0850080085 – Văn Trung Nghĩa – 08\_CNPM

**LAB THỰC HÀNH TUẦN 1**

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

**MỤC LỤC**

[I. HƯỚNG DẪN THIẾT LẬP MÔI TRƯỜNG ẢO HÓA TRÊN VIRTUAL BOX 1](#_Toc133431017)

[1. Cài đặt và cấu hình Virtualbox 2](#_Toc133431018)

[2. Triển khai máy ảo Attack 5](#_Toc133431019)

[3. Triển khai máy ảo Server 12](#_Toc133431020)

[II. LUYỆN TẬP 13](#_Toc133431021)

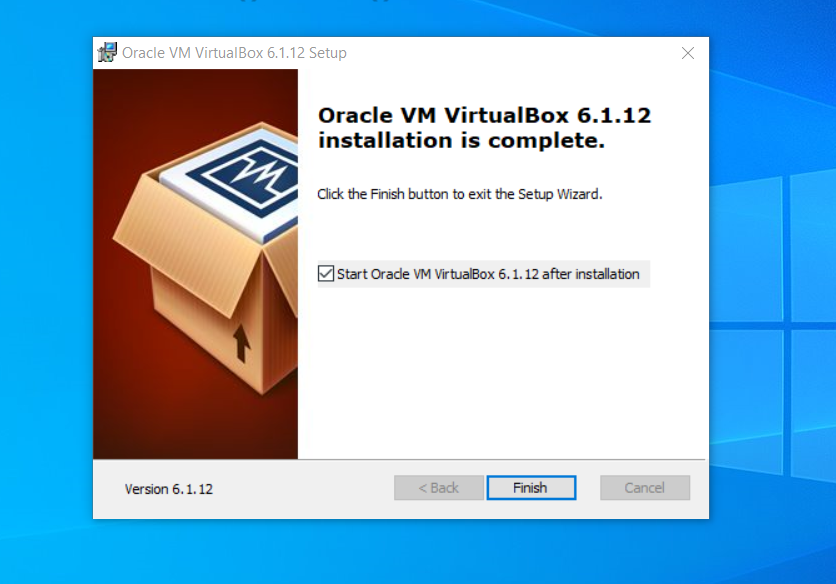
[1. Quét thăm dò mạng 13](#_Toc133431022)

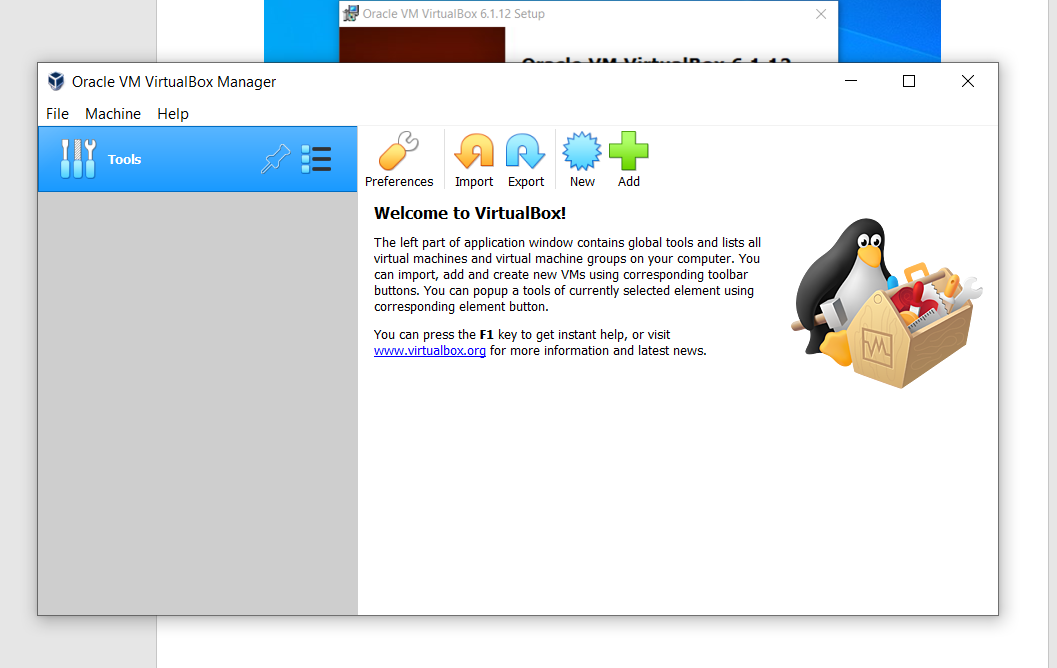
[2. Quét thăm dò dịch vụ 15](#_Toc133431023)

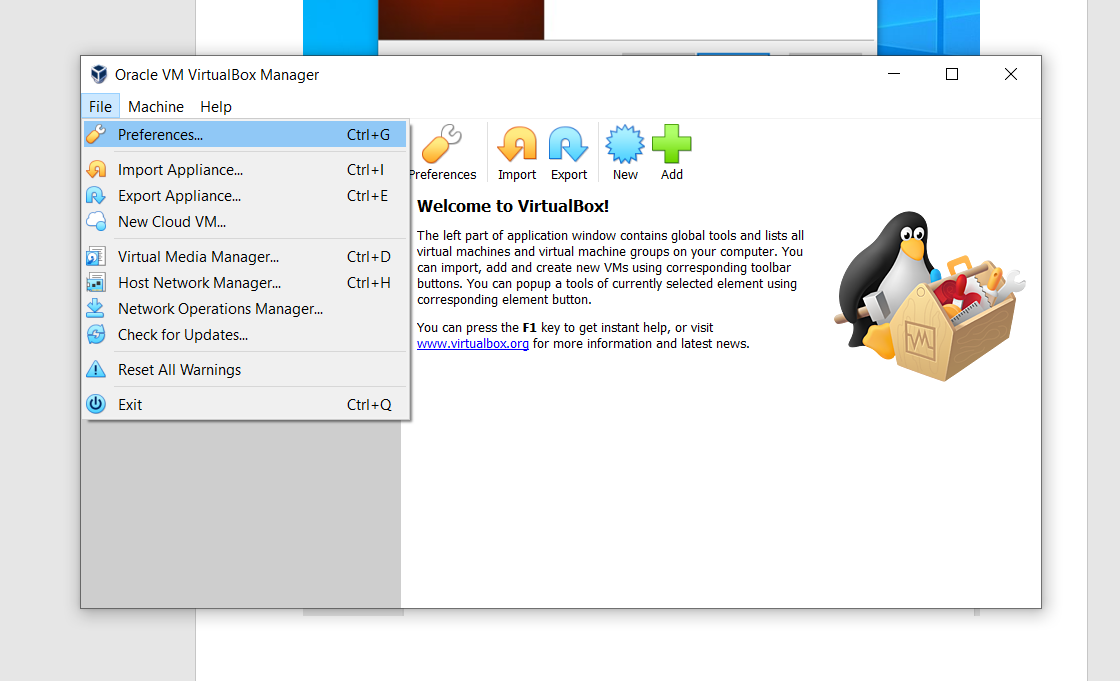
[3. Quét cổng dịch vụ 18](#_Toc133431024)

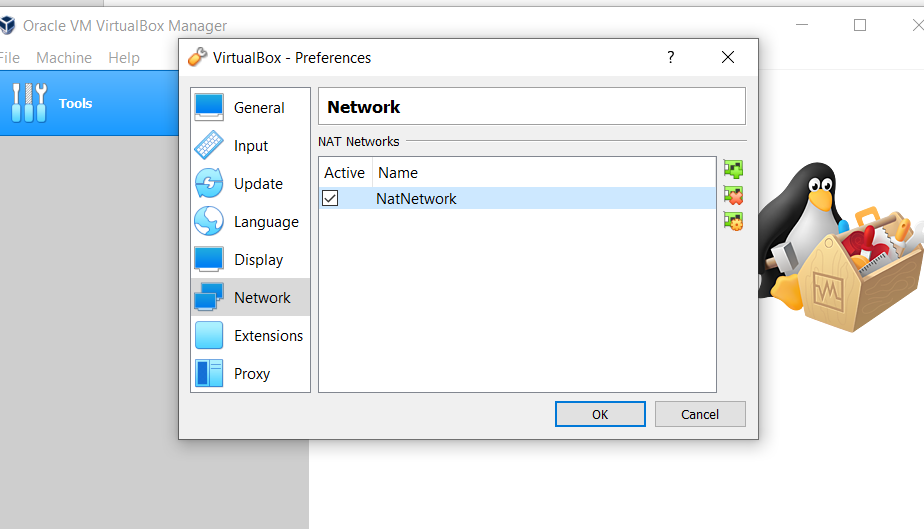
[4. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap 19](#_Toc133431025)

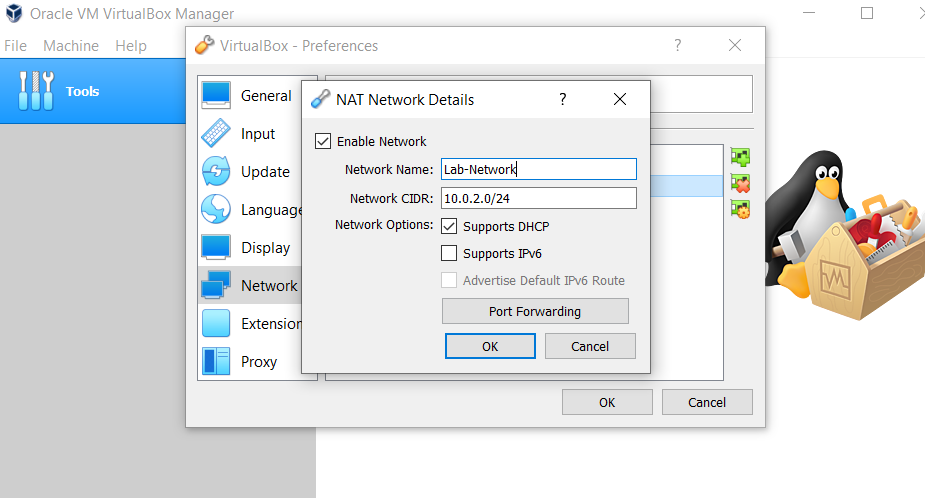
1. HƯỚNG DẪN THIẾT LẬP MÔI TRƯỜNG ẢO HÓA TRÊN VIRTUAL BOX
   1. Cài đặt và cấu hình Virtualbox

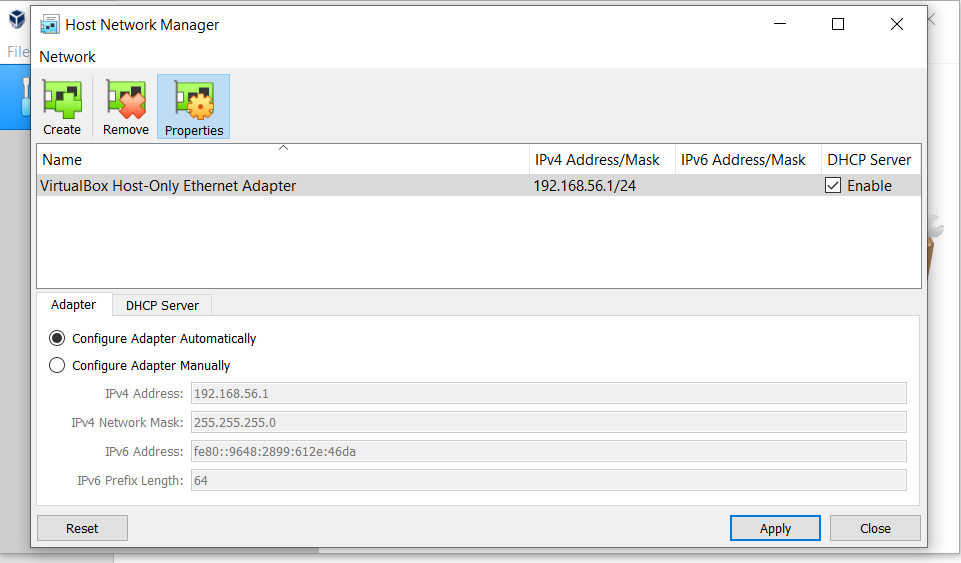


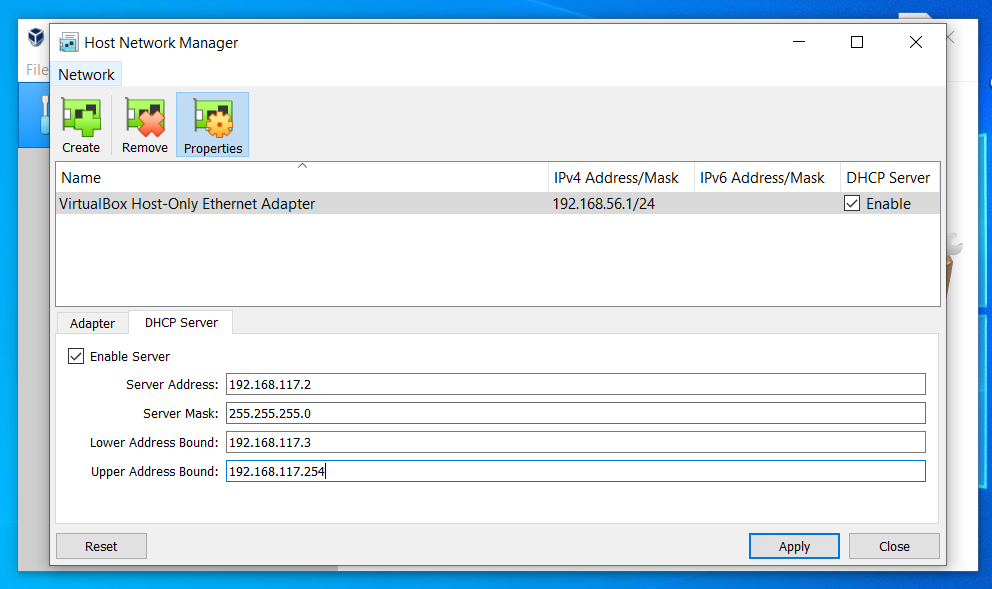




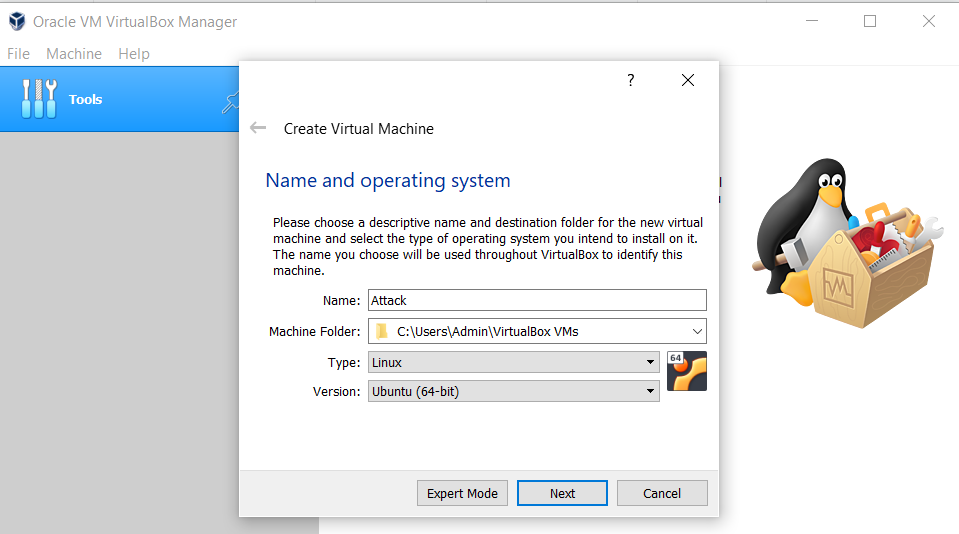


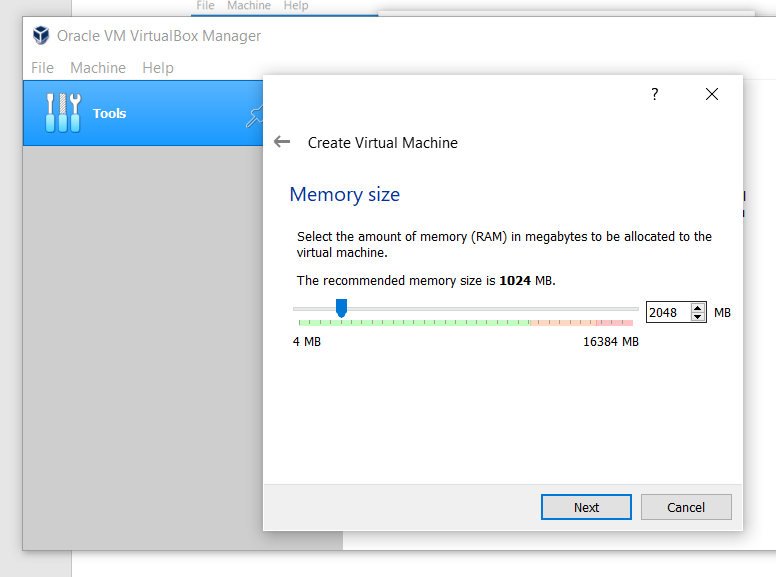


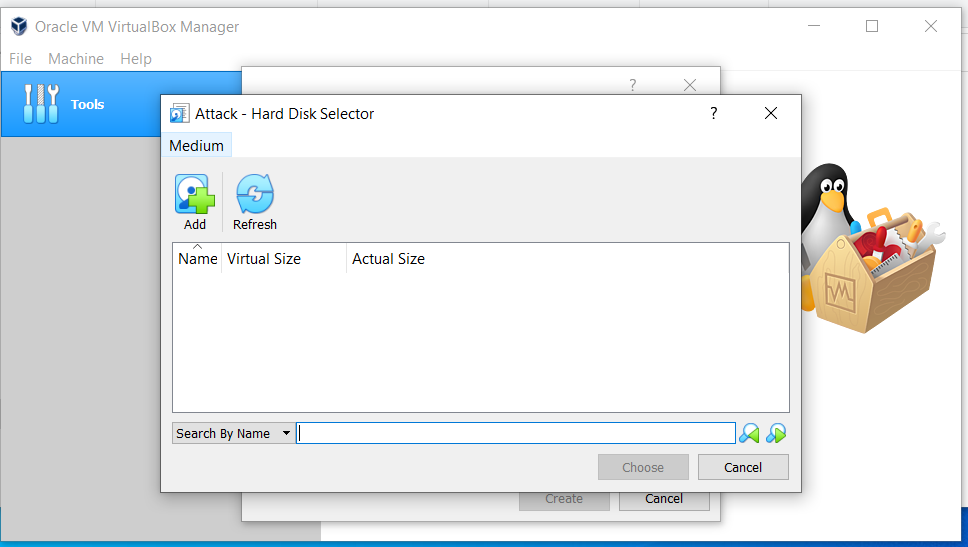


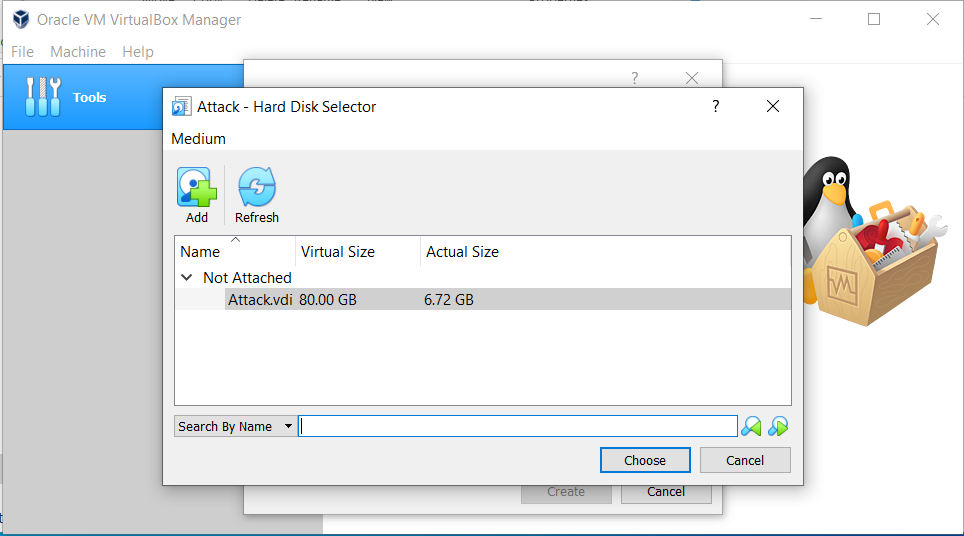


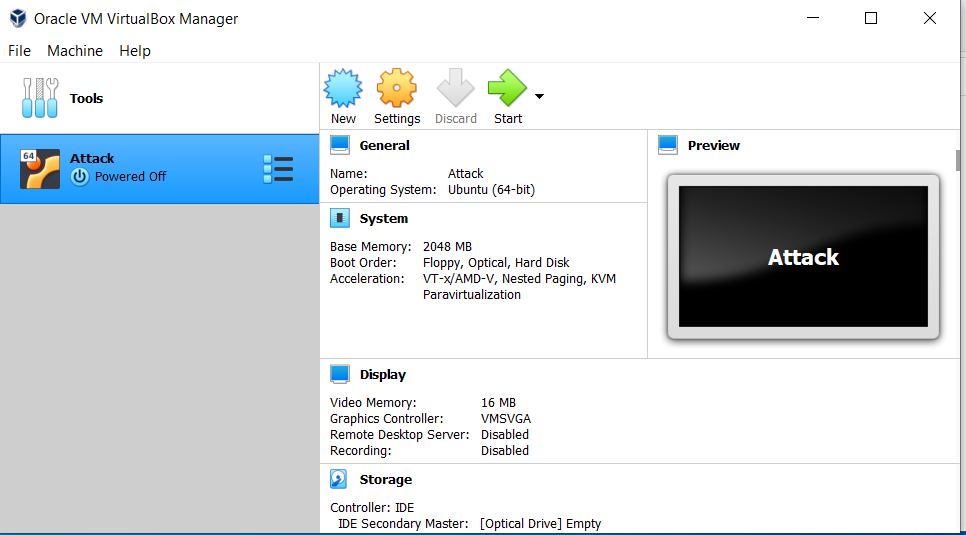
* 1. Triển khai máy ảo Attack

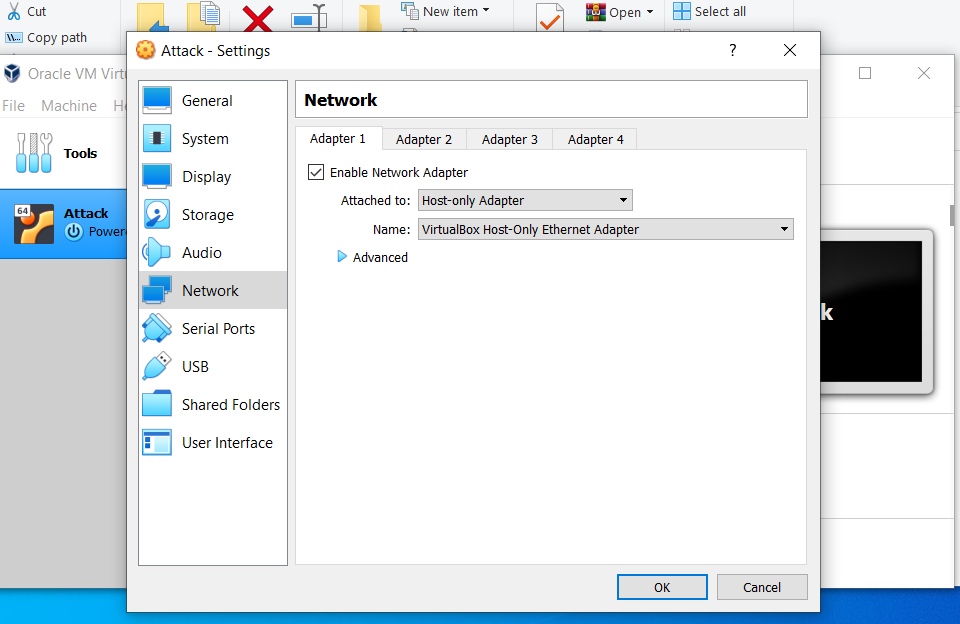


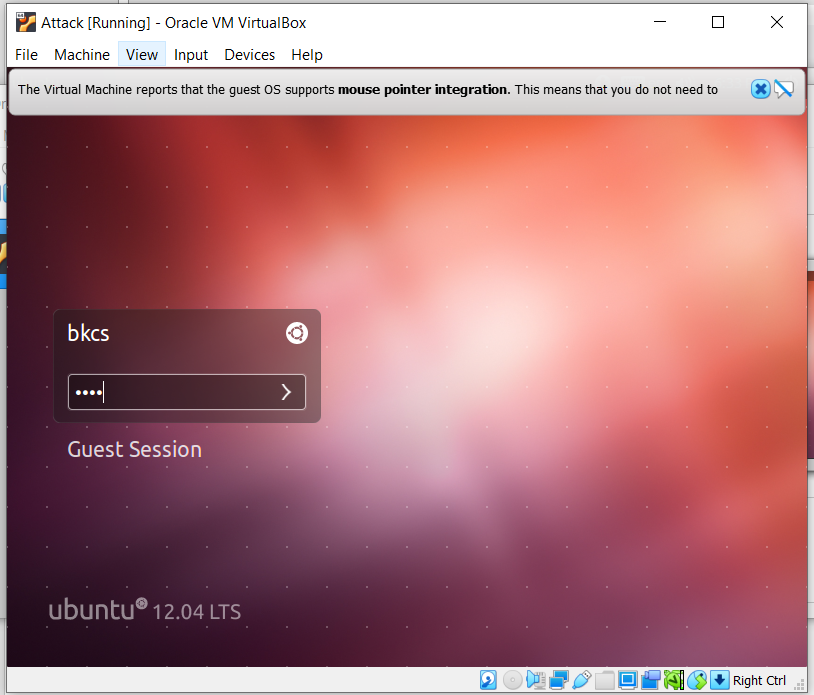


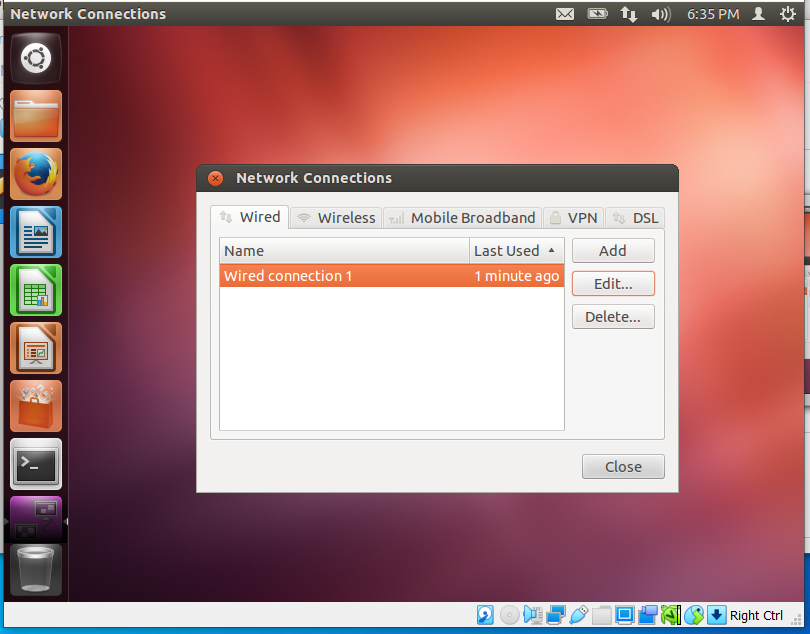


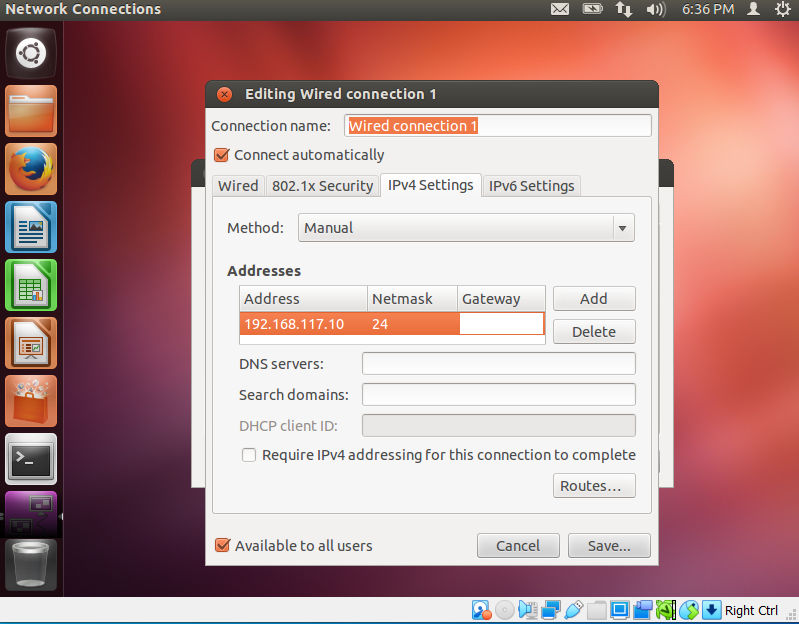


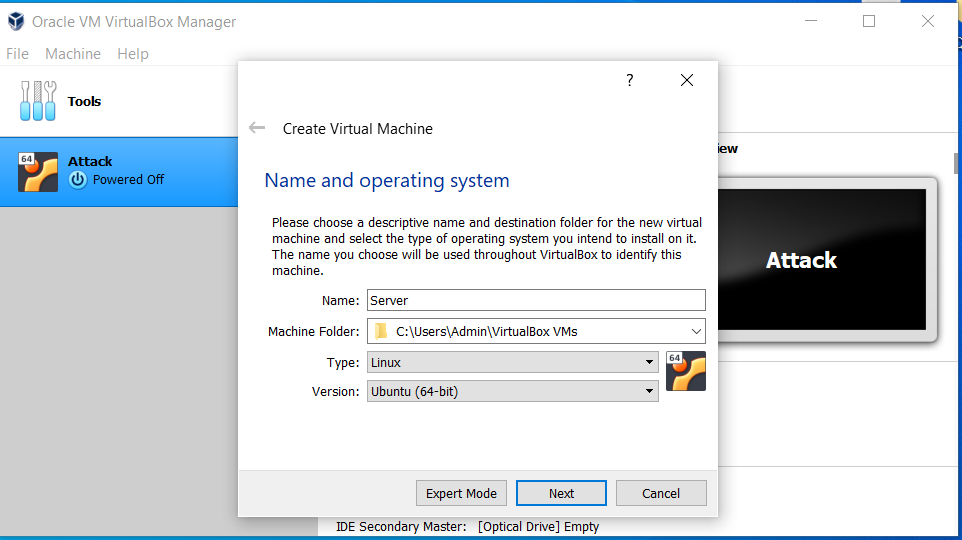


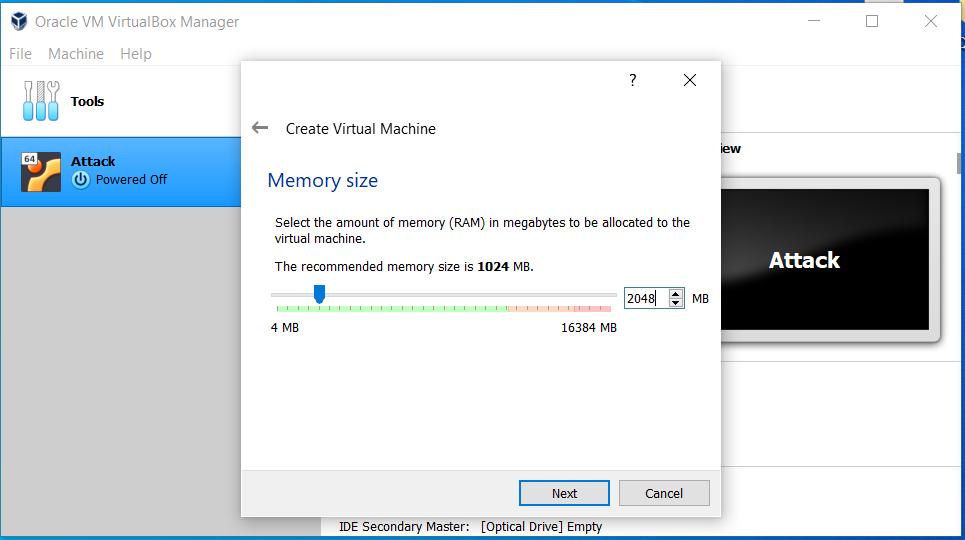


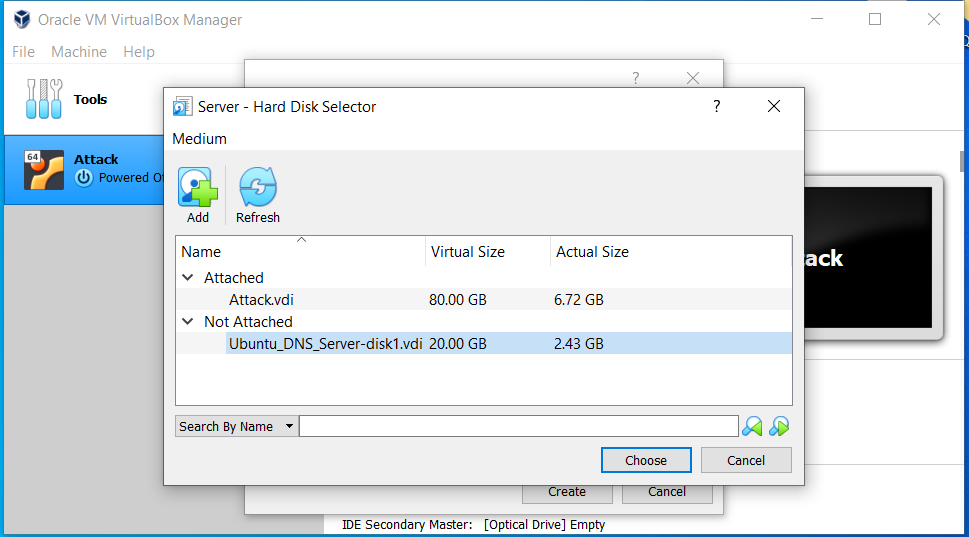


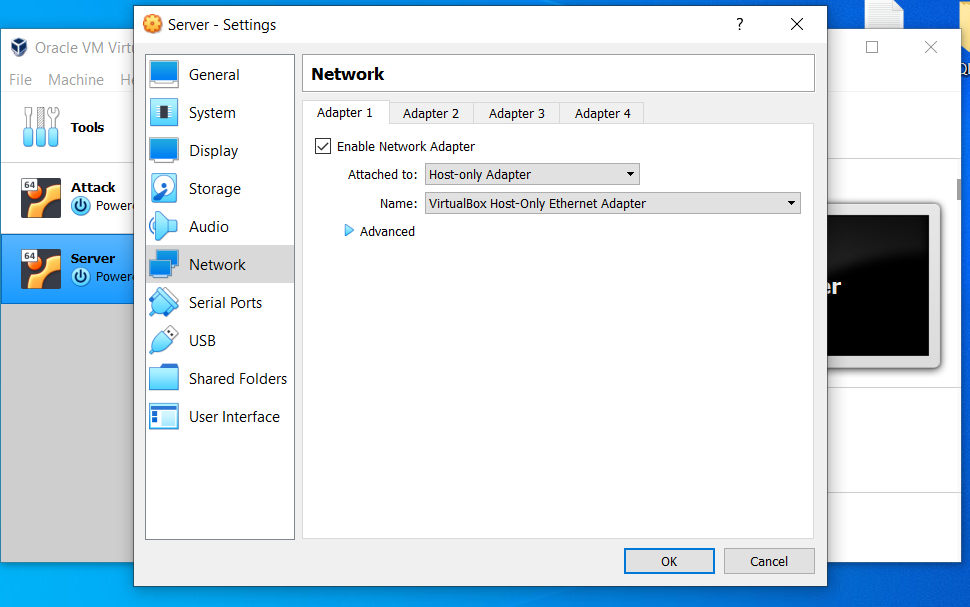




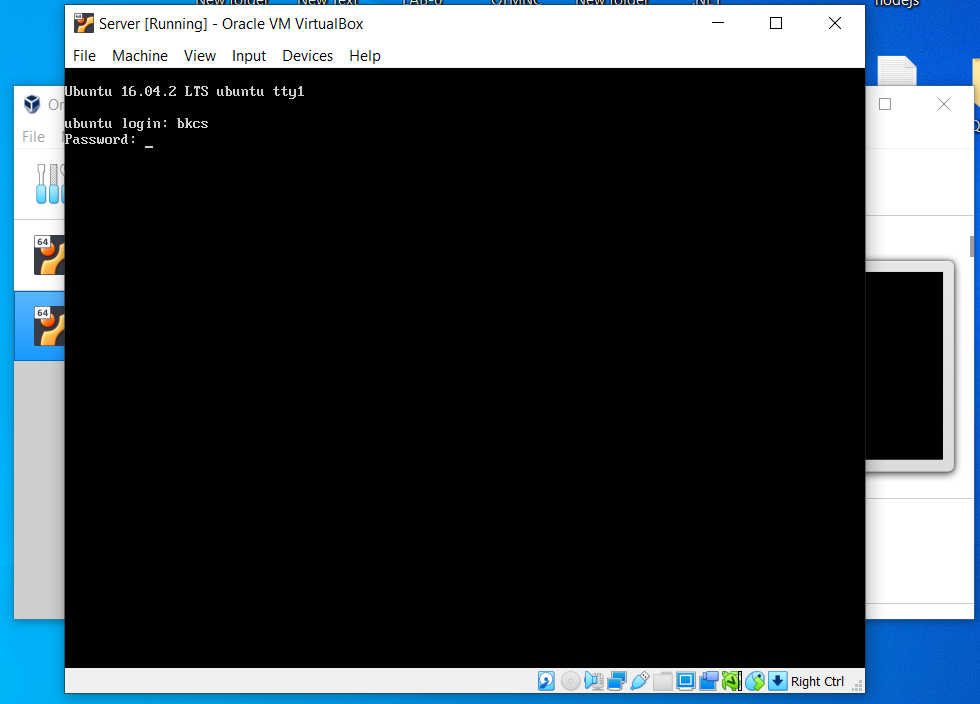


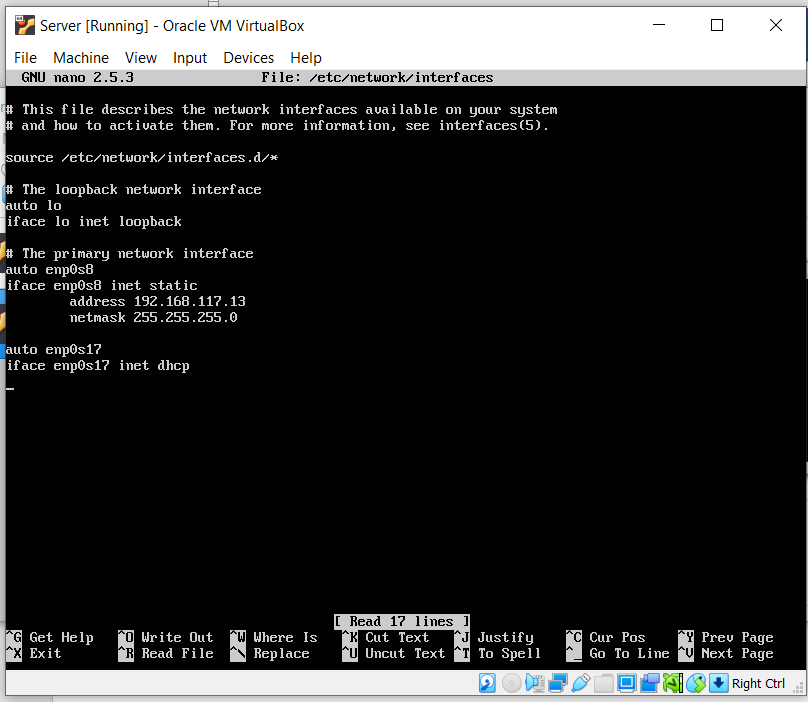




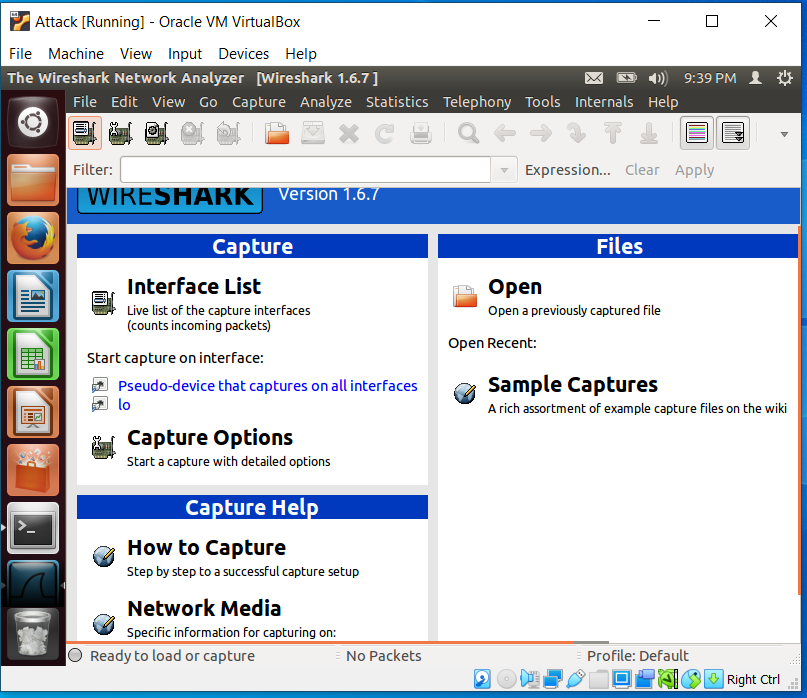


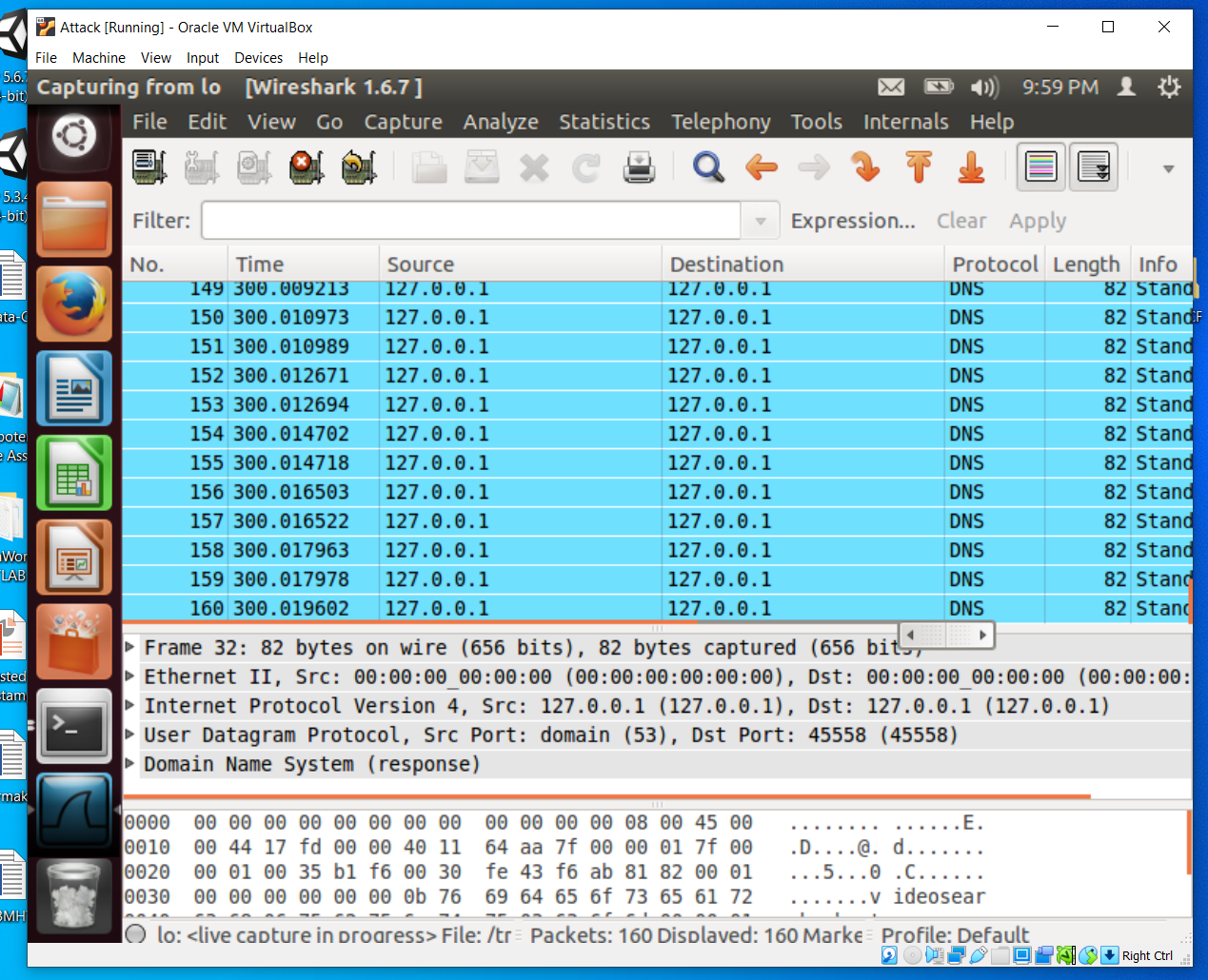
* 1. Triển khai máy ảo Server

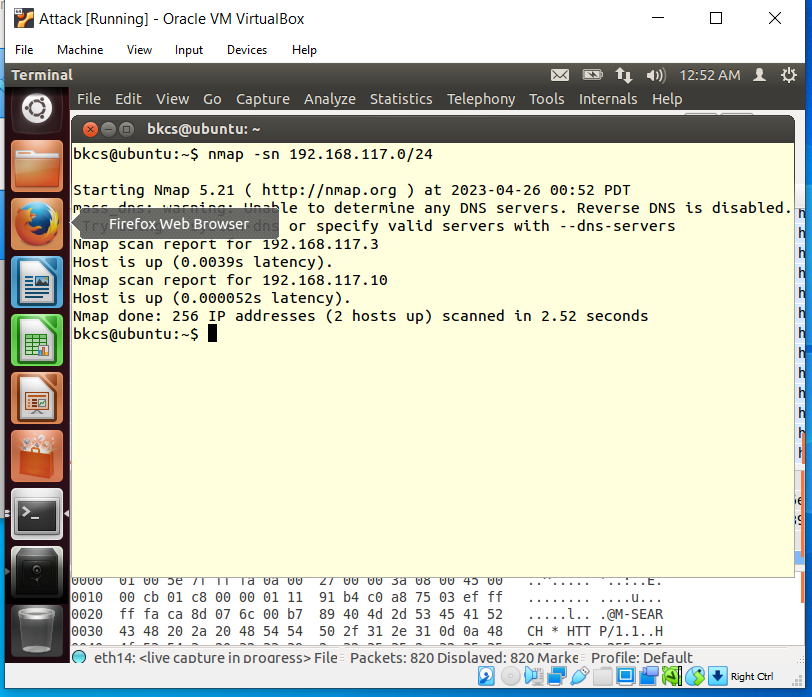




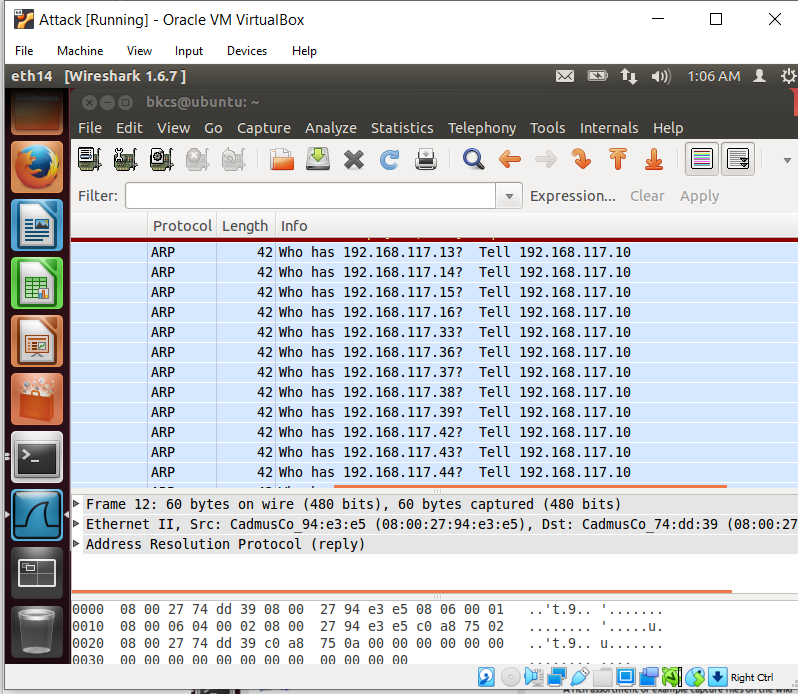
1. LUYỆN TẬP
   1. Quét thăm dò mạng





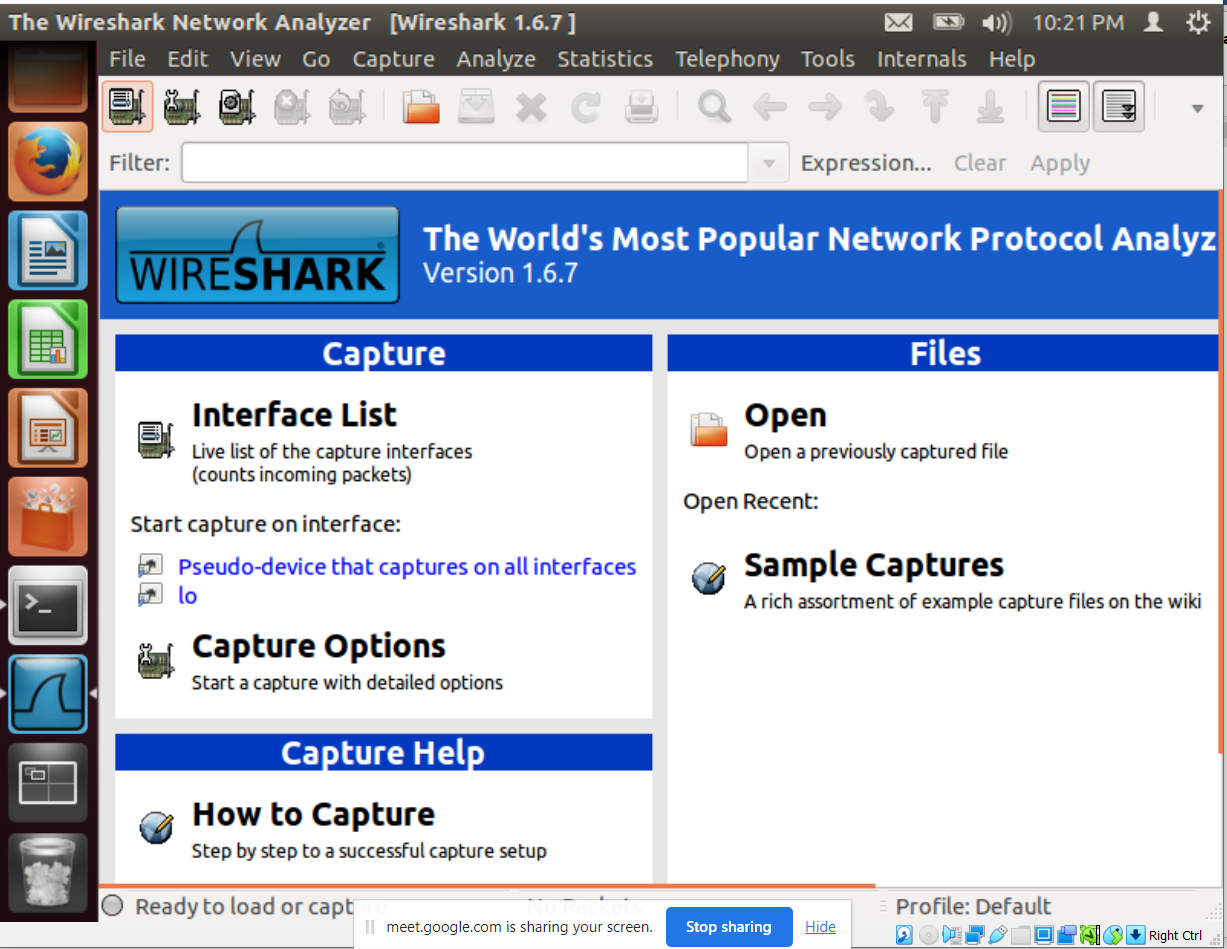


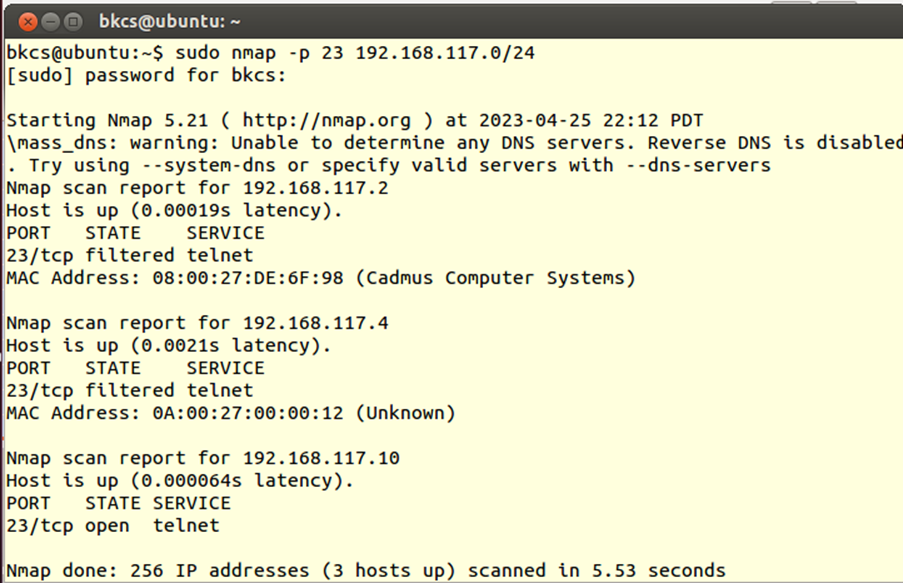
Phân tích lưu lượng

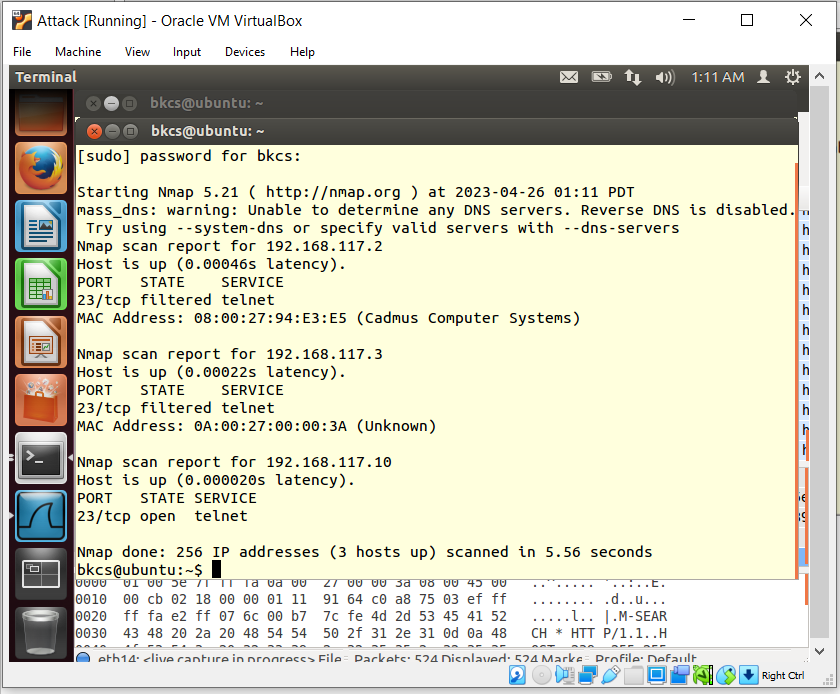




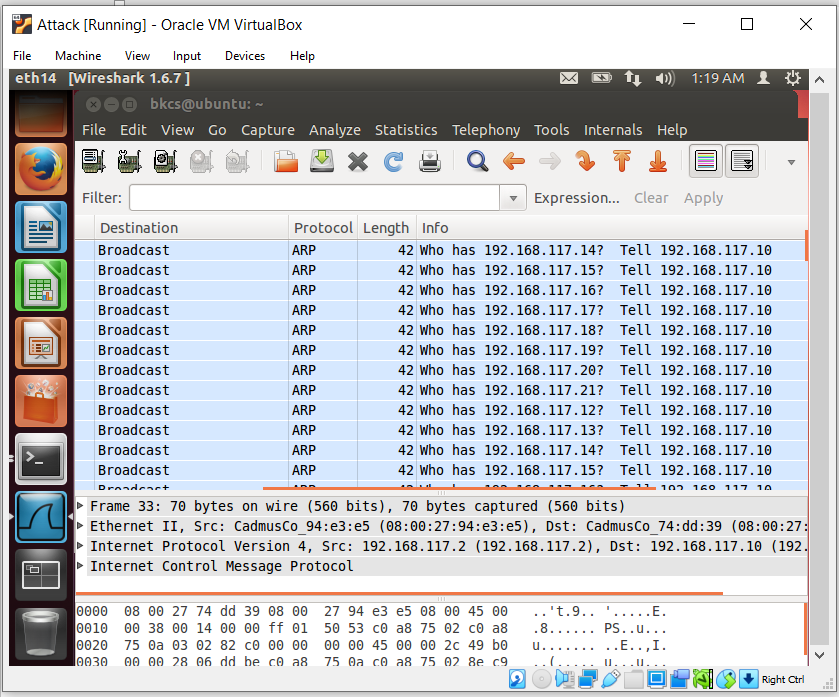
* 1. Quét thăm dò dịch vụ

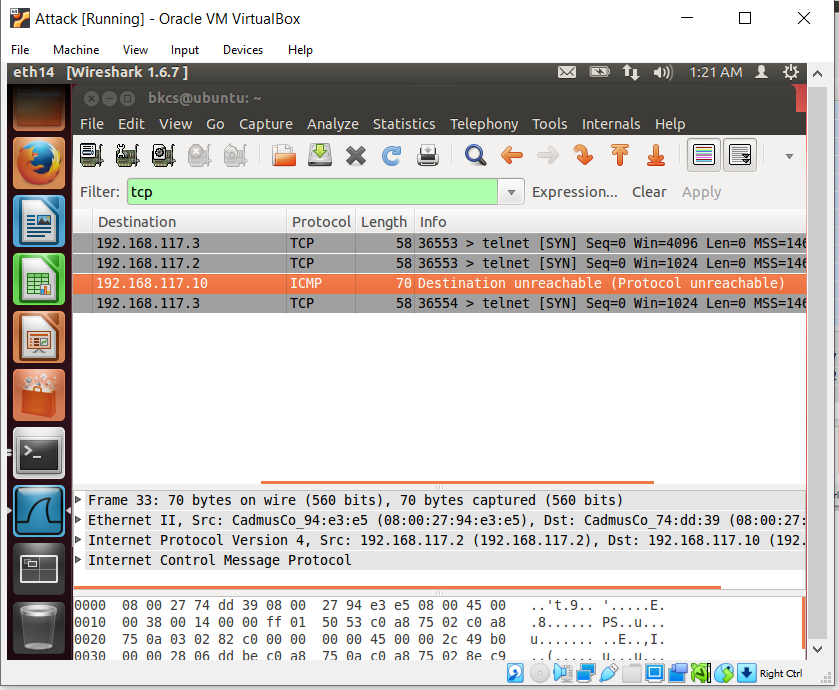




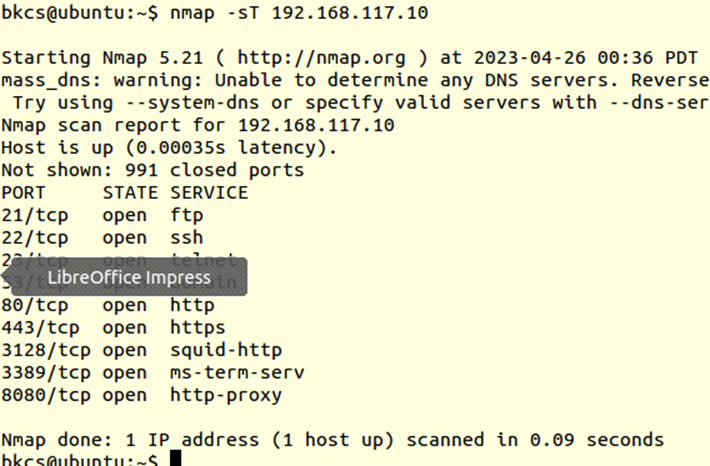


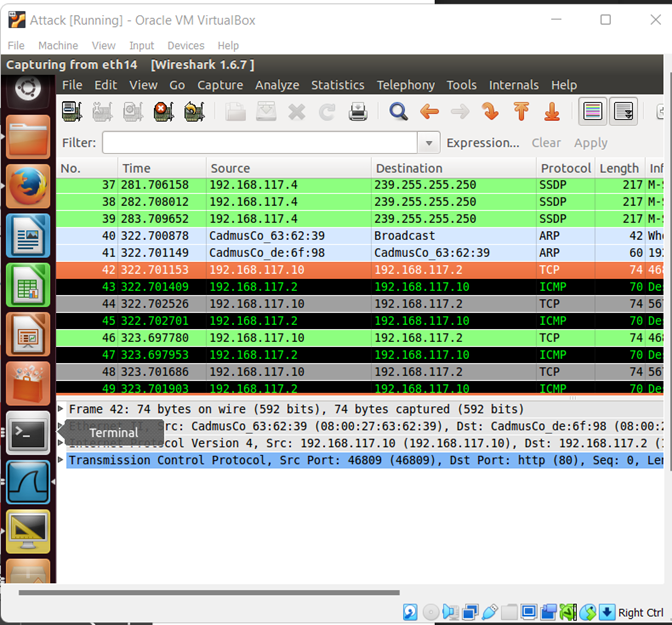
Phân tích lưu lượng





* 1. Quét cổng dịch vụ







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

**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).

**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

**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.