РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

Отчет лабораторной работы 16

Дисциплина: Администрирование сетевых подсистем

Студент: Астахова Марина

Группа: НПИбд-02-23

Тема: Базовая защита от атак типа «brute force»

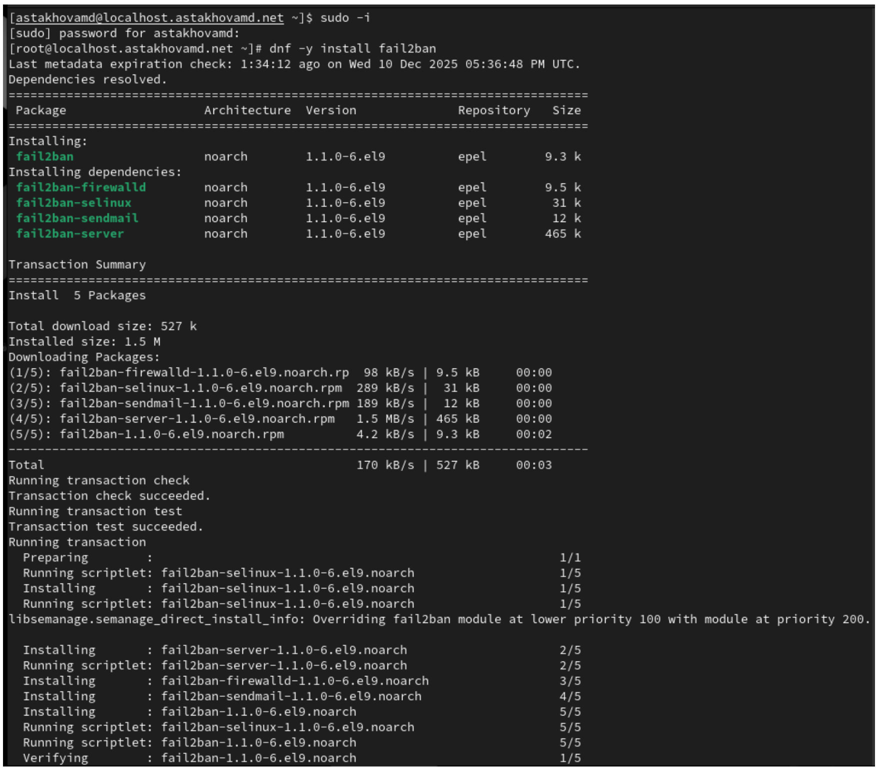
16.1. Цель работы.

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

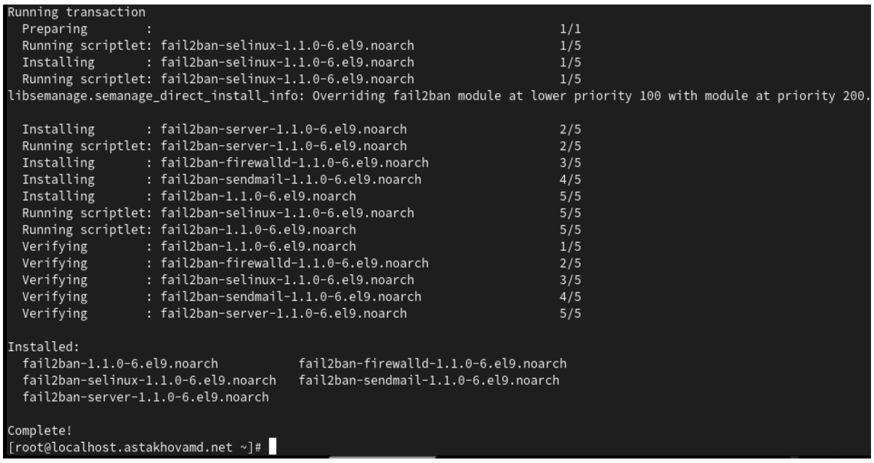
16.2. Выполнение работы

16.2.1. Защита с помощью Fail2ban

На сервере установим Fail2ban

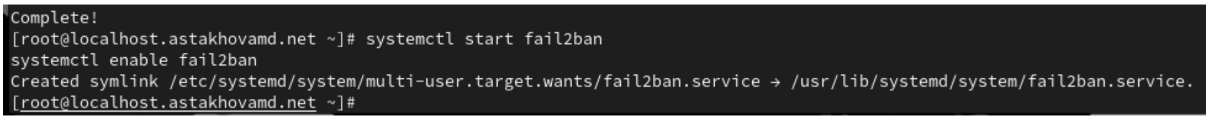


```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i
[sudo] password for astakhovamd:
[root@localhost.astakhovamd.net ~]# dnf -y install fail2ban
Last metadata expiration check: 1:34:12 ago on Wed 10 Dec 2025 05:36:48 PM UTC.
Dependencies resolved.
================================================================================
 Package                   Architecture  Version             Repository   Size
================================================================================
Installing:
 fail2ban                  noarch        1.1.0-6.el9         epel        9.3 k
Installing dependencies:
 fail2ban-firewalld        noarch        1.1.0-6.el9         epel        9.5 k
 fail2ban-selinux          noarch        1.1.0-6.el9         epel         31 k
 fail2ban-sendmail         noarch        1.1.0-6.el9         epel         12 k
 fail2ban-server           noarch        1.1.0-6.el9         epel        465 k

Transaction Summary
================================================================================
Install  5 Packages

Total download size: 527 k
Installed size: 1.5 M
Downloading Packages:
(1/5): fail2ban-firewalld-1.1.0-6.el9.noarch.rp  98 kB/s | 9.5 kB     00:00
(2/5): fail2ban-selinux-1.1.0-6.el9.noarch.rpm  289 kB/s |  31 kB     00:00
(3/5): fail2ban-sendmail-1.1.0-6.el9.noarch.rpm 189 kB/s |  12 kB     00:00
(4/5): fail2ban-server-1.1.0-6.el9.noarch.rpm   1.5 MB/s | 465 kB     00:00
(5/5): fail2ban-1.1.0-6.el9.noarch.rpm          4.2 kB/s | 9.3 kB     00:02
--------------------------------------------------------------------------------
Total                                           170 kB/s | 527 kB     00:03
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Installing       : fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower priority 100 with module at priority 200.

  Installing       : fail2ban-server-1.1.0-6.el9.noarch                     2/5
  Running scriptlet: fail2ban-server-1.1.0-6.el9.noarch                     2/5
  Installing       : fail2ban-firewalld-1.1.0-6.el9.noarch                  3/5
  Installing       : fail2ban-sendmail-1.1.0-6.el9.noarch                   4/5
  Installing       : fail2ban-1.1.0-6.el9.noarch                            5/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    5/5
  Running scriptlet: fail2ban-1.1.0-6.el9.noarch                            5/5
  Verifying        : fail2ban-1.1.0-6.el9.noarch                            1/5
```



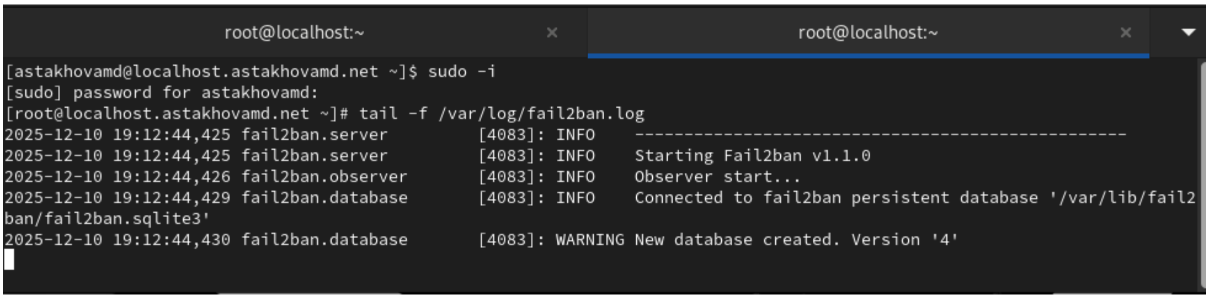
```
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Installing       : fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower priority 100 with module at priority 200.

  Installing       : fail2ban-server-1.1.0-6.el9.noarch                     2/5
  Running scriptlet: fail2ban-server-1.1.0-6.el9.noarch                     2/5
  Installing       : fail2ban-firewalld-1.1.0-6.el9.noarch                  3/5
  Installing       : fail2ban-sendmail-1.1.0-6.el9.noarch                   4/5
  Installing       : fail2ban-1.1.0-6.el9.noarch                            5/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    5/5
  Running scriptlet: fail2ban-1.1.0-6.el9.noarch                            5/5
  Verifying        : fail2ban-1.1.0-6.el9.noarch                            1/5
  Verifying        : fail2ban-firewalld-1.1.0-6.el9.noarch                  2/5
  Verifying        : fail2ban-selinux-1.1.0-6.el9.noarch                    3/5
  Verifying        : fail2ban-sendmail-1.1.0-6.el9.noarch                   4/5
  Verifying        : fail2ban-server-1.1.0-6.el9.noarch                     5/5

Installed:
  fail2ban-1.1.0-6.el9.noarch          fail2ban-firewalld-1.1.0-6.el9.noarch
  fail2ban-selinux-1.1.0-6.el9.noarch   fail2ban-sendmail-1.1.0-6.el9.noarch
  fail2ban-server-1.1.0-6.el9.noarch

Complete!
[root@localhost.astakhovamd.net ~]# 
```

Запустим сервер fail2ban:



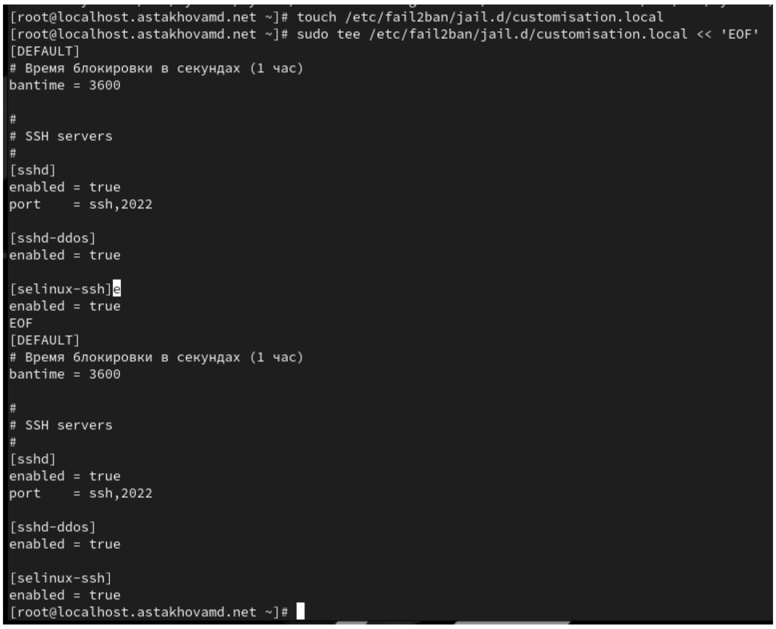
```
Complete!
[root@localhost.astakhovamd.net ~]# systemctl start fail2ban
systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[root@localhost.astakhovamd.net ~]#
```

В дополнительном терминале запустим просмотр журнала событий fail2ban:



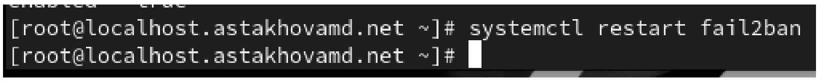
```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i
[sudo] password for astakhovamd:
[root@localhost.astakhovamd.net ~]# tail -f /var/log/fail2ban.log
2025-12-10 19:12:44,425 fail2ban.server         [4083]: INFO    --------------------------------------------------
2025-12-10 19:12:44,425 fail2ban.server         [4083]: INFO    Starting Fail2ban v1.1.0
2025-12-10 19:12:44,426 fail2ban.observer       [4083]: INFO    Observer start...
2025-12-10 19:12:44,429 fail2ban.database       [4083]: INFO    Connected to fail2ban persistent database '/var/lib/fail2
ban/fail2ban.sqlite3'
2025-12-10 19:12:44,430 fail2ban.database       [4083]: WARNING New database created. Version '4'
```

Создаем файл с локальной конфигурацией fail2ban:



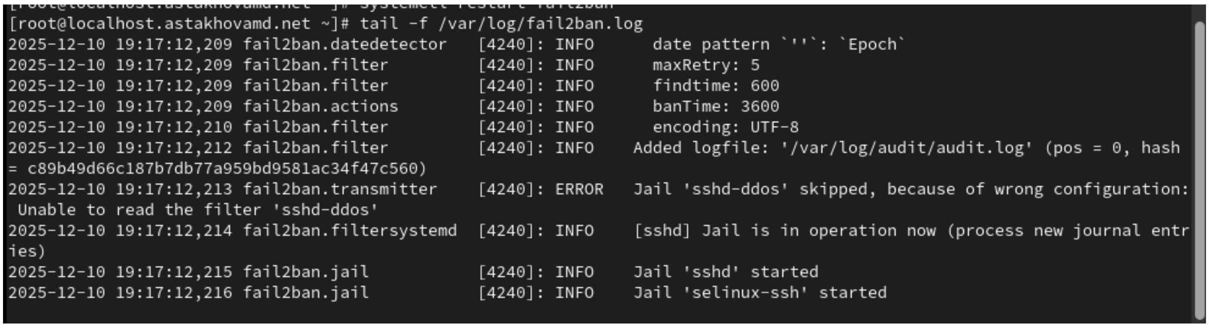
```
[root@localhost.astakhovamd.net ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@localhost.astakhovamd.net ~]# sudo tee /etc/fail2ban/jail.d/customisation.local << 'EOF'
[DEFAULT]
# Время блокировки в секундах (1 час)
bantime = 3600

#
# SSH servers
#
[sshd]
enabled = true
port    = ssh,2022

[sshd-ddos]
enabled = true

[selinux-ssh]e
enabled = true
EOF
[DEFAULT]
# Время блокировки в секундах (1 час)
bantime = 3600

#
# SSH servers
#
[sshd]
enabled = true
port    = ssh,2022

[sshd-ddos]
enabled = true

[selinux-ssh]
enabled = true
[root@localhost.astakhovamd.net ~]#
```

Перезапустим



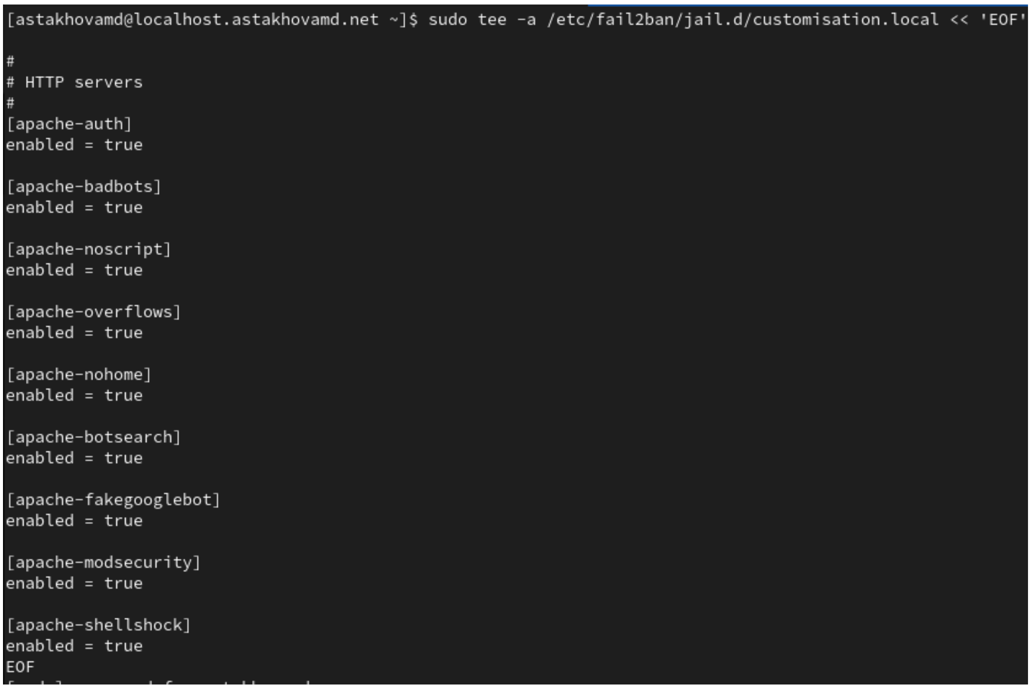
```
[root@localhost.astakhovamd.net ~]# systemctl restart fail2ban
[root@localhost.astakhovamd.net ~]#
```

Посмотрим журнал событий



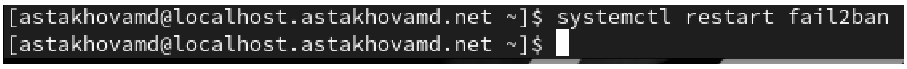
```
[root@localhost.astakhovamd.net ~]# systemctl restart fail2ban
[root@localhost.astakhovamd.net ~]# tail -f /var/log/fail2ban.log
2025-12-10 19:17:12,209 fail2ban.datedetector   [4240]: INFO      date pattern `''`: `Epoch`
2025-12-10 19:17:12,209 fail2ban.filter         [4240]: INFO      maxRetry: 5
2025-12-10 19:17:12,209 fail2ban.filter         [4240]: INFO      findtime: 600
2025-12-10 19:17:12,209 fail2ban.actions        [4240]: INFO      banTime: 3600
2025-12-10 19:17:12,210 fail2ban.filter         [4240]: INFO      encoding: UTF-8
2025-12-10 19:17:12,212 fail2ban.filter         [4240]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash
= c89b49d66c187b7db77a959bd9581ac34f47c560)
2025-12-10 19:17:12,213 fail2ban.transmitter    [4240]: ERROR   Jail 'sshd-ddos' skipped, because of wrong configuration:
 Unable to read the filter 'sshd-ddos'
2025-12-10 19:17:12,214 fail2ban.filtersystemd  [4240]: INFO    [sshd] Jail is in operation now (process new journal entr
ies)
2025-12-10 19:17:12,215 fail2ban.jail           [4240]: INFO    Jail 'sshd' started
2025-12-10 19:17:12,216 fail2ban.jail           [4240]: INFO    Jail 'selinux-ssh' started
```

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



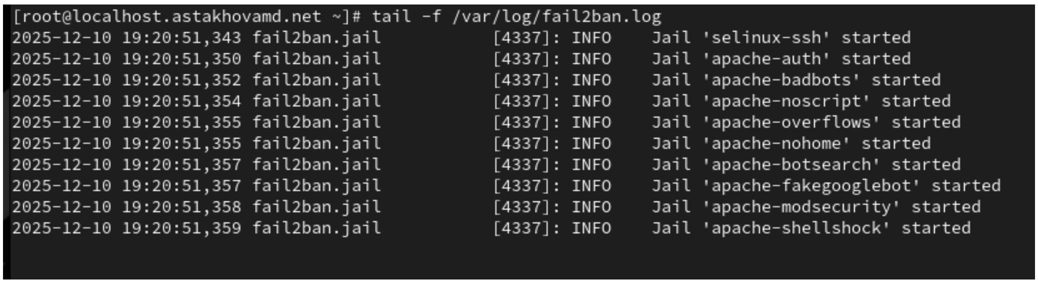
```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo tee -a /etc/fail2ban/jail.d/customisation.local << 'EOF'

#
# 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
EOF
```

Перезапустим:



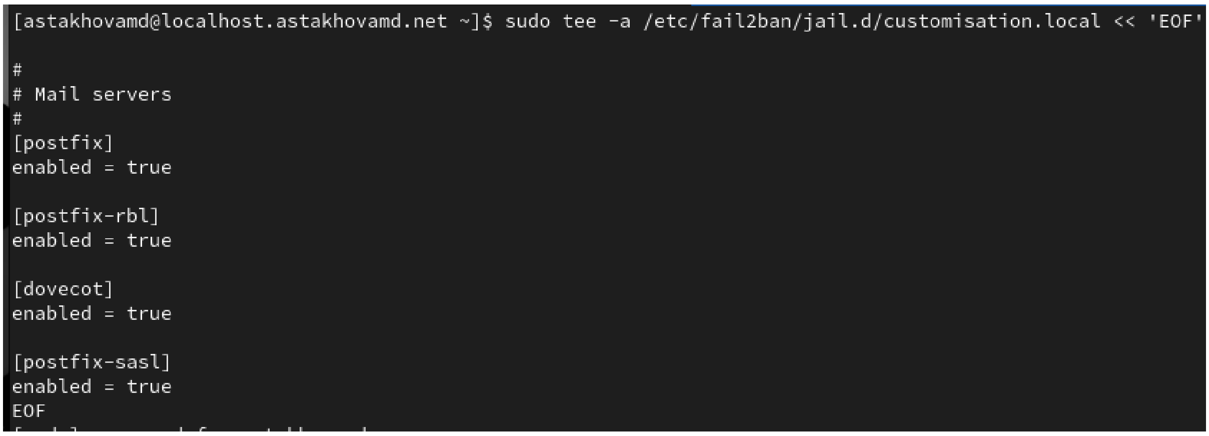
```
[astakhovamd@localhost.astakhovamd.net ~]$ systemctl restart fail2ban
[astakhovamd@localhost.astakhovamd.net ~]$
```

Посмотрим журнал событий:



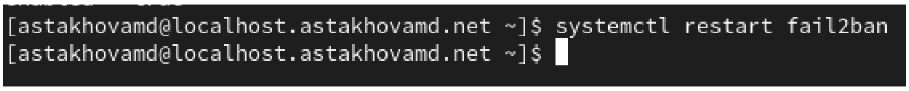
```
[root@localhost.astakhovamd.net ~]# tail -f /var/log/fail2ban.log
2025-12-10 19:20:51,343 fail2ban.jail           [4337]: INFO    Jail 'selinux-ssh' started
2025-12-10 19:20:51,350 fail2ban.jail           [4337]: INFO    Jail 'apache-auth' started
2025-12-10 19:20:51,352 fail2ban.jail           [4337]: INFO    Jail 'apache-badbots' started
2025-12-10 19:20:51,354 fail2ban.jail           [4337]: INFO    Jail 'apache-noscript' started
2025-12-10 19:20:51,355 fail2ban.jail           [4337]: INFO    Jail 'apache-overflows' started
2025-12-10 19:20:51,355 fail2ban.jail           [4337]: INFO    Jail 'apache-nohome' started
2025-12-10 19:20:51,357 fail2ban.jail           [4337]: INFO    Jail 'apache-botsearch' started
2025-12-10 19:20:51,357 fail2ban.jail           [4337]: INFO    Jail 'apache-fakegooglebot' started
2025-12-10 19:20:51,358 fail2ban.jail           [4337]: INFO    Jail 'apache-modsecurity' started
2025-12-10 19:20:51,359 fail2ban.jail           [4337]: INFO    Jail 'apache-shellshock' started
```

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

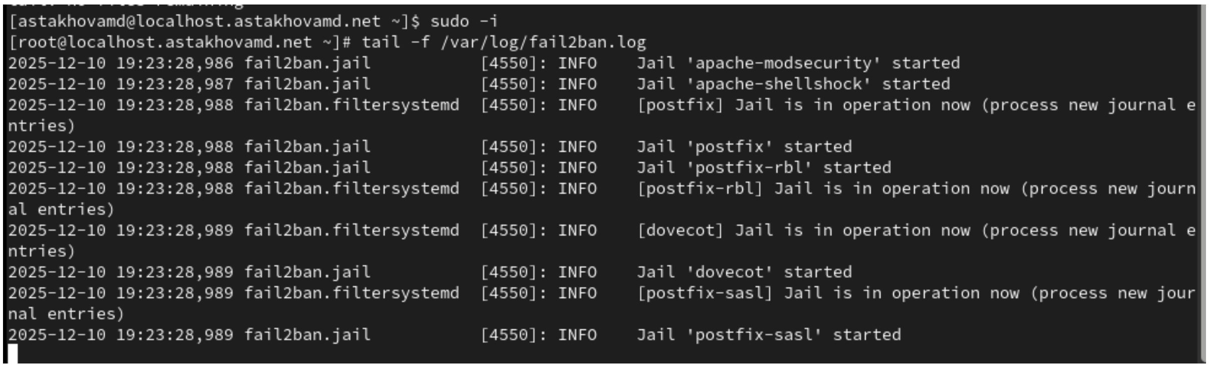


```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo tee -a /etc/fail2ban/jail.d/customisation.local << 'EOF'

#
# Mail servers
#
[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
EOF
```

Перезапустим и посмотрим журнал:



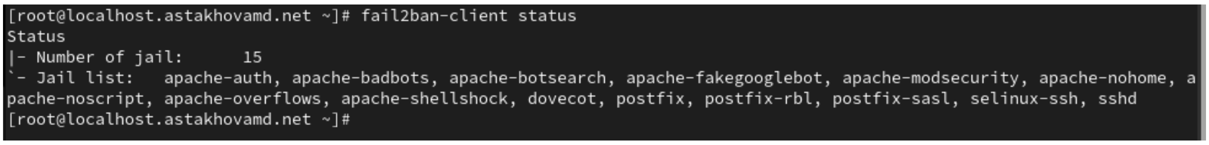
```
[astakhovamd@localhost.astakhovamd.net ~]$ systemctl restart fail2ban
[astakhovamd@localhost.astakhovamd.net ~]$ 
```



```
[astakhovamd@localhost.astakhovamd.net ~]$ sudo -i
[root@localhost.astakhovamd.net ~]# tail -f /var/log/fail2ban.log
2025-12-10 19:23:28,986 fail2ban.jail           [4550]: INFO    Jail 'apache-modsecurity' started
2025-12-10 19:23:28,987 fail2ban.jail           [4550]: INFO    Jail 'apache-shellshock' started
2025-12-10 19:23:28,988 fail2ban.filtersystemd  [4550]: INFO    [postfix] Jail is in operation now (process new journal e
ntries)
2025-12-10 19:23:28,988 fail2ban.jail           [4550]: INFO    Jail 'postfix' started
2025-12-10 19:23:28,988 fail2ban.jail           [4550]: INFO    Jail 'postfix-rbl' started
2025-12-10 19:23:28,988 fail2ban.filtersystemd  [4550]: INFO    [postfix-rbl] Jail is in operation now (process new journ
al entries)
2025-12-10 19:23:28,989 fail2ban.filtersystemd  [4550]: INFO    [dovecot] Jail is in operation now (process new journal e
ntries)
2025-12-10 19:23:28,989 fail2ban.jail           [4550]: INFO    Jail 'dovecot' started
2025-12-10 19:23:28,989 fail2ban.filtersystemd  [4550]: INFO    [postfix-sasl] Jail is in operation now (process new jour
nal entries)
2025-12-10 19:23:28,989 fail2ban.jail           [4550]: INFO    Jail 'postfix-sasl' started
```

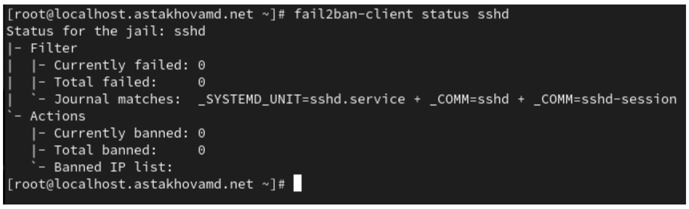
16.2.2. Проверка работы Fail2ban

Посмотрим статус:



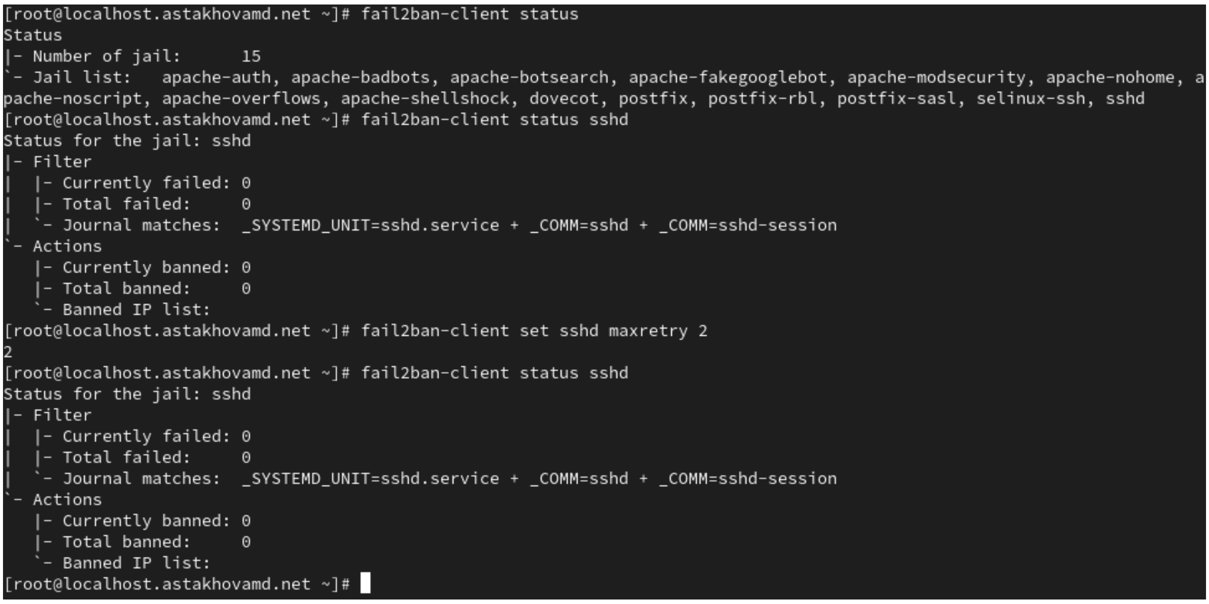
```
[root@localhost.astakhovamd.net ~]# fail2ban-client status
Status
|- Number of jail:      15
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, a
pache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@localhost.astakhovamd.net ~]#
```

Посмотрим статус защиты SSH



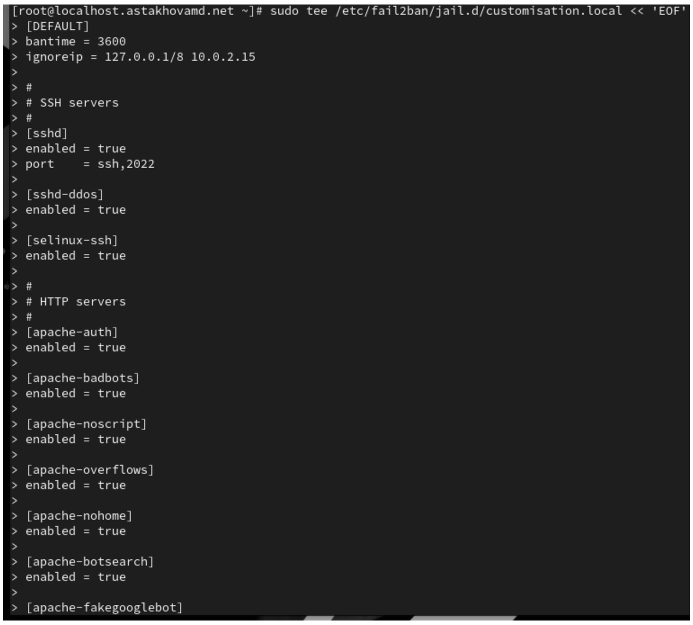
```
[root@localhost.astakhovamd.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@localhost.astakhovamd.net ~]# 
```

Установим максимальное количество ошибок для SSH, равное 2:

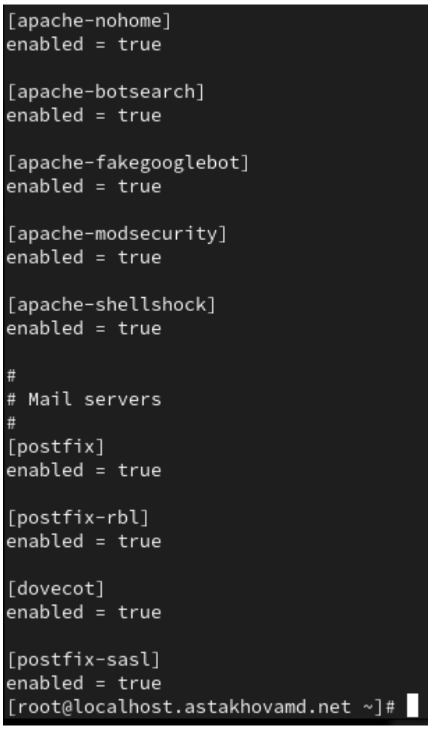


```
[root@localhost.astakhovamd.net ~]# fail2ban-client status
Status
|- Number of jail:      15
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, a
pache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@localhost.astakhovamd.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@localhost.astakhovamd.net ~]# fail2ban-client set sshd maxretry 2
2
[root@localhost.astakhovamd.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@localhost.astakhovamd.net ~]# 
```

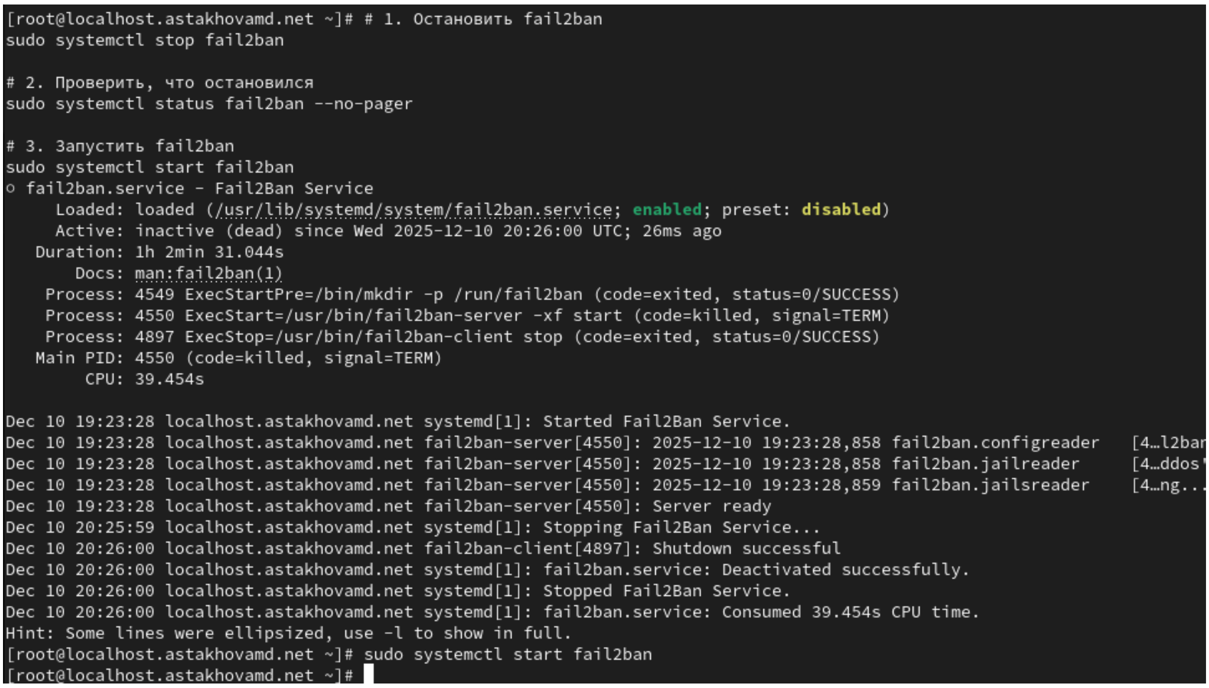
Проверим снятие блокировки:



```
[root@localhost.astakhovamd.net ~]# sudo tee /etc/fail2ban/jail.d/customisation.local << 'EOF'
> [DEFAULT]
> bantime = 3600
> ignoreip = 127.0.0.1/8 10.0.2.15
>
> #
> # SSH servers
> #
> [sshd]
> enabled = true
> port    = ssh,2022
>
> [sshd-ddos]
> enabled = true
>
> [selinux-ssh]
> enabled = true
>
> #
> # HTTP servers
> #
> [apache-auth]
> enabled = true
>
> [apache-badbots]
> enabled = true
>
> [apache-noscript]
> enabled = true
>
> [apache-overflows]
> enabled = true
>
> [apache-nohome]
> enabled = true
>
> [apache-botsearch]
> enabled = true
>
> [apache-fakegooglebot]
```

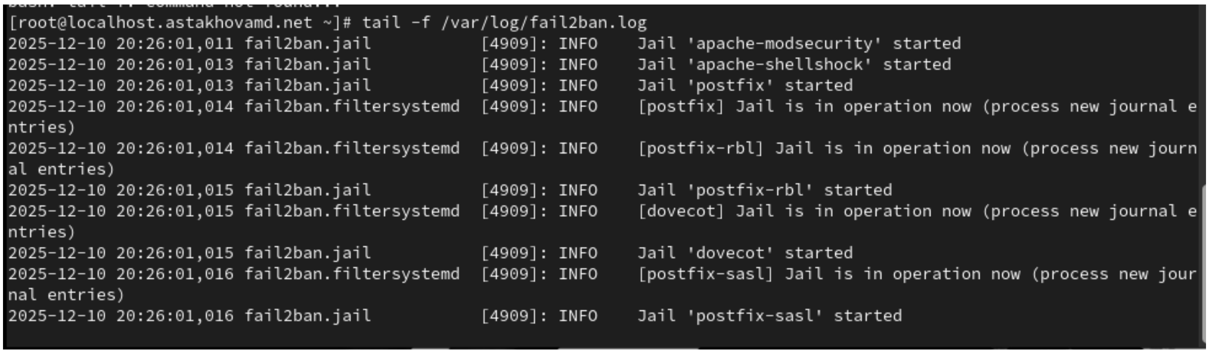


```
[apache-nohome]
enabled = true

[apache-botsearch]
enabled = true

[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true

#
# Mail servers
#
[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
[root@localhost.astakhovamd.net ~]#
```



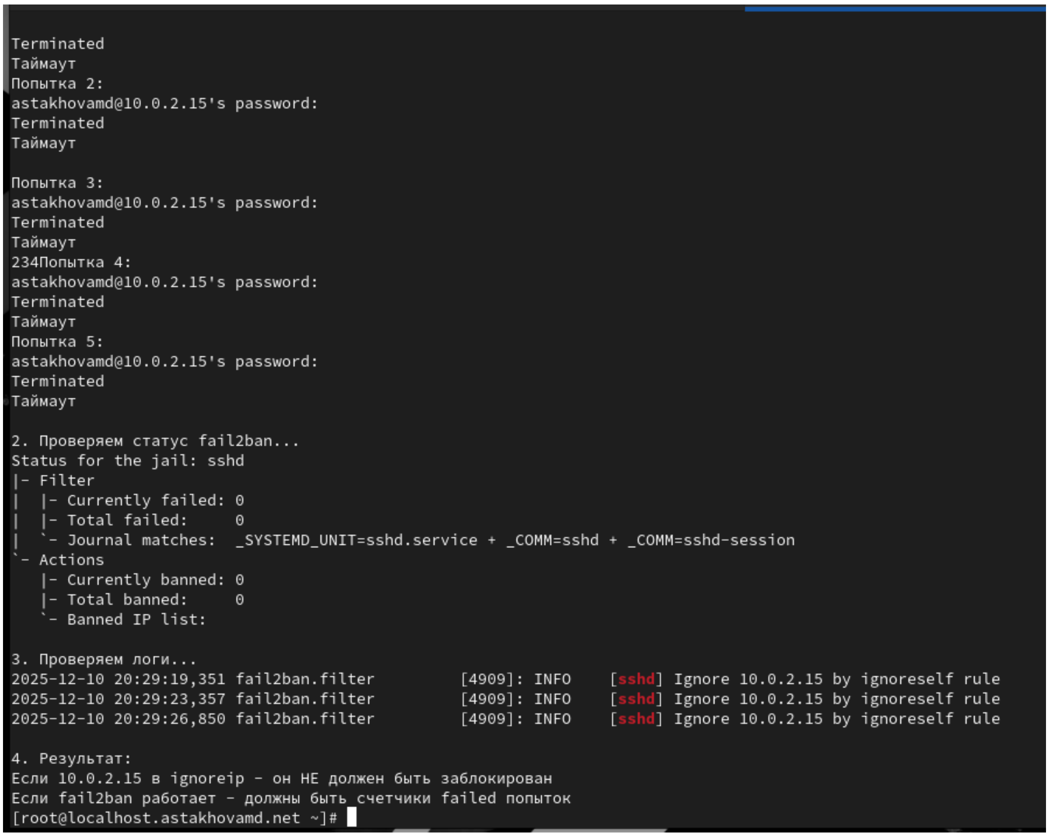
```
[root@localhost.astakhovamd.net ~]# # 1. Остановить fail2ban
sudo systemctl stop fail2ban

# 2. Проверить, что остановился
sudo systemctl status fail2ban --no-pager

# 3. Запустить fail2ban
sudo systemctl start fail2ban
○ fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: disabled)
     Active: inactive (dead) since Wed 2025-12-10 20:26:00 UTC; 26ms ago
   Duration: 1h 2min 31.044s
       Docs: man:fail2ban(1)
    Process: 4549 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
    Process: 4550 ExecStart=/usr/bin/fail2ban-server -xf start (code=killed, signal=TERM)
    Process: 4897 ExecStop=/usr/bin/fail2ban-client stop (code=exited, status=0/SUCCESS)
   Main PID: 4550 (code=killed, signal=TERM)
        CPU: 39.454s

Dec 10 19:23:28 localhost.astakhovamd.net systemd[1]: Started Fail2Ban Service.
Dec 10 19:23:28 localhost.astakhovamd.net fail2ban-server[4550]: 2025-12-10 19:23:28,858 fail2ban.configreader   [4…l2ban
Dec 10 19:23:28 localhost.astakhovamd.net fail2ban-server[4550]: 2025-12-10 19:23:28,858 fail2ban.jailreader     [4…ddos'
Dec 10 19:23:28 localhost.astakhovamd.net fail2ban-server[4550]: 2025-12-10 19:23:28,859 fail2ban.jailsreader    [4…ng...
Dec 10 19:23:28 localhost.astakhovamd.net fail2ban-server[4550]: Server ready
Dec 10 20:25:59 localhost.astakhovamd.net systemd[1]: Stopping Fail2Ban Service...
Dec 10 20:26:00 localhost.astakhovamd.net fail2ban-client[4897]: Shutdown successful
Dec 10 20:26:00 localhost.astakhovamd.net systemd[1]: fail2ban.service: Deactivated successfully.
Dec 10 20:26:00 localhost.astakhovamd.net systemd[1]: Stopped Fail2Ban Service.
Dec 10 20:26:00 localhost.astakhovamd.net systemd[1]: fail2ban.service: Consumed 39.454s CPU time.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost.astakhovamd.net ~]# sudo systemctl start fail2ban
[root@localhost.astakhovamd.net ~]#
```

Опять посмотрим журнал:



```
[root@localhost.astakhovamd.net ~]# tail -f /var/log/fail2ban.log
2025-12-10 20:26:01,011 fail2ban.jail           [4909]: INFO    Jail 'apache-modsecurity' started
2025-12-10 20:26:01,013 fail2ban.jail           [4909]: INFO    Jail 'apache-shellshock' started
2025-12-10 20:26:01,013 fail2ban.jail           [4909]: INFO    Jail 'postfix' started
2025-12-10 20:26:01,014 fail2ban.filtersystemd  [4909]: INFO    [postfix] Jail is in operation now (process new journal e
ntries)
2025-12-10 20:26:01,014 fail2ban.filtersystemd  [4909]: INFO    [postfix-rbl] Jail is in operation now (process new journ
al entries)
2025-12-10 20:26:01,015 fail2ban.jail           [4909]: INFO    Jail 'postfix-rbl' started
2025-12-10 20:26:01,015 fail2ban.filtersystemd  [4909]: INFO    [dovecot] Jail is in operation now (process new journal e
ntries)
2025-12-10 20:26:01,015 fail2ban.jail           [4909]: INFO    Jail 'dovecot' started
2025-12-10 20:26:01,016 fail2ban.filtersystemd  [4909]: INFO    [postfix-sasl] Jail is in operation now (process new jour
nal entries)
2025-12-10 20:26:01,016 fail2ban.jail           [4909]: INFO    Jail 'postfix-sasl' started
```

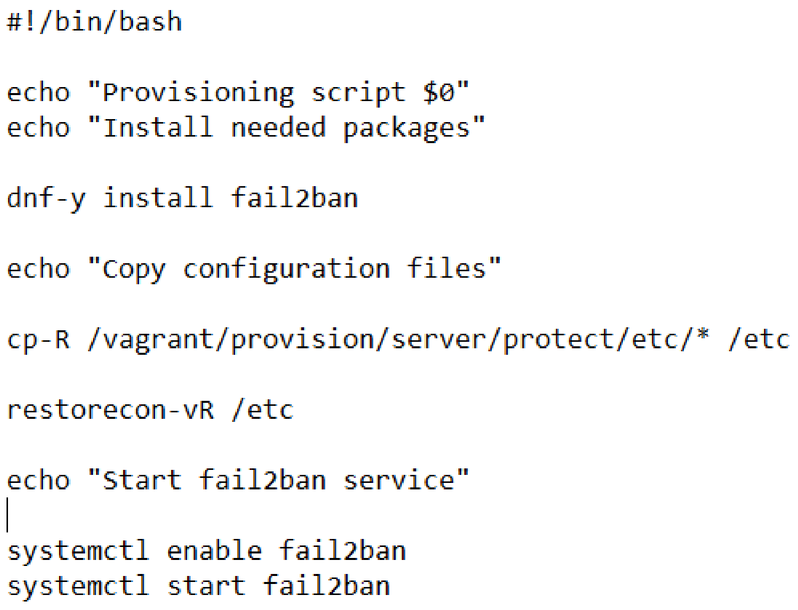
Попытаемся зайти с неправильным паролем и проверить статус защиты



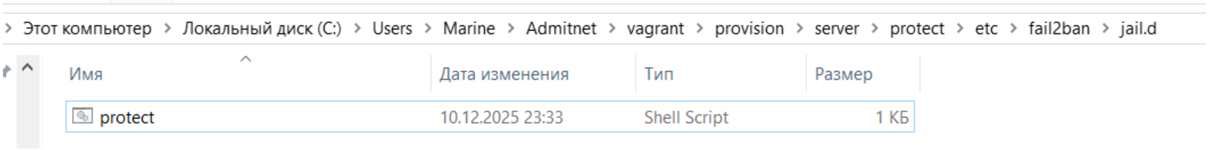
```
Terminated
Таймаут
Попытка 2:
astakhovamd@10.0.2.15's password:
Terminated
Таймаут

Попытка 3:
astakhovamd@10.0.2.15's password:
Terminated
Таймаут
234Попытка 4:
astakhovamd@10.0.2.15's password:
Terminated
Таймаут
Попытка 5:
astakhovamd@10.0.2.15's password:
Terminated
Таймаут

2. Проверяем статус fail2ban...
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:

3. Проверяем логи...
2025-12-10 20:29:19,351 fail2ban.filter         [4909]: INFO    [sshd] Ignore 10.0.2.15 by ignoreself rule
2025-12-10 20:29:23,357 fail2ban.filter         [4909]: INFO    [sshd] Ignore 10.0.2.15 by ignoreself rule
2025-12-10 20:29:26,850 fail2ban.filter         [4909]: INFO    [sshd] Ignore 10.0.2.15 by ignoreself rule

4. Результат:
Если 10.0.2.15 в ignoreip - он НЕ должен быть заблокирован
Если fail2ban работает - должны быть счетчики failed попыток
[root@localhost.astakhovamd.net ~]#
```

16.2.3. Внесение изменений в настройки внутреннего окружения виртуальных машин

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



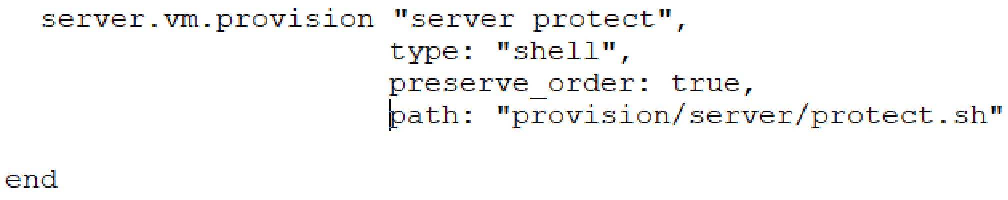
```
#!/bin/bash

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
```



Этот компьютер > Локальный диск (C:) > Users > Marine > Admitnet > vagrant > provision > server > protect > etc > fail2ban > jail.d

Имя	Дата изменения	Тип	Размер
protect	10.12.2025 23:33	Shell Script	1 КБ

Добавим изменения в vagrantfile



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

end
```

16.3. Итог работы

Были получены навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «bruteforce».

16.4 Контрольные вопросы

1. Принцип работы Fail2ban

Fail2ban — это система предотвращения вторжений, которая работает по следующему принципу:

Логи приложений → Анализ по фильтрам → Обнаружение атак → Блокировка IP → (опционально) Уведомление

2. Приоритетность файлов конфигурации

Более приоритетными являются настройки в jail.local.

Порядок приоритета:

1. */etc/fail2ban/jail.d/*.local*
2. */etc/fail2ban/jail.local*
3. */etc/fail2ban/jail.d/*.conf*
4. */etc/fail2ban/jail.conf*

3. Настройка оповещения администратора

Способ 1: Email уведомления

ini

```
[DEFAULT]
destemail = admin@ваш-домен.com
sender = fail2ban@ваш-домен.com
action = %(action_mwl)s  # mwl = ban + email с whois + лог
```

Способ 2: Telegram/Slack

bash

```
# Создайте файл действия для Telegram
sudo tee /etc/fail2ban/action.d/telegram.conf << 'EOF'
[Definition]
actionstart =
actionstop =
actioncheck =
actionban = curl -s -X POST
"https://api.telegram.org/bot<BOT_TOKEN>/sendMessage" \
-d "chat_id=<CHAT_ID>&text=IP <ip> заблокирован в <name>"
actionunban =
EOF
```

Способ 3: Использование mailx

ini

```
[DEFAULT]
mta = mailx
destemail = admin@example.com
action = %(action_mail)s
```

4. Настройки для веб-службы в /etc/fail2ban/jail.conf

Ini

```
# APACHE - аутентификация
[apache-auth]
enabled  = false                 # по умолчанию выключено
port     = http,https            # порты для мониторинга
filter   = apache-auth           # файл фильтра: /etc/fail2ban/filter.d/apache-auth.conf
logpath  = /var/log/apache2/*error.log  # путь к логам
maxretry = 6                     # максимум 6 попыток

# APACHE - плохие боты
[apache-badbots]
enabled  = false
port     = http,https
filter   = apache-badbots
logpath  = /var/log/apache2/*access.log
maxretry = 2                     # всего 2 попытки
bantime  = 172800                # блокировка на 48 часов (для ботов)
```

```
# APACHE - атаки на скрипты
[apache-noscript]
enabled  = false
port     = http,https
filter   = apache-noscript
logpath  = /var/log/apache2/*error.log
maxretry = 6

# APACHE - переполнение буфера
[apache-overflows]
enabled  = false
port     = http,https
filter   = apache-overflows
logpath  = /var/log/apache2/*error.log
maxretry = 2
```

5. Настройки для почтовой службы в /etc/fail2ban/jail.conf

ini

```
# POSTFIX - основная защита
[postfix]
enabled  = false                    # по умолчанию выключено
port     = smtp,ssmtp,submission   # SMTP порты
filter   = postfix                 # фильтр: /etc/fail2ban/filter.d/postfix.conf
logpath  = /var/log/mail.log       # путь к логам почты
maxretry = 6

# POSTFIX - SASL аутентификация
[postfix-sasl]
enabled  = false
port     = smtp,ssmtp,submission,imap2,imap3,imaps,pop3,pop3s
filter   = postfix-sasl
logpath  = /var/log/mail.log
maxretry = 6

# DOVECOT - IMAP/POP3 сервер
[dovecot]
enabled  = false
port     = pop3,pop3s,imap,imaps   # почтовые протоколы
filter   = dovecot
```

```
logpath  = /var/log/mail.log
maxretry = 5
bantime  = 1800                  # 30 минут блокировки

# SENDMAIL (альтернатива Postfix)
[sendmail-auth]
enabled  = false
port     = smtp,ssmtp,submission
filter   = sendmail-auth
logpath  = /var/log/mail.log
```

6. Действия Fail2ban при обнаружении атак

Основные действия:

1. ***Блокировка в firewall (iptables, firewalld, nftables)***
2. ***Отправка email***
3. ***Выполнение произвольной команды***
4. ***Отправка в Slack/Telegram***
5. ***Запись в syslog***

7. Получить список действующих правил

```
# 1. Список активных тюрем
sudo fail2ban-client status

# 2. Подробно о конкретной тюрьме
sudo fail2ban-client status sshd

# 3. Проверить правила firewall
sudo iptables -L -n -v | grep f2b
# или для firewalld
sudo firewall-cmd --list-all | grep -A10 "fail2ban"

# 4. Все тюрьмы с их фильтрами
sudo fail2ban-client -d | grep "\[" | head –20
```

8. Статистика заблокированных адресов

```
# 1. Общая статистика по всем тюрьмам
sudo fail2ban-client status

# 2. Статистика конкретной тюрьмы
sudo fail2ban-client status sshd | grep -E "(Currently banned|Total banned|Banned IP list)"

# 3. Логи блокировок
sudo grep "Ban " /var/log/fail2ban.log
sudo grep "Unban " /var/log/fail2ban.log

# 4. Статистика за период
sudo journalctl -u fail2ban --since "today" | grep -E "(Ban|Unban)"

# 5. Утилита fail2ban-stat
sudo fail2ban-stat
```

9. Как разблокировать IP-адрес

```
# 1. Разблокировать конкретный IP в конкретной тюрьме
sudo fail2ban-client set sshd unbanip 192.168.1.100

# 2. Разблокировать несколько IP
sudo fail2ban-client set sshd unbanip 192.168.1.100 192.168.1.101

# 3. Разблокировать во всех тюрьмах
for jail in $(sudo fail2ban-client status | grep "Jail list:" | cut -d: -f2 | tr ',' ' '); do
    sudo fail2ban-client set $jail unbanip 192.168.1.100
done

# 4. Сбросить счетчик попыток (без разблокировки)
sudo fail2ban-client set sshd delip 192.168.1.100

# 5. Посмотреть заблокированные IP перед разблокировкой
sudo fail2ban-client status sshd | grep "Banned IP list"
```

```
# 6. Полная перезагрузка тюрьмы (сброс всех блокировок)
sudo fail2ban-client reload sshd

# 7. Проверить, что IP разблокирован
sudo iptables -L -n -v | grep 192.168.1.100
```