

Липецкий государственный технический университет
Факультет автоматизации и информатики
Кафедра автоматизированных систем управления

Лабораторная работа №7
по Дисциплине «Операционная система Linux»
на тему «Работа с SSH»

Студент

Глебов Д.А.

Группа АИ-18

Руководитель

Кургасов В.В.

к.п.н.

Липецк 2020 г.

Цель работы

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

Задание кафедры

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 stud12@178.234.29.197`. Сервер просит пароль, который был нам выдан, после успешного ввода попадаем в директорию пользователя.

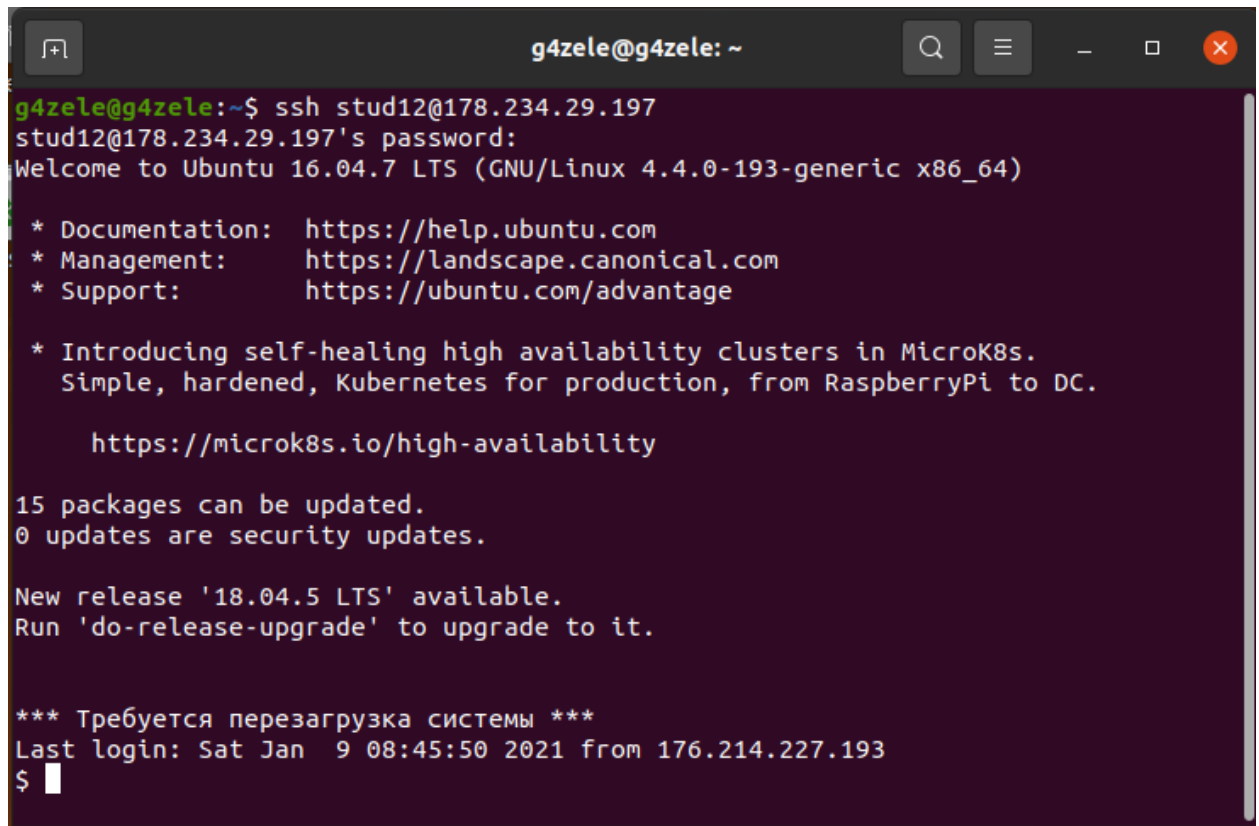
A screenshot of a terminal window titled 'g4zele@g4zele: ~'. The terminal shows the execution of the command 'ssh stud12@178.234.29.197'. The user is prompted for a password, and after successful authentication, they are logged into the remote host. The terminal displays the Ubuntu 16.04.7 LTS welcome message, including links for documentation, management, and support. It also shows system update information, stating that 15 packages can be updated and 0 security updates are available. A new release '18.04.5 LTS' is mentioned as available. At the bottom, it shows the last login time and IP address: 'Last login: Sat Jan 9 08:45:50 2021 from 176.214.227.193'. The prompt is '\$ '.

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

2. Для просмотра окружения пользователя в появившемся окне доступа пишем `ls -f`

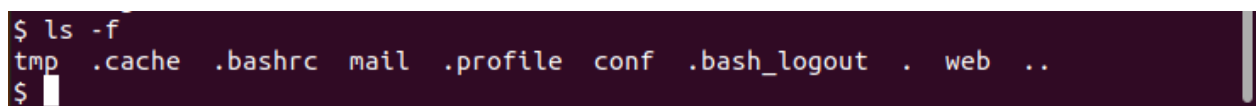
A screenshot of a terminal window showing the output of the command 'ls -f'. The output lists the files and directories in the current directory: 'tmp .cache .bashrc mail .profile conf .bash_logout . web ..'. The prompt is '\$ '.

Рисунок 2- Окружение пользователя

3. Генерируем ключ и передаем публичный ключ на удалённый хост происходит по следующими командами представленными на скриншоте ниже

```
g4zele@g4zele:~$ ssh-keygen -t rsa -q -N '' -f ~/.ssh/id_rsa
g4zele@g4zele:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud12@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/g4zele/.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 the new keys
stud12@178.234.29.197's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'stud12@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

g4zele@g4zele:~$
```

Рисунок 3 – Генерация ключа и передача публичного ключа на удалённый сервер

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

```
g4zele@g4zele:~$ ssh stud12@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 12:09:06 2021 from 176.214.227.193
$
```

Рисунок 4 – Проверка подключения с помощью ключа

```
$ cd .ssh
$ ls
authorized_keys
$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC6UkfhZU5xhqhgX9uQRA0u9JfL55/g/Eqg0INpj70v
83mwtASF+pNSJ4LDHBeOfjdrDkv+b1ABe92/UthcdLWfd8PpJjZznwCA288ImVsRweywcDXWTD82ZnfS
DoWDYJ+RJUCUxJgKLAJWliCdp5cN3G04ns7dhmC3KZ/YU4ViZd51liYfuRWIPQpwanjtsNRdSCQOR2iD
YkpJLjADokZLL/zeUtJpRbTFNipgTTnTHPXbXhclQItm1eLZjwiZudt2n3X18LbE56TJLRREuYiqymMp
q1+2GJHfONYOQHSgLYVlpuiHSIb0EslkAgrqHjYhgppqwfDANVeQBdGD0htXLIuiyNFh0CG2aAlq8u6y
iWkIoohopWVnl3uL001vxNIwqtbYR2xGrVXKJjymvndZdMHu5AttRpITbqEcNAs1zR3fuNGpJA+6lpH
Px0C0QAw9zgHtYtFoREcWdH+7D5fQFMRC2r91hy2d5kg8Me6011r1pCqFRZJJImivovu/pU= g4zele@
g4zele
$
```

Рисунок 5 – Проверка публичного ключа на сервере

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

```
Host 178.234.29.197
HostName www.kurgasov.ru
User stud12
Port 22
IdentityFile ~/.ssh/id_rsa
```

Рисунок 6 – Настройка конфигурационного файла

```
g4zele@g4zele:~/.ssh$ service ssh restart
g4zele@g4zele:~/.ssh$ ssh 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 12:28:03 2021 from 176.214.227.193
$
```

Рисунок 7 – 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 ssh-протоколу.

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

Невозможно из «секретного» ключа сгенерировать «публичный» и/или наоборот.

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, благодаря генератору 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 с ОС Windows, в которой запущен OpenSSH сервер?

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.