Writeup for Bandit Level 0—>5

Title: Bandit Level 0→1 - Logging into the Game Server

Introduction

Bandit is a wargame by OverTheWire that teaches Linux commands and basic security concepts. Level 0 starts you off with a simple goal: logging into the game server through SSH. This writeup shows you how to complete Level 0 and find the password for Level 1.

Level Goal

- Log into the game server using SSH.
- Host: `bandit.labs.overthewire.org`
- Port: `2220`
- Username: `bandit0`
- Password: `bandit0`

Methodology

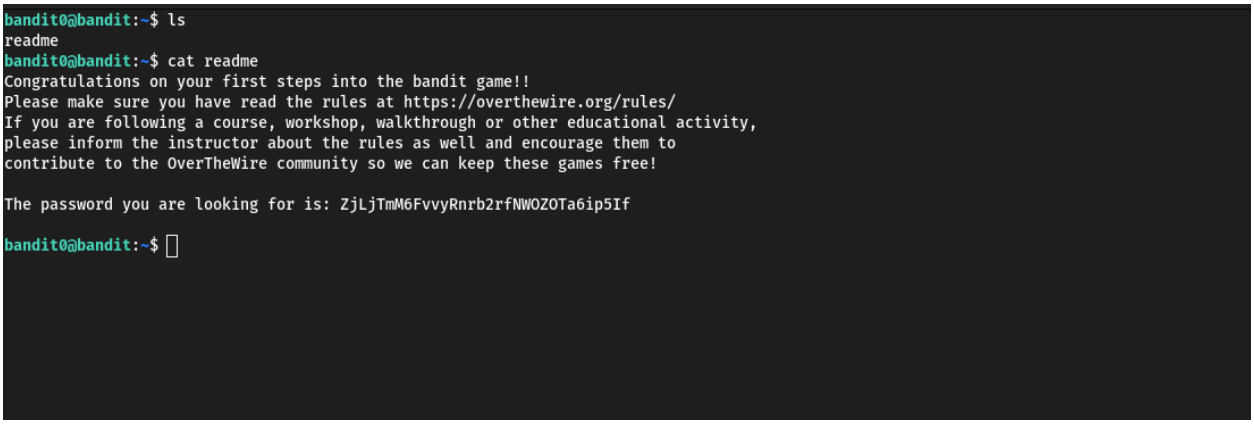
1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command to connect to the server.
    - The command used is:

      `ssh bandit0@bandit.labs.overthewire.org -p 2220`
    - When prompted, enter the password: `bandit0`.

2. **Access the Server**:
    - After successfully logging in, you will be greeted with a welcome message from the OverTheWire server.

Retrieve the Password for Level 1:

- Once logged in, list the files in the home directory using the `ls` command.
- You will find a file named `readme`.
- Use the `cat` command to display the contents of the `readme` file, which contains the password for Level 1.



Findings/Results

- The password for Level 1 is: `ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If`

Discussion/Analysis

- Level 0 is a straightforward introduction to the Bandit wargame. The primary objective is to familiarize users with the SSH protocol and basic Linux commands like `ls` and `cat`.
- The password for the next level is stored in a file within the home directory, emphasizing the importance of file navigation and reading file contents in Linux.

Conclusion

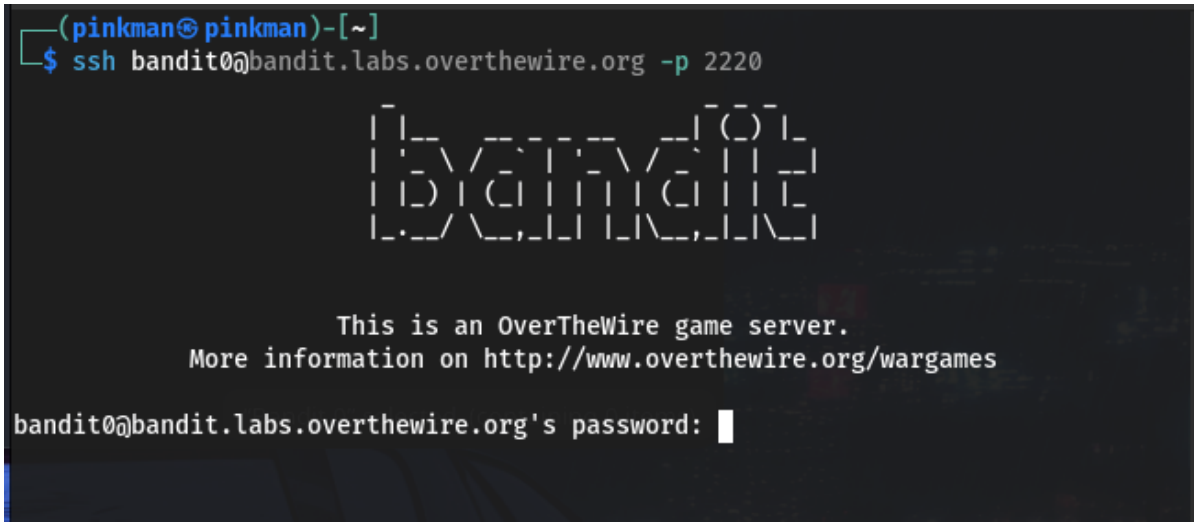
- Successfully logged into the Bandit game server using SSH.
- Retrieved the password for Level 1 by reading the contents of the `readme` file.
- This level serves as a good starting point for beginners to get comfortable with basic Linux commands and the game's interface.

Commands Used

- `ssh bandit0@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `cat readme`: Display the contents of the `readme` file.

Screenshots

1. **SSH Connection**:



2. **Retrieving the Password**:

Writeup for Bandit Level 1 → Level 2

Title: Bandit Level 1 - Retrieving the Password from a File Named `-`

Introduction

Bandit Level 1 introduces a slightly more challenging task compared to Level 0. The goal is to retrieve the password for Level 2, which is stored in a file named `-` located in the home directory. This writeup documents the steps taken to complete Level 1 and retrieve the password for Level 2.

Methodology

1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command to connect to the server.
    - The command used is:
      `ssh bandit1@bandit.labs.overthewire.org -p 2220`
    - When prompted, enter the password retrieved from Level 1:
      `ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If`.

1. **Access the Server**:

- After successfully logging in, you will be in the home directory of the `bandit1` user.

2. **Locate the File Named** :
    - List the files in the home directory using the `ls` command.
    - You will see a file named .
3. **Retrieve the Password for Level 2**:

- Use the `cat` command to display the contents of the file named .
- Since is a special character in the shell, you need to use a specific syntax to read the file:

  `cat < -`

  The password for Level 2 will be displayed.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat < -
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Findings/Results

- The password for Level 2 is: `263JGJPfgU6LtdEvgfWU1XP5yac29mFx`

Discussion/Analysis

- Level 1 introduces a common challenge in Linux: dealing with files that have special characters in their names. The file named requires a specific approach to read its contents, as the character is often interpreted as a command-line option.
- This level emphasizes the importance of understanding how to handle special characters in filenames and the use of input redirection (`<`) to read such files.

Conclusion

- Successfully logged into the Bandit game server as `bandit1`.

- Retrieved the password for Level 2 by reading the contents of the file named .
- This level reinforces the importance of understanding shell syntax and handling special characters in filenames.

Commands Used

- `ssh bandit1@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `cat < -`: Display the contents of the file named .

Screenshots

1. **SSH Connection:**

2. **Retrieving the Password**:

Writeup for Bandit Level 2 → Level 3

Title: Bandit Level 2 - Retrieving the Password from a File with Spaces in the Filename

Introduction

Bandit Level 2 presents a challenge involving a file with spaces in its name. The goal is to retrieve the password for Level 3, which is stored in a file named `spaces in this filename` located in the home directory. This writeup documents the steps taken to complete Level 2 and retrieve the password for Level 3.

Level Goal

- The password for the next level is stored in a file named `spaces in this filename` located in the home directory.

Methodology

1. **Connect to the Server Using SSH**:
    - Open a terminal and use the `ssh` command to connect to the server.
    - The command used is:
      `ssh bandit2@bandit.labs.overthewire.org -p 2220`
    - When prompted, enter the password retrieved from Level 1:
      `263JGJPfgU6LtdEvgfWU1XP5yac29mFx`.

2. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit2` user.
3. **Locate the File with Spaces in the Filename**:
    - List the files in the home directory using the `ls` command.
    - You will see a file named `spaces in this filename`.
4. **Retrieve the Password for Level 3**:
    - Use the `cat` command to display the contents of the file.
    - Since the filename contains spaces, you need to enclose the filename in quotes to read it properly:

      `cat "spaces in this filename"`
    - The password for Level 3 will be displayed.

Findings/Results

- The password for Level 3 is: `MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx`

Discussion/Analysis

- Level 2 introduces the challenge of handling filenames with spaces. In Linux, filenames with spaces must be enclosed in quotes or escaped using backslashes to be interpreted correctly by the shell.
- This level emphasizes the importance of understanding how to handle filenames with special characters, such as spaces, in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit2`.
- Retrieved the password for Level 3 by reading the contents of the file named `spaces in this filename`.
- This level reinforces the importance of proper handling of filenames with spaces in Linux.

Commands Used

- `ssh bandit2@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `cat "spaces in this filename"`: Display the contents of the file named `spaces in this filename`.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:

Writeup for Bandit Level 3 → Level 4

Title: Bandit Level 3 - Retrieving the Password from a Hidden File

Introduction

Bandit Level 3 introduces the concept of hidden files in Linux. The goal is to retrieve the password for Level 4, which is stored in a hidden file within the `inhere` directory. This writeup documents the steps taken to complete Level 3 and retrieve the password for Level 4.

Level Goal

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

Methodology

1. **Connect to the Server Using SSH**:
   - Open a terminal and use the `ssh` command to connect to the server.
   - The command used is:

     `ssh` `bandit3@bandit.labs.overthewire.org` `-p 2220`
   - When prompted, enter the password retrieved from Level 2:

     `MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx`.

2. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit3` user.
3. **Navigate to the `inhere` Directory**:
    - List the contents of the home directory using the `ls` command.
    - You will see a directory named `inhere`.
    - Change to the `inhere` directory using the `cd` command: `cd inhere`
4. **Locate the Hidden File**:
    - List all files in the `inhere` directory, including hidden files, using the `ls -la` command.
    - You will see a hidden file named `.Hiding-From-You`.
5. **Retrieve the Password for Level 4**:
    - Use the `cat` command to display the contents of the hidden file: `cat .Hiding-From-You`
    - The password for Level 4 will be displayed.

Findings/Results

- The password for Level 4 is: `2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ` .

Discussion/Analysis

- Level 3 introduces the concept of hidden files in Linux, which are files that start with a dot (`.`). These files are not displayed by default when using the `ls` command without the `a` option.
- This level emphasizes the importance of understanding how to list and access hidden files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit3`.
- Retrieved the password for Level 4 by reading the contents of the hidden file `.Hiding-From-You` in the `inhere` directory.
- This level reinforces the importance of being familiar with hidden files and the `ls -la` command in Linux.

Commands Used

- `ssh bandit3@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `cd inhere`: Change to the `inhere` directory.
- `ls -la`: List all files, including hidden files, in the current directory.
- `cat .Hiding-From-You`: Display the contents of the hidden file.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:

Writeup for Bandit Level 4 → Level 5

Title: Bandit Level 4 - Finding the Human-Readable File

Introduction

Bandit Level 4 challenges users to identify the only human-readable file among a set of files in the `inhere` directory. The goal is to retrieve the password for Level 5 from this file. This writeup documents the steps taken to complete Level 4 and retrieve the password for Level 5.

Level Goal

- The password for the next level is stored in the only human-readable file in the `inhere` directory.

Methodology

1. **Connect to the Server Using SSH**:
   - Open a terminal and use the `ssh` command to connect to the server.
   - The command used is:

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

- When prompted, enter the password retrieved from Level 3:

  `2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ`

2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit4` user.
3. **Navigate to the `inhere` Directory**:
   - List the contents of the home directory using the `ls` command.
   - You will see a directory named `inhere`.
   - Change to the `inhere` directory using the `cd` command:

     `cd inhere` .
4. **Identify the Human-Readable File**:

- List the contents of the `inhere` directory using the `ls` command.
- You will see several files named `file00` to `file09`.
- Use the `file` command to determine the type of each file:

  `file -- -file{00..09}` .
- The output will indicate that `-file07` is an ASCII text file, which is human-readable.

5. **Retrieve the Password for Level 5**:

- Use the `cat` command to display the contents of the human-readable file:

  `cat -- -file07`.

- The password for Level 5 will be displayed.

Findings/Results

- The password for Level 5 is: `4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw` .

Discussion/Analysis

- Level 4 introduces the challenge of identifying a human-readable file among a set of files with different formats. The `file` command is crucial for determining the type of each file.
- This level emphasizes the importance of understanding file types and using the appropriate commands to inspect and read files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit4`.
- Retrieved the password for Level 5 by identifying and reading the human-readable file `file07` in the `inhere` directory.
- This level reinforces the importance of using the `file` command to inspect file types and the `cat` command to read file contents.

Commands Used

- `ssh bandit4@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `cd inhere`: Change to the `inhere` directory.
- `file -- -file[00..09]`: Determine the type of each file in the `inhere` directory.
- `cat -- -file07`: Display the contents of the human-readable file.

Screenshots

1. **SSH Connection**:

2. **Identifying the Human-Readable File**:

3. **Retrieving the Password**:


bandit4@bandit:~/inhere$ cat -- -file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$