Администрирование сетевых подсистем

Лабораторная работа №16

Машков И. Е.

13 февраля 2026

Российский университет дружбы народов, Москва, Россия

Информация

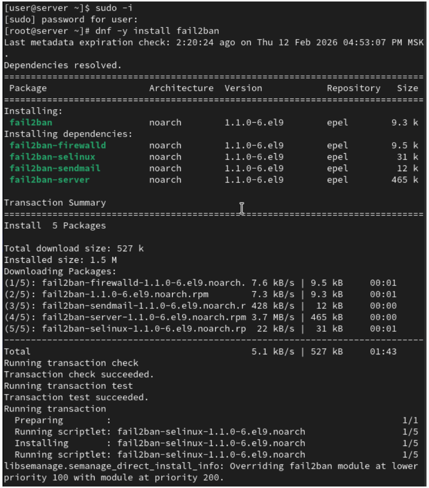
Докладчик

- Машков Илья Евгеньевич
- Студент 3-го курса, группа НФИбд-02-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- https://github.com/7S7eVe7N7

Цель работы

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

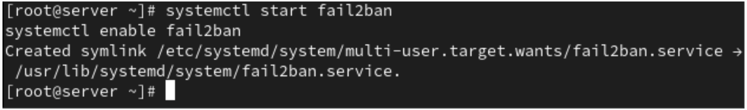
Выполнение лабораторной работы



```
[user@server ~]$ sudo -i
[sudo] password for user:
[root@server ~]# dnf -y install fail2ban
Last metadata expiration check: 2:20:24 ago on Thu 12 Feb 2026 04:53:07 PM MSK
.
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. 7.6 kB/s | 9.5 kB     00:01
(2/5): fail2ban-1.1.0-6.el9.noarch.rpm        7.3 kB/s | 9.3 kB     00:01
(3/5): fail2ban-sendmail-1.1.0-6.el9.noarch.r 428 kB/s |  12 kB     00:00
(4/5): fail2ban-server-1.1.0-6.el9.noarch.rpm 3.7 MB/s | 465 kB     00:00
(5/5): fail2ban-selinux-1.1.0-6.el9.noarch.rp  22 kB/s |  31 kB     00:01
------------------------------------------------------------------------------
Total                                         5.1 kB/s | 527 kB     01:43
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.
```

Рис. 1: Установка fail2ban

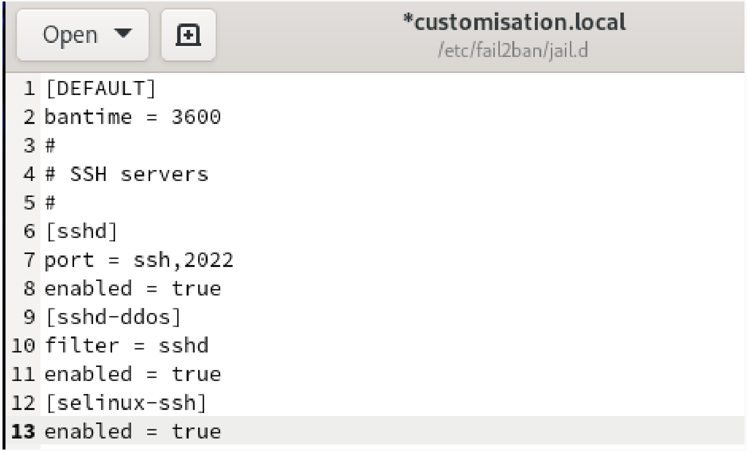
Выполнение лабораторной работы



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

Рис. 2: Запускаю сервер fail2ban

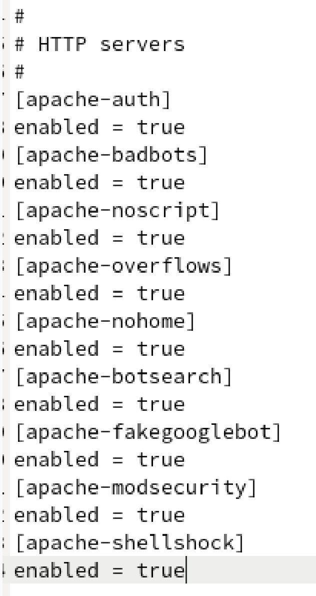
Выполнение лабораторной работы



```
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

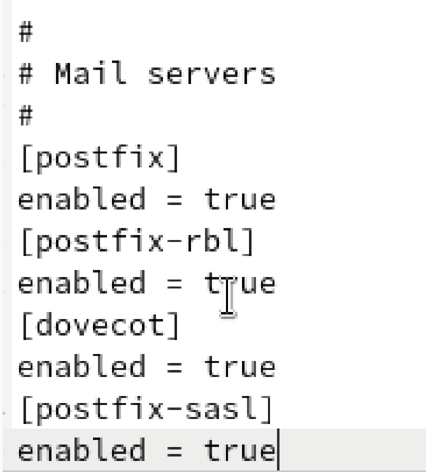
Рис. 3: customisation.local

Выполнение лабораторной работы



```
#
# 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
```

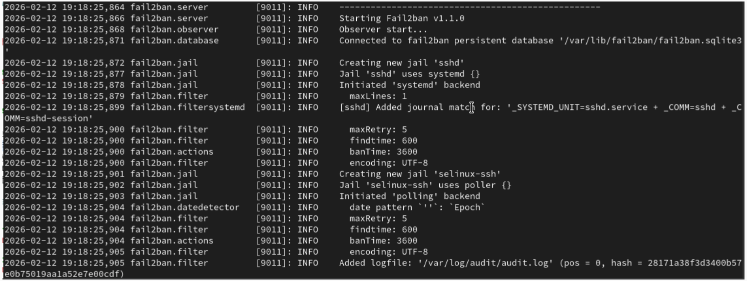
Выполнение лабораторной работы



```
#
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```

Рис. 5: Включение защиты почты

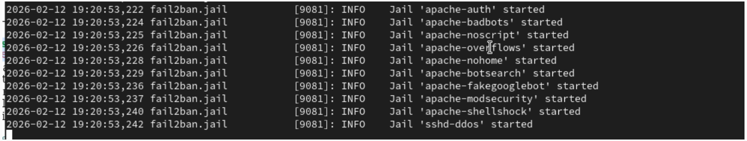
Выполнение лабораторной работы



```
2026-02-12 19:18:25,864 fail2ban.server         [9011]: INFO    --------------------------------------------------
2026-02-12 19:18:25,866 fail2ban.server         [9011]: INFO    Starting Fail2ban v1.1.0
2026-02-12 19:18:25,868 fail2ban.observer       [9011]: INFO    Observer start...
2026-02-12 19:18:25,871 fail2ban.database       [9011]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3
'
2026-02-12 19:18:25,872 fail2ban.jail           [9011]: INFO    Creating new jail 'sshd'
2026-02-12 19:18:25,877 fail2ban.jail           [9011]: INFO    Jail 'sshd' uses systemd {}
2026-02-12 19:18:25,878 fail2ban.jail           [9011]: INFO    Initiated 'systemd' backend
2026-02-12 19:18:25,879 fail2ban.filter         [9011]: INFO      maxLines: 1
2026-02-12 19:18:25,899 fail2ban.filtersystemd  [9011]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd + _C
OMM=sshd-session'
2026-02-12 19:18:25,900 fail2ban.filter         [9011]: INFO      maxRetry: 5
2026-02-12 19:18:25,900 fail2ban.filter         [9011]: INFO      findtime: 600
2026-02-12 19:18:25,900 fail2ban.actions        [9011]: INFO      banTime: 3600
2026-02-12 19:18:25,900 fail2ban.filter         [9011]: INFO      encoding: UTF-8
2026-02-12 19:18:25,901 fail2ban.jail           [9011]: INFO    Creating new jail 'selinux-ssh'
2026-02-12 19:18:25,902 fail2ban.jail           [9011]: INFO    Jail 'selinux-ssh' uses poller {}
2026-02-12 19:18:25,903 fail2ban.jail           [9011]: INFO    Initiated 'polling' backend
2026-02-12 19:18:25,904 fail2ban.datedetector   [9011]: INFO      date pattern `''`: `Epoch`
2026-02-12 19:18:25,904 fail2ban.filter         [9011]: INFO      maxRetry: 5
2026-02-12 19:18:25,904 fail2ban.filter         [9011]: INFO      findtime: 600
2026-02-12 19:18:25,904 fail2ban.actions        [9011]: INFO      banTime: 3600
2026-02-12 19:18:25,905 fail2ban.filter         [9011]: INFO      encoding: UTF-8
2026-02-12 19:18:25,905 fail2ban.filter         [9011]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 28171a38f3d3400b57
e0b75019aa1a52e7e00cdf)
```

Рис. 6: Удачная активация настроенных параметров

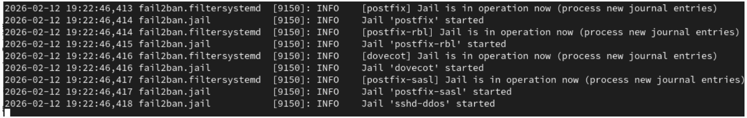
Выполнение лабораторной работы



```
2026-02-12 19:20:53,222 fail2ban.jail           [9081]: INFO    Jail 'apache-auth' started
2026-02-12 19:20:53,224 fail2ban.jail           [9081]: INFO    Jail 'apache-badbots' started
2026-02-12 19:20:53,225 fail2ban.jail           [9081]: INFO    Jail 'apache-noscript' started
2026-02-12 19:20:53,226 fail2ban.jail           [9081]: INFO    Jail 'apache-overflows' started
2026-02-12 19:20:53,228 fail2ban.jail           [9081]: INFO    Jail 'apache-nohome' started
2026-02-12 19:20:53,229 fail2ban.jail           [9081]: INFO    Jail 'apache-botsearch' started
2026-02-12 19:20:53,236 fail2ban.jail           [9081]: INFO    Jail 'apache-fakegooglebot' started
2026-02-12 19:20:53,237 fail2ban.jail           [9081]: INFO    Jail 'apache-modsecurity' started
2026-02-12 19:20:53,240 fail2ban.jail           [9081]: INFO    Jail 'apache-shellshock' started
2026-02-12 19:20:53,242 fail2ban.jail           [9081]: INFO    Jail 'sshd-ddos' started
```

Рис. 7: Удачная активация защиты HTTP

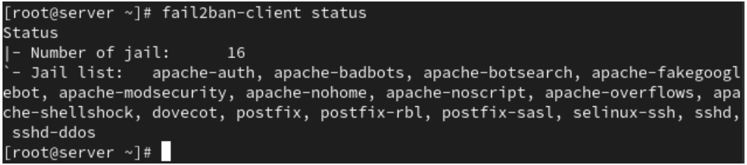
Выполнение лабораторной работы



```
2026-02-12 19:22:46,413 fail2ban.filtersystemd  [9150]: INFO    [postfix] Jail is in operation now (process new journal entries)
2026-02-12 19:22:46,414 fail2ban.jail           [9150]: INFO    Jail 'postfix' started
2026-02-12 19:22:46,414 fail2ban.filtersystemd  [9150]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2026-02-12 19:22:46,415 fail2ban.jail           [9150]: INFO    Jail 'postfix-rbl' started
2026-02-12 19:22:46,416 fail2ban.filtersystemd  [9150]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2026-02-12 19:22:46,416 fail2ban.jail           [9150]: INFO    Jail 'dovecot' started
2026-02-12 19:22:46,417 fail2ban.filtersystemd  [9150]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2026-02-12 19:22:46,417 fail2ban.jail           [9150]: INFO    Jail 'postfix-sasl' started
2026-02-12 19:22:46,418 fail2ban.jail           [9150]: INFO    Jail 'sshd-ddos' started
```

Рис. 8: Удачная активация защиты почты

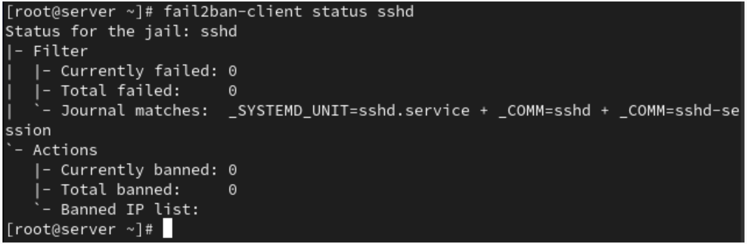
Выполнение лабораторной работы



```
[root@server ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegoogl
ebot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apa
che-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd,
 sshd-ddos
[root@server ~]# 
```

Рис. 9: Проверка списков служб, находящихся под защитой

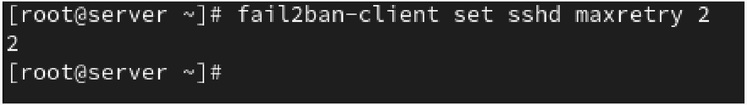
Выполнение лабораторной работы



```
[root@server ~]# 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-se
ssion
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server ~]# 
```

Рис. 10: Статус защиты sshd

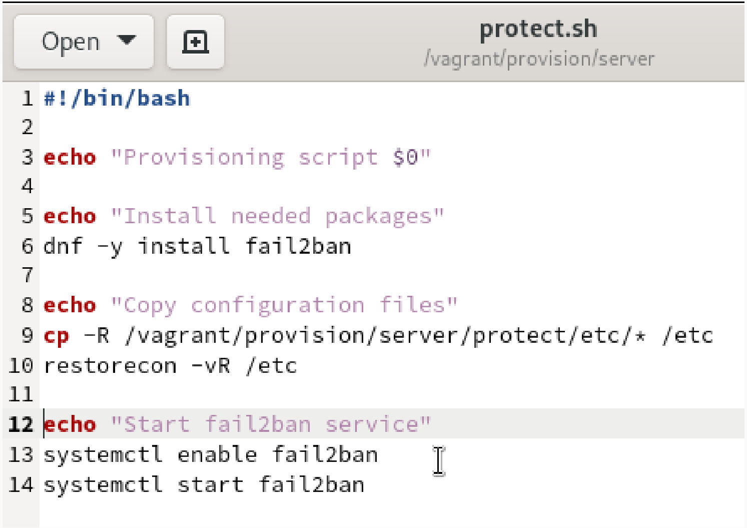
Выполнение лабораторной работы



```
[root@server ~]# fail2ban-client set sshd maxretry 2
2
[root@server ~]#
```

Рис. 11: Коррекция максимального кол-ва ошибок

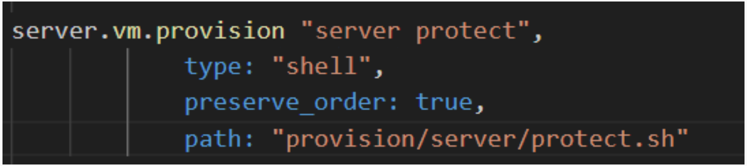
Выполнение лабораторной работы



```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
```

Рис. 12: protect.sh

Выполнение лабораторной работы



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

Рис. 13: Правки в Vagrantfile

Выводы

В процессе выполнения данной лабораторной работы я освоил навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».