

Отчёт о лабораторной работе

Лабораторная работа 16

Мошаров Денис Максимович

Содержание

Цель работы

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

Выполнение лабораторной работы

Для начала на сервере устанавливаем fail2ban (рис. [-@fig:001]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo dnf -y install fail2ban
[sudo] password for dmmosharov:
tstack_lnav                               67 B/s | 819 B   00:12
tstack_lnav-source                         402 B/s | 819 B   00:02
Dependencies resolved.
=====
 Package           Architecture Version      Repository  Size
 =====
 Installing:
 fail2ban          noarch     1.1.0-6.el10_0    epel       9.4 k
 Installing dependencies:
 fail2ban-firewalld    noarch     1.1.0-6.el10_0    epel       9.6 k
 fail2ban-selinux     noarch     1.1.0-6.el10_0    epel      31 k
 fail2ban-sendmail    noarch     1.1.0-6.el10_0    epel      12 k
 fail2ban-server      noarch     1.1.0-6.el10_0    epel      561 k
 Transaction Summary
 =====
 Install 5 Packages

 Total download size: 623 k
 Installed size: 1.8 M
 Downloading Packages:
 [1/5]: fail2ban-1.1.0-6.el10_0.noarch.rpm 9.0 kB/s | 9.4 kB   00:01
 [2/5]: fail2ban-firewalld-1.1.0-6.el10_0.noarch.rpm 9.6 kB/s | 9.6 kB   00:01
 [3/5]: fail2ban-selinux-1.1.0-6.el10_0.noarch.rpm 31 kB/s | 31 kB   00:01
 [4/5]: fail2ban-sendmail-1.1.0-6.el10_0.noarch.rpm 12 kB/s | 12 kB   00:01
 [5/5]: fail2ban-server-1.1.0-6.el10_0.noarch.rpm 561 kB/s | 561 kB   00:01
```

Установка fail2ban

Запускаем сервер fail2ban (рис. [-@fig:002]).

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

Запуск сервера fail2ban

В дополнительном терминале запускаем просмотр журнала событий fail2ban (рис. [-@fig:003]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for dmmosharov:
2026-02-11 21:24:24,800 fail2ban.server      [90071]: INFO  -----
2026-02-11 21:24:24,800 fail2ban.server      [90071]: INFO  Starting Fai
l2ban v1.1.0
2026-02-11 21:24:24,800 fail2ban.observer    [90071]: INFO  Observer sta
rt...
2026-02-11 21:24:24,809 fail2ban.database     [90071]: INFO  Connected to
fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 21:24:24,811 fail2ban.database     [90071]: WARNING New database
created. Version '4'
```

Журнал событий

Создаем файл с локальной конфигурацией fail2ban и открываем на редактирование /etc/fail2ban/jail.d/customisation.local (рис. [-@fig:004]).

```
[root]
[dmmosharov@server.dmmosharov.net ~]$ sudo touch /etc/fail2ban/jail.d/customi
sation.local
[dmmosharov@server.dmmosharov.net ~]$ sudo nano customisation.local
```

Файл с локальной конфигурацией

В файле customisation.local содержатся параметры для блокирования на 1 час, также включили защиту SSH (рис. [-@fig:005]).

```
GNU nano 8.1                               customisation.local
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

Редактирование customisation.local

Перезапускаем fail2ban (рис. [-@fig:006]).

```
[dmmosharov@server.dmmosharov.net ~]$ systemctl restart fail2ban
[dmmosharov@server.dmmosharov.net ~]$
```

Перезапуск fail2ban

Снова смотрим журнал событий (рис. [-@fig:007]).

```

2026-02-11 21:24:24,809 fail2ban.database      [90071]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 21:24:24,811 fail2ban.database      [90071]: WARNING New database created. Version '4'
2026-02-11 21:26:34,787 fail2ban.server      [90071]: INFO    Shutdown in progress...
2026-02-11 21:26:34,788 fail2ban.observer     [90071]: INFO    Observer stop... try to end queue 5 seconds
2026-02-11 21:26:34,810 fail2ban.observer     [90071]: INFO    Observer stopped, 0 events remaining.
2026-02-11 21:26:34,859 fail2ban.server      [90071]: INFO    Stopping all jails
2026-02-11 21:26:34,860 fail2ban.database      [90071]: INFO    Connection to database closed.
2026-02-11 21:26:34,860 fail2ban.server      [90071]: INFO    Exiting Fail2ban
2026-02-11 21:26:35,039 fail2ban.server      [90730]: INFO    -----
2026-02-11 21:26:35,040 fail2ban.server      [90730]: INFO    Starting Fail2ban v1.1.0
2026-02-11 21:26:35,040 fail2ban.observer     [90730]: INFO    Observer start...
2026-02-11 21:26:35,048 fail2ban.database      [90730]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'

```

Журнал событий

Редактируем файл customisation.local и включаем защиту HTTP (рис. [-@fig:008]).

```

GNU nano 8.1                               customisation.local
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[ssh-ddos]
filter = sshd
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]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]

```

Редактирование customisation.local

Перезапускаем fail2ban и смотрим логи (рис. [-@fig:009]).

```

[dmonashirov@server dmonashirov.net ~]$ sudo tail -f /var/log/fail2ban.log
2026-02-11 21:27:59,610 fail2ban.server      [90730]: INFO    Shutdown in progress...
2026-02-11 21:27:59,611 fail2ban.observer     [90730]: INFO    Observer stop... try to end queue 5 seconds
2026-02-11 21:27:59,646 fail2ban.observer     [90730]: INFO    Observer stopped, 0 events remaining.
2026-02-11 21:27:59,693 fail2ban.server      [90730]: INFO    Stopping all jails
2026-02-11 21:27:59,694 fail2ban.database      [90730]: INFO    Connection to database closed.
2026-02-11 21:27:59,694 fail2ban.server      [90730]: INFO    Exiting Fail2ban
2026-02-11 21:27:59,836 fail2ban.server      [90984]: INFO    -----
2026-02-11 21:27:59,836 fail2ban.server      [90984]: INFO    Starting Fail2ban v1.1.0
2026-02-11 21:27:59,836 fail2ban.observer     [90984]: INFO    Observer start...
2026-02-11 21:27:59,843 fail2ban.database      [90984]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'

```

Просмотр логов

В файл customisation.local добавляем защиту почты (рис. [-@fig:010]).

```
enabled = true

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

Защита почты

Перезапустили fail2ban и смотрим логи (рис. [-@fig:011]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo tail -f /var/log/fail2ban.log
2026-02-11 21:27:59.610 fail2ban.server [00730]: INFO Shutdown in progress...
2026-02-11 21:27:59.611 fail2ban.observer [00730]: INFO Observer stop ... try to end queue 5 seconds
2026-02-11 21:27:59.646 fail2ban.observer [00730]: INFO Observer stopped, 0 events remaining.
2026-02-11 21:27:59.693 fail2ban.database [00730]: INFO Stopping all jails
2026-02-11 21:27:59.694 fail2ban.database [00730]: INFO Connection to database closed.
2026-02-11 21:27:59.694 fail2ban.server [00730]: INFO Exiting Fail2ban
2026-02-11 21:27:59.836 fail2ban.server [00984]: INFO Starting Fail2ban v1.1.0
2026-02-11 21:27:59.836 fail2ban.observer [00984]: INFO Observer start...
2026-02-11 21:27:59.843 fail2ban.database [00984]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 21:29:00.869 fail2ban.server [00984]: INFO Shutdown in progress...
2026-02-11 21:29:00.870 fail2ban.observer [00984]: INFO Observer stop ... try to end queue 5 seconds
2026-02-11 21:29:00.900 fail2ban.observer [00984]: INFO Observer stopped, 0 events remaining.
2026-02-11 21:29:00.940 fail2ban.server [00984]: INFO Stopping all jails
2026-02-11 21:29:00.941 fail2ban.database [00984]: INFO Connection to database closed.
2026-02-11 21:29:00.941 fail2ban.server [00984]: INFO Exiting Fail2ban
2026-02-11 21:29:01.063 fail2ban.server [01185]: INFO -----
2026-02-11 21:29:01.064 fail2ban.server [01185]: INFO Starting Fail2ban v1.1.0
2026-02-11 21:29:01.064 fail2ban.observer [01185]: INFO Observer start...
2026-02-11 21:29:01.070 fail2ban.database [01185]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
C
```

Просмотр логов

Смотрим статус нашего fail2ban, далее смотрим статус защиты SSH и устанавливаем максимальное кол-во ошибок для SSH равное двум (рис. [-@fig:011.1]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client status
Status
|- Number of jail:    16
|- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohone, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[dmmosharov@server.dmmosharov.net ~]$ sudo 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:
[dmmosharov@server.dmmosharov.net ~]$ fail2ban-client set sshd maxretry 2
2026-02-11 21:32:37.070 fail2ban          [01903]: ERROR  Permission denied to socket: /var/run/fail2ban/fail2ban.sock, (you must be root)
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[dmmosharov@server.dmmosharov.net ~]$
```

Проверка состояния

С клиента пробуем зайти по SSH на сервер с неправильным паролем (рис. [-@fig:012]).

```
[dmmosharov@client.dmmosharov.net ~]$ ssh -p22 server@dmmosharov.net
The authenticity of host 'dmmosharov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:F8sREGOc3d3bqO3xJrbnrCFDPDWDr/+seyPoj
5DX9uI.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: server.dmmosharov.net
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'dmmosharov.net' (ED25519) to the list of known hosts.
server@dmmosharov.net's password:
Permission denied, please try again.
server@dmmosharov.net's password: [REDACTED]
```

Проверка неверного пароля

После этого на сервере смотрим статус защиты SSH и видим что произошла блокировка одного айпи адреса, 192.168.1.30 (рис. [-@fig:013]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| |- 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
[dmmosharov@server.dmmosharov.net ~]$ [REDACTED]
```

Появление блокировки

Разблокируем данный IP-адрес клиента и убеждемся, что он был действительно разблокирован(рис. [-@fig:014]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client set sshd unbanip 192.168.1.30
1
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  `- Banned IP list:
[dmmosharov@server.dmmosharov.net ~]$ [REDACTED]
```

Разблокировка IP-адреса

На сервере вносим изменение в конфигурационный файл, добавив в раздел по умолчанию игнорирование адреса нашего клиента (рис. [-@fig:015]).

```
GNU nano 8.1
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.30[REDACTED]
#
```

Игнорирование IP-адреса

Перезапускаем fail2ban (рис. [-@fig:016]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo nano /etc/fail2ban/jail.d/customisation.local
[dmmosharov@server.dmmosharov.net ~]$ systemctl restart fail2ban
```

Перезапуск fail2ban

Вновь пыгаемся подключится используя неправильный пароль (рис. [-@fig:017]).

```
[dmmosharov@client.dmmosharov.net ~]$ ssh -p22 server@dmmosharov.net
server@dmmosharov.net's password:
Permission denied, please try again.
server@dmmosharov.net's password:
Permission denied, please try again.
server@dmmosharov.net's password: █
```

Повторная попытка подключения

Выведя статус защиты SSH убеждаемся, что бан был снят (рис. [-@fig:018]).

```
[dmmosharov@server.dmmosharov.net ~]$ sudo 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:
[dmmosharov@server.dmmosharov.net ~]$ █
```

Отсутствие блокировки

На виртуальной машине server переходим в каталог для внесения изменений в настройки внутреннего окружения, создаем в нем каталог protect и помещаем туда все соответствующие подкаталоги и конфигурационные файлы, после чего открываем на редактирование наш protect.sh (рис. [-@fig:019]).

```
[dmmosharov@server.dmmosharov.net ~]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ mkdir -p /vagrant/provision/server/protect/etc
/vfail2ban/jail.d
[dmmosharov@server.dmmosharov.net server]$ cp -R /etc/fail2ban/jail.d/customisation.local
/vagrant/provision/server/protect/etc/fail2ban/jail.d/
cp: missing destination file operand after '/etc/fail2ban/jail.d/customisation.local/vagr
ant/provision/server/protect/etc/fail2ban/jail.d/'
Try 'cp --help' for more information.
[dmmosharov@server.dmmosharov.net server]$ cp -R /etc/fail2ban/jail.d/customisation.local
/vagrant/provision/server/protect/etc/fail2ban/jail.d/
[dmmosharov@server.dmmosharov.net server]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ touch protect.sh
[dmmosharov@server.dmmosharov.net server]$ chmod +x protect.sh
[dmmosharov@server.dmmosharov.net server]$ nano protect.sh █
```

Конфигурационный файл

Прописываем следующий скрипт (рис. [-@fig:020]).

```
dmmosharov@server:/vagrant/provision/server - sudo nano p × dmmosharov@server:
GNU nano 8.1                                     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
```

Скрипт

Для отработки созданного скрипта во время загрузки нашей виртуальной машины server в конфигурационный файл Vagrantfile добавляем нужные конфигурации (рис. [-@fig:021]).

```
136     |     |     |     | path: "provision/server/netlog.sh"
137     |     |     |     |
138     |     |     |     | server.vm.provision "server protect",
139     |     |     |     |     | type: "shell",
140     |     |     |     |     | preserve_order: true,
141     |     |     |     |     | path: "provision/server/protect.sh"
142     |     |     |     end
143
144
```

Vagrantfile

Выводы

В результате выполнения лабораторной работы были получены навыки работы с программным средством Fail2ban.