

Лабораторная работа

№16

Базовая защита от атак типа «brute force»

Студент: БАНСИМБА КЛОДЕЛИ ДЬЕГРА

Группа: НПИбд 02–22

дисциплина: Администрирование сетевых подсистем (Lab 16)

Цель работы

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

Защита с помощью 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  
=====
```

Install	5 Packages
---------	------------

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

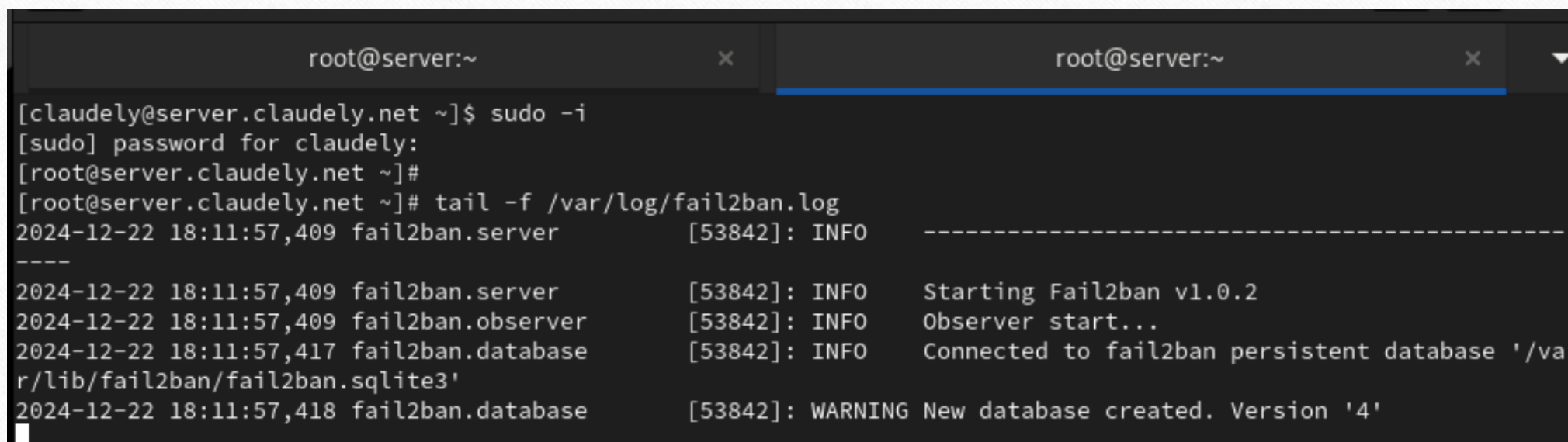
Рис. 1.1. Установка на сервере fail2ban.

Защита с помощью 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.

Защита с помощью Fail2ban



```
root@server:~ x root@server:~ x
[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'
```

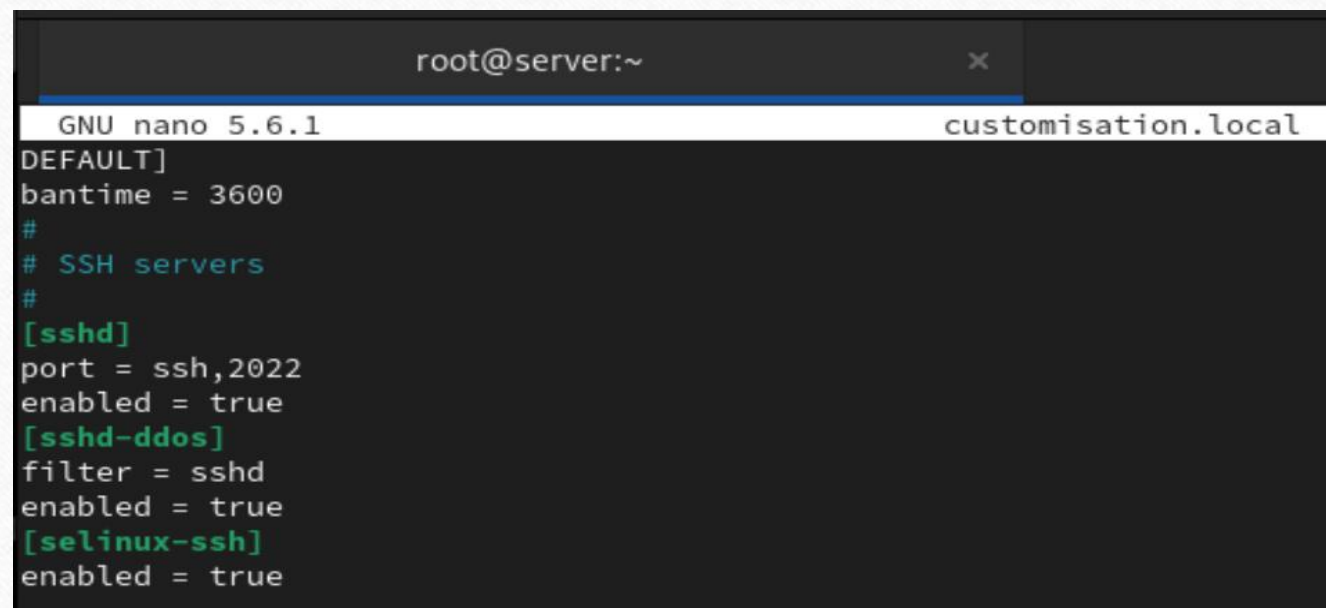
Рис. 1.3. Запуск просмотра в дополнительном терминале журнала событий fail2ban.

Защита с помощью Fail2ban

```
[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.

Защита с помощью Fail2ban



```
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.

Защита с помощью 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.

Защита с помощью Fail2ban

```
[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.

Защита с помощью Fail2ban

```
#  
# 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.

Защита с помощью Fail2ban

```
[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'
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.

Защита с помощью Fail2ban

```
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

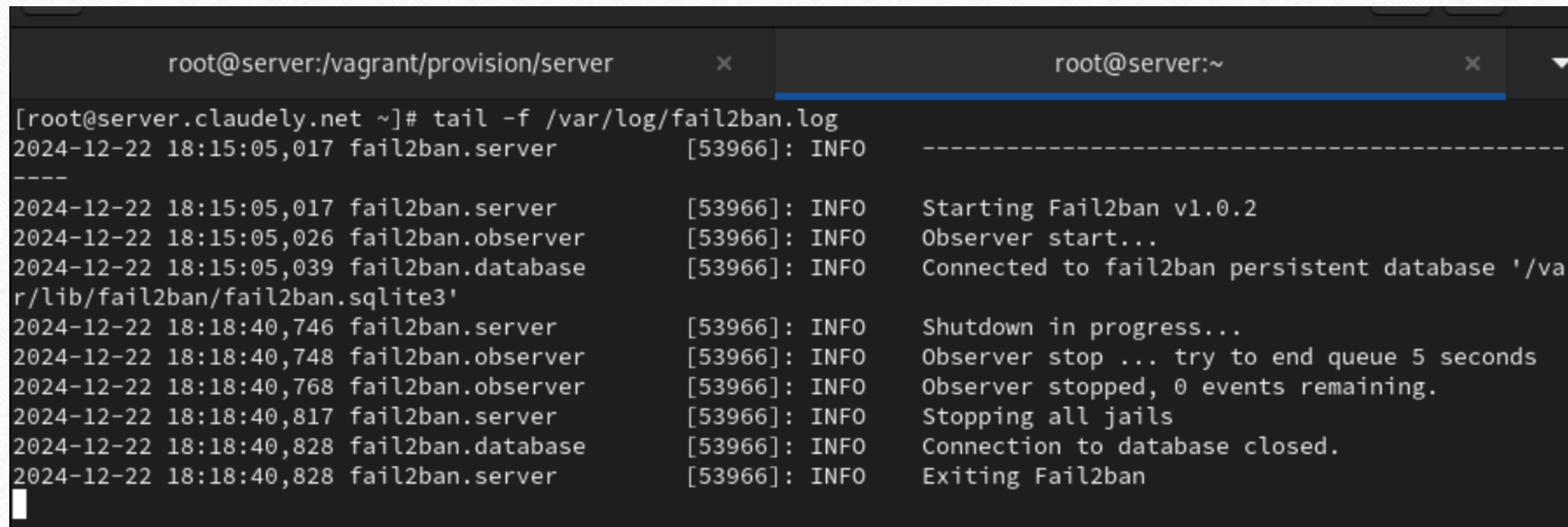
Рис. 1.11. Включение защиты почты в файле /etc/fail2ban/jail.d/customisation.local.

Защита с помощью Fail2ban

```
[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.

Защита с помощью Fail2ban



The image shows a terminal window with two tabs. The active tab is titled 'root@server:~'. The terminal displays the output of the command 'tail -f /var/log/fail2ban.log'. The logs show the Fail2ban service starting at 18:15:05, connecting to a SQLite database, and then shutting down at 18:18:40. The shutdown process includes stopping the observer, stopping all jails, and closing the database connection.

```
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.

Проверка работы Fail2ban

```
[postfix-sasl]
enabled = true

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

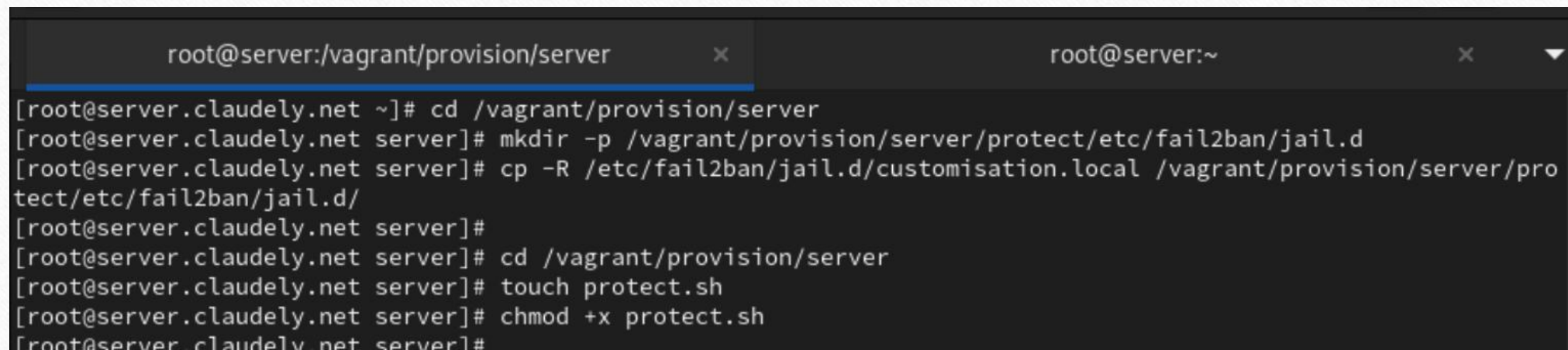
Рис. 2.4. Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле `/etc/fail2ban/jail.d/customisation.local`.

Проверка работы Fail2ban

```
[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. 2.6. Просмотр журнала событий.

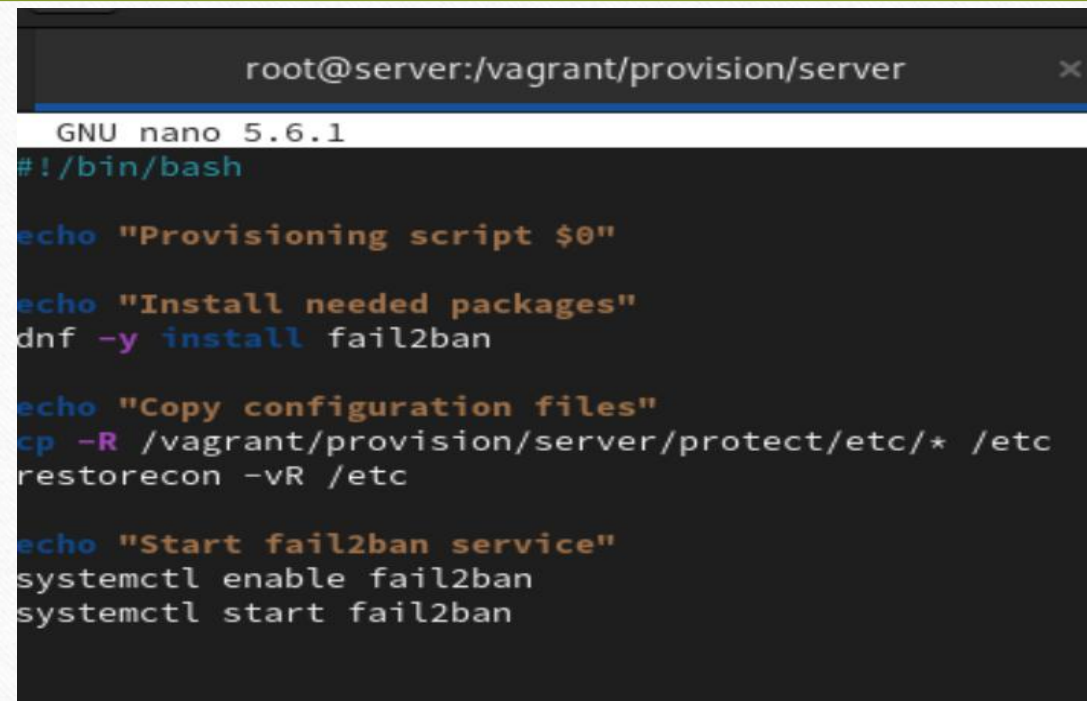
Внесение изменений в настройки внутреннего окружения виртуальных машин



```
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`.

Внесение изменений в настройки внутреннего окружения виртуальных машин



```
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.

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
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».

Спасибо за внимание!