

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI TẬP TRÊN LỚP**

**Lập trình ứng dụng di động**

**Giảng viên: Nguyễn Hoàng Anh**

**Nhóm lớp: 01**

**Sinh viên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

**Hà Nội – 2024**

**Mục lục**

1. [Tổng quan về Bộ tiền xử lý danh tiếng 3](#_bookmark0)
2. [Cài đặt snort 3](#_bookmark1)
3. [Cấu hình Bộ tiền xử lý danh tiếng (reputation preprocessor) 3](#_bookmark2)
4. [Thêm mục nhập vào danh sách IP theo cách thủ công 5](#_bookmark3)
5. [Chạy snort 6](#_bookmark4)

# Tổng quan về Bộ tiền xử lý danh tiếng

* + Bộ tiền xử lý danh tiếng được tạo ra để cho phép Snort sử dụng một tệp chỉ có địa chỉ IP để xác định các máy chủ xấu và máy chủ đáng tin cậy. Địa chỉ IP độc hại được lưu trữ trong danh sách đen và địa chỉ IP đáng tin cậy được lưu trữ trong danh sách trắng. Bộ tiền xử lý danh

tiếng tải các danh sách này khi Snort khởi động và so sánh tất cả lưu lượng truy cập với các danh sách đó. Snort kiểm tra cả địa chỉ IP gửi và nhận trong mỗi gói đối với mọi mục trong danh sách IP và nếu địa chỉ IP trong gói khớp với địa chỉ IP trong danh sách đen, danh sách

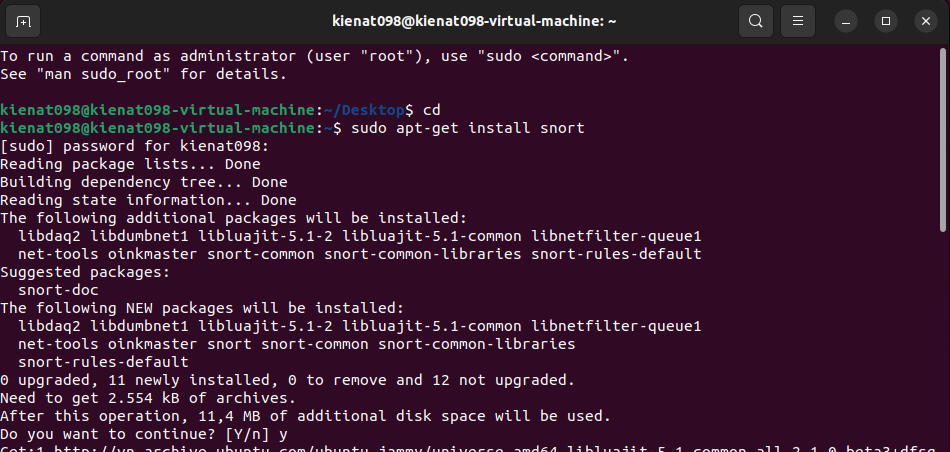
trắng hoặc cả hai danh sách, Snort có thể thực hiện một số hành động khác nhau: Snort có thể tạo cảnh báo, chặn gói, cho phép gói mà không cần xử lý nào khác (bỏ qua tất cả các quy tắc khác) hoặc để gói tiếp tục vượt qua phần còn lại của quá trình kiểm tra quy tắc thông

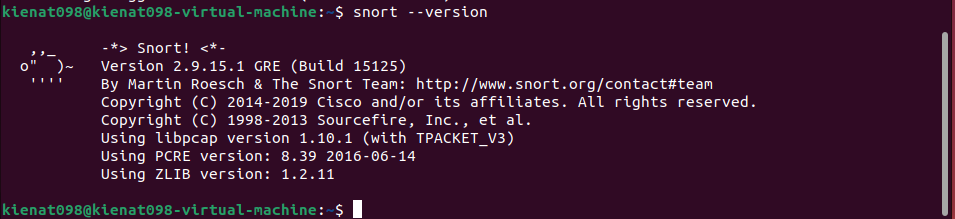
thường. Hành động mà Snort thực hiện tùy thuộc vào cách chúng ta định cấu hình bộ tiền xử lý danh tiếng và nếu Snort đang chạy ở chế độ IDS hoặc IPS (Snort chỉ có thể loại bỏ các gói khi chạy ở chế độ IPS, vì những lý do rõ ràng).

- Bộ tiền xử lý danh tiếng là bộ tiền xử lý đầu tiên mà một gói gặp phải trong Snort (sau khi được bộ giải mã tập hợp). Lý do cho điều này là vì bộ tiền xử lý danh tiếng có thể đánh dấu các gói tin cậy để bỏ qua phần còn lại của bộ tiền xử lý và công cụ quy tắc hoặc có thể loại bỏ gói, điều đó có thể giúp giảm tải cho hệ thống Snort.

# Cài đặt snort

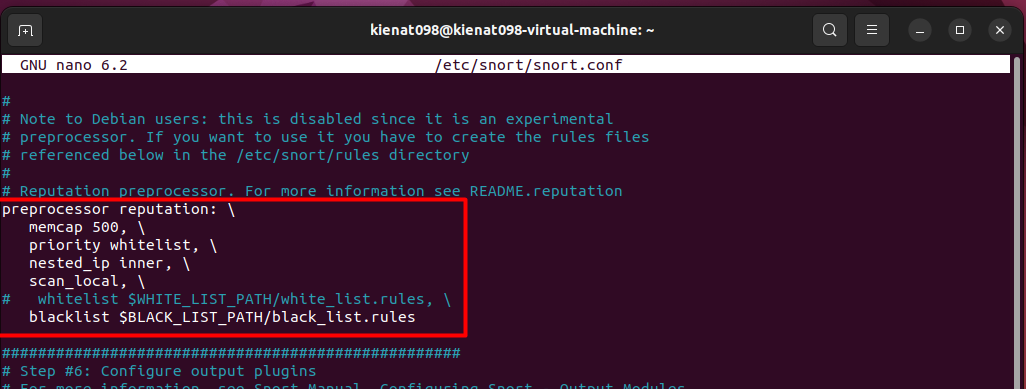
* + Cài đặt snort với câu lệnh *sudo apt install snort .*
  + Nếu cài đặt thành công, sử dụng lệnh *snort –version* sẽ hiển thị phiên bản của snort.



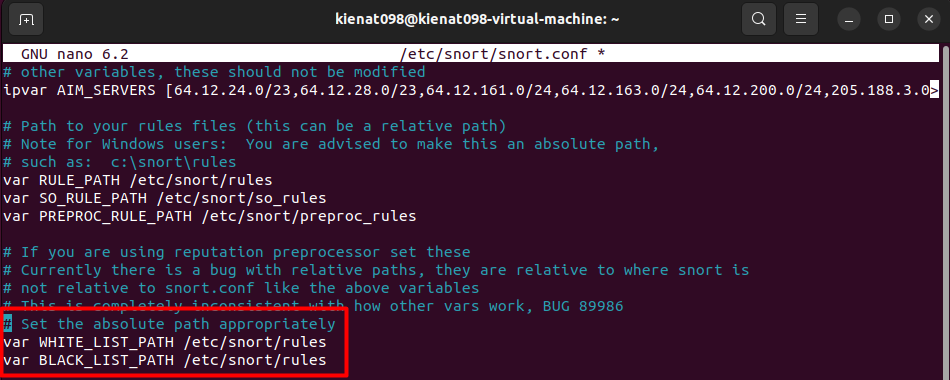


# Cấu hình Bộ tiền xử lý danh tiếng (reputation preprocessor)

* + Bộ tiền xử lý danh tiếng được cấu hình trong snort.conf .
  + Nếu Nhiều cài đặt Snort tiêu chuẩn đặt tệp này tại **/etc/snort/snort.conf**. Mở tệp cấu hình snort này và tìm phần dành cho bộ tiền xử lý danh tiếng.bộ tiền xử lý bị vô hiệu hóa với ký hiệu băm (#) ở đầu mỗi dòng cho bộ tiền xử lý, có thể bật nó bằng cách xóa ký hiệu băm khỏi đầu mỗi dòng. Cấu hình tiền xử lý sẽ trông giống như sau khi được bật:



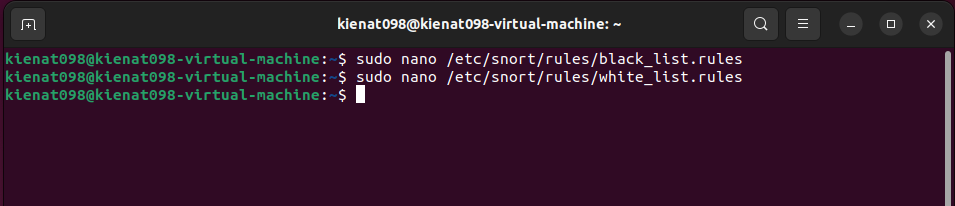
- Có một vài dòng khác trong snort.conf cũng liên quan đến danh sách IP. Hai dòng sau đây cho Snort biết thư mục chứa white\_list và black\_list:



- Sử dụng lệnh sau để tạo blacklist và whitelist.

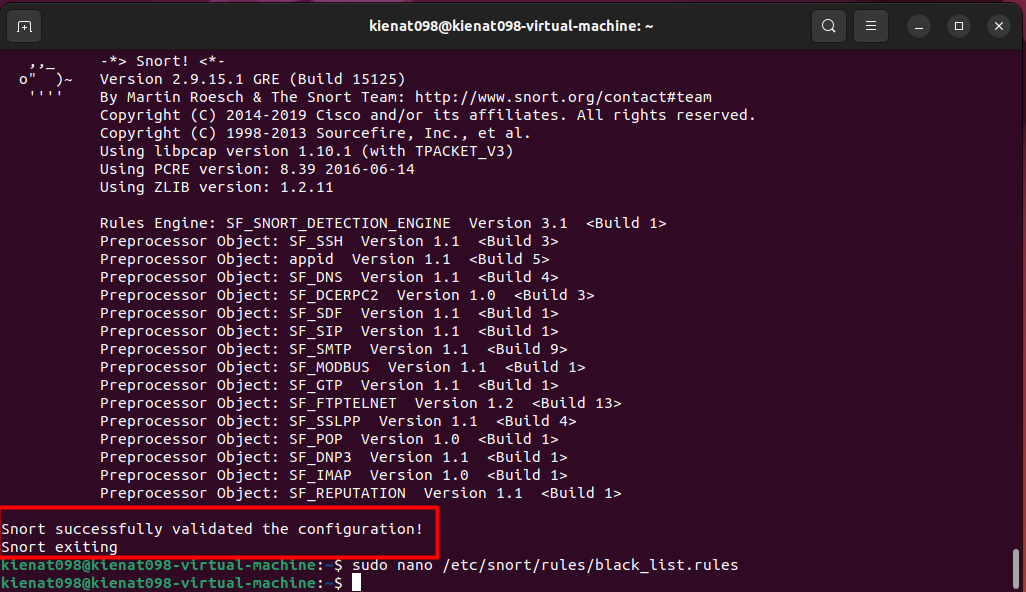
*sudo nano /etc/snort/rules/black\_list.rules*

*sudo nano /etc/snort/rules/white\_list.rules*



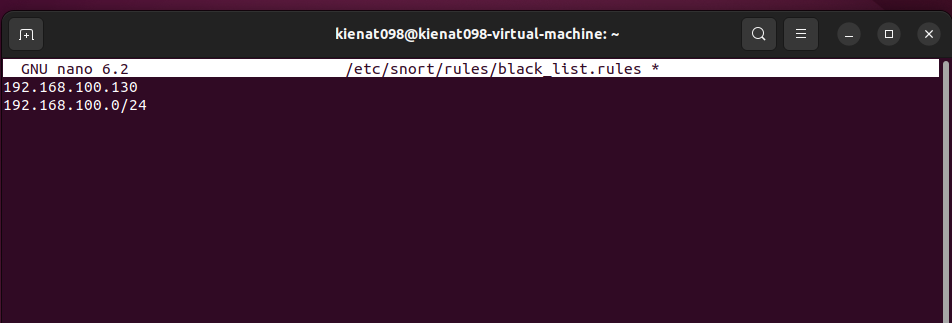
- Sau khi cấu hình xong, kiểm tra xem file snort.config có lỗi không.

*sudo snort -T -c /etc/snort/snort.conf -i ens33*

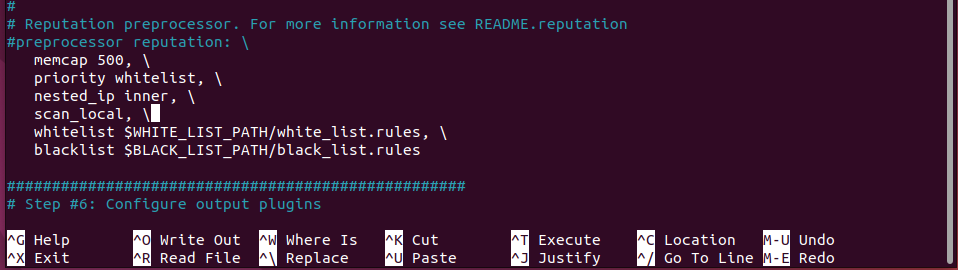


# Thêm mục nhập vào danh sách IP theo cách thủ công

* + Snort có thể dễ dàng tải nhiều whitelist và blacklist. Danh sách phải là tài liệu văn bản có địa chỉ IP đơn giản (chỉ định một máy chủ) hoặc địa chỉ IP ở định dạng CIDR, với một mục nhập trên mỗi dòng. Có thể có nhận xét đầy đủ và nội tuyến bằng cách sử dụng ký hiệu băm (#).



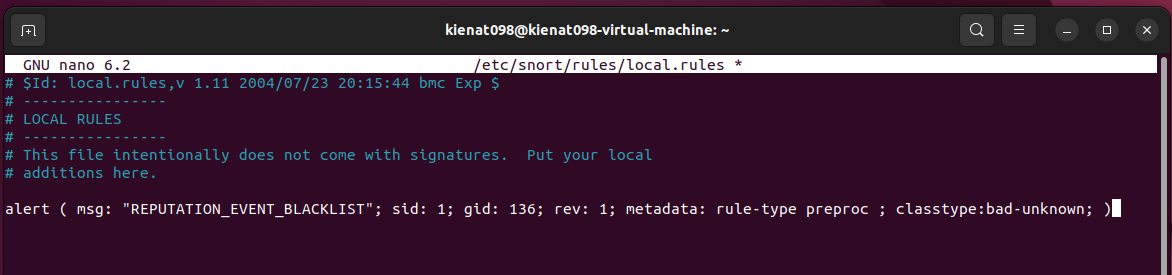
* + Sau đó thêm tùy chọn scan\_local vào bộ tiền xử lý danh tiếng.



* + Thiết lập local.rules để tạo cảnh báo cho các sự kiện trong blacklist.

alert ( msg: "REPUTATION\_EVENT\_BLACKLIST"; sid: 1; gid: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )

* + Các quy tắc có GID 136 là các quy tắc được kích hoạt bởi bộ tiền xử lý danh tiếng.



# Chạy snort

# Máy tấn công

# 

* + Bắt đầu Snort bằng lệnh sẽ tạo cảnh báo cho bảng điều khiển:

*sudo snort -i ens33 -q -A console -c /etc/snort/snort.conf*

* + Từ máy có địa chỉ 192.168.150.128 ping đến máy snort sẽ hiện cảnh báo.

