МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное   
учреждение высшего образования

**"Южно-Уральский государственный университет**

**(национальный исследовательский университет)"**

**Высшая школа электроники и компьютерных наук**

**Кафедра системного программирования**

ОТЧЕТ

о выполнении практического задания № 6

по дисциплине

«Операционные системы семейства Unix/Linux»

|  |  |
| --- | --- |
|  | Выполнил:  студент группы КЭ-303  Старостенок Д.В.  Проверил:  ст. преподаватель кафедры СП  Варкентин В.В. |

Челябинск-2023

ОГЛАВЛЕНИЕ

[ЗАДАНИЕ 3](#_Toc131631601)

[1. ИСПОЛЬЗОВАНИЕ И НАСТРОЙКА SSH 4](#_Toc131631602)

[1.1. Вариант и ход работы 4](#_Toc131631603)

[КОНТРОЛЬНЫЕ ВОПРОСЫ 9](#_Toc131631604)

[СПИСОК ЛИТЕРАТУРЫ 11](#_Toc131631605)

# ЗАДАНИЕ

Цель работы: изучить процесс настройки организации удаленного доступа к серверу при помощи технологии OpenSSH.

Задачи:

* Установить OpenSSH.
* Изучить способы подключения по SSH к удаленному серверу.
* Настроить SSH-сервер для удаленного подключения по связке login/password с запретом на вход от имени учетной записи root.
* Настроить SSH-сервер для удаленного подключения по SSH-ключу.
* Настроить SSH-сервер для удаленного подключения по одноразовому паролю при помощи технологии GoogleAuth.

# ИСПОЛЬЗОВАНИЕ И НАСТРОЙКА SSH

* 1. Вариант и ход работы

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | Способ | Порт | Шифрование |
| 29 | init.d | 2384 | RSA |

1. Проверьте, установлен ли в вашей OpenSSH (Рис. 1). Если он не установлен, установите (Рис. 2).

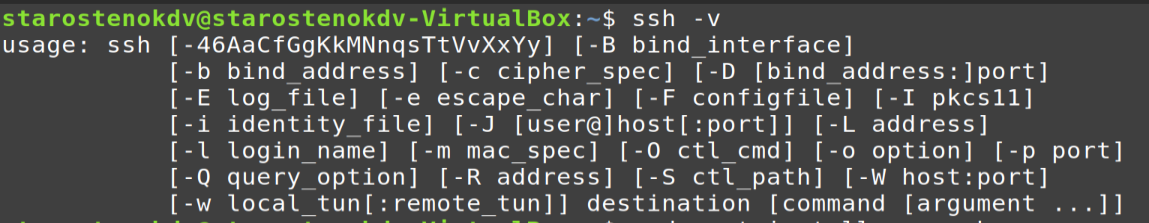


Рис. 1 – Проверка: установлен ли OpenSSH

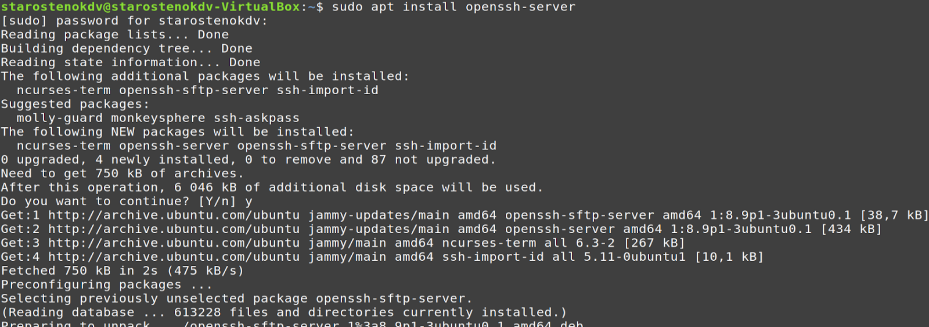


Рис. 2 – Строка установки OpenSSH

2. Используйте один из способов запуска ssh-сервера в соответствии с вашим вариантом (Рис. 3).



Рис. 3 – Строка запуска ssh

3. Проверьте статус вашего ssh-сервера (Рис. 4).

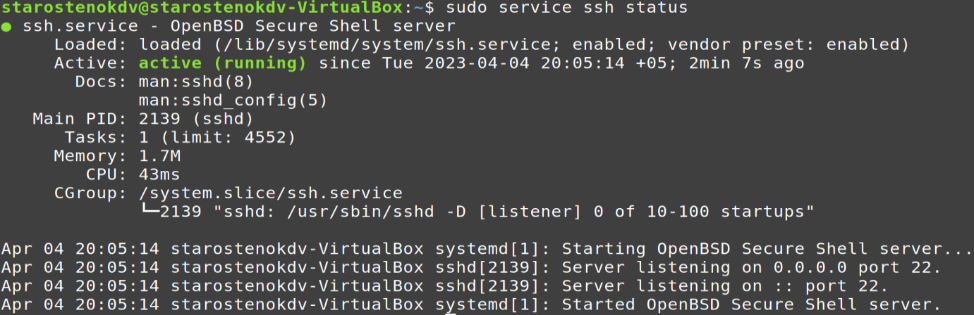


Рис. 4 – Статус ssh-сервера

4. Определите IP-адрес вашего ssh-сервера (Рис. 5) и подключитесь к нему по ssh (Рис. 6).

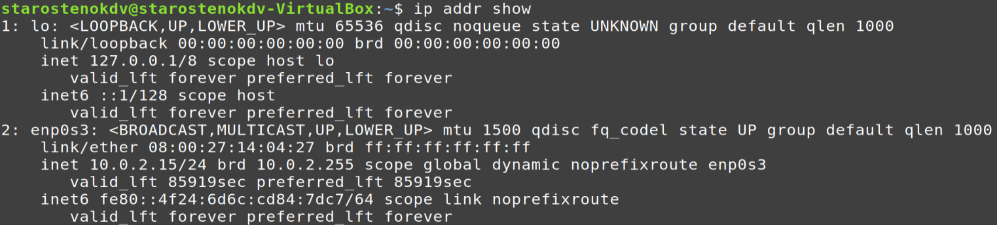


Рис. 5 – IP-адрес ssh-сервера

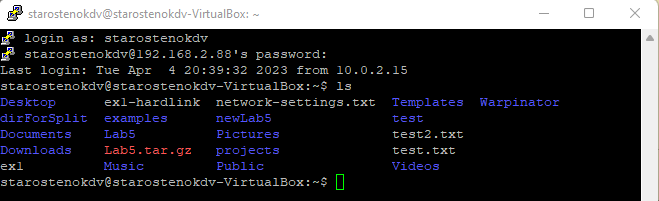


Рис. 6 – Подключение к серверу по SSH

5. Создайте резервную копию конфигурационного файла с настройками ssh.

Создание резервной копии с помощью: sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak

6. Измените порт подключения по ssh в соответствующем конфигурационном файле согласно вашему варианту.

Запретите вход по ssh от имени root.

Установите время, за которое пользователь должен успеть подключиться по ssh. Время выберите из диапазона [20;40].

Ограничьте максимальное количество попыток входа по ssh значением из диапазона [2-5].

Ограничьте максимальное количество одновременных подключений с одного IP значением из диапазона [1-4] (Рис 7).

Перезапустите ssh-сервер (Рис. 8).



Рис. 7 – Настройки ssh-сервера



Рис. 8 – Строка перезапуска ssh-сервера

7. Подключитесь к серверу с учетом новых настроек (Рис. 9).

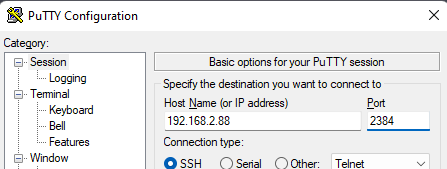


Рис. 9 – Подключение к ssh-серверу

8. Запретите вход по паролю и настройте способ входа на ваш ssh-сервер по ключу (Рис. 10). Сгенерируйте публичный и приватный ключи (Рис. 11). Алгоритм шифрования выбирается в соответствии с вашим вариантом

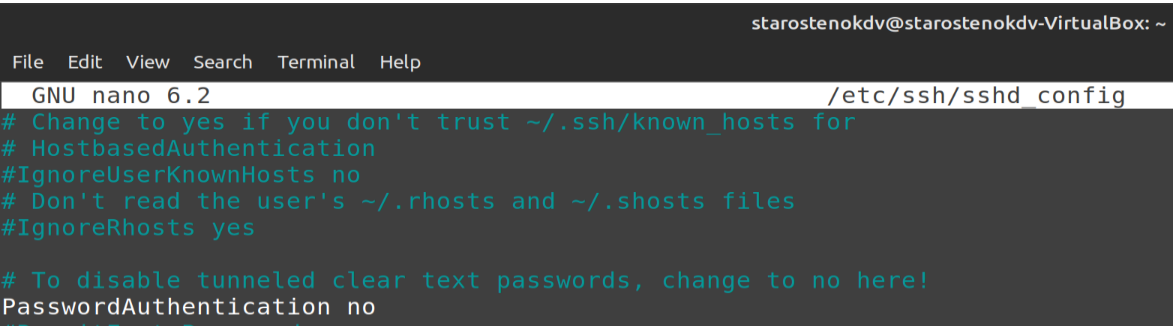
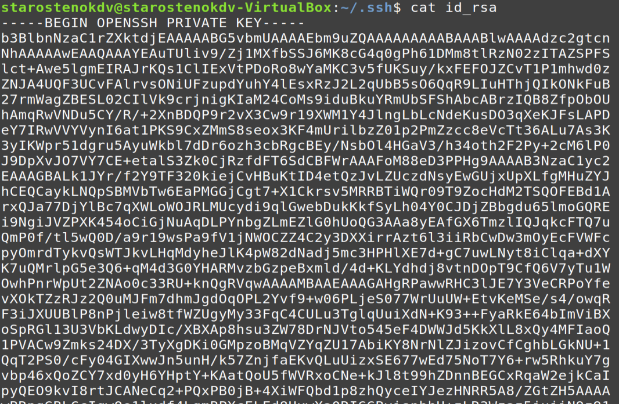


Рис. 10 – Настройки ssh-сервера



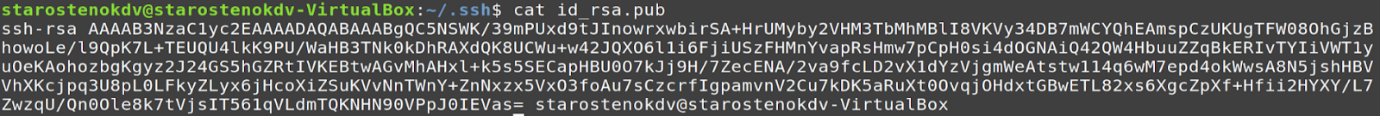


Рис. 11 – Публичный и приватный ключи

9. Перезапустите ssh-сервер и подключитесь к нему, используя ключи для

Входа (Рис. 12).



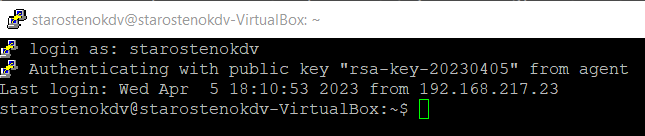
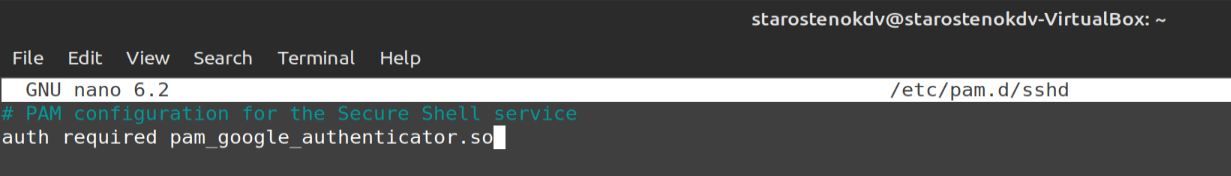


Рис. 12 – Подключение по ssh с использованием ключей

10. Настройте подключение к серверу по одноразовому паролю (Googleauthentication) (Рис. 13, 14, 15).



Рис. 13 – Уникальный ключ и QR-код



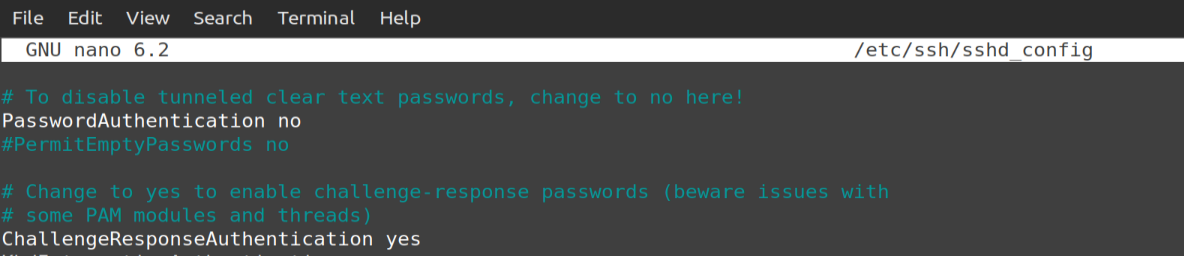


Рис. 14 – Настройка файла конфигурации

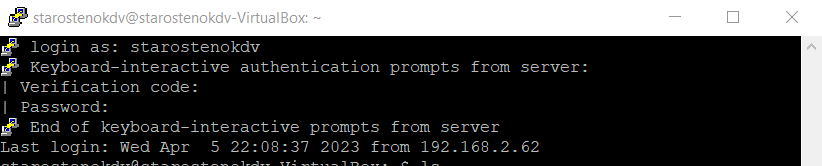


Рис. 15 – Подключение к серверу по одноразовому паролю

11. Измените приветственное сообщение: должна выводиться строка «ФИО

студента, номер группы» (Рис. 16).



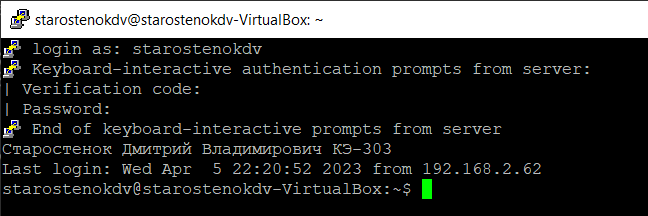


Рис. 16 – Приветственное сообщение

# КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Как определить, установлен ли в вашей системе OpenSSH?

ssh -v

2) При помощи какой команды вы установили в своей системе OpenSSH?

sudo apt install openssh-server

3) При помощи какой команды вы запускали свой ssh-сервер? Какая альтернативная команда может быть применена?

sudo service ssh start

4) Как определить состояние ssh-сервера?

sudo service ssh status

5) Для чего используется настройка PermitRootLogin?

Настройка PermitRootLogin определяет, разрешен ли вход на сервер под учетной записью root. Если установлено значение "no", то вход под учетной записью root запрещен.

6) Для чего используется настройка PasswordAuthentication?

Настройка PasswordAuthentication определяет, разрешен ли вход на сервер с использованием пароля. Если установлено значение "no", то вход по паролю запрещен.

7) Для чего используется настройка PermitEmptyPasswords?

Настройка PermitEmptyPasswords определяет, разрешены ли пустые пароли. Если установлено значение "no", то вход с пустым паролем запрещен.

8) Для чего используется настройка PubkeyAuthentication?

Настройка PubkeyAuthentication определяет, разрешен ли вход на сервер с использованием SSH-ключей. Если установлено значение "no", то вход по ключу запрещен.

9) Для чего используется настройка MaxAuthTries?

Настройка MaxAuthTries определяет максимальное количество попыток аутентификации. Если пользователь превышает это число попыток, то соединение закрывается.

10) Для чего используется настройка MaxStartups?

Настройка MaxStartups определяет максимальное количество одновременных подключений к серверу. Если количество подключений превышает это значение, то сервер начинает отклонять новые подключения.

11) Для чего используется настройка LoginGraceTime?

Настройка LoginGraceTime определяет время ожидания подключения пользователя. Если пользователь не аутентифицируется в течение этого времени, то соединение закрывается.

12) Что такое SSH-ключи? Какие выделяют виды этих ключей?

SSH-ключи – это механизм аутентификации, который позволяет пользователям подключаться к серверам без ввода паролей. Существуют два вида ключей: приватные и публичные. Приватный ключ хранится на клиентской машине, а публичный ключ располагается на сервере.

13) Как сгенерировать ключи для входа по ssh?

ssh-keygen

# СПИСОК ЛИТЕРАТУРЫ

1. Курячий, Г. В. Операционная система Linux: Курс лекций : учебное пособие / Г. В. Курячий, К. А. Маслинский. – Москва : ДМК Пресс, 2010. – 348 с. – ISBN 978-5-94074-591-4. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: для авториз. пользователей. <https://e.lanbook.com/book/1202>
2. Романов, С. Л. Утилиты обработки текста в операционной системе Linux : учебное пособие / С. Л. Романов. – Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2013. – 21 с. – ISBN 978-5-85546-744-4. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/63721
3. Романов, С. Л. Работа в операционной среде Linux: практикум для вузов : учебное пособие / С. Л. Романов. – Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2017. – 74 с. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/121866
4. Войтов, Н. М. Основы работы с Linux. Учебный курс : учебное пособие / Н. М. Войтов. – Москва : ДМК Пресс, 2010. – 216 с. – ISBN 978-5-94074-148-0. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/1198
5. Зубков, С. В. Linux. Русские версии / С. В. Зубков. – Москва : ДМК Пресс, 2007. – 347 с. – ISBN 5-94074-013-8. – Текст : электронный // Лань : электронно-библиотечная система. – Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/1192