Защита сервера с использованием Fail2ban

Лабораторная работа №16

Элсаиед Адел

7 января 2026

Российский университет дружбы народов, Москва, Россия

Цель и задачи работы

Цель лабораторной работы

Получение практических навыков настройки и использования программного средства Fail2ban для обеспечения базовой защиты сервера от атак типа brute force.

Выполнение работы

Контроль запуска Fail2ban

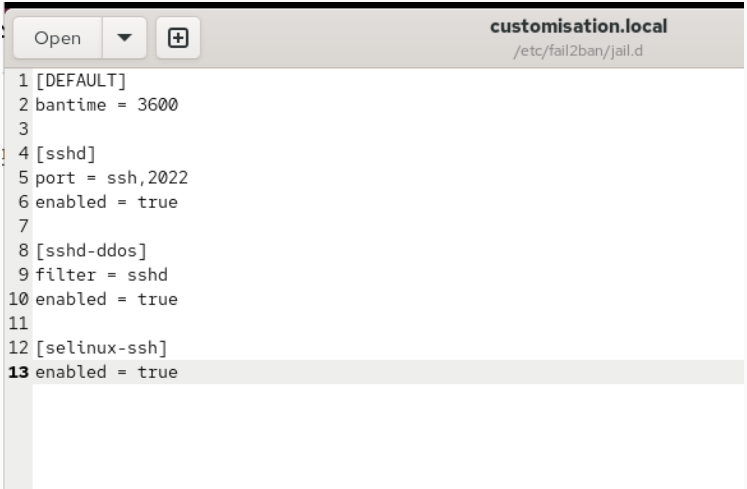
Выполнен мониторинг журнала Fail2ban для проверки корректности запуска сервиса и подключения к базе данных.

```
[elsaiedadel@server.elsaiedadel.net sambashare]$
[elsaiedadel@server.elsaiedadel.net sambashare]$ sudo -i tail -f /var/log/fail2ban.log
[sudo] password for elsaiedadel:
2026-01-07 08:39:48,789 fail2ban.server         [23375]: INFO    --------------------------------------------------
2026-01-07 08:39:48,789 fail2ban.server         [23375]: INFO    Starting Fail2ban v1.1.0
2026-01-07 08:39:48,790 fail2ban.observer       [23375]: INFO    Observer start...
2026-01-07 08:39:48,793 fail2ban.database       [23375]: INFO    Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2026-01-07 08:39:48,794 fail2ban.database       [23375]: WARNING New database created. Version '4'
```

Рис. 1: Просмотр журнала Fail2ban

Локальная конфигурация Fail2ban

Создан файл локальной конфигурации `customisation.local`, используемый для задания пользовательских параметров защиты.



Применение конфигурации

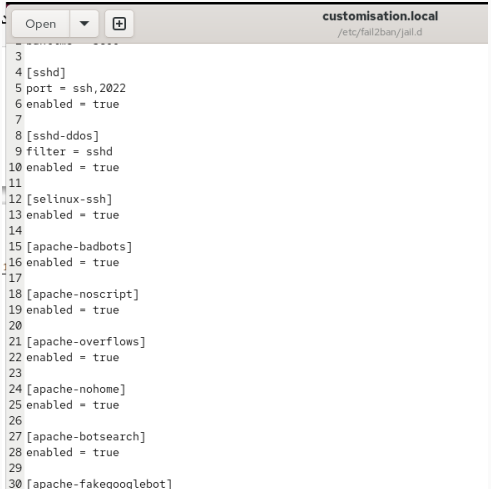
После внесения изменений выполнен перезапуск Fail2ban.

В журнале подтверждён запуск jail-модулей SSH.

```
2026-01-07 08:42:41,730 fail2ban.server         [24048]: INFO    Starting Fail2ban v1.1.0
2026-01-07 08:42:41,730 fail2ban.observer       [24048]: INFO    Observer start...
2026-01-07 08:42:41,733 fail2ban.database       [24048]: INFO    Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2026-01-07 08:42:41,733 fail2ban.jail           [24048]: INFO    Creating new jail 'sshd'
2026-01-07 08:42:41,736 fail2ban.jail           [24048]: INFO    Jail 'sshd' uses systemd {}
2026-01-07 08:42:41,736 fail2ban.jail           [24048]: INFO    Initiated 'systemd' backend
2026-01-07 08:42:41,737 fail2ban.filter         [24048]: INFO      maxLines: 1
2026-01-07 08:42:41,741 fail2ban.filtersystemd  [24048]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.s
ervice + _COMM=sshd + _COMM=sshd-session'
2026-01-07 08:42:41,741 fail2ban.filter         [24048]: INFO      maxRetry: 5
2026-01-07 08:42:41,741 fail2ban.filter         [24048]: INFO      findtime: 600
2026-01-07 08:42:41,741 fail2ban.actions        [24048]: INFO      banTime: 3600
2026-01-07 08:42:41,741 fail2ban.filter         [24048]: INFO      encoding: UTF-8
2026-01-07 08:42:41,741 fail2ban.jail           [24048]: INFO    Creating new jail 'selinux-ssh'
2026-01-07 08:42:41,744 fail2ban.jail           [24048]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2026-01-07 08:42:41,744 fail2ban.jail           [24048]: INFO    Initiated 'pyinotify' backend
2026-01-07 08:42:41,745 fail2ban.datedetector   [24048]: INFO      date pattern `''': 'Epoch`
2026-01-07 08:42:41,745 fail2ban.filter         [24048]: INFO      maxRetry: 5
2026-01-07 08:42:41,745 fail2ban.filter         [24048]: INFO      findtime: 600
2026-01-07 08:42:41,745 fail2ban.actions        [24048]: INFO      banTime: 3600
2026-01-07 08:42:41,745 fail2ban.filter         [24048]: INFO      encoding: UTF-8
2026-01-07 08:42:41,746 fail2ban.filter         [24048]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, h
ash = f8c1aeeca7e18a160e53b0659c09e9f813656be4)
2026-01-07 08:42:41,746 fail2ban.jail           [24048]: INFO    Creating new jail 'sshd-ddos'
2026-01-07 08:42:41,746 fail2ban.jail           [24048]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:42:41,747 fail2ban.jail           [24048]: INFO    Initiated 'pyinotify' backend
2026-01-07 08:42:41,748 fail2ban.filter         [24048]: INFO      maxLines: 1
2026-01-07 08:42:41,748 fail2ban.filter         [24048]: INFO      maxRetry: 5
2026-01-07 08:42:41,748 fail2ban.filter         [24048]: INFO      findtime: 600
2026-01-07 08:42:41,748 fail2ban.actions        [24048]: INFO      banTime: 3600
2026-01-07 08:42:41,748 fail2ban.filter         [24048]: INFO      encoding: UTF-8
2026-01-07 08:42:41,748 fail2ban.jail           [24048]: INFO    Jail 'sshd' started
```

Защита Apache

Включены модули защиты веб-сервера Apache: - защита от вредоносных ботов; - защита от атак Shellshock; - фильтрация подозрительных HTTP-запросов.



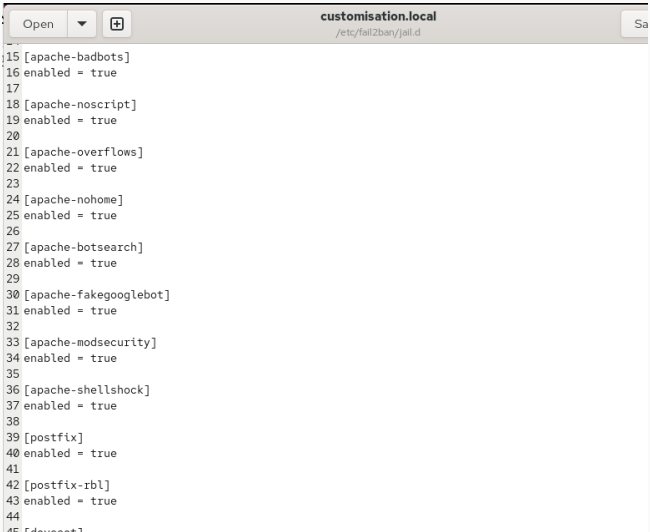
После перезапуска Fail2ban в журнале зафиксирован запуск всех Apache jail-модулей.

```
2026-01-07 08:45:11,751 fail2ban.filter         [24450]: INFO    Added logfile: '/var/log/httpd/www.elsaiedadel.net-er
ror_log' (pos = 0, hash = 666653b87fc18faa79b1a5cfd17ab8f0e8276044)
2026-01-07 08:45:11,751 fail2ban.filter         [24450]: INFO    Added logfile: '/var/log/httpd/server.elsaiedadel.net
-error_log' (pos = 0, hash = )
2026-01-07 08:45:11,752 fail2ban.jail           [24450]: INFO    Creating new jail 'sshd-ddos'
2026-01-07 08:45:11,752 fail2ban.jail           [24450]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:45:11,753 fail2ban.jail           [24450]: INFO    Initiated 'pyinotify' backend
2026-01-07 08:45:11,753 fail2ban.filter         [24450]: INFO      maxLines: 1
2026-01-07 08:45:11,753 fail2ban.filter         [24450]: INFO      maxRetry: 5
2026-01-07 08:45:11,753 fail2ban.filter         [24450]: INFO      findtime: 600
2026-01-07 08:45:11,753 fail2ban.actions        [24450]: INFO      banTime: 3600
2026-01-07 08:45:11,753 fail2ban.filter         [24450]: INFO      encoding: UTF-8
2026-01-07 08:45:11,754 fail2ban.jail           [24450]: INFO    Jail 'sshd' started
2026-01-07 08:45:11,754 fail2ban.filtersystemd  [24450]: INFO    [sshd] Jail is in operation now (process new journal
entries)
2026-01-07 08:45:11,754 fail2ban.jail           [24450]: INFO    Jail 'selinux-ssh' started
2026-01-07 08:45:11,756 fail2ban.jail           [24450]: INFO    Jail 'apache-badbots' started
2026-01-07 08:45:11,757 fail2ban.jail           [24450]: INFO    Jail 'apache-noscript' started
2026-01-07 08:45:11,758 fail2ban.jail           [24450]: INFO    Jail 'apache-overflows' started
2026-01-07 08:45:11,758 fail2ban.jail           [24450]: INFO    Jail 'apache-nohome' started
2026-01-07 08:45:11,759 fail2ban.jail           [24450]: INFO    Jail 'apache-botsearch' started
2026-01-07 08:45:11,759 fail2ban.jail           [24450]: INFO    Jail 'apache-fakegooglebot' started
2026-01-07 08:45:11,761 fail2ban.jail           [24450]: INFO    Jail 'apache-modsecurity' started
2026-01-07 08:45:11,761 fail2ban.jail           [24450]: INFO    Jail 'apache-shellshock' started
2026-01-07 08:45:11,762 fail2ban.jail           [24450]: INFO    Jail 'sshd-ddos' started
```

Рис. 5: Журнал Fail2ban (HTTP)

Настройка почты

Включена защита почтовых служб: - Postfix; - Postfix RBL; - Dovecot; - Postfix SASL.



Применение настроек

После перезапуска Fail2ban подтверждён запуск jail-модулей почтовых сервисов.

```
2026-01-07 08:46:46,104 fail2ban.jail           [24734]: INFO    Creating new jail 'sshd-ddos'
2026-01-07 08:46:46,104 fail2ban.jail           [24734]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2026-01-07 08:46:46,105 fail2ban.jail           [24734]: INFO    Initiated 'pyinotify' backend
2026-01-07 08:46:46,105 fail2ban.filter         [24734]: INFO      maxLines: 1
2026-01-07 08:46:46,106 fail2ban.filter         [24734]: INFO      maxRetry: 5
2026-01-07 08:46:46,106 fail2ban.filter         [24734]: INFO      findtime: 600
2026-01-07 08:46:46,106 fail2ban.actions        [24734]: INFO      banTime: 3600
2026-01-07 08:46:46,106 fail2ban.filter         [24734]: INFO      encoding: UTF-8
2026-01-07 08:46:46,106 fail2ban.jail           [24734]: INFO    Jail 'sshd' started
2026-01-07 08:46:46,106 fail2ban.filtersystemd  [24734]: INFO    [sshd] Jail is in operation now (process new journal
entries)
2026-01-07 08:46:46,107 fail2ban.jail           [24734]: INFO    Jail 'selinux-ssh' started
2026-01-07 08:46:46,107 fail2ban.jail           [24734]: INFO    Jail 'apache-badbots' started
2026-01-07 08:46:46,108 fail2ban.jail           [24734]: INFO    Jail 'apache-noscript' started
2026-01-07 08:46:46,108 fail2ban.jail           [24734]: INFO    Jail 'apache-overflows' started
2026-01-07 08:46:46,109 fail2ban.jail           [24734]: INFO    Jail 'apache-nohome' started
2026-01-07 08:46:46,109 fail2ban.jail           [24734]: INFO    Jail 'apache-botsearch' started
2026-01-07 08:46:46,109 fail2ban.jail           [24734]: INFO    Jail 'apache-fakegooglebot' started
2026-01-07 08:46:46,110 fail2ban.jail           [24734]: INFO    Jail 'apache-modsecurity' started
2026-01-07 08:46:46,110 fail2ban.jail           [24734]: INFO    Jail 'apache-shellshock' started
2026-01-07 08:46:46,110 fail2ban.jail           [24734]: INFO    Jail 'postfix' started
2026-01-07 08:46:46,110 fail2ban.jail           [24734]: INFO    Jail 'postfix-rbl' started
2026-01-07 08:46:46,111 fail2ban.filtersystemd  [24734]: INFO    [dovecot] Jail is in operation now (process new journ
al entries)
2026-01-07 08:46:46,112 fail2ban.filtersystemd  [24734]: INFO    [postfix-rbl] Jail is in operation now (process new j
ournal entries)
2026-01-07 08:46:46,112 fail2ban.jail           [24734]: INFO    Jail 'dovecot' started
2026-01-07 08:46:46,112 fail2ban.filtersystemd  [24734]: INFO    [postfix] Jail is in operation now (process new journ
al entries)
2026-01-07 08:46:46,112 fail2ban.jail           [24734]: INFO    Jail 'postfix-sasl' started
2026-01-07 08:46:46,113 fail2ban.filtersystemd  [24734]: INFO    [postfix-sasl] Jail is in operation now (process new
journal entries)
2026-01-07 08:46:46,113 fail2ban.jail           [24734]: INFO    Jail 'sshd-ddos' started
```

Статус Fail2ban

Проверен общий статус Fail2ban и список активных jail-модулей.

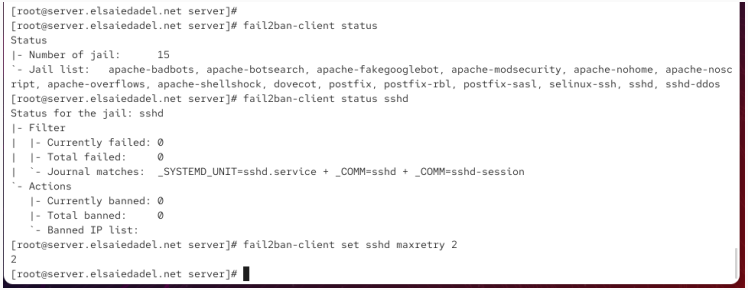


Рис. 8: Статус Fail2ban

Проверка блокировки SSH

Выполнена имитация атаки перебора пароля по SSH.

Fail2ban успешно заблокировал IP-адрес клиента.

Рис. 9: Блокировка IP-адреса

Исключение доверенного IP

В конфигурации Fail2ban добавлен параметр `ignoreip` для исключения доверенного IP-адреса.

Open

customisation.local
/etc/fail2ban/jail.d

```
1 [DEFAULT]
2 bantime = 3600
3 ignoreip = 127.0.0.1/8 192.168.1.30
4
5 [sshd]
6 port = ssh,2022
7 enabled = true
8
9 [sshd-ddos]
10 filter = sshd
11 enabled = true
12
13 [selinux-ssh]
14 enabled = true
15
16 [apache-badbots]
17 enabled = true
18
19 [apache-noscript]
20 enabled = true
21
22 [apache-overflows]
```

Проверка ignoreip

Попытки входа с доверенного IP-адреса игнорируются Fail2ban, блокировка не применяется.

```
2026-01-07 08:52:07,082 fail2ban.filter         [25511]: INFO    [sshd] Ignore 192.168.1.30 by ip
2026-01-07 08:52:11,017 fail2ban.filter         [25511]: INFO    [sshd] Ignore 192.168.1.30 by ip
2026-01-07 08:52:16,041 fail2ban.filter         [25511]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

Рис. 11: Журнал ignoreip

Подготовка provisioning-скрипта

Создан каталог `protect` и размещены конфигурационные файлы Fail2ban для автоматической установки.

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

Рис. 12: Каталог protect

Скрипт 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
```

Рис. 13: Скрипт protect.sh

Выводы

Вывод

В ходе лабораторной работы выполнена настройка Fail2ban для защиты SSH, HTTP и почтовых сервисов. Проведена проверка блокировки и разблокировки IP-адресов, реализовано исключение доверенных адресов и автоматизация конфигурации с использованием Vagrant. Полученные результаты подтверждают эффективность Fail2ban как средства базовой защиты сервера от атак типа brute force.