

Лабораторная работа

Номер 16

Мошаров Д.М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

Приобретение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа "brute force".

```
[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 7.3 kB/s | 9.6 kB    00:01
```

Рис. 1: Установка fail2ban

```
[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 ~]$
```

Рис. 2: Запуск fail2ban

tail -f /var/log/fail2ban.log

```
[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'
```

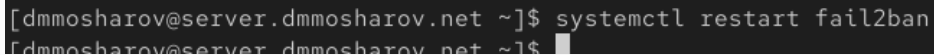
Рис. 3: tail -f /var/log/fail2ban.log

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

Рис. 4: customisation.local


```
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
```

Рис. 5: Параметры customisation.local

A terminal window with a dark background and light gray text. The prompt is [dmmosharov@server.dmmosharov.net ~]\$. The command systemctl restart fail2ban has been entered. The next line shows the prompt again, [dmmosharov@server.dmmosharov.net ~]\$, with a white cursor block at the end.

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

Рис. 6: Перезапуск fail2ban

```
2026-02-11 21:24:24,809 fail2ban.database [90071]: INFO Connected to f
ail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 21:24:24,811 fail2ban.database [90071]: WARNING New database c
reated. Version '4'
2026-02-11 21:26:34,787 fail2ban.server [90071]: INFO Shutdown in pr
ogress...
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 stopp
ed, 0 events remaining.
2026-02-11 21:26:34,859 fail2ban.server [90071]: INFO Stopping all j
ails
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 Fail2b
an
2026-02-11 21:26:35,039 fail2ban.server [90730]: INFO -----
-----
2026-02-11 21:26:35,040 fail2ban.server [90730]: INFO Starting Fail2
ban 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 f
ail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
```

Рис. 7: Журнал событий

```
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

#
# 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]
```

Рис. 8: HTTP

```
[dmmosharov@server.dmmosharov.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'
```

Рис. 9: Журнал событий

```
enabled = true

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

Рис. 10: Защита почты

```
[dmmosharov@server.dmmosharov.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'
2026-02-11 21:29:00,869 fail2ban.server [90984]: INFO Shutdown in progress...
2026-02-11 21:29:00,870 fail2ban.observer [90984]: INFO Observer stop ... try to end queue 5 seconds
2026-02-11 21:29:00,900 fail2ban.observer [90984]: INFO Observer stopped, 0 events remaining.
2026-02-11 21:29:00,940 fail2ban.server [90984]: INFO Stopping all jails
2026-02-11 21:29:00,941 fail2ban.database [90984]: INFO Connection to database closed.
2026-02-11 21:29:00,941 fail2ban.server [90984]: INFO Exiting Fail2ban
2026-02-11 21:29:01,063 fail2ban.server [91185]: INFO -----
2026-02-11 21:29:01,064 fail2ban.server [91185]: INFO Starting Fail2ban v1.1.0
2026-02-11 21:29:01,064 fail2ban.observer [91185]: INFO Observer start...
2026-02-11 21:29:01,070 fail2ban.database [91185]: INFO Connected to fail2ban persistent database '/var/lib
/fail2ban/fail2ban.sqlite3'
^C
```

Рис. 11: Просмотр журнала

Настройка fail2ban

```
[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-noho
me, 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          [91903]: ERROR    Permission denied to socket: /var/run/fail2ban/fail
2ban.sock, (you must be root)
[dmmosharov@server.dmmosharov.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[dmmosharov@server.dmmosharov.net ~]$
```

Рис. 12: Настройка fail2ban

Попытка зайти с неправильным паролем

```
[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:F8sREGCc3d3bq03xJrbnrCFDPDWDr/+seyPOj5DX9uI.
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: █
```

Рис. 13: Попытка зайти с неправильным паролем

```
[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 ~]$
```

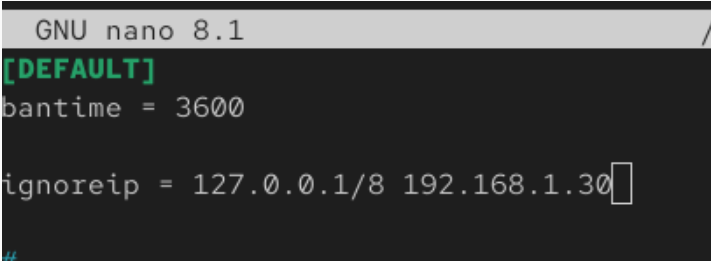
Рис. 14: Проверка защиты

```
Microsoft Windows [Version 10.0.19045.6456]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\denis>cd C:\work_asp\dmmosharov\vagrant

C:\work_asp\dmmosharov\vagrant>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
    client: Adapter 1: nat
    client: Adapter 2: intnet
==> client: Forwarding ports...
    client: 22 (guest) => 2200 (host) (adapter 1)
==> client: Running 'pre-boot' VM customizations...
==> client: Booting VM...
```

Рис. 15: unbanip

A screenshot of a terminal window showing the GNU nano 8.1 text editor. The editor's title bar is light gray and contains the text "GNU nano 8.1" followed by a cursor. The main editing area has a dark background with light gray text. The text "[DEFAULT]" is displayed in green. Below it, the line "bantime = 3600" is visible. The next line shows "ignoreip = 127.0.0.1/8 192.168.1.30" with a white cursor box at the end of the line. At the bottom left, a blue hash symbol "#" is visible.

```
GNU nano 8.1 /  
[DEFAULT]  
bantime = 3600  
ignoreip = 127.0.0.1/8 192.168.1.30  
#
```

Рис. 16: Конфигурационный файл

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

Рис. 17: Перезапуск fail2ban

```
connection closed by 192.168.1.1 port 22  
[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: █
```

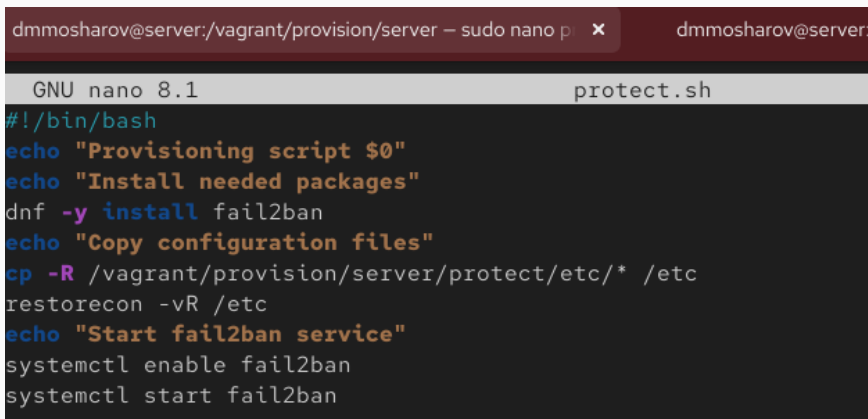
Рис. 18: Попытка подключения

```
[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 ~]$
```

Рис. 19: Статус SSH

```
[dmmosharov@server.dmmosharov.net ~]$ cd /vagrant/provision/server
[dmmosharov@server.dmmosharov.net server]$ mkdir -p /vagrant/provision/server/protect/etc
/vagrant/provision/server/protect/etc/fail2ban/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
```

Рис. 20: protect.sh



The image shows a terminal window with a dark background. The title bar at the top indicates the user is 'dmmosharov' on a 'server' machine, editing a file named 'protect.sh' using 'sudo nano'. The terminal content shows the script's execution flow: it starts with a shebang, prints a provisioning message, installs 'fail2ban' using 'dnf', copies configuration files from a specific path to '/etc', restores permissions, and finally enables and starts the 'fail2ban' service using 'systemctl'.

```
dmmosharov@server:/vagrant/provision/server — sudo nano p x 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
```

Рис. 21: Скрипт protect.sh

```
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
```

Рис. 22: Vagrantfile

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