Asymmetric Key SSH Workout

In this workout, you will configure one of the most common forms of secure administrative access to a server using Secure Shell or SSH. Because SSH allows remote administration, the connection provides a very high level of security. However, when administrators use passwords for authentication, the protocol is weakened. Likewise, administrators are encouraged to create public and private key pairs for authentication using asymmetric-key cryptography instead of password authentication.

Start and then enter your workout. Then from inside your workout, follow the instructions below and look for what to turn in.

Instructions

1. **Open PowerShell.** Open a Windows PowerShell command prompt on the Windows taskbar.
2. **Generate your Asymmetric Keys.** Run `ssh-keygen` on the command line, and accept all of the defaults (including the blank password). This will create your public and private key pairs. You can see them from your home directory under the directory *.ssh*. The public key will be called *id_rsa.pub*, and the private key will be called *id_rsa*.
3. **Copy the Public Key for Later.** From Windows PowerShell, run `more .ssh/id_rsa.pub`. You will copy this into the authorized key file later.
4. **Login to Linux Server.** From Windows PowerShell, login to your Debian Linux server with the following:
   ssh melon@10.1.1.20
   User: melon
   Password: 'Let's workout!' (no quotes)
5. **Add the Public Key for Linux**. *Keep in mind, you are now in a completely different server using Secure Shell (SSH)*. Run the following commands to create the authorized public key files for the user *melon*
   `sudo mkdir .ssh && touch .ssh/authorized_keys`
   Now, edit the authorized keys using the *vim* text editor. In the SSH command prompt, type `sudo vim .ssh/authorized_keys`. In vim, you'll type the letter 'i' (for insert). Then, paste the id_rsa.pub public key contents that you earlier copied into your clipboard. Once complete, type escape, and then ':wq' (command for write and then quit)
6. **Login through SSH using your private key.** If you are already in ssh, type *exit*. Then login using your private key by typing: `ssh -i id_rsa melon@10.1.1.20`

What to Turn In?

Turn in a copy of both your public and private key and a screenshot showing you logged in to the Linux server.