BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

***Họ và tên sinh viên:* Phạm Hoàng Anh**

***MSSV:* 0850080003**

**Mục lục**

[**1.** **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap** 1](#_Toc133429259)

[**1.1.** **Kịch bản 1** 1](#_Toc133429260)

[**1.2.** **Kịch bản 2** 4](#_Toc133429261)

[**1.3.** **Kịch bản 3** 7](#_Toc133429262)

[**2.** **Thu thập thông tin hệ thống** 9](#_Toc133429263)

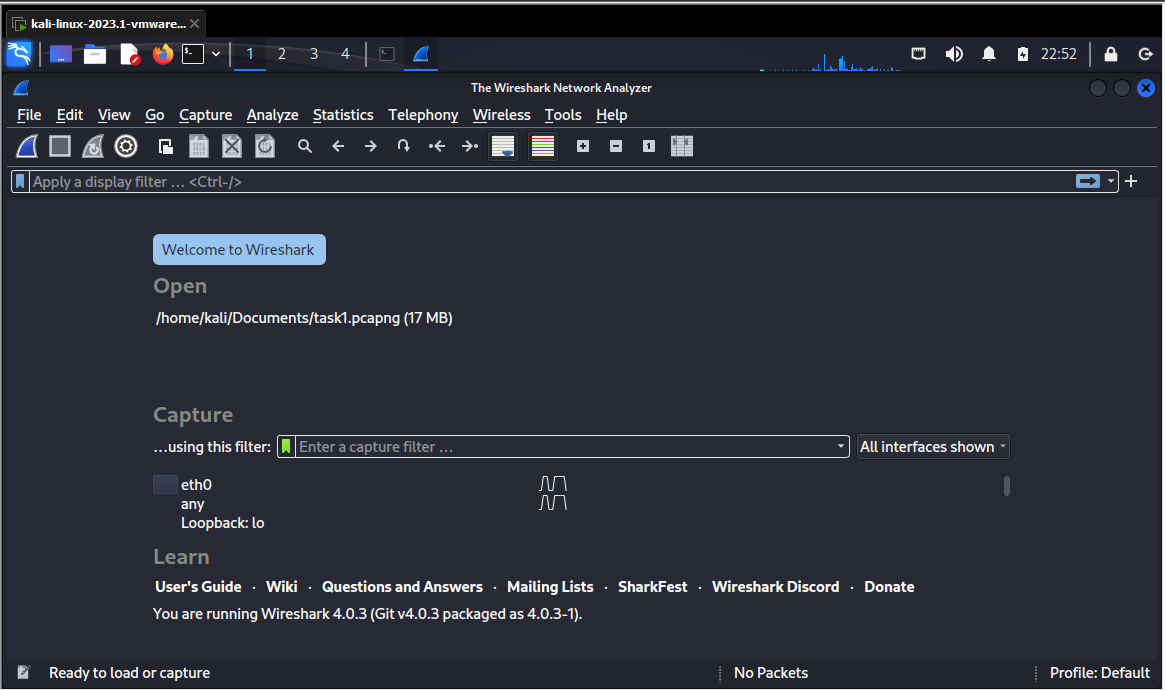
**KẾT QUẢ THỰC HÀNH**

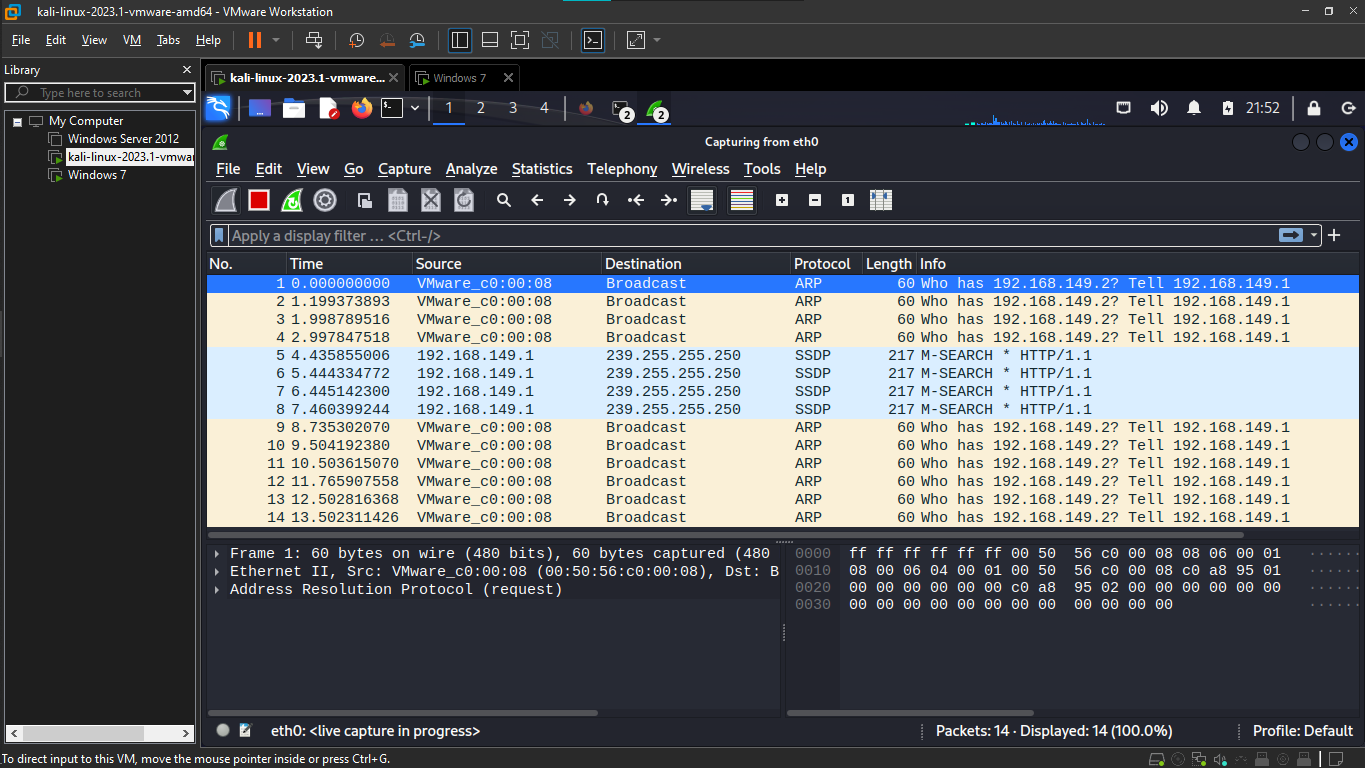
1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

Bước 1: Truy cập máy ảo Kali linux:



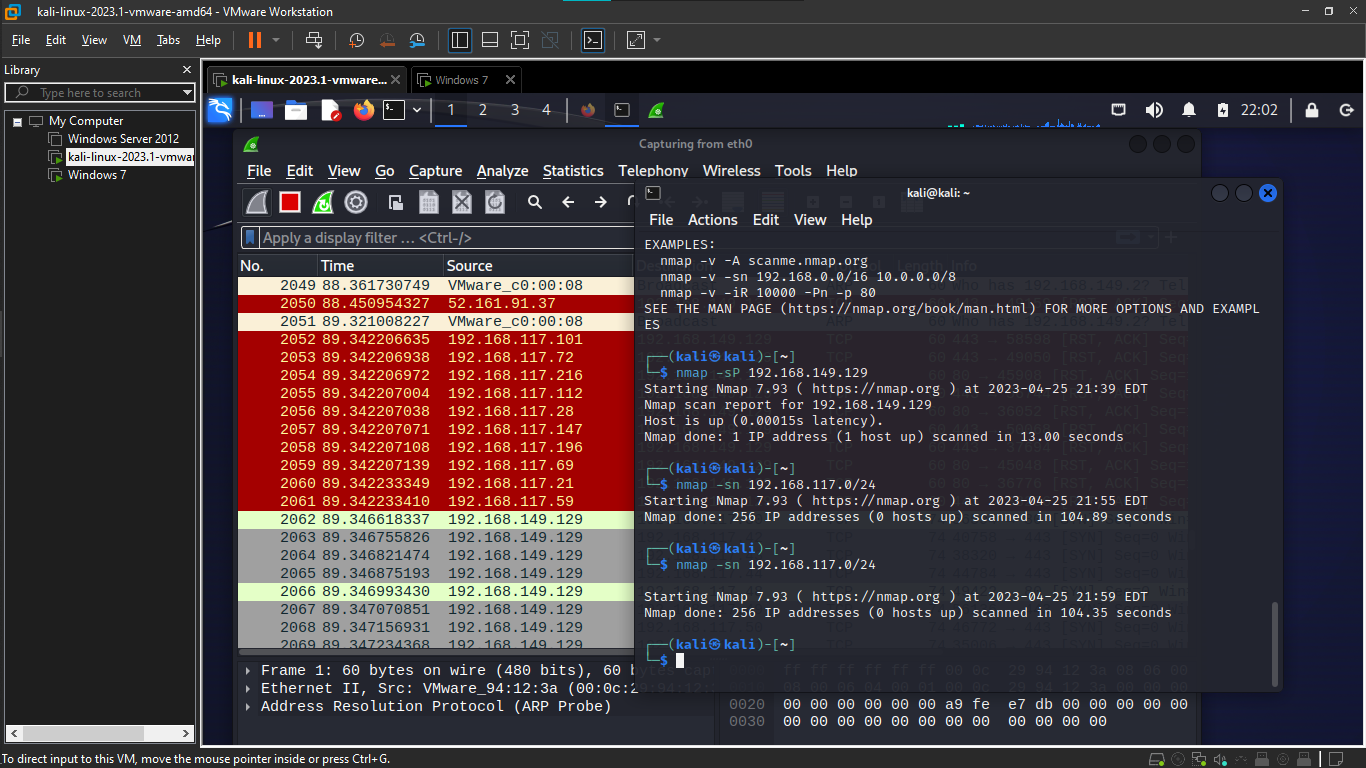
Bước 2: Mở cửa sổ khởi động wireshark:

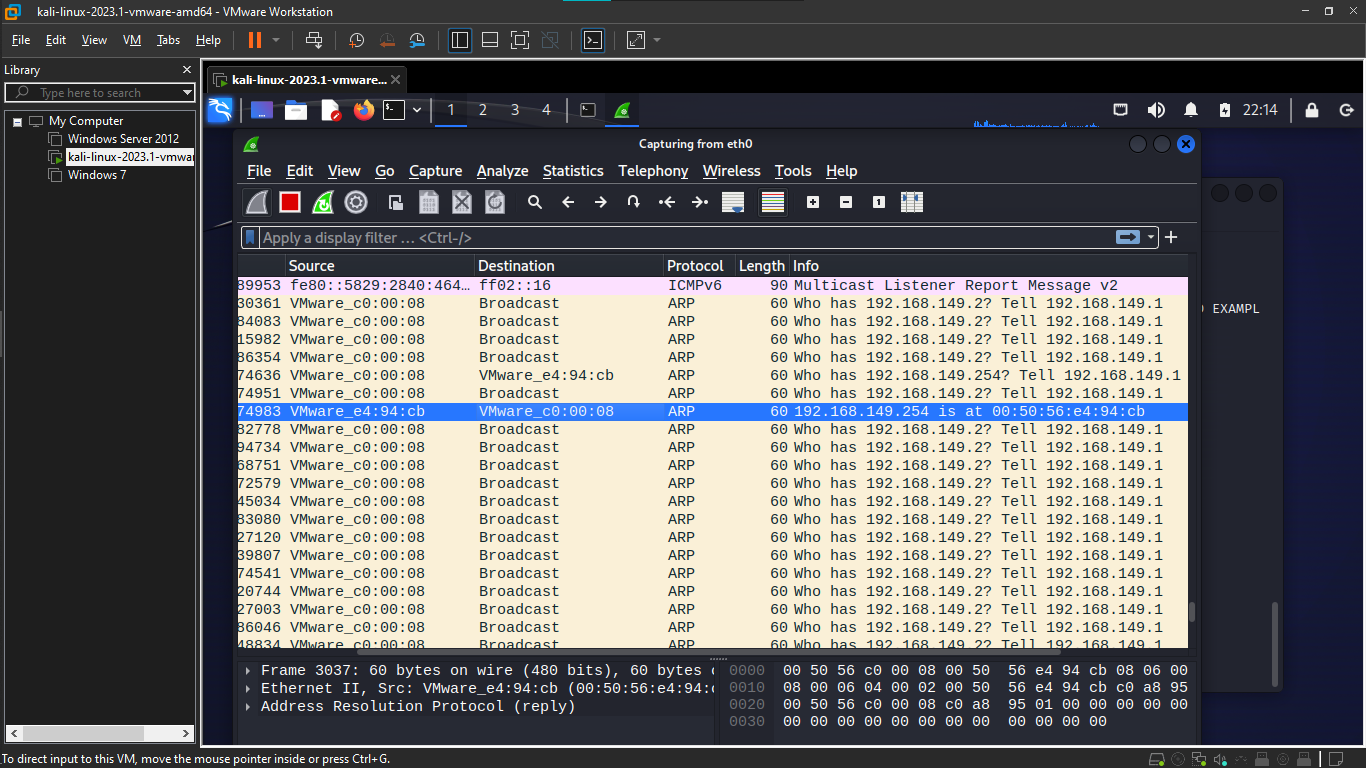




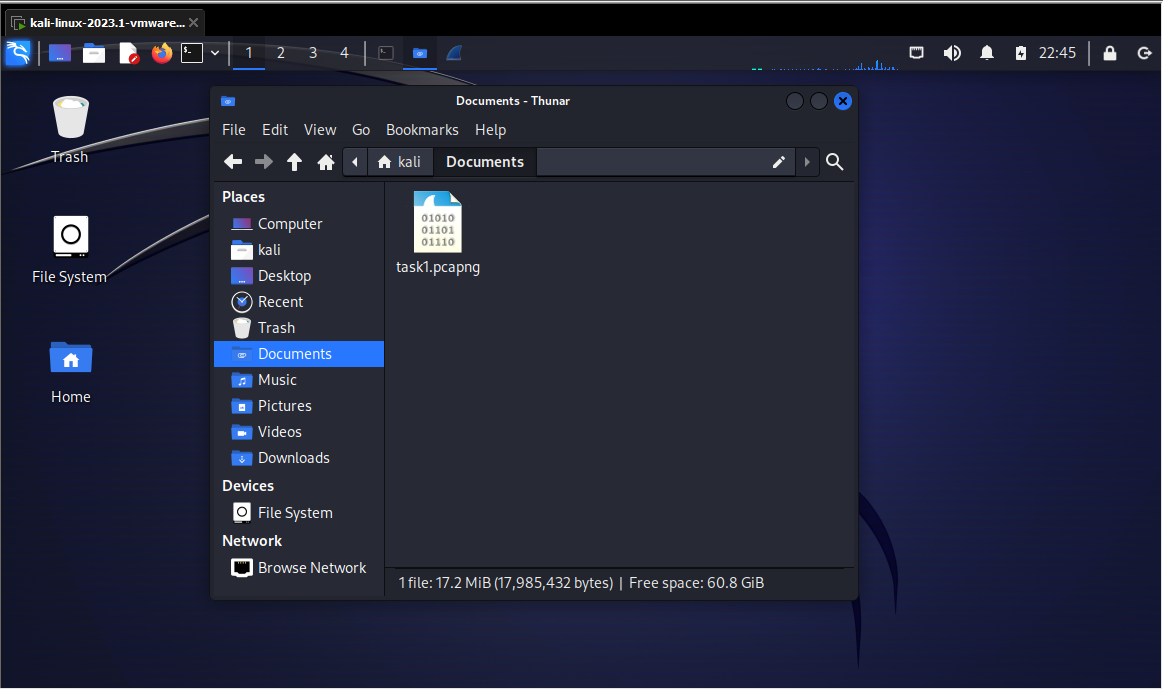
Bước 3: Mở terminal để sử dụng nmap để quét mạng với lệnh sau:

nmap -sn 192.168.149.0/24



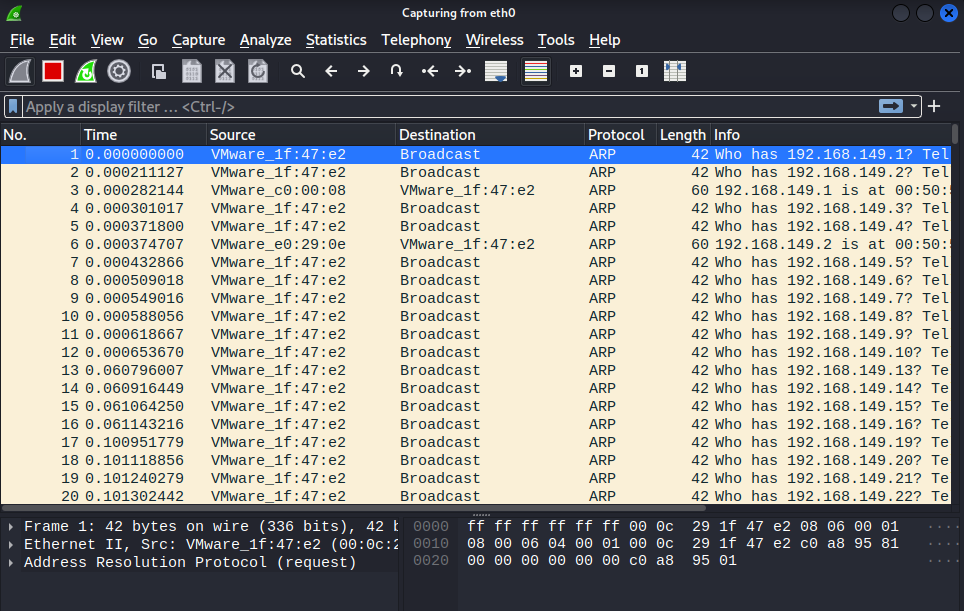


* Phân tích lưu lượng:
  + Màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.149.0/24
  + Kết quả trả về chỉ có một địa chỉ IP được liệt kê và được đánh dấu là "Host is up" - Điều này cho thấy quét được thực hiện bằng cách gửi các gói tin ping đến địa chỉ IP để xác định xem host có đang hoạt động hay không.
  + Thời gian hoàn thành quét là 13 giây - Điều này cho thấy quét thăm dò đã được thực hiện nhanh chóng, vì không có nhiều gói tin ping được gửi đến các địa chỉ IP khác.

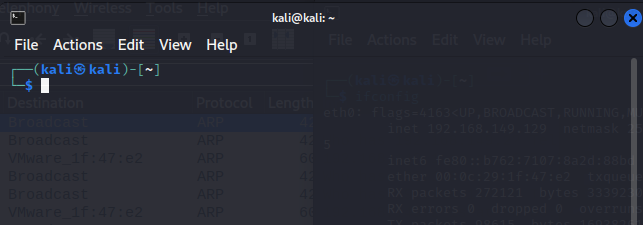


* Đây là kỹ thuật kiểm tra xem host còn alive không.
  1. **Kịch bản 2**

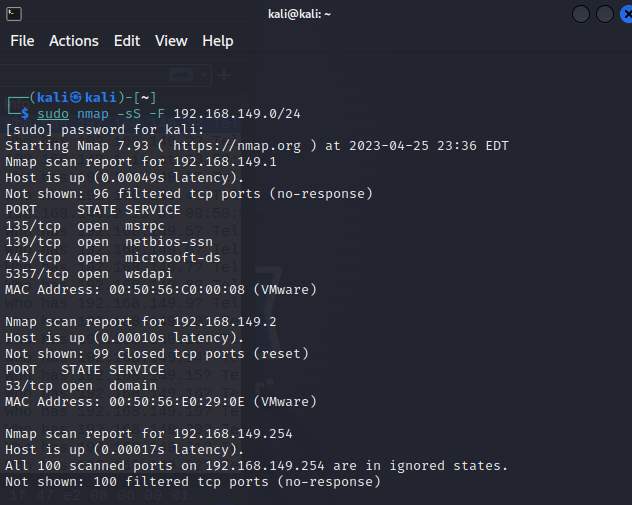
Bước 1: Khởi chạy wireshark:



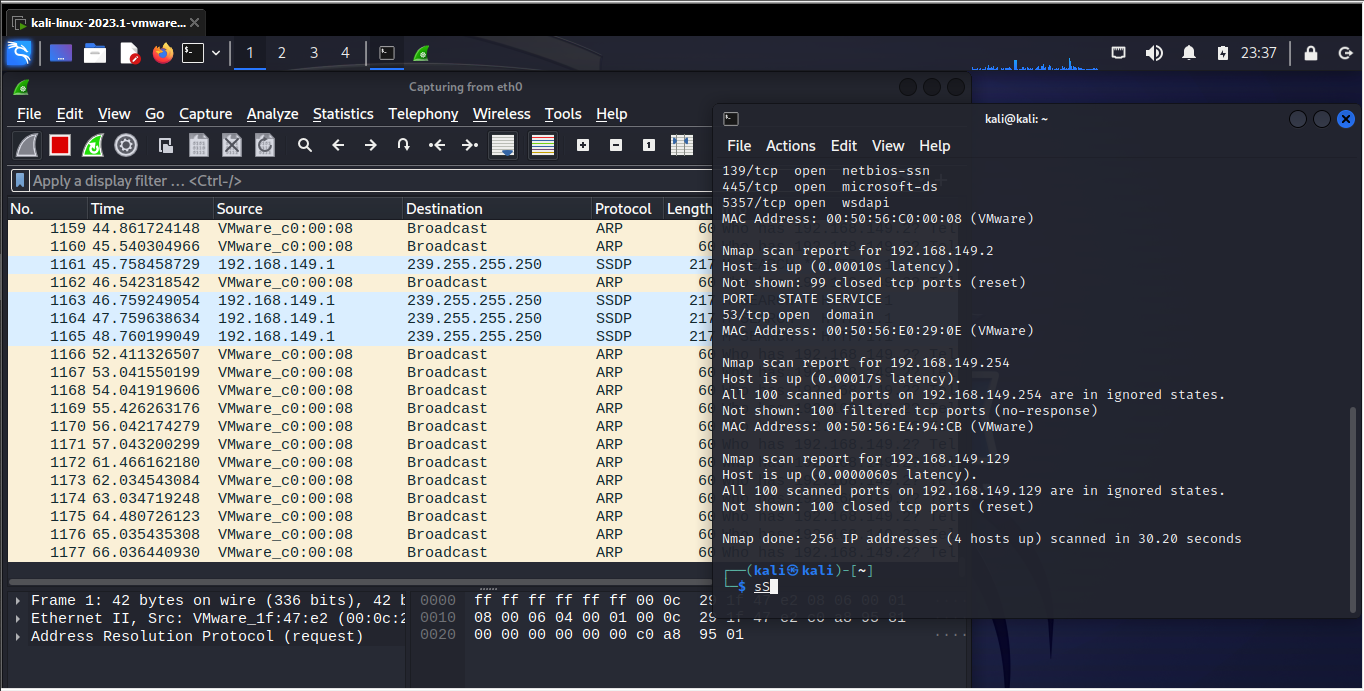
Bước 2: Mở terminal và chạy lệnh:



sudo nmap -sS -F 192.168.149.0/24



Được kết quả:

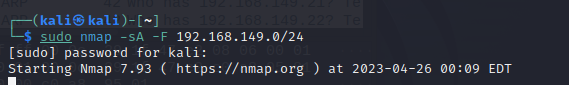


* Phân tích đặc điểm lưu lượng:
  + Kỹ thuật quét cổng TCP SYN (-sS) được sử dụng để kiểm tra tình trạng hoạt động của các cổng TCP trên các host được quét. Kỹ thuật này không hoàn thành việc thiết lập kết nối TCP và gửi gói tin SYN đến các cổng được chỉ định. Nếu cổng được mở, host đó sẽ trả lời lại với một gói tin SYN/ACK và nếu cổng đóng, host sẽ trả lời lại với một gói tin RST.
  + Lệnh sudo được sử dụng để chạy lệnh nmap với quyền root để truy cập vào các cổng được ẩn.
  + Tham số -F được sử dụng để quét nhanh các cổng TCP được phổ biến nhất (1000 cổng đầu tiên). Khi thực hiện quét nhanh, Nmap chỉ kiểm tra một số cổng TCP quan trọng nhất để tiết kiệm thời gian và tài nguyên.
  + Các đặc điểm lưu lượng cho thấy kỹ thuật quét thăm dò bằng SYN scan trong lệnh nmap -sS -F bao gồm:
    - Lưu lượng quét chỉ tập trung vào một phạm vi địa chỉ IP cụ thể, trong trường hợp này là 192.168.149.0/24.
    - Kỹ thuật quét sử dụng giao thức TCP để quét các cổng mạng, nói cách khác, SYN scan sẽ tìm kiếm các cổng TCP đang mở trên các máy chủ được quét.
    - Quá trình quét được thực hiện nhanh chóng, trong trường hợp này chỉ mất khoảng 30 giây để quét 256 địa chỉ IP.
    - Kết quả quét bao gồm danh sách các cổng mạng đang mở trên các máy chủ được quét, thông tin về dịch vụ đang chạy trên cổng mạng đó cùng với địa chỉ MAC của máy chủ được quét.
  + Dưới đây là một số hình ảnh chụp màn hình minh họa cho các đặc điểm lưu lượng của kỹ thuật quét thăm dò bằng SYN scan trong lệnh nmap -sS -F:
  + Đây là một hình ảnh chụp màn hình cho kết quả quét mẫu sử dụng lệnh nmap -sS -F 192.168.149.0/24: nmap\_scan\_result
  + Trong kết quả quét này, chúng ta có thể thấy rằng nmap đang quét các cổng TCP trên các máy chủ được liệt kê trong phạm vi địa chỉ IP đã chỉ định.
  1. **Kịch bản 3**

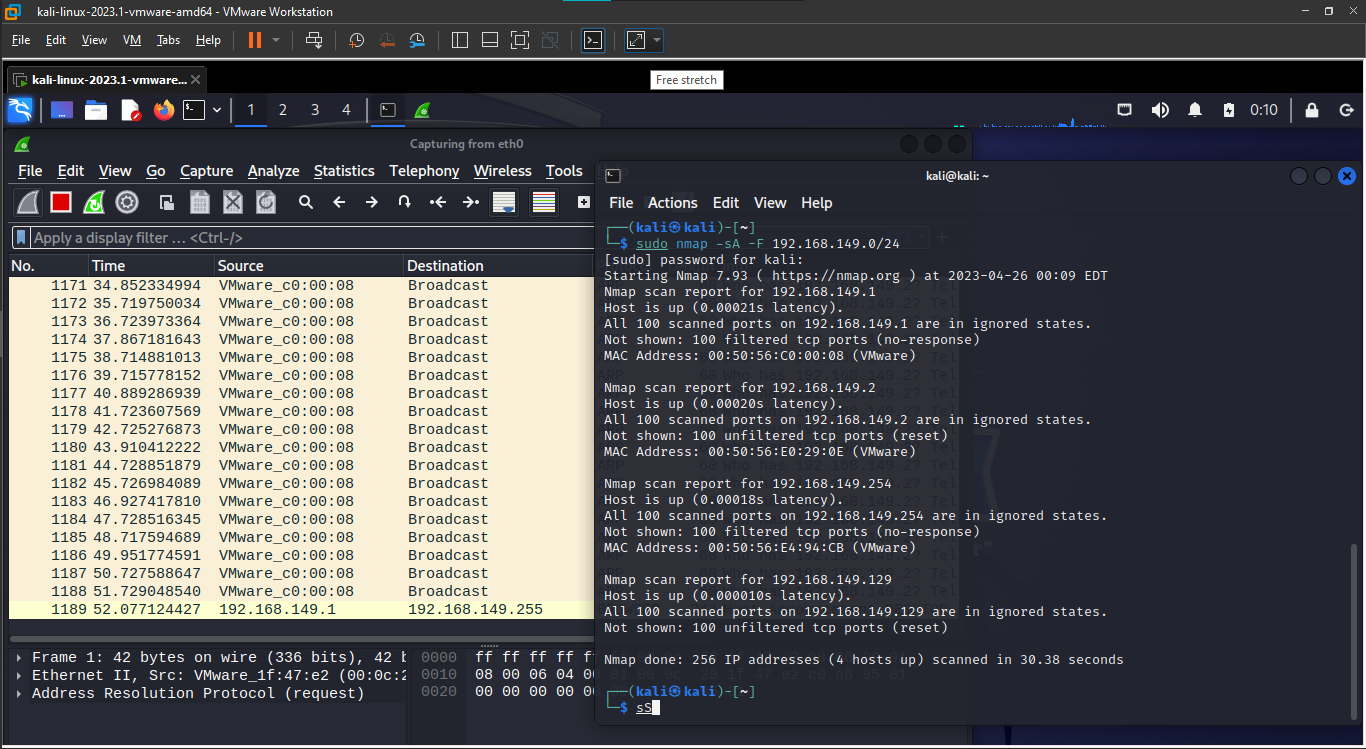
Bước 1: Khởi chạy wireshark:

Bước 2: Mở terminal và nhập lệnh:

sudo nmap -sA -F 192.168.149.0/24



Kết quả:

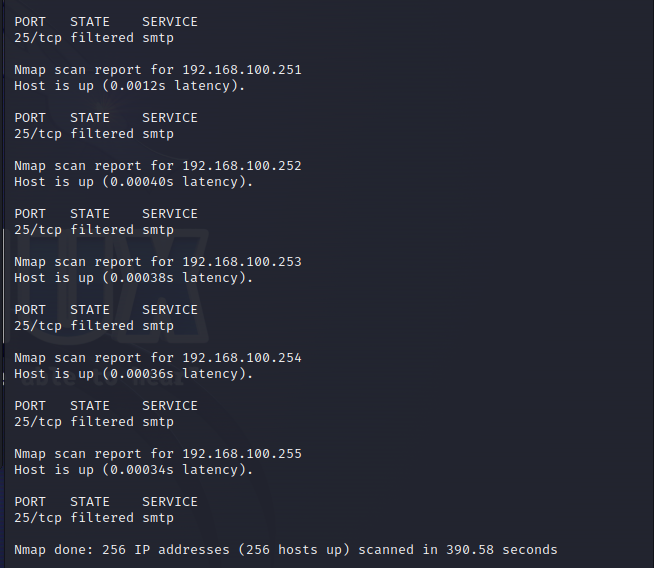
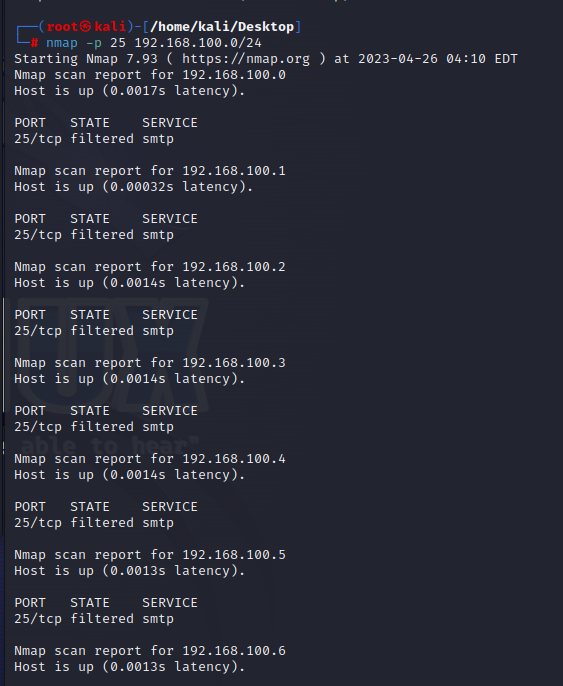


* Phân tích đặc điểm lưu lượng:
  + Lệnh "sudo nmap -sA -F 192.168.149.0/24" là một lệnh sử dụng phần mềm Nmap để quét mạng với các tùy chọn -sA và -F trên địa chỉ mạng IP 192.168.149.0/24.
  + Cụ thể, tùy chọn -sA đặt Nmap vào chế độ quét tàng hình (stealth scan) bằng cách gửi các gói tin ACK để kiểm tra xem các cổng mạng có mở hay không, trong khi tùy chọn -F chỉ quét các cổng phổ biến.
  + Kết quả của quét mạng này cho thấy có 4 máy tính đang hoạt động trên mạng với địa chỉ IP lần lượt là 192.168.149.1, 192.168.149.2, 192.168.149.254 và 192.168.149.129. Các cổng trên máy tính đều được báo cáo là ở trạng thái bị bỏ qua hoặc bị lọc, chỉ có một số cổng được báo cáo là không lọc hoặc đã reset kết nối.
  + Việc quét mạng như vậy thường được sử dụng trong bảo mật mạng để tìm ra các lỗ hổng bảo mật hoặc các thiết bị không được cài đặt đúng cách trên mạng. Tuy nhiên, việc sử dụng Nmap để quét mạng cũng cần được thực hiện với cẩn thận để tránh việc xâm nhập trái phép vào hệ thống của người khác.

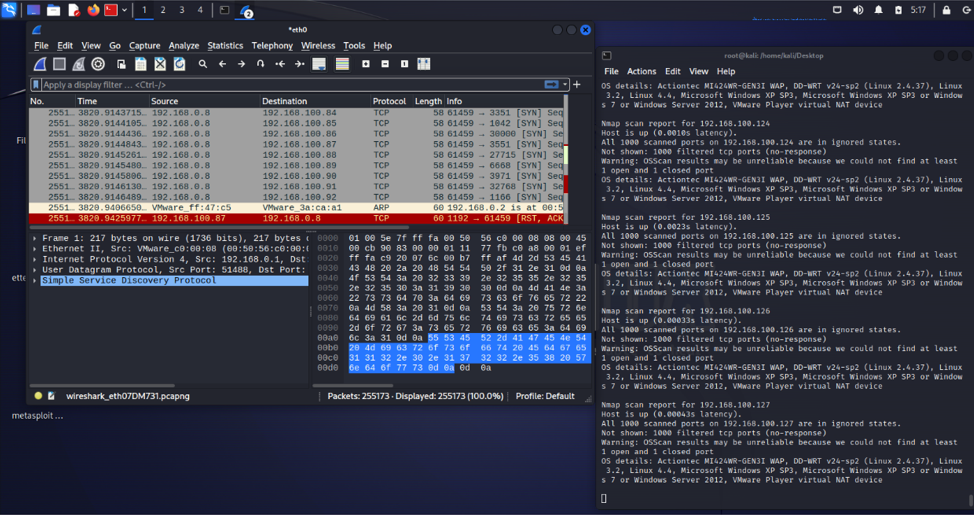
1. **Thu thập thông tin hệ thống**

Bước 1: mở wireshar và thực hiện bắt gói tin.

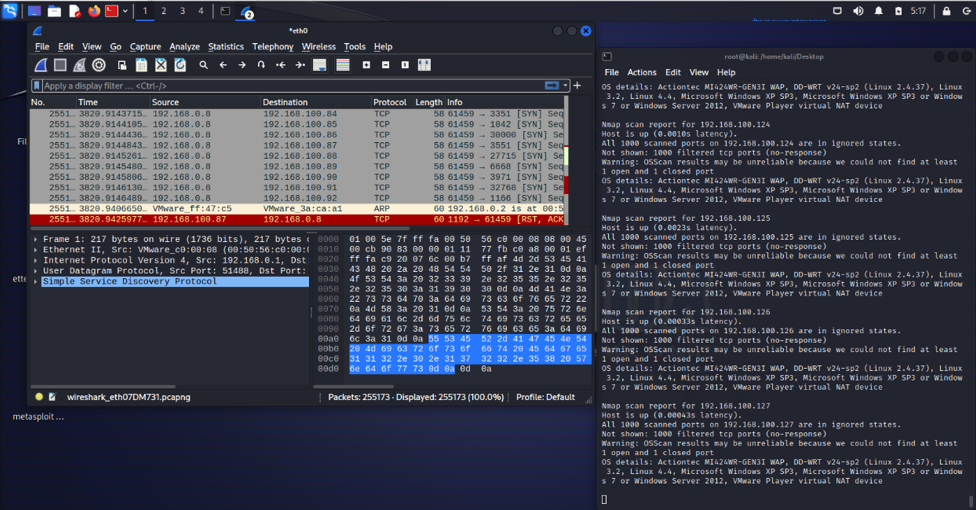
Bước 2: mở nmap và thực hiện lệnh nmap -p 25 192.168.100.0/24 để xác định nút mạng trong mạng 192.168.100.0/24 cung cấp dịch vụ email.

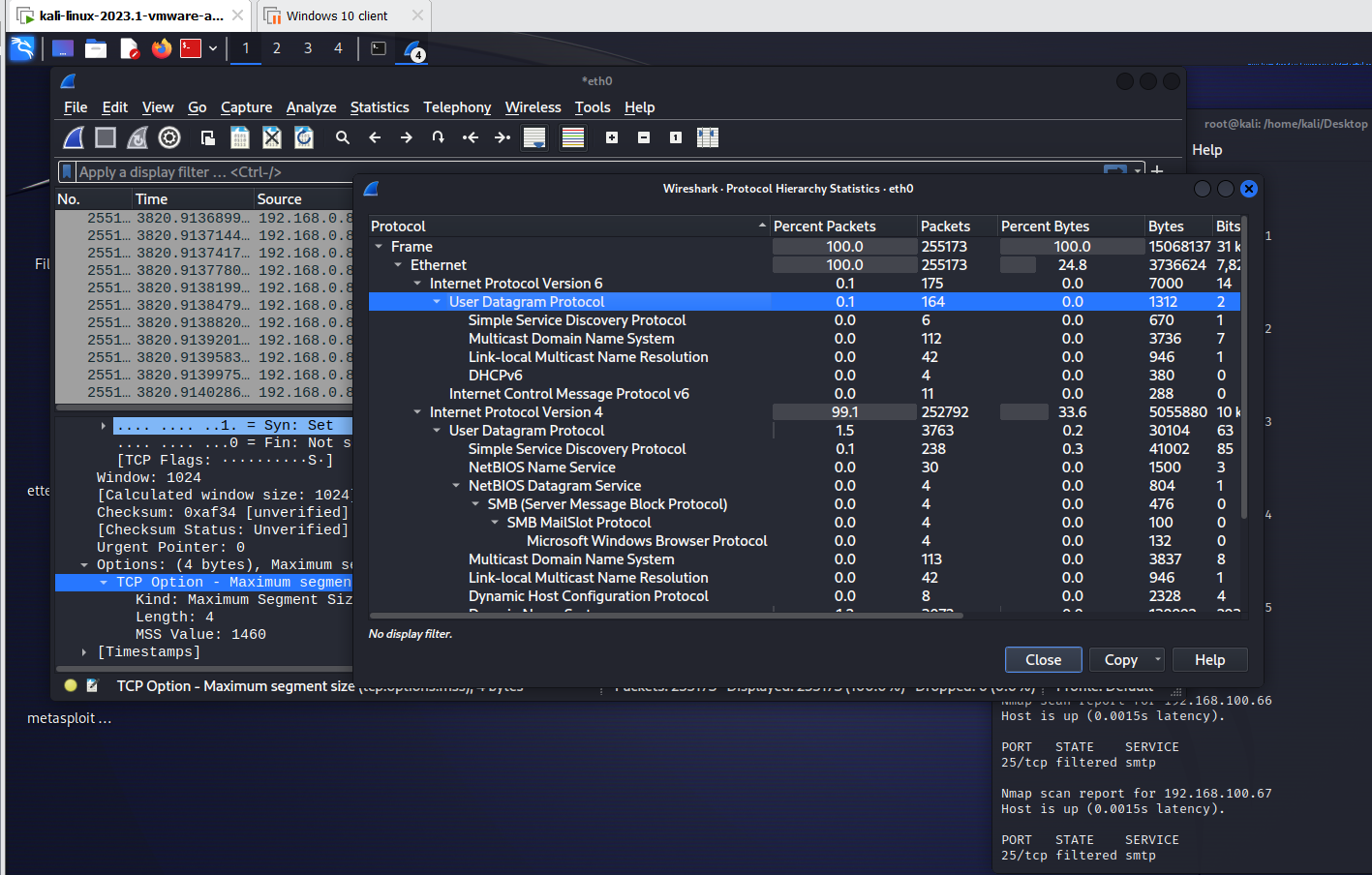


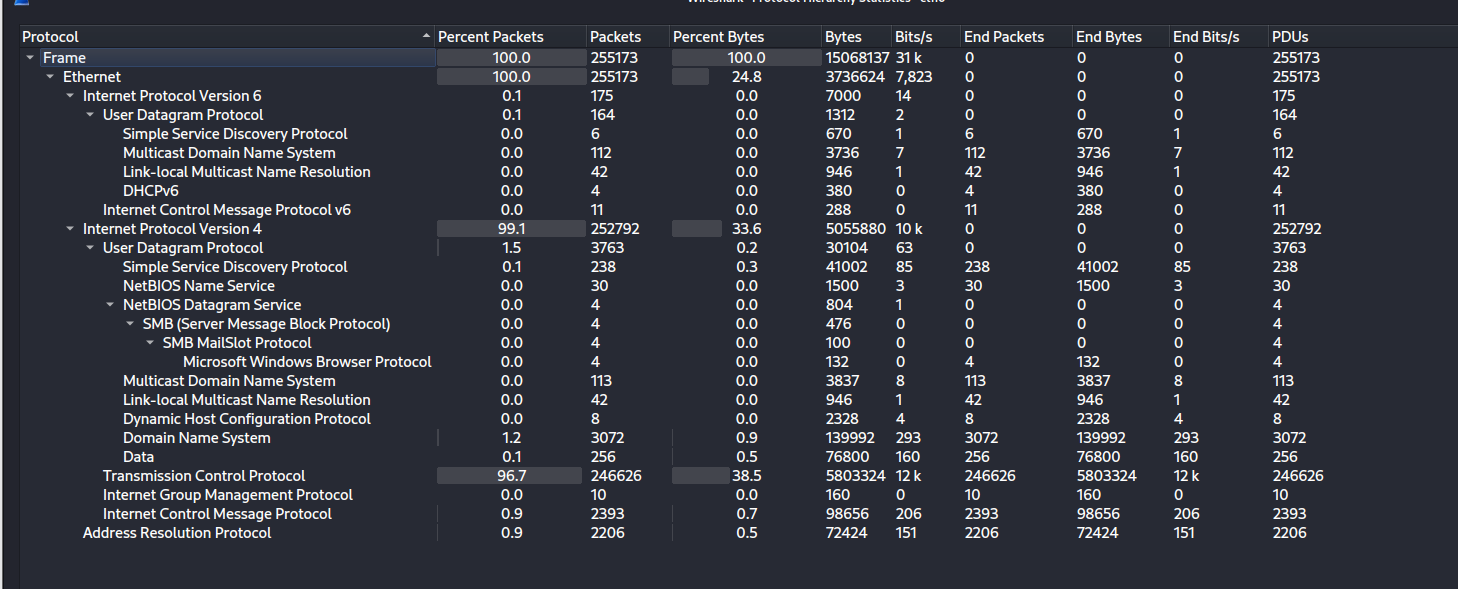
Bước 3: dùng lệnh nmap -sV -O 192.168.100.0/24 để quét, thu thập thông tin về hệ điều hành và các dịch vụ trên nút mạng 192.169.100.0

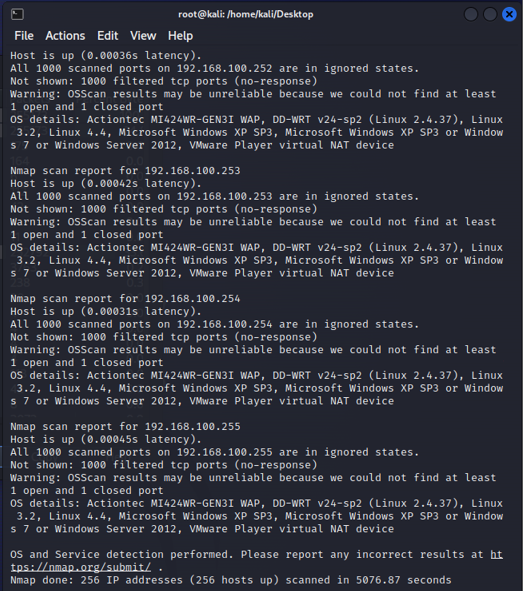


Bước 4: Dừng bắt gói tin. Trên thanh công cụ, chọn "Statistics" và chọn "Protocol Hierarchy".

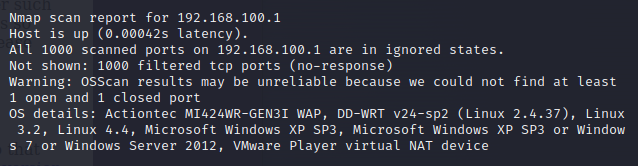




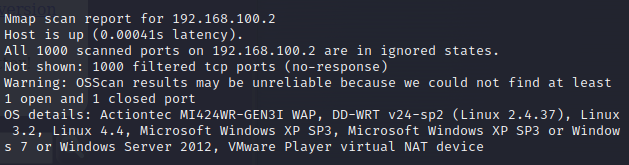




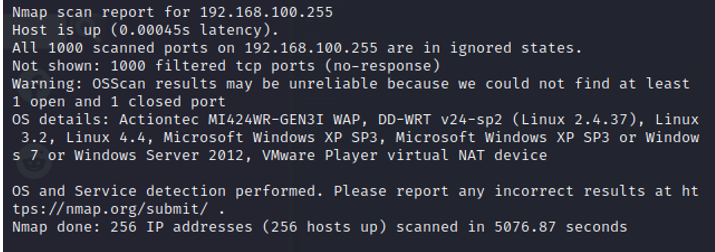
* Các hệ điều hành có thể có của địa chỉ thứ 1 là:
  + Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.

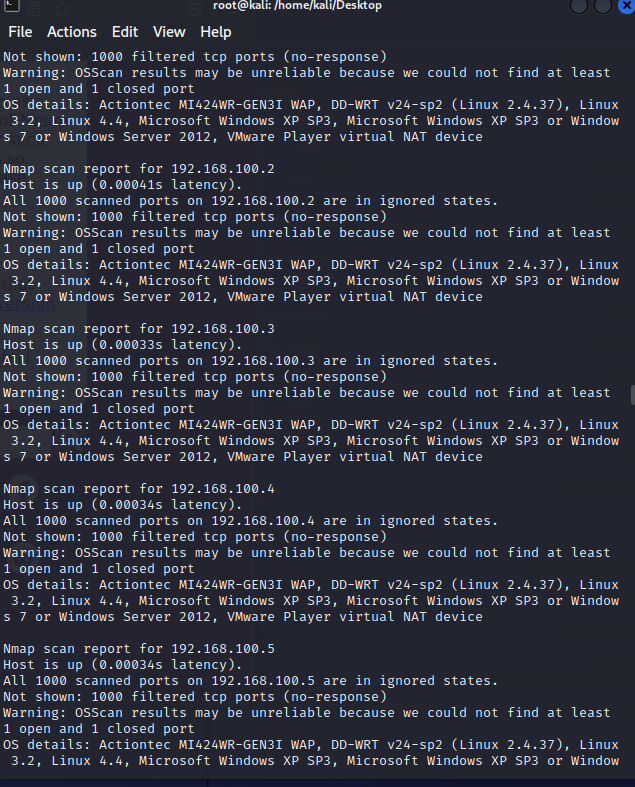


* Các hệ điều hành có thể có của địa chỉ thứ 2 là:
  + ctiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.



* Các hệ điều hành có thể có của địa chỉ thứ 255 là:
  + Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012.





Dịch vụ được chạy trên từng port này hiển thị ở phần Not shown và tất cả port đều chạy trên dịch vụ tcp.

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.

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)** |
|  |  |  |
|  |  |  |