Fail2ban 杜絕很煩人的 bot-net 攻擊

張明泰 mtchang.tw@gmail.com

fail2ban 是一個針對 log 檔案(/var/log/secure 或 /var/log/apache2/error_log 之類的)中密碼輸入錯誤的紀錄，檢查並更新防火牆規則進行 ban ip 動作的服務，可以有效的對付 bot-net(殭屍網路) 的惡意掃瞄程式。

在 rhel/centos 的版本中預設套件中沒有收錄，如果要安裝需要安裝 EPEL 的套件 EPEL 是針對 fedora 中沒有被收錄在 rhel 的套件，做打包彙整。提供給 RHEL/CENTOS 使用的套件。如果要安裝 EPEL 套件來源方法很簡單，請在系統的 /etc/yum.repos.d/ 目錄建立一個檔案 epel.repo 並且放入底下的內容，皆下來安裝軟體的時候就會更新了。底下是以 5 版 x86_64 為安裝來源如果你的版本比較新，請觀看 EPEL 官方網站(http://fedoraproject.org/wiki/EPEL)找比較新的安裝來源。

```
[root@lab yum.repos.d]# nano epel.repo
[epel5]
enabled = 1
name = epel 5
baseurl = http://mirror01.idc.hinet.net/EPEL/5/x86_64/
gpgcheck = 0

[epel5Server]
enabled = 1
name = epel 5Server
baseurl = http://mirror01.idc.hinet.net/EPEL/5Server/x86_64/
gpgcheck = 0

[epel5Client]
enabled = 1
name = epel 5Client
baseurl = http://mirror01.idc.hinet.net/EPEL/5Client/x86_64/
gpgcheck = 0
```

* yum EPEL 安裝路徑來源設定好後，就可以透過 yum 安裝 fail2ban 軟體

```
# 安莊 fail2ban
[root@lab ~]# yum install fail2ban
```

```
# 因為他是以服務型態在系統中工綽，需要重新啟動此服務才會工作
[root@lab ~]# /etc/init.d/fail2ban restart
```

* 驗證看有沒有真的跑起來 ps –auxww

```
[root@lab ~]# ps auxw | grep fail2ban
root      15572  0.0  0.4 198536  5324 ?        Sl   10:18   0:00
/usr/bin/python /usr/bck -x
root      26071  0.0  0.0  61172   748 pts/1    S+   10:42   0:00 grep
fail2ban
```

此服務的系統服務設定檔主要為 /etc/fail2ban/fail2ban.conf ，另一個為服務監控的設定檔 /etc/fail2ban/jail.conf 格式類似底下這樣，設定檔案有很多設定的範例，底下以 sshd 服務做說明：

```
[ssh-iptables]
# 需要啟動的服務把 enabled 設定為 true ，此 sshd 的偵測 log 功能才會啟動。
enabled = true
filter = sshd
# 當發現符合條件時，該做什麼動作
action = iptables[name=SSH, port=ssh, protocol=tcp]
sendmail-whois[name=SSH, dest=root, sender=fail2ban@mail.com]
# 針對那個 log 檔做紀錄分析
logpath = /var/log/secure
# 密碼可以失敗幾次
maxretry = 5
```

實驗測試：我從 110.110.69.10 連續五次故意密碼錯誤，系統的 log 就會有這樣的紀錄

```
[root@lab log]# tail /var/log/secure -n 10 | grep 'Failed password '
Mar 31 10:23:51 lab sshd[17679]: Failed password for mtchang from 110.110.69.10
port 41814 ssh2
Mar 31 10:25:55 lab sshd[19771]: Failed password for mtchang from 110.110.69.10
port 41815 ssh2
Mar 31 10:25:55 lab sshd[19771]: Failed password for mtchang from 110.110.69.10
port 41815 ssh2
Mar 31 10:25:57 lab sshd[19773]: Failed password for mtchang from 110.110.69.10
port 41816 ssh2
Mar 31 10:25:57 lab sshd[19773]: Failed password for mtchang from 110.110.69.10
port 41816 ssh2
```

這時候 fail2ban 發現此 ip 一直產生錯誤的密碼紀錄，自動將此 ip 加入 iptables 規則中，這疑似有問題的連線就自動被擋在外面了。

```
[root@lab log]# iptables -nL -t filter
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-SSH  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-SSH (1 references)
target     prot opt source               destination
DROP       all  --  110.110.69.10        0.0.0.0/0
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

但不用擔心，這個規則並不會永久存在。在設定檔 /etc/fail2ban/jail.conf 內預設是 600 秒後自動解開。

```
# "bantime" is the number of seconds that a host is banned.
bantime  = 600
```

這服務很簡單就可以啟動，且針對目前存在的殭屍網路服務的阻擋非常的有效。至於其他的服務可以觀看 fail2ban 的官方網站，有更多的說明。

http://www.fail2ban.org/wiki/index.php/Main_Page