

Лабораторная работа №11

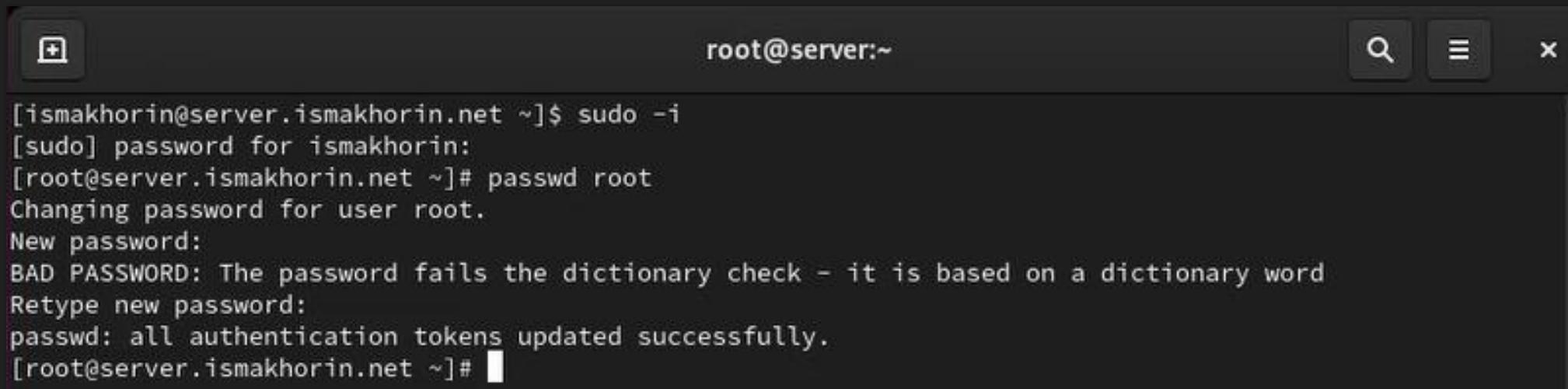
Настройка безопасного удалённого доступа по протоколу SSH

Махорин Иван Сергеевич

1032211221

НПИБд-02-21

Запрет удалённого доступа по SSH для пользователя root

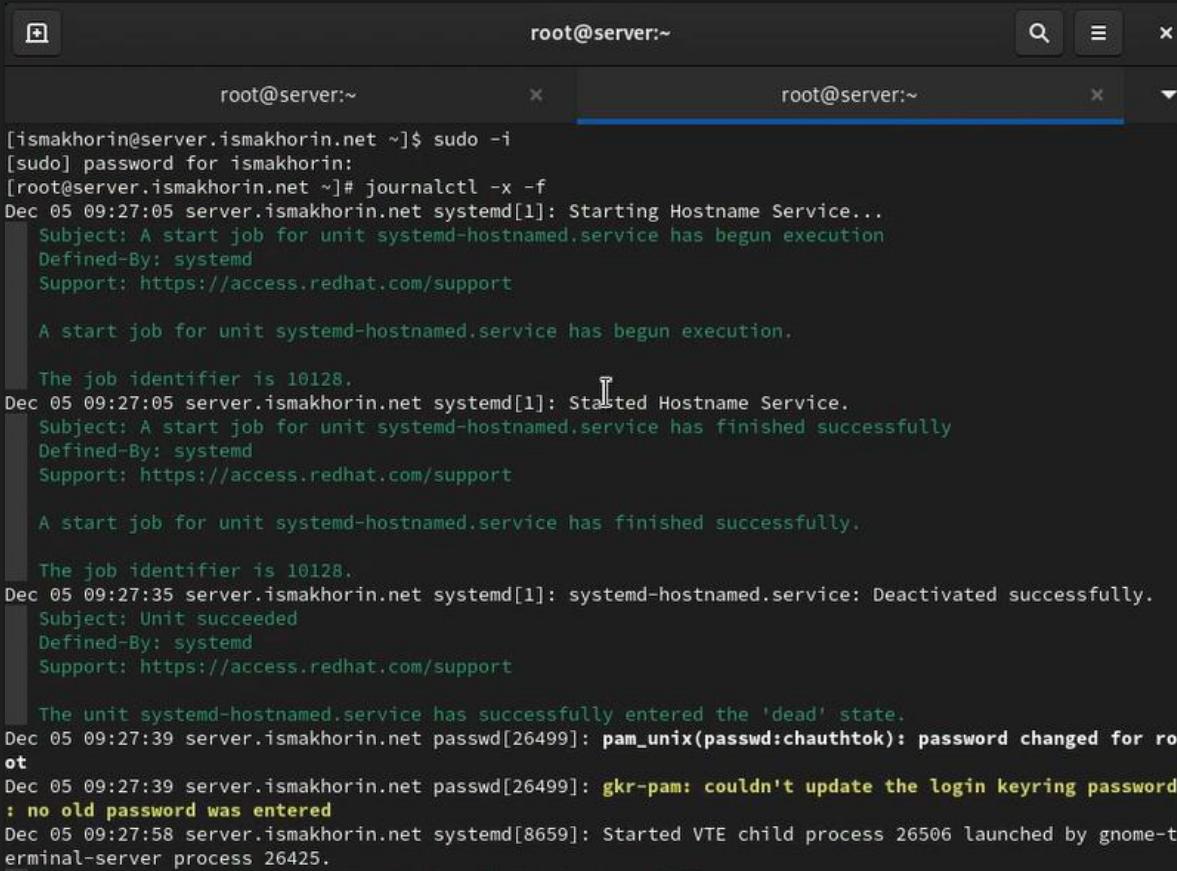


A screenshot of a terminal window titled "root@server:~". The window contains the following command-line session:

```
[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.

Запрет удалённого доступа по SSH для пользователя root



The screenshot shows a terminal window titled "root@server:~". It displays the output of the command "journalctl -x -f". The log entries show the start, success, and deactivation of the "systemd-hostnamed" service, along with a password change event for user "root".

```
[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

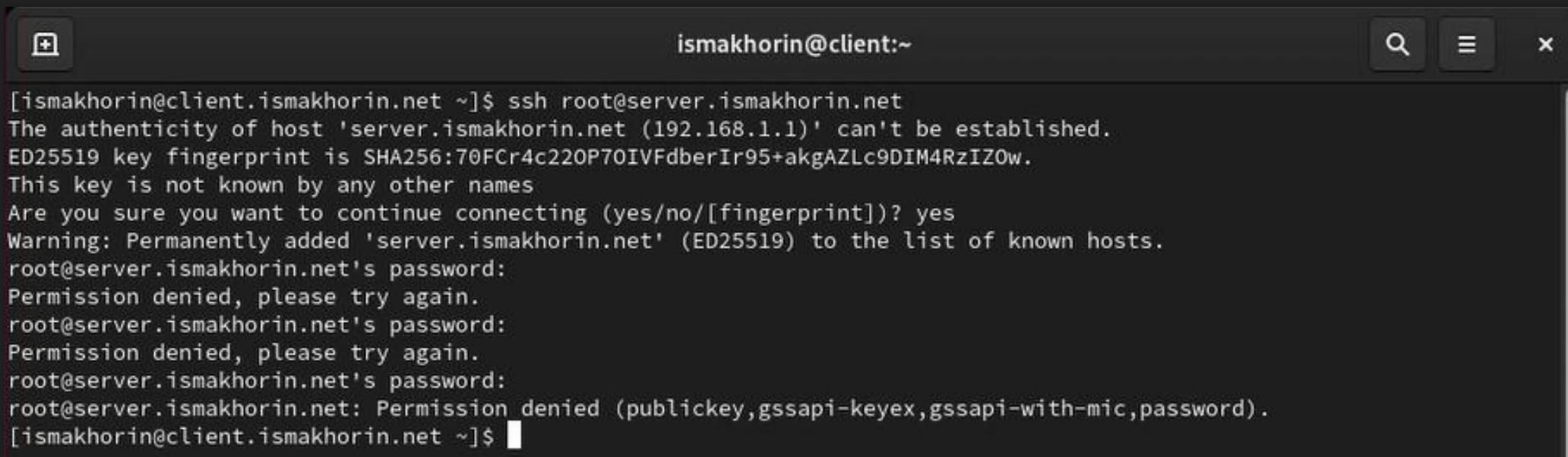
  A start job for unit systemd-hostnamed.service has finished successfully.

  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.

Запрет удалённого доступа по SSH для пользователя root



The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "ismakhorin@client:~". The window contains the following text:

```
[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.

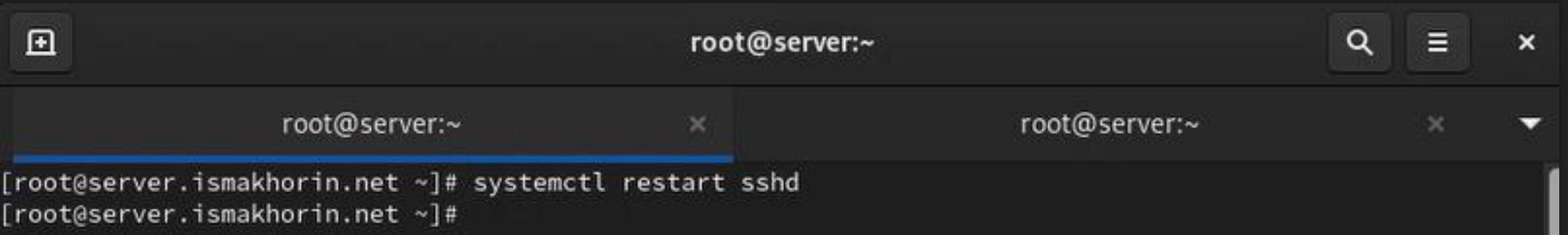
Запрет удалённого доступа по SSH для пользователя root



```
Open *sshd_config /etc/ssh Save ×
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.

Запрет удалённого доступа по SSH для пользователя root

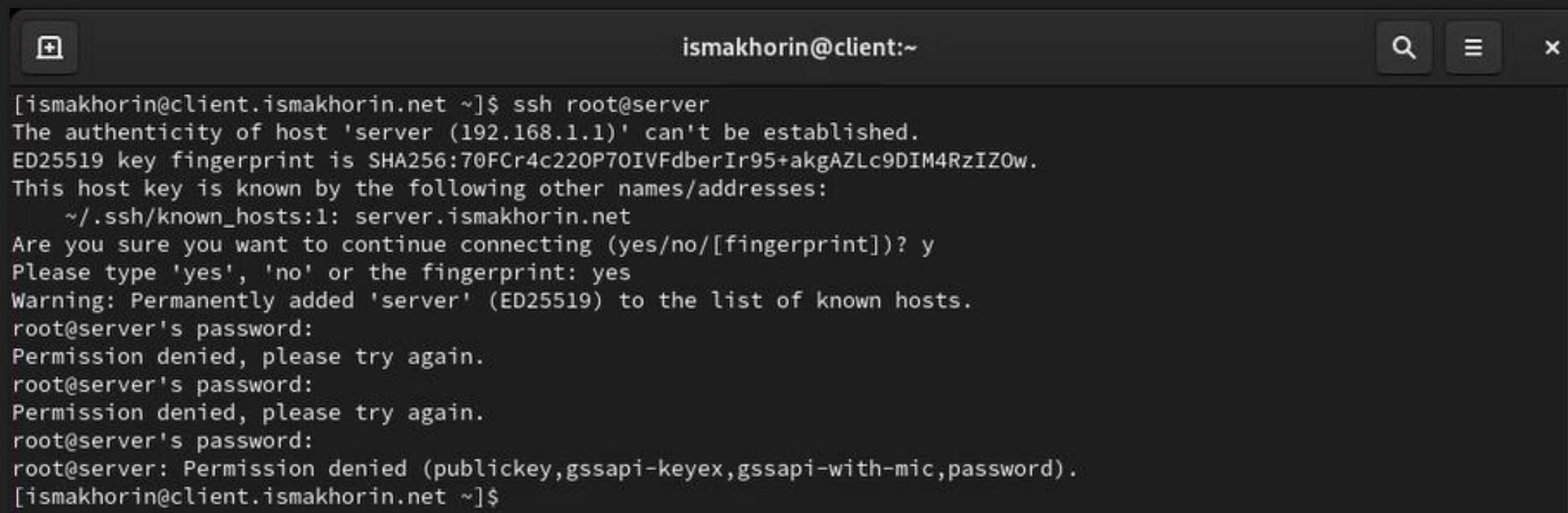


The screenshot shows a terminal window with a dark theme. At the top, there is a header bar with icons for a new tab, search, and other functions. Below it, the title bar shows the session is running as 'root@server:~'. The main area of the terminal contains two tabs, both labeled 'root@server:~'. The bottom tab is active and shows the command line. The user has typed '[root@server.ismakhordin.net ~]# systemctl restart sshd' and pressed Enter. The command is displayed in white text on a black background.

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

Рис. 1.5. Перезапуск sshd.

Запрет удалённого доступа по SSH для пользователя root

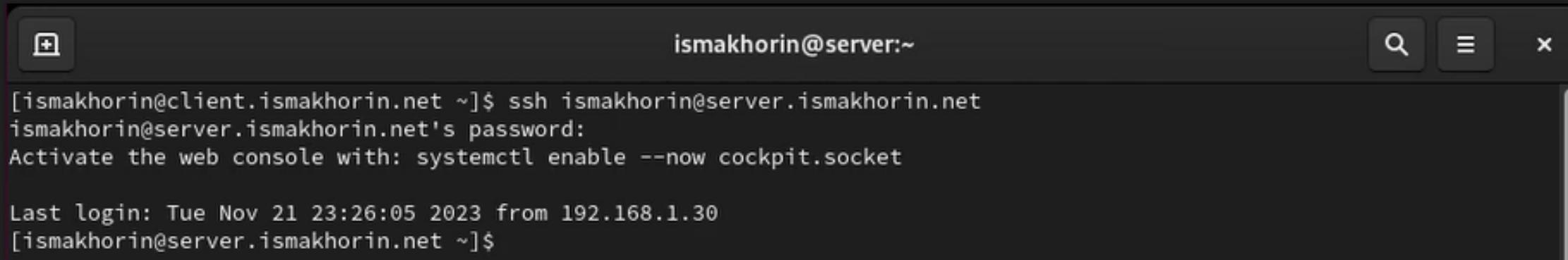


The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "ismakhorin@client:~". The window contains the following text:

```
[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.

Ограничение списка пользователей для удалённого доступа по SSH



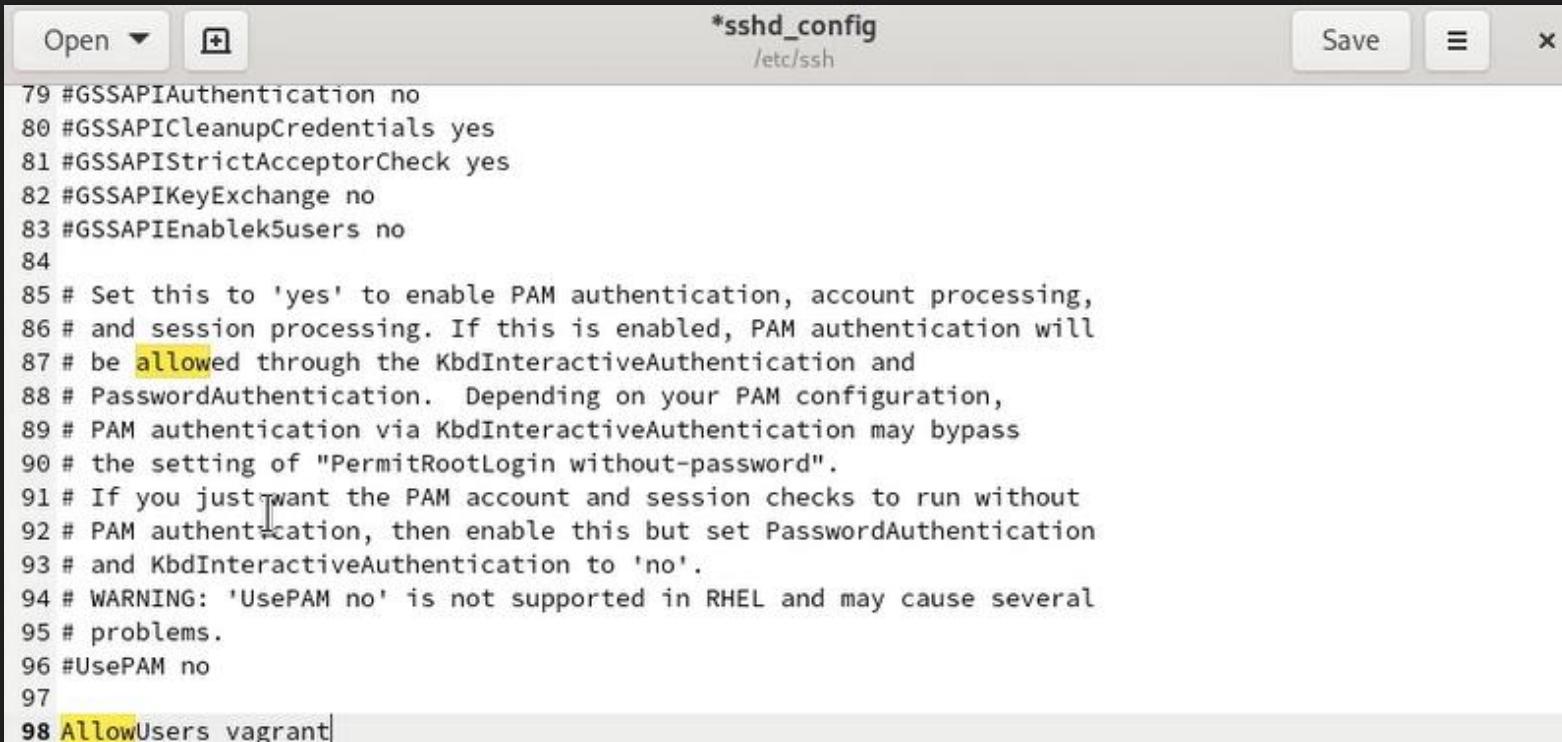
The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "ismakhorin@server:~". The window contains the following text:

```
[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.

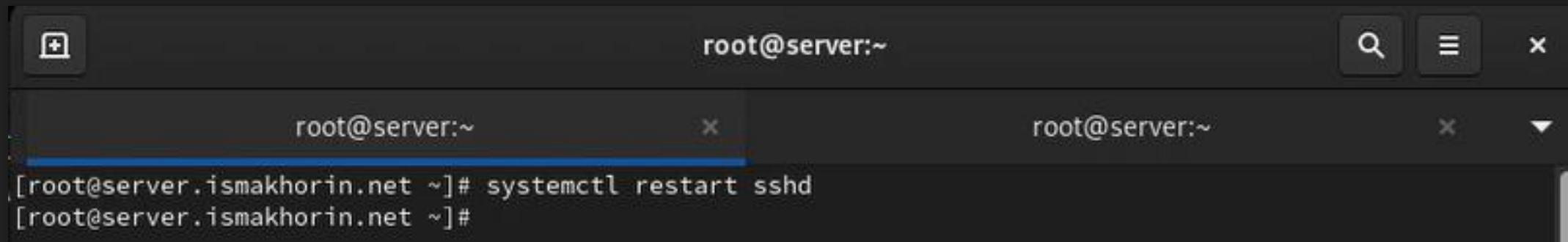
Ограничение списка пользователей для удалённого доступа по SSH



```
*sshd_config  
/etc/ssh  
Save x  
Open +  
79 #GSSAPIAuthentication no  
80 #GSSAPICleanupCredentials yes  
81 #GSSAPIStrictAcceptorCheck yes  
82 #GSSAPIKeyExchange no  
83 #GSSAPIEnablek5users no  
84  
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
```

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

Ограничение списка пользователей для удалённого доступа по SSH

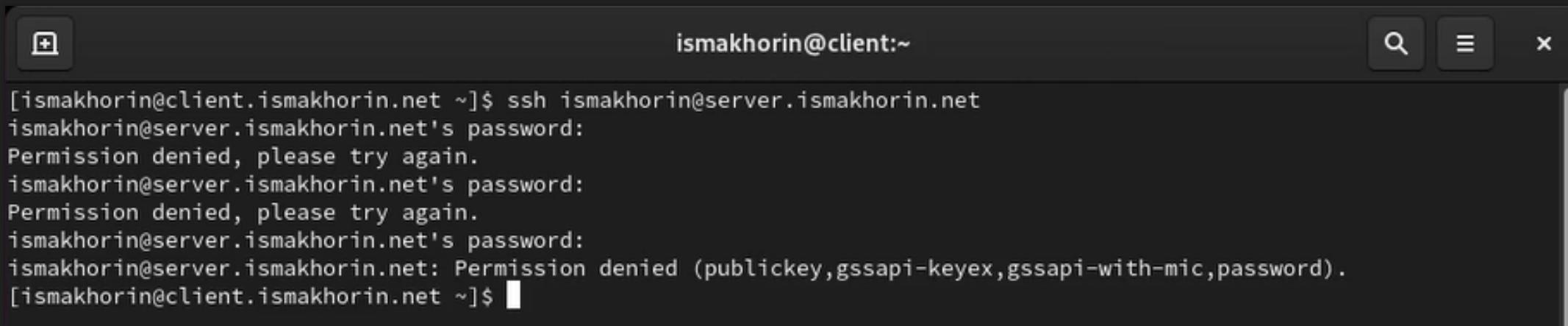


The screenshot shows a terminal window with a dark theme. The title bar says "root@server:~". The window contains two tabs, both labeled "root@server:~". The bottom tab is active and shows the command [root@server.ismakhorin.net ~]# systemctl restart sshd followed by a prompt [root@server.ismakhorin.net ~]#. The top tab is inactive.

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

Рис. 2.3. Перезапуск sshd.

Ограничение списка пользователей для удалённого доступа по SSH

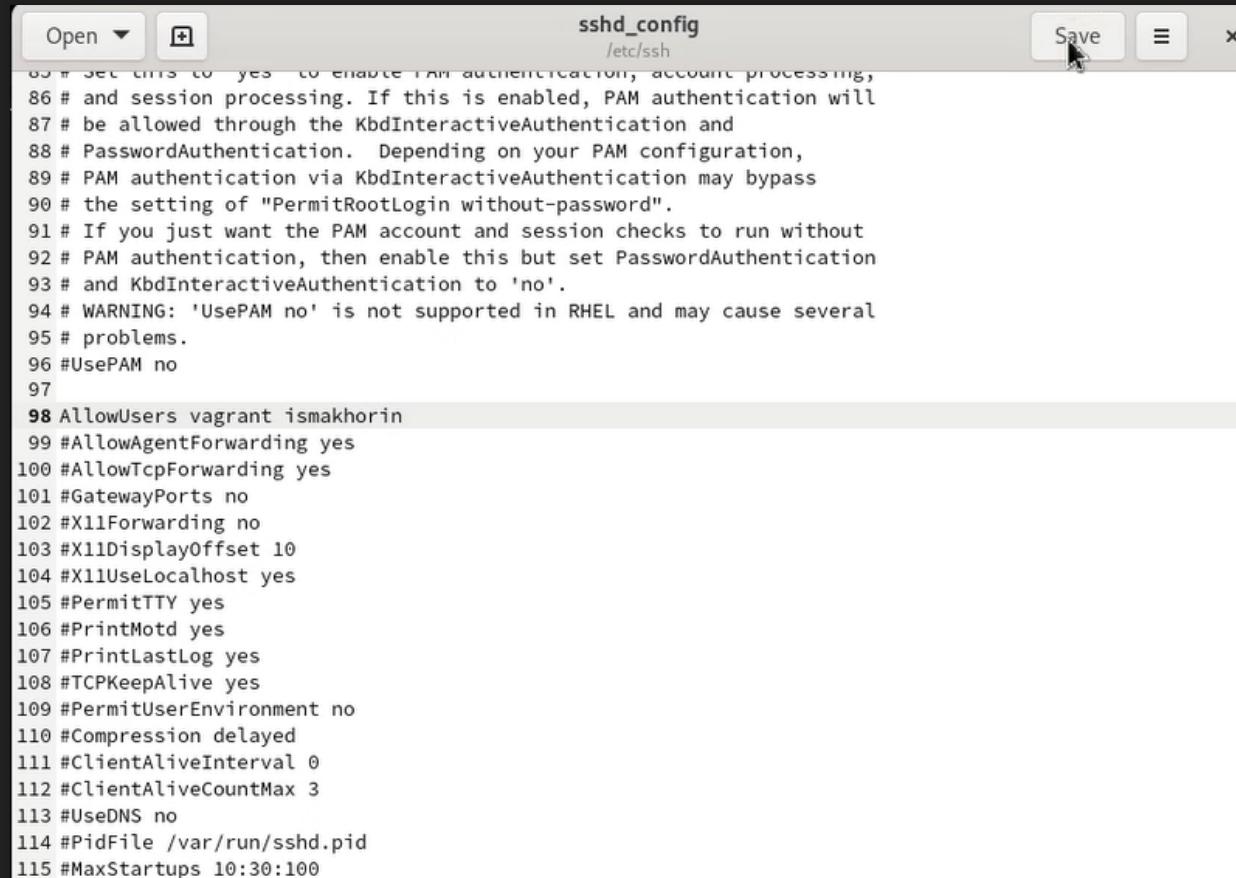


The screenshot shows a terminal window with a dark theme. The title bar reads "ismakhorin@client:~". The main area of the terminal displays the following text:

```
[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.

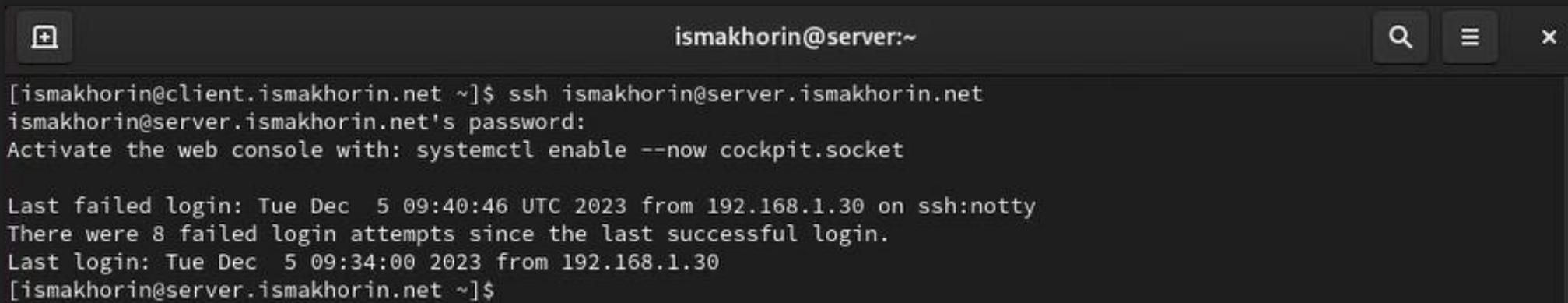
Ограничение списка пользователей для удалённого доступа по SSH



```
Open + sshd_config /etc/ssh Save x
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.

Ограничение списка пользователей для удалённого доступа по SSH



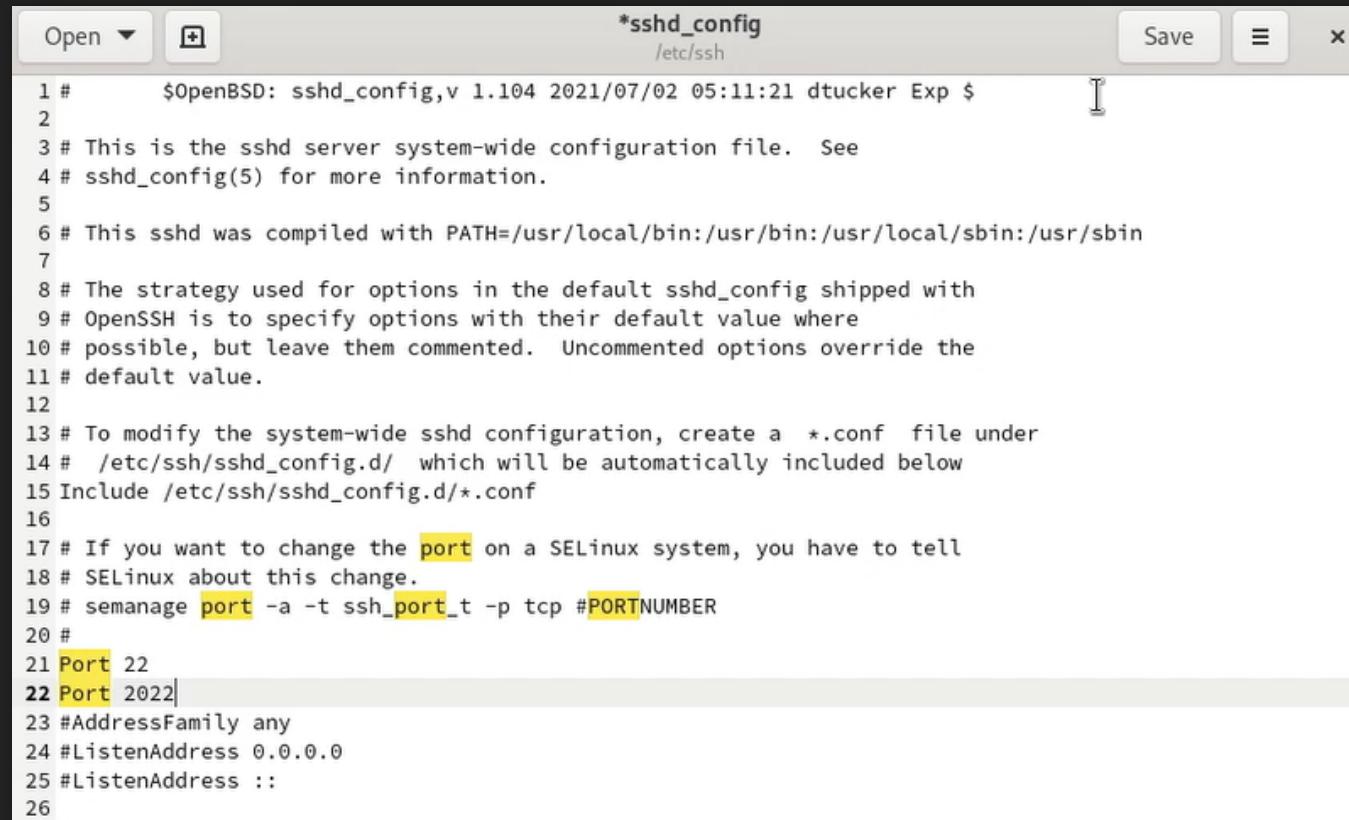
The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "ismakhorin@server:~". The command entered was "ssh ismakhorin@server.ismakhorin.net". The response shows a password prompt and a message about enabling the cockpit web console. It then displays a "Last failed login" message from December 5, 2023, followed by a message about failed login attempts since the last successful one, and finally a "Last login" message from the same date and time.

```
[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.

Настройка дополнительных портов для удалённого доступа по SSH

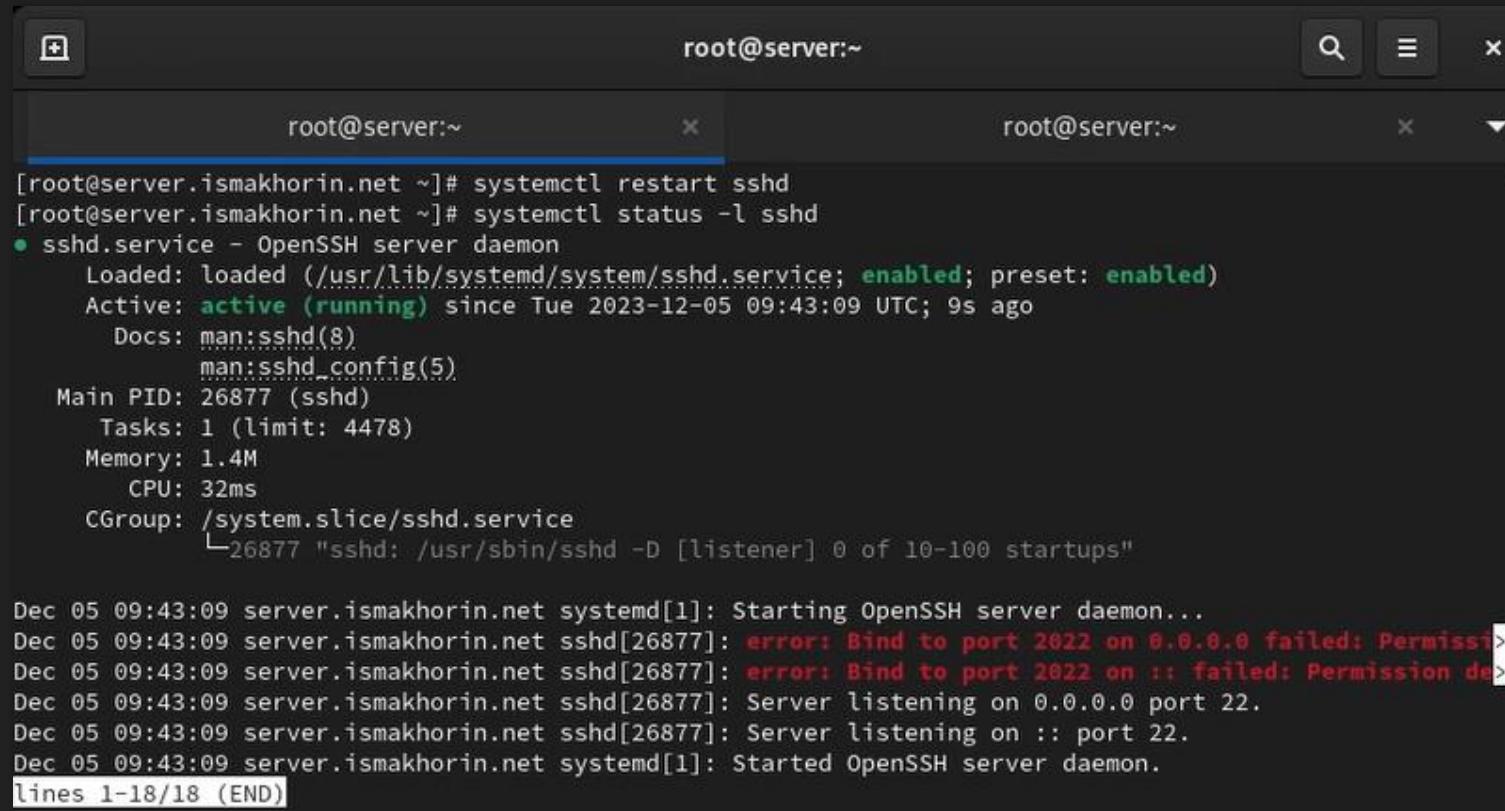


```
*sshd_config
/etc/ssh
Save  x

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 ::
```

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

Настройка дополнительных портов для удалённого доступа по SSH



The screenshot shows a terminal window with two tabs, both titled "root@server:~". The left tab displays the command output:

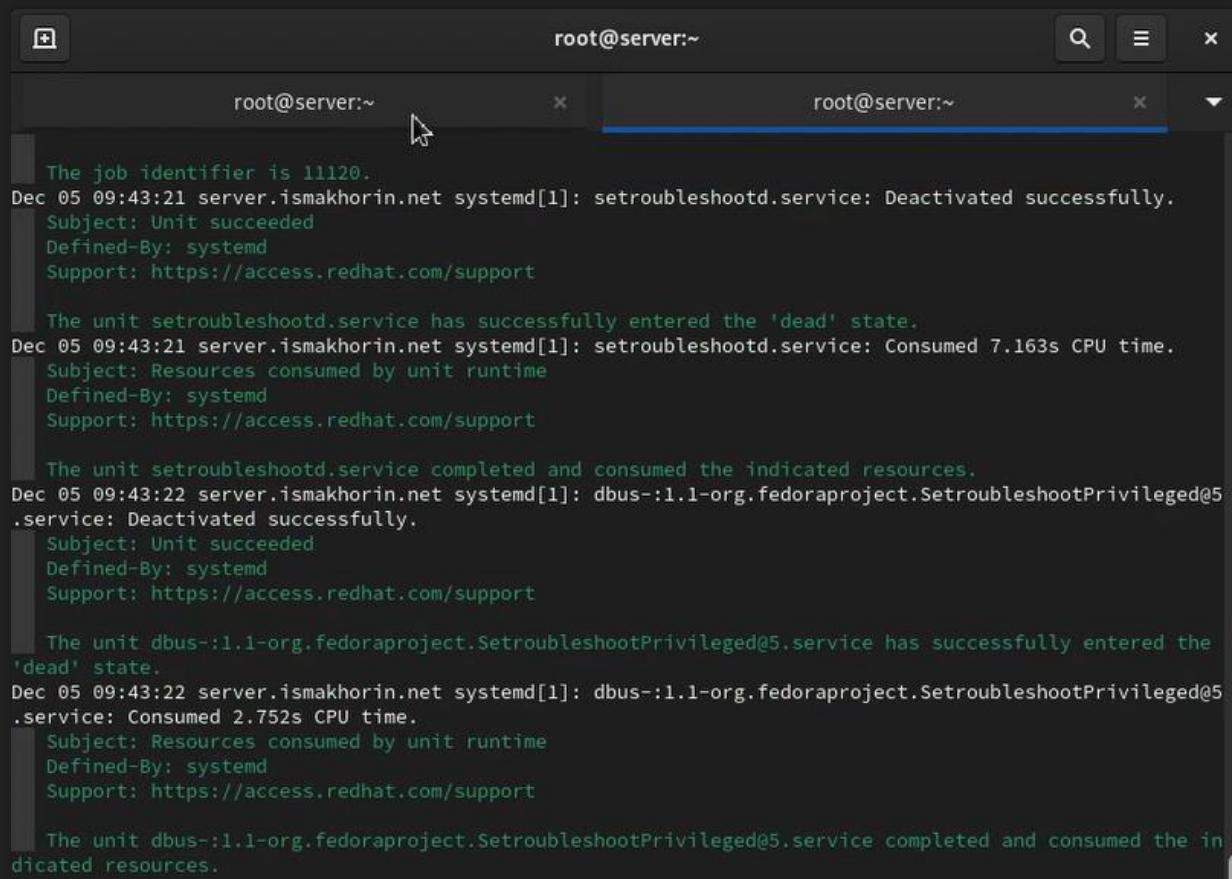
```
[root@server.ismakhordin.net ~]# systemctl restart sshd
[root@server.ismakhordin.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
  Active: active (running) since Tue 2023-12-05 09:43:09 UTC; 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.ismakhordin.net systemd[1]: Starting OpenSSH server daemon...
Dec 05 09:43:09 server.ismakhordin.net sshd[26877]: error: Bind to port 2022 on 0.0.0.0 failed: Permission de>
Dec 05 09:43:09 server.ismakhordin.net sshd[26877]: error: Bind to port 2022 on :: failed: Permission de>
Dec 05 09:43:09 server.ismakhordin.net sshd[26877]: Server listening on 0.0.0.0 port 22.
Dec 05 09:43:09 server.ismakhordin.net sshd[26877]: Server listening on :: port 22.
Dec 05 09:43:09 server.ismakhordin.net systemd[1]: Started OpenSSH server daemon.
```

The right tab shows the command "lines 1-18/18 (END)".

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

Настройка дополнительных портов для удалённого доступа по SSH



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

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

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

The unit dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@5.service has successfully entered the
'dead' state.
Dec 05 09:43:22 server.ismakhorin.net systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@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.SetroubleshootPrivileged@5.service completed and consumed the in
dicated resources.
```

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

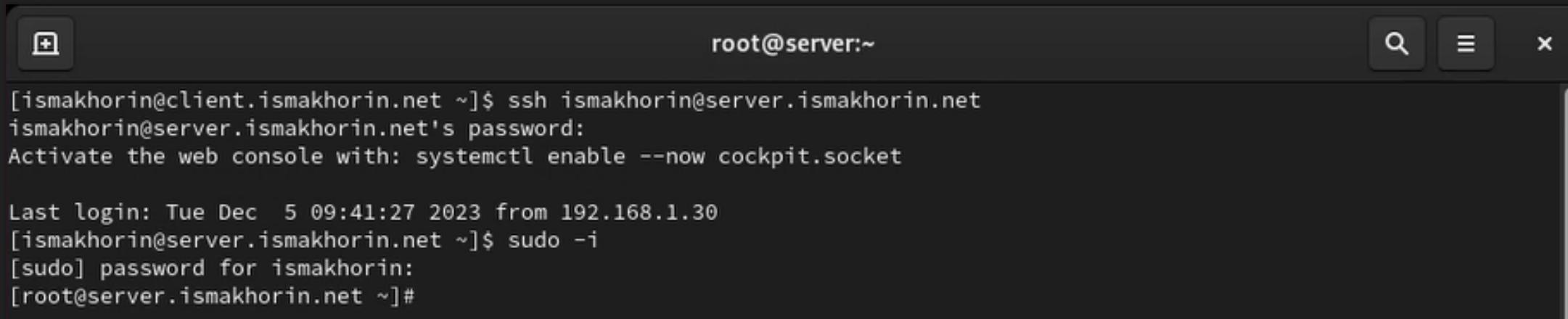
Настройка дополнительных портов для удалённого доступа по SSH

```
[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.

Настройка дополнительных портов для удалённого доступа по SSH

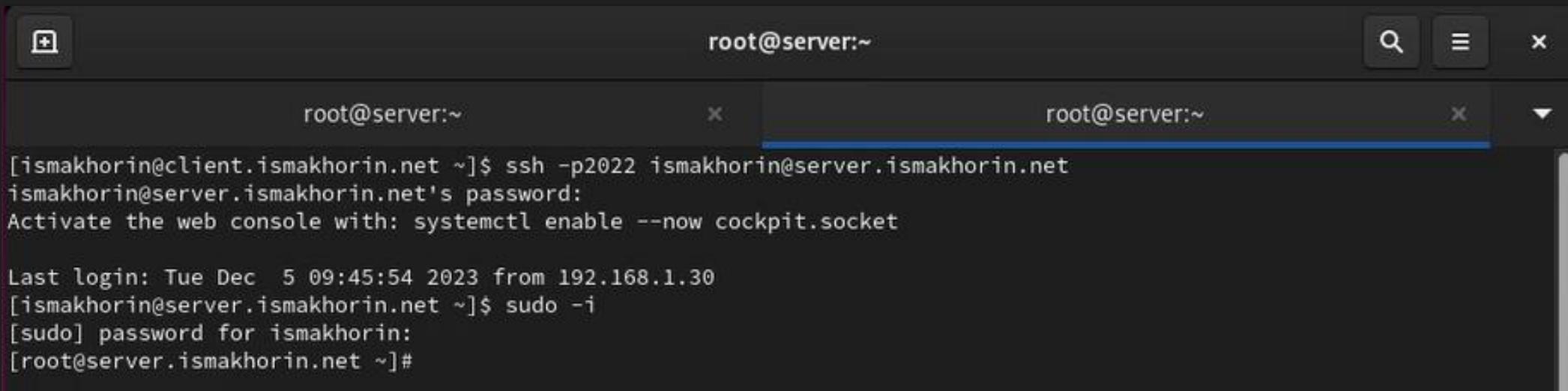


The screenshot shows a terminal window with a dark background and light-colored text. The title bar indicates the session is running as root on a server. The terminal displays the following command-line interaction:

```
[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.

Настройка дополнительных портов для удалённого доступа по SSH



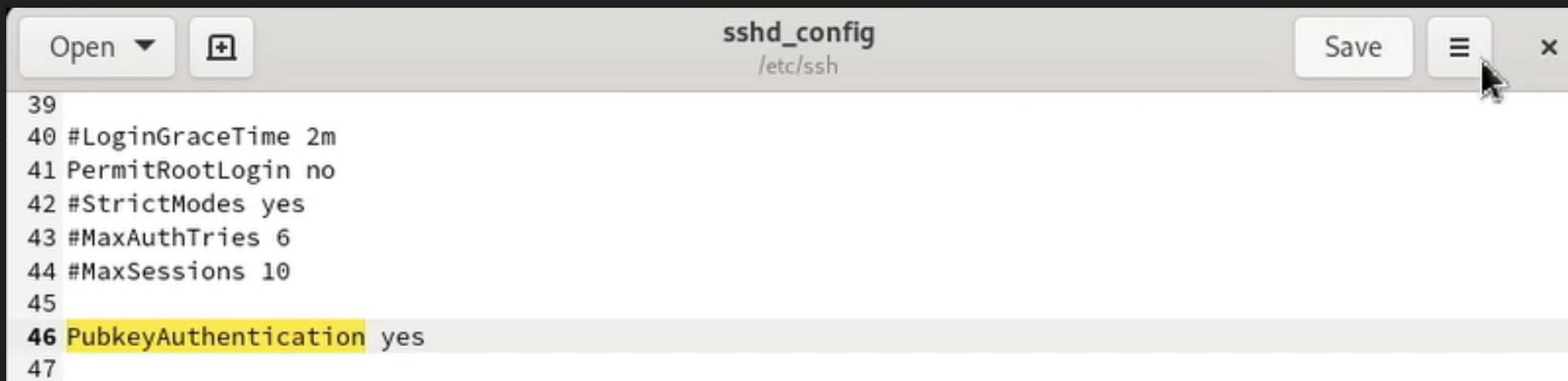
The screenshot shows a terminal window with two tabs. The active tab is titled 'root@server:~' and contains the following text:

```
[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.

Настройка удалённого доступа по SSH по ключу

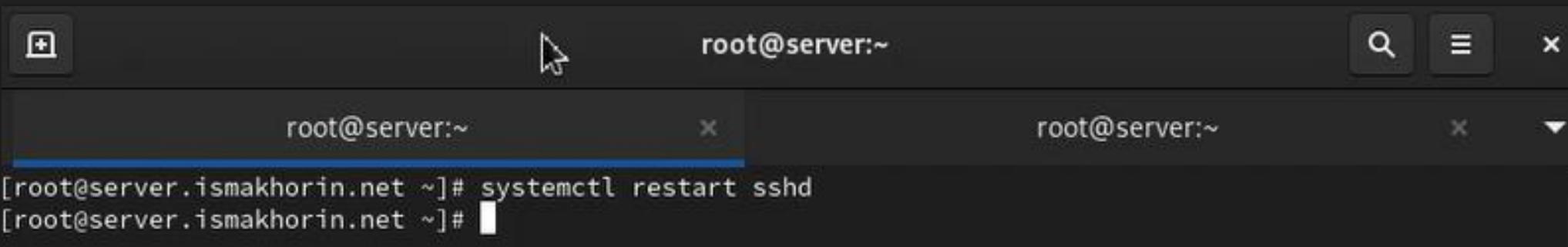


The screenshot shows a terminal window with the title bar "sshd_config /etc/ssh". The file content is displayed in a code editor-like interface. The "PubkeyAuthentication yes" line is highlighted with a yellow background. The terminal window includes standard buttons for "Open", "Save", and "Close".

```
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.

Настройка удалённого доступа по SSH по ключу

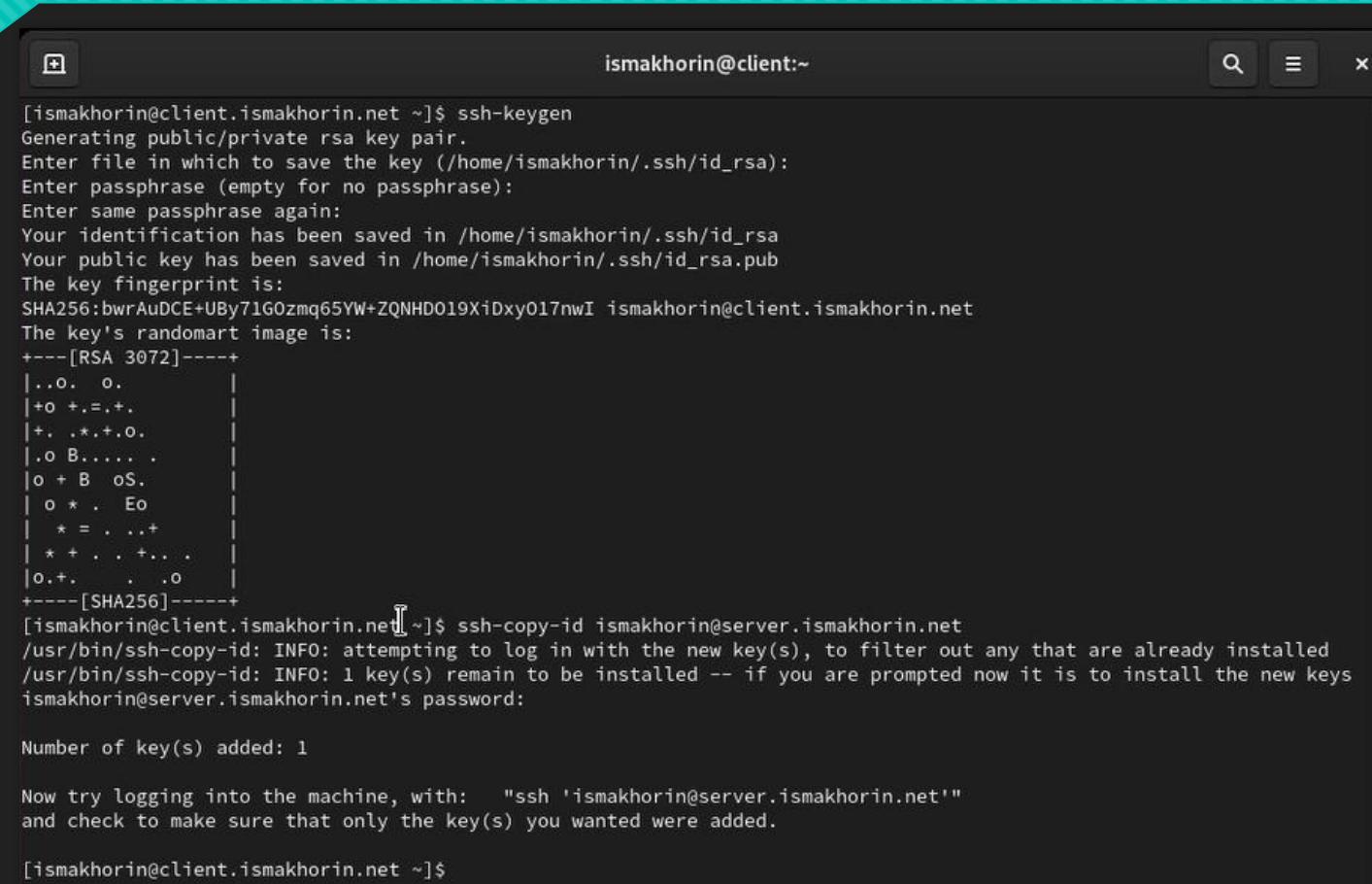


The screenshot shows a terminal window with two tabs open, both titled "root@server:~". The user is running the command `systemctl restart sshd`. The terminal interface includes a header bar with a search icon, a menu icon, and a close button.

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

Рис. 4.2. Перезапуск sshd.

Настройка удалённого доступа по SSH по ключу



```
[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+ZQNHDO19XiDxy017nwI 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.

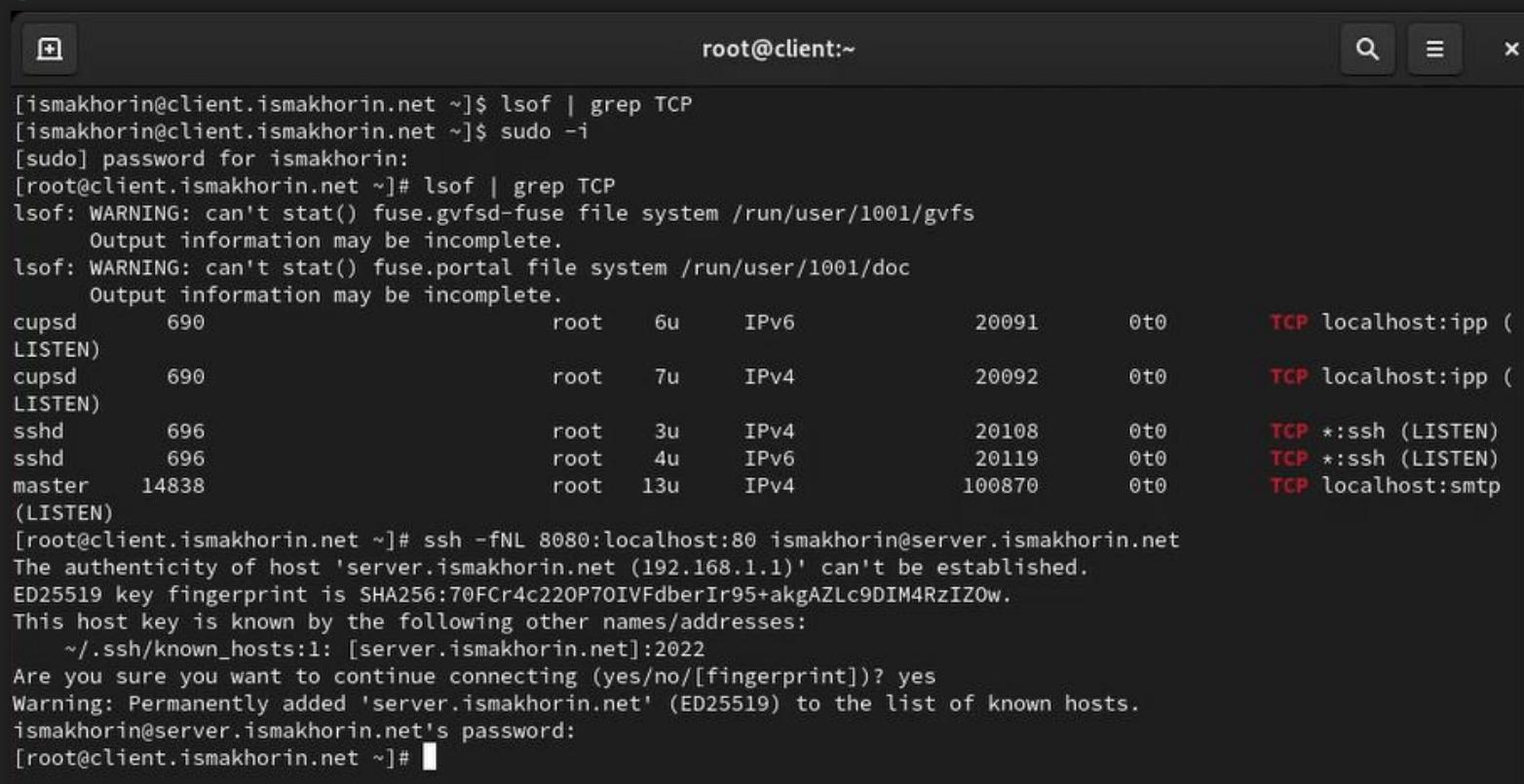
Настройка удалённого доступа по SSH по ключу

```
[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.

Организация туннелей SSH, перенаправление TCP-портов



```
[ismakhорin@client.ismakhорin.net ~]$ lsof | grep TCP
[ismakhорин@client.ismakhорин.net ~]$ sudo -
[sudo] password for ismakhорин:
[root@client.ismakhорин.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.ismakhорин.net ~]# ssh -fNL 8080:localhost:80 ismakhорин@server.ismakhорин.net
The authenticity of host 'server.ismakhорин.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.ismakhорин.net]:22
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.ismakhорин.net' (ED25519) to the list of known hosts.
ismakhорин@server.ismakhорин.net's password:
[root@client.ismakhорин.net ~]#
```

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

Организация туннелей SSH, перенаправление TCP-портов

```
[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.

Организация туннелей SSH, перенаправление TCP-портов

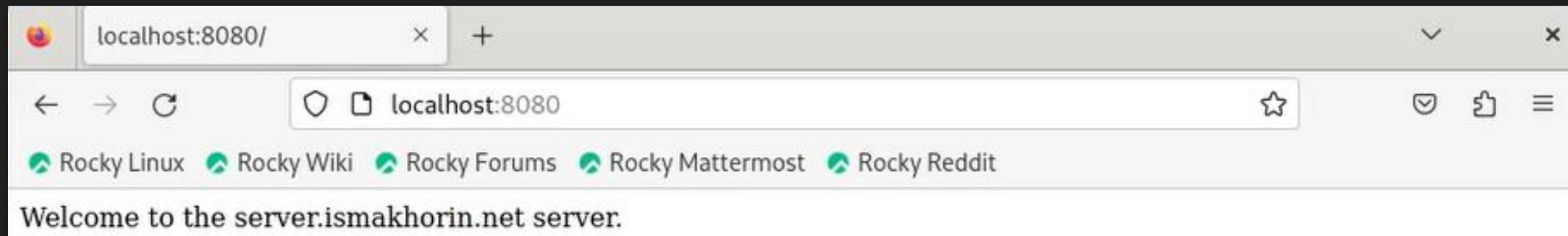
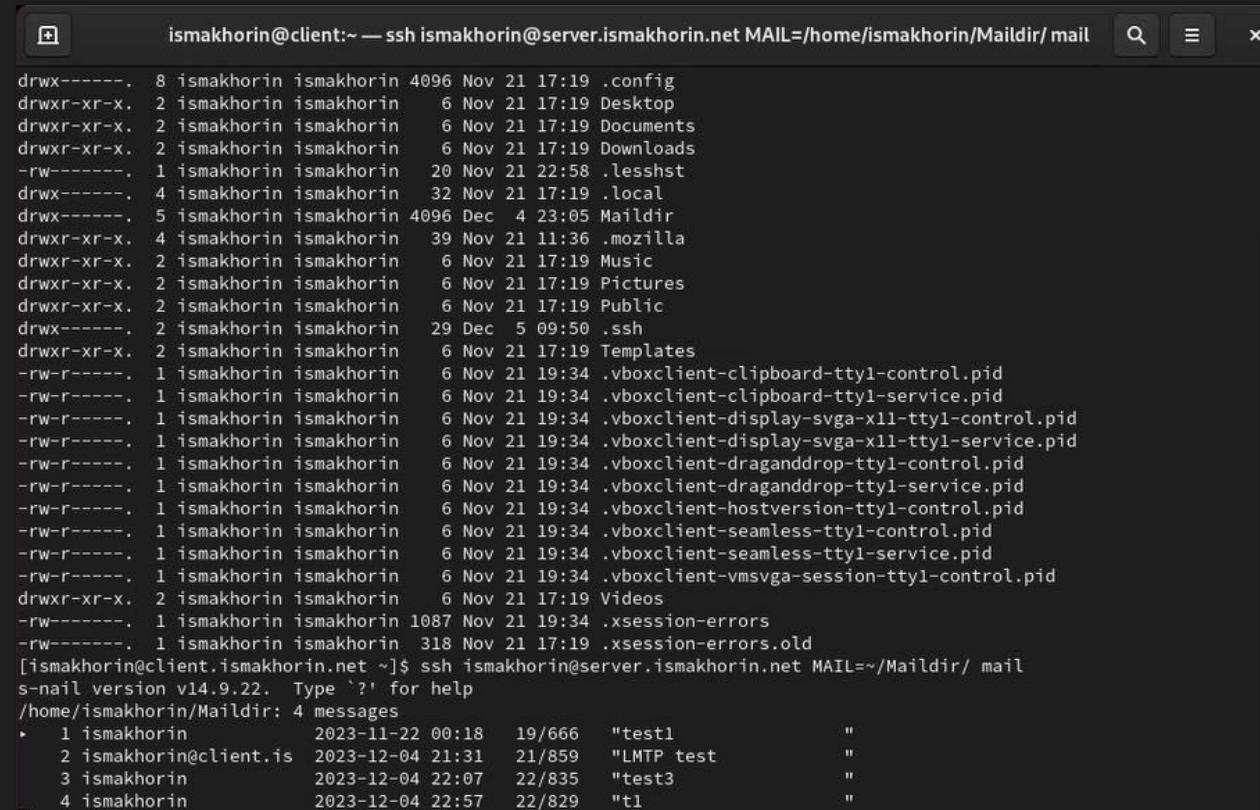


Рис. 5.3. Запуск на клиенте браузера и ввод в адресной строке localhost:8080.

Запуск консольных приложений через SSH

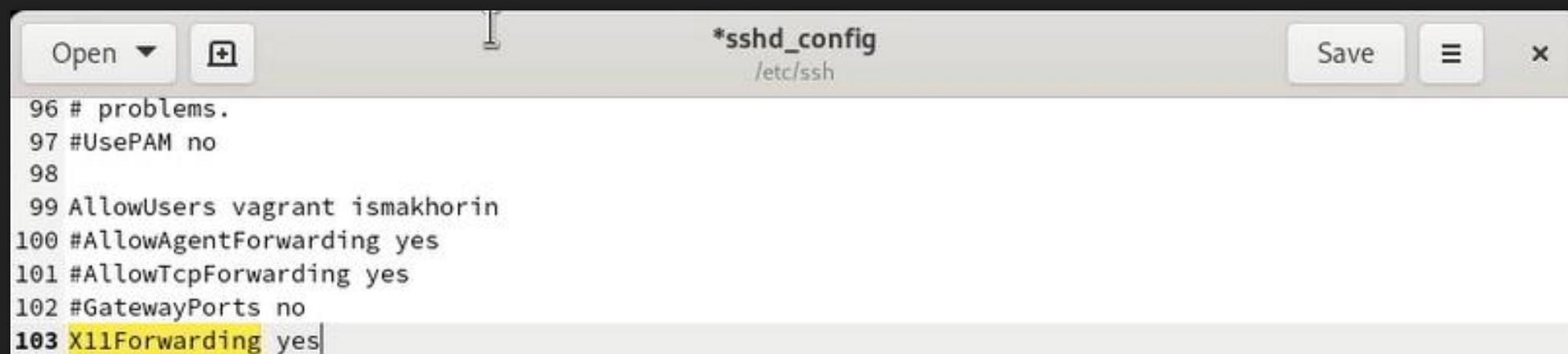


Screenshot of a terminal window titled "ismakhorin@client:~ — ssh ismakhorin@server.ismakhorin.net MAIL=/home/ismakhorin/Maildir/ mail". The window shows a file listing from the server's Maildir directory and a mail retrieval command.

```
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-svga-xll-tty1-control.pid
-rw-r----- 1 ismakhorin ismakhorin 6 Nov 21 19:34 .vboxclient-display-svga-xll-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-vmsvga-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=~/.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.

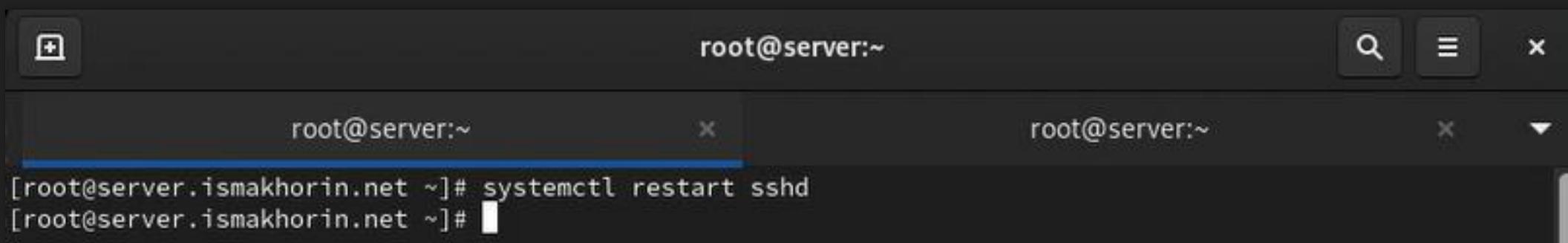
Запуск графических приложений через SSH (X11Forwarding)



```
*sshd_config
/etc/ssh
Open ▾  Save  ⌂  x
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.

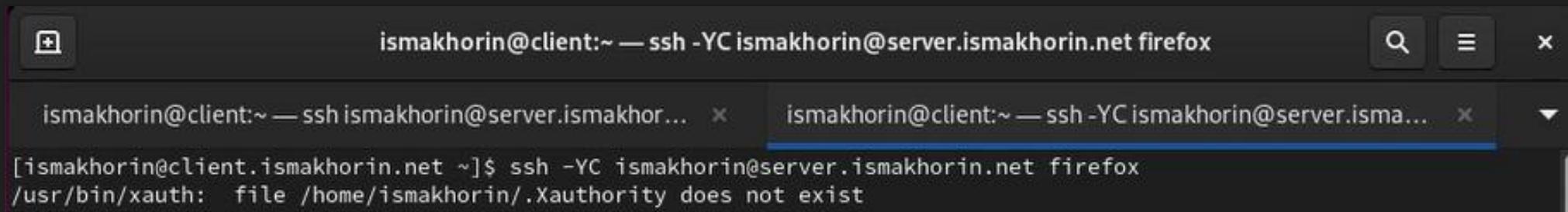
Запуск графических приложений через SSH (X11Forwarding)



The screenshot shows a terminal window with a dark theme. At the top, there is a header bar with a magnifying glass icon, a search field, and a close button. Below the header, there are two tabs: 'root@server:~' and another tab which is partially visible. The main area of the terminal shows the command line interface. The user has run the command `[root@server.ismakhorin.net ~]# systemctl restart sshd`. The terminal is currently in a single-line mode, indicated by the lack of a prompt at the end of the line.

Рис. 7.2. Перезапуск sshd.

Запуск графических приложений через SSH (X11Forwarding)



The screenshot shows a terminal window with two tabs. The top tab has the command `ismakhorin@client:~ — ssh -YC ismakhorin@server.ismakhorin.net firefox`. The bottom tab is active and shows the output of the command: `[ismakhorin@client.ismakhorin.net ~]$ ssh -YC ismakhorin@server.ismakhorin.net firefox` followed by the error message `/usr/bin/xauth: file /home/ismakhorin/.Xauthority does not exist`.

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

Запуск графических приложений через SSH (X11Forwarding)

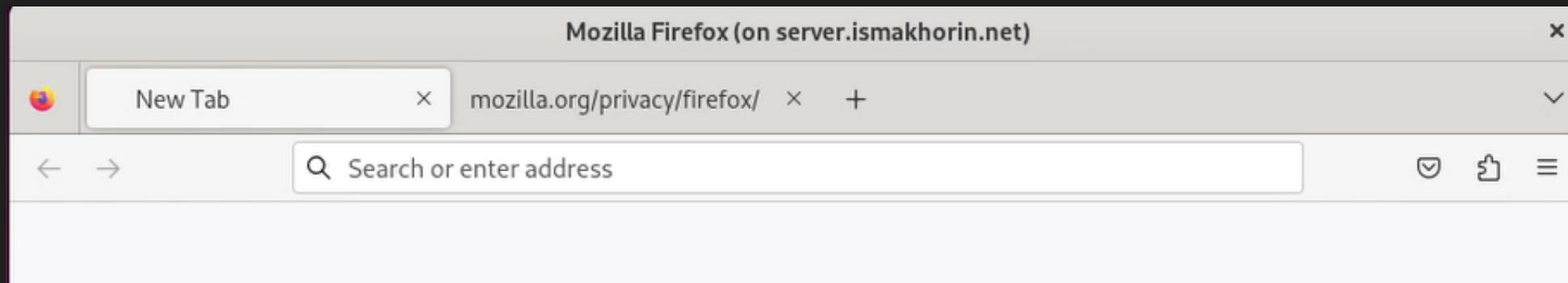
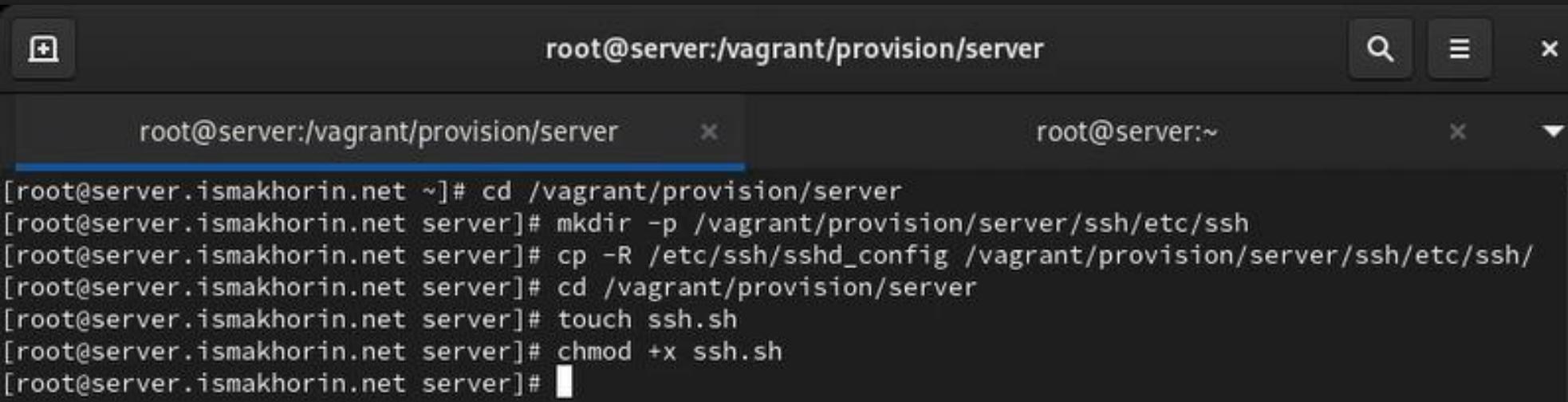


Рис. 7.4. Запуск графического приложения firefox.

Внесение изменений в настройки внутреннего окружения виртуальной машины



The screenshot shows a terminal window with two tabs. The active tab is titled "root@server:/vagrant/provision/server". The command history in this tab shows the following sequence:

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

Внесение изменений в настройки внутреннего окружения виртуальной машины



The screenshot shows a terminal window titled "ssh.sh" with the path "/vagrant/provision/server". The window has standard OS X-style controls (Open, Save, Close) at the top right. The script content is as follows:

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

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

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
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.



Спасибо за внимание!