

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ  
ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 11**

*Дисциплина «Администрирование сетевых подсистем»*

*Тема «Настройка безопасного удалённого доступа по протоколу SSH»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

## Цель работы

Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

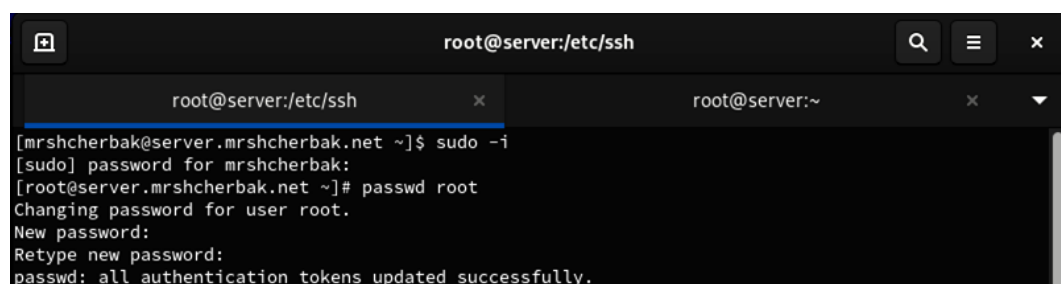
## Задание

1. Настроить запрет удалённого доступа на сервер по SSH для пользователя root.
2. Настроить разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя.
3. Настроить удалённый доступ к серверу по SSH через порт 2022.
4. Настроить удалённый доступ к серверу по SSH по ключу.
5. Организовать SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080.
6. Используя удалённое SSH-соединение, выполнить с клиента несколько команд на сервере.
7. Используя удалённое SSH-соединение, запустить с клиента графическое приложение на сервере.
8. Написать скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Внести изменения в Vagrantfile.

## Выполнение

### 1. Запрет удалённого доступа по SSH для пользователя root

1. На сервере задала пароль для пользователя root (рис.1.1), а в дополнительном терминале запустила мониторинг системных событий.



```
root@server:/etc/ssh
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Рис.1.1. Создание пароля для пользователя root на сервере

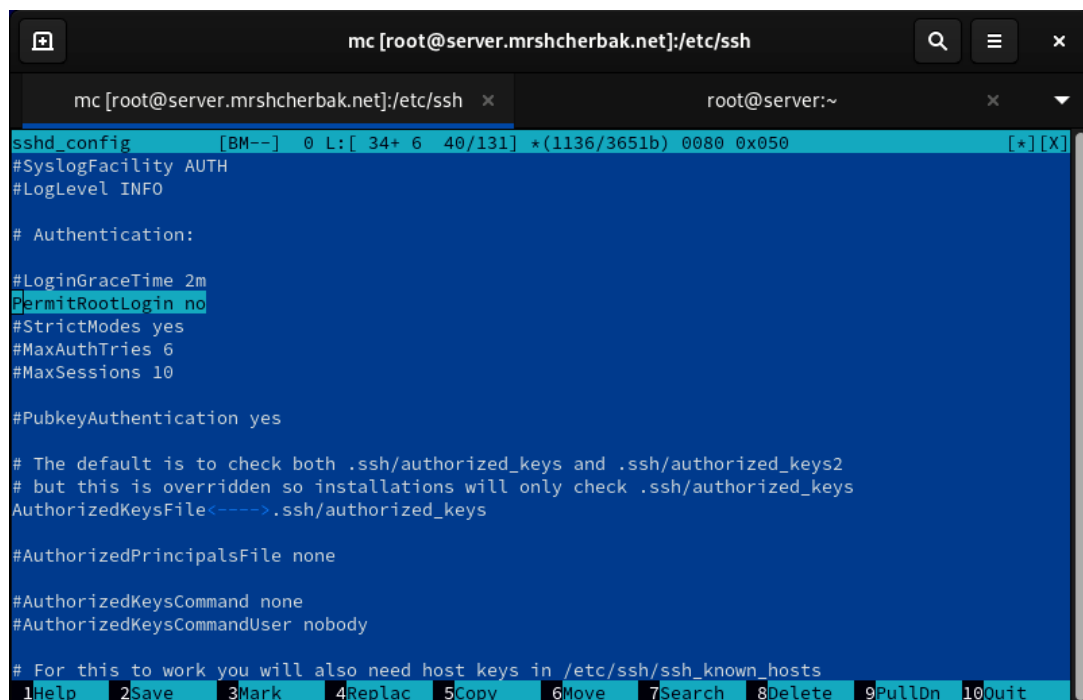
2. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя root (рис.1.2). Доступ есть. Я зашла под рутом на сервер.

```
[mrshcherbak@client.mrshcherbak.net ~]$ ssh root@server.mrshcherbak.net
root@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Dec  7 13:38:08 2023 from 192.168.1.31
[root@server ~]# hostname
server.mrshcherbak.net
[root@server ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@server ~]# logout
Connection to server.mrshcherbak.net closed.
```

Рис.1.2. Получение доступа к серверу посредством SSH-соединения через пользователя root

3. На сервере открыла файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретила вход на сервер пользователю root (рис.1.3).



```
mc [root@server.mrshcherbak.net]:/etc/ssh
mc [root@server.mrshcherbak.net]:/etc/ssh x root@server:~ x
sshd_config [BM--] 0 L: [ 34+ 6 40/131] *(1136/3651b) 0080 0x050 [*] [X]
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<---->.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис.1.3. Запрет входа на сервер пользователю root

4. После сохранения изменений в файле конфигурации перезапустила sshd с помощью команды `systemctl restart sshd`.

5. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root (рис.1.4). Доступа нет.

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

Рис.1.4. Отказ в доступе к серверу посредством SSH-соединения через пользователя root

## 2. Ограничение списка пользователей для удалённого доступа по SSH

1. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя mrshcherbak (рис.2.1). Доступ есть.

```
[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Dec  7 13:02:51 2023
[mrshcherbak@server.mrshcherbak.net ~]$ logout
Connection to server.mrshcherbak.net closed.
```

Рис.2.1. Получение доступа к серверу посредством SSH-соединения через пользователя mrshcherbak

2. На сервере открыла файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавила строку AllowUsers vagrant (рис.2.2).

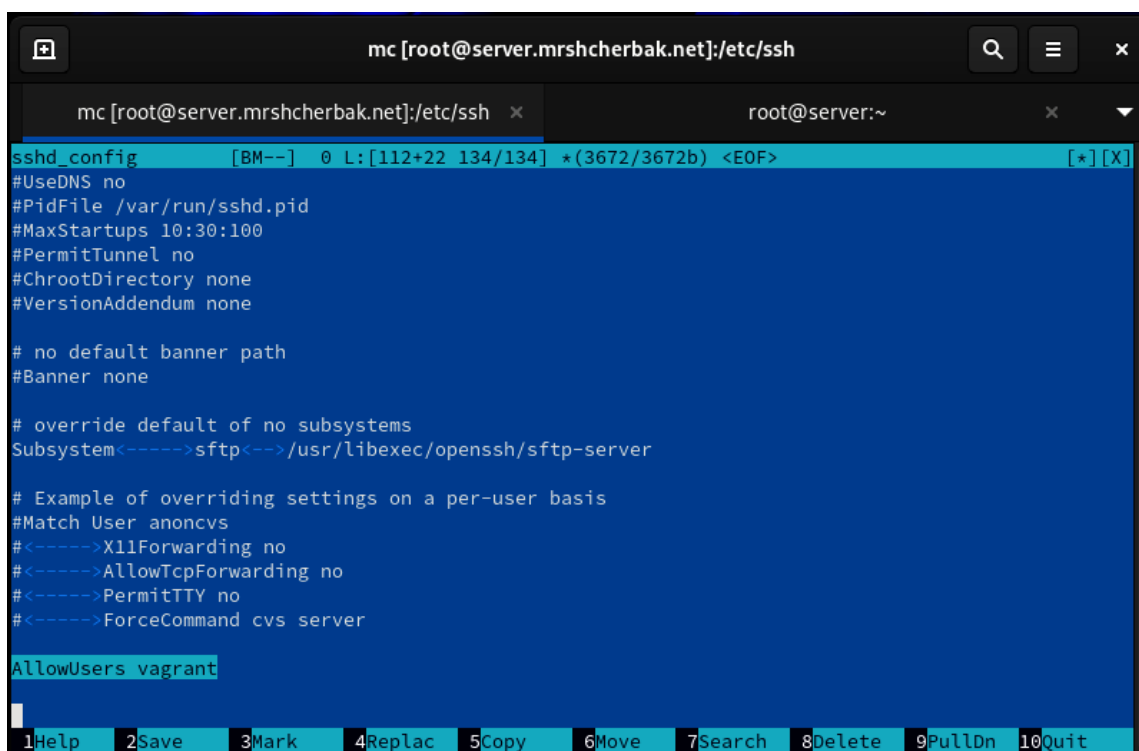


Рис.2.2. Редактирование файла /etc/ssh/sshd\_config

3. После сохранения изменений в файле конфигурации перезапустила sshd с

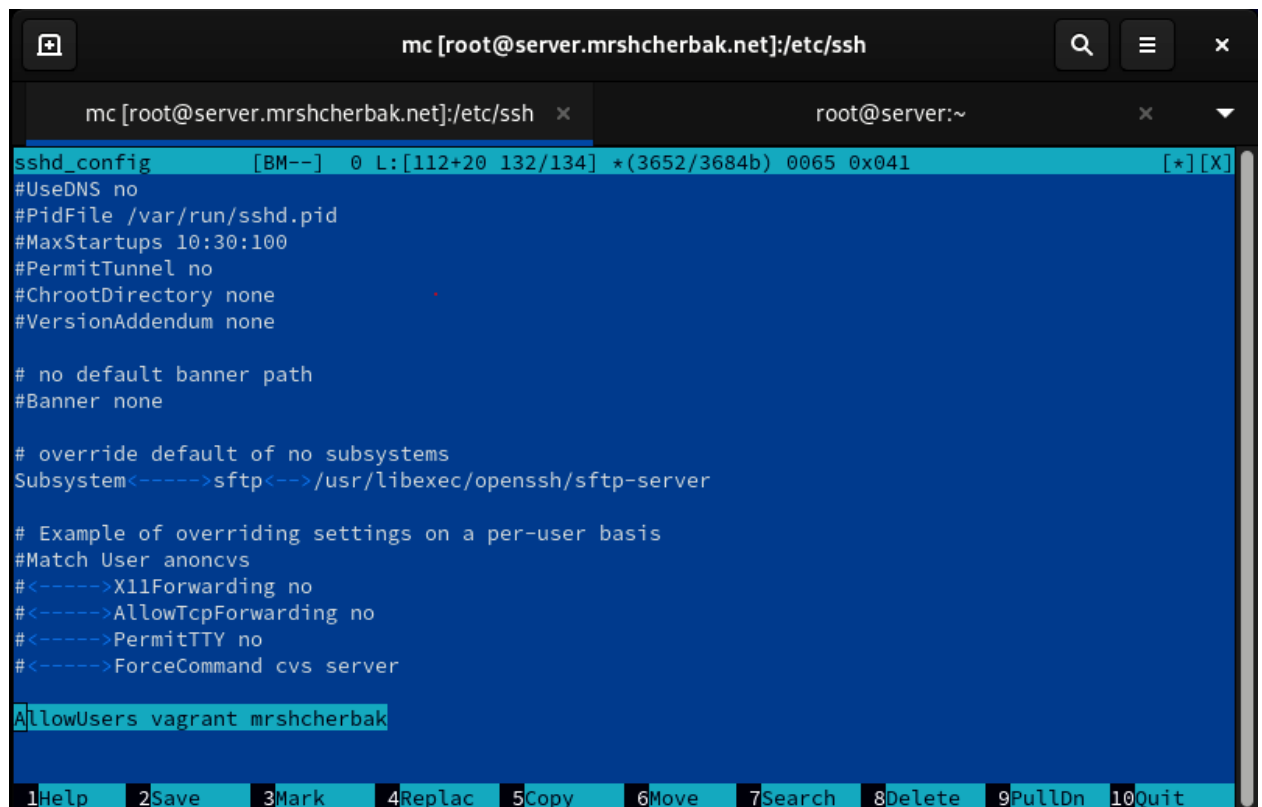
помощью команды `systemctl restart sshd`.

4. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `mrshcherbak` (рис.2.3). Доступа нет.

```
[mrshcherbak@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).
```

Рис.2.3. Отказ в доступе к серверу посредством SSH-соединения через пользователя `mrshcherbak`

5. В файле `/etc/ssh/sshd_config` конфигурации `sshd` внесла следующее изменение: `AllowUsers vagrant mrshcherbak` (рис.2.4).



```
mc [root@server.mrshcherbak.net]:/etc/ssh
ssh_d_config [BM--] 0 L:[112+20 132/134] *(3652/3684b) 0065 0x041 [*][X]
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# 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

AllowUsers vagrant mrshcherbak

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис.2.4. Редактирование файла `/etc/ssh/sshd_config`

6. После сохранения изменений в файле конфигурации перезапустила `sshd` и вновь попыталась получить доступ с клиента к серверу посредством SSH-соединения через пользователя `mrshcherbak` (рис.2.5). Доступ есть.

```

[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last failed login: Thu Dec 7 14:06:03 UTC 2023 from 192.168.1.31 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Thu Dec 7 14:03:59 2023 from 192.168.1.31
[mrshcherbak@server.mrshcherbak.net ~]$

```

Рис.2.5. Получение доступа к серверу посредством SSH-соединения через пользователя mrshcherbak

### 3. Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config добавила запись (рис.3.1), которая сообщает процессу sshd о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.

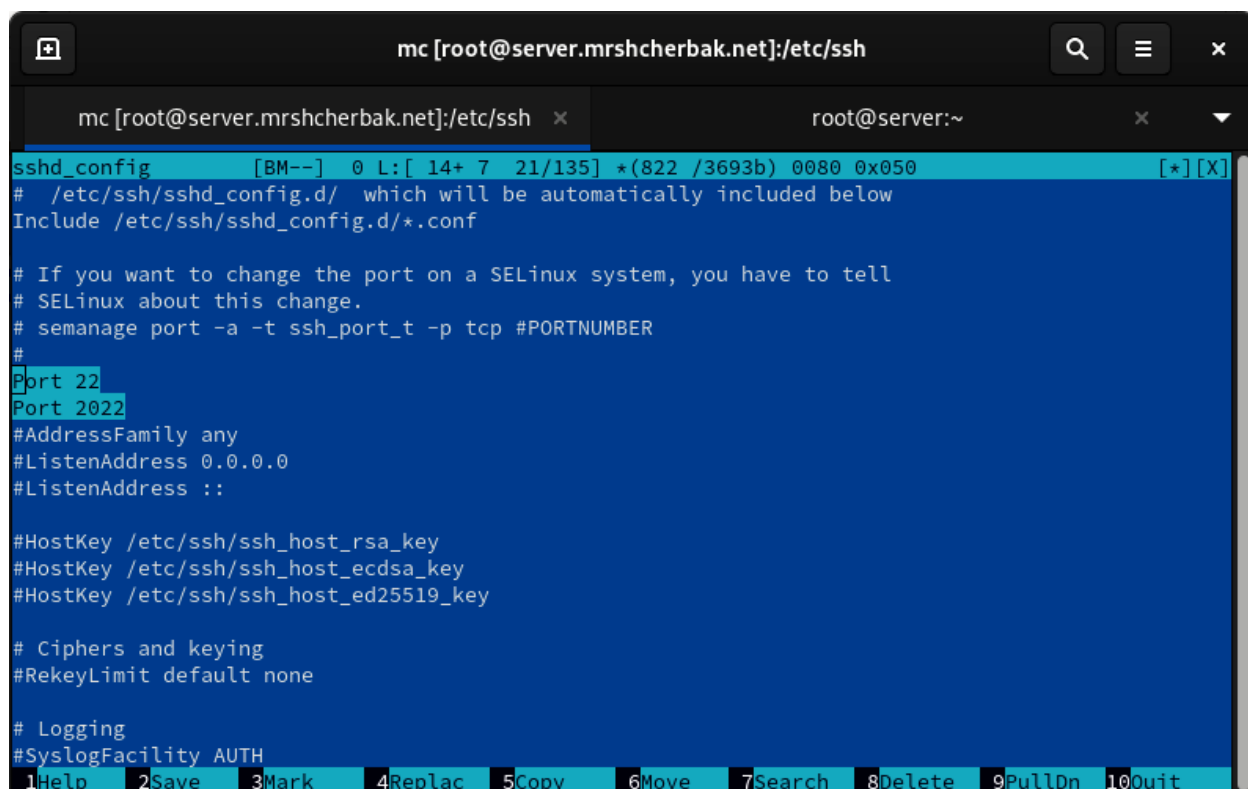
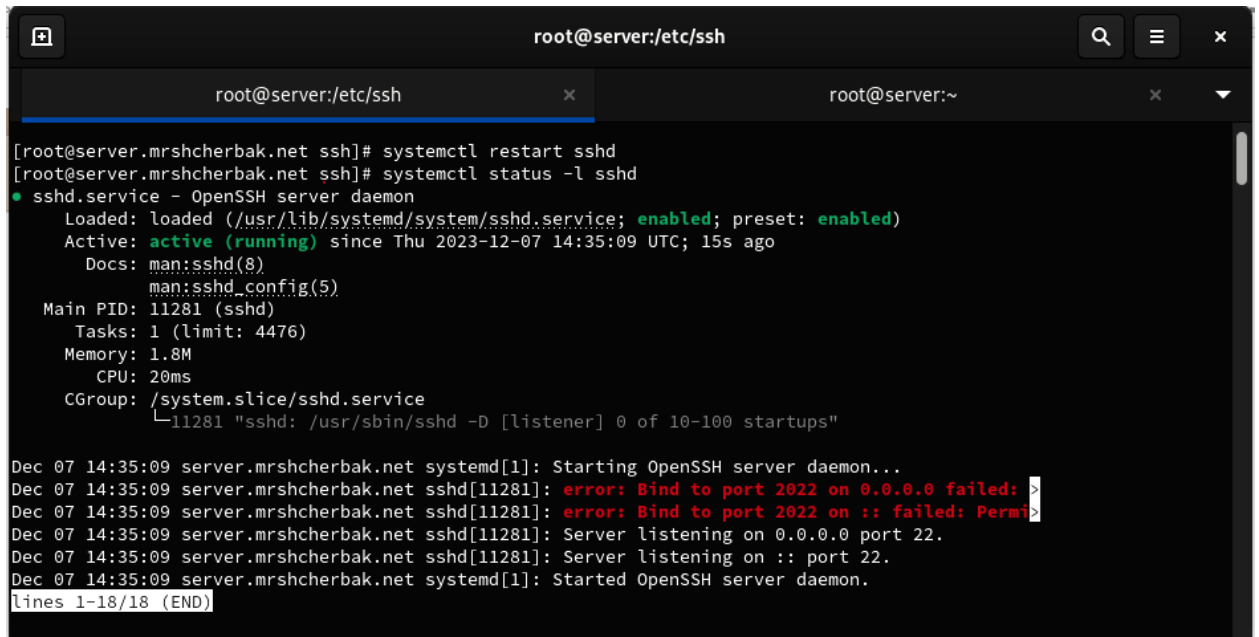


Рис.3.1. Редактирование файла /etc/ssh/sshd\_config

2. После сохранения изменений в файле конфигурации перезапустила sshd и посмотрела расширенный статус работы sshd (рис.3.2). Система сообщает об отказе в работе sshd через порт 2022. Дополнительно посмотрела сообщения в терминале с мониторингом системных событий (рис.3.3). SELinux запрещает подключение к порту 2022. Чтобы подключиться, необходимо изменить тип порта

с помощью предложенной команды в сообщениях мониторинга.

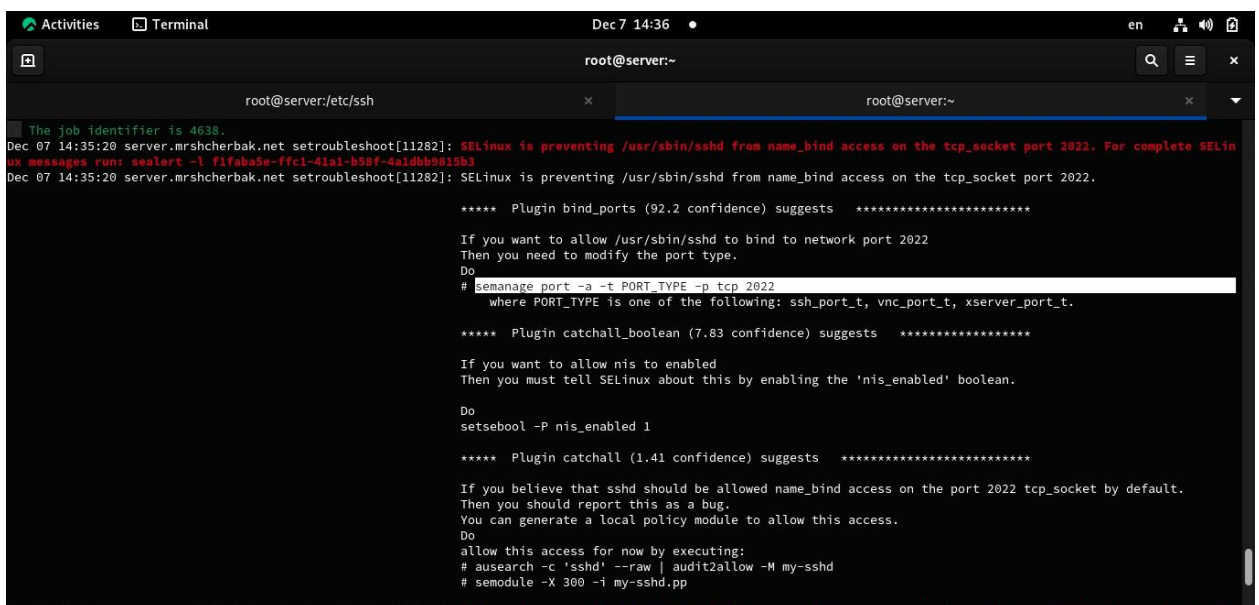


```
root@server:/etc/ssh

[root@server.mrshcherbak.net ssh]# systemctl restart sshd
[root@server.mrshcherbak.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-12-07 14:35:09 UTC; 15s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 11281 (sshd)
     Tasks: 1 (limit: 4476)
    Memory: 1.8M
       CPU: 20ms
    CGroup: /system.slice/sshd.service
            └─11281 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 07 14:35:09 server.mrshcherbak.net systemd[1]: Starting OpenSSH server daemon...
Dec 07 14:35:09 server.mrshcherbak.net sshd[11281]: error: Bind to port 2022 on 0.0.0.0 failed: >
Dec 07 14:35:09 server.mrshcherbak.net sshd[11281]: error: Bind to port 2022 on :: failed: Perm>
Dec 07 14:35:09 server.mrshcherbak.net sshd[11281]: Server listening on 0.0.0.0 port 22.
Dec 07 14:35:09 server.mrshcherbak.net sshd[11281]: Server listening on :: port 22.
Dec 07 14:35:09 server.mrshcherbak.net systemd[1]: Started OpenSSH server daemon.
lines 1-18/18 (END)
```

Рис.3.2. Просмотр расширенного статуса работы sshd



```
Activities Terminal Dec 7 14:36
root@server:/etc/ssh

The job identifier is 4638.
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELin
ux messages run: ausearch -l #fbaf8e-ffe1-53a3-b50f-4a3d0b0515b3
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.

***** Plugin bind_ports (92.2 confidence) suggests *****

If you want to allow /usr/sbin/sshd to bind to network port 2022
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 2022
   where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.

***** Plugin catchall_boolean (7.83 confidence) suggests *****

If you want to allow nis to be enabled
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.
Do
setsebool -P nis_enabled 1

***** Plugin catchall (1.41 confidence) suggests *****

If you believe that sshd should be allowed name_bind access on the port 2022 tcp_socket by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c 'sshd' --raw | audit2allow -M my-sshd
# semodule -X 300 -i my-sshd.pp
```

Рис.3.3. Мониторинг системных событий

3. Исправила на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана открыла порт 2022 протокола TCP, после чего вновь перезапустила sshd и посмотрела расширенный статус его работы. Действия представлены на рис.3.4. Статус показывает, что процесс sshd теперь прослушивает два порта.



```
[root@server.mrshcherbak.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.mrshcherbak.net ~]# systemctl restart sshd
[root@server.mrshcherbak.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-12-07 14:37:51 UTC; 7s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 11317 (sshd)
    Tasks: 1 (limit: 4476)
   Memory: 1.7M
      CPU: 17ms
   CGroup: /system.slice/sshd.service
           └─11317 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Starting OpenSSH server daemon...
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 2022.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 2022.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 22.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 22.
Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Started OpenSSH server daemon.
[root@server.mrshcherbak.net ~]#
```

Рис.3.4. Выполнение команд

4. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя mrshcherbak. После открытия оболочки пользователя ввела `sudo -i` для получения доступа root. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя mrshcherbak, указав порт 2022. После открытия оболочки пользователя ввела `sudo -i` для получения доступа root. Действия представлены на рис.3.5.

```
[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Dec 7 14:46:51 2023 from 192.168.1.1
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]# ssh -p2022 mrshcherbak@server.mrshcherbak.net
The authenticity of host '[server.mrshcherbak.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:EoLX8lU4wXJbhFwfl+w4A0lKyMetD3BSoelm1jYlsek.
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.mrshcherbak.net]:2022' (ED25519) to the list of known hosts.
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

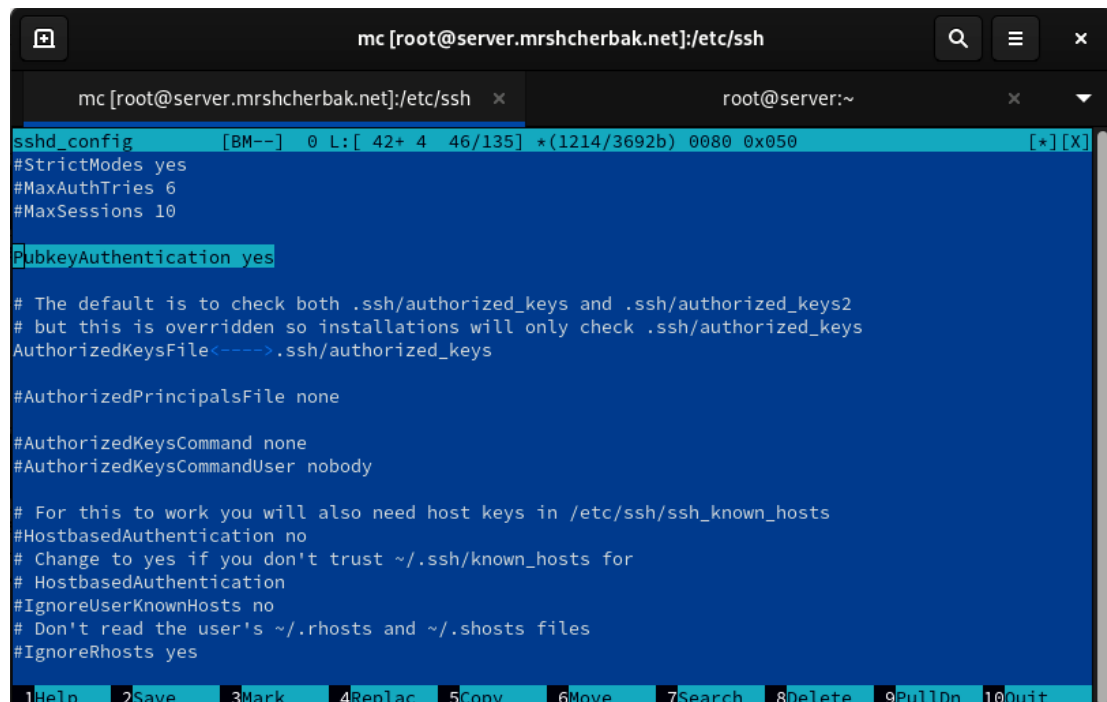
Last login: Thu Dec 7 14:47:56 2023 from 192.168.1.31
[mrshcherbak@server.mrshcherbak.net ~]$ sudo -i
[sudo] password for mrshcherbak:
Sorry, try again.
[sudo] password for mrshcherbak:
Sorry, try again.
[sudo] password for mrshcherbak:
[root@server.mrshcherbak.net ~]#
```

Рис.3.5. Выполнение команд



#### 4. Настройка удалённого доступа по SSH по ключу

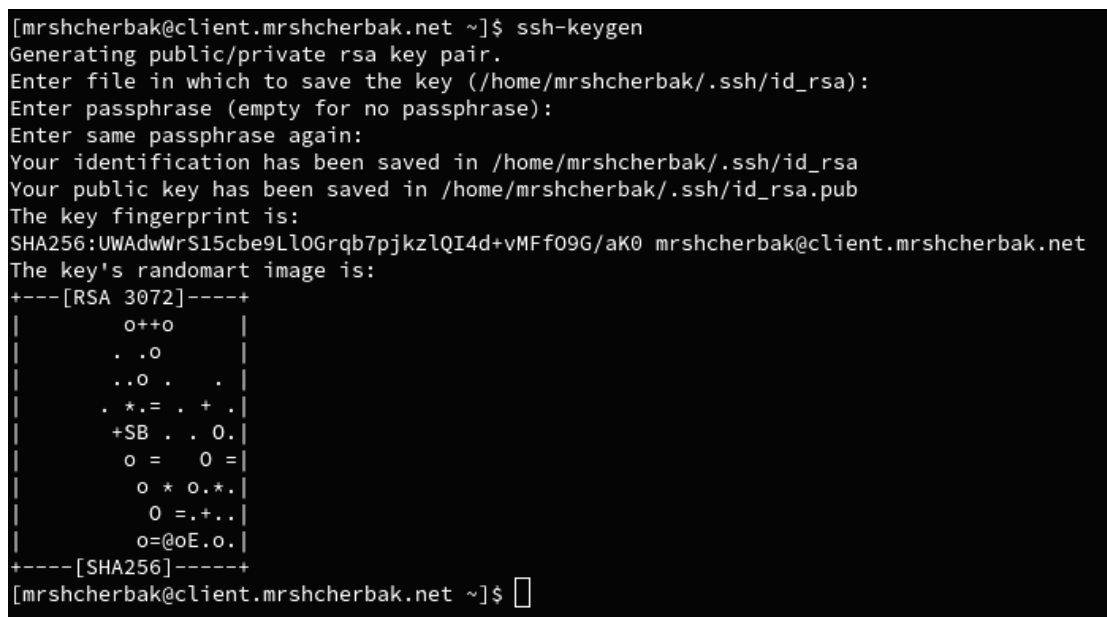
1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` задала параметр, разрешающий аутентификацию по ключу (рис.4.1).



```
mc [root@server.mrshcherbak.net]:/etc/ssh
ssh_config [BM--] 0 L: [ 42+ 4 46/135] *(1214/3692b) 0080 0x050 [*] [X]
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile<---->.ssh/authorized_keys
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис.4.1. Редактирование файла `/etc/ssh/sshd_config`

2. После сохранения изменений в файле конфигурации перезапустила `sshd`.
3. На клиенте сформировала SSH-ключ (рис.4.2).



```
[mrshcherbak@client.mrshcherbak.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mrshcherbak/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mrshcherbak/.ssh/id_rsa
Your public key has been saved in /home/mrshcherbak/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UWAdwWrS15cbe9Ll0Grqb7pjkz1QI4d+vmFf09G/aK0 mrshcherbak@client.mrshcherbak.net
The key's randomart image is:
+----[RSA 3072]-----+
|      o++o      |
|      . .o      |
|     ..o . .    |
|    . *. = . + . |
|   +SB . . 0.   |
|    o = 0 =     |
|    o * o.*     |
|    0 =.+..     |
|    o=@oE.o     |
+----[SHA256]-----+
[mrshcherbak@client.mrshcherbak.net ~]$
```

Рис.4.2. Выполнение команды `ssh-keygen`



```

[mrshcherbak@client.mrshcherbak.net ~]$ ssh -fNL 8080:localhost:80 mrshcherbak@server.mrshcherbak.net
[mrshcherbak@client.mrshcherbak.net ~]$ lsof | grep TCP
ssh       7218      mrshcherbak    3u    IPv4        45943      0t0      TCP client.mrshcherbak.net:39578->ns.mrshcherbak.net:ssh (ESTABLISHED)
ssh       7754      mrshcherbak    3u    IPv4        53076      0t0      TCP client.mrshcherbak.net:49330->ns.mrshcherbak.net:ssh (ESTABLISHED)
ssh       8237      mrshcherbak    3u    IPv4        58414      0t0      TCP client.mrshcherbak.net:43064->ns.mrshcherbak.net:ssh (ESTABLISHED)
firefox   8457      mrshcherbak   60u    IPv4        74952      0t0      TCP client.mrshcherbak.net:39280->lj-in-fl47.1e100.net:https (ESTABLISHED)

```

Рис.5.2. Выполнение команды

2. На клиенте запустила браузер и в адресной строке ввела localhost:8080. Отобразилась страница с приветствием (рис.5.3).

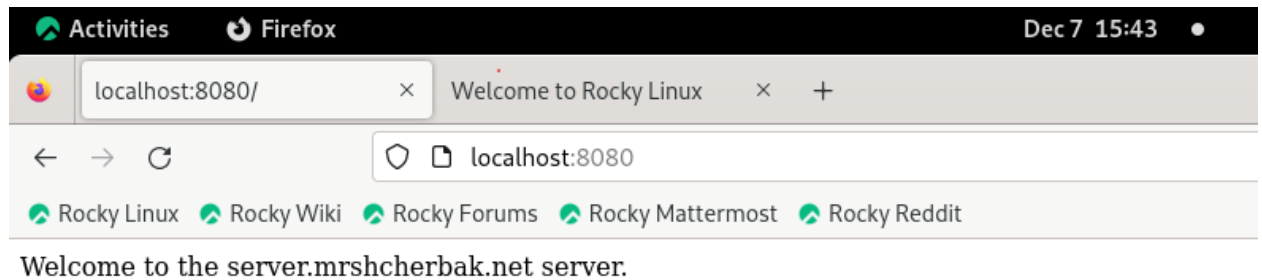


Рис.5.3. Отображение страницы по запросу localhost:8080

## 6. Запуск консольных приложений через SSH

1. На клиенте открыла терминал под пользователем mrshcherbak и посмотрела имя узла сервера, а также список файлов на сервере и почту (рис.6.1 – рис.6.2).

```

[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net hostname
server.mrshcherbak.net
[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net ls -Al
total 72
-rw-----, 1 mrshcherbak mrshcherbak 3282 Dec  7 15:55 .bash_history
-rw-r--r--, 1 mrshcherbak mrshcherbak  18 Jan 23  2023 .bash_logout
-rw-r--r--, 1 mrshcherbak mrshcherbak  141 Jan 23  2023 .bash_profile
-rw-r--r--, 1 mrshcherbak mrshcherbak  519 Nov  7 13:49 .bashrc
drwxr-xr-x, 16 mrshcherbak mrshcherbak 4096 Nov 23 22:42 .cache
drwx-----, 15 mrshcherbak mrshcherbak 4096 Nov 23 22:42 .config
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Desktop
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Documents
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Downloads
-rw-----, 1 mrshcherbak mrshcherbak  20 Nov 28 21:46 .lessshst
drwx-----, 4 mrshcherbak mrshcherbak   32 Nov  7 13:51 .local
drwx-----, 5 mrshcherbak mrshcherbak 4096 Dec  3 13:57 Maildir
drwxr-xr-x, 5 mrshcherbak mrshcherbak   54 Nov  9 14:23 .mozilla
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Music
drwxr-xr-x, 3 mrshcherbak mrshcherbak  65 Dec  7 15:43 Pictures
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Public
drwx-----, 2 mrshcherbak mrshcherbak  103 Dec  7 15:54 .ssh
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Templates
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-clipboard-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-clipboard-tty1-service.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Nov  9 17:04 .vboxclient-display-svga-x11-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-draganddrop-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-draganddrop-tty1-service.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   6 Dec  7 13:03 .vboxclient-hostversion-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-seamless-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-seamless-tty1-service.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-vmvga-session-tty1-control.pid
-rw-r-----, 1 mrshcherbak mrshcherbak   5 Dec  7 13:02 .vboxclient-vmvga-session-tty1-service.pid
drwxr-xr-x, 2 mrshcherbak mrshcherbak   6 Nov  7 13:51 Videos
-rw-----, 1 mrshcherbak mrshcherbak   0 Dec  7 13:02 .xsession-errors
-rw-----, 1 mrshcherbak mrshcherbak   0 Dec  3 09:39 .xsession-errors.old
[mrshcherbak@client.mrshcherbak.net ~]$

```

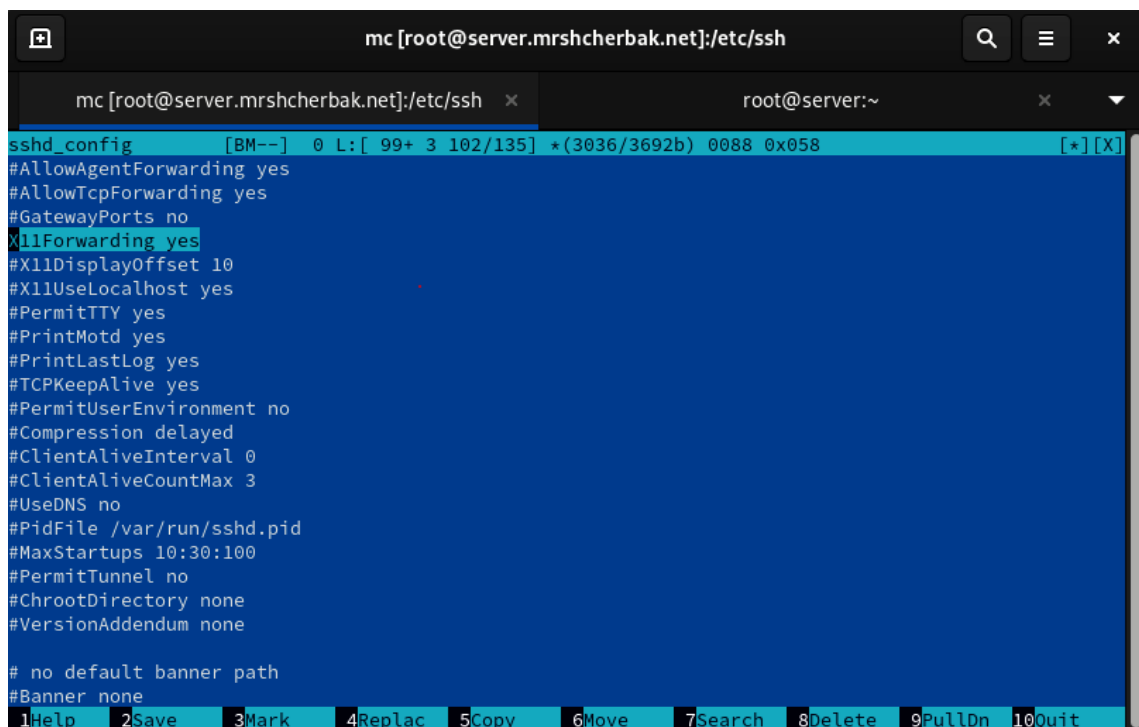
Рис.6.1. Просмотр имени узла сервера и списка файлов на сервере

```
[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/mrshcherbak/Maildir: 6 messages 2 unread
 1 mrshcherbak      2023-12-03 10:52   18/684   "Test1           "
 2 mrshcherbak      2023-12-03 10:57   18/684   "Test3           "
+U 3 mrshcherbak@client.m 2023-12-03 12:53   21/880   "LMTP test       "
 U 4 mrshcherbak@client.m 2023-12-03 13:06   21/880   "LMTP test       "
 5 mrshcherbak      2023-12-03 13:55   22/864   "test_smtp       "
 6 mrshcherbak      2023-12-03 13:57   22/865   "test1_smtp      "
q
Held 6 messages in /home/mrshcherbak/Maildir
[mrshcherbak@client.mrshcherbak.net ~]$
```

Рис.6.2. Просмотр почты на сервере с клиента

## 7. Запуск графических приложений через SSH (X11Forwarding)

1. На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешила отображать на локальном клиентском компьютере графические интерфейсы X11 (рис.7.1).



```
mc [root@server.mrshcherbak.net]:/etc/ssh
sshd_config [BM--] 0 L:[ 99+ 3 102/135] *(3036/3692b) 0088 0x058 [*][X]
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис.7.1. Редактирование файла `/etc/ssh/sshd_config`

2. После сохранения изменения в конфигурационном файле перезапустила `sshd`.

3. Попробовала с клиента удалённо подключиться к серверу и запустить графическое приложение `firefox` (рис.7.2).

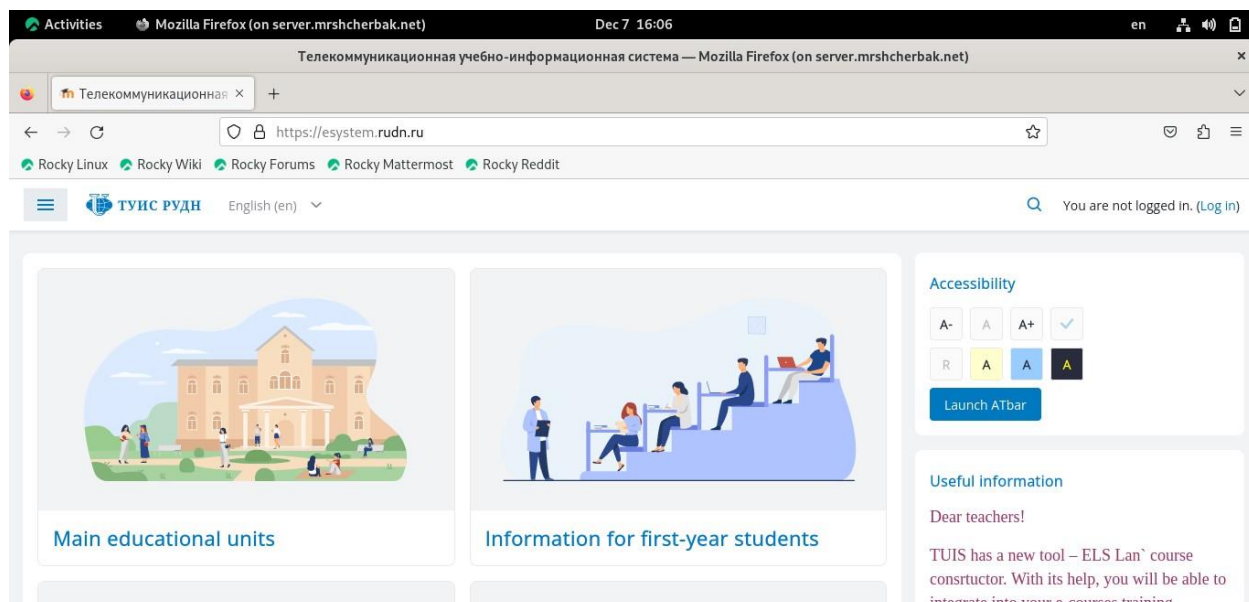


Рис.7.2. Страница сайта ТУИС на сервере в запущенном firefox

## 8. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создала в нём каталог `ssh`, в который поместила в соответствующие подкаталоги конфигурационный файл `sshd_config`, а в каталоге `/vagrant/provision/server` создала исполняемый файл `ssh.sh` и прописала в нём скрипт (рис.8.2). Действия представлены на рис.8.1.

```
[root@server.mrshcherbak.net ssh]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.mrshcherbak.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.mrshcherbak.net server]# cd /vagrant/provision/server
[root@server.mrshcherbak.net server]# touch ssh.sh
[root@server.mrshcherbak.net server]# chmod +x ssh.sh
[root@server.mrshcherbak.net server]# mc
```

Рис.8.1. Выполнение команд

```
mc [root@server.mrshcherbak.net]:/vagrant/provision/server
/vagrant/provision/server/ssh.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc

restorecon -vR /etc

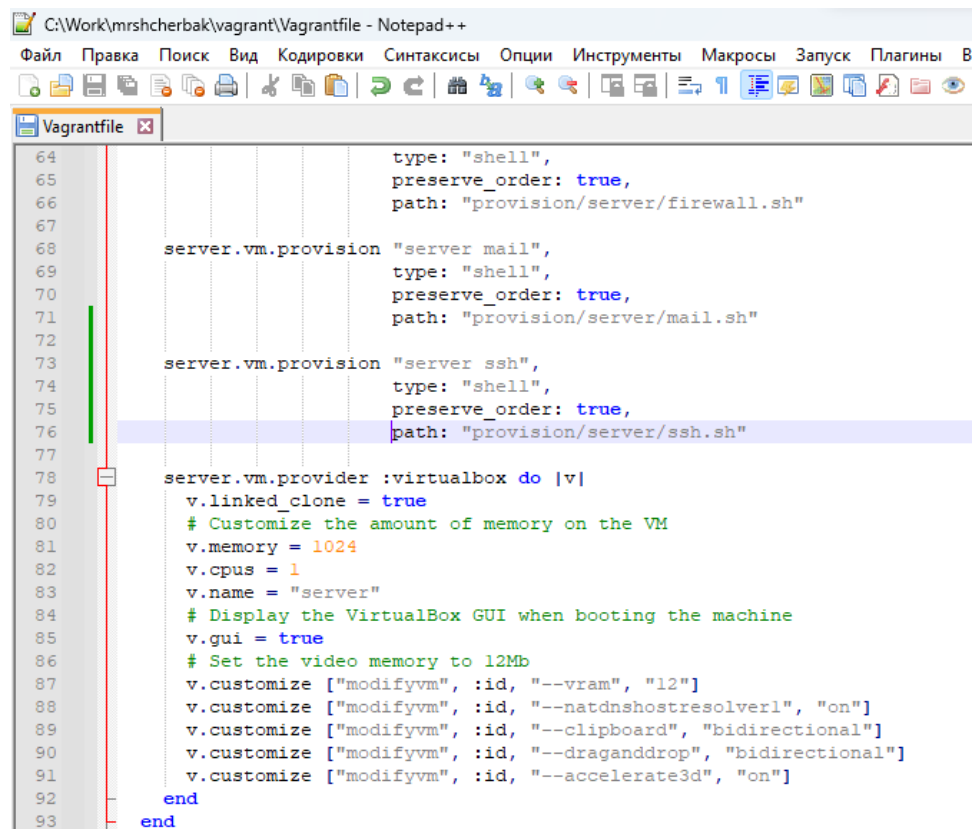
echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent

echo "Tuning SELinux"
semanage port -a -t ssh_port_t -p tcp 2022

echo "Restart sshd service"
systemctl restart sshd
```

Рис.8.2. Содержимое файла ssh.sh

2. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавила в разделе конфигурации для сервера запись (рис.8.3).



```
C:\Work\mrshcherbak\vagrant\Vagrantfile - Notepad++
Файл  Правка  Поиск  Вид  Кодировки  Синтаксисы  Опции  Инструменты  Макросы  Запуск  Плагины  В
Vagrantfile
64                                     type: "shell",
65                                     preserve_order: true,
66                                     path: "provision/server/firewall.sh"
67
68     server.vm.provision "server mail",
69                         type: "shell",
70                         preserve_order: true,
71                         path: "provision/server/mail.sh"
72
73     server.vm.provision "server ssh",
74                         type: "shell",
75                         preserve_order: true,
76                         path: "provision/server/ssh.sh"
77
78     server.vm.provider :virtualbox do |v|
79       v.linked_clone = true
80       # Customize the amount of memory on the VM
81       v.memory = 1024
82       v.cpus = 1
83       v.name = "server"
84       # Display the VirtualBox GUI when booting the machine
85       v.gui = true
86       # Set the video memory to 12Mb
87       v.customize ["modifyvm", :id, "--vram", "12"]
88       v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
89       v.customize ["modifyvm", :id, "--clipboard", "bidirectional"]
90       v.customize ["modifyvm", :id, "--draganddrop", "bidirectional"]
91       v.customize ["modifyvm", :id, "--accelerate3d", "on"]
92     end
93 end
```

Рис.8.3. Редактирование файла Vagrantfile

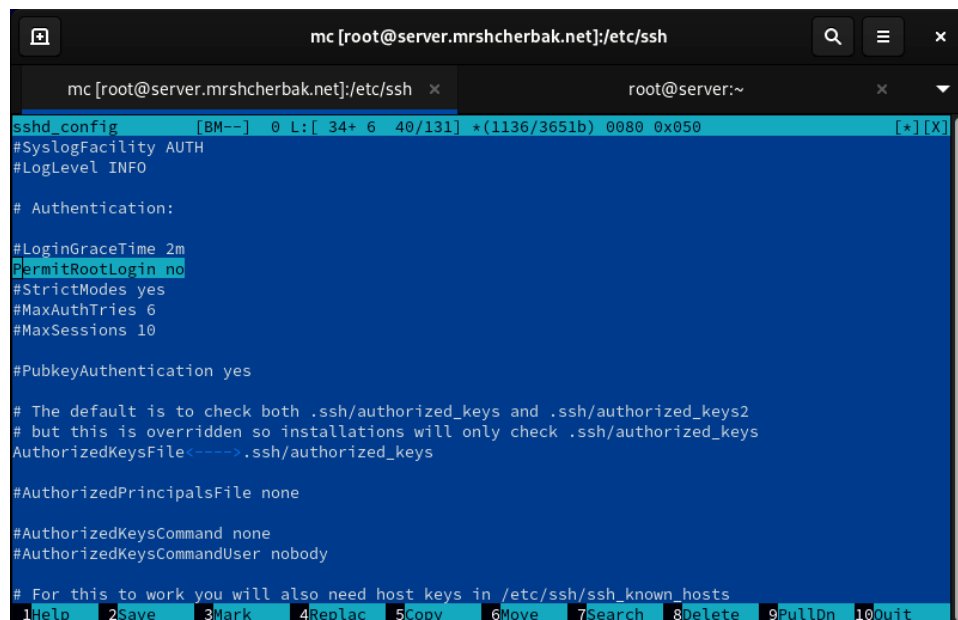
**Вывод:** таким образом, в ходе выполнения л/р №11, я приобрела практические навыки по настройке удалённого доступа к серверу с помощью SSH.

## Контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

Чтобы запретить удалённый доступ по SSH пользователю root и разрешить доступ пользователю alice, нужно:

- отредактировать файл конфигурации SSH (/etc/ssh/sshd\_config) — найти строку PermitRootLogin и установить ее значение в no, после сохранения изменений в файле конфигурации перезапустить sshd: systemctl restart sshd.



```
mc [root@server.mrshcherbak.net]:/etc/ssh
mc [root@server.mrshcherbak.net]:/etc/ssh x root@server:~ x
sshd_config [BM--] 0 L: [ 34+ 6 40/131] *(1136/3651b) 0080 0x050 [*][X]
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile----- .ssh/authorized_keys

#AuthorizedPrincipalsFile none

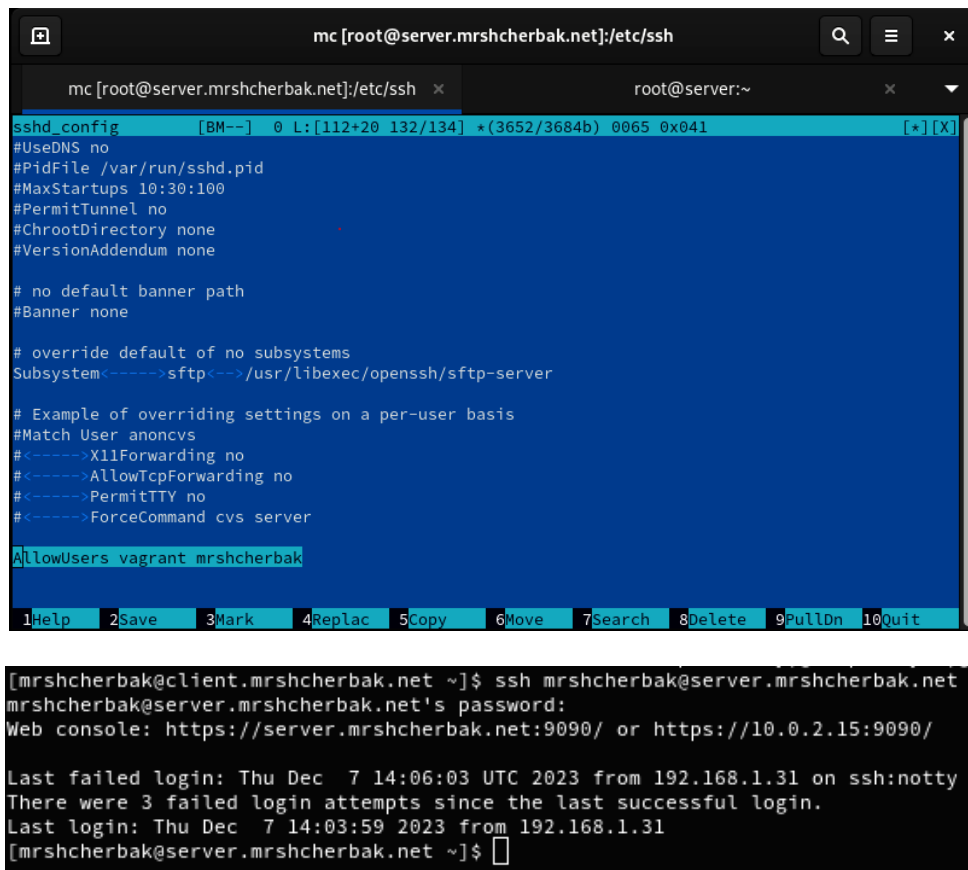
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

- открыть файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и прописать строку AllowUsers vagrant alice, после сохранения изменений в файле конфигурации перезапустить sshd: systemctl restart sshd. Так, будет получен доступ к серверу посредством SSH-соединения через пользователя alice.

В данной л/р в разделах 1 и 2 я запрещала удалённый доступ по SSH на сервер пользователю root и разрешала доступ пользователю mrshcherbak.





The image shows two terminal windows. The top window is titled 'mc [root@server.mrshcherbak.net]:/etc/ssh' and displays the contents of the `/etc/ssh/sshd_config` file. The file contains various configuration options for the SSH daemon, including `#UseDNS no`, `#PidFile /var/run/sshd.pid`, `#MaxStartups 10:30:100`, `#PermitTunnel no`, `#ChrootDirectory none`, `#VersionAddendum none`, `#Banner none`, `Subsystem sftp /usr/libexec/openssh/sftp-server`, and an example of overriding settings for the `anoncvs` user. The line `AllowUsers vagrant mrshcherbak` is highlighted in blue. The bottom window shows an SSH login attempt from a client to the server. It displays the password prompt, the web console URL (`https://server.mrshcherbak.net:9090/`), and login history information, including the last failed login attempt and the last successful login.

```
mc [root@server.mrshcherbak.net]:/etc/ssh
ssh_config [BM--] 0 L:[112+20 132/134] *(3652/3684b) 0065 0x041 [*][X]
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# 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

AllowUsers vagrant mrshcherbak

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit

[mrshcherbak@client.mrshcherbak.net ~]$ ssh mrshcherbak@server.mrshcherbak.net
mrshcherbak@server.mrshcherbak.net's password:
Web console: https://server.mrshcherbak.net:9090/ or https://10.0.2.15:9090/

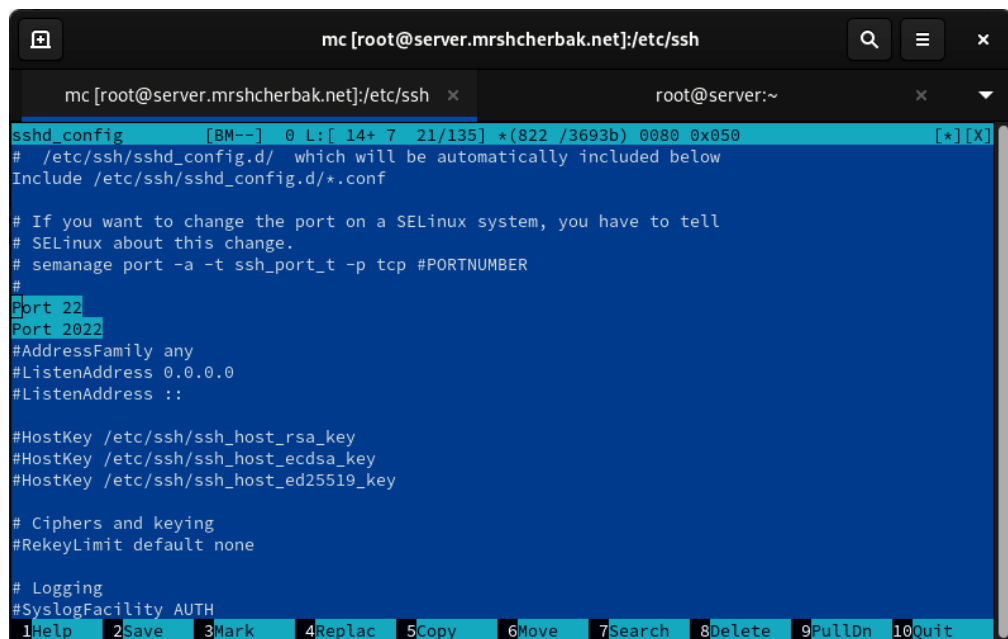
Last failed login: Thu Dec 7 14:06:03 UTC 2023 from 192.168.1.31 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Thu Dec 7 14:03:59 2023 from 192.168.1.31
[mrshcherbak@server.mrshcherbak.net ~]$
```

2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

Для настройки удалённого доступа по SSH через несколько портов, необходимо отредактировать файл конфигурации SSH и добавить параметр `Port`, указав нужные порты, после чего, чтобы подключиться, необходимо изменить тип порта с помощью команды `semanage` в сообщениях мониторинга (более подробные действия описаны чуть ниже). Это может быть полезно для повышения безопасности, так как стандартный порт 22 может быть целью атак. Злоумышленник может использовать тот факт, что удалённый доступ по SSH обычно организуется через порт 22, а каждый узел Unix/Linux имеет учётную запись `root`. Основываясь на этой информации, злоумышленник может попытаться войти в систему как `root`, просто подбирая пароль. Возможные меры по усилению безопасности при организации удалённого доступа как раз включают в себя переадресацию стандартного для SSH порта 22 на нестандартный.

В данной л/р я на сервере в файле конфигурации `sshd /etc/ssh/sshd_config` добавляла запись, которая сообщает процессу `sshd` о необходимости организации

соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.



```
mc [root@server.mrshcherbak.net]:/etc/ssh
mc [root@server.mrshcherbak.net]:/etc/ssh x root@server:~
sshd_config [BM--] 0 L: [ 14+ 7 21/135] *(822 /3693b) 0080 0x050 [*] [X]
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

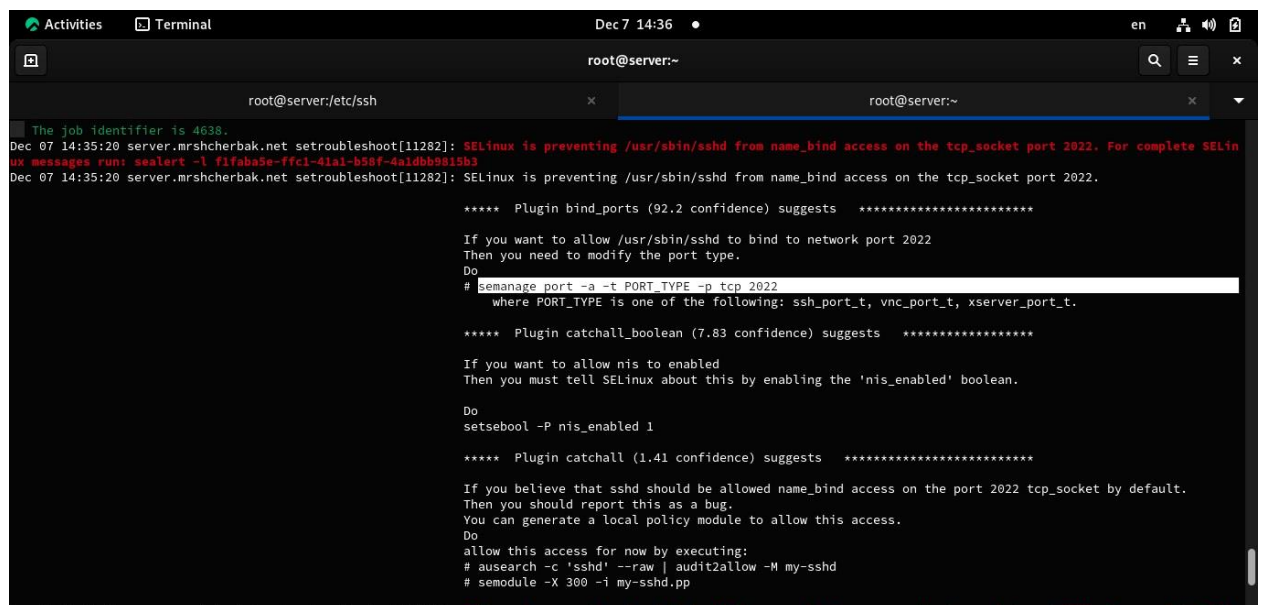
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

После сохранения изменений в файле конфигурации перезапускала sshd и, чтобы подключиться, изменяла тип порта с помощью предложенной команды в сообщениях мониторинга.



```
Activities Terminal Dec 7 14:36 en
root@server:~
root@server:/etc/ssh
The job identifier is 4638.
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux messages run: sealert -t f1fabase-ffci-41a1-b58f-4a1dbb9a15b3
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.

**** Plugin bind_ports (92.2 confidence) suggests ****
If you want to allow /usr/sbin/sshd to bind to network port 2022
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 2022
where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.

**** Plugin catchall_boolean (7.83 confidence) suggests ****
If you want to allow nis to enabled
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.
Do
setsebool -P nis_enabled 1

**** Plugin catchall (1.41 confidence) suggests ****
If you believe that sshd should be allowed name_bind access on the port 2022 tcp_socket by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c 'sshd' --raw | audit2allow -M my-sshd
# semodule -X 300 -i my-sshd.pp
```

Исправляла на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана открывала порт 2022 протокола TCP, после чего перезапускала sshd. Статус показывал, что процесс sshd теперь прослушивает два порта.

```
[root@server.mrshcherbak.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.mrshcherbak.net ~]# systemctl restart sshd
[root@server.mrshcherbak.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-12-07 14:37:51 UTC; 7s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 11317 (sshd)
    Tasks: 1 (limit: 4476)
   Memory: 1.7M
      CPU: 17ms
   CGroup: /system.slice/ssh.service
           └─11317 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Starting OpenSSH server daemon...
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 2022.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 2022.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 22.
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 22.
Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Started OpenSSH server daemon.
[root@server.mrshcherbak.net ~]#
```

3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

Чтобы создать туннель SSH в фоновом режиме без выполнения конкретной команды, можно использовать опции -fN. Пример:

ssh -fN -L локальный\_порт:удаленный\_хост:удаленный\_порт →  
пользователь@удаленный\_хост

Где:

-f указывает на фоновый режим.

-N говорит SSH не выполнять удаленную команду.

-L определяет локальный порт проброса.

локальный\_порт - порт на вашей локальной машине.

удаленный\_хост - удаленный хост, к которому вы подключаетесь.

удаленный\_порт - порт на удаленном хосте.

Это создаст SSH-туннель, сброшенный через указанный удаленный хост и порт, и установит его в фоновом режиме.

В л/р я перенаправляла порт 80 на server.mrshcherbak.net на порт 8080 на локальной машине.

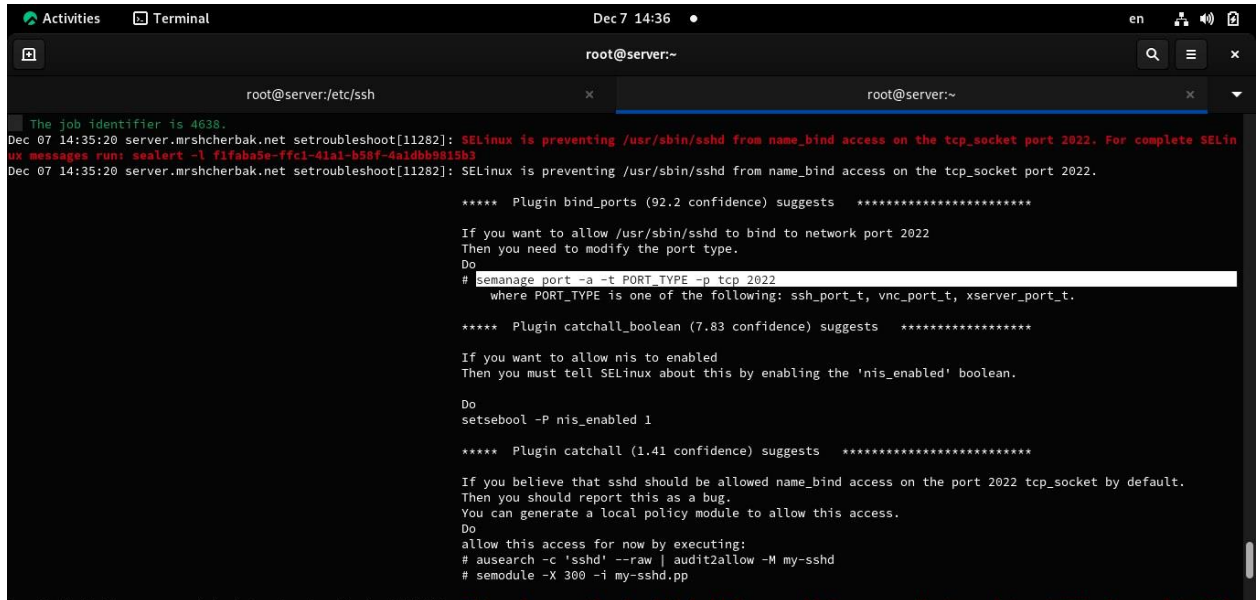
```
[mrshcherbak@server.mrshcherbak.net ~]$ ssh -fNL 8080:localhost:80 mrshcherbak@server.mrshcherbak.net
```

4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

ssh -L 5555:server2.example.com:80 user@your\_server.

## 5. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

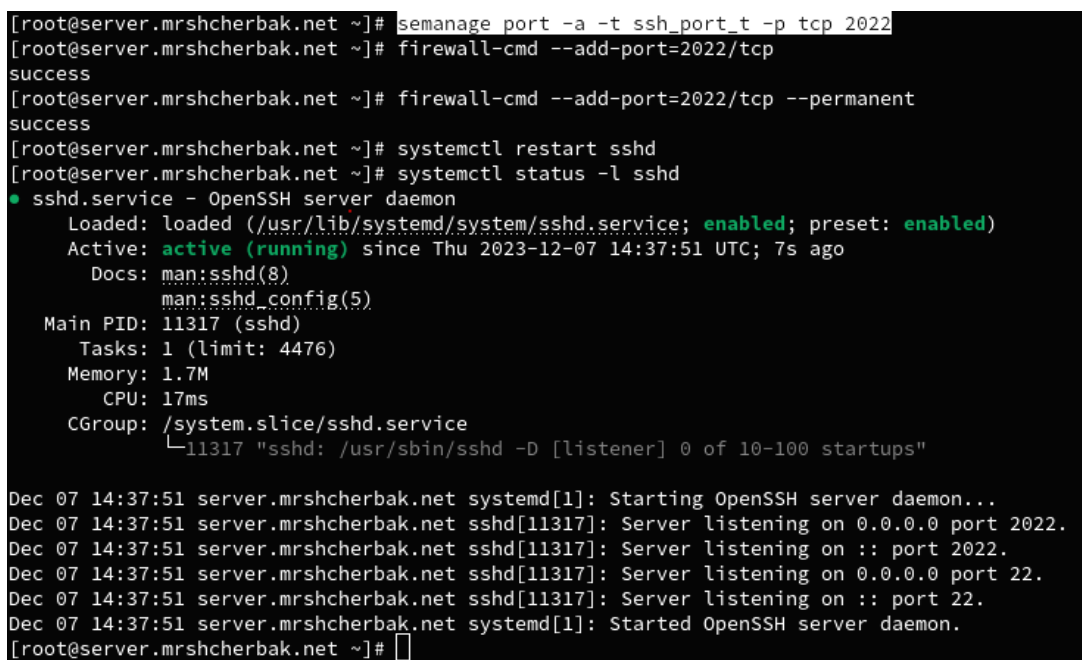
Чтобы SELinux позволял SSH связываться с портом 2022, необходимо выполнить команду: `semanage port -a -t ssh_port_t -p tcp 2022`.



```
root@server:~  
root@server:/etc/ssh  
The job identifier is 4638.  
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022. For complete SELinux messages run: sealert -l f1faba5e-ffc1-41a1-b58f-4a1dbb9d15b3  
Dec 07 14:35:20 server.mrshcherbak.net setroubleshoot[11282]: SELinux is preventing /usr/sbin/sshd from name_bind access on the tcp_socket port 2022.  
  
***** Plugin bind_ports (92.2 confidence) suggests *****  
  
If you want to allow /usr/sbin/sshd to bind to network port 2022  
Then you need to modify the port type.  
Do  
# semanage port -a -t PORT_TYPE -p tcp 2022  
where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.  
  
***** Plugin catchall_boolean (7.83 confidence) suggests *****  
  
If you want to allow nis to enabled  
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.  
Do  
setsebool -P nis_enabled 1  
  
***** Plugin catchall (1.41 confidence) suggests *****  
  
If you believe that sshd should be allowed name_bind access on the port 2022 tcp_socket by default.  
Then you should report this as a bug.  
You can generate a local policy module to allow this access.  
Do  
allow this access for now by executing:  
# ausearch -c 'sshd' --raw | audit2allow -M my-sshd  
# semodule -X 300 -i my-sshd.pp
```

## 6. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

Открыла порт 2022 на уровне межсетевого экрана. Важно добавить `--permanent`, чтобы изменения сохранялись после перезагрузки системы. Далее перезапуск `sshd` и просмотр его статуса, чтобы проверить, правильно ли применены изменения.



```
[root@server.mrshcherbak.net ~]# semanage port -a -t ssh_port_t -p tcp 2022  
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp  
success  
[root@server.mrshcherbak.net ~]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@server.mrshcherbak.net ~]# systemctl restart sshd  
[root@server.mrshcherbak.net ~]# systemctl status -l sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)  
   Active: active (running) since Thu 2023-12-07 14:37:51 UTC; 7s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Main PID: 11317 (sshd)  
    Tasks: 1 (limit: 4476)  
  Memory: 1.7M  
     CPU: 17ms  
   CGroup: /system.slice/sshd.service  
           └─11317 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Starting OpenSSH server daemon...  
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 2022.  
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 2022.  
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on 0.0.0.0 port 22.  
Dec 07 14:37:51 server.mrshcherbak.net sshd[11317]: Server listening on :: port 22.  
Dec 07 14:37:51 server.mrshcherbak.net systemd[1]: Started OpenSSH server daemon.  
[root@server.mrshcherbak.net ~]#
```