### Créer une image Docker pour Snort

1. \*\*Créer un fichier Dockerfile :\*\*

- Créez un répertoire pour votre projet Docker :

```bash

mkdir snort-docker

cd snort-docker

```

- Créez un fichier nommé `Dockerfile` avec le contenu suivant :

```Dockerfile

FROM ubuntu:20.04

# Installer les dépendances

RUN apt-get update && apt-get install -y \

build-essential \

libpcap-dev \

libpcre3-dev \

libdumbnet-dev \

bison \

flex \

zlib1g-dev \

liblzma-dev \

openssl \

libssl-dev \

wget \

tar

# Télécharger et installer Snort

RUN wget https://www.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 && \

make install && \

ldconfig

# Créer les répertoires de configuration

RUN mkdir -p /etc/snort/rules /etc/snort/preproc\_rules /var/log/snort /usr/local/lib/snort\_dynamicrules

# Copier les fichiers de configuration

COPY snort.conf /etc/snort/snort.conf

COPY local.rules /etc/snort/rules/local.rules

# Exposer le port utilisé par Snort

EXPOSE 2525

# Commande par défaut pour exécuter Snort

CMD ["snort", "-c", "/etc/snort/snort.conf", "-i", "eth0"]

```

2. \*\*Créer des fichiers de configuration :\*\*

- Créez un fichier `snort.conf` avec une configuration de base :

```plaintext

var RULE\_PATH /etc/snort/rules

var SO\_RULE\_PATH /etc/snort/so\_rules

var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules

var WHITE\_LIST\_PATH /etc/snort/rules

var BLACK\_LIST\_PATH /etc/snort/rules

include $RULE\_PATH/local.rules

output unified2: filename snort.log, limit 128

```

- Créez un fichier `local.rules` pour définir des règles locales :

```plaintext

alert icmp any any -> any any (msg:"ICMP Packet"; sid:1000001; rev:1;)

```

3. \*\*Construire l'image Docker :\*\*

- Exécutez la commande suivante pour construire l'image Docker :

```bash

docker build -t custom-snort .

```

### Exécuter Snort avec Docker

1. \*\*Exécuter le conteneur Snort :\*\*

- Exécutez la commande suivante pour démarrer le conteneur Snort :

```bash

docker run --rm --net=host --cap-add=NET\_ADMIN custom-snort

```

### Utiliser Elasticsearch, Logstash, et Kibana avec Docker

1. \*\*Télécharger les images Docker pour Elasticsearch, Logstash, et Kibana :\*\*

```bash

docker pull elasticsearch:7.13.2

docker pull logstash:7.13.2

docker pull kibana:7.13.2

```

2. \*\*Créer un réseau Docker pour les conteneurs ELK :\*\*

```bash

docker network create elk

```

3. \*\*Démarrer Elasticsearch :\*\*

```bash

docker run -d --name elasticsearch --net elk -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" elasticsearch:7.13.2

```

4. \*\*Démarrer Logstash avec une configuration pour Snort :\*\*

- Créez un fichier de configuration `logstash.conf` avec le contenu suivant :

```plaintext

input {

file {

path => "/var/log/snort/alert"

start\_position => "beginning"

sincedb\_path => "/dev/null"

}

}

filter {

grok {

match => { "message" => "%{SYSLOGTIMESTAMP:timestamp} %{IP:src\_ip} -> %{IP:dst\_ip} %{WORD:protocol} %{GREEDYDATA:message}" }

}

}

output {

elasticsearch {

hosts => ["elasticsearch:9200"]

index => "snort-alerts-%{+YYYY.MM.dd}"

}

stdout { codec => rubydebug }

}

```

- Démarrez Logstash en montant le fichier de configuration :

```bash

docker run -d --name logstash --net elk -v $(pwd)/logstash.conf:/usr/share/logstash/pipeline/logstash.conf logstash:7.13.2

```

5. \*\*Démarrer Kibana :\*\*

```bash

docker run -d --name kibana --net elk -p 5601:5601 kibana:7.13.2

```

### Installer Grafana avec Docker

1. \*\*Télécharger l'image Docker de Grafana :\*\*

```bash

docker pull grafana/grafana

```

2. \*\*Démarrer Grafana :\*\*

```bash

docker run -d --name grafana -p 3000:3000 grafana/grafana

```

### Configuration de Grafana

1. \*\*Accéder à Grafana :\*\*

- Ouvrez un navigateur web et accédez à `http://localhost:3000`.

- Connectez-vous avec les identifiants par défaut (admin/admin) et changez le mot de passe.

2. \*\*Ajouter Elasticsearch comme source de données :\*\*

- Allez dans `Configuration` -> `Data Sources` -> `Add data source`.

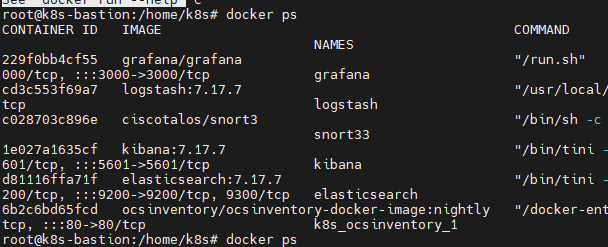
- Sélectionnez `Elasticsearch` et configurez l’URL à `http://elasticsearch:9200`.

- Définissez `Index name` à `snort-alerts-\*` et cliquez sur `Save & Test`.

3. \*\*Créer un tableau de bord :\*\*

- Cliquez sur `Create` -> `Dashboard`.

- Ajoutez des panneaux (panels) pour visualiser les données des alertes Snort selon vos besoins.

.