

Защита лабораторной работы №16

дисциплина: администрирование сетевых подсистем

Студент: Оулед сале яссин

Группа: НПИбд-02-20

Постановка задачи

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

Защита с помощью 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]#
```

```
root@server:~
root@server:/vagrant/... x root@server:~ x
[DEFAULT]
bantime = 3600
#
# SSHservers
#

[sshd]
port = ssh.2022
enable = true

[sshd-ddos]
filter = sshd
enable = true

[selinux-ssh]
enable = true
```

```
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

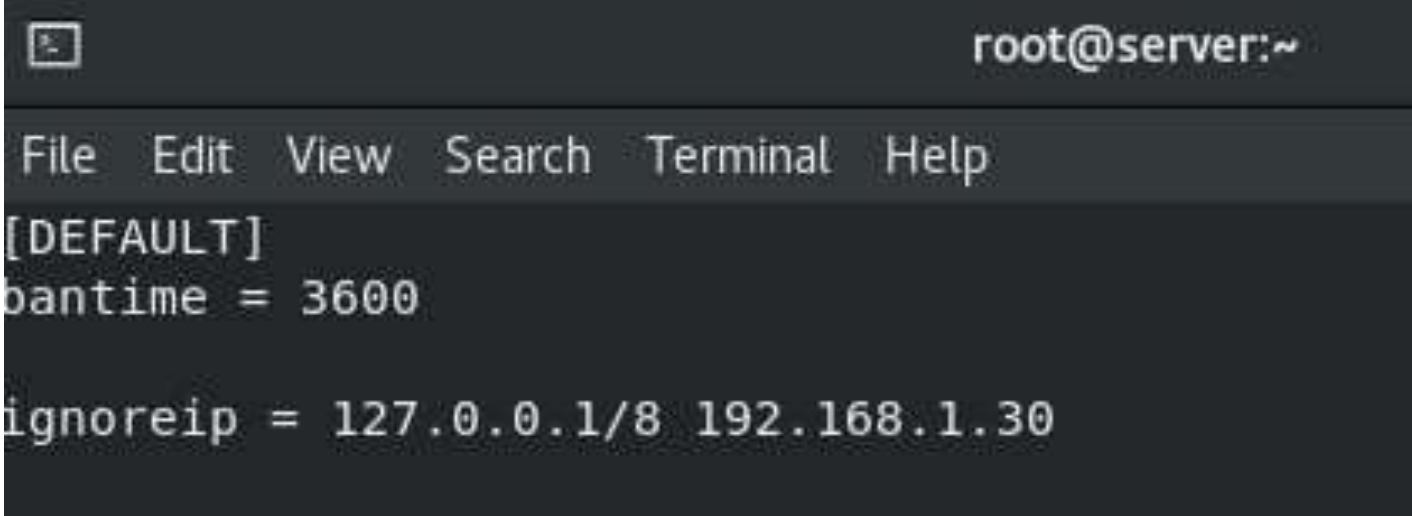
Complete!
[root@server server]#
```

Проверка работы 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 ~]#
```

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

Проверка работы Fail2ban



```
root@server:~  
File Edit View Search Terminal Help  
[DEFAULT]  
bantime = 3600  
  
ignoreip = 127.0.0.1/8 192.168.1.30
```

A terminal window with a dark background and light gray text. The title bar at the top shows a window icon on the left and the text 'root@server:~' on the right. Below the title bar is a menu bar with the items 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main content area of the terminal displays the following text: '[DEFAULT]', 'bantime = 3600', a blank line, and 'ignoreip = 127.0.0.1/8 192.168.1.30'.

Проверка работы Fail2ban

```
2021-12-23 18:38:13,741 fail2ban.jail      [10101]: INFO    Jail 'postfix-sasl' started
2021-12-23 18:38:13,796 fail2ban.jail      [10101]: INFO    Jail 'sshd-ddos' started
2021-12-23 18:40:41,815 fail2ban.filter  [10101]: INFO    [sshd] Ignore 192.168.1.30 by ip
2021-12-23 18:40:41,817 fail2ban.filter  [10101]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

Вывод

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