РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 16

**Базовая защита от атак типа «brute force»**

*дисциплина: Администрирование* *Сетевых Подсистем*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

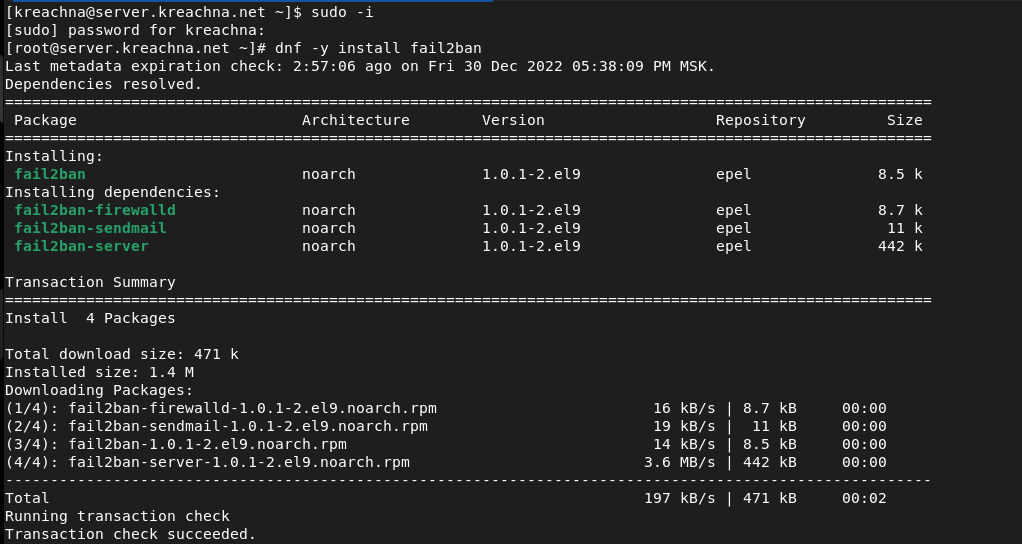
**Цель работы:**

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

**Выполнение работы:**

1. **Защита с помощью Fail2ban**
2. На сервере установите fail2ban:

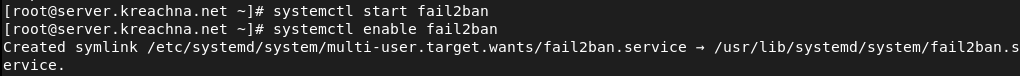
dnf -y install fail2ban



1. Запустите сервер fail2ban:

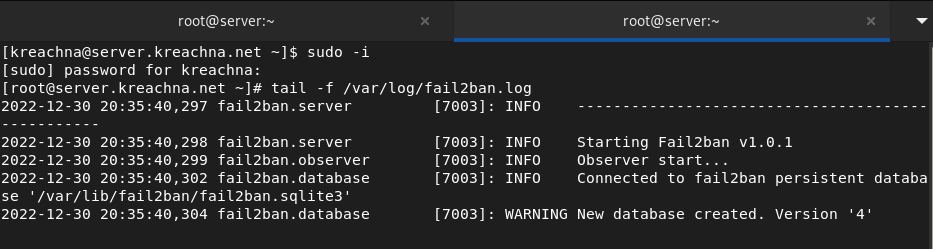
systemctl start fail2ban

systemctl enable fail2ban



1. В дополнительном терминале запустите просмотр журнала событий fail2ban:

tail -f /var/log/fail2ban.log

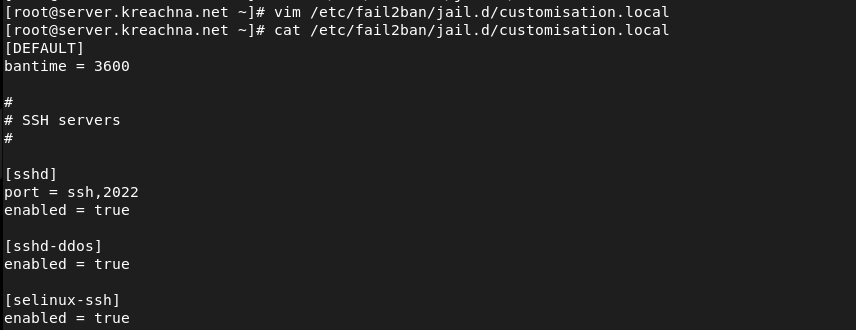


1. Создайте файл с локальной конфигурацией fail2ban:

touch /etc/fail2ban/jail.d/customisation.local



1. В файле /etc/fail2ban/jail.d/customisation.local:



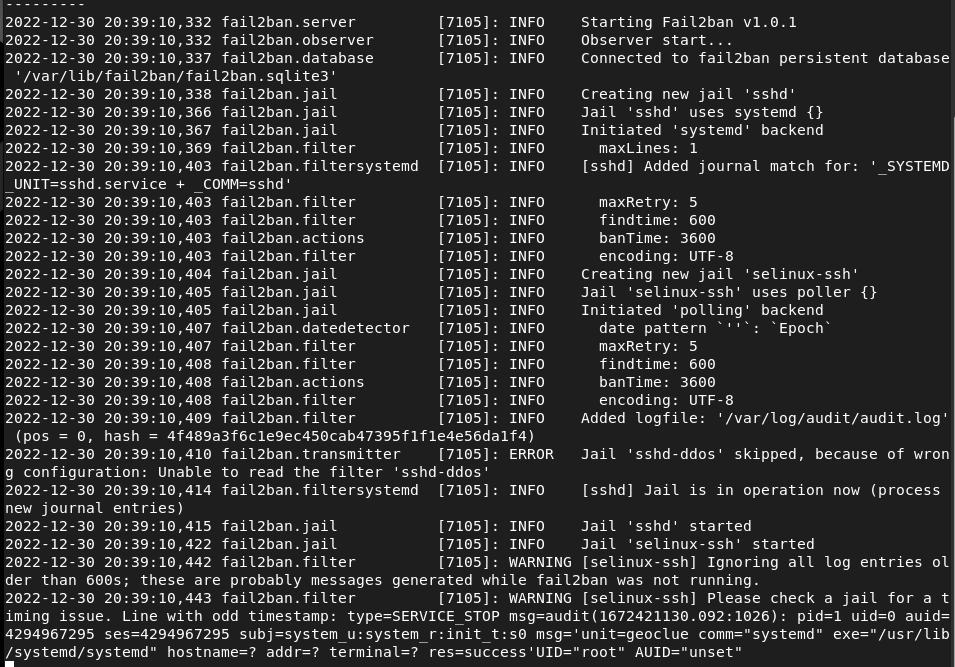
1. Перезапустите fail2ban

systemctl restart fail2ban



1. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log



1. В файле /etc/fail2ban/jail.d/customisation.local включите защиту HTTP:

****

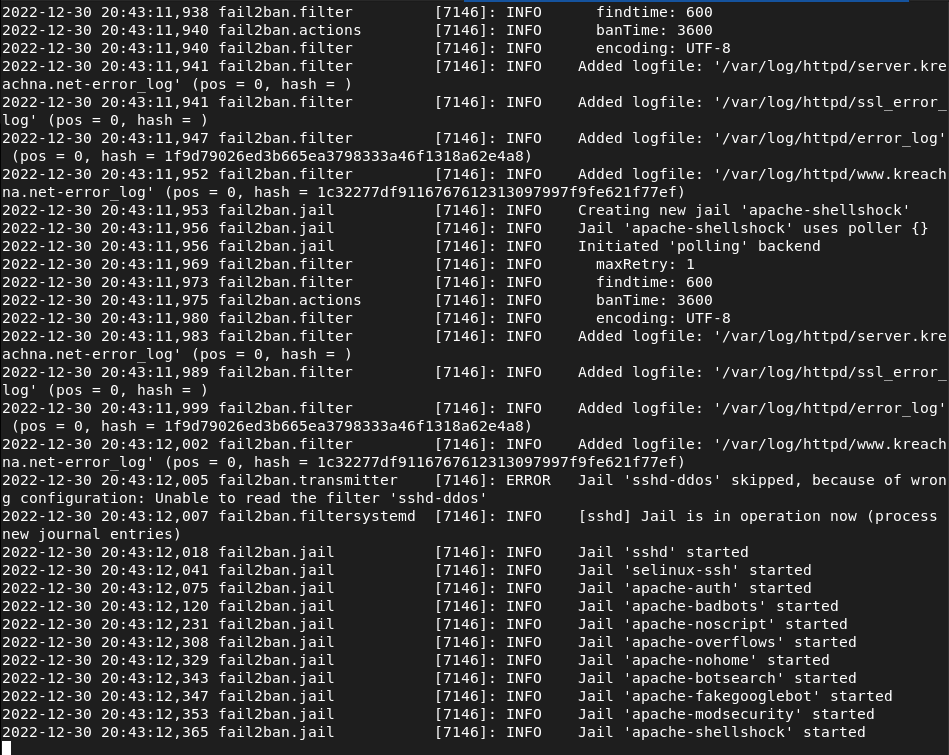
1. Перезапустите fail2ban

systemctl restart fail2ban



1. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log

****

1. В файле /etc/fail2ban/jail.d/customisation.local включите защиту почты:

****

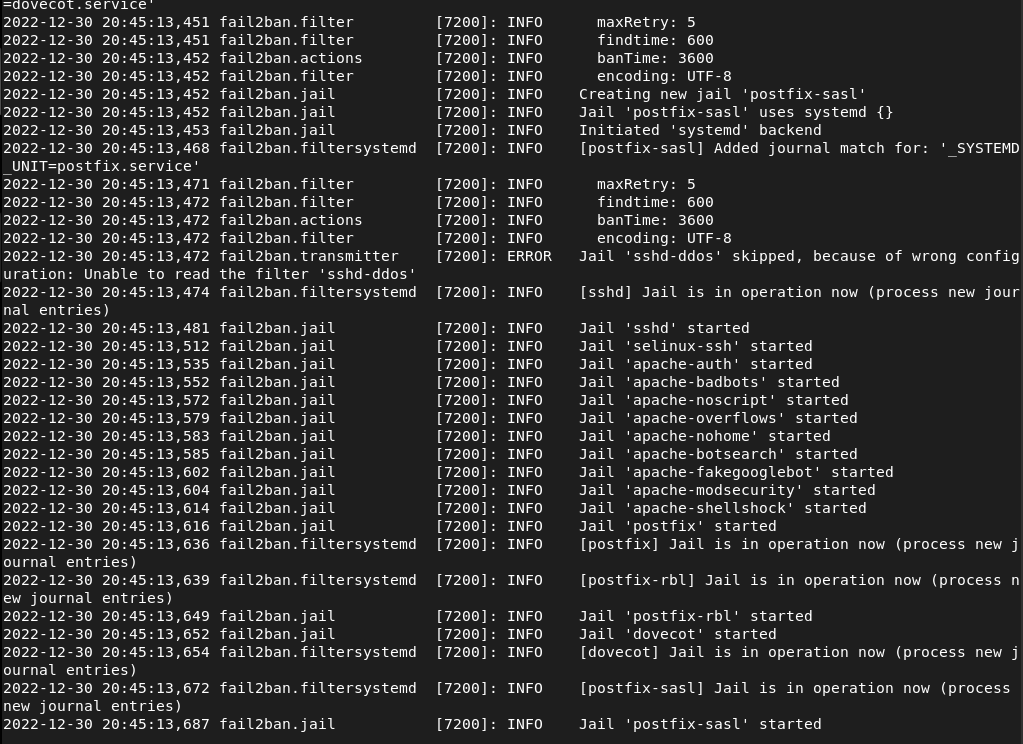
1. Перезапустите fail2ban:

systemctl restart fail2ban



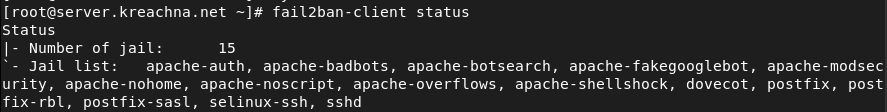
1. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log



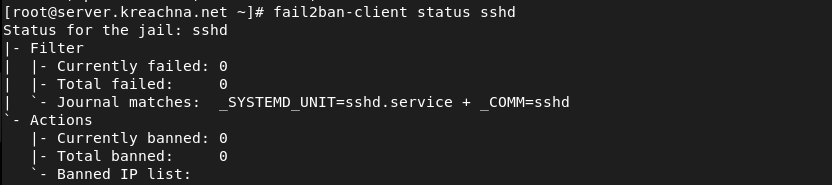
1. **Проверка работы Fail2ban**
2. На сервере посмотрите статус fail2ban:

fail2ban-client status



1. Посмотрите статус защиты SSH в fail2ban:

fail2ban-client status sshd

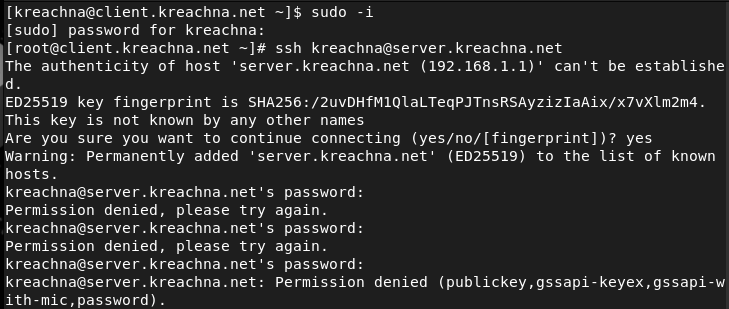


1. Установите максимальное количество ошибок для SSH, равное 2:

fail2ban-client set sshd maxretry 2

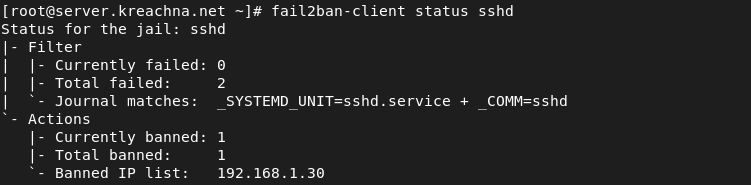


1. С клиента попытайтесь зайти по SSH на сервер с неправильным паролем.

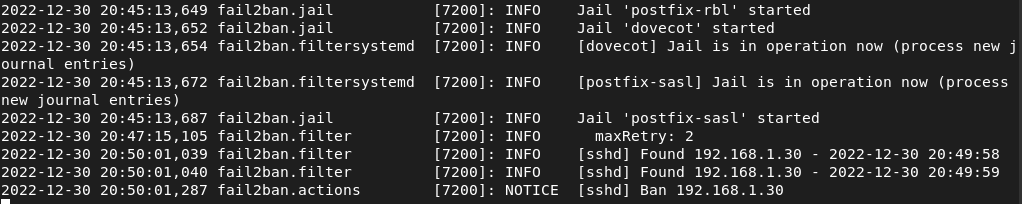


1. На сервере посмотрите статус защиты SSH:

fail2ban-client status sshd



Убедитесь, что произошла блокировка адреса клиента.



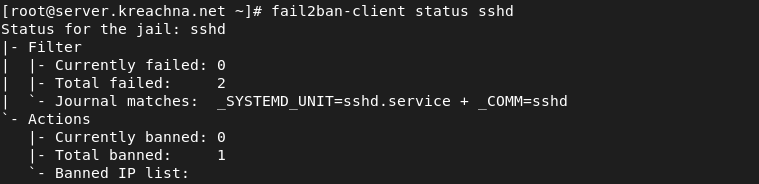
1. Разблокируйте IP-адрес клиента:

fail2ban-client set sshd unbanip 192.168.1.30



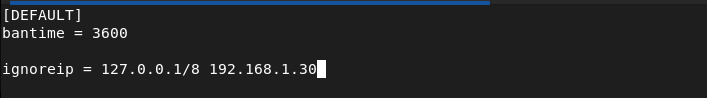
1. Вновь посмотрите статус защиты SSH:

fail2ban-client status sshd



Убедитесь, что блокировка клиента снята.

1. На сервере внесите изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента:

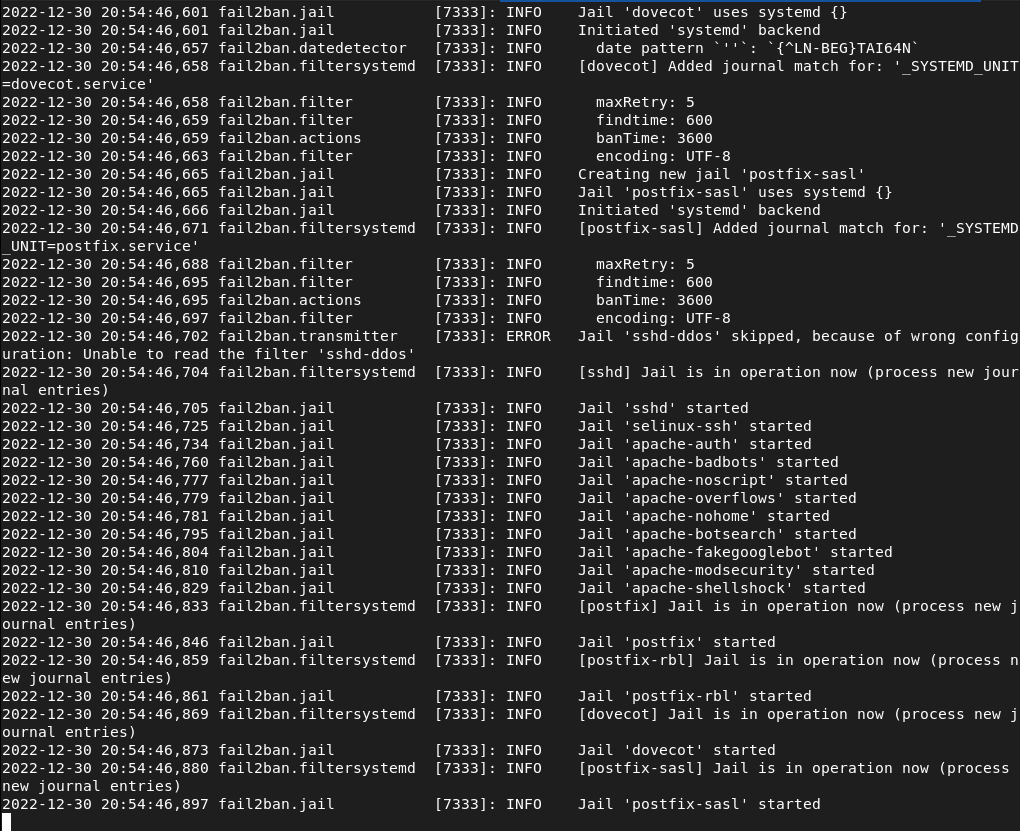


1. Перезапустите fail2ban.

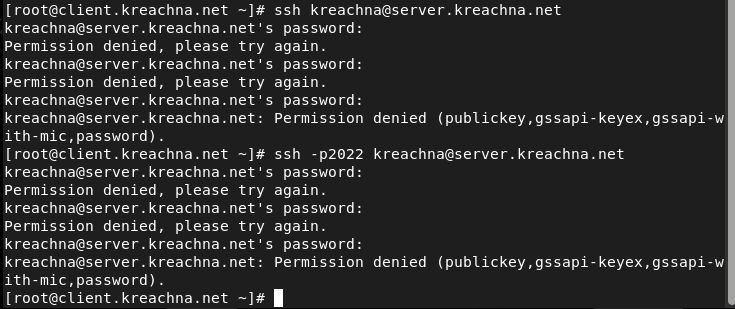


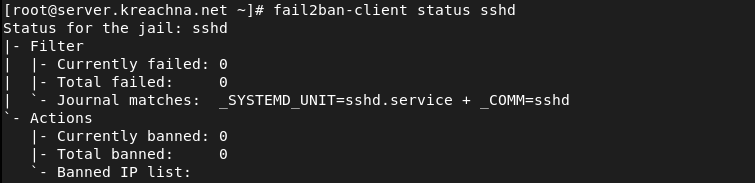
1. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log

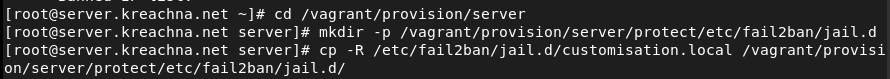


1. Вновь попытайтесь войти с клиента на сервер с неправильным паролем и посмотрите статус защиты SSH.





1. **Внесение изменений в настройки внутреннего окружения виртуальных машин**
2. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог protect, в который поместите в соответствующие подкаталоги конфигурационные файлы:

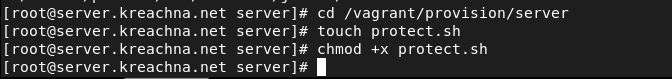


1. В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh:

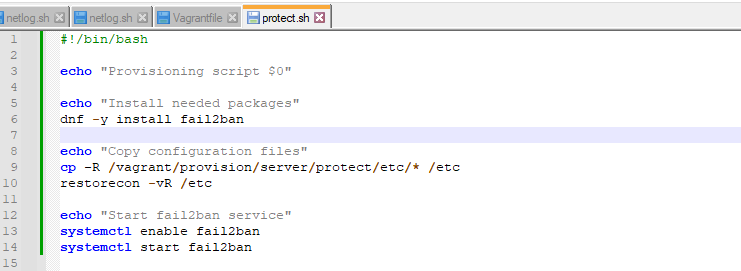
cd /vagrant/provision/server

touch protect.sh

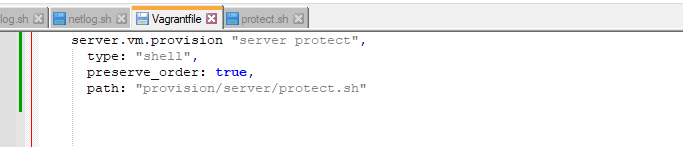
chmod +x protect.sh



Открыв его на редактирование, пропишите в нём следующий скрипт:



1. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера:



**Ответы на контрольные вопросы**

1. Поясните принцип работы Fail2ban.

Fail2ban считывает логи (например, /var/log/apache2/error.log) и блокирует IP-адреса, активность которых является подозрительной(например, большое количество попыток войти с неправильно введенным паролем, выполнение опасных или бессмысленных действий и т.д.). В случае обнаружения подобных действий программа обновляет правила брандмауэра для блокировки такого IPадреса на определенный промежуток времени.

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

После установки в каталоге /etc/fail2ban будет такая структура конфигурационных файлов

* /etc/fail2ban/jail.conf
* /etc/fail2ban/jail.d/\*.conf
* /etc/fail2ban/jail.local
* /etc/fail2ban/jail.d/\*.local

Конфигурационные файлы считываются сверху вниз. Последний считанный файл имеет высший приоритет. В данном случае при существовании фалов с расширением local будут более приоритетны.

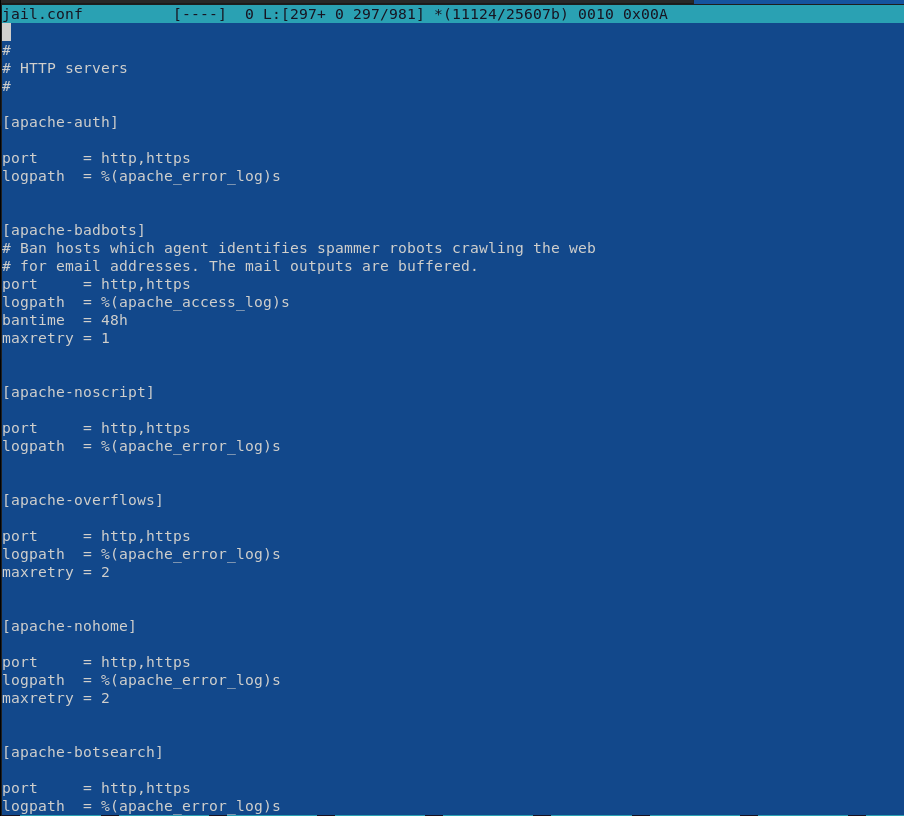
1. Как настроить оповещение администратора при срабатывании Fail2ban?

Если вы хотите настроить оповещение о срабатывании блокировки Fail2ban по электронной почте, это тоже настраивается в разделе [DEFAULT]. Только необходимо чтобы на вашей машине был настроен почтовый сервер и он мог отправлять письма на внешний адрес. Иначе все письма будут доставлены к локальной учетной записи Linux.

* destemail - этот параметр задает адрес электронной почты, на который вы хотите получать сообщения. Значение по умолчанию root@localhost;
* mta - определяет почтовый агент, который будет использоваться для доставки почты. Если у вас настроен Sendmail, оставьте значение по умолчанию. Если же письма нужно доставлять на локальную машину поменяйте значение на mail.
* Также для локальной почты нужно заменить строчку action\_mw на action\_mwl

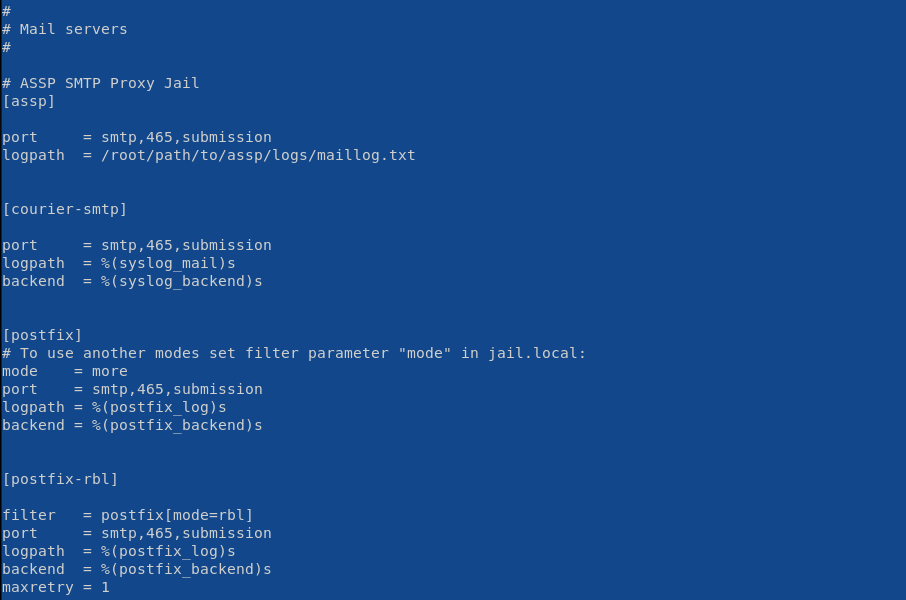
1. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.

В данном файле, если мы откроем часть «HTTP servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: [название правила], port — порт целевого сервиса, logpath — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, bantime — время бана в секундах, по истечении которого IP–адрес удаляется из списка заблокированных, maxretry — количество подозрительных совпадений, после которых применяется правило. Здесь присутствуют несколько секций, например, [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. Но они не активированы, чтобы это исправить, нужно в каждую секцию добавить параметр enabled = true.



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

В данном файле, если мы откроем часть «MAIL servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: [название правила], port — порт целевого сервиса, logpath — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, maxretry — количество подозрительных совпадений, после которых применяется правило.



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

Действие определяется в переменной action в зависимости от предпочтений администратора. Все правила реагирования на действия злоумышленника описаны в файле /etc/fail2ban/action.d. Соответственно, в качестве значения параметра action не может быть указана информация, которой нет в файле /etc/fail2ban/action.d

1. Как получить список действующих правил Fail2ban?

fail2ban-client status

1. Как получить статистику заблокированных Fail2ban адресов?

fail2ban-client status <имя клетки>

1. Как разблокировать IP-адрес?

fail2ban-client set <имя клетки> unbanip <ip-адрес>

**Вывод:**

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