Passwordless SSH Login

Passwordless SSH login can save the user and administrator time and hassles. To use this method of login one must login to the user's account once using a password to then setup passwordless entry.

The method involves creating a private/public key pair. The keys are placed in the user's .ssh subdirectory of the user's home directory on the local machine. A copy of the public key is placed into the authorized_keys file in the .ssh directory of the remote machine. Once that is done one can log into the remote machine from the local machine without a password.

Here are step by step instructions:
1) On the local machine cd to your home directory:
local $ cd

2) Create a subdirectory named .ssh:
local $ mkdir .ssh
Make sure the permissions of that directory allow all users to read files in that directory. e.g.
local $ chmod 755 .ssh

3) Change directory to .ssh:
local $ cd .ssh

4) Create the 2048 bit RSA public/private key pair. Accept the default file name and path of the key, and use an empty passphrase:
local $ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key: <press enter>
Enter passphrase (empty for no passphrase): <press enter>
Enter same passphrase again: <press enter>
Your identification has been saved in <default directory>/id_rsa.
Your public key has been saved in /<default directory>/id_rsa.pub.
The key fingerprint is:
<16 pairs of hex digits> username@machine-ip
The key's randomart image is:
<some ascii art>

5) Check that in your .ssh directory are these two files: id_rsa and id_rsa.pub.
local $ ls id*
id_rsa id_rsa.pub

You have created an RSA 2048 bit public/private key pair. The file with the .pub extension is the public key.

6) Now login to the remote machine:
local $ ssh my.remote.machine
password:<enter your password>
remote $
You are now logged into your home directory on the remote machine.

7) Change directory to the .ssh subdirectory. If it doesn't exist create it as was done above.
remote $ mkdir .ssh
remote $ cd .ssh

8) Copy your public key from the local machine to the remote machine's .ssh directory:
remote $ scp -p my.local.machine:~/.ssh/id_rsa.pub .

If that doesn't work due to a firewall issue try the copy from the other direction. That will require using your password. Go back to the local machine and do:
local $ scp -p ~/.ssh/id_rsa.pub my.remote.machine:~/.ssh
password:<enter your password>

9) Add the public key to the authorized_keys file in the .ssh directory:
remote $ cat id_rsa.pub >> authorized_keys

10) You can now log out from the remote machine so that you are back on the local machine, and then log into the remote machine again without using a password.
remote $ exit
local $ ssh my.remote.machine
remote $

For further info see the man pages for ssh-keygen, ssh, and sshd.

Joel Snow 2015-12-10