РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ №16

дисциплина: администрирование локальных подсистем

Студент: Саинт-Амур Измаэль

Группа: НПИбд-02-20

МОСКВА

2023 г.

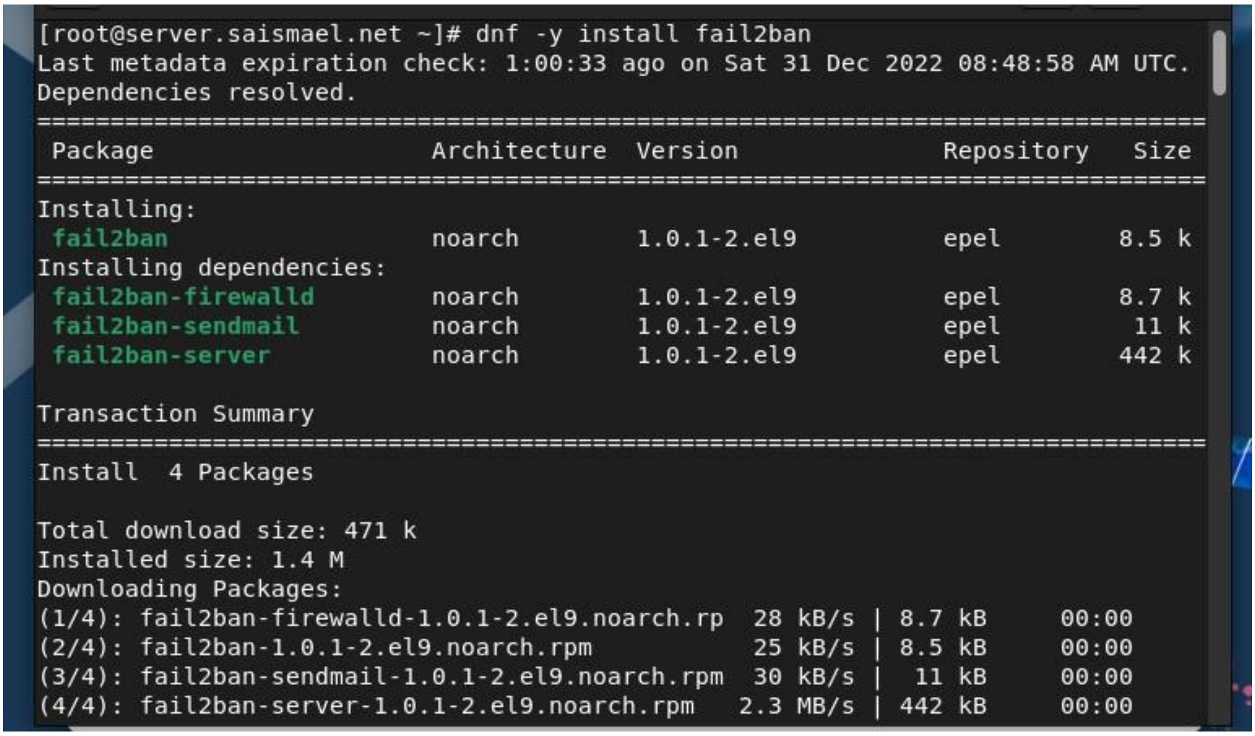
Постановка задачи

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

Выполнение работы

16.4.1. Защита с помощью Fail2ban

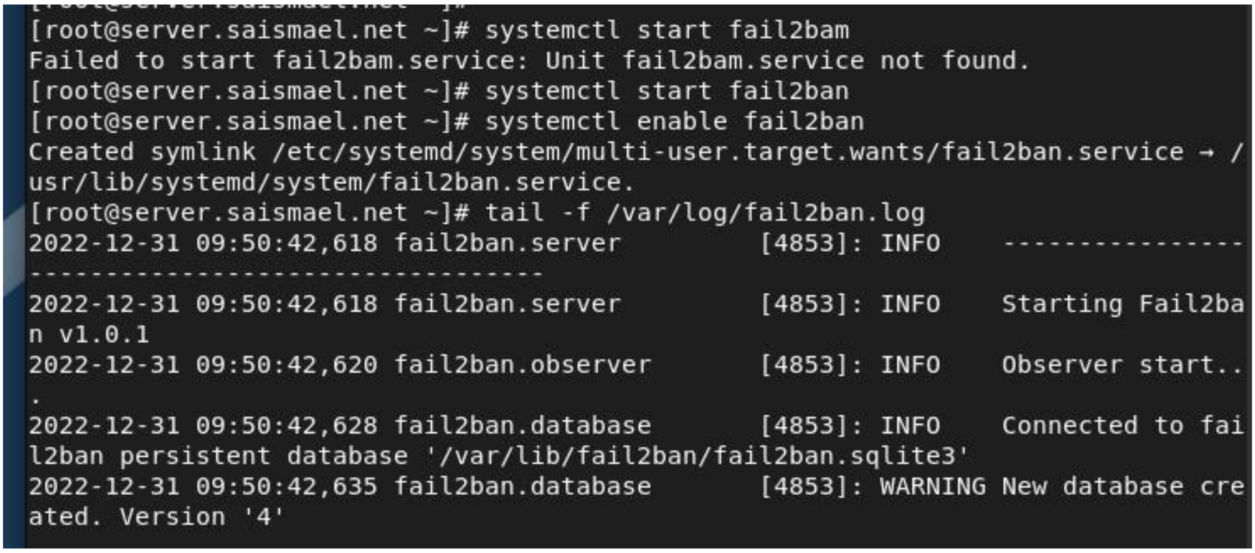
1. На сервере установил fail2ban:



```
[root@server.saismael.net ~]# dnf -y install fail2ban
Last metadata expiration check: 1:00:33 ago on Sat 31 Dec 2022 08:48:58 AM UTC.
Dependencies resolved.
================================================================================
 Package                   Architecture  Version              Repository   Size
================================================================================
Installing:
 fail2ban                  noarch        1.0.1-2.el9          epel        8.5 k
Installing dependencies:
 fail2ban-firewalld        noarch        1.0.1-2.el9          epel        8.7 k
 fail2ban-sendmail         noarch        1.0.1-2.el9          epel         11 k
 fail2ban-server           noarch        1.0.1-2.el9          epel        442 k

Transaction Summary
================================================================================
Install  4 Packages

Total download size: 471 k
Installed size: 1.4 M
Downloading Packages:
(1/4): fail2ban-firewalld-1.0.1-2.el9.noarch.rp  28 kB/s | 8.7 kB     00:00
(2/4): fail2ban-1.0.1-2.el9.noarch.rpm           25 kB/s | 8.5 kB     00:00
(3/4): fail2ban-sendmail-1.0.1-2.el9.noarch.rpm  30 kB/s |  11 kB     00:00
(4/4): fail2ban-server-1.0.1-2.el9.noarch.rpm   2.3 MB/s | 442 kB     00:00
```

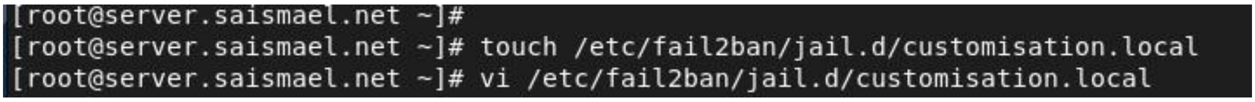
2. Запустил сервер fail2ban:

3. В дополнительном терминале запустил просмотр журнала событий fail2ban:



```
[root@server.saismael.net ~]# systemctl start fail2bam
Failed to start fail2bam.service: Unit fail2bam.service not found.
[root@server.saismael.net ~]# systemctl start fail2ban
[root@server.saismael.net ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /
usr/lib/systemd/system/fail2ban.service.
[root@server.saismael.net ~]# tail -f /var/log/fail2ban.log
2022-12-31 09:50:42,618 fail2ban.server         [4853]: INFO    ----------------
----------------------------------
2022-12-31 09:50:42,618 fail2ban.server         [4853]: INFO    Starting Fail2ba
n v1.0.1
2022-12-31 09:50:42,620 fail2ban.observer       [4853]: INFO    Observer start..
.
2022-12-31 09:50:42,628 fail2ban.database       [4853]: INFO    Connected to fai
l2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2022-12-31 09:50:42,635 fail2ban.database       [4853]: WARNING New database cre
ated. Version '4'
```

4. Создал файл с локальной конфигурацией fail2ban:

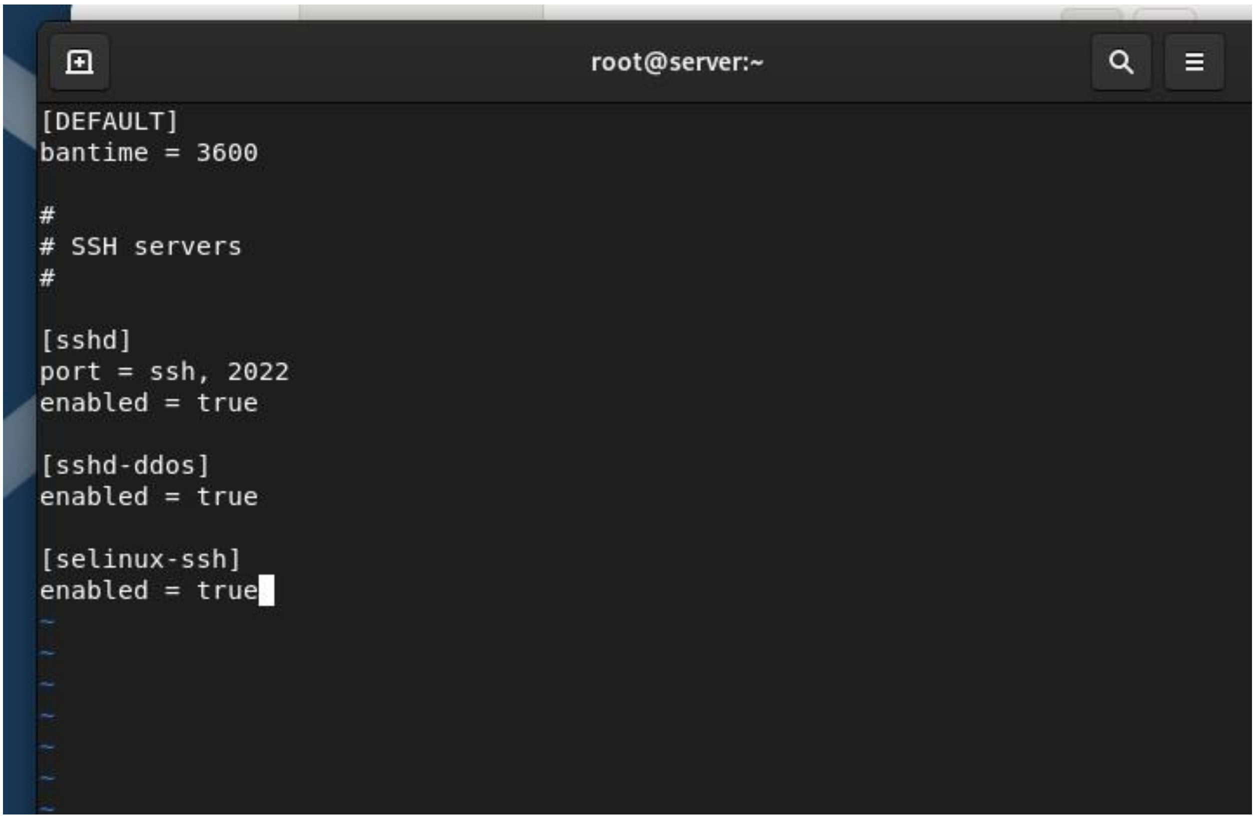


```
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@server.saismael.net ~]# vi /etc/fail2ban/jail.d/customisation.local
```

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

(a) задал время блокирования на 1 час

(b) включил защиту SSH

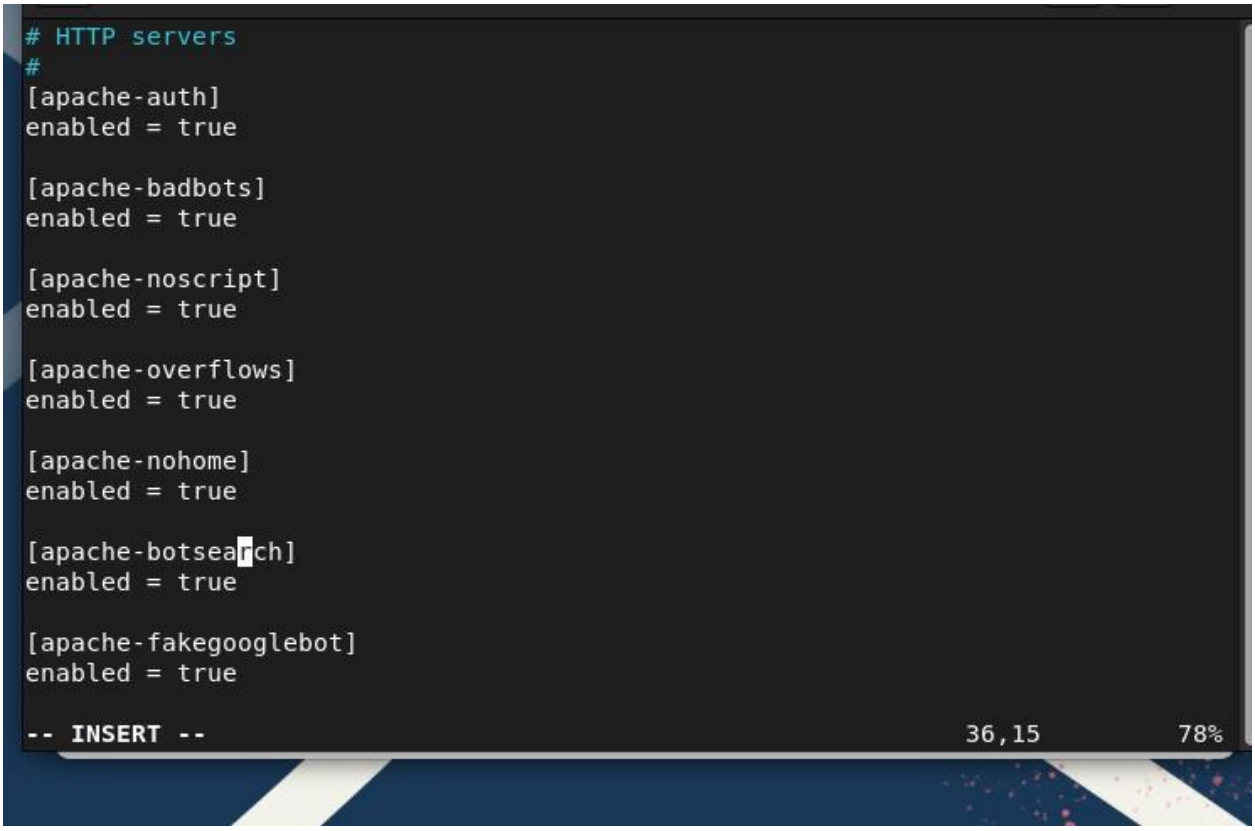


```
[DEFAULT]
bantime = 3600

#
# SSH servers
#

[sshd]
port = ssh, 2022
enabled = true

[sshd-ddos]
enabled = true

[selinux-ssh]
enabled = true
~
~
~
~
~
~
~
```

6. Перезапустил fail2ban

7. Посмотрел журнал событий:

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

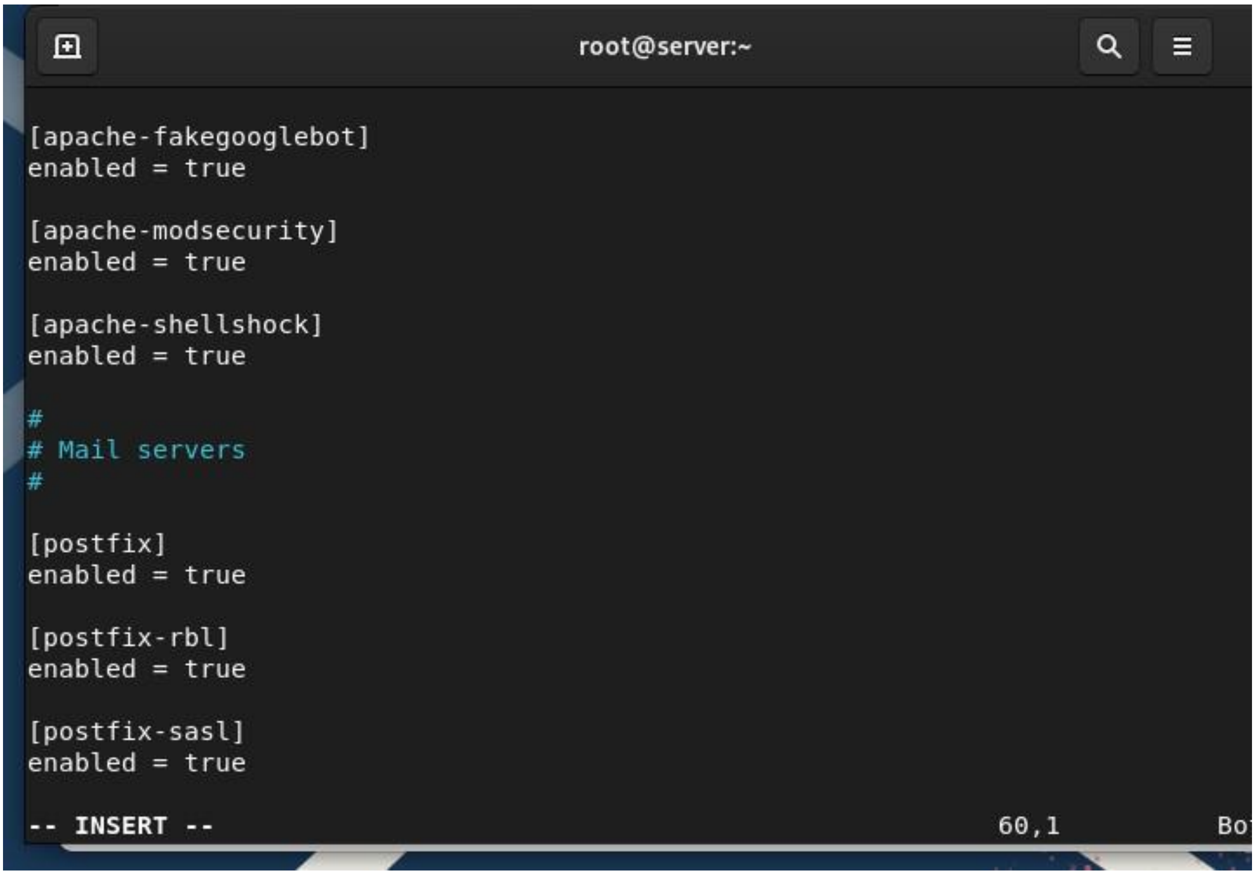


```
# HTTP servers
#
[apache-auth]
enabled = true

[apache-badbots]
enabled = true

[apache-noscript]
enabled = true

[apache-overflows]
enabled = true

[apache-nohome]
enabled = true

[apache-botsearch]
enabled = true

[apache-fakegooglebot]
enabled = true

-- INSERT --                                              36,15          78%
```

9. Перезапустил fail2ban

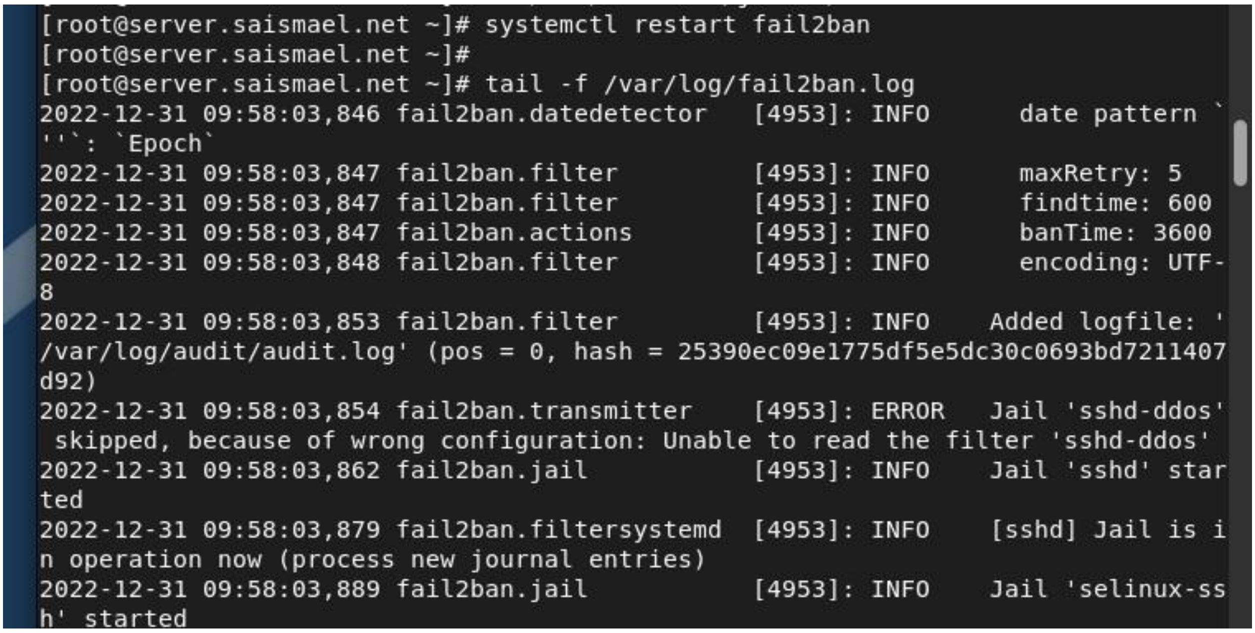
10. Посмотрел журнал событий:

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

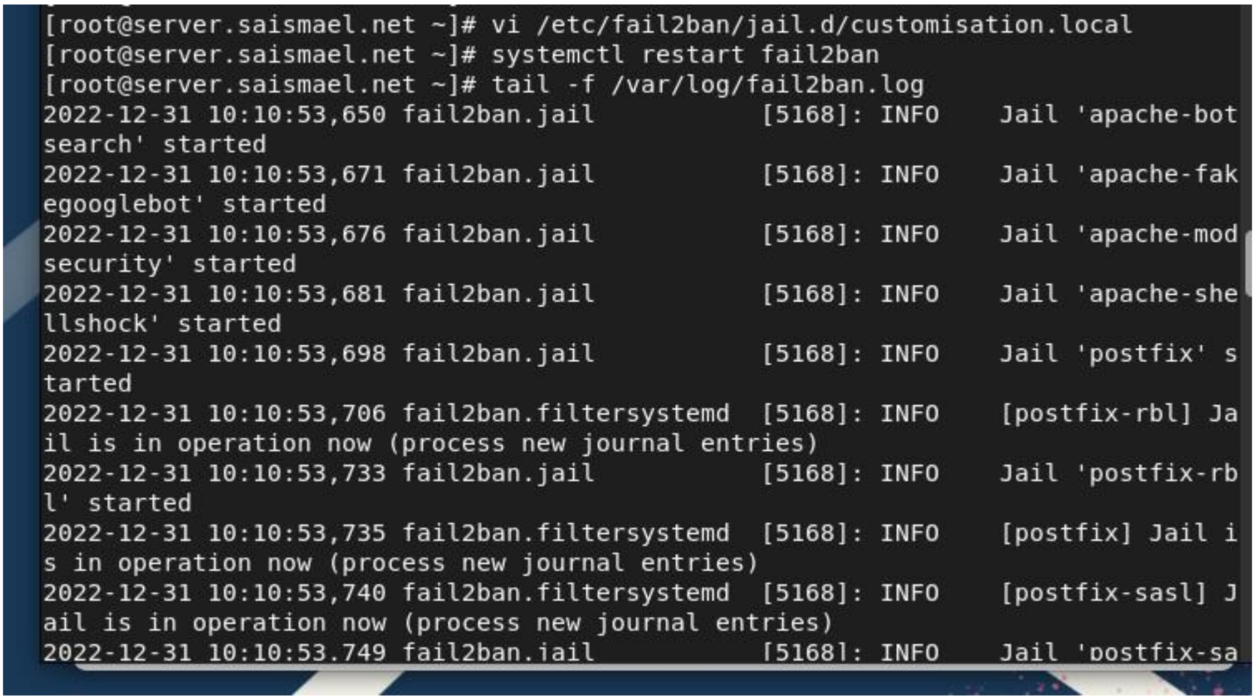


```
[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true

#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[postfix-sasl]
enabled = true

-- INSERT --                                              60,1          Bo
```

12. Перезапустил fail2ban:



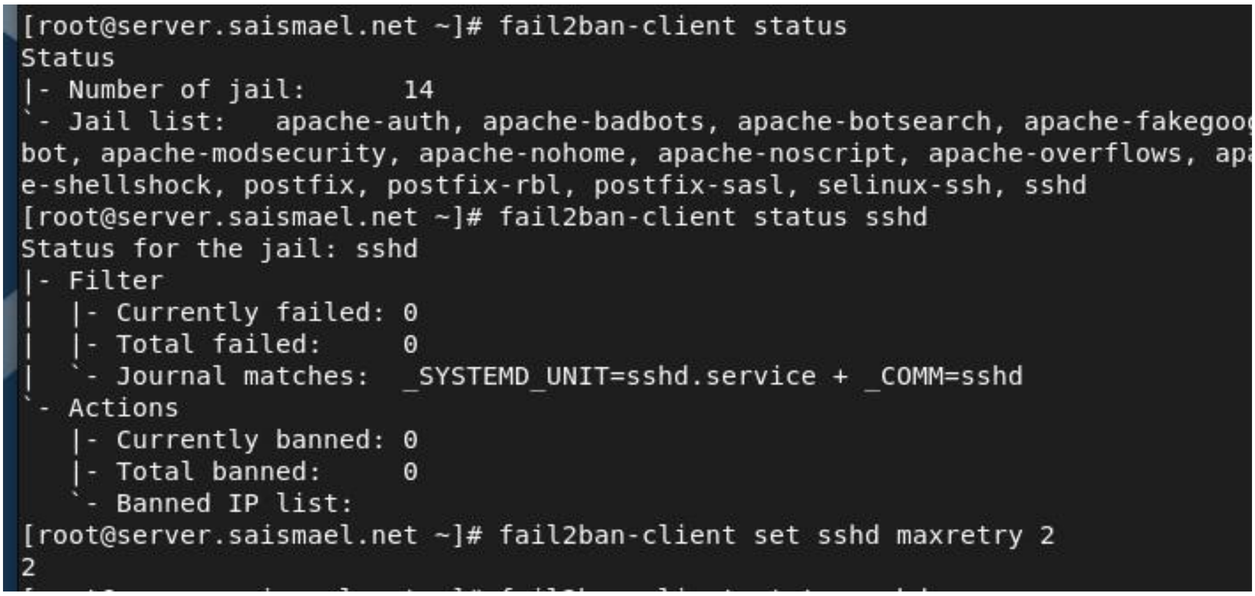
```
[root@server.saismael.net ~]# systemctl restart fail2ban
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# tail -f /var/log/fail2ban.log
2022-12-31 09:58:03,846 fail2ban.datedetector   [4953]: INFO      date pattern `
''`: `Epoch`
2022-12-31 09:58:03,847 fail2ban.filter         [4953]: INFO      maxRetry: 5
2022-12-31 09:58:03,847 fail2ban.filter         [4953]: INFO      findtime: 600
2022-12-31 09:58:03,847 fail2ban.actions        [4953]: INFO      banTime: 3600
2022-12-31 09:58:03,848 fail2ban.filter         [4953]: INFO      encoding: UTF-
8
2022-12-31 09:58:03,853 fail2ban.filter         [4953]: INFO    Added logfile: '
/var/log/audit/audit.log' (pos = 0, hash = 25390ec09e1775df5e5dc30c0693bd7211407
d92)
2022-12-31 09:58:03,854 fail2ban.transmitter    [4953]: ERROR   Jail 'sshd-ddos'
 skipped, because of wrong configuration: Unable to read the filter 'sshd-ddos'
2022-12-31 09:58:03,862 fail2ban.jail           [4953]: INFO    Jail 'sshd' star
ted
2022-12-31 09:58:03,879 fail2ban.filtersystemd  [4953]: INFO    [sshd] Jail is i
n operation now (process new journal entries)
2022-12-31 09:58:03,889 fail2ban.jail           [4953]: INFO    Jail 'selinux-ss
h' started
```



```
[root@server.saismael.net ~]# vi /etc/fail2ban/jail.d/customisation.local
[root@server.saismael.net ~]# systemctl restart fail2ban
[root@server.saismael.net ~]# tail -f /var/log/fail2ban.log
2022-12-31 10:10:53,650 fail2ban.jail           [5168]: INFO    Jail 'apache-bot
search' started
2022-12-31 10:10:53,671 fail2ban.jail           [5168]: INFO    Jail 'apache-fak
egooglebot' started
2022-12-31 10:10:53,676 fail2ban.jail           [5168]: INFO    Jail 'apache-mod
security' started
2022-12-31 10:10:53,681 fail2ban.jail           [5168]: INFO    Jail 'apache-she
llshock' started
2022-12-31 10:10:53,698 fail2ban.jail           [5168]: INFO    Jail 'postfix' s
tarted
2022-12-31 10:10:53,706 fail2ban.filtersystemd  [5168]: INFO    [postfix-rbl] Ja
il is in operation now (process new journal entries)
2022-12-31 10:10:53,733 fail2ban.jail           [5168]: INFO    Jail 'postfix-rb
l' started
2022-12-31 10:10:53,735 fail2ban.filtersystemd  [5168]: INFO    [postfix] Jail i
s in operation now (process new journal entries)
2022-12-31 10:10:53,740 fail2ban.filtersystemd  [5168]: INFO    [postfix-sasl] J
ail is in operation now (process new journal entries)
2022-12-31 10:10:53,749 fail2ban.jail           [5168]: INFO    Jail 'postfix-sa
```

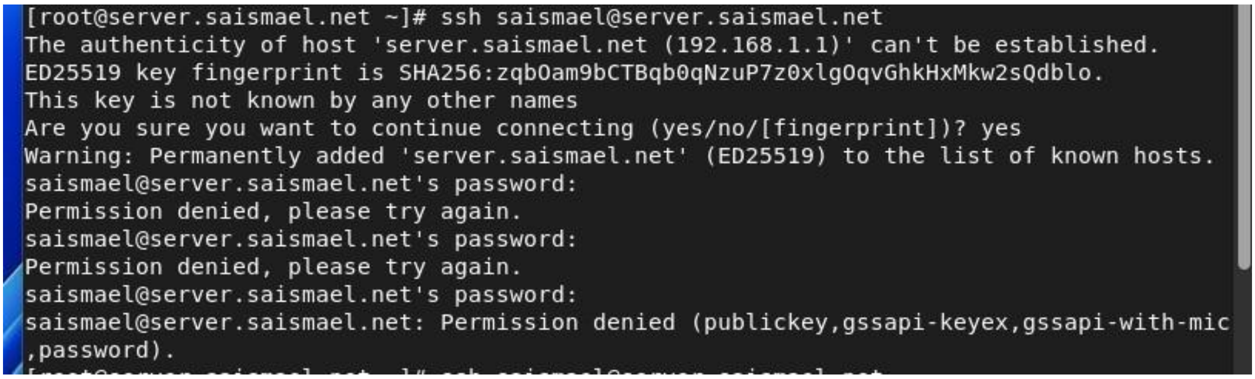
16.4.2. Проверка работы Fail2ban

1. На сервере посмотрел статус fail2ban:



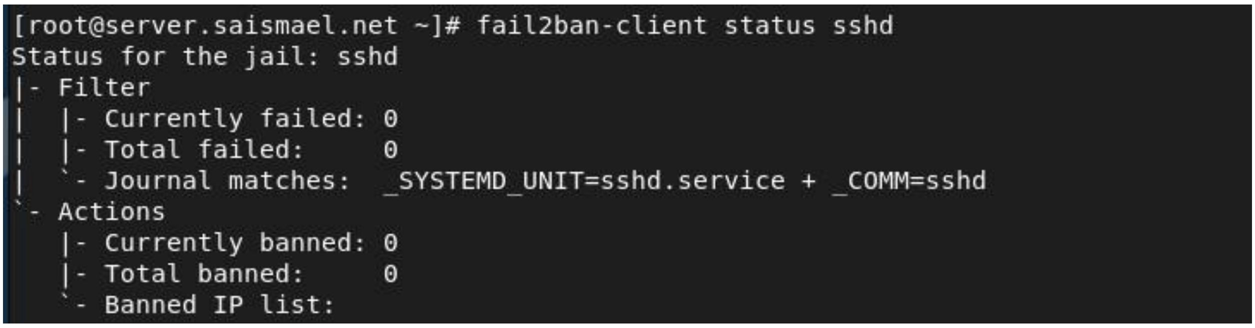
```
[root@server.saismael.net ~]# fail2ban-client status
Status
|- Number of jail:      14
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegoog
bot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apa
e-shellshock, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@server.saismael.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.saismael.net ~]# fail2ban-client set sshd maxretry 2
2
```

2. Посмотрел статус защиты SSH в fail2ban:



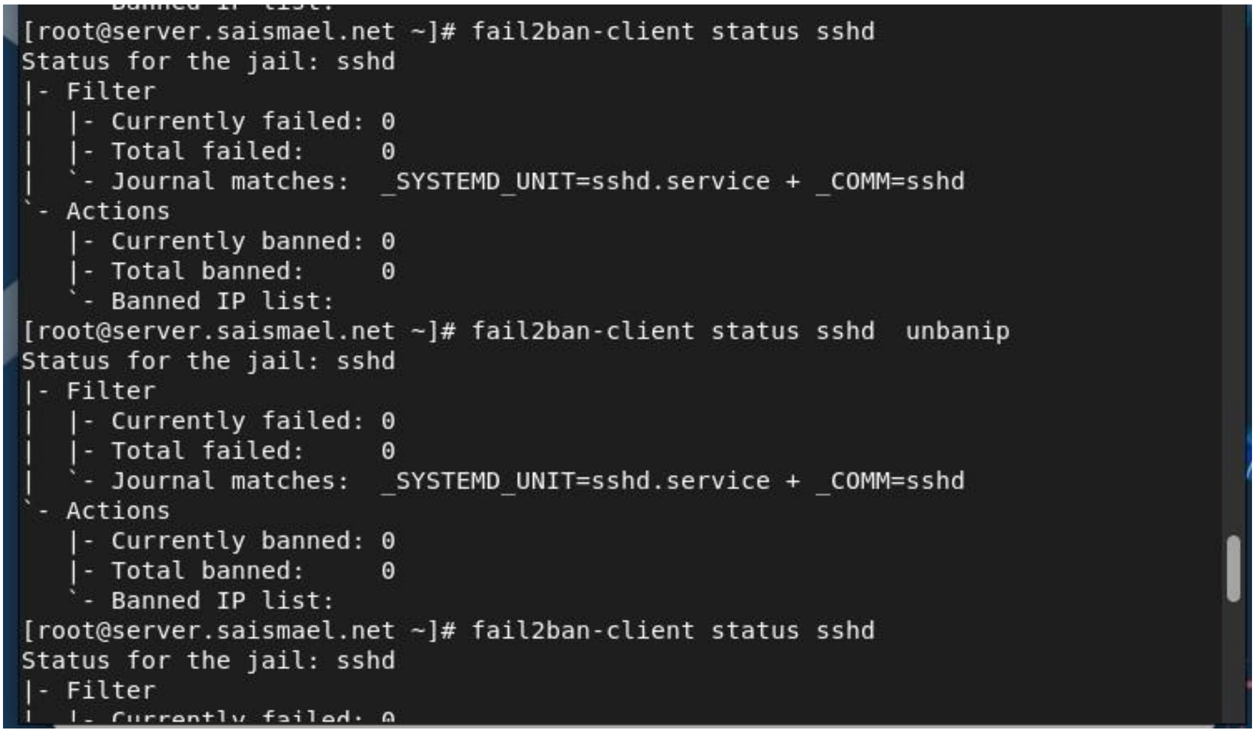
```
[root@server.saismael.net ~]# ssh saismael@server.saismael.net
The authenticity of host 'server.saismael.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqbOam9bCTBqb0qNzuP7z0xlgOqvGhkHxMkw2sQdblo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.saismael.net' (ED25519) to the list of known hosts.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
saismael@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic
,password).
```

3. Установил максимальное количество ошибок для SSH, равное 2:



```
[root@server.saismael.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:
```

4. С клиента попытался зайти по SSH на сервер с неправильным паролем.



```
   `- Banned IP list:
[root@server.saismael.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.saismael.net ~]# fail2ban-client status sshd  unbanip
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.saismael.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
```

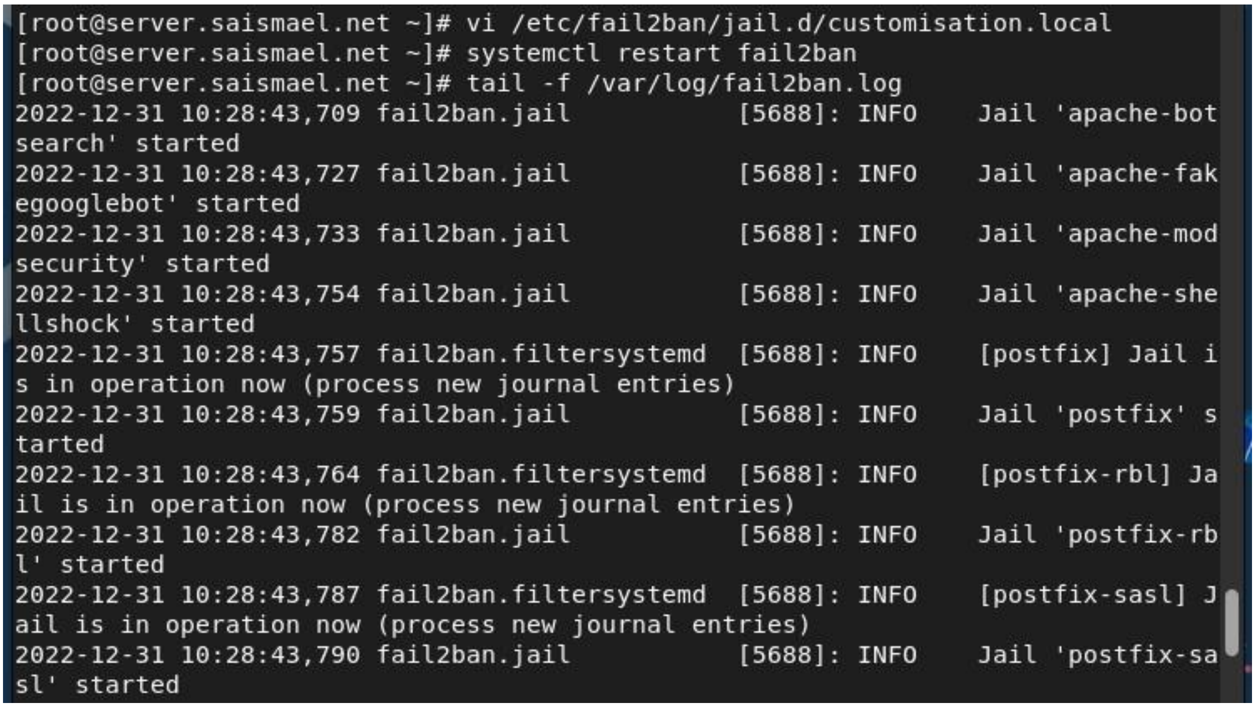
5. На сервере посмотрел статус защиты SSH:

(В первый раз блокировка не попала на запись, пришлось повторить)

6. Разблокировал IP-адрес клиента:

7. Вновь посмотрел статус защиты SSH

8. На сервере внес изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента:

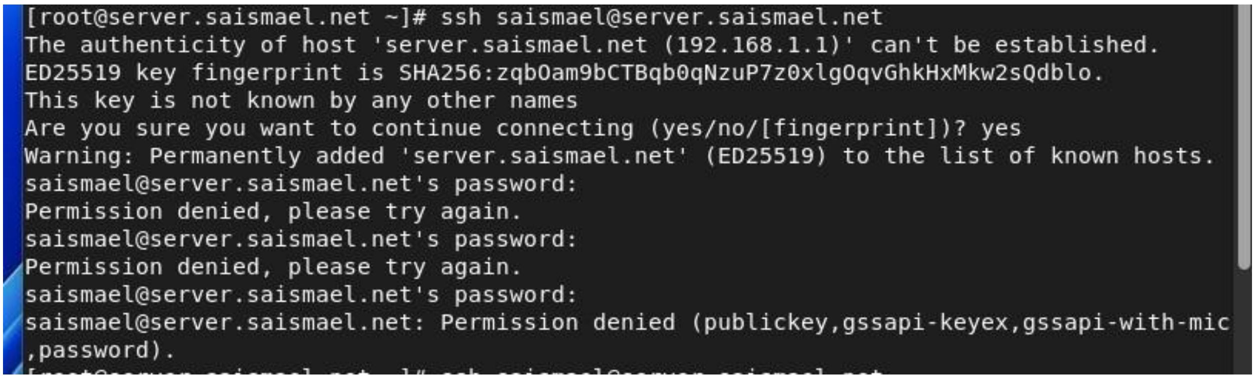


```
[root@server.saismael.net ~]# vi /etc/fail2ban/jail.d/customisation.local
[root@server.saismael.net ~]# systemctl restart fail2ban
[root@server.saismael.net ~]# tail -f /var/log/fail2ban.log
2022-12-31 10:28:43,709 fail2ban.jail           [5688]: INFO    Jail 'apache-bot
search' started
2022-12-31 10:28:43,727 fail2ban.jail           [5688]: INFO    Jail 'apache-fak
egooglebot' started
2022-12-31 10:28:43,733 fail2ban.jail           [5688]: INFO    Jail 'apache-mod
security' started
2022-12-31 10:28:43,754 fail2ban.jail           [5688]: INFO    Jail 'apache-she
llshock' started
2022-12-31 10:28:43,757 fail2ban.filtersystemd  [5688]: INFO    [postfix] Jail i
s in operation now (process new journal entries)
2022-12-31 10:28:43,759 fail2ban.jail           [5688]: INFO    Jail 'postfix' s
tarted
2022-12-31 10:28:43,764 fail2ban.filtersystemd  [5688]: INFO    [postfix-rbl] Ja
il is in operation now (process new journal entries)
2022-12-31 10:28:43,782 fail2ban.jail           [5688]: INFO    Jail 'postfix-rb
l' started
2022-12-31 10:28:43,787 fail2ban.filtersystemd  [5688]: INFO    [postfix-sasl] J
ail is in operation now (process new journal entries)
2022-12-31 10:28:43,790 fail2ban.jail           [5688]: INFO    Jail 'postfix-sa
sl' started
```

9. Перезапустил fail2ban.

10. Посмотрел журнал событий:

11. Вновь попытался войти с клиента на сервер с неправильным паролем и посмотрел статус защиты SSH

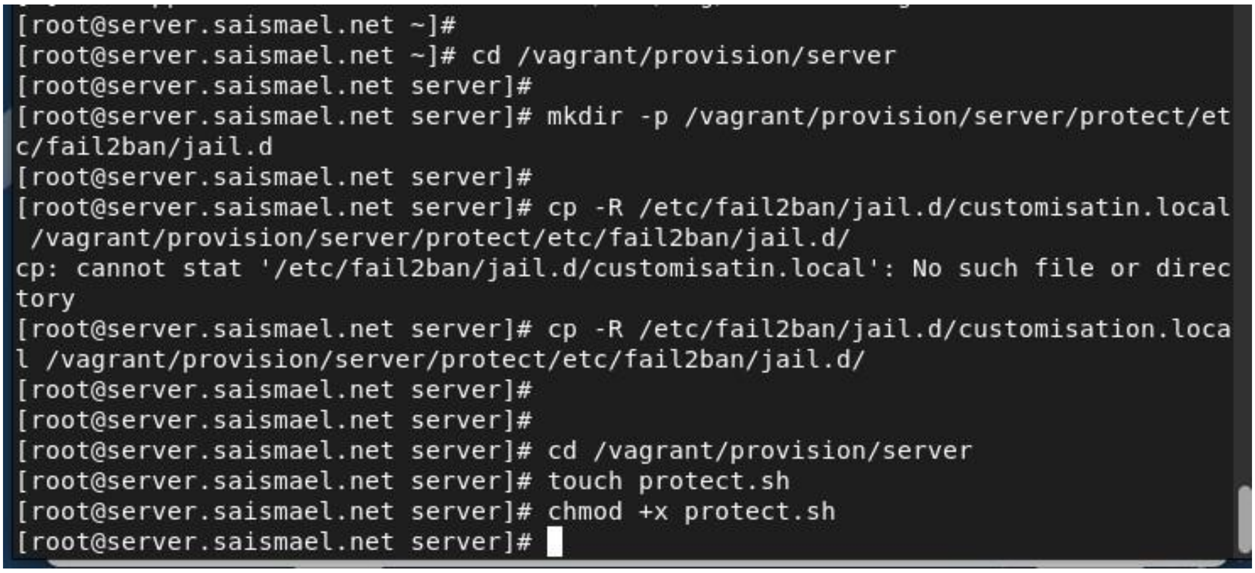


```
[root@server.saismael.net ~]# ssh saismael@server.saismael.net
The authenticity of host 'server.saismael.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqbOam9bCTBqb0qNzuP7z0xlgOqvGhkHxMkw2sQdblo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.saismael.net' (ED25519) to the list of known hosts.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
saismael@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic
,password).
[root@server.saismael.net ~]# ssh saismael@server.saismael.net
```

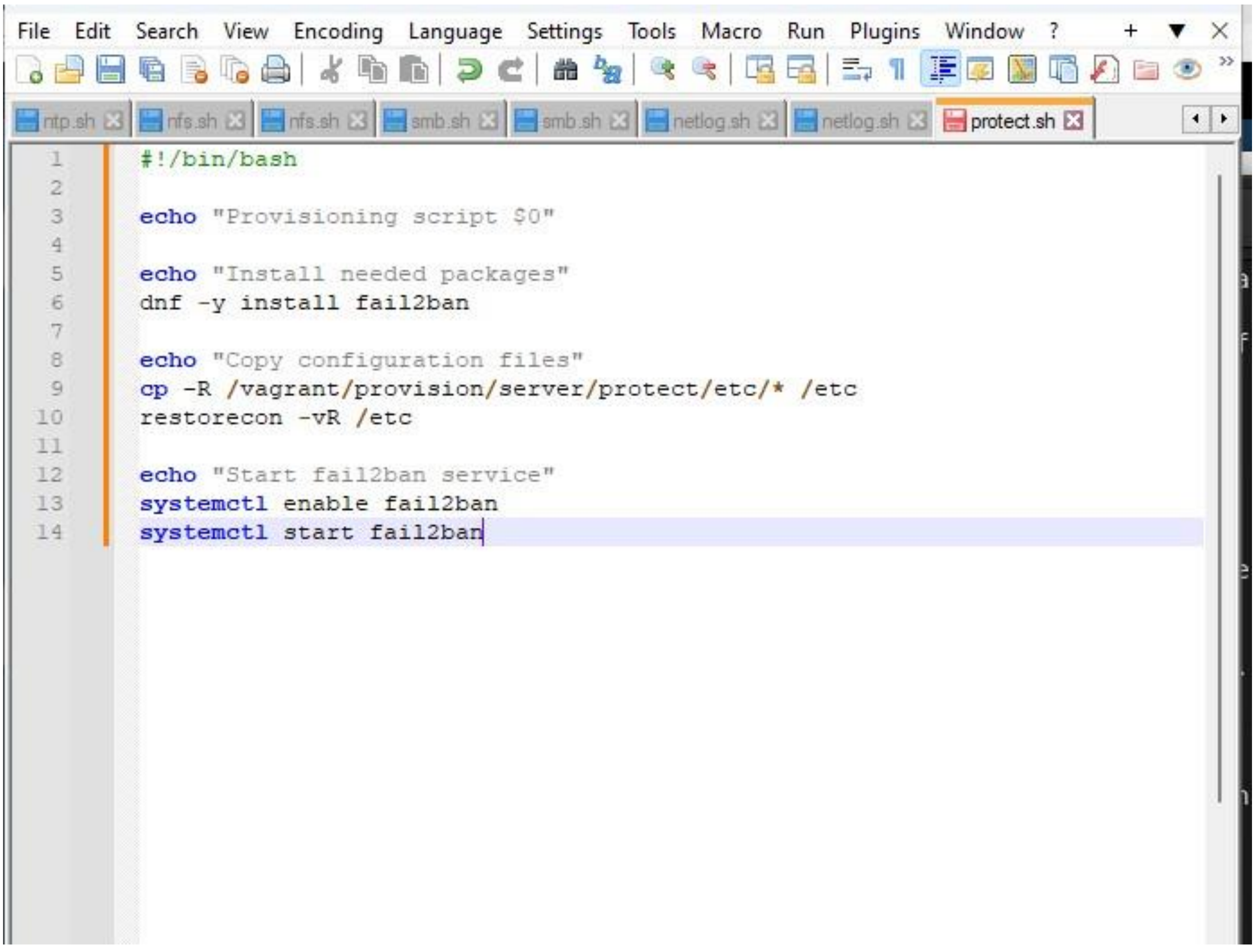
16.4.3. Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог protect,

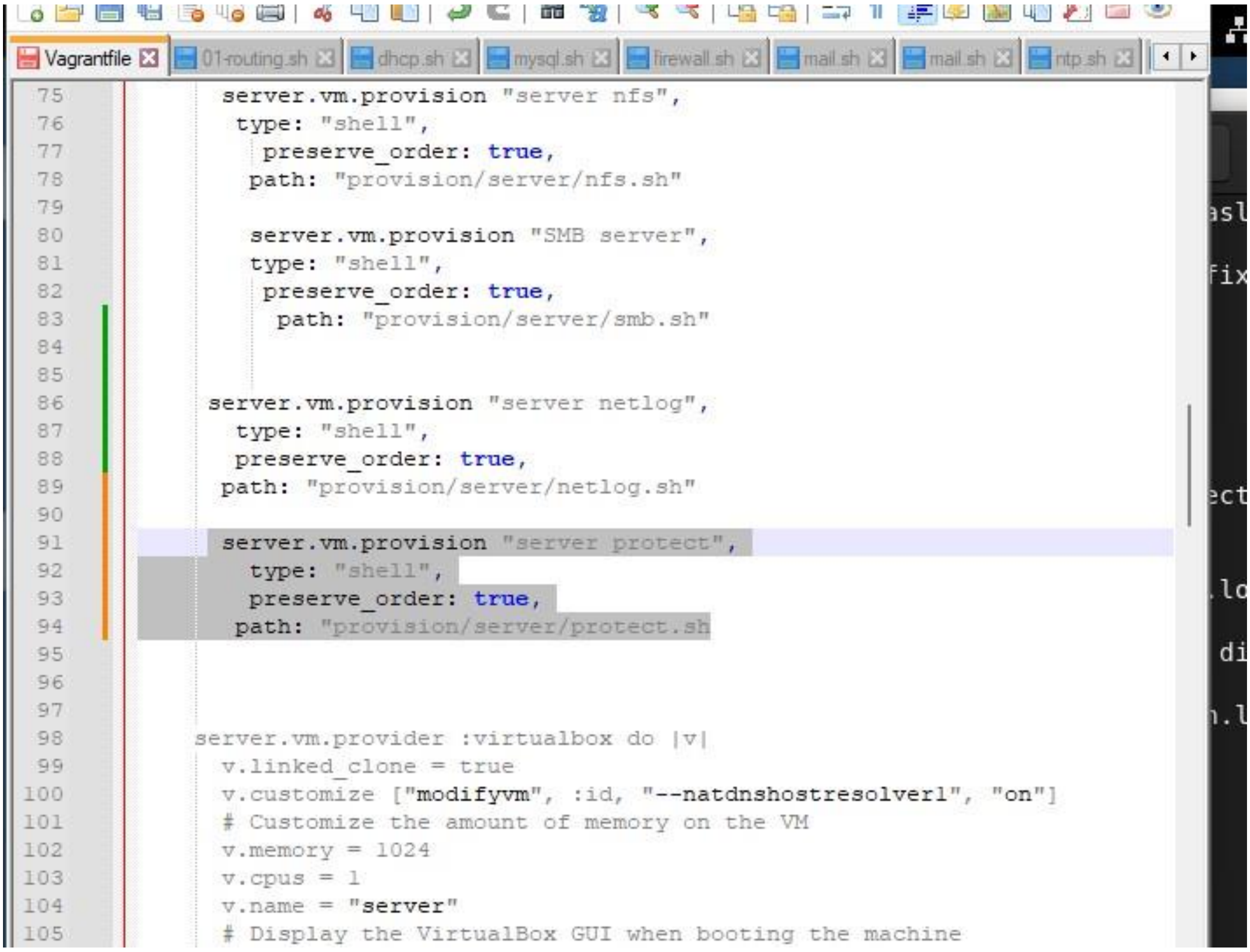
2. В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh:



```
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# cd /vagrant/provision/server
[root@server.saismael.net server]#
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/protect/et
c/fail2ban/jail.d
[root@server.saismael.net server]#
[root@server.saismael.net server]# cp -R /etc/fail2ban/jail.d/customisatin.local
 /vagrant/provision/server/protect/etc/fail2ban/jail.d/
cp: cannot stat '/etc/fail2ban/jail.d/customisatin.local': No such file or direc
tory
[root@server.saismael.net server]# cp -R /etc/fail2ban/jail.d/customisation.loca
l /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.saismael.net server]#
[root@server.saismael.net server]#
[root@server.saismael.net server]# cd /vagrant/provision/server
[root@server.saismael.net server]# touch protect.sh
[root@server.saismael.net server]# chmod +x protect.sh
[root@server.saismael.net server]#
```


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
ntp.sh
nfs.sh
nfs.sh
smb.sh
smb.sh
netlog.sh
netlog.sh
protect.sh

```bash
#!/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
```



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

          server.vm.provision "SMB server",
          type: "shell",
           preserve_order: true,
            path: "provision/server/smb.sh"


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

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



      server.vm.provider :virtualbox do |v|
        v.linked_clone = true
        v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
        # Customize the amount of memory on the VM
        v.memory = 1024
        v.cpus = 1
        v.name = "server"
        # Display the VirtualBox GUI when booting the machine
```

Вывод

Получил навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».