BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

***Họ và tên sinh viên:*** Nguyễn Thanh Tùng

***MSSV:*** 0850080052

**MỤC LỤC**

[**1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap** 2](#_Toc133437226)

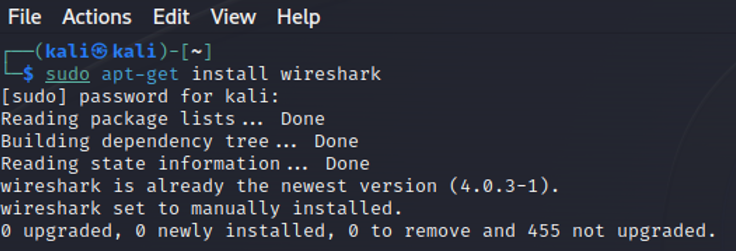
[**1.1. Kịch bản 1:** 2](#_Toc133437227)

[**1.2. Kịch bản 2:** 5](#_Toc133437228)

[**1.3. Kịch bản 3:** 9](#_Toc133437229)

[**2. Thu thập thông tin hệ thống** 11](#_Toc133437230)

**sudo apt-get install wireshark**



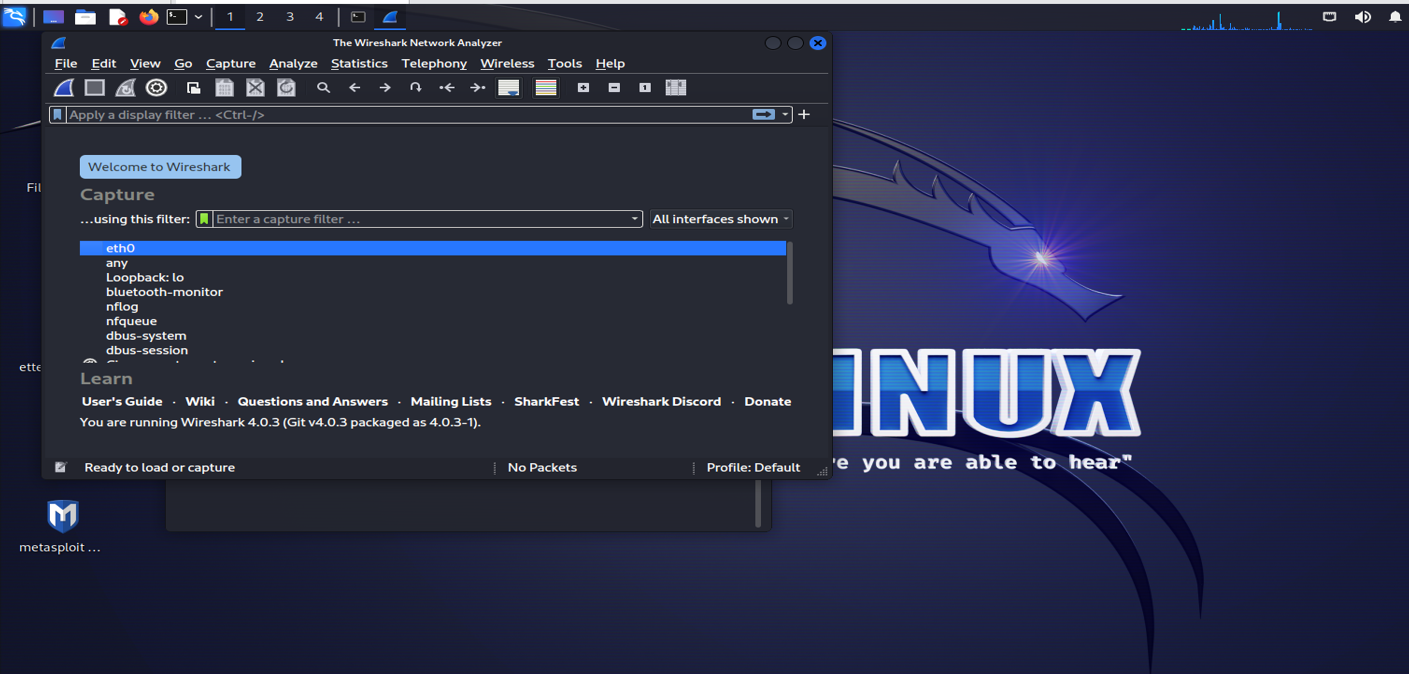
**Kết quả thực hiện**

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

## **1.1. Kịch bản 1:**

Bước 1: Truy cập máy ảo Kali Linux.

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

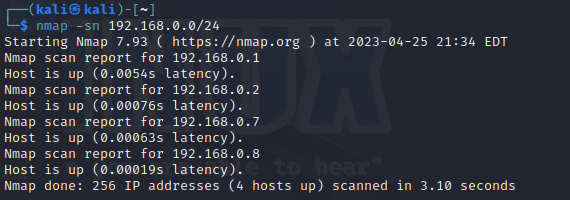


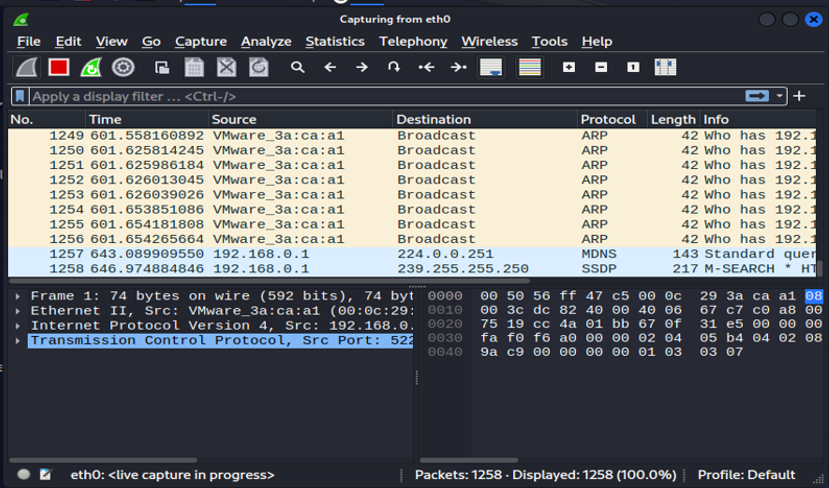
Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

**nmap -sn 192.168.0.0/24.**

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

như sau:

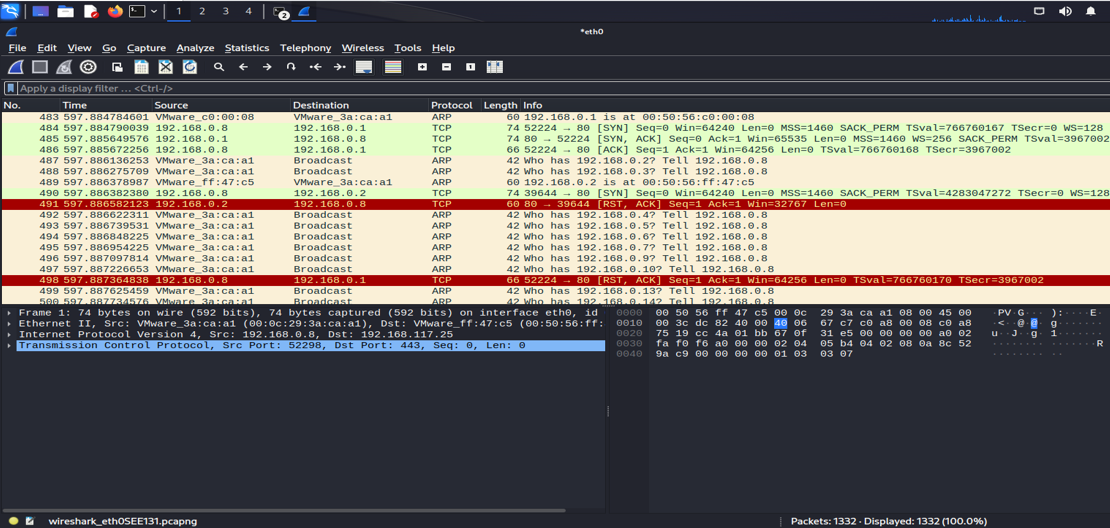




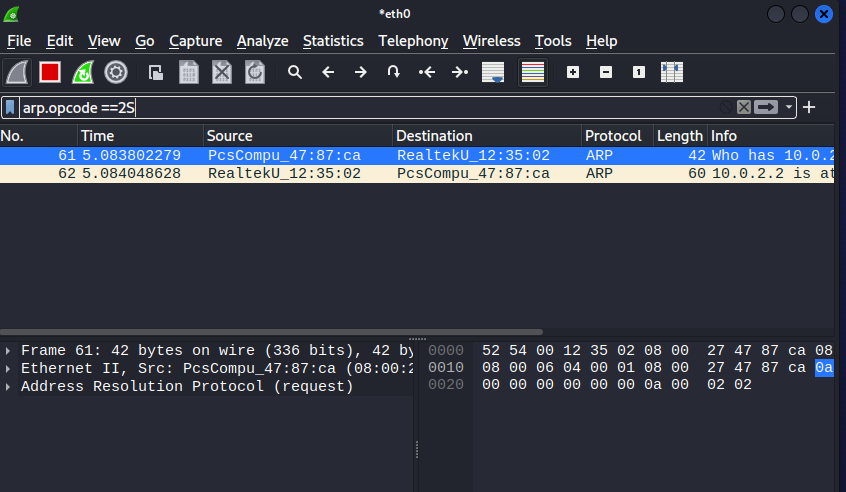
Bước 5: Dừng bắt gói tin trên Wireshark.

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 192.168.0.0/24

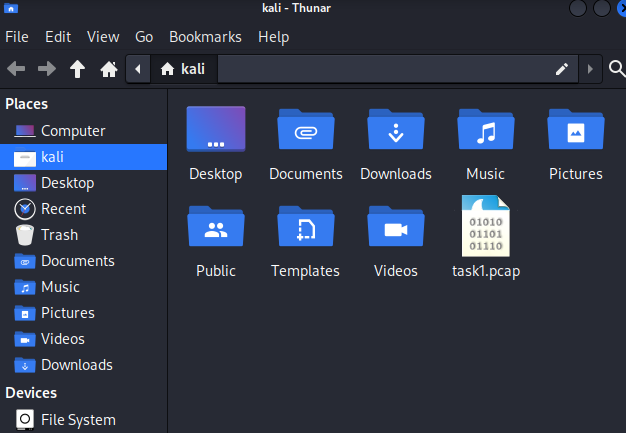


Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



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.

Bước 6: lưu file với tên là task1.pcapng



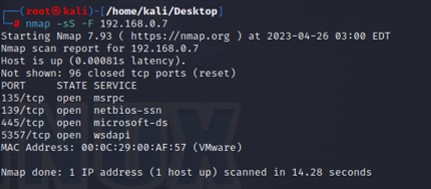
## **1.2. Kịch bản 2:**

Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ Domain (số hiệu cổng ứng dụng là 53).

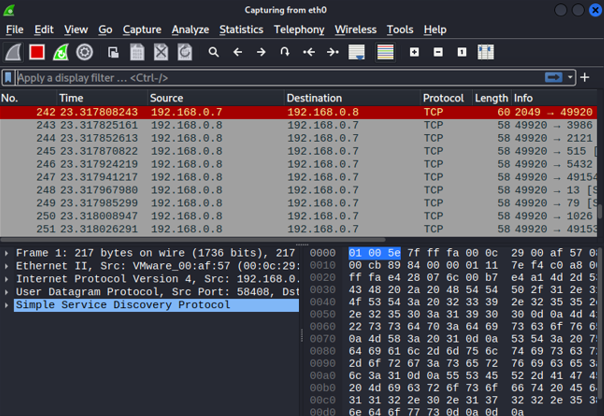
Bước 1: Truy cập máy ảo Attack

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

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: sudo su để đăng nhập với quyền root, sau đó dùng lệnh **nmap -sS -F 192.168.0.7**



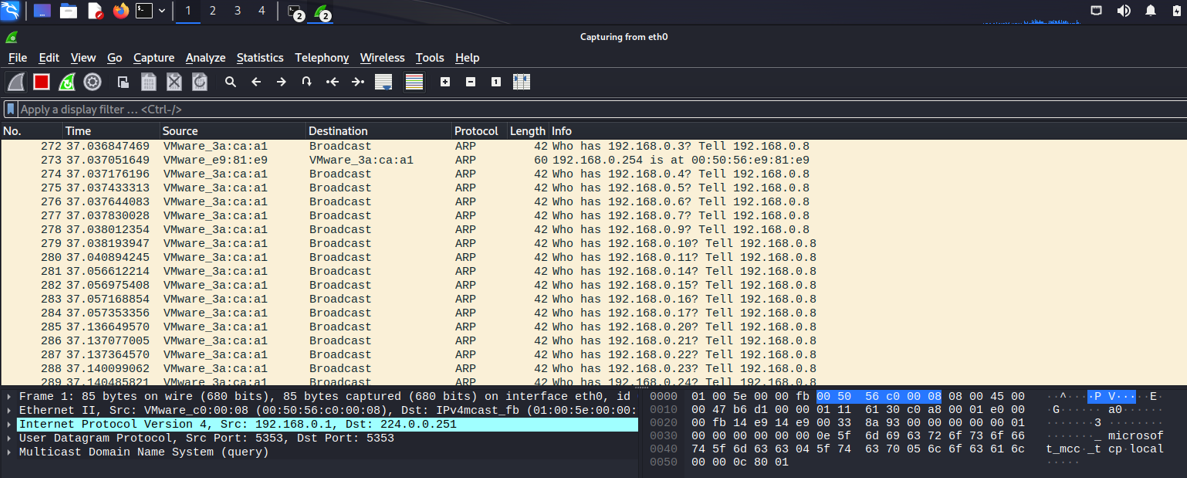
Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.0.2, 192.168.0.254 và 192.168.0.8 có trạng thái cổng dịch vụ là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Domain.

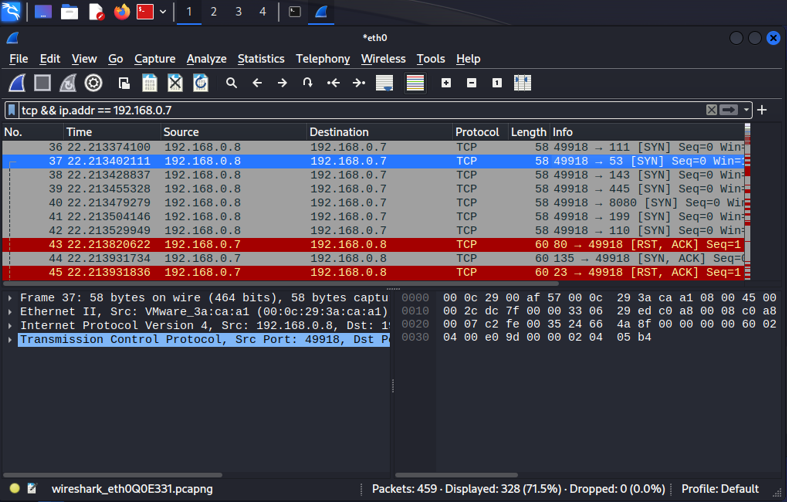


Bước 5: Dừng bắt gói tin trên Wireshark

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 192.168.0.7.

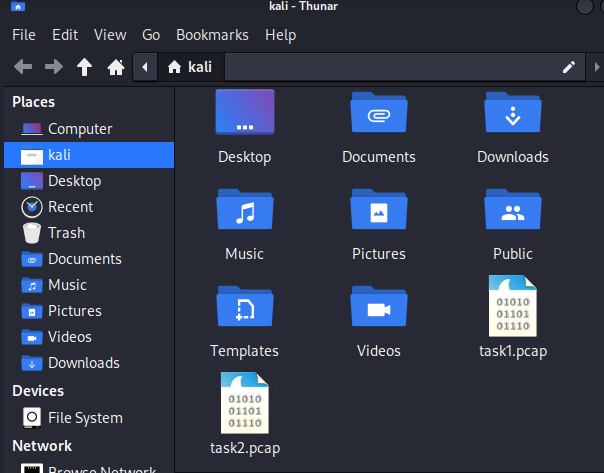


Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 53 của các máy đang hoạt động.

Sử dụng giá trị tcp && ip.addr == 192.168.0.7 ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 37 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 53 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Domain).

Kết quả: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

Bước 6: Lưu tập tin với file task2.pcapng



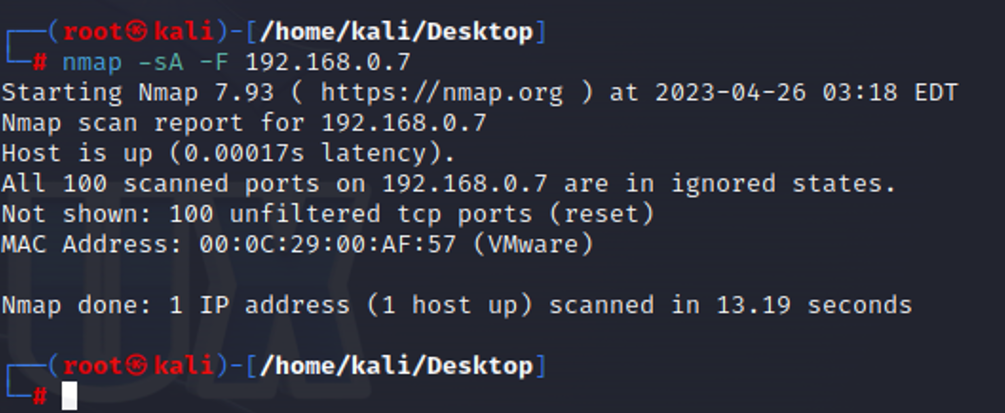
## **1.3. Kịch bản 3:**

Bước 1: Truy cập máy ảo Attack

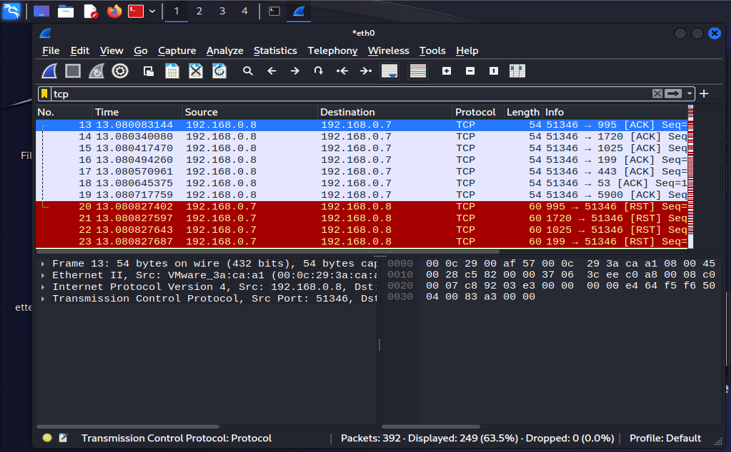
Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: **nmap -sA -F 192.168.0.7**

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 tất cả 100 cổng được quét trên địa chỉ IP 192.168.0.7 đang trong trạng thái bị bỏ qua (ignored), có nghĩa là không có máy chủ hoặc dịch vụ nào phản hồi trên các cổng này. Tuy nhiên, kết quả quét cũng cho thấy địa chỉ MAC của máy tính đích được quét là 00:0C:29:00:AF:57, cho thấy máy tính đó là một máy ảo VMware. Vì vậy, máy tính của bạn không bị gì cả, nhưng không có bất kỳ dịch vụ hoặc máy chủ nào phản hồi trên các cổng được quét.



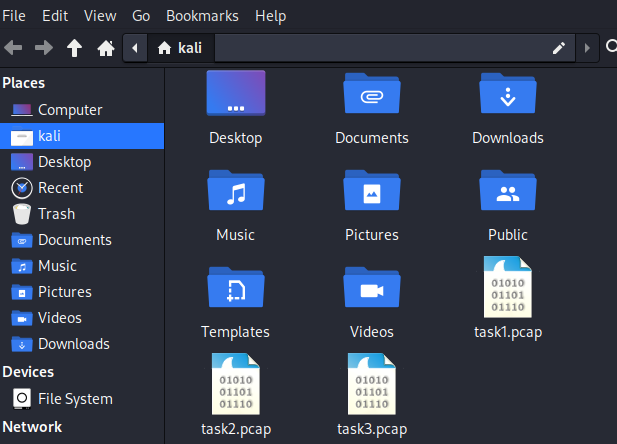
Bước 5: dừng bắt gói tin wireshark và kiểm tra.



Sử dụng giá trị tcp && ip.addr == 192.168.0.7 ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 53, 143, 443 được quét ở kịch bản 2 vẫn chạy.

Kết quả: Lệnh nmap –sA –F 192.168.0.7 trong nmap được sử dụng để quét mạng bằng phương thức ACK. Tùy chọn -F chỉ quét các cổng phổ biến nhất. Khi sử dụng tùy chọn này, nmap sẽ gửi một yêu cầu ACK tới các cổng mạng đích và chờ đợi phản hồi. Nếu phản hồi ACK được trả về, nó cho biết rằng cổng đó có thể đang mở hoặc bị chặn bởi tường lửa. Nếu không có phản hồi, nó cho biết rằng cổng đó bị đóng. Việc sử dụng ACK quét có thể giúp người dùng phát hiện các cổng bị chặn bởi tường lửa hoặc các thiết bị bảo mật.

Bước 6: lưu file với tên task3.pcapng.



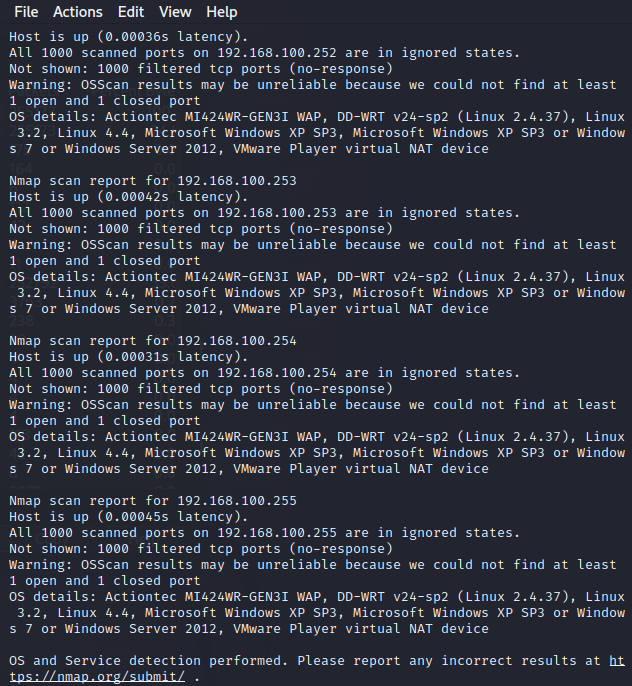
# **2. Thu thập thông tin hệ thống**

Để xem thông tin hệ điều hành của một máy chủ từ xa bằng Nmap, sử dụng tùy chọn “-O” trong lệnh quét của Nmap. Ví dụ: “nmap -O <địa chỉ IP>” sẽ thực hiện một cuộc tấn công thăm dò trên máy chủ và cố gắng xác định hệ điều hành đang chạy trên máy chủ đó

Để quét thông tin dịch vụ sử dụng lệnh “nmap -sV” trong Terminal. Lệnh này sẽ quét tất cả các cổng mạng trên máy tính của bạn và hiển thị thông tin chi tiết về các dịch vụ đang chạy trên các cổng đó1. Bạn cũng có thể chỉ định một địa chỉ IP cụ thể để quét bằng cách nhập "nmap -sV <địa chỉ IP>".

* Chúng ta có thể kết hợp lại thành một lệnh nmap -sV –O để có thể kiểm tra cả hệ điều hành lận thông tin dịch vụ.

Tiếp theo 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



-có thể thấy được hệ điều hành đã thu thấp được ở các dòng OS details.