Bandit – Stage by Stage explanation

Level 0

All you have to do here is ssh onto the bandit server. This can be done with the command `$ ssh -p 2220 bandit0@bandit.labs.overthewire.org` and then entering the password `bandit0`

Level 1

The password for the next level is stored in a file on the desktop named 'readme'.

This can be revealed with the `ls` command, and read with `cat readme`.

The password for bandit1 is `boJ9jbbUNNfktd78OOpsqOltutMc3MY1`

Level 2

The password here is stored in a file called '-'

This can be revealed with the `ls` command, but running `cat -` confuses the system, as `-` normally denotes a flag. We can get around this by using the complete file path, './-'. This gives us the command `cat ./-`

The password for bandit2 is `CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9`

Level 3

The password for the next level is stored in a file called spaces in this filename located in the home directory

This cannot be accessed by simply running `cat spaces in this file name`, as the system will register this as four separate files. Instead, we can either use the escape character, '', in front of the spaces, or specify the file name in quotation marks. This gives us either `cat spaces\ in\ this\ filename` or `cat "spaces in this file name"`

The password for bandit3 is `UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK`

Level 4

The password for the next level is stored in a hidden file in the inhere directory.

We can change into this directory using `cd inhere`, and then reveal the hidden file, which is called '.hidden'. We can then read the contents of this file with the command `cat .hidden`.

The password for bandit4 is `pIwrPrtPN36QITSp3EQaw936yaFoFgAB`

Level 5

The password for the next level is stored in the only human-readable file in the inhere directory. Tip: if your terminal is messed up, try the "reset" command.

Again, we can change to the inhere directory using `cd inhere`. Running `ls` then reveals that there are ten files in this directory. As we know that the password is contained in a human readable file, we need to somehow filter the files by filetype. This can be done with the command `find . -type f | xargs file`. This works by finding all the files in the current directory, and passing these as an argument into the file command, which then lists them by type. Doing so reveals to us that 9 of the 10 files are of type 'data', but one is of type 'ASCII text'. Therefore, the password must be in this file.

This works given the relatively small number of files in this directory, but what if it were larger? We could extend this command by piping the output into `grep text`, giving us a complete command of

```
find . -type f | xargs file | grep text
```

This would return only the file marked as ASCII text, omitting all others.

The password for bandit5 is koReBOKuIDDepwhWk7jZC0RTdopnAYKh