

Лабораторная работа № 16

Базовая защита от атак типа «brute force»

Демидова Е. А.

18 декабря 2023

Российский университет дружбы народов, Москва, Россия

Вводная часть

Получить навыки 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.

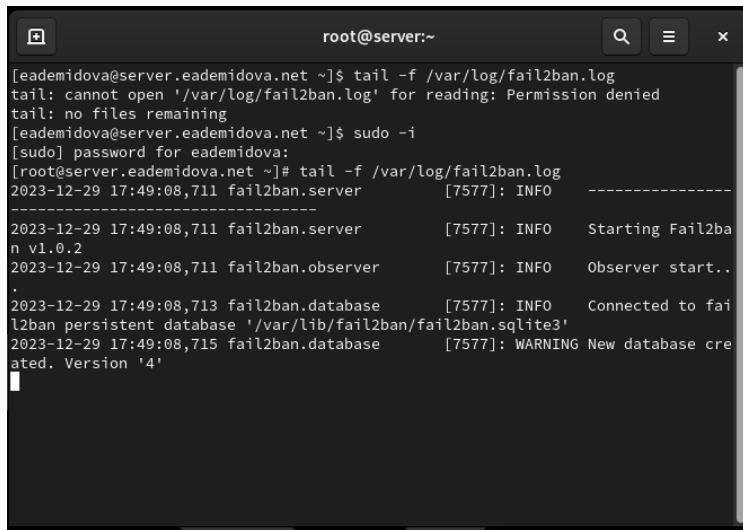
Выполнение лабораторной работы

На сервере установим fail2ban:

```
dnf -y install fail2ban
```

Запустим сервер fail2ban:

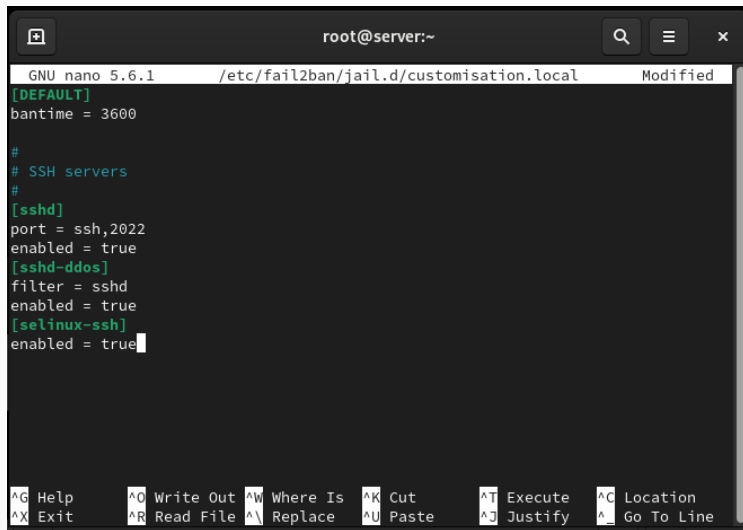
```
systemctl start fail2ban  
systemctl enable fail2ban
```



```
root@server:~  
[eademidova@server.eademidova.net ~]$ tail -f /var/log/fail2ban.log  
tail: cannot open '/var/log/fail2ban.log' for reading: Permission denied  
tail: no files remaining  
[eademidova@server.eademidova.net ~]$ sudo -i  
[sudo] password for eademidova:  
[root@server.eademidova.net ~]# tail -f /var/log/fail2ban.log  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO -----  
-----  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO Starting Fail2ban v1.0.2  
2023-12-29 17:49:08,711 fail2ban.observer [7577]: INFO Observer start..  
.  
2023-12-29 17:49:08,713 fail2ban.database [7577]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'  
2023-12-29 17:49:08,715 fail2ban.database [7577]: WARNING New database created. Version '4'
```

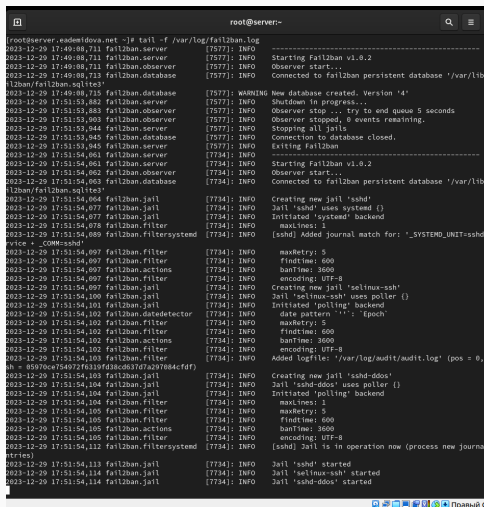
Рис. 1: Запуск просмотра журнала событий fail2ban

```
touch /etc/fail2ban/jail.d/customisation.local
```

```
root@server:~  
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified  
[DEFAULT]  
bantime = 3600  
  
#  
# SSH servers  
#  
[sshd]  
port = ssh,2022  
enabled = true  
[sshd-ddos]  
filter = sshd  
enabled = true  
[selinux-ssh]  
enabled = true  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

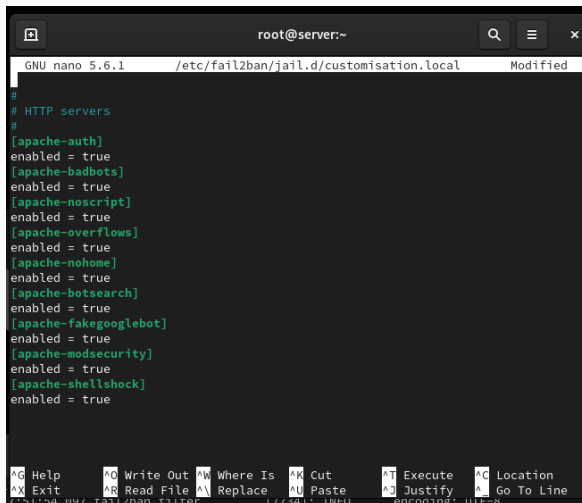
Рис. 2: Добавление времени блокировки и включение защиты SSH customisation.local



```
root@server:~# tail -f /var/log/fail2ban.log
[2023-12-29 17:49:08.711] fail2ban.server [7577]: INFO
[2023-12-29 17:49:08.711] fail2ban.server [7577]: INFO Starting Fail2ban v1.0.2
[2023-12-29 17:49:08.711] fail2ban.observer [7577]: INFO Observer start...
[2023-12-29 17:49:08.713] fail2ban.database [7577]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
[2023-12-29 17:49:08.715] fail2ban.database [7577]: WARNING New database created. Version '4'
[2023-12-29 17:51:53.880] fail2ban.server [7577]: INFO Sslsdman in progress...
[2023-12-29 17:51:53.883] fail2ban.observer [7577]: INFO Observer stop ... try to end queue 5 seconds
[2023-12-29 17:51:53.903] fail2ban.observer [7577]: INFO Observer stopped, 0 events remaining.
[2023-12-29 17:51:53.944] fail2ban.server [7577]: INFO Stopping all jails
[2023-12-29 17:51:53.945] fail2ban.database [7577]: INFO Connection to database closed.
[2023-12-29 17:51:53.945] fail2ban.server [7577]: INFO Exiting Fail2ban
[2023-12-29 17:51:54.061] fail2ban.server [7734]: INFO
[2023-12-29 17:51:54.061] fail2ban.server [7734]: INFO Starting Fail2ban v1.0.2
[2023-12-29 17:51:54.062] fail2ban.observer [7734]: INFO Observer start...
[2023-12-29 17:51:54.063] fail2ban.database [7734]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
[2023-12-29 17:51:54.064] fail2ban.jail [7734]: INFO Creating new jail 'sshd'
[2023-12-29 17:51:54.077] fail2ban.jail [7734]: INFO Jail 'sshd' uses systemd ()
[2023-12-29 17:51:54.077] fail2ban.jail [7734]: INFO Initiated 'systemd' backend
[2023-12-29 17:51:54.078] fail2ban.filter [7734]: INFO maxLines: 1
[2023-12-29 17:51:54.089] fail2ban.filtersystemd [7734]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
[2023-12-29 17:51:54.097] fail2ban.filter [7734]: INFO maxRetry: 5
[2023-12-29 17:51:54.097] fail2ban.filter [7734]: INFO findTime: 600
[2023-12-29 17:51:54.097] fail2ban.actions [7734]: INFO banTime: 3600
[2023-12-29 17:51:54.097] fail2ban.filter [7734]: INFO encoding: UTF-8
[2023-12-29 17:51:54.097] fail2ban.jail [7734]: INFO Creating new jail 'selinux-ssh'
[2023-12-29 17:51:54.100] fail2ban.jail [7734]: INFO Jail 'selinux-ssh' uses poller ()
[2023-12-29 17:51:54.101] fail2ban.jail [7734]: INFO Initiated 'polling' backend
[2023-12-29 17:51:54.102] fail2ban.datadector [7734]: INFO date pattern '%%Y%%m%%d%%H%%M%%S%%f'
[2023-12-29 17:51:54.102] fail2ban.filter [7734]: INFO maxRetry: 5
[2023-12-29 17:51:54.102] fail2ban.filter [7734]: INFO findTime: 600
[2023-12-29 17:51:54.102] fail2ban.actions [7734]: INFO banTime: 3600
[2023-12-29 17:51:54.102] fail2ban.filter [7734]: INFO encoding: UTF-8
[2023-12-29 17:51:54.103] fail2ban.filter [7734]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0, sh = 05970ce754972f6339f43dc087d7a297084cfd)
[2023-12-29 17:51:54.103] fail2ban.jail [7734]: INFO Creating new jail 'sshd-ddos'
[2023-12-29 17:51:54.104] fail2ban.jail [7734]: INFO Jail 'sshd-ddos' uses poller ()
[2023-12-29 17:51:54.104] fail2ban.jail [7734]: INFO Initiated 'polling' backend
[2023-12-29 17:51:54.104] fail2ban.filter [7734]: INFO maxLines: 1
[2023-12-29 17:51:54.105] fail2ban.filter [7734]: INFO maxRetry: 5
[2023-12-29 17:51:54.105] fail2ban.filter [7734]: INFO findTime: 600
[2023-12-29 17:51:54.105] fail2ban.actions [7734]: INFO banTime: 3600
[2023-12-29 17:51:54.105] fail2ban.filter [7734]: INFO encoding: UTF-8
[2023-12-29 17:51:54.112] fail2ban.filtersystemd [7734]: INFO [sshd] Jail is in operation now (process new journal entries)
[2023-12-29 17:51:54.113] fail2ban.jail [7734]: INFO Jail 'sshd' started
[2023-12-29 17:51:54.114] fail2ban.jail [7734]: INFO Jail 'selinux-ssh' started
[2023-12-29 17:51:54.114] fail2ban.jail [7734]: INFO Jail 'sshd-ddos' started
```

Рис. 3: Просмотр журнала событий fail2ban

Защита с помощью Fail2ban



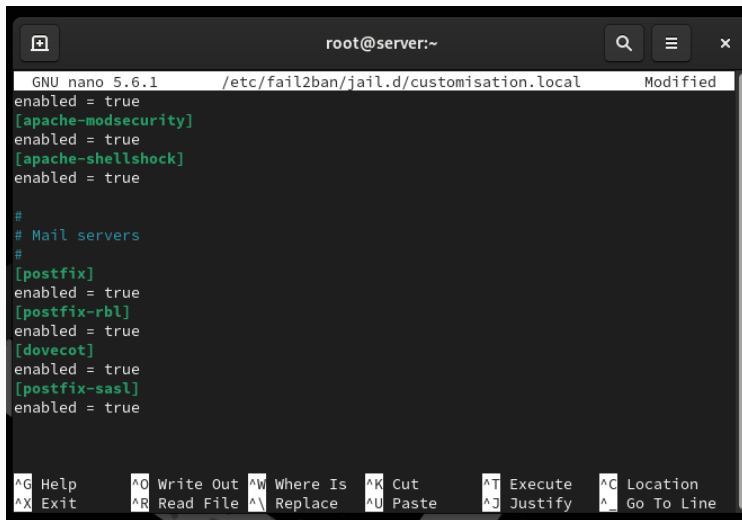
```
root@server:~  
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified  
#  
# HTTP servers  
#  
[apache-auth]  
enabled = true  
[apache-badbots]  
enabled = true  
[apache-noscript]  
enabled = true  
[apache-overflows]  
enabled = true  
[apache-nohome]  
enabled = true  
[apache-botsearch]  
enabled = true  
[apache-fakegooglebot]  
enabled = true  
[apache-modsecurity]  
enabled = true  
[apache-shellshock]  
enabled = true  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line  
//34:54:09 /etc/fail2ban/filter.d//34: INFO encoding: UTF-8
```

Рис. 4: Включение защиты HTTP в файле customisation.local

Защита с помощью Fail2ban

```
root@server:~  
2023-12-29 17:53:40,577 fail2ban.jail [7775]: INFO Jail 'apache-modsecurity' uses poller {}  
2023-12-29 17:53:40,577 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,578 fail2ban.filter [7775]: INFO maxRetry: 2  
2023-12-29 17:53:40,578 fail2ban.filter [7775]: INFO findtime: 600  
2023-12-29 17:53:40,579 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/server.eadenidova.net-  
error_log' (pos = 0, hash = )  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0,  
sh = 0dd417186aac838b6221688ec9cca9f0ee4a3757)  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos  
, hash = 3837407b2265d724d1c6cfb9943fdce67f980517)  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/www.eadenidova.net-e  
r_log' (pos = 0, hash = 4451f17b3b874cbb36bae5e8792cd99583b50772)  
2023-12-29 17:53:40,579 fail2ban.jail [7775]: INFO Creating new jail 'apache-shellshock'  
2023-12-29 17:53:40,580 fail2ban.jail [7775]: INFO Jail 'apache-shellshock' uses poller {}  
2023-12-29 17:53:40,580 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO maxRetry: 1  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO findtime: 600  
2023-12-29 17:53:40,581 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/server.eadenidova.net-  
error_log' (pos = 0, hash = )  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0,  
sh = 0dd417186aac838b6221688ec9cca9f0ee4a3757)  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos  
, hash = 3837407b2265d724d1c6cfb9943fdce67f980517)  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/www.eadenidova.net-e  
r_log' (pos = 0, hash = 4451f17b3b874cbb36bae5e8792cd99583b50772)  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Creating new jail 'sshd-ddos'  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Jail 'sshd-ddos' uses poller {}  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO maxLines: 1  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO maxRetry: 5  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO findtime: 600  
2023-12-29 17:53:40,583 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,584 fail2ban.filterssystemd [7775]: INFO [sshd] Jail is in operation now (process new journa  
ntries)  
2023-12-29 17:53:40,584 fail2ban.jail [7775]: INFO Jail 'sshd' started  
2023-12-29 17:53:40,585 fail2ban.jail [7775]: INFO Jail 'selinux-ssh' started  
2023-12-29 17:53:40,587 fail2ban.jail [7775]: INFO Jail 'apache-auth' started  
2023-12-29 17:53:40,588 fail2ban.jail [7775]: INFO Jail 'apache-badbots' started  
2023-12-29 17:53:40,589 fail2ban.jail [7775]: INFO Jail 'apache-noscript' started  
2023-12-29 17:53:40,592 fail2ban.jail [7775]: INFO Jail 'apache-overflows' started  
2023-12-29 17:53:40,603 fail2ban.jail [7775]: INFO Jail 'apache-nohomo' started  
2023-12-29 17:53:40,604 fail2ban.jail [7775]: INFO Jail 'apache-botsearch' started  
2023-12-29 17:53:40,605 fail2ban.jail [7775]: INFO Jail 'apache-fakegooglebot' started  
2023-12-29 17:53:40,606 fail2ban.jail [7775]: INFO Jail 'apache-modsecurity' started  
2023-12-29 17:53:40,607 fail2ban.jail [7775]: INFO Jail 'apache-shellshock' started  
2023-12-29 17:53:40,607 fail2ban.jail [7775]: INFO Jail 'sshd-ddos' started
```

Рис. 5: Просмотр журнала событий fail2ban



```
root@server:~
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true

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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Рис. 6: Включение защиты почты в файле customisation.local

Защита с помощью Fail2ban

```
root@server:~  
2023-12-29 17:55:04,280 fail2ban.jail [7834]: INFO Initiated 'systemd' backend  
2023-12-29 17:55:04,294 fail2ban.datedetector [7834]: INFO date pattern '%Y-%m-%d %H:%M:%S' [LN-BEG]TAI64N'  
2023-12-29 17:55:04,294 fail2ban.filterssystemd [7834]: INFO [dovecot] Added journal match for: '_SYSTEMD_UNIT=do  
not.service'  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,294 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Creating new jail 'postfix-sasl'  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Jail 'postfix-sasl' uses systemd ()  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Initiated 'systemd' backend  
2023-12-29 17:55:04,296 fail2ban.filterssystemd [7834]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_U  
nit=postfix.service'  
2023-12-29 17:55:04,296 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,296 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,297 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,297 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,297 fail2ban.jail [7834]: INFO Creating new jail 'sshd-ddos'  
2023-12-29 17:55:04,297 fail2ban.jail [7834]: INFO Jail 'sshd-ddos' uses poller ()  
2023-12-29 17:55:04,298 fail2ban.jail [7834]: INFO Initiated 'polling' backend  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO maxlines: 1  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,300 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,301 fail2ban.filterssystemd [7834]: INFO [sshd] Jail is in operation now (process new journa  
l entries)  
2023-12-29 17:55:04,302 fail2ban.jail [7834]: INFO Jail 'sshd' started  
2023-12-29 17:55:04,303 fail2ban.jail [7834]: INFO Jail 'selinux-ssh' started  
2023-12-29 17:55:04,303 fail2ban.jail [7834]: INFO Jail 'apache-auth' started  
2023-12-29 17:55:04,304 fail2ban.jail [7834]: INFO Jail 'apache-badbots' started  
2023-12-29 17:55:04,304 fail2ban.jail [7834]: INFO Jail 'apache-noscript' started  
2023-12-29 17:55:04,305 fail2ban.jail [7834]: INFO Jail 'apache-overflows' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-nohome' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-botsearch' started  
2023-12-29 17:55:04,310 fail2ban.jail [7834]: INFO Jail 'apache-fakegooglebot' started  
2023-12-29 17:55:04,320 fail2ban.jail [7834]: INFO Jail 'apache-modsecurity' started  
2023-12-29 17:55:04,321 fail2ban.jail [7834]: INFO Jail 'apache-shellshock' started  
2023-12-29 17:55:04,322 fail2ban.jail [7834]: INFO Jail 'postfix' started  
2023-12-29 17:55:04,323 fail2ban.jail [7834]: INFO Jail 'postfix-rbl' started  
2023-12-29 17:55:04,323 fail2ban.filterssystemd [7834]: INFO [postfix] Jail is in operation now (process new jou  
l entries)  
2023-12-29 17:55:04,324 fail2ban.filterssystemd [7834]: INFO [postfix-rbl] Jail is in operation now (process new  
journal entries)  
2023-12-29 17:55:04,329 fail2ban.jail [7834]: INFO Jail 'dovecot' started  
2023-12-29 17:55:04,331 fail2ban.filterssystemd [7834]: INFO [dovecot] Jail is in operation now (process new jou  
l entries)  
2023-12-29 17:55:04,331 fail2ban.filterssystemd [7834]: INFO [postfix-sasl] Jail is in operation now (process ne  
w journal entries)  
2023-12-29 17:55:04,332 fail2ban.jail [7834]: INFO Jail 'postfix-sasl' started  
2023-12-29 17:55:04,332 fail2ban.jail [7834]: INFO Jail 'sshd-ddos' started
```

Рис. 7: Просмотр журнала событий fail2ban

```
[root@server.eademidova.net ~]# systemctl restart fail2ban
[root@server.eademidova.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, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.eademidova.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.eademidova.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.eademidova.net ~]#
```

Рис. 8: Просмотр статуса fail2ban, защиты SSH и установка количества ошибок для SSH

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

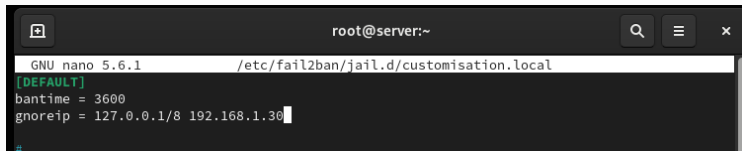
Рис. 9: Попытки соединения по SSH с сервером с неправильным паролем


```
[root@server.eademidova.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 1
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  `-- Banned IP list:
[root@server.eademidova.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: 192.168.1.30
[root@server.eademidova.net ~]#
```

Рис. 10: Проверка блокировки клиента на сервере

```
- Banned IP list: 192.168.1.30
[root@server.eademidova.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.eademidova.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.eademidova.net ~]#
```

Рис. 11: Снятие блокировки с клиента



```
root@server:~  
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local  
[DEFAULT]  
bantime = 3600  
ignoreip = 127.0.0.1/8 192.168.1.30
```

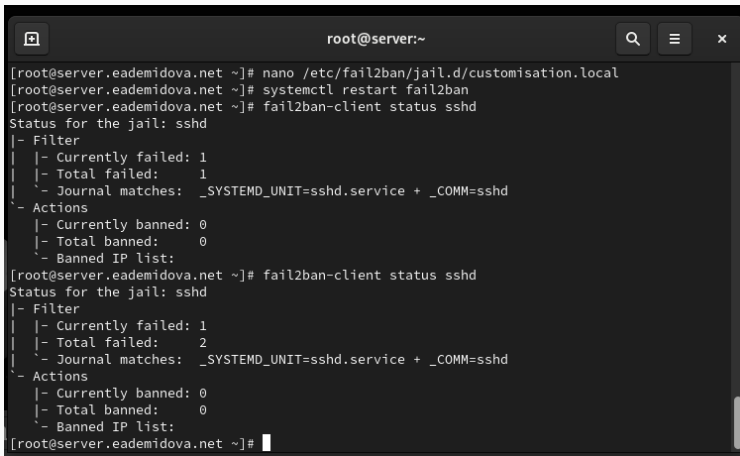
Рис. 12: Добавление в конфигурационный файл игнорирования адреса клиента

Проверка работы Fail2ban

```
root@server:~# journalctl -u fail2ban.service --no-pager --output=cat

2023-12-29 18:08:22,000 fail2ban.jail [8234]: INFO Initiated 'systemd' backend
2023-12-29 18:08:22,010 fail2ban.datedetector [8234]: INFO date pattern '': ['%LN-BEG']TAI64N'
2023-12-29 18:08:22,020 fail2ban.filterssystemd [8234]: INFO [dovecot] Added journal match for: '_SYSTEMD_UNIT=
cot.service'
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,020 fail2ban.actions [8234]: INFO bantime: 3600
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Creating new jail 'postfix-sasl'
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Jail 'postfix-sasl' uses systemd {}
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Initiated 'systemd' backend
2023-12-29 18:08:22,023 fail2ban.filterssystemd [8234]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_
postfix.service'
2023-12-29 18:08:22,023 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,024 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,024 fail2ban.actions [8234]: INFO bantime: 3600
2023-12-29 18:08:22,024 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,024 fail2ban.jail [8234]: INFO Creating new jail 'sshd-ddos'
2023-12-29 18:08:22,025 fail2ban.jail [8234]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-29 18:08:22,025 fail2ban.jail [8234]: INFO Initiated 'polling' backend
2023-12-29 18:08:22,026 fail2ban.filter [8234]: INFO maxlines: 1
2023-12-29 18:08:22,030 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,031 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,031 fail2ban.actions [8234]: INFO bantime: 3600
2023-12-29 18:08:22,031 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,034 fail2ban.filterssystemd [8234]: INFO [sshd] Jail is in operation now (process new jour
n entries)
2023-12-29 18:08:22,035 fail2ban.jail [8234]: INFO Jail 'sshd' started
2023-12-29 18:08:22,036 fail2ban.jail [8234]: INFO Jail 'selinux-ssh' started
2023-12-29 18:08:22,037 fail2ban.jail [8234]: INFO Jail 'apache-auth' started
2023-12-29 18:08:22,037 fail2ban.jail [8234]: INFO Jail 'apache-badbots' started
2023-12-29 18:08:22,038 fail2ban.jail [8234]: INFO Jail 'apache-noscript' started
2023-12-29 18:08:22,039 fail2ban.jail [8234]: INFO Jail 'apache-overflows' started
2023-12-29 18:08:22,039 fail2ban.jail [8234]: INFO Jail 'apache-nohome' started
2023-12-29 18:08:22,040 fail2ban.jail [8234]: INFO Jail 'apache-botsearch' started
2023-12-29 18:08:22,040 fail2ban.jail [8234]: INFO Jail 'apache-fakegooglebot' started
2023-12-29 18:08:22,041 fail2ban.jail [8234]: INFO Jail 'apache-modsecurity' started
2023-12-29 18:08:22,040 fail2ban.jail [8234]: INFO Jail 'apache-shellshock' started
2023-12-29 18:08:22,050 fail2ban.filterssystemd [8234]: INFO [postfix] Jail is in operation now (process new jo
urn entries)
2023-12-29 18:08:22,051 fail2ban.jail [8234]: INFO Jail 'postfix' started
2023-12-29 18:08:22,051 fail2ban.filterssystemd [8234]: INFO [postfix-rbl] Jail is in operation now (process ne
w journal entries)
2023-12-29 18:08:22,052 fail2ban.jail [8234]: INFO Jail 'postfix-rbl' started
2023-12-29 18:08:22,052 fail2ban.filterssystemd [8234]: INFO [dovecot] Jail is in operation now (process new jo
urn entries)
2023-12-29 18:08:22,052 fail2ban.jail [8234]: INFO Jail 'dovecot' started
2023-12-29 18:08:22,053 fail2ban.filterssystemd [8234]: INFO [postfix-sasl] Jail is in operation now (process n
ew journal entries)
2023-12-29 18:08:22,053 fail2ban.jail [8234]: INFO Jail 'postfix-sasl' started
2023-12-29 18:08:22,053 fail2ban.jail [8234]: INFO Jail 'sshd-ddos' started
```

Рис. 13: Просмотр журнала событий fail2ban



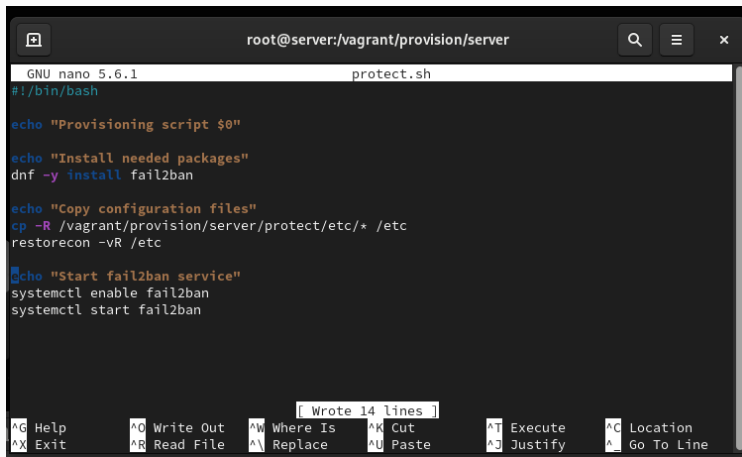
```
root@server:~  
[root@server.eademidova.net ~]# nano /etc/fail2ban/jail.d/customisation.local  
[root@server.eademidova.net ~]# systemctl restart fail2ban  
[root@server.eademidova.net ~]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 1  
| |- Total failed: 1  
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| `-- Banned IP list:  
[root@server.eademidova.net ~]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 1  
| |- Total failed: 2  
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| `-- Banned IP list:  
[root@server.eademidova.net ~]#
```

Рис. 14: Просмотр статуса защиты SSH после подключения к серверу с клиента по SSH с неправильным паролем

```
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/

touch protect.sh
chmod +x protect.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



The screenshot shows a terminal window with a dark background. The title bar at the top reads "root@server:/vagrant/provision/server". Inside the terminal, the GNU nano 5.6.1 editor is open, editing a file named "protect.sh". The script content is as follows:

```
#!/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
```

At the bottom of the terminal, a status bar indicates "Wrote 14 lines". Below this, a row of keyboard shortcuts is displayed:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^I Replace	^U Paste	^J Justify	^_ Go To Line

Рис. 15: Скрипта файла /vagrant/provision/server/protect.sh

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


Заключение

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