

Отчет по лабораторной работе №16

Базовая защита от атак типа «brute force»

Галацан Николай, НПИбд-01-22

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Защита с помощью Fail2ban	5
2.2	Проверка работы Fail2ban	9
2.3	Внесение изменений в настройки внутреннего окружения виртуальной машины	11
3	Выводы	13
4	Ответы на контрольные вопросы	14

Список иллюстраций

2.1	Установка и запуск fail2ban	5
2.2	Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH	6
2.3	Просмотр журнала событий fail2ban	6
2.4	Редактирование файла с локальной конфигурацией: защита HTTP	7
2.5	Просмотр журнала событий fail2ban	7
2.6	Редактирование файла с локальной конфигурацией: защита почты	8
2.7	Просмотр журнала событий fail2ban	8
2.8	Подключение к серверу по SSH с вводом неправильного пароля	9
2.9	Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента	10
2.10	Редактирование файла с локальной конфигурацией: игнорирование адреса клиента	10
2.11	Просмотр журнала событий 'fail2ban'	11
2.12	Просмотр статуса защиты SSH после неудачного входа	11
2.13	Редактирование protect.sh на сервере	12

1 Цель работы

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

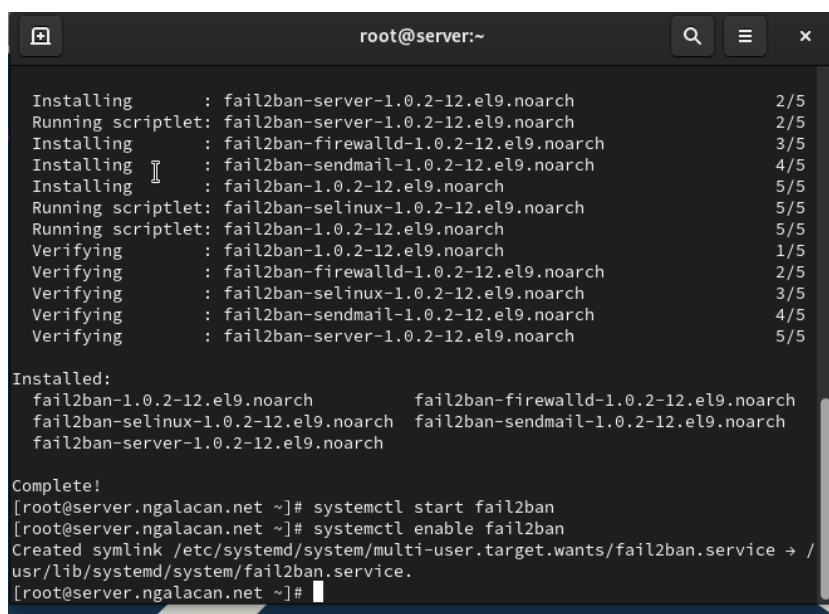
2 Выполнение лабораторной работы

2.1 Защита с помощью Fail2ban

На сервере устанавливаю fail2ban:

```
dnf -y install fail2ban
```

Запускаю сервер fail2ban (рис. 2.1).



```
root@server:~  
Installing      : fail2ban-server-1.0.2-12.el9.noarch      2/5  
Running scriptlet: fail2ban-server-1.0.2-12.el9.noarch    2/5  
Installing      : fail2ban-firewalld-1.0.2-12.el9.noarch  3/5  
Installing      : fail2ban-sendmail-1.0.2-12.el9.noarch  4/5  
Installing      : fail2ban-1.0.2-12.el9.noarch           5/5  
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch   5/5  
Running scriptlet: fail2ban-1.0.2-12.el9.noarch          5/5  
Verifying       : fail2ban-1.0.2-12.el9.noarch           1/5  
Verifying       : fail2ban-firewalld-1.0.2-12.el9.noarch 2/5  
Verifying       : fail2ban-selinux-1.0.2-12.el9.noarch   3/5  
Verifying       : fail2ban-sendmail-1.0.2-12.el9.noarch  4/5  
Verifying       : fail2ban-server-1.0.2-12.el9.noarch    5/5  
  
Installed:  
fail2ban-1.0.2-12.el9.noarch      fail2ban-firewalld-1.0.2-12.el9.noarch  
fail2ban-selinux-1.0.2-12.el9.noarch fail2ban-sendmail-1.0.2-12.el9.noarch  
fail2ban-server-1.0.2-12.el9.noarch  
  
Complete!  
[root@server.ngalacan.net ~]# systemctl start fail2ban  
[root@server.ngalacan.net ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.  
[root@server.ngalacan.net ~]#
```

Рис. 2.1: Установка и запуск fail2ban

В доп. терминале запускаю просмотр журнала событий fail2ban. Создаю файл с локальной конфигурацией /etc/fail2ban/jail.d/customisation.local. Задаю время блокирования, включаю защиту SSH, после чего перезапускаю fail2ban (рис. 2.2).

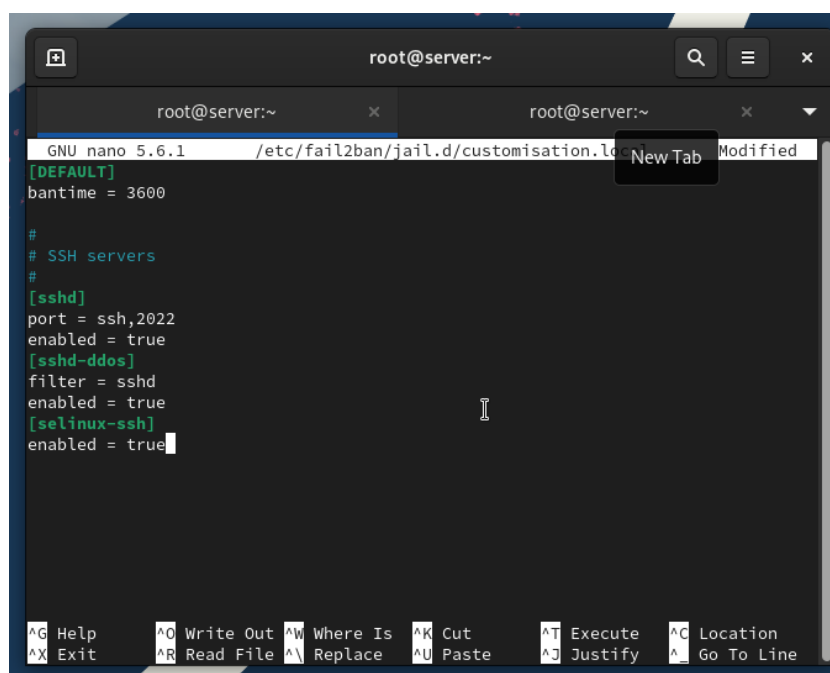


Рис. 2.2: Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH

Просматриваю журнал событий fail2ban и вижу сообщения об активации jail-ов (рис. 2.3).

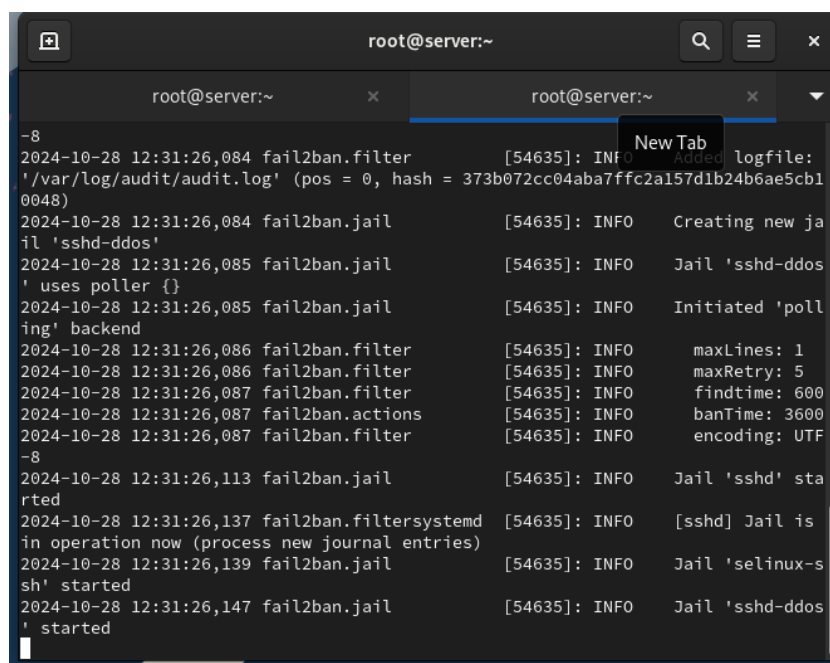
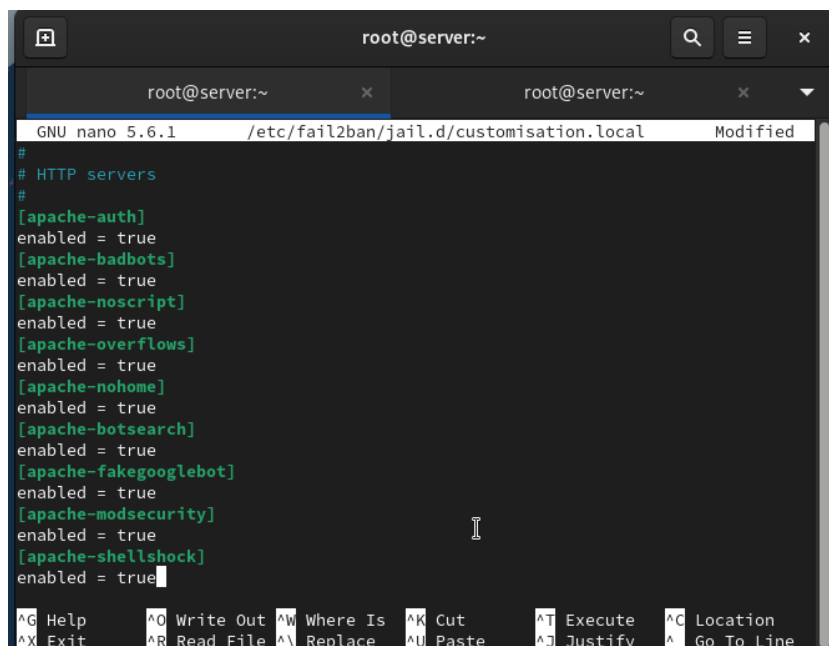


Рис. 2.3: Просмотр журнала событий fail2ban

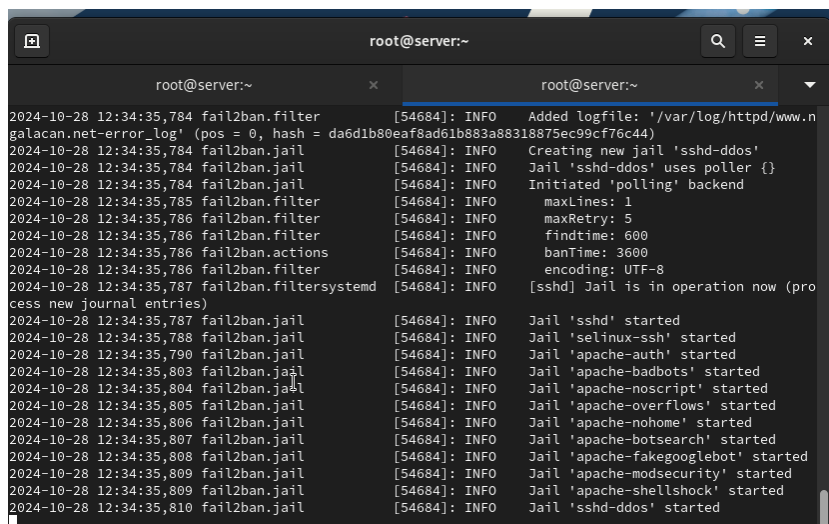
В файле конфигурации включаю защиту HTTP, после чего перезапускаю fail2ban (рис. 2.4).



```
root@server:~  
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified  
#  
# 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]  
enabled = true  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
```

Рис. 2.4: Редактирование файла с локальной конфигурацией: защита HTTP

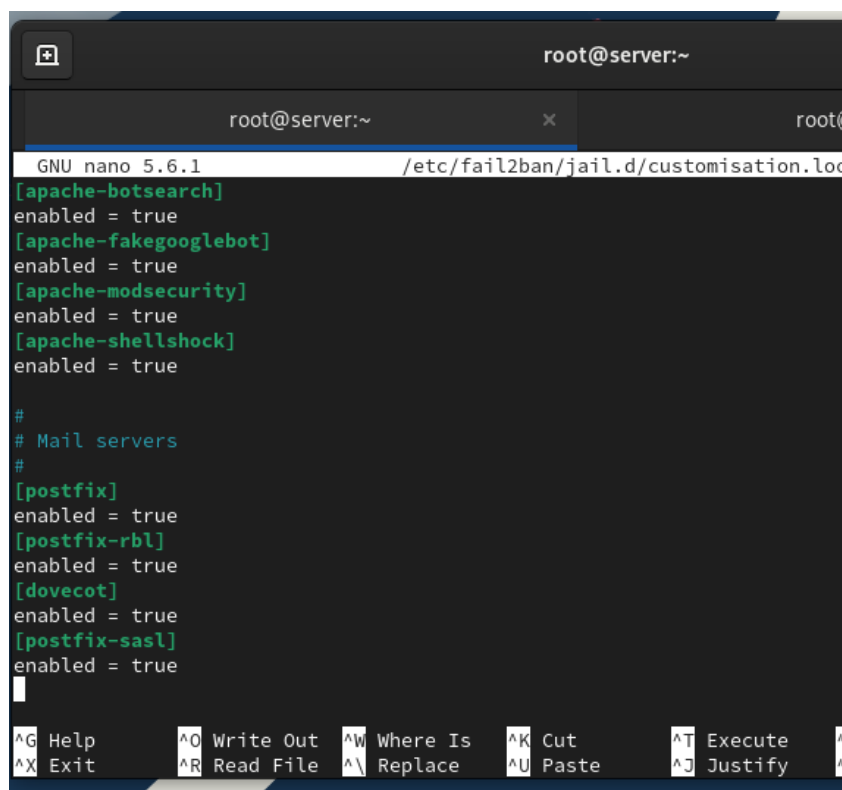
Просматриваю журнал событий fail2ban (рис. 2.5).



```
root@server:~  
2024-10-28 12:34:35,784 fail2ban.filter [54684]: INFO Added logfile: '/var/log/httpd/www.n  
galacan.net-error_log' (pos = 0, hash = da6dlb80eaf8ad61b883a88318875ec99cf76c44)  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Creating new jail 'sshd-ddos'  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Jail 'sshd-ddos' uses poller {}  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Initiated 'polling' backend  
2024-10-28 12:34:35,785 fail2ban.filter [54684]: INFO maxLines: 1  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO maxRetry: 5  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO findtime: 600  
2024-10-28 12:34:35,786 fail2ban.actions [54684]: INFO banTime: 3600  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO encoding: UTF-8  
2024-10-28 12:34:35,787 fail2ban.filtersystemd [54684]: INFO [sshd] Jail is in operation now (pro  
cess new journal entries)  
2024-10-28 12:34:35,787 fail2ban.jail [54684]: INFO Jail 'sshd' started  
2024-10-28 12:34:35,788 fail2ban.jail [54684]: INFO Jail 'selinux-ssh' started  
2024-10-28 12:34:35,790 fail2ban.jail [54684]: INFO Jail 'apache-auth' started  
2024-10-28 12:34:35,803 fail2ban.jail [54684]: INFO Jail 'apache-badbots' started  
2024-10-28 12:34:35,804 fail2ban.jail [54684]: INFO Jail 'apache-noscript' started  
2024-10-28 12:34:35,805 fail2ban.jail [54684]: INFO Jail 'apache-overflows' started  
2024-10-28 12:34:35,806 fail2ban.jail [54684]: INFO Jail 'apache-nohome' started  
2024-10-28 12:34:35,807 fail2ban.jail [54684]: INFO Jail 'apache-botsearch' started  
2024-10-28 12:34:35,808 fail2ban.jail [54684]: INFO Jail 'apache-fakegooglebot' started  
2024-10-28 12:34:35,809 fail2ban.jail [54684]: INFO Jail 'apache-modsecurity' started  
2024-10-28 12:34:35,809 fail2ban.jail [54684]: INFO Jail 'apache-shellshock' started  
2024-10-28 12:34:35,810 fail2ban.jail [54684]: INFO Jail 'sshd-ddos' started
```

Рис. 2.5: Просмотр журнала событий fail2ban

В файле конфигурации включаю защиту почты, после чего перезапускаю fail2ban (рис. 2.6).



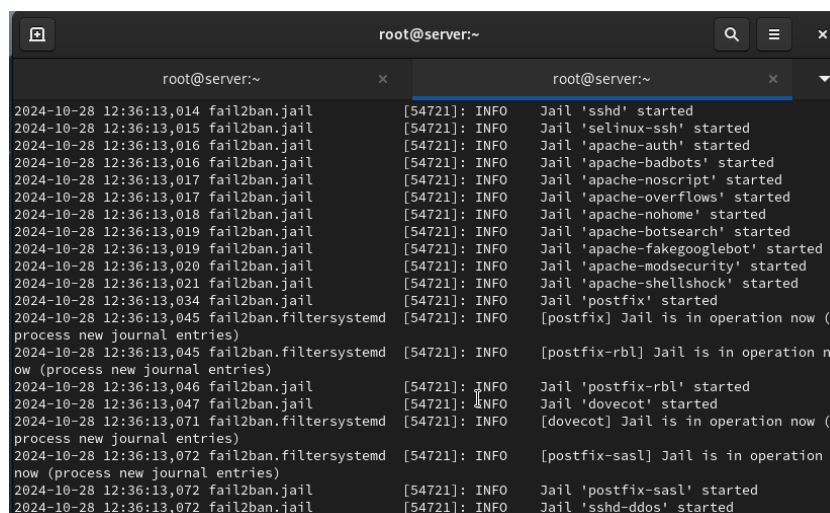
```
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local
[apache-botsearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true

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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Рис. 2.6: Редактирование файла с локальной конфигурацией: защита почты

Просматриваю журнал событий fail2ban (рис. 2.7).



```
root@server:~
2024-10-28 12:36:13,014 fail2ban.jail [54721]: INFO Jail 'sshd' started
2024-10-28 12:36:13,015 fail2ban.jail [54721]: INFO Jail 'selinux-ssh' started
2024-10-28 12:36:13,016 fail2ban.jail [54721]: INFO Jail 'apache-auth' started
2024-10-28 12:36:13,016 fail2ban.jail [54721]: INFO Jail 'apache-badbots' started
2024-10-28 12:36:13,017 fail2ban.jail [54721]: INFO Jail 'apache-noscript' started
2024-10-28 12:36:13,017 fail2ban.jail [54721]: INFO Jail 'apache-overflows' started
2024-10-28 12:36:13,018 fail2ban.jail [54721]: INFO Jail 'apache-nohome' started
2024-10-28 12:36:13,019 fail2ban.jail [54721]: INFO Jail 'apache-botsearch' started
2024-10-28 12:36:13,019 fail2ban.jail [54721]: INFO Jail 'apache-fakegooglebot' started
2024-10-28 12:36:13,020 fail2ban.jail [54721]: INFO Jail 'apache-modsecurity' started
2024-10-28 12:36:13,021 fail2ban.jail [54721]: INFO Jail 'apache-shellshock' started
2024-10-28 12:36:13,034 fail2ban.jail [54721]: INFO Jail 'postfix' started
2024-10-28 12:36:13,045 fail2ban.filtersystemd [54721]: INFO [postfix] Jail is in operation now (
process new journal entries)
2024-10-28 12:36:13,045 fail2ban.filtersystemd [54721]: INFO [postfix-rbl] Jail is in operation n
ow (process new journal entries)
2024-10-28 12:36:13,046 fail2ban.jail [54721]: INFO Jail 'postfix-rbl' started
2024-10-28 12:36:13,047 fail2ban.jail [54721]: INFO Jail 'dovecot' started
2024-10-28 12:36:13,071 fail2ban.filtersystemd [54721]: INFO [dovecot] Jail is in operation now (
process new journal entries)
2024-10-28 12:36:13,072 fail2ban.filtersystemd [54721]: INFO [postfix-sasl] Jail is in operation
now (process new journal entries)
2024-10-28 12:36:13,072 fail2ban.jail [54721]: INFO Jail 'postfix-sasl' started
2024-10-28 12:36:13,072 fail2ban.jail [54721]: INFO Jail 'sshd-ddos' started
```

Рис. 2.7: Просмотр журнала событий fail2ban

2.2 Проверка работы Fail2ban

На сервере просматриваю статус службы, статус защиты SSH, устанавливаю максимальное количество ошибок для SSH, равное 2:

```
fail2ban-client status
```

```
fail2ban-client status sshd
```

```
fail2ban-client set sshd maxretry 2
```

С клиента пытаюсь подключиться к серверу по SSH и намеренно ввожу неверный пароль (рис. 2.8).

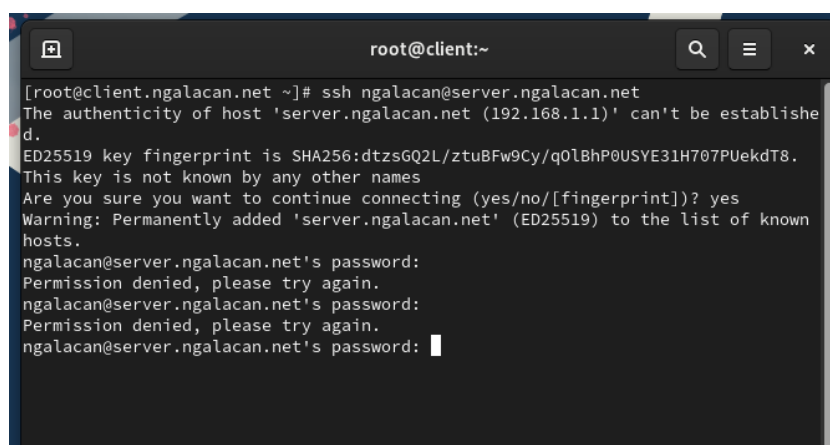


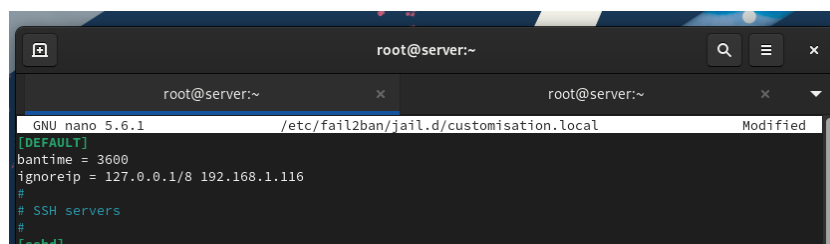
Рис. 2.8: Подключение к серверу по SSH с вводом неправильного пароля

Снова просматриваю статус защиты SSH на сервере и вижу 2 попытки неудачного входа и 1 забаненный IP-адрес. Разблокирую адрес клиента и вновь просматриваю статус. Убеждаюсь, что заблокированных IP нет (рис. 2.9).

```
[root@server.ngalacan.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 1
| |- Total banned: 1
| |- Banned IP list: 192.168.1.116
[root@server.ngalacan.net ~]# fail2ban-client set sshd unbanip 192.168.1.116
1
[root@server.ngalacan.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 0
| |- Total banned: 1
| |- Banned IP list:
[root@server.ngalacan.net ~]#
```

Рис. 2.9: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

Вношу изменения в конфигурационный файл, добавив в раздел по умолчанию игнорирование адреса клиента (рис. 2.10).



```
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.116
#
# SSH servers
#
[sshd]
```

Рис. 2.10: Редактирование файла с локальной конфигурацией: игнорирование адреса клиента

Перезапускаю службу и просматриваю журнал событий (рис. 2.11).

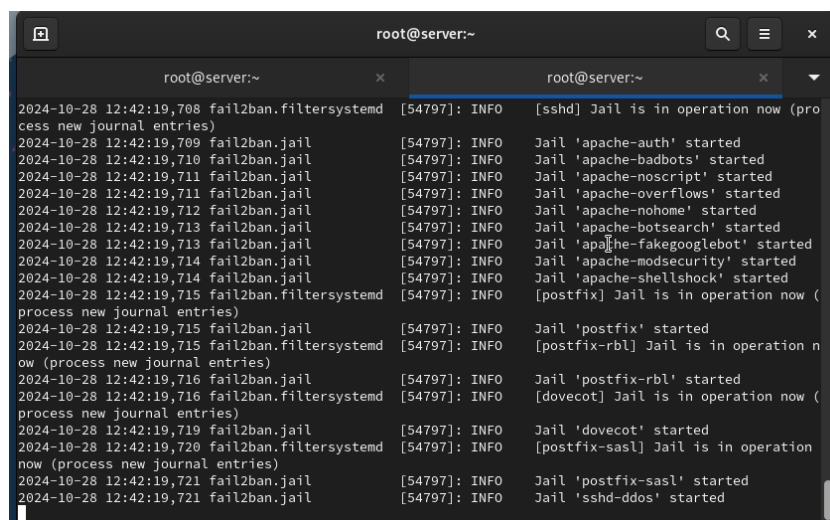


Рис. 2.11: Просмотр журнала событий 'fail2ban'

С клиента вновь пытаюсь аналогичным образом войти на сервер с неправильным паролем. Просматриваю статус защиты SSH и вижу 0 заблокированных адресов, так как адрес клиента находится в списке игнорируемых (рис. 2.12)

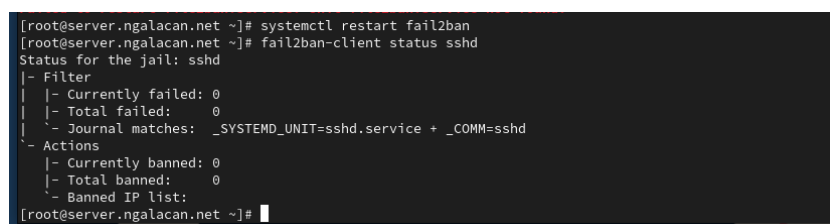


Рис. 2.12: Просмотр статуса защиты SSH после неудачного входа

2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
```

```
mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
```

```
cp -R /etc/fail2ban/jail.d/customisation.local  
  ↪ /vagrant/provision/server/protect/etc/fail2ban/jail.d/
```

Вношу изменения в файл /vagrant/provision/server/protect.sh (рис. 2.13).

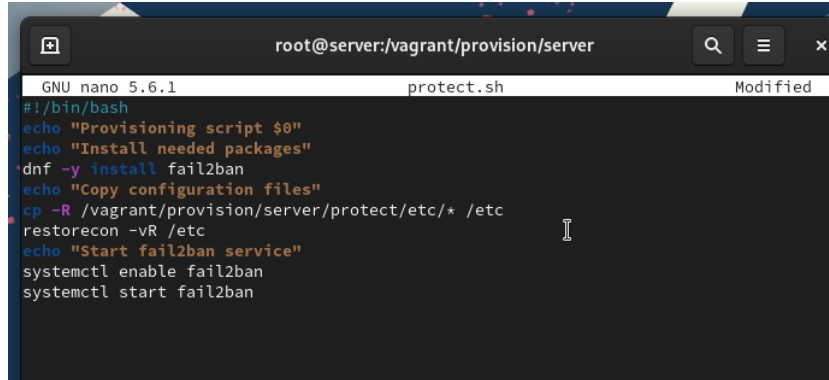


Рис. 2.13: Редактирование protect.sh на сервере

Для отработки созданного скрипта во время загрузки VM server в конфигурационном файле Vagrantfile добавляю запись в соответствующий раздел конфигураций для сервера:

```
server.vm.provision "server protect",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/protect.sh"
```

3 Выводы

В результате выполнения работы были получены навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

4 Ответы на контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban - это программное обеспечение, которое предотвращает атаки на сервер, анализируя лог-файлы и блокируя IP-адреса, с которых идут подозрительные или злонамеренные действия. Он работает следующим образом:

- Мониторит указанные лог-файлы на наличие заданных событий (например, неудачных попыток входа).
- Когда число попыток превышает определенный порог, Fail2ban временно блокирует IP-адрес, добавляя правила в фаервол.
- Заблокированный IP-адрес может быть разблокирован автоматически после определенного периода времени

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

Настройки файла `jail.local` более приоритетны, чем настройки файла `jail.conf`.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Чтобы настроить оповещение администратора при срабатывании Fail2ban, необходимо настроить отправку уведомлений по электронной почте или другим способом. Это можно сделать, изменяя настройки в файле `jail.local`, добавляя адрес электронной почты администратора и настройки SMTP-сервера.

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

Примеры настроек по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к веб-службе:

- `[apache]` - секция, относящаяся к веб-серверу Apache.
- `enabled = true` - включение проверки лог-файлов Apache.
- `port = http,https` - указание портов для мониторинга.
- `filter = apache-auth` - указание фильтра для обработки лог-файлов.
- `logpath = /var/log/apache*/error.log` - путь к лог-файлам Apache.
- `maxretry = 5` - максимальное количество попыток до блокировки адреса.
- `bantime = 600` - продолжительность блокировки в секундах.

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

Примеры настроек по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе:

- `[postfix]` - секция, относящаяся к почтовому серверу Postfix.
- `enabled = true` - включение проверки лог-файлов Postfix.
- `port = smtp,ssmtp` - указание портов для мониторинга.
- `filter = postfix` - указание фильтра для обработки лог-файлов.
- `logpath = /var/log/mail.log` - путь к лог-файлам Postfix.
- `maxretry = 3` - максимальное количество попыток до блокировки адреса.
- `bantime = 3600` - продолжительность блокировки в секундах.

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

Fail2ban может выполнять различные действия при обнаружении атакующего IP-адреса, такие как блокировка адреса через файрвол, добавление правил в IP-таблицы, отправка уведомлений администратору и другие. Описание доступных действий можно найти в документации или руководстве Fail2ban.

7. Как получить список действующих правил Fail2ban?

Можно использовать команду: `fail2ban-client status`.

8. Как получить статистику заблокированных Fail2ban адресов?

Можно использовать команду `fail2ban-client status <jail-name>`, где `<jail-name>` - имя конкретного jail, например, "ssh" или "apache".

9. Как разблокировать IP-адрес?

`fail2ban-client set sshd unbanip <ip-адрес клиента>`