

# Лабораторная работа №16

Тема «Базовая защита от атак типа “brute force”»  
по дисциплине «Администрирование сетевых подсистем»

Выполнил: Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«23» декабря 2023г.

## **Цель работы:**

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

## **Задание**

1. Установить и настроить Fail2ban для отслеживания работы установленных на сервере служб.
2. Проверить работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
3. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban.

# Выполнение работы

## Защита с помощью Fail2ban

```
root@server:~  
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i  
[sudo] password for mrshcherbak:  
[root@server.mrshcherbak.net ~]# dnf -y install fail2ban  
Last metadata expiration check: 0:12:08 ago on Wed 20 Dec 2023 08:16:18 PM MSK.  
Dependencies resolved.  
=====
```

Package	Architecture	Size	Ver
sion	Repository		
Installing:			
fail2ban	noarch	8.5 k	1.0

```
=====
```

```
[root@server.mrshcherbak.net ~]# systemctl start fail2ban  
[root@server.mrshcherbak.net ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.  
[root@server.mrshcherbak.net ~]# touch /etc/fail2ban/jail.d/customisation.local  
[root@server.mrshcherbak.net ~]# mc
```

```
mc [root@server.mrshcherbak.net]:/etc/fail2ban/jail.d  
root@server:... x mrshcherbak... x mc [root@se... x root@server:~ x  
/etc/fail2ban/jail.d/customisation.local 154/154 100%  
[DEFAULT]  
bantime = 3600  
#  
# SSH servers  
#  
[sshd]  
port = ssh,2022  
enabled = true  
[sshd-ddos]  
filter = sshd  
enabled = true  
[selinux-ssh]  
enabled = true  
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

Содержимое файла с локальной конфигурацией fail2ban

root@server:/vagrant/provision/server ×	root@server:~ ×	root@server:/vagrant/provision/server ×	mrshcherbak@server:~
2023-12-20 20:31:44,579 fail2ban.observer	[9239]: INFO	Observer start...	
2023-12-20 20:31:44,584 fail2ban.database	[9239]: INFO	Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'	
2023-12-20 20:31:44,585 fail2ban.jail	[9239]: INFO	Creating new jail 'sshd'	
2023-12-20 20:31:44,617 fail2ban.jail	[9239]: INFO	Jail 'sshd' uses systemd {}	
2023-12-20 20:31:44,618 fail2ban.jail	[9239]: INFO	Initiated 'systemd' backend	
2023-12-20 20:31:44,619 fail2ban.filter	[9239]: INFO	maxLines: 1	
2023-12-20 20:31:44,669 fail2ban.filtersystemd	[9239]: INFO	[sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'	
2023-12-20 20:31:44,670 fail2ban.filter	[9239]: INFO	maxRetry: 5	
2023-12-20 20:31:44,670 fail2ban.filter	[9239]: INFO	findtime: 600	
2023-12-20 20:31:44,670 fail2ban.actions	[9239]: INFO	banTime: 3600	
2023-12-20 20:31:44,671 fail2ban.filter	[9239]: INFO	encoding: UTF-8	
2023-12-20 20:31:44,671 fail2ban.jail	[9239]: INFO	Creating new jail 'selinux-ssh'	
2023-12-20 20:31:44,678 fail2ban.jail	[9239]: INFO	Jail 'selinux-ssh' uses poller {}	
2023-12-20 20:31:44,679 fail2ban.jail	[9239]: INFO	Initiated 'polling' backend	
2023-12-20 20:31:44,683 fail2ban.datedetector	[9239]: INFO	date pattern '': 'Epoch'	
2023-12-20 20:31:44,683 fail2ban.filter	[9239]: INFO	maxRetry: 5	
2023-12-20 20:31:44,683 fail2ban.filter	[9239]: INFO	findtime: 600	
2023-12-20 20:31:44,684 fail2ban.actions	[9239]: INFO	banTime: 3600	
2023-12-20 20:31:44,684 fail2ban.filter	[9239]: INFO	encoding: UTF-8	
2023-12-20 20:31:44,686 fail2ban.filter	[9239]: INFO	Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 5ff4429bfdbc6fc7f30c76f31c1634bc68130b4a)	
2023-12-20 20:31:44,686 fail2ban.jail	[9239]: INFO	Creating new jail 'sshd-ddos'	
2023-12-20 20:31:44,687 fail2ban.jail	[9239]: INFO	Jail 'sshd-ddos' uses poller {}	
2023-12-20 20:31:44,687 fail2ban.jail	[9239]: INFO	Initiated 'polling' backend	
2023-12-20 20:31:44,691 fail2ban.filter	[9239]: INFO	maxLines: 1	
2023-12-20 20:31:44,694 fail2ban.filter	[9239]: INFO	maxRetry: 5	
2023-12-20 20:31:44,695 fail2ban.filter	[9239]: INFO	findtime: 600	
2023-12-20 20:31:44,695 fail2ban.actions	[9239]: INFO	banTime: 3600	
2023-12-20 20:31:44,695 fail2ban.filter	[9239]: INFO	encoding: UTF-8	
2023-12-20 20:31:44,713 fail2ban.filtersystemd	[9239]: INFO	[sshd] Jail is in operation now (process new journal entries)	
2023-12-20 20:31:44,714 fail2ban.jail	[9239]: INFO	Jail 'sshd' started	
2023-12-20 20:31:44,716 fail2ban.jail	[9239]: INFO	Jail 'selinux-ssh' started	
2023-12-20 20:31:44,719 fail2ban.jail	[9239]: INFO	Jail 'sshd-ddos' started	

## Просмотр журнала событий

```
mc[root@server.mrshcherbak.net]:/etc/fail2ban/jail.d
root@serv... x mrshcherb... x mc [root@... x root@serv... x
/etc/fail2ban/jail.d/customisation.local 486/486 100%
[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

[apache-shellshock]
enabled = true
1?help 2UnWrap 3Quit
```

Содержимое файла с локальной конфигурацией fail2ban

```
root@server:/vagrant/provision/server x root@server:~ x root@server:/vagrant/provision/server x mrshcherbak@server:~ x
2023-12-20 20:34:06,008 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = acc4421da8e224c93793175cbdb6952313e915b2)
2023-12-20 20:34:06,022 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 8cc870a592c5e53181c1alecbefb311f0a4b47df)
2023-12-20 20:34:06,023 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/www.mrshcherbak.net-error_log' (pos = 0, hash = 286ff0c121674bf00b660c85285eccd1f674362a)
2023-12-20 20:34:06,023 fail2ban.jail [9289]: INFO Creating new jail 'apache-shellshock'
2023-12-20 20:34:06,025 fail2ban.jail [9289]: INFO Jail 'apache-shellshock' uses poller {}
2023-12-20 20:34:06,025 fail2ban.jail [9289]: INFO Initiated 'polling' backend
2023-12-20 20:34:06,031 fail2ban.filter [9289]: INFO maxRetry: 1
2023-12-20 20:34:06,043 fail2ban.filter [9289]: INFO findtime: 600
2023-12-20 20:34:06,043 fail2ban.actions [9289]: INFO banTime: 3600
2023-12-20 20:34:06,044 fail2ban.filter [9289]: INFO encoding: UTF-8
2023-12-20 20:34:06,044 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/server.mrshcherbak.net-error_log' (pos = 0, hash = )
2023-12-20 20:34:06,045 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = acc4421da8e224c93793175cbdb6952313e915b2)
2023-12-20 20:34:06,046 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 8cc870a592c5e53181c1alecbefb311f0a4b47df)
2023-12-20 20:34:06,046 fail2ban.filter [9289]: INFO Added logfile: '/var/log/httpd/www.mrshcherbak.net-error_log' (pos = 0, hash = 286ff0c121674bf00b660c85285eccd1f674362a)
2023-12-20 20:34:06,047 fail2ban.jail [9289]: INFO Creating new jail 'sshd-ddos'
2023-12-20 20:34:06,049 fail2ban.jail [9289]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-20 20:34:06,051 fail2ban.jail [9289]: INFO Initiated 'polling' backend
2023-12-20 20:34:06,056 fail2ban.filter [9289]: INFO maxLines: 1
2023-12-20 20:34:06,074 fail2ban.filter [9289]: INFO maxRetry: 5
2023-12-20 20:34:06,075 fail2ban.filter [9289]: INFO findtime: 600
2023-12-20 20:34:06,075 fail2ban.actions [9289]: INFO banTime: 3600
2023-12-20 20:34:06,076 fail2ban.filter [9289]: INFO encoding: UTF-8
2023-12-20 20:34:06,077 fail2ban.filtersystemd [9289]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-12-20 20:34:06,078 fail2ban.jail [9289]: INFO Jail 'sshd' started
2023-12-20 20:34:06,091 fail2ban.jail [9289]: INFO Jail 'selinux-ssh' started
2023-12-20 20:34:06,104 fail2ban.jail [9289]: INFO Jail 'apache-auth' started
2023-12-20 20:34:06,106 fail2ban.jail [9289]: INFO Jail 'apache-badbots' started
2023-12-20 20:34:06,146 fail2ban.jail [9289]: INFO Jail 'apache-noscript' started
2023-12-20 20:34:06,159 fail2ban.jail [9289]: INFO Jail 'apache-overflows' started
2023-12-20 20:34:06,167 fail2ban.jail [9289]: INFO Jail 'apache-nohome' started
2023-12-20 20:34:06,189 fail2ban.jail [9289]: INFO Jail 'apache-botsearch' started
2023-12-20 20:34:06,194 fail2ban.jail [9289]: INFO Jail 'apache-fakegooglebot' started
2023-12-20 20:34:06,198 fail2ban.jail [9289]: INFO Jail 'apache-modsecurity' started
2023-12-20 20:34:06,215 fail2ban.jail [9289]: INFO Jail 'apache-shellshock' started
2023-12-20 20:34:06,218 fail2ban.jail [9289]: INFO Jail 'sshd-ddos' started
```

```
mc [root@server.mrshcherbak.net]:/etc/fail2ban/jail.d
root@ser... x mrshcher... x mc [root... x root@serv... x
customis~n.local [----] 0 L: [ 43+22 65/ 65] *(619 / 619b) <E0F> [*] [X]

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true

#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true

1Help 2Save 3Mark
```

Содержимое файла с локальной конфигурацией fail2ban

root@server:/vagrant/provision/server	root@server:~	root@server:/vagrant/provision/server
2023-12-20 20:35:45,536 fail2ban.filtersystemd	[9356]: INFO	[postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2023-12-20 20:35:45,541 fail2ban.filter	[9356]: INFO	maxRetry: 5
2023-12-20 20:35:45,542 fail2ban.filter	[9356]: INFO	findtime: 600
2023-12-20 20:35:45,542 fail2ban.actions	[9356]: INFO	banTime: 3600
2023-12-20 20:35:45,543 fail2ban.filter	[9356]: INFO	encoding: UTF-8
2023-12-20 20:35:45,543 fail2ban.jail	[9356]: INFO	Creating new jail 'sshd-ddos'
2023-12-20 20:35:45,545 fail2ban.jail	[9356]: INFO	Jail 'sshd-ddos' uses poller {}
2023-12-20 20:35:45,546 fail2ban.jail	[9356]: INFO	Initiated 'polling' backend
2023-12-20 20:35:45,552 fail2ban.filter	[9356]: INFO	maxLines: 1
2023-12-20 20:35:45,568 fail2ban.filter	[9356]: INFO	maxRetry: 5
2023-12-20 20:35:45,569 fail2ban.filter	[9356]: INFO	findtime: 600
2023-12-20 20:35:45,569 fail2ban.actions	[9356]: INFO	banTime: 3600
2023-12-20 20:35:45,569 fail2ban.filter	[9356]: INFO	encoding: UTF-8
2023-12-20 20:35:45,570 fail2ban.filtersystemd	[9356]: INFO	[sshd] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,571 fail2ban.jail	[9356]: INFO	Jail 'sshd' started
2023-12-20 20:35:45,573 fail2ban.jail	[9356]: INFO	Jail 'selinux-ssh' started
2023-12-20 20:35:45,577 fail2ban.jail	[9356]: INFO	Jail 'apache-auth' started
2023-12-20 20:35:45,581 fail2ban.jail	[9356]: INFO	Jail 'apache-badbots' started
2023-12-20 20:35:45,583 fail2ban.jail	[9356]: INFO	Jail 'apache-noscript' started
2023-12-20 20:35:45,586 fail2ban.jail	[9356]: INFO	Jail 'apache-overflows' started
2023-12-20 20:35:45,587 fail2ban.jail	[9356]: INFO	Jail 'apache-nohome' started
2023-12-20 20:35:45,588 fail2ban.jail	[9356]: INFO	Jail 'apache-botsearch' started
2023-12-20 20:35:45,589 fail2ban.jail	[9356]: INFO	Jail 'apache-fakegooglebot' started
2023-12-20 20:35:45,597 fail2ban.jail	[9356]: INFO	Jail 'apache-modsecurity' started
2023-12-20 20:35:45,602 fail2ban.jail	[9356]: INFO	Jail 'apache-shellshock' started
2023-12-20 20:35:45,605 fail2ban.jail	[9356]: INFO	Jail 'postfix' started
2023-12-20 20:35:45,618 fail2ban.filtersystemd	[9356]: INFO	[postfix] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,619 fail2ban.filtersystemd	[9356]: INFO	[postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,620 fail2ban.jail	[9356]: INFO	Jail 'postfix-rbl' started
2023-12-20 20:35:45,627 fail2ban.jail	[9356]: INFO	Jail 'dovecot' started
2023-12-20 20:35:45,636 fail2ban.filtersystemd	[9356]: INFO	[dovecot] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,637 fail2ban.filtersystemd	[9356]: INFO	[postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-20 20:35:45,638 fail2ban.jail	[9356]: INFO	Jail 'postfix-sasl' started
2023-12-20 20:35:45,638 fail2ban.jail	[9356]: INFO	Jail 'sshd-ddos' started

# Проверка работы Fail2ban

```
root@server:/vagrant/provision/server

root@server:/vagr... x root@server:~ x root@server:/vagr... x mrshcherbak@se... x

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

Попытка входа с клиента по SSH на сервер с неправильным паролем

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

Просмотр журнала событий

```
root@server:/vagr... x root@server:~ x root@server:/vagra... x mrshcherbak@serv... x

2023-12-20 20:37:11,270 fail2ban.filter [9356]: INFO maxRetry: 2
2023-12-20 20:49:13,255 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:49:12
2023-12-20 20:50:06,331 fail2ban.filter [9356]: INFO maxRetry: 2
2023-12-20 20:59:02,984 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:02
2023-12-20 20:59:03,423 fail2ban.actions [9356]: NOTICE [sshd] Ban 192.168.1.142
2023-12-20 20:59:08,019 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:07
2023-12-20 20:59:14,269 fail2ban.filter [9356]: INFO [sshd] Found 192.168.1.142 - 2023-12-20 20:59:13
2023-12-20 20:59:14,424 fail2ban.actions [9356]: NOTICE [sshd] 192.168.1.142 already banned
```



```
[root@server.mrshcherbak.net jail.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: 1
    |- Total banned:     1
    `-- Banned IP list:  192.168.1.142

[root@server.mrshcherbak.net jail.d]# fail2ban-client set sshd unbanip 192.168.1.142
1
[root@server.mrshcherbak.net jail.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:
```

Просмотр статуса защиты SSH

Содержимое файла  
/etc/fail2ban/jail.d/customisation.local

```
mc [root@server.mrshcherbak.net]:/etc/fail2ban/jail.d
root@ser... x mrshcher... x mc [root... x root@ser... x
customis~n.local [B---] 0 L:[ 1+ 2 3/ 66] *(25 / 656b) 0105 0x[*][X]
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.142
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
#
# HTTP servers
#
[apache-auth]
enabled = true
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Se~ch 8Delete 9PullDn10Quit
```

```
root@server:/vagr... x root@server:~ x root@server:/vagr... x mrshcherbak@ser... x
2023-12-20 21:03:41,588 fail2ban.jail [9912]: INFO Initiated 'polling' backend
2023-12-20 21:03:41,592 fail2ban.filter [9912]: INFO maxLines: 1
2023-12-20 21:03:41,601 fail2ban.filter [9912]: INFO maxRetry: 5
2023-12-20 21:03:41,606 fail2ban.filter [9912]: INFO findtime: 600
2023-12-20 21:03:41,607 fail2ban.actions [9912]: INFO banTime: 3600
2023-12-20 21:03:41,607 fail2ban.filter [9912]: INFO encoding: UTF-8
2023-12-20 21:03:41,609 fail2ban.filtersystemd [9912]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,612 fail2ban.jail [9912]: INFO Jail 'sshd' started
2023-12-20 21:03:41,632 fail2ban.jail [9912]: INFO Jail 'selinux-ssh' started
2023-12-20 21:03:41,635 fail2ban.jail [9912]: INFO Jail 'apache-auth' started
2023-12-20 21:03:41,637 fail2ban.jail [9912]: INFO Jail 'apache-badbots' started
2023-12-20 21:03:41,648 fail2ban.jail [9912]: INFO Jail 'apache-noscript' started
2023-12-20 21:03:41,663 fail2ban.jail [9912]: INFO Jail 'apache-overflows' started
2023-12-20 21:03:41,665 fail2ban.jail [9912]: INFO Jail 'apache-nohome' started
2023-12-20 21:03:41,667 fail2ban.jail [9912]: INFO Jail 'apache-botsearch' started
2023-12-20 21:03:41,669 fail2ban.jail [9912]: INFO Jail 'apache-fakegooglebot' started
2023-12-20 21:03:41,678 fail2ban.jail [9912]: INFO Jail 'apache-modsecurity' started
2023-12-20 21:03:41,683 fail2ban.jail [9912]: INFO Jail 'apache-shellshock' started
2023-12-20 21:03:41,684 fail2ban.filtersystemd [9912]: INFO [postfix] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,686 fail2ban.jail [9912]: INFO Jail 'postfix' started
2023-12-20 21:03:41,687 fail2ban.filtersystemd [9912]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,688 fail2ban.jail [9912]: INFO Jail 'postfix-rbl' started
2023-12-20 21:03:41,689 fail2ban.filtersystemd [9912]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,691 fail2ban.jail [9912]: INFO Jail 'dovecot' started
2023-12-20 21:03:41,692 fail2ban.filtersystemd [9912]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-12-20 21:03:41,693 fail2ban.jail [9912]: INFO Jail 'postfix-sasl' started
2023-12-20 21:03:41,694 fail2ban.jail [9912]: INFO Jail 'sshd-ddos' started
2023-12-20 21:04:49,039 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
2023-12-20 21:04:53,769 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
2023-12-20 21:04:56,769 fail2ban.filter [9912]: INFO [sshd] Ignore 192.168.1.142 by ip
```

```
[root@client.mrshcherbak.net ~]# ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
Permission denied, please try again.
mrshcherbak@server.mrshcherbak.net's password:
mrshcherbak@server.mrshcherbak.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.mrshcherbak.net ~]# ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

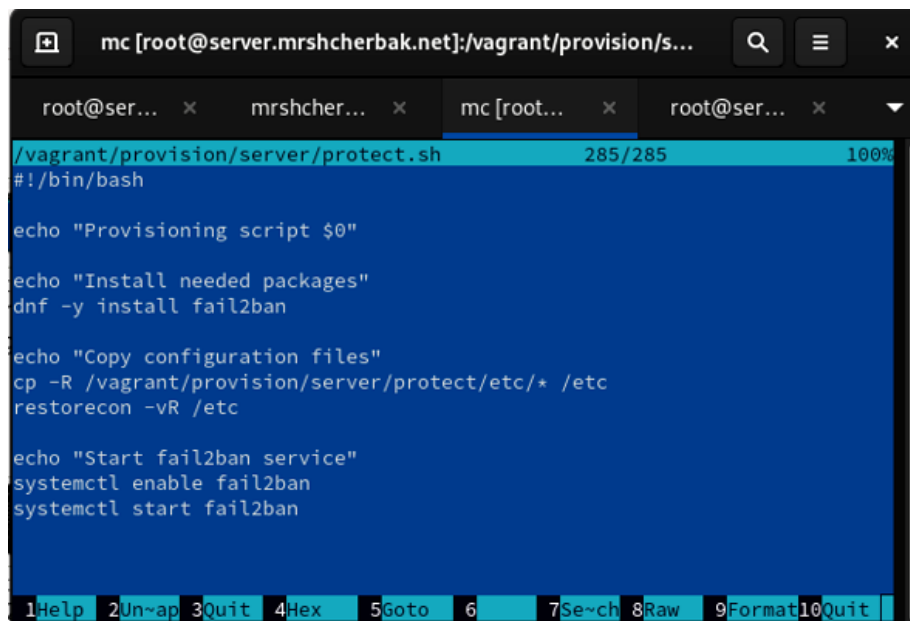
Last failed login: Wed Dec 20 21:04:56 MSK 2023 from 192.168.1.142 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Wed Dec 20 21:01:47 2023 from 192.168.1.142
[mrshcherbak@server.mrshcherbak.net ~]#
```

```
[root@server.mrshcherbak.net jail.d]# systemctl restart fail2ban
[root@server.mrshcherbak.net jail.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:
```

Просмотр статуса защиты SSH

## Внесение изменений в настройки внутреннего окружения виртуальных машин

```
[root@server.mrshcherbak.net jail.d]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.mrshcherbak.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.mrshcherbak.net server]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# touch protect.sh
[root@server.mrshcherbak.net server]# chmod +x protect.sh
[root@server.mrshcherbak.net server]# mc
```



```
mc [root@server.mrshcherbak.net]:/vagrant/provision/s...
root@ser... x mrshcher... x mc [root... x root@ser... x
/vagrant/provision/server/protect.sh 285/285 100%
#!/bin/bash

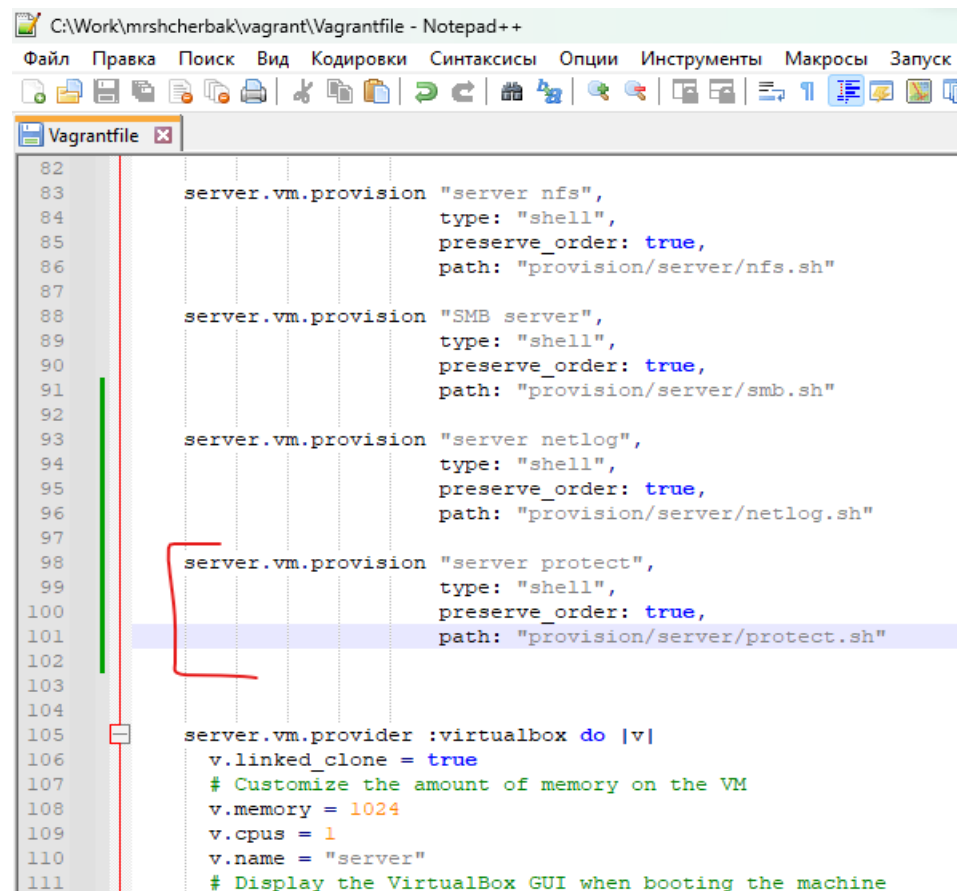
echo "Provisioning script $0"

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

1Help 2Un~ap 3Quit 4Hex 5Goto 6 7Se~ch 8Raw 9Format10Quit
```



```
C:\Work\mrshcherbak\vagrant\Vagrantfile - Notepad++
Файл  Правка  Поиск  Вид  Кодировки  Синтаксисы  Опции  Инструменты  Макросы  Запуск

Vagrantfile x
82
83     server.vm.provision "server nfs",
84         type: "shell",
85         preserve_order: true,
86         path: "provision/server/nfs.sh"
87
88     server.vm.provision "SMB server",
89         type: "shell",
90         preserve_order: true,
91         path: "provision/server/smb.sh"
92
93     server.vm.provision "server netlog",
94         type: "shell",
95         preserve_order: true,
96         path: "provision/server/netlog.sh"
97
98     server.vm.provision "server protect",
99         type: "shell",
100        preserve_order: true,
101        path: "provision/server/protect.sh"
102
103
104
105     server.vm.provider :virtualbox do |v|
106         v.linked_clone = true
107         # Customize the amount of memory on the VM
108         v.memory = 1024
109         v.cpus = 1
110         v.name = "server"
111         # Display the VirtualBox GUI when booting the machine
```

**Вывод:** таким образом, в ходе выполнения л/р №16 я получила навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».