**OverTheWire Bandit - Level 4 to Level 5 Writeup**

**Introduction**: This writeup documents my experience solving Levels 4 to 5 of the OverTheWire Bandit challenge, a CTF-style game focused on learning about security concepts.

**Author**: Misha Jain

**Date**: October 19, 2023

**Tools Used:**

Terminal (SSH client)

**Challenge Description:**

Level 4 to Level 5 of Bandit involves connecting to a remote server via SSH and retrieving the flag located in the home directory of the server. These levels require basic shell commands and handling of hidden files.

**Enumeration:**

For Level 4, we need to connect to the server using the credentials we obtained in Level 3. This will reveal a password for Level 5.

**Exploitation - Level 4:**

To connect to the server for Level 4 using SSH, we use the provided credentials:

ssh bandit4@bandit.labs.overthewire.org -p 2220

Use the password obtained from Level 3, which is 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe to gain access.



**Password Retrieval - Level 4:**

The password for Level 5 is stored in the only human-readable file in the inhere directory. We can use the cd command to access the contents of the directory and the ls command to list the files in that directory. Then we can use the find command to display the filetypes.

cd inhere/

ls -alps

find . -type f | xargs file

‘find . -type f’ uses the find command to search for files within the current directory (.) and its subdirectories. The -type f option specifies that it should only search for regular files (not directories or other types of files).

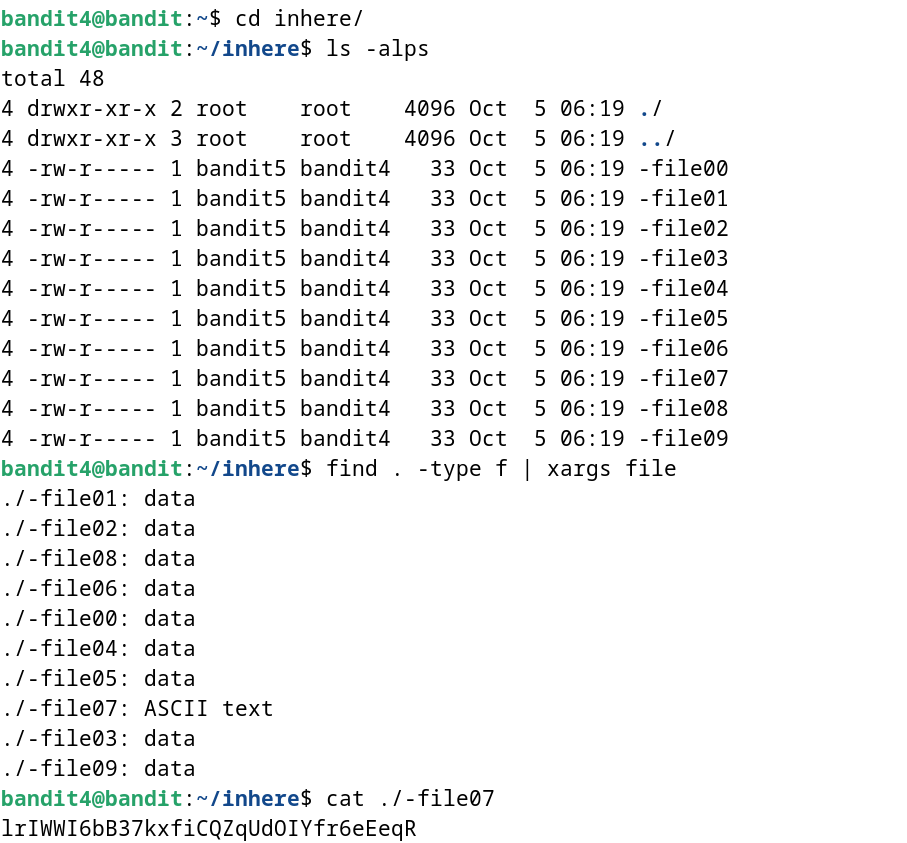
‘|’ is a pipe symbol, and it is used to take the output of the find command and pass it as input to the next command, which is xargs.

The xargs command reads the list of file paths provided by find via the pipe and applies the file command to each of these files. The file command is used to determine and display information about the type of file. For example, it will identify whether a file is a text file, an image, an executable binary, and so on.

After using the find command, we get to know that -file07 is the only human readable file. Hence, we use the cat command to access the contents of -file07.

cat ./-file07

These commands will display the Level 5 password.



**Password – Level 5:**

The password for Level 5 is: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

**Exploitation – Level 5:**

Now that we have the Level 5 password, we can connect to the server for Level 5 using SSH:

ssh bandit5@bandit.labs.overthewire.org -p 2220

Use the Level 5 password to gain access.



**Lessons Learned:** Level 4 to 5 reinforced the use of the cd command for directory navigation, the ls command for listing directory contents, and the cat command for reading file contents.

Level 5 introduced us to the find command for searching the filesystem for specific files.

**Conclusion:**

Levels 4 to 5 of the OverTheWire Bandit challenge continue to build on shell command knowledge while introducing new challenges. These levels are suitable for beginners to learn more about directory navigation, file search, and manipulation.