

Лабораторная работа №11

Администрирование сетевых подсистем

Иванов Сергей Владимирович, НПИбд-01-23

5 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Задание

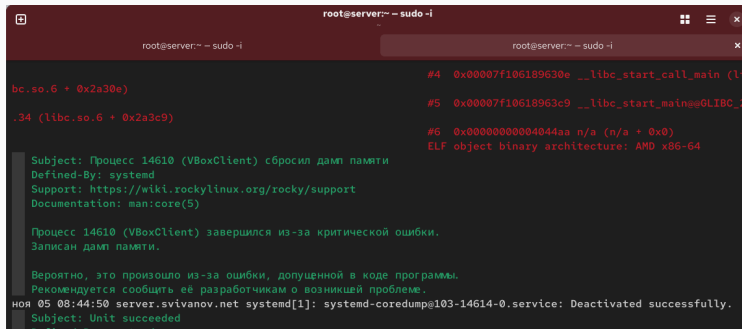
Задание

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

Выполнение лабораторной работы

Запрет удалённого доступа по SSH для пользователя root

На сервере в дополнительном терминале запустим мониторинг системных событий: (рис. 1).



```
root@server:~ - sudo -i
root@server:~ - sudo -i
root@server:~ - sudo -i

bc.so.6 + 0x2a30e)
#4 0x00007f106189630e __libc_start_call_main (li
#5 0x00007f10618963c9 __libc_start_main@@GLIBC_2
#6 0x00000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86-64

Subject: Процесс 14610 (VBoxClient) сбросил дамп памяти
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support
Documentation: man:core(5)

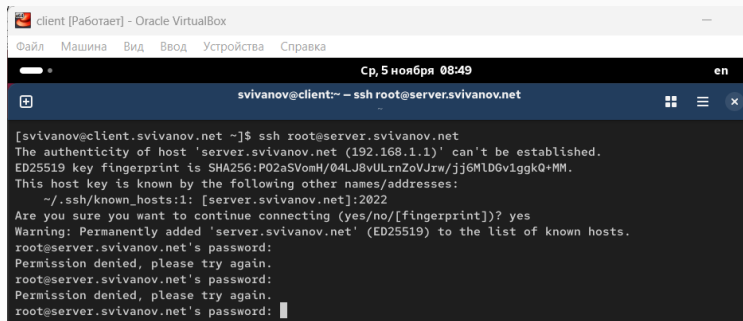
Процесс 14610 (VBoxClient) завершился из-за критической ошибки.
Записан дамп памяти.

Вероятно, это произошло из-за ошибки, допущенной в коде программы.
Рекомендуется сообщить её разработчикам о возникшей проблеме.
ноя 05 08:44:50 server.svivanov.net systemd[1]: systemd-coredump@103-14614-0.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
```

Рис. 1: Запуск мониторинга

Запрет удалённого доступа по SSH для пользователя root

С клиента попытаемся получить доступ к серверу через пользователя root: (рис. 2).



```
client [Работает] - Oracle VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Ср, 5 ноября 08:49  en
svivanov@client:~ - ssh root@server.svivanov.net

[svivanov@client.svivanov.net ~]$ ssh root@server.svivanov.net
The authenticity of host 'server.svivanov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:PO2aSVomH/04LJ8vULrnZoVJrw/jj6MLDGvlggkQ+MM.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.svivanov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.svivanov.net' (ED25519) to the list of known hosts.
root@server.svivanov.net's password:
Permission denied, please try again.
root@server.svivanov.net's password:
Permission denied, please try again.
root@server.svivanov.net's password: 
```

Рис. 2: Попытка получить доступ к серверу по SSH

Запрет удалённого доступа по SSH для пользователя root

На сервере откроем файл `/etc/ssh/sshd_config` для редактирования и запретим вход пользователю root (рис. 3)

```
#PasswordAuthentication yes
#PermitEmptyPasswords no

PermitRootLogin no

# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes
```

Рис. 3: Запрет входа для root

Запрет удалённого доступа по SSH для пользователя root

Перезапустим sshd (рис. 4)

```
[root@server.svivanov.net ssh]# systemctl restart sshd  
[root@server.svivanov.net ssh]#
```

Рис. 4: Перезапуск sshd

Запрет удалённого доступа по SSH для пользователя root

Повторим попытку получения доступа с клиента к серверу (рис. 5)

!

```
[svivanov@client.svivanov.net ~]$ ssh root@server.svivanov.net
root@server.svivanov.net's password:
Permission denied, please try again.
root@server.svivanov.net's password:
Permission denied, please try again.
root@server.svivanov.net's password:
Connection closed by 192.168.1.1 port 22
[svivanov@client.svivanov.net ~]$
[svivanov@client.svivanov.net ~]$
[svivanov@client.svivanov.net ~]$ ssh root@server.svivanov.net
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.1.1 port 22
```

Рис. 5: Попытка подключения

Ограничение списка пользователей для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу через пользователя user (рис. 6)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Web console: https://server.svivanov.net:9090/ or https://192.168.1.1:9090/

Last login: Wed Nov  5 08:36:21 2025
[svivanov@server.svivanov.net ~]$
```

Рис. 6: Попытка подключения юзера к серверу

Ограничение списка пользователей для удалённого доступа по SSH

На сервере откроем файл `/etc/ssh/sshd_config` и добавим строку `AllowUsers vagrant` (рис. 7)

```
PermitRootLogin no

AllowUsers vagrant
# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes
```

Рис. 7: Редактирование `sshd_config`

Ограничение списка пользователей для удалённого доступа по SSH

Перезапустим sshd. Повторим попытку получения доступа с клиента к серверу. (рис. 8)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Permission denied, please try again.
svivanov@server.svivanov.net's password: █
```

Рис. 8: Попытка подключения к серверу

Ограничение списка пользователей для удалённого доступа по SSH

В файле `/etc/ssh/sshd_config` внесем следующее изменение: (рис. 9)

```
PermitRootLogin no

AllowUsers vagrant svivanov
# Change to no to disable s/key passwords
#KbdInteractiveAuthentication yes
```

Рис. 9: Редактирование `sshd_config`

Ограничение списка пользователей для удалённого доступа по SSH

Перезапустим sshd и попытаемся получить доступ с клиента к серверу (рис. 10)

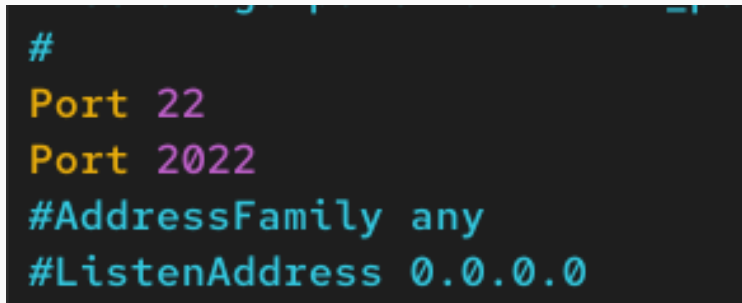
```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Web console: https://server.svivanov.net:9090/ or https://192.168.1.1:9090/

Last failed login: Wed Nov  5 09:23:55 UTC 2025 from 192.168.1.30 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Wed Nov  5 09:04:23 2025 from 192.168.1.30
[svivanov@server.svivanov.net ~]$
```

Рис. 10: Попытка подключения к серверу

Настройка дополнительных портов для удалённого доступа по SSH

На сервере в файле `sshd /etc/ssh/sshd_config` найдем строку `Port` и добавим (рис. 11)

A screenshot of a terminal window showing the configuration of the sshd_config file. The text is as follows:

```
#  
Port 22  
Port 2022  
#AddressFamily any  
#ListenAddress 0.0.0.0
```

The word "Port" is highlighted in yellow, and the port numbers "22" and "2022" are highlighted in purple. The other text is in a light blue/cyan color on a dark background.

Рис. 11: Редактирование `sshd_config`

Настройка дополнительных портов для удалённого доступа по SSH

Перезапустим sshd. Посмотрим расширенный статус работы sshd. (рис. 12)

```
[root@server.svivanov.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-11-05 09:09:26 UTC; 8s ago
     Invocation: 97945e4d425042a4a99c6e7dcaef7c41
       Docs: man:sshd(8)
            man:sshd_config(5)
    Main PID: 17964 (sshd)
      Tasks: 1 (limit: 23144)
     Memory: 1M (peak: 1.4M)
        CPU: 8ms
     CGroup: /system.slice/sshd.service
            └─17964 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

ноя 05 09:09:26 server.svivanov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
ноя 05 09:09:26 server.svivanov.net (sshd)[17964]: sshd.service: Referenced but unset environment variable evaluat
ноя 05 09:09:26 server.svivanov.net sshd[17964]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
ноя 05 09:09:26 server.svivanov.net sshd[17964]: error: Bind to port 2022 on :: failed: Permission denied.
ноя 05 09:09:26 server.svivanov.net sshd[17964]: Server listening on 0.0.0.0 port 22.
ноя 05 09:09:26 server.svivanov.net sshd[17964]: Server listening on :: port 22.
ноя 05 09:09:26 server.svivanov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
[...]
```

Рис. 12: Перезапуск и просмотр статуса службы

Настройка дополнительных портов для удалённого доступа по SSH

Дополнительно посмотрим сообщения в терминале с мониторингом системных событий. (рис. 13)

```
ноя 05 09:09:55 server.svivanov.net named[1295]: timed out resolving 'cac-ocsp.digicert.com.edgekey.net/A/IN': 127.0.0.1#53
ноя 05 09:09:55 server.svivanov.net named[1295]: timed out resolving 'cac-ocsp.digicert.com.edgekey.net/AAAA/IN': 127.0.0.1#53
ноя 05 09:09:56 server.svivanov.net named[1295]: timed out resolving 'com.edgekey.net/NS/IN': 127.0.0.1#53
ноя 05 09:09:56 server.svivanov.net named[1295]: timed out resolving 'com.edgekey.net/NS/IN': 127.0.0.1#53
ноя 05 09:09:57 server.svivanov.net named[1295]: timed out resolving 'ultradns.info/NS/IN': 127.0.0.1#53
ноя 05 09:09:57 server.svivanov.net named[1295]: timed out resolving 'ultradns.info/NS/IN': 127.0.0.1#53
ноя 05 09:09:59 server.svivanov.net named[1295]: shut down hung fetch while resolving 'pdns5.ultradns.info/A'
ноя 05 09:09:59 server.svivanov.net named[1295]: shut down hung fetch while resolving 'pdns5.ultradns.info/AAAA'
ноя 05 09:10:00 server.svivanov.net kernel: traps: VBoxClient[18098] trap int3 ip:41dd1b sp:7f1053235cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
ноя 05 09:10:00 server.svivanov.net systemd-coredump[18099]: Process 18095 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
ноя 05 09:10:00 server.svivanov.net systemd[1]: Started systemd-coredump@397-18099-0.service - Process Core Dump (PID 18099/UID 0).
Subject: Запуск юнита systemd-coredump@397-18099-0.service завершен
```

Рис. 13: Просмотр мониторинга системных событий

Исправим на сервере метки SELinux к порту 2022: (рис. 14)

```
[root@server.svivanov.net ssh]# semanage port -a -t ssh_port_t -p tcp 2022  
[root@server.svivanov.net ssh]#
```

Рис. 14: Исправление меток SELinux

Настройка дополнительных портов для удалённого доступа по SSH

В настройках межсетевого экрана откроем порт 2022 протокола TCP (рис. 15)

```
[root@server.svivanov.net ssh]# firewall-cmd --add-port=2022/tcp  
success  
[root@server.svivanov.net ssh]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@server.svivanov.net ssh]#
```

Рис. 15: Настройка firewall

Настройка дополнительных портов для удалённого доступа по SSH

Перезапустим sshd и посмотрим расширенный статус его работы. (рис. 16)

```
[root@server.svivanov.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-11-05 09:13:21 UTC; 8s ago
     Invocation: 4d24ff3b2a584e61bff839c4f8452d17
       Docs: man:sshd(8)
            man:sshd_config(5)
    Main PID: 18701 (sshd)
      Tasks: 1 (limit: 23144)
     Memory: 1M (peak: 1.2M)
        CPU: 9ms
     CGroup: /system.slice/sshd.service
            └─18701 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

ноя 05 09:13:21 server.svivanov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
ноя 05 09:13:21 server.svivanov.net (sshd)[18701]: sshd.service: Referenced but unset environment variable evalu
ноя 05 09:13:21 server.svivanov.net sshd[18701]: Server listening on 0.0.0.0 port 2022.
ноя 05 09:13:21 server.svivanov.net sshd[18701]: Server listening on :: port 2022.
ноя 05 09:13:21 server.svivanov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
ноя 05 09:13:21 server.svivanov.net sshd[18701]: Server listening on 0.0.0.0 port 22.
ноя 05 09:13:21 server.svivanov.net sshd[18701]: Server listening on :: port 22.
lines 1-20/20 (END)
```

Рис. 16: Перезапуск службы и просмотр статуса

Настройка дополнительных портов для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу через пользователя (рис. 17)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Web console: https://server.svivanov.net:9090/ or https://192.168.1.1:9090/

Last login: Wed Nov  5 09:30:18 2025 from 192.168.1.30
[svivanov@server.svivanov.net ~]$ sudo -i
[sudo] пароль для svivanov:
[root@server.svivanov.net ~]#
logout
[svivanov@server.svivanov.net ~]$
logout
Connection to server.svivanov.net closed.
[svivanov@client.svivanov.net ~]$
```

Рис. 17: Подключение к серверу, получение root

Настройка дополнительных портов для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу через пользователя, указав порт 2022 (рис. 18)

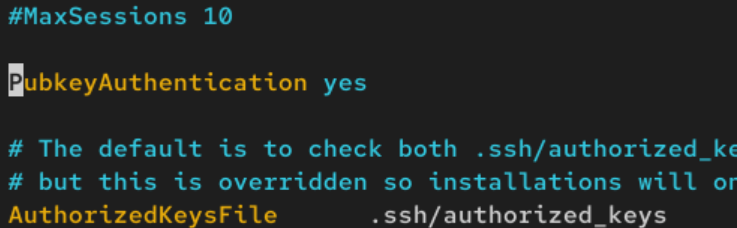
```
[svivanov@client.svivanov.net ~]$ ssh -p 2022 svivanov@server.svivanov.net
svivanov@server.svivanov.net's password:
Web console: https://server.svivanov.net:9090/ or https://192.168.1.1:9090/

Last login: Wed Nov  5 09:28:19 2025 from 192.168.1.30
[svivanov@server.svivanov.net ~]$ sudo -i
[sudo] пароль для svivanov:
[root@server.svivanov.net ~]#
logout
[svivanov@server.svivanov.net ~]$
logout
Connection to server.svivanov.net closed.
[svivanov@client.svivanov.net ~]$
```

Рис. 18: Подключение к серверу через порт 2022, получение root

Настройка удалённого доступа по SSH по ключу

На сервере в файле `/etc/ssh/sshd_config` зададим параметр, разрешающий аутентификацию по ключу. (рис. 19)



```
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys
# but this is overridden so installations will or
AuthorizedKeysFile .ssh/authorized_keys
```

Рис. 19: Редактирование `sshd_config`

Настройка удалённого доступа по SSH по ключу

На клиенте сформируем SSH-ключ (рис. 20)

```
[svivanov@client.svivanov.net ~]$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/svivanov/.ssh/id_ed25519):
Enter passphrase for "/home/svivanov/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/svivanov/.ssh/id_ed25519
Your public key has been saved in /home/svivanov/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:2xP6gV3nysu/bz/LH2wwT/5fLWcc5ai0XCQkMzUNFJE svivanov@client.svivanov.net
The key's randomart image is:
+--[ED25519 256]--+
|      .B*      |
|      .E..     |
|      + . .    |
|      =       o.|
|      S o oooo.|
|      * = +B.o|
|      + = o o**|
```

Рис. 20: Создание SSH ключа

Настройка удалённого доступа по SSH по ключу

Скопируем открытый ключ на сервер (рис. 21)

```
[svivanov@client.svivanov.net ~]$ ssh-copy-id svivanov@server.svivanov.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
/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
svivanov@server.svivanov.net's password:

Number of key(s) added: 1

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

[svivanov@client.svivanov.net ~]$
```

Рис. 21: Копирование ключа на сервер

Настройка удалённого доступа по SSH по ключу

Попробуем получить доступ с клиента к серверу: (рис. 22)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net
Web console: https://server.svivanov.net:9090/ or https://192.168.1.1:9090/

Last login: Wed Nov  5 09:31:48 2025 from 192.168.1.30
[svivanov@server.svivanov.net ~]$
logout
Connection to server.svivanov.net closed.
[svivanov@client.svivanov.net ~]$
```

Рис. 22: Подключение к серверу

Организация туннелей SSH, перенаправление TCP-портов

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP (рис. 23)

```
[svivanov@client.svivanov.net ~]$ lsof | grep TCP
ssh      12257      svivanov    3u    IPv4        36426      0t0      TCP c
lient.svivanov.net:45222->dhcp.svivanov.net:ssh (CLOSE_WAIT)
ssh      13472      svivanov    3u    IPv4        55639      0t0      TCP c
lient.svivanov.net:51904->dhcp.svivanov.net:ssh (CLOSE_WAIT)
ssh      15004      svivanov    3u    IPv4        79682      0t0      TCP c
lient.svivanov.net:52562->dhcp.svivanov.net:ssh (CLOSE_WAIT)
ssh      16886      svivanov    3u    IPv4       107826      0t0      TCP c
lient.svivanov.net:43650->dhcp.svivanov.net:ssh (CLOSE_WAIT)
ssh      17011      svivanov    3u    IPv4       110889      0t0      TCP c
lient.svivanov.net:47038->dhcp.svivanov.net:ssh (CLOSE_WAIT)
[svivanov@client.svivanov.net ~]$
```

Рис. 23: Просмотр служб с протоколом TCP

Перенаправим порт 80 на server.user.net на порт 8080 на локальной машине (рис. 24)

```
[svivanov@client.svivanov.net ~]$ ssh -fNL 8080:localhost:80 svivanov@server.svivanov.net  
[svivanov@client.svivanov.net ~]$
```

Рис. 24: Перенаправление порта

Организация туннелей SSH, перенаправление TCP-портов

Вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP (рис. 25)

```
[svivanov@client.svivanov.net ~]$ lsof | grep TCP
ssh      12257      svivanov    3u      IPv4        36426      0t0      TCP client.svivanov.net:45222->www.svivanov.net:ssh
ssh      13472      svivanov    3u      IPv4        55639      0t0      TCP client.svivanov.net:51904->www.svivanov.net:ssh
ssh      15004      svivanov    3u      IPv4        79682      0t0      TCP client.svivanov.net:52562->www.svivanov.net:ssh
ssh      16886      svivanov    3u      IPv4        107826     0t0      TCP client.svivanov.net:43650->www.svivanov.net:ssh
ssh      17011      svivanov    3u      IPv4        110889     0t0      TCP client.svivanov.net:47038->www.svivanov.net:ssh
ssh      24587      svivanov    3u      IPv4        245921     0t0      TCP client.svivanov.net:51262->www.svivanov.net:ssh
ssh      24587      svivanov    4u      IPv6        245929     0t0      TCP localhost:webcache (LISTEN)
ssh      24587      svivanov    5u      IPv4        245930     0t0      TCP localhost:webcache (LISTEN)
[svivanov@client.svivanov.net ~]$
```

Рис. 25: Просмотр служб с протоколом TCP

Организация туннелей SSH, перенаправление TCP-портов

На клиенте запустим браузер и в адресной строке введем localhost:8080. (рис. 26)

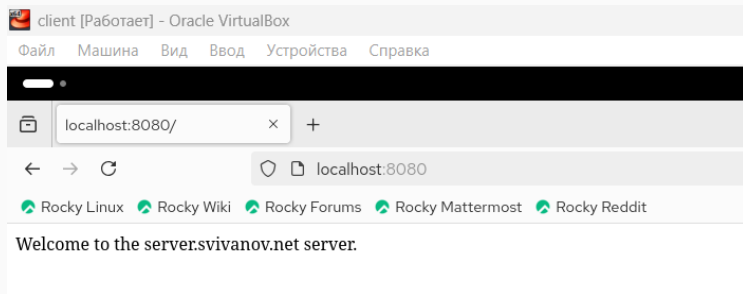


Рис. 26: Страница с приветствием в браузере

Запуск консольных приложений через SSH

Посмотрим с клиента имя узла сервера и список файлов на сервере: (рис. 27)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net hostname
server.svivanov.net
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net ls -Al
total 64
drwxr-xr-x.  2 svivanov svivanov 4096 сен 22 14:47 aus
-rw-----.  1 svivanov svivanov  800 ноя  5 09:31 .bash_history
-rw-r--r--.  1 svivanov svivanov   18 окт 29  2024 .bash_logout
-rw-r--r--.  1 svivanov svivanov  144 окт 29  2024 .bash_profile
-rw-r--r--.  1 svivanov svivanov  603 сен  4 13:30 .bashrc
drwx-----. 12 svivanov svivanov 4096 сен  9 09:35 .cache
drwx-----. 13 svivanov svivanov 4096 сен 22 14:45 .config
drwx-----.  4 svivanov svivanov   32 сен  4 13:06 .local
drwx-----.  5 svivanov svivanov 4096 окт 27 11:30 Maildir
drwxr-xr-x.  5 svivanov svivanov   54 сен  9 09:35 .mozilla
drwx-----.  2 svivanov svivanov   29 ноя  5 10:20 .ssh
```

Рис. 27: Просмотр файлов на сервере

Запуск консольных приложений через SSH

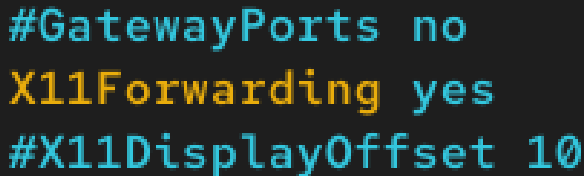
Посмотрим с клиента почту на сервере (рис. 28)

```
[svivanov@client.svivanov.net ~]$ ssh svivanov@server.svivanov.net MAIL=~/.Maildir/ mail
s-nail version v14.9.24. Type '?' for help
/home/svivanov/Maildir: 11 messages 4 deleted
▶ 1 Sergey Ivanov      2025-10-18 08:40   18/674   "Тест 2"           "
  2 Sergey Ivanov      2025-10-18 08:39   19/782   "Тестирование"      "
  3 Sergey Ivanov      2025-10-18 08:46   18/648   "Тест 4"           "
  4 Sergey Ivanov      2025-10-18 09:06   18/628   "Test 5"           "
  5 svivanov@client.sviv 2025-10-25 09:29   21/803   "LMTP test"         "
  6 Sergey Ivanov      2025-10-25 15:52   22/791   "efwef"             "
 11 Sergey Ivanov      2025-10-27 11:30   22/823   "uifijewhiewlighierhig"
```

Рис. 28: Просмотр почты на сервере

Запуск графических приложений через SSH (X11Forwarding)

На сервере в файле `/etc/ssh/sshd_config` разрешим отображать на клиентском компьютере графические интерфейсы X11. (рис. 29)

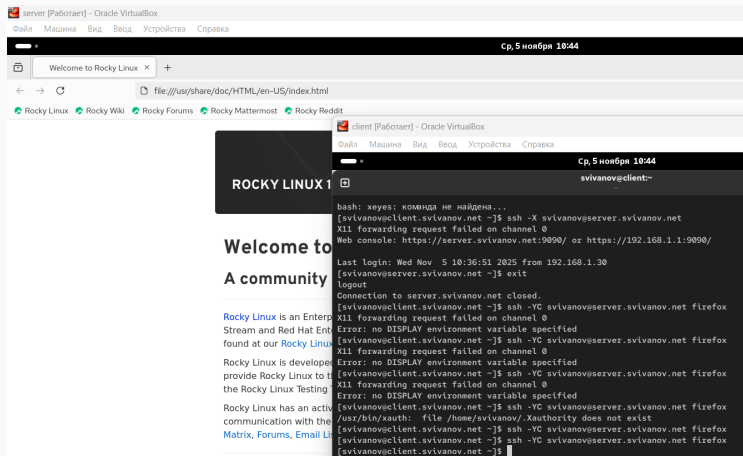
A screenshot of a terminal window showing the configuration of the sshd_config file. The text is displayed in a monospaced font with syntax highlighting: '#GatewayPorts no' in cyan, 'X11Forwarding yes' in yellow, and '#X11DisplayOffset 10' in cyan.

```
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
```

Рис. 29: Редактирование `sshd_config`

Запуск графических приложений через SSH (X11Forwarding)

Перезапустим sshd. Попробуем с клиента удалённо подключиться к серверу и запустить firefox. (рис. 30)



Внесение изменений в настройки внутреннего окружения виртуальной машины

На машине `server` перейдем в каталог для внесения изменений в настройки внутреннего окружения. В соответствующие подкаталоги поместим конф. файлы `sshd_config`: (рис. 31)

```
[root@server.svivanov.net ssh]# cd /vagrant/provision/server  
[root@server.svivanov.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh  
[root@server.svivanov.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/  
[root@server.svivanov.net server]#
```

Рис. 31: Замена конф. файлов

Внесение изменений в настройки внутреннего окружения виртуальной машины

В каталоге `/vagrant/provision/server` создадим исполняемый файл `ssh.sh` и пропишем в нём следующий скрипт: (рис. 32)

```
#!/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
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

Для отработки скрипта во время загрузки виртуальной машины server в Vagrantfile необходимо добавить: (рис. 33)

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

Рис. 33: Коррекция vagrantfile

В ходе выполнения лабораторной работы мы приобрели практические навыки по настройке удалённого доступа к серверу с помощью SSH.