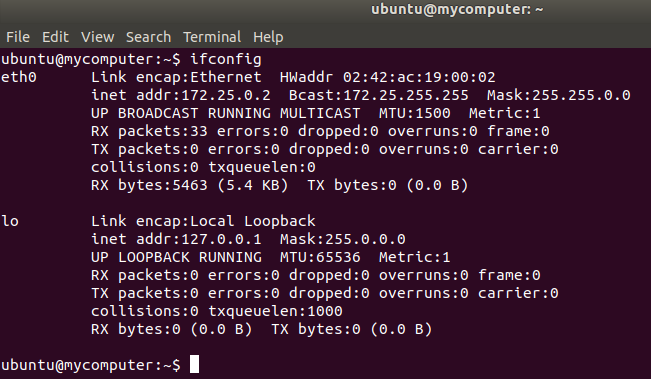
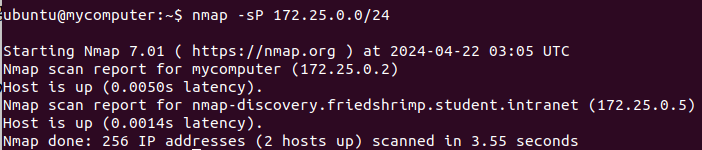
**BÀI 2. PHÁT HIỆN CÁC LỖ HỔNG BẢO MẬT SỬ DỤNG CÔNG CỤ RÀ QUÉT**

1. Xác định địa chỉ IP và địa chỉ mạng LAN bằng lệnh ifconfig:

****

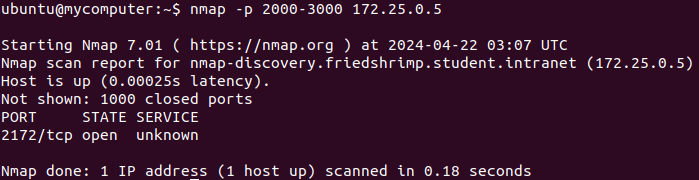
🡪IP mạng LAN: 172.25.0.0/24

1. Trên máy khách mycomputer sử dung nmap để tìm ra địa chỉ IP của máy friedshrimp vì chúng cùng nằm trong mạng LAN: nmap –sP <IP mạng LAN>



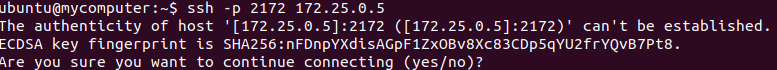
Suy ra: IP máy friedshrimp là 172.25.0.5

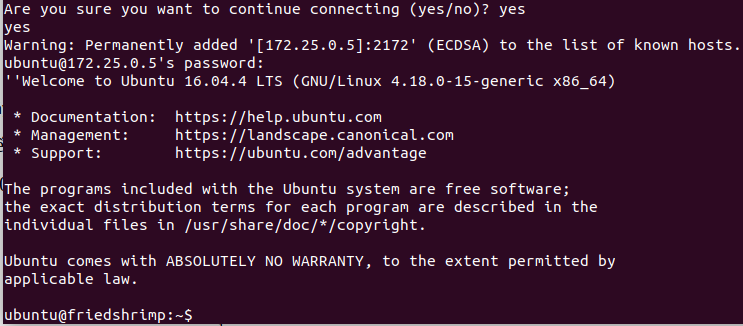
1. Sử dụng nmap để tìm cổng dịch vụ đang mở trên máy friedshrimp biết rằng cổng (port) nằm từ 2000-3000.



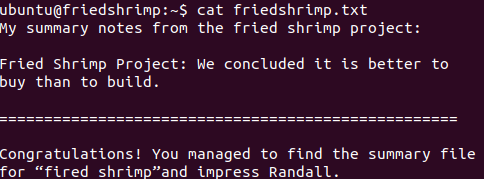
Suy ra: Cổng dịch vụ đang mở là 2172

1. Ssh để truy cập vào máy chủ với cả tên và đăng nhập là ubuntu: ssh –p <port> <IP friedshrimp>





1. Tìm và đọc file friedshrimp.txt



1. Đóng kết nối từ máy computer đến friedshrimp

