

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №16

дисциплина: администрирование локальных подсистем

Студент:

Яссин

Группа: НПИбд-02-20

МОСКВА

2021 г.

Постановка задачи

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

Выполнение работы

16.4.1. Защита с помощью Fail2ban

1. На сервере установил fail2ban:

```
Installed:
  esmtp-1.2-19.el9.x86_64                fail2ban-1.0.1-2.el9.noarch
  fail2ban-firewalld-1.0.1-2.el9.noarch fail2ban-sendmail-1.0.1-2.el9.noarch
  fail2ban-server-1.0.1-2.el9.noarch     libesmtp-1.0.6-24.el9.x86_64
  liblockfile-1.14-10.el9.x86_64

Complete!
[root@server server]#
```

2. Запустил сервер fail2ban:

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

3. В дополнительном терминале запустил просмотр журнала событий fail2ban:

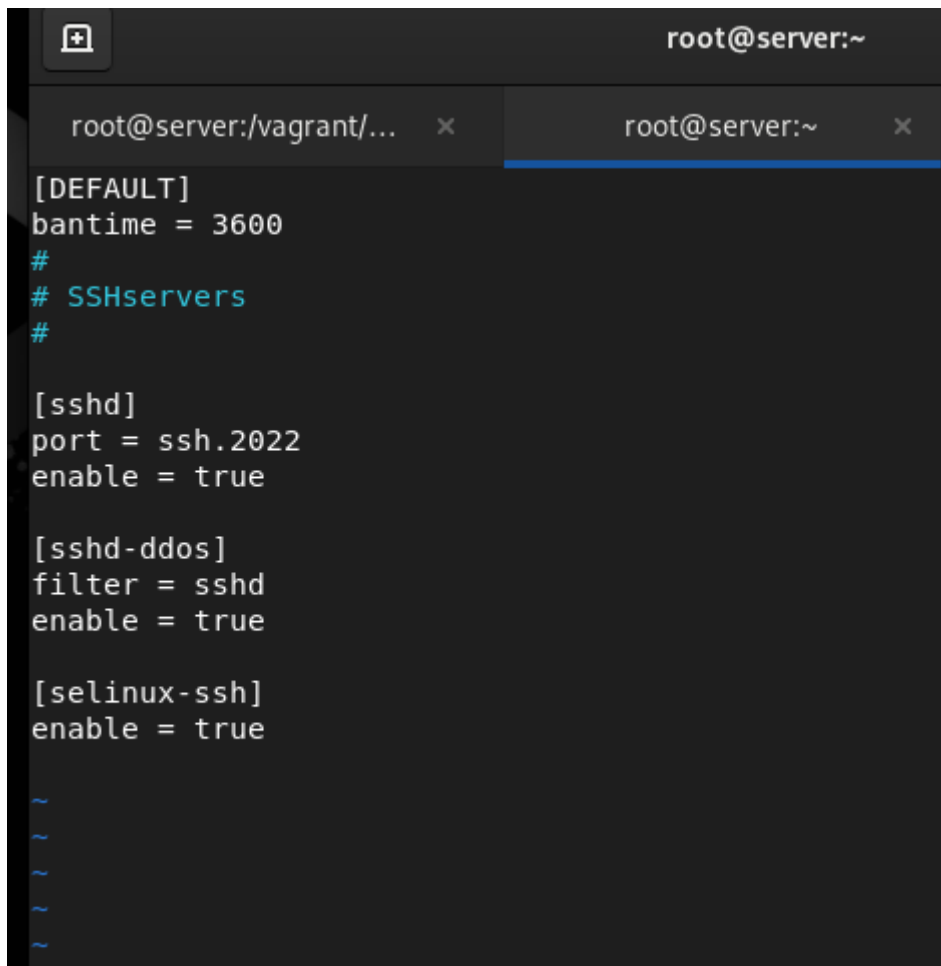
```
[root@server server]# tail -f /var/log/fail2ban.log
2023-01-07 17:40:53,790 fail2ban.server [124240]: INFO -----
-----
2023-01-07 17:40:53,790 fail2ban.server [124240]: INFO Starting Fail2
ban v1.0.1
2023-01-07 17:40:53,791 fail2ban.observer [124240]: INFO Observer start
...
2023-01-07 17:40:53,804 fail2ban.database [124240]: INFO Connected to f
ail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-01-07 17:40:53,807 fail2ban.database [124240]: WARNING New database c
reated. Version '4'
```

4. Создал файл с локальной конфигурацией fail2ban:

```
[root@server ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@server ~]# vi /etc/fail2ban/jail.d/customisation.local
[root@server ~]# systemctl restart fail2ban
```

5. В файле /etc/fail2ban/jail.d/customisation.local:

- (a) задал время блокирования на 1 час
- (b) включил защиту SSH

A terminal window with a dark background. The title bar shows 'root@server:~'. There are two tabs: 'root@server:/vagrant/...' and 'root@server:~'. The active tab shows the following configuration for fail2ban:

```
[DEFAULT]
bantime = 3600
#
# SSHservers
#

[sshd]
port = ssh.2022
enable = true

[sshd-ddos]
filter = sshd
enable = true

[selinux-ssh]
enable = true

~
~
~
~
~
```

6. Перезапустил fail2ban

```
[root@server ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@server ~]# vi /etc/fail2ban/jail.d/customisation.local
[root@server ~]# systemctl restart fail2ban
```

7. Посмотрел журнал событий:

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

```
#
# HTTP servers
#
[apache-auth]
enable = true

[apache-badbots]
enabled = true

[apache-noscript]
enabled = true

[apache-overflows]
enable = true

[apache-botsearch]
enable = true

[apache-fakegooglebot]
enable = true

[apache-modsecurity]
enable = true

[apache-shellshock]
enable = true
```

9. Перезапустил fail2ban

```
[root@server ~]# vi /etc/fail2ban/jail.d/customisation.local
[root@server ~]# systemctl restart fail2ban
```

10. Посмотрел журнал событий:

```
-----
2023-01-07 17:45:11,853 fail2ban.server [124373]: INFO Starting Fail2ban v1.0.1
2023-01-07 17:45:11,854 fail2ban.observer [124373]: INFO Observer start...
2023-01-07 17:45:11,856 fail2ban.database [124373]: INFO Connected to fail2ban persis
tent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-01-07 17:52:22,299 fail2ban.server [124373]: INFO Shutdown in progress...
2023-01-07 17:52:22,299 fail2ban.observer [124373]: INFO Observer stop ... try to end
queue 5 seconds
2023-01-07 17:52:22,320 fail2ban.observer [124373]: INFO Observer stopped, 0 events r
emaining.
2023-01-07 17:52:22,362 fail2ban.server [124373]: INFO Stopping all jails
2023-01-07 17:52:22,362 fail2ban.database [124373]: INFO Connection to database close
d.
2023-01-07 17:52:22,363 fail2ban.server [124373]: INFO Exiting Fail2ban
2023-01-07 17:52:22,788 fail2ban.server [124390]: INFO -----
-----
2023-01-07 17:52:22,788 fail2ban.server [124390]: INFO Starting Fail2ban v1.0.1
2023-01-07 17:52:22,789 fail2ban.observer [124390]: INFO Observer start...
2023-01-07 17:52:22,795 fail2ban.database [124390]: INFO Connected to fail2ban persis
tent database '/var/lib/fail2ban/fail2ban.sqlite3'
```

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

```
#
# Mail servers
#

[postfix]
enable = true

[postfix-rbl]
enable=true

[dovecot]
enable = true

[postfix-sasl]
enable = true
```

12. Перезапустил fail2ban:

```
[root@server ~]# systemctl restart fail2ban
[root@server ~]# systemctl restart fail2ban
[root@server ~]#
```

После исправления синтаксических ошибок и добавления строки “filter = sshd” под [sshd-ddos]:

```
2023-01-07 17:56:19,227 fail2ban.observer [124390]: INFO Observer stop ... try to end
queue 5 seconds
2023-01-07 17:56:19,249 fail2ban.observer [124390]: INFO Observer stopped, 0 events r
emaining.
2023-01-07 17:56:19,290 fail2ban.server [124390]: INFO Stopping all jails
2023-01-07 17:56:19,291 fail2ban.database [124390]: INFO Connection to database close
d.
2023-01-07 17:56:19,291 fail2ban.server [124390]: INFO Exiting Fail2ban
2023-01-07 17:56:19,920 fail2ban.server [124403]: INFO -----
2023-01-07 17:56:19,920 fail2ban.server [124403]: INFO Starting Fail2ban v1.0.1
2023-01-07 17:56:19,921 fail2ban.observer [124403]: INFO Observer start...
2023-01-07 17:56:19,929 fail2ban.database [124403]: INFO Connected to fail2ban persis
tent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-01-07 17:56:29,495 fail2ban.server [124403]: INFO Shutdown in progress...
2023-01-07 17:56:29,495 fail2ban.observer [124403]: INFO Observer stop ... try to end
queue 5 seconds
2023-01-07 17:56:29,516 fail2ban.observer [124403]: INFO Observer stopped, 0 events r
emaining.
2023-01-07 17:56:29,558 fail2ban.server [124403]: INFO Stopping all jails
2023-01-07 17:56:29,559 fail2ban.database [124403]: INFO Connection to database close
d.
2023-01-07 17:56:29,560 fail2ban.server [124403]: INFO Exiting Fail2ban
2023-01-07 17:56:30,050 fail2ban.server [124412]: INFO -----
2023-01-07 17:56:30,051 fail2ban.server [124412]: INFO Starting Fail2ban v1.0.1
2023-01-07 17:56:30,051 fail2ban.observer [124412]: INFO Observer start...
2023-01-07 17:56:30,060 fail2ban.database [124412]: INFO Connected to fail2ban persis
tent database '/var/lib/fail2ban/fail2ban.sqlite3'
```

16.4.2. Проверка работы Fail2ban

1. На сервере посмотрел статус fail2ban:

```
[root@server ~]# fail2ban-client status
Status
|- Number of jail:      0
`- Jail list:
[root@server ~]#
```

2. Посмотрел статус защиты SSH в fail2ban:

```
- Jail list:
[root@server ~]# fail2ban-client status sshd
2023-01-07 17:58:38,557 fail2ban [124422]: ERROR NOK: ('sshd',)
Sorry but the jail 'sshd' does not exist
[root@server ~]#
```

3. Установил максимальное количество ошибок для SSH, равное 2:

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

5. На сервере посмотрел статус защиты SSH:

(В первый раз блокировка не попала на запись, пришлось повторить)

6. Разблокировал IP-адрес клиента:

7. Вновь посмотрел статус защиты SSH

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

```
enable = true
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 <10.0.2.15>
-- INSERT --
```

9. Перезапустил fail2ban.

```
[root@server jail.d]# systemctl restart fail2ban
[root@server jail.d]#
```

10. Посмотрел журнал событий:

```

[root@server jail.d]# systemctl restart fail2ban
[root@server jail.d]# tail -f /var/log/fail2ban.log
2023-01-07 17:56:30,060 fail2ban.database [124412]: INFO Connected to fail2ban persis
tent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-01-07 17:58:38,556 fail2ban.transmitter [124412]: ERROR Command ['status', 'sshd'] h
as failed. Received UnknownJailException('sshd')
2023-01-07 17:59:21,413 fail2ban.transmitter [124412]: ERROR Command ['set', 'sshd', 'max
retry', '2'] has failed. Received UnknownJailException('sshd')
2023-01-07 18:01:13,487 fail2ban.transmitter [124412]: ERROR Command ['status', 'sshd'] h
as failed. Received UnknownJailException('sshd')
2023-01-07 18:05:08,589 fail2ban.server [124412]: INFO Shutdown in progress...
2023-01-07 18:05:08,589 fail2ban.observer [124412]: INFO Observer stop ... try to end
queue 5 seconds
2023-01-07 18:05:08,610 fail2ban.observer [124412]: INFO Observer stopped, 0 events r
emaining.
2023-01-07 18:05:08,652 fail2ban.server [124412]: INFO Stopping all jails
2023-01-07 18:05:08,653 fail2ban.database [124412]: INFO Connection to database close
d.
2023-01-07 18:05:08,653 fail2ban.server [124412]: INFO Exiting Fail2ban

```

11. Вновь попытался войти с клиента на сервер с неправильным паролем и посмотрел статус защиты SSH

Вывод

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