



Fail2ban使用心得分享

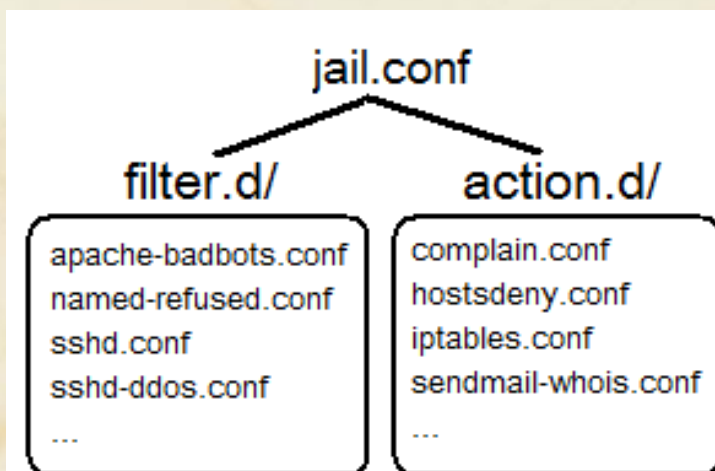
復旦高中 陳宏智

Fail2ban

- Fail2ban 是一套以 Python 語言所撰寫的 GPLv2 授權軟體，藉由分析**系統紀錄檔**，設定過濾條件 (filter) 及動作 (action)。當符合我們所設定的過濾條件時，將觸發相對動作來達到防禦效果。

Fail2ban架構

- **jail.(conf|local)**
用來設定 jail，即是定義 filter 與 action 的對應關係。
- **filter.d/**
用來定義過濾條件 (filter)，目錄下已定義多種既有的過濾條件，常見的軟體有 apache、sshd、vsftpd、postfix 等，而常見記錄檔格式也可能為 Syslog、Common Log Format 等。
- **action.d/**
用來定義動作內容 (action)，目錄下已定義多種既有的動作內容，如「sendmail 寄信通知」、「iptables 阻擋來源位址」、「使用 whois 查詢來源 domain 資訊」或「自動通知該來源 IP 的管理者」。





目前郵件伺服器設定功能

- 監看maillog檔，除了本機(127.0.0.1)IP之外：
- 同一IP，在20分鐘內，達6次SASL登入失敗，使用iptables設定檔，阻斷1小時。



目前郵件伺服器設定功能

- 監看Fail2ban.log檔，除了本機(127.0.0.1)IP之外：
- 同一IP，在1天之內，達3次阻斷1小時之後，第4次阻斷時間延長為3天。

Jail.conf

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)

[DEFAULT]
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1

# "bantime" is the number of seconds that a host is banned.
bantime = 3600

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 1200

# "maxretry" is the number of failures before a host get banned.
maxretry = 6

[sasl-iptables]

enabled = true
filter = sasl
backend = polling
action = iptables[name=sasl, port=smtp, protocol=tcp]
logpath = /var/log/maillog
```

設定過濾條件 (maillog)

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
Apr 19 08:22:49 mail postfix/smtpd[12888]: lost connection after AUTH from unknown[222.248.230.6]
Apr 19 08:22:49 mail postfix/smtpd[12888]: disconnect from unknown[222.248.230.6]
Apr 19 08:22:51 mail postfix/smtpd[13168]: connect from unknown[222.248.230.6]
Apr 19 08:22:51 mail postfix/smtpd[13138]: connect from unknown[222.248.230.6]
Apr 19 08:22:51 mail postfix/smtpd[12888]: connect from unknown[222.248.230.6]
Apr 19 08:22:51 mail postfix/smtpd[13428]: connect from unknown[195.45.98.189]
Apr 19 08:22:52 mail postfix/smtpd[13168]: warning: unknown[222.248.230.6]: SASL LOGIN authentication failed: authentication failure
Apr 19 08:22:52 mail postfix/smtpd[13138]: warning: unknown[222.248.230.6]: SASL LOGIN authentication failed: authentication failure
Apr 19 08:22:52 mail postfix/smtpd[12888]: warning: unknown[222.248.230.6]: SASL LOGIN authentication failed: authentication failure
Apr 19 08:22:53 mail postfix/smtpd[13168]: lost connection after AUTH from unknown[222.248.230.6]
Apr 19 08:22:53 mail postfix/smtpd[13168]: disconnect from unknown[222.248.230.6]
Apr 19 08:22:53 mail postfix/smtpd[13138]: lost connection after AUTH from unknown[222.248.230.6]
Apr 19 08:22:53 mail postfix/smtpd[13138]: disconnect from unknown[222.248.230.6]
Apr 19 08:22:53 mail postfix/smtpd[12888]: lost connection after AUTH from unknown[222.248.230.6]
Apr 19 08:22:53 mail postfix/smtpd[12888]: disconnect from unknown[222.248.230.6]
@
641824,1 99%
```

正規表示語法

- **/var/log/maillog:**
- warning: unknown[222.248.230.6]: SASL LOGIN authentication failed: authentication failure
- **/etc/fail2ban/filter.d/sasl.conf :**
- warning: .*\[<HOST>\]: SASL LOGIN authentication failed

Filter.d/sasl.conf

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)

#
# Author: Yaroslav Halchenko
#
# $Revision: 728 $
#

[Definition]

# Option: failregex
# Notes: regex to match the password failures messages in the logfile. The
#       host must be matched by a group named "host". The tag "<HOST>" can
#       be used for standard IP/hostname matching and is only an alias for
#       (?:::f{4,6}:)?(?P<host>[\w\.-^_]+)
# Values: TEXT
#
#failregex = (?i): warning: [-_\w]+\[<HOST>\]: SASL (?:(LOGIN|PLAIN)(?:(CRAM|DIGEST)
#              (MD5) authentication failed/[-_A-Za-z0-9+/]*=[0,2])?$
failregex = warning: .*\[<HOST>\]: SASL LOGIN authentication failed
# Option: ignoreregex
# Notes: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#
ignoreregex =
```

Action.d/iptables.conf

```
root@mail:/etc/fail2ban/action.d [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
I iptables.conf Row 31 Col 1 12:06 Ctrl-K H for help
# Option: actionban
# Notes.: command executed when banning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   <ip> IP address
#         <failures> number of failures
#         <time> unix timestamp of the ban time
# Values: CMD
#
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
#
# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   <ip> IP address
#         <failures> number of failures
#         <time> unix timestamp of the ban time
# Values: CMD
#
actionunban = iptables -D fail2ban-<name> -s <ip> -j DROP
[Init]
```



/var/log/fail2ban.log

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
2011-04-19 00:39:01,185 fail2ban.actions: WARNING [sasl-iptables] Unban 110.203.8
6.161
2011-04-19 01:50:59,466 fail2ban.actions: WARNING [sasl-iptables] Ban 60.22.246.4
5
2011-04-19 02:00:41,838 fail2ban.actions: WARNING [dovecot-pop3imap] Ban 210.77.7
5.173
2011-04-19 02:11:11,557 fail2ban.actions: WARNING [sasl-iptables] Ban 222.246.85.
121
2011-04-19 02:50:59,725 fail2ban.actions: WARNING [sasl-iptables] Unban 60.22.246
.45
2011-04-19 02:53:50,274 fail2ban.actions: WARNING [longban] Unban 117.44.56.180
2011-04-19 03:00:42,110 fail2ban.actions: WARNING [dovecot-pop3imap] Unban 210.77
.75.173
2011-04-19 03:11:11,811 fail2ban.actions: WARNING [sasl-iptables] Unban 222.246.8
5.121
2011-04-19 03:38:28,909 fail2ban.actions: WARNING [sasl-iptables] Ban 60.22.235.2
43
2011-04-19 04:38:29,173 fail2ban.actions: WARNING [sasl-iptables] Unban 60.22.235
.243
2011-04-19 08:22:54,095 fail2ban.actions: WARNING [sasl-iptables] Ban 222.248.230
.6
2011-04-19 09:18:50,554 fail2ban.actions: WARNING [longban] Unban 119.142.184.159
@
318,1 99%
```


/var/log/messages

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
Apr 19 08:01:01 mail freshclam[13084]: ClamAV update process started at Tue Apr 19 08:01:01 2011
Apr 19 08:01:01 mail freshclam[13084]: main.cvd is up to date (version: 53, sigs: 846214, f-level: 53, builder: sven)
Apr 19 08:01:01 mail freshclam[13084]: daily.cld is up to date (version: 12995, sigs: 99073, f-level: 60, builder: ccordes)
Apr 19 08:01:01 mail freshclam[13084]: bytecode.cld is up to date (version: 143, sigs: 40, f-level: 60, builder: edwin)
Apr 19 08:22:49 mail saslauthd[2675]: do_auth : auth failure: [user=afu0208] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:22:49 mail saslauthd[2677]: do_auth : auth failure: [user=ts6336] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:22:49 mail saslauthd[2676]: do_auth : auth failure: [user=ingrid] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:22:52 mail saslauthd[2675]: do_auth : auth failure: [user=ts6336] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:22:52 mail saslauthd[2674]: do_auth : auth failure: [user=ingrid] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:22:52 mail saslauthd[2676]: do_auth : auth failure: [user=afu0208] [service=smtp] [realm=] [mech=shadow] [reason=Unknown]
Apr 19 08:57:05 mail freshclam[12829]: Received signal: wake up
Apr 19 08:57:05 mail freshclam[12829]: ClamAV update process started at Tue Apr 19 08:57:05 2011
4000,1 99%
```


Fail2ban-clients status

```
root@mail:/var/log [81x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
cron.2      messages.1      rpmpkgs.3      yum.log.1
cron.3      messages.2      rpmpkgs.4
cron.4      messages.3      samba
cups        messages.4      scrollkeeper.log
[root@mail log]# vim /etc/fail2ban/filter.d/sasl.conf
[root@mail log]# vim /etc/fail2ban/jail.conf
[root@mail log]# vim /etc/fail2ban/jail.conf
[root@mail log]# fail2ban-clients status
-bash: fail2ban-clients: command not found
[root@mail log]# fail2ban-client status
Status
|- Number of jail:      4
`- Jail list:          dovecot-pop3imap, ssh-iptables, longban, sasl-iptables
[root@mail log]# fail2ban-client status sasl-iptables
Status for the jail: sasl-iptables
|- filter
| |- File list:        /var/log/maillog
| |- Currently failed: 1
| `-- Total failed:    921
`- action
  |- Currently banned: 0
  | `-- IP list:
  `-- Total banned:    134
[root@mail log]#
```

SASL 認證失敗次數 統計

安裝後		安裝前	
100-04-24	144	100-03-29	5217
100-04-23	124	100-03-28	2707
100-04-22	226	100-03-27	2907

資訊來源

- 清華大學計算機與通訊中心－網路系統組
- <http://net.nthu.edu.tw/2009/security:fail2ban>
- 個人實做