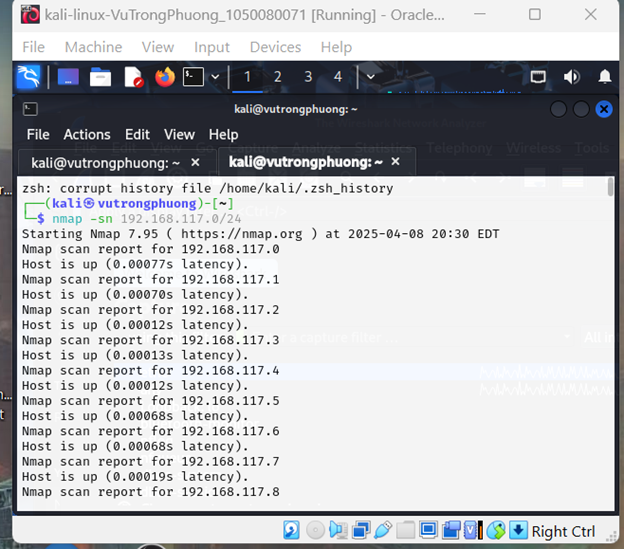
KẾT QUẢ THỰC HÀNH

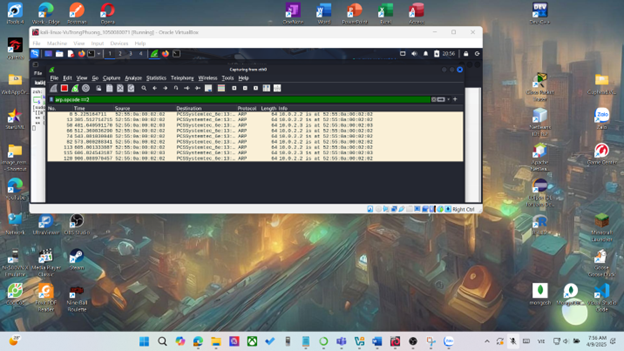
1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap

1.1. Kịch bản 1

- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm



- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm



1. Giao thức ARP liên tục

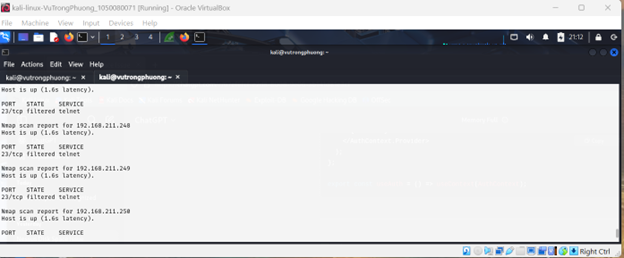
* Giao thức: ARP (Address Resolution Protocol).
* Mọi gói trong hình đều là ARP Request – "Who has X.X.X.X? Tell Y.Y.Y.Y".
* Điều này có nghĩa là máy đang quét để xác định địa chỉ MAC của các IP trong mạng nội bộ.

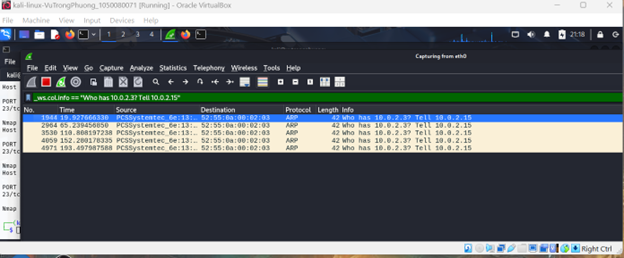
2. IP đích thay đổi liên tục

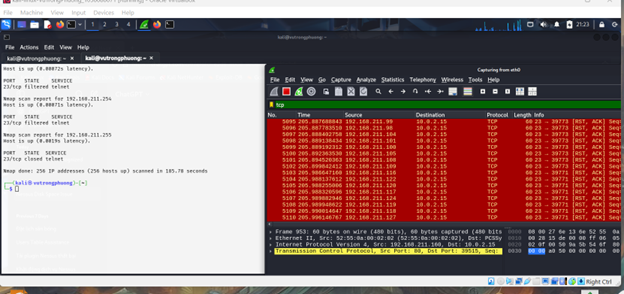
* IP nguồn là: 10.0.2.15.
* IP đích thay đổi tuần tự: 10.0.2.1, 10.0.2.2, 10.0.2.3, … → chứng tỏ đang quét toàn bộ dải mạng.
* Đây là kiểu quét ARP Scan, thường dùng để phát hiện các thiết bị đang hoạt động trong cùng mạng LAN.

1.2. Kịch bản 2

- Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm







- Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được

Kỹ thuật quét thăm dò: TCP SYN scan – một kỹ thuật stealth scan, gửi gói SYN để dò xem cổng có mở không.

Lưu lượng mạng:

* TCP SYN gửi đến nhiều cổng → port scanning.
* Không hoàn tất kết nối → stealth behavior.
* Nguồn cố định, đích cố định → Vertical scan.

Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm