

Отчет по лабораторной работе № 11.
Настройка безопасного удалённого доступа по
протоколу SSH

Сущенко Алина
НПИбд-01-23

2025

Содержание

1 Цель работы	3
2 Выполнение работы	4
2.1 Запрет удалённого доступа по SSH для пользователя root	4
2.2 Ограничение списка пользователей для удалённого доступа по SSH	5
2.3 Настройка дополнительных портов для удалённого доступа по SSH	6
2.4 Настройка удалённого доступа по SSH по ключу	8
2.5 Организация туннелей SSH, перенаправление TCP-портов	9
2.6 Запуск консольных приложений через SSH	10
2.7 Запуск графических приложений через SSH (X11Forwarding)	11
2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины	12
3 Выводы	13

1 Цель работы

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

2 Выполнение работы

2.1 Запрет удалённого доступа по SSH для пользователя root

- На сервере задали пароль для пользователя root (Рис. 1):

```
sudo -i  
passwd 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. 1: Задание пароля для пользователя root.

- На сервере в дополнительном терминале запустили мониторинг системных событий:

```
sudo -i  
journalctl -x -f
```

- С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя root (Рис. 2):

```
ssh root@server.ansusenko.net
```

```
[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+k4lWG+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. 2: Подключение к серверу через SSH-соединение.

Несмотря на корректный пароль для пользователя root, не получилось подключиться, так как в конфигурации ssh запрещен подключение для пользователя root с помощью пароля (по умолчанию используется настройка `PermitRootLogin prohibit-password`).

- На сервере открыли файл `/etc/ssh/sshd_config` конфигурации `sshd` для редактирования и запретили вход на сервер пользователю `rootf`, установив:

```
PermitRootLogin no
```

- После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

- Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `root`:

```
ssh root@server.ansusenko.net
```

Теперь также запрещен доступ `root` пользователю на сервер любыми средствами аутентификации.

2.2 Ограничение списка пользователей для удалённого доступа по SSH

- С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя `ansusenko` (Рис. 3):

```
ssh ansusenko@server.ansusenko.net
```

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

Рис. 3: Успешное подключение к серверу пользователем `ansusenko`.

- На сервере открыли файл `/etc/ssh/sshd_config` конфигурации `sshd` на редактирование и добавили строку

```
AllowUsers vagrant
```

- После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

- Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `ansusenko` (Рис. 4):

```
ssh ansusenko@server.ansusenko.net
```

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

Рис. 4: Отказ в доступе на сервер пользователю ansusenko.

5. В файле `/etc/ssh/sshd_config` конфигурации `sshd` внесли следующее изменение:

```
AllowUsers vagrant ansusenko
```

6. После сохранения изменений в файле конфигурации перезапустили `sshd` и вновь попытались получить доступ с клиента к серверу посредством SSH-соединения через пользователя `ansusenko` (Рис. 5).

```
[vagrant@client ~]$ ssh ansusenko@server.ansusenko.net
ansusenko@server.ansusenko.net's password:
Last failed login: Mon Nov 10 08:16:51 UTC 2025 from 192.168.1.30 on ssh:notty
There were 5 failed login attempts since the last successful login.
Last login: Mon Nov  3 11:03:16 2025
[ansusenko@server.ansusenko.net ~]$
```

Рис. 5: Восстановление доступа на сервер пользователю ansusenko.

2.3 Настройка дополнительных портов для удалённого доступа по SSH

1. На сервере в файле конфигурации `sshd` `/etc/ssh/sshd_config` нашли строку `Port` и ниже этой строки добавили:

```
Port 22
Port 2022
```

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

2. После сохранения изменений в файле конфигурации перезапустили `sshd`:

```
systemctl restart sshd
```

3. Посмотрели расширенный статус работы `sshd` (Рис. 6):

```
systemctl status -l sshd
```

```

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. 6: Проверка расширенного статуса работы sshd.

Видно, что получен отказ в работе sshd через порт 2022.

- Исправили на сервере метки SELinux к порту 2022 (Рис. 7):

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

- В настройках межсетевого экрана открыли порт 2022 протокола TCP (Рис. 7):

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

```

[root@server ~]# semanage port -a -t ssh_port_t -p tcp 2022
Port tcp/2022 already defined, modifying instead
[root@server ~]# firewall-cmd --add-port=2022/tcp
firewall-cmd --add-port=2022/tcp --permanent
Warning: ALREADY_ENABLED: '2022:tcp' already in 'public'
success
Warning: ALREADY_ENABLED: 2022:tcp
success
[root@server ~]#

```

Рис. 7: Настройка межсетевого экрана.

- Вновь перезапустили sshd и посмотрели расширенный статус его работы. Статус показал, что процесс sshd теперь прослушивает два порта.
- С клиента попытались получить доступ к серверу посредством SSH-соединения через пользователя ansusenko (Рис. 8):

```
ssh ansusenko@server.ansusenko.net
```

После открытия оболочки пользователя ввели `sudo -i` для получения доступа `root`. Отлогинились от `root` и пользователя `ansusenko` на сервере, введя дважды `logout` (Рис. 8).

```
[vagrant@client ~]$ ssh ansusenko@server.ansusenko.net
ansusenko@server.ansusenko.net's password:
Last login: Mon Nov 10 09:09:36 2025 from 192.168.1.30
[ansusenko@server.ansusenko.net ~]$ sudo -i
[sudo] password for ansusenko:
```

Рис. 8: Успешное подключение к серверу.

- Повторили попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя `ansusenko`, указав порт 2022 (Рис. 9):

```
ssh -p2022 ansusenko@server.ansusenko.net
```

После открытия оболочки пользователя ввели `sudo -i` для получения доступа `root`. Отлогинились от `root` и пользователя `ansusenko` на сервере, введя дважды `logout` (Рис. 9).

```
[vagrant@client ~]$ ssh -p2022 ansusenko@server.ansusenko.net
ansusenko@server.ansusenko.net's password:
Last login: Mon Nov 10 09:11:42 2025 from 192.168.1.30
[ansusenko@server.ansusenko.net ~]$ sudo -i
[sudo] password for ansusenko:
[root@server.ansusenko.net ~]#
logout
[ansusenko@server.ansusenko.net ~]$
logout
Connection to server.ansusenko.net closed.
[vagrant@client ~]$ |
```

Рис. 9: Успешное подключение к серверу по порту 2022.

2.4 Настройка удалённого доступа по SSH по ключу

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

```
PubkeyAuthentication yes
```

- После сохранения изменений в файле конфигурации перезапустили `sshd`.

- На клиенте сформировали SSH-ключ, введя в терминале под пользователем `ansusenko`:

```
ssh-keygen
```

- Закрытый ключ был записан в файл `/.ssh/id_rsa`, а открытый ключ записывается в файл `/.ssh/id_rsa.pub`.
- Скопировали открытый ключ на сервер, введя на клиенте (Рис. 10):

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

При запросе ввели пароль пользователя на удалённом сервере.

```
[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. 10: Копирование открытого ключа на сервер.

- Попробовали получить доступ с клиента к серверу посредством SSH-соединения (Рис. 11):

```
ssh ansusenko@server.ansusenko.net
```

Теперь аутентификация пройдена без ввода пароля для учетной записи удаленного пользователя.

```
[ansusenko@client.ansusenko.net ~]$ ssh ansusenko@server.ansusenko.net
Last login: Mon Nov 10 09:12:43 2025 from 192.168.1.30
[ansusenko@server.ansusenko.net ~]$
```

Рис. 11: Успешное подключение к серверу с использованием SSH-ключа.

2.5 Организация туннелей SSH, перенаправление TCP-портов

- На клиенте посмотрели, запущены ли какие-то службы с протоколом TCP (Рис. 12):

```
lsof | grep TCP
```
- Перенаправили порт 80 на `server.ansusenko.net` на порт 8080 на локальной машине (Рис. 12):

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

3. Вновь на клиенте посмотрели, запущены ли какие-то службы с протоколом TCP (Рис. 12):

```
lsof | grep TCP
```

```
[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.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 host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.ansusenko.net]:2222
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)
ssh      8990          root    4u      IPv6          43679    0t0
  TCP localhost:webcache (LISTEN)
ssh      8990          root    5u      IPv4          43680    0t0
  TCP localhost:webcache (LISTEN)
[root@client.ansusenko.net ~]#
```

Рис. 12: Перенаправление TCP-портов.

4. На клиенте запустили браузер и в адресной строке введите localhost:8080. Убедились, что отобразится страница с приветствием «Welcome to the server.ansusenko.net server».

2.6 Запуск консольных приложений через SSH

1. На клиенте открыли терминал под пользователем ansusenko.

- Посмотрели с клиента имя узла сервера (Рис. 13):

```
ssh ansusenko@server.ansusenko.net hostname
```

- Посмотрели с клиента список файлов на сервере (Рис. 13):

```
ssh ansusenko@server.ansusenko.net ls -Al
```

```
[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. 13: Просмотр имени узла сервера и списка файлов через ssh.

- Посмотрели с клиента почту на сервере (Рис. 14):

```
ssh ansusenko@server.ansusenko.net MAIL=~/.Maildir/ mail
```

```
[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. 14: Просмотр почты на сервере через ssh.

2.7 Запуск графических приложений через SSH (X11Forwarding)

- На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешили отображать на локальном клиентском компьютере графические интерфейсы X11:

```
X11Forwarding yes
```

- После сохранения изменения в конфигурационном файле перезапустили `sshd`.
- Попробовали с клиента удалённо подключиться к серверу и запустить графическое приложение `firefox` (Рис. 15):

```
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. 15: Просмотр графического приложения (firefox) через ssh.

2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

- На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создали в нём каталог `ssh`, в который поместите в соответствующие подкаталоги конфигурационный файл `sshd_config`:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
```

- В каталоге `/vagrant/provision/server` создали исполняемый файл `ssh.sh`:

```
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

Открыв его на редактирование, прописали в нём следующий скрипт:

```
#!/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
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины **server** в конфигурационном файле Vagrantfile добавили в разделе конфигурации для сервера:

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

3 Выводы

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