

<b>Name: Cruz, Daniel Y.</b>	<b>Date Performed: 08/26/2023</b>
<b>Course/Section: CPE 232-CPE31S4</b>	<b>Date Submitted: 08/26/2023</b>
<b>Instructor: Dr. Jonathan Taylor</b>	<b>Semester and SY: 1<sup>st</sup> Semester</b>
<b>Activity 2: SSH Key-Based Authentication and Setting up Git</b>	
<b>1. Objectives:</b> <ul style="list-style-type: none"> <li>1.1 Configure remote and local machine to connect via SSH using a KEY instead of using a password</li> <li>1.2 Create a public key and private key</li> <li>1.3 Verify connectivity</li> <li>1.4 Setup Git Repository using local and remote repositories</li> <li>1.5 Configure and Run ad hoc commands from local machine to remote servers</li> </ul>	
<b>Part 1: Discussion</b> <p>It is assumed that you are already done with the last Activity (<b>Activity 1: Configure Network using Virtual Machines</b>). <i>Provide screenshots for each task.</i></p> <p>It is also assumed that you have VMs running that you can SSH but requires 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.</p> <p><b>What Is ssh-keygen?</b></p> <p>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.</p> <p><b>SSH Keys and Public Key Authentication</b></p> <p>The SSH protocol uses public key cryptography for authenticating hosts and users. The authentication keys, called SSH keys, are created using the keygen program.</p> <p>SSH introduced public key authentication as a more secure alternative to the older .rhosts authentication. It improved security by avoiding the need to have password stored in files and eliminated the possibility of a compromised server stealing the user's password.</p> <p>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.</p>	
<b>Task 1: Create an SSH Key Pair for User Authentication</b> <ul style="list-style-type: none"> <li>1. The simplest way to generate a key pair is to run <i>ssh-keygen</i> 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</li> </ul>	

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*.

```
cruz@cruz-Desktop:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cruz/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:PbVRtYxgACcDASXvhz+V1vLRxoe5oY/vzKbNe71g5k cruz@cruz-Desktop
The key's randomart image is:
+---[RSA 2048]---+
|oo.....+.o.o ...|
| . o.  + . ..o .|
|  o      o. o |
|  o      . . o |
| o o  S o .   |
|  +      * .   |
|   .   . O *o+.|
|   .   . o @+Eo..|
|   .   o+O=. o |
+-----[SHA256]-----+
```

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.
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.

```
cruz@cruz-Desktop:~$ ssh-keygen -t rsa -b 4096
Generating public/private key pair.
Enter file in which to save the key (/home/cruz/.ssh/id_rsa): id_rsa
id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:M9BaQ7kJgsciRFnXYSrUwUqkjq7neYTyFr7NWTWFGyU cruz@cruz-Desktop
The key's randomart image is:
+---[RSA 4096]---+
| .+0000E .      |
| =..000 +       |
| +..... = .     |
|+ ..  + =       |
|.o . . . S      |
|+00 .  + +      |
|+=+0. +         |
|00==.+ o        |
|.++0+ o         |
+-----[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*.

```
cruz@cruz-Desktop:~$ ls -la .ssh
total 12
drwx----- 2 cruz cruz 4096 Aug 15 17:50 .
-rw-r--r-- 1 cruz cruz 222 Aug 15 17:50 known_hosts
```

### 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.

```
cruz@cruz-Desktop:~$ ssh-copy-id
Usage: /usr/bin/ssh-copy-id [-h|-?|-f|-n] [-i [identity_file]] [-p port] [[-o <ssh -o op
tions>] ...] [user@]hostname
-f: force mode -- copy keys without trying to check if they are already installed
-n: dry run -- no keys are actually copied
-h|-?: print this help
```

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

### Reflections:

Answer the following:

1. How will you describe the ssh-program? What does it do?
2. How do you know that you already installed the public key to the remote 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*

```
cruz@cruz-Desktop:~$ sudo apt install git
[sudo] password for cruz:
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.17.1-1ubuntu0.18).
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
cruz@cruz-Desktop:~$
```

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

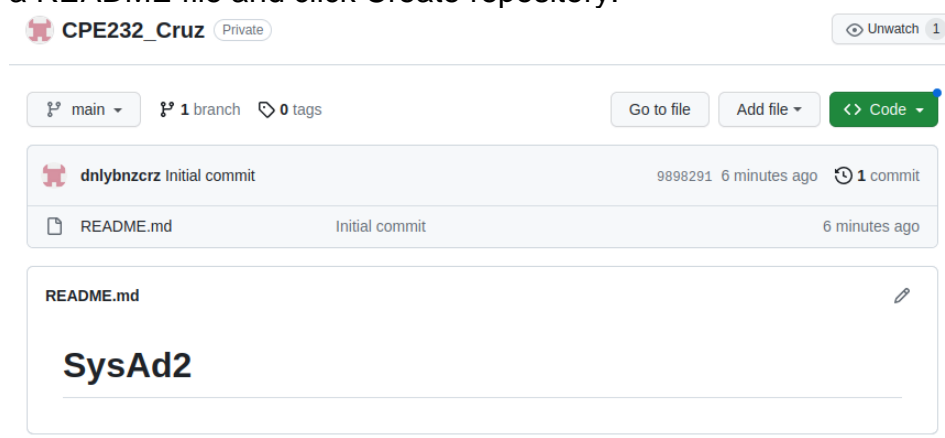
```
cruz@cruz-Desktop:~$ which git
/usr/bin/git
cruz@cruz-Desktop:~$
```

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

```
cruz@cruz-Desktop:~$ git -version
unknown option: -version
usage: git [--version] [--help] [-C <path>] [-c <name>=<value>]
      [--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
      [-p | --paginate | --no-pager] [--no-replace-objects] [--bare]
      [--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
      <command> [<args>]
```

4. Using the browser in the local machine, go to [www.github.com](https://www.github.com).
5. Sign up in case you don't have an account yet. Otherwise, login to your GitHub account.

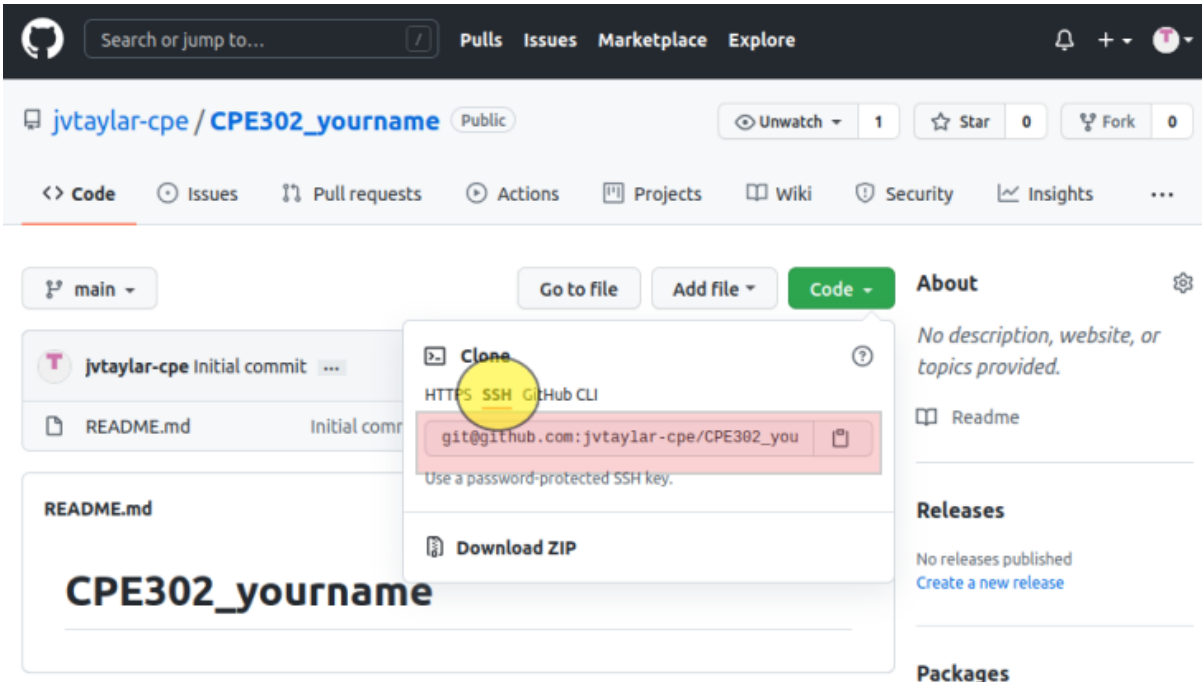
- a. Create a new repository and name it as CPE232\_yourname. Check Add a README file and click Create repository.



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

You have successfully added the key 'CPE232'.

- 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.
- 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:jvtaylor-cpe/CPE232_yourname.git`. When prompted to continue connecting, type yes and press enter.

```
cruz@cruz-Desktop:~$ git clone https://github.com/dnlybnzcrz/CPE232
Cloning into 'CPE232_Cruz'...
Username for 'https://github.com': dnlybnzcrz
Password for 'https://dnlybnzcrz@github.com':
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking 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`.

```
cruz@cruz-Desktop:~$ ls
CPE232_Cruz  Documents  examples.desktop  Pictures  Public  Vid
Desktop      Downloads  Music             project  Templates
cruz@cruz-Desktop:~$ cd CPE232_Cruz
```

- 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`

```
cruz@cruz-Desktop:~/CPE232_Cruz$ git config --global user.name "dnlybnzcrz"
cruz@cruz-Desktop:~/CPE232_Cruz$ git config --global user.email qdycruz@tip.edu.ph
cruz@cruz-Desktop:~/CPE232_Cruz$ cat ~/.gitconfig
[user]
  name = dnlybnzcrz
  email = qdycruz@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.

```
GNU nano 2.9.3 README.md Modified
# SysAd2
#Example lang po ito
```

- 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?

```
cruz@cruz-Desktop:~/CPE232_Cruz$ 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 checkout -- <file>..." to discard changes in working directory)

        modified:   README.md

no changes added to commit (use "git add" and/or "git commit -a")
```

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

```
cruz@cruz-Desktop:~/CPE232_Cruz$ 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.

```
cruz@cruz-Desktop:~/CPE232_Cruz$ git commit -m "first file in github"
[main a8a1e88] first file in github
1 file changed, 3 insertions(+), 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*.

```
cruz@cruz-Desktop:~/CPE232_Cruz$ git status
On branch main
Your branch is ahead of 'origin/main' by 1 commit.
  (use "git push" to publish your local commits)

nothing to commit, working tree clean
cruz@cruz-Desktop:~/CPE232_Cruz$ git push origin
Username for 'https://github.com': dnlybnzcrz
Password for 'https://dnlybnzcrz@github.com':
Counting objects: 3, done.
Writing objects: 100% (3/3), 280 bytes | 280.00 KiB/s, done
Total 3 (delta 0), reused 0 (delta 0)
To https://github.com/dnlybnzcrz/CPE232_Cruz.git
   9898291..a8a1e88  main -> main
cruz@cruz-Desktop:~/CPE232_Cruz$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
```

- 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 the 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.

 dnlybnzcrz first python file		4d5091c now 3 commits
 README.md	first file in github	5 minutes ago
 main.py	first python file	now

### Reflections:

Answer the following:

3. What sort of things have we so far done to the remote servers using ansible commands?

It provides security for communication and doesn't require agents on remote servers, reducing attack vendors and simplifying security management.

4. How important is the inventory file?

It provides a detailed record of the inventory in ubuntu. This file helps define the scope of operations and facilitates efficient management of files.

**Conclusions/Learnings:**

**When setting up Git, we can associate our SSH public key with the Git provider account, allowing us to securely push and pull code without constantly entering credentials.**