Blacklist IP's from a file

fail2ban is designed to dynamically watch logs and ban/unban IP's with bad reputations. However, with a little sneakiness, it can be abused to also load a list of permenantly banned IP addresses.

First, we need to create an action, a file to be placed in action.d. I named it blacklistip.conf, and the name is important when you define the jail it goes in, ie action = blacklistip means *look in action.d for a file names blacklistip.conf and load it as the action*.

action.d/blacklistip.conf

```
# action file to allow loading of IP's from a text file to be blocked
# along with fail2ban.
# The file contains one IP or subnet per line, and may be placed
# anywhere on the system.
#
# This is a perversion of fail2ban's basic purpose, which is to
dynamically
# add/remove IP's from IPTables, but it allows us to permenantly ban
# some really, really bad people
#
# example of file
# 172.104.94.112
# 190.40.235.20
# 190.4.51.122
# 210.186.135.78
# 39.45.148.0/24
#
# NOTE: I did not set it up to ignore comments, so you can't put
comments
# into the file.
#
# Works on fail2ban v9


[INCLUDES]

before = iptables-common.conf


[Definition]

# what to do when fail2ban starts
# taken directly from the multiport ban script, with the last line
# inserted to load the IP file
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -j f2b-<name>
              cat <filename> | while read IP; do <iptables> -I f2b-
```

```
<name> 1 -s $IP -j DROP; done


# these actions are taken when fail2ban is shut down
#
actionstop = <iptables> -D <chain> -p <protocol> -j f2b-<name>
             <iptables> -F f2b-<name>
             <iptables> -X f2b-<name>


actioncheck =
actionban =
actionunban =

[Init]
```

Now,

filter.d/blacklistip.conf

```
# dummy filter file for blacklistip jail. Expect a warning that
failregex is
# not defined, or, if you uncomment failregex, expect a warning that
there
# is no <Host> entry in it
#
# Since this is a static read, we don't actually parse any logs

[INCLUDES]


[Definition]

#failregex = ''

[Init]
```

Finally, add the following block to jail.local

```
[blacklistip]
enabled = true
action = blacklistip[name=blacklistip,filename='/etc/fail2ban/ip.blacklist']
```

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/software/fail2ban/blacklist?rev=1565678698

Last update: **2019/08/13 06:44**