Portsentry & Fail2ban

Portsenrty

Fail2ban

fail2ban

Première étape

Il faut trouver où se trouve le fichier de log de Nextcloud : il se trouve dans le répertoire : `/home/htdocs/nextcloud/data/nextcloud.log`

Une fois qu'on l'a trouvé, on peut installer fail2ban :

- D'abord mettre à jour notre serveur avec :

`

```
apt update
```

`

- Puis faire un :

`

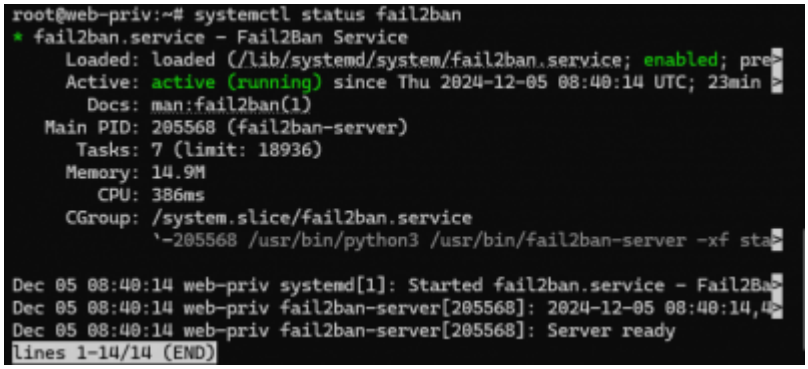
```
apt install fail2ban -y
```

`

```
  Le `-y` c'est pour spécifier le yes lors de la confirmation
d'installation.
```

Ensuite, une fois que fail2ban a été créé, il faut s'assurer qu'il est bien en marche : `

```
systemctl status fail2ban
```



`

Documentation officielle

Une fois que c'est fait, on peut suivre la documentation officielle de Nextcloud : https://docs.nextcloud.com/server/19/admin_manual/installation/harden_server.html#setup-fail2ban
Cette documentation indique comment mettre en place une prison fail2ban pour Nextcloud et comment mettre un filtre pour bannir les adresses IP qui tenteront des connexions répétées sur le service Nextcloud.

Dans le répertoire `/etc/fail2ban/filter.d`, on va créer un fichier nommé `nextcloud.conf` avec le contenu suivant :

```
[Definition]
_groupsre = (?:(?:,?\s*"\w+":(?:"[^"]+"|\w+))*)
failregex =
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Login
failed:
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Trust
ed domain error.
datepattern = ,?\s*"time"\s*:\s*"%%Y-%%m-%%d[T ]%%H:%%M:%%S(%%z)?"
```

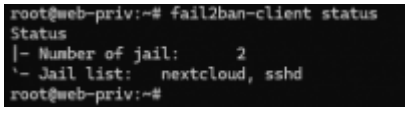
Puis, dans le répertoire `/etc/fail2ban/jail.d`, on va créer un fichier nommé `nextcloud.local` avec les lignes suivantes :

```
[nextcloud]
backend = auto
enabled = true
port = 80,443
protocol = tcp
filter = nextcloud
maxretry = 3
bantime = 86400
findtime = 43200
logpath = /home/htdocs/nextcloud/data/nextcloud.log
```

Pour tester, on fait : `

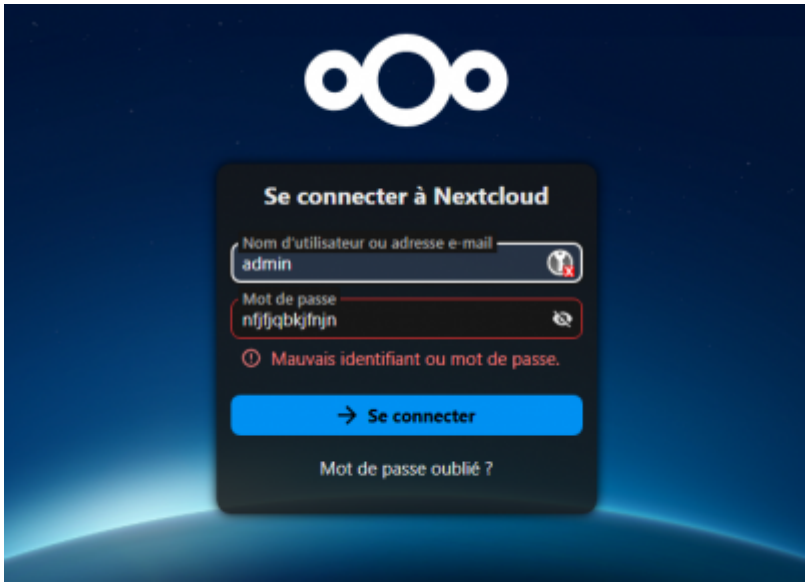
```
 fail2ban-client status
```

`



Cela nous indique le nombre de prisons existantes. Il y a `sshd` par défaut, et `nextcloud` que nous avons créé. Cela signifie que notre prison est bien prise en compte.

On teste la connexion sur Nextcloud avec de faux identifiants pour vérifier que cela fonctionne bien :



Pour vérifier, on tape : `

```
fail2ban-client status nextcloud
```

`

Résultat : 

En cas de bannissement, on débloque avec : `

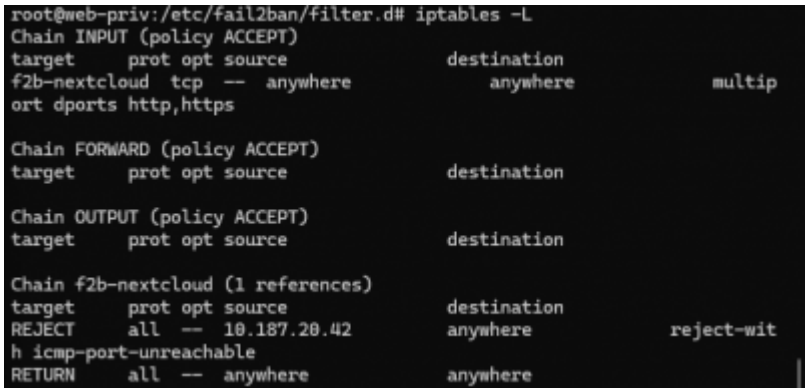
```
fail2ban-client set nextcloud unbanip 10.187.20.42
```

` Et on peut voir les règles avec : `

```
iptables -L
```

`

Chaîne	Protocole	Source	Destination	Ports cibles	Explication
f2b-nextcloud	tcp	anywhere	anywhere	http, https	Chaîne spécifique de Fail2Ban appliquée pour surveiller Nextcloud.



fail2ban : wordpress

Premièrement, il va falloir se connecter à nos deux WordPress via les pages de connexion : https://oceanie.gsb.org/wp-admin/ https://gsb.org/wp-admin/

Cependant, on s'est rendu compte qu'on a très vite oublié nos mots de passe, donc il va falloir trouver une solution à cela : Nos WordPress utilisent un serveur de base de données commun : priv-db2, dont l'IP est 10.31.208.33.

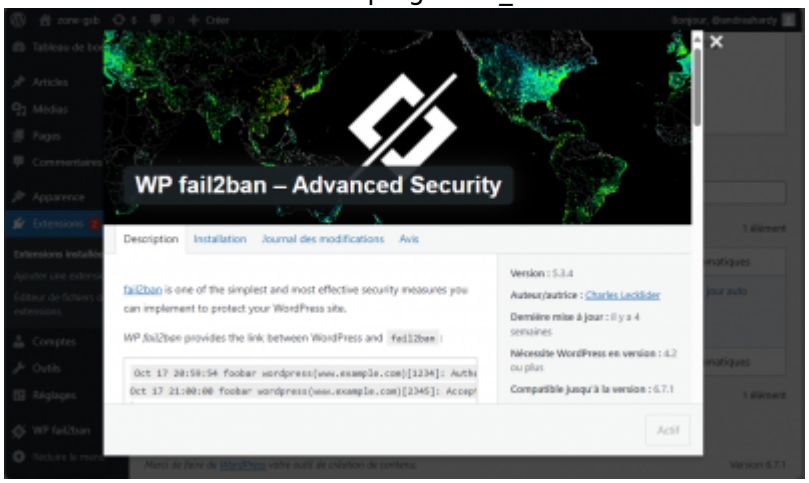
Liste des commandes nécessaires pour changer le mot de passe des utilisateurs de chacun de nos WordPress :

```
SHOW databases; # Affiche la liste des bases de données
USE wordpress_gsb; # Utiliser la base de données WordPress de GSB
SHOW tables; # Affiche les tables de la base de données wordpress_gsb
UPDATE wp_users SET user_pass = MD5('password') WHERE user_login =
'@andreahardy'; # Met à jour le mot de passe pour l'utilisateur @andreahardy
```

Et normalement, c'est bon !

Du coup, revenons à notre WordPress. Après avoir changé le mot de passe, on peut donc à nouveau se connecter.

1. **Installation du plugin WP_Fail2ban** On va installer le plugin WP_fail2ban dans le menu Extensions de notre WordPress.



Une fois que cela a été installé sur notre WordPress, on va intégrer le filtre WordPress dans les filtres de Fail2ban.

2. **Intégration du filtre WordPress dans Fail2ban** On va se rendre dans le répertoire où se trouve le plugin Fail2ban qu'on a installé dans WordPress.

```
    cd
/home/htdocs/www.oceanie.gsb.org/wp-content/plugins/wp-fail2ban/filters.d
```

Ce répertoire contient 3 fichiers de configuration pour notre filtre WordPress, qu'on copiera dans le répertoire de filtres de Fail2ban :

```
    cp
/home/htdocs/www.oceanie.gsb.org/wp-content/plugins/wp-fail2ban/filters.d/wo
rdpress-extra.conf wordpress-hard.conf wordpress-soft.conf
/etc/fail2ban/filter.d
```

Après avoir copié ces fichiers, on va de ce pas créer une jail pour WordPress.

3. **Création d'une jail WordPress** Dans le répertoire `/etc/fail2ban/jail.d`, on va créer une prison pour WordPress qui s'appellera `wordpress.conf`.

```
    [wordpress]  # Nom du jail, spécifique pour protéger WordPress.
    enabled = true  # Active ce jail.
    port = http,https  # Surveille les connexions sur les ports HTTP et
HTTPS.
    filter = wordpress-soft  # Fichier de filtre spécifique pour WordPress,
défini dans /etc/fail2ban/filter.d.
    findtime = 1m  # Intervalle de temps (1 minute) pendant lequel les
tentatives sont comptabilisées.
    bantime = 24h  # Durée pendant laquelle l'IP sera bannie en cas de
dépassement des tentatives.
    maxretry = 3  # Nombre maximal de tentatives autorisées avant de bannir
l'IP.
    logpath = /var/log/auth.log  # Chemin vers le fichier journal à
surveiller pour détecter les tentatives échouées.
```

On va mettre en place une jail récidive pour bannir définitivement des utilisateurs qui se sont fait bannir au moins 3 fois d'un service tel que SSH.

Le but de la récidive est de lire les logs de Fail2ban pour repérer les adresses IP qui ont été bannies au moins 3 fois, afin de les bannir à vie. Dans le répertoire `jail.d`, on va créer la prison `recidive.conf`.

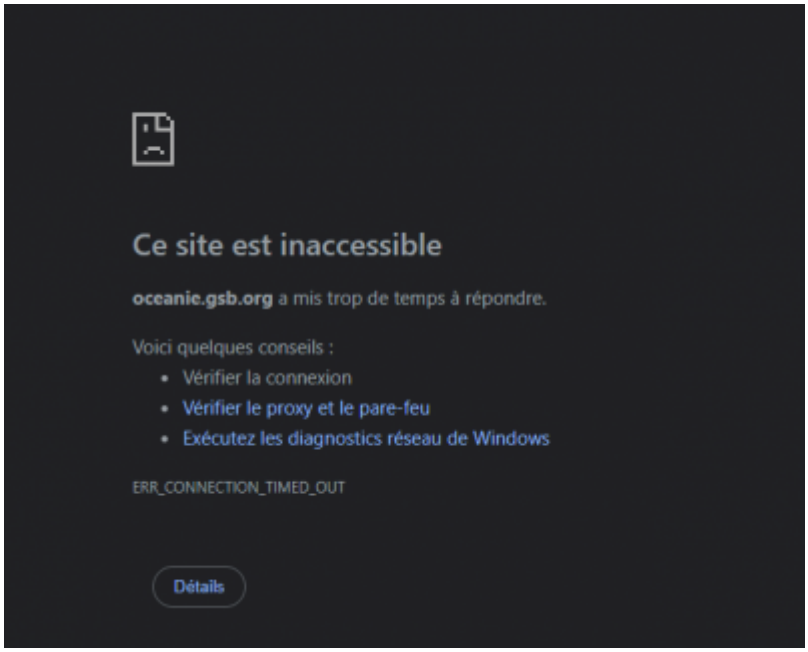
```
    [recidive]  # Nom du jail, conçu pour gérer les récidivistes (adresses
IP qui continuent d'échouer malgré un bannissement précédent).
    enabled = true  # Active ce jail.
    filter = recidive  # Utilise le filtre "recidive" (préconfiguré dans
Fail2Ban).
    bantime = -1  # Bannissement permanent (-1 signifie que l'IP restera
bannie indéfiniment).
    maxretry = 3  # Nombre maximal de récidives autorisées avant de bannir
définitivement l'IP.
    logpath = /var/log/fail2ban.log  # Chemin du journal Fail2Ban où les
bannissements précédents sont enregistrés.
    banaction = %(banaction_allports)s  # Bloque l'accès sur tous les ports
pour les IP bannies.
```

Une fois que tout cela a été configuré, il faudra redémarrer le service en faisant :

```
service fail2ban restart
```

4. **Test de la sécurité WordPress avec Fail2ban** Pour tester notre protection, on va effectuer des tests en s'authentifiant avec de fausses informations :

Au bout de la troisième tentative, je serai définitivement banni et je n'aurai plus accès au site

WordPress. 

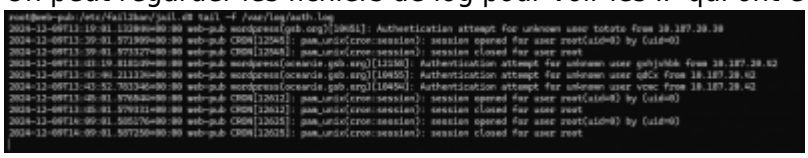
Pour vérifier tout cela :

```
fail2ban-client status wordpress
```

Cependant, je ne serai banni définitivement que si je tente de m'authentifier au total 9 fois d'après les règles qu'on a établies dans la jail. Pour le voir :

```
root@web-pub:/etc/fail2ban/jail.d# fail2ban-client status recidive
Status for the jail: recidive
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     4
|  `- File list:        /var/log/fail2ban.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
root@web-pub:/etc/fail2ban/jail.d#
```

On peut regarder les fichiers de log pour voir les IP qui ont été bannies :



fail2ban: DOKUWIKI