

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №16

дисциплина: Администрирование сетевых подсистем

Студент: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

МОСКВА

2024 г.

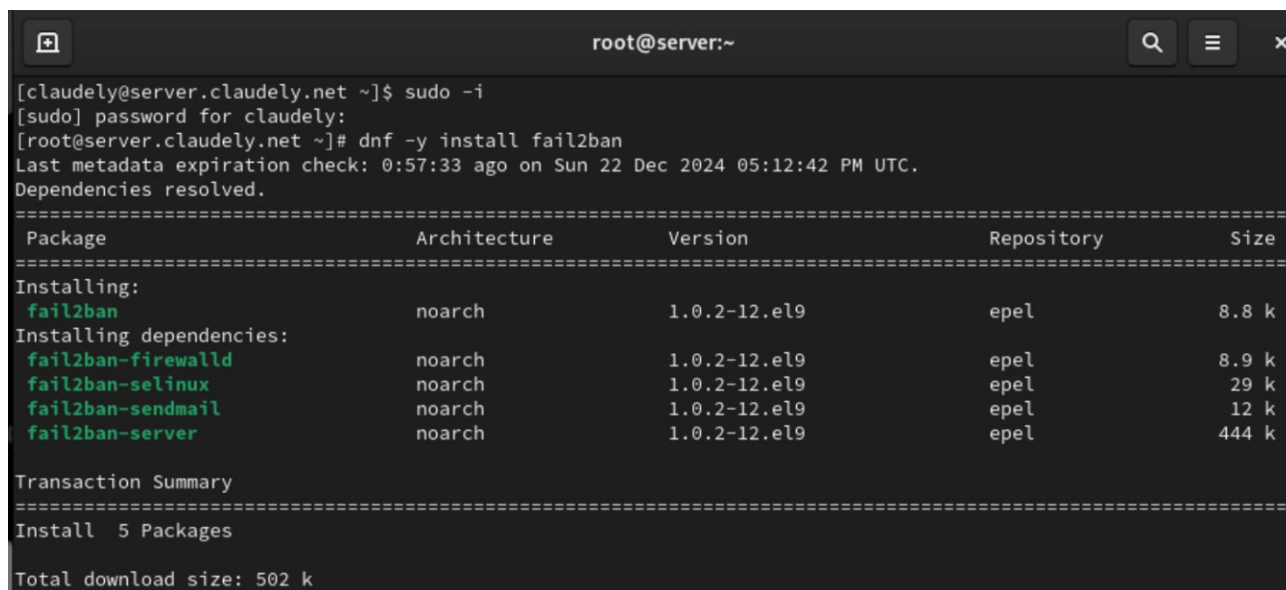
Цель работы:

Целью данной работы является получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

Выполнение работы:

На сервере установим fail2ban (Рис. 1.1):

`dnf -y install fail2ban`



```
root@server:~  
[claudely@server.claudely.net ~]$ sudo -i  
[sudo] password for claudely:  
[root@server.claudely.net ~]# dnf -y install fail2ban  
Last metadata expiration check: 0:57:33 ago on Sun 22 Dec 2024 05:12:42 PM UTC.  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
Installing:				
fail2ban	noarch	1.0.2-12.el9	epel	8.8 k
Installing dependencies:				
fail2ban-firewalld	noarch	1.0.2-12.el9	epel	8.9 k
fail2ban-selinux	noarch	1.0.2-12.el9	epel	29 k
fail2ban-sendmail	noarch	1.0.2-12.el9	epel	12 k
fail2ban-server	noarch	1.0.2-12.el9	epel	444 k

```
Transaction Summary  
=====
```

Transaction Summary	
Install	5 Packages

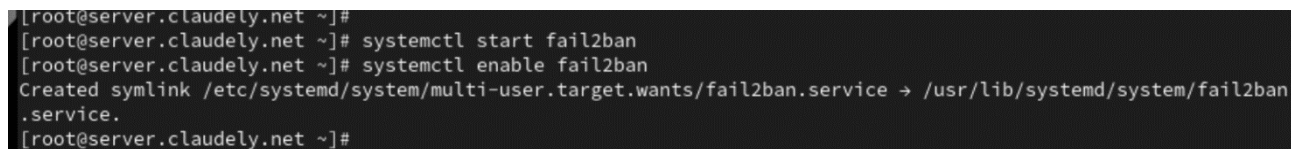
```
Total download size: 502 k
```

Рис. 1.1. Установка на сервере fail2ban.

Запустим сервер fail2ban (Рис. 1.2):

`systemctl start fail2ban`

`systemctl enable fail2ban`

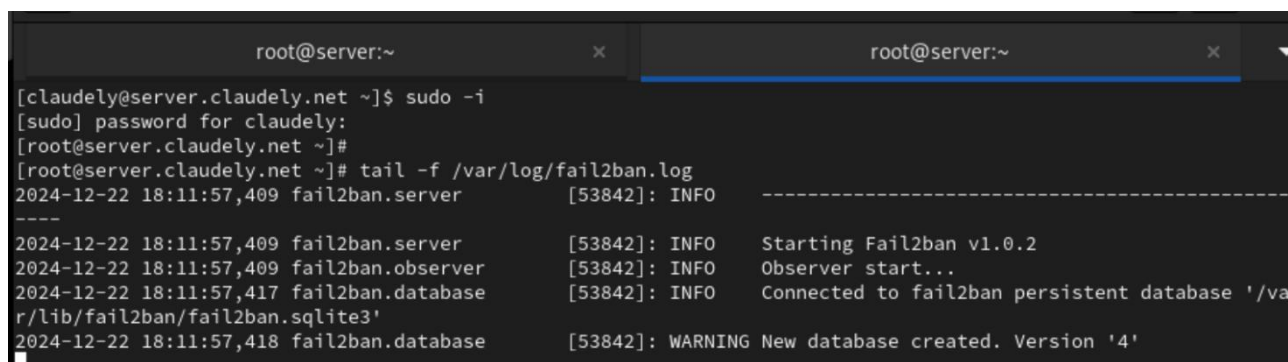


```
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# systemctl start fail2ban  
[root@server.claudely.net ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.  
[root@server.claudely.net ~]#
```

Рис. 1.2. Запуск сервера fail2ban.

В дополнительном терминале запустим просмотр журнала событий fail2ban (Рис. 1.3):

```
tail -f /var/log/fail2ban.log
```



```
root@server:~  
[claudely@server.claudely.net ~]$ sudo -i  
[sudo] password for claudely:  
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# tail -f /var/log/fail2ban.log  
2024-12-22 18:11:57,409 fail2ban.server [53842]: INFO -----  
-----  
2024-12-22 18:11:57,409 fail2ban.server [53842]: INFO Starting Fail2ban v1.0.2  
2024-12-22 18:11:57,409 fail2ban.observer [53842]: INFO Observer start...  
2024-12-22 18:11:57,417 fail2ban.database [53842]: INFO Connected to fail2ban persistent database '/va  
r/lib/fail2ban/fail2ban.sqlite3'  
2024-12-22 18:11:57,418 fail2ban.database [53842]: WARNING New database created. Version '4'
```

Рис. 1.3. Запуск просмотра в дополнительном терминале журнала событий fail2ban.

Создадим файл с локальной конфигурацией fail2ban (Рис. 1.4):

```
touch /etc/fail2ban/jail.d/customisation.local
```



```
[root@server.claudely.net ~]#  
[root@server.claudely.net ~]# touch /etc/fail2ban/jail.d/customisation.local  
[root@server.claudely.net ~]#
```

Рис. 1.4. Создание файла с локальной конфигурацией fail2ban.

В файле /etc/fail2ban/jail.d/customisation.local зададим время блокирования на 1 час и включим защиту SSH (Рис. 1.5):

```
root@server:~
GNU nano 5.6.1 customisation.local
DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

Рис. 1.5. Настройка в файле `/etc/fail2ban/jail.d/customisation.local` времени блокирования на 1 час и включение защиты SSH.

Перезапустим fail2ban (Рис. 1.6):

`systemctl restart fail2ban`

```
[root@server.claudely.net server]#
[root@server.claudely.net server]# systemctl restart fail2ban
[root@server.claudely.net server]#
[root@server.claudely.net server]#
```

Рис. 1.6. Перезапуск fail2ban.

Посмотрим журнал событий (Рис. 1.7):

```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# tail -f /var/log/fail2ban.log
2024-12-22 18:15:04,590 fail2ban.server [53842]: INFO Shutdown in progress...
2024-12-22 18:15:04,683 fail2ban.observer [53842]: INFO Observer stop ... try to end queue 5 seconds
2024-12-22 18:15:04,723 fail2ban.observer [53842]: INFO Observer stopped, 0 events remaining.
2024-12-22 18:15:04,778 fail2ban.server [53842]: INFO Stopping all jails
2024-12-22 18:15:04,814 fail2ban.database [53842]: INFO Connection to database closed.
2024-12-22 18:15:04,818 fail2ban.server [53842]: INFO Exiting Fail2ban
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO -----
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO Starting Fail2ban v1.0.2
2024-12-22 18:15:05,026 fail2ban.observer [53966]: INFO Observer start...
2024-12-22 18:15:05,039 fail2ban.database [53966]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
```

Рис. 1.7. Просмотр журнала событий.

В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту HTTP (Рис. 1.8):

```
#
# 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
```

Рис. 1.8. Включение защиты HTTP в файле
`/etc/fail2ban/jail.d/customisation.local`.

Перезапустим fail2ban (Рис. 1.9):

```
[root@server.claudely.net server]#
[root@server.claudely.net server]# systemctl restart fail2ban
[root@server.claudely.net server]#
[root@server.claudely.net server]#
```

Рис. 1.9. Перезапуск fail2ban.

После чего посмотрим журнал событий (Рис. 1.10):

```
[root@server.claudely.net ~]# tail -f /var/log/fail2ban.log
2024-12-22 18:15:04,590 fail2ban.server [53842]: INFO Shutdown in progress...
2024-12-22 18:15:04,683 fail2ban.observer [53842]: INFO Observer stop ... try to end queue 5 seconds
2024-12-22 18:15:04,723 fail2ban.observer [53842]: INFO Observer stopped, 0 events remaining.
2024-12-22 18:15:04,778 fail2ban.server [53842]: INFO Stopping all jails
2024-12-22 18:15:04,814 fail2ban.database [53842]: INFO Connection to database closed.
2024-12-22 18:15:04,818 fail2ban.server [53842]: INFO Exiting Fail2ban
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO -----
-----
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO Starting Fail2ban v1.0.2
2024-12-22 18:15:05,026 fail2ban.observer [53966]: INFO Observer start...
2024-12-22 18:15:05,039 fail2ban.database [53966]: INFO Connected to fail2ban persistent database '/v
r/lib/fail2ban/fail2ban.sqlite3'
2024-12-22 18:18:40,746 fail2ban.server [53966]: INFO Shutdown in progress...
2024-12-22 18:18:40,748 fail2ban.observer [53966]: INFO Observer stop ... try to end queue 5 seconds
2024-12-22 18:18:40,768 fail2ban.observer [53966]: INFO Observer stopped, 0 events remaining.
2024-12-22 18:18:40,817 fail2ban.server [53966]: INFO Stopping all jails
2024-12-22 18:18:40,828 fail2ban.database [53966]: INFO Connection to database closed.
2024-12-22 18:18:40,828 fail2ban.server [53966]: INFO Exiting Fail2ban
```

Рис. 1.10. Просмотр журнала событий.

В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту почты (Рис. 1.11):

```
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 [^]C Location M-U Undo
[^]X Exit [^]R Read File [^]\ Replace [^]U Paste [^]J Justify [^]_ Go To Line M-E Redo

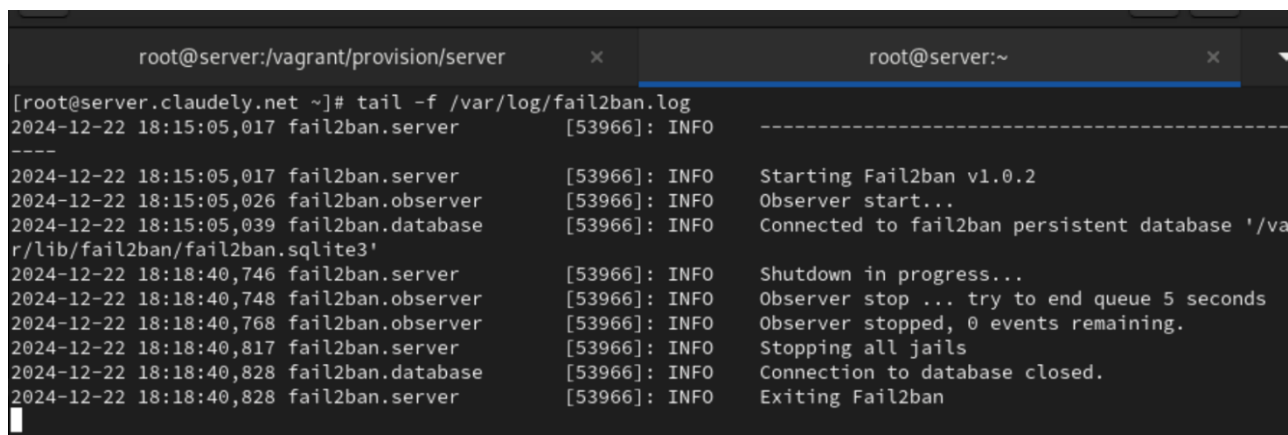
Рис. 1.11. Включение защиты почты в файле
`/etc/fail2ban/jail.d/customisation.local`.

Снова перезапустим fail2ban (Рис. 1.12):

```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# systemctl restart fail2ban
[root@server.claudely.net ~]#
```

Рис. 1.12. Повторный перезапуск fail2ban.

И посмотрим журнал событий (Рис. 1.13):

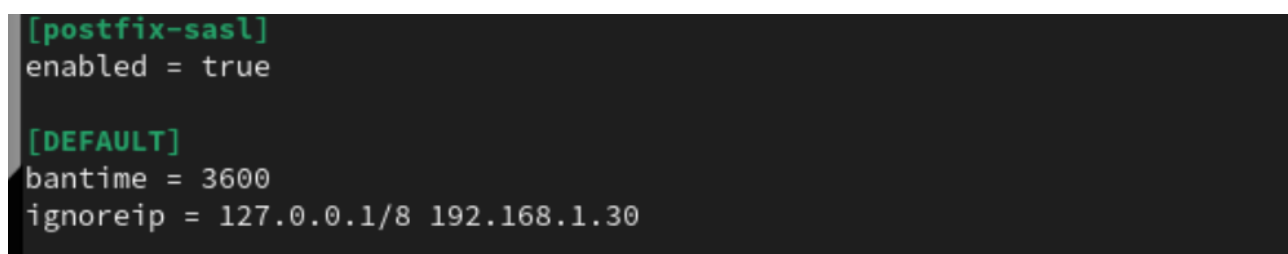


```
root@server:/vagrant/provision/server x root@server:~ x
[root@server.claudely.net ~]# tail -f /var/log/fail2ban.log
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO -----
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO Starting Fail2ban v1.0.2
2024-12-22 18:15:05,026 fail2ban.observer [53966]: INFO Observer start...
2024-12-22 18:15:05,039 fail2ban.database [53966]: INFO Connected to fail2ban persistent database '/va
r/lib/fail2ban/fail2ban.sqlite3'
2024-12-22 18:18:40,746 fail2ban.server [53966]: INFO Shutdown in progress...
2024-12-22 18:18:40,748 fail2ban.observer [53966]: INFO Observer stop ... try to end queue 5 seconds
2024-12-22 18:18:40,768 fail2ban.observer [53966]: INFO Observer stopped, 0 events remaining.
2024-12-22 18:18:40,817 fail2ban.server [53966]: INFO Stopping all jails
2024-12-22 18:18:40,828 fail2ban.database [53966]: INFO Connection to database closed.
2024-12-22 18:18:40,828 fail2ban.server [53966]: INFO Exiting Fail2ban
```

Рис. 1.13. Просмотр журнала событий.

На сервере посмотрим статус защиты SSH и разблокируем IP-адрес клиента. После чего вновь посмотрим статус защиты SSH и убедимся, что блокировка клиента снята (Рис. 2.3):

На сервере внесём изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента (Рис. 2.4):



```
[postfix-sasl]
enabled = true

[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
```

Рис. 2.4. Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле `/etc/fail2ban/jail.d/customisation.local`.

Перезапустим fail2ban (Рис. 2.5):


```
[root@server.claudely.net ~]#
[root@server.claudely.net ~]# systemctl restart fail2ban
[root@server.claudely.net ~]#
[root@server.claudely.net ~]#
```

Рис. 2.5. Перезапуск fail2ban.

Далее посмотрим журнал событий (Рис. 2.6):

```
[root@server.claudely.net ~]# tail -f /var/log/fail2ban.log
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO -----
-----
2024-12-22 18:15:05,017 fail2ban.server [53966]: INFO Starting Fail2ban v1.0.2
2024-12-22 18:15:05,026 fail2ban.observer [53966]: INFO Observer start...
2024-12-22 18:15:05,039 fail2ban.database [53966]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2024-12-22 18:18:40,746 fail2ban.server [53966]: INFO Shutdown in progress...
2024-12-22 18:18:40,748 fail2ban.observer [53966]: INFO Observer stop ... try to end queue 5 seconds
2024-12-22 18:18:40,768 fail2ban.observer [53966]: INFO Observer stopped, 0 events remaining.
2024-12-22 18:18:40,817 fail2ban.server [53966]: INFO Stopping all jails
2024-12-22 18:18:40,828 fail2ban.database [53966]: INFO Connection to database closed.
2024-12-22 18:18:40,828 fail2ban.server [53966]: INFO Exiting Fail2ban
```

Рис. 2.6. Просмотр журнала событий.

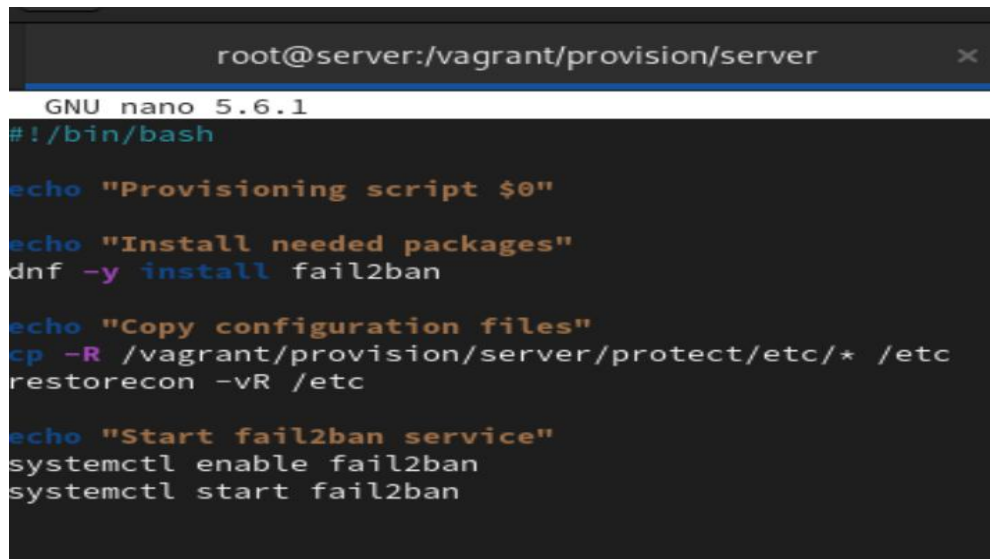
На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `protect`, в который поместим в соответствующие подкаталоги конфигурационные файлы. В каталоге `/vagrant/provision/server` создадим исполняемый файл `protect.sh` (Рис. 3.1):

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

Рис. 3.1. Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `protect`, в который помещаем в соответствующие

подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла protect.sh.

Открыв его на редактирование, пропишем в нём скрипт (Рис. 3.2):



```
root@server:/vagrant/provision/server
GNU nano 5.6.1
#!/bin/bash

echo "Provisioning script $0"

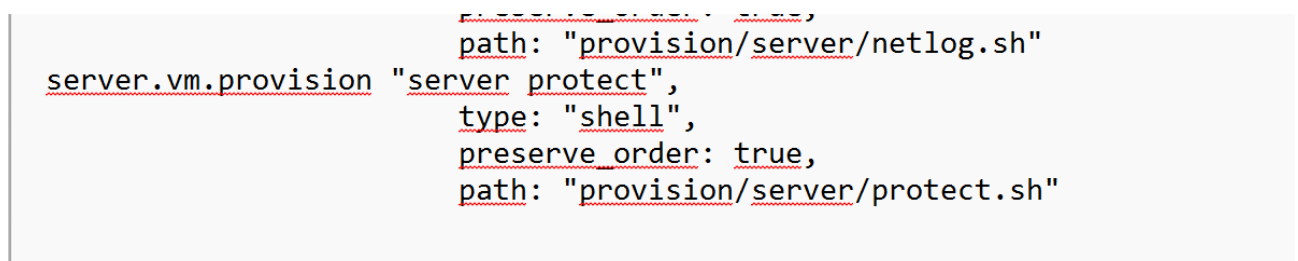
echo "Install needed packages"
dnf -y install fail2ban

echo "Copy configuration files"
cp -R /vagrant/provision/server/protect/etc/* /etc
restorecon -vR /etc

echo "Start fail2ban service"
systemctl enable fail2ban
systemctl start fail2ban
```

Рис. 3.2. Открытие файла на редактирование и добавление в него скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в соответствующем разделе конфигураций для сервера (Рис. 3.3):



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

Рис. 3.3. Добавление конфигураций в конфигурационном файле Vagrantfile для сервера.

Вывод:

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

Ответы на контрольные вопросы:

1. Поясните принцип работы Fail2ban. - **Fail2ban является инструментом для защиты от атак на серверы, основанных на анализе журналов. Он мониторит журналы системы на предмет неудачных попыток входа или других событий, а затем блокирует IP-адреса атакующих с использованием системных средств, таких как iptables. Принцип работы:**

Мониторинг журналов на предмет определенных событий.

Обнаружение повторных неудачных попыток входа или других нарушений.

Динамическое обновление правил брандмауэра для блокировки атакующих IP-адресов.

2. Настройки какого файла более приоритетны: jail.conf или jail.local? - **Настройки файла jail.local имеют более высокий приоритет и перекрывают настройки из jail.conf. Таким образом, если есть конфликтующие настройки, они будут использоваться из jail.local.**
3. Как настроить оповещение администратора при срабатывании Fail2ban? - **В файле jail.local нужно указать параметр destemail и задать адрес электронной почты, а также параметр action с указанием определенного действия (например, action_mw для отправки почты).**

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

Пример настроек для веб-службы в файле `jail.conf`:

[apache]

enabled = true

port = http,https

filter = apache-auth

logpath = /var/log/apache*/error.log

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

Пример настроек для почтовой службы в файле `jail.conf`:

[postfix]

enabled = true

filter = postfix

action = iptables-multiport[name=postfix, port="submission,smtps", protocol=tcp]

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, такие как блокировка IP-адреса с использованием брандмауэра, отправка уведомлений, добавление в**

черные списки и т.д. Описание действий можно найти в конфигурационных файлах в разделе action.

- 7. Как получить список действующих правил Fail2ban? - Используйте команду: `fail2ban-client status`.**
- 8. Как получить статистику заблокированных Fail2ban адресов? - Используйте команду: `fail2ban-client status <jail_name>`.**
- 9. Как разблокировать IP-адрес? - Используйте команду: `fail2ban-client set <jail_name> unbanip <ip_address>`.**