BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

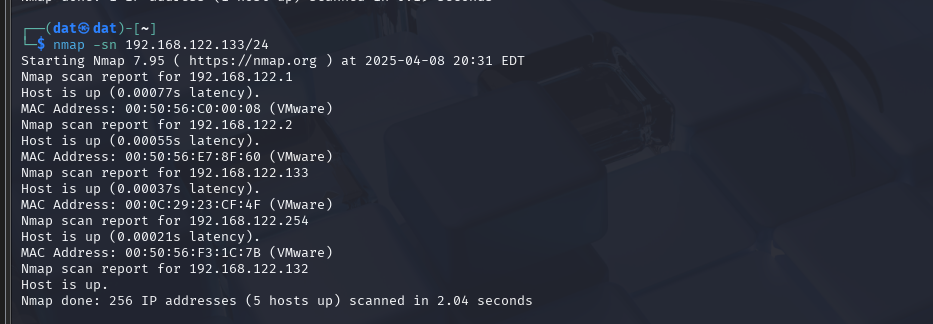
***Họ và tên sinh viên:Trần Công Đạt***

***MSSV: 1050080047***

**KẾT QUẢ THỰC HÀNH**

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

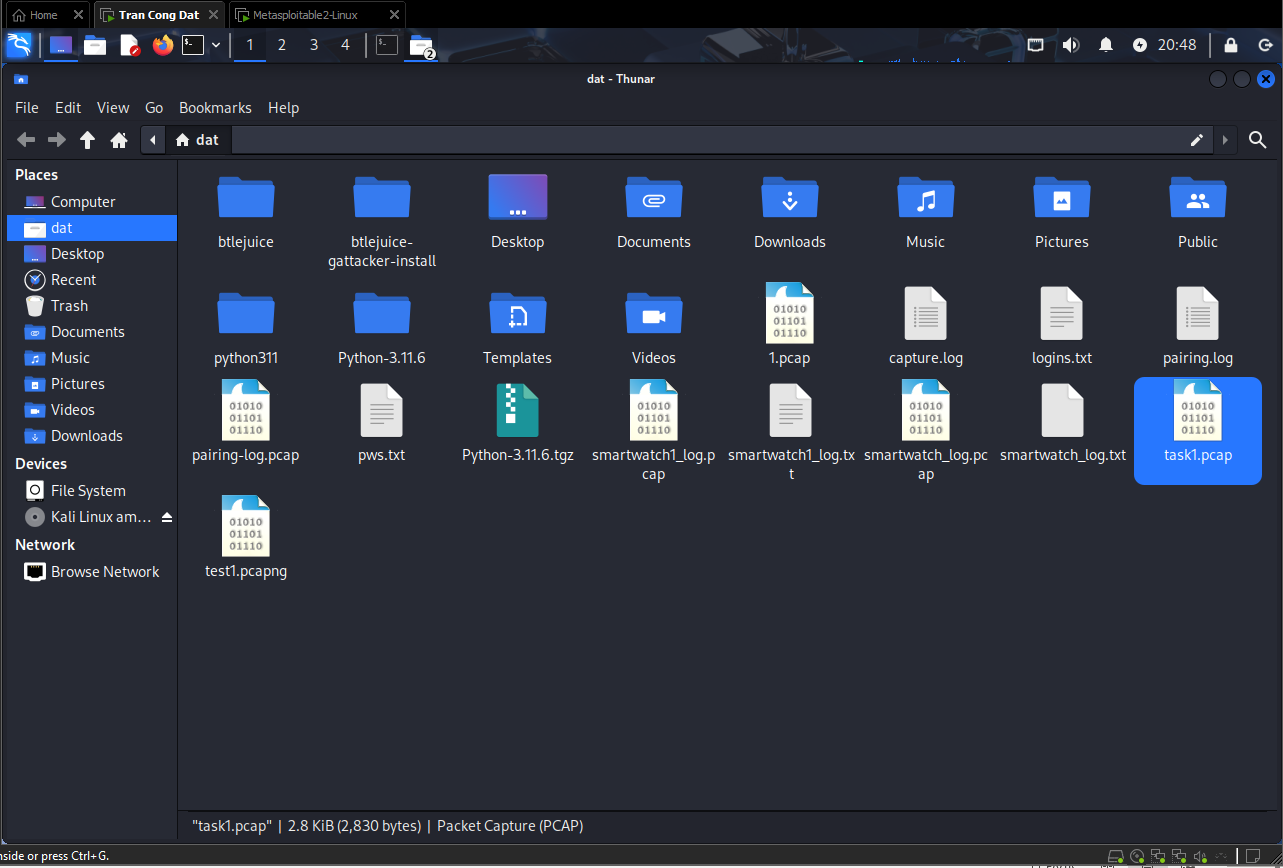
* Ảnh chụp kết quả thực hiện của nmap:



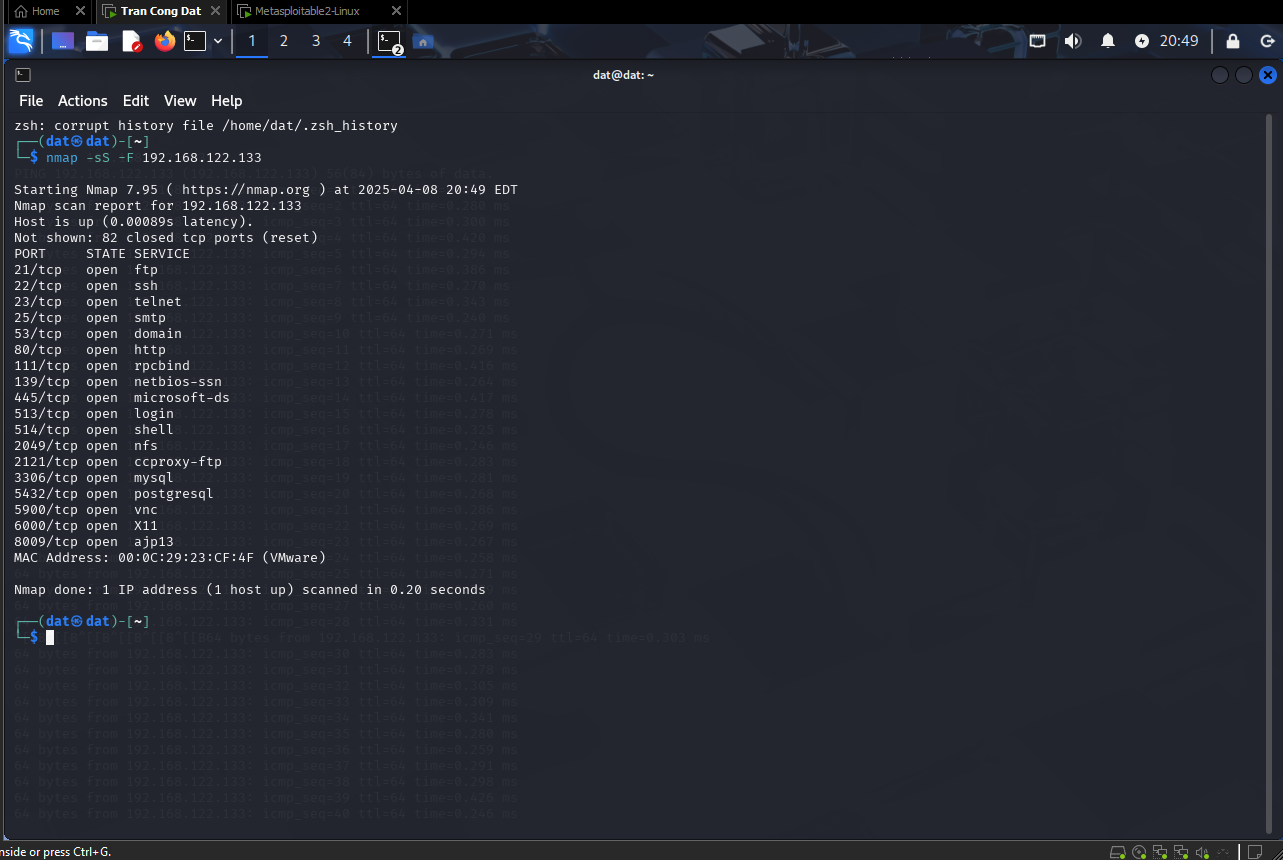
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng:
* Kỹ thuật Ping Scan (Host Discovery) – -sn

|  |  |
| --- | --- |
| **Đặc điểm nhận biết** | Giải thích |
| -sn trong lệnh | Tùy chọn này dùng để không quét cổng, chỉ kiểm tra xem host có hoạt động không (ping scan) |
| Host is up | Kết quả thông báo địa chỉ IP nào đang hoạt động |
| Không thấy thông tin cổng (port) | Không có bất kỳ dòng nào về dịch vụ hay port, nghĩa là không quét cổng TCP/UDP |
| Có MAC Address | Cho biết host được phát hiện là thực sự hoạt động trong mạng nội bộ |

* Khi dùng -sn, nmap chỉ gửi ICMP echo request hoặc ARP request (nếu trong cùng lớp mạng) để kiểm tra xem host có hoạt động không.
* Không thực hiện bất kỳ thao tác nào liên quan đến TCP SYN hay kết nối dịch vụ.
* Trong ảnh, có 5 địa chỉ IP đang hoạt động được phát hiện, và kèm theo MAC Address → Nmap đã dùng ARP scan vì đang trong cùng subnet.
* **Lưu lại file lưu lượng trên máy do thám với tên là task1.pcap**



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:

**Tên kỹ thuật: TCP SYN Scan (quét SYN bán kết nối)**

Tùy chọn trong Nmap: -sS

Mục đích: Phát hiện các cổng (port) đang mở mà không hoàn tất kết nối TCP, giúp tránh bị phát hiện bởi hệ thống giám sát (IDS/IPS).

Đặc điểm:

Gửi gói TCP có cờ SYN đến nhiều port khác nhau.

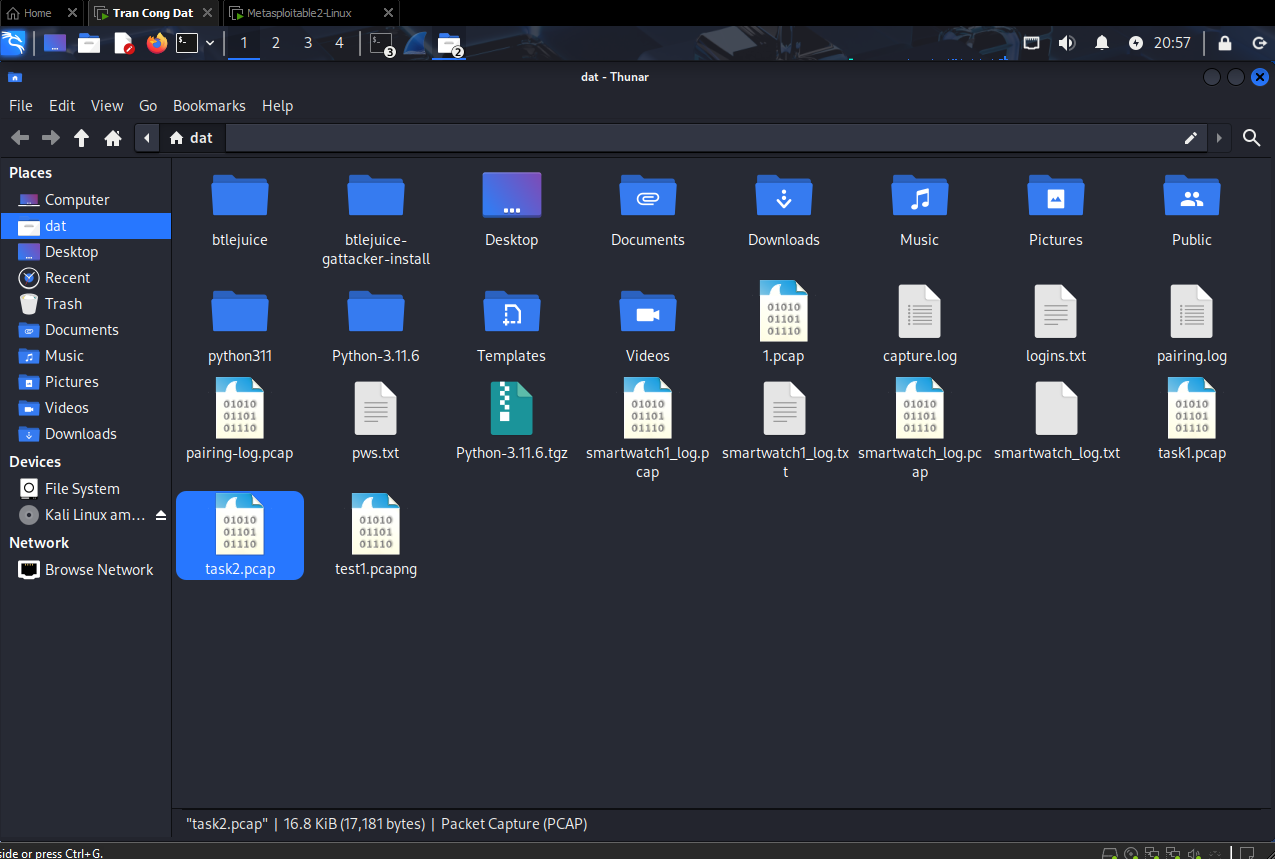
Nếu port mở, máy đích sẽ phản hồi lại bằng gói SYN-ACK.

Máy quét sẽ không hoàn tất kết nối (không gửi ACK), mà gửi gói RST để hủy kết nối.

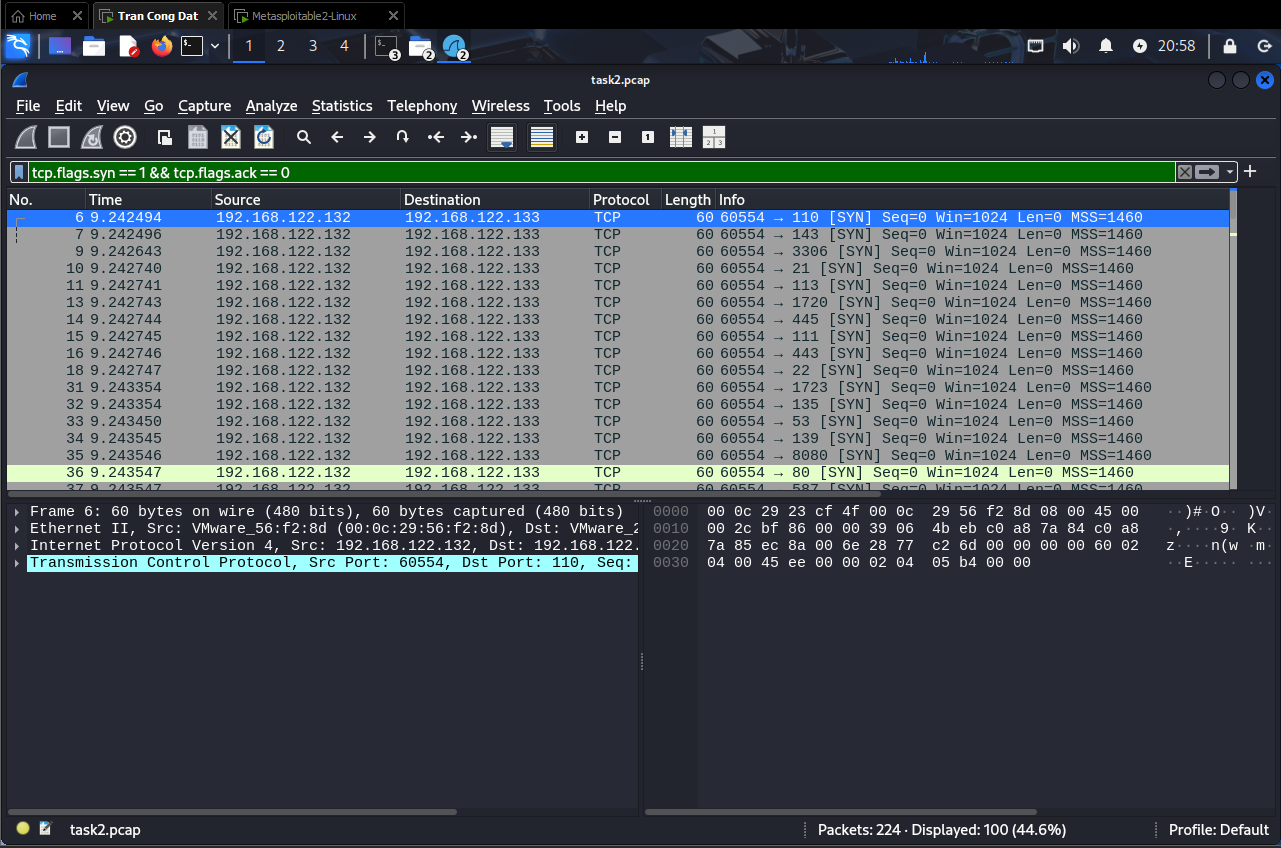
Nếu port đóng, máy đích sẽ phản hồi bằng gói RST.



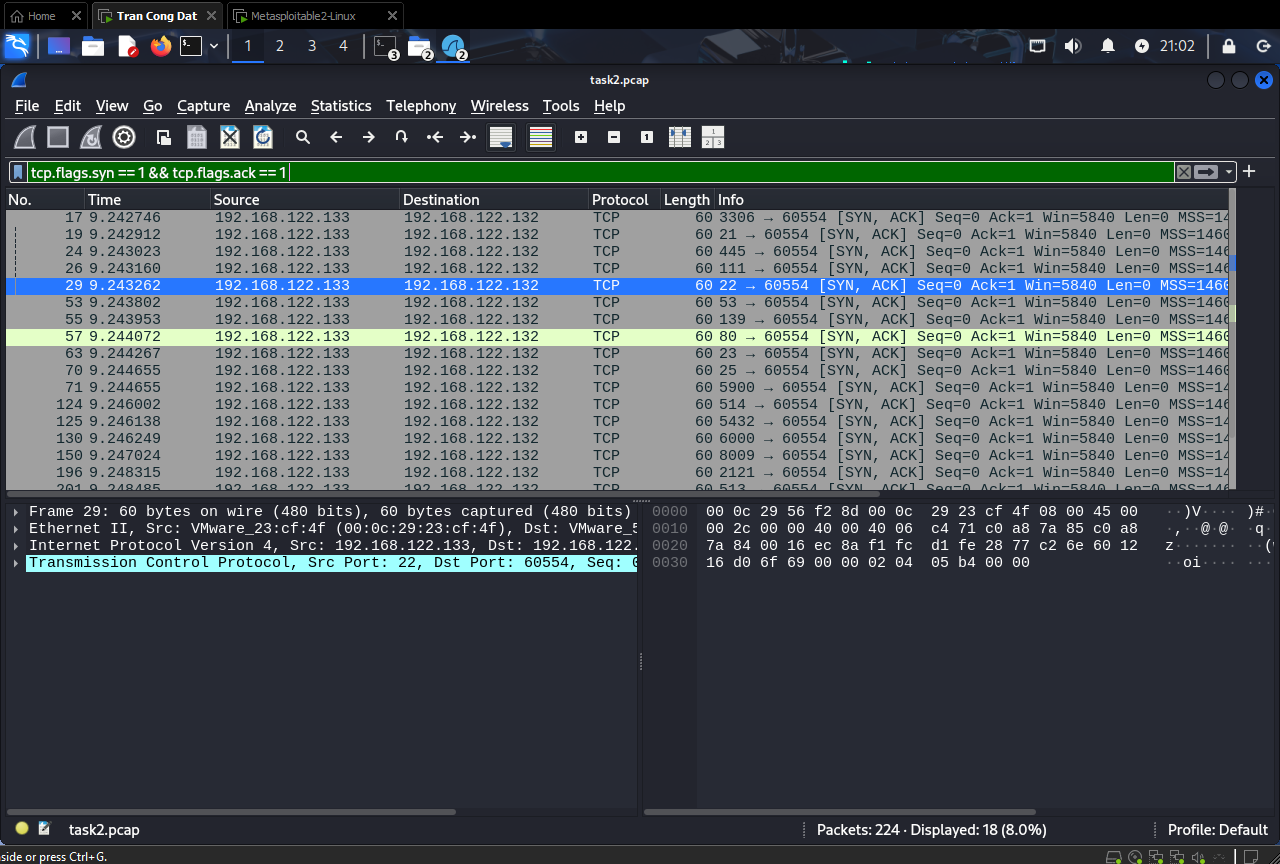
Lưu file task2.pcap



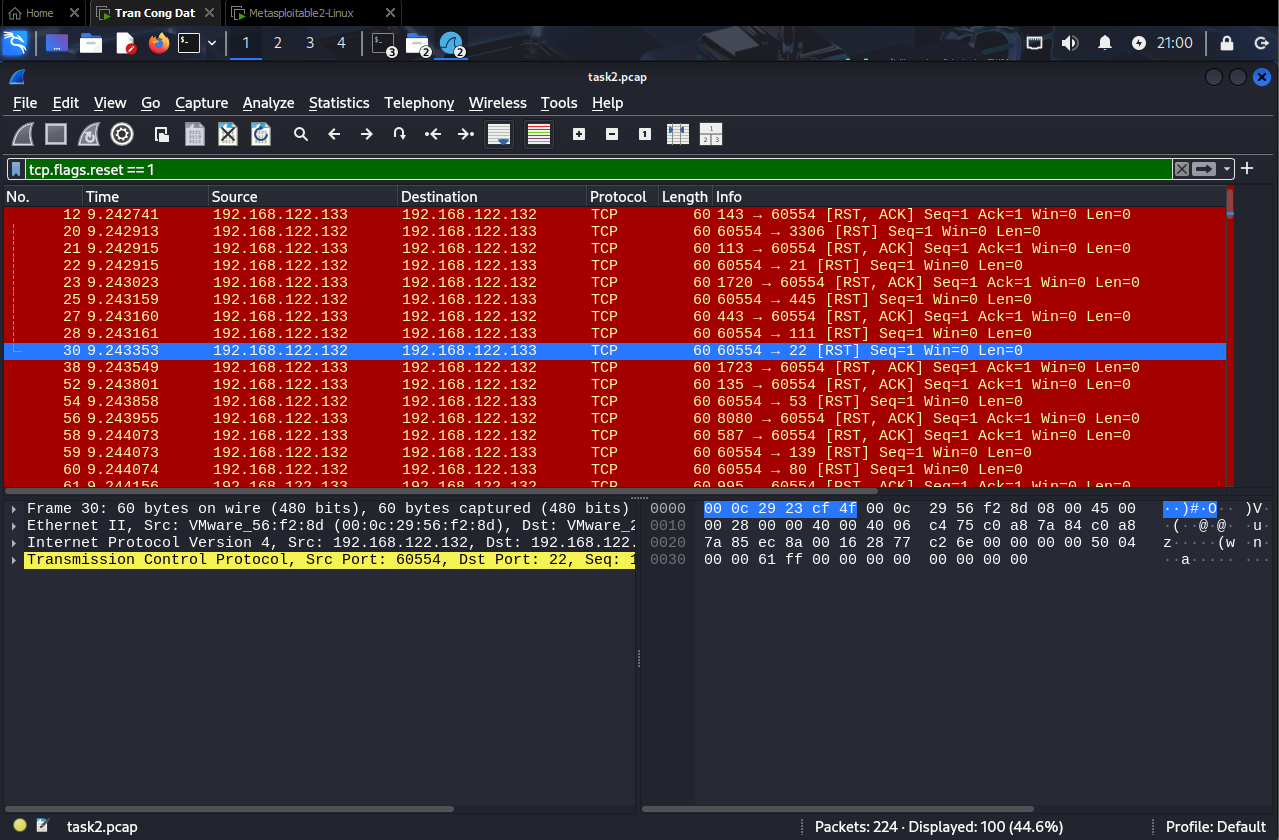
Gói SYN gửi đi từ máy do thám🡪 bắt đầu quét.



Gói SYN-ACK trả về từ host đích=> cổng đang mở.

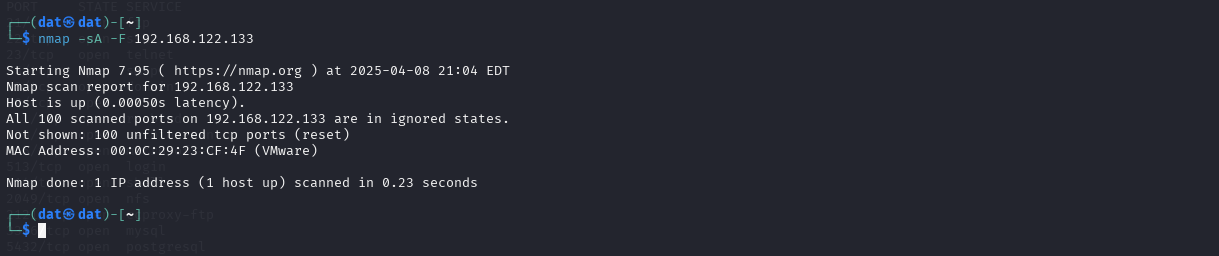


Gói RST từ máy do thám → hủy kết nối ngay sau SYN-ACK.



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:

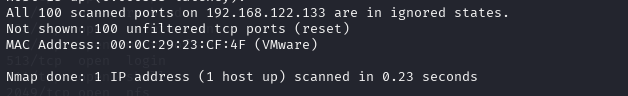
**Kỹ thuật: TCP ACK Scan (-sA)**

Mục đích của kỹ thuật

Xác định trạng thái lọc (filtering) của firewall.

Dùng để phân biệt giữa các cổng bị lọc và không bị lọc, chứ không xác định port có mở (open) hay đóng (closed).

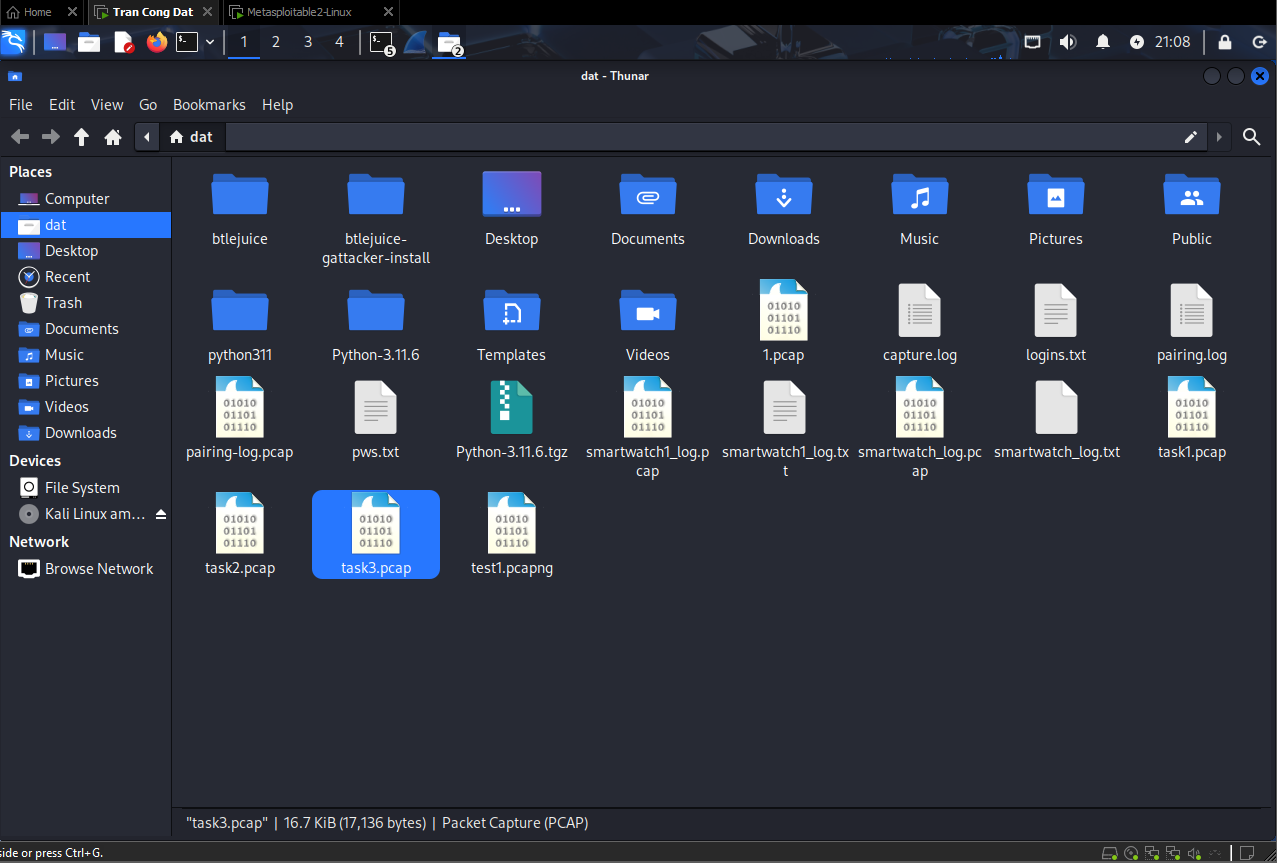
Không gửi SYN mà gửi ACK — thường tránh được sự phát hiện của các IDS/IPS.

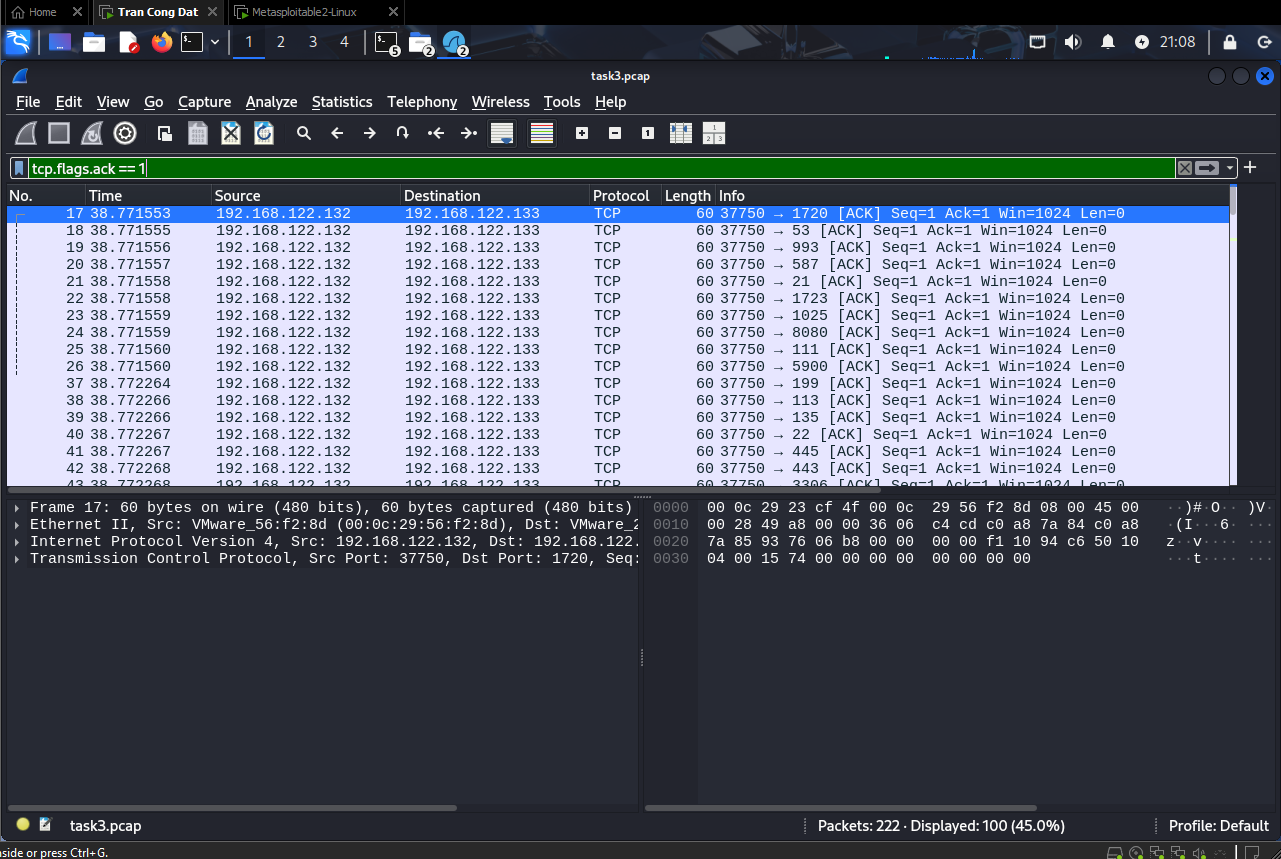


Điều này nghĩa là không có cổng nào bị lọc, và các cổng không được hiển thị đều đã phản hồi bằng gói RST → hệ thống không có firewall hoặc firewall không lọc ACK.

Tất cả các cổng được liệt kê là unfiltered, tức là chúng không bị chặn bởi firewall (gửi ACK nhận lại RST)

Lưu file task3





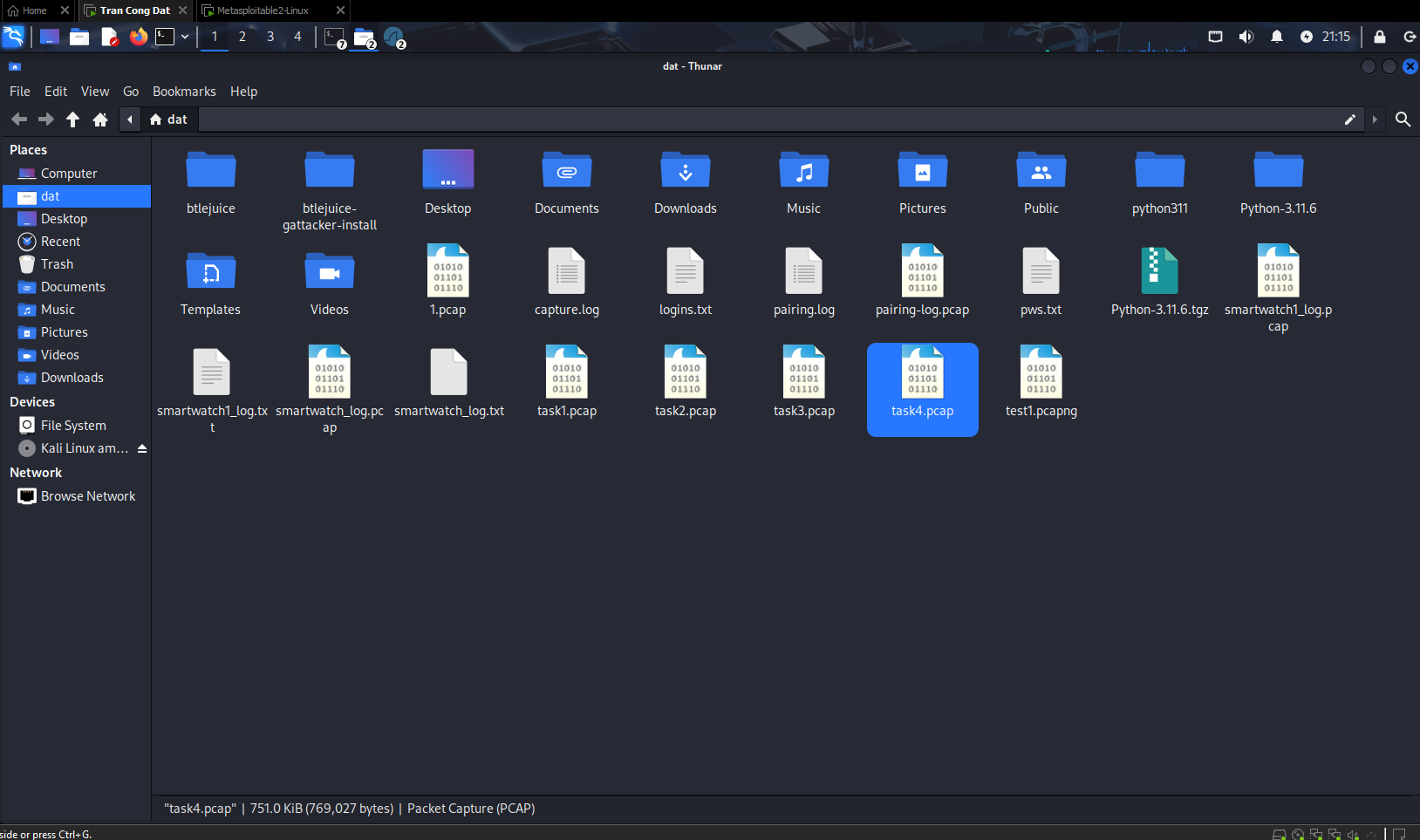
Lọc ra **các gói tin TCP** có **cờ ACK được bật** (ACK flag = 1).

Dựa vào phản hồi:

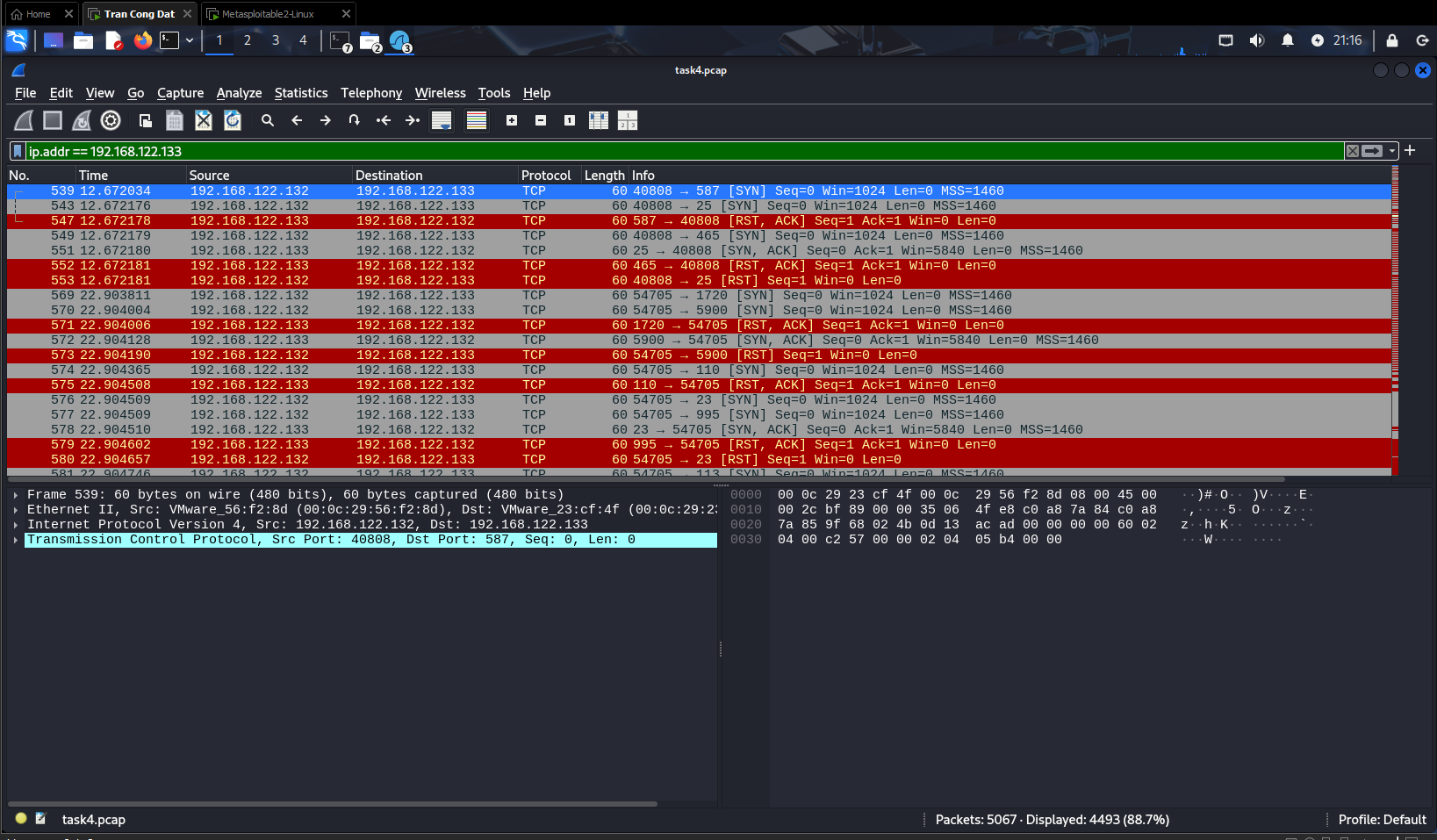
* Nhận **RST** → cổng **không bị lọc (unfiltered)**.
* Không phản hồi / ICMP unreachable → cổng **bị lọc (filtered)**.

1. **Thu thập thông tin hệ thống**

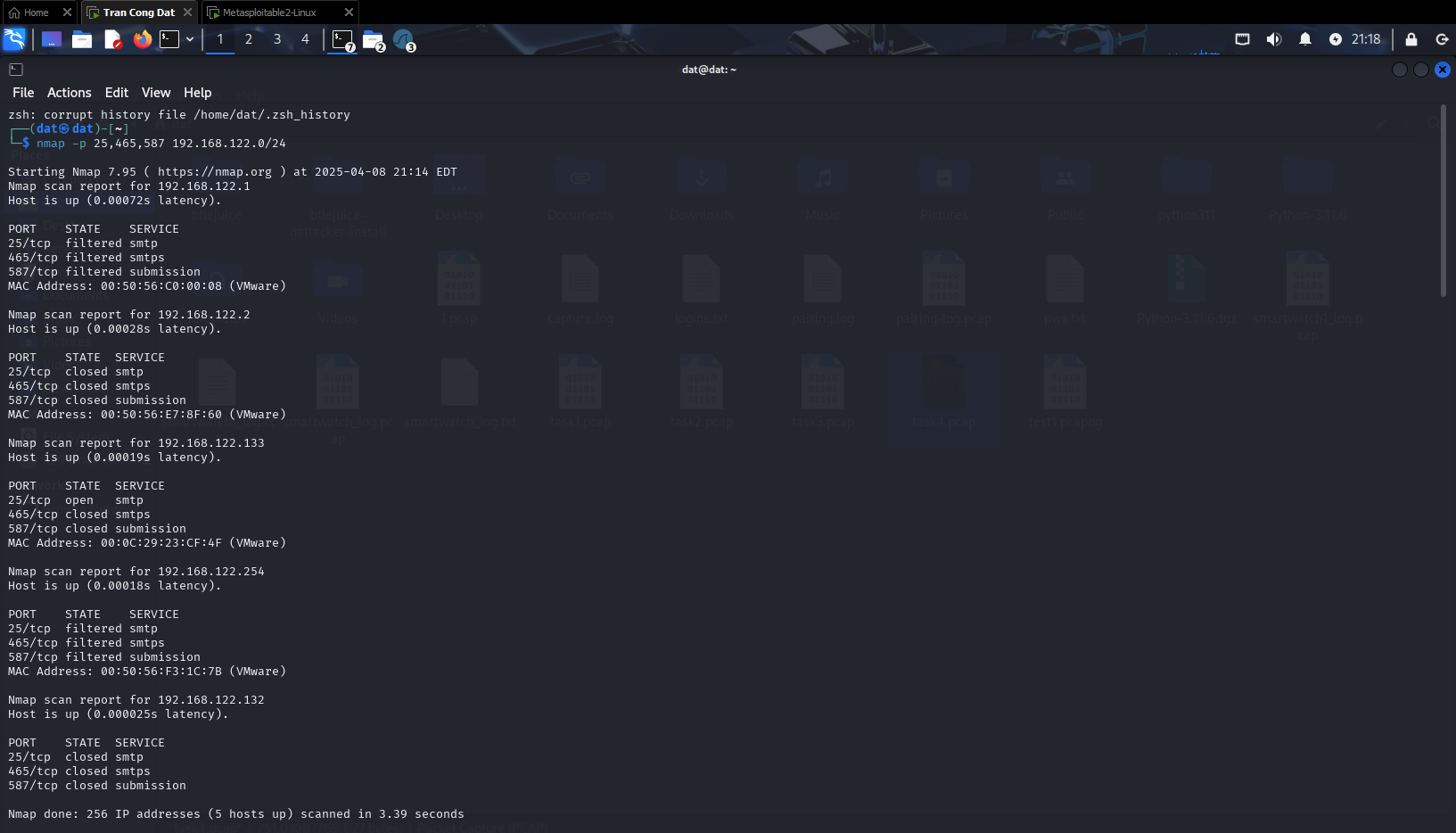
* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?

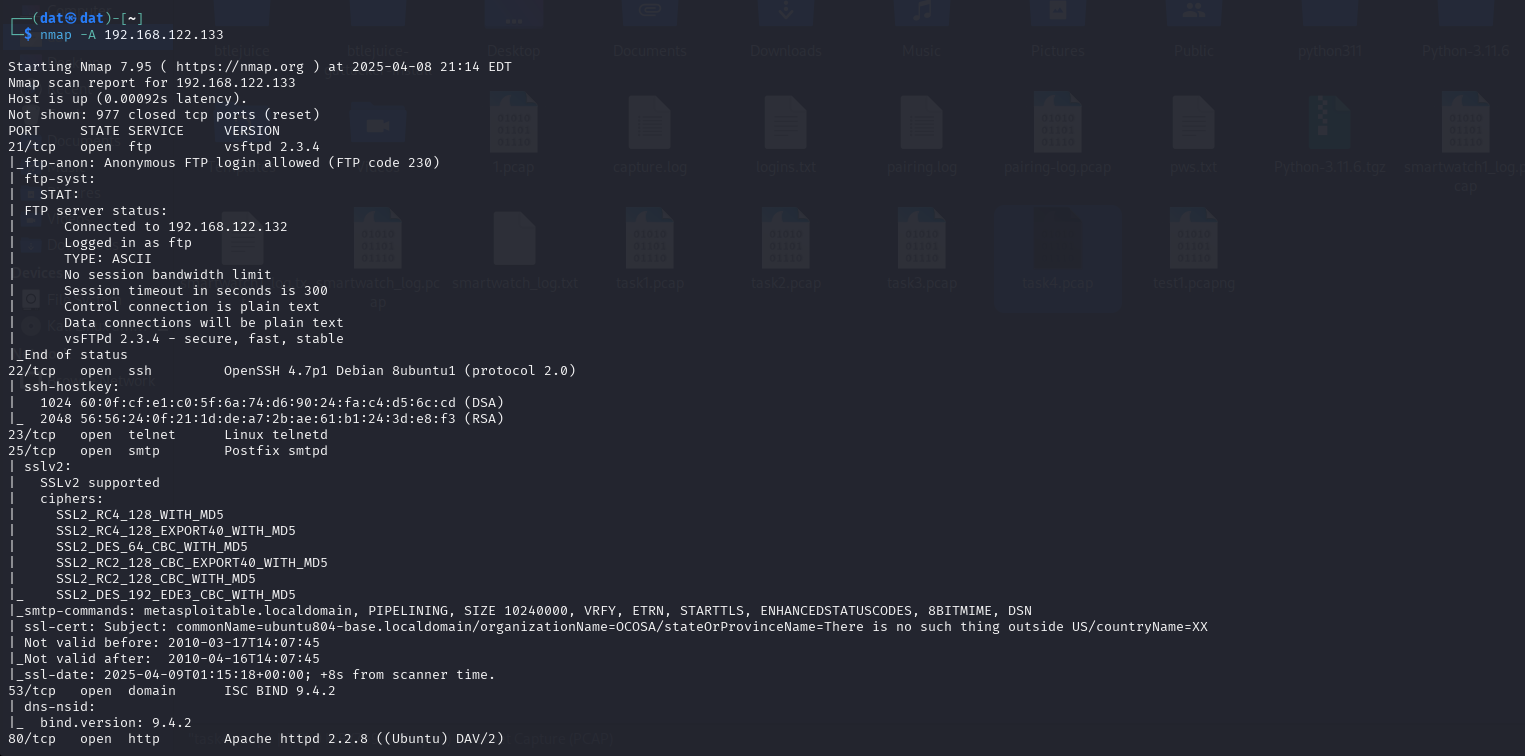


Lưu Task4 theo yêu cầu



Lọc gói theo địa chỉ IP mục tiêu ip.addr == 192.168.122.133 sau khi đã thăm dò tìm kiếm máy chủ email





Lệnh : nmap -p 25,465,587 192.168.122.0/24 là lệnh thăm dò tìm kiếm máy chủ email

|  |  |
| --- | --- |
| **Thành phần** | Ý nghĩa |
| nmap | Công cụ quét mạng, dùng để kiểm tra các cổng dịch vụ trên thiết bị. |
| -p 25,465,587 | Chỉ định quét các cổng liên quan đến dịch vụ email: |
| 25 | SMTP – dịch vụ gửi email cơ bản, thường dùng giữa các máy chủ. |
| 465 | SMTPS – phiên bản SMTP bảo mật (sử dụng SSL). |
| 587 | SMTP Submission – dùng để gửi email từ client lên server (bảo mật hơn). |
| 192.168.122.0/24 | Dải địa chỉ mạng lớp C (từ 192.168.122.1 đến 192.168.122.254), quét toàn bộ mạng để tìm máy chủ nào có các cổng này mở |

**Mục đích lệnh này**

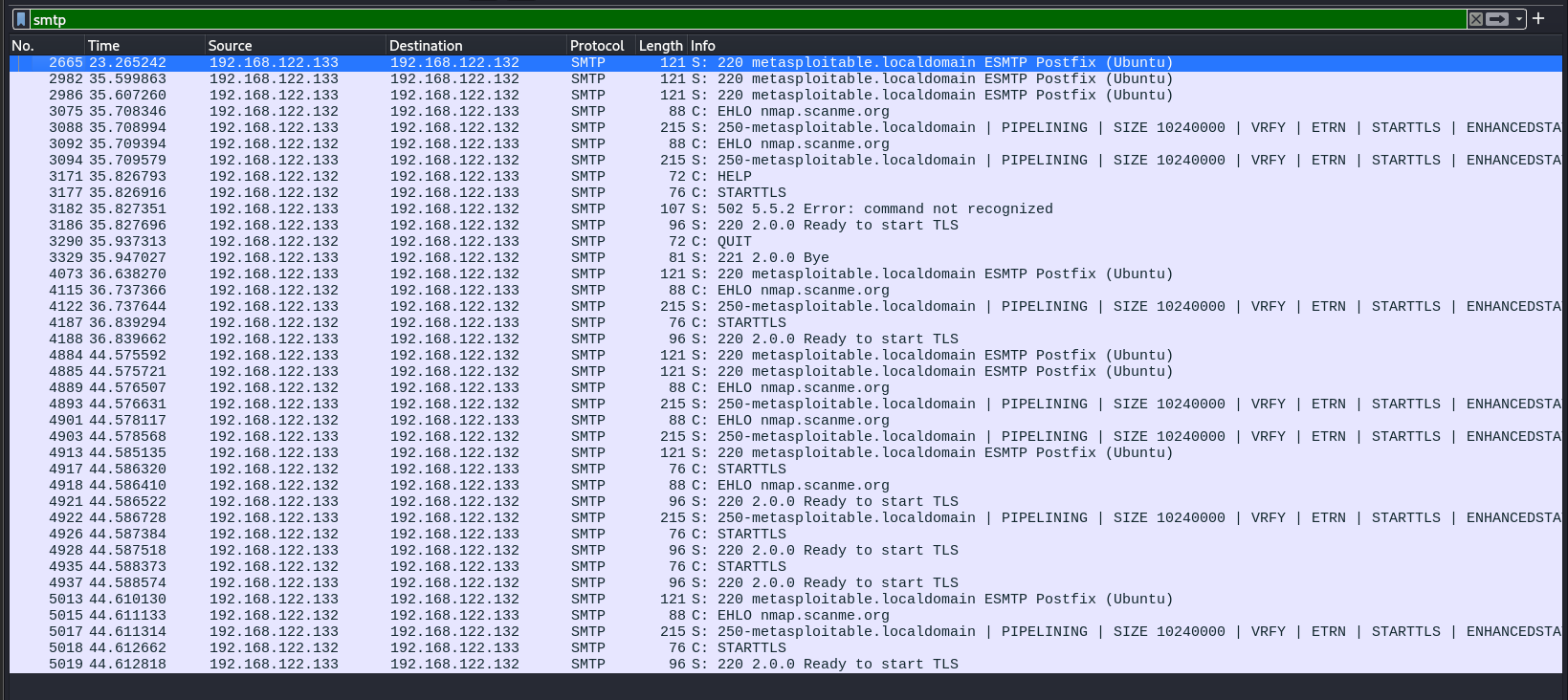
 **Xác định** trong mạng LAN có **máy nào đang cung cấp dịch vụ email**.

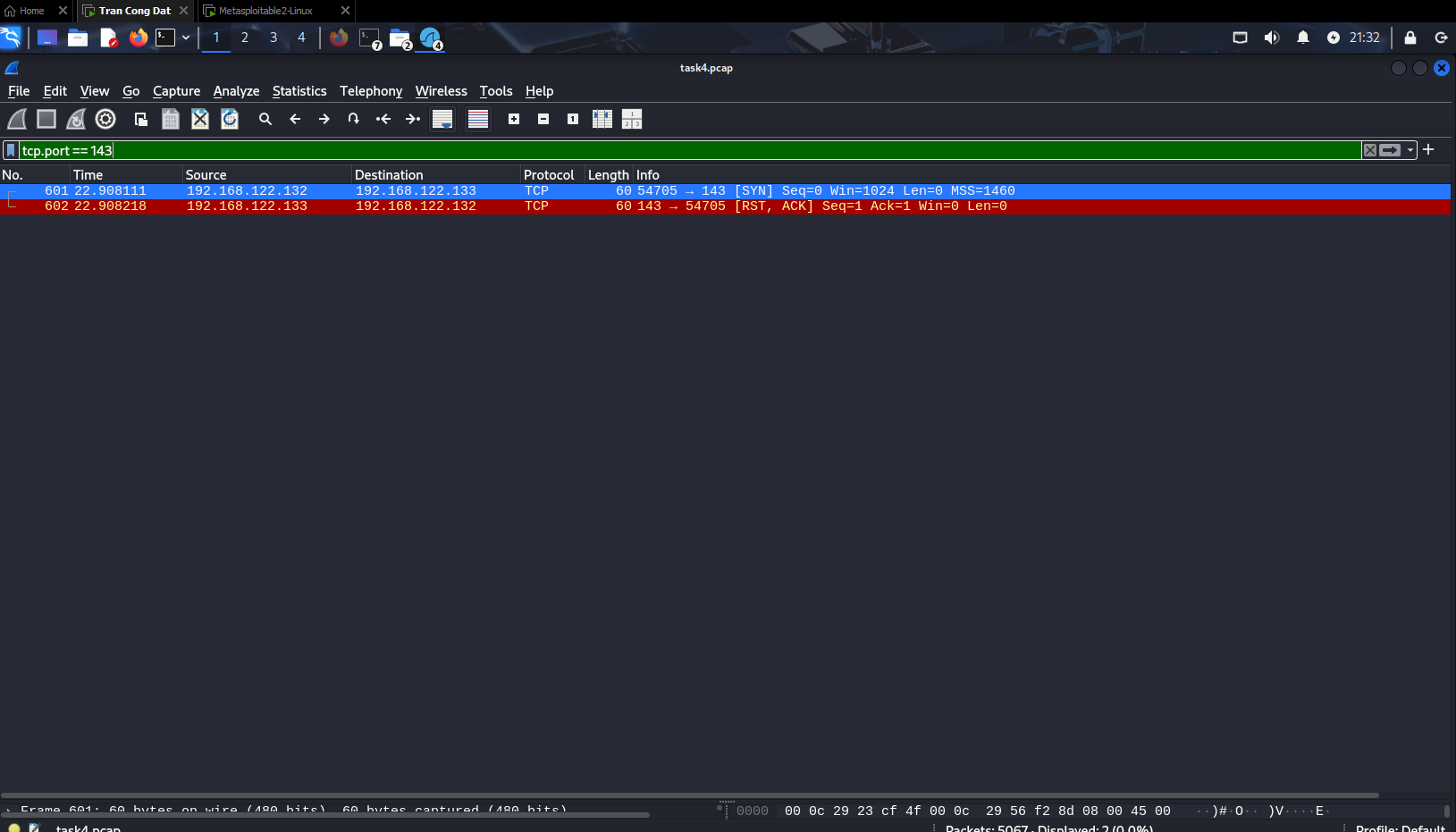
 **Hiển thị IP** của các máy có mở một trong các cổng: 25, 465, hoặc 587.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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** | Số CVE tiêu biểu | Mô tả ngắn gọn về lỗ hổng (Tiếng Việt) |
| Postfix (Ubuntu) | |  | | --- | |  |  |  | | --- | | CVE-2023-51764 | | Lỗ hổng vượt qua xác thực SMTP STARTTLS bằng cách chèn các gói lỗi (packet injection) để chiếm kết nối |
| Postfix (Ubuntu 18.04, 20.04) | CVE-2021-20177 | Cho phép tiết lộ thông tin nhạy cảm do xử lý không đúng dữ liệu trong quá trình xử lý email. |
| Postfix (nhiều phiên bản) | CVE-2020-19260 | Lỗi tràn bộ đệm có thể dẫn đến thực thi mã tùy ý trên máy chủ. |
| SMTP - Postfix (Ubuntu) | CVE-2023-51764 | Cho phép vượt qua STARTTLS bằng cách chèn gói lỗi. |
| SMTP - Postfix (Ubuntu) | CVE-2021-20177 | Rò rỉ thông tin nhạy cảm trong quá trình xử lý email. |
| SMTP - Postfix (Ubuntu) | CVE-2020-19260 | Lỗi tràn bộ đệm dẫn đến thực thi mã từ xa. |
| IMAP (port 143) | Không có dịch vụ | Port 143 bị từ chối kết nối, không có dịch vụ hoạt động. |
| POP3 (port 110) | Không có dịch vụ | Port 110 bị từ chối kết nối, không có dịch vụ hoạt động |