**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №16**

*дисциплина: Администрирование сетевых подсистем*

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

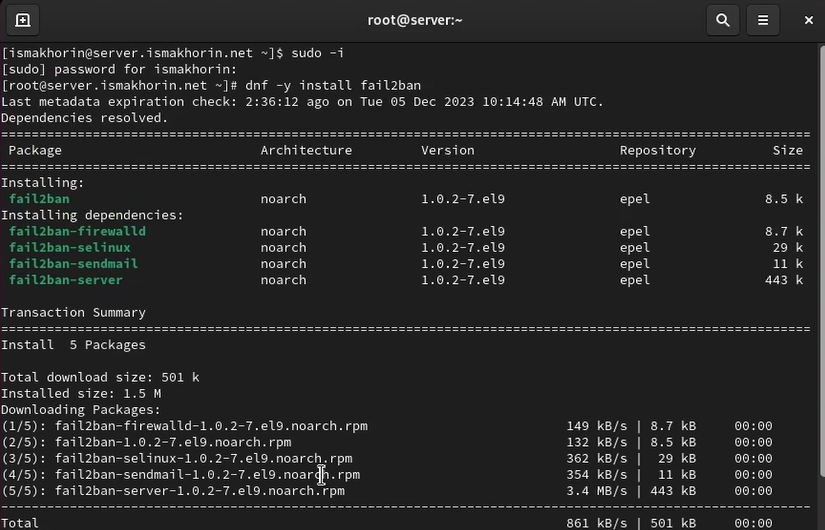
# Цель работы:

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

**Выполнение работы:**

На сервере установим fail2ban (Рис. 1.1):

dnf -y install fail2ban

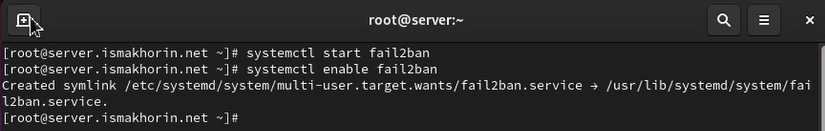
****

**Рис. 1.1.** Установка на сервере fail2ban.

Запустим сервер fail2ban (Рис. 1.2):

systemctl start fail2ban

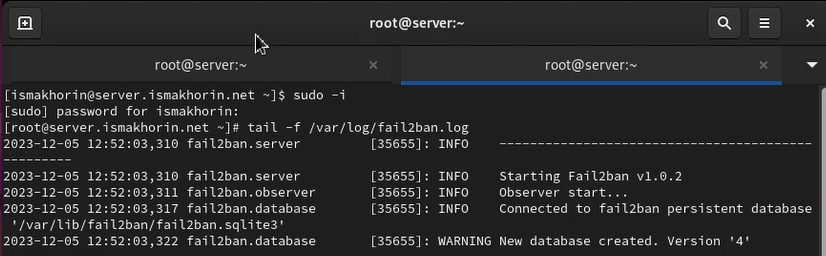
systemctl enable fail2ban

****

**Рис. 1.2.** Запуск сервера fail2ban.

В дополнительном терминале запустим просмотр журнала событий fail2ban (Рис. 1.3):

tail -f /var/log/fail2ban.log

****

**Рис. 1.3.** Запуск просмотра в дополнительном терминале журнала событий fail2ban.

Создадим файл с локальной конфигурацией fail2ban (Рис. 1.4):

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

****

**Рис. 1.4.** Создание файла с локальной конфигурацией fail2ban.

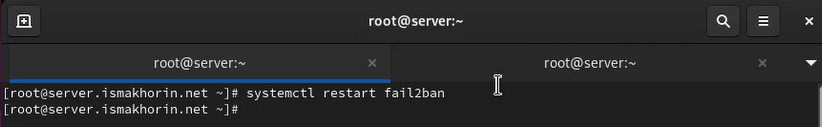
В файле /etc/fail2ban/jail.d/customisation.local зададим время блокирования на 1 час и включим защиту SSH (Рис. 1.5):

****

**Рис. 1.5.** Настройка в файле /etc/fail2ban/jail.d/customisation.local времени блокирования на 1 час и включение защиты SSH.

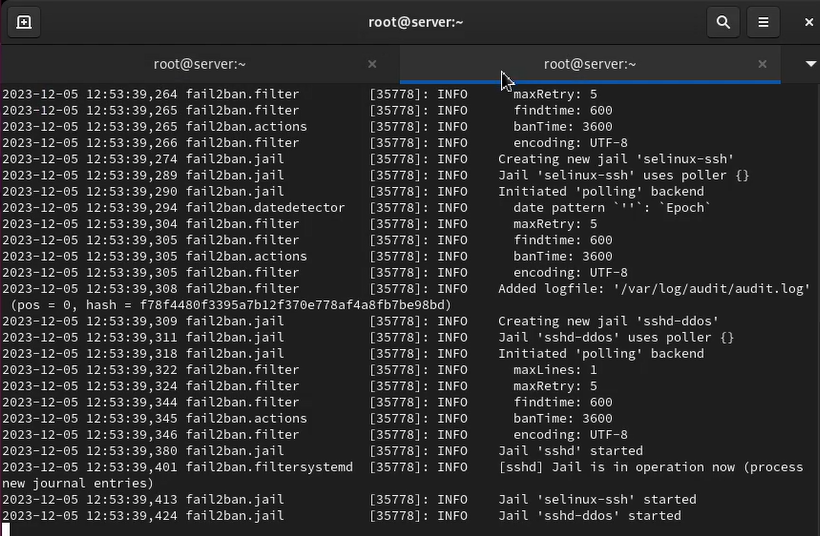
Перезапустим fail2ban (Рис. 1.6):

systemctl restart fail2ban

****

**Рис. 1.6.** Перезапуск fail2ban.

Посмотрим журнал событий (Рис. 1.7):

****

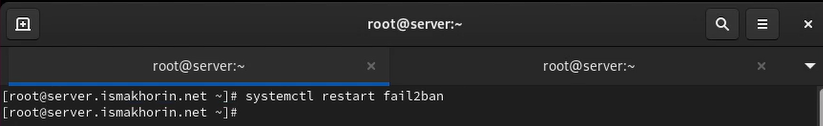
**Рис. 1.7.** Просмотр журнала событий.

В файле /etc/fail2ban/jail.d/customisation.local включим защиту HTTP (Рис. 1.8):

****

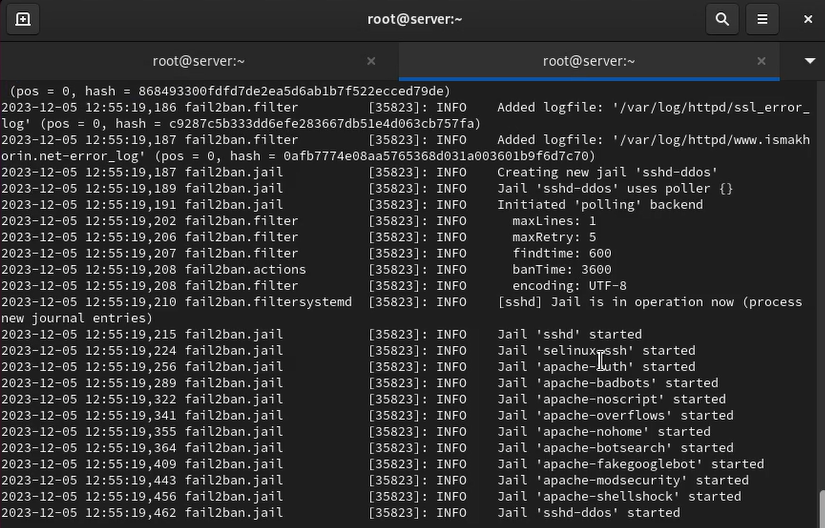
**Рис. 1.8.** Включение защиты HTTP в файле /etc/fail2ban/jail.d/customisation.local.

Перезапустим fail2ban (Рис. 1.9):

****

**Рис. 1.9.** Перезапуск fail2ban.

После чего посмотрим журнал событий (Рис. 1.10):

****

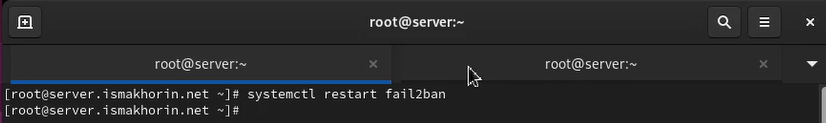
**Рис. 1.10.** Просмотр журнала событий.

В файле /etc/fail2ban/jail.d/customisation.local включим защиту почты (Рис. 1.11):

****

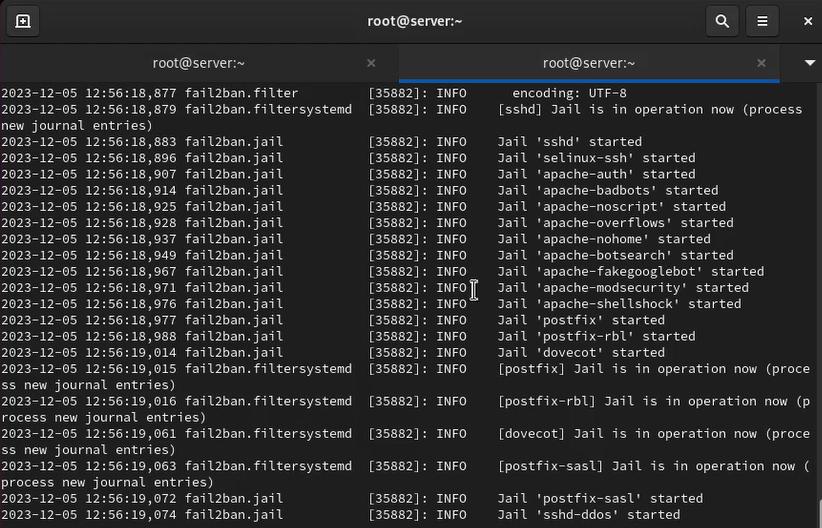
**Рис. 1.11.** Включение защиты почты в файле /etc/fail2ban/jail.d/customisation.local.

Снова перезапустим fail2ban (Рис. 1.12):

****

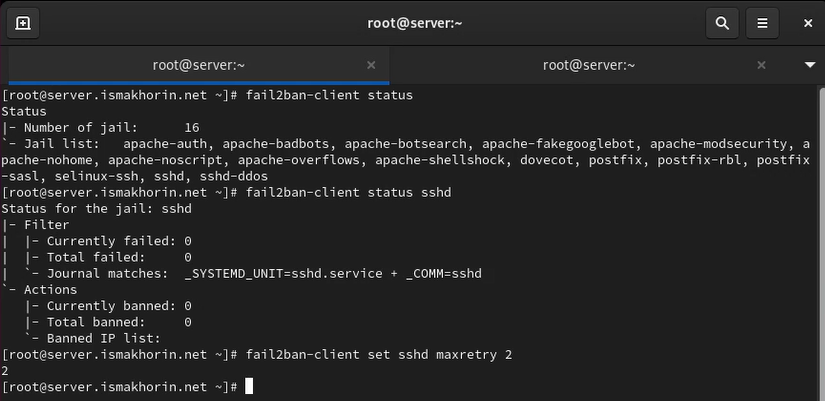
**Рис. 1.12.** Повторный перезапуск fail2ban.

И посмотрим журнал событий (Рис. 1.13):

****

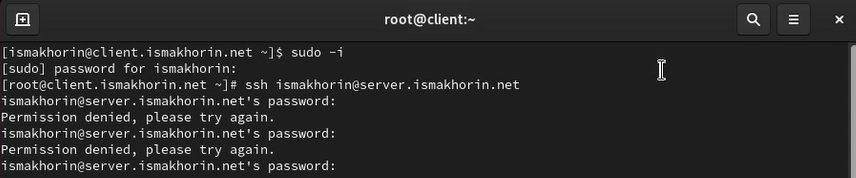
**Рис. 1.13.** Просмотр журнала событий.

На сервере посмотрим статус fail2ban, статус защиты SSH в fail2ban и установим максимальное количество ошибок для SSH, равное 2 (Рис. 2.1):

****

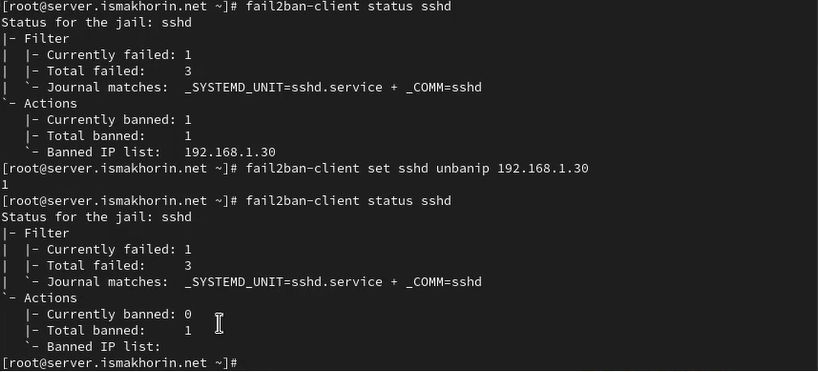
**Рис. 2.1.** Просмотр на сервере статуса fail2ban, статуса защиты SSH в fail2ban и установка максимального количества ошибок для SSH (=2).

С клиента попытаемся зайти по SSH на сервер с неправильным паролем (Рис. 2.2):

****

**Рис. 2.2.** 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. 2.3):

****

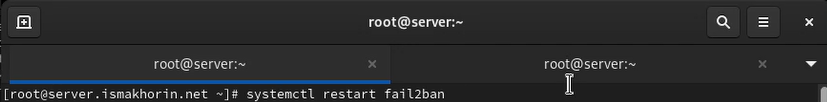
**Рис. 2.3.** Просмотр на сервере статуса защиты SSH, разблокировка IP-адреса клиента и повторная проверка.

На сервере внесём изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента (Рис. 2.4):

****

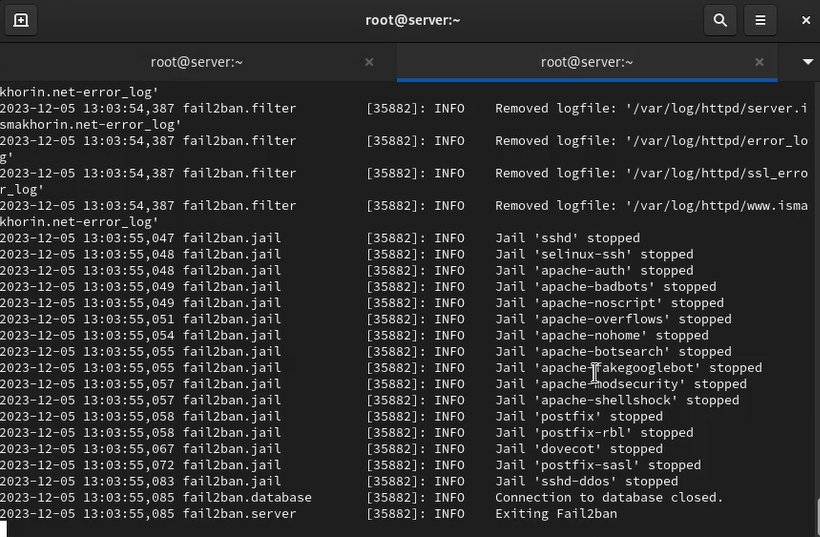
**Рис. 2.4.** Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле /etc/fail2ban/jail.d/customisation.local.

Перезапустим fail2ban (Рис. 2.5):

****

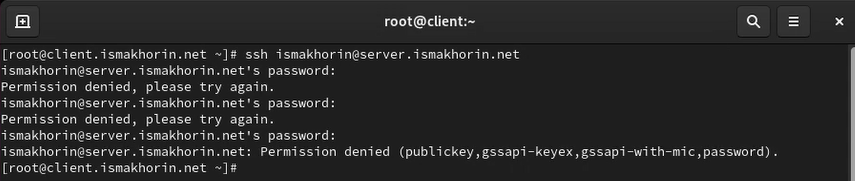
**Рис. 2.5.** Перезапуск fail2ban.

Далее посмотрим журнал событий (Рис. 2.6):

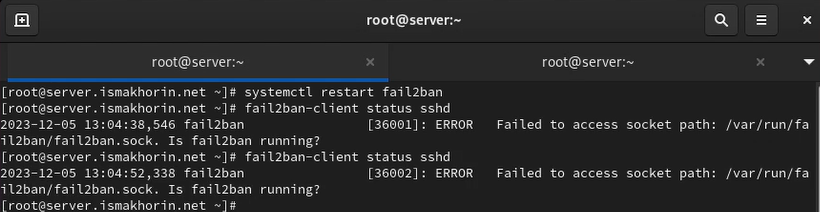
****

**Рис. 2.6.** Просмотр журнала событий.

Вновь попытаемся войти с клиента на сервер с неправильным паролем (Рис. 2.7) и посмотрим статус защиты SSH (Рис. 2.8):

****

**Рис. 2.7.** Попытка войти с клиента на сервер с неправильным паролем.

****

**Рис. 2.8.** 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. 3.1):

****

**Рис. 3.1.** 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. 3.2):

****

**Рис. 3.2.** 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. 3.3):

****

**Рис. 3.3.** Добавление конфигураций в конфигурационном файле Vagrantfile для сервера.

**Вывод:**

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

**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**.

1. 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.**
2. 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).**
3. 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**

1. 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]**

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, 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.**
2. Как получить список действующих правил Fail2ban? - **Используйте команду: fail2ban-client status.**
3. Как получить статистику заблокированных Fail2ban адресов? - **Используйте команду: fail2ban-client status <jail\_name>.**
4. Как разблокировать IP-адрес? - **Используйте команду: fail2ban-client set <jail\_name> unbanip <ip\_address>.**