

Лабораторная работа 16

Ярметов Камран

17 февраля, 2023,, Москва, Россия

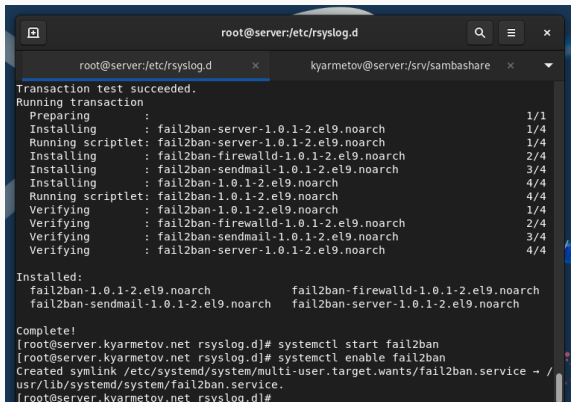
Российский Университет Дружбы Народов

Цель лабораторной работы

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

Выполнение лабораторной работы

Защита с помощью Fail2ban



A terminal window titled 'root@server:/etc/rsyslog.d' showing the installation of Fail2ban services. The window has two tabs: 'root@server:/etc/rsyslog.d' and 'kyarmetov@server:/srv/sambashare'. The output shows a successful transaction test, followed by the installation of four services: fail2ban-server, fail2ban-firewalld, fail2ban-sendmail, and fail2ban. Each service is installed and verified. The installation is complete, and the services are started and enabled using systemctl. A symlink is also created for the fail2ban.service.

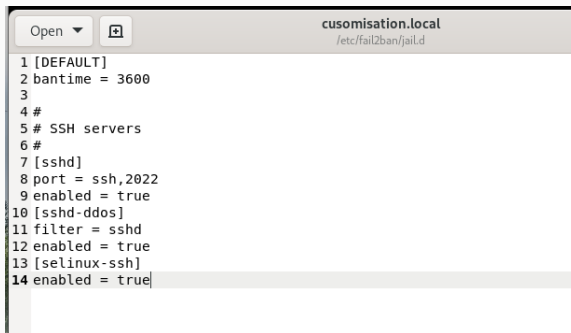
```
Transaction test succeeded.
Running transaction
  Preparing                : 1/1
  Installing                : fail2ban-server-1.0.1-2.el9.noarch 1/4
  Running scriptlet: fail2ban-server-1.0.1-2.el9.noarch 1/4
  Installing                : fail2ban-firewalld-1.0.1-2.el9.noarch 2/4
  Installing                : fail2ban-sendmail-1.0.1-2.el9.noarch 3/4
  Installing                : fail2ban-1.0.1-2.el9.noarch 4/4
  Running scriptlet: fail2ban-1.0.1-2.el9.noarch 4/4
  Verifying                : fail2ban-1.0.1-2.el9.noarch 1/4
  Verifying                : fail2ban-firewalld-1.0.1-2.el9.noarch 2/4
  Verifying                : fail2ban-sendmail-1.0.1-2.el9.noarch 3/4
  Verifying                : fail2ban-server-1.0.1-2.el9.noarch 4/4

Installed:
  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

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

Figure 1: установка службы

Защита с помощью Fail2ban

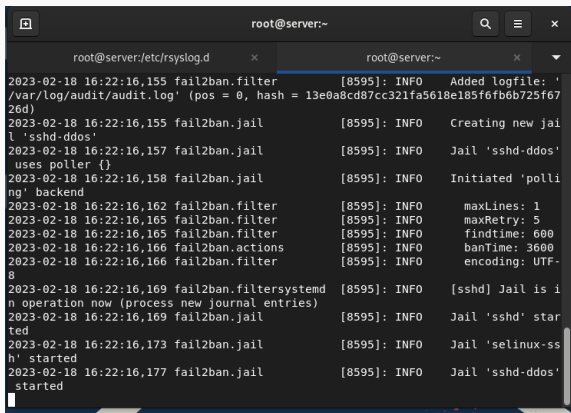


```
cusomisation.local
/etc/fail2ban/jail.d

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

Figure 2: файл `/etc/fail2ban/jail.d/customisation.local`

Защита с помощью Fail2ban



The screenshot shows a terminal window with a dark theme. The title bar indicates the user is 'root@server:~'. There are two tabs open: 'root@server:/etc/rsyslog.d' and 'root@server:~'. The active tab shows a log of Fail2ban service startup. The logs are timestamped '2023-02-18 16:22:16' and show the progression from adding a logfile to starting various jails like 'sshd-ddos', 'selinux-ss', and 'sshd'.

```
root@server:/etc/rsyslog.d x root@server:~ x
2023-02-18 16:22:16,155 fail2ban.filter [8595]: INFO Added logfile: '
/var/log/audit/audit.log' (pos = 0, hash = 13e0a8cd87cc321fa5618e185f6fb6b725f67
26d)
2023-02-18 16:22:16,155 fail2ban.jail [8595]: INFO Creating new jai
l 'sshd-ddos'
2023-02-18 16:22:16,157 fail2ban.jail [8595]: INFO Jail 'sshd-ddos'
uses poller {}
2023-02-18 16:22:16,158 fail2ban.jail [8595]: INFO Initiated 'polli
ng' backend
2023-02-18 16:22:16,162 fail2ban.filter [8595]: INFO maxLines: 1
2023-02-18 16:22:16,165 fail2ban.filter [8595]: INFO maxRetry: 5
2023-02-18 16:22:16,165 fail2ban.filter [8595]: INFO findtime: 600
2023-02-18 16:22:16,166 fail2ban.actions [8595]: INFO banTime: 3600
2023-02-18 16:22:16,166 fail2ban.filter [8595]: INFO encoding: UTF-
8
2023-02-18 16:22:16,169 fail2ban.filterssystemd [8595]: INFO [sshd] Jail is i
n operation now (process new journal entries)
2023-02-18 16:22:16,169 fail2ban.jail [8595]: INFO Jail 'sshd' star
ted
2023-02-18 16:22:16,173 fail2ban.jail [8595]: INFO Jail 'selinux-ss
h' started
2023-02-18 16:22:16,177 fail2ban.jail [8595]: INFO Jail 'sshd-ddos'
started
```

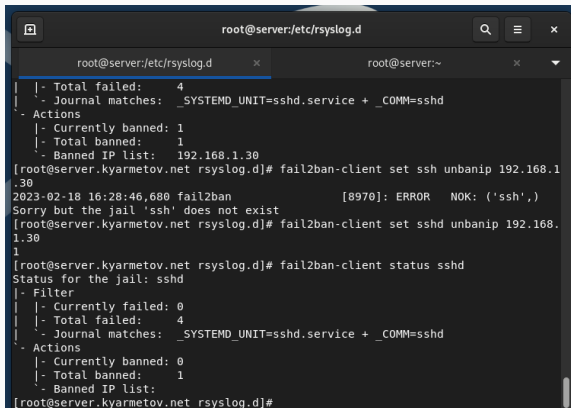
Figure 3: лог службы fail2ban

Проверка работы Fail2ban

```
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client status
Status
|- Number of jail:      16
|_ Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegoogle
bot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, apach
e-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, ss
hd-ddos
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:     0
| |- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 0
| |- Total banned:     0
|_- Banned IP list:
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client status sshd maxretry 2
2023-02-18 16:27:17,188 fail2ban [8947]: ERROR NOK: ('Invalid c
ommand (no status)',)
Invalid command (no status)
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client set sshd maxretry 2
2
[root@server.kyarmetov.net rsyslog.d]#
```

Figure 4: статус службы

Проверка работы Fail2ban

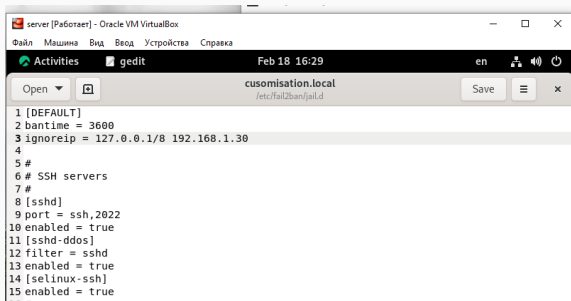


The screenshot shows a terminal window with two tabs. The active tab is titled 'root@server:~' and displays the output of the 'fail2ban-client status sshd' command. The output shows that the 'ssh' jail has 4 total failures, 1 currently banned IP (192.168.1.30), and 1 total banned IP. The other tab is titled 'root@server:/etc/rsyslog.d' and shows the output of the 'fail2ban-client set sshd unbanip 192.168.1.30' command, which returns an error: '[8970]: ERROR NOK: ('ssh',) Sorry but the jail 'ssh' does not exist'.

```
root@server:/etc/rsyslog.d
| - Total failed: 4
|   - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
| - Actions
|   - Currently banned: 1
|   - Total banned: 1
|   - Banned IP list: 192.168.1.30
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client set ssh unbanip 192.168.1.30
2023-02-18 16:28:46,680 fail2ban [8970]: ERROR NOK: ('ssh',)
Sorry but the jail 'ssh' does not exist
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.kyarmetov.net rsyslog.d]# fail2ban-client status sshd
Status for the jail: sshd
| - Filter
|   - Currently failed: 0
|   - Total failed: 4
|   - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
| - Actions
|   - Currently banned: 0
|   - Total banned: 1
|   - Banned IP list:
[root@server.kyarmetov.net rsyslog.d]#
```

Figure 5: статус службы

Проверка работы Fail2ban



```
server [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  gedit  Feb 18 16:29  en  [system icons]
Open  [icon]  cusomisation.local  Save  [menu]  x
/etc/fail2ban/jail.d

1 [DEFAULT]
2 bantime = 3600
3 ignoreip = 127.0.0.1/8 192.168.1.30
4
5 #
6 # SSH servers
7 #
8 [sshd]
9 port = ssh,2022
10 enabled = true
11 [sshd-ddos]
12 filter = sshd
13 enabled = true
14 [selinux-ssh]
15 enabled = true
```

Figure 6: опция ignore

Приобретены практические навыки работы с fail2ban