Fail2Ban

Un attaquant peut tenter de découvrir le mot de passe d'un compte utilisateur sur un service en essayant toutes les combinaisons possibles par force brute. Pour détecter cette méthode, il est nécessaire qu'une journalisation permette d'identifier un échec de connexion.

Ni le serveur Apache ni le code ne permettent de détecter cela. Il est donc indispensable d'ajouter un utilitaire capable de repérer les comportements anormaux dans les accès aux services d'une machine : tentatives de connexion trop fréquentes et échouées, connexions multiples en un court laps de temps, etc.

C'est le rôle de l'outil Fail2Ban : de l'échec (Fail) à (2) un bannissement (Ban).

Installation

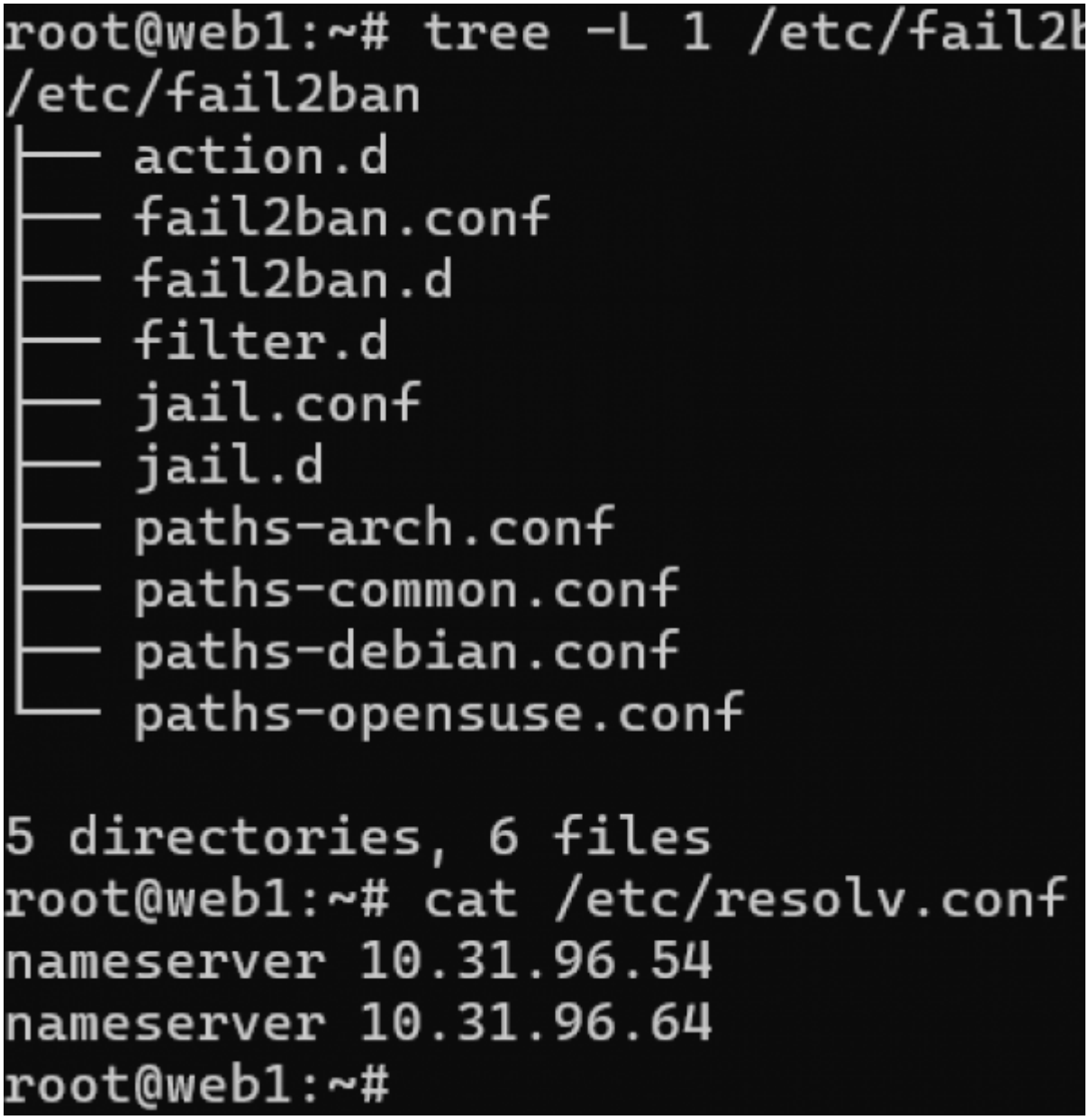
Il est nécessaire de taper cette commande sur le serveur ou dans le conteneur que nous voulons protéger. Cependant, avant de taper cette commande, il faut d'abord vérifier la configuration des DNS. Pour ce faire, il faut consulter le fichier avec la commande suivante :

```
cat /etc/resolv.conf
```

On doit d'abord installer Fail2Ban à partir des dépôts :

```
apt update
apt install fail2ban
```

Arborescence du répertoire de Fail2Ban



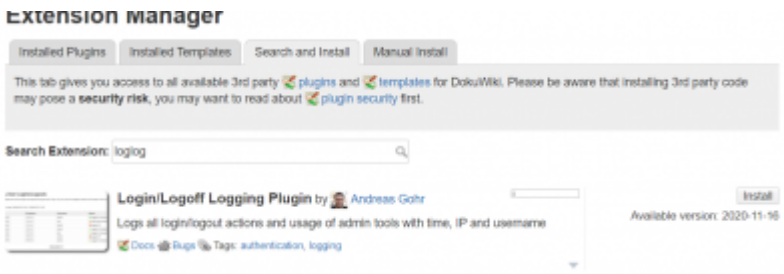
jail.conf : est le fichier de configuration principal des jails. Ne le modifiez pas directement, mais faites-en une copie appelée jail.local et modifiez cette copie. Il est également possible (et préférable) de créer des jails pour ses applications dans le répertoire jail.d.

action.d : Le répertoire action.d contient différentes configurations d'actions à mener en cas de détection de menace. Par défaut, ce sont des règles iptables qui sont appliquées.

filter.d : Le répertoire filter.d contient tous les filtres (patterns - regex) qui permettent de détecter des actions malveillantes dans les fichiers de logs des services/applications.

Ajout de l'extension loglog sur DocuWiki

NB : Une fois que vous avez fini de remplir le formulaire, n'oubliez pas votre mot de passe car il vous permettra de vous connecter par la suite. Enfin, téléchargez et installez l'extension loglog.



Configuration de Fail2Ban pour DocuWiki

Créer un fichier nommé /etc/fail2ban/jail.d/dokuwiki.local et ajoutez :

```
[dokuwiki]
enabled = true
mode = aggressive
port = http,https
filter = dokuwiki
action = iptables-allports
maxretry = 2
bantime = -1
logpath =  /home/htdocs/m2l.org/wiki/data/cache/
```

On doit aussi disposer de l'outil iptables qui gèrera les règles de bannissement :

```
apt install iptables
```

Création du fichier filter

Créer un fichier nommé /etc/fail2ban/filter.d/dokuwiki.conf et ajoutez :

```
[Definition]
failregex = ^.*:\d{2}\s{1,}<HOST>\s.*failed
ignoreregex =
```

tester le filtre

cette commande est utilisée pour tester et vérifier si les expressions régulières (regex) définies dans le fichier de filtre dokuwiki.conf capturent correctement les événements de sécurité dans le fichier de log loglog.log.

fail2ban-regex /home/htdocs/wiki/data/cache/loglog.log /etc/fail2ban/filter.d/dokuwiki.conf

rédémarrer le service Fail2ban

```
systemctl restart fail2ban
```

Vérifier le statut de la jail dokuwiki

```
fail2ban-client status dokuwiki
```