

Липецкий государственный технический университет

Отчет по Лабораторной работе № 7 по дисциплине «Операционная система Linux» на тему «Авторизация по ключу ssh»

Студент

Руководитель

доцент, к.п.н.

учёная степень, учёное звание

подпись, дата

подпись, дата

Елфимова Д.А.

фамилия, инициалы

Кургасов В.В.

фамилия, инициалы

Липецк 2019 г.

Задание

Организовать доступ к удаленному серверу по ssh (без ввода пароля (по ключу)) имея следующие исходные данные:

Web-интерфейс: www.kurgasov.ru:8084

stud9 rV6MBb6zgC

IP: 178.234.29.197 Порт:22

Оглавление

1. Ход работы	4
2. Вопросы	5
Заключение	8

1. Ход работы

1. Создаем открытый и закрытый ключ нашей локальной системы:

```
$ ssh-keygen -t rsa -q -N '' -f ~/.ssh/id_rsa
```

2. Настраиваем удаленную систему на то, чтобы она авторизовывала SSH по открытому ключу:

```
$ ssh-copy-id -i ~/.ssh/id_rsa.pub stud9@178.234.29.197
```

или следующим образом

```
scp ~/.ssh/id_rsa.pub user@remote.org.ua:~
```

```
$ ssh user@remote.org.ua
```

```
remote$ [ -d ~/.ssh ] || (mkdir ~/.ssh; chmod 711 ~/.ssh)
```

```
remote$ cat ~/id_rsa.pub >> ~/.ssh/authorized_keys
```

```
remote$ chmod 600 ~/.ssh/authorized_keys
```

```
remote$ rm ~/id_rsa.pub
```

```
elfida@elfida:~$ scp ~/.ssh/id_rsa.pub stud9@edu.kurgasov.ru:~
stud9@edu.kurgasov.ru's password:
Permission denied, please try again.
stud9@edu.kurgasov.ru's password:
id_rsa.pub                                     100% 395      0.3KB/s   00:01
elfida@elfida:~$ _
```

Рисунок 1. Открытый ключ

3. Ключом можно воспользоваться и войти без пароля следующим образом

```
elfida@elfida:~$ ssh -i ~/.ssh/id_key stud9@edu.kurgasov.ru
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)

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

 * Overheard at KubeCon: "microk8s.status just blew my mind".
    https://microk8s.io/docs/commands#microk8s.status

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

New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

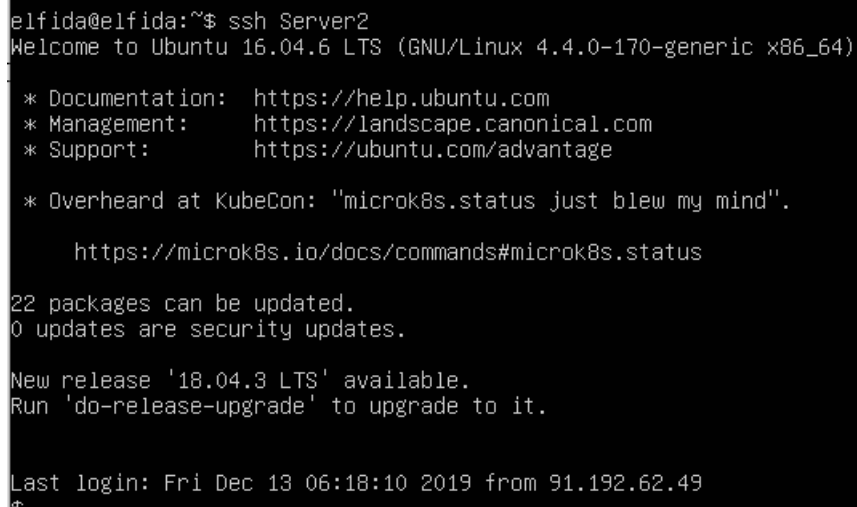
Last login: Fri Dec 13 06:10:33 2019 from 91.192.62.49
```

Рисунок 2. Ключ

4. Пропишем сервера в конфигурационном файле `/.ssh/config`

```
Host Server2 #"имя по желанию"#
HostName 178.234.29.197 #" IP или доменное имя сервера "
User stud9 #"Или другой пользователь, который есть на сер
Port 22 #"Лучше 22 не использовать, но по умолчанию именн
IdentityFile ~/.ssh/id_rsa #"Его закрытый ключ"#
```

5. Теперь подключаться можно простой командой используя прописанное нами в `config` имя хоста:



```
elfida@elfida:~$ ssh Server2
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)

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

 * Overheard at KubeCon: "microk8s.status just blew my mind".
    https://microk8s.io/docs/commands#microk8s.status

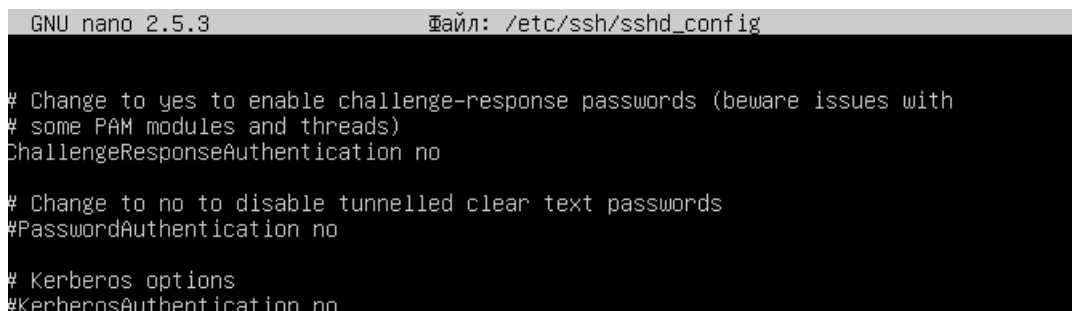
22 packages can be updated.
0 updates are security updates.

New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec 13 06:18:10 2019 from 91.192.62.49
```

Рисунок 3. Подключение

6. Также рекомендуется отключить пароли в файле `sshd_config`, однако данному пользователю не хватает для этого прав доступа.



```
GNU nano 2.5.3          Файл: /etc/ssh/sshd_config

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication no

# Kerberos options
#KerberosAuthentication no
```

Рисунок 4. Отключение паролей

2. Вопросы

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

Secure Shell - это зашифрованный протокол, который часто используется для взаимодействия и удаленного управления серверами. Если необходимо что-либо сделать на удаленном сервере, скорее всего, придется воспользоваться SSH и работать через терминал. Существуют способы дополнительной безопасности, например, fail2ban1, но аутентификация по ключу SSH более надежна. В отличие от пароля, взломать SSH-ключ практически невозможно.

2. Как сгенерировать ключи ssh в разных ОС?

В Linux для генерации ключа достаточно использовать утилиту ssh-keygen. Она позволяет генерировать ключи разными алгоритмами и с дополнительными параметрами. В Windows можно использовать программу Putty, которая кроме доступа по ssh протоколу позволяет генерировать ssh – ключи.

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

Нет. А если и возможно, то это займет огромное количество времени.

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 отличаться из-за использования генератора случайных чисел.

5. Перечислите доступные ключи для ssh-keygen.exe

- RSA
- DSA
- ECDSA
- ed25519

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

Можно, однако не стоит из соображений безопасности.

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

Да, возможно. Можно использовать программу Putty

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

Заключение

В ходе данной лабораторной работы были изучены или повторно рассмотрены некоторые команды ОС Linux, было проведено ознакомление и анализ рекомендованной литературы, а также информации об использовании SSH в ОС Ubuntu для авторизации.