**Phần 1: Cài đặt**

Cài đặt **VituarBox**

Mở file VirtualBos.exe

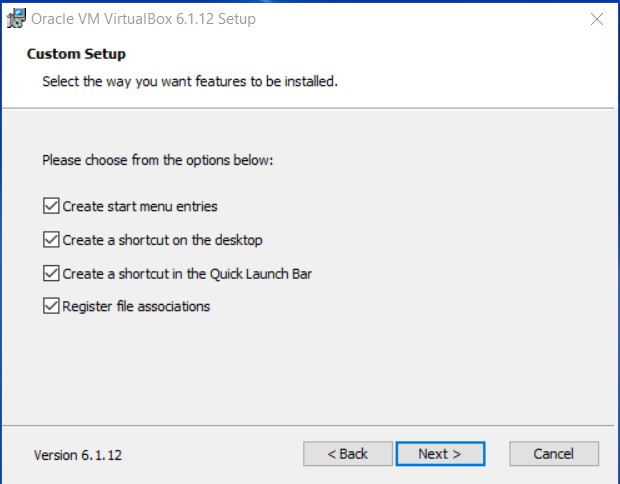
Chọn next



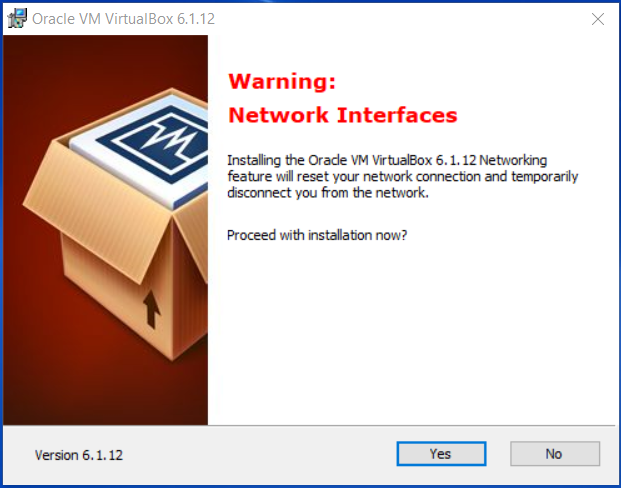
Next



Next



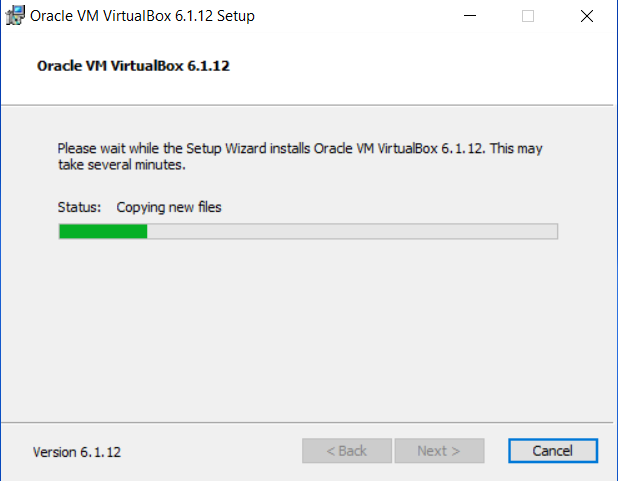
Chọn yes



Chọn Install



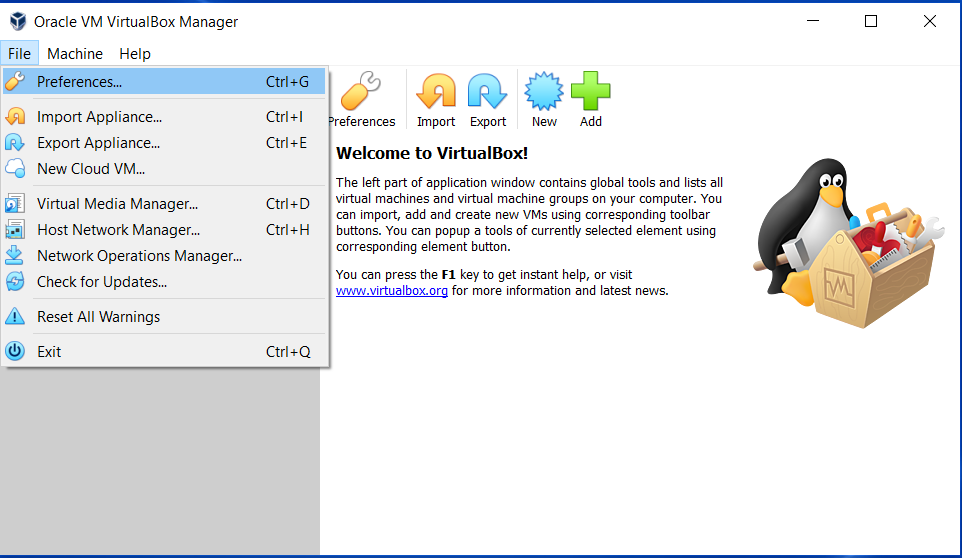
Đợi phần mềm khởi động



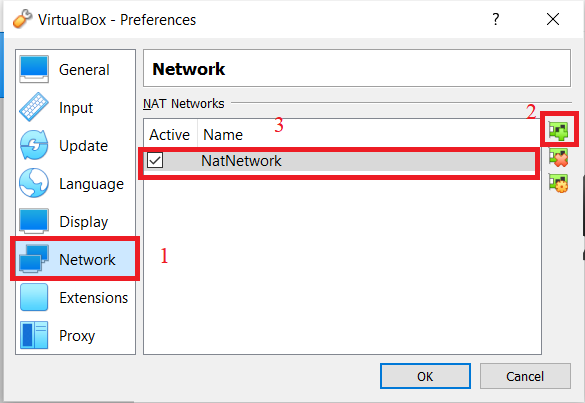
Đã cài đặt thành công ta chọn finish



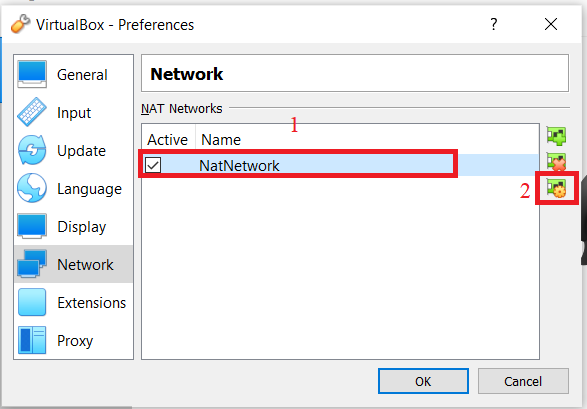
Trên thanh menu chính, lựa chọn File 🡪 Preferences...



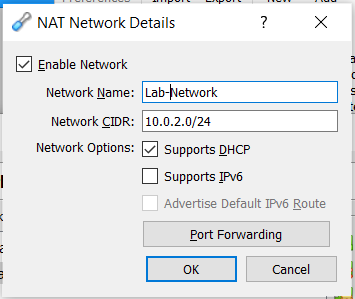
Trên thanh menu chính, lựa chọn File 🡪 Preferences...



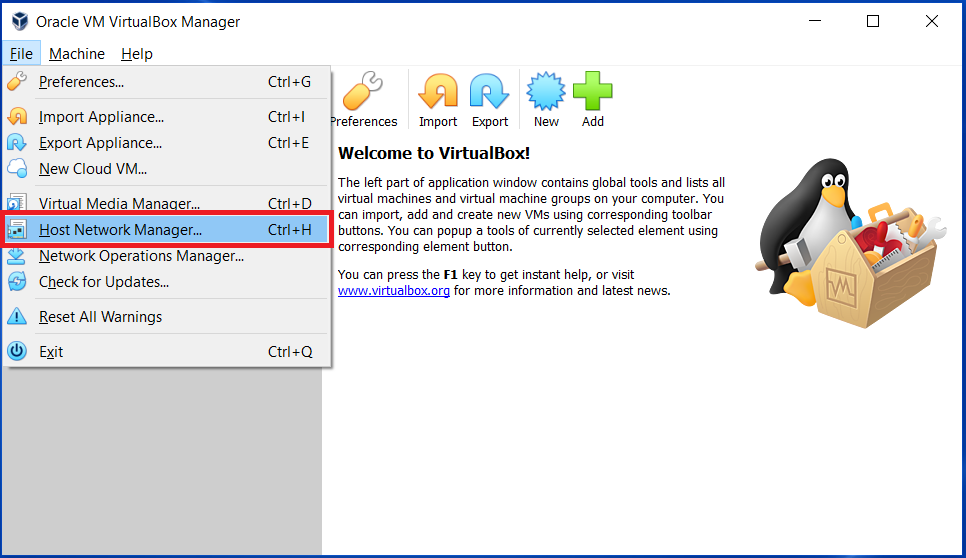
Chọn mạng ảo vừa được tạo ra và nhấn nút Edits selected NAT network



Thiết lập các thông số và nhấn OK

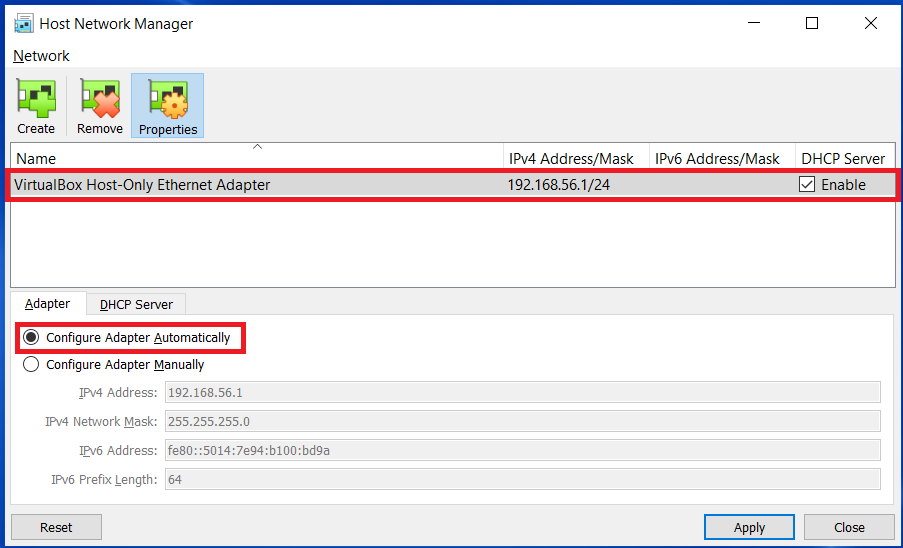


Trên giao diện của Virtualbox, chọn File  Host Network Manager...

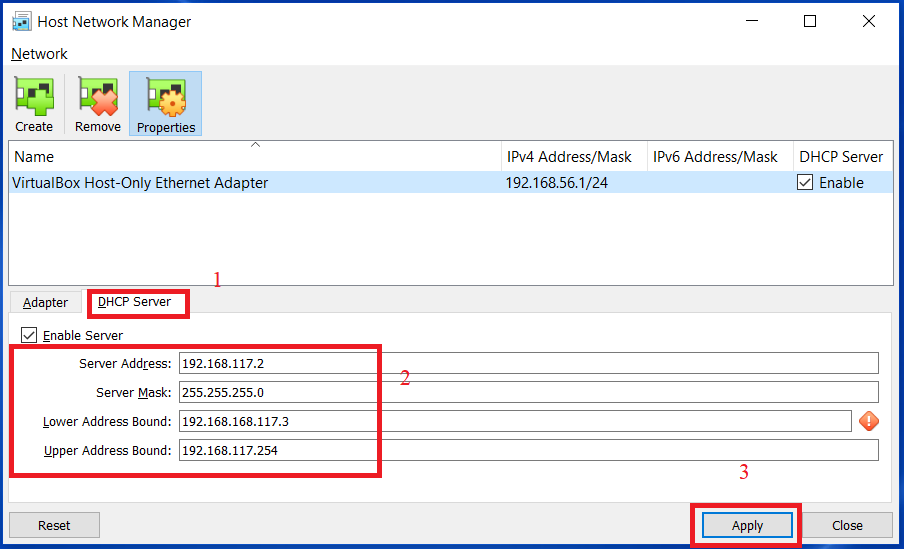


Chọn cạc mạng ảo VirtualBox Host-Only Ethernet Adapter.

Chọn thẻ Adapter và lựa chọn Configure Adapter Automatically.



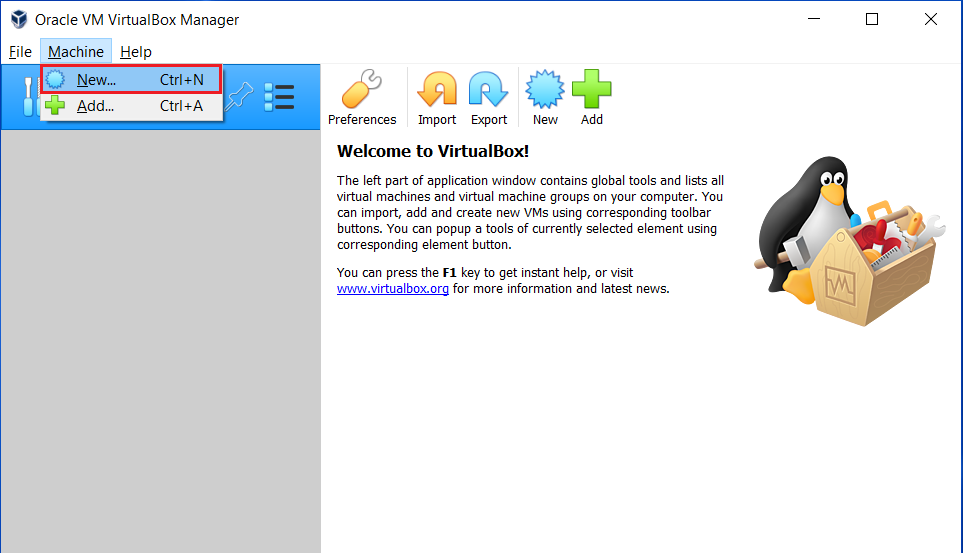
Chọn thẻ DHCP Server và thiết lập các thông số



Nhấp nút Apply và Close để hoàn tất.

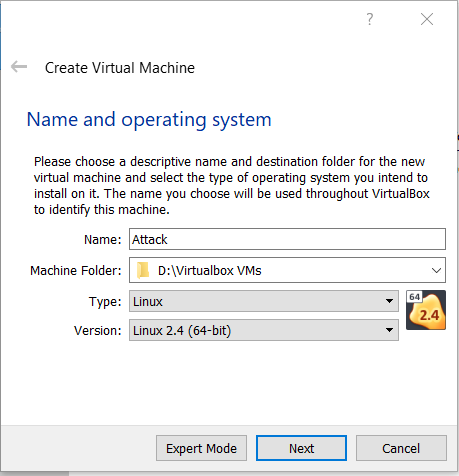
**Cài Attack**

Trên cửa sổ chính của Virtualbox, chọn Machine 🡪 New...

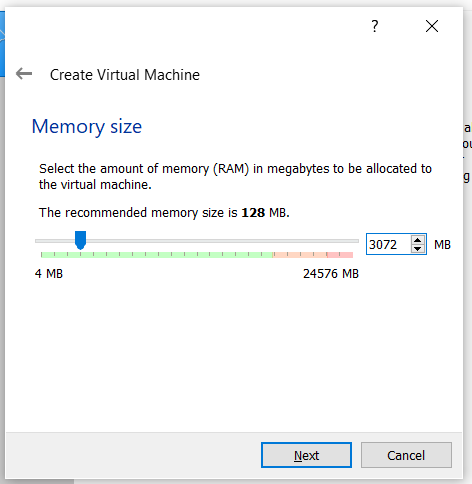


Trên cửa sổ tạo máy ảo, đặt các thông số như sau. Sau đó nhấn Next.

* Name: Tên máy ảo
* Machine Folder: Thư mục chứa máy ảo
* Type: Linux
* Version: Ubuntu (64-bit)

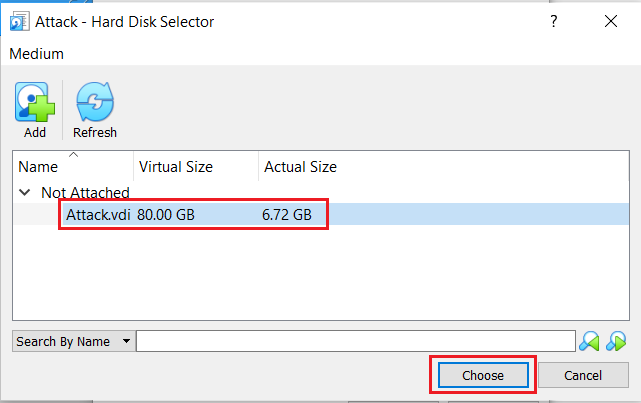


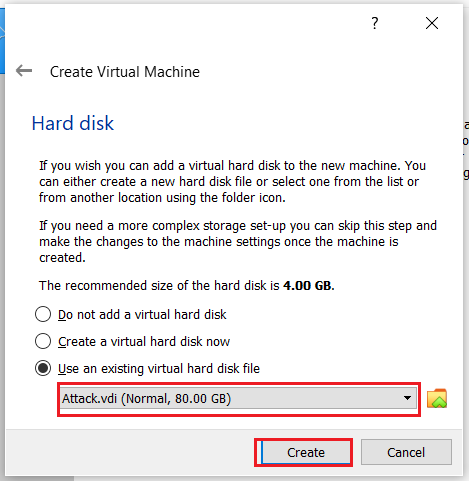
Chọn dung lượng bộ nhớ RAM cho máy ảo là 2048 MB. Nhấn Next để tiếp tục.



Trong cửa sổ tạo ổ cứng máy ảo, chọn mục Use an existing virtual hard disk file. Sau

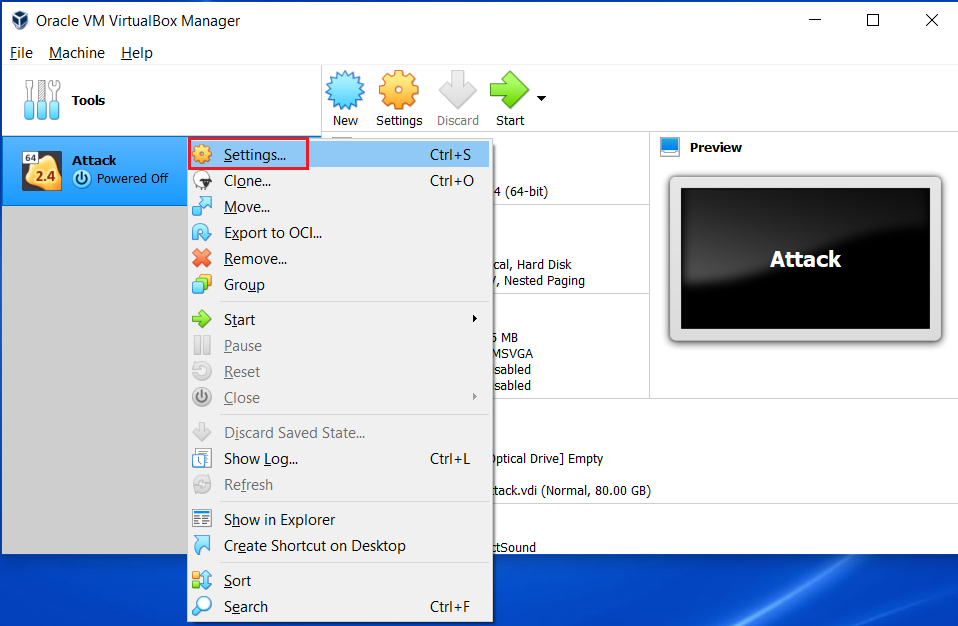
đó bấm nút Choose a virtual hard disk file...





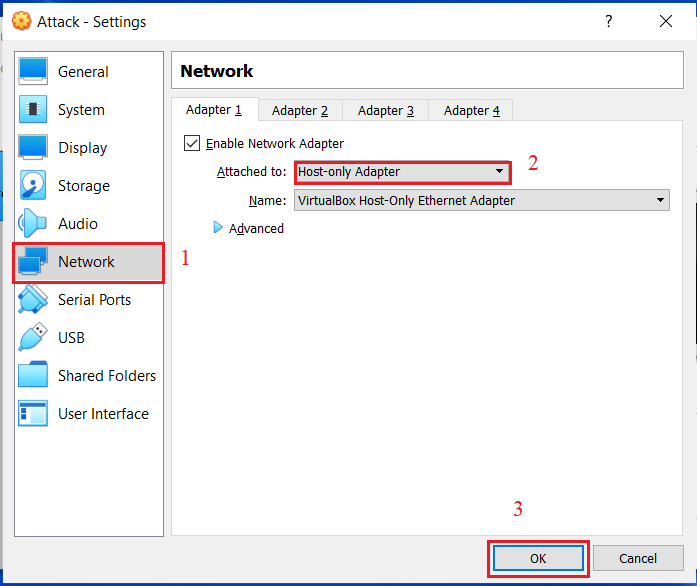
Trên cửa sổ chính của Virtualbox, chọn máy ảo vừa tạo và nhấp chuột phải. Chọn

Settings...



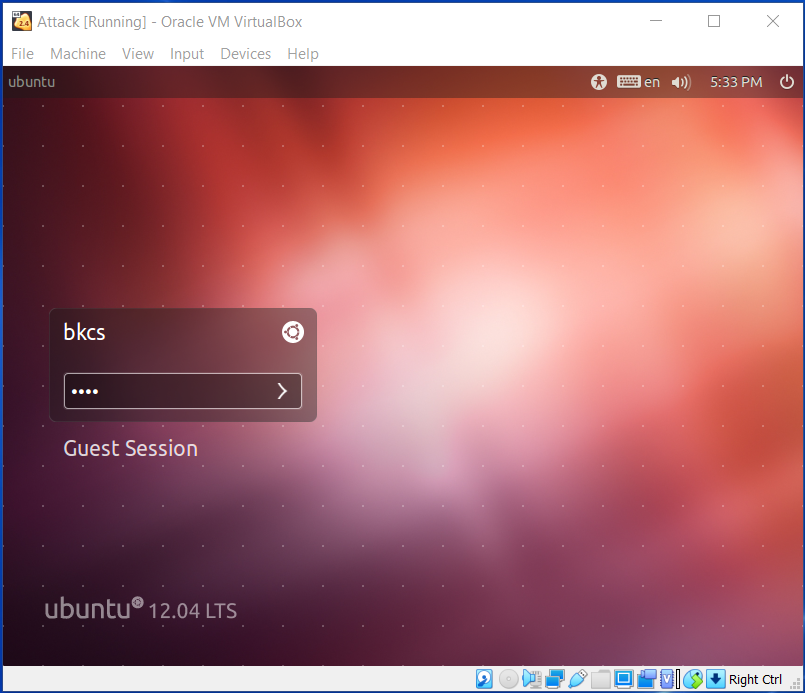
Chọn Network 🡪 Adapter 1. Thiết lập các thông số như sau:

* Attached to: Host-only Adapter
* Name: VirtualBox Host-Only Ethernet Adapter (hoặc còn gọi là VirtualBox Host-Only
* Network)



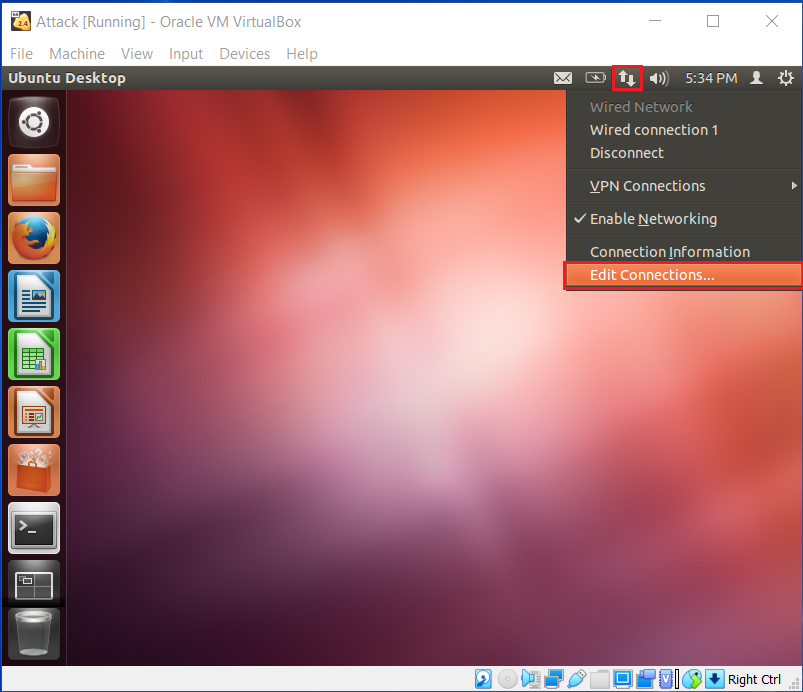
Sau khi máy ảo khởi động xong, đăng nhập bằng tài khoản sau:

* Username: bkcs
* Password: bkcs

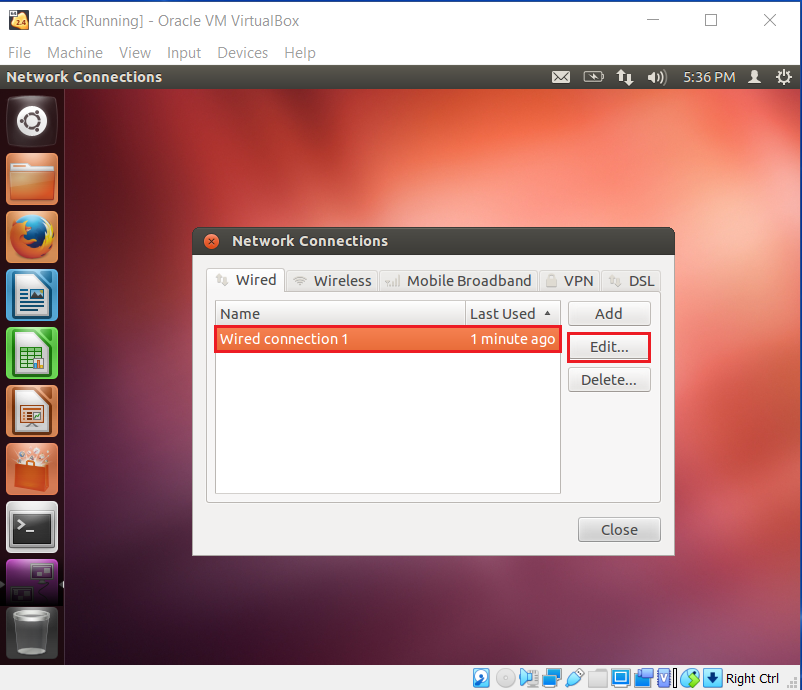


Trên màn hình máy ảo lựa chọn nhất chuột phải vào biểu tượng kết nối mạng và

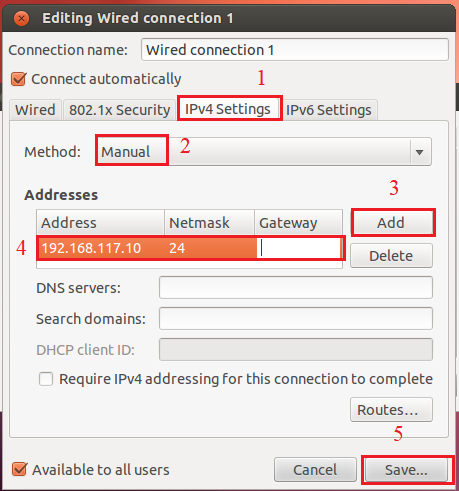
chọn Edit Connections...



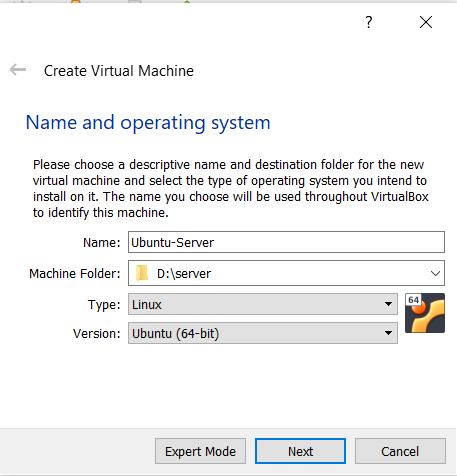
Chọn cạc mạng Wired connection 1 và nhấn Edit...

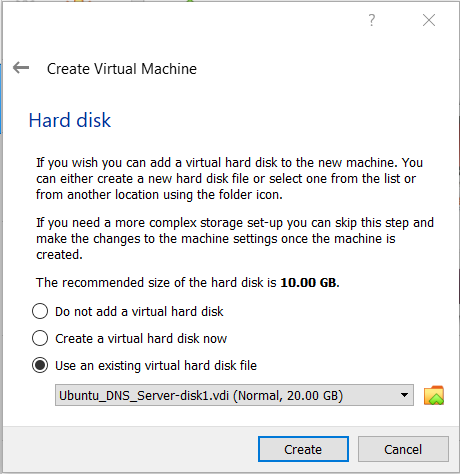


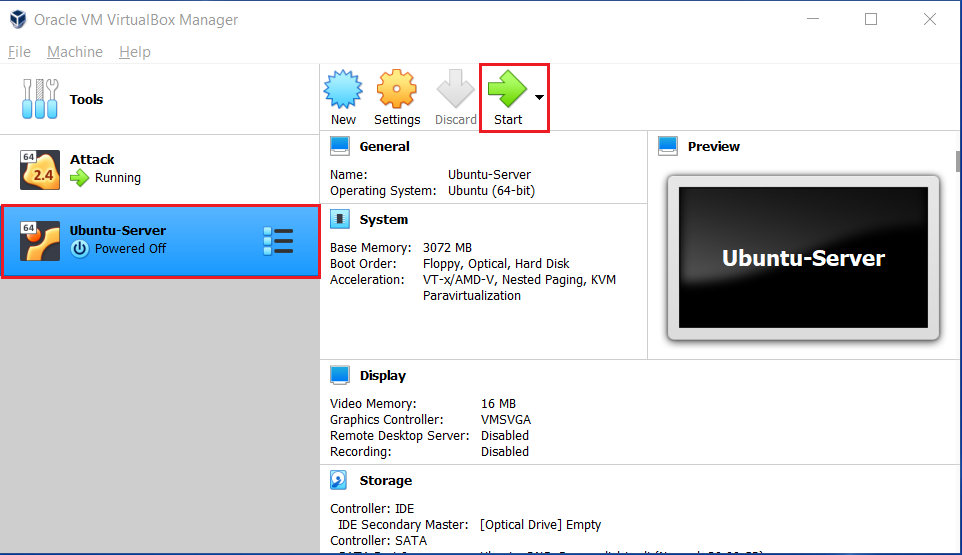
* Chọn thẻ IPv4 Settings và chọn Method là Manual
* Nhấn nút Add và thiết lập các thông số địa chỉ IP cho cạc mạng
* Nhấn nút Save để hoàn tất



**Tương tự cài đặt Attack, ta cài đặt Ubuntu-server**

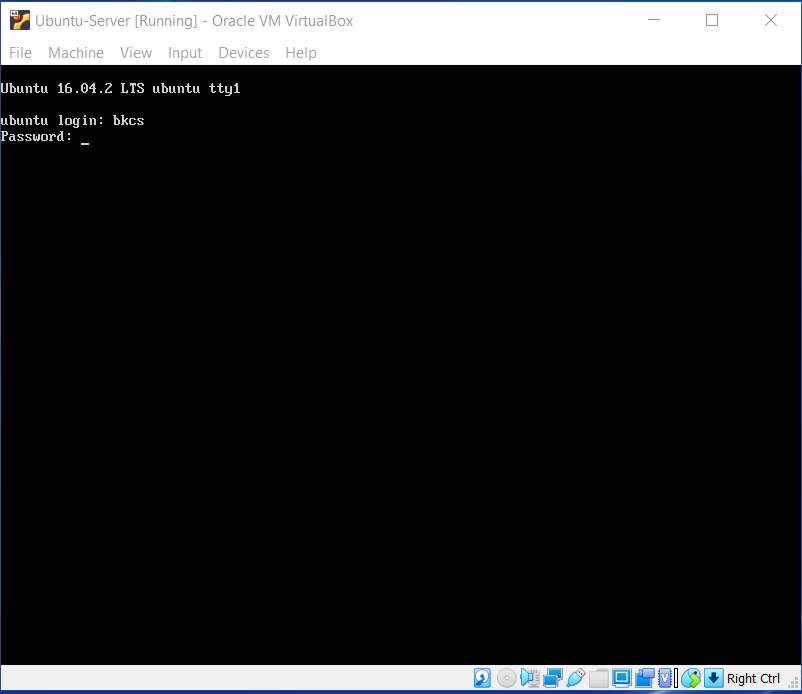






Khởi động máy ảo và đăng nhập với tài khoản:

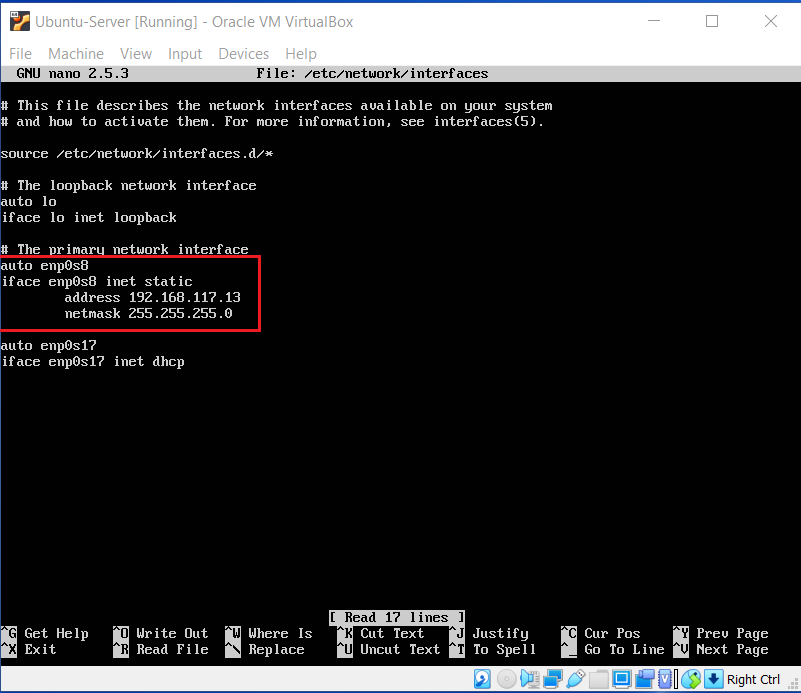
* Username: bkcs
* Password: bkcs



Mở cửa sổ Terminal và thực hiện lệnh sudo **nano /etc/network/interfaces**



Thiết lập thông số địa chỉ IP cho cạc mạng



**Phần 2: Thực hành phân tích các kỹ thuật do thám hệ thống**

* **Quét thăm dò mạng**

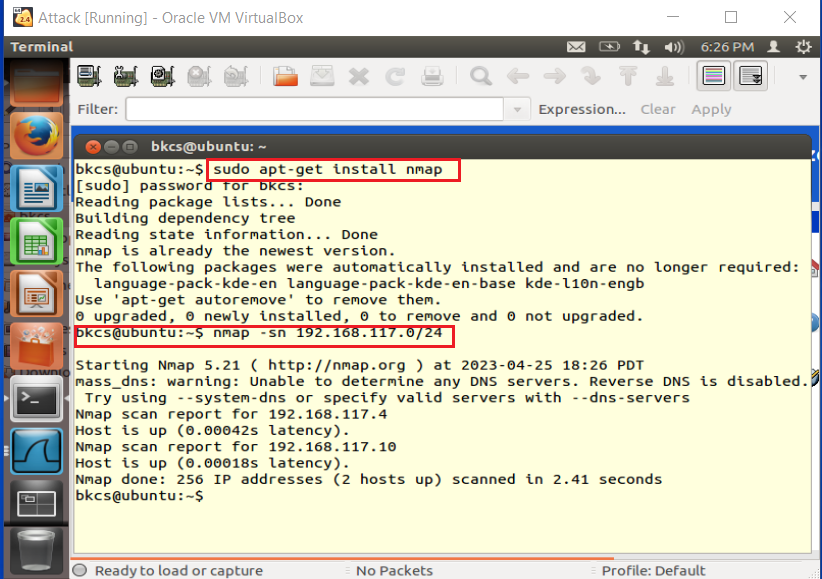
- Bước 1: Truy cập máy ảo Attack

- 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:



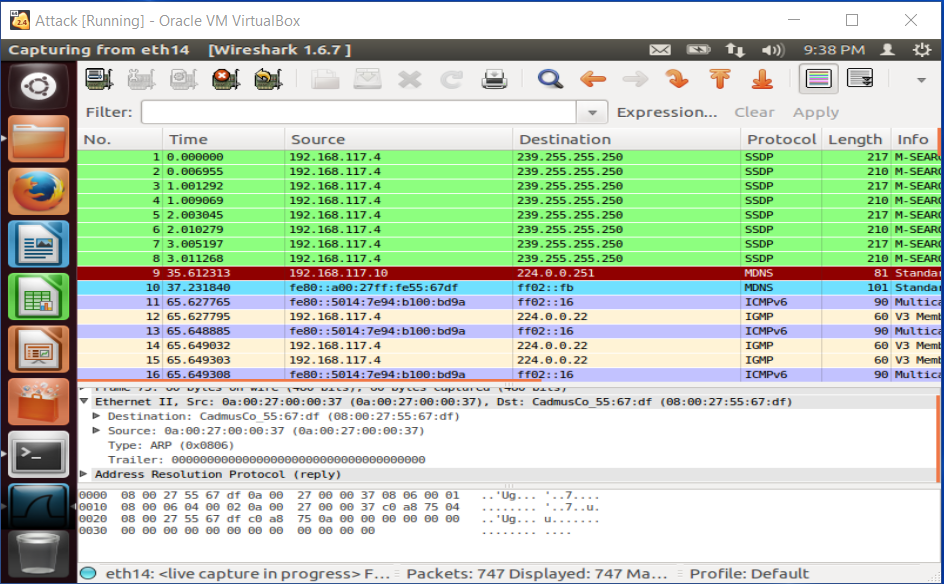
Ở màn hình Wireshark ta sẽ thấy các gói tin

Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 1 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.4

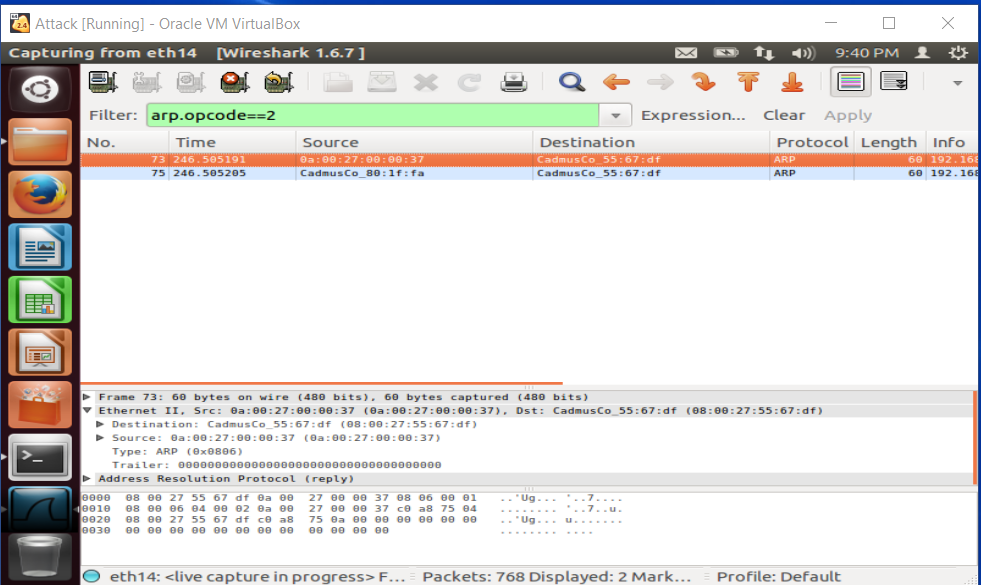
- Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

- Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. 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



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 đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.



* **Quét thăm dò dịch vụ**

Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

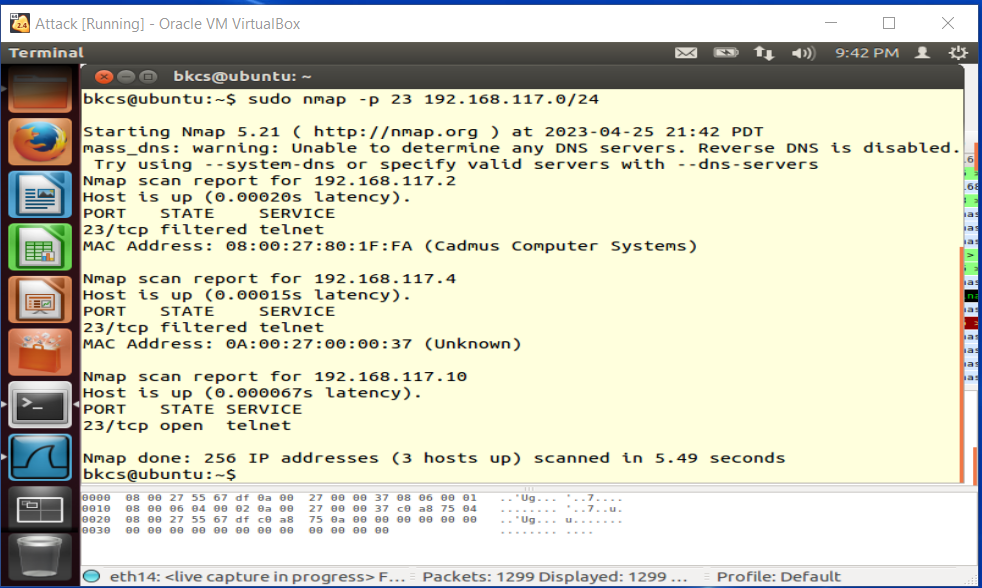
- Bước 1: Truy cập máy ảo Attack

- 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 192.168.117.4 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.

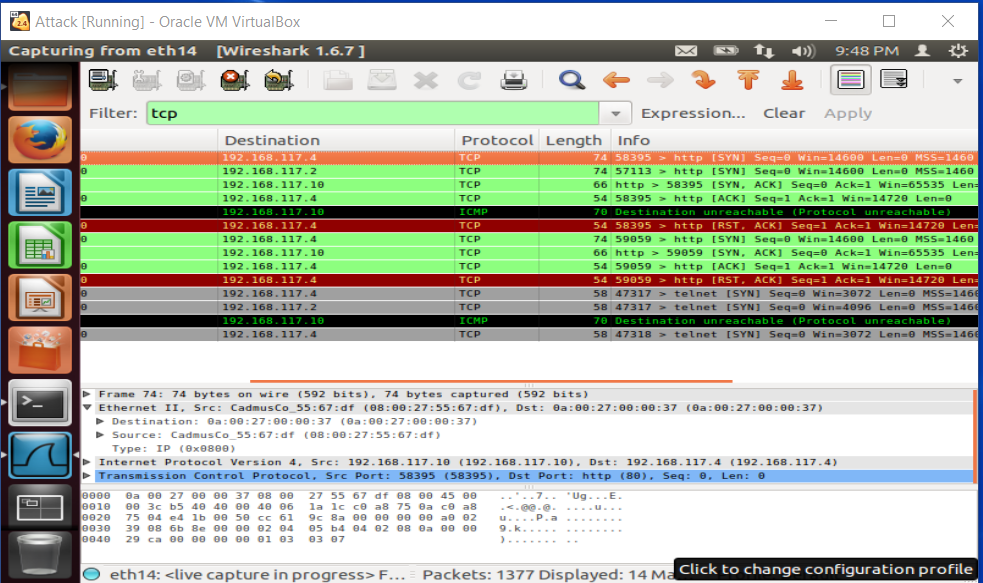


Phân tích lưu lượng:

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.



Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.117.4 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)



* **Quét cổng dịch vụ**

Bước 1: Truy cập máy ảo Attack

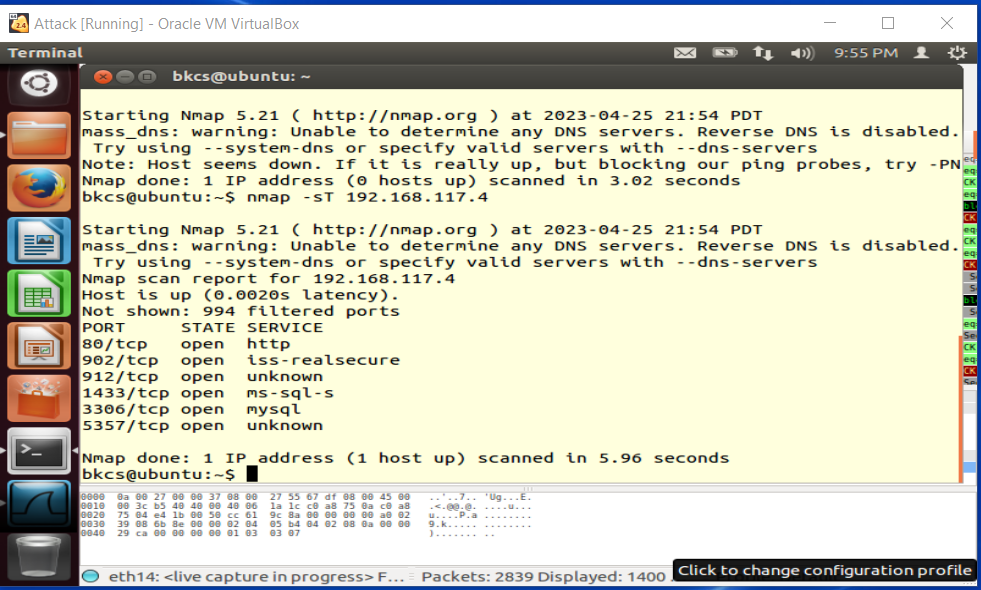
- Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

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

**nmap -sT 192.168.117.4**

Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 80, 902, 912, 1433, 3306, 5357 trên máy mục tiêu 192.168.117.4 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và

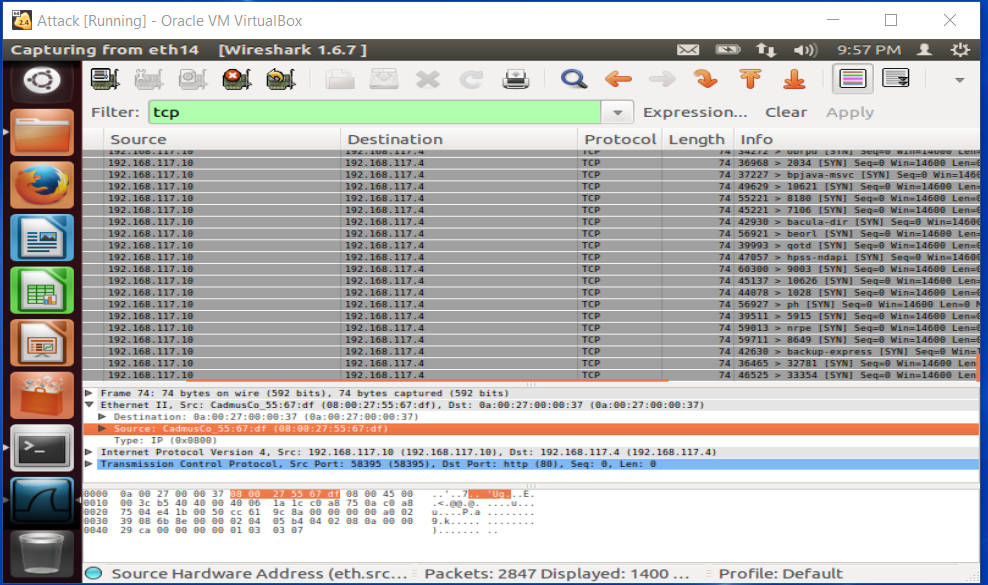
dns.



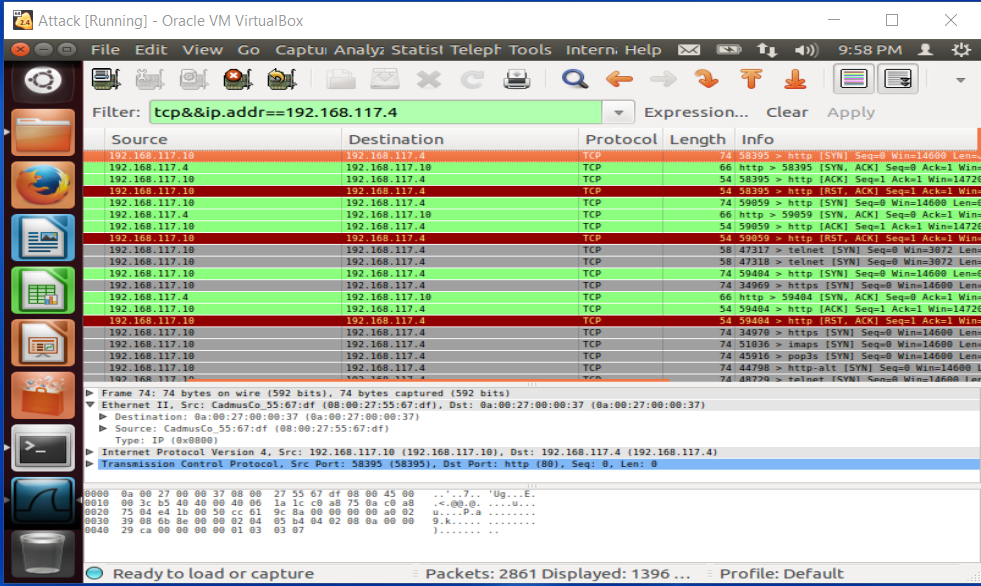
Bước 5: Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.4 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.4. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



Sử dụng giá trị tcp && ip.addr == 192.168.117.4 ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 55984 đã được thiết lập (các gói tin 12, 16, 17 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin 30) để hủy kết nối này.



Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 22, 23. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan