fail2ban

context

dit document beschrijft de werking van fail2ban, een intrusion-prevention system (**IPS**) dat ip adressen blokkeert waarvan meermaals gefaalde aanmeldpogingen afkomstig zijn.

werking

fail2ban monitort **logboeken** van Linux services op gefaalde aanmeldpogingen. Zodra het aantal pogingen is overschreden, voegt fail2ban een firewall regel toe waardoor het ipdres voor bepaalde tijd wordt geblokkkeerd.
Zodra die tijd is verstreken, wordt de firewall regel automatisch verwijderd waardoor het adres wordt vrijgegeven en de host opnieuw kan aanmelden.

Het programma bestaat uit 3 componenten: server, client en configuratiebestanden

server

- fail2ban-server monitort de **logboeken** van Linux services op basis van **filters**.
  Voor elke gefaalde of onrechtmatige aanmeldpoging bestaat er een reguliere expressie
- op basis van het aantal gefaalde pogingen onderneemt de server **actions** die meestal neerkomen op een firewall regel toevoegen die verkeer vanaf die bepaalde host blokkeert (**ban**)
- voor elke service die wordt bewaakt, wordt een zgn **jail** aangemaakt, een combinatie van filters en actions.
- na bepaalde tijd wordt die firewall regel automatisch gewist zodat een host vrijgegeven (**unban**) wordt.
- het logbestand staat onder /var/log/fail2ban.log

```
2019-11-21 16:32:30,396 fail2ban.actions        [23475]: INFO      banTime: 600
2019-11-21 16:32:30,400 fail2ban.jail           [23475]: INFO    Jail 'sshd' started
2019-11-21 16:38:07,795 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:38:07
2019-11-21 16:38:17,014 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:38:17
2019-11-21 16:38:23,298 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:38:23
2019-11-21 16:38:29,720 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:38:29
2019-11-21 16:38:34,742 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:38:34
2019-11-21 16:38:34,899 fail2ban.actions        [23475]: NOTICE  [sshd] Ban 213.246.197.130
2019-11-21 16:39:01,279 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:39:01
2019-11-21 16:39:11,194 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:39:11
2019-11-21 16:39:16,117 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:39:16
2019-11-21 16:39:22,050 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:39:21
2019-11-21 16:39:29,571 fail2ban.filter         [23475]: INFO    [sshd] Found 213.246.197.130 - 2019-11-21 16:39:29
2019-11-21 16:39:29,611 fail2ban.actions        [23475]: NOTICE  [sshd] 213.246.197.130 already banned
```

client

- fail2ban-client: configureert de server en kan ipadressen handmatig vrijgeven.
- meestbruikte commando's:
  - status van faiL2ban

```
fail2ban-client status
```

  - status van een specifieke jail:

```
fail2ban-client status sshd
```

  - ip adres vrijgeven:

```
fail2ban-client unban 10.11.12.13
```

configuratiebestanden

/etc/fail2ban/

fail2ban.conf

- algemene programma werking
- bewaar je eigen instellingen in **fail2ban.local** zodat je instellingen niet overschreven worden bij eerstvolgende update. vb:
  [Definition]
  loglevel = DEBUG
  logtarget = /var/log/fail2ban.log

filter.d

- deze directory bevat voor elke Linux service een .conf-bestand waarin de reguliere expressies staat voor een gefaalde aanmeldpoging.

actions.d

- voor elke firewall staat hier de specifieke syntax om een firewall regel toe te voegen om een ipadres te bannen en unbannen.
- bevat ook enkele bruikbare mail configuraties zodat een mail kan verstuurd worden zodra een ipadres is geblokkeerd.

jail.conf

- globale instellingen voor het vergrendelingsbeleid:
  - maximaal aantal foutieve aanmeldpogingen

    - hoelang wordt het ip adres geblokkeerd
    - welke ipadressen moeten gewhitelist worden?
- bewaar je eigen instellingen in **jail.local** zodat je instellingen niet overschreven worden bij eerstvolgende update. vb:
  [DEFAULT]
  bantime = 30m
  findtime = 10m
  maxretry = 10
  banaction = ufw
  banaction_allports = ufw

jail.d

- een jail per service
- voorbeeld:
  [sshd]
  enabled = true
  port = 12345
  filter = sshd
  logpath = /var/log/auth.log
  maxretry = 3
  bantime = 10 min

Great Fun

Als je fail2ban es lekker aan het werk wilt zetten:

- zet een Linux bakkie op het internet
- maak die bereikbaar op een standaard poort.
- zorg dat er enkel kan aangemeld worden met private/public key
- stel fail2ban in dattie gedurende 1 uur ip adressen blokkeert
- laat em een weekje ongemoeid en ga dan es door je logboek.

opvolgen

zie: fail2ban opvolgen

meer info

- man page
- installatie
- fail2ban opvolgen
- using fail2ban

Linux