Akash Nagabandhi

29th January 2023

CS 647 852

Prof. Martin

Pippin Assignment

Executive Summary

This task involves analyzing the file "/home/student/pippin/SaveForPippin.zip" to gain access to the Pippin account and retrieve the file "pippinflag.txt." The file is a text file that has been repeatedly compressed using various programs, such as zip, bzip2, tar, gz, and xz. Pippin attempts to conceal the compression method by renaming the file extension, a security technique known as "security through obscurity," which is not a reliable method and can be easily bypassed. The final step in Pippin's security is to conceal his private key within a digital copy of "The Lord of the Rings." Once the private key is obtained, it is easy to access Pippin's account using SSH.

Vulnerabilities Identified

Security through obscurity is a technique in which the security of a system assumes that an attacker does not have enough knowledge or resources to find and exploit vulnerabilities in the system. It relies on keeping the details of the system's design and implementation secret, rather than on publicly disclosed, well-vetted, and well-tested methods. In this assignment, Pippin uses a digital copy of “The lord of the rings” to hide his private key which is gives its holder entry to pippin’s account.

Recommendations

Security through obscurity is a flawed security strategy because it relies on keeping the details of a system's design and implementation secret, rather than on publicly disclosed, well-vetted, and well-tested methods. An attacker targeting Pippin would likely try to find and use every piece of information they can obtain, making STO ineffective. Additionally, if an attacker does discover a vulnerability, there is no way for the system's defenders to know about it and therefore no way to fix it. It is more effective to use encryption on the private key to hide it, or to carry it on a USB drive. Leaving the private key in another account is not a secure approach, and a strong password would be a better option for logging in.

Assumptions

The private key is hidden within the SaveForPippin.zip file.

Pippin's account is set up to use a private key.

Steps to Reproduce the Attack

The Exploit requires 5 main commands, **'file'**, '**chmod'**, '**ssh'**, '**mv'** and decompression commands for all different compressors used.

file command is used to get the type of the file.

chmod is used to change permissions of a file.

ssh command is used to use a secure shell portal to login to a different system or account.

Decompressor commands used:

Types of compressors used and their decompressor commands:

zip : "**unzip** FileName"

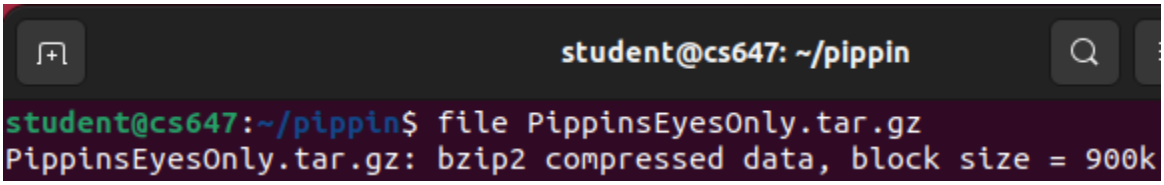
bzip2 : "**bunzip2** FileName"

tar : "**tar** -xvf FileName", the flags -xvf mean extract, verbose and filename.

gz : **gunzip** FileName

xz : **unxz** FileName

1. The file SaveForPippin.zip, uses a regular zip compression, which can be decompressed using its decompressor command.
2. The file PippinsEyesOnly.tar.gz is extracted from SaveForPippin.zip. As pippin tries to achieve security through obscurity, using the **file** command reveals the try type of the file.



3. There are many layers of compression on the file PippinsEyesOnly using the file command to find the compressor used and decompressing the file ends with a text file.
    - When decompressing gz its imperative that the file be renamed with the extension ending in .gz. This can be done using the “mv” command.

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

4. The contents of the of the text file PippinsEyesOnly contains a digital copy of “The Lord of the Rings”, in which Pippin’s SSH Private key is hidden. To open the file, **open** command can be used. This opens the file in a text editor.

```
student@cs647:~/pippin$ open PippinsEyesOnly
student@cs647:~/pippin$
Open                                PippinsEyesOnly
                                    ~/pippin

The Lord of the Rings
BY
J.R.R. Tolkien

Three Rings for the Elven-kings under the sky,
Seven for the Dwarf-lords in their halls of stone, Nine for Mortal Men doomed to die,
One for the Dark Lord on his dark throne In the Land of Mordor where the Shadows lie.
One Ring to rule them all, One Ring to .nd them,
One Ring to bring them all and in the darkness bind them In the Land of Mordor where the Shadows lie.
CONTENTS
J.R.R. TOLKIEN
NOTE
ON
THE
TEXT
NOTE
ON
THE
```

5. Using the find function in the text editor, to find: SSH, the SSH Private key can be found easily.

```
Nay! The riders are little more than .ve leagues distant, said Legolas.
Five leagues or one, said Gimli, we cannot escape them in this bare land. Shall we wait fo
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAqnm2fa9DBip6eZG9MV5OwK6bhsP49ZkD/mQiKaFGxmGXPQTDIalY
KCLpJb2btNfoV4qCFllkN3P0pxgmH1xblHqH+fZR9MNwDVVWINrKFCENark+av2U5FyGhh
tB/NxiTDHb0jkJLQrJ/tDpJrMDAP/po84Y/vLunRPZalovEV3OFtVS1L19xylsaylYE0ed
Ns/dDFzuHPo6EiRCqsIS05zoo3QLt/61Y1vqn0UUdf5xe0JfothsQn3qIqWy5Dnb1f6Kcq
PbCvT2xganWOpgL0O0Lv4uObGI63KkXFv+Vh8h2CIJl/NrH6aAvih/hJ3urTdhq2qIv/BB
SSH
0 of 18
```

6. The **touch** command can be used to create a new text file in which the private key can be stored and used to SSH. This can be done using the **open** command to open the new file in a text editor and simply copy pasting the Private key to the new text file.
7. To use an SSH private key, it is required to change the permissions of the file, so that only the owner of the key can read/write. This can be done using the command **chmod 600.** This

command sets permissions so that, User/owner can read, can write, and can't execute. Group can't read, can't write, and can't execute. Others can't read, can't write, and can't execute.

8. Finally, to gain entry to pippins account the **ssh** command with the flag **-i** as such, can be used:

   ssh -i PrivateKeyFile pippin@cs647

Findings

Once logged in as the user pippin, I was able to retrieve the file pippinflag.txt. Also shown in screenshot 1, the file contained the following contents: