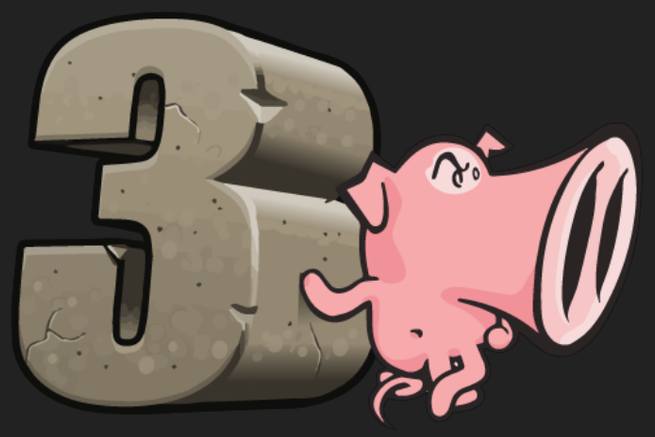
GUIA DE INSTALAÇÃO E TESTE

SNORT 3



PREPARAÇÃO

- **Atualização de updates;**
- `sudo apt-get update && sudo apt-get dist-upgrade -y`
- **Criação da pasta p/ armazenar os pré-requisitos;**
- `mkdir ~/snort_src`
- `cd ~/snort_src`

PREPARAÇÃO

- **Instalação dos pré-requisitos;**

- `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`

- **Instalação do cmake (Ubuntu 16 e 18);**

- `sudo apt-get install -y cmake`

PREPARAÇÃO

- **Instalação do cmake (Ubuntu 14);**
- `sudo apt-get remove -y cmake`
- `cd ~/snort_src`
- `wget https://cmake.org/files/v3.10/cmake-3.10.3.tar.gz`
- `tar -xzvf cmake-3.10.3.tar.gz`
- `cd cmake-3.10.3`
- `./bootstrap`
- `make`
- `sudo make install`

PREPARAÇÃO

- **Instalação de opcionais (porém recomendados);**
- `sudo apt-get install -y liblzma-dev openssl libssl-dev cpputest libsqlite3-dev uuid-dev`
- **Instalação de ferramentas p/ poder instalar o Snort do Github;**
- `sudo apt-get install -y libtool git autoconf`

PREPARAÇÃO

- **Instalação dos pré-requisitos do Snort DAQ (Data Acquisition Library);**
- `sudo apt-get install -y bison flex`
- **Instalação de pacotes;**
- `sudo apt-get install -y libnetfilter-queue-dev`

PREPARAÇÃO

- **Instalação do safec;**
- `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`

PREPARAÇÃO

- **Instalação do gperftools;**
- `cd ~/snort_src`
- `wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.7/gperftools-2.7.tar.gz`
- `tar xzvf gperftools-2.7.tar.gz`
- `cd gperftools-2.7`
- `./configure`
- `make`
- `sudo make install`

PREPARAÇÃO

- **O Snort 3 utiliza o Hyperscan p/ *fast pattern matching;***
- **O Hyperscan requer a instalação do Ragel e da Boost lib.;**
- `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`

PREPARAÇÃO

- `cd ~/snort_src`
- `wget https://dl.bintray.com/boostorg/release/1.67.0/source/boost_1_67_0.tar.gz`
- `tar -xvzf boost_1_67_0.tar.gz`

PREPARAÇÃO

- **Instalação do Hyperscan;**
- `cd ~/snort_src`
- `wget https://github.com/intel/hyperscan/archive/v4.7.0.tar.gz`
- `tar -xvzf v4.7.0.tar.gz`
- `mkdir ~/snort_src/hyperscan-4.7.0-build`
- `cd hyperscan-4.7.0-build/`
- `cmake -DCMAKE_INSTALL_PREFIX=/usr/local -DBOOST_ROOT=~/snort_src/boost_1_67_0/ ../hyperscan-4.7.0`
- `make`
- `sudo make install`

PREPARAÇÃO

- **Verificação da instalação do Hyperscan;**
- `cd ~/snort_src/hyperscan-4.7.0-build/`
- `./bin/unit-hyperscan`

PREPARAÇÃO

- **Instalação do flatbuffers;**
- `cd ~/snort_src`
- `wget https://github.com/google/flatbuffers/archive/v1.9.0.tar.gz -O flatbuffers-v1.9.0.tar.gz`
- `tar -xzvf flatbuffers-1.9.0.tar.gz`
- `mkdir flatbuffers-build`
- `cd flatbuffers-build`
- `cmake ../flatbuffers-1.9.0`
- `make`
- `sudo make install`

PREPARAÇÃO

- **Instalação do Snort DAQ;**
- `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`

PREPARAÇÃO

- **Atualização das bibliotecas compartilhadas;**
- `sudo ldconfig`

INSTALAÇÃO

- **Clonagem do últ. Snort no Github e Instalação;**
- `cd ~/snort_src`
- `git clone git://github.com/snortadmin/snort3.git`
- `cd snort3`
- `./configure_cmake.sh --prefix=/usr/local —enable-tcmalloc`
- `cd build`
- `make`
- `sudo make install`

INSTALAÇÃO

- **Verificação da instalação do Snort;**
- `/usr/local/bin/snort -V`
- **Criação de um link p/ o Snort em /usr/local/bin;**
- `sudo ln -s /usr/local/bin/snort /usr/local/sbin/snort`

INSTALAÇÃO

- **Configuração de variáveis de ambiente;**
- `export LUA_PATH=/usr/local/include/snort/lua/\?.lua\;\;`
- `export SNORT_LUA_PATH=/usr/local/etc/snort`
- `sh -c "echo 'export LUA_PATH=/usr/local/include/snort/lua/\?.lua\;\;' >> ~/.bashrc"`
- `sh -c "echo 'export SNORT_LUA_PATH=/usr/local/etc/snort' >> ~/.bashrc”`

INSTALAÇÃO

- **Para deixar essas variáveis disponíveis quando o “sudo” for utilizado, é preciso adicioná-las no arquivo /etc/sudoers;**
- `sudo visudo`
- **Na última linha:**
- `Defaults env_keep += "LUA_PATH SNORT_LUA_PATH”`

INSTALAÇÃO

- **Validação do Snort com o arquivo de configuração padrão;**
- `snort -c /usr/local/etc/snort/snort.lua`

INSTALAÇÃO

- **Instalação de regras no Snort;**
- `cd ~/snort_src/`
- `wget https://www.snort.org/downloads/community/snort3-community-rules.tar.gz`
- `tar -xvzf snort3-community-rules.tar.gz`
- `cd snort3-community-rules`
- `sudo mkdir /usr/local/etc/snort/rules`
- `sudo mkdir /usr/local/etc/snort/builtin_rules`
- `sudo mkdir /usr/local/etc/snort/so_rules`
- `sudo mkdir /usr/local/etc/snort/lists`
- `sudo cp snort3-community.rules /usr/local/etc/snort/rules/`
- `sudo cp sid-msg.map /usr/local/etc/snort/rules/`

INSTALAÇÃO

- **Validação do Snort com o arquivo de regras;**

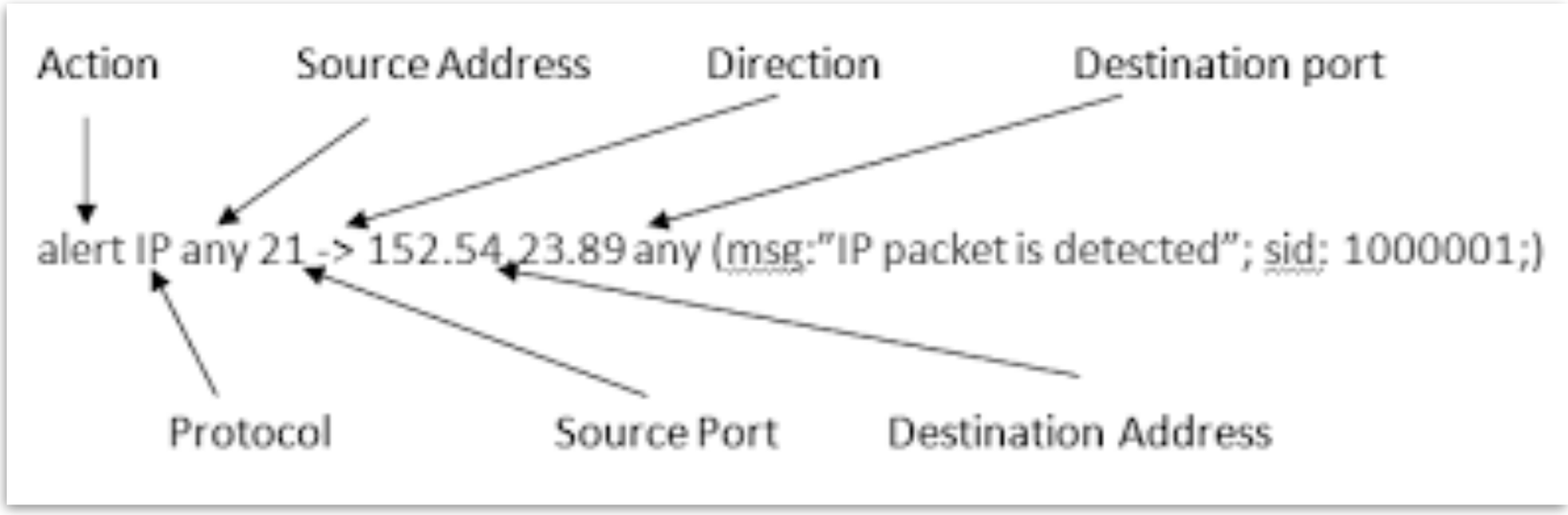
- `snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/snort/rules/snort3-community.rules`

TESTE

- **Para testar as regras do Snort, recomenda-se a criação de um novo arquivo de regras;**
- `sudo nano /usr/local/etc/snort/rules/custom.rules`

TESTE

- **Toda regra no Snort segue a seguinte estrutura;**



TESTE

- **Para a criação de uma regra para detecção de conexões FTP, basta inserir no arquivo custom.rules:**

- `alert tcp any 21 -> any any ( msg:"FTP Test”; sid:1000001; rev:1; )`

- **E então, executar:**

- `sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/snort/rules/custom.rules -i <interface> -A alert_full`

- **A interface pode ser consultada c/ o comando:**

- `ifconfig`

TESTE

- **Com o Snort em execução, utilize um outro terminal (na mesma máquina ou em outra) e inicie a conexão FTP:**
- `ftp <ip da máquina com snort em execução>`
- **No terminal com o Snort em execução, um novo alerta deverá ser gerado;**
- **Obs.: Se o teste for realizado em uma única máquina, execute o Snort sobre a interface local (e.g. "lo");**

TESTE

- **Para a criação de uma regra para detecção de pings ICMP, basta inserir no arquivo custom.rules:**

- `alert icmp any any -> any any ( msg:"ICMP Test"; sid:1000002; rev:1; )`

- **E então, executar:**

- `sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/snort/rules/custom.rules -i <interface> -A alert_full`

TESTE

- **Com o Snort em execução, utilize um outro terminal (na mesma máquina ou em outra) e realize o ping ICMP:**
- `ping <ip da máquina com snort em execução>`
- **No terminal com o Snort em execução, um novo alerta deverá ser gerado;**
- **Obs.: Se o teste for realizado em uma única máquina, execute o Snort sobre a interface local (e.g. “lo");**

TESTE

- **Além dessas opções, o Snort disponibiliza muitas outras, por exemplo, “content”, que permite realizar buscas nos payloads dos pacotes processados pelo IDS:**

- `alert ip any any -> any any ( msg:"IP Test"; content:”unesp”; :sid:1000003; rev:1; )`

- **Em seguida, para testá-la, acesse o site:**

- **http://www.unesp.br**

- **Todos os pacotes que tiverem o conteúdo "unesp" no payload gerarão alertas;**

REFERÊNCIAS

- **Snort 3 User Guide.** Disponível em: <https://www.snort.org/documents>.