fail2ban opvolgen

context

dit document beschrijft hoe je de werking van fail2ban opvolgt.

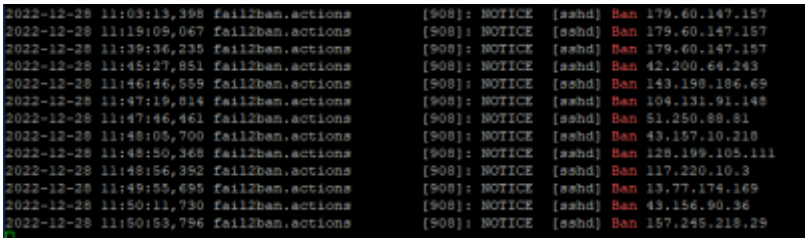
stappenplan

- meld aan op het Linux systeem en voer uit: `fail2ban-client status sshd`
- dit geeft de activiteit op je systeem weer:

```
Status for the jail: sshd
|- Filter
|  |- Currently failed: 10
|  |- Total failed:     1661
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 6
   |- Total banned:     358
   `- Banned IP list:   65.108.213.31 103.250.10.186 137.184.41.13
24.69.190.84 208.109.13.144 94.101.178.121
```

- analyseer de eingelijke activiteit (`view /var/log/fail2ban.log`)
  - worden hosts geband na het aangegeven aantal aanmeldpogingen (`maxretry =`) binnen aangeduide tijd (`findtime =`) voor de aangeduide duur (`bantime =`)?
  - kijk de 10 meest voorkomende IP meerdere na die geband worden: `grep Ban /var/log/fail2ban.log |awk '{print $8}'|sort|uniq -d -c|sort -k1 -n -r|head -10`
  - kijk de 10 meest voorkomende gebruikers na waarmee wordt aangemeld: `grep invalid /var/log/auth.log|awk '{print $10}'|sort|uniq -d -c|sort -k1 -n -r|head -10`
  - blokkeer IP's die meermaals worden geband: `ufw deny from <ip> to any`
- Om Bans online te volgen:

```
tail -f /var/log/fail2ban.log|grep Ban
```



meer info

- fail2ban
- using fail2ban

Linux