Отчёт по лабораторной работе 11

Настройка безопасного удалённого доступа по протоколу SSH

Метвалли Ахмед Фарг Набеех

Содержание

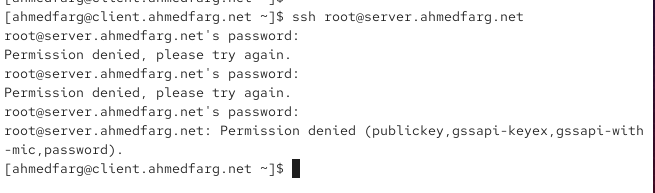
# 1 Цель работы

Освоение приёмов настройки SSH-сервера для ограничения удалённого доступа: запрета входа под пользователем root и разрешения подключения только определённым пользователям.

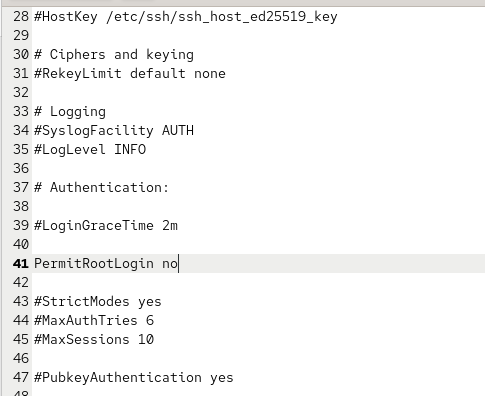
# 2 Выполнение

## 2.1 Запрет удалённого доступа по SSH для пользователя root

1. С клиента выполнена попытка подключения к серверу от имени пользователя root.  
   Сервер трижды запрашивал пароль, после чего выдал сообщение об ошибке.  
   Это означает, что вход под root запрещён на уровне конфигурации SSH.

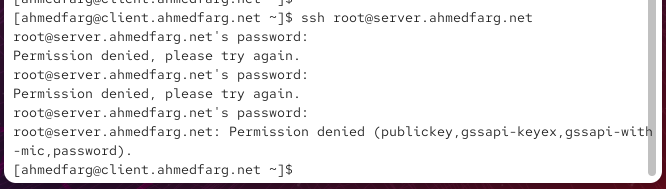
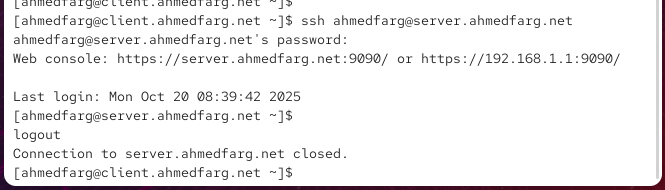
* 
* Рис. 1: Ошибка подключения по SSH под root

1. В конфигурационном файле /etc/ssh/sshd\_config установлено значение параметра PermitRootLogin no.  
   После перезапуска службы sshd подключение под root остаётся невозможным, что подтверждает корректную работу настройки.

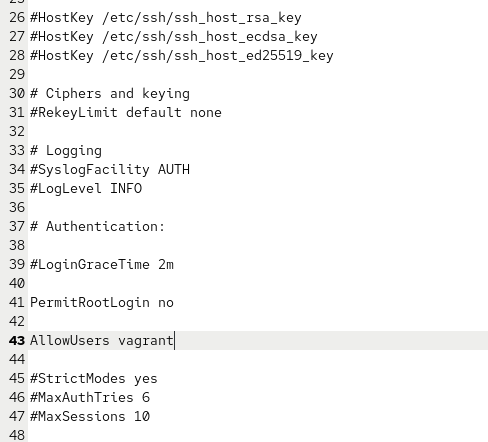
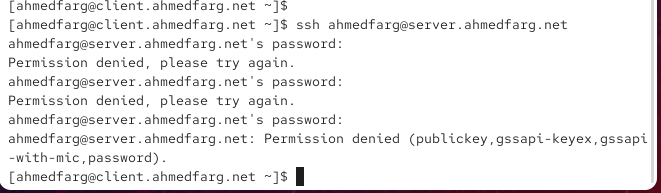
* 
* Рис. 2: Файл sshd\_config с запретом root-входа

## 2.2 Ограничение списка пользователей для удалённого доступа по SSH

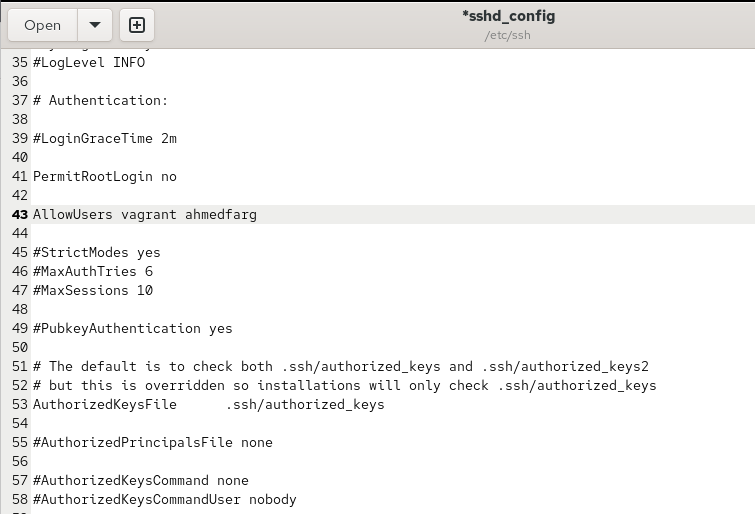
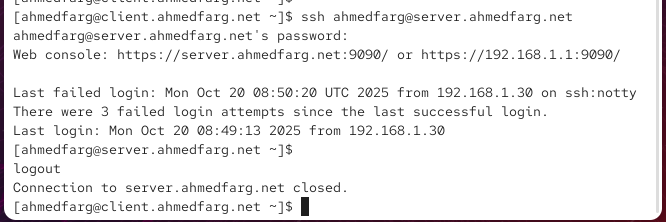
1. При попытке входа на сервер под пользователем ahmedfarg с клиента доступ был успешно получен, так как данный пользователь разрешён в текущей конфигурации SSH.

*  

1. Для ограничения доступа только определённым пользователям в файл /etc/ssh/sshd\_config добавлена строка AllowUsers vagrant.  
   После перезапуска службы sshd подключение под пользователем ahmedfarg стало невозможным.

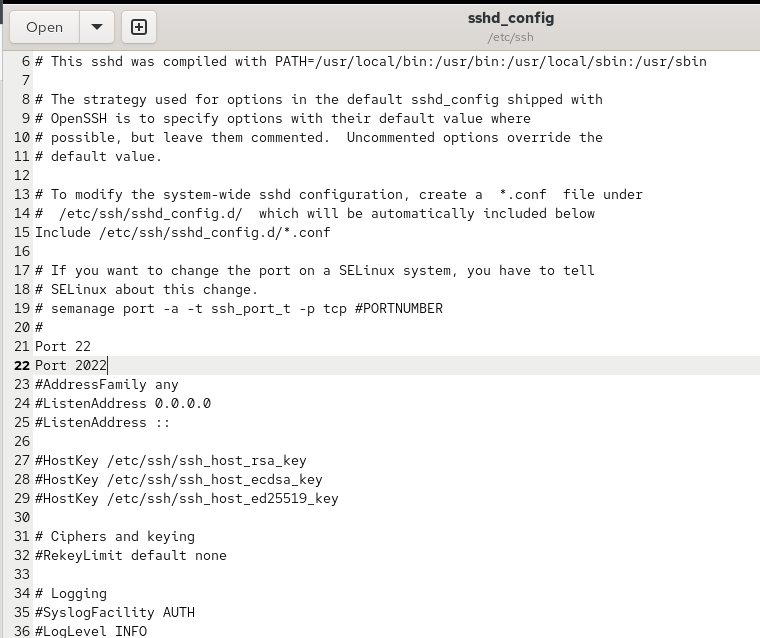
*  

1. После добавления обоих пользователей в список разрешённых AllowUsers vagrant ahmedfarg вход под ahmedfarg снова стал возможен.

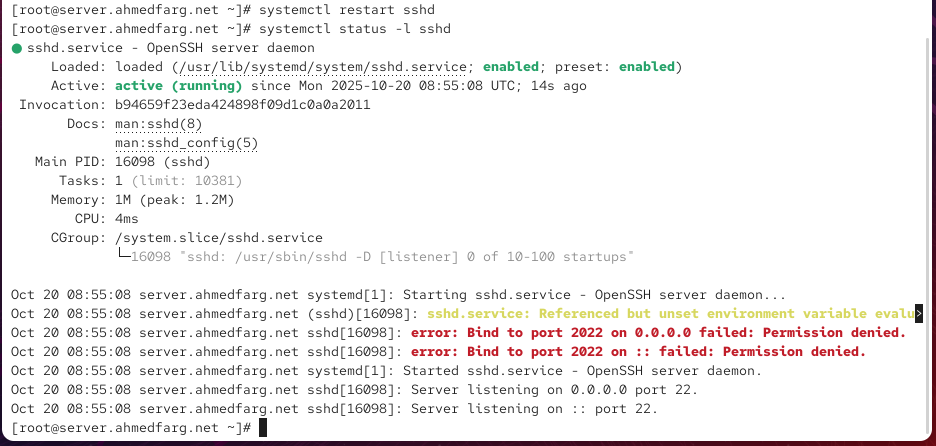
*  

## 2.3 Настройка дополнительных портов для удалённого доступа по SSH

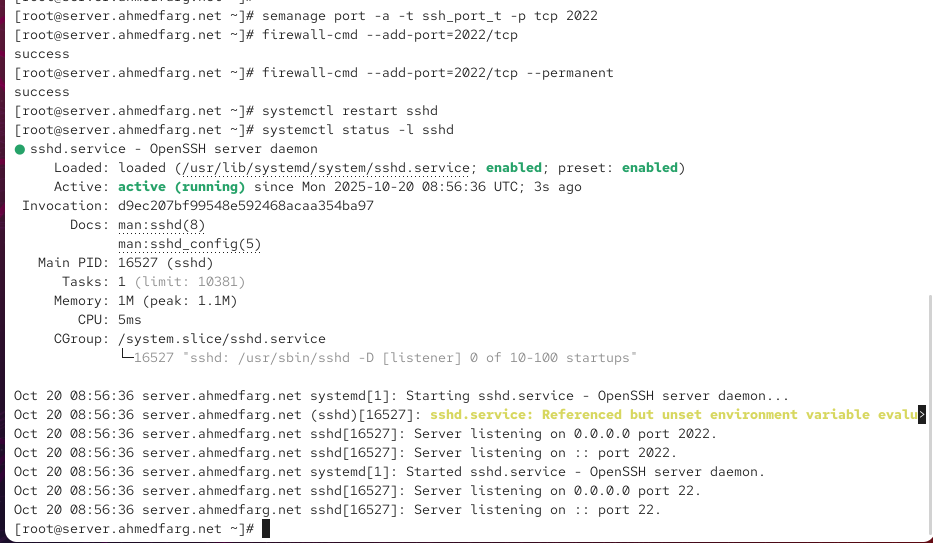
1. В конфигурационном файле /etc/ssh/sshd\_config добавлены строки Port 22 и Port 2022.  
   Это позволяет использовать два порта для подключения по SSH, обеспечивая резервное соединение в случае ошибки конфигурации.

* 
* Рис. 3: Добавление второго порта в sshd\_config

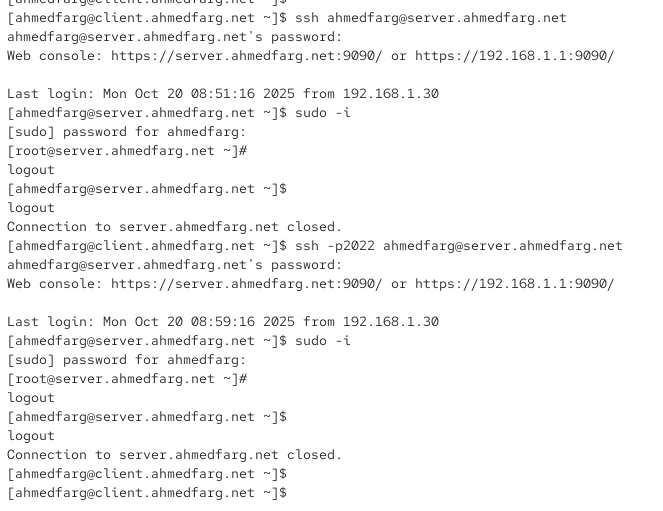
1. После сохранения изменений и перезапуска службы sshd команда systemctl status -l sshd показала сообщение об ошибке.  
   Система выдала предупреждение об отказе в доступе к порту 2022 из-за ограничений SELinux.

* 
* Рис. 4: Ошибка доступа к порту 2022
* Это означает, что SELinux блокировал использование нового порта для SSH-подключений.

1. Для устранения проблемы к порту 2022 была добавлена метка SELinux, разрешающая его использование для SSH: команда semanage port -a -t ssh\_port\_t -p tcp 2022.
2. В настройках межсетевого экрана открыт порт 2022 для протокола TCP с помощью команд firewall-cmd.  
   После этого служба sshd была перезапущена, и статус показал, что теперь сервер прослушивает оба порта.

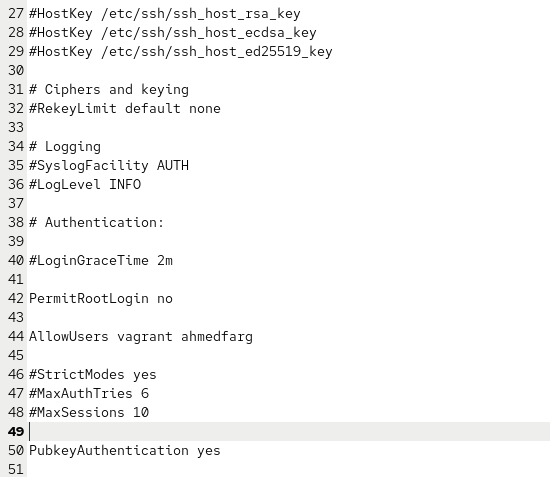
* 
* Рис. 5: Открытие порта 2022 и успешный запуск sshd

1. С клиента выполнено подключение к серверу по стандартному порту 22, а затем по дополнительному порту 2022.  
   В обоих случаях соединение установлено успешно, вход выполнен под пользователем ahmedfarg, после чего получен доступ root с помощью sudo -i.

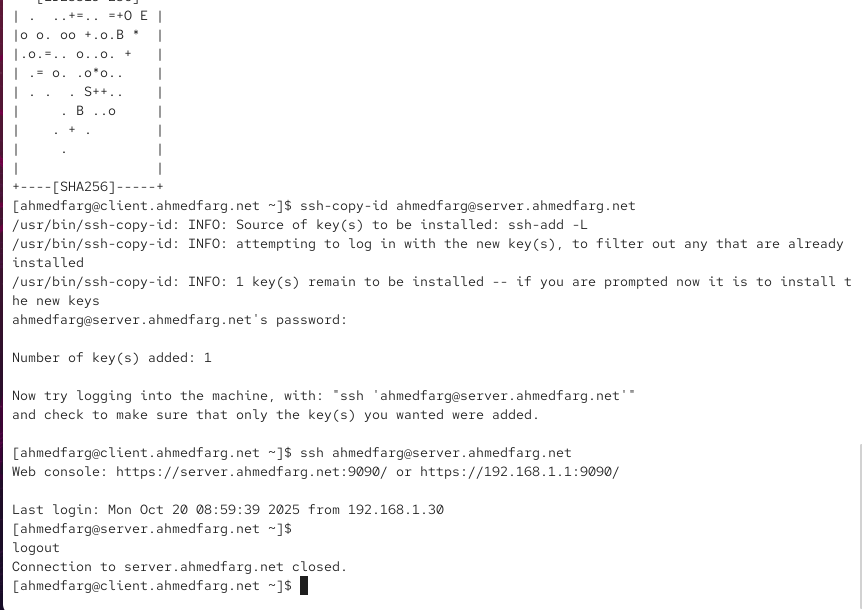
* 
* Рис. 6: Подключение по стандартному и дополнительному портам

## 2.4 Настройка удалённого доступа по SSH по ключу

1. В конфигурационном файле /etc/ssh/sshd\_config на сервере установлен параметр PubkeyAuthentication yes, разрешающий аутентификацию по ключам.

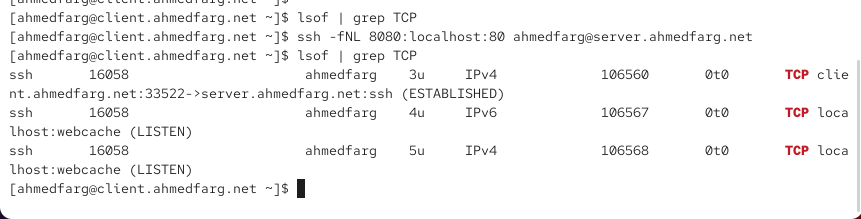
* 
* Рис. 7: Разрешение аутентификации по ключу в sshd\_config

1. На клиенте сгенерирована пара SSH-ключей. Закрытый ключ сохранён в ~/.ssh/id\_rsa, открытый — в ~/.ssh/id\_rsa.pub.  
   Открытый ключ скопирован на сервер с помощью команды ssh-copy-id.
2. После копирования ключа выполнено подключение к серверу. Аутентификация прошла без запроса пароля, что подтверждает корректную настройку SSH-доступа по ключу.

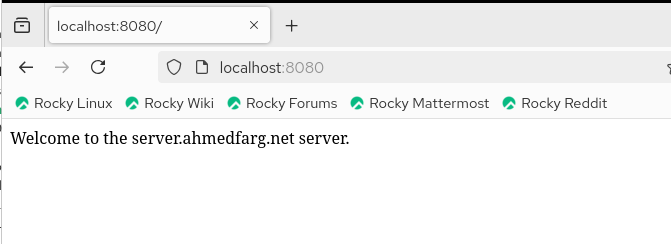
* 
* Рис. 8: Передача ключа и успешное подключение без пароля

## 2.5 Организация туннелей SSH и перенаправление TCP-портов

1. На клиенте выполнена проверка активных TCP-соединений — активных процессов, использующих TCP, не обнаружено.
2. Затем выполнено перенаправление порта 80 сервера на порт 8080 локальной машины с помощью SSH-туннеля.  
   После выполнения команды lsof | grep TCP отображается установленное SSH-соединение и локальное прослушивание порта 8080.

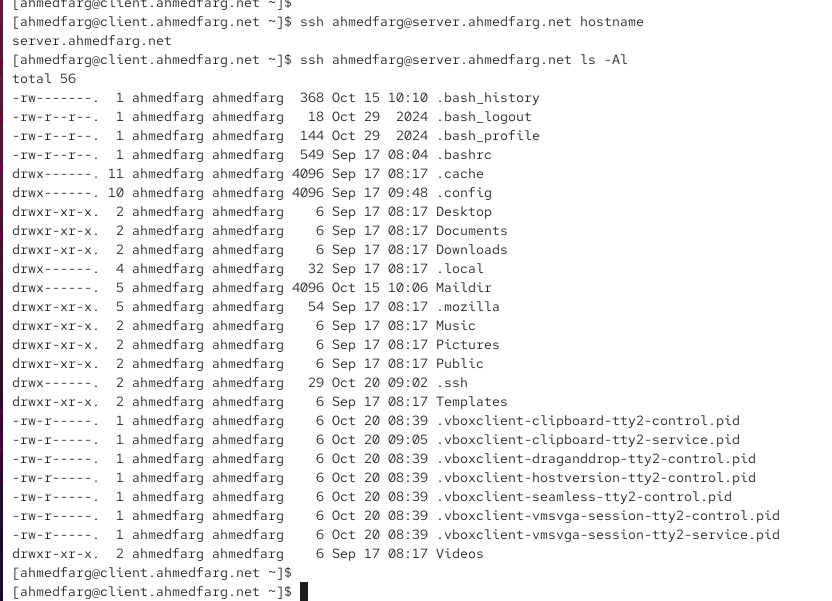
* 
* Рис. 9: Проверка TCP-соединений и организация туннеля SSH

1. При обращении к адресу localhost:8080 в браузере открылась страница приветствия сервера, что подтверждает успешное создание SSH-туннеля.

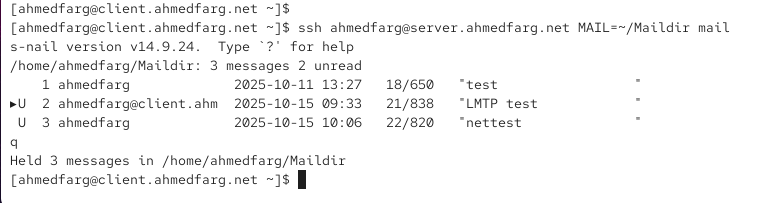
* 
* Рис. 10: Отображение веб-страницы через туннель SSH

## 2.6 Запуск консольных приложений через SSH

1. С клиента получено имя узла сервера с помощью команды hostname, результат — server.ahmedfarg.net.
2. Выведен список файлов домашнего каталога пользователя на сервере, что подтвердило успешное выполнение удалённой команды через SSH.

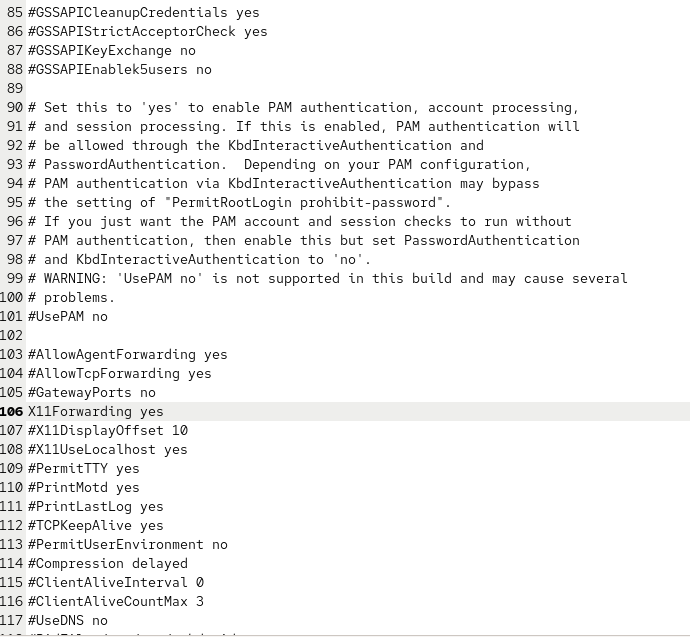
* 
* Рис. 11: Проверка имени хоста и содержимого домашнего каталога

1. Проверена работа почтовой программы в каталоге Maildir удалённого пользователя.  
   На экране отобразился список писем, хранящихся в почтовом каталоге.

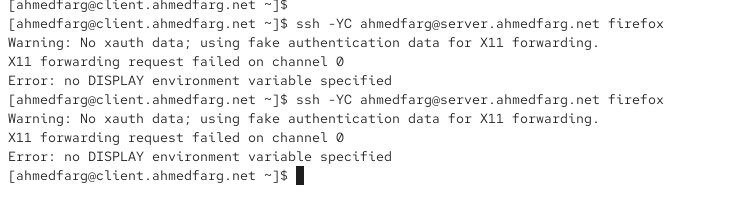
* 
* Рис. 12: Просмотр почты пользователя через SSH

## 2.7 Запуск графических приложений через SSH (X11 Forwarding)

1. В конфигурационном файле /etc/ssh/sshd\_config на сервере включён параметр X11Forwarding yes и перезапущен sshd.

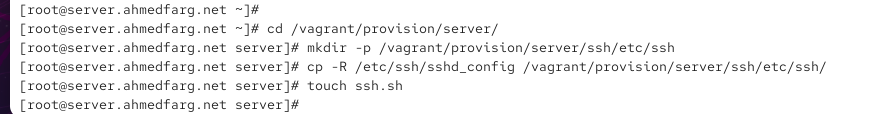
* 
* Рис. 13: Разрешение X11Forwarding в sshd\_config

1. При попытке запустить графическое приложение firefox через SSH с клиента выводится сообщение об ошибке — отсутствует переменная DISPLAY, что свидетельствует о невозможности запуска X11-сеанса в текущих настройках среды.

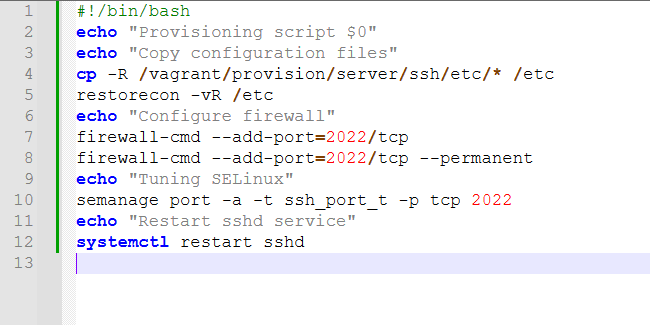
* 
* Рис. 14: Ошибка при попытке запуска графического приложения через SSH

## 2.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На сервере создан каталог /vagrant/provision/server/ssh с подкаталогом etc/ssh, в который был скопирован текущий файл конфигурации sshd\_config.  
   Это позволяет хранить настройки SSH в структуре проекта Vagrant.

* 
* Рис. 15: Создание каталогов и копирование файла sshd\_config

1. В каталоге /vagrant/provision/server создан исполняемый файл ssh.sh, содержащий команды для автоматической настройки SSH.  
   Скрипт выполняет копирование конфигурационных файлов, настройку SELinux и межсетевого экрана, а также перезапускает службу sshd.

* 
* Рис. 16: Содержимое скрипта ssh.sh для автоматизации настройки SSH

# 3 Заключение

В ходе лабораторной работы были освоены методы администрирования SSH-сервера: настройка портов, ограничение доступа пользователей, создание туннелей, запуск консольных и графических приложений, а также автоматизация конфигурации с помощью скрипта.  
Результаты подтвердили корректность работы SSH при изменённых параметрах безопасности и сетевого взаимодействия.

# 4 Контрольные вопросы

1. **Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?**  
   В файле /etc/ssh/sshd\_config установить параметр PermitRootLogin no для запрета входа root и добавить строку AllowUsers alice для разрешения входа пользователю alice.  
   После внесения изменений необходимо перезапустить службу SSH.
2. **Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?**  
   В файле /etc/ssh/sshd\_config указать несколько строк с параметром Port, например Port 22 и Port 2022.  
   Это обеспечивает резервный канал подключения в случае блокировки или ошибки на основном порту.
3. **Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?**  
   Используются параметры fNL, где f переводит соединение в фоновый режим, N запрещает выполнение удалённых команд, а L задаёт локальное перенаправление портов.
4. **Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?**  
   Необходимо использовать перенаправление с указанием локального и удалённого портов, чтобы обращения к адресу localhost:5555 перенаправлялись на порт 80 сервера server2.example.com.
5. **Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?**  
   Добавить разрешение для SELinux, установив метку безопасности ssh\_port\_t для порта 2022, чтобы процесс SSH мог использовать этот порт.
6. **Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?**  
   Добавить разрешающее правило в межсетевой экран firewalld для порта 2022 протокола TCP и сохранить изменения для постоянного применения.