Лабораторная работа №16

Базовая защита от атак типа «brute force»

Спелов Андрей Николаевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данной работы является получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

2 Выполнение лабораторной работы

На сервере установим fail2ban (рис. 2.1):

```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# dnf -y install fail2ban
Extra Packages for Enterprise Linux 10 - x86_64                  94 kB/s |  32 kB     00:00
Extra Packages for Enterprise Linux 10 - x86_64                 2.4 MB/s | 5.6 MB     00:02
Rocky Linux 10 - BaseOS                                          14 kB/s | 4.3 kB     00:00
Rocky Linux 10 - BaseOS                                         3.9 MB/s | 5.3 MB     00:01
Rocky Linux 10 - AppStream                                       15 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                                      3.4 MB/s | 2.0 MB     00:00
Rocky Linux 10 - CRB                                             11 kB/s | 4.3 kB     00:00
Rocky Linux 10 - CRB                                            1.1 MB/s | 486 kB     00:00
Rocky Linux 10 - Extras                                          10 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                                         6.6 kB/s | 4.8 kB     00:00
Dependencies resolved.
================================================================================================================================
 Package                       Architecture        Version                                    Repository                Size
================================================================================================================================
Installing:
 fail2ban                      noarch              1.1.0-6.el10_0                             epel                     9.4 k
Installing dependencies:
 exim                          x86_64              4.98.2-2.el10_1                            epel                     1.5 M
 fail2ban-firewalld            noarch              1.1.0-6.el10_0                             epel                     9.6 k
 fail2ban-selinux              noarch              1.1.0-6.el10_0                             epel                      31 k
 fail2ban-sendmail             noarch              1.1.0-6.el10_0                             epel                      12 k
 fail2ban-server               noarch              1.1.0-6.el10_0                             epel                     561 k
 libdb                         x86_64              5.3.28-64.el10_0                           epel                     763 k
 libgsasl                      x86_64              1.10.0-12.el10_1                           epel                     154 k
 libidn                        x86_64              1.42-4.el10_0                              epel                     198 k
 libnsl2                       x86_64              2.0.1-1.el10_0                             epel                      30 k
 libntlm                       x86_64              1.8-1.el10_0                               epel                      32 k
 libopendmarc                  x86_64              1.4.2-33.el10_1                            epel                      31 k
 libspf2                       x86_64              1.2.11-16.20210922git4915c308.el10_0       epel                      68 k
Installing weak dependencies:
 publicsuffix-list             noarch              20240107-5.el10                            appstream                 87 k
```

Рис. 2.1: Установка на сервере fail2ban.

Запустим сервер fail2ban (рис. 2.2):

```
[root@server.anspelov.net ~]# systemctl start fail2ban
[root@server.anspelov.net ~]# systemctl enable fail2ban
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.anspelov.net ~]#
```

Рис. 2.2: Запуск сервера fail2ban.

В дополнительном терминале запустим просмотр журнала событий fail2ban (рис. 2.3):

Рис. 2.3: Запуск просмотра в дополнительном терминале журнала событий fail2ban.

Создадим файл с локальной конфигурацией fail2ban (рис. 2.4):

Рис. 2.4: Создание файла с локальной конфигурацией fail2ban.

В файле /etc/fail2ban/jail.d/customisation.local зададим время блокирования на 1 час и включим защиту SSH (рис. 2.5):

Рис. 2.5: Настройка в файле /etc/fail2ban/jail.d/customisation.local времени блокирования на 1 час и включение защиты SSH.

Перезапустим fail2ban (рис. 2.6):

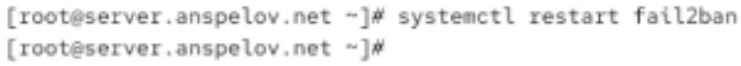

Рис. 2.6: Перезапуск fail2ban.

Посмотрим журнал событий (рис. 2.7):

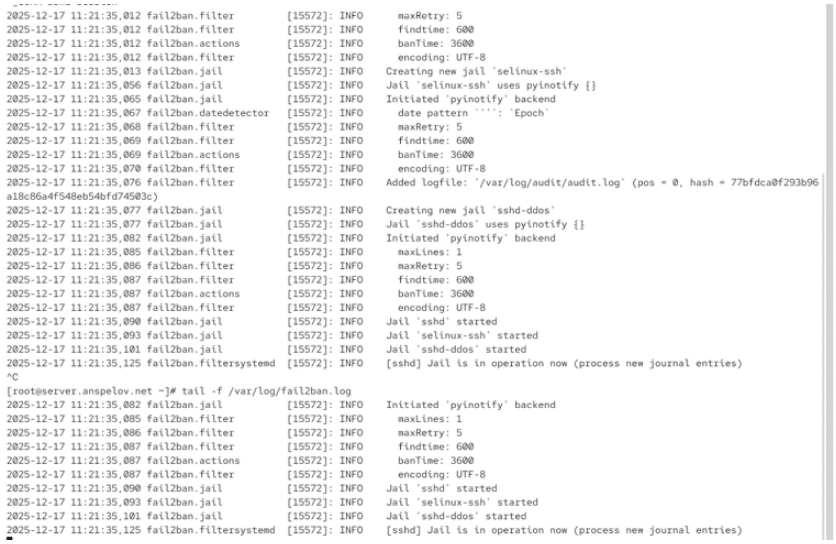

Рис. 2.7: Просмотр журнала событий.

В файле /etc/fail2ban/jail.d/customisation.local включим защиту HTTP (рис. 2.8):

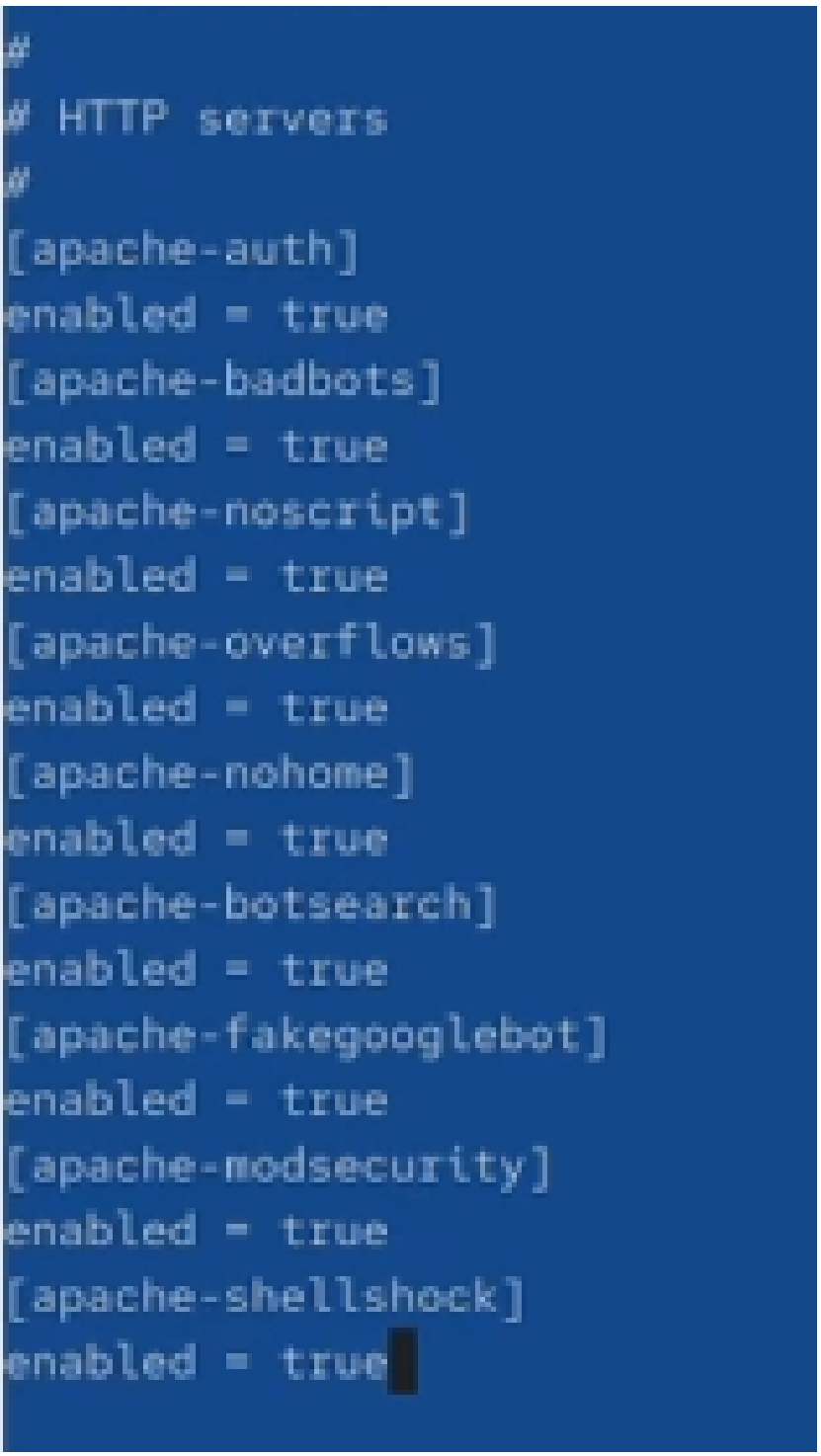

Рис. 2.8: Включение защиты HTTP в файле /etc/fail2ban/jail.d/customisation.local.

Перезапустим fail2ban (рис. 2.9):

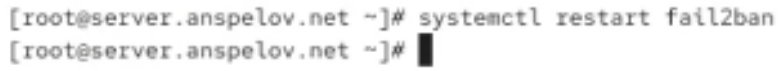

Рис. 2.9: Перезапуск fail2ban.

После чего посмотрим журнал событий (рис. 2.10):

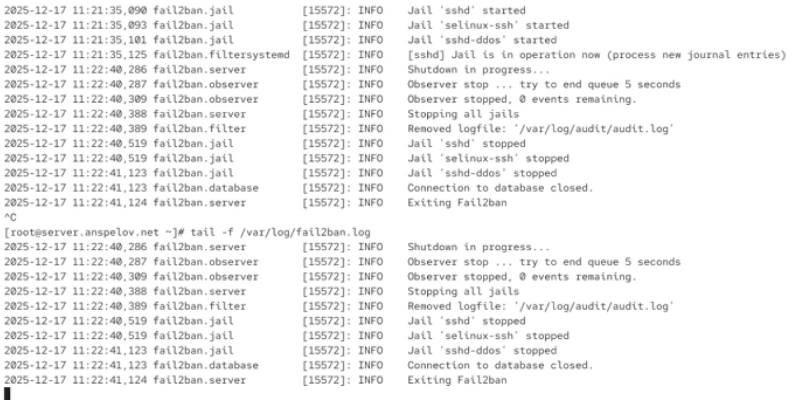

Рис. 2.10: Просмотр журнала событий.

В файле /etc/fail2ban/jail.d/customisation.local включим защиту почты (рис. 2.11):

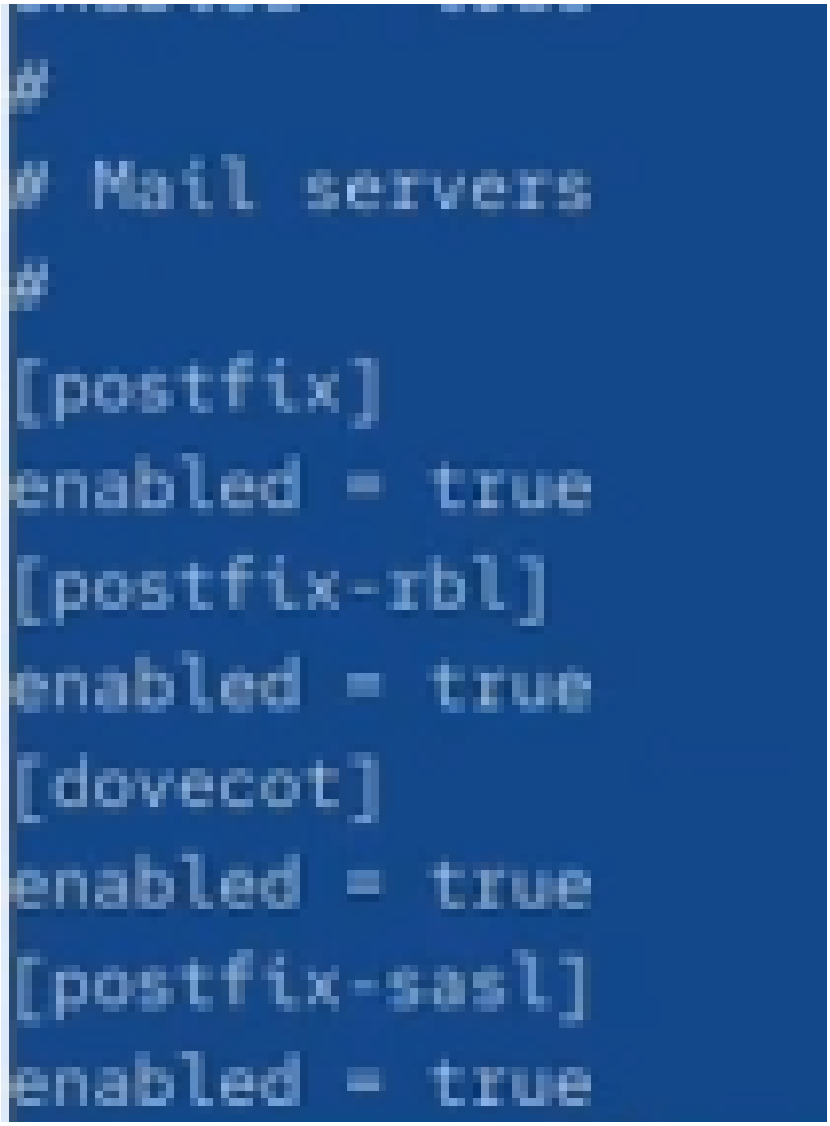

Рис. 2.11: Включение защиты почты в файле /etc/fail2ban/jail.d/customisation.local.

Снова перезапустим fail2ban (рис. 2.12):

```
[root@server.anspelov.net ~]# systemctl restart fail2ban
[root@server.anspelov.net ~]#
```

Рис. 2.12: Повторный перезапуск fail2ban.

И посмотрим журнал событий (рис. 2.13):

Рис. 2.13: Просмотр журнала событий.

На сервере посмотрим статус fail2ban, статус защиты SSH в fail2ban и установим максимальное количество ошибок для SSH, равное 2 (рис. 2.14):

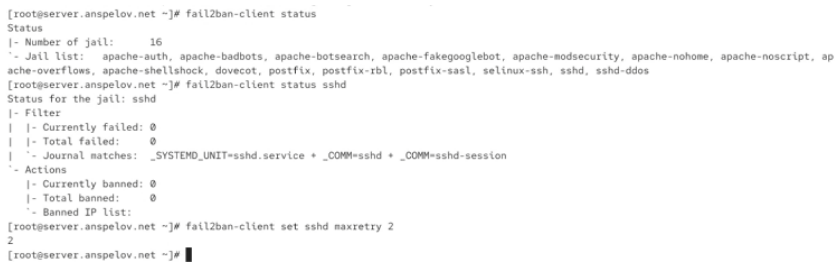

Рис. 2.14: Просмотр на сервере статуса fail2ban, статуса защиты SSH в fail2ban и установка максимального количества ошибок для SSH (=2).

С клиента попытаемся зайти по SSH на сервер с неправильным паролем (рис. 2.15):

Рис. 2.15: Попытка зайти с клиента по SSH на сервер с неправильным паролем.

На сервере посмотрим статус защиты SSH и разблокируем IP-адрес клиента. После чего вновь посмотрим статус защиты SSH и убедимся, что блокировка клиента снята (рис. 2.16):

```
[root@server.anspelov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     1
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.anspelov.net ~]# fail2ban-client set sshd unbanip 127.0.1.1
0
[root@server.anspelov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     2
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.2
[root@server.anspelov.net ~]#
```

Рис. 2.16: Просмотр на сервере статуса защиты SSH, разблокировка IP-адреса клиента и повторная проверка.

На сервере внесём изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.lo добавив в раздел по умолчанию игнорирование адреса клиента (рис. 2.17):

```
customisation.local   [-M--] 32 L:[  1+ 3   4/ 47] *(58  / 633b) 0010 0x00A
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 127.0.1.1
#
```

Рис. 2.17: Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле /etc/fail2ban/jail.d/customisation.local.

Перезапустим fail2ban (рис. 2.18):

```
[root@server.anspelov.net ~]# systemctl restart fail2ban
[root@server.anspelov.net ~]#
```

Рис. 2.18: Перезапуск fail2ban.

Далее посмотрим журнал событий (рис. 2.19):

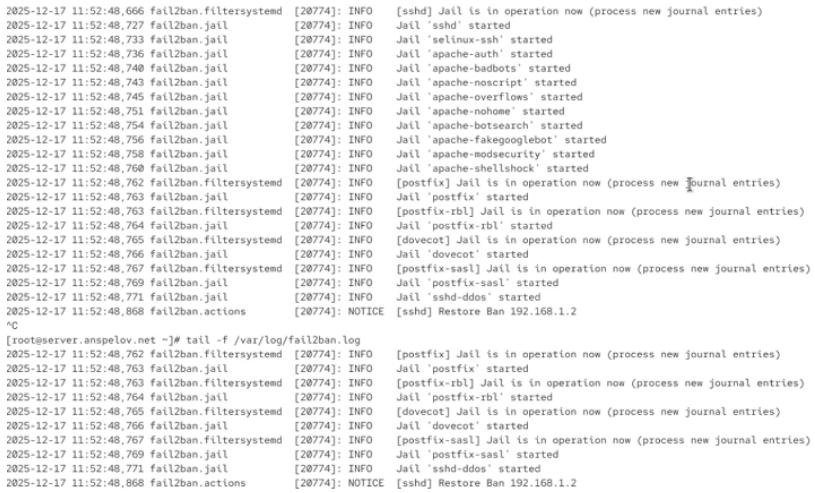

Рис. 2.19: Просмотр журнала событий.

Вновь попытаемся войти с клиента на сервер с неправильным паролем (рис. 2.20) и посмотрим статус защиты SSH (рис. 2.21):

Рис. 2.20: Попытка войти с клиента на сервер с неправильным паролем.

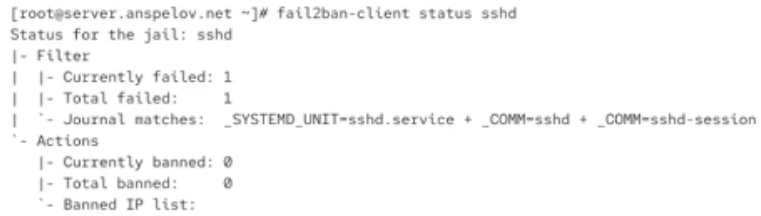

Рис. 2.21: Просмотр статуса защиты SSH.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог protect, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге /vagrant/provision/server создадим исполняемый файл protect.sh (рис. 2.22):

Рис. 2.22: Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога protect, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла protect.sh.

Открыв его на редактирование, пропишем в нём скрипт (рис. 2.23):

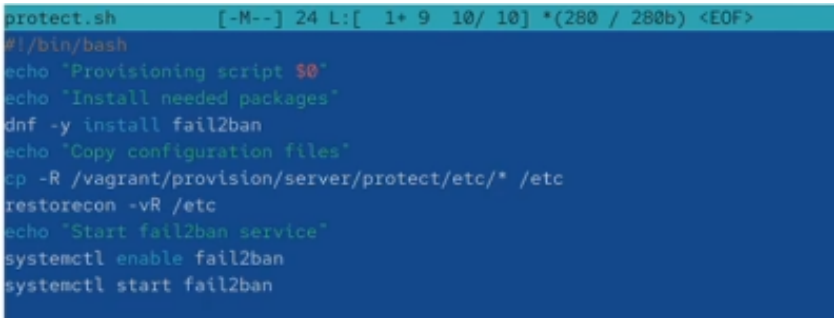

Рис. 2.23: Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в соответствующем разделе конфигураций для сервера (рис. 2.24):

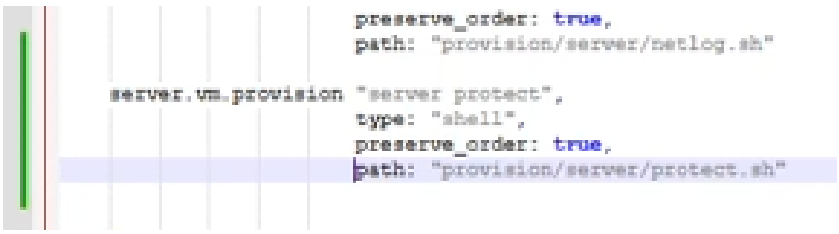

Рис. 2.24: Добавление конфигураций в конфигурационном файле Vagrantfile для сервера

3 Выводы

В ходе выполнения лабораторной работы были получены навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

4 Ответы на контрольные вопросы:

1. Поясните принцип работы Fail2ban. - Fail2ban является инструментом для защиты от атак на серверы, основанных на анализе журналов. Он мониторит журналы системы на предмет неудачных попыток входа или других событий, а затем блокирует IP-адреса атакующих с использованием системных средств, таких как iptables. Принцип работы: Мониторинг журналов на предмет определенных событий. Обнаружение повторных неудачных попыток входа или других нарушений. Динамическое обновление правил брандмауэра для блокировки атакующих IP-адресов.

2. Настройки какого файла более приоритетны: jail.conf или jail.local? - Настройки файла jail.local имеют более высокий приоритет и перекрывают настройки из jail.conf. Таким образом, если есть конфликтующие настройки, они будут использоваться из jail.local.

3. Как настроить оповещение администратора при срабатывании Fail2ban? - В файле jail.local нужно указать параметр destemail и задать адрес электронной почты, а также параметр action с указанием определенного действия (например, action_mw для отправки почты).

4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе. – Пример настроек для веб-службы в файле jail.conf: [apache] enabled = true port = http,https filter = apache-auth logpath = /var/log/apache/error.log

5. Поясните построчно настройки по умолчанию в конфигурационном

файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе. – Пример настроек для почтовой службы в файле jail.conf: [postfix] enabled = true filter = postfix action = iptables-multiport[name=postfix, port="submission,smtps", protocol=tcp]

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban? - Fail2ban может выполнять различные действия, такие как блокировка IP-адреса с использованием брандмауэра, отправка уведомлений, добавление в черные списки и т.д. Описание действий можно найти в конфигурационных файлах в разделе action.

7. Как получить список действующих правил Fail2ban? - Используйте команду: fail2ban-client status.

8. Как получить статистику заблокированных Fail2ban адресов? - Используйте команду: fail2ban-client status .

9. Как разблокировать IP-адрес? - Используйте команду: fail2ban-client set unbanip .

Список литературы