Липецкий государственный технический университет

Факультет автоматизации и информатики

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №7

по Операционной системе Linux

Работа с SSH

Студент Лобов М.Ю.

Группа АИ-18

Руководитель Кургасов В.В.

Доцент, к.п.н.

Липецк 2021 г.

Цель работы

Ознакомиться с программным обеспечением удалённого доступа к распределённым системам обработки данных.

Задание

1. Подключиться к удалённому серверу по паролю;
2. Просмотреть окружение пользователя;
3. Сгенерировать пару ключей доступа к серверу, передать публичный ключ на сервер;
4. Проверить работоспособность подключения к хосту по ключу;
5. Организовать подключение к хосту по имени.

Ход работы

Первым шагом будет авторизация на сервере по выданным нам данным. Войдём под пользователем stud4 с помощью команды ***ssh*** (использованием в качестве операнда ***–l stud4***) и введём пароль. Попадаем в директорию нашего пользователя на сервере:

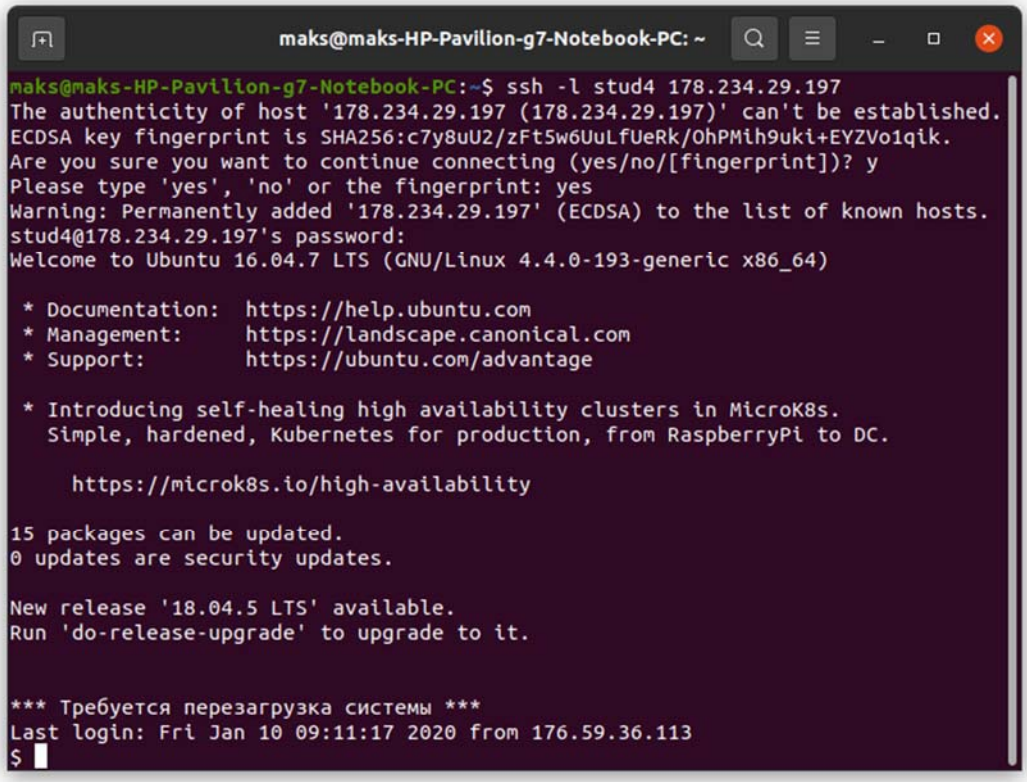

Рисунок 1 – Подключение к серверу с паролем

Теперь посмотрим окружение пользователя на хосте:

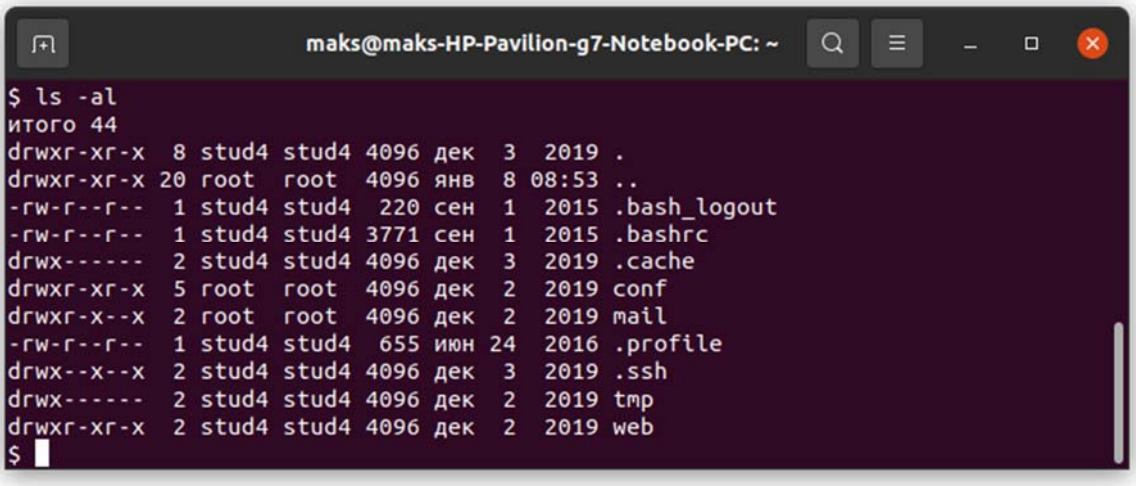

Рисунок 2 – Окружение пользователя

Теперь займёмся генерацией ключей. Для этого используется команда ***ssh-keygen***. После этого консоль спросит нас, где хранить ключи (рекомендуется оставить по умолчанию) и ввести секретную фразу для входа. После этого сгенерируется пара ключей: приватный (по умолчанию хранится в ~/.ssh/id_rsa) и публичный (по умолчанию хранится в ~/.ssh/id_rsa.pub):

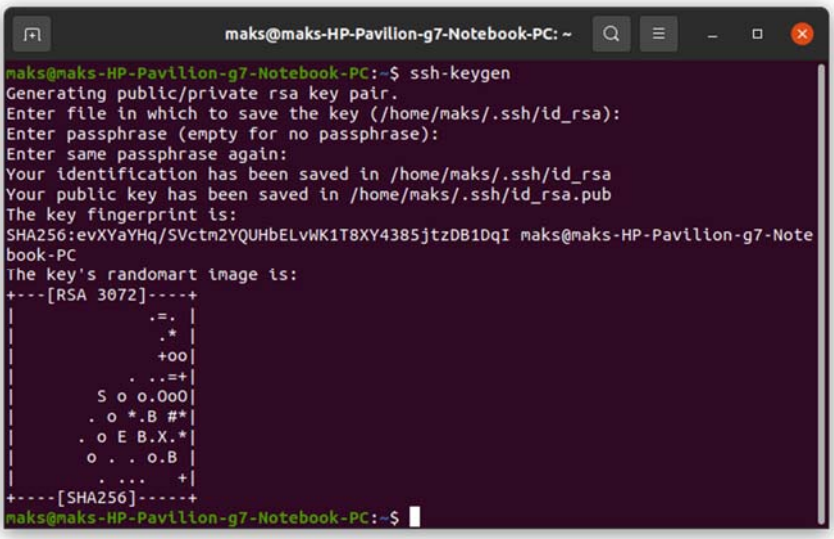

Рисунок 3 – Генерация ключей

Проверим наличие созданных файлов:

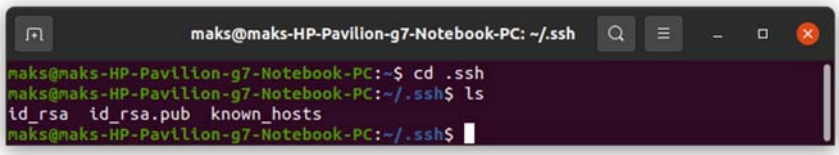

Рисунок 4 – Файлы с ключами

После этого мы должны передать публичный ключ на сервер с помощью команды ***ssh-copy-id*** с использованием опции –i, которая позволяет передать в качестве операнда расположение файла, хранящего публичный ключ:

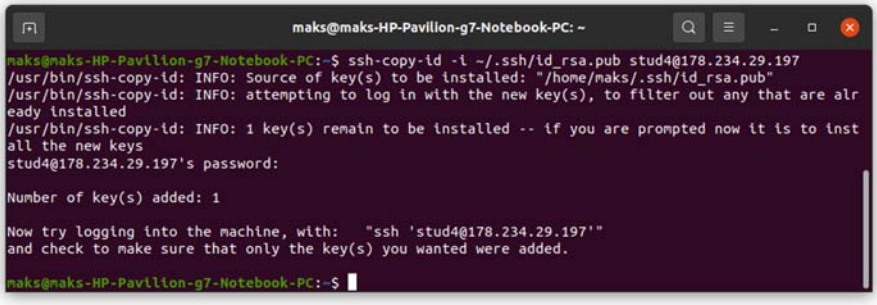

Рисунок 5 – Передача публичного ключа на сервер

И теперь пробуем подключиться к серверу без использования пароля:

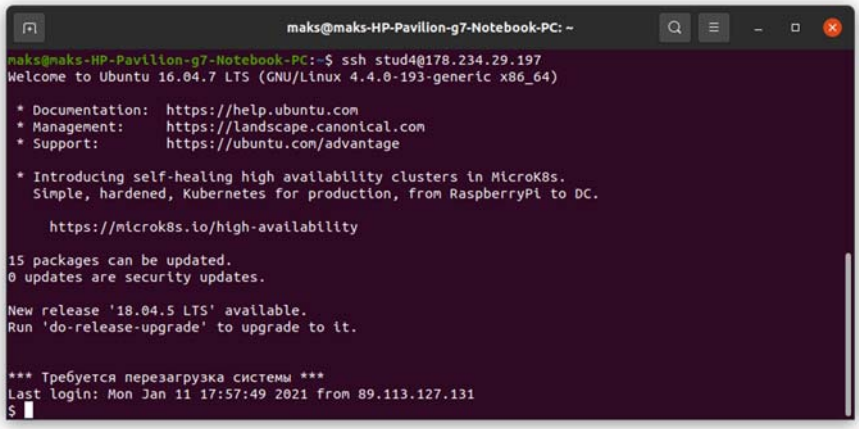

Рисунок 6 – Подключение к серверу по ключу

Теперь настроим доступ к серверу по заданному имени. Для этого инициализируем файл конфигурации в директории ~/.ssh и заполним файл следующим образом:

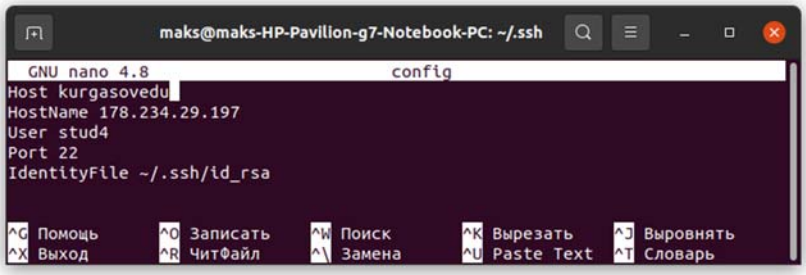

Рисунок 7 – Файл конфигурации

И теперь пробуем подключиться к хосту по заданному имени:

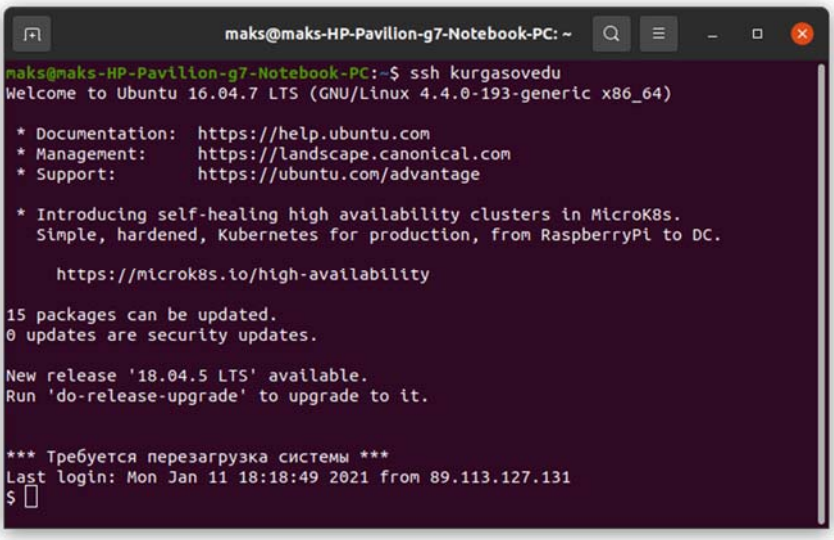

Рисунок 8 – Подключение к серверу по заданному имени

Вывод

В ходе выполнения лабораторной работы были изучены основы работы с программным обеспечением удалённого доступа к распределённым системам обработки данных.

Ответы на контрольные вопросы

1. Что такое ключ ssh? В чем преимущество их использования?

SSH-ключи используются для идентификации клиента при подключении к удалённому серверу. SSH-ключи представляют собой пару ключей – приватный и публичный. Приватный ключ хранится в закрытом доступе у клиента, публичный отправляется на сервер.

Преимущество использования ключей в удобстве (не нужно запоминать пароли) и безопасности (взломать приватный ssh-ключ достаточно сложно).

2. Как сгенерировать ключи ssh в разных ОС?

Генерация ssh-ключа в ОС Linux возможна с помощью команды ssh-keygen.

В ОС Windows можно использовать программу PuTTY для генерации ssh-ключей и подключения по shh-протоколу.

3. Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Нет, невозможно.

4. Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Да, будут. Утилита ssh-keygen каждый раз случайно генерирует пару ключей.

5. Перечислите доступные ключи для ssh-keygen.exe

- DSA;
- RSA;
- ECDASA;
- Ed25519.

6. Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Можно, но безопасность такого ключа уже не гарантирована.

7. Возможно ли организовать подключение «по ключу» ssh к системе с ОС Windows, в которой запущен OpenSSH сервер?

Да, возможно, с использованием программы PuTTY.

8. Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

Один из самых известных – GitHub.