VM 접속 보안 강화 방법 – fail 2 ban 설치 및 설정

서비스 개요 >>>

fail2ban은 python(2.4 Ver 이상)으로 만들어진 특정 서비스로 로그인을 몇 회 이상 실패할 경우, logfiles을 읽어서 일정기간 동안 접속을 차단하는 툴로 ssh, ftp 등에 무작위로 로그인하는 brute force attack에 대응 하기 위한 모듈입니다.

iptables, tcpwrapper 등에 해당 host를 등록하여 특정 host의 접속을 차단하는 기능을 가지고 있으며, ssh, apache, ftp 등을 이용한 접속 방어에 사용됩니다.

과 정 >>>

1. rpm 으로 fail2ban이 설치되어 있는지 확인합니다.

```
[localhost]rpm -qa | grep fail2ban
fail2ban-0.8.4-23.el5
```

설치가 되어 있다면 위와 같은 메시지가 보입니다. 만일 설치되어 있지 않다면 yum install fail2ban' 명령을 통해 설치할 수 있습니다.

```
[localhost]yum install fail2ban
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * addons: mirror01.idc.hinet.net
 * base: ftp.osuosl.org
 * epel: mirror01.idc.hinet.net
 * extras: ftp.osuosl.org
 * updates: mirror01.idc.hinet.net
addons                                                  |  951 B     00:00
base                                                    | 2.1 kB     00:00
elff                                                    | 1.9 kB     00:00
epel                                                    | 3.7 kB     00:00
extras                                                  | 2.1 kB     00:00
updates                                                 | 1.9 kB     00:00
updates/primary_db                                      | 572 kB     00:00
Setting up Install Process
Package fail2ban-0.8.4-23.el5.noarch already installed and latest version
Nothing to do
```

yum 명령을 이용한 설치 방법 이외에도 rpm 명령을 이용한 설치방법을 2~3번에 설명하였습니다.

2. http://www.fail2ban.org 에서 centos 5.5, x86_64에 맞는 package를 download 받습니다. 아래는 해당 package download link입니다.
   http://download.fedora.redhat.com/pub/epel/5/x86_64/fail2ban-0.8.4-23.el5.noarch.rpm
   wget 명령을 통해 쉽게 다운로드 받을 수 있습니다.

```
[localhost]wget http://download.fedora.redhat.com/pub/epel/5/x86_64/fail2ban-0.8.4-23.el5.noarch.rpm
--2011-06-02 13:36:13--  http://download.fedora.redhat.com/pub/epel/5/x86_64/fail2ban-0.8.4-23.el5.noarch.rpm
Resolving download.fedora.redhat.com... 209.132.181.24, 209.132.181.23, 209.132.181.27, ...
Connecting to download.fedora.redhat.com|209.132.181.24|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 138132 (135K) [application/x-rpm]
Saving to: `fail2ban-0.8.4-23.el5.noarch.rpm'

100%[======================================================================>] 138,132      181K/s   in 0.7s

2011-06-02 13:36:14 (181 KB/s) - `fail2ban-0.8.4-23.el5.noarch.rpm' saved [138132/138132]
```

3. 다운받은 package 설치(rpm 명령으로 설치)

   rpm -Uvh fail2ban-0.8.4-23.el5.noarch.rpm

```
[localhost]rpm -Uvh fail2ban-0.8.4-23.el5.noarch.rpm
Preparing...                ########################################### [100%]
        package fail2ban-0.8.4-23.el5.noarch is already installed
```

4. usr/bin 에 fail2ban 명령어가 존재하는지 확인

```
[localhost]cd /usr/bin
[localhost]ls -la fail2*
-rwxr-xr-x 1 root root 11491 2009-09-16 02:17 fail2ban-client
-rwxr-xr-x 1 root root 10700 2009-09-16 02:17 fail2ban-regex
-rwxr-xr-x 1 root root  4220 2009-09-16 02:17 fail2ban-server
```

   /etc/fail2ban 에 fail2ban 설정파일이 위치하게 됩니다..

```
[localhost]cd /etc/fail2ban/
[localhost]ls -al
total 32
drwxr-xr-x  4 root root 4096 2011-05-31 20:11 .
drwxr-xr-x 80 root root 4096 2011-06-02 11:18 ..
drwxr-xr-x  2 root root 4096 2011-02-16 12:33 action.d
-rw-r--r--  1 root root  844 2009-09-16 02:17 fail2ban.conf
drwxr-xr-x  2 root root 4096 2011-02-16 12:33 filter.d
-rw-r--r--  1 root root 6480 2011-05-31 20:11 jail.conf
```

5. 설정파일인 jail.conf를 열어 [default] section에서 bantime(차단시간)과 maxretry(차단할 실패 횟수)를 적절하게 변경해주세요.

```
[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  = 600

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 600

# "maxretry" is the number of failures before a host get banned.
maxretry = 3
```

   각 항목 설명

   - Ignoreip : 여기에 지정된 주소는 fail2ban에 의해 차단되지 않습니다. 원격에서 VM 에 접속하는 고객님의 경우, 해당 PC나 노트북의 ip를 여기에 등록한다면 혹시라도

패스워드 입력 실패로 인해 고객님의 ip가 차단되는 경우를 예방할 수 있습니다.

- Bantime : 특정 호스트가 일정 횟수를 넘어서 패스워드 입력 실패가 될 때, 해당 호스트가 차단될 시간입니다.
- Maxretry : 특정 호스트가 차단 될 실패 횟수입니다.

6. 적용하려는 service section을 찾아서 enabled = true로 고쳐주면 해당 서비스만 적용됩니다. 기본으로 ssh 서비스만 적용이 되어 있습니다.
   [ssh-iptables] 의미는 ssh 접속의 경우, iptables을 이용해 특정 호스트를 차단한다는 뜻이며, ssh section 이외에도 여러 다른 서비스의 경우 다양한 필터링 툴(tcpwrapper, badbots, shorewall 등)을 사용하고 있습니다.

```
[ssh-iptables]

enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
           sendmail-whois[name=SSH, dest=root, sender=fail2ban@mail.com]
logpath  = /var/log/secure
maxretry = 5
```

Section 내의 설정 내용

- Enabled : 해당 서비스 사용여부
- Filter : 로그를 읽을 때 사용할 필터 → /etc/fail2ban/filter
- Action : iptable로 차단하고, 메일을 발송(/var/spool/mail/root 에서 확인)

➔ Dest mail 은 일반 메일 주소도 등록 가능합니다. 단 이 때에는 본인의 mail service가 동작하고 있어야 합니다.

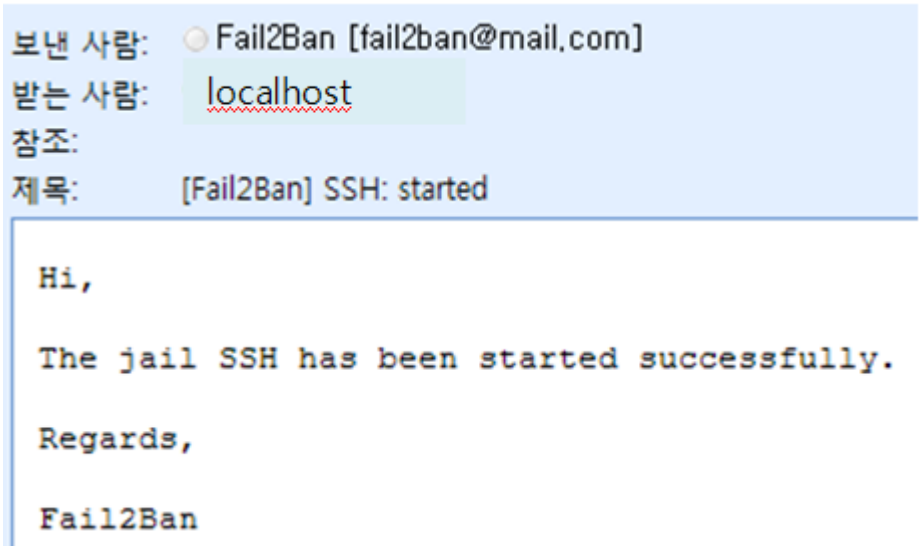
➔ ps –ef | grep sendmail 명령으로 mail process가 동작하는지 확인 할 수 있습니다.

```
[localhost]ps -ef | grep sendmail
root      9562     1  0 14:15 ?        00:00:00 sendmail: accepting connections
smmsp     9570     1  0 14:15 ?        00:00:00 sendmail: Queue runner@01:00:00
root      9913  7689  0 14:22 pts/0    00:00:00 grep sendmail
```

➔ 만약 mail process가 동작하지 않으면 service sendmail start 명령으로 해당 process를 실행 시킬 수 있습니다.

```
[localhost]service sendmail start
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

➔ 제 개인 메일을 입력했을 때, 아래와 같이 메일을 받을 수 있습니다.



- Logpath : 읽어서 처리할 로그파일 위치
- Maxretry : 차단할 실패 횟수
- Bantime : 차단시간
-

7. 서비스 시작.

```
[localhost]service fail2ban start
Starting fail2ban:                                         [  OK  ]
```

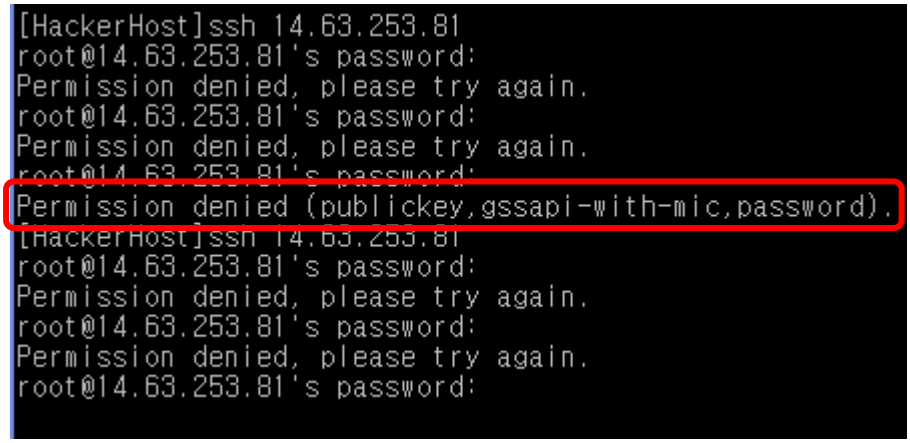
8. 부팅 시 자동 시작하도록 ntsysv 명령으로 등록하거나, chkconfig –levels 235 fail2ban on 명령실행

```
[localhost]chkconfig --levels 235 fail2ban on
```

적용 사례 >>>

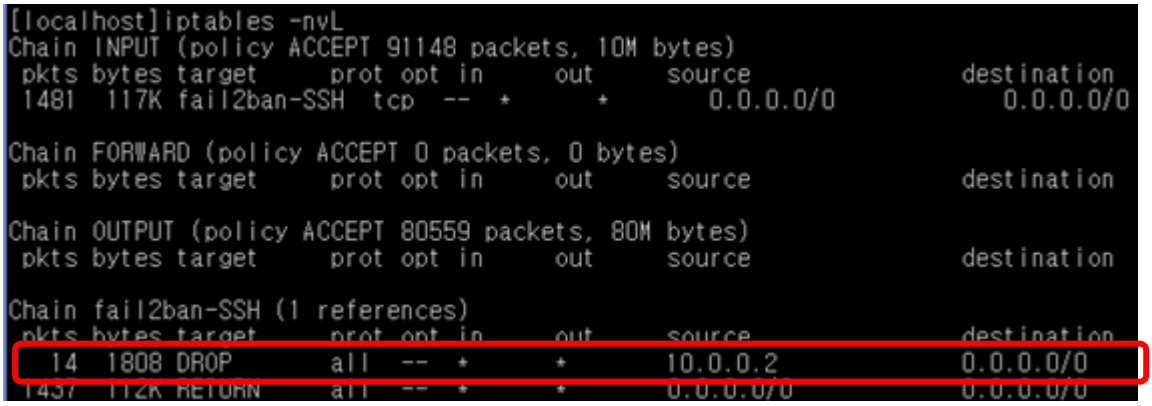
fail2ban이 작동하여 특정 host에서 일정 횟수 이상 VM에 접속 시도 시 iptables에서 해당 host를 일정 기간 차단하는 기능 시연

1. 특정 host에서 fail2ban이 설치된 VM에 접속 시도(password 인증 실패)



➔ jail.conf 내의 maxretry(차단할 실패 횟수)는 password 입력 실패 횟수와는 다릅니다. Fail2ban은 /var/log/secure 의 log에서 표시되는 패스워드 입력 실패 log의 횟수를 확인합니다. 위의 화면에서는 permission denied라고 표시되는 횟수(빨간색으로 표시)가 maxretry에 설정한 횟수와 동일하면 fail2ban은 해당 host의 ip를 iptables에 등록하여 차단합니다.

2. 일정 횟수 이상 접속시도 실패 시 VM에 설치한 fail2ban이 작동하여 해당 host의 ip를 iptables에 등록하여 차단합니다.

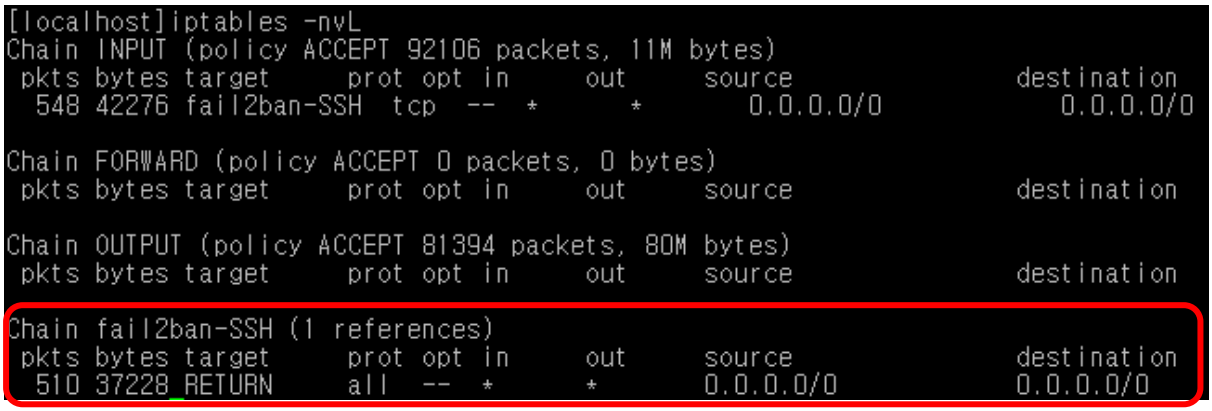


접속 실패(password인증 실패) host의 ip : 10.0.0.2

/var/log/message 에서 해당 host가 차단되는 모습을 볼 수 있습니다.

접속 실패(password인증 실패) host의 ip : 10.0.0.2

3. Jail.conf에서 설정한 bantime(차단시간)을 넘으면 해당 host의 ip는 iptables에서 자동으로 삭제됩니다.



Fail2ban chain에서 해당 host의 ip가 삭제되었음을 확인 할 수 있습니다.

/var/log/message 에서 해당 host가 unban 되었음을 확인할 수 있습니다.

접속 실패(password인증 실패) host의 ip : 10.0.0.2

참 조 : http://www.fail2ban.org/wiki/index.php/Manual