Pippin Assessment

Executive Summary

The problem statement asked us to analyze the file **/home/student/pippin/SaveForPippin.zip** and use it to gain entry in **pippin** account and recover the **pippinflag.txt** file. After I unzipped the file **SaveForPippin.zip** using the pre-installed **unzip** tool, I received the **PippinsEyesOnly.tar.gz**. I failed to extract the file using **tar** command, therefore, I checked the file type and found the file to be **bzip2 compressed data**. Ultimately, I obtained the **Non-ISO extended-ASCII text** file after repeatedly renaming the file to the correct extension and then extracting it.

The file **PippinsEyesOnly** was a huge text file and according to the problem statement, somewhere in this file was the key to login to Pippin's account. I used the vim editor to find the **OPENSSH PRIVATE KEY** from this file. I copied the private key in a separate text file **key.txt** to use it in order to enter Pippin's account. Finally, after changing the permissions of the file to read to **600**, I was successfully able to login to Pippin's account using the command **ssh -i <text file with key> pippin@cs647**.

Vulnerabilities Identified

1. One major vulnerability that was identified was that all the users had access to the file **SaveForPippin.zip** and anyone could extract the data present inside it. The file's permissions should not allow any user other than the owner of the file to access the contents and perform any actions on it.
2. Inside the file **PippinsEyesOnly**, there was little to no efforts put in order to hide the private key required to gain access to the account through SSH.

Recommendations

As much as I have learned from this assessment, using the ***Security Through Obscurity*** technique to hide private data should not be encouraged because it relies solely on keeping the details of a security system secret, rather than actually strengthening the system through proper design and implementation. As demonstrated through this assessment, it is clear that obscuring SSH keys to hide them from potential bad actors was not a sufficient way to protect his account.

Assumptions

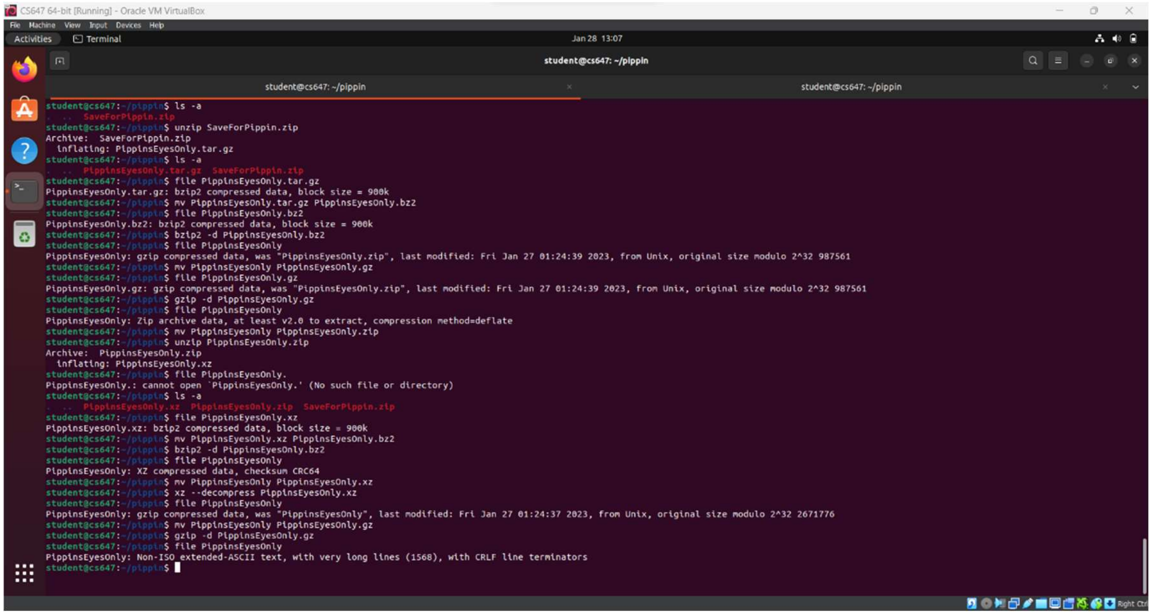
Some of the assumptions I made during this assessment were:

1. After extracting the file **SaveForPippin.zip**, I checked the file format and assumed that the file would require nested renaming and decompressions' steps.
2. Another assumption made was that Internet access would not be required.
3. One last assumption that I made was that after extracting the text file **PippinsEyesOnly**, nano editor would not be able to extract the key properly. Hence, I used vim editor.

Steps to Reproduce the Attack

1. First of all, I unzipped the file **SaveForPippin.zip** in order to get the file **PippinsEyesOnly.tar.gz**.
2. After that, I tried extracting the file using **gzip** command.

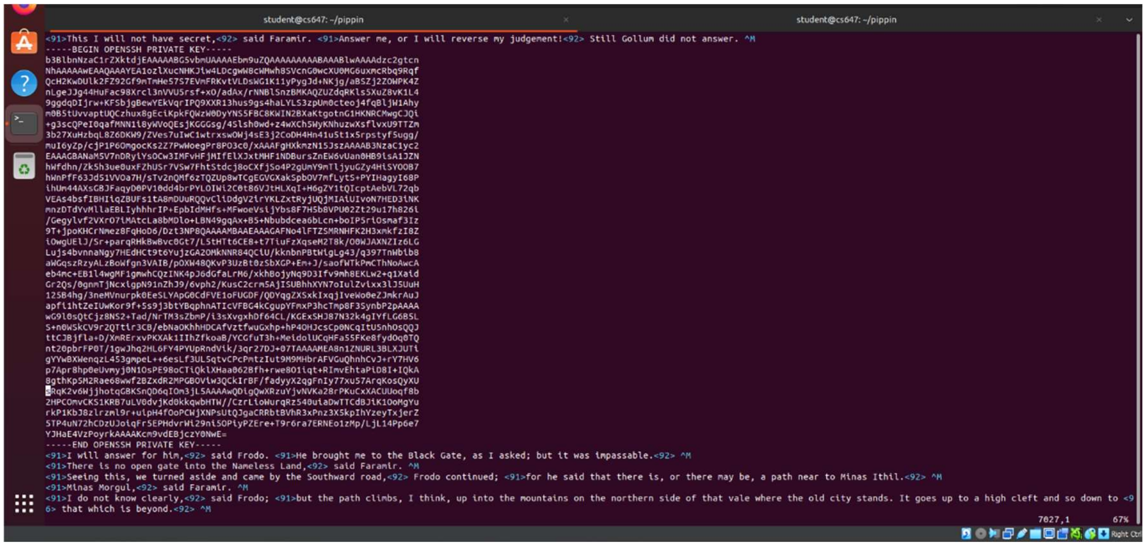
3. Failing to do that, I checked the file type and found it to be a bzip2 compressed data file.
4. I tried to rename the file using **mv** command and then was able to extract it using the command **bzip2 -d PippinEyesOnly.bz2**.
5. Subsequently, as shown in *Figure 1*, I obtained a file compressed with **gzip** format and realized that the file would require nested decompression steps.



```
student@cs647:~/pippin$ ls -a
.  ..  SaveForPippin.zip
student@cs647:~/pippin$ unzip SaveForPippin.zip
Archive:  SaveForPippin.zip
  inflating: PippinsEyesOnly.tar.gz
student@cs647:~/pippin$ ls -a
.  ..  PippinsEyesOnly.tar.gz  SaveForPippin.zip
student@cs647:~/pippin$ file PippinsEyesOnly.tar.gz
PippinsEyesOnly.tar.gz: bzip2 compressed data, block size = 900k
student@cs647:~/pippin$ mv PippinsEyesOnly.tar.gz PippinsEyesOnly.bz2
student@cs647:~/pippin$ file PippinsEyesOnly.bz2
PippinsEyesOnly.bz2: bzip2 compressed data, block size = 900k
student@cs647:~/pippin$ bzip2 -d PippinsEyesOnly.bz2
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: gzip compressed data, was "PippinsEyesOnly.zip", last modified: Fri Jan 27 01:24:39 2023, from Unix, original size modulo 2^32 987561
student@cs647:~/pippin$ mv PippinsEyesOnly PippinsEyesOnly.gz
student@cs647:~/pippin$ file PippinsEyesOnly.gz
PippinsEyesOnly.gz: gzip compressed data, was "PippinsEyesOnly.zip", last modified: Fri Jan 27 01:24:39 2023, from Unix, original size modulo 2^32 987561
student@cs647:~/pippin$ gzip -d PippinsEyesOnly.gz
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: Zip archive data, at least v2.0 to extract, compression method=deflate
student@cs647:~/pippin$ mv PippinsEyesOnly PippinsEyesOnly.zip
student@cs647:~/pippin$ unzip PippinsEyesOnly.zip
Archive:  PippinsEyesOnly.zip
  inflating: PippinsEyesOnly.xz
student@cs647:~/pippin$ file PippinsEyesOnly.
PippinsEyesOnly.: cannot open `PippinsEyesOnly.' (No such file or directory)
student@cs647:~/pippin$ ls -a
.  ..  PippinsEyesOnly.xz  PippinsEyesOnly.zip  SaveForPippin.zip
student@cs647:~/pippin$ file PippinsEyesOnly.xz
PippinsEyesOnly.xz: bzip2 compressed data, block size = 900k
student@cs647:~/pippin$ mv PippinsEyesOnly.xz PippinsEyesOnly.bz2
student@cs647:~/pippin$ bzip2 -d PippinsEyesOnly.bz2
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: XZ compressed data, checksum CRC64
student@cs647:~/pippin$ mv PippinsEyesOnly PippinsEyesOnly.xz
student@cs647:~/pippin$ xz --decompress PippinsEyesOnly.xz
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: gzip compressed data, was "PippinsEyesOnly", last modified: Fri Jan 27 01:24:37 2023, from Unix, original size modulo 2^32 2671776
student@cs647:~/pippin$ mv PippinsEyesOnly PippinsEyesOnly.gz
student@cs647:~/pippin$ gzip -d PippinsEyesOnly.gz
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: Non-ISO extended-ASCII text, with very long lines (1568), with CRLF line terminators
student@cs647:~/pippin$ 
```

Figure 1

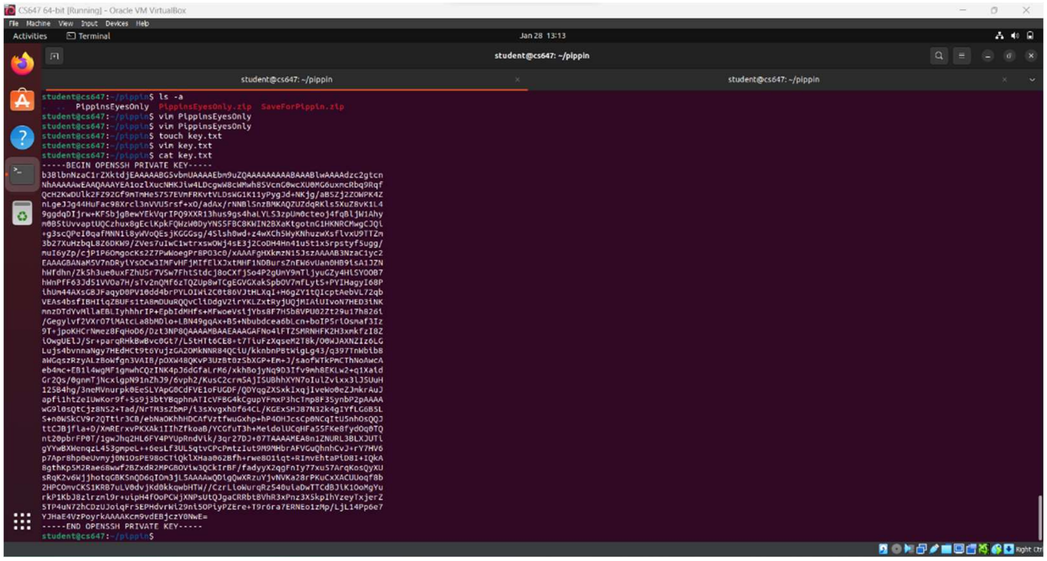
6. Ultimately after receiving the ASCII text file, I scanned the file for the **OPENSSH PRIVATE KEY** hidden somewhere in the file as mentioned in the information provided in the problem statement.
7. I found the private key using the **grep** command and extracted it using the vim editor, as shown in *Figure 2*.



```
<91>This I will not have secret,<92> said Faramir. <91>Answer me, or I will reverse my judgement!<92> Still Gollum did not answer. ^M
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA1ozlXucNHKJiw4LDcgwW8cWMwh8SVcnG0wcXU0MG6uxmcRbq9Rqf
QcH2KwDUlk2FZ92Gf9mTmHe57S7EVmFRKvtVLDsWG1K11yPygJd+NKjg/aBSZj2ZOWPK4Z
nLgeJJg44HuFac98Xrcl3nVVU5rsf+xO/adAx/rNNBlSnzBMKAQZUZdqRKls5XuZ8vK1L4
9ggdqDIjrw+KFSbjgBewYEkVqrIPQ9XXR13hus9gs4haLYLS3zpUm0cteoj4fqBljW1Ahy
m0B5tUvvaptUQCzhux8gEciKpkFQWzW0DyYNS5FBC8KWIN2BXaKtgotnG1HKNRCMwgCJQi
+g3scQPeI0qafMNN1i8yWVoQEsjKGGGsg/4Slsh0wd+z4wXCh5WyKNhuzwXsflvxU9TTZm
3b27XuHzbqL8Z6DKW9/ZVes7uIwC1wtrxswOWj4sE3j2CoDH4Hn41u5t1x5rpstyf5ugg/
muI6yZp/cjP1P6OmgocKs2Z7PwWoegPr8PO3c0/xAAAFgHXkmzN15JszAAAAB3NzaC1yc2
EAAAGBANaM5V7nDRyiYsOCw3IMFvHFjMIfElXJxtMHF1NDBursZnEW6vUan0HB9isA1JZN
hWfdhn/Zk5h3ue0uxFZhUSr7VSw7FhtStdcj8oCXfjSo4P2gUmY9mTljyuGZy4HiSYOOB7
hWnPfF63Jd51VVOa7H/sTv2nQMf6zTQZUp8wTCgEGVGXakSpbOV7mfLytS+PYIHagyI68P
ihUm44AXsGBJFaqyD0PV10dd4brPYLOIWi2C0t86VJtHLXqI+H6gZY1tQIcptAebVL72qb
VEAs4bsfIBHIiqZBUFs1tA8mDUuRQQvCliDdgV2irYKLZxtRyjUQjMIAiUIvoN7HED3iNK
mnzDTdYvMllaEBLIyhhhrIP+EpbIdMHfs+MFwoeVsijYbs8F7H5b8VPU02Zt29u17h826i
/Gegylvf2VXrO7iMAtcLa8bMDlo+LBN49gqAx+B5+Nbubdcea6bLcn+boIP5riOsmaf3Iz
9T+jpoKHCrNmez8FqHoD6/Dzt3NP8QAAAAMBAAEAAAGAFNo4lFTZSMRNHFK2H3xmkfzI8Z
iOwgUElJ/Sr+parqRHkBwBvc0Gt7/L5tHTt6CE8+t7TiuFzXqseM2T8k/O0WJAXNZIz6LG
Lujs4bvnnaNgy7HEdHCt9t6YujzGA2OMkNNR84QCiU/kknbnPBtWigLg43/q397TnWbib8
aWGqszRzyALzBoWfgn3VAIB/pOXW48QKvP3UzBt0zSbXGP+Em+J/saofWTkPmCThNoAwcA
eb4mc+EB1l4wgMF1gmwhCQzINK4pJ6dGfaLrM6/xkhBojyNq9D3Ifv9mh8EKLw2+q1Xaid
Gr2Qs/0gnmTjNcxigpN91nZhJ9/6vph2/KusC2crm5AjISUBhhXYN7oIulZvixx3lJ5UuH
125B4hg/3neMVnurpk0EeSLYApG0CdFVE1oFUGDF/QDYqgZXSxkIxqjIveWo0eZJmkrAuJ
apfi1htZeIUwKor9f+5s9j3btYBqphnATIcVFBG4kCgupYFmxP3hcTmp8F3SynbP2pAAAA
wG9l0sQtCjz8NS2+Tad/NrTM3sZbmP/i3sXvgxhDf64CL/KGExSHJ87N32k4gIYfLG6BSL
S+n0WSkCV9r2QTtir3CB/ebNaOKhhHDCAfVztfwuGxhp+hP4OHJcsCp0NCqItU5nhOsQQJ
ttCJBjfla+D/XmRErxvPKXAk1IIhZfkoaB/YCGfuT3h+MeidolUCqHFa55FKe8fydOq0TQ
nt20pbrFP0T/1gwJhq2HL6FY4PYUpRndVik/3qr27DJ+07TAAAAMEA8n1ZNURL3BLXJUTi
gYYwBXWenqzL453gmpeL++6esLf3ULSqtvCPcPmtzIut9M9MHbrAFVGuQhnhCvJ+rY7HV6
p7Apr8hp0eUvmyj0N1OsPE98oCTiQklXHaa062Bfh+rwe8O1iqt+RImvEhtaPiD8I+IQkA
8gthKp5M2Rae68wwf2BZxdR2MPGBOViw3QCkIrBF/fadyyX2qgFnIy77xu57ArqKosQyXU
sRqK2v6WjjhotqGBKSnQD6qIOm3jL5AAAAwQDigQwXRzuYjvNVKa28rPKuCxXACUUoqf8b
2HPCOmvCKS1KRB7uLV0dvjKd0kkqwbHTW//CzrLioWurqRz540uiaDwTTCdBJiK1OoMgYu
rkP1KbJ8zlrzml9r+uipH4fOoPCWjXNPsUtQJgaCRRbtBVhR3xPnz3X5kpIhYzeyTxjerZ
5TP4uN72hCDzUJoiqFr5EPHdvrWi29ni5OPiyPZEre+T9r6ra7ERNEo1zMp/LjL14Pp6e7
YJHaE4VzPoyrkAAAAKcm9vdEBjczY0NwE=
-----END OPENSSH PRIVATE KEY-----
<91>I will answer for him,<92> said Frodo. <91>He brought me to the Black Gate, as I asked; but it was impassable.<92> ^M
<91>There is no open gate into the Nameless Land,<92> said Faramir. ^M
<91>Seeing this, we turned aside and came by the Southward road,<92> Frodo continued; <91>for he said that there is, or there may be, a path near to Minas Ithil.<92> ^M
<91>Minas Morgul,<92> said Faramir. ^M
<91>I do not know clearly,<92> said Frodo; <91>but the path climbs, I think, up into the mountains on the northern side of that vale where the old city stands. It goes up to a high cleft and so down to <9
6> that which is beyond.<92> ^M
                                                                                            7027,1        67%
```

Figure 2

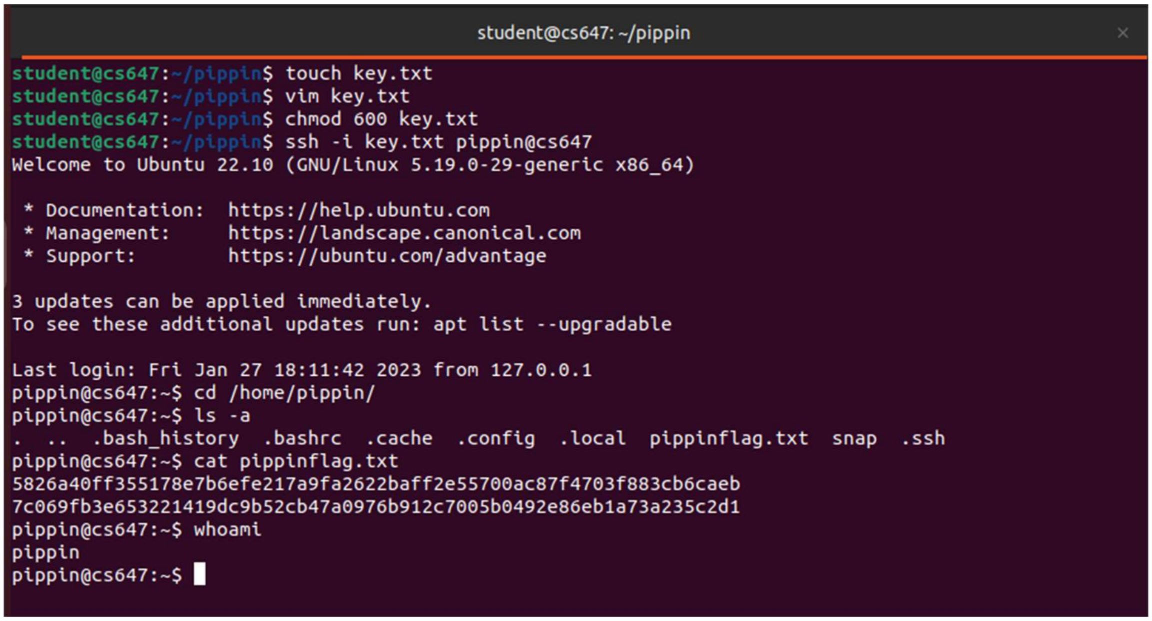
8. I created a text file and copied the private key inside it in order to use that file to gain access to Pippin's account. *Figure 3* shows the file I created.



```
student@cs647:~/pippin$ ls -a
.  ..  PippinsEyesOnly  PippinsEyesOnly.zip  SaveForPippin.zip
student@cs647:~/pippin$ vim PippinsEyesOnly
student@cs647:~/pippin$ vim PippinsEyesOnly
student@cs647:~/pippin$ touch key.txt
student@cs647:~/pippin$ vim key.txt
student@cs647:~/pippin$ cat key.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA1ozlXucNHKJiw4LDcgwW8cWMwh8SVcnG0wcXU0MG6uxmcRbq9Rqf
QcH2KwDUlk2FZ92Gf9mTmHe57S7EVmFRKvtVLDsWG1K11yPygJd+NKjg/aBSZj2ZOWPK4Z
nLgeJJg44HuFac98Xrcl3nVVU5rsf+xO/adAx/rNNBlSnzBMKAQZUZdqRKls5XuZ8vK1L4
9ggdqDIjrw+KFSbjgBewYEkVqrIPQ9XXR13hus9gs4haLYLS3zpUm0cteoj4fqBljW1Ahy
m0B5tUvvaptUQCzhux8gEciKpkFQWzW0DyYNS5FBC8KWIN2BXaKtgotnG1HKNRCMwgCJQl
+g3scQPel0qafMNN1i8yWVoQEsjKGGGsg/4Slsh0wd+z4wXCh5WyKNhuzwXsflvxU9TTZm
3b27XuHzbqL8Z6DKW9/ZVes7uIwC1wtrxswOWj4sE3j2CoDH4Hn41u5t1x5rpstyf5ugg/
muI6yZp/cjP1P6OmgocKs2Z7PwWoegPr8PO3c0/xAAAFgHXkmzN15JszAAAAB3NzaC1yc2
EAAAGBANaM5V7nDRylYsOCw3IMFvHFjMIfElXJxtMHF1NDBursZnEW6vUan0HB9lsA1JZN
hWfdhn/Zk5h3ue0uxFZhUSr7VSw7FhtStdcj8oCXfjSo4P2gUmY9mTljyuGZy4HlSYOOB7
hWnPfF63Jd51VVOa7H/sTv2nQMf6zTQZUp8wTCgEGVGXakSpbOV7mfLytS+PYIHagyI68P
ihUm44AXsGBJFaqyD0PV10dd4brPYLOIWi2C0t86VJtHLXqI+H6gZY1tQIcptAebVL72qb
VEAs4bsfIBHIiqZBUFs1tA8mDUuRQQvCliDdgV2irYKLZxtRyjUQjMIAiUIvoN7HED3iNK
mnzDTdYvMllaEBLIyhhhrIP+EpbIdMHfs+MFwoeVsijYbs8F7H5b8VPU02Zt29u17hB26i
/Gegylvf2VXrO7iMAtcLa8bMDlo+LBN49gqAx+B5+Nbubdcea6bLcn+boIP5rlOsmaf3Iz
9T+jpoKHCrNmez8FqHoD6/Dzt3NP8QAAAAMBAAEAAAGAFNo4lFTZSMRNHFK2H3xmkfzI8Z
iOwgUElJ/Sr+parqRHkBwBvc0Gt7/L5tHTt6CE8+t7TiuFzXqseM2T8k/O0WJAXNZIz6LG
Lujs4bvnnaNgy7HEdHCt9t6YujzGA2OMkNNR84QCiU/kknbnPBtWigLg43/q397TnWbibB
aWGqszRzyALzBoWfgn3VAIB/pOXW48QKvP3UzBt0zSbXGP+Em+J/saofWTkPmCThNoAwcA
eb4mc+EB1l4wgMF1gmwhCQzINK4pJ6dGfaLrM6/xkhBojyNq9D3Ifv9mh8EKLw2+q1Xaid
Gr2Qs/0gnmTjNcxigpN91nZhJ9/6vph2/KusC2crm5AjISUBhhXYN7oIulZvixx3lJSUuH
125B4hg/3neMVnurpk0EeSLYApG0CdFVE1oFUGDF/QDYqgZXSxkIxqjIveWo0eZJmkrAuJ
apfi1htZeIUwKor9f+5s9j3btYBqphnATIcVFBG4kCgupYFmxP3hcTmp8F3SynbP2pAAAA
wG9l0sQtCjz8NS2+Tad/NrTM3sZbmP/i3sXvgxhDf64CL/KGExSHJ87N32k4gIYfLG6B5L
S+n0WSkCV9r2QTtir3CB/ebNaOKhhHDCAfVztfwuGxhp+hP4OHJcsCp0NCqItU5nhOsQQJ
ttCJBjfla+D/XmRErxvPKXAk1IIhZfkoaB/YCGfuT3h+MeidolUCqHFa5SFKe8fydOq0TQ
nt20pbrFP0T/1gwJhq2HL6FY4PYUpRndVik/3qr27DJ+07TAAAAMEA8n1ZNURL3BLXJUTi
gYYwBXWenqzL453gmpeL++6esLf3UL5qtvCPcPmtzIut9M9MHbrAFVGuQhnhCvJ+rY7HV6
p7Apr8hp0eUvmyj0N1OsPE98oCTiQklXHaa062Bfh+rwe8O1iqt+RImvEhtaPiD8I+IQkA
8gthKp5M2Rae68wwf2BZxdR2MPGBOViw3QCkIrBF/fadyyX2qgFnIy77xu57ArqKosQyXU
sRqK2v6WjjhotqGBKSnQD6qIOm3jL5AAAAwQDigQwXRzuYjvNVKa28rPKuCxXACUUoqf8b
2HPCOmvCKS1KRB7uLV0dvjKd0kkqwbHTW//CzrLioWurqRz540uiaDwTTCdBJiK1OoMgYu
rkP1KbJ8zlrzml9r+uipH4fOoPCWjXNPsUtQJgaCRRbtBVhR3xPnz3X5kpIhYzeyTxjerZ
5TP4uN72hCDzUJoiqFr5EPHdvrWi29ni5OPiyPZEre+T9r6ra7ERNEo1zMp/LjL14Pp6e7
YJHaE4VzPoyrkAAAAKcm9vdEBjczY0NwE=
-----END OPENSSH PRIVATE KEY-----
student@cs647:~/pippin$
```

Figure 3

9. The openssh requires private keys to have **600** permission i.e., only the owner has read and write access for the file in order to prevent unauthorized access by other users, I changed the permission of the text file using **chmod 600 key.txt** command.
10. Finally, as shown in *Figure 4*, I used the text file containing the key to successfully get inside Pippin's account using openssh with the command **ssh -i key.txt pippin@cs647** and checked the contents of the file **pippinflag.txt** using the **cat** command.



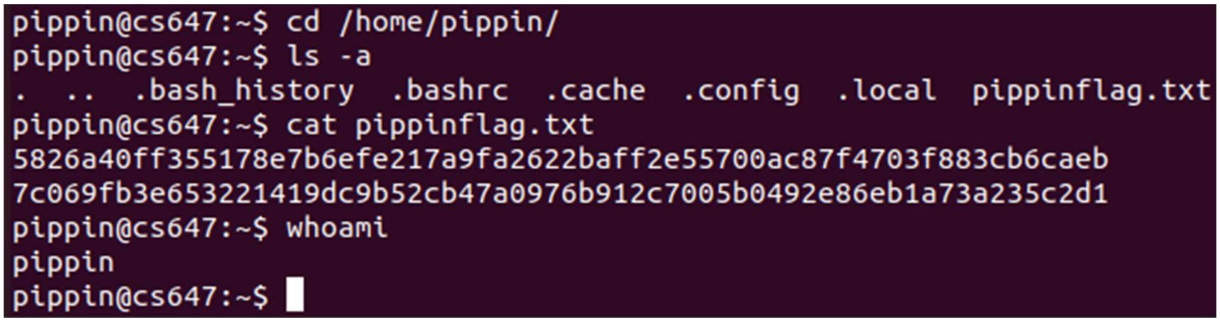
```
student@cs647:~/pippin$ touch key.txt
student@cs647:~/pippin$ vim key.txt
student@cs647:~/pippin$ chmod 600 key.txt
student@cs647:~/pippin$ ssh -i key.txt pippin@cs647
Welcome to Ubuntu 22.10 (GNU/Linux 5.19.0-29-generic x86_64)

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

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

Last login: Fri Jan 27 18:11:42 2023 from 127.0.0.1
pippin@cs647:~$ cd /home/pippin/
pippin@cs647:~$ ls -a
.  ..  .bash_history  .bashrc  .cache  .config  .local  pippinflag.txt  snap  .ssh
pippin@cs647:~$ cat pippinflag.txt
5826a40ff355178e7b6efe217a9fa2622baff2e55700ac87f4703f883cb6caeb
7c069fb3e653221419dc9b52cb47a0976b912c7005b0492e86eb1a73a235c2d1
pippin@cs647:~$ whoami
pippin
pippin@cs647:~$ 
```

Figure 4

Findings

Once logged in as the user pippin, I was able to retrieve the file pippinflag.txt. Also shown in *Figure 3*, the file contained the following contents:

5826a40ff355178e7b6efe217a9fa2622baff2e55700ac87f4703f883cb6caeb7c069f
b3e653221419dc9b52cb47a0976b912c7005b0492e86eb1a73a235c2d1



```
pippin@cs647:~$ cd /home/pippin/
pippin@cs647:~$ ls -a
.  ..  .bash_history  .bashrc  .cache  .config  .local  pippinflag.txt
pippin@cs647:~$ cat pippinflag.txt
5826a40ff355178e7b6efe217a9fa2622baff2e55700ac87f4703f883cb6caeb
7c069fb3e653221419dc9b52cb47a0976b912c7005b0492e86eb1a73a235c2d1
pippin@cs647:~$ whoami
pippin
pippin@cs647:~$ 
```