**Ngô Phúc Thịnh**

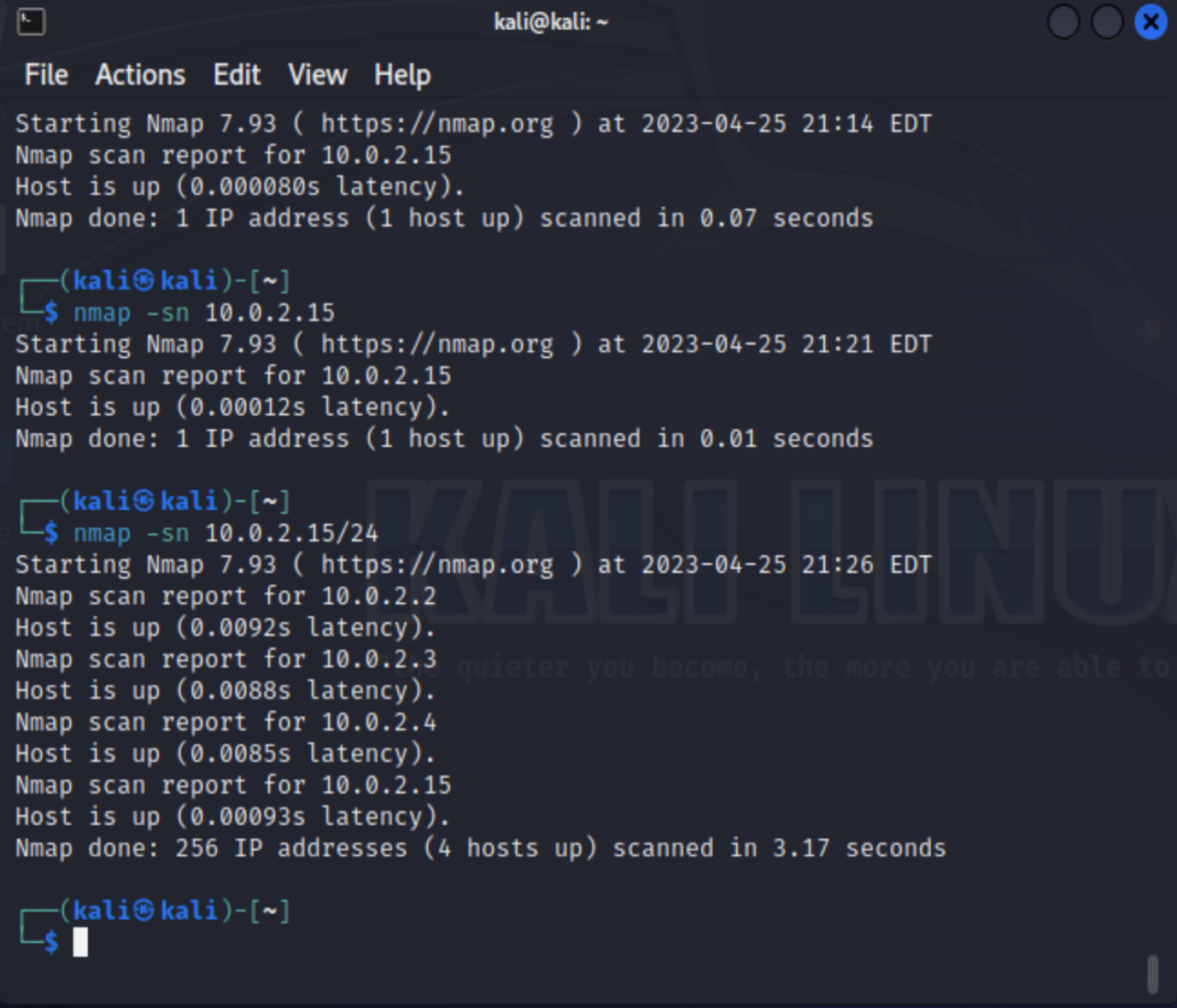
**MSSV: 0850080106**

**Bài Lab 1**

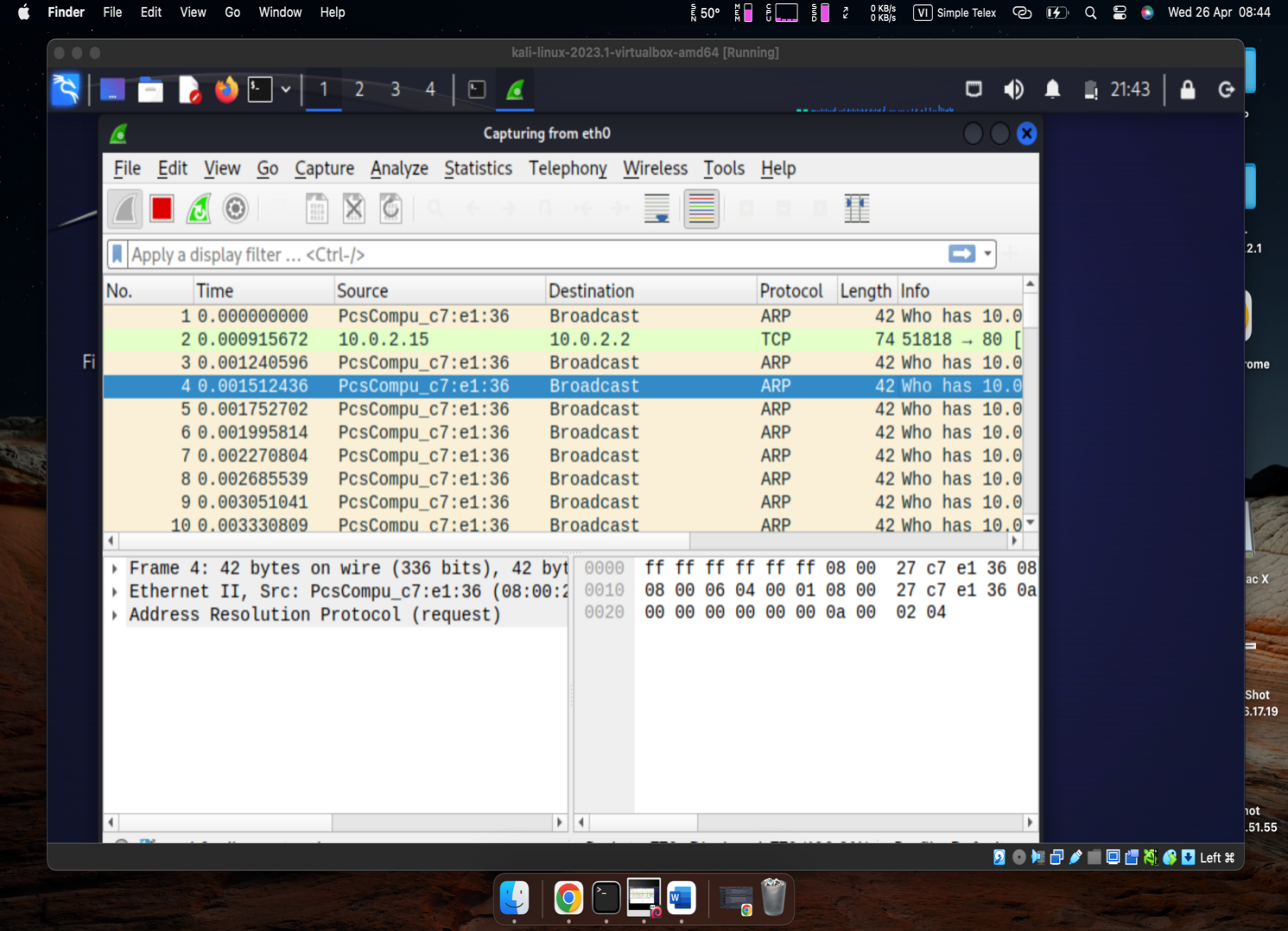
**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

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



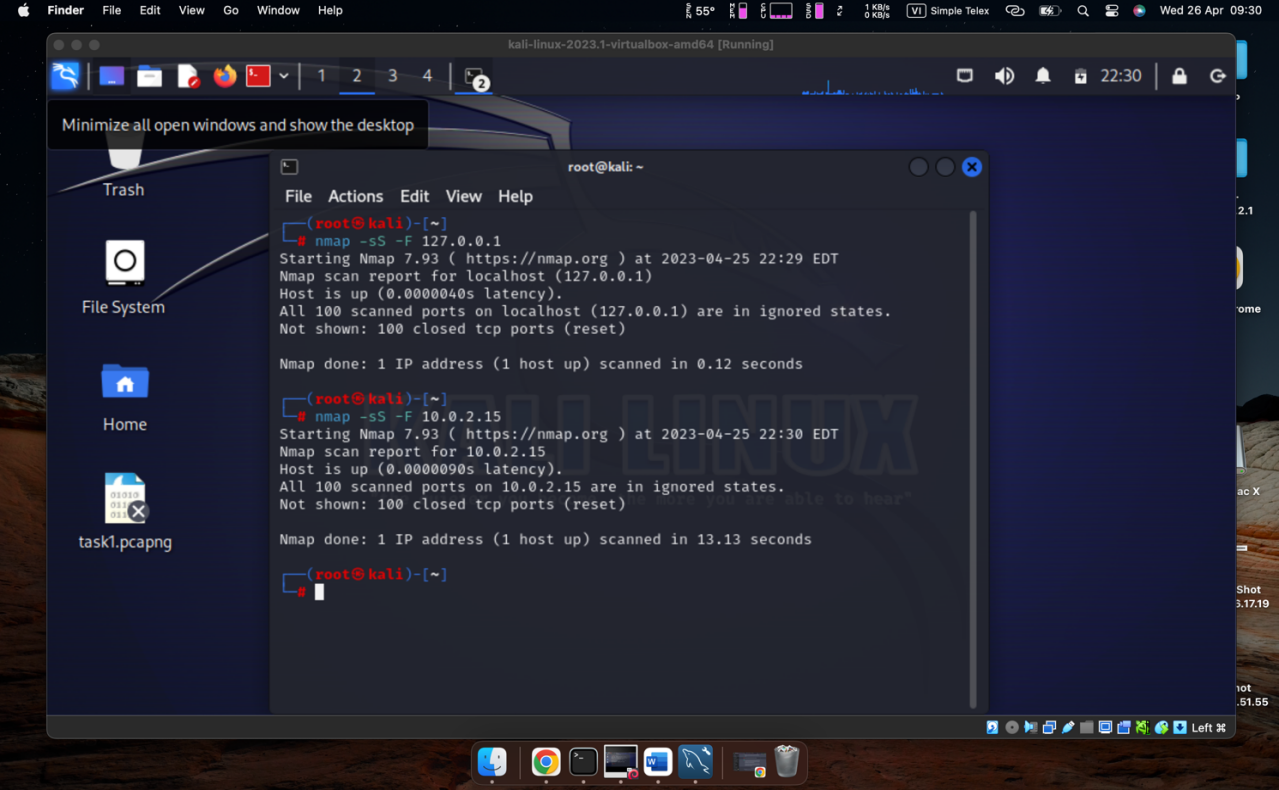
* Là kĩ thuật ping scan host discovery" scan bằng Nmap. Kỹ thuật ping scan được sử dụng để xác định xem các máy chủ nào trong một mạng có sẵn hoặc đang hoạt động.

*Phân tích:*

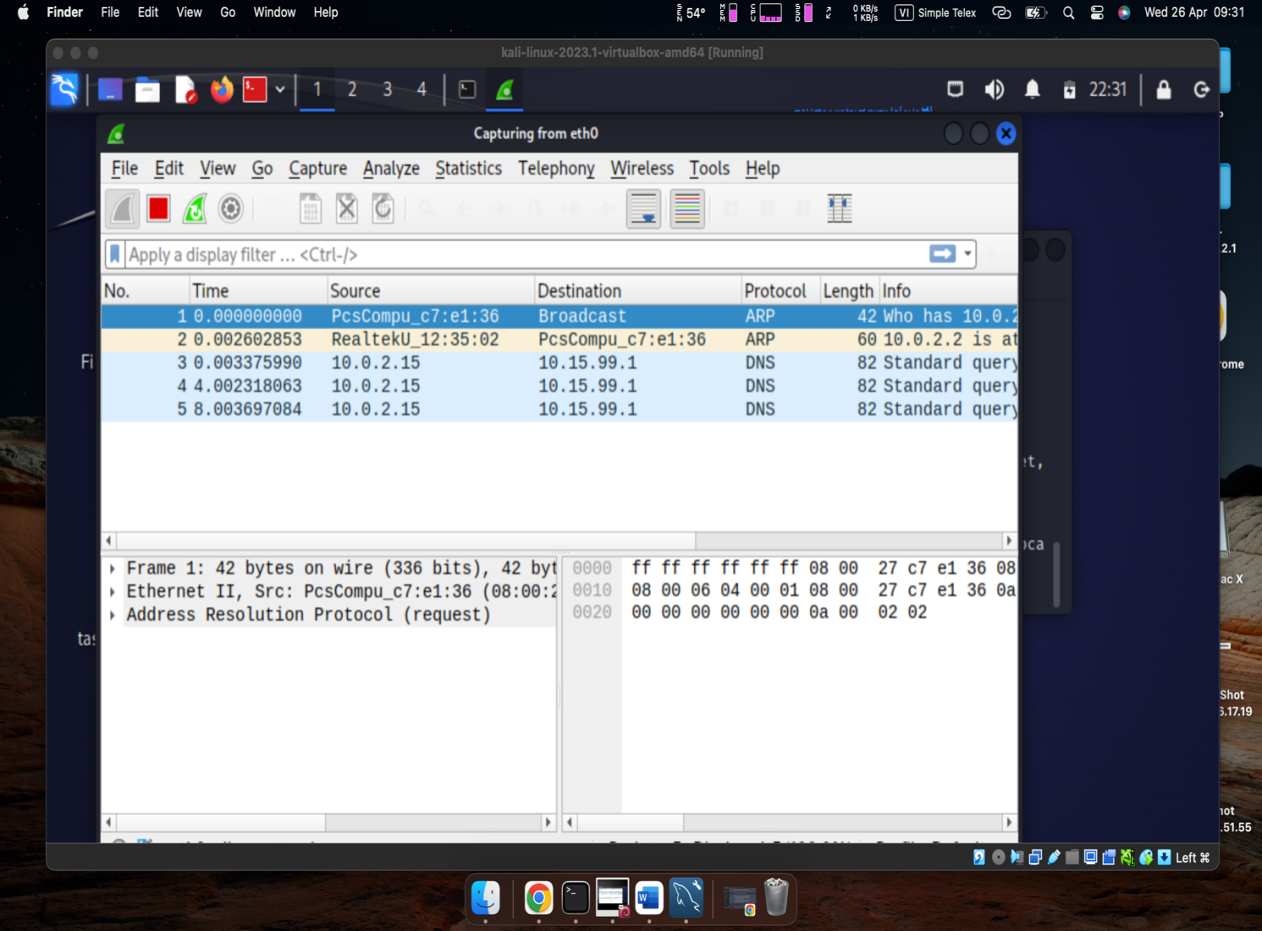
địa chỉ IP 10.0.2.4 và thông báo rằng địa chỉ IP của chính nó là 10.0.2.15. Gói tin này được gửi trong mạng LAN để giải quyết địa chỉ vật lý của một địa chỉ IP. Khi máy có địa chỉ IP 10.0.2.4 nhận được yêu cầu này, nó sẽ trả lời với một gói tin ARP khác chứa địa chỉ MAC của nó.

* 1. **Kịch bản 2**

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: 1 điểm



- Dòng 1: Máy tính có địa chỉ MAC là PcsCompu\_c7:e1:36 gửi một yêu cầu ARP (Who has 10.0.2.2?) để tìm địa chỉ MAC của máy tính có địa chỉ IP là 10.0.2.2.

- Dòng 2: Máy tính có địa chỉ MAC là RealtekU\_12:35:02 trả lời yêu cầu ARP ở dòng trước bằng một gói tin ARP khác, cho biết địa chỉ MAC của máy tính có địa chỉ IP là 10.0.2.2.

- Dòng 3-5: Máy tính có địa chỉ IP là 10.0.2.15 gửi các yêu cầu DNS (domain name system) để tìm kiếm địa chỉ IP của một tên miền được định nghĩa bởi chuỗi ký tự "15.2.0.10.in-addr.arpa". Các yêu cầu này được gửi đến địa chỉ IP 10.15.99.1, có thể là máy chủ DNS.

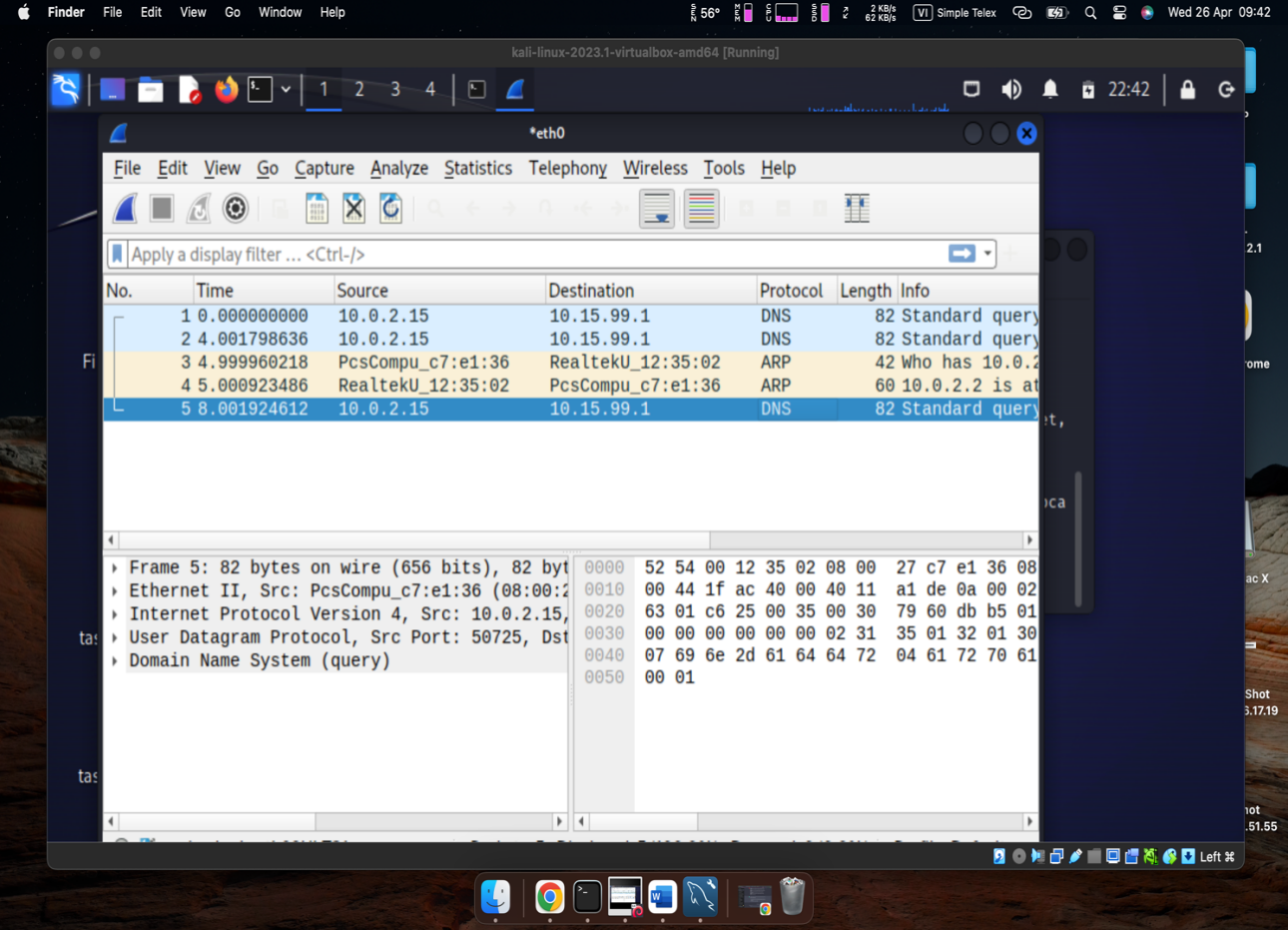
- Tên kĩ thuật trên là"TCP SYN scan" và "Fast scan".

* 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



- Gói tin DNS: Máy tính có địa chỉ IP 10.0.2.15 gửi yêu cầu tìm kiếm địa chỉ DNS (PTR) cho địa chỉ IP 10.2.0.15.in-addr.arpa với mã xác thực (query ID) là 0xdbb3 đến máy chủ DNS có địa chỉ IP 10.15.99.1.

- Gói tin DNS: Máy tính có địa chỉ IP 10.0.2.15 gửi yêu cầu tìm kiếm địa chỉ DNS (PTR) cho địa chỉ IP 10.2.0.15.in-addr.arpa với mã xác thực (query ID) là 0xdbb4 đến máy chủ DNS có địa chỉ IP 10.15.99.1.

- Gói tin ARP: Máy tính có địa chỉ IP 10.0.2.15 gửi yêu cầu ARP để tìm địa chỉ MAC của địa chỉ IP 10.0.2.2. Đây là một yêu cầu broadcast, nghĩa là gửi đến tất cả các máy tính trên mạng local.

- Gói tin ARP: Máy tính có địa chỉ MAC là 52:54:00:12:35:02 và địa chỉ IP là 10.0.2.2 trả lời yêu cầu ARP của máy tính có địa chỉ IP 10.0.2.15 bằng cách cung cấp địa chỉ MAC của mình.

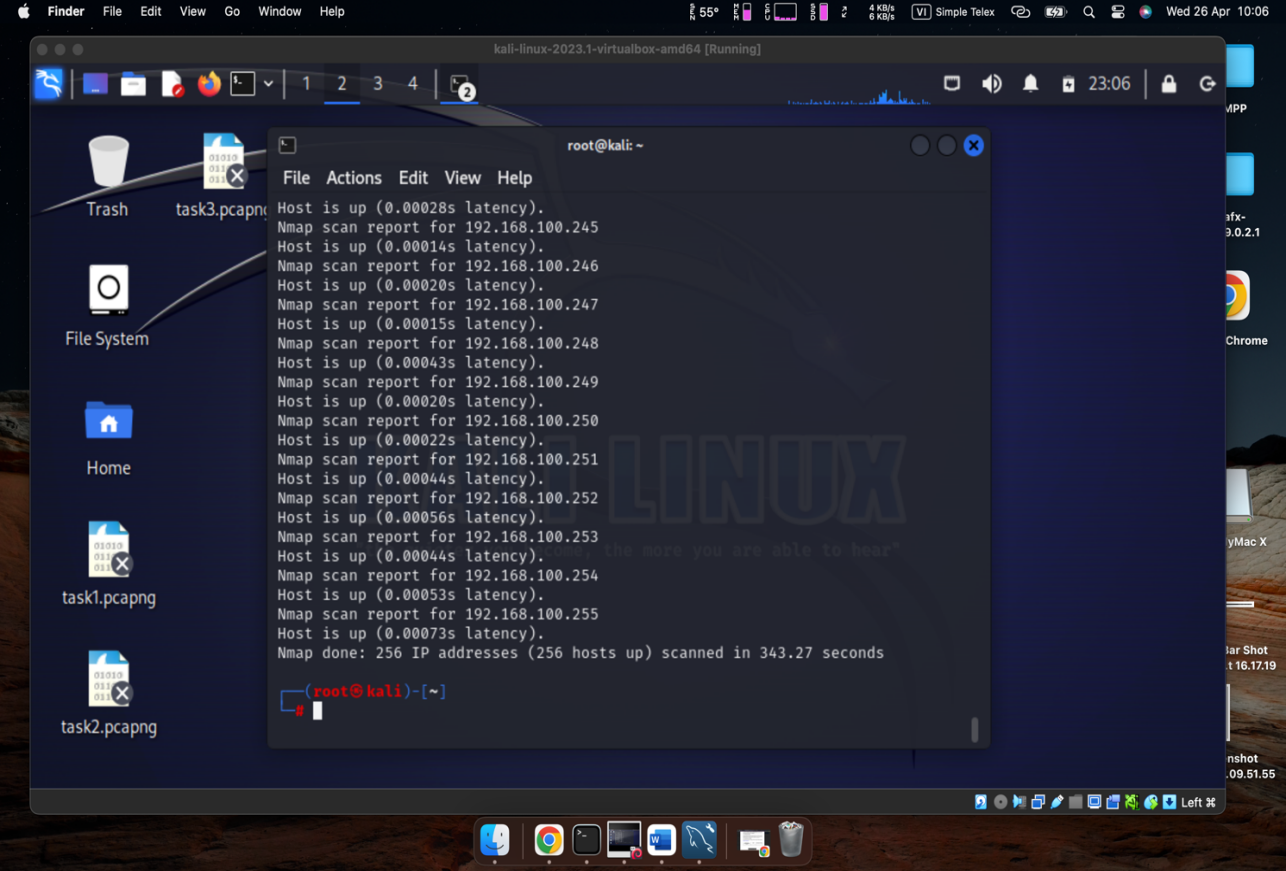
- Gói tin DNS: Máy tính có địa chỉ IP 10.0.2.15 gửi yêu cầu tìm kiếm địa chỉ DNS (PTR) cho địa chỉ IP 10.2.0.15.in-addr.arpa với mã xác thực (query ID) là 0xdbb5 đến máy chủ DNS có địa chỉ IP 10.15.99.1.

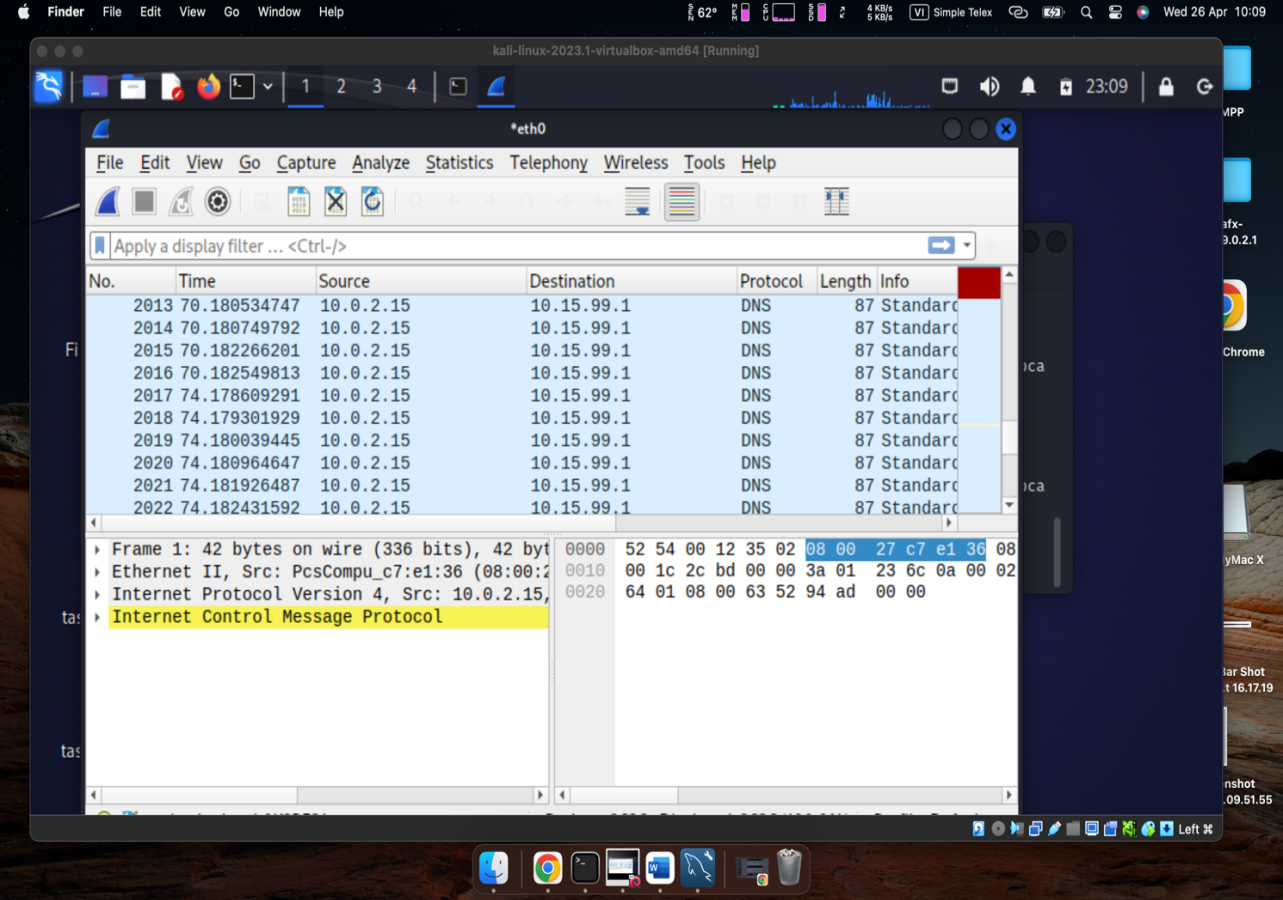
- Tên kĩ thuật trên là "ACK scan" và "Fast scan".

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?

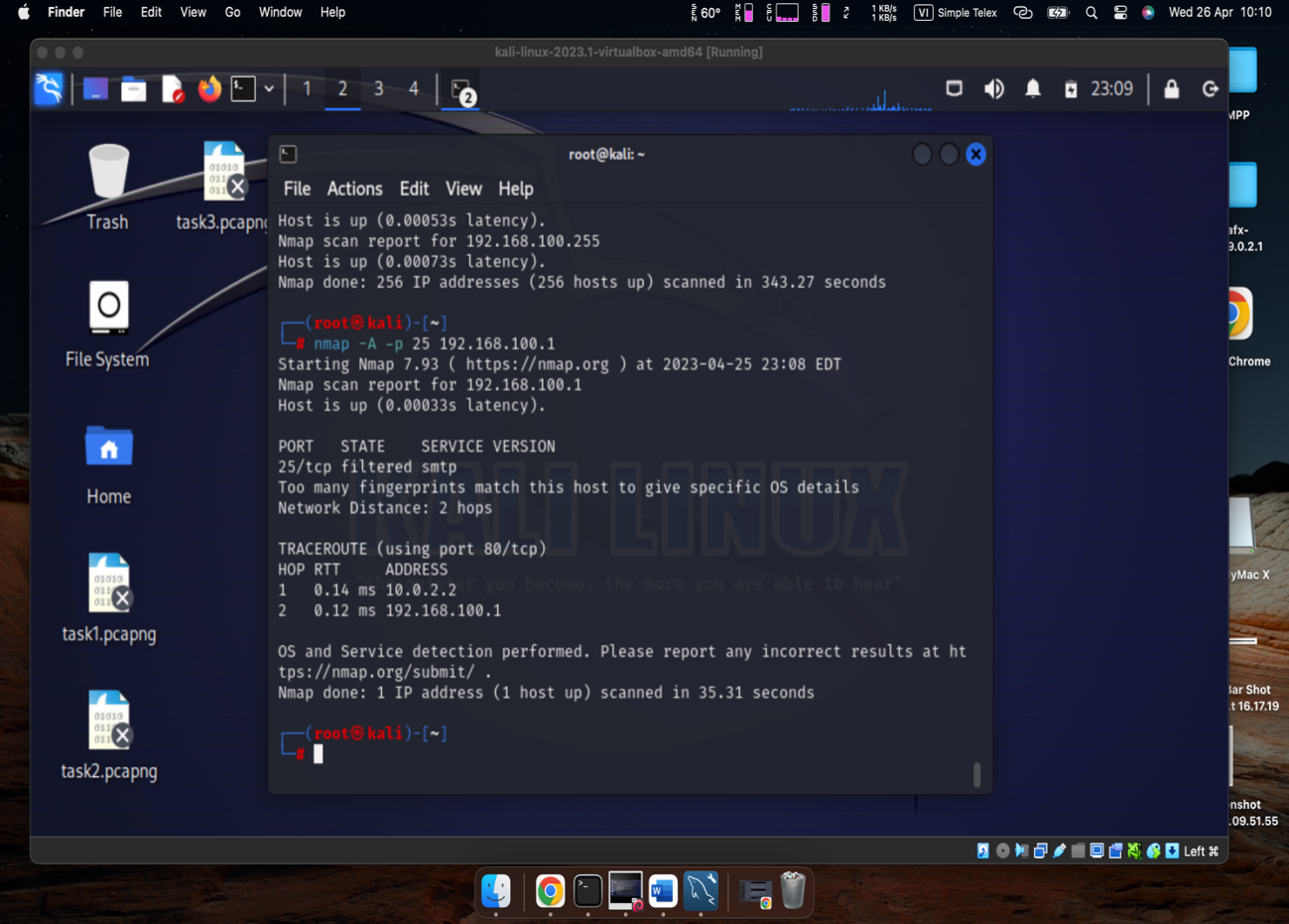
lệnh thăm dò tìm kiếm máy chủ email là: nmap -sn 192.168.100.0/24

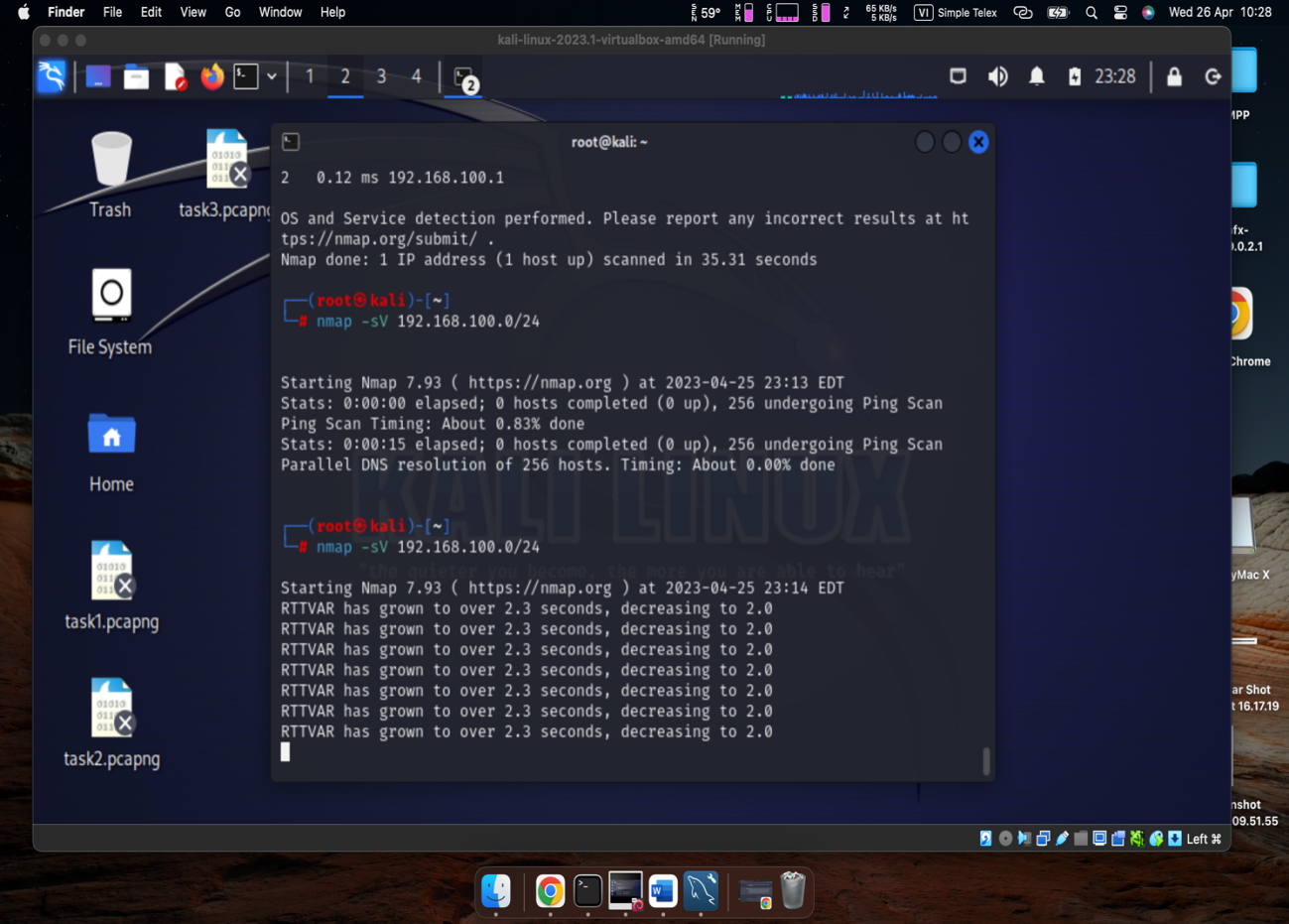




**Thông tin hệ điều hành:**

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/" \o "CVE-2022-35410 security vulnerability details) | 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/" \o "CVE-2022-35403 security vulnerability details) | 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/" \o "CVE-2022-35168 security vulnerability details) | 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/" \o "CVE-2022-34903 security vulnerability details) | 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/" \o "CVE-2022-34894 security vulnerability details) | 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. |