Добавление ssh ключа - id_rsa.pub

Копирование публичного ключа вручную

Необходимо убедиться, что директория *~/.ssh* существует (в папке пользователя)

`mkdir -p ~/.ssh` - Если ее нет то данная команда создаст. Далее можно создать или отредактировать файл *authorized_keys*, это можно сделать командой `echo` **`строка_публичного_ключа`** `>> ~/.ssh/authorized_keys` Строка должна начинаться с *ssh-rsa AAAA...*

Далее убедимся, что директория *~/.ssh* и файл *authorized_keys* имеют подходящие права доступа: `chmod -R go= ~/.ssh`

`chmod 700 ~/.ssh` - ограничьте права доступа к этому каталогу только себе!

Эта команда удаляет права доступа для “group” и “other” для директории *~/.ssh/.*

Если вы используете аккаунт *root* для настройки ключей для аккаунта пользователя, важно, чтобы директория *~/.ssh* принадлежала этому самому пользователю, а не пользователю *root* :

`chown -R yuzer:yuzer ~/.ssh`

В нашем руководстве мы используем пользователя с именем ***yuzer*** , вам же следует использовать имя своего пользователя в команде выше.

Аутентификация на сервере Ubuntu с использованием ключей SSH

`ssh username@remote_host` - вход на сервер по *ssh*

Если вы заходите на удалённый хост по SSH в первый раз, вы можете увидеть вывод следующего вида:

```
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

Это означает, что ваш локальный компьютер не узнал удалённый хост. Напечатайте “*yes*” и нажмите `ENTER` для продолжения.

Отключение аутентификации по паролю на вашем сервере

вход на сервер с использованием пароля всё есть активен, что означает, что сервер уязвим для атак с перебором пароля (brute-force attacks). Вход *ssh* по паролю можно отключить отредактировав файл *sshd_config*

`sudo nano /etc/ssh/sshd_config`

Внутри файла найдите директиву *PasswordAuthentication*. Она может быть закомментирована. Раскомментируйте её при необходимости и установите её значение в “*no* ”. Это отключит возможность входа на сервер по паролю.

```
...
PasswordAuthentication no
...
```

Для применения внесённых изменений нам необходимо перезапустить сервис *sshd* - `sudo systemctl restart ssh`

В качестве меры предосторожности откроем новое окно терминала и проверим, что соединение по *ssh* работает корректно, перед тем, как закрывать текущую сессию.

Скопировать ключ так же можно с помощью scp (с одного хоста на другой)

`scp -p /home/yuzer/.ssh/authorized_keys yuzer@10.0.10.48:/home/yuzer/.ssh/`

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2   #Пример синтакса
```

> SCP - перезапишет уже сущесвующий файл!

Revision #11
Created 2020-10-29 21:22:47 UTC by yuzer
Updated 2023-09-11 22:28:14 UTC by yuzer