Для организации простенькой защиты от ботов, которые постоянно проверяют на прочность вашу wordpress админку, быстрее всего настроить fail2ban. Это многофункциональное и эффективное средство для защиты сервисов от постороннего доступа. Рассмотрим его применительно к wordpress.

Содержание:

Введение

В интернете постоянно пасутся стада ботов, проверяющие доступ к тем или иным сервисам. Чаще всего это боты очень простые, они просто подбирают по словарю доступ к ресурсам. Иногда они используют известные уязвимости. Так как wordpress самый популярный движок для сайта, пробовать его на прочность будут регулярно. Если у вас постоянно обновляется версия и уникальный пароль, которого нет в словарях, то вам скорее всего беспокоиться не о чем. Fail2ban какой-то уникальной защиты не предоставляет.

Лично я предпочитаю обезопасить себя на всякий случай и закрыть доступ к админке wordpress от слишком назойливых глаз. Будем анализировать лог web сервера и банить всех тех, кто более 3-х раз ввел неверный пароль на доступ к внутренностям сайта.

Я буду показывать настройку fail2ban на примере CentOS 7, но версия ОС тут не имеет принципиального значения. Все настройки самого сервиса подойдут и для других систем.

Установка fail2ban в CentOS 7

Первым делом установим fail2ban в систему с помощью yum. Тут ничего сложного, все как обычно.

```
# yum install fail2ban
```

Если у вас Debian/Ubuntu, воспользуйтесь командой apt-get install fail2ban.

Настройка fail2ban

Теперь необходимо отредактировать файл настроек, добавив туда информацию о нашем сайте wordpress. Открываем /etc/fail2ban/jail.conf и добавляем в самый конец:

```
# mcedit /etc/fail2ban/jail.conf

[wp-login]
enabled = true
port = http,https
action = iptables-multiport[name=WP, port="http,https", protocol=tcp]
# включаем отправку оповещения на почту, если вам это необходимо
         sendmail[name=wp-login, dest=zeroxzed@gmail.com, sender=fail2ban@serveradmin.ru]
filter = wp-login
logpath = /web/sites/serveradmin.ru/log/access.log
maxretry = 3
```

enabled	включаем секцию
port	порты, которые будут забанены

action	действие, которое будет выполняться, в данном случае включается блокировка iptables и отправляется оповещение, но может быть указано что-то одно
filter	название фильтра, по которому будет проходить проверка
logpath	путь до лог файла, которые будет анализироваться
maxretry	количество срабатываний фильтра, после которого хост будет забанен

Дальше нужно создать фильтр, который мы указали ранее. Создаем новый фильтр:

```
# mcedit /etc/fail2ban/filter.d/wp-login.conf

[Definition]
failregex = ^<HOST> .* "POST /wp-login.php
```

Сохраняем его и проверяем работу фильтра:

```
# fail2ban-regex /web/sites/serveradmin.ru/log/access.log /etc/fail2ban/filter.d/wp-login.conf
```

У меня получилось 240 срабатываний фильтра на этом лог файле. Если вы хотите увидеть строки, которые пометил фильтр, то можете запустить эту же команду с ключом:

```
--print-all-matched
```

Запускаем сервис и добавляем в автозагрузку:

```
# systemctl start fail2ban
# systemctl enable fail2ban
```

На этом все, защита админки wordpress с помощью fail2ban настроена.

Проверка работы

На всякий случай проверьте в */etc/fail2ban/fail2ban.conf* куда будут складываться логи сервиса. За них отвечает параметр:

```
logtarget = /var/log/fail2ban.log
```

Убедитесь, что у вас настроена ротация этого файла. В CentOS 7 для этого нужно проверить, что в папке /etc/logrotate.d есть файл fail2ban примерно следующего содержания:

```
/var/log/fail2ban.log {
 rotate 7
 missingok
 compress
 postrotate
 /usr/bin/fail2ban-client flushlogs 1>/dev/null || true
 endscript
}
```

Во время работы автобана в лог файле будут появляться примерно такие строки:

```
2015-12-15 16:57:27,878 fail2ban.filter [12814]: INFO [wp-login] Found 188.138.220.43
2015-12-15 17:00:29,738 fail2ban.filter [12814]: INFO [wp-login] Found 188.138.220.43
2015-12-15 17:03:03,292 fail2ban.filter [12814]: INFO [wp-login] Found 185.93.187.31
2015-12-15 17:03:29,419 fail2ban.filter [12814]: INFO [wp-login] Found 188.138.220.43
2015-12-15 17:03:30,184 fail2ban.actions [12814]: NOTICE [wp-login] Ban 188.138.220.43
2015-12-15 17:13:31,082 fail2ban.actions [12814]: NOTICE [wp-login] Unban 188.138.220.43
```

Проверить, забанены ли реально эти адреса можно посмотрев текущие правила iptables:

```
# iptables -L -v -n
```

Либо можно проверить статус командой:

```
# fail2ban-client status wp-login
```

Если вам нужно будет вручную кого-нибудь забанить, то можно воспользоваться командой:

```
# fail2ban-client set [name-of-jail] banip [ip-address]
```

Это в общем случае, в нашем случае команда будет выглядеть вот так:

```
# fail2ban-client set wp-login banip 188.138.220.43
```

Чтобы разбанить какой-нибудь адрес, поступаем следующим образом:

```
# fail2ban-client set wp-login unbanip 188.138.220.43
```

Заключение

Такая нехитрая и эффективная в некоторых случаях защита у нас получилась. Я в течении дня собираю около тысячи попыток залогиниться через wp-admin. Не все боты долбятся 3 раза подряд и попадают в бан. Я бы даже сказал, большая часть этого не делает. Но они и не представляют опасности. Подобная этой настройка защитит в первую очередь от массового нашествия, которое способно серьезно замедлить работу сайта и хостинга в целом. Закрытие доступа на уровне iptables очень эффективный способ сохранить ресурсы сервера.

Помогла статья? Есть возможность отблагодарить автора

Рекомендую полезные материалы по схожей тематике:

- Важность своевременного обновления сервера — взлом centos сервера через уязвимость bash.
- Эпидемия вируса шифровальщика vault — как защитить свои данные.
- Базовая настройка centos для обеспечения минимальной защиты сервера.
- Создание резервной копии сайта и ее хранение на Яндекс.Диске.