Fail2ban ist bei mir so eingestellt, dass jeder angreifer für 24 Stunden blockiert wird. In letzer Zeit häufen sich die Angriffe, die nach 24 Stunden einfach weitermachen.

Ich habe mich auf die suche nach einer Möglichkeit der Erkennung und längerfristigen blockierung gemacht und bin fündig geworden.

Fail2ban-Regel

Als nächstes sollte man das folgende rule-file nach `/etc/fail2ban/filter.d` kopieren.

fail2ban.conf

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
#
# $Revision$
#

#[INCLUDES]

# Read common prefixes. If any customizations available -- read them
from
# common.local
#before = apache-common.conf

[Definition]

# Option:  failregex
# Notes.:  regex to match the password failure messages in the logfile.
The
#          host must be matched by a group named "host". The tag
"<HOST>" can
#          be used for standard IP/hostname matching and is only an
alias for
#          (?:::f{4,6}:)?(?P<host>[\w\-.^_]+)
# Values:  TEXT
#
failregex = ^.* fail2ban.actions: WARNING \[(postfix|ssh.*|pam-
generic|apache.*|owncloud)\] Ban <HOST>

# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
```

Zum aktivieren muss folgender Eintrag zu der Datei `/etc/fail2ban/jail.local` hinzugefügt

werden

jail.local

```
[fail2ban]

enabled  = true
port     = http,https,ssh,smtp,ssmtp
filter   = fail2ban
logpath  = /var/log/fail2ban.log*
maxretry = 3
# findtime: 2 Wochen
findtime = 1209600
# bantime: 2 Wochen
bantime = 1209600
```

Zum Schluss muss noch fail2ban neu gestartet werden und man ist gegen die lästigen Script-Kiddies geschützt.