

Exploring Bandit Levels

De Silva K.R.K.D

Abstract

This report chronicles my playthrough of OverTheWire's Bandit stages, an entertaining examination of Linux security. From fundamental commands for Linux to complex security and cryptography problems, I provide knowledge, tactics, and solutions at every stage. This report shows my development and flexibility as I move through the Bandit levels in the cybersecurity industry. For those exploring novel tasks or ready to set off on their own adventure, it is an invaluable resource I cordially invite you to come with me on this fascinating journey, where each level advances our progress toward becoming adept keepers of digital forts. This abstraction offers a brief overview of the most important findings and training made along the advancement of Bandit levels, from first discovery to expert impact strategies.

Table of Contents

ABSTRACT.....	2
INTRODUCTION TO THE TOPIC.....	5
METHODOLOGY.....	6
Bandit levels and solutions.....	7
Bandit0.....	7
Bandit0 -> Bandit1.....	8
Bandit1 -> Bandit2.....	11
Bandit2 -> Bandit3.....	13
Bandit3 -> Bandit4.....	15
Bandit4 -> Bandit5.....	17
Bandit5 -> Bandit6.....	19
Bandit6 -> Bandit7.....	21
Bandit7 -> Bandit8.....	22
Bandit8 -> Bandit9.....	24
Bandit9 -> Bandit10.....	25
Bandit10 -> Bandit11.....	27
Bandit11 -> Bandit12.....	28
Bandit12 -> Bandit13.....	30
Bandit13 -> Bandit14.....	33
Bandit14 -> Bandit15.....	34
Bandit15 -> Bandit16.....	36
Bandit16 -> Bandit17.....	38
Bandit17 -> Bandit18.....	40
Bandit18 -> Bandit19.....	42
Bandit19 -> Bandit20.....	43

CONCLUSION.....	45
REFERENCES.....	46

Introduction to the topic

A necessity in the constantly changing field of cybersecurity is being able to secure Linux computers. In this field, practical knowledge, strong problem-solving skills, and a thorough grasp of system vulnerabilities and exploits are essential. Enter the Bandit levels, a gripping set of tasks carefully created by overtheWire to engross both novices and veterans in the area of Linux security. Bandit levels are fundamentally a place of play for hacking ethics, a digital testing field where competitors are exposed to a variety of Linux security situations, from the fundamentals of shell scripting and system administration to the complexities of increasing privileges and cryptographic enigmas.

My quest begins with a modest introduction to the fundamentals, unraveling the complexities of system permissions and interpreting basic Linux commands. Each level offers a different difficulty as I advance, like a puzzle that needs to be solved. Whether it's taking advantage of configuration errors, getting around access limitations, or cracking cryptographic ciphers, I explain my solutions and offer a thorough manual for individuals who want to overcome these obstacles on their own.

However, this study extends beyond simple fixes; it captures the heart of training in cybersecurity and the practice of ethical hacking. It emphasizes the value of accurate records and the continuous search of information in the quest for mastery. I hope to inspire and illuminate by the sharing of my experiences, demonstrating that anyone is able to begin on a similar road of learning and development throughout the cybersecurity field if they have the will and the necessary tools.

However, this study aims to go beyond only fixing issues. It captures the very core of ethical hacking and cybersecurity pedagogy- an attitude that emphasizes the practice of thorough documentation, celebrates the musical harmony produced by teamwork, and reverses the never-ending pursuit of knowledge that acts as the oven of expertise. Our goal in sharing our personal stories on these pages is not just to chronicle our experiences, but also to motivate and instruct.

I encourage you, my valued reader, to go with me as I navigate the convoluted passageways of Bandit, removing the veils of mystery that envelop Linux security layer by layer. Whether you are an adventurous beginner, an experienced guardian looking for fresh challenges, or simply an interested bystander, I can guarantee you that this report will not only offer insightful insights but will also heighten your understanding of the complex web ethical hacking. I go closer to becoming alert guards of digital fortresses with each challenge I successfully complete. Consequently, I cordially invite you to read my riveting account, "Exploring Bandit Levels."

Methodology

We take a thorough and organized approach to navigating the Bandit levels on OverTheWire. We start by carefully examining the guidelines and requirements for the first level to make sure we understand the goals at hand. Setting up a separate, safe Linux environment for testing is essential since it enables us to explore freely while preserving system integrity. At the same time, I keep comprehensive records of my progress, revelations, and responses to compile a thorough logbook of my adventure. As I examine every stage, I use critical thinking to uncover the challenge's core, spot possible vulnerabilities, and learn about the system's complexity. I put a lot of focus on lifelong learning, doing research when faced with new ideas, and using discussions, instructions, and internet tools to further my expertise. During this method, automation and scripting proved to be vital allies in cutting routine tasks and increasing my productivity.

I take on every problem with determination and perseverance, knowing that mistakes can teach us important lessons. Each level is finished at the end of my tour, and I provide thorough documentation of my answers and lessons learned. I continually evaluate my development, realizing how each level builds on the information learned from earlier ones, and I use this knowledge to take on the increasingly difficult challenge. The last step entails putting my solutions, observations, and progress diary into a thorough report. This report serves as both a personal account of my experiences and a resource for the larger community, facilitating information sharing and advancing our understanding of Linux security. In the end, my approach guarantees a methodical and instructive study of the Bandit levels, encouraging skill advancement and individual development in the field of ethical hacking and cyber security.

Bandit levels and solutions

Bandit0

Before starting Bandit 0 we are given a brief introduction about Bandit and how the game progresses.

The screenshot shows a web browser displaying the OverTheWire Bandit wargame introduction. The URL is https://overthewire.org/wargames/bandit/. The page has a dark theme with white text. At the top left is a small icon of two figures. On the right is the OverTheWire logo with the tagline "We're hackers, and we are good-looking. We are the T1s.". Below the logo are two buttons: "Donate!" and "Help?". The main content area is titled "Bandit" and contains the following text:

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Note for beginners

This Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. If you notice something essential is missing or have ideas for new levels, please let us know!

Level Progression

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
Level 27 → Level 28
Level 28 → Level 29
Level 29 → Level 30

Additional Information

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level >X<" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidebar menu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. Don't panic! Don't give up! The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information. If you've never used the command line before, a good first read is this introduction to user commands.

There are several things you can try when you are unsure how to continue:

- First, if you know a command, but don't know how to use it, try the **manual** (man page) by entering `man <command>`. For example, `man ls` to learn about the "ls" command. The "man" command also has a manual, try it! When using `man`, press q to quit (you can also use `/` and `n` to search).
- Second, if there is no man page, the command might be a **shell built-in**. In that case use the "`help <X>`" command. E.g. `help cd`
- Also, your favorite **search-engine** is your friend. Learn how to use it! I recommend Google.
- Lastly, if you are still stuck, you can join us via [chat](#).

You're ready to start! Begin with Level 0, linked at the left of this page. Good luck!

Note for VMs: You may fail to connect to overthewire.org via SSH with a "broken pipe error" when the network adapter for the VM is configured to use NAT mode. Adding the setting `IPQoS throughput` to `/etc/ssh/sshd_config` should resolve the issue. If this does not solve your issue, the only option then is to change the adapter to Bridged mode.

Here we can continue the Bandit game on Windows or Linux. Must log in via SSH to start. We have been given the username and password for Bandit 0.

The screenshot shows a web browser displaying the OverTheWire Bandit Level 0 page. The URL is https://overthewire.org/wargames/bandit/level0/. The page has a dark theme with white text. At the top left is a small icon of two figures. On the right is the OverTheWire logo with the tagline "We're hackers, and we are good-looking. We are the T1s.". Below the logo are two buttons: "Donate!" and "Help?". The main content area is titled "Bandit Level 0" and contains the following text:

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is `bandit.labs.overthewire.org`, on port 2220. The username is `bandit0` and the password is `bandit0`. Once logged in, go to the `Level 1` page to find out how to beat Level 1.

Commands you may need to solve this level

`ssh`

Helpful Reading Material

[Secure Shell \(SSH\) on Wikipedia](#)
[How to use SSH on wikiHow](#)

Level Progression

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
Level 27 → Level 28
Level 28 → Level 29
Level 29 → Level 30

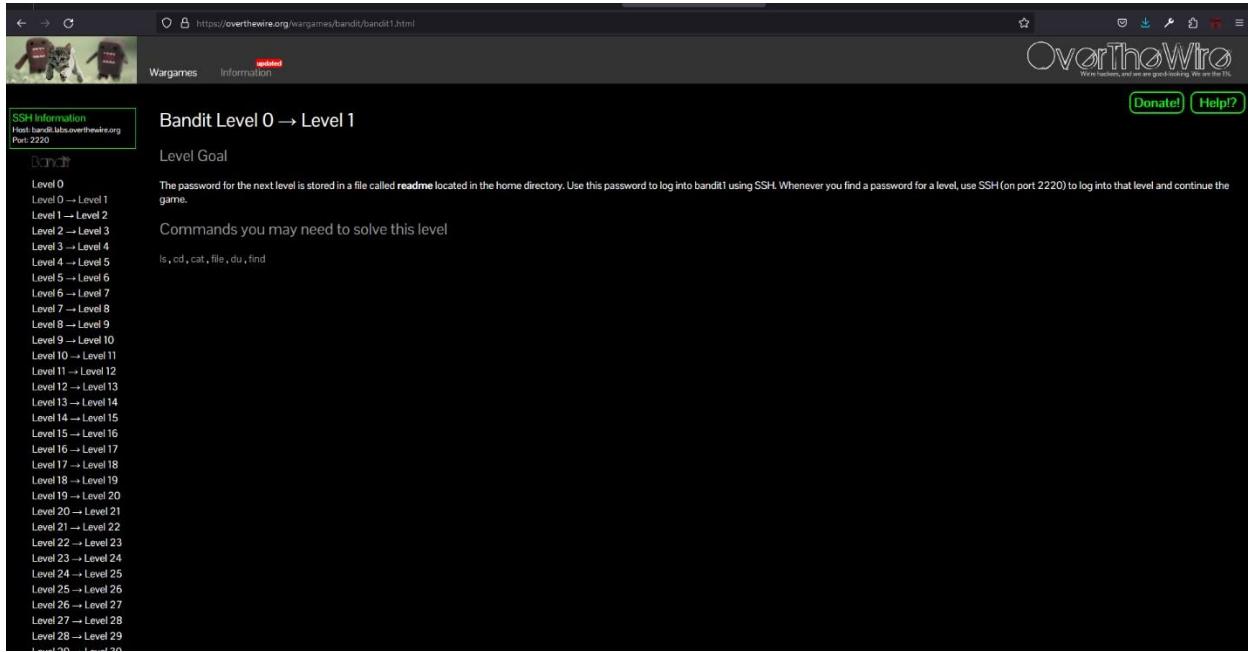
Type, "ssh bandit.labs.overthewire.org -p 2220 -l bandit0" and use the given password and log Bandit0.

Bandi0 -> Bandit1

Once we log Bandit0 we need to find the password of Bandit 1. They give us a hint and some commands.

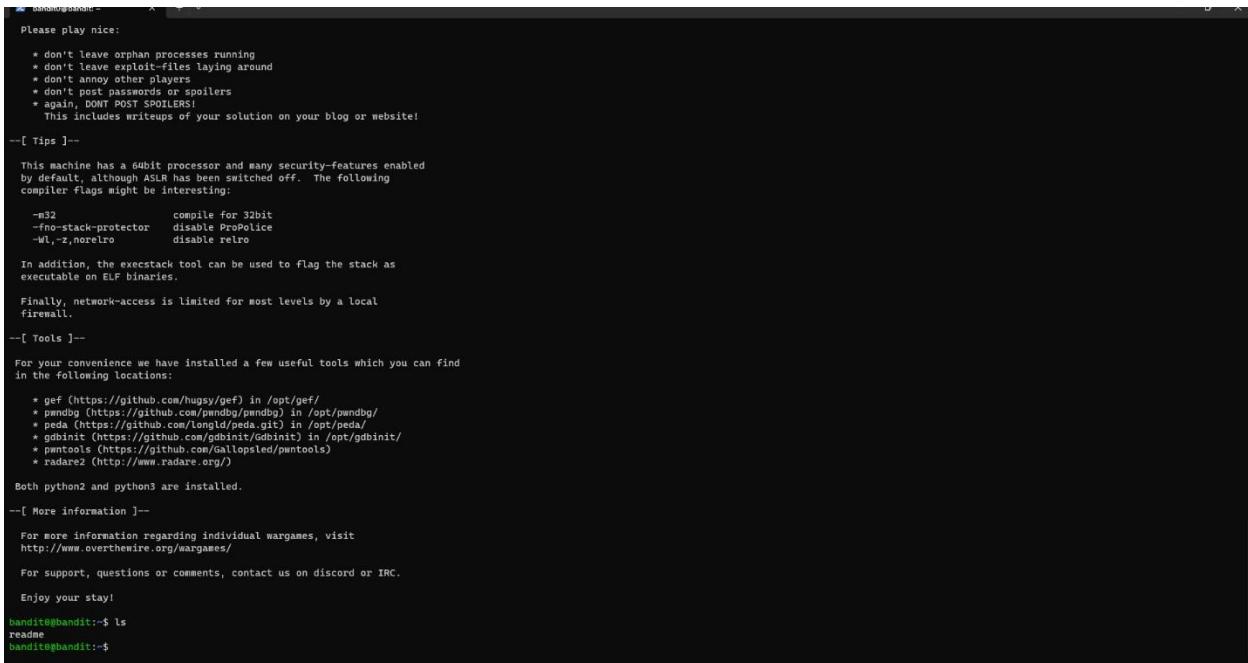
Here are those commands.

- ls – list directory
 - cd – change the working directory
 - cat - print the content of a file onto the standard output stream.
 - file – determine file type
 - du – measure the disk space occupied by files or directories.
 - find - search for files in a directory hierarchy.



The screenshot shows a web browser displaying the OverTheWire Bandit Level 0 page. The URL is https://overthewire.org/wargames/bandit/bandit1.html. The page has a header with the OverTheWire logo and navigation links for Wargames and Information. A sidebar on the left contains "SSH Information" with the host being bandit1.labs.overthewire.org and port 2220. It also lists levels from 0 to 29. The main content area is titled "Bandit Level 0 → Level 1" and contains a "Level Goal" section with the instruction: "The password for the next level is stored in a file called `readme` located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game." Below this is a "Commands you may need to solve this level" section with a list of commands: ls, cd, cat, file, du, find.

Use the “ls” command to see the file `readme`.



```
Please play nice:
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
This includes writeups of your solution on your blog or website!

--[ Tips ]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelo  disable relo

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbsniffer (https://github.com/gdbinit/GdbSniffer) in /opt/gdbinit/
* pwnools (https://github.com/gallopsled/pwnutils)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
bandit@bandit:~$ ls
readme
bandit@bandit:~$
```

Run “cat readme” to see the contents of the readme and to get the password.

```
bandit0@bandit:~      x  +  ~
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

  -m32          compile for 32bit
  -fno-stack-protector  disable ProPolice
  -Wl,-z,noexec  disable retro

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

  * gef (https://github.com/hugsy/gef) in /opt/gef/
  * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
  * peda (https://github.com/longld/peda.git) in /opt/peda/
  * gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
  * pwnools (https://github.com/Gallopsled/pwnools)
  * radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpnTxi3bvEHMSH66vXjL
bandit0@bandit:~$ |
```

To logout, run “exit”

```
Windows PowerShell      x  +  ~
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

  * gef (https://github.com/hugsy/gef) in /opt/gef/
  * pwndbg (https://github.com/pwendbg/pwendbg) in /opt/pwendbg/
  * peda (https://github.com/longld/peda.git) in /opt/peda/
  * gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
  * pwnools (https://github.com/Gallopsled/pwnools)
  * radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpnTxi3bvEHMSH66vXjL
bandit0@bandit:~$ exit
exit: command not found
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN>
```

Bandit1 > Bandit2

Read the hint and try to get an idea.

 https://overthewire.org/wargames/bandit/bandit2.html

OverTheWire
We're hackers, and we are good-looking. We are the 7%.

Wargames updated **Information**

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
Level 27 → Level 28
Level 28 → Level 29
Level 29 → Level 30

Bandit Level 1 → Level 2

Level Goal

The password for the next level is stored in a file called - located in the home directory

Commands you may need to solve this level

ls, cd, cat, file, du, find

Helpful Reading Material

Google Search for "dashed filename"
Advanced Bash-scripting Guide - Chapter 3 - Special Characters

Donate! **Help?**

Now log in to Bandit1, from the found password.

Run the “ls” command and find the “-“ file

```
b3n3t@b3n3t:~ + - X
Please play nice:
 * don't leave orphan processes running
 * don't leave exploit-files laying around
 * don't leave shellcodes
 * don't post passwords or spoilers
 * again, DON'T POST SPOILERS!
 This includes writeups of your solution on your blog or website!

--[ Tips ]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32           compile for 32bit
-fno-stack-protector    disable ProPolice
-Wl,-z,noexecro        disable r尔ro

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--
For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/huguyueh/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnutils (https://github.com/angr/pwnutils)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$
```

Use the “cat” command to find the Bandit2 password. But we cannot use the cat command and only “-“ because the system thinks “-“ is a command. So we need to use the cat command within “./-“ these commands and get the password.

Log out using the “exit” command.

Bandit2 > Bandit3

They tell us the next password is in a “spaces in this filename” file.

SSH Information
Host: bandit3.labs.overthewire.org
Port: 2220

Bandit

Level 0
Level 1 → Level 1
Level 2 → Level 2
Level 3 → Level 3
Level 4 → Level 4
Level 5 → Level 5
Level 6 → Level 6
Level 7 → Level 7
Level 8 → Level 8
Level 9 → Level 9
Level 10 → Level 10
Level 11 → Level 11
Level 12 → Level 12
Level 13 → Level 13
Level 14 → Level 14
Level 15 → Level 15
Level 16 → Level 16
Level 17 → Level 17
Level 18 → Level 18
Level 19 → Level 19
Level 20 → Level 20
Level 21 → Level 21
Level 22 → Level 22
Level 23 → Level 23
Level 24 → Level 24
Level 25 → Level 25
Level 26 → Level 26
Level 27 → Level 27
Level 28 → Level 28
Level 29

Bandit Level 2 → Level 3

Level Goal

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

Commands you may need to solve this level

ls, cd, cat, file, du, find

Helpful Reading Material

Google Search for "spaces in filename"

Log into Bandit2 using the username and the password.

```
bandit3@bandit:~$ gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit/) in /opt/gdbinit/
* pmtools (https://github.com/Gallopsled/pmtools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces in this filename
abZWSEmuFA7WHTQeQw0bauFj2LAIG
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit3
[REDACTED]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit3@bandit.labs.overthewire.org's password:
[REDACTED]
```

Using the “ls” command find the file name.

```
[ bandit2@bandit: ~ ] + - x
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$
```

Run the “cat” command with the file name. You can get the Bandit3 password.

```
[ bandit2@bandit: ~ ] + - x
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
abZw5EmuFa7tH7Qe0wd8bauFJ2lAig
bandit2@bandit:~$
```

Bandit3 > Bandit4

Log Bandit 3 to use the password.

The screenshot shows a web browser displaying the OverTheWire Wargames website at <https://overthewire.org/wargames/bandit/bandit4.html>. The page title is "Bandit Level 3 → Level 4". On the left, there's a sidebar titled "SSH Information" with the host set to "bandit.labs.overthewire.org" and port "2220". Below it is a "Bandit" section listing levels from 0 to 30. The main content area contains a "Level Goal" section with the text: "The password for the next level is stored in a hidden file in the `inhere` directory." and a "Commands you may need to solve this level" section with the command: "ls, cd, cat, file, du, find".

The screenshot shows a terminal window titled "bandit3@bandit:". The user has run several commands to gather information about the system:

```
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pmntools (https://github.com/GalllopSteed/pmntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.
```

Then, the user attempts to log in to the "bandit3" account:

```
--[ More information ]--
```

For more information regarding individual wargames, visit <http://www.overthewire.org/wargames/>

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

```
bandit3@bandit:~$ ls
spaces in this filename
bandit3@bandit:~$ cat "spaces in this filename"
ab28e0EmFAf7KHTQeWm8baufJ2lAig
bandit3@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit3

The terminal then displays a distorted version of the OverTheWire logo, followed by the message:

```
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

bandit3@bandit.labs.overthewire.org's password:

The password is partially obscured by a distorted graphic of the OverTheWire logo.

The next level password is hidden in the `inhere` file. Using the "ls" command find the "`inhere`" file name.

```
[bandit3@bandit: ~] x + v
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ |
```

Using the “cd” command change the directory. Only non-hidden files are displayed by the “ls” command. With the “-a” flag, however, it displays all files, including hidden files.

```
[bandit3@bandit:~/inhere] x + v
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
. . . .hidden
bandit3@bandit:~/inhere$ |
```

We can read the contents of the file because it is named “.hidden” and includes the password.

```

bandit3@bandit:~/inhere  x  +  v

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7B8srGAMoJ2HjW67dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Bandit4 -> Bandit5

SSH Information
Host: bandit5s.OverTheWire.org
Port: 2220

Bandit

- Level 0
- Level 1 → Level 1
- Level 1 → Level 2
- Level 2 → Level 3
- Level 3 → Level 4
- Level 4 → Level 5
- Level 5 → Level 6
- Level 6 → Level 7
- Level 7 → Level 8
- Level 8 → Level 9
- Level 9 → Level 10
- Level 10 → Level 11
- Level 11 → Level 12
- Level 12 → Level 13
- Level 13 → Level 14
- Level 14 → Level 15
- Level 15 → Level 16
- Level 16 → Level 17
- Level 17 → Level 18
- Level 18 → Level 19
- Level 19 → Level 20
- Level 20 → Level 21
- Level 21 → Level 22
- Level 22 → Level 23
- Level 23 → Level 24
- Level 24 → Level 25
- Level 25 → Level 26
- Level 26 → Level 27
- Level 27 → Level 28
- Level 28 → Level 29
- Level 29 → Level 30

Bandit Level 4 → Level 5

Level Goal

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.

Commands you may need to solve this level

ls, cd, cat, file, du, find

Log into the Bandit4 using the password. Use the “ls” command and find the file.

```
[bandit4@bandit: ~] + 
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$
```

Using the “cd” command change the directory. And use the “ls” command.

```
[bandit4@bandit:~/inhere] + 
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$
```

Type “./file*” to get a list of all the files in the directory along with their data types.

```
[bandit4@bandit:~/inhere] + 
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./*
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: ASCII text
./file09: Non-ISO extended-ASCII text, with no line terminators
bandit4@bandit:~/inhere$
```

The “-file07” has ASCII text. Type “cat ./file07” to get the password of Bandit5.

```

bandit4@bandit:~/inhere  x + v
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pmwtools (https://github.com/Gallopsled/pmwtools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ cd inhere
bandit4@bandit:~/inhere$ ls
./file01  ./file02  ./file03  ./file04  ./file05  ./file06  ./file07  ./file08  ./file09
bandit4@bandit:~/inhere$ file ./*
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: Non-ISO extended-ASCII text, with no line terminators
bandit4@bandit:~/inhere$ cat ./file09
lrTWzb6B37kxKficQzQu0OYFr6eEqR
bandit4@bandit:~/inhere$
```

Bandit05 -> Bandit06

Log in to Bandit05 using the password.

SSH Information
Host: bandit5s.OverTheWire.org
Port: 2220

Level Goal

The password for the next level is stored in a file somewhere under the `inhere` directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

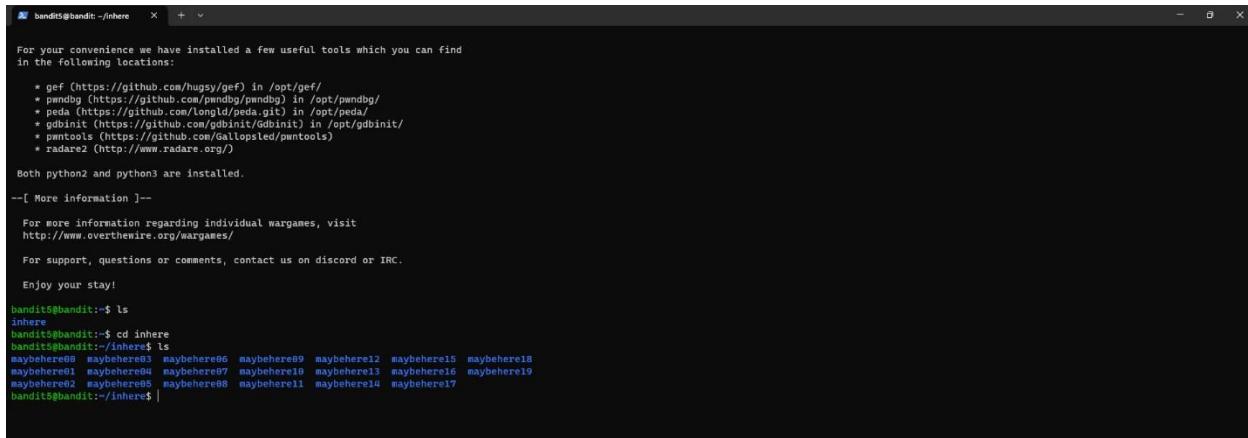
Commands you may need to solve this level

ls, cd, cat, file, du, find

Level Goal

Level 0
Level 1 → Level 1
Level 2 → Level 2
Level 3 → Level 3
Level 4 → Level 4
Level 5 → Level 5
Level 6 → Level 6
Level 7 → Level 7
Level 8 → Level 8
Level 9 → Level 9
Level 10 → Level 10
Level 11 → Level 11
Level 12 → Level 12
Level 13 → Level 13
Level 14 → Level 14
Level 15 → Level 15
Level 16 → Level 16
Level 17 → Level 17
Level 18 → Level 18
Level 19 → Level 19
Level 20 → Level 20
Level 21 → Level 21
Level 22 → Level 22
Level 23 → Level 23
Level 24 → Level 24
Level 25 → Level 25
Level 26 → Level 26
Level 27 → Level 27
Level 28 → Level 28
Level 29 → Level 29

Type the “ls” to find the file name. Next type the “cd inhere” to change the directory. Again type the “ls” to list directory.



```
bandit5@bandit:~/inhere X + v
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/overthewire/gdbinit) in /opt/gdbinit/
* pmntools (https://github.com/Gallopsled/pmntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

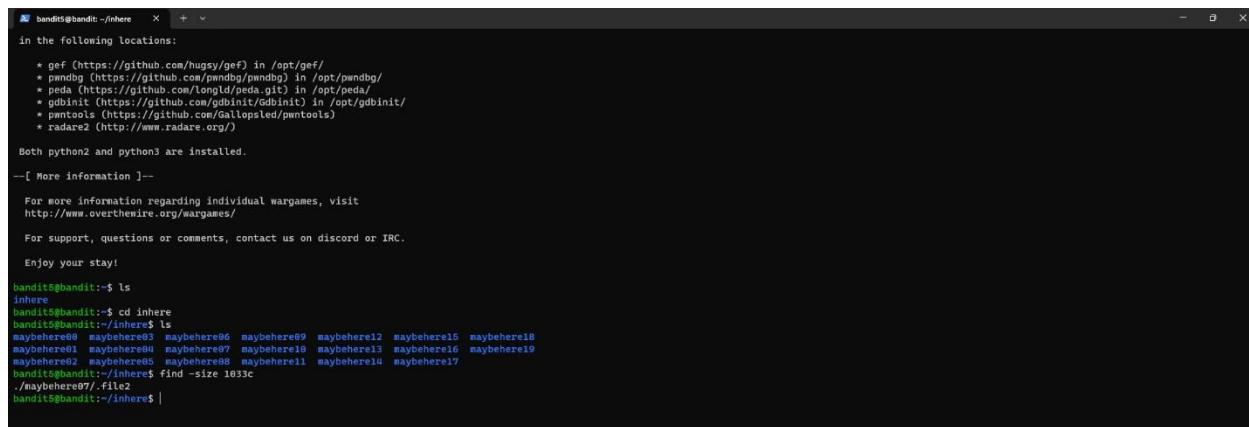
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~/inhere$ |
```

Type the “find -size 1033c” to find files that are readable with a size of 1033c.



```
bandit5@bandit:~/inhere X + v
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/overthewire/gdbinit) in /opt/gdbinit/
* pmntools (https://github.com/Gallopsled/pmntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

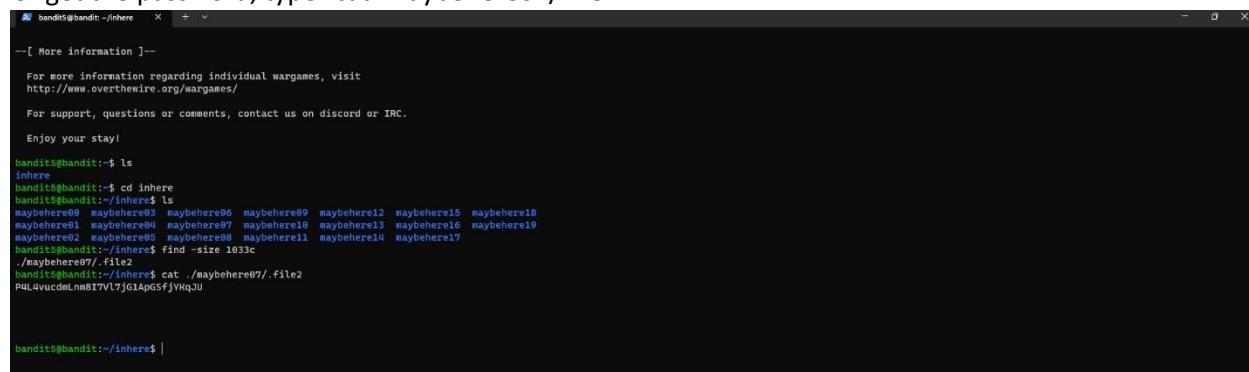
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ |
```

For get the password, type “cat .maybehere07/.file2”



```
bandit5@bandit:~/inhere X + v
--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
PQLuvuCDcm8mI7vL7jG1aGSGfjYKqJU

bandit5@bandit:~/inhere$ |
```

Bandit6 → Bandit7

The screenshot shows the OverTheWire Wargames website at https://overthewire.org/wargames/bandit/bandit7.html. The page title is "Bandit Level 6 → Level 7". On the left, there's a sidebar titled "SSH Information" with the host "bandit6.OverTheWire.org" and port "2220". Below it is a list of levels from 0 to 28. The "Level Goal" section contains the following text: "The password for the next level is stored somewhere on the server and has all of the following properties: owned by user bandit7, owned by group bandit6, 33 bytes in size". The "Commands you may need to solve this level" section lists various Linux commands: ls, cd, cat, file, du, find, grep.

Log into the Bandit6 using the password. Use the root directory command to search the system.

```
bandit6@bandit6: ~
bandit6@bandit6: $ find / -user bandit7 -group bandit6 -size 33c
find: /var/swap: Permission denied
find: /var/crash: Permission denied
find: /var/spool/rsyslog: Permission denied
find: /var/spool/bandit24: Permission denied
find: /var/spool/cron/crontabs: Permission denied
find: /var/tmp: Permission denied
find: /var/lib/polkit-1: Permission denied
find: /var/lib/dpkg/info/bandit7.password: Permission denied
find: /var/lib/libcryptsetup: Permission denied
find: /var/lib/apt/lists/partial: Permission denied
find: /var/lib/amazon: Permission denied
find: /var/lib/update-notifier/package-data-downloads/partial: Permission denied
find: /var/lib/snapd/void: Permission denied
find: /var/lib/snapd/cookie: Permission denied
find: /var/lib/ubuntu-adantage/apt-esm/var/lib/apt/lists/partial: Permission denied
find: /var/lib/libapt: Permission denied
find: /var/lib/libapt/l10n: Permission denied
find: /var/cache/ldconfig: Permission denied
find: /var/cache/apt/archives/partial: Permission denied
find: /var/cache/pollinate: Permission denied
find: /var/cache/private: Permission denied
find: /var/cache/apparmor/4dd8d84e.0: Permission denied
find: /var/cache/apparmor/eeeb6286.0: Permission denied
find: /drifter/drifter14_src/axTLS: Permission denied
find: /home/bandit6/.ssh/authorized_keys: Permission denied
find: /home/bandit6/.drifters/data: Permission denied
find: /home/bandit24-git: Permission denied
find: /home/drifter/chroot: Permission denied
find: /home/ubuntu: Permission denied
find: /home/bandit5/inhere: Permission denied
find: /home/bandit27-git: Permission denied
find: /home/bandit28-git: Permission denied
find: /home/bandit29-git: Permission denied
find: /boot/efi: Permission denied
find: /proc/pty/driver: Permission denied
find: /proc/271937/kash/271937/fd/6: No such file or directory
find: /proc/271937/kash/271937/fdinfo/6: No such file or directory
find: /proc/271937/fd/5: No such file or directory
find: /proc/271937/fdinfo/5: No such file or directory
find: /etc/polkit-1/localauthority: Permission denied
find: /etc/polkit-1/localauthority/10-guest: Permission denied
find: /etc/polkit-1/localauthority/20-sys: Permission denied
find: /etc/polkit-1/localauthority/30-guest: Permission denied
find: /etc/sudoers.d: Permission denied
find: /dev/mqueue: Permission denied
find: /dev/shm: Permission denied
find: /tmp: Permission denied
find: /snap: Permission denied
find: /lost+found: Permission denied
find: /run/chrony: Permission denied
find: /run/user/11026: Permission denied
```

Type this command “cat /var/lib/dpkg/info/bandit7.password” and find the password.

```

bandit6@bandit:~ % 
Find: '/run/user/11013': Permission denied
Find: '/run/user/11001': Permission denied
Find: '/run/user/11065': Permission denied
Find: '/run/user/11024': Permission denied
Find: '/run/user/11016': Permission denied
Find: '/run/user/11027': Permission denied
Find: '/run/user/11002': Permission denied
Find: '/run/user/11009': Permission denied
Find: '/run/sudo': Permission denied
Find: '/run/screen/S-bandit20': Permission denied
Find: '/run/multipath': Permission denied
Find: '/run/cryptsetup': Permission denied
Find: '/run/lvm': Permission denied
Find: '/run/credentials/systemd-sysvinit.service': Permission denied
Find: '/run/systemd/greenter-root': Permission denied
Find: '/run/systemd/unit-root': Permission denied
Find: '/run/systemd/inaccessible/dir': Permission denied
Find: '/run/lock/lvm': Permission denied
Find: '/run/initrafs': Permission denied
Find: '/root': Permission denied
Find: '/sys/kernel/tracing': Permission denied
Find: '/sys/kernel/dragong': Permission denied
Find: '/sys/firmware': Permission denied
bandit6@bandit:~ $ find / user bandit7 -group bandit6 -size 33c 2>/dev/null//var/lib/dpkg/info/bandit7.password
-bash: /dev/null//var/lib/dpkg/info/bandit7.password: Not a directory
bandit6@bandit:~ $ cat /var/lib/dpkg/info/bandit7.password
z7WtOhQU2XjMtwAABuSNwvzquav95
bandit6@bandit:~ $

```

Bandit7 → Bandit8

The screenshot shows a web browser window for the OverTheWire Wargames Bandit7 level. The URL is <https://overthewire.org/wargames/bandit/bandit7.html>. The page has a header with the OverTheWire logo and navigation links for Wargames and Information. On the left, there's a sidebar titled "SSH Information" with host details: bandit7s.OverTheWire.org, Port: 2220, and a "Connected" status. The main content area is titled "Bandit Level 7 → Level 8". It contains a "Level Goal" section stating "The password for the next level is stored in the file **data.txt** next to the word **millionth**". Below it is a "Commands you may need to solve this level" section listing: man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd. A large list of levels follows, ranging from Level 0 to Level 28, each preceded by a link icon.

Log into Bandit7 using the password and first check the size of the “data.txt” file.

```
bandit7@bandit: ~ + - x
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit7@bandit:~$ du -b data.txt
4184396 data.txt
bandit7@bandit:~$ |
```

Now we need to use the “grep” command. grep command can be used to search lines that follow a particular pattern. Using the “grep” command and the pipe “|” we can find the password.

```
bandit7@bandit: ~ + - x
--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit7@bandit:~$ du -b data.txt
4184396 data.txt
bandit7@bandit:~$ cat 4184396 data.txt | grep millionth
cat: 4184396: No such file or directory
millionth    TE5KZC8VtetK059xNwm2557K5iWr8vP
bandit7@bandit:~$ |
```

Bandit8 -> Bandit9

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit9.html>. The page title is "Bandit Level 8 → Level 9". On the left, there's a sidebar with "SSH Information" (Host: bandit.labs.overthewire.org, Port: 2220) and a "Bandit" section listing levels from 0 to 29. The main content area contains a "Level Goal" section with the text: "The password for the next level is stored in the file `data.txt` and is the only line of text that occurs only once". It also lists "Commands you may need to solve this level" including grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd. A "Helpful Reading Material" section includes links to Piping and Redirection and Level 17.

Log into Bandit8 using the password.

The screenshot shows a Windows PowerShell window titled "Windows PowerShell". The command entered is `PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit8`. The session starts with a graphical login screen. After logging in, the user is prompted for the password: "bandit8@bandit.labs.overthewire.org's password:". The password is entered and the user is welcomed with "Welcome to OverTheWire!". The message continues with instructions for reporting problems and playing the games. It also provides information about usernames, levels, and passwords, and cautions against leaving processes running or exploiting files in /tmp.

Sort – sorts the lines of a text file

Uniq – filters input and writers to the output

So, using “sort data.txt | uniq -u” we can get the password.

```

bandit@bandit:~$ 
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/husg/gef) in /opt/gef/
* pwndbg (https://github.com/swmbp/pwndbg) in /opt/pwndbg/
* peda (https://github.com/tongld/peda.git) in /opt/peda/
* gdbinit (https://github.com/Gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More Information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit@bandit:~$ sort data.txt | uniq -u
EN5JZPcFY1ZBnSPNVR3X0AS1N1NNEDt
bandit@bandit:~$ 

```

Bandit9 → Bandit10

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit10.html>. The page is titled "Bandit Level 9 → Level 10". It features a sidebar with "SSH Information" (Host: bandit10s overthewire.org, Port: 2220) and a "Level Goal" section. Below these are two columns: "Commands you may need to solve this level" (grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd) and a list of 28 previous levels (Level 0 → Level 1, Level 1 → Level 2, ..., Level 27 → Level 28). The OverTheWire logo and navigation links are visible at the top right.

Using the “ls” command find the “data.txt” file.

```
[bandit@bandit: ~] + - x
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

-[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

-[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ |
```

We need to use the “string” command to separate human-readable strings in “data.txt”. And use “grep” within the equal sign “=”.

```
[bandit9@bandit: ~] + - x
firewall.

-[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

-[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt |grep ==
u***** the#
***** password
***** GTwBLIiG3NtB8A7j9LgrywtEUYyp6s
bandit9@bandit:~$ |
```

Bandit10 -> Bandit11

The screenshot shows a web browser displaying the OverTheWire Wargames website at <https://overthewire.org/wargames/bandit/bandit11.html>. The page title is "Bandit Level 10 → Level 11". On the left, there's a sidebar with "SSH Information" (Host: bandit10s.OverTheWire.org, Port: 2220) and a "Bandit" navigation menu listing levels from 0 to 29. The main content area contains a "Level Goal" section with the text: "The password for the next level is stored in the file `data.txt`, which contains base64 encoded data". It also lists "Commands you may need to solve this level": grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd. A "Helpful Reading Material" section links to "Base64 on Wikipedia". The OverTheWire logo is in the top right corner.

First, log into Bandit10. Run the “cat” command with the file name.

```
bandit10@bandit10:~$ cat data.txt
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pmntools (https://github.com/Gallopsled/pmntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit10@bandit10:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGVeaUxkJz5s05kTlLGTMz2b1ZD5pwaGXYSEJNCg==
```

Use the “base64 -d data.txt” command for decoding to the password.

```

bandit10@bandit: ~ + 
--[ Tools ]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwntools (https://github.com/angr/pwntools) in /opt/pwntools/
* peda (https://github.com/L0phtCtrlF/peda.git) in /opt/peda/
* gdbinit (https://github.com/dbhinit/gdbinit) in /opt/gdbinit/
* pwnlib (https://github.com/Gallopsled/pwnlib)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit10@bandit:~$ cat data.txt
VGHtIHBr3Wb3jKIGlzlDZ6UG96auXkUj5sS05kTllGTM12blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezilR2RHNdNYFnB6nVKzphlxHBM
bandit10@bandit:~$ |

```

Bandit11 -> Bandit12

SSH Information
Host: bandit11.overthewire.org
Port: 2220

Level Goal
The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

Commands you may need to solve this level
grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material
Rot13 on Wikipedia

Log into Bandit11 with the password. Use the "ls" command.

```
[bandit1@bandit:~] x + v
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ |
```

Use the “cat” command to get the password.

```
[bandit11@bandit:~] x + v
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSHBbJ8puQm5lIEi
bandit11@bandit:~$
```

Now use the “tr” command for translation, allowing replacing the characters with others. And “A ->N,, Z ->M” to get the password.

```
[bandit11@bandit:~] x + v
For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
Tqd ozzrvng hc JVNBBFSLzVxKHP0PxaX0nwBpbDy5xvRu
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKHOPOXbFXOoWchDz5yVRv
bandit11@bandit:~$
```

Bandit12 -> Bandit13

Log into Bandit12 using the password.

The screenshot shows a web browser window for the OverTheWire Wargames site at <https://overthewire.org/wargames/bandit/bandit13.html>. The page title is "Bandit Level 12 → Level 13". On the left, there's a sidebar with "SSH Information" showing "Host: bandit12bs.OverTheWire.org" and "Port: 2220". Below it is a list of levels from 0 to 29. The main content area contains a "Level Goal" section with instructions about compressing files and creating temporary directories, followed by a "Commands you may need to solve this level" section listing tools like grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv, file, and hex dump. There's also a "Helpful Reading Material" section with a link to Wikipedia.

Use the “cp” command to copy files. Type “cp data.txt /tmp/pc” first and next type “cd /tmp/pc” to change directory.

```
bandit12@bandit12:~$ cp data.txt /tmp/pc
bandit12@bandit12:~$ cd /tmp/pc
bandit12@bandit12:~/tmp/pc$
```

The terminal window shows the user is in a Bandit12 shell. It displays a welcome message about network access being limited by a local firewall, a list of installed tools (gef, pwndbg, peda, gdbinit, pwntools, radare2), and information about Python versions. The user then runs the commands "cp data.txt /tmp/pc" and "cd /tmp/pc" to prepare for the next step.

Type “ls” and find the list. Use the “file myfile.txt” and find the file to know what the password is.

```
bandit12@bandit:~/tmp/pc  x  +  v
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg
* peda (https://github.com/torvalds/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/GdbInit) in /opt/gdbinit/
* pwntools (https://github.com/galoopsd/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit12@bandit:~$ cp data.txt /tmp/pc
bandit12@bandit:~$ cd /tmp/pc
bandit12@bandit:/tmp/pc$ ls
dataA.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data6.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:/tmp/pc$ file myself.txt
myself.txt: cannot open `myself.txt' (No such file or directory)
bandit12@bandit:/tmp/pc$ file myfile.txt
myfile.txt: ASCII text
bandit12@bandit:/tmp/pc$
```

Run the “cat myfile.txt”

Run “xxd -r myfile.txt >myfile1.bin” and next run the “ls” to find all the files.

```

bandit12@bandit:~/tmp/pc$ xterm -e ./bandit12
[1] 11888
bandit12@bandit:~/tmp/pc$ ./bandit12
[1]+ 11888 Done                  ./bandit12
bandit12@bandit:~/tmp/pc$ cat myfile1.txt
data5.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data6.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data6.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ rm myfile1 myfile3 myfile7
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ rm myfile2 myfile4
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile9
bandit12@bandit:~/tmp/pc$ rm myfile9
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin
bandit12@bandit:~/tmp/pc$ rm data5 bin
bandit12@bandit:~/tmp/pc$ ls
data8.bin
bandit12@bandit:~/tmp/pc$ rm data8 bin
bandit12@bandit:~/tmp/pc$ ls

```

A command called “zcat” is included with “gzip” and is used to decompress “gzip” compressed files. Using the file command on myfile2, we can find bzip2 compressed data. Use that command to all 9 files and use the “tar” for archiving files and options. Finally, we can find the password.

```

bandit12@bandit:~/tmp/pc$ xterm -e ./bandit12
[1] 11888
bandit12@bandit:~/tmp/pc$ ./bandit12
[1]+ 11888 Done                  ./bandit12
bandit12@bandit:~/tmp/pc$ cat myfile1.txt
data5.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data6.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data6.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ rm myfile1 myfile3 myfile7
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ rm myfile2 myfile4
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin myfile9
bandit12@bandit:~/tmp/pc$ rm myfile9
bandit12@bandit:~/tmp/pc$ ls
data5.bin data8.bin
bandit12@bandit:~/tmp/pc$ rm data5 bin
bandit12@bandit:~/tmp/pc$ ls
data8.bin
bandit12@bandit:~/tmp/pc$ rm data8 bin
bandit12@bandit:~/tmp/pc$ ls

```

Bandit13 -> Bandit14

The screenshot shows a web browser displaying the OverTheWire Wargames website at <https://overthewire.org/wargames/bandit/bandit14.html>. The page title is "Bandit Level 13 → Level 14". It contains the following sections:

- SSH Information**: Host bandit14s overthewire.org Port 2220
- Level Goal**: The password for the next level is stored in `/etc/bandit_pass/bandit14` and can only be read by user `bandit14`. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: `localhost` is a hostname that refers to the machine you are working on.
- Commands you may need to solve this level**: ssh, telnet, nc, openssl, s_client, nmap
- Helpful Reading Material**: SSH/OpenSSH Keys
- Level Progress**: Level 0 → Level 1, Level 1 → Level 2, Level 2 → Level 3, Level 3 → Level 4, Level 4 → Level 5, Level 5 → Level 6, Level 6 → Level 7, Level 7 → Level 8, Level 8 → Level 9, Level 9 → Level 10, Level 10 → Level 11, Level 11 → Level 12, Level 12 → Level 13, Level 13 → Level 14, Level 14 → Level 15, Level 15 → Level 16, Level 16 → Level 17, Level 17 → Level 18, Level 18 → Level 19, Level 19 → Level 20, Level 20 → Level 21, Level 21 → Level 22, Level 22 → Level 23, Level 23 → Level 24, Level 24 → Level 25, Level 25 → Level 26, Level 26 → Level 27, Level 27 → Level 28, Level 28 → Level 29, Level 29 → Level 30.

Use the “ls” command to find the file.

```
bandit13@bandit:~ % ls
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/get/
* Immunity (https://github.com/immunityfwd/Immunity) in /opt/immunity/
* peda (https://github.com/l�ngld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ |
```

For remote machine access and command execution, use the “ssh” command. The “sshkey.private” file and the option “-i” are used to choose the identified file for RSA or DSA authentication.

```

bandit3@bandit: ~ [ Tools ] --
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/longld/pwndbg) in /opt/pwndbg/
* peda (https://github.com/radareorg/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

-- [ More information ] --
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit13$ ls
sshkey.private
bandit13$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:CzihUBV7iHnViwURhRrEcLFXCSCXlhMAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? |

```

Bandit14 -> Bandit15

Log into Bandit14 first.

SSH Information
Host: bandit14.overthewire.org
Port: 2220

Level Goal
The password for the next level can be retrieved by submitting the password of the current level to **port 30000** on localhost.

Commands you may need to solve this level
ssh, telnet, nc, openssl, s_client, nmap

Helpful Reading Material
How the Internet works in 5 minutes (YouTube) (Not completely accurate, but good enough for beginners)
IP Addresses
IP Address on Wikipedia
Localhost on Wikipedia
Ports
Ports (computer networking) on Wikipedia

The command “nc” enables the reading and writing of data across a network connection. Both TCP and UDP connections are supported by it. Use that command and try to get the password. But they asked us for the password. So we need to find the password first.

```
[bandit4@bandit: ~] + ~
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit:~$ nc localhost 30000
****
Wrong! Please enter the correct current password
|
```

Run this command “cat /etc/bandit_pass/bandit14” and get the password.

```
[bandit4@bandit: ~] + ~
--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit:~$ nc localhost 30000
****
Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHpx#02xGc7U7rxXOaxiwFToiF0ENq
bandit14@bandit:~$
```

```
[bandit4@bandit: ~] + ~
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit:~$ nc localhost 30000
****
Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHpx#02xGc7U7rxXOaxiwFToiF0ENq
bandit14@bandit:~$ nc localhost 30000
fGrHpx#02xGc7U7rxXOaxiwFToiF0ENq
Correct!
jN2kgmIXJ6f5hzht2avhotn4Zcka6tn
```

Bandit15 -> Bandit16

OverTheWire.org

Wargames Information

SSH Information
Host: bandit16.OverTheWire.org
Port: 2220

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
Level 27 → Level 28
Level 28 → Level 29
Level 29 → Level 30

Bandit Level 15 → Level 16

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to port **30001** on **localhost** using SSL encryption.

Helpful note: Getting "HEARTBEATING" and "Read R BLOCK"? Use -ign_eof and read the "CONNECTED COMMANDS" section in the manpage. Next to 'R' and 'Q', the 'B' command also works in this version of that command...

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

Helpful Reading Material

Secure Socket Layer/Transport Layer Security on Wikipedia
OpenSSL Cookbook - Testing with OpenSSL

Openssl – library for secure communication over networks.

Openssl s_client – implementation of a basic SSL/TLS client that communicates with a server.

Run “`openssl s_client -connect localhost:30001`” this command, after run that we need to type the password of bandit 15. When we type it shows the Bandit16 password.

```

bandit5@bandit: ~ + 
0050 - ff ef dc 14 ab 03 c3 b8-7b 17 bc d5 cd 6c 46 6e ... .H..{...!Fn
0060 - 03 8d 85 d6 76 64 66 7f-42 81 13 28 7a 6d ae 8f ... .vdf.B..rm.
0070 - 39 f9 c2 8e 09 85 ab 89-ee 9f d7 de 8a 85 53 2b 9.....,....S+
0080 - 9e 34 ca d4 94 0c 05 23-84 2b f9 49 5c a3 c2 4.....,#+.!V...
0090 - 98 56 3a 08 b4 43 94 b6-c2 e1 2c d3 cc 67 cc V>..C....9..
00a0 - 38 ab a2 6f 94 da 24-b5 e8 b3 0f 66 de f1 d5 8..o.D$...fn.
00b0 - 2c b5 d2 07 09 77 94 ef-7f a8 83 71 bb 51 de ce ...W..q.Q..
00c0 - 29 65 1e 9a 9e 03 d5 df d7-a0 b2 1e e5 17 9f c7 55 )e.....U

Start Time: 1693935286
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
--- read R BLOCK
Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_256_GCM_SHA384
Session-ID: FC0064B8F5796834C8CD83CF848E6794C3C421D11F6E77C59C4B1E386E37208C
Resumption PSK: ABC9AAADE1928FB50D58E6210B5E178A7F1247H5DE019770D9C6173C08EFC850382C1E66464E6499AE54E04B2022D46
PSK Identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 0a 08 a5 32 50 0e cb 4c-36 de e2 24 47 c1 4f 66 .H.2T..L6..$G.OF
0010 - 30 43 9d 98 c2 38 90 73-7a 7d 7f 89 ff 24 cc 9e 0C..8.s2z...$.
0020 - 04 0d 05 04 06 05 07 08 09 0a 0b 0c 0d 0e 0f 0g 0h ..V.....,....I.
0030 - a7 01 08 25 03 00 02 01 00 0f 07 00 0t 09 08 05 085..n.w.g91..e
0040 - cd f3 94 91 61 85 fu 59-0d 63 b3 f6 e6 58 d7 ea 4..a..Y.c..X.
0050 - 2f af 04 af aa 91 27 3c-5d fb 05 47 eb 8d 74 0a /N...`*]....t.
0060 - 69 b5 92 84 5b ac 58 a1-c8 92 8f 11 78 21 c0 0f 1..T!.X....x!.
0070 - 39 f9 00 c5 92 63 d3-44 13 17 e8 27 a5 52 53 9....,D....R.
0080 - c1 19 7c 57 c3 da 4f 3d-52 13 43 83 eb 3c 65 62 ..|W..O=R.C..

```

Bandit16 -> Bandit17

Log into the Bandit16.

The screenshot shows a web browser window for the OverTheWire Wargames site at <https://overthewire.org/wargames/bandit/bandit17.html>. The page title is "Bandit Level 16 → Level 17". On the left, there's a sidebar titled "SSH Information" with a link to "Host: localhost:overthewire.org Port:2220". Below it is a list of levels from 0 to 29. The main content area has a "Level Goal" section with instructions about port scanning and a list of commands ("sh, telnet, nc, openssl s_client, nmap"). It also includes a "Helpful Reading Material" section with a link to "Port scanner on Wikipedia". The OverTheWire logo is at the top right, along with "Donate!" and "Help?".

Run “nmap localhost -p31000-32000” to check what services are running on them.

A terminal window titled "bandit16@bandit16" shows the output of an nmap scan. The command run was "nmap localhost -p31000-32000". The output shows several open ports, notably 31790/tcp and 31790/udp, which are identified as "uncommon" services. Other ports listed include 31118/tcp, 31691/tcp, 31798/tcp, and 31968/tcp.

```
bandit16@bandit16:~$ ls
bandit16@bandit16:~$ nmap localhost -p31000-32000
Starting Nmap 7.88 ( https://nmap.org ) at 2023-09-05 17:58 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31118/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31790/udp open  unknown
31798/tcp  open  unknown
31968/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
bandit16@bandit16:~$
```

The port that shows promise appears to be 31790, which is used by an unidentified service.

Use “Openssl” and connect to this port on localhost

Save this key locally. Use a ssh private key.

```
“ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220”
```

```
[bandit17@bandit: ~] -[ Playing the games ]-
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are stored in "/somegame/" ...
* MOST LEVELS are stored in "/somegame/" ...
* PASSWORDS for each level are stored in "/etc/somegame_pass/".

Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in "/tmp/". You can use the command "mktemp" to quickly create a temporary directory in a specified directory in "/tmp/". Read-access to both "/tmp/" is disabled and to "/proc" restricted so that users cannot snoop on eachother. Files and directories with easily guessable or short names will be periodically deleted! The "/tmp" directory will be periodically wiped.
Please play nice!
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post answers to your own spoilers
* again, DON'T POST SPOILERS!
This includes writeups of your solution on your blog or website!
-[ Tips ]-
This machine has a DEBIL processor and many security features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:
-a32
-fno-stack-protector disable ProPolice
-Wl,-z,nowlro disable rrolo

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.
-[ Tools ]-
For your convenience we have installed a few useful tools which you can find in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* aspw (https://github.com/0x00sec/aspw) in /opt/aspw/
* gbininit (https://github.com/gbininit/gbininit) in /opt/gbininit/
* pwnutils (https://github.com/Gallopsled/pwnutils)
* radare2 (https://www.radare.org/)

Both python and python3 are installed.

-[ More Information ]-
For more information regarding individual wargames, visit
http://www.ovethenirw.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
```

But this file could be edited by the owner and was readable by the group and the entire world. Using a command, we switch the owner's account to read-only mode. Now can get the access to the Bandit17.

```

bandit16@bandit:~/tmp/bandit > + -
closed
bandit16@bandit:~$ mkdir /tmp/bandit77
bandit16@bandit:~$ cd /tmp/bandit77
bandit16@bandit:~/tmp/bandit77$ ls
bandit16@bandit:~/tmp/bandit77$ nano sshkey.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:~/tmp/bandit77$ nano sshkey.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory

Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:~/tmp/bandit77$ ls
sshkey.private
bandit16@bandit:~/tmp/bandit77$ chmod 400 sshkey.private
bandit16@bandit:~/tmp/bandit77$ ls
sshkey.private
bandit16@bandit:~/tmp/bandit77$ ls -hal
total 1M
drwxrwx-x  2 bandit16 bandit16 4.0K Sep  5 18:14 .
drwxrwx-wt 269 root   root    11M Sep  5 18:15 ..
-rw-r--r--  1 bandit16 bandit16 1.7M Sep  5 18:14 sshkey.private
bandit16@bandit:~/tmp/bandit77$ ssh -i sshkey.private bandit17@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:c2inU8v7ihViawRb4RrEcLFxCSCXlhMAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes|

```

Bandit17 -> Bandit18

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit18.html>. The page title is "Bandit Level 17 → Level 18". On the left, there's a sidebar titled "SSH Information" with the host "bandit18s.OverTheWire.org" and port "2220". Below it is a "Bandit" navigation menu with links from Level 0 to Level 28. The main content area contains a "Level Goal" section with the following text:

There are 2 files in the homedirectory: `passwords.old` and `passwords.new`. The password for the next level is in `passwords.new` and is the only line that has been changed between `passwords.old` and `passwords.new`

NOTE: if you have solved this level and see 'Byebyef' when trying to log into bandit18, this is related to the next level, bandit19

Commands you may need to solve this level

cat, grep, ls, diff

diff – program compares files line by line.

Run the ls command and get the file name.

```
[bandit7@bandit:~] x + v
compiler flags might be interesting:
-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,noexecro  disable r尔ro

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit7@bandit:~$ ls
passwords.new passwords.old
bandit7@bandit:~$ |
```

Now run the “diff passwords.old passwords.new” to get different passwords called old and new.

```
[bandit7@bandit:~] x + v
For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit7@bandit:~$ ls
passwords.new passwords.old
bandit7@bandit:~$ diff passwords.old passwords.new
u2c02
< g1ZreTEH1V3cGKL6g4conYqZqaEj0wte
> hpa5tutuCLf6ffzUpnagiMN8ssu9LFrdg
bandit7@bandit:~$ |
```

Bandit18 -> Bandit19

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit19.html>. The page title is "Bandit Level 18 → Level 19". On the left, there's a sidebar with "SSH Information" and a list of levels from 0 to 29. The main content area contains a "Level Goal" message: "The password for the next level is stored in a file `readme` in the homedirectory. Unfortunately, someone has modified `.bashrc` to log you out when you log in with SSH." Below this, there's a section titled "Commands you may need to solve this level" with the command "ssh, ls, cat".

We can try using SSH to log in with them. The terminal window to be used to log into the system is specified using the “-t” flag of the SSH command.

The screenshot shows a Windows PowerShell window. The terminal output is as follows:

```
Windows PowerShell
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32      compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,noexecro  disable relro

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsweat/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN> ssh bandit19@bandit.labs.overthewire.org -p 2220 -t */bin/sh*
```

At the bottom, there's a decorative ASCII art banner and a note: "This is an OverTheWire game server. More information on <http://www.overthewire.org/wargames>".

Run the “ls” command and then run the “cat readme” command. When we run those commands we can find the flag.

```
Windows PowerShell x + ->
Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN> ssh bandit18@bandit.labs.overthewire.org -p 2228 -t "/bin/sh"
[!] [!] [!] [!] [!] [!] [!]
[!] [!] [!] [!] [!] [!] [!]
[!] [!] [!] [!] [!] [!] [!]
[!] [!] [!] [!] [!] [!] [!]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
readme
$ cat readme
awhqfInAbcInaukrpqDycF95h7HoMTzC
$ |
```

Bandit19 -> Bandit20

OverTheWire.org

Wargames Information

SSH Information

Host: bandit13.OverTheWire.org
Port: 2220

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
Level 27 → Level 28
Level 28 → Level 29
Level 29 → Level 29

Bandit Level 19 → Level 20

Level Goal

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (`/etc/bandit_pass`), after you have used the setuid binary.

Helpful Reading Material

setuid on Wikipedia

https://overthewire.org/wargames/bandit/bandit20.html

Log into Bandit19 and first we need to check the owner of the setuid binary.

```
[bandit19@bandit:~] + ~
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root    4096 Apr 23 18:04 .
drwxr-xr-x 78 root      root    4096 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:04 bandit20-do
-rw-r--r--  1 root      root    220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root      root    3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root      root     897 Jan  6 2022 .profile
bandit19@bandit:~$ |
```

The binary just runs another command as a different user when it is executed, as started. This indicates that we have access to the password file for the Bandit20 user, which is only readable by that user.

```
[bandit19@bandit:~] + ~
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root    4096 Apr 23 18:04 .
drwxr-xr-x 78 root      root    4096 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:04 bandit20-do
-rw-r--r--  1 root      root    220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root      root    3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root      root     897 Jan  6 2022 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ |
```

```
[bandit19@bandit:~] + ~
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

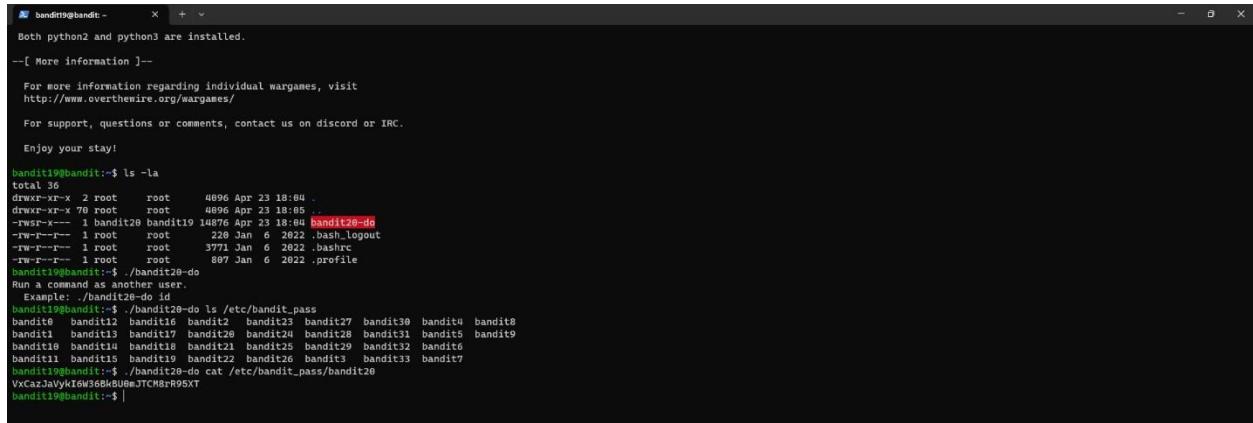
--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root    4096 Apr 23 18:04 .
drwxr-xr-x 78 root      root    4096 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:04 bandit20-do
-rw-r--r--  1 root      root    220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root      root    3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root      root     897 Jan  6 2022 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit6  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit3  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10 bandit11  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit13 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit19@bandit:~$ |
```



A screenshot of a terminal window titled "bandit9@bandit:". The window displays a series of commands and their outputs related to a Bandit challenge. It includes a welcome message from the challenge, a file listing command (ls -la), and a password extraction command (./bandit20-do cat /etc/bandit_pass/bandit20). The terminal ends with a password (VxCazJaVyki636BkBU0eJTCM8rR95XT) and a final prompt.

```
bandit9@bandit: ~ + 
Both python2 and python3 are installed.
--[ More information ]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
bandit9@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root      4096 Apr 23 18:04 .
drwxr-xr-x 70 root      root      4096 Apr 23 18:04 ..
-rw-r--r--  1 bandit20  bandit19 14676 Jan  6 2022 bandit20-id
-rw-r--r--  1 root      root      220 Jan  6 2022 bash.logout
-rw-r--r--  1 root      root      3771 Jan  6 2022 bashrc
-rw-r--r--  1 root      root      807 Jan  6 2022 .profile
bandit9@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit9@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit1  bandit12  bandit13  bandit14  bandit15  bandit16  bandit17  bandit18  bandit19  bandit20  bandit21  bandit22  bandit23  bandit24  bandit25  bandit26  bandit27  bandit28  bandit29  bandit30  bandit31  bandit32  bandit33  bandit34  bandit35  bandit36  bandit37  bandit38  bandit39  bandit40
bandit9@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVyki636BkBU0eJTCM8rR95XT
bandit9@bandit:~$ |
```

Conclusion

I moved to the limits of security as I made my way through the rich pattern of Bandit levels, solving problems that put my skills, creativity, and strength to the test. This investigation has been more than just a practice, it has been a life-changing journey that has expanded my perspectives and strengthened my knowledge of cybersecurity and ethical hacking. In addition to the legal responsibilities that come along with my newfound knowledge, I've learned the value of thorough documentation. My investigation of Bandit levels has expanded not just my knowledge but also my understanding of Linux security. I have not reached the end of my journey in the ethical hacking spirit. It gives an open welcome to everyone who wants to start their own learning and mastering skills missions.

References

1) Medium –

- <https://david-varghese.medium.com/overthewire-bandit-level-16-level-17c137701b3af1>
- <https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-12-level-13e5b687760d15>

2) YouTube –

- <https://www.youtube.com/watch?v=hvSFPyqLizw>
- <https://www.youtube.com/watch?v=H8L0P5oKcP0>

3) OverTheWire - <https://overthewire.org/wargames/bandit/bandit20.html>