BÁO CÁO BÀI THỰC HÀNH SỐ 7

Họ và Tên: Trầm Xuân Trọng

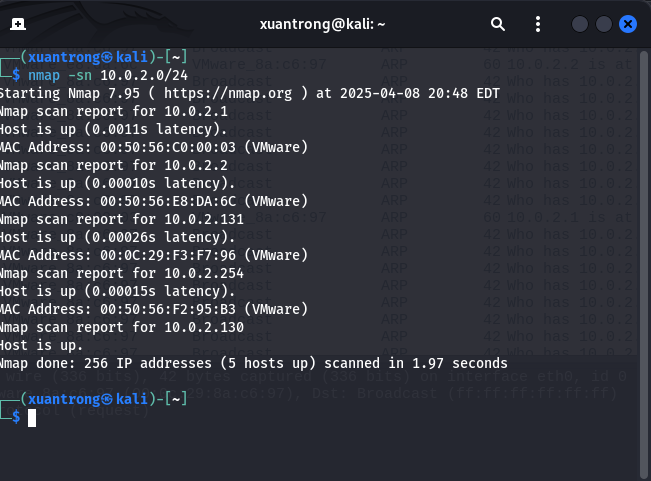
Lớp 10ĐH\_CNPM1

MSSV: 1050080081

1. Kịch bản 1: Quét thăm dò mạng

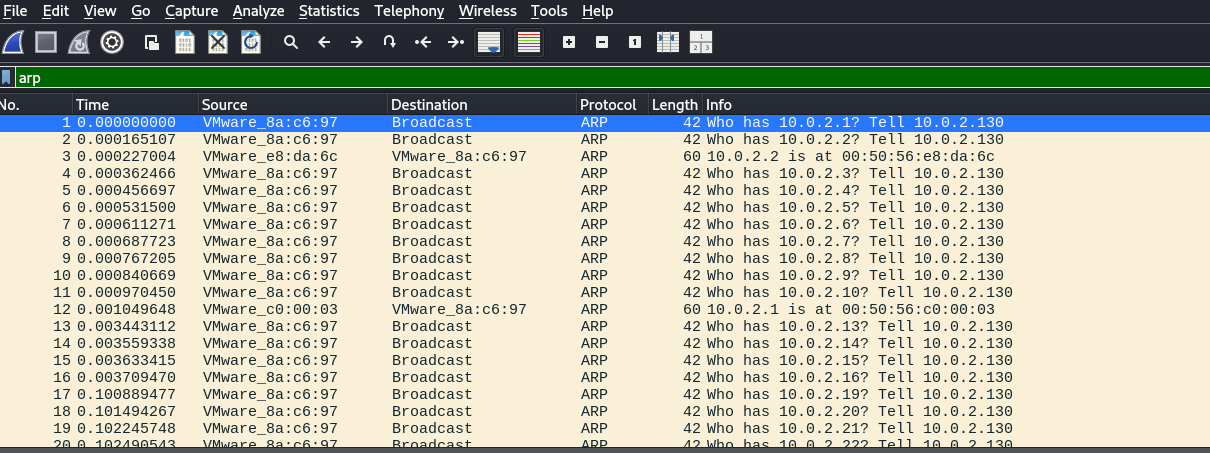
Đầu tiên tiến hành bắt gói tin wireshark và tiến hành lệnh quét với lệnh là

**nmap -sn 10.0.2.0/24**

****

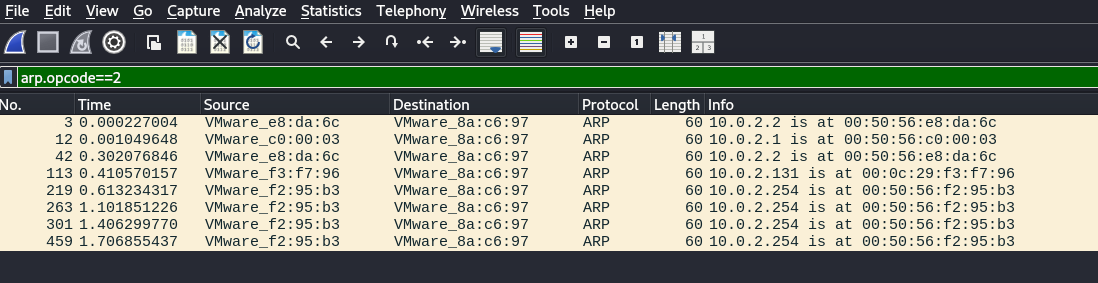
Kết quả sau khi tiến hành thực hiện câu lệnh

Tiến hành dừng bắt gói tin wireshark



Có thể thấy rằng máy tấn công đang gửi đi một loạt gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy trong mạng 10.0.2.0/24

Tiếp theo tiến hành sử dụng giá trị arp.opcode==2 cho bộ lọc.



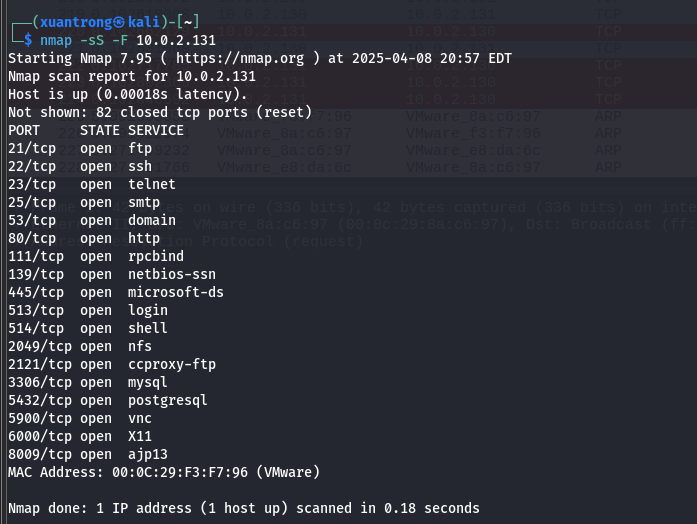
Đây là kĩ thuật thăm dò mạng, sau khi thực hiện xong Nmap này đã sử dụng kỹ thuật ARP Ping scan để phát hiện các nút mạng đang hoạt động trong mạng.

1. Kịch bản 2:

Đầu tiên tiến hành bắt gói tin wireshark mới và cần thực hiện lệnh quét như sau:

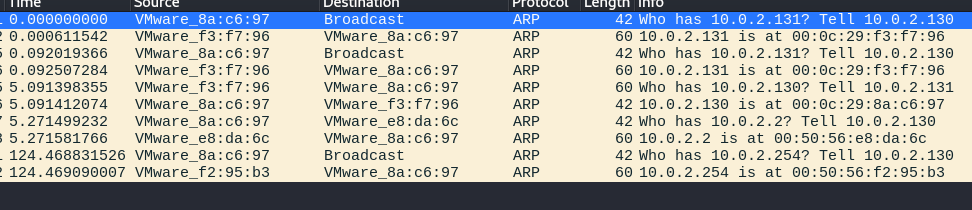
**nmap -sS -F 10.0.2.131**

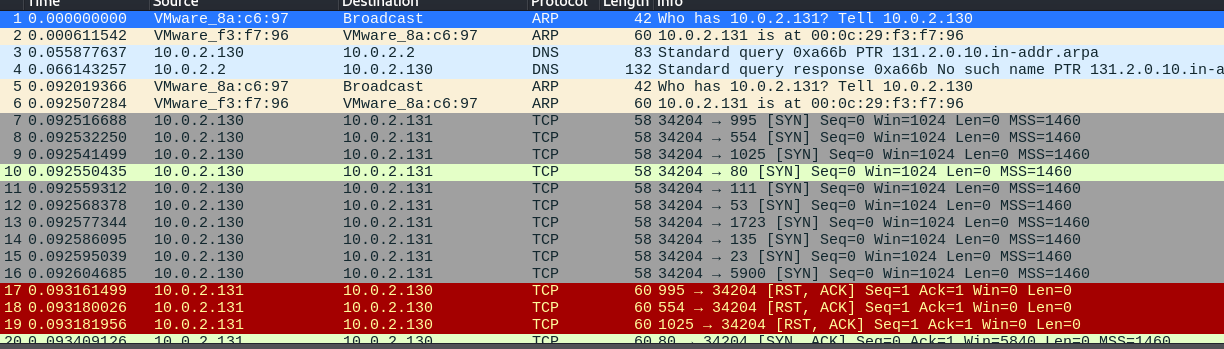
Kết quả sau khi thực hiện lệnh nmap trong terminal:

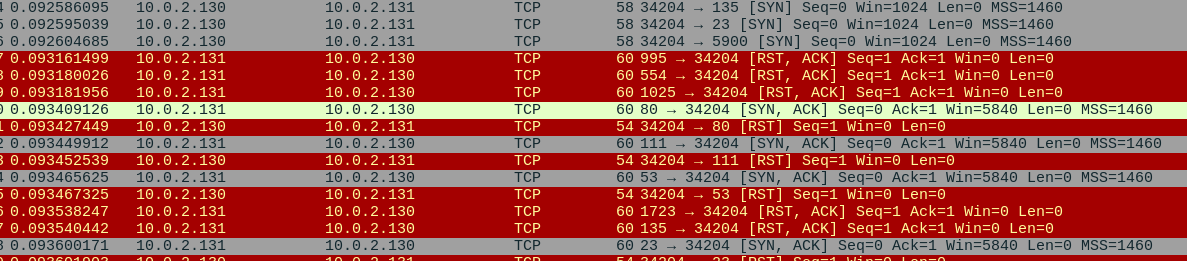


Tiến hành dừng bắt gói tin wireshark

Kết quả sau khi dừng bắt gói tin wireshark

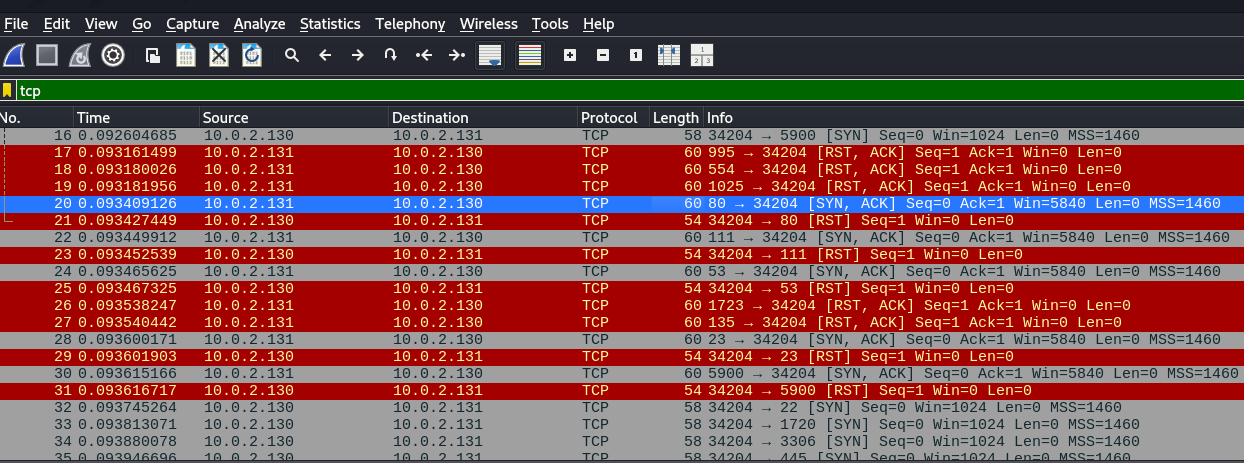






Tương tự như kịch bản đầu tiên có thể thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request.

Tuy nhiên sau khi tiếp tục quan sát lưu lượng mạng mà Wireshark đã phân tích chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 80 của máy đang hoạt động.



Nhập vào giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark gói tin TCP SYN/ACK được gửi từ cổng 80 từ địa chỉ Source của máy tấn công.

Đây là kỹ thuật quét SYN Scan ( -sS ) với chế độ quét nhanh ( -F )

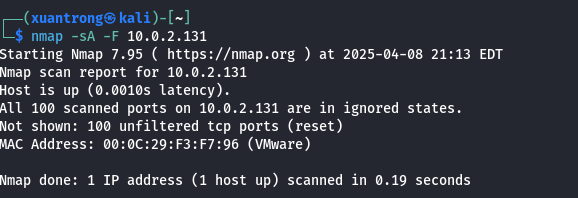
1. Kịch bản 3

Tiến hành bắt luôn gói tin wireshark

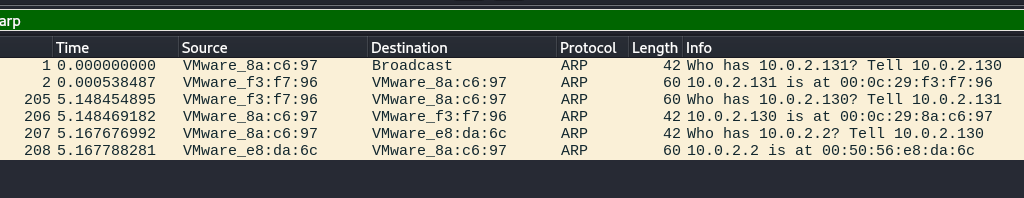
Tiến hành thực hiện lệnh quét

**nmap -sA -F 10.0.2.131**

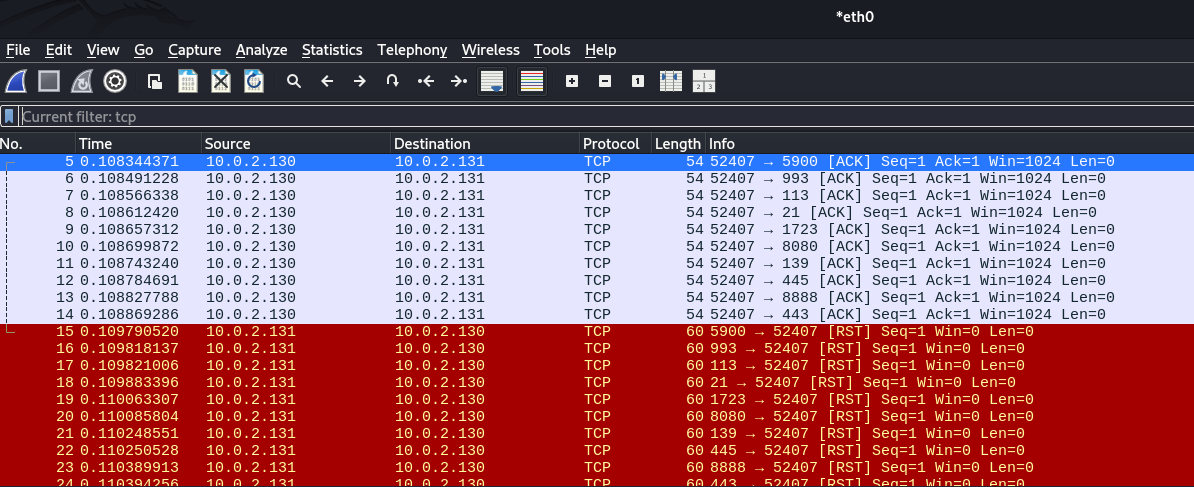
Kết quả sau khi thực hiện lệnh quét trong terminal:



Kết quả sau khi dừng gói tin wireshark



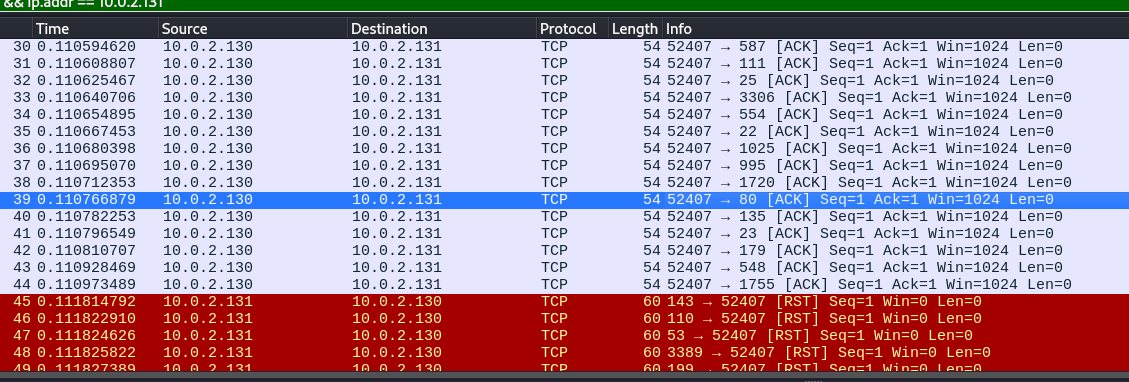
Tiến hành nhập tcp vào bộ lọc



Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy Destination có hoạt động hay không.

Sau đó ta có thể thấy một số lượng lớn các gói tin TCP ACK được gửi từ máy Source tấn công đến máy Destination tức là các cổng này đã bị lọc đi rồi.

Sử dụng giá trị tcp&&ip.addr == 10.0.2.131 ta lọc ra được các gói tin TCP. Có thể tháy một liên kết tới cổng 80 đã được thiết lập



Kỹ thuật quét đã được sử dụng trong kịch bản này là ACK Scan.

1. Thu thập thông tin về hệ thống
2. Tìm kiếm thông tin về các lỗ hỏng

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả nguyên nhân về lỗ hổng** |
| SSH, OpenSSH, 8.2 | CVE-2020-14145 | Xử lý không đúng trong giao thức SSH, có thể cho phép tấn công "man-in-the-middle". |
| SMTP, Postfix, 3.4 | CVE-2020-6102 | Xử lý không đúng email có định dạng đặc biệt, có thể dẫn đến thực thi mã từ xa. |
| MySQL, MySQL, 5.7 | CVE-2021-2022 | Xác thực không đúng, có thể cho phép kẻ tấn công thực thi mã tùy ý qua giao thức mạng. |
| PostgreSQL, PostgreSQL, 12.0 | CVE-2020-25694 | Xử lý không đúng trong cơ chế xác thực, có thể cho phép bỏ qua xác thực và truy cập dữ liệu. |
| HTTP, Apache, 2.4.41 | CVE-2020-9490 | Xử lý không đúng trong module mod\_cache, có thể dẫn đến crash hoặc thực thi mã từ xa. |