Cómo utilizar las llaves SSH para conectarse sin una contraseña.

OpenSSH es una forma muy segura de conectarse de forma remota a una máquina Slackware. Pero la forma más fácil de usar SSH es, simplemente, usar sus llaves.

El concepto de claves públicas/privadas puede ser difícil de explicar, trataremos de hacerlo de la manera más simple posible.

Permítanme decir esto de nuevo, para todos ustedes, crypto nerds allí afuera: Sí, ya sé que esta es una versión muy simplificada de SSH. Esto se crea para todos los novatos SSH… mmmmkay?

Esencialmente, las llaves SSH se basan en la criptografía de clave pública. Esto significa que creas dos claves: una se llama llave pública y se usa para cifrar datos que solo usted puede descifrar. Puede dar su llave pública a cualquier persona, ya que su única función es cifrar datos - No hay mucho más que puedas hacer con él. La otra llave se llama llave PRIVADA, y es esta llave la que se utiliza para descifrar los datos cifrados con la llave pública.

Hasta ahora todo bien … Ahora, ¿cómo se usa esto con SSH?

Cada vez que se comunique con una máquina Slackware (o cualquier máquina que ejecute OpenSSH, en realidad) a través del protocolo SSH, su SSH cliente (el programa, instalado en la computadora que tiene delante, que utiliza para conectarse) hablará con el SSH server instalado en la máquina distante. Determinarán en conjunto las capacidades que ambos pueden usar y la versión del protocolo que deben usar para comunicarse de forma segura.

Luego, intentarán determinar cómo usted (el usuario) iniciará sesión en la máquina remota. Si no se usan las claves, usualmente SSH (pero no siempre) predeterminará para pedirle una contraseña. Por otro lado, si se usan claves, las máquinas las usarán en el siguiente orden:

Then, they will try to determine how you (the user) will login on the remote machine. If keys are not used, SSH will usually (but not always) default to asking you a password. On the other hand, if keys are used, the machines are going to use them in the following order:

1. El servidor SSH cifrará un mensaje corto (técnicamente un valor hash) con su llave pública y lo enviará a su computadora.
2. Su cliente de SSH descifrará este mensaje con la clave privada (cuya única copia debe estar en su computadora) y lo enviará de vuelta al servidor de SSH.
3. El servidor de SSH estará satisfecho de que usted 'sea usted', por así decirlo, ya que teóricamente es la única persona capaz de descifrar el mensaje enviado y le otorgará acceso de inmediato.

Si todo esto parece un poco complicado, solo recuerda esto: tienes una clave pública y una privada. La clave pública debe estar en la computadora a la que desea acceder, o la computadora 'remota'. La clave privada debe estar en su computadora.

¡Vamos a pasar por este proceso paso a paso!

Create the public/private key pair

To create a public and a private key, use the OpenSSH `ssh-keygen` utility. This will automatically generate a key pair, using the default values. Here is a small example:

```
noryungi@mypc:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/noryungi/.ssh/id_rsa): TEST.rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in TEST.rsa.
Your public key has been saved in TEST.rsa.pub.
The key fingerprint is:
1a:99:51:a6:12:69:53:aa:d8:f6:c2:56:66:6e:68:5a noryungi@udon
The key's randomart image is:
+--[ RSA 2048]----+
|    .o. o        |
|    +o +         |
|   .o.o          |
| o . . +         |
|. + + + S        |
| o B   o         |
|  E + .          |
| = o             |
|.                |
+-----------------+
noryungi@mypc:~$ ls TEST*
TEST.rsa  TEST.rsa.pub
```

OK, what is going on here? First, `ssh-keygen` is going to generate a key pair. So far, so good, please make sure you read the ssh-keygen man page to understand all the options, and there are many of them.

Next, `ssh-keygen` is going to respond that it is creating the RSA key pair (public and private key). RSA is the name of the encryption algorithm used. There are three such encryption possible: DSA, RSA and ECDSA. Which one is the best is left as an exercice for the reader... 

It is then going to ask you where to save the key. Here, `TEST.rsa` is entered, since there are other keys on the system. Giving a proper name to the key is important, since it makes it much easier to remember which key connects to what.

For instance, if you had an account on a machine named: `stang.slackware.com`, a good name for the key pair would be `stang_slackware_com.rsa` or some such.

Next, `ssh-keygen` asks you for a passphrase. It is always a good idea to enter a passphrase! This allows you to protect your private key, even if it falls into the wrong hands. If you are absolutely, 100% sure that your private key is **not** going to fall into the wrong hands (how optimistic you are!), just press `Enter` here.

The rest are just informative messages, and you will note that the key pair has been saved as follows:

1. The private key is named TEST.rsa.
2. The public key - the one you want to copy on the remote machine - is named TEST.rsa.pub

Congratulations! You are halfway there!

Configure your public key on the remote computer

All right, now, how to use the public/private key? That's simple enough: copy the public key (named TEST.rsa.pub as we have seen) onto the remote computer. The best way to do this is to use scp the OpenSSH secure copy program. For instance:

```
noryungi@mypc$ scp TEST.rsa.pub
nr@test.example.com:/home/nr/.ssh/authorized_keys
```

In the example above, I copy the public key TEST.rsa.pub on the remote machine named test.example.com, as user nr. The file is renamed authorized_keys which is the name of the file that contains all the public keys authorized to connect to the server.

A word of caution here: do not execute the scp command above if you already have an authorized_keys file on the remote computer! This will replace the content of the file with your public key!! If you already have an authorized_keys file, execute a cat TEST.rsa.pub » authorized_keys on the remote machine to add your public key at the end of authorized keys.

Since all the SSH keys you use should be placed in the .ssh directory, that's where it goes on the remote machine.

So, are we done? Not really, there is just one small thing to do, but it is truly important, since it is the source of a lot of problems...

Check the public key permissions on the remote machine

Since the private and public keys are very sensitive, they should be protected against prying eyes. To do this, on both the remote and the local machine, enter the following command:

```
nr@test.example.com$ chmod -R -v g-rwx,o-rwx ./.ssh/
mode of `./.ssh/' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of `./.ssh/authorized_keys' changed from 0644 (rw-r--r--) to 0600 (rw--
------)
```

This command allows you to make sure nobody (except you and the SSH server) can read the public key.

Please note: if the permissions on the authorized_keys file OR the .ssh directory are not correct OpenSSH won't use the keys! If you have any problem with a public/private key, check the permissions and/or run the above command to make sure they are correct!

Connect using your newly created SSH key

Let's try to connect, back on the local machine, to the remote server named `test.example.com`:

```
noryungi@mypc$ ssh -i TEST.rsa nr@test.example.com
```

Please note that I have entered the option `-i` right after the `ssh` command: this option selects the private key to be used to connect, as user `nr`, to the remote server named `test.example.com`.

If you have chosen to protect the private key with a passphrase, `ssh` will ask you this passphrase before connecting. If not... Well, if the permissions are correct (see above), you should see the equivalent of the following:

```
nr@test.example.com$
```

That's it! You are connected to a remote machine, without ever entering a password, and with a much better security than with a password - which can be guessed, while a key is way too long to be ever guessed.

What could go wrong at this point?

Well, not much, really, except the possibility that your system administrator does not want you to connect with a public/private key pair...

In which case, let's face it, he is not a very good system administrator. This can be checked, however, with the following command on the remote machine:

```
nr@test.example.com$ grep -i pubkeyauth /etc/ssh/sshd_config
#PubkeyAuthentication yes
```

Please note the `#PubkeyAuthentication yes` line: this is the default value for public key authentication, and, as you can see, it is set to `yes`. You are good to go and use your key! On the other hand, if you see something like this:

```
nr@test.example.com$ grep -i pubkeyauth /etc/ssh/sshd_config
PubkeyAuthentication no
```

Then you are not allowed to connect to the remote machine (`test.example.com` above) with a public key. Time to contact your system administrator or your security administrator and request politely to be able to use them.

(Yes, there are other, more sneaky, ways to connect without entering a password, but none of them are as secure as a public/private key pair - maybe in another documentation on this wiki?) 🙂

You have reached the end of this short documentation - go forth, and use OpenSSH keys!

See Also

- The OpenSSH manual pages (online)

Sources

- Originally written by Noryungi

howtos, security, ssh, sshkeys, author noryungi