Fail2ban - установка и настройка

Fail2ban - это простенькая система для защиты от атак связанных с подбором пароля. Например можно применить следующее правило: после трех неверных попыток авторизации IP атакующего банится (а именно блокируется средствами iptables) на 60 минут. Очевидно, что fail2ban не способен защитить от массовых распределенных атак, но тут уж применяются совершенно другие методы и средства.

Установка

Просто устанавливаем и все. Для Ubuntu 10.04 LTS можно добавить сторонний PPA для установки более новой версии (в стандартном репозитории 0.8.4, выпущенный аж в 2009 году) командой

```
# sudo apt-add-repository ppa:skurylo/fail2ban
# sudo apt-get update
<code>

и устанавливаем:

<code>
# sudo apt-get install fail2ban
```

Все настройки хранятся в /etc/fail2ban и весьма очевидны благодаря хорошо комментированным файлам конфигурации.

- fail2ban.conf - общие настройки (уровень логирования, куда пишем логи и т.д.)
- jail.conf - собственно сами правила защиты, так же все предельно понятно.
- в папке action.d хранятся файлы, осуществляющие взаимодействие с утилитами операционной системы - здесь и отдаются конкретные указания как реагировать на опасность.
- в папке filter.d хранится логика работы - критерии по которым и происходит срабатывание правил.

Пример: надоели боты, ищущие некоторые скрипты на нашем веб-сервере (например, ищущие уязвимые версии phpmyadmin). И сейчас мы их будем отстреливать.

- Создаем правила, по которым вредитель будет обнаруживаться:

Файл filter.d/apache-nobots.conf

```
# Fail2Ban configuration file
#
# Author: Evgeny Cheremnykh <rtzra@mail.ru>
#
# $Revision: 717 $
#
[Definition]
```

```
# Option:  failregex
# Notes.:  regex to match failures to find a home directory on a server,
which
#          became popular last days. Most often attacker just uses IP
instead of
#          domain name -- so expect to see them in generic error.log if you
have
#          per-domain log files.
# Values:  TEXT
#
failregex = [[]client <HOST>[]] File does not exist: .*/*/phpmyadmin*
            [[]client <HOST>[]] File does not exist: .*/*/phpmyadmin1*
            [[]client <HOST>[]] File does not exist: .*/*/phpmyadmin2*
            [[]client <HOST>[]] File does not exist: .*/*/phpMyAdmin*
            [[]client <HOST>[]] File does not exist: .*/*/php-My-Admin*
            [[]client <HOST>[]] File does not exist: .*/*/php-my-admin*
            [[]client <HOST>[]] File does not exist: .*/*/dbadmin*
            [[]client <HOST>[]] File does not exist: .*/*/myadmin*
            [[]client <HOST>[]] File does not exist: .*/*/mysqladmin*
            [[]client <HOST>[]] File does not exist: .*/*/mysql-admin*
            [[]client <HOST>[]] File does not exist: .*/*/webdav*
            [[]client <HOST>[]] File does not exist: .*/*/pma*
            [[]client <HOST>[]] File does not exist: .*/*/PMA*
# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
```

- Добавляем наше правило в список

Файл jail.conf

```
[apache-nobots]

enabled = true
port    = http,https
filter  = apache-nobots
logpath = /var/log/apache*/*error.log
maxretry = 2
```

fail2ban, защита