Fail2ban - konfiguracija i uporaba, 2. dio

U prvom nastavku [1] iz serije članaka o fail2ban sustavu zaštite uveli smo vas u osnovne postavke i način rada fail2ban sustava. U ovom nastavku ćemo malo više obratiti pažnju na ono što se zbiva “ispod haube”.

Fail2ban rabi standardni način rada, putem *daemona* i klijentskog programa. S daemon programom ne bismo trebali imati nikakav direktan kontakt, jer se sve poruke daemonu mogu navesti preko klijenta. Daemon, ipak, kod starta prima određene opcije, pa ćemo ih navesti.

```
  -b start in background
 -f start in foreground
 -s <FILE> socket path
 -x force execution of the server (remove socket file)
 -h, --help display this help message
 -V, --version print the version
```

Kao što se može vidjeti, opcije su iskoristive praktički samo kod *debugiranja* i testiranja, pa se nećemo na njima zadržavati, jer je opis samorazumljiv. S druge strane, klijent prima sljedeće naredbe:

```
  -c <DIR> configuration directory
 -s <FILE> socket path
 -d dump configuration. For debugging
 -i  interactive mode
 -v increase verbosity
 -q decrease verbosity
 -x force execution of the server (remove socket file)
 -h, --help display this help message
 -V, --version print the version
```

I ovdje možemo vidjeti da opcije prije svega služe za razna testiranja prije puštanja u produkciju. Najzanimljivije su opcije za smanjivanje i povećavanje razine zapisa u logovima (*verbosity*). Razina 1 je minimalna razina, a razina 4 se rabi samo u postupku eventualnog *debugiranja*.

No, najsnažnija karakteristika klijenta je direktna mogućnost konfiguriranja cijelog sustava, baš kao da smo rabili konfiguracijske datoteke. Naredbi je mnogo, pa ćemo opisati najkorisnije, a druge ćemo samo spomenuti. Za daljnje informacije pogledajte dokumentaciju na adresi http://www.fail2ban.org/wiki/index.php/MANUAL_0_8 [2].

Naredbe koje fail2ban-client podržava:

```
  start          pokre?e se daemon i svi "zatvori" (jailovi)
 reload        ponovno se u?itava konfiguracija
```

```
 reload <JAIL> ponovo se u?itava samo zatvor pod imenom <JAIL>
 stop          zaustavlja se daemon i svi zatvori
 status        dobija se informacija o trenutnom stanju daemona
 ping          provjerava se je li daemon uop?e pokrenut

  set loglevel <LEVEL>
postavlja se razina informativnosti (verbosity) na razinu <LEVEL>.
 get loglevel ispisuje razinu informativnosti
 get/set …
```

Opcija iza get/set naredbi ima mnogo, primjerice *addignoreip*, *addlogpath*, *addfailregex*, *findtime* i tako dalje. No, vjerojatno je besmisleno na ovaj način učiti konfigurirati fail2ban, i držati se konfiguriranja preko standardnih konfiguracijskih datoteka. Ipak, neke naredbe bi bilo dobro znati, primjerice:

```
# fail2ban-client get loglevel
 Current logging level is INFO
```

Dakle, trenutna razina je INFO (razina 3). Ostale razine su: ERROR (1), WARN (2) i DEBUG (4).

Fail2ban ima i interaktivni način, pa ćemo ostale opcije demonstarirati na taj način. Ulazak u interaktivni način je pomoću opcije "-i".

```
# fail2ban-client -i
fail2ban> get logtarget
Current logging target is:
`- /var/log/fail2ban.log
```

Dakle, ova naredba se isto mogla izvršiti i direktno iz naredbene linije, a prikazuje u koju datoteku se zapisuju logovi.

```
fail2ban> ping
Server replied: pong
```

Slično kao i standardna naredba "ping" koja daje osnovnu informaciju je li mrežni uređaj aktivan, i ovdje ona samo daje potvrdu da je daemon "živ", bez dodatnih informacija.

```
fail2ban> status
Status
|- Number of jail: 2
`- Jail list: pam-generic, ssh
```

Naredba "status" bez dodatnih opcija daje samo popis trenutno aktivnih zatvora.

```
fail2ban> status ssh
Status for the jail: ssh
|- filter
| |- File list: /var/log/auth.log
| |- Currently failed: 8
| `- Total failed: 6143
`- action
    |- Currently banned: 0
    | `- IP list:
    `- Total banned: 17
```

Nešto izdašniji ispis daje naredba "status <JAIL>", gdje ćemo dobiti statističke podatke o tome koliko je adresa trenutno na "čekanju", te koliko ih je trenutno na crnoj listi. Adresa će na crnu listu doći kad prekorači zadane parametre.

```
fail2ban> stop ssh
Jail stopped
```

Sa naredbom "stop" možemo određene zatvore zaustaviti, bilo radi dodatne konfiguracije, bilo radi pogrešnog rada, (pre)opeterećenja sustava i slično.

Kad smo se upoznali s osnovama i načinom rada, dalje je prilično jednostavno. Nakon instalacije paketa, automatski miate zaštitu od SSH i PAM napada (a autentikaciju preko PAM-a rabi većina servisa, primjerice login). Neki za autentikaciju ne rabe PAM, primjerice Apache može rabiti direktno LDAP, ili vlastiti htpasswd mehanizam. U tom slučaju, sve što trebate učiniti je uključiti odgovrajući zatvor u jail.conf:

```
[apache]

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

Za uključivanje je dovoljno promijeniti prvi redak u:

```
enabled = true
```

Nakon toga samo treba napraviti *reload*:

```
# fail2ban-client reload
```

i provjeriti je li zatvor uključen:

```
# fail2ban-client status
Status
|- Number of jail:      3
`- Jail list:           apache, pam-generic, ssh
```

Od tog trenutka je aktivna i zaštita definirana s parametrom *failregex* unutar datoteke /etc/fail2ban/filter.d/apache-auth.conf.

Slična stvar je i sa drugim servisima, jedino kod mail servisa (kod nas je standardan Postfix), možda će trebati promijeniti putanju do logova:

```
[postfix]
enabled  = true
port     = smtp,ssmtp
filter   = postfix
logpath  = /var/log/mail.log
```

u

```
logpath  = /var/log/mail/mail.log
```

U sljedećem, zadnjem, nastavku, pokazat ćemo vam kako prilagoditi fail2ban svojim potrebama, te napraviti vlastite filtere i akcije, u slučaju da ne postoje odgovarajuće u postojećoj distribuciji.

- Logirajte [3] se za dodavanje komentara

čet, 2009-04-16 15:46 - Željko Boroš**Kuharice:** Linux [4]
Kategorije: Software [5]
Servisi [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/557

Links
[1] https://sysportal.carnet.hr./node/544
[2] http://www.fail2ban.org/wiki/index.php/MANUAL_0_8
[3] https://sysportal.carnet.hr./sysportallogin
[4] https://sysportal.carnet.hr./taxonomy/term/17
[5] https://sysportal.carnet.hr./taxonomy/term/25
[6] https://sysportal.carnet.hr./taxonomy/term/28