

Липецкий государственный технический университет

Факультет автоматизации и информатики

Кафедра автоматизированных систем управления

ЛАБОРАТОРНАЯ РАБОТА №6

по Операционной системе Linux

Работа с SSH

Студент

Жидков И.А.

Группа АС-19

Руководитель

Кургасов В.В.

Доцент, к.п.н.

Липецк 2022 г.

Оглавление

Цель работы	3
Ход работы	4
Вывод	12
Контрольные вопросы	13

Цель работы

Ознакомиться с программным обеспечением удаленного доступа к распределенным системам обработки данных.

Задание кафедры

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 stud3 с помощью команды ssh (использованием в качестве операнда -l stud3) и введем пароль. Попадаем в директорию нашего пользователя на сервере:

```
author@testserver:~$ ssh -l stud3 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/OhPMih9uki+EY2Vo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '178.234.29.197' (ECDSA) to the list of known hosts.
stud3@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

22 packages can be updated.
5 updates are security updates.

Last login: Sat Jan 30 21:40:08 2021 from 178.234.219.186
stud3@kurgasov:~$
```

Рисунок 1 - подключение к серверу с паролем

Теперь посмотрим окружение пользователя на хосте:

```
Last login: Sat Jan 30 21:40:08 2021 from 178.234.219.186
stud3@kurgasov:~$ ls
conf  file  mail  new_text.txt  stud_LR7.txt  tmp  web
stud3@kurgasov:~$ ls -al
итого 64
drwxr-xr-x 10 stud3 stud3 4096 янв 29  2021 .
drwxr-xr-x 20 root  root  4096 янв  8  2021 ..
-rw-r--r--  1 stud3 stud3  220 сен  1  2015 .bash_logout
-rw-r--r--  1 stud3 stud3 3771 сен  1  2015 .bashrc
drwx-----  3 stud3 stud3 4096 янв 29  2021 .cache
drwxr-xr-x  5 root  root  4096 дек  2  2019 conf
drwx-----  3 stud3 stud3 4096 янв 29  2021 .config
-rw-r--r--  1 stud3 stud3   10 янв 28  2021 file
drwx-----  3 stud3 stud3 4096 янв 29  2021 .local
drwxr-x--x  2 root  root  4096 дек  2  2019 mail
-rw-r--r--  1 stud3 stud3   10 янв 29  2021 new_text.txt
-rw-r--r--  1 stud3 stud3  655 июн 24  2016 .profile
drwx-----  2 stud3 stud3 4096 дек 13  2019 .ssh
-rw-r--r--  1 stud3 stud3   90 янв 29  2021 stud_LR7.txt
drwx-----  2 stud3 stud3 4096 дек  2  2019 tmp
drwxr-xr-x  2 stud3 stud3 4096 дек  2  2019 web
stud3@kurgasov:~$ _
```

Рисунок 2 - окружение

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 генерируется пара ключей: приватный (по умолчанию хранится в ~/.ssh/id_rsa) и публичный (по умолчанию хранится в ~/.ssh/id_rsa.pub): Проверим наличие созданных файлов:

```

stud3@kurgasov:~$ выход
Connection to 178.234.29.197 closed.
author@testserver:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/author/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/author/.ssh/id_rsa
Your public key has been saved in /home/author/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:HXZNVKP14PXTGdYBFMOQd9zKstKBwB1hR1P70gKNUog author@testserver
The key's randomart image is:
+---[RSA 3072]-----+
|
| . oB=*B*0=|
| oo.o.*0o0|
| .o.++o=0|
| =.oo.o .|
| S o. +.|
| . . . o.|
| . . . .0|
| . . . . .|
| E . . . .|
+---[SHA256]-----+
author@testserver:~$ _

```

Рисунок 3 - генерация ключа

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:

```

author@testserver:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud3@178.234.29.197
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/author/.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
stud3@178.234.29.197's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud3@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.
author@testserver:~$

```

Рисунок 4 - передача ключа

И теперь пробуем подключиться к серверу без использования пароля:

```
Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'stud3@178.234.29.197'"
and check to make sure that only the key(s) you wanted were added.

author@testserver:~$ ssh stud3@178.234.29.197
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 18:11:44 2022 from 100.112.176.147
stud3@kurgasov:~$
```

Рисунок 5 - подключение без пароля

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

```
author@testserver:~/.ssh$ ls
config id_rsa id_rsa.pub known_hosts
author@testserver:~/.ssh$ cat config
Host kurgasovedu
HostName 178.234.29.197
User stud3
Port 22
IdentityFile ~/.ssh/id_rsa
author@testserver:~/.ssh$ ssh kurgasovedu
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 18:21:56 2022 from 100.112.176.147
stud3@kurgasov:~$ _
```

Рисунок 6 - содержание файла и подключение без пароля

Теперь проверим публичный ключ.

```
Last login: Tue Jan 25 18:21:56 2022 from 100.112.176.147
stud3@kurgasov:~$ cd .ssh
stud3@kurgasov:~/.ssh$ ls
authorized_keys  config
stud3@kurgasov:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQQDEYKq/8lwWIZGSiZAhI7ek2WtyoDZikcJaTmgN0VqPqDuL7zp3LiuU0f21EauG
h8Vck7ynBHptzYBxA6axJXM19TAdDGxAnJzSwtNYSIEZLekvsMAWEckphiYURKMxKTg/HEBv2br+i/7ijQHv7uJLQU04FCgbK6/+
uoWNm4hUwdMvoapRlgiighc/JVI1n1QxxQQSv6fhh/RMKRFdYkGziAm2AjUbh6LZ13sdrNGRxn/0wpsK0XqrPDxZ4f8Xyb5zXZq
Y5KH/1GSaqPaRCbcIQaJ+zY1oVfVf+/IOToJpsXSCctCI4WP/ds8WkmdCQSDR9XNti+G2Y21m1Js8zxMwpVq8BhHJgCp3K/UXZLQ
oTcIRJIFevWeDd9FNW17eHPHBK7+2gKrno2bK1Kj+WLe43rndDLHUefSm2emHS//La8GGXdK2JtY+JdXkxGXL1HkzTr0EQW0WWZ5
x0ShjURwCcRHa8gn0rwINVxZfe1sAB/x1IyvTF2254j89hjLhHE= tatyana@arianrod
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQD16yYwsWThNMz6iYggtQNm/KHV11XSQ84Lh0hZCC6KVBZFzth0NpMfV2huGEFY
NYX41vwABR/yVUg11W+yFz16Q9BmPvmgtAjrJ6H213IGKtdsie2DpxoDpZ0yBG0TL6i3RVzxUXgpN5Ta1FA4q0hsbA5VDDLJDpWW
GS5zXn2FYRAqKhP1kCNkuGvV5Fh0Bqv1Jg28AezBaCRhGeJmccLifw63ceyLo26vp6HcWdCHdJ3VI9VP0Auxrkk3wDJWYEBUgM1S
+/KazYy9A6WbgUNmmz78Gs+1SgoqT4q09r1JbE1K2xBSR+F9tSAk+BSG115t2+2knNRCdcRYA5+mY1FtnVNYtJTr1NnRBfjiBvR4
fKLTVgE0ehuIy1zfT2TeCY0Y91zYuSzx7uBmDERo3p+rDGGFKxrCb3d/UU0PRbqfjx3Fz7ofWCcn5XJ7sQmL0krHciYvPMbnB1j
v6nFERScVu+aBCYe0Z90zzvgXf79Q2T1vzQzpwWqoKGpbfVBnM8= author@testserver
stud3@kurgasov:~/.ssh$ _
```

Рисунок 7 - публичный ключ на сервере

Вывод

В ходе выполнения лабораторной работы были изучены основы работы с программным обеспечением удаленного доступа к распределенным 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;
- ECDSA;
- 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