

Отчёт по лабораторной работе 16

Базовая защита от атак типа «brute force»

Сейдалиев Тагиетдин Ровшенович

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Защита с помощью Fail2ban	6
2.1.1 Настройка защиты SSH	7
2.1.2 Включение защиты HTTP	8
2.1.3 Включение защиты почтовых служб	10
2.2 Проверка работы Fail2ban	12
2.3 Внесение изменений в настройки внутреннего окружения ВМ	17
3 Заключение	18
4 Контрольные вопросы	19
4.1 1. Поясните принцип работы Fail2ban.	19
4.2 2. Настройки какого файла более приоритетны: jail.conf или jail.local?	19
4.3 3. Как настроить оповещение администратора при срабатывании Fail2ban?	19
4.4 4. Поясните построчно настройки по умолчанию в /etc/fail2ban/jail.conf, относящиеся к веб-службе.	20
4.5 5. Поясните построчно настройки по умолчанию в jail.conf, относящиеся к почтовой службе.	21
4.6 6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий?	21
4.7 7. Как получить список действующих правил Fail2ban?	22
4.8 8. Как получить статистику заблокированных Fail2ban адресов?	22
4.9 9. Как разблокировать IP-адрес?	22

Список иллюстраций

2.1 Установка и запуск сервиса fail2ban	6
2.2 Первичный запуск и создание базы fail2ban	6
2.3 Локальная конфигурация Fail2ban для защиты SSH	7
2.4 Создание и запуск SSH-jails в журнале Fail2ban	8
2.5 Добавление jails для защиты HTTP-служб	9
2.6 Создание и запуск HTTP-jails в журнале Fail2ban	10
2.7 Добавление jails для защиты почтовых сервисов	11
2.8 Создание и запуск почтовых jails в журнале Fail2ban	12
2.9 Статус сервиса fail2ban	13
2.10 Статус защиты sshd	13
2.11 Установка maxretry	13
2.12 Ошибочные попытки SSH	14
2.13 IP-адрес заблокирован	14
2.14 Статус sshd с заблокированным IP	15
2.15 Разблокировка IP	15
2.16 Проверка статуса после разблокировки	16
2.17 Добавление ignoreip	16
2.18 Fail2ban игнорирует IP	17
2.19 Содержимое скрипта protect.sh	17

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 с помощью Fail2ban

Для обеспечения защиты сервера от сетевых атак и попыток подбора паролей был установлен и сконфигурирован сервис Fail2ban. После установки сервис был запущен и добавлен в автозагрузку. На скриншоте отображён результат установки пакетов и активации службы.

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

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

Рис. 2.1: Установка и запуск сервиса fail2ban

В отдельном терминале был открыт журнал `/var/log/fail2ban.log` для наблюдения за работой сервиса. В логах фиксируется запуск Fail2ban, создание новой базы данных и подключение к ней.

```
[trseidaliev@server.trseidaliev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for trseidaliev:
2025-12-11 11:02:41,375 fail2ban.server      [16733]: INFO      -----
2025-12-11 11:02:41,375 fail2ban.server      [16733]: INFO      Starting Fail2ban v1.1.0
2025-12-11 11:02:41,376 fail2ban.observer     [16733]: INFO      Observer start...
2025-12-11 11:02:41,380 fail2ban.database     [16733]: INFO      Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ba
n.sqlite3'
2025-12-11 11:02:41,381 fail2ban.database     [16733]: WARNING New database created. Version '4'
```

Рис. 2.2: Первичный запуск и создание базы fail2ban

2.1.1 Настройка защиты SSH

Для локальной конфигурации Fail2ban был создан файл /etc/fail2ban/jail.d/customisation. В него были добавлены параметры:

- время блокировки – 3600 секунд;
- защита SSH и SSH DDoS;
- включение SELinux-защиты.

Содержимое файла представлено на скриншоте:

The screenshot shows a text editor window with the following configuration file content:

```
Open ▾ +  
1 [DEFAULT]  
2 bantime = 3600  
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|
```

Рис. 2.3: Локальная конфигурация Fail2ban для защиты SSH

После перезапуска Fail2ban в журнале фиксируется создание и запуск jails:

- sshd
- sshd-ddos
- selinux-ssh

Отображаются параметры backend, количество попыток, encoding и время блокировки.

```

2025-12-11 11:06:25,815 fail2ban.server [1/434]: INFO -----
2025-12-11 11:06:25,815 fail2ban.server [17434]: INFO Starting Fail2ban v1.1.0
2025-12-11 11:06:25,815 fail2ban.observer [17434]: INFO Observer start...
2025-12-11 11:06:25,821 fail2ban.database [17434]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ba
n.sqlite3'
2025-12-11 11:06:25,822 fail2ban.jail [17434]: INFO Creating new jail 'sshd'
2025-12-11 11:06:25,824 fail2ban.jail [17434]: INFO Jail 'sshd' uses systemd {}
2025-12-11 11:06:25,826 fail2ban.jail [17434]: INFO Initiated 'systemd' backend
2025-12-11 11:06:25,826 fail2ban.filter [17434]: INFO maxLines: 1
2025-12-11 11:06:25,831 fail2ban.filtersystemd [17434]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=
sshd + _COMM=sshd-session'
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO findtime: 600
2025-12-11 11:06:25,831 fail2ban.actions [17434]: INFO banTime: 3600
2025-12-11 11:06:25,831 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,831 fail2ban.jail [17434]: INFO Creating new jail 'selinux-ssh'
2025-12-11 11:06:25,833 fail2ban.jail [17434]: INFO Jail 'selinux-ssh' uses pyinotify {}
2025-12-11 11:06:25,834 fail2ban.jail [17434]: INFO Initiated 'pyinotify' backend
2025-12-11 11:06:25,835 fail2ban.datedetector [17434]: INFO date pattern ':::: Epoch'
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,835 fail2ban.actions [17434]: INFO findtime: 600
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO banTime: 3600
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,835 fail2ban.filter [17434]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 943773af9
0a21e5e54a84e7f08f9cf468fe6551e)
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:06:25,836 fail2ban.jail [17434]: INFO Initiated 'pyinotify' backend
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO maxLines: 1
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO maxRetry: 5
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO findtime: 600
2025-12-11 11:06:25,837 fail2ban.actions [17434]: INFO banTime: 3600
2025-12-11 11:06:25,837 fail2ban.filter [17434]: INFO encoding: UTF-8
2025-12-11 11:06:25,837 fail2ban.jail [17434]: INFO Jail 'sshd' started
2025-12-11 11:06:25,838 fail2ban.jail [17434]: INFO Jail 'selinux-ssh' started
2025-12-11 11:06:25,838 fail2ban.jail [17434]: INFO Jail 'sshd-ddos' started
2025-12-11 11:06:25,839 fail2ban.filtersystemd [17434]: INFO [sshd] Jail is in operation now (process new journal entries)

```

Рис. 2.4: Создание и запуск SSH-jails в журнале Fail2ban

2.1.2 Включение защиты HTTP

Далее в конфигурационный файл были добавлены jails для защиты веб-сервера Apache, включая защиту от перебора паролей, вредоносных ботов, опасных запросов и известных уязвимостей.

Добавленные секции:

- apache-auth
- apache-badbots
- apache-noscript
- apache-overflows
- apache-nohome
- apache-botsearch
- apache-fakegooglebot
- apache-modsecurity
- apache-shellshock

Скриншот конфигурации:

```
1 [DEFAULT]
2 bantime = 3600
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-auth]
16 enabled = true
17
18 [apache-badbots]
19 enabled = true
20
21 [apache-noscript]
22 enabled = true
23
24 [apache-overflows]
25 enabled = true
26
27 [apache-nohome]
28 enabled = true
29
30 [apache-botsearch]
31 enabled = true
32
33 [apache-fakegooglebot]
34 enabled = true
35
36 [apache-modsecurity]
37 enabled = true
38
39 [apache-shellshock]
40 enabled = true
```

Рис. 2.5: Добавление jails для защиты HTTP-служб

После перезапуска Fail2ban в журнале отображается успешное создание и запуск всех HTTP-jails.

```

2025-12-11 11:09:05,881 fail2ban.jail [17802]: INFO Creating new jail 'apache-shellshock'
2025-12-11 11:09:05,881 fail2ban.jail [17802]: INFO Jail 'apache-shellshock' uses pyinotify {}
2025-12-11 11:09:05,882 fail2ban.jail [17802]: INFO Initiated 'pyinotify' backend
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO maxRetry: 1
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO findtime: 600
2025-12-11 11:09:05,882 fail2ban.actions [17802]: INFO banTime: 3600
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO encoding: UTF-8
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/server.trseidaliev.net-error_log' (pos = 0, hash = )
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = c3f7d2f2b31c82c8e57529a05ff2330425da3e45)
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 834dc9d05de26a7046271efadca06ebc418c4b23)
2025-12-11 11:09:05,882 fail2ban.filter [17802]: INFO Added logfile: '/var/log/httpd/www.trseidaliev.net-error_log' (pos = 0, hash = 98d0fcfcfc8091598a78988025c306ce0346456)
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:09:05,883 fail2ban.jail [17802]: INFO Initiated 'pyinotify' backend
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO maxLines: 1
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO maxRetry: 5
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO findtime: 600
2025-12-11 11:09:05,884 fail2ban.actions [17802]: INFO banTime: 3600
2025-12-11 11:09:05,884 fail2ban.filter [17802]: INFO encoding: UTF-8
2025-12-11 11:09:05,884 fail2ban.filtersystemd [17802]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:09:05,884 fail2ban.jail [17802]: INFO Jail 'sshd' started
2025-12-11 11:09:05,885 fail2ban.jail [17802]: INFO Jail 'selinux-ssh' started
2025-12-11 11:09:05,886 fail2ban.jail [17802]: INFO Jail 'apache-auth' started
2025-12-11 11:09:05,886 fail2ban.jail [17802]: INFO Jail 'apache-badbots' started
2025-12-11 11:09:05,887 fail2ban.jail [17802]: INFO Jail 'apache-noscript' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-overflows' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-nohome' started
2025-12-11 11:09:05,888 fail2ban.jail [17802]: INFO Jail 'apache-botsearch' started
2025-12-11 11:09:05,889 fail2ban.jail [17802]: INFO Jail 'apache-fakegooglebot' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'apache-modsecurity' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'apache-shellshock' started
2025-12-11 11:09:05,890 fail2ban.jail [17802]: INFO Jail 'sshd-ddos' started

```

Рис. 2.6: Создание и запуск HTTP-jails в журнале Fail2ban

2.1.3 Включение защиты почтовых служб

Завершающим этапом было включение защиты почтовых сервисов. Добавлены секции:

- postfix
- postfix-rbl
- dovecot
- postfix-sasl

Конфигурация на скриншоте:

```
Open ▾ +  
13 enabled = true  
14  
15 [apache-auth]  
16 enabled = true  
17  
18 [apache-badbots]  
19 enabled = true  
20  
21 [apache-noscript]  
22 enabled = true  
23  
24 [apache-overflows]  
25 enabled = true  
26  
27 [apache-nohome]  
28 enabled = true  
29  
30 [apache-botsearch]  
31 enabled = true  
32  
33 [apache-fakegooglebot]  
34 enabled = true  
35  
36 [apache-modsecurity]  
37 enabled = true  
38  
39 [apache-shellshock]  
40 enabled = true  
41  
42 [postfix]  
43 enabled = true  
44  
45 [postfix-rbl]  
46 enabled = true  
47  
48 [dovecot]  
49 enabled = true  
50  
51 [postfix-sasl]  
52 enabled = true
```

Рис. 2.7: Добавление jails для защиты почтовых сервисов

После перезапуска Fail2ban лог подтверждает создание и активацию jails для всех указанных почтовых служб.

Все SSH-, HTTP- и Mail-jails работают корректно и обрабатывают новые события журналов.

```

2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Initiated 'systemd' backend
2025-12-11 11:10:48,768 fail2ban.filtersystemd [18093]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.servi
ce _SYSTEMD_UNIT=postfix@.service'
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO maxRetry: 5
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO findtime: 600
2025-12-11 11:10:48,768 fail2ban.actions [18093]: INFO banTime: 3600
2025-12-11 11:10:48,768 fail2ban.filter [18093]: INFO encoding: UTF-8
2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:10:48,768 fail2ban.jail [18093]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:10:48,769 fail2ban.jail [18093]: INFO Initiated 'pyinotify' backend
2025-12-11 11:10:48,769 fail2ban.filter [18093]: INFO maxLines: 1
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO maxRetry: 5
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO findtime: 600
2025-12-11 11:10:48,770 fail2ban.actions [18093]: INFO banTime: 3600
2025-12-11 11:10:48,770 fail2ban.filter [18093]: INFO encoding: UTF-8
2025-12-11 11:10:48,770 fail2ban.jail [18093]: INFO Jail 'sshd' started
2025-12-11 11:10:48,770 fail2ban.filtersystemd [18093]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,771 fail2ban.jail [18093]: INFO Jail 'selinux-ssh' started
2025-12-11 11:10:48,771 fail2ban.jail [18093]: INFO Jail 'apache-auth' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-badbots' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-noscript' started
2025-12-11 11:10:48,772 fail2ban.jail [18093]: INFO Jail 'apache-overflows' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-nohome' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-botsearch' started
2025-12-11 11:10:48,773 fail2ban.jail [18093]: INFO Jail 'apache-fakegooglebot' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'apache-modsecurity' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'apache-shellshock' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'postfix' started
2025-12-11 11:10:48,774 fail2ban.jail [18093]: INFO Jail 'postfix-rbl' started
2025-12-11 11:10:48,775 fail2ban.jail [18093]: INFO Jail 'dovecot' started
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix-sasl] Jail is in operation now (process new journal entries
)
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.jail [18093]: INFO Jail 'postfix-sasl' started
2025-12-11 11:10:48,776 fail2ban.filtersystemd [18093]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:10:48,776 fail2ban.jail [18093]: INFO Jail 'sshd-ddos' started

```

Рис. 2.8: Создание и запуск почтовых jails в журнале Fail2ban

В результате сервер получил комплексную защиту: для SSH, веб-сервера Apache и почтовых служб, что обеспечивает многоуровневое предотвращение вредоносной активности.

2.2 Проверка работы Fail2ban

После настройки Fail2ban была выполнена проверка его функционирования при защите SSH-доступа.

Ниже представлены результаты выполнения всех шагов лабораторной работы.

На сервере был выполнен запрос статуса Fail2ban. В выводе отображено количество активных jails и их список:

```
[root@client.trseidaliev.net client]# ssh trseidaliev@server.trseidaliev.net
The authenticity of host 'server.trseidaliev.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.trseidaliev.net' (ED25519) to the list of known hosts.
trseidaliev@server.trseidaliev.net's password:
Permission denied, please try again.
trseidaliev@server.trseidaliev.net's password:
Permission denied, please try again.
trseidaliev@server.trseidaliev.net's password:
trseidaliev@server.trseidaliev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.trseidaliev.net client]#
```

Рис. 2.9: Статус сервиса fail2ban

Был просмотрен статус jail sshd. На момент проверки не было заблокированных IP-адресов:

```
[root@server.trseidaliev.net server]# 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-zbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set sshd maxretry 2
2
```

Рис. 2.10: Статус защиты sshd

Для тестирования блокировки был уменьшен параметр maxretry до 2 попыток:

```
[root@server.trseidaliev.net server]# 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-zbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set sshd maxretry 2
2
```

Рис. 2.11: Установка maxretry

С клиента было выполнено несколько попыток подключения к серверу по SSH с неверным паролем.

После нескольких неудачных попыток сервер отказал в доступе:

```
[root@client.trseidaliev.net client]# ssh trseidaliev@server.trseidaliev.net
The authenticity of host 'server.trseidaliev.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.trseidaliev.net' (ED25519) to the list of known hosts.
trseidaliev@server.trseidaliev.net's password:
Permission denied, please try again.
trseidaliev@server.trseidaliev.net's password:
Permission denied, please try again.
trseidaliev@server.trseidaliev.net's password:
trseidaliev@server.trseidaliev.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.trseidaliev.net client]#
```

Рис. 2.12: Ошибочные попытки SSH

После попыток входа журнал Fail2ban отразил факт блокировки IP-адреса клиента:

```
[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban                                [18598]: ERROR  NOK: ('Invalid command '192.168.1.30' (no set action or not yet implemented')
Invalid command '192.168.1.30' (no set action or not yet implemented)
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.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.trseidaliev.net server]#
```

Рис. 2.13: IP-адрес заблокирован

Статус jail sshd показывает заблокированный IP-адрес в списке:

```
[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban          [18598]: ERROR  NOK: ("Invalid command '192.168.1.30' (no set action or not yet implemented")
)
Invalid command '192.168.1.30' (no set action or not yet implemented)
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.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.trseidaliev.net server]#
```

Рис. 2.14: Статус sshd с заблокированным IP

Адрес был успешно разблокирован командой **fail2ban-client set sshd unbanip <ip>**:

```
[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban          [18598]: ERROR  NOK: ("Invalid command '192.168.1.30' (no set action or not yet implemented")
)
Invalid command '192.168.1.30' (no set action or not yet implemented)
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.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.trseidaliev.net server]#
```

Рис. 2.15: Разблокировка IP

Повторная проверка показывает, что список заблокированных IP пуст:

```

[root@server.trseidaliev.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.trseidaliev.net server]# fail2ban-client set unbanip 192.168.1.30
2025-12-11 11:14:30,306 fail2ban          [18598]: ERROR  NOK: ('Invalid command '192.168.1.30' (no set action or not yet implemented')
[root@server.trseidaliev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.trseidaliev.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.trseidaliev.net server]#

```

Рис. 2.16: Проверка статуса после разблокировки

Чтобы Fail2ban не блокировал клиентский адрес, он был добавлен в параметр `ignoreip` в файле

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

```

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

```

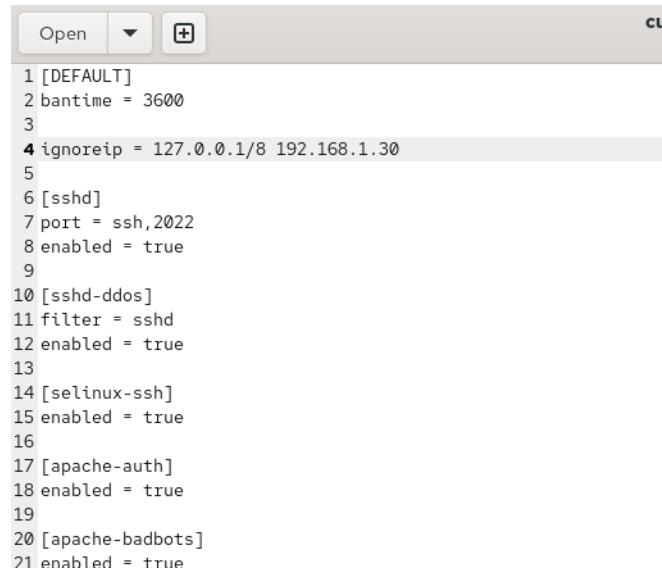


Рис. 2.17: Добавление ignoreip

После перезапуска сервиса Fail2ban в журнале появилось сообщение о том, что IP-адрес клиента игнорируется:

```
2025-12-11 11:16:09,574 fail2ban.filtersystemd [18868]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:16:09,574 fail2ban.jail [18868]: INFO Jail 'postfix-sasl' started
2025-12-11 11:16:09,574 fail2ban.jail [18868]: INFO Jail 'sshd-ddos' started

2025-12-11 11:16:19,551 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:16:23,789 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:16:27,691 fail2ban.filter [18868]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рис. 2.18: Fail2ban игнорирует IP

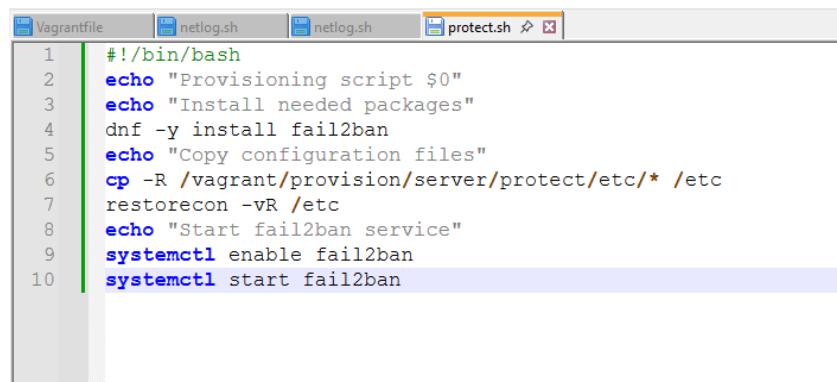
Была предпринята попытка снова войти с клиента, однако блокировка не происходила, что подтверждает правильную работу механизма ignoreip.

2.3 Внесение изменений в настройки внутреннего окружения ВМ

В каталоге `/vagrant/provision/server` был создан подкаталог `protect`, предназначенный для хранения копии настроек Fail2ban:

Был создан исполняемый файл `protect.sh`:

Его содержимое выполняет автоматическую установку Fail2ban и копирование конфигурации при развертывании стенда:



```
Vagrantfile netlog.sh netlog.sh 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
```

Рис. 2.19: Содержимое скрипта `protect.sh`

Скрипт выполняет копирование конфигурационных файлов, применение контекстов SELinux и запуск Fail2ban.

3 Заключение

В ходе выполнения работы:

- выполнена установка и базовая настройка Fail2ban на виртуальной машине `server`;
- активированы механизмы защиты для служб SSH, HTTP и почтового подсистемы, расширены настройки jails;
- проведена проверка работоспособности Fail2ban: определено состояние сервиса и отдельных jails через `fail2ban-client`;
- протестирована блокировка SSH-доступа при превышении порога ошибок авторизации, подтверждена фиксация и занесение IP-адреса клиента в список заблокированных;
- выполнена разблокировка IP-адреса клиента и проверено успешное снятие блокировки;
- внесены изменения в конфигурацию Fail2ban, включая добавление клиентского адреса в список `ignoreip`, что предотвращает его блокировку в дальнейшем;
- проанализированы записи журнала `/var/log/fail2ban.log`, подтверждающие корректность обработки запросов и игнорирование указанного IP;
- подготовлена инфраструктура для автоматизации развёртывания Fail2ban: создан каталог `protect`, экспортированы конфигурационные файлы и разработан скрипт `protect.sh` для автоматизированного применения настроек при провижининге.

4 Контрольные вопросы

4.1 1. Поясните принцип работы Fail2ban.

Fail2ban анализирует журналы системы и отслеживает повторяющиеся неудачные попытки доступа.

Если количество ошибок превышает установленный порог, Fail2ban автоматически выполняет заданное действие — чаще всего блокирует IP-адрес нарушителя с помощью правил межсетевого экрана, предотвращая дальнейшие попытки атаки.

4.2 2. Настройки какого файла более приоритетны:

jail.conf или jail.local?

Более приоритетным является файл **jail.local**.

Он предназначен для пользовательских настроек и переопределяет параметры, заданные в **jail.conf**, который служит шаблоном по умолчанию и не должен изменяться.

4.3 3. Как настроить оповещение администратора при срабатывании Fail2ban?

Для включения оповещений необходимо указать:

- параметры отправителя и получателя в секции [DEFAULT] (destemail, sender);
- действие, включающее отправку e-mail, например action_mw или action_mail.

Например, в jail-конфигурации можно указать:

```
action = %(action_mwl)s
```

что приведёт к отправке письма администратору при блокировке IP.

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

Для веб-служб используются jails, такие как apache-auth, apache-badbots, apache-noscript, apache-overflows и др.

Основные параметры:

- **enabled** — включает или отключает jail; по умолчанию отключён (false).
- **filter** — задаёт фильтр, содержащий правила поиска злонамеренных записей в логах Apache.
- **logpath** — путь к файлам журнала веб-сервера (например, /var/log/httpd/error_log).
- **maxretry** — число допустимых ошибок до блокировки.
- **bantime** — время, на которое блокируется IP-адрес.
- **findtime** — период, в течение которого учитываются ошибки.

Эти параметры определяют, какие события считаются нарушениями и как Fail2ban реагирует на них.

4.5 5. Поясните построчно настройки по умолчанию в jail.conf, относящиеся к почтовой службе.

Jails почтовых служб (postfix, postfix-sasl, dovecot, postfix-rbl) включают следующие параметры:

- **enabled** — по умолчанию отключён, требуется включение вручную.
- **filter** — определяет шаблоны поиска ошибок аутентификации или подозрительных действий в логах почтовых сервисов.
- **logpath** — путь к файлам журналов, например /var/log/maillog.
- **maxretry** — количество попыток, допускаемых до блокировки.
- **action** — определяет, что Fail2ban делает при нарушении (например, добавляет правило блокировки в Firewall).
- **port** — порты, относящиеся к почтовым сервисам (SMTP, IMAP, POP3).

Эти настройки позволяют Fail2ban защищать почтовые серверы от попыток перебора учётных данных и других атак.

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

Fail2ban может выполнять:

- блокировку IP через firewall;
- отправку уведомлений администратору;
- выполнение пользовательских скриптов;
- запись событий в отдельные журналы;
- комбинированные действия (например, блокировка + уведомление).

Описание всех доступных действий находится в каталоге:

/etc/fail2ban/action.d/

В каждом файле определено конкретное действие и его параметры.

4.7 7. Как получить список действующих правил

Fail2ban?

Список активных jails можно посмотреть командой:

fail2ban-client status

Вывод содержит перечень всех включённых правил защиты.

4.8 8. Как получить статистику заблокированных Fail2ban адресов?

Статистика по конкретному jail выводится командой:

fail2ban-client status <jail-name>

В секции **Actions** отображаются:

- количество текущих блокировок,
- общее число заблокированных IP,
- список забаненных адресов.

4.9 9. Как разблокировать IP-адрес?

Для разблокировки IP используется команда:

fail2ban-client set <jail-name> unbanip <ip-адрес>

После выполнения команды `fail2ban-client status <jail-name>` подтверждается, что адрес отсутствует в списке заблокированных.