for PIAF

jail.conf

...

```
[apache-tcpwrapper]

enabled  = true
filter   = apache-auth
action   = iptables-allports[name=APACHE, port=http, protocol=tcp]
           sendmail-whois[name=APACHE, dest=root@localhost, sender=fail2ban@pbx.dyndns.org]
logpath  = /var/log/httpd/error_log
maxretry = 3

# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.

[apache-badbots]

enabled  = true
filter   = apache-badbots
action   = iptables-multiport[name=BadBots, port="http,https"]
           sendmail-whois[name=APACHE, dest=root@localhost, sender=fail2ban@pbx.dyndns.org]
logpath  = /var/log/httpd/*access_log
bantime  = 1800
maxretry = 1
```

...

filter.d/apache-auth.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>\S+)
# Values: TEXT
#
failregex = [[]client <HOST>[]] user .* authentication failure
[[]client <HOST>[]] user .* not found
[[]client <HOST>[]] user .* password mismatch
[[]client <HOST>[]] user .* not found.*
[[]client <HOST>[]] user .* Password Mismatch
[[]client <HOST>[]] access .* failed, .*

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

```
# Values: TEXT
#
ignoreregex =
```

filter.d/apache-badbots.conf?

```
[Definition]

badbotscustom = EmailCollector|WebEMailExtrac|TrackBack/1\.02|sogou music spider
badbots = atSpider/1\.0|autoemailspider|China Local Browse 2\.6|ContentSmartz|DataCha0s/
2\.0|DataCha0s/2\.0|DBrowse 1\.4b|DBrowse 1\.4d|Demo Bot DOT 16b|Demo Bot Z 16b|DSurf15a
01|DSurf15a 71|DSurf15a 81|DSurf15a VA|EBrowse 1\.4b|Educate Search VxB|EmailSiphon|EmailWolf
1\.00|ESurf15a 15|ExtractorPro|Franklin Locator 1\.8|FSurf15a 01|Full Web Bot 0416B|Full Web Bot
0516B|Full Web Bot 2816B|Industry Program 1\.0\.x|ISC Systems iRc Search 2\.1|IUPUI Research Bot v
1\.9a|LARBIN-EXPERIMENTAL \(efp@gmx\.net\)|LetsCrawl\.com/1\.0 +http\://letscrawl\.com/|Lincoln
State Web Browser|LWP\:\:Simple/5\.803|Mac Finder 1\.0\.xx|MFC Foundation Class Library
4\.0|Microsoft URL Control - 6\.00\.8xxx|Missauga Locate 1\.0\.0|Missigua Locator 1\.9|Missouri College
Browse|Mizzu Labs 2\.2|Mo College 1\.9|Mozilla/2\.0 \(compatible; NEWT ActiveX; Win32\)|Mozilla/3\.0
\(compatible; Indy Library\)|Mozilla/4\.0 \(compatible; Advanced Email Extractor v2\.xx\)|Mozilla/4\.0
\(compatible; Iplexx Spider/1\.0 http\://www\.iplexx\.at\)|Mozilla/4\.0 \(compatible; MSIE 5\.0;
Windows NT; DigExt; DTS Agent|Mozilla/4\.0 efp@gmx\.net|Mozilla/5\.0 \(Version\: xxxx
Type\:xx\)|MVAClient|NASA Search 1\.0|Nsauditor/1\.x|PBrowse 1\.4b|PEval 1\.4b|Poirot|Port Huron
Labs|Production Bot 0116B|Production Bot 2016B|Production Bot DOT 3016B|Program Shareware
1\.0\.2|PSurf15a 11|PSurf15a 51|PSurf15a VA|psycheclone|RSurf15a 41|RSurf15a 51|RSurf15a 81|searchbot
admin@google\.com|sogou spider|sohu agent|SSurf15a 11 |TSurf15a 11|Under the Rainbow
2\.2|User-Agent\: Mozilla/4\.0 \(compatible; MSIE 6\.0; Windows NT
5\.1\)|WebVulnCrawl\.blogspot\.com/1\.0 libwww-perl/5\.803|Wells Search II|WEP Search 00

# Option:  failregex
# Notes.:  Regexp to catch known spambots and software alike. Please verify
#          that it is your intent to block IPs which were driven by
#          abovementioned bots.
# Values:  TEXT
#
failregex = ^<HOST> -.*"(GET|POST).*HTTP.*"(?:%(badbots)s|%(badbotscustom)s)"$

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

????

- Banning phpMyAdmin bots using fail2ban
- Fail2ban protect web server http DoS attack
- ????????: ??????