BÁO CÁO BÀI THỰC HÀNH SỐ 1

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

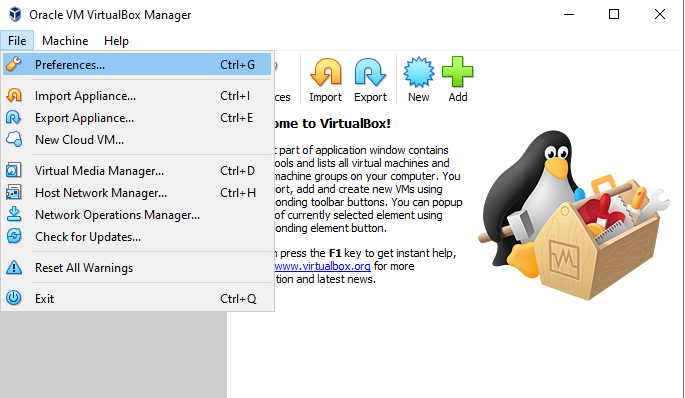
**Họ và tên sinh viên:** Võ Trương Phát Tài

**MSSV:** 0850080044

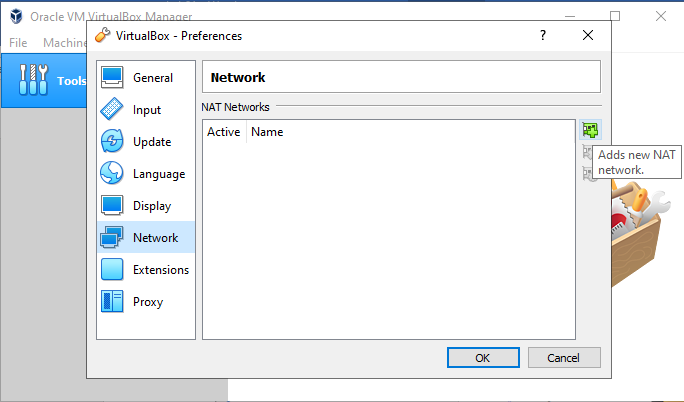
**PHẦN I: CÀI ĐẶT**

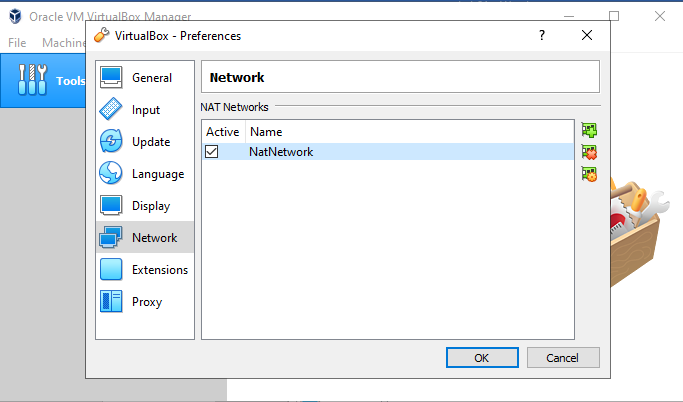
**1. Cài đặt và cấu hình Virtualbox**

**Bước 1:** Khởi động VirtualBox 🡪 Trên thanh menu chính, lựa chọn File 🡪 Preferences...

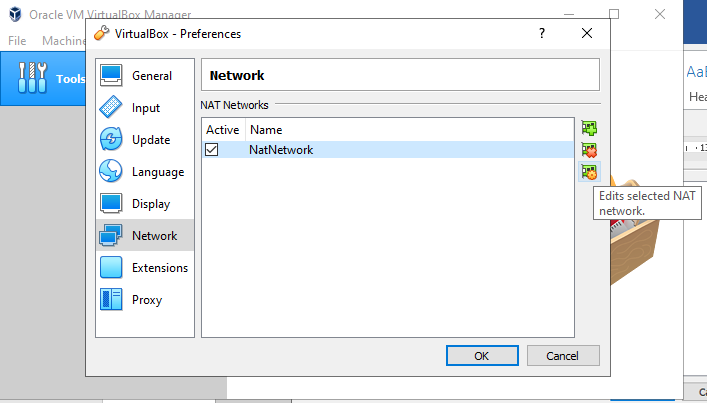
****

**Bước 2:** Trên cửa sổ Preferences, chọn mục Network. Lựa chọn Adds a new NAT network từ nút chức năng bên thay phải để thêm một mạng ảo mới

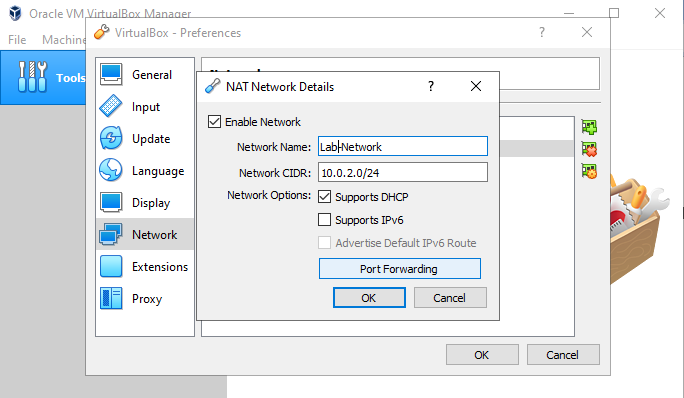
****

****

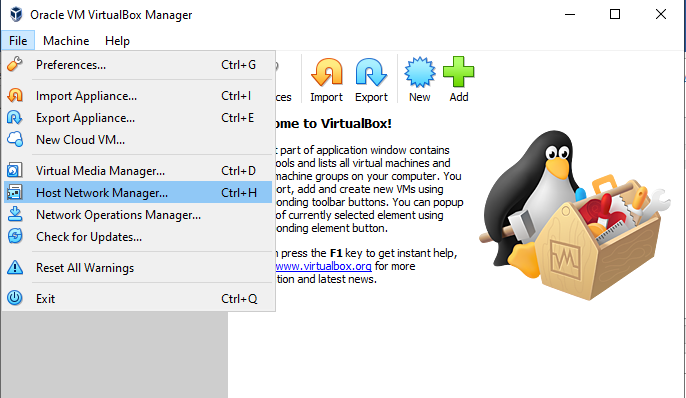
**Bước 3:** Chọn mạng ảo vừa được tạo ra và nhấn nút Edits selected NAT network

****

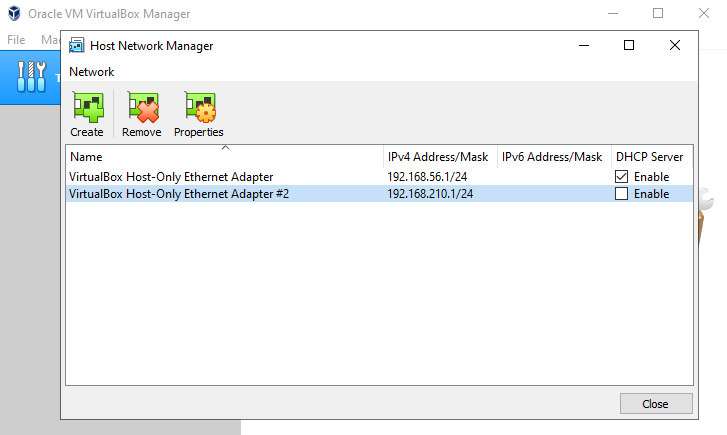
**Bước 4:** Thiết lập các thông số như hình ảnh sau và nhấn OK 🡪 Trên cửa sổ Preferences nhấn OK để hoàn tất và đóng cửa sổ

****

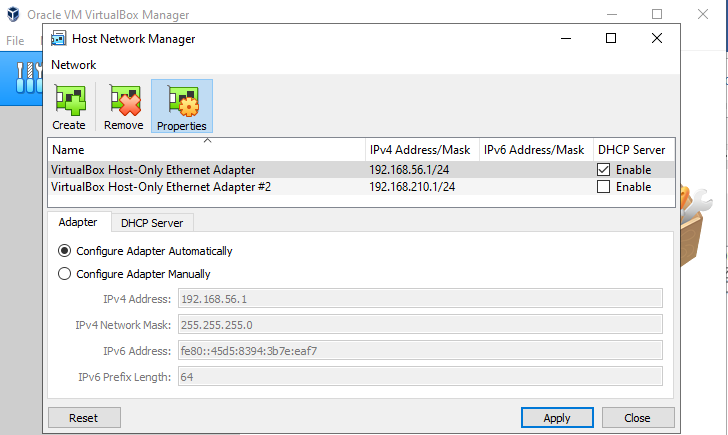
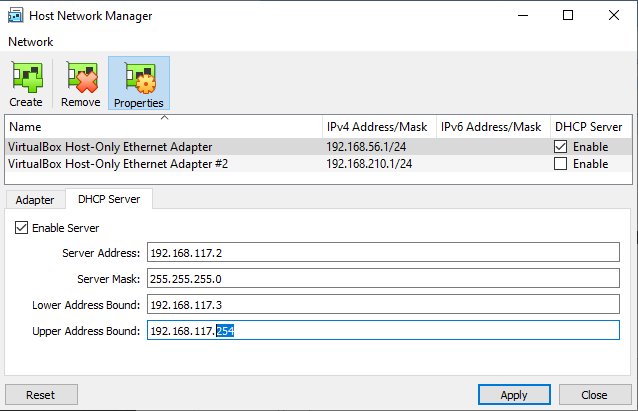
**Bước 5:** Trên giao diện của Virtualbox, chọn File 🡪 Host Network Manager...

****

**Bước 6:** Chọn các mạng ảo VirtualBox Host-Only Ethernet Adapter 🡪 Nhấn Create để tạo các mạng ảo



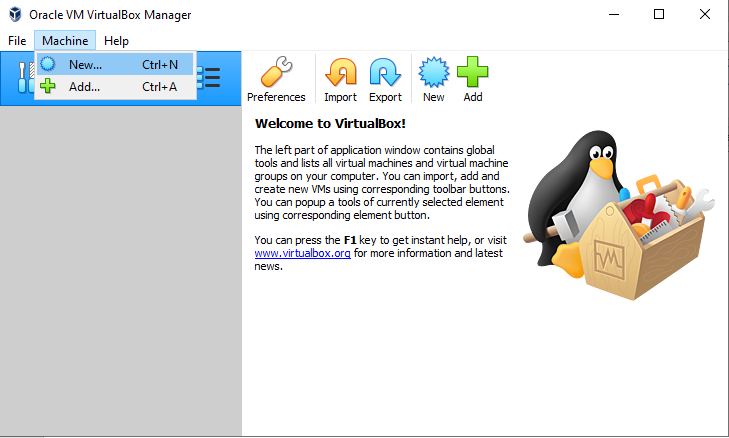
**Bước 7:** Chọn thẻ Adapter và lựa chọn Configure Adapter Automatically **🡪** Chọn thẻ DHCP Server và thiết lập các thông số như hình ảnh

****

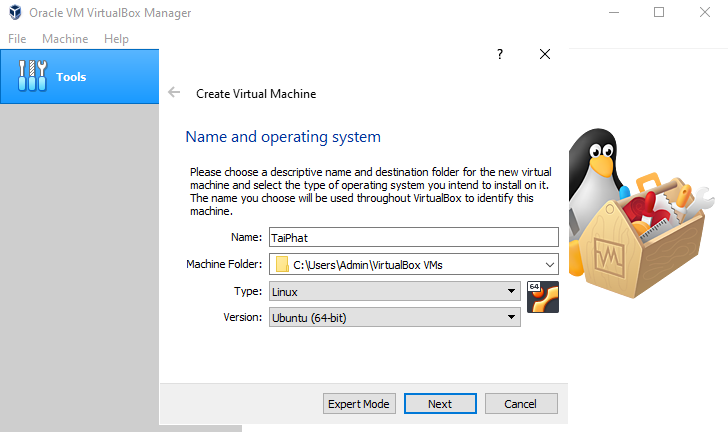
**Bước 8:** Nhấp nút Apply và Close để hoàn tất

**2. Triển khai máy ảo Attack**

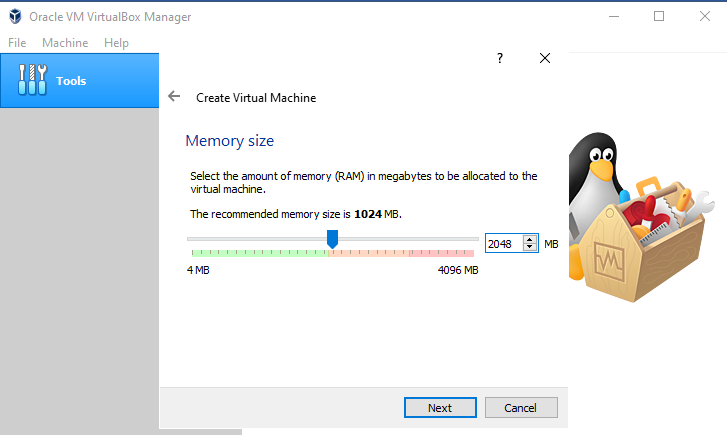
**Bước 1:** Trên cửa sổ chính của Virtualbox, chọn Machine 🡪 New...



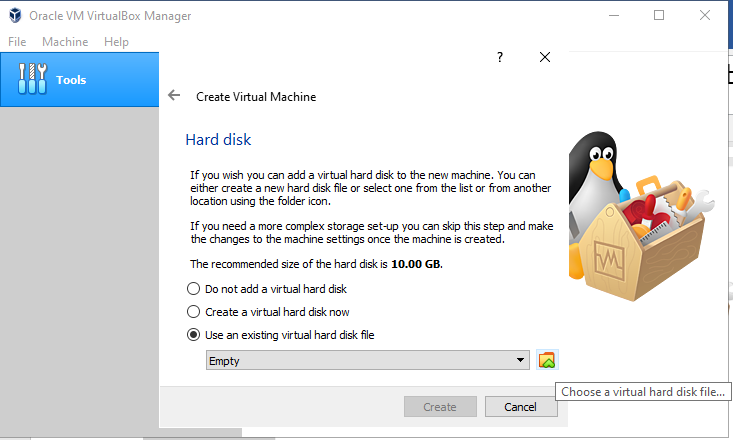
**Bước 2:** Trên cửa sổ tạo máy ảo, đặt các thông số như sau. Sau đó nhấn Next.



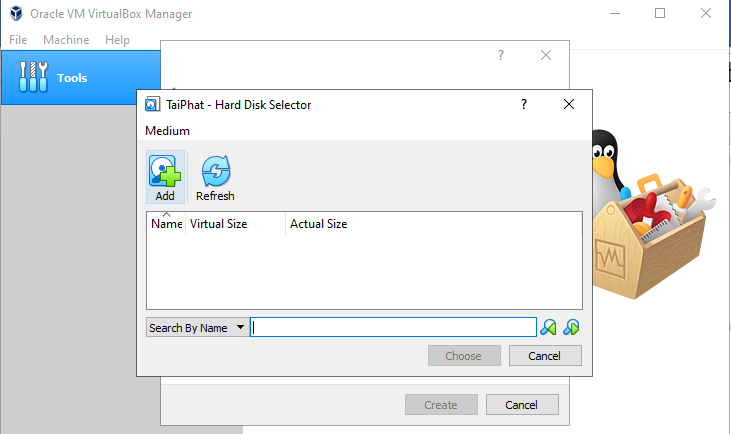
**Bước 3:** Chọn dung lượng bộ nhớ RAM cho máy ảo là 2048 MB. Nhấn Next để tiếp tục

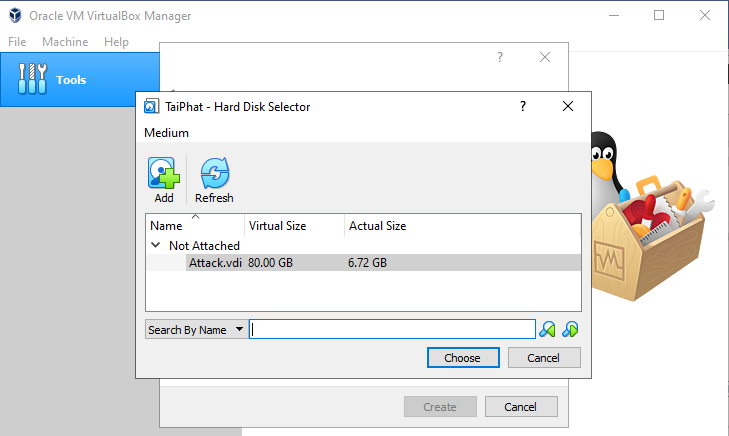
****

**Bước 4:** Trong cửa sổ tạo ổ cứng máy ảo, chọn mục Use an existing virtual hard disk file. Sau đó bấm nút Choose a virtual hard disk file...

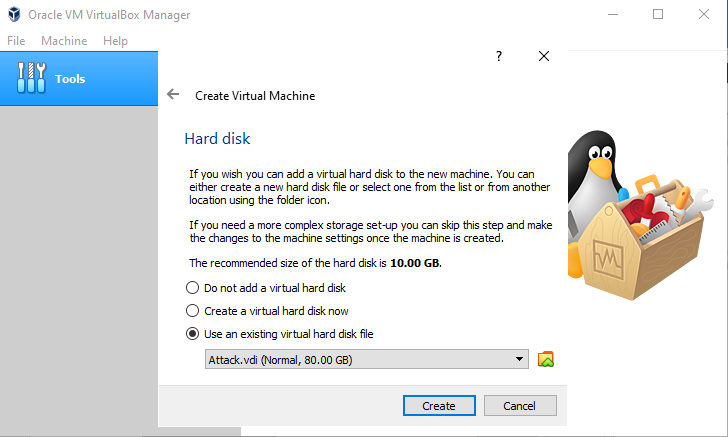
****

**Bước 5:** Trên cửa sổ Hard Disk Selector, nhấn Add và chọn file Attack.vdi đã download ở bước 1 để thêm vào danh sách

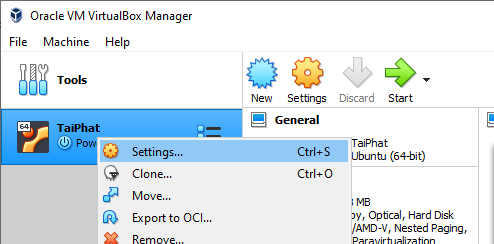
****

**Bước 6:** Chọn file Attack.vdi vừa được thêm vào trong danh sách ổ cứng ảo. Nhấn Choose để lựa chọn và đóng cửa sổ****

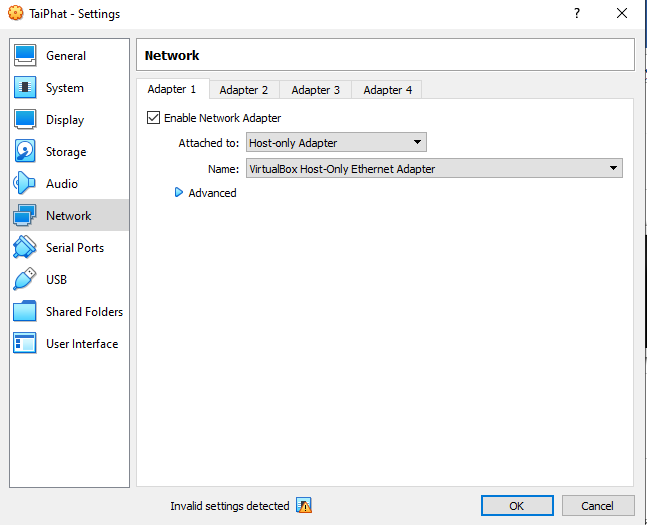
**Bước 7:** Trên cửa sổ Hard disk, nhấn Create để tạo ổ cứng ảo



**Bước 8:** Trên cửa sổ chính của Virtualbox, chọn máy ảo vừa tạo và nhấp chuột phải 🡪 Chọn Settings...



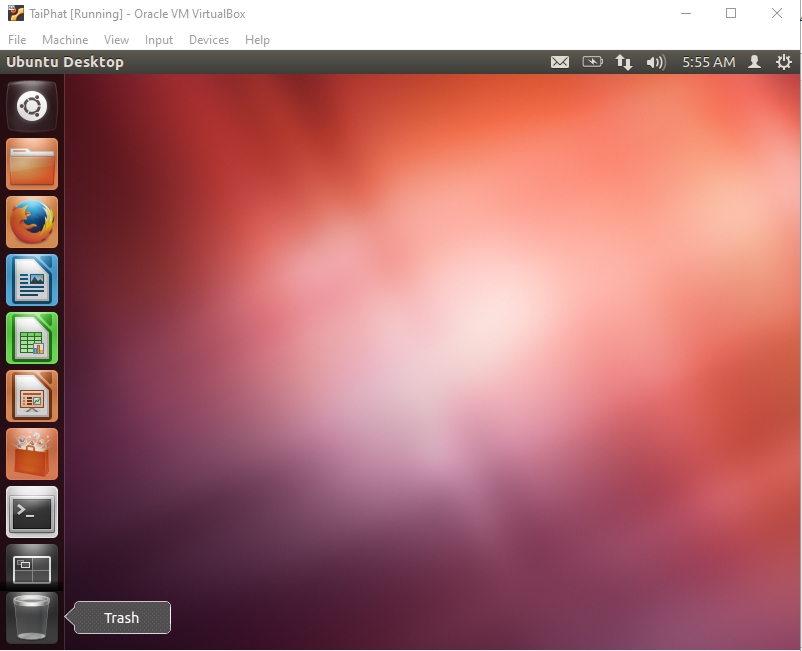
**Bước 9:** Chọn Network 🡪 Adapter 1. Thiết lập các thông số như sau



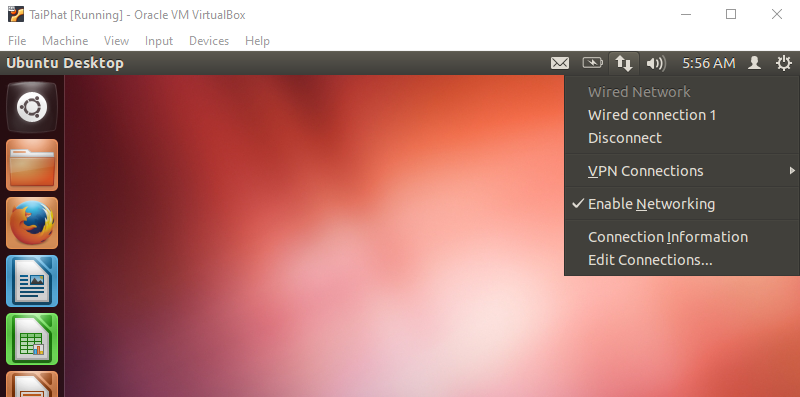
Sau khi máy ảo khởi động xong, đăng nhập bằng tài khoản sau:

- Username: bkcs

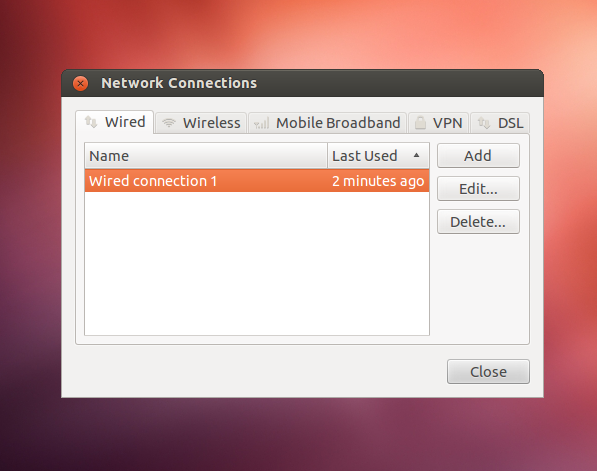
- Password: bkcs



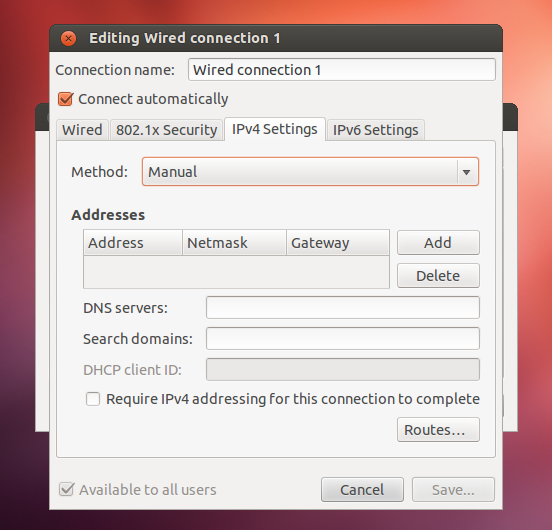
**Bước 10:** Trên màn hình máy ảo lựa chọn nhất chuột phải vào biểu tượng kết nối mạng và chọn Edit Connections...



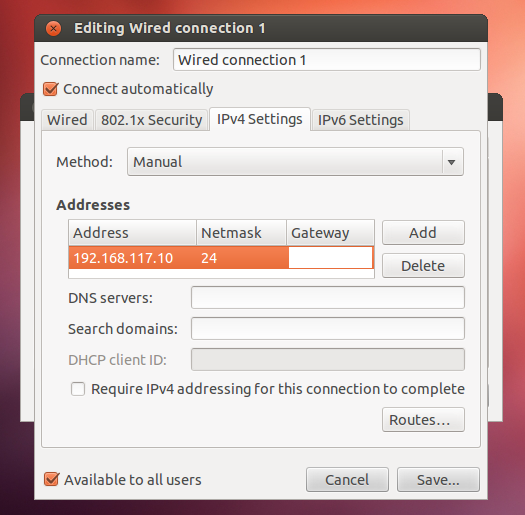
**Bước 11:** Chọn cạc mạng Wired connection 1 và nhấn Edit...



**Bước 12:** Chọn thẻ IPv4 Settings và chọn Method là Manual

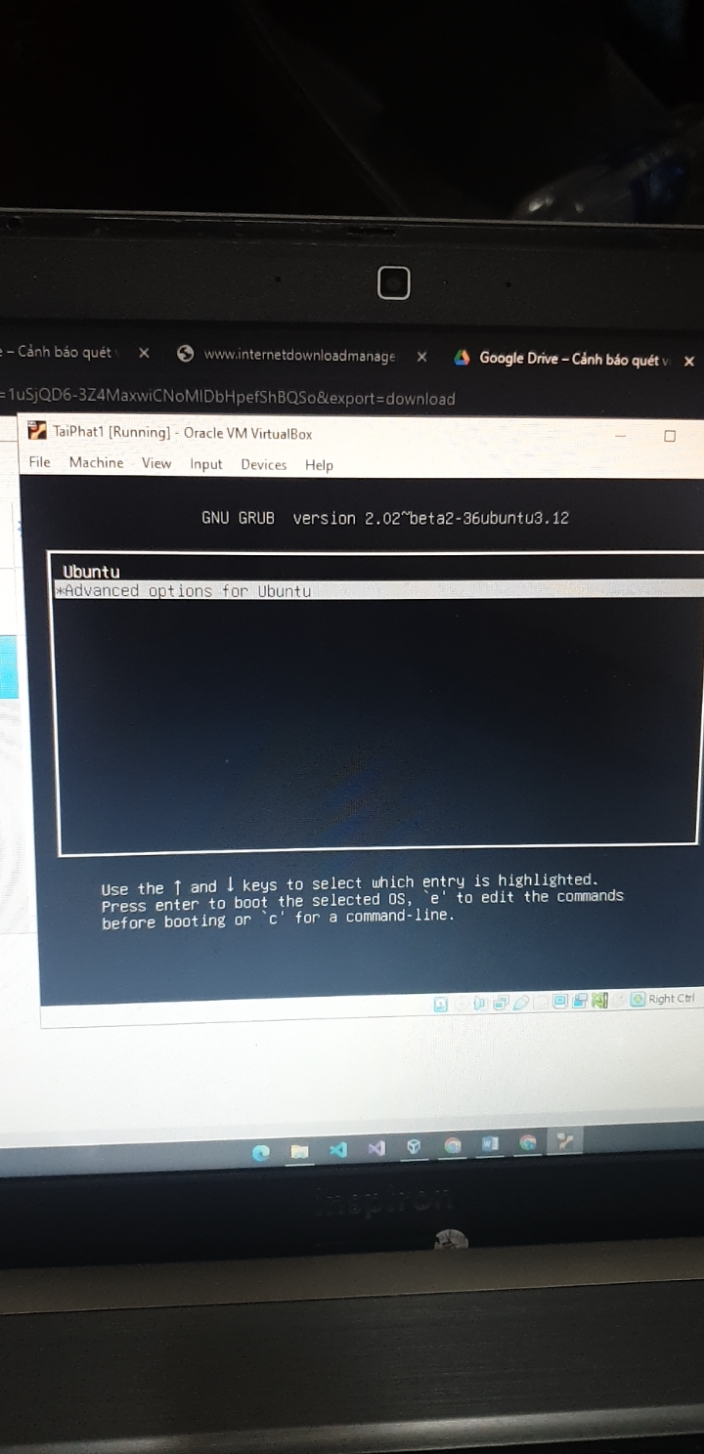


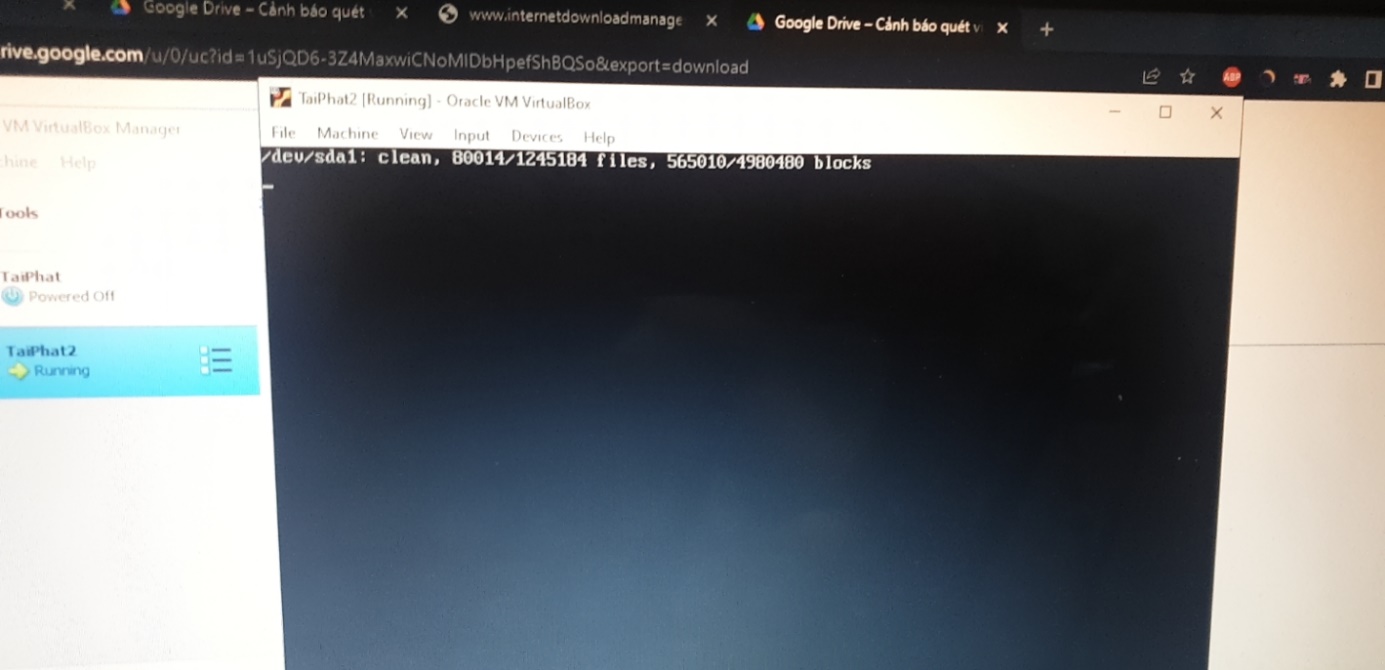
**Bước 13:** Nhấn nút Add và thiết lập các thông số địa chỉ IP cho cạc mạng này như hình ảnh dưới 🡪 nhấn nút Save để hoàn tất



**3. Triển khai máy ảo Server**

Thực hiện tương tự mục trên





**PHẦN II: 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

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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

**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

chỉ ra phải có hình ảnh chụp màn hình để minh chứng: 1 điểm

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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

**1.3. Kịch bản 3**

- 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

Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm

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

**2. Thu thập thông tin hệ thống**

- Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này? (1 điểm)

**Thông tin hệ điều hành:**

- Hình ảnh chụp kết quả của nmap: 0.25 điểm

- Nêu tên và phiên bản hệ điều hành: 0.25 điểm

**Thông tin dịch vụ: 1 điểm**

- Hình ảnh chụp kết quả của nmap: 0.25 điểm

- Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
|  |  |  |  |
|  |  |  |  |

**3. Tìm kiếm thông tin về các lỗ hổng**

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

Mỗi lỗ hổng: 1 điểm

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng**  **(Tiếng Việt)** |
|  |  |  |
|  |  |  |