SSH_Key_Based_Authentication

November 9, 2017

1 Linux/Mac Tutorial: SSH Key-Based Authentication - How to SSH Without a Password

Video Tutorial by: Corey Schafer

1.0.1 Generating Private and Public Keys

- `$ ssh-keygen -t rsa -b 4096`
  - `-t rsa` just says what kind of key we want
  - `-b 4096` (default values is 248) said to make our keys more secure.
  - Public Keys reside on your machine, and the private keys reside on the hosts your remoting into.
- Once executed it will ask: `Enter file in which to save the key (/home/<user>/.ssh/id_rsa):`
  - Press enter to save in default location.
- You'll then be prompted with: `Enter passphrase (empty for no passphrase):`
  - You may enter one if you would like a password to type in.

1.0.2 Navigate to Keys in filesystem

- `$ cd ~/.ssh`
- `$ ls -al`
  - Prints out the following input:
  - `total 24 drwx------ 5 lawerencelee staff 160 Nov 8 15:17 . drwxr-xr-x+ 41 lawerencelee staff 1312 Nov 8 09:24 .. -rw------- 1 lawerencelee staff 3243 Nov 8 15:17 id_rsa -rw-r--r-- 1 lawerencelee staff 790 Nov 8 15:17 id_rsa.pub`
  - `id_rsa` is the private key, and `id_rsa.pub` is the public key.
  - Make sure remote machine has `.ssh` directory in the home directory.
    - If not, on remote machine `mkdir ~/.ssh`

1.0.3 Transfer Public Key to remote machine

- `$ scp ~/.ssh/id_rsa.pub <user>@<ip_address>:/<path to .ssh>/<new_key_name_if_you_like>`
- On remote machine: `$ cat ~/.ssh/<public_key_name> >> ~/.ssh/authorized_keys`
  - Copy public key to authorized_keys file.

1.0.4 Change Permissions of `.ssh` directory, and its contents.

- On remote machine: `$ chmod 700 ~/.ssh/`
- On remote machine: `$ chmod 600 ~/.ssh/*`

1.0.5 Check if we can now SSH in without a password.

- `$ ssh <user>@<ip_address>`

1.0.6 If you want to turn off Password Authentication and use only your Keys

- On remote machine: sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
  - Create a backup up the config file in case something goes wrong.
- On remote machine: `sudo nano /etc/ssh/sshd_config`
  - Within the file, look for:
    - `# Change to no to disable tunnelled clear text passwords`
      `#PasswordAuthentication yes`
  - Uncomment `PasswordAuthentication` line and change answer to `no`.
- On remote machine: `sudo service ssh restart`
  - Now changes are active.

1.0.7 The Easy Way to Transfer Public Keys to remote machine:

- For Mac users with Homebrew: `$ brew install ssh-copy-id`
- `$ ssh-copy-id <user>@<ip_address`
  - This automates the process of making a .ssh directory, copying the public key to the remote machine, creating the authorized_keys file, as well as setting the correct permissions for .ssh directory and its files.