**CYB101 Project 2 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb101/unit/2#!projects)**)**

👤 Student Name: Sila Tamang

✉️ Student Email: stamang3@uco.edu

**Reflection (Required)**

| **🤔 Reflection Question #1:** If I had to **explain “what is SSH?” in 3 emojis,** they would be…  (Feel free to put other comments about your experience this unit here, too!) |
| --- |
| 🧐😇😉 |

| **🐧Reflection Question #2:** Why would we want to use Kali linux and not just Windows or Mac? |
| --- |
| Kali Linux is an open-source operating system which comes pre-installed with various security tools and software packages that are not available on Windows or Mac operating systems. Some other reasons are it is a secure operating system that can help to identify vulnerabilities and security threats in the system. It is also highly customizable and an excellent tool for learning about security and ethical hacking. |

| **📣 Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better! |
| --- |
| The CodePath Team instructor and mentor, especially the mentor from pod-52 |

**Required Challenge Screenshots (Required)**

Use the answer boxes below to paste in your screenshots from completing the project. Clarifying notes are optional.

(You don’t need any screenshots for **Part 1** or **Part 2.**)

#### **Part 3: SSH Encryption and Decryption**

| **Screenshot #1:** The appropriate encryption command and its’ output |
| --- |
|  |
| **Notes** (Optional)**: I first created the ssh keys and used the public key to encrypt the secret message and private key to decrypt the message.** |

#### 

| **Screenshot #2:** The appropriate decryption command |
| --- |
|  |
| **Notes** (Optional)**: I first created the ssh keys and used the public key to encrypt the secret message and private key to decrypt the message.** |

#### 

#### 

| **Screenshot #3:** The contents of all 3 files: original, encrypted, decrypted |
| --- |
|  |
| **Notes** (Optional)**: Printed out the contents of the files** |

#### 

#### **Part 4: SSH Git Commit Signing**

| **Screenshot #4:** The git commit command and its’ output |
| --- |
|  |
| **Notes** (Optional)**: Committed to the git with the signing key** |

#### 

| **Screenshot #5:** The git show --show-signature command and its’ output, showing a successful signature |
| --- |
|  |
| **Notes** (Optional)**: Got the committed contents with signature** |

**Stretch Challenge (Optional)**

| **Stretch Challenge #1:** A screenshot showing an additional use of SSH keys |
| --- |
|  |
| **Notes** (Optional)**: SSH public key authentication is a secure and convenient way to authenticate remote users and enable secure file transfers using SCP (Secure Copy). Using the same public key in both remote and local, I did a secure copy (scp) of a filename pikachu.txt from local to remote. Here's the steps to showcase the use of SSH public key authentication to do SCP:**   * **Generate an SSH key pair: On your local computer, generate a public/private key pair using the ssh-keygen command. This will create two files: a private key (id\_rsa) and a public key (id\_rsa.pub).** * **Copy the public key to the remote server: Copy the public key to the remote server using the ssh-copy-id command or by manually adding the public key to the authorized\_keys file on the remote server.** * **Connect to the remote server using SCP: Once the public key is installed on the remote server, you can use SCP to securely transfer files between your local computer and the remote server without having to enter a password.** |

#### 

| **Stretch Challenge #1:** A description of an additional use of SSH keys |
| --- |
| * **SSH keys can be used in automated processes, such as scripts and cron jobs, to automate system management tasks. Here's an example of how SSH keys can be used for automation:**   + **Let's say you have a script that needs to access a remote server to perform a task, such as backing up files or running a command. Instead of hardcoding the password in the script, which can be a security risk, you can use SSH keys for authentication.**   + **First, generate an SSH key pair on the system where the script will be run. This will create a public key and a private key. The private key should be kept secure and not shared with anyone, while the public key can be added to the authorized\_keys file on the remote server.**   + **Then, configure the script to use the private key for authentication when connecting to the remote server via SSH. This can be done using the ssh command with the -i option to specify the path to the private key.**   + **Now, when the script is run, it will automatically authenticate with the remote server using the SSH key pair, without the need for a password. This makes the script more secure and efficient, as it can be run without human intervention and without the risk of the password being compromised.**   + **Overall, using SSH keys for automation can help to streamline system management tasks and improve security by eliminating the need for passwords in automated processes.** |

#### 

**Submission Checklist**

**👉***Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

**Reflection**

* ~~Reflection Question #1 answered above~~
* ~~Reflection Question #2 answered above~~

**Required Challenge Screenshots**

* ~~Screenshot #1~~
* ~~Screenshot #2~~
* ~~Screenshot #3~~
* ~~Screenshot #4~~
* ~~Screenshot #5~~

**Stretch Challenge**

* ~~Challenge #1: Screenshot~~
* ~~Challenge #2: Description~~

**Submit your work!**

| Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)      Step 2: **Copy** the link to this document.    Step 3: **Submit** the link on the portal. |
| --- |

**Grader Comments**

| *Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.* **Grading Rubric**  | Reflection Questions | Total Received | Total Possible | | --- | --- | --- | | Reflection Question #1 answered above | 2 | 2 | | Reflection Question #2 answered above | 2 | 2 | | **PART A TOTAL** | 4 | **4** | | Required Challenge Screenshots | Total Received Points | Total Possible | | Screenshot #1 | 2 | 2 | | Screenshot #2 | 2 | 2 | | Screenshot #3 | 5 | 5 | | Screenshot #4 | 3 | 3 | | Screenshot #5 | 4 | 4 | | **PART B TOTAL** | **16** | **16** | | Stretch Challenge | Total Received Points | Total Possible | | Screenshot showing an additional use of SSH keys | 2 | +2 bonus | | Description of an additional use of SSH keys | 2 | +2 bonus | | **Total Possible Points (Part A + Part B)** | **4** | **20** (+4) | |  | **24** |  |   **Grader Feedback** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |