**Tìm hiểu Nmap**

**Lý thuyết**

**Nmap (Network mapper)** là một tiện ích mã nguồn mở và miễn phí dùng để khai thác thông tin mạng và kiểm tra bảo mật. Nhiều quản trị viên hệ thống và quản trị viên network đã chứng minh sự hữu dụng của Nmap trong các tác vụ như kiểm tra mạng, quản lý dịch vụ và theo dõi thời gian hoạt động của máy chủ và dịch vụ.

**Nmap** sử dụng các kĩ thuật set cờ trong các gói IP cùng một số kĩ thuật tương tác nâng cao nhằm xác định máy chủ nào có sẵn trên mạng, những dịch vụ nào (tên ứng dụng và phiên bản OS) đang hoạt động, những bộ lọc packet / tường lửa nào đang sử dụng và hàng tá những đặc điểm khác.

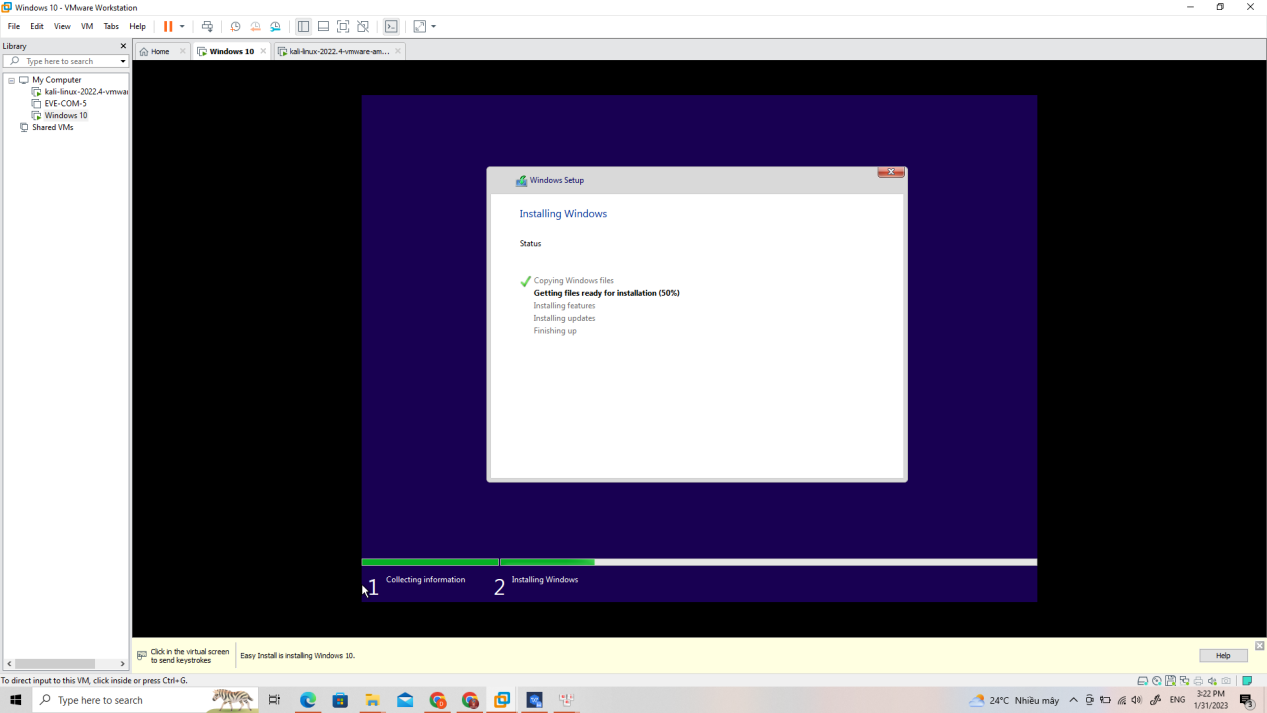
**Nmap** được thiết kế để nhanh chóng quét các mạng lớn nhưng đạt hiệu suất cao với một máy chủ duy nhất. Nmap có thể hoạt động trên rất nhiều các hệ điều hành quen thuộc và các gói binary chính thức có sẵn trên Linux, Windows và Mac OS X. Ngoài lệnh Nmap thực thi nguyên bản, Nmap còn cung cấp giao diện phần mềm (Zenmap), một công cụ chuyển data, chuyển hướng linh hoạt và gỡ lỗi (Ncat), một tiện ích để so sánh kết quả (Ndiff) và một công cụ phân tích và tạo gói (Nping).

**Thực hành**

**B1: Cài đặt máy ảo**

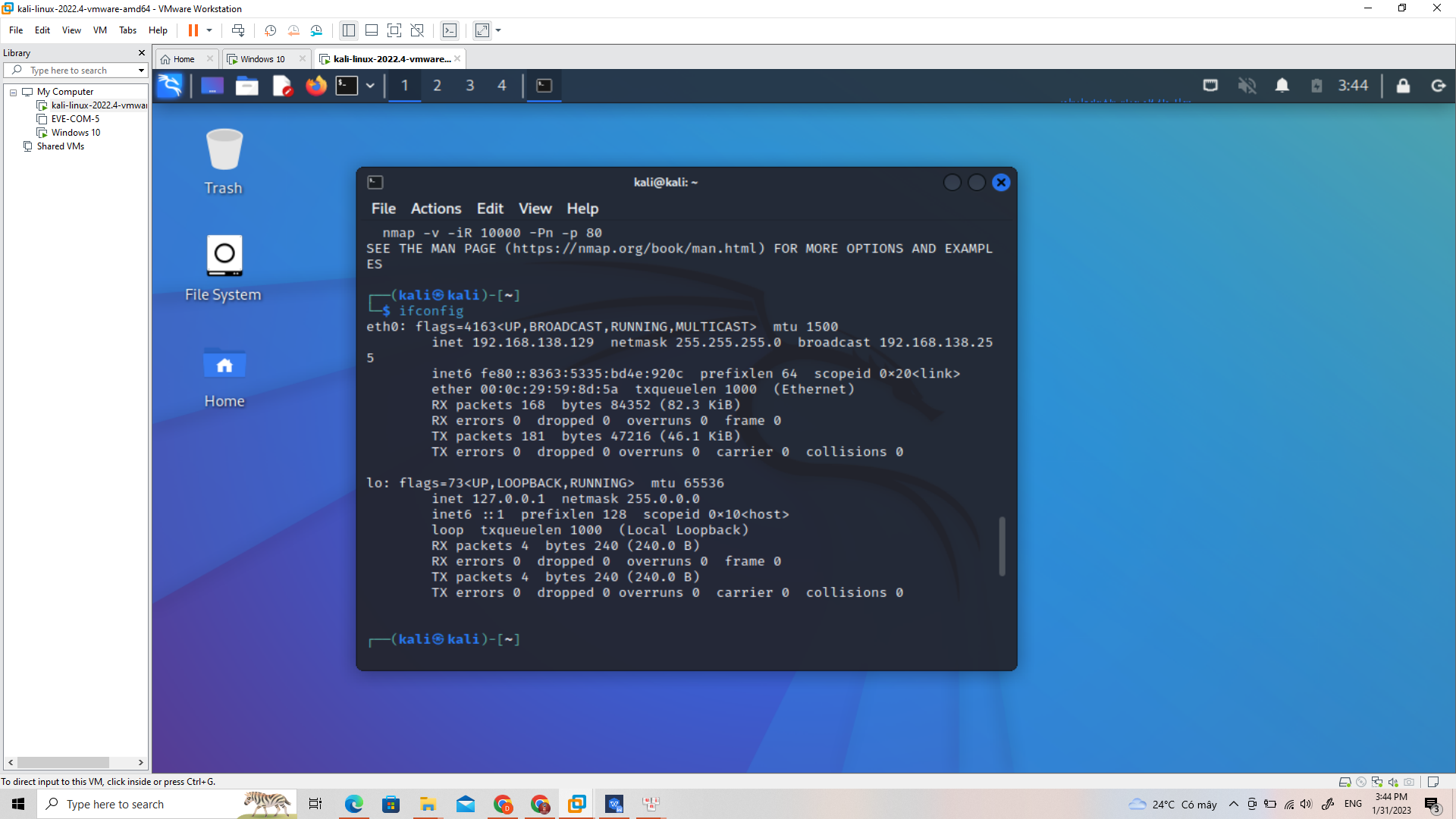
- Máy đã có sẵn Kali Linux

- Cài đặt Windows vào VM

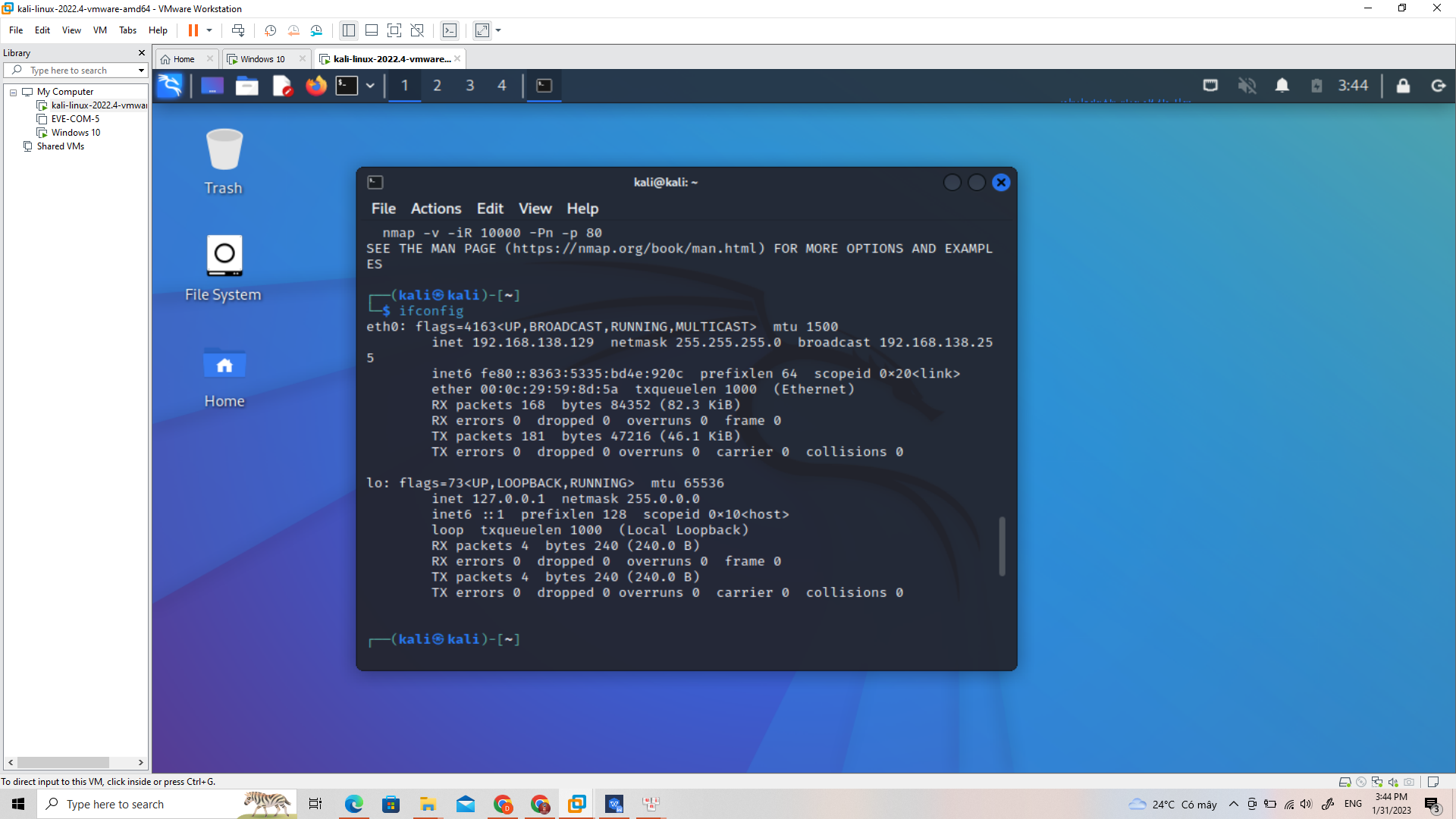


**B2: Kết nối 2 máy ảo thông qua card mạng NAT**

**B3: Kiểm tra máy kali - linux đang dùng mạng nào**

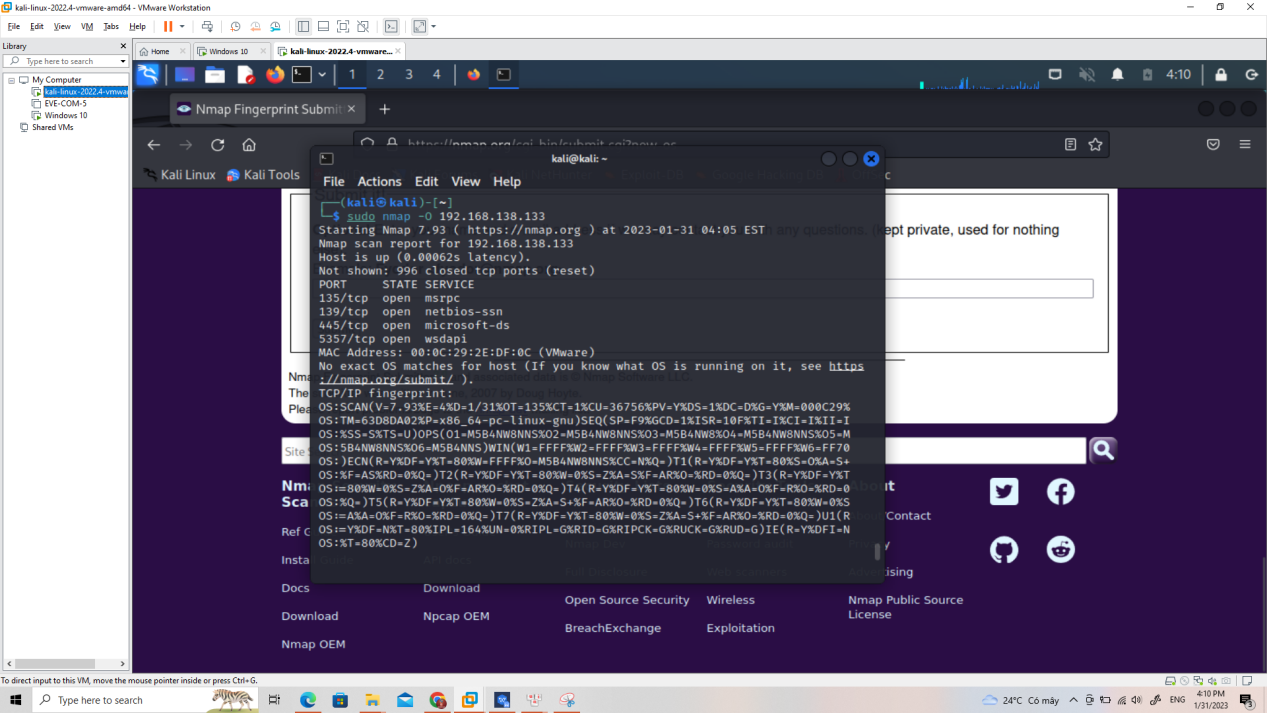


B4: nmap cho mạng 192.168.138.0/24



B5:192.168.138.133 chính là IP của máy Windows -> là máy mục tiêu.

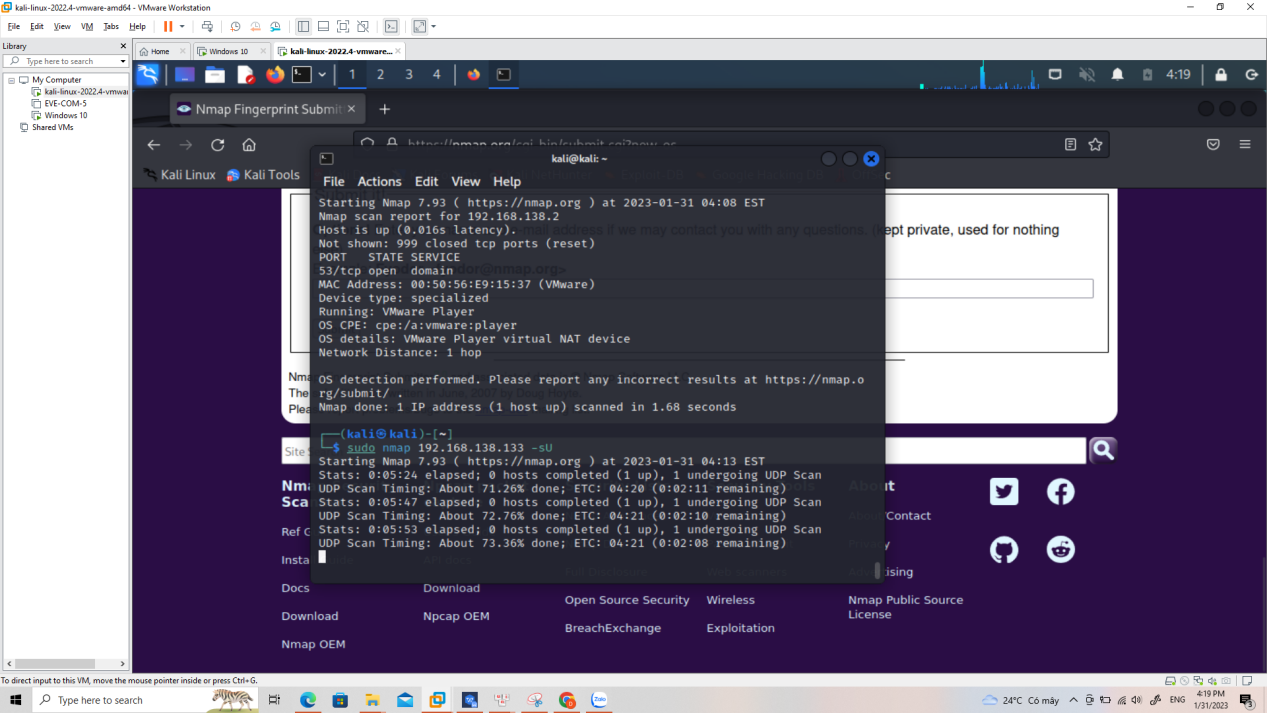
sudo nmap -O 192.168.138.133 để xem hệ điều hành

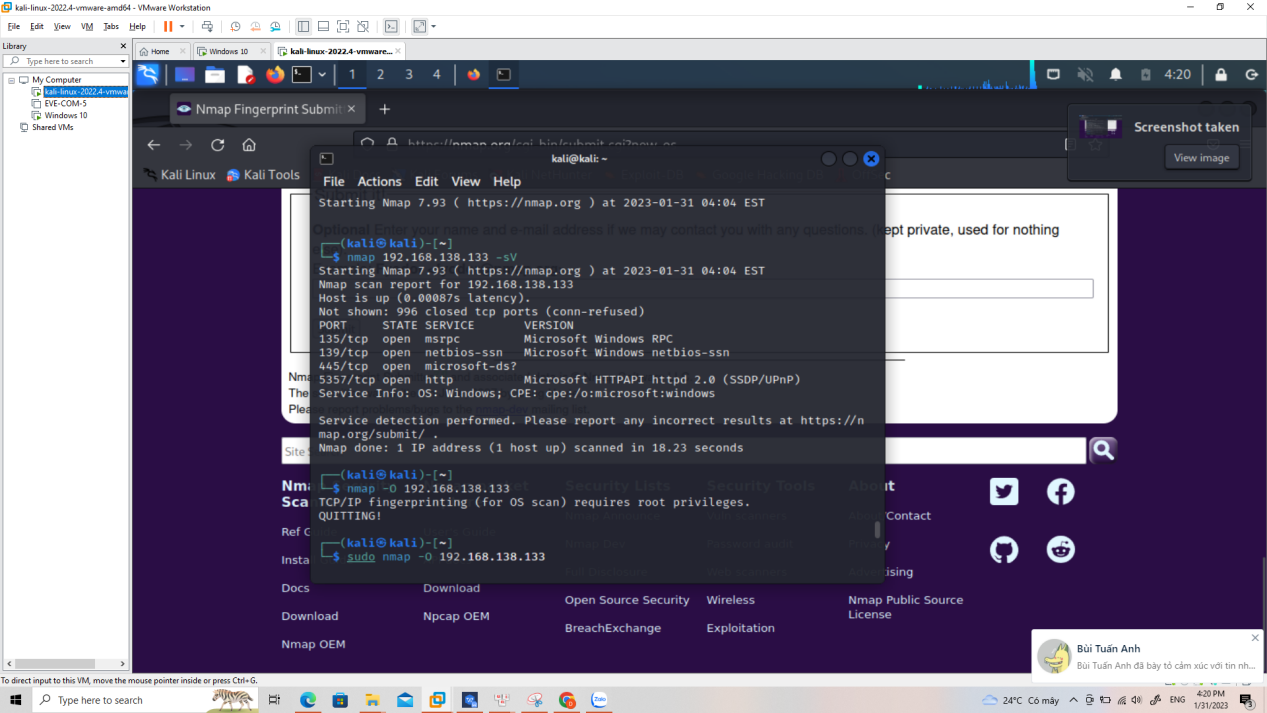


B6: Check các cổng TCP và UDP

sudo nmap -sV 192.168.138.133

sudo nmap -sU 192.168.138.133





B7: Thu thập lỗi

sudo nmap -sC 192.168.138.133

