

Презентация по лабораторной работе №16

Базовая защита от атак типа «brute force»

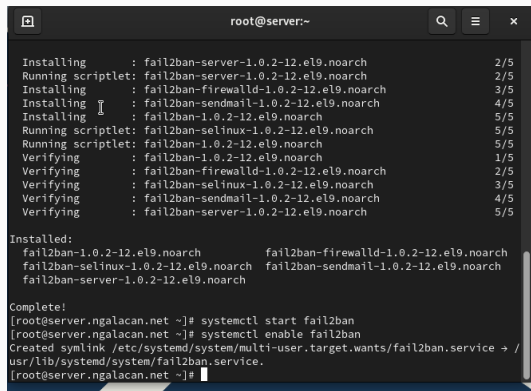
Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

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

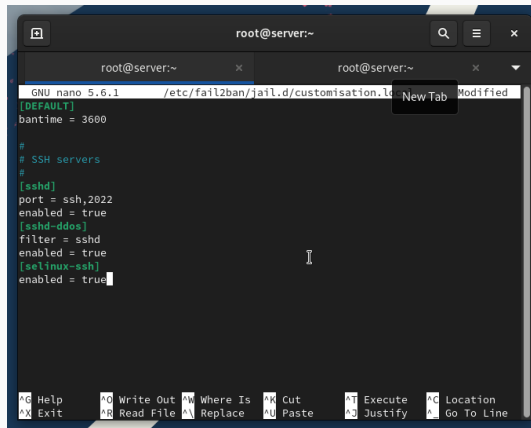
Защита с помощью Fail2ban



```
root@server:~  
  
Installing      : fail2ban-server-1.0.2-12.el9.noarch                2/5  
Running scriptlet: fail2ban-server-1.0.2-12.el9.noarch                2/5  
Installing      : fail2ban-firewalld-1.0.2-12.el9.noarch            3/5  
Installing      : fail2ban-sendmail-1.0.2-12.el9.noarch             4/5  
Installing      : fail2ban-1.0.2-12.el9.noarch                      5/5  
Running scriptlet: fail2ban-selinux-1.0.2-12.el9.noarch             5/5  
Running scriptlet: fail2ban-1.0.2-12.el9.noarch                     5/5  
Verifying       : fail2ban-1.0.2-12.el9.noarch                      1/5  
Verifying       : fail2ban-firewalld-1.0.2-12.el9.noarch           2/5  
Verifying       : fail2ban-selinux-1.0.2-12.el9.noarch             3/5  
Verifying       : fail2ban-sendmail-1.0.2-12.el9.noarch            4/5  
Verifying       : fail2ban-server-1.0.2-12.el9.noarch              5/5  
  
Installed:  
fail2ban-1.0.2-12.el9.noarch      fail2ban-firewalld-1.0.2-12.el9.noarch  
fail2ban-selinux-1.0.2-12.el9.noarch fail2ban-sendmail-1.0.2-12.el9.noarch  
fail2ban-server-1.0.2-12.el9.noarch  
  
Complete!  
[root@server.ngalacan.net ~]# systemctl start fail2ban  
[root@server.ngalacan.net ~]# systemctl enable fail2ban  
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service →  
usr/lib/systemd/system/fail2ban.service.  
[root@server.ngalacan.net ~]#
```

Рис. 1: Установка и запуск fail2ban

Выполнение лабораторной работы



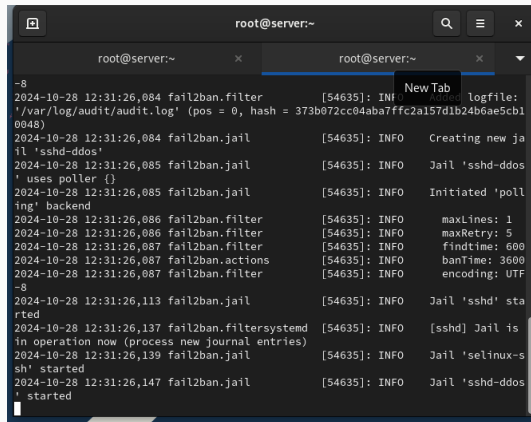
The screenshot shows a terminal window with a dark background. At the top, the prompt is `root@server:~`. Below it, the terminal title bar shows two tabs, both labeled `root@server:~`. The active tab is displaying the contents of the file `/etc/fail2ban/jail.d/customisation.local` using the `nano` text editor (version 5.6.1). The file content is as follows:

```
[DEFAULT]
bantime = 3600

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

The cursor is positioned at the end of the last line. At the bottom of the terminal, a status bar displays various keyboard shortcuts for the nano editor, such as `^G Help`, `^O Write Out`, `^W Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `^X Exit`, `^R Read File`, `^A Replace`, `^U Paste`, `^J Justify`, and `^_ Go To Line`.

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

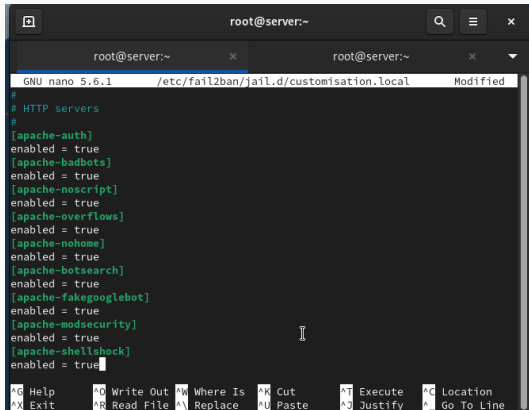


The screenshot shows a terminal window titled 'root@server:~' with a search icon, a menu icon, and a close button. The terminal displays the output of the 'fail2ban' service, which is logging its configuration and startup process. The logs are timestamped '2024-10-28 12:31:26' and show the following sequence of events:

- fail2ban.filter [54635]: INFO logfile: '/var/log/audit/audit.log' (pos = 0, hash = 373b072cc04aba7ffc2a157d1b24b6ae5cb10048)
- fail2ban.jail [54635]: INFO Creating new jail 'sshd-ddos'
- fail2ban.jail [54635]: INFO Jail 'sshd-ddos' uses poller {}
- fail2ban.jail [54635]: INFO Initiated 'polling' backend
- fail2ban.filter [54635]: INFO maxLines: 1
- fail2ban.filter [54635]: INFO maxRetry: 5
- fail2ban.filter [54635]: INFO findtime: 600
- fail2ban.actions [54635]: INFO banTime: 3600
- fail2ban.filter [54635]: INFO encoding: UTF-8
- fail2ban.jail [54635]: INFO Jail 'sshd' started
- fail2ban.filtersystemd [54635]: INFO [sshd] Jail is in operation now (process new journal entries)
- fail2ban.jail [54635]: INFO Jail 'selinux-sh' started
- fail2ban.jail [54635]: INFO Jail 'sshd-ddos' started

Рис. 3: Просмотр журнала событий fail2ban

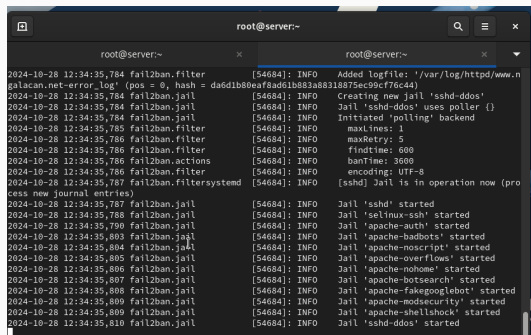
Выполнение лабораторной работы



```
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
```

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

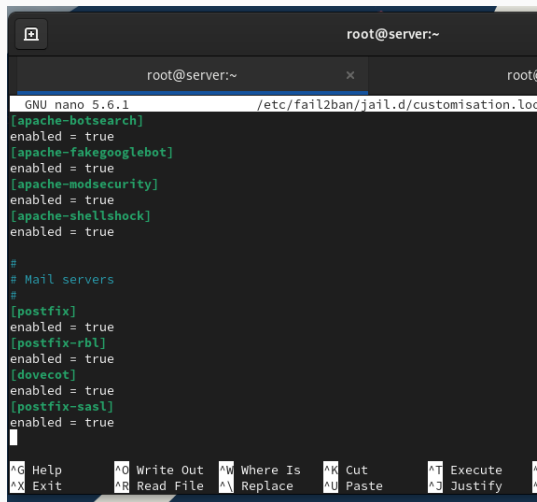
Выполнение лабораторной работы



```
root@server:~  
root@server:~  
2024-10-28 12:34:35,784 fail2ban.filter [54684]: INFO Added logfile: '/var/log/httpd/www.n  
galacan.net_error_log' (pos = 0, hash = da6d1b80eaf8ad61b883a88318875ec99cf76c44)  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Creating new jail 'sshd-ddos'  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Jail 'sshd-ddos' uses poller {}  
2024-10-28 12:34:35,784 fail2ban.jail [54684]: INFO Initiated 'polling' backend  
2024-10-28 12:34:35,785 fail2ban.filter [54684]: INFO maxlines: 1  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO maxRetry: 5  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO findtime: 600  
2024-10-28 12:34:35,786 fail2ban.actions [54684]: INFO banTime: 3600  
2024-10-28 12:34:35,786 fail2ban.filter [54684]: INFO encoding: UTF-8  
2024-10-28 12:34:35,787 fail2ban.Filtersystemd [54684]: INFO [sshd] Jail is in operation now (pro  
cess new journal entries)  
2024-10-28 12:34:35,787 fail2ban.jail [54684]: INFO Jail 'sshd' started  
2024-10-28 12:34:35,788 fail2ban.jail [54684]: INFO Jail 'selinux-ssh' started  
2024-10-28 12:34:35,790 fail2ban.jail [54684]: INFO Jail 'apache-auth' started  
2024-10-28 12:34:35,803 fail2ban.jail [54684]: INFO Jail 'apache-badbots' started  
2024-10-28 12:34:35,804 fail2ban.jail [54684]: INFO Jail 'apache-noscript' started  
2024-10-28 12:34:35,805 fail2ban.jail [54684]: INFO Jail 'apache-overflows' started  
2024-10-28 12:34:35,806 fail2ban.jail [54684]: INFO Jail 'apache-nohome' started  
2024-10-28 12:34:35,807 fail2ban.jail [54684]: INFO Jail 'apache-botsearch' started  
2024-10-28 12:34:35,808 fail2ban.jail [54684]: INFO Jail 'apache-fakegooglebot' started  
2024-10-28 12:34:35,809 fail2ban.jail [54684]: INFO Jail 'apache-modsecurity' started  
2024-10-28 12:34:35,809 fail2ban.jail [54684]: INFO Jail 'apache-shellshock' started  
2024-10-28 12:34:35,810 fail2ban.jail [54684]: INFO Jail 'sshd-ddos' started
```

Рис. 5: Просмотр журнала событий fail2ban

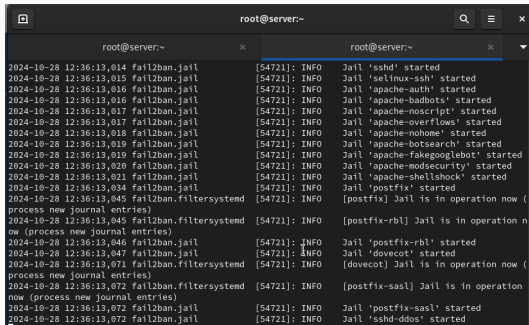
Выполнение лабораторной работы.



```
root@server:~  
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local  
[apache-botsearch]  
enabled = true  
[apache-fakegooglebot]  
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  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

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

Выполнение лабораторной работы



```
root@server:~  
2024-10-28 12:36:13,014 fail2ban.jail [54721]: INFO Jail 'sshd' started  
2024-10-28 12:36:13,015 fail2ban.jail [54721]: INFO Jail 'selinux-ssh' started  
2024-10-28 12:36:13,016 fail2ban.jail [54721]: INFO Jail 'apache-auth' started  
2024-10-28 12:36:13,016 fail2ban.jail [54721]: INFO Jail 'apache-badbots' started  
2024-10-28 12:36:13,017 fail2ban.jail [54721]: INFO Jail 'apache-noscript' started  
2024-10-28 12:36:13,017 fail2ban.jail [54721]: INFO Jail 'apache-overflows' started  
2024-10-28 12:36:13,018 fail2ban.jail [54721]: INFO Jail 'apache-nohome' started  
2024-10-28 12:36:13,019 fail2ban.jail [54721]: INFO Jail 'apache-botsearch' started  
2024-10-28 12:36:13,019 fail2ban.jail [54721]: INFO Jail 'apache-fakegooglebot' started  
2024-10-28 12:36:13,020 fail2ban.jail [54721]: INFO Jail 'apache-modsecurity' started  
2024-10-28 12:36:13,021 fail2ban.jail [54721]: INFO Jail 'apache-shellshock' started  
2024-10-28 12:36:13,034 fail2ban.jail [54721]: INFO Jail 'postfix' started  
2024-10-28 12:36:13,045 fail2ban.filtersystemd [54721]: INFO [postfix] Jail is in operation now (process new journal entries)  
2024-10-28 12:36:13,045 fail2ban.filtersystemd [54721]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)  
2024-10-28 12:36:13,046 fail2ban.jail [54721]: INFO Jail 'postfix-rbl' started  
2024-10-28 12:36:13,047 fail2ban.jail [54721]: INFO Jail 'dovecot' started  
2024-10-28 12:36:13,071 fail2ban.filtersystemd [54721]: INFO [dovecot] Jail is in operation now (process new journal entries)  
2024-10-28 12:36:13,072 fail2ban.filtersystemd [54721]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)  
2024-10-28 12:36:13,072 fail2ban.jail [54721]: INFO Jail 'postfix-sasl' started  
2024-10-28 12:36:13,072 fail2ban.jail [54721]: INFO Jail 'sshd-ddos' started
```

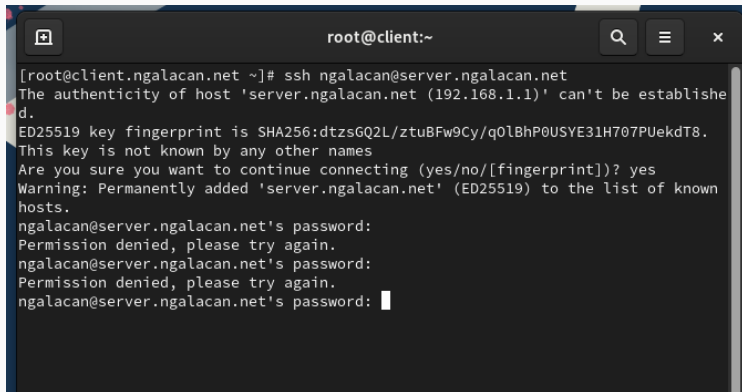
Рис. 7: Просмотр журнала событий fail2ban

Проверка работы Fail2ban

```
fail2ban-client status
```

```
fail2ban-client status sshd
```

```
fail2ban-client set sshd maxretry 2
```

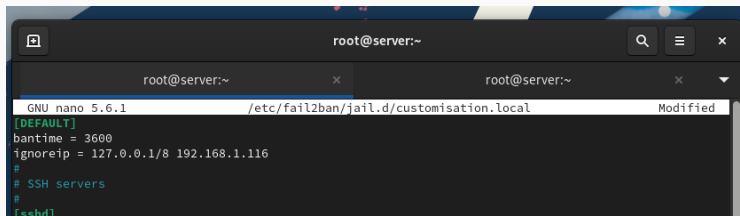


```
root@client:~  
[root@client.ngalacan.net ~]# ssh ngalacan@server.ngalacan.net  
The authenticity of host 'server.ngalacan.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.ngalacan.net' (ED25519) to the list of known hosts.  
ngalacan@server.ngalacan.net's password:  
Permission denied, please try again.  
ngalacan@server.ngalacan.net's password:  
Permission denied, please try again.  
ngalacan@server.ngalacan.net's password: 
```

Рис. 8: Подключение к серверу по SSH с вводом неправильного пароля

```
[root@server.ngalacan.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: 192.168.1.116
[root@server.ngalacan.net ~]# fail2ban-client set sshd unbanip 192.168.1.116
1
[root@server.ngalacan.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.ngalacan.net ~]#
```

Рис. 9: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента



The image shows a terminal window with a dark background. At the top, the prompt is `root@server:~`. Below the prompt, there are two tabs for the nano text editor. The active tab is titled `root@server:~` and shows the file `/etc/fail2ban/jail.d/customisation.local` being edited. The editor's status bar at the top indicates `GNU nano 5.6.1` and `Modified`. The content of the file is as follows:

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.116
#
# SSH servers
#
[sshd]
```

Рис. 10: Редактирование файла с локальной конфигурацией: игнорирование адреса клиента

Выполнение лабораторной работы

```
root@server:~  
root@server:~  
2024-10-28 12:42:19,708 fail2ban.filtersystemd [54797]: INFO [sshd] Jail is in operation now (pro  
cess new journal entries)  
2024-10-28 12:42:19,709 fail2ban.jail [54797]: INFO Jail 'apache-auth' started  
2024-10-28 12:42:19,710 fail2ban.jail [54797]: INFO Jail 'apache-badbots' started  
2024-10-28 12:42:19,711 fail2ban.jail [54797]: INFO Jail 'apache-noscript' started  
2024-10-28 12:42:19,711 fail2ban.jail [54797]: INFO Jail 'apache-overflows' started  
2024-10-28 12:42:19,712 fail2ban.jail [54797]: INFO Jail 'apache-nohome' started  
2024-10-28 12:42:19,713 fail2ban.jail [54797]: INFO Jail 'apache-botsearch' started  
2024-10-28 12:42:19,713 fail2ban.jail [54797]: INFO Jail 'apache-fakegooglebot' started  
2024-10-28 12:42:19,714 fail2ban.jail [54797]: INFO Jail 'apache-modsecurity' started  
2024-10-28 12:42:19,714 fail2ban.jail [54797]: INFO Jail 'apache-shellshock' started  
2024-10-28 12:42:19,715 fail2ban.filtersystemd [54797]: INFO [postfix] Jail is in operation now (pro  
cess new journal entries)  
2024-10-28 12:42:19,715 fail2ban.jail [54797]: INFO Jail 'postfix' started  
2024-10-28 12:42:19,715 fail2ban.filtersystemd [54797]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)  
2024-10-28 12:42:19,716 fail2ban.jail [54797]: INFO Jail 'postfix-rbl' started  
2024-10-28 12:42:19,716 fail2ban.filtersystemd [54797]: INFO [dovecot] Jail is in operation now (process new journal entries)  
2024-10-28 12:42:19,719 fail2ban.jail [54797]: INFO Jail 'dovecot' started  
2024-10-28 12:42:19,720 fail2ban.filtersystemd [54797]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)  
2024-10-28 12:42:19,721 fail2ban.jail [54797]: INFO Jail 'postfix-sasl' started  
2024-10-28 12:42:19,721 fail2ban.jail [54797]: INFO Jail 'sshd-ddos' started
```

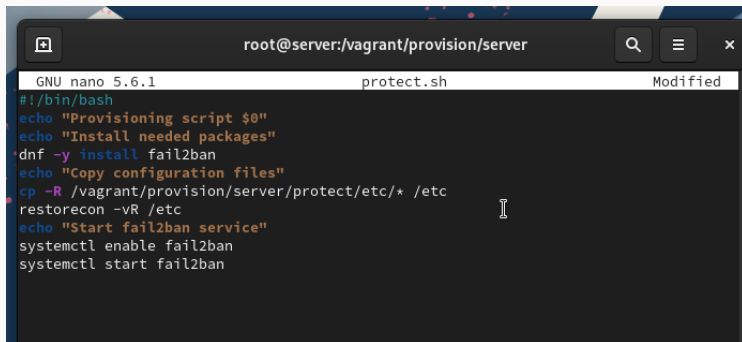
Рис. 11: Просмотр журнала событий 'fail2ban'

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

Рис. 12: Просмотр статуса защиты SSH после неудачного входа

Внесение изменений в настройки
внутреннего окружения
виртуальной машины

```
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/
```



The screenshot shows a terminal window with the title bar 'root@server:/vagrant/provision/server'. The window contains the GNU nano 5.6.1 editor editing the file 'protect.sh'. The editor's status bar at the top indicates 'GNU nano 5.6.1', 'protect.sh', and 'Modified'. The code in the editor 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
```

A cursor is visible on the line 'restorecon -vR /etc'.

Рис. 13: Редактирование protect.sh на сервере

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

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