ssh — вход по ключу

Есть рабочий ПК (Linux) и сервер, нужно сделать вход на сервер по ключу с этого ПК. На ПК с которого будем заходить на сервер в терминале выполняем:

```
$ ssh-keygen
```

или

```
$ ssh-keygen -f .ssh/note
```

-f тут — указать на файл ключа. Если её не использовать — ssh-keygen предложит сохранить в файл с именем по умолчанию — .ssh/id_rsa.

В процессе вы увидите

```
Enter passphrase (empty for no passphrase):
```

здесь можно ввести парольную фразу для ключа, как еще одна из ступеней защиты.

```
The key's randomart image is:
+--[ RSA 2048]----+
|      ..o        |
|       E o= .    |
|       o. o      |
|          ..     |
|      ..S        |
|     o o.        |
|   =o.+.         |
|. =++..          |
|o=++.            |
+-----------------+
```

Теперь у вас есть открытый и закрытый ключи, которые можно использовать для аутентификации. После этого нужно скопировать открытый ключ на сервер, чтобы затем настроить беспарольную аутентификацию на основе SSH-ключей.

Передадим ключ на сервер утилитой ssh-copy-id

```
ssh-copy-id username@remote_host
```

Если будет ругаться

```
$ ssh-copy-id username@remote_host
Could not open a connection to your authentication agent.
no keys found
```

нужно помочь ключем -i:

```
$ ssh-copy-id -i .ssh/id_rsa.pub username@remote_host
```

Пробуем подключиться

```
$ ssh username@remote_host
```

В .ssh создаем файлик conf с таким содержанием:

```
$ cat .ssh/config

Host remote_host
    HostName 192.168.0.15
    User username
```

Теперь можно подключаться так:

```
$ ssh remote_host
```

Отключение парольной аутентификации

Теперь можно отключить механизм парольной аутентификации, чтобы защитить сервер от brute-force атак.

> Важно! Прежде чем выполнять этот раздел, убедитесь, что на этом сервере вы настроили аутентификацию на основе SSH-ключей для учетной записи root или для пользователя с привилегиями sudo. Этот раздел заблокирует поддержку паролей для входа в систему, и вы можете случайно заблокировать себя на собственном сервере.

Убедившись, что ваша удаленная учетная запись имеет все необходимые привилегии, зайдите на свой удаленный сервер с помощью SSH-ключей (либо с правами администратора, либо через

учетную запись с привилегиями sudo). Затем откройте файл конфигурации демона SSH:

```
$ sudo nano /etc/ssh/sshd_config
```

Внутри файла найдите директиву PasswordAuthentication. Она может быть закомментирована. Раскомментируйте строку и установите значение «no». Это отключит возможность входа в систему через SSH с использованием паролей учетных записей:

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

Сохраните и закройте файл. Чтобы обновить настройки, необходимо перезапустить сервис sshd:

```
$ sudo systemctl restart sshd.service
```

В качестве меры предосторожности откройте новое окно терминала и проверьте работу сервиса SSH:

```
ssh username@remote_host
```

После того как вы подтвердите работу сервиса SSH, можете закрыть все текущие сеансы сервера.

Демон SSH теперь поддерживает только аутентификацию по SSH-ключам. Парольная аутентификация успешно отключена.

https://www.8host.com/blog/ustanovka-ssh-klyuchej-v-centos-7/