

# **Отчёт по лабораторной работе №16**

**Дисциплина: Администрирование сетевых подсистем**

**Мишина Анастасия Алексеевна**

# Содержание

|  |           |
|--|-----------|
| <b>1 Цель работы</b>   | <b>5</b>  |
| <b>2 Выполнение лабораторной работы</b>  | <b>6</b>  |
| 2.1 Защита с помощью Fail2ban . . . . .  | 6         |
| 2.2 Проверка работы Fail2ban . . . . .   | 12        |
| 2.3 Внесение изменений в настройки внутреннего окружения<br>виртуальной машины . . . . . | 16        |
| <b>3 Контрольные вопросы</b>   | <b>18</b> |
| <b>4 Выводы</b>  | <b>21</b> |

# Список иллюстраций

|  |    |
|--|----|
| 2.1 Установка и запуск fail2ban . . . . .  | 6  |
| 2.2 Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH . . . . . | 7  |
| 2.3 Просмотр журнала событий fail2ban . . . . .  | 8  |
| 2.4 Редактирование файла с локальной конфигурацией: защита HTTP . . . . .                            | 9  |
| 2.5 Просмотр журнала событий fail2ban . . . . .  | 10 |
| 2.6 Редактирование файла с локальной конфигурацией: защита почты . . . . .                           | 11 |
| 2.7 Просмотр журнала событий fail2ban . . . . .  | 12 |
| 2.8 Просмотр статуса службы, статус защиты SSH, установка макс. кол-ва ошибок для SSH . . . . .      | 12 |
| 2.9 Подключение к серверу по SSH с вводом неправильного пароля                                       | 13 |
| 2.10 Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента . . . . .   | 14 |
| 2.11 Редактирование файла с локальной конфигурацией: игнорирование адреса клиента . . . . .          | 14 |
| 2.12 Просмотр журнала событий ‘fail2ban’ . . . . .   | 15 |
| 2.13 Просмотр статуса защиты SSH после неудачного входа . .  | 16 |
| 2.14 Редактирование protect.sh на сервере . . . . .  | 17 |

# **Список таблиц**

# **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 устанавливаем fail2ban:

```
dnf -y install fail2ban
```

Запускаем сервер fail2ban (рис. 2.1).

```
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch          1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower priority 100 with module at
priority 200.

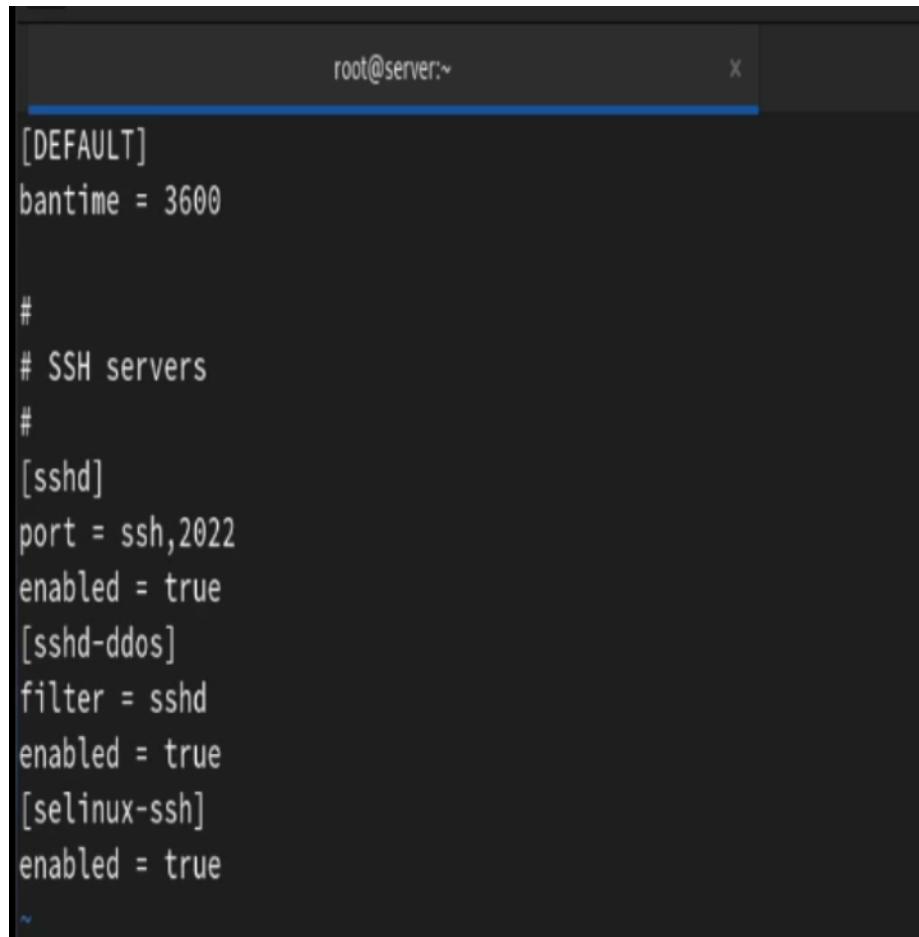
Installing      : fail2ban-server-1.0.2-12.el9.noarch              2/5
Running scriptlet: fail2ban-server-1.0.2-12.el9.noarch
Installing      : fail2ban-firewalld-1.0.2-12.el9.noarch            3/5
Installing      : fail2ban-sendmail-1.0.2-12.el9.noarch             4/5
Installing      : fail2ban-1.0.2-12.el9.noarch                   5/5
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch
Running scriptlet: fail2ban-1.0.2-12.el9.noarch
Verifying       : fail2ban-1.0.2-12.el9.noarch                   1/5
Verifying       : fail2ban-firewalld-1.0.2-12.el9.noarch            2/5
Verifying       : fail2ban-selinux-1.0.2-12.el9.noarch             3/5
Verifying       : fail2ban-sendmail-1.0.2-12.el9.noarch             4/5
Verifying       : fail2ban-server-1.0.2-12.el9.noarch               5/5

Installed:
fail2ban-1.0.2-12.el9.noarch                  fail2ban-firewalld-1.0.2-12.el9.noarch
fail2ban-selinux-1.0.2-12.el9.noarch           fail2ban-sendmail-1.0.2-12.el9.noarch
fail2ban-server-1.0.2-12.el9.noarch

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

Рис. 2.1: Установка и запуск fail2ban

В доп. терминале запускаем просмотр журнала событий fail2ban. Создаем файл с локальной конфигурацией /etc/fail2ban/jail.d/customisation.local. Задаем время блокирования, включаем защиту SSH, после чего перезапускаем fail2ban (рис. 2.2).

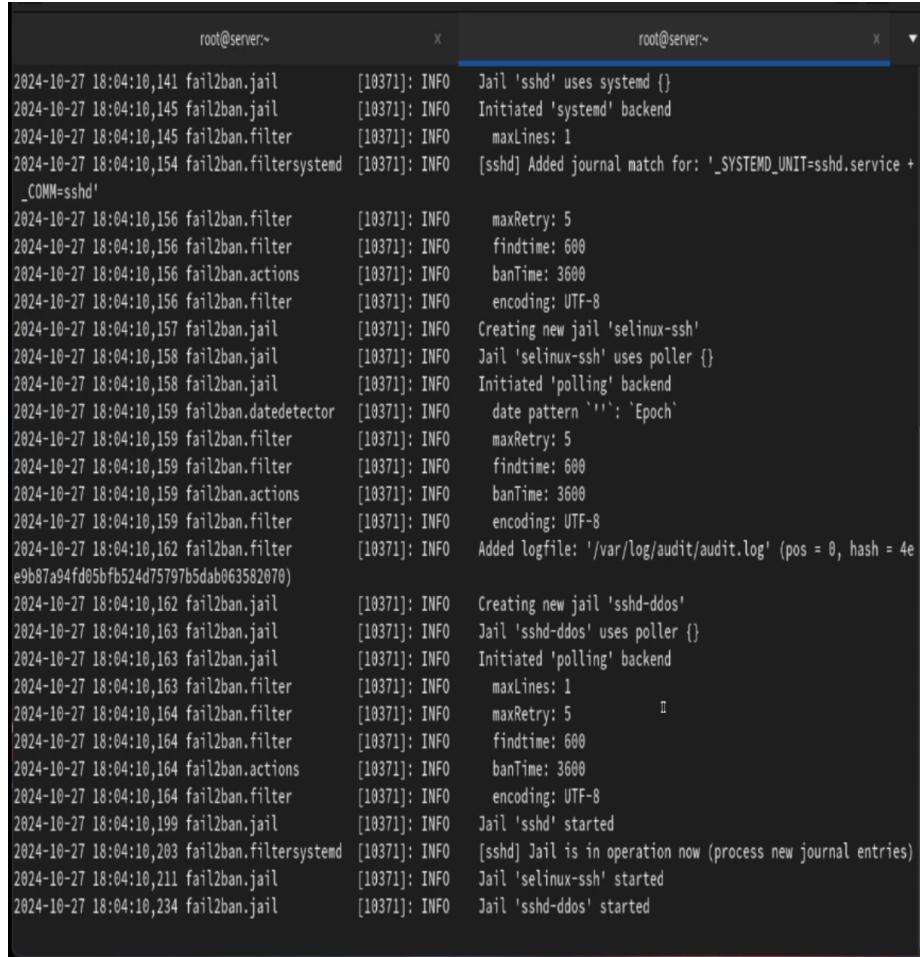


```
root@server:~ [DEFAULT]
bantime = 3600

#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

Рис. 2.2: Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH

Просматриваем журнал событий fail2ban и видим сообщения об активации jail-ов (рис. 2.3).



The screenshot shows two terminal windows side-by-side. Both windows have a title bar 'root@server:~' and a close button 'X'. The left window's scroll bar is at the bottom, while the right window's scroll bar is at the top. The log output is as follows:

```
root@server:~          root@server:~  
2024-10-27 18:04:10,141 fail2ban.jail      [10371]: INFO  Jail 'sshd' uses systemd {}  
2024-10-27 18:04:10,145 fail2ban.jail      [10371]: INFO  Initiated 'systemd' backend  
2024-10-27 18:04:10,145 fail2ban.filter    [10371]: INFO  maxLines: 1  
2024-10-27 18:04:10,154 fail2ban.filtersystemd [10371]: INFO  [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'  
2024-10-27 18:04:10,156 fail2ban.filter    [10371]: INFO  maxRetry: 5  
2024-10-27 18:04:10,156 fail2ban.filter    [10371]: INFO  findtime: 600  
2024-10-27 18:04:10,156 fail2ban.actions   [10371]: INFO  banTime: 3600  
2024-10-27 18:04:10,156 fail2ban.filter    [10371]: INFO  encoding: UTF-8  
2024-10-27 18:04:10,157 fail2ban.jail      [10371]: INFO  Creating new jail 'selinux-ssh'  
2024-10-27 18:04:10,158 fail2ban.jail      [10371]: INFO  Jail 'selinux-ssh' uses poller {}  
2024-10-27 18:04:10,158 fail2ban.jail      [10371]: INFO  Initiated 'polling' backend  
2024-10-27 18:04:10,159 fail2ban.datedetector [10371]: INFO  date pattern '': 'Epoch'  
2024-10-27 18:04:10,159 fail2ban.filter    [10371]: INFO  maxRetry: 5  
2024-10-27 18:04:10,159 fail2ban.filter    [10371]: INFO  findtime: 600  
2024-10-27 18:04:10,159 fail2ban.actions   [10371]: INFO  banTime: 3600  
2024-10-27 18:04:10,159 fail2ban.filter    [10371]: INFO  encoding: UTF-8  
2024-10-27 18:04:10,162 fail2ban.filter    [10371]: INFO  Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 4e e9b87a94fd05fb524d75797b5dab063582070)  
2024-10-27 18:04:10,162 fail2ban.jail      [10371]: INFO  Creating new jail 'sshd-ddos'  
2024-10-27 18:04:10,163 fail2ban.jail      [10371]: INFO  Jail 'sshd-ddos' uses poller {}  
2024-10-27 18:04:10,163 fail2ban.jail      [10371]: INFO  Initiated 'polling' backend  
2024-10-27 18:04:10,163 fail2ban.filter    [10371]: INFO  maxLines: 1  
2024-10-27 18:04:10,164 fail2ban.filter    [10371]: INFO  maxRetry: 5  
2024-10-27 18:04:10,164 fail2ban.filter    [10371]: INFO  findtime: 600  
2024-10-27 18:04:10,164 fail2ban.actions   [10371]: INFO  banTime: 3600  
2024-10-27 18:04:10,164 fail2ban.filter    [10371]: INFO  encoding: UTF-8  
2024-10-27 18:04:10,164 fail2ban.filter    [10371]: INFO  Jail 'sshd' started  
2024-10-27 18:04:10,199 fail2ban.jail      [10371]: INFO  [sshd] Jail is in operation now (process new journal entries)  
2024-10-27 18:04:10,203 fail2ban.filtersystemd [10371]: INFO  Jail 'selinux-ssh' started  
2024-10-27 18:04:10,211 fail2ban.jail      [10371]: INFO  Jail 'sshd' started  
2024-10-27 18:04:10,234 fail2ban.jail      [10371]: INFO  Jail 'sshd-ddos' started
```

Рис. 2.3: Просмотр журнала событий fail2ban

В файле конфигурации включаем защиту HTTP, после чего перезапускаем fail2ban (рис. 2.4).

The screenshot shows three terminal windows side-by-side, all running under the root user on a server. Each window displays a portion of a configuration file, likely /etc/fail2ban/filter.d/httpd.conf, which contains rules for various services. The configuration includes sections for SELinux, Apache authentication, badbots, noscript, overflows, nohome, botsearch, and fakegooglebot. The last line in each window is ':wq'.

```
[selinux-ssh]
enabled = true

#
# 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]
:wq
```

Рис. 2.4: Редактирование файла с локальной конфигурацией: защита HTTP

Просматриваем журнал событий fail2ban (рис. 2.5).

```
2024-10-27 18:06:03,192 fail2ban.filter [10453]: INFO encoding: UTF-8
2024-10-27 18:06:03,193 fail2ban.filter [10453]: INFO Added logfile: '/var/log/httpd/server.aamishina.net-error_log' (pos = 0, hash = )
2024-10-27 18:06:03,196 fail2ban.filter [10453]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 2e2455c4818983f841481ff27cf9b31dc9
ba48a6)
2024-10-27 18:06:03,196 fail2ban.filter [10453]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 7606d2197a88a6656d717d7df899bd
d74d5e9a8a)
2024-10-27 18:06:03,196 fail2ban.filter [10453]: INFO Added logfile: '/var/log/httpd/www.aamishina.net-error_log' (pos = 0, hash = bb968c6db69265b7
456ea49508b6b099ff76d1f7c)
2024-10-27 18:06:03,197 fail2ban.jail [10453]: INFO Creating new jail 'sshd-ddos'
2024-10-27 18:06:03,197 fail2ban.jail [10453]: INFO Jail 'sshd-ddos' uses poller {}
2024-10-27 18:06:03,207 fail2ban.jail [10453]: INFO Initiated 'polling' backend
2024-10-27 18:06:03,208 fail2ban.filter [10453]: INFO maxLines: 1
2024-10-27 18:06:03,209 fail2ban.filter [10453]: INFO maxRetry: 5
2024-10-27 18:06:03,210 fail2ban.filter [10453]: INFO findtime: 600
2024-10-27 18:06:03,210 fail2ban.actions [10453]: INFO banTime: 3600
2024-10-27 18:06:03,210 fail2ban.filter [10453]: INFO encoding: UTF-8
2024-10-27 18:06:03,210 fail2ban.filtersystemd [10453]: INFO [sshd] Jail is in operation now (process new journal entries)
2024-10-27 18:06:03,211 fail2ban.jail [10453]: INFO Jail 'sshd' started
2024-10-27 18:06:03,212 fail2ban.jail [10453]: INFO Jail 'selinux-ssh' started
2024-10-27 18:06:03,214 fail2ban.jail [10453]: INFO Jail 'apache-auth' started
2024-10-27 18:06:03,224 fail2ban.jail [10453]: INFO Jail 'apache-badbots' started
2024-10-27 18:06:03,231 fail2ban.jail [10453]: INFO Jail 'apache-noscript' started
2024-10-27 18:06:03,250 fail2ban.jail [10453]: INFO Jail 'apache-overflows' started
2024-10-27 18:06:03,253 fail2ban.jail [10453]: INFO Jail 'apache-nohome' started
2024-10-27 18:06:03,254 fail2ban.jail [10453]: INFO Jail 'apache-botsearch' started
2024-10-27 18:06:03,271 fail2ban.jail [10453]: INFO Jail 'apache-fakegooglebot' started
2024-10-27 18:06:03,273 fail2ban.jail [10453]: INFO Jail 'apache-modsecurity' started
2024-10-27 18:06:03,275 fail2ban.jail [10453]: INFO Jail 'apache-shellshock' started
2024-10-27 18:06:03,280 fail2ban.jail [10453]: INFO Jail 'sshd-ddos' started
```

Рис. 2.5: Просмотр журнала событий fail2ban

В файле конфигурации включаем защиту почты, после чего перезапускаем fail2ban (рис. 2.6).

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

Рис. 2.6: Редактирование файла с локальной конфигурацией: защита почты

Просматриваем журнал событий fail2ban (рис. 2.7).

```
[root@server.aamishina.net ~]# tail -f /var/log/fail2ban.log
2024-10-27 18:07:04,094 fail2ban.jail          [10548]: INFO  Jail 'apache-shellshock' started
2024-10-27 18:07:04,095 fail2ban.jail          [10548]: INFO  Jail 'postfix' started
2024-10-27 18:07:04,104 fail2ban.jail          [10548]: INFO  Jail 'postfix-rbl' started
2024-10-27 18:07:04,109 fail2ban.filtersystemd [10548]: INFO  [postfix] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,110 fail2ban.filtersystemd [10548]: INFO  [postfix-rbl] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,113 fail2ban.jail          [10548]: INFO  Jail 'dovecot' started
2024-10-27 18:07:04,117 fail2ban.filtersystemd [10548]: INFO  [postfix-sasl] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,120 fail2ban.filtersystemd [10548]: INFO  [dovecot] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,121 fail2ban.jail          [10548]: INFO  Jail 'postfix-sasl' started
2024-10-27 18:07:04,131 fail2ban.jail          [10548]: INFO  Jail 'sshd-ddos' started
```

Рис. 2.7: Просмотр журнала событий fail2ban

## 2.2 Проверка работы Fail2ban

На сервере просматриваем статус службы, статус защиты SSH, устанавливаем максимальное количество ошибок для SSH, равное 2 (рис. 2.8).

```
[root@server.aamishina.net ~]# fail2ban-client status
Status
|- Number of jail:    16
`- Jail list: apache-auth, 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.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- Journal matches: _SYSTEMD_UNIT:sshd.service + _COMM:sshd
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  `- Banned IP list:
[root@server.aamishina.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.aamishina.net ~]#
```

Рис. 2.8: Просмотр статуса службы, статус защиты SSH, установка макс. кол-ва ошибок для SSH

С клиента пытаемся подключиться к серверу по SSH и намеренно вводим неверный пароль (рис. 2.9).

```
[root@client.aamishina.net ~]# ssh aamishina@server.aamishina.net
The authenticity of host 'server.aamishina.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:9t38xEDGq4lcr5/Tsoa80ISQoztxdmZFH71zorIzZ7g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.aamishina.net' (ED25519) to the list of known hosts.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password: [REDACTED]
```

Рис. 2.9: Подключение к серверу по SSH с вводом неправильного пароля

Снова просматриваем статус защиты SSH на сервере и видим 2 попытки неудачного входа и 1 забаненный IP-адрес. Разблокируем адрес клиента и вновь просматриваем статус. Убеждаемся, что заблокированных IP нет (рис. 2.10).

```
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    2
| `-' Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd
`- Actions
  |- Currently banned: 1
  |- Total banned:    1
  `-' Banned IP list:  192.168.1.57
[root@server.aamishina.net ~]# fail2ban-client set sshd unbanip 192.168.1.57
1
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    2
| `-' Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd
`- Actions
  |- Currently banned: 0
  |- Total banned:    1
  `-' Banned IP list:
[root@server.aamishina.net ~]#
```

Рис. 2.10: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

Вносим изменения в конфигурационный файл, добавив в раздел по умолчанию игнорирование адреса клиента (рис. 2.11).

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.57
#
# SSH servers
```

Рис. 2.11: Редактирование файла с локальной конфигурацией: игнорирование адреса клиента

Перезапускаем службу и просматриваем журнал событий (рис. 2.12).

```
2024-10-27 18:16:03,456 fail2ban.filter      [10810]: INFO  [sshd] Ignore 192.168.1.57 by ip
2024-10-27 18:16:03,457 fail2ban.filtersystemd [10810]: INFO  [sshd] Jail is in operation now (process
new journal entries)
2024-10-27 18:16:03,458 fail2ban.jail        [10810]: INFO  Jail 'selinux-ssh' started
2024-10-27 18:16:03,466 fail2ban.jail        [10810]: INFO  Jail 'apache-auth' started
2024-10-27 18:16:03,470 fail2ban.jail        [10810]: INFO  Jail 'apache-badbots' started
2024-10-27 18:16:03,478 fail2ban.jail        [10810]: INFO  Jail 'apache-noscript' started
2024-10-27 18:16:03,479 fail2ban.jail        [10810]: INFO  Jail 'apache-overflows' started
2024-10-27 18:16:03,480 fail2ban.jail        [10810]: INFO  Jail 'apache-nohome' started
2024-10-27 18:16:03,488 fail2ban.jail        [10810]: INFO  Jail 'apache-botsearch' started
2024-10-27 18:16:03,488 fail2ban.jail        [10810]: INFO  Jail 'apache-fakegooglebot' started
2024-10-27 18:16:03,489 fail2ban.jail        [10810]: INFO  Jail 'apache-modsecurity' started
2024-10-27 18:16:03,490 fail2ban.jail        [10810]: INFO  Jail 'apache-shellshock' started
2024-10-27 18:16:03,491 fail2ban.filtersystemd [10810]: INFO  [postfix] Jail is in operation now (proc
ess new journal entries)
2024-10-27 18:16:03,500 fail2ban.jail        [10810]: INFO  Jail 'postfix' started
2024-10-27 18:16:03,501 fail2ban.filtersystemd [10810]: INFO  [postfix-rbl] Jail is in operation now (
process new journal entries)
2024-10-27 18:16:03,501 fail2ban.jail        [10810]: INFO  Jail 'postfix-rbl' started
2024-10-27 18:16:03,502 fail2ban.filtersystemd [10810]: INFO  [dovecot] Jail is in operation now (proc
ess new journal entries)
2024-10-27 18:16:03,509 fail2ban.jail        [10810]: INFO  Jail 'dovecot' started
2024-10-27 18:16:03,519 fail2ban.filtersystemd [10810]: INFO  [postfix-sasl] Jail is in operation now
(process new journal entries)
2024-10-27 18:16:03,520 fail2ban.jail        [10810]: INFO  Jail 'postfix-sasl' started
2024-10-27 18:16:03,520 fail2ban.jail        [10810]: INFO  Jail 'sshd-ddos' started
```

Рис. 2.12: Просмотр журнала событий ‘fail2ban’

С клиента вновь пытаемся аналогичным образом войти на сервер с неправильным паролем. Просматриваем статус защиты SSH и вижу 0 заблокированных адресов, так как адрес клиента находится в списке игнорируемых (рис. 2.13)

```
[root@server.aamishina.net ~]# systemctl restart fail2ban
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter           I
|  |- Currently failed: 0
|  |- Total failed:    0
|  `-' Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `-' Banned IP list:
[root@server.aamishina.net ~]#
```

Рис. 2.13: Просмотр статуса защиты SSH после неудачного входа

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На ВМ `server` переходим в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/` и копируем 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/
```

Вносим изменения в файл `/vagrant/provision/server/protect.sh` (рис. 2.14).

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install fail2ban

echo "Copy configuration files"
cp -R /vagrant/provision/server/protect/etc/* /etc
restorecon -vR /etc

echo "Start fail2ban service"
systemctl enable fail2ban
systemctl start fail2ban
~
```

Рис. 2.14: Редактирование protect.sh на сервере

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

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

### 3 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

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

Настройки файла `jail.local` более приоритетны, чем настройки файла `jail.conf`.

3. 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.

4. 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.

5. 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
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 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.

7. Как получить список действующих правил Fail2ban?

Можно использовать команду: fail2ban-client status.

8. Как получить статистику заблокированных Fail2ban адресов?

Можно использовать команду fail2ban-client status <jail-name>, где <jail-name> - имя конкретного jail, например, “ssh” или “apache”.

9. Как разблокировать IP-адрес?

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

## **4 Выводы**

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