5.2 Solutions and Guided Walkthrough

5.2.1 Solutions

1. Flag 1 can be found in the `/etc/shadow` file. The flag is: **encryptedpasswordsarekeptin/etc/shadow**. Navigate to a directory by using the `cd` command. Ex: `$ cd /etc/`. To view the contents of a file, use the `cat` command. Ex: `$ cat /etc/shadow`.

2. Flag 2 can be found in `/bin/weirdfile`. The flag is: **thingsarenotalwaysastheyappear**. In order to list all the files in the current directory (folder), use the `ls` command. Ex: `$ ls /bin/`. .

3. Flag 3 can be found in the `/sbin` directory. There are four files named **tilapia, salmon, bass, and hering** each containing a part of the flag. The flag is: **systembinariesaren'tfishy**. Commands in Linux can be run in sequence by separating each command using the semicolon (;) character. Ex: `$ cat tilapia ; cat salmon ; cat bass ; cat hering`.

4. Flag 4 can be found in the `/dev` directory. The flag is: **hugepages**.

5. Flag 5 can be found in the `/proc` directory. In the file `partitions`, you will find a partition sda2 with a number of blocks. The flag is whatever the number of blocks in sda2 is. **Note: Your machine may not have an sda2 partition.**

6. Flag 6 can be found in the `/var/backups` directory. In the file `apt.extended_states.0`, there are three lines commented out which contain the flag. The flag is: **itsalwaysgoodtokeeparecordofwhatversionswereinstalled**

7. Flag 7 can be found in the `/tmp` directory. Well, it would be if not for the fact that the /tmp directory is flushed regularly (hence the name). For this challenge, give the student the flag when they have identified why there isn not a flag there. The flag for this task will be: **tempfilesareremoved**.

8. Flag 8 can be found in the `/usr/games/` directory. In this directory, there is a hidden directory titled `.spaceinvaders`, inside is a file containing the flag. The flag is: **therearenogamesonthismachine!**. **Note: Your machine may have other games installed in this folder. If so, laugh about the inaccuracy of the flag**. Hidden files can be difficult to find. Using the normal `ls` command does not display these files. Using the `-a` option, `ls` will also display hidden files. Ex: `$ ls -a /usr/games/`.

9. Flag 9 can be found in the `/lib/ufw` directory. There is a file in this folder containing the flag. The flag is: **ufwissuitedforhostbasedfirewalls**.

10. Flag 10 can be found in the `/media` directory. Here there is a file containing a cipher text. The key used to decrypt the cipher text in a vigenere cipher is in the file name. The flag is: **thisiswhereusbdirvesappear**.

5.2.2 Guided Walkthrough

In order to complete the challenges in this laboratory exercise, see the steps in this guided walkthrough.

Most Linux-based OSs have the option for a terminal to be opened using the **Ctrl + T** hotkey. Additionally, if the OS has a GUI, the terminal is an application which can be opened by finding the terminal in the application viewer and clicking it. You will need to open a terminal to complete each of the challenges in this exercise.

In Linux, files have paths within the file system. The root location in the file system, the location from which all other file paths originate. In the Linux file system, the root location is indicated with the forward slash **(/)** character. The **/etc** directory is one of the directories one level deep from the root directory. One of the files in the **/etc** directory is the **shadow** file. This file contains encrypted formats of the passwords for users on the machine.

In order to navigate to directories in the Linux terminal, use the command **cd**. Follow the command with the file path of the target directory. For example, consider the file path: **/home/Desktop/Misc/random.txt**. In order to access the file, **random.txt**, one can first navigate to the directory containing the file, in this case, the **Misc** directory. To accomplish this, use the following command:

```
$ cd /home/Desktop/Misc
```

From there, one can view the contents of the file using the **cat** command. While in the **Misc** directory, one can view the contents of the **random.txt** file by running the command:

```
$ cat random.txt
```

Additionally, one can use the **cat** command with the file path rather than navigating to the directory first. For example, one could run the following command to display the contents of the **random.txt** file:

```
$ cat /home/Desktop/Misc/random.txt
```

This laboratory exercise has the flags hidden as contents of the files. In order to discover the flags, display the contents of the files.

Challenge 1

Use the command:

```
$ cat /etc/shadow
```

One of the lines in the file has the following contents:

"flag:$encryptedpasswordsarekeptin/etc/shadow".

Challenge 2

Use the command:

```
$ cat /bin/weirdfile
```

The contents of this file are: *"thingsarenotalwaysastheyappear"*.

Challenge 3

The flag for this challenge is spread across four files in the **/sbin** directory. These files are all fish themed, namely, *tilapia, salmon, bass,* and *hering.* By displaying the contents of these files, the flag is revealed. One can take advantage of the ability to chain commands to display the contents of all four files at one time. Use the command:

```
$ cat tilapia ; cat salmon ; cat bass ; cat hering
```

The flag revealed is: *"systembinariesaren'tfishy"*.

Challenge 4

The flag for this challenge is the name of the file where larger page sizes are handled, in the directory which contains information on device files. The directory in question is the **/dev** directory. The file is **hugepages**. The flag is the file name: *hugepages*

Challenge 5

The flag for this file is kept in the directory where process information is typically kept. In this case, the directory in question is the **/proc** directory. There is a specific file in this directory, the **partitions** file, which contains information on the partitions of the file system. The number of blocks in the **sda2** partition is the flag for this challenge.

Challenge 6

The flag for this challenge is contained in the directory where backups are kept, namely: **/var/backups**. The specific file in question is titled **apt.extended_states.0**. Display the contents of the file by using the command:

```
$ cat /var/backups/apt.extended_states.0
```

This will reveal the flag: *itsalwaysgoodtokeeparecordofwhatversionswereinstalled.*

Challenge 7

The flag for this challenge is actually missing. The directory which would contain the flag is where temporary files are kept, namely, the **/tmp** directory. The flag, which was stored there is removed because temporary files are deleted regularly. Rather, simply use the flag *tempfilesareremoved* for this challenge.

Challenge 8

The flag for this challenge is kept in a hidden file. Files can be listed in the Linux terminal using the command **ls**. However, files which are hidden (prefaced with the **.** symbol, ex: .hiddenfile.txt), will not be displayed using the basic **ls** command. In order to display hidden files, use the **-a** option with the **ls** command. Navigate to the directory where games are located, namely: **/usr/games**. This can be done using the command:

```
$ cd /usr/games
```

From there list all files using the command:

```
ls -a
```

This will display a file **.spaceinvaders**. Displaying its contents using the **cat** command will reveal the flag: *therearenogamesonthismachine!*

Challenge 9

The flag for this file can be found in the **/lib/ufw** directory. Navigate to the directory using the **cd** command:

```
$ cd /lib/ufw
```

The flag is kept in one of the files. The flag is *ufwissuitedforhostbasedfirewalls*.

Challenge 10

The flag for this challenge exists in the directory where removable devices are kept, namely **/media**. There is a file in this directory named **flag**. The contents are a ciphertext, meaning it is encrypted text. The type of cipher used is known as a vigenere cipher. The key for the encryption and decryption is the name of the file, **flag**. By decrypting the ciphertext with the key, the flag is revealed to be *thisiswhereusbdrivesappear*.