

Лабораторная работа 11

Генералов Даниил, НПИбд-01-21, 1032202280

2023

¹RUDN University, Moscow, Russian Federation

Задача

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).

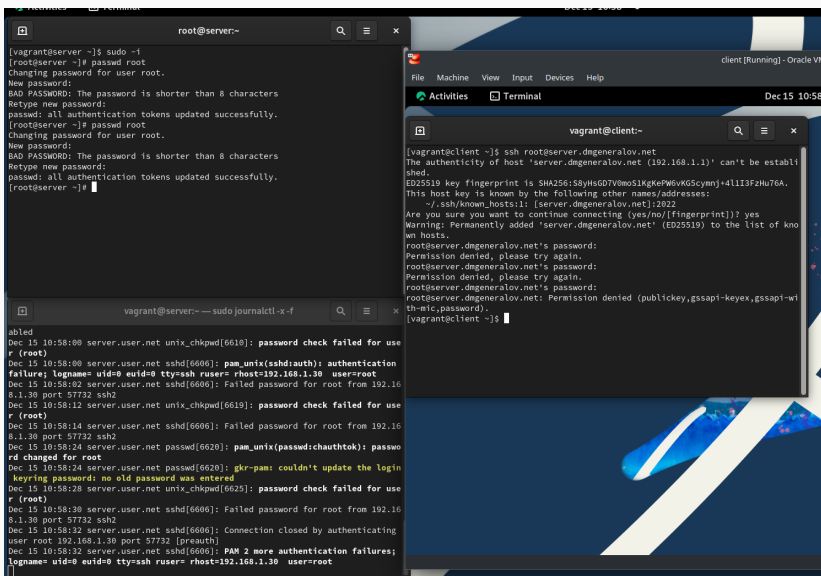
1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере (см. раздел 11.4.6).

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере (см. раздел 11.4.6).
7. Используя удалённое SSH-соединение, запустите с клиента

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере (см. раздел 11.4.6).
7. Используя удалённое SSH-соединение, запустите с клиента

Выполнение



```

root@server:~
[vagrant@server ~]$ sudo -i
[root@server ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]#

vagrant@server:~ — sudo journalctl -x -f
Dec 15 10:58:00 server.user.net unix_chkpwd[6610]: password check failed for use
r (root)
Dec 15 10:58:00 server.user.net sshd[6606]: pam_unix(sshd:auth): authentication
failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root
Dec 15 10:58:02 server.user.net sshd[6606]: Failed password for root from 192.16
8.1.30 port 57732 ssh2
Dec 15 10:58:12 server.user.net unix_chkpwd[6619]: password check failed for use
r (root)
Dec 15 10:58:14 server.user.net sshd[6606]: Failed password for root from 192.16
8.1.30 port 57732 ssh2
Dec 15 10:58:24 server.user.net passwd[6620]: pam_unix(passwd:chauthtok): passwo
rd changed for root
Dec 15 10:58:24 server.user.net passwd[6620]: gkr-pam: couldn't update the login
keyring password: no old password was entered
Dec 15 10:58:28 server.user.net unix_chkpwd[6625]: password check failed for use
r (root)
Dec 15 10:58:30 server.user.net sshd[6606]: Failed password for root from 192.16
8.1.30 port 57732 ssh2
Dec 15 10:58:32 server.user.net sshd[6606]: Connection closed by authenticating
user root 192.168.1.30 port 57732 [preauth]
Dec 15 10:58:32 server.user.net sshd[6606]: PAM 2 more authentication failures;
logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root

```

```

vagrant@client:~
[vagrant@client ~]$ ssh root@server.dmgeneralov.net
The authenticity of host 'server.dmgeneralov.net (192.168.1.1)' can't be establ
ished.
ED25519 key fingerprint is SHA256:S8yHsGD7V0moS1KgKePW6vK6GScymnj+4lI3FzHu76A.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:1: [server.dmgeneralov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.dmgeneralov.net' (ED25519) to the list of kno
wn hosts.
root@server.dmgeneralov.net's password:
Permission denied, please try again.
root@server.dmgeneralov.net's password:
Permission denied, please try again.
root@server.dmgeneralov.net's password:
root@server.dmgeneralov.net: Permission denied (publickey,gssapi-keyex,gssapi-wi
th-mic,password).
[vagrant@client ~]$

```

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes
```

Рис. 2: ssh

The image displays three terminal windows illustrating the process of setting up and testing SSH access.

Top Left Window (root@server): Shows the configuration of the root user's password and the SSH daemon.

```
[vagrant@server ~]$ sudo -i
[root@server ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]# nano /etc/ssh/sshd_config
[root@server ~]# systemctl restart sshd
[root@server ~]#
```

Top Right Window (vagrant@client): Shows an attempt to connect to the server via SSH.

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

Bottom Window (vagrant@server): Shows the system logs for the SSH daemon, indicating failed password attempts.

```
vagrant@server:~$ sudo journalctl -x -f

Dec 15 11:01:49 server.user.net sshd[6684]: main: sshd: ssh-rsa algorithm is dis
abled
Dec 15 11:01:52 server.user.net unix_chkpwd[6686]: password check failed for use
r (root)
Dec 15 11:01:52 server.user.net sshd[6684]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root
Dec 15 11:01:54 server.user.net sshd[6684]: Failed password for root from 192.16
8.1.30 port 38350 ssh2
Dec 15 11:01:56 server.user.net unix_chkpwd[6687]: password check failed for use
r (root)
Dec 15 11:01:58 server.user.net sshd[6684]: Failed password for root from 192.16
8.1.30 port 38350 ssh2
Dec 15 11:02:02 server.user.net unix_chkpwd[6690]: password check failed for use
r (root)
Dec 15 11:02:04 server.user.net sshd[6684]: Failed password for root from 192.16
8.1.30 port 38350 ssh2
Dec 15 11:02:04 server.user.net sshd[6684]: Connection closed by authenticating
user root 192.168.1.30 port 38350 [preauth]
Dec 15 11:02:04 server.user.net sshd[6684]: PAM 2 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30 user=root
```

```
The user manager instance for user 1002 has been started. All services queued
for starting have been started. Note that other services might still be start
ing
up or be started at any later time.

Startup of the manager took 371867 microseconds.
Dec 15 11:06:37 server.user.net systemd[1]: Started User Manager for UID 1002.
Subject: A start job for unit user@1002.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit user@1002.service has finished successfully.

The job identifier is 2522.
Dec 15 11:06:37 server.user.net systemd[1]: Started Session 6 of User dmgeneral
v.
Subject: A start job for unit session-6.scope has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit session-6.scope has finished successfully.

The job identifier is 2600.
Dec 15 11:06:37 server.user.net sshd[6740]: pam_unix(sshd:session): session open
ed for user dmgeneralov(uid=1002) by (uid=0)
Dec 15 11:06:37 server.user.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 2679.
Dec 15 11:06:37 server.user.net systemd[1]: Started Hostname Service.
Subject: A start job for unit systemd-hostnamed.service has finished successf
ul.
```

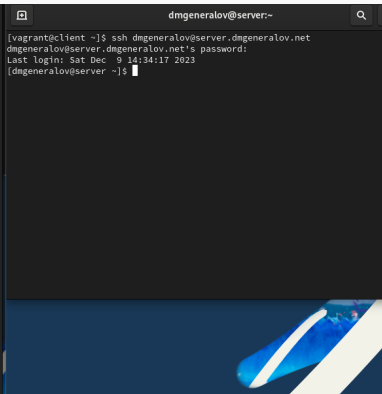


Рис. 4: ssh

The screenshot displays a Linux desktop with three terminal windows open.

Top-Left Terminal (root@server): Editing the `/etc/ssh/sshd_config` file with nano. The configuration includes logging settings, authentication options, and a list of allowed users.

```

GNU nano 5.6.1 /etc/ssh/sshd_config
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

AllowUsers vagrant

#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

[ Wrote 133 lines ]
[ Help | Write Out | Where Is | Cut | Execute | Exit | Read File | Replace | Paste | Justify ]

```

Top-Right Terminal (root@server): Executing commands to restart the sshd service.

```

[vagrant@server ~]$ sudo -i
[root@server ~]# systemctl restart sshd
[root@server ~]#

```

Bottom Terminal (vagrant@server): Running `sudo journalctl -x -f` to view the sshd service logs.

```

The unit system-hostnamed.service has successfully entered the 'dead' state.
Dec 15 11:11:55 server.user.net sudo[6591]: pam_unix(sudo:session): session closed for user root
Dec 15 11:11:57 server.user.net sudo[6974]: vagrant : TTY=pts/1 ; PWD=/home/vagrant ; USER=root ; COMMAND=/bin/journalctl -x -f
Dec 15 11:11:57 server.user.net sudo[6974]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)

Dec 15 11:12:01 server.user.net sshd[6948]: Failed password for invalid user dmgeneralov from 192.168.1.30 port 36754 ssh2
Dec 15 11:12:02 server.user.net sshd[6948]: Failed password for invalid user dmgeneralov from 192.168.1.30 port 36754 ssh2
Dec 15 11:12:02 server.user.net sshd[6948]: Connection closed by invalid user dmgeneralov 192.168.1.30 port 36754 [preauth]
Dec 15 11:12:04 server.user.net sshd[6981]: main: sshd: ssh-rsa algorithm is disabled
Dec 15 11:12:04 server.user.net sshd[6981]: User dmgeneralov from 192.168.1.30 not allowed because not listed in AllowUsers

```

Bottom-Right Terminal (vagrant@client): Attempting to connect to `dmgeneralov@server.dmgeneralov.net` via ssh.

```

[vagrant@client ~]$ ssh dmgeneralov@server.dmgeneralov.net
dmgeneralov@server.dmgeneralov.net's password:
Last login: Sat Dec 9 14:34:17 2023
[dmgeneralov@server ~]$
logout
Connection to server.dmgeneralov.net closed.
[vagrant@client ~]$ ssh dmgeneralov@server.dmgeneralov.net
dmgeneralov@server.dmgeneralov.net's password:
Permission denied, please try again.
dmgeneralov@server.dmgeneralov.net's password:
dmgeneralov@server.dmgeneralov.net's password:
dmgeneralov@server.dmgeneralov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[vagrant@client ~]$ ssh dmgeneralov@server.dmgeneralov.net
dmgeneralov@server.dmgeneralov.net's password:

```



```

root@server:~
GNU nano 3.6.1 /etc/ssh/sshd_config
# 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
#RekeyInterval default none

# Logging

[Help] [Write Out] [Where Is] [Cut] [Execute]
[Exit] [Read File] [Replace] [Paste] [Justify]

vagrant@server:~
[vagrant@server ~]$ firewall-cmd --add-port=2022/tcp
Authorization failed.
Make sure polkit agent is running or run the application as superuser.
[vagrant@server ~]$ sudo firewall-cmd --add-port=2022/tcp
success
[vagrant@server ~]$ sudo firewall-cmd --runtime-to-permanent
success
[vagrant@server ~]$ systemctl restart sshd
Failed to restart sshd.service: Access denied
See system logs and 'systemctl status sshd.service' for details.
[vagrant@server ~]$ sudo systemctl restart sshd
[vagrant@server ~]$

root@server:~
• sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
Active: active (running) since Fri 2023-12-15 11:16:18 UTC; 12s ago
Docs: man:sshd(8)
      man:sshd_config(5)
Main PID: 7151 (sshd)
Tasks: 1 (Limit: 5722)
Memory: 1.5M
CPU: 17ms
CGroup: /system.slice/ssh.service
└─7151 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 15 11:16:18 server.user.net systemd[1]: Starting OpenSSH server daemon...
Dec 15 11:16:18 server.user.net sshd[7151]: main: sshd: ssh-rsa algorithm is disabled
Dec 15 11:16:18 server.user.net sshd[7151]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied
Dec 15 11:16:18 server.user.net sshd[7151]: error: Bind to port 2022 on *: failed: Permission denied
Dec 15 11:16:18 server.user.net sshd[7151]: Server listening on 0.0.0.0 port 22.
Dec 15 11:16:18 server.user.net sshd[7151]: Server listening on *: port 22.
Dec 15 11:16:18 server.user.net systemd[1]: Started OpenSSH server daemon.

```

Рис. 6: ssh

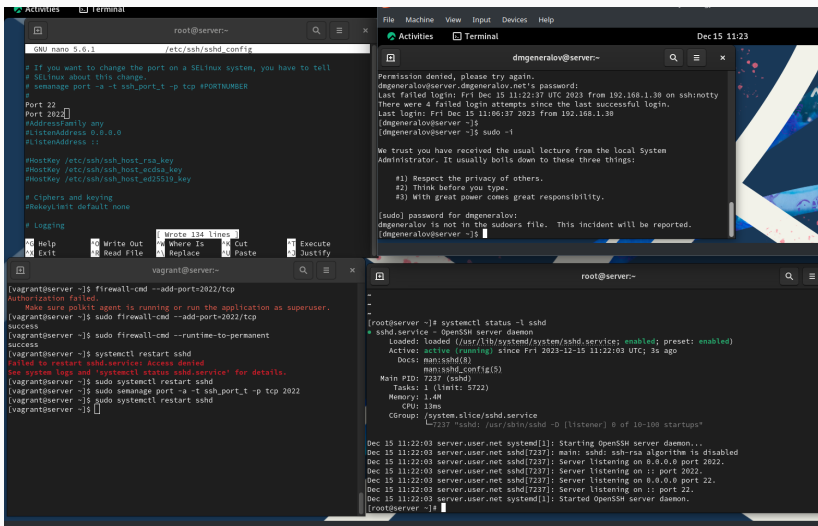


Рис. 7: ssh

```

[dmgeneralov@client ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dmgeneralov/.ssh/id_rsa):
Created directory '/home/dmgeneralov/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dmgeneralov/.ssh/id_rsa
Your public key has been saved in /home/dmgeneralov/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:k/sG4wb+s6iew5dNzFF5/CbEW7LAs/FGvQTSNgy8uA dmgeneralov@client.user.net
The key's randomart image is:
+----[RSA 3072]-----+
|      .0+o      |
|      o @oX +   |
|      . = % B .  |
|      E.o * +   |
|      oS. . o   |
|      . +o      |
|      . . *.o   |
|      o.+.=.    |
|      .++..oo+. |
+----[SHA256]-----+
[dmgeneralov@client ~]$ ssh-copy-id server.dmgeneralov.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/dmgeneralov/.ssh/id_rsa.pub"
The authenticity of host 'server.dmgeneralov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:S8yHsGD7V0moS1KgKePW6vKG5cymnj+4lI13FzHu76A.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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
dmgeneralov@server.dmgeneralov.net's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'server.dmgeneralov.net'"
and check to make sure that only the key(s) you wanted were added.

[dmgeneralov@client ~]$ ssh server.dmgeneralov.net
Last login: Fri Dec 15 11:24:01 2023 from 192.168.1.1
[dmgeneralov@server ~]$ sudo -i
[sudo] password for dmgeneralov:
dmgeneralov is not in the sudoers file. This incident will be reported.
[dmgeneralov@server ~]$

```

```
[dmgeneralov@client ~]$ lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
[dmgeneralov@client ~]$ ssh -fNL 8080:localhost:80 server.dmgeneralov.net
[dmgeneralov@client ~]$ lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
ssh      7333      dmgeneralov    3u  IPv4  47805      0t0  TCP client.user.net:58700->server.dmgeneralov.net:ssh (ESTABLISHED)
ssh      7333      dmgeneralov    4u  IPv6  47822      0t0  TCP localhost:webcache (LISTEN)
ssh      7333      dmgeneralov    5u  IPv4  47823      0t0  TCP localhost:webcache (LISTEN)
[dmgeneralov@client ~]$ curl localhost:8080
Welcome to the server.dmgeneralov.net server.
[dmgeneralov@client ~]$
```

Рис. 9: ssh

```
[dmgeneralov@client vagrant]$ ssh server.dmgeneralov.net hostname
server.user.net
[dmgeneralov@client vagrant]$ ssh server.dmgeneralov.net ls -Al
total 20
-rw-----. 1 dmgeneralov dmgeneralov 254 Dec 15 11:37 .bash_history
-rw-r--r--. 1 dmgeneralov dmgeneralov 18 Jan 23 2023 .bash_logout
-rw-r--r--. 1 dmgeneralov dmgeneralov 141 Jan 23 2023 .bash_profile
-rw-r--r--. 1 dmgeneralov dmgeneralov 492 Jan 23 2023 .bashrc
drwx-----. 2 dmgeneralov dmgeneralov 6 Dec 7 13:18 .cache
drwx-----. 5 dmgeneralov dmgeneralov 4096 Dec 15 10:51 Maildir
drwxr-xr-x. 4 dmgeneralov dmgeneralov 39 Nov 9 15:51 .mozilla
drwx-----. 2 dmgeneralov dmgeneralov 103 Dec 15 11:23 .ssh
[dmgeneralov@client vagrant]$ ssh server.dmgeneralov.net MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/dmgeneralov/.Maildir: 4 messages 1 new
  1 Dmgeneralov      2023-12-07 13:33   18/689   "Test 1"
  2 alice@example.com 2023-12-07 14:03   14/575   "An exciting investment"
  A 3 root           2023-12-09 14:34   18/616   "LMTP test"
  N 4 Mail Delivery System 2023-12-15 10:46  88/3024 "Undelivered Mail Retu"
2
s-nail: The empty (default) command is ignored here, but has arguments: 2
p 2
[-- Message 2 -- 14 lines, 575 bytes --]:
From: alice@example.com
To: dmgeneralov@dmgeneralov.net
Subject: An exciting investment opportunity for you!
Message-Id: <20231207140313.4FB3247401F@server.dmgeneralov.net>
Date: Thu, 7 Dec 2023 14:03:03 +0000 (UTC)

Spam spam spam, lovely spam...
```

The screenshot shows a terminal window with the following commands and output:

```

[dmgeneralov@client vagrant]$ ssh -YC server.dmgeneralov.net xterm
bash: xterm: command not found
[dmgeneralov@client vagrant]$ ssh -YC server.dmgeneralov.net gnome-
gnome-calculator          gnome-extensions          gnome-keyring-daemon      gnome-session-inhibit     gnome-shell-exter
gnome-characters           gnome-font-viewer         gnome-logs                gnome-session-quit        gnome-shell-perf
gnome-control-center       gnome-help                gnome-screenshot          gnome-session-selector    gnome-software
gnome-disk-image-mounter   gnome-keyring             gnome-session             gnome-shell                gnome-system-mon
gnome-disks                gnome-keyring-3           gnome-session-custom-session gnome-shell-extension-prefs gnome-terminal
[dmgeneralov@client vagrant]$ ssh -YC server.dmgeneralov.net gnome-terminal
# Error creating terminal: Could not activate remote peer.

```

Below the terminal window, a "Processes" window is open, displaying a table of running processes:

Process Name	User	% CPU	ID	Memory	Disk read tota	Disk writ
master	root	0.00	1120	34.2 kB	N/A	N/A
mcelog	root	0.00	569	41.0 kB	N/A	N/A
md	root	0.00	37	N/A	N/A	N/A
migration/0	root	0.00	18	N/A	N/A	N/A
mld	root	0.00	52	N/A	N/A	N/A
mm_percpu_wq	root	0.00	11	N/A	N/A	N/A
ModemManager	root	0.00	623	352.3 kB	N/A	N/A
named	named	0.00	864	3.6 MB	N/A	N/A
nano	root	0.00	6864	733.2 kB	N/A	N/A
netns	root	0.00	6	N/A	N/A	N/A
NetworkManager	root	0.00	4239	1.4 MB	N/A	N/A
oom_reaper	root	0.00	27	N/A	N/A	N/A
packagekitd	root	0.00	5904	74.3 MB	N/A	N/A
php-fpm.conf)	root	0.00	793	155.6 kB	N/A	N/A
php-fpm: pool www	apache	0.00	884	69.6 kB	N/A	N/A

At the bottom of the Processes window, there is an "End Process" button and a search icon.

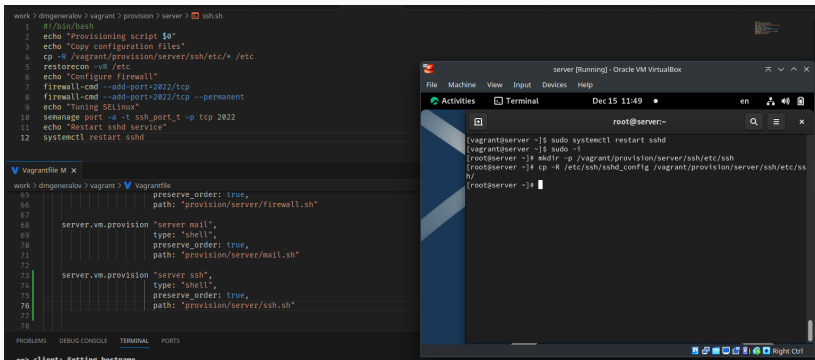


Рис. 12: vagrant

Я получил опыт настройки SSH-сервера.