

Fail2ban

Fail2ban - сканирует лог-файлы и блокирует IP-адреса, которые ведут себя подозрительно, к примеру, делая слишком много попыток входа с неверным паролем в попытках найти уязвимость. Данная атака часто называется брутфорсом.

Модуль «Fail2ban» расположен в Меню «Защита», и имеет четыре вкладки: «Fail2ban», «Настройки», «Заблокированные ip-адреса», и «Журнал».


Общие сведения

Fail2ban

Настройки

Заблокированные ip-адреса

Журнал

 Fail2ban

Блокирует IP-адреса, с которых предпринимается слишком много попыток авторизации

запущен

Выключить

Журнал

↓↑↺

INFO Jail 'gui-pf' uses pyinotify {}
14:11:34

INFO Initiated 'pyinotify' backend
14:11:34

INFO maxRetry: 3
14:11:34

INFO findtime: 600
14:11:34

INFO banTime: 600
14:11:34

INFO encoding: utf-8
14:11:34

INFO Added logfile: '/var/log/messages' (pos = 0, hash = e7657f44774ec5c7d55e1ad3c0bea933cb4279e4)
14:11:34

INFO Jail 'asterisk-pf' started
14:11:34

INFO Jail 'ssh-pf' started
14:11:34

INFO Jail 'gui-pf' started
14:11:34

На данной вкладке отображается состояние модуля (включен/выключен/не настроен), кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале модуля.

Настройки

Fail2ban	Настройки	Заблокированные ip-адреса	Журнал
<input type="checkbox"/> Защитить почтовый сервер <input checked="" type="checkbox"/> SSH	<input type="checkbox"/> Защитить веб-почту <input type="checkbox"/> FTP	<input checked="" type="checkbox"/> Защитить сервер телефонии <input checked="" type="checkbox"/> GUI	<input type="checkbox"/> Защитить VPN-сервер
Количество неудачных попыток авторизаций * <input type="text" value="3"/>	Интервал неудачных попыток авторизаций * <input type="text" value="10"/> мин.	Блокировать на * <input type="text" value="10"/> мин.	
<input type="checkbox"/> Увеличивать время бана			
Количество обычных банов перед увеличением времени бана * <input type="text" value="3"/>	Интервал обычных банов * <input type="text" value="10"/> мин.	Добавить к обычному времени блокировки * <input type="text" value="10"/> мин.	
<div>Белый список</div>			
<div>Сохранить</div> <div>Обновить</div>			

Данная вкладка предназначена для настройки работы модуля «Fail2ban».

Флаги: **«Защитить почтовый сервер»**, **«Защитить веб-почту»**, **«Защитить сервер телефонии»**, **«Защитить VPN-сервер»**, **«SSH»**, **«FTP»**, **«GUI»** - позволяют fail2ban анализировать логи авторизации в соответствующих модулях.

Поле **«Количество неудачных попыток авторизаций»** - позволяет задать количество неудачных попыток авторизации в одном из модулей, отмеченных флагом, после чего ip-адресу будет заблокирован доступ к «ИКС» полностью.

Поле **«Интервал неудачных попыток авторизаций»** - время, в течении которого подсчитывается количество неудачных попыток авторизации, в каждом модуле.

Поле **«Блокировать на»** - При срабатывании блокировки, доступ с ip-адреса, будет прекращен на заданное количество минут.

Флаг **«Увеличивать время бана»** - позволяет включить дополнительные настройки fail2ban (**«Количество обычных банов перед увеличением времени бана»**, **«Интервал обычных банов»**, **«Добавить к обычному времени блокировки»**) для инкрементации времени бана. Так при срабатывании бана **n**-раз (указанных в поле «Количество обычных банов перед увеличением времени бана») в течении времени **t** (указанного в «Интервал обычных банов») доступ к «ИКС» ip-адресу будет заблокирован. На **n+1** бане доступ будет заблокирован на время = **t** + значение из поля «Блокировать на».

ВАЖНО

- Стоит отметить, что значение указанное в поле «Интервал обычных банов» должно быть больше, чем произведение значений полей «Блокировать на» и «Количество обычных банов перед увеличением времени бана».

- Если авторизация на FTP идет через браузер, то количество попыток авторизации, указанное в поле «Количество неудачных попыток авторизаций», будет в два раза меньше. Так как браузер пытается первоначально авторизоваться под учетной записью Anonymous.

Белый список

Добавить

Удалить

Удалить все

1 запись

192.168.1.1

SSH

Сохранить

Отмена

Кнопка «Белый список». При нажатии будет открыто новое диалоговое окно, в котором возможно задать соответствие IP-адреса/подсети/диапазона (192.168.1.1 или 192.168.1.1/28 или 192.168.1.1-192.168.1.3) и сервиса/всех сервисов, для которых fail2ban не будет срабатывать.

Стоит отметить, что если fail2ban заблокирует IP-адрес по одному из сервисов, то доступ с IP-адреса к другим сервисам, также будет заблокирован, в том числе добавленным в белый список.

Заблокированные ip-адреса

Fail2ban

Настройки

Заблокированные ip-адреса

Журнал

Добавить в перманентный бан

Разблокировать

Добавить в белый список

Белый список

Поиск...

SSH ^

192.168.1.1

Ip-адрес

Добавить в перманентный бан

Разблокировать

Добавить в белый список

На данной вкладке отображаются текущие блокировки IP-адресов, распределенные по блокам (модулям), где произошла блокировка. При необходимости, Пользователь с ролью Администратор, может добавить IP-адрес в перманентный бан (т.е. навсегда и по всем сервисам), в белый список (произойдет разблокировка IP-адреса и он не будет проверяться Fail2ban по сервису добавленному в белый список) или разблокировать IP-адрес до истечения бана.

При добавлении в перманентный бан, возможно добавить: IP (например, 192.168.1.1), сеть (например, 192.168.1.1/30), диапазон IP (например, 192.168.1.1-192.168.1.4).

Журнал

Fail2ban Настройки Заблокированные ip-адреса **Журнал**

17.03.2020 - 17.03.2020 Сегодня Неделя Месяц Другой период ▾ ↺

Экспорт Удалить логи Поиск...

INFO -----
14:11:33
INFO Starting Fail2ban v0.11.1
14:11:33
INFO Daemon started
14:11:33
INFO Observer start...
14:11:33
INFO -----
14:11:33
INFO Starting Fail2ban v0.11.1
14:11:33
INFO Daemon started
14:11:33
INFO Observer start...
14:11:33
ERROR Fail2ban seems to be already running
14:11:33
WARNING Forcing execution of the server

« < Стр 1 из 1 > »

Показаны записи 1 - 82 из 82

Отображает сводку всех системных сообщений модуля «Fail2ban» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения - желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска, а также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

From:

<https://doc-old.a-real.ru/> - Документация

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:fail2ban&rev=1584709884>

Last update: **2020/03/20 16:11**

