Fail2ban

Немного начали напрягать брутом популярных портов.

```
cd /usr/ports/security/py-fail2ban/
make install clean
```

В процессе установки у меня вывалилась ошибка, связанная с py27-setuptools, примерно такая

```
===>  Installing for py27-setuptools-32.1.0_1
===>  Checking if py27-setuptools already installed
===>   Registering installation for py27-setuptools-32.1.0_1 as automatic
Installing py27-setuptools-32.1.0_1...
pkg-static: py27-setuptools-32.1.0_1 conflicts with py27-setuptools27-32.1.0 (installs files into the same place). Problematic file: /usr/local/lib/python2.7/site-packages/easy-install.pth.dist
*** Error code 70
Stop.
make: stopped in /usr/ports/devel/py27-setuptools
```

Решение

```
pkg set -n py27-setuptools27:py27-setuptools
pkg set -o devel/py-setuptools27:devel/py27-setuptools
```

Далее

```
echo 'fail2ban_enable="YES"' >> /etc/rc.conf
```

Переходим

```
cd /usr/local/etc/fail2ban
cp jail.conf jail.local
```

– чтобы при обновлении не потерлись конфиги.

```
cat /jail.local
[DEFAULT]
ignoreip = 127.0.0.1 192.168.1.12
# время бана в секундах (отрицательное число - навсегда)
```

```
bantime = -600

# время проверки,за которое событие успеет повторится
findtime = 900

# максимальное число правонарушений
maxretry = 2

# метод парсинга логов
backend = auto
usedns= no

[ssh-ipfw]
enabled = true
filter = bsd-sshd
action = bsd-ipfw[table “” not found /]
sendmail[name=ssh, dest=svm@tst-amo.pp.ua]
logpath = /var/log/auth.log
```

В ipfw добавляем таблицы 3, 4, 5

```
#fail2ban table
 add 2 deny log all from table(3) to me
 add 2 deny log all from me to table(3)
```

и запускаем

```
/etc/rc.d/ipfw restart
service fail2ban restart
```

Делаем

```
tail -f /var/log/fail2ban.log
```

и пробуем ошибочно залогинится.

Защищаем Postfix

В /usr/local/etc/fail2ban/jail.local добавляем

```
[postfix-sasl-ipfw]
enabled = true
filter = postfix-sasl
action = bsd-ipfw[table “” not found /]
```

```
logpath = /var/log/maillog
bantime = 604800
findtime = 3600
maxretry = 3
ignoreip = 127.0.0.1 192.168.1.0/24
backend = auto

[postfix-ipfw]
enabled = true
filter = postfix
action = bsd-ipfw[table “” not found /]
logpath = /var/log/maillog
bantime = 604800
findtime = 3600
maxretry = 3
ignoreip = 127.0.0.1 192.168.1.0/24
backend = auto
```

В /usr/local/etc/fail2ban/filter.d/postfix-sasl.local правим до состояния

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = postfix(-\w+)?/(submission/)?smtp(d|s)
failregex = ^%(__prefix_line)swarning: [-._\w]+\[<HOST>\]: SASL ((?i)LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication failed(: [ A-Za-z0-9+/:]*={0,2})?\s*$
ignoreregex =
```

Защищаем Dovecot

```
[dovecot-ipfw]
enabled = true
filter = dovecot
action = bsd-ipfw
# mail-whois[name=Dovecot, dest=svm@tst-amo.pp.ua]
logpath = /var/log/dovecot.log
maxretry = 3
bantime = 3600
findtime = 600
ignoreip = 127.0.0.1 192.168.1.47
```

```
backend = auto
```

Защищаем Roundcube

В /usr/local/etc/fail2ban/jail.local добавляем

```
[roundcube-ipfw]
enabled = true
filter = roundcube-auth
action = bsd-ipfw[table “” not found /]
port = http,https
bantime = 240
findtime = 3600
maxretry = 3
logpath = /usr/local/www/roundcube/logs/errors
ignoreip = 127.0.0.1 192.168.1.0.24
backend = auto
```

Фильтр /usr/local/etc/fail2ban/filter.d/roundcube-auth.local подошел дефолтный.

Защищаем ProFTPd

```
[proftpd-ipfw]
enabled = true
filter = proftpd
action = bsd-ipfw[table “” not found /]
port = ftp,ftps,sftp
bantime = 240
findtime = 3600
maxretry = 3
logpath = /var/log/proftpd/proftpd.log
ignoreip = 127.0.0.1 192.168.1.47 194.44.219.161
backend = auto
```

Полезные команды:

Рестарт

```
# service fail2ban restart
```

Получить список правил:

```
# fail2ban-client status
```

Получить статистику заблокированных адресов:

```
# fail2ban-client status <имя правила>
```

Для удаление адреса из списка вводим:

```
fail2ban-client set <имя правила> unbanip <IP-адрес>
```

Например:

```
fail2ban-client set ssh unbanip 5.234.11.168
```

https://www.dmosk.ru/instruktions.php?object=fail2ban