﻿Hướng dẫn cài dặt snort trên Ubuntu

Demo sử dụng bản Ubuntu 16.04LTS và cài dặt snort bản snort-2.9.11.1

Bước 1:

- Cài dặt và nâng cấp hệ thống -chạy các lệnh sau:

sudo apt-get update

sudo apt-get dist-upgrade -y

sudo apt-get install -y openssh-server

Khởi động lại hệ thống:

sudo reboot

Bước 2: Cấu hình card mạng

- Chúng ta tắt LRO và GRO và sử dụng công cụ ethtool:

Vào sửa file interfaces, bằng cách chạy lệnh:

sudo vim /etc/network/interfaces (có thể thay vim bằng nano)

Thêm vào file 2 dòng sau:

post-up ethtool -K ens33 gro off

post-up ethtool -K ens33 lro off

Khởi động lại networking nếu không được thì khởi động lại máy.

sudo service networking restart (Ubuntu 16.04 trở về trước)

Kiểm tra:

sudo ifconfig ens33 down && sudo ifconfig ens33 up

ethtool -k ens33 | grep receive-offload

kết quả như sau tức đã thành công:

generic-receive-offload: off

large-receive-offload: off

Bước 3: Cài đặt các gói cần thiết cho Snort

sudo apt-get install -y build-essential

sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev

sudo apt-get install -y bison flex

Tạo thư mục riêng cho snort

mkdir ~/snort\_src

cd ~/snort\_src

Cài đặt gói DAQ:

cd ~/snort\_src

wget https://snort.org/downloads/snort/daq-2.0.7.tar.gz

tar -xvzf daq-2.0.7.tar.gz

cd daq-2.0.7

./configure

make

sudo make install

Bước 4: cài đặt snort

sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev

với Ubuntu 16: sudo apt-get install -y libnghttp2-dev

Ubutu 14:

sudo apt-get install -y autoconf libtool pkg-config

cd ~/snort\_src

wget https://github.com/nghttp2/nghttp2/releases/download/v1.17.0/nghttp2-1.17.0.tar.gz

tar -xzvf nghttp2-1.17.0.tar.gz

cd nghttp2-1.17.0

autoreconf -i --force

automake

autoconf

./configure --enable-lib-only

make

sudo make install

Cài đặt snort-2.9.11.1

cd ~/snort\_src

wget https://snort.org/downloads/snort/snort-2.9.20.tar.gz

tar -xvzf snort-2.9.20.tar.gz

cd snort-2.9.20

./configure --enable-sourcefire

make

sudo make install

Chạy thử kiểm tra Snort

sudo ldconfig

sudo ln -s /usr/local/bin/snort /usr/sbin/snort

snort -V