

# **Отчёт по лабораторной работе №11**

**Дисциплина: Администрирование сетевых подсистем**

**Мишина Анастасия Алексеевна**

# Содержание

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
2.1 Запрет удалённого доступа по SSH для пользователя root .	6
2.2 Ограничение списка пользователей для удалённого доступа по SSH . . . . .	7
2.3 Настройка дополнительных портов для удалённого доступа по SSH . . . . .	9
2.4 Настройка удалённого доступа по SSH по ключу . . . . .	13
2.5 Организация туннелей SSH, перенаправление TCP-портов	15
2.6 Запуск консольных приложений через SSH . . . . .	16
2.7 Запуск графических приложений через SSH (X11Forwarding)	16
2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	18
<b>3 Контрольные вопросы</b>	<b>20</b>
<b>4 Выводы</b>	<b>22</b>

# Список иллюстраций

2.1	Попытка установить SSH-соединение . . . . .	6
2.2	Файл /etc/ssh/sshd_config. Запрет входа на сервер пользователю root . . . . .	7
2.3	Попытка установить SSH-соединение с клиента . . . . .	7
2.4	Файл /etc/ssh/sshd_config. Изменение разрешенных пользователей для sshd . . . . .	8
2.5	Определение службы аутентификации пользователей . . . . .	8
2.6	Файл /etc/ssh/sshd_config. Изменение разрешенных пользователей для sshd . . . . .	9
2.7	Временный запуск SMTP-сервера . . . . .	9
2.8	Файл /etc/ssh/sshd_config. Добавление портов в файл конфигураций . . . . .	10
2.9	Расширенный статус работы sshd . . . . .	10
2.10	Мониторинг системных сообщений . . . . .	11
2.11	Просмотр расширенного статуса работы sshd после настройки работы по порту 2022 . . . . .	12
2.12	Установка SSH-соединение с клиента . . . . .	13
2.13	Формирования SSH-ключа на клиенте . . . . .	14
2.14	Установка SSH-соединения с сервером с клиентом . . . . .	14
2.15	Просмотр активных служб с протоколом TCP. Перенаправление порта 80 на server.aamishina.net на порт 8080 . . . . .	15
2.16	Просмотр локального сервера в браузере на клиенте . . . . .	15
2.17	Просмотр имени узла сервера и файлов на сервере через ssh . . . . .	16
2.18	Просмотр почты через ssh . . . . .	16
2.19	Запуск графического приложения через ssh . . . . .	17
2.20	Создание окружения для внесения изменений в настройки окружающей среды . . . . .	18
2.21	Скрипт файла /vagrant/provision/server/ssh.sh . . . . .	19
2.22	Изменение конфигурационного файла Vagrant . . . . .	19

# **Список таблиц**

# **1 Цель работы**

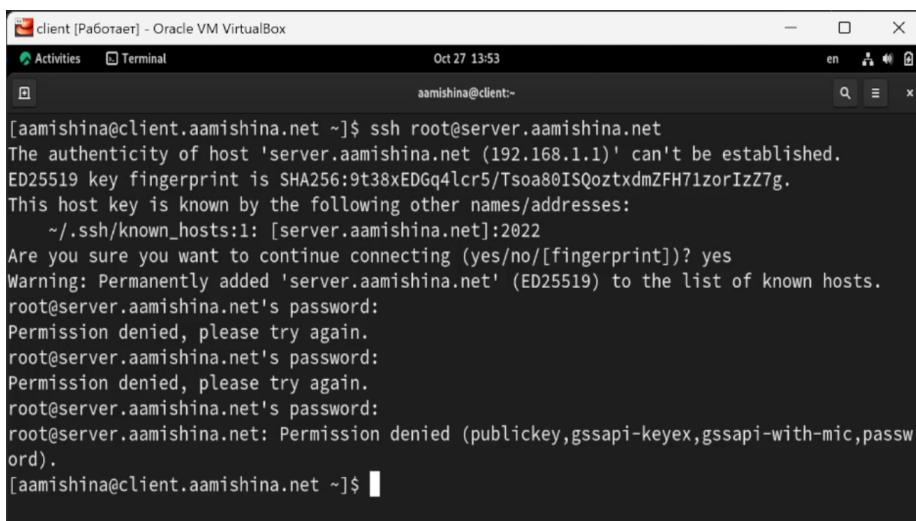
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

# 2 Выполнение лабораторной работы

## 2.1 Запрет удалённого доступа по SSH для пользователя root

Затем запустим виртуальную машину server. Откроем терминал и перейдем в режим суперпользователя.

В дополнительном терминале запустим мониторинг системных событий с помощью команды `journalctl -x -f`. С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя root(рис. fig. 2.1):



The screenshot shows a terminal window titled "client [Работает] - Oracle VM VirtualBox". The terminal session is running under user "aamishina" on the client machine. The command entered is `ssh root@server.aamishina.net`. The output shows the following:

```
[aamishina@client.aamishina.net ~]$ ssh root@server.aamishina.net
The authenticity of host 'server.aamishina.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:9t38xEDGq4lcr5/Tsoa80ISQoztxdmZFH71zorIzZ7g.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [server.aamishina.net]:22
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.aamishina.net' (ED25519) to the list of known hosts.
root@server.aamishina.net's password:
Permission denied, please try again.
root@server.aamishina.net's password:
Permission denied, please try again.
root@server.aamishina.net's password:
root@server.aamishina.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[aamishina@client.aamishina.net ~]$
```

Рис. 2.1: Попытка установить SSH-соединение

При попытке соединения, так как мы делаем это первый раз, добавляем сервер в список известных хостов. Затем требуется ввести пароль от

пользователя root, но соединение отклоняется.

На сервере откроем файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретим вход на сервер пользователю root, установив(рис. fig. 2.2):

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

Рис. 2.2: Файл /etc/ssh/sshd\_config. Запрет входа на сервер пользователю root

После сохранения изменений в файле конфигурации перезапустим sshd с помощью команды `systemctl restart sshd`. Повторяем попытку получения доступа через root, вновь получаем отказ в доступе.

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя aamishina (рис. fig. 2.3):

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

Last login: Sun Oct 27 13:46:20 2024
[aamishina@server.aamishina.net ~]$
```

Рис. 2.3: Попытка установить SSH-соединение с клиента

Соединение проходит удачно.

На сервере откроем файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавим строку(fig. 2.4):

```
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#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
AuthorizedKeysFile      .ssh/authorized_keys
AllowUsers vagrant
#AuthorizedPrincipalsFile none
```

Рис. 2.4: Файл /etc/ssh/sshd\_config. Изменение разрешенных пользователей для sshd

После сохранения изменений в файле конфигурации перезапустим sshd. Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя aamishina(рис. fig. 2.5):

```
[aamishina@server.aamishina.net ~]$ ssh aamishina@server.aamishina.net
The authenticity of host 'server.aamishina.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:9t38xEDGq4lcr5/Tsoa80ISQoztxdmZFH71zorIzZ7g.
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.aamishina.net' (ED25519) to the list of known hosts.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password:
Permission denied, please try again.
aamishina@server.aamishina.net's password:
aamishina@server.aamishina.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,
password).
[aamishina@server.aamishina.net ~]$
```

Рис. 2.5: Определение службы аутентификации пользователей

В этот раз соединение не устанавливается, так как в списке разрешенных пользователей нет нашего.

В файле /etc/ssh/sshd\_config конфигурации sshd внесем следующее изменение(fig. 2.6):

```
# The default is to check both .ssh/authorized_keys and .so
# but this is overridden so installations will only check
AuthorizedKeysFile      .ssh/authorized_keys
AllowUsers vagrant aamishina
#AuthorizedPrincipalsFile none
```

Рис. 2.6: Файл /etc/ssh/sshd\_config. Изменение разрешенных пользователей для sshd

Снова попытаемся установить соединение с клиента к серверу(fig. 2.7):

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

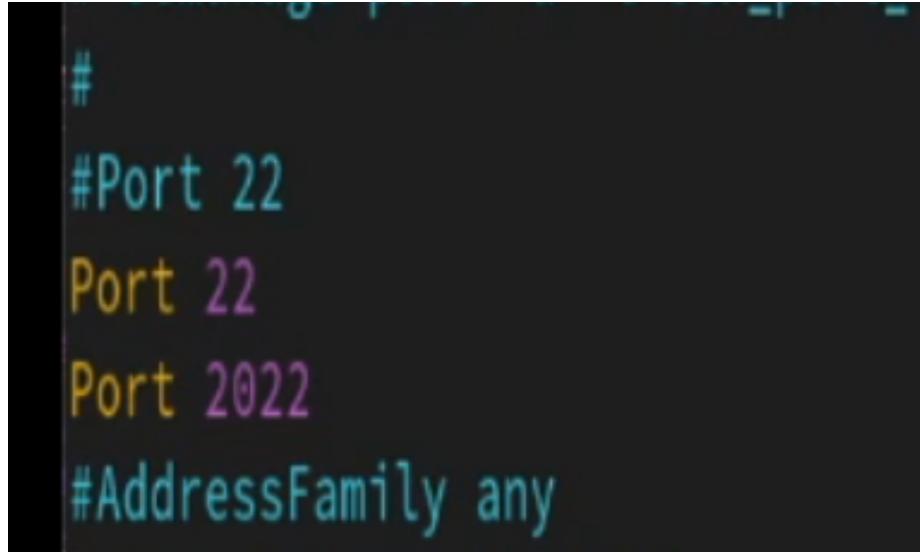
Last failed login: Sun Oct 27 13:59:49 UTC 2024 from 192.168.1.1 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Sun Oct 27 13:56:53 2024 from 192.168.1.57
[aamishina@server.aamishina.net ~]$
```

Рис. 2.7: Временный запуск SMTP-сервера

В этот раз доступ получен.

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдем строку Port и ниже этой строки добавим(fig. 2.8):



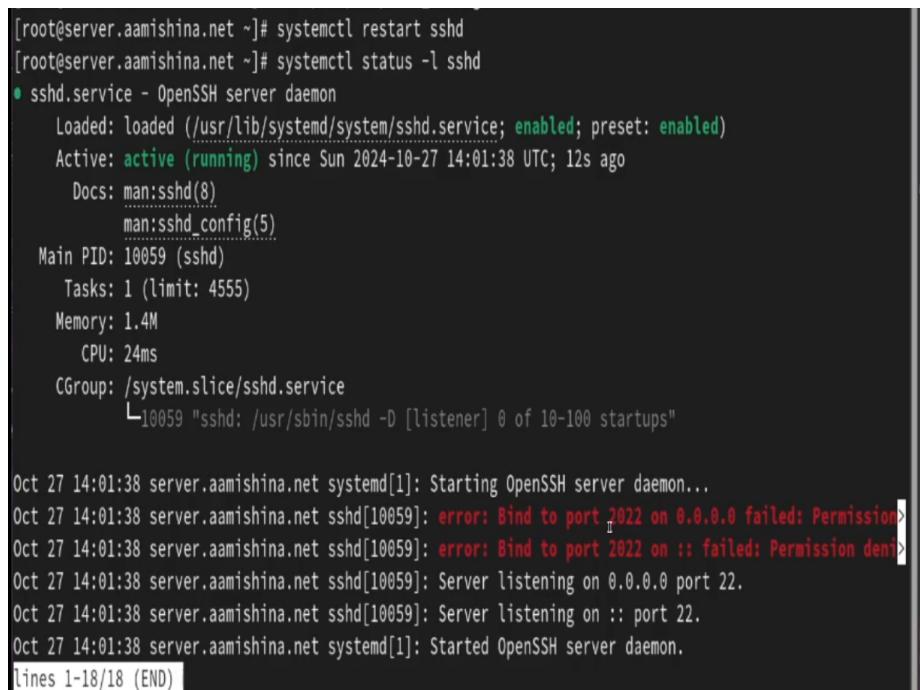
```
#  
#Port 22  
Port 22  
Port 2022  
#AddressFamily any
```

Рис. 2.8: Файл /etc/ssh/sshd\_config. Добавление портов в файл конфигураций

Эта запись сообщает процессу sshd о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.

После сохранения изменений в файле конфигурации перезапустим sshd.

Посмотрим расширенный статус работы sshd(fig. 2.9):



```
[root@server.aamishina.net ~]# systemctl restart sshd
[root@server.aamishina.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 Sun 2024-10-27 14:01:38 UTC; 12s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Main PID: 10059 (sshd)
      Tasks: 1 (limit: 4555)
     Memory: 1.4M
        CPU: 24ms
       CGroup: /system.slice/sshd.service
               └─10059 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 27 14:01:38 server.aamishina.net systemd[1]: Starting OpenSSH server daemon...
Oct 27 14:01:38 server.aamishina.net sshd[10059]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied
Oct 27 14:01:38 server.aamishina.net sshd[10059]: error: Bind to port 2022 on :: failed: Permission denied
Oct 27 14:01:38 server.aamishina.net sshd[10059]: Server listening on 0.0.0.0 port 22.
Oct 27 14:01:38 server.aamishina.net sshd[10059]: Server listening on :: port 22.
Oct 27 14:01:38 server.aamishina.net systemd[1]: Started OpenSSH server daemon.
lines 1-18/18 (END)
```

Рис. 2.9: Расширенный статус работы sshd

Система сообщает об отказе в работе sshd через порт 2022. Дополнительно посмотрим сообщения в терминале с мониторингом системных событий(рис. fig. 2.10):

```
Oct 27 14:01:47 server.aamishina.net setroubleshoot[10060]: SELinux is preventing /usr/sbin/sshd from name_bind access on the
tcp_socket port 2022. For complete SELinux messages run: sealert -L 21137477-0734-4c00-b73b-697598b0ee70
Oct 27 14:01:47 server.aamishina.net setroubleshoot[10060]: SELinux is preventing /usr/sbin/sshd from name_bind access on the
tcp_socket port 2022.
```

Рис. 2.10: Мониторинг системных сообщений

Можно увидеть, что отказ происходит из-за запрета SELinux на работу с этим портом.

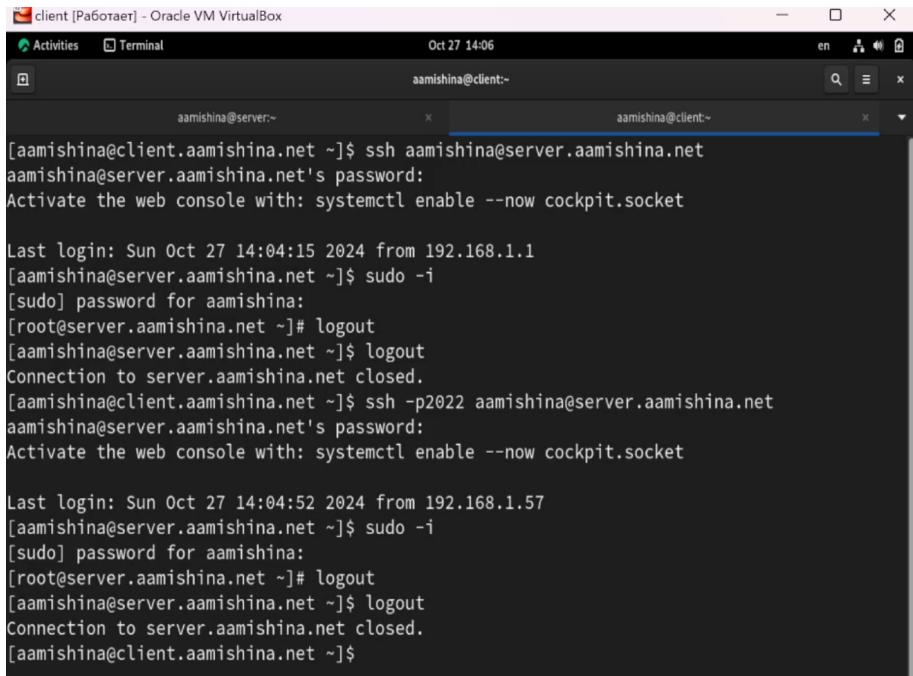
Исправим на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана откроем порт 2022 протокола. Вновь перезапустим sshd и посмотрите расширенный статус его работы. Статус показывает, что процесс sshd теперь прослушивает два порта(fig. 2.11)

```
[root@server.aamishina.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.aamishina.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.aamishina.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.aamishina.net ~]# systemctl restart sshd
[root@server.aamishina.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 Sun 2024-10-27 14:03:27 UTC; 7s ago
        Docs: man:sshd(8)
               man:sshd_config(5)
     Main PID: 10085 (sshd)
       Tasks: 1 (limit: 4555)
      Memory: 1.4M
         CPU: 14ms
        CGroup: /system.slice/sshd.service
                  └─10085 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 27 14:03:27 server.aamishina.net systemd[1]: Starting OpenSSH server daemon...
Oct 27 14:03:27 server.aamishina.net sshd[10085]: Server listening on 0.0.0.0 port 2022.
Oct 27 14:03:27 server.aamishina.net sshd[10085]: Server listening on :: port 2022.
Oct 27 14:03:27 server.aamishina.net sshd[10085]: Server listening on 0.0.0.0 port 22.1
Oct 27 14:03:27 server.aamishina.net sshd[10085]: Server listening on :: port 22.
Oct 27 14:03:27 server.aamishina.net systemd[1]: Started OpenSSH server daemon.
[root@server.aamishina.net ~]#
```

Рис. 2.11: Просмотр расширенного статуса работы sshd после настройки работы по порту 2022

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя aamishina обычным способом и указав порт 2022(рис. fig. 2.12):



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

Last login: Sun Oct 27 14:04:15 2024 from 192.168.1.1
[aamishina@server.aamishina.net ~]$ sudo -i
[sudo] password for aamishina:
[root@server.aamishina.net ~]# logout
[aamishina@server.aamishina.net ~]$ logout
Connection to server.aamishina.net closed.
[aamishina@client.aamishina.net ~]$ ssh -p2022 aamishina@server.aamishina.net
aamishina@server.aamishina.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Oct 27 14:04:52 2024 from 192.168.1.57
[aamishina@server.aamishina.net ~]$ sudo -i
[sudo] password for aamishina:
[root@server.aamishina.net ~]# logout
[aamishina@server.aamishina.net ~]$ logout
Connection to server.aamishina.net closed.
[aamishina@client.aamishina.net ~]$
```

Рис. 2.12: Установка SSH-соединение с клиента

## 2.4 Настройка удалённого доступа по SSH по ключу

Создадим пару из открытого и закрытого ключей для входа на сервер.

На сервере в конфигурационном файле /etc/ssh/sshd\_config зададим параметр, разрешающий аутентификацию по ключу, написав:

```
PubkeyAuthentication yes
```

После сохранения изменений в файле конфигурации перезапустим sshd.

На клиенте сформируем SSH-ключ, введя в терминале (fig. 2.13):

```
[aamishina@client.aamishina.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aamishina/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/aamishina/.ssh/id_rsa
Your public key has been saved in /home/aamishina/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:A9qqGoMyUkjv0IQfo14zlPRjZmP7hhNwxU+pX6a1cL0 aamishina@client.aamishina.net
The key's randomart image is:
+---[RSA 3072]---+
| . .. .
| o o .. o
| o B X. +
| ..B Xo+o o =
| ..o.B.o. S B ..
| o.+ o.+ + . E
| B. ...o o
| o+ . o
| ...
+---[SHA256]---+
[aamishina@client.aamishina.net ~]$
```

Рис. 2.13: Формирования SSH-ключа на клиенте

Закрытый ключ теперь будет записан в файл `~/.ssh/id_rsa`, а открытый ключ записывается в файл `~/.ssh/id_rsa.pub`.

Скопируем открытый ключ на сервер, введя на клиенте:

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

Попробуем получить доступ с клиента к серверу посредством SSH-соединения (fig. 2.14):

```
[aamishina@client.aamishina.net ~]$ ssh-copy-id aamishina@server.aamishina.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
aamishina@server.aamishina.net's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'aamishina@server.aamishina.net'"
and check to make sure that only the key(s) you wanted were added.
[aamishina@client.aamishina.net ~]$ ssh aamishina@server.aamishina.net
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Oct 27 14:05:58 2024 from 192.168.1.57
[aamishina@server.aamishina.net ~]$
```

Рис. 2.14: Установка SSH-соединения с сервером с клиента

## 2.5 Организация туннелей SSH, перенаправление TCP-портов

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP, на данный момент их нет. Перенаправим порт 80 на server.aamishina.net на порт 8080 на локальной машине и вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP(рис. fig. 2.15)

```
[aamishina@client.aamishina.net ~]$ lsof | grep TCP
ssh      9797          aamishina  3u      IPv4          44594    0t0      TCP cli
nt.aamishina.net:54528->www.aamishina.net:ssh (ESTABLISHED)
[aamishina@client.aamishina.net ~]$ ssh -fNL 8080:localhost:80 aamishina@server.aamishina.net
[aamishina@client.aamishina.net ~]$ lsof | grep TCP
ssh      9797          aamishina  3u      IPv4          44594    0t0      TCP cli
ent.aamishina.net:54528->server.aamishina.net:ssh (ESTABLISHED)
ssh     10016          aamishina  3u      IPv4          58809    0t0      TCP cli
ent.aamishina.net:50454->server.aamishina.net:ssh (ESTABLISHED)
ssh     10016          aamishina  4u      IPv6          58830    0t0      TCP loc
alhost:webcache (LISTEN)
ssh     10016          aamishina  5u      IPv4          58831    0t0      TCP loc
alhost:webcache (LISTEN)
[aamishina@client.aamishina.net ~]$
```

Рис. 2.15: Просмотр активных служб с протоколом TCP. Перенаправление порта 80 на server.aamishina.net на порт 8080

Появилось три новые службы, использующие TCP протокол – появился доступ к server.aamishina.net по ssh, а также к локальному хосту по IPv4 и IPv6.

На клиенте запустим браузер и в адресной строке введем localhost:8080. Отображается страница с приветствием «Welcome to the server.aamishina.net server»(fig. 2.16):

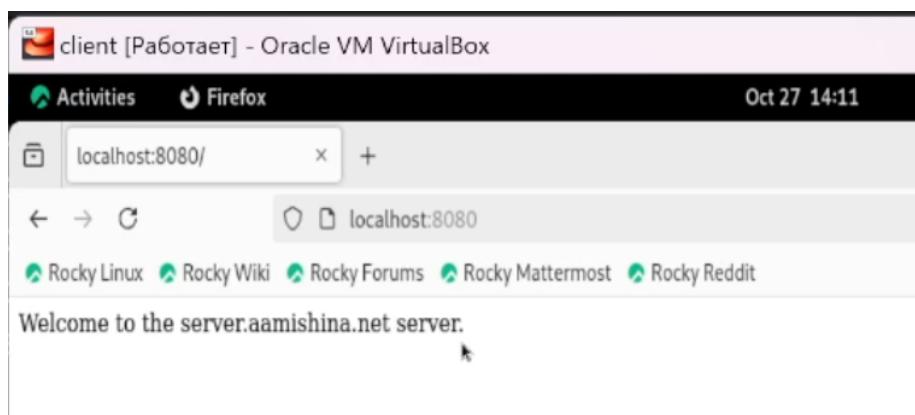


Рис. 2.16: Просмотр локального сервера в браузере на клиенте

## 2.6 Запуск консольных приложений через SSH

На клиенте откроем терминал под пользователем aamishina и посмотрим с клиента имя узла сервера, файлов на сервере (рис. fig. 2.17) и почту(рис. fig. 2.18):

```
[aamishina@client.aamishina.net ~]$ ssh aamishina@server.aamishina.net hostname  
server.aamishina.net  
[aamishina@client.aamishina.net ~]$ ssh aamishina@server.aamishina.net ls -Al  
total 68  
-rw-----. 1 aamishina aamishina 908 Oct 27 14:06 .bash_history  
-rw-r--r--. 1 aamishina aamishina 18 Apr 30 11:28 .bash_logout  
-rw-r--r--. 1 aamishina aamishina 141 Apr 30 11:28 .bash_profile  
-rw-r--r--. 1 aamishina aamishina 519 Sep 18 18:24 .bashrc  
drwx-----. 10 aamishina aamishina 4096 Oct 24 11:07 .cache  
drwx-----. 10 aamishina aamishina 4096 Oct 24 11:06 .config  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Desktop  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Documents  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Downloads  
drwx-----. 4 aamishina aamishina 32 Sep 18 18:29 .local  
drwx-----. 5 aamishina aamishina 4096 Oct 25 20:47 Maildir  
drwxr-xr-x. 2 aamishina aamishina 39 Sep 18 16:41 .mozilla  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Music  
drwxr-xr-x. 2 aamishina aamishina 4096 Oct 25 19:29 Pictures  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Public  
drwx-----. 2 aamishina aamishina 71 Oct 27 14:08 .ssh  
drwxr-xr-x. 2 aamishina aamishina 6 Sep 18 18:29 Templates  
-rw-----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-clipboard-tty1-control.pid  
-rw-----. 1 aamishina aamishina 5 Oct 27 13:46 .vboxclient-clipboard-tty1-service.pid  
-rw-----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-draganddrop-tty1-control.pid  
-rw-----. 1 aamishina aamishina 5 Oct 27 13:46 .vboxclient-draganddrop-tty1-service.pid  
-rw-----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-hostversion-tty1-control.pid  
-rw-----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-seamless-tty1-control.pid
```

Рис. 2.17: Просмотр имени узла сервера и файлов на сервере через ssh

```
[aamishina@client.aamishina.net ~]$ ssh aamishina@server.aamishina.net MAIL=~/Maildir/ mail  
s-nail version v14.9.22. Type '?' for help  
/home/aamishina/Maildir: 3 messages 1 unread  
 1 aamishina 2024-10-25 18:02 18/640  
•U 2 aamishina@client.aam 2024-10-25 20:23 21/864 "LMTP test"  
 3 aamishina 2024-10-25 20:47 22/818
```

Рис. 2.18: Просмотр почты через ssh

## 2.7 Запуск графических приложений через SSH (X11Forwarding)

На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешим отображать на локальном клиентском компьютере графические интер-

файлы X11, прописав:

```
X11Forwarding yes
```

После сохранения изменения в конфигурационном файле перезапустим sshd.

Попробуем с клиента удалённо подключиться к серверу и запустить графическое приложение firefox(рис. fig. 2.19):

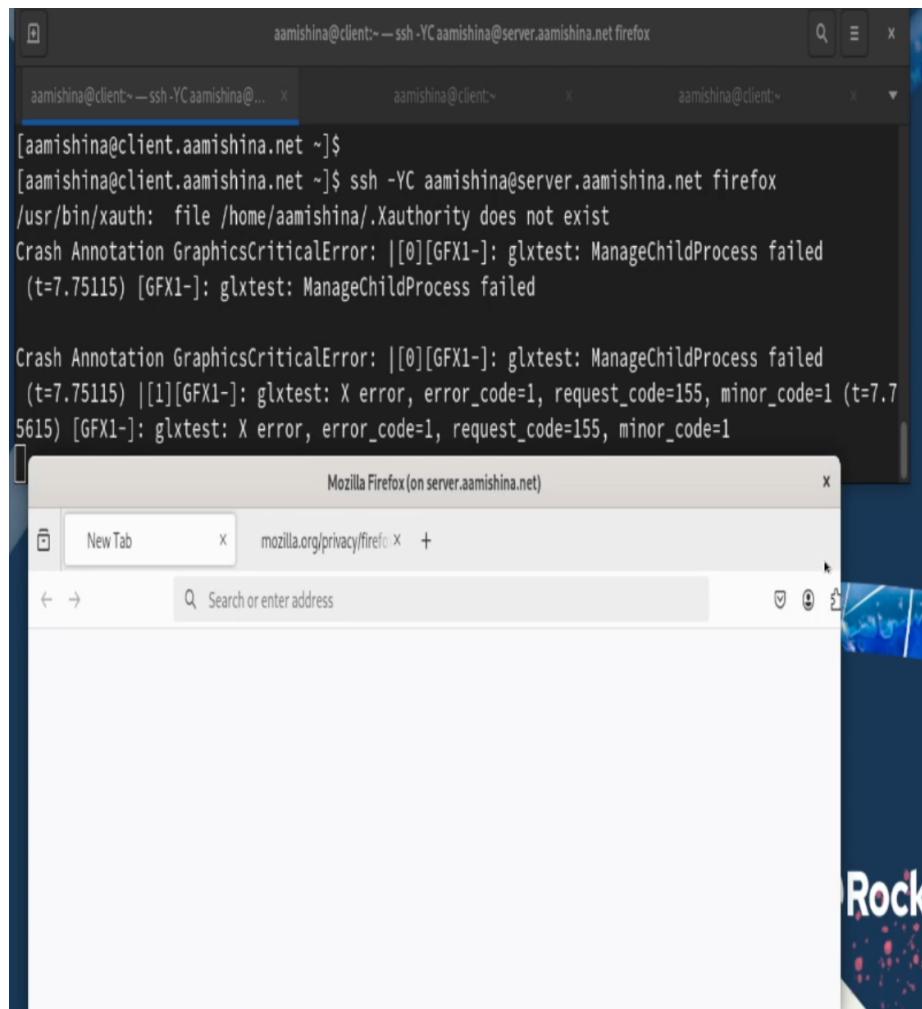


Рис. 2.19: Запуск графического приложения через ssh

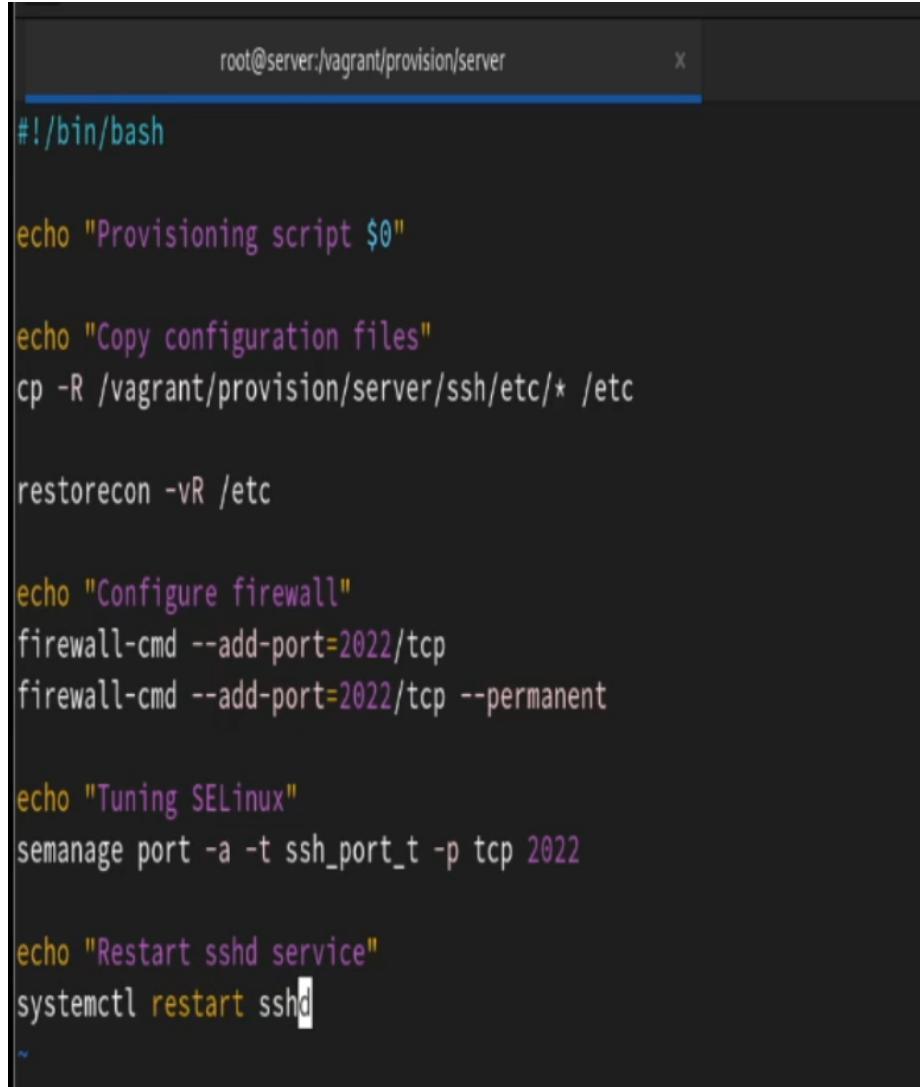
## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем 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 и в каталоге /vagrant/provision/server создадим исполняемый файл ssh.sh(рис. fig. 2.20)

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

Рис. 2.20: Создание окружения для внесения изменений в настройки окружающей среды

Пропишем скрипт в /vagrant/provision/server/ssh.sh (fig. 2.21):



The screenshot shows a terminal window titled "root@server:/vagrant/provision/server". The script content is as follows:

```
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/ssh/etc/* /etc

restorecon -vR /etc

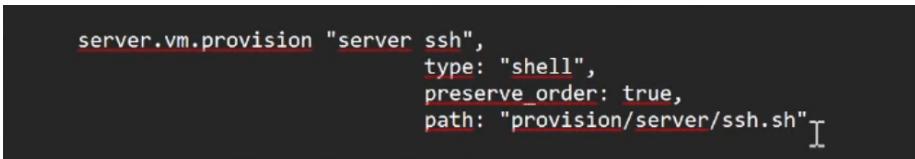
echo "Configure firewall"
firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent

echo "Tuning SELinux"
semanage port -a -t ssh_port_t -p tcp 2022

echo "Restart sshd service"
systemctl restart sshd
```

Рис. 2.21: Скрипт файла /vagrant/provision/server/ssh.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим следующую запись в разделе конфигурации для сервера (fig. 2.22):



```
server.vm.provision "server ssh",
  type: "shell",
  preserve_order: true,
  path: "provision/server/ssh.sh"
```

Рис. 2.22: Изменение конфигурационного файла Vagrant

### 3 Контрольные вопросы

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

В файле /etc/ssh/sshd\_config конфигурации прописать PermitRootLogin no и AllowUsers alice.

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

Для настройки удалённого доступа по SSH через несколько портов нужно отредактировать файл конфигурации SSH и добавить строку Port <порт>.

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

Для установки фонового соединения без команды используется параметр -N при использовании команды ssh: ssh -N <hostname>

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

```
ssh -fNL 80:localhost:5555 server2.example.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 --permanent
```

## **4 Выводы**

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