

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI THỰC HÀNH**

**Kiểm thử xâm nhập**

**Phát hiện lỗ hổng sử dụng công cụ rà quét**

**Giảng viên: Đinh Trường Duy**

**Nhóm lớp: 01**

**Sinh viên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

**Hà Nội – 2024**

1. Mục đích

Giúp sinh viên hiểu về khái niệm về lỗ hổng bảo mật và cách phát hiện các lỗ hổng bảo mật sử dụng các công cụ rà quét nmap.

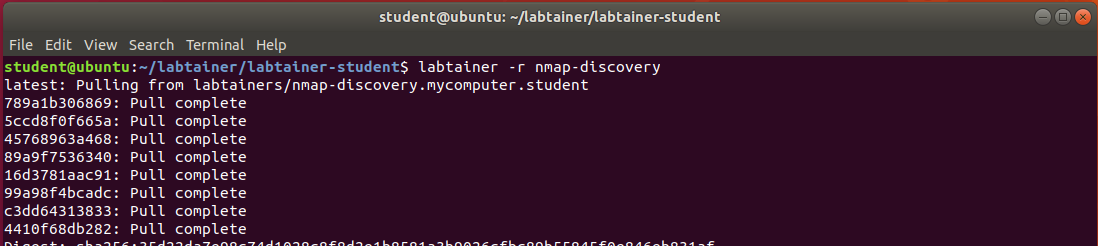
2. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.

3. Nội dung thực hành

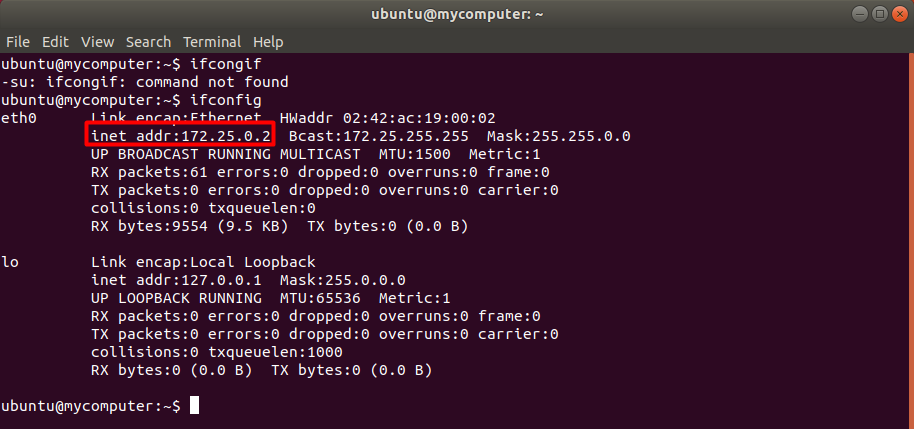
Khởi động bài lab:

Vào terminal, gõ: labtainer -r nmap-discovery



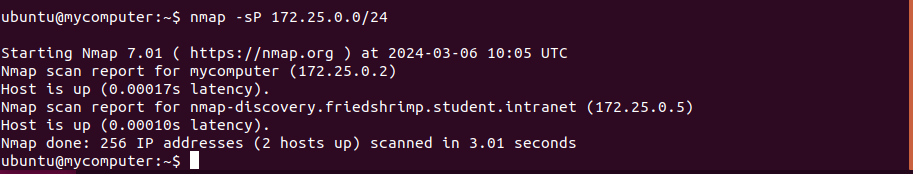
Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: mycomputer, một cái là đại diện cho máy chủ: friedshrimp. Biết rằng 2 máy nằm cùng mạng LAN.

Trên terminal mycomputer sử dụng lệnh “ifconfig”, xác định địa chỉ IP và địa chỉ mạng LAN



Trên máy khách mycomputer sử dung nmap để tìm ra địa chỉ IP của máy friedshrimp

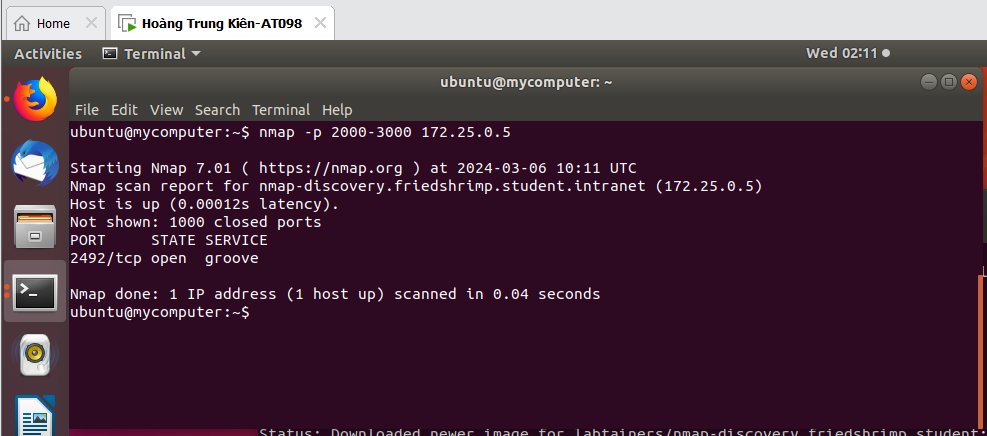
nmap –sP 172.25.0.0/24



Ta tìm thấy địa chỉ IP của máy friedshrimp là: 172.25.0.5

Tiếp tục sử dụng nmap để tìm cổng dịch vụ đang mở trên máy friedshrimp biết rằng cổng (port) nằm từ 2000-3000.

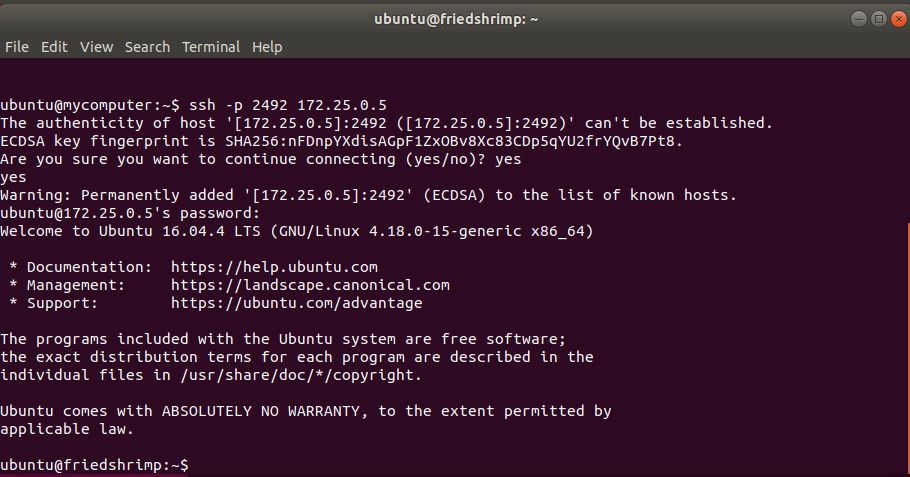
nmap –p 2000-3000 172.25.0.5



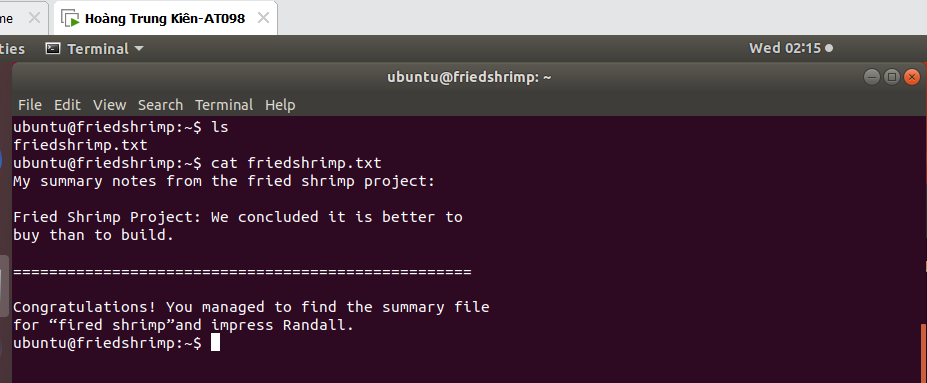
cổng dịch vụ đang mở trên máy friedshrimp là 2492

Sau khi xác định được cổng ssh đang mở. Sử dụng ssh để truy cập vào máy chủ. Tên máy chủ và mật khẩu là: ubuntu.

nmap –p 2000-3000 172.25.0.5



Sau khi truy cập được vào máy chủ friedshrimp đi tìm file friedshrimp.txt. Mở và đọc file.





Checkwork

