

Лабораторная работа №16

Администрирование сетевых подсистем

Мишина А. А.

5 декабря 2024

Цели и задачи

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

Защита с помощью Fail2ban

Выполнение лабораторной работы

```
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch          1/5
libsemanage.semanage_direct_install_info: Overriding fail2ban module at lower priority 100 with module at
priority 200.

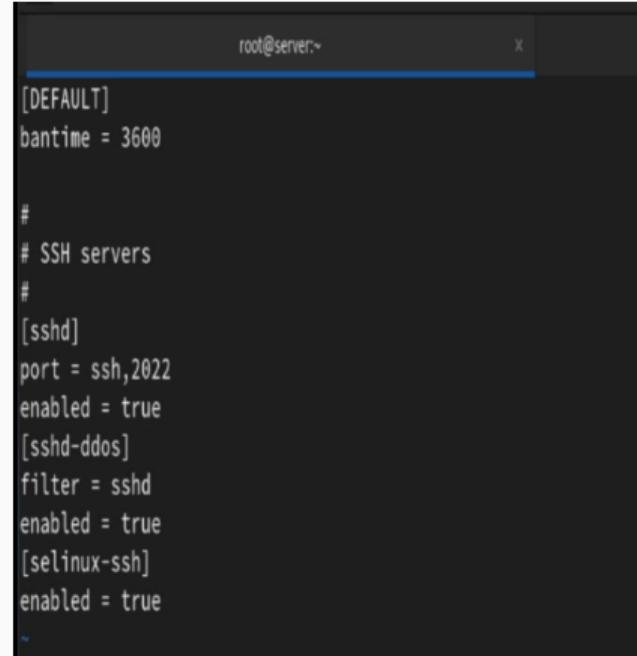
Installing : fail2ban-server-1.0.2-12.el9.noarch                2/5
Running scriptlet: fail2ban-server-1.0.2-12.el9.noarch
Installing : fail2ban-firewalld-1.0.2-12.el9.noarch              3/5
Installing : fail2ban-sendmail-1.0.2-12.el9.noarch               4/5
Installing : fail2ban-1.0.2-12.el9.noarch                         5/5
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch
Running scriptlet: fail2ban-1.0.2-12.el9.noarch
Verifying   : fail2ban-1.0.2-12.el9.noarch                         1/5
Verifying   : fail2ban-firewalld-1.0.2-12.el9.noarch               2/5
Verifying   : fail2ban-selinux-1.0.2-12.el9.noarch                 3/5
Verifying   : fail2ban-sendmail-1.0.2-12.el9.noarch               4/5
Verifying   : fail2ban-server-1.0.2-12.el9.noarch                 5/5

Installed:
fail2ban-1.0.2-12.el9.noarch                      fail2ban-firewalld-1.0.2-12.el9.noarch
fail2ban-selinux-1.0.2-12.el9.noarch            fail2ban-sendmail-1.0.2-12.el9.noarch
fail2ban-server-1.0.2-12.el9.noarch

Complete!
[root@server.aamishina.net ~]# systemctl start fail2ban
[root@server.aamishina.net ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fa
il2ban.service.
[root@server.aamishina.net ~]#
```

Рис. 1: Установка и запуск fail2ban

Выполнение лабораторной работы



The screenshot shows a terminal window with a dark background and light-colored text. The title bar indicates the session is running as 'root@server:~'. The content of the terminal shows a configuration file with several sections and parameters:

```
[DEFAULT]
bantime = 3600

#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
"
```

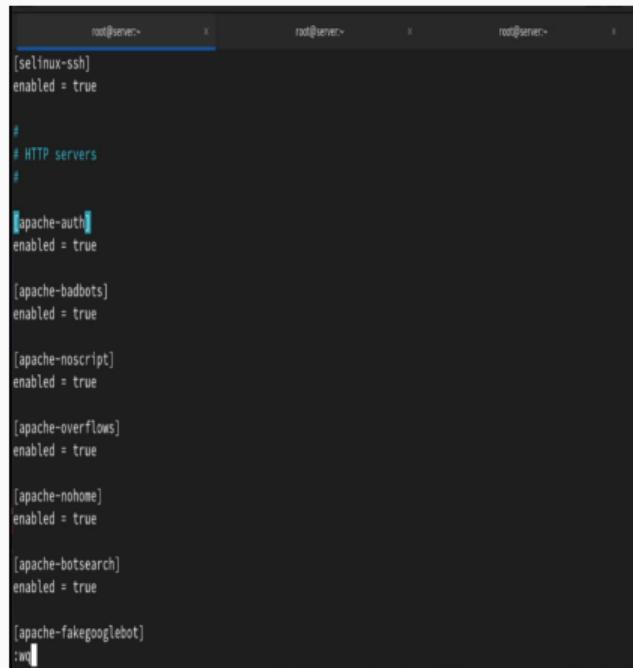
Рис. 2: Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH

Выполнение лабораторной работы

root@server~		root@server~
2024-10-27 18:04:10,141 fail2ban.jail	[19371]: INFO	Jail 'sshd' uses systemd ()
2024-10-27 18:04:10,145 fail2ban.jail	[19371]: INFO	Initiated 'systemd' backend
2024-10-27 18:04:10,145 fail2ban.filter	[19371]: INFO	maxLines: 1
2024-10-27 18:04:10,145 fail2ban.filtersystemd	[19371]: INFO	[sshd] Added journal match for: '_SYSTEMD_UNIT:sshd.service _COMM:sshd'
2024-10-27 18:04:10,156 fail2ban.filter	[19371]: INFO	maxRetry: 5
2024-10-27 18:04:10,156 fail2ban.filter	[19371]: INFO	findtime: 600
2024-10-27 18:04:10,156 fail2ban.actions	[19371]: INFO	banTime: 3600
2024-10-27 18:04:10,156 fail2ban.filter	[19371]: INFO	encoding: UTF-8
2024-10-27 18:04:10,157 fail2ban.jail	[19371]: INFO	Creating new jail 'selinux-ssh'
2024-10-27 18:04:10,158 fail2ban.jail	[19371]: INFO	Jail 'selinux-ssh' uses poller { }
2024-10-27 18:04:10,158 fail2ban.jail	[19371]: INFO	Initiated 'polling' backend
2024-10-27 18:04:10,159 fail2ban.detectedator	[19371]: INFO	date pattern ' ': 'Epoch'
2024-10-27 18:04:10,159 fail2ban.filter	[19371]: INFO	maxRetry: 5
2024-10-27 18:04:10,159 fail2ban.filter	[19371]: INFO	findtime: 600
2024-10-27 18:04:10,159 fail2ban.actions	[19371]: INFO	banTime: 3600
2024-10-27 18:04:10,159 fail2ban.filter	[19371]: INFO	encoding: UTF-8
2024-10-27 18:04:10,161 fail2ban.filter	[19371]: INFO	Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 4988764af605b052d47597b5d6de03502070)
2024-10-27 18:04:10,162 fail2ban.jail	[19371]: INFO	Creating new jail 'sshd-ddos'
2024-10-27 18:04:10,163 fail2ban.jail	[19371]: INFO	Jail 'sshd-ddos' uses poller {}
2024-10-27 18:04:10,163 fail2ban.jail	[19371]: INFO	Initiated 'polling' backend
2024-10-27 18:04:10,163 fail2ban.filter	[19371]: INFO	maxLines: 1
2024-10-27 18:04:10,164 fail2ban.filter	[19371]: INFO	maxRetry: 5
2024-10-27 18:04:10,164 fail2ban.filter	[19371]: INFO	findtime: 600
2024-10-27 18:04:10,164 fail2ban.actions	[19371]: INFO	banTime: 3600
2024-10-27 18:04:10,164 fail2ban.filter	[19371]: INFO	encoding: UTF-8
2024-10-27 18:04:10,199 fail2ban.jail	[19371]: INFO	Jail 'sshd' started
2024-10-27 18:04:10,203 fail2ban.filtersystemd	[19371]: INFO	[sshd] Jail is in operation now (process new journal entries)
2024-10-27 18:04:10,211 fail2ban.jail	[19371]: INFO	Jail 'selinux-ssh' started
2024-10-27 18:04:10,234 fail2ban.jail	[19371]: INFO	Jail 'sshd-ddos' started

Рис. 3: Просмотр журнала событий fail2ban

Выполнение лабораторной работы



```
root@server:~# [selinux-ssh]
root@server:~# enabled = true
#
# 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
:wq
```

Рис. 4: Редактирование файла с локальной конфигурацией: защита HTTP

Выполнение лабораторной работы

```
[2024-10-27 18:06:03,192 fail2ban.filter          [10453]: INFO  encoding: UTF-8
2024-10-27 18:06:03,193 fail2ban.filter          [10453]: INFO  Added logfile: '/var/log/httpd/server.aamishina.net-error_log' (pos = 0, hash =
2024-10-27 18:06:03,196 fail2ban.filter          [10453]: INFO  Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 2e2465c481893f641481ff27cf9b31dc9
ba40a6)
2024-10-27 18:06:03,196 fail2ban.filter          [10453]: INFO  Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 7606d2197a88a6656d717d7df899d
d74d5e9a8a)
2024-10-27 18:06:03,196 fail2ban.filter          [10453]: INFO  Added logfile: '/var/log/httpd/www.aamishina.net-error_log' (pos = 0, hash = bb968c6d06026507
466e495008b0b9ffff76df7c)
2024-10-27 18:06:03,197 fail2ban.jail          [10453]: INFO  Creating new jail 'sshd-ddos'
2024-10-27 18:06:03,197 fail2ban.jail          [10453]: INFO  Jail 'sshd-ddos' uses poller {}
2024-10-27 18:06:03,207 fail2ban.jail          [10453]: INFO  Initiated 'polling' backend
2024-10-27 18:06:03,208 fail2ban.filter          [10453]: INFO  maxlines: 1
2024-10-27 18:06:03,209 fail2ban.filter          [10453]: INFO  maxRetry: 5
2024-10-27 18:06:03,210 fail2ban.filter          [10453]: INFO  findtime: 600
2024-10-27 18:06:03,210 fail2ban.actions        [10453]: INFO  banTime: 3600
2024-10-27 18:06:03,210 fail2ban.filter          [10453]: INFO  encoding: UTF-8
2024-10-27 18:06:03,210 fail2ban.filtersystemd [10453]: INFO  [sshd] Jail is in operation now (process new journal entries)
2024-10-27 18:06:03,211 fail2ban.jail          [10453]: INFO  Jail 'sshd' started
2024-10-27 18:06:03,212 fail2ban.jail          [10453]: INFO  Jail 'selinux-ssh' started
2024-10-27 18:06:03,214 fail2ban.jail          [10453]: INFO  Jail 'apache-auth' started
2024-10-27 18:06:03,224 fail2ban.jail          [10453]: INFO  Jail 'apache-badbots' started
2024-10-27 18:06:03,231 fail2ban.jail          [10453]: INFO  Jail 'apache-noscript' started
2024-10-27 18:06:03,250 fail2ban.jail          [10453]: INFO  Jail 'apache-overflows' started
2024-10-27 18:06:03,252 fail2ban.jail          [10453]: INFO  Jail 'apache-nohome' started
2024-10-27 18:06:03,254 fail2ban.jail          [10453]: INFO  Jail 'apache-botsearch' started
2024-10-27 18:06:03,271 fail2ban.jail          [10453]: INFO  Jail 'apache-fakegooglebot' started
2024-10-27 18:06:03,273 fail2ban.jail          [10453]: INFO  Jail 'apache-modsecurity' started
2024-10-27 18:06:03,275 fail2ban.jail          [10453]: INFO  Jail 'apache-shellshock' started
2024-10-27 18:06:03,280 fail2ban.jail          [10453]: INFO  Jail 'sshd-ddos' started
```

Рис. 5: Просмотр журнала событий fail2ban

Выполнение лабораторной работы.

```
#  
# Mail servers  
#  
  
[postfix]  
enabled = true  
  
[postfix-rbl]  
enabled = true  
  
[dovecot]  
enabled = true  
  
[postfix-sasl]  
enabled = true
```

Рис. 6: Редактирование файла с локальной конфигурацией: защита почты

Выполнение лабораторной работы

```
[root@server.aamishina.net ~]# tail -f /var/log/fail2ban.log
2024-10-27 18:07:04,094 fail2ban.jail      [10548]: INFO  Jail 'apache-shellshock' started
2024-10-27 18:07:04,095 fail2ban.jail      [10548]: INFO  Jail 'postfix' started
2024-10-27 18:07:04,104 fail2ban.jail      [10548]: INFO  Jail 'postfix-rbl' started
2024-10-27 18:07:04,109 fail2ban.filtersystemd [10548]: INFO  [postfix] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,110 fail2ban.filtersystemd [10548]: INFO  [postfix-rbl] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,113 fail2ban.jail      [10548]: INFO  Jail 'dovecot' started
2024-10-27 18:07:04,117 fail2ban.filtersystemd [10548]: INFO  [postfix-sasl] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,120 fail2ban.filtersystemd [10548]: INFO  [dovecot] Jail is in operation now (process new journal entries)
2024-10-27 18:07:04,121 fail2ban.jail      [10548]: INFO  Jail 'postfix-sasl' started
2024-10-27 18:07:04,131 fail2ban.jail      [10548]: INFO  Jail 'sshd-ddos' started
```

Рис. 7: Просмотр журнала событий fail2ban

Проверка работы Fail2ban

Выполнение лабораторной работы

```
[root@server.aamishina.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity,
apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postf
ix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.aamishina.net ~]# 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.aamishina.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.aamishina.net ~]#
```

Рис. 8: Просмотр статуса службы, статус защиты SSH, установка макс. кол-ва ошибок для SSH

Выполнение лабораторной работы

```
[root@client.aamishina.net ~]# ssh aamishina@server.aamishina.net
The authenticity of host 'server.aamishina.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:9t38xEDGq4lcr5/Tsoa80ISQoztxdmZFH71zorIzZ7g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.aamishina.net' (ED25519) to the list of known hosts.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password: █
```

Рис. 9: Подключение к серверу по SSH с вводом неправильного пароля

Выполнение лабораторной работы

```
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| '- Banned IP list: 192.168.1.57
[root@server.aamishina.net ~]# fail2ban-client set sshd unbanip 192.168.1.57
1
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM:sshd
- Actions
| |- Currently banned: 0
| |- Total banned: 1
| '- Banned IP list:
[root@server.aamishina.net ~]#
```

Рис. 10: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

Выполнение лабораторной работы

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.57
#
# SSH servers
```

Рис. 11: Редактирование файла с локальной конфигурацией: игнорирование адреса клиента

Выполнение лабораторной работы

```
2024-10-27 18:16:03,456 fail2ban.filter      [10810]: INFO  [sshd] Ignore 192.168.1.57 by ip
2024-10-27 18:16:03,457 fail2ban.filtersystemd [10810]: INFO  [sshd] Jail is in operation now (process
new journal entries)
2024-10-27 18:16:03,458 fail2ban.jail       [10810]: INFO  Jail 'selinux-ssh' started
2024-10-27 18:16:03,466 fail2ban.jail       [10810]: INFO  Jail 'apache-auth' started
2024-10-27 18:16:03,470 fail2ban.jail       [10810]: INFO  Jail 'apache-baddbots' started
2024-10-27 18:16:03,478 fail2ban.jail       [10810]: INFO  Jail 'apache-noscript' started
2024-10-27 18:16:03,479 fail2ban.jail       [10810]: INFO  Jail 'apache-overflows' started
2024-10-27 18:16:03,480 fail2ban.jail       [10810]: INFO  Jail 'apache-nohome' started
2024-10-27 18:16:03,488 fail2ban.jail       [10810]: INFO  Jail 'apache-botsearch' started
2024-10-27 18:16:03,488 fail2ban.jail       [10810]: INFO  Jail 'apache-fakegooglebot' started
2024-10-27 18:16:03,489 fail2ban.jail       [10810]: INFO  Jail 'apache-modsecurity' started
2024-10-27 18:16:03,490 fail2ban.jail       [10810]: INFO  Jail 'apache-shellshock' started
2024-10-27 18:16:03,491 fail2ban.filtersystemd [10810]: INFO  [postfix] Jail is in operation now (proc
ess new journal entries)
2024-10-27 18:16:03,500 fail2ban.jail       [10810]: INFO  Jail 'postfix' started
2024-10-27 18:16:03,501 fail2ban.filtersystemd [10810]: INFO  [postfix-rbl] Jail is in operation now (
process new journal entries)
2024-10-27 18:16:03,501 fail2ban.jail       [10810]: INFO  Jail 'postfix-rbl' started
2024-10-27 18:16:03,502 fail2ban.filtersystemd [10810]: INFO  [dovecot] Jail is in operation now (proc
ess new journal entries)
2024-10-27 18:16:03,509 fail2ban.jail       [10810]: INFO  Jail 'dovecot' started
2024-10-27 18:16:03,519 fail2ban.filtersystemd [10810]: INFO  [postfix-sasl] Jail is in operation now
(process new journal entries)
2024-10-27 18:16:03,520 fail2ban.jail       [10810]: INFO  Jail 'postfix-sasl' started
2024-10-27 18:16:03,520 fail2ban.jail       [10810]: INFO  Jail 'sshd-ddos' started
```

Рис. 12: Просмотр журнала событий ‘fail2ban’

Выполнение лабораторной работы

```
[root@server.aamishina.net ~]# systemctl restart fail2ban
[root@server.aamishina.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter           I
|  |- 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.aamishina.net ~]#
```

Рис. 13: Просмотр статуса защиты SSH после неудачного входа

Внесение изменений в настройки
внутреннего окружения
виртуальной машины

Выполнение лабораторной работы

```
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/protect/etc/fail2ban/jail.d/
```

Выполнение лабораторной работы

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install fail2ban

echo "Copy configuration files"
cp -R /vagrant/provision/server/protect/etc/* /etc
restorecon -vR /etc

echo "Start fail2ban service"
systemctl enable fail2ban
systemctl start fail2ban

~
```

Рис. 14: Редактирование protect.sh на сервере

Выполнение лабораторной работы

```
server.vm.provision "server protect",
  type: "shell",
  preserve_order: true,
  path: "provision/server/protect.sh"
```

Выводы

В результате выполнения работы были получены навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».