

Отчёт по лабораторной работе 16

Базовая защита от атак типа "brute force"

Цвелев С.А. НПИБд-02-22

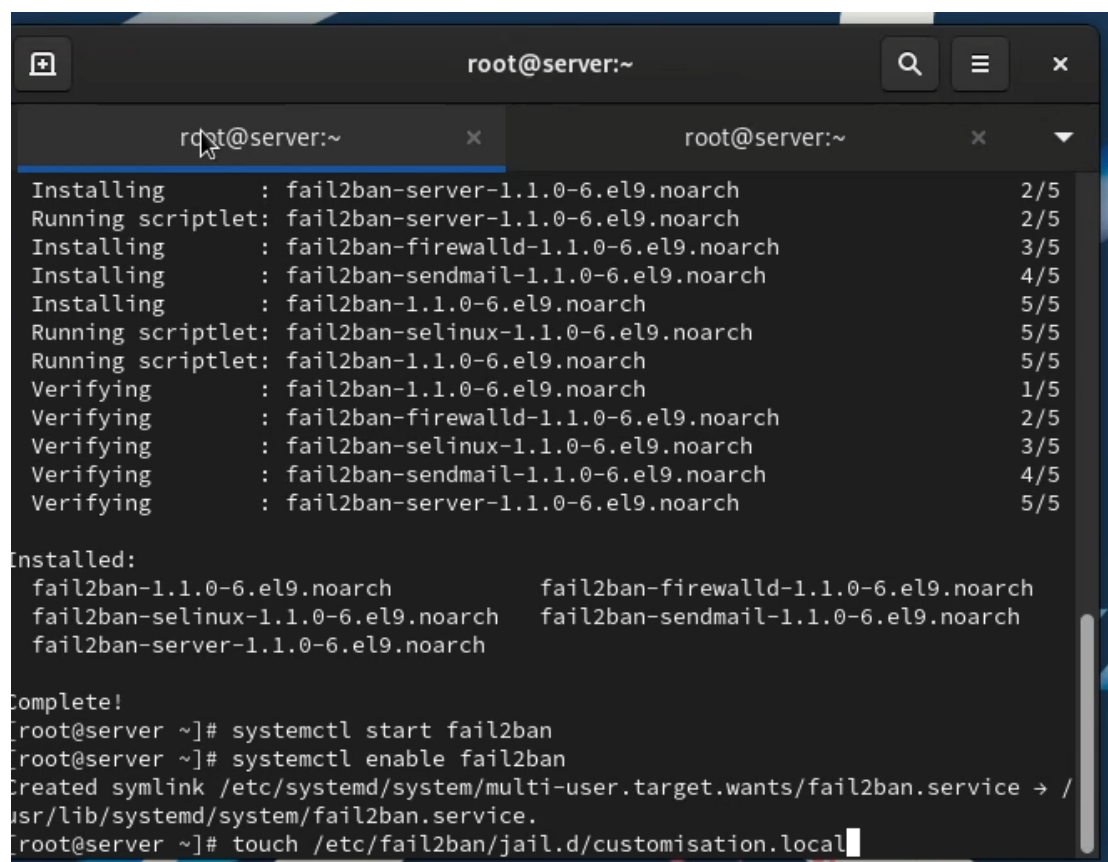
Содержание

1 Цель работы

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

2 Ход работы

Запускаем машину server и устанавливаем необходимые пакеты Fail2ban. Создаем файл customisation.local после запуска службы. В этом файле включаем защиту SSH и задаем время блокирования на 3600 секунд.



```
root@server:~  
Installing      : fail2ban-server-1.1.0-6.el9.noarch      2/5  
Running scriptlet: fail2ban-server-1.1.0-6.el9.noarch      2/5  
Installing      : fail2ban-firewalld-1.1.0-6.el9.noarch    3/5  
Installing      : fail2ban-sendmail-1.1.0-6.el9.noarch     4/5  
Installing      : fail2ban-1.1.0-6.el9.noarch              5/5  
Running scriptlet: fail2ban-selinux-1.1.0-6.el9.noarch      5/5  
Running scriptlet: fail2ban-1.1.0-6.el9.noarch              5/5  
Verifying       : fail2ban-1.1.0-6.el9.noarch              1/5  
Verifying       : fail2ban-firewalld-1.1.0-6.el9.noarch     2/5  
Verifying       : fail2ban-selinux-1.1.0-6.el9.noarch       3/5  
Verifying       : fail2ban-sendmail-1.1.0-6.el9.noarch      4/5  
Verifying       : fail2ban-server-1.1.0-6.el9.noarch        5/5  
  
Installed:  
fail2ban-1.1.0-6.el9.noarch      fail2ban-firewalld-1.1.0-6.el9.noarch  
fail2ban-selinux-1.1.0-6.el9.noarch fail2ban-sendmail-1.1.0-6.el9.noarch  
fail2ban-server-1.1.0-6.el9.noarch  
  
Complete!  
[root@server ~]# systemctl start fail2ban  
[root@server ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.  
[root@server ~]# touch /etc/fail2ban/jail.d/customisation.local
```

A terminal window titled 'root@server:~' with a search icon, a menu icon, and a close icon in the top right. It contains two tabs, both labeled 'root@server:~'. The active tab shows the following configuration:

```
[DEFAULT]
bantime = 3600

#
# SSH servers
#

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

At the bottom, there is a status bar with '-- INSERT --' on the left, '17,15' in the center, and 'All' on the right.

Перезапускаем службу. Включаем защиту HTTP.

A terminal window titled 'root@server:~' with a search icon, a menu icon, and a close icon in the top right. It contains two tabs, both labeled 'root@server:~'. The active tab shows the following configuration:

```
[apache-noscript]
enabled = true

[apache-overflows]
enabled = true

[apache-nohome]
enabled = true

[apache-botsearch]
enabled = true

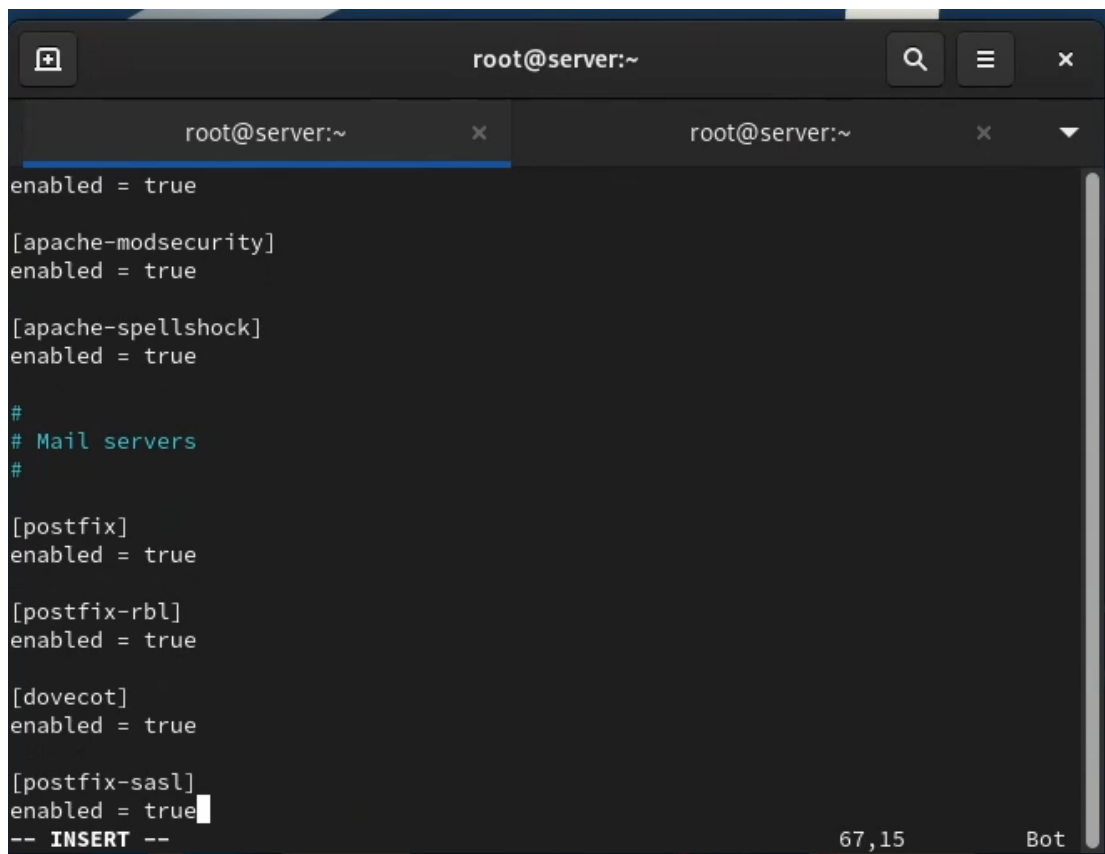
[apache-botsearch]
enabled = true

[apache-fakegooglebot]
enabled = true

[apache-modsecurity]
enabled = true
```

At the bottom, there is a status bar with '-- INSERT --' on the left, '50,1' in the center, and 'Bot' on the right.

Включаем защиту почты.



A terminal window titled 'root@server:~' with two tabs. The active tab shows the following configuration:

```
enabled = true

[apache-modsecurity]
enabled = true

[apache-spellshock]
enabled = true

#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
-- INSERT --
```

The bottom right corner of the terminal displays '67,15' and 'Bot'.

Перезапускаем службу. Проверяем статус fail2ban и проверяем его работу с клиента.

3 Вывод

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