**Author: Aaron Valoroso**

**Title: How to SSH without a password**

**Date: August 20th, 2017**

**OS: Ubuntu 16.10**

**Setup:**

To start you will need to machines that are connected to one another either through a switch or on the same network. Now this can be applied to as many machines as you want but we will just focus on two for now. If you don’t know how to setup two virtual machines together then look at my document for setting up static IP addresses. If you don’t know how to setup a virtual machine then look at my document for setting up a virtual machine to your correct needs.

**Part 1:**

You will not have to be root for any of the following instructions. Do the following on both machines.

* Type: sudo apt-get install openssh-server
* Type: service ssh restart
* Type: mkdir ~/.ssh
  + You will already have this directory if you have used the ssh command to get into another machine before.
* Type: cd ~/.ssh
* Type: ssh-keygen -t rsa
  + Now there should be an id\_rsa and a id\_rsa.pub in this directory. The id\_rsa is your private key and the other one is the public key. The known\_host file is what keeps track of all the ssh connections that you made before.
* Type: scp -p id\_rsa.pub “username”@”enp0s8 ip address”:
  + Don’t forget the colon at the end.

**Part 2:**

Go onto each system and finish the process up.

* Type: cd ~
* Type: mv id\_rsa.pub ~/.ssh
  + If this doesn’t work then make sure that they have the ~/.ssh directory.
* Type: cp id\_rsa.pub authorized\_keys
  + The authorized\_keys file is used with ssh to look for the public keys from other machines.
* Type: rm id\_rsa.pub

**Other:**

Now when you go to ssh into the other machine it should not prompt you for a password. If you are getting stuck, then google is your friend and the -vvv option for ssh is going to help in some aspects. Another thing to keep an eye out for is the permissions on the files and directories.