BÁO CÁO BÀI THỰC HÀNH SỐ 7

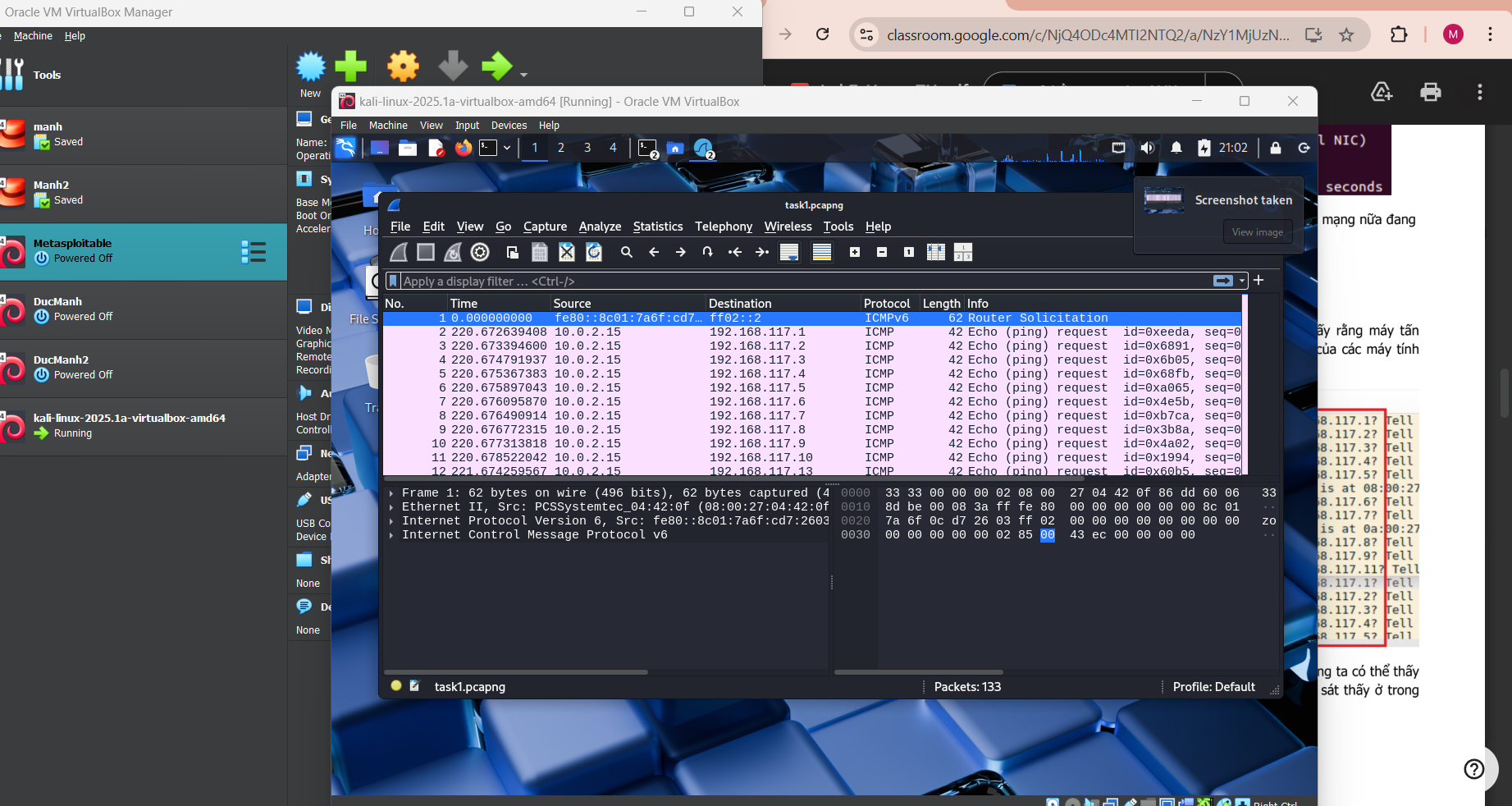
PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG

Họ và tên sinh viên:Nguyễn Huỳnh Đức Mạnh

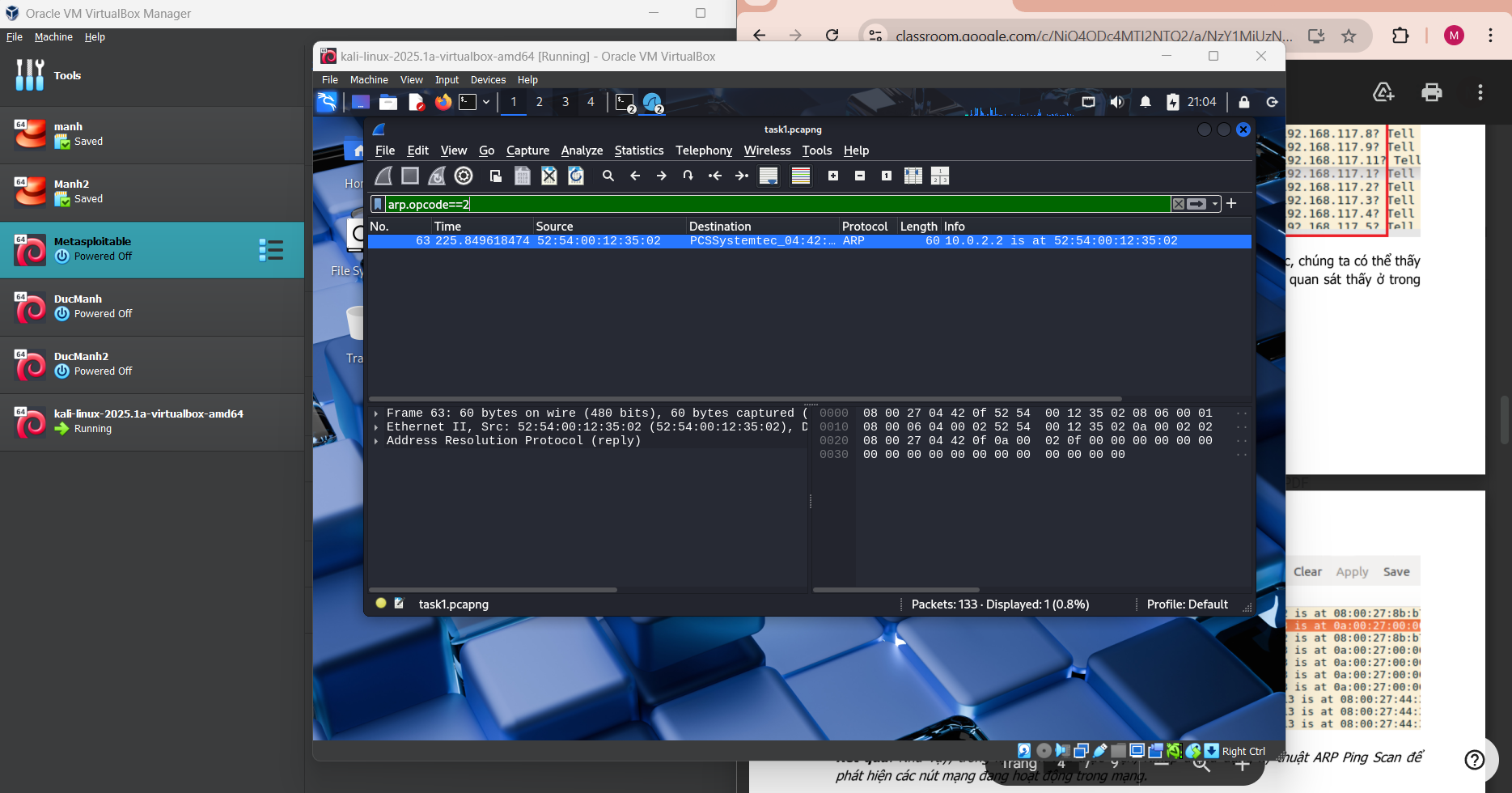
MSSV:1050080022

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

1.1. Kịch bản 1(arp ping scan)

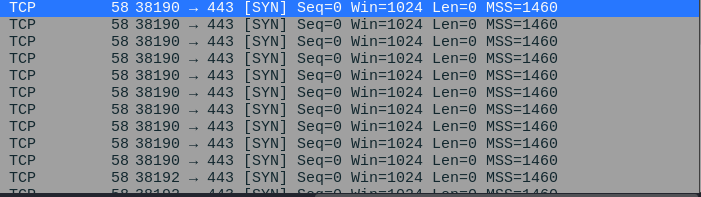


arp.opcode == 2

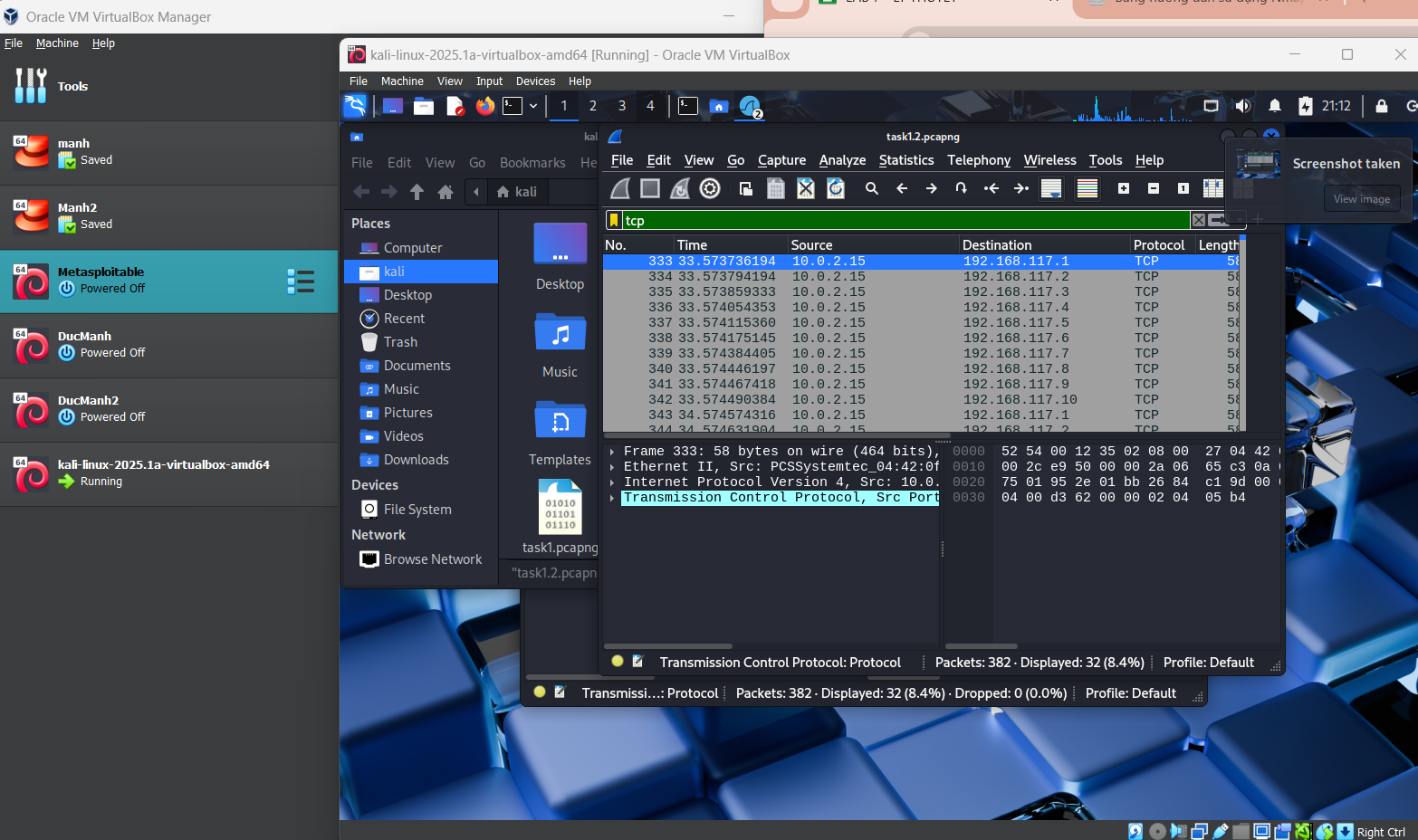


Lệnh quét tìm máy chủ email

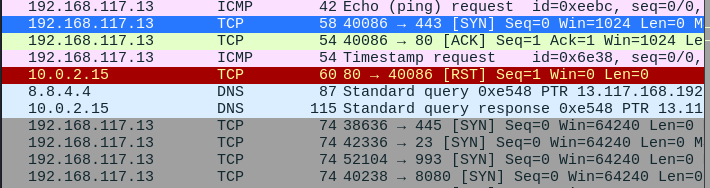
1.2 kịch bản 2(ARP Ping Scan và TCP SYN Scan)



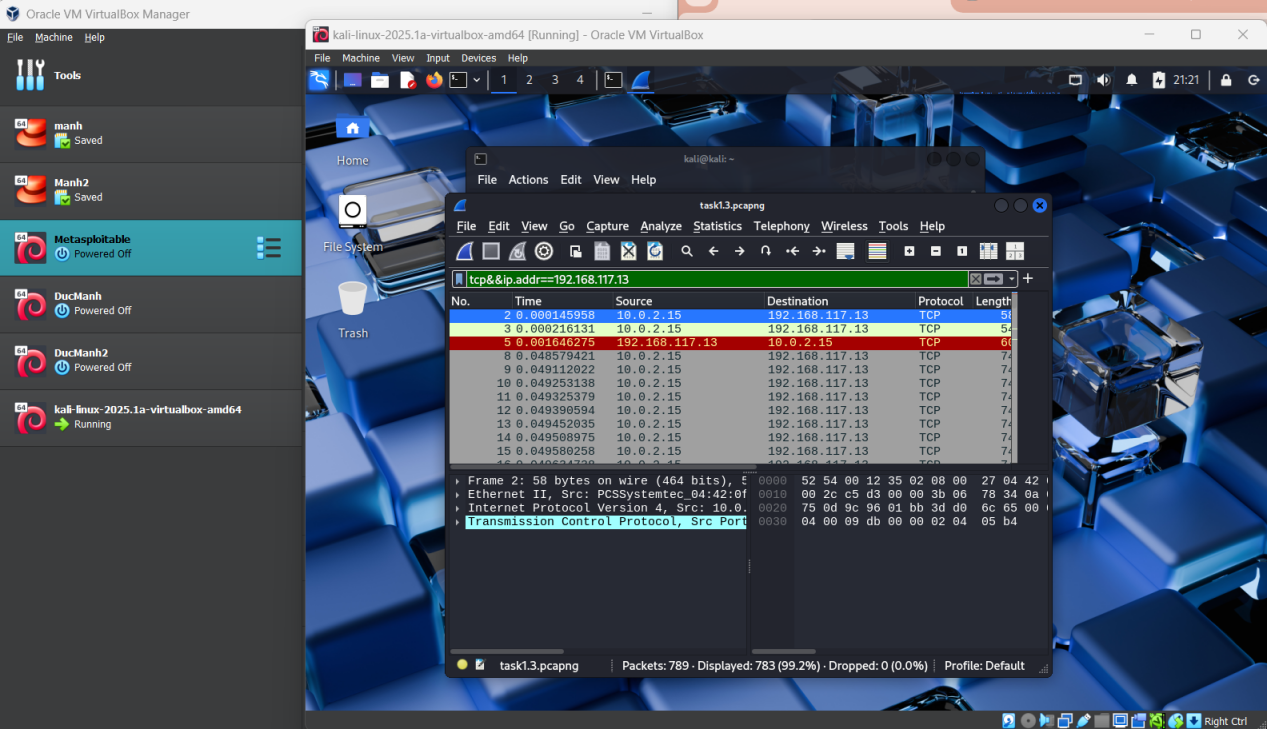
Tcp



1.3 kịch bản 3



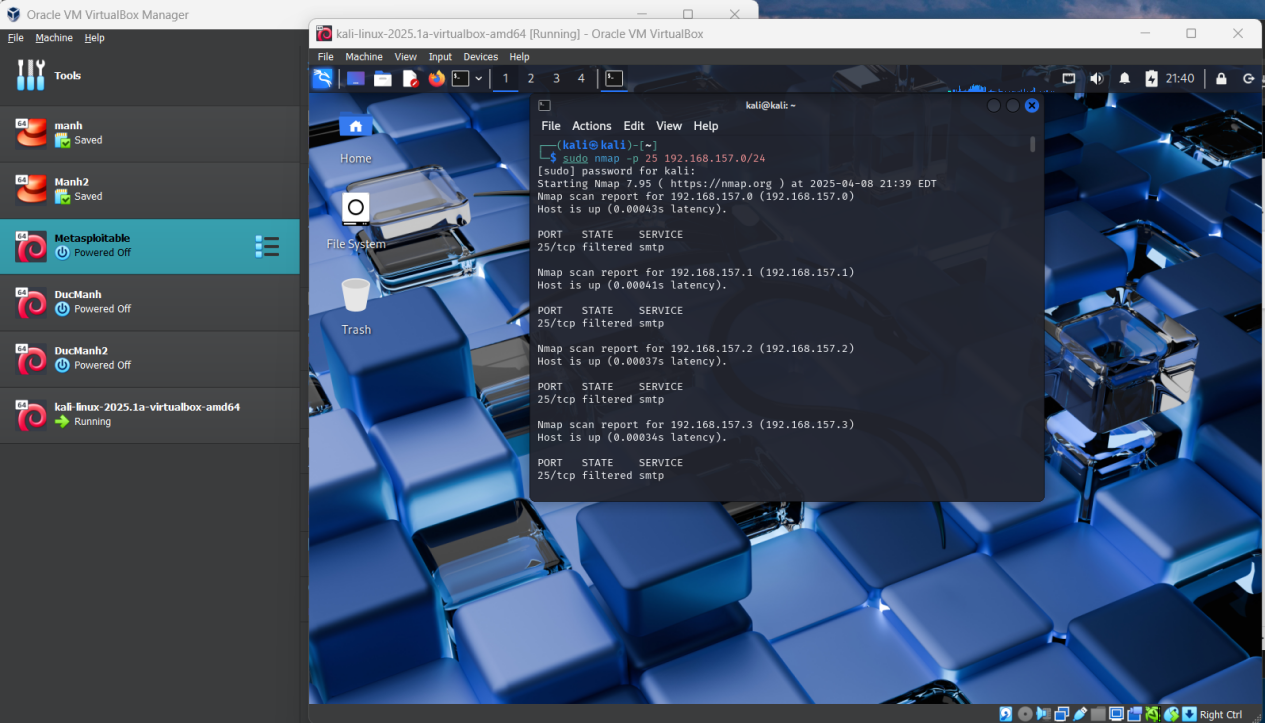
tcp && ip.addr == 192.168.117.13

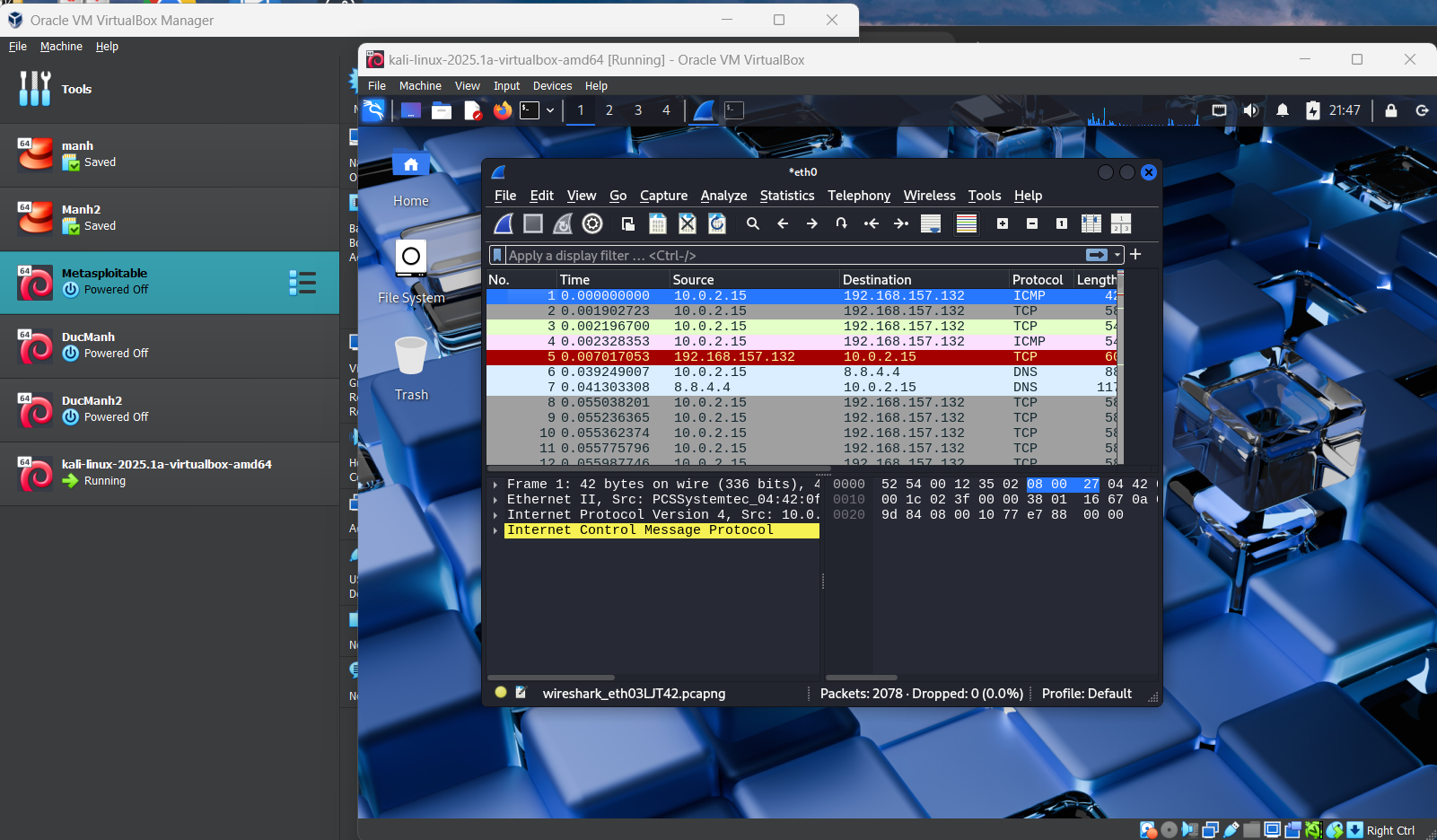


1. Thu thập thông tin hệ thống

Lệnh quét tìm máy chủ email

Lệnh: sudo nmap -p 25 192.168.157.0/24





3. Tìm kiếm thông tin về các lỗ hổng

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| http, Nginx 1.14.0 | CVE-2019-9516 | Lỗ hổng từ chối dịch vụ (DoS) do tấn công HTTP/2 "0-Length Headers Leak". |
| ftp, ProFTPD 1.3.5 | CVE-2019-12815 | Lỗ hổng thực thi mã từ xa do lỗi trong mod\_copy khi xử lý lệnh SITE CPFR/CPTO. |
| ssh, OpenSSH 7.6p1 | CVE-2018-15473 | Lỗ hổng tiết lộ thông tin qua giao thức SSH do lỗi kiểm tra tên người dùng. |
| smtp, Exim 4.92 | CVE-2019-10149 | Lỗ hổng thực thi mã từ xa do lỗi xử lý chuỗi trong deliver\_message(). |