**HƯỚNG DẪN CÀI ĐẶT SNORT MACHINE LEARNING**

1. **Yêu cầu tiên quyết**

Snort3 Alpha ở Ubuntu 14 và 16. Hướng dẫn dưới đây có thể không hoạt động ở Ubuntu 12. Phiên bản Snort3 là phiên bản alpha nên nó có thể chứa một số lỗi và tùy thuộc vào những phiên bản khác nhau có thể yêu cầu thêm những thư viện bổ sung. Hướng dẫn dưới đây được viết và sử dụng ở phiên bản Snort 3.0.0-a4.

1. **Cài đặt Snort 3**

Đầu tiên phải đảm bảo hệ thống được cập nhập phân bản mới nhất.

|  |
| --- |
| sudo apt-get update && sudo apt-get dist-upgrade -y |

Cài đặt những gói cần thiết để chạy Snort3

sudo apt-get install -y build-essential autotools-dev libdumbnet-dev libluajit-5.1-dev libpcap-dev \

libpcre3-dev zlib1g-dev pkg-config libhwloc-dev cmake

Tiếp theo cài thêm những công cụ phát triển (tùy chọn nhưng khuyến khích cài)

sudo apt-get install -y liblzma-dev openssl libssl-dev cpputest libsqlite3-dev uuid-dev

Để cài đặt Snort từ github repository ta cần một số công cụ như sau

sudo apt-get install -y libtool git autoconf

Snort DAQ (Data Acquisition library) đây là một trong những gói tin cần thiết để cài đặt snort:

sudo apt-get install -y bison flex

sudo apt-get install -y libnetfilter-queue-dev

Chúng ta sẽ tài một số tarballs từ những nguồn khác nhau nên ta cần lưu chúng vào một folder

mkdir ~/snort\_src

cd ~/snort\_src

Cài đặt safec phục vụ cho việc biên dịch thư viện ngôn ngữ C

cd ~/snort\_src

wget https://downloads.sourceforge.net/project/safeclib/libsafec-10052013.tar.gz

tar -xzvf libsafec-10052013.tar.gz

cd libsafec-10052013

./configure

make

sudo make install

Snort3 sẽ dùng Hyperscan để cho việc quét và tìm kiếm:

cd ~/snort\_src

wget http://www.colm.net/files/ragel/ragel-6.10.tar.gz

tar -xzvf ragel-6.10.tar.gz

cd ragel-6.10

./configure

make

sudo make install

Hyperscan yêu cầu phải có thư viện Boost C++. Ghi chú: Ở đây chúng ta không sử dụng Ubutnu repository phiên bản boost headers (libboost-all-dev) bởi vì Hyperscan yêu cầu thư viện boost phiên bản 1.58 và các Ubuntu repository có thể khá cũ. Để tài thư viện Boost 1.65.1, nhưng không cài đặt

cd ~/snort\_src

wget https://dl.bintray.com/boostorg/release/1.65.1/source/boost\_1\_65\_1.tar.gz

tar -xvzf boost\_1\_65\_1.tar.gz

Cài đặt Hyperscan 4.6.0 từ source

cd ~/snort\_src

wget https://github.com/intel/hyperscan/archive/v4.6.0.tar.gz

tar -xvzf v4.6.0.tar.gz

mkdir ~/snort\_src/hyperscan-4.6.0-build

cd hyperscan-4.6.0-build/

cmake -DCMAKE\_INSTALL\_PREFIX=/usr/local -DBOOST\_ROOT=~/snort\_src/boost\_1\_65\_1/ ../hyperscan-4.6.0

make

sudo make install

Nếu ta muốn kiểm tra Hyperscan có hoạt động hay không, từ thư mục build chạy lệnh:

cd ~/snort\_src/hyperscan-4.6.0-build/

./bin/unit-hyperscan

Snort cũng yêu cầu cài đặt flatbuffers

cd ~/snort\_src

wget https://github.com/google/flatbuffers/archive/master.tar.gz -O flatbuffers-master.tar.gz

tar -xvzf flatbuffers-master.tar.gz

mkdir flatbuffers-build

cd flatbuffers-build

cmake ../flatbuffers-master

make

sudo make install

Tiếp theo cài đặt thư viện DataAcQuisition (DAQ) từ trang web Snort. Ghi chú: Snort 3 sử dụng phiên bản DAQ khác với snort 2.9.x.x

cd ~/snort\_src

wget https://www.snort.org/downloads/snortplus/daq-2.2.2.tar.gz

tar -xvzf daq-2.2.2.tar.gz

cd daq-2.2.2

./configure

make

sudo make install

Cập nhập lại shared libraries:

sudo ldconfig

Tải và cài đặt Snort3 master từ github và cài đặt:

cd ~/snort\_src

git clone git://github.com/snortadmin/snort3.git

cd snort3

./configure\_cmake.sh --prefix=/opt/snort

cd build

make

sudo make install

Ta có thể kiểm tra Snort bằng cách chạy

noah@snort3:~$ /opt/snort/bin/snort -V  
,,\_ -\*> Snort++ <\*-  
o" )~ Version 3.0.0 (Build 241) from 2.9.11  
'''' By Martin Roesch & The Snort Team  
http://snort.org/contact#team  
Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using DAQ version 2.2.2  
Using LuaJIT version 2.0.4  
Using OpenSSL 1.0.2g 1 Mar 2016  
Using libpcap version 1.7.4  
Using PCRE version 8.38 2015-11-23  
Using ZLIB version 1.2.8  
Using FlatBuffers 1.7.0  
Using Hyperscan version 4.6.0 2017-12-03  
Using LZMA version 5.1.0alpha

Cuối cùng, ta có thể tạo soft link đến snort /usr/sbin

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

**3. Chạy Snort**

Snort 3 yêu cầu miến môi trường để vận hành chính xác.

export LUA\_PATH=/opt/snort/include/snort/lua/\?.lua\;\;

export SNORT\_LUA\_PATH=/opt/snort/etc/snort

sh -c "echo 'export LUA\_PATH=/opt/snort/include/snort/lua/\?.lua\;\;' >> ~/.bashrc"

sh -c "echo 'export SNORT\_LUA\_PATH=/opt/snort/etc/snort' >> ~/.bashrc"

Để đảm bảo biến môi trường vẫn có thể sử dụng khi dùng sudo, ta có thể thêm nó vào sudoers file

sudo visudo

Thêm dòng sau ở cuối

Defaults env\_keep += "LUA\_PATH SNORT\_LUA\_PATH"

Ta có thể kiểm tra Snort với file cấu hình mặc định:

/opt/snort/bin/snort -c /opt/snort/etc/snort/snort.lua

Nếu chạy thành công ta sẽ nhận được thông báo sau

Snort successfully validated the configuration.

o")~ Snort exiting

**4. Cài đặt locations**

Khi ta chạy **./configure –prefix=/opt/snort** ta có thể gọi snort cài đặt tết cả các files ở thư mục /opt/snort.

Sau khi hoàn thành cài đặt snort ta cài đặt python server

Yêu cầu: Python 3++

sudo add-apt-repository ppa:jonathonf/python-3.6

sudo apt-get update

sudo apt-get install python3.6

Tham khảo: http://ubuntuhandbook.org/index.php/2017/07/install-python-3-6-1-in-ubuntu-16-04-lts/

Cài đặt thư viện pandas

pip install pandas

Đặt biến môi trường để thuận tiện cho việc sử dụng

export my\_path=/usr/local

export PKG\_CONFIG\_PATH=$my\_path/lib/pkgconfig

export SNORT\_LUA\_PATH=$my\_path/etc/snort

export LUA\_PATH=$my\_path/include/snort/lua/\?.lua\;\;

1. **Cài đặt Snort Plugin**

Thêm hai dòng sau vào cmake để có thể biên dịch plugin ở extra/src/cmakelist.txt

add\_subdirectory ( inspectors )

Cài đặt plugin ở thư mục extra

wget -O snort3\_extra.tar.gz <https://github.com/snort3/snort3_extra/archive/master.tar.gz>

tar -xzvf snort3\_extra.tar.gz

copy toàn bộ thư mục extractor vào snort3\_extra-master/src/inspectors/dpx/extractor

mv extractor snort3\_extra-master/src/inspectors/dpx/extractor

Sau đó thêm các file CMakeLists.txt dpx.cc packet\_generated.h vào trong snort3\_extra-master/src/inspectors/dpx/

mv CMakeLists.txt dpx.cc packet\_generated.h -t snort3\_extra-master/src/inspectors/dpx/

Chạy lệnh sau để cài đặt plug in

export PKG\_CONFIG\_PATH=/opt/snort/lib/pkgconfig/ && cd snort3\_extra-master && ./configure\_cmake.sh --prefix=/opt/snort && cd build && make && make install

Hiển thị danh sách plugins được cài đặt

$my\_path/bin/snort --list-plugins

Thay đổi snort.lua để chạy plugin

cd $my\_path/etc/snort

sudo gedit snort.lua

Thêm vào trong snort.lua plugin dpx

dpx = { port = '80' }

example: plugin\_name = { } //use plugin with name plugin\_name with default option

Để có thể sử dụng được snort plug in lắng nghe mọi kết nối trên mạng ta dùng lệnh

sudo $my\_path/bin/snort -c $my\_path/etc/snort/snort.lua --plugin-path /usr/local/snort/lib/snort\_extra -i ens33

Cài đặt gói sau để biên dịch c++ file

apt-get install libcurl4-openssl-dev

1. **Cài đặt python-pip**

sudo apt install python-pip

Chạy python server

Vào thư mục chứa source code

cd ids-machine-learning

Cài đặt môi trường ảo (nhằm cô lập môi trường phát triển của project, không làm ảnh hướng tới project khác)

pip install virtualenv

virtualenv env

source env/bin/activate

Cài đặt những gói cần thiết

pip install -r requirements.txt

Chạy python

python main.py

Thử tấn công bằng công cụ hping3

sudo hping3 --rand-source --udp -p 5000 -i u50 -d 10 victimIP