Jacquemart Paul

Suricata

4 septembre 20XX

Installation et Configuration de Suricata pour bloquer des attaques ssh

OBJECTIFS

- Installer et configurer Suricata
- Installer et configurer Fail2ban

© Paul Jacquemart 2024 CC BY-NC-ND 4.0 – Version du 2025-03-27

Sommaire

1. Introduction à Suricata

Suricata est un **système de détection (IDS)** et de **prévention (IPS)** d'intrusion open source. Il analyse le trafic réseau en temps réel pour repérer des comportements suspects ou malveillants, en s'appuyant sur des **règles de détection** prédéfinies ou personnalisées. Grâce à sa flexibilité, ses performances sur des réseaux à haut débit, et sa compatibilité avec les règles de Snort, Suricata est largement utilisé pour sécuriser les infrastructures.

Cas d'usage typiques :

- Surveillance de la sécurité réseau.
- Détection de malwares, exploits, et tentatives d'intrusion.
- Conformité aux politiques de sécurité.

---

2. Installation de Suricata sur Ubuntu

Voici les étapes pour installer Suricata sur un serveur Ubuntu via la ligne de commande.

2.1. Mise à jour du système

Avant toute installation, mettez à jour votre système :

```
sudo apt update
```

```
sudo apt upgrade -y
```

2.2. Installation de Suricata

Installez Suricata depuis les dépôts officiels d'Ubuntu :

```
sudo apt install suricata -y
```

3. Configuration initiale de Suricata

3.1. Édition du fichier de configuration

Ouvrez le fichier avec un éditeur comme **nano** :

sudo nano /etc/suricata/suricata.yaml

3.2. Configuration de l'interface réseau

Suricata doit surveiller une interface réseau spécifique (par exemple, **eth0**). Modifiez la section **af-packet** :

```
af-packet:
 - interface: eth0  # Remplacez par votre interface réseau
   threads: auto
   defrag: yes
   cluster-type: cluster_flow
   cluster-id: 99
   use-mmap: yes
```

Astuce : Pour identifier votre interface réseau :

ip link show

3.3. Démarrer le service au démarrage du serveur

sudo systemctl enable fail2ban

4. Configuration de Fail2Ban pour SSH

4.1. Installation de Fail2Ban

Si non installé :

sudo apt install fail2ban -y

4.2. Personnalisation des règles SSH

Ouvrir le fichier de configuration local :

cd /etc/fail2ban/

sudo nano /etc/fail2ban/jail.local

Modifiez les paramètres dans la section [sshd] :

[sshd]

banaction = iptables

enabled = true

maxretry = 5

findtime = 2m

bantime = 1m

port   = ssh

logpath = /var/log/auth.log

backend = %(sshd_backend)s

4.3. Redémarrez Fail2Ban

Appliquez les changements :

sudo systemctl restart fail2ban

Vérifiez le statut :

sudo systemctl status fail2ban