Bandit_6→10

Writeup for Bandit Level 5 → Level 6

Title: Bandit Level 5 - Finding the Password File with Specific Properties

---

Introduction

Bandit Level 5 requires users to locate a file within the `inhere` directory that meets specific criteria: it must be human-readable, 1033 bytes in size, and not executable. This writeup documents the steps taken to complete Level 5 and retrieve the password for Level 6.

Level Goal

- The password for the next level is stored in a file somewhere under the `inhere` directory with the following properties:
  - Human-readable
  - 1033 bytes in size
  - Not executable

Methodology

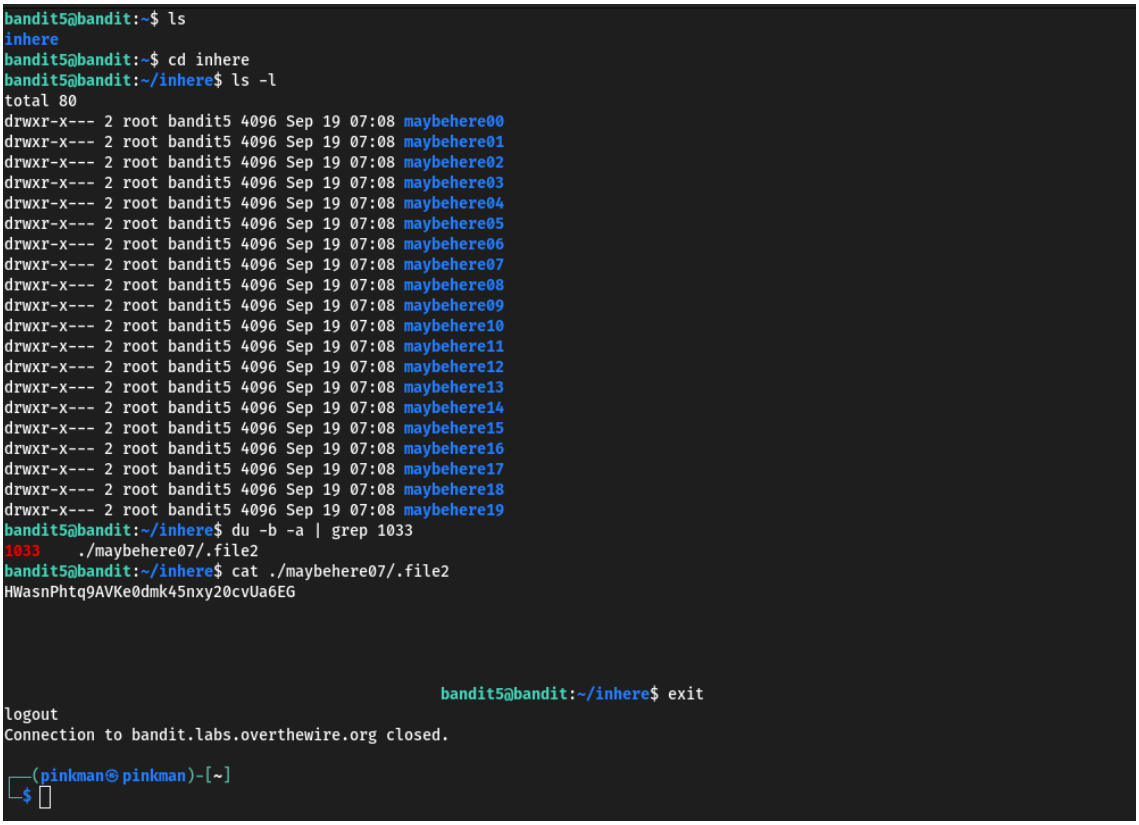
1. **Connect to the Server Using SSH**:
   - Open a terminal and use the `ssh` command to connect to the server.
   - The command used is:
     `ssh bandit5@bandit.labs.overthewire.org -p 2220`
   - When prompted, enter the password retrieved from Level 4:
     `4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw`.

2. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit5` 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 File with Specific Properties**:
    - Use the `du` command to find files that are exactly 1033 bytes in size:

      `du -b -a | grep 1033`
    - The output will indicate the path to the file that meets the size requirement.
5. **Retrieve the Password for Level 6**:
    - Use the `cat` command to display the contents of the identified file:

      `cat ./maybehere07/.file2` .
    - The password for Level 6 will be displayed.



Findings/Results

- The password for Level 6 is: `HWasnPhtq9AVKe0dmk45nxy20cvUa6EG` .

Discussion/Analysis

- Level 5 introduces the challenge of locating a file with specific properties within a directory structure. The `du` command is used to find files of a particular size, and the `grep` command helps filter the results.
- This level emphasizes the importance of understanding file properties and using commands like `du` and `grep` to efficiently locate files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit5`.
- Retrieved the password for Level 6 by locating and reading the file `./maybehere07/.file2` in the `inhere` directory.

- This level reinforces the importance of using commands to filter and locate files based on specific properties.

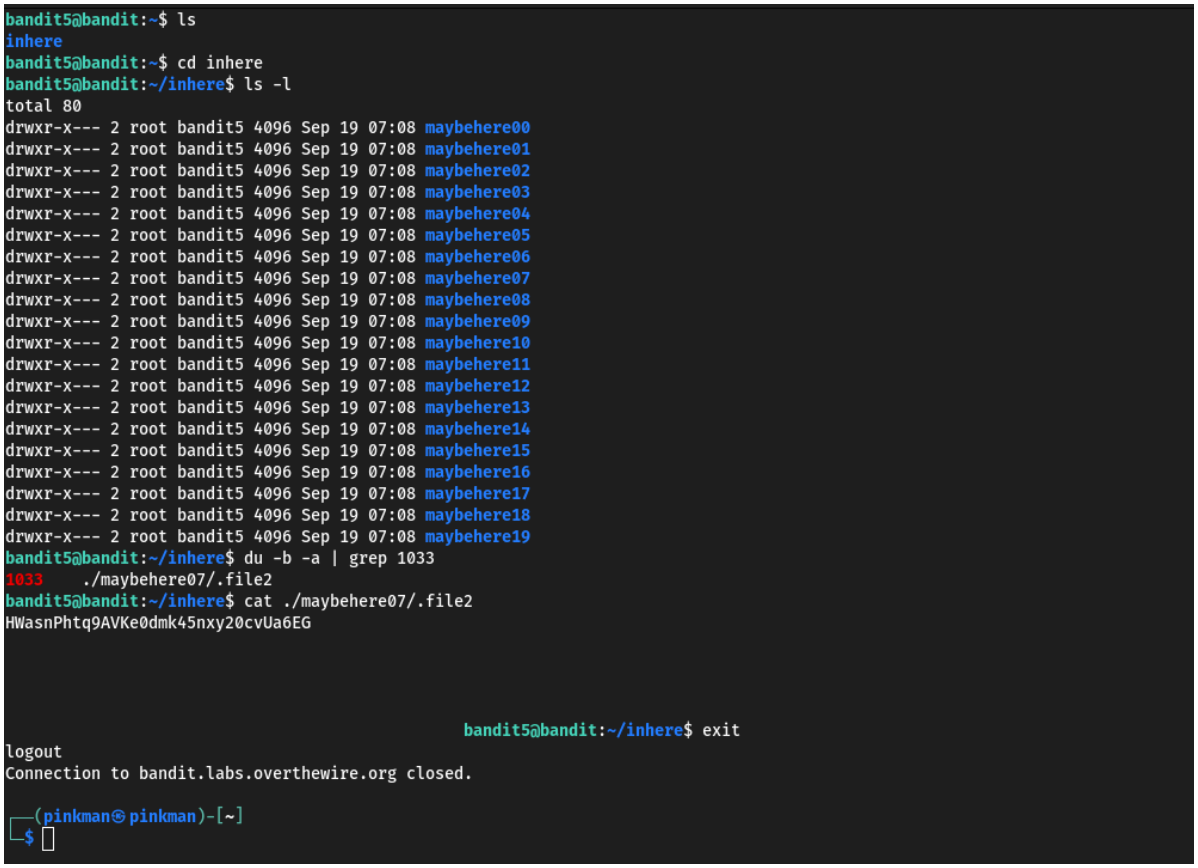
Commands Used

- `ssh bandit5@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.
- `du -b -a | grep 1033`: Find files that are exactly 1033 bytes in size.
- `cat ./maybehere07/.file2`: Display the contents of the identified file.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:



Writeup for Bandit Level 6 → Level 7

Title: Bandit Level 6 - Finding the Password File with Specific Ownership and Size

Introduction

Bandit Level 6 requires users to locate a file on the server that meets specific criteria: it must be owned by user `bandit7`, owned by group `bandit6`, and be exactly 33 bytes in size. This writeup documents the steps taken to complete Level 6 and retrieve the password for Level 7.

Level Goal

- The password for the next level is stored somewhere on the server and has the following properties:
  - Owned by user `bandit7`
  - Owned by group `bandit6`
  - 33 bytes in size

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` `bandit6@bandit.labs.overthewire.org` `-p 2220`
   - When prompted, enter the password retrieved from Level 5:

     `HWasnPhtq9AVKe0dmk45nxy20cvUa6E6`.

2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit6` user.
3. **Locate the File with Specific Properties**:
   - Use the `find` command to search for a file that meets the specified criteria:

     `find / -type f -user bandit7 -group bandit6 -size 33c 2> /dev/null`
   - The `2> /dev/null` part of the command suppresses error messages, making the output cleaner.
   - The output will indicate the path to the file that meets the criteria.
4. **Retrieve the Password for Level 7**:
   - Use the `cat` command to display the contents of the identified file:

     `cat /var/lib/dpkg/info/bandit7.password` .
   - The password for Level 7 will be displayed.

Findings/Results

- The password for Level 7 is: `morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj`

Discussion/Analysis

- Level 6 introduces the challenge of locating a file with specific ownership and size properties across the entire server. The `find` command is essential for searching files based on these criteria.
- This level emphasizes the importance of understanding file ownership, group permissions, and using the `find` command to efficiently locate files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit6`.
- Retrieved the password for Level 7 by locating and reading the file `/var/lib/dpkg/info/bandit7.password`.
- This level reinforces the importance of using the `find` command to search for files based on specific properties.

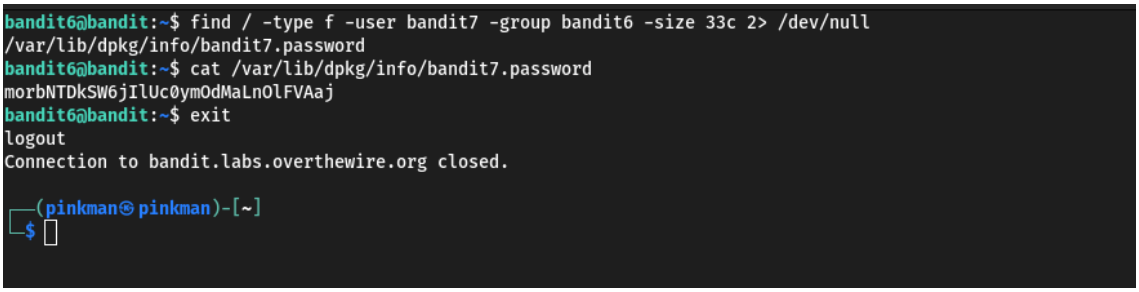
Commands Used

- `ssh bandit6@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `find / -type f -user bandit7 -group bandit6 -size 33c 2> /dev/null`: Find files owned by user `bandit7`, group `bandit6`, and exactly 33 bytes in size.
- `cat /var/lib/dpkg/info/bandit7.password`: Display the contents of the identified file.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:



Writeup for Bandit Level 7 → Level 8

Title: Bandit Level 7 - Finding the Password Next to the Word "millionth"

Introduction

Bandit Level 7 requires users to locate a password stored in a file named `data.txt`. The password is located next to the word "millionth". This writeup documents the steps taken to complete Level 7 and retrieve the password for Level 8.

Level Goal

- The password for the next level is stored in the file `data.txt` next to the word "millionth".

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 bandit7@bandit.labs.overthewire.org -p 2220`
   - When prompted, enter the password retrieved from Level 6: `morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj`.

2. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit7` user.
3. **Locate the `data.txt` File**:
    - List the contents of the home directory using the `ls` command.
    - You will see a file named `data.txt`.
4. **Retrieve the Password for Level 8**:
    - Use the `grep` command to search for the word "millionth" in the `data.txt` file:

      `grep millionth data.txt`
    - The password for Level 8 will be displayed next to the word "millionth".

Findings/Results

- The password for Level 8 is: `dfwvzFQi4mU0wfNbFOe9ROWSkMLg7eEc`

Discussion/Analysis

- Level 7 introduces the challenge of searching for specific text within a file. The `grep` command is essential for finding lines that match a given pattern.
- This level emphasizes the importance of using text processing tools like `grep` to efficiently locate information within files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit7`.
- Retrieved the password for Level 8 by searching for the word "millionth" in the `data.txt` file using the `grep` command.
- This level reinforces the importance of using text processing commands to find specific information within files.

Commands Used

- `ssh bandit7@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `grep millionth data.txt`: Search for the word "millionth" in the `data.txt` file.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:

Writeup for Bandit Level 8 → Level 9

Title: Bandit Level 8 - Finding the Unique Line in `data.txt`

Introduction

Bandit Level 8 requires users to locate a password stored in a file named `data.txt`. The password is the only line of text that occurs once in the file. This writeup documents the steps taken to complete Level 8 and retrieve the password for Level 9.

Level Goal

- The password for the next level is stored in the file `data.txt` and is the only line of text that occurs only once.

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 bandit8@bandit.labs.overthewire.org -p 2220`
   - When prompted, enter the password retrieved from Level 7: `dfwvzFQi4mU0wfNbFOe9ROWSkMLg7eEc`.
2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit8` user.
3. **Locate the `data.txt` File**:
   - List the contents of the home directory using the `ls` command.
   - You will see a file named `data.txt`.
4. **Retrieve the Password for Level 9**:
   - Use the `sort` and `uniq -u` commands to find the unique line in the `data.txt` file:

`sort data.txt | uniq -u`

- The `sort` command sorts the lines in the file, and `uniq -u` filters out lines that occur more than once, leaving only the unique line.
- The password for Level 9 will be displayed.

Findings/Results

- The password for Level 9 is: `4CKMh1JI91bUIZZPXDqGanal4xvAg0JM` .

Discussion/Analysis

- Level 8 introduces the challenge of identifying a unique line in a file. The combination of `sort` and `uniq -u` commands is essential for filtering out duplicate lines and finding the unique one.
- This level emphasizes the importance of using text processing tools like `sort` and `uniq` to efficiently manipulate and analyze text data in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit8` .
- Retrieved the password for Level 9 by identifying the unique line in the `data.txt` file using the `sort` and `uniq -u` commands.
- This level reinforces the importance of using text processing commands to find specific information within files.

Commands Used

- `ssh bandit8@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `sort data.txt | uniq -u`: Sort the lines in `data.txt` and filter out duplicates to find the unique line.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:

Writeup for Bandit Level 9 → Level 10

Title: Bandit Level 9 - Finding the Human-Readable String Preceded by '=' Characters

---

Introduction

Bandit Level 9 requires users to locate a password stored in a file named `data.txt`. The password is one of the few human-readable strings in the file and is preceded by several '=' characters. This writeup documents the steps taken to complete Level 9 and retrieve the password for Level 10.

Level Goal

- The password for the next level is stored in the file `data.txt` in one of the few human-readable strings, preceded by several '=' characters.

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 bandit9@bandit.labs.overthewire.org -p 2220` .
   - When prompted, enter the password retrieved from Level 8: `4CKMH11J19IbUIZZPXDqGana14xVAg0JM`.

2. **Access the Server**:
    - After successfully logging in, you will be in the home directory of the `bandit9` user.
3. **Locate the `data.txt` File**:
    - List the contents of the home directory using the `ls` command.
    - You will see a file named `data.txt`.
4. **Retrieve the Password for Level 10**:
    - Use the `strings` command to extract human-readable strings from the `data.txt` file.
    - Pipe the output to `grep` to filter lines containing '=' characters:

      `strings data.txt | grep ===` .
    - The password for Level 10 will be displayed in one of the lines that contain several '=' characters.

Findings/Results

- The password for Level 10 is: `FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey`.

Discussion/Analysis

- Level 9 introduces the challenge of extracting human-readable strings from a file that may contain non-text data. The `strings` command is essential for this task.

- This level emphasizes the importance of using text processing tools like `strings` and `grep` to efficiently locate specific patterns within files in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit9`.
- Retrieved the password for Level 10 by extracting human-readable strings from the `data.txt` file and filtering for lines containing '=' characters using the `strings` and `grep` commands.
- This level reinforces the importance of using text processing commands to find specific information within files.

Commands Used

- `ssh bandit9@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `strings data.txt | grep ===`: Extract human-readable strings from `data.txt` and filter for lines containing '=' characters.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**:

Writeup for Bandit Level 10 → Level 11

Title: Bandit Level 10 - Decoding Base64 Encoded Data

Introduction

Bandit Level 10 requires users to decode a base64 encoded string stored in a file named `data.txt`. The password for the next level is contained within this decoded data. This writeup documents the steps taken to complete Level 10 and retrieve the password for Level 11.

Level Goal

- The password for the next level is stored in the file `data.txt`, which contains base64 encoded data.

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 bandit10@bandit.labs.overthewire.org -p 2220`.
   - When prompted, enter the password retrieved from Level 9: `FGUMJ511LVJTrX9kMYMmLM4MgbpfMiqey`.
2. **Access the Server**:
   - After successfully logging in, you will be in the home directory of the `bandit10` user.
3. **Locate the `data.txt` File**:
   - List the contents of the home directory using the `ls` command.
   - You will see a file named `data.txt`.
4. **Retrieve the Password for Level 11**:
   - Use the `base64` command to decode the contents of the `data.txt` file:

`base64 -d data.txt` .

- The `d` option tells the `base64` command to decode the input.
- The decoded output will contain the password for Level 11.

Findings/Results

- The password for Level 11 is: `dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr`.

Discussion/Analysis

- Level 10 introduces the challenge of decoding base64 encoded data. The `base64` command is essential for decoding such data.
- This level emphasizes the importance of understanding encoding schemes and using the appropriate tools to decode data in a Linux environment.

Conclusion

- Successfully logged into the Bandit game server as `bandit10`.
- Retrieved the password for Level 11 by decoding the base64 encoded data in the `data.txt` file using the `base64 -d` command.
- This level reinforces the importance of using decoding tools to extract information from encoded data.

Commands Used

- `ssh bandit10@bandit.labs.overthewire.org -p 2220`: Connect to the server via SSH.
- `ls`: List files in the current directory.
- `base64 -d data.txt`: Decode the base64 encoded data in `data.txt`.

Screenshots

1. **SSH Connection**:

2. **Retrieving the Password**: