BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên:Hoàng Văn Thái***

***MSSV: 1050080074***

***Yêu cầu kết quả thực hành:***

**KẾT QUẢ THỰC HÀNH**

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

**Quét thăm dò mạng**

Bước 1: Truy cập máy ảo Attack

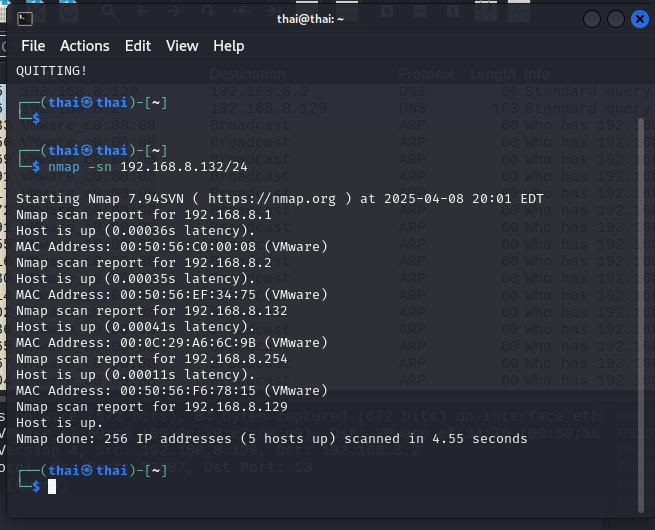
Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

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

nmap –sn 192.168.8.132/24

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

như sau:

****

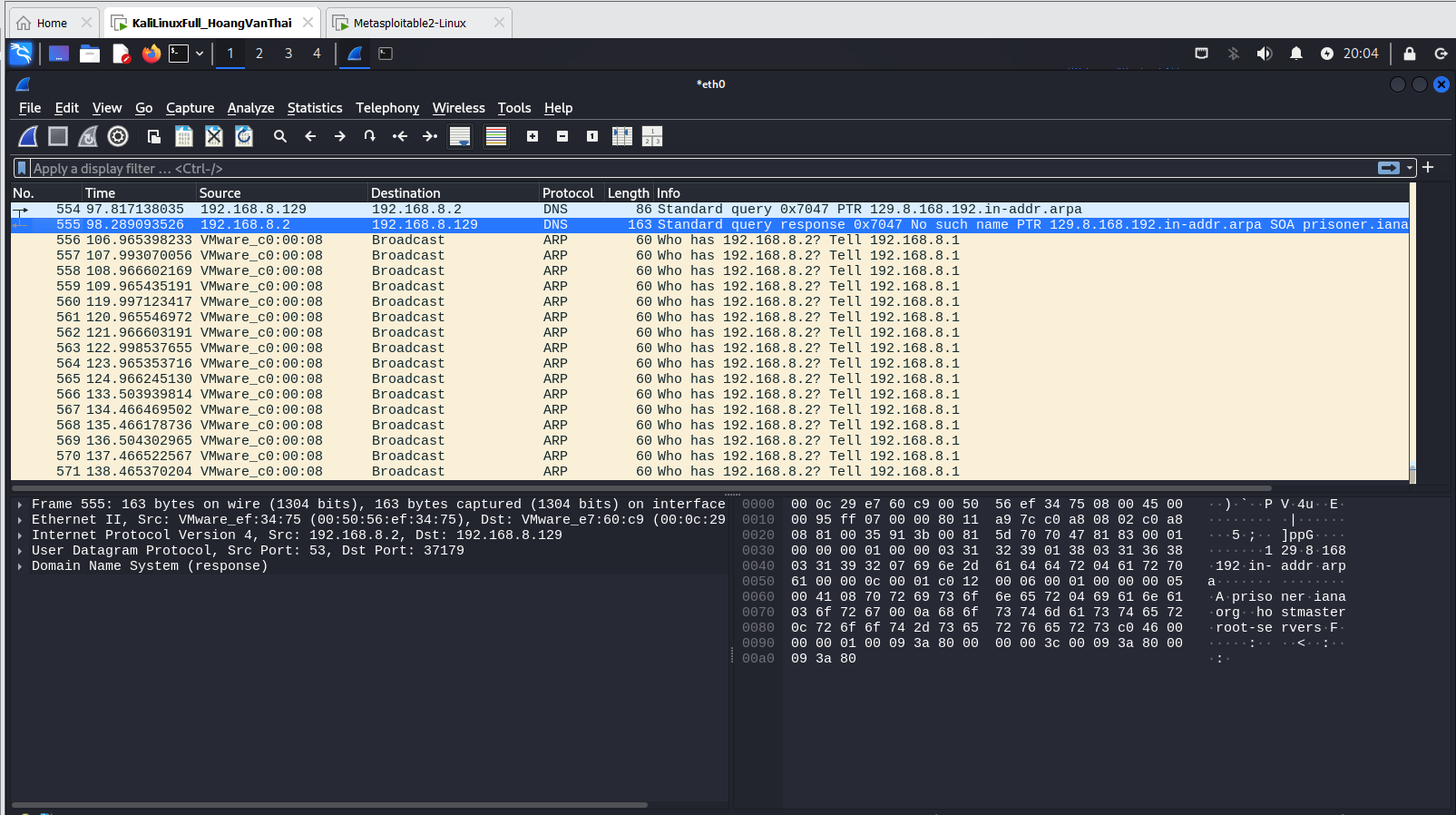
Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

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

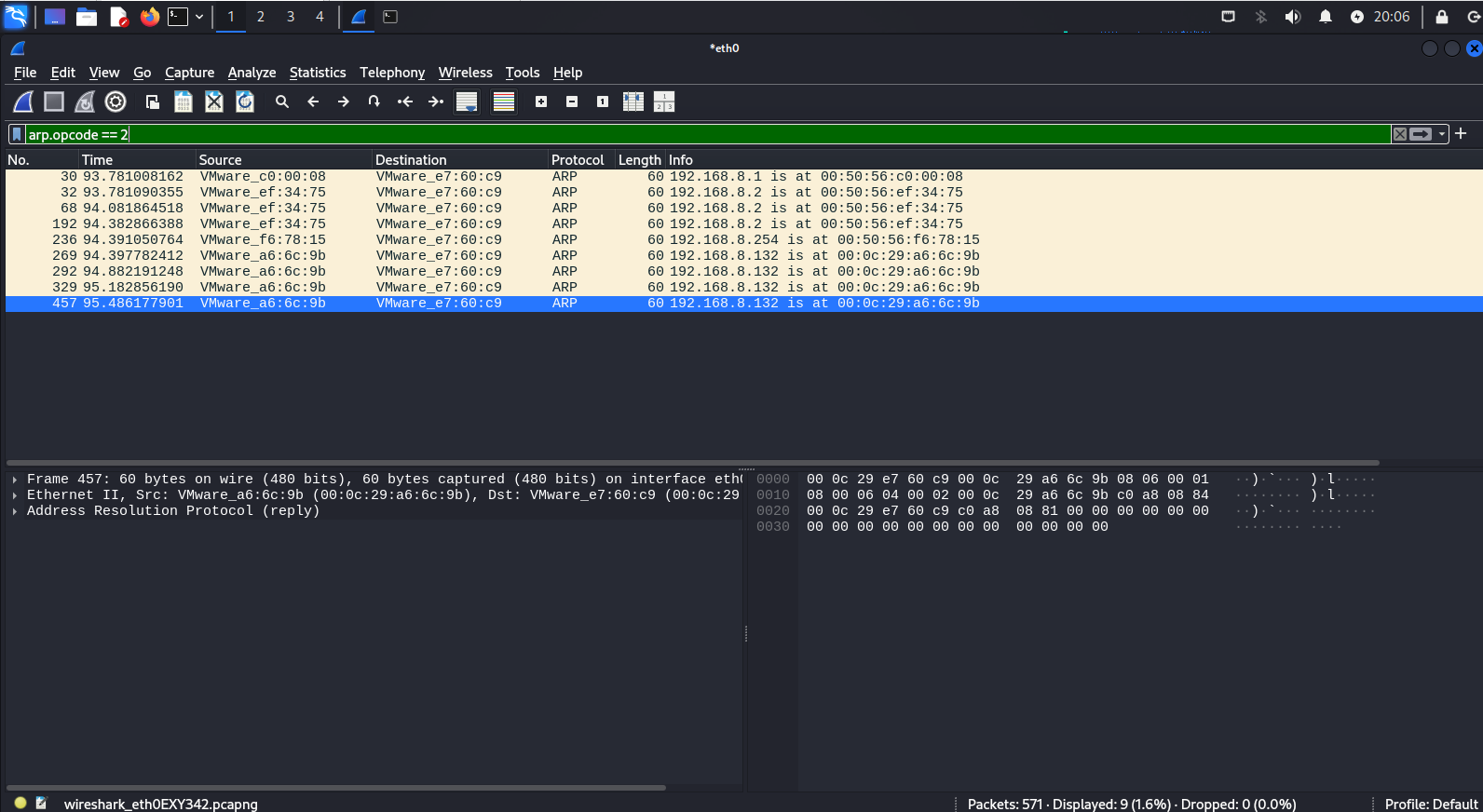
trong mạng 192.168.8.132/24

****

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

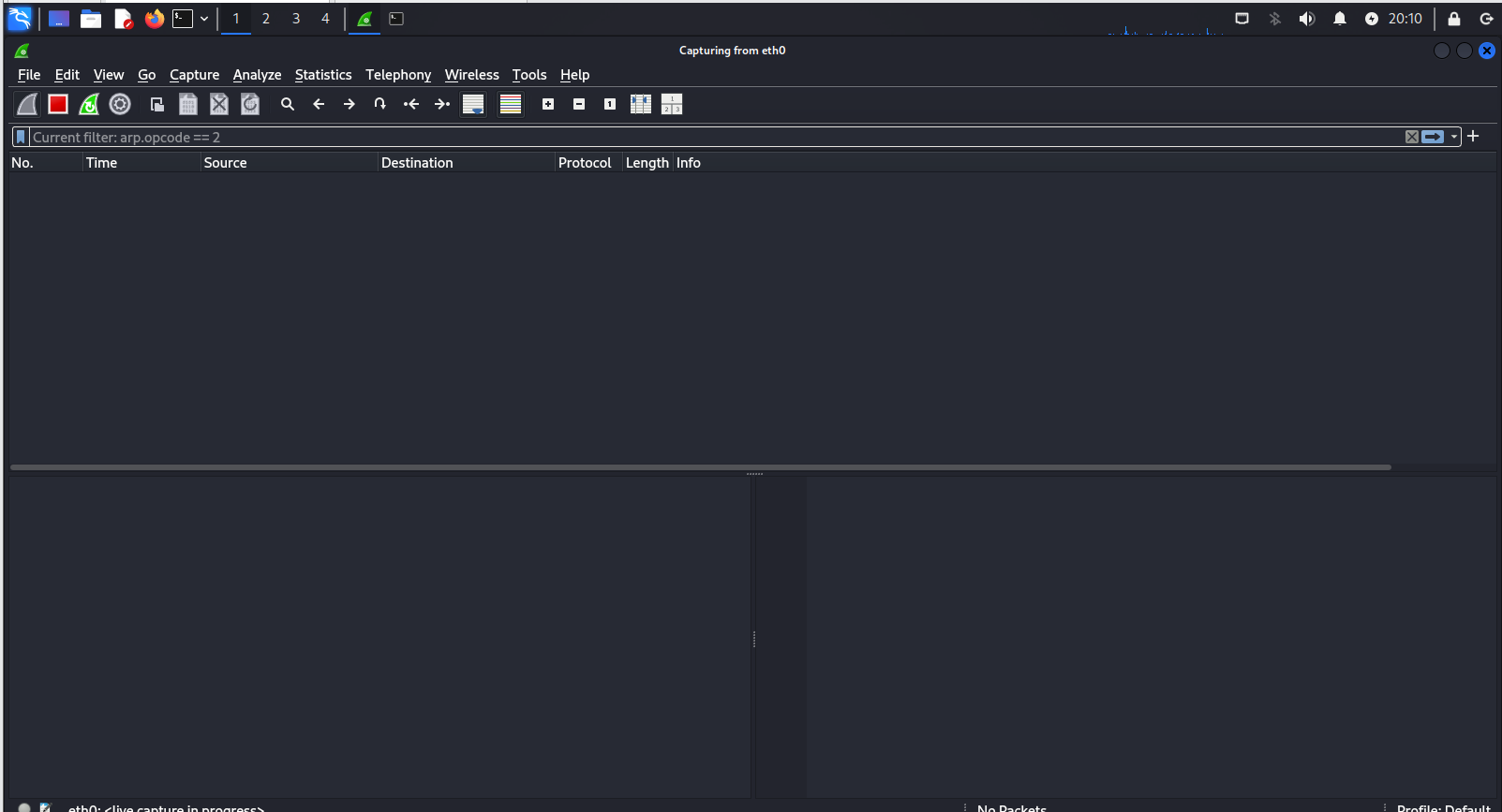
phát hiện các nút mạng đang hoạt động trong mạng.

* 1. **Kịch bản 2**

**Quét thăm dò 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.

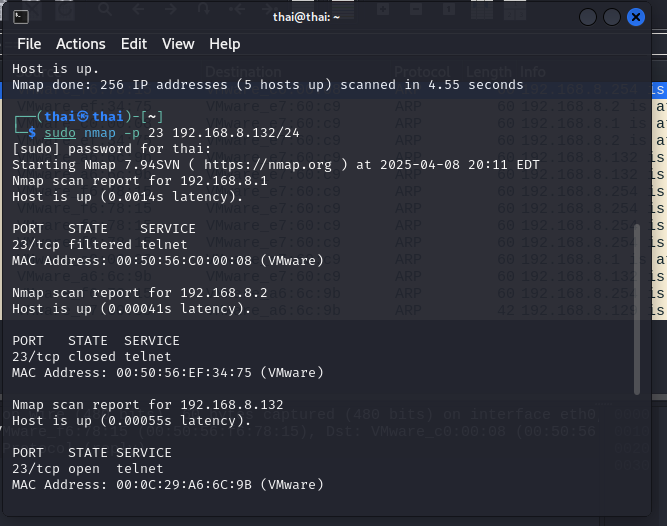


- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**sudo nmap -p 23 192.168.8.132/24**

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

192.168.8.132và 192.168.8.2 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể

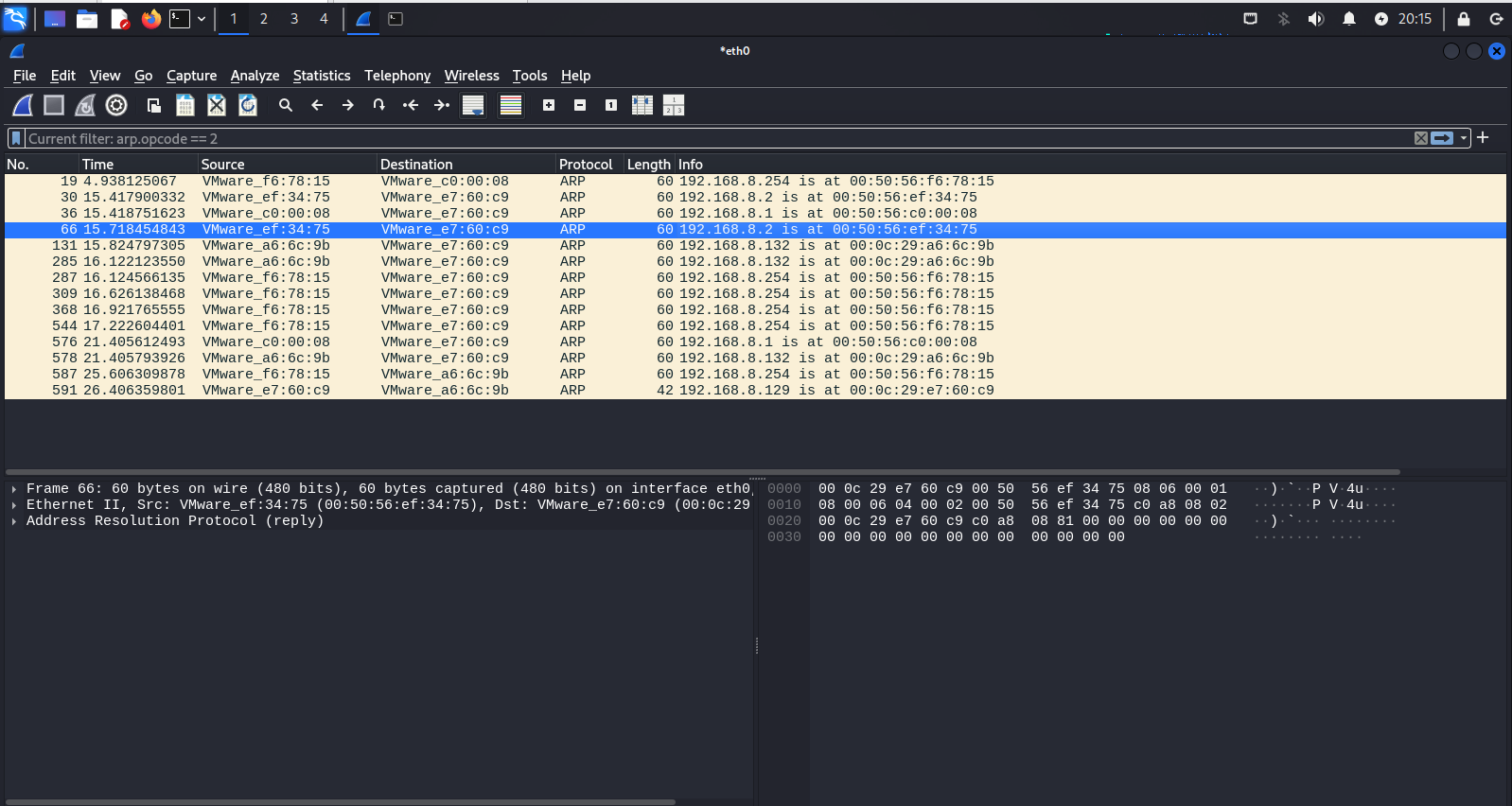


Phân tích lưu lượng:

- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể

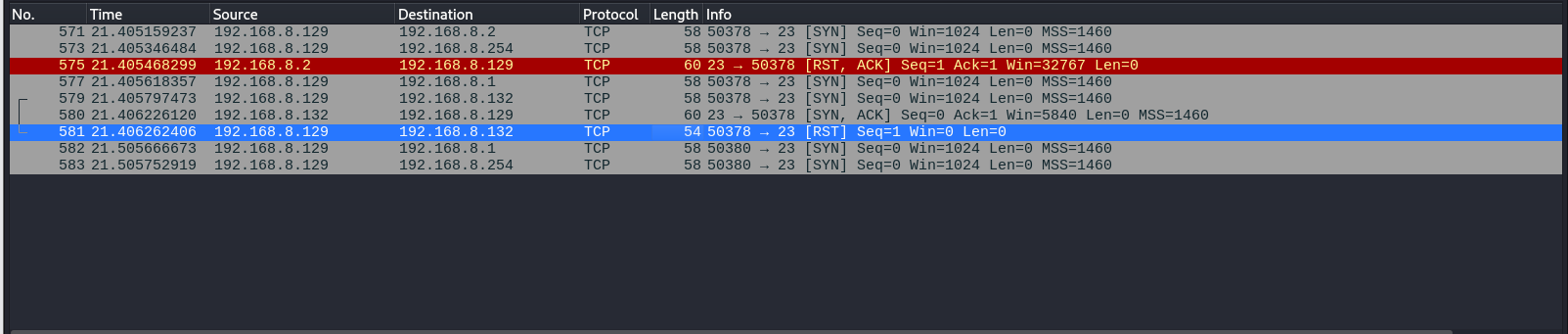
thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC

của các máy tính trong mạng 192.168.8.132/24.



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.

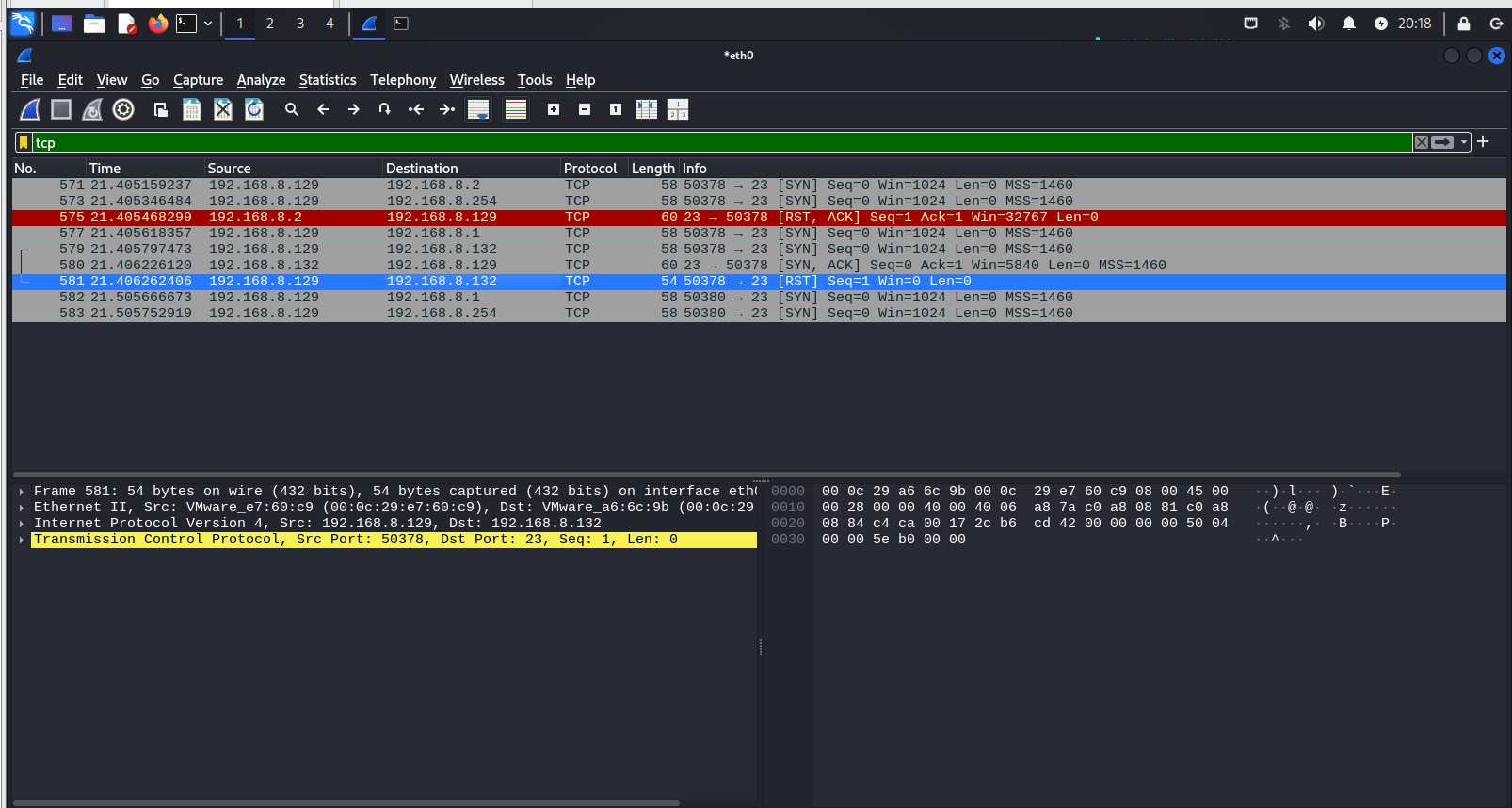


- Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy

gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.8.129 về máy tấn công. Như vậy,

điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.8.2 trong kết quả trả về

là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)



* 1. **Kịch bản 3**

- 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.

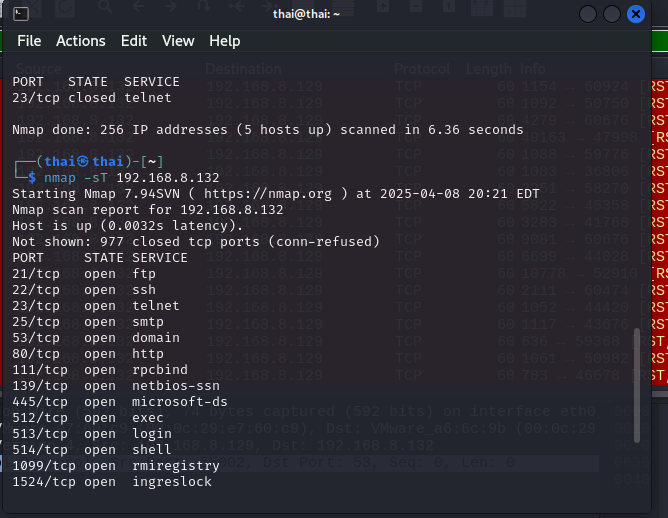
- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**nmap -sT 192.168.8.132**

- 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 21, 22, 23, 25,53 …. trên máy mục tiêu 192.168.8.132 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

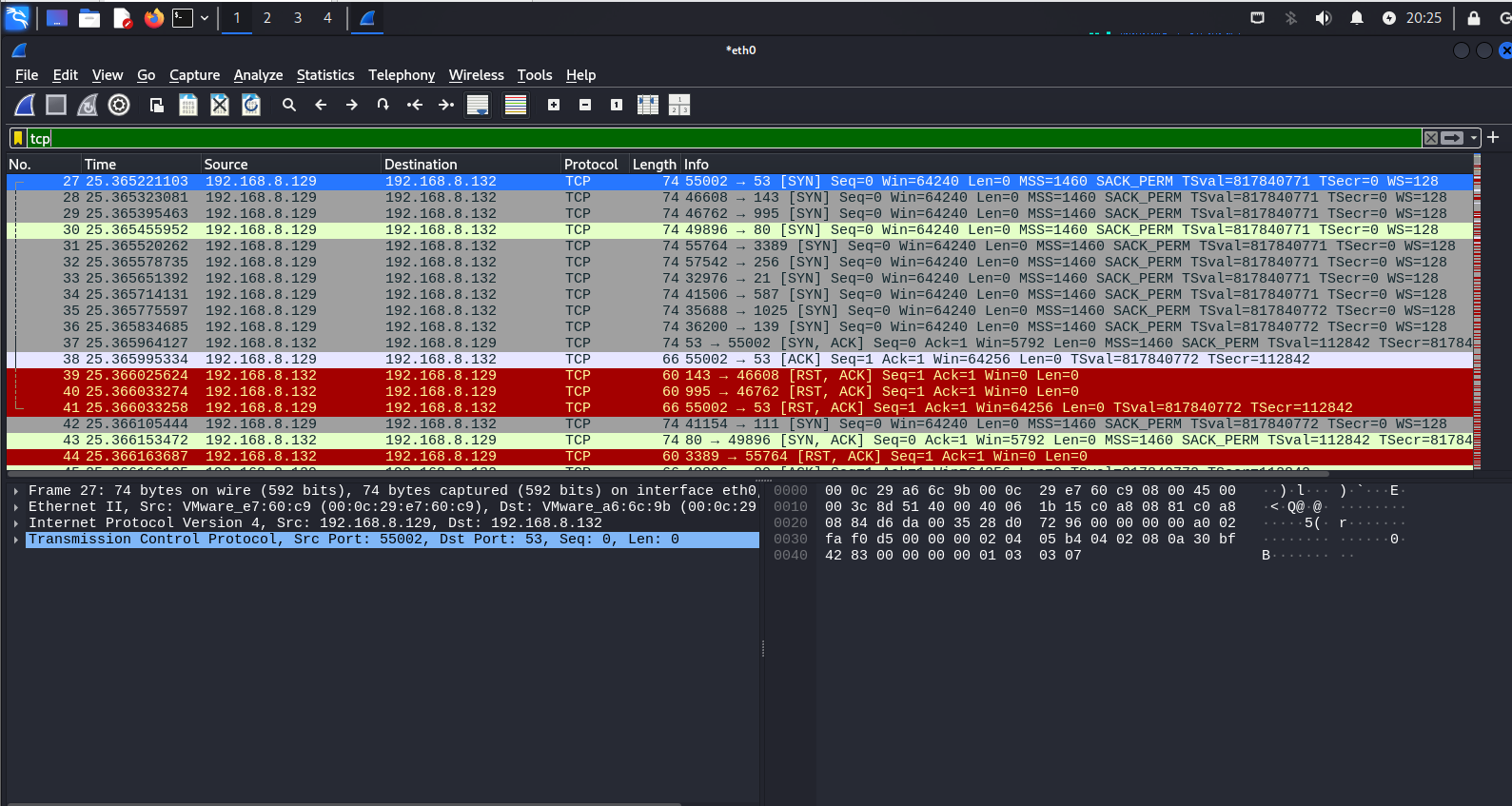
Phân tích lưu lượng:

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

máy mục tiêu 192.168.8.129 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói

tin TCP SYN được gửi từ máy tấn công (192.168.8.132) tới máy mục tiêu là 192.168.117.129.

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

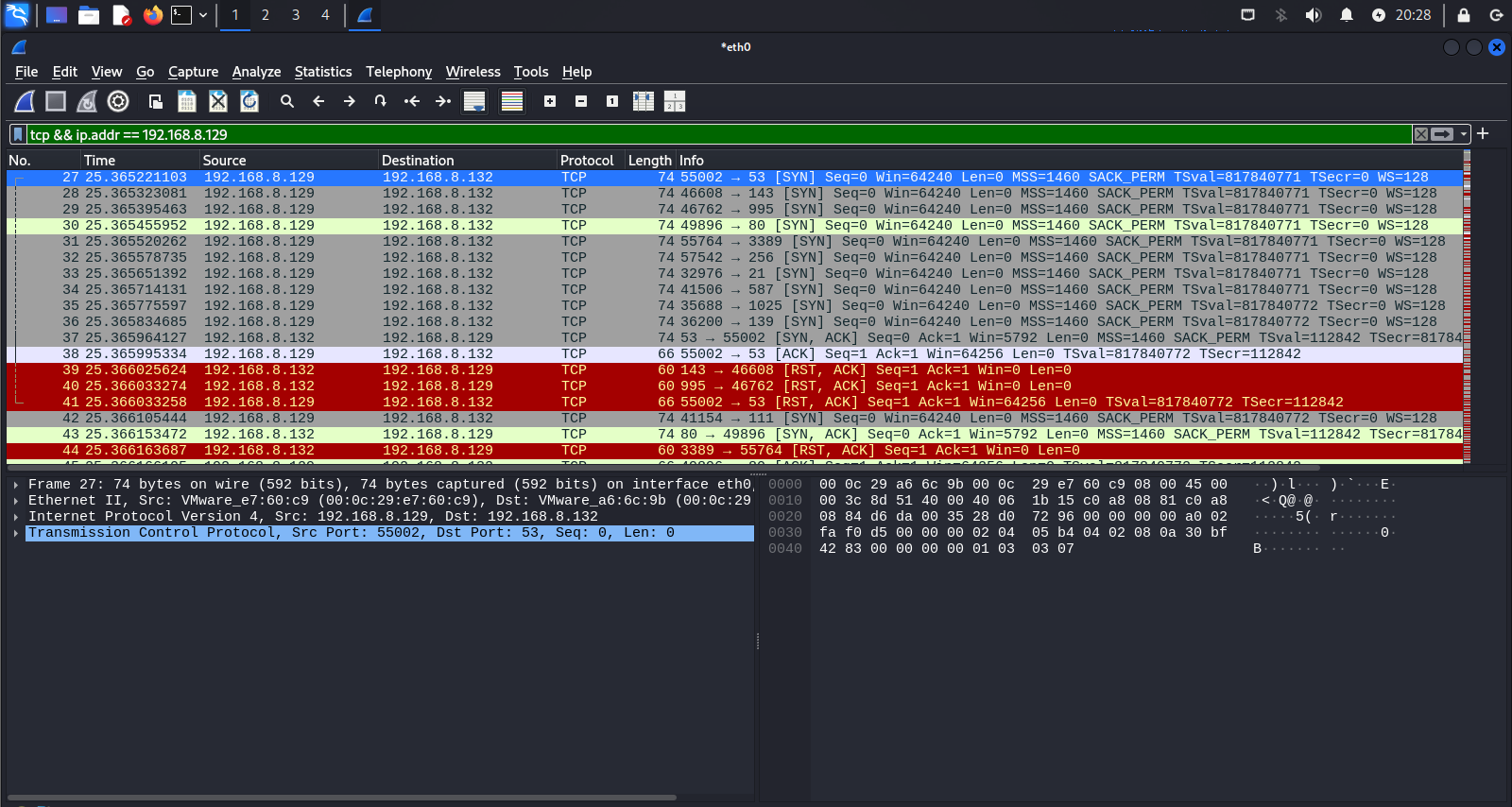


- Sử dụng giá trị tcp && ip.addr == 192.168.8.129 ta lọc được các gói tin TCP. Có thể nhận

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

30) 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 22, 23. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ

thuật TCP Connection Scan

- Danh sách các cổng ứng dụng trên máy mục tiêu có thiết lập kết nối với máy do thám trùng

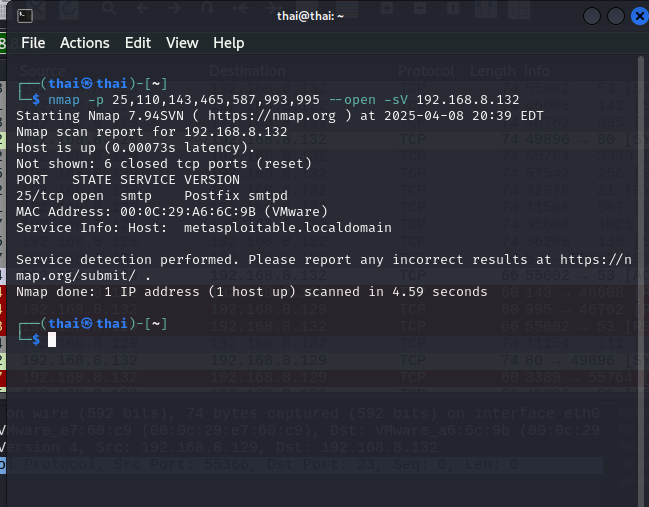
khớp với kết quả trả về của lệnh quét nmap trên máy do thám.

1. **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**

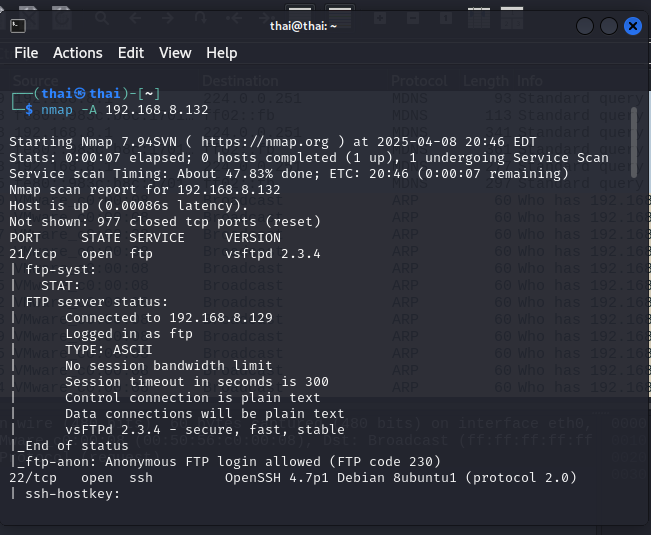
|  |  |
| --- | --- |
| Tham số | Ý nghĩa |
| nmap | Công cụ quét mạng để thăm dò các thiết bị và dịch vụ đang hoạt động |
| -p 25,110,143,465,587,993,995 | Chỉ định các cổng của dịch vụ email cần quét: • 25 – SMTP (Simple Mail Transfer Protocol) • 110 – POP3 (Post Office Protocol v3) • 143 – IMAP (Internet 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) |

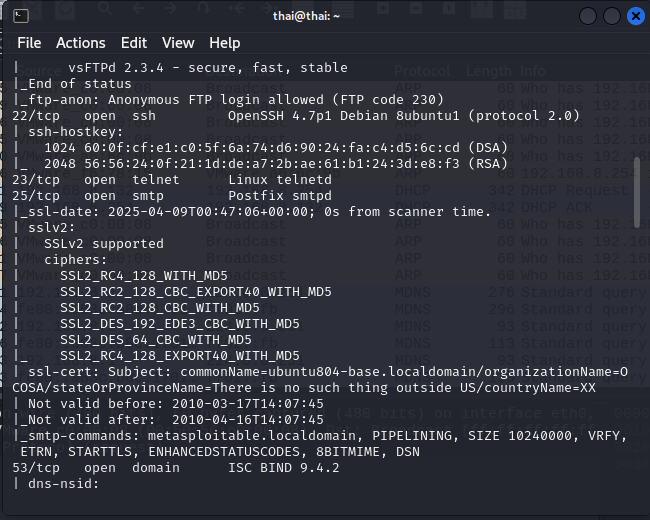


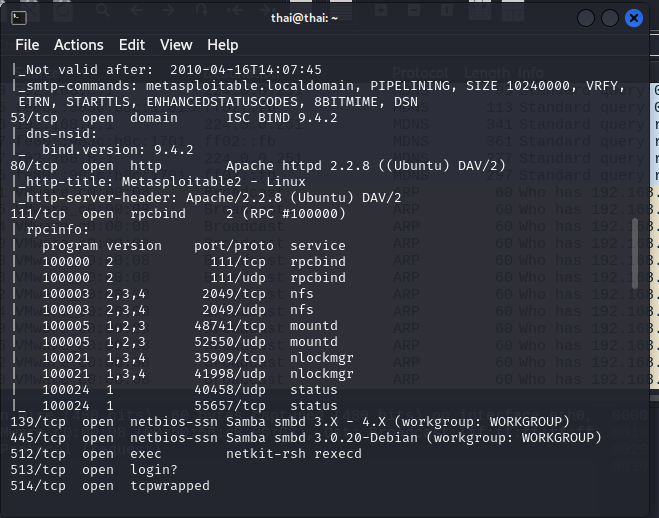
* Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

**Thông tin hệ điều hành:** **nmap -A 192.168.8.132**

Hình ảnh chụp kết quả của nmap:

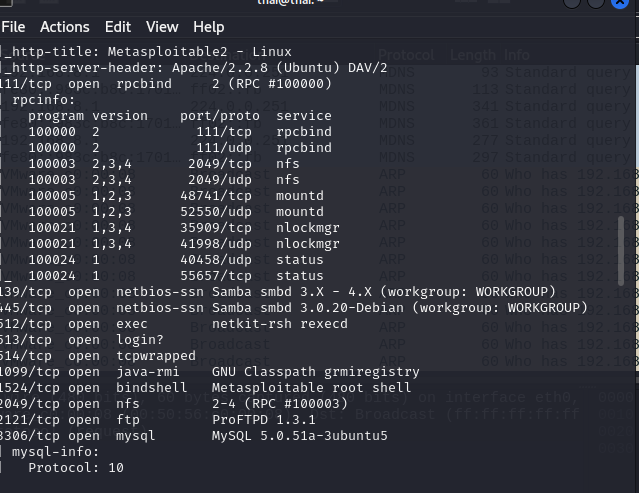
****

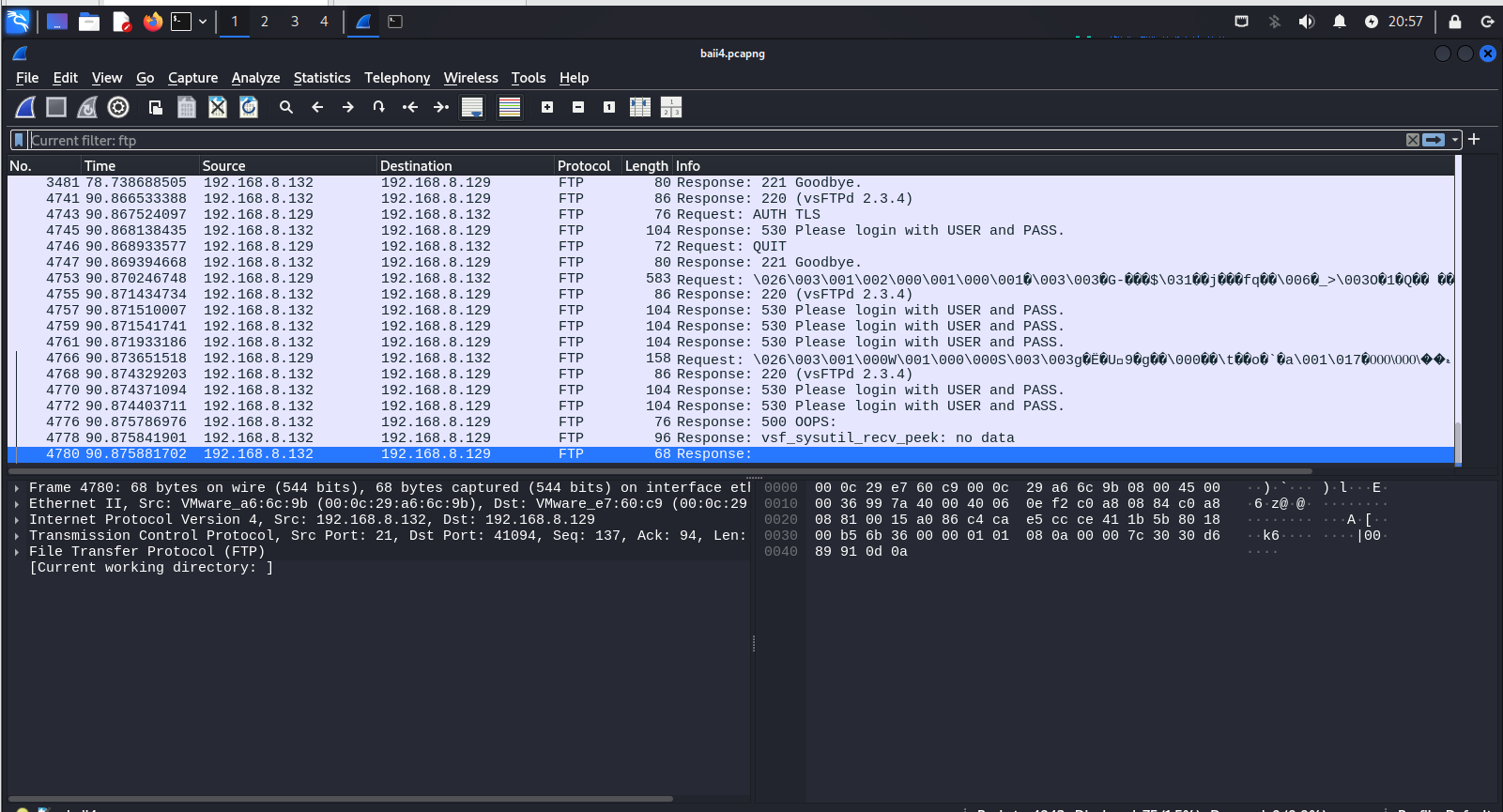
****

****

* Nêu tên và phiên bản hệ điều hành:
* **hệ điều hành Linux phiên bản kernel 2.6.x.**

**Thông tin dịch vụ:**

****



|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng** | **Tên phần mềm & Phiên bản** |
| 1 | FTP | 21 | vsftpd 2.3.4 |
| 2 | SSH | 22 | OpenSSH 4.7p1 Debian 8ubuntu1 |
| 3 | Telnet | 23 | Linux telnetd |
| 4 | SMTP | 25 | Postfix smtpd |
| 5 | DNS | 53 | ISC BIND 9.4.2 |
| 6 | HTTP | 80 | Apache httpd 2.2.8 |
| 7 | SMB (NetBIOS) | 139, 445 | Samba 3.0.20-Debian |
| 8 | MySQL | 3306 | MySQL 5.0.51a-3ubuntu5 |
| 9 | PostgreSQL | 5432 | PostgreSQL 8.3.0 - 8.3.7 |
| 10 | VNC | 5900 | VNC protocol 3.3 |

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.

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

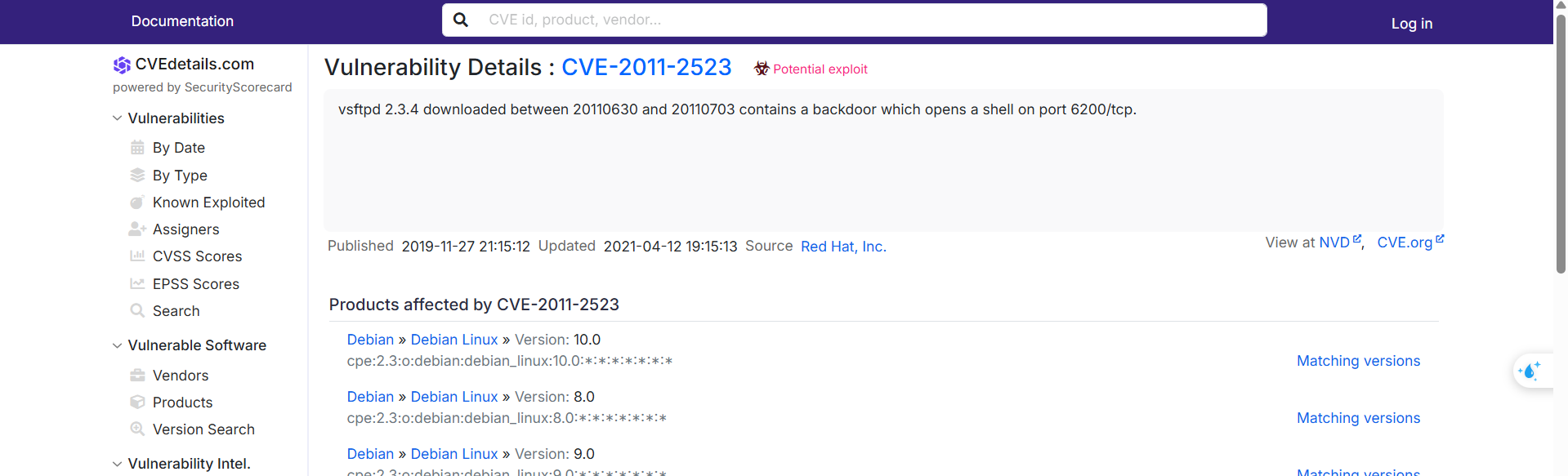
các phần mềm cung cấp dịch vụ. Thông tin về các lỗ hổng có thể tìm kiếm trên

https://www.cvedetails.com/

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

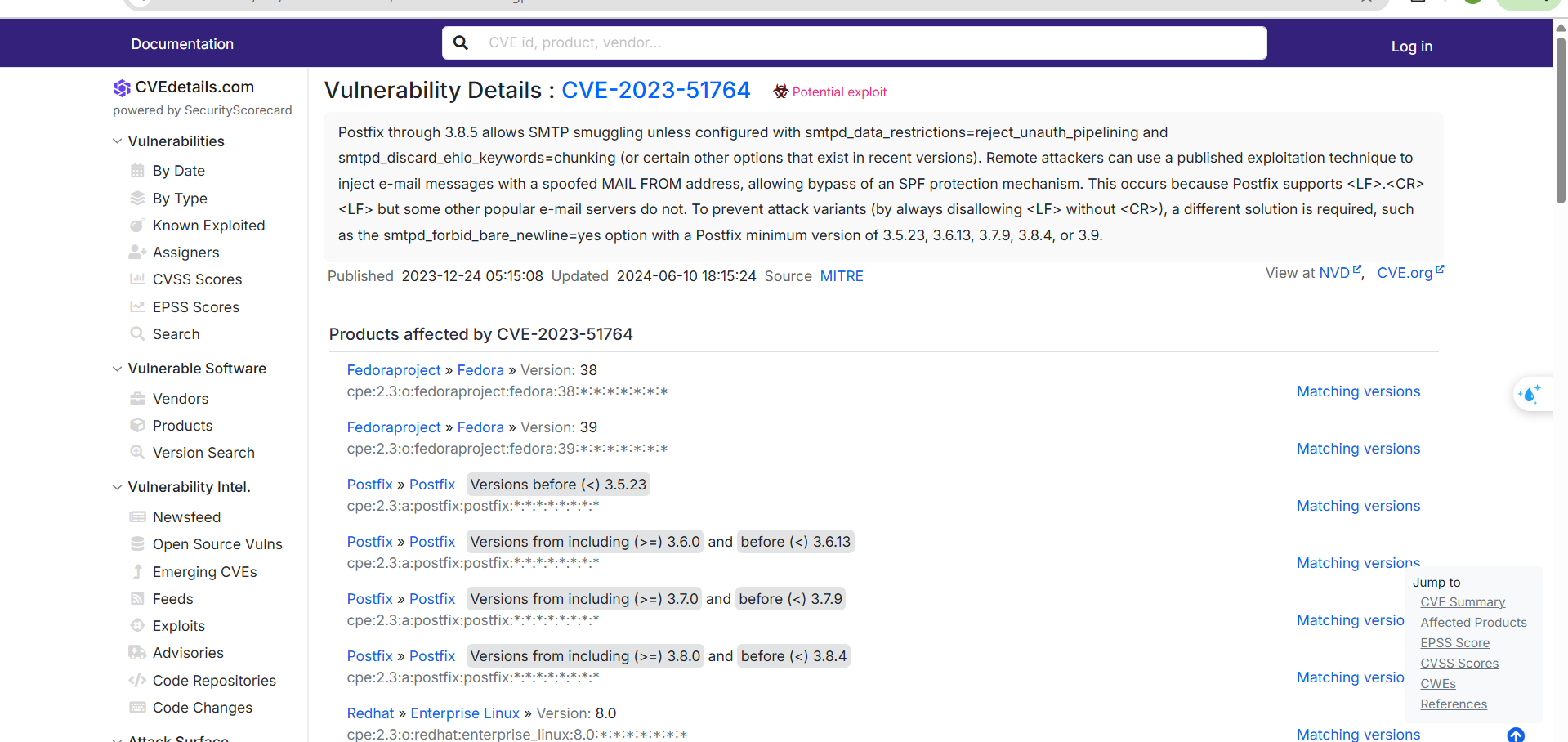
Bước 2: Tìm kiếm các tên phần mềm ở phần 2

1.vsftpd 2.3.4: link: <https://www.cvedetails.com/cve/CVE-2011-2523/>



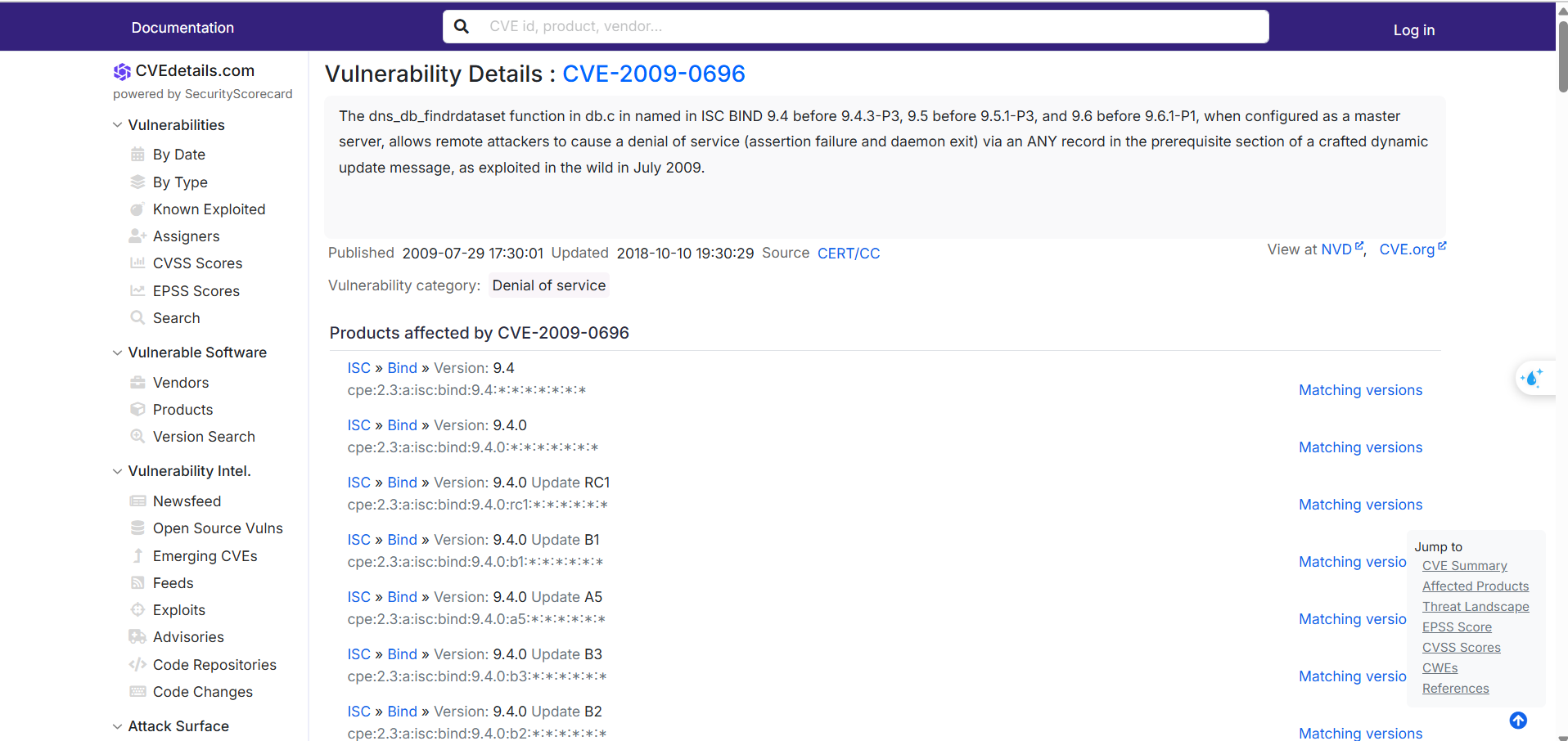
2. SMTP - Postfix smtpd

Link: <https://www.cvedetails.com/cve/CVE-2009-0696/>



3. DNS - ISC BIND 9.4.2​

Link: <https://www.cvedetails.com/cve/CVE-2009-0696>



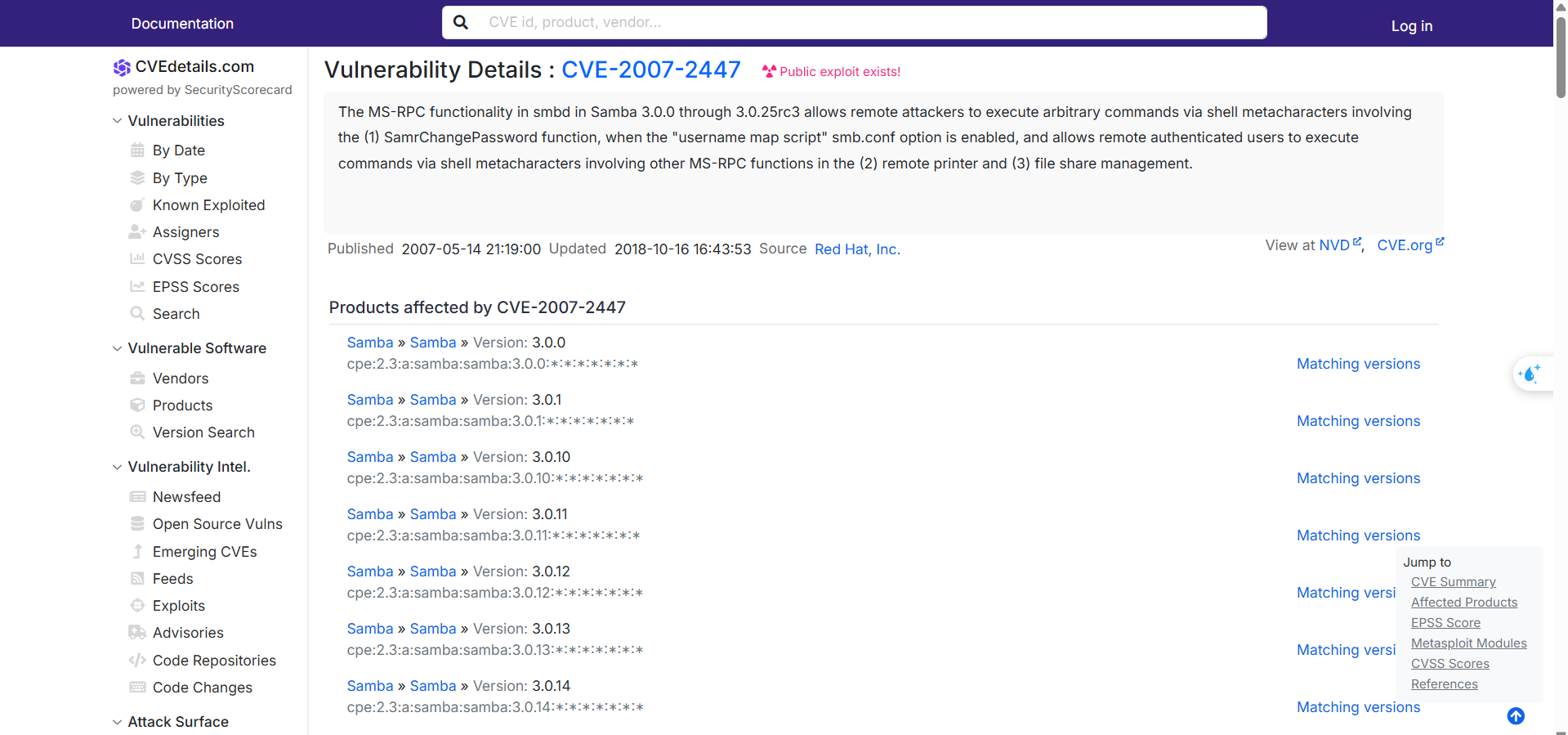
4. HTTP - Apache httpd 2.2.8​

Link: <https://www.cvedetails.com/cve/CVE-2010-0408/>



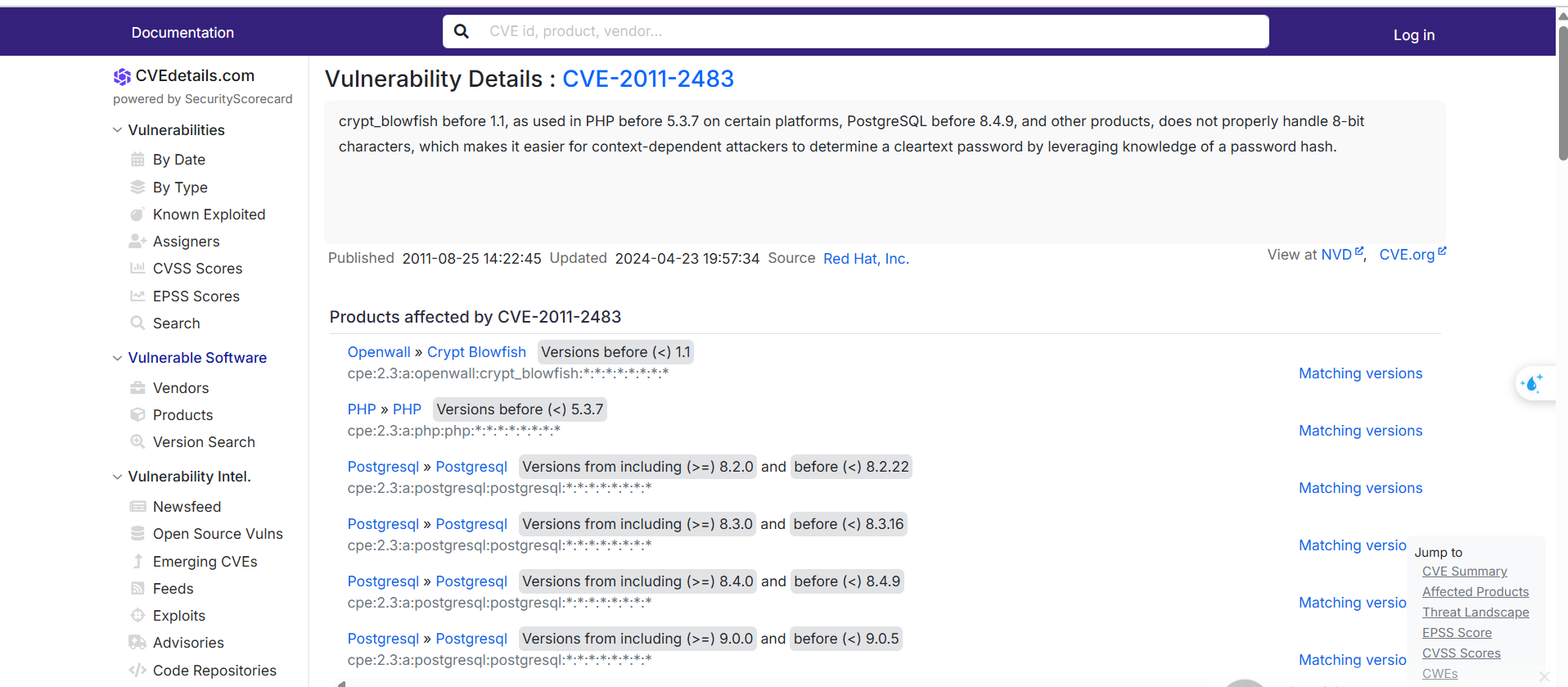
5. SMB (NetBIOS) - Samba 3.0.20-Debian

Link:<https://www.cvedetails.com/cve/CVE-2007-2447>



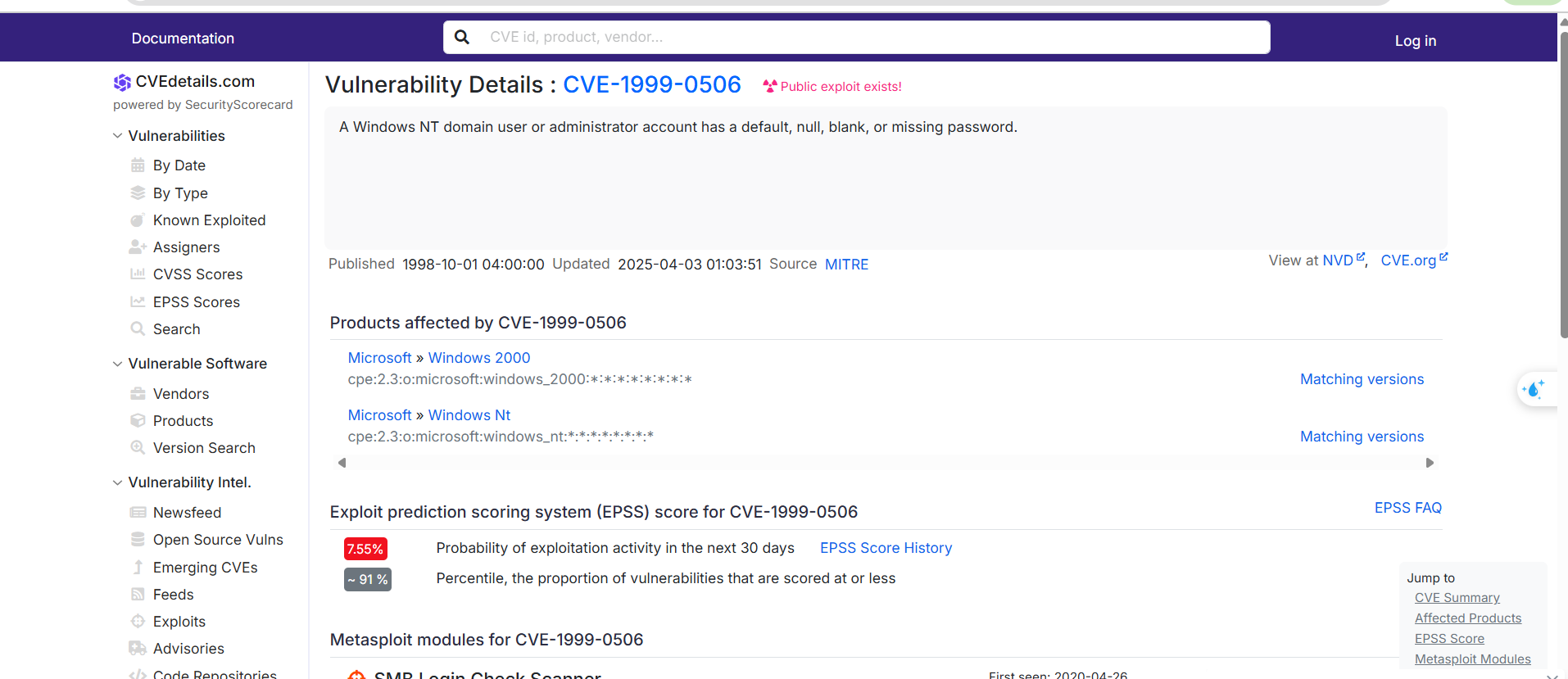
6. PostgreSQL - PostgreSQL 8.3.0​

Link: <https://www.cvedetails.com/cve/CVE-2011-2483>



7. VNC - VNC protocol 3.3

Link: <https://www.cvedetails.com/cve/CVE-1999-0506/>



|  |  |  |  |
| --- | --- | --- | --- |
| **Tên dịch vụ** | **Tên phần mềm & Phiên bản** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| FTP | vsftpd 2.3.4 | CVE-2011-2523 | Phiên bản vsftpd 2.3.4 tải xuống từ 30/06/2011 đến 03/07/2011 chứa cửa hậu cho phép mở shell trên cổng 6200/tcp. |
|  |  |  |  |
| SMTP | Postfix smtpd | CVE-2023-51764 | Postfix đến phiên bản 3.8.5 cho phép tấn công SMTP smuggling trừ khi được cấu hình với các tham số bảo mật cụ thể. |
| DNS | ISC BIND 9.4.2 | CVE-2009-0696 | Chức năng dns\_db\_findrdataset trong ISC BIND 9.4.2 cho phép kẻ tấn công từ xa gây từ chối dịch vụ thông qua bản ghi ANY trong phần điều kiện tiên quyết của thông điệp cập nhật động được tạo đặc biệt. |
| HTTP | Apache httpd 2.2.8 | CVE-2010-0408 | Hàm ap\_proxy\_ajp\_request trong mod\_proxy\_ajp của Apache HTTP Server 2.2.8 không xử lý đúng các tình huống khi máy khách không gửi nội dung yêu cầu, cho phép kẻ tấn công từ xa gây từ chối dịch vụ. |
| SMB (NetBIOS) | Samba 3.0.20-Debian | CVE-2007-2447 | Samba 3.0.20 đến 3.0.25rc3 với tùy chọn "username map script" không mặc định cho phép thực thi lệnh tùy ý thông qua tên người dùng chứa ký tự đặc biệt. |
| PostgreSQL | PostgreSQL 8.3.0 | CVE-2011-2483 | crypt\_blowfish trước 1.1, được sử dụng trong PostgreSQL trước 8.4.9, không xử lý đúng các ký tự 8-bit, giúp kẻ tấn công xác định mật khẩu rõ ràng thông qua hash mật khẩu. |
| VNC | VNC protocol 3.3 | CVE-1999-0506 | VNC cho phép truy cập không được xác thực, cho phép kẻ tấn công từ xa truy cập hệ thống mà không cần thông tin xác thực. |