

Table of Contents

Tutorial Instalasi Fail2Ban & Tips Trick 1

Instalasi fail2ban di Centos 1

Konfigurasi Fail2Ban 1

Tutorial Instalasi Fail2Ban & Tips Trick

Fail2ban adalah aplikasi bruteforce detection berdasarkan log file.

Instalasi fail2ban di Centos

```
yum install fail2ban -y
```

Konfigurasi Fail2Ban

Kami menggunakan fail2ban untuk membaca log haproxy. Log yang kami baca adalah aktifitas login menggunakan mekanisme POST pada url wp-login.php

```
nano nano /etc/fail2ban/filter.d/haproxy-wp.conf
```

kami isi

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = haproxy

failregex = ^.*haproxy\[([0-9]+\)]*: <HOST>:.* "POST /wp-login.php HTTP/1.1"$
ignoreregex =
```

Pastikan anda sudah menguji regular expresion tersebut dengan menggunakan

```
fail2ban-regex /var/log/haproxy.log /etc/fail2ban/filter.d/haproxy-wp.conf
```

dan apabila regex nya benar hasilnya seperti ini

```
Results
=====

Failregex: 7660 total
|- #) [# of hits] regular expression
|  1) [7660] ^.*haproxy\[([0-9]+\)]*: <HOST>:.* "POST /wp-login.php
HTTP/1.1"$
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
```

```
| [520991] (?:DAY )?MON Day 24hour:Minute:Second(?:\.\Microseconds)?(?:Year)?  
`-  
  
Lines: 520991 lines, 0 ignored, 7660 matched, 513331 missed  
[processed in 126.74 sec]
```

sekitar 7660 baris match dengan regex tersebut.

selanjutnya adalah membuat jail

```
nano /etc/fail2ban/jail.d/haproxy-wp.conf
```

isi dengan

```
[haproxy-wp]  
enabled = true  
bantime = 36000  
findtime = 120  
maxretry = 6  
filter = haproxy-wp  
logpath = /var/log/haproxy.log  
port = http,https  
action = csf-ip-deny
```

selanjutnya membuat action yang di integrasikan dengan CSF.

```
nano /etc/fail2ban/action.d/csf-ip-deny.conf
```

isi dengan

```
# CSF / fail2ban integration from The Digital FAQ (digitalFAQ.com)  
  
[Definition]  
actionstart =  
actionstop =  
actioncheck =  
actionban = csf -d <ip> Added by Fail2Ban for <name>  
actionunban = csf -dr <ip>  
  
[Init]  
name = haproxy-wp
```

From:
<https://www.pusathosting.com/kb/> - **PusatHosting Wiki**

Permanent link:
<https://www.pusathosting.com/kb/linux/fail2ban?rev=1520156427>

Last update: **2018/03/04 04:40**



