CYB101 Project 2

👤 Student Name: Weicong Xie

✉ Student Email: Weicong.wx@gmail.com

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 open sourced and is designed for cybersecurity.

📢**Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

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

```
codepath@idx-cyb101-idx-1741398687267:~$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted
codepath@idx-cyb101-idx-1741398687267:~$ ls
Documents  code  john  secret.txt  secret.txt.encrypted  setoolkit  startup.sh  unit2  unit3  unit6
codepath@idx-cyb101-idx-1741398687267:~$ cat secret.txt.encrypted
```

Notes (Optional):

Screenshot #2: The appropriate decryption command

```
codepath@idx-cyb101-idx-1741398687267:~$ openssl pkeyutl -decrypt -inkey  ~/.ssh/privatekey.pem -in secret.txt.encrypted  -out secret.txt.decrypted
codepath@idx-cyb101-idx-1741398687267:~$ ls
Documents  code  john  secret.txt  secret.txt.decrypted  secret.txt.encrypted  setoolkit  startup.sh  unit2  unit3  unit6
codepath@idx-cyb101-idx-1741398687267:~$ cat secret.txt.decrypted
My secret code is CHEESE
codepath@idx-cyb101-idx-1741398687267:~$
```

Notes (Optional):

Screenshot #3: The contents of all 3 files: original, encrypted, decrypted

```
codepath@idx-cyb101-idx-1741398687267:~$ cat secret.txt
My secret code is CHEESE
codepath@idx-cyb101-idx-1741398687267:~$ cat secret.txt.encrypted

My secret code is CHEESE
codepath@idx-cyb101-idx-1741398687267:~$
```

Notes (Optional):

Part 4: SSH Git Commit Signing

Screenshot #4: The `git commit` command and its' output

```
codepath@idx-cyb101-idx-1741398687267:~/DemoProject$ git commit --allow-empty --message="Did the SSH signing work?"
[master (root-commit) 9cef858] Did the SSH signing work?
```

Notes (Optional):

Screenshot #5: The `git show --show-signature` command and its' output, showing a successful signature

```
codepath@idx-cyb101-idx-1741398687267:~/DemoProject$ git show --show-signature
commit 9cef858c5d63ffecd62f071f663366c5bd6ddc68 (HEAD -> master)
Good "git" signature for * with RSA key SHA256:emf5IjvbneBKhFFOyeyMhdSJ3W/zsWoZH1NxmBS0/r0
Author: cyber <rebyc@gmail.com>
Date:   Sat Mar 8 03:13:36 2025 +0000

    Did the SSH signing work?
```

Notes (Optional)**:**

Stretch Challenge (Optional)

Stretch Challenge #1: A screenshot showing an additional use of SSH keys

[Insert Screenshot Here]

Notes (Optional)**:**

Stretch Challenge #1: A description of an additional use of SSH keys

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~~

- [x] ~~Screenshot #3~~
- [x] ~~Screenshot #4~~
- [x] ~~Screenshot #5~~

Stretch Challenge

- [ ] Challenge #1: Screenshot
- [ ] Challenge #2: Description