Introduction à FAIL2BAN CONFIGURATION D'UN IPS

Installation du server fail2ban .

Cmd: apt install fail2ban

Vérification que le service ssh soit opérationnel sur ma machine.

Apt install ssh car je ne l'avait pas apres on entre dans le fichier de conf est on le configure.

Vérifier que iptables soit bien installé.

apt intall iptables

Dans quel(s) fichier(s) sont stockés les logs concernant authentification ?

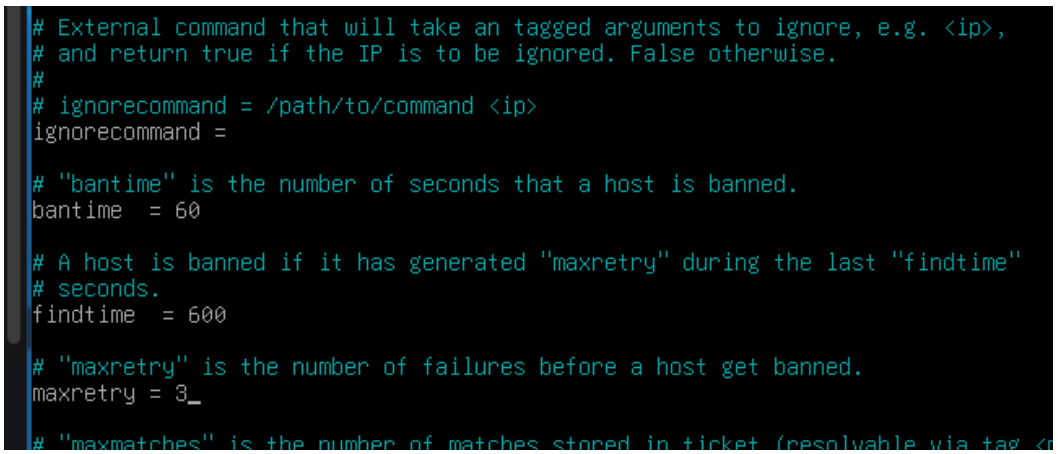
Les journaux de log sont stockés dans le répertoire /var/log/auth.lo get sont consultables grâce aux commandes tail, grep et zgrep.

Architecture de l'app fail2ban :

a) Architecture de l'application:

```
/etc/fail2ban/
├── action.d
│   ├── dummy.conf
│   ├── hostsdeny.conf
│   ├── iptables.conf
│   ├── mail-whois.conf
│   ├── mail.conf
│   └── shorewall.conf
├── fail2ban.conf
├── fail2ban.local
├── filter.d
│   ├── apache-auth.conf
│   ├── apache-noscript.conf
│   ├── couriersmtp.conf
│   ├── postfix.conf
│   ├── proftpd.conf
│   ├── sshd.conf
│   └── vsftpd.conf
├── jail.conf
└── jail.local
```

Mettre le temps de bannissement à 60 secondes, le nombre maximum de tentatives échouées à 3 (Rappel redémarrer le service Fail2ban à chaque modification de la configuration



6)

```
oot@debian:~# ssh root@172.17.1.107
he authenticity of host '172.17.1.107 (172.17.1.107)' can't be established.
D25519 key fingerprint is SHA256:KJ1Ohk8mzP+B0axc1Ft35CsgB91TGkt1jA5e7zTDkFg.
his key is not known by any other names.
re you sure you want to continue connecting (yes/no/[fingerprint])? yes
arning: Permanently added '172.17.1.107' (ED25519) to the list of known hosts.
oot@172.17.1.107's password:
ermission denied, please try again.
oot@172.17.1.107's password:
ermission denied, please try again.
oot@172.17.1.107's password:
oot@172.17.1.107: Permission denied (publickey,password).
oot@debian:~# ssh root@172.17.1.107
oot@172.17.1.107's password:
inux debian 6.1.0-39-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.148-1 (2025-08-26) x86

he programs included with the Debian GNU/Linux system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.

ebian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
ermitted by applicable law.
ast login: Wed Nov 19 10:04:36 2025 from 172.17.10.46
oot@debian:~# exit
éconnexion
onnection to 172.17.1.107 closed.
oot@debian:~#
```

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
port    = 22
logpath = /var/log/auth.log
backend = systemd
```

8)

V1

```
 GNU nano 7.2                                                abd.conf *
[INCLUDES]
before =common.conf
[Definition]
failregex= Invalid user.* <HOST>\b
           Failed password
ignoreregex=
```

V2

```
 GNU nano 7.2                                                abd.conf
[INCLUDES]
before =common.conf
[Definition]
failregex= Invalid user.* <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
ignoreregex=
```

9)

```
2025-11-19 11:41:33,720 fail2ban.filtersystemd  [2486]: INFO    [abd] Jail is in operation now (process new journal entries)
2025-11-19 11:41:33,828 fail2ban.actions        [2486]: INFO    [abd] Ignore 172.17.1.4, expired bantime
2025-11-19 11:41:33,828 fail2ban.actions        [2486]: INFO    [abd] Ignore 172.17.1.4, expired bantime
2025-11-19 11:41:33,829 fail2ban.actions        [2486]: INFO    [abd] Ignore 172.17.1.4, expired bantime
^[[A2025-11-19 11:41:49,921 fail2ban.filter         [2486]: INFO    [abd] Found 172.17.1.4 - 2025-11-19 11:41:49
2025-11-19 11:41:50,039 fail2ban.actions        [2486]: NOTICE  [abd] Ban 172.17.1.4
^C
```

10)

```
root@debian:/etc/fail2ban# fail2ban-regex /var/log/fail2ban.log /etc/fail2ban/filter.d/abd.conf

Running tests
=============

Use    failregex filter file : abd, basedir: /etc/fail2ban
Use      datepattern : {^LN-BEG} : Default Detectors
Use         log file : /var/log/fail2ban.log
Use         encoding : UTF-8


Results
=======

Failregex: 0 total

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [399] {^LN-BEG}ExYear(?P<_sep>[-/.])Month(?P=_sep)Day(?:T|  ?)24hour:Minute:Second(?:[.,]Microseconds)?(?:\s*Zone offs
`-

Lines: 399 lines, 0 ignored, 0 matched, 399 missed
[processed in 0.01 sec]

Missed line(s): too many to print.  Use --print-all-missed to print all 399 lines
root@debian:/etc/fail2ban#
```

Plus :

Pour faire fonctionné mon regex il fallait utiliser rsyslog pour centralisé les log dans un seul fichier :

installation de rsyslog :
commande : apt install rsyslog
systemctl enable --now rsyslog

activation de la prise en charge des logs ssh :
comande : nano /etc/rsyslog.d/50-default.conf

contenue : auth,authpriv.* /var/log/auth.log

redémarrage de rsyslog
commande : systemctl restart rsyslog

résulta obtenue :