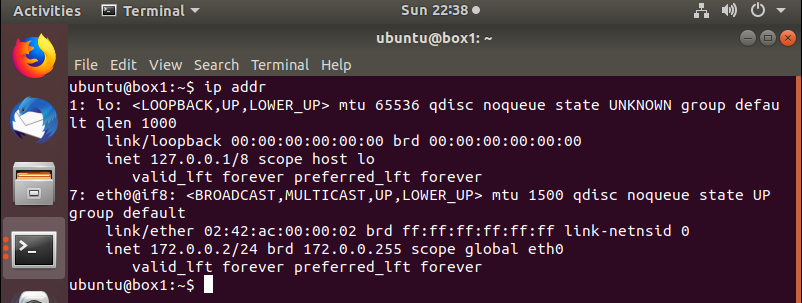
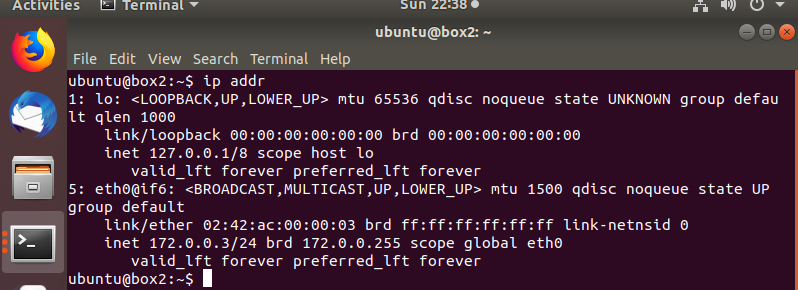
**1.Các giao thức mạng cơ bản**

\*Trên terminal ***box1*** và ***box2***sử dụng lệnh “ip addr” để kiểm tra địa chỉ IP





\*Trên máy **box2** thực hiện *arp –a* để kiểm tra bản đồ mạng lúc này, tuy nhiên không có kết quả trả về do chưa có kết nối giữa **box1** và **box2**

\*Trên “box1” chạy tcpdump để theo dõi đường mạng trước khi thực hiện kết nối giữa 2 máy:

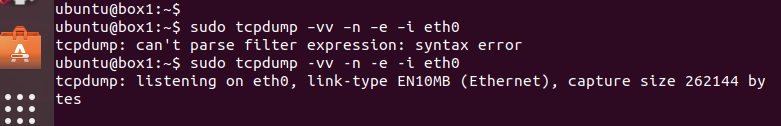
*Sudo tcpdump –vv –n –e –i eth0*

-vv: cung cấp kết quả đầy đủ

-n: Không thực hiện tra cứu DNS ngược, chỉ hiển thị địa chỉ IP.

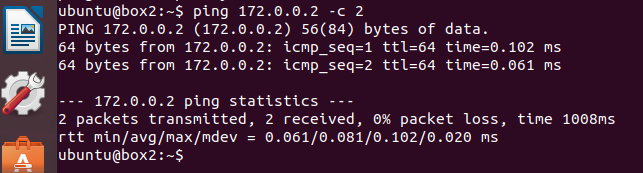
-e: hiển thị địa chỉ Ethernet MAC

-i eth0: hiển thị lưu lượng trên eth0

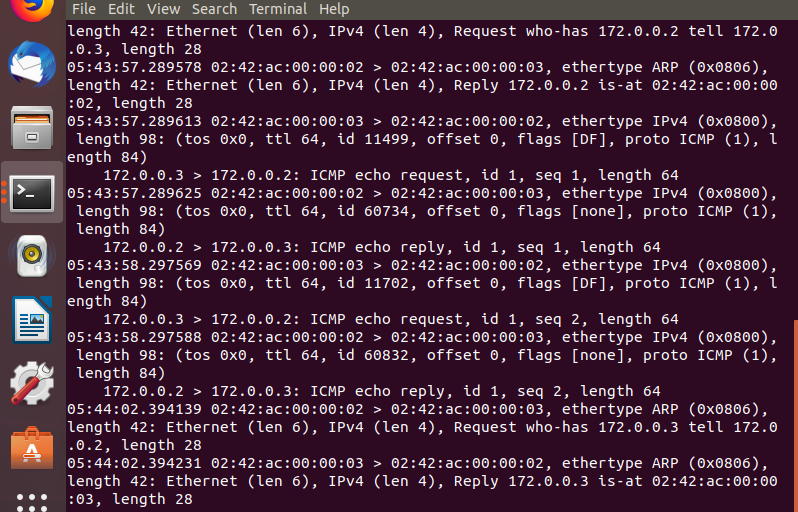


\*Trên máy “box2” thực hiện ping đến máy “box1”

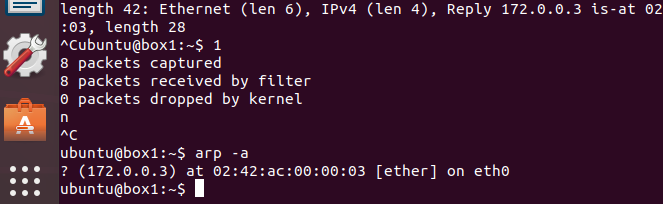
*Ping 172.0.0.2 –c 2*



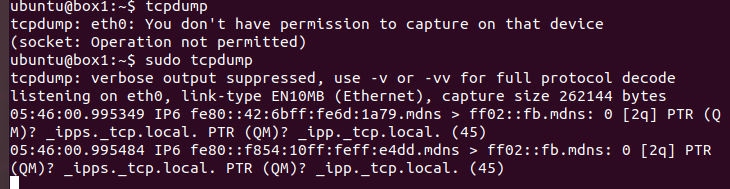
\*Lúc này trên **box1** ta có thể theo dõi các gói tin gửi qua lại giữa 2 máy



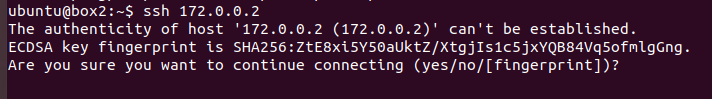
\*Sử dụng *ctrl+c* để kết thúc tcpdump và chạy lệnh *arp –a* trên **box1** để thấy bản đồ mạng lúc này (ARP table)



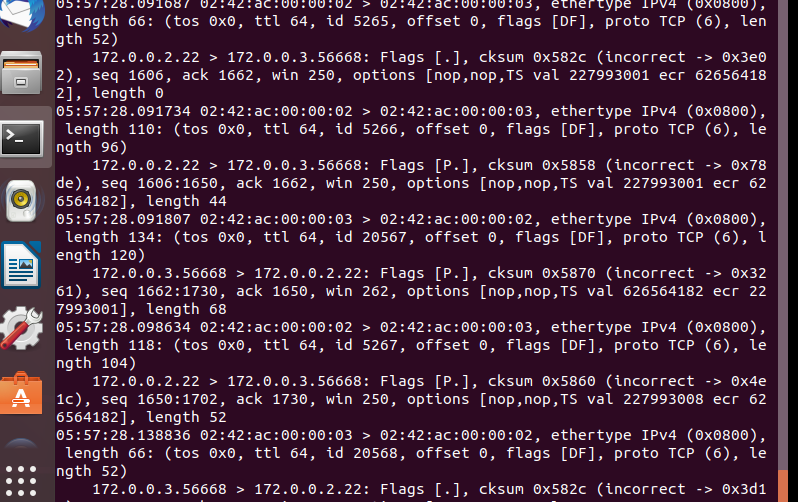
\*Trên **box1** bật tcpdump để theo dõi bắt tay 3 bước trong kết nối TCP.



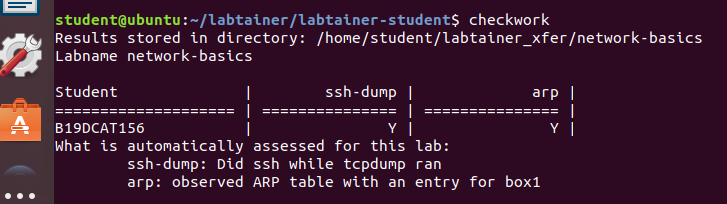
\*Trên **box2** thực hiện ssh đến **box1**, chỉ cần chạy không cần kết nối.



\*Giải thích các thuật ngữ xuất hiện khi kiểm tra các gói tin thu nhận được trên **box1**

****

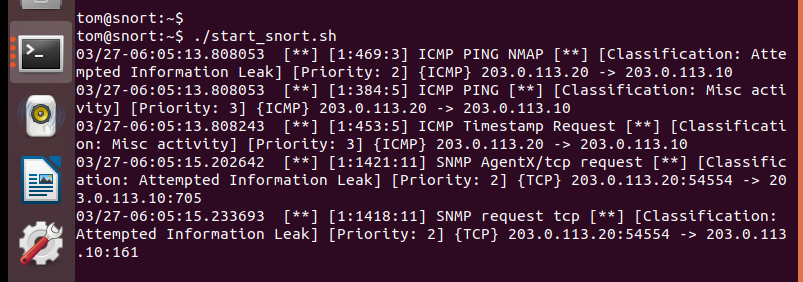
**\*Checkwork**

****

# 2.Phát hiện xâm nhập mạng với Snort

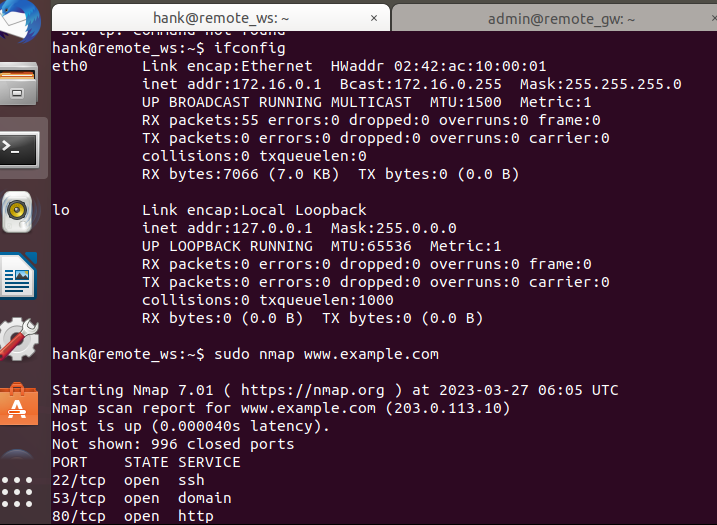
\*Khởi động snort trên máy “snort” để theo dõi lưu lượng mạng:

./start\_snort.sh



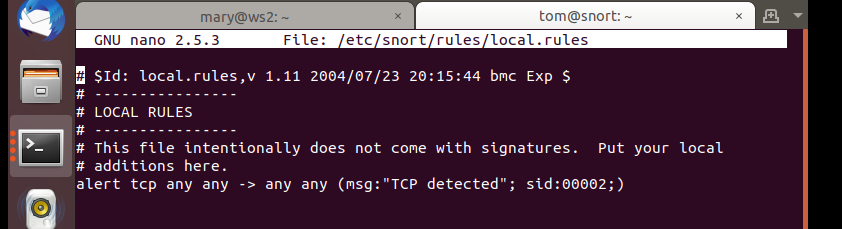
\*Để xem ví dụ về một số quy tắc được cấu hình sẵn, thực hiện quét nmap của www.example.com từ máy trạm từ xa:

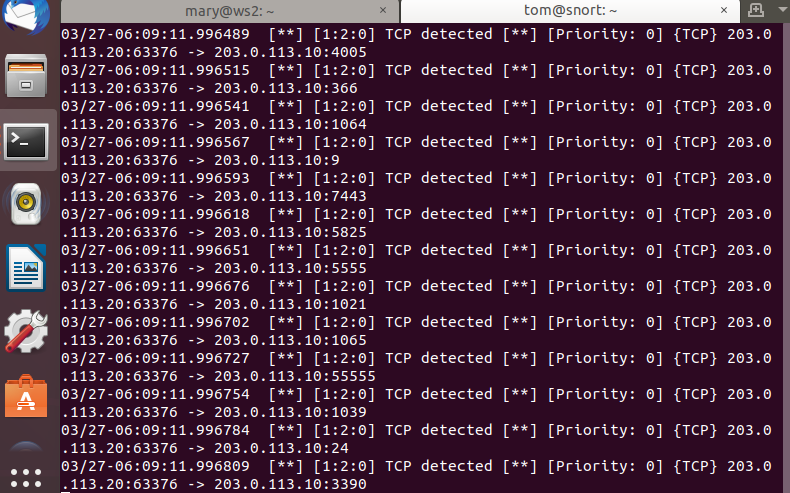
sudo nmap [www.example.com](http://www.example.com)



\*Tạm dừng snort. Thêm luật sau vào file /etc/snort/rules/local.rules, khởi động lại snort và chạy lại bước 2 để theo dõi kết quả trên máy “snort”:

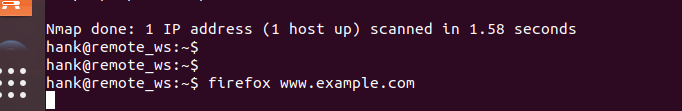
alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)

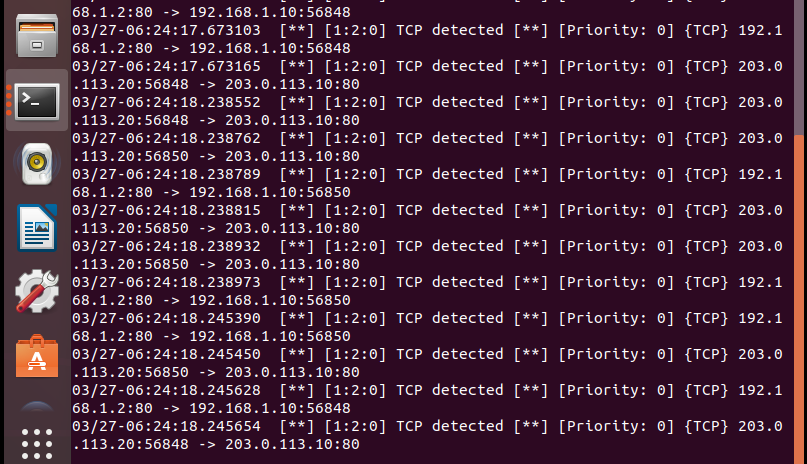




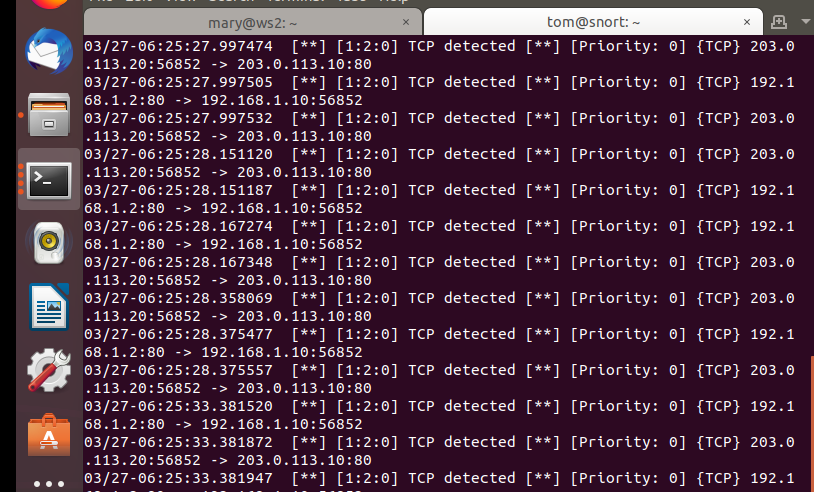
\*Sinh viên khởi động lại snort. Kiểm tra luật vừa tạo bằng cách khởi động Firefox trên máy trạm từ xa:

firefox [www.example.com](http://www.example.com)



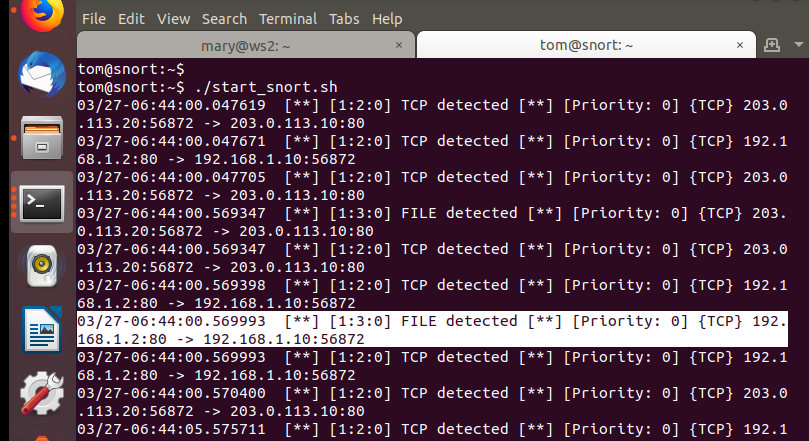


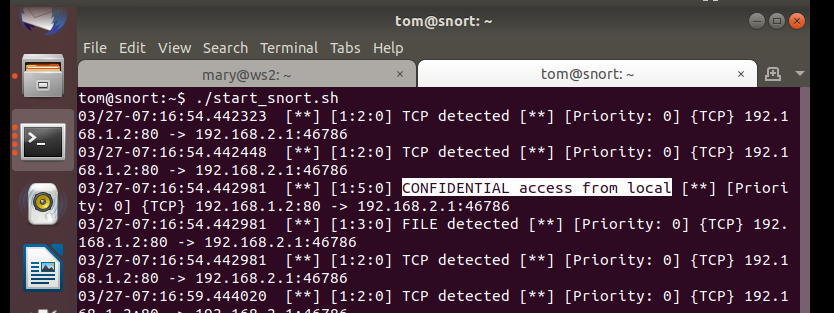
\*Giả sử bạn đã nghe nói rằng một công ty khởi nghiệp đã đặt kế hoạch kinh doanh bí mật của họ tại www.example.com/plan.html. Truy cập link trên bằng máy trạm từ xa và kiểm tra cảnh báo của snort.

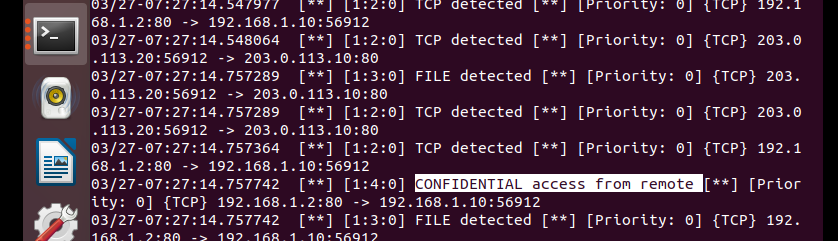


\*Sinh viên viết thêm luật vào file /etc/snort/rules/local.rules trên snort để tạo cảnh báo bất cứ khi nào văn bản "CONFIDENTIAL" được gửi ra internet. Sau khi thêm luật, khởi động lại snort. Xóa lịch sử truy cập trên firefox và thử truy cập lại [www.example.com/plan.html](http://www.example.com/plan.html) từ máy trạm từ xa. Kiểm tra các cảnh báo mới của snort.









\*Chuyển đến cointainer “ws2” (mary) và chạy nmap:

sudo nmap www.example.com

\*Cấu hình lại gateway để ánh xạ lưu lượng vào snort để theo dõi các cảnh báo bằng cách thêm vào file /etc/rc.local dòng lệnh:

iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1

\*Sau đó chạy lại snort để theo dõi lưu lượng.

\*Phân biệt lưu lượng theo địa chỉ: viết các luật snort sao cho:

\*Quyền truy cập bên ngoài vào kế hoạch kinh doanh sẽ tạo ra một cảnh báo.

\*Truy cập nội bộ vào kế hoạch kinh doanh không tạo cảnh báo.

\*Việc sử dụng nmap bên ngoài hoặc bên trong sẽ tạo cảnh báo ICMP NMAP PING

\*Checkwork

