

Лабораторная работа №11

Настройка безопасного удалённого доступа по протоколу SSH

Спелов Андрей Николаевич

Содержание

1	Цель работы	6
2	Выполнение лабораторной работы	7
3	Выводы	20
4	Ответы на контрольные вопросы:	21
	Список литературы	23

Список иллюстраций

2.1	Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.	7
2.2	Запуск в дополнительном терминале мониторинга системных событий.	8
2.3	Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.	8
2.4	Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd для редактирования и запрет входа на сервер пользователю root.	9
2.5	Перезапуск sshd.	9
2.6	Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя root.	9
2.7	Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя anspelov.	9
2.8	Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd на редактирование и добавление нужной строки.	10
2.9	Перезапуск sshd.	10
2.10	Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov.	10
2.11	Внесение изменения в файле /etc/ssh/sshd_config конфигурации sshd.	11
2.12	Перезапуск sshd и повторная попытка получить доступ с клиента к серверу посредством SSH-соединения через пользователя anspelov.	11
2.13	Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.	11
2.14	Перезапуск sshd и просмотр расширенного статуса работы.	12
2.15	Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.	12
2.16	Попытка получить с клиента доступа к серверу посредством SSH-соединения через пользователя anspelov и получение доступа root.	13
2.17	Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov, указав порт 2022. Получение доступа root.	13
2.18	Настройка параметра на сервере в конфигурационном файле /etc/ssh/sshd_config, разрешающего аутентификацию по ключу.	13
2.19	Перезапуск sshd.	14

2.20	Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.	14
2.21	Попытка получения доступа с клиента к серверу посредством SSH-соединения.	14
2.22	Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.anspelov.net на порт 8080 на локальной машине.	15
2.23	Повторный просмотр на клиенте запущенных служб с протоколом TCP.	15
2.24	Запуск на клиенте браузера и ввод в адресной строке localhost:8080.	16
2.25	Открытие на клиенте терминала под пользователем anspelov. Просмотр имени узла сервера, списка файлов на сервере и почты на сервере.	16
2.26	Разрешение отображать на сервере в конфигурационном файле /etc/ssh/sshd_config на локальном клиентском компьютере графические интерфейсы X11.	17
2.27	Перезапуск sshd.	17
2.28	Попытка с клиента удалённо подключиться к серверу и запустить графическое приложение firefox.	18
2.29	Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога ssh, в который поместили в соответствующие подкаталоги конфигурационный файл sshd_config. Создание в каталоге /vagrant/provision/server исполняемого файла ssh.sh.	18
2.30	Открытие файла на редактирование и написание в нём скрипта.	19
2.31	Редактирование конфигурационного файла Vagrantfile.	19

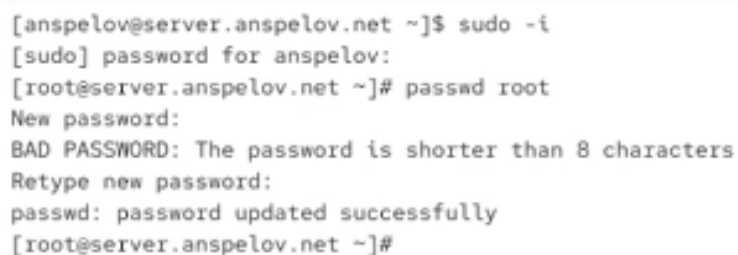
Список таблиц

1 Цель работы

Целью данной работы является приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

2 Выполнение лабораторной работы

На сервере зададим пароль для пользователя root: passwd root(рис. 2.1).



```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# passwd root
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
[root@server.anspelov.net ~]#
```

Рис. 2.1: Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

На сервере в дополнительном терминале запустим мониторинг системных событий (рис. 2.2).

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

#8 0x00000000435890 n/a (n/a + 0x0)
#9 0x00007ffa4f4b6b68 start_thread (libc.so.6 + 0x94b68)
#10 0x00007ffa4f5216bc __clone3 (libc.so.6 + 0x1056bc)

Stack trace of thread 12505:
#0 0x00007ffa4f51f4bd syscall (libc.so.6 + 0x1034bd)
#1 0x0000000004347a2 n/a (n/a + 0x0)
#2 0x0000000004506d6 n/a (n/a + 0x0)
#3 0x000000000405123 n/a (n/a + 0x0)
#4 0x00007ffa4f44630e __libc_start_call_main (libc.so.6 + 0x2a30e)
#5 0x00007ffa4f4463c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)
#6 0x0000000004044aa n/a (n/a + 0x0)
ELF object binary architecture: AMD x86_64

Subject: Process 12505 (VBoxClient) dumped core
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support
Documentation: man:core(5)

Process 12505 (VBoxClient) crashed and dumped core.

This usually indicates a programming error in the crashing program and
should be reported to its vendor as a bug.
Nov 13 11:54:56 server.anspelov.net systemd[1]: systemd-coredump[27-12509-0.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

The unit systemd-coredump[27-12509-0.service has successfully entered the 'dead' state.
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/A/IN': 127.0.0.1#53
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/AAAA/IN': 127.0.0.1#53
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/A/IN': 127.0.0.1#53
Nov 13 11:54:57 server.anspelov.net named[1374]: timed out resolving 'mirror.team-host.ru/AAAA/IN': 127.0.0.1#53
Nov 13 11:54:59 server.anspelov.net named[1374]: timed out resolving 'team-host.ru/DS/IN': 127.0.0.1#53
Nov 13 11:54:59 server.anspelov.net named[1374]: timed out resolving 'team-host.ru/DS/IN': 127.0.0.1#53
```

Рис. 2.2: Запуск в дополнительном терминале мониторинга системных событий.

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

```
[anspelov@client.anspelov.net ~]$ ssh root@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjem1Px1VkFkq9Eq9laMvpgqUuTCjHA.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:1: [server.anspelov.net]:2022
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.anspelov.net' (ED25519) to the list of known hosts.
root@server.anspelov.net's password:
Permission denied, please try again.
root@server.anspelov.net's password:
Permission denied, please try again.
root@server.anspelov.net's password:
root@server.anspelov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[anspelov@client.anspelov.net ~]$
```

Рис. 2.3: Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя root.

На сервере откроем файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретим вход на сервер пользователю root(рис. 2.4).


```
#LoginGraceTime 2m
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

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

Рис. 2.4: Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd для редактирования и запрет входа на сервер пользователю root.

После сохранения изменений в файле конфигурации перезапустим sshd (рис. 2.5).

```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]#
```

Рис. 2.5: Перезапуск sshd.

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root (рис. 2.6).

```
[anspelov@client.anspelov.net ~]$ ssh root@server
ssh: Could not resolve hostname server: Name or service not known
```

Рис. 2.6: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя root.

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя anspelov (рис. 2.7).

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 11:53:30 2025
[anspelov@server.anspelov.net ~]$
```

Рис. 2.7: Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя anspelov.

На сервере откроем файл /etc/ssh/sshd_config конфигурации sshd на редактирование и добавим строку(рис. 2.8).

```
#UsePrivilegeSeparation no
AllowUsers vagrant
#AllowAgentForwarding yes
#AllowTcpForwarding yes
```

Рис. 2.8: Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd на редактирование и добавление нужной строки.

После сохранения изменений в файле конфигурации перезапустим sshd (рис. 2.9).

```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]#
```

Рис. 2.9: Перезапуск sshd.

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov(рис. 2.10).

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Permission denied, please try again.
anspelov@server.anspelov.net's password:
Permission denied, please try again.
anspelov@server.anspelov.net's password:
anspelov@server.anspelov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[anspelov@client.anspelov.net ~]$
```

Рис. 2.10: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov.

В файле /etc/ssh/sshd_config конфигурации sshd внесём следующее изменение: AllowUsers vagrant anspelov(рис. 2.11).

```

AllowUsers vagrant anspelov
#AllowAgentForwarding yes

```

Рис. 2.11: Внесение изменения в файле /etc/ssh/sshd_config конфигурации sshd.

После сохранения изменений в файле конфигурации перезапустим sshd и вновь попытаемся получить доступ с клиента к серверу посредством SSH-соединения через пользователя anspelov(рис. 2.12).

```

[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last failed login: Thu Nov 13 12:12:40 UTC 2025 from 192.168.1.2 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Thu Nov 13 12:09:52 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$

```

Рис. 2.12: Перезапуск sshd и повторная попытка получить доступ с клиента к серверу посредством SSH-соединения через пользователя anspelov.

На сервере в файле конфигурации sshd /etc/ssh/sshd_config найдём строку Port и ниже этой строки добавим (рис. 2.13).

```

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

```

Рис. 2.13: Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.

После сохранения изменений в файле конфигурации перезапустим sshd: `systemctl restart sshd` И посмотрим расширенный статус работы: `systemctl status -l sshd` Система сообщила нам об отказе в работе sshd через порт 2022(рис. 2.14).

```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-11-13 12:14:56 UTC; 27s ago
     Invocation: bce79aca95ad419086049f822f776795
       Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 15156 (sshd)
      Tasks: 1 (Limit: 10395)
    Memory: 1M (peak: 1.2M)
       CPU: 24ms
    CGroup: /system.slice/ssh.service
            └─15156 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 13 12:14:56 server.anspelov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 13 12:14:56 server.anspelov.net sshd[15156]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPT2025
Nov 13 12:14:56 server.anspelov.net sshd[15156]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: error: Bind to port 2022 on :: failed: Permission denied.
Nov 13 12:14:56 server.anspelov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: Server listening on 0.0.0.0 port 22.
Nov 13 12:14:56 server.anspelov.net sshd[15156]: Server listening on :: port 22.
[root@server.anspelov.net ~]#
```

Рис. 2.14: Перезапуск sshd и просмотр расширенного статуса работы.

Исправим на сервере метки SELinux к порту 2022: `semanage port -a -t ssh_port_t -p tcp 2022` В настройках межсетевого экрана откроем порт 2022 протокола TCP: `firewall-cmd --add-port=2022/tcp` `firewall-cmd --add-port=2022/tcp --permanent` Вновь перезапустим sshd и посмотрим расширенный статус его работы (статус показывает, что процесс sshd теперь прослушивает два порта) (рис. 2.15).

```
[root@server.anspelov.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.anspelov.net ~]# firewall-cmd --add-port=2022/tcp
success
[root@server.anspelov.net ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-11-13 12:17:35 UTC; 8s ago
     Invocation: ca8c66f4c70b4bcf81e8793f6a624e97
       Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 15494 (sshd)
      Tasks: 1 (Limit: 10395)
    Memory: 1M (peak: 1.2M)
       CPU: 23ms
    CGroup: /system.slice/ssh.service
            └─15494 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 13 12:17:35 server.anspelov.net systemd[1]: Starting sshd.service - OpenSSH server daemon...
Nov 13 12:17:35 server.anspelov.net sshd[15494]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPT2025
Nov 13 12:17:35 server.anspelov.net sshd[15494]: Server listening on 0.0.0.0 port 2022.
Nov 13 12:17:35 server.anspelov.net sshd[15494]: Server listening on :: port 2022.
Nov 13 12:17:35 server.anspelov.net systemd[1]: Started sshd.service - OpenSSH server daemon.
Nov 13 12:17:35 server.anspelov.net sshd[15494]: Server listening on 0.0.0.0 port 22.
Nov 13 12:17:35 server.anspelov.net sshd[15494]: Server listening on :: port 22.
lines 1-20/20 (END)
```

Рис. 2.15: Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя anspelov: `ssh anspelov@server.anspelov.net` После открытия оболочки пользователя введём `sudo -i` для получения доступа root (рис. 2.16).

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:13:04 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]#
```

Рис. 2.16: Попытка получить с клиента доступа к серверу посредством SSH-соединения через пользователя anspelov и получение доступа root.

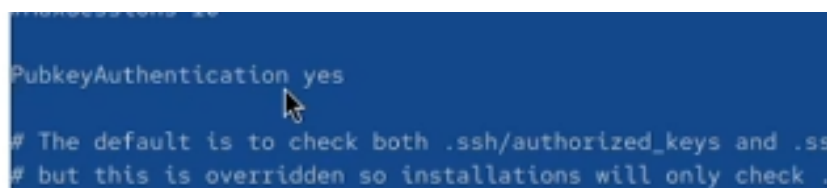
Теперь повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov, указав порт 2022: `ssh -p2022 anspelov@server.anspelov.net` После открытия оболочки пользователя введём `sudo -i` для получения доступа root(рис. 2.17).

```
[anspelov@client.anspelov.net ~]$ ssh -p2022 anspelov@server.anspelov.net
anspelov@server.anspelov.net's password:
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:18:23 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]#
```

Рис. 2.17: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov, указав порт 2022. Получение доступа root.

На сервере в конфигурационном файле `/etc/ssh/sshd_config` зададим параметр, разрешающий аутентификацию по ключу: `PubkeyAuthentication yes` (рис. 2.18).



```
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ss
# but this is overridden so installations will only check .
```

Рис. 2.18: Настройка параметра на сервере в конфигурационном файле `/etc/ssh/sshd_config`, разрешающего аутентификацию по ключу.

После сохранения изменений в файле конфигурации перезапустим `sshd` (рис. 2.19).

```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]#
```

Рис. 2.19: Перезапуск sshd.

На клиенте сформируем SSH-ключ, введя в терминале под пользователем anspelov `ssh-keygen`. Далее скопируем открытый ключ на сервер, введя на клиенте (рис. 2.20).

```
[anspelov@client.anspelov.net ~]$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/anspelov/.ssh/id_ed25519):
Enter passphrase for "/home/anspelov/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/anspelov/.ssh/id_ed25519
Your public key has been saved in /home/anspelov/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:zvscwb+PycAA+FKRMqhw5QyyH3ylx4HIGVTvAwLnOQ anspelov@client.anspelov.net
The key's randomart image is:
+--[ED25519 256]--+
|o+*EB0ooo      |
|ooB ==o=o      |
|.oooo*o=       |
|..oo.* +       |
| . S =         |
| o +          |
| o . +        |
| o o +        |
|..o O..       |
+----[SHA256]-----+
[anspelov@client.anspelov.net ~]$ ssh-copy-id anspelov@server.anspelov.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
anspelov@server.anspelov.net's password:

Number of key(s) added: 1

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

[anspelov@client.anspelov.net ~]$ █
```

Рис. 2.20: Формирование на клиенте SSH-ключа и копирование открытого ключа на сервер.

Попробуем получить доступ с клиента к серверу посредством SSH-соединения: `ssh anspelov@server.anspelov.net`. Теперь мы проходим аутентификацию без ввода пароля для учётной записи удалённого пользователя (рис. 2.21).

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net
Web console: https://server.anspelov.net:9090/ or https://10.0.2.15:9090/

Last login: Thu Nov 13 12:20:57 2025 from 192.168.1.2
[anspelov@server.anspelov.net ~]$ █
```

Рис. 2.21: Попытка получения доступа с клиента к серверу посредством SSH-соединения.

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP: `lsf`

| grep TCP После чего перенаправим порт 80 на server.anspelov.net на порт 8080 на локальной машине (рис. 2.22).

```
[root@client.anspelov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd      1                root    79u    IPv6        8922      0t0      TCP *:websm (LISTEN)
)
cupsd        1242             root    7u     IPv6        11311     0t0      TCP localhost:ipp (
LISTEN)
cupsd        1242             root    8u     IPv4        11312     0t0      TCP localhost:ipp (
LISTEN)
sshd         1251             root    7u     IPv4        10551     0t0      TCP *:ssh (LISTEN)
sshd         1251             root    8u     IPv6        10553     0t0      TCP *:ssh (LISTEN)
master       1373             root    13u    IPv4        11531     0t0      TCP localhost:smtp
(LISTEN)
[root@client.anspelov.net ~]# ssh -fNL 8080:localhost
Bad local forwarding specification '8080:localhost'
[root@client.anspelov.net ~]# ssh -fNL 8080:localhost:80 anspelov@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjemIPx1VfKq9Eq9laMvpgqUuTCjHA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
[root@client.anspelov.net ~]# ssh -fNL 8080:localhost:80 anspelov@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjemIPx1VfKq9Eq9laMvpgqUuTCjHA.
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.anspelov.net' (ED25519) to the list of known hosts.
anspelov@server.anspelov.net's password:
[root@client.anspelov.net ~]#
```

Рис. 2.22: Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.anspelov.net на порт 8080 на локальной машине.

Вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP (рис. 2.23).

```
[root@client.anspelov.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
Output information may be incomplete.
systemd      1                root    79u    IPv6        8922      0t0      TCP *:websm (LISTEN)
)
cupsd        1242             root    7u     IPv6        11311     0t0      TCP localhost:ipp (
LISTEN)
cupsd        1242             root    8u     IPv4        11312     0t0      TCP localhost:ipp (
LISTEN)
sshd         1251             root    7u     IPv4        10551     0t0      TCP *:ssh (LISTEN)
sshd         1251             root    8u     IPv6        10553     0t0      TCP *:ssh (LISTEN)
master       1373             root    13u    IPv4        11531     0t0      TCP localhost:smtp
(LISTEN)
ssh          12184            root    3u     IPv4        105587    0t0      TCP client.anspelov
.net:46748->server.anspelov.net:ssh (ESTABLISHED)
ssh          12184            root    4u     IPv6        105836    0t0      TCP localhost:webca
che (LISTEN)
ssh          12184            root    5u     IPv4        105837    0t0      TCP localhost:webca
che (LISTEN)
[root@client.anspelov.net ~]#
```

Рис. 2.23: Повторный просмотр на клиенте запущенных служб с протоколом TCP.

На клиенте запустим браузер и в адресной строке введём localhost:8080. Убедимся, что отобразилась страница с приветствием «Welcome to the server.anspelov.net server» (рис. 2.24).

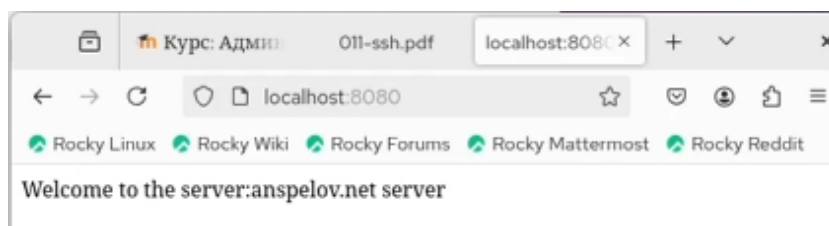


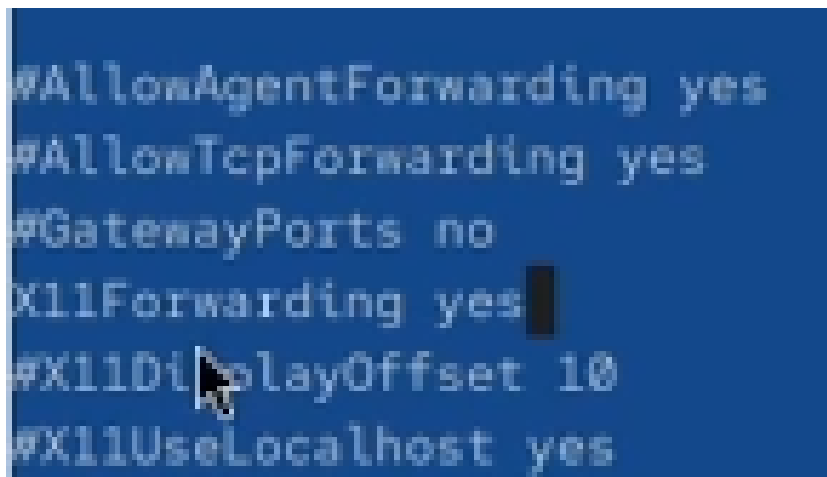
Рис. 2.24: Запуск на клиенте браузера и ввод в адресной строке localhost:8080.

На клиенте откроем терминал под пользователем anspelov и посмотрим с клиента имя узла сервера: `ssh anspelov@server.anspelov.net hostname` Посмотрим с клиента список файлов на сервере: `ssh anspelov@server.anspelov.net ls -Al` Посмотрим с клиента почту на сервере (рис. 2.25).

```
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net hostname
server.anspelov.net
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net ls -Al
total 56
-rw-r--r--. 1 anspelov user 248 Nov 13 12:49 .bash_history
-rw-r--r--. 1 anspelov user 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 anspelov user 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 anspelov user 549 Sep 13 17:04 .bashrc
drwx----- 11 anspelov user 4096 Sep 22 11:21 .cache
drwx----- 10 anspelov user 4096 Oct 20 15:00 .config
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Desktop
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Documents
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Downloads
drwx----- 4 anspelov user 32 Sep 22 10:49 .local
drwx----- 5 anspelov user 4096 Oct 27 12:26 Maildir
drwxr-xr-x. 5 anspelov user 54 Sep 22 11:21 .mozilla
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Music
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Pictures
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Public
drwx----- 2 anspelov user 29 Nov 13 12:24 .ssh
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Templates
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-clipboard-tty2-control.pid
-rw-r----- 1 anspelov user 6 Nov 13 12:51 .vboxclient-clipboard-tty2-service.pid
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-draganddrop-tty2-control.pid
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-hostversion-tty2-control.pid
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-seamless-tty2-control.pid
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-vmsvga-session-tty2-control.pid
-rw-r----- 1 anspelov user 6 Nov 13 11:53 .vboxclient-vmsvga-session-tty2-service.pid
drwxr-xr-x. 2 anspelov user 6 Sep 22 10:49 Videos
[anspelov@client.anspelov.net ~]$ ssh anspelov@server.anspelov.net MAIL=~/.Maildir/ mail
s-nail version v14.9.24. Type '?' for help
/home/anspelov/Maildir: 1 message
└─ 1 Andrei Spelov 2025-10-27 12:18 18/623 *test1 *
```

Рис. 2.25: Открытие на клиенте терминала под пользователем anspelov. Просмотр имени узла сервера, списка файлов на сервере и почты на сервере.

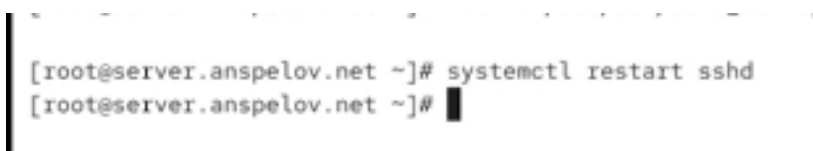
На сервере в конфигурационном файле `/etc/ssh/sshd_config` разрешим отображать на локальном клиентском компьютере графические интерфейсы X11 (рис. 2.26).



```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
```

Рис. 2.26: Разрешение отображать на сервере в конфигурационном файле /etc/ssh/sshd_config на локальном клиентском компьютере графические интерфейсы X11.

После сохранения изменения в конфигурационном файле перезапустим sshd (рис. 2.27).



```
[root@server.anspelov.net ~]# systemctl restart sshd
[root@server.anspelov.net ~]#
```

Рис. 2.27: Перезапуск sshd.

Попробуем с клиента удалённо подключиться к серверу и запустить графическое приложение firefox (рис. 2.28).

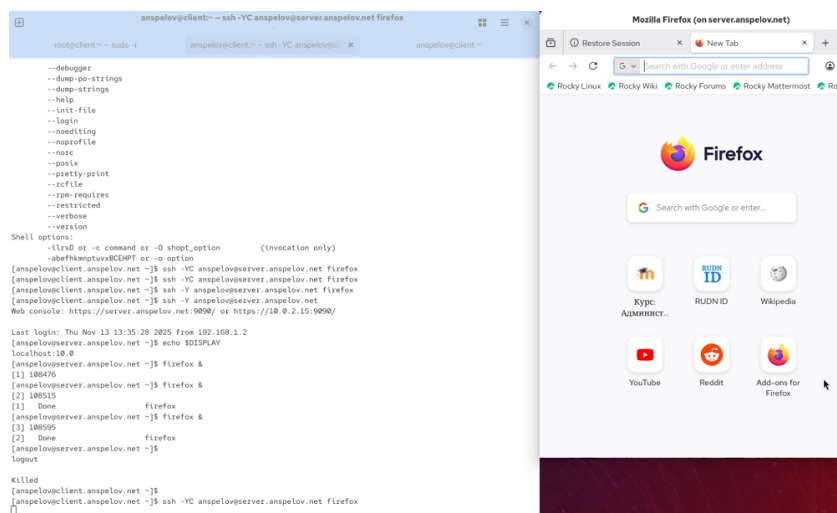


Рис. 2.28: Попытка с клиента удалённо подключиться к серверу и запустить графическое приложение firefox.

На виртуальной машине server перейдём 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`. В каталоге `/vagrant/provision/server` создадим исполняемый файл `ssh.sh` (рис. 2.29).

```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# cd /vagrant/provision/server
[root@server.anspelov.net server]# mkdir -p /vagrant/provision/server/ssh/etc/ssh
[root@server.anspelov.net server]# cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.anspelov.net server]# cd /vagrant/provision/server
[root@server.anspelov.net server]# touch ssh.sh
[root@server.anspelov.net server]# chmod +x ssh.sh
```

Рис. 2.29: Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создание в нём каталога `ssh`, в который поместили в соответствующие подкаталоги конфигурационный файл `sshd_config`. Создание в каталоге `/vagrant/provision/server` исполняемого файла `ssh.sh`.

Открыв его на редактирование, пропишем в нём скрипт из лабораторной работы (рис. 2.30).

```

ssh.sh      [-M--] 0 L:[ 1+12 13/ 13] *(361 / 361b) <EOF>
#!/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. 2.30: Открытие файла на редактирование и написание в нём скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим в разделе конфигурации для сервера (рис. 2.31).

```

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

```

Рис. 2.31: Редактирование конфигурационного файла Vagrantfile.

3 Выводы

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

4 Ответы на контрольные вопросы:

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать? – В конфигурационном файле SSH `/etc/ssh/sshd_config`: # Запрет удалённого доступа пользователю root `PermitRootLogin no` # Разрешение доступа пользователю alice `AllowUsers alice` После внесения изменений, необходимо перезапустить службу SSH: `sudo service ssh restart`
2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться? – В конфигурационном файле `/etc/ssh/sshd_config` добавьте строки: # Первый порт (по умолчанию 22) `Port 22` # Второй порт `Port 2222` После изменений перезапустите службу SSH. Это может быть полезно для повышения безопасности, а также для избежания конфликтов с другими службами, использующими порт 22.
3. Какие параметры используются для создания туннеля SSH, когда команда `ssh` устанавливает фоновое соединение и не ожидает какой-либо конкретной команды? – `ssh -N -f -L local_port:destination_host:remote_port user@ssh_server` -N: Не выполнять команду на удаленном хосте. -f: Перевести ssh в фоновый режим после установки туннеля.
4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера `server2.example.com`? – `ssh -L 5555:server2.example.com:80 user@ssh_server` Теперь, при подключении к локальному порту 5555, трафик будет перенаправляться через SSH к порту 80 на сервере

server2.example.com.

5. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?
– `sudo semanage port -a -t ssh_port_t -p tcp 2022` Данная команда добавляет правило SELinux, разрешая использование порта 2022 для сервиса ssh.
6. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022? – `sudo firewall-cmd --permanent --add-port=2022/tcp` `sudo firewall-cmd --reload` Эти команды добавляют правило в межсетевой экран для разрешения входящих подключений по SSH через порт 2022 и перезагружают конфигурацию межсетевого экрана.

Список литературы