**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

ОТЧЕТ

по лабораторной работе № 16

Дисциплина «Администрирование сетевых подсистем»

*Тема «Базовая защита от атак типа “brute force”»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы

Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

# Задание

1. Установить и настроить Fail2ban для отслеживания работы установленных на сервере служб.
2. Проверить работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
3. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban.

**Выполнение**

**1. Защита с помощью Fail2ban**

1. На сервере установила fail2ban (рис.1.1).

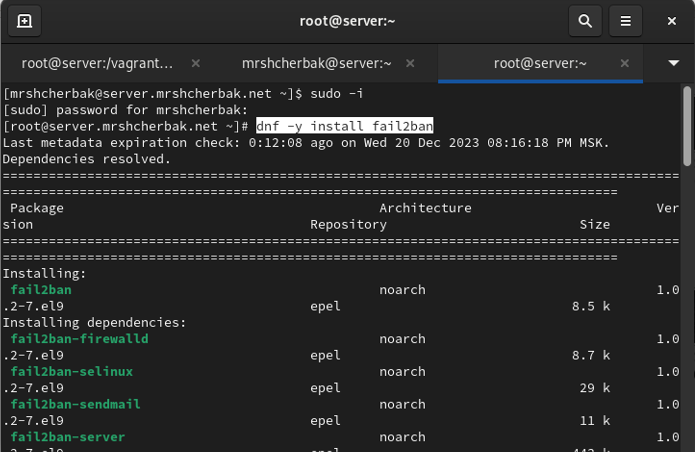


Рис.1.1. Установка fail2ban

2. Запустила сервер fail2ban и в дополнительном терминале запустила просмотр журнала событий fail2ban. Создала файл с локальной конфигурацией fail2ban и в нем задала время блокирования на 1 час (время задаётся в секундах) и включила защиту SSH.После чего перезапустила fail2ban с помощью команды systemctl restart fail2ban и просмотрела журнал событий. Действия представлены на рис.1.2 – рис.1.4.

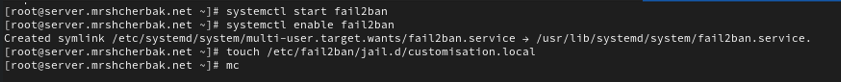


Рис.1.2. Выполнение команд

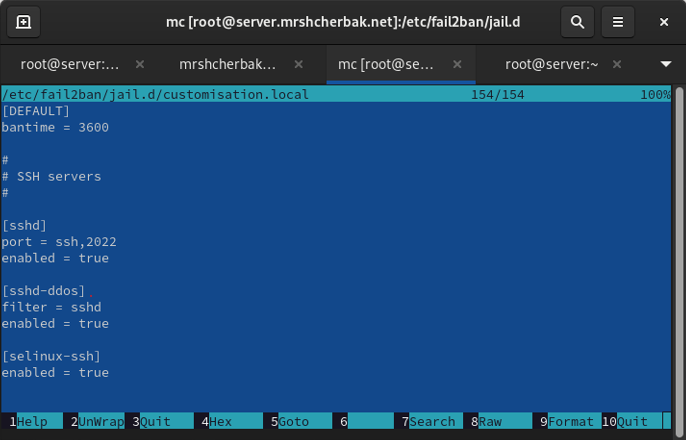


Рис.1.3. Содержимое файла с локальной конфигурацией fail2ban

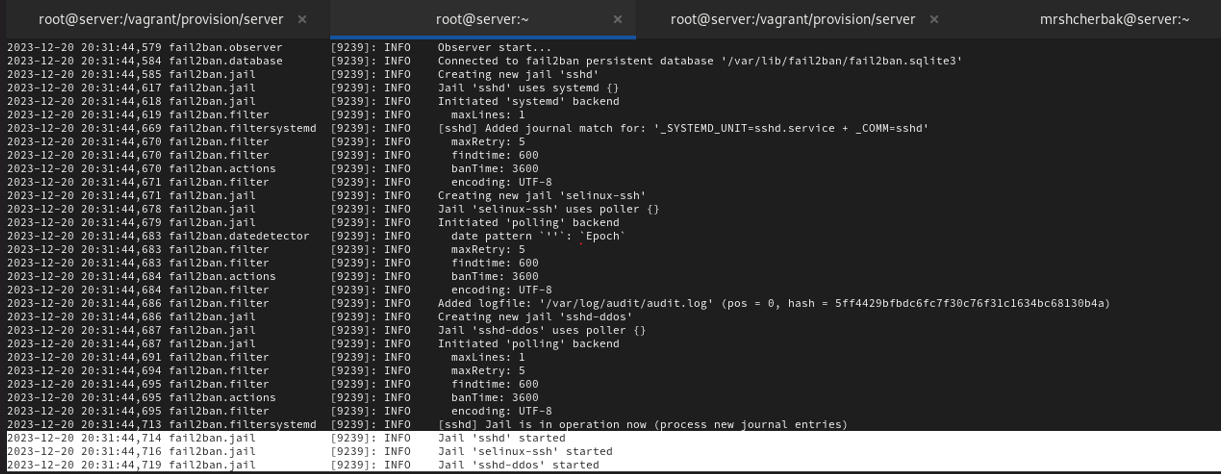


Рис.1.4. Просмотр журнала событий

3. В файле /etc/fail2ban/jail.d/customisation.local включила защиту HTTP (рис.1.5).

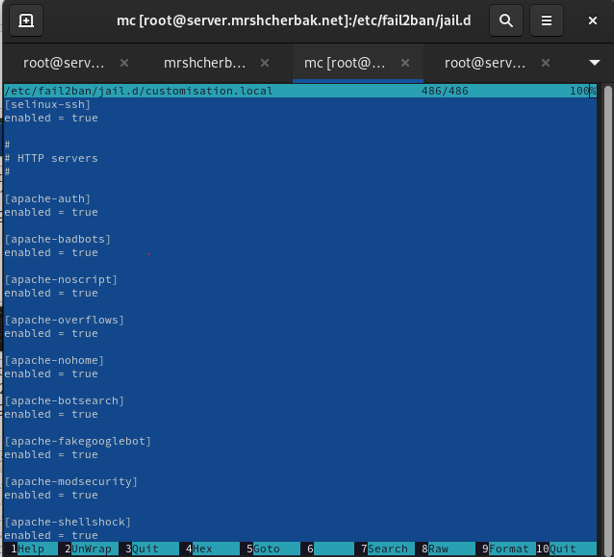


Рис.1.5. Содержимое файла с локальной конфигурацией fail2ban

4. Перезапустила fail2ban и посмотрела журнал событий (рис.1.6).

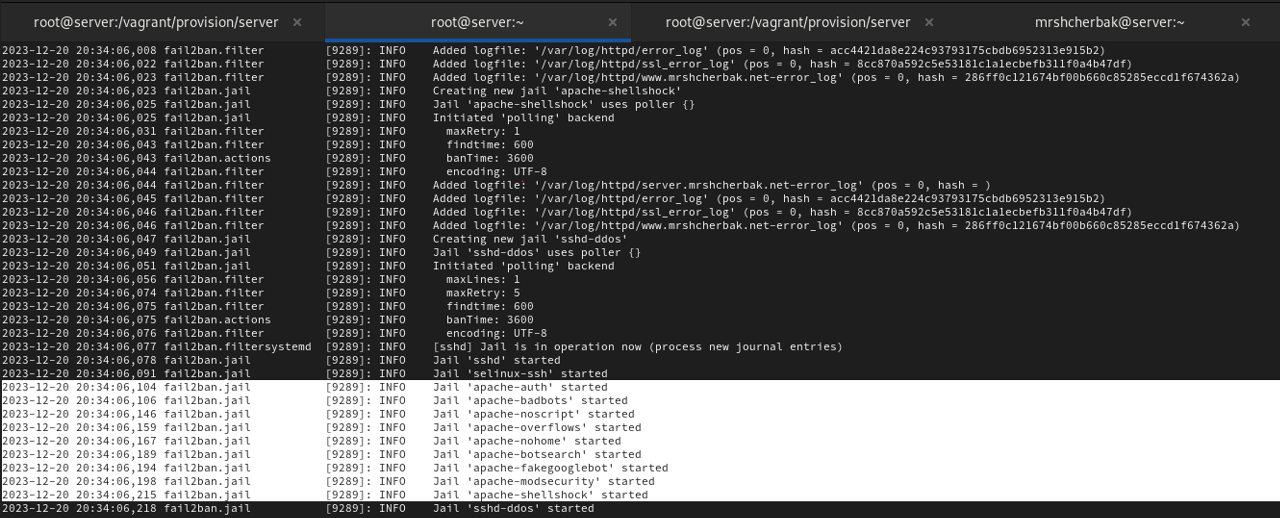


Рис.1.6. Просмотр журнала событий

5. В файле /etc/fail2ban/jail.d/customisation.local включила защиту почты (рис.1.7).

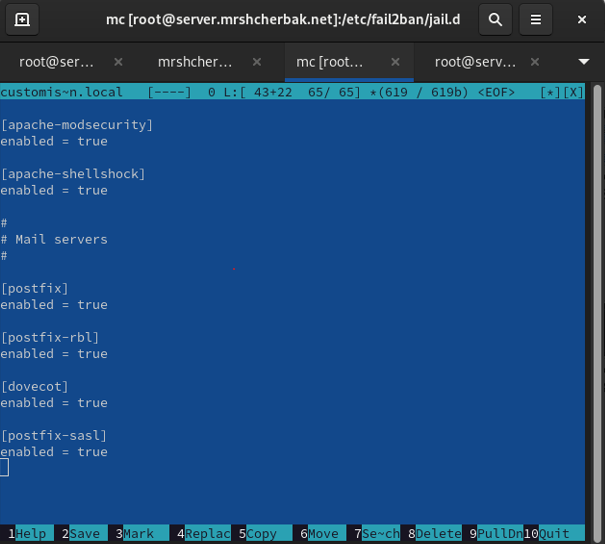


Рис.1.7. Содержимое файла с локальной конфигурацией fail2ban

6. Перезапустила fail2ban и посмотрела журнал событий (рис.1.8).

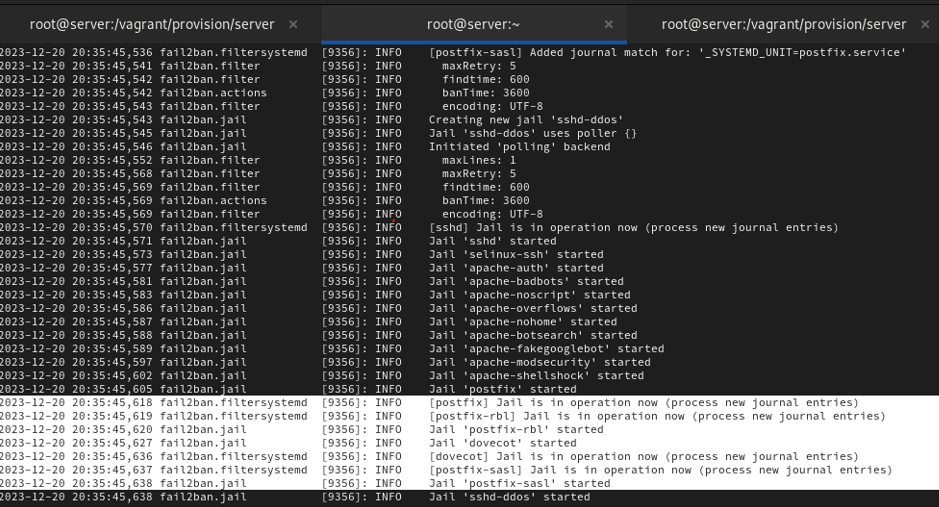


Рис.1.8. Просмотр журнала событий

**2. Проверка работы Fail2ban**

1. На сервере посмотрела статус fail2ban и статус защиты SSH в fail2ban, также установила максимальное количество ошибок для SSH, равное 2. Действия представлены на рис.2.1.

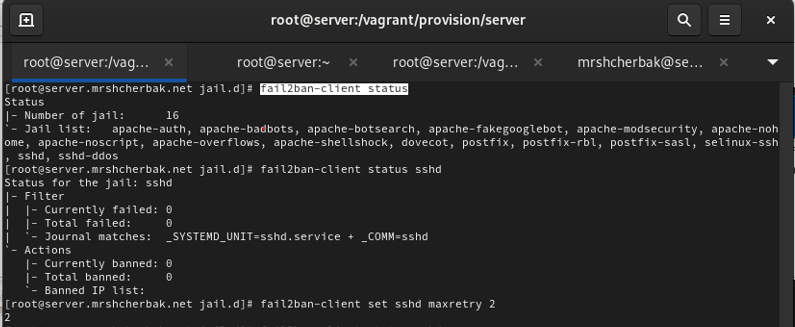


Рис.2.1. Выполнение команд

2. С клиента попыталась зайти по SSH на сервер с неправильным паролем (рис.2.2).

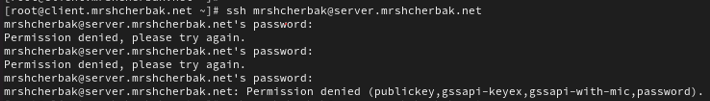


Рис.2.2. Попытка входа с клиента по SSH на сервер с неправильным паролем

3. На сервере посмотрела статус защиты SSH и убедилась, что произошла блокировка адреса клиента (рис.2.3 – рис.2.4).

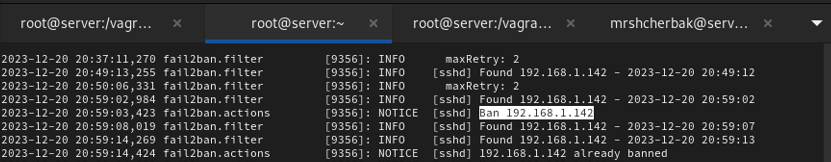


Рис.2.3. Просмотр журнала событий

Разблокировала IP-адрес клиента и вновь посмотрела статус защиты SSH (рис.2.4). Убедилась, что блокировка клиента снята.

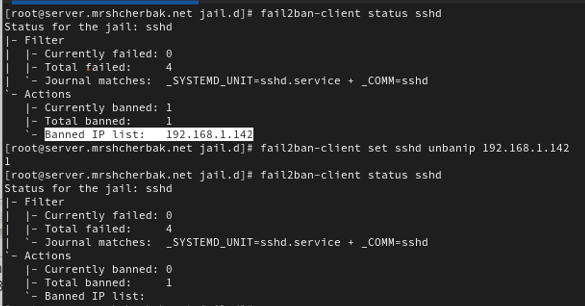


Рис.2.4. Просмотр статуса защиты SSH

4. На сервере внесла изменение в файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента (рис.2.5).

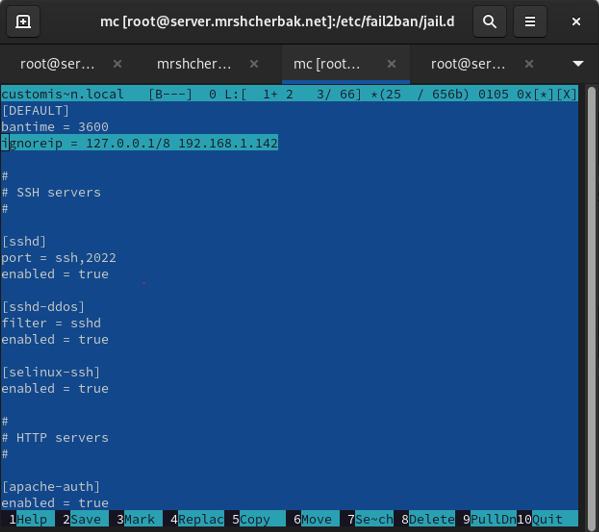


Рис.2.5. Содержимое файла /etc/fail2ban/jail.d/customisation.local

5. Перезапустила fail2ban и посмотрела журнал событий (рис.2.6).

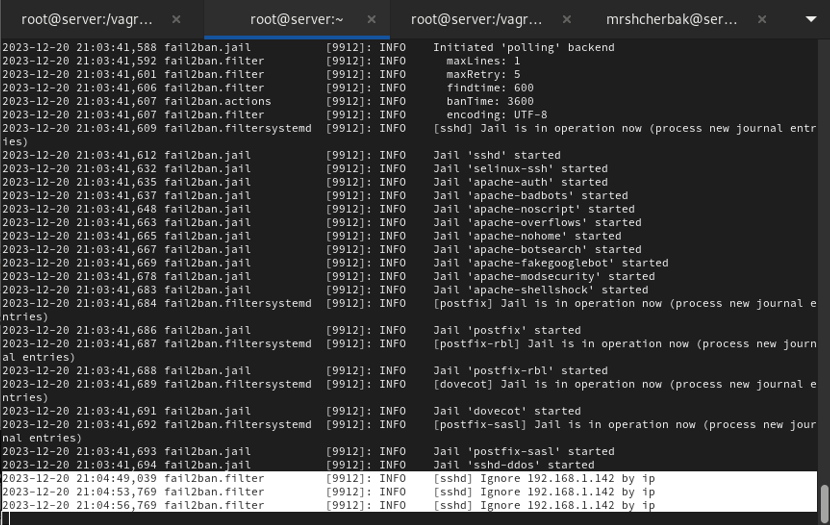


Рис.2.6. Просмотр журнала событий

6. Вновь попыталась войти с клиента на сервер с неправильным паролем и посмотрела статус защиты SSH (рисс.2.7 – рис.2.8).

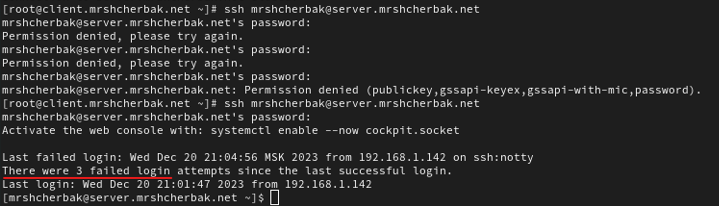


Рис.2.7. Выполнение команд

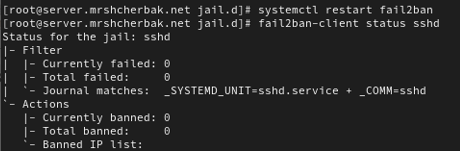


Рис.2.8. Просмотр статуса защиты SSH

**3. Внесение изменений в настройки внутреннего окружения виртуальных машин**

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создала в нём каталог protect, в который поместила в соответствующие подкаталоги конфигурационные файлы и в каталоге /vagrant/provision/server создала исполняемый файл protect.sh, в котором прописала скрипт (рис.3.2). Действия представлены на рис.3.1.



Рис.3.1. Выполнение команд

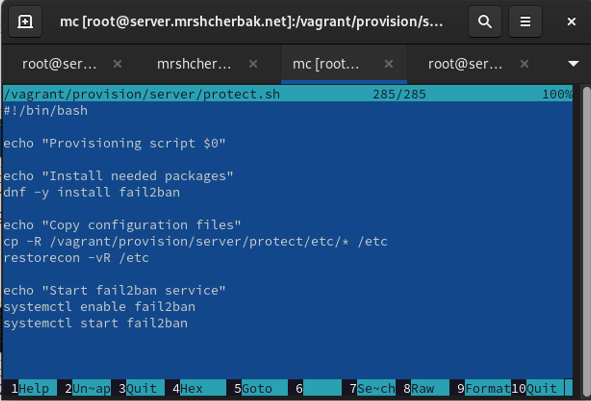


Рис.3.2. Содержимое файла protect.sh

2. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавила в соответствующем разделе конфигураций для сервера запись (рис.3.3).

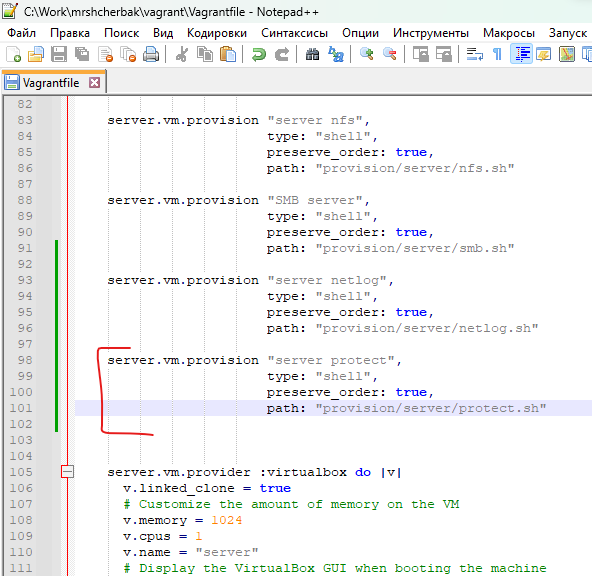


Рис.3.3. Содержимое файла Vagrantfile

**Вывод:** таким образом, в ходе выполнения л/р №16 я получила навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

# Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Принцип работы Fail2ban заключается в отслеживании сетевой активности на портах узла через анализ текстовых лог-файлов. При обнаружении неадекватной активности, например, brute force атаки, программа помещает IP-адрес атакующего в черный список, блокируя все пакеты с этого адреса. Блокировка осуществляется путем изменения правил межсетевого экрана.

1. Настройки какого файла более приоритетны: jail.conf или jail.local?

Настройки файла jail.local более приоритетны, так как они переопределяют соответствующие настройки из jail.conf. Jail.conf может обновляться и перезаписываться, то есть настройки могут не сохраниться. А конфигурационный файл jail.local имеет высший приоритет перед jail.conf, соответственно настройки в первую очередь будут применяться из данного файла.

1. Как настроить оповещение администратора при срабатывании Fail2ban?

Для настройки оповещений администратора при срабатывании Fail2ban, можно использовать некоторые параметры из секции [DEFAULT] в конфигурационных файлах.

destemail ⎯ параметр, задающий адрес эл.почты. Значение по умолчанию root@localhost;

mta ⎯ определяет почтовый агент, который будет использоваться для доставки почты. Если настроен Sendmail, оставить значение по умолчанию. Если же письма нужно доставлять на локальную машину поменять значение на mail.

destemail = ваш\_адрес\_электронной\_почты

mta = sendmail/mail

action = %(action\_mwl)s

Для локальной почты нужно заменить строчку action\_mw на action\_mwl. Это добавит лог к оповещению, чтобы было легче отслеживать события.

Перезапустить Fail2ban: sudo service fail2ban restart.

Теперь, когда Fail2ban обнаруживает неудачные попытки входа, администратор будет оповещен по электронной почте.

1. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.

[apache-auth] ⎯ определяет неудачные попытки ввода пароля.

[apache-badbots] ⎯ определяет ботов, которые ищут email адреса

[apache-noscript] ⎯ блокирует доступ к определенным скриптам

[apache-overflows] ⎯ предотвращает попытки переполнения Apache

[apache-nohome] ⎯ блокирует неудачные попытки поиска домашней директории

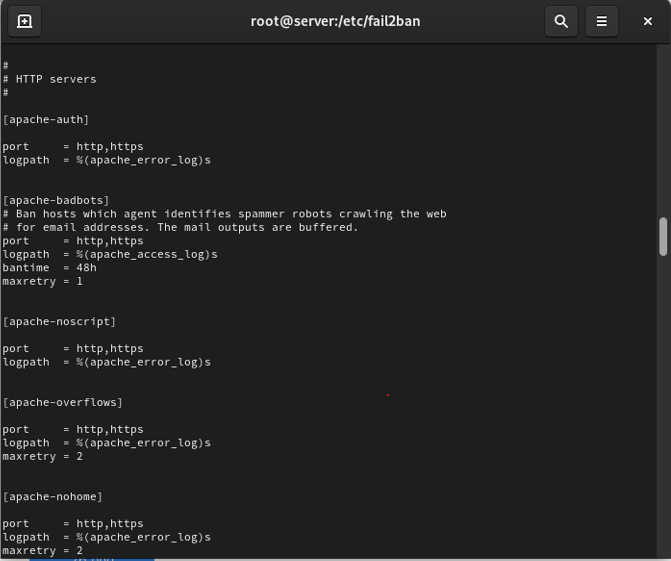
[apache-botsearch] ⎯ определяет ботов, которые перебором ищут популярные скрипты.

В строке port указываются порты, на которых слушает веб-служба Apache (HTTP и HTTPS).

В строке logpath указывается путь к лог-файлу ошибок Apache, который Fail2ban будет мониторить.

В строке maxretry указывается количество попыток, после которого IP-адрес будет заблокирован.

В строке bantime указывается время в секундах, на которое нарушитель будет заблокирован.



1. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе.

В строке filter указывается используемый фильтр, который указывает Fail2ban анализировать логи в режиме аутентификации (auth), либо в режиме RBL (Real-time Blackhole List).

В строке port указываются порты, которые Fail2ban будет мониторить для данной службы.

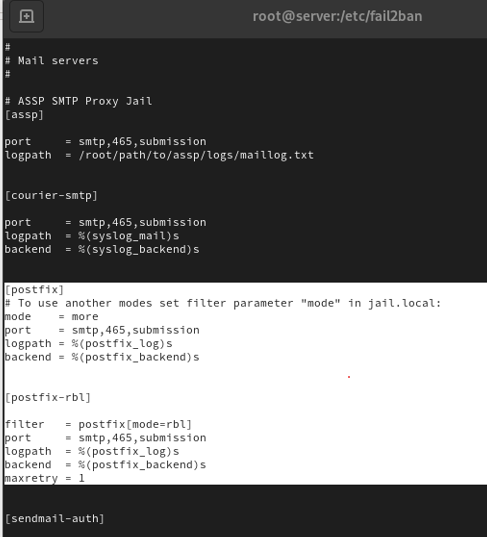
В строке logpath указывается путь к логам, который Fail2ban анализирует.

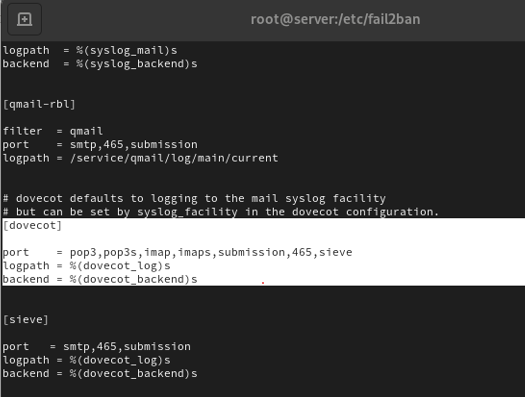
В сроке backend указывается используемый backend для анализа логов.

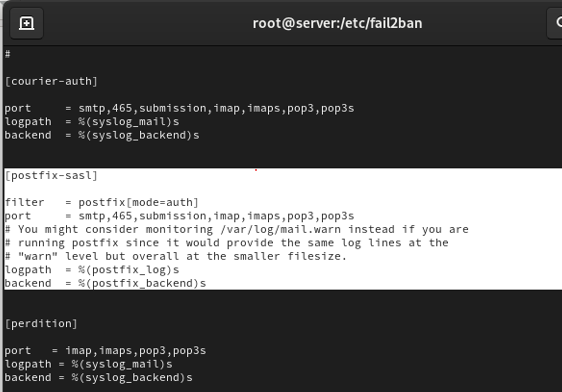
В строке mode указывается режим работы Fail2ban для данной службы.

В строке maxretry указывается количество попыток, после которого IP-адрес будет заблокирован.

Эти настройки определяют, как Fail2ban будет реагировать на подозрительную активность в логах почтовых служб Postfix и Dovecot.







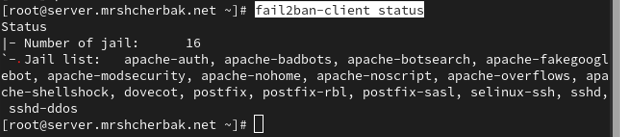
1. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Fail2ban при обнаружении атакующего IP-адреса может выполнять различные действия, в зависимости от конфигурации. Некоторые из базовых действий включают в себя блокировку IP-адреса на определенное время (bantime), игнорирование определенных IP-адресов (ignoreip), отправку уведомлений администратору и так далее.

Описания этих действий обычно содержатся в конфигурационных файлах Fail2ban, таких как jail.conf или jail.local. В этих файлах можно найти секции, посвященные определенным Jail'ам (группам правил), и внутри этих секций будут указаны параметры, связанные с действиями.

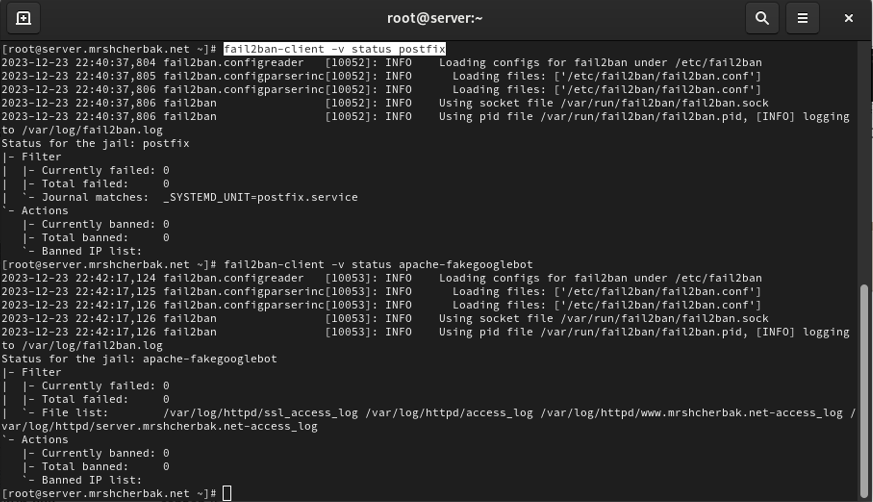
1. Как получить список действующих правил Fail2ban?

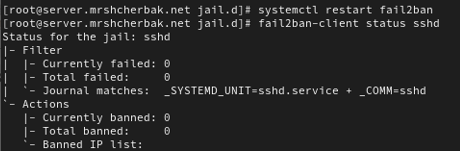
Для получения списка действующих правил Fail2ban можно воспользоваться командой: fail2ban-client status. В настоящий момент активны 16 правил Fail2ban.



1. Как получить статистику заблокированных Fail2ban адресов?

Для получения статистики заблокированных адресов можно использовать команду: fail2ban-client status <jail-name>, где <jail-name> ⎯ конкретное правило (jail). В данном случае, статистика для правил 'postfix' и 'apache-fakegooglebot' показывает, что в настоящий момент нет заблокированных IP-адресов.





1. Как разблокировать IP-адрес?

Для разблокировки IP-адреса можно воспользоваться командой:

fail2ban-client set <jail-name> unbanip <ip-address>

Разблокировала IP-адрес клиента и вновь посмотрела статус защиты SSH. Убедилась, что блокировка клиента снята.

