Отчет по лабораторной работе №16

Дисциплина: Администрирование сетевых подсистем

Иванов Сергей Владимирович

Содержание

1 Цель работы **4**

2 Задание **5**

3 Выполнение лабораторной работы **6**
3.1 Защита с помощью Fail2ban 6
3.2 Проверка работы Fail2ban 12
3.3 Внесение изменений в настройки внутреннего окружения виртуальных машин 15

4 Ответы на контрольные вопросы **17**

5 Выводы **20**

Список иллюстраций

3.1 Запуск Server 6
3.2 Установка fail2ban 6
3.3 Запуск fail2ban 7
3.4 Запуск журнала событий 7
3.5 Создание конфигурации 8
3.6 Перезапуск fail2ban 8
3.7 Просмотр журнала событий 8
3.8 Редактирование конф. файла 10
3.9 Перезапуск службы и просмотр журнала 10
3.10 Редактирование конф. файла 11
3.11 Перезапуск службы и просмотр журнала 12
3.12 Просмотр статуса службы 12
3.13 Просмотр статуса защиты SSH 12
3.14 Установка макс. кол-ва ошибок 12
3.15 Запуск Client 13
3.16 Попытка зайти по ssh с клиента 13
3.17 Блокировка адреса клиаента 13
3.18 Разблокировка клиента 13
3.19 Редактирование конф. файла 14
3.20 Перезапуск службы и просмотр журнала 14
3.21 Попытка входа 14
3.22 Статус защиты 15
3.23 Создание директорий и копирование конф. файлов 15
3.24 Создание скрипта 16
3.25 Редактирование Vagrantfile 16

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 Fail2ban для отслеживания работы установленных на сервере служб (см. раздел 16.4.1).
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH (см. раздел 16.4.2).
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban (см. раздел 16.4.3).

3 Выполнение лабораторной работы

3.1 Защита с помощью Fail2ban

Запускаю виртуальную машину Server. (рис. 1)

```
C:\Users\1serg>cd C:\work_asp\svivanov\vagrant

C:\work_asp\svivanov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
```

Рис. 3.1: Запуск Server

На сервере установим fail2ban: dnf -y install fail2ban (рис. 2)

```
[root@server.svivanov.net ~]# dnf install fail2ban
Extra Packages for Enterprise Linux 10 - x86_64                  679 kB/s | 5.5 MB     00:08
Last metadata expiration check: 0:00:01 ago on Сб 06 дек 2025 10:53:29.
Dependencies resolved.
================================================================================
 Package                Architecture      Version                Repository     Size
================================================================================
Installing:
 fail2ban               noarch            1.1.0-6.el10_0         epel          9.4 k
Installing dependencies:
 fail2ban-firewalld     noarch            1.1.0-6.el10_0         epel          9.6 k
 fail2ban-selinux       noarch            1.1.0-6.el10_0         epel           31 k
 fail2ban-sendmail      noarch            1.1.0-6.el10_0         epel           12 k
 fail2ban-server        noarch            1.1.0-6.el10_0         epel          561 k

Transaction Summary
================================================================================
Install  5 Packages
```

Рис. 3.2: Установка fail2ban

Запустим сервер fail2ban:

systemctl start fail2ban

systemctl enable fail2ban (рис. 3)

Рис. 3.3: Запуск fail2ban

В дополнительном терминале запустим просмотр журнала событий fail2ban: tail -f /var/log/fail2ban.log (рис. 4)

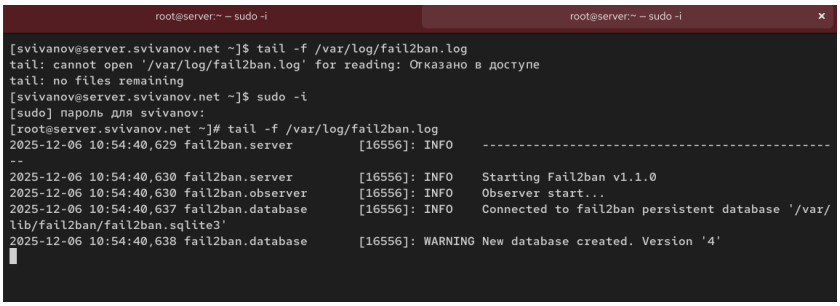

Рис. 3.4: Запуск журнала событий

Создадим файл с локальной конфигурацией fail2ban:

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

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

(a) зададим время блокирования на 1 час (время задаётся в секундах): (рис. 5)

```
[DEFAULT]
bantime = 3600
(b) включите защиту SSH:
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
```

```
enabled = true

[selinux-ssh]

enabled = true
```

Рис. 3.5: Создание конфигурации

Перезапустим fail2ban: systemctl restart fail2ban. (рис. 6)

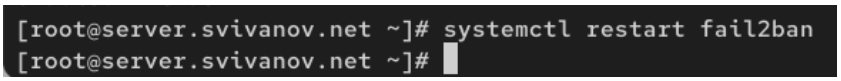

Рис. 3.6: Перезапуск fail2ban

Посмотрим журнал событий: tail -f /var/log/fail2ban.log (рис. 7)

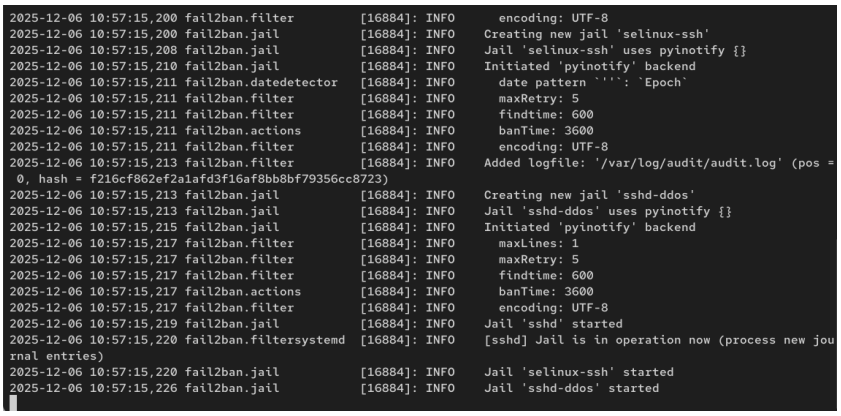

Рис. 3.7: Просмотр журнала событий

В файле /etc/fail2ban/jail.d/customisation.local включим защиту HTTP: (рис. 8)

```
#
# HTTP servers
#
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-noscript]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botsearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
112 Лабораторная работа № 16
[apache-shellshock]
enabled = true
```

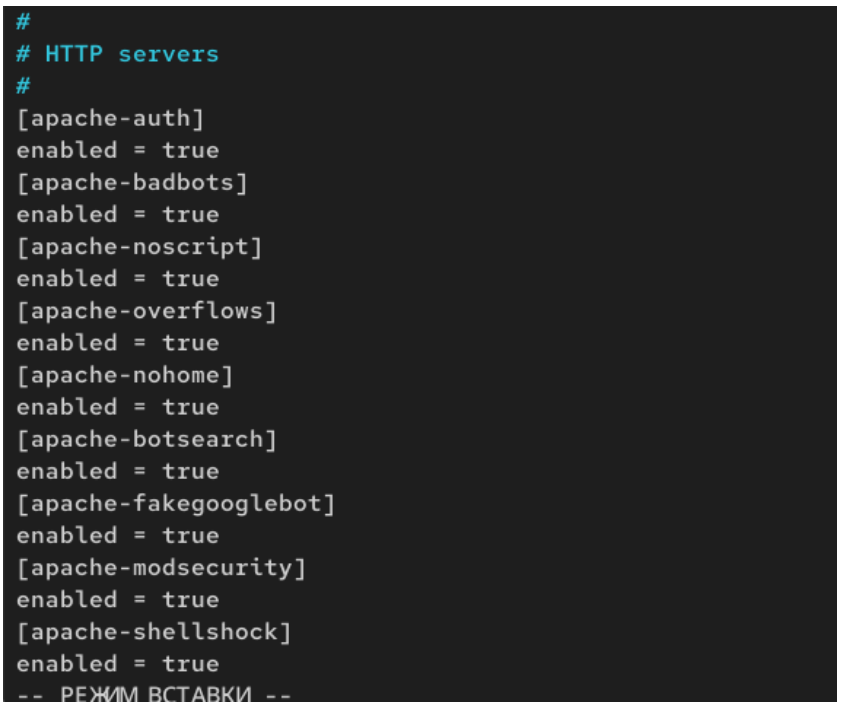

Рис. 3.8: Редактирование конф. файла

Перезапустим fail2ban: systemctl restart fail2ban. Посмотрим журнал событий: tail -f /var/log/fail2ban.log (рис. 9)

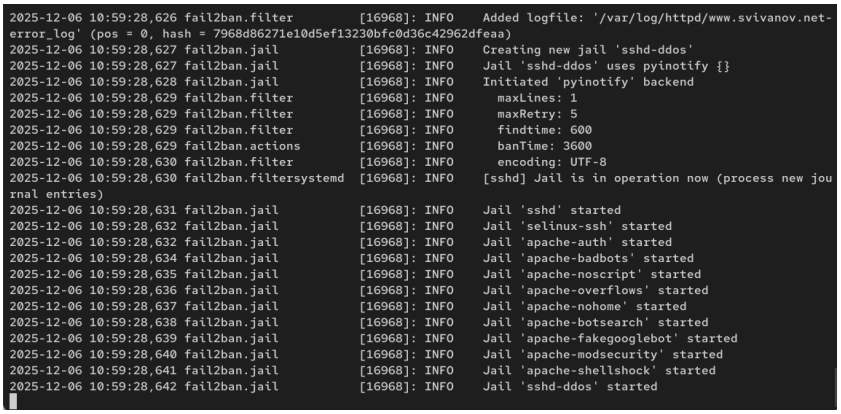

Рис. 3.9: Перезапуск службы и просмотр журнала

В файле /etc/fail2ban/jail.d/customisation.local включим защиту почты: (рис. 10)

#

```
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```

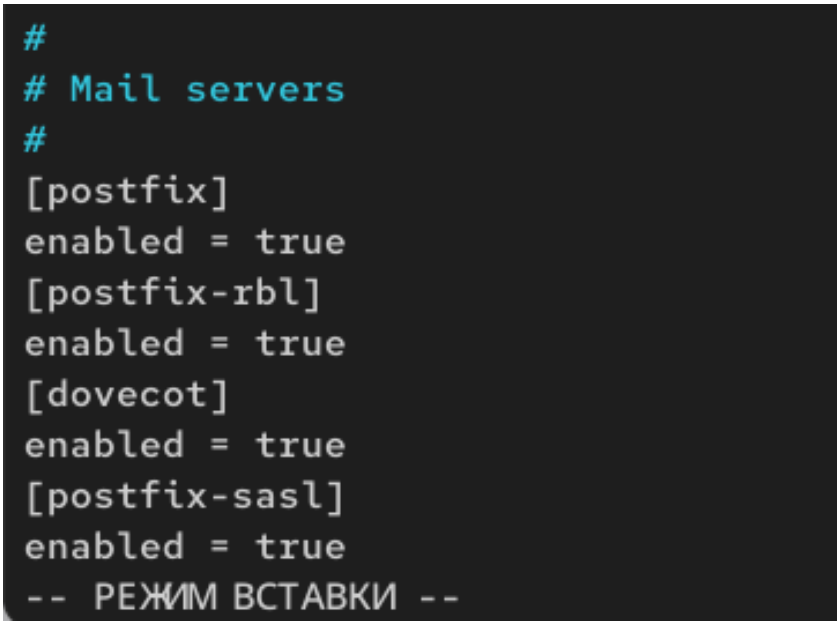

Рис. 3.10: Редактирование конф. файла

Перезапустим fail2ban: systemctl restart fail2ban. Посмотрим журнал событий: tail -f /var/log/fail2ban.log (рис. 11)

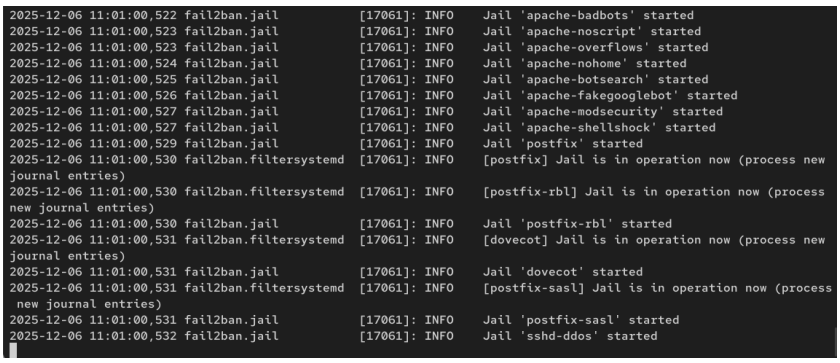

Рис. 3.11: Перезапуск службы и просмотр журнала

3.2 Проверка работы Fail2ban

На сервере посмотрим статус fail2ban: fail2ban-client status (рис. 12)

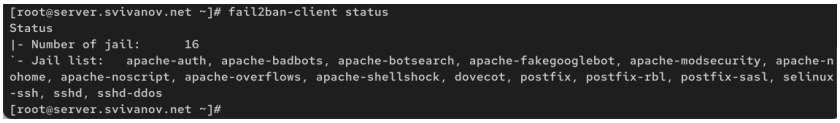

Рис. 3.12: Просмотр статуса службы

Посмотрим статус защиты SSH в fail2ban: fail2ban-client status sshd (рис. 13)

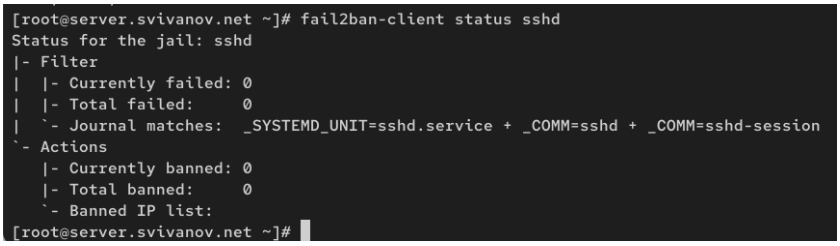

Рис. 3.13: Просмотр статуса защиты SSH

Установим максимальное количество ошибок для SSH, равное 2: fail2ban-client set sshd maxretry 2 (рис. 14)

Рис. 3.14: Установка макс. кол-ва ошибок

Запускаю виртуальную машину Client. (рис. 15)

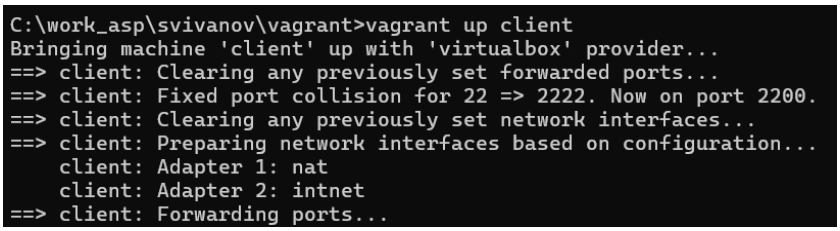

Рис. 3.15: Запуск Client

С клиента попытаемся зайти по SSH на сервер с неправильным паролем. (рис. 16)

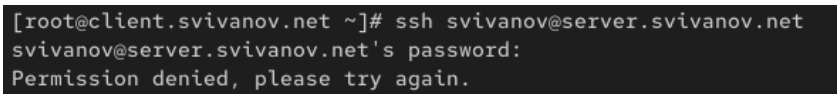

Рис. 3.16: Попытка зайти по ssh с клиента

На сервере посмотрим статус защиты SSH: fail2ban-client status sshd. Убеждаюсь, что произошла блокировка адреса клиента. (рис. 17)

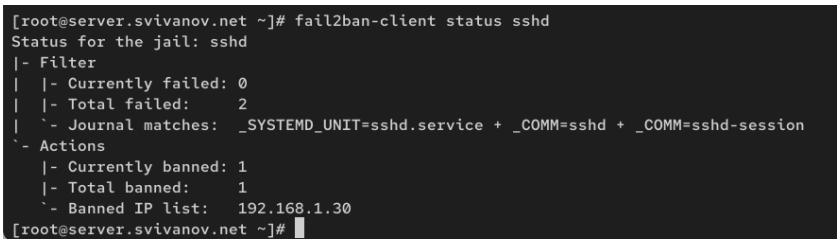

Рис. 3.17: Блокировка адреса клиаента

Разблокируем IP-адрес клиента: fail2ban-client set sshd unbanip . Вновь посмотрим статус защиты SSH: fail2ban-client status sshd (рис. 18)

Рис. 3.18: Разблокировка клиента

На сервере внесем изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.lo
добавив в раздел по умолчанию игнорирование адреса клиента: (рис. 19)

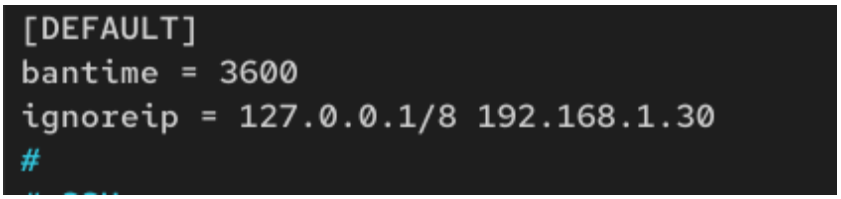

Рис. 3.19: Редактирование конф. файла

Перезапустим fail2ban. Посмотрим журнал событий: tail -f /var/log/fail2ban.log
(рис. 20)

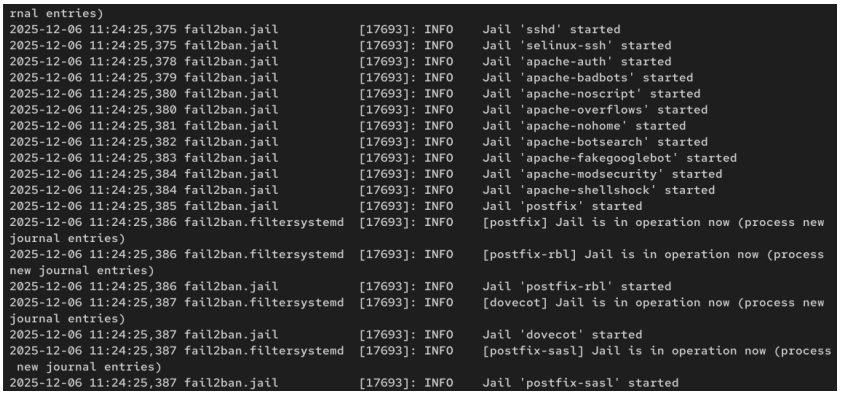

Рис. 3.20: Перезапуск службы и просмотр журнала

Вновь попытаемся войти с клиента на сервер с неправильным паролем и посмотрим статус защиты SSH. Видим, что клиент игнорируется, как и предполагалось. (рис. 21, 22)

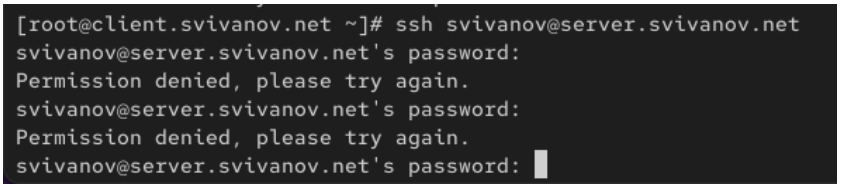

Рис. 3.21: Попытка входа

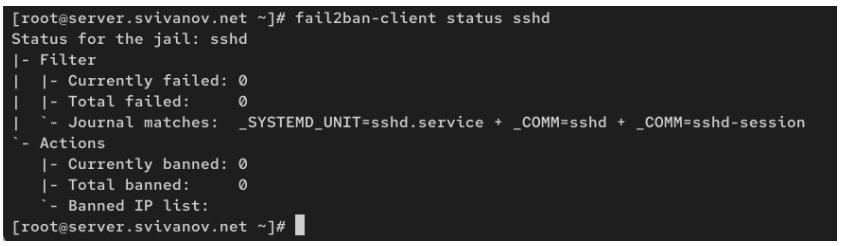

Рис. 3.22: Статус защиты

3.3 Внесение изменений в настройки внутреннего окружения виртуальных машин

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 соответствующие подкаталоги конфигурационные файлы: (рис. 23)

```
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/
```

Рис. 3.23: Создание директорий и копирование конф. файлов

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

```
cd /vagrant/provision/server
touch protect.sh
chmod +x protect.sh
```

Открыв его на редактирование, пропишем в нём следующий скрипт: (рис. 24)

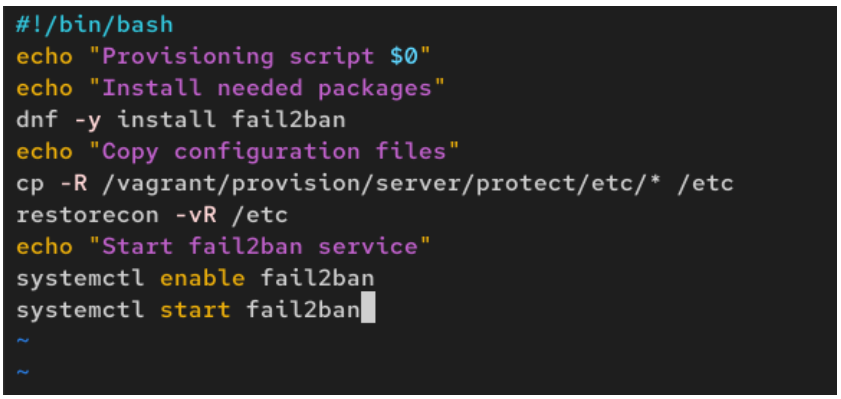

Рис. 3.24: Создание скрипта

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера: (рис. 25)

```
server.vm.provision "server protect",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/protect.sh"
```

Рис. 3.25: Редактирование Vagrantfile

4 Ответы на контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban - это система предотвращения атак типа «brute force» путем мониторинга лог-файлов служб (например, SSH, Apache, Postfix). При обнаружении подозрительной активности (например, множественных неудачных попыток входа) система добавляет IP-адрес нарушителя в черный список и блокирует его с помощью правил межсетевого экрана (например, iptables). После истечения заданного времени блокировки адрес автоматически разблокируется.

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

Настройки в файле jail.local имеют более высокий приоритет, чем в jail.conf. Это позволяет изменять конфигурацию без редактирования основного файла, что упрощает обновление системы и предотвращает потерю настроек при обновлении пакета Fail2ban.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Для отправки уведомлений администратору при срабатывании Fail2ban необходимо настроить параметры в секции `[DEFAULT]` файла конфигурации (например, /etc/fail2ban/jail.local):

```
[DEFAULT]
destemail = admin@example.com
sender = fail2ban@example.com
mta = sendmail
action = %(action_mwl)s
```

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

```
[apache-auth]
enabled  = false
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache2/*error.log
maxretry = 3
```

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

```
[postfix]
enabled  = false
port     = smtp,ssmtp
filter   = postfix
logpath  = /var/log/mail.log
maxretry = 3
```

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

Fail2ban может выполнять:

- Блокировка IP через iptables/nftables.
- Отправка email-уведомления.
- Выполнение пользовательского скрипта.
- Добавление IP в черный список DNSBL.

7. Как получить список действующих правил Fail2ban?

Выполнить команду:

fail2ban-client status

Для конкретной службы:

fail2ban-client status sshd

8. Как получить статистику заблокированных Fail2ban адресов?

Просмотреть статистику можно в журнале:

tail -f /var/log/fail2ban.log

Или с помощью команды:

fail2ban-client status

9. Как разблокировать IP-адрес?

fail2ban-client set unbanip

5 Выводы

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