

Лабораторная работа №11

Администрирование сетевых подсистем

Мишина А. А.

16 ноября 2024

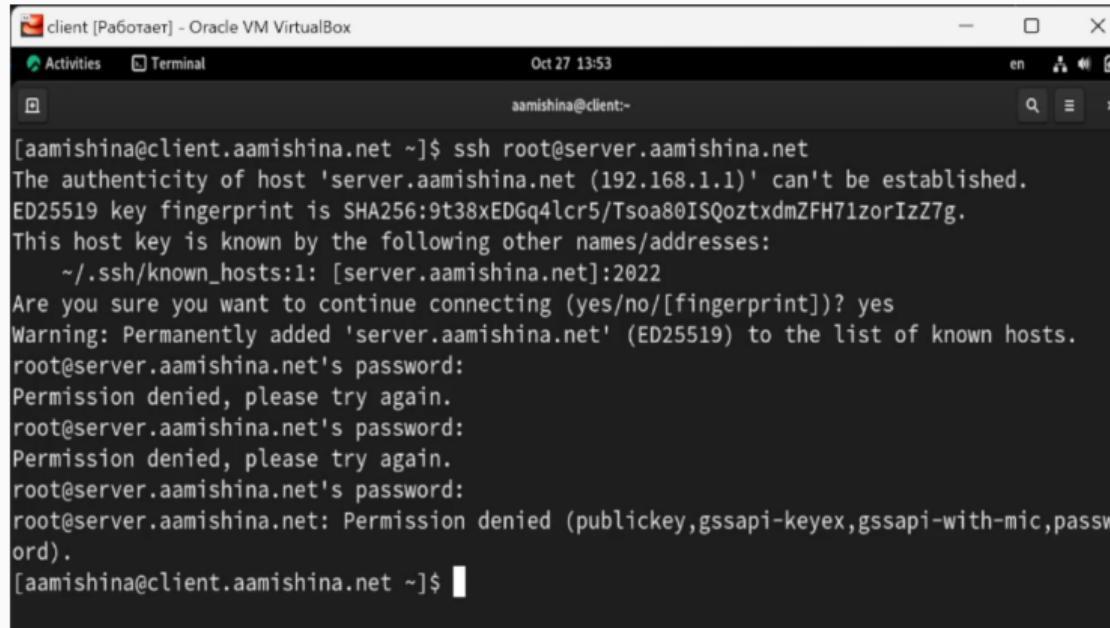
Цель работы

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

Выполнение лабораторной работы

Запрет удалённого доступа по SSH для пользователя root

Запрет удалённого доступа по SSH для пользователя root



The screenshot shows a terminal window titled "client [Работает] - Oracle VM VirtualBox". The terminal interface includes a header bar with "Activities", "Terminal", the date "Oct 27 13:53", and user information "en ⚡ 🔍". The main area displays the following command-line session:

```
[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,ssapi-keyex,ssapi-with-mic,password).
[aamishina@client.aamishina.net ~]$
```

Рис. 1: Попытка установить SSH-соединение

Запрет удалённого доступа по SSH для пользователя root

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

Рис. 2: Файл /etc/ssh/sshd_config. Запрет входа на сервер пользователю root

Ограничение списка пользователей для удалённого доступа по SSH

Ограничение списка пользователей для удалённого доступа по SSH

```
[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. 3: Попытка установить SSH-соединение с клиента

Ограничение списка пользователей для удалённого доступа по SSH

```
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. 4: Файл /etc/ssh/sshd_config. Изменение разрешенных пользователей для sshd

Ограничение списка пользователей для удалённого доступа по SSH

```
[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. 5: Определение службы аутентификации пользователей

Ограничение списка пользователей для удалённого доступа по SSH

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

Рис. 6: Файл /etc/ssh/sshd_config. Изменение разрешенных пользователей для sshd

Ограничение списка пользователей для удалённого доступа по SSH

```
[aamishina@server.aamishina.net ~]$ ssh aamishina@server.aamishina.net
aamishina@server.aamishina.net's password:   I
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. 7: Временный запуск SMTP-сервера

Настройка дополнительных портов для удалённого доступа по SSH

Настройка дополнительных портов для удалённого доступа по SSH

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

Рис. 8: Файл /etc/ssh/sshd_config. Добавление портов в файл конфигураций

Настройка дополнительных портов для удалённого доступа по SSH

```
[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 2222 on 0.0.0.0 failed: Permission denied
Oct 27 14:01:38 server.aamishina.net sshd[10059]: error: Bind to port 2222 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. 9: Расширенный статус работы sshd

Настройка дополнительных портов для удалённого доступа по SSH

```
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.
```

I

Рис. 10: Мониторинг системных сообщений

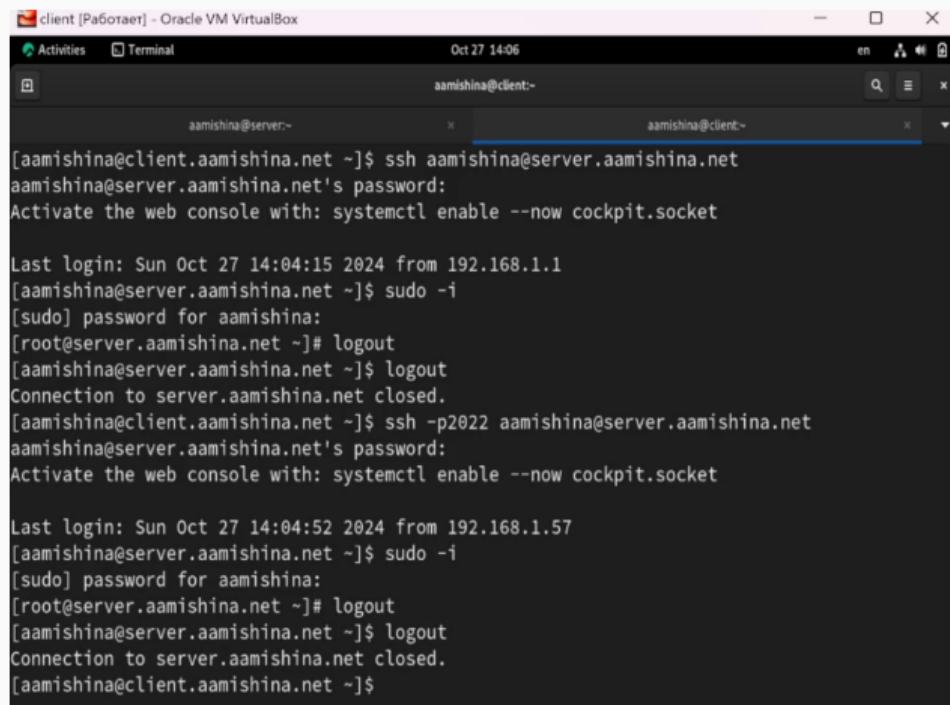
Настройка дополнительных портов для удалённого доступа по SSH

```
[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] @ of 10-100 startup"

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

Настройка дополнительных портов для удалённого доступа по SSH



```
aamishina@client:~]$ 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. 12: Установка SSH-соединение с клиента

Настройка удалённого доступа по SSH по ключу

Настройка удалённого доступа по SSH по ключу

На сервере в конфигурационном файле `/etc/ssh/sshd_config` зададим параметр, разрешающий аутентификацию по ключу, написав:

```
PubkeyAuthentication yes
```

Настройка удалённого доступа по SSH по ключу

```
[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+pX6alcL0 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. 13: Формирования SSH-ключа на клиенте

Настройка удалённого доступа по SSH по ключу

```
[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 th
at 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. 14: Установка SSH-соединения с сервером с клиента

Организация туннелей SSH,
перенаправление TCP-портов

Организация туннелей SSH, перенаправление TCP-портов

```
[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. 15: Просмотр активных служб с протоколом TCP. Перенаправление порта 80 на server.aamishina.net на порт 8080

Организация туннелей SSH, перенаправление TCP-портов

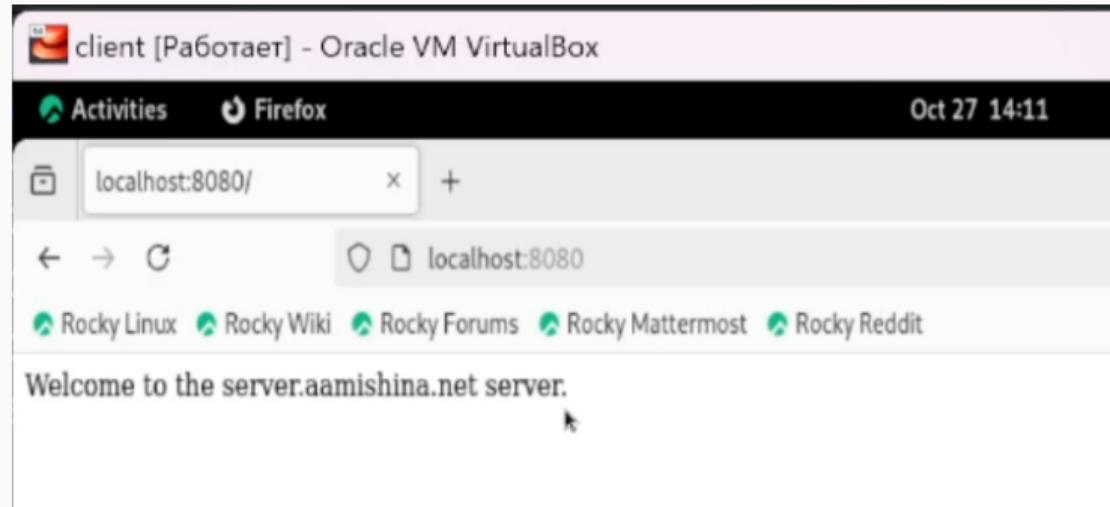


Рис. 16: Просмотр локального сервера в браузере на клиенте

Запуск консольных приложений через SSH

Запуск консольных приложений через SSH

```
[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. 4 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-r----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-clipboard-tty1-control.pid  
-rw-r----. 1 aamishina aamishina 5 Oct 27 13:46 .vboxclient-clipboard-tty1-service.pid  
-rw-r----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-draganddrop-tty1-control.pid  
-rw-r----. 1 aamishina aamishina 5 Oct 27 13:46 .vboxclient-draganddrop-tty1-service.pid  
-rw-r----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-hostversion-tty1-control.pid  
-rw-r----. 1 aamishina aamishina 6 Oct 27 13:46 .vboxclient-seamless-tty1-control.pid
```

Рис. 17: Просмотр имени узла сервера и файлов на сервере через ssh

Запуск консольных приложений 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. 18: Просмотр почты через ssh

Запуск графических приложений через SSH (X11Forwarding)

Запуск графических приложений через SSH (X11Forwarding)

На сервере в конфигурационном файле /etc/ssh/sshd_config разрешим отображать на локальном клиентском компьютере графические интерфейсы X11, прописав:

```
X11Forwarding yes
```

Запуск графических приложений через SSH (X11Forwarding)

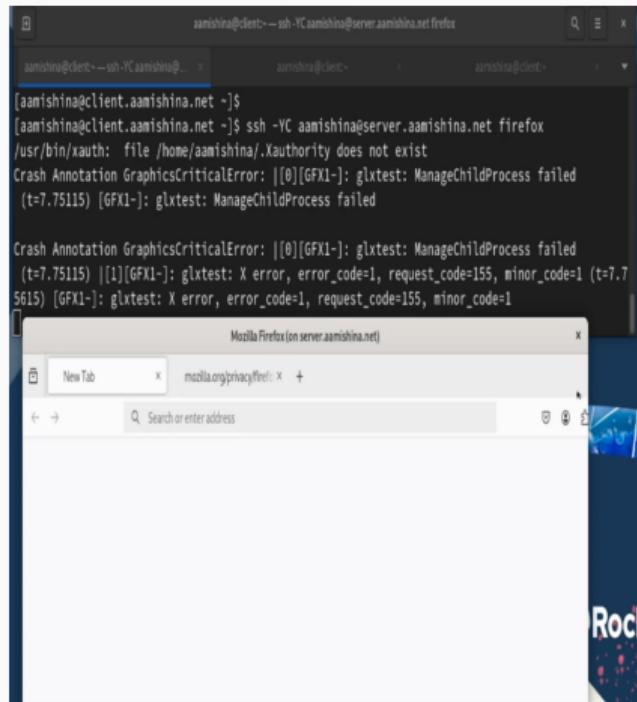


Рис. 19: Запуск графического приложения через ssh

Внесение изменений в настройки внутреннего окружения виртуальной машины

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
[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. 20: Создание окружения для внесения изменений в настройки окружающей среды

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
root@server:/vagrant/provision/server
#!/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. 21: Скрипта файла /vagrant/provision/server/ssh.sh

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Рис. 22: Изменение конфигурационного файла Vagrant

Вывод

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