

# **Отчет по лабораторной работе 16**

Генералов Даниил, НПИбд-01-21, 1032202280

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
5	Контрольные вопросы	11

# Список иллюстраций

3.1	fail2ban . . . . .	7
3.2	fail2ban . . . . .	8
3.3	fail2ban . . . . .	8
3.4	vagrant . . . . .	9

## Список таблиц

# 1 Цель работы

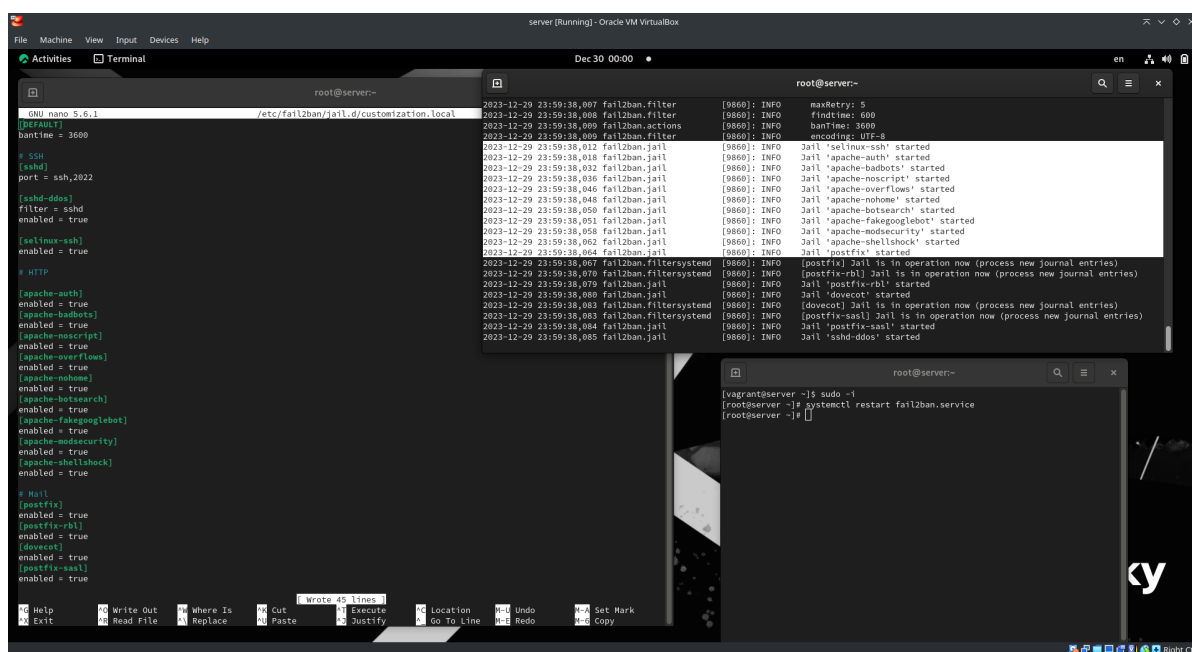
Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

## 2 Задание

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).

## 3 Выполнение лабораторной работы

Сначала я установил fail2ban на сервер, и добавил в файл конфигурации команды, включающие защиту SSH, HTTP и почтовых служб.



The screenshot shows a terminal window with the fail2ban configuration file open in nano. The configuration includes settings for SSH, HTTP, and various mail services. The status output shows that fail2ban is running and has successfully started jails for these services.

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

# SSH
[sshd]
filter = sshd
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

# HTTP
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-noscript]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botssearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true

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

2023-12-29 23:59:38.007 fail2ban.filter [9860]: INFO maxRetry: 5
2023-12-29 23:59:38.008 fail2ban.filter [9860]: INFO findtime: 600
2023-12-29 23:59:38.009 fail2ban.actions [9860]: INFO bantime: 3600
2023-12-29 23:59:38.009 fail2ban.filter [9860]: INFO encoding: UTF-8
2023-12-29 23:59:38.012 fail2ban.jail [9860]: INFO Jail 'sshd-ddos' started
2023-12-29 23:59:38.018 fail2ban.jail [9860]: INFO Jail 'sshd' started
2023-12-29 23:59:38.032 fail2ban.jail [9860]: INFO Jail 'apache-badbots' started
2023-12-29 23:59:38.036 fail2ban.jail [9860]: INFO Jail 'apache-noscript' started
2023-12-29 23:59:38.046 fail2ban.jail [9860]: INFO Jail 'apache-overflows' started
2023-12-29 23:59:38.048 fail2ban.jail [9860]: INFO Jail 'apache-nohome' started
2023-12-29 23:59:38.050 fail2ban.jail [9860]: INFO Jail 'apache-botssearch' started
2023-12-29 23:59:38.051 fail2ban.jail [9860]: INFO Jail 'apache-fakegooglebot' started
2023-12-29 23:59:38.058 fail2ban.jail [9860]: INFO Jail 'apache-modsecurity' started
2023-12-29 23:59:38.062 fail2ban.jail [9860]: INFO Jail 'apache-shellshock' started
2023-12-29 23:59:38.064 fail2ban.jail [9860]: INFO Jail 'postfix' started
2023-12-29 23:59:38.067 fail2ban.filterssystemd [9860]: INFO [postfix] Jail is in operation now (process new journal entries)
2023-12-29 23:59:38.070 fail2ban.filterssystemd [9860]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-29 23:59:38.079 fail2ban.jail [9860]: INFO Jail 'postfix-rbl' started
2023-12-29 23:59:38.080 fail2ban.jail [9860]: INFO Jail 'dovecot' started
2023-12-29 23:59:38.083 fail2ban.filterssystemd [9860]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-12-29 23:59:38.083 fail2ban.filterssystemd [9860]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-29 23:59:38.084 fail2ban.jail [9860]: INFO Jail 'postfix-sasl' started
2023-12-29 23:59:38.085 fail2ban.jail [9860]: INFO Jail 'sshd-ddos' started
```

Рис. 3.1: fail2ban

После этого я попытался подключиться с клиента с неправильным паролем. Это было замечено, и IP-адрес клиента был заблокирован, что можно увидеть с помощью логов и команды status, а также отменить с помощью команды unban.

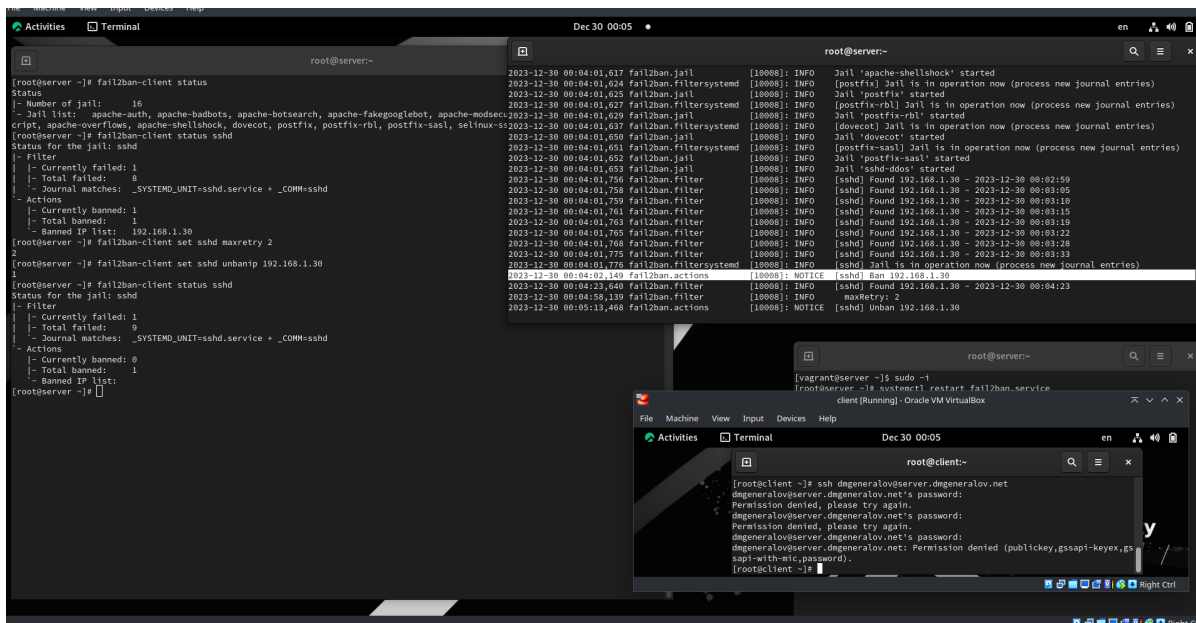


Рис. 3.2: fail2ban

Однако, если добавить IP-адрес клиента в игнорируемый список, то он не будет заблокирован, даже если он появляется в списке ошибок.

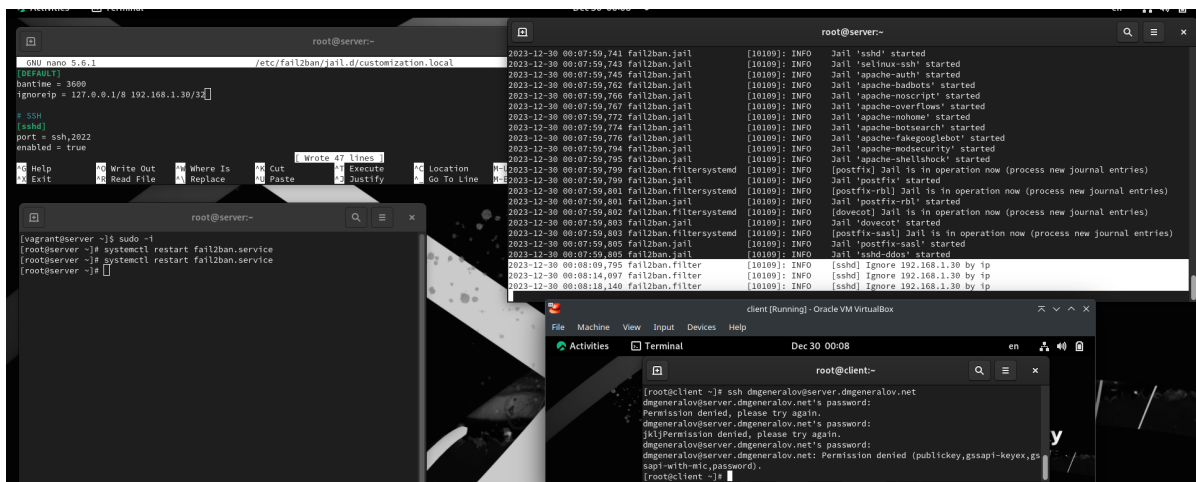


Рис. 3.3: fail2ban

Наконец, экспортируем настройки в Vagrantfile.



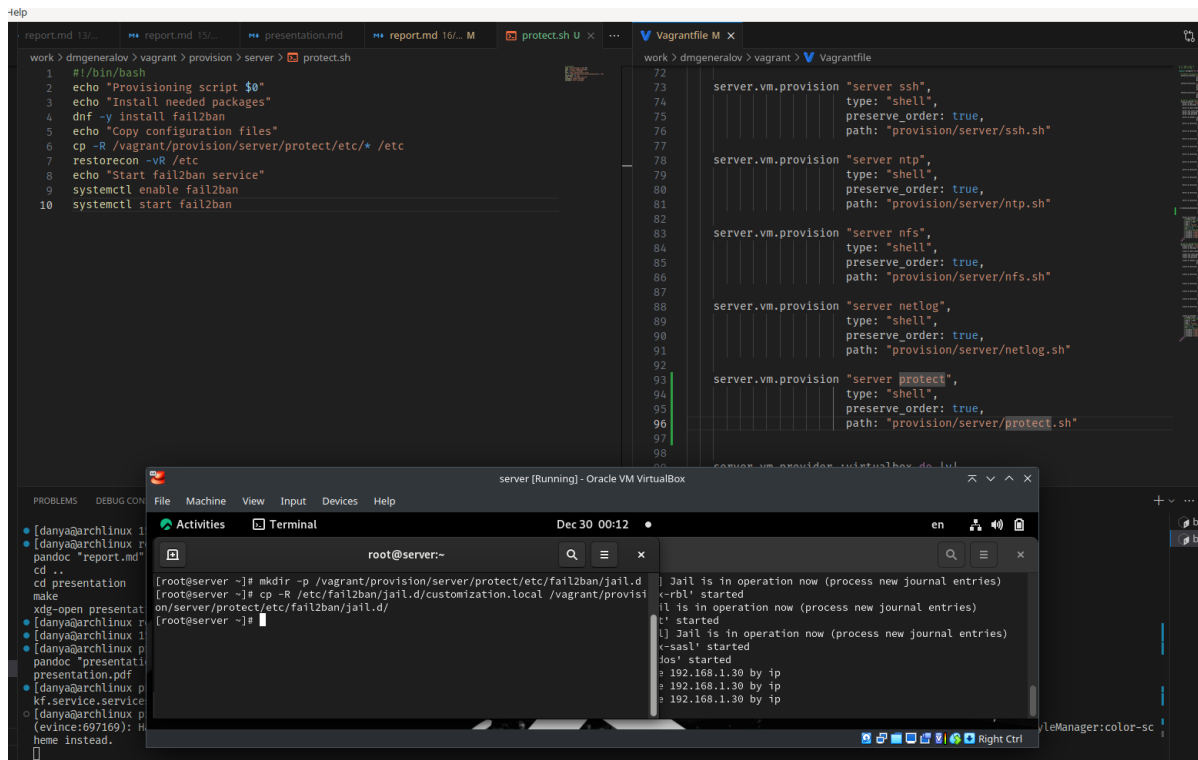


Рис. 3.4: vagrant

## 4 Выводы

Я получил опыт настройки защиты важных служб с помощью fail2ban.

## 5 Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Сервис отслеживает лог-файлы различных веб-служб, и если строка с IP-адресом появляется чаще настроенного ограничения, то этот IP-адрес блокируется.

2. Настройки какого файла более приоритетны: jail.conf или jail.local?

Файл jail.conf устанавливает базовые настройки, которые затем могут быть дополнены файлами .local в jail.d

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Надо добавить действие в настройку jail:

```
action = iptables[name=SSH,port=22,protocol=tcp] sendmsg
```

Затем нужно создать настройку действия sendmsg.conf

```
[Definition]
```

```
actionstart =
```

```
actionstop =
```

```
actioncheck =
```

```
actionban = curl -X POST https://example.com/webhook/banned/<ip>
```

```
actionunban =
```

4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.

Они имеют вид:

```
[apache-auth] # название модуля
port      = http,https # если блокировать, то эти порты
logpath   = %(apache_error_log)s # принимать решение о блокировке относительно эт
```

5. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе.

Они имеют вид:

```
[sendmail-auth] # название модуля

port      = submission,465,smtp # если блокировать, то эти порты
logpath   = %(syslog_mail)s      # следить за этим файлом логов
backend   = %(syslog_backend)s   # сообщения будут приходить через syslog
```

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Все действия можно найти в `/etc/fail2ban/action.d` и их описания обычно находятся в начале каждого файла.

7. Как получить список действующих правил Fail2ban?

```
fail2ban-client status
```

8. Как получить статистику заблокированных Fail2ban адресов?

```
fail2ban-client banned
```

9. Как разблокировать IP-адрес?

```
fail2ban-client unban 1.2.3.4
```