ECE455
Lab #0.5: Care and Feeding of Your VM

Name: _____

This is an introduction to your new personal Cyber Security VM.

```
$ man ssh

SSH(1)                    BSD General Commands Manual                    SSH(1)

NAME
     ssh – OpenSSH SSH client (remote login program)
```

Overview

Goals

- Log into your VM
- Change password
- Generate and exchange SSH keys for password-less logins

Grading & Submission

- Authentication check (I will make sure you have secured your VM)
- Submit a copy of your SSH public key to me via email

Things to think about

- SSH keys what do these represent?
- What does the -t ed25519 option actually do? Why use this?
- Checkout sshd_config. What can you do with this? Can you make SSH safer or more dangerous?
- Checkout /var/log/auth.log on your VM. What do you see here? What if you grep for “sshd”?

Cyber Security VMs

For your convenience we have configured a few VMs in the ee.cooper.edu subdomain. Reach out via email to obtain access.

You may log into these with:

```
Username:cooperhat
Password:changeme
```

Change your password

After logging in please change the password and create your own username:

```
$ passwd
Changing password for user cooperhat

$ adduser gitzel
Adding user `gitzel' ...
Adding new group `gitzel' (1001) ...
Adding new user `gitzel' (1001) with group `gitzel' ...
Creating home directory `/home/gitzel' ...
Copying files from `/etc/skel' ...
```

Exchange SSH keys

Exchanging SSH keys will allow for password-less logins.

First generate your keys:

```
$ ssh-keygen -t ed25519

Generating public/private ed25519 key pair.
```

```
Enter file in which to save the key (/afs/ee.cooper.edu/user/g/gitzel/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /afs/ee.cooper.edu/user/g/gitzel/.ssh/id_ed25519.
Your public key has been saved in /afs/ee.cooper.edu/user/g/gitzel/.ssh/id_ed25519.pub.
```

This will place your public and private key pairs in the location you specified protected by an optional password.

Then copy your **public key** to the remote server:

```
$ ssh-copy-id -i .ssh/id_ed25519.pub [USER]@[VM_ADDR]
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
gitzel@199.98.27.210's password:
bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)

Number of key(s) added: 1
```

You should now be able to SSH into the server without a password.

To further harden your VM, remove the password login option. **Warning!** You will only be able to SSH into the VM from a host that has a copy of you SSH keys.

```
$ su cooperhat
...
$ sudo vim /etc/ssh/sshd_config
...
[Within VIM or some text editor]
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```