Лабораторная работа №16

Базовая защита от атак типа «brute force»

Студент: Пакавира Арсениу Висенте Луиш

Группа: Нфибд 02 –23

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

```
================================================================================
 Package                 Arch        Version              Repository    Size
================================================================================
Installing:
 fail2ban                noarch      1.1.0-6.el9          epel         9.3 k
Upgrading:
 selinux-policy          noarch      38.1.65-1.el9        baseos        42 k
 selinux-policy-targeted noarch      38.1.65-1.el9        baseos       6.5 M
Installing dependencies:
 fail2ban-firewalld      noarch      1.1.0-6.el9          epel         9.5 k
 fail2ban-selinux        noarch      1.1.0-6.el9          epel          31 k
 fail2ban-sendmail       noarch      1.1.0-6.el9          epel          12 k
 fail2ban-server         noarch      1.1.0-6.el9          epel         465 k

Transaction Summary
================================================================================
Install  5 Packages
Upgrade  2 Packages
```

Рис. 1.1. Установка на сервере fail2ban.

Защита с помощью Fail2ban

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

Рис. 1.2. Запуск сервера fail2ban.

Защита с помощью Fail2ban

```
[root@server.user.net ~]# sudo -i
[root@server.user.net ~]# tail -f /var/log/fail2ban.log
2026-01-05 16:34:15,243 fail2ban.server         [41656]: INFO    --------------------------------------------------
2026-01-05 16:34:15,244 fail2ban.server         [41656]: INFO    Starting Fail2ban v1.1.0
2026-01-05 16:34:15,246 fail2ban.observer       [41656]: INFO    Observer start...
2026-01-05 16:34:15,256 fail2ban.database       [41656]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
2026-01-05 16:34:15,258 fail2ban.database       [41656]: WARNING New database created. Version '4'
```

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

Защита с помощью Fail2ban

```
[user@server.user.net ~]$ touch /etc/fail2ban/jail.d/customisation.local
touch: cannot touch '/etc/fail2ban/jail.d/customisation.local': Permission denied
[user@server.user.net ~]$
```

Рис. 1.4. Создание файла с локальной конфигурацией fail2ban.

Защита с помощью Fail2ban

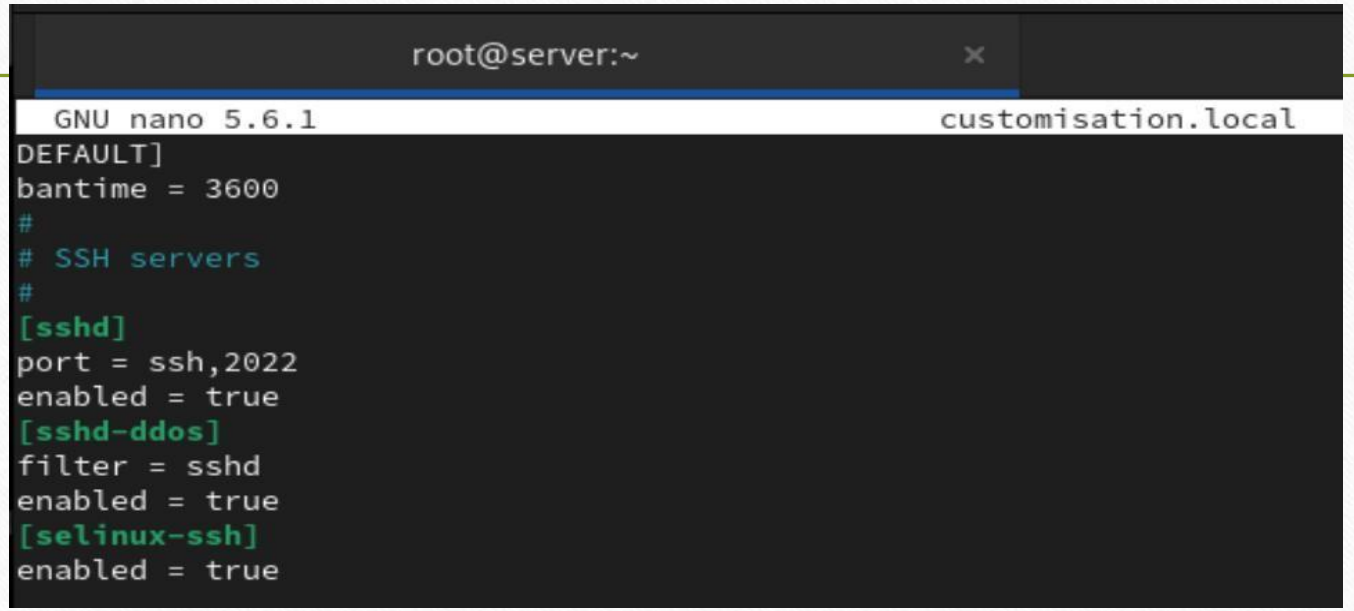

Рис. 1.5. Настройка в файле /etc/fail2ban/jail.d/customisation.local времени блокирования на 1 час и включение защиты SSH.

Защита с помощью Fail2ban

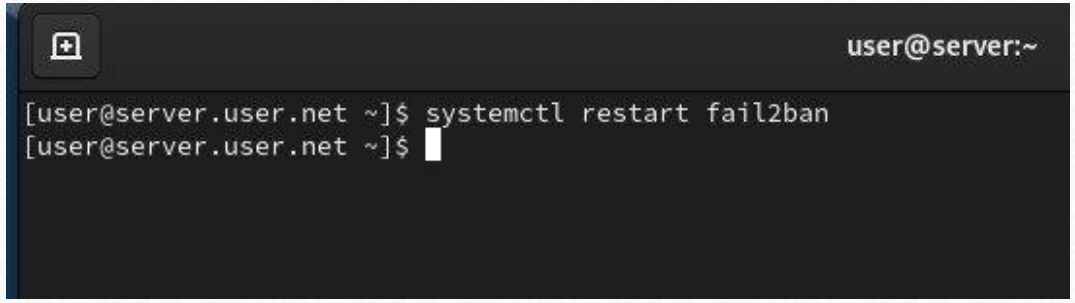

Рис. 1.6. Перезапуск fail2ban.

Защита с помощью Fail2ban

```
[root@server.user.net ~]# tail -f /var/log/fail2ban.log
2026-01-05 16:53:32,165 fail2ban.server         [41859]: INFO    Shutdown in progress...
2026-01-05 16:53:32,167 fail2ban.observer       [41859]: INFO    Observer stop ... try to end queue 5 seconds
2026-01-05 16:53:32,191 fail2ban.observer       [41859]: INFO    Observer stopped, 0 events remaining.
2026-01-05 16:53:32,237 fail2ban.server         [41859]: INFO    Stopping all jails
2026-01-05 16:53:32,239 fail2ban.database       [41859]: INFO    Connection to database closed.
2026-01-05 16:53:32,239 fail2ban.server         [41859]: INFO    Exiting Fail2ban
2026-01-05 16:53:32,438 fail2ban.server         [42034]: INFO    --------------------------------------------------
2026-01-05 16:53:32,440 fail2ban.server         [42034]: INFO    Starting Fail2ban v1.1.0
2026-01-05 16:53:32,469 fail2ban.observer       [42034]: INFO    Observer start...
2026-01-05 16:53:32,492 fail2ban.database       [42034]: 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.user.net ~]# tail -f /var/log/fail2ban.log
2026-01-05 17:01:56,635 fail2ban.server         [42034]: INFO    Shutdown in progress...
2026-01-05 17:01:56,636 fail2ban.observer       [42034]: INFO    Observer stop ... try to end queue 5 seconds
2026-01-05 17:01:56,658 fail2ban.observer       [42034]: INFO    Observer stopped, 0 events remaining.
2026-01-05 17:01:56,737 fail2ban.server         [42034]: INFO    Stopping all jails
2026-01-05 17:01:56,738 fail2ban.database       [42034]: INFO    Connection to database closed.
2026-01-05 17:01:56,738 fail2ban.server         [42034]: INFO    Exiting Fail2ban
2026-01-05 17:01:56,984 fail2ban.server         [42212]: INFO    --------------------------------------------------
2026-01-05 17:01:56,984 fail2ban.server         [42212]: INFO    Starting Fail2ban v1.1.0
2026-01-05 17:01:56,985 fail2ban.observer       [42212]: INFO    Observer start...
2026-01-05 17:01:56,990 fail2ban.database       [42212]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
```

Рис. 1.10. Просмотр журнала событий.

Защита с помощью Fail2ban

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

Защита с помощью Fail2ban

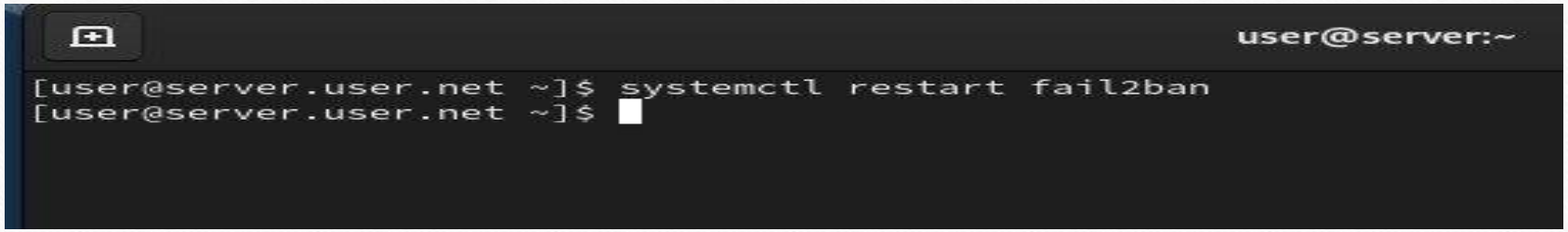

Рис. 1.12. Повторный перезапуск fail2ban.

Защита с помощью Fail2ban

```
[root@server.user.net ~]# tail -f /var/log/fail2ban.log
2026-01-05 17:07:59,457 fail2ban.server         [42212]: INFO    Shutdown in progress...
2026-01-05 17:07:59,459 fail2ban.observer       [42212]: INFO    Observer stop ... try to end queue 5 seconds
2026-01-05 17:07:59,493 fail2ban.observer       [42212]: INFO    Observer stopped, 0 events remaining.
2026-01-05 17:07:59,528 fail2ban.server         [42212]: INFO    Stopping all jails
2026-01-05 17:07:59,528 fail2ban.database       [42212]: INFO    Connection to database closed.
2026-01-05 17:07:59,529 fail2ban.server         [42212]: INFO    Exiting Fail2ban
2026-01-05 17:08:00,063 fail2ban.server         [42355]: INFO    --------------------------------------------------
2026-01-05 17:08:00,063 fail2ban.server         [42355]: INFO    Starting Fail2ban v1.1.0
2026-01-05 17:08:00,072 fail2ban.observer       [42355]: INFO    Observer start...
2026-01-05 17:08:00,094 fail2ban.database       [42355]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
```

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.user.net ~]# tail -f /var/log/fail2ban.log
2026-01-05 17:07:59,457 fail2ban.server          [42212]: INFO    Shutdown in progress...
2026-01-05 17:07:59,459 fail2ban.observer        [42212]: INFO    Observer stop ... try to end queue 5 seconds
2026-01-05 17:07:59,493 fail2ban.observer        [42212]: INFO    Observer stopped, 0 events remaining.
2026-01-05 17:07:59,528 fail2ban.server          [42212]: INFO    Stopping all jails
2026-01-05 17:07:59,528 fail2ban.database        [42212]: INFO    Connection to database closed.
2026-01-05 17:07:59,529 fail2ban.server          [42212]: INFO    Exiting Fail2ban
2026-01-05 17:08:00,063 fail2ban.server          [42355]: INFO    --------------------------------------------------
2026-01-05 17:08:00,063 fail2ban.server          [42355]: INFO    Starting Fail2ban v1.1.0
2026-01-05 17:08:00,072 fail2ban.observer        [42355]: INFO    Observer start...
2026-01-05 17:08:00,094 fail2ban.database        [42355]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
```

Рис. 2.6. Просмотр журнала событий.

Внесение изменений в настройки внутреннего окружения виртуальных машин

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

```
                        path: "provision/server/netlog.sh"
server.vm.provision "server protect",
                        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!