

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ  
ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 16**

*Дисциплина «Администрирование сетевых подсистем»*

*Тема «Базовая защита от атак типа “brute force”»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

## Цель работы

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

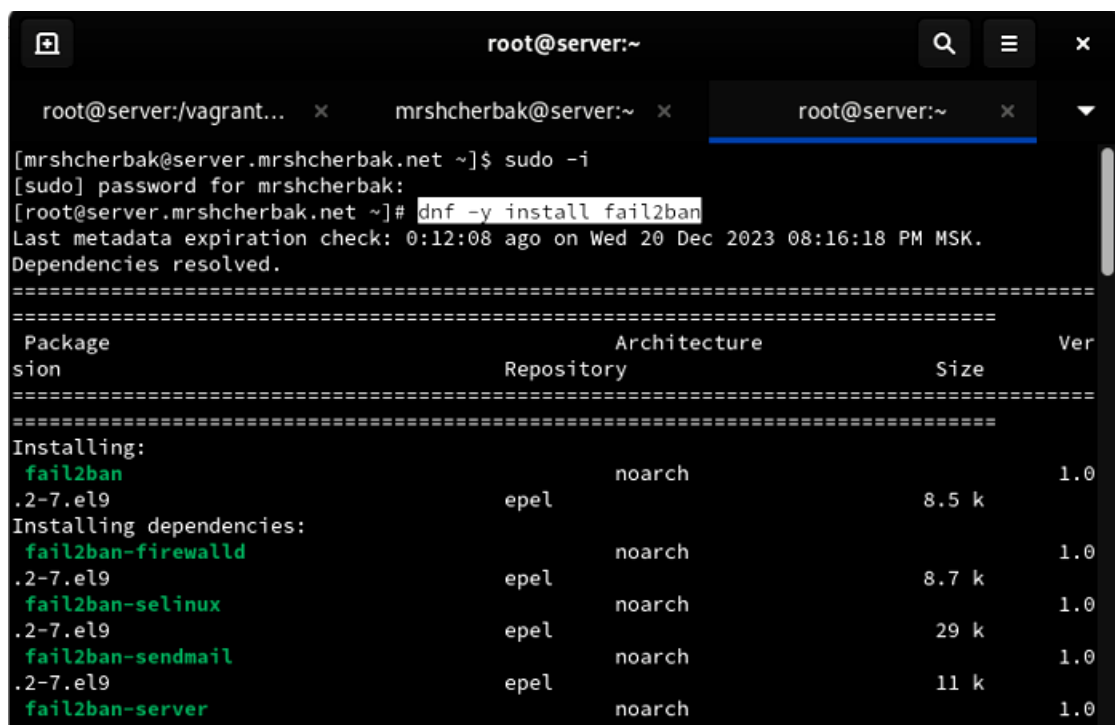
## Задание

1. Установить и настроить Fail2ban для отслеживания работы установленных на сервере служб.
2. Проверить работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
3. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban.

## Выполнение

### 1. Защита с помощью Fail2ban

1. На сервере установила fail2ban (рис.1.1).



```
root@server:~  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# dnf -y install fail2ban  
Last metadata expiration check: 0:12:08 ago on Wed 20 Dec 2023 08:16:18 PM MSK.  
Dependencies resolved.  
=====
```

| Package            | Repository | Architecture | Size  | Version |
|--------------------|------------|--------------|-------|---------|
| fail2ban           | epel       | noarch       | 8.5 k | 1.0     |
| fail2ban-firewalld | epel       | noarch       | 8.7 k | 1.0     |
| fail2ban-selinux   | epel       | noarch       | 29 k  | 1.0     |
| fail2ban-sendmail  | epel       | noarch       | 11 k  | 1.0     |
| fail2ban-server    | epel       | noarch       | 443 k | 1.0     |

```
Installing:  
fail2ban  
Installing dependencies:  
fail2ban-firewalld  
fail2ban-selinux  
fail2ban-sendmail  
fail2ban-server
```

Рис.1.1. Установка fail2ban

2. Запустила сервер fail2ban и в дополнительном терминале запустила просмотр журнала событий fail2ban. Создала файл с локальной конфигурацией fail2ban и в

нем задала время блокирования на 1 час (время задаётся в секундах) и включила защиту SSH. После чего перезапустила fail2ban с помощью команды `systemctl restart fail2ban` и просмотрела журнал событий. Действия представлены на рис.1.2 – рис.1.4.

```
[root@server.mrshcherbak.net ~]# systemctl start fail2ban
[root@server.mrshcherbak.net ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[root@server.mrshcherbak.net ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@server.mrshcherbak.net ~]# mc
```

Рис.1.2. Выполнение команд

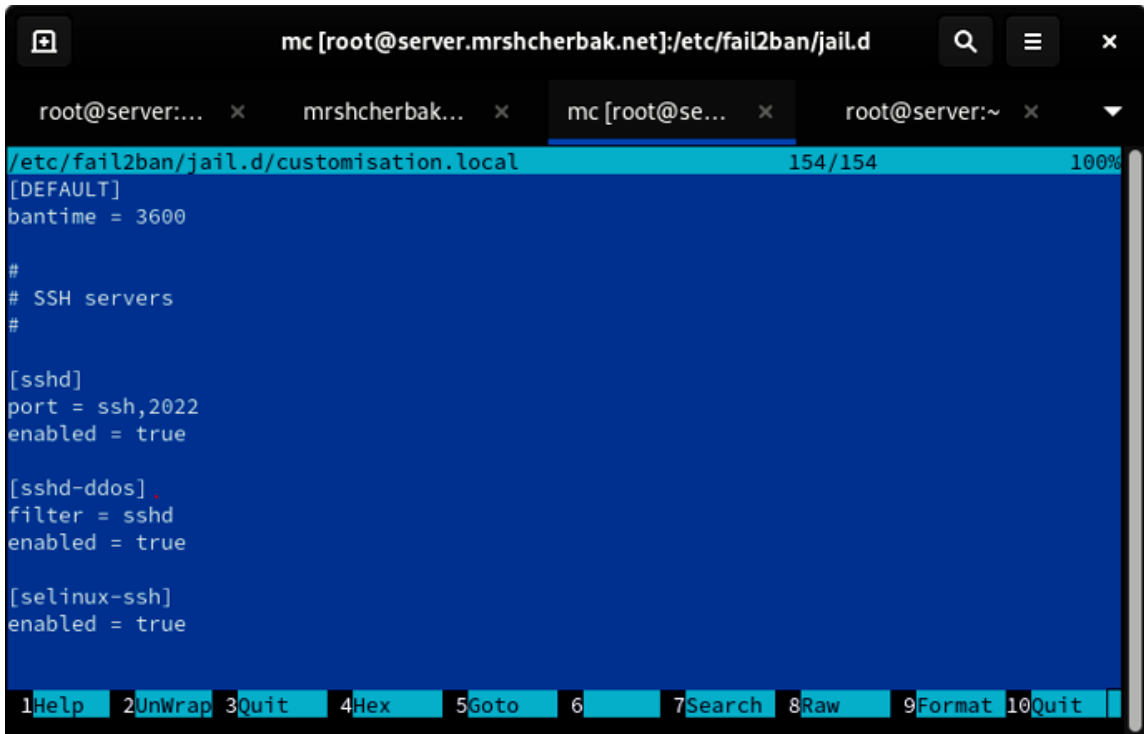


Рис.1.3. Содержимое файла с локальной конфигурацией fail2ban

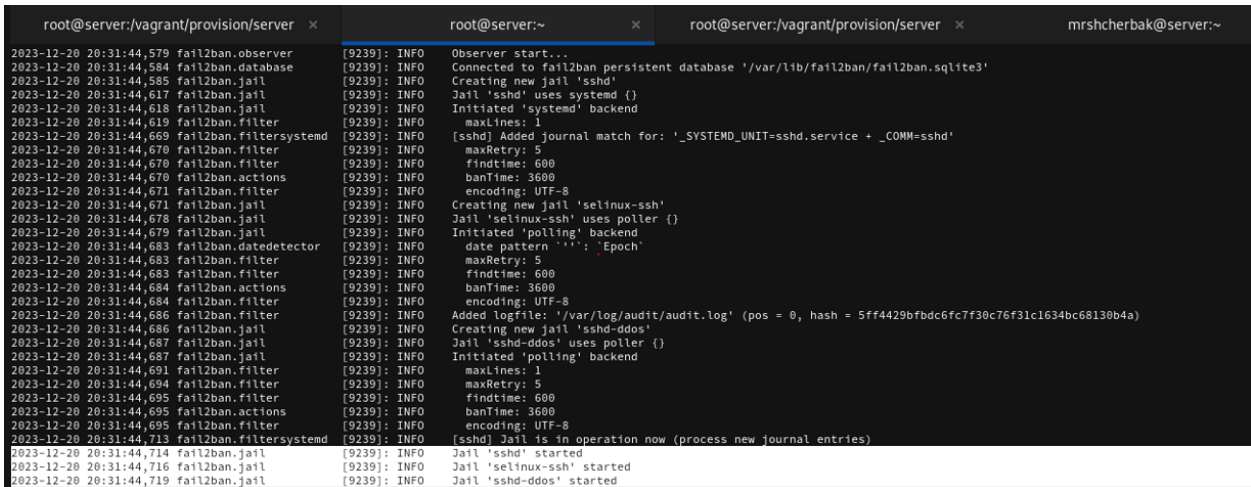
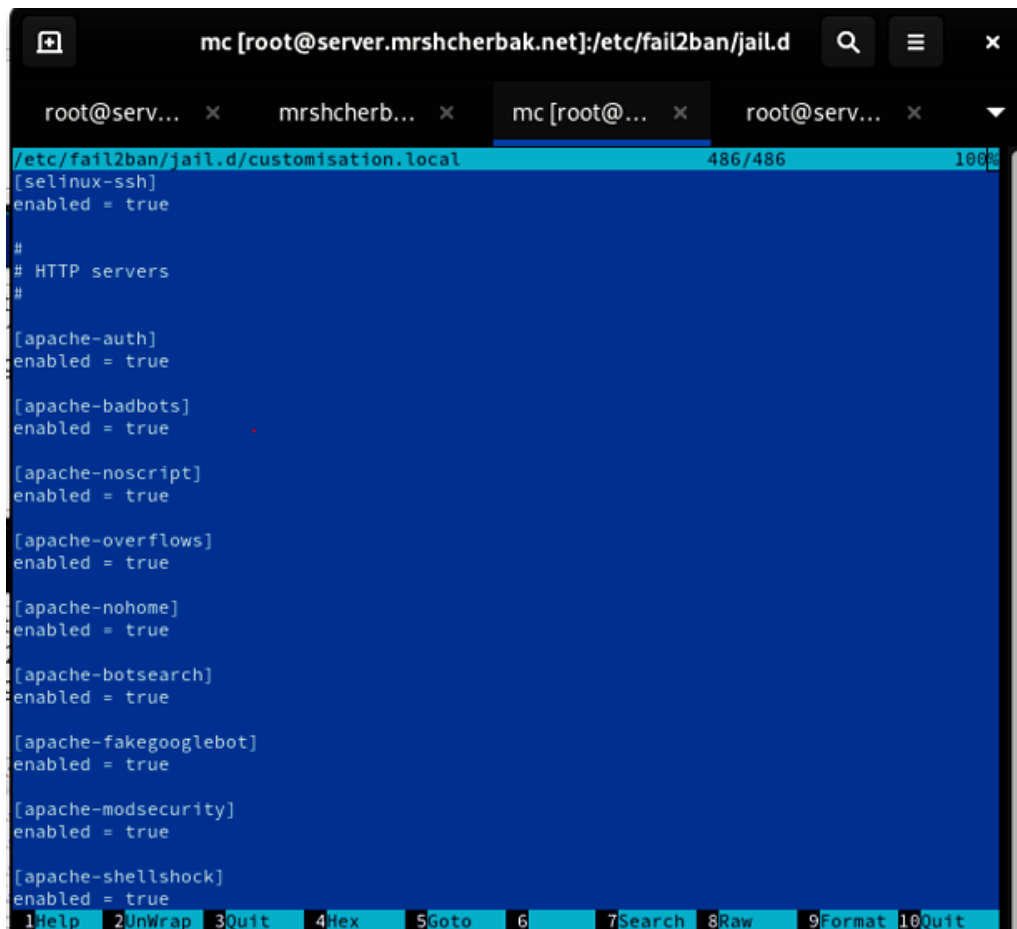


Рис.1.4. Просмотр журнала событий

3. В файле /etc/fail2ban/jail.d/customisation.local включила защиту HTTP (рис.1.5).



```
mc [root@server.mrshcherbak.net]:/etc/fail2ban/jail.d
/etc/fail2ban/jail.d/customisation.local 486/486 100%
[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

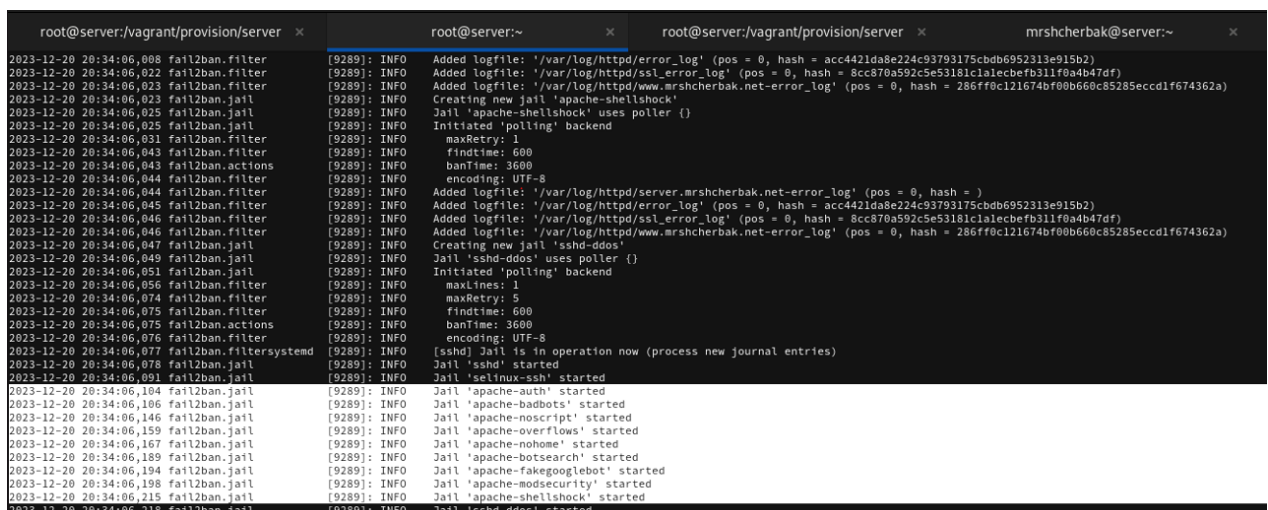
[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

Рис.1.5. Содержимое файла с локальной конфигурацией fail2ban

4. Перезапустила fail2ban и посмотрела журнал событий (рис.1.6).



```
root@server:/vagrant/provision/server x root@server:~ x root@server:/vagrant/provision/server x mrshcherbak@server:~ x
2023-12-20 20:34:06,008 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = acc4421da8e224c93793175cbdb6952313e915b2)
2023-12-20 20:34:06,022 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 8cc870a592c5e53181c1a1ecbefb311f0a4b47df)
2023-12-20 20:34:06,023 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/www.mrshcherbak.net-error_log' (pos = 0, hash = 286ff0c121674bf0b660c85285eccd1f674362a)
2023-12-20 20:34:06,025 fail2ban.jail [9289]: INFO Creating new jail 'apache-shellshock'
2023-12-20 20:34:06,025 fail2ban.jail [9289]: INFO Jail 'apache-shellshock' uses poller {}
2023-12-20 20:34:06,031 fail2ban.filter [9289]: INFO Initiated 'polling' backend
2023-12-20 20:34:06,031 fail2ban.filter [9289]: INFO maxRetry: 1
2023-12-20 20:34:06,043 fail2ban.filter [9289]: INFO findTime: 600
2023-12-20 20:34:06,043 fail2ban.actions [9289]: INFO banTime: 3600
2023-12-20 20:34:06,044 fail2ban.filter [9289]: INFO encoding: UTF-8
2023-12-20 20:34:06,044 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/server.mrshcherbak.net-error_log' (pos = 0, hash = )
2023-12-20 20:34:06,045 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = acc4421da8e224c93793175cbdb6952313e915b2)
2023-12-20 20:34:06,046 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 8cc870a592c5e53181c1a1ecbefb311f0a4b47df)
2023-12-20 20:34:06,046 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/www.mrshcherbak.net-error_log' (pos = 0, hash = 286ff0c121674bf0b660c85285eccd1f674362a)
2023-12-20 20:34:06,047 fail2ban.jail [9289]: INFO Creating new jail 'sshd-ddos'
2023-12-20 20:34:06,049 fail2ban.jail [9289]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-20 20:34:06,051 fail2ban.jail [9289]: INFO Initiated 'polling' backend
2023-12-20 20:34:06,056 fail2ban.filter [9289]: INFO maxLines: 1
2023-12-20 20:34:06,074 fail2ban.filter [9289]: INFO maxRetry: 5
2023-12-20 20:34:06,075 fail2ban.filter [9289]: INFO findTime: 600
2023-12-20 20:34:06,075 fail2ban.actions [9289]: INFO banTime: 3600
2023-12-20 20:34:06,076 fail2ban.filter [9289]: INFO encoding: UTF-8
2023-12-20 20:34:06,077 fail2ban.filtersystemd [9289]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-12-20 20:34:06,078 fail2ban.jail [9289]: INFO Jail 'sshd' started
2023-12-20 20:34:06,091 fail2ban.jail [9289]: INFO Jail 'selinux-ssh' started
2023-12-20 20:34:06,104 fail2ban.jail [9289]: INFO Jail 'apache-auth' started
2023-12-20 20:34:06,106 fail2ban.jail [9289]: INFO Jail 'apache-badbots' started
2023-12-20 20:34:06,146 fail2ban.jail [9289]: INFO Jail 'apache-noscript' started
2023-12-20 20:34:06,159 fail2ban.jail [9289]: INFO Jail 'apache-overflows' started
2023-12-20 20:34:06,167 fail2ban.jail [9289]: INFO Jail 'apache-nohome' started
2023-12-20 20:34:06,189 fail2ban.jail [9289]: INFO Jail 'apache-botsearch' started
2023-12-20 20:34:06,194 fail2ban.jail [9289]: INFO Jail 'apache-fakegooglebot' started
2023-12-20 20:34:06,198 fail2ban.jail [9289]: INFO Jail 'apache-modsecurity' started
2023-12-20 20:34:06,215 fail2ban.jail [9289]: INFO Jail 'apache-shellshock' started
2023-12-20 20:34:06,218 fail2ban.jail [9289]: INFO Jail 'sshd-ddos' started
```

Рис.1.6. Просмотр журнала событий

5. В файле /etc/fail2ban/jail.d/customisation.local включила защиту почты (рис.1.7).

```
customis~n.local  [----]  0 L:[ 43+22  65/ 65] *(619 / 619b) <EOF>  [*][X]

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true

#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true

```

Рис.1.7. Содержимое файла с локальной конфигурацией fail2ban

6. Перезапустила fail2ban и посмотрела журнал событий (рис.1.8).

```
root@server:/vagrant/provision/server x root@server:~ x root@server:/vagrant/provision/server x

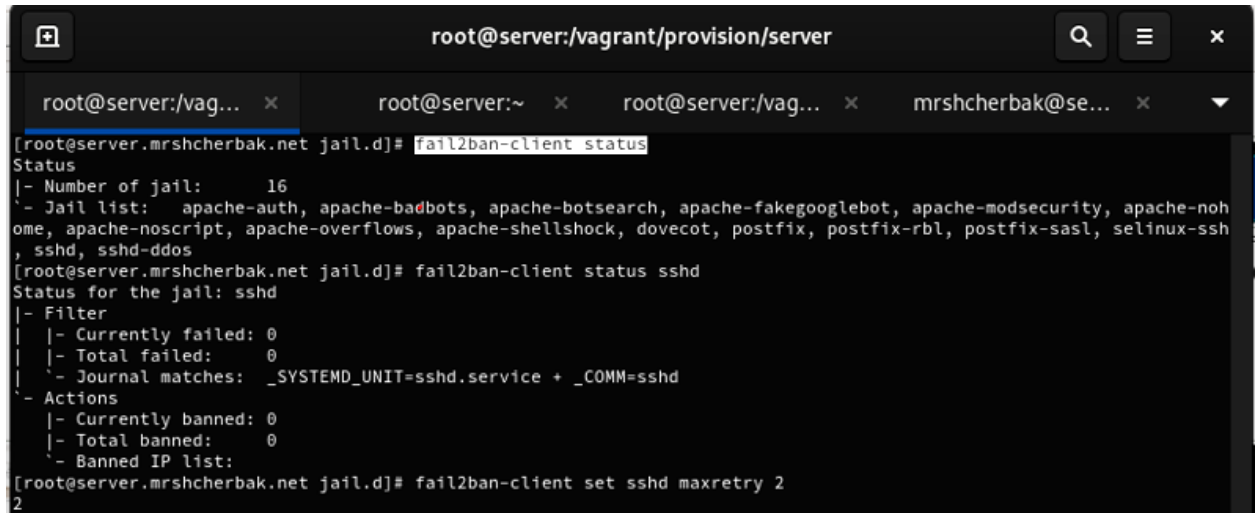
2023-12-20 20:35:45,536 fail2ban.filtersystemd [9356]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2023-12-20 20:35:45,541 fail2ban.filter [9356]: INFO maxRetry: 5
2023-12-20 20:35:45,542 fail2ban.filter [9356]: INFO findtime: 600
2023-12-20 20:35:45,542 fail2ban.actions [9356]: INFO banTime: 3600
2023-12-20 20:35:45,543 fail2ban.filter [9356]: INFO encoding: UTF-8
2023-12-20 20:35:45,543 fail2ban.jail [9356]: INFO Creating new jail 'sshd-ddos'
2023-12-20 20:35:45,545 fail2ban.jail [9356]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-20 20:35:45,546 fail2ban.jail [9356]: INFO Initiated 'polling' backend
2023-12-20 20:35:45,552 fail2ban.filter [9356]: INFO maxLines: 1
2023-12-20 20:35:45,568 fail2ban.filter [9356]: INFO maxRetry: 5
2023-12-20 20:35:45,569 fail2ban.filter [9356]: INFO findtime: 600
2023-12-20 20:35:45,569 fail2ban.actions [9356]: INFO banTime: 3600
2023-12-20 20:35:45,569 fail2ban.filter [9356]: INFO encoding: UTF-8
2023-12-20 20:35:45,570 fail2ban.filtersystemd [9356]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,571 fail2ban.jail [9356]: INFO Jail 'sshd' started
2023-12-20 20:35:45,573 fail2ban.jail [9356]: INFO Jail 'selinux-ssh' started
2023-12-20 20:35:45,577 fail2ban.jail [9356]: INFO Jail 'apache-auth' started
2023-12-20 20:35:45,581 fail2ban.jail [9356]: INFO Jail 'apache-badbots' started
2023-12-20 20:35:45,583 fail2ban.jail [9356]: INFO Jail 'apache-noscript' started
2023-12-20 20:35:45,586 fail2ban.jail [9356]: INFO Jail 'apache-overflows' started
2023-12-20 20:35:45,587 fail2ban.jail [9356]: INFO Jail 'apache-nohome' started
2023-12-20 20:35:45,588 fail2ban.jail [9356]: INFO Jail 'apache-botsearch' started
2023-12-20 20:35:45,589 fail2ban.jail [9356]: INFO Jail 'apache-fakegooglebot' started
2023-12-20 20:35:45,597 fail2ban.jail [9356]: INFO Jail 'apache-modsecurity' started
2023-12-20 20:35:45,602 fail2ban.jail [9356]: INFO Jail 'apache-shellshock' started
2023-12-20 20:35:45,605 fail2ban.jail [9356]: INFO Jail 'postfix-sasl' started
2023-12-20 20:35:45,618 fail2ban.filtersystemd [9356]: INFO [postfix] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,619 fail2ban.filtersystemd [9356]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,620 fail2ban.jail [9356]: INFO Jail 'postfix-rbl' started
2023-12-20 20:35:45,627 fail2ban.jail [9356]: INFO Jail 'dovecot' started
2023-12-20 20:35:45,636 fail2ban.filtersystemd [9356]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,637 fail2ban.filtersystemd [9356]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,638 fail2ban.jail [9356]: INFO Jail 'postfix-sasl' started
2023-12-20 20:35:45,638 fail2ban.jail [9356]: INFO Jail 'sshd-ddos' started

```

Рис.1.8. Просмотр журнала событий

## 2. Проверка работы Fail2ban

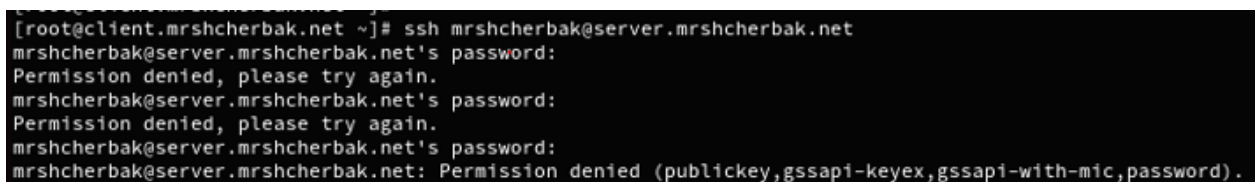
1. На сервере посмотрела статус fail2ban и статус защиты SSH в fail2ban, также установила максимальное количество ошибок для SSH, равное 2. Действия представлены на рис.2.1.



```
root@server:/vagrant/provision/server
root@server:/vagrant/provision/server
root@server:/vagrant/provision/server
mrshcherbak@se...
[root@server.mrshcherbak.net jail.d]# fail2ban-client status
Status
|- Number of jail:      16
|- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-noh
ome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh
, sshd, sshd-ddos
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 0
  |- Total banned:    0
  `-- Banned IP list:
[root@server.mrshcherbak.net jail.d]# fail2ban-client set sshd maxretry 2
2
```

Рис.2.1. Выполнение команд

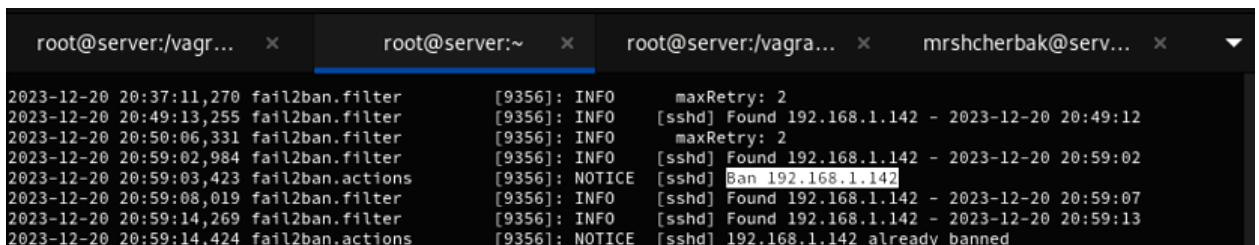
2. С клиента попыталась зайти по SSH на сервер с неправильным паролем (рис.2.2).



```
[root@client.mrshcherbak.net ~]# ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
mrshcherbak@server.mrshcherbak.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

Рис.2.2. Попытка входа с клиента по SSH на сервер с неправильным паролем

3. На сервере посмотрела статус защиты SSH и убедилась, что произошла блокировка адреса клиента (рис.2.3 – рис.2.4).



```
root@server:/vagr...
root@server:/vagr...
root@server:/vagr...
mrshcherbak@serv...
2023-12-20 20:37:11,270 fail2ban.filter [9356]: INFO maxRetry: 2
2023-12-20 20:49:13,255 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:49:12
2023-12-20 20:50:06,331 fail2ban.filter [9356]: INFO maxRetry: 2
2023-12-20 20:59:02,984 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:02
2023-12-20 20:59:03,423 fail2ban.actions [9356]: NOTICE [sshd] Ban 192.168.1.142
2023-12-20 20:59:08,019 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:07
2023-12-20 20:59:14,269 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:13
2023-12-20 20:59:14,424 fail2ban.actions [9356]: NOTICE [sshd] 192.168.1.142 already banned
```

Рис.2.3. Просмотр журнала событий

Разблокировала IP-адрес клиента и вновь посмотрела статус защиты SSH (рис.2.4). Убедилась, что блокировка клиента снята.

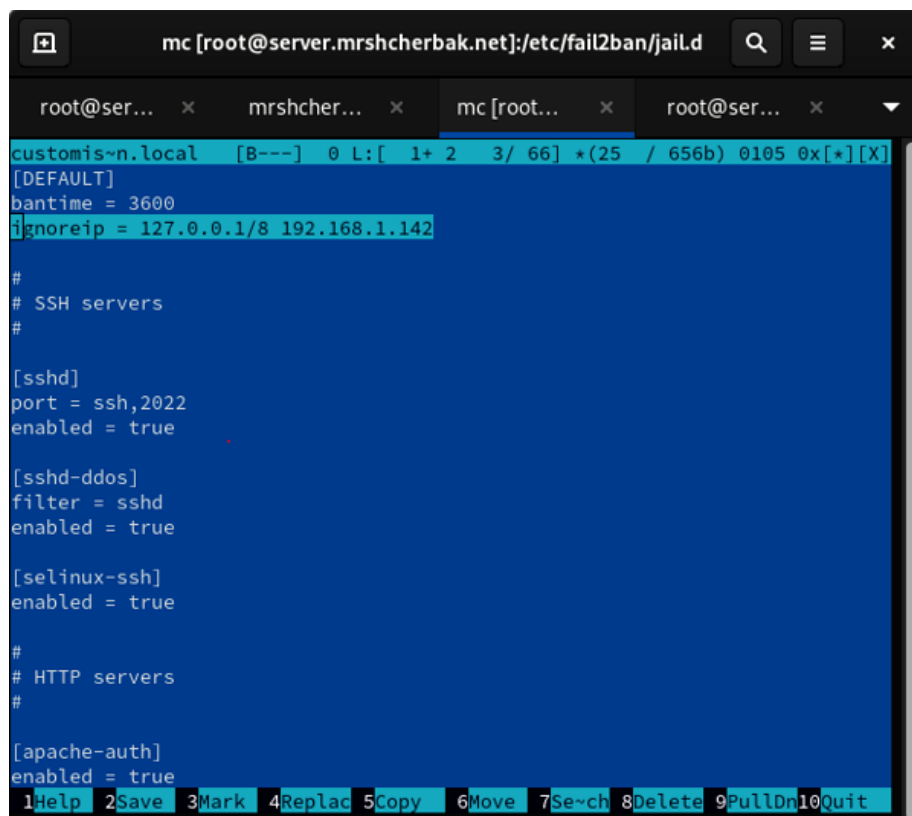
```

[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed: 4
|   '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
    |- Currently banned: 1
    |- Total banned: 1
    '- Banned IP list: 192.168.1.142
[root@server.mrshcherbak.net jail.d]# fail2ban-client set sshd unbanip 192.168.1.142
1
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed: 4
|   '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
    |- Currently banned: 0
    |- Total banned: 1
    '- Banned IP list:

```

Рис.2.4. Просмотр статуса защиты SSH

4. На сервере внесла изменение в файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента (рис.2.5).



```

mc [root@server.mrshcherbak.net]:/etc/fail2ban/jail.d
root@ser... x mrshcher... x mc [root... x root@ser... x
customis~n.local [B---] 0 L: [ 1+ 2 3/ 66] *(25 / 656b) 0105 0x[*][X]
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.142
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
#
# HTTP servers
#
[apache-auth]
enabled = true
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Se~ch 8Delete 9PullDn10Quit

```

Рис.2.5. Содержимое файла `/etc/fail2ban/jail.d/customisation.local`

5. Перезапустила fail2ban и посмотрела журнал событий (рис.2.6).



```
root@server:/vagr... x root@server:~ x root@server:/vagr... x mrshcherbak@ser... x
2023-12-20 21:03:41,588 fail2ban.jail [9912]: INFO Initiated 'polling' backend
2023-12-20 21:03:41,592 fail2ban.filter [9912]: INFO maxLines: 1
2023-12-20 21:03:41,601 fail2ban.filter [9912]: INFO maxRetry: 5
2023-12-20 21:03:41,606 fail2ban.filter [9912]: INFO findTime: 600
2023-12-20 21:03:41,607 fail2ban.actions [9912]: INFO banTime: 3600
2023-12-20 21:03:41,607 fail2ban.filter [9912]: INFO encoding: UTF-8
2023-12-20 21:03:41,609 fail2ban.filtersystemd [9912]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,612 fail2ban.jail [9912]: INFO Jail 'sshd' started
2023-12-20 21:03:41,632 fail2ban.jail [9912]: INFO Jail 'selinux-ssh' started
2023-12-20 21:03:41,635 fail2ban.jail [9912]: INFO Jail 'apache-auth' started
2023-12-20 21:03:41,637 fail2ban.jail [9912]: INFO Jail 'apache-badbots' started
2023-12-20 21:03:41,648 fail2ban.jail [9912]: INFO Jail 'apache-noscript' started
2023-12-20 21:03:41,663 fail2ban.jail [9912]: INFO Jail 'apache-overflows' started
2023-12-20 21:03:41,665 fail2ban.jail [9912]: INFO Jail 'apache-nohome' started
2023-12-20 21:03:41,667 fail2ban.jail [9912]: INFO Jail 'apache-botsearch' started
2023-12-20 21:03:41,669 fail2ban.jail [9912]: INFO Jail 'apache-fakegooglebot' started
2023-12-20 21:03:41,678 fail2ban.jail [9912]: INFO Jail 'apache-modsecurity' started
2023-12-20 21:03:41,683 fail2ban.jail [9912]: INFO Jail 'apache-shellshock' started
2023-12-20 21:03:41,684 fail2ban.filtersystemd [9912]: INFO [postfix] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,686 fail2ban.jail [9912]: INFO Jail 'postfix' started
2023-12-20 21:03:41,687 fail2ban.filtersystemd [9912]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,688 fail2ban.jail [9912]: INFO Jail 'postfix-rbl' started
2023-12-20 21:03:41,689 fail2ban.filtersystemd [9912]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,691 fail2ban.jail [9912]: INFO Jail 'dovecot' started
2023-12-20 21:03:41,692 fail2ban.filtersystemd [9912]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,693 fail2ban.jail [9912]: INFO Jail 'postfix-sasl' started
2023-12-20 21:03:41,694 fail2ban.jail [9912]: INFO Jail 'sshd-ddos' started
2023-12-20 21:04:49,039 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
2023-12-20 21:04:53,769 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
2023-12-20 21:04:56,769 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
```

Рис.2.6. Просмотр журнала событий

6. Вновь попыталась войти с клиента на сервер с неправильным паролем и посмотрела статус защиты SSH (рисс.2.7 – рис.2.8).

```
[root@client.mrshcherbak.net ~]# ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
mrshcherbak@server.mrshcherbak.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.mrshcherbak.net ~]# ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Wed Dec 20 21:04:56 MSK 2023 from 192.168.1.142 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Wed Dec 20 21:01:47 2023 from 192.168.1.142
[mrshcherbak@server.mrshcherbak.net ~]$
```

Рис.2.7. Выполнение команд

```
[root@server.mrshcherbak.net jail.d]# systemctl restart fail2ban
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
-- Actions
| |- Currently banned: 0
| |- Total banned: 0
| `-- Banned IP list:
```

Рис.2.8. Просмотр статуса защиты SSH



### 3. Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создала в нём каталог `protect`, в который поместила в соответствующие подкаталоги конфигурационные файлы и в каталоге `/vagrant/provision/server` создала исполняемый файл `protect.sh`, в котором прописала скрипт (рис.3.2). Действия представлены на рис.3.1.

```
[root@server.mrshcherbak.net jail.d]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.mrshcherbak.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.mrshcherbak.net server]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# touch protect.sh
[root@server.mrshcherbak.net server]# chmod +x protect.sh
[root@server.mrshcherbak.net server]# mc
```

Рис.3.1. Выполнение команд

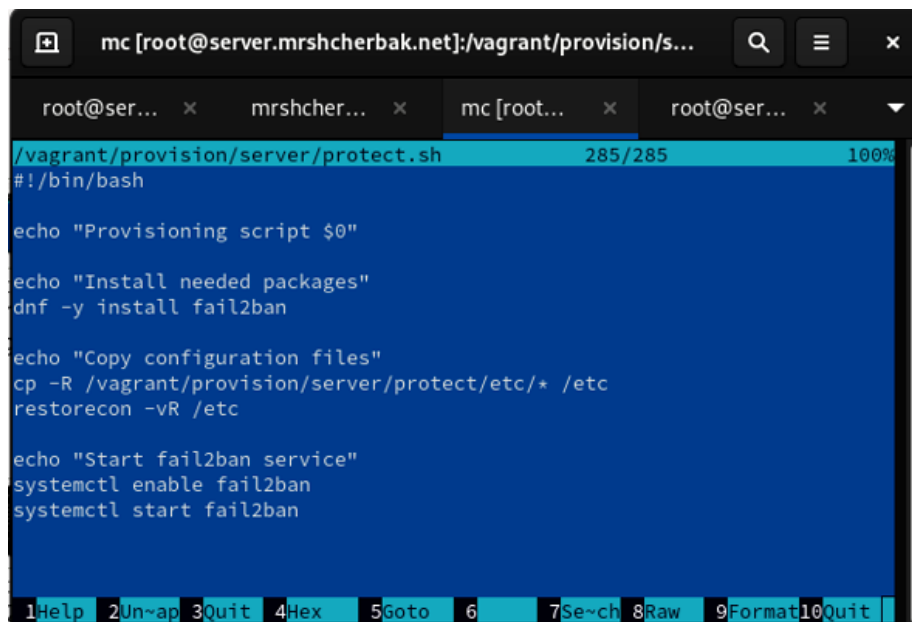
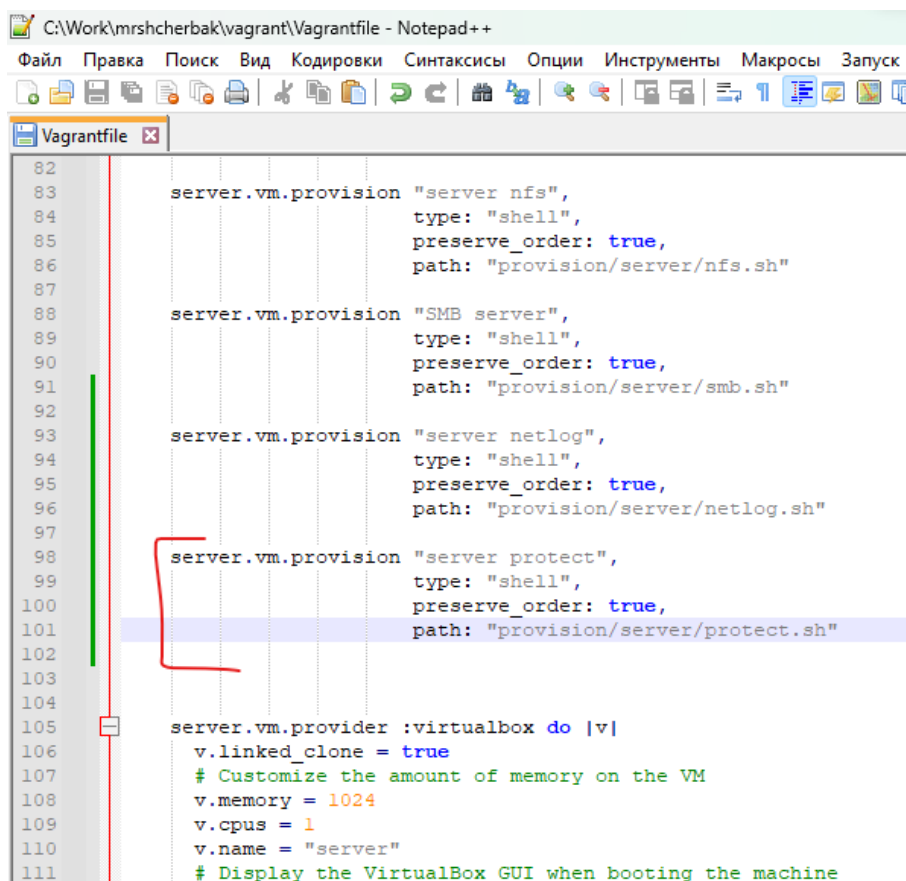


Рис.3.2. Содержимое файла `protect.sh`

2. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле `Vagrantfile` добавила в соответствующем разделе конфигураций для сервера запись (рис.3.3).



```
82
83     server.vm.provision "server nfs",
84                         type: "shell",
85                         preserve_order: true,
86                         path: "provision/server/nfs.sh"
87
88     server.vm.provision "SMB server",
89                         type: "shell",
90                         preserve_order: true,
91                         path: "provision/server/smb.sh"
92
93     server.vm.provision "server netlog",
94                         type: "shell",
95                         preserve_order: true,
96                         path: "provision/server/netlog.sh"
97
98     server.vm.provision "server protect",
99                         type: "shell",
100                        preserve_order: true,
101                        path: "provision/server/protect.sh"
102
103
104
105     server.vm.provider :virtualbox do |v|
106         v.linked_clone = true
107         # Customize the amount of memory on the VM
108         v.memory = 1024
109         v.cpus = 1
110         v.name = "server"
111         # Display the VirtualBox GUI when booting the machine
```

Рис.3.3. Содержимое файла Vagrantfile

**Вывод:** таким образом, в ходе выполнения л/р №16 я получила навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

### Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Принцип работы Fail2ban заключается в отслеживании сетевой активности на портах узла через анализ текстовых лог-файлов. При обнаружении неадекватной активности, например, brute force атаки, программа помещает IP-адрес атакующего в черный список, блокируя все пакеты с этого адреса. Блокировка осуществляется путем изменения правил межсетевого экрана.

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

Настройки файла jail.local более приоритетны, так как они переопределяют соответствующие настройки из jail.conf. Jail.conf может обновляться и перезаписываться, то есть настройки могут не сохраниться. А конфигурационный файл jail.local имеет высший приоритет перед jail.conf,

соответственно настройки в первую очередь будут применяться из данного файла.

### 3. Как настроить оповещение администратора при срабатывании Fail2ban?

Для настройки оповещений администратора при срабатывании Fail2ban, можно использовать некоторые параметры из секции [DEFAULT] в конфигурационных файлах.

`destemail` — параметр, задающий адрес эл.почты. Значение по умолчанию `root@localhost`;

`mta` — определяет почтовый агент, который будет использоваться для доставки почты. Если настроен Sendmail, оставить значение по умолчанию. Если же письма нужно доставлять на локальную машину поменять значение на `mail`.

`destemail` = ваш\_адрес\_электронной\_почты

`mta` = sendmail/mail

`action` = %(action\_mwl)s

Для локальной почты нужно заменить строчку `action_mw` на `action_mwl`. Это добавит лог к оповещению, чтобы было легче отслеживать события.

Перезапустить Fail2ban: `sudo service fail2ban restart`.

Теперь, когда Fail2ban обнаруживает неудачные попытки входа, администратор будет оповещен по электронной почте.

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

`[apache-auth]` — определяет неудачные попытки ввода пароля.

`[apache-badbots]` — определяет ботов, которые ищут email адреса

`[apache-noscript]` — блокирует доступ к определенным скриптам

`[apache-overflows]` — предотвращает попытки переполнения Apache

`[apache-nohome]` — блокирует неудачные попытки поиска домашней директории

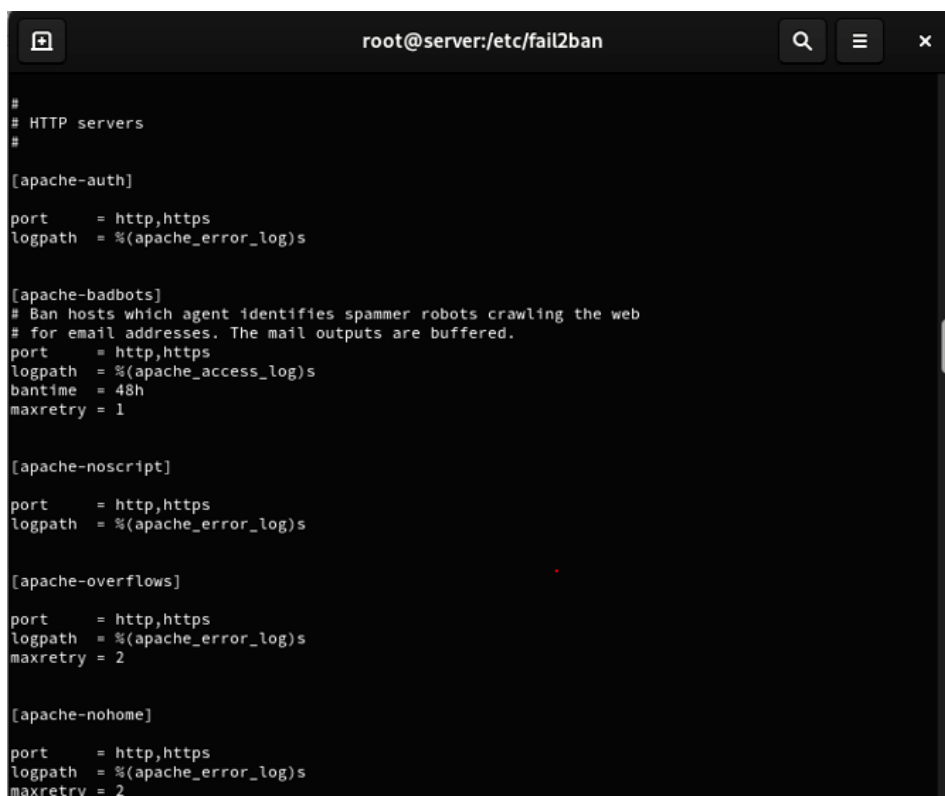
`[apache-botsearch]` — определяет ботов, которые перебором ищут популярные скрипты.

В строке `port` указываются порты, на которых слушает веб-служба Apache (HTTP и HTTPS).

В строке `logpath` указывается путь к лог-файлу ошибок Apache, который Fail2ban будет мониторить.

В строке `maxretry` указывается количество попыток, после которого IP-адрес будет заблокирован.

В строке `bantime` указывается время в секундах, на которое нарушитель будет заблокирован.



```
#
# HTTP servers
#

[apache-auth]
port      = http,https
logpath   = %(apache_error_log)s

[apache-badbots]
# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.
port      = http,https
logpath   = %(apache_access_log)s
bantime   = 48h
maxretry  = 1

[apache-noscript]
port      = http,https
logpath   = %(apache_error_log)s

[apache-overflows]
port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2

[apache-nohome]
port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2
```

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

В строке `filter` указывается используемый фильтр, который указывает Fail2ban анализировать логи в режиме аутентификации (`auth`), либо в режиме RBL (Real-time Blackhole List).

В строке `port` указываются порты, которые Fail2ban будет мониторить для данной службы.

В строке `logpath` указывается путь к логам, который Fail2ban анализирует.

В строке `backend` указывается используемый backend для анализа логов.

В строке `mode` указывается режим работы Fail2ban для данной службы.

В строке `maxretry` указывается количество попыток, после которого IP-адрес будет заблокирован.

Эти настройки определяют, как Fail2ban будет реагировать на подозрительную активность в логах почтовых служб Postfix и Dovecot.

```

root@server:/etc/fail2ban

#
# Mail servers
#

# ASSP SMTP Proxy Jail
[assp]

port      = smtp,465,submission
logpath   = /root/path/to/assp/logs/maillog.txt

[courier-smtp]

port      = smtp,465,submission
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s

[postfix]
# To use another modes set filter parameter "mode" in jail.local:
mode      = more
port      = smtp,465,submission
logpath   = %(postfix_log)s
backend   = %(postfix_backend)s

[postfix-rbl]

filter     = postfix[mode=rbl]
port      = smtp,465,submission
logpath    = %(postfix_log)s
backend    = %(postfix_backend)s
maxretry   = 1

[sendmail-auth]

```

```

root@server:/etc/fail2ban

logpath    = %(syslog_mail)s
backend    = %(syslog_backend)s

[qmail-rbl]

filter     = qmail
port      = smtp,465,submission
logpath    = /service/qmail/log/main/current

# dovecot defaults to logging to the mail syslog facility
# but can be set by syslog_facility in the dovecot configuration.
[dovecot]

port      = pop3,pop3s,imap,imaps,submission,465,sieve
logpath   = %(dovecot_log)s
backend   = %(dovecot_backend)s

[sieve]

port      = smtp,465,submission
logpath   = %(dovecot_log)s
backend   = %(dovecot_backend)s

```

```

root@server:/etc/fail2ban

#

[courier-auth]

port      = smtp,465,submission,imap,imaps,pop3,pop3s
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s

[postfix-sasl]

filter     = postfix[mode=auth]
port      = smtp,465,submission,imap,imaps,pop3,pop3s
# You might consider monitoring /var/log/mail.warn instead if you are
# running postfix since it would provide the same log lines at the
# "warn" level but overall at the smaller filesize.
logpath    = %(postfix_log)s
backend    = %(postfix_backend)s

[perdition]

port      = imap,imaps,pop3,pop3s
logpath    = %(syslog_mail)s
backend    = %(syslog_backend)s

```

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

Fail2ban при обнаружении атакующего IP-адреса может выполнять различные действия, в зависимости от конфигурации. Некоторые из базовых действий включают в себя блокировку IP-адреса на определенное время (bantime), игнорирование определенных IP-адресов (ignoreip), отправку уведомлений администратору и так далее.

Описания этих действий обычно содержатся в конфигурационных файлах Fail2ban, таких как jail.conf или jail.local. В этих файлах можно найти секции, посвященные определенным Jail'ам (группам правил), и внутри этих секций будут указаны параметры, связанные с действиями.

7. Как получить список действующих правил Fail2ban?

Для получения списка действующих правил Fail2ban можно воспользоваться командой: fail2ban-client status. В настоящий момент активны 16 правил Fail2ban.

```
[root@server.mrshcherbak.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`-- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegoogl
    ebot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apa
    che-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd,
    sshd-ddos
[root@server.mrshcherbak.net ~]#
```

8. Как получить статистику заблокированных Fail2ban адресов?

Для получения статистики заблокированных адресов можно использовать команду: fail2ban-client status <jail-name>, где <jail-name> — конкретное правило (jail). В данном случае, статистика для правил 'postfix' и 'apache-fakegooglebot' показывает, что в настоящий момент нет заблокированных IP-адресов.



```
root@server:~  
[root@server.mrshcherbak.net ~]# fail2ban-client -v status postfix  
2023-12-23 22:40:37,804 fail2ban.configreader [10052]: INFO Loading configs for fail2ban under /etc/fail2ban  
2023-12-23 22:40:37,805 fail2ban.configparserinc[10052]: INFO Loading files: ['/etc/fail2ban/fail2ban.conf']  
2023-12-23 22:40:37,806 fail2ban.configparserinc[10052]: INFO Loading files: ['/etc/fail2ban/fail2ban.conf']  
2023-12-23 22:40:37,806 fail2ban [10052]: INFO Using socket file /var/run/fail2ban/fail2ban.sock  
2023-12-23 22:40:37,806 fail2ban [10052]: INFO Using pid file /var/run/fail2ban/fail2ban.pid, [INFO] logging  
to /var/log/fail2ban.log  
Status for the jail: postfix  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 0  
| '- Journal matches: _SYSTEMD_UNIT=postfix.service  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| '- Banned IP list:  
[root@server.mrshcherbak.net ~]# fail2ban-client -v status apache-fakegooglebot  
2023-12-23 22:42:17,124 fail2ban.configreader [10053]: INFO Loading configs for fail2ban under /etc/fail2ban  
2023-12-23 22:42:17,125 fail2ban.configparserinc[10053]: INFO Loading files: ['/etc/fail2ban/fail2ban.conf']  
2023-12-23 22:42:17,126 fail2ban.configparserinc[10053]: INFO Loading files: ['/etc/fail2ban/fail2ban.conf']  
2023-12-23 22:42:17,126 fail2ban [10053]: INFO Using socket file /var/run/fail2ban/fail2ban.sock  
2023-12-23 22:42:17,126 fail2ban [10053]: INFO Using pid file /var/run/fail2ban/fail2ban.pid, [INFO] logging  
to /var/log/fail2ban.log  
Status for the jail: apache-fakegooglebot  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 0  
| '- File list: /var/log/httpd/ssl_access_log /var/log/httpd/access_log /var/log/httpd/www.mrshcherbak.net-access_log /  
var/log/httpd/server.mrshcherbak.net-access_log  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| '- Banned IP list:  
[root@server.mrshcherbak.net ~]#
```

```
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 0  
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| '- Banned IP list:
```

## 9. Как разблокировать IP-адрес?

Для разблокировки IP-адреса можно воспользоваться командой:

```
fail2ban-client set <jail-name> unbanip <ip-address>
```

Разблокировала IP-адрес клиента и вновь посмотрела статус защиты SSH.

Убедилась, что блокировка клиента снята.

```
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 4  
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 1  
| |- Total banned: 1  
| '- Banned IP list: 192.168.1.142  
[root@server.mrshcherbak.net jail.d]# fail2ban-client set sshd unbanip 192.168.1.142  
1  
[root@server.mrshcherbak.net jail.d]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 4  
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 1  
| '- Banned IP list:
```