

# **Отчёт по лабораторной работе 16**

**Базовая защита от атак типа «brute force»**

Заур Мустафеев

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение работы</b>	<b>6</b>
2.1	Защита сервера с помощью Fail2ban . . . . .	6
2.1.1	Включение защиты HTTP . . . . .	8
2.1.2	Включение защиты почтовых сервисов . . . . .	10
2.2	Проверка работы Fail2ban . . . . .	12
2.3	Внесение изменений в настройки внутреннего окружения виртуальных машин . . . . .	16
<b>3</b>	<b>Вывод</b>	<b>17</b>
<b>4</b>	<b>Контрольные вопросы</b>	<b>18</b>
<b>5</b>	<b>Список литературы</b>	<b>21</b>

## Список иллюстраций

2.1	Запуск fail2ban и включение автозагрузки . . . . .	6
2.2	Просмотр журнала fail2ban.log . . . . .	6
2.3	Настройка bantime и включение SSH-защиты . . . . .	7
2.4	Журнал после включения jail'ов для SSH . . . . .	8
2.5	Включение HTTP-защиты (Apache jail'ы) . . . . .	9
2.6	Журнал после включения HTTP-защиты . . . . .	10
2.7	Включение защиты почты (Postfix/Dovecot jail'ы) . . . . .	11
2.8	Журнал после включения защиты почты . . . . .	12
2.9	Статус jail sshd до блокировки . . . . .	13
2.10	Фиксация блокировки IP-адреса клиента . . . . .	13
2.11	Статус jail sshd после разблокировки IP . . . . .	14
2.12	Добавление ignoreip в конфигурацию Fail2ban . . . . .	15
2.13	Журнал Fail2ban с игнорированием IP-адреса . . . . .	15
2.14	Скрипт protect.sh для 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 работы

### 2.1 Защита сервера с помощью Fail2ban

1. На сервере установлен пакет **fail2ban** с помощью **dnf**, после чего выполнена первичная инициализация службы.
2. Сервис **fail2ban** запущен и добавлен в автозагрузку командами **systemctl start fail2ban** и **systemctl enable fail2ban**.

```
Running scriptlet: fail2ban-1.1.0-6.el10_0.noarch
Installed:
fail2ban-1.1.0-6.el10_0.noarch
fail2ban-selinux-1.1.0-6.el10_0.noarch
fail2ban-server-1.1.0-6.el10_0.noarch
fail2ban-firewalld-1.1.0-6.el10_0.noarch
fail2ban-sendmail-1.1.0-6.el10_0.noarch

Complete!
[root@server.zmustafaev.net zmustafaev]#
[root@server.zmustafaev.net zmustafaev]# systemctl start fail2ban
[root@server.zmustafaev.net zmustafaev]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' -> '/usr/lib/systemd/system/fail2ban.service'.
[root@server.zmustafaev.net zmustafaev]#
```

Рис. 2.1: Запуск fail2ban и включение автозагрузки

3. В дополнительном терминале запущен просмотр журнала событий Fail2ban командой **tail -f /var/log/fail2ban.log**. Убедились, что сервис стартует корректно и подключается к базе.

```
[zmustafaev@server.zmustafaev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for zmustafaev:
2025-12-12 14:48:07,879 fail2ban.server [10680]: INFO -----
-----
2025-12-12 14:48:07,879 fail2ban.server [10680]: INFO Starting Fail2ban v1.1.0
2025-12-12 14:48:07,879 fail2ban.observer [10680]: INFO Observer start...
2025-12-12 14:48:07,882 fail2ban.database [10680]: INFO Connected to fail2ban persistent database
'/var/lib/fail2ban/fail2ban.sqlite3'
2025-12-12 14:48:07,883 fail2ban.database [10680]: WARNING New database created. Version '4'
```

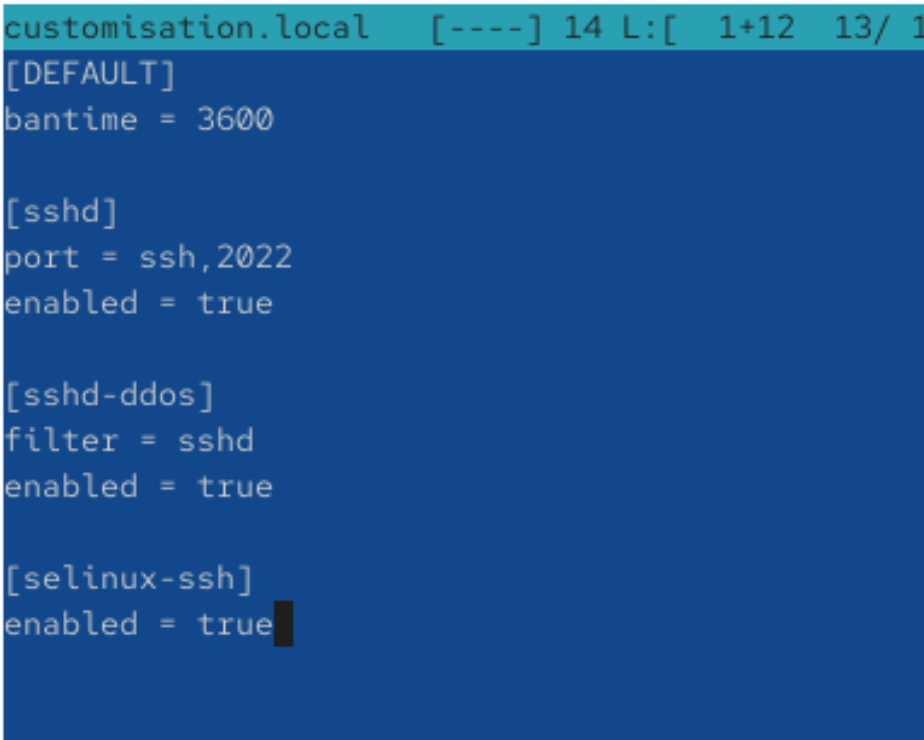
Рис. 2.2: Просмотр журнала fail2ban.log

4. Создан файл локальной конфигурации Fail2ban:

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

5. В файле `/etc/fail2ban/jail.d/customisation.local` выполнена настройка параметров блокировки и включена защита **SSH**:

- задано время блокировки `bantime = 3600` (1 час);
- активированы jail'ы: `sshd`, `sshd-ddos`, `selinux-ssh`;
- для `sshd` указан порт `ssh,2022`.



```
customisation.local  [----] 14 L:[ 1+12 13/ 1
[DEFAULT]
bantime = 3600

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

Рис. 2.3: Настройка `bantime` и включение SSH-защиты

6. Для применения настроек Fail2ban выполнен перезапуск службы командой `systemctl restart fail2ban`. После перезапуска в журнале подтверждено создание и запуск jail'ов для SSH.

```

2025-12-12 14:51:20,893 fail2ban.jail [11344]: INFO Creating new jail 'sshd'
2025-12-12 14:51:20,895 fail2ban.jail [11344]: INFO Jail 'sshd' uses systemd {}
2025-12-12 14:51:20,895 fail2ban.jail [11344]: INFO Initiated 'systemd' backend
2025-12-12 14:51:20,896 fail2ban.filter [11344]: INFO maxLines: 1
2025-12-12 14:51:20,901 fail2ban.filtersystemd [11344]: INFO [sshd] Added journal match for: '_SYSTEMD_
UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session'
2025-12-12 14:51:20,901 fail2ban.filter [11344]: INFO maxRetry: 5
2025-12-12 14:51:20,901 fail2ban.filter [11344]: INFO findtime: 600
2025-12-12 14:51:20,901 fail2ban.actions [11344]: INFO banTime: 3600
2025-12-12 14:51:20,901 fail2ban.filter [11344]: INFO encoding: UTF-8
2025-12-12 14:51:20,901 fail2ban.jail [11344]: INFO Creating new jail 'selinux-ssh'
2025-12-12 14:51:20,903 fail2ban.jail [11344]: INFO Jail 'selinux-ssh' uses pyinotify {}
2025-12-12 14:51:20,904 fail2ban.jail [11344]: INFO Initiated 'pyinotify' backend
2025-12-12 14:51:20,905 fail2ban.datedetector [11344]: INFO date pattern '': 'Epoch'
2025-12-12 14:51:20,905 fail2ban.filter [11344]: INFO maxRetry: 5
2025-12-12 14:51:20,905 fail2ban.filter [11344]: INFO findtime: 600
2025-12-12 14:51:20,905 fail2ban.actions [11344]: INFO banTime: 3600
2025-12-12 14:51:20,905 fail2ban.filter [11344]: INFO encoding: UTF-8
2025-12-12 14:51:20,905 fail2ban.filter [11344]: INFO Added logfile: '/var/log/audit/audit.log'
(pos = 0, hash = 2bac1d1460b4ddb65dad9af08e925a24fbee1cb)
2025-12-12 14:51:20,906 fail2ban.jail [11344]: INFO Creating new jail 'sshd-ddos'
2025-12-12 14:51:20,906 fail2ban.jail [11344]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-12 14:51:20,906 fail2ban.jail [11344]: INFO Initiated 'pyinotify' backend
2025-12-12 14:51:20,907 fail2ban.filter [11344]: INFO maxLines: 1
2025-12-12 14:51:20,907 fail2ban.filter [11344]: INFO maxRetry: 5
2025-12-12 14:51:20,907 fail2ban.filter [11344]: INFO findtime: 600
2025-12-12 14:51:20,907 fail2ban.actions [11344]: INFO banTime: 3600
2025-12-12 14:51:20,907 fail2ban.filter [11344]: INFO encoding: UTF-8
2025-12-12 14:51:20,907 fail2ban.jail [11344]: INFO Jail 'sshd' started
2025-12-12 14:51:20,908 fail2ban.jail [11344]: INFO Jail 'selinux-ssh' started
2025-12-12 14:51:20,909 fail2ban.jail [11344]: INFO Jail 'sshd-ddos' started
2025-12-12 14:51:20,911 fail2ban.filtersystemd [11344]: INFO [sshd] Jail is in operation now (process n
ew journal entries)

```

Рис. 2.4: Журнал после включения jail'ов для SSH

### 2.1.1 Включение защиты HTTP

1. В файле `/etc/fail2ban/jail.d/customisation.local` включена защита веб-сервера (HTTP) путём активации следующих jail'ов: `apache-auth`, `apache-badbots`, `apache-noscript`, `apache-overflows`, `apache-nohome`, `apache-botsearch`, `apache-fakegooglebot`, `apache-modsecurity`, `apache-shellshock`.

```
customisation.local [----] 14 L:[ 11+29 40/ 40] *(4

[selinux-ssh]
enabled = true

[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

[apache-shellshock]
enabled = true

1Help 2Save 3Mark 4Replac 5Copy
```

Рис. 2.5: Включение HTTP-защиты (Apache jail'ы)

2. Выполнен перезапуск Fail2ban (`systemctl restart fail2ban`). В журнале подтверждён запуск jail'ов Apache и привязка к соответствующим лог-файлам.

```

(pos = 0, hash = 6beb785d2d04563df04eacb022af427599573363)
2025-12-12 14:56:21.903 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/ssl_error_l
og' (pos = 0, hash = 207f373360c71fa65be6d05e5267fcfa3aaa4d8b)
2025-12-12 14:56:21.903 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/www.zmustaf
aev.net-error_log' (pos = 0, hash = ed421f0035abcca6a40a8dd472467db53dc7f581)
2025-12-12 14:56:21.903 fail2ban.jail [12058]: INFO Creating new jail 'apache-shellshock'
2025-12-12 14:56:21.903 fail2ban.jail [12058]: INFO Jail 'apache-shellshock' uses pyinotify {}
2025-12-12 14:56:21.904 fail2ban.jail [12058]: INFO Initiated 'pyinotify' backend
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO maxRetry: 1
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO findtime: 600
2025-12-12 14:56:21.905 fail2ban.actions [12058]: INFO banTime: 3600
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO encoding: UTF-8
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/server.zmus
tafaev.net-error_log' (pos = 0, hash = )
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/error_log'
(pos = 0, hash = 66eb785d2d04563df04eacb022af427599573363)
2025-12-12 14:56:21.905 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/ssl_error_l
og' (pos = 0, hash = 207f373360c71fa65be6d05e5267fcfa3aaa4d8b)
2025-12-12 14:56:21.906 fail2ban.filter [12058]: INFO Added logfile: '/var/log/httpd/www.zmustaf
aev.net-error_log' (pos = 0, hash = ed421f0035abcca6a40a8dd472467db53dc7f581)
2025-12-12 14:56:21.906 fail2ban.jail [12058]: INFO Creating new jail 'sshd-ddos'
2025-12-12 14:56:21.906 fail2ban.jail [12058]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-12 14:56:21.907 fail2ban.jail [12058]: INFO Initiated 'pyinotify' backend
2025-12-12 14:56:21.907 fail2ban.filter [12058]: INFO maxLines: 1
2025-12-12 14:56:21.908 fail2ban.filter [12058]: INFO maxRetry: 5
2025-12-12 14:56:21.908 fail2ban.filter [12058]: INFO findtime: 600
2025-12-12 14:56:21.908 fail2ban.actions [12058]: INFO banTime: 3600
2025-12-12 14:56:21.908 fail2ban.filter [12058]: INFO encoding: UTF-8
2025-12-12 14:56:21.908 fail2ban.jail [12058]: INFO Jail 'sshd' started
2025-12-12 14:56:21.908 fail2ban.filtersystemd [12058]: INFO [sshd] Jail is in operation now (process n
ew journal entries)
2025-12-12 14:56:21.910 fail2ban.jail [12058]: INFO Jail 'selinux-ssh' started
2025-12-12 14:56:21.910 fail2ban.jail [12058]: INFO Jail 'apache-auth' started

```

Рис. 2.6: Журнал после включения HTTP-защиты

## 2.1.2 Включение защиты почтовых сервисов

1. В файле `/etc/fail2ban/jail.d/customisation.local` включена защита почтовых сервисов путём активации jail'ов: `postfix`, `postfix-rbl`, `dovecot`, `postfix-sasl`.

```
enabled = true

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
```

1Help 2Save 3Mark 4Replac

Рис. 2.7: Включение защиты почты (Postfix/Dovecot jail'ы)

2. Fail2ban перезапущен командой `systemctl restart fail2ban`. В журнале подтверждён запуск jail'ов для почтовых сервисов и корректная работа механизмов блокировки.

```
2025-12-12 14:58:14,612 fail2ban.filter [12362]: INFO maxRetry: 5
2025-12-12 14:58:14,612 fail2ban.filter [12362]: INFO findtime: 600
2025-12-12 14:58:14,612 fail2ban.actions [12362]: INFO banTime: 3600
2025-12-12 14:58:14,612 fail2ban.filter [12362]: INFO encoding: UTF-8
2025-12-12 14:58:14,612 fail2ban.jail [12362]: INFO Jail 'sshd' started
2025-12-12 14:58:14,613 fail2ban.filtersystemd [12362]: INFO [sshd] Jail is in operation now (process n
ew journal entries)
2025-12-12 14:58:14,613 fail2ban.jail [12362]: INFO Jail 'selinux-ssh' started
2025-12-12 14:58:14,613 fail2ban.jail [12362]: INFO Jail 'apache-auth' started
2025-12-12 14:58:14,614 fail2ban.jail [12362]: INFO Jail 'apache-badbots' started
2025-12-12 14:58:14,614 fail2ban.jail [12362]: INFO Jail 'apache-noscript' started
2025-12-12 14:58:14,614 fail2ban.jail [12362]: INFO Jail 'apache-overflows' started
2025-12-12 14:58:14,615 fail2ban.jail [12362]: INFO Jail 'apache-nohome' started
2025-12-12 14:58:14,615 fail2ban.jail [12362]: INFO Jail 'apache-botsearch' started
2025-12-12 14:58:14,615 fail2ban.jail [12362]: INFO Jail 'apache-fakegooglebot' started
2025-12-12 14:58:14,615 fail2ban.jail [12362]: INFO Jail 'apache-modsecurity' started
2025-12-12 14:58:14,616 fail2ban.jail [12362]: INFO Jail 'apache-shellshock' started
2025-12-12 14:58:14,616 fail2ban.jail [12362]: INFO Jail 'postfix' started
2025-12-12 14:58:14,616 fail2ban.jail [12362]: INFO Jail 'postfix-rbl' started
2025-12-12 14:58:14,617 fail2ban.filtersystemd [12362]: INFO [postfix] Jail is in operation now (proces
s new journal entries)
2025-12-12 14:58:14,617 fail2ban.filtersystemd [12362]: INFO [postfix-rbl] Jail is in operation now (pr
ocess new journal entries)
2025-12-12 14:58:14,617 fail2ban.filtersystemd [12362]: INFO [dovecot] Jail is in operation now (proces
s new journal entries)
2025-12-12 14:58:14,617 fail2ban.jail [12362]: INFO Jail 'dovecot' started
2025-12-12 14:58:14,618 fail2ban.filtersystemd [12362]: INFO [postfix-sasl] Jail is in operation now (p
rocess new journal entries)
2025-12-12 14:58:14,618 fail2ban.jail [12362]: INFO Jail 'postfix-sasl' started
2025-12-12 14:58:14,618 fail2ban.jail [12362]: INFO Jail 'sshd-ddos' started
```

Рис. 2.8: Журнал после включения защиты почты

## 2.2 Проверка работы Fail2ban

1. На сервере проверен общий статус Fail2ban с помощью команды `fail2ban-client status`. Убедились, что служба запущена и активны все настроенные jail'ы.
2. Проверен статус защиты SSH командой `fail2ban-client status sshd`. Установлено, что на момент проверки заблокированных адресов нет.

```

[root@server.zmustafaev.net zmustafaev]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, ap
  apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-s
  asl, selinux-ssh, sshd, sshd-ddos
[root@server.zmustafaev.net zmustafaev]# 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.zmustafaev.net zmustafaev]# fail2ban-client set sshd maxretry 2
2
[root@server.zmustafaev.net zmustafaev]#

```

Рис. 2.9: Статус jail sshd до блокировки

3. Для SSH установлен параметр максимального количества неудачных попыток аутентификации, равный 2:

```
fail2ban-client set sshd maxretry 2
```

4. С клиентской машины выполнены попытки подключения к серверу по SSH с неверным паролем.
5. После превышения допустимого числа ошибок повторно проверен статус защиты SSH. В результате зафиксирована блокировка IP-адреса клиента.

```

2025-12-12 14:58:14,618 fail2ban.jail      [12362]: INFO    Jail 'postfix-sasl' started
2025-12-12 14:58:14,618 fail2ban.jail      [12362]: INFO    Jail 'sshd-ddos' started
2025-12-12 15:00:35,943 fail2ban.filter    [12362]: INFO    maxRetry: 2
2025-12-12 15:01:55,175 fail2ban.filter    [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
01:54
2025-12-12 15:01:58,660 fail2ban.filter    [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
01:58
2025-12-12 15:01:58,746 fail2ban.actions    [12362]: NOTICE [sshd] Ban 192.168.1.30
2025-12-12 15:02:02,375 fail2ban.filter    [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
02:02

```

Рис. 2.10: Фиксация блокировки IP-адреса клиента

6. Выполнена разблокировка IP-адреса клиента с помощью команды:

```
fail2ban-client set sshd unbanip 192.168.1.30
```

7. Повторно проверен статус jail sshd. Убедились, что IP-адрес удалён из списка заблокированных.

```

[root@server.zmustafaev.net zmustafaevj#
[root@server.zmustafaev.net zmustafaevj# 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.zmustafaev.net zmustafaevj# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.zmustafaev.net zmustafaevj# 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.zmustafaev.net zmustafaevj# █

```

Рис. 2.11: Статус jail sshd после разблокировки IP

8. В файл `/etc/fail2ban/jail.d/customisation.local` внесено изменение: в разделе `[DEFAULT]` добавлено игнорирование IP-адреса клиента с помощью параметра `ignoreip`.

```
zmustafaev@server:/home/zmustafaev - mcedit /etc/fail2ban/jail.conf x
customisation.local [----] 35 L:[ 1+ 3 4/ 54] *(61
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.30

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true

[apache-auth]
enabled = true

[apache-badbots]
enabled = true
```

Рис. 2.12: Добавление ignoreip в конфигурацию Fail2ban

9. Fail2ban перезапущен для применения изменений:

```
systemctl restart fail2ban
```

10. Выполнен просмотр журнала событий Fail2ban. В журнале зафиксировано, что попытки подключения с указанного IP-адреса игнорируются.

```
process new journal entries)
2025-12-12 15:03:31,551 fail2ban.jail [13141]: INFO Jail 'postfix-sasl' started
2025-12-12 15:03:31,551 fail2ban.jail [13141]: INFO Jail 'sshd-ddos' started

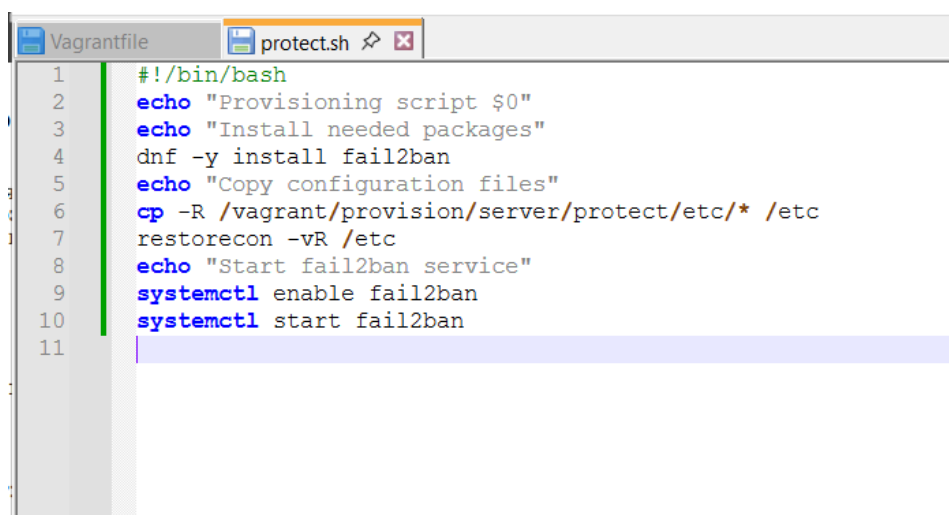
2025-12-12 15:03:45,378 fail2ban.filter [13141]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-12 15:03:50,661 fail2ban.filter [13141]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-12 15:03:54,644 fail2ban.filter [13141]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рис. 2.13: Журнал Fail2ban с игнорированием IP-адреса

11. С клиента повторно выполнены попытки подключения по SSH с неверным паролем. Проверка статуса `jail sshd` показала отсутствие блокировки, что подтверждает корректность настройки параметра `ignoreip`.

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине **server** выполнен переход в каталог `/vagrant/provision/server`. Создан каталог `protect` для хранения конфигурационных файлов внутреннего окружения.
2. В каталоге `protect` создана структура под конфигурацию Fail2ban и скопирован файл локальной настройки `customisation.local`.
3. В каталоге `/vagrant/provision/server` создан исполняемый файл `protect.sh`, предназначенный для автоматической установки и запуска Fail2ban при развёртывании окружения.



```
Vagrantfile  protect.sh
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. 2.14: Скрипт `protect.sh` для настройки Fail2ban

## 3 Вывод

В ходе работы была реализована защита сервера с использованием Fail2ban. Сервис установлен, запущен и настроен для защиты SSH, веб-служб и почтовых сервисов. Проведена проверка корректности работы механизмов блокировки и разблокировки IP-адресов, а также настроено игнорирование доверенного клиента. Дополнительно выполнена подготовка конфигурационных файлов и скрипта автоматизации для повторного развёртывания среды, что упрощает администрирование и повышает надёжность системы защиты.

## 4 Контрольные вопросы

**1. Поясните принцип работы Fail2ban.**

Fail2ban анализирует журналы системных и прикладных сервисов, выявляет повторяющиеся ошибки аутентификации или подозрительные действия и при превышении заданных порогов применяет меры блокировки к IP-адресу нарушителя (как правило, с помощью правил файрвола).

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

Более приоритетными являются настройки из файла `jail.local`. Они переопределяют параметры, заданные в `jail.conf`, и используются для пользовательской конфигурации, чтобы избежать потери изменений при обновлении пакета.

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

Для этого необходимо настроить параметр `action` в конфигурации Fail2ban, указав действие с отправкой почты (например, `action_mwl`). Также требуется корректно настроить почтовую подсистему сервера и задать адрес администратора в параметре `destemail`.

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

- `enabled` — включает или отключает защиту конкретной веб-службы;

- `port` — указывает порт или сервис (обычно `http`, `https`);
- `filter` — задаёт фильтр, по которому анализируются логи;
- `logpath` — путь к файлам журналов веб-сервера;
- `maxretry` — допустимое количество нарушений до блокировки;
- `findtime` — временной интервал для подсчёта ошибок;
- `bantime` — время блокировки IP-адреса.

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

- `enabled` — активирует защиту почтового сервиса;
- `filter` — определяет шаблоны ошибок аутентификации в логах;
- `logpath` — путь к журналам Postfix, Dovecot и других почтовых сервисов;
- `port` — используемые почтовые порты (`smtp`, `pop3`, `imap` и др.);
- `maxretry`, `findtime`, `bantime` — параметры, определяющие условия и длительность блокировки.

**6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий?**

Fail2ban может добавлять правила блокировки в файрвол (`iptables`, `firewalld`), отправлять уведомления администратору, выполнять пользовательские скрипты. Описание доступных действий находится в каталоге

`/etc/fail2ban/action.d/.`

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

Для просмотра активных jail'ов используется команда:

`fail2ban-client status.`

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

Статистика по конкретному jail'у отображается командой:

`fail2ban-client status <jail_name>,`

где выводится информация о текущих и суммарно заблокированных IP-адресах.

**9. Как разблокировать IP-адрес?**

Разблокировка выполняется командой:

`fail2ban-client set <jail_name> unbanip <IP-адрес>.`

## **5 Список литературы**

1. Сайт Fail2ban. — URL: <https://www.fail2ban.org> (visited on 09/13/2021).