Surveillance de l'exécution de commandes malveillantes

Docker automatise le déploiement de diverses applications dans des conteneurs logiciels. Le module **Wazuh** dédié à **Docker** détecte en temps réel les incidents de sécurité survenant dans ces conteneurs. Dans ce cas précis, la configuration de **Wazuh** vise à surveiller les événements **Docker** sur un point de terminaison **Ubuntu** qui héberge des conteneurs **Docker**.

I – Configuration du point de terminaison Ubuntu

1. Installation et activation de **Python** et **Pip** :
   - On commence par installer **Python** et **Pip** sur l'hôte **Ubuntu** :

```
sudo apt install python3 python3-pip
```

2. On met à jour **Pip** :

```
pip3 install --upgrade pip
```

3. On procède à l'installation de Docker et de la bibliothèque **Python Docker** :

```
curl -sSL https://get.docker.com/ | sh
sudo pip3 install docker==4.2.0 urllib3==1.26.18
```

4. On édite le fichier de configuration de l'agent **Wazuh /var/ossec/etc/ossec.conf** et on ajoute ce bloc pour activer le module **docker-listener** :

```
<ossec_config>
  <wodle name="docker-listener">
    <interval>10m</interval>
    <attempts>5</attempts>
    <run_on_start>yes</run_on_start>
    <disabled>no</disabled>
  </wodle>
</ossec_config>
```

5. On redémarre l'agent **Wazuh** :

```
sudo systemctl restart wazuh-agent
```

II – Test de la configuration

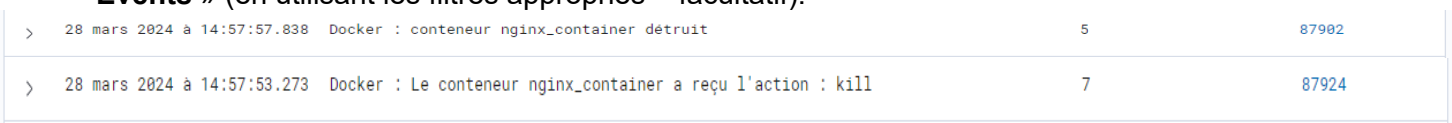
1. On effectue plusieurs activités **Docker**, comme extraire une image **Docker**, lancer une instance, exécuter d'autres commandes Docker, puis supprimer le conteneur.
   - On extrait une image, telle que l'image **NGINX**, et on exécute un conteneur :

```
sudo docker pull nginx
sudo docker run -d -P --name nginx_container nginx
sudo docker exec -it nginx_container cat /etc/passwd
sudo docker exec -it nginx_container /bin/bash
exit
```

2. On arrête et retire le conteneur :

```
sudo docker stop nginx_container
sudo docker rm nginx_container
```

- On accède au tableau de bord **Wazuh** et on consulte les alertes générées dans le module « **Security Events** » (en utilisant les filtres appropriés = facultatif).



Alertes événement Docker

Surveillance de l’exécution de commandes malveillantes