

Лабораторная работа № 11

Настройка безопасного удалённого доступа по протоколу SSH

Абд эль хай мохамад

Содержание

1. Цель работы	2
2. Задание	2
3. Выполнение лабораторной работы	2
3.2 Ограничение списка пользователей для удалённого доступа по SSH	3
3.3 Настройка дополнительных портов для удалённого доступа по SSH	6
3.4 Настройка удалённого доступа по SSH по ключу	8
3.5 Организация туннелей SSH, перенаправление TCP-портов	9
3.6 Запуск графических приложений через SSH (X11Forwarding)	10
4. Вывод	12
Контрольные вопросы	12

Список иллюстраций

фигура 1	2
фигура 2	3
фигура 3	4
фигура 4	4
фигура 5	5
фигура 6	6
фигура 7	6
фигура 8	7
фигура 9	7
фигура 10	7
фигура 11	8
фигура 12	9

1. Цель работы

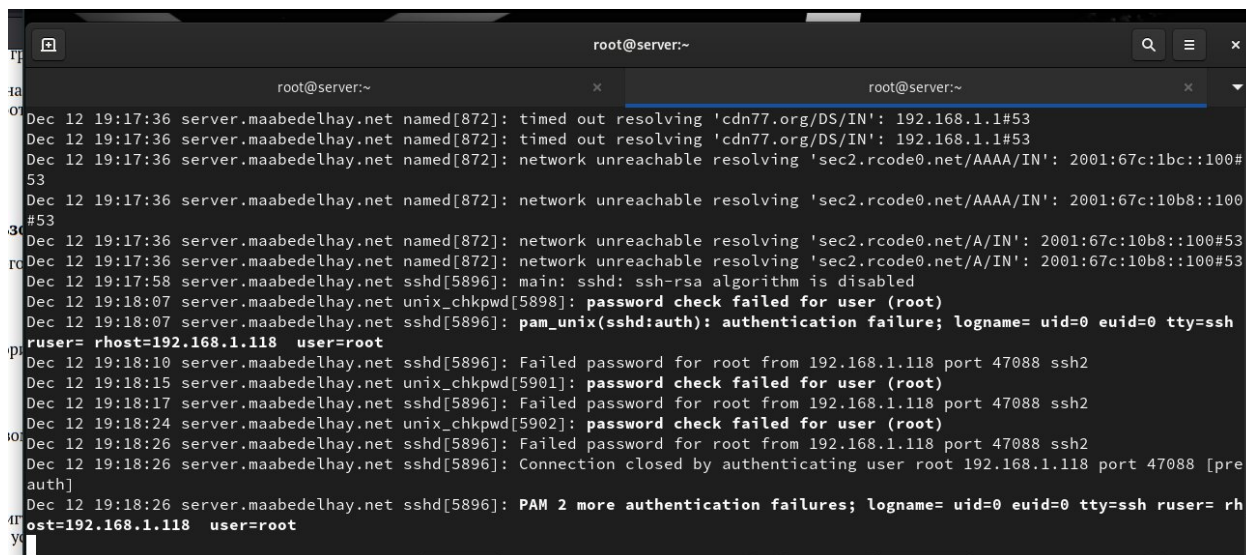
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2. Задание

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

3. Выполнение лабораторной работы

3.1 Запрет удалённого доступа по SSH для пользователя root



фигура 1

С клиента я попытался получить доступ к серверу через SSH-соединение через пользователя root:

```
ssh root@server.maabedelhay.net
```

Я не смог получить доступ к серверу как пользователь root (рис. 1).

На сервере я открыл файл конфигурации sshd /etc/ssh/sshd_config, чтобы отредактировать настройку и запретить пользователю root вход на сервер, установив:

«PermitRootLogin нет»

После сохранения изменений в файле конфигурации я перезапустил sshd:

systemctl перезапустить sshd

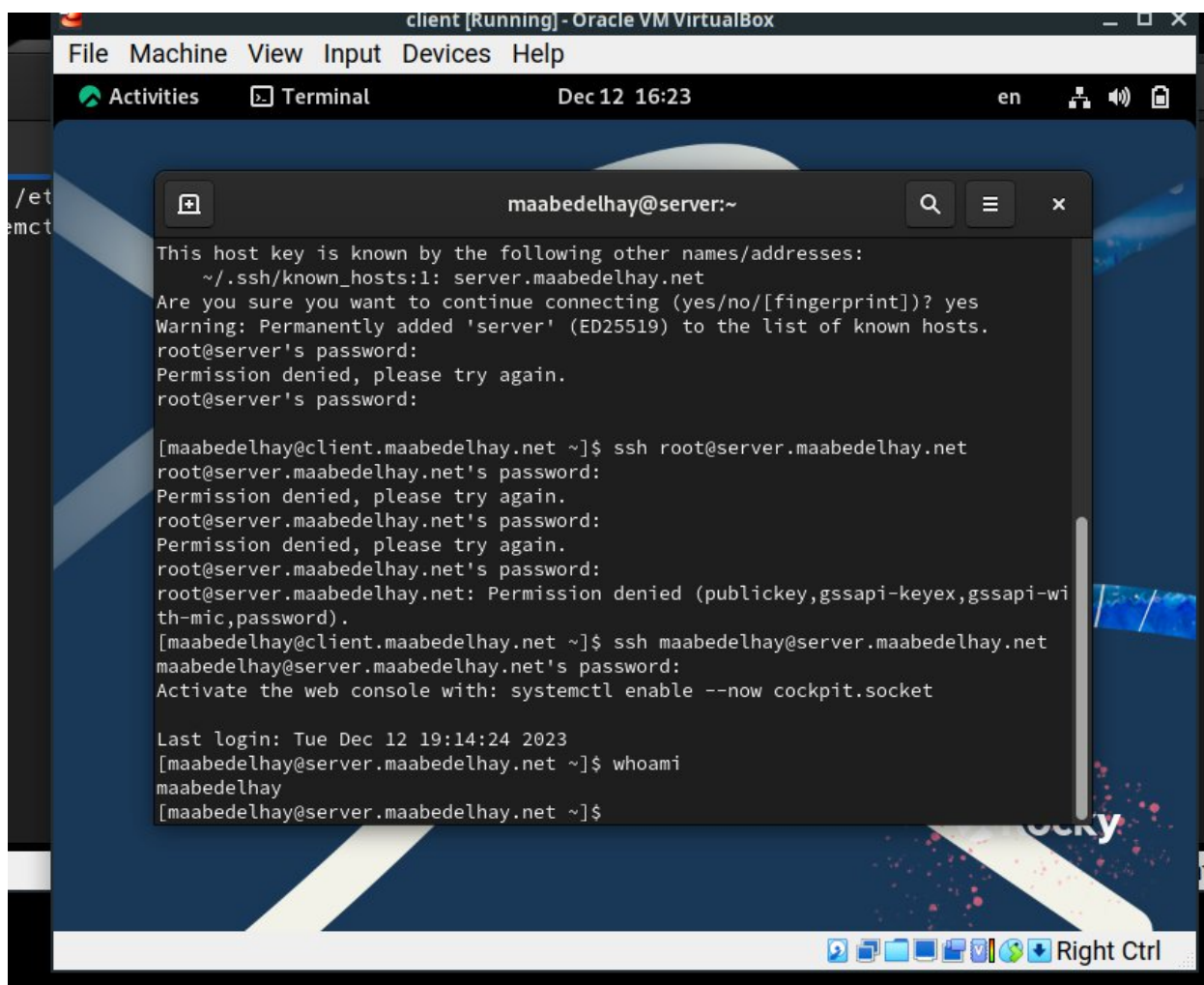
Я снова попытался получить доступ клиента к серверу через SSH-соединения через пользователя root:

ssh root@server.maabedelhay.net

У меня не было доступа к серверу.

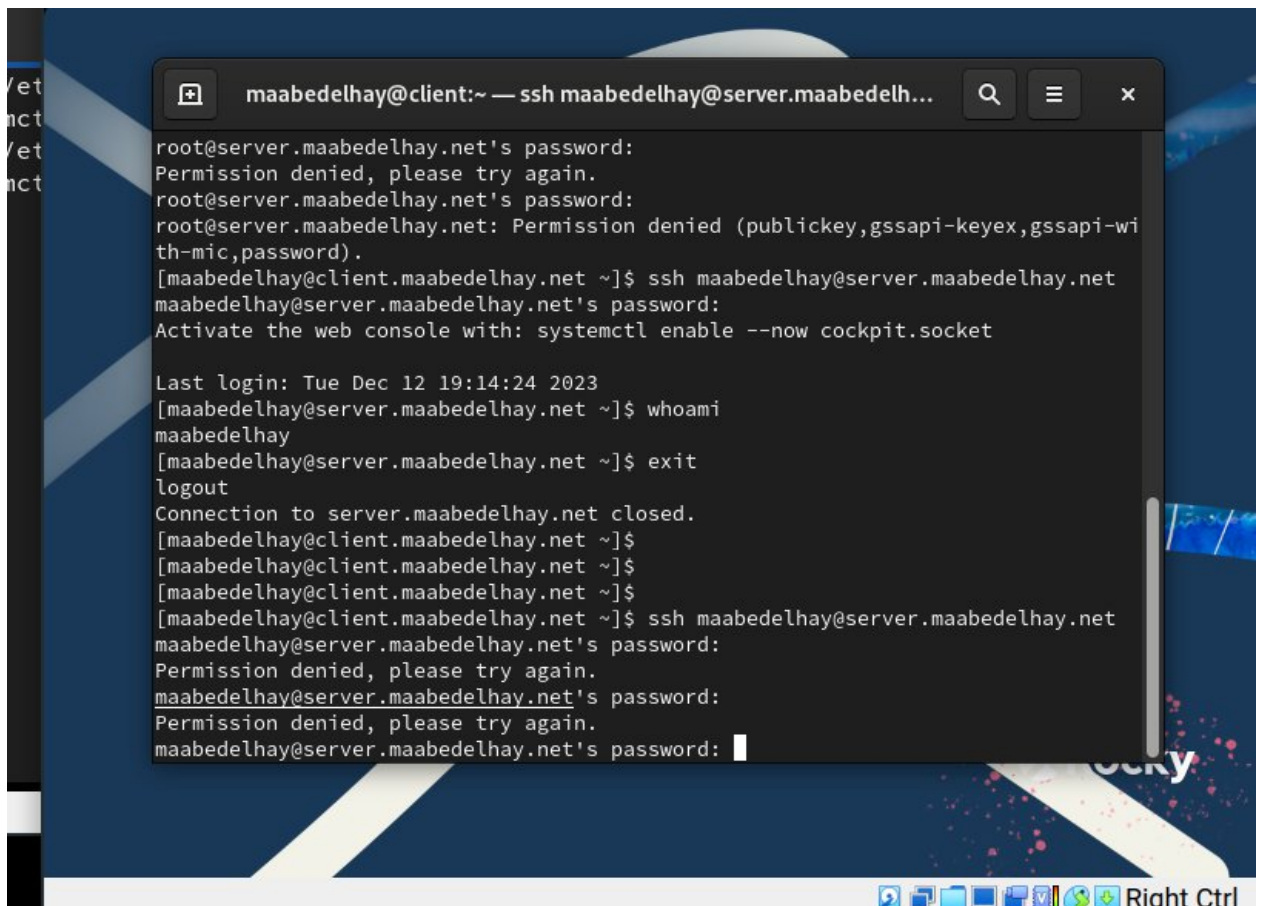
3.2 Ограничение списка пользователей для удалённого доступа по SSH

прежде чем я добавил конкретных пользователей, которые могут подключаться, в файл конфигурации, к которому я смог подключиться.



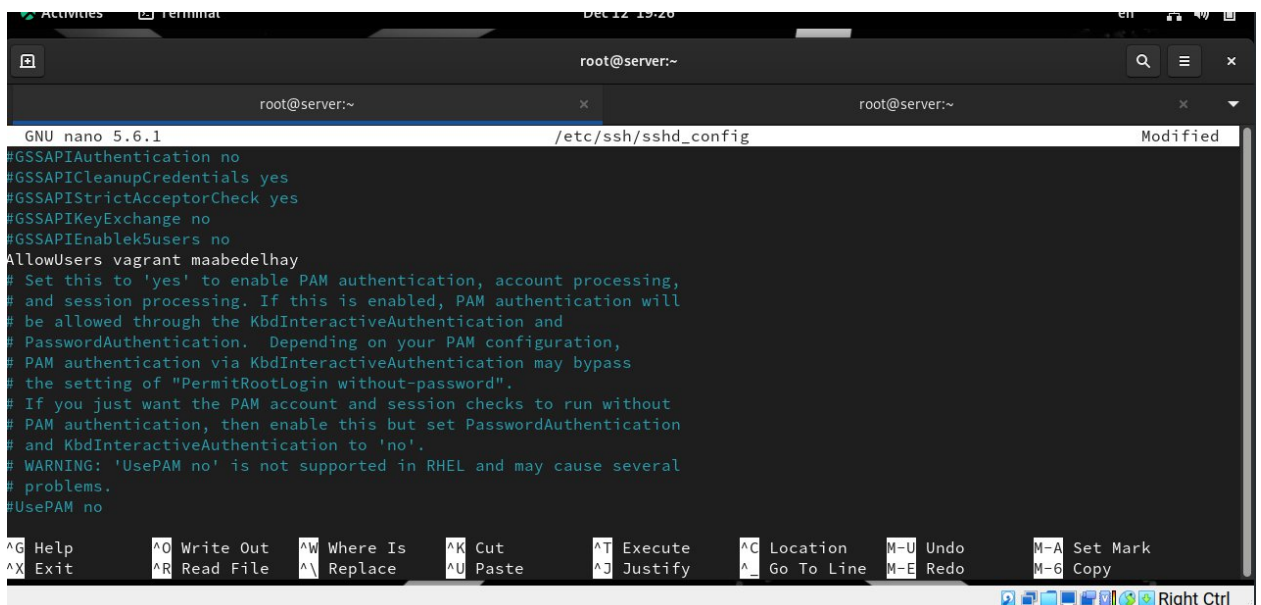
фигура 2

после того, как я добавил бродячего пользователя, я не смог подключиться к серверу, используя другого пользователя.



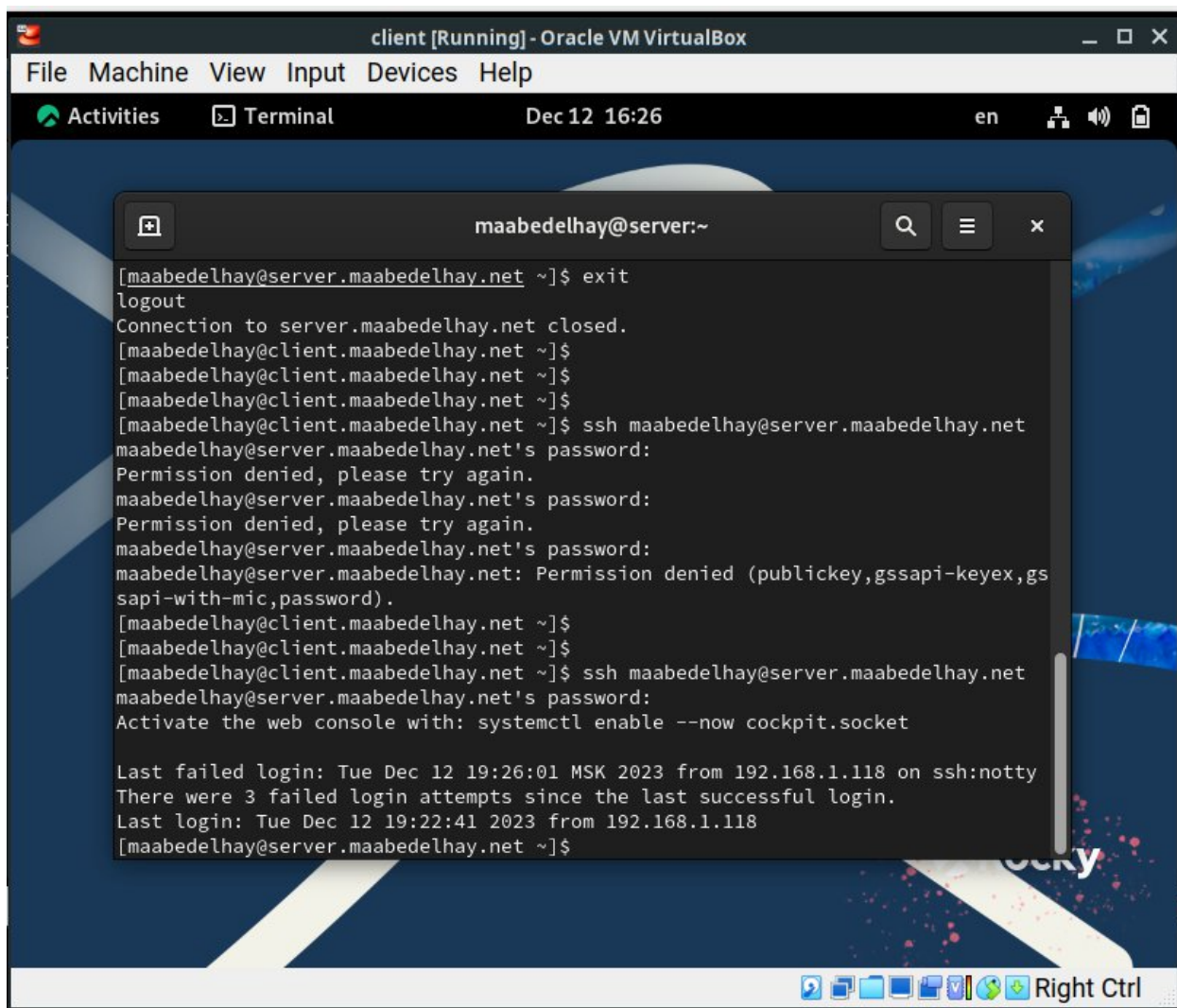
фигура 3

Добавил пользователя в файл конфигурации.



фигура 4

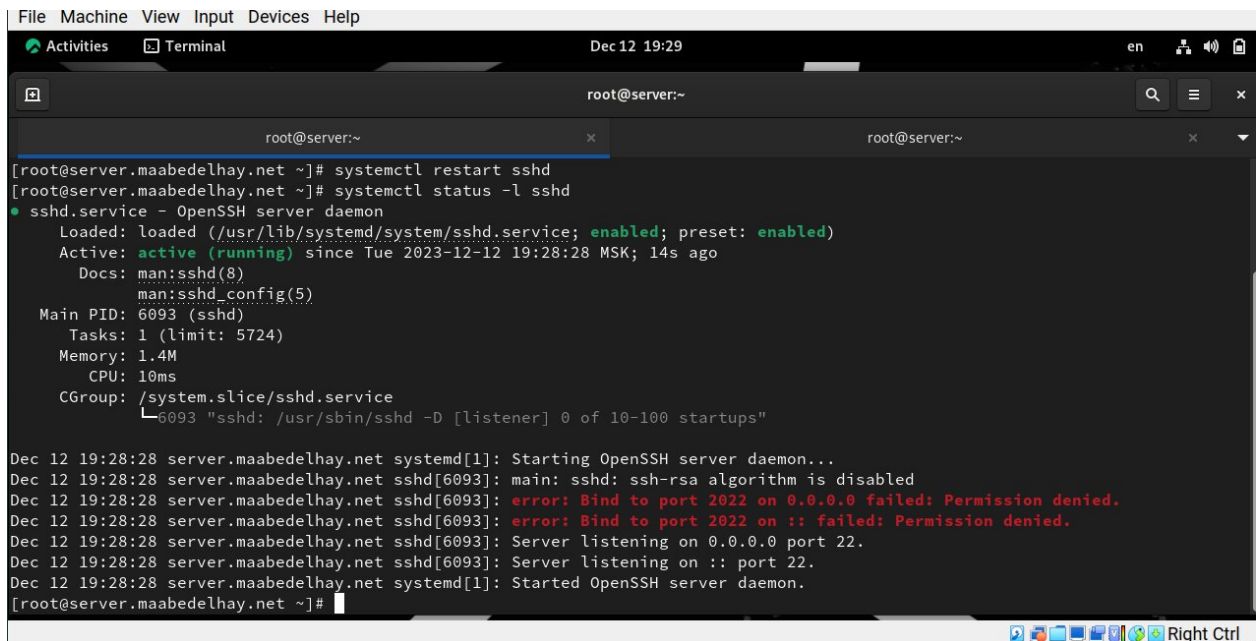
После того, как я добавил пользователя в файл конфигурации, я смог подключиться к серверу для пользователя maabeldelhay.



фигура 5

3.3 Настройка дополнительных портов для удалённого доступа по SSH

При просмотре статуса sshd показывает, что службе не удалось привязаться к порту 222.

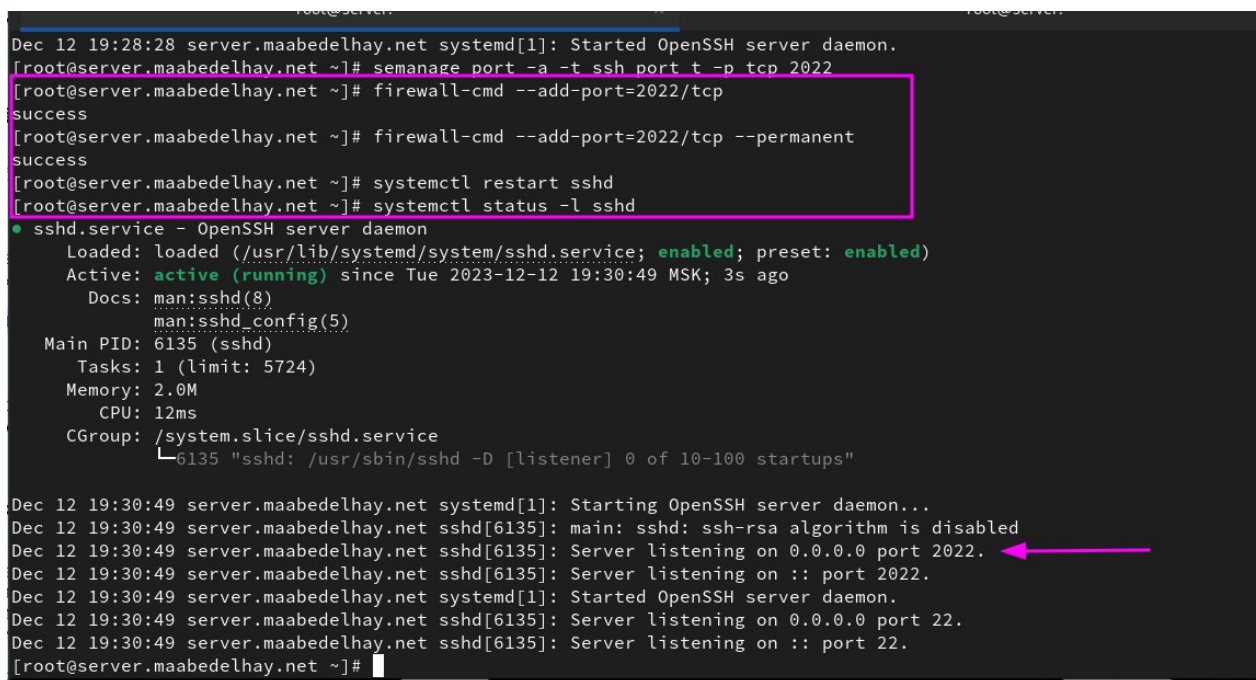


```
File Machine View Input Devices Help
Activities Terminal Dec 12 19:29
root@server:~
root@server:~
root@server:~
[root@server.maabeldelhay.net ~]# systemctl restart sshd
[root@server.maabeldelhay.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Tue 2023-12-12 19:28:28 MSK; 14s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 6093 (sshd)
    Tasks: 1 (limit: 5724)
   Memory: 1.4M
      CPU: 10ms
   CGroup: /system.slice/sshd.service
           └─6093 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 12 19:28:28 server.maabeldelhay.net systemd[1]: Starting OpenSSH server daemon...
Dec 12 19:28:28 server.maabeldelhay.net sshd[6093]: main: sshd: ssh-rsa algorithm is disabled
Dec 12 19:28:28 server.maabeldelhay.net sshd[6093]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Dec 12 19:28:28 server.maabeldelhay.net sshd[6093]: error: Bind to port 2022 on :: failed: Permission denied.
Dec 12 19:28:28 server.maabeldelhay.net sshd[6093]: Server listening on 0.0.0.0 port 22.
Dec 12 19:28:28 server.maabeldelhay.net sshd[6093]: Server listening on :: port 22.
Dec 12 19:28:28 server.maabeldelhay.net systemd[1]: Started OpenSSH server daemon.
[root@server.maabeldelhay.net ~]#
```

фигура 6

Я открыл порт 2022 в брандмауэре с помощью команды firewall-cmd.



```
Dec 12 19:28:28 server.maabeldelhay.net systemd[1]: Started OpenSSH server daemon.
[root@server.maabeldelhay.net ~]# semanage port -a -t ssh port t -p tcp 2022
[root@server.maabeldelhay.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.maabeldelhay.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.maabeldelhay.net ~]# systemctl restart sshd
[root@server.maabeldelhay.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 2023-12-12 19:30:49 MSK; 3s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 6135 (sshd)
    Tasks: 1 (limit: 5724)
   Memory: 2.0M
      CPU: 12ms
   CGroup: /system.slice/sshd.service
           └─6135 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 12 19:30:49 server.maabeldelhay.net systemd[1]: Starting OpenSSH server daemon...
Dec 12 19:30:49 server.maabeldelhay.net sshd[6135]: main: sshd: ssh-rsa algorithm is disabled
Dec 12 19:30:49 server.maabeldelhay.net sshd[6135]: Server listening on 0.0.0.0 port 2022.
Dec 12 19:30:49 server.maabeldelhay.net sshd[6135]: Server listening on :: port 2022.
Dec 12 19:30:49 server.maabeldelhay.net systemd[1]: Started OpenSSH server daemon.
Dec 12 19:30:49 server.maabeldelhay.net sshd[6135]: Server listening on 0.0.0.0 port 22.
Dec 12 19:30:49 server.maabeldelhay.net sshd[6135]: Server listening on :: port 22.
[root@server.maabeldelhay.net ~]#
```

фигура 7

Затем я перезапустил службу sshd на сервере и попытался подключиться к серверу с помощью SSH. Мне удалось успешно подключиться к серверу (рис 9).


```
[maabelhay@client.maabelhay.net ~]$  
[maabelhay@client.maabelhay.net ~]$  
[maabelhay@client.maabelhay.net ~]$ ssh maabelhay@server.maabelhay.net  
maabelhay@server.maabelhay.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Tue Dec 12 19:26:54 2023 from 192.168.1.118  
[maabelhay@server.maabelhay.net ~]$ sudo -i  
[sudo] password for maabelhay:  
[root@server.maabelhay.net ~]#
```

фигура 8

```
[maabelhay@client.maabelhay.net ~]$  
[maabelhay@client.maabelhay.net ~]$ ssh -p2022 maabelhay@server.maabelhay.net  
maabelhay@server.maabelhay.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Tue Dec 12 19:32:58 2023 from 192.168.1.118  
[maabelhay@server.maabelhay.net ~]$ sudo -i  
[sudo] password for maabelhay:  
[root@server.maabelhay.net ~]#
```

фигура 9

3.4 Настройка удалённого доступа по SSH по ключу

```
[maabelhay@client.maabelhay.net ~]$ ssh-copy-id maabelhay@server.maabelhay.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  
maabelhay@server.maabelhay.net's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'maabelhay@server.maabelhay.net'"  
and check to make sure that only the key(s) you wanted were added.  
  
[maabelhay@client.maabelhay.net ~]$ ssh maabelhay@server.maabelhay.net  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Tue Dec 12 20:16:46 2023  
[maabelhay@server.maabelhay.net ~]$
```

фигура 10

На сервере в файле конфигурации `/etc/ssh/sshd_config` я изменил параметр, чтобы разрешить аутентификацию по ключу:

PubkeyAuthentication yes

После сохранения изменений в файле конфигурации я перезапустил sshd.

На клиенте я начал генерировать ключ SSH, введя в терминал под пользователем maabeldelhay:

```
ssh-keygen
```

Закрытый ключ был записан в файл ~/.ssh/id_rsa, а открытый ключ — в файл ~/.ssh/id_rsa.pub.

Скопировал открытый ключ на сервер, введя на клиенте:

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

В конце концов я попытался получить доступ к серверу с клиента через SSH-соединение:

```
ssh maabeldelhay@server.maabeldelhay.net
```

теперь я смог пройти аутентификацию без ввода пароля для учетной записи удаленного пользователя.

3.5 Организация туннелей SSH, перенаправление TCP-портов

```
[maabeldelhay@client.maabeldelhay.net ~]$ ssh -fNL 8080:localhost:80 maabeldelhay@server.maabeldelhay.net
[maabeldelhay@client.maabeldelhay.net ~]$ lsof | grep TCP
ssh        6369          maabeldelhay    3u  IPv4        70139      0t0  TCP client.maabeldelhay.net:51776->dhcp.maabeldelhay.net:ssh (E
ABLISHED)
ssh        6369          maabeldelhay    4u  IPv6        70159      0t0  TCP localhost:webcache (LISTEN)
ssh        6369          maabeldelhay    5u  IPv4        70160      0t0  TCP localhost:webcache (LISTEN)
```

фигура 11

сначала я проверил, работают ли какие-либо службы на клиенте по протоколу TCP:

```
lsof | grep TCP
```

по-видимому, не было никаких служб, работающих с TCP.

Я перенаправил порт 80 на server.maabedelhay.net на порт 8080 на локальном компьютере.

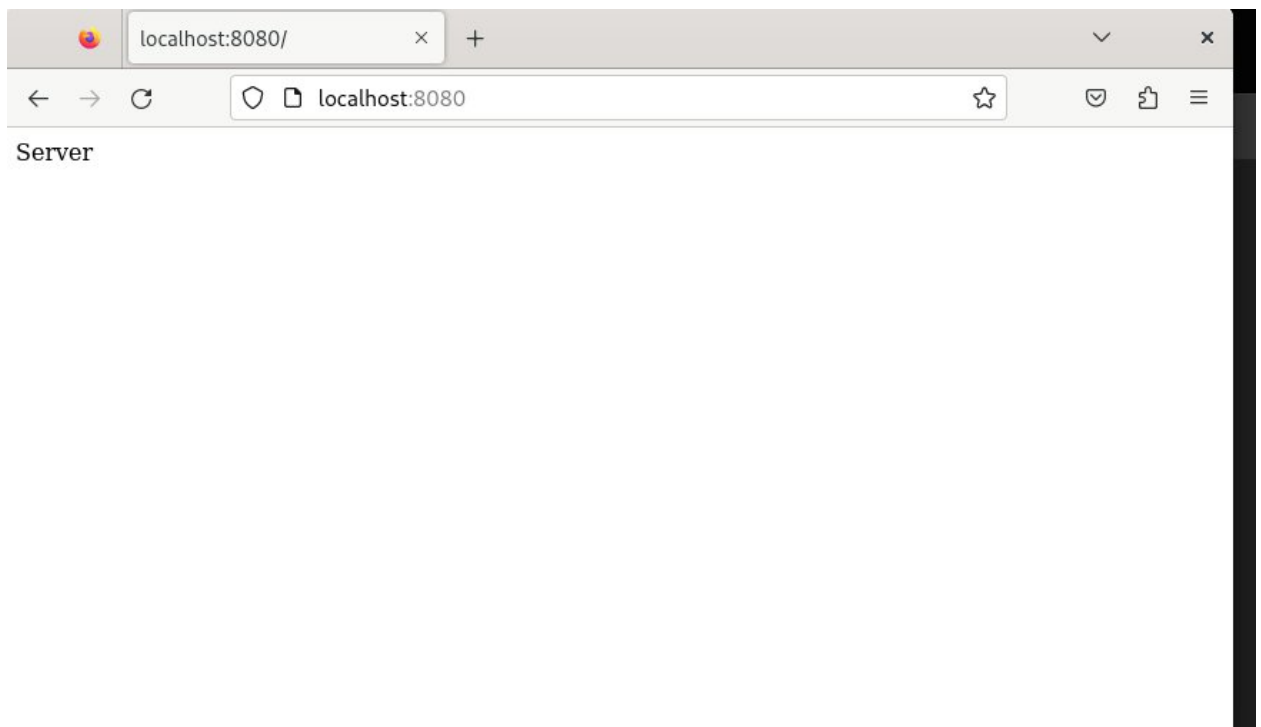
```
ssh -fNL 8080:localhost:80 maabedelhay@server.maabedelhay.net
```

Снова на клиенте я проверил, работают ли какие-либо службы по протоколу TCP:

```
lsof | grep TCP
```

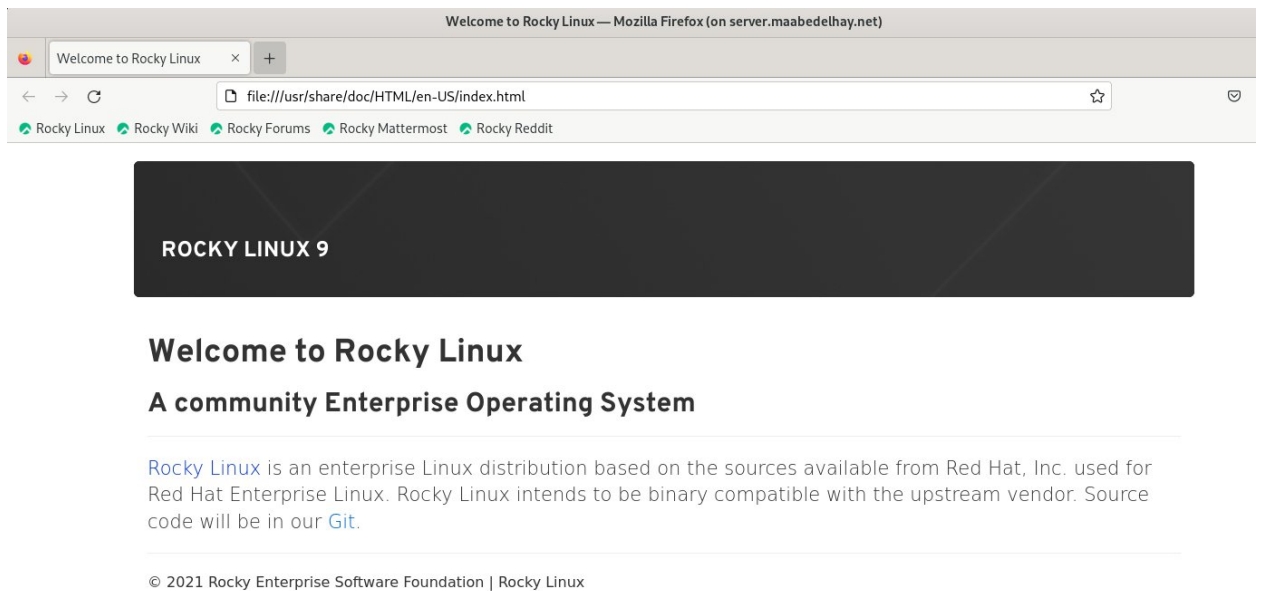
Он показывает, что служба, использующая протокол TCP, — это ssh, а также пользователь, использующий эту службу, и расположение файла.

На клиенте я запустил Firefox и в адресной строке ввел localhost:8080. На веб-странице было указано «Сервер», поскольку он настроен для этого.



фигура 12

3.6 Запуск графических приложений через SSH (X11Forwarding)



фигура 13

На сервере в файле конфигурации `/etc/ssh/sshd_config` я разрешил отображение графического интерфейса X11 на локальном клиентском компьютере:

X11Переадресация да

После сохранения изменений в файле конфигурации я перезапустил `sshd`.

Я подключился к серверу удаленно с клиента и запустил графическое приложение:

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

4. Вывод

Получил практические навыки настройки удаленного доступа к серверу по SSH.

Контрольные вопросы

1. Из файла конфигурации `ssh «/etc/ssh/sshd_config»` я могу запретить удаленный доступ через SSH к серверу пользователю `root`, добавив «`PermitRootLogin no`». Чтобы предоставить доступ пользователю Алисе «Пользователь `AllowUsers`».
2. `ssh -fNL 8080:localhost:80 maabedelhay@server.maabedelhay.net -f` Requests ssh to go to background just before command execution.