Fail2ban – telepítése és beállítása

Írta: YouCanToo

Mit csinál a Fail2ban

A Fail2ban átnézi a napló fájlokat (pl. /var/log/apache/error_log) és letiltja a rosszindulatúnak tűnő IP-ket – túlságosan sok jelszóhiba, exploit keresése stb.. Általában a Fail2ban ezután frissíti a tűzfal beállításait, hogy kitiltsa az adott IP címeket meghatározott időre. A Fail2ban alapból különféle szolgáltatásokhoz (apache, curier, ftp, ssh, stb.) való szűrővel rendelkezik.

Rendszerkövetelmények

Az egyetlen igényelt függőség, ami a Fail2ban futásához kell, a Python. A PCLinuxOS a Pythont alapból telepíti.

Főbb jellemzők

Íme a Fail2ban-ben elérhető főbb funkciók listája.

* Kliens-szerver architektúra.
* Többszálas.
* Nagymértékben állítható.
* FAM-, Gamin-, Pyinotify támogatás.
* Log fájlok elemzése és meghatározott minták keresése.
* Parancs végrehajtása adott minta, azonos IP-cím felől, X-nél több alkalommal történő érzékelése esetén. Az X változtatható.
* Adott idő után egy másik parancs végrehajtása, hogy feloldja az adott IP-cím tiltását.
* Netfilter, illetve Iptables használata alapból, de használhat TCP Wrapper-t (/etc/hosts.deny) és sok más tűzfalat, műveletet.
* Kezeli a naplófájlok rotálását.
* Több szolgáltatást képes egyidejűleg kezelni (sshd, apache, vsftpd, stb.).
* Visszafejti a DNS hostname-t IP címre (óvatosan használd, kikapcsolása „usedns = no”-val).

Telepítés

A fail2ban megtalálható a Synaptic tárolójában. Kérlek, telepítsd a Synaptic-kal. Ha már telepítetted Synaptic-kal, el kell indítani a szolgáltatást.

Konzolban root-ként írd be a következőt.

```
service fail2ban start
```

Valami ilyesmit kell látnod.

```
[root@laptop dwmoar]# service
fail2ban start
Starting fail2ban: [ OK ]
[root@laptop dwmoar]#
```

A fail2ban-szerver státusának ellenőrzése:

Konzolban root-ként írd be a következőt.

```
service fail2ban status
```

Valami ilyesmit kell látnod.

```
[root@laptop dwmoar]# service
fail2ban status
Fail2ban (pid 5166) is running...
Status
|- Number of jail:    1
`- Jail list:    ssh-iptables
[root@laptop dwmoar]#
```

Megjegyzés: a jail (börtön) listája eltérhet, a jail.conf beállítása szerint, a használt szolgáltatások függvényében.

Beállítás

A Fail2Ban-t beállíthatod a /etc/fail2ban/fail2ban.conf fájlon keresztül.

Az alapbeállítások biztonsággal meghagyhatók.

Az /etcfail2ban/jail.conf fájl szerkesztése: a [DEFAULT] résznél a következő változókat keressük

ignoreip = 127.0.0.1/8 ← engedélyezni akarjuk a saját gépet

bantime = 3600 ← Ez 3600 másodperc, vagyis egy óra. Az IP-cím rendszeredből történő kitiltása idejének kiterjesztéséhez növeld.

Maxretry = 3 ← Egy felhasználó ennyiszer próbálkozhat, mielőtt kitiltaná. Nem tanácsos ezt túl nagyra növelni.

Az [ssh-iptables] résznél a következőket ellenőrizzük:

enabled = false ← Váltsd true-ra (igaz) – engedélyezés!

Action = ← Cseréld ki a dest (címzett) részt a saját e-mail címedre

maxretry = 5 ← Ne legyen magasra. (Max. újra-próbálkozás.) Én 3 próbálkozásra csökkentettem.

NE változtass semmi mást, hacsak nem használod az adott szolgáltatást. Pl. a proftpd-t, vsftpd-t stb..

Ha változtattál a jail.conf fájlon, akkor újra kell indítanod a fail2ban szolgáltatást.

Konzolban root-ként írd be a következő parancsot.

```
service fail2ban restart
```

Valami ilyesmit kell látnod.

```
[root@laptop fail2ban]# service
fail2ban restart
 Stopping fail2ban:        [ OK ]
 Starting fail2ban:        [ OK ]
 [root@laptop fail2ban]#
```

A fail2ban futtatása

A fail2ban a PCLinuxOS-ben úgy állítja be magát, hogy automatikusan fusson a rendszer indításakor, vagy újraindításakor.

Javítások a beállításon

Ha Very Secure FTP (VSFTP)-t használsz:

1. javítás: a VSFTP-t úgy állítsd be, hogy „dual_log_enable=YES” legyen és a fail2ban a /var/log/vsftpd.log-ot figyelje. Ez a log fájl mutatja a bejövő IP-címeket a DNS nevek helyett.

2. javítás: a /etc/vsftpd/vsftpd.conf-hoz add a „use_localtime=YES”-t és indítsd újra a vsftpd szolgáltatást.

További információk

A fail2ban-nel kapcsolatos további információkért keresd az online kézikönyvüket a http://www.fail2ban.org/wiki/index.php/MANUAL_0_8 címen.