﻿Sau khi cài đặt xong snort, ta cấu hình cho snort để chạy dưới chế độ NIDS

1. Tạo snort user và group.

sudo groupadd snort

sudo useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort

2. Tạo thư mục Snort

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/rules/iplists

sudo mkdir /etc/snort/preproc\_rules

sudo mkdir /usr/local/lib/snort\_dynamicrules

sudo mkdir /etc/snort/so\_rules

3. Tạo một số file chứa rule và ip list

sudo touch /etc/snort/rules/iplists/black\_list.rules

sudo touch /etc/snort/rules/iplists/white\_list.rules

sudo touch /etc/snort/rules/local.rules

sudo touch /etc/snort/sid-msg.map

4. Tạo file logg

sudo mkdir /var/log/snort

sudo mkdir /var/log/snort/archived\_logs

5.Cấp quyền

sudo chmod -R 5775 /etc/snort

sudo chmod -R 5775 /var/log/snort

sudo chmod -R 5775 /var/log/snort/archived\_logs

sudo chmod -R 5775 /etc/snort/so\_rules

sudo chmod -R 5775 /usr/local/lib/snort\_dynamicrules

6. Thay đổi quyền sở hữu

sudo chown -R snort:snort /etc/snort

sudo chown -R snort:snort /var/log/snort

sudo chown -R snort:snort /usr/local/lib/snort\_dynamicrules

7. Copy một số file mẫu

cd ~/snort\_src/snort-2.9.20/etc/

sudo cp \*.conf\* /etc/snort

sudo cp \*.map /etc/snort

sudo cp \*.dtd /etc/snort

cd ~/snort\_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/

sudo cp \* /usr/local/lib/snort\_dynamicpreprocessor/

8. Chỉnh sửa file cấu hình snort "/etc/snort/snort.conf"

sudo sed -i "s/include \$RULE\\_PATH/#include \$RULE\\_PATH/" /etc/snort/snort.conf

sudo nano /etc/snort/snort.conf

- Chỉnh sửa dòng 45: thành địa chỉ lớp mạng và subnet-mask của máy Snort

- Chỉnh sửa dòng 104: thành các đường dẫn đã tạo ở trước

- Bỏ comment line ở dòng: 546: để chạy file rule local.rules

Chạy kiểm tra: sudo snort -T -i ens33 -c /etc/snort/snort.conf

9. Viết 1 rule đơn giản: cảnh báo gói ICMP

- Thêm rule vào file "/etc/snort/rules/local.rules"

alert icmp any any -> $HOME\_NET any (msg:"Co ai do dang ping"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

- Thêm dòng sau vào file "etc/snort/sid-msg.map"

#v2

1 || 10000001 || 001 || icmp-event || 0 || ICMP Test detected || url,tools.ietf.org/html/rfc792

- Kiểm tra Snort: sudo snort -T -c /etc/snort/snort.conf -i ens33

- Chạy Snort: sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

- Sang máy khác để ping đển máy Snort, xem kết quả.