

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

The screenshot shows the Fail2ban web interface. At the top, there are four tabs: "Fail2ban", "Настройки", "Заблокированные ip-адреса", and "Журнал". The "Fail2ban" tab is active. Below the tabs, there is a status bar for the Fail2ban module. It features a red "no" icon, the text "Fail2ban" and "Блокирует IP-адреса, с которых предпринимается слишком много попыток авторизации", and a green "запущен" (running) status. A "Выключить" (Turn off) button is visible on the right. Below this is a "Журнал" (Log) section with a scrollable list of log entries. The log entries include: "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", and "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 type="checkbox"/> Защитить веб-почту	<input checked="" type="checkbox"/> Защитить сервер телефонии	<input type="checkbox"/> Защитить VPN-сервер
<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> FTP	<input checked="" type="checkbox"/> GUI	
Количество неудачных попыток авторизаций *	Интервал неудачных попыток авторизаций *	Блокировать на *	
<input type="text" value="3"/>	<input type="text" value="10"/> мин.	<input type="text" value="10"/> мин.	
<input type="checkbox"/> Увеличивать время бана	Количество обычных банов перед увеличением времени бана *	Интервал обычных банов *	Добавить к обычному времени блокировки *
	<input type="text" value="3"/>	<input type="text" value="10"/> мин.	<input type="text" value="10"/> мин.
<input type="button" value="Белый список"/>			
<input type="button" value="Сохранить"/> <input type="button" value="Обновить"/>			

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 модуле, отмеченном флагом, после чего ip-адресу будет заблокирован доступ к «ИКС»

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

Поле «**Блокировать на**» - При срабатывании блокировки, доступ с ip-адреса будет прекращен на заданной 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 способствования увеличения 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 на время = t + «Блокировать на». *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».

Кнопка «Белый список». При нажатии будет открыто новое диалоговое окно, в котором возможно задать соответствие ip-адреса и сервиса/всех сервисов, для которых fail2ban не

будет срабатывать.

Заблокированные ip-адреса

Муми-дол > DLP Туве Янссон 30

- DLP
- Настройки
- База DLP
- События
- Журнал

DLP

Обеспечивает защиту от утечек информации

запущен

Выключить

Журнал ↓↑ ↻

locale loaded
11:24:57

config loaded
11:24:58

Журнал

- Fail2ban
- Настройки
- Заблокированные ip-адреса
- Журнал**

17.03.2020 - 17.03.2020 Сегодня Неделя Месяц Другой период ▾ ↻

Экспорт

Удалить логи

↓↑

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=1584450890>

Last update: **2020/03/17 16:14**

