

2. Система SSH

Система SSH



- Защищенная криптографией альтернатива r-командам, telnet и ftp
- Помимо пакета OpenSSH могут применяться другие реализации, например droidbear
- Может применять криптографическую аутентификацию
- Может создавать туннельные соединения

Система SSH (Secure Shell) предоставляет защищенную криптографически надежную альтернативу r-командам и службе telnet.

Она открывает зашифрованный канал связи между удаленными узлами, предоставляет возможность аутентификации с использованием публичных и частных ключей (несимметричное шифрование), защищает от подмены IP адресов.

В GNU/Linux используется версия системы SSH - OpenSSH, распространяемая на свободной основе.

Пакет OpenSSH представлен тремя основными программами:

- sshd - сервер SSH, прослушивающий 22 порт TCP.
- ssh - клиент службы SSH, позволяющий инициировать удаленный сеанс.
- scp – клиентская программа для удаленного копирования.
- sftp – безопасный вариант ftp клиента

Серверная и клиентская части системы OpenSSH обладают разными файлами конфигурации:

- сервер sshd имеет конфигурационный файл /etc/ssh/sshd_config.
- клиенты ssh и scp - /etc/ssh/ssh_config.

Сервер OpenSSH запускается самостоятельно (standalone), поэтому для автоматического старта сервера OpenSSH при переходе в многопользовательский режим следует надлежащим образом настроить систему инициализации.

Пример :

Глава 5. Службы удаленного доступа

```
# systemctl enable sshd
```

Для инициирования сеанса на удаленной машине с запущенным сервером OpenSSH достаточно на клиентском узле просто выполнить команду `ssh`, указав ей в качестве аргумента имя или IP адрес узла назначения.

Пример:

```
$ ssh sinix
The authenticity of host 'sinix (198.11.11.25)' can't be established.
RSA key fingerprint is ac:1d:51:58:6f:f4:3a:b9:a7:ac:82:b3:25:1e:3a:30.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sinix,198.11.11.25' (RSA) to the list of known
hosts.
user@sinix's password:
Last login: Fri Jul  2 19:33:26 2004

$ hostname
sinix.gruss.de

$ exit
logout
Connection to sinix closed.
```

Примечание: В этом примере пользователь `user` открыл с помощью команды `ssh` удаленный сеанс на узле `sinix.gruss.de`. При этом был использован простейший вариант аутентификации с использованием пароля. Обратите внимание на то, что так как вход в сеанс с данного узла осуществлялся впервые, сервер OpenSSH предупредил, что внес данные о клиентском узле в файл `~/.ssh/known_hosts`. В этом файле хранятся специальные шифрованные сигнатуры, позволяющие идентифицировать клиентский узел.

Одна из наиболее часто используемых опций команды `ssh` является `-l`, с помощью которой можно указать имя пользователя для входа в удаленный сеанс.

Пример:

```
susel> ssh -l apox restrict.nocom.com
```

Примечание: В этом примере пользователь `susel` иницирует удаленный сеанс на узле `restrict.nocom.com` под именем пользователя `apox`, зарегистрированного на этом узле.

Команда `scp` позволяет копировать файлы на удаленную машину и с нее.

Пример:

```
$ scp sinix:~/linux.tar /tmp
apox@sinix's password:

linux.tar                                100% 210KB  0.0KB/s  00:00

$ ls /tmp/li*
/tmp/linux.tar
```

Примечание: Команда `scp` скопировала с удаленного компьютера файл `linux.tar` и поместила его в каталог `/tmp` на локальной машине.

Также можно в явном виде указать имя пользователя на удаленной машине.

Пример:

Глава 5. Службы удаленного доступа

```
susel> scp webadm@sinix:/var/www/html/susel.php .  
webadm@sinix's password:
```

```
susel.php                                100%   22KB   0.0KB/s   00:00
```

Примечание: В этом примере пользователь susel скопировал с удаленной машины файл, аутентифицировавшись на ней как пользователь webadm.



Система SSH

- **Криптографическая аутентификация**
 1. Создается пара ключей (публичный и частный) на клиенте
 2. Публичный ключ копируется на сервер
 3. Публичный ключ на сервере добавляется в файл доверенных ключей `.ssh/authorized_keys`

Не смотря на то, что команды `ssh` и `scp` используют зашифрованный канал, во многих случаях аутентификацию с помощью пароля нельзя признать безопасной.

В таких случаях можно использовать криптографическую аутентификацию.

SSH предоставляет возможность использовать аутентификацию по протоколам RSA и DSA.

Несимметричное шифрование используется лишь на стадии аутентификации. После подтверждения аутентичности пользователя дальнейшая связь осуществляется с применением симметричного шифрования, так как оно обеспечивает приемлемый уровень быстродействия системы, а несимметричное - нет.

Первое, что необходимо сделать для обеспечения возможности аутентификации с помощью RSA - это создать командой `ssh-keygen` пару ключей несимметричного шифрования.

После создания пары ключей несимметричного шифрования, необходимых для аутентификации пользователя, требуется поместить каким-либо путем публичный ключ на удаленный хост, с которым требуется обеспечить связь. Для этого можно зайти на него, используя `ssh`, и скопировать с помощью `scp` публичный ключ с собственного узла на удаленный узел.

Пример :

```
sa@cl:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sa/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sa/.ssh/id_rsa
Your public key has been saved in /home/sa/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:nmPIEXtLKbZa3fgrEHns0WrSV4oRpt5yBg1TNG/3Ly0 sa@cl
```

Глава 5. Службы удаленного доступа

The key's randomart image is:

```
+----[RSA 3072]-----+
|      o+      |
|      o oo     |
|      .O oo .   |
|      =o*o.....|
|      .=BS= o   |
|      o=XX=o    o|
|      =BO..     E o|
|      o ..o     o|
|      .   .o.   |
+----[SHA256]-----+
```

***Примечание:** Эта команда создает пару ключей RSA. Они помещаются в подкаталог `.ssh` домашнего каталога пользователя, вызвавшего команду. Файл `id_rsa` содержит частный ключ, доступ к которому должен быть предоставлен лишь его владельцу. Файл `id_rsa.pub` должен быть помещен на удаленный узел, с которым необходимо обеспечить связь по зашифрованному каналу.*

Парольная фраза, которую требуется ввести здесь - это "пропуск" к частному ключу. Допускается не вводить ее, но в таком случае частный ключ не будет защищен.

Пример: копирование публичного ключа на удаленный узел.

```
sa@c1:~$ scp .ssh/id_rsa.pub 10.0.200.1:/home/sa/c1.key.pub
sa@10.0.200.1's password:
id_rsa.pub                                100% 559      65.5KB/s   00:00
sa@c1:~$ ssh 10.0.200.1
sa@10.0.200.1's password:

sa@r2:~$ cat c1.key.pub >> .ssh/authorized_keys
sa@r2:~$ crщв 600 .ssh/authorized_keys
sa@r2:~$ rm c1.key.pub
sa@r2:~$ exit
```

***Примечание:** На первом шаге этой процедуры пользователь копирует ключ на узел `10.0.200.1`.*

Далее он подключается к этой машине, и находясь в сеансе на удаленном узле, публичный ключ добавляется к базе данных публичных ключей, находящейся в файле `.ssh/authorized_keys`, права доступа к которому должны быть ограничены лишь его владельцем.

После выхода из сеанса следующий инициированный сеанс будет открыт при условии успешной аутентификации с помощью частного и публичного ключей.

Ключ можно добавить в файл `.ssh/authorized_keys` простой командой, запущенной на клиенте:

Пример: копирование публичного ключа на удаленный узел.

```
sa@c1:~$ ssh-copy-id 10.255.255.101
The authenticity of host '10.255.255.101 (10.255.255.101)' can't be established.
ED25519 key fingerprint is SHA256:Q138Pxa07MEo+jqRq8ndjbdNa1wdou0R0Vmc60nMTDs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
sa@10.255.255.101's password:

Number of key(s) added: 1
```

Глава 5. Службы удаленного доступа

Now try logging into the machine, with: `"ssh '10.255.255.101'"`
and check to make sure that only the key(s) you wanted were added.