Отчет по лабораторной работе № 16. Базовая защита от атак типа "brute force"

Данила Стариков
НПИбд-02-22

2024

Содержание

1 Цель работы

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

2 Выполнение работы

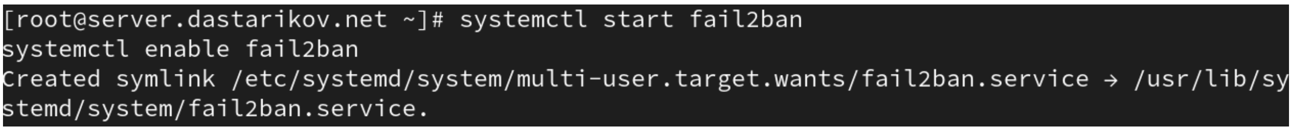
2.1 Защита с помощью Fail2ban

1. На сервере установили `fail2ban`:

   ```
   dnf -y install fail2ban
   ```

2. Запустили сервис `fail2ban` (Рис. 1):

   ```
   systemctl start fail2ban
   systemctl enable fail2ban
   ```

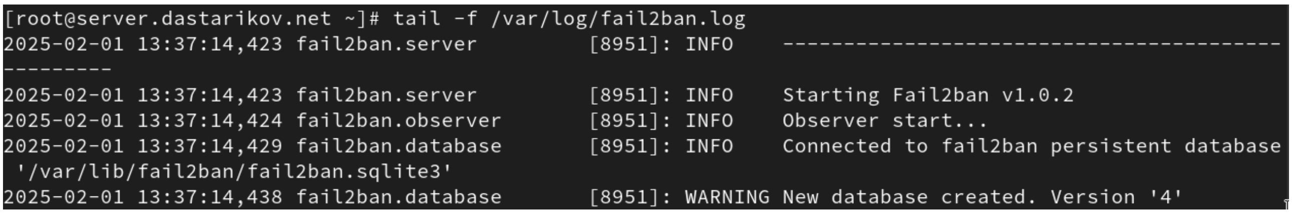


```
[root@server.dastarikov.net ~]# systemctl start fail2ban
systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/sy
stemd/system/fail2ban.service.
```

Рис. 1: Запуск сервиса `fail2ban`.

3. В дополнительном терминале запустили просмотр журнала событий `fail2ban` (Рис. 2):

   ```
   tail -f /var/log/fail2ban.log
   ```



```
[root@server.dastarikov.net ~]# tail -f /var/log/fail2ban.log
2025-02-01 13:37:14,423 fail2ban.server         [8951]: INFO    ----------------------------------------
---------
2025-02-01 13:37:14,423 fail2ban.server         [8951]: INFO    Starting Fail2ban v1.0.2
2025-02-01 13:37:14,424 fail2ban.observer       [8951]: INFO    Observer start...
2025-02-01 13:37:14,429 fail2ban.database       [8951]: INFO    Connected to fail2ban persistent database
 '/var/lib/fail2ban/fail2ban.sqlite3'
2025-02-01 13:37:14,438 fail2ban.database       [8951]: WARNING New database created. Version '4'
```

Рис. 2: Просмотр журнала событий `fail2ban`.

4. Создали файл с новой конфигурацией `fail2ban`:

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

5. В файле `/etc/fail2ban/jail.d/customisation.local`:

   - задали время блокирования на 1 час (время задаётся в секундах):

     ```
     [DEFAULT]
     bantime = 3600
     ```

   - включили защиту SSH:

     ```
     [sshd]
     port = ssh,2022
     enabled = true

     [sshd-dos]
     filter = sshd
     ```

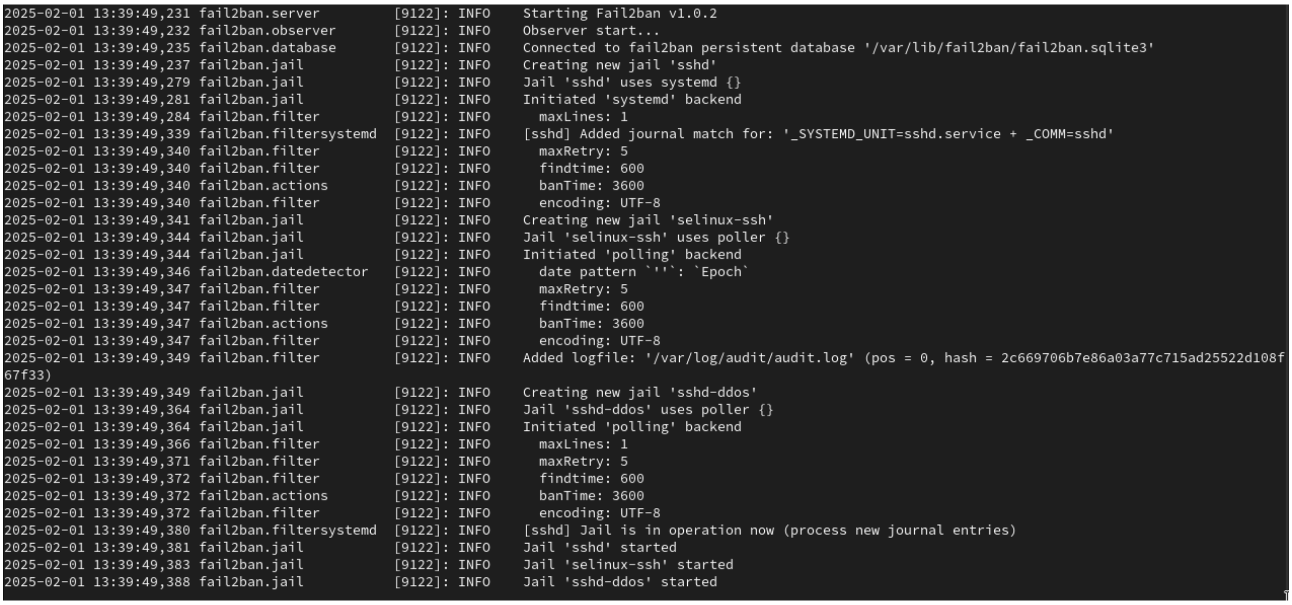
```
enabled = true

[selinux-ssh]
enabled = true
```

6. Перезапустили `fail2ban`:

   ```
   systemctl restart fail2ban
   ```

7. Просмотрели журналы событий (Рис. 3):

   ```
   tail -f /var/log/fail2ban.log
   ```



```
2025-02-01 13:39:49,231 fail2ban.server         [9122]: INFO    Starting Fail2ban v1.0.2
2025-02-01 13:39:49,232 fail2ban.observer       [9122]: INFO    Observer start...
2025-02-01 13:39:49,235 fail2ban.database       [9122]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-02-01 13:39:49,237 fail2ban.jail           [9122]: INFO    Creating new jail 'sshd'
2025-02-01 13:39:49,279 fail2ban.jail           [9122]: INFO    Jail 'sshd' uses systemd {}
2025-02-01 13:39:49,281 fail2ban.jail           [9122]: INFO    Initiated 'systemd' backend
2025-02-01 13:39:49,284 fail2ban.filter         [9122]: INFO      maxLines: 1
2025-02-01 13:39:49,339 fail2ban.filtersystemd  [9122]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2025-02-01 13:39:49,340 fail2ban.filter         [9122]: INFO      maxRetry: 5
2025-02-01 13:39:49,340 fail2ban.filter         [9122]: INFO      findtime: 600
2025-02-01 13:39:49,340 fail2ban.actions        [9122]: INFO      banTime: 3600
2025-02-01 13:39:49,340 fail2ban.filter         [9122]: INFO      encoding: UTF-8
2025-02-01 13:39:49,341 fail2ban.jail           [9122]: INFO    Creating new jail 'selinux-ssh'
2025-02-01 13:39:49,344 fail2ban.jail           [9122]: INFO    Jail 'selinux-ssh' uses poller {}
2025-02-01 13:39:49,344 fail2ban.jail           [9122]: INFO    Initiated 'polling' backend
2025-02-01 13:39:49,346 fail2ban.datedetector   [9122]: INFO      date pattern `''`: `Epoch`
2025-02-01 13:39:49,347 fail2ban.filter         [9122]: INFO      maxRetry: 5
2025-02-01 13:39:49,347 fail2ban.filter         [9122]: INFO      findtime: 600
2025-02-01 13:39:49,347 fail2ban.actions        [9122]: INFO      banTime: 3600
2025-02-01 13:39:49,347 fail2ban.filter         [9122]: INFO      encoding: UTF-8
2025-02-01 13:39:49,349 fail2ban.filter         [9122]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 2c669706b7e86a03a77c715ad25522d108f
67f33)
2025-02-01 13:39:49,349 fail2ban.jail           [9122]: INFO    Creating new jail 'sshd-ddos'
2025-02-01 13:39:49,364 fail2ban.jail           [9122]: INFO    Jail 'sshd-ddos' uses poller {}
2025-02-01 13:39:49,364 fail2ban.jail           [9122]: INFO    Initiated 'polling' backend
2025-02-01 13:39:49,366 fail2ban.filter         [9122]: INFO      maxLines: 1
2025-02-01 13:39:49,371 fail2ban.filter         [9122]: INFO      maxRetry: 5
2025-02-01 13:39:49,372 fail2ban.filter         [9122]: INFO      findtime: 600
2025-02-01 13:39:49,372 fail2ban.actions        [9122]: INFO      banTime: 3600
2025-02-01 13:39:49,372 fail2ban.filter         [9122]: INFO      encoding: UTF-8
2025-02-01 13:39:49,380 fail2ban.filtersystemd  [9122]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-02-01 13:39:49,381 fail2ban.jail           [9122]: INFO    Jail 'sshd' started
2025-02-01 13:39:49,383 fail2ban.jail           [9122]: INFO    Jail 'selinux-ssh' started
2025-02-01 13:39:49,388 fail2ban.jail           [9122]: INFO    Jail 'sshd-ddos' started
```

Рис. 3: Просмотр журнала событий после первоначальной настройки `fail2ban`.

8. В файле `/etc/fail2ban/jail.d/customisation.local` включите защиту HTTP:

   ```
   #
   # HTTP servers
   #

   [apache-auth]
   enabled = true

   [apache-badbots]
   enabled = true

   [apache-noscript]
   enabled = true

   [apache-overflows]
   enabled = true
   ```

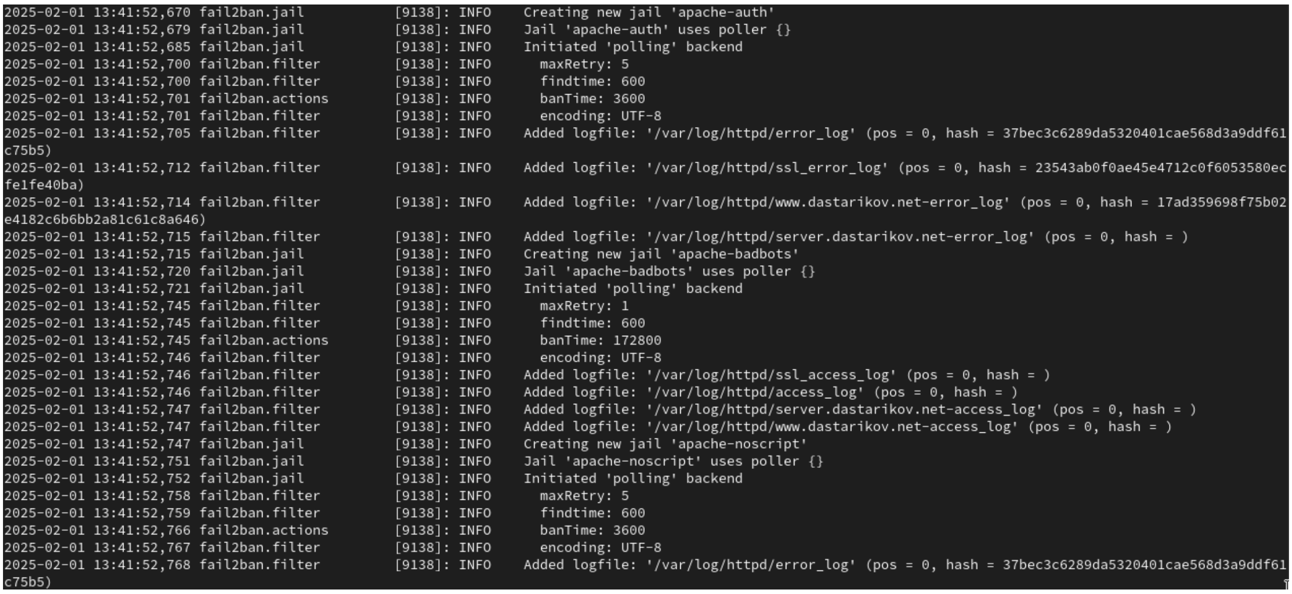
```
[apache-nohome]
enabled = true

[apache-botsearch]
enabled = true

[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true
```

9. Перезапустили `fail2ban`

   ```
   systemctl restart fail2ban
   ```

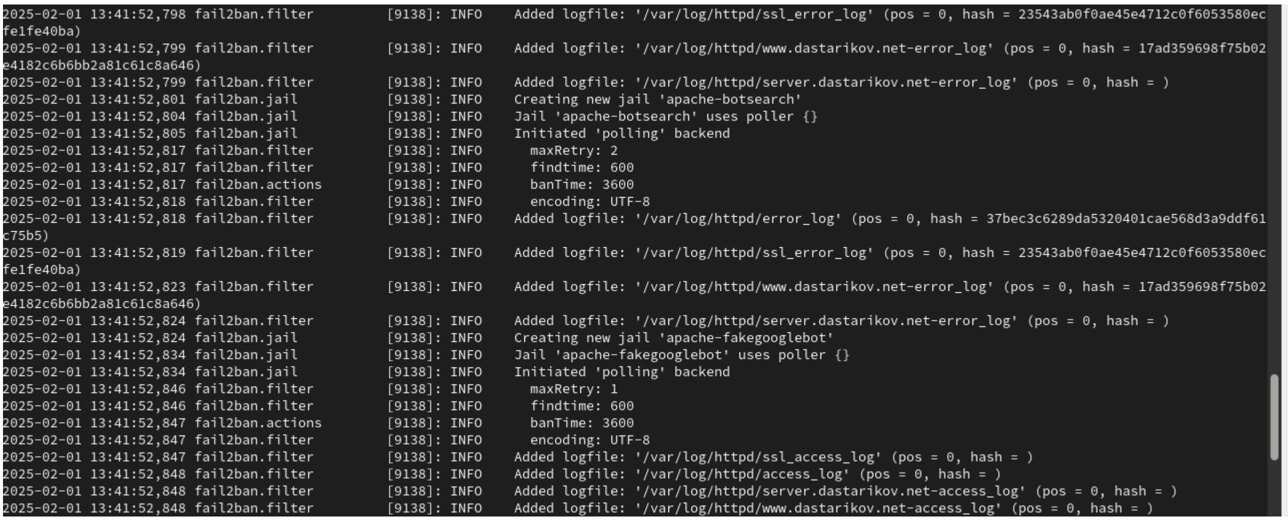
10. Посмотрели журнал событий (Рис. 4-6):

    ```
    tail -f /var/log/fail2ban.log
    ```



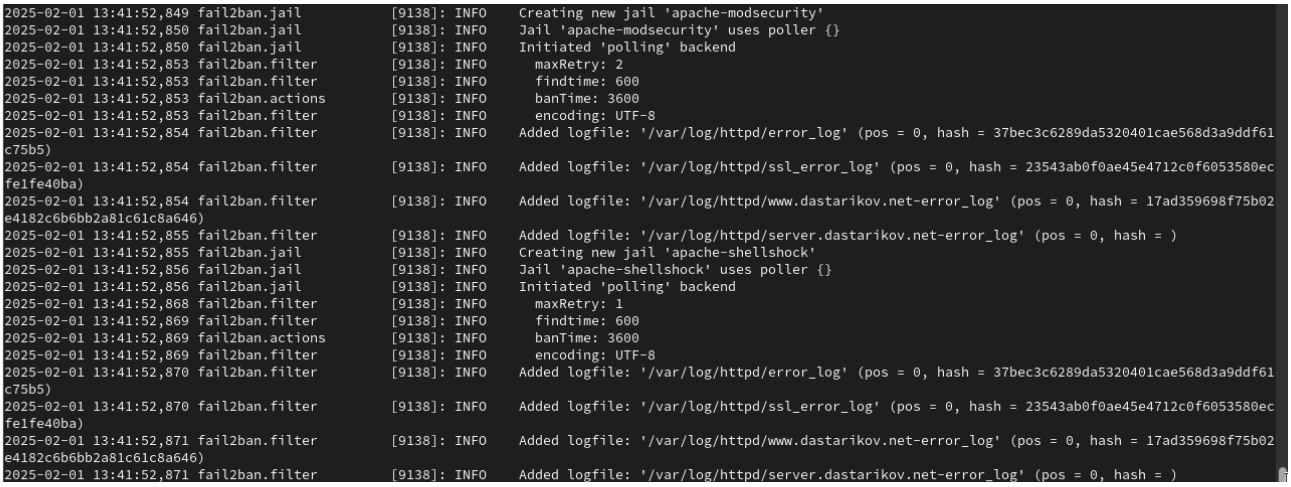
```
2025-02-01 13:41:52,670 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-auth'
2025-02-01 13:41:52,679 fail2ban.jail           [9138]: INFO    Jail 'apache-auth' uses poller {}
2025-02-01 13:41:52,685 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,700 fail2ban.filter         [9138]: INFO      maxRetry: 5
2025-02-01 13:41:52,700 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,701 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,701 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,705 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 37bec3c6289da5320401cae568d3a9ddf61
c75b5)
2025-02-01 13:41:52,712 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 23543ab0f0ae45e4712c0f6053580ec
fe1fe40ba)
2025-02-01 13:41:52,714 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-error_log' (pos = 0, hash = 17ad359698f75b02
e4182c6b6bb2a81c61c8a646)
2025-02-01 13:41:52,715 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-error_log' (pos = 0, hash = )
2025-02-01 13:41:52,715 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-badbots'
2025-02-01 13:41:52,720 fail2ban.jail           [9138]: INFO    Jail 'apache-badbots' uses poller {}
2025-02-01 13:41:52,721 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,745 fail2ban.filter         [9138]: INFO      maxRetry: 1
2025-02-01 13:41:52,745 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,745 fail2ban.actions        [9138]: INFO      banTime: 172800
2025-02-01 13:41:52,746 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,746 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_access_log' (pos = 0, hash = )
2025-02-01 13:41:52,746 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/access_log' (pos = 0, hash = )
2025-02-01 13:41:52,747 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-access_log' (pos = 0, hash = )
2025-02-01 13:41:52,747 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-access_log' (pos = 0, hash = )
2025-02-01 13:41:52,747 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-noscript'
2025-02-01 13:41:52,751 fail2ban.jail           [9138]: INFO    Jail 'apache-noscript' uses poller {}
2025-02-01 13:41:52,752 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,758 fail2ban.filter         [9138]: INFO      maxRetry: 5
2025-02-01 13:41:52,759 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,766 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,767 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,768 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 37bec3c6289da5320401cae568d3a9ddf61
c75b5)
```

Рис. 4: Логи, связанные с защитой HTTP (Часть 1).



```
2025-02-01 13:41:52,798 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 23543ab0f0ae45e4712c0f6053580ec
fe1fe40ba)
2025-02-01 13:41:52,799 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-error_log' (pos = 0, hash = 17ad359698f75b02
e4182c6b6bb2a81c61c8a646)
2025-02-01 13:41:52,799 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-error_log' (pos = 0, hash = )
2025-02-01 13:41:52,801 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-botsearch'
2025-02-01 13:41:52,804 fail2ban.jail           [9138]: INFO    Jail 'apache-botsearch' uses poller {}
2025-02-01 13:41:52,805 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,817 fail2ban.filter         [9138]: INFO      maxRetry: 2
2025-02-01 13:41:52,817 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,817 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,818 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,818 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 37bec3c6289da5320401cae568d3a9ddf61
c75b5)
2025-02-01 13:41:52,819 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 23543ab0f0ae45e4712c0f6053580ec
fe1fe40ba)
2025-02-01 13:41:52,823 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-error_log' (pos = 0, hash = 17ad359698f75b02
e4182c6b6bb2a81c61c8a646)
2025-02-01 13:41:52,824 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-error_log' (pos = 0, hash = )
2025-02-01 13:41:52,824 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-fakegooglebot'
2025-02-01 13:41:52,834 fail2ban.jail           [9138]: INFO    Jail 'apache-fakegooglebot' uses poller {}
2025-02-01 13:41:52,834 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,846 fail2ban.filter         [9138]: INFO      maxRetry: 1
2025-02-01 13:41:52,846 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,847 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,847 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,847 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_access_log' (pos = 0, hash = )
2025-02-01 13:41:52,848 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/access_log' (pos = 0, hash = )
2025-02-01 13:41:52,848 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-access_log' (pos = 0, hash = )
2025-02-01 13:41:52,848 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-access_log' (pos = 0, hash = )
```

Рис. 5: Логи, связанные с защитой HTTP (Часть 2).



```
2025-02-01 13:41:52,849 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-modsecurity'
2025-02-01 13:41:52,850 fail2ban.jail           [9138]: INFO    Jail 'apache-modsecurity' uses poller {}
2025-02-01 13:41:52,850 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,853 fail2ban.filter         [9138]: INFO      maxRetry: 2
2025-02-01 13:41:52,853 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,853 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,853 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,854 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 37bec3c6289da5320401cae568d3a9ddf61
c75b5)
2025-02-01 13:41:52,854 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 23543ab0f0ae45e4712c0f6053580ec
fe1fe40ba)
2025-02-01 13:41:52,854 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-error_log' (pos = 0, hash = 17ad359698f75b02
e4182c6b6bb2a81c61c8a646)
2025-02-01 13:41:52,855 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-error_log' (pos = 0, hash = )
2025-02-01 13:41:52,855 fail2ban.jail           [9138]: INFO    Creating new jail 'apache-shellshock'
2025-02-01 13:41:52,856 fail2ban.jail           [9138]: INFO    Jail 'apache-shellshock' uses poller {}
2025-02-01 13:41:52,856 fail2ban.jail           [9138]: INFO    Initiated 'polling' backend
2025-02-01 13:41:52,868 fail2ban.filter         [9138]: INFO      maxRetry: 1
2025-02-01 13:41:52,869 fail2ban.filter         [9138]: INFO      findtime: 600
2025-02-01 13:41:52,869 fail2ban.actions        [9138]: INFO      banTime: 3600
2025-02-01 13:41:52,869 fail2ban.filter         [9138]: INFO      encoding: UTF-8
2025-02-01 13:41:52,870 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 37bec3c6289da5320401cae568d3a9ddf61
c75b5)
2025-02-01 13:41:52,870 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 23543ab0f0ae45e4712c0f6053580ec
fe1fe40ba)
2025-02-01 13:41:52,871 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/www.dastarikov.net-error_log' (pos = 0, hash = 17ad359698f75b02
e4182c6b6bb2a81c61c8a646)
2025-02-01 13:41:52,871 fail2ban.filter         [9138]: INFO    Added logfile: '/var/log/httpd/server.dastarikov.net-error_log' (pos = 0, hash = )
```

Рис. 6: Логи, связанные с защитой HTTP (Часть 3).

11. В файле `/etc/fail2ban/jail.d/customisation.local` включите защиту почты:

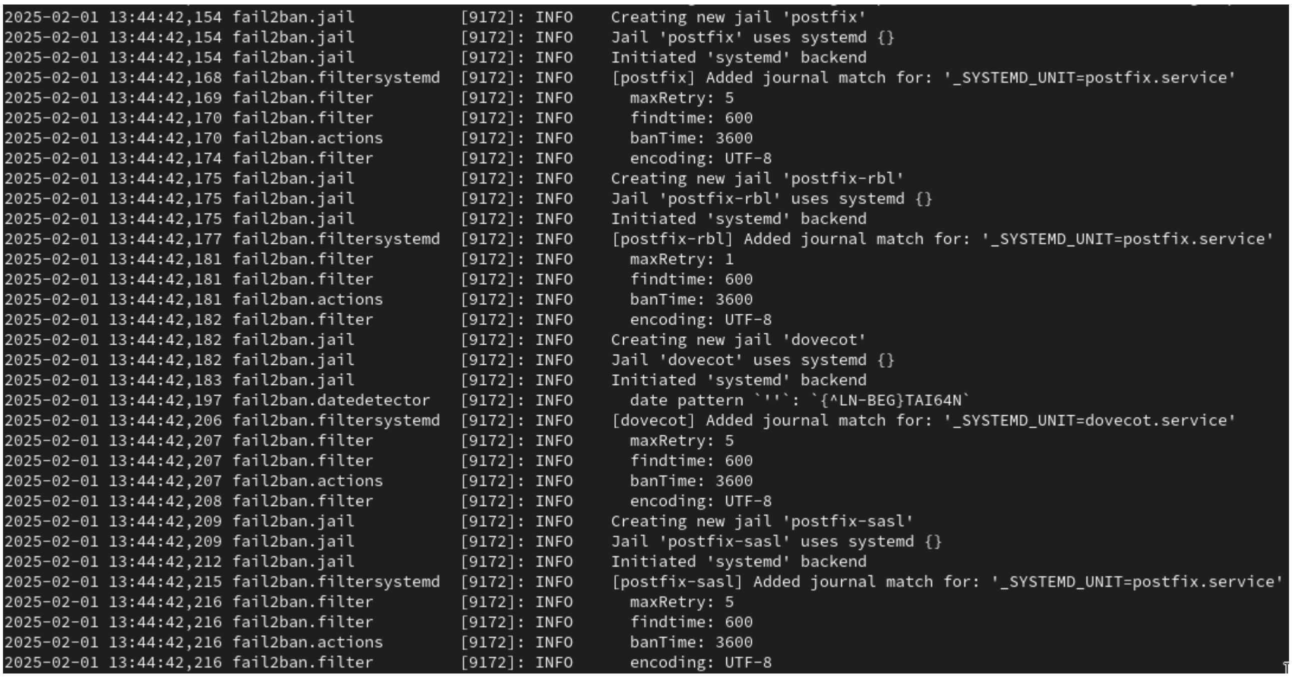
```
#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
```

12. Перезапустили fail2ban:

    ```
    systemctl restart fail2ban
    ```

13. Посмотрели журнал событий (Рис. 7):

    ```
    tail -f /var/log/fail2ban.log
    ```



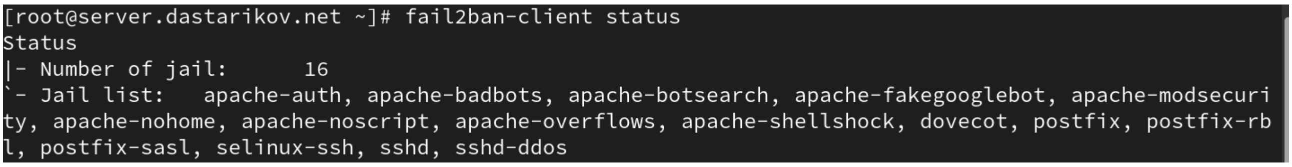
```
2025-02-01 13:44:42,154 fail2ban.jail           [9172]: INFO    Creating new jail 'postfix'
2025-02-01 13:44:42,154 fail2ban.jail           [9172]: INFO    Jail 'postfix' uses systemd {}
2025-02-01 13:44:42,154 fail2ban.jail           [9172]: INFO    Initiated 'systemd' backend
2025-02-01 13:44:42,168 fail2ban.filtersystemd  [9172]: INFO    [postfix] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2025-02-01 13:44:42,169 fail2ban.filter         [9172]: INFO      maxRetry: 5
2025-02-01 13:44:42,170 fail2ban.filter         [9172]: INFO      findtime: 600
2025-02-01 13:44:42,170 fail2ban.actions        [9172]: INFO      banTime: 3600
2025-02-01 13:44:42,174 fail2ban.filter         [9172]: INFO      encoding: UTF-8
2025-02-01 13:44:42,175 fail2ban.jail           [9172]: INFO    Creating new jail 'postfix-rbl'
2025-02-01 13:44:42,175 fail2ban.jail           [9172]: INFO    Jail 'postfix-rbl' uses systemd {}
2025-02-01 13:44:42,175 fail2ban.jail           [9172]: INFO    Initiated 'systemd' backend
2025-02-01 13:44:42,177 fail2ban.filtersystemd  [9172]: INFO    [postfix-rbl] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2025-02-01 13:44:42,181 fail2ban.filter         [9172]: INFO      maxRetry: 1
2025-02-01 13:44:42,181 fail2ban.filter         [9172]: INFO      findtime: 600
2025-02-01 13:44:42,181 fail2ban.actions        [9172]: INFO      banTime: 3600
2025-02-01 13:44:42,182 fail2ban.filter         [9172]: INFO      encoding: UTF-8
2025-02-01 13:44:42,182 fail2ban.jail           [9172]: INFO    Creating new jail 'dovecot'
2025-02-01 13:44:42,182 fail2ban.jail           [9172]: INFO    Jail 'dovecot' uses systemd {}
2025-02-01 13:44:42,183 fail2ban.jail           [9172]: INFO    Initiated 'systemd' backend
2025-02-01 13:44:42,197 fail2ban.datedetector   [9172]: INFO      date pattern `''`: `{^LN-BEG}TAI64N`
2025-02-01 13:44:42,206 fail2ban.filtersystemd  [9172]: INFO    [dovecot] Added journal match for: '_SYSTEMD_UNIT=dovecot.service'
2025-02-01 13:44:42,207 fail2ban.filter         [9172]: INFO      maxRetry: 5
2025-02-01 13:44:42,207 fail2ban.filter         [9172]: INFO      findtime: 600
2025-02-01 13:44:42,207 fail2ban.actions        [9172]: INFO      banTime: 3600
2025-02-01 13:44:42,208 fail2ban.filter         [9172]: INFO      encoding: UTF-8
2025-02-01 13:44:42,209 fail2ban.jail           [9172]: INFO    Creating new jail 'postfix-sasl'
2025-02-01 13:44:42,209 fail2ban.jail           [9172]: INFO    Jail 'postfix-sasl' uses systemd {}
2025-02-01 13:44:42,212 fail2ban.jail           [9172]: INFO    Initiated 'systemd' backend
2025-02-01 13:44:42,215 fail2ban.filtersystemd  [9172]: INFO    [postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2025-02-01 13:44:42,216 fail2ban.filter         [9172]: INFO      maxRetry: 5
2025-02-01 13:44:42,216 fail2ban.filter         [9172]: INFO      findtime: 600
2025-02-01 13:44:42,216 fail2ban.actions        [9172]: INFO      banTime: 3600
2025-02-01 13:44:42,216 fail2ban.filter         [9172]: INFO      encoding: UTF-8
```

Рис. 7: Логи, связанные с защитой почты.

2.2 Проверка работы Fail2ban

1. На сервере посмотрели статус fail2ban (Рис. 8):

    ```
    fail2ban-client status
    ```

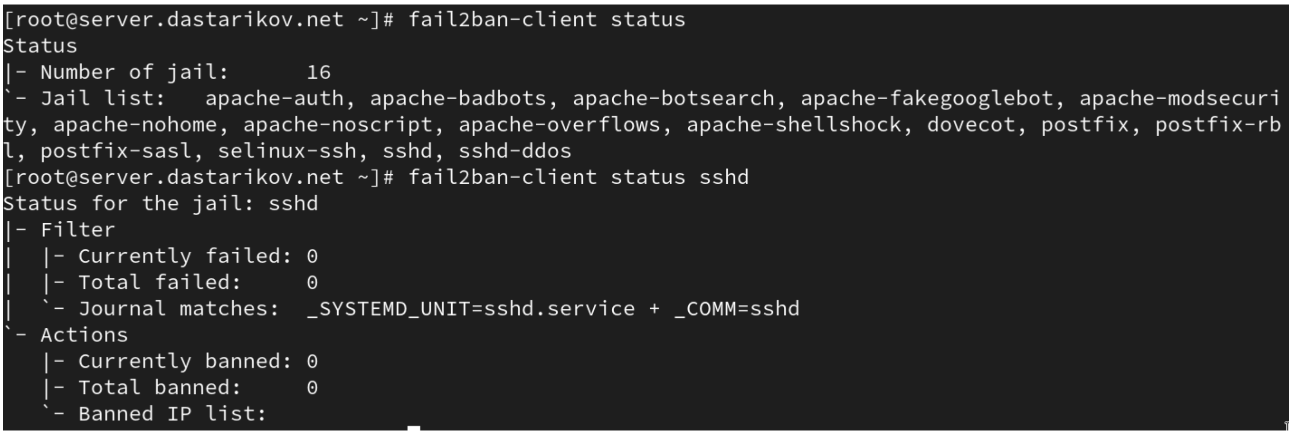


```
[root@server.dastarikov.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecuri
ty, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rb
l, postfix-sasl, selinux-ssh, sshd, sshd-ddos
```

Рис. 8: Просмотр статуса fail2ban.

2. Посмотрели статус защиты SSH и fail2ban (Рис. 9):

    ```
    fail2ban-client status sshd
    ```

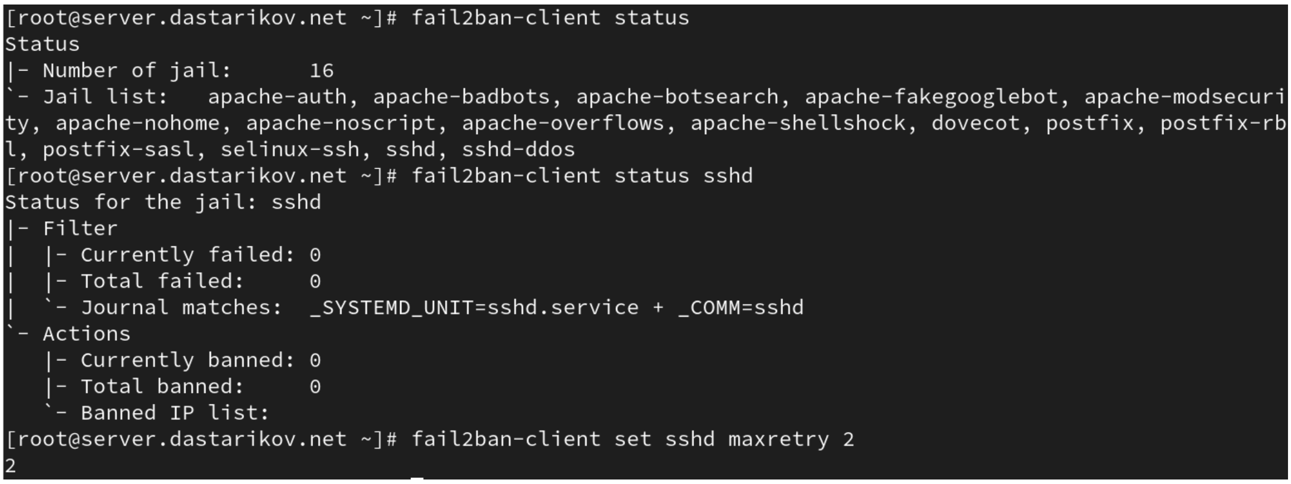


```
[root@server.dastarikov.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecuri
ty, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rb
l, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dastarikov.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:
```

Рис. 9: Просмотр статуса защиты SSH.

3. Установили максимальное количество ошибок для SSH, равное 2 (Рис. 10):

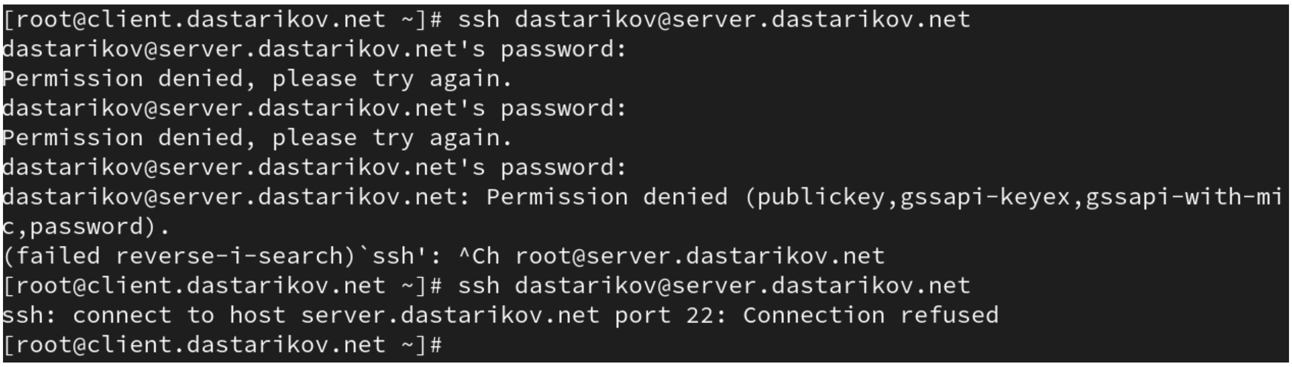
```
fail2ban-client set sshd maxretry 2
```



```
[root@server.dastarikov.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecuri
ty, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rb
l, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dastarikov.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.dastarikov.net ~]# fail2ban-client set sshd maxretry 2
2
```

Рис. 10: Установка максимального количества ошибок для SSH.

4. С клиента попытались зайти по SSH на сервер с неправильным паролем (Рис. 11).



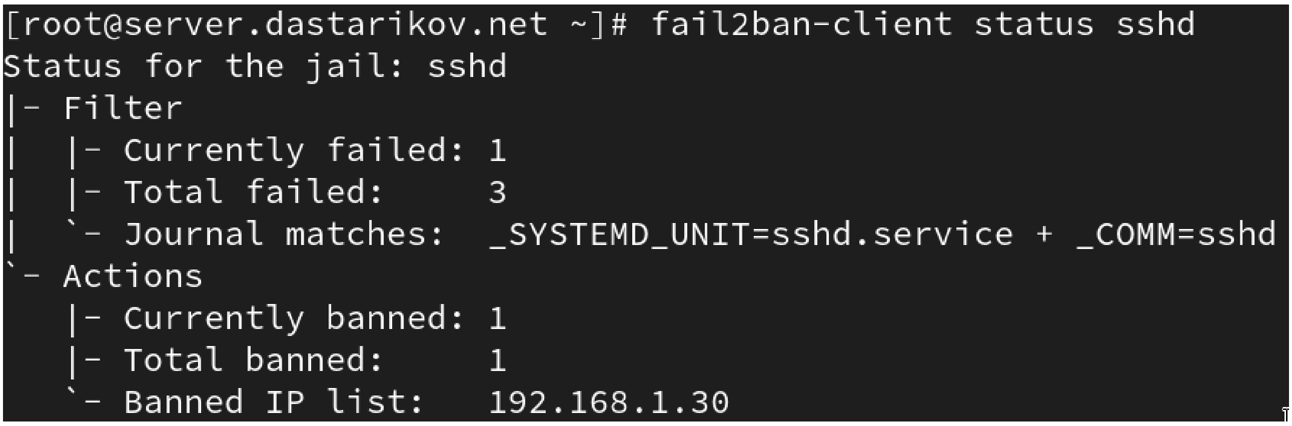
```
[root@client.dastarikov.net ~]# ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
dastarikov@server.dastarikov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mi
c,password).
(failed reverse-i-search)`ssh': ^Ch root@server.dastarikov.net
[root@client.dastarikov.net ~]# ssh dastarikov@server.dastarikov.net
ssh: connect to host server.dastarikov.net port 22: Connection refused
[root@client.dastarikov.net ~]#
```

Рис. 11: Попытка зайти на сервер через SSH с неправильным паролем.

5. На сервере посмотрели статус SSH (Рис. 12):

   ```
   fail2ban-client status sshd
   ```

6. Убедились, что произошла блокировка адреса клиента (Рис. 12).



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

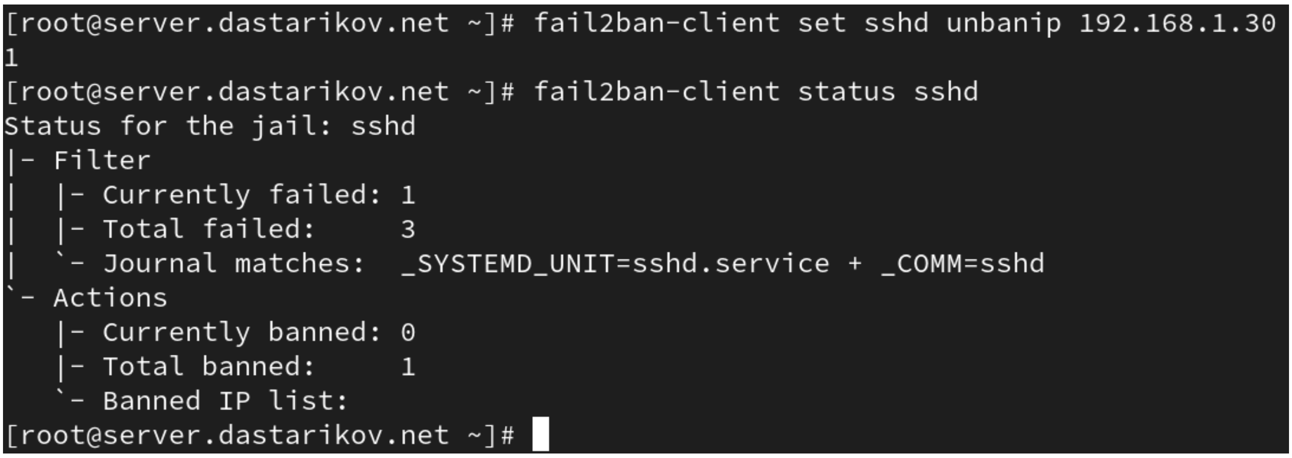
Рис. 12: Просмотр статуса защиты SSH.

7. Разблокировали IP-адрес клиента (Рис. 13):

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

8. Вновь посмотрели статус защиты SSH (Рис. 13):

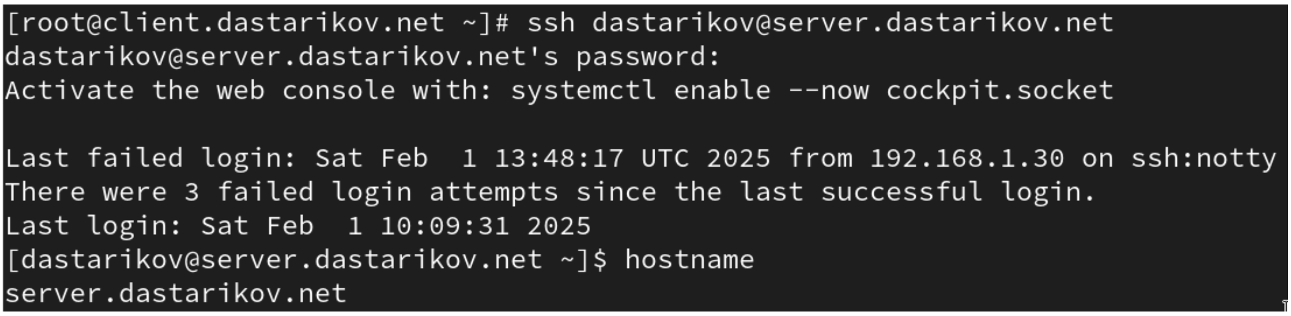
   ```
   fail2ban-client status sshd
   ```



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

Рис. 13: Разблокировка ip-адреса клиента.

Убедились, что блокировка клиента снята.



```
[root@client.dastarikov.net ~]# ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Feb  1 13:48:17 UTC 2025 from 192.168.1.30 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Sat Feb  1 10:09:31 2025
[dastarikov@server.dastarikov.net ~]$ hostname
server.dastarikov.net
```

Рис. 14: Проверка снятия блокировки.

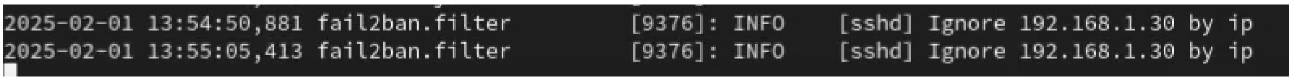
9. На сервере внесли изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation` добавив в раздел по умолчанию игнорирование адреса клиента

```
[DEFAULT]
bantime = 3600

ingoreip = 127.0.0.1/8 192.168.1.30
```

10. Перезапустили `fail2ban`.

11. Посмотрели журнал событий (Рис. 15):

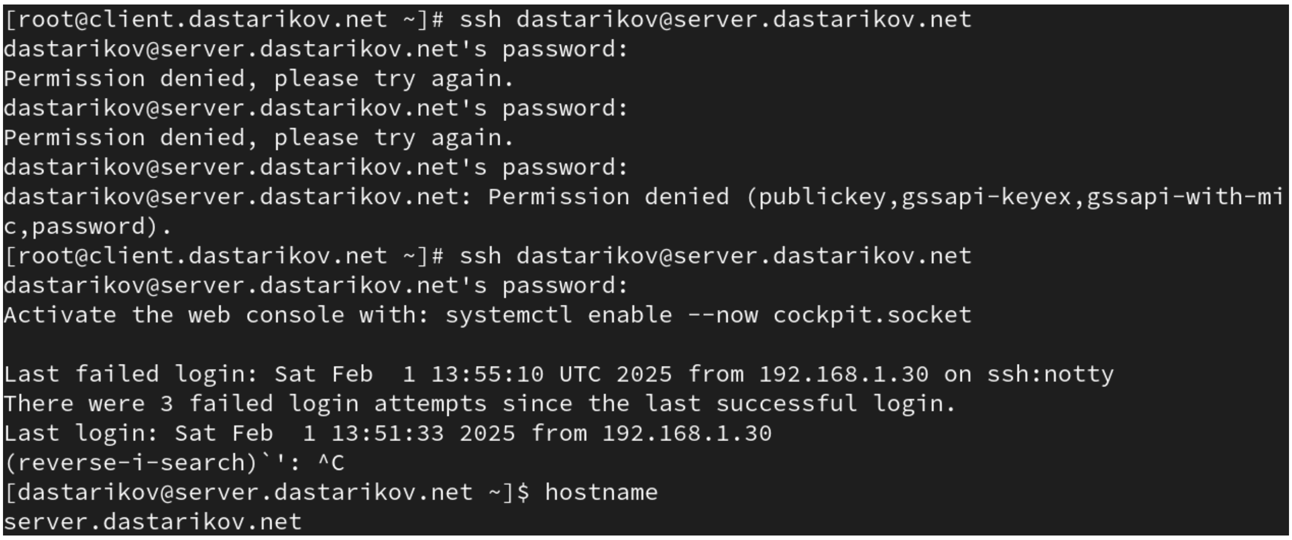
```
tail -f /var/log/fail2ban.log
```



```
2025-02-01 13:54:50,881 fail2ban.filter         [9376]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-02-01 13:55:05,413 fail2ban.filter         [9376]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

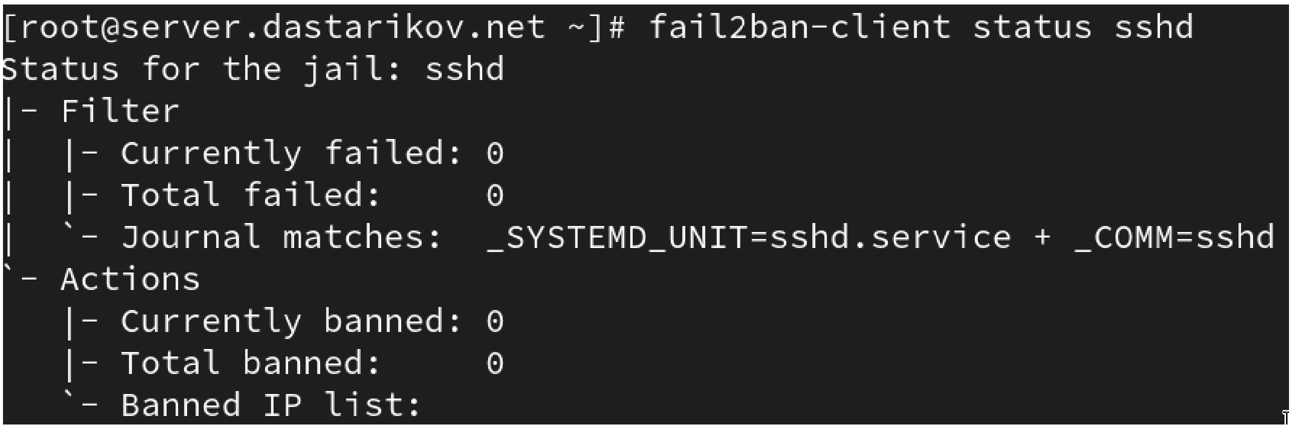
Рис. 15: Логи журнала об игнорировании адреса клиента.

12. Вновь попытались войти с клиента на сервер с неправильным паролем (Рис. 16) и посмотрели статус защиты SSH (Рис. 17).



```
[root@client.dastarikov.net ~]# ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
Permission denied, please try again.
dastarikov@server.dastarikov.net's password:
dastarikov@server.dastarikov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mi
c,password).
[root@client.dastarikov.net ~]# ssh dastarikov@server.dastarikov.net
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Feb  1 13:55:10 UTC 2025 from 192.168.1.30 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Sat Feb  1 13:51:33 2025 from 192.168.1.30
(reverse-i-search)`': ^C
[dastarikov@server.dastarikov.net ~]$ hostname
server.dastarikov.net
```

Рис. 16: Демонстрация игнорирования безуспешных попыток подключения по SSH.



```
[root@server.dastarikov.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:
```

Рис. 17: Просмотр информации о защите SSH.

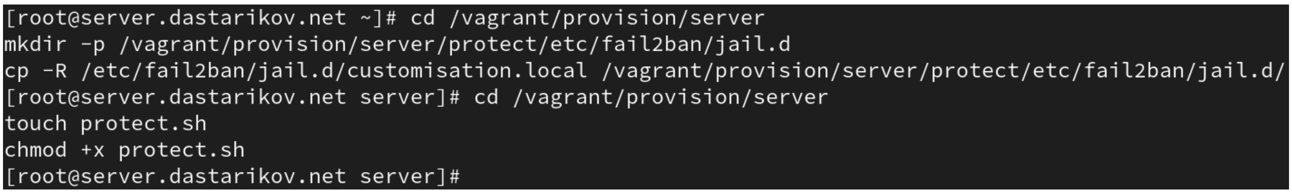
2.3 Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создали в нём каталог `protect`, в который поместили в соответствующие подкаталоги конфигурационные файлы (Рис. 18):

   ```
   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/
   ```

2. В терминале `/vagrant/provision/server` создали исполняемый файл `protect.sh` (Рис. 18):

   ```
   cd /vagrant/provision/server
   touch protect.sh
   chmod +x protect.sh
   ```



```
[root@server.dastarikov.net ~]# 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.dastarikov.net server]# cd /vagrant/provision/server
touch protect.sh
chmod +x protect.sh
[root@server.dastarikov.net server]#
```

Рис. 18: Настройка внутреннего окружения сервера.

Открыли его для редактирования, написали в нём следующий скрипт:

```
#!/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
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавили в соответствующем разделе конфигураций для сервера:

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

3 Выводы

Во время выполнения лабораторной работы получили навыки настройки обеспечения базовой защиты от атак типа "brute force"с помощью программы Fail2ban.