Лабораторная работа № 16

Базовая защита от атак типа «brute force»

Митрофанов Тимур Александрович

2025-12-17

Содержание I

Раздел 1

1. Информация

1.1 Докладчик

- Митрофанов Тимур Александрович

1.1 Докладчик

- Митрофанов Тимур Александрович
- Российский университет дружбы народов им. П. Лумумбы

Раздел 2

2. Вводная часть

2.1 Цели и задачи

Цель - получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб.

2.1 Цели и задачи

Цель - получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

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.

2.1 Цели и задачи

Цель - получение навыков работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

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.

Раздел 3

3. Выполнение заданий

3.1 Установка fail2ban

```
[root@server.tamitrofanov.net server]# dnf -y install fail2ban
Extra Packages for Enterprise Linux 10 - x86_64                         11 kB/s |  37 kB     00:03
Extra Packages for Enterprise Linux 10 - x86_64                        3.6 MB/s | 5.6 MB     00:01
Rocky Linux 10 - BaseOS                                                521  B/s | 4.3 kB     00:08
Rocky Linux 10 - BaseOS                                                6.0 MB/s | 5.3 MB     00:00
Rocky Linux 10 - AppStream                                              17 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                                             3.9 MB/s | 2.0 MB     00:00
Rocky Linux 10 - CRB                                                    17 kB/s | 4.3 kB     00:00
Rocky Linux 10 - CRB                                                   251 kB/s | 486 kB     00:01
Rocky Linux 10 - Extras                                                8.6 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                                                 12 kB/s | 4.8 kB     00:00
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

Total download size: 623 k
Installed size: 1.8 M
Downloading Packages:
(1/5): fail2ban-1.1.0-6.el10_0.noarch.rpm                              113 kB/s | 9.4 kB     00:00
(2/5): fail2ban-firewalld-1.1.0-6.el10_0.noarch.rpm                    100 kB/s | 9.6 kB     00:00
(3/5): fail2ban-selinux-1.1.0-6.el10_0.noarch.rpm                      298 kB/s |  31 kB     00:00
(4/5): fail2ban-sendmail-1.1.0-6.el10_0.noarch.rpm                     282 kB/s |  12 kB     00:00
(5/5): fail2ban-server-1.1.0-6.el10_0.noarch.rpm                       4.5 MB/s | 561 kB     00:00
------------------------------------------------------------------------------------------------------
Total                                                                  1.1 MB/s | 623 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                              1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el10_0.noarch                                       1/5
  Installing       : fail2ban-selinux-1.1.0-6.el10_0.noarch                                       1/5
```

3.2 Запуск fail2ban

```
[root@server.tamitrofanov.net server]# systemctl start fail2ban
systemctl enable fail2ban
[root@server.tamitrofanov.net server]#
```

Рисунок 2: Запуск fail2ban

3.3 журнал событий fail2ban

```
[tamitrofanov@server.tamitrofanov.net ~]$ tail -f /var/log/fail2ban.log
tail: cannot open '/var/log/fail2ban.log' for reading: Permission denied
tail: no files remaining
[tamitrofanov@server.tamitrofanov.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for tamitrofanov:
2025-12-16 22:21:08,391 fail2ban.server         [6438]: INFO    --------------------------------------------------
2025-12-16 22:21:08,392 fail2ban.server         [6438]: INFO    Starting Fail2ban v1.1.0
2025-12-16 22:21:08,393 fail2ban.observer       [6438]: INFO    Observer start...
2025-12-16 22:21:08,400 fail2ban.database       [6438]: INFO    Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2025-12-16 22:21:08,402 fail2ban.database       [6438]: WARNING New database created. Version '4'
```

Рисунок 3: журнал событий fail2ban

3.4 базовая настройка fail2ban

```
[root@server.tamitrofanov.net server]# touch /etc/fail2ban/jail.d/customisation.local
[root@server.tamitrofanov.net server]# nano /etc/fail2ban/jail.d/customisation.local
[root@server.tamitrofanov.net server]#
[root@server.tamitrofanov.net server]# nano /etc/fail2ban/jail.d/customisation.local
[root@server.tamitrofanov.net server]# 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.tamitrofanov.net server]# systemctl restart fail2ban
[root@server.tamitrofanov.net server]#
```

3.5 журнал событий fail2ban

```
2025-12-16 22:21:08,400 fail2ban.database       [6438]: INFO    Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2025-12-16 22:21:08,402 fail2ban.database       [6438]: WARNING New database created. Version '4'
2025-12-16 22:25:25,565 fail2ban.server         [6438]: INFO    Shutdown in progress...
2025-12-16 22:25:25,566 fail2ban.observer       [6438]: INFO    Observer stop ... try to end queue 5 seconds
2025-12-16 22:25:25,588 fail2ban.observer       [6438]: INFO    Observer stopped, 0 events remaining.
2025-12-16 22:25:25,630 fail2ban.server         [6438]: INFO    Stopping all jails
2025-12-16 22:25:25,630 fail2ban.database       [6438]: INFO    Connection to database closed.
2025-12-16 22:25:25,630 fail2ban.server         [6438]: INFO    Exiting Fail2ban
2025-12-16 22:25:25,740 fail2ban.server         [6683]: INFO    --------------------------------------------------
2025-12-16 22:25:25,741 fail2ban.server         [6683]: INFO    Starting Fail2ban v1.1.0
2025-12-16 22:25:25,743 fail2ban.observer       [6683]: INFO    Observer start...
2025-12-16 22:25:25,749 fail2ban.database       [6683]: INFO    Connected to fail2ban persistent database '/var/lib/f
ail2ban/fail2ban.sqlite3'
2025-12-16 22:25:25,749 fail2ban.jail           [6683]: INFO    Creating new jail 'sshd'
2025-12-16 22:25:25,753 fail2ban.jail           [6683]: INFO    Jail 'sshd' uses systemd {}
2025-12-16 22:25:25,755 fail2ban.jail           [6683]: INFO    Initiated 'systemd' backend
2025-12-16 22:25:25,756 fail2ban.filter         [6683]: INFO      maxLines: 1
2025-12-16 22:25:25,762 fail2ban.filtersystemd  [6683]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.s
ervice + _COMM=sshd + _COMM=sshd-session'
2025-12-16 22:25:25,763 fail2ban.filter         [6683]: INFO      maxRetry: 5
2025-12-16 22:25:25,763 fail2ban.filter         [6683]: INFO      findTime: 600
2025-12-16 22:25:25,763 fail2ban.actions        [6683]: INFO      banTime: 3600
2025-12-16 22:25:25,763 fail2ban.filter         [6683]: INFO      encoding: UTF-8
2025-12-16 22:25:25,764 fail2ban.jail           [6683]: INFO    Creating new jail 'selinux-ssh'
2025-12-16 22:25:25,772 fail2ban.jail           [6683]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2025-12-16 22:25:25,775 fail2ban.jail           [6683]: INFO    Initiated 'pyinotify' backend
2025-12-16 22:25:25,775 fail2ban.datedetector   [6683]: INFO      date pattern `''': `Epoch'
2025-12-16 22:25:25,776 fail2ban.filter         [6683]: INFO      maxRetry: 5
2025-12-16 22:25:25,776 fail2ban.filter         [6683]: INFO      findTime: 600
2025-12-16 22:25:25,776 fail2ban.actions        [6683]: INFO      banTime: 3600
2025-12-16 22:25:25,776 fail2ban.filter         [6683]: INFO      encoding: UTF-8
2025-12-16 22:25:25,777 fail2ban.filter         [6683]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, h
ash = ecaf8d0643b566ab6bf7ed4cc1d27113f120e8dc)
2025-12-16 22:25:25,778 fail2ban.jail           [6683]: INFO    Creating new jail 'sshd-ddos'
2025-12-16 22:25:25,779 fail2ban.jail           [6683]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-16 22:25:25,781 fail2ban.jail           [6683]: INFO    Initiated 'pyinotify' backend
2025-12-16 22:25:25,781 fail2ban.filter         [6683]: INFO      maxLines: 1
2025-12-16 22:25:25,782 fail2ban.filter         [6683]: INFO      maxRetry: 5
2025-12-16 22:25:25,782 fail2ban.filter         [6683]: INFO      findTime: 600
2025-12-16 22:25:25,782 fail2ban.actions        [6683]: INFO      banTime: 3600
2025-12-16 22:25:25,782 fail2ban.filter         [6683]: INFO      encoding: UTF-8
2025-12-16 22:25:25,783 fail2ban.jail           [6683]: INFO    Jail 'sshd' started
```

3.6 включение защиты HTTP

```
[root@server.tamitrofanov.net server]# nano /etc/fail2ban/jail.d/customisation.local
[root@server.tamitrofanov.net server]# 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


#
# 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
```

3.7 журнал событий fail2ban

```
2025-12-16 22:28:14,086 fail2ban.actions        [6738]: INFO      banTime: 3600
2025-12-16 22:28:14,086 fail2ban.filter         [6738]: INFO      encoding: UTF-8
2025-12-16 22:28:14,086 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/server.tamitrofanov.ne
t-error_log' (pos = 0, hash = )
2025-12-16 22:28:14,087 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, h
ash = 6c93f536a59bc91517552d8990a412122926d3c0)
2025-12-16 22:28:14,087 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos =
0, hash = 220e3d1532fc0b99d21f2441052b90207c65b6de)
2025-12-16 22:28:14,087 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/www.tamitrofanov.net-e
rror_log' (pos = 0, hash = ab0e6a3d290159071e514bc8e01ce2b3eada66bf)
2025-12-16 22:28:14,087 fail2ban.jail           [6738]: INFO    Creating new jail 'apache-shellshock'
2025-12-16 22:28:14,087 fail2ban.jail           [6738]: INFO    Jail 'apache-shellshock' uses pyinotify {}
2025-12-16 22:28:14,089 fail2ban.jail           [6738]: INFO    Initiated 'pyinotify' backend
2025-12-16 22:28:14,090 fail2ban.filter         [6738]: INFO      maxRetry: 1
2025-12-16 22:28:14,090 fail2ban.filter         [6738]: INFO      findtime: 600
2025-12-16 22:28:14,090 fail2ban.actions        [6738]: INFO      banTime: 3600
2025-12-16 22:28:14,090 fail2ban.filter         [6738]: INFO      encoding: UTF-8
2025-12-16 22:28:14,090 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/server.tamitrofanov.ne
t-error_log' (pos = 0, hash = )
2025-12-16 22:28:14,091 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/error_log' (pos = 0, h
ash = 6c93f536a59bc91517552d8990a412122926d3c0)
2025-12-16 22:28:14,091 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/ssl_error_log' (pos =
0, hash = 220e3d1532fc0b99d21f2441052b90207c65b6de)
2025-12-16 22:28:14,091 fail2ban.filter         [6738]: INFO    Added logfile: '/var/log/httpd/www.tamitrofanov.net-e
rror_log' (pos = 0, hash = ab0e6a3d290159071e514bc8e01ce2b3eada66bf)
2025-12-16 22:28:14,091 fail2ban.jail           [6738]: INFO    Creating new jail 'sshd-ddos'
2025-12-16 22:28:14,091 fail2ban.jail           [6738]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-16 22:28:14,093 fail2ban.jail           [6738]: INFO    Initiated 'pyinotify' backend
2025-12-16 22:28:14,094 fail2ban.filter         [6738]: INFO      maxLines: 1
2025-12-16 22:28:14,094 fail2ban.filter         [6738]: INFO      maxRetry: 5
2025-12-16 22:28:14,094 fail2ban.filter         [6738]: INFO      findtime: 600
2025-12-16 22:28:14,095 fail2ban.actions        [6738]: INFO      banTime: 3600
2025-12-16 22:28:14,095 fail2ban.filter         [6738]: INFO      encoding: UTF-8
2025-12-16 22:28:14,096 fail2ban.filtersystemd  [6738]: INFO    [sshd] Jail is in operation now (process new journal
entries)
2025-12-16 22:28:14,097 fail2ban.jail           [6738]: INFO    Jail 'sshd' started
2025-12-16 22:28:14,099 fail2ban.jail           [6738]: INFO    Jail 'selinux-ssh' started
2025-12-16 22:28:14,100 fail2ban.jail           [6738]: INFO    Jail 'apache-auth' started
2025-12-16 22:28:14,102 fail2ban.jail           [6738]: INFO    Jail 'apache-badbots' started
2025-12-16 22:28:14,104 fail2ban.jail           [6738]: INFO    Jail 'apache-noscript' started
2025-12-16 22:28:14,105 fail2ban.jail           [6738]: INFO    Jail 'apache-overflows' started
2025-12-16 22:28:14,106 fail2ban.jail           [6738]: INFO    Jail 'apache-nohome' started
2025-12-16 22:28:14,107 fail2ban.jail           [6738]: INFO    Jail 'apache-botsearch' started
```

3.8 Настройка запуска службы на клиенте

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

3.9 журнал событий fail2ban

```
2025-12-16 22:42:52,846 fail2ban.filter         [6919]: INFO      maxRetry: 5
2025-12-16 22:42:52,846 fail2ban.filter         [6919]: INFO      findtime: 600
2025-12-16 22:42:52,846 fail2ban.actions        [6919]: INFO      banTime: 3600
2025-12-16 22:42:52,846 fail2ban.filter         [6919]: INFO      encoding: UTF-8
2025-12-16 22:42:52,846 fail2ban.jail           [6919]: INFO    Creating new jail 'postfix-sasl'
2025-12-16 22:42:52,846 fail2ban.jail           [6919]: INFO    Jail 'postfix-sasl' uses systemd {}
2025-12-16 22:42:52,846 fail2ban.jail           [6919]: INFO    Initiated 'systemd' backend
2025-12-16 22:42:52,847 fail2ban.filtersystemd  [6919]: INFO    [postfix-sasl] Added journal match for: '_SYSTEMD_UNI
T=postfix.service _SYSTEMD_UNIT=postfix@-.service'
2025-12-16 22:42:52,847 fail2ban.filter         [6919]: INFO      maxRetry: 5
2025-12-16 22:42:52,847 fail2ban.filter         [6919]: INFO      findtime: 600
2025-12-16 22:42:52,847 fail2ban.actions        [6919]: INFO      banTime: 3600
2025-12-16 22:42:52,847 fail2ban.filter         [6919]: INFO      encoding: UTF-8
2025-12-16 22:42:52,847 fail2ban.jail           [6919]: INFO    Creating new jail 'sshd-ddos'
2025-12-16 22:42:52,847 fail2ban.jail           [6919]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-16 22:42:52,849 fail2ban.jail           [6919]: INFO    Initiated 'pyinotify' backend
2025-12-16 22:42:52,850 fail2ban.filter         [6919]: INFO      maxLines: 1
2025-12-16 22:42:52,851 fail2ban.filter         [6919]: INFO      maxRetry: 5
2025-12-16 22:42:52,851 fail2ban.filter         [6919]: INFO      findtime: 600
2025-12-16 22:42:52,851 fail2ban.actions        [6919]: INFO      banTime: 3600
2025-12-16 22:42:52,851 fail2ban.filter         [6919]: INFO      encoding: UTF-8
2025-12-16 22:42:52,852 fail2ban.filtersystemd  [6919]: INFO    [sshd] Jail is in operation now (process new journal
entries)
2025-12-16 22:42:52,852 fail2ban.jail           [6919]: INFO    Jail 'sshd' started
2025-12-16 22:42:52,854 fail2ban.jail           [6919]: INFO    Jail 'selinux-ssh' started
2025-12-16 22:42:52,855 fail2ban.jail           [6919]: INFO    Jail 'apache-auth' started
2025-12-16 22:42:52,855 fail2ban.jail           [6919]: INFO    Jail 'apache-badbots' started
2025-12-16 22:42:52,857 fail2ban.jail           [6919]: INFO    Jail 'apache-noscript' started
2025-12-16 22:42:52,857 fail2ban.jail           [6919]: INFO    Jail 'apache-overflows' started
2025-12-16 22:42:52,858 fail2ban.jail           [6919]: INFO    Jail 'apache-nohome' started
2025-12-16 22:42:52,859 fail2ban.jail           [6919]: INFO    Jail 'apache-botsearch' started
2025-12-16 22:42:52,859 fail2ban.jail           [6919]: INFO    Jail 'apache-fakegooglebot' started
2025-12-16 22:42:52,861 fail2ban.jail           [6919]: INFO    Jail 'apache-modsecurity' started
2025-12-16 22:42:52,862 fail2ban.jail           [6919]: INFO    Jail 'apache-shellshock' started
2025-12-16 22:42:52,863 fail2ban.jail           [6919]: INFO    Jail 'postfix' started
2025-12-16 22:42:52,864 fail2ban.jail           [6919]: INFO    Jail 'postfix-rbl' started
2025-12-16 22:42:52,867 fail2ban.filtersystemd  [6919]: INFO    [dovecot] Jail is in operation now (process new journ
al entries)
2025-12-16 22:42:52,868 fail2ban.filtersystemd  [6919]: INFO    [postfix-rbl] Jail is in operation now (process new j
ournal entries)
2025-12-16 22:42:52,869 fail2ban.jail           [6919]: INFO    Jail 'dovecot' started
2025-12-16 22:42:52,870 fail2ban.filtersystemd  [6919]: INFO    [postfix-sasl] Jail is in operation now (process new
 journal entries)
```

3.10 Доп настройка fail2ban

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

Рисунок 10: Доп настройка fail2ban

3.11 Пробное подключение с клиента

```
[tamitrofanov@client.tamitrofanov.net ~]$ ssh tamitrofanov@server.tamitrofanov.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 13 20:53:48 2025
[tamitrofanov@server.tamitrofanov.net ~]$ ^C
[tamitrofanov@server.tamitrofanov.net ~]$ exit
logout
Connection to server.tamitrofanov.net closed.
[tamitrofanov@client.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@client.tamitrofanov.net ~]# ^C
[root@client.tamitrofanov.net ~]# ssh tamitrofanov@server.tamitrofanov.net
tamitrofanov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofanov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofanov@server.tamitrofanov.net's password:
tamitrofanov@server.tamitrofanov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.tamitrofanov.net ~]#
```

Рисунок 11: Пробное подключение с клиента

3.12 Снятие бана с клиента

```
[root@server.tamitrofanov.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- 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.tamitrofanov.net server]#
[root@server.tamitrofanov.net server]#
[root@server.tamitrofanov.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.tamitrofanov.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
```

3.13 Добавление клиента в исключения

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
[root@server.tamitrofanov.net server]# systemctl restart fail2ban
[root@server.tamitrofanov.net server]#
```

Рисунок 13: Добавление клиента в исключения

3.14 журнал событий fail2ban

```
2025-12-16 23:15:13,816 fail2ban.filter         [7363]: INFO      encoding: UTF-8
2025-12-16 23:15:13,816 fail2ban.jail           [7363]: INFO    Creating new jail 'postfix-sasl'
2025-12-16 23:15:13,816 fail2ban.jail           [7363]: INFO    Jail 'postfix-sasl' uses systemd {}
2025-12-16 23:15:13,816 fail2ban.jail           [7363]: INFO    Initiated 'systemd' backend
2025-12-16 23:15:13,817 fail2ban.filtersystemd  [7363]: INFO    [postfix-sasl] Added journal match for: '_SYSTEMD_UNI
T=postfix.service _SYSTEMD_UNIT=postfix@-.service'
2025-12-16 23:15:13,817 fail2ban.filter         [7363]: INFO      maxRetry: 5
2025-12-16 23:15:13,817 fail2ban.filter         [7363]: INFO      findTime: 600
2025-12-16 23:15:13,817 fail2ban.actions        [7363]: INFO      banTime: 3600
2025-12-16 23:15:13,817 fail2ban.filter         [7363]: INFO      encoding: UTF-8
2025-12-16 23:15:13,817 fail2ban.jail           [7363]: INFO    Creating new jail 'sshd-ddos'
2025-12-16 23:15:13,817 fail2ban.jail           [7363]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-16 23:15:13,820 fail2ban.jail           [7363]: INFO    Initiated 'pyinotify' backend
2025-12-16 23:15:13,820 fail2ban.filter         [7363]: INFO      maxLines: 1
2025-12-16 23:15:13,821 fail2ban.filter         [7363]: INFO      maxRetry: 5
2025-12-16 23:15:13,821 fail2ban.filter         [7363]: INFO      findTime: 600
2025-12-16 23:15:13,821 fail2ban.actions        [7363]: INFO      banTime: 3600
2025-12-16 23:15:13,821 fail2ban.filter         [7363]: INFO      encoding: UTF-8
2025-12-16 23:15:13,823 fail2ban.jail           [7363]: INFO    Jail 'sshd' started
2025-12-16 23:15:13,824 fail2ban.jail           [7363]: INFO    Jail 'selinux-ssh' started
2025-12-16 23:15:13,825 fail2ban.jail           [7363]: INFO    Jail 'apache-auth' started
2025-12-16 23:15:13,826 fail2ban.jail           [7363]: INFO    Jail 'apache-badbots' started
2025-12-16 23:15:13,826 fail2ban.jail           [7363]: INFO    Jail 'apache-noscript' started
2025-12-16 23:15:13,827 fail2ban.jail           [7363]: INFO    Jail 'apache-overflows' started
2025-12-16 23:15:13,827 fail2ban.jail           [7363]: INFO    Jail 'apache-nohome' started
2025-12-16 23:15:13,833 fail2ban.jail           [7363]: INFO    Jail 'apache-botsearch' started
2025-12-16 23:15:13,834 fail2ban.jail           [7363]: INFO    Jail 'apache-fakegooglebot' started
2025-12-16 23:15:13,838 fail2ban.jail           [7363]: INFO    Jail 'apache-modsecurity' started
2025-12-16 23:15:13,840 fail2ban.jail           [7363]: INFO    Jail 'apache-shellshock' started
2025-12-16 23:15:13,840 fail2ban.filtersystemd  [7363]: INFO    [postfix] Jail is in operation now (process new journ
al entries)
2025-12-16 23:15:13,841 fail2ban.jail           [7363]: INFO    Jail 'postfix' started
2025-12-16 23:15:13,841 fail2ban.filtersystemd  [7363]: INFO    [postfix-rbl] Jail is in operation now (process new j
ournal entries)
2025-12-16 23:15:13,842 fail2ban.jail           [7363]: INFO    Jail 'postfix-rbl' started
2025-12-16 23:15:13,842 fail2ban.filtersystemd  [7363]: INFO    [dovecot] Jail is in operation now (process new journ
al entries)
2025-12-16 23:15:13,844 fail2ban.filter         [7363]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-12-16 23:15:13,844 fail2ban.filter         [7363]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-12-16 23:15:13,844 fail2ban.filter         [7363]: INFO    [sshd] Ignore 192.168.1.30 by ip
2025-12-16 23:15:13,845 fail2ban.jail           [7363]: INFO    Jail 'dovecot' started
2025-12-16 23:15:13,846 fail2ban.filtersystemd  [7363]: INFO    [postfix-sasl] Jail is in operation now (process new
```

3.15 Попытка входа

```
[root@client.tamitrofanov.net ~]# ssh tamitrofanov@server.tamitrofanov.net
tamitrofanov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofanov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofanov@server.tamitrofanov.net's password:
tamitrofanov@server.tamitrofanov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.tamitrofanov.net ~]#
```

Рисунок 15: Попытка входа

3.16 Проверка бан-листа

```
[root@server.tamitrofanov.net server]# 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.tamitrofanov.net server]#
```

Рисунок 16: Проверка бан-листа

3.17 Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[root@server.tamitrofanov.net server]# 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/
[root@server.tamitrofanov.net server]#
[root@server.tamitrofanov.net server]# cd /vagrant/provision/server
touch protect.sh
chmod +x protect.sh
[root@server.tamitrofanov.net server]# nano protect.sh
[root@server.tamitrofanov.net server]# cat protect.sh
#!/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
```

3.18 изменение Vagrantfile

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

end
```

Рисунок 18: изменение Vagrantfile

Раздел 4

4. Выводы

4.1 слайд 1

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