

## 06. Модуль 1. Задание 5



### Задание

#### Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV

- Для подключения используйте порт 2024
- Разрешите подключения только пользователю sshuser
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only»

### Реализация

#### Настройка SELinux



Необходимо внести изменения в политики SELinux

##### Вариант 1

Если он включен - разрешить этот порт для работы по нему SSH.

```
1 | # semanage port -a -t ssh_port_t -p tcp 2024
2 |
3 | # setenforce 0
```

##### Вариант 2

На время настройки переведите [selinux](#) в режим уведомлений. Для этого измените содержимое конфигурационного файла:

```
1 | # nano /etc/selinux/config
```

Заменяем текст `SELINUX=enforcing` на `SELINUX=permissive`.

Затем выполните:

```
1 | # setenforce 0
```

## Настройка на HQ-SRV

Открываем файл конфигурации SSH `/etc/ssh/sshd_config`

```
1 | # nano /etc/ssh/sshd_config
```



### Изменение порта

Находим директиву `Port 22`

Снимаем комментарий и прописываем номер порта `2024`

```
GNU nano 7.2 /etc/ssh/sshd_co
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2024
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```



### Подключение только пользователю sshuser

Добавляем следующую строку:

1 | AllowUsers sshuser



### Число попыток авторизации

Находим директиву `MaxAuthTries` - количество попыток ввода пароля. По умолчанию `6`. При неудачном переборе сеанс связи обрывается.

1 | MaxAuthTries 2

Снимаем комментарий и изменяем параметр на `2`

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
AllowUsers      sshuser

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 2
#MaxSessions 10
```



### Баннер

Находим директиву `# Banner none`

Снимаем комментарий и указываем путь к файлу `/etc/ssh-banner`, который будет содержать текст баннера.

```
# no default banner path
Banner /etc/ssh-banner

# override default of no subsystems
Subsystem      sftp      /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server
```

Сохраняемся и выходим



Создаем файл в котором содержится пользовательский баннер.

```
1 | # nano /etc/ssh-banner
```

В Файле прописываем текст баннера

```
GNU nano 7.2 /etc/ssh-banner
* * * * *
*
*   Authorized access only   *
*
* * * * *
* * * * *
```



Чтобы применить изменения, перезапускаем службу SSH

```
1 | # systemctl restart sshd
```

## Проверка



С **HQ-CLI** подключаемся по **SSH** к **HQ-SRV**

```
sshuser@hq-srv:~ (на localhost.localdomain)
Файл  Правка  Вид  Поиск  Терминал  Справка
[user@hq-cli ~]$ ssh sshuser@192.168.100.2 -p 2024
* * * * *
*
*   Authorized access only   *
*
* * * * *
sshuser@192.168.100.2's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Fri Oct 11 17:32:15 MSK 2024 from 192.168.100.66 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Oct 11 17:31:56 2024 from 192.168.100.66
[sshuser@hq-srv ~]$
```

## Настройка на BR-SRV



Настройка на **BR-SRV** аналогичная

Содержимое доступно в соответствии с Всеобщее достояние, от Кабинет 2.20. | Powered by [Wiki.js](#)