Лабораторная работа №16

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Задание

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб.
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban.

3 Выполнение лабораторной работы

3.1 Защита с помощью Fail2ban

На сервере устанавливаю fail2ban (рис. [3.1]).

```
[user@server ~]$ sudo -i
[sudo] password for user:
[root@server ~]# dnf -y install fail2ban
Last metadata expiration check: 2:20:24 ago on Thu 12 Feb 2026 04:53:07 PM MSK
.
Dependencies resolved.
================================================================================
 Package                  Architecture  Version           Repository   Size
================================================================================
Installing:
 fail2ban                 noarch        1.1.0-6.el9       epel        9.3 k
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

Total download size: 527 k
Installed size: 1.5 M
Downloading Packages:
(1/5): fail2ban-firewalld-1.1.0-6.el9.noarch. 7.6 kB/s | 9.5 kB     00:01
(2/5): fail2ban-1.1.0-6.el9.noarch.rpm        7.3 kB/s | 9.3 kB     00:01
(3/5): fail2ban-sendmail-1.1.0-6.el9.noarch.r 428 kB/s |  12 kB     00:00
(4/5): fail2ban-server-1.1.0-6.el9.noarch.rpm 3.7 MB/s | 465 kB     00:00
(5/5): fail2ban-selinux-1.1.0-6.el9.noarch.rp  22 kB/s |  31 kB     00:01
--------------------------------------------------------------------------------
Total                                          5.1 kB/s | 527 kB     01:43
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Installing       : fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
  Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch                    1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower
priority 100 with module at priority 200.
```

Рис. 3.1: Установка fail2ban

Запускаю сервер fail2ban (рис. [3.2]).

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

Рис. 3.2: Запускаю сервер fail2ban

В доп. терминале запускаю просмотр журнала событий этой службы (рис. [3.3]).

```
[user@server ~]$ sudo -i
[sudo] password for user:
[root@server ~]# tail -f /var/log/fail2ban.log
2026-02-12 19:15:55,634 fail2ban.server         [8868]: INFO    --------------
----------------------------------
2026-02-12 19:15:55,634 fail2ban.server         [8868]: INFO    Starting Fail2
ban v1.1.0
2026-02-12 19:15:55,634 fail2ban.observer       [8868]: INFO    Observer start
...
2026-02-12 19:15:55,638 fail2ban.database       [8868]: INFO    Connected to f
ail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-12 19:15:55,639 fail2ban.database       [8868]: WARNING New database c
reated. Version '4'
```

Рис. 3.3: Журнал событий сервера fail2ban

Создаю конфигурационный файл с локальной конфигурацией и вношу в него строки, отвечающие за время блокировки(1 час) и защиту SSH (рис. [3.4]).

Open

*customisation.local
/etc/fail2ban/jail.d

```
1 [DEFAULT]
2 bantime = 3600
3 #
4 # SSH servers
5 #
6 [sshd]
7 port = ssh,2022
8 enabled = true
9 [sshd-ddos]
10 filter = sshd
11 enabled = true
12 [selinux-ssh]
13 enabled = true
```

Рис. 3.4: customisation.local

Перезапускаю fail2ban и в журнале вижу, что защита shh была активирована (рис. [3.5]).

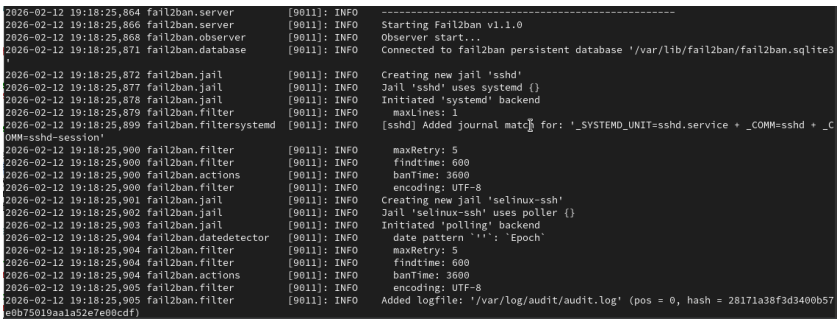

Рис. 3.5: Удачная активация настроенных параметров

Теперь включаю защиту HTTP (рис. [3.6]).

```
#
# 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
```

Рис. 3.6: Включение защиты HTTP

Перезапускаю fail2ban и в журнале вижу, что произошла удачная активация защиты HTTP (рис. [3.7]).

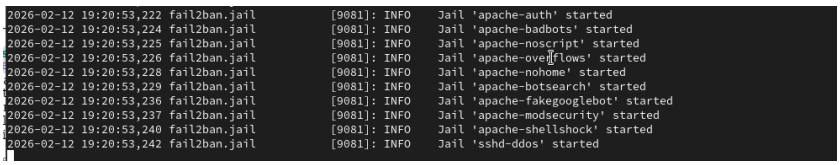

Рис. 3.7: Удачная активация защиты HTTP

В завершение, включаем защиту почты (рис. [3.8]).

Рис. 3.8: Включение защиты почты

Перезапускаю fail2ban и в журнале вижу, что произошла удачная активация защиты почты (рис. [3.9]).

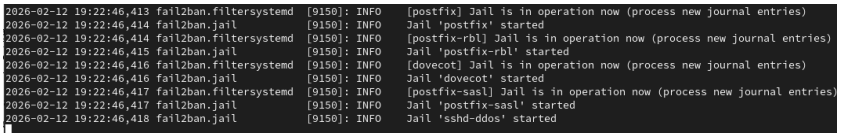

Рис. 3.9: Удачная активация защиты почты

3.2 Проверка работы Fail2ban

Проверяю, что все 16 параметров находятся под защитой (рис. [3.10]).

```
[root@server ~]# 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 ~]#
```

Рис. 3.10: Проверка списков служб, находящихся под защитой

Просматриваю статус защиты sshd (рис. [3.11]).

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

Рис. 3.11: Статус защиты sshd

Устанавливаю максимальное кол-во ошибок равным 2 (рис. [3.12]).

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

Рис. 3.12: Коррекция максимального кол-ва ошибок

Этапы проверки защиты, путём попыток получить доступ к серверу с клиента, я намеренно пропустил из-за тех же проблем, что и до этого у меня наблюдались

3.3 Внесение изменений в настройки внутреннего окружения виртуальных машин

Вношу файл локальной конфигурации в каталог с настройками внутреннего окружения машины server (рис. [3.13]).

```
[root@server ~]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protec
t/etc/fail2ban/jail.d/
[root@server server]#
```

Рис. 3.13: Настройка параметров внутреннего окружения

Создаю скрипт protect.sh, который будет повторять ключевые действия, совершённые на машине server за время выполнения лабораторной работы, при запуске сервера (рис. [3.14]).

Open

protect.sh
/vagrant/provision/server

```
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Install needed packages"
6 dnf -y install fail2ban
7
8 echo "Copy configuration files"
9 cp -R /vagrant/provision/server/protect/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start fail2ban service"
13 systemctl enable fail2ban
14 systemctl start fail2ban
```

Рис. 3.14: protect.sh

Для отработки скрипта добавляю записи для сервера в Vagrantfile (рис. [3.15]).

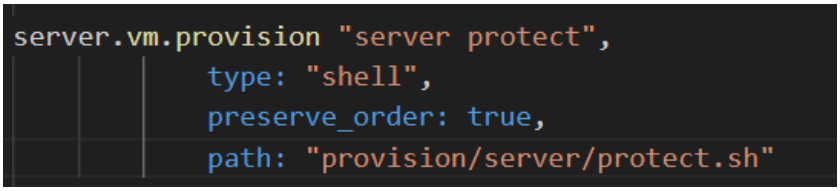

Рис. 3.15: Правки в Vagrantfile

4 Выводы

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

Список литературы

Администрирование сетевых подсисем