**Nguyễn Phi Trường\_0850080110**

**K08\_CNPM**

**LAB THỰC HÀNH TUẦN 1**

**PHÂN TÍCH CÁC KỸ THUẬT DO THÁM HỆ THỐNG**

Mục Lục

[THIẾT LẬP MÔI TRƯỜNG ẢO HÓA TRÊN VIRTUAL BOX 1](#_Toc133435003)

[**1)Cài đặt và cấu hình Virtualbox** 1](#_Toc133435004)

[**2)** **Triển khai máy ảo Attack** 9](#_Toc133435005)

[**3)** **Triển khai máy ảo Server** 16](#_Toc133435006)

[LUYỆN TẬP 19](#_Toc133435007)

[**1. Quét thăm dò mạng** 21](#_Toc133435008)

[**2. Quét thăm dò dịch vụ** 23](#_Toc133435009)

[**3. Quét cổng dịch vụ** 25](#_Toc133435010)

[PHÂN TÍCH MỘT SỐ KĨ THUẬT QUÉT CỔNG ỨNG DỤNG CỦA NMAP 27](#_Toc133435011)

[**1) Kịch bản 1:** nmap –sn 192.168.117.0/24 27](#_Toc133435012)

[**2) Kịch bản 2:** nmap –sS –F 192.168.117.2 27](#_Toc133435013)

[**3) Kịch bản 3:** nmap –sA –F 192.168.117.2 28](#_Toc133435014)

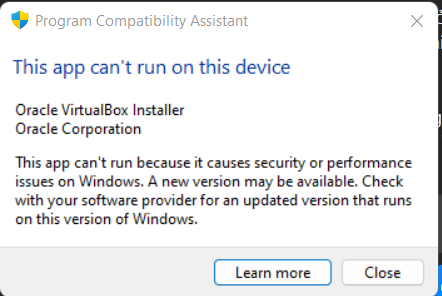
[**4) Thu thập thông tin hệ thống :**nmap -A -p 25,465,587 192.168.100.0/24 28](#_Toc133435015)

[**5) Tìm kiếm thông tin về các lỗ hổng** 29](#_Toc133435016)

# THIẾT LẬP MÔI TRƯỜNG ẢO HÓA TRÊN VIRTUAL BOX

## **1)Cài đặt và cấu hình Virtualbox**

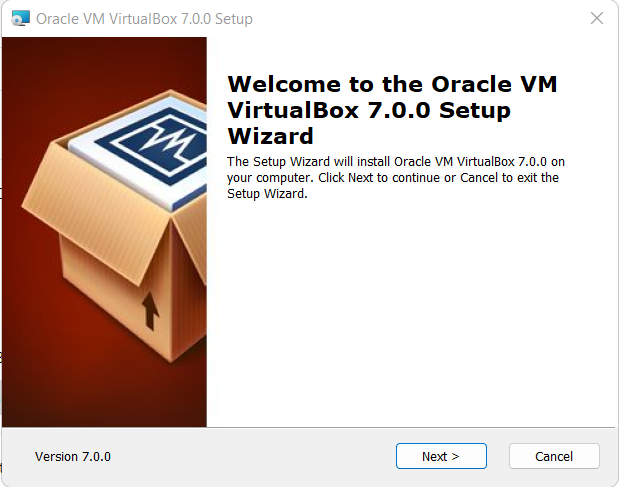
Khi em cài đặt (trên Win 11) bản trên link thầy đính kèm thì báo lỗi như bên dưới nên em sẽ phải tự tìm 1 phiên bản mới hơn



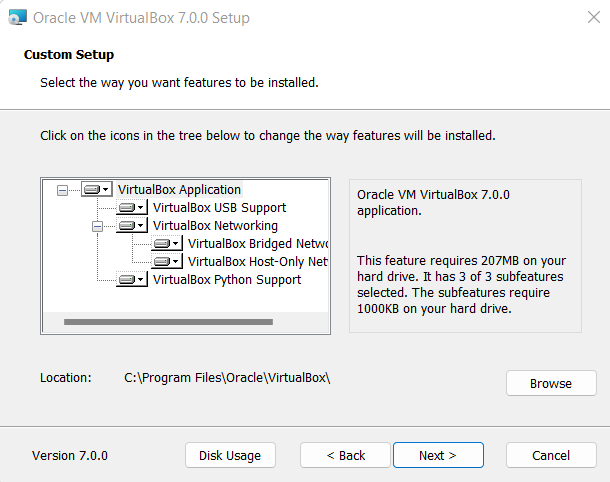
Em sẽ thử với bản 7.0



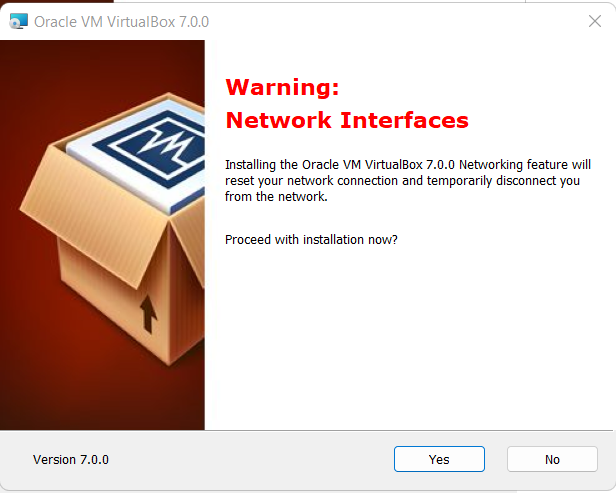
Em tiến hành cài đặt :Chọn Next



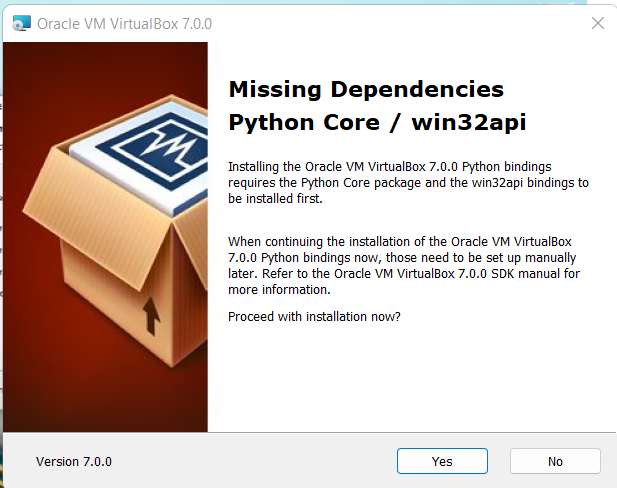
Chọn next



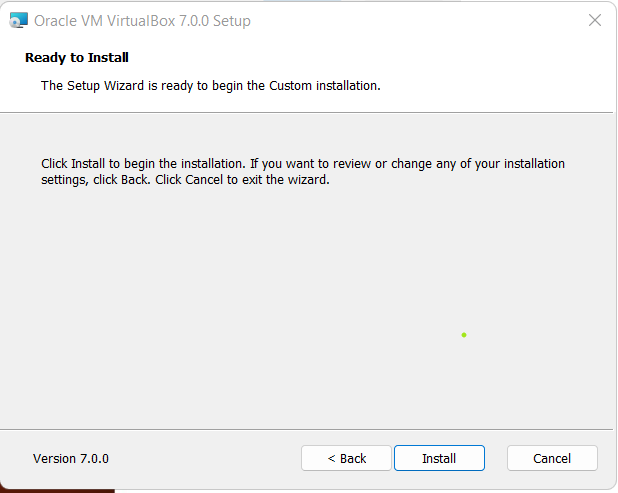
Hiện cảnh báo lên thì xác nhận yes



Báo thiếu Dependencies thì ta cho yes để cài thêm



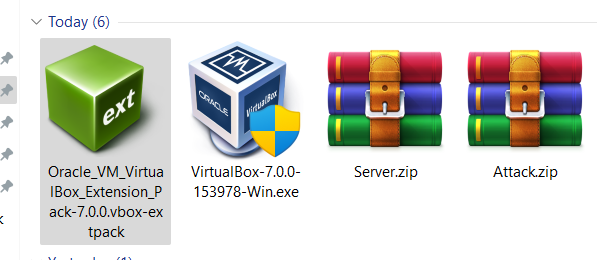
Chọn Install



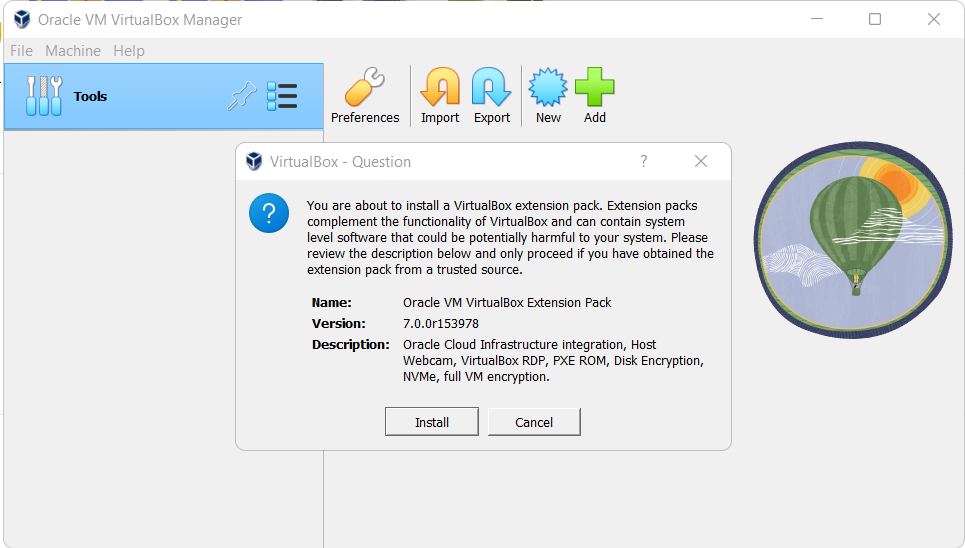
Cài đặt thành công



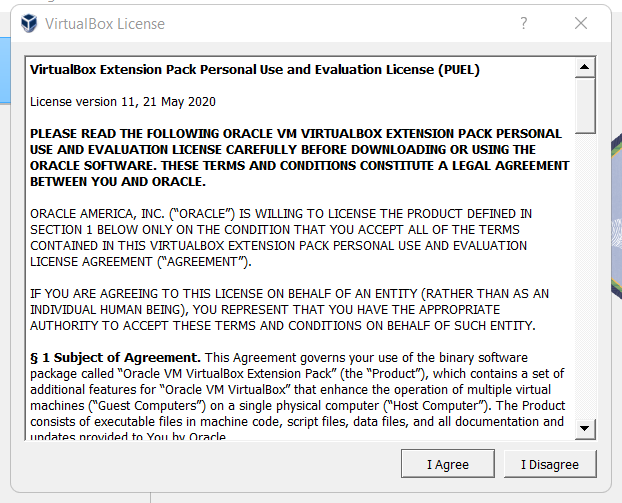
Kích đúp vào file để cài đặt gói mở rộng



Chọn Install

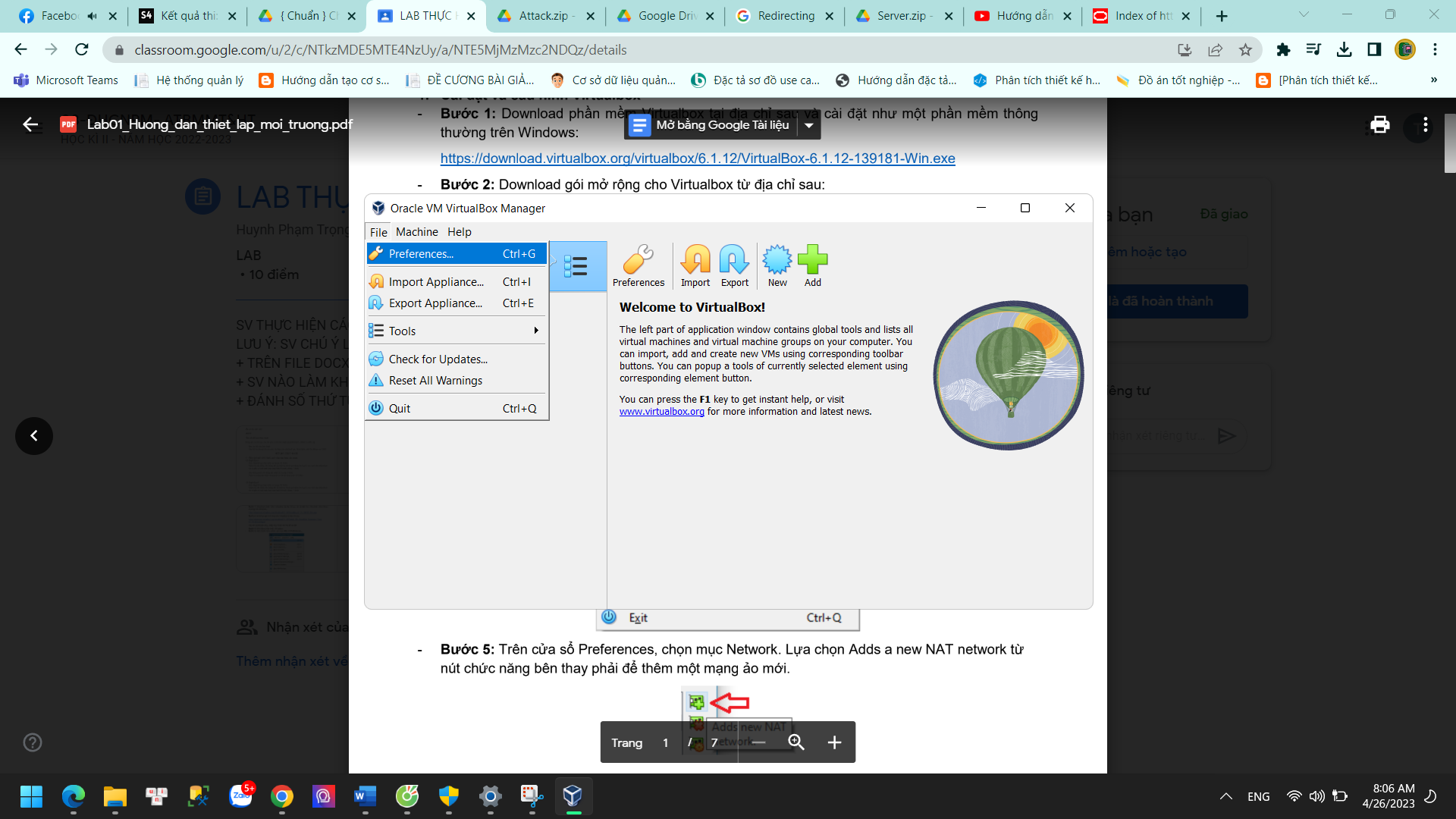


Đọc các điều khoản rồi chọn I Agree

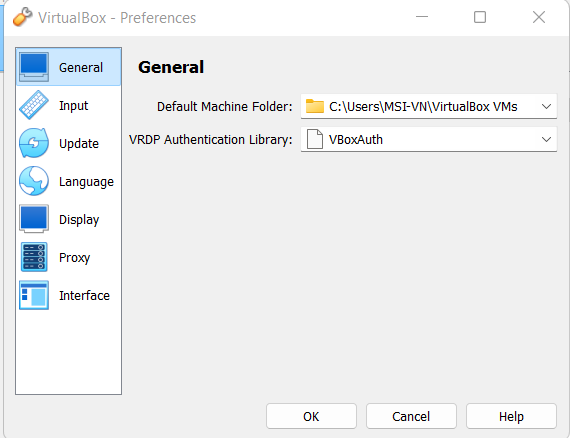


Khởi động VirtualBox

Chọn File-Preferences

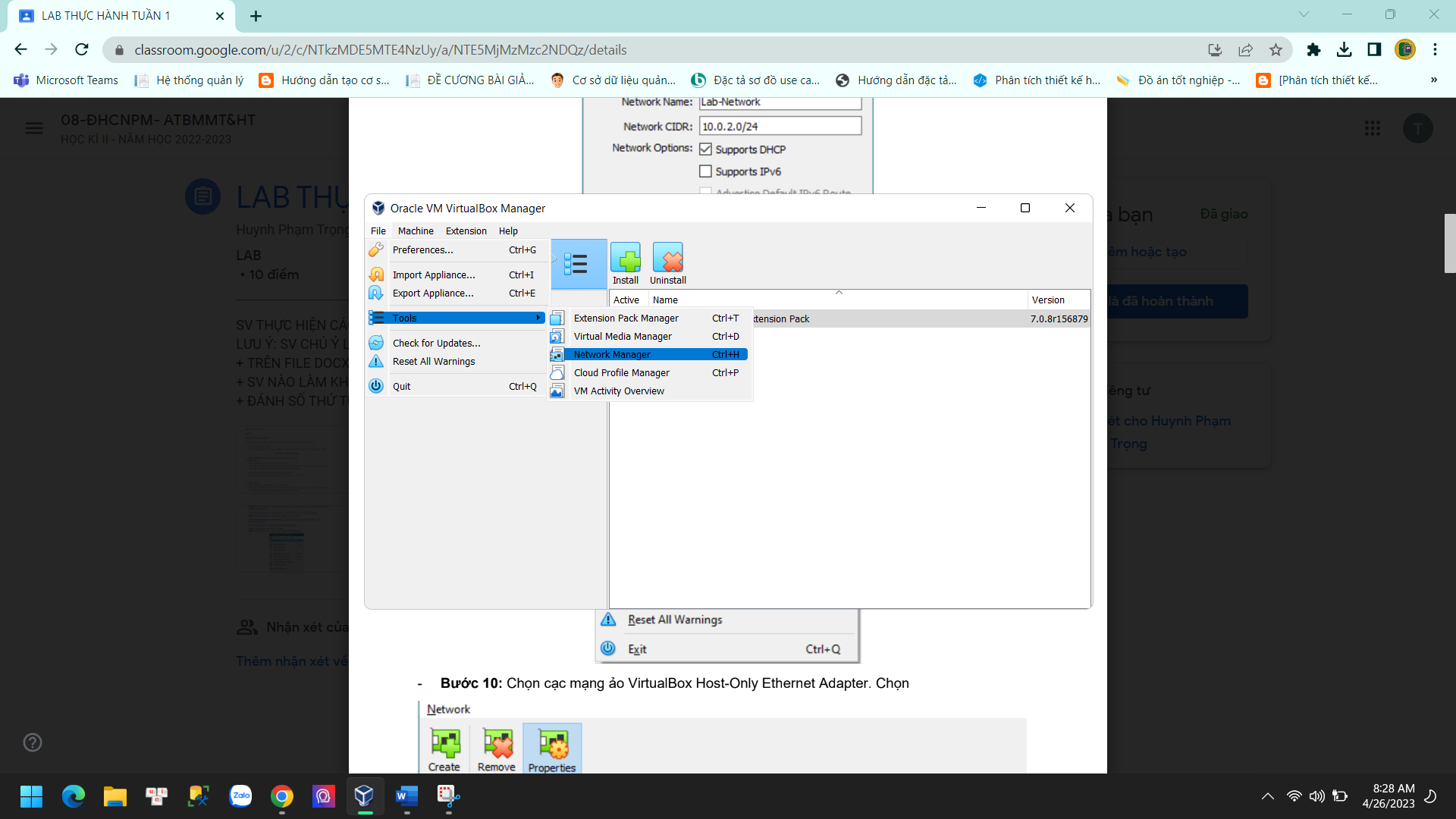


Em không kiếm thấy được mục network



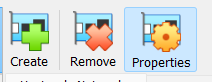
Sau một lúc tìm khiến thì em đã tìm thấy

Chọn Tools-Network Manager

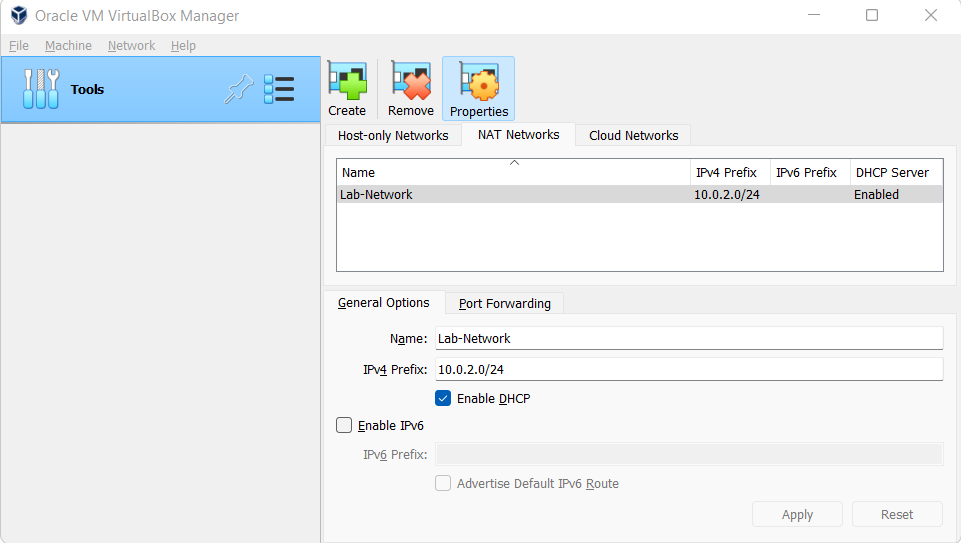


Chuyển tab sang NAT Networks

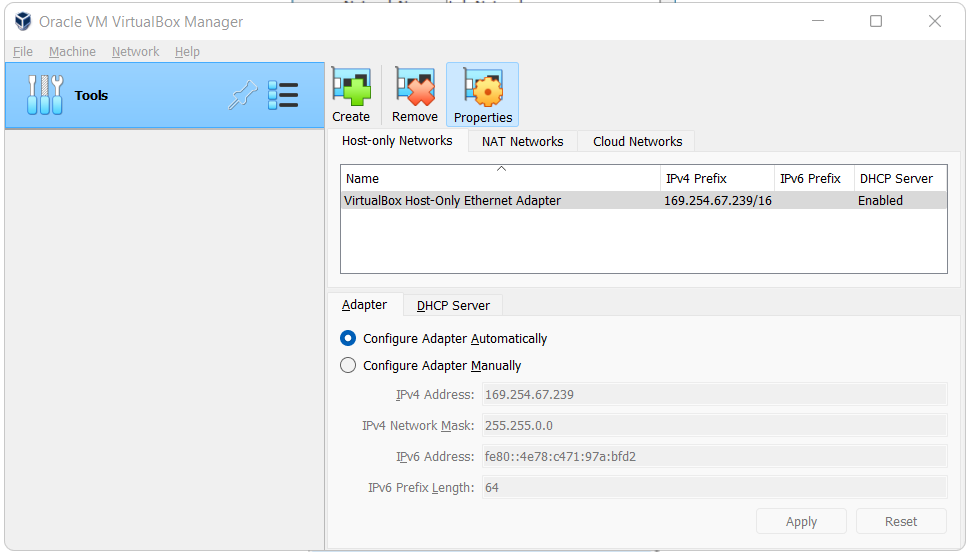
Chọn Create xong Chọn Properties để thay đổi



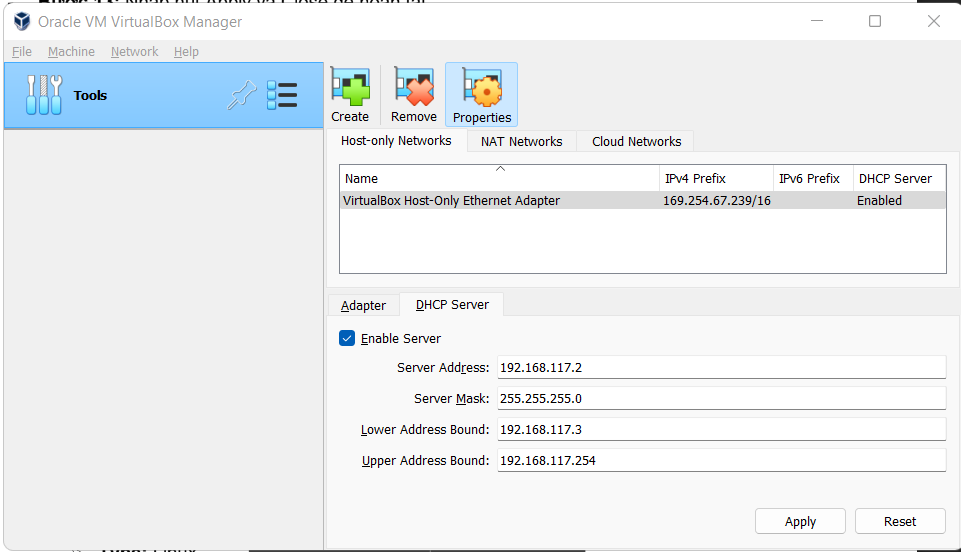
Thiết lập thông số-Hoàn tất thì chọn Apply



Chuyển sang Tab Host-only Networks. Tab Adaper để mặc định Automatically

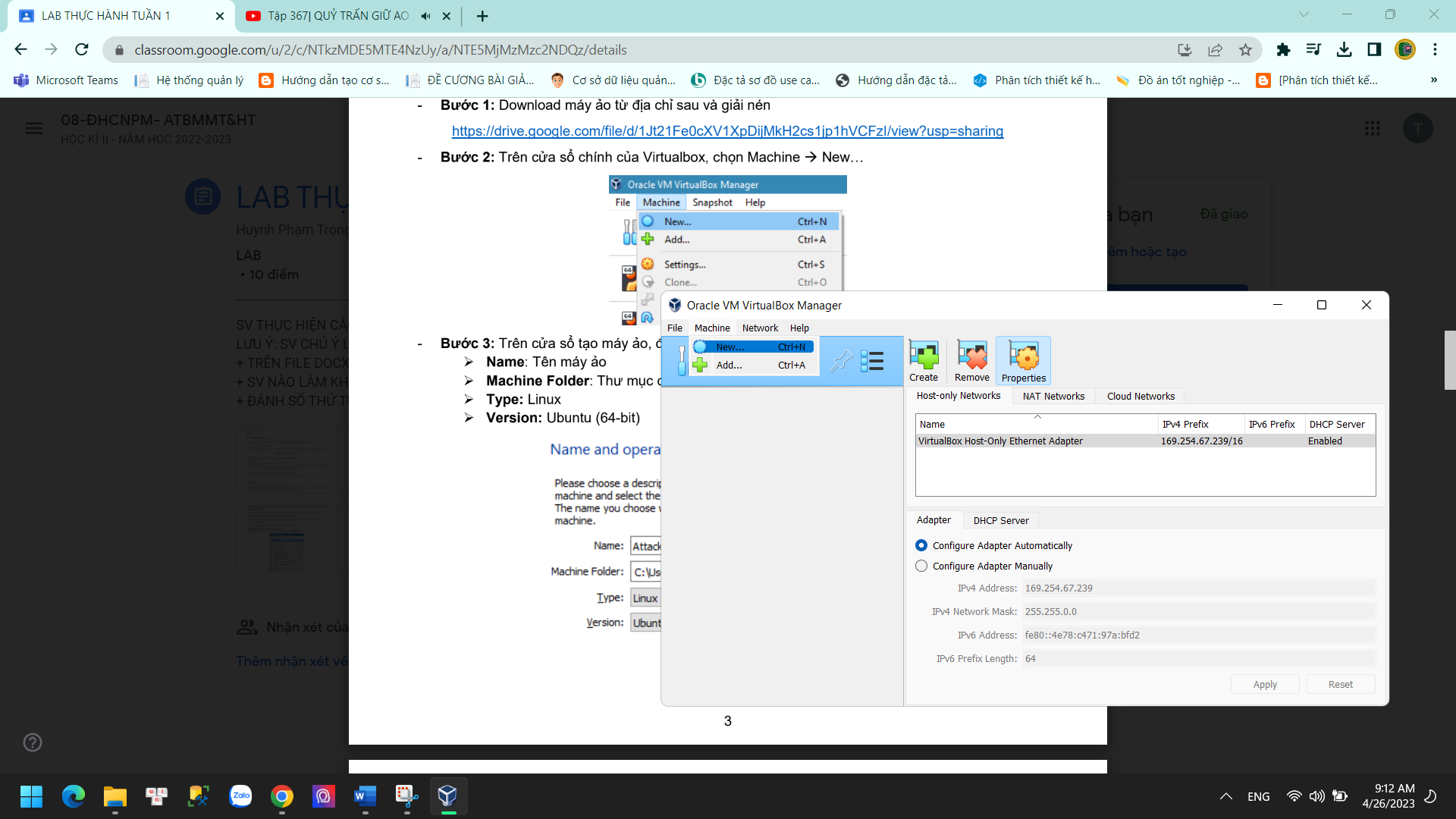


Sang tab DHCP Server thiết lập như sau. Sau đó chon Apply

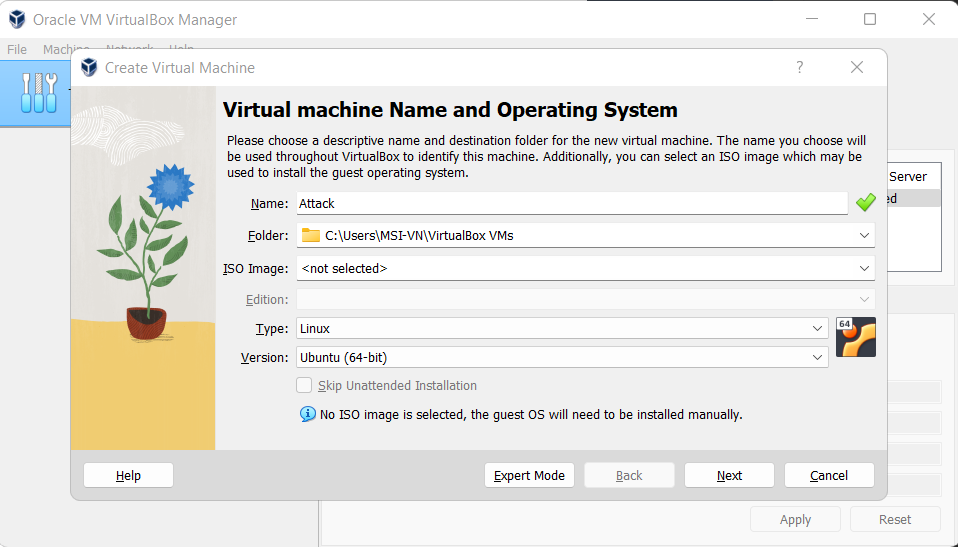


## **2)** **Triển khai máy ảo Attack**

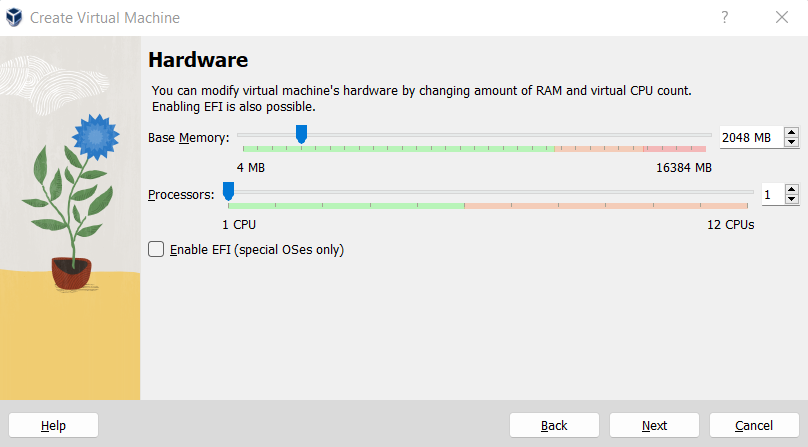
Chọn Machine-New…



Đặt các thông số



Chọn dung lượng bộ nhớ RAM cho máy ảo là 2048 MB

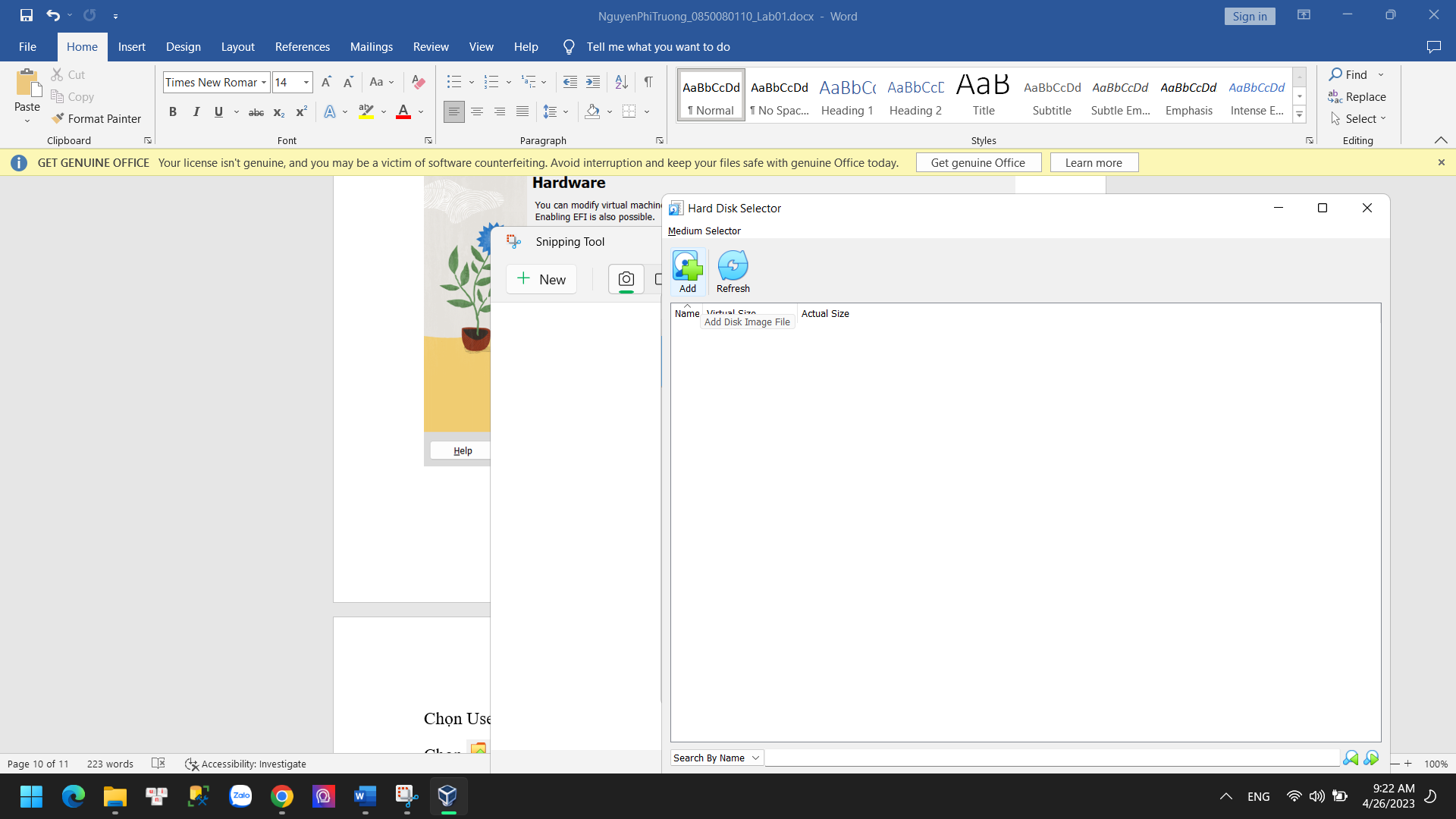


Chọn Use an Existing Virtual Hard Disk File

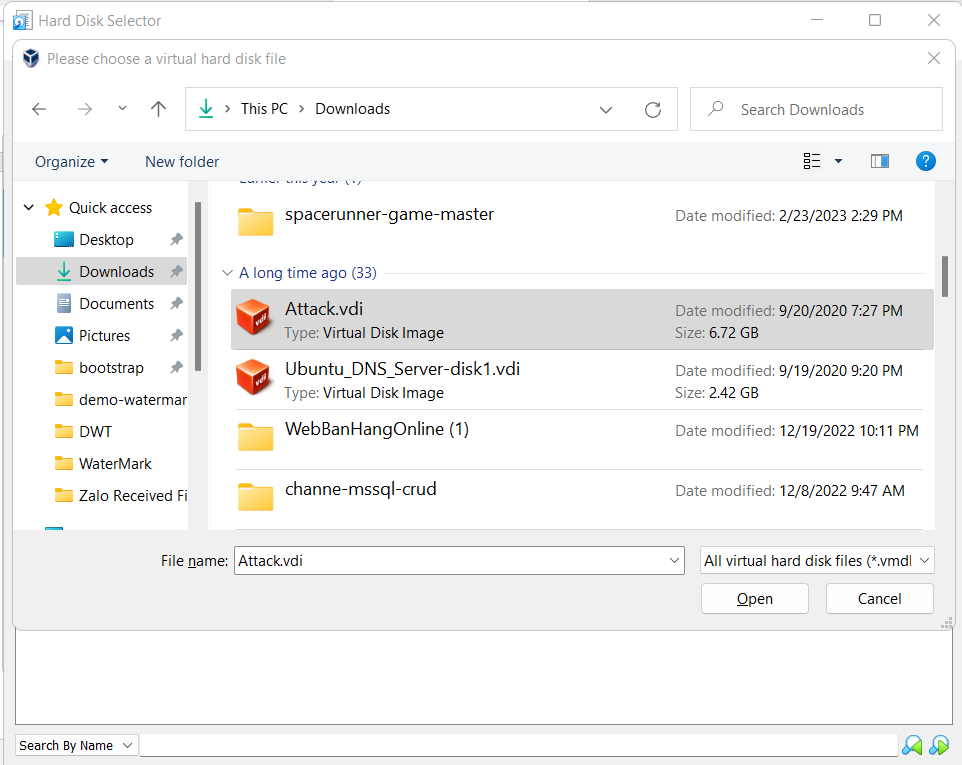
Chọn 



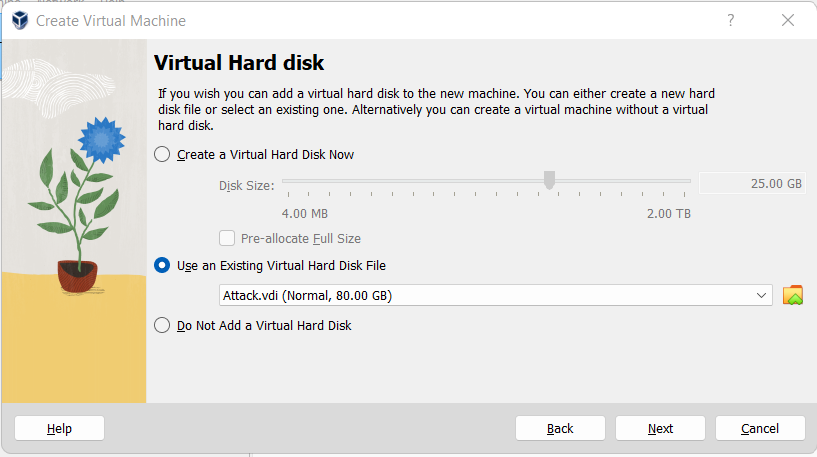
Chọn Add



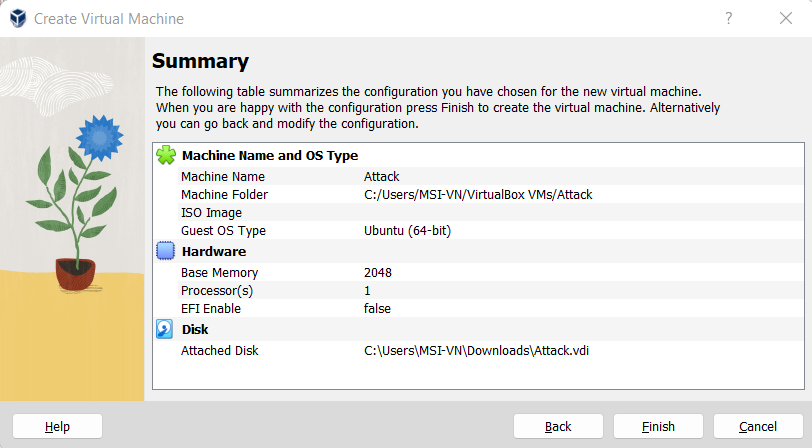
Chọn file Attack.vdi đã download



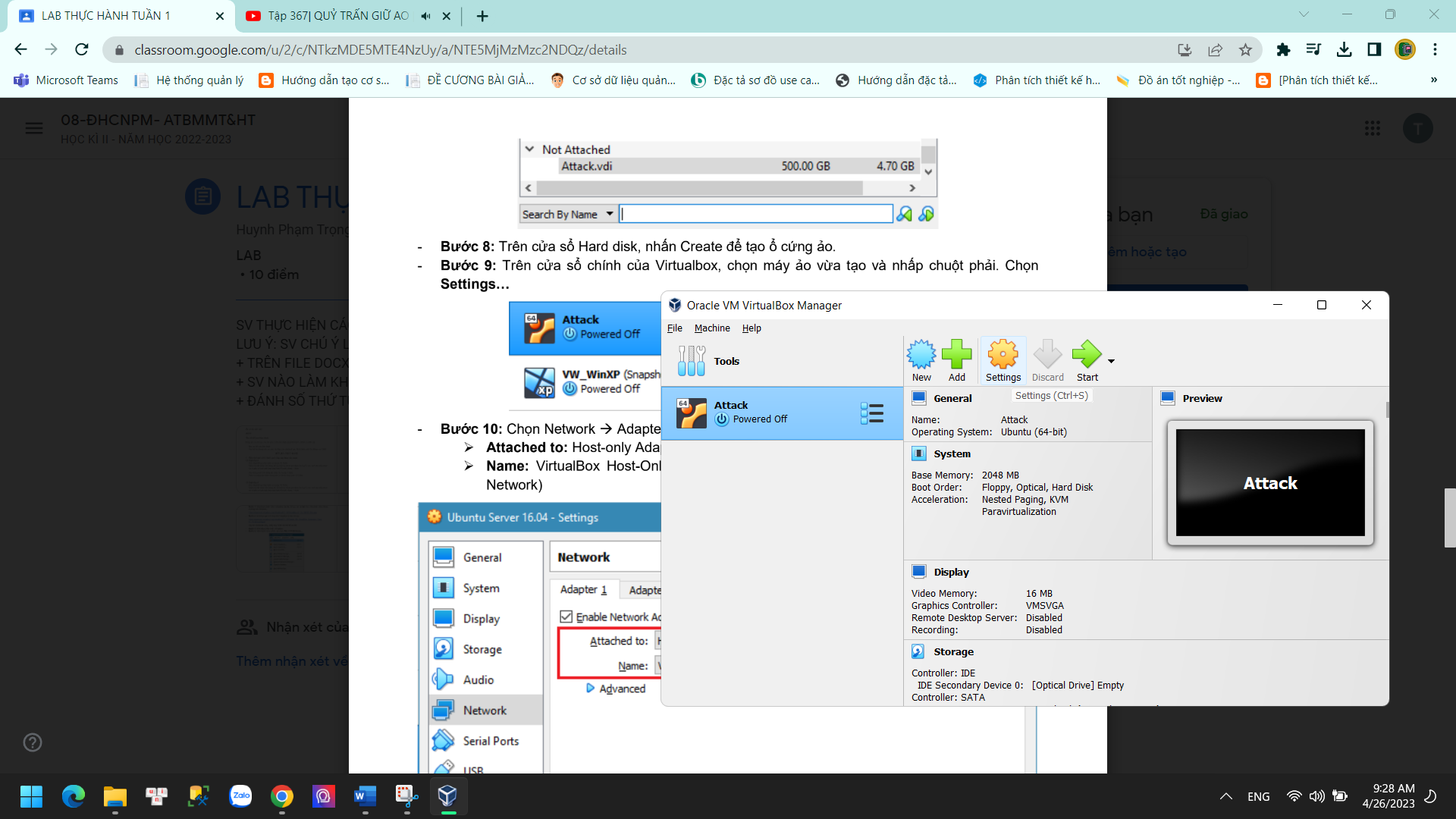
Chọn Next



Chọn Finish



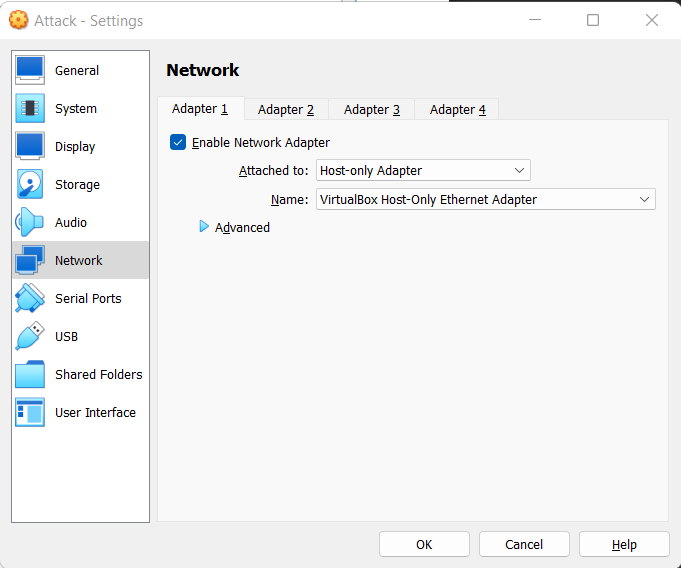
Chọn Settings



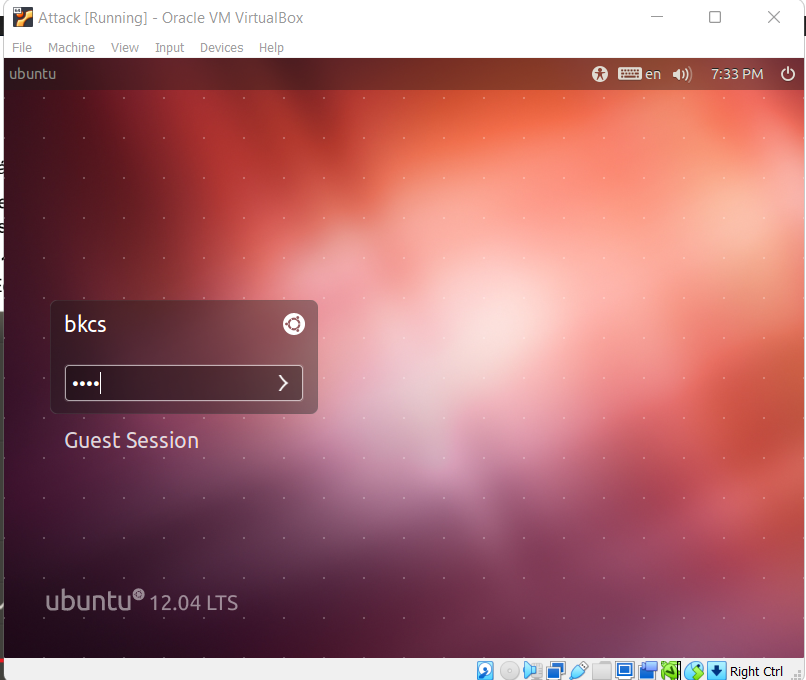
Chọn Network-Adapter 1

Attached to: Host-onlt Adapter

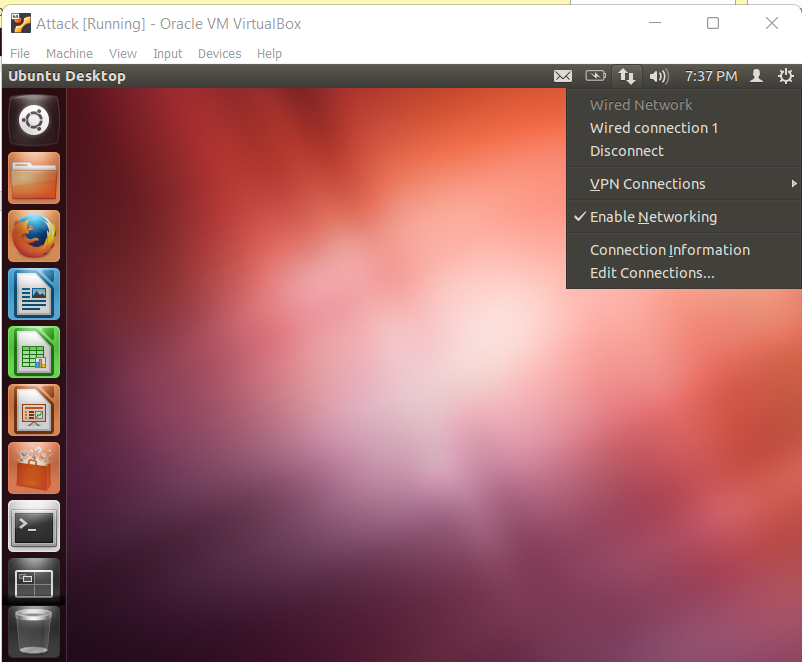
Name: VirtualBox Host-Only Ethernet Adapter



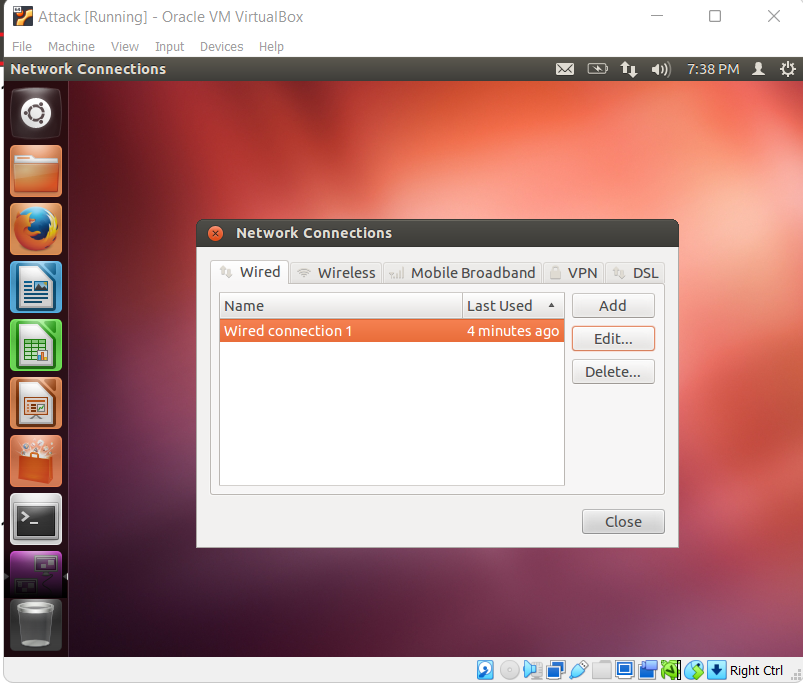
Khởi động máy ảo, Pass là bkcs



Chọn Edit Connections…

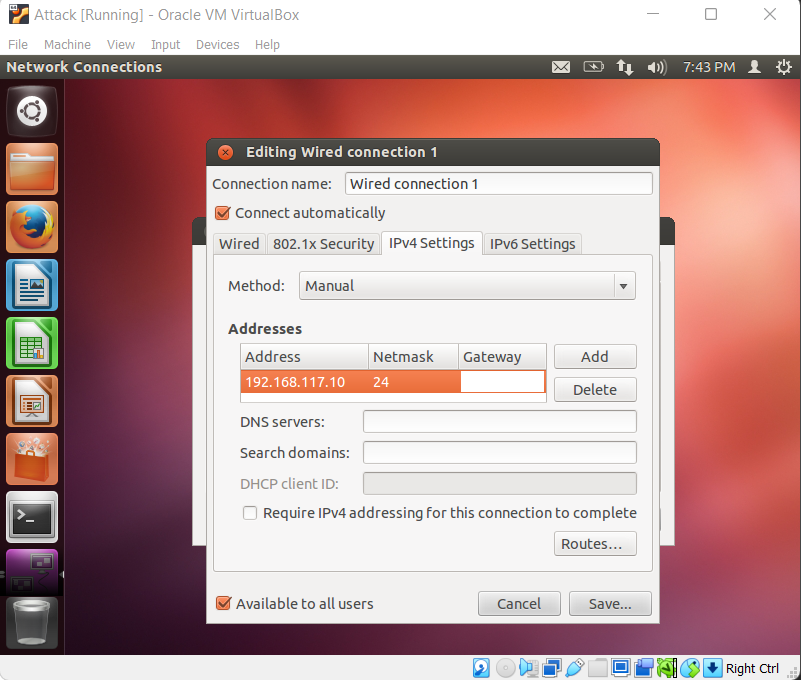


Chọn Edit

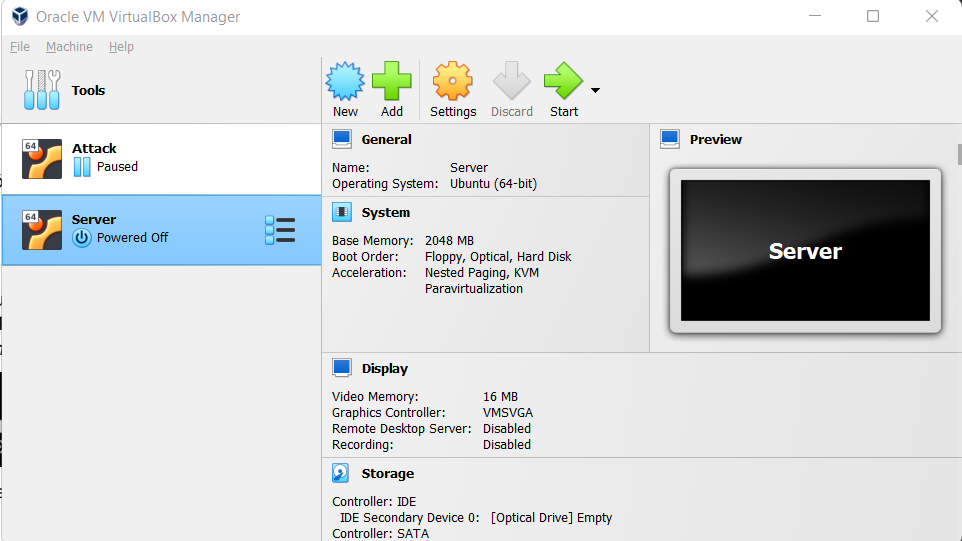


Chuyển qua Tab Ipv4 Settings-Chọn Manual

Chọn Add-Thiết lập các thông số- Chọn Save…

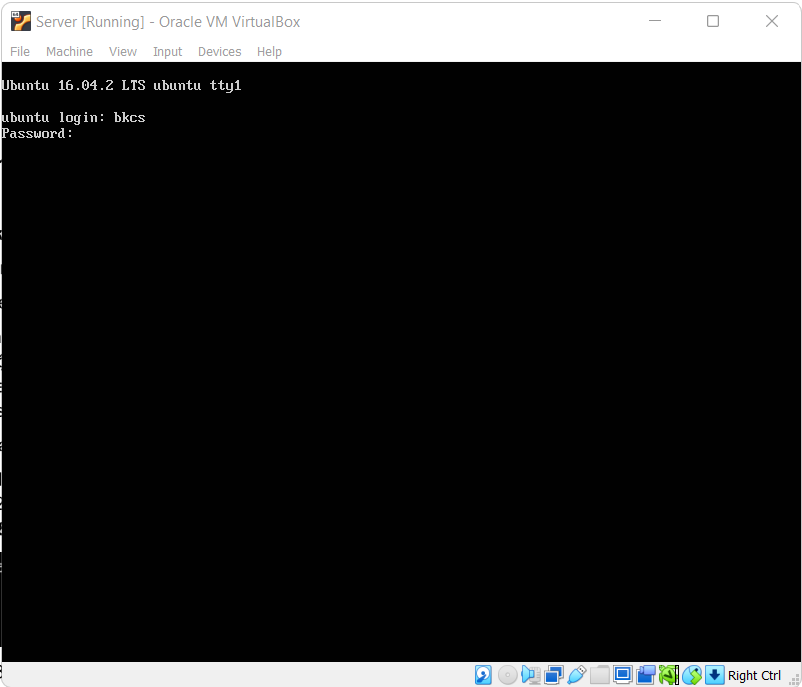


## **3)** **Triển khai máy ảo Server**

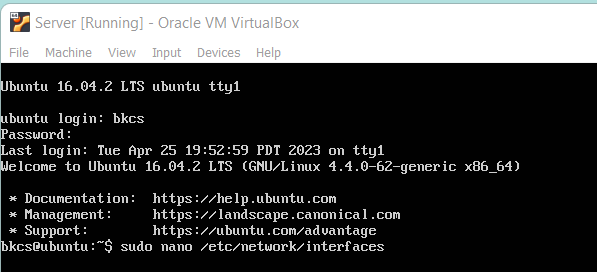
****

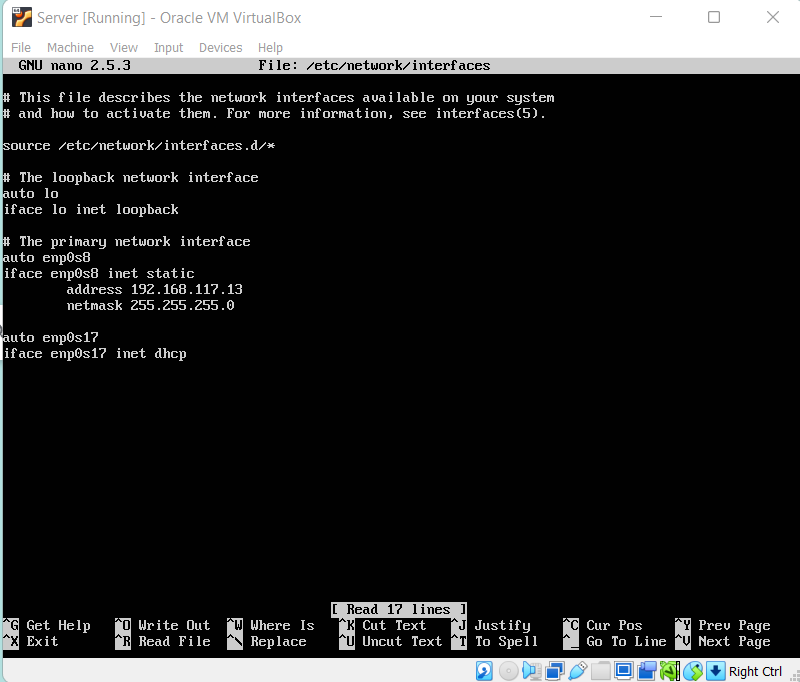
Username: bkcs

Password: bkcs

****

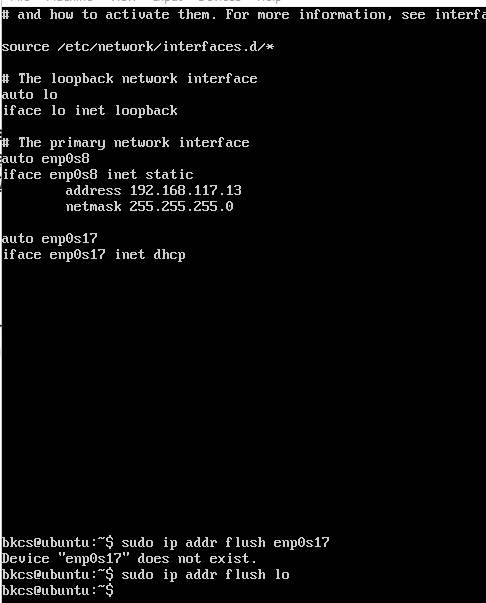
Nhập sudo nano /etc/network/interfaces

****

****

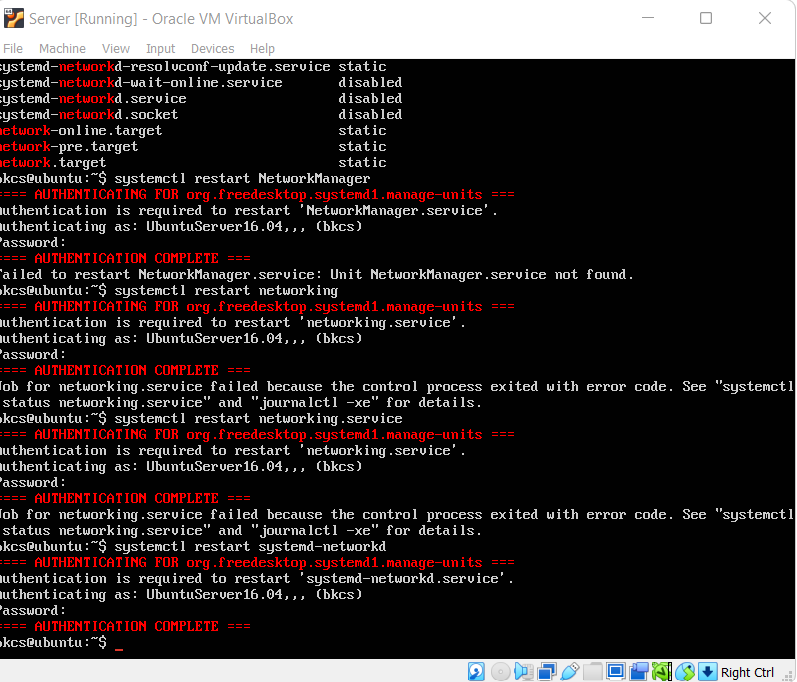
Nhấp Ctrl + O để lưu lại file. Nhấn Ctrl + X để đóng chương trình

sudo ip addr flush lo



Sau khi thử nhiều cách thì em sửa dụng lệnh:

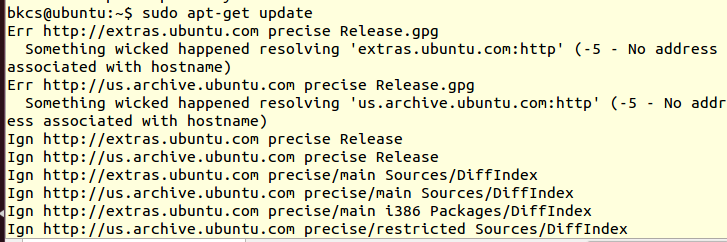
systemctl restart systemd-networkd



# LUYỆN TẬP

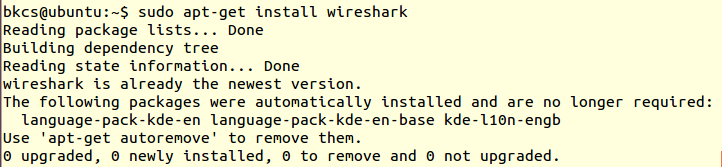
Cài Wireshark

sudo apt-get update



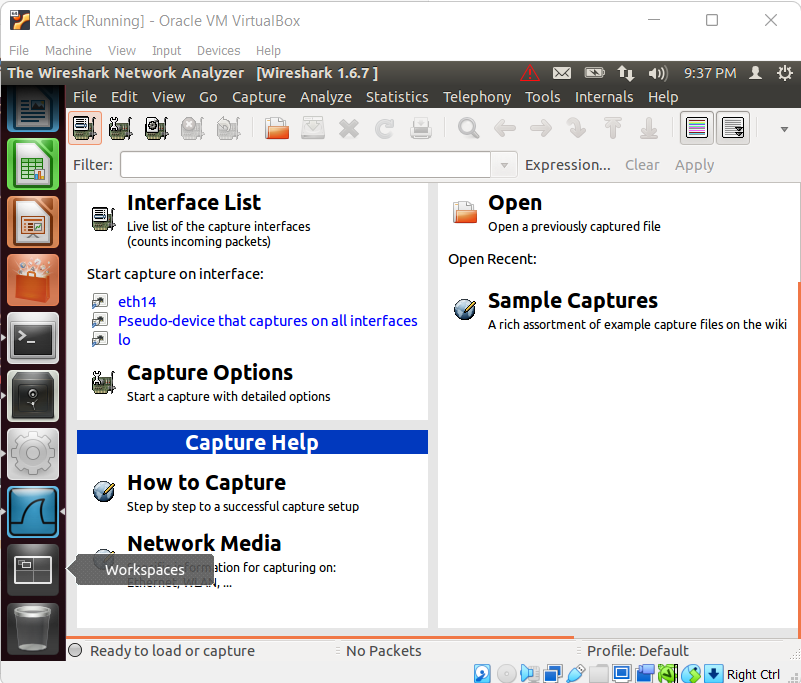
Lệnh cài

sudo apt-get install wireshark

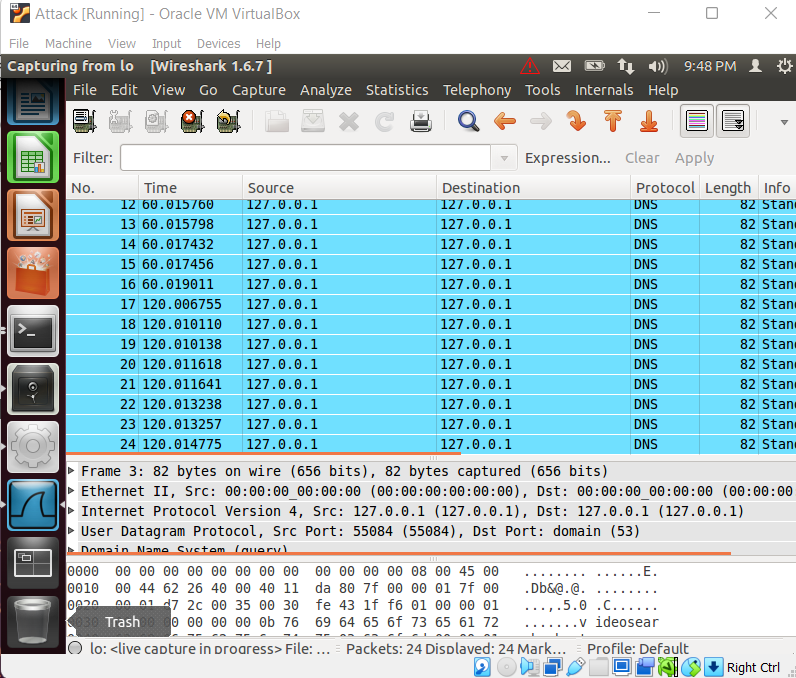


Để khởi động

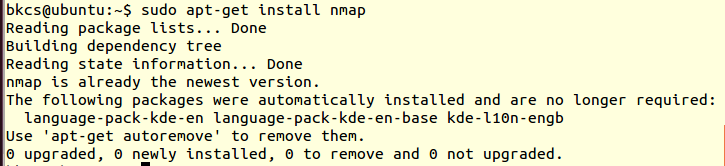
sudo wireshark



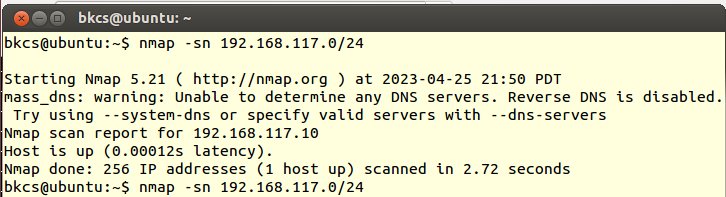
## **1. Quét thăm dò mạng**



Cài đặt nmap

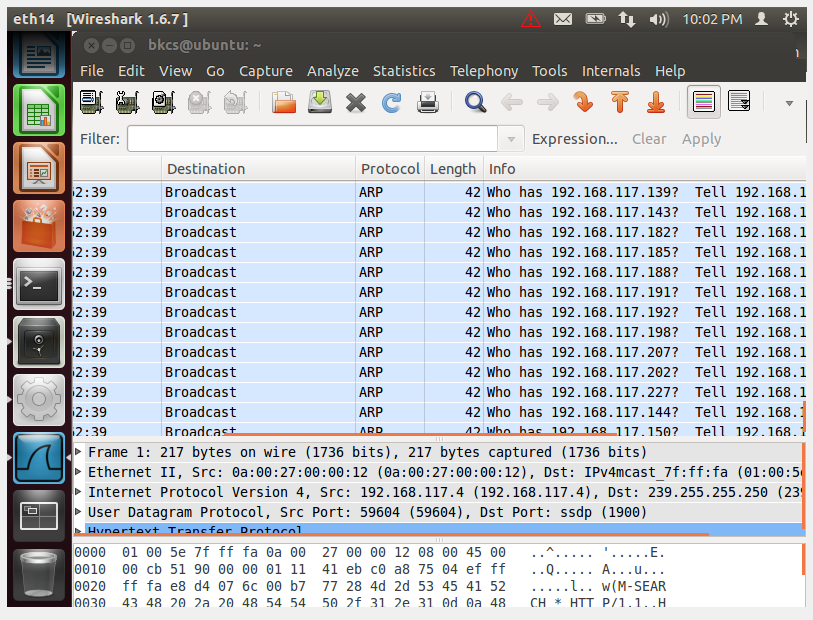


Chạy thử dòng lệnh

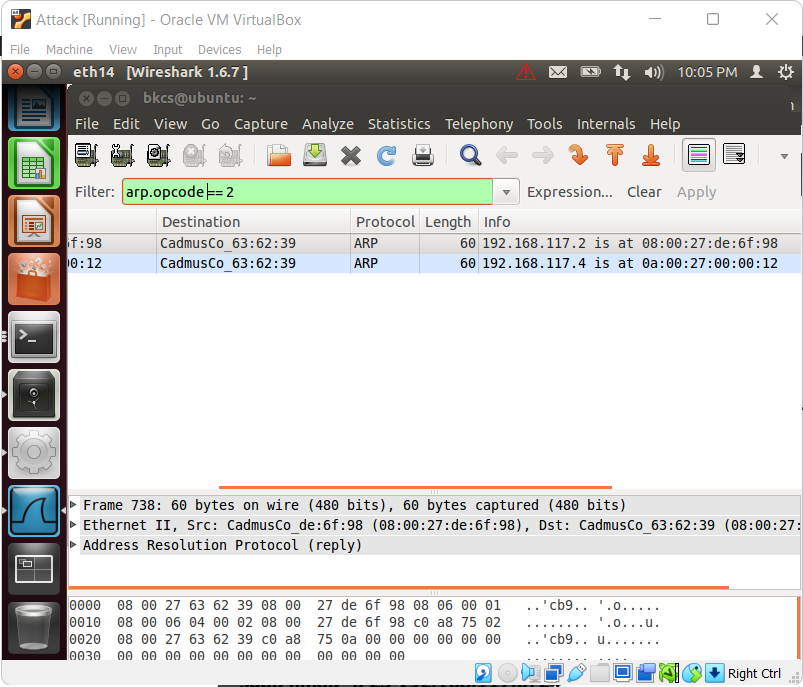


Dừng wireshark

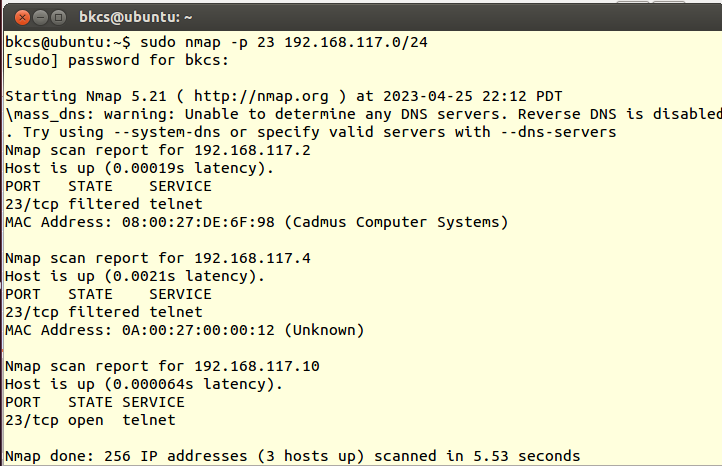
**Phân tích lưu lượng:**



Sử dụng giá trị arp.opcode == 2



## **2. Quét thăm dò dịch vụ**

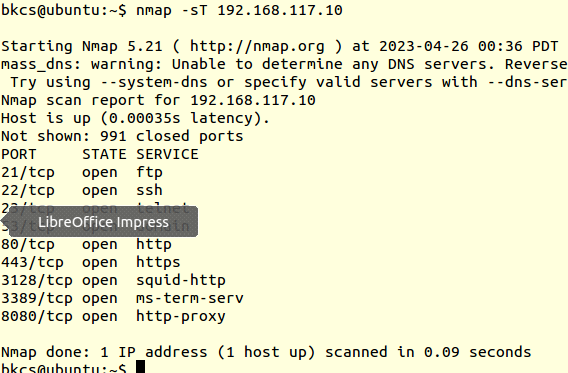
****

**Phân tích lưu lượng:**

****

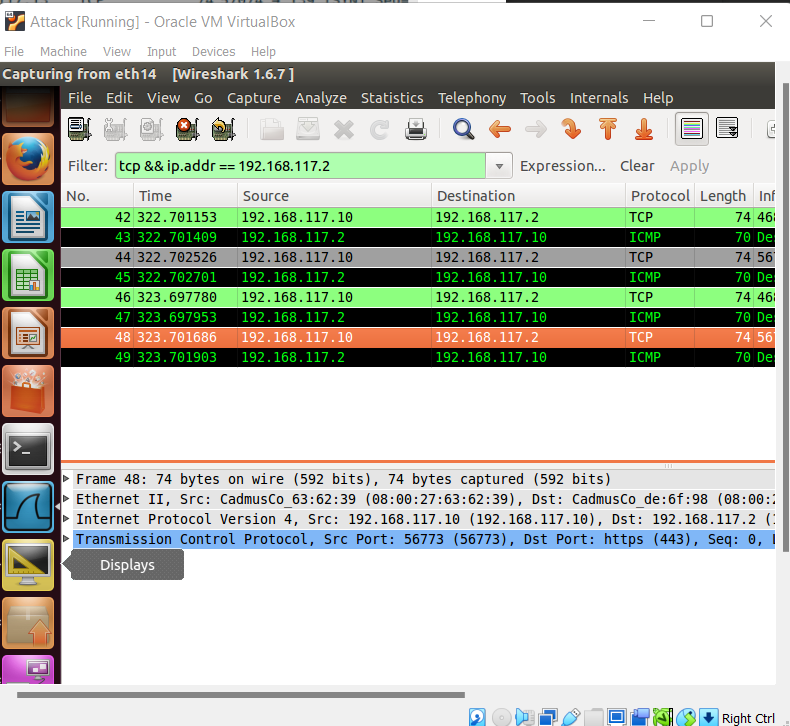


## **3. Quét cổng dịch vụ**

****

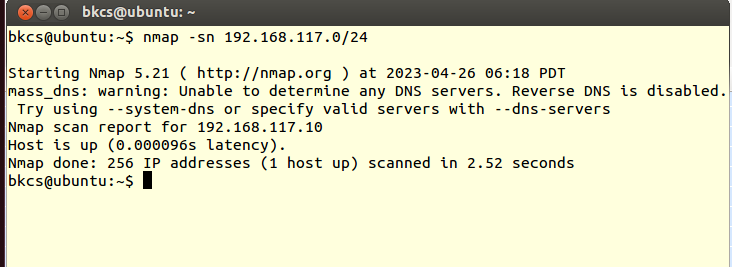
**Phân tích lưu lượng:**

****

****

# PHÂN TÍCH MỘT SỐ KĨ THUẬT QUÉT CỔNG ỨNG DỤNG CỦA NMAP

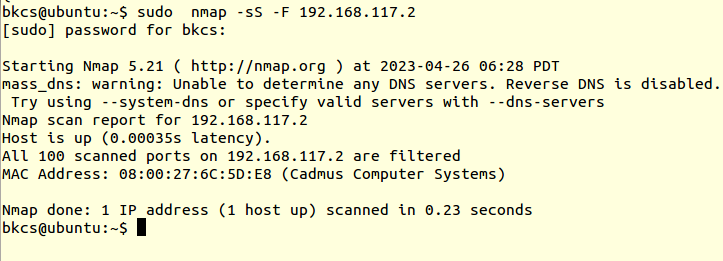
## **1) Kịch bản 1:** nmap –sn 192.168.117.0/24



Lựa chọn `nmap -sn 192.168.117.0/24` là để thực hiện quét "Ping Scan" (còn được gọi là "Host Discovery Scan") trên mạng con 192.168.117.0/24 bằng công cụ nmap trên máy do thám.

Dựa trên việc phân tích lưu lượng trên máy do thám, có thể xác định kỹ thuật quét đã được sử dụng là "Ping Scan" bởi vì các gói tin ping (ICMP Echo Request và ICMP Echo Reply) được bắt ghi lại trong lưu lượng được thu thập bởi Wireshark hoặc các công cụ bắt ghi lưu lượng mạng khác. Các gói tin ping này thường được sử dụng trong quá trình thực hiện quét "Ping Scan" để kiểm tra tính hoạt động của các địa chỉ IP trong mạng con mục tiêu.

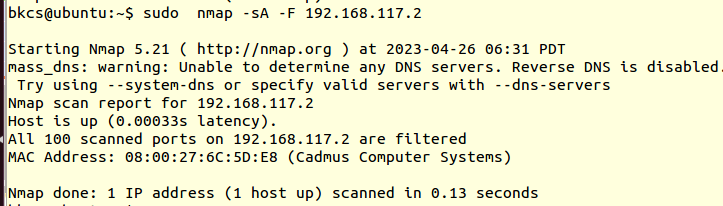
## **2) Kịch bản 2:** nmap –sS –F 192.168.117.2



Lựa chọn `nmap -sS -F 192.168.117.2` là để thực hiện quét "TCP SYN Scan" (còn được gọi là "Half-open Scan") trên địa chỉ IP 192.168.117.2 bằng công cụ nmap trên máy do thám.

Dựa trên việc phân tích lưu lượng trên máy do thám, có thể xác định kỹ thuật quét đã được sử dụng là "TCP SYN Scan" bởi vì các gói tin SYN (TCP SYN Packet) được gửi đi và các phản hồi từ máy chủ đích được bắt ghi lại trong lưu lượng được thu thập bởi Wireshark hoặc các công cụ bắt ghi lưu lượng mạng khác. Các gói tin SYN này thường được sử dụng trong quá trình thực hiện quét "TCP SYN Scan" để kiểm tra trạng thái của các cổng TCP trên máy chủ đích.

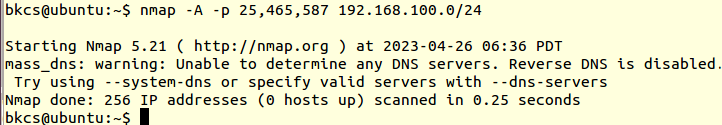
## **3) Kịch bản 3:** nmap –sA –F 192.168.117.2



Lựa chọn `nmap -sA -F 192.168.117.2` là để thực hiện quét "ACK Scan" trên địa chỉ IP 192.168.117.2 bằng công cụ nmap trên máy do thám.

Dựa trên việc phân tích lưu lượng trên máy do thám, có thể xác định kỹ thuật quét đã được sử dụng là "ACK Scan" bởi vì các gói tin ACK (TCP ACK Packet) được gửi đi và các phản hồi từ máy chủ đích được bắt ghi lại trong lưu lượng được thu thập bởi Wireshark hoặc các công cụ bắt ghi lưu lượng mạng khác. Các gói tin ACK này thường được sử dụng trong quá trình thực hiện quét "ACK Scan" để kiểm tra trạng thái của các cổng TCP trên máy chủ đích.

## **4) Thu thập thông tin hệ thống :**nmap -A -p 25,465,587 192.168.100.0/24



Sau khi bắt ghi lại lưu lượng mạng bằng Wireshark, bạn có thể phân tích các gợp tin và các gói dữ liệu trong đó để xác định các dịch vụ đang được cung cấp trên máy mục tiêu. Cụ thể, bạn có thể tìm kiếm các giao thức hoạt động trên các cổng mạng tương ứng với dịch vụ email, chẳng hạn là SMTP (cổng 25), POP3 (cổng 110), IMAP (cổng 143), và SSL/TLS (cổng 465, 993), để xác định các dịch vụ email đang hoạt động trên các máy chủ đã được quét bằng nmap.

Sau khi phân tích các gói dữ liệu trong lưu lượng mạng, bạn có thể xác định các thông tin liên quan đến dịch vụ email đang hoạt động trên các máy chủ, chẳng hạn như tên miền, tên của máy chủ email (như là tên máy chủ SMTP, POP3 hoặc IMAP), phiên bản của phần mềm email (nếu có), các tên người dùng hoặc địa chỉ email được sử dụng, và các tùy chọn cấu hình khác của dịch vụ email.

## **5) Tìm kiếm thông tin về các lỗ hổng**

|  |  |  |
| --- | --- | --- |
| Phần mềm dịch vụ | Số CVE | Mô tả ngắn gọn về lỗ hổng |
| Tên phần mềm: Apache HTTP Server  Phiên bản: 2.4.49 | CVE-2021-41773 | CVE-2021-41773: Lỗ hổng LFI (Local File Inclusion) cho phép tấn công đọc dữ liệu từ xa trên hệ thống mục tiêu. |
| Tên phần mềm: OpenSSH  Phiên bản: 8.7p1 | CVE-2020-15778  CVE-2021-28041 | CVE-2020-15778: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu.  CVE-2021-28041: Lỗ hổng DoS (Denial of Service) cho phép tấn công gây ngừng hoạt động dịch vụ trên hệ thống mục tiêu. |
| Tên phần mềm: MySQL Server  Phiên bản: 5.7.35 | CVE-2020-28942  CVE-2021-23842  CVE-2021-32596 | CVE-2020-28942: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu.  CVE-2021-23842: Lỗ hổng DoS (Denial of Service) cho phép tấn công gây ngừng hoạt động dịch vụ trên hệ thống mục tiêu.  CVE-2021-32596: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu. |
| Tên phần mềm: Microsoft Exchange Server  Phiên bản: 2016, 2019 | CVE-2020-0688  CVE-2021-26855  CVE-2021-26857  CVE-2021-26858  CVE-2021-27065 | CVE-2020-0688: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu.  CVE-2021-26855: Lỗ hổng SSRF (Server-Side Request Forgery) cho phép tấn công thực hiện yêu cầu từ xa trên hệ thống mục tiêu.  CVE-2021-26857: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu.  CVE-2021-26858: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu.  CVE-2021-27065: Lỗ hổng RCE (Remote Code Execution) cho phép tấn công thực hiện mã từ xa và kiểm soát hệ thống mục tiêu. |