

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №11**

дисциплина: Администрирование сетевых подсистем

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

## Цель работы:

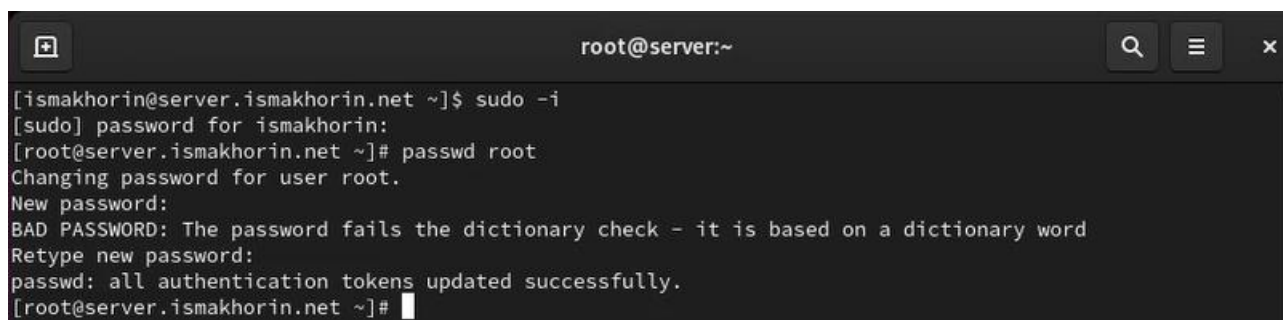
Целью данной работы является приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

## Выполнение работы:

На сервере зададим пароль для пользователя root (Рис. 1.1):

```
sudo -i
```

```
passwd root
```

A screenshot of a terminal window with a dark background. The title bar at the top shows 'root@server:~' and standard window controls. The terminal text shows a user 'ismakhorin' at 'server.ismakhorin.net' running 'sudo -i'. This prompts for a password for 'ismakhorin'. Then, the prompt changes to root, and 'passwd root' is run. It prompts for a new password, which fails a dictionary check. The user retypes the password, and the message 'passwd: all authentication tokens updated successfully.' is shown. The prompt returns to root.

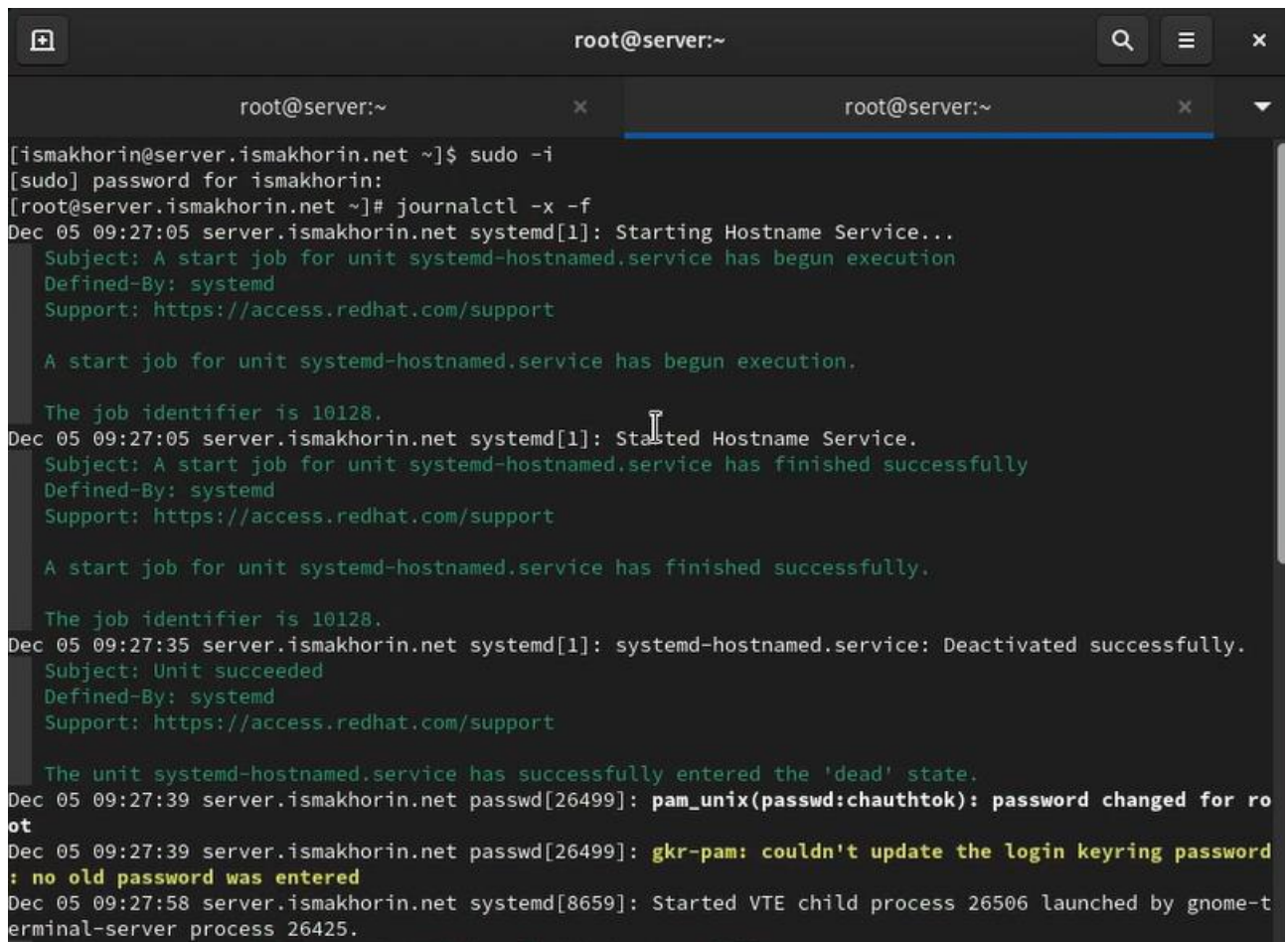
```
root@server:~  
[ismakhorin@server.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@server.ismakhorin.net ~]# passwd root  
Changing password for user root.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@server.ismakhorin.net ~]#
```

**Рис. 1.1.** Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

На сервере в дополнительном терминале запустим мониторинг системных событий (Рис. 1.2):

```
sudo -i
```

```
journalctl -x -f
```



```
root@server:~  
[ismakhorin@server.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@server.ismakhorin.net ~]# journalctl -x -f  
Dec 05 09:27:05 server.ismakhorin.net systemd[1]: Starting Hostname Service...  
Subject: A start job for unit systemd-hostnamed.service has begun execution  
Defined-By: systemd  
Support: https://access.redhat.com/support  
  
A start job for unit systemd-hostnamed.service has begun execution.  
  
The job identifier is 10128.  
Dec 05 09:27:05 server.ismakhorin.net systemd[1]: Started Hostname Service.  
Subject: A start job for unit systemd-hostnamed.service has finished successfully  
Defined-By: systemd  
Support: https://access.redhat.com/support  
  
A start job for unit systemd-hostnamed.service has finished successfully.  
  
The job identifier is 10128.  
Dec 05 09:27:35 server.ismakhorin.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.  
Subject: Unit succeeded  
Defined-By: systemd  
Support: https://access.redhat.com/support  
  
The unit systemd-hostnamed.service has successfully entered the 'dead' state.  
Dec 05 09:27:39 server.ismakhorin.net passwd[26499]: pam_unix(passwd:chauthtok): password changed for root  
Dec 05 09:27:39 server.ismakhorin.net passwd[26499]: gkr-pam: couldn't update the login keyring password: no old password was entered  
Dec 05 09:27:58 server.ismakhorin.net systemd[8659]: Started VTE child process 26506 launched by gnome-terminal-server process 26425.
```

**Рис. 1.2.** Запуск в дополнительном терминале мониторинга системных событий.

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя root (Рис. 1.3):

```
ssh root@server.ismakhorin.net
```



```
ismakhorin@client:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh root@server.ismakhorin.net  
The authenticity of host 'server.ismakhorin.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:70FCr4c220P70IVFdberIr95+akgAZLc9DIM4RzIZ0w.  
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.ismakhorin.net' (ED25519) to the list of known hosts.  
root@server.ismakhorin.net's password:  
Permission denied, please try again.  
root@server.ismakhorin.net's password:  
Permission denied, please try again.  
root@server.ismakhorin.net's password:  
root@server.ismakhorin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[ismakhorin@client.ismakhorin.net ~]$
```

**Рис. 1.3.** Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.

На сервере откроем файл `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запретим вход на сервер пользователю `root`, установив (Рис. 1.4):

`PermitRootLogin no`

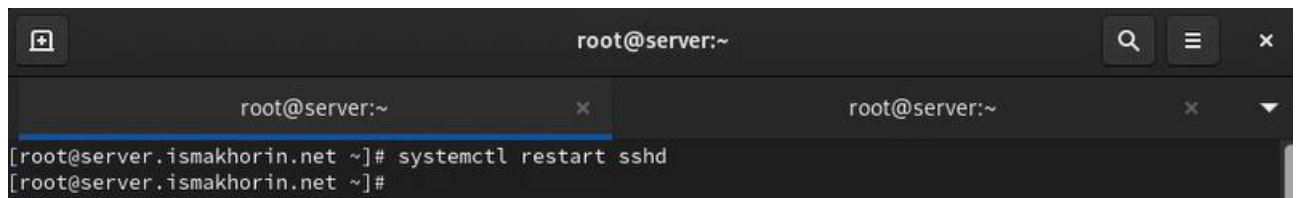


```
*sshd_config  
/etc/ssh  
32  
33 # Logging  
34 #SyslogFacility AUTH  
35 #LogLevel INFO  
36  
37 # Authentication:  
38  
39 #LoginGraceTime 2m  
40 PermitRootLogin no  
41 #StrictModes yes  
42 #MaxAuthTries 6  
43 #MaxSessions 10
```

**Рис. 1.4.** Открытие на сервере файла `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запрет входа на сервер пользователю `root`.

После сохранения изменений в файле конфигурации перезапустим `sshd` (Рис. 1.5):

`systemctl restart sshd`

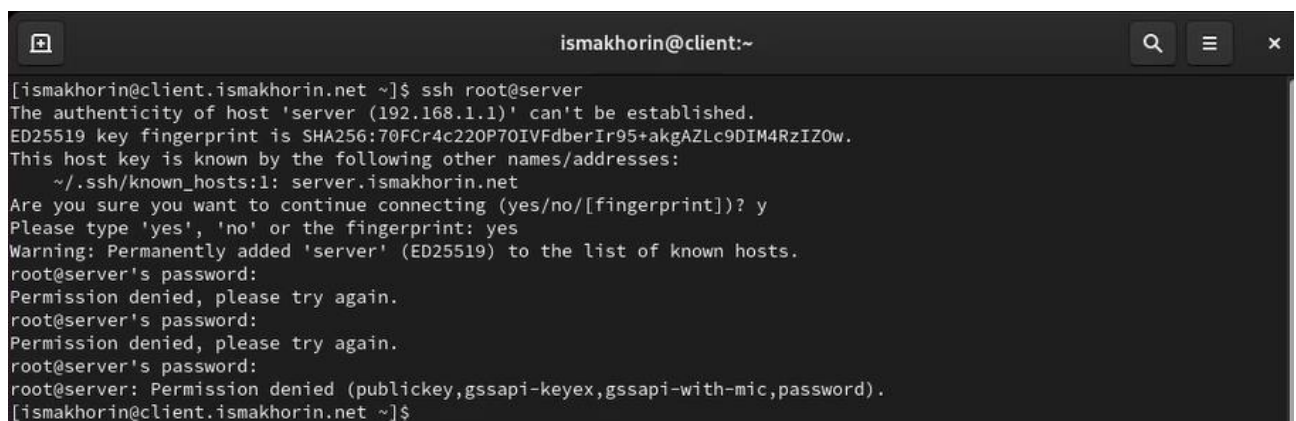


```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl restart sshd  
[root@server.ismakhorin.net ~]#
```

**Рис. 1.5.** Перезапуск sshd.

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root (Рис. 1.6):

```
ssh root@server
```

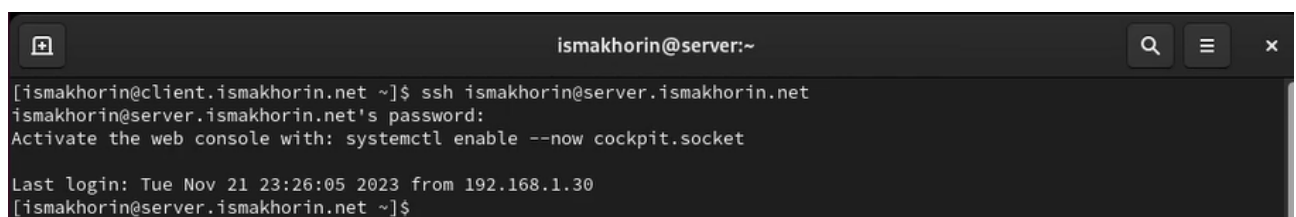


```
ismakhorin@client:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh root@server  
The authenticity of host 'server (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:70FCr4c220P70IVFdberIr95+akgAZLc9DIM4RzIZ0w.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: server.ismakhorin.net  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added 'server' (ED25519) to the list of known hosts.  
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).  
[ismakhorin@client.ismakhorin.net ~]$
```

**Рис. 1.6.** Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя root.

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя ismakhorin (Рис. 2.1):

```
ssh ismakhorin@server.ismakhorin.net
```

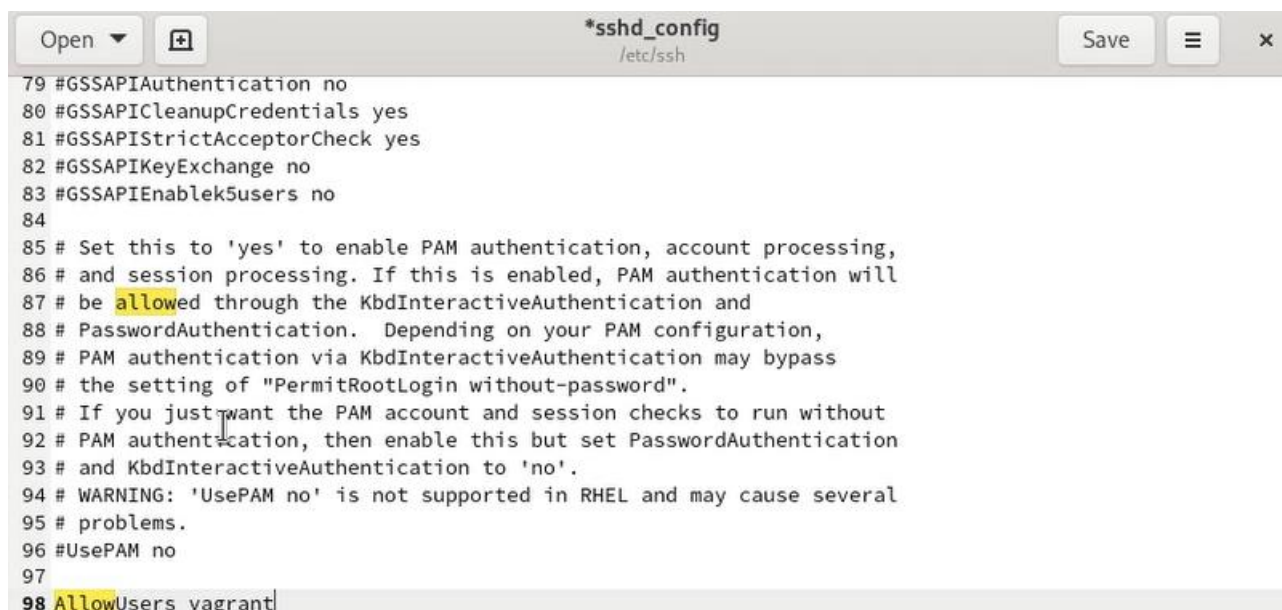


```
ismakhorin@server:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net  
ismakhorin@server.ismakhorin.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Tue Nov 21 23:26:05 2023 from 192.168.1.30  
[ismakhorin@server.ismakhorin.net ~]$
```

**Рис. 2.1.** Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя ismakhorin.

На сервере откроем файл `/etc/ssh/sshd_config` конфигурации `sshd` на редактирование и добавим строку (Рис. 2.2):

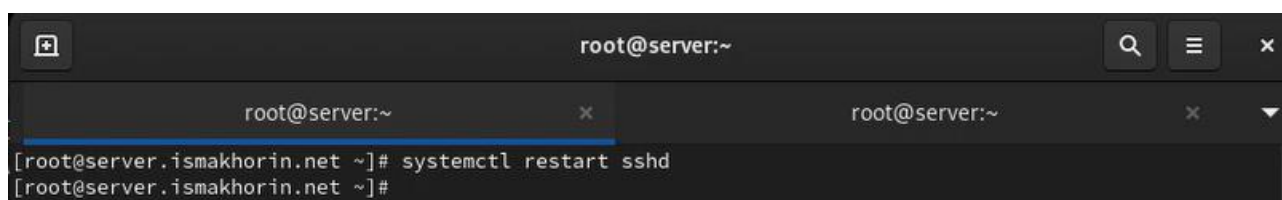
`AllowUsers vagrant`



**Рис. 2.2.** Открытие на сервере файла `/etc/ssh/sshd_config` конфигурации `sshd` на редактирование и добавление нужной строки.

После сохранения изменений в файле конфигурации перезапустим `sshd` (Рис. 2.3):

`systemctl restart sshd`



**Рис. 2.3.** Перезапуск `sshd`.

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `ismakhorin` (Рис. 2.4):

`ssh ismakhorin@server.ismakhorin.net`



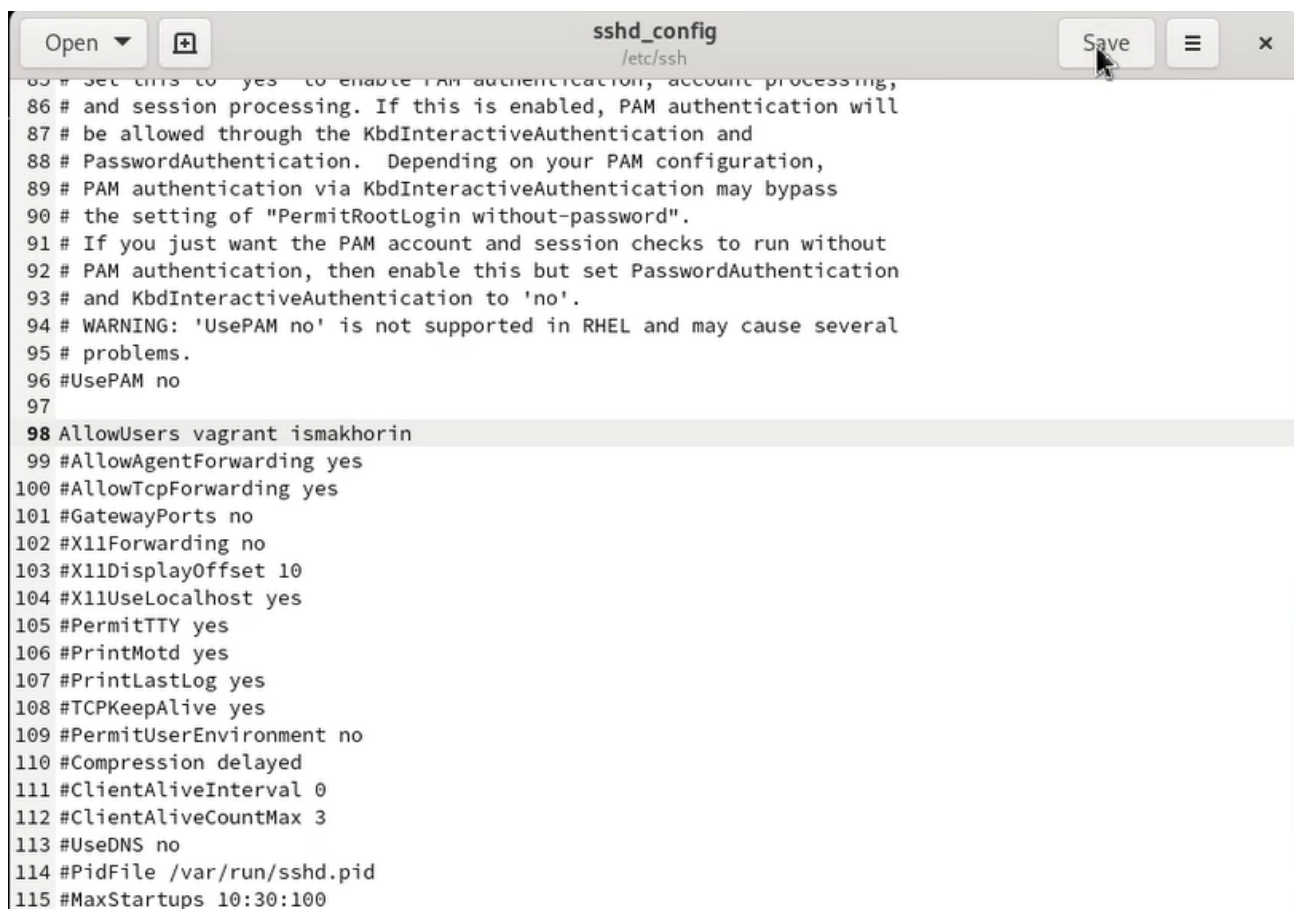


```
ismakhorin@client:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's password:  
Permission denied, please try again.  
ismakhorin@server.ismakhorin.net's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

**Рис. 2.4.** Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя ismakhorin.

В файле `/etc/ssh/sshd_config` конфигурации `sshd` внесём следующее изменение (Рис. 2.5):

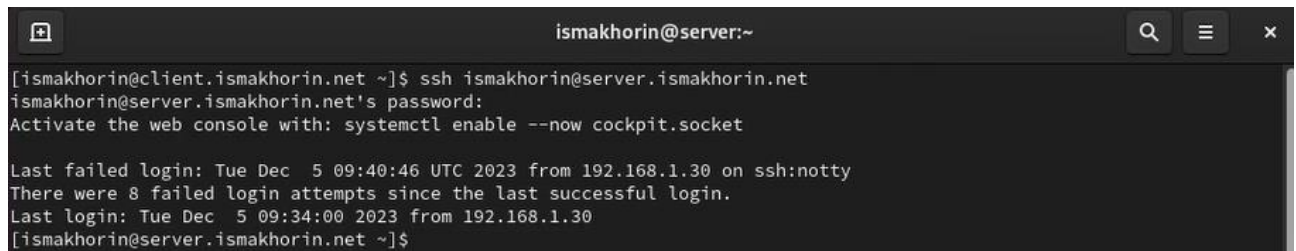
`AllowUsers vagrant ismakhorin`



```
Open  sshd_config /etc/ssh Save  
85 # Set this to yes to enable PAM authentication, account processing,  
86 # and session processing. If this is enabled, PAM authentication will  
87 # be allowed through the KbdInteractiveAuthentication and  
88 # PasswordAuthentication. Depending on your PAM configuration,  
89 # PAM authentication via KbdInteractiveAuthentication may bypass  
90 # the setting of "PermitRootLogin without-password".  
91 # If you just want the PAM account and session checks to run without  
92 # PAM authentication, then enable this but set PasswordAuthentication  
93 # and KbdInteractiveAuthentication to 'no'.  
94 # WARNING: 'UsePAM no' is not supported in RHEL and may cause several  
95 # problems.  
96 #UsePAM no  
97  
98 AllowUsers vagrant ismakhorin  
99 #AllowAgentForwarding yes  
100 #AllowTcpForwarding yes  
101 #GatewayPorts no  
102 #X11Forwarding no  
103 #X11DisplayOffset 10  
104 #X11UseLocalhost yes  
105 #PermitTTY yes  
106 #PrintMotd yes  
107 #PrintLastLog yes  
108 #TCPKeepAlive yes  
109 #PermitUserEnvironment no  
110 #Compression delayed  
111 #ClientAliveInterval 0  
112 #ClientAliveCountMax 3  
113 #UseDNS no  
114 #PidFile /var/run/sshd.pid  
115 #MaxStartups 10:30:100
```

**Рис. 2.5.** Внесение изменения в файле `/etc/ssh/sshd_config` конфигурации `sshd`.

После сохранения изменений в файле конфигурации перезапустим sshd и вновь попытаемся получить доступ с клиента к серверу посредством SSH-соединения через пользователя ismakhorin (Рис. 2.6):



```
ismakhorin@server:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net  
ismakhorin@server.ismakhorin.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last failed login: Tue Dec 5 09:40:46 UTC 2023 from 192.168.1.30 on ssh:notty  
There were 8 failed login attempts since the last successful login.  
Last login: Tue Dec 5 09:34:00 2023 from 192.168.1.30  
[ismakhorin@server.ismakhorin.net ~]$
```

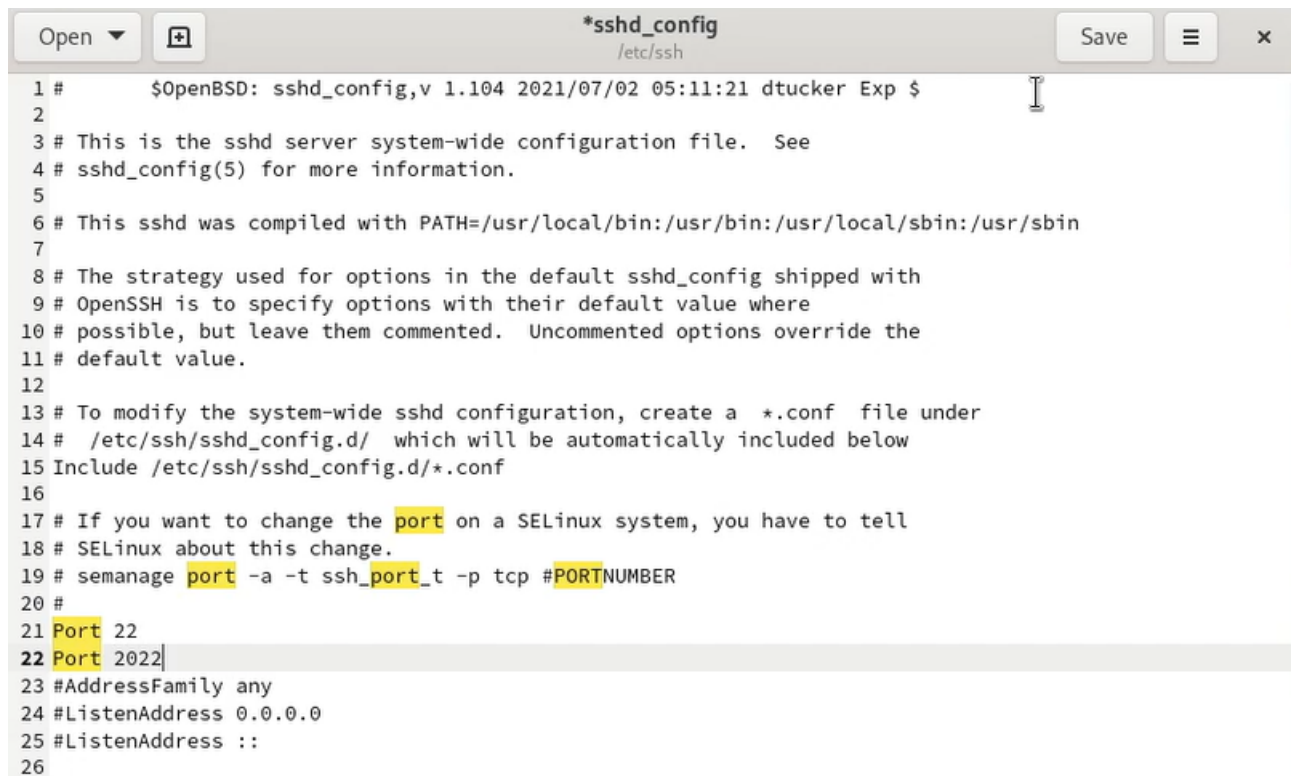
**Рис. 2.6.** Перезапуск sshd и повторная попытка получить доступ с клиента к серверу посредством SSH-соединения через пользователя ismakhorin.

На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдём строку Port и ниже этой строки добавим (Рис. 3.1):

Port 22

Port 2022





```
1 # $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $
2
3 # This is the sshd server system-wide configuration file. See
4 # sshd_config(5) for more information.
5
6 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
7
8 # The strategy used for options in the default sshd_config shipped with
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented. Uncommented options override the
11 # default value.
12
13 # To modify the system-wide sshd configuration, create a *.conf file under
14 # /etc/ssh/sshd_config.d/ which will be automatically included below
15 Include /etc/ssh/sshd_config.d/*.conf
16
17 # If you want to change the port on a SELinux system, you have to tell
18 # SELinux about this change.
19 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
20 #
21 Port 22
22 Port 2022
23 #AddressFamily any
24 #ListenAddress 0.0.0.0
25 #ListenAddress ::
26
```

**Рис. 3.1.** Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd\_config на сервере.

После сохранения изменений в файле конфигурации перезапустим sshd:

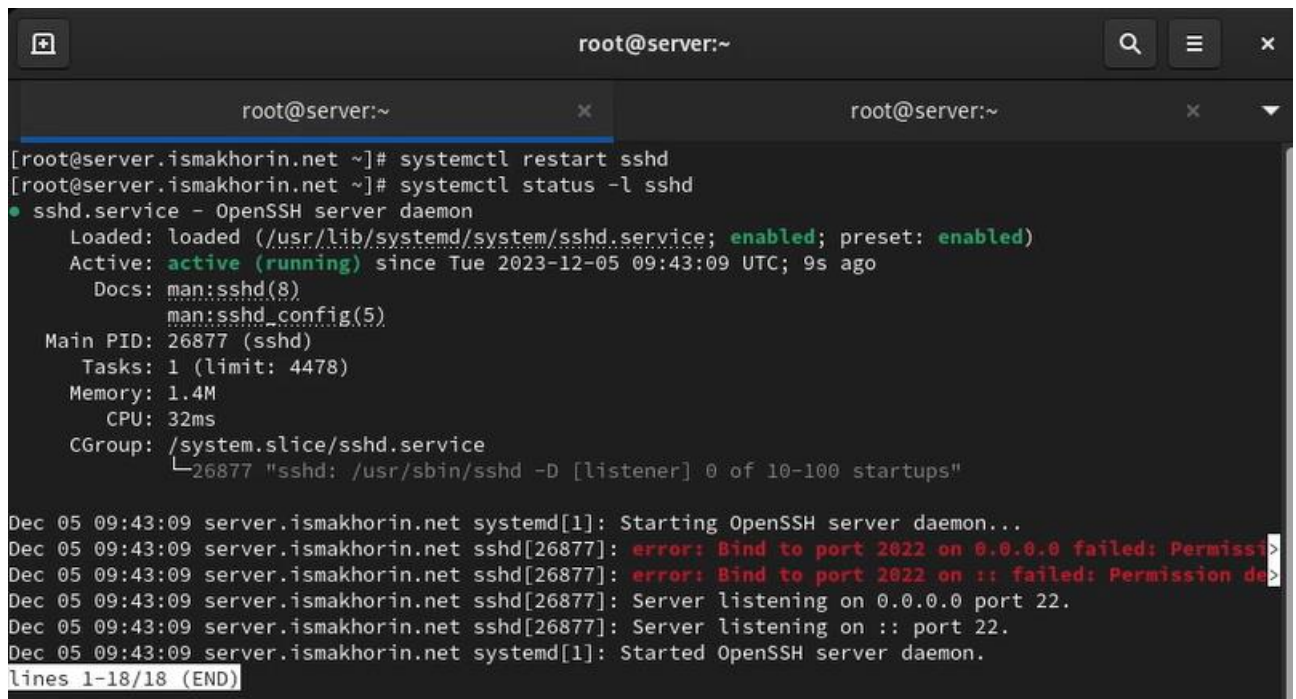
```
systemctl restart sshd
```

И посмотрим расширенный статус работы:

```
systemctl status -l sshd
```

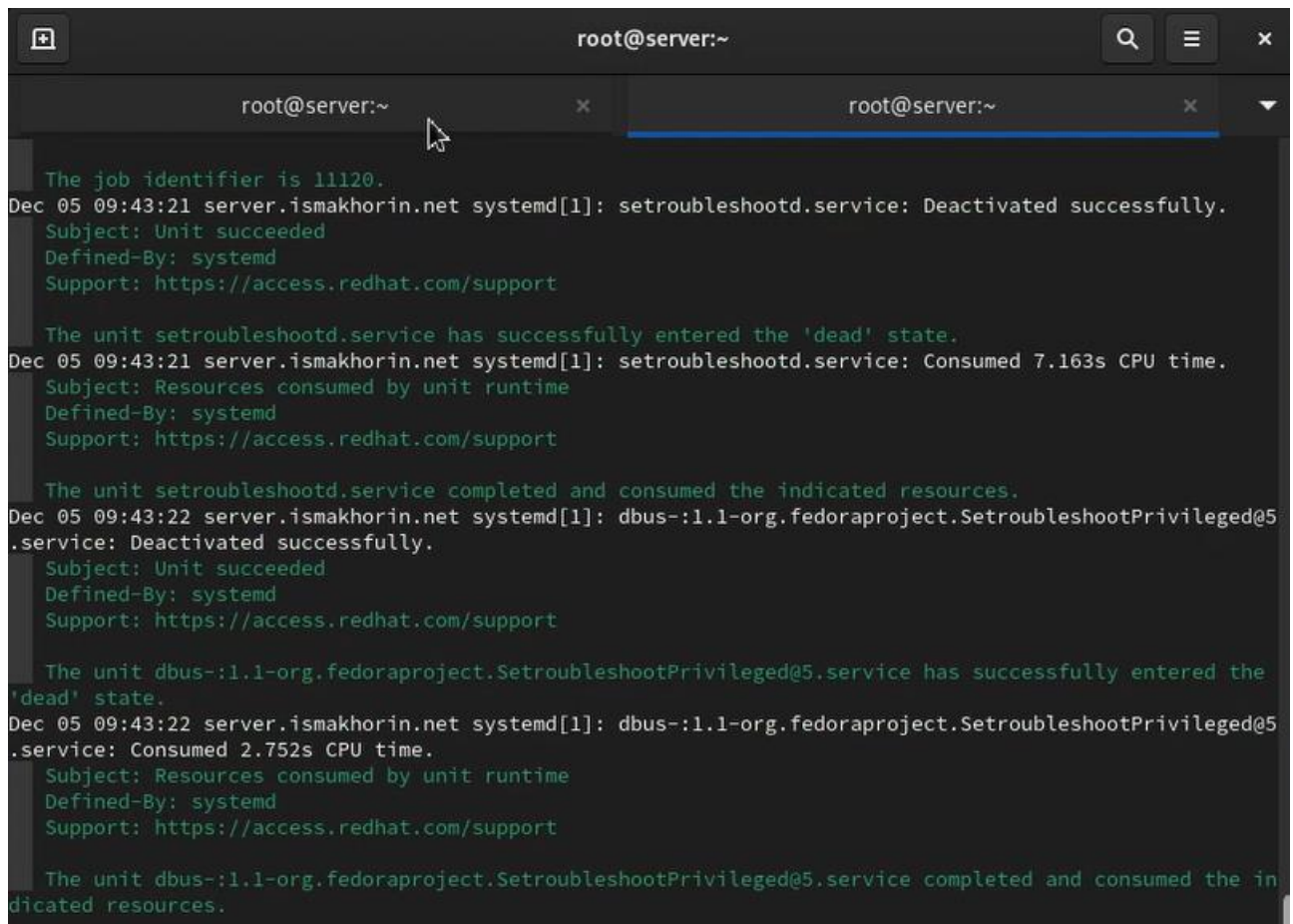
Система сообщила нам об отказе в работе sshd через порт 2022 (Рис. 3.2):

Дополнительно посмотрим сообщения в терминале с мониторингом системных событий (Рис. 3.3):



```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl restart sshd  
[root@server.ismakhorin.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 Tue 2023-12-05 09:43:09 UTC; 9s ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Main PID: 26877 (sshd)  
    Tasks: 1 (limit: 4478)  
   Memory: 1.4M  
      CPU: 32ms  
   CGroup: /system.slice/sshd.service  
           └─26877 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Dec 05 09:43:09 server.ismakhorin.net systemd[1]: Starting OpenSSH server daemon...  
Dec 05 09:43:09 server.ismakhorin.net sshd[26877]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied  
Dec 05 09:43:09 server.ismakhorin.net sshd[26877]: error: Bind to port 2022 on :: failed: Permission denied  
Dec 05 09:43:09 server.ismakhorin.net sshd[26877]: Server listening on 0.0.0.0 port 22.  
Dec 05 09:43:09 server.ismakhorin.net sshd[26877]: Server listening on :: port 22.  
Dec 05 09:43:09 server.ismakhorin.net systemd[1]: Started OpenSSH server daemon.  
lines 1-18/18 (END)
```

**Рис. 3.2.** Перезапуск sshd и просмотр расширенного статуса работы.

A screenshot of a terminal window titled 'root@server:~'. The terminal displays a series of systemd logs. The first log entry is at 09:43:21, showing 'setroublshootd.service: Deactivated successfully'. The second log entry is at 09:43:21, showing 'setroublshootd.service: Consumed 7.163s CPU time'. The third log entry is at 09:43:22, showing 'dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5.service: Deactivated successfully'. The fourth log entry is at 09:43:22, showing 'dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5.service: Consumed 2.752s CPU time'. The logs are color-coded: green for success and state changes, and white for resource consumption and timestamps. The terminal window has a dark background and a light-colored cursor pointing at the first log entry.

```
The job identifier is 11120.
Dec 05 09:43:21 server.ismakhorin.net systemd[1]: setroublshootd.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://access.redhat.com/support

The unit setroublshootd.service has successfully entered the 'dead' state.
Dec 05 09:43:21 server.ismakhorin.net systemd[1]: setroublshootd.service: Consumed 7.163s CPU time.
Subject: Resources consumed by unit runtime
Defined-By: systemd
Support: https://access.redhat.com/support

The unit setroublshootd.service completed and consumed the indicated resources.
Dec 05 09:43:22 server.ismakhorin.net systemd[1]: dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5
.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://access.redhat.com/support

The unit dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5.service has successfully entered the
'dead' state.
Dec 05 09:43:22 server.ismakhorin.net systemd[1]: dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5
.service: Consumed 2.752s CPU time.
Subject: Resources consumed by unit runtime
Defined-By: systemd
Support: https://access.redhat.com/support

The unit dbus-:1.1-org.fedoraproject.SetroublshootPrivileged@5.service completed and consumed the in
dicated resources.
```

**Рис. 3.3.** Просмотр сообщения в терминале с мониторингом системных событий.

Исправим на сервере метки SELinux к порту 2022:

```
semanage port -a -t ssh_port_t -p tcp 2022
```

В настройках межсетевого экрана откроем порт 2022 протокола TCP:

```
firewall-cmd --add-port=2022/tcp
```

```
firewall-cmd --add-port=2022/tcp --permanent
```

Вновь перезапустим sshd и посмотрим расширенный статус его работы (статус показывает, что процесс sshd теперь прослушивает два порта) (Рис. 3.4):

```
[root@server.ismakhorin.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.ismakhorin.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.ismakhorin.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.ismakhorin.net ~]# systemctl restart sshd
[root@server.ismakhorin.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 Tue 2023-12-05 09:44:45 UTC; 4s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 26902 (sshd)
    Tasks: 1 (limit: 4478)
   Memory: 2.4M
      CPU: 36ms
   CGroup: /system.slice/sshd.service
           └─26902 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 05 09:44:45 server.ismakhorin.net systemd[1]: Starting OpenSSH server daemon...
Dec 05 09:44:45 server.ismakhorin.net sshd[26902]: Server listening on 0.0.0.0 port 2022.
Dec 05 09:44:45 server.ismakhorin.net sshd[26902]: Server listening on :: port 2022.
Dec 05 09:44:45 server.ismakhorin.net sshd[26902]: Server listening on 0.0.0.0 port 22.
Dec 05 09:44:45 server.ismakhorin.net sshd[26902]: Server listening on :: port 22.
Dec 05 09:44:45 server.ismakhorin.net systemd[1]: Started OpenSSH server daemon.
[root@server.ismakhorin.net ~]#
```

**Рис. 3.4.** Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя ismakhorin:

```
ssh ismakhorin@server.ismakhorin.net
```

После открытия оболочки пользователя введём `sudo -i` для получения доступа root (Рис. 3.5):

```
root@server:~
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net
ismakhorin@server.ismakhorin.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

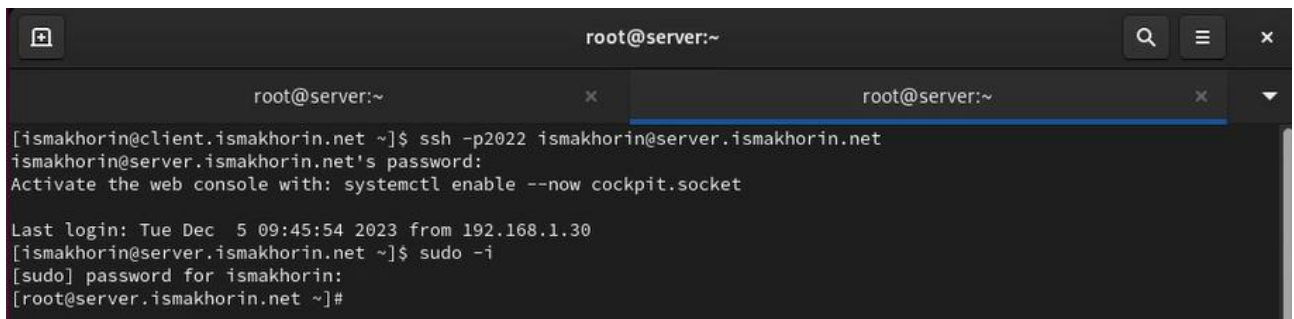
Last login: Tue Dec  5 09:41:27 2023 from 192.168.1.30
[ismakhorin@server.ismakhorin.net ~]$ sudo -i
[sudo] password for ismakhorin:
[root@server.ismakhorin.net ~]#
```

**Рис. 3.5.** Попытка получить с клиента доступа к серверу посредством SSH-соединения через пользователя ismakhorin и получение доступа root.

Теперь повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя ismakhorin, указав порт 2022:

```
ssh -p2022 ismakhorin@server.ismakhorin.net
```

После открытия оболочки пользователя введём `sudo -i` для получения доступа root (рис. 3.6):



```
root@server:~
[ismakhorin@client.ismakhorin.net ~]$ ssh -p2022 ismakhorin@server.ismakhorin.net
ismakhorin@server.ismakhorin.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Dec  5 09:45:54 2023 from 192.168.1.30
[ismakhorin@server.ismakhorin.net ~]$ sudo -i
[sudo] password for ismakhorin:
[root@server.ismakhorin.net ~]#
```

**Рис. 3.6.** Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя ismakhorin, указав порт 2022. Получение доступа root.

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

```
PubkeyAuthentication yes
```

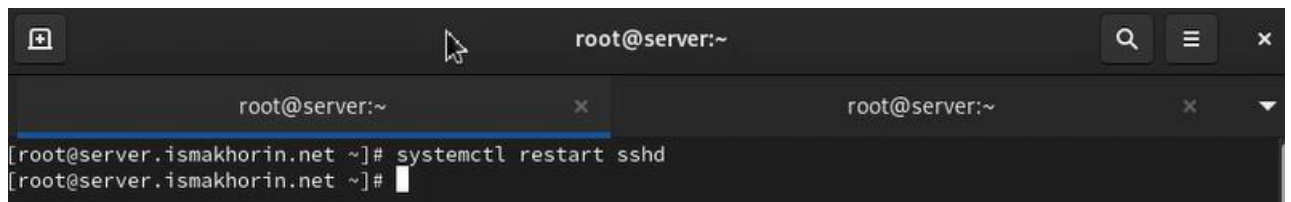


```
Open  sshd_config /etc/ssh Save
39
40 #LoginGraceTime 2m
41 PermitRootLogin no
42 #StrictModes yes
43 #MaxAuthTries 6
44 #MaxSessions 10
45
46 PubkeyAuthentication yes
47
```

**Рис. 4.1.** Настройка параметра на сервере в конфигурационном файле `/etc/ssh/sshd_config`, разрешающего аутентификацию по ключу.

После сохранения изменений в файле конфигурации перезапустим `sshd` (рис. 4.2):





```
root@server:~  
[root@server.ismakhorin.net ~]# systemctl restart sshd  
[root@server.ismakhorin.net ~]#
```

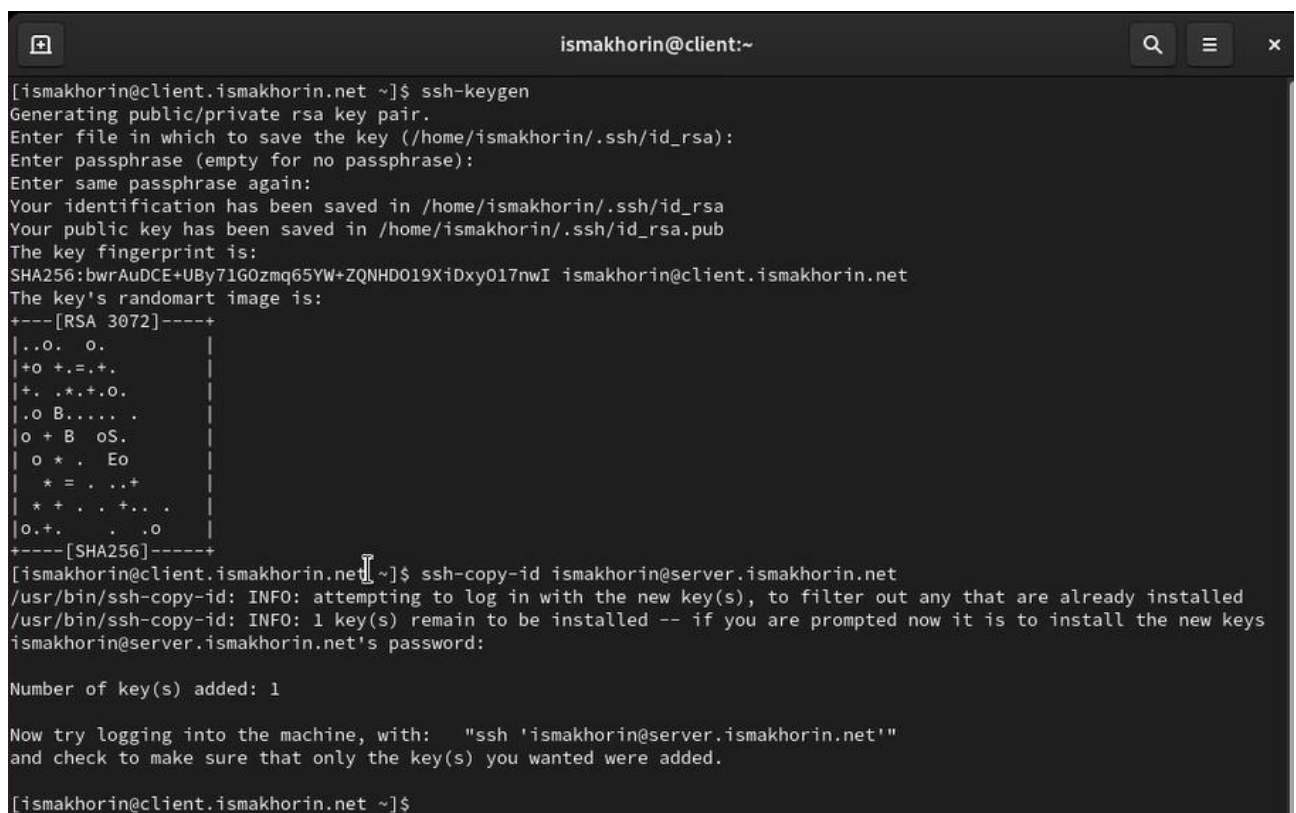
**Рис. 4.2.** Перезапуск sshd.

На клиенте сформируем SSH-ключ, введя в терминале под пользователем ismakhorin

```
ssh-keygen
```

Далее скопируем открытый ключ на сервер, введя на клиенте (рис. 4.3):

```
ssh-copy-id ismakhorin@server.ismakhorin.net
```



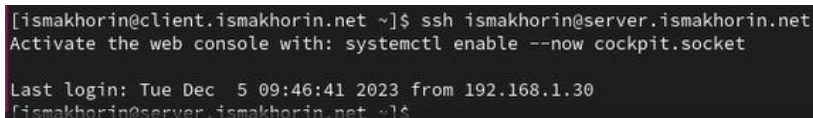
```
ismakhorin@client:~  
[ismakhorin@client.ismakhorin.net ~]$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/ismakhorin/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/ismakhorin/.ssh/id_rsa  
Your public key has been saved in /home/ismakhorin/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:bwrAuDCE+UBy71G0zmq65YW+ZQNHD019XiDxy017nwI ismakhorin@client.ismakhorin.net  
The key's randomart image is:  
+----[RSA 3072]-----+  
|.O. O.  
|+o +.=.+.  
|+. .*.+.O.  
|.O B.....  
|o + B oS.  
| o * . Eo  
| * = . ..+  
| * + . . +..  
|o+. . .o  
+----[SHA256]-----+  
[ismakhorin@client.ismakhorin.net ~]$ ssh-copy-id ismakhorin@server.ismakhorin.net  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys  
ismakhorin@server.ismakhorin.net's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'ismakhorin@server.ismakhorin.net'"  
and check to make sure that only the key(s) you wanted were added.  
[ismakhorin@client.ismakhorin.net ~]$
```

**Рис. 4.3.** Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.

Попробуем получить доступ с клиента к серверу посредством SSH-соединения:

```
ssh ismakhorin@server.ismakhorin.net
```

Теперь мы проходим аутентификацию без ввода пароля для учётной записи удалённого пользователя (рис. 4.4):



```
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Dec  5 09:46:41 2023 from 192.168.1.30
ismakhorin@server.ismakhorin.net ~$
```

**Рис. 4.4.** Попытка получения доступа с клиента к серверу посредством SSH-соединения.

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP:

```
lsof | grep TCP
```

После чего перенаправим порт 80 на server.ismakhorin.net на порт 8080 на локальной машине (рис. 5.1):

```
ssh -fNL 8080:localhost:80 ismakhorin@server.ismakhorin.net
```



```
root@client:~  
[ismakhorin@client.ismakhorin.net ~]$ lsof | grep TCP  
[ismakhorin@client.ismakhorin.net ~]$ sudo -i  
[sudo] password for ismakhorin:  
[root@client.ismakhorin.net ~]# lsof | grep TCP  
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs  
Output information may be incomplete.  
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc  
Output information may be incomplete.  
cupsd      690          root      6u      IPv6      20091      0t0      TCP localhost:ipp (LISTEN)  
cupsd      690          root      7u      IPv4      20092      0t0      TCP localhost:ipp (LISTEN)  
sshd       696          root      3u      IPv4      20108      0t0      TCP *:ssh (LISTEN)  
sshd       696          root      4u      IPv6      20119      0t0      TCP *:ssh (LISTEN)  
master    14838        root     13u      IPv4     100870     0t0      TCP localhost:smtp (LISTEN)  
[root@client.ismakhorin.net ~]# ssh -fNL 8080:localhost:80 ismakhorin@server.ismakhorin.net  
The authenticity of host 'server.ismakhorin.net (192.168.1.1)' can't be established.  
ED25519 key fingerprint is SHA256:70FCr4c220P70IVFdberIr95+akgAZLc9DIM4RzIZ0w.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [server.ismakhorin.net]:2022  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'server.ismakhorin.net' (ED25519) to the list of known hosts.  
ismakhorin@server.ismakhorin.net's password:  
[root@client.ismakhorin.net ~]#
```

**Рис. 5.1.** Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.ismakhorin.net на порт 8080 на локальной машине.

Вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP (рис. 5.2):

`lsof | grep TCP`

```
[root@client.ismakhorin.net ~]# lsof | grep TCP  
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs  
Output information may be incomplete.  
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc  
Output information may be incomplete.  
cupsd      690          root      6u      IPv6      20091      0t0      TCP localhost:ipp (LISTEN)  
cupsd      690          root      7u      IPv4      20092      0t0      TCP localhost:ipp (LISTEN)  
sshd       696          root      3u      IPv4      20108      0t0      TCP *:ssh (LISTEN)  
sshd       696          root      4u      IPv6      20119      0t0      TCP *:ssh (LISTEN)  
master    14838        root     13u      IPv4     100870     0t0      TCP localhost:smtp (LISTEN)  
ssh        21316        root      3u      IPv4     193614     0t0      TCP client.ismakhor  
in.net:37836->mail.ismakhorin.net:ssh (ESTABLISHED)  
ssh        21316        root      4u      IPv6     193666     0t0      TCP localhost:webca  
che (LISTEN)  
ssh        21316        root      5u      IPv4     193667     0t0      TCP localhost:webca  
che (LISTEN)  
[root@client.ismakhorin.net ~]# clear
```

**Рис. 5.2.** Повторный просмотр на клиенте запущенных служб с протоколом TCP.

На клиенте запустим браузер и в адресной строке введём localhost:8080. Убедимся, что отобразилась страница с приветствием «Welcome to the server.ismakhorin.net server» (Рис. 5.3):



**Рис. 5.3.** Запуск на клиенте браузера и ввод в адресной строке localhost:8080.

На клиенте откроем терминал под пользователем ismakhorin и посмотрим с клиента имя узла сервера:

```
ssh ismakhorin@server.ismakhorin.net hostname
```

Посмотрим с клиента список файлов на сервере:

```
ssh ismakhorin@server.ismakhorin.net ls -Al
```

Посмотрим с клиента почту на сервере (рис. 6):

```
ssh ismakhorin@server.ismakhorin.net MAIL=~/.Maildir/ mail
```

```
ismakhorin@client:~ — ssh ismakhorin@server.ismakhorin.net MAIL=/home/ismakhorin/Maildir/ mail
drwx-----. 8 ismakhorin ismakhorin 4096 Nov 21 17:19 .config
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Desktop
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Documents
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Downloads
-rw-----. 1 ismakhorin ismakhorin 20 Nov 21 22:58 .lessht
drwx-----. 4 ismakhorin ismakhorin 32 Nov 21 17:19 .local
drwx-----. 5 ismakhorin ismakhorin 4096 Dec 4 23:05 Maildir
drwxr-xr-x. 4 ismakhorin ismakhorin 39 Nov 21 11:36 .mozilla
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Music
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Pictures
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Public
drwx-----. 2 ismakhorin ismakhorin 29 Dec 5 09:50 .ssh
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Templates
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-clipboard-tty1-control.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-clipboard-tty1-service.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-display-svg-x11-tty1-control.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-display-svg-x11-tty1-service.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-draganddrop-tty1-control.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-draganddrop-tty1-service.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-hostversion-tty1-control.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-seamless-tty1-control.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-seamless-tty1-service.pid
-rw-r-----. 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-vmvga-session-tty1-control.pid
drwxr-xr-x. 2 ismakhorin ismakhorin 6 Nov 21 17:19 Videos
-rw-----. 1 ismakhorin ismakhorin 1087 Nov 21 19:34 .xsession-errors
-rw-----. 1 ismakhorin ismakhorin 318 Nov 21 17:19 .xsession-errors.old
[ismakhorin@client.ismakhorin.net ~]$ ssh ismakhorin@server.ismakhorin.net MAIL=/home/ismakhorin/Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/ismakhorin/Maildir: 4 messages
• 1 ismakhorin 2023-11-22 00:18 19/666 "test1"
  2 ismakhorin@client.is 2023-12-04 21:31 21/859 "LMTP test"
  3 ismakhorin 2023-12-04 22:07 22/835 "test3"
  4 ismakhorin 2023-12-04 22:57 22/829 "t1"
```

**Рис. 6.** Открытие на клиенте терминала под пользователем ismakhorin.

Просмотр имени узла сервера, списка файлов на сервере и почты на сервере.

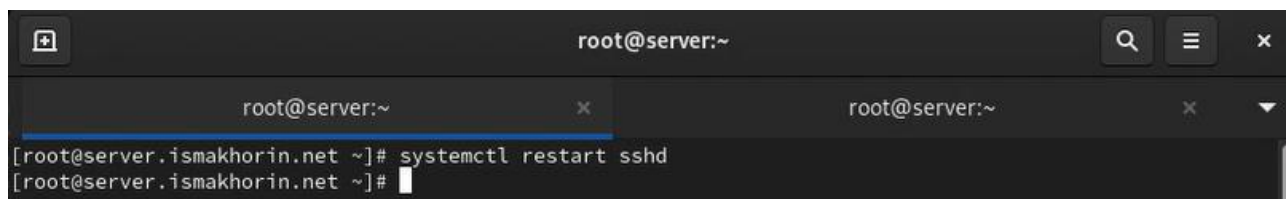
На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешим отображать на локальном клиентском компьютере графические интерфейсы X11 (рис. 7.1):

X11Forwarding yes

```
*sshd_config
/etc/ssh
Save
96 # problems.
97 #UsePAM no
98
99 AllowUsers vagrant ismakhorin
100 #AllowAgentForwarding yes
101 #AllowTcpForwarding yes
102 #GatewayPorts no
103 X11Forwarding yes
```

**Рис. 7.1.** Разрешение отображать на сервере в конфигурационном файле `/etc/ssh/sshd_config` на локальном клиентском компьютере графические интерфейсы X11.

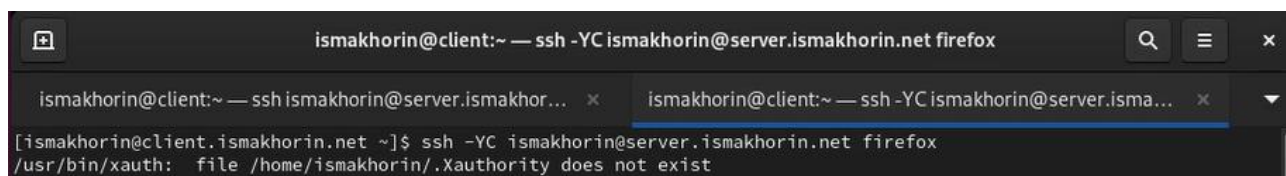
После сохранения изменения в конфигурационном файле перезапустим sshd (рис. 7.2):



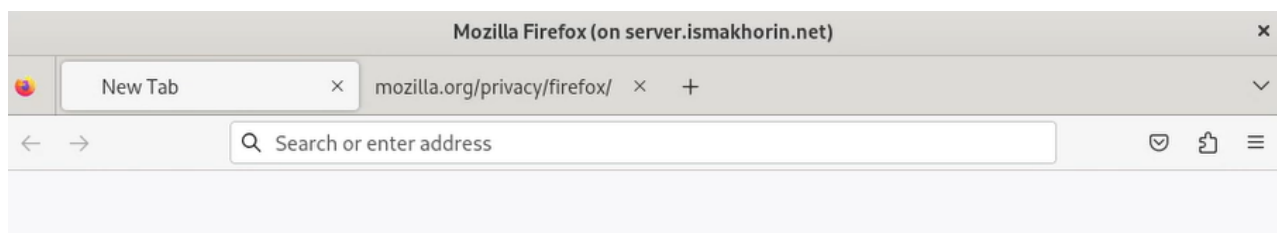
**Рис. 7.2.** Перезапуск sshd.

Попробуем с клиента удалённо подключиться к серверу и (рис. 7.3) запустить графическое приложение firefox (рис. 7.4):

```
ssh -YC ismakhorin@server.ismakhorin.net firefox
```



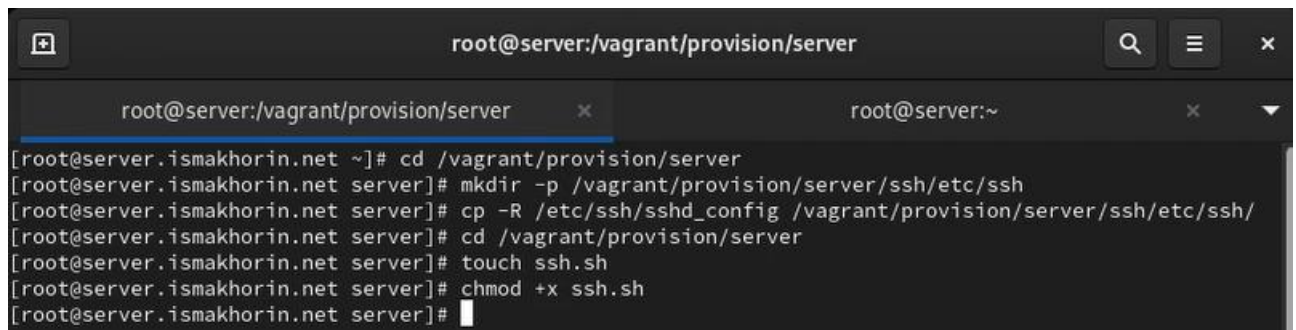
**Рис. 7.3.** Попытка с клиента удалённо подключиться к серверу и запустить графическое приложение firefox.



**Рис. 7.4.** Запуск графического приложения firefox.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `ssh`, в который поместим в соответствующие подкаталоги

конфигурационный файл `sshd_config`. В каталоге `/vagrant/provision/server` создадим исполняемый файл `ssh.sh` (рис. 8.1):



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

**Рис. 8.1.** Переход на виртуальной машине `server` в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `ssh`, в который поместили в соответствующие подкаталоги конфигурационный файл `sshd_config`. Создание в каталоге `/vagrant/provision/server` исполняемого файла `ssh.sh`.

Открыв его на редактирование, пропишем в нём скрипт из лабораторной работы (Рис. 8.2):



```
ssh.sh
/vagrant/provision/server
Save
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Copy configuration files"
6 cp -R /vagrant/provision/server/ssh/etc/* /etc
7
8 restorecon -vR /etc
9
10 echo "Configure firewall"
11 firewall-cmd --add-port=2022/tcp
12 firewall-cmd --add-port=2022/tcp --permanent
13
14 echo "Tuning SELinux"
15 semanage port -a -t ssh_port_t -p tcp 2022
16
17 echo "Restart sshd service"
18 systemctl restart sshd
```

**Рис. 8.2.** Открытие файла на редактирование и написание в нём скрипта.



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

```
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
```

**Рис. 8.3.** Редактирование конфигурационного файла Vagrantfile.

### **Вывод:**

В ходе выполнения лабораторной работы были приобретены практические навыки по настройке удалённого доступа к серверу с помощью SSH.

### **Ответы на контрольные вопросы:**

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

**В конфигурационном файле SSH /etc/ssh/sshd\_config:**

**# Запрет удалённого доступа пользователю root**

**PermitRootLogin no**

**# Разрешение доступа пользователю alice**

**AllowUsers alice**

**После внесения изменений, необходимо перезапустить службу SSH:**

**sudo service ssh restart**

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

**В конфигурационном файле /etc/ssh/sshd\_config добавьте строки:**

**# Первый порт (по умолчанию 22)**

**Port 22**

**# Второй порт**

**Port 2222**

**После изменений перезапустите службу SSH. Это может быть полезно для повышения безопасности, а также для избежания конфликтов с другими службами, использующими порт 22.**

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

**ssh -N -f -L local\_port:destination\_host:remote\_port user@ssh\_server**

**-N: Не выполнять команду на удаленном хосте.**

**-f: Перевести ssh в фоновый режим после установки туннеля.**

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

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



Теперь, при подключении к локальному порту 5555, трафик будет перенаправляться через SSH к порту 80 на сервере `server2.example.com`.

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

```
sudo semanage port -a -t ssh_port_t -p tcp 2022
```

Данная команда добавляет правило SELinux, разрешая использование порта 2022 для сервиса ssh.

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

```
sudo firewall-cmd --permanent --add-port=2022/tcp
```

```
sudo firewall-cmd --reload
```

Эти команды добавляют правило в межсетевой экран для разрешения входящих подключений по SSH через порт 2022 и перезагружают конфигурацию межсетевого экрана.