Лабораторная работа №16

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

Раздел 1

1. Цель работы

1.1 Цель работы

- Получение навыков работы с Fail2ban
- Настройка базовой защиты от атак типа brute force

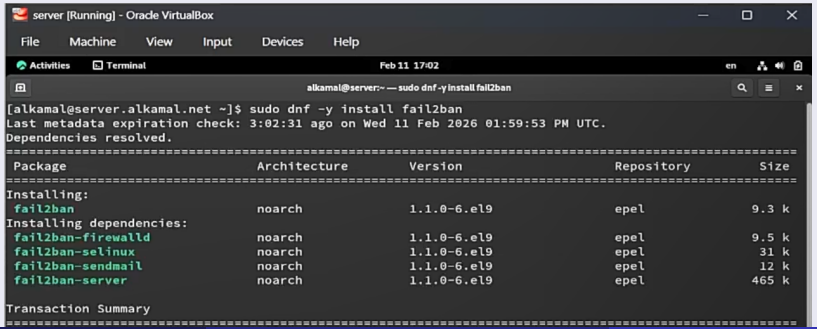
Раздел 2

2. Выполнение лабораторной работы

2.1 Защита с помощью Fail2ban

2.1.1 Установка Fail2ban

- Установлен пакет `fail2ban` через `dnf`
- Установлены зависимости: `fail2ban-firewalld`, `fail2ban-selinux`, `fail2ban-sendmail`, `fail2ban-server`
- Использован репозиторий `epel`



2.1.2 Запуск и добавление службы в автозагрузку

- Выполнен `systemctl start fail2ban`
- Выполнен `systemctl enable fail2ban`
- Создана ссылка в `multi-user.target.wants`

```
Complete!
[alkamal@server.alkamal.net ~]$ sudo systemctl start fail2ban
[alkamal@server.alkamal.net ~]$ sudo systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/f
ail2ban.service.
[alkamal@server.alkamal.net ~]$
```

Рисунок 2: Запуск службы fail2ban и включение автозагрузки

2.1.3 Контроль журнала событий Fail2ban

- Выполнен `tail -f /var/log/fail2ban.log`
- Зафиксирован запуск Fail2ban 1.1.0
- Инициализирован observer
- Создана база `fail2ban.sqlite3`

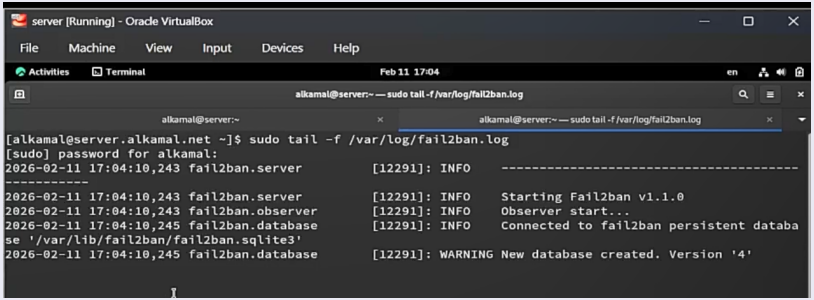


Рисунок 3: Просмотр журнала fail2ban.log в реальном времени

2.1.4 Создание файла локальной конфигурации

- Создан файл `/etc/fail2ban/jail.d/customisation.local`
- Выполнено редактирование в `nano`

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

Рисунок 4: Создание и перезапуск службы после настройки

2.1.5 Настройка параметров блокирования и защиты SSH

- В [DEFAULT] установлен bantime = 3600
- Активированы [sshd], [sshd-ddos], [selinux-ssh]
- Указан порт ssh, 2022
- Для всех секций enabled = true

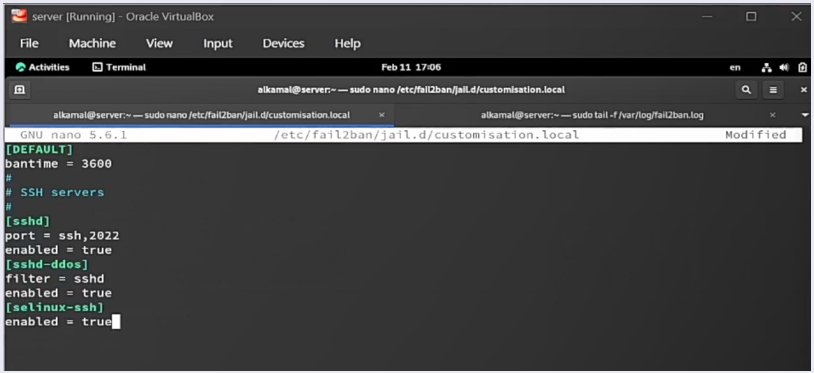


Рисунок 5: Конфигурация customisation.local с параметрами bantime и SSH

2.1.6 Перезапуск службы Fail2ban

- Выполнен `systemctl restart fail2ban`
- Применена новая конфигурация

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

Рисунок 6: Создание и перезапуск службы после настройки

2.1.7 Просмотр журнала после настройки SSH

- Инициализирован backend `pyinotify`
- Установлены параметры `maxRetry`, `findtime`, `banTime = 3600`
- Запущены jail-модули `sshd`, `selinux-ssh`, `sshd-ddos`

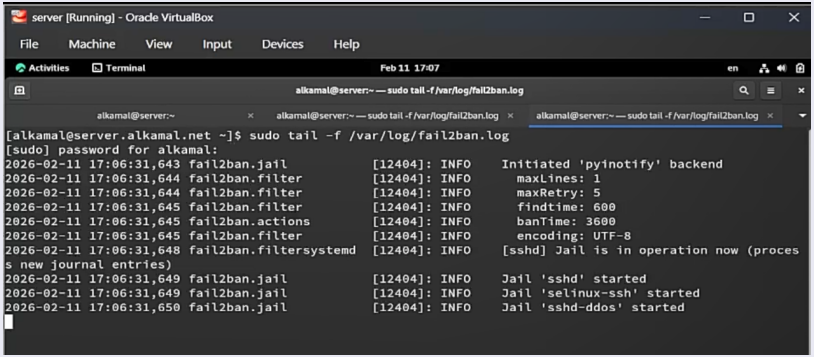
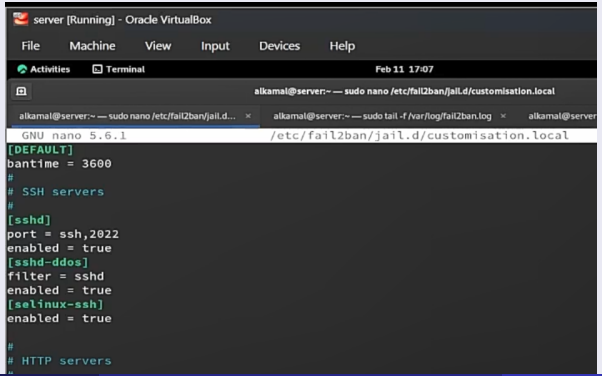


Рисунок 7: Журнал запуска jail-модулей SSH в fail2ban

2.1.8 Включение защиты HTTP

- Активированы jail-модули: `apache-auth`, `apache-badbots`, `apache-noscript`, `apache-overflows`, `apache-nohome`, `apache-botsearch`, `apache-fakegooglebot`, `apache-modsecurity`, `apache-shellshock`
- Для всех `enabled = true`



2.1.9 Перезапуск после настройки HTTP

- Выполнен `systemctl restart fail2ban`
- Загружены HTTP jail-модули

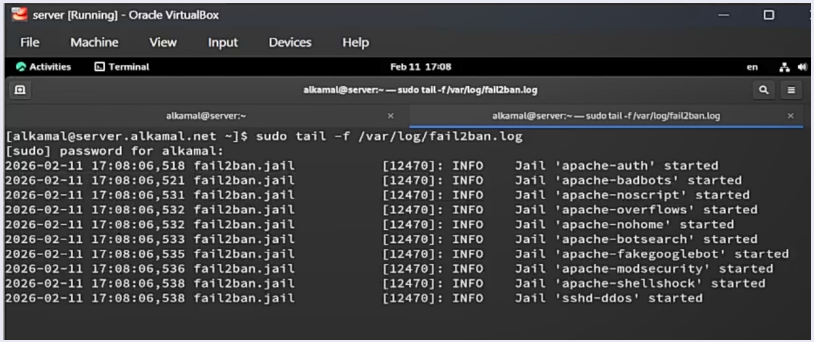


Рисунок 9: Журнал запуска HTTP jail-модулей

2.1.10 Контроль журнала HTTP-защиты

- В журнале зафиксирован запуск всех `apache-*` jail
- Подтверждена активация `sshd-ddos`

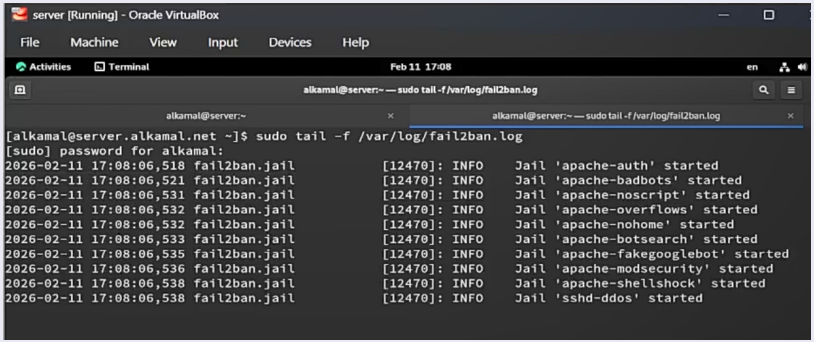


Рисунок 10: Подтверждение запуска HTTP jail-модулей в журнале

2.1.11 Включение защиты почтовых сервисов

- Активированы jail-модули: `postfix`, `postfix-rbl`, `dovecot`, `postfix-sasl`
- Установлено `enabled = true`

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

2.1.12 Перезапуск после настройки почтовых служб

- Выполнен перезапуск `fail2ban`
- Загружены почтовые jail-модули

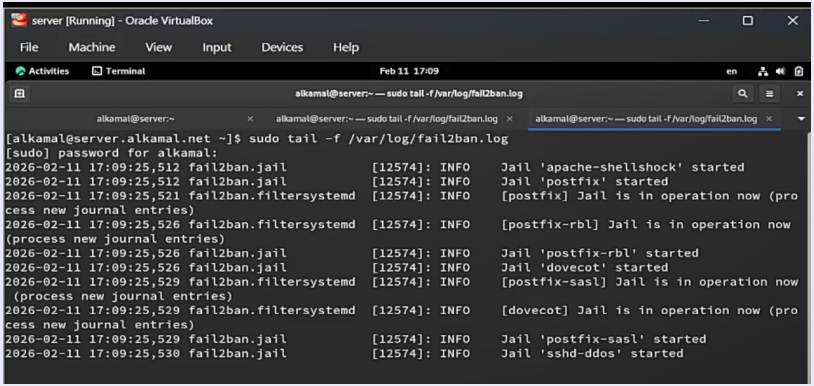


Рисунок 12: Журнал запуска jail-модулей почтовых сервисов

2.1.13 Контроль журнала почтовой защиты

- Зафиксировано `Jail is in operation now`
- Подтверждена активация `postfix`, `dovecot`, `postfix-sasl`

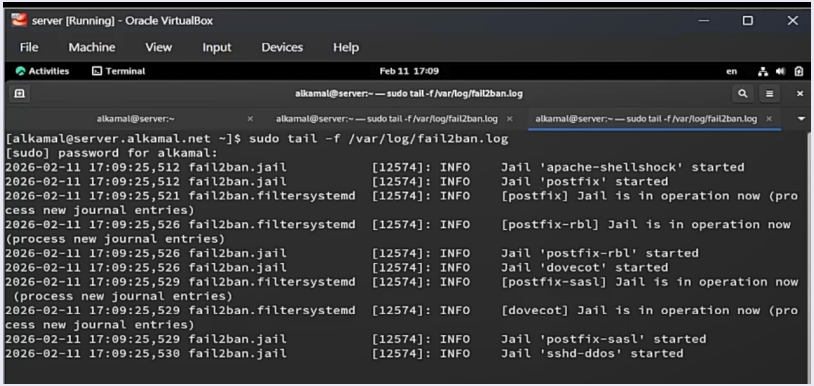
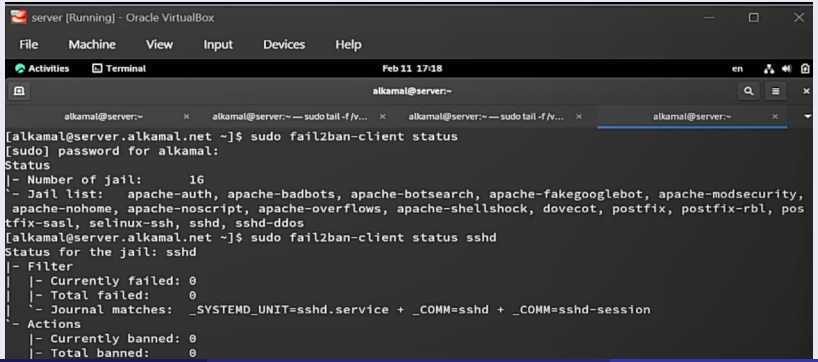


Рисунок 13: Подтверждение работы jail-модулей почтовых сервисов

2.2 Проверка работы Fail2ban

2.2.1 Просмотр общего статуса

- Выполнен `fail2ban-client status`
- Активировано 16 jail-модулей
- Отображены `apache-*`, `sshd`, `dovecot`, `postfix`



2.2.2 Просмотр статуса SSH

- Выполнен `fail2ban-client status sshd`
- `Currently banned: 0`
- `Total banned: 0`

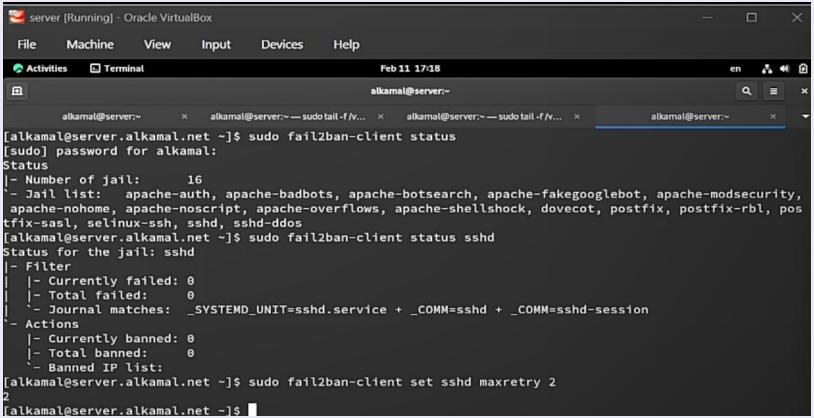


Рисунок 15: Статус jail модуля sshd до проверки

2.2.3 Установка maxretry

- Выполнено `fail2ban-client set sshd maxretry 2`
- После 2 ошибок IP должен блокироваться

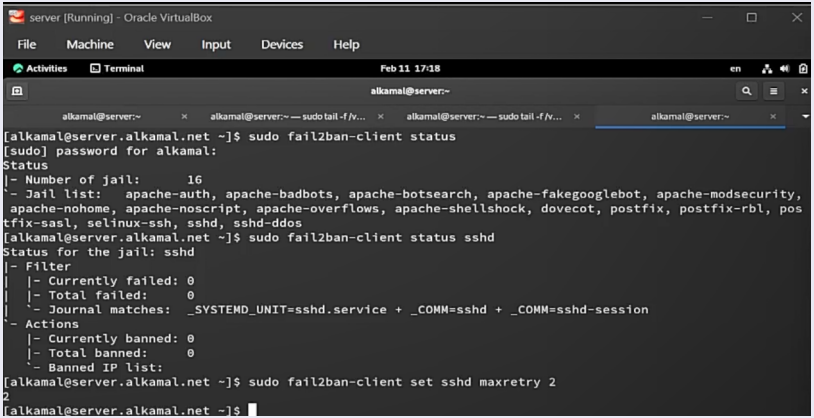


Рисунок 16: Установка параметра maxretry для sshd

2.2.4 Попытка входа с неверным паролем

- С клиента выполнены неудачные попытки SSH-входа
- Зафиксированы ошибки `Permission denied`

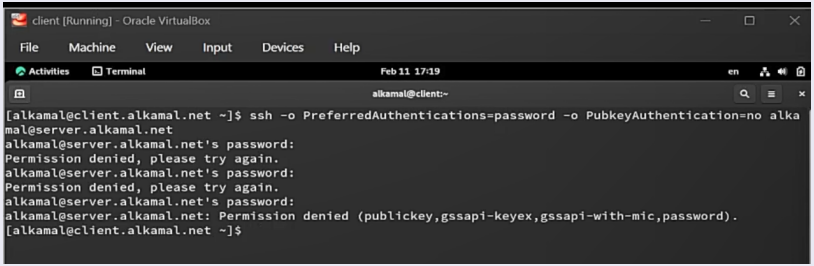


Рисунок 17: Попытки входа по SSH с неверным паролем

2.2.5 Проверка блокировки IP

- Выполнен `fail2ban-client status sshd`
- `Currently banned: 1`
- IP `192.168.1.30` в списке блокировки

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status sshd
[sudo] password for alkamal:
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- 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
[alkamal@server.alkamal.net ~]$
```

Рисунок 18: Блокировка IP-адреса клиента в sshd

2.2.6 Разблокировка IP

- Выполнено `fail2ban-client set sshd unbanip 192.168.1.30`

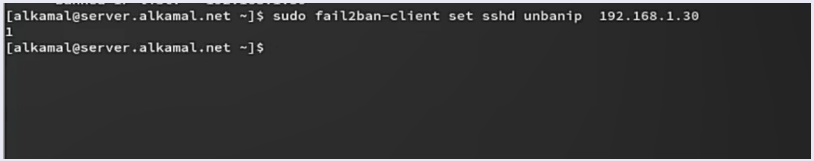


Рисунок 19: Команда разблокировки IP-адреса клиента

2.2.7 Проверка снятия блокировки

- Повторный `status sshd`
- `Currently banned: 0`
- Список пуст

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[alkamal@server.alkamal.net ~]$
```

Рисунок 20: Статус sshd после снятия блокировки

2.2.8 Добавление ignoreip

- В [DEFAULT] добавлен `ignoreip = 127.0.0.1/8 192.168.1.30`
- IP клиента исключён из блокировки

Рисунок 21: Добавление параметра ignoreip в customisation.local

2.2.9 Перезапуск службы

- Выполнен `systemctl restart fail2ban`
- Применена новая конфигурация

```
[alkamal@client.alkamal.net ~]$ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no alka
mal@server.alkamal.net
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
alkamal@server.alkamal.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[alkamal@client.alkamal.net ~]$
```

Рисунок 22: Попытка входа с клиента после изменения конфигурации

2.2.10 Просмотр журнала ignoreip

- В журнале отображено `Ignore 192.168.1.30 by ip`
- IP корректно исключён

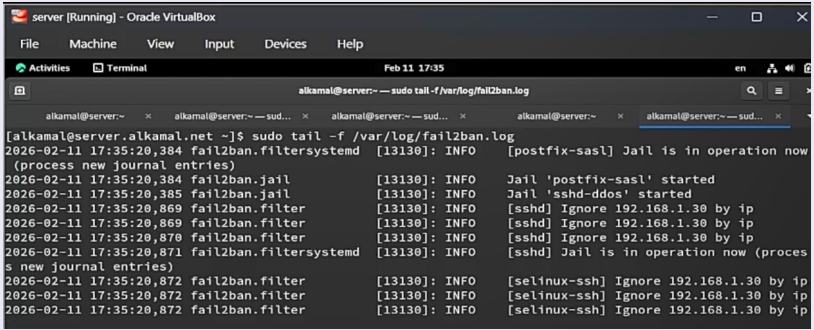


Рисунок 23: Сообщения журнала о игнорировании IP-адреса

2.2.11 Повторная проверка SSH

- Повторные ошибки входа не приводят к блокировке
- `Currently banned: 0`
- Список IP пуст

```
[alkamal@server.alkamal.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:
[alkamal@server.alkamal.net ~]$
```

Рисунок 24: Статус sshd после включения ignoreip

2.3.1 Подготовка конфигурации

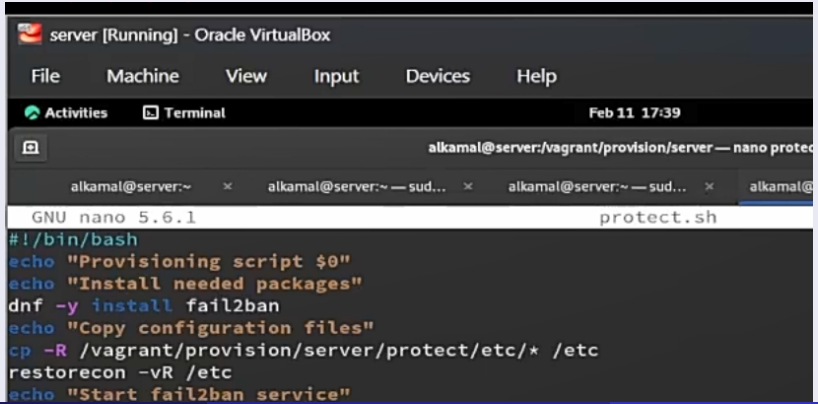
- Создан каталог `protect/etc/fail2ban/jail.d`
- Скопирован `customisation.local`

```
[alkamal@server.alkamal.net ~]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[alkamal@server.alkamal.net server]$ sudo cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provis
ion/server/protect/etc/fail2ban/jail.d/
[alkamal@server.alkamal.net server]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ touch protect.sh
[alkamal@server.alkamal.net server]$ chmod +x protect.sh
[alkamal@server.alkamal.net server]$ nano protect.sh
```

Рисунок 25: Создание каталога protect и копирование customisation.local

2.3.2 Создание скрипта protect.sh

- Установка `fail2ban`
- Копирование конфигурации в `/etc`
- Выполнен `restorecon -vR /etc`
- Включена и запущена служба



2.3.3 Добавление provisioning в Vagrantfile

- Добавлен блок `server.vm.provision`
- Указан путь `provision/server/protect.sh`
- Использован `preserve_order: true`

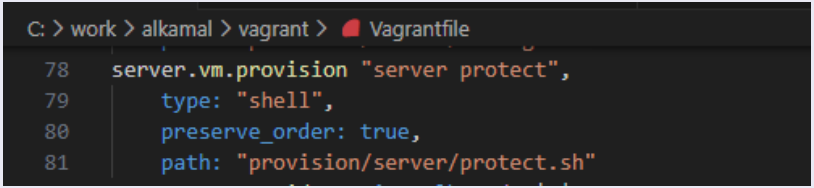


Рисунок 27: Добавление блока provision в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Установлен и настроен Fail2ban
- Реализована защита SSH, HTTP и почтовых сервисов
- Проверена блокировка IP при превышении `maxretry`
- Выполнена ручная разблокировка
- Настроен параметр `ignoreip`
- Подтверждена корректная работа jail-модулей
- Настройка автоматизирована через provisioning
- Обеспечена воспроизводимая базовая защита от brute force