```
#!/bin/bash
#
#####################################################################
#
#   Name:           Fail2Ban_mail.sh
#   Author:         Chris Fedun 31/01/2017
#   Description:    Fail2Ban Configuration
#
#   Copyright (C) 2017  Christopher Fedun
#
#   This program is free software: you can redistribute it and/or modify
#   it under the terms of the GNU General Public License as published by
#   the Free Software Foundation, either version 3 of the License, or
#   (at your option) any later version.
#
#   This program is distributed in the hope that it will be useful,
#   but WITHOUT ANY WARRANTY; without even the implied warranty of
#   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#   GNU General Public License for more details.
#
#   You should have received a copy of the GNU General Public License
#   along with this program.  If not, see <http://www.gnu.org/licenses/>.
#####################################################################
#####Constants#####
domain_name=$1

function config_jailLocal
{
cat >> /etc/fail2ban/jail.local << EOF
# # Fail2Ban configuration file.
# #
# # This file was composed for Debian systems from the original one
# # provided now under /usr/share/doc/fail2ban/examples/jail.conf
# # for additional examples.
# #
# # Comments: use '#' for comment lines and ';' for inline comments
# #
# # To avoid merges during upgrades DO NOT MODIFY THIS FILE
# # and rather provide your changes in /etc/fail2ban/jail.local
# #
#
# # The DEFAULT allows a global definition of the options. They can be overridden
# # in each jail afterwards.
#
[DEFAULT]
#
# # "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# # ban a host which matches an address in this list. Several addresses can be
# # defined using space separator.
ignoreip = 127.0.0.1/8
#

# # "bantime" is the number of seconds that a host is banned.
bantime  = 1200
#
# # A host is banned if it has generated "maxretry" during the last "findtime"
# # seconds.
findtime = 1800
maxretry = 6

# #
# # Destination email address used solely for the interpolations in
# # jail.{conf,local} configuration files.
destemail = root@$domain_name
#
# #
```

```
# # Name of the sender for mta actions
sendername = Fail2BanAlerts
#
# # Email address of the sender
#sender = fail2ban@$domain_name
#
# #
# # ACTIONS

# # email action. Since 0.8.1 upstream fail2ban uses sendmail
# # MTA for the mailing. Change mta configuration parameter to mail
# # if you want to revert to conventional 'mail'.
mta = mail
#
# # Default protocol
# protocol = tcp
#
# # Specify chain where jumps would need to be added in iptables-* actions
# chain = INPUT
#
# #
# # Action shortcuts. To be used to define action parameter
#
# # The simplest action to take: ban only
# action_ = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s",
chain="%(chain)s"]
#
# # ban & send an e-mail with whois report to the destemail.
# action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s",
chain="%(chain)s"]
#               %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s", protocol="%(protocol)s",
chain="%(chain)s", sendername="%(sendername)s"]
#
# # ban & send an e-mail with whois report and relevant log lines
# # to the destemail.
# action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s",
chain="%(chain)s"]
#                %(mta)s-whois-lines[name=%(__name__)s, dest="%(destemail)s",
logpath=%(logpath)s, chain="%(chain)s", sendername="%(sendername)s"]
#
# # Choose default action.  To change, just override value of 'action' with the
# # interpolation to the chosen action shortcut (e.g.  action_mw, action_mwl, etc) in jail.local
# # globally (section [DEFAULT]) or per specific section
action = %(action_mwl)s
#
# #
# # JAILS
# #
#
# # Next jails corresponds to the standard configuration in Fail2ban 0.6 which
# # was shipped in Debian. Enable any defined here jail by including
# #
# # [SECTION_NAME]
# # enabled = true
#
# #
# # in /etc/fail2ban/jail.local.
# #
# # Optionally you may override any other parameter (e.g. banaction,
# # action, port, logpath, etc) in that section within jail.local
#
[ssh]

enabled  = true
port     = ssh
filter   = sshd
```

```
logpath  = /var/log/auth.log
maxretry = 6
#
# [dropbear]
#
# enabled  = false
# port     = ssh
# filter   = dropbear
# logpath  = /var/log/auth.log
# maxretry = 6
#
# # Generic filter for pam. Has to be used with action which bans all ports
# # such as iptables-allports, shorewall
# [pam-generic]
#
# enabled  = false
# # pam-generic filter can be customized to monitor specific subset of 'tty's
# filter   = pam-generic
# # port actually must be irrelevant but lets leave it all for some possible uses
# port     = all
# banaction = iptables-allports
# port     = anyport
# logpath  = /var/log/auth.log
# maxretry = 6
#
# [xinetd-fail]
#
# enabled   = false
# filter    = xinetd-fail
# port      = all
# banaction = iptables-multiport-log
# logpath   = /var/log/daemon.log
# maxretry  = 2
#
#
# [ssh-ddos]
#
# enabled  = false
# port     = ssh
# filter   = sshd-ddos
# logpath  = /var/log/auth.log
# maxretry = 6
#
#
# # Here we use blackhole routes for not requiring any additional kernel support
# # to store large volumes of banned IPs
#
# [ssh-route]
#
# enabled = false
# filter = sshd
# action = route
# logpath = /var/log/sshd.log
# maxretry = 6
#
# # Here we use a combination of Netfilter/Iptables and IPsets
# # for storing large volumes of banned IPs
# #
# # IPset comes in two versions. See ipset -V for which one to use
# # requires the ipset package and kernel support.
# [ssh-iptables-ipset4]
#
# enabled  = false
# port     = ssh
# filter   = sshd
# banaction = iptables-ipset-proto4
```

```
# logpath  = /var/log/sshd.log
# maxretry = 6
#
# [ssh-iptables-ipset6]
#
# enabled  = false
# port     = ssh
# filter   = sshd
# banaction = iptables-ipset-proto6
# logpath  = /var/log/sshd.log
# maxretry = 6
#
#
# #
# # HTTP servers
# #
#
[apache]

enabled  = true
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache*/*error.log
maxretry = 6

# # default action is now multiport, so apache-multiport jail was left
# # for compatibility with previous (<0.7.6-2) releases
# [apache-multiport]
#
# enabled   = false
# port      = http,https
# filter    = apache-auth
# logpath   = /var/log/apache*/*error.log
# maxretry  = 6
#
# [apache-noscript]
#
# enabled  = false
# port     = http,https
# filter   = apache-noscript
# logpath  = /var/log/apache*/*error.log
# maxretry = 6
#
[apache-overflows]

enabled  = true
port     = http,https
filter   = apache-overflows
logpath  = /var/log/apache*/*error.log
maxretry = 2

[apache-badbots]

enabled  = true
port     = http,https
filter   = apache-badbots
logpath  = /var/log/apache*/*error.log
maxretry = 2
#
# [apache-modsecurity]
#
# enabled  = false
# filter   = apache-modsecurity
# port     = http,https
# logpath  = /var/log/apache*/*error.log
# maxretry = 2
```

```
#
[apache-nohome]

enabled  = true
filter   = apache-nohome
port     = http,https
logpath  = /var/log/apache*/*error.log
maxretry = 2
#
# # Ban attackers that try to use PHP's URL-fopen() functionality
# # through GET/POST variables. - Experimental, with more than a year
# # of usage in production environments.
#
[php-url-fopen]

enabled = true
port    = http,https
filter  = php-url-fopen
logpath = /var/log/apache*/*access.log
#

#
# # Monitor roundcube server
#
[roundcube-auth]

enabled  = true
filter   = roundcube-auth
port     = http,https
logpath  = /var/log/roundcube/userlogins
#

# # FTP servers
# #
#
# [vsftpd]
#
# enabled  = false
# port     = ftp,ftp-data,ftps,ftps-data
# filter   = vsftpd
# logpath  = /var/log/vsftpd.log
# # or overwrite it in jails.local to be
# # logpath = /var/log/auth.log
# # if you want to rely on PAM failed login attempts
# # vsftpd's failregex should match both of those formats
# maxretry = 6
#
#
# [proftpd]
#
# enabled  = false
# port     = ftp,ftp-data,ftps,ftps-data
# filter   = proftpd
# logpath  = /var/log/proftpd/proftpd.log
# maxretry = 6
#
#
# [pure-ftpd]
#
# enabled  = false
# port     = ftp,ftp-data,ftps,ftps-data
# filter   = pure-ftpd
# logpath  = /var/log/syslog
# maxretry = 6
#
#
```

```
# [wuftpd]
#
# enabled  = false
# port     = ftp,ftp-data,ftps,ftps-data
# filter   = wuftpd
# logpath  = /var/log/syslog
# maxretry = 6
#
#
# #
# # Mail servers
# #
#
[postfix]

enabled  = true
port     = smtp,ssmtp,submission
filter   = postfix
logpath  = /var/log/mail.log
#
#
# [couriersmtp]
#
# enabled  = false
# port     = smtp,ssmtp,submission
# filter   = couriersmtp
# logpath  = /var/log/mail.log
#
#
# #
# # Mail servers authenticators: might be used for smtp,ftp,imap servers, so
# # all relevant ports get banned
# #
#
# [courierauth]
#
# enabled  = false
# port     = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
# filter   = courierlogin
# logpath  = /var/log/mail.log
#
#
[sasl]

enabled  = true
port     = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter   = postfix-sasl
# You might consider monitoring /var/log/mail.warn instead if you are
# running postfix since it would provide the same log lines at the
# "warn" level but overall at the smaller filesize.
logpath  = /var/log/mail.warn
#
[dovecot]

enabled = true
port    = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter  = dovecot
logpath = /var/log/mail.log
#
# # To log wrong MySQL access attempts add to /etc/my.cnf:
# # log-error=/var/log/mysqld.log
# # log-warning = 2
# [mysqld-auth]
#
# enabled  = false
# filter   = mysqld-auth
```

```
# port     = 3306
# logpath  = /var/log/mysqld.log
#
#
# # DNS Servers
#
#
# # These jails block attacks against named (bind9). By default, logging is off
# # with bind9 installation. You will need something like this:
# #
# # logging {
# #     channel security_file {
# #         file "/var/log/named/security.log" versions 3 size 30m;
# #         severity dynamic;
# #         print-time yes;
# #     };
# #     category security {
# #         security_file;
# #     };
# # };
# #
# # in your named.conf to provide proper logging
#
# # !!! WARNING !!!
# #   Since UDP is connection-less protocol, spoofing of IP and imitation
# #   of illegal actions is way too simple.  Thus enabling of this filter
# #   might provide an easy way for implementing a DoS against a chosen
# #   victim. See
# #    http://nion.modprobe.de/blog/archives/690-fail2ban-+-dns-fail.html
# #   Please DO NOT USE this jail unless you know what you are doing.
# #[named-refused-udp]
# #
# #enabled  = false
# #port     = domain,953
# #protocol = udp
# #filter   = named-refused
# #logpath  = /var/log/named/security.log
#
# [named-refused-tcp]
#
# enabled  = false
# port     = domain,953
# protocol = tcp
# filter   = named-refused
# logpath  = /var/log/named/security.log
#
# [freeswitch]
#
# enabled  = false
# filter   = freeswitch
# logpath  = /var/log/freeswitch.log
# maxretry = 10
# action   = iptables-multiport[name=freeswitch-tcp, port="5060,5061,5080,5081", protocol=tcp]
#            iptables-multiport[name=freeswitch-udp, port="5060,5061,5080,5081", protocol=udp]
#
# [ejabberd-auth]
#
# enabled  = false
# filter   = ejabberd-auth
# port     = xmpp-client
# protocol = tcp
# logpath  = /var/log/ejabberd/ejabberd.log
#
#
# # Multiple jails, 1 per protocol, are necessary ATM:
# # see https://github.com/fail2ban/fail2ban/issues/37
```

```
# [asterisk-tcp]
#
# enabled  = false
# filter   = asterisk
# port     = 5060,5061
# protocol = tcp
# logpath  = /var/log/asterisk/messages
#
# [asterisk-udp]
#
# enabled  = false
# filter     = asterisk
# port     = 5060,5061
# protocol = udp
# logpath  = /var/log/asterisk/messages
#
#
# # Jail for more extended banning of persistent abusers
# # !!! WARNING !!!
# #   Make sure that your loglevel specified in fail2ban.conf/.local
# #   is not at DEBUG level -- which might then cause fail2ban to fall into
# #   an infinite loop constantly feeding itself with non-informative lines
# [recidive]
#
# enabled  = false
# filter   = recidive
# logpath  = /var/log/fail2ban.log
# action   = iptables-allports[name=recidive]
#            sendmail-whois-lines[name=recidive, logpath=/var/log/fail2ban.log]
# bantime  = 604800  ; 1 week
# findtime = 86400   ; 1 day
# maxretry = 5
#
# # See the IMPORTANT note in action.d/blocklist_de.conf for when to
# # use this action
# #
# # Report block via blocklist.de fail2ban reporting service API
# # See action.d/blocklist_de.conf for more information
# [ssh-blocklist]
#
# enabled  = false
# filter   = sshd
# action   = iptables[name=SSH, port=ssh, protocol=tcp]
#            sendmail-whois[name=SSH, dest="%(destemail)s", sender="%(sender)s",
sendername="%(sendername)s"]
#            blocklist_de[email="%(sender)s", apikey="xxxxxx", service="%(filter)s"]
# logpath  = /var/log/sshd.log
# maxretry = 20
#
#
# # consider low maxretry and a long bantime
# # nobody except your own Nagios server should ever probe nrpe
# [nagios]
# enabled  = false
# filter   = nagios
# action   = iptables[name=Nagios, port=5666, protocol=tcp]
#            sendmail-whois[name=Nagios, dest="%(destemail)s", sender="%(sender)s",
sendername="%(sendername)s"]
# logpath  = /var/log/messages     ; nrpe.cfg may define a different log_facility
# maxretry = 1

EOF

}

config_jailLocal
```

```
####### END :) #######
```