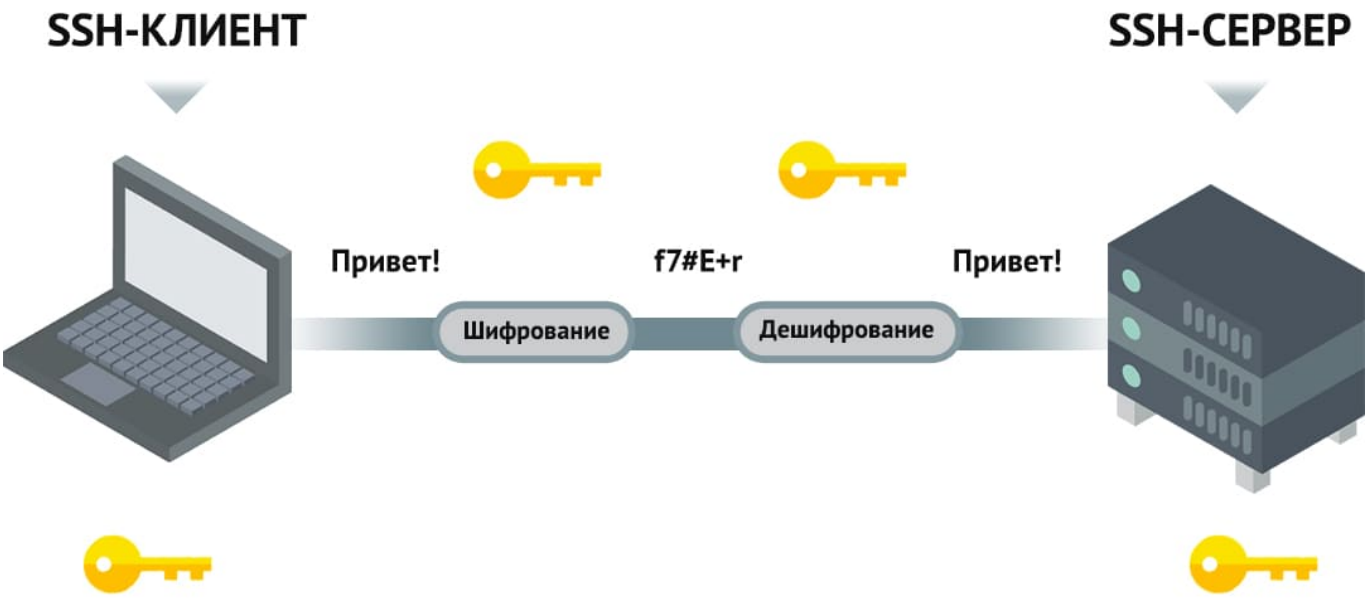
SSH в VPS по адресу 45.89.230.189

Логин с помощью ssh

Теория

SSH (англ. `Secure Shell` — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой. Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, **шифрует весь трафик**, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем. SSH — это протокол прикладного уровня. SSH-сервер обычно прослушивает соединения на TCP-порту **22**.



Способы входа:

- Аутентификация **по паролю** распространена (необходимо ввести пароль пользователя).
- Аутентификация **по ключевой паре** предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. На машине, с которой требуется произвести подключение, **хранится закрытый ключ**, а на удалённой машине — **открытый**. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.
- Аутентификация **по ip-адресу небезопасна**, эту возможность чаще всего отключают.

Примеры

Утилита `ssh` по-умолчанию установленна в ОС Windows. Предположим, что необходимо зайти с помощью `ssh` на выделенный сервер по `ipv4` адресу `45.89.230.189`, имя пользователя, к аккаунту которого необходимо подключиться - `test`:

```
PS C:\Shlack> ssh test@45.89.230.189
test@45.89.230.189's password:
```

После чего нас спрашвают пароль, ввод которого по причинам безопасности не будет отображаться. После успешного ввода, видим следующее стандартное сообщение при входе в систему для дистрибутива Ubuntu:

```
PS C:\Shlack> ssh test@45.89.230.189
test@45.89.230.189's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Tue Nov 23 19:00:10 2021 from 79.142.197.154
$
```

Если пароль невенрный, видим следующие сообщение (пару секунд задержка):

```
PS C:\Shlack> ssh test@$vps1
test@45.89.230.189's password:
Permission denied, please try again.
test@45.89.230.189's password:
```

Задание 1, ввойти в систему с помощью логина и пароля

При помощи `ssh` зайти на `ipv4` адресс `45.89.230.189` с помощью предоставленного логина и пароля.

Создание файлов и директорий

После выполнения входа, есть возможность создавать, редактировать, удалять и запускать файлы, что находятся в директории. Также есть возможность выполнять установленные программы.

С помощью команды `mkdir` можно созать директорию:

```
test@vm355614:~$ mkdir test_dir
test@vm355614:~$ ls
test  test_dir
test@vm355614:~$
```

Также можно перейти в эту директорию и создать там файл:

```
test@vm355614:~$ cd test_dir/
test@vm355614:~/test_dir$ touch test_file.txt
test@vm355614:~/test_dir$
```

Можно воспользоваться встроенным редактором `nano` или `vi` (не надо `vi`)))))) для редактирования файла:

```
test@vm355614:~/test_dir$ nano test_file.txt
```

После чего откроется окошко редактора. Список сочитаний клавишь и что они делают можно посмотреть внизу экрана (например `^S` - сохранить содержимое, `^X` - выход), где значек `^` - означает кнопку `CTRL`.

Задание 2

Создать папку с вашем именем, в которой создать два файла:

1. `name.txt`, в котором написать ФИО;
2. `date.txt`, в котором указать дату.

Логин с помощью ssh ключей

Пары ключей SSH представляют собой два защищенных шифрованием ключа, которые можно использовать для аутентификации клиента на сервере SSH. Каждая пара ключей состоит из **открытого ключа** и **закрытого ключа**.

Закрытый ключ хранится **клиентом** и должен быть **защищен**. Любое нарушение безопасности закрытого ключа позволит злоумышленникам входить на серверы с соответствующим открытым ключом без дополнительной аутентификации. В качестве дополнительной меры предосторожности ключ можно зашифровать на диске с помощью парольной фразы.

Соответствующий открытый ключ можно **свободно передавать**, не опасаясь негативных последствий. Открытый ключ можно использовать для шифрования сообщений, расшифровать которые можно **только** с помощью открытого ключа. Это свойство применяется как способ аутентификации с использованием пары ключей.

Открытый ключ выгружается на удаленный сервер, на который вы хотите заходить, используя SSH. Этот ключ добавляется в специальный файл `~/.ssh/authorized_keys` в учетной записи пользователя, которую вы используете для входа, где символ `~` - это домашняя директория пользователя, для которого устанавливается вход с помощью ключей.

Генерация ключей

Для начала ключи необходимо создать, это делается с помощью встроенной утилиты `ssh-keygen`, после чего нужно указать путь к файлам, которые будут хранить ключи:

```
PS C:\Shlack\keys> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key:
```

После чего, нам необходимо дважды ввести кодовую фразу (пароль при использовании) для ключей, **для удобства можно оставлять поля пустыми**:

```
PS C:\Shlack\keys> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\den/.ssh/id_rsa): test-key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in test-key.
Your public key has been saved in test-key.pub.
The key fingerprint is:
SHA256:vMKNdtrfx4gS2/xbw490/8MSzP/L72hvd7gkpzwn4KU den@DESKTOP-FH4OCQB
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|                 |
|       .         |
```

```
|        S   o    |
|     . o... .=   |
|      = +* =.o@..|
|     . =o Eo+OBX=|
|      . .o..*B=B^|
+----[SHA256]-----+
PS C:\Shlack\keys>
```

Видим небольшую превью нашего ключа. Файлы можно увидеть внутри текущего каталога:

```
PS C:\Shlack\keys> dir | findstr test
-a----        11/25/2021  11:57 PM           2610 test-key
-a----        11/25/2021  11:57 PM            574 test-key.pub
PS C:\Shlack\keys>
```

Конфигурация сервера

Необходимо ввойти на выделенный сервер с помощью **пароля**:

```
PS C:\Shlack\keys> ssh test@45.89.230.189
test@45.89.230.189's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Nov 26 00:45:17 2021 from 79.142.196.227
test@vm355614:~$
```

Перейти в домашний каталог (скорее всего избыточно):

```
test@vm355614:~$ cd ~
test@vm355614:~$
```

Создать скрытую папку `.ssh`:

```
test@vm355614:~$ mkdir .ssh
```

Папка будет скрытой, для того чтоб ее увидеть необходимо использовать параметр `ls -a`:

```
test@vm355614:~$ ls -a
.  ..  .bash_history  .cache  .local  .ssh
```

Переходим в папку:

```
cd .ssh
```

Открытый ключ хранится в файле с форматом .pub, закрытый формата не имеет. Создаем файл `authorized_keys` с (или дополняем), содержимым открытого ключа:

```
test@vm355614:~/.ssh$ echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC8I+CBFIJmvhY2O9CQluC4kgT63iyoqVsEOVd5jBDhZ9WzxkqPw0
ifhPuhb1IJojDtdTpA5KBrbFStwxpmVclX9srw4jtEBs+4736P+P1VH2bwCSSKAH3UmUT2HTaPzGNIr0u+
B2inPvYfI7J3JViDEF/pMoLNQDXYNvJ8d872al4NfGWToM861cEJc6OdSahFaC+9/LE3xAM7in6f2DQT2T
1igGw8GdMR84m0Pzi+wusl8X1q54fxTS9vGrjyZRtrfV4eYtuSJ9HENTzG+CgBt8HNKxlSBemFGs0BXeg3
RtAKgwl9qeC0w0RF2Zt/BaBCkMHKl3Qo0h/2m178M260f8IufpdQQyh9hvAUavaBH+I4JHYYyu0Hmsbaqq
Zga1LdUyAlrGX1cn4jgaJZEZwhZWyIQWHxggy9s1I00+EpPfUkYdSblb7ZyysJ7RKSB+FiExTJ8xyKYkl+
l7nX7Aekzi2lDG89xUHMNhoWNtMGy3nCStPP17NLIkbpRpsYSN0= den@DESKTOP-FH4OCQB
>> authorized_keys
test@vm355614:~/.ssh$
```

Можем убедиться в его содержимом с помощью `cat`:

```
test@vm355614:~/.ssh$ cat authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC8I+CBFIJmvhY2O9CQluC4kgT63iyoqVsEOVd5jBDhZ9WzxkqPw0
ifhPuhb1IJojDtdTpA5KBrbFStwxpmVclX9srw4jtEBs+4736P+P1VH2bwCSSKAH3UmUT2HTaPzGNIr0u+
B2inPvYfI7J3JViDEF/pMoLNQDXYNvJ8d872al4NfGWToM861cEJc6OdSahFaC+9/LE3xAM7in6f2DQT2T
1igGw8GdMR84m0Pzi+wusl8X1q54fxTS9vGrjyZRtrfV4eYtuSJ9HENTzG+CgBt8HNKxlSBemFGs0BXeg3
RtAKgwl9qeC0w0RF2Zt/BaBCkMHKl3Qo0h/2m178M260f8IufpdQQyh9hvAUavaBH+I4JHYYyu0Hmsbaqq
Zga1LdUyAlrGX1cn4jgaJZEZwhZWyIQWHxggy9s1I00+EpPfUkYdSblb7ZyysJ7RKSB+FiExTJ8xyKYkl+
l7nX7Aekzi2lDG89xUHMNhoWNtMGy3nCStPP17NLIkbpRpsYSN0= den@DESKTOP-FH4OCQB
test@vm355614:~/.ssh$
```

Конфигурация завершена. Можем попробовать зайти с помощью ключей. Для этого нам необходимо использовать параметр `-i` и указать файл **секретного** ключа:

```
PS C:\Shlack\keys> ssh test@45.89.230.189 -i .\test-key
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Nov 26 01:07:30 2021 from 79.142.196.227
test@vm355614:~$
```

Задание 3, ввойти в систему с помощью пары ключей

Сгенерировать пару ключей в `ssh-keygen`, при помощи `ssh` зайти на `ipv4` адресс `45.89.230.189` с помощью логина и пароля, предоставленного в таблице. Сконфигурировать возможность входа с помощью ключа.