# I. Cài đặt Nginx, modsecurity, EFK stack trên Ubuntu Server 18.04.3 LTS

## 1. Cài đặt Nginx

* Tiến hành cài đặt các công cụ hỗ trợ

sudo apt install -y apt-utils autoconf automake build-essential git libcurl4-openssl-dev libgeoip-dev liblmdb-dev libpcre++-dev libtool libxml2-dev libyajl-dev pkgconf wget zlib1g-dev curl gnupg2 ca-certificates lsb-release git

* Để cài đặt nginx từ mainline tiến hành thêm dòng lệnh sau:

echo "deb http://nginx.org/packages/mainline/debian `lsb\_release -cs` nginx" | sudo tee /etc/apt/sources.list.d/nginx.list

* Tiếp theo, nhập nginx signing key để apt có thể xác minh tính xác thực của các gói:

curl -fsSL https://nginx.org/keys/nginx\_signing.key | sudo apt-key add –

* Xác minh khóa thích hợp:

sudo apt-key fingerprint ABF5BD827BD9BF62

* Tiến hành cài đặt nginx

sudo apt update && sudo apt install nginx

## 2. Biên dịch và cài đặt modsecurity

* Tại thư mục làm việc tiến hành clone modsecurity repository

git clone --depth 1 -b v3/master --single-branch <https://github.com/SpiderLabs/ModSecurity>

* Thay đổi thư mục ModSecurity và biên dịch mã nguồn:

cd ModSecurity &&

git submodule init &&

git submodule update &&

./build.sh &&

./configure &&

make &&

make install

* Tải xuống Trình kết nối NGINX cho ModSecurity và Biên dịch nó dưới dạng Mô-đun động:

git clone --depth 1 <https://github.com/SpiderLabs/ModSecurity-nginx.git>

* Kiểm tra phiên bản nginx hiện tại:

nginx –v

nginx version: nginx/1.17.6

* Tải xuống mã nguồn tương ứng với phiên bản NGINX đã cài đặt

wget <http://nginx.org/download/nginx-1.13.1.tar.gz> &&

tar zxvf nginx-1.13.1.tar.gz

* Biên dịch mô-đun động và sao chép nó vào thư mục tiêu chuẩn cho các mô-đun:

cd nginx-1.13.1 &&

./configure --with-compat --add-dynamic-module=../ModSecurity-nginx &&

make modules &&

cp objs/ngx\_http\_modsecurity\_module.so /etc/nginx/modules

* Thêm chỉ thị [load\_module](https://nginx.org/en/docs/ngx_core_module.html#load_module) vào đầu file  **/etc/nginx/nginx.conf**

load\_module modules/ngx\_http\_modsecurity\_module.so;

* Thiết lập tệp cấu hình ModSecurity  được đề xuất bởi TrustWave Spiderlabs, nhà tài trợ của công ty ModSecurity.

mkdir /etc/nginx/modsec &&

wget -P /etc/nginx/modsec/ https://raw.githubusercontent.com/SpiderLabs/ModSecurity/v3/master/modsecurity.conf-recommended &&

mv /etc/nginx/modsec/modsecurity.conf-recommended /etc/nginx/modsec/modsecurity.conf

* Thay đổi chỉ thị SecRuleEngine trong cấu hình để thay đổi từ chế độ chỉ phát hiện mặc định của chế độ mật khẩu sang chế độ chủ động bỏ lưu lượng độc hại

sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/' /etc/nginx/modsec/modsecurity.conf

* Thêm chỉ thị Include "/etc/nginx/modsec/modsecurity.conf" vào file **/etc/nginx/modsec/main.conf**
* Thêm các chỉ thị modsecurity và modsecurity\_rules\_file vào cấu hình NGINX để bật ModSecurity:

server {

# ...

modsecurity on;

modsecurity\_rules\_file /etc/nginx/modsec/main.conf;

}

## 3. Thêm CRS cho Modsecurity

* Dowload CRS từ github:

wget https://github.com/SpiderLabs/owasp-modsecurity-crs/archive/v3.0.2.tar.gz

&&

tar -xzvf v3.0.2.tar.gz

* Thay đổi extension của file để kích hoạt rule

cp /usr/local/owasp-modsecurity-crs-3.0.2/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example /usr/local/owasp-modsecurity-crs-3.0.2/rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf

&&

cp /usr/local/owasp-modsecurity-crs-3.0.2/rules/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example /usr/local/owasp-modsecurity-crs-3.0.2/rules/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf

&&

cp /usr/local/owasp-modsecurity-crs-3.0.2/rules/crs-setup.conf.example  /usr/local/owasp-modsecurity-crs-3.0.2/rules/crs-setup.conf

* Load lại cấu hình nginx

Nginx –t && nginx –s reload