

# Лабораторная работа 16

---

Генералов Даниил, НПИбд-01-21, 1032202280

2023

<sup>1</sup>RUDN University, Moscow, Russian Federation

## Задача

---

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб (см. раздел 16.4.1).

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб (см. раздел 16.4.1).
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH (см. раздел 16.4.2).

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб (см. раздел 16.4.1).
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH (см. раздел 16.4.2).
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban (см. раздел 16.4.3).

## Выполнение

---

# fail2ban

The screenshot shows a terminal window with the fail2ban configuration file `/etc/fail2ban/jail.d/customization.local` and the service status output.

```
root@server:~# cat /etc/fail2ban/jail.d/customization.local
[DEFAULT]
bantime = 3600

# ssh
[ssh]
filter = sshd
port = ssh,2222

[sshd-ddos]
filter = sshd
enabled = true

[sshd-tcp]
enabled = true

# HTTP
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-modsecurity]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botsearch]
enabled = true
[apache-fawgointelct]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true

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

The service status output shows the following information:

```
2023-12-20 23:59:38,007 fail2ban.filter (9860): INFO maxRetry: 5
2023-12-20 23:59:38,008 fail2ban.filter (9860): INFO findtime: 600
2023-12-20 23:59:38,009 fail2ban.action (9860): INFO bantime: 3600
2023-12-20 23:59:38,009 fail2ban.filter (9860): INFO encoding: UTF-8
2023-12-20 23:59:38,018 fail2ban.jail (9860): INFO Jail 'apache-auth' started
2023-12-20 23:59:38,032 fail2ban.jail (9860): INFO Jail 'apache-badbots' started
2023-12-20 23:59:38,036 fail2ban.jail (9860): INFO Jail 'apache-modsecurity' started
2023-12-20 23:59:38,040 fail2ban.jail (9860): INFO Jail 'apache-overflows' started
2023-12-20 23:59:38,048 fail2ban.jail (9860): INFO Jail 'apache-nohome' started
2023-12-20 23:59:38,058 fail2ban.jail (9860): INFO Jail 'apache-botsearch' started
2023-12-20 23:59:38,061 fail2ban.jail (9860): INFO Jail 'apache-fawgointelct' started
2023-12-20 23:59:38,058 fail2ban.jail (9860): INFO Jail 'apache-modsecurity' started
2023-12-20 23:59:38,062 fail2ban.jail (9860): INFO Jail 'apache-shellshock' started
2023-12-20 23:59:38,064 fail2ban.jail (9860): INFO Jail 'postfix' started
2023-12-20 23:59:38,067 fail2ban.filtersystem (9860): INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-20 23:59:38,070 fail2ban.filtersystem (9860): INFO Jail 'postfix-rbl' started
2023-12-20 23:59:38,079 fail2ban.jail (9860): INFO Jail 'dovecot' started
2023-12-20 23:59:38,083 fail2ban.filtersystem (9860): INFO [dovecot] Jail is in operation now (process new journal entries)
2023-12-20 23:59:38,083 fail2ban.filtersystem (9860): INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-20 23:59:38,084 fail2ban.jail (9860): INFO Jail 'postfix-sasl' started
2023-12-20 23:59:38,085 fail2ban.jail (9860): INFO Jail 'sshd-ddos' started
```

The terminal also shows the command `systemctl restart fail2ban.service` being executed.

Рис. 1: fail2ban

# fail2ban

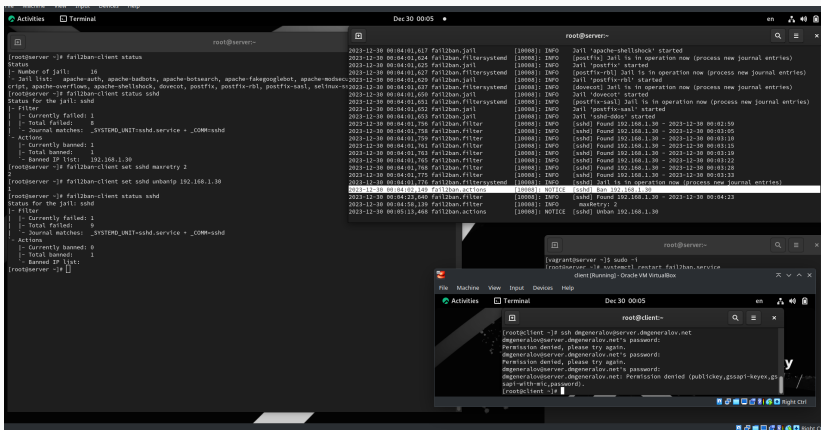


Рис. 2: fail2ban



# fail2ban

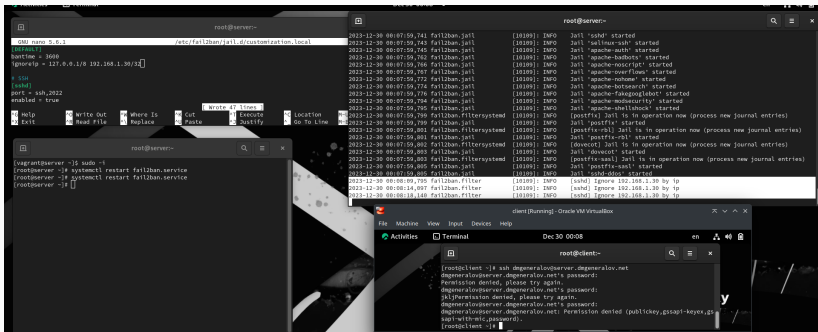


Рис. 3: fail2ban

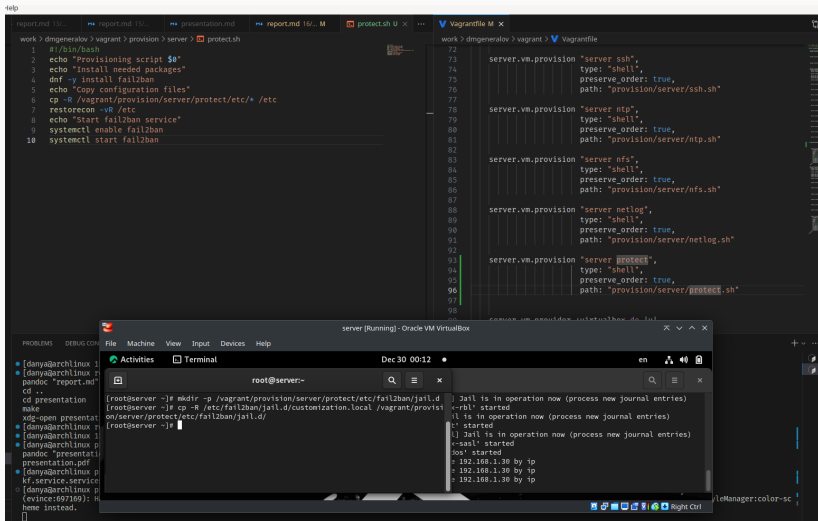


Рис. 4: vagrant

Я получил опыт настройки защиты важных служб с помощью fail2ban.