H??ng d?n cài ??t Fail2Ban b?o v? SSH trên CentOS 6

admin Sun, Apr 14, 2019 Cài Đặt Cơ Bản & Hướng Dẫn 0 1721

Fail2Ban là m?t ?ng d?ng ch?y n?n theo dõi log file ?? phát hi?n nh?ng ??a ch? IP ??ng nh?p sai password SSH nhi?u l?n. Sau ?ó, Fail2Ban s? d?ng **iptable firewall rules** ?? block ngay ??a ch? IP v?i m?t kho?ng th?i gian ??nh tr??c.

Cài ??t Fail2Ban

Chúng ta s? cài ??t Fail2Ban thông qua Repo EPEL

```
# yum install epel-release# yum install fail2ban
```

C?u hình Fail2Ban

```
# nano /etc/fail2ban/jail.conf
```

Sau khi cài ??t xong, b?n m? file c?u hình c?a Fail2Ban lên s? th?y m?t s? thông s? nh? sau:

```
[DEFAULT]# "ignoreip" can be an IP address, a CIDR mask or
 a DNS host. Fail2ban will not# ban a host which matches a
```

```
n address in this list. Several addresses can be# defined
using space separator.ignoreip = 127.0.0.1# "bantime" is t
he number of seconds that a host is banned.bantime = 600#
A host is banned if it has generated "maxretry" during the
 last "findtime"# seconds.findtime = 600# "maxretry" is th
e number of failures before a host get banned.maxretry = 3
```

Trong ?ó

- **ignoreip**: không block nh?ng ??a ch? này
- **bantime**: kho?ng th?i gian (giây) block IP
- **findtime**: kho?ng th?i gian (giây) m?t IP ph?i login thành công
- **maxretry**: s? l?n login false t?i ?a

C?u hình m?c ??nh c?a Fail2Ban khá là ?n r?i, chúng ta không c?n thi?t ph?i c?p nh?t mà ??n b??c ti?p theo.

C?u hình Fail2Ban b?o v? SSH

T?o file c?u hình

```
# nano /etc/fail2ban/jail.local
```

Và s? d?ng n?i dung sau:

```
  GNU nano 2.0.9          File: /etc/fail2ban/jail.local                Modified

[ssh-iptables]

enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
#           sendmail-whois[name=SSH, dest=root, sender=fail2ban@example.com]
logpath  = /var/log/secure
maxretry = 2
bantime = 3600
```

Trong ?ó

- **enabled**: kích ho?t b?o v?, n?u mu?n t?t b?n hãy chuy?n thành false
- **filter**: gi? m?c ??nh ?? s? d?ng file c?u hình /etc/fail2ban/filter.d/sshd.conf
- **action**: fail2ban s? ban ??a ch? IP n?u match filter /etc/fail2ban/action.d/iptables.conf. N?u b?n ?ã thay ??i port ssh, s?a ?o?n port=ssh b?ng port m?i, ví d? port=2222
- **logpath**: ???ng d?n file log fail2ban s? d?ng ?? theo dõi
- **maxretry**: s? l?n login false t?i ?a

Kh?i ??ng Service Fail2Ban

```
# chkconfig --level 23 fail2ban on# service fail2ban start
```

Cu?i cùng check l?i iptables xem ?ã có rule c?a Fail2Ban ch?a:

```
# iptables -L
```

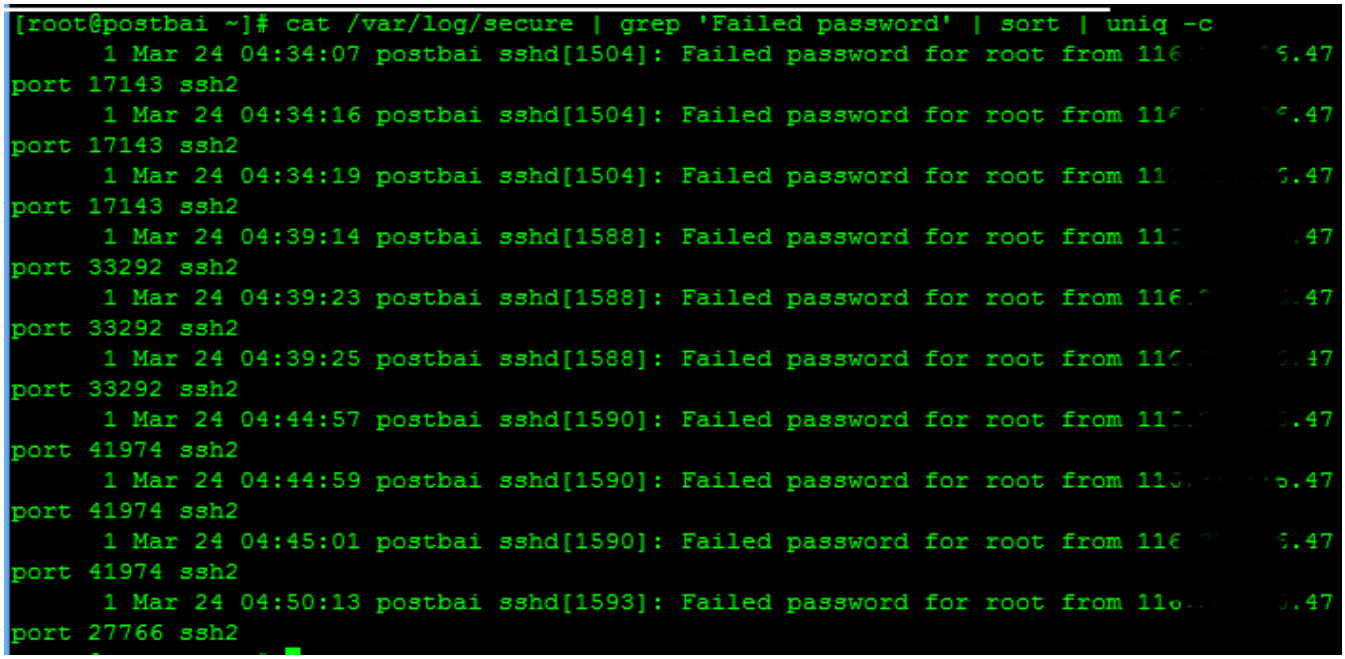
```
Running Transaction
  Installing : nano-2.0.9-7.el6.x86_64                                      1/1
  Verifying  : nano-2.0.9-7.el6.x86_64                                      1/1

Installed:
  nano.x86_64 0:2.0.9-7.el6

Complete!
[root@postbai ~]# nano /etc/fail2ban/jail.conf
[root@postbai ~]# nano /etc/fail2ban/jail.local
[root@postbai ~]# chkconfig --level 23 fail2ban on
[root@postbai ~]# service fail2ban start
Starting fail2ban:                                          [  OK  ]
[root@postbai ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-SSH    tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISH
ED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-p
rohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-p
rohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-SSH (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

Theo dõi SSH login

B?n có th? s? d?ng l?nh sau ?? bi?t ???c VPS/Server ?ã t?ng b? t?n công SSH ch?a:

```
# cat /var/log/secure | grep ’Failed password’ | sort | uniq -c
```

K?t qu? th??ng s? là nh? bên d??i, ?ã t?ng có r?t nhi?u ??t t?n công:



```
[root@postbai ~]# cat /var/log/secure | grep 'Failed password' | sort | uniq -c
      1 Mar 24 04:34:07 postbai sshd[1504]: Failed password for root from 116.[illegible]5.47
port 17143 ssh2
      1 Mar 24 04:34:16 postbai sshd[1504]: Failed password for root from 116.[illegible].47
port 17143 ssh2
      1 Mar 24 04:34:19 postbai sshd[1504]: Failed password for root from 11[illegible].47
port 17143 ssh2
      1 Mar 24 04:39:14 postbai sshd[1588]: Failed password for root from 11[illegible].47
port 33292 ssh2
      1 Mar 24 04:39:23 postbai sshd[1588]: Failed password for root from 116.[illegible].47
port 33292 ssh2
      1 Mar 24 04:39:25 postbai sshd[1588]: Failed password for root from 11[illegible].47
port 33292 ssh2
      1 Mar 24 04:44:57 postbai sshd[1590]: Failed password for root from 11[illegible].47
port 41974 ssh2
      1 Mar 24 04:44:59 postbai sshd[1590]: Failed password for root from 11[illegible].47
port 41974 ssh2
      1 Mar 24 04:45:01 postbai sshd[1590]: Failed password for root from 116.[illegible].47
port 41974 ssh2
      1 Mar 24 04:50:13 postbai sshd[1593]: Failed password for root from 11[illegible].47
port 27766 ssh2
```

?? xem IP ?ã b? banned b?i Fail2Ban b?n s? d?ng l?nh:

```
# fail2ban-client status ssh-iptables
```

Output tr? v? s? có d?ng nh? th? này:

```
Status for the jail: ssh-iptables|- Filter| |- Currently failed: 1| |- Total failed: 6| `- File list: /var/log/secure`- Actions|- Currently banned: 1|- Total banned: 1`- Banned IP list: 116.***.***.147(ip b? banned)
```

?? xóa IP kh?i danh sách banned, b?n s? d?ng l?nh sau

```
# fail2ban-client set ssh-iptables unbanip 116.***.***.147
(ip mu?n xóa kh?i danh sách banned)
```

Hi v?ng v?i **Fail2Ban**, chúng ta s? ng?n ch?n ???c các cu?c t?n công s? b? vào SSH, h?n g?p l?i các b?n trong các bài ti?p theo, chúc các b?n thành công.

Online URL: https://huongdan.maxserver.com/article-85.html