

Отчет по лабораторной работе 11

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	17
5	Контрольные вопросы	18

Список иллюстраций

3.1	ssh	7
3.2	ssh	8
3.3	ssh	8
3.4	ssh	9
3.5	ssh	10
3.6	ssh	11
3.7	ssh	12
3.8	ssh	13
3.9	ssh	14
3.10	ssh	14
3.11	ssh	15
3.12	vagrant	16

Список таблиц

1 Цель работы

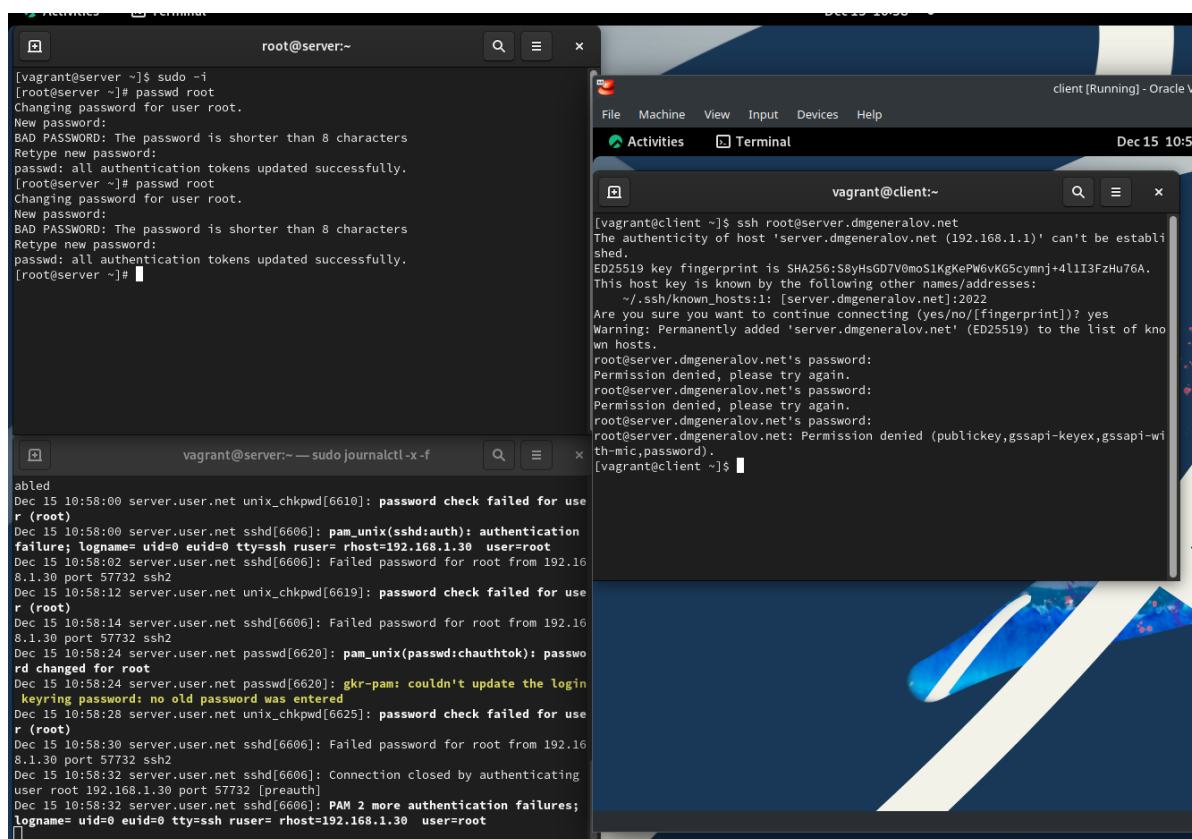
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2 Задание

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 графическое приложение на сервере (см. раздел 11.4.7).
8. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile (см. раздел 11.4.8).

3 Выполнение лабораторной работы

Сначала мы попробовали подключиться к root-аккаунту на сервере, но, несмотря на то, что пароль правильный, сервер не разрешил это сделать.



```
[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@client ~]$ ssh root@server.dmgeneralov.net
The authenticity of host 'server.dmgeneralov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:S8YHsGD7V0moS1KgKePW6vKG5cymnj+4l1I3FzHu76A.
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 known 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-with-mic,password).
[vagrant@client ~]$
```

```
vagrant@server:~$ sudo journalctl -x -f
ailed
Dec 15 10:58:00 server.user.net unix_chkpwd[6610]: password check failed for user 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 192.168.1.30 port 57732 ssh2
Dec 15 10:58:12 server.user.net unix_chkpwd[6619]: password check failed for user r (root)
Dec 15 10:58:14 server.user.net sshd[6606]: Failed password for root from 192.168.1.30 port 57732 ssh2
Dec 15 10:58:24 server.user.net passwd[6620]: pam_unix(passwd:chautok): password 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 user r (root)
Dec 15 10:58:30 server.user.net sshd[6606]: Failed password for root from 192.168.1.30 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
```

Рис. 3.1: ssh

Это потому, что по умолчанию SSH настроен, чтобы запрещать вход для root по паролю, но он все равно возможен по ключу. Мы отключаем это.

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

Рис. 3.2: ssh

Ошибка выглядит таким же образом.

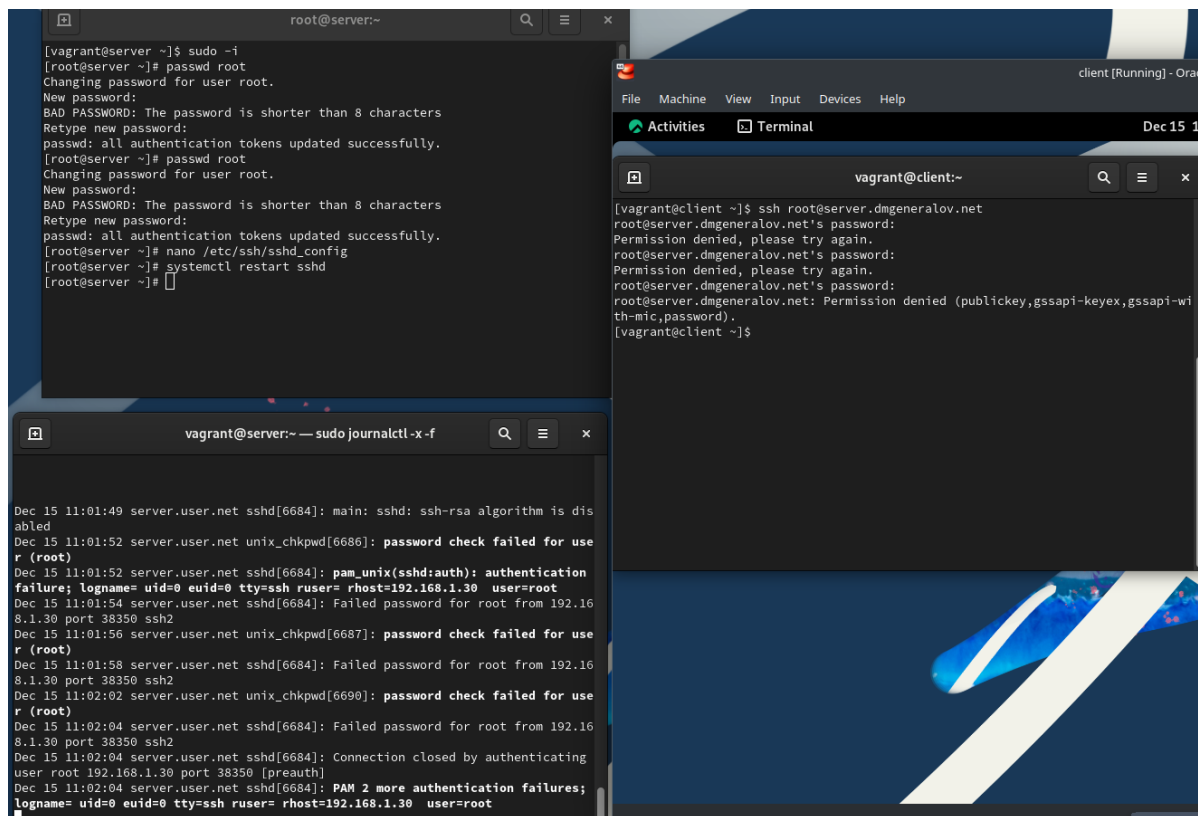


Рис. 3.3: ssh

Однако подключаться от имени пользователя `dmgeneralov` можно, и открывается терминал этого пользователя.

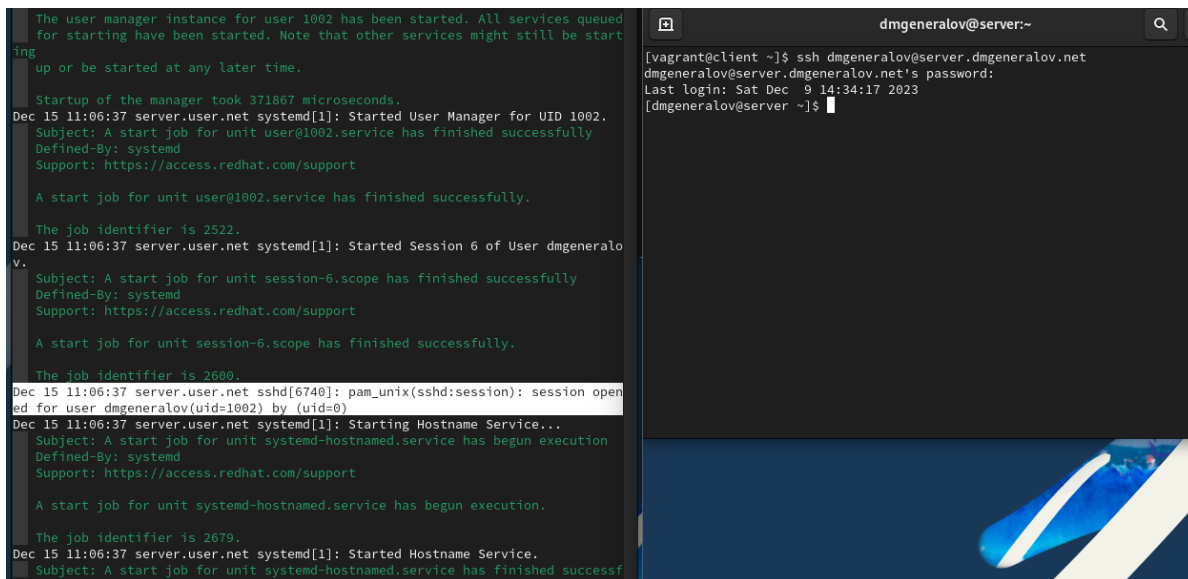


Рис. 3.4: ssh

Чтобы запретить это, нужно добавить строчку `AllowUsers` в `sshd_config`, тогда только указанные пользователи смогут подключаться. Другим пользователям все равно будет показываться приглашение ввести пароль, но сервер еще в начале соединения решил, что он не даст этому пользователю подключиться, потому что он не в списке `AllowedUsers`. Мы оставляем в этом списке только пользователей `vagrant` и `dmgeneralov`.

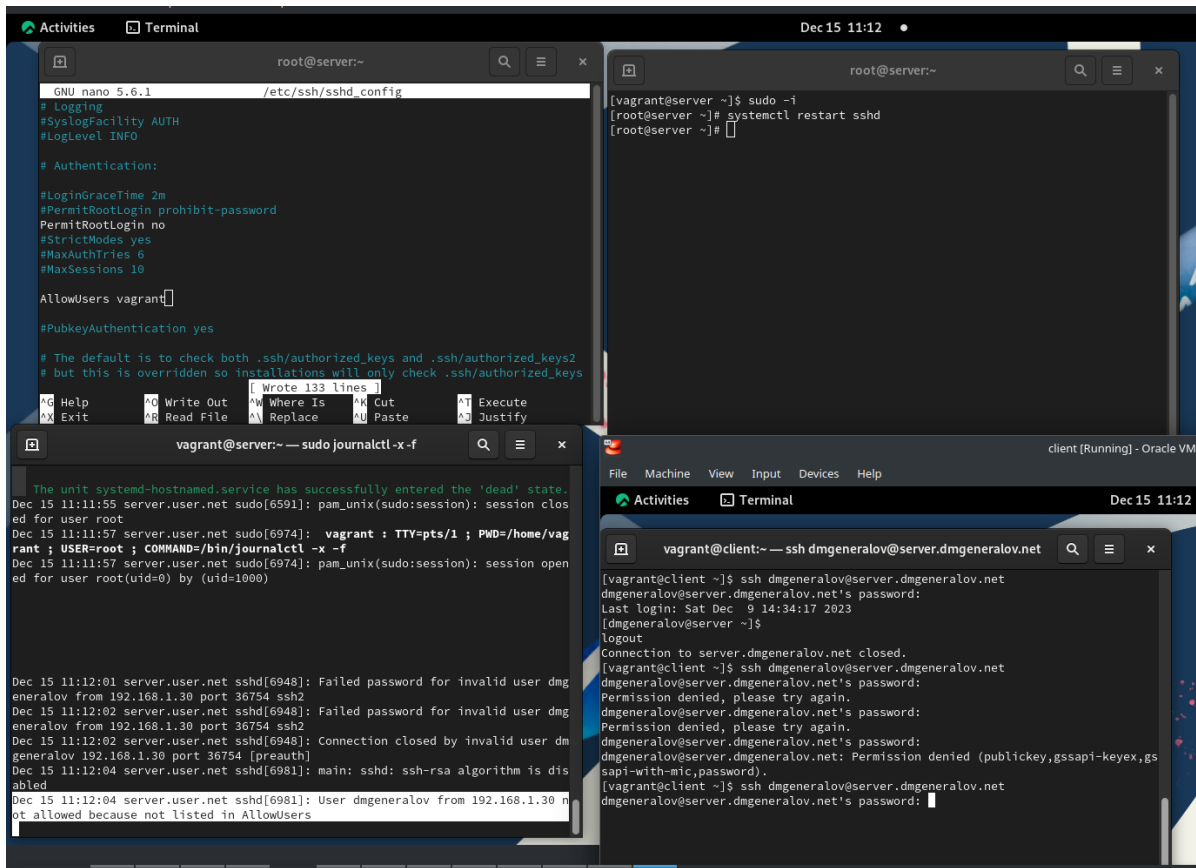


Рис. 3.5: ssh

Дальше мы настраиваем, чтобы SSH-сервер слушал порт 2022 в дополнение к порту 22. Однако, если сделать только это, то SSH-сервер напишет ошибку, что он не может слушать этот порт.

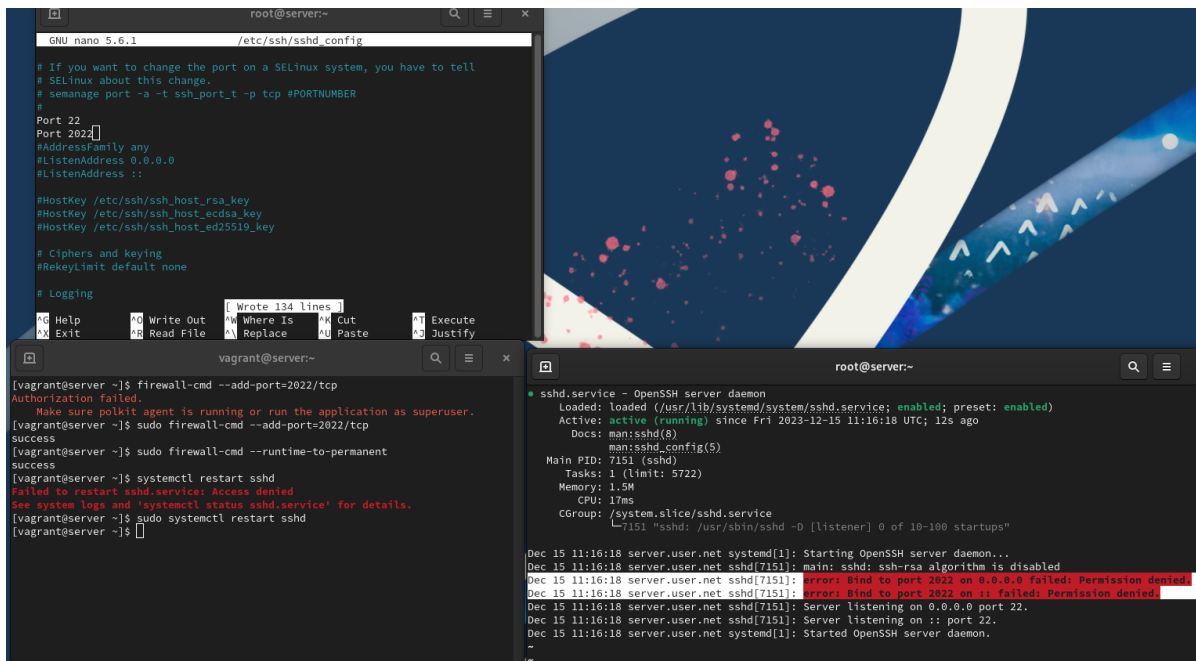


Рис. 3.6: ssh

Это из-за SELinux-политики, которая разрешает SSH только на порту 22. Если изменить это, то можно подключаться к серверу по альтернативному порту.

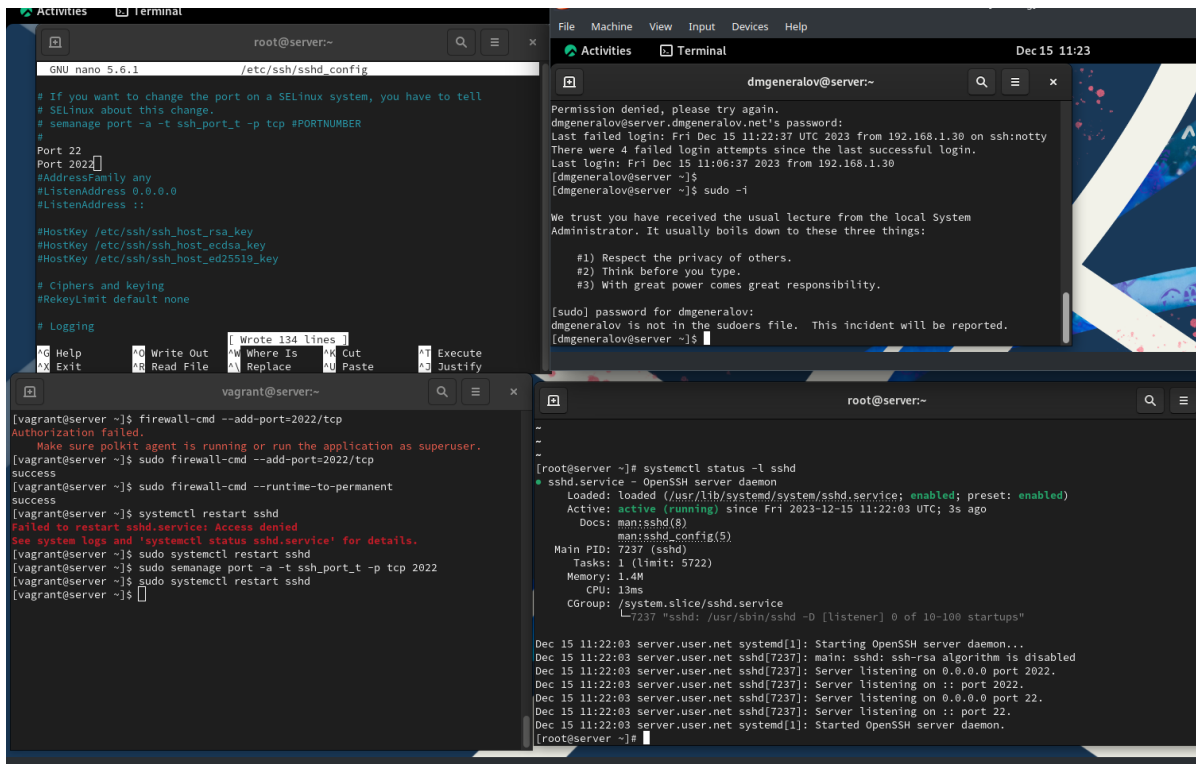


Рис. 3.7: ssh

Дальше мы используем аутентификацию по ключу, которая лучше чем пароли и поэтому включена по умолчанию. Для этого нужно создать ключ на клиенте с помощью `ssh-keygen`, добавить его на сервер с помощью `ssh-copy-id`, и после этого соединения не требуют пароля.

```

[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/FGvQTSZNGy8uA 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+4l1I3FzHu76A.
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 ~]$

```

Рис. 3.8: ssh

После этого можно использовать SSH, чтобы создавать туннели TCP. Сначала на клиенте не было открыто никаких TCP-сокетов. Но мы подключились к серверу, перенаправив локальный порт 8080 на его порт 80, и теперь у нас открыто соединение с сервером, а также мы слушаем порт webcache (то есть 8080) по IPv4 и IPv6. Если подключиться к этому порту, то мы увидим там HTTP-сервер – тот же самый, который запущен на сервере.

```

[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. 3.9: ssh

Через SSH можно запускать консольные программы – как неинтерактивные, так и интерактивные.

```

[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 investmen"
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...

```

Рис. 3.10: ssh

Можно даже запускать графические программы, и они будут выглядеть, будто они запущены на этом компьютере. Например, здесь мы запустили монитор процессов, и он показывается на клиенте, хотя он показывает процессы, которые есть только на сервере (вроде named).

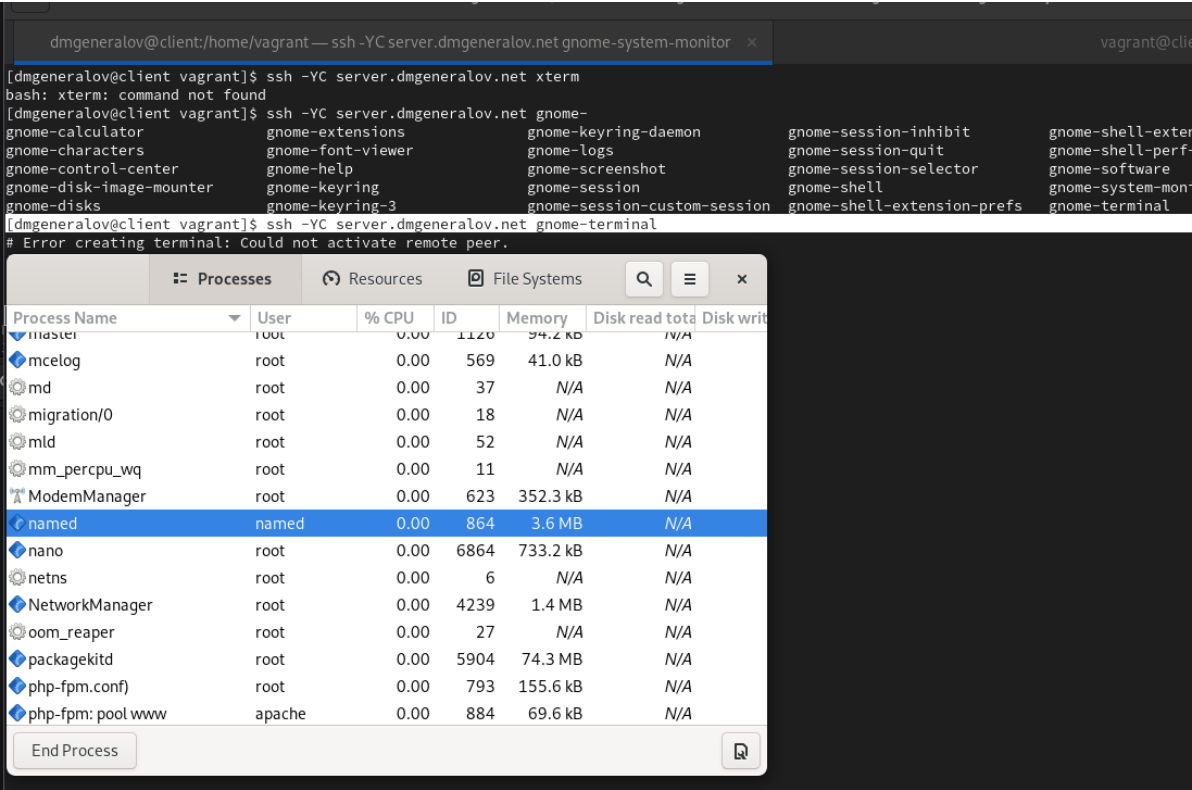


Рис. 3.11: ssh

В конце, как обычно, мы экспортируем настройки в Vagrant.

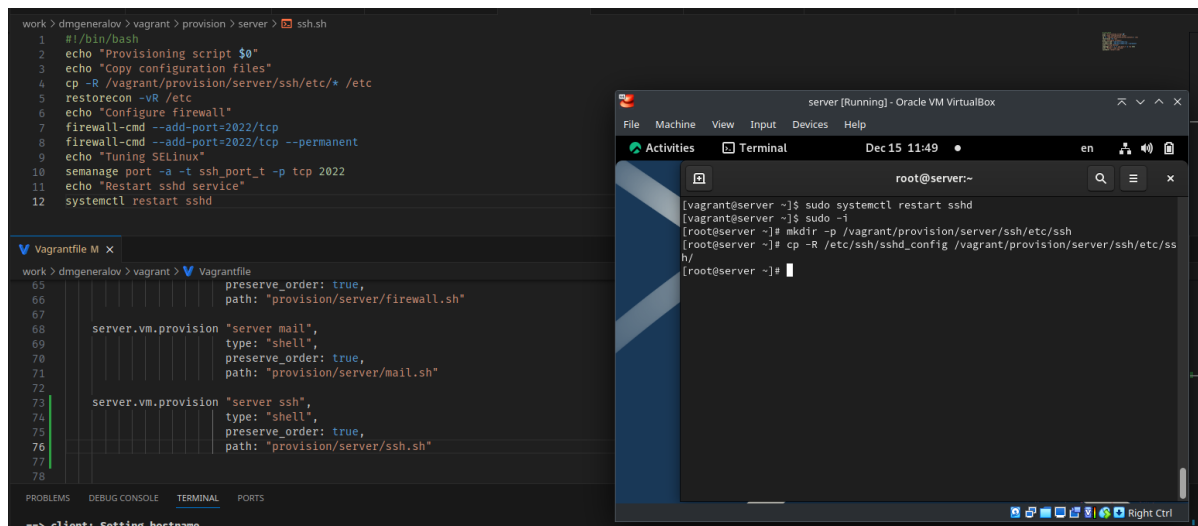


Рис. 3.12: vagrant

4 Выводы

Я получил опыт настройки SSH-сервера.

5 Контрольные вопросы

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

В файл настройки SSH-сервера надо добавить строки `PermitRootLogin no` и `AllowUsers alice`.

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

Несколько строк `Port` настраивают, чтобы сервер слушал несколько портов, и это полезно, если клиент имеет `firewall`, который запрещает ему использовать стандартный порт.

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

`-N` делает так, чтобы SSH-соединение не открывало терминала, `-n` делает так, что SSH не пытается читать `stdin`, и `-f` просит SSH перейти в фоновый режим после успешного подключения.

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

```
ssh -L 5555:server2.example.com:80 dmgeneralov@server1.dmgeneralov.com
```

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

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

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

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