**MỤC LỤC**

[1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap 1](#_Toc133431753)

[1.1 Kịch bản 1 1](#_Toc133431754)

[2.1 Kịch bản 2 3](#_Toc133431755)

[3.1 Kịch bản 3 4](#_Toc133431756)

[2. Thu thập thông tin hệ thống 5](#_Toc133431757)

[3. Tìm kiếm thông tin về các lỗ hổng 6](#_Toc133431758)

BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

***Họ và tên sinh viên: Nguyễn Quang Huy***

***MSSV: 0850080075***

***Yêu cầu kết quả thực hành:***

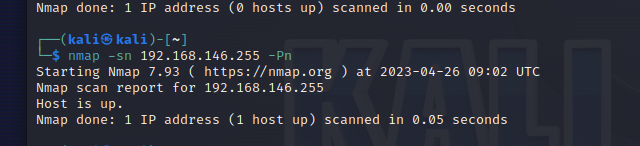
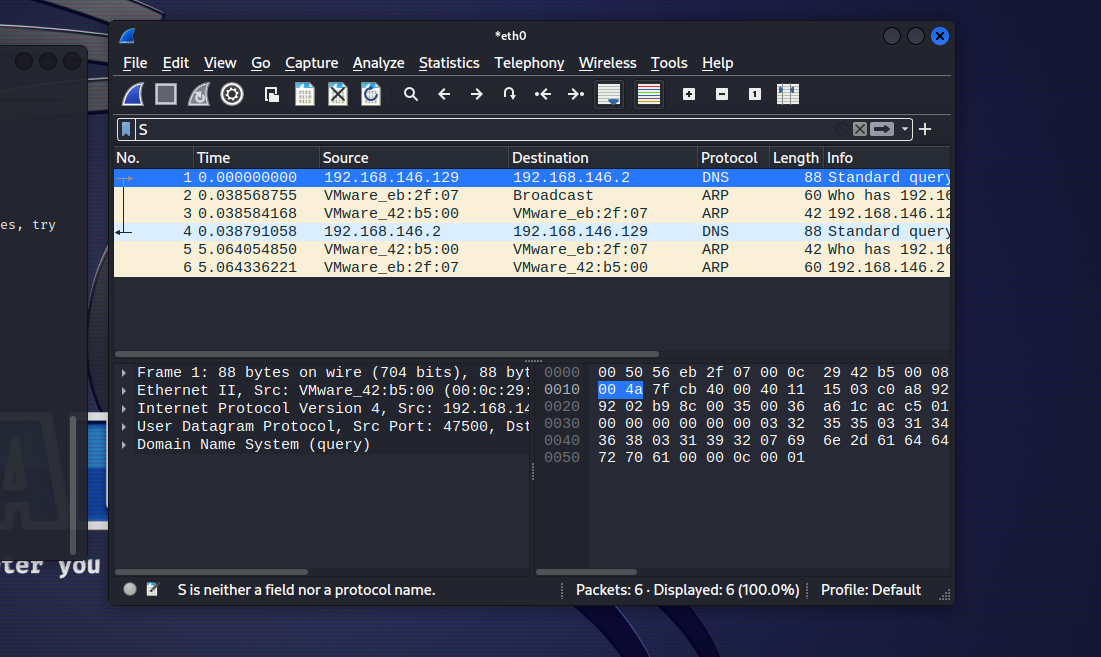
Đóng gói các kết quả vào file nén có tên theo định dạng HoTenSV\_MSSV\_Lab01.zip

* 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.

**KẾT QUẢ THỰC HÀNH**

# 1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

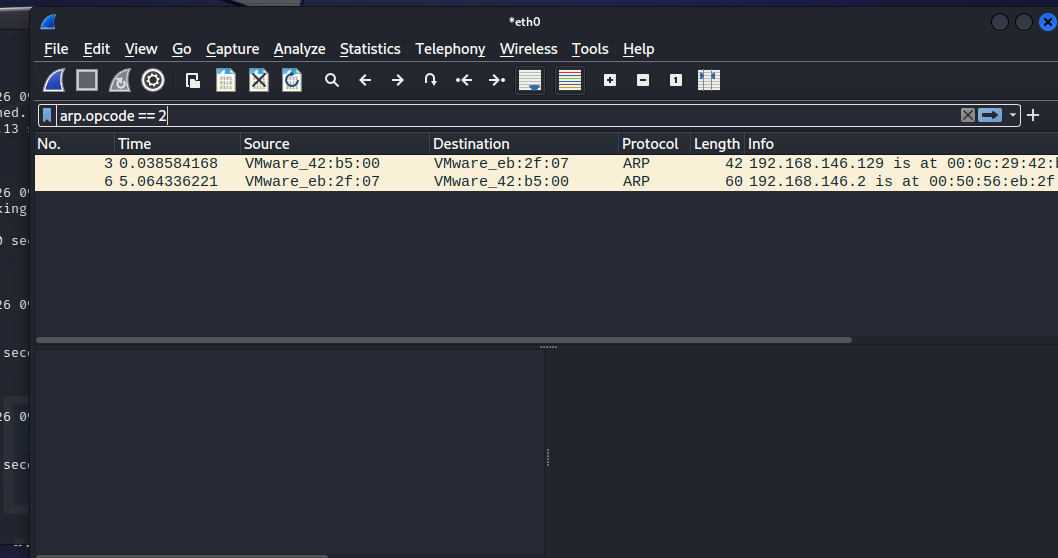
## 1.1 Kịch bản 1

* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được
* *Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*
* *Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*
* 
* 

-Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn

công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính

trong mạng 192.168.146.255



Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy

các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong

kết quả quét mạng bằng công cụ nmap.

*Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để*

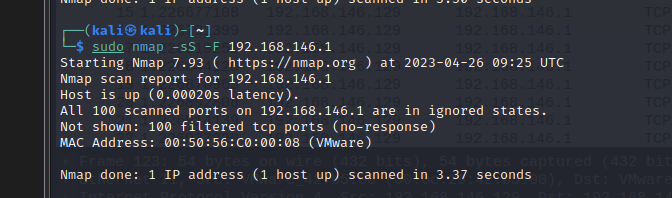
*phát hiện các nút mạng đang hoạt động trong mạng.*

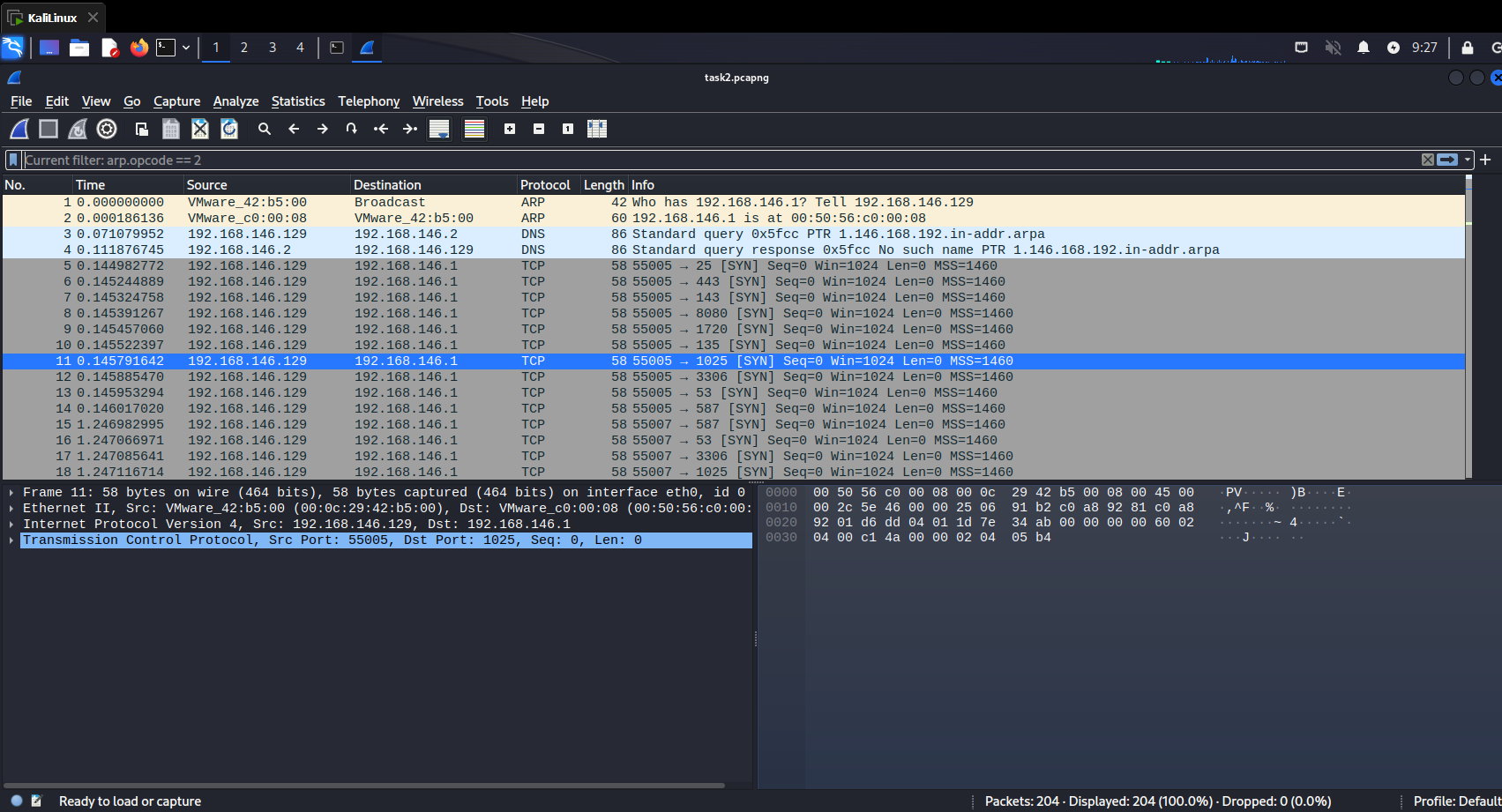
## 2.1 Kịch bản 2

* 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

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

**

**

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.

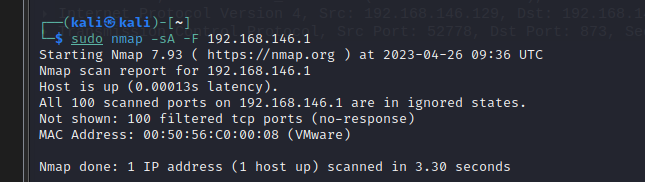
* TCP SYN Scan

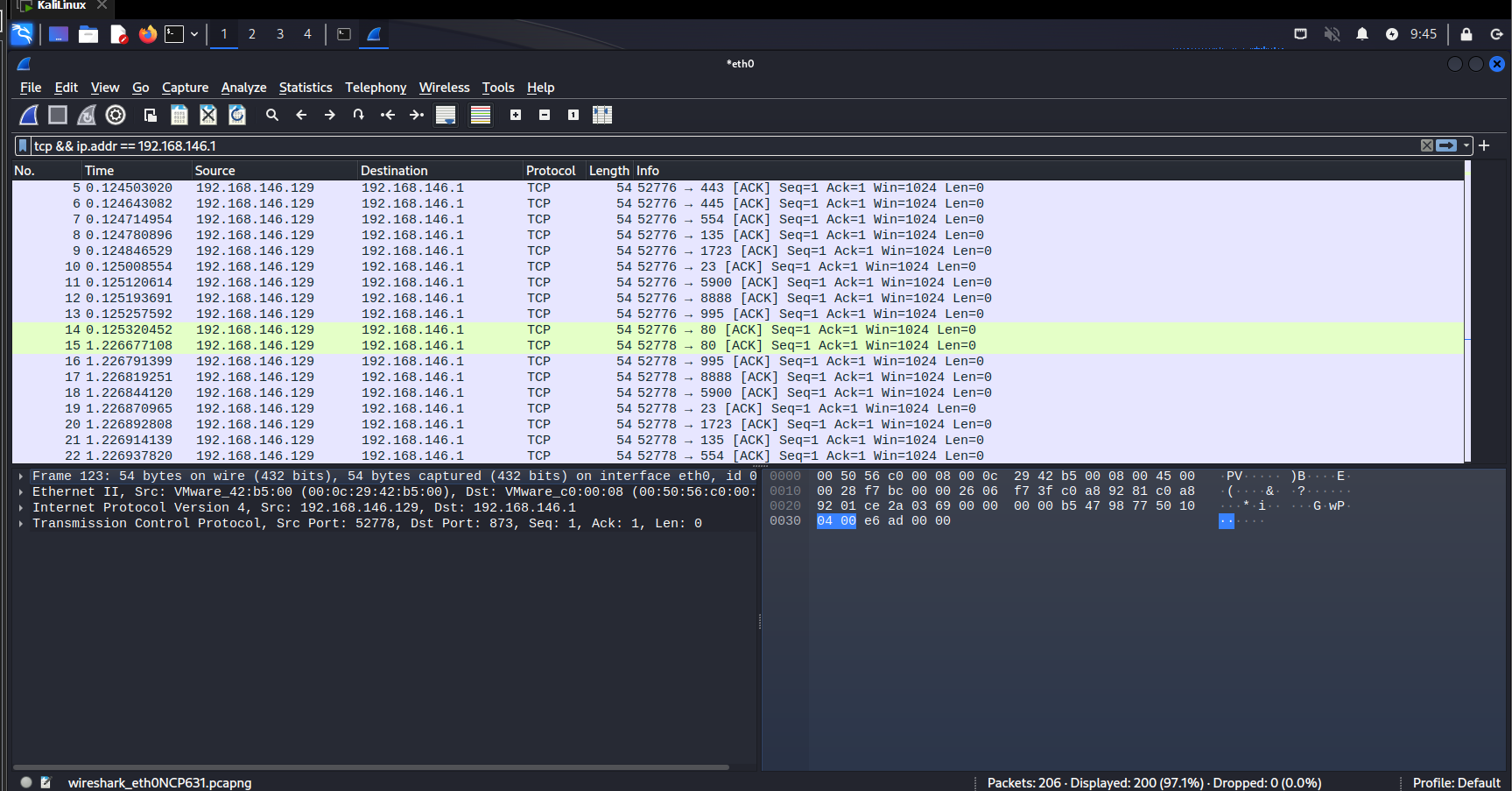
## 3.1 Kịch bản 3

* 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

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

**

**

tương tự như TCP SYN Scan. Điểm khác biệt nhỏ là Nmap sẽ gửi lại gói

tin ACK để hoàn tất quá trình thiết lập liên kết. Sau đó, Nmap gửi lại ngay các gói tin RST để

hủy liên kết này.

* TCP Connection Scan:

# 2. 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)

nmap -p 25,465,587 --script smtp-enum-users <target>

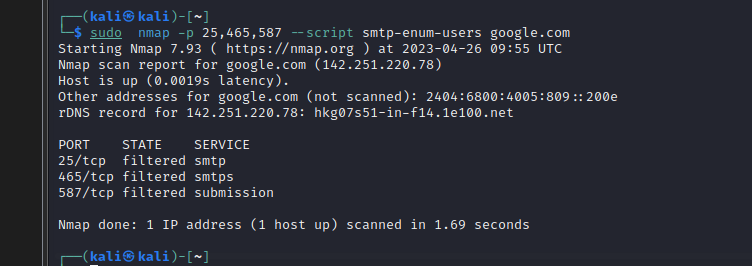
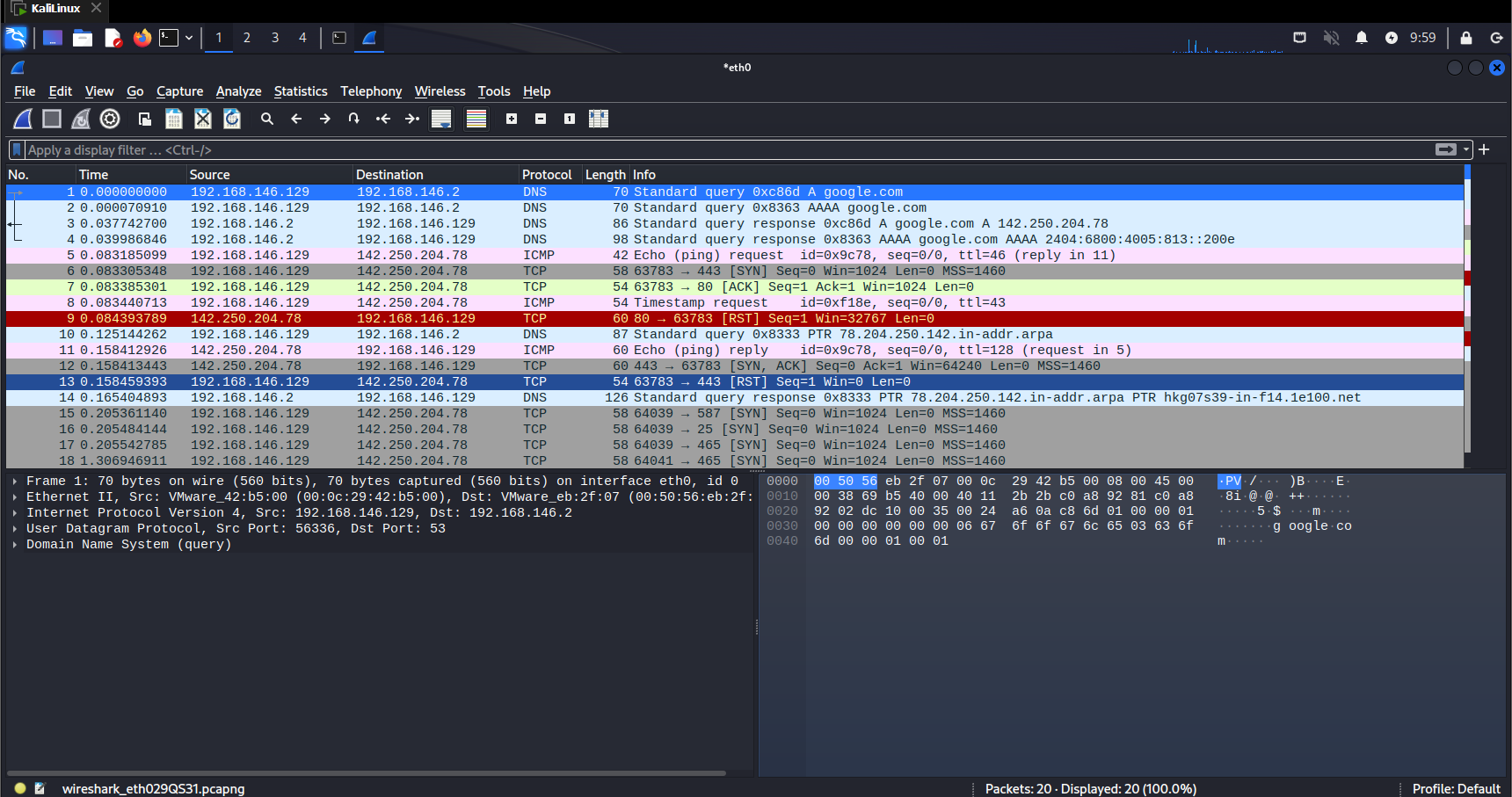
Trong đó:

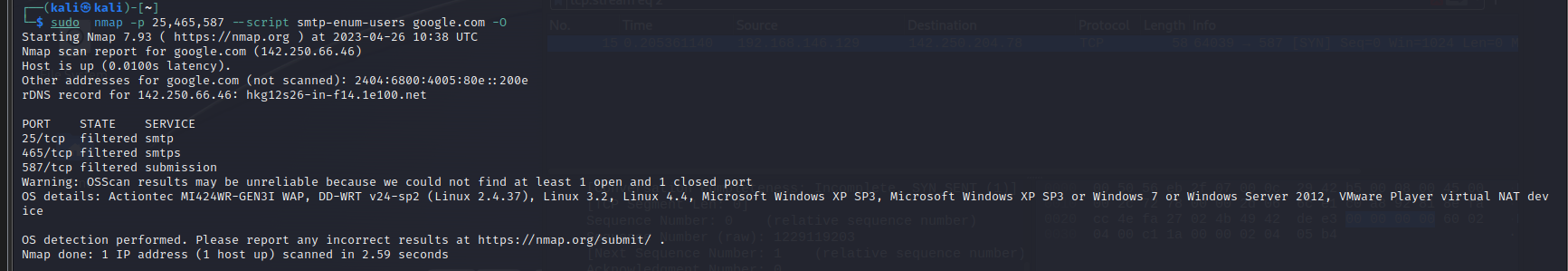
-p: Tham số này được sử dụng để chỉ định các cổng mà nmap sẽ quét tìm kiếm. Trong trường hợp này, chúng ta chỉ quan tâm đến các cổng liên quan đến email, bao gồm cổng 25 (SMTP), 465 (SMTPS) và 587 (submission).

--script smtp-enum-users: Đây là tùy chọn thực hiện kịch bản (script) smtp-enum-users được tích hợp trong nmap để quét tìm các tài khoản email tồn tại trên máy chủ. Tùy chọn này sẽ giúp nmap tự động thực hiện việc tìm kiếm một cách tự động, thay vì phải nhập tay các lệnh để tìm kiếm.

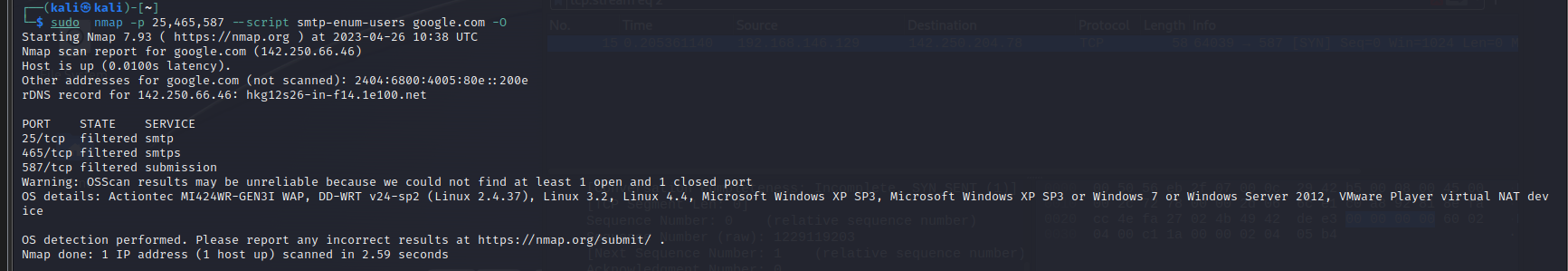
<target>: Đây là địa chỉ IP hoặc tên miền của máy chủ email cần quét tìm kiếm.

**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
* 

# 3. 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)** |
| 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/) | Lỗ 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. |