BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Trần Minh Phát***

***MSSV: 1050080279***

***Lớp: K10\_DH\_CNPM3***

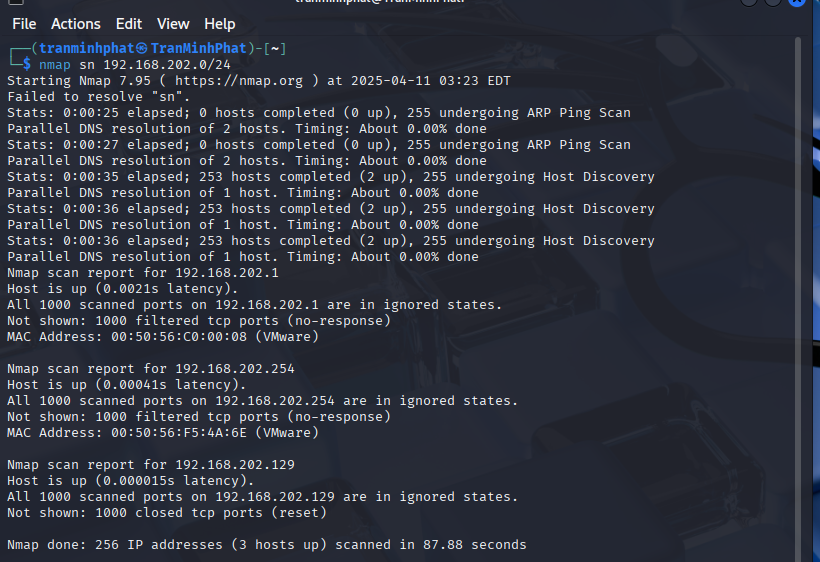
**KẾT QUẢ THỰC HÀNH**

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

Thực hiện lệnh quét nmap –sn Dia\_chi\_mang/Mat\_na trên máy do thám. Dựa trên việc phân

tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì?

Đây là khi thực hiện lệnh nmap



|  |
| --- |
| **ARP scan** |

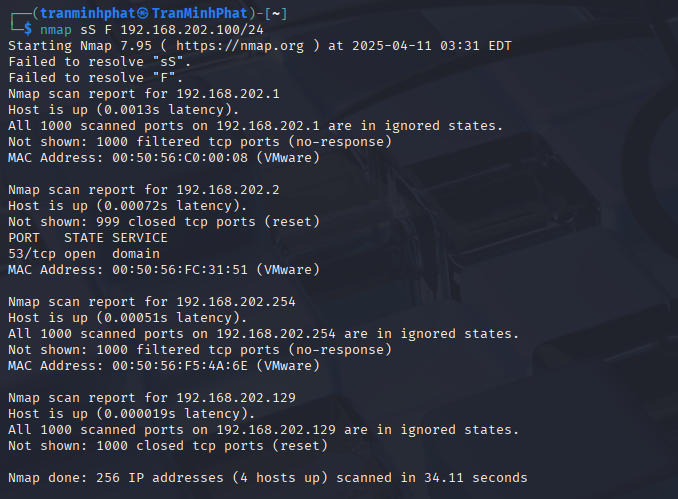
|  |
| --- |
| Gửi gói ARP để xác định host trong cùng subnet |

|  |
| --- |
| Trong mạng LAN |
| |  | | --- | | **ICMP Echo scan** |  |  | | --- | | Gửi ping ICMP để kiểm tra host sống |  |  |  | | --- | --- | | Nếu khác subnet hoặc không dùng ARP | | |  | | | **TCP Ping scan** |  |  | | --- | | Gửi gói SYN/ACK đến cổng 80/443 để xác định host sống |  |  | | --- | | Khi ICMP bị firewall chặn | |  | |

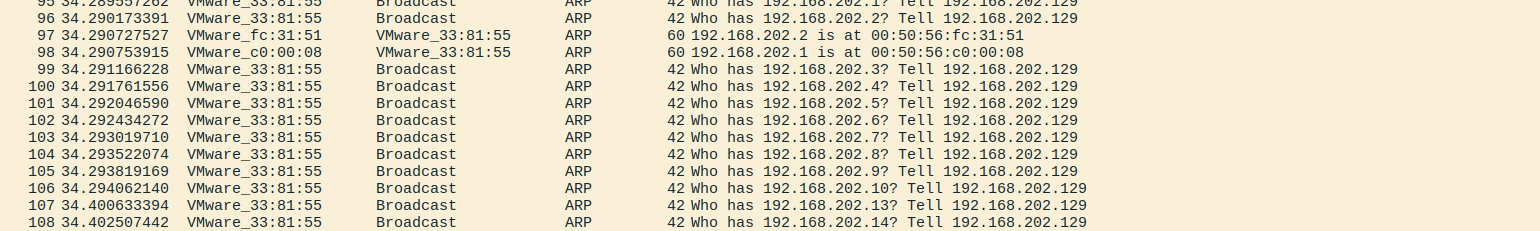
**Kịch bản 2**

Thực hiện lệnh quét nmap –sS –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên

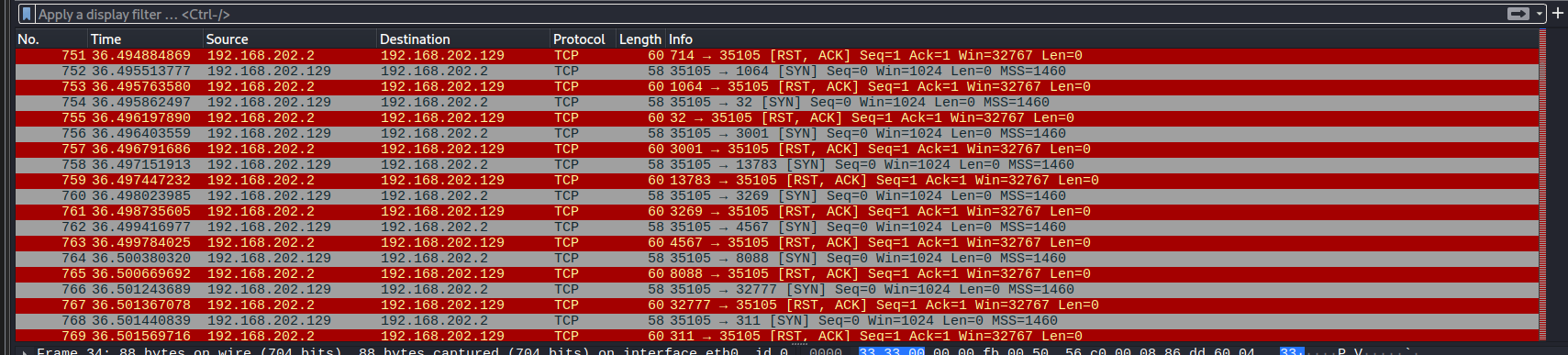
việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì?

****

Khi ta chạy thì hệ thống bắt được

****

**SYN Scan**

****

Gửi gói TCP có cờ **SYN** đến cổng cần kiểm tra.

Dựa vào phản hồi (SYN-ACK hay RST) để xác định trạng thái cổng:

SYN-ACK là Cổng **mở**

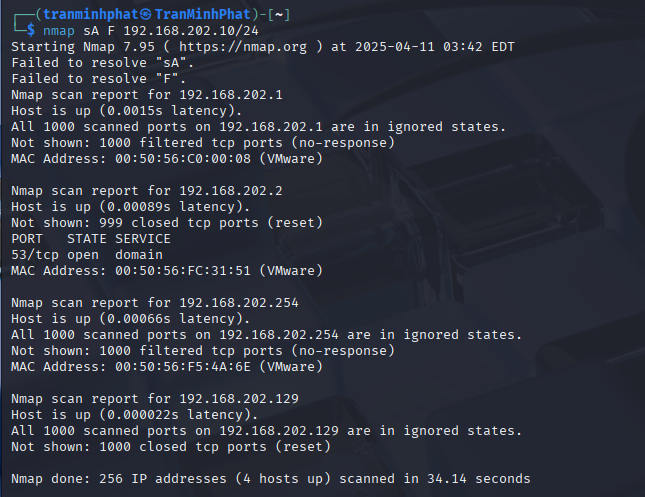
RST là Cổng **đóng**

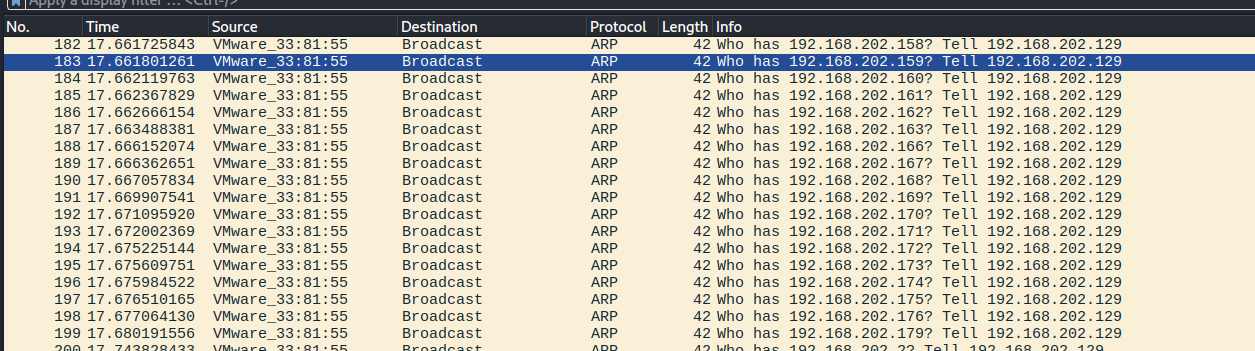
Không hoàn tất bắt tay TCP → khó bị phát hiện hơn so với Full TCP scan.

* 1. **Kịch bản 3**

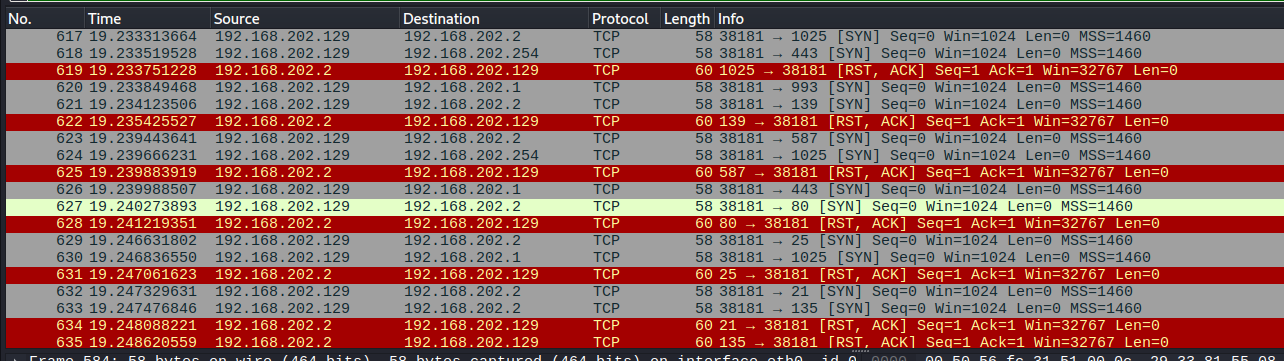
Thực hiện lệnh quét nmap –sA –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên

việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì?





**ACK Scan (quét ACK)**

****

Mục đích: Xác định xem firewall có lọc cổng hay không

Cơ chế hoạt động: Gửi gói TCP với cờ ACK đến cổng đích

Quan sát lưu lượng: Gói ACK đến từ máy do thám → máy mục tiêu phản hồi RST nếu không lọc

1. **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)

**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

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

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)** |
|  |  |  |
|  |  |  |