**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

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

Họ và tên sinh viên:Trần Minh Hợp

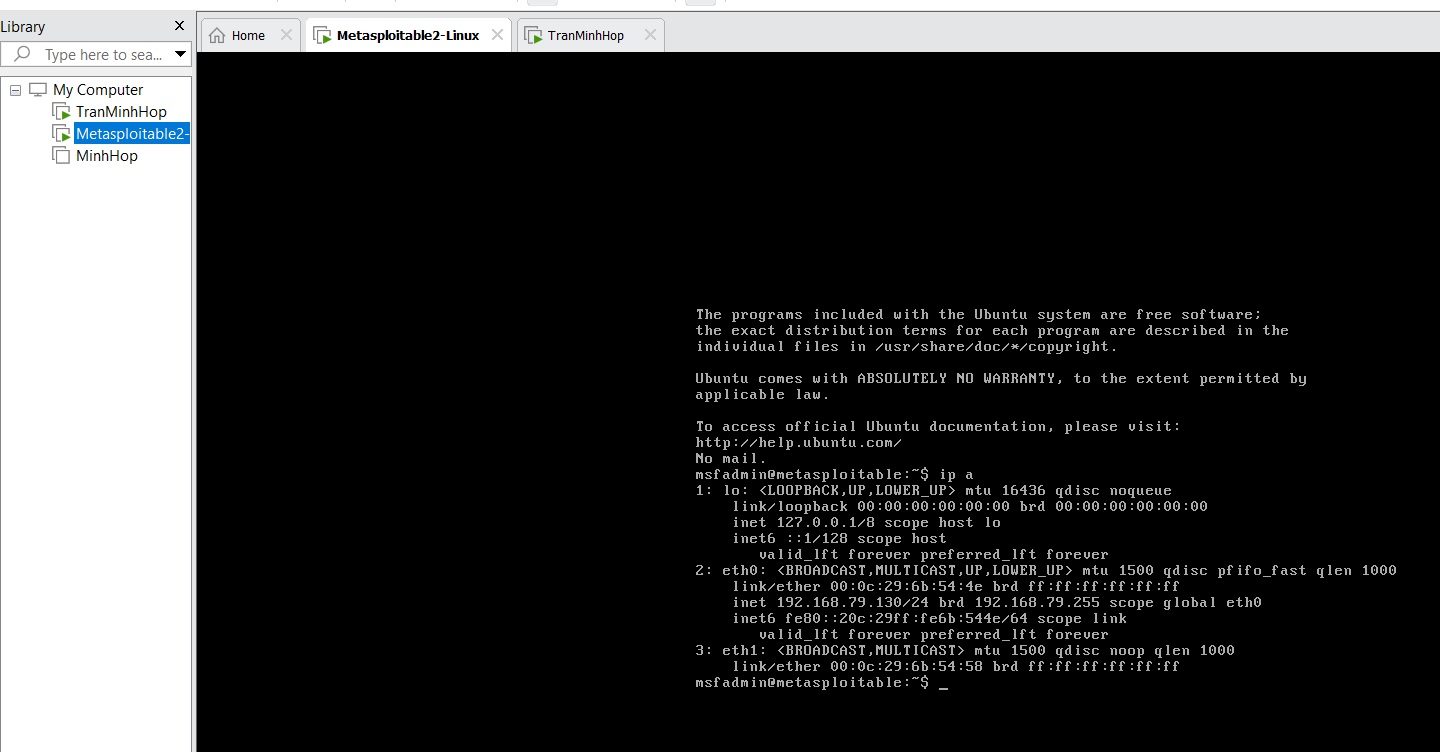
MSSV:1050080180

KẾT QUẢ THỰC HÀNH

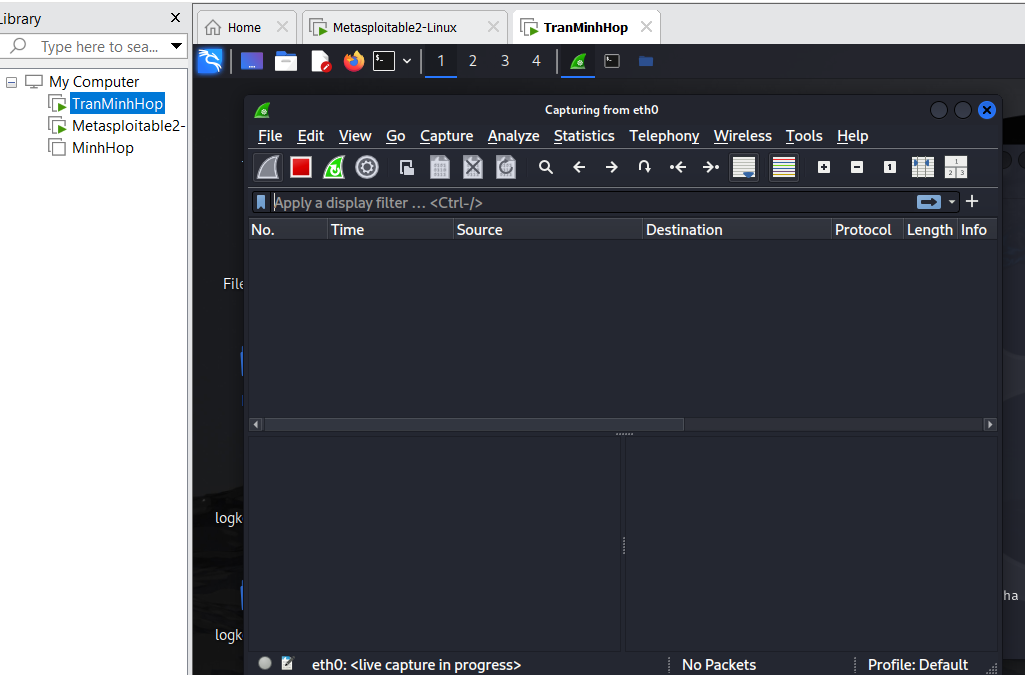
1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

1.1. Kịch bản 1

- Bước 1: Truy cập máy ảo Attack



- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

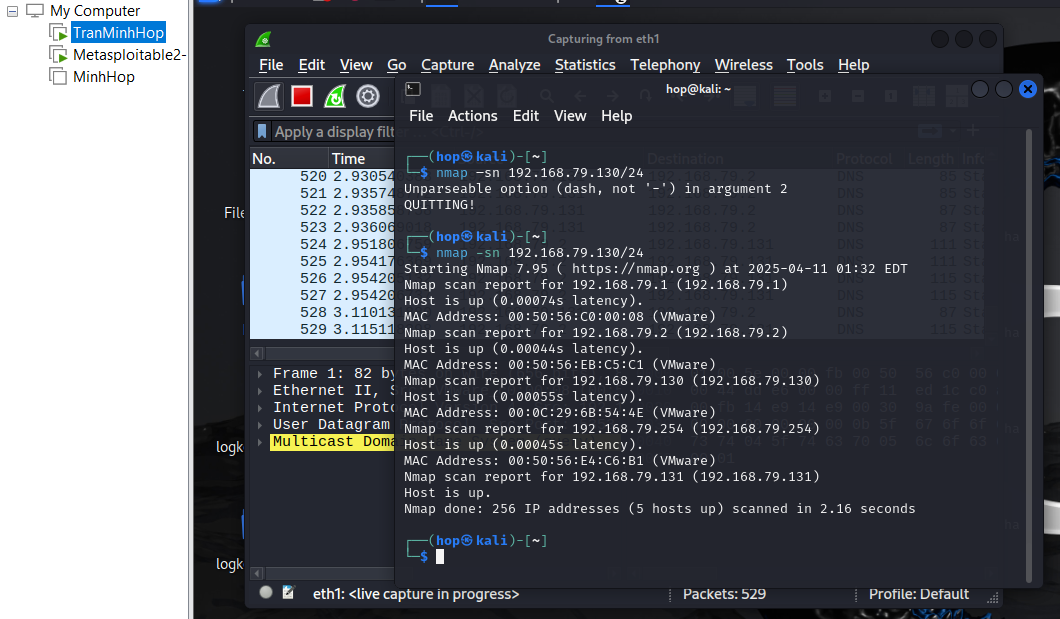


- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

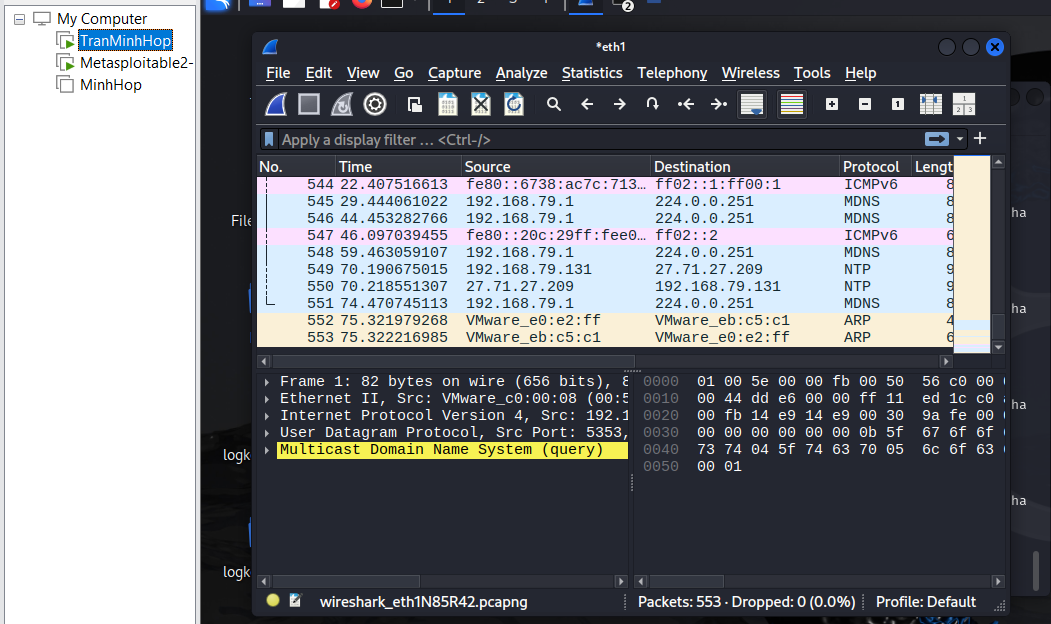
nmap -sn 192.168.79.130/24

- Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự

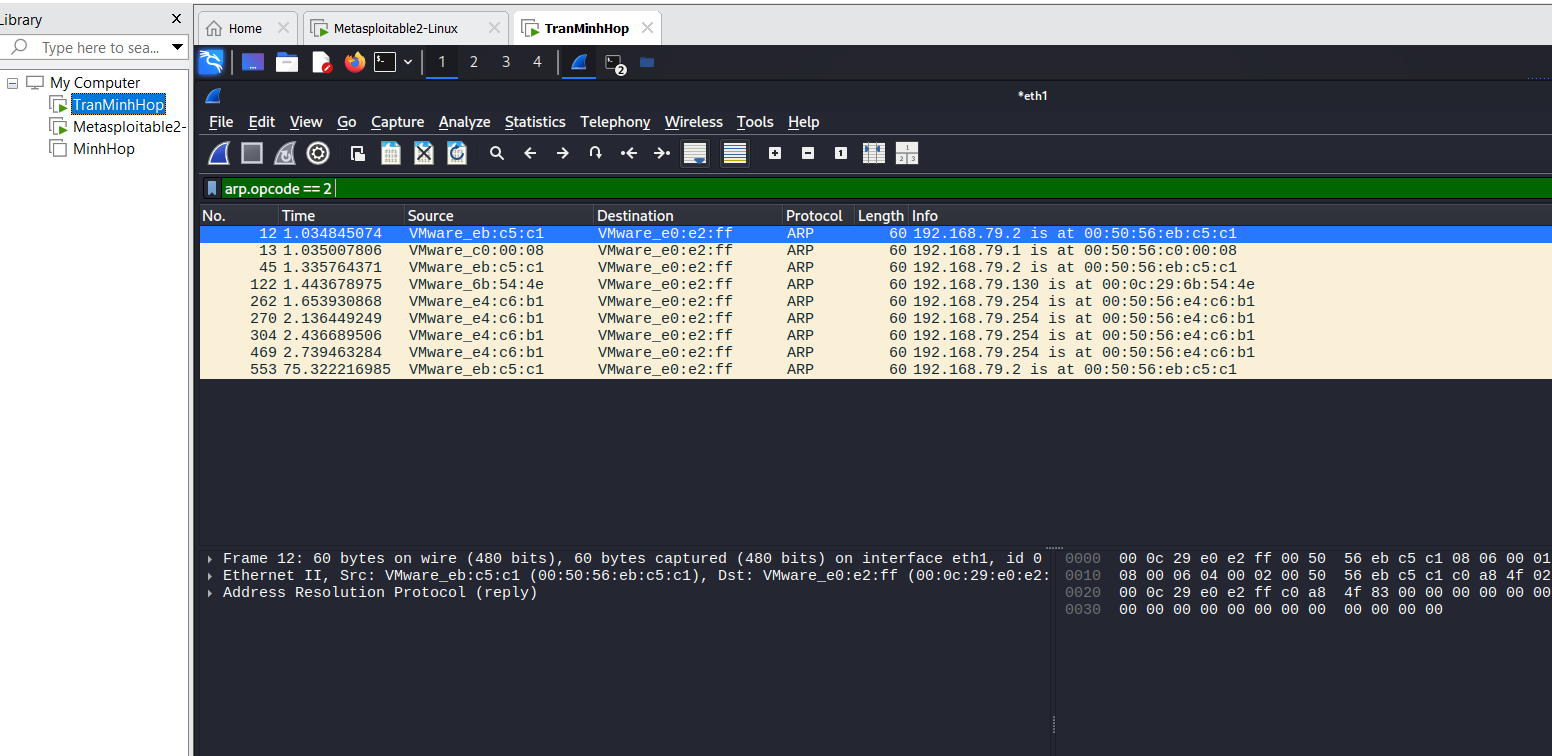
như sau:



Bước 5: Dừng bắt gói tin trên Wireshark



Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2



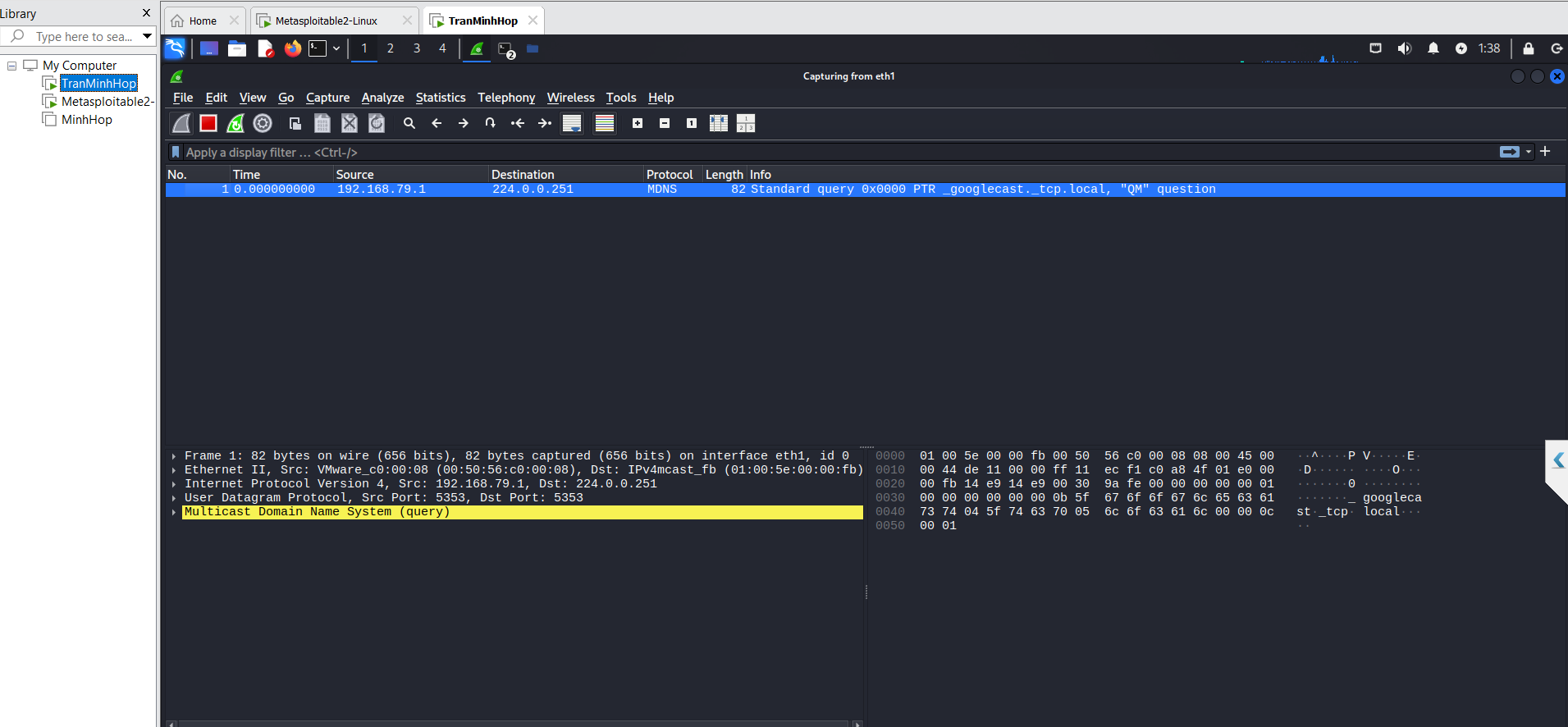
2.2. Quét thăm dò dịch vụ

Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang

cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

- Bước 1: Truy cập máy ảo Attack

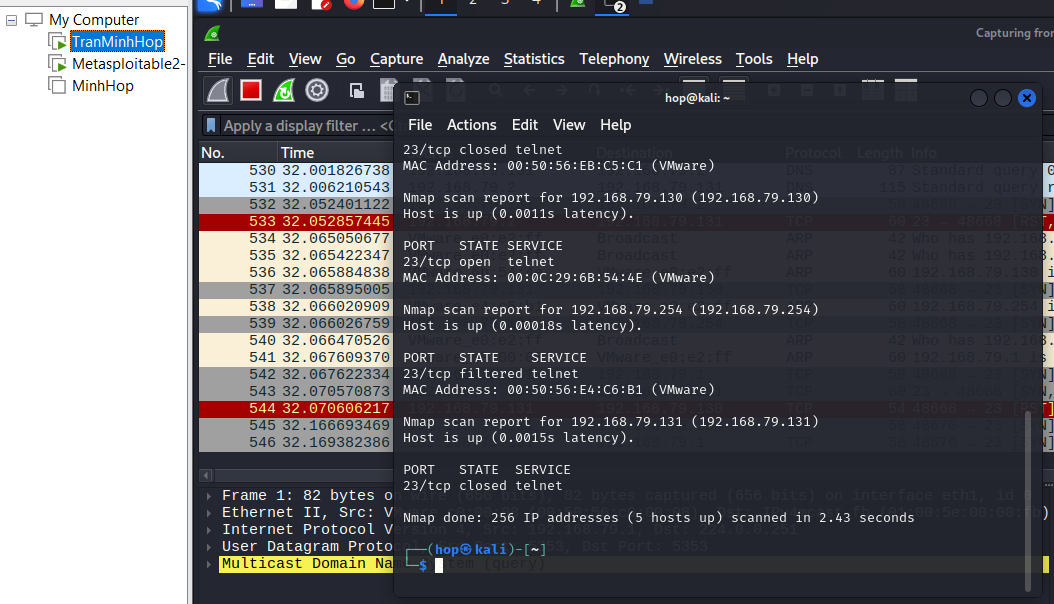
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.



- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

sudo nmap -p 23 192.168.79.130/24

- Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng



Nmap scan report for 192.168.79.130 (192.168.79.130)

Host is up (0.0011s latency).

PORT STATE SERVICE

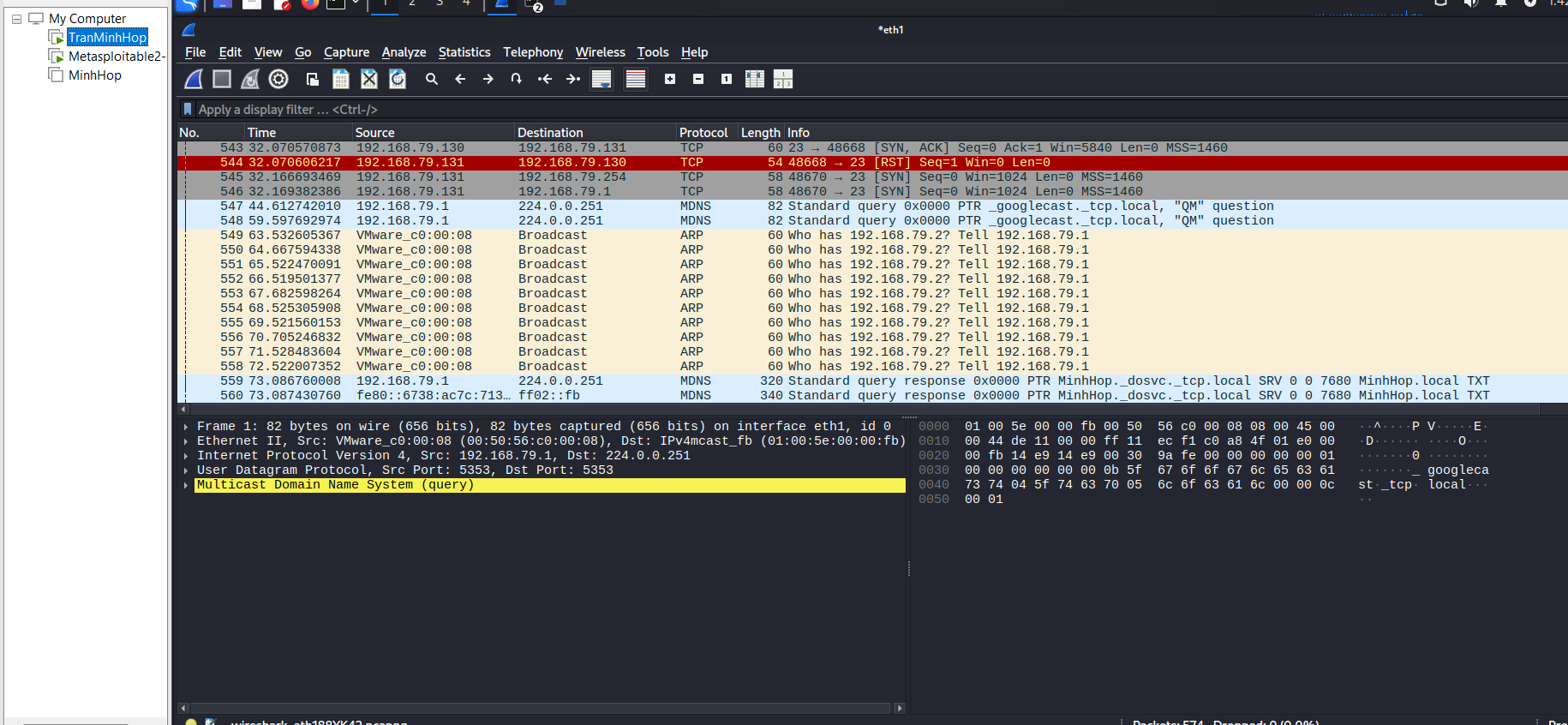
23/tcp open telnet

MAC Address: 00:0C:29:6B:54:4E (VMware)

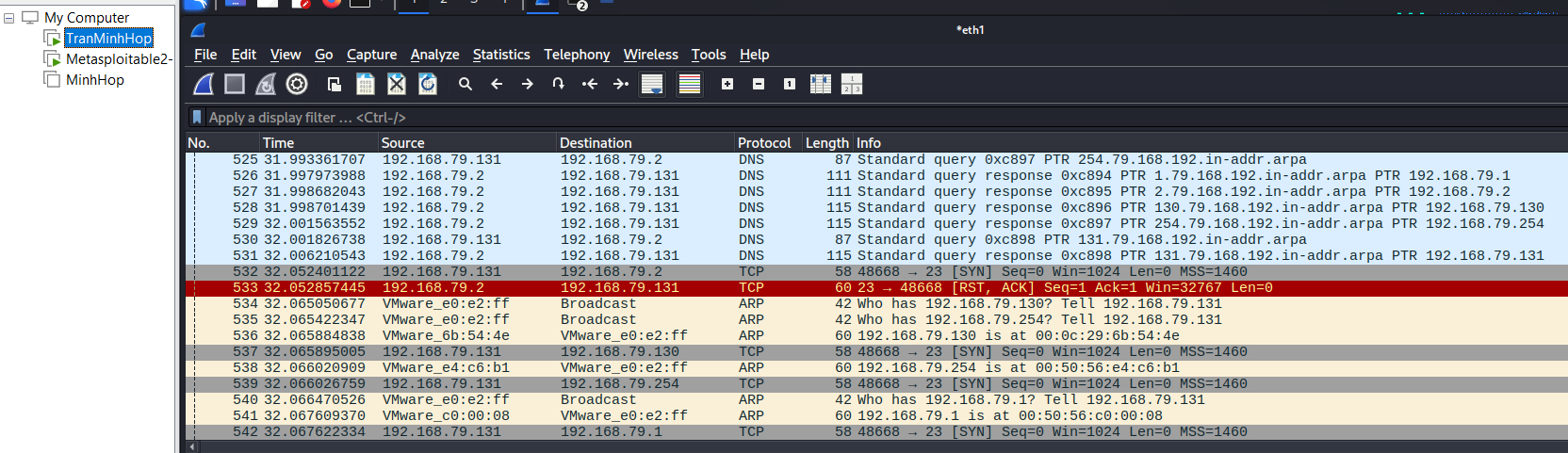
192.168.79.130 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể

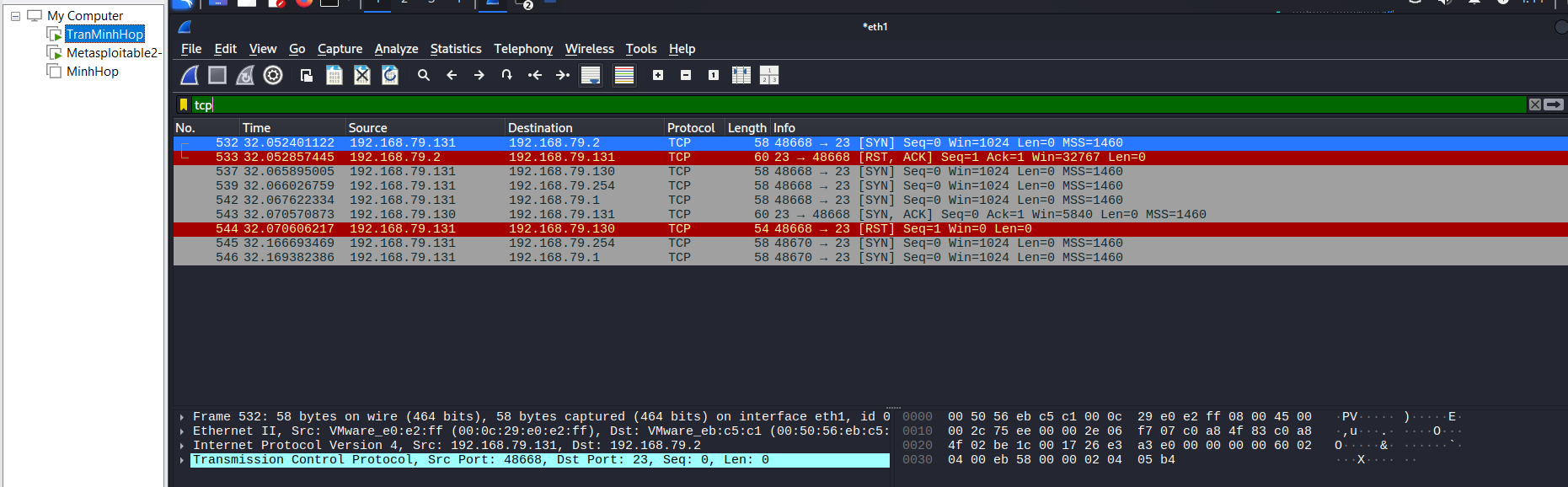
phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

- Bước 5: Dừng bắt gói tin trên Wireshark



Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 23 của các máy đang hoạt động.

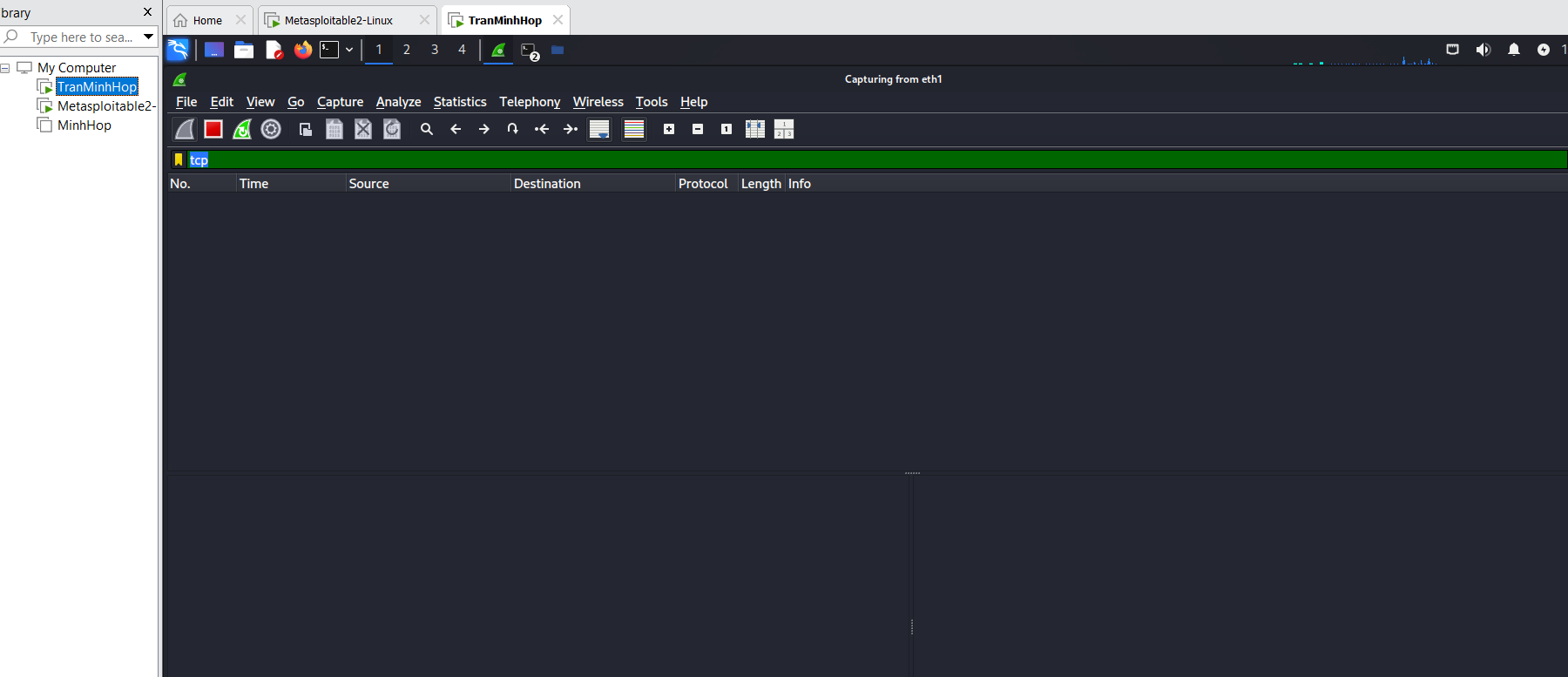


- Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.79.131 về máy tấn công. 

2.3. Quét cổng dịch vụ

- Bước 1: Truy cập máy ảo Attack

- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

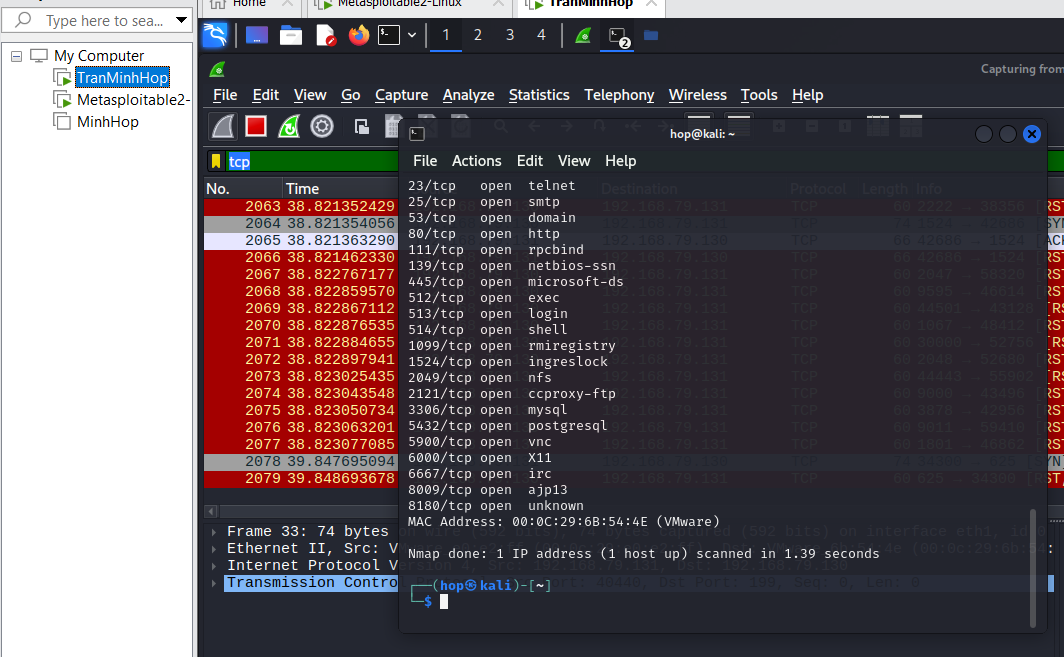


- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

nmap -sT 192.168.79.130

- Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 22, 23, 53…

trên máy mục tiêu 192.168.79.130 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.



- Bước 5: Dừng bắt gói tin trên Wireshark

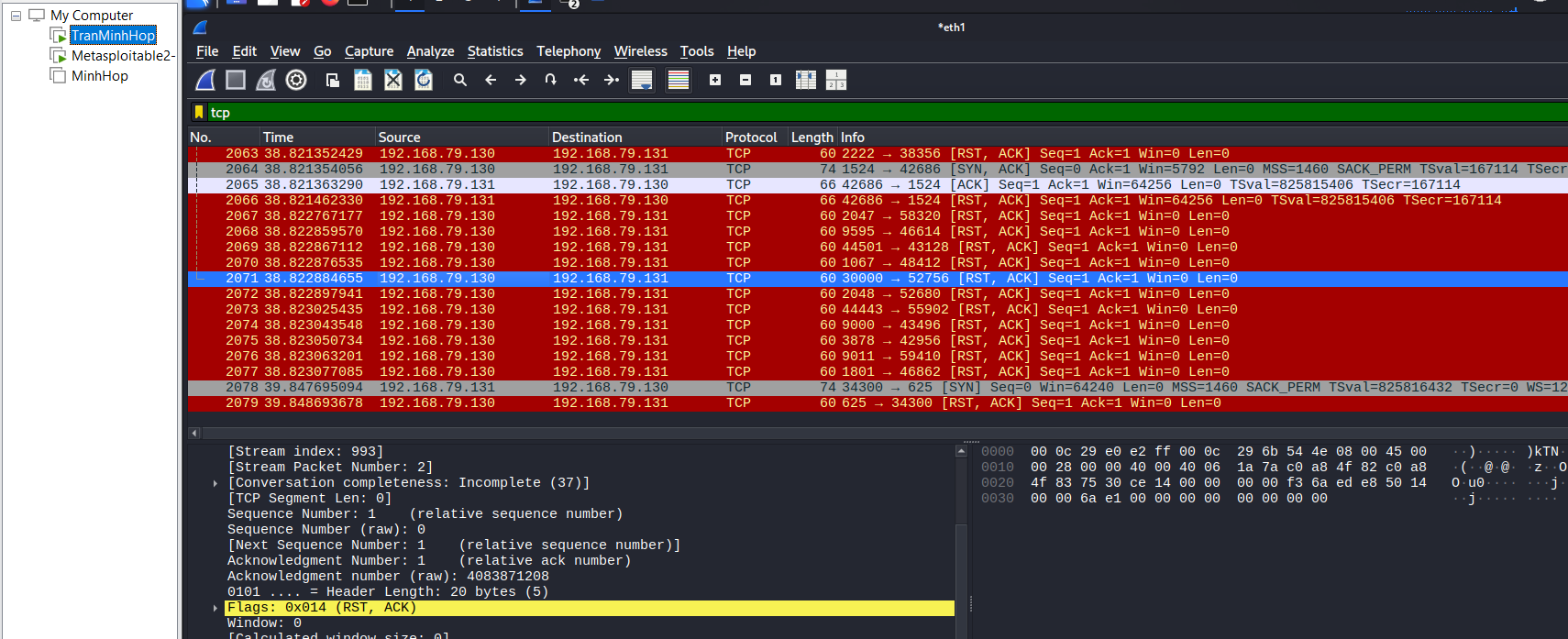
Phân tích lưu lượng:

- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra

máy mục tiêu 192.168.79.130 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói

tin TCP SYN được gửi từ máy tấn công ( 192.168.79.131) tới máy mục tiêu là 192.168.79.130.

Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.

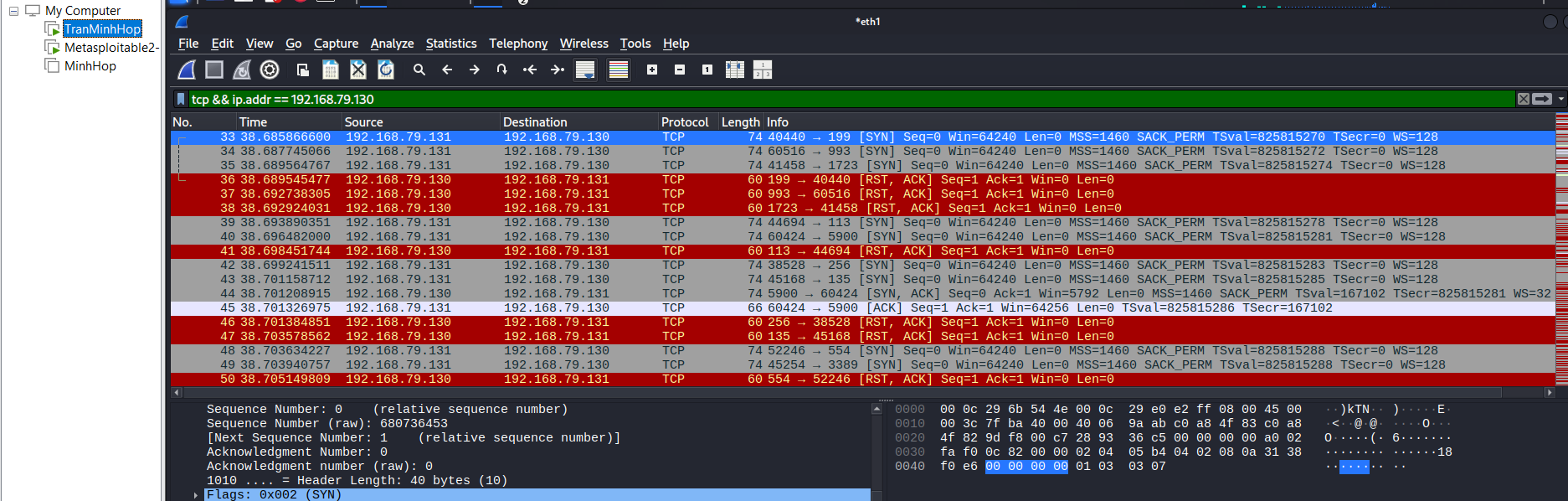


Sử dụng giá trị tcp && ip.addr == 192.168.79.130 ta lọc được các gói tin TCP. Có thể nhận

thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 12, 16, 17 của quá trình bắt tay 3

bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin

1. để hủy kết nối này.

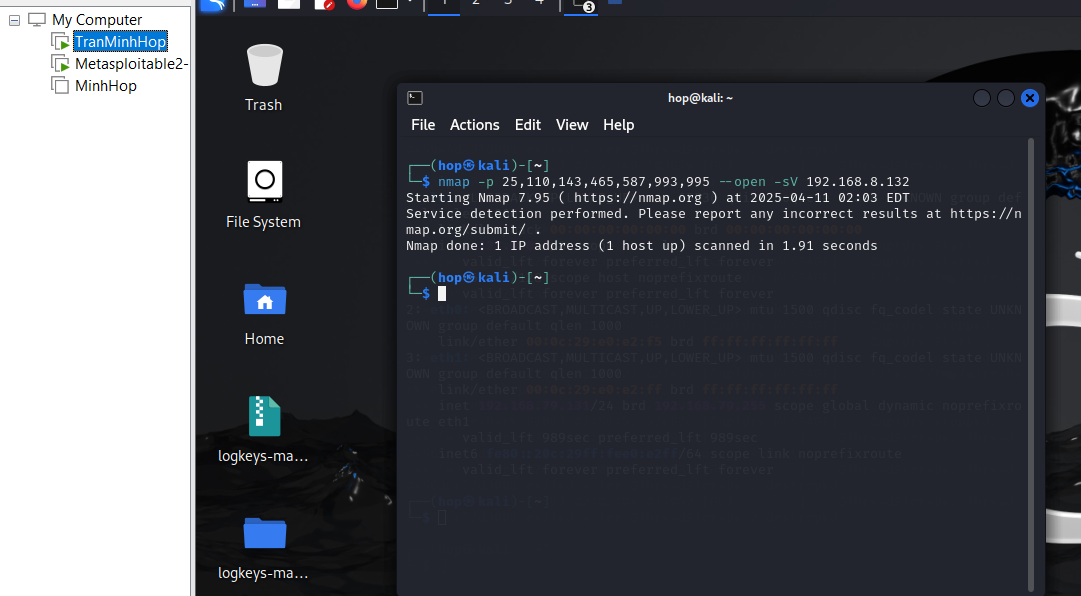


**2.Thu thập thông tin hệ thống**

**Lệnh quét thăm dò tìm kiếm máy chủ email**

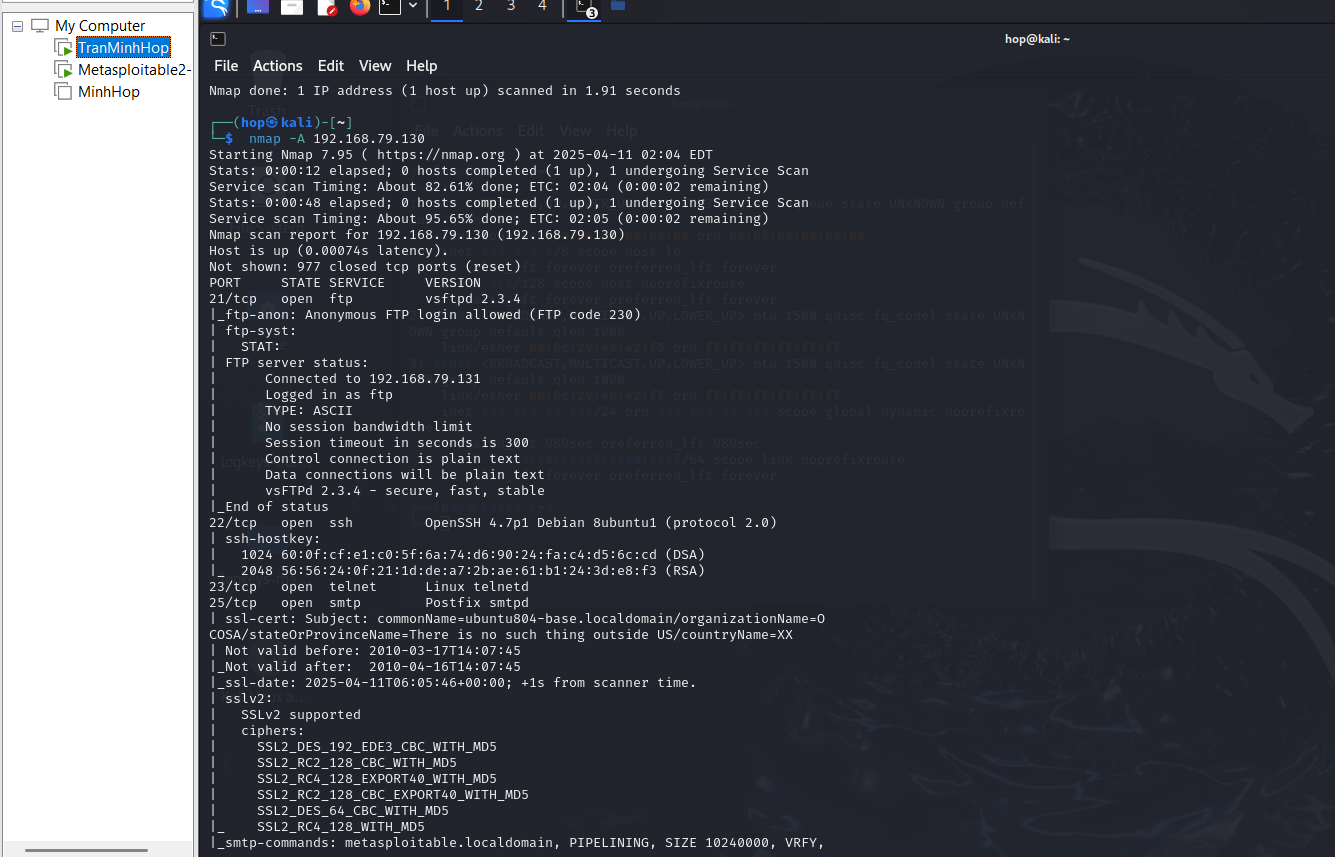
**nmap -p 25,110,143,465,587,993,995 --open -sV 192.168.8.132**

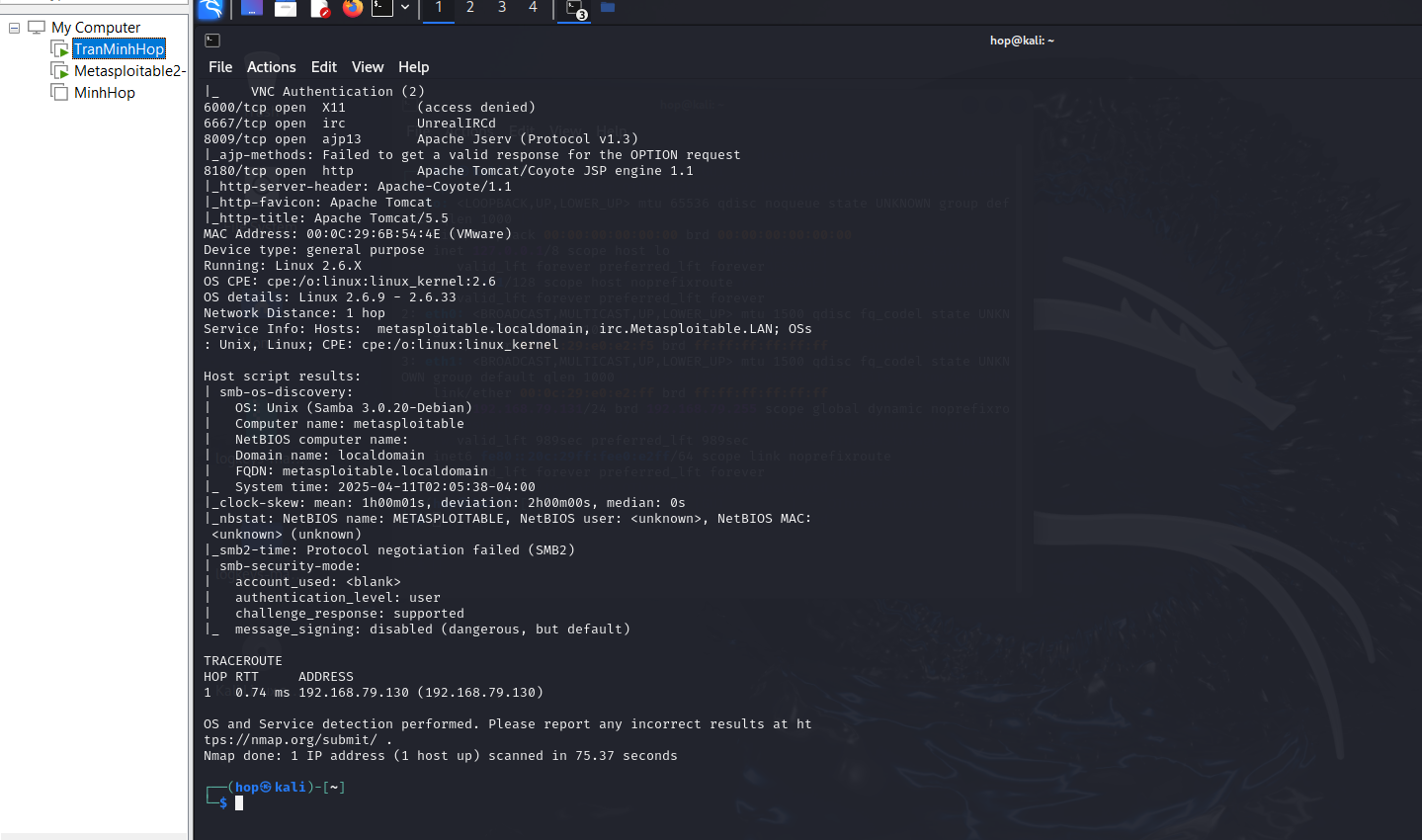
|  |  |
| --- | --- |
| Tham số | Ý nghĩa |
| nmap | Công cụ quét mạng để thăm dò các thiết bị và dịch vụ đang hoạt động |
| -p 25,110,143,465,587,993,995 | Chỉ định các cổng của dịch vụ email cần quét: • 25 – SMTP (Simple Mail Transfer Protocol) • 110 – POP3 (Post Office Protocol v3) • 143 – IMAP (Internet Message Access Protocol) • 465, 587 – SMTP sử dụng SSL/TLS • 993 – IMAP qua SSL • 995 – POP3 qua SSL |
| --open | Chỉ hiển thị các host có cổng đang mở |
| -sV | Kích hoạt tính năng version detection: xác định tên dịch vụ và phiên bản đang chạy trên cổng |
| 192.168.8.0/24 | Mạng con cần quét (từ 192.168.8.1 đến 192.168.8.254) |



**-Thông tin hệ điều hành:** **nmap -A 192.168.79.130**

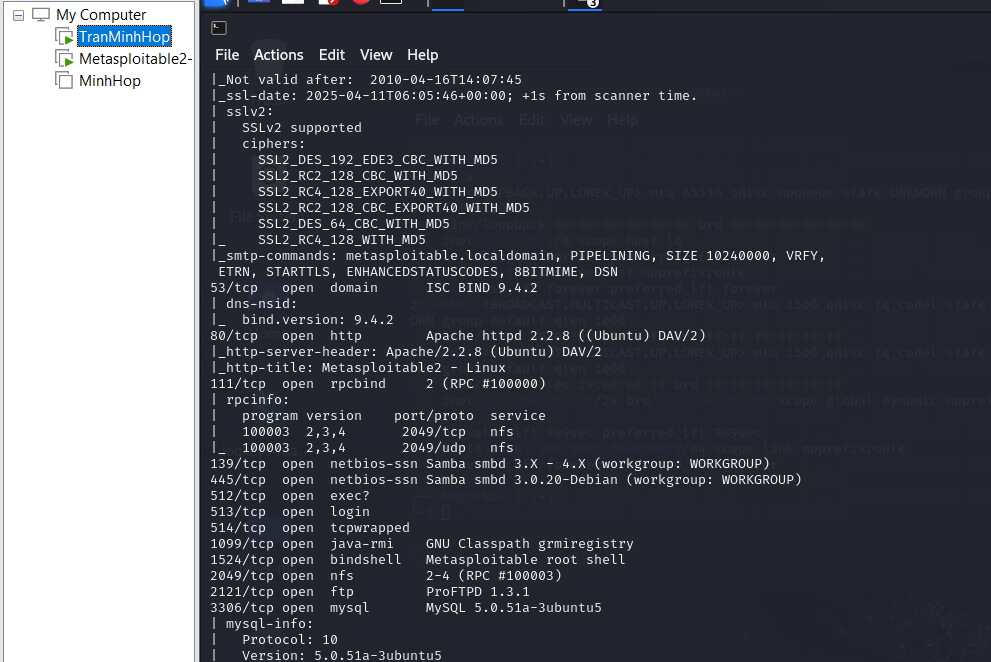
Hình ảnh chụp kết quả của nmap:





* Nêu tên và phiên bản hệ điều hành:
* **hệ điều hành Linux phiên bản kernel 2.6.9.**

**Thông tin dịch vụ:**



|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên dịch vụ | Số hiệu cổng | Tên phần mềm & Phiên bản |
| 1 | netbios-ssn | 139/tcp | Samba smbd 3.X - 4.X |
| 2 | netbios-ssn | 445/tcp | Samba smbd 3.0.20-Debian |
| 3 | exec? | 512/tcp | - |
| 4 | login | 513/tcp | - |
| 5 | tcpwrapped | 514/tcp | - |
| 6 | java-rmi | 1099/tcp | GNU Classpath grmiregistry |
| 7 | bindshell | 1524/tcp | Metasploitable root shell |
| 8 | nfs | 2049/tcp | 2-4 (RPC #100003) |
| 9 | ftp | 2121/tcp | ProFTPD 1.3.1 |
| 10 | mysql | 3306/tcp | MySQL 5.0.51a-3ubuntu5 |

**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.

Dựa vào kết quả quét ở phần 2, hãy lập báo cáo ngắn gọn về các lỗ hổng đã được công bố trên

các phần mềm cung cấp dịch vụ. Thông tin về các lỗ hổng có thể tìm kiếm trên

https://www.cvedetails.com/

Bước 1: Truy cập website: <https://www.cvedetails.com/>

Bước 2: Tìm kiếm các tên phần mềm ở phần 2

|  |  |  |
| --- | --- | --- |
| Phần mềm dịch vụ | Số CVE | Mô tả ngắn gọn về lỗ hổng |
| Samba smbd 3.X - 4.X | CVE-2015-5252 | Cho phép kẻ tấn công từ xa vượt qua hạn chế truy cập tệp bằng cách sử dụng symlink trỏ ra ngoài thư mục chia sẻ.  <https://www.cvedetails.com/cve/CVE-2015-5252/> |
| Samba smbd 3.X - 4.X | CVE-2015-7560 | Cho phép người dùng xác thực từ xa sửa đổi ACL tùy ý bằng cách sử dụng cuộc gọi SMB1 UNIX và non-UNIX. <https://www.cvedetails.com/cve/CVE-2015-7560/> |
| Samba smbd 3.X - 4.X | CVE-2015-0240 | Thực hiện thao tác free trên con trỏ chưa được khởi tạo, cho phép thực thi mã tùy ý qua các gói Netlogon được tạo đặc biệt. <https://www.cvedetails.com/cve/CVE-2015-0240/> |
| Samba smbd 3.X - 4.X | CVE-2013-4124 | Tràn số nguyên trong hàm read\_nttrans\_ea\_list, cho phép kẻ tấn công gây ra từ chối dịch vụ (DoS) qua gói tin bị định dạng sai. <https://www.cvedetails.com/cve/CVE-2013-4124/> |
| Samba smbd 3.X - 4.X | CVE-2010-0926 | Cấu hình mặc định cho phép người dùng xác thực từ xa truy cập tệp tùy ý bằng cách sử dụng lệnh symlink chứa chuỗi "..". <https://www.cvedetails.com/cve/CVE-2010-0926/> |
| Samba smbd 3.X - 4.X | CVE-2007-2447 | Cho phép thực thi lệnh tùy ý thông qua cấu hình "username map script" không mặc định.  <https://www.cvedetails.com/cve/CVE-2007-2447/> |
| ProFTPD 1.3.1 | CVE-2009-0543 | Cho phép kẻ tấn công từ xa vượt qua cơ chế bảo vệ SQL injection qua các ký tự đa byte được mã hóa không hợp lệ.  <https://www.cvedetails.com/cve/CVE-2009-0543/> |
| ProFTPD 1.3.1 | CVE-2010-3867 | Lỗ hổng traversal trong module mod\_site\_misc cho phép người dùng xác thực từ xa tạo, xóa thư mục và symlink thông qua chuỗi traversal. <https://www.cvedetails.com/cve/CVE-2010-3867/> |
| ProFTPD 1.3.1 | CVE-2011-4130 | Lỗi use-after-free trong Response API cho phép người dùng xác thực từ xa thực thi mã tùy ý sau khi xảy ra lỗi trong quá trình truyền dữ liệu FTP. <https://www.cvedetails.com/cve/CVE-2011-4130/> |
| ProFTPD 1.3.1 | CVE-2008-4242 | Cho phép kẻ tấn công thực hiện tấn công CSRF và thực thi lệnh FTP tùy ý thông qua URI ftp:// dài. <https://www.cvedetails.com/cve/CVE-2008-4242/> |