BÁO CÁO BÀI THỰC HÀNH SỐ 1

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

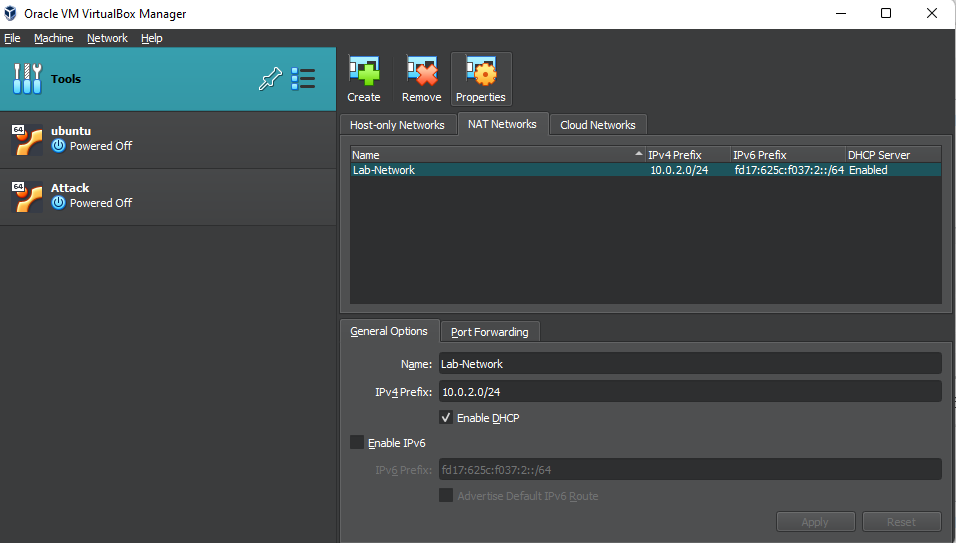
***Họ và tên sinh viên: Đoàn Dzoãn Tường Anh***

***MSSV: 0850080002***

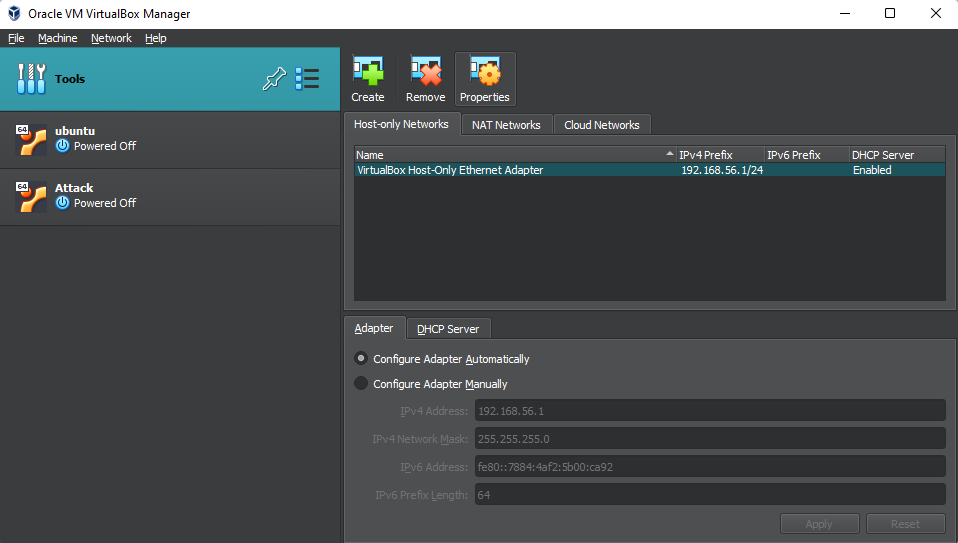
**KẾT QUẢ THỰC HÀNH**

**Thiết lập môi trường:**

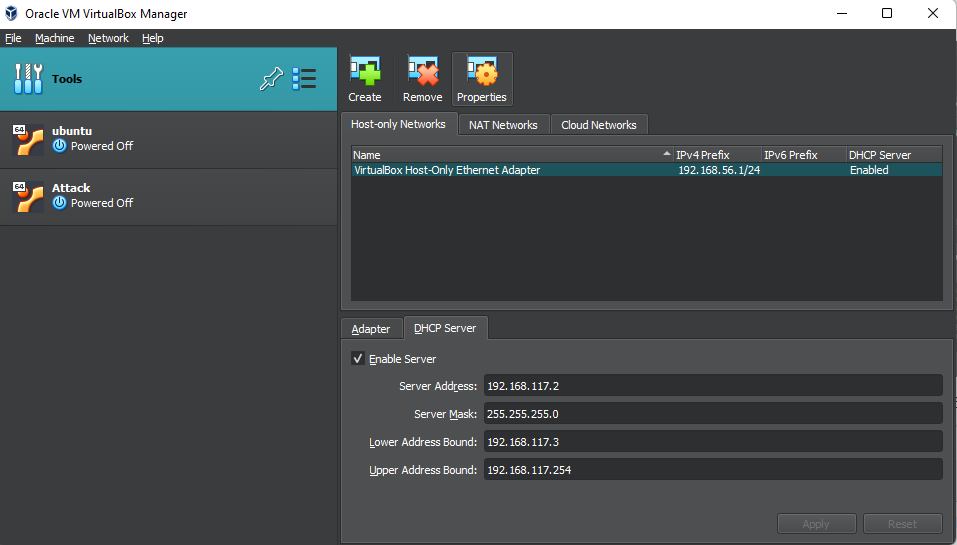
* **Thiết lập thông số Network**

****

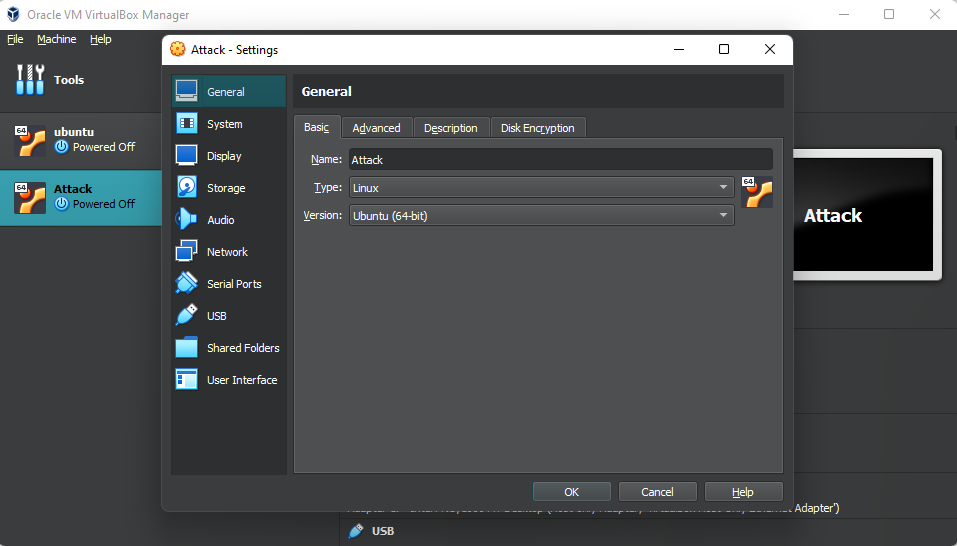
* **Chọn thẻ Adapter và lựa chọn Configure Adapter Automatically**

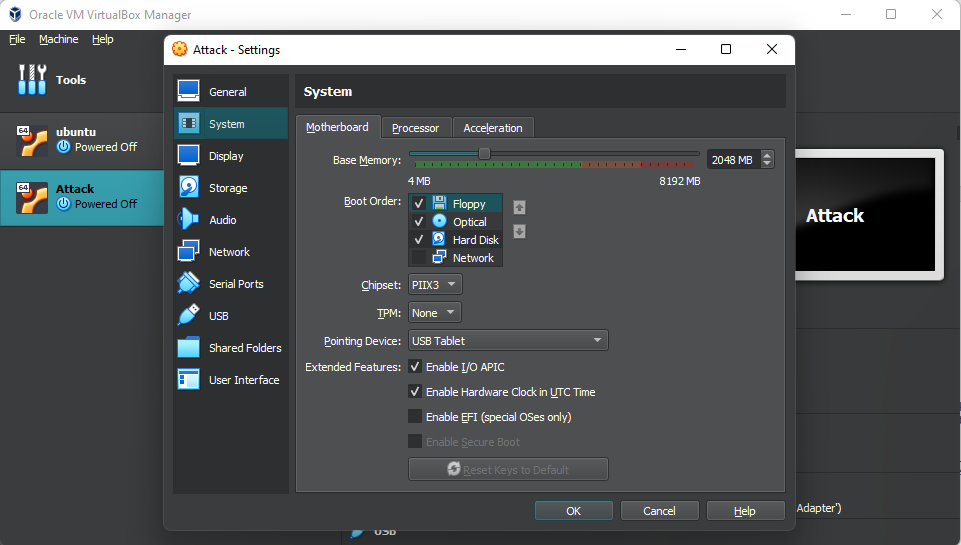
****

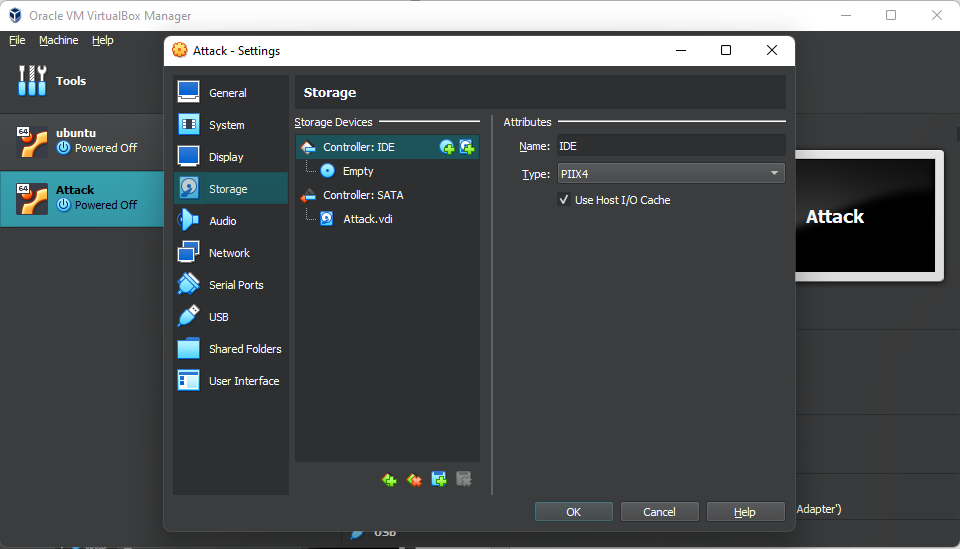
* **Chọn thẻ DHCP Server và thiết lập các thông số**

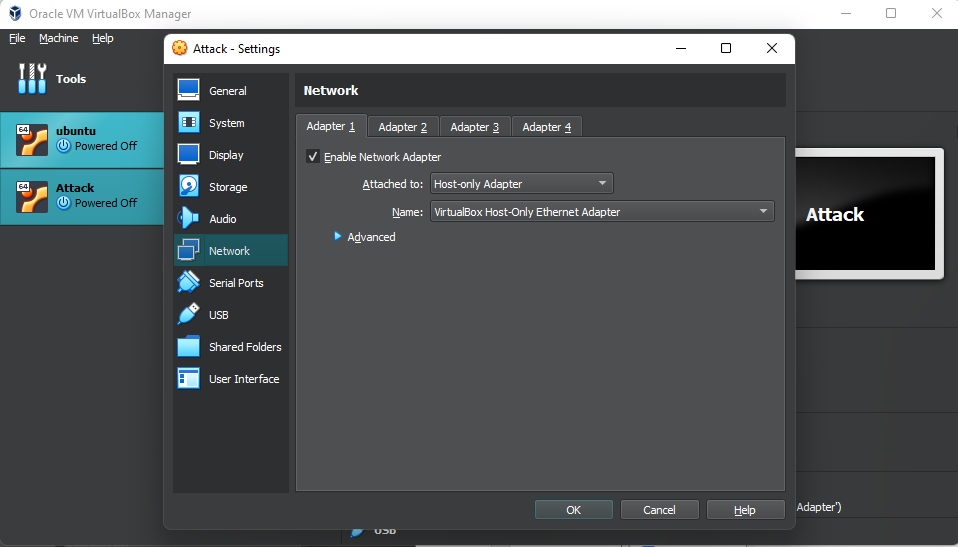
****

* **Cài đặt máy ảo Attack**

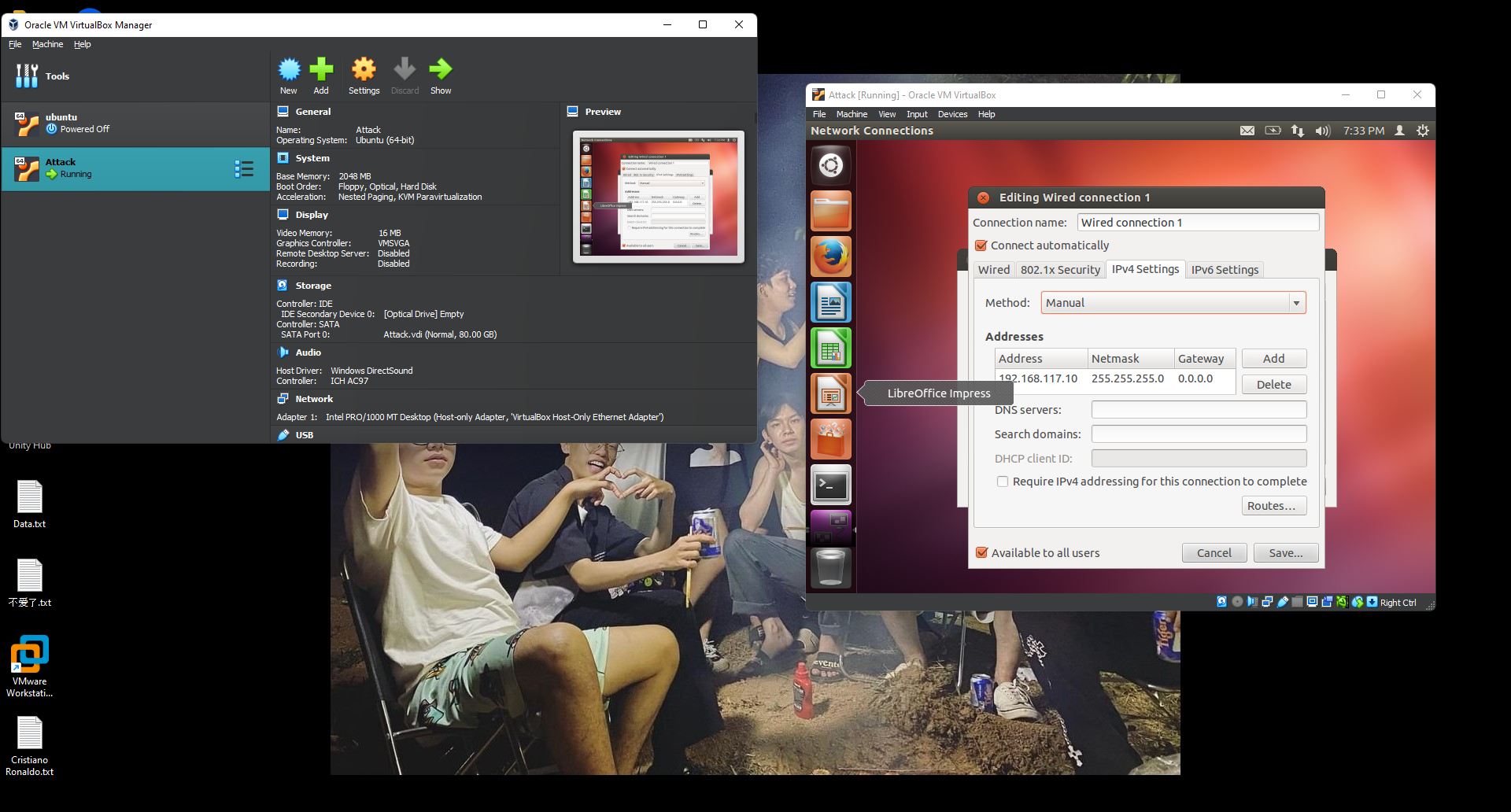
****

****

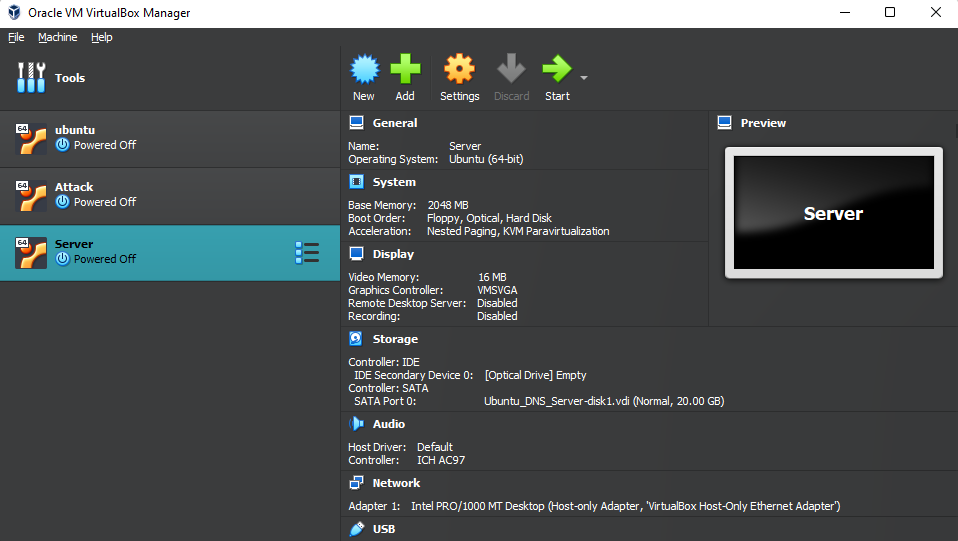
****

****

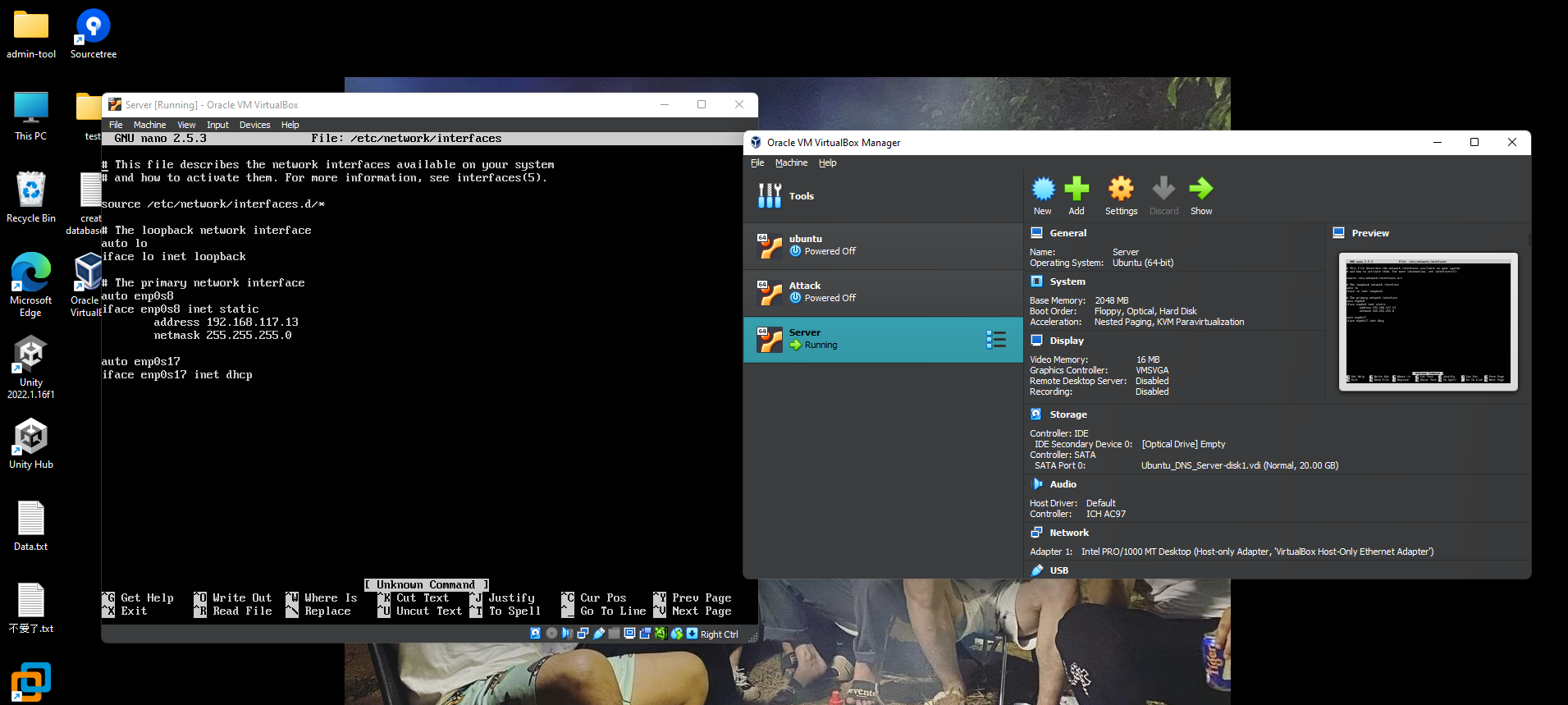
* **Edit network connection**

****

* **Triển khai máy ảo Server**

****

* **Thiết lập thông số địa chỉ IP**

****

* **Quét thăm dò mạng**

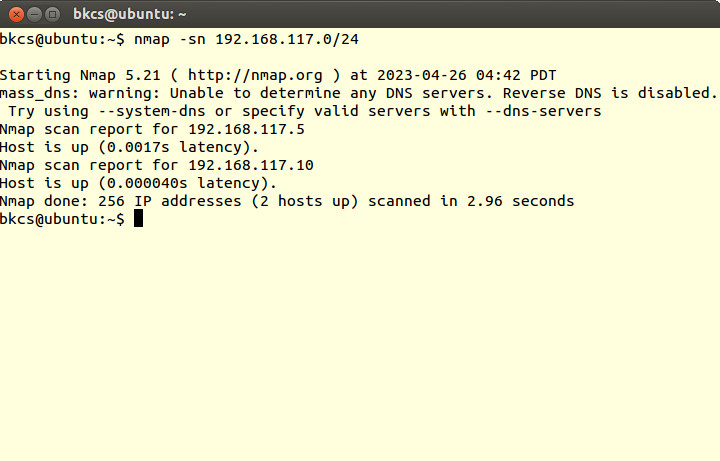
Bước 1: Truy cập máy ảo Attack

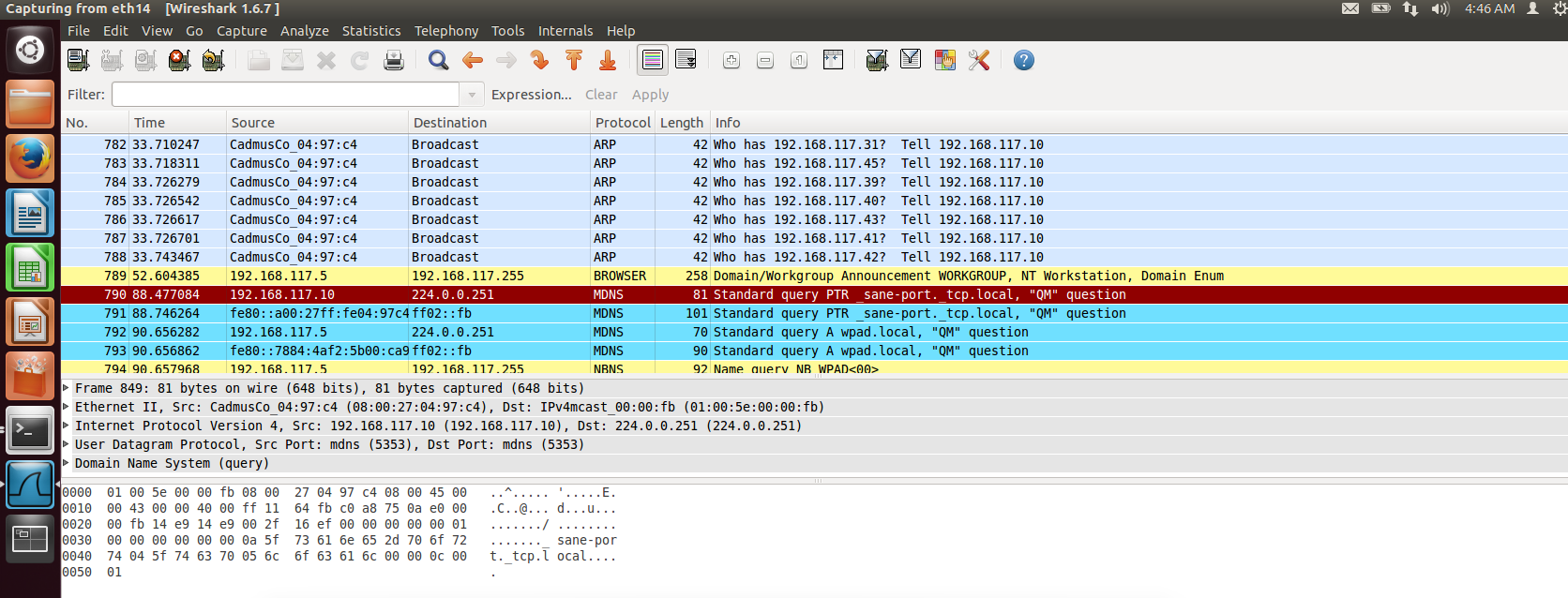
Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: nmap –sn 192.168.117.0/24

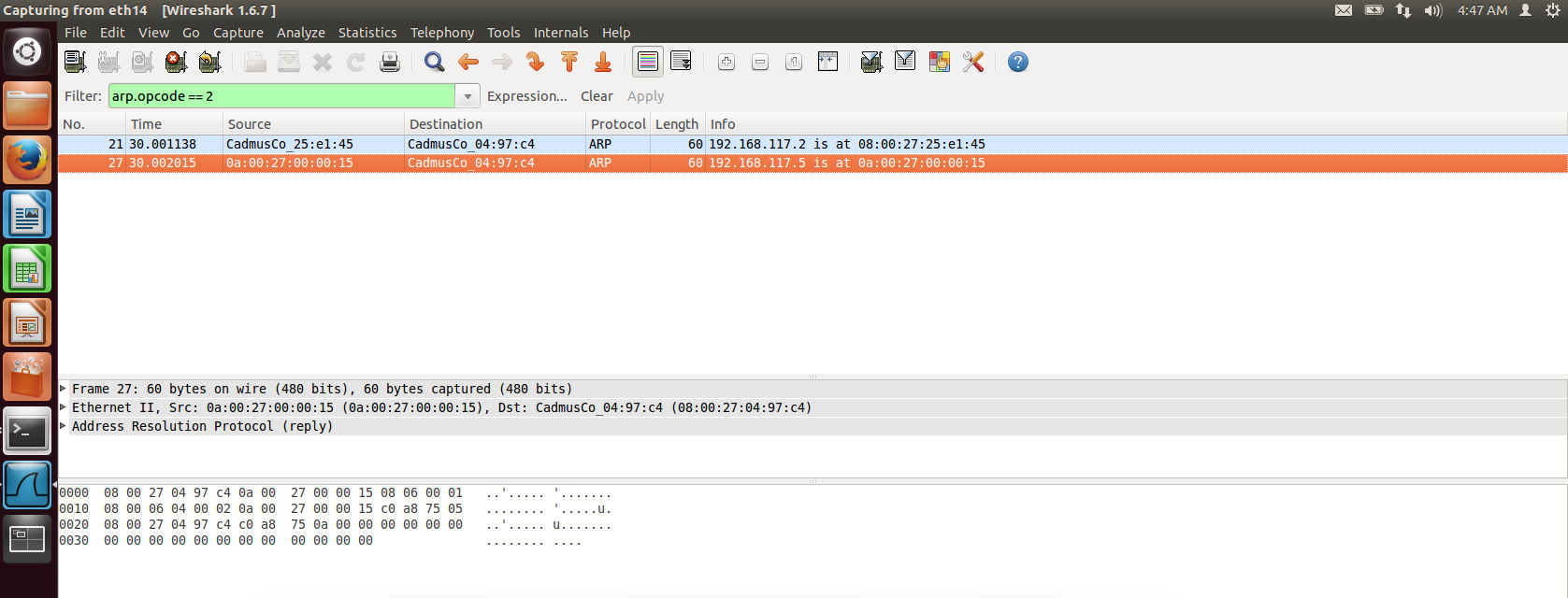
Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự

như sau:





Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động



* **Quét thăm dò dịch vụ**

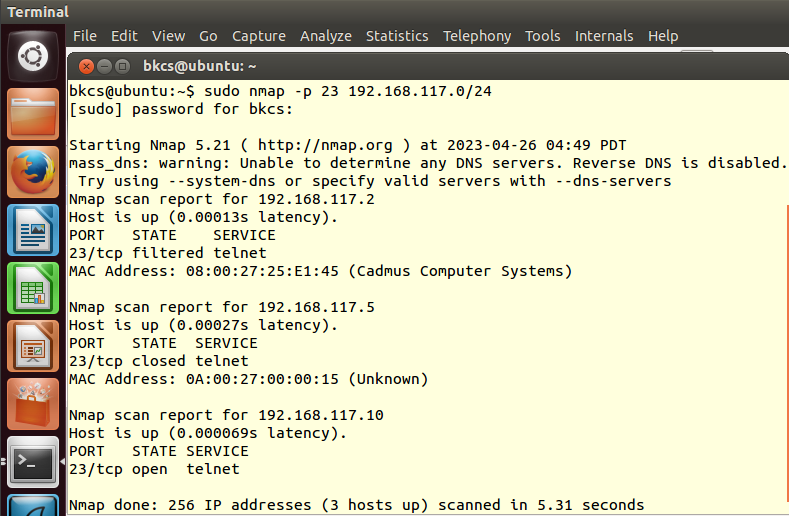
Bước 1: Truy cập máy ảo Attack

Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

sudo nmap -p 23 192.168.117.0/24

Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

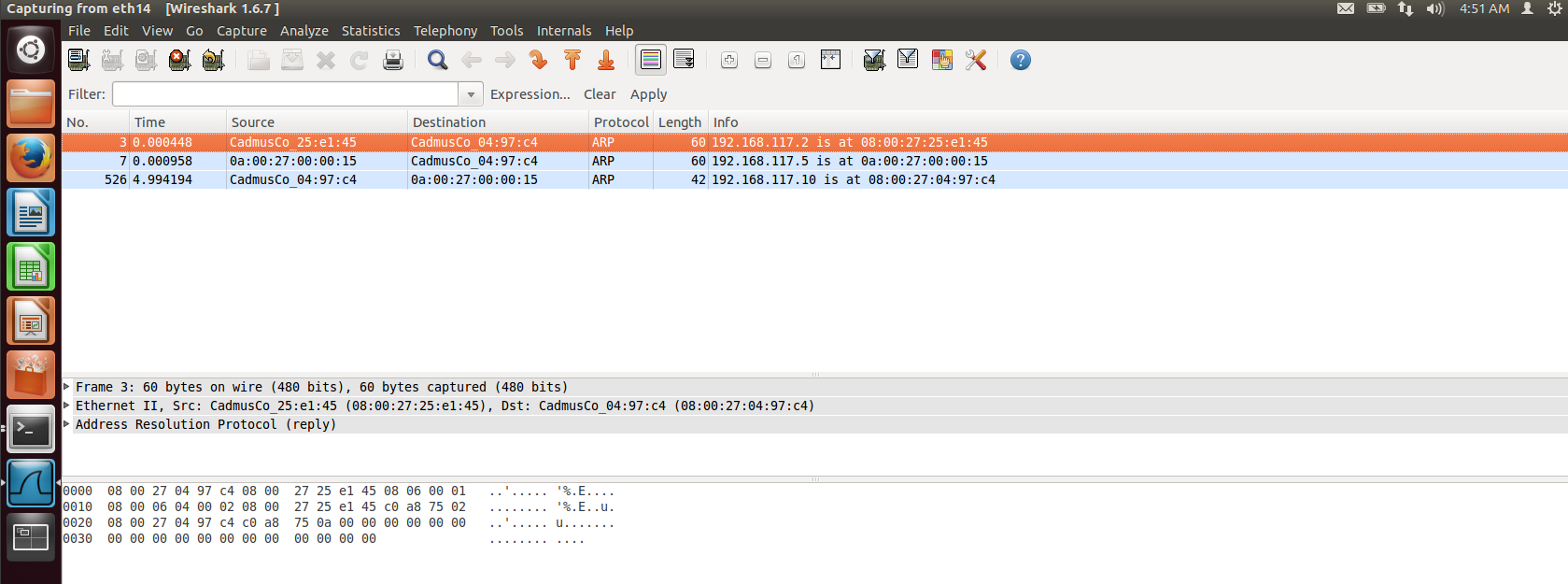


Bước 5: Dừng bắt gói tin trên Wireshark

Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, có thể

thấy rằng máy tấn công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC

của các máy tính trong mạng 192.168.117.0/24.

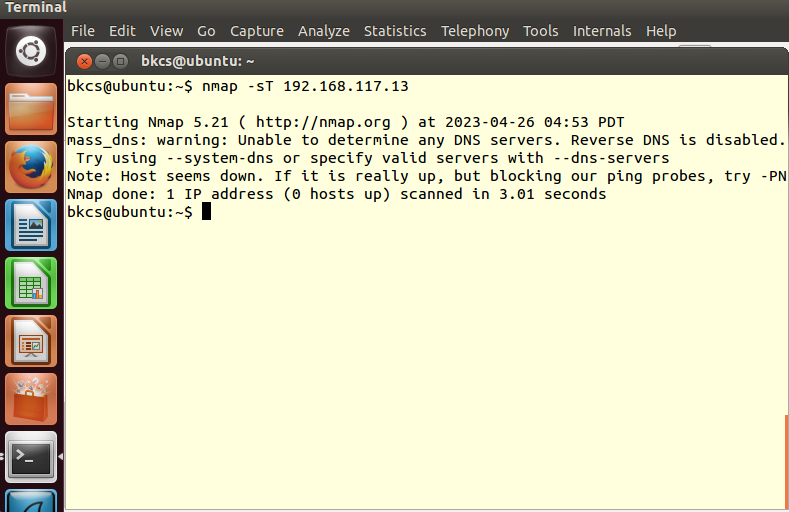


* **Quét cổng dịch vụ**

Bước 1: Truy cập máy ảo Attack

Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:



1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1:** *nmap –sn 192.168.117.0/24*

Lệnh nmap -sn 192.168.117.0/24 được sử dụng để thực hiện một quét ping (ping sweep) trên một mạng IP con nhất định. Cụ thể, nó sử dụng kỹ thuật quét ping (ICMP echo request) để gửi một gói tin ping đến từng địa chỉ IP trong mạng con 192.168.117.0/24 và chờ đợi phản hồi (ICMP echo reply) từ các thiết bị trong mạng con.

Kỹ thuật quét này cho phép kiểm tra xem những địa chỉ IP nào đang hoạt động trong mạng con này và đưa ra báo cáo về các địa chỉ IP đã phản hồi, cho biết máy chủ nào có thể đang hoạt động, và những thiết bị nào đã khởi động và sẵn sàng cho việc truy cập mạng.

Tuy nhiên, cần lưu ý rằng kỹ thuật quét ping này không hiệu quả trên các mạng mà các firewall hoặc các bảo mật mạng khác đã chặn các gói tin ping (ICMP).

1. **Kịch bản 2:** *nmap –sS –F 192.168.117.2*

Sử dụng kỹ thuật quét TCP SYN để kiểm tra các cổng TCP trên máy chủ mục tiêu mà không kích hoạt các trình báo bảo mật hoặc ghi lại các dòng lịch sử trong các bản ghi.

Kỹ thuật quét TCP SYN gửi một yêu cầu mở kết nối TCP bằng cách gửi một gói tin SYN đến cổng đích. Nếu cổng đó đang mở, nó sẽ trả lời bằng một gói tin SYN-ACK. Khi đó, máy quét gửi một gói tin RST để đóng kết nối.

Tùy thuộc vào kết quả trả về từ các cổng được quét, nó cung cấp thông tin về các dịch vụ đang chạy và các lỗ hổng bảo mật trên máy chủ mục tiêu

1. **Kịch bản 3:** *nmap –sA –F 192.168.117.2*

Sử dụng kỹ thuật quét TCP ACK để kiểm tra các cổng TCP trên máy chủ mục tiêu mà không kích hoạt các trình báo bảo mật hoặc ghi lại các dòng lịch sử trong các bản ghi.

Kỹ thuật quét TCP ACK sử dụng một kỹ thuật tương tự như quét TCP SYN, tuy nhiên, nó sử dụng gói tin ACK thay vì gói tin SYN. Gói tin ACK được sử dụng để xác nhận việc gửi dữ liệu TCP trước đó đã được chấp nhận bởi máy chủ. Khi máy quét gửi một gói tin ACK đến cổng đích, nếu cổng đó đang mở, nó sẽ trả lời bằng một gói tin RST để đóng kết nối.

1. **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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **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)** |
|  |  |  |
|  |  |  |