Лабораторная работа №11

Настройка безопасного удалённого доступа по протоколу SSH

Спелов Андрей Николаевич

Содержание

Список иллюстраций

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).

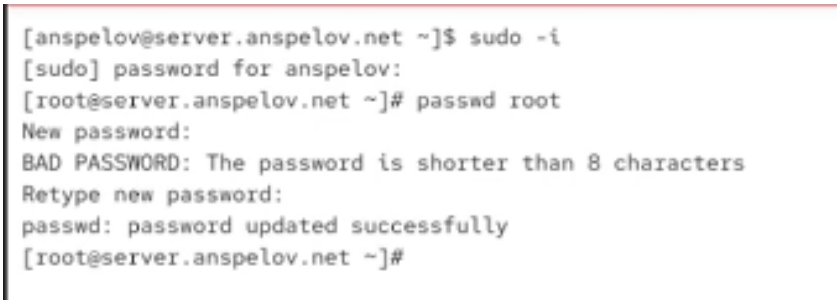

Рис. 2.1: Открытие режима суперпользователя на виртуальной машине server и создание пароля для пользователя root.

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

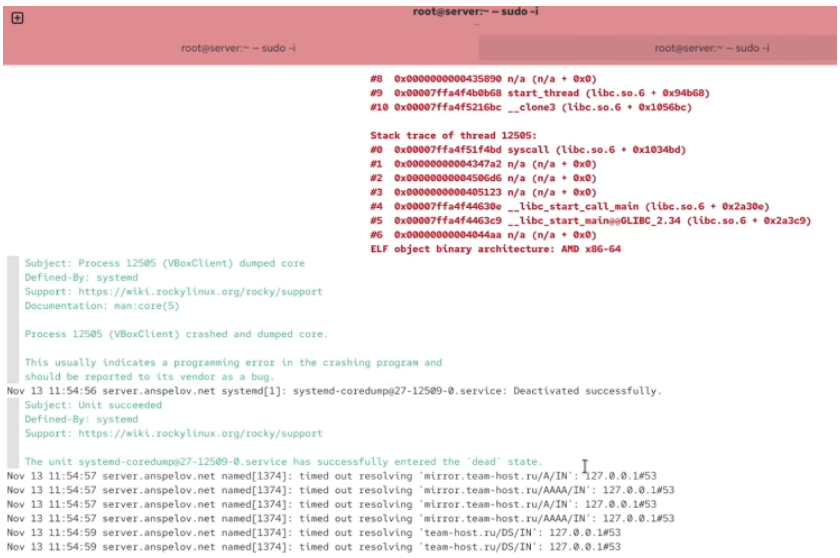

Рис. 2.2: Запуск в дополнительном терминале мониторинга системных событий.

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

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).

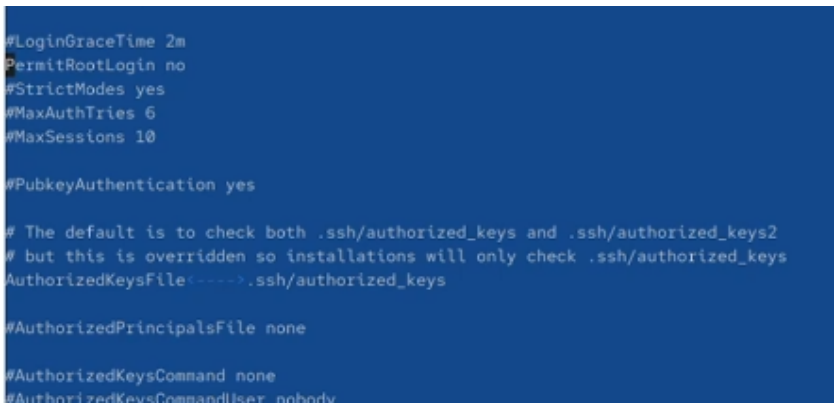

Рис. 2.4: Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd для редактирования и запрет входа на сервер пользователю root.

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

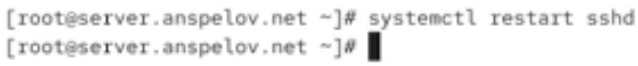

Рис. 2.5: Перезапуск sshd.

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

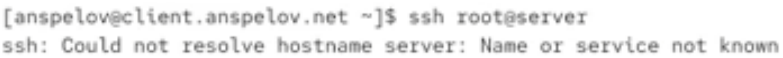

Рис. 2.6: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя root.

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

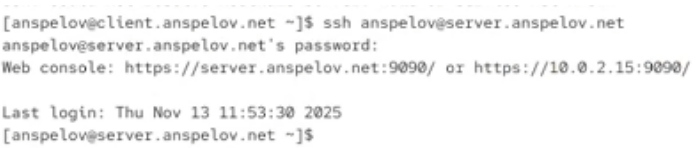

Рис. 2.7: Попытка получить с клиента доступ к серверу посредством SSH-соединения через пользователя anspelov.

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

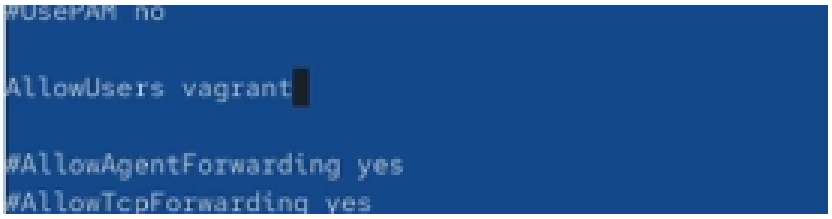

Рис. 2.8: Открытие на сервере файла /etc/ssh/sshd_config конфигурации sshd на редактирование и добавление нужной строки.

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

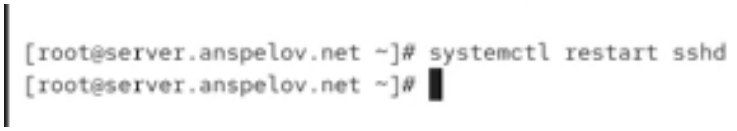

Рис. 2.9: Перезапуск sshd.

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

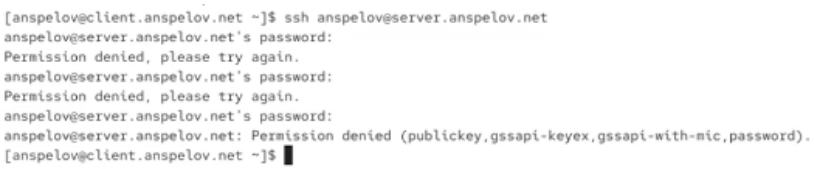

Рис. 2.10: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov.

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

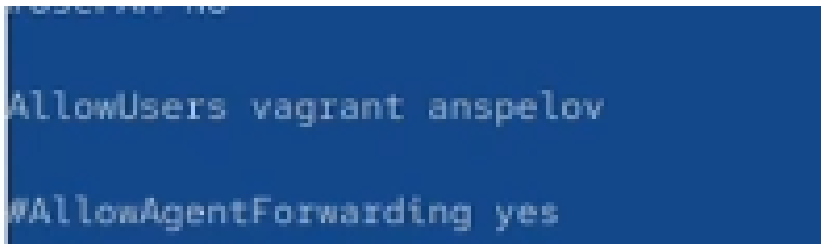

Рис. 2.11: Внесение изменения в файле /etc/ssh/sshd_config конфигурации sshd.

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).

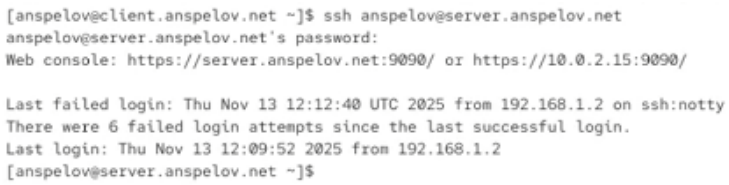

Рис. 2.12: Перезапуск sshd и повторная попытка получить доступ с клиента к серверу посредством SSH-соединения через пользователя anspelov.

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

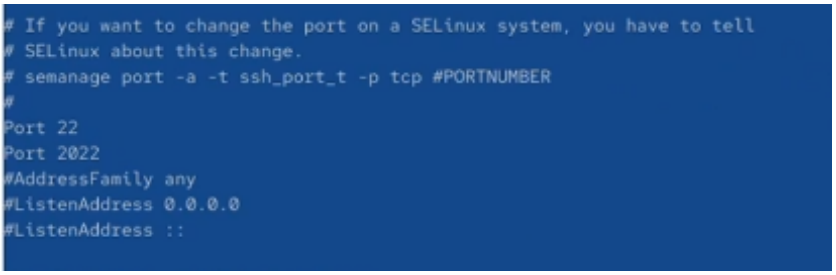

Рис. 2.13: Добавление ниже строки Port записей в файле конфигурации sshd /etc/ssh/sshd_config на сервере.

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).

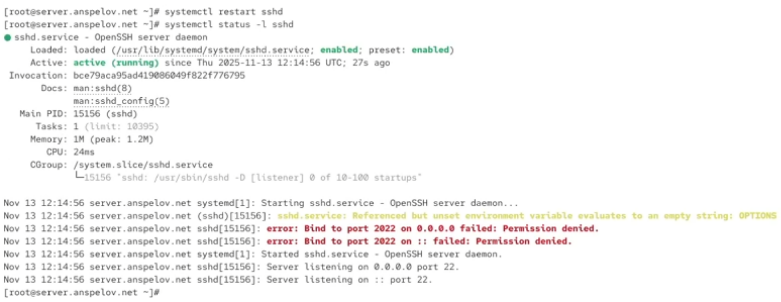

Рис. 2.14: Перезапуск sshd и просмотр расширенного статуса работы.

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).

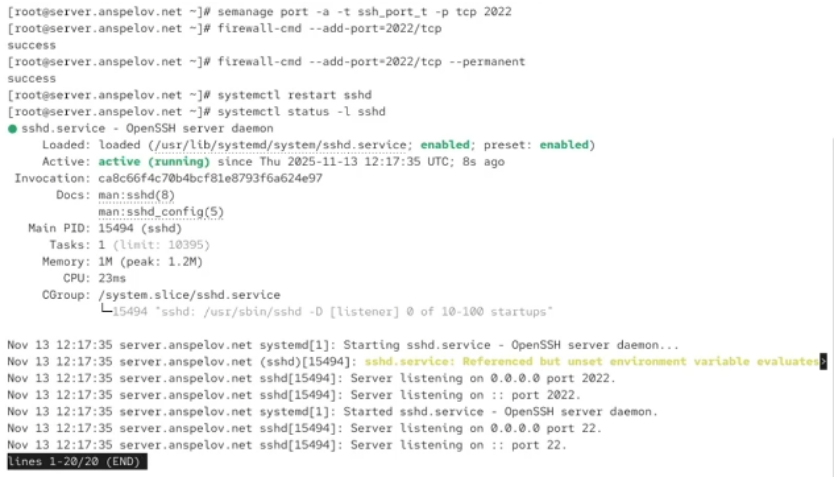

Рис. 2.15: Исправление на сервере метки SELinux к порту 2022, открытие в настройках межсетевого порта 2022 протокола TCP, повторный перезапуск sshd и просмотр расширенного статуса его работы.

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).

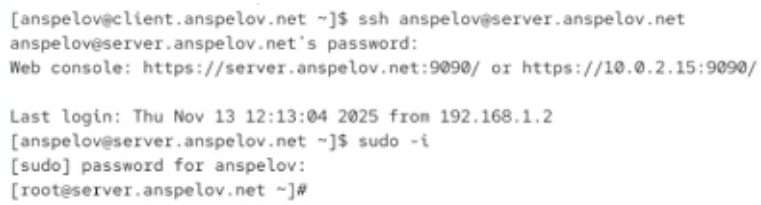

Рис. 2.16: Попытка получить с клиента доступа к серверу посредством SSH-соединения через пользователя anspelov и получение доступа root.

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).

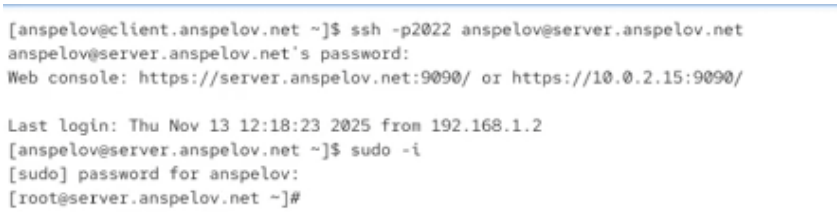

Рис. 2.17: Повторная попытка получения доступа с клиента к серверу посредством SSH-соединения через пользователя anspelov, указав порт 2022. Получение доступа root.

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

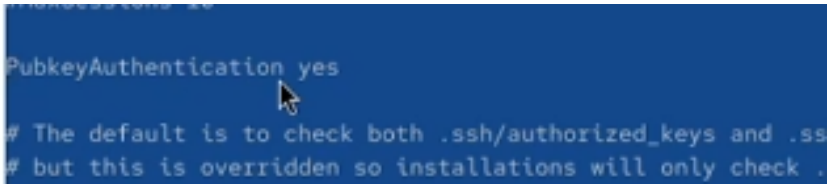

Рис. 2.18: Настройка параметра на сервере в конфигурационном файле /etc/ssh/sshd_config, разрешающего аутентификацию по ключу.

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+FkRMqhwSQyyH3ylx4HIGVTVmAvLnQQ anspelov@client.anspelov.net
The key's randomart image is:
+--[ED25519 256]--+
|o*+*EBOooo       |
|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: lsof

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

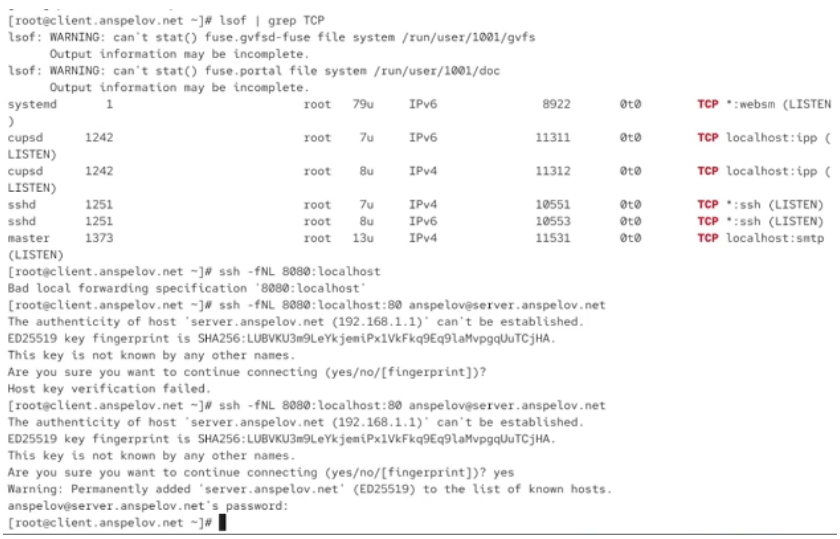

Рис. 2.22: Просмотр на клиенте запущенных служб с протоколом TCP и перенаправление порта 80 на server.anspelov.net на порт 8080 на локальной машине.

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

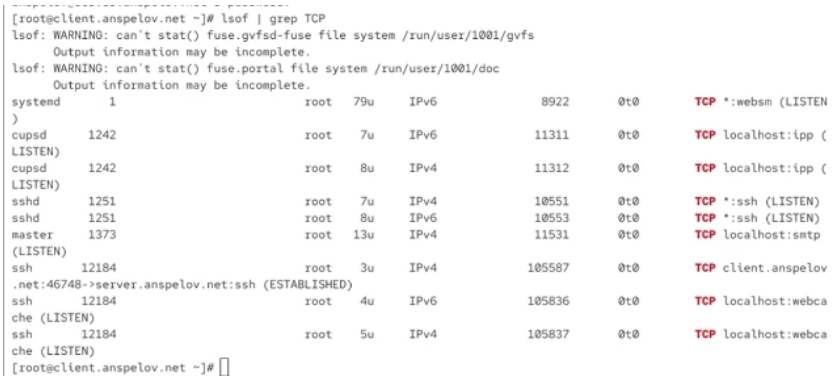

Рис. 2.23: Повторный просмотр на клиенте запущенных служб с протоколом TCP.

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).

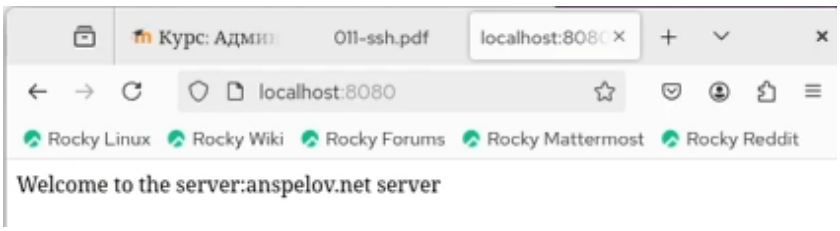

Рис. 2.24: Запуск на клиенте браузера и ввод в адресной строке localhost:8080.

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-------.  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               "

^C[anspelov@client.anspelov.net ~]$
```

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).

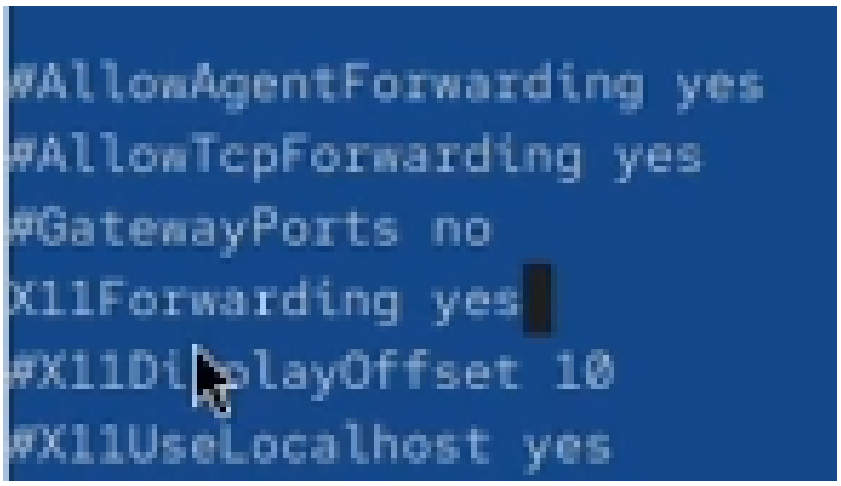

Рис. 2.26: Разрешение отображать на сервере в конфигурационном файле /etc/ssh/sshd_config на локальном клиентском компьютере графические интерфейсы X11.

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

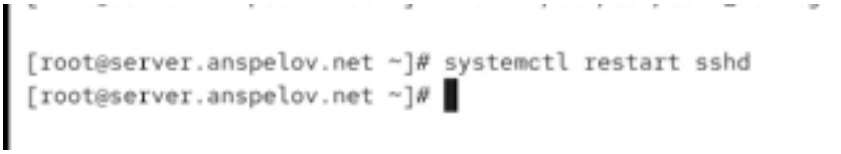

Рис. 2.27: Перезапуск sshd.

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

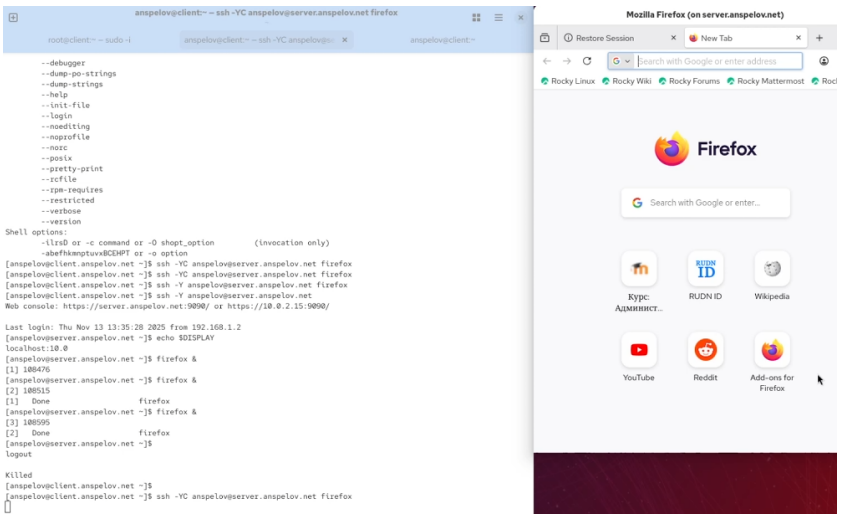

Рис. 2.28: Попытка с клиента удалённо подключиться к серверу и запустить графическое приложение firefox.

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).

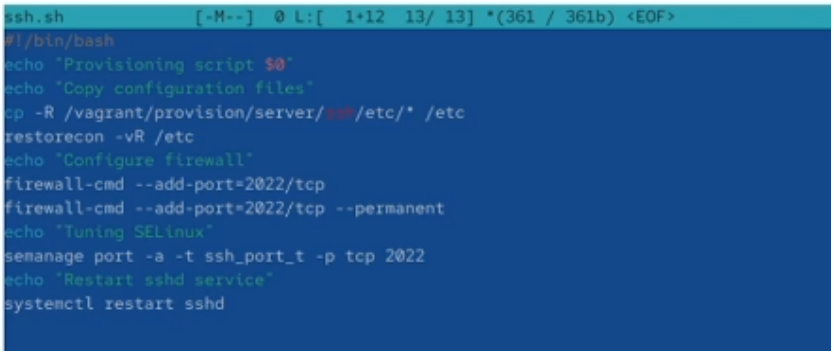

Рис. 2.30: Открытие файла на редактирование и написание в нём скрипта.

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

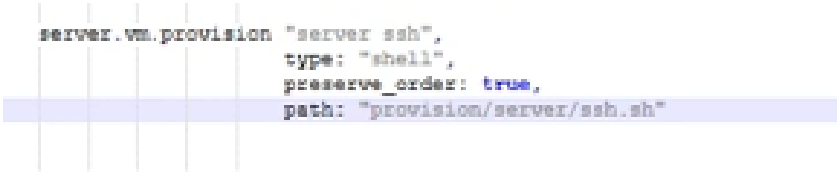

Рис. 2.31: Редактирование конфигурационного файла Vagrantfile.

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