

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 клиента	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\lserg>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:

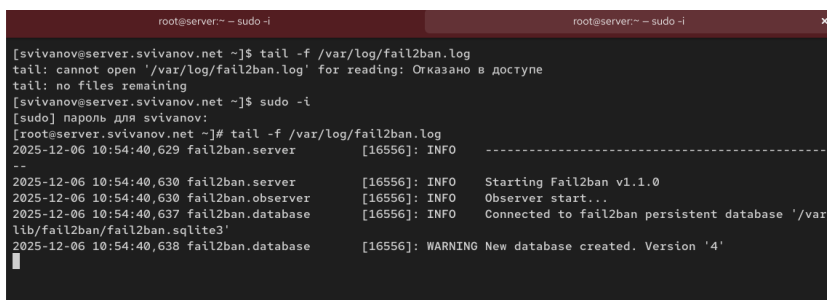
systemctl start fail2ban

systemctl enable fail2ban (рис. 3)

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

Рис. 3.3: Запуск fail2ban

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



```
root@server:~ - sudo -i
[svivanov@server.svivanov.net ~]$ tail -f /var/log/fail2ban.log
tail: cannot open '/var/log/fail2ban.log' for reading: Отказано в доступе
tail: no files remaining
[svivanov@server.svivanov.net ~]$ sudo -i
[sudo] пароль для svivanov:
[root@server.svivanov.net ~]# tail -f /var/log/fail2ban.log
2025-12-06 10:54:40,629 fail2ban.server [16556]: INFO -----
--
2025-12-06 10:54:40,630 fail2ban.server [16556]: INFO Starting Fail2ban v1.1.0
2025-12-06 10:54:40,630 fail2ban.observer [16556]: INFO Observer start...
2025-12-06 10:54:40,637 fail2ban.database [16556]: INFO Connected to fail2ban persistent database '/var/
lib/fail2ban/fail2ban.sqlite3'
2025-12-06 10:54:40,638 fail2ban.database [16556]: WARNING New database created. Version '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
```

```
[root@server.svivanov.net ~]# touch /etc/fail2ban/jail.d/customisation.local  
[root@server.svivanov.net ~]# vim /etc/fail2ban/jail.d/customisation.local  
[root@server.svivanov.net ~]# cat /etc/fail2ban/jail.d/customisation.local  
[DEFAULT]  
bantime = 3600  
#  
# SSH servers  
#  
[sshd]  
port = ssh,2022  
enabled = true  
[sshd-ddos]  
filter = sshd  
enabled = true  
[selinux-ssh]  
enabled = true  
[root@server.svivanov.net ~]#
```

Рис. 3.5: Создание конфигурации

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

```
[root@server.svivanov.net ~]# systemctl restart fail2ban  
[root@server.svivanov.net ~]#
```

Рис. 3.6: Перезапуск fail2ban

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

```
2025-12-06 10:57:15.200 fail2ban.filter [16884]: INFO encoding: UTF-8  
2025-12-06 10:57:15.200 fail2ban.jail [16884]: INFO Creating new jail 'selinux-ssh'  
2025-12-06 10:57:15.208 fail2ban.jail [16884]: INFO Jail 'selinux-ssh' uses pyinotify {}  
2025-12-06 10:57:15.210 fail2ban.jail [16884]: INFO Initiated 'pyinotify' backend  
2025-12-06 10:57:15.211 fail2ban.datedetector [16884]: INFO date pattern '': 'Epoch'  
2025-12-06 10:57:15.211 fail2ban.filter [16884]: INFO maxRetry: 5  
2025-12-06 10:57:15.211 fail2ban.filter [16884]: INFO findtime: 600  
2025-12-06 10:57:15.211 fail2ban.actions [16884]: INFO bantime: 3600  
2025-12-06 10:57:15.211 fail2ban.filter [16884]: INFO encoding: UTF-8  
2025-12-06 10:57:15.213 fail2ban.filter [16884]: INFO Added logfile: '/var/log/audit/audit.log' (pos =  
0, hash = f216cf862ef2a1afd3f16af8bb8bf79356cc8723)  
2025-12-06 10:57:15.213 fail2ban.jail [16884]: INFO Creating new jail 'sshd-ddos'  
2025-12-06 10:57:15.213 fail2ban.jail [16884]: INFO Jail 'sshd-ddos' uses pyinotify {}  
2025-12-06 10:57:15.215 fail2ban.jail [16884]: INFO Initiated 'pyinotify' backend  
2025-12-06 10:57:15.217 fail2ban.filter [16884]: INFO maxLines: 1  
2025-12-06 10:57:15.217 fail2ban.filter [16884]: INFO maxRetry: 5  
2025-12-06 10:57:15.217 fail2ban.filter [16884]: INFO findtime: 600  
2025-12-06 10:57:15.217 fail2ban.actions [16884]: INFO bantime: 3600  
2025-12-06 10:57:15.217 fail2ban.filter [16884]: INFO encoding: UTF-8  
2025-12-06 10:57:15.219 fail2ban.jail [16884]: INFO Jail 'sshd' started  
2025-12-06 10:57:15.220 fail2ban.filtersystemd [16884]: INFO [sshd] Jail is in operation now (process new jou  
rnal entries)  
2025-12-06 10:57:15.220 fail2ban.jail [16884]: INFO Jail 'selinux-ssh' started  
2025-12-06 10:57:15.226 fail2ban.jail [16884]: INFO Jail 'sshd-ddos' started
```

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
```

```
#
# 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
[apache-shellshock]
enabled = true
-- РЕЖИМ ВСТАВКИ --
```

Рис. 3.8: Редактирование конф. файла

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

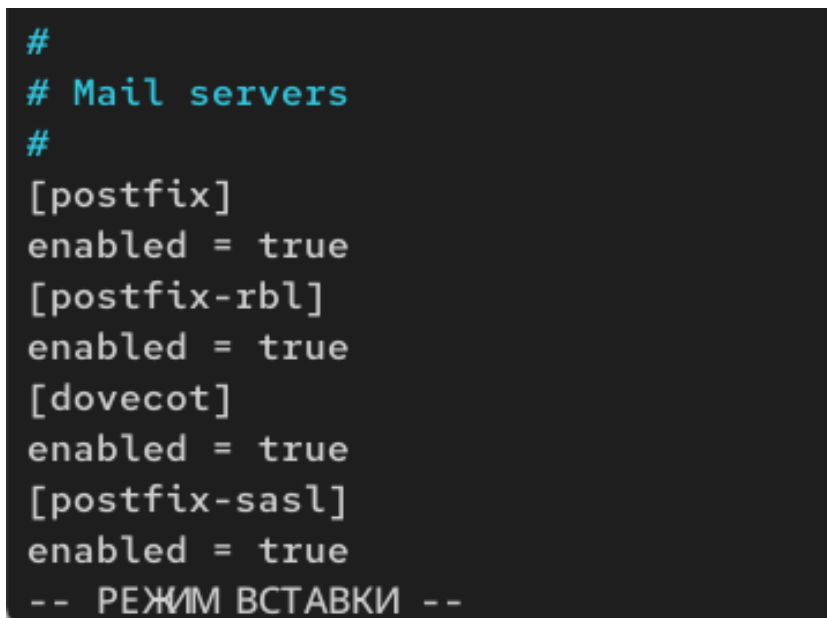
```
2025-12-06 10:59:28,626 fail2ban.filter [16968]: INFO Added logfile: '/var/log/httpd/www.svivanov.net-
error_log' (pos = 0, hash = 7968d86271e10d5ef13230bfc0d36c42962dfeaa)
2025-12-06 10:59:28,627 fail2ban.jail [16968]: INFO Creating new jail 'sshd-ddos'
2025-12-06 10:59:28,627 fail2ban.jail [16968]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-06 10:59:28,628 fail2ban.jail [16968]: INFO Initiated 'pyinotify' backend
2025-12-06 10:59:28,629 fail2ban.filter [16968]: INFO maxLines: 1
2025-12-06 10:59:28,629 fail2ban.filter [16968]: INFO maxRetry: 5
2025-12-06 10:59:28,629 fail2ban.filter [16968]: INFO findtime: 600
2025-12-06 10:59:28,629 fail2ban.actions [16968]: INFO banTime: 3600
2025-12-06 10:59:28,630 fail2ban.filter [16968]: INFO encoding: UTF-8
2025-12-06 10:59:28,630 fail2ban.filtersystemd [16968]: INFO [sshd] Jail is in operation now (process new jou
rnal entries)
2025-12-06 10:59:28,631 fail2ban.jail [16968]: INFO Jail 'sshd' started
2025-12-06 10:59:28,632 fail2ban.jail [16968]: INFO Jail 'selinux-ssh' started
2025-12-06 10:59:28,632 fail2ban.jail [16968]: INFO Jail 'apache-auth' started
2025-12-06 10:59:28,634 fail2ban.jail [16968]: INFO Jail 'apache-badbots' started
2025-12-06 10:59:28,635 fail2ban.jail [16968]: INFO Jail 'apache-noscript' started
2025-12-06 10:59:28,636 fail2ban.jail [16968]: INFO Jail 'apache-overflows' started
2025-12-06 10:59:28,637 fail2ban.jail [16968]: INFO Jail 'apache-nohome' started
2025-12-06 10:59:28,638 fail2ban.jail [16968]: INFO Jail 'apache-botsearch' started
2025-12-06 10:59:28,639 fail2ban.jail [16968]: INFO Jail 'apache-fakegooglebot' started
2025-12-06 10:59:28,640 fail2ban.jail [16968]: INFO Jail 'apache-modsecurity' started
2025-12-06 10:59:28,641 fail2ban.jail [16968]: INFO Jail 'apache-shellshock' started
2025-12-06 10:59:28,642 fail2ban.jail [16968]: INFO Jail 'sshd-ddos' started
```

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
```



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

Рис. 3.10: Редактирование конф. файла

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

```

2025-12-06 11:01:00,522 fail2ban.jail [17061]: INFO Jail 'apache-badbots' started
2025-12-06 11:01:00,523 fail2ban.jail [17061]: INFO Jail 'apache-noscript' started
2025-12-06 11:01:00,523 fail2ban.jail [17061]: INFO Jail 'apache-overflows' started
2025-12-06 11:01:00,524 fail2ban.jail [17061]: INFO Jail 'apache-nohome' started
2025-12-06 11:01:00,525 fail2ban.jail [17061]: INFO Jail 'apache-botsearch' started
2025-12-06 11:01:00,526 fail2ban.jail [17061]: INFO Jail 'apache-fakegooglebot' started
2025-12-06 11:01:00,527 fail2ban.jail [17061]: INFO Jail 'apache-modsecurity' started
2025-12-06 11:01:00,527 fail2ban.jail [17061]: INFO Jail 'apache-shellshock' started
2025-12-06 11:01:00,529 fail2ban.jail [17061]: INFO Jail 'postfix' started
2025-12-06 11:01:00,530 fail2ban.filtersystemd [17061]: INFO [postfix] Jail is in operation now (process new
journal entries)
2025-12-06 11:01:00,530 fail2ban.filtersystemd [17061]: INFO [postfix-rbl] Jail is in operation now (process
new journal entries)
2025-12-06 11:01:00,530 fail2ban.jail [17061]: INFO Jail 'postfix-rbl' started
2025-12-06 11:01:00,531 fail2ban.filtersystemd [17061]: INFO [dovecot] Jail is in operation now (process new
journal entries)
2025-12-06 11:01:00,531 fail2ban.jail [17061]: INFO Jail 'dovecot' started
2025-12-06 11:01:00,531 fail2ban.filtersystemd [17061]: INFO [postfix-sasl] Jail is in operation now (process
new journal entries)
2025-12-06 11:01:00,531 fail2ban.jail [17061]: INFO Jail 'postfix-sasl' started
2025-12-06 11:01:00,532 fail2ban.jail [17061]: INFO Jail 'sshd-ddos' started

```

Рис. 3.11: Перезапуск службы и просмотр журнала

3.2 Проверка работы Fail2ban

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

```

[root@server.svivanov.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.svivanov.net ~]#

```

Рис. 3.12: Просмотр статуса службы

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

```

[root@server.svivanov.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 + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  `-- Banned IP list:
[root@server.svivanov.net ~]#

```

Рис. 3.13: Просмотр статуса защиты SSH

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

```

[root@server.svivanov.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.svivanov.net ~]#

```

Рис. 3.14: Установка макс. кол-ва ошибок

Запускаю виртуальную машину Client. (рис. 15)

```
C:\work_asp\svivanov\vagrant>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
      client: Adapter 1: nat
      client: Adapter 2: intnet
==> client: Forwarding ports...
```

Рис. 3.15: Запуск Client

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

```
[root@client.svivanov.net ~]# ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Permission denied, please try again.
```

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)

```
[root@server.svivanov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.1.30
[root@server.svivanov.net ~]#
```

Рис. 3.17: Блокировка адреса клиента

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

```
[root@server.svivanov.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.svivanov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned: 1
   `-- Banned IP list:
[root@server.svivanov.net ~]#
```

Рис. 3.18: Разблокировка клиента

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

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
#
```

Рис. 3.19: Редактирование конф. файла

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

```
2025-12-06 11:24:25,375 fail2ban.jail [17693]: INFO Jail 'sshd' started
2025-12-06 11:24:25,375 fail2ban.jail [17693]: INFO Jail 'selinux-ssh' started
2025-12-06 11:24:25,378 fail2ban.jail [17693]: INFO Jail 'apache-auth' started
2025-12-06 11:24:25,379 fail2ban.jail [17693]: INFO Jail 'apache-badbots' started
2025-12-06 11:24:25,380 fail2ban.jail [17693]: INFO Jail 'apache-noscript' started
2025-12-06 11:24:25,380 fail2ban.jail [17693]: INFO Jail 'apache-overflows' started
2025-12-06 11:24:25,381 fail2ban.jail [17693]: INFO Jail 'apache-nohome' started
2025-12-06 11:24:25,382 fail2ban.jail [17693]: INFO Jail 'apache-botsearch' started
2025-12-06 11:24:25,383 fail2ban.jail [17693]: INFO Jail 'apache-fakegooglebot' started
2025-12-06 11:24:25,384 fail2ban.jail [17693]: INFO Jail 'apache-modsecurity' started
2025-12-06 11:24:25,384 fail2ban.jail [17693]: INFO Jail 'apache-shellshock' started
2025-12-06 11:24:25,385 fail2ban.jail [17693]: INFO Jail 'postfix' started
2025-12-06 11:24:25,386 fail2ban.filtersystemd [17693]: INFO [postfix] Jail is in operation now (process new
journal entries)
2025-12-06 11:24:25,386 fail2ban.filtersystemd [17693]: INFO [postfix-rbl] Jail is in operation now (process
new journal entries)
2025-12-06 11:24:25,386 fail2ban.jail [17693]: INFO Jail 'postfix-rbl' started
2025-12-06 11:24:25,387 fail2ban.filtersystemd [17693]: INFO [dovecot] Jail is in operation now (process new
journal entries)
2025-12-06 11:24:25,387 fail2ban.jail [17693]: INFO Jail 'dovecot' started
2025-12-06 11:24:25,387 fail2ban.filtersystemd [17693]: INFO [postfix-sasl] Jail is in operation now (process
new journal entries)
2025-12-06 11:24:25,387 fail2ban.jail [17693]: INFO Jail 'postfix-sasl' started
```

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)

```
[root@client.svivanov.net ~]# ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Permission denied, please try again.
svivanov@server.svivanov.net's password:
Permission denied, please try again.
svivanov@server.svivanov.net's password: █
```

Рис. 3.21: Попытка входа

```
[root@server.svivanov.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 + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  `-- Banned IP list:
[root@server.svivanov.net ~]#
```

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/
```

```
[root@server.svivanov.net ~]# cd /vagrant/provision/server
[root@server.svivanov.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.svivanov.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/
ct/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)

```
#!/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. 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».