Отчет по лабораторной работе №16

Базовая защита от атак типа «brute force»

Галацан Николай, НПИбд-01-22

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 устанавливаю fail2ban:

dnf -y install fail2ban

Запускаю сервер fail2ban (рис. 1).

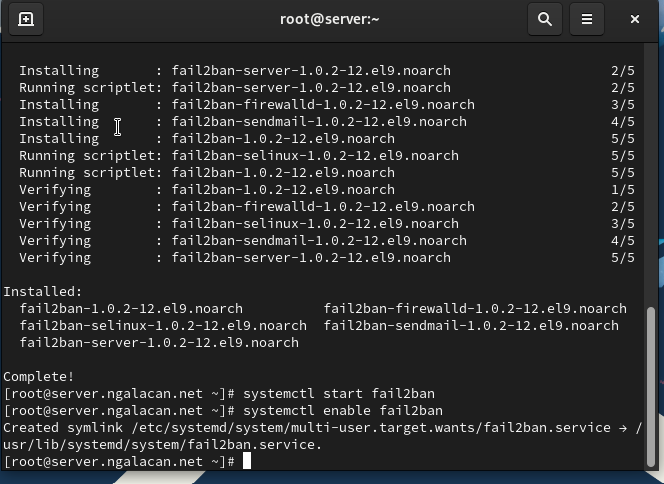


Рис. 1: Установка и запуск fail2ban

В доп. терминале запускаю просмотр журнала событий fail2ban. Создаю файл с локальной конфигурацией /etc/fail2ban/jail.d/customisation.local. Задаю время блокирования, включаю защиту SSH, после чего перезапускаю fail2ban (рис. 2).

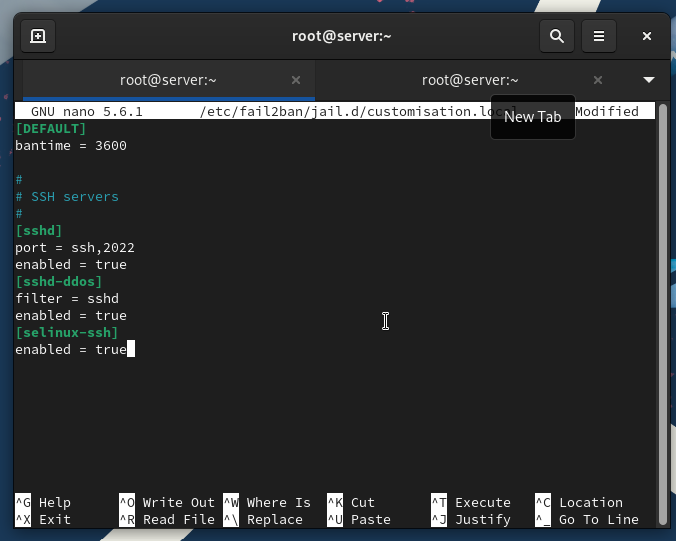


Рис. 2: Редактирование файла c локальной конфигурацией: задание времени блокировки, защита SSH

Просматриваю журнал событий fail2ban и вижу сообщения об активации jail-ов (рис. 3).

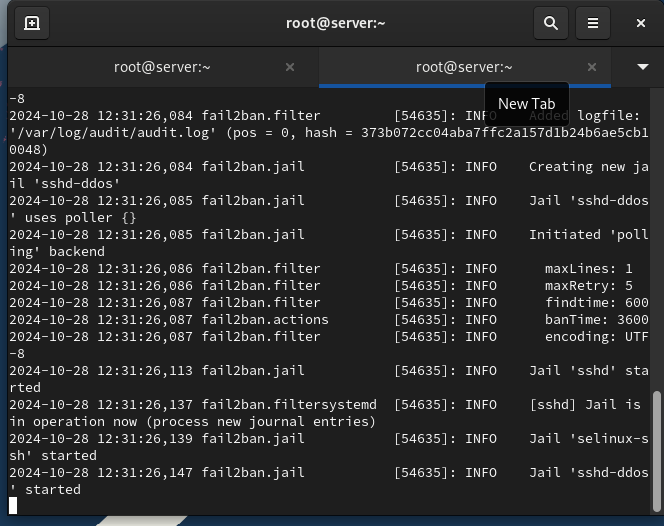


Рис. 3: Просмотр журнала событий fail2ban

В файле конфигурации включаю защиту HTTP, после чего перезапускаю fail2ban (рис. 4).

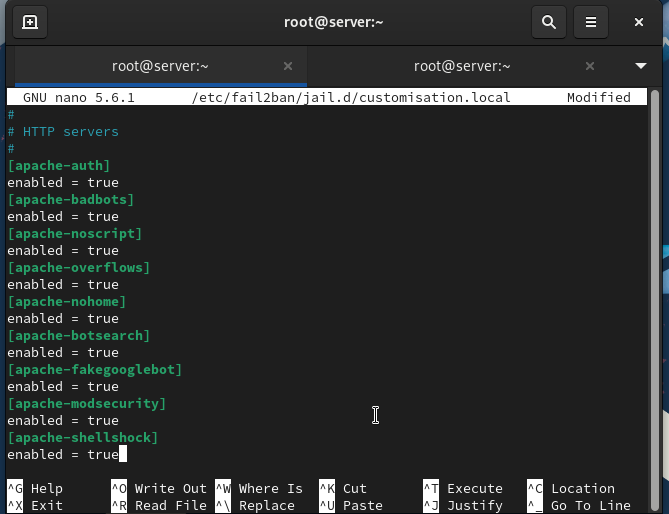


Рис. 4: Редактирование файла c локальной конфигурацией: защита HTTP

Просматриваю журнал событий fail2ban (рис. 5).

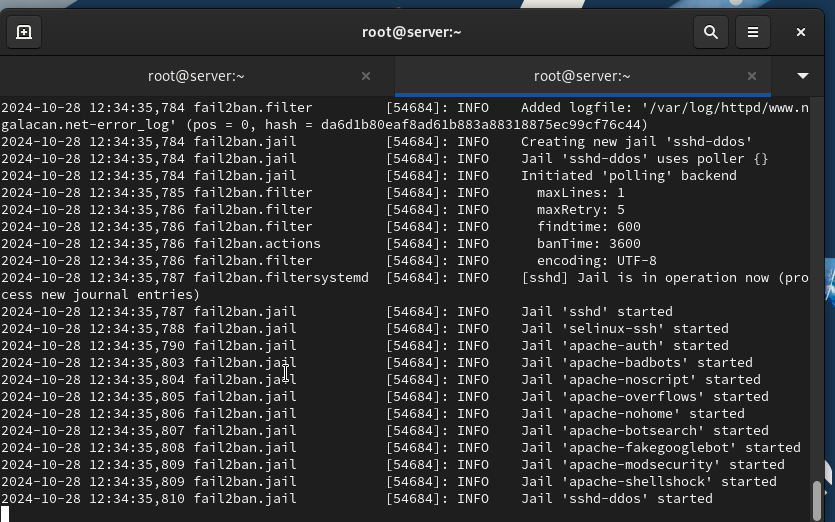


Рис. 5: Просмотр журнала событий fail2ban

В файле конфигурации включаю защиту почты, после чего перезапускаю fail2ban (рис. 6).

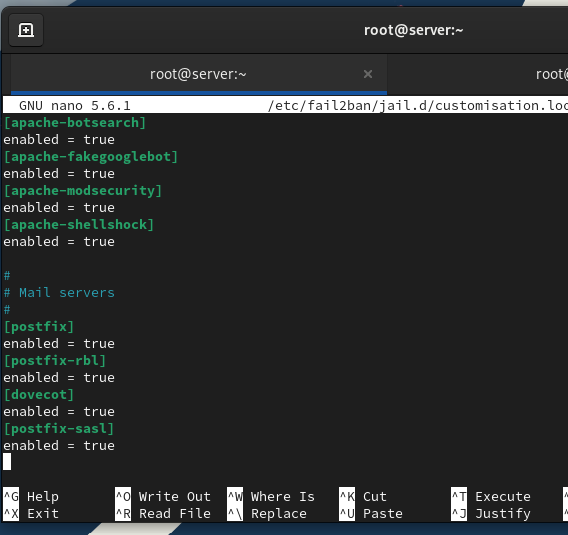


Рис. 6: Редактирование файла c локальной конфигурацией: защита почты

Просматриваю журнал событий fail2ban (рис. 7).

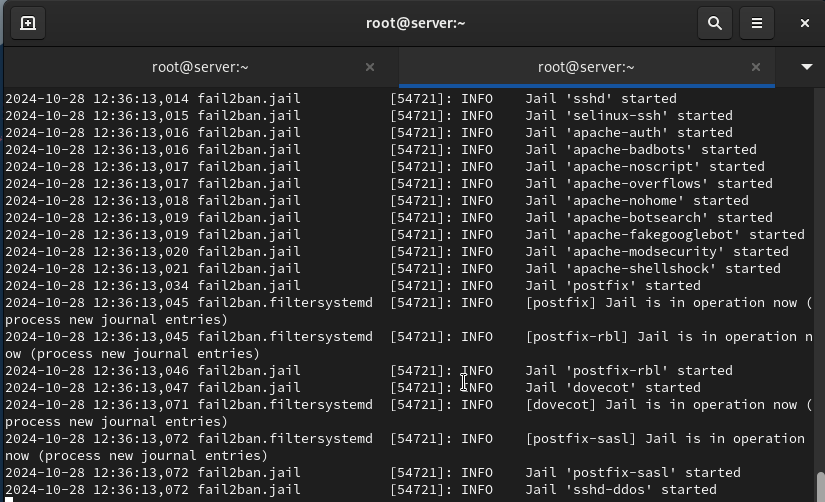


Рис. 7: Просмотр журнала событий fail2ban

## 2.2 Проверка работы Fail2ban

На сервере просматриваю статус службы, статус защиты SSH, устанавливаю максимальное количество ошибок для SSH, равное 2:

fail2ban-client status  
fail2ban-client status sshd  
fail2ban-client set sshd maxretry 2

С клиента пытаюсь подключиться к серверу по SSH и намеренно ввожу неверный пароль (рис. 8).

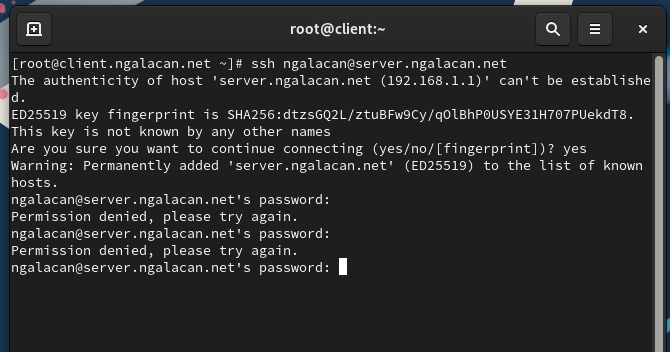


Рис. 8: Подключение к серверу по SSH с вводом неправильного пароля

Снова просматриваю статус защиты SSH на сервере и вижу 2 попытки неудачного входа и 1 забаненный IP-адрес. Разблокирую адрес клиента и вновь просматриваю статус. Убеждаюсь, что заблокированных IP нет (рис. 9).

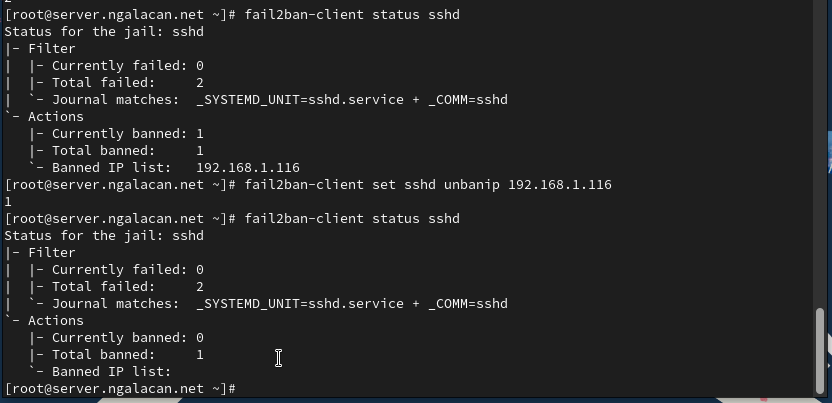


Рис. 9: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

Вношу изменения в конфигурационный файл, добавив в раздел по умолчанию игнорирование адреса клиента (рис. 10).

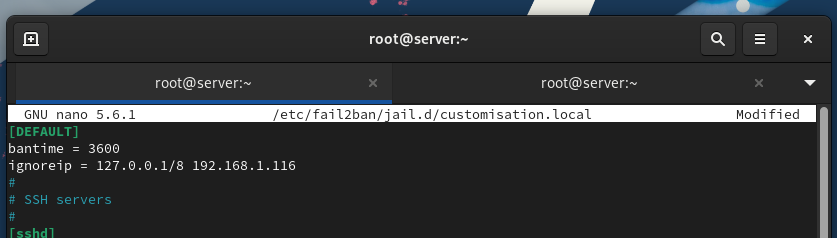


Рис. 10: Редактирование файла c локальной конфигурацией: игнорирование адреса клиента

Перезапускаю службу и просматриваю журнал событий (рис. 11).

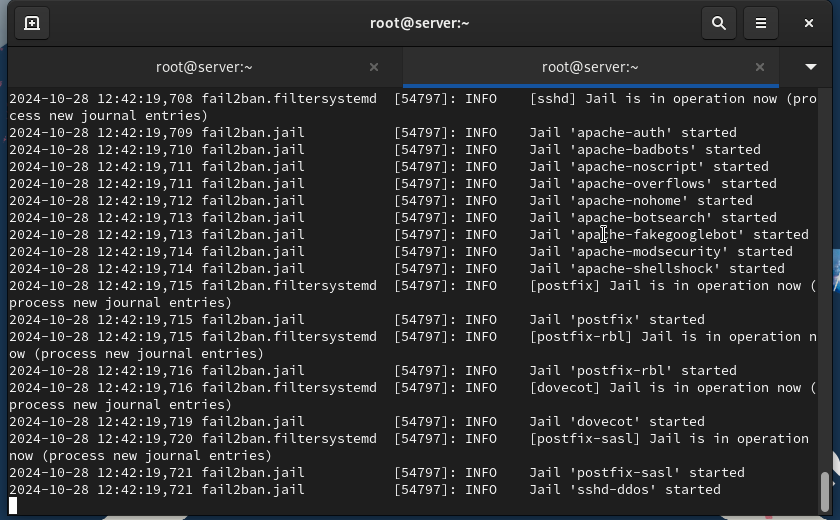


Рис. 11: Просмотр журнала событий `fail2ban’

С клиента вновь пытаюсь аналогичным образом войти на сервер с неправильным паролем. Просматриваю статус защиты SSH и вижу 0 заблокированных адресов, так как адрес клиента находится в списке игнорируемых (рис. 12)

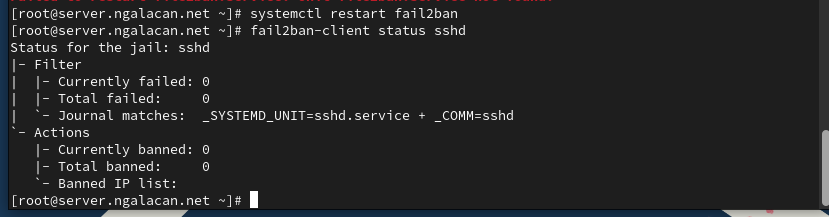


Рис. 12: Просмотр статуса защиты SSH после неудачного входа

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую 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/

Вношу изменения в файл /vagrant/provision/server/protect.sh (рис. 13).

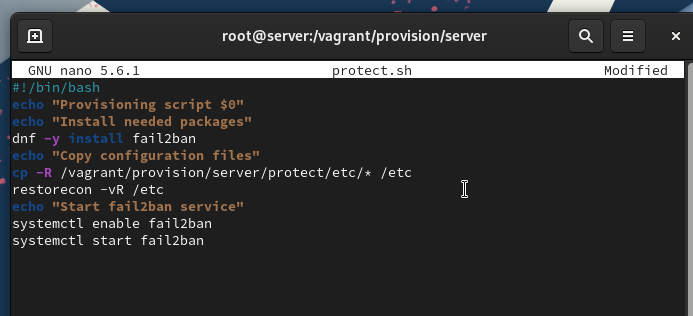


Рис. 13: Редактирование protect.sh на сервере

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

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

# 3 Выводы

В результате выполнения 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 - 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>