Отчёт по лабораторной работе №16

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

## 2.1 Защита с помощью Fail2ban

На сервере устанавливаем fail2ban:

dnf -y install fail2ban

Запускаем сервер fail2ban (рис. 1).

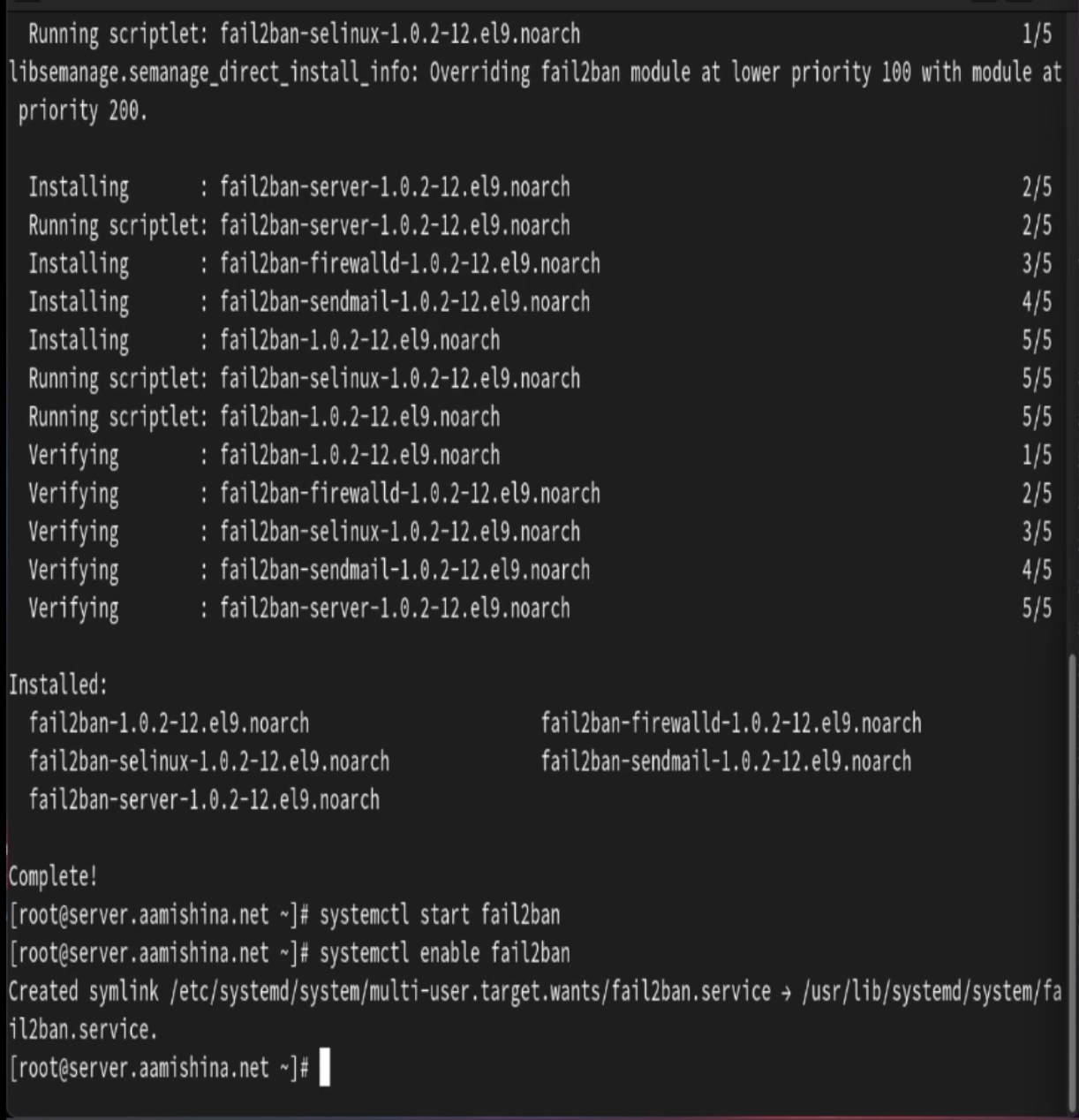


Рис. 1: Установка и запуск fail2ban

В доп. терминале запускаем просмотр журнала событий fail2ban. Создаем файл с локальной конфигурацией /etc/fail2ban/jail.d/customisation.local. Задаем время блокирования, включаем защиту SSH, после чего перезапускаем fail2ban (рис. 2).

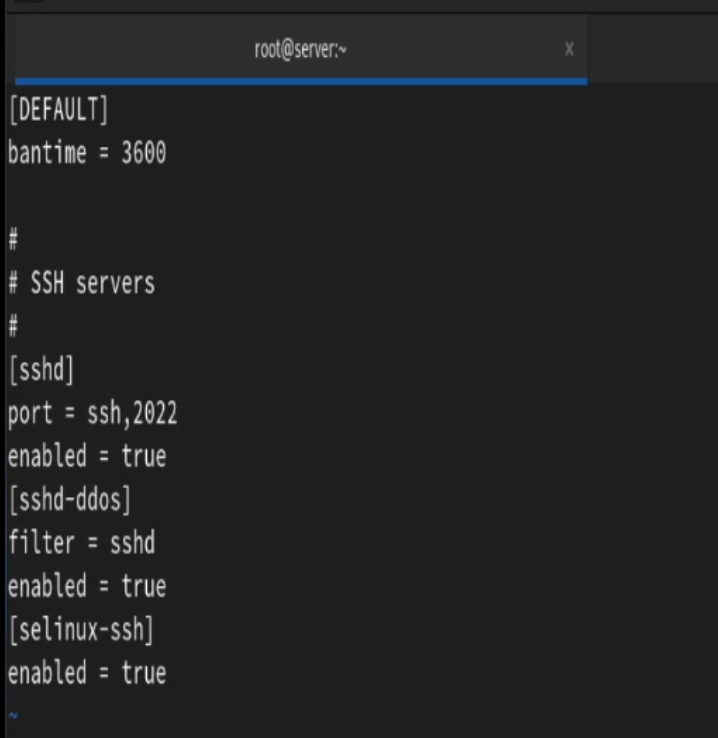


Рис. 2: Редактирование файла c локальной конфигурацией: задание времени блокировки, защита SSH

Просматриваем журнал событий fail2ban и видим сообщения об активации jail-ов (рис. 3).



Рис. 3: Просмотр журнала событий fail2ban

В файле конфигурации включаем защиту HTTP, после чего перезапускаем fail2ban (рис. 4).

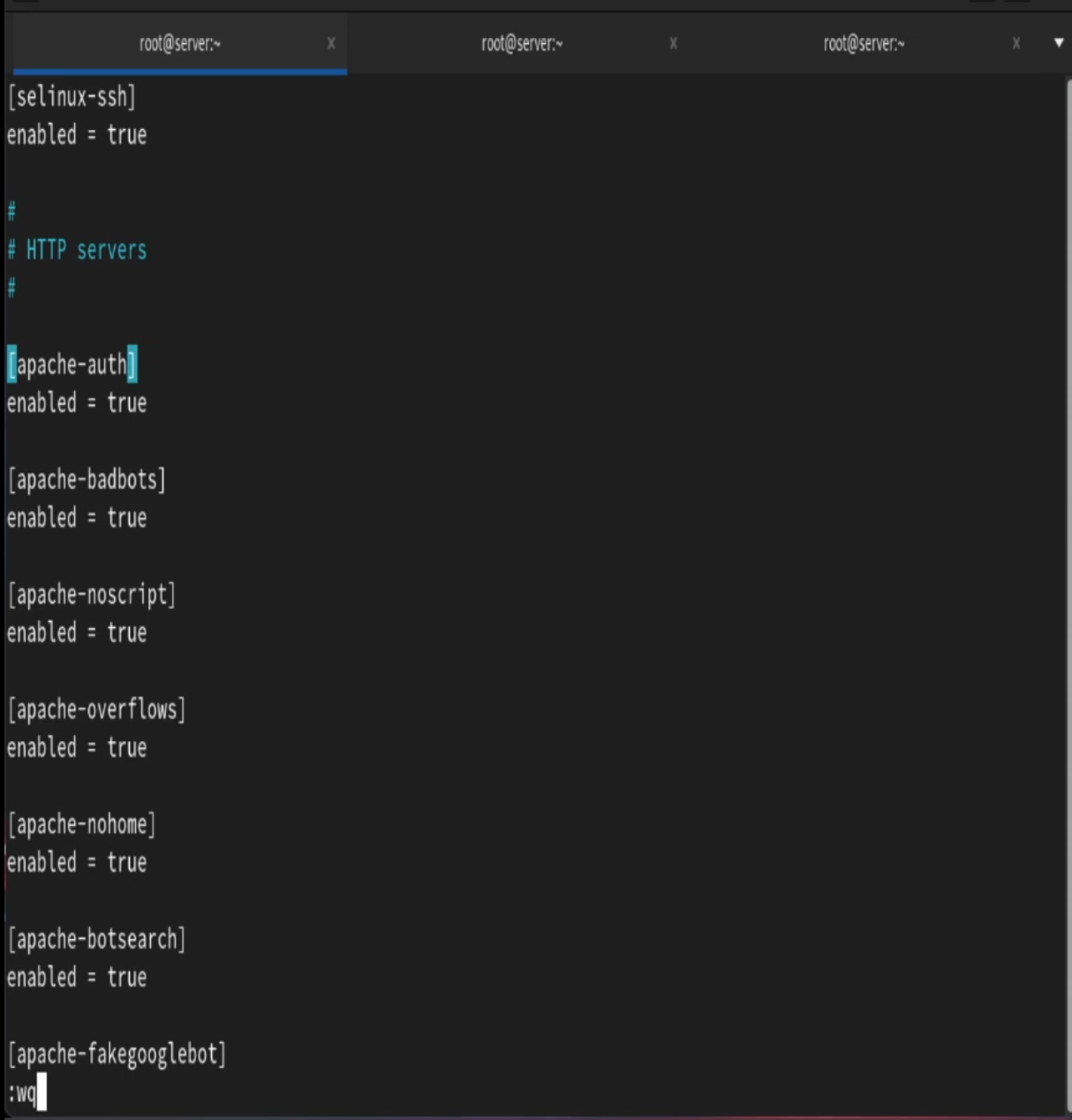


Рис. 4: Редактирование файла c локальной конфигурацией: защита HTTP

Просматриваем журнал событий fail2ban (рис. 5).

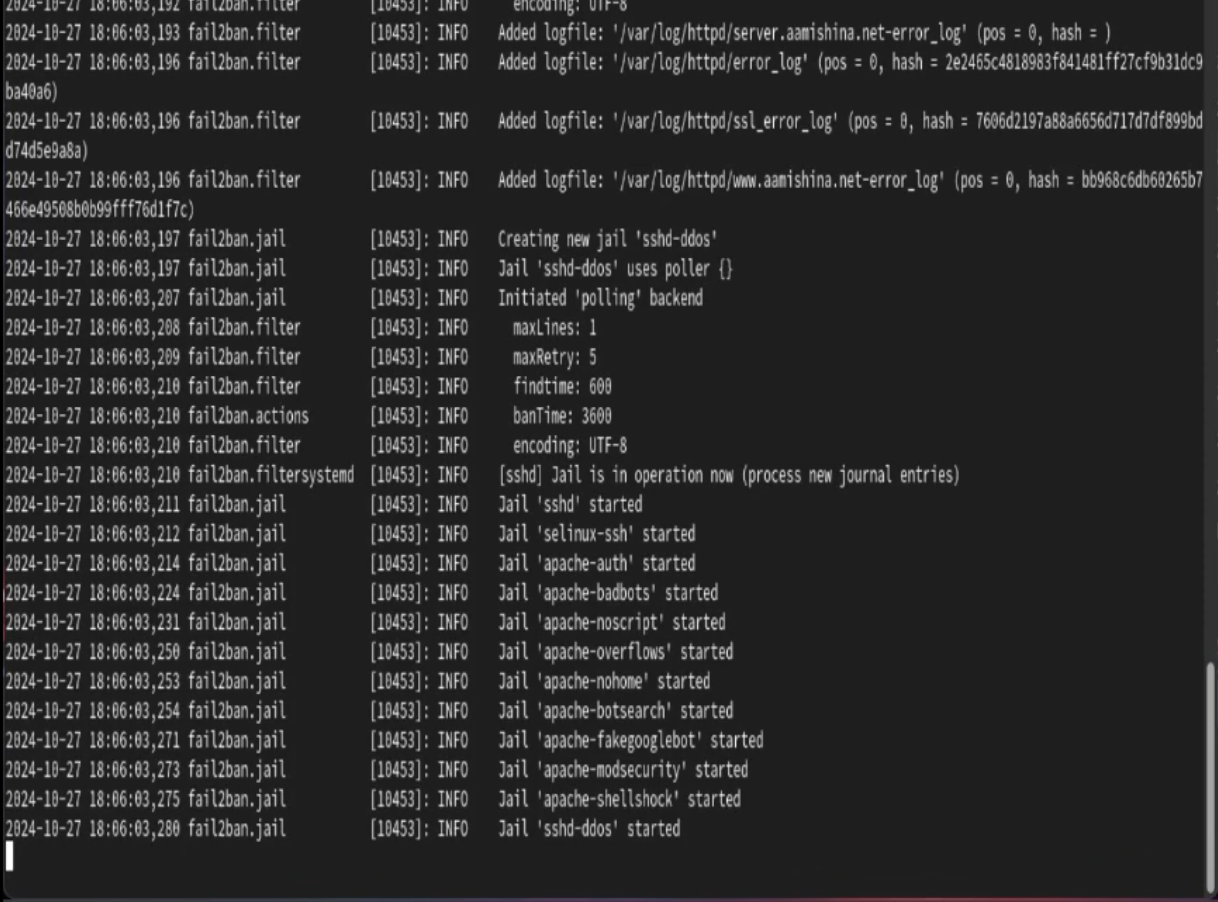


Рис. 5: Просмотр журнала событий fail2ban

В файле конфигурации включаем защиту почты, после чего перезапускаем fail2ban (рис. 6).

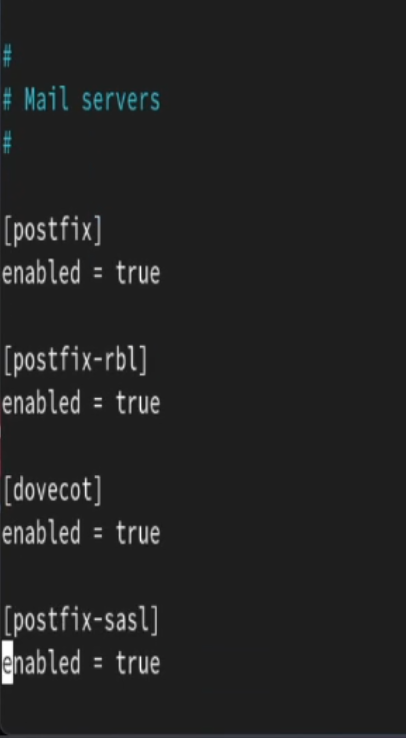


Рис. 6: Редактирование файла c локальной конфигурацией: защита почты

Просматриваем журнал событий fail2ban (рис. 7).

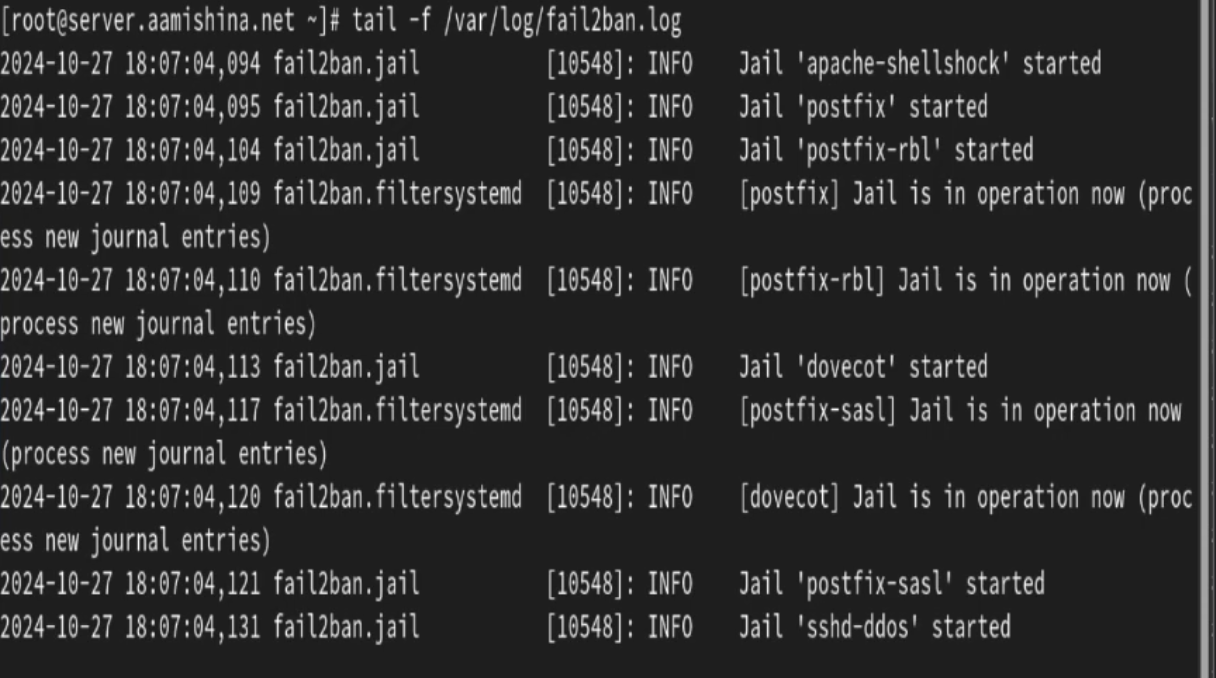


Рис. 7: Просмотр журнала событий fail2ban

## 2.2 Проверка работы Fail2ban

На сервере просматриваем статус службы, статус защиты SSH, устанавливаем максимальное количество ошибок для SSH, равное 2 (рис. 8).

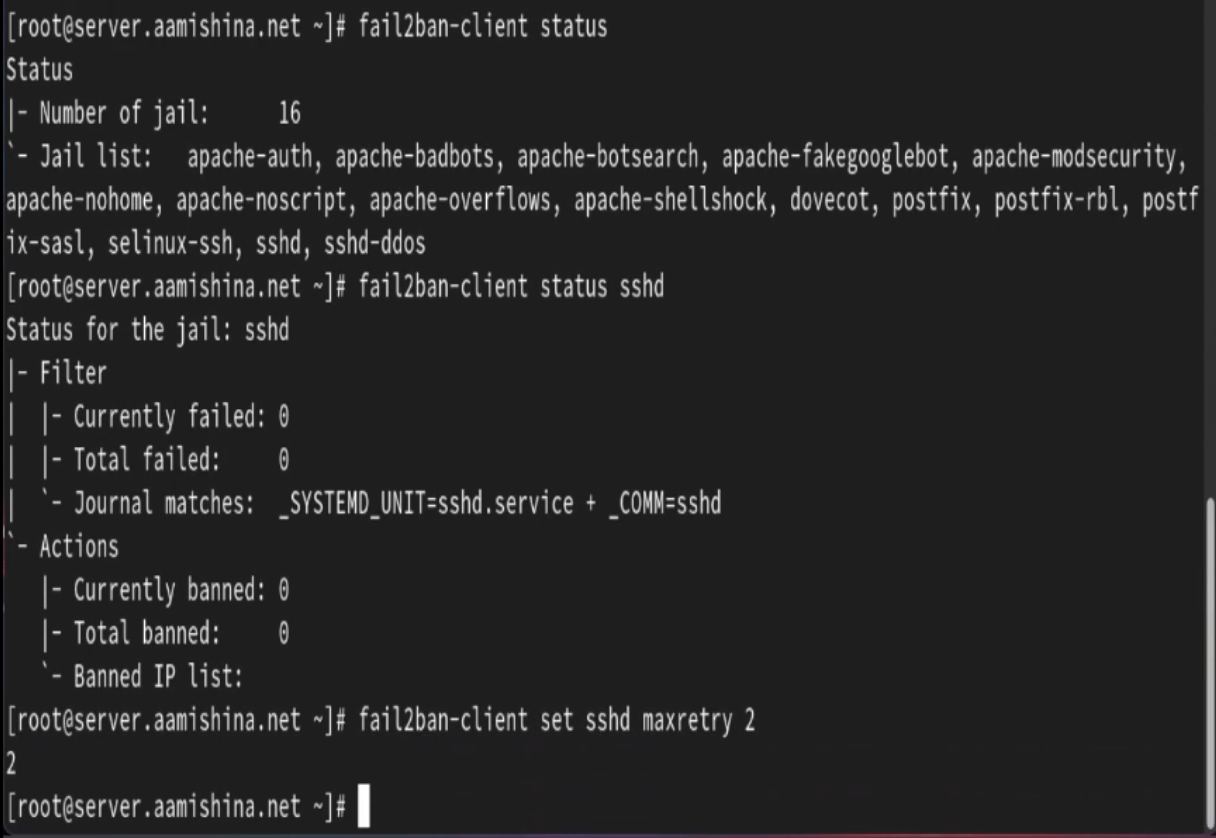


Рис. 8: Просмотр статуса службы, статус защиты SSH, установка макс. кол-ва ошибок для SSH

С клиента пытаемся подключиться к серверу по SSH и намеренно вводим неверный пароль (рис. 9).

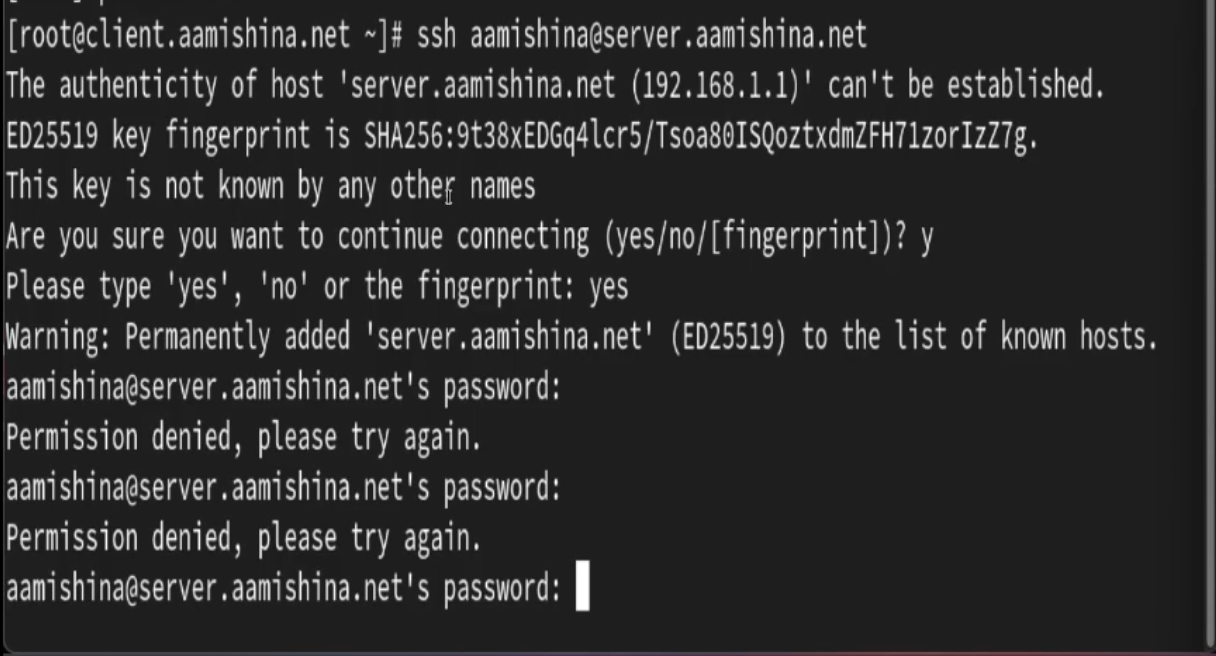


Рис. 9: Подключение к серверу по SSH с вводом неправильного пароля

Снова просматриваем статус защиты SSH на сервере и видим 2 попытки неудачного входа и 1 забаненный IP-адрес. Разблокируем адрес клиента и вновь просматриваем статус. Убеждаемся, что заблокированных IP нет (рис. 10).

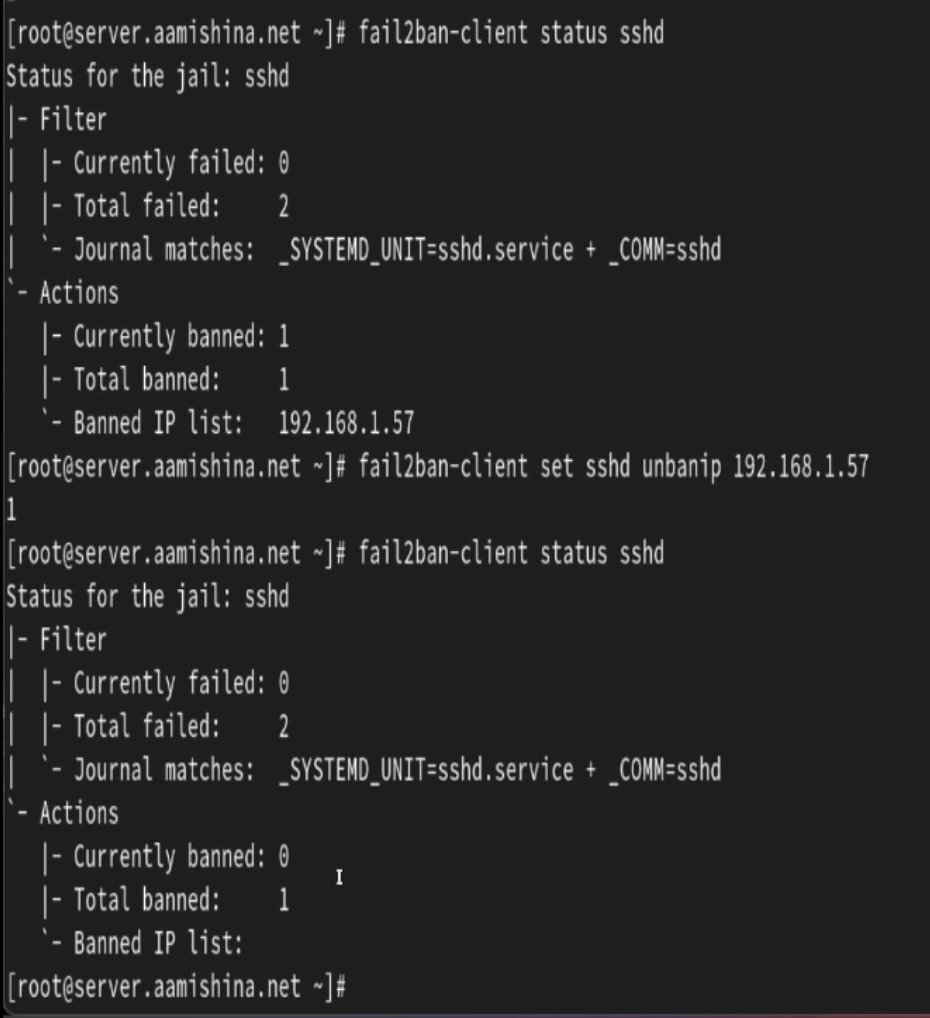


Рис. 10: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

Вносим изменения в конфигурационный файл, добавив в раздел по умолчанию игнорирование адреса клиента (рис. 11).

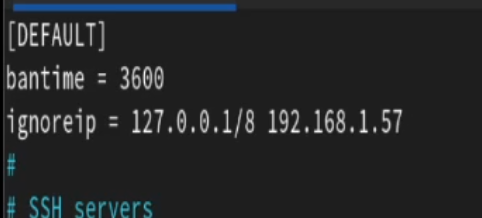


Рис. 11: Редактирование файла c локальной конфигурацией: игнорирование адреса клиента

Перезапускаем службу и просматриваем журнал событий (рис. 12).

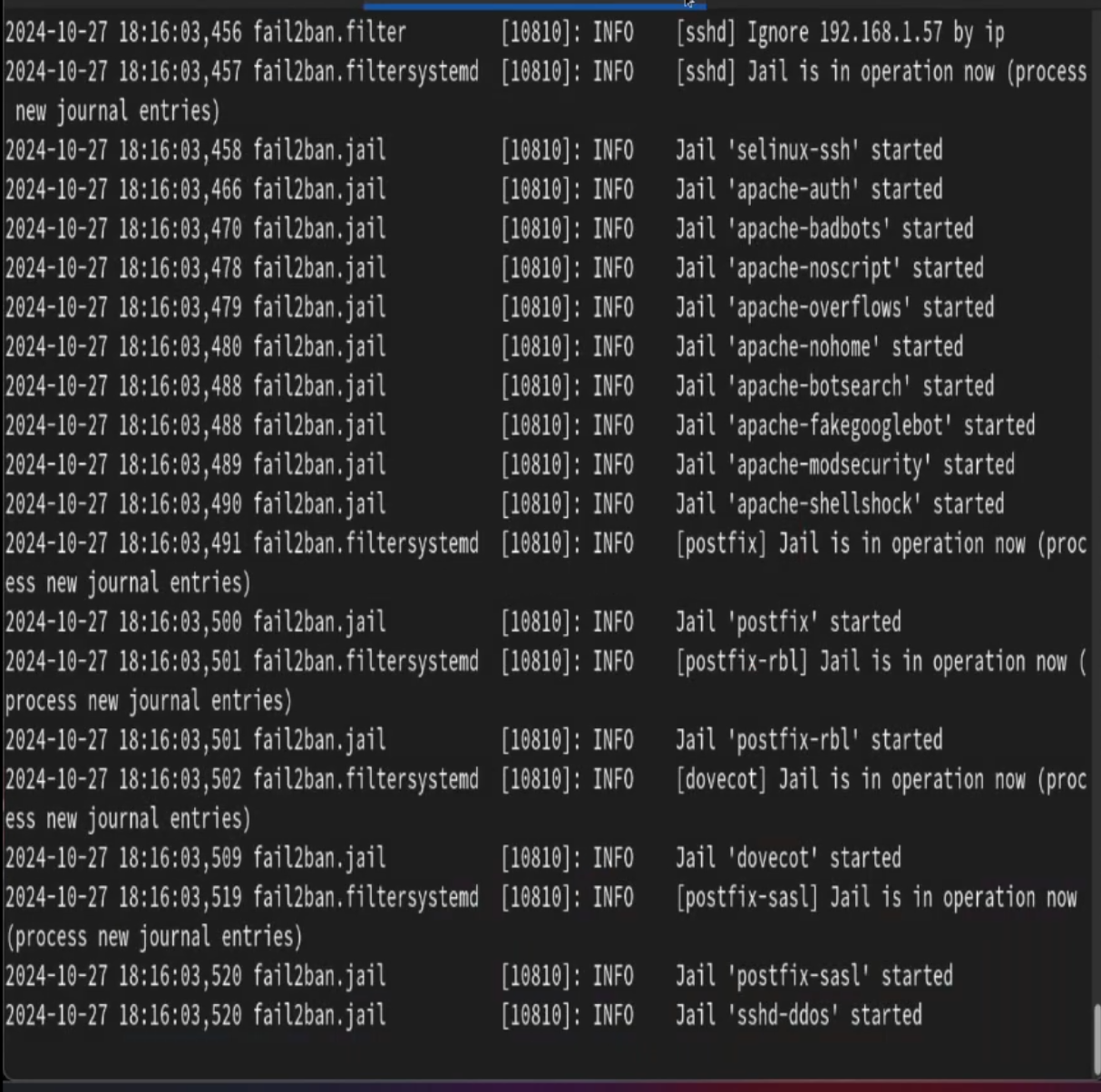


Рис. 12: Просмотр журнала событий `fail2ban’

С клиента вновь пытаемся аналогичным образом войти на сервер с неправильным паролем. Просматриваем статус защиты SSH и вижу 0 заблокированных адресов, так как адрес клиента находится в списке игнорируемых (рис. 13)

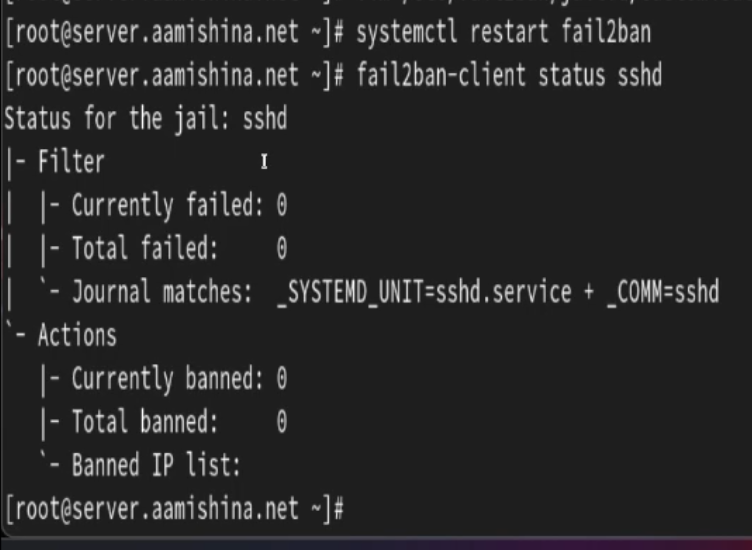


Рис. 13: Просмотр статуса защиты SSH после неудачного входа

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копируем в соответствующие каталоги конфигурационные файлы:

cd /vagrant/provision/server  
mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d  
cp -R /etc/fail2ban/jail.d/customisation.local  
 /vagrant/provision/server/protect/etc/fail2ban/jail.d/

Вносим изменения в файл /vagrant/provision/server/protect.sh (рис. 14).

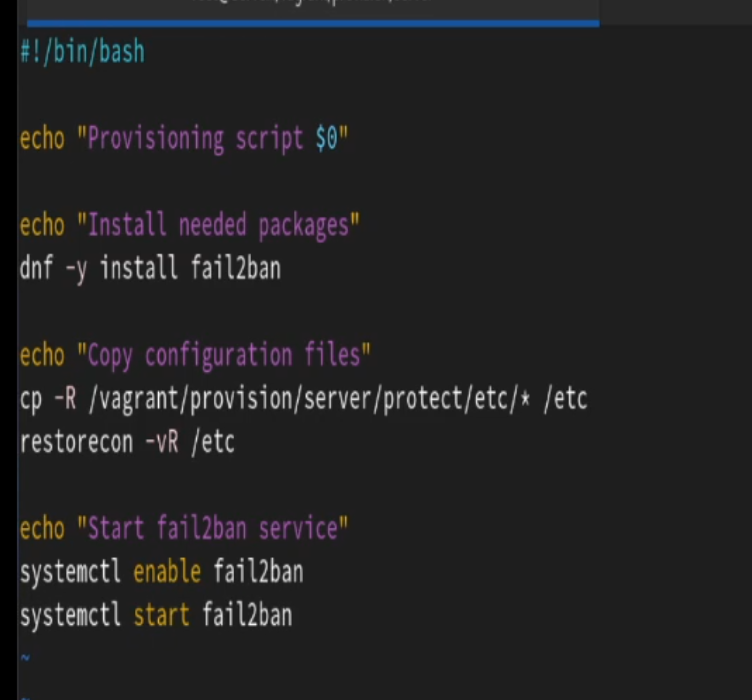


Рис. 14: Редактирование protect.sh на сервере

Для отработки созданного скрипта во время загрузки ВМ server в конфигурационном файле Vagrantfile добавляем запись в соответствующий раздел конфигураций для сервера:

server.vm.provision "server protect",  
 type: "shell",  
 preserve\_order: true,  
 path: "provision/server/protect.sh"

# 3 Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban - это программное обеспечение, которое предотвращает атаки на сервер, анализируя лог-файлы и блокируя IP-адреса, с которых идут подозрительные или злонамеренные действия. Он работает следующим образом:

* Мониторит указанные лог-файлы на наличие заданных событий (например, неудачных попыток входа).
* Когда число попыток превышает определенный порог, Fail2ban временно блокирует IP-адрес, добавляя правила в файрвол.
* Заблокированный IP-адрес может быть разблокирован автоматически после определенного периода времени

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

Настройки файла jail.local более приоритетны, чем настройки файла jail.conf.

1. Как настроить оповещение администратора при срабатывании Fail2ban?

Чтобы настроить оповещение администратора при срабатывании Fail2ban, необходимо настроить отправку уведомлений по электронной почте или другим способом. Это можно сделать, изменяя настройки в файле jail.local, добавляя адрес электронной почты администратора и настройки SMTPсервера.

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

Примеры настроек по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе:

* [apache] - секция, относящаяся к веб-серверу Apache.
* enabled = true - включение проверки лог-файлов Apache.
* port = http,https - указание портов для мониторинга.
* filter = apache-auth - указание фильтра для обработки лог-файлов.
* logpath = /var/log/apache\*/\*error.log - путь к лог-файлам Apache.
* maxretry = 5 - максимальное количество попыток до блокировки адреса.
* bantime = 600 - продолжительность блокировки в секундах.

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

Примеры настроек по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе:

* [postfix] - секция, относящаяся к почтовому серверу Postfix.
* enabled = true - включение проверки лог-файлов Postfix.
* port = smtp,ssmtp - указание портов для мониторинга.
* filter = postfix - указание фильтра для обработки лог-файлов.
* logpath = /var/log/mail.log - путь к лог-файлам Postfix.
* maxretry = 3 - максимальное количество попыток до блокировки адреса.
* bantime = 3600 - продолжительность блокировки в секундах

1. 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 при обнаружении атакующего IP-адреса, такие как блокировка адреса через файрвол, добавление правил в IP-таблицы, отправка уведомлений администратору и другие. Описание доступных действий можно найти в документации или руководстве Fail2ban.

1. Как получить список действующих правил Fail2ban?

Можно использовать команду: fail2ban-client status.

1. Как получить статистику заблокированных Fail2ban адресов?

Можно использовать команду fail2ban-client status <jail-name>, где <jail-name> - имя конкретного jail, например, “ssh” или “apache”.

1. Как разблокировать IP-адрес?

fail2ban-client set sshd unbanip <ip-адрес клиента>

# 4 Выводы

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