Name: Planta, Calvin Earl L.	**Date Performed: Aug 15, 2025**
Course/Section: CPE 212 - CPE31S2	**Date Submitted: Aug 15, 2025**
Instructor: Engr. Robin Valenzuela	**Semester and SY: 1st Sem S.Y 2025-2026**

Activity 2: SSH Key-Based Authentication and Setting up Git

1. **Objectives:**

1.1 Configure remote and local machine to connect via SSH using a KEY instead of using a password
1.2 Create a public key and private key
1.3 Verify connectivity
1.4 Setup Git Repository using local and remote repositories
1.5 Configure and Run ad hoc commands from local machine to remote servers

Part 1: Discussion

It is assumed that you are already done with the last Activity (**Activity 1: Configure Network using Virtual Machines).** *Provide screenshots for each task*.

It is also assumed that you have VMs running that you can SSH but require a password. Our goal is to remotely login through SSH using a key without using a password. In this activity, we create a public and a private key. The private key resides in the local machine while the public key will be pushed to remote machines. Thus, instead of using a password, the local machine can connect automatically using SSH through an authorized key.

What Is ssh-keygen?

Ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

SSH Keys and Public Key Authentication

The SSH protocol uses public key cryptography for authenticating hosts and users. The authentication keys, called SSH keys, are created using the keygen program.

SSH introduced public key authentication as a more secure alternative to the older .rhosts authentication. It improved security by avoiding the need to have passwords stored in files and eliminated the possibility of a compromised server stealing the user's password.

However, SSH keys are authentication credentials just like passwords. Thus, they must be managed somewhat analogously to usernames and passwords. They should have a proper termination process so that keys are removed when no longer needed.

Task 1: Create an SSH Key Pair for User Authentication

1. The simplest way to generate a key pair is to run *ssh-keygen* without arguments. In this case, it will prompt for the file in which to store keys. First, the tool asked where to save the file. SSH keys for user authentication are usually stored in the users .ssh directory under the home directory. However, in enterprise environments, the location is often different. The default key file name depends on the algorithm, in this case *id_rsa* when using the default RSA algorithm. It could also be, for example, *id_dsa* or *id_ecdsa*.

```
vbearl@workstation:~$ ssh-keygen -t rsa -b 4096
```

2. Issue the command *ssh-keygen -t rsa -b 4096.* The algorithm is selected using the -t option and key size using the -b option.

```
vbearl@workstation:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vbearl/.ssh/id_rsa):
```

3. When asked for a passphrase, just press enter. The passphrase is used for encrypting the key, so that it cannot be used even if someone obtains the private key file. The passphrase should be cryptographically strong.

```
vbearl@workstation:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vbearl/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/vbearl/.ssh/id_rsa
Your public key has been saved in /home/vbearl/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:wKqpoCdntp1OckQuRQmcszz3qC2eXgHSar1YjnJuXg0 vbearl@workstation
The key's randomart image is:
+---[RSA 4096]----+
| ..o..           |
| .+...           |
|..ooo o          |
| o==.. .         |
|...=Eo  S        |
|. ==o+.          |
|oo=== .          |
|=+OO..           |
|o@B++            |
+----[SHA256]-----+
```

4. Verify that you have created the key by issuing the command *ls -la .ssh.* The command should show the .ssh directory containing a pair of keys. For example, id_rsa.pub and id_rsa.

```
vbearl@workstation:~$ ls -la .ssh
total 24
drwx------  2 vbearl vbearl 4096 Aug 15 09:35 .
drwxr-x--- 15 vbearl vbearl 4096 Aug  8 08:54 ..
-rw-------  1 vbearl vbearl    0 Aug  1 09:38 authorized_keys
-rw-------  1 vbearl vbearl 3381 Aug 15 09:35 id_rsa
-rw-r--r--  1 vbearl vbearl  744 Aug 15 09:35 id_rsa.pub
-rw-------  1 vbearl vbearl 1404 Aug  8 10:23 known_hosts
-rw-r--r--  1 vbearl vbearl  142 Aug  8 10:15 known_hosts.old
```

Task 2: Copying the Public Key to the remote servers

1. To use public key authentication, the public key must be copied to a server and installed in an *authorized_keys* file. This can be conveniently done using the *ssh-copy-id* tool.

```
vbearl@workstation:~$ ssh-copy-id -i ~/.ssh/id_rsa vbearl@192.168.56.106
```

2. Issue the command similar to this: *ssh-copy-id -i ~/.ssh/id_rsa user@host*

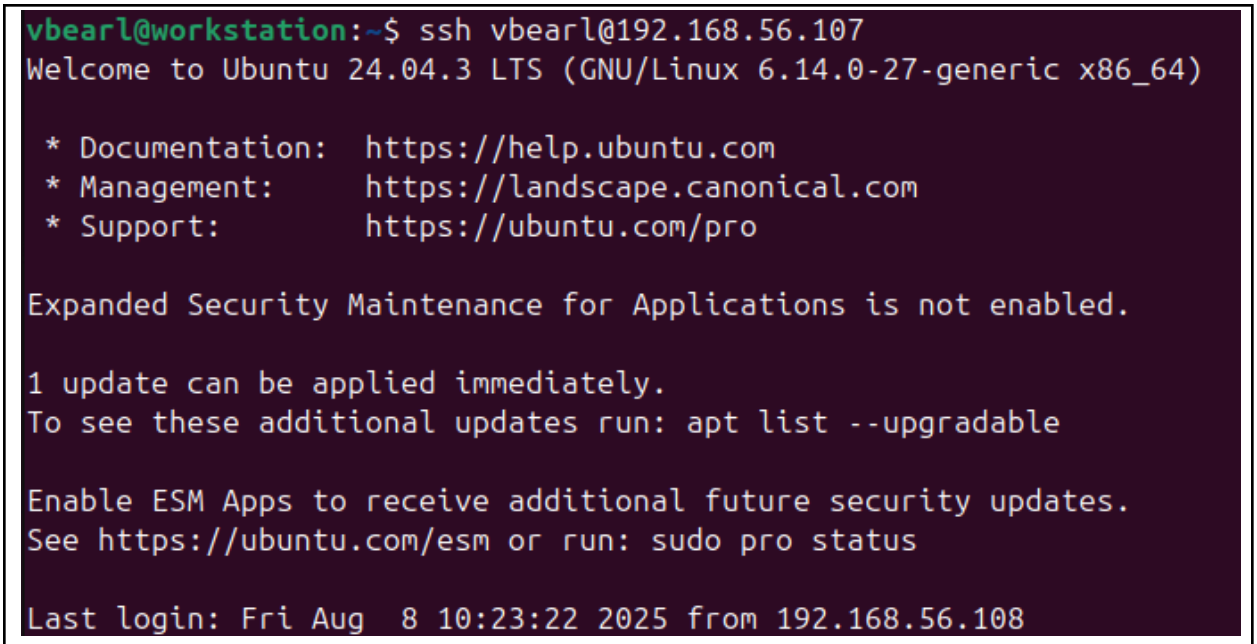
```
vbearl@workstation:~$ ssh-copy-id -i ~/.ssh/id_rsa vbearl@192.168.56.106
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/vbearl/.ssh
/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
vbearl@192.168.56.106's password:
Permission denied, please try again.
vbearl@192.168.56.106's password:
Permission denied, please try again.
vbearl@192.168.56.106's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'vbearl@192.168.56.106'"
and check to make sure that only the key(s) you wanted were added.
```

```
vbearl@workstation:~$ ssh-copy-id -i ~/.ssh/id_rsa vbearl@192.168.56.107
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/vbearl/.ssh
/id_rsa.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 prompt
ed now it is to install the new keys
vbearl@192.168.56.107's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'vbearl@192.168.56.107'"
and check to make sure that only the key(s) you wanted were added.
```

3. Once the public key has been configured on the server, the server will allow any connecting user that has the private key to log in. During the login process, the client proves possession of the private key by digitally signing the key exchange.

4. On the local machine, verify that you can SSH with Server 1 and Server 2. What did you notice? Did the connection ask for a password? If not, why?

```
vbearl@workstation:~$ ssh vbearl@192.168.56.106
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Aug  8 10:23:50 2025 from 192.168.56.108
```



The connection no longer asked for the password before connecting to the servers via ssh. This is because I already paired them with public and private keys.

Reflections:

Answer the following:

1. How will you describe the ssh-program? What does it do?
   - SSH program is a client that provides high-level security to your workstations and servers. It even allows us to provide public and private keys, offering automated logins and encryption, as demonstrated in the previous part of this activity.
2. How do you know that you already installed the public key to the remote servers?
   - When connecting to the remote server via ssh, it prompts you to enter the server's password first. If the client instantly connects you to the remote servers without asking for the password, it means that the public keys are already installed to the servers.

Part 2: Discussion

Provide screenshots for each task.

It is assumed that you are done with the last activity (**Activity 2: SSH Key-Based Authentication**).

Set up Git

At the heart of GitHub is an open-source version control system (VCS) called Git. Git is responsible for everything GitHub-related that happens locally on your computer. To use Git on the command line, you'll need to download, install, and configure Git on

your computer. You can also install GitHub CLI to use GitHub from the command line. If you don't need to work with files locally, GitHub lets you complete many Git-related actions directly in the browser, including:

- Creating a repository
- Forking a repository
- Managing files
- Being social

Task 3: Set up the Git Repository

1. On the local machine, verify the version of your git using the command *which git*. If a directory of git is displayed, then you don't need to install git. Otherwise, to install git, use the following command: *sudo apt install git*

```
vbearl@workstation:~$ sudo apt install git
[sudo] password for vbearl:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requir
  libgl1-amber-dri libglapi-mesa libllvm17t64 python3-netifaces
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb
  git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 4,806 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ph.archive.ubuntu.com/ubuntu noble/main amd64 liberror-perl all
7029-2 [25.6 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man a
:2.43.0-1ubuntu7.3 [1,100 kB]
```

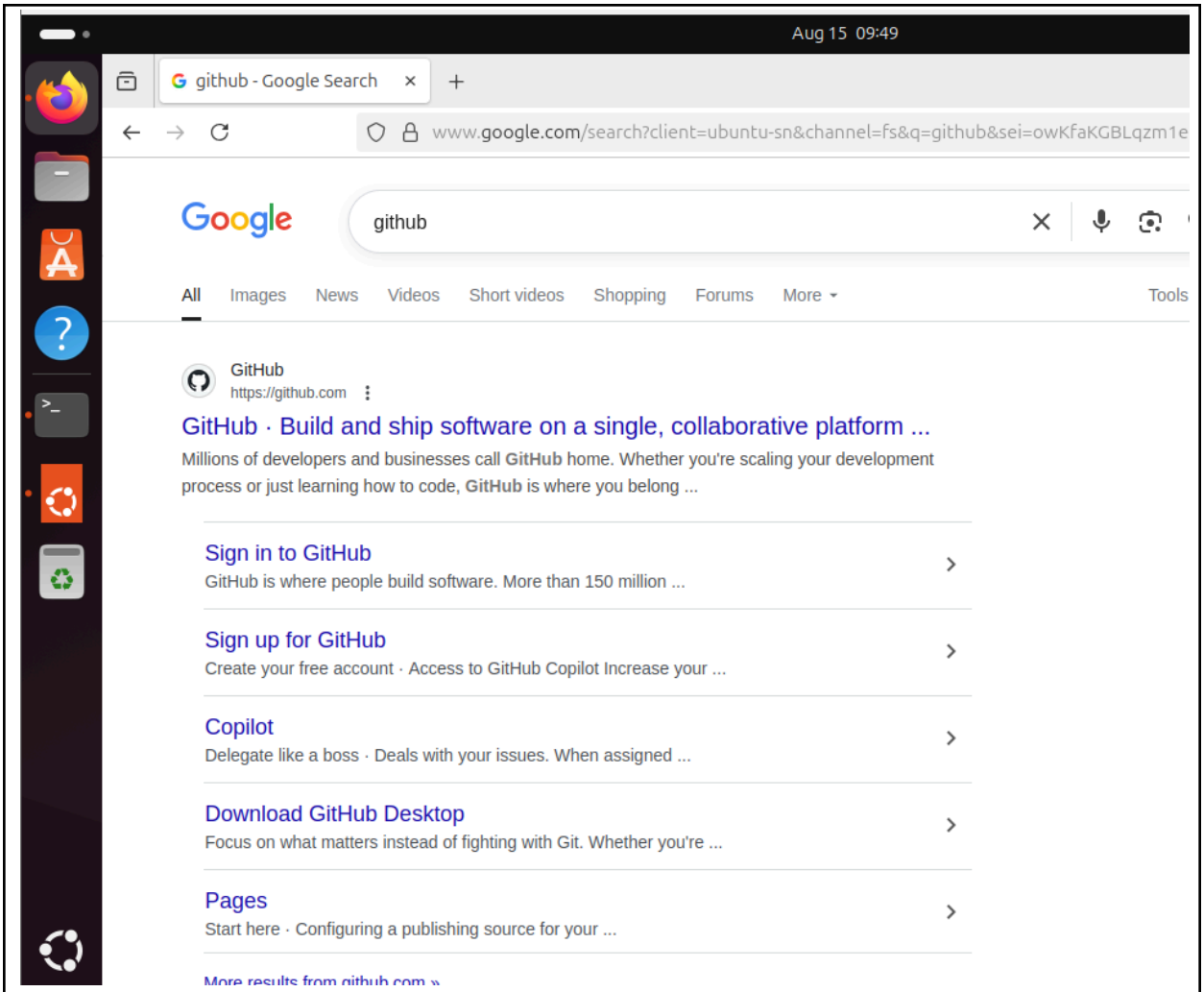
2. After the installation, issue the command *which git* again. The directory of git is usually installed in this location: *user/bin/git*.

```
vbearl@workstation:~$ which git
/usr/bin/git
```

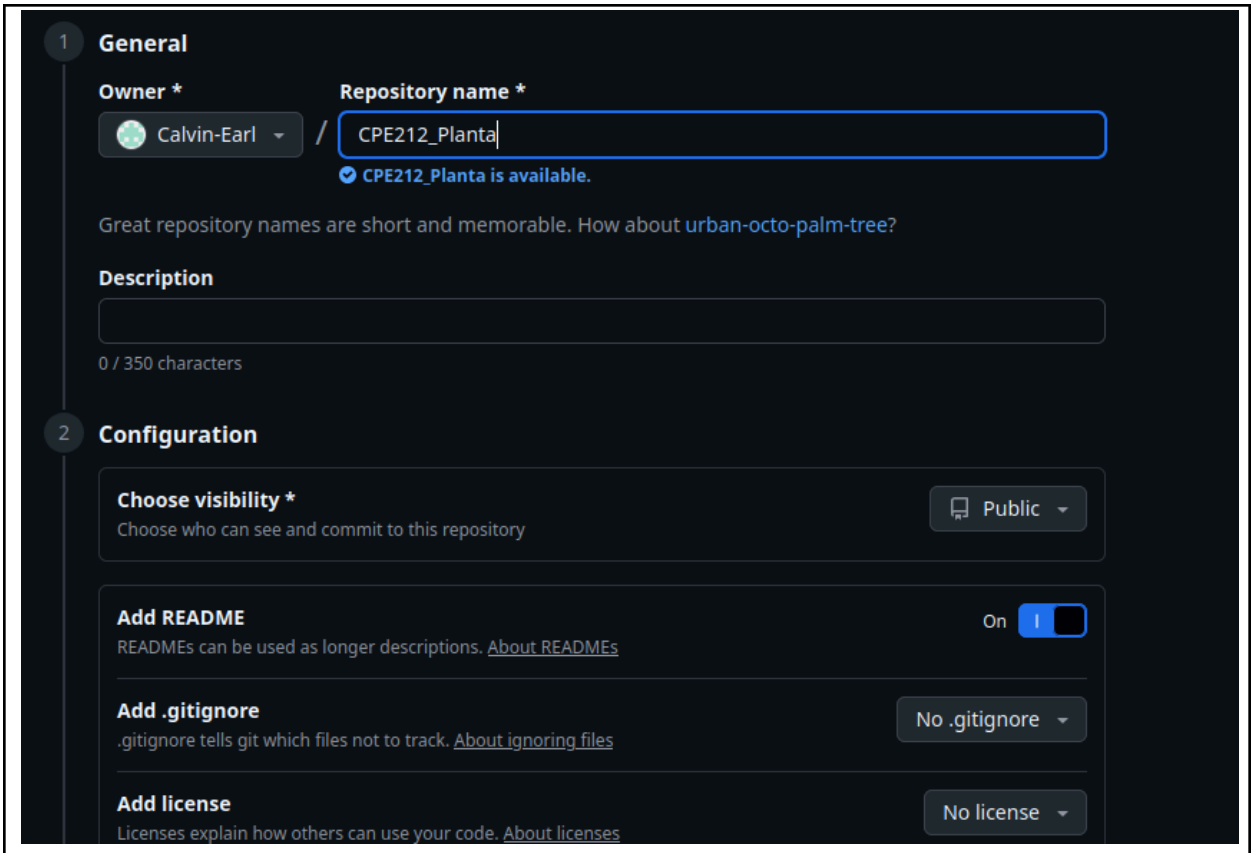
3. The version of git installed in your device is the latest. Try issuing the command *git --version* to know the version installed.

```
vbearl@workstation:~$ git --version
git version 2.43.0
```

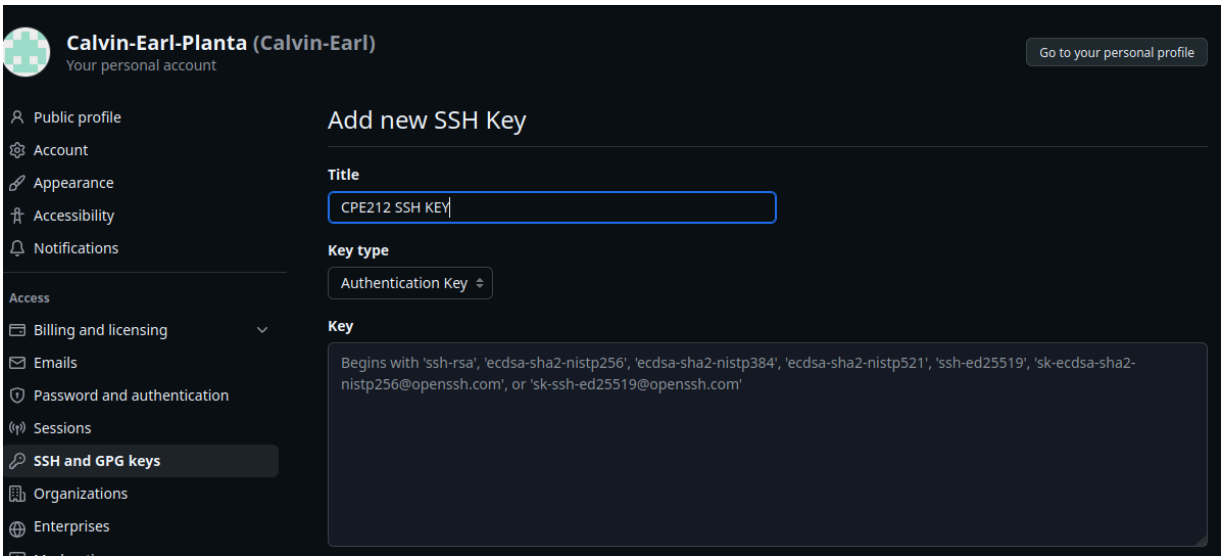
4. Using the browser in the local machine, go to www.github.com.



5. Sign up in case you don't have an account yet. Otherwise, login to your GitHub account.
    a. Create a new repository and name it as CPE232_yourname. Check Add a README file and click Create repository.



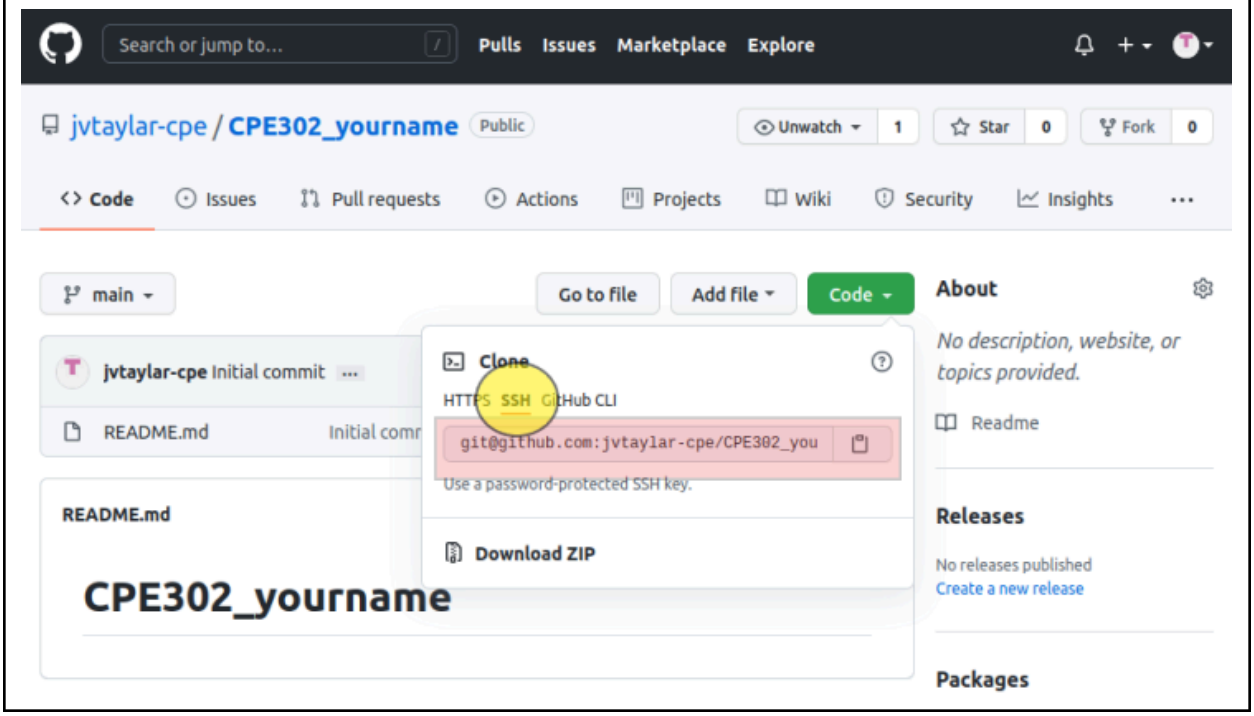
b. Create a new SSH key on GitHub. Go to your profile's settings and click SSH and GPG keys. If there is an existing key, make sure to delete it. To create new SSH keys, click New SSH Key. Write CPE232 key as the title of the key.

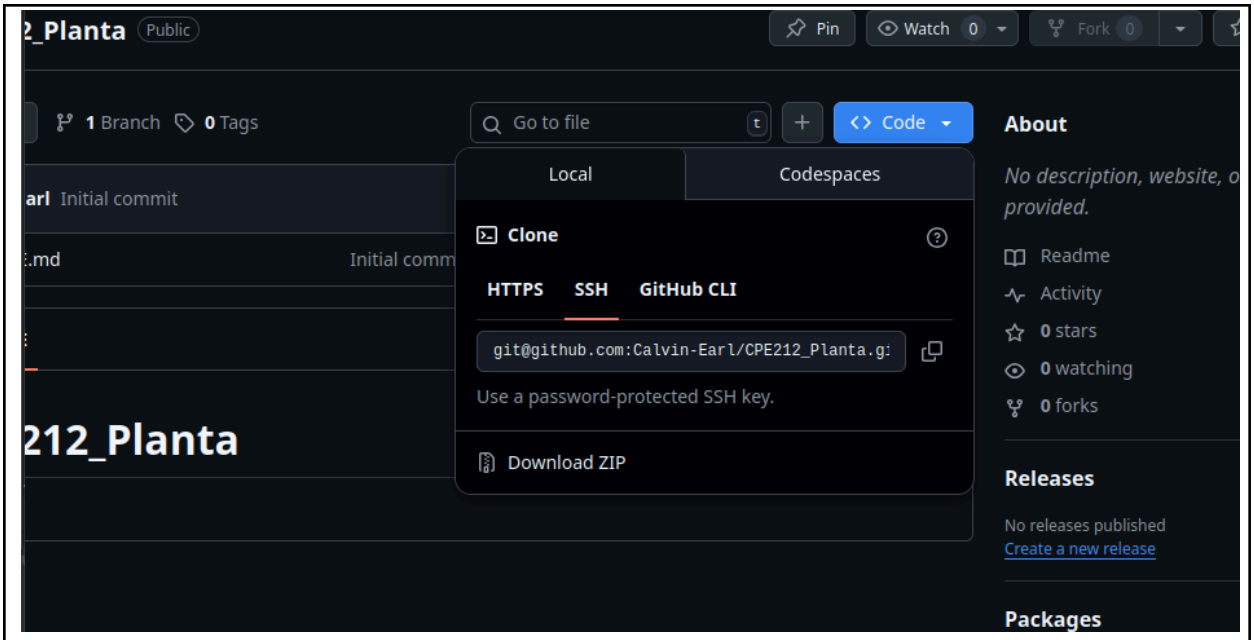


c. On the local machine's terminal, issue the command cat .ssh/id_rsa.pub and copy the public key. Paste it on the GitHub key and press Add SSH key.

```
vbearl@workstation:~$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDaSjbemdzXOgUYFSl/88d+V807lg4atNyBL3ajPSgZ
awtsrgAjP3cuKXkwgUr4/ETK8RYQSL7JYUkxhouRPU+OePLbZ/dm72Vu4p1ihM/Xo6pPLaFCBN6dY/J8
+DU+5921OOsVoPw9fO1ekuXwaIDEfVvib1JZ2hyUxfOny1vKweegIZovwKEzmyYqYAldq25q7RydriBt
1KBxKluuevJiXhtLTRRla5YaFHOCAFlTVz5japblBWH7iQH+fBldCQ4MPx/v4G59ZydVlVjrENhRXxHs
89kmpUlw+RXTZUFMpigH/kaMIeHKldwOH0kUp5lUW7yL69Pay8bXP56janovwI8BYWSBMzLqfn0jwn5Z
/1gJlO0DFMOCpklqySt2g6YHvaZ9yqC508laDNUCOJ4y5qLgMUfC9bno/nJPpw6qGStFcNb1RerM1INZ
ZyO/XWBSuQpBpBPsYW2i5L41a3krv4fNJlCBP9T5zDguOIGHeq+sDFm8vuXue+T4Ij/dGyl6q2VWHyVX
83AAXRw4oM50cUXeSRDc1YOdpVpyoCh3fJ9f4IHggKWNBD+aT5BnMGl+/F5B1yJiDSY7dUyP0Rx+ju5p
ccSeIhPZVC3R3A3g81F1BLRiUFf8HWI2ntq+0W3szIXWD6TxzmM/bsi0uaIcJaGHpa8b+v1O/ubmC2si
EQ== vbearl@workstation
```

d. Clone the repository that you created. In doing this, you need to get the link from GitHub. Browse to your repository as shown below. Click on the Code drop down menu. Select SSH and copy the link.





e. Issue the command git clone followed by the copied link. For example, *git clone git@github.com:jvtaylar-cpe/CPE232_yourname.git*. When prompted to continue connecting, type yes and press enter.

```
vbearl@workstation:~$ git clone git@github.com:Calvin-Earl/CPE212_Planta.git
Cloning into 'CPE212_Planta'...
The authenticity of host 'github.com (4.237.22.38)' can't be established.
ED25519 key fingerprint is SHA256:+DiY3wvvV6TuJJhbpZisF/zLDA0zPMSvHdkr4UvCOqU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'github.com' (ED25519) to the list of known hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (3/3), done.
```

f. To verify that you have cloned the GitHub repository, issue the command *ls*. Observe that you have the CPE232_yourname in the list of your directories. Use CD command to go to that directory and LS command to see the file README.md.

```
vbearl@workstation:~$ ls
CPE212_Planta  Documents  Music     Public  Templates
Desktop        Downloads  Pictures  snap    Videos
```

```
vbearl@workstation:~$ cd CPE212_Planta
vbearl@workstation:~/CPE212_Planta$ ls
README.md
```

g. Use the following commands to personalize your git.

- *git config --global user.name "Your Name"*

- *git config --global user.email yourname@email.com*
- Verify that you have personalized the config file using the command *cat ~/.gitconfig*

```
vbearl@workstation:~$ git config --global user.name "Bearl"
vbearl@workstation:~$ git config --global user email qcelplanta@tip.edu.ph
error: key does not contain a section: user
vbearl@workstation:~$ git config --global user.email qcelplanta@tip.edu.ph
vbearl@workstation:~$ cat ~/.gitconfig
[user]
        name = Bearl
        email = qcelplanta@tip.edu.ph
```

h. Edit the README.md file using nano command. Provide any information on the markdown file pertaining to the repository you created. Make sure to write out or save the file and exit.

i. Use the *git status* command to display the state of the working directory and the staging area. This command shows which changes have been staged, which haven't, and which files aren't being tracked by Git. Status output does not show any information regarding the committed project history. What is the result of issuing this command?

```
vbearl@workstation:~/CPE212_Planta$ nano README.md
vbearl@workstation:~/CPE212_Planta$ git status
On branch main
Your branch is up to date with 'origin/main'.

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   README.md

no changes added to commit (use "git add" and/or "git commit -a")
vbearl@workstation:~/CPE212_Planta$
```

The command showed changes not stage for the commit and what files have been modified..

j. Use the command *git add README.md* to add the file into the staging area.

```
vbearl@workstation:~/CPE212_Planta$ git add README.md
```

k. Use the *git commit -m "your message"* to create a snapshot of the staged changes along the timeline of the Git projects history. The use of this command is required to select the changes that will be staged for the next commit.

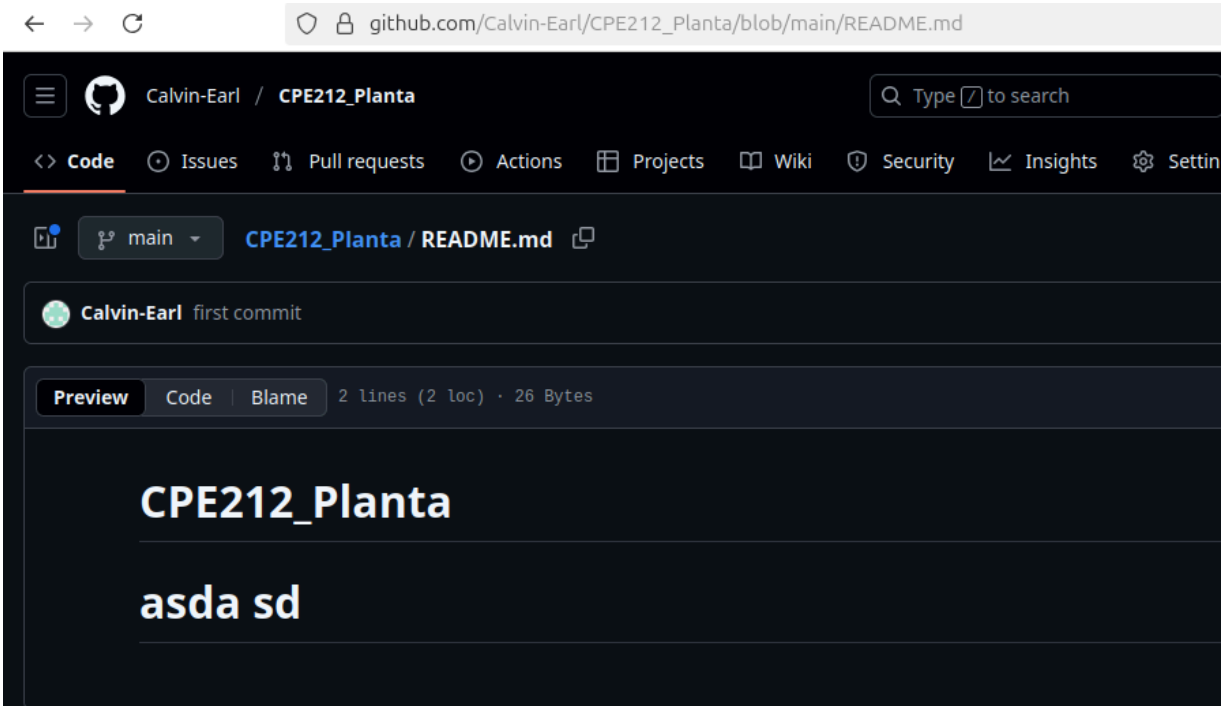
```
vbearl@workstation:~/CPE212_Planta$ git commit -m "first commit"
[main 031cb41] first commit
 1 file changed, 1 insertion(+), 1 deletion(-)
```

l. Use the command *git push <remote><branch>* to upload the local repository content to GitHub repository. Pushing means to transfer commits from the local repository to the remote repository. As an example, you may issue *git push origin main.*

```
vbearl@workstation:~/CPE212_Planta$ git push origin main
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Writing objects: 100% (3/3), 264 bytes | 264.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:Calvin-Earl/CPE212_Planta.git
   ea249dc..c844df1  main -> main
```

m. On the GitHub repository, verify that the changes have been made to README.md by refreshing the page. Describe the README.md file. You can notice how long was the last commit. It should be some minutes ago and the message you typed on the git commit command

should be there. Also, the README.md file should have been edited according to the text you wrote.



Conclusions/Learnings:

This lab activity taught me how to apply key pairs into my local machine and the remote servers. I first generated the encryption key in my local machine, then copied the ID to my servers, ensuring secured logins and encrypted passwords for my logins. Additionally, I learned how to set up my github for backup and automation purposes in the future. Overall, this taught me how to apply SSH security to my servers as I take another step in setting up and managing my servers.