Tasks

WikiSuite | Fail2ban should be checked in clearos (attack detector) to ensure the correct param are set to prevent more than just a few (<10) connection attempts

Fail2ban should be checked in clearos (attack detector) to ensure the correct param are set to prevent more than just a few (<10) connection attempts

Status

Closed

Description

Fail2ban should be checked in clearos (attack detector) to ensure the correct param are set to prevent more than just a few (<10) connection attempts

Reported by

Xavier de Pedro

Priority

2

Area

ClearOS (deprecated)

Details

It currently allowed more than 7000 ssh attempts per day in a real case using ClearOS 7.2. where we installed the attack detector app.

See:

https://www.clearos.com/resources/documentation/clearos/content:en_us:7_ug_attack_detector

And see:

https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-centos-7

Related

- Attack detector (Fail2ban) for Clearos: add more info and options to admin panel

Created

Friday May 20, 2016 02:03:49 EDT

by Xavier de Pedro

LastModif

Saturday July 24, 2021 12:01:40 EDT

Comments

Marc Laporte 2016-11-14 11:07

Should be OK now:
http://wikisuite.org/How-to-install-Attack-Detector-Fail2ban-on-ClearOS

Bernard Sfez 2019-01-18 03:34

Please note that due to some errors in updates fail2ban may fail (silently) to start (3 Clearos 7 for me so far);

I tested using:

```
/usr/bin/fail2ban-client -v -v start
```

to have more information and saw:

```
INFO     Loading files: ['/etc/fail2ban/jail.d/clearos-cyrus-imap.conf']
ERROR  Failed during configuration: File contains no section headers.
file: /etc/fail2ban/jail.d/clearos-cyrus-imap.conf, line: 1
'port = imap,imap3,imaps,pop3,pop3s\n'
```

I deleted "/etc/fail2ban/jail.d/clearos-cyrus-imap.conf" and fail2ban restarted right successfully.

https://www.clearos.com/clearfoundation/social/community/attack-detector-fail2ban-stopped

Nick Howitt 2020-01-27 05:14

This was a bug during an update and has been fixed. Please see https://gitlab.com/clearos/clearfoundation/app-imap/blob/master/packaging/clearos-cyrus-imap.conf for correct entries.

Bernard Sfez 2020-01-30 01:44

Hello Nick, nice to see you here (too).

I recreate clearos-cyrus-imap.conf and copied

exactly what is at
https://gitlab.com/clearos/clearfoundation/app-imap/blob/master/packaging/clearos-cyrus-imap.conf

I stopped fail2ban and start it back.

I had a new error (maybe not related):

```
[root@server jail.d]# fail2ban-client start
2020-01-30 08:34:26,740
fail2ban.configreader   [63796]: ERROR
Found no accessible config files for
'filter.d/sshd-ddos' under /etc/fail2ban
2020-01-30 08:34:26,740 fail2ban.jailreader
[63796]: ERROR   Unable to read the filter
'sshd-ddos'
2020-01-30 08:34:26,740
fail2ban.jailsreader    [63796]: ERROR
Errors in jail 'sshd-ddos'. Skipping...
```

I create manually /etc/fail2ban/filter.d/sshd-ddos.conf and pasted content from :
https://github.com/mikechau/fail2ban-configs/blob/master/filter.d/sshd-ddos.conf

Started normally.
Crossing fingers... 😀

Marc Laporte 2021-07-24 12:02

https://wikisuite.org/blogpost16-WikiSuite-will-now-support-all-major-Linux-distros