TP FAIL2BAN

Je télécharge le paquet fail2ban

Ensuite je renomme tout les fichiers .conf dans /etc/fail2ban en .conf.local

Je renomme en masse les fichier pour aller plus rapidement grâce à cette commande

« for i in $(ls);do cp -r $i $i.local;done »

```
root@smtp:/etc/fail2ban# for i in $(ls);do cp -r $i $i.local;done
root@smtp:/etc/fail2ban# ls
action.d          fail2ban.d       jail.conf       paths-arch.conf        paths-debian.conf
action.d.local    fail2ban.d.local jail.conf.local paths-arch.conf.local  paths-debian.conf.local
fail2ban.conf     filter.d         jail.d          paths-common.conf      paths-opensuse.conf
fail2ban.conf.local filter.d.local jail.d.local    paths-common.conf.local paths-opensuse.conf.local
root@smtp:/etc/fail2ban#
```

Pour modifier le temps de bannissement,tentative etc je dois modifier le fichier jail.conf.local

Je souhaite que l'utilisateur sois bloquer au bout de 3 tentatives

```
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 1m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3
```

J'essaie maintenant 3 connexions erronées depuis une autre machine

Voila ce que j'ai trouvé dans les logs je vois que le fichier « .local » n'a pas été prit en compte

```
2022-03-23 12:01:10,626 fail2ban.jail        [2091982]: INFO    Jail 'sshd' started
2022-03-23 12:02:02,164 fail2ban.filter      [2091982]: INFO    [sshd] Found 172.17.1.88 - 2022-03-23 12:02:02
2022-03-23 12:02:08,927 fail2ban.filter      [2091982]: INFO    [sshd] Found 172.17.1.88 - 2022-03-23 12:02:08
2022-03-23 12:02:12,492 fail2ban.filter      [2091982]: INFO    [sshd] Found 172.17.1.88 - 2022-03-23 12:02:12
2022-03-23 12:02:19,349 fail2ban.filter      [2091982]: INFO    [sshd] Found 172.17.1.88 - 2022-03-23 12:02:19
2022-03-23 12:02:25,260 fail2ban.filter      [2091982]: INFO    [sshd] Found 172.17.1.88 - 2022-03-23 12:02:24
2022-03-23 12:02:25,332 fail2ban.actions     [2091982]: NOTICE  [sshd] Ban 172.17.1.88
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: ERROR   7f1a2c1b3710 -- exec: iptables -w -N f2b-sshd
iptables -w -A f2b-sshd -j RETURN
iptables -w -I INPUT -p tcp -m multiport --dports ssh -j f2b-sshd
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: ERROR   7f1a2c1b3710 -- stderr: '/bin/sh: 1: iptables: not found'
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: ERROR   7f1a2c1b3710 -- stderr: '/bin/sh: 2: iptables: not found'
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: ERROR   7f1a2c1b3710 -- stderr: '/bin/sh: 3: iptables: not found'
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: ERROR   7f1a2c1b3710 -- returned 127
2022-03-23 12:02:25,336 fail2ban.utils       [2091982]: INFO    HINT on 127: "Command not found".  Make sure that all command
s in 'iptables -w -N f2b-sshd\niptables -w -A f2b-sshd -j RETURN\niptables -w -I INPUT -p tcp -m multiport --dports ssh -j f2b-s
shd' are in the PATH of fail2ban-server process (grep -a PATH= /proc/`pidof -x fail2ban-server`/environ). You may want to start
"fail2ban-server -f" separately, initiate it with "fail2ban-client reload" in another shell session and observe if additional in
formative error messages appear in the terminals.
2022-03-23 12:02:25,337 fail2ban.actions     [2091982]: ERROR   Failed to execute ban jail 'sshd' action 'iptables-multiport'
info 'ActionInfo({'ip': '172.17.1.88', 'family': 'inet4', 'fid': <function Actions.ActionInfo.<lambda> at 0x7f1a2b913b80>, 'raw
```

La machine a été bloquée au bout de 5 tentatives

Le fichier .conf n'est pas prit en compte je repars donc sur le fichier « .conf » normal

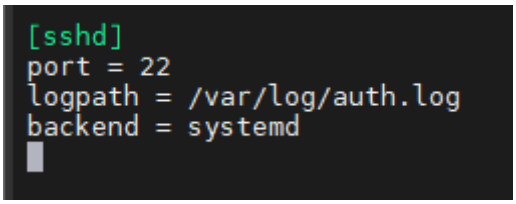
Pour faire une « jail » personnalisé il faut modifier le fichier « jail.conf » et rajouter notre bloc de directive

La directive backend il y'en a 4 qui sont paramétrés automatiquement :

pyinotify : un module Python permettant de monitorer les modifications sur un fichier.
gamin : même usage que le précédent, mais il s'agit d'un module du projet Gnome.
polling : le fichier est simplement vérifier à intervales régulièrs afin de vérifier s'il y a eu des écritures.
systemd : ici, Fail2Ban se greffe sur SystemD afin d'être alerté de nouveaux logs.
auto : mode automatique, qui va tenter toutes les solutions sus-mentionnées, dans cet ordre.

Je veux qu'il ce greffe sur systemd donc je vais mettre systemD

Le fichier jail.conf a été modifier comme sa



Ensuite je définis le fichier à surveiller avec la directive logpath

Mise en place d'un filtre avec des regex

Les filtres sont stockés dans ce répertoire « /etc/fail2ban/filter.d/ »

Ils ont tous cette syntaxe de base

```
  [INCLUDES]
before = common.conf
[Definition]
failregex =
ignoreregex =
```

Common.conf est dans la majorité des filtres

Ensuite dans ce répertoire je dois créer mon propre fichier de conf et y mettre cette syntaxe de base

Je l'appellerai filtre.conf

Mon fichier ressemble à sa

```
  [INCLUDES]
before = common.conf
[Definition]
failregex= Invalid user [a-z]{2,10} from <HOST>
ignoreregex=
```

Dans ma regex je précise que dans la ligne il y'a obligatoirement « Invalid user » ensuite le nom de l'user qui est composé de lettres de a-z composer de 2 caractère minimum et maximum 10

Ensuite « from » doit obligatoirement être présent ensuite l'IP de l'attaquant apparait

```
  [INCLUDES]
before = common.conf
[Definition]
failregex= Invalid user .* from <HOST>\b
           Failed password [a-z]{2,10} .* from <HOST> \b
ignoreregex=
```

Pour que la deuxième regex fonctionne correctement il faut que j'enlève « .* » avant from

Pour mettre plusieurs regex il faut mettre « \b » à la fin des regex ensuite sur la première ligne au lieu de mette une regex [a-z] je mets «.* » « qui me permet de dire « n'importe quel caractère » mais si je veux être très précis il faut utiliser des regex plus précise avec [a-z]{2,10}

Je peux aussi utiliser « ^ » au début de la ligne qui me permet de dire que la ligne dans les logs doit obligatoirement commencer par ce caractère.

Je rajoute une regex qui vient affiner mes autres regex

```
  [INCLUDES]
before = common.conf
[Definition]
failregex= Invalid user .* from <HOST>\b
           Failed password for [a-z]{2,10} from <HOST> .* \b
          .* authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=<HOST> user=[a-z]{2,10}\b
```

Je teste mon filtre avec la commande fail2ban-regex

Syntax = fail2ban-regex /var/log/auth.log /etc/fail2ban/filter.d/filtre.conf

Résultat de la commande :

```
Results
=======

Failregex: 20 total
|-  #) [# of hits] regular expression
|   1) [7] Invalid user .* from <HOST>\b
|   2) [13] Failed password [a-z]{2,10} .* from <HOST> \b
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [6423] {^LN-BEG}(?:DAY )?MON Day %k:Minute:Second(?:\.Microseconds)?(?: ExYear)?
`-

Lines: 6423 lines, 0 ignored, 20 matched, 6403 missed
[processed in 0.21 sec]

Missed line(s): too many to print.  Use --print-all-missed to print all 6403 lines
```

Test de mon filtre

Je test 3 connexions depuis une autre machine

```
2022-04-06 09:54:10,393 fail2ban.filter         [42352]: INFO    [sshd] Found 172.17.1.88 - 2022-04-06 09:54:09
2022-04-06 09:54:32,115 fail2ban.filter         [42352]: INFO    [sshd] Found 172.17.1.88 - 2022-04-06 09:54:31
2022-04-06 09:54:50,615 fail2ban.filter         [42352]: INFO    [sshd] Found 172.17.1.88 - 2022-04-06 09:54:50
2022-04-06 09:54:51,077 fail2ban.actions        [42352]: NOTICE  [sshd] Ban 172.17.1.88
```

Sa fonctionne juste il faut que j'affine un peu la regex car avec mon filtre c'est seulement au bout de la première tentative de connexion que c'est pris en compte par connexion

Il faut 3 première tentative pour que le ban soit accessible

Syntax fichier jail.conf

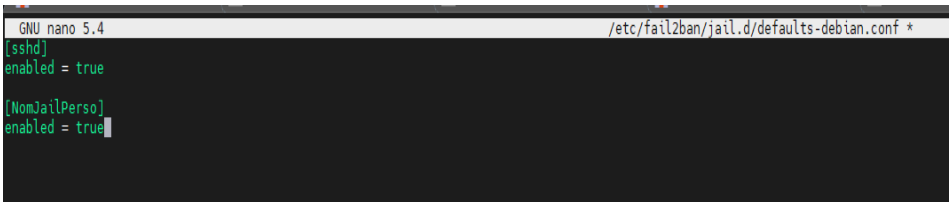
```
[sshd]
port = 22
logpath = /var/log/auth.log
backend = systemd
filter = filtre
```

Il faut mettre le fichier de conf sans « .conf »

Activer nos jails personnalisées

Il faut aller dans le fichier **« /etc/fail2ban/jail.d/defaults-debian.conf »**

La syntax à respecter ressemble à sa



Le nom à renseigner est celui qu'on a mit au tout début pour identifier la jail

Ne surtout pas oublier d'activer nos jails personnalisée sinon elle ne fonctionneront pas