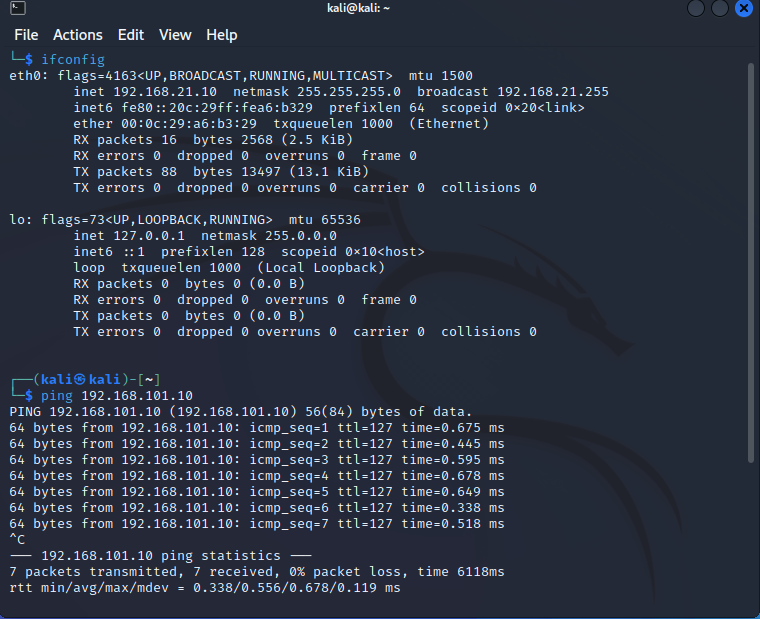
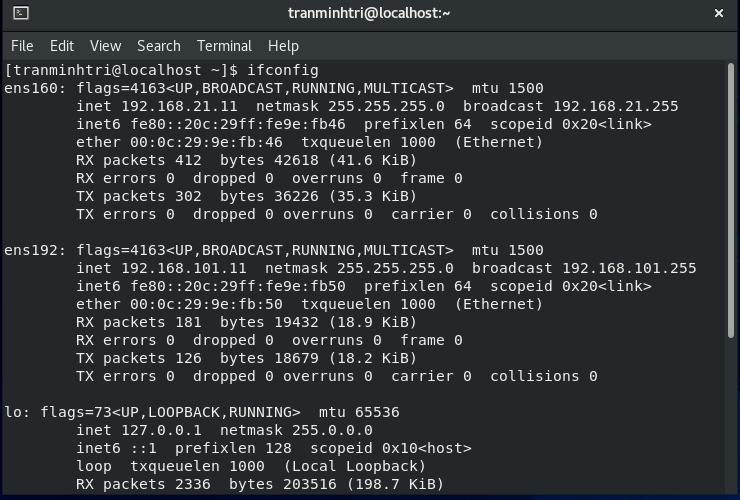
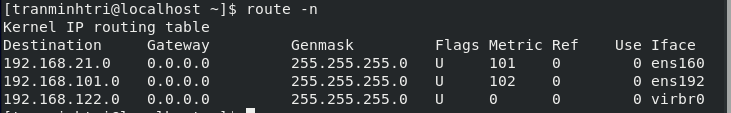
Cấu hình máy attacker:



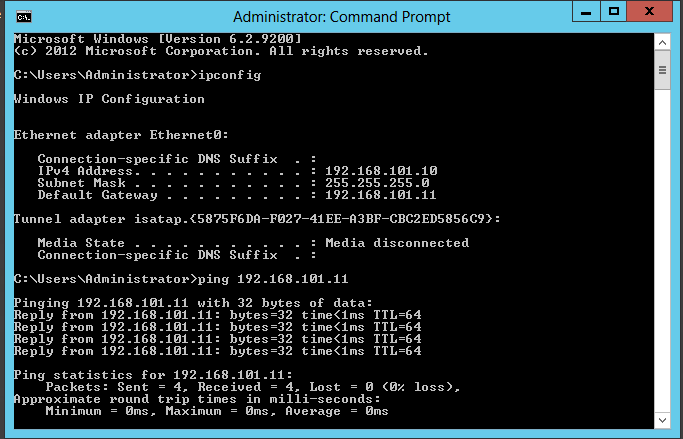
Cấu hình máy IPS/IDS:



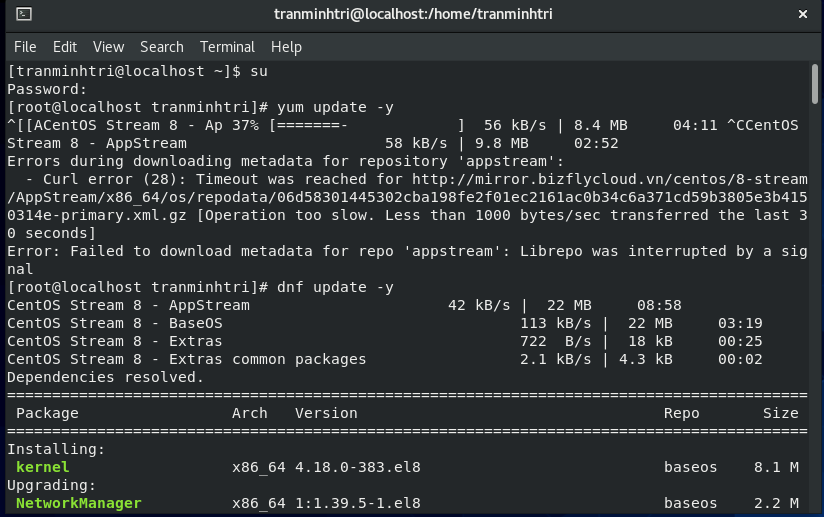
Kiểm tra kết nối của máy ips/ids:

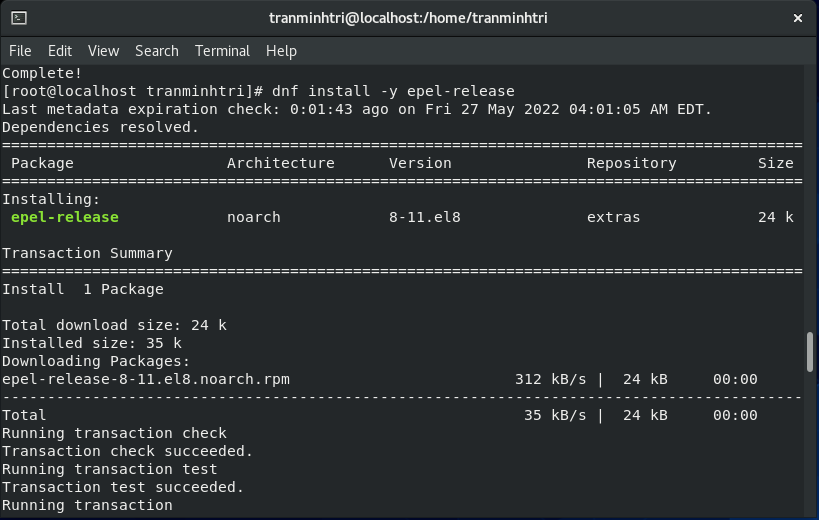


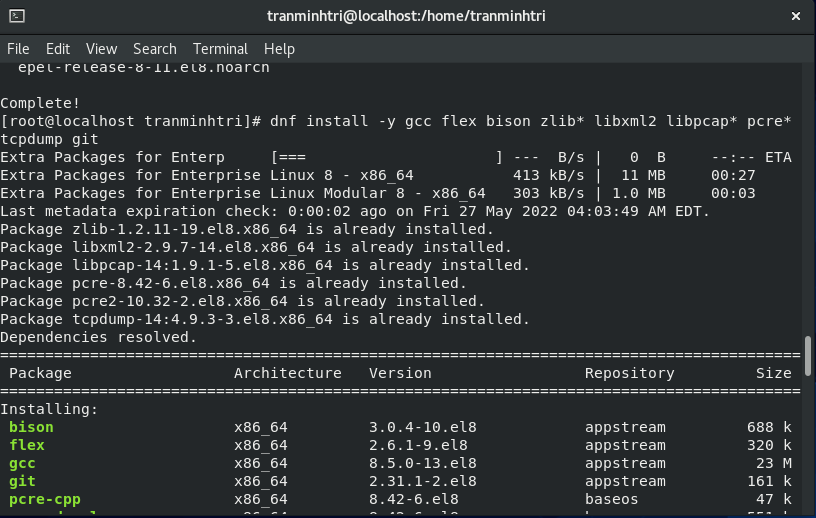
Máy nạn nhân kiểm tra ping tới card mạng của máy IPS/IDS:

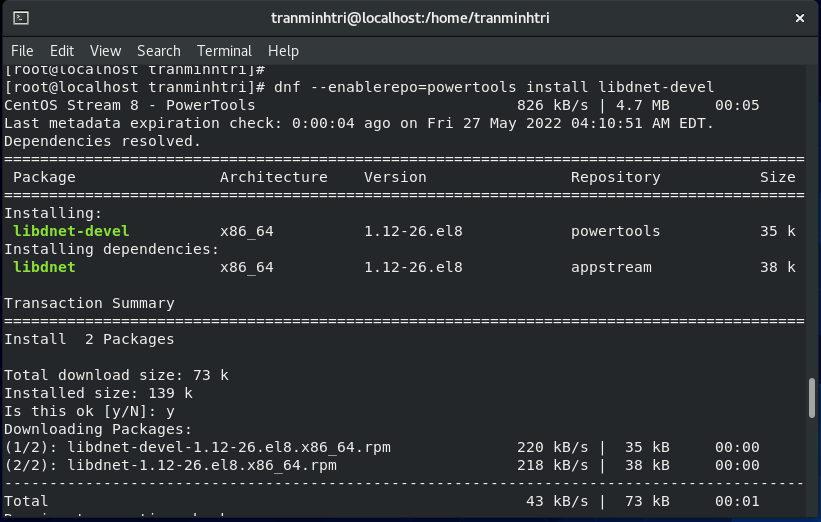


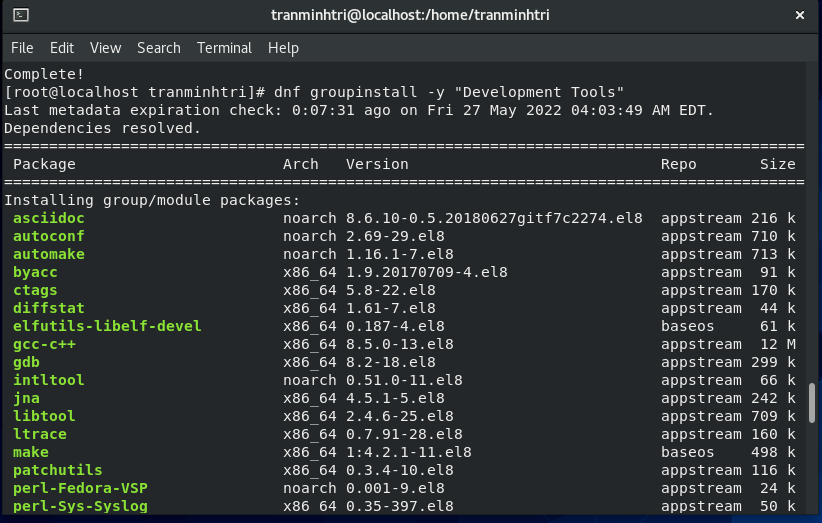
Tiến hành cài đặt snort:

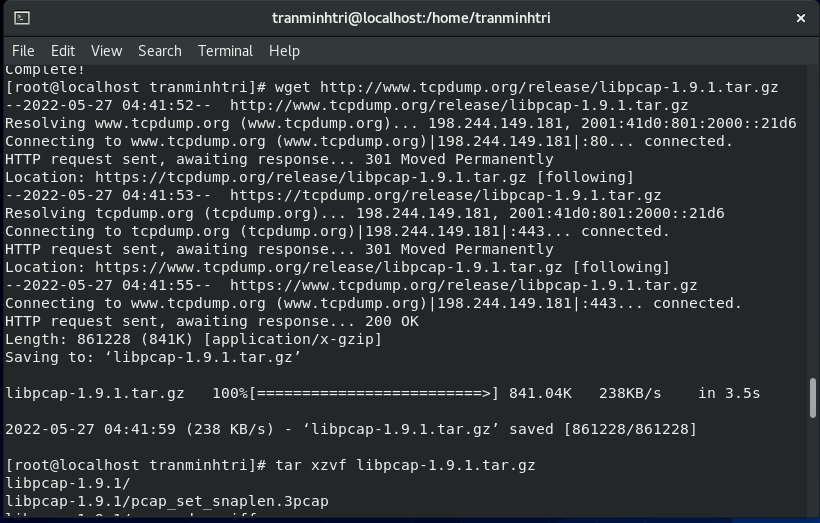


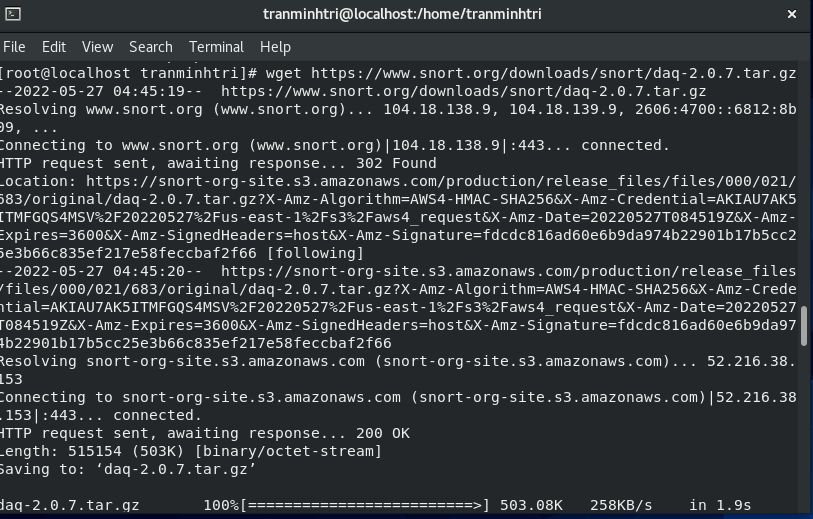




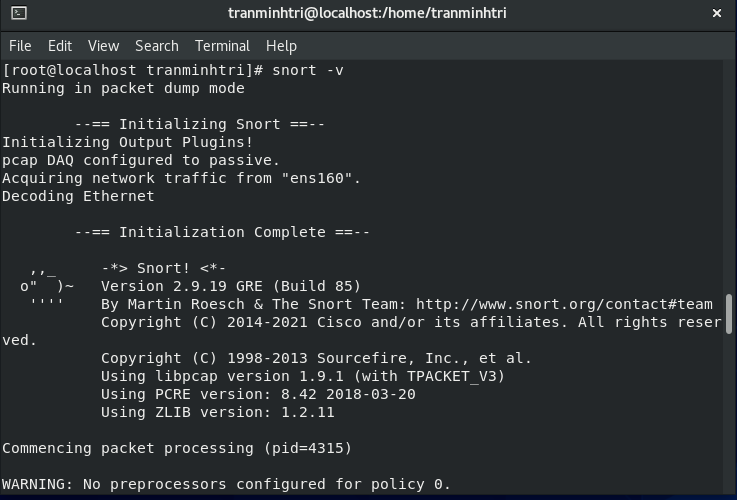




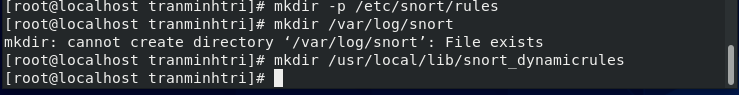




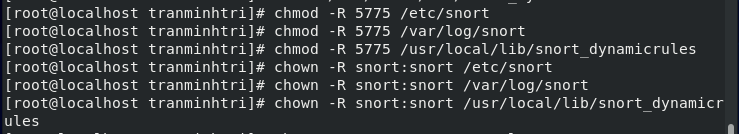




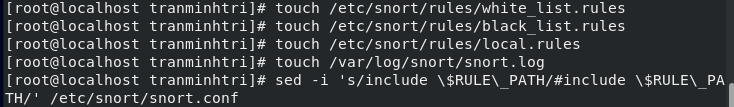
Ta tiến hành tạo thư mục lưu trữ rule cho snort



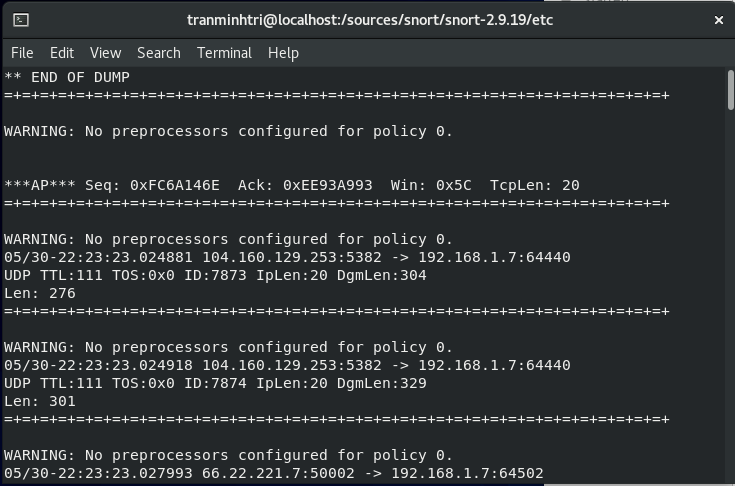
Ta tiến hành cấp quyền sỡ hữu và điều chỉnh các thư mục vừa tạo



Ta tiến hành tạo các tệp tin cần thiết cho các thư mục trong snort



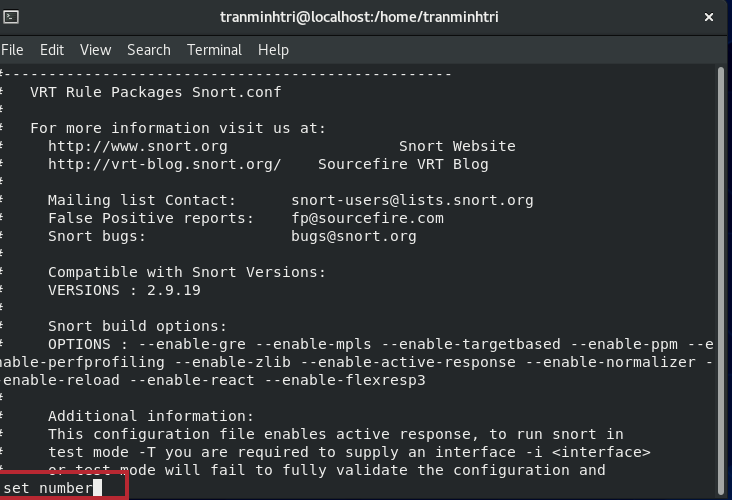
Test snort



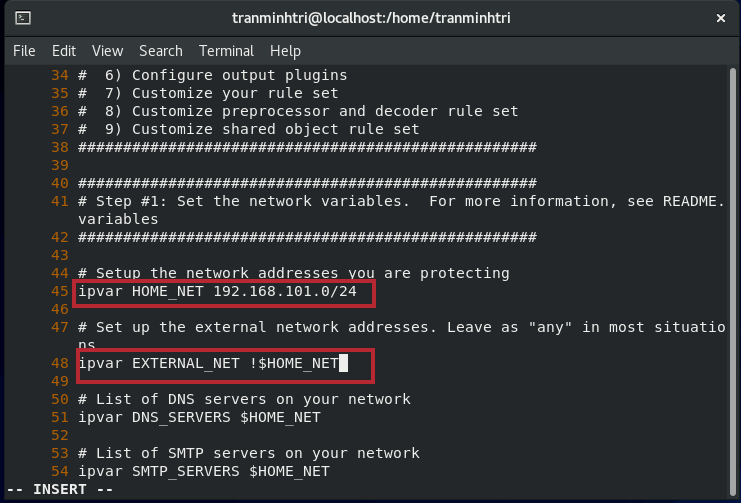
Cấu hình snort



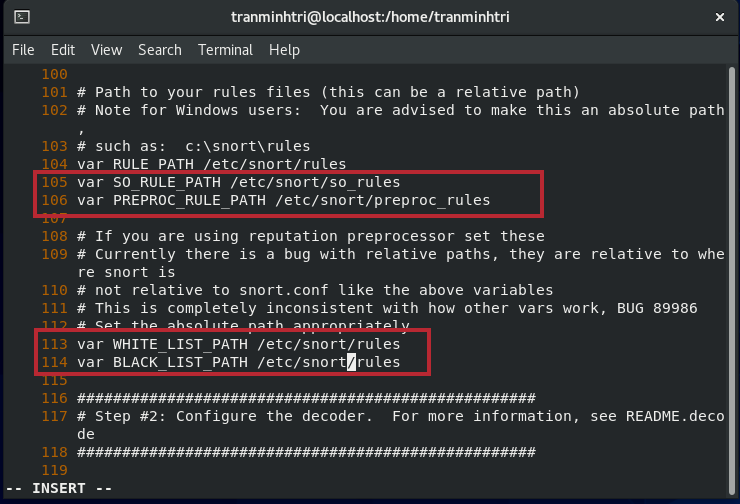
Bật chú thích đánh số các dòng



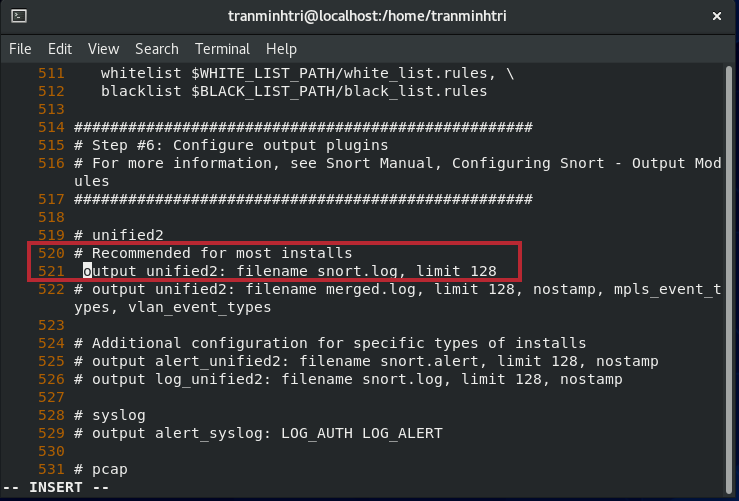
Ta nhấn i để vô trạng thái insert và tiến hành sửa ip any dòng 45 thành ip vùng internal Vmnet2 vùng bảo vệ máy nạn theo bài lab, sửa any dòng 48 thành !$HOME\_NET



Dòng 105,106,113,114 thay .. thành /etc/snort , ta đổi đường dẫn trỏ tới snort cho các tập tin vừa tạo ở trên

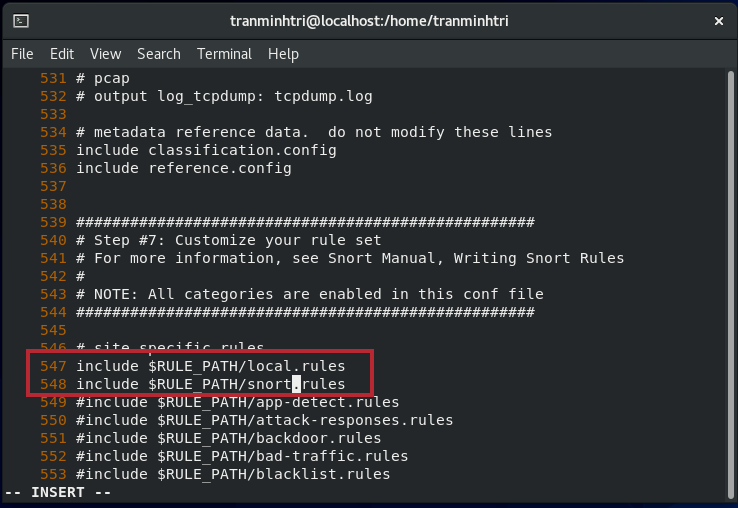


Dòng 520 enter xuống và chèn vô dòng 521 thêm dòng lệnh như trong hình, để tải thêm file snort.log – nhật ký snort

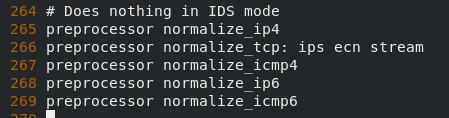


Dòng 546 tại vì ta chèn thêm 1 dòng 521 nên giờ sẽ là 547, xoá dấu # phía trước

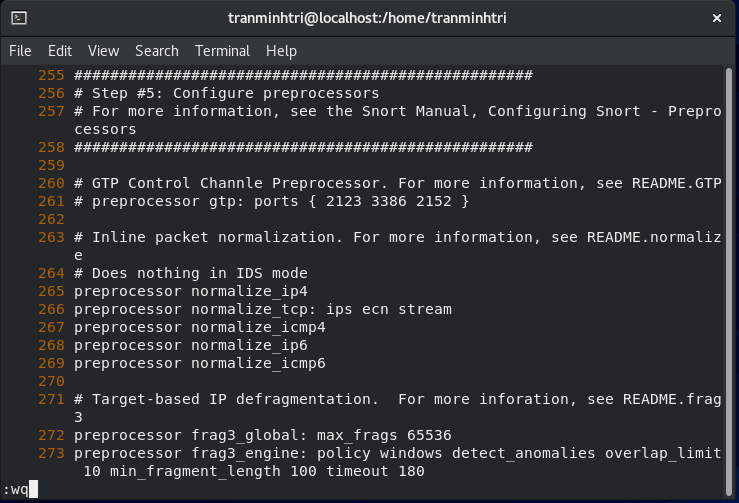
include $RULE\_PATH/local.rules

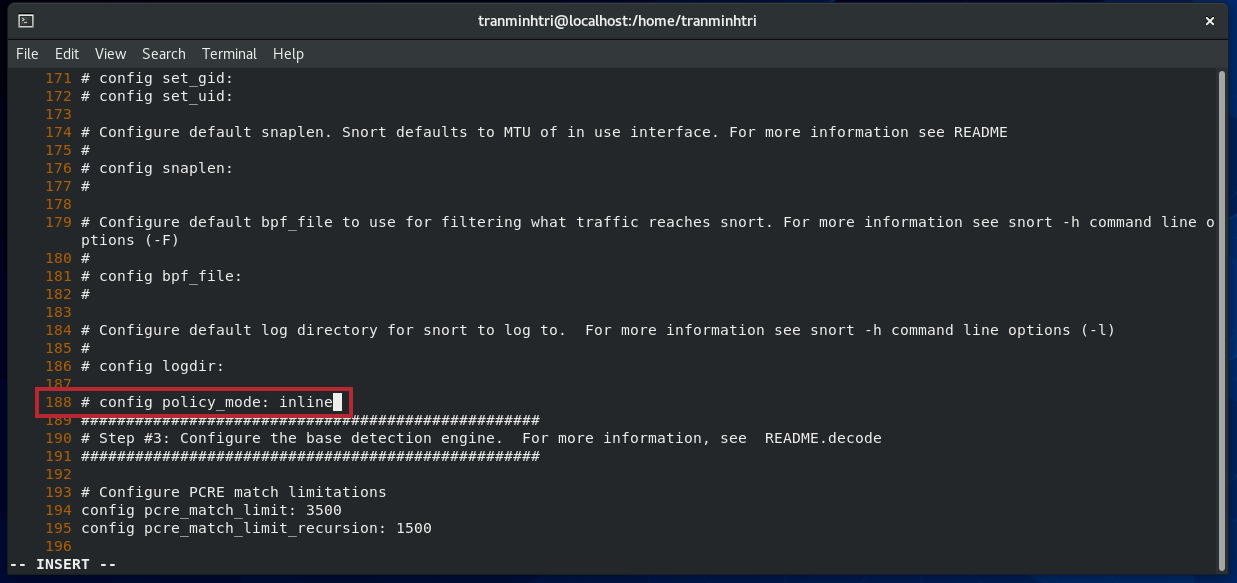


Thực hiện kiểm tra dòng 264 tới 269 sau đó lưu lại file bằng lên :wq

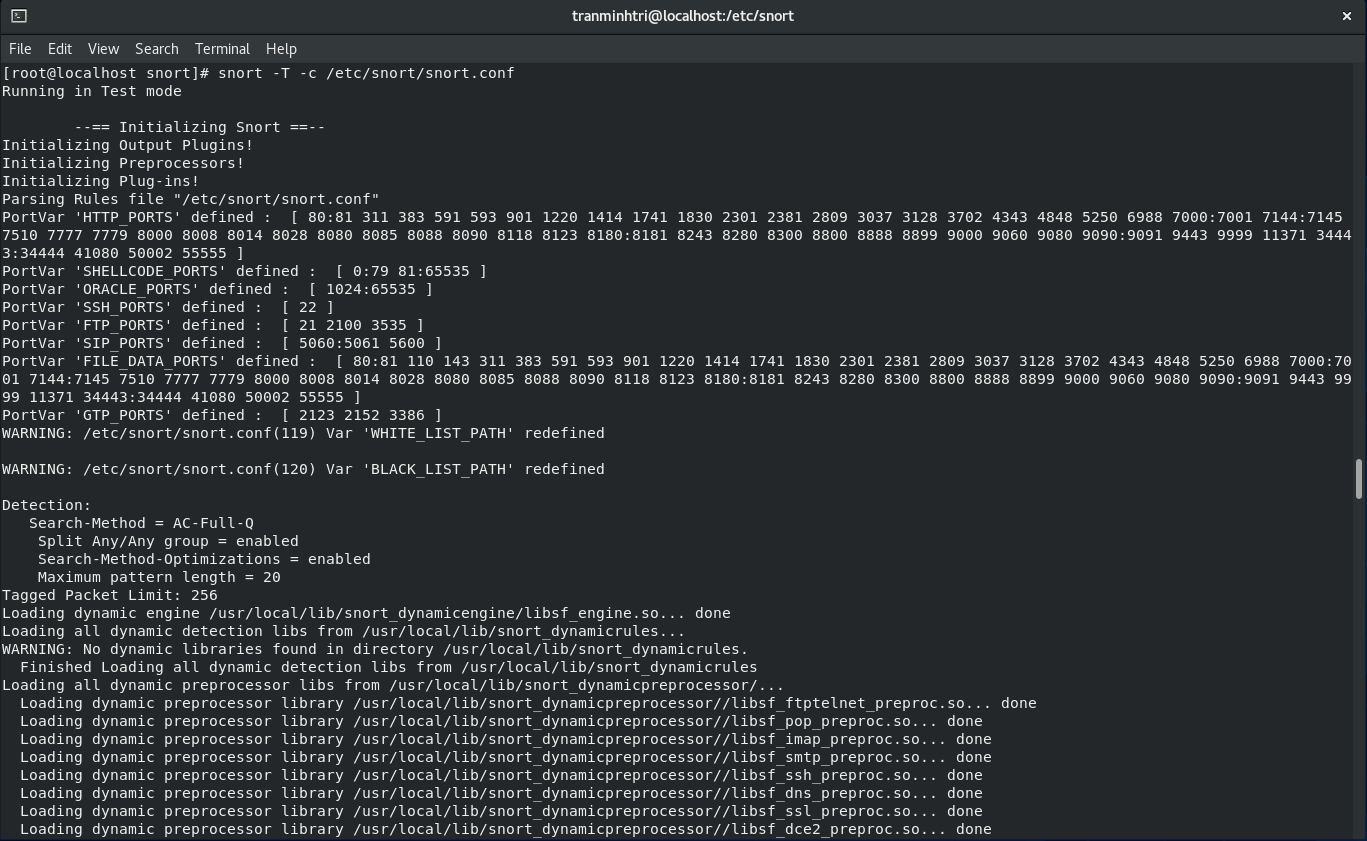


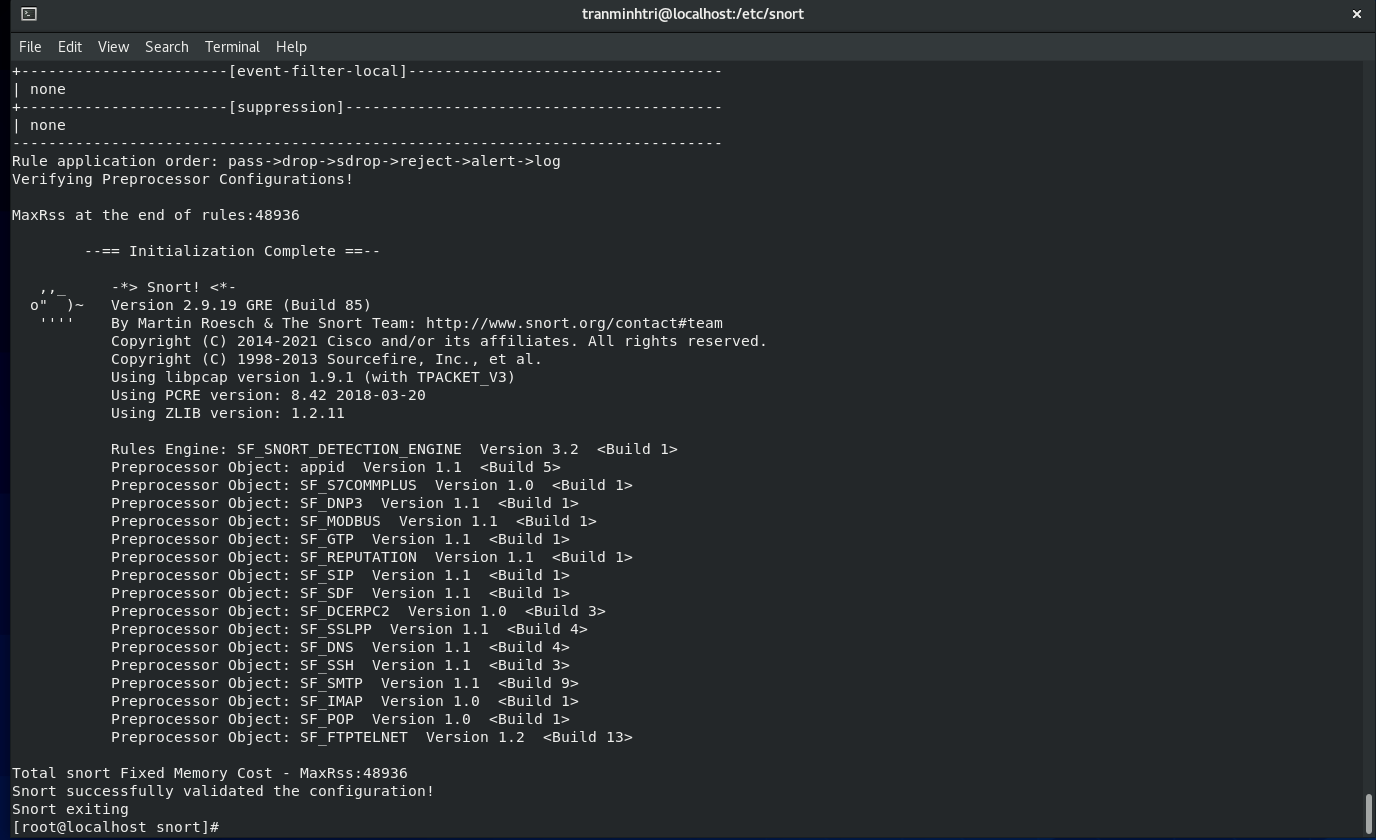
Ta nhấn esc để thoát trạng thái insert và gõ :wq để lưu lại file vừa sửa



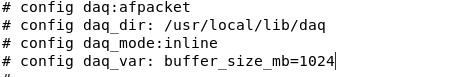


Chạy test file cấu hình snort

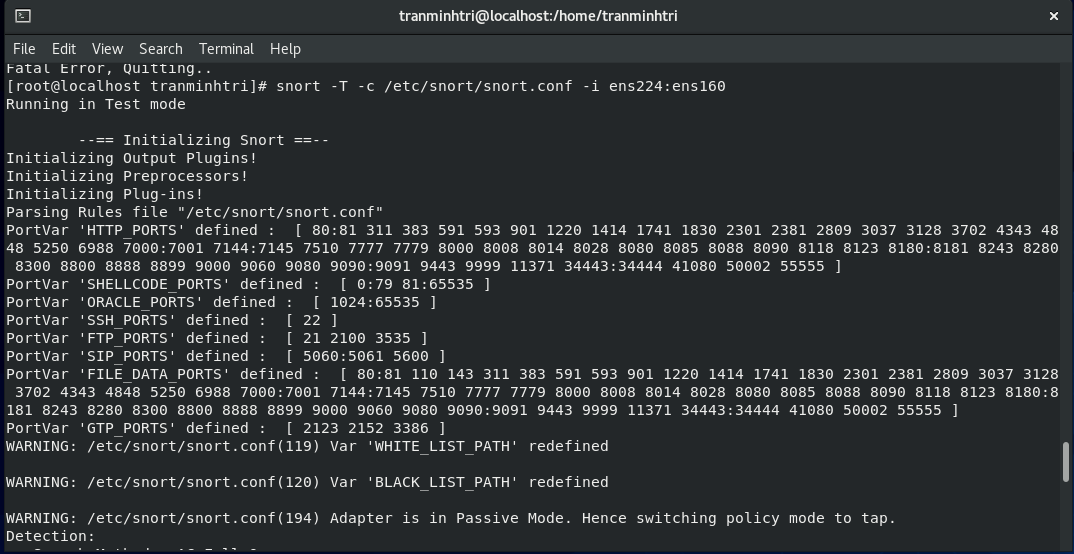




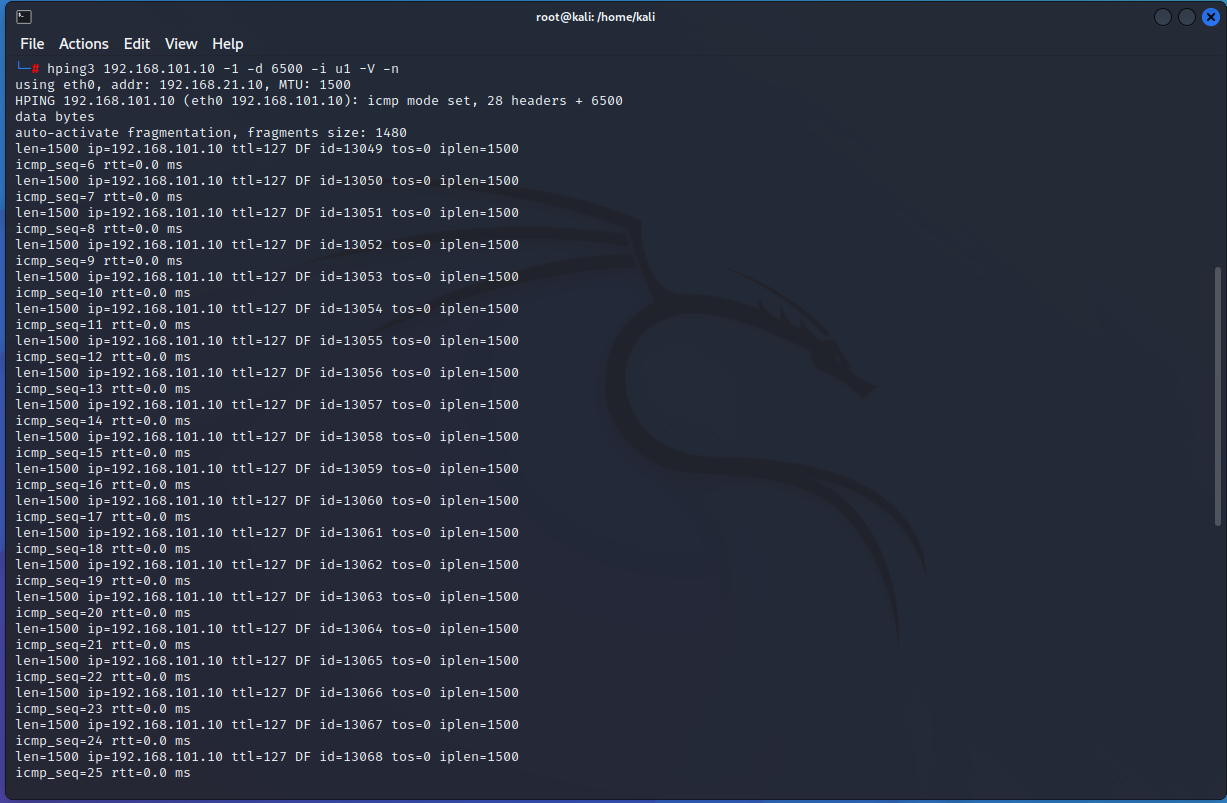


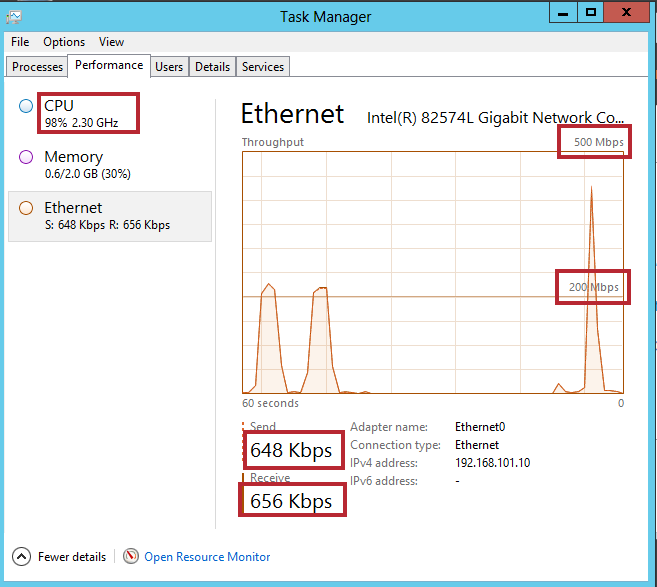


Lưu lại cấu hình cho 2 đường mạng từ máy nạn nhân tới máy attacker



Thực hiện ping of death qua máy nạn nhân

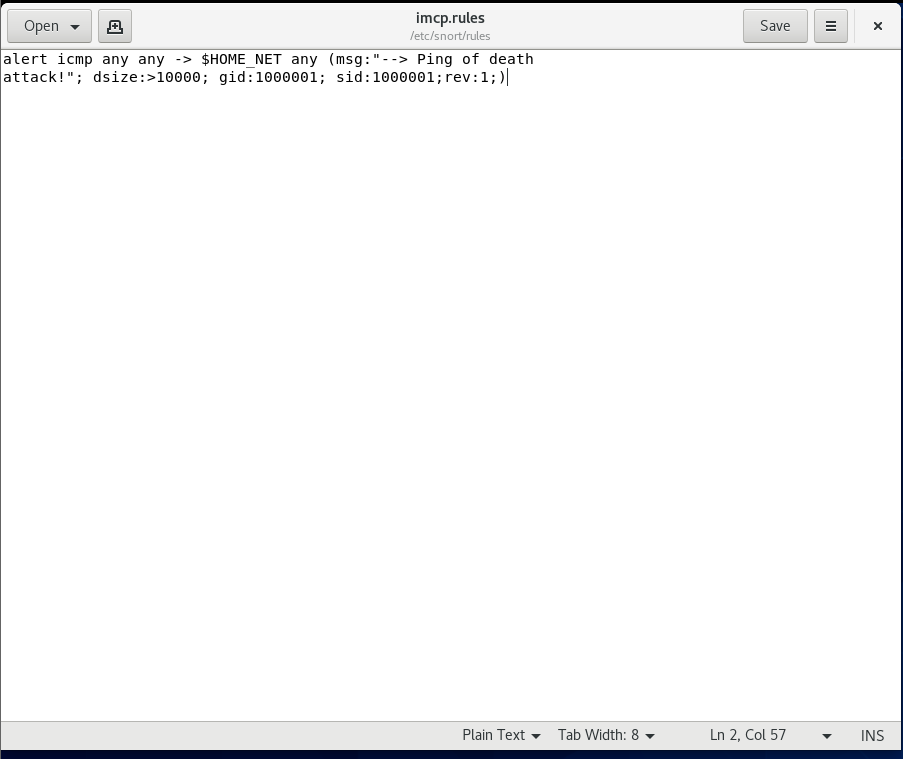




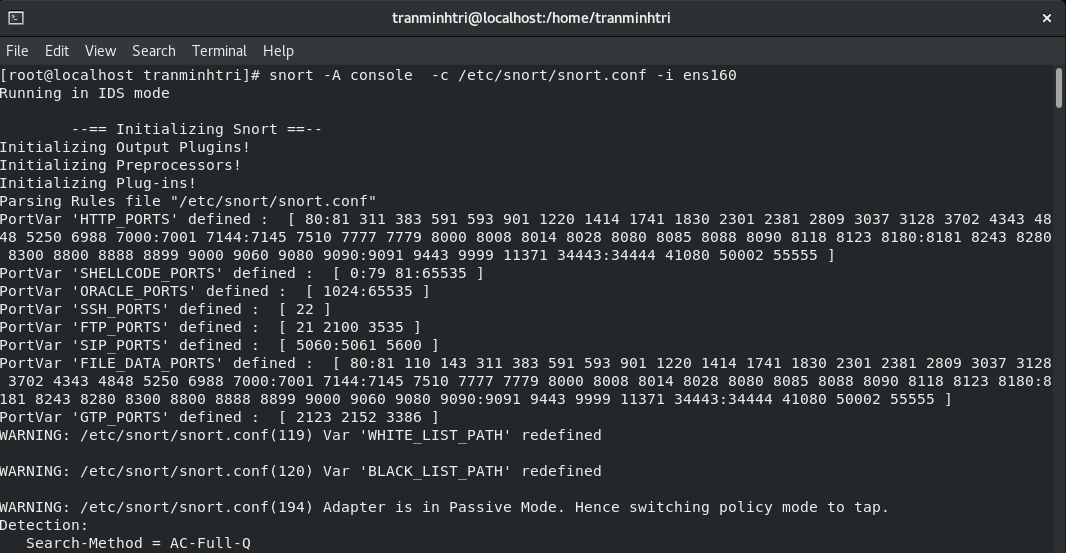
Ta bỏ dấu than để viết rule cảnh báo lượng icmp chặn việc ping of death

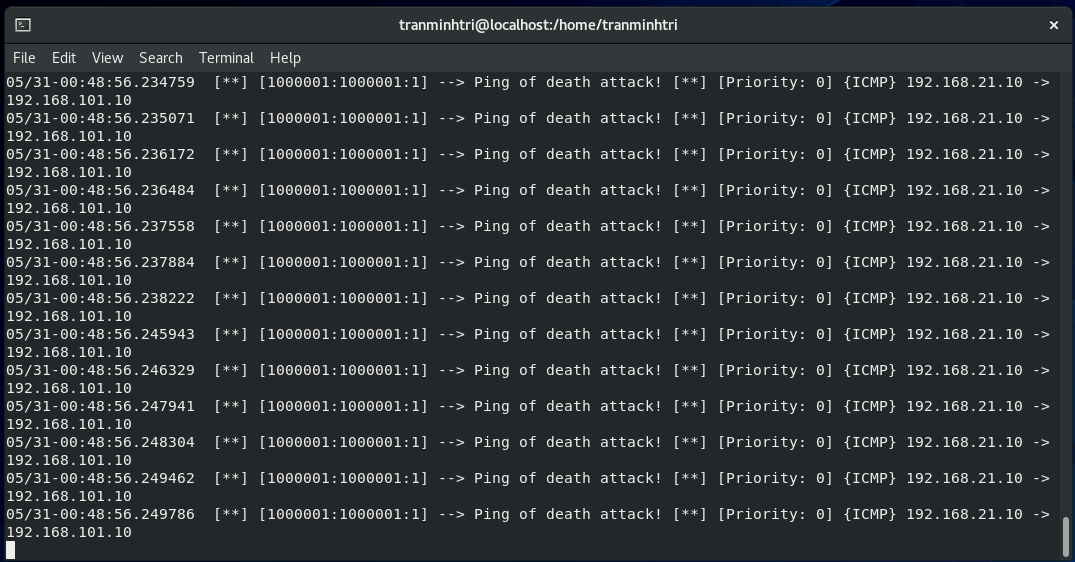


Viết rule cảnh báo ping of death



Test rule thành công





Chan ping of death sau khi bat snort len

