BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

**Họ và tên sinh viên: Nguyễn Thị Anh Thư**

**MSSV: 1050080246**

***Yêu cầu kết quả thực hành:***

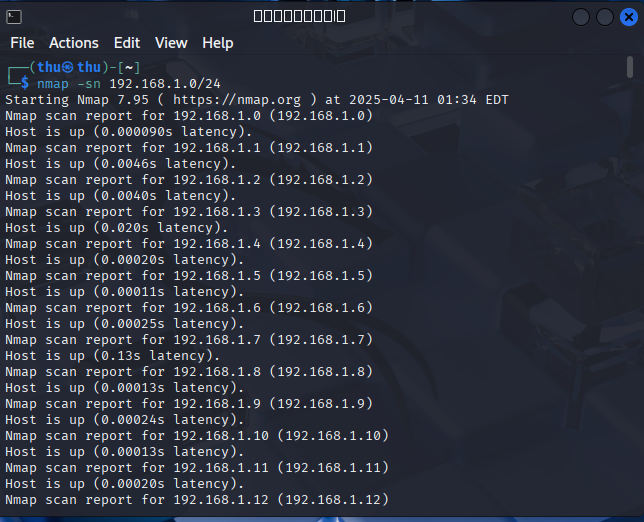
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

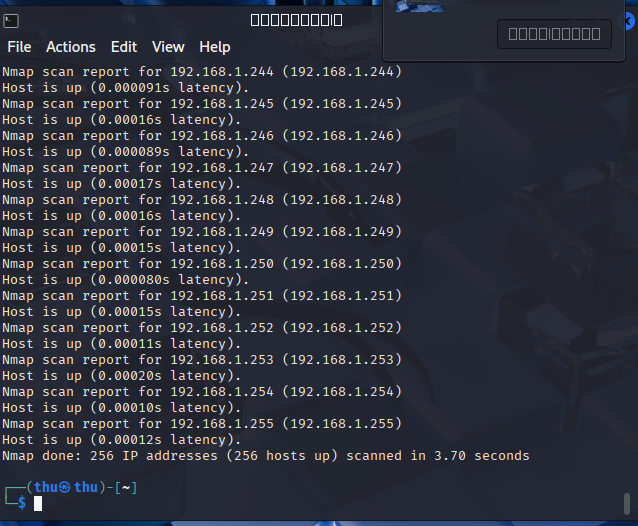
* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

**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





* 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

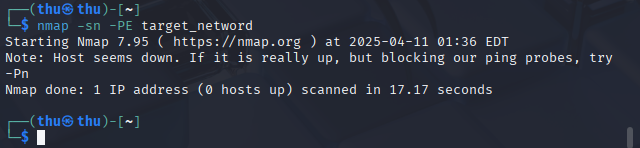
**Kỹ thuật này là kỹ thuật quét**

**ICMP Ping Scan:**

+ Nmap gửi lần lượt các gói tin ICMP Echo Request tới tất cả các địa chỉ IP. Nếu

có gói tin ICMP Echo Reply trả lại có địa chỉ nguồn là một địa chỉ IP nào đó, chứng tỏ có nút

mạng sử dụng địa chỉ IP đó đang hoạt động

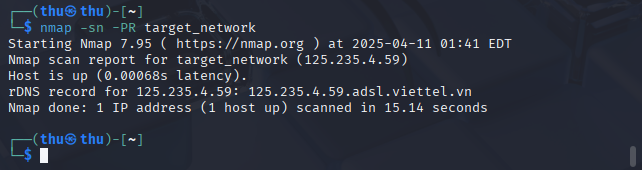


**ARP Ping Scan:**

- Nmap gửi quảng bá lần lượt các gói tin ARP Request để tìm kiếm thông tin địa

chỉ MAC của tất cả các địa chỉ IP. Nếu có gói tin ARP Response trả lại cho biết thông tin địa chỉ

MAC của một nút nào đó, chứng tỏ nút đó đang hoạt động



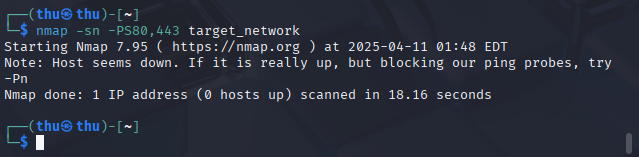
**TCP SYN Ping:**

- Nmap gửi lần lượt các gói tin TCP SYN tới cổng 80 và 443 của tất cả các địa chỉ

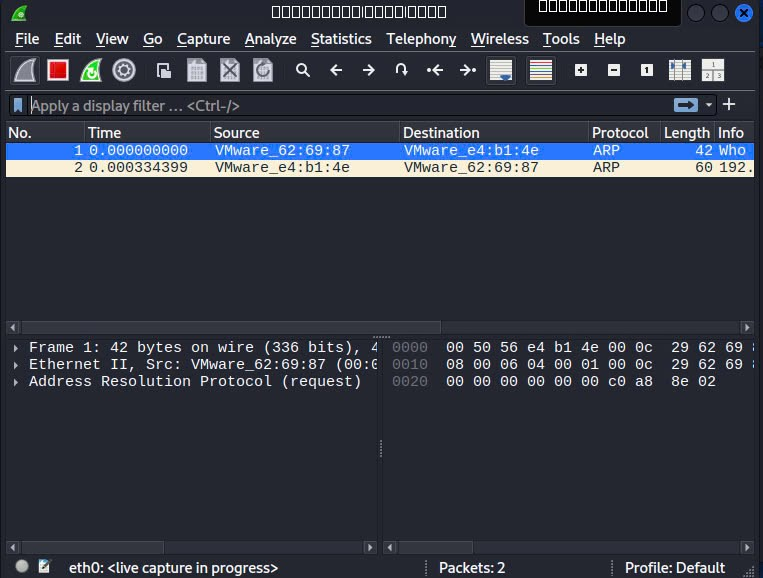
IP trong mạng cần quét. Nếu có gói tin TCP ACK hoặc TCP RST trả về từ một địa chỉ IP nào đó,

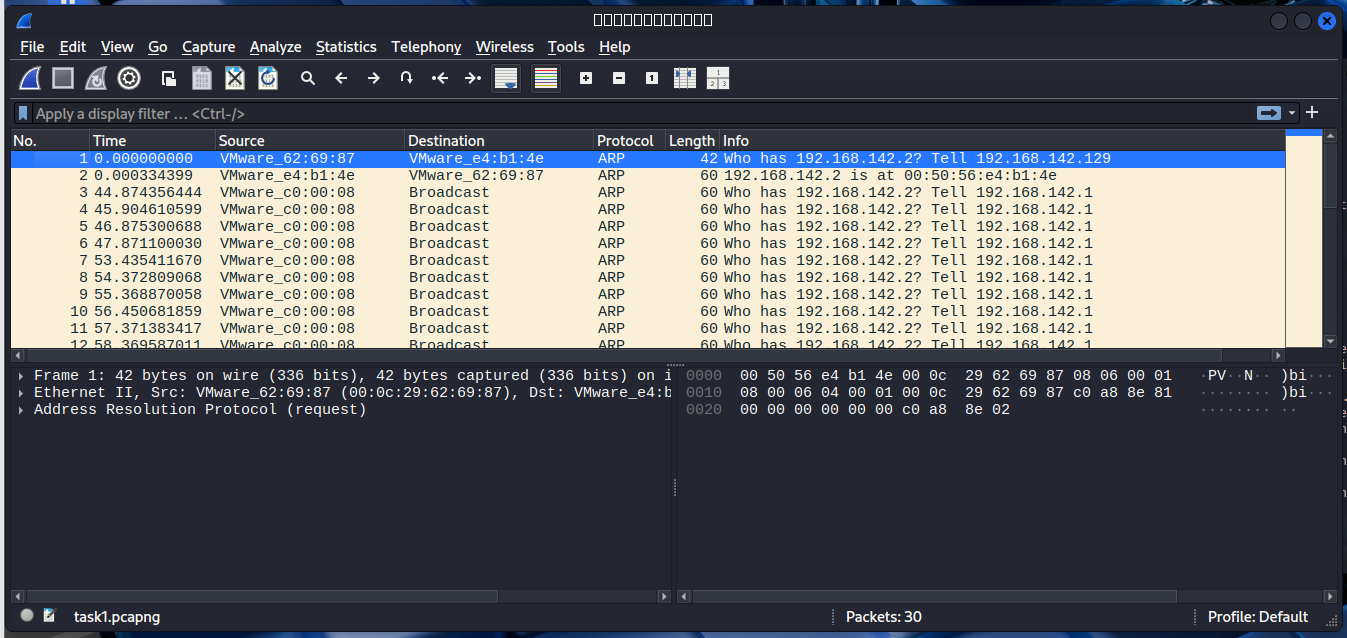
chứng tỏ có nút mạng sử dụng địa chỉ IP đó đang hoạt động. Kỹ thuật này được sử dụng khi

quét mạng mục tiêu là mạng ở xa, mà nút mạng thực thi Nmap không nằm trong mạng đó.

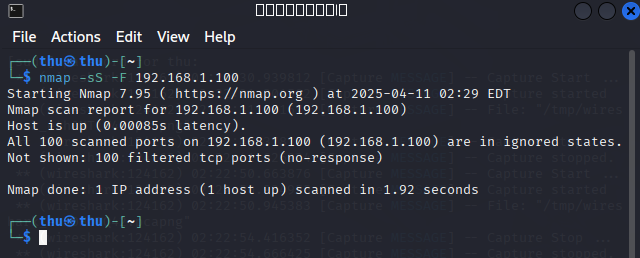


Bắt gói tin trên Wireshark





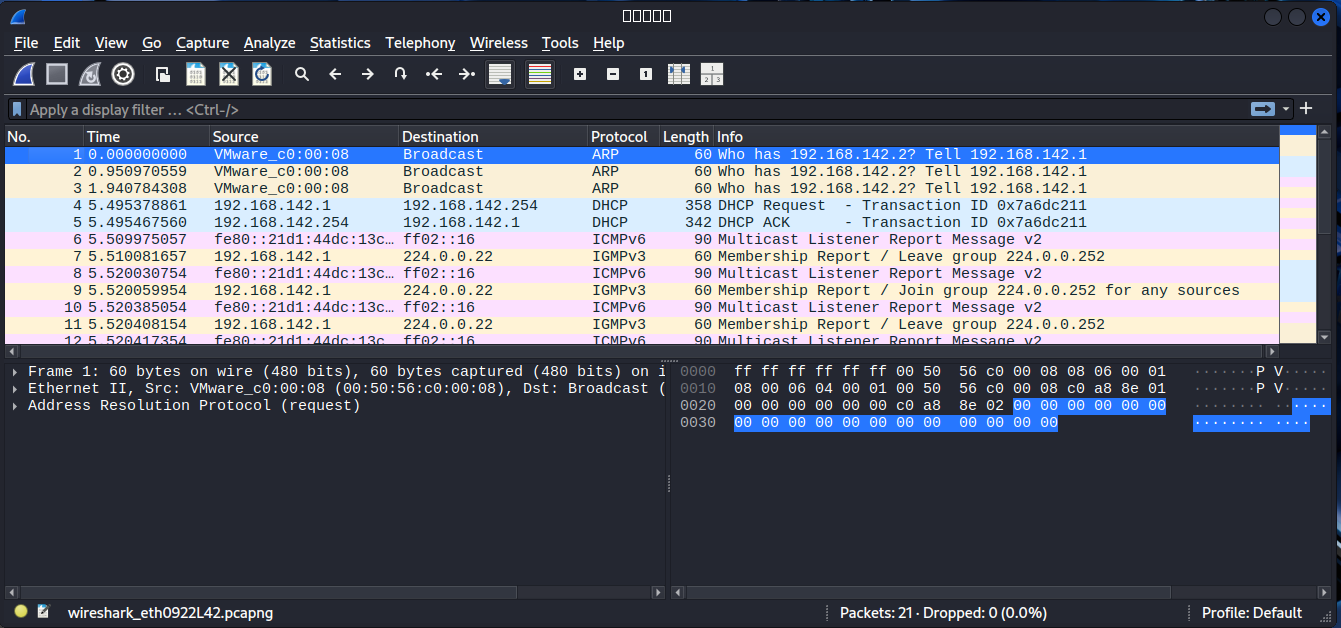
* 1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap

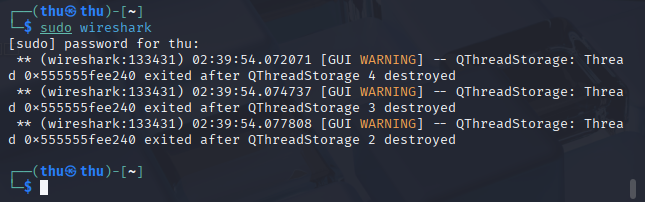


* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng

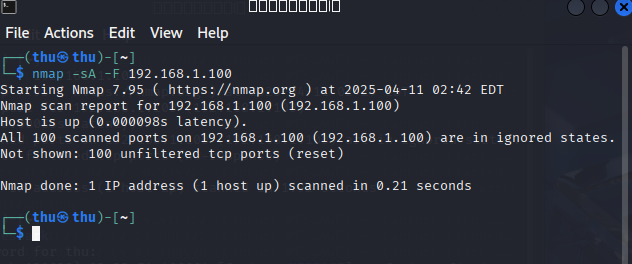
Kỹ thuật quét:

-sS: Sử dụng TCP SYN Scan. nmap gửi gói tin TCP SYN tới các cổng. Nếu nhận được TCP SYN/ACK, cổng mở (Open). Nếu nhận TCP RST, cổng đóng (Closed).





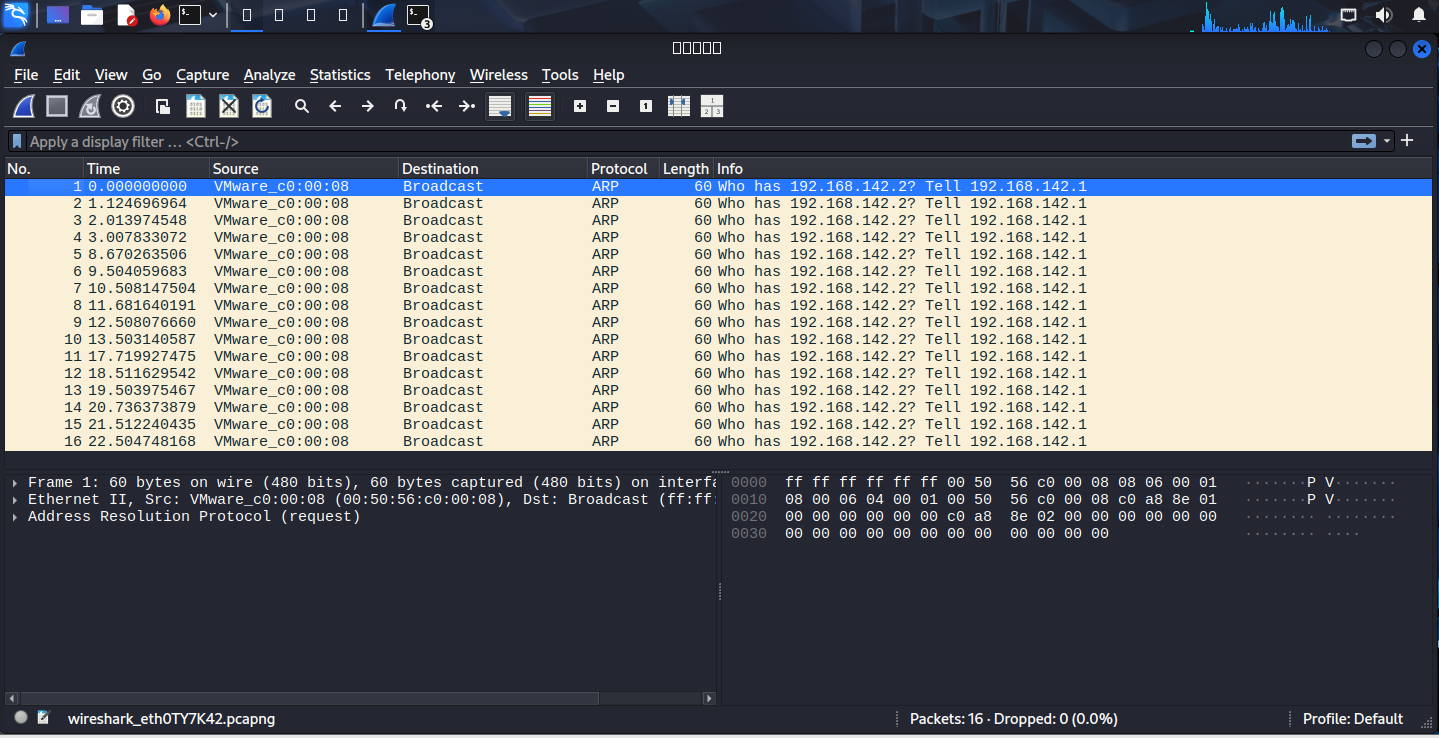
* 1. **Kịch bản 3**
* Ảnh chụp kết quả thực hiện của nmap

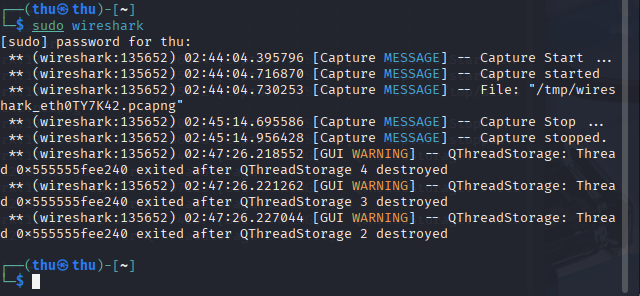


* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng

Kỹ thuật quét:

-sA: Sử dụng TCP ACK Scan. nmap gửi gói tin TCP ACK tới các cổng. Nếu nhận được TCP RST, cổng không bị lọc (unfiltered), cho thấy có thể có firewall. Kỹ thuật này không xác định cổng mở hay đóng, mà chủ yếu để phát hiện firewall.





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?

Bước 1: Xác định nút mạng cung cấp dịch vụ email

Dịch vụ email thường chạy trên các cổng:

SMTP: Cổng 25 (hoặc 587 cho SMTPS).

IMAP: Cổng 143 (hoặc 993 cho IMAPS).

POP3: Cổng 110 (hoặc 995 cho POP3S).

Sử dụng nmap để quét mạng và tìm các cổng liên quan đến email:

**Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap
* Nêu tên và phiên bản hệ điều hành

**Thông tin dịch vụ**

* Hình ảnh chụp kết quả của nmap
* Danh sách dịch vụ

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

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