Лабораторная работа № 16

Базовая защита от атак типа «brute force

Демидова Екатерина Алексеевна

Содержание

# 1 Цель работы

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

# 2 Задание

1. Установите и настройте сервер Samba.
2. Настройте на клиенте доступ к разделяемым ресурсам.
3. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сервера Samba для доступа к разделяемым ресурсам во внутреннем окружении виртуальных машин server и client. Соответствующим образом необходимо внести изменения в Vagrantfile.

# 3 Выполнение лабораторной работы

## 3.1 Защита с помощью Fail2ban

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

cd /var/tmp/eademidova/vagrant

Затем запустим виртуальную машину server:

make server-up

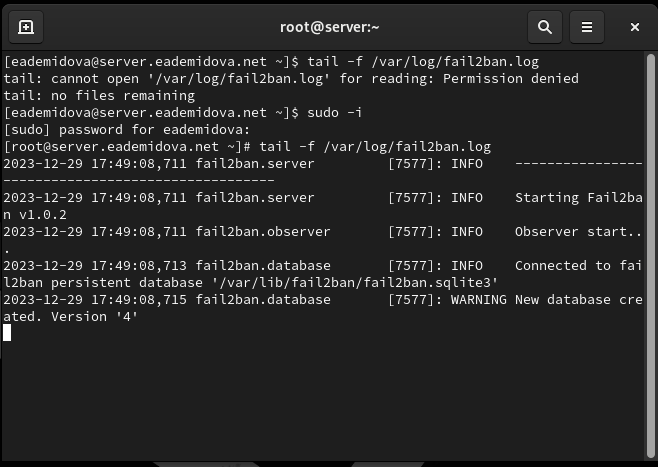
На сервере установите fail2ban:

dnf -y install fail2ban

Запустим сервер fail2ban:

systemctl start fail2ban  
systemctl enable fail2ban

В дополнительном терминале запустим просмотр журнала событий fail2ban(рис. ??):

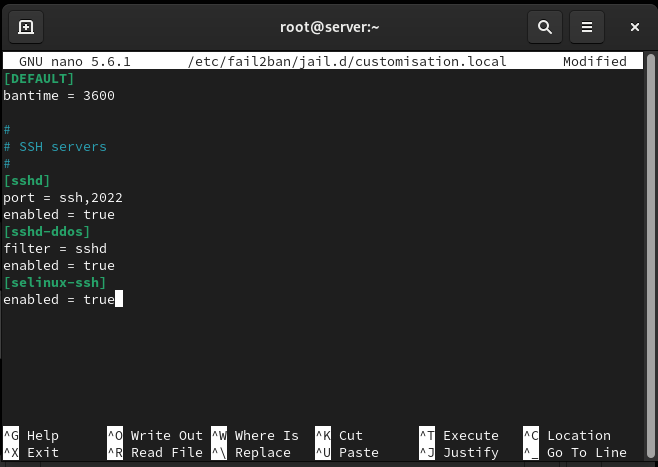


Запуск просмотра журнала событий fail2ban

Создадим файл с локальной конфигурацией fail2ban:

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

И в этом файле etc/fail2ban/jail.d/customisation.local зададим время блокирования на 1 час (время задаётся в секундах) и включим защиту SSH(рис. ??):

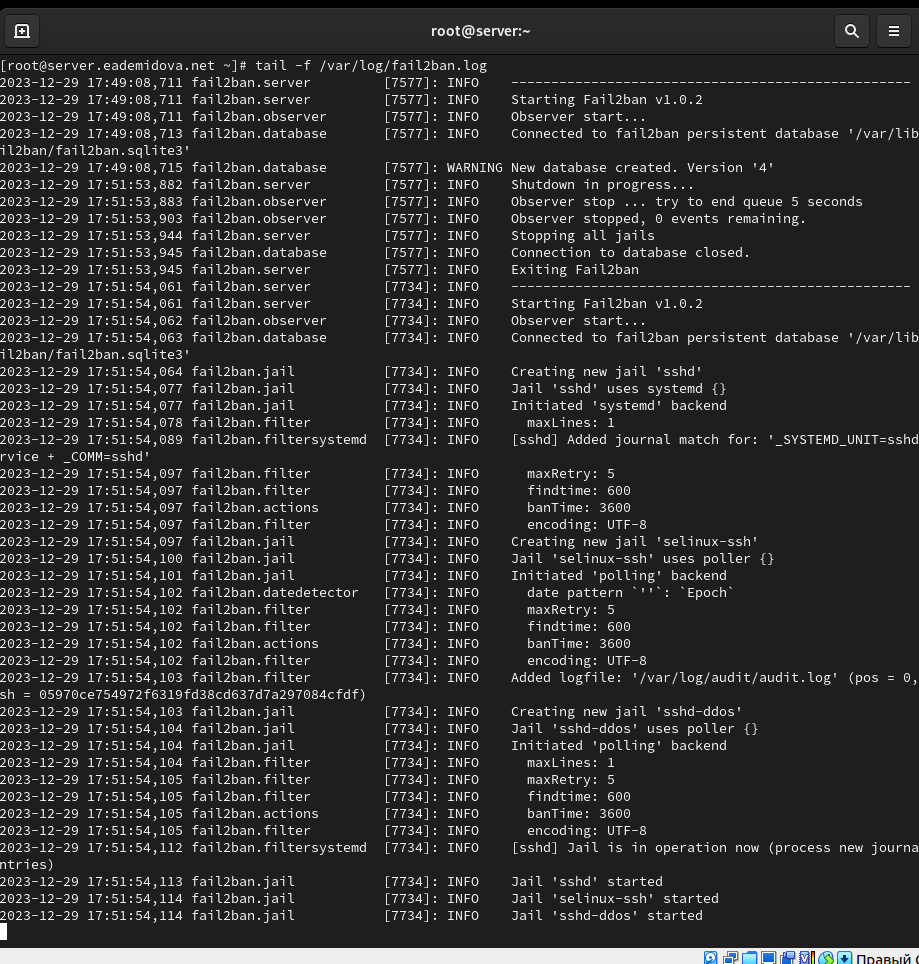


Добавление времени блокировкии и включение защиты SSH customisation.local

Перезапустим сервер fail2ban:

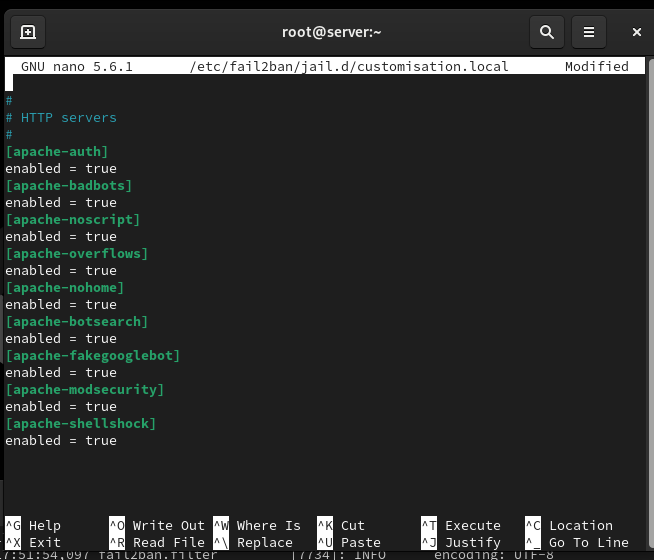
systemctl restart fail2ban

И посмотрим журнал событий(??):



Просмотр журнала событий fail2ban

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

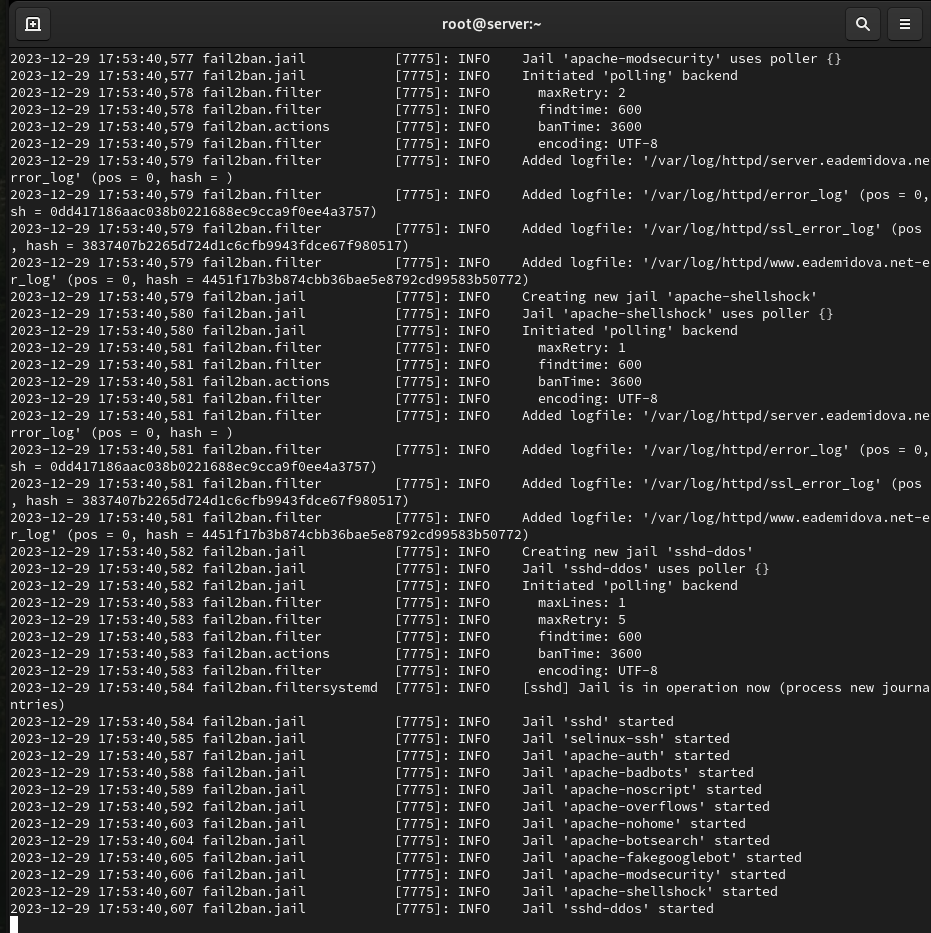


Включение защиты HTTP в файле customisation.local

Перезапустим сервер fail2ban:

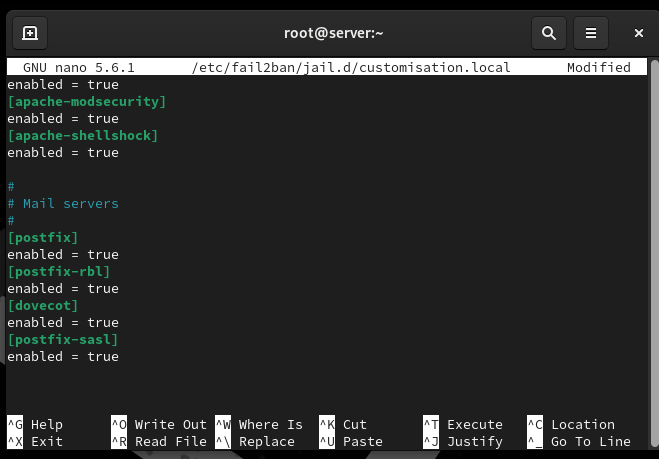
systemctl restart fail2ban

И посмотрим журнал событий(??):



Просмотр журнала событий fail2ban

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

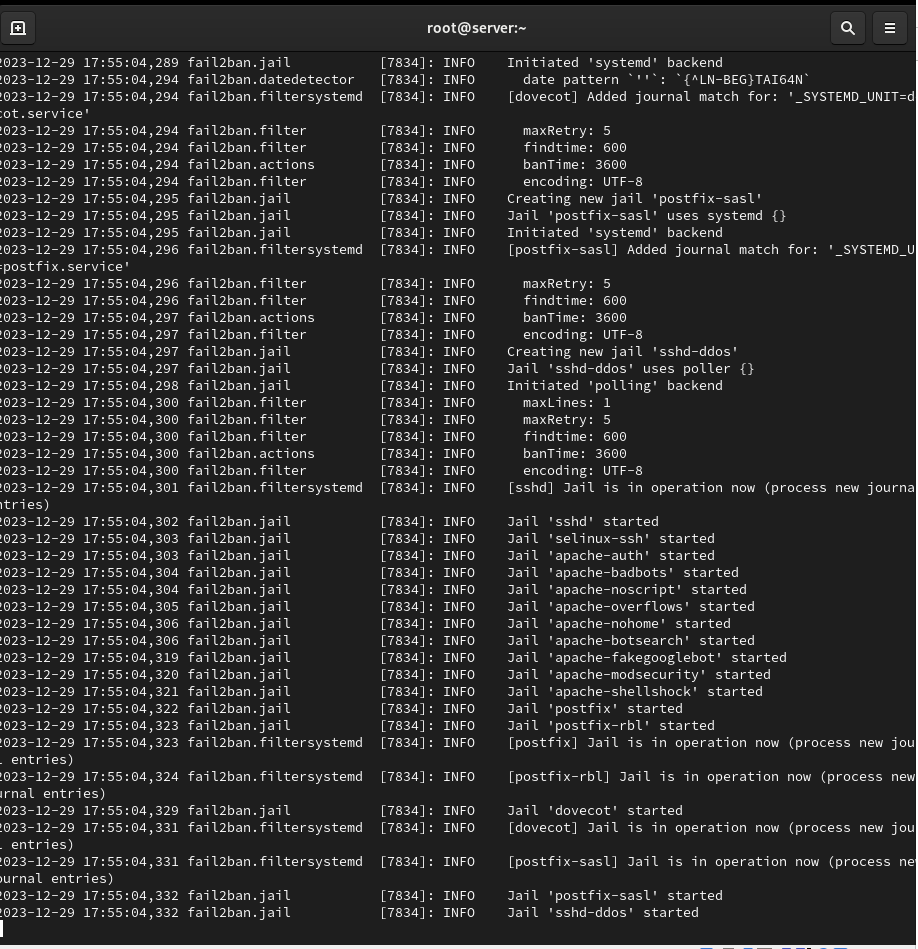


Включение защиты почты в файле customisation.local

Перезапустим сервер fail2ban:

systemctl restart fail2ban

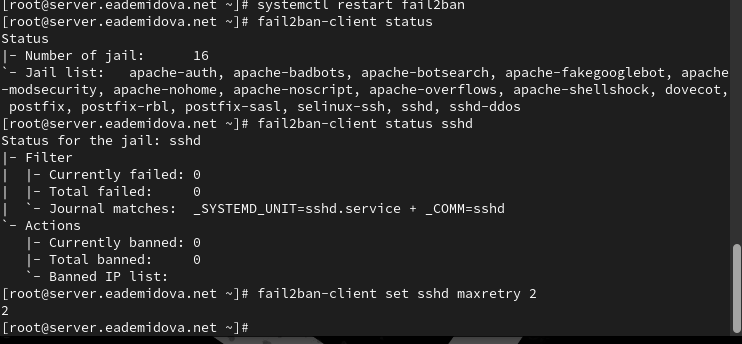
И посмотрим журнал событий(??):



Просмотр журнала событий fail2ban

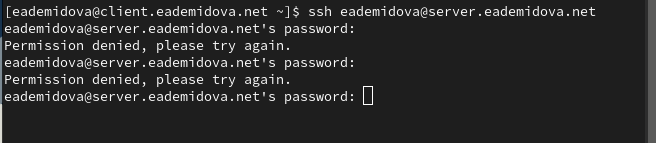
## 3.2 Проверка работы Fail2ban

На сервере посмотрим статус fail2ban и статус защиты SSH в fail2ban, а затем установим максимальное количество ошибок для SSH, равное 2(??):



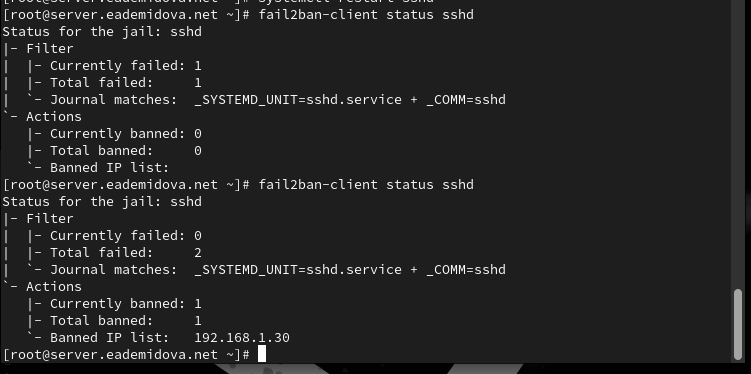
Просмотр статуса fail2ban, защиты SSH и установка количества ошибок для SSH

С клиента попытайтесь зайти по SSH на сервер с неправильным паролем(??):



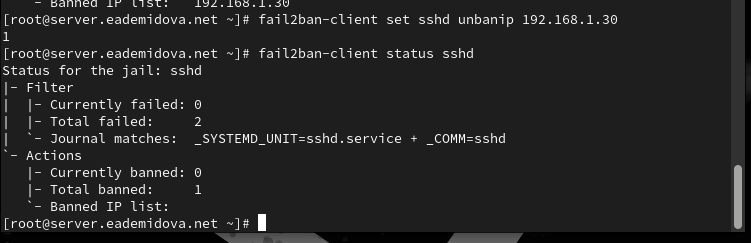
Попытки соединения по SSH с сервером с неправильным паролем

На сервере посмотрите статус защиты SSH, убедившись, что произошла блокировка адреса клиента(??):



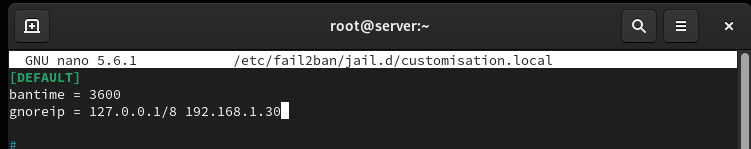
Проверка блокировки клиента на сервере

Разблокируем IP-адрес клиента и вновь посмотрим статус защиты SSH, убедившись, что блокировка с клиента снята(рис. ??):



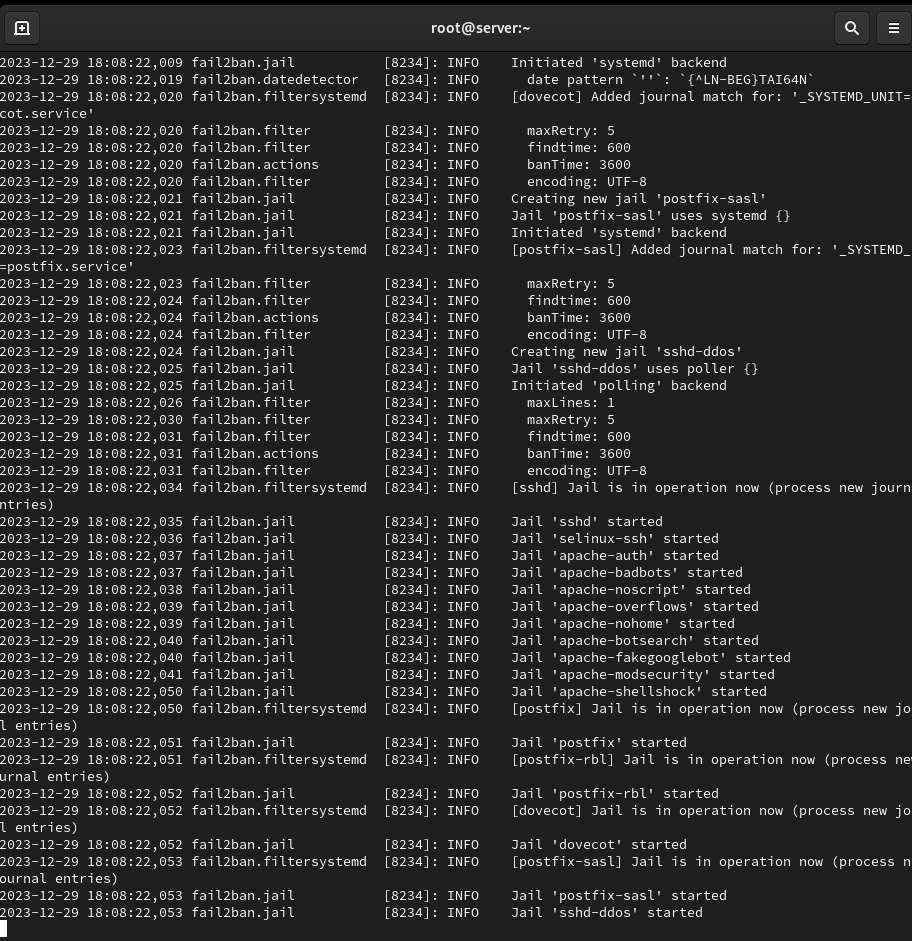
Снятие блокировки с клиента

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



Добавление в конфигурационный файл игнорирования адреса клиента

Перезапустим fail2ban и посмотрим журнал событий(??)



Просмотр журнала событий fail2ban

Вновь попытаемся войти с клиента на сервер с неправильным паролем и посмотрим статус защиты SSH(??):



Просмотр статусазащиты SSH после подключение к серверу с клиента по SSH с неправильным паролем

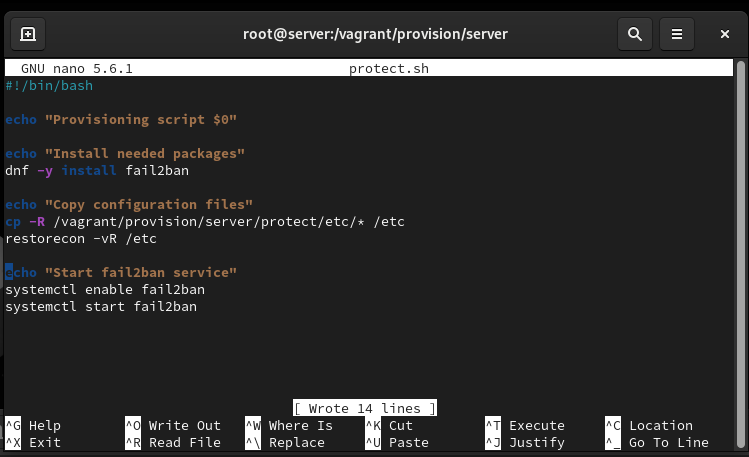
Теперь клиент не блокируется.

## 3.3 Внесение изменений в настройки внутреннего окружения виртуальных машины

На виртуальной машине server перейдем 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, а также создадим исполняемый файл protect.sh:

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/  
  
touch protect.sh  
chmod +x protect.sh

В каталоге /vagrant/provision/server создадим исполняемый файл smb.sh и внесем скрипт(??):



Скрипта файла /vagrant/provision/server/protect.sh

Затем для отработки созданных скриптов в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера:

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

# 4 Контрольные вопросы

1. Поясните принцип работы Fail2ban.
2. Настройки какого файла более приоритетны: jail.conf или jail.local?
3. Как настроить оповещение администратора при срабатывании Fail2ban?
4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.
5. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе.
6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в на- стройках Fail2ban?
7. Как получить список действующих правил Fail2ban?
8. Как получить статистику заблокированных Fail2ban адресов?
9. Как разблокировать IP-адрес?
10. 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.
11. Настройки файла jail.local более приоритетны, чем настройки файла jail.conf. Если в файле jail.local определены одни и те же параметры, они будут использованы вместо параметров из jail.conf.
12. 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 SMTP-сервера.
13. 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.
14. 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.
15. 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.
16. Для получения списка действующих правил Fail2ban можно использовать команду: fail2ban-client status.
17. Для получения статистики заблокированных адресов Fail2ban можно использовать команду: fail2ban-client status <jail-name>, где <jail-name> - имя конкретного jail, например, “ssh” или “apache”.
18. Разблокировать адрес момжно с помощью следующей команды

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

# 5 Выводы

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