BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

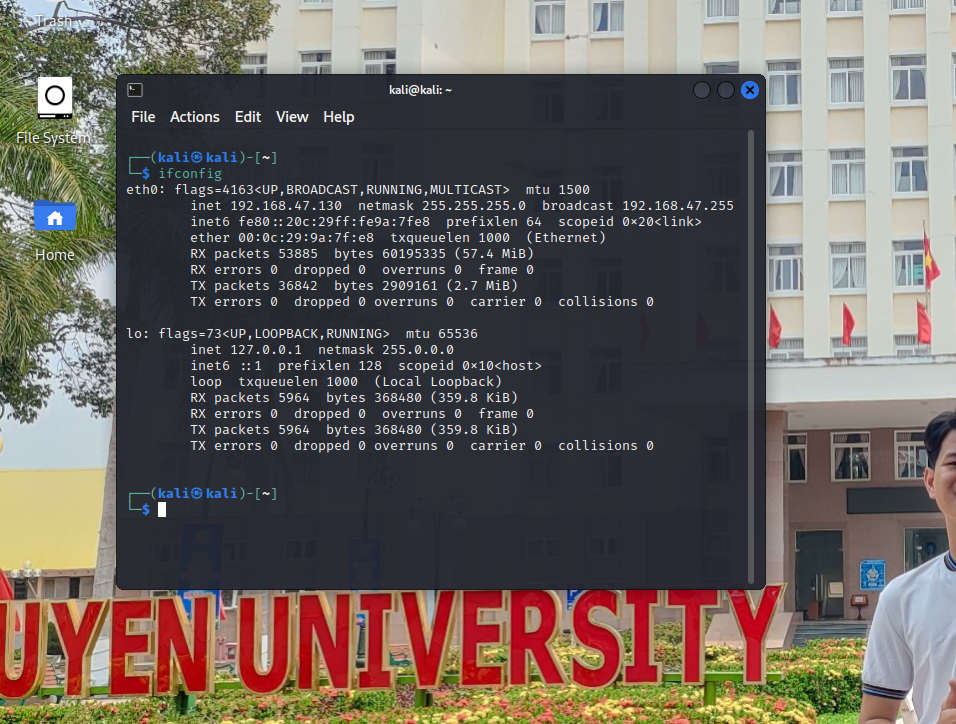
***Họ và tên sinh viên: Nguyễn Thanh Ý***

***MSSV: 0850080056***

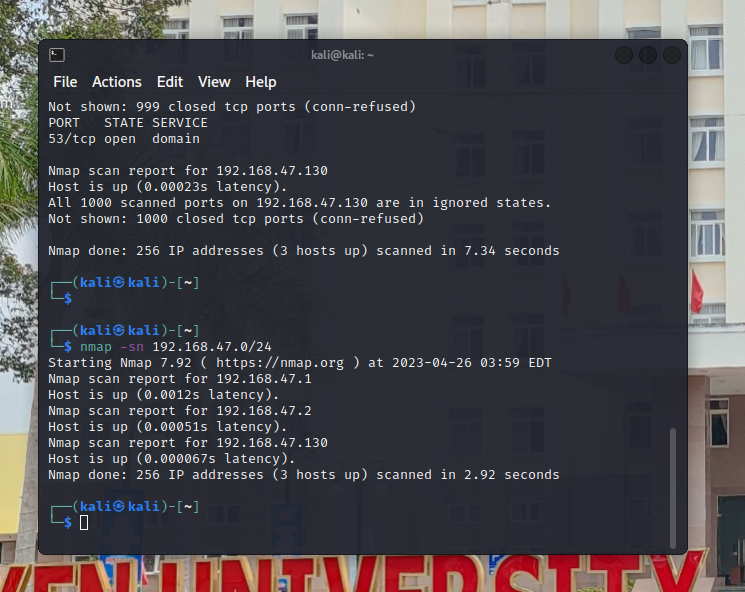
**KẾT QUẢ THỰC HÀNH**

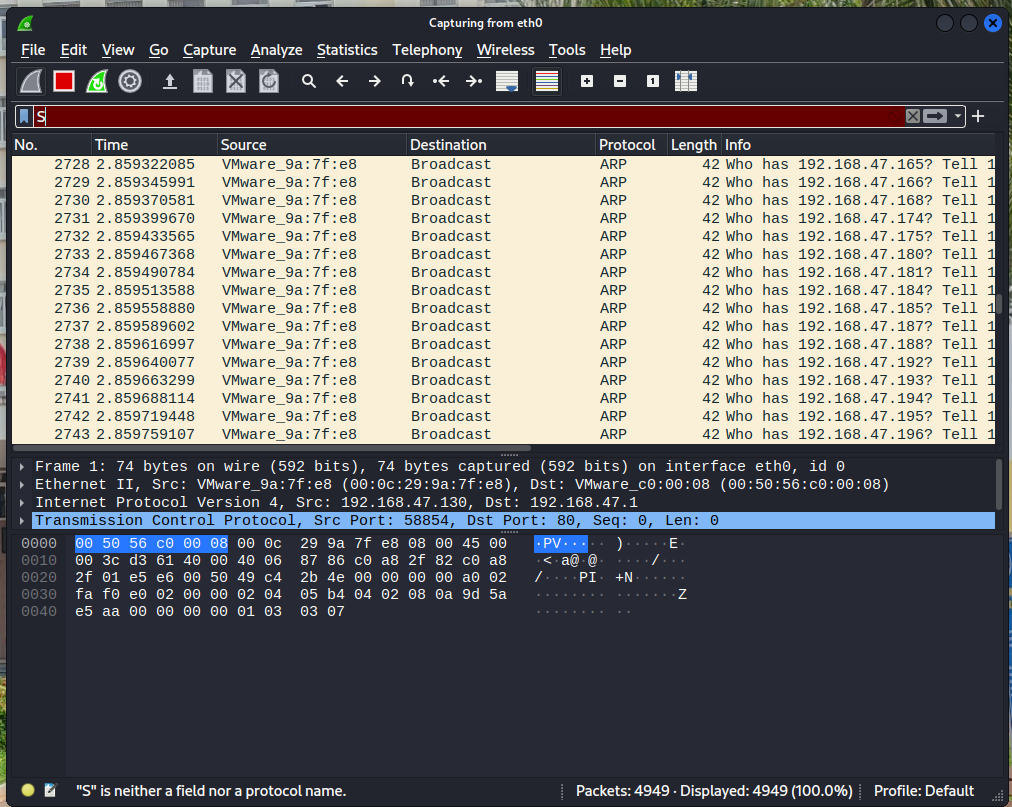
1. **Luyện tập tại nhà**
   1. **Quét thăm dò mạng**

* Kiểm ta ip là: 192.168.47.130



* Chạy lệnh và bât wireshark để bắt gói tin: nmap –sn 192.168.47.0/24

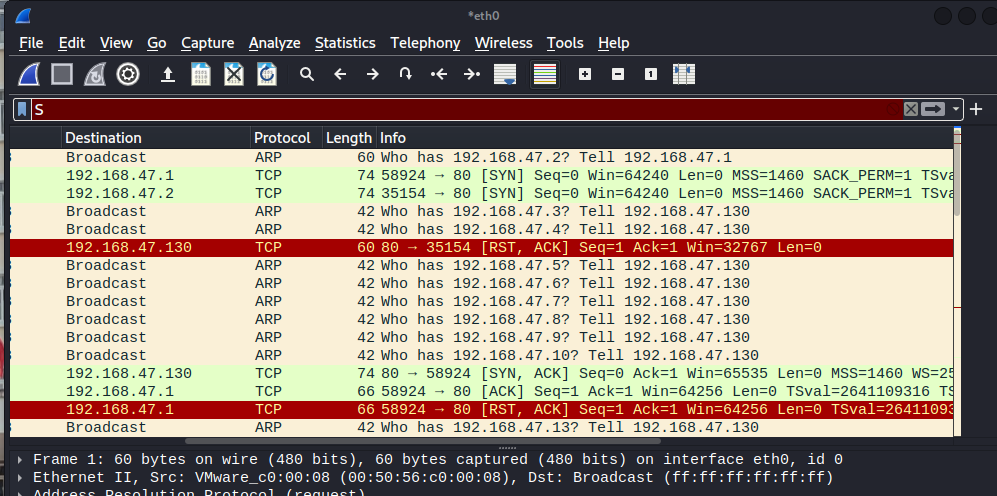




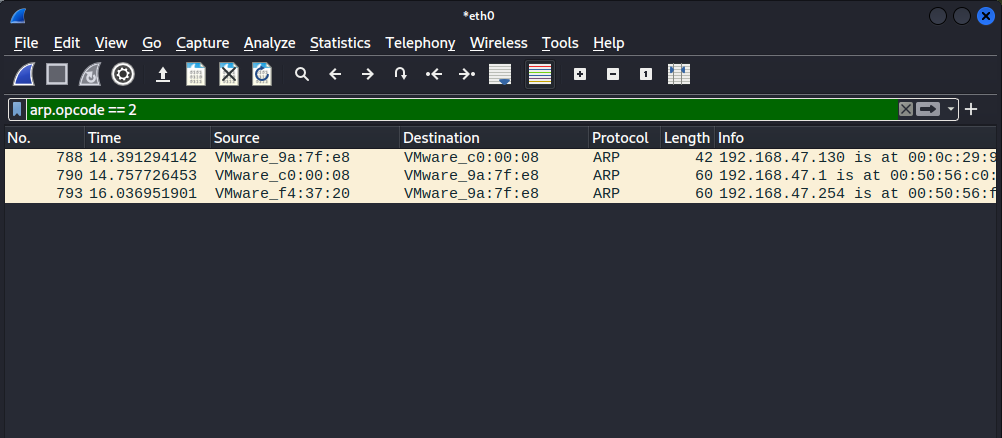
Có thể thấy ngoài địa chỉ 192.168.47.130 là địa chỉ của máy tấn công thì còn 2 nút mạng nữa đang  hoạt động có địa chỉ là 192.168.47.2 và 192.168.47.1

**Phân tích lưu lượng**

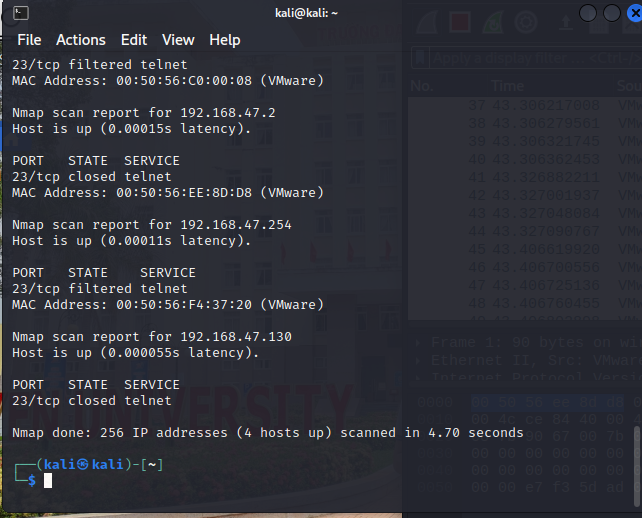
* Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn  công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính  trong mạng 192.168.47.0/24



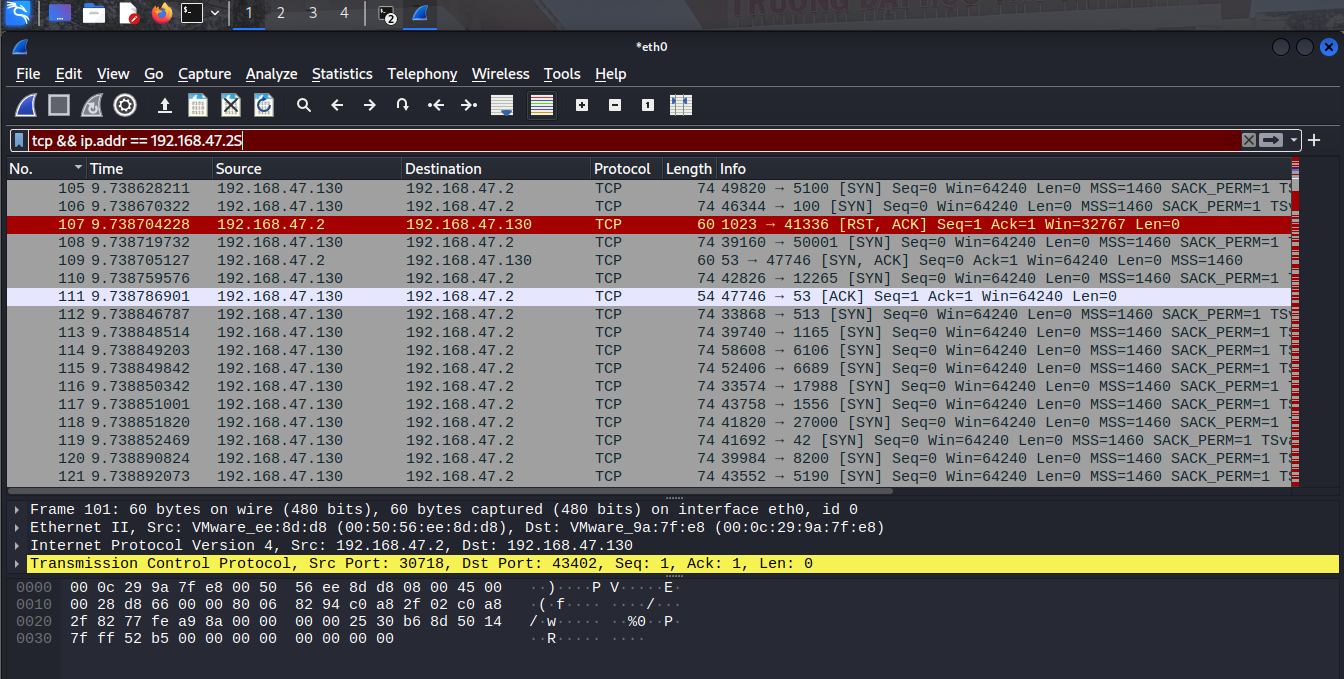
* Khi áp dụng arp.opcode == 2

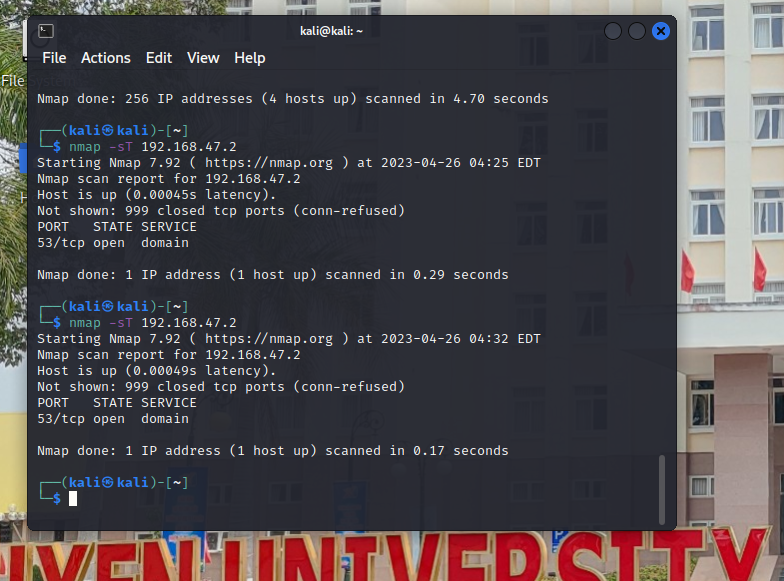


* 1. **Quét thăm dò dịch vụ**

****

* 1. **Quét cổng dịch vụ**

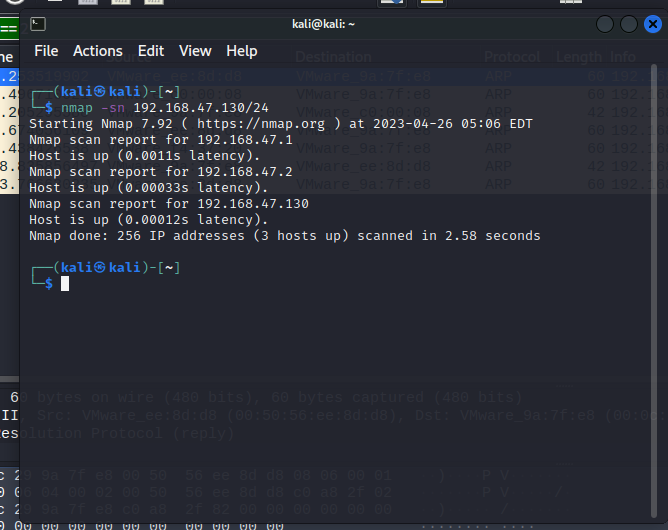
****

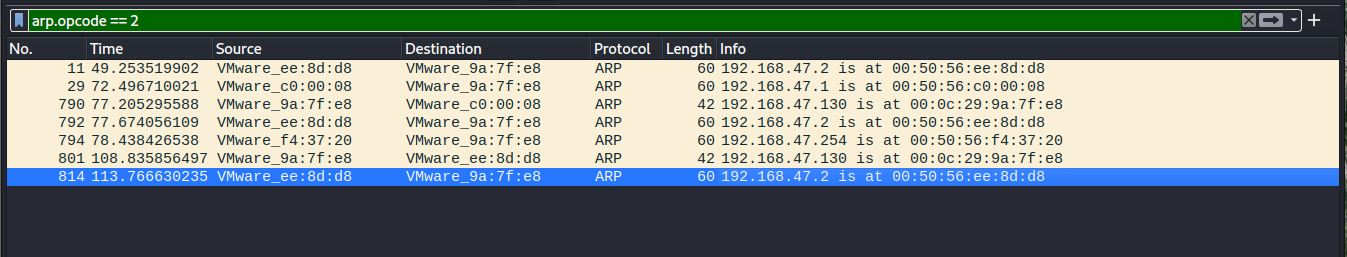
****

# **2. Yêu cầu thực hành trên lớp**

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

Chạynmap –sn 192.168.47.130/24

****

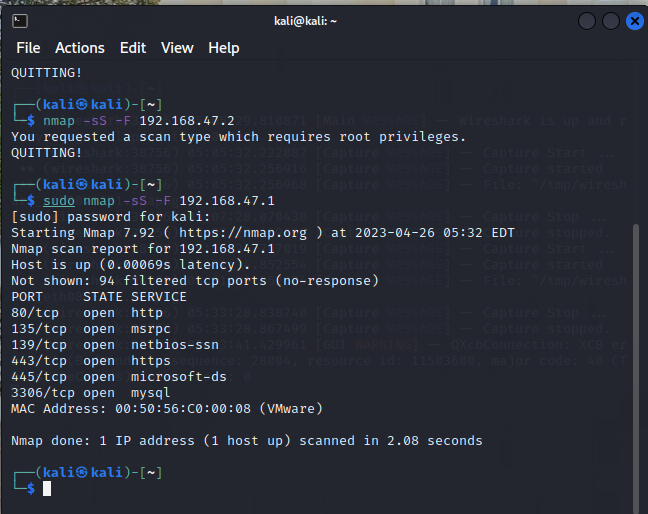


sử dụng giá trị **arp.opcode == 2** cho bộ lọc, chúng ta có thể thấy  các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong  kết quả quét mạng bằng công cụ nmap là các lớp mạng 192.168.47.1 và 192.168.47.2

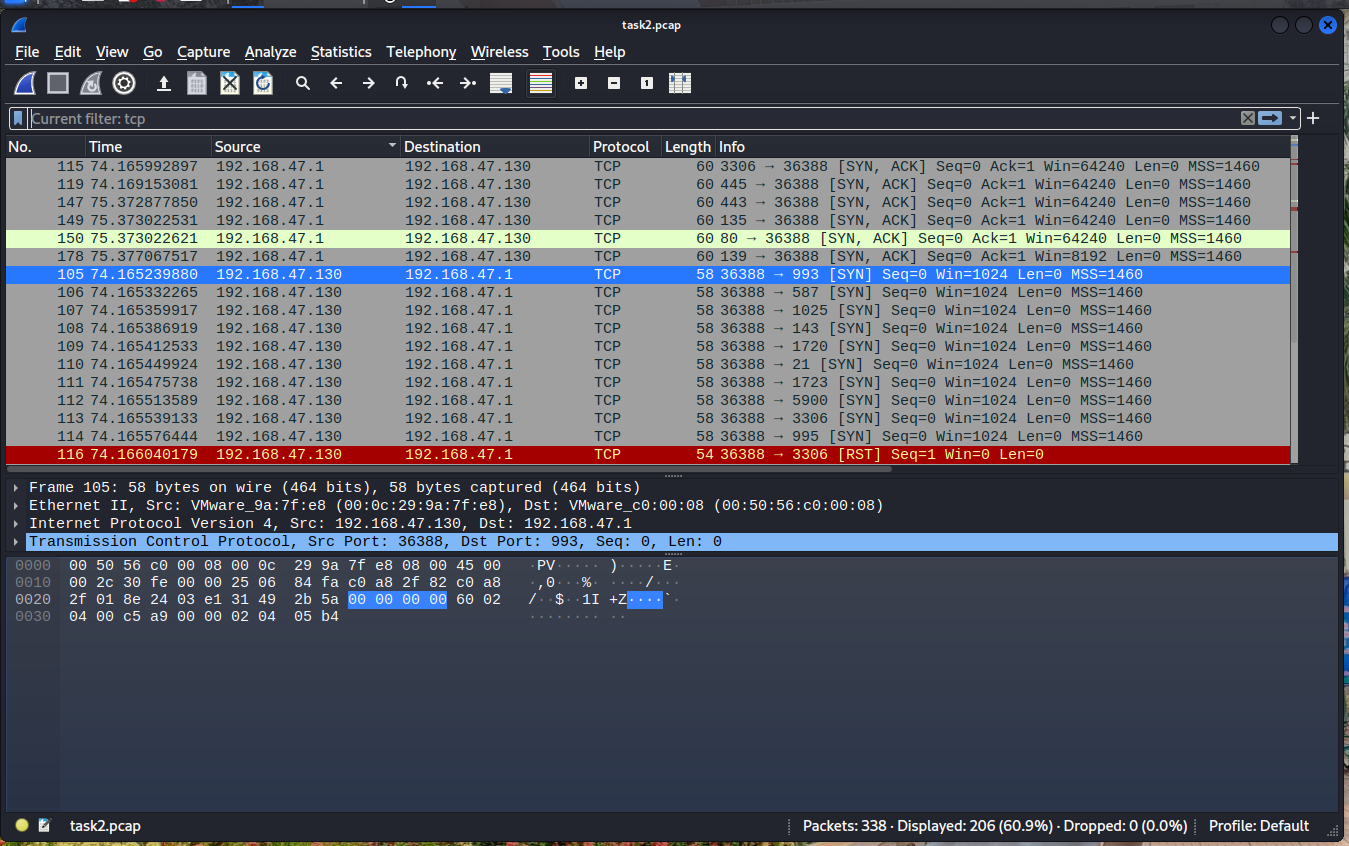
**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

## **2.2. Kịch bản 2**

Chạy sudonmap –sS -F 192.168.47.1



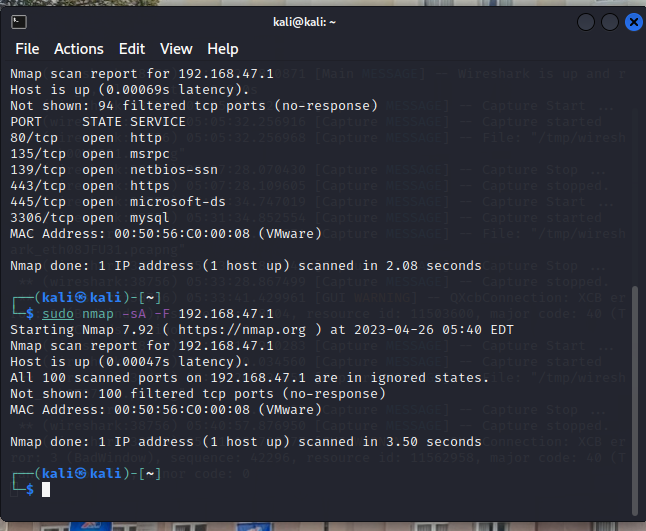
Phân tích lưu lượng

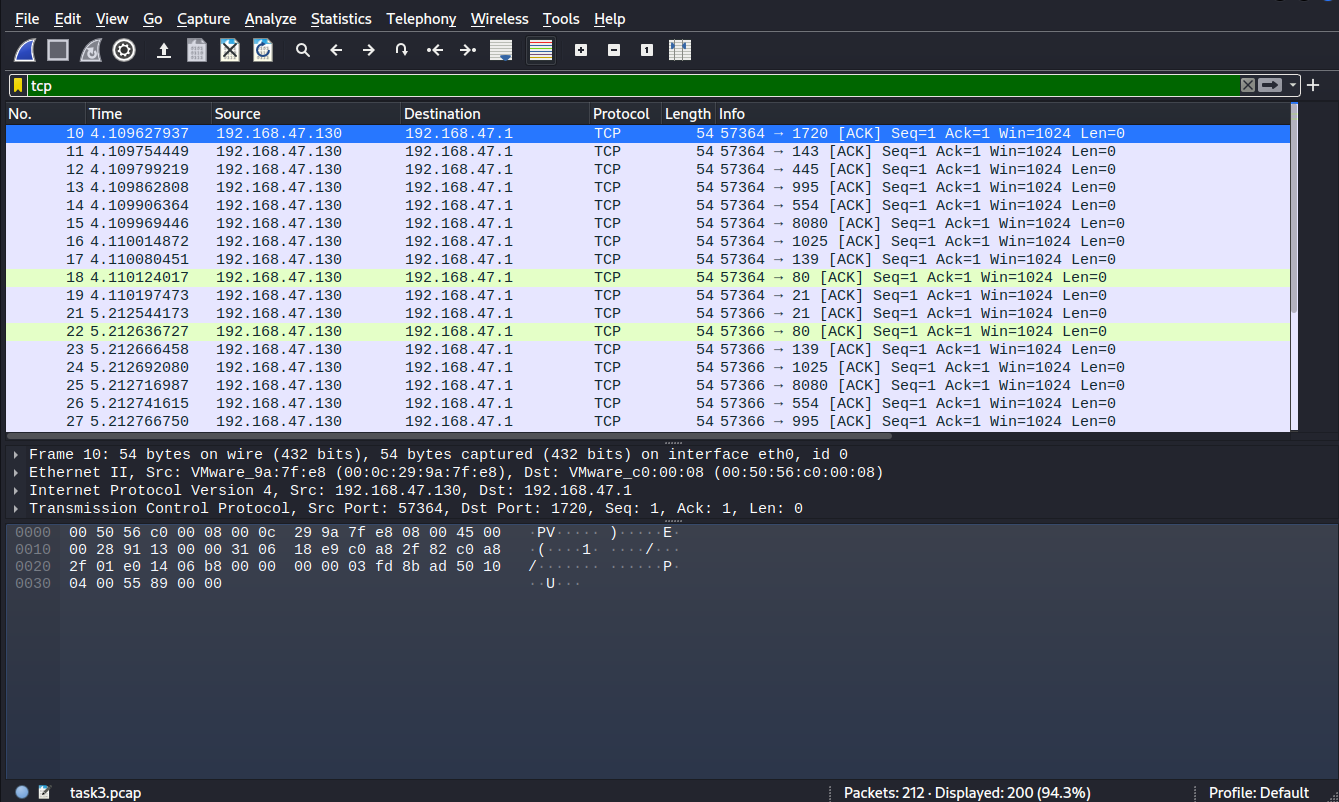


Lệnh quét nmap –sS –F được sử dụng để thực hiện một quét đầy đủ (TCP SYN scan) và nhanh (Fast scan) của một địa chỉ IP mục tiêu. Kỹ thuật quét này sử dụng giao thức TCP để tìm kiếm các cổng đang mở trên máy chủ đích bằng cách gửi các gói tin SYN đến các cổng cụ thể và xem xét phản hồi. Kết quả quét sẽ cho phép người dùng biết được các dịch vụ và ứng dụng đang chạy trên các cổng mở của máy chủ đích. Dựa trên lệnh quét này, chúng ta có thể nhận thấy rằng kỹ thuật quét sử dụng là TCP SYN scan và Fast scan. Lệnh -sS được sử dụng để chỉ định quét TCP SYN scan, trong đó các gói tin SYN được gửi đến các cổng để xem xét phản hồi. Lệnh -F được sử dụng để chỉ định quét Fast scan, nghĩa là chỉ quét một số cổng phổ biến để tìm kiếm các dịch vụ và ứng dụng đang chạy trên các cổng này.

## **2.3. Kịch bản 3**

Chạy sudonmap –sA -F 192.168.47.1



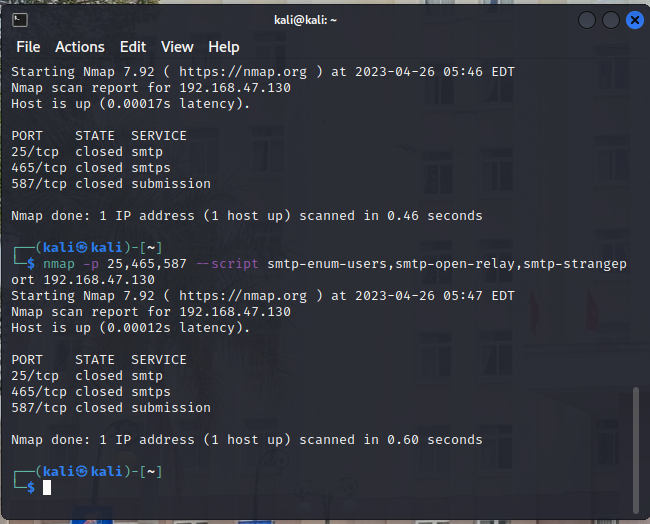


Lệnh quét nmap –sA –F được sử dụng để thực hiện một quét đầy đủ (ACK scan) và nhanh (Fast scan) của một địa chỉ IP mục tiêu. Kỹ thuật quét này sử dụng giao thức TCP để tìm kiếm các cổng đang mở trên máy chủ đích bằng cách gửi các gói tin ACK đến các cổng cụ thể và xem xét phản hồi. Kết quả quét sẽ cho phép người dùng biết được các dịch vụ và ứng dụng đang chạy trên các cổng mở của máy chủ đích.

Dựa trên lệnh quét này, chúng ta có thể nhận thấy rằng kỹ thuật quét sử dụng là ACK scan và Fast scan. Lệnh -sA được sử dụng để chỉ định quét ACK scan, trong đó các gói tin ACK được gửi đến các cổng để xem xét phản hồi. Lệnh -F được sử dụng để chỉ định quét Fast scan, nghĩa là chỉ quét một số cổng phổ biến để tìm kiếm các dịch vụ và ứng dụng đang chạy trên các cổng này.

# **3. Thu thập thông tin hệ thống**

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



Chạy lệnh nmap -p 25,465,587 --script smtp-enum-users,smtp-open-relay,smtp-strangeport 192.168.47.130

Trong đó: -p 25,465,587: Tham số này chỉ định cổng cần quét, ở đây là các cổng liên quan đến giao thức SMTP, bao gồm cổng 25, 465 và 587.

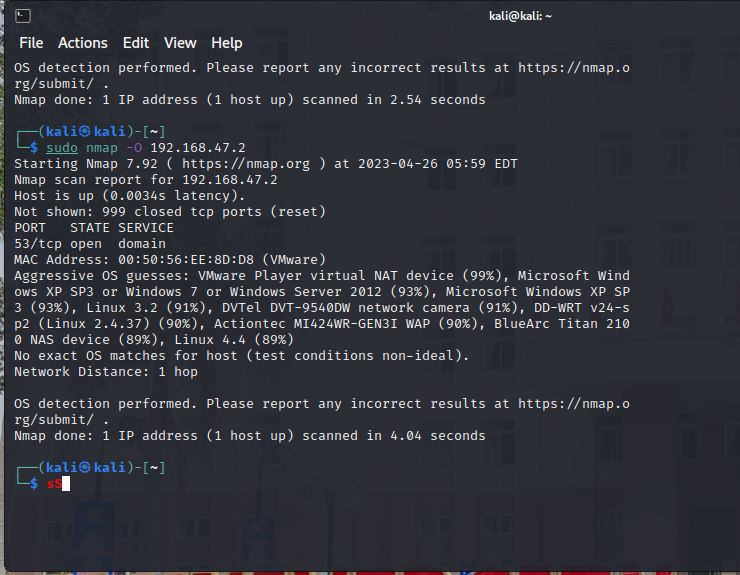
--script smtp-enum-users: Tham số này cho phép thực hiện kịch bản "smtp-enum-users" để liệt kê các tên người dùng hợp lệ trên máy chủ email.

--script smtp-open-relay: Tham số này cho phép thực hiện kịch bản "smtp-open-relay" để kiểm tra xem máy chủ email có phải là máy chủ mở relay hay không.

--script smtp-strangeport: Tham số này cho phép thực hiện kịch bản "smtp-strangeport" để kiểm tra xem có các cổng SMTP khác đang mở không.

## **3.2. Thông tin hệ điều hành:**

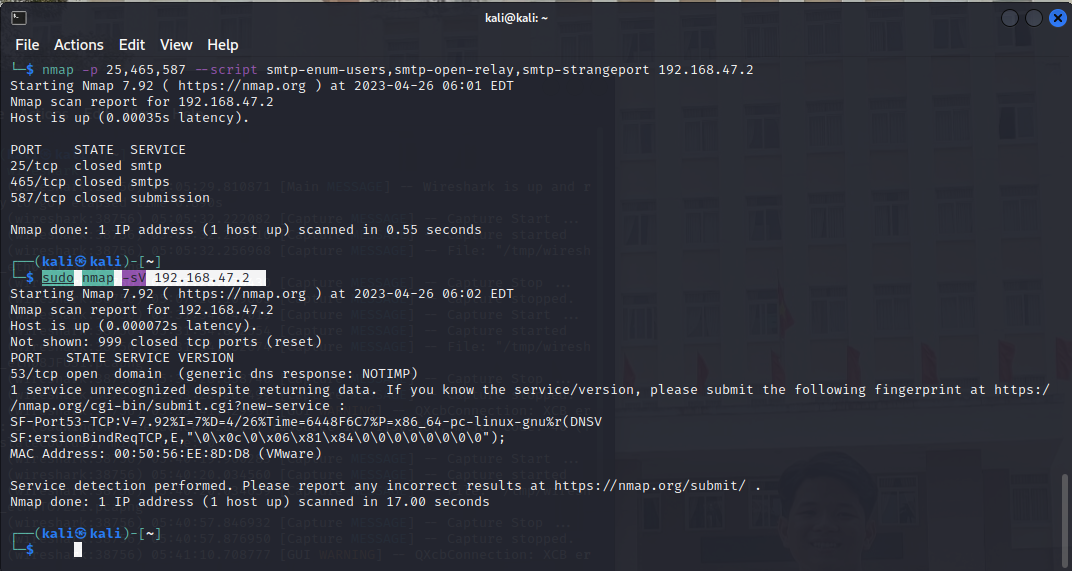
để xác định hệ điều hành của máy có địa chỉ IP là 192.168.47.2, bạn có thể sử dụng lệnh sau:



* Các phiên bản có thể là VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), Linux 3.2 (91%), DVTel DVT-9540DW network camera (91%), DD-WRT v24-sp2 (Linux 2.4.37) (90%), Actiontec MI424WR-GEN3I WAP (90%), BlueArc Titan 2100 NAS device (89%), Linux 4.4 (89%)

## **3.3. thông tin dịch vụ**

Chạy lệnh sudo nmap -sV 192.168.47.2



|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên Dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | Domain | 53/tcp | (generic dns response: NOTIMP)  1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :  SF-Port53-TCP:V=7.92%I=7%D=4/26%Time=6448F6C7%P=x86\_64-pc-linux-gnu%r(DNSV  SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\0");  MAC Address: 00:50:56:EE:8D:D8 (VMware) |

## **3.4. Tìm kiếm thông tin về các lỗ hổng**

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm,  phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| Apache HTTP Server | CVE-2021-41773 | Lỗ hổng cho phép tấn công thực thi mã từ xa và xem trộm các file không được phép truy cập. |
| Microsoft Exchange Server | CVE-2021-26855 | Lỗ hổng cho phép tấn công từ xa để truy cập trái phép vào các tài khoản và dữ liệu. |
| MySQL | CVE-2021-32527 | Lỗ hổng cho phép tấn công từ xa và tấn công từ chối dịch vụ. |