HỌ VÀ TÊN : **Lâm Vĩnh Kiện** LỚP: **10\_ĐH\_TMĐT** MSSV: **1050070008**

**BÀI TẬP 7 LÝ THUYẾT – 11/04/2025**

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

**Kịch bản 1:**

**-** Cài đặt nnmap, kiểm tra ip và khởi động wireshark

**A screenshot of a computer

AI-generated content may be incorrect.**

**-** Mở thêm terminal và sử dụng lệnh: nmap -sn 10.0.2.0/24

A screenshot of a computer

AI-generated content may be incorrect.

- Phân tích lưu lượng:

Nguồn phát là máy do thám (PCSSystemec\_04:42), gửi các gói ARP broadcast để xác định IP trong dải 10.0.2.0/24.

A screenshot of a computer

AI-generated content may be incorrect.

- lọc theo arp.opcode == 2:

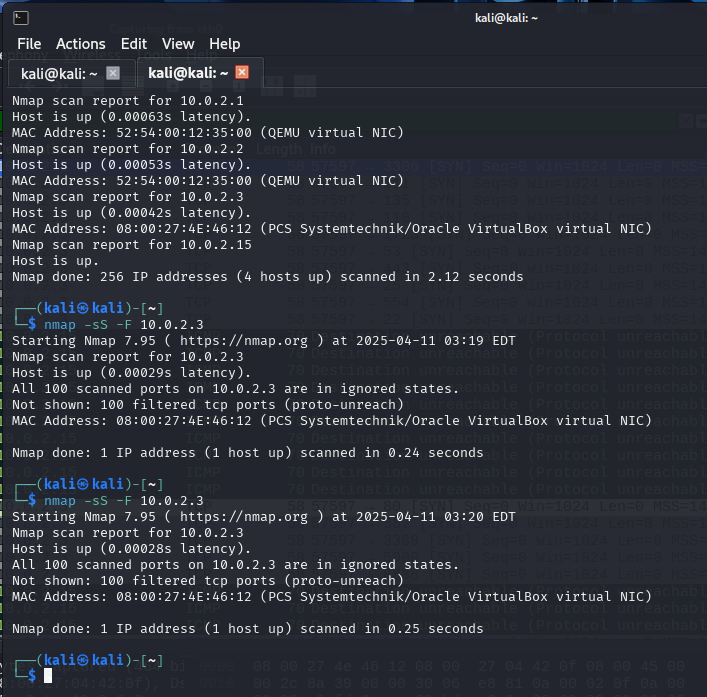
A screenshot of a computer

AI-generated content may be incorrect.

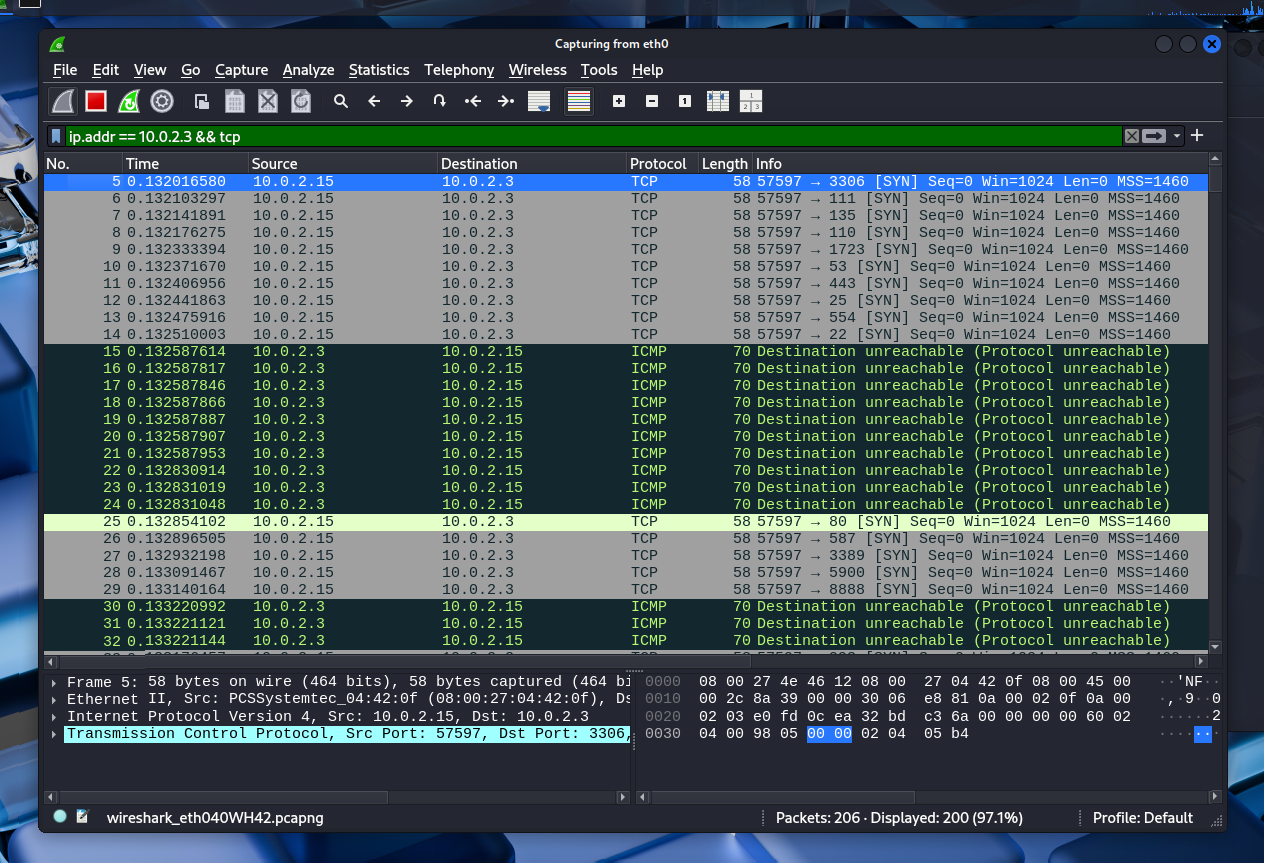
**-** Kết quả cho thấy kỹ thuật quét được sử dụng là ARP Scan. Wireshark cho thấy hàng loạt gói ARP request từ máy do thám đến toàn bộ dải mạng 10.0.2.0/24 và các ARP reply từ các máy đang hoạt động.

**Kịch bản 2:**

**-** Thực hiện lệnh nmap -sS -F 10.0.2.3

****

**-** Kiểm tra gói tin trên Wireshark và lọc theo ip.addr==10.0.2.3 && tcp:



- Tất cả là các gói SYN gửi đến nhiều cổng khác nhau (23, 111, 135, 139, 443, ...) và kỹ thuật quét là: TCP SYN Scan.

**Kịch bản 3:**

**-** Thực hiện lệnh: nmap -sA -F 10.0.2.3

**A screenshot of a computer

AI-generated content may be incorrect.**

**-** Kiểm tra các gói tin trên wireshark và lọc theo ip.addr == 10.0.2.3 && tcp

A screenshot of a computer

AI-generated content may be incorrect.

- Nhiều gói TCP ACK từ máy do thám 10.0.2.15 đến 10.0.2.3. Và phản hồi ICMPtừ 10.0.2.3. Đây là kỹ thuật được sử dụng là: TCP ACK Scan

**Câu 2. Thu thập thông tin hệ thống**

**-** Thực hiện lệnh: sudo nmap 192.168.100.0/24

**A screenshot of a computer

AI-generated content may be incorrect.**

**-** Kiểm tra các gói tin trên Wireshark và lọc theo tcp.port == 25 (email)

A screenshot of a computer

AI-generated content may be incorrect.

- Máy 10.0.2.15 đang quét toàn bộ dải mạng 192.168.100.0/24 để kiểm tra máy nào đang mở dịch vụ email (SMTP – cổng 25), máy 192.168.100.59 trong mạng 192.168.100.0/24 đang chạy dịch vụ email (SMTP) trên cổng 25.