РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 16

дисциплина: Администрирование сетевых подсистем

Базовая защита от атак типа «brute force»

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы

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

Ход работы

1. Защита с помощью Fail2ban

1. На сервере установите fail2ban

```
[root@server.etanribergenov.net ~]# dnf -y install fail2ban
Last metadata expiration check: 0:07:36 ago on Fri 14 Apr 2023 07:58:03 PM UTC.
Dependencies resolved.
================================================================================
 Package                      Arch     Version              Repository   Size
================================================================================
Installing:
 fail2ban                     noarch   1.0.2-3.el9          epel        8.3 k
Upgrading:
 libselinux                   x86_64   3.4-3.el9            baseos       85 k
 libselinux-utils             x86_64   3.4-3.el9            baseos      158 k
 libsemanage                  x86_64   3.4-2.el9            baseos      118 k
 libsepol                     x86_64   3.4-1.1.el9          baseos      315 k
 policycoreutils              x86_64   3.4-4.el9            baseos      202 k
 policycoreutils-python-utils noarch   3.4-4.el9            appstream    69 k
 python3-libselinux           x86_64   3.4-3.el9            appstream   185 k
 python3-libsemanage          x86_64   3.4-2.el9            appstream    80 k
 python3-policycoreutils      noarch   3.4-4.el9            appstream   2.0 M
 selinux-policy               noarch   34.1.43-1.el9_1.2    baseos       52 k
 selinux-policy-targeted      noarch   34.1.43-1.el9_1.2    baseos      6.4 M
Installing dependencies:
 fail2ban-firewalld           noarch   1.0.2-3.el9          epel        8.5 k
```

Рис. 1. Установка fail2ban

2. Запустите сервер fail2ban

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

Рис. 2. Запуск сервера fail2ban

3. В дополнительном терминале запустите просмотр журнала событий fail2ban

```
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]# tail -f /var/log/fail2ban.log
2023-04-14 20:11:39,182 fail2ban.server         [46696]: INFO    --------------
----------------------------------
2023-04-14 20:11:39,182 fail2ban.server         [46696]: INFO    Starting Fail2b
an v1.0.2
2023-04-14 20:11:39,184 fail2ban.observer       [46696]: INFO    Observer start.
..
2023-04-14 20:11:39,209 fail2ban.database       [46696]: INFO    Connected to fa
il2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-04-14 20:11:39,215 fail2ban.database       [46696]: WARNING New database cr
eated. Version '4'
2023-04-14 20:17:08,610 fail2ban.server         [46696]: INFO    Shutdown in pro
gress...
2023-04-14 20:17:08,611 fail2ban.observer       [46696]: INFO    Observer stop .
.. try to end queue 5 seconds
2023-04-14 20:17:08,632 fail2ban.observer       [46696]: INFO    Observer stoppe
d, 0 events remaining.
2023-04-14 20:17:08,674 fail2ban.server         [46696]: INFO    Stopping all ja
ils
2023-04-14 20:17:08,674 fail2ban.database       [46696]: INFO    Connection to d
atabase closed.
2023-04-14 20:17:08,675 fail2ban.server         [46696]: INFO    Exiting Fail2ba
```

Рис. 3. Просмотр журнала событий fail2ban

4. Создайте файл с локальной конфигурацией fail2ban

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

Рис. 4. Создание файла с локальной конфигурацией fail2ban

5. В файле /etc/fail2ban/jail.d/customisation.local
   a) задайте время блокирования на 1 час (время задаётся в секундах)

```
customis~on.local
[DEFAULT]
bantime = 3600
```

Рис. 5. Настройка времени блокирования

b) включите защиту SSH

```
#
#  SSH servers
#

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

Рис. 6. Включение защиты SSH

6. Перезапустите fail2ban

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

Рис. 7. Перезапуск fail2ban

7. Посмотрите журнал событий

```
2023-04-14 20:17:10,070 fail2ban.filter         [46823]: INFO    Added logfile:
'/var/log/audit/audit.log' (pos = 0, hash = 7c234ea41e96fe055c87355690edf0fe2078
a4e7)
2023-04-14 20:17:10,072 fail2ban.jail           [46823]: INFO    Creating new ja
il 'sshd-ddos'
2023-04-14 20:17:10,096 fail2ban.jail           [46823]: INFO    Jail 'sshd-ddos
' uses poller {}
2023-04-14 20:17:10,097 fail2ban.jail           [46823]: INFO    Initiated 'poll
ing' backend
2023-04-14 20:17:10,113 fail2ban.filter         [46823]: INFO      maxLines: 1
2023-04-14 20:17:10,130 fail2ban.filter         [46823]: INFO      maxRetry: 5
2023-04-14 20:17:10,130 fail2ban.filter         [46823]: INFO      findtime: 600
2023-04-14 20:17:10,131 fail2ban.actions        [46823]: INFO      banTime: 3600
2023-04-14 20:17:10,133 fail2ban.filter         [46823]: INFO      encoding: UTF
-8
2023-04-14 20:17:10,164 fail2ban.jail           [46823]: INFO    Jail 'sshd' sta
rted
2023-04-14 20:17:10,183 fail2ban.filtersystemd  [46823]: INFO    [sshd] Jail is
in operation now (process new journal entries)
2023-04-14 20:17:10,201 fail2ban.jail           [46823]: INFO    Jail 'selinux-s
sh' started
2023-04-14 20:17:10,209 fail2ban.jail           [46823]: INFO    Jail 'sshd-ddos
' started
```

Рис. 8. Просмотр журнала событий

8. В файле /etc/fail2ban/jail.d/customisation.local включите защиту HTTP

```
customisation.local
#
#  HTTP servers
#

[apache-auth]
enabled = true

[apache-badbots]
enabled = true

[apache-noscript]
enabled = true

[apache-overflows]
enabled = true
```

```
customisation.local   [
[apache-nohome]
enabled = true

[apache-botsearch]
enabled = true

[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true
```

Рис. 9. Включение защиты HTTP

9. Перезапустите fail2ban

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

Рис. 10. Перезапуск fail2ban

10. Посмотрите журнал событий

```
2023-04-14 20:24:30,721 fail2ban.jail           [46888]: INFO    Jail 'selinux-s
sh' started
2023-04-14 20:24:30,750 fail2ban.jail           [46888]: INFO    Jail 'apache-au
th' started
2023-04-14 20:24:30,798 fail2ban.jail           [46888]: INFO    Jail 'apache-ba
dbots' started
2023-04-14 20:24:30,836 fail2ban.jail           [46888]: INFO    Jail 'apache-no
script' started
2023-04-14 20:24:30,876 fail2ban.jail           [46888]: INFO    Jail 'apache-ov
erflows' started
2023-04-14 20:24:30,885 fail2ban.jail           [46888]: INFO    Jail 'apache-no
home' started
2023-04-14 20:24:30,905 fail2ban.jail           [46888]: INFO    Jail 'apache-bo
tsearch' started
2023-04-14 20:24:30,948 fail2ban.jail           [46888]: INFO    Jail 'apache-fa
kegooglebot' started
2023-04-14 20:24:30,980 fail2ban.jail           [46888]: INFO    Jail 'apache-mo
dsecurity' started
2023-04-14 20:24:30,990 fail2ban.jail           [46888]: INFO    Jail 'apache-sh
ellshock' started
2023-04-14 20:24:31,008 fail2ban.jail           [46888]: INFO    Jail 'sshd-ddos
' started
```

Рис. 11. Просмотр журнала событий

11. В файле /etc/fail2ban/jail.d/customisation.local включите защиту почты

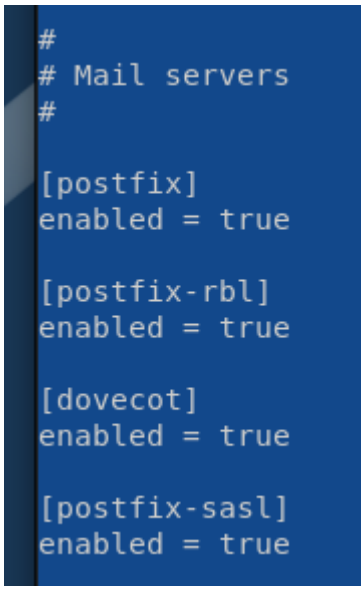

Рис. 12. Включение защиты почты

12. Перезапустите fail2ban

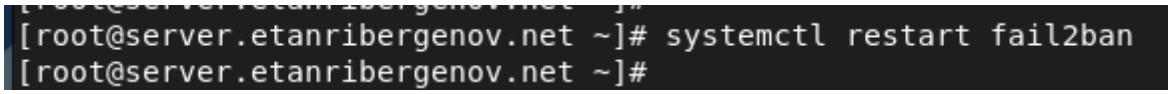

Рис. 13. Перезапуск fail2ban

13. Посмотрите журнал событий

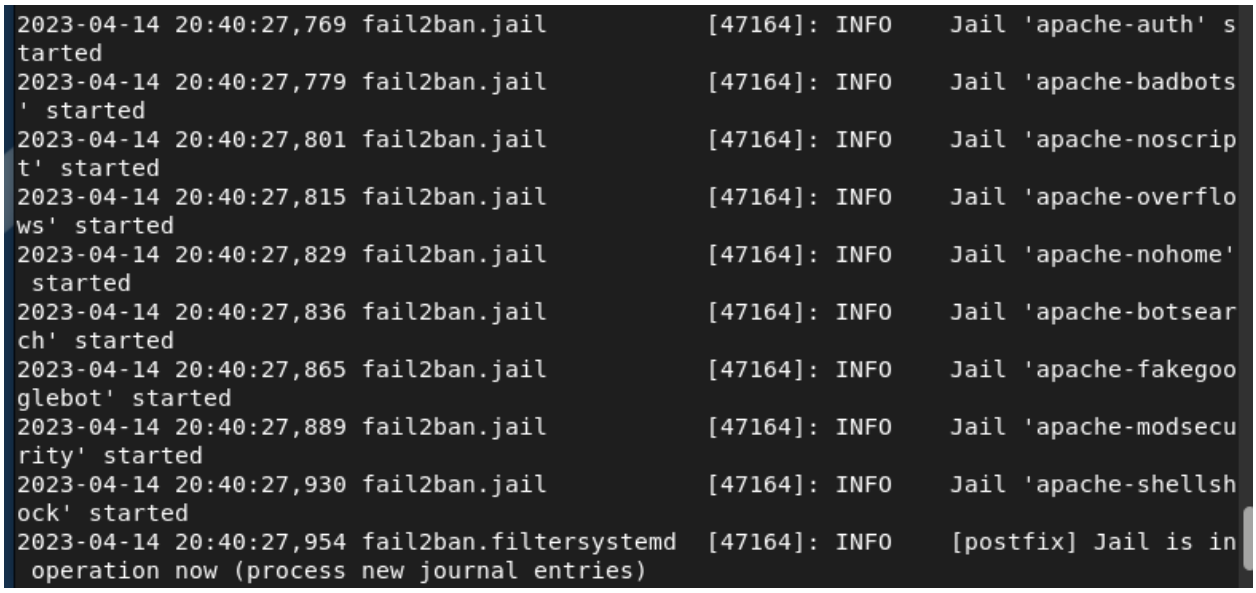

Рис. 14. Просмотр журнала событий

2. Проверка работы Fail2ban

1. На сервере посмотрите статус fail2ban

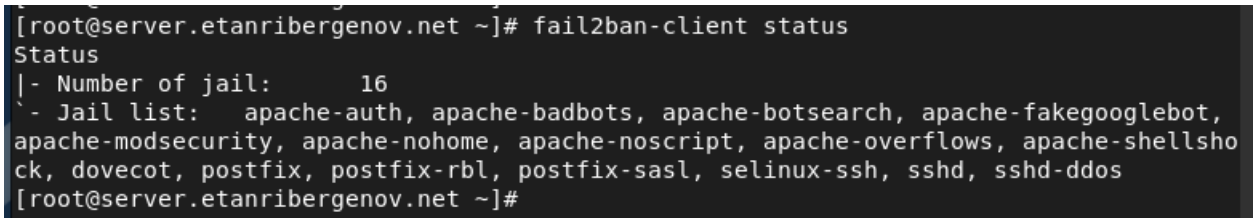

Рис. 15. Просмотр статуса fail2ban

2. Посмотрите статус защиты SSH в fail2ban

```
[root@server.etanribergenov.net ~]# 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.etanribergenov.net ~]#
```

Рис. 16. Просмотр статуса защиты SSH в fail2ban

3. Установите максимальное количество ошибок для SSH, равное 2

   fail2ban-client set sshd maxretry 2

```
[root@server.etanribergenov.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.etanribergenov.net ~]#
```

Рис. 17. Просмотр статуса защиты SSH в fail2ban

4. С клиента попытайтесь зайти по SSH на сервер с неправильным паролем.

```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribe
rgenov.net
The authenticity of host 'server.etanribergenov.net (192.168.1.1)' can't be esta
blished.
ED25519 key fingerprint is SHA256:zqbOam9bCTBqb0qNzuP7z0xlgOqvGhkHxMkw2sQdblo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.etanribergenov.net' (ED25519) to the list of
known hosts.
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
etanribergenov@server.etanribergenov.net: Permission denied (publickey,gssapi-ke
yex,gssapi-with-mic,password).
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 18. Попытка подключения к серверу по SSH с неправильным паролем

5. На сервере посмотрите статус защиты SSH

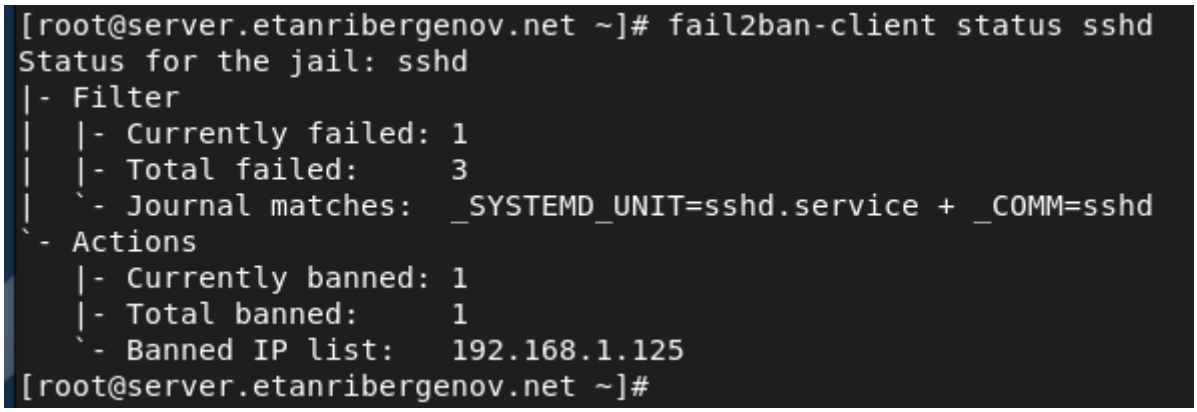

Рис. 19. Просмотр статуса защиты SSH

Видим, что было три провальных попытки подключиться, и отныне ip-адрес клиента был заблокирован.

6. Разблокируйте IP-адрес клиента

   fail2ban-client set sshd unbanip <ip-адрес>

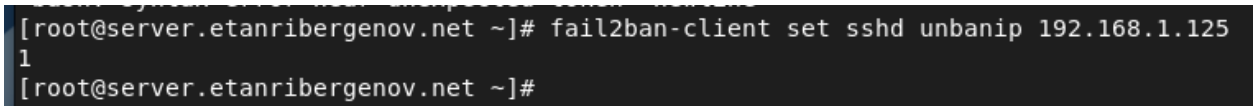

Рис. 20. Разблокировка IP-адреса клиента

7. Вновь посмотрите статус защиты SSH

IP-адрес клиента разблокирован

```
[root@server.etanribergenov.net ~]# 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:
[root@server.etanribergenov.net ~]#
```

Рис. 21. Просмотр статуса защиты SSH

8. На сервере внесите изменение в конфигурационный файл /etc/fail2ban/jail.d/customisation.local, добавив в раздел по умолчанию игнорирование адреса клиента

```
customisation.local   [----]  9 L:[  1
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.125
```

Рис. 22. Добавление в раздел по умолчанию игнорирование адреса клиента

9. Перезапустите fail2ban

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

Рис. 23. Перезапуск fail2ban

10. Посмотрите журнал событий

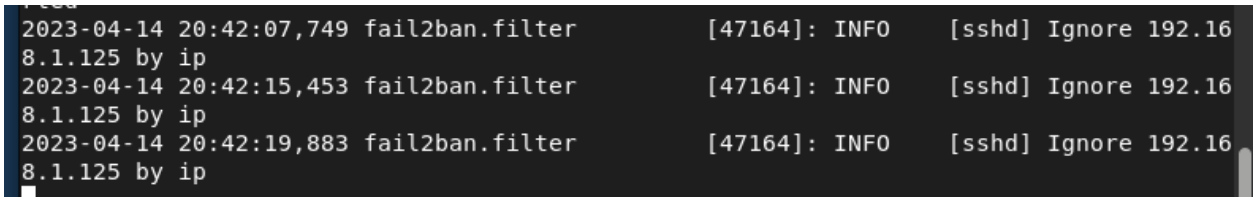

Рис. 24. Просмотр журнала событий

11. Вновь попытайтесь войти с клиента на сервер с неправильным паролем и посмотрите статус защиты SSH.

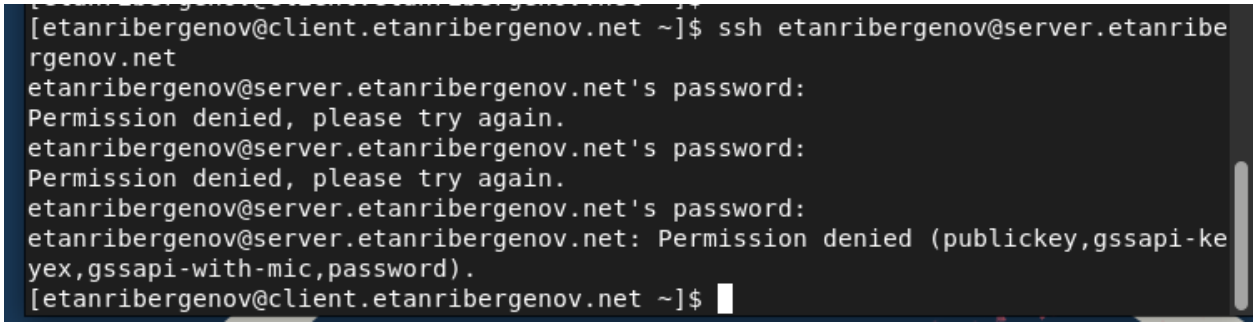

Рис. 25. Попытка входа с клиента на сервер с неправильным паролем

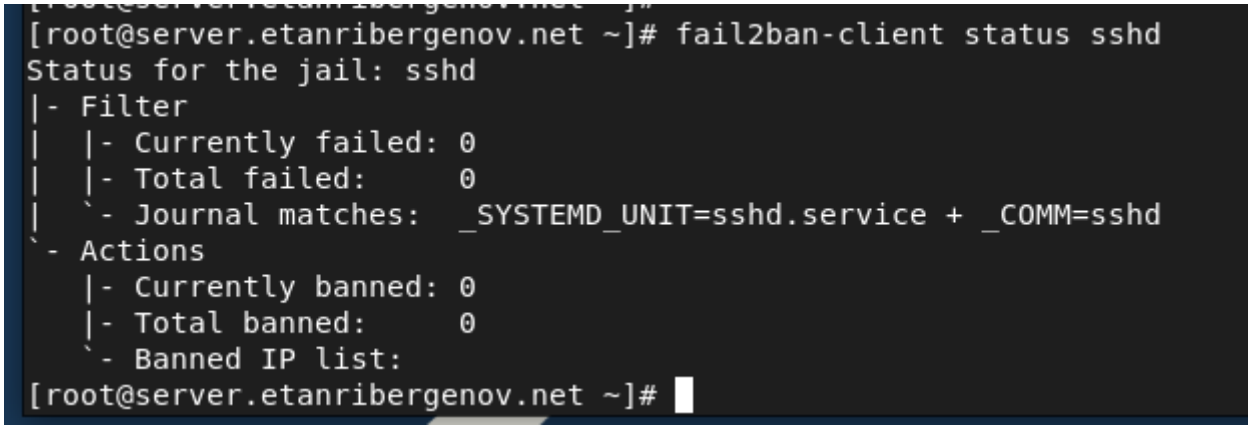

Рис. 26. Просмотр статуса защиты SSH

Теперь адрес игнорируется, а не блокируется при неудачном входе.

3. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог protect, в который поместите в соответствующие подкаталоги конфигурационные файлы.

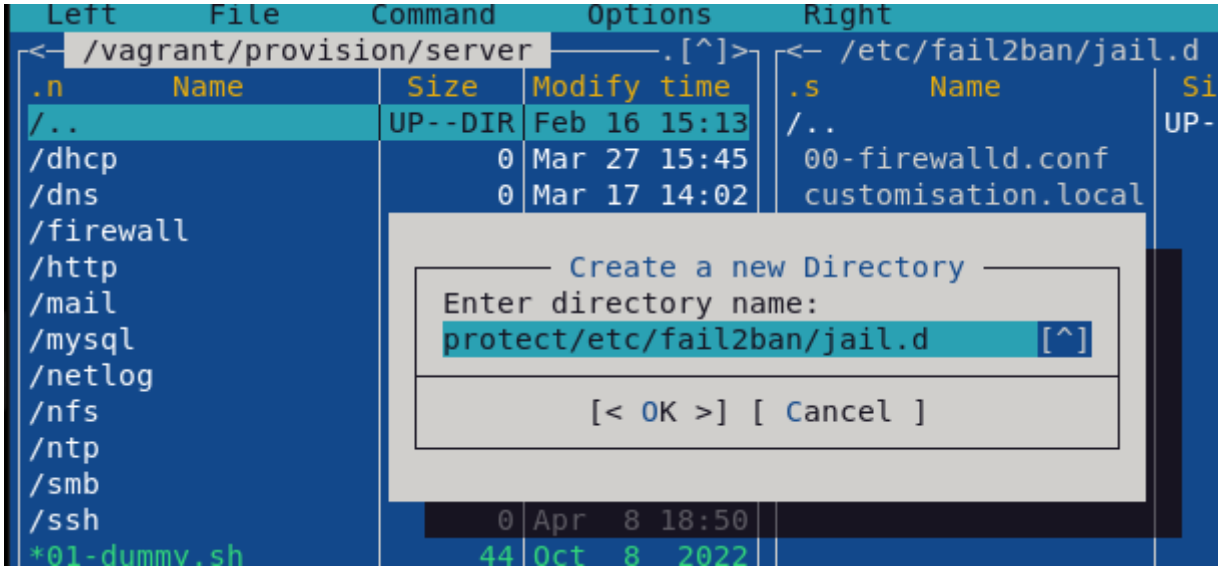

Рис. 27. Создание подкаталогов

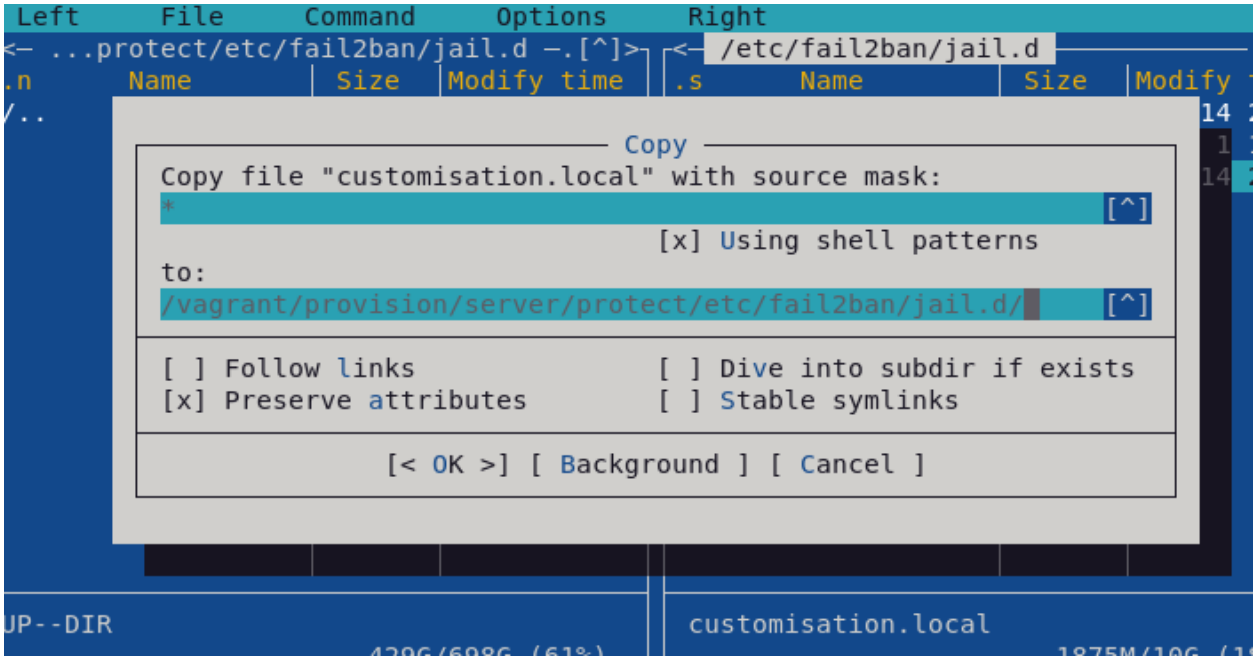

Рис. 28. Копирование конфигурационного файла fail2ban на сервере

2. В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh

```
[root@server.etanribergenov.net server]# touch protect.sh
[root@server.etanribergenov.net server]# chmod protect.sh
chmod: missing operand after ‘protect.sh’
Try 'chmod --help' for more information.
[root@server.etanribergenov.net server]# chmod +x protect.sh
[root@server.etanribergenov.net server]#
```

Рис. 29. Создание исполняемого файла

3. Для отработки созданного скрипта во время загрузки виртуальных машин в конфигурационном файле Vagrantfile необходимо добавить в конфигурации сервера запись.

```
protect.sh          [----]  0 L:[  1+14  15/ 15] *(28
#!/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. 30. Скрипт в исполняемом файле

Вывод

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

Ответы на контрольные вопросы

1. Программа Fail2ban считывает логи, ища подозрительные действия со стороны клиента, такие как многократный неправильный ввод пароля, запрос на выполнение опасных скриптов. При обнаружении таковых, он вносит изменения в настройки межсетевого экрана для блокировки IP-адреса подозрительного клиента.
2. Файл jail.local.
3. Оповещение через почту: в разделе по умолчанию нужно указать почту для параметра «destemail», параметр «sendermail» отвечает за имя отправителя, и параметру «mta» следует указать значение «sendmail», что значит отправить письмо.
4. Правила: «apache-auth» - блокировка при неправильном вводе пароля; «apache-блокировка при попытке получения доступа к содержимому домашнего каталоге без разрешения; «apache-botsearch» - определение ботов, ищущих перебором популярные скрипты; «apache-fakegooglebot» - блокировка клиентов, выдающих себя за google-ботов; «apache-modsecurity» - блокировка приложения при его недопустимом поведении; «apache-shellshock» - блокировка при shellshock-атаке; подозрительных URL-адресов.

5. Защита postfix, защита dovecot и защита ssh.
6. Блокировка ip-адреса, порта; оповещение по почте. В файле jail.conf,
7. Команда fail2ban-client status.
8. Команда fail2ban-client status sshd.
9. Команда fail2ban-client set sshd unbanip <ip>.