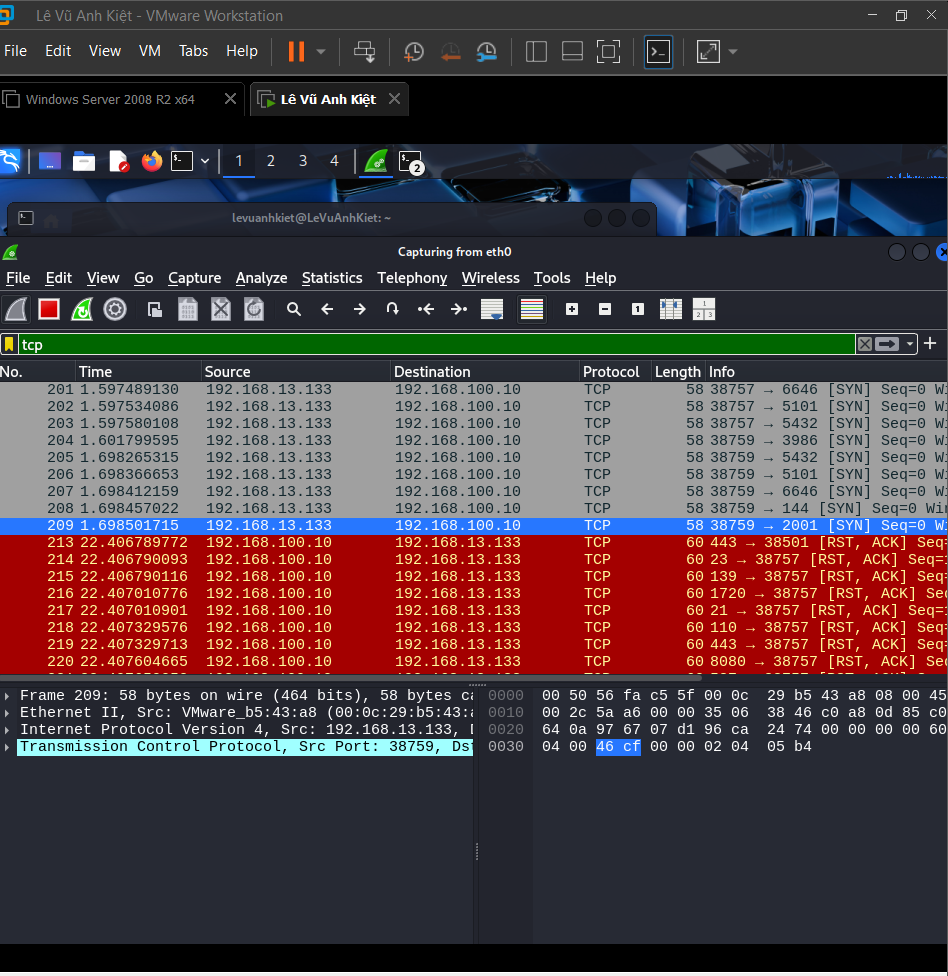


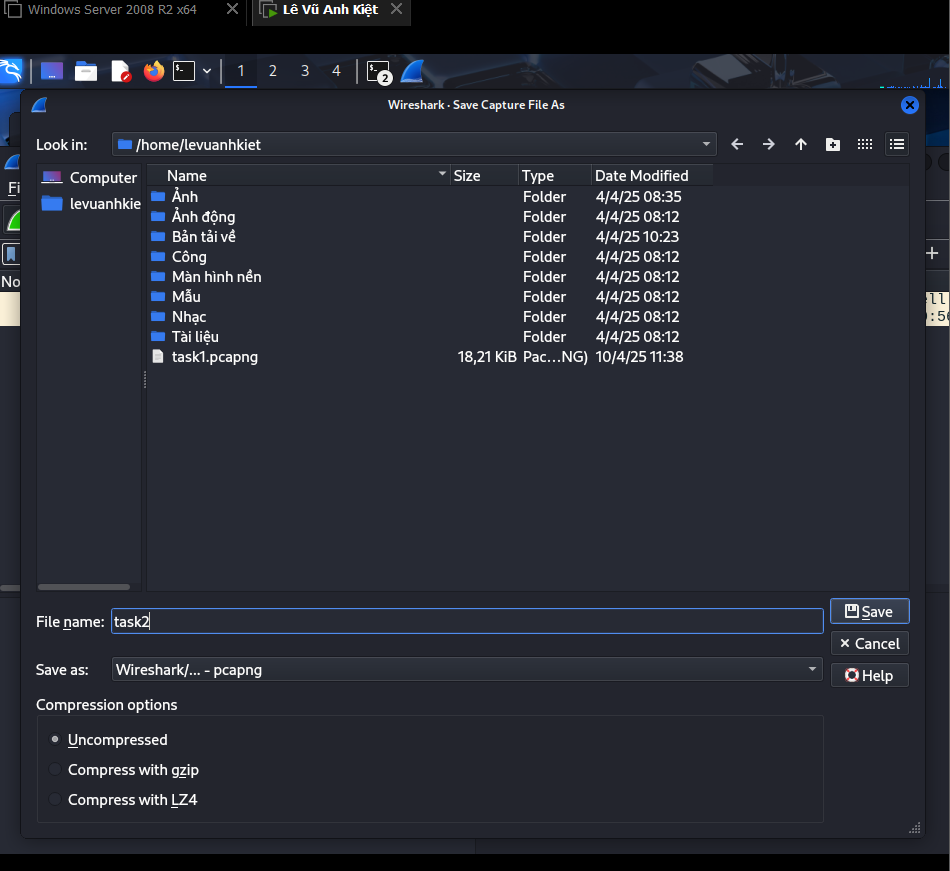
- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

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

+ Kỹ thuật quét là **TCP SYN Scan**

**máy mục tiêu trả về TCP SYN/ACK, cổng đó mở; nếu trả về TCP RST, cổng đóng**



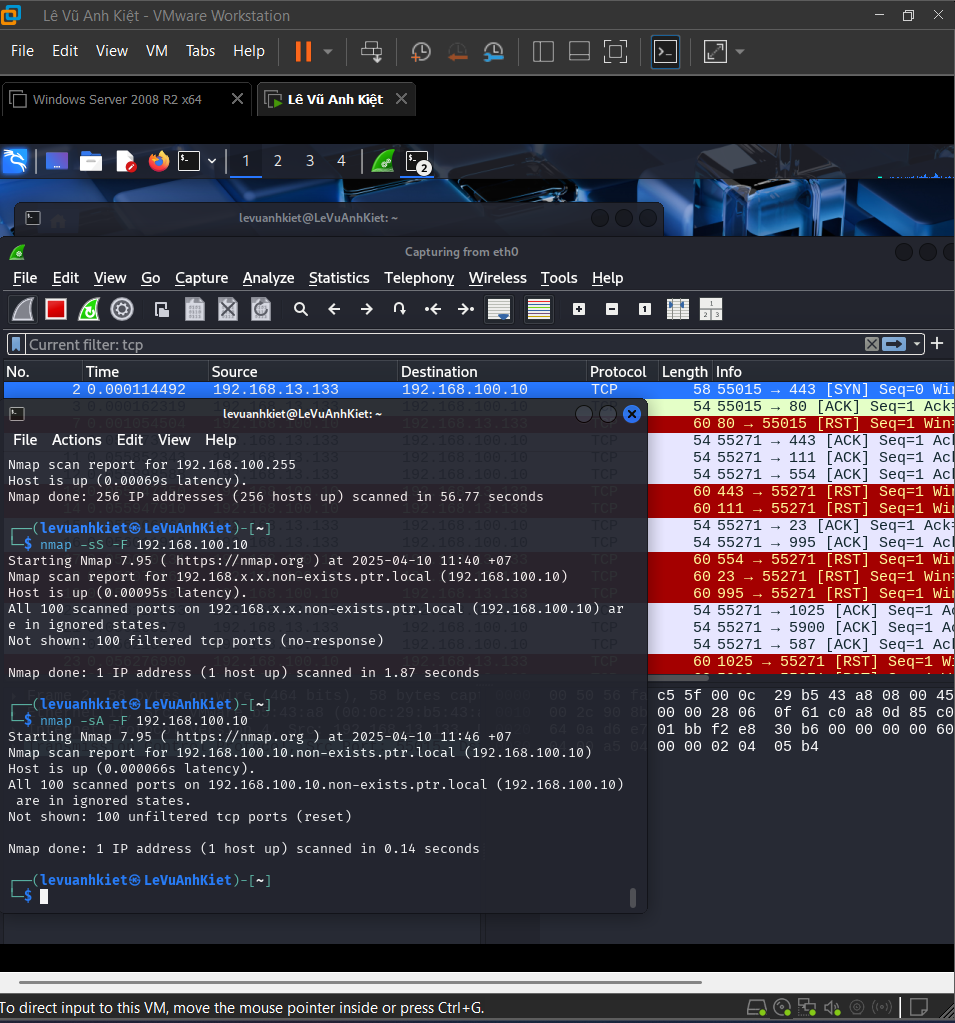


Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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

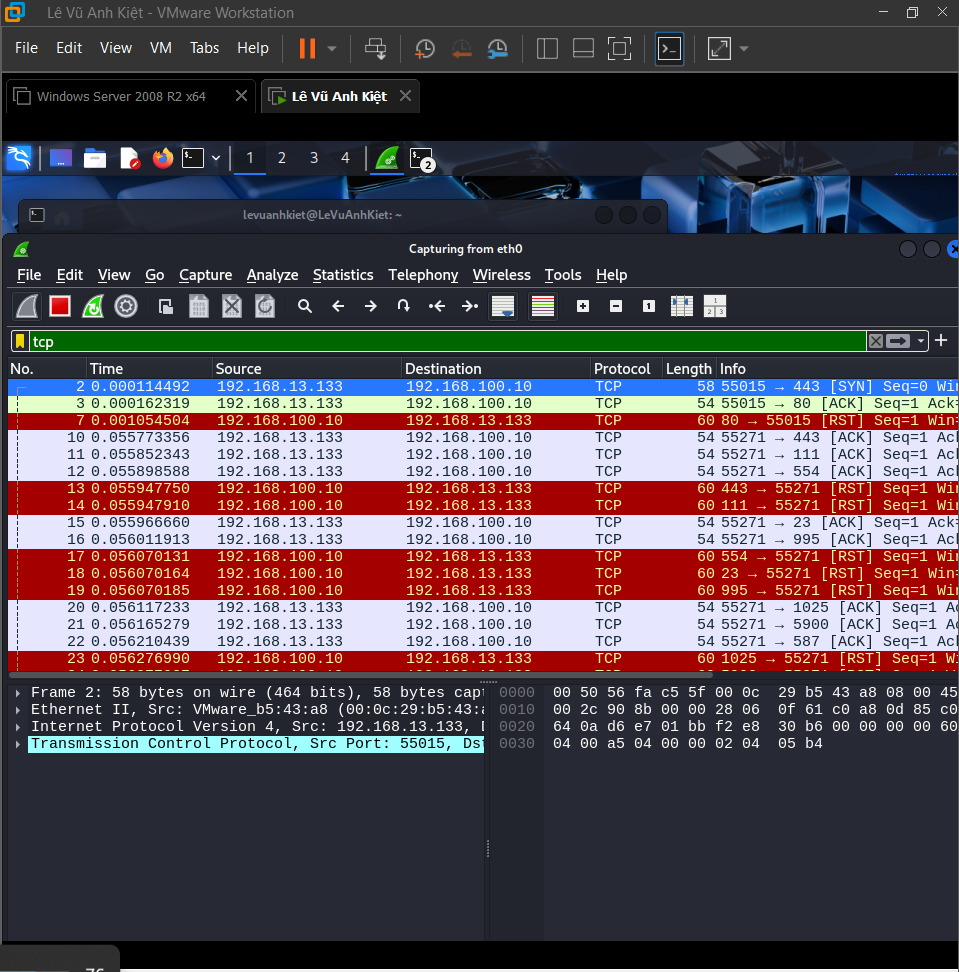


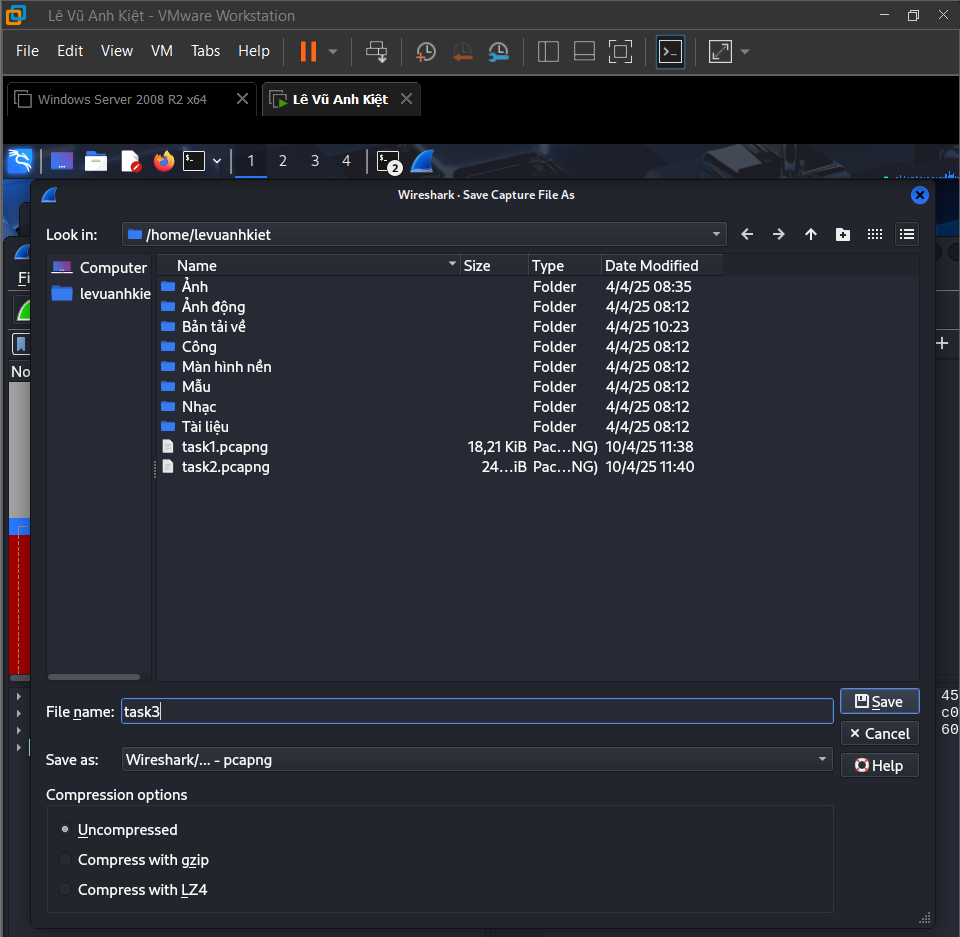
- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

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

+ Kỹ thuật quét là **TCP ACK Scan**

máy mục tiêu trả về TCP RST, cổng không bị lọc (unfiltered); nếu không có phản hồi, cổng bị firewall chặn (filtered)

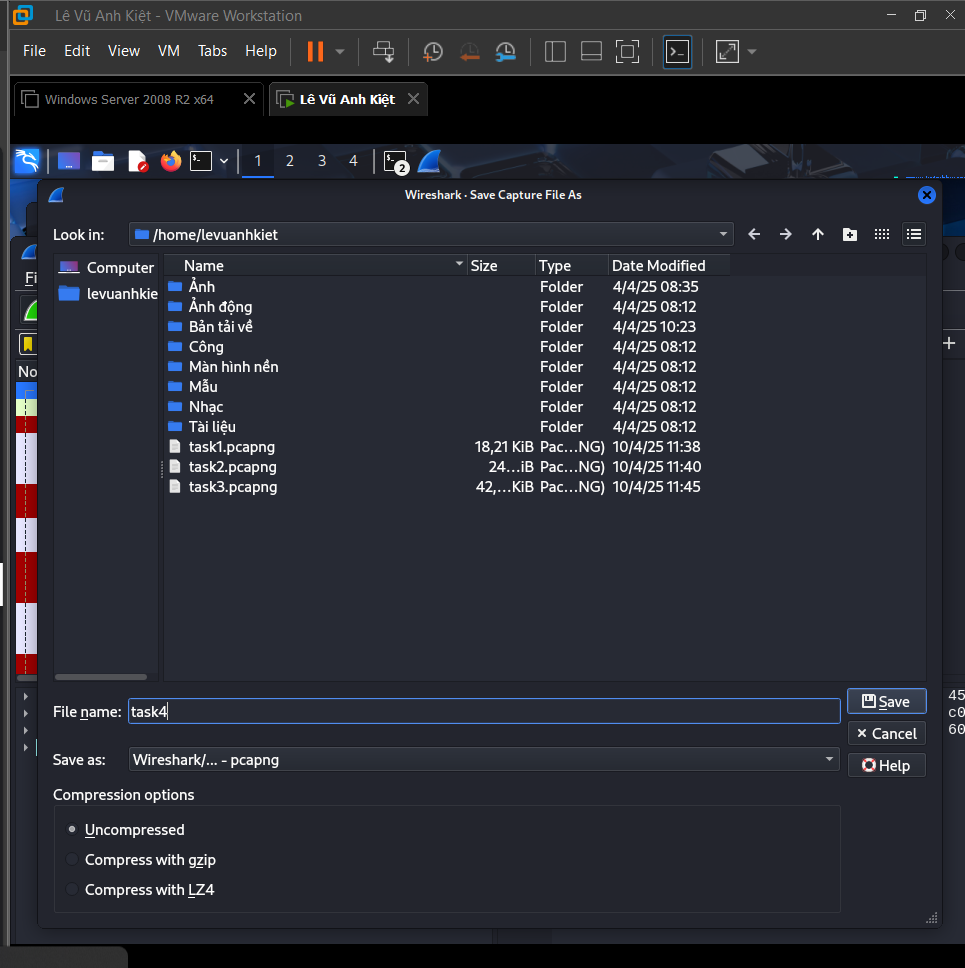




Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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 dụng

trong lệnh này?(1 điểm)

nmap -p 25,110,143 192.168.100.0/24

**Giải thích các tham số:**

nmap: Công cụ quét mạng mã nguồn mở dùng để thăm dò và thu thập thông tin.

-p 25,110,143: Tùy chọn chỉ định các cổng cần quét:

25: Cổng SMTP (Simple Mail Transfer Protocol), dùng để gửi email.

110: Cổng POP3 (Post Office Protocol version 3), dùng để nhận email.

143: Cổng IMAP (Internet Message Access Protocol), dùng để truy cập email.

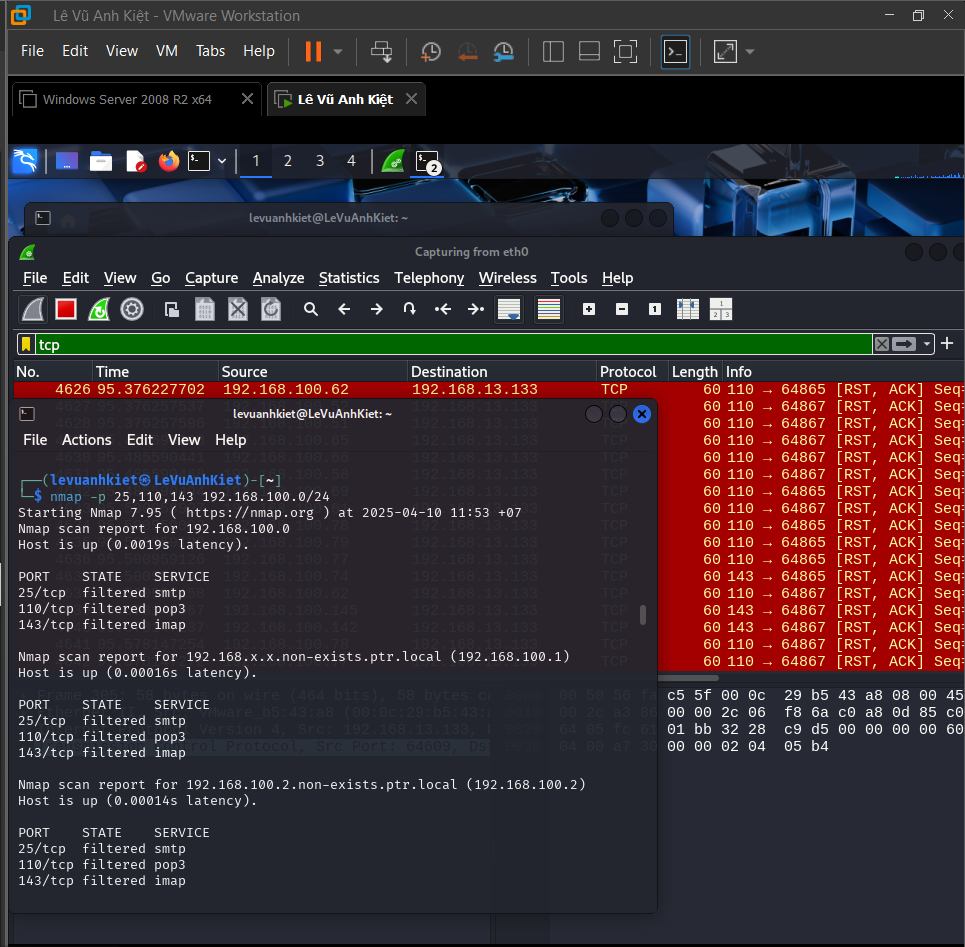
Dấu phẩy (,) phân tách các cổng cần quét.

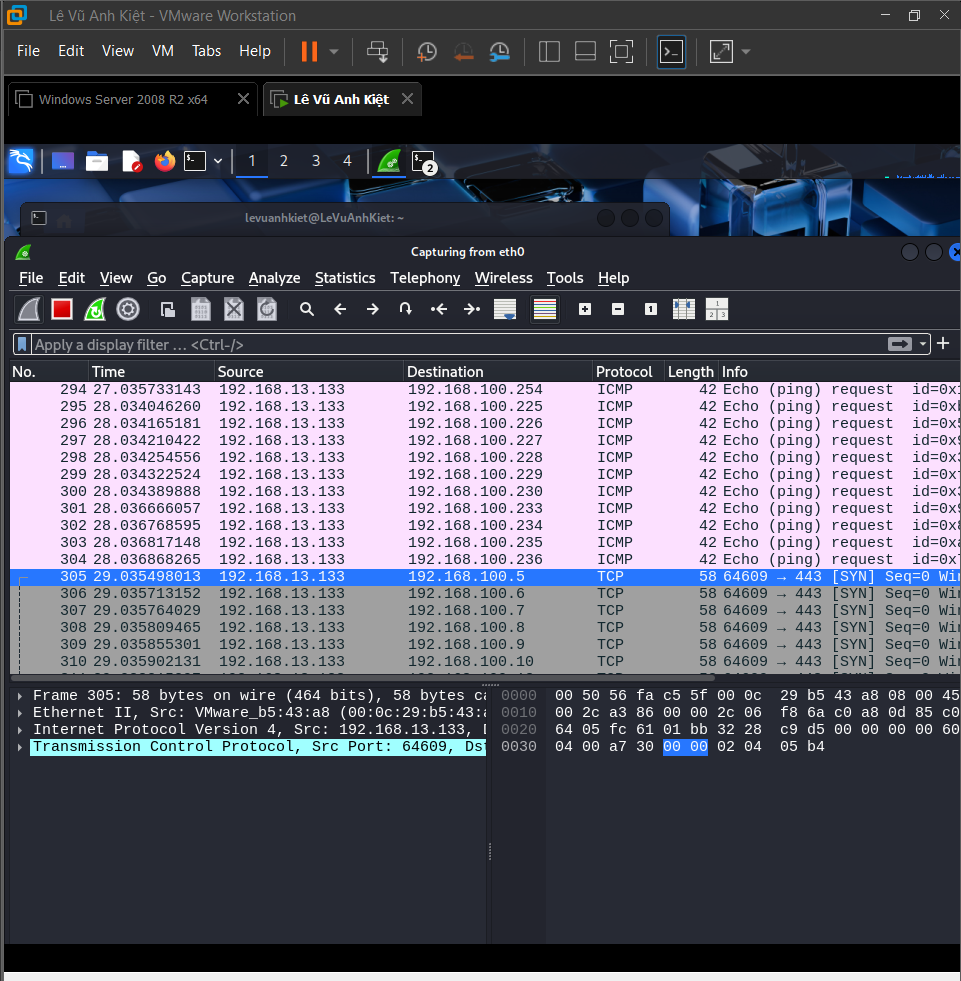
192.168.100.0/24: Dải địa chỉ IP mục tiêu, tương ứng với 256 địa chỉ từ 192.168.100.0 đến 192.168.100.255. Đây là phạm vi mạng cần tìm máy chủ email.

Lệnh này sẽ quét tất cả các host trong mạng 192.168.100.0/24 để kiểm tra xem cổng 25, 110 hoặc 143 có mở (open) hay không. Nếu một cổng mở, ta có thể kết luận host đó đang cung cấp dịch vụ email tương ứng (SMTP, POP3 hoặc IMAP).

Thông tin hệ điều hành:

- Hình ảnh chụp kết quả của nmap: 0.25 điểm



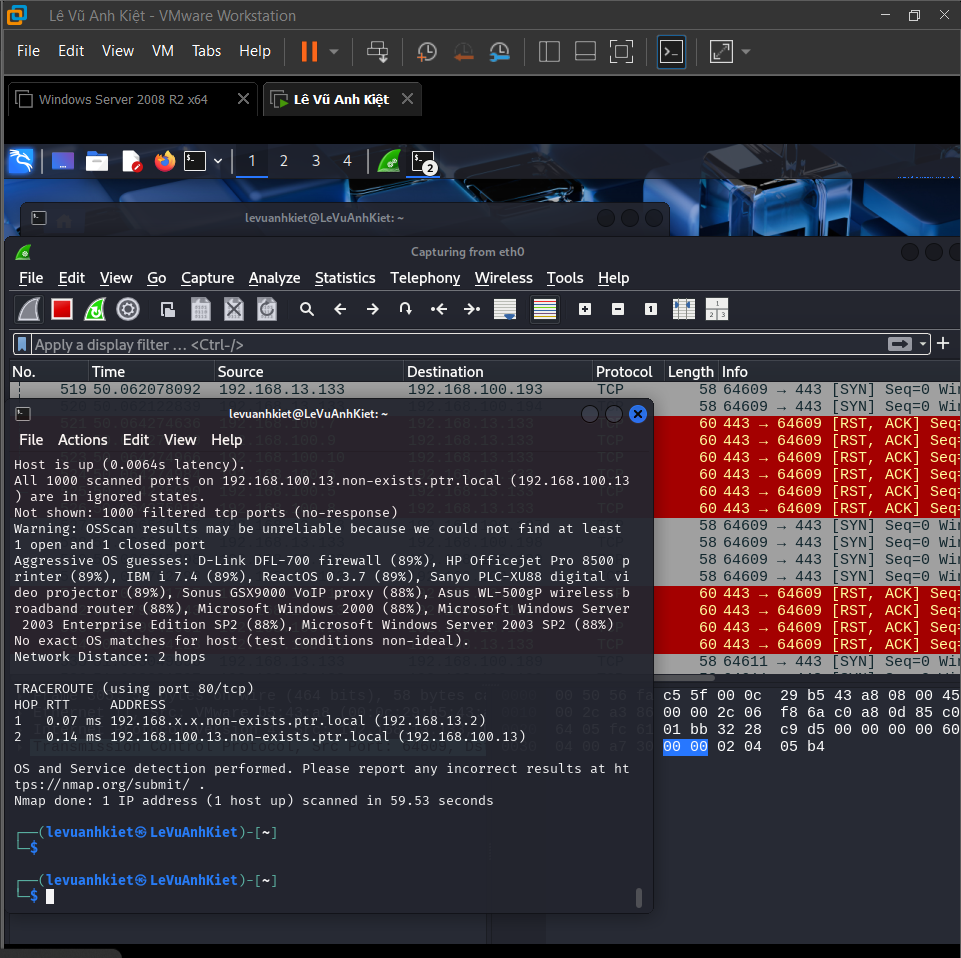


- Nêu tên và phiên bản hệ điều hành: 0.25 điểm

Hệ điều hành: Không xác định chính xác do không có cổng mở/đóng để phân tích. Nmap phán đoán có thể là D-Link DFL-700 firewall hoặc Microsoft Windows Server 2003 SP2 (độ chính xác 88-89%).

Thông tin dịch vụ: 1 điểm

- Hình ảnh chụp kết quả của nmap: 0.25 điểm



- Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng**  **dụng** | **Tên phần mềm và phiên bản** |
| 1 |  |  |  |
|  |  |  |  |
|  |  |  |  |

3. 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) |
| **Tên dịch vụ:** SMTP  **Tên phần mềm:** Postfix  **Phiên bản:** Giả định là Postfix 3.8 (phiên bản phổ biến trước 2025). | CVE-2023-51764 | Lỗ hổng "SMTP Smuggling" trong Postfix cho phép kẻ tấn công gửi email giả mạo bằng cách khai thác sự khác biệt trong cách xử lý ký tự xuống dòng (line ending) giữa các máy chủ email. Kẻ tấn công có thể chèn lệnh SMTP độc hại vào email, dẫn đến việc gửi email giả mạo mà không bị phát hiện |
| **Tên dịch vụ:** IMAP  **Tên phần mềm:** Dovecot  **Phiên bản:** Giả định là Dovecot 2.3.14 (phiên bản trước khi vá lỗi). | CVE-2022-30550 | Lỗ hổng trong Dovecot cho phép nâng cao đặc quyền (privilege escalation) khi sử dụng cùng lúc passdb master và non-master có cấu hình tương tự. Kẻ tấn công có thể khai thác để truy cập trái phép vào tài nguyên hệ thống với quyền cao hơn. |
| **Tên dịch vụ:** Hệ điều hành (liên quan đến dịch vụ email).  **Tên phần mềm:** Microsoft Windows Server 2003  **Phiên bản:** SP2 | CVE-2010-2550 | Lỗ hổng trong thành phần SMTP của Windows Server 2003 SP2 cho phép kẻ tấn công từ xa gây ra tình trạng từ chối dịch vụ (DoS) bằng cách gửi phản hồi MX record được tạo đặc biệt, làm gián đoạn hoạt động của máy chủ email |