

Вход по ключу в SSH

Помимо использования SSH на не стандартном порту (не панацея), лучше усилить защиту используя вход по ключу. Пару ключей SSH сложнее взломать по сравнению с обычным паролем. Содержимое ключей генерируется с использованием алгоритмов, что затрудняет его перебор. Доступ может получить только машина, на которой находится закрытый ключ.

Аутентификация с открытым ключом никогда не показывает серверу содержимое закрытого ключа. В случае компрометации сервера локальная машина останется в безопасности.

Тк в течении 2023 года появлялись научные статьи о возможной компрометации алгоритма RSA, для генерации ключа мы будем использовать алгоритм использующий эллиптические кривые. На машине Linux (Хост А или Б) выполните следующую команду:

```
ssh-keygen -t ecdsa -b 521
```

Далее нажимаем просто клавишу Enter. Либо можно задать имя для ключевой пары или добавить пароль.

Добавление пароля к закрытому ключу добавляет многофакторную аутентификацию.

Выполняем действия на машине на которую хотим заходить по SSH (Хост Б), в корневой директории пользователя если нет папки `.ssh`, то ее необходимо создать:

```
cd ~  
mkdir .ssh
```

Копируем содержимое публичного ключа (`my_key.pub`) и добавляем его содержимое в файл домашней директории пользователя `root` `authorized_keys` в папке `.ssh` пример команды ниже, для удобства можно использовать удобный вам текстовый редактор (в нашем случае публичный ключ был скопирован на Хост Б):

```
cat my_key.pub >> .ssh/authorized_keys
```

Либо операцию выше можно выполнить с помощью другой команды:

```
ssh-copy-id -i /root/.ssh/my_key root@<Хост Б>
```

Теперь на Хосте Б нужно поменять конфиг сервиса `sshd`, чтобы по SSH по паролю вход был запрещен:

```
vi /etc/ssh/sshd_config
```

Раскомментируем/Добавляем следующие строки:

```
PasswordAuthentication no  
PermitEmptyPasswords no
```

Получем следующее:

```
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication no  
PermitEmptyPasswords no
```

Выходим из редактирования с сохранением (для vi потребуется отдельная статья, чтобы узнать как оттуда выйти - шутка).

Перезапускаем службу сервиса SSH на Хосте Б:

```
systemctl restart sshd.service
```

Теперь на Хост Б можно зайти из машины, где присутствует закрытый ключ, пример команды подключения с ключом на Linux системах:

```
ssh -i my_key root@<Хост Б>
```

А при попытке входа по паролю на Хост Б будет возникать подобная ошибка:

```
C:\Users\boris>ssh root@[redacted].ru -p 22  
root@[redacted].ru: Permission denied (publickey).
```

Revision #2

Created 14 December 2023 09:52:53 by Boris RZR

Updated 12 August 2024 13:53:51 by Boris RZR