Лабораторная работа № 11. Настройка безопасного удалённого доступа по протоколу SSH

Сущенко Алина
НПИбд-01-23

Российский университет дружбы народов имени Патриса Лумумбы

2025

Цель работы

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

Запрет удалённого доступа по SSH для пользователя root

```
[vagrant@server ~]$ sudo -i
[root@server ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server ~]#
```

Рис.: Задание пароля для пользователя root.

Запрет удалённого доступа по SSH для пользователя root

Запретили пользователю root подключение к серверу через SSH:

```
PermitRootLogin no
```

```
[vagrant@client ~]$ ssh root@server.ansusenko.net
The authenticity of host 'server.ansusenko.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:2uFslNbEsrU0NmX8+xPyOPR+k41WG+FIucs+olmyc6c.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'server.ansusenko.net' (ED25519) to the list of known hosts.
root@server.ansusenko.net's password:
Permission denied, please try again.
root@server.ansusenko.net's password:
Permission denied, please try again.
root@server.ansusenko.net's password:
```

Рис.: Подключение к серверу через SSH-соединение.

Ограничение списка пользователей для удалённого доступа по SSH

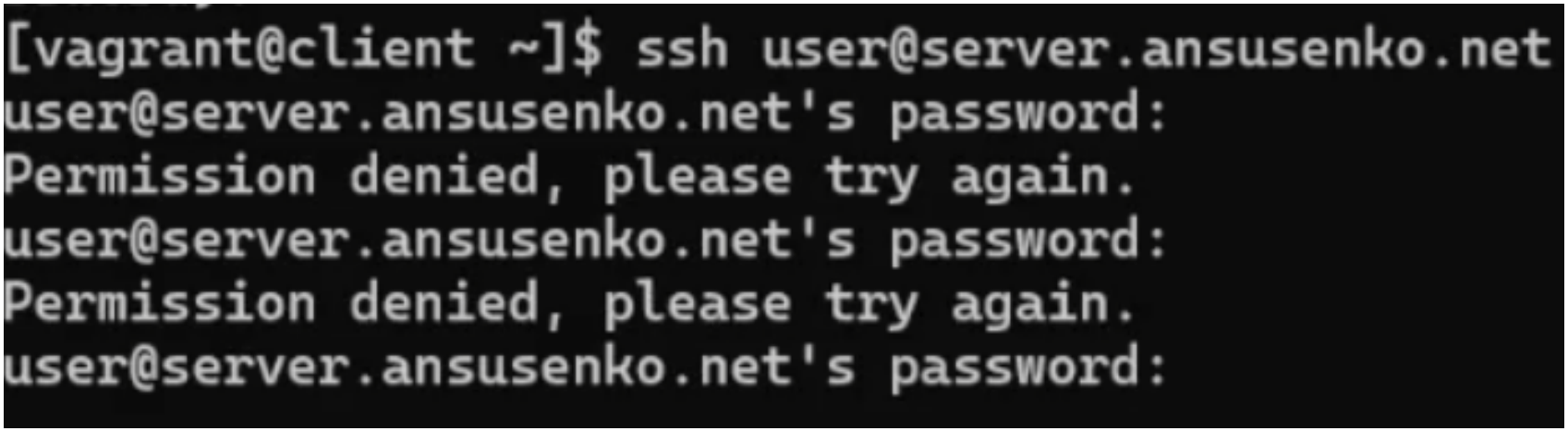

Рис.: Успешное подключение к серверу пользователем ansusenko.

Ограничение списка пользователей для удалённого доступа по SSH

Явно указали разрешенных к подключению пользователей:

```
AllowUsers vagrant
```

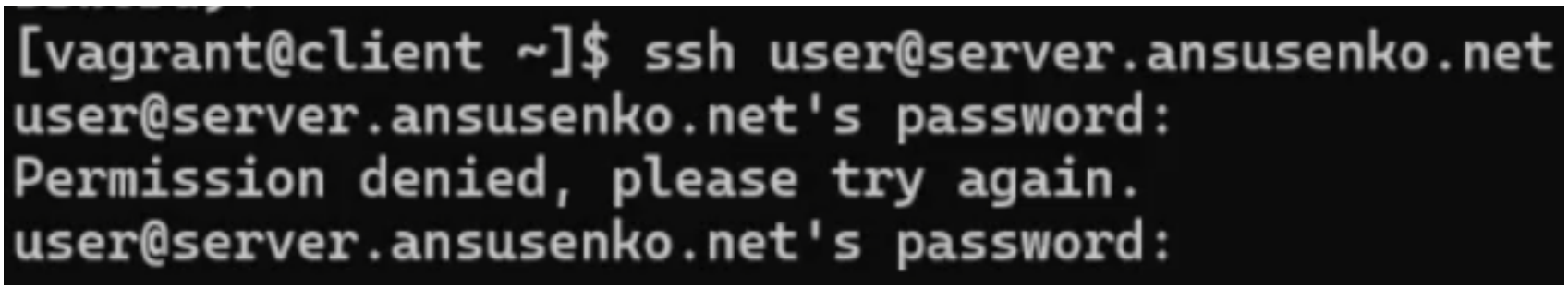

Рис.: Отказ в доступе на сервер пользователю ansusenko.

Ограничение списка пользователей для удалённого доступа по SSH

Обновили список разрешенных пользователей:

```
AllowUsers vagrant ansusenko
```

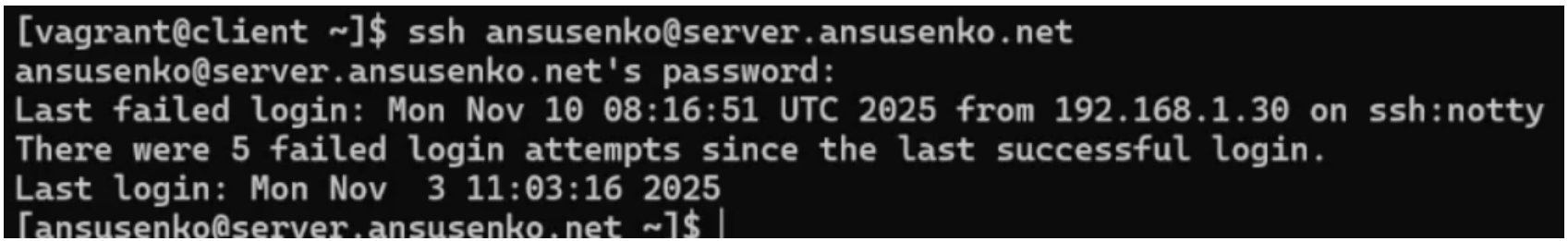

Рис.: Восстановление доступа на сервер пользователю ansusenko.

Настройка дополнительных портов для удалённого доступа по SSH

В файле конфигурации `sshd_config` добавили строки:

```
Port 22
Port 2022
```

```
[root@server ~]# systemctl restart sshd
[root@server ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-11-10 09:10:42 UTC; 7s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 8890 (sshd)
      Tasks: 1 (limit: 4656)
     Memory: 1.4M
        CPU: 7ms
     CGroup: /system.slice/sshd.service
             └─8890 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 10 09:10:42 server.ansusenko.net systemd[1]: Starting OpenSSH server daemon...
Nov 10 09:10:42 server.ansusenko.net sshd[8890]: Server listening on 0.0.0.0 port 2022.
Nov 10 09:10:42 server.ansusenko.net sshd[8890]: Server listening on :: port 2022.
Nov 10 09:10:42 server.ansusenko.net sshd[8890]: Server listening on 0.0.0.0 port 22.
Nov 10 09:10:42 server.ansusenko.net sshd[8890]: Server listening on :: port 22.
Nov 10 09:10:42 server.ansusenko.net systemd[1]: Started OpenSSH server daemon.
```

Рис.: Проверка расширенного статуса работы sshd.

Настройка дополнительных портов для удалённого доступа по SSH

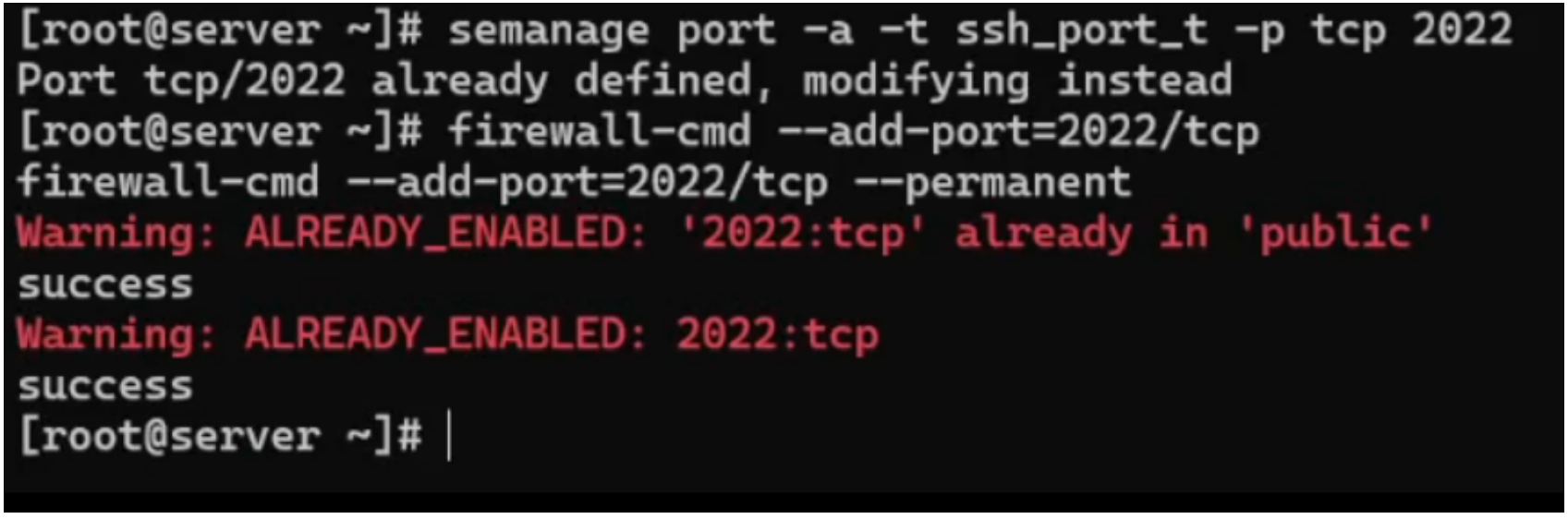

Рис.: Настройка межсетевого экрана.

Настройка дополнительных портов для удалённого доступа по SSH

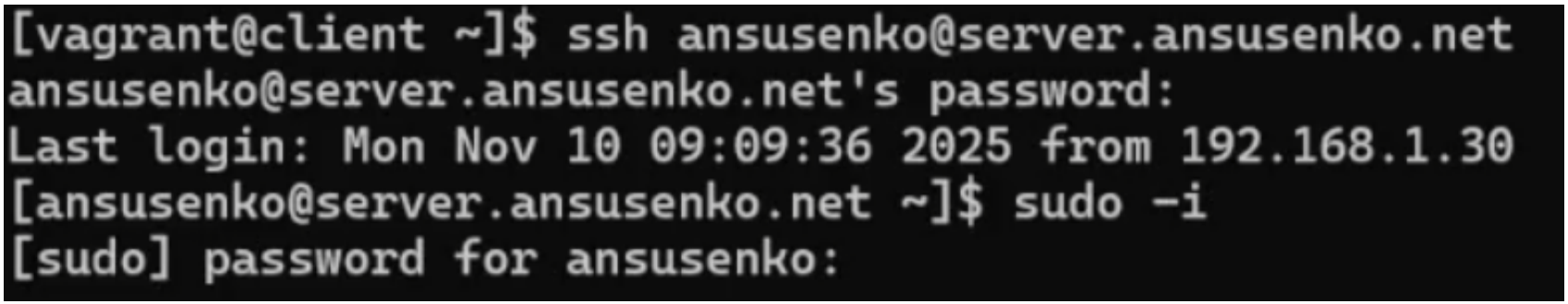

Рис.: Успешное подключение к серверу.

Настройка дополнительных портов для удалённого доступа по SSH

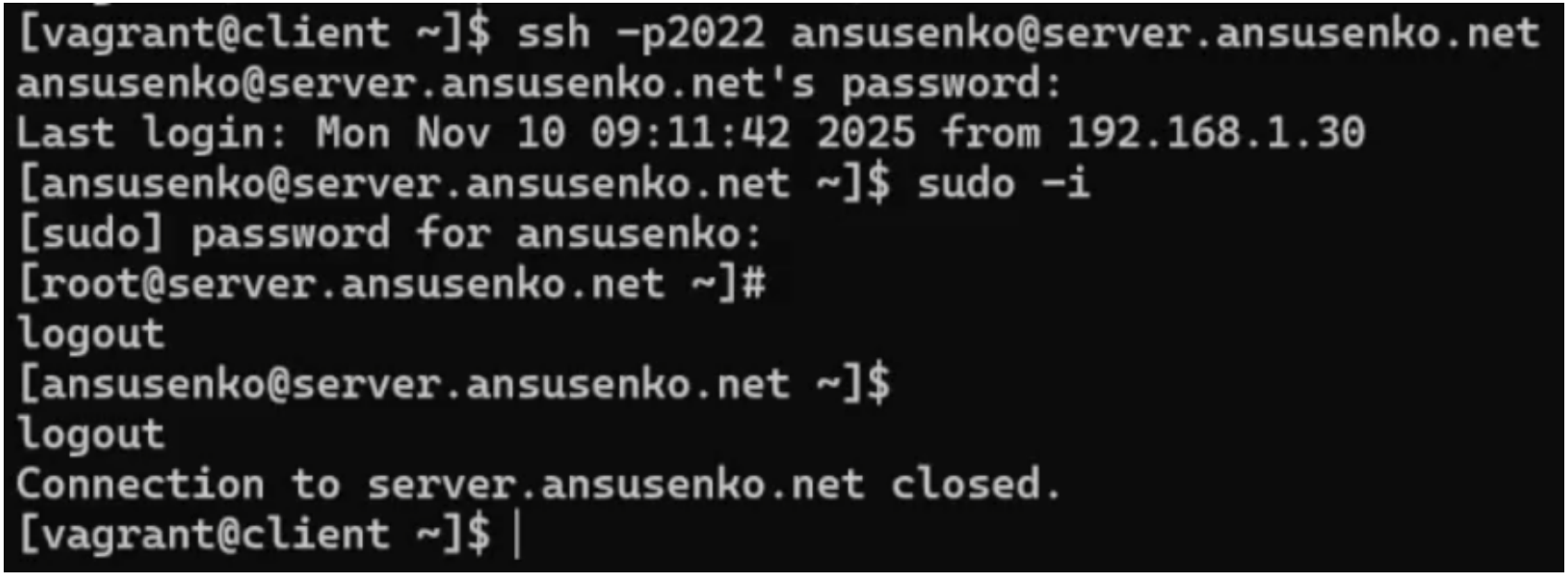

Рис.: Успешное подключение к серверу по порту 2022.

Настройка удалённого доступа по SSH по ключу

```
[ansusenko@client.ansusenko.net ~]$ ssh-copy-id ansusenko@server.ansusenko.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ansusenko/.ssh/id_
rsa.pub"
The authenticity of host 'server.ansusenko.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:2uFslNbEsrU0NmX8+xPyOPR+k41WG+FIucs+olmyc6c.
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
ansusenko@server.ansusenko.net's password:
```

Рис.: Копирование открытого ключа на сервер.

Настройка удалённого доступа по SSH по ключу

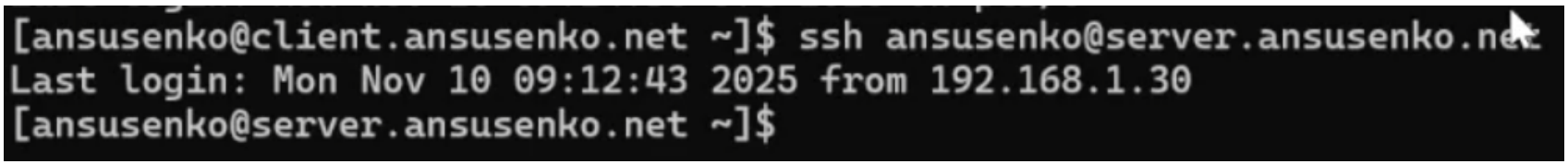

Рис.: Успешное подключение к серверу с использованием SSH-ключа.

Организация туннелей SSH, перенаправление TCP-портов

```
[root@client.ansusenko.net ~]# lsof | grep TCP
sshd       854                    root    3u     IPv4              21723      0t0
   TCP *:ssh (LISTEN)
sshd       854                    root    4u     IPv6              21732      0t0
   TCP *:ssh (LISTEN)
master     989                    root   13u     IPv4              22485      0t0
   TCP localhost:smtp (LISTEN)
sshd      8711                    root    4u     IPv4              38904      0t0
   TCP client.ansusenko.net:ssh->10.0.2.2:52032 (ESTABLISHED)
sshd      8725                 vagrant    4u     IPv4              38904      0t0
   TCP client.ansusenko.net:ssh->10.0.2.2:52032 (ESTABLISHED)
[root@client.ansusenko.net ~]# ssh -fNL 8080:localhost:80 ansusenko@server.ansusenko.ne
t
The authenticity of host 'server.ansusenko.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:2uFslNbEsrU0NmX8+xPyOPR+k41WG+FIucs+olmyc6c.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [server.ansusenko.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.ansusenko.net' (ED25519) to the list of known hosts.
ansusenko@server.ansusenko.net's password:
[root@client.ansusenko.net ~]# lsof | grep TCP
sshd       854                    root    3u     IPv4              21723      0t0
   TCP *:ssh (LISTEN)
sshd       854                    root    4u     IPv6              21732      0t0
   TCP *:ssh (LISTEN)
master     989                    root   13u     IPv4              22485      0t0
   TCP localhost:smtp (LISTEN)
sshd      8711                    root    4u     IPv4              38904      0t0
   TCP client.ansusenko.net:ssh->10.0.2.2:52032 (ESTABLISHED)
sshd      8725                 vagrant    4u     IPv4              38904      0t0
   TCP client.ansusenko.net:ssh->10.0.2.2:52032 (ESTABLISHED)
ssh       8990                    root    3u     IPv4              43661      0t0
   TCP client.ansusenko.net:35068->www.ansusenko.net:ssh (ESTABLISHED)
```

Запуск консольных приложений через SSH

```
[ansusenko@client.ansusenko.net ~]$ ssh ansusenko@server.ansusenko.net hostname
server.ansusenko.net
[ansusenko@client.ansusenko.net ~]$ ssh ansusenko@server.ansusenko.net ls -Al
total 20
-rw-------. 1 ansusenko ansusenko 1271 Nov  3 12:41 .bash_history
-rw-r--r--. 1 ansusenko ansusenko   18 Apr 30  2024 .bash_logout
-rw-r--r--. 1 ansusenko ansusenko  141 Apr 30  2024 .bash_profile
-rw-r--r--. 1 ansusenko ansusenko  546 Oct 30 18:04 .bashrc
drwx------. 6 ansusenko ansusenko 4096 Nov  3 12:37 Maildir
drwx------. 2 ansusenko ansusenko   29 Nov 10 09:15 .ssh
```

Рис.: Просмотр имени узла сервера и списка файлов через ssh.

Запуск консольных приложений через SSH

```
[ansusenko@client.ansusenko.net ~]$ ssh ansusenko@server.ansusenko.net MAIL=~/Maildir/
mail
s-nail version v14.9.22.  Type '?' for help
/home/ansusenko/Maildir: 4 messages 2 unread
    1 root                  2025-11-01 15:01   20/863
▸U  2 ansusenko@client.ans  2025-11-03 11:09   21/814   "LMTP test            "
 U  3 root                  2025-11-03 11:48   21/842   "SMTP Auth Test       "
    4 ansusenko             2025-11-03 12:35   21/798   "Test from Alpine     "
```

Рис.: Просмотр почты на сервере через ssh.

Запуск графических приложений через SSH (X11Forwarding)

Разрешили отображать на локальном клиентском компьютере графические интерфейсы X11:

```
X11Forwarding yes
```

Запустили графическое приложение на сервере:

```
ssh -Y -v ansusenko@server.ansusenko.net firefox
```

```
[ansusenko@client.ansusenko.net ~]$ ssh -Y -v ansusenko@server.ansusenko.net firefox
OpenSSH_8.7p1, OpenSSL 3.2.2 4 Jun 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/50-redhat.conf
debug1: Reading configuration data /etc/crypto-policies/back-ends/openssh.config
debug1: configuration requests final Match pass
debug1: re-parsing configuration
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/50-redhat.conf
debug1: Reading configuration data /etc/crypto-policies/back-ends/openssh.config
debug1: Connecting to server.ansusenko.net [192.168.1.1] port 22.
debug1: Connection established.
debug1: identity file /home/ansusenko/.ssh/id_rsa type 0
debug1: identity file /home/ansusenko/.ssh/id_rsa-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_dsa type -1
debug1: identity file /home/ansusenko/.ssh/id_dsa-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_ecdsa type -1
debug1: identity file /home/ansusenko/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/ansusenko/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_ed25519 type -1
debug1: identity file /home/ansusenko/.ssh/id_ed25519-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_ed25519_sk type -1
debug1: identity file /home/ansusenko/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/ansusenko/.ssh/id_xmss type -1
debug1: identity file /home/ansusenko/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.7
debug1: Remote protocol version 2.0, remote software version OpenSSH_8.7
debug1: compat_banner: match: OpenSSH_8.7 pat OpenSSH* compat 0x04000000
```

Рис : Просмотр графического приложения (firefox) через ssh

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config
 ↪  /vagrant/provision/server/ssh/etc/ssh/
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
#!/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

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

Ответы на контрольные вопросы

1. **Как запретить удалённый доступ по SSH пользователю root и разрешить пользователю alice?**
   В файле `/etc/ssh/sshd_config` нужно установить:

   ```
   PermitRootLogin no
   AllowUsers alice
   ```

   Затем перезапустить службу: `systemctl restart sshd`

Ответы на контрольные вопросы

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

   В файле `/etc/ssh/sshd_config` добавить:

   ```
   Port 22
   Port 2022
   ```

   Это может потребоваться для:

   - Резервного подключения при блокировке основного порта
   - Разделения доступа для разных групп пользователей
   - Обхода ограничений межсетевого экрана

Ответы на контрольные вопросы

3. **Какие параметры используются для создания туннеля SSH в фоновом режиме?**
   Используются параметры:

   `ssh -f -N -L локальный_порт:удаленный_хост:удаленный_пор`

   где:
   - `-f` - переход в фоновый режим
   - `-N` - не выполнять удалённую команду
   - `-L` - локальная переадресация портов

Ответы на контрольные вопросы

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

   `ssh -L 5555:server2.example.com:80 пользователь@промежут`

   После этого обращение к `localhost:5555` будет перенаправляться на `server2.example.com:80` через промежуточный сервер.

Ответы на контрольные вопросы

5. **Как настроить SELinux для работы SSH с портом 2022?**

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

   Эта команда добавляет порт 2022 в список разрешённых портов для SSH в SELinux.

Ответы на контрольные вопросы

6. **Как настроить межсетевой экран для разрешения SSH через порт 2022?**

   Для firewalld:

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

   Для iptables:

   ```
   iptables -A INPUT -p tcp --dport 2022 -j ACCEPT
   service iptables save
   ```

Выводы

- В результате выполнения лабораторной работы приобрели практические навыки по настройке удалённого доступа к серверу с помощью SSH.
- Освоили методы ограничения доступа пользователей и настройки дополнительных портов.
- Изучили организацию туннелей SSH и настройку аутентификации по ключам.