BÁO CÁO BÀI THỰC HÀNH SỐ 7

PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

Họ và tên sinh viên: Lê Nguyễn Hà My

MSSV:1050080185

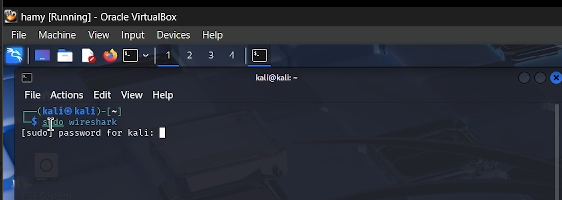
2. Luyện tập tại nhà

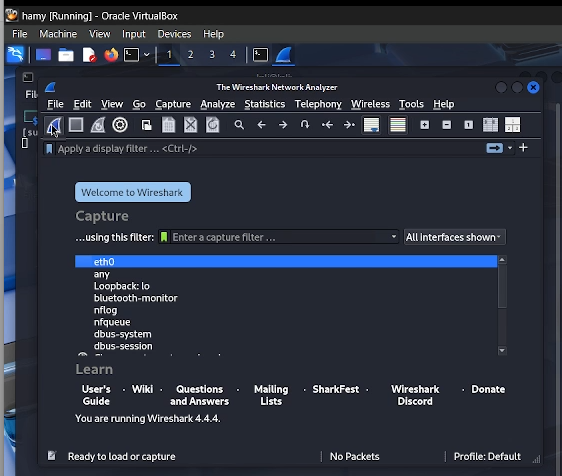
Triển khai môi trường thực hành theo hướng dẫn.

2.1. Quét thăm dò mạng

- Bước 1: Truy cập máy ảo Attack

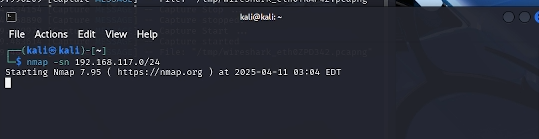
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.



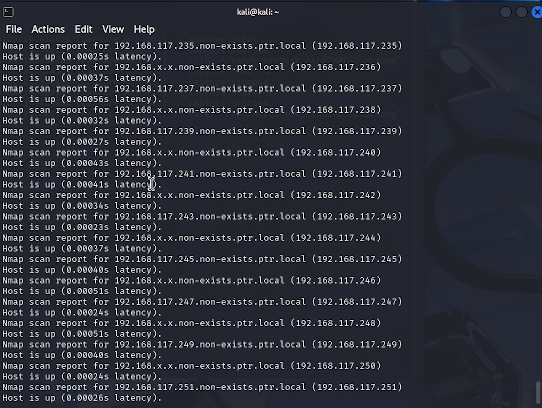


- Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

nmap –sn 192.168.117.0/24



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

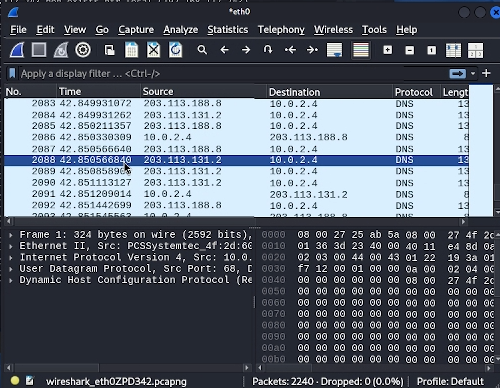


Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.2, 192.168.117.3 và 192.168.117.13

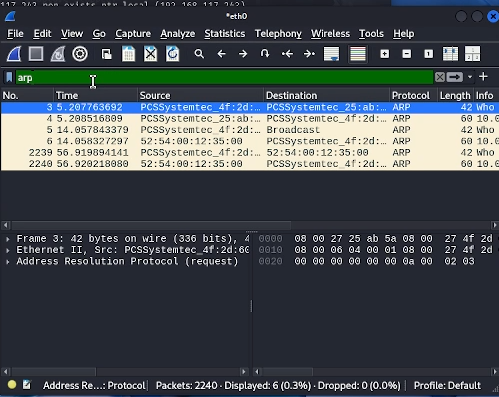
- Bước 5: Dừng bắt gói tin trên Wireshark

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.

2.2. Quét thăm dò dịch vụ

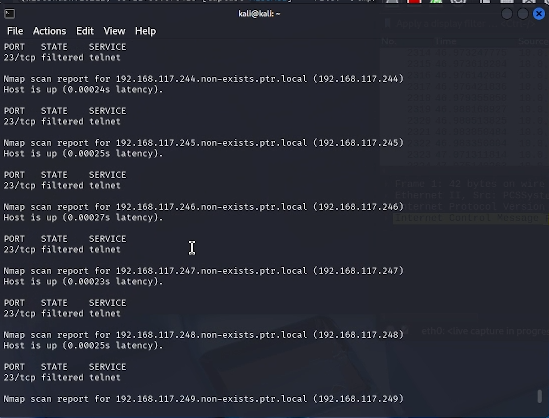
Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

- 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:

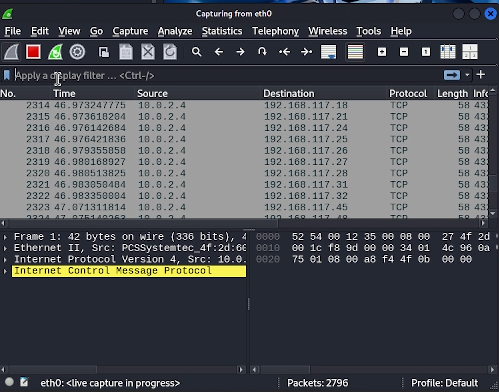
sudo nmap -p 23 192.168.117.0/24



- 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:

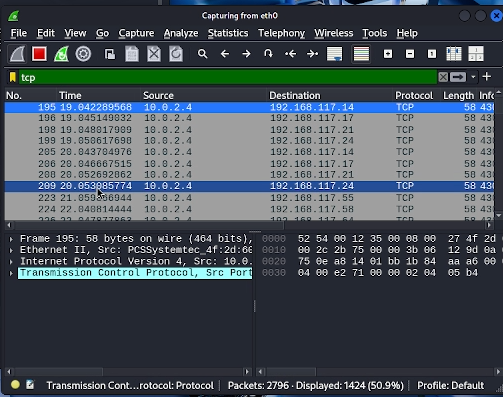


- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể

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.

2.3. Quét cổng dịch vụ

- Bước 1: Truy cập máy ảo Attack

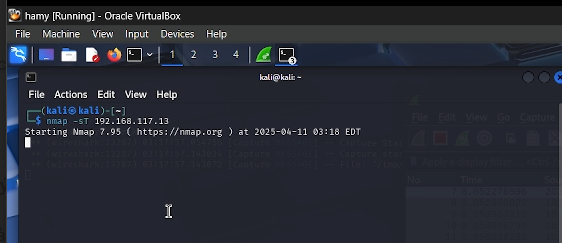
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

- 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.



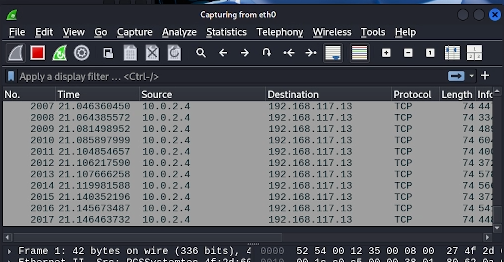
Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

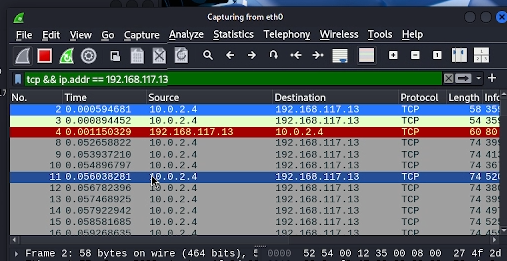
- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra

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.



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.