BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

***Họ và tên sinh viên: Nguyễn Xuân Tiến Dũng***

***MSSV: 0850080012***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng HoTenSV\_MSSV\_Lab01.zip

* 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.

**Mục lục**

[1. Kịch bản 1 1](#_Toc133442662)

[1.1. Bước thực hiện và kết quả: 1](#_Toc133442663)

[1.2. Phân tích: 3](#_Toc133442664)

[2. Kịch bản 2 3](#_Toc133442665)

[2.1. Các bước thực hiện và kết quả: 3](#_Toc133442666)

[2.2. Phân tích: 5](#_Toc133442667)

[3. Kịch bản 3 6](#_Toc133442668)

[3.1. Các bước thực hiện: 6](#_Toc133442669)

[3.2. Phân tích: 7](#_Toc133442670)

[4. Thu thập thông tin hệ thống 8](#_Toc133442671)

[4.1. Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này? 8](#_Toc133442672)

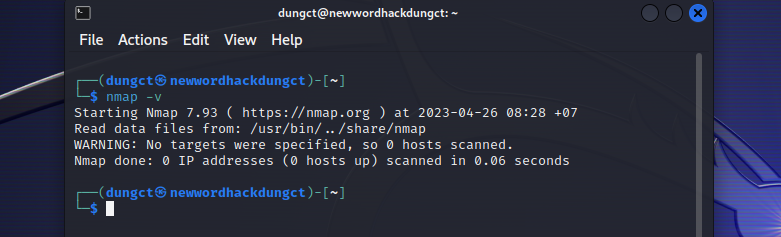
[4.2. Thông tin hệ điều hành: 9](#_Toc133442673)

[5. Tìm kiếm thông tin về các lỗ hổng 10](#_Toc133442674)

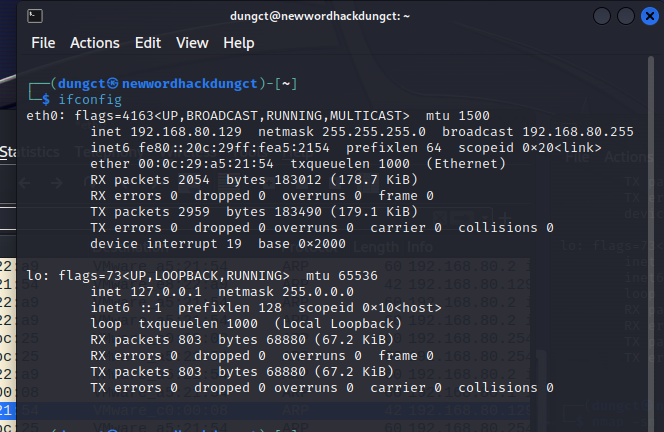
**KẾT QUẢ THỰC HÀNH**

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
2. Kịch bản 1
   1. Bước thực hiện và kết quả:

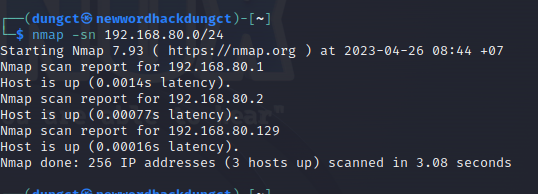
Bước 1: kiểm tra phiên bản version



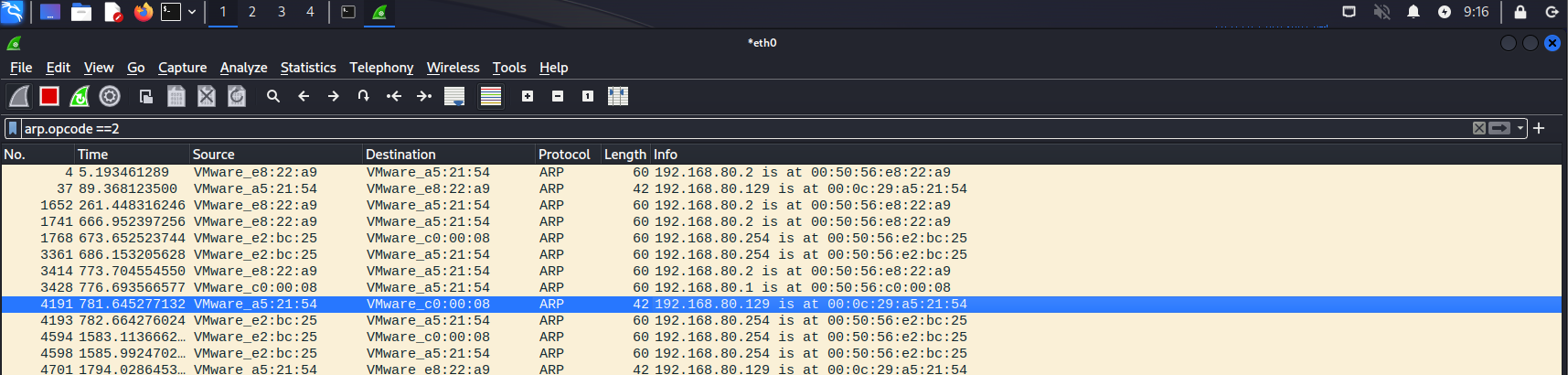
Bước 2: sử dụng lệnh nmap -sn với cổng mạng máy tính



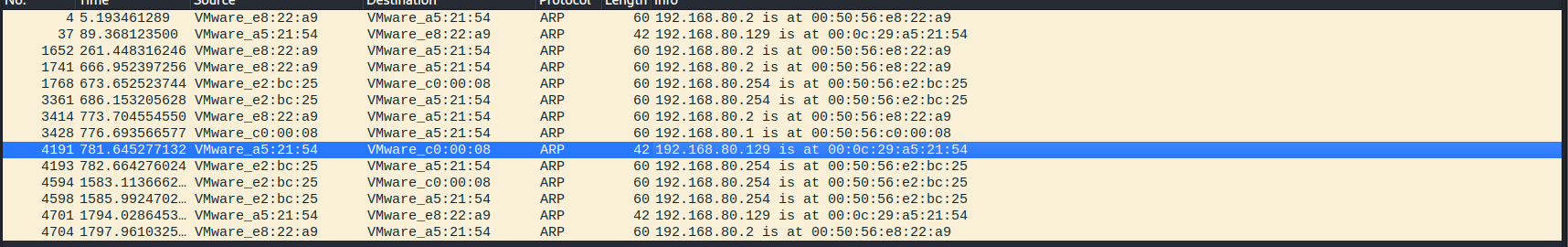
+ Cổng máy tính port:192.168.80.129



Mở wireshark và nhập lệnh: arp.opcode == 2



Kết quả sau khi kiểm tra wire shark





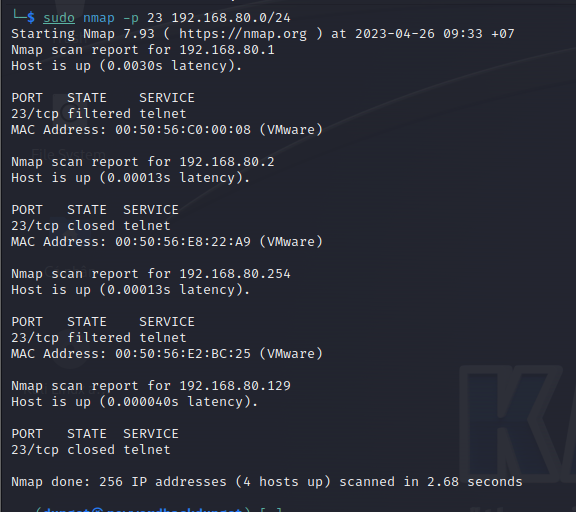
Địa chỉ cổng mạng phát hiện: 192.168.80.1,192.168.80.2,192.168.80.129

* 1. Phân tích:
* Là kĩ thuật ping scan host discovery" scan bằng Nmap. Kỹ thuật ping scan được sử dụng để xác định xem các máy chủ nào trong một mạng có sẵn hoặc đang hoạt động.
* địa chỉ IP 192.168.80.1 và thông báo rằng địa chỉ IP của chính nó là 192.168.80.0. Gói tin này được gửi trong mạng LAN để giải quyết địa chỉ vật lý của một địa chỉ IP. Khi máy có địa chỉ IP 192.168.80.1 nhận được yêu cầu này, nó sẽ trả lời với một gói tin ARP khác chứa địa chỉ MAC của nó.

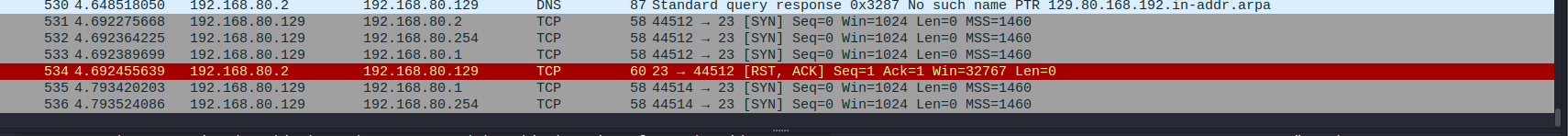
1. Kịch bản 2
   1. Các bước thực hiện và kết quả:

Bước 1: thực hiện quét cổng mạng với lệnh

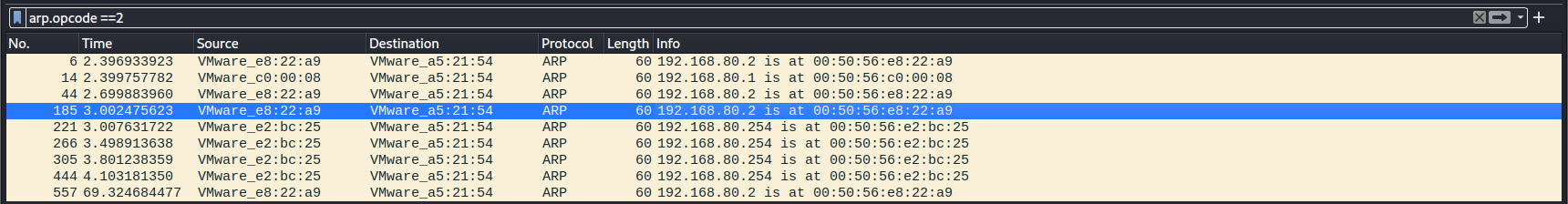
Sudo nmap -p 23 192.168.80.0/24

****

Kết quả thu được sau khi chạy lệnh trên bên wire shark:

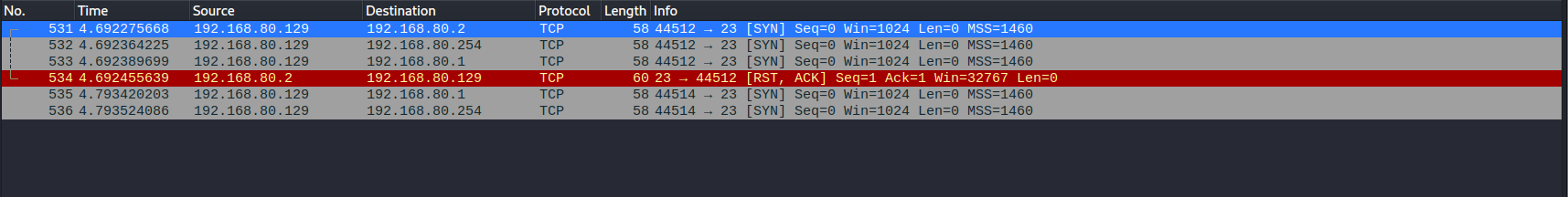


+ kiểm tra các gói tin TCP

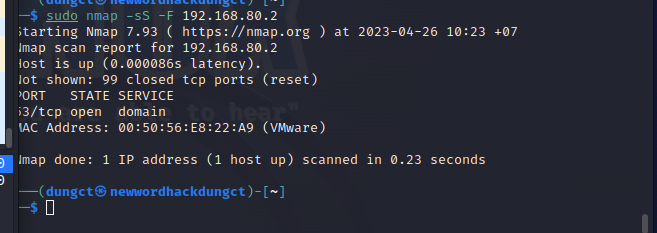


+ Kiểm tra các gói ARP: bằng lệnh arp.opcode==2

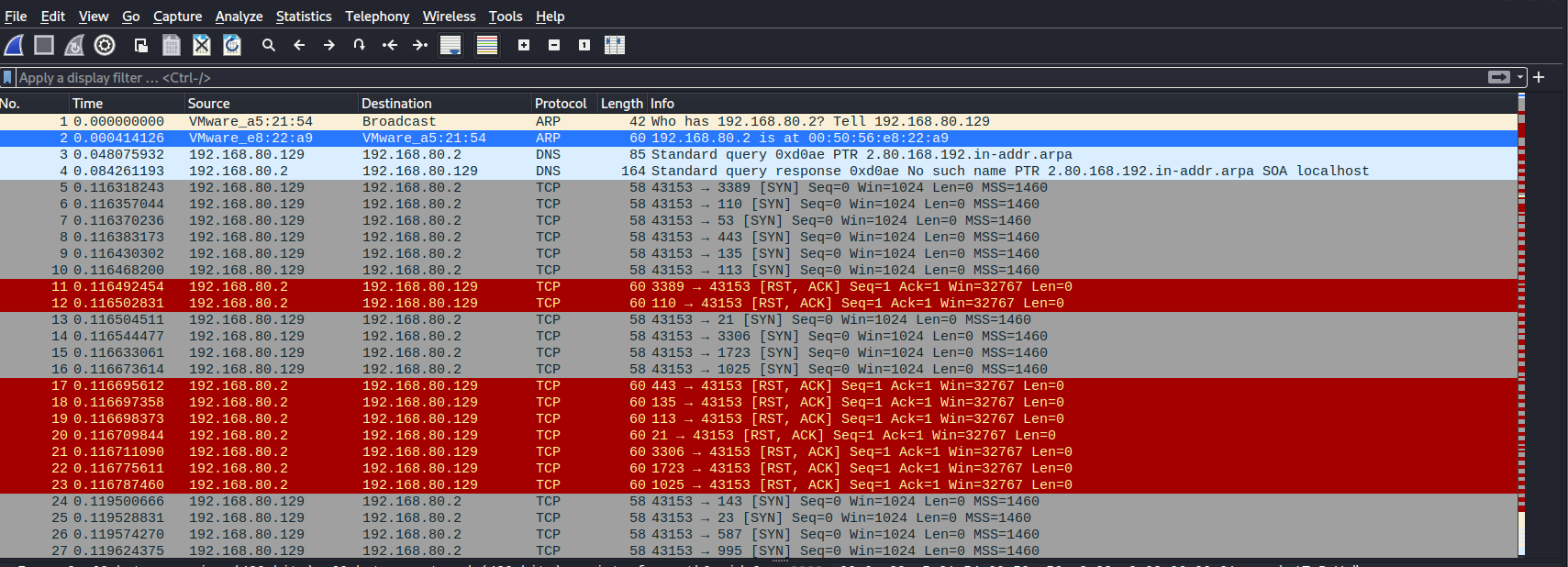
Bước 2: tìm kiếm các gói TCP trên wireshark

****

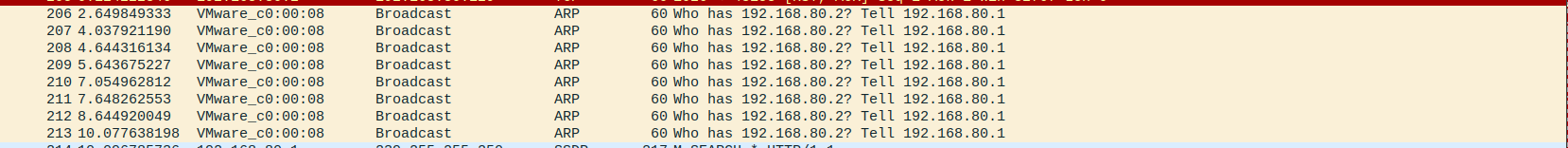
Bước 3: chạy lệnh quét cổng sudo nmap -sS -F 192.168.80.2



Bước 4: kiểm tra kết quả các gói TCP

****

+ Ta thấy được các gói TCP gửi đến cổng 192.168.80.2 từ nmap

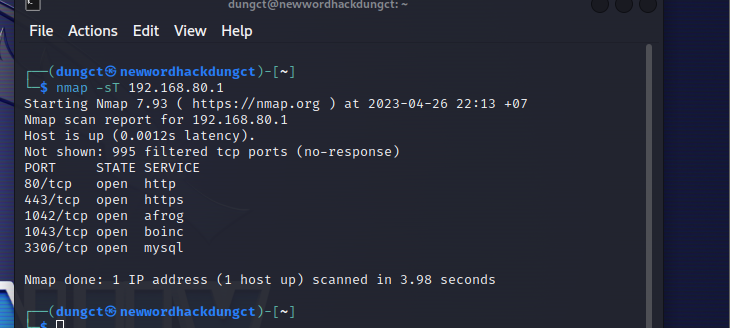


+ Ngoài ra chúng ta còn phát hiện các gói ARP

* 1. Phân tích:
* Lệnh "nmap -sS -F địa\_chỉ\_IP\_máy\_mục\_tiêu" là một lệnh quét cổng TCP được thực hiện bằng Nmap. Cụ thể:
* -sS: Tùy chọn để thực hiện một quét TCP SYN. Nó là một phương pháp quét cổng TCP nhanh chóng và ẩn danh, được sử dụng để tìm kiếm các cổng TCP mở trên một máy chủ.
* -F: Tùy chọn để chỉ quét các cổng TCP phổ biến nhất, bao gồm các cổng từ 1 đến 1.024.
* "địa\_chỉ\_IP\_máy\_mục\_tiêu": Là địa chỉ IP của máy tính mà bạn muốn quét cổng TCP.
* Do đó, lệnh "nmap -sS -F địa\_chỉ\_IP\_máy\_mục\_tiêu" sẽ thực hiện một quét TCP SYN trên các cổng phổ biến nhất trên địa chỉ IP được chỉ định. Nó sẽ tìm kiếm các cổng TCP mở trên máy tính đó và hiển thị kết quả quét trên màn hình terminal.
* + Sau khi chạy nmap gửi tới cổng 192.168.80.2 các gói TCP SYN/ACK phù hợp với cơ chế TCP SYN Scan: Nmap gửi lần lượt các gói tin TCP SYN tới các cổng cần quét. Nếu quá trình quét cổng nhận được bất kỳ gói tin TCP SYN/ACK trả lời từ một cổng nào đó, chứng tỏ cổng đó đang ở trạng thái Open.

1. Kịch bản 3
   1. Các bước thực hiện:

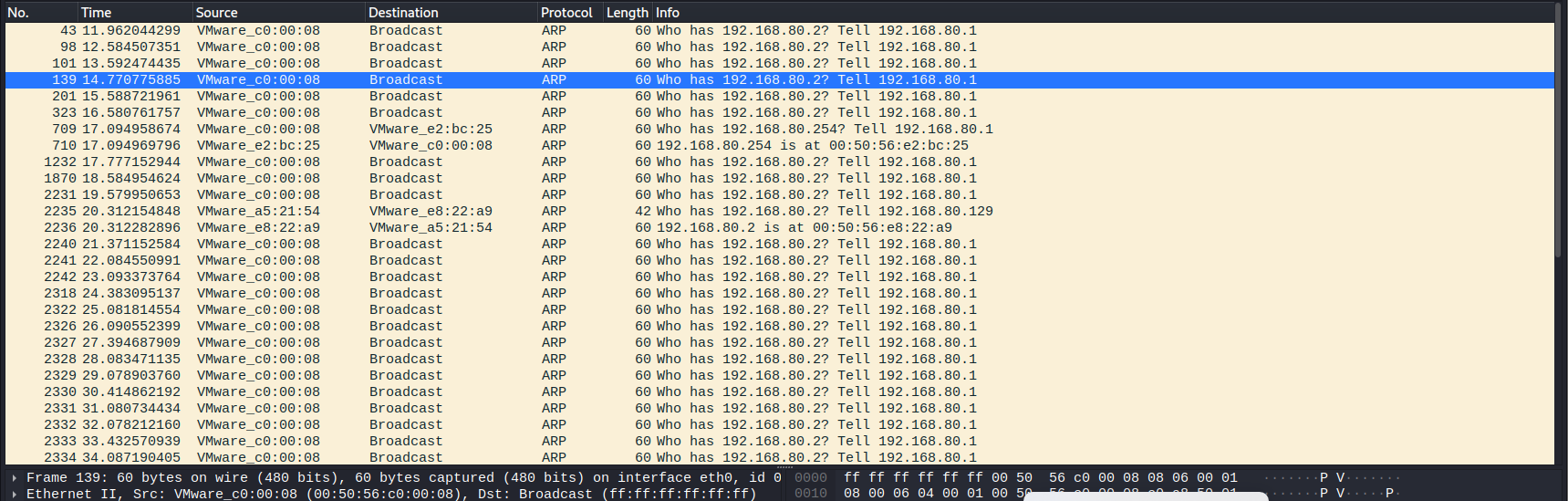
Bước 1: thực hiện chạy lệnh sudo nmap -St 192.168.80.1



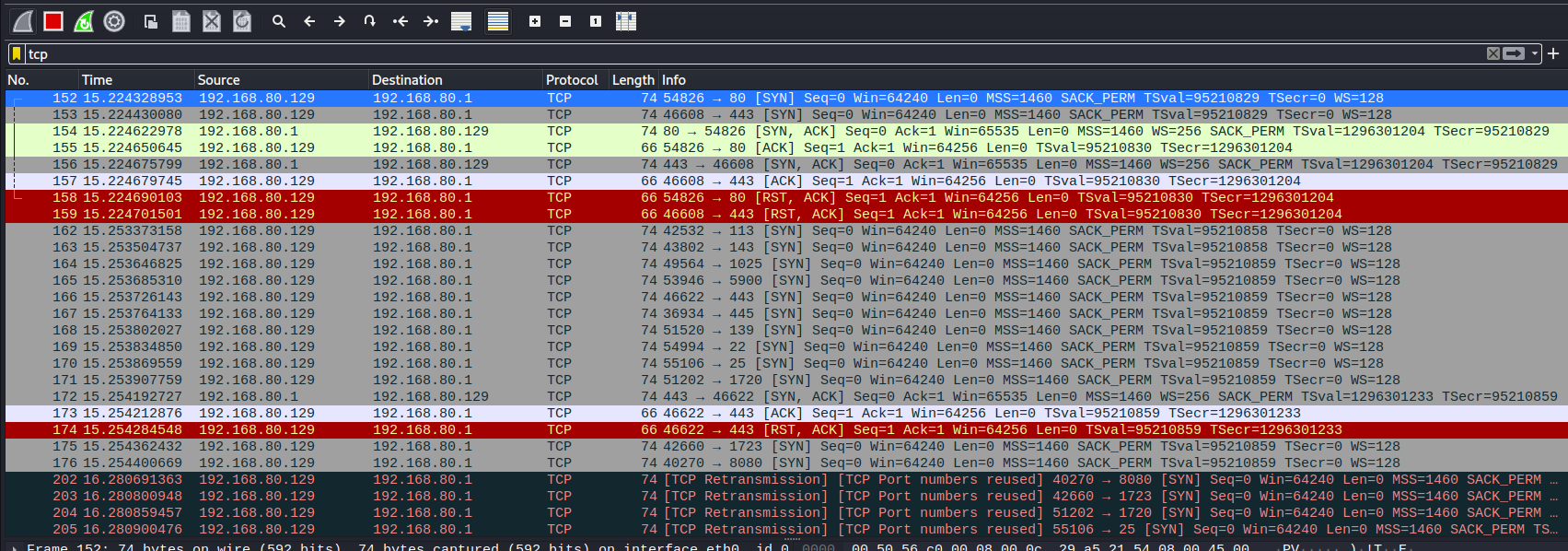
Bước 2: thực hiện kiểm tra các gói tin bằng wireshark

Máy tấn công 192.168.80.192 gửi tới 192.168.80.1

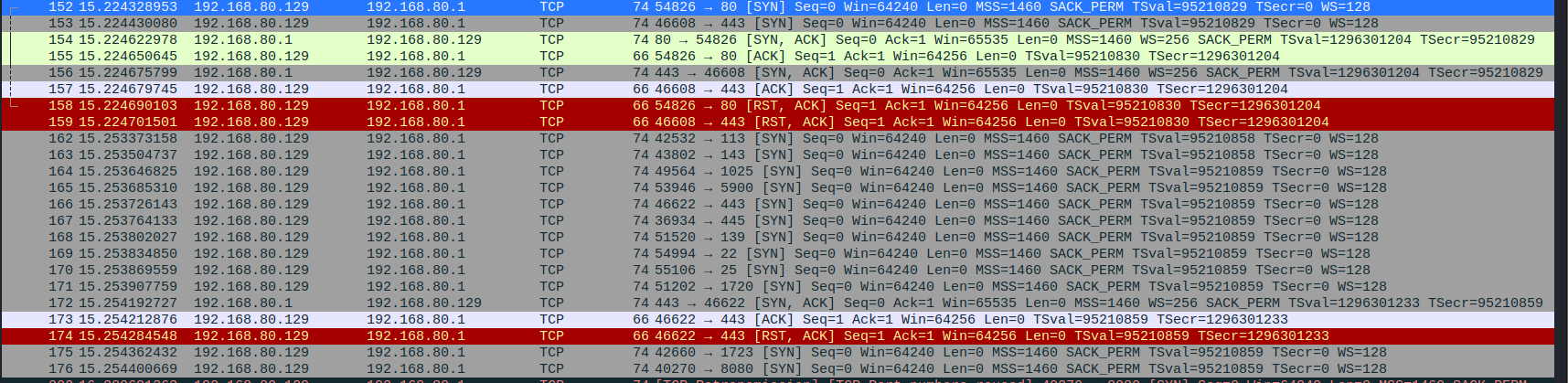
Các gói tin ARP Request:



Các gói tin TCP SYN:



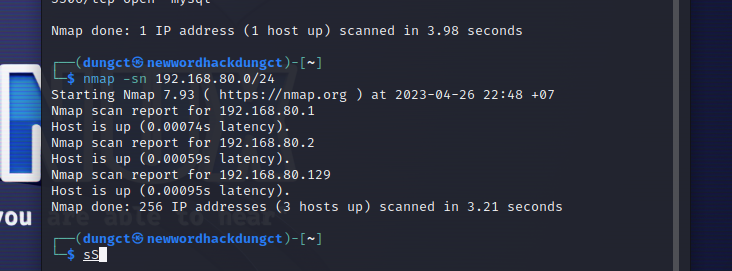
Bước 2: Sử dụng lệnh tcp && ip.addr == 192.168.80.1 trên Wireshark

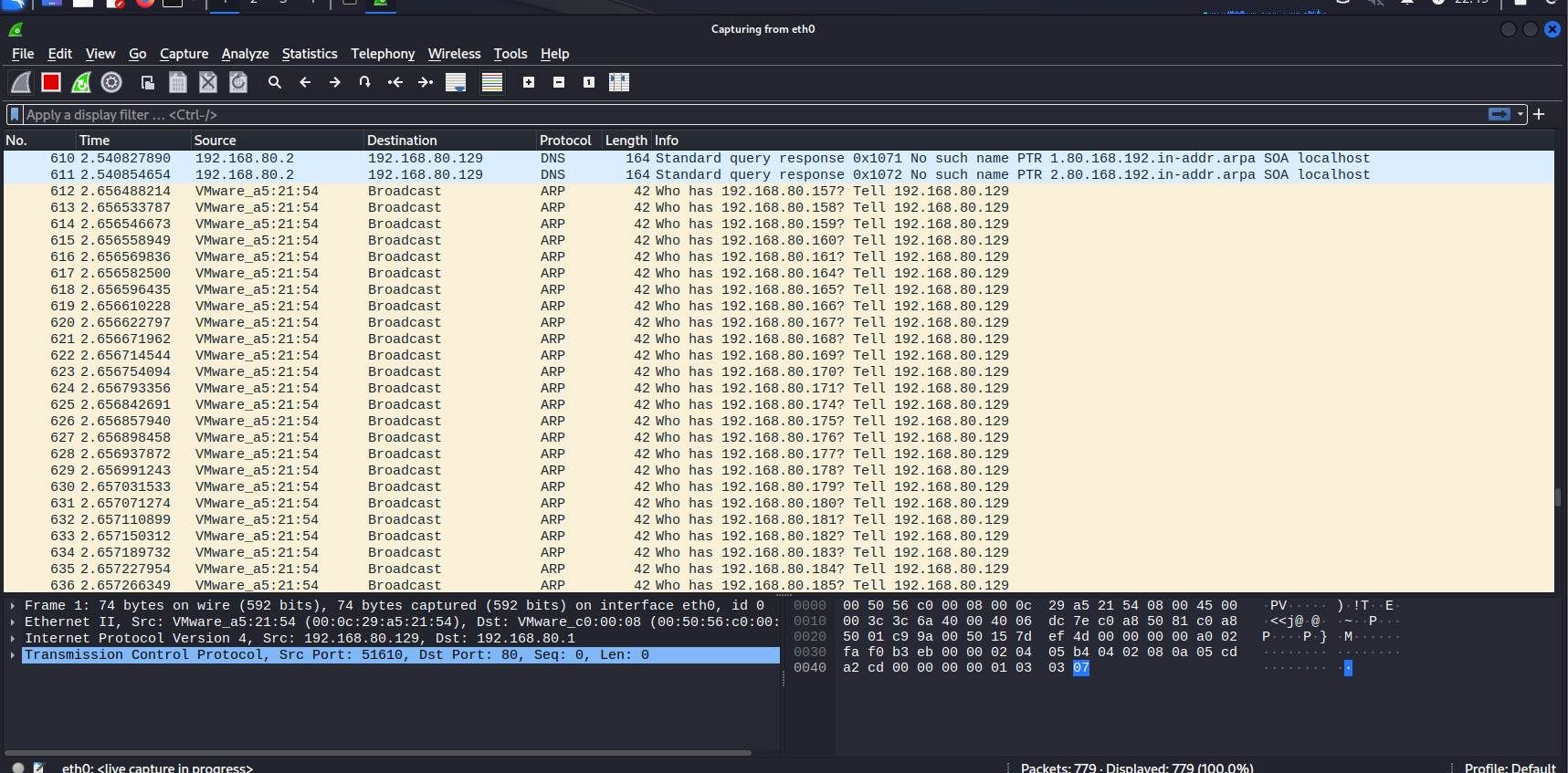


* 1. Phân tích:
* Sử dụng giá trị tcp && ip.addr == 192.168.117.1 ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 153 nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin 174) để hủy kết nối này.
* Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 158, 159. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan.

1. Thu thập thông tin hệ thống
   1. Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?

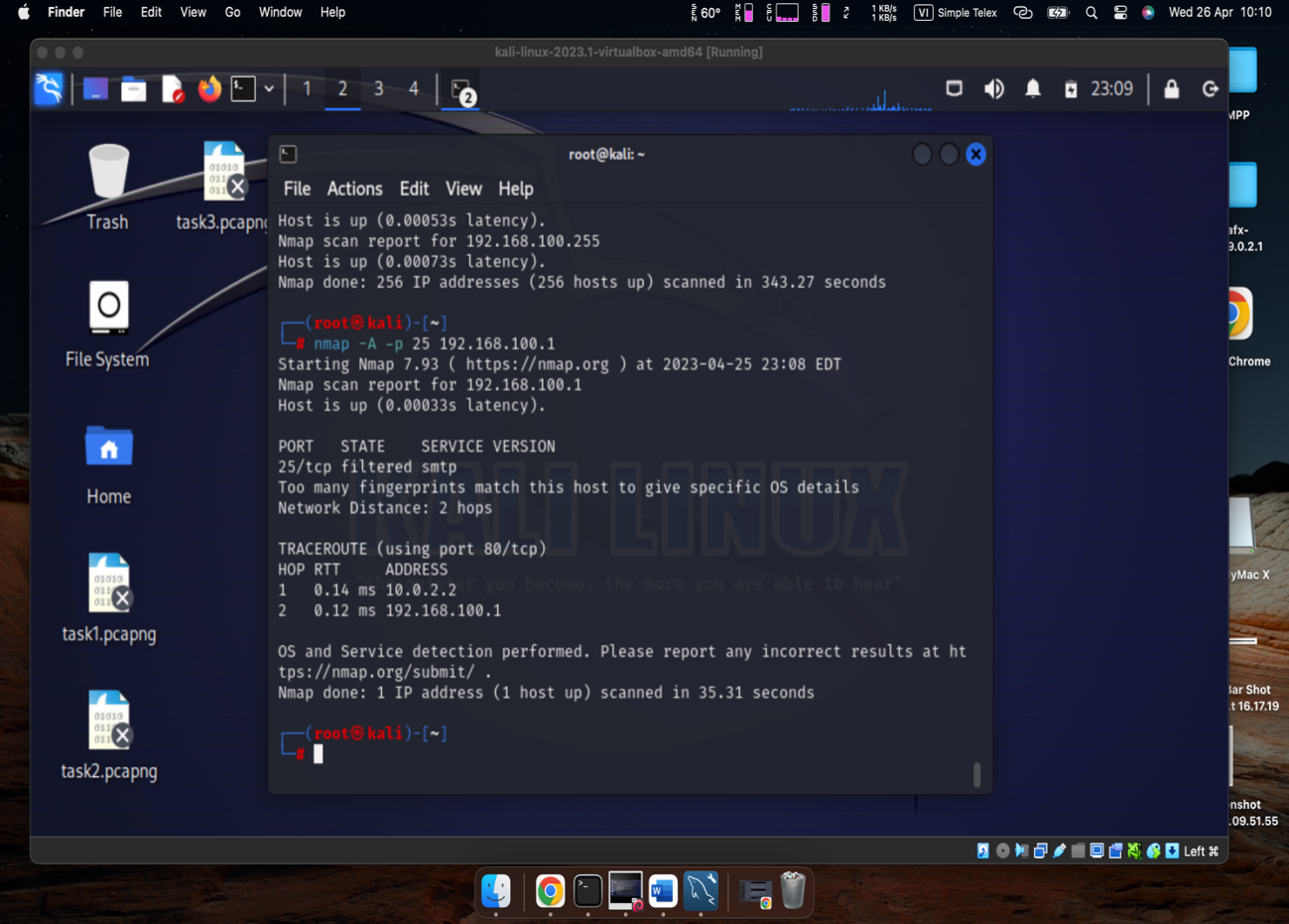
lệnh thăm dò tìm kiếm máy chủ email là: nmap -sn 192.168.100.0/24

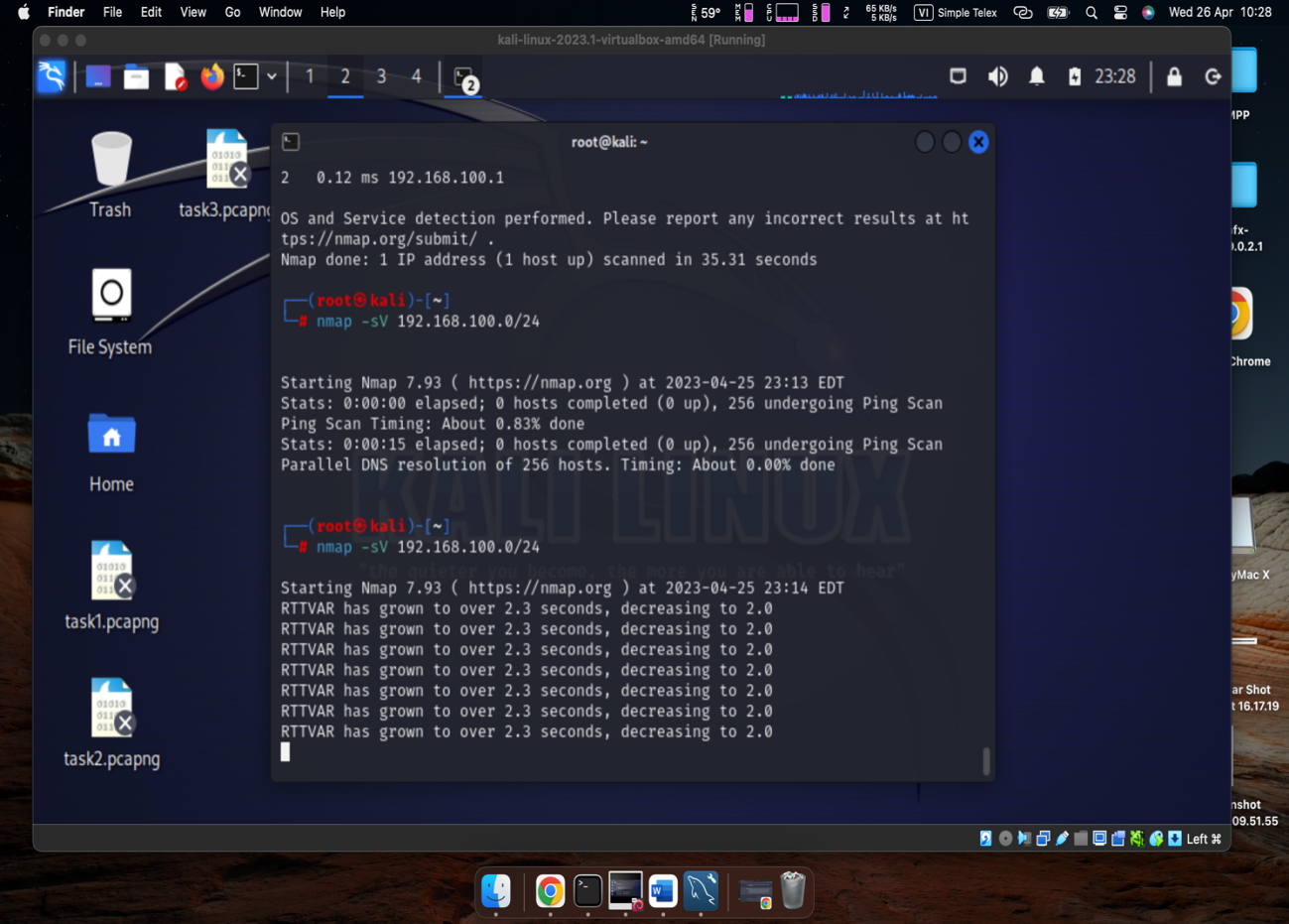


****

* 1. Thông tin hệ điều hành:

Hình ảnh chụp kết quả của nmap





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.

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| Linux kernel | [CVE-2022-35410](https://www.cvedetails.com/cve/CVE-2022-35410/) | Tin tặc có thể tạo ra các yêu cầu đặc biệt đến máy chủ mục tiêu để kích hoạt lỗ hổng này và thực thi các lệnh bất hợp pháp trên hệ thống. |
| Cisco Webex Meetings Desktop App | [CVE-2022-35403](https://www.cvedetails.com/cve/CVE-2022-35403/) | ỗ hổng này xảy ra khi phần mềm Cisco Webex Meetings Desktop App không kiểm tra tính hợp lệ của các yêu cầu đến từ máy chủ tải xuống của họ. Điều này có nghĩa là tin tặc có thể giả mạo yêu cầu và chèn mã độc vào tập tin để đánh lừa người dùng tải xuống và cài đặt. |
| Google Chrome | [CVE-2022-35168](https://www.cvedetails.com/cve/CVE-2022-35168/) | Lỗ hổng này cho phép tin tặc tấn công và thực thi mã độc từ xa trên máy tính của người dùng thông qua các trang web được tạo ra bởi tin tặc. |
| Adobe Acrobat | [CVE-2022-34903](https://www.cvedetails.com/cve/CVE-2022-34903/) | Lỗ hổng này cho phép tin tặc thực hiện tấn công từ xa và thực thi mã độc trên hệ thống của người dùng thông qua các tệp PDF độc hại. |
| Microsoft Exchange Server. | [CVE-2022-34894](https://www.cvedetails.com/cve/CVE-2022-34894/) | Lỗ hổng này cho phép tin tặc thực hiện cuộc tấn công từ xa và thực thi mã độc trên hệ thống của người dùng. |