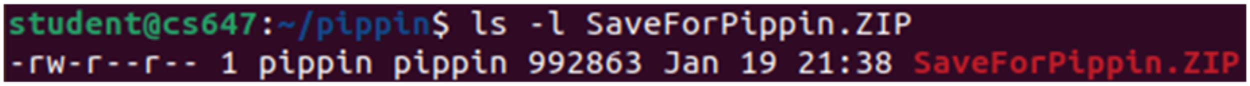
# Security risks of obscuring private keys

## Executive Summary

This assessment explained the vulnerability that was identified when the owner of the account had hidden the access to his account in a file without following proper procedures. Ignoring this vulnerability could have been very risky because the attacker would have accessed the owner's account with that weakness and stolen the information without the owner realizing it. In this assessment, the attacker was able to break through a series of recurring files and retrieve the key present inside them.

## Vulnerabilities Identified

The vulnerability identified in this scenario is that the zip file "SaveForPippin.ZIP" that contains the private key was not password protected, and the file permissions were set such that there were no restrictions for other users. This is a critical level vulnerability, which means any user could unzip the file and extract the key inside it. In screenshot 1, 'r' in "-rw-r--r--" means read, this allows any user to unzip the file.



```
student@cs647:~/pippin$ ls -l SaveForPippin.ZIP
-rw-r--r-- 1 pippin pippin 992863 Jan 19 21:38 SaveForPippin.ZIP
```

*Screenshot 1: Checking file permissions.*

## Recommendations

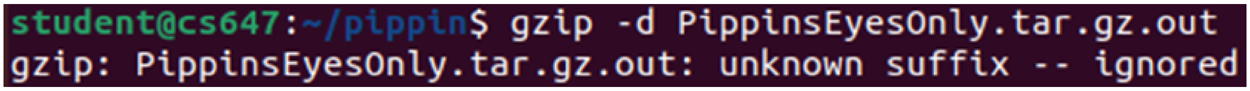
To mitigate the vulnerability listed above, the owner needs to set the file permissions of the zip file as, "`chmod 600 SaveForPippin.ZIP`". "chmod" is used to change the permissions of the file or folder, and `600` means only the owner has full read and write access to the file while no other user can access the file.

The client could set a password for "SaveForPippin.ZIP" using "`zip -e SaveForPippin.ZIP`". The `-e` flag will encrypt the file, and the owner will be prompted to set a password for the file. This could add additional protection from attackers unzipping the "SaveForPippin.ZIP" file.

## Steps to reproduce the attack

I saw that a zip archive named "SaveForPippin.zip" is present in the path "/home/student/pippin". Then I unzipped this file using the unzip command and the file extracted was "PippinsEyesOnly.tar.gz". To extract this type of file, I needed to know the exact file type so that I could use the right command. As shown in screenshot 1, we can use the "`file file_name`" command to see what kind of file it is.

To decompress the bzip2 file, I used “`bzip2 -d PippinsEyesOnly.tar.gz`”. Here I used the `-d` flag to decompress the file. I have used the `-d` flag to decompress any type of compressed file in this attack. This extracted a gzip file, “PippinsEyesOnly.tar.gz.out” which was another type of compressed file. If I tried to extract its contents using “`gzip –d PippinsEyesOnly.tar.gz.out`”, it showed an unknown suffix error because it had ‘.gz.out’ instead of ‘.gz’ as shown in screenshot 2.



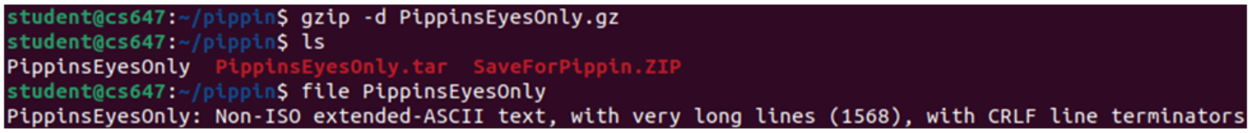
```
student@cs647:~/pippin$ gzip -d PippinsEyesOnly.tar.gz.out
gzip: PippinsEyesOnly.tar.gz.out: unknown suffix -- ignored
```

*Screenshot 2: Unknown suffix error.*

Since the suffix name was wrong, I corrected it by changing the name of the file using the `mv` command. “`mv PippinsEyesOnly.tar.gz.out PippinsEyesOnly.tar.gz`”. Then I extracted the file using “`gzip –d PippinsEyesOnly.tar.gz`”. Then a file named “PippinsEyesOnly.tar” got extracted, which was a zip archive, and to unzip this archive, I used “`unzip PippinsEyesOnly.tar`”. This extracted the “PippinsEyesOnly.xz” file.

‘PippinsEyesOnly.xz’ was bzip2 compressed data with ‘.xz’ extension. Just like I have done previously, I again changed the extension from ‘.xz’ to ‘.bz’ to extract the file by changing the file name to “PippinsEyesOnly.bz”. Now I extracted the bzip file using “`bzip2 -d PippinsEyesOnly.bz`” and I got a file named “PippinsEyesOnly”. This was an xz compressed file with no extension, and I added ‘.xz’ extension by renaming the file to “PippinsEyesOnly.xz” using `mv` command.

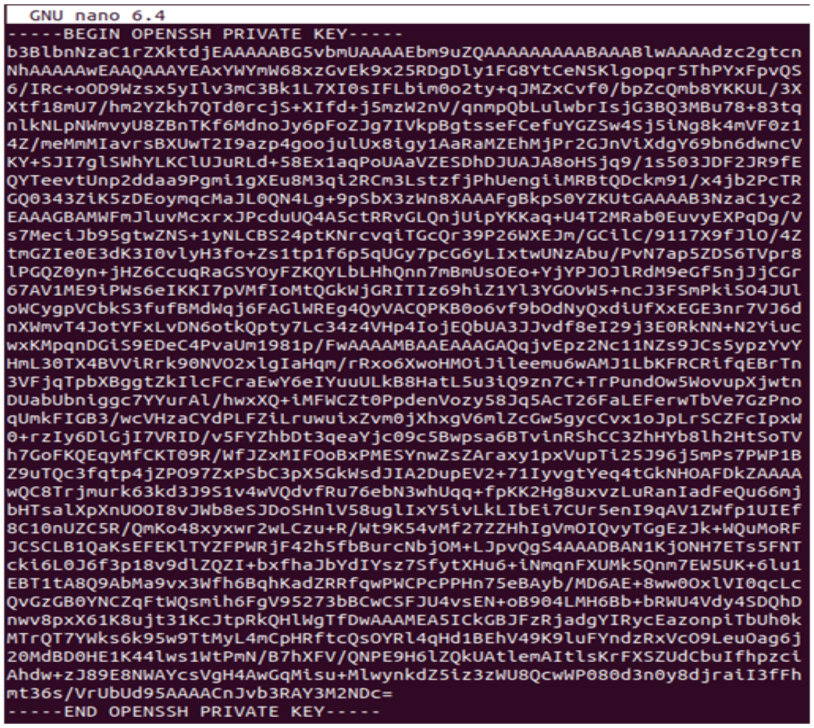
Then, I decompressed the xz file using “`xz –d PippinsEyesOnly.bz`” and printed another “PippinsEyesOnly” gzip file. I extracted this file by using a similar method as above and changing the name of the file to “PippinsEyesOnly.gz”. After that I used “`gzip -d PippinsEyesOnly.gz`” to extract the file. After this step, I got a text file named “PippinsEyesOnly” as shown in screenshot 3.



```
student@cs647:~/pippin$ gzip -d PippinsEyesOnly.gz
student@cs647:~/pippin$ ls
PippinsEyesOnly  PippinsEyesOnly.tar  SaveForPippin.ZIP
student@cs647:~/pippin$ file PippinsEyesOnly
PippinsEyesOnly: Non-ISO extended-ASCII text, with very long lines (1568), with CRLF line terminators
```

*Screenshot 3: Text file that contains the private key.*

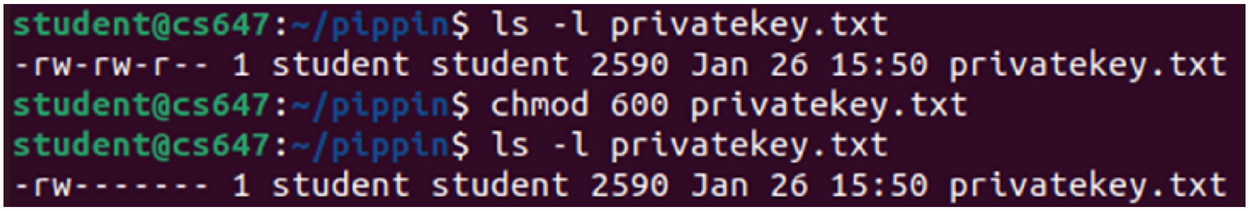
I opened this file using the “nano” editor which is prebuilt in Linux systems to check the contents of the file. This file contains a lot of text so I found the private key using the “ctrl + w” shortcut and typed “PRIVATE KEY” to go to the line where the private key was hidden in the file. Using this key, I could gain access to the user “pippin”. To do that first I copied the whole text into a new file and named it “privatekey.txt” as shown in the screenshot 4.



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxYWYmW68xzGvEk9x25RDgDly1FG8YtCeNSKlgopqr5ThPYxFpvQS
6/IRc+oOD9Wzsx5yIlv3mC3Bk1L7XI0sIFLbim0o2ty+qJMZxCvf0/bpZcQmb8YKKUL/3X
Xtf18mU7/hm2YZkh7QTd0rcjS+XIfd+j5mzW2nV/qnmpQbLulwbrIsjG3BQ3MBu78+83tq
nlkNLpNWmvyU8ZBnTKf6MdnoJy6pFoZJg7IVkpBgtsseFCefuYGZSw4Sj5iNg8k4mVF0z1
4Z/meMmMIavrsBXUwT2I9azp4goojulUx8igy1AaRaMZEhMjPr2GJnViXdgY69bn6dwncV
KY+SJI7glSWhYLKClUJuRLd+58Ex1aqPoUAaVZESDhDJUAJA8oHSjq9/1s503JDF2JR9fE
QYTeevtUnp2ddaa9Pgmi1gXEu8M3qi2RCm3LstzfjPhUengiiMRBtQDckm91/x4jb2PcTR
GQ0343ZiK5zDEoymqcMaJL0QN4Lg+9pSbX3zWn8XAAAFgBkpS0YZKUtGAAAAB3NzaC1yc2
EAAAGBAMWFmJluvMcxrxJPcduUQ4A5ctRRvGLQnjUipYKKaq+U4T2MRab0EuvyEXPqDg/V
s7MeciJb95gtwZNS+1yNLCBS24ptKNrcvqiTGcQr39P26WXEJm/GCilC/9117X9fJlO/4Z
tmGZIe0E3dK3I0vlyH3fo+Zs1tp1f6p5qUGy7pcG6yLIxtwUNzAbu/PvN7ap5ZDS6TVpr8
lPGQZ0yn+jHZ6CcuqRaGSYOyFZKQYLbLHhQnn7mBmUsOEo+YjYPJOJlRdM9eGf5njJjCGr
67AV1ME9iPWs6eIKKI7pVMfIoMtQGkWjGRITIz69hiZ1Yl3YGOvW5+ncJ3FSmPkiSO4JUl
oWCygpVCbkS3fufBMdWqj6FAGlWREg4QyVACQPKB0o6vf9bOdNyQxdiUfXxEGE3nr7VJ6d
nXWmvT4JotYFxLvDN6otkQpty7Lc34z4VHp4IojEQbUA3JJvdf8eI29j3E0RkNN+N2Yiuc
wxKMpqnDGiS9EDeC4PvaUm1981p/FwAAAAMBAAEAAAGAQqjvEpz2Nc11NZs9JCs5ypzYvY
HmL30TX4BVViRrk90NVO2xlgIaHqm/rRxo6XwoHMOiJileemu6wAMJ1LbKFRCRifqEBrTn
3VFjqTpbXBggtZkIlcFCraEwY6eIYuuULkB8HatL5u3iQ9zn7C+TrPundOw5WovupXjwtn
DUabUbniggc7YYurAl/hwxXQ+iMFWCZt0PpdenVozy58Jq5AcT26FaLEFerwTbVe7GzPno
qUmkFIGB3/wcVHzaCYdPLFZiLruwuixZvm0jXhxgV6mlZcGw5gycCvx1oJpLrSCZFcIpxW
0+rzIy6DlGjI7VRID/v5FYZhbDt3qeaYjc09c5Bwpsa6BTvinRShCC3ZhHYb8lh2HtSoTV
h7GoFKQEqyMfCKT09R/WfJZxMIFOoBxPMESYnwZsZAraxy1pxVupTi25J96j5mPs7PWP1B
Z9uTQc3fqtp4jZPO97ZxPSbC3pX5GkWsdJIA2DupEV2+71IyvgtYeq4tGkNHOAFDkZAAAA
wQC8Trjmurk63kd3J9S1v4wVQdvfRu76ebN3whUqq+fpKK2Hg8uxvzLuRanIadFeQu66mj
bHTsalXpXnUOOI8vJWb8eSJDoSHnlV58uglIxY5ivLkLIbEi7CUr5enI9qAV1ZWfp1UIEf
8C10nUZC5R/QmKo48xyxwr2wLCzu+R/Wt9K54vMf27ZZHhIgVmOIQvyTGgEzJk+WQuMoRF
JCSCLB1QaKsEFEKlTYZFPWRjF42h5fbBurcNbjOM+LJpvQgS4AAADBAN1KjONH7ETs5FNT
cki6L0J6f3p18v9dlZQZI+bxfhaJbYdIYsz7SfytXHu6+iNmqnFXUMk5Qnm7EW5UK+6lu1
EBT1tA8Q9AbMa9vx3Wfh6BqhKadZRRfqwPWCPcPPHn75eBAyb/MD6AE+8ww0OxlVI0qcLc
QvGzGB0YNCZqFtWQsmih6FgV95273bBCwCSFJU4vsEN+oB904LMH6Bb+bRWU4Vdy4SDQhD
nwv8pxX61K8ujt31KcJtpRkQHlWgTfDwAAAMEA5ICkGBJFzRjadgYIRycEazonpiTbUh0k
MTrQT7YWks6k95w9TtMyL4mCpHRftcQsOYRl4qHd1BEhV49K9luFYndzRxVcO9LeuOag6j
20MdBD0HE1K44lws1WtPmN/B7hXFV/QNPE9H6lZQkUAtlemAItlsKrFXSZUdCbuIfhpzci
Ahdw+zJ89E8NWAYcsVgH4AwGqMisu+MlwynkdZ5iz3zWU8QcwWP080d3n0y8djraiI3fFh
mt36s/VrUbUd95AAAACnJvb3RAY3M2NDc=
-----END OPENSSH PRIVATE KEY-----
```

*Screenshot 4: Fully copied private key from the text file.*

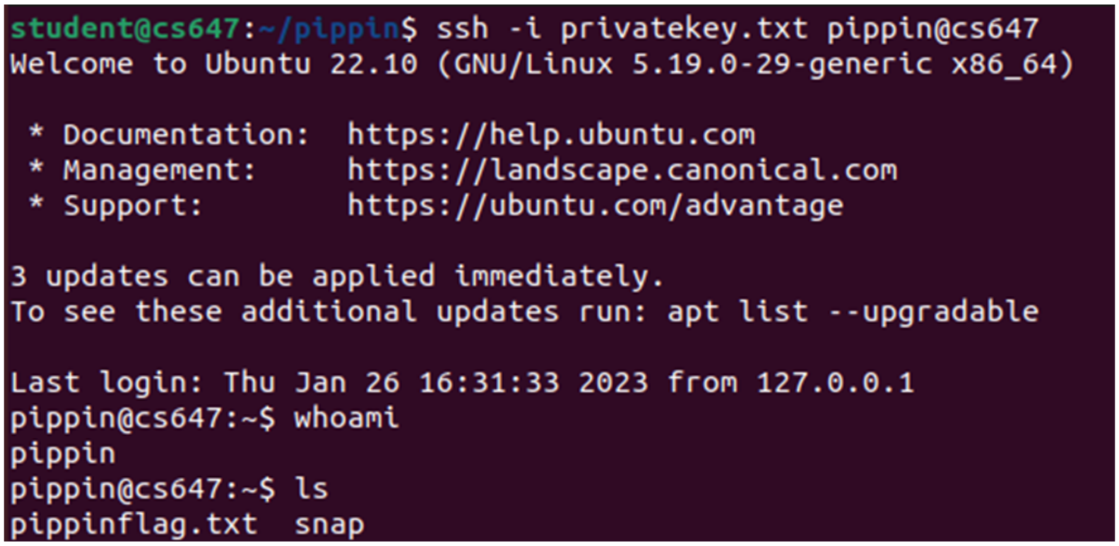
I changed the file permissions so that the key file had the correct permissions i.e., the key should be accessed only by the owner. So I used the command "`chmod 600 privatekey.txt`". This will allow only the owner to make any changes to the file, whereas other users will not have access to it. I was able to check the permissions of the file using "`ls -l privatekey.txt`" as shown in the screenshot 5.



```
student@cs647:~/pippin$ ls -l privatekey.txt
-rw-rw-r-- 1 student student 2590 Jan 26 15:50 privatekey.txt
student@cs647:~/pippin$ chmod 600 privatekey.txt
student@cs647:~/pippin$ ls -l privatekey.txt
-rw------- 1 student student 2590 Jan 26 15:50 privatekey.txt
```

*Screenshot 5: Checking and changing file permissions.*

After changing the permissions of the key, I used the command "`ssh -i privatekey.txt pippin@cs647`" to start the connection. Here, `ssh` is the secure shell protocol used to make secure network connections over an unsecure network. `-i` flag is used to identify the private key for the authentication, and '`-i privatekey.txt`' means privatekey.txt will be identified as the key. `pippin@cs647` means we were going to access the user pippin whose host is cs647.



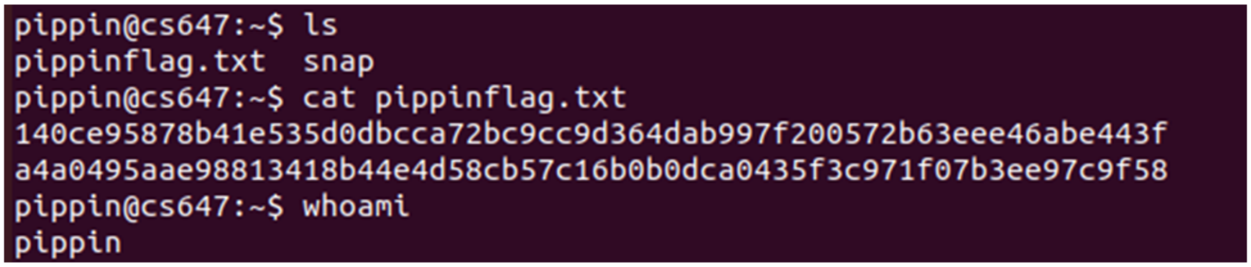
```
student@cs647:~/pippin$ ssh -i privatekey.txt pippin@cs647
Welcome to Ubuntu 22.10 (GNU/Linux 5.19.0-29-generic x86_64)

 * 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: Thu Jan 26 16:31:33 2023 from 127.0.0.1
pippin@cs647:~$ whoami
pippin
pippin@cs647:~$ ls
pippinflag.txt  snap
```

*Screenshot 6: Access to pippin's account.*

From screenshot 6, I was able to infer that the exploit was working.

## Findings

After logging into the pippin account I was able to retrieve the pippinflag.txt file. The file contained the following information as shown in the screenshot 7.



```
pippin@cs647:~$ ls
pippinflag.txt  snap
pippin@cs647:~$ cat pippinflag.txt
140ce95878b41e535d0dbcca72bc9cc9d364dab997f200572b63eee46abe443f
a4a0495aae98813418b44e4d58cb57c16b0b0dca0435f3c971f07b3ee97c9f58
pippin@cs647:~$ whoami
pippin
```

*Screenshot 7: Contents of pippinflag.txt as user pippin.*

Contents of pippinflag.txt:

140ce95878b41e535d0dbcca72bc9cc9d364dab997f200572b63eee46abe443f

a4a0495aae98813418b44e4d58cb57c16b0b0dca0435f3c971f07b3ee97c9f58