

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.

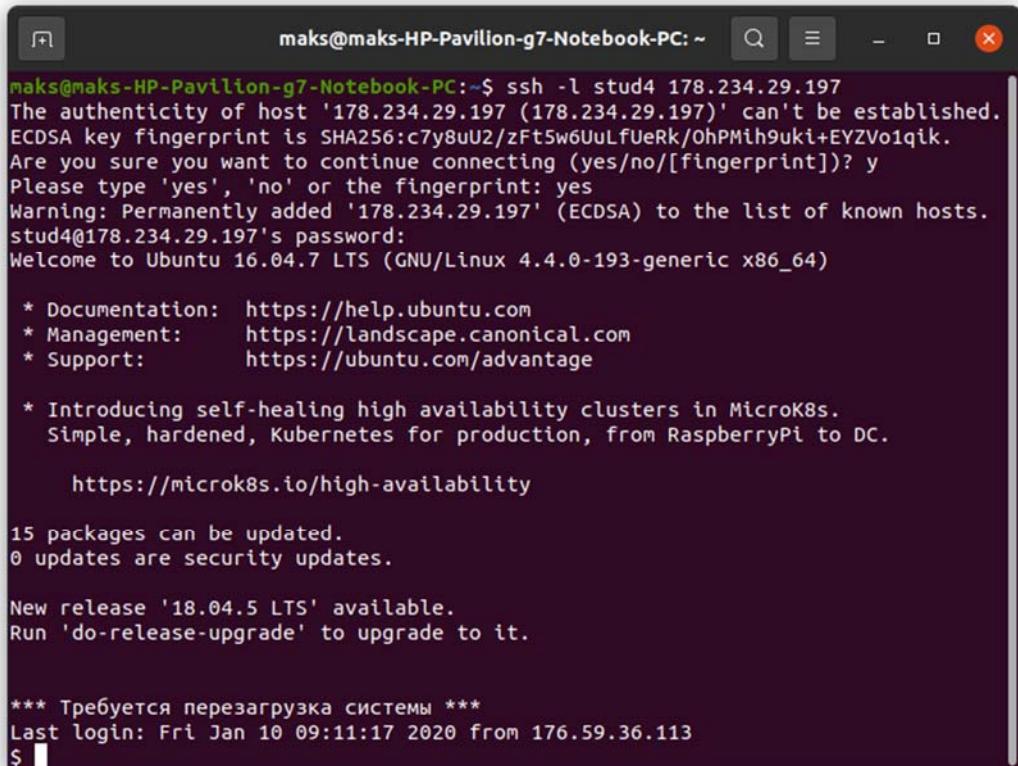
Задание

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:



```
maks@maks-HP-Pavilion-g7-Notebook-PC:~$ ssh -l stud4 178.234.29.197
The authenticity of host '178.234.29.197 (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/0hPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '178.234.29.197' (ECDSA) to the list of known hosts.
stud4@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

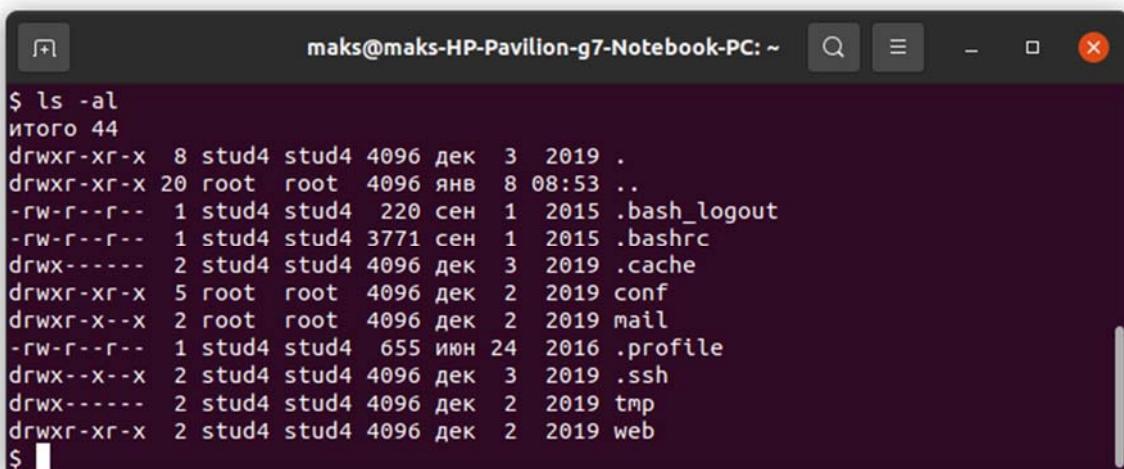
15 packages can be updated.
0 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Fri Jan 10 09:11:17 2020 from 176.59.36.113
$ 
```

Рисунок 1 – Подключение к серверу с паролем

Теперь посмотрим окружение пользователя на хосте:



```
maks@maks-HP-Pavilion-g7-Notebook-PC:~$ ls -al
итого 44
drwxr-xr-x  8 stud4 stud4 4096 дек  3  2019 .
drwxr-xr-x 20 root  root  4096 янв  8 08:53 ..
-rw-r--r--  1 stud4 stud4  220 сен  1 2015 .bash_logout
-rw-r--r--  1 stud4 stud4 3771 сен  1 2015 .bashrc
drwx----- 2 stud4 stud4 4096 дек  3  2019 .cache
drwxr-xr-x  5 root  root  4096 дек  2  2019 conf
drwxr-xr-x  2 root  root  4096 дек  2  2019 mail
drwxr-xr-x  2 root  root  4096 дек  2  2019 tmp
-rw-r--r--  1 stud4 stud4  655 июн 24 2016 .profile
drwxr-xr-x  2 stud4 stud4 4096 дек  3  2019 .ssh
drwx----- 2 stud4 stud4 4096 дек  2  2019 web
$ 
```

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`):

```
maks@maks-HP-Pavilion-g7-Notebook-PC: ~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/maks/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/maks/.ssh/id_rsa
Your public key has been saved in /home/maks/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:evXYaYHq/SVctm2YQUhbELvWK1T8XY4385jtzDB1DqI maks@maks-HP-Pavilion-g7-Notebook-PC
The key's randomart image is:
+---[RSA 3072]---+
|          . = |
|         .* |
|        +oo|
|       . .-+|
|      S o o.oo|
|     . o *.*B #*|
|     . o E B.X.*|
|     o . . o.B |
|     .... +|
+---[SHA256]---+
maks@maks-HP-Pavilion-g7-Notebook-PC: ~$
```

Рисунок 3 – Генерация ключей

Проверим наличие созданных файлов:

```
maks@maks-HP-Pavilion-g7-Notebook-PC: ~/ssh$ cd .ssh
maks@maks-HP-Pavilion-g7-Notebook-PC: ~/ssh$ ls
id_rsa id_rsa.pub known_hosts
maks@maks-HP-Pavilion-g7-Notebook-PC: ~/ssh$
```

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:

```
maks@maks-HP-Pavilion-g7-Notebook-PC: ~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud4@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/maks/.ssh/id_rsa.pub"
/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 all the new keys
stud4@178.234.29.197's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'stud4@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

maks@maks-HP-Pavilion-g7-Notebook-PC: ~$
```

Рисунок 5 – Передача публичного ключа на сервер

И теперь пробуем подключиться к серверу без использования пароля:



```
maks@maks-HP-Pavilion-g7-Notebook-PC:~$ ssh stud4@178.234.29.197
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

15 packages can be updated.
0 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Mon Jan 11 17:57:49 2021 from 89.113.127.131
$ 
```

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:

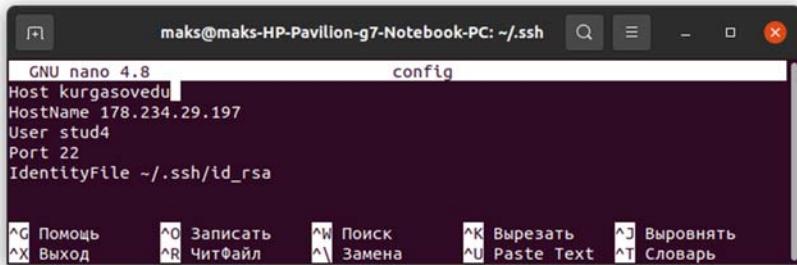
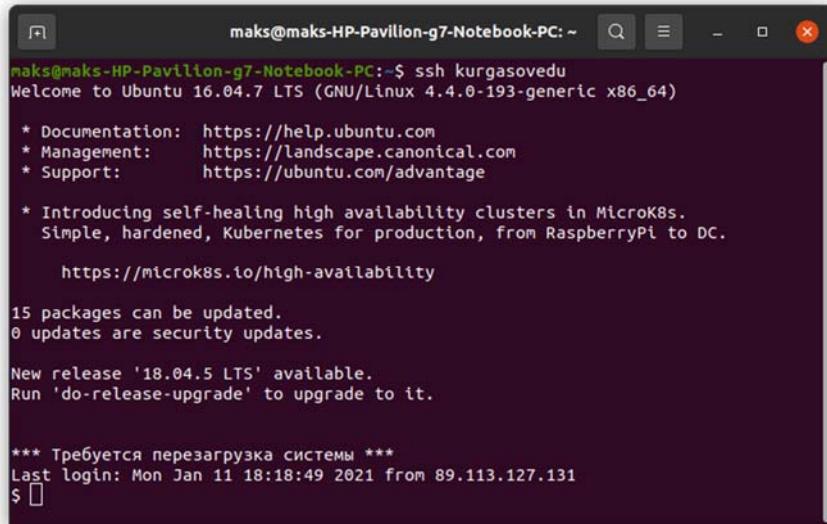


Рисунок 7 – Файл конфигурации

И теперь пробуем подключиться к хосту по заданному имени:



```
maks@maks-HP-Pavilion-g7-Notebook-PC:~$ ssh kurgasovedu
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

15 packages can be updated.
0 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** Требуется перезагрузка системы ***
Last login: Mon Jan 11 18:18:49 2021 from 89.113.127.131
$ 
```

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 ssh-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.