Администрирование сетевых подсистем

Базовая защита от атак типа «brute force» (Лабораторная работа №16)

Заур Мустафаев

12 декабря 2025

Российский университет дружбы народов, Москва, Россия

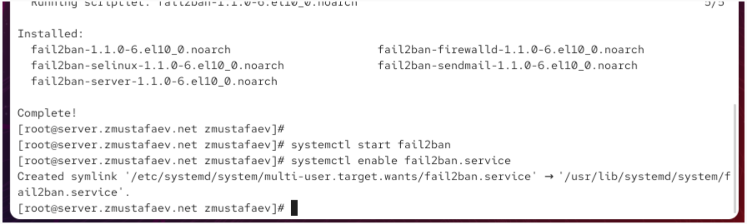
Цели и задачи работы

Цель лабораторной работы

Получение практических навыков настройки и использования Fail2ban для защиты серверных служб от атак типа «brute force».

Установка и запуск Fail2ban

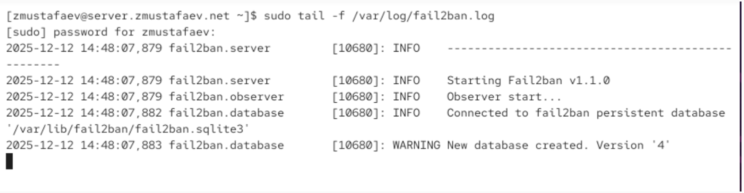
Установка пакета



```
  Running scriptlet: fail2ban-1.1.0-6.el10_0.noarch                                                       5/5

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

Complete!
[root@server.zmustafaev.net zmustafaev]#
[root@server.zmustafaev.net zmustafaev]# systemctl start fail2ban
[root@server.zmustafaev.net zmustafaev]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/f
ail2ban.service'.
[root@server.zmustafaev.net zmustafaev]# 
```

Рис. 1: Установка и запуск Fail2ban

Запуск службы

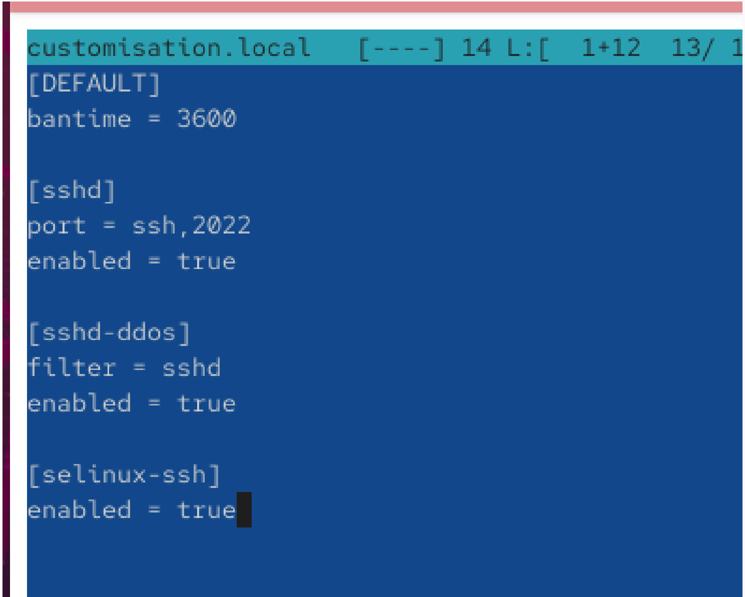


```
[zmustafaev@server.zmustafaev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for zmustafaev:
2025-12-12 14:48:07,879 fail2ban.server         [10680]: INFO    ------------------------------------------
--------
2025-12-12 14:48:07,879 fail2ban.server         [10680]: INFO    Starting Fail2ban v1.1.0
2025-12-12 14:48:07,879 fail2ban.observer       [10680]: INFO    Observer start...
2025-12-12 14:48:07,882 fail2ban.database       [10680]: INFO    Connected to fail2ban persistent database
'/var/lib/fail2ban/fail2ban.sqlite3'
2025-12-12 14:48:07,883 fail2ban.database       [10680]: WARNING New database created. Version '4'
```

Рис. 2: Запуск fail2ban и автозагрузка

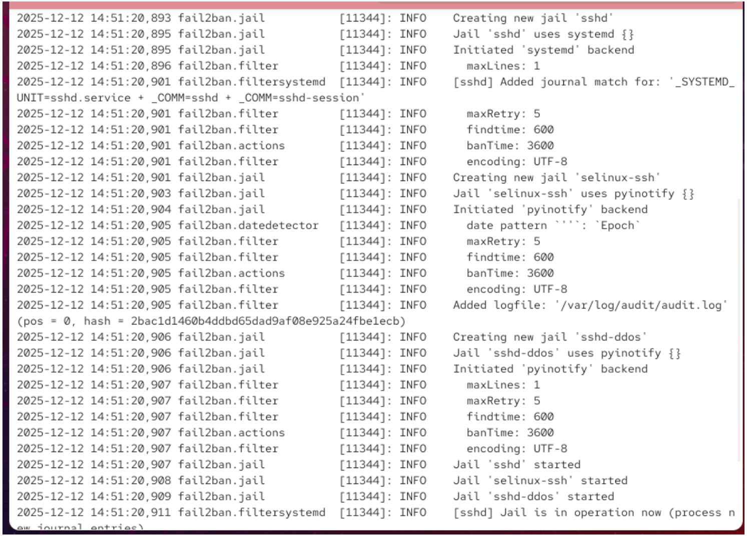
Базовая настройка Fail2ban

Просмотр журнала событий



```
customisation.local    [----] 14 L:[  1+12  13/ 1
[DEFAULT]
bantime = 3600

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

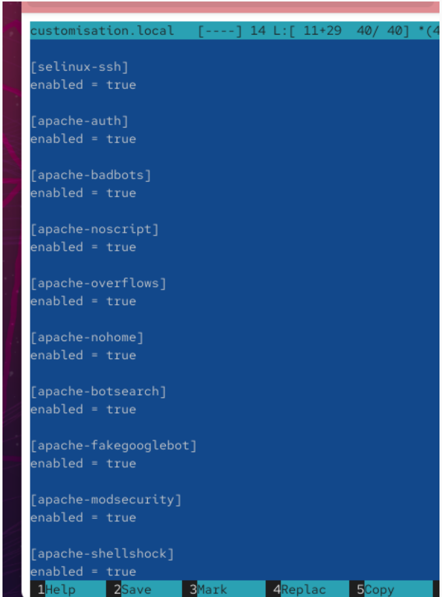
Настройка параметров SSH



```
2025-12-12 14:51:20,893 fail2ban.jail           [11344]: INFO    Creating new jail 'sshd'
2025-12-12 14:51:20,895 fail2ban.jail           [11344]: INFO    Jail 'sshd' uses systemd {}
2025-12-12 14:51:20,895 fail2ban.jail           [11344]: INFO    Initiated 'systemd' backend
2025-12-12 14:51:20,896 fail2ban.filter         [11344]: INFO      maxLines: 1
2025-12-12 14:51:20,901 fail2ban.filtersystemd  [11344]: INFO    [sshd] Added journal match for: '_SYSTEMD_
UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session'
2025-12-12 14:51:20,901 fail2ban.filter         [11344]: INFO      maxRetry: 5
2025-12-12 14:51:20,901 fail2ban.filter         [11344]: INFO      findtime: 600
2025-12-12 14:51:20,901 fail2ban.actions        [11344]: INFO      banTime: 3600
2025-12-12 14:51:20,901 fail2ban.filter         [11344]: INFO      encoding: UTF-8
2025-12-12 14:51:20,901 fail2ban.jail           [11344]: INFO    Creating new jail 'selinux-ssh'
2025-12-12 14:51:20,903 fail2ban.jail           [11344]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2025-12-12 14:51:20,904 fail2ban.jail           [11344]: INFO    Initiated 'pyinotify' backend
2025-12-12 14:51:20,905 fail2ban.datedetector   [11344]: INFO      date pattern `''`: `Epoch`
2025-12-12 14:51:20,905 fail2ban.filter         [11344]: INFO      maxRetry: 5
2025-12-12 14:51:20,905 fail2ban.filter         [11344]: INFO      findtime: 600
2025-12-12 14:51:20,905 fail2ban.actions        [11344]: INFO      banTime: 3600
2025-12-12 14:51:20,905 fail2ban.filter         [11344]: INFO      encoding: UTF-8
2025-12-12 14:51:20,905 fail2ban.filter         [11344]: INFO    Added logfile: '/var/log/audit/audit.log'
(pos = 0, hash = 2bac1d1460b4ddbd65dad9af08e925a24fbe1ecb)
2025-12-12 14:51:20,906 fail2ban.jail           [11344]: INFO    Creating new jail 'sshd-ddos'
2025-12-12 14:51:20,906 fail2ban.jail           [11344]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-12 14:51:20,906 fail2ban.jail           [11344]: INFO    Initiated 'pyinotify' backend
2025-12-12 14:51:20,907 fail2ban.filter         [11344]: INFO      maxLines: 1
2025-12-12 14:51:20,907 fail2ban.filter         [11344]: INFO      maxRetry: 5
2025-12-12 14:51:20,907 fail2ban.filter         [11344]: INFO      findtime: 600
2025-12-12 14:51:20,907 fail2ban.actions        [11344]: INFO      banTime: 3600
2025-12-12 14:51:20,907 fail2ban.filter         [11344]: INFO      encoding: UTF-8
2025-12-12 14:51:20,907 fail2ban.jail           [11344]: INFO    Jail 'sshd' started
2025-12-12 14:51:20,908 fail2ban.jail           [11344]: INFO    Jail 'selinux-ssh' started
2025-12-12 14:51:20,909 fail2ban.jail           [11344]: INFO    Jail 'sshd-ddos' started
2025-12-12 14:51:20,911 fail2ban.filtersystemd  [11344]: INFO    [sshd] Jail is in operation now (process n
ew journal entries)
```

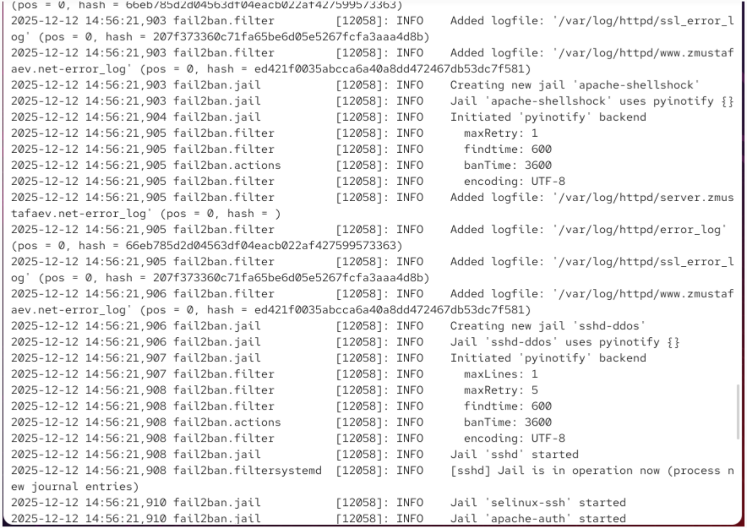
Рис. 4: Настройка SSH-защиты

Применение настроек



```
customisation.local    [----] 14 L:[ 11+29  40/ 40] *(4

[selinux-ssh]
enabled = true

[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
```

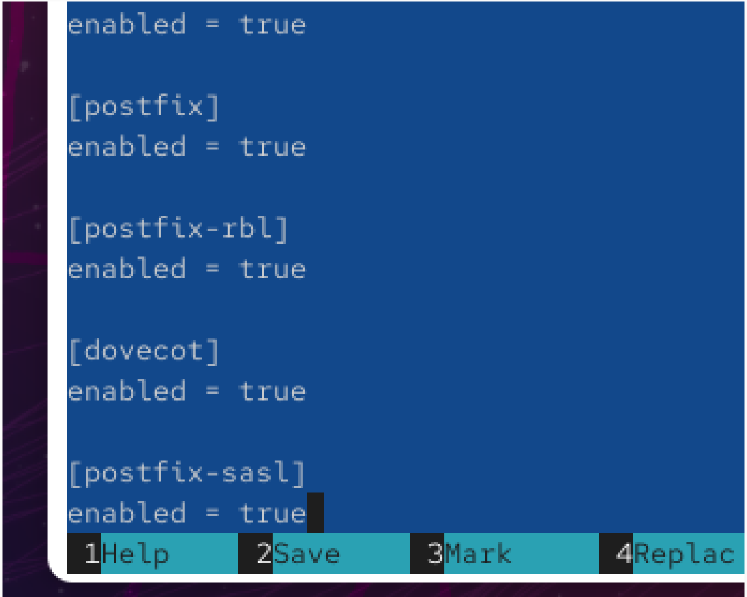
Включение HTTP-защиты



```
(pos = 0, hash = 66eb785d2d04563df04eacb022af427599573363)
2025-12-12 14:56:21,903 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/ssl_error_l
og' (pos = 0, hash = 207f373360c71fa65be6d05e5267fcfa3aaa4d8b)
2025-12-12 14:56:21,903 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/www.zmustaf
aev.net-error_log' (pos = 0, hash = ed421f0035abcca6a40a8dd472467db53dc7f581)
2025-12-12 14:56:21,903 fail2ban.jail           [12058]: INFO    Creating new jail 'apache-shellshock'
2025-12-12 14:56:21,903 fail2ban.jail           [12058]: INFO    Jail 'apache-shellshock' uses pyinotify {}
2025-12-12 14:56:21,904 fail2ban.jail           [12058]: INFO    Initiated 'pyinotify' backend
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO      maxRetry: 1
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO      findtime: 600
2025-12-12 14:56:21,905 fail2ban.actions        [12058]: INFO      banTime: 3600
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO      encoding: UTF-8
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/server.zmus
tafaev.net-error_log' (pos = 0, hash = )
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/error_log'
(pos = 0, hash = 66eb785d2d04563df04eacb022af427599573363)
2025-12-12 14:56:21,905 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/ssl_error_l
og' (pos = 0, hash = 207f373360c71fa65be6d05e5267fcfa3aaa4d8b)
2025-12-12 14:56:21,906 fail2ban.filter         [12058]: INFO    Added logfile: '/var/log/httpd/www.zmustaf
aev.net-error_log' (pos = 0, hash = ed421f0035abcca6a40a8dd472467db53dc7f581)
2025-12-12 14:56:21,906 fail2ban.jail           [12058]: INFO    Creating new jail 'sshd-ddos'
2025-12-12 14:56:21,906 fail2ban.jail           [12058]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-12 14:56:21,907 fail2ban.jail           [12058]: INFO    Initiated 'pyinotify' backend
2025-12-12 14:56:21,907 fail2ban.filter         [12058]: INFO      maxLines: 1
2025-12-12 14:56:21,908 fail2ban.filter         [12058]: INFO      maxRetry: 5
2025-12-12 14:56:21,908 fail2ban.filter         [12058]: INFO      findtime: 600
2025-12-12 14:56:21,908 fail2ban.actions        [12058]: INFO      banTime: 3600
2025-12-12 14:56:21,908 fail2ban.filter         [12058]: INFO      encoding: UTF-8
2025-12-12 14:56:21,908 fail2ban.jail           [12058]: INFO    Jail 'sshd' started
2025-12-12 14:56:21,908 fail2ban.filtersystemd  [12058]: INFO    [sshd] Jail is in operation now (process n
ew journal entries)
2025-12-12 14:56:21,910 fail2ban.jail           [12058]: INFO    Jail 'selinux-ssh' started
2025-12-12 14:56:21,910 fail2ban.jail           [12058]: INFO    Jail 'apache-auth' started
```

Рис. 6: HTTP-защита Apache

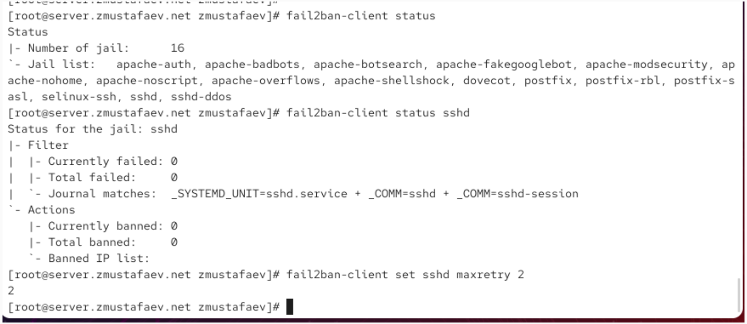
Проверка работы



```
enabled = true

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
```

Проверка работы Fail2ban

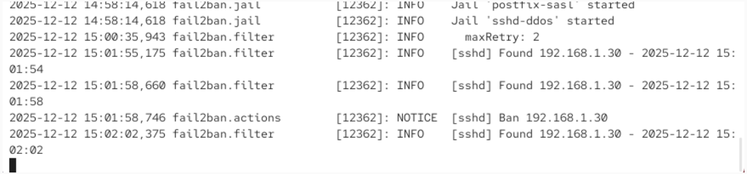
Проверка статуса



```
[root@server.zmustafaev.net zmustafaev]#
[root@server.zmustafaev.net zmustafaev]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, ap
ache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-s
asl, selinux-ssh, sshd, sshd-ddos
[root@server.zmustafaev.net zmustafaev]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.zmustafaev.net zmustafaev]# fail2ban-client set sshd maxretry 2
2
[root@server.zmustafaev.net zmustafaev]# 
```

Рис. 9: Статус jail sshd

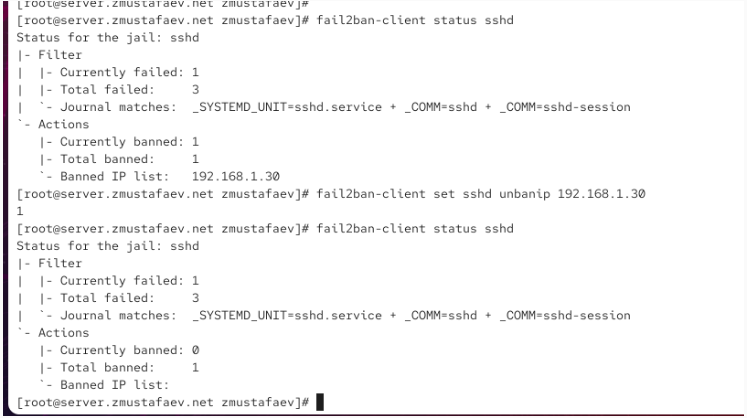
Проверка блокировки клиента



```
2025-12-12 14:58:14,618 fail2ban.jail         [12362]: INFO    Jail 'postfix-sasl' started
2025-12-12 14:58:14,618 fail2ban.jail         [12362]: INFO    Jail 'sshd-ddos' started
2025-12-12 15:00:35,943 fail2ban.filter       [12362]: INFO      maxRetry: 2
2025-12-12 15:01:55,175 fail2ban.filter       [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
01:54
2025-12-12 15:01:58,660 fail2ban.filter       [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
01:58
2025-12-12 15:01:58,746 fail2ban.actions      [12362]: NOTICE  [sshd] Ban 192.168.1.30
2025-12-12 15:02:02,375 fail2ban.filter       [12362]: INFO    [sshd] Found 192.168.1.30 - 2025-12-12 15:
02:02
```

Рис. 10: Блокировка IP-адреса

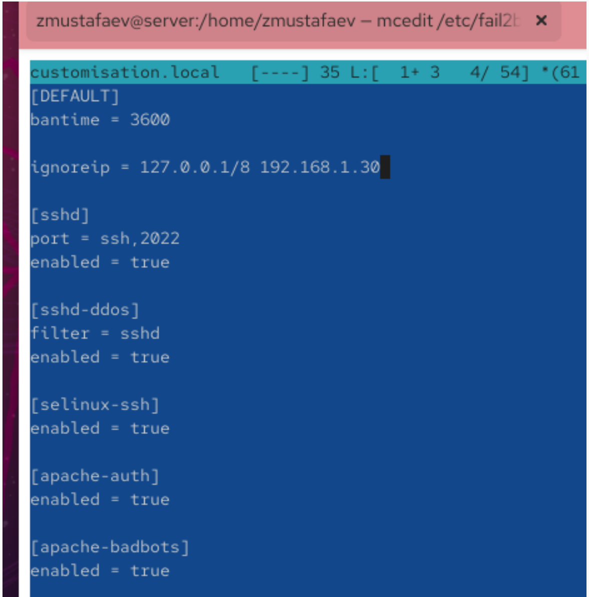
Разблокировка IP-адреса



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

Рис. 11: Разблокировка IP-адреса

Игнорирование доверенного IP



```
customisation.local    [----] 35 L:[  1+ 3   4/ 54] *(61
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.30

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true

[apache-auth]
enabled = true

[apache-badbots]
enabled = true
```

Выводы по проделанной работе

Вывод

В ходе лабораторной работы была настроена система защиты сервера с использованием Fail2ban. Реализована защита SSH, веб-служб и почтовых сервисов, выполнена проверка механизмов блокировки и разблокировки IP-адресов, а также подготовлена автоматизация конфигурации для повторного развёртывания.