Documentation Crowdsec

Lucas MAIGNE

12/05/24

Développement :

Table des matières

Crowdsec

Qu'est-ce que CrowdSec ?

CrowdSec est une solution de sécurité open-source spécialisée dans la détection et la prévention des menaces en ligne. Elle utilise une approche collaborative pour collecter et partager des données sur les attaques afin de protéger les utilisateurs contre une variété de menaces, telles que les attaques par force brute, les tentatives d'intrusion, les attaques DDoS, etc. Cette solution analyse en temps réel les logs des serveurs, des applications et des dispositifs réseau pour identifier les comportements malveillants. En utilisant des scénarios de détection prédéfinis, des règles de sécurité et des listes de réputation, CrowdSec peut reconnaître les modèles d'attaques connus et inconnus. Une fois qu'une menace est détectée, CrowdSec peut prendre des mesures automatiques pour bloquer l'attaquant en utilisant des bouncers, qui sont des scripts ou des règles configurables pour bloquer ou limiter l'accès des attaquants. En résumé, CrowdSec offre une protection proactive contre les cybermenaces en identifiant, bloquant et partageant les informations sur les attaques en temps réel, contribuant ainsi à renforcer la sécurité des infrastructures informatiques.

Qu'est-ce qu'un Bouncer ?

Dans le contexte de CrowdSec, un bouncer est un mécanisme de réponse automatique aux menaces détectées. Il agit comme une couche de protection en prenant des mesures pour bloquer, limiter ou contrer les attaques sur les systèmes informatiques. Les bouncers de CrowdSec sont des scripts ou des règles configurables qui sont déployés pour réagir aux menaces détectées par le système. Ils peuvent inclure des actions telles que le blocage d'adresses IP, la modification de règles de pare-feu, la notification des administrateurs, ou d'autres mesures pour contrer les activités malveillantes. En résumé, les bouncers de CrowdSec sont des outils puissants qui permettent d'automatiser la réponse aux menaces en appliquant des actions défensives appropriées pour protéger les systèmes contre les attaques en ligne.

Création de la VM

Nous commençons par la création de la machine virtuelle Debian, vous avez le choix entre Debian 12 ou bien Ubuntu. Nous la laisserons configurée en mode NAT, ce qui lui permettra d'accéder à Internet. Cette connectivité Internet est essentielle pour installer les différents services, effectuer les mises à jour et obtenir les outils nécessaires pour la configuration.

Configuration de la VM

Ici je vais utiliser l'éditeur de texte par défaut « nano ». On commence par une mise à jour des paquets du système :

• sudo apt-get update && sudo apt-get upgrade -y

Nous allons désormais passer en mode administrateur pour faciliter les commandes tout au long de ce tutoriel. Il est essentiel de noter que cette pratique est uniquement spécifique à ce guide. Il est déconseillé de s'y habituer, car une manipulation incorrecte peut compromettre le fonctionnement de votre machine.

• su - root

Ensuite, nous allons ajouter le dépôt de l'outil pour accéder aux dernières mises à jour, ainsi qu'aux paquets et bouncers associés :

• curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh | sudo bash

La configuration initiale de la machine virtuelle est achevée. Nous allons désormais entamer l'installation et la configuration de CrowdSec sur cette machine.

Installation de CrowdSec

Ici je vais utiliser l'éditeur de texte par défaut « nano ». On commence par installer l'outil :

- apt-get install crowdsec -y

Installation d'un Bouncer

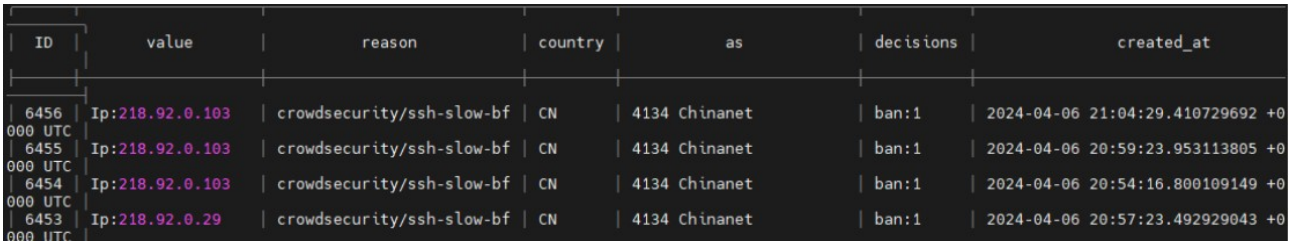
Comme définis précédemment, nous allons installer un Bouncer :

- apt install crowdsec-firewall-bouncer-iptables -y

Commandes utiles

Voici quelques commandes utiles que vous pourriez avoir besoin d'utiliser pour administrer votre VM et surveiller les actions de CrowdSec :

- cscli alerts list



ID	value	reason	country	as	decisions	created_at
6456	Ip:218.92.0.103	crowdsecurity/ssh-slow-bf	CN	4134 Chinanet	ban:1	2024-04-06 21:04:29.410729692 +0000 UTC
6455	Ip:218.92.0.103	crowdsecurity/ssh-slow-bf	CN	4134 Chinanet	ban:1	2024-04-06 20:59:23.953113805 +0000 UTC
6454	Ip:218.92.0.103	crowdsecurity/ssh-slow-bf	CN	4134 Chinanet	ban:1	2024-04-06 20:54:16.800109149 +0000 UTC
6453	Ip:218.92.0.29	crowdsecurity/ssh-slow-bf	CN	4134 Chinanet	ban:1	2024-04-06 20:57:23.492929043 +0000 UTC

- cscli bouncers list

Name	IP Address	Valid	Last API pull	Type	Version	Auth Type
wordpress-bouncer	127.0.0.1	✔	2024-04-07T08:36:02Z	csphplapi_WordPress	v2.6.3	api-key

- cscli collections list

COLLECTIONS

Name	Status	Version	Local Path
crowdsecurity/apache2	✔ enabled	0.1	/etc/crowdsec/collections/apache2.yaml
crowdsecurity/base-http-scenarios	✔ enabled	0.8	/etc/crowdsec/collections/base-http-scenarios.yaml
crowdsecurity/http-cve	✔ enabled	2.6	/etc/crowdsec/collections/http-cve.yaml
crowdsecurity/linux	✔ enabled	0.2	/etc/crowdsec/collections/linux.yaml
crowdsecurity/sshd	✔ enabled	0.3	/etc/crowdsec/collections/sshd.yaml

Administration via le tableau de bord CrowdSec

Il est également possible d'administrer votre VM via le tableau de bord de l'outil, accessible sur leur site web. Voici comment procéder : Accédez au tableau de bord en suivant le lien ci-dessous et créez un compte utilisateur sur leur plateforme : https://app.crowdsec.net/

Un code de liaison vous sera alors affiché :

Voici à quoi ressemble l'affichage des alertes reçues par l'outil :