## Các kỹ thuật quét mạng của Nmap

Để quét và phát hiện các nút mạng đang có kết nối và hoạt động trên mạng, Nmap sử dụng 2 kỹ thuật quét:

* ICMP Ping Scan: Nmap gửi lần lượt các gói tin ICMP Echo Request tới tất cả các địa chỉ IP. Nếu có gói tin ICMP Echo Reply trả lại có địa chỉ nguồn là một địa chỉ IP nào đó, chứng tỏ có nút mạng sử dụng địa chỉ IP đó đang hoạt động
* ARP Ping Scan: Nmap gửi quảng bá lần lượt các gói tin ARP Request để tìm kiếm thông tin địa chỉ MAC của tất cả các địa chỉ IP. Nếu có gói tin ARP Response trả lại cho biết thông tin địa chỉ MAC của một nút nào đó, chứng tỏ nút đó đang hoạt động
* TCP SYN Ping: Nmap gửi lần lượt các gói tin TCP SYN tới cổng 80 và 443 của tất cả các địa chỉ IP trong mạng cần quét. Nếu có gói tin TCP ACK hoặc TCP RST trả về từ một địa chỉ IP nào đó, chứng tỏ có nút mạng sử dụng địa chỉ IP đó đang hoạt động. Kỹ thuật này được sử dụng khi quét mạng mục tiêu là mạng ở xa, mà nút mạng thực thi Nmap không nằm trong mạng đó.

## Các kỹ thuật quét cổng ứng dụng

Mục đích của các kỹ thuật quét cổng ứng dụng là để phát hiện các dịch vụ mạng nào đang hoạt động trên máy trạm. Giả sử, quá trình quét cổng cho kết quả cổng 80 đang mở(Open), chứng tỏ trên nút mạng đó đang cung cấp dịch vụ Web. Nmap cung cấp các kỹ thuật quét cổng sau:

* TCP SYN Scan: Nmap gửi lần lượt các gói tin TCP SYN tới các cổng cần quét. Nếu quá trình quét cổng nhận được bất kỳ gói tin TCP SYN/ACK trả lời từ một cổng nào đó, chứng tỏ cổng đó đang ở trạng thái Open
* TCP Connection Scan: tương tự như TCP SYN Scan. Điểm khác biệt nhỏ là Nmap sẽ gửi lại gói tin ACK để hoàn tất quá trình thiết lập liên kết. Sau đó, Nmap gửi lại ngay các gói tin RST để hủy liên kết này.
* TCP Null Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là NULL tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ công đó

đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.

* TCP FIN Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là FIN tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ công đó đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.
* TCP Xmas Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là FIN, PSH, và URG tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ cổng đó đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.
* TCP ACK Scan: Kỹ thuật này được sử dụng để phát hiện trên mục tiêu có sử dụng firewall hay không. Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là ACK tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ mục tiêu có thể đã được bảo vệ bởi firewall.

## Quét thu thập thông tin hệ thống

Nmap có khả năng xác định được các thông tin về hệ thống mục tiêu như phiên bản hệ điều hành hay phần mềm dịch vụ. Để thực hiện điều này, Nmap gửi các yêu cầu truy cập tới các cổng dịch vụ đang mở trên máy mục tiêu và thu thập thông tin từ thông điệp phản hồi. Thông tin này được so sánh với các bộ dấu hiêu đặc trưng mà Nmap đã có về những hệ điều hành và phần mềm phổ biến. Dựa trên dữ kiện so sánh, Nmap phán đoán được thông tin về phiên bản hệ điều hành và phần mềm dịch vụ.

Có 2 cách thức để thực hiện hoạt động quét và thu thập:

## Cách 1: nmap -sV -O Địa\_chỉ\_máy\_mục\_tiêu

* Cách 2: **nmap -A Địa\_chỉ\_máy\_mục\_tiêu**

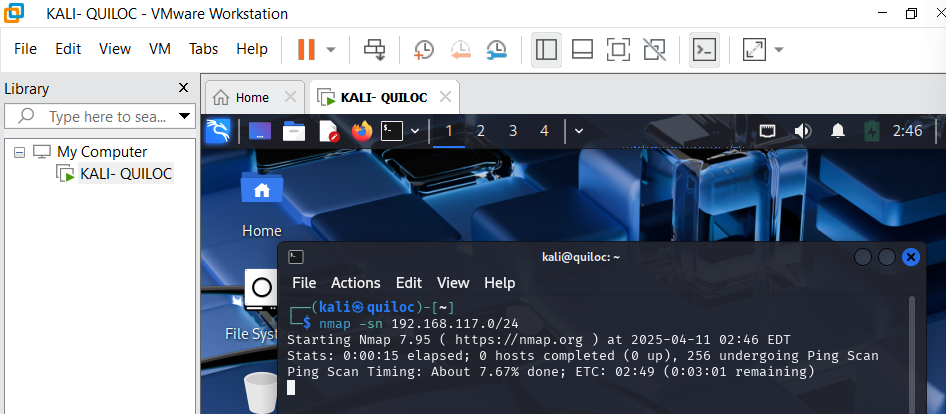
## Luyện tập tại nhà

Triển khai môi trường thực hành theo hướng dẫn.

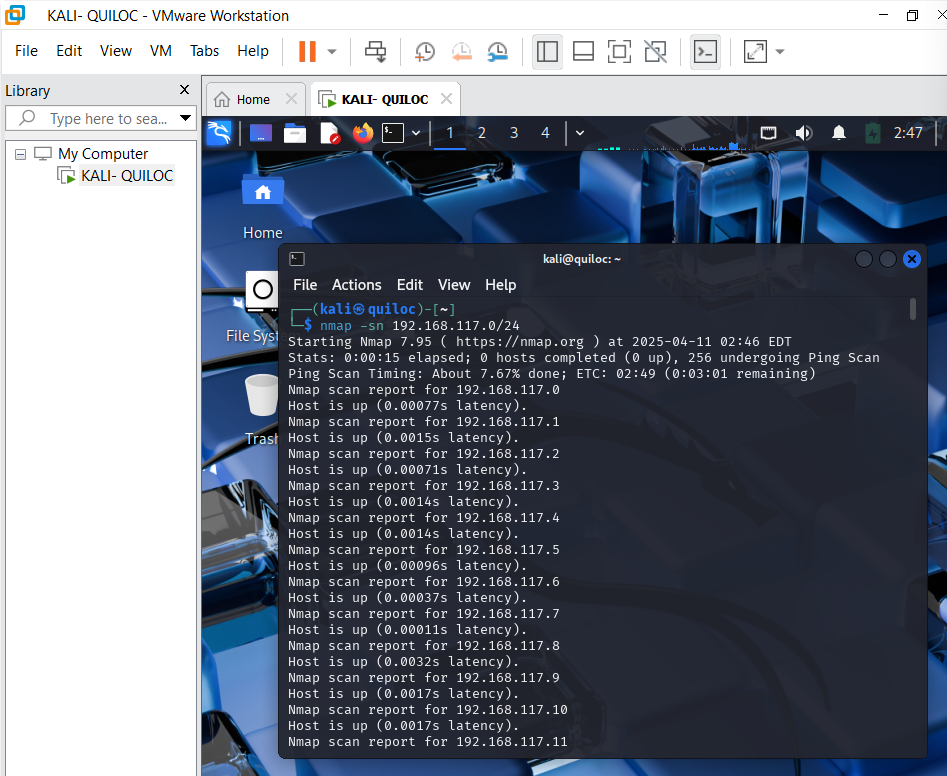
## Quét thăm dò mạng

* **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 192.168.117.0/24



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



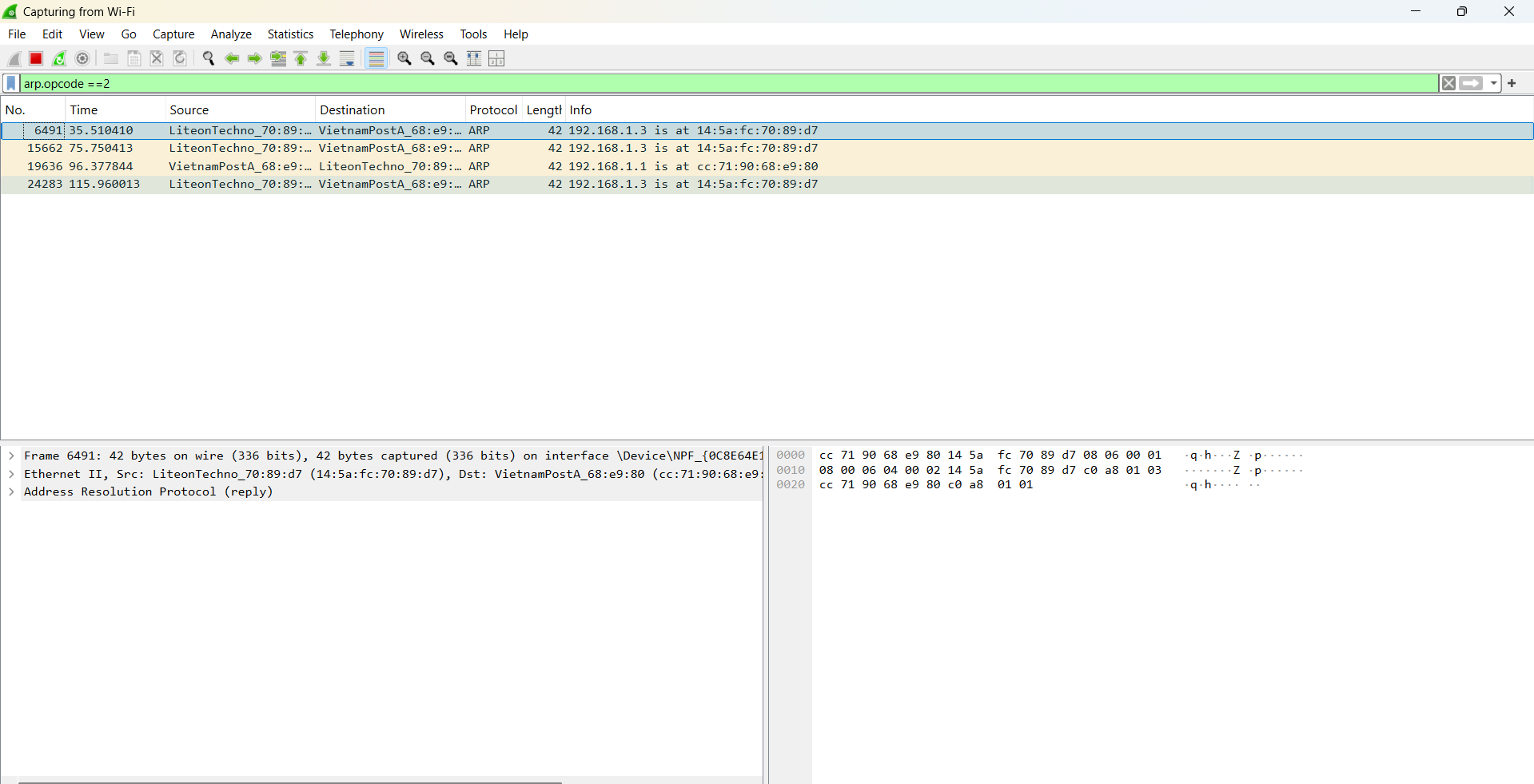
Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang

hoạt động có địa chỉ là 192.168.117.2, 192.168.117.3 và 192.168.117.13

* **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 192.168.117.0/24
* 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.

## 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:

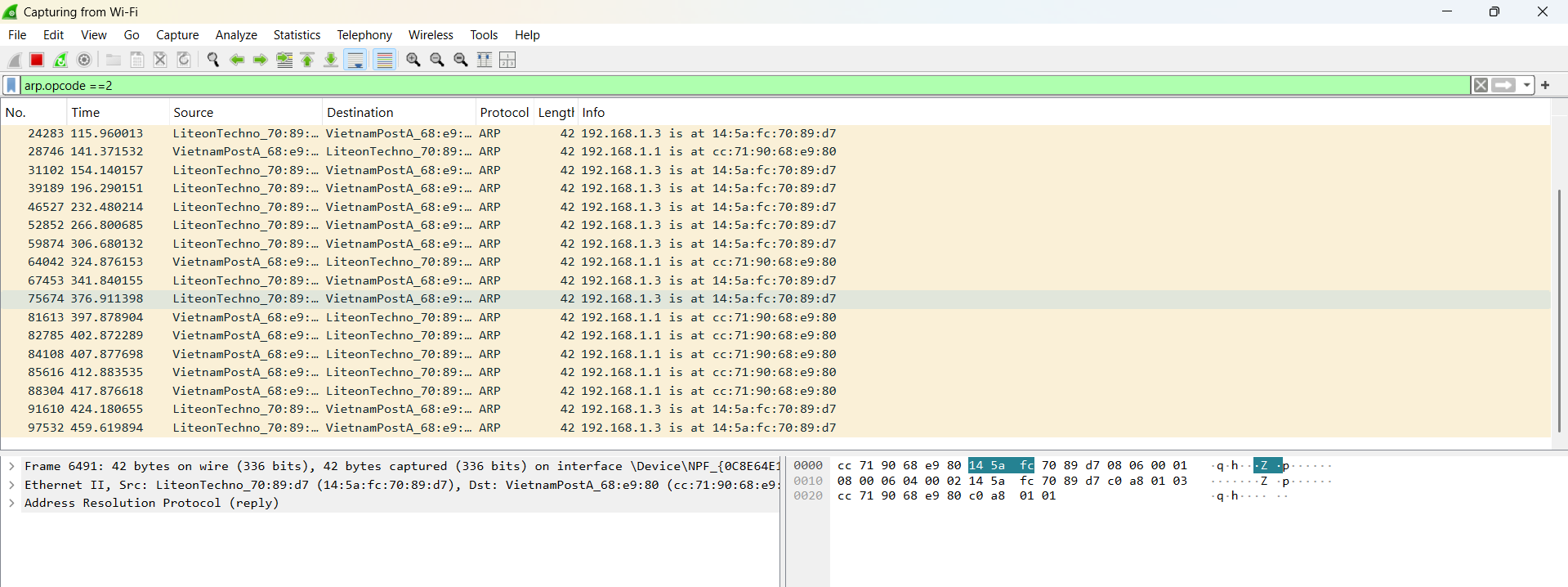
## sudo nmap -p 23 192.168.117.0/24

## 

* **Bước 4:** Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 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

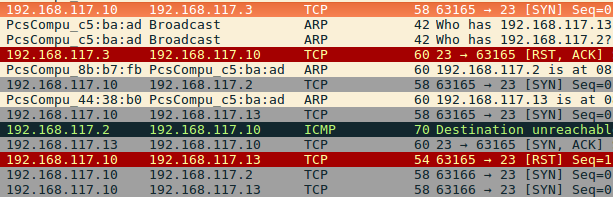
## Phân tích lưu lượng:

* 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 192.168.117.0/24.

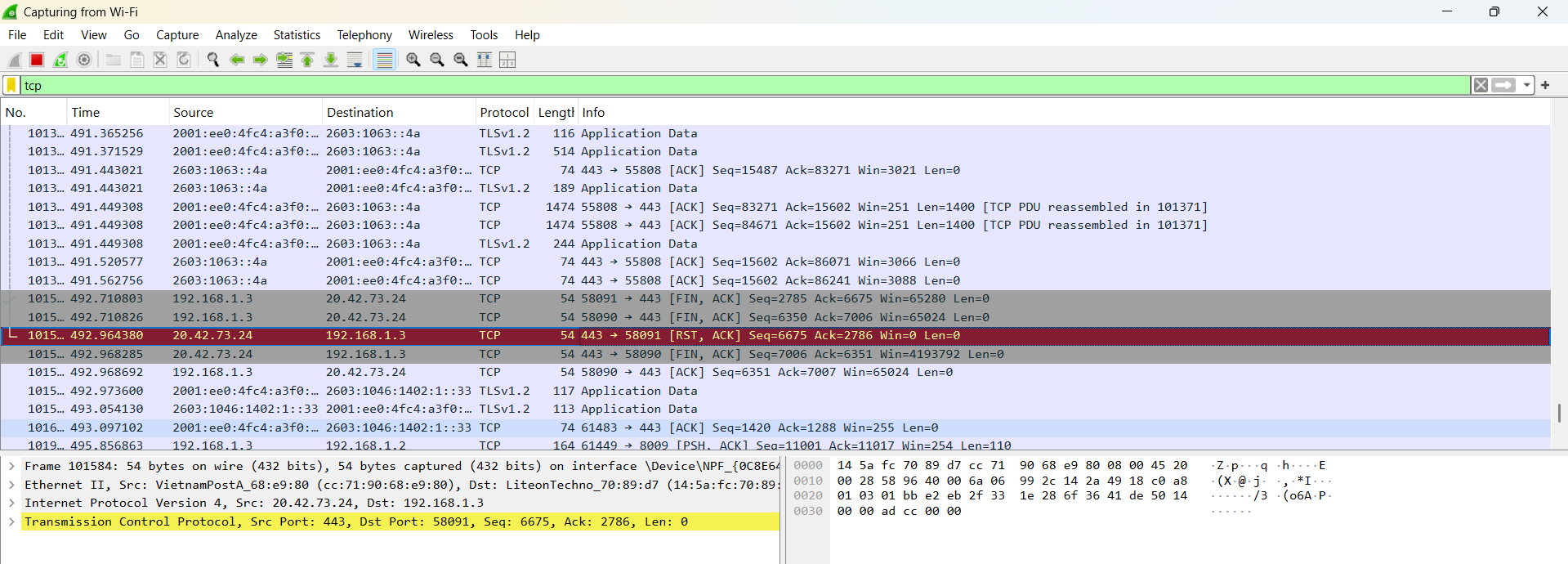


* Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP

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 192.168.117.13 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 Telnet)



**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP

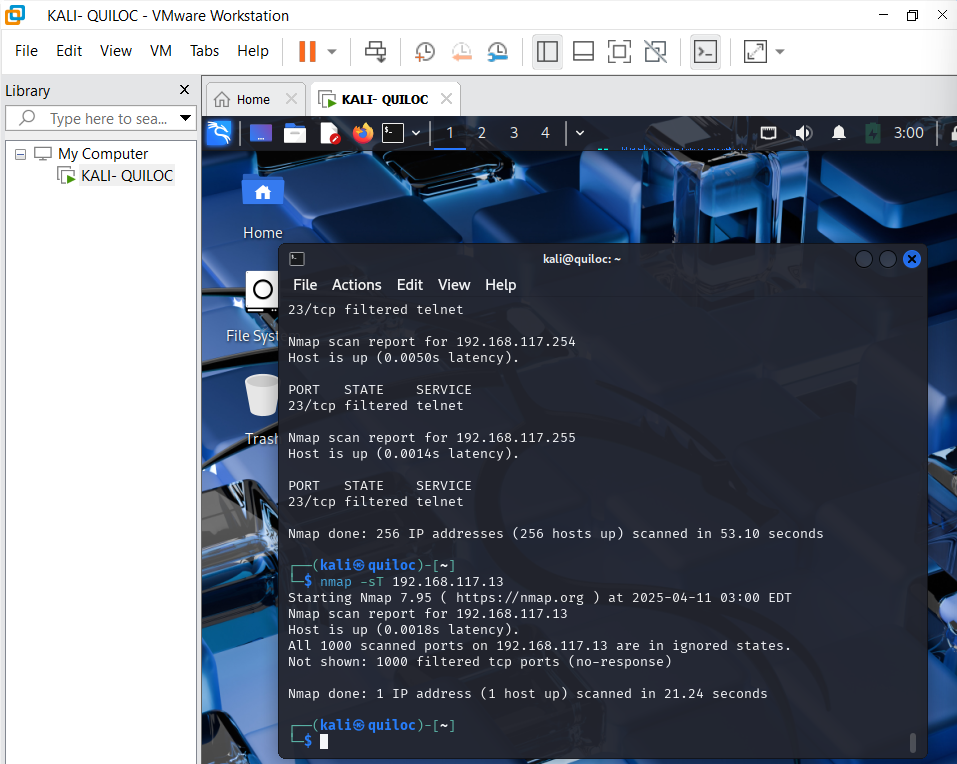
SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.

## 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 192.168.117.13

* **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 192.168.117.13 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

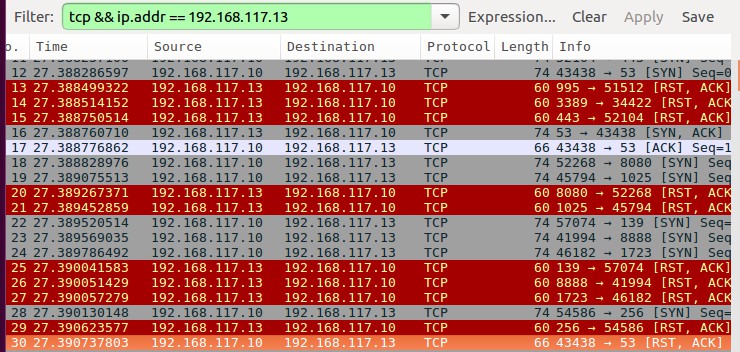
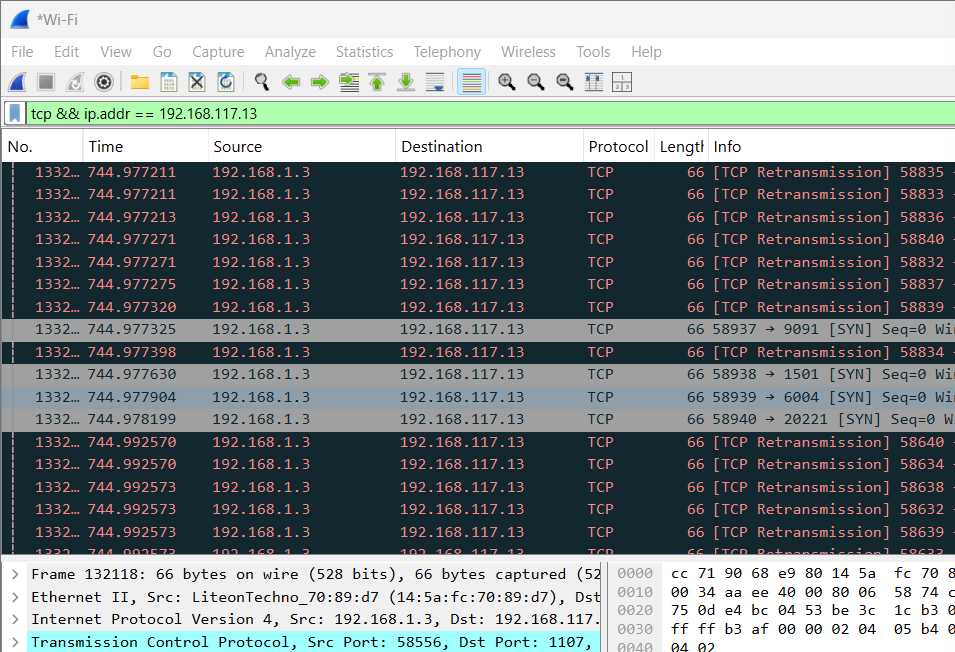
## Phân tích lưu lượng:

* Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói

tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.13.

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

* Sử dụng giá trị **tcp && ip.addr == 192.168.117.13** 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.



Link YTB

<https://youtu.be/4-eZtIGXRGU>

<https://youtu.be/sYWa3MQBTnQ>

<https://youtu.be/hmEgTMeU8_8>

Link GB