Projet 1 - Fail2ban

Instalation de fail2ban

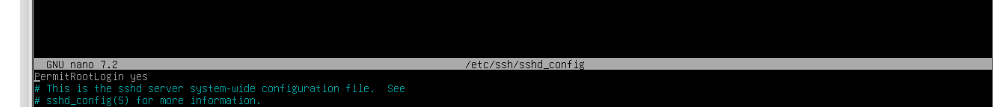


Mise en place du démarrage automatique après chaque redémarrage de la machine



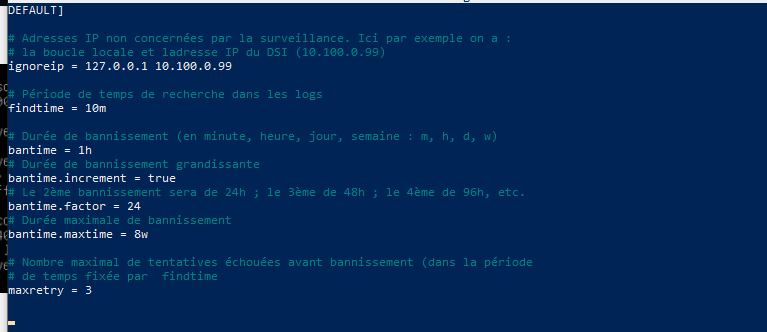
Adress ip



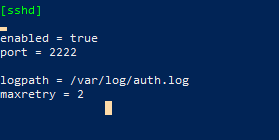
Pour accéder au PowerShell, il faut autoriser l'accès (PermitRootLogin Yes)

Paramétrage général

Les paramètres de configuration doivent normalement être ajoutés dans le fichier principal de configuration : /etc/fail2ban/jail.conf. Cependant, ce fichier contient déjà de nombreux paramètres et peut être remplacé lors des mises à jour du logiciel. Il est donc recommandé de créer un fichier séparé dans le répertoire /etc/fail2ban/jail.d/. Tous les fichiers présents dans ce répertoire seront automatiquement inclus par le fichier principal de configuration.  
De plus, si certains paramètres sont déjà définis dans jail.conf, ceux spécifiés dans le répertoire jail.d/ auront toujours priorité et seront pris en compte.  
Il suffit donc de créer un fichier comme /etc/fail2ban/jail.d/monParametrage.conf et d’y inscrire les paramètres souhaités



Activation de la premiere prison :



Gestion des prisons

On peut vérifier les prisons mises en place :

fail2ban-client status

Status

|- Number of jail: 1

`- Jail list: sshd

Ou bien contrôler une prison spécifique (exemple SSH) :

fail2ban-client status sshd

Status for the jail: sshd

|- Filter

| |- Currently failed: 0

| |- Total failed: 0

| `- File list: /var/log/auth.log

`- Actions

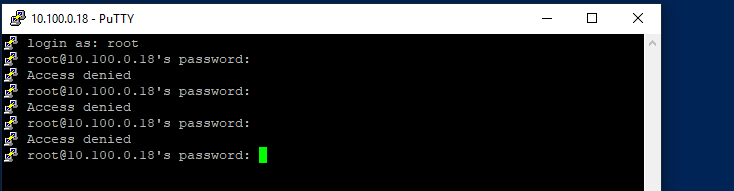
|- Currently banned: 0

|- Total banned: 0

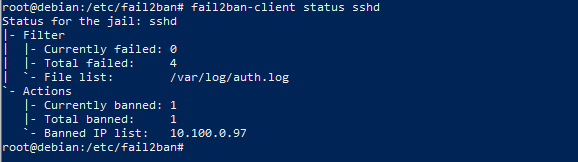
`- Banned IP list:

Test

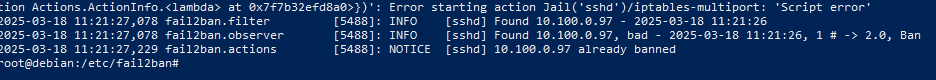
1.Une fois la protection SSH en place pour bloquer les adresses IP après deux tentatives infructueuses de connexion (mots de passe incorrects), vous pouvez effectuer le test suivant



2.Il est possible de constater qu'une adresse IP a été bannie, généralement pour une durée d'une heure, comme spécifié dans la configuration de notre protection SSH.



3. Les journaux (/var/log/fail2ban.log) montrent que Fail2Ban a détecté deux tentatives infructueuses correspondant à ses filtres et a bloqué l'IP après la troisième tentative.

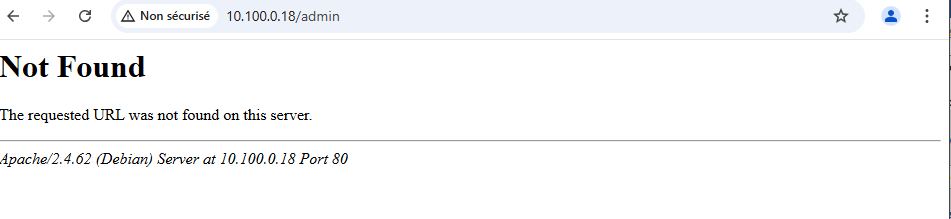


2ème prison de site internet

On install apache2

Après avoir installé Apache2 sur Debian, il est possible d'héberger un site web en utilisant l'adresse IP de la machine Debian 10.100.0.18

Lorsque qu'un utilisateur malveillant tente d'accéder à une page inexistante, comme par exemple http://10.100.0.18/admin, cela génère une erreur 404 qui est enregistrée dans les logs du serveur



Configuration d'une nouvelle règle, nommée « attaqueWeb », dans le fichier de configuration de Fail2Ban : /etc/fail2ban/jail.d/monParametrage.conf, en insérant les lignes suivantes :

Nano /etc/fail2ban/jail.d/monParametrage.conf

[attaqueWeb]

enabled = true

# On lui dit quel filtre utiliser pour détecter l’attaque (filtre qui va être créé dans l’étape suivante)

filter = attaqueWeb

# On utilise ce fichier de log pour rechercher les attaques

logpath = /var/log/apache2/access.log

# On bloque dès la 1ère tentative

maxretry = 0

Ensuite, nous définissons un filtre pour détecter la chaîne de caractères 'GET /admin HTTP/1.1' 404 dans les fichiers journaux. Pour cela, nous créons un fichier de filtre appelé /etc/fail2ban/filter.d/attaqueWeb.conf avec le contenu suivant

Nano /etc/fail2ban/filter.d/attaqueWeb.conf

[Definition]

failregex = ^<HOST>.\*"GET /admin HTTP/1.1" 404.\*

# Ou bien le filtre suivant si on veut bloquer /admin, ou /private ou /administration

#failregex = ^<HOST>.\*"GET /(admin|private|administration) HTTP/1.1" 404.\*

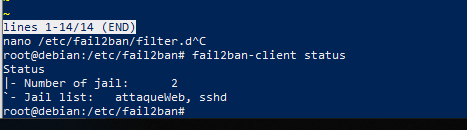
# Ou bien le filtre suivant si on veut bloquer quand la personne essaye /contact puis tout de suite après /about, puis /search

# Typiquement, ça serait l’œuvre d’une énumération par force brute (comme avec Gobuster ) via le dictionnaire suivant :

# /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt 😊

#failregex = ^<HOST>.\*"GET /contact HTTP/1.1" 404.\*\n.\*"GET /about HTTP/1.1" 404.\*\n.\*"GET /search HTTP/1.1" 404.\*

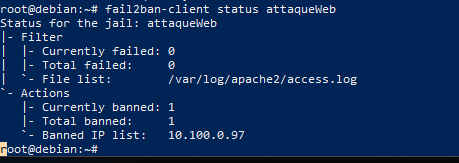
On vérifie les prisons actives



On simule une tentative d'attaque en accédant à l'URL <http://10.100.0.18/admin>

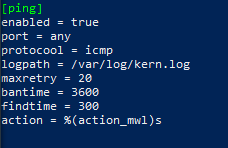
(ce qui devrait entraîner un bannissement immédiat)

On vérifie la prison « attaqueWeb » : l’IP est bannie

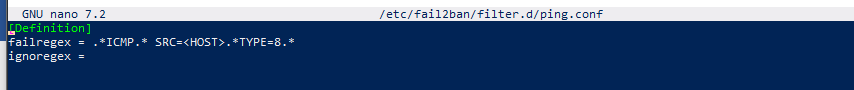


3ème prison les attaques DDOS

Paramètre dans le fichier **/etc/fail2ban/jail.d/monParametrage.conf**



Parametre pour le filtre de



Verificationa des prison



Cela ne suffit pas, il faut créer des règles de filtrages. Pour cela on utilise iptables, voici les règles a utilisé :

**iptables -A INPUT -p icmp --icmp-type 8 -j LOG --log-prefix "ICMP: " --log-level 4**

**iptables -A INPUT -p icmp --icmp-type 8 -j LOG --log-prefix "PING-LOG: " --log-level 4**

 -A INPUT → Ajoute la règle à la chaîne INPUT (trafic entrant).

 -p icmp → S'applique aux paquets ICMP.

 --icmp-type 8 → Filtre uniquement les paquets ICMP de type 8, qui correspondent aux **requêtes ping (echo request)**.

 -j LOG → Journalise les paquets correspondants sans les bloquer.

 --log-prefix "ICMP: " et --log-prefix "PING-LOG: " → Ajoutent un préfixe pour distinguer les logs dans /var/log/kern.log.

 --log-level 4 → Définit le niveau de journalisation (warning).

Test

