

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №16

дисциплина: Администрирование сетевых подсистем

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

МОСКВА

2023 г.

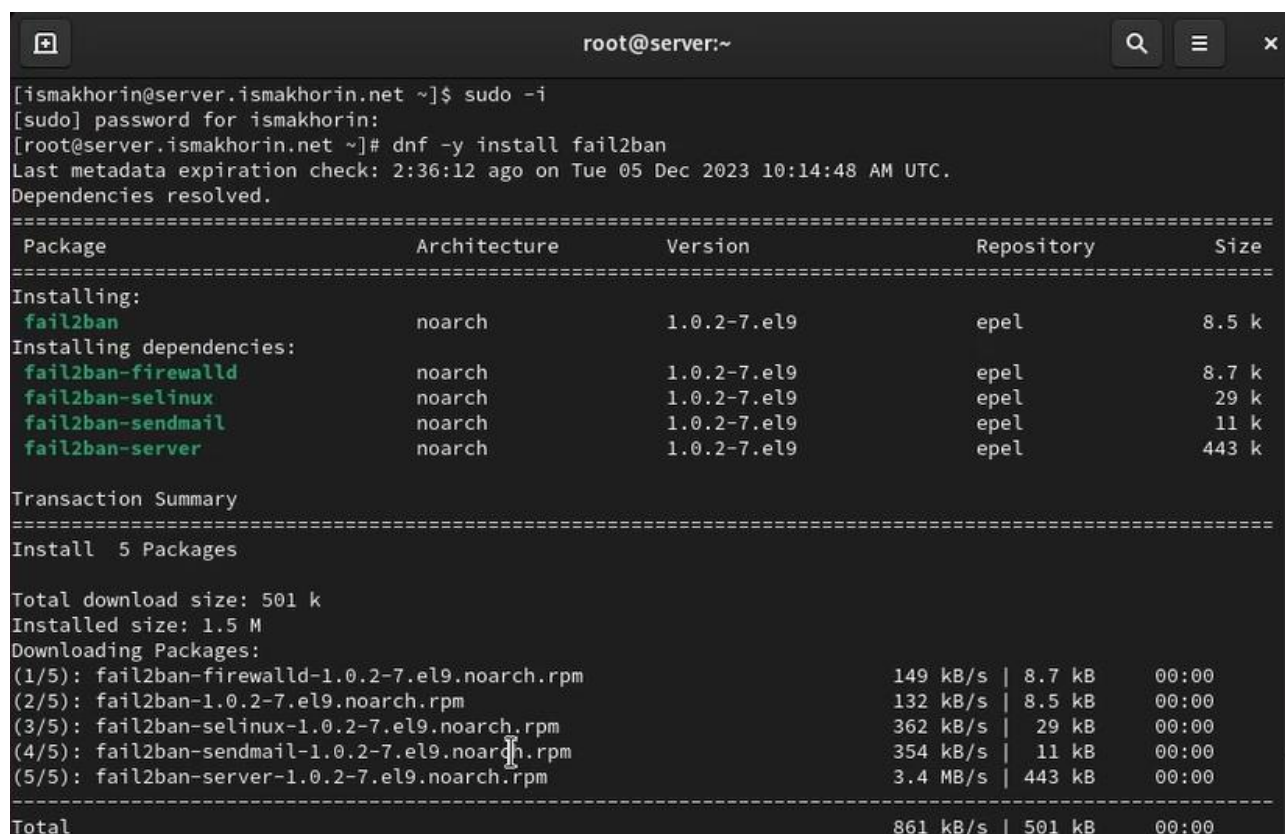
Цель работы:

Целью данной работы является получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

Выполнение работы:

На сервере установим fail2ban (Рис. 1.1):

```
dnf -y install fail2ban
```



```
root@server:~  
[ismakhorin@server.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@server.ismakhorin.net ~]# dnf -y install fail2ban  
Last metadata expiration check: 2:36:12 ago on Tue 05 Dec 2023 10:14:48 AM UTC.  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
Installing:				
fail2ban	noarch	1.0.2-7.el9	epel	8.5 k
Installing dependencies:				
fail2ban-firewalld	noarch	1.0.2-7.el9	epel	8.7 k
fail2ban-selinux	noarch	1.0.2-7.el9	epel	29 k
fail2ban-sendmail	noarch	1.0.2-7.el9	epel	11 k
fail2ban-server	noarch	1.0.2-7.el9	epel	443 k

```
Transaction Summary  
=====
```

Transaction Summary			
Install 5 Packages			
Total download size: 501 k			
Installed size: 1.5 M			
Downloading Packages:			
(1/5): fail2ban-firewalld-1.0.2-7.el9.noarch.rpm	149 kB/s	8.7 kB	00:00
(2/5): fail2ban-1.0.2-7.el9.noarch.rpm	132 kB/s	8.5 kB	00:00
(3/5): fail2ban-selinux-1.0.2-7.el9.noarch.rpm	362 kB/s	29 kB	00:00
(4/5): fail2ban-sendmail-1.0.2-7.el9.noarch.rpm	354 kB/s	11 kB	00:00
(5/5): fail2ban-server-1.0.2-7.el9.noarch.rpm	3.4 MB/s	443 kB	00:00

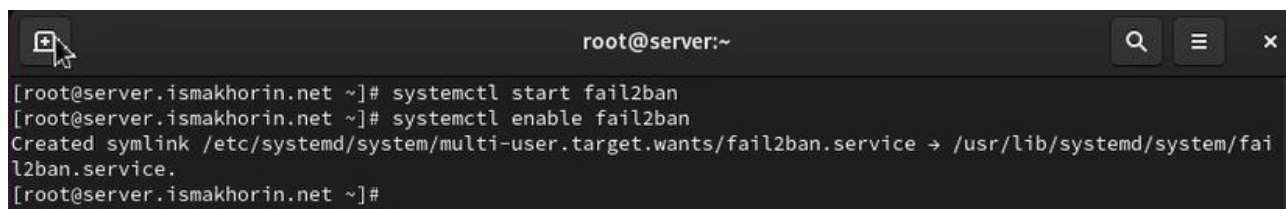
Total	861 kB/s	501 kB	00:00

Рис. 1.1. Установка на сервере fail2ban.

Запустим сервер fail2ban (Рис. 1.2):

```
systemctl start fail2ban
```

```
systemctl enable fail2ban
```

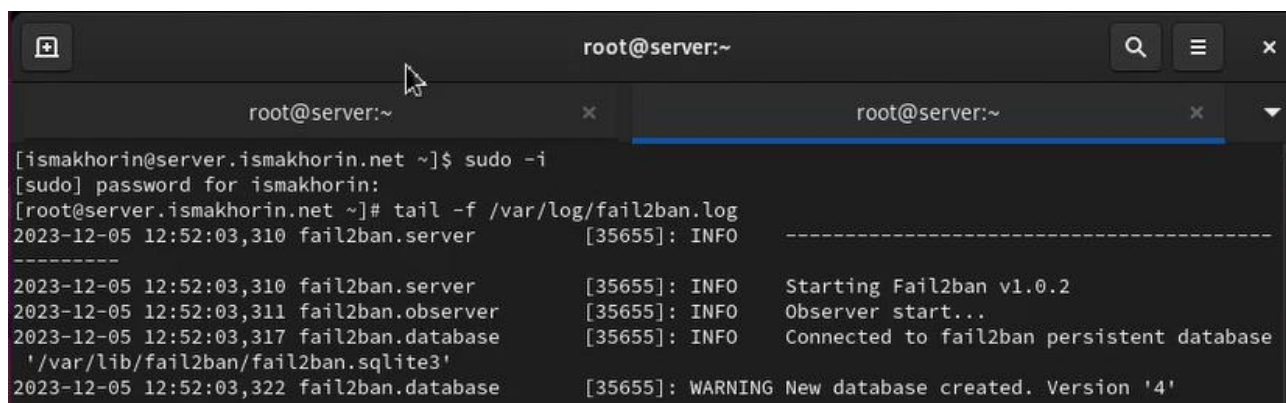


```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl start fail2ban  
[root@server.ismakhorin.net ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.  
[root@server.ismakhorin.net ~]#
```

Рис. 1.2. Запуск сервера fail2ban.

В дополнительном терминале запустим просмотр журнала событий fail2ban (Рис. 1.3):

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

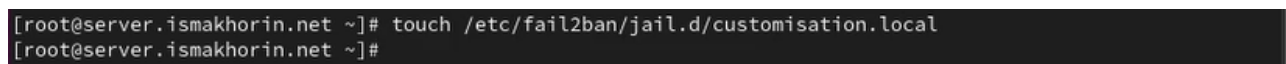


```
root@server:~  
[ismakhorin@server.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@server.ismakhorin.net ~]# tail -f /var/log/fail2ban.log  
2023-12-05 12:52:03,310 fail2ban.server [35655]: INFO -----  
-----  
2023-12-05 12:52:03,310 fail2ban.server [35655]: INFO Starting Fail2ban v1.0.2  
2023-12-05 12:52:03,311 fail2ban.observer [35655]: INFO Observer start...  
2023-12-05 12:52:03,317 fail2ban.database [35655]: INFO Connected to fail2ban persistent database  
'/var/lib/fail2ban/fail2ban.sqlite3'  
2023-12-05 12:52:03,322 fail2ban.database [35655]: WARNING New database created. Version '4'
```

Рис. 1.3. Запуск просмотра в дополнительном терминале журнала событий fail2ban.

Создадим файл с локальной конфигурацией fail2ban (Рис. 1.4):

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



```
[root@server.ismakhorin.net ~]# touch /etc/fail2ban/jail.d/customisation.local  
[root@server.ismakhorin.net ~]#
```

Рис. 1.4. Создание файла с локальной конфигурацией fail2ban.

В файле /etc/fail2ban/jail.d/customisation.local зададим время блокирования на 1 час и включим защиту SSH (Рис. 1.5):



Рис. 1.5. Настройка в файле `/etc/fail2ban/jail.d/customisation.local` времени блокирования на 1 час и включение защиты SSH.

Перезапустим fail2ban (Рис. 1.6):

```
systemctl restart fail2ban
```

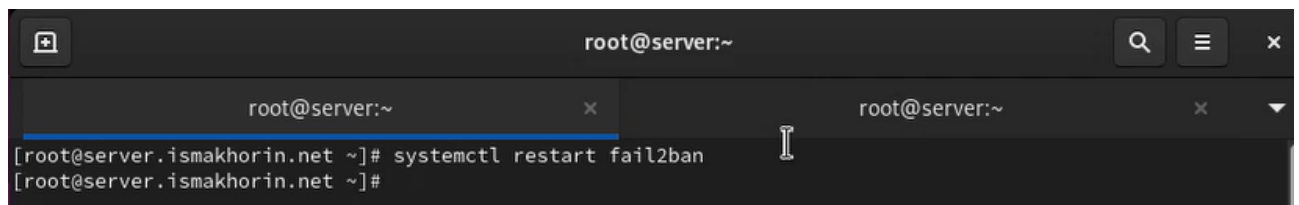


Рис. 1.6. Перезапуск fail2ban.

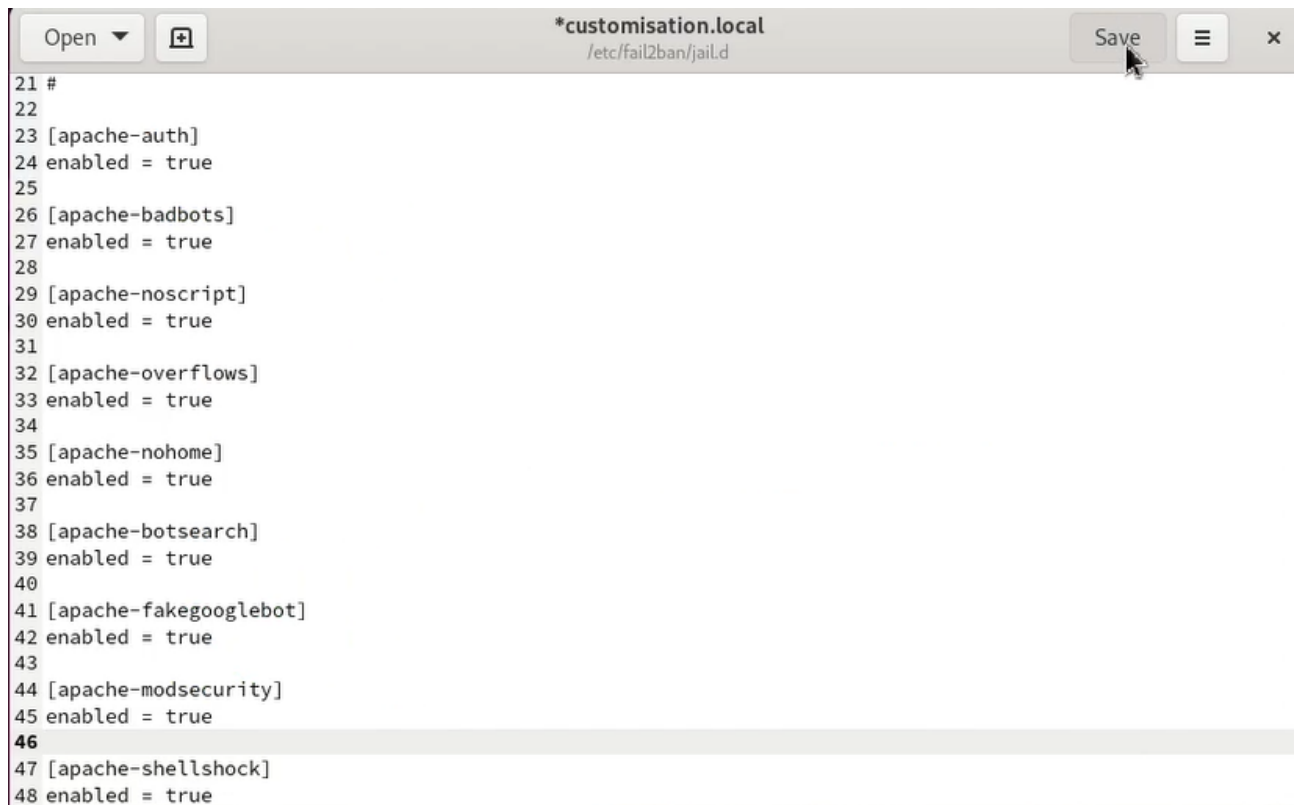
Посмотрим журнал событий (Рис. 1.7):

The screenshot shows a terminal window with two tabs. The active tab displays the following log output:

```
2023-12-05 12:53:39,264 fail2ban.filter [35778]: INFO maxRetry: 5
2023-12-05 12:53:39,265 fail2ban.filter [35778]: INFO findtime: 600
2023-12-05 12:53:39,265 fail2ban.actions [35778]: INFO banTime: 3600
2023-12-05 12:53:39,266 fail2ban.filter [35778]: INFO encoding: UTF-8
2023-12-05 12:53:39,274 fail2ban.jail [35778]: INFO Creating new jail 'selinux-ssh'
2023-12-05 12:53:39,289 fail2ban.jail [35778]: INFO Jail 'selinux-ssh' uses poller {}
2023-12-05 12:53:39,290 fail2ban.jail [35778]: INFO Initiated 'polling' backend
2023-12-05 12:53:39,294 fail2ban.datedetector [35778]: INFO date pattern '': 'Epoch'
2023-12-05 12:53:39,304 fail2ban.filter [35778]: INFO maxRetry: 5
2023-12-05 12:53:39,305 fail2ban.filter [35778]: INFO findtime: 600
2023-12-05 12:53:39,305 fail2ban.actions [35778]: INFO banTime: 3600
2023-12-05 12:53:39,305 fail2ban.filter [35778]: INFO encoding: UTF-8
2023-12-05 12:53:39,308 fail2ban.filter [35778]: INFO Added logfile: '/var/log/audit/audit.log'
(pos = 0, hash = f78f4480f3395a7b12f370e778af4a8fb7be98bd)
2023-12-05 12:53:39,309 fail2ban.jail [35778]: INFO Creating new jail 'sshd-ddos'
2023-12-05 12:53:39,311 fail2ban.jail [35778]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-05 12:53:39,318 fail2ban.jail [35778]: INFO Initiated 'polling' backend
2023-12-05 12:53:39,322 fail2ban.filter [35778]: INFO maxLines: 1
2023-12-05 12:53:39,324 fail2ban.filter [35778]: INFO maxRetry: 5
2023-12-05 12:53:39,344 fail2ban.filter [35778]: INFO findtime: 600
2023-12-05 12:53:39,345 fail2ban.actions [35778]: INFO banTime: 3600
2023-12-05 12:53:39,346 fail2ban.filter [35778]: INFO encoding: UTF-8
2023-12-05 12:53:39,380 fail2ban.jail [35778]: INFO Jail 'sshd' started
2023-12-05 12:53:39,401 fail2ban.filtersystemd [35778]: INFO [sshd] Jail is in operation now (process
new journal entries)
2023-12-05 12:53:39,413 fail2ban.jail [35778]: INFO Jail 'selinux-ssh' started
2023-12-05 12:53:39,424 fail2ban.jail [35778]: INFO Jail 'sshd-ddos' started
```

Рис. 1.7. Просмотр журнала событий.

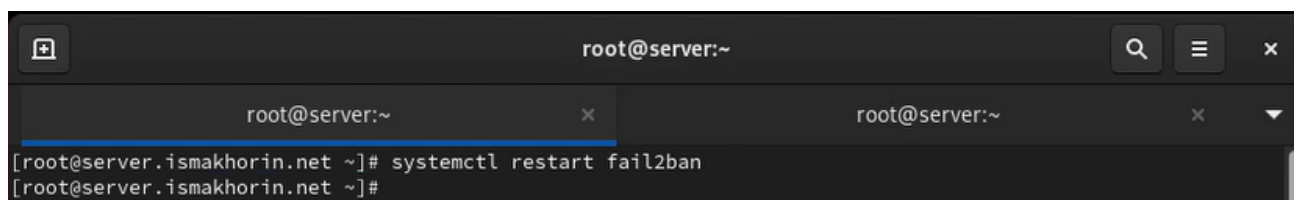
В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту HTTP (Рис. 1.8):



```
21 #
22
23 [apache-auth]
24 enabled = true
25
26 [apache-badbots]
27 enabled = true
28
29 [apache-noscript]
30 enabled = true
31
32 [apache-overflows]
33 enabled = true
34
35 [apache-nohome]
36 enabled = true
37
38 [apache-botsearch]
39 enabled = true
40
41 [apache-fakegooglebot]
42 enabled = true
43
44 [apache-modsecurity]
45 enabled = true
46
47 [apache-shellshock]
48 enabled = true
```

Рис. 1.8. Включение защиты HTTP в файле
/etc/fail2ban/jail.d/customisation.local.

Перезапустим fail2ban (Рис. 1.9):



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

Рис. 1.9. Перезапуск fail2ban.

После чего посмотрим журнал событий (Рис. 1.10):


```
root@server:~  
(pos = 0, hash = 868493300dfd7de2ea5d6ab1b7f522ecced79de)  
2023-12-05 12:55:19,186 fail2ban.filter [35823]: INFO Added logfile: '/var/log/httpd/ssl_error_  
log' (pos = 0, hash = c9287c5b333dd6efe283667db51e4d063cb757fa)  
2023-12-05 12:55:19,187 fail2ban.filter [35823]: INFO Added logfile: '/var/log/httpd/www.ismakh  
orin.net-error_log' (pos = 0, hash = 0afb7774e08aa5765368d031a003601b9f6d7c70)  
2023-12-05 12:55:19,187 fail2ban.jail [35823]: INFO Creating new jail 'sshd-ddos'  
2023-12-05 12:55:19,189 fail2ban.jail [35823]: INFO Jail 'sshd-ddos' uses poller {}  
2023-12-05 12:55:19,191 fail2ban.jail [35823]: INFO Initiated 'polling' backend  
2023-12-05 12:55:19,202 fail2ban.filter [35823]: INFO maxLines: 1  
2023-12-05 12:55:19,206 fail2ban.filter [35823]: INFO maxRetry: 5  
2023-12-05 12:55:19,207 fail2ban.filter [35823]: INFO findtime: 600  
2023-12-05 12:55:19,208 fail2ban.actions [35823]: INFO banTime: 3600  
2023-12-05 12:55:19,208 fail2ban.filter [35823]: INFO encoding: UTF-8  
2023-12-05 12:55:19,210 fail2ban.filtersystemd [35823]: INFO [sshd] Jail is in operation now (process  
new journal entries)  
2023-12-05 12:55:19,215 fail2ban.jail [35823]: INFO Jail 'sshd' started  
2023-12-05 12:55:19,224 fail2ban.jail [35823]: INFO Jail 'selinux-ssh' started  
2023-12-05 12:55:19,256 fail2ban.jail [35823]: INFO Jail 'apache-auth' started  
2023-12-05 12:55:19,289 fail2ban.jail [35823]: INFO Jail 'apache-badbots' started  
2023-12-05 12:55:19,322 fail2ban.jail [35823]: INFO Jail 'apache-noscript' started  
2023-12-05 12:55:19,341 fail2ban.jail [35823]: INFO Jail 'apache-overflows' started  
2023-12-05 12:55:19,355 fail2ban.jail [35823]: INFO Jail 'apache-nohome' started  
2023-12-05 12:55:19,364 fail2ban.jail [35823]: INFO Jail 'apache-botsearch' started  
2023-12-05 12:55:19,409 fail2ban.jail [35823]: INFO Jail 'apache-fakegooglebot' started  
2023-12-05 12:55:19,443 fail2ban.jail [35823]: INFO Jail 'apache-modsecurity' started  
2023-12-05 12:55:19,456 fail2ban.jail [35823]: INFO Jail 'apache-shellshock' started  
2023-12-05 12:55:19,462 fail2ban.jail [35823]: INFO Jail 'sshd-ddos' started
```

Рис. 1.10. Просмотр журнала событий.

В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту почты (Рис. 1.11):

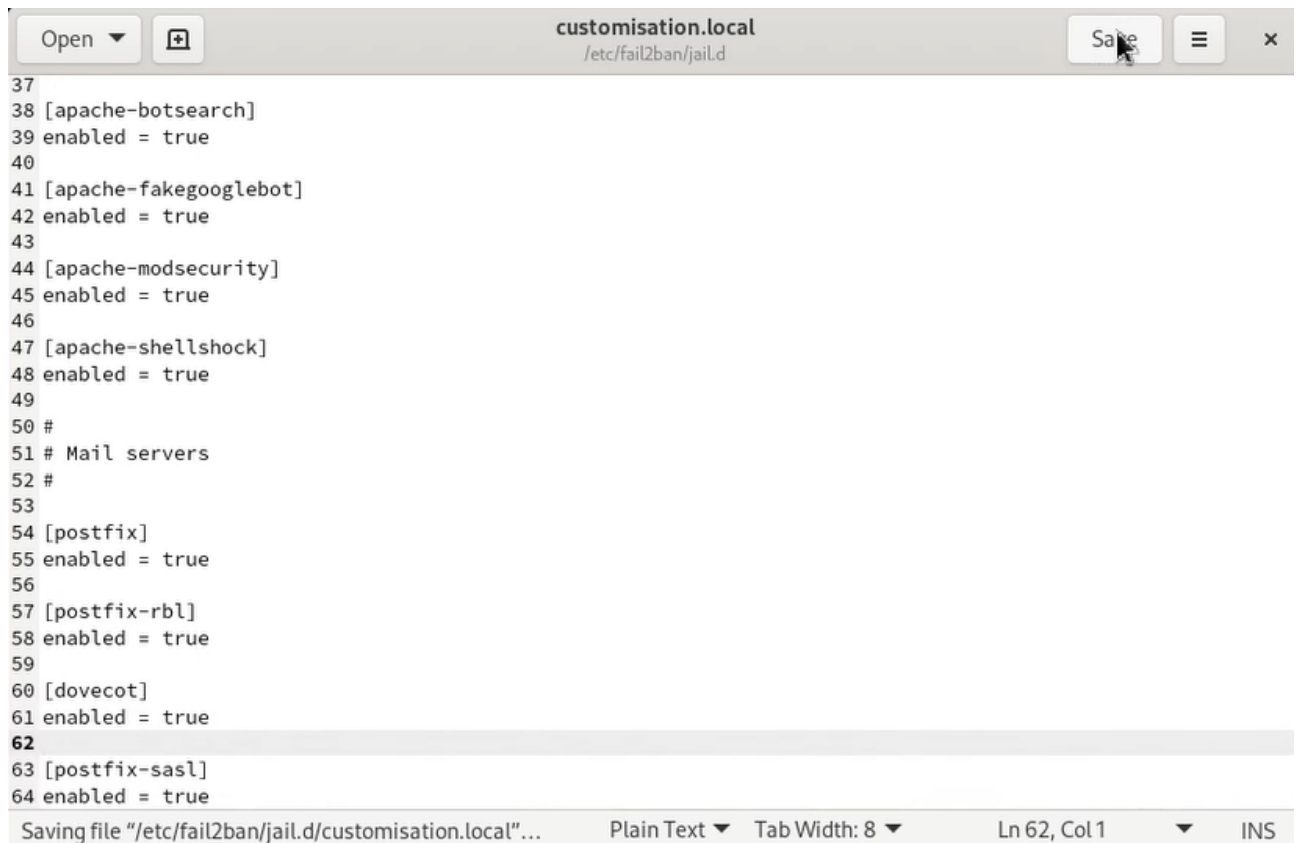


Рис. 1.11. Включение защиты почты в файле
/etc/fail2ban/jail.d/customisation.local.

Снова перезапустим fail2ban (Рис. 1.12):

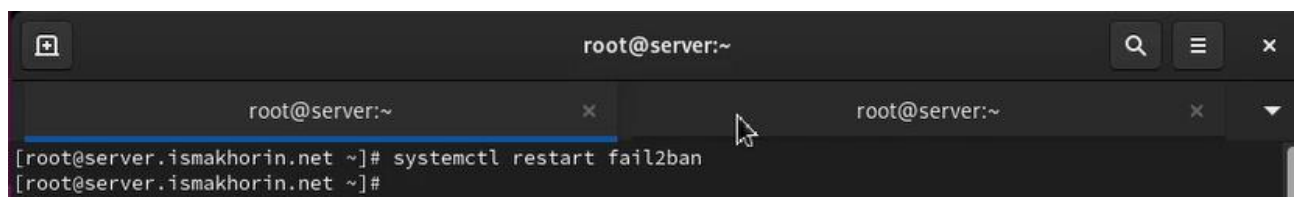
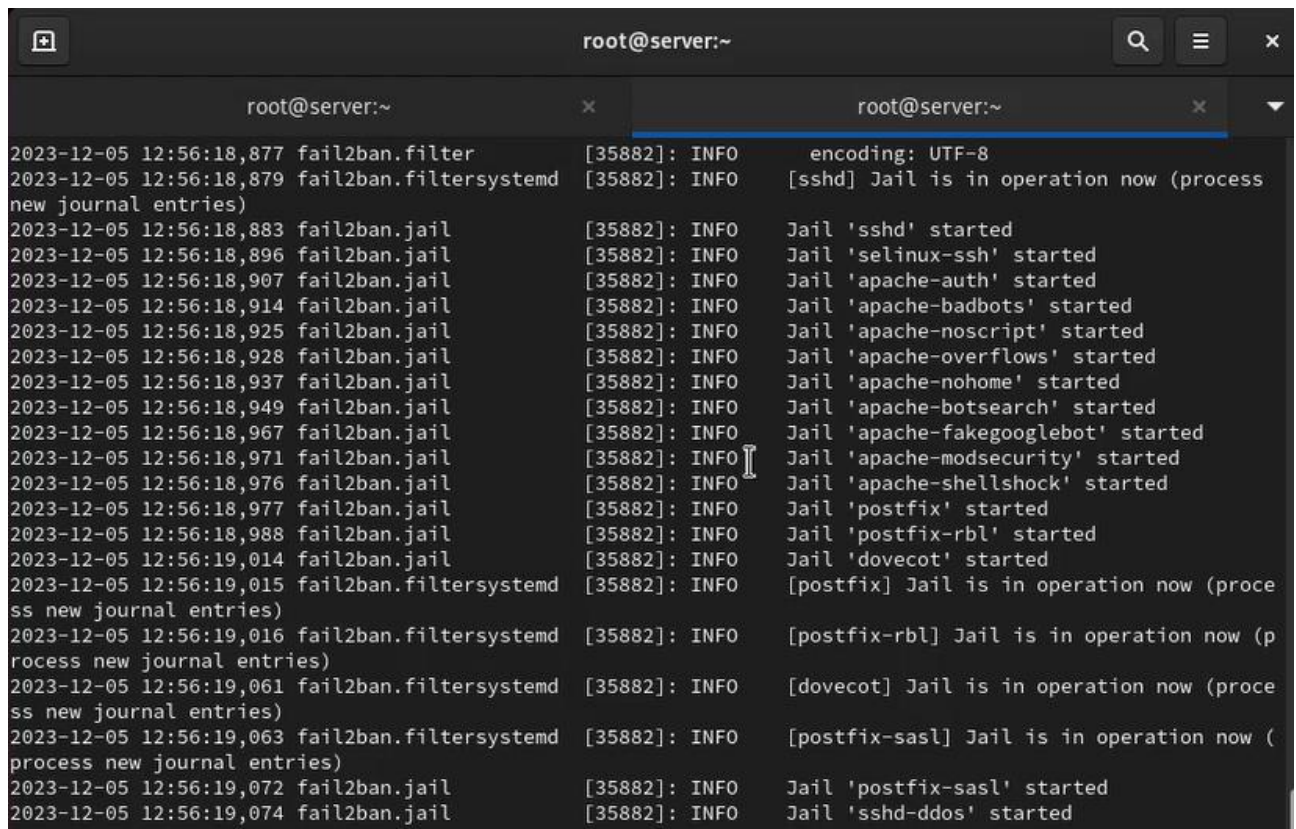


Рис. 1.12. Повторный перезапуск fail2ban.

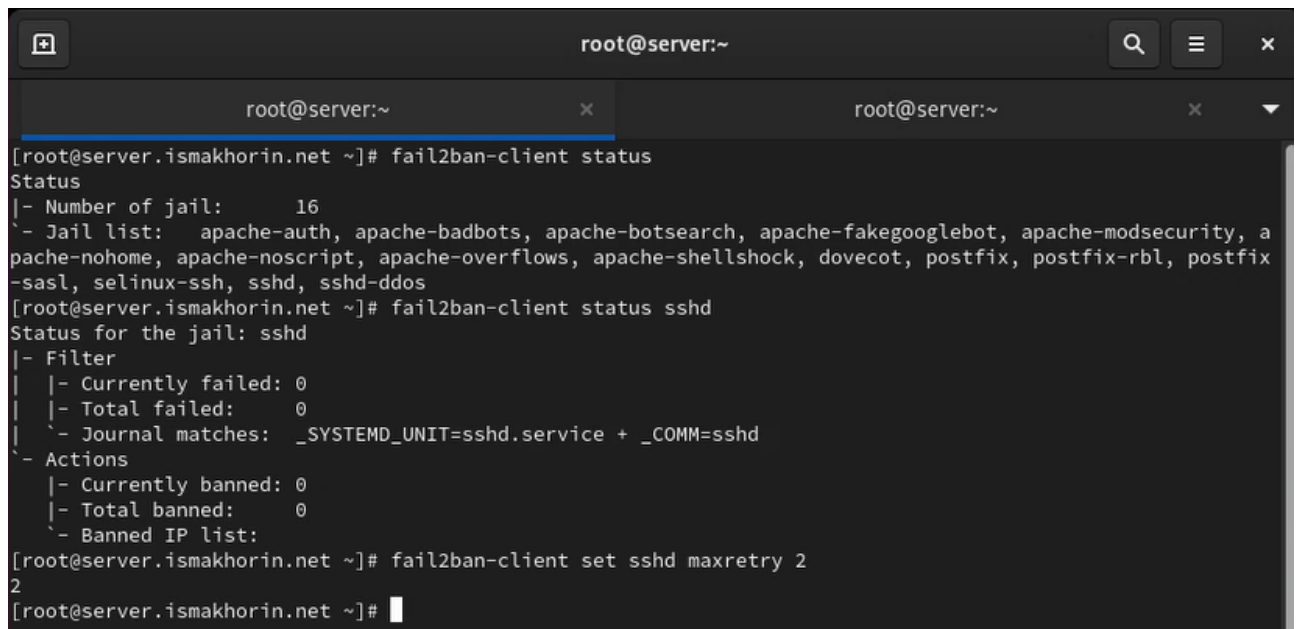
И посмотрим журнал событий (Рис. 1.13):



```
root@server:~
2023-12-05 12:56:18,877 fail2ban.filter [35882]: INFO encoding: UTF-8
2023-12-05 12:56:18,879 fail2ban.filtersystemd [35882]: INFO [sshd] Jail is in operation now (process
new journal entries)
2023-12-05 12:56:18,883 fail2ban.jail [35882]: INFO Jail 'sshd' started
2023-12-05 12:56:18,896 fail2ban.jail [35882]: INFO Jail 'selinux-ssh' started
2023-12-05 12:56:18,907 fail2ban.jail [35882]: INFO Jail 'apache-auth' started
2023-12-05 12:56:18,914 fail2ban.jail [35882]: INFO Jail 'apache-badbots' started
2023-12-05 12:56:18,925 fail2ban.jail [35882]: INFO Jail 'apache-noscript' started
2023-12-05 12:56:18,928 fail2ban.jail [35882]: INFO Jail 'apache-overflows' started
2023-12-05 12:56:18,937 fail2ban.jail [35882]: INFO Jail 'apache-nohome' started
2023-12-05 12:56:18,949 fail2ban.jail [35882]: INFO Jail 'apache-botsearch' started
2023-12-05 12:56:18,967 fail2ban.jail [35882]: INFO Jail 'apache-fakegooglebot' started
2023-12-05 12:56:18,971 fail2ban.jail [35882]: INFO Jail 'apache-modsecurity' started
2023-12-05 12:56:18,976 fail2ban.jail [35882]: INFO Jail 'apache-shellshock' started
2023-12-05 12:56:18,977 fail2ban.jail [35882]: INFO Jail 'postfix' started
2023-12-05 12:56:18,988 fail2ban.jail [35882]: INFO Jail 'postfix-rbl' started
2023-12-05 12:56:19,014 fail2ban.jail [35882]: INFO Jail 'dovecot' started
2023-12-05 12:56:19,015 fail2ban.filtersystemd [35882]: INFO [postfix] Jail is in operation now (proce
ss new journal entries)
2023-12-05 12:56:19,016 fail2ban.filtersystemd [35882]: INFO [postfix-rbl] Jail is in operation now (p
rocess new journal entries)
2023-12-05 12:56:19,061 fail2ban.filtersystemd [35882]: INFO [dovecot] Jail is in operation now (proce
ss new journal entries)
2023-12-05 12:56:19,063 fail2ban.filtersystemd [35882]: INFO [postfix-sasl] Jail is in operation now (
process new journal entries)
2023-12-05 12:56:19,072 fail2ban.jail [35882]: INFO Jail 'postfix-sasl' started
2023-12-05 12:56:19,074 fail2ban.jail [35882]: INFO Jail 'sshd-ddos' started
```

Рис. 1.13. Просмотр журнала событий.

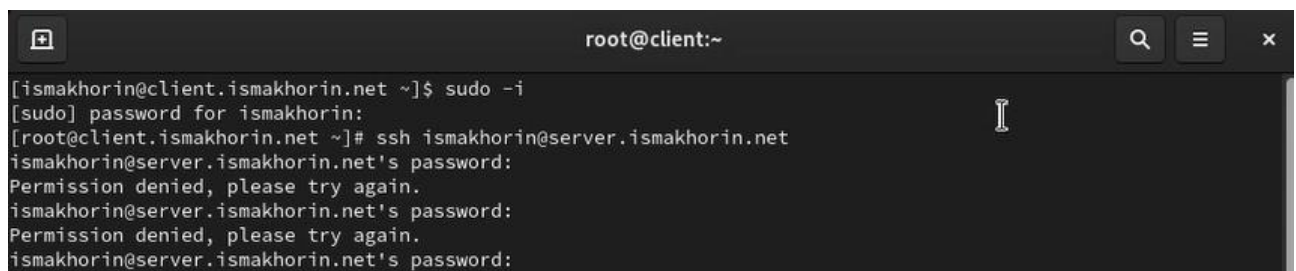
На сервере посмотрим статус fail2ban, статус защиты SSH в fail2ban и установим максимальное количество ошибок для SSH, равное 2 (Рис. 2.1):



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

Рис. 2.1. Просмотр на сервере статуса fail2ban, статуса защиты SSH в fail2ban и установка максимального количества ошибок для SSH (=2).

С клиента попытаемся зайти по SSH на сервер с неправильным паролем (Рис. 2.2):



```
root@client:~  
[ismakhorin@client.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@client.ismakhorin.net ~]# ssh ismakhorin@server.ismakhorin.net  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's password:
```

Рис. 2.2. Попытка зайти с клиента по SSH на сервер с неправильным паролем.

На сервере посмотрим статус защиты SSH и разблокируем IP-адрес клиента. После чего вновь посмотрим статус защиты SSH и убедимся, что блокировка клиента снята (Рис. 2.3):

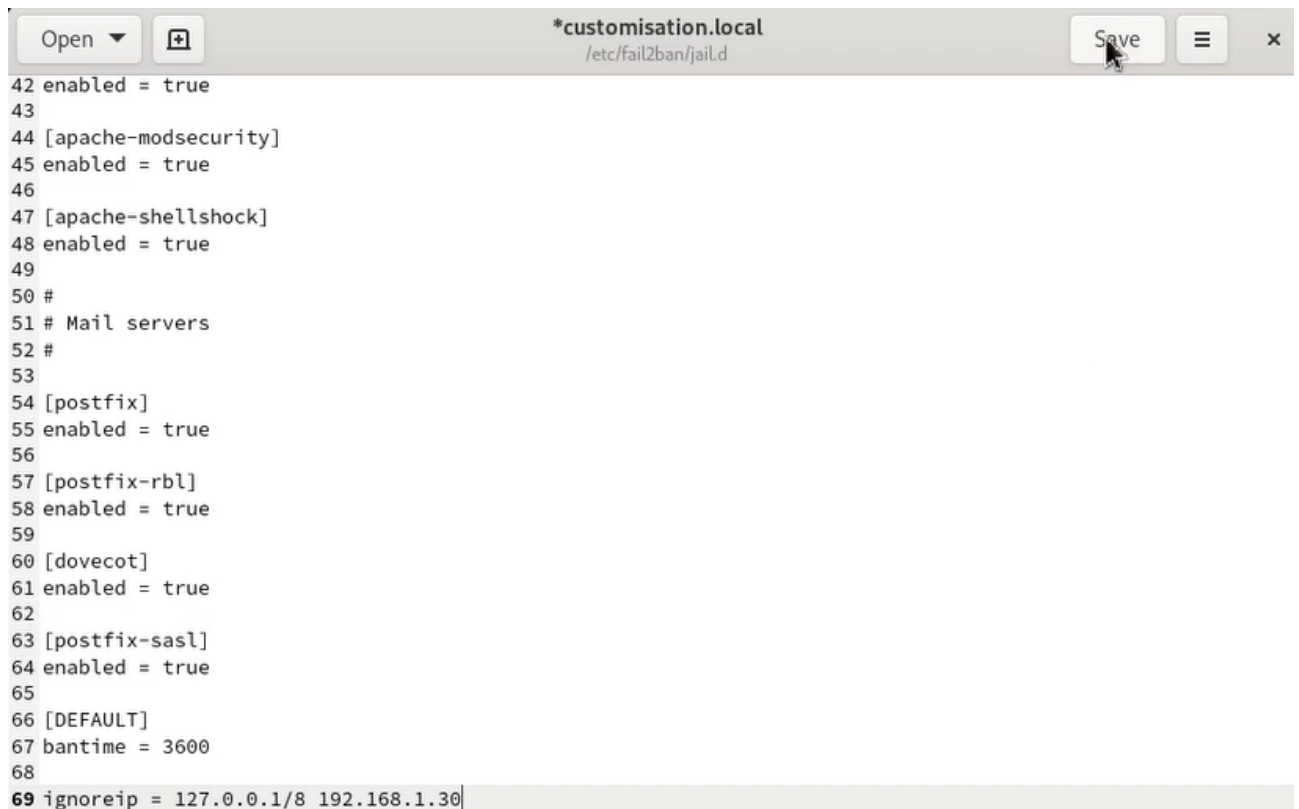
```

[root@server.ismakhorin.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
[root@server.ismakhorin.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.ismakhorin.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.ismakhorin.net ~]#

```

Рис. 2.3. Просмотр на сервере статуса защиты SSH, разблокировка IP-адреса клиента и повторная проверка.

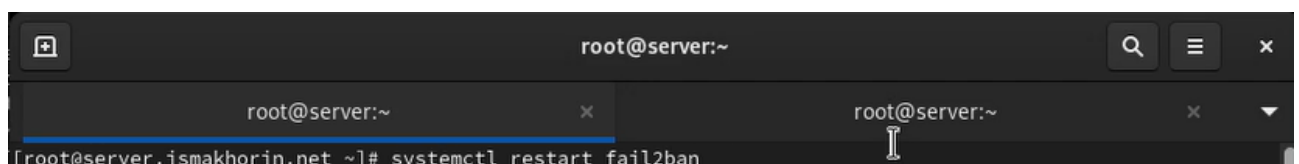
На сервере внесём изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента (Рис. 2.4):



```
42 enabled = true
43
44 [apache-modsecurity]
45 enabled = true
46
47 [apache-shellshock]
48 enabled = true
49
50 #
51 # Mail servers
52 #
53
54 [postfix]
55 enabled = true
56
57 [postfix-rbl]
58 enabled = true
59
60 [dovecot]
61 enabled = true
62
63 [postfix-sasl]
64 enabled = true
65
66 [DEFAULT]
67 bantime = 3600
68
69 ignoreip = 127.0.0.1/8 192.168.1.30
```

Рис. 2.4. Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле `/etc/fail2ban/jail.d/customisation.local`.

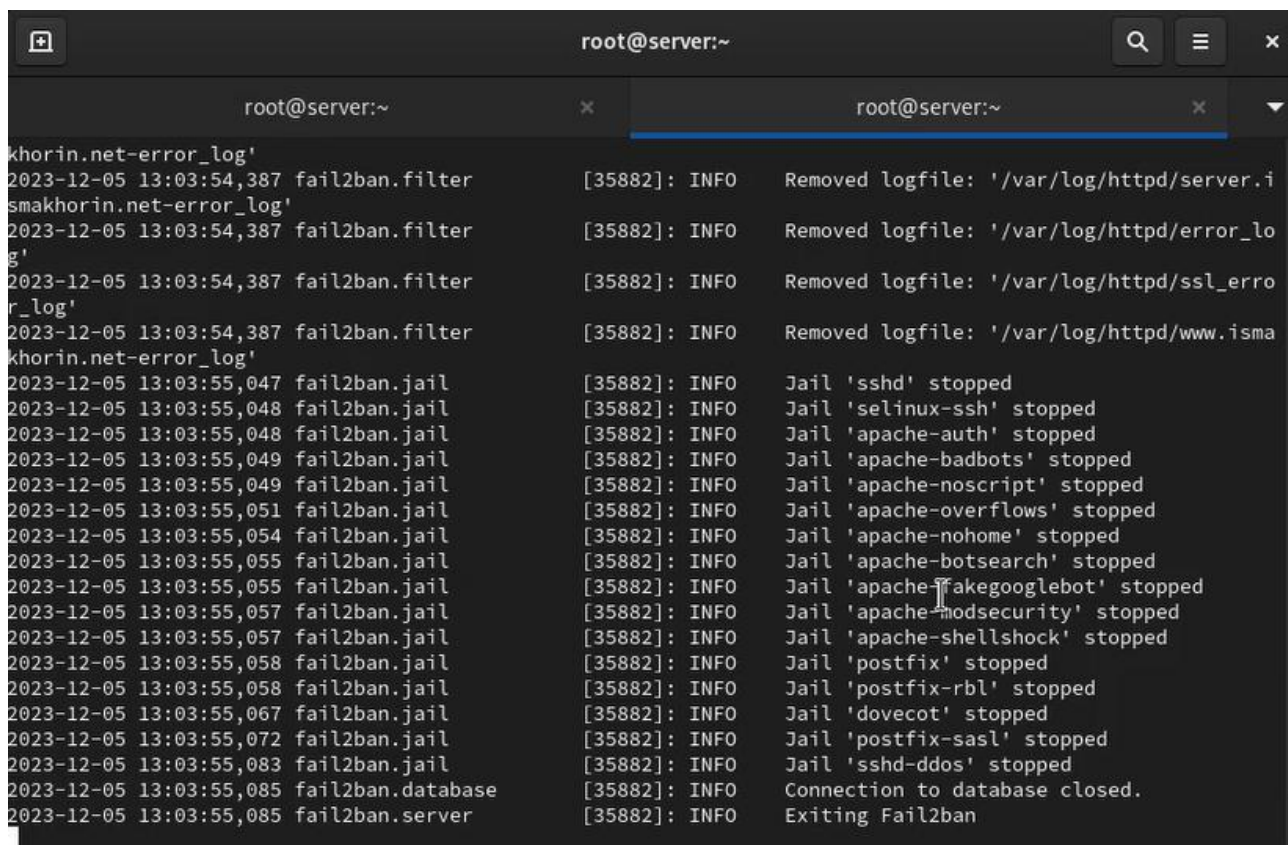
Перезапустим fail2ban (Рис. 2.5):



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

Рис. 2.5. Перезапуск fail2ban.

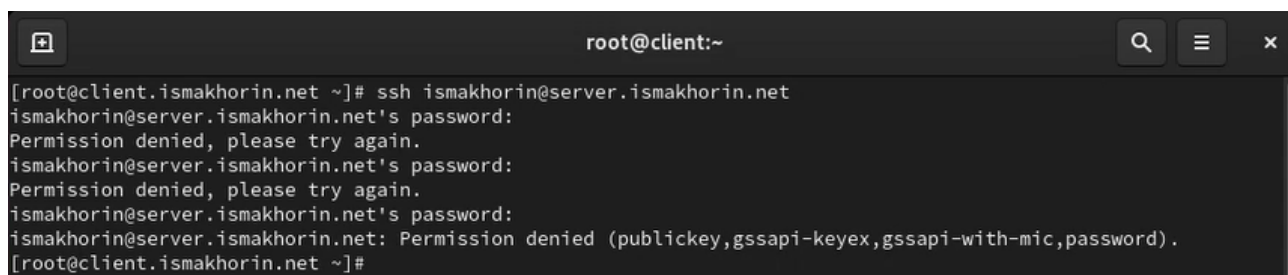
Далее посмотрим журнал событий (Рис. 2.6):



```
root@server:~  
ismakhorin.net-error_log'  
2023-12-05 13:03:54,387 fail2ban.filter [35882]: INFO Removed logfile: '/var/log/httpd/server.i  
ismakhorin.net-error_log'  
2023-12-05 13:03:54,387 fail2ban.filter [35882]: INFO Removed logfile: '/var/log/httpd/error_lo  
g'  
2023-12-05 13:03:54,387 fail2ban.filter [35882]: INFO Removed logfile: '/var/log/httpd/ssl_erro  
r_log'  
2023-12-05 13:03:54,387 fail2ban.filter [35882]: INFO Removed logfile: '/var/log/httpd/www.isma  
ismakhorin.net-error_log'  
2023-12-05 13:03:55,047 fail2ban.jail [35882]: INFO Jail 'sshd' stopped  
2023-12-05 13:03:55,048 fail2ban.jail [35882]: INFO Jail 'selinux-ssh' stopped  
2023-12-05 13:03:55,048 fail2ban.jail [35882]: INFO Jail 'apache-auth' stopped  
2023-12-05 13:03:55,049 fail2ban.jail [35882]: INFO Jail 'apache-badbots' stopped  
2023-12-05 13:03:55,049 fail2ban.jail [35882]: INFO Jail 'apache-noscript' stopped  
2023-12-05 13:03:55,051 fail2ban.jail [35882]: INFO Jail 'apache-overflows' stopped  
2023-12-05 13:03:55,054 fail2ban.jail [35882]: INFO Jail 'apache-nohome' stopped  
2023-12-05 13:03:55,055 fail2ban.jail [35882]: INFO Jail 'apache-botsearch' stopped  
2023-12-05 13:03:55,055 fail2ban.jail [35882]: INFO Jail 'apache-fakegooglebot' stopped  
2023-12-05 13:03:55,057 fail2ban.jail [35882]: INFO Jail 'apache-modsecurity' stopped  
2023-12-05 13:03:55,057 fail2ban.jail [35882]: INFO Jail 'apache-shellshock' stopped  
2023-12-05 13:03:55,058 fail2ban.jail [35882]: INFO Jail 'postfix' stopped  
2023-12-05 13:03:55,058 fail2ban.jail [35882]: INFO Jail 'postfix-rbl' stopped  
2023-12-05 13:03:55,067 fail2ban.jail [35882]: INFO Jail 'dovecot' stopped  
2023-12-05 13:03:55,072 fail2ban.jail [35882]: INFO Jail 'postfix-sasl' stopped  
2023-12-05 13:03:55,083 fail2ban.jail [35882]: INFO Jail 'sshd-ddos' stopped  
2023-12-05 13:03:55,085 fail2ban.database [35882]: INFO Connection to database closed.  
2023-12-05 13:03:55,085 fail2ban.server [35882]: INFO Exiting Fail2ban
```

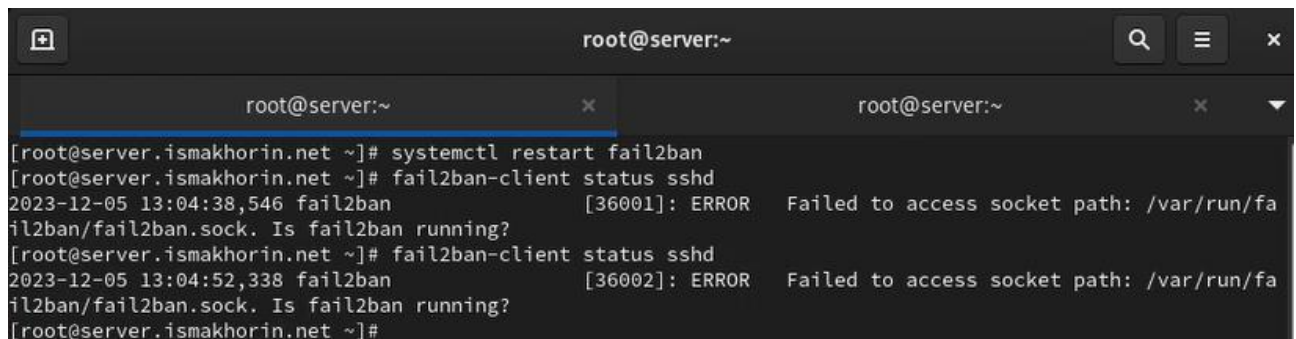
Рис. 2.6. Просмотр журнала событий.

Вновь попытаемся войти с клиента на сервер с неправильным паролем (Рис. 2.7) и посмотрим статус защиты SSH (Рис. 2.8):



```
root@client:~  
[root@client.ismakhorin.net ~]# ssh ismakhorin@server.ismakhorin.net  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's password:  
ismakhorin@server.ismakhorin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[root@client.ismakhorin.net ~]#
```

Рис. 2.7. Попытка войти с клиента на сервер с неправильным паролем.

A terminal window titled 'root@server:~' showing the execution of fail2ban commands. The user runs 'systemctl restart fail2ban' and then 'fail2ban-client status sshd' twice. The output shows the service is running but reports errors: 'Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?'.

```
[root@server.ismakhorin.net ~]# systemctl restart fail2ban
[root@server.ismakhorin.net ~]# fail2ban-client status sshd
2023-12-05 13:04:38,546 fail2ban [36001]: ERROR    Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?
[root@server.ismakhorin.net ~]# fail2ban-client status sshd
2023-12-05 13:04:52,338 fail2ban [36002]: ERROR    Failed to access socket path: /var/run/fail2ban/fail2ban.sock. Is fail2ban running?
[root@server.ismakhorin.net ~]#
```

Рис. 2.8. Просмотр статуса защиты SSH.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `protect`, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/server` создадим исполняемый файл `protect.sh` (Рис. 3.1):

A terminal window titled 'root@server:/vagrant/provision/server' showing the creation of a directory structure and a script. The user runs '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/', 'cd /vagrant/provision/server', 'touch protect.sh', and 'chmod +x protect.sh'.

```
[root@server.ismakhorin.net ~]# cd /vagrant/provision/server
[root@server.ismakhorin.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.ismakhorin.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.ismakhorin.net server]# cd /vagrant/provision/server
[root@server.ismakhorin.net server]# touch protect.sh
[root@server.ismakhorin.net server]# chmod +x protect.sh
[root@server.ismakhorin.net server]#
```

Рис. 3.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `protect`, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге `/vagrant/provision/server` исполняемого файла `protect.sh`.

Открыв его на редактирование, пропишем в нём скрипт (Рис. 3.2):



```
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Install needed packages"
6 dnf -y install fail2ban
7
8 echo "Copy configuration files"
9 cp -R /vagrant/provision/server/protect/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start fail2ban service"
13 systemctl enable fail2ban
14 systemctl start fail2ban
15
```

Рис. 3.2. Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` добавим в соответствующем разделе конфигураций для сервера (Рис. 3.3):



```
97
98   server.vm.provision "server_protect",
99                       type: "shell",
100                       preserve_order: true,
101                       path: "provision/server/protect.sh"
102
```

Рис. 3.3. Добавление конфигураций в конфигурационном файле `Vagrantfile` для сервера.

Вывод:

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

Ответы на контрольные вопросы:

1. Поясните принцип работы `Fail2ban`. - **`Fail2ban` является инструментом для защиты от атак на серверы, основанных на**

анализе журналов. Он мониторит журналы системы на предмет неудачных попыток входа или других событий, а затем блокирует IP-адреса атакующих с использованием системных средств, таких как iptables. Принцип работы:

Мониторинг журналов на предмет определенных событий.

Обнаружение повторных неудачных попыток входа или других нарушений.

Динамическое обновление правил брандмауэра для блокировки атакующих IP-адресов.

- 2. Настройки какого файла более приоритетны: jail.conf или jail.local? - Настройки файла jail.local имеют более высокий приоритет и перекрывают настройки из jail.conf. Таким образом, если есть конфликтующие настройки, они будут использоваться из jail.local.**
- 3. Как настроить оповещение администратора при срабатывании Fail2ban? - В файле jail.local нужно указать параметр destemail и задать адрес электронной почты, а также параметр action с указанием определенного действия (например, action_mw для отправки почты).**
- 4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе. –**

Пример настроек для веб-службы в файле jail.conf:

[apache]

enabled = true

port = http,https

filter = apache-auth

logpath = /var/log/apache*/error.log

5. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе. —

Пример настроек для почтовой службы в файле jail.conf:

[postfix]

enabled = true

filter = postfix

action = iptables-multiport[name=postfix, port='submission,smtps', protocol=tcp]

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, такие как блокировка IP-адреса с использованием брандмауэра, отправка уведомлений, добавление в черные списки и т.д. Описание действий можно найти в конфигурационных файлах в разделе action.**
7. Как получить список действующих правил Fail2ban? - **Используйте команду: fail2ban-client status.**
8. Как получить статистику заблокированных Fail2ban адресов? - **Используйте команду: fail2ban-client status <jail_name>.**
9. Как разблокировать IP-адрес? - **Используйте команду: fail2ban-client set <jail_name> unbanip <ip_address>.**