BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Nguyễn Khánh Duy***

***MSSV: 1050080173***

***Yêu cầu kết quả thực hành:***

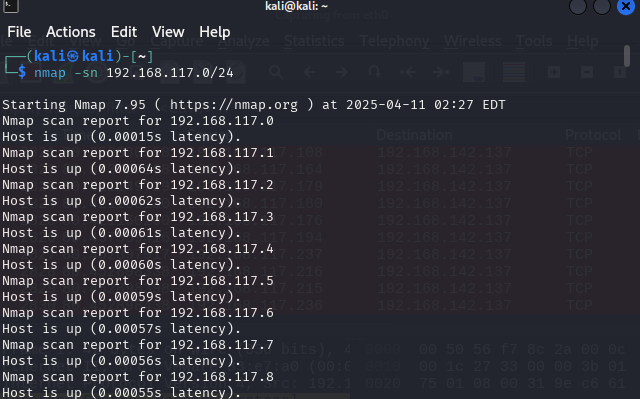
Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

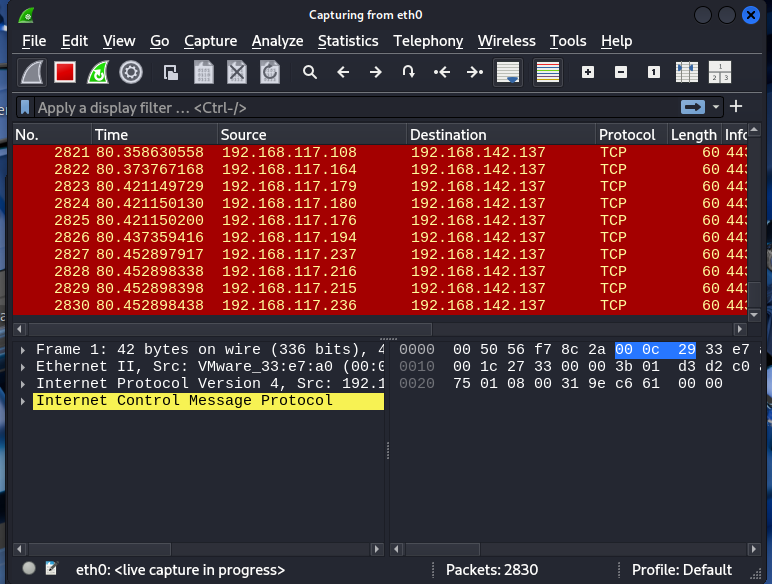
* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

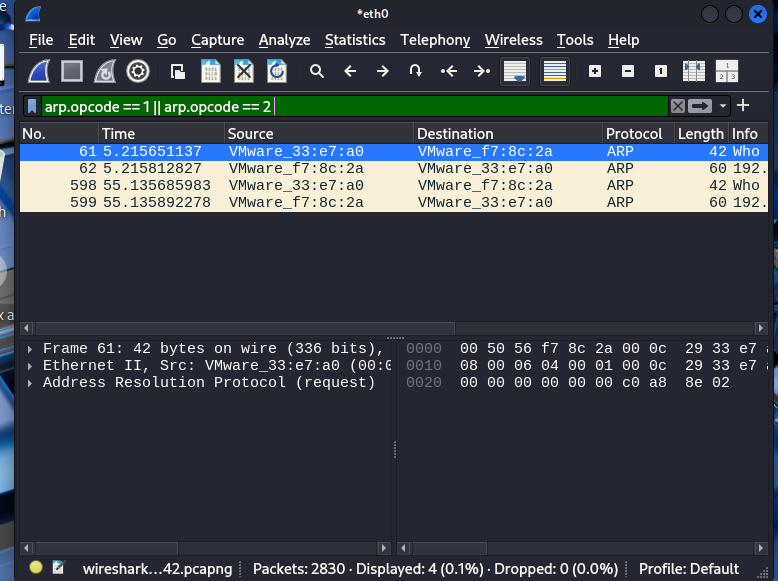
**KẾT QUẢ THỰC HÀNH**

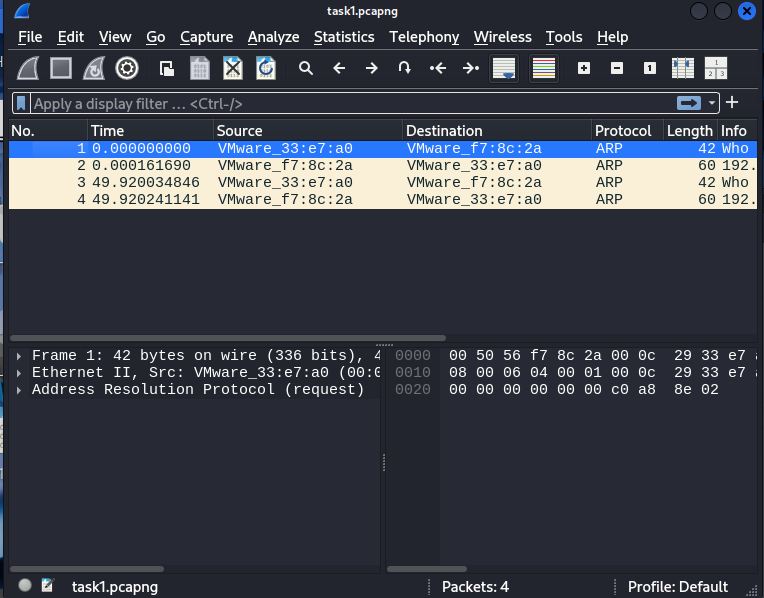
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

* 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

|  |  |  |
| --- | --- | --- |
| **Đặc điểm** | **Giải thích** | **Ví dụ hiển thị trên Wireshark** |
| Gửi nhiều gói ARP Request liên tục | Máy tấn công gửi gói ARP để hỏi “ai đang sở hữu IP này?” → thu thập danh sách IP đang hoạt động | Who has 192.168.117.X? Tell 192.168.117.1 |
| Không có lưu lượng TCP/UDP đi kèm | Chỉ dùng ARP (Layer 2) để dò IP đang online, không cần kết nối | Gói tin chỉ có Protocol: ARP, không có TCP |
| Hồi đáp là ARP Reply | Máy nạn nhân trả lời “Tôi là IP đó, MAC của tôi là...” → máy quét thu thập thông tin MAC/IP | 192.168.117.X is at 08:00:27:XX:XX:XX |
| **Từ đó kết luận:** Đây là kỹ thuật quét lớp 2 (Layer 2 scanning), thường dùng trong mạng nội bộ để tìm các máy đang hoạt động → chính là kỹ thuật do thám hệ thống (reconnaissance). | | |

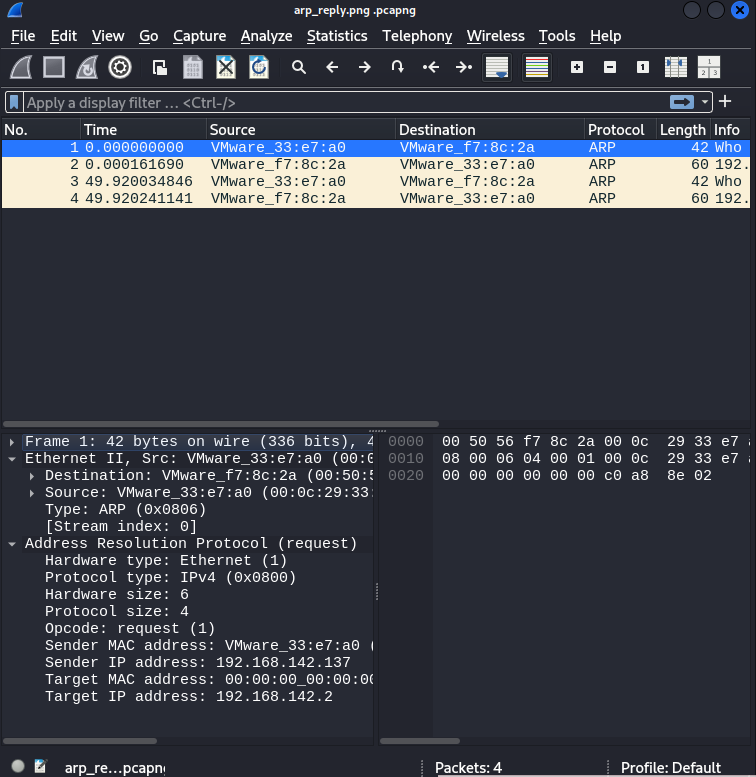
**Ảnh 1: Gói ARP Reply**

File: arp\_reply.png

Thể hiện gói phản hồi ARP từ máy đích.

Dòng "192.168.142.2 is at 00:50:56:f7:8c:2a"

Có phần Ethernet II và ARP Reply bên dưới.

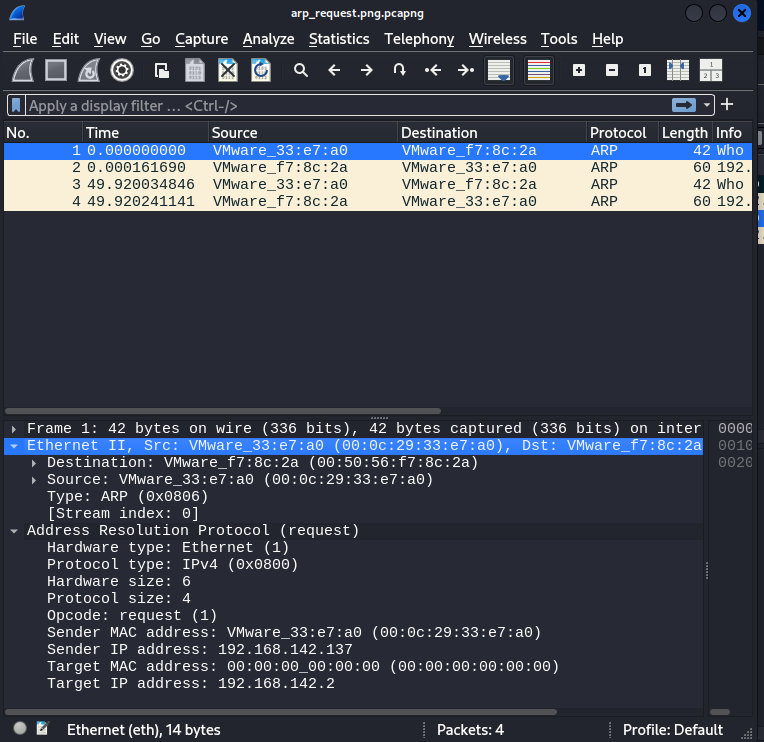


**Ảnh 2: Gói ARP Request**

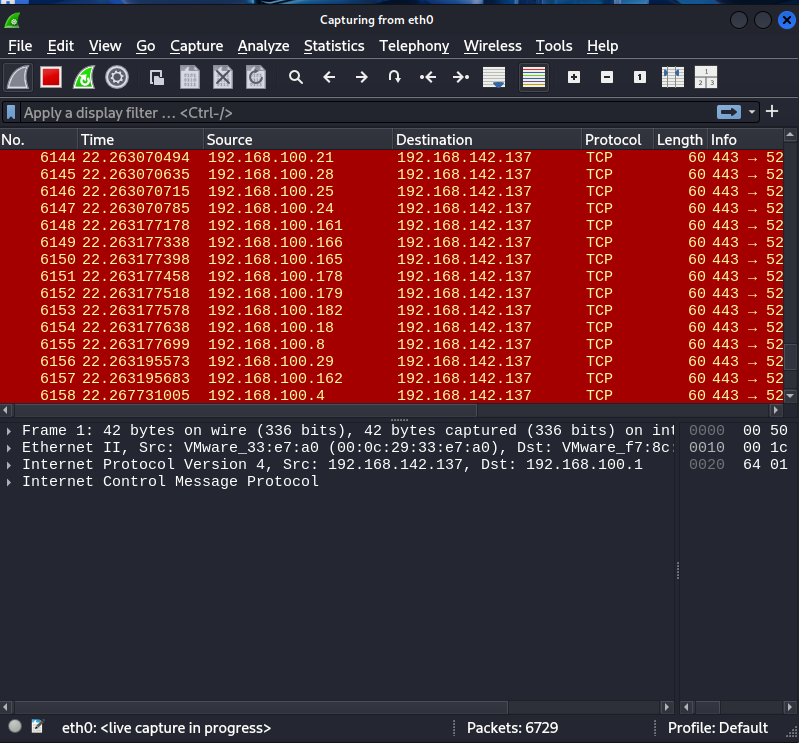
File: arp\_request.png

Thể hiện rõ thông tin:

Gói ARP Request với dòng "Who has 192.168.142.2? Tell 192.168.142.137"

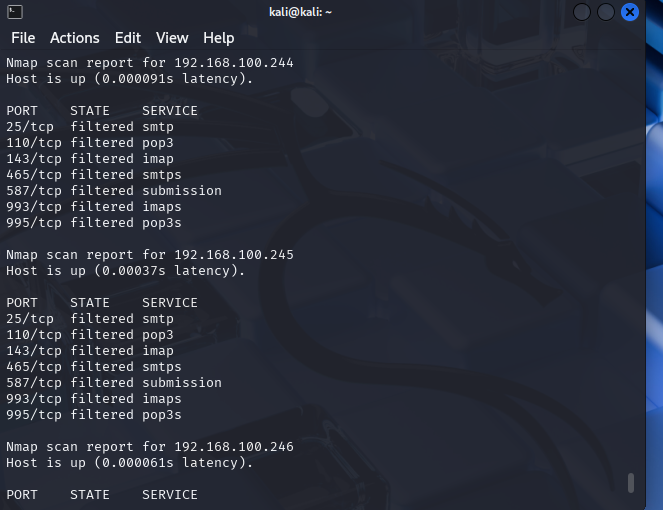


* 1. **Kịch bản 2**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

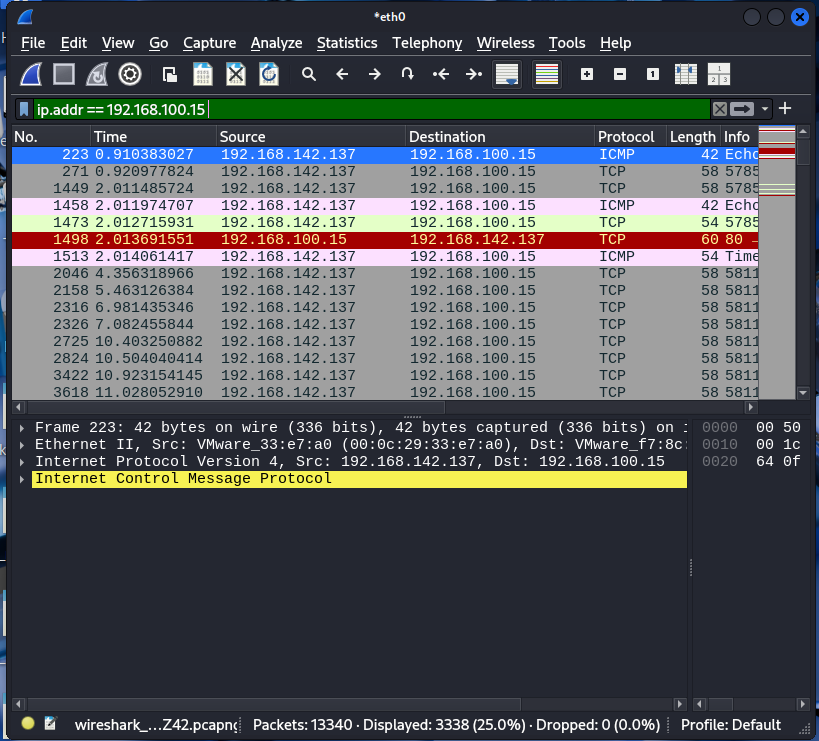


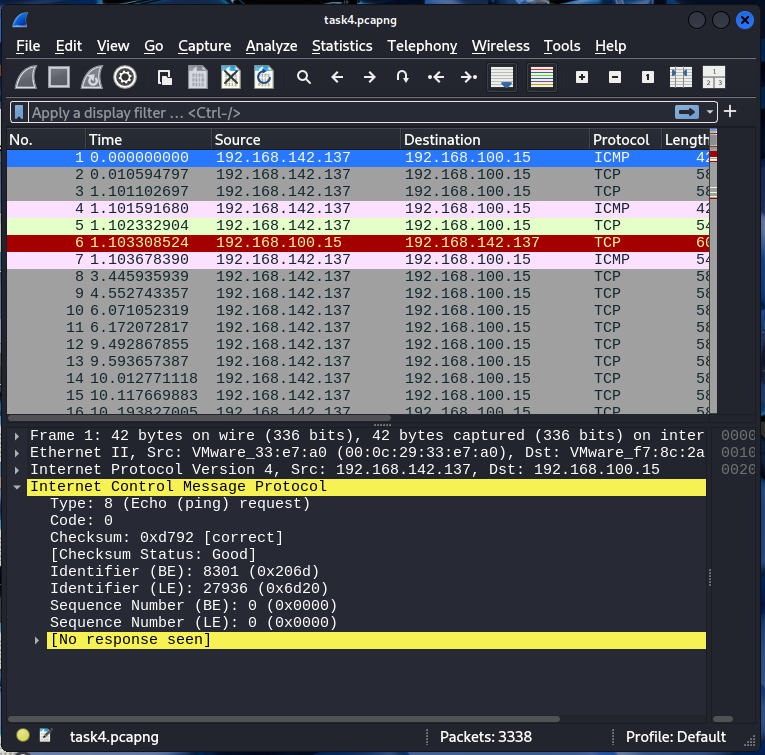
sudo nmap -p 25,465,587,110,995,143,993 192.168.100.0/24

sudo nmap -A 192.168.100.15



ip.addr == 192.168.100.15





* 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** | **Đặc điểm** | **Gói tin quan sát được** |
| TCP Connect Scan | Hoàn tất bắt tay 3 bước (3-way handshake: SYN → SYN-ACK → ACK) | Gói TCP SYN, sau đó là SYN-ACK, rồi ACK |
| TCP SYN Scan | Gửi SYN, nếu nhận SYN-ACK, attacker không gửi ACK mà gửi RST để tránh bị phát hiện | Gói SYN → SYN-ACK → RST |
| UDP Scan | Gửi gói UDP, nếu không có phản hồi hoặc nhận ICMP Port Unreachable thì port đóng | Gói UDP + ICMP |
| ICMP Echo Scan (ping sweep) | Gửi ICMP Echo Request (ping) đến nhiều IP | Gói ICMP (Echo Request / Reply) |

**Kỹ thuật quét: ICMP Echo Scan (Ping Sweep)**  
Đặc điểm lưu lượng: Gói ICMP Echo Request (Type 8) được gửi từ 192.168.142.137 đến 192.168.100.15. Trong phần chi tiết gói tin cho thấy "No response seen", nghĩa là không có phản hồi Echo Reply. Điều này chứng tỏ đây là một kỹ thuật ICMP Scan nhằm kiểm tra xem máy đích có đang hoạt động hay không.

**Gói số 1:**

Source: 192.168.142.137 (máy quét)

Destination: 192.168.100.15 (máy bị quét)

Protocol: ICMP

Type: 8 (Echo Request – yêu cầu ping)

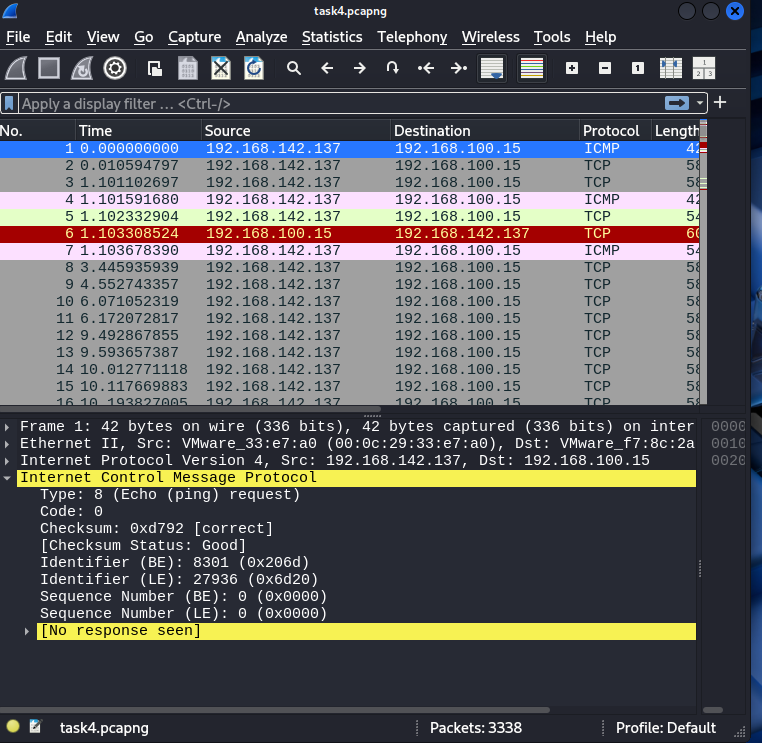
Thông tin bổ sung: [No response seen] → không có phản hồi (máy kia có thể tắt ping, firewall chặn, hoặc đang hoạt động bất thường).

**Đặc điểm kỹ thuật quét ICMP Echo Scan:**

ICMP Echo Request được gửi đi để xác định máy nào đang hoạt động (online).

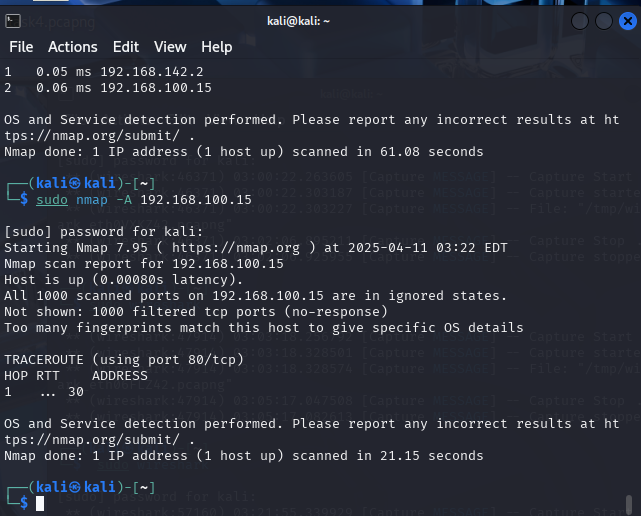
Kỹ thuật này không kiểm tra cổng dịch vụ cụ thể mà chỉ kiểm tra xem hệ thống có phản hồi không.

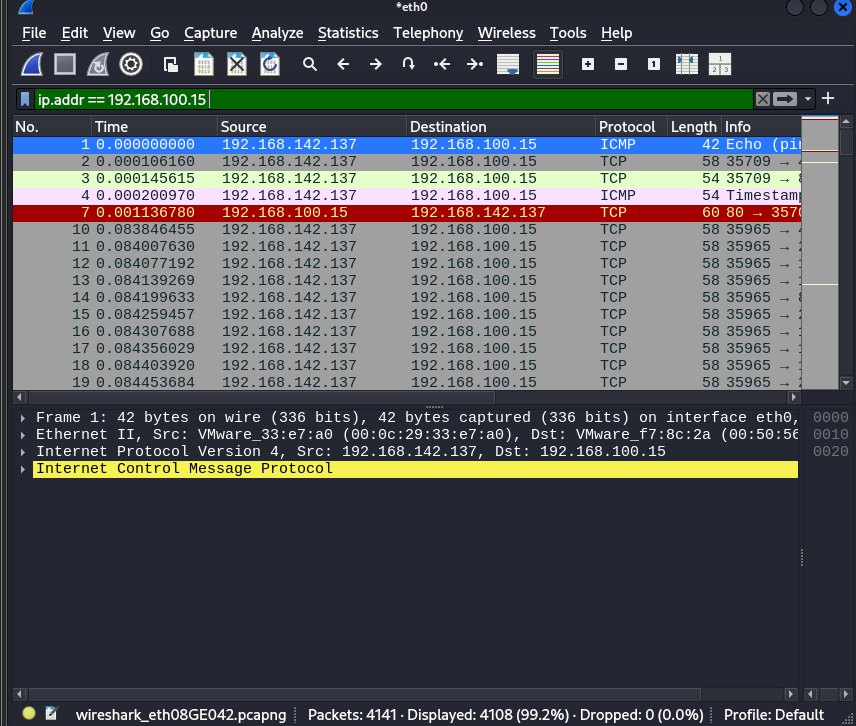
Đây là bước phổ biến để xác định mục tiêu tiềm năng trước khi quét cổng TCP/UDP.

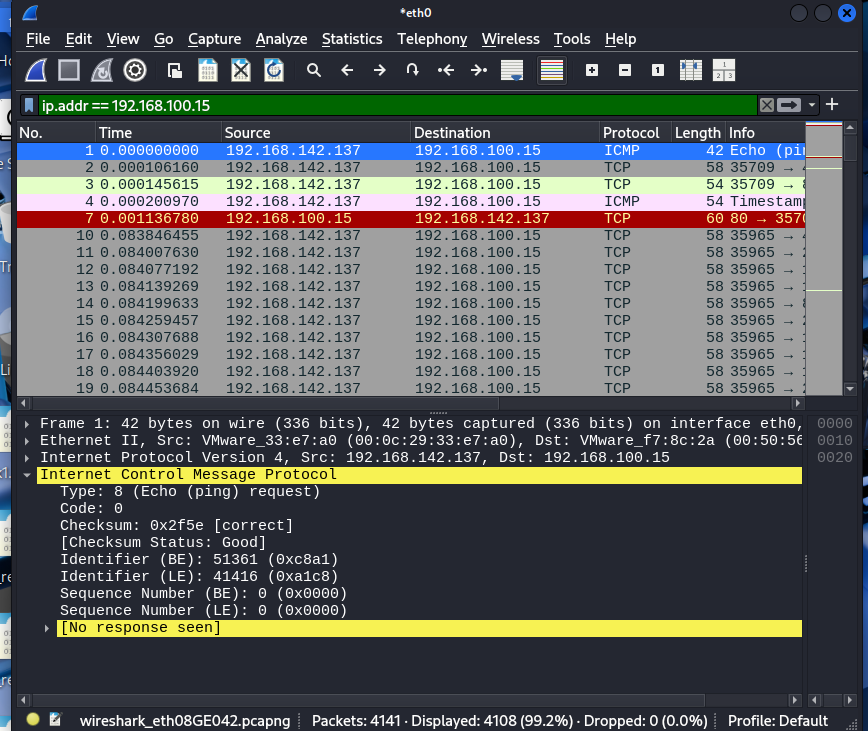


* 1. **Kịch bản 3**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

sudo nmap -A 192.168.100.15







**Kỹ thuật 1: ICMP Echo Scan**

Gói ICMP với Type 8 (Echo Request) từ máy 192.168.142.137 đến 192.168.100.15

Không có phản hồi → máy có thể không trả lời ping

→ Đây là kỹ thuật Ping Sweep để kiểm tra host có hoạt động không

**Kỹ thuật 2: TCP SYN Scan**

Gói TCP SYN gửi tới nhiều cổng của máy 192.168.100.15

Có phản hồi SYN-ACK thì lập tức gửi RST → không hoàn tất kết nối

→ Đây là kỹ thuật TCP SYN Scan (Stealth Scan)

1. **Thu thập thông tin hệ thống**

sudo nmap -A 192.168.100.15

Lệnh này giúp:

Xác định hệ điều hành

Liệt kê các cổng mở

Tên dịch vụ và phiên bản phần mềm tương ứng

sudo nmap -p 25,110,143,465,587,993,995 --script=banner 192.168.100.15

Lệnh này quét các cổng liên quan đến email như:

SMTP: 25, 465, 587

POP3: 110, 995

IMAP: 143, 993  
Và dùng --script=banner để hiển thị thông tin banner (tên phần mềm và phiên bản).

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