

# **Отчёт по лабораторной работе 16**

**Базовая защита от атак типа brute force**

Элсаиед Адел

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение</b>	<b>6</b>
2.1	Защита сервера с использованием Fail2ban . . . . .	6
2.2	Проверка работы Fail2ban и автоматизация конфигурации . . . . .	12
2.3	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	16
<b>3</b>	<b>Вывод</b>	<b>18</b>
<b>4</b>	<b>Контрольные вопросы</b>	<b>19</b>

## Список иллюстраций

2.1	Просмотр журнала Fail2ban . . . . .	6
2.2	Создание файла customisation.local . . . . .	7
2.3	Журнал Fail2ban после включения SSH-защиты . . . . .	8
2.4	Настройка защиты HTTP . . . . .	9
2.5	Журнал Fail2ban после включения HTTP-защиты . . . . .	10
2.6	Настройка защиты почтовых сервисов . . . . .	11
2.7	Итоговый журнал Fail2ban . . . . .	12
2.8	Статус Fail2ban и список jail-модулей . . . . .	12
2.9	Статус SSH после разблокировки . . . . .	14
2.10	Добавление ignoreip в конфигурацию Fail2ban . . . . .	15
2.11	Игнорирование IP-адреса клиента . . . . .	15
2.12	Подготовка каталога protect и копирование конфигурации . . . . .	16
2.13	Скрипт автоматической настройки Fail2ban . . . . .	16

## **Список таблиц**

# 1 Цель работы

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

## 2 Выполнение

### 2.1 Защита сервера с использованием Fail2ban

1. На сервере выполнена установка средства защиты Fail2ban с использованием менеджера пакетов `dnf`. В результате выполнения команды `dnf -y install fail2ban` пакет Fail2ban был успешно установлен вместе со всеми необходимыми зависимостями.
2. После установки произведён запуск сервиса Fail2ban и добавление его в автозагрузку операционной системы. Команды `systemctl start fail2ban` и `systemctl enable fail2ban` обеспечили немедленный запуск службы и её автоматический старт при загрузке системы.
3. Для контроля работы Fail2ban в дополнительном терминале был запущен просмотр журнала событий с помощью команды `tail -f /var/log/fail2ban.log`. В журнале зафиксирован старт сервиса Fail2ban, инициализация наблюдателя и подключение к постоянной базе данных.

```
[elsaiedadel@server.elsaiedadel.net sambashare]$ sudo -i tail -f /var/log/fail2ban.log
[sudo] password for elsaiedadel:
2026-01-07 08:39:48,789 fail2ban.server [23375]: INFO -----
2026-01-07 08:39:48,789 fail2ban.server [23375]: INFO Starting Fail2ban v1.1.0
2026-01-07 08:39:48,790 fail2ban.observer [23375]: INFO Observer start...
2026-01-07 08:39:48,793 fail2ban.database [23375]: INFO Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2026-01-07 08:39:48,794 fail2ban.database [23375]: WARNING New database created. Version '4'
```

Рис. 2.1: Просмотр журнала Fail2ban

4. Для задания пользовательской конфигурации Fail2ban был создан локальный конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`.

Использование отдельного файла в каталоге `jail.d` позволяет сохранять пользовательские настройки при обновлении пакета.



Рис. 2.2: Создание файла `customisation.local`

5. В файле `/etc/fail2ban/jail.d/customisation.local` выполнена базовая настройка параметров Fail2ban. В секции `[DEFAULT]` задано время блокирования нарушителей `bantime = 3600`, что соответствует одному часу. Также включена защита службы SSH, включая стандартный демон `sshd`, дополнительную защиту от DDoS-атак `sshd-ddos` и модуль контроля событий SELinux `selinux-ssh`.
6. После внесения изменений выполнена перезагрузка сервиса Fail2ban. Перезапуск необходим для применения новых правил и активации настроенных jail-модулей.
7. В журнале `/var/log/fail2ban.log` зафиксировано создание и запуск jail-модулей `sshd`, `sshd-ddos` и `selinux-ssh`. Логи подтверждают успешную инициализацию фильтров, backend-механизмов и начало мониторинга журналов системы.

```

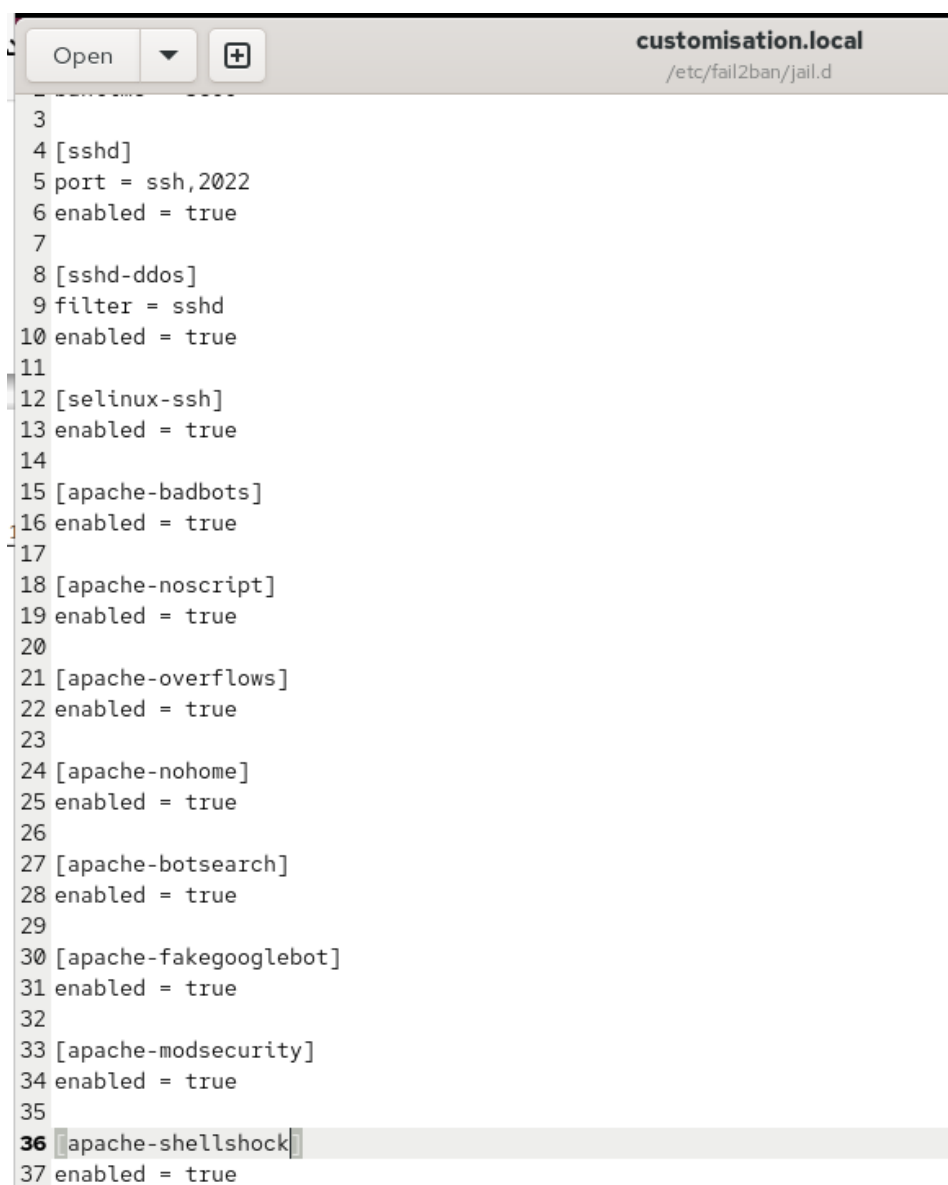
2026-01-07 08:42:41,730 fail2ban.server [24048]: INFO Starting Fail2ban v1.1.0
2026-01-07 08:42:41,730 fail2ban.observer [24048]: INFO Observer start...
2026-01-07 08:42:41,733 fail2ban.database [24048]: INFO Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2026-01-07 08:42:41,733 fail2ban.jail [24048]: INFO Creating new jail 'sshd'
2026-01-07 08:42:41,736 fail2ban.jail [24048]: INFO Jail 'sshd' uses systemd {}
2026-01-07 08:42:41,736 fail2ban.jail [24048]: INFO Initiated 'systemd' backend
2026-01-07 08:42:41,737 fail2ban.filter [24048]: INFO maxLines: 1
2026-01-07 08:42:41,741 fail2ban.filtersystemd [24048]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.s
ervice + _COMM=sshd + _COMM=sshd-session'
2026-01-07 08:42:41,741 fail2ban.filter [24048]: INFO maxRetry: 5
2026-01-07 08:42:41,741 fail2ban.filter [24048]: INFO findtime: 600
2026-01-07 08:42:41,741 fail2ban.actions [24048]: INFO banTime: 3600
2026-01-07 08:42:41,741 fail2ban.filter [24048]: INFO encoding: UTF-8
2026-01-07 08:42:41,741 fail2ban.jail [24048]: INFO Creating new jail 'selinux-ssh'
2026-01-07 08:42:41,744 fail2ban.jail [24048]: INFO Jail 'selinux-ssh' uses pyinotify {}
2026-01-07 08:42:41,744 fail2ban.jail [24048]: INFO Initiated 'pyinotify' backend
2026-01-07 08:42:41,745 fail2ban.datedetector [24048]: INFO date pattern '': 'Epoch'
2026-01-07 08:42:41,745 fail2ban.filter [24048]: INFO maxRetry: 5
2026-01-07 08:42:41,745 fail2ban.filter [24048]: INFO findtime: 600
2026-01-07 08:42:41,745 fail2ban.actions [24048]: INFO banTime: 3600
2026-01-07 08:42:41,745 fail2ban.filter [24048]: INFO encoding: UTF-8
2026-01-07 08:42:41,746 fail2ban.filter [24048]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0, h
ash = f8c1aeeca7e18a160e53b0659c09e9f813656be4)
2026-01-07 08:42:41,746 fail2ban.jail [24048]: INFO Creating new jail 'sshd-ddos'
2026-01-07 08:42:41,746 fail2ban.jail [24048]: INFO Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:42:41,747 fail2ban.jail [24048]: INFO Initiated 'pyinotify' backend
2026-01-07 08:42:41,748 fail2ban.filter [24048]: INFO maxLines: 1
2026-01-07 08:42:41,748 fail2ban.filter [24048]: INFO maxRetry: 5
2026-01-07 08:42:41,748 fail2ban.filter [24048]: INFO findtime: 600
2026-01-07 08:42:41,748 fail2ban.actions [24048]: INFO banTime: 3600
2026-01-07 08:42:41,748 fail2ban.filter [24048]: INFO encoding: UTF-8
2026-01-07 08:42:41,748 fail2ban.jail [24048]: INFO Jail 'sshd' started
2026-01-07 08:42:41,749 fail2ban.jail [24048]: INFO Jail 'selinux-ssh' started
2026-01-07 08:42:41,749 fail2ban.jail [24048]: INFO Jail 'sshd-ddos' started

```

Рис. 2.3: Журнал Fail2ban после включения SSH-защиты

8. Далее в файле `/etc/fail2ban/jail.d/customisation.local` была включена защита HTTP-сервера Apache. Активированы модули защиты от несанкционированных запросов, вредоносных ботов, попыток эксплуатации уязвимостей и атак типа Shellshock.





```
3
4 [sshd]
5 port = ssh,2022
6 enabled = true
7
8 [sshd-ddos]
9 filter = sshd
10 enabled = true
11
12 [selinux-ssh]
13 enabled = true
14
15 [apache-badbots]
16 enabled = true
17
18 [apache-noscript]
19 enabled = true
20
21 [apache-overflows]
22 enabled = true
23
24 [apache-nohome]
25 enabled = true
26
27 [apache-botsearch]
28 enabled = true
29
30 [apache-fakegooglebot]
31 enabled = true
32
33 [apache-modsecurity]
34 enabled = true
35
36 [apache-shellshock]
37 enabled = true
```

Рис. 2.4: Настройка защиты HTTP

9. После настройки HTTP-защиты выполнен повторный перезапуск Fail2ban. Сервис успешно перечитал конфигурацию и применил новые правила фильтрации для веб-сервера.
10. Анализ журнала Fail2ban показал успешный запуск jail-модулей apache-badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity и apache-shellshock,

что подтверждает корректную активацию защиты HTTP-сервиса.

```
0, hash = 666653b87fc18faa79b1a5cfd17ab8f0e8276044)
2026-01-07 08:45:11,751 fail2ban.filter [24450]: INFO Added logfile: '/var/log/httpd/www.elsaiedadel.net-er
ror_log' (pos = 0, hash = 666653b87fc18faa79b1a5cfd17ab8f0e8276044)
2026-01-07 08:45:11,751 fail2ban.filter [24450]: INFO Added logfile: '/var/log/httpd/server.elsaiedadel.net
-error_log' (pos = 0, hash = )
2026-01-07 08:45:11,752 fail2ban.jail [24450]: INFO Creating new jail 'sshd-ddos'
2026-01-07 08:45:11,752 fail2ban.jail [24450]: INFO Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:45:11,753 fail2ban.jail [24450]: INFO Initiated 'pyinotify' backend
2026-01-07 08:45:11,753 fail2ban.filter [24450]: INFO maxLines: 1
2026-01-07 08:45:11,753 fail2ban.filter [24450]: INFO maxRetry: 5
2026-01-07 08:45:11,753 fail2ban.filter [24450]: INFO findtime: 600
2026-01-07 08:45:11,753 fail2ban.actions [24450]: INFO banTime: 3600
2026-01-07 08:45:11,753 fail2ban.filter [24450]: INFO encoding: UTF-8
2026-01-07 08:45:11,754 fail2ban.jail [24450]: INFO Jail 'sshd' started
2026-01-07 08:45:11,754 fail2ban.filtersystemd [24450]: INFO [sshd] Jail is in operation now (process new journal
entries)
2026-01-07 08:45:11,754 fail2ban.jail [24450]: INFO Jail 'selinux-ssh' started
2026-01-07 08:45:11,756 fail2ban.jail [24450]: INFO Jail 'apache-badbots' started
2026-01-07 08:45:11,757 fail2ban.jail [24450]: INFO Jail 'apache-noscript' started
2026-01-07 08:45:11,758 fail2ban.jail [24450]: INFO Jail 'apache-overflows' started
2026-01-07 08:45:11,758 fail2ban.jail [24450]: INFO Jail 'apache-nohome' started
2026-01-07 08:45:11,759 fail2ban.jail [24450]: INFO Jail 'apache-botsearch' started
2026-01-07 08:45:11,759 fail2ban.jail [24450]: INFO Jail 'apache-fakegooglebot' started
2026-01-07 08:45:11,761 fail2ban.jail [24450]: INFO Jail 'apache-modsecurity' started
2026-01-07 08:45:11,761 fail2ban.jail [24450]: INFO Jail 'apache-shellshock' started
2026-01-07 08:45:11,762 fail2ban.jail [24450]: INFO Jail 'sshd-ddos' started
```

Рис. 2.5: Журнал Fail2ban после включения HTTP-защиты

11. На заключительном этапе в файле `/etc/fail2ban/jail.d/customisation.local` была включена защита почтовых сервисов. Активированы jail-модули для сервисов postfix, postfix-rbl, dovecot и postfix-sasl, обеспечивающие защиту от атак на SMTP- и IMAP/POP3-службы.

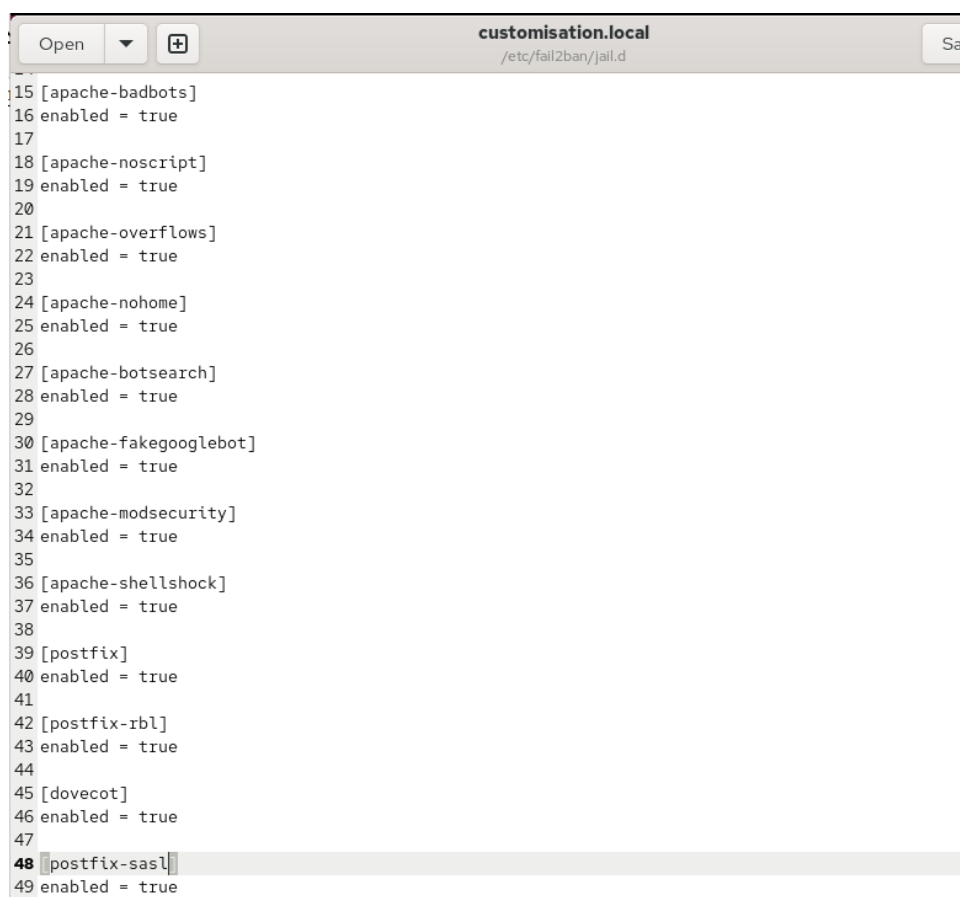


Рис. 2.6: Настройка защиты почтовых сервисов

12. После внесения изменений выполнен очередной перезапуск Fail2ban. Сервис успешно применил конфигурацию и инициировал мониторинг журналов почтовых служб.
13. В журнале событий Fail2ban подтверждён запуск всех настроенных jail-модулей, включая SSH, HTTP и почтовые сервисы. Fail2ban функционирует в штатном режиме и осуществляет защиту сервера от попыток несанкционированного доступа.

```

2026-01-07 08:46:46,104 fail2ban.jail [24734]: INFO Creating new jail 'sshd-ddos'
2026-01-07 08:46:46,104 fail2ban.jail [24734]: INFO Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:46:46,105 fail2ban.jail [24734]: INFO Initiated 'pyinotify' backend
2026-01-07 08:46:46,105 fail2ban.filter [24734]: INFO maxLines: 1
2026-01-07 08:46:46,106 fail2ban.filter [24734]: INFO maxRetry: 5
2026-01-07 08:46:46,106 fail2ban.filter [24734]: INFO findtime: 600
2026-01-07 08:46:46,106 fail2ban.actions [24734]: INFO banTime: 3600
2026-01-07 08:46:46,106 fail2ban.filter [24734]: INFO encoding: UTF-8
2026-01-07 08:46:46,106 fail2ban.jail [24734]: INFO Jail 'sshd' started
2026-01-07 08:46:46,106 fail2ban.filtersystemd [24734]: INFO [sshd] Jail is in operation now (process new journal
entries)
2026-01-07 08:46:46,107 fail2ban.jail [24734]: INFO Jail 'selinux-ssh' started
2026-01-07 08:46:46,107 fail2ban.jail [24734]: INFO Jail 'apache-badbots' started
2026-01-07 08:46:46,108 fail2ban.jail [24734]: INFO Jail 'apache-noscript' started
2026-01-07 08:46:46,108 fail2ban.jail [24734]: INFO Jail 'apache-overflows' started
2026-01-07 08:46:46,109 fail2ban.jail [24734]: INFO Jail 'apache-nohome' started
2026-01-07 08:46:46,109 fail2ban.jail [24734]: INFO Jail 'apache-botsearch' started
2026-01-07 08:46:46,109 fail2ban.jail [24734]: INFO Jail 'apache-fakegooglebot' started
2026-01-07 08:46:46,110 fail2ban.jail [24734]: INFO Jail 'apache-modsecurity' started
2026-01-07 08:46:46,110 fail2ban.jail [24734]: INFO Jail 'apache-shellshock' started
2026-01-07 08:46:46,110 fail2ban.jail [24734]: INFO Jail 'postfix' started
2026-01-07 08:46:46,110 fail2ban.jail [24734]: INFO Jail 'postfix-rbl' started
2026-01-07 08:46:46,111 fail2ban.filtersystemd [24734]: INFO [dovecot] Jail is in operation now (process new journa
l entries)
2026-01-07 08:46:46,112 fail2ban.filtersystemd [24734]: INFO [postfix-rbl] Jail is in operation now (process new j
ournal entries)
2026-01-07 08:46:46,112 fail2ban.jail [24734]: INFO Jail 'dovecot' started
2026-01-07 08:46:46,112 fail2ban.filtersystemd [24734]: INFO [postfix] Jail is in operation now (process new journa
l entries)
2026-01-07 08:46:46,112 fail2ban.jail [24734]: INFO Jail 'postfix-sasl' started
2026-01-07 08:46:46,113 fail2ban.filtersystemd [24734]: INFO [postfix-sasl] Jail is in operation now (process new
journal entries)
2026-01-07 08:46:46,113 fail2ban.jail [24734]: INFO Jail 'sshd-ddos' started

```

Рис. 2.7: Итоговый журнал Fail2ban

## 2.2 Проверка работы Fail2ban и автоматизация конфигурации

1. На сервере выполнена проверка общего состояния Fail2ban с использованием клиента управления. В результате анализа статуса подтверждено, что сервис активен, а также отображён список всех задействованных jail-модулей, включающих защиту SSH, HTTP и почтовых сервисов.

```

[root@server.elsaiedadel.net server]#
[root@server.elsaiedadel.net server]# fail2ban-client status
Status
|- Number of jail:      15
|- Jail list:  apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.elsaiedadel.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
'- Actions
  |- Currently banned: 0
  |- Total banned:    0
  '- Banned IP list:
[root@server.elsaiedadel.net server]# fail2ban-client set sshd maxretry 2
2
[root@server.elsaiedadel.net server]#

```

Рис. 2.8: Статус Fail2ban и список jail-модулей

2. Выполнена проверка состояния защиты SSH. Полученная информация показала отсутствие неудачных попыток аутентификации и заблокированных адресов на момент проверки, что свидетельствует о корректной работе jail-модуля sshd.
3. Для демонстрации работы механизма блокировки было изменено максимальное количество допустимых ошибок аутентификации для SSH до значения 2. Данное ограничение позволяет ускорить срабатывание Fail2ban при подборе пароля.
4. С клиентской машины выполнены попытки подключения к серверу по SSH с заведомо неверным паролем. В результате превышения допустимого количества ошибок Fail2ban зафиксировал нарушение и применил санкции к IP-адресу клиента.
5. Повторная проверка статуса jail-модуля sshd показала наличие одного заблокированного IP-адреса. В журнале отражено увеличение счётчиков неудачных попыток и факт применения блокировки.
6. Для восстановления доступа выполнена ручная разблокировка IP-адреса клиента. После выполнения операции блокировка была снята.
7. Повторный просмотр статуса защиты SSH подтвердил отсутствие активных блокировок, при этом общее количество ранее применённых санкций сохранено в статистике Fail2ban.

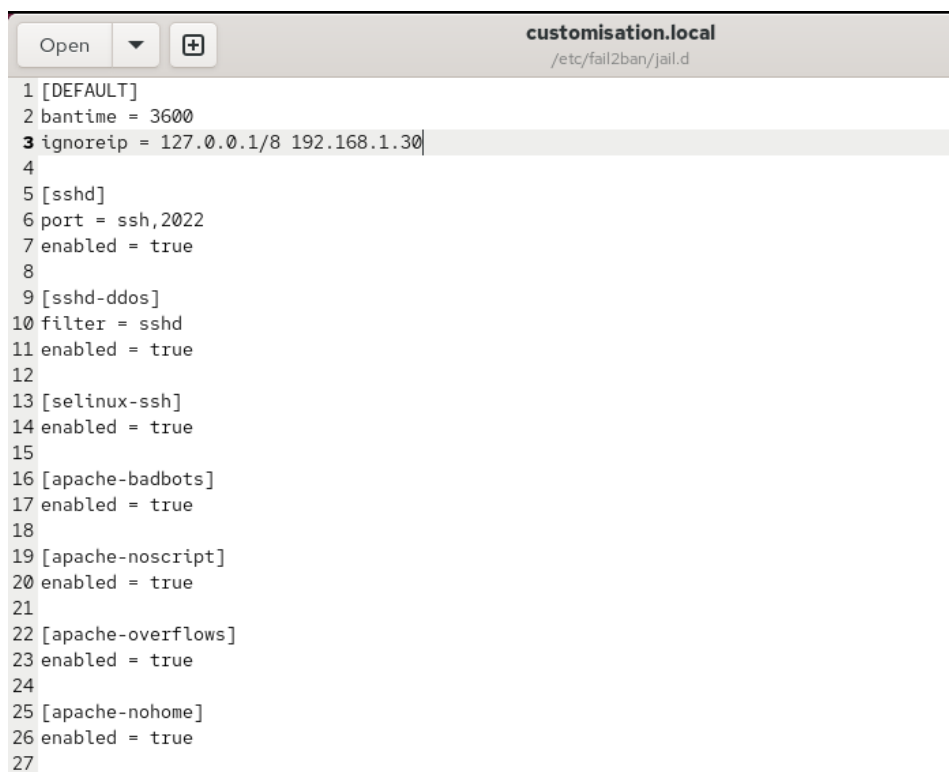
```

[root@server.elsaiedadel.net server]#
[root@server.elsaiedadel.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.1.30
[root@server.elsaiedadel.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.elsaiedadel.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned: 1
   `-- Banned IP list:
[root@server.elsaiedadel.net server]# █

```

Рис. 2.9: Статус SSH после разблокировки

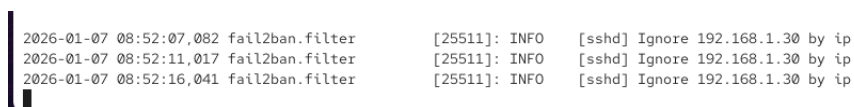
8. Для исключения ложных срабатываний в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local` внесено изменение. В секции `[DEFAULT]` добавлен параметр `ignoreip`, включающий локальный адрес и IP-адрес клиента, что исключает его из обработки Fail2ban.



```
1 [DEFAULT]
2 bantime = 3600
3 ignoreip = 127.0.0.1/8 192.168.1.30
4
5 [sshd]
6 port = ssh,2022
7 enabled = true
8
9 [sshd-ddos]
10 filter = sshd
11 enabled = true
12
13 [selinux-ssh]
14 enabled = true
15
16 [apache-badbots]
17 enabled = true
18
19 [apache-noscript]
20 enabled = true
21
22 [apache-overflows]
23 enabled = true
24
25 [apache-nohome]
26 enabled = true
27
```

Рис. 2.10: Добавление ignoreip в конфигурацию Fail2ban

9. После внесения изменений выполнен перезапуск Fail2ban для применения обновлённой конфигурации.
10. Анализ журнала событий Fail2ban показал, что попытки аутентификации с IP-адреса клиента игнорируются, что подтверждает корректность настройки параметра ignoreip.



```
2026-01-07 08:52:07,082 fail2ban.filter [25511]: INFO [sshd] Ignore 192.168.1.30 by ip
2026-01-07 08:52:11,017 fail2ban.filter [25511]: INFO [sshd] Ignore 192.168.1.30 by ip
2026-01-07 08:52:16,041 fail2ban.filter [25511]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рис. 2.11: Игнорирование IP-адреса клиента

11. Повторные попытки подключения по SSH с неверным паролем не приводят к блокировке клиента. Проверка статуса защиты SSH подтверждает отсутствие применённых санкций.

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

12. На виртуальной машине `server` выполнен переход в каталог `/vagrant/provision/server`, предназначенный для хранения provisioning-скриптов. Создан каталог `protect` с необходимой иерархией подкаталогов для размещения конфигурационных файлов Fail2ban. В созданный каталог скопирован файл пользовательской конфигурации `customisation.local`.

```
[root@server.elsaiedadel.net server]# cd /vagrant/provision/server/
[root@server.elsaiedadel.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.elsaiedadel.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect
/etc/fail2ban/jail.d/
[root@server.elsaiedadel.net server]# touch protect.sh
[root@server.elsaiedadel.net server]# chmod +x protect.sh
[root@server.elsaiedadel.net server]#
```

Рис. 2.12: Подготовка каталога `protect` и копирование конфигурации

13. В каталоге `/vagrant/provision/server` создан исполняемый файл `protect.sh`, предназначенный для автоматической установки и настройки Fail2ban при запуске виртуальной машины.
14. В файл `protect.sh` добавлен provisioning-скрипт, выполняющий установку Fail2ban, копирование конфигурационных файлов в системный каталог `/etc`, восстановление контекстов SELinux и запуск сервиса Fail2ban с добавлением в автозагрузку.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install fail2ban
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/protect/etc/* /etc
7  restorecon -vR /etc
8  echo "Start fail2ban service"
9  systemctl enable fail2ban
10 systemctl start fail2ban
11
```

Рис. 2.13: Скрипт автоматической настройки Fail2ban



15. Для автоматического выполнения созданного скрипта при загрузке виртуальной машины в конфигурационный файл `Vagrantfile` добавлена секция `provisioning` с указанием пути к скрипту `protect.sh`. Это обеспечивает воспроизводимую настройку защиты сервера при каждом развёртывании окружения.

## 3 Вывод

В ходе выполнения лабораторной работы была реализована защита сервера от несанкционированного доступа с использованием средства Fail2ban. Выполнена установка и запуск сервиса, произведена настройка локальной конфигурации с заданием времени блокировки, включением защиты для служб SSH, HTTP и почтовых сервисов. Проведена проверка корректности работы Fail2ban путём имитации атак с клиента, подтверждена блокировка IP-адреса при превышении допустимого количества ошибок аутентификации, а также выполнена ручная разблокировка адреса. Дополнительно настроено игнорирование доверенного IP-адреса и реализована автоматизация конфигурации Fail2ban с использованием provisioning-скрипта Vagrant. Результаты работы подтверждают корректное функционирование Fail2ban и эффективность его применения для повышения безопасности серверной системы.

## 4 Контрольные вопросы

### 1. Поясните принцип работы Fail2ban.

Fail2ban осуществляет мониторинг журналов системных и сетевых служб, анализируя записи на наличие признаков атак, таких как многократные неудачные попытки аутентификации. При обнаружении подозрительной активности Fail2ban применяет заранее настроенные действия, чаще всего временную блокировку IP-адреса атакующего с использованием механизмов межсетевого экранирования.

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

Более приоритетными являются настройки файла `jail.local`. Файл `jail.conf` содержит параметры по умолчанию и не предназначен для редактирования, тогда как `jail.local` и файлы в каталоге `jail.d` используются для переопределения и расширения стандартной конфигурации.

### 3. Как настроить оповещение администратора при срабатывании Fail2ban?

Оповещение администратора настраивается с помощью параметров `destemail`, `sender` и `action` в конфигурационных файлах Fail2ban. Для отправки уведомлений по электронной почте используется действие `action_mwl` или аналогичное, обеспечивающее отправку письма с информацией о срабатывании блокировки.

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

В конфигурации веб-служб задаются параметры активации jail-модуля, используемый фильтр для анализа журналов Apache, пути к лог-файлам веб-сервера,

а также значения `maxretry`, `findtime` и `bantime`, определяющие условия и длительность блокировки IP-адресов при подозрительной активности.

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

Для почтовых служб в конфигурации определяются jail-модули для сервисов Postfix и Dovecot, фильтры анализа журналов аутентификации, пути к лог-файлам, а также параметры количества допустимых ошибок и времени блокировки, применяемые при попытках подбора учётных данных.

**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 блокировку IP-адреса с помощью `iptables`, `firewalld` или `nftables`, отправку уведомлений администратору, запись информации в журнал, а также выполнение пользовательских скриптов. Описание доступных действий содержится в каталоге `/etc/fail2ban/action.d`.

**7. Как получить список действующих правил Fail2ban?**

Список активных jail-модулей и действующих правил можно получить с помощью команды `fail2ban-client status`, которая отображает общее состояние Fail2ban и перечень задействованных механизмов защиты.

**8. Как получить статистику заблокированных Fail2ban адресов?**

Статистика заблокированных адресов доступна через команду `fail2ban-client status <имя_jail>`, где отображается количество текущих и общих блокировок, а также список заблокированных IP-адресов.

**9. Как разблокировать IP-адрес?**

Разблокировка IP-адреса выполняется с помощью команды `fail2ban-client set <имя_jail> unbanip <IP-адрес>`, после чего указанный адрес удаляется из списка заблокированных.