**Липецкий государственный технический университет**  
Факультет автоматизации и информатики  
Кафедра Автоматизированных систем управления

Лабораторная работа №7

по курсу «Операционная система Linux»

Работа с SSH

Курбатова К.А.

Студент

Группа АИ-17

Кургасов В.В.

Руководитель

Доцент

Липецк 2019 г.

Цель работы

Лабораторная работа предназначена для практического ознакомления с программным обеспечением удаленного доступа к распределённым системам обработки данных.

Задание

1. Подключиться к удаленному хосту по ssh используя выданные данные.
2. Просмотреть окружение пользователя.
3. Сгенерировать ключ доступа по ssh без пароля, передать ключи на удаленный сервер.
4. Проверить работоспособность подключения по ключу.
5. Настроить файл конфигурации ssh, и добавить подключение к хосту по заданному имени.

Ход работы

1. Подключение к удалённому хосту происходит по выданному адресу следующей командой *ssh* *stud5@www.kurgasov.ru* . Сервер просит пароль, который был нам выдан, после успешного ввода попадаем в директорию пользователя.



Рисунок 1- Подключение к удалённому хосту по shh используя выданные данные

1. Посмотреть окружение пользователя можно с помощью команды ls.
2. Генерируем ключ и передаем публичный ключ на удалённый хост происходит по следующими командами представленными на скриншоте ниже:

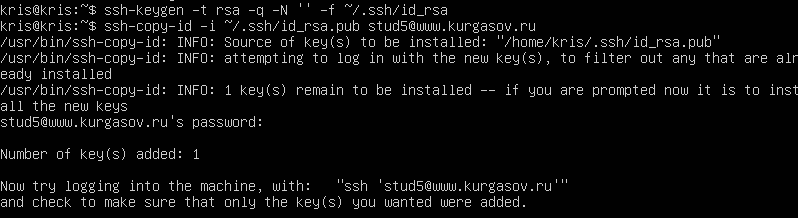


Рисунок 2 – Генерация ключа и передача публичного ключа на удалённый сервер

1. Проверяем работоспособность подключения без пароля, с помощью ключа к хосту:

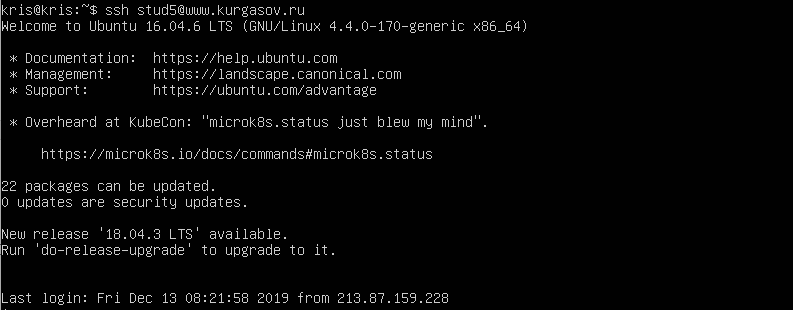


Рисунок 3 – Проверка подключения с помощью ключа

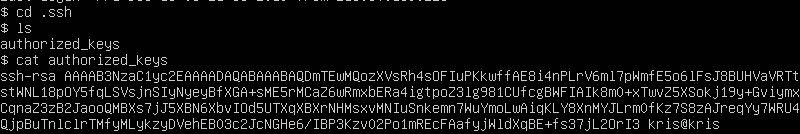


Рисунок 4 – Проверка нашего публичного ключа на сервере

1. Настройка файл конфигурации ssh, и добавление подключения к хосту по заданному имени:

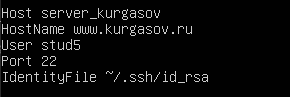


Рисунок 5 – Настройка конфигурационного файла

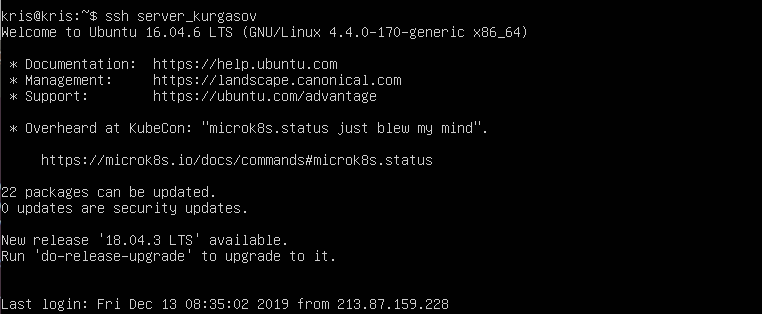


Рисунок 6 – Подключение к хосту по заданному имени в конфигурационном файле

Контрольные вопросы

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

SSH-ключи используются для идентификации клиента при подключении к серверу. SSH-ключи представляют собой пару — закрытый и открытый ключ. Закрытый должен храниться в закрытом доступе у клиента, открытый отправляется на сервер.

Преимущества в том, что не нужно запоминать пароли и взломать ssh-ключ, который хранится у пользователя очень проблематично.

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?

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, конечно будут, благодаря генератора случайного ключа.

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 c 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.

Вывод

Ознакомилась с программным обеспечением удаленного доступа к распределённым системам обработки данных, а именно подключение к удалённому серверу с помощью ssh-ключа.