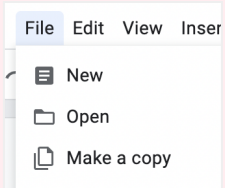
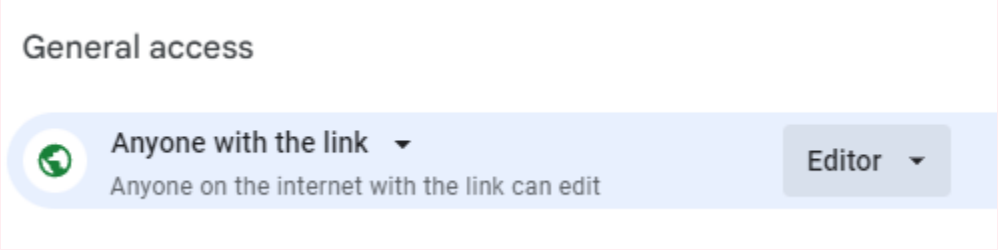
Instructions for Copying and Sharing this Document

📣 **DELETE THIS BOX BEFORE SUBMITTING!!**

Step 1: **Click** "File -> Make a Copy" to make a copy of this document that you can edit.



Step 2: **Change** the Share settings to "Anyone with Link -> Editor". This will allow our graders to leave comments on your submission.



CYB101 Project 2

(🔗 [Instructions Page])

👤 Student Name: Jonathan Siegel

✉️ Student Email: jsiegel0516@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 appears to be an environment/Operating system that is more meant for learning penetration testing, security research, getting familiar with terminal. It seem to be more flexible then windows and mac when it comes to the provided tools.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> Everyone in group 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
>
> **[Insert Screenshot Here]**

```
┌──(chomps443㉿kali)-[~]
└─$ openssl genrsa -out ~/.ssh/privatekey.pem 2048

┌──(chomps443㉿kali)-[~]
└─$ openssl rsa -in  ~/.ssh/privatekey.pem -out ~/.ssh/publickey.pem -pubout -outform PEM
writing RSA key

┌──(chomps443㉿kali)-[~]
└─$ ls ~/.ssh
authorized_keys  id_rsa  id_rsa.pub  privatekey.pem  publickey.pem

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE is apple" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE is apple

┌──(chomps443㉿kali)-[~]
└─$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt.encrypted
◆mQ◆◆◆◆%r□^◆/◆◆yh◆Q%fb◆9KM◌"p;◆□◆J◆◆◆◆W◆◆◆◆JE◆5◆g/zW◆◆□U%□Q◆◆□yH&□◆◆C◆–◆◆◆3◆ϟZq$RK◆Z◆◆◆N◆<◆q◆Y2◆◆J◆◆◆□⿻@
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
◆□◆t◆◆◆x[◆◆]S◆◆ᵣ:◆E□□O□◆"◆M◆◆◆◆1;od◆◆◆◆V□◆=◆◆Rmd6_◆C◆◆4◆
◆U◆◆◆◆žt◆◆z◆rP&◆
◆□◆|T◆C"◆□◆E
     ◆}F□◆◆□◆|"W◆◆□◆◆□□□T□$◆◆.0◆vR◆     ◌◆

┌──(chomps443㉿kali)-[~]
└─$ openssl pkeyutl -decrypt -inkey  ~/.ssh/privatekey.pem -in secret.txt.encrypted  -out secret.txt.decrypted

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt.decrypted
MY SECRET MESSAGE is apple
```

Notes (Optional)**:**

Screenshot #2: The appropriate decryption command

[Insert Screenshot Here]

```
┌──(chomps443㉿kali)-[~]
└─$ openssl genrsa -out ~/.ssh/privatekey.pem 2048

┌──(chomps443㉿kali)-[~]
└─$ openssl rsa -in  ~/.ssh/privatekey.pem -out ~/.ssh/publickey.pem -pubout -outform PEM
writing RSA key

┌──(chomps443㉿kali)-[~]
└─$ ls ~/.ssh
authorized_keys  id_rsa  id_rsa.pub  privatekey.pem  publickey.pem

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE is apple" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE is apple

┌──(chomps443㉿kali)-[~]
└─$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt.encrypted
◆mQ◆◆◆◆%r□^◆/◆◆yh◆Q%fb◆9KM◌"p;◆□◆J◆◆◆◆W◆◆◆◆JE◆5◆g/zW◆◆□U%□Q◆◆□yH&□◆◆C◆–◆◆◆3◆ϟZq$RK◆Z◆◆◆N◆<◆q◆Y2◆◆J◆◆◆□⍈@
                                                
```

```
┌──(chomps443㉿kali)-[~]
└─$ openssl genrsa -out ~/.ssh/privatekey.pem 2048

┌──(chomps443㉿kali)-[~]
└─$ openssl rsa -in  ~/.ssh/privatekey.pem -out ~/.ssh/publickey.pem -pubout -outform PEM
writing RSA key

┌──(chomps443㉿kali)-[~]
└─$ ls ~/.ssh
authorized_keys  id_rsa  id_rsa.pub  privatekey.pem  publickey.pem

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE

┌──(chomps443㉿kali)-[~]
└─$ echo "MY SECRET MESSAGE is apple" > secret.txt

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt
MY SECRET MESSAGE is apple

┌──(chomps443㉿kali)-[~]
└─$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt.encrypted
◆mQ◆◆◆◆%r□^◆/◆◆yh◆Q%fb◆9KM◌"p;◆□◆J◆◆◆◆W◆◆◆◆JE◆5◆g/zW◆◆□U%□Q◆◆□yH&□◆◆C◆–◆◆◆3◆ϟZq$RK◆Z◆◆◆N◆<◆q◆Y2◆◆J◆◆◆□⍨@
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
◆□◆t◆◆◆x[◆◆]S◆◆ᵣ:◆E□□O□◆"◆M◆◆◆◆1;od◆◆◆◆V□◆=◆◆Rmd6_◆C◆◆4◆
◆U◆◆◆◆žt◆◆z◆rP&◆
◆□◆|T◆C"◆□◆E
     ◆}F□◆◆□◆|"W◆◆□◆◆□□□T□$◆◆.0◆vR◆     ◌◆̂

┌──(chomps443㉿kali)-[~]
└─$ openssl pkeyutl -decrypt -inkey  ~/.ssh/privatekey.pem -in secret.txt.encrypted  -out secret.txt.decrypted

┌──(chomps443㉿kali)-[~]
└─$ cat secret.txt.decrypted
MY SECRET MESSAGE is apple
```

Notes (Optional)**: I just took a screenshot of what the instructions told me to take a screenshot of during the moment.**

Part 4: SSH Git Commit Signing

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

[Insert Screenshot Here]

```
┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global user.name "Jonathan Siegel"

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global commit.gpgsign true

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global gpg.format ssh

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ eval `ssh-agent -s`
Agent pid 56630

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ssh-add ~/.ssh/id_rsa
Identity added: /home/chomps443/.ssh/id_rsa (cyberstudent@kali.local)

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ssh-add -L
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC1GVR5KEOaUSDs3rKh2LZQHgg7BQ2rY+T7h5j+q4yHViq0cIkMNE7jRwO95J22uJWVRtr2XIxChs4dPZf9X4JyvMQjSi+jBvjw+F2X+wSCH5LU4gGJHfAaPk/HG7kktDfXdBTsiT3v7N1oBbLNFrAjEptBI0VMplYedcTX6Ewoob2efRH2iaoLGrpi1bo29MC7FB2
imW2emAEMf9G/qU8D+06XhhWuv/7v2i3FVpjm9cPM9In/YcSCdKvai0KizQxeCk/FqK2uCQttm62KqKzu5rDi6DWpcULzpS0JBBdEptl4DTOvmBHu9LEshhrU1GqoGwnp8y0x/9ryb75E6AVcWTr2/coIFBWW7I9AcnhVm///xCZ5Iv3oKtzgZJIrl49gLKQt0Eh5BmPQp/gpL5+kS64TqqJWrLGiGbfUQHUvBWouvakUr4q5FVxCzbeKHFVX6RyE5P6GcB97tB8EgzjEw5mo52Om5KcOsspB5N++4cIUrV++M75/6O4xGSN/g3jsXdjJCWiKZEKWBuWkOP92ryqiqoZy9K5EsSMAGTgZ7/Lo3sj+L0fkqGyPECBcLE4niqYYH12mZdzIdc5hBmqcTo/ZZ6uKShooPll2PeG7ouNCnulL73U1UXUnuTd50FYlAzsZfvhEli1i+J3zKockOQJ0FhGYeH/2EA7ORdrc/7Q== cyberstudent@kali.local

┌──(chomps443㉿kali)-[~/DemoProject]
└─$

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global user.signingkey "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC1GVR5KEOaUSDs3rKh2LZQHgg7BQ2rY+T7h5j+q4yHViq0cIkMNE7jRwO95J22uJWVRtr2XIxChs4dPZf9X4JyvMQjSi+jBvjw+F2X+wSCH5LU4gGJHfAaPk/HG7kktDfXdBTsiT3v7N1oBbLNFrAjEptBI0VMplYedcTX6Ewoob2efRH2iaoLGrpi1bo29MC7FB2imW2emAEMf9G/qU8D+06XhhWuv/7v2i3FVpjm9cPM9In/Yc5CdKvai0KizQxeCk/FqK2uCQttm62KqKzu5rDi6DWpcULzpS0JBBdEptl4DTOvmBHu9LEshhrU1GqoGwnp8y0x/9ryb75E6AVcWTr2/coIFBWW7I9AcnhVm///xCZ5Iv3oKtzgZJIrl49gLKQt0Eh5BmPQp/gpL5+kS64TqqJWrLGiGbfUQHUvBWouvakUr4q5FVxCzbeKHFVX6RyE5P6GcB97tB8EgzjEw5mo52Om5KcOsspB5N++4cIUrV++M75/6O4xGSN/g3jsXdjJCWiKZEKWBuWkOP92ryqiqoZy9K5EsSMAGTgZ7/Lo3sj+L0fkqGyPECBcLE4niqYYH12mZdzIdc5hBmqcTo/ZZ6uKShooPll2PeG7ouNCnulL73U1UXUnuTd50FYlAzsZfvhEli1i+J3zKockOQJ0FhGYeH/2EA7ORdrc/7Q== jsiegel0516@gmail.com.local"

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ~/.ssh/git_allowed_signers
zsh: no such file or directory: /home/chomps443/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ echo -n "cyberstudent@kali.local " > ~/.ssh/git_allowed_signers && ssh-add -L >> ~/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global gpg.ssh.allowedSignersFile ~/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git commit --allow-empty --message="Did the SSH signing work?"
[master (root-commit) 308d958] Did the SSH signing work?

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git show --show-signature
commit 308d958dc28615dcc878a9ae527954592ea1c835 (HEAD -> master)
Good "git" signature for cyberstudent@kali.local with RSA key SHA256:niOK/v9p+uNGbkldRIqJLoxgFbo9/mT6EwblIydwGhY
Author: Jonathan Siegel <jsiegel0516@gmail.com>
Date:   Sat Mar 11 03:43:41 2023 +0000

    Did the SSH signing work?
```

Notes (Optional)**: I just took a screenshot of what the instructions told me to take a screenshot of during the moment.**

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

[Insert Screenshot Here]


```
┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global user.name "Jonathan Siegel"

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global commit.gpgsign true

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global gpg.format ssh

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ eval `ssh-agent -s`
Agent pid 56630

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ssh-add ~/.ssh/id_rsa
Identity added: /home/chomps443/.ssh/id_rsa (cyberstudent@kali.local)

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ssh-add -L
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC1GVR5KEOaUSDs3rKh2LZQHgg7BQ2rY+T7h5j+q4yHViq0cIkMNE7jRwO95J22uJWVRtr2XIxChs4dPZf9X4JyvMQjSi+jBvjw+F2X+wSCH5LU4gGJHfAaPk/HG7kktDfXdBTsiT3v7N1oBbLNFrAjEptBI0VMplYedcTX6Ewoob2efRH2iaoLGrpi1bo29MC7FB2
imW2emAEMf9G/qU8D+06XhhWuv/7v2i3FVpjm9cPM9In/YcSCdKvai0KizQxeCk/FqK2uCQttm62KqKzu5rDi6DWpcULzpS0JBBdEptl4DTOvmBHu9LEshhrU1GqoGwnp8y0x/9ryb75E6AVcWTr2/coIFBWW7I9AcnhVm///xCZ5Iv3oKtzgZJIrl49gLKQt0Eh5BmPQp/gpL5+kS64TqqJWrLGiGbfUQHUvBWouvakUr4q5FVxCzbeKHFVX6RyE5P6GcB97tB8EgzjEw5mo52Om5KcOsspB5N++4cIUrV++M75/6O4xGSN/g3jsXdjJCWiKZEKWBuWkOP92ryqiqoZy9K5EsSMAGTgZ7/Lo3sj+L0fkqGyPECBcLE4niqYYH12mZdzIdc5hBmqcTo/ZZ6uKShooPll2PeG7ouNCnulL73U1UXUnuTd50FYlAzsZfvhEli1i+J3zKockOQJ0FhGYeH/2EA7ORdrc/7Q== cyberstudent@kali.local

┌──(chomps443㉿kali)-[~/DemoProject]
└─$

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global user.signingkey "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC1GVR5KEOaUSDs3rKh2LZQHgg7BQ2rY+T7h5j+q4yHViq0cIkMNE7jRwO95J22uJWVRtr2XIxChs4dPZf9X4JyvMQjSi+jBvjw+F2X+wSCH5LU4gGJHfAaPk/HG7kktDfXdBTsiT3v7N1oBbLNFrAjEptBI0VMplYedcTX6Ewoob2efRH2iaoLGrpi1bo29MC7FB2imW2emAEMf9G/qU8D+06XhhWuv/7v2i3FVpjm9cPM9In/Yc5CdKvai0KizQxeCk/FqK2uCQttm62KqKzu5rDi6DWpcULzpS0JBBdEptl4DTOvmBHu9LEshhrU1GqoGwnp8y0x/9ryb75E6AVcWTr2/coIFBWW7I9AcnhVm///xCZ5Iv3oKtzgZJIrl49gLKQt0Eh5BmPQp/gpL5+kS64TqqJWrLGiGbfUQHUvBWouvakUr4q5FVxCzbeKHFVX6RyE5P6GcB97tB8EgzjEw5mo52Om5KcOsspB5N++4cIUrV++M75/6O4xGSN/g3jsXdjJCWiKZEKWBuWkOP92ryqiqoZy9K5EsSMAGTgZ7/Lo3sj+L0fkqGyPECBcLE4niqYYH12mZdzIdc5hBmqcTo/ZZ6uKShooPll2PeG7ouNCnulL73U1UXUnuTd50FYlAzsZfvhEli1i+J3zKockOQJ0FhGYeH/2EA7ORdrc/7Q== jsiegel0516@gmail.com.local"

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ ~/.ssh/git_allowed_signers
zsh: no such file or directory: /home/chomps443/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ echo -n "cyberstudent@kali.local " > ~/.ssh/git_allowed_signers && ssh-add -L >> ~/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git config --global gpg.ssh.allowedSignersFile ~/.ssh/git_allowed_signers

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git commit --allow-empty --message="Did the SSH signing work?"
[master (root-commit) 308d958] Did the SSH signing work?

┌──(chomps443㉿kali)-[~/DemoProject]
└─$ git show --show-signature
commit 308d958dc28615dcc878a9ae527954592ea1c835 (HEAD -> master)
Good "git" signature for cyberstudent@kali.local with RSA key SHA256:niOK/v9p+uNGbkldRIqJLoxgFbo9/mT6EwblIydwGhY
Author: Jonathan Siegel <jsiegel0516@gmail.com>
Date:   Sat Mar 11 03:43:41 2023 +0000

    Did the SSH signing work?
```

> **Notes** (Optional)**: I just took a screenshot of what the instructions told me to take a screenshot of during the moment.**

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~~
- ☑ ~~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 Points	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	0	+2 bonus
Description of an additional use of SSH keys	0	+2 bonus
Total Possible Points (Part A + Part B)	**20**	**20** (+4)

Grader Feedback