

Лабораторная работа №16

Администрирование сетевых подсистем

Иванов Сергей Владимирович, НПИбд-01-23

07 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

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

Задание

Задание

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban

Выполнение лабораторной работы

Защита с помощью Fail2ban

```
C:\Users\1serg>cd C:\work_asp\svivanov\vagrant  
C:\work_asp\svivanov\vagrant>vagrant up server  
Bringing machine 'server' up with 'virtualbox' provider...  
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.  
==> server: This is very often used by the router and can cause the  
==> server: network to not work properly. If the network doesn't work  
==> server: properly, try changing this IP.  
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.  
==> server: This is very often used by the router and can cause the  
==> server: network to not work properly. If the network doesn't work  
==> server: properly, try changing this IP.  
==> server: Clearing any previously set forwarded ports...  
==> server: Clearing any previously set network interfaces...  
==> server: Preparing network interfaces based on configuration...
```

Рис. 1: Запуск Server

Защита с помощью Fail2ban

На сервере установим fail2ban

```
[root@server.svivanov.net ~]# dnf install fail2ban
Extra Packages for Enterprise Linux 10 - x86_64
Last metadata expiration check: 0:00:01 ago on Сб 06 дек 2025 10:53:29.
Dependencies resolved.
=====
           Package          Architecture      Version       Repository      Size
=====
Installing:
  fail2ban                noarch        1.1.0-6.el10_0    epel            9.4 k
Installing dependencies:
  fail2ban-firewalld      noarch        1.1.0-6.el10_0    epel            9.6 k
  fail2ban-selinux         noarch        1.1.0-6.el10_0    epel            31 k
  fail2ban-sendmail        noarch        1.1.0-6.el10_0    epel            12 k
  fail2ban-server          noarch        1.1.0-6.el10_0    epel           561 k
=====
Transaction Summary
=====
Install 5 Packages
```

Рис. 2: Установка fail2ban

Защита с помощью Fail2ban

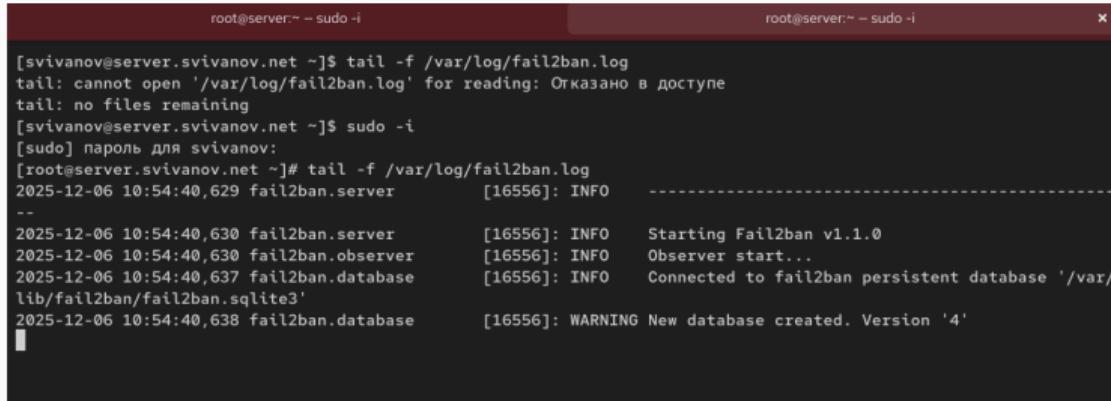
Запустим сервер fail2ban:

```
[root@server.svivanov.net ~]# systemctl start fail2ban
[root@server.svivanov.net ~]# systemctl enable fail2ban
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/u
n.service'.
[root@server.svivanov.net ~]#
```

Рис. 3: Запуск fail2ban

Защита с помощью Fail2ban

В дополнительном терминале запустим просмотр журнала событий fail2ban:



```
[svivanov@server.svivanov.net ~]$ tail -f /var/log/fail2ban.log
tail: cannot open '/var/log/fail2ban.log' for reading: Отказано в доступе
tail: no files remaining
[svivanov@server.svivanov.net ~]$ sudo -i
[sudo] пароль для svivanov:
[root@server.svivanov.net ~]# tail -f /var/log/fail2ban.log
2025-12-06 10:54:40,629 fail2ban.server      [16556]: INFO  -----
-- 
2025-12-06 10:54:40,630 fail2ban.server      [16556]: INFO  Starting Fail2ban v1.1.0
2025-12-06 10:54:40,630 fail2ban.observer    [16556]: INFO  Observer start...
2025-12-06 10:54:40,637 fail2ban.database   [16556]: INFO  Connected to fail2ban persistent database '/var/
lib/fail2ban/fail2ban.sqlite3'
2025-12-06 10:54:40,638 fail2ban.database   [16556]: WARNING New database created. Version '4'
```

Рис. 4: Запуск журнала событий

Защита с помощью Fail2ban

Создадим файл с конфигурацией. Зададим время блокирования на 1 час и включим защиту SSH:

```
[root@server.svivanov.net ~]# touch /etc/fail2ban/jail.d/customisation.local
[root@server.svivanov.net ~]# vim /etc/fail2ban/jail.d/customisation.local
[root@server.svivanov.net ~]# cat /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
[root@server.svivanov.net ~]#
```

Рис. 5: Создание конфигурации

Защита с помощью Fail2ban

```
[root@server.svivanov.net ~]# systemctl restart fail2ban  
[root@server.svivanov.net ~]# █
```

Рис. 6: Перезапуск fail2ban

Защита с помощью Fail2ban

Посмотрим журнал событий:

```
2025-12-06 10:57:15,200 fail2ban.filter      [16884]: INFO      encoding: UTF-8
2025-12-06 10:57:15,200 fail2ban.jail       [16884]: INFO      Creating new jail 'selinux-ssh'
2025-12-06 10:57:15,208 fail2ban.jail       [16884]: INFO      Jail 'selinux-ssh' uses pyinotify {}
2025-12-06 10:57:15,210 fail2ban.jail       [16884]: INFO      Initiated 'pyinotify' backend
2025-12-06 10:57:15,211 fail2ban.datedetector [16884]: INFO      date pattern '': 'Epoch'
2025-12-06 10:57:15,211 fail2ban.filter       [16884]: INFO      maxRetry: 5
2025-12-06 10:57:15,211 fail2ban.filter       [16884]: INFO      findtime: 600
2025-12-06 10:57:15,211 fail2ban.actions     [16884]: INFO      banTime: 3600
2025-12-06 10:57:15,211 fail2ban.filter       [16884]: INFO      encoding: UTF-8
2025-12-06 10:57:15,213 fail2ban.filter       [16884]: INFO      Added logfile: '/var/log/audit/audit.log' (pos =
0, hash = f216cf862ef2a1af3f16af8bb8bf79356cc8723)
2025-12-06 10:57:15,213 fail2ban.jail       [16884]: INFO      Creating new jail 'sshd-ddos'
2025-12-06 10:57:15,213 fail2ban.jail       [16884]: INFO      Jail 'sshd-ddos' uses pyinotify {}
2025-12-06 10:57:15,215 fail2ban.jail       [16884]: INFO      Initiated 'pyinotify' backend
2025-12-06 10:57:15,217 fail2ban.filter       [16884]: INFO      maxLines: 1
2025-12-06 10:57:15,217 fail2ban.filter       [16884]: INFO      maxRetry: 5
2025-12-06 10:57:15,217 fail2ban.filter       [16884]: INFO      findtime: 600
2025-12-06 10:57:15,217 fail2ban.actions     [16884]: INFO      banTime: 3600
2025-12-06 10:57:15,217 fail2ban.filter       [16884]: INFO      encoding: UTF-8
2025-12-06 10:57:15,219 fail2ban.jail       [16884]: INFO      Jail 'sshd' started
2025-12-06 10:57:15,220 fail2ban.filtersystemd [16884]: INFO      [sshd] Jail is in operation now (process new jour
rnal entries)
2025-12-06 10:57:15,220 fail2ban.jail       [16884]: INFO      Jail 'selinux-ssh' started
2025-12-06 10:57:15,226 fail2ban.jail       [16884]: INFO      Jail 'sshd-ddos' started
```

Рис. 7: Просмотр журнала событий

Защита с помощью Fail2ban

Включим защиту HTTP

```
#  
# 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  
[apache-modsecurity]  
enabled = true
```

Защита с помощью Fail2ban

```
2025-12-06 10:59:28,626 fail2ban.filter      [16968]: INFO    Added logfile: '/var/log/httpd/www.svivanov.net-error_log' (pos = 0, hash = 7968d86271e10d5ef13230bfc0d36c42962dfeaa)
2025-12-06 10:59:28,627 fail2ban.jail       [16968]: INFO    Creating new jail 'sshd-ddos'
2025-12-06 10:59:28,627 fail2ban.jail       [16968]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-06 10:59:28,628 fail2ban.jail       [16968]: INFO    Initiated 'pyinotify' backend
2025-12-06 10:59:28,629 fail2ban.filter      [16968]: INFO    maxLines: 1
2025-12-06 10:59:28,629 fail2ban.filter      [16968]: INFO    maxRetry: 5
2025-12-06 10:59:28,629 fail2ban.filter      [16968]: INFO    findtime: 600
2025-12-06 10:59:28,629 fail2ban.actions   [16968]: INFO    banTime: 3600
2025-12-06 10:59:28,630 fail2ban.filter      [16968]: INFO    encoding: UTF-8
2025-12-06 10:59:28,630 fail2ban.filtersystemd [16968]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-06 10:59:28,631 fail2ban.jail       [16968]: INFO    Jail 'sshd' started
2025-12-06 10:59:28,632 fail2ban.jail       [16968]: INFO    Jail 'selinux-ssh' started
2025-12-06 10:59:28,632 fail2ban.jail       [16968]: INFO    Jail 'apache-auth' started
2025-12-06 10:59:28,634 fail2ban.jail       [16968]: INFO    Jail 'apache-badbots' started
2025-12-06 10:59:28,635 fail2ban.jail       [16968]: INFO    Jail 'apache-noscript' started
2025-12-06 10:59:28,636 fail2ban.jail       [16968]: INFO    Jail 'apache-overflows' started
2025-12-06 10:59:28,637 fail2ban.jail       [16968]: INFO    Jail 'apache-nohome' started
2025-12-06 10:59:28,638 fail2ban.jail       [16968]: INFO    Jail 'apache-botsearch' started
2025-12-06 10:59:28,639 fail2ban.jail       [16968]: INFO    Jail 'apache-fakegooglebot' started
2025-12-06 10:59:28,640 fail2ban.jail       [16968]: INFO    Jail 'apache-modsecurity' started
2025-12-06 10:59:28,641 fail2ban.jail       [16968]: INFO    Jail 'apache-shellshock' started
2025-12-06 10:59:28,642 fail2ban.jail       [16968]: INFO    Jail 'sshd-ddos' started
```

Рис. 9: Перезапуск службы и просмотр журнала

Защита с помощью Fail2ban

Включим защиту почты

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

Защита с помощью Fail2ban

```
2025-12-06 11:01:00,522 fail2ban.jail [17061]: INFO Jail 'apache-badbots' started
2025-12-06 11:01:00,523 fail2ban.jail [17061]: INFO Jail 'apache-noscript' started
2025-12-06 11:01:00,523 fail2ban.jail [17061]: INFO Jail 'apache-overflows' started
2025-12-06 11:01:00,524 fail2ban.jail [17061]: INFO Jail 'apache-nohome' started
2025-12-06 11:01:00,525 fail2ban.jail [17061]: INFO Jail 'apache-botsearch' started
2025-12-06 11:01:00,526 fail2ban.jail [17061]: INFO Jail 'apache-fakegooglebot' started
2025-12-06 11:01:00,527 fail2ban.jail [17061]: INFO Jail 'apache-modsecurity' started
2025-12-06 11:01:00,527 fail2ban.jail [17061]: INFO Jail 'apache-shellshock' started
2025-12-06 11:01:00,529 fail2ban.jail [17061]: INFO Jail 'postfix' started
2025-12-06 11:01:00,530 fail2ban.filtersystemd [17061]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-12-06 11:01:00,530 fail2ban.filtersystemd [17061]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-06 11:01:00,530 fail2ban.jail [17061]: INFO Jail 'postfix-rbl' started
2025-12-06 11:01:00,531 fail2ban.filtersystemd [17061]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-12-06 11:01:00,531 fail2ban.jail [17061]: INFO Jail 'dovecot' started
2025-12-06 11:01:00,531 fail2ban.filtersystemd [17061]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-06 11:01:00,531 fail2ban.jail [17061]: INFO Jail 'postfix-sasl' started
2025-12-06 11:01:00,532 fail2ban.jail [17061]: INFO Jail 'sshd-ddos' started
```

Рис. 11: Перезапуск службы и просмотр журнала

Проверка работы Fail2ban

На сервере посмотрим статус fail2ban

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

Рис. 12: Просмотр статуса службы

Проверка работы Fail2ban

Посмотрим статус защиты SSH в fail2ban

```
[root@server.svivanov.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 + _COMM:sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned:    0
  `-. Banned IP list:
[root@server.svivanov.net ~]#
```

Рис. 13: Просмотр статуса защиты SSH

Проверка работы Fail2ban

```
[root@server.svivanov.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.svivanov.net ~]# █
```

Рис. 14: Установка макс. кол-ва ошибок

Проверка работы Fail2ban

Запускаю виртуальную машину Client

```
C:\work_asp\svivanov>vagrant up client
Bringing machine 'client' up with 'virtualbox' provider...
==> client: Clearing any previously set forwarded ports...
==> client: Fixed port collision for 22 => 2222. Now on port 2200.
==> client: Clearing any previously set network interfaces...
==> client: Preparing network interfaces based on configuration...
      client: Adapter 1: nat
      client: Adapter 2: intnet
==> client: Forwarding ports...
```

Рис. 15: Запуск Client

Проверка работы Fail2ban

С клиента попытаемся зайти по SSH на сервер с неправильным паролем.

```
[root@client.svivanov.net ~]# ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Permission denied, please try again.
```

Рис. 16: Попытка зайти по ssh с клиента

Проверка работы Fail2ban

На сервере посмотрим статус защиты SSH

```
[root@server.svivanov.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 + _COMM:sshd-session
`- Actions
  |- Currently banned: 1
  |- Total banned:     1
  `-- Banned IP list:   192.168.1.30
[root@server.svivanov.net ~]#
```

Рис. 17: Блокировка адреса клиента

Проверка работы Fail2ban

Разблокируем IP-адрес клиента:

```
[root@server.svivanov.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.svivanov.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 + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned:     1
    `- Banned IP list:
[root@server.svivanov.net ~]# █
```

Рис. 18: Разблокировка клиента

Проверка работы Fail2ban

Внесем изменение в конфигурационный файл, добавив игнорирование адреса клиента

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
#
```

Рис. 19: Редактирование конф. файла

Проверка работы Fail2ban

```
rnal entries)
2025-12-06 11:24:25,375 fail2ban.jail      [17693]: INFO    Jail 'sshd' started
2025-12-06 11:24:25,375 fail2ban.jail      [17693]: INFO    Jail 'selinux-ssh' started
2025-12-06 11:24:25,378 fail2ban.jail      [17693]: INFO    Jail 'apache-auth' started
2025-12-06 11:24:25,379 fail2ban.jail      [17693]: INFO    Jail 'apache-badbots' started
2025-12-06 11:24:25,380 fail2ban.jail      [17693]: INFO    Jail 'apache-noscript' started
2025-12-06 11:24:25,380 fail2ban.jail      [17693]: INFO    Jail 'apache-overflows' started
2025-12-06 11:24:25,381 fail2ban.jail      [17693]: INFO    Jail 'apache-nohome' started
2025-12-06 11:24:25,382 fail2ban.jail      [17693]: INFO    Jail 'apache-botsearch' started
2025-12-06 11:24:25,383 fail2ban.jail      [17693]: INFO    Jail 'apache-fakegooglebot' started
2025-12-06 11:24:25,384 fail2ban.jail      [17693]: INFO    Jail 'apache-modsecurity' started
2025-12-06 11:24:25,384 fail2ban.jail      [17693]: INFO    Jail 'apache-shellshock' started
2025-12-06 11:24:25,385 fail2ban.jail      [17693]: INFO    Jail 'postfix' started
2025-12-06 11:24:25,386 fail2ban.filtersystemd [17693]: INFO    [postfix] Jail is in operation now (process new
journal entries)
2025-12-06 11:24:25,386 fail2ban.filtersystemd [17693]: INFO    [postfix-rbl] Jail is in operation now (process
new journal entries)
2025-12-06 11:24:25,386 fail2ban.jail      [17693]: INFO    Jail 'postfix-rbl' started
2025-12-06 11:24:25,387 fail2ban.filtersystemd [17693]: INFO    [dovecot] Jail is in operation now (process new
journal entries)
2025-12-06 11:24:25,387 fail2ban.jail      [17693]: INFO    Jail 'dovecot' started
2025-12-06 11:24:25,387 fail2ban.filtersystemd [17693]: INFO    [postfix-sasl] Jail is in operation now (process
new journal entries)
2025-12-06 11:24:25,387 fail2ban.jail      [17693]: INFO    Jail 'postfix-sasl' started
```

Рис. 20: Перезапуск службы и просмотр журнала

Проверка работы Fail2ban

```
[root@client.svivanov.net ~]# ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Permission denied, please try again.
svivanov@server.svivanov.net's password:
Permission denied, please try again.
svivanov@server.svivanov.net's password: █
```

Рис. 21: Попытка входа

Проверка работы Fail2ban

```
[root@server.svivanov.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 + _COMM:sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned:    0
  `-. Banned IP list:
[root@server.svivanov.net ~]# █
```

Рис. 22: Статус защиты

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[root@server.svivanov.net ~]# cd /vagrant/provision/server  
[root@server.svivanov.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d  
[root@server.svivanov.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/  
ct/etc/fail2ban/jail.d/
```

Рис. 23: Создание директорий и копирование конф. файлов

Внесение изменений в настройки внутреннего окружения виртуальных машин

```
#!/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. 24: Создание скрипта

Внесение изменений в настройки внутреннего окружения виртуальных машин

Для отработки скрипта во время загрузки машины server в файле Vagrantfile необходимо добавить:

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

Рис. 25: Редактирование Vagrantfile

Вывод

В ходе выполнения лабораторной работы мы получили навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».