**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



Học phần: **Kỹ thuật xâm nhập**

Thực hành:

**Bài Thực hành số 1**

**Giảng viên hướng dẫn**: Nguyễn Ngọc Diệp

**Sinh viên thực hiện:**

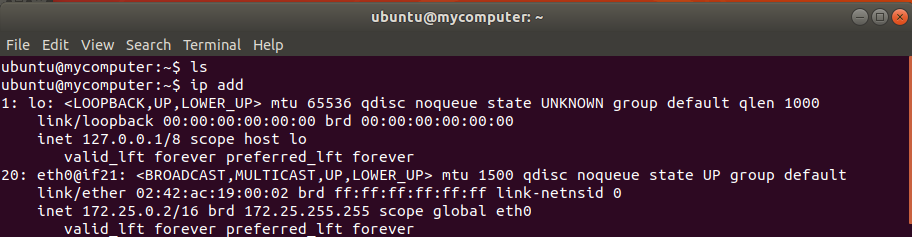
Đỗ Quang Huy B18DCAT106

Hà Nội 2022

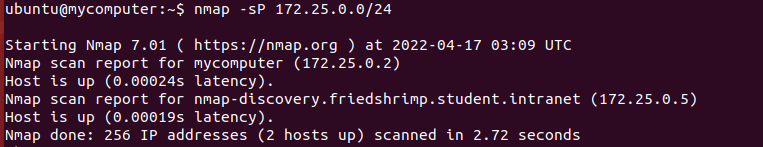
Bài 1 : Nmap – discovery

+ tìm IP bằng lệnh

#ip add

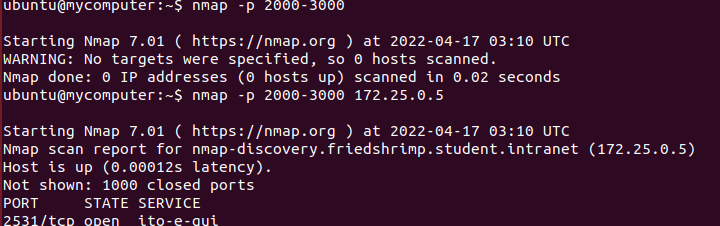


+ Tìm địa chỉ máy cùng lớp mạng



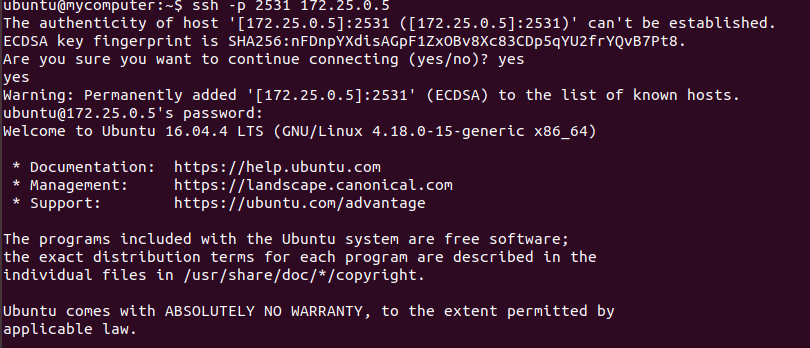
* địa chỉ ip máy đối tượng là 172.25.0.5

+ Tìm port dịch vụ mở ở máy đối tượng

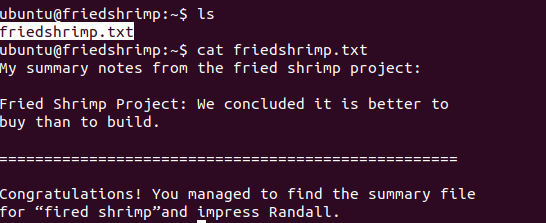


* Port mở là 2531

+ Mở dịch vụ ssh ở máy nạn nhân



+ check file txt và mở nó lên và hoàn thành bài lab

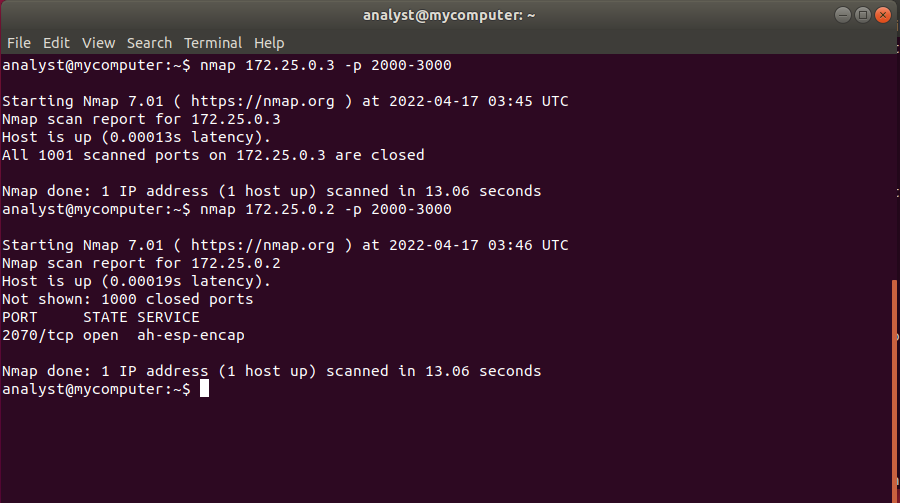


Bài 2 : Nmap-ssh

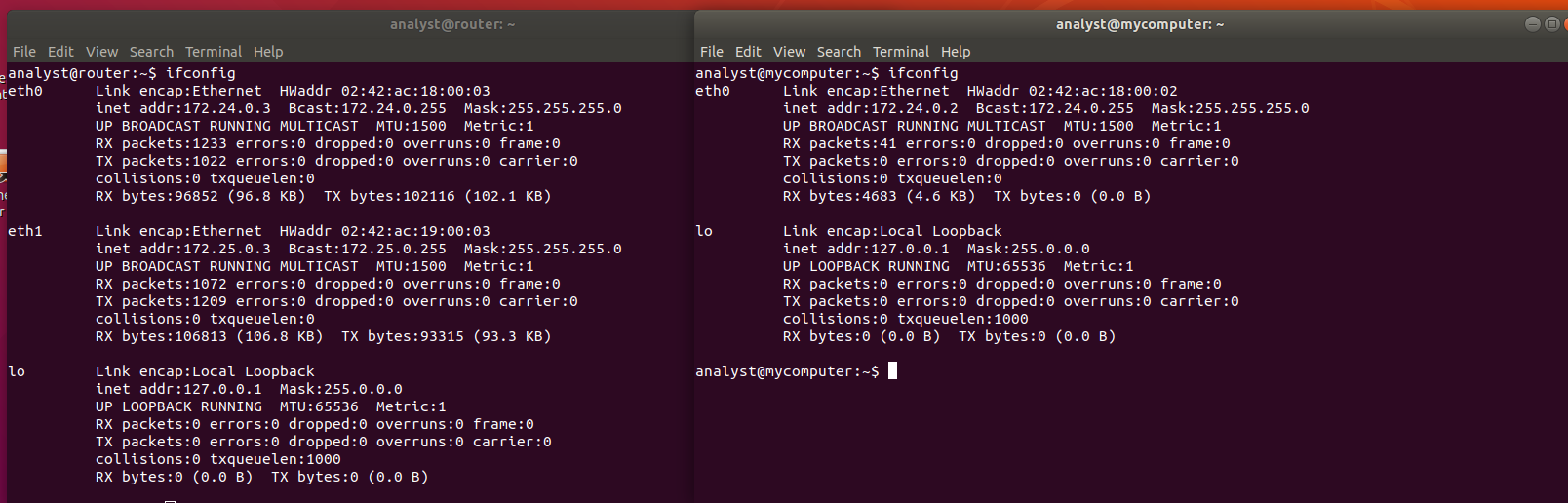
+ Cổng SSH trong máy tính cá nhân là : 2070.

Được biết sau khi sử dụng nmap

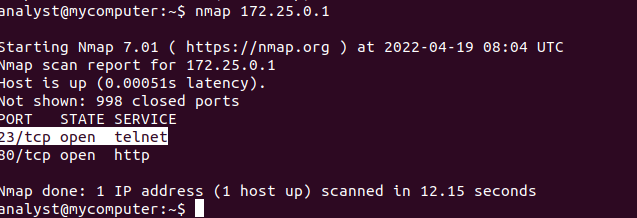
và kết nối ssh với router đang bị đóng



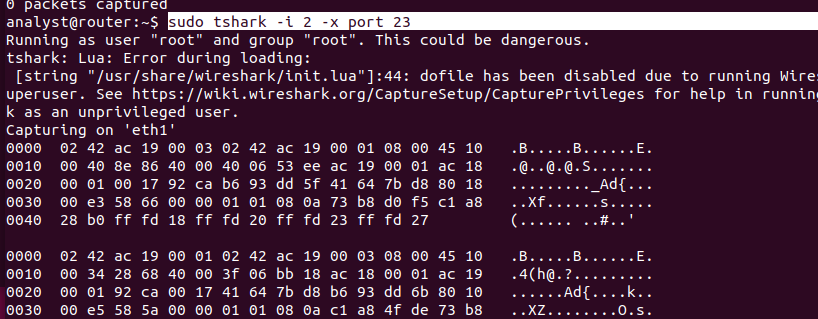
Địa chỉ ip của các máy thành phần



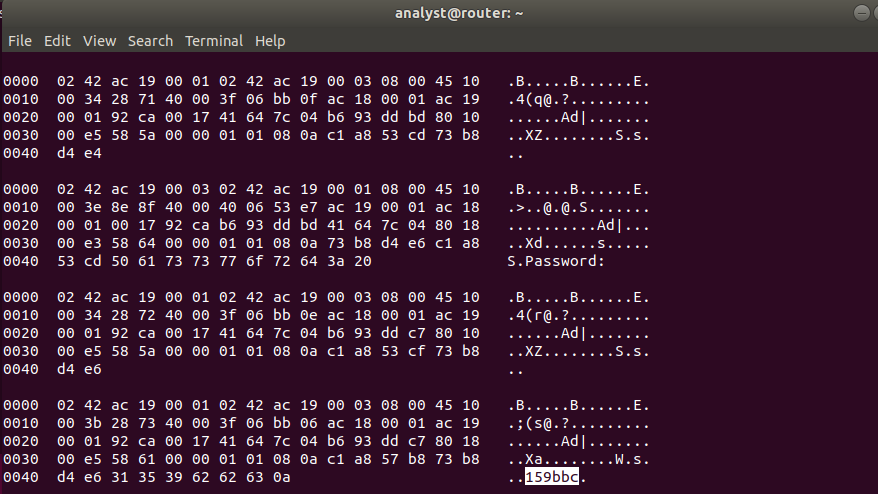
Sau khi biết cùng lớp mạng của máy 172.25.0.2 còn 1 máy nữa là .0.1 thì thử tìm xem có gì không



Có mở cổng ssh từ đây ta thực hiện tshark bắt gói tin xem pass word của máy .0.2 là gì dựa trên kết nối của máy trên cổng 23 và kết nối ssh thôi



Và hiện ra pass word



Vậy pass là 159bbc .

Kết nối ssh và hoàn thành bài lab này

