



Sri Lanka Institute of Information Technology

System And Network Programming – IE2012

Lab 01

Exploring Bandit Levels

IT22151056

De Silva K.R.K.D

Group – WD.CS 01.02

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 the OverTheWire Bandit0 page. At the top, there's a navigation bar with links for 'Wargames' and 'Information'. On the right, there's a logo for OverTheWire with the tagline 'We're hackers, and we are good-looking. We are the IT!'. Below the navigation, there's a sidebar titled 'SSH Information' with the host 'bandit.labs.overthewire.org' and port '2220'. The main content area is titled 'Bandit' and contains a section for 'Note for beginners'. It explains that the game is aimed at absolute beginners and provides instructions for using the command line, mentioning 'man', 'help', and 'Google'. It also includes a note for VM users about network configuration. A list of level transitions from Level 0 to Level 30 is provided.

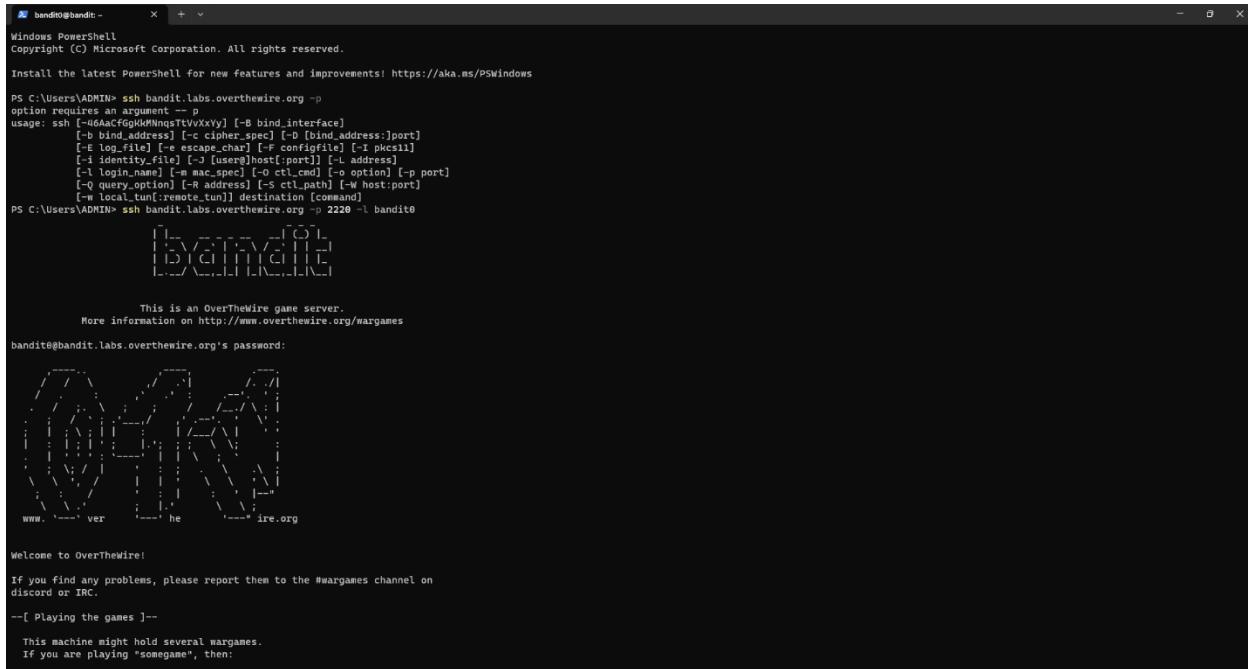
Level	Transition
0	→ Level 1
1	→ Level 2
2	→ Level 3
3	→ Level 4
4	→ Level 5
5	→ Level 6
6	→ Level 7
7	→ Level 8
8	→ Level 9
9	→ Level 10
10	→ Level 11
11	→ Level 12
12	→ Level 13
13	→ Level 14
14	→ Level 15
15	→ Level 16
16	→ Level 17
17	→ Level 18
18	→ Level 19
19	→ Level 20
20	→ Level 21
21	→ Level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

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 the OverTheWire Bandit Level 0 page. The main content area is titled 'Bandit Level 0'. It starts with a 'Level Goal' section stating the objective is to log in using SSH. It then lists 'Commands you may need to solve this level' which includes 'ssh'. Below that is a 'Helpful Reading Material' section with links to 'Secure Shell (SSH) on Wikipedia' and 'How to use SSH on wikiHow'. A sidebar on the left provides SSH information for the host 'bandit.labs.overthewire.org' on port 2220.

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

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



The screenshot shows a Windows PowerShell window titled "bandit0@bandit:". The command entered is "ssh bandit.labs.overthewire.org -p 2220 -l bandit0". The output includes the usage information for the ssh command, followed by a password prompt. The password is displayed as a grid of characters. Below the password, there is a welcome message from OverTheWire, a note about reporting problems, and a hint about playing games. The hint says: "This machine might hold several wargames. If you are playing 'somename', then:"

```
PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit0
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit0
option requires an argument -- p
usage: ssh [-46AaCcGgIiKkNnSsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-F file_address:port]
           [-f log_file] [-g escape_char] [-P configfile] [-I pkeyid]
           [-i identity_file] [-J [useg]host:[port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-s mac_address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit0
[REDACTED]

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

bandit0@bandit.labs.overthewire.org's password:
[REDACTED]

Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
Discord or IRC.
--[ Playing the games ]--
This machine might hold several wargames.
If you are playing 'somename', then:
```

Bandit0 -> 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.

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220
Warning: This level is deleted.

Bandit Level 0 → Level 1

Level Goal

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.

Commands you may need to solve this level

```
ls, cd, cat, file, du, find
```

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 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,noexecro      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/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:~$ ls
readme
bandit@bandit:~$
```

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

```
bandit0@bandit:~      x  +  v
* 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 GUPPI 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 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
NH25XQwC8dpmTEx13bVHNM9H66vVxJL
bandit0@bandit:~$
```

To logout, run “exit”

```
Windows PowerShell      x  +  v
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
NH25XQwC8dpmTEx13bVHNM9H66vVxJL
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

Wargames Information updated

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

Bandit

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

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

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

Now log in to Bandit1, from the found password.

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

```
[bandit@bandit: ~] x + v
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,noexec   disable rlevo

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!
bandit3@bandit:~$ ls
-
bandit3@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.

```
[bandit2@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!
bandit2@bandit:~$ ls
-
bandit2@bandit:~$ cat ./-
xRGiisXaXbK1RTb1cNQoxTcvZwU6lgzi
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

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

bandit2@bandit.labs.overthewire.org's password:
 [REDACTED]
```

Log out using the “exit” command.

Bandit2 -> Bandit3

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

The screenshot shows the OverTheWire Wargames interface at <https://overthewire.org/wargames/bandit/bandit3.html>. The page title is "Bandit Level 2 → Level 3". On the left, there's a sidebar titled "SSH Information" with a host list from bandit.labs.overthewire.org: Port 2220. The main content area contains the following text:

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/mndbd/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 ]--

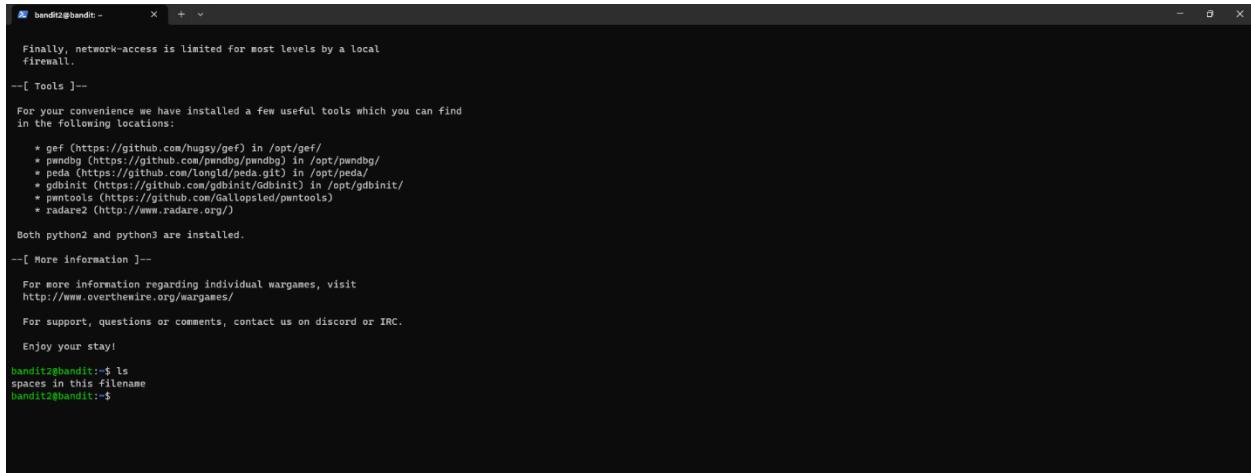
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames

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

Enjoy your stay!

bandit2@bandit: ~$ ls
spaces in this filename
bandit2@bandit: ~$ cat "spaces in this filename"
aBZ956mUFAF7kITQeWdhsbauFJ2lAiG
bandit2@bandit: ~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ADMIN> ssh bandit.labs.overthewire.org -p 2220 -l bandit3
[1]..[2]..[3]..[4]..[5]..[6]..[7]..[8]..[9]..[10]..[11]..[12]..[13]..[14]..[15]..[16]..[17]..[18]..[19]..[20]..[21]..[22]..[23]..[24]..[25]..[26]..[27]..[28]..[29]..[30]..[31]..[32]..[33]..[34]..[35]..[36]..[37]..[38]..[39]..[40]..[41]..[42]..[43]..[44]..[45]..[46]..[47]..[48]..[49]..[50]..[51]..[52]..[53]..[54]..[55]..[56]..[57]..[58]..[59]..[60]..[61]..[62]..[63]..[64]..[65]..[66]..[67]..[68]..[69]..[70]..[71]..[72]..[73]..[74]..[75]..[76]..[77]..[78]..[79]..[80]..[81]..[82]..[83]..[84]..[85]..[86]..[87]..[88]..[89]..[90]..[91]..[92]..[93]..[94]..[95]..[96]..[97]..[98]..[99]..[100]..[101]..[102]..[103]..[104]..[105]..[106]..[107]..[108]..[109]..[110]..[111]..[112]..[113]..[114]..[115]..[116]..[117]..[118]..[119]..[120]..[121]..[122]..[123]..[124]..[125]..[126]..[127]..[128]..[129]..[130]..[131]..[132]..[133]..[134]..[135]..[136]..[137]..[138]..[139]..[140]..[141]..[142]..[143]..[144]..[145]..[146]..[147]..[148]..[149]..[150]..[151]..[152]..[153]..[154]..[155]..[156]..[157]..[158]..[159]..[160]..[161]..[162]..[163]..[164]..[165]..[166]..[167]..[168]..[169]..[170]..[171]..[172]..[173]..[174]..[175]..[176]..[177]..[178]..[179]..[180]..[181]..[182]..[183]..[184]..[185]..[186]..[187]..[188]..[189]..[190]..[191]..[192]..[193]..[194]..[195]..[196]..[197]..[198]..[199]..[200]..[201]..[202]..[203]..[204]..[205]..[206]..[207]..[208]..[209]..[210]..[211]..[212]..[213]..[214]..[215]..[216]..[217]..[218]..[219]..[220]..[221]..[222]..[223]..[224]..[225]..[226]..[227]..[228]..[229]..[230]..[231]..[232]..[233]..[234]..[235]..[236]..[237]..[238]..[239]..[240]..[241]..[242]..[243]..[244]..[245]..[246]..[247]..[248]..[249]..[250]..[251]..[252]..[253]..[254]..[255]..[256]..[257]..[258]..[259]..[260]..[261]..[262]..[263]..[264]..[265]..[266]..[267]..[268]..[269]..[270]..[271]..[272]..[273]..[274]..[275]..[276]..[277]..[278]..[279]..[280]..[281]..[282]..[283]..[284]..[285]..[286]..[287]..[288]..[289]..[290]..[291]..[292]..[293]..[294]..[295]..[296]..[297]..[298]..[299]..[300]..[301]..[302]..[303]..[304]..[305]..[306]..[307]..[308]..[309]..[310]..[311]..[312]..[313]..[314]..[315]..[316]..[317]..[318]..[319]..[320]..[321]..[322]..[323]..[324]..[325]..[326]..[327]..[328]..[329]..[330]..[331]..[332]..[333]..[334]..[335]..[336]..[337]..[338]..[339]..[340]..[341]..[342]..[343]..[344]..[345]..[346]..[347]..[348]..[349]..[350]..[351]..[352]..[353]..[354]..[355]..[356]..[357]..[358]..[359]..[360]..[361]..[362]..[363]..[364]..[365]..[366]..[367]..[368]..[369]..[370]..[371]..[372]..[373]..[374]..[375]..[376]..[377]..[378]..[379]..[380]..[381]..[382]..[383]..[384]..[385]..[386]..[387]..[388]..[389]..[390]..[391]..[392]..[393]..[394]..[395]..[396]..[397]..[398]..[399]..[400]..[401]..[402]..[403]..[404]..[405]..[406]..[407]..[408]..[409]..[410]..[411]..[412]..[413]..[414]..[415]..[416]..[417]..[418]..[419]..[420]..[421]..[422]..[423]..[424]..[425]..[426]..[427]..[428]..[429]..[430]..[431]..[432]..[433]..[434]..[435]..[436]..[437]..[438]..[439]..[440]..[441]..[442]..[443]..[444]..[445]..[446]..[447]..[448]..[449]..[450]..[451]..[452]..[453]..[454]..[455]..[456]..[457]..[458]..[459]..[460]..[461]..[462]..[463]..[464]..[465]..[466]..[467]..[468]..[469]..[470]..[471]..[472]..[473]..[474]..[475]..[476]..[477]..[478]..[479]..[480]..[481]..[482]..[483]..[484]..[485]..[486]..[487]..[488]..[489]..[490]..[491]..[492]..[493]..[494]..[495]..[496]..[497]..[498]..[499]..[500]..[501]..[502]..[503]..[504]..[505]..[506]..[507]..[508]..[509]..[510]..[511]..[512]..[513]..[514]..[515]..[516]..[517]..[518]..[519]..[520]..[521]..[522]..[523]..[524]..[525]..[526]..[527]..[528]..[529]..[530]..[531]..[532]..[533]..[534]..[535]..[536]..[537]..[538]..[539]..[540]..[541]..[542]..[543]..[544]..[545]..[546]..[547]..[548]..[549]..[550]..[551]..[552]..[553]..[554]..[555]..[556]..[557]..[558]..[559]..[560]..[561]..[562]..[563]..[564]..[565]..[566]..[567]..[568]..[569]..[570]..[571]..[572]..[573]..[574]..[575]..[576]..[577]..[578]..[579]..[580]..[581]..[582]..[583]..[584]..[585]..[586]..[587]..[588]..[589]..[590]..[591]..[592]..[593]..[594]..[595]..[596]..[597]..[598]..[599]..[600]..[601]..[602]..[603]..[604]..[605]..[606]..[607]..[608]..[609]..[610]..[611]..[612]..[613]..[614]..[615]..[616]..[617]..[618]..[619]..[620]..[621]..[622]..[623]..[624]..[625]..[626]..[627]..[628]..[629]..[630]..[631]..[632]..[633]..[634]..[635]..[636]..[637]..[638]..[639]..[640]..[641]..[642]..[643]..[644]..[645]..[646]..[647]..[648]..[649]..[650]..[651]..[652]..[653]..[654]..[655]..[656]..[657]..[658]..[659]..[660]..[661]..[662]..[663]..[664]..[665]..[666]..[667]..[668]..[669]..[670]..[671]..[672]..[673]..[674]..[675]..[676]..[677]..[678]..[679]..[680]..[681]..[682]..[683]..[684]..[685]..[686]..[687]..[688]..[689]..[690]..[691]..[692]..[693]..[694]..[695]..[696]..[697]..[698]..[699]..[700]..[701]..[702]..[703]..[704]..[705]..[706]..[707]..[708]..[709]..[710]..[711]..[712]..[713]..[714]..[715]..[716]..[717]..[718]..[719]..[720]..[721]..[722]..[723]..[724]..[725]..[726]..[727]..[728]..[729]..[730]..[731]..[732]..[733]..[734]..[735]..[736]..[737]..[738]..[739]..[740]..[741]..[742]..[743]..[744]..[745]..[746]..[747]..[748]..[749]..[750]..[751]..[752]..[753]..[754]..[755]..[756]..[757]..[758]..[759]..[760]..[761]..[762]..[763]..[764]..[765]..[766]..[767]..[768]..[769]..[770]..[771]..[772]..[773]..[774]..[775]..[776]..[777]..[778]..[779]..[770]..[771]..[772]..[773]..[774]..[775]..[776]..[777]..[778]..[779]..[780]..[781]..[782]..[783]..[784]..[785]..[786]..[787]..[788]..[789]..[790]..[791]..[792]..[793]..[794]..[795]..[796]..[797]..[798]..[799]..[800]..[801]..[802]..[803]..[804]..[805]..[806]..[807]..[808]..[809]..[8010]..[8011]..[8012]..[8013]..[8014]..[8015]..[8016]..[8017]..[8018]..[8019]..[8020]..[8021]..[8022]..[8023]..[8024]..[8025]..[8026]..[8027]..[8028]..[8029]..[8030]..[8031]..[8032]..[8033]..[8034]..[8035]..[8036]..[8037]..[8038]..[8039]..[8040]..[8041]..[8042]..[8043]..[8044]..[8045]..[8046]..[8047]..[8048]..[8049]..[8050]..[8051]..[8052]..[8053]..[8054]..[8055]..[8056]..[8057]..[8058]..[8059]..[8060]..[8061]..[8062]..[8063]..[8064]..[8065]..[8066]..[8067]..[8068]..[8069]..[8070]..[8071]..[8072]..[8073]..[8074]..[8075]..[8076]..[8077]..[8078]..[8079]..[8080]..[8081]..[8082]..[8083]..[8084]..[8085]..[8086]..[8087]..[8088]..[8089]..[80810]..[80811]..[80812]..[80813]..[80814]..[80815]..[80816]..[80817]..[80818]..[80819]..[80820]..[80821]..[80822]..[80823]..[80824]..[80825]..[80826]..[80827]..[80828]..[80829]..[80830]..[80831]..[80832]..[80833]..[80834]..[80835]..[80836]..[80837]..[80838]..[80839]..[80840]..[80841]..[80842]..[80843]..[80844]..[80845]..[80846]..[80847]..[80848]..[80849]..[80850]..[80851]..[80852]..[80853]..[80854]..[80855]..[80856]..[80857]..[80858]..[80859]..[80860]..[80861]..[80862]..[80863]..[80864]..[80865]..[80866]..[80867]..[80868]..[80869]..[80870]..[80871]..[80872]..[80873]..[80874]..[80875]..[80876]..[80877]..[80878]..[80879]..[80880]..[80881]..[80882]..[80883]..[80884]..[80885]..[80886]..[80887]..[80888]..[80889]..[80890]..[80891]..[80892]..[80893]..[80894]..[80895]..[80896]..[80897]..[80898]..[80899]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[808106]..[808107]..[808108]..[808109]..[808110]..[808111]..[808112]..[808113]..[808114]..[808115]..[808116]..[808117]..[808118]..[808119]..[808120]..[808121]..[808122]..[808123]..[808124]..[808125]..[808126]..[808127]..[808128]..[808129]..[808130]..[808131]..[808132]..[808133]..[808134]..[808135]..[808136]..[808137]..[808138]..[808139]..[808140]..[808141]..[808142]..[808143]..[808144]..[808145]..[808146]..[808147]..[808148]..[808149]..[808150]..[808151]..[808152]..[808153]..[808154]..[808155]..[808156]..[808157]..[808158]..[808159]..[808160]..[808161]..[808162]..[808163]..[808164]..[808165]..[808166]..[808167]..[808168]..[808169]..[808170]..[808171]..[808172]..[808173]..[808174]..[808175]..[808176]..[808177]..[808178]..[808179]..[808180]..[808181]..[808182]..[808183]..[808184]..[808185]..[808186]..[808187]..[808188]..[808189]..[808190]..[808191]..[808192]..[808193]..[808194]..[808195]..[808196]..[808197]..[808198]..[808199]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[808106]..[808107]..[808108]..[808109]..[808110]..[808111]..[808112]..[808113]..[808114]..[808115]..[808116]..[808117]..[808118]..[808119]..[808120]..[808121]..[808122]..[808123]..[808124]..[808125]..[808126]..[808127]..[808128]..[808129]..[808130]..[808131]..[808132]..[808133]..[808134]..[808135]..[808136]..[808137]..[808138]..[808139]..[808140]..[808141]..[808142]..[808143]..[808144]..[808145]..[808146]..[808147]..[808148]..[808149]..[808150]..[808151]..[808152]..[808153]..[808154]..[808155]..[808156]..[808157]..[808158]..[808159]..[808160]..[808161]..[808162]..[808163]..[808164]..[808165]..[808166]..[808167]..[808168]..[808169]..[808170]..[808171]..[808172]..[808173]..[808174]..[808175]..[808176]..[808177]..[808178]..[808179]..[808180]..[808181]..[808182]..[808183]..[808184]..[808185]..[808186]..[808187]..[808188]..[808189]..[808190]..[808191]..[808192]..[808193]..[808194]..[808195]..[808196]..[808197]..[808198]..[808199]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[808106]..[808107]..[808108]..[808109]..[808110]..[808111]..[808112]..[808113]..[808114]..[808115]..[808116]..[808117]..[808118]..[808119]..[808120]..[808121]..[808122]..[808123]..[808124]..[808125]..[808126]..[808127]..[808128]..[808129]..[808130]..[808131]..[808132]..[808133]..[808134]..[808135]..[808136]..[808137]..[808138]..[808139]..[808140]..[808141]..[808142]..[808143]..[808144]..[808145]..[808146]..[808147]..[808148]..[808149]..[808150]..[808151]..[808152]..[808153]..[808154]..[808155]..[808156]..[808157]..[808158]..[808159]..[808160]..[808161]..[808162]..[808163]..[808164]..[808165]..[808166]..[808167]..[808168]..[808169]..[808170]..[808171]..[808172]..[808173]..[808174]..[808175]..[808176]..[808177]..[808178]..[808179]..[808180]..[808181]..[808182]..[808183]..[808184]..[808185]..[808186]..[808187]..[808188]..[808189]..[808190]..[808191]..[808192]..[808193]..[808194]..[808195]..[808196]..[808197]..[808198]..[808199]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[808106]..[808107]..[808108]..[808109]..[808110]..[808111]..[808112]..[808113]..[808114]..[808115]..[808116]..[808117]..[808118]..[808119]..[808120]..[808121]..[808122]..[808123]..[808124]..[808125]..[808126]..[808127]..[808128]..[808129]..[808130]..[808131]..[808132]..[808133]..[808134]..[808135]..[808136]..[808137]..[808138]..[808139]..[808140]..[808141]..[808142]..[808143]..[808144]..[808145]..[808146]..[808147]..[808148]..[808149]..[808150]..[808151]..[808152]..[808153]..[808154]..[808155]..[808156]..[808157]..[808158]..[808159]..[808160]..[808161]..[808162]..[808163]..[808164]..[808165]..[808166]..[808167]..[808168]..[808169]..[808170]..[808171]..[808172]..[808173]..[808174]..[808175]..[808176]..[808177]..[808178]..[808179]..[808180]..[808181]..[808182]..[808183]..[808184]..[808185]..[808186]..[808187]..[808188]..[808189]..[808190]..[808191]..[808192]..[808193]..[808194]..[808195]..[808196]..[808197]..[808198]..[808199]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[808106]..[808107]..[808108]..[808109]..[808110]..[808111]..[808112]..[808113]..[808114]..[808115]..[808116]..[808117]..[808118]..[808119]..[808120]..[808121]..[808122]..[808123]..[808124]..[808125]..[808126]..[808127]..[808128]..[808129]..[808130]..[808131]..[808132]..[808133]..[808134]..[808135]..[808136]..[808137]..[808138]..[808139]..[808140]..[808141]..[808142]..[808143]..[808144]..[808145]..[808146]..[808147]..[808148]..[808149]..[808150]..[808151]..[808152]..[808153]..[808154]..[808155]..[808156]..[808157]..[808158]..[808159]..[808160]..[808161]..[808162]..[808163]..[808164]..[808165]..[808166]..[808167]..[808168]..[808169]..[808170]..[808171]..[808172]..[808173]..[808174]..[808175]..[808176]..[808177]..[808178]..[808179]..[808180]..[808181]..[808182]..[808183]..[808184]..[808185]..[808186]..[808187]..[808188]..[808189]..[808190]..[808191]..[808192]..[808193]..[808194]..[808195]..[808196]..[808197]..[808198]..[808199]..[808100]..[808101]..[808102]..[808103]..[808104]..[808105]..[
```

Using the “ls” command find the file name.



```
bandit2@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 ]--

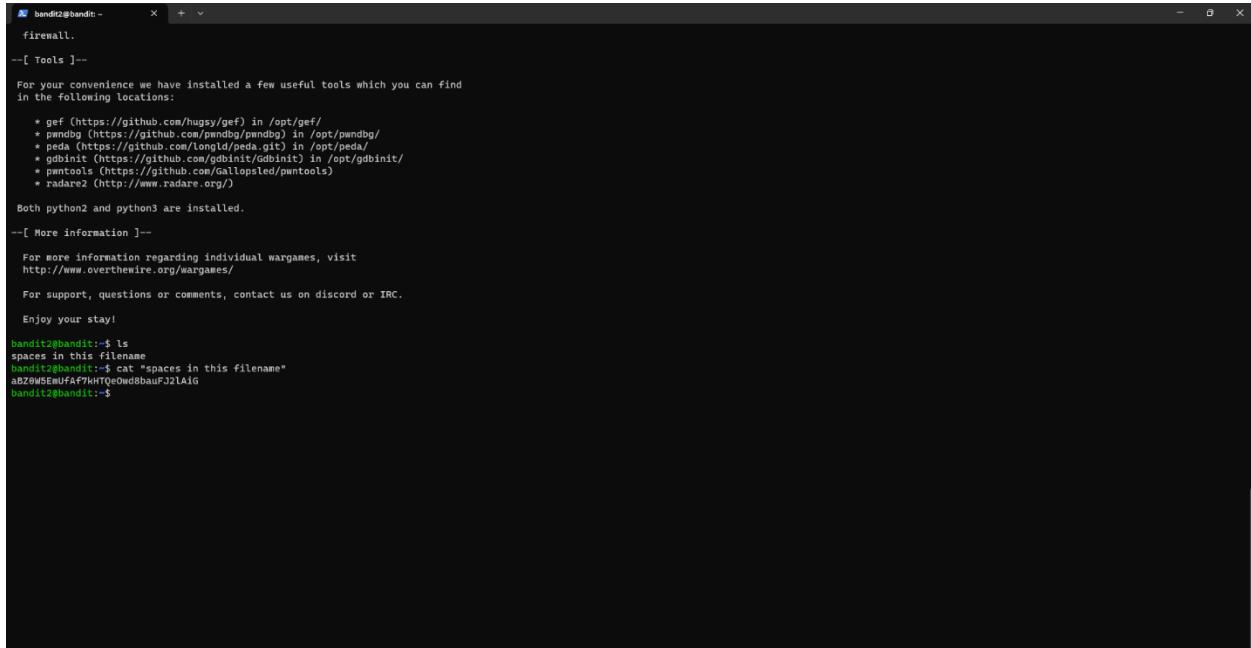
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

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  +  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/

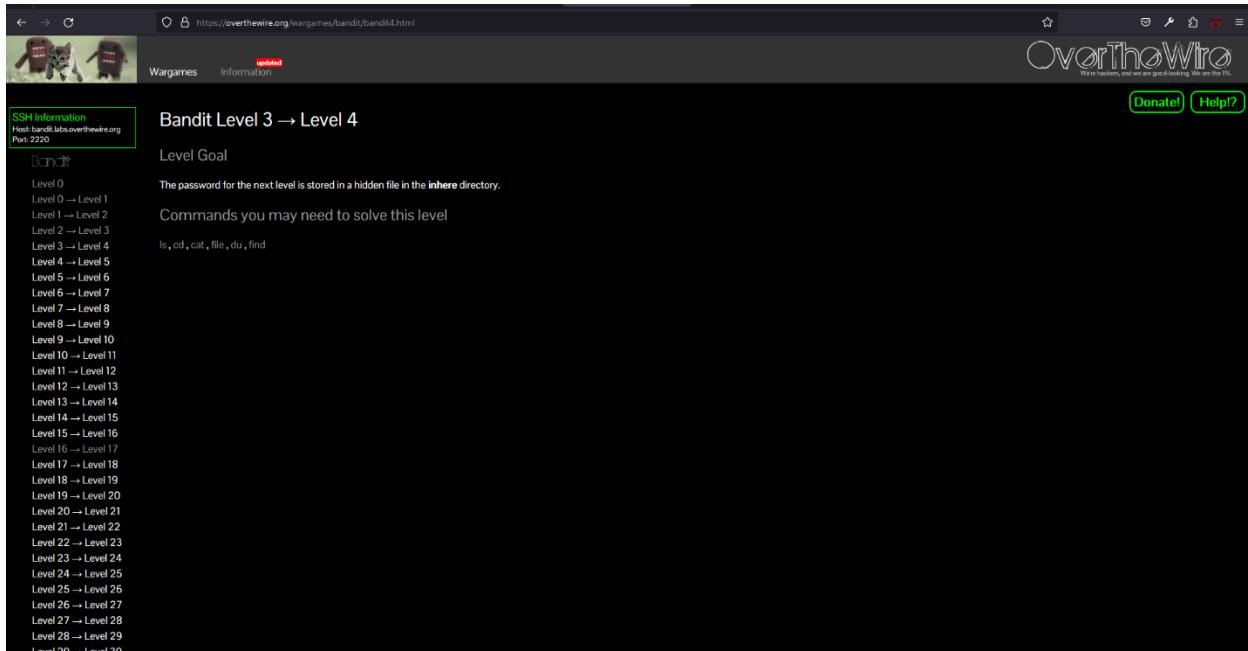
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBZ9WSEmUfA7kHtQeOwdsbauFJ2lAig
bandit2@bandit:~$
```

Bandit3 -> Bandit4

Log Bandit 3 to use the password.



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

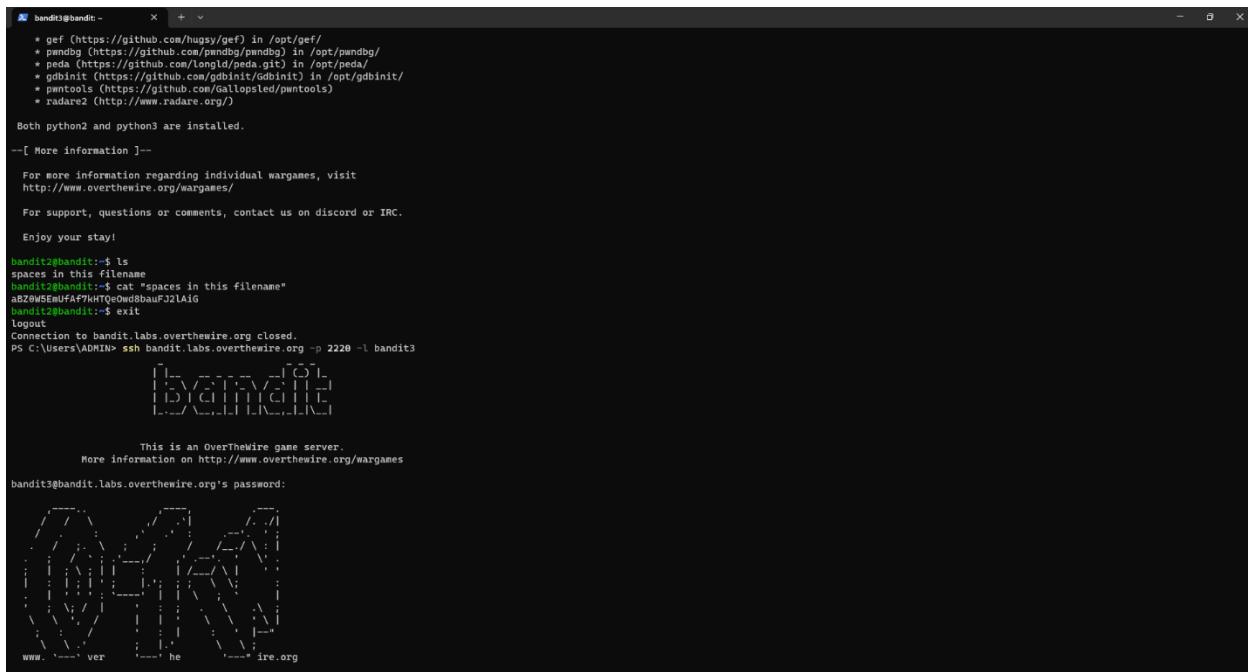
Level Goal

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

Commands you may need to solve this level

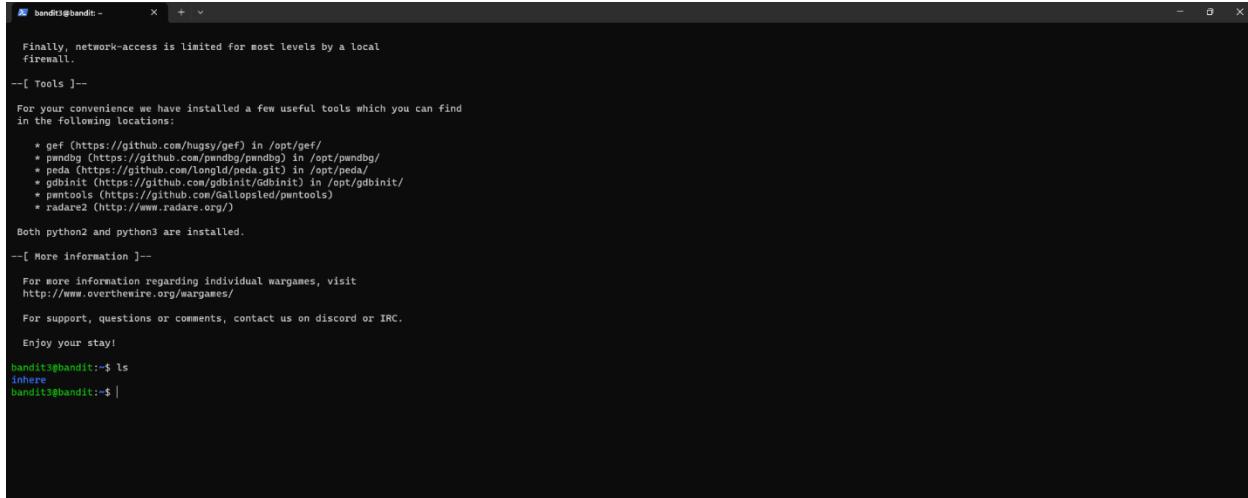
ls, cd, cat, file, du, find

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
+ ... 20 → ... 49



```
bandit3@bandit:~ [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"  
aBZ05EfUFAf7kHtQe0wdhsauFJ2lAiG  
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]
```

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/
* pwnools (https://github.com/Gallopsled/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

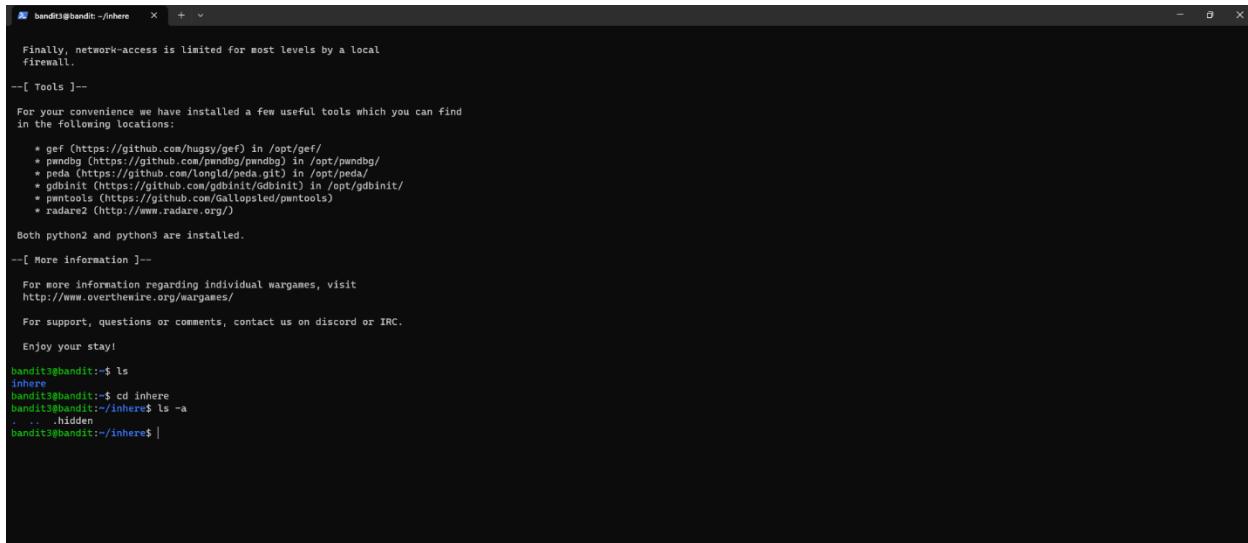
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

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

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/
* 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$ |
```

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
2EW7B8t6AMK02H2Wb67mB9gX26xKe
bandit3@bandit:~/inhere$
```

Bandit4 -> Bandit5

SSH Information
Host: bandit5.OverTheWire.org
Port: 2220

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
- 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

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

```
bandit4@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!

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

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

```
bandit4@bandit:~/inhere + - 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!

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$
```

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

```
bandit4@bandit:~/inhere + - 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 ]--

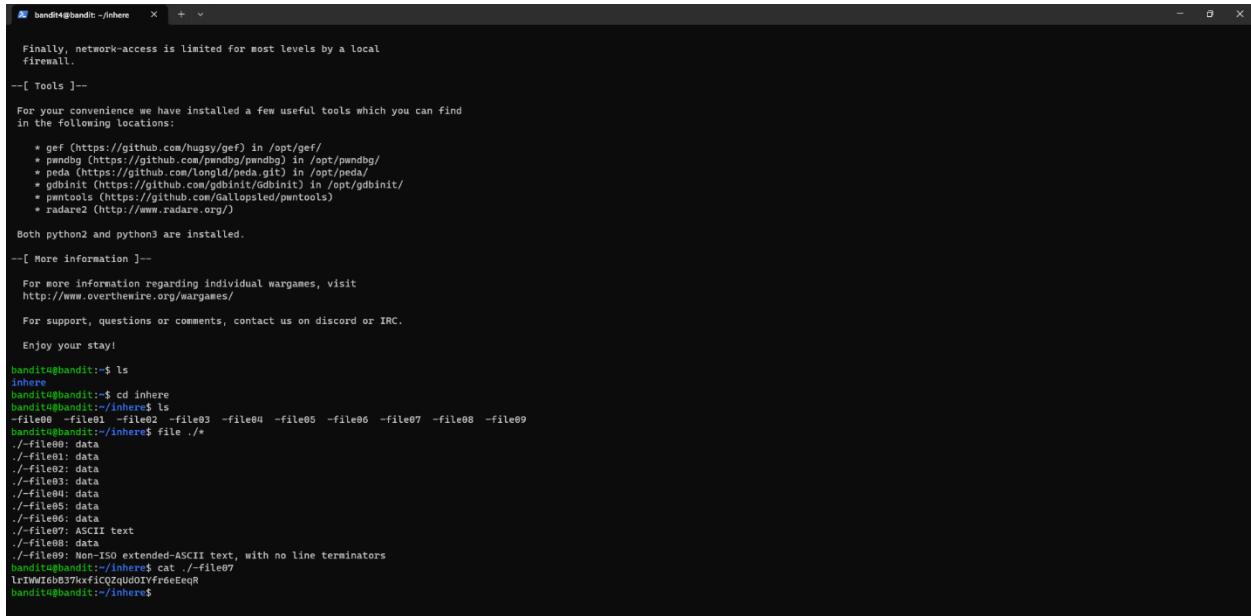
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

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: data
./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
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/mnndbg/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

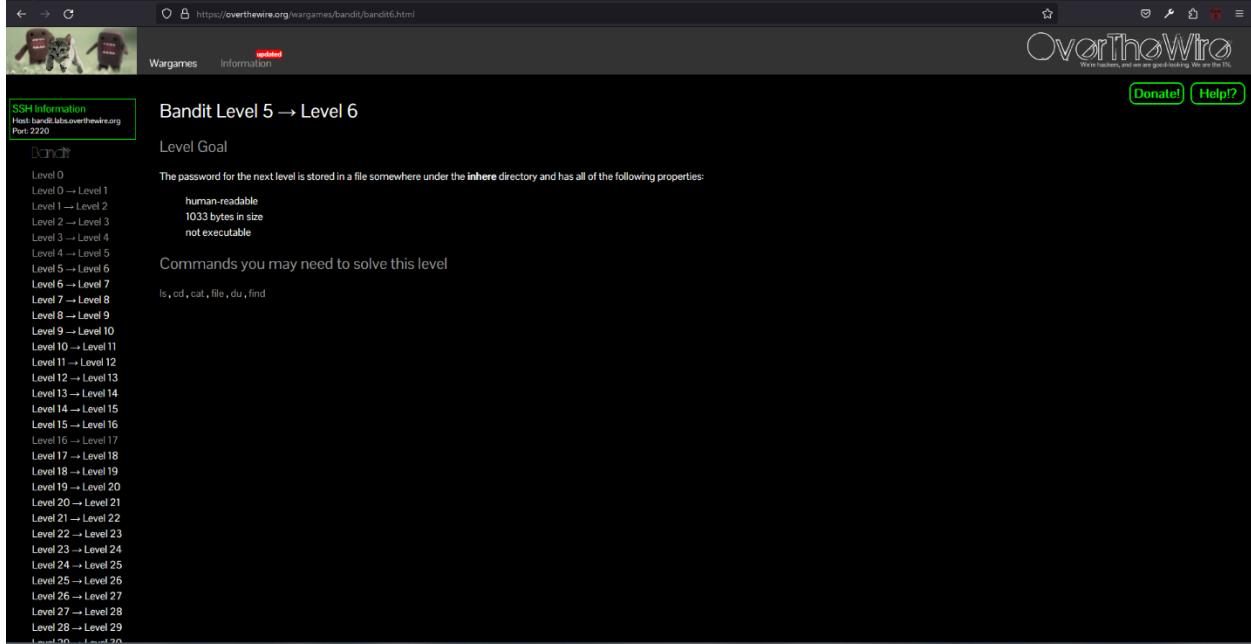
For support, questions or comments, contact us on discord or IRC.

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: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, build-id [REDACTED]
./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$ cat ./file07
lrvWt6B37KxfICQzQdDfYfrGeEqR
bandit4@bandit:~/inhere$
```

Bandit05 -> Bandit06

Log in to Bandit05 using the password.

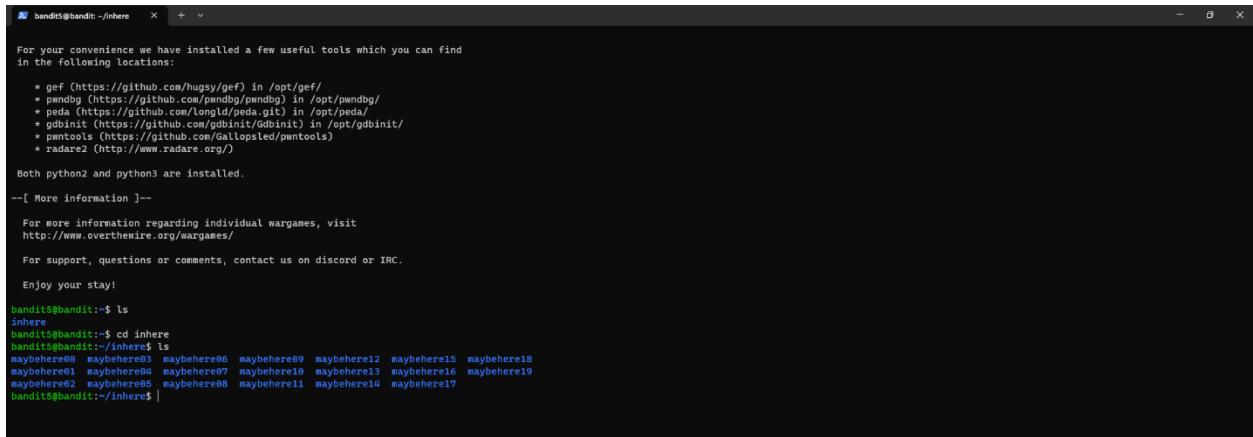


SSH Information
Host bandit5.OverTheWire.org
Port 2220

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

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
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/huguy/gef) in /opt/gef/
* pwndbg (https://github.com/mnndbg/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 ]--

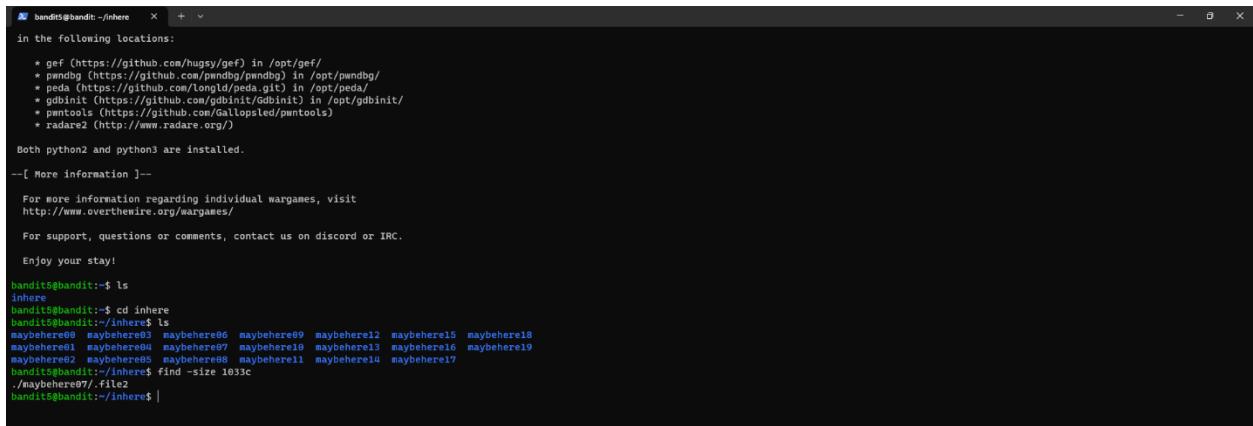
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~/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
in the following locations:
* gef (https://github.com/huguy/gef) in /opt/gef/
* pwndbg (https://github.com/mnndbg/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 ]--

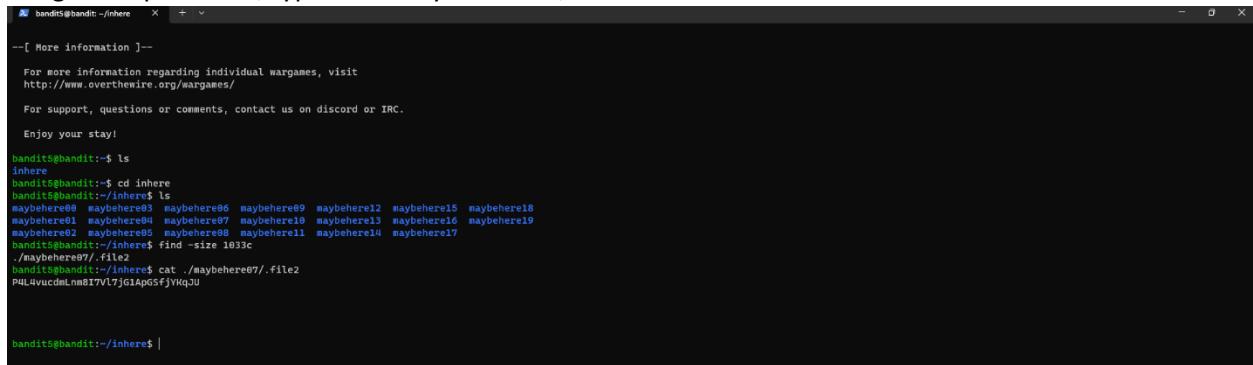
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~/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”



```
--[ 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:~/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
PwL4vucdmLnm8T7Vl7jGIApGSfjYKqJU

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

Bandit6 -> Bandit7

The screenshot shows the OverTheWire Wargames interface. At the top, there's a navigation bar with links for 'Wargames' and 'Information'. On the right, there's a logo for OverTheWire with the tagline 'We're hackers, and we are good-looking. We are the 1%.' Below the navigation, there's a green box titled 'SSH Information' containing the host information: 'Host bandit6.OverTheWire.org' and 'Port 2220'. A 'Donate!' button and a 'Help?' link are also present.

Bandit Level 6 → Level 7

Level Goal

The password for the next level is stored somewhere on the server and has all of the following properties:

- 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

Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

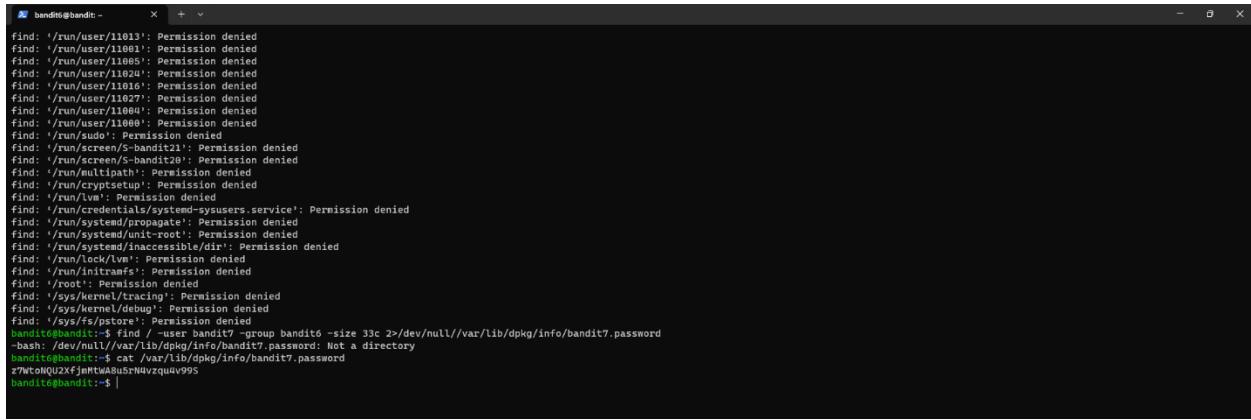
Log into the Bandit6 using the password. Use the root directory command to search the system.

The terminal window shows a user named 'bandit6' running a 'find' command with specific permissions and size constraints. The command is as follows:

```
bandit6@bandit6:~$ find / -user bandit7 -group bandit6 -size 33c
```

The output of the command shows numerous errors indicating permission denied for various system files and directories, such as '/var/log', '/var/crash', '/var/spool/rsyslog', '/var/spool/bufrit24', '/var/spool/cron/crontabs', '/var/tmp', '/var/lib/polkit-1', '/var/lib/polkit-agent-helper-1', '/var/lib/apt/lists/partial', '/var/lib/amazon', '/var/lib/update-notifier/package-data-downloads/partial', '/var/lib/snapd/void', '/var/lib/snapd/cookie', '/var/lib/ubuntu-adantage/apt-esm/var/lib/apt/lists/partial', '/var/lib/private', '/var/cache/ldconfig', '/var/cache/ldconfig/partial', '/var/cache/apt/archives/partial', '/var/cache/pollinate', '/var/cache/private', '/var/cache/apparmor/uidd848e:0', '/var/cache/apparmor/beeb6286:0', '/drifter/drifter4_src/axTLS', '/home/bandit29-git', '/home/bandit29-drifted', '/home/bandit28-git', '/home/bandit28-drifted', '/home/drifter8/chroot', '/home/ubuntu', '/home/bandits/inhere', '/home/bandit27-git', '/home/bandit27-drifted', '/home/bandit26-git', '/home/bandit26-drifted', '/proc/tty/driver', '/proc/271937/task/271937/fd/6', '/proc/271937/task/271937/fdinfo/6', '/proc/271937/fd/5', '/proc/271937/fdinfo/5', '/etc/polkit-1/localauthority', '/etc/polkit-1/localauthority/6', '/etc/polkit-1/localauthority/6/auth', '/etc/sudoers.d', '/etc/sudoers', '/dev/queue', '/dev/shm', '/tmp', '/snap', '/lost+found', '/run/chrony', '/run/user/11028'.

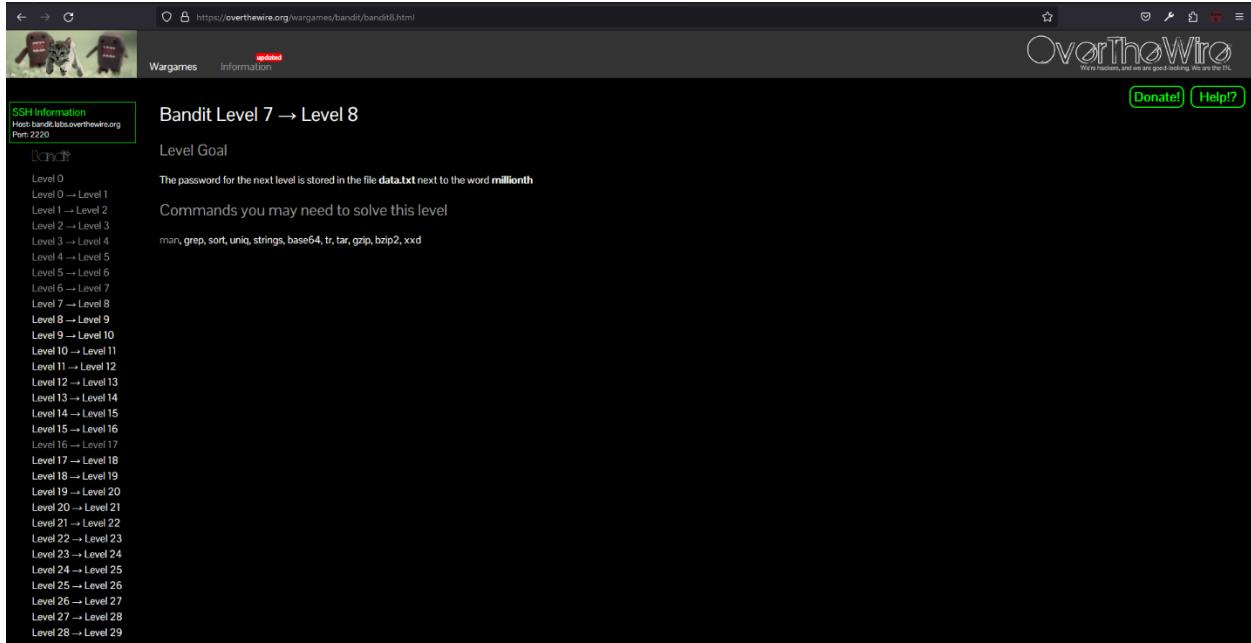
Type this command “cat /var/lib/dpkg/info/bandit7.password” and find the password.



```
bandit6@bandit:~
```

```
find: '/run/user/1001': Permission denied
find: '/run/user/1001': Permission denied
find: '/run/user/1008': Permission denied
find: '/run/user/1008': Permission denied
find: '/run/user/10016': Permission denied
find: '/run/user/10027': Permission denied
find: '/run/user/10004': Permission denied
find: '/run/user/10004': Permission denied
find: '/run/screen/5-bandit21': Permission denied
find: '/run/screen/5-bandit20': Permission denied
find: '/run/multipath': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/credentials/systemd-sysusers.service': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/inaccessible/fir': Permission denied
find: '/run/lock/lv*': Permission denied
find: '/run/initramfs': Permission denied
find: '/root': Permission denied
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
bandit6@bandit:~$ find -user bandit7 -group bandit7 -size 33c 2>/dev/null //var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat //var/lib/dpkg/info/bandit7.password
z7tCnQ2XfJmTkw8usrnM4vzquuv99s
bandit6@bandit:~$
```

Bandit7 -> Bandit8



The screenshot shows a web browser displaying the OverTheWire Wargames Bandit7 level page. The URL is https://overthewire.org/wargames/bandit/bandit8.html. The page includes navigation links for 'Bandit', 'Wargames', and 'Information'. A green box on the left contains 'SSH Information' with the host being bandit8s overthewire.org and port 2220. The main content area is titled 'Bandit Level 7 → Level 8' and includes a 'Level Goal' section stating 'The password for the next level is stored in the file data.txt next to the word millionth'. It also lists 'Commands you may need to solve this level' such as man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd. A sidebar on the right features the OverTheWire logo and links for 'Donate' and 'Help?'

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      TESKZC8XVtETH059xHmZ5Tkh5iWr8V
bandit7@bandit:~$ |
```

Bandit8 -> Bandit9

SSH Information
Host bandit8.labs.overthewire.org
Port 2220

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

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

Helpful Reading Material
Piping and Redirection

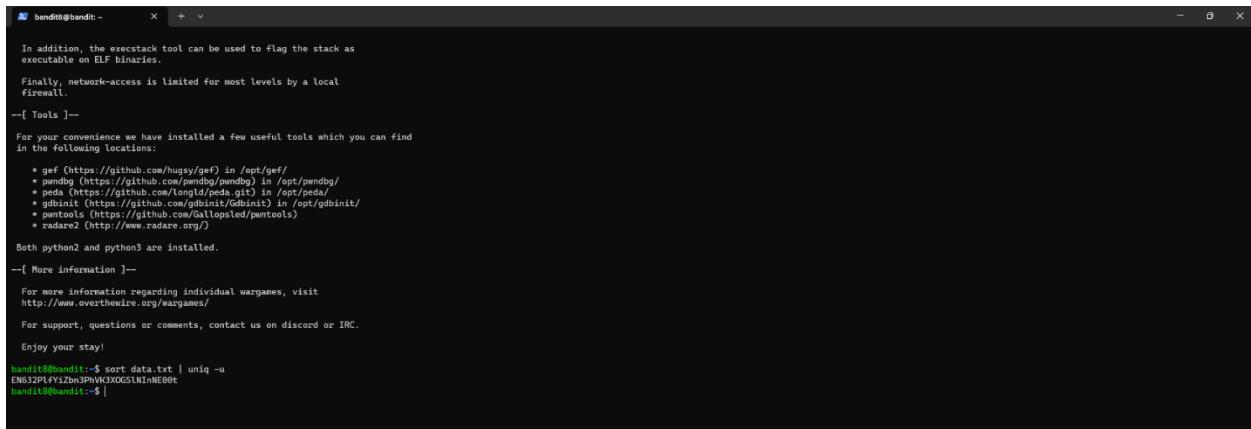
Log into Bandit8 using the password.

```
PS C:\Users\ADMIN> ssh bandit8.labs.overthewire.org -p 2220 -l bandit8
[bandit8@bandit8 ~]$ This is an OverTheWire game server.
[bandit8@bandit8 ~]$ More information on http://www.overthewire.org/wargames
[bandit8@bandit8 ~]$ bandit8@bandit8.labs.overthewire.org's password:
[bandit8@bandit8 ~]$ Welcome to OverTheWire!
[bandit8@bandit8 ~]$ If you find any problems, please report them to the #wargames channel on
[bandit8@bandit8 ~]$ discord or IRC.
[bandit8@bandit8 ~]$ --[ Playing the games ]--
[bandit8@bandit8 ~]$ This machine might hold several wargames.
[bandit8@bandit8 ~]$ If you are playing "somegame", then:
[bandit8@bandit8 ~]$ * USERNAMES are somegame1, somegame1, ...
[bandit8@bandit8 ~]$ * Most LEVELS are stored in /somegame/
[bandit8@bandit8 ~]$ * PASSWORDS for each level are stored in /etc/somegame_pass/
[bandit8@bandit8 ~]$ Write-access to homedirectories is disabled. It is advised to create a
[bandit8@bandit8 ~]$ working directory with a hard-to-guess name in /tmp/. You can use the
[bandit8@bandit8 ~]$ command "mktemp -d" in order to generate a random and hard to guess
[bandit8@bandit8 ~]$ directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
[bandit8@bandit8 ~]$ restricted so that users cannot snoop on other users. Files and directories
[bandit8@bandit8 ~]$ created by you will be periodically deleted, the /tmp
[bandit8@bandit8 ~]$ directory is regularly wiped.
[bandit8@bandit8 ~]$ Please play nice:
[bandit8@bandit8 ~]$ * don't leave orphan processes running
[bandit8@bandit8 ~]$ * don't leave exploit-files laying around
[bandit8@bandit8 ~]$ * don't annoy other players
[bandit8@bandit8 ~]$ * don't post passwords or spoilers
[bandit8@bandit8 ~]$ * again, DON'T POST SPOILERS!
```

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.



```
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 ]--

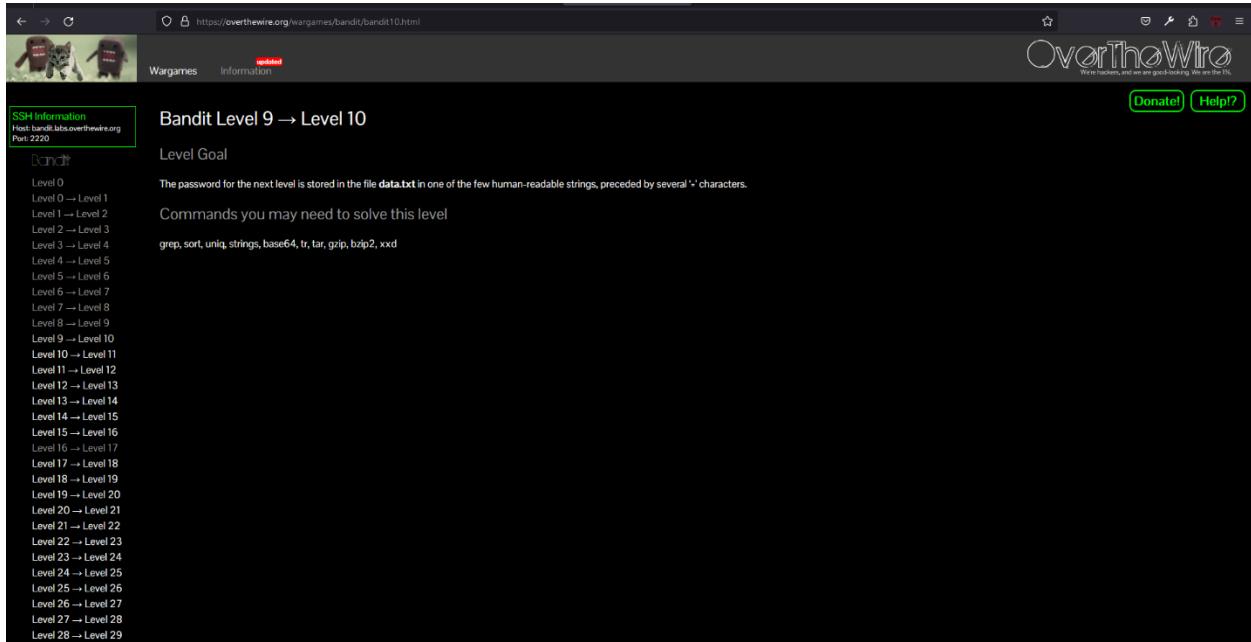
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

bandit9@bandit:~$ sort data.txt | uniq -u
EN32PLYz1bm3PnVK3XG5tN1nNE80t
bandit9@bandit:~$
```

Bandit9 -> Bandit10



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

Level Goal

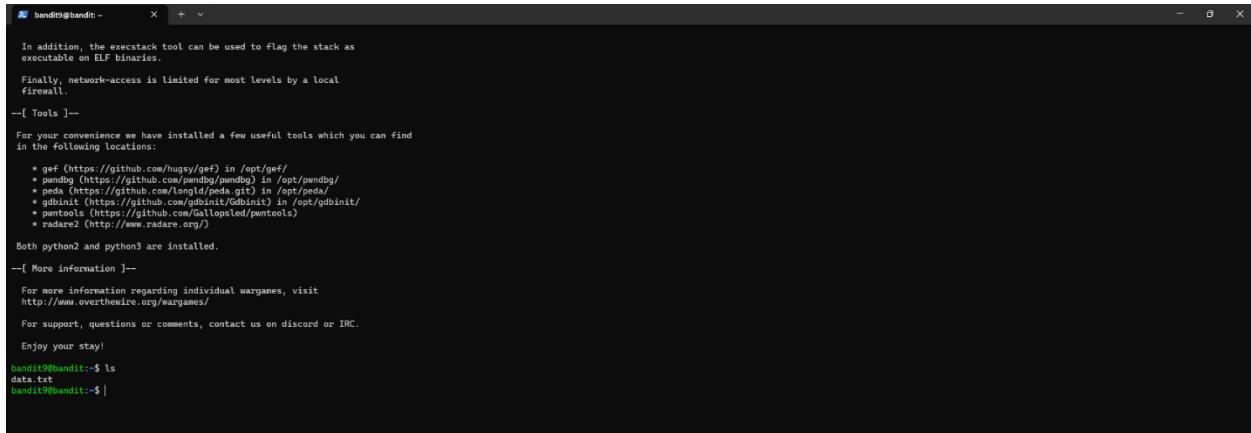
The password for the next level is stored in the file `data.txt` in one of the few human-readable strings, preceded by several '-' characters.

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

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

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



```
bandit9@bandit:~      X  +  v
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/tongld/peda.git) in /opt/peda/
* gdbinit (https://github.com/Gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsted/pwnools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

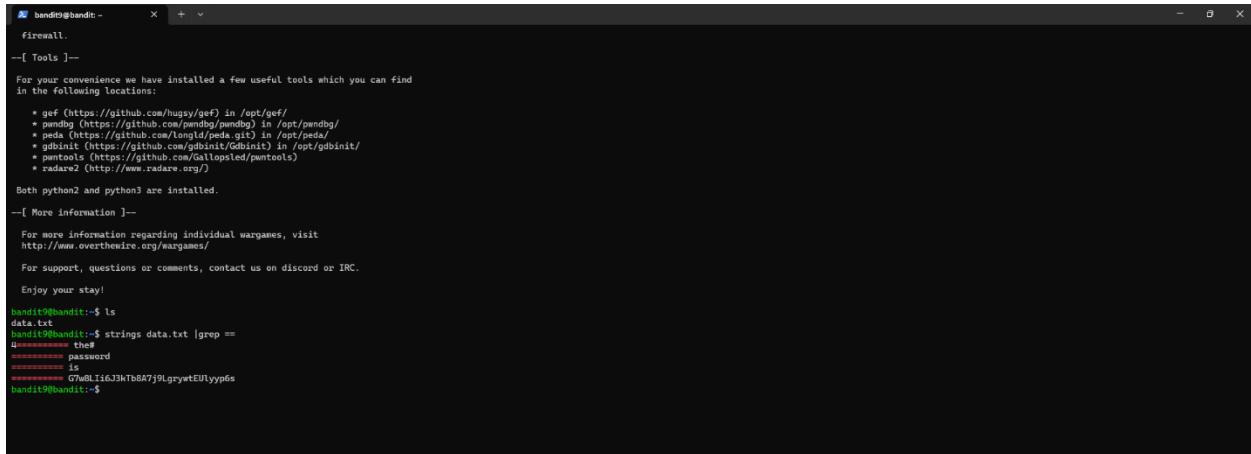
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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  +  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/tongld/peda.git) in /opt/peda/
* gdbinit (https://github.com/Gdbinit/Gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsted/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 ==
===== the#
===== password
===== is
===== G7wBL16J3hTb8A7j9LgrywtEUYpp6s
bandit9@bandit:~$ |
```

Bandit10 -> Bandit11

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit11.html>. The page title is "Bandit Level 10 → Level 11". On the left, there's a sidebar titled "SSH Information" with the host "bandit10s.OverTheWire.org" and port "2220". Below it is a "Level Goal" section with a large list of levels from 0 to 29. To the right, there's a "Commands you may need to solve this level" section listing various Unix commands like grep, sort, uniq, strings, base64, tr, tar, gzip, bzcat, and xxd. At the bottom, there's a "Helpful Reading Material" section with a link to "Base64 on Wikipedia". The OverTheWire logo is at the top right.

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

The screenshot shows a terminal window with the prompt "bandit10@bandit:". The user has run the "cat data.txt" command, which outputs the following base64 encoded string:

```
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/gallopted/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!

bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGZlZGUGV6auXkJUjJS5e5kTllGtMIZblZD53pmaGxSEJNCg==
bandit10@bandit:~$ |
```

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

```

bandit10@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/
* pmdbg (https://github.com/andrewsmadhaven/pmdbg)
* 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!

bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlIDZ6UGV6auXkUjJSS05KllGTmI2blZDS3pmaGxYSEJNCg==
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezilDr2RNdnNYFnB6nVCKzphLXHBM
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.

```

bandit11@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!

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

```

Use the “cat” command to get the password.

```

bandit11@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!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIaOOSFzMjXXBC0Ko5KbbJ8puQm5lxEi
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
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 WIaOOSFzMjXXBC0Ko5KbbJ8puQm5lxEi
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
Tgd ozzrvnqc hr JVWBBS1sZwK0P0kafX0nwBgbDySxRv
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBS1sZwK0P0kafX0nwBgbDz5yVrV
bandit11@bandit:~$ |

```

Bandit12 -> Bandit13

Log into Bandit12 using the password.

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit13.html>. The page title is "Bandit Level 12 → Level 13". On the left, there's a sidebar titled "SSH Information" with the host "bandit12s.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 reading a hex dump file named "data.txt". It also lists commands like grep, sort, uniq, strings, base64, tr, tar, gzip, bzzip2, xxd, mkdir, cp, mv, file, and provides links to Wikipedia and a hex dump guide. A "Helpful Reading Material" section is also present.

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

The terminal window shows a root shell on "bandit12@bandit:~". The user runs "cat data.txt" and sees the message "Finally, network-access is limited for most levels by a local firewall.". The user then runs "ls" and sees a list of tools: gef, pwndbg, peda, gdbinit, pwnools, and radare2. The user runs "cd /tmp/pc" and "ls" again to verify the directory exists. The terminal ends with a prompt "bandit12@bandit:/tmp/pc\$ |".

```
bandit12@bandit:~$ 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/
* 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!

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

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 ~ + ~
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!

bandit12@bandit:~$ cp data.txt /tmp/pc
bandit12@bandit:~$ cd /tmp/pc
bandit12@bandit:~/tmp/pc$ ls
data8.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data8.data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ file myfile.txt
myfile: ASCII text
bandit12@bandit:~/tmp/pc$ file myfile.txt
myfile.txt: ASCII text
bandit12@bandit:~/tmp/pc$
```

Run the “cat myfile.txt”

```
bandit12@bandit:~/tmp/pc ~ + ~
myself.txt: cannot open 'myfile.txt' (No such file or directory)
bandit12@bandit:~/tmp/pc$ file myfile.txt
myfile: ASCII text
bandit12@bandit:~/tmp/pc$ cat myfile.txt
00000000: 1f8b 0808 2773 0561 0203 6461 322e ...sEd..data2.
00000010: 6269 6000 0145 02ba fd42 5a60 3931 4159 bin.E..BZ91AY
00000020: 2653 597b 4f96 5f08 0018 ffff fd6f c7ed $SY10.....0..
00000030: bf7f beff 9fd8 d7ca ffcb edff 8def dfd7 .....0.....
00000040: bf7f bfff bfdb ffbb ff9f b001 3b56 .....;V
00000050: 0404 0068 0064 3400 d341 a000 0600 0659 ..h.dA.A.....
00000060: 0008 0000 0000 1a00 1a00 0034 0035 03d0 ..h..dA.A.....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 ..h..dA.A.....
00000080: 1a68 060d 3a03 4006 8d00 0c80 00f5 0003 h..4.M.....
00000090: 4031 3119 00d0 1a68 1a34 c861 4640 00d0 @11...h.4.FB..
000000a0: 0007 a80d 00d0 00e9 a300 d934 0341 a000 .....@.A..
000000b0: 0699 07a9 881e a8d9 d488 6834 0c43 486c .....h.C@h
000000c0: 6432 0340 0c80 6800 0346 8006 8000 d831 d2.0..h..F....4
000000d0: 0001 f0e1 810e 1958 b752 927c 0406 4820 .....X..d.B.
000000e0: 0007 0007 0007 0007 0007 0007 0007 0007 ..h..dA.A.....
000000f0: 41f4 1207 661d b593 0705 3d87 0600 0420 ..h..dA.A.....
00000100: 1907 e883 0b65 6077 a547 e963 7810 29f9 G.....w.B..x.).
00000110: 429d e1d7 ad8b 0078 056b e37c 06df 4917 B.....x.w.I..I.
00000120: 9b46 f69d 0473 88b4 edc2 e10 04e3 3e52 .F..Ds.....R
00000130: dd34 2244 08cb 5e64 9314 9521 505e e767 ^D..^d..P^g
00000140: 9821 d629 857e 9ce2 dice d44f 5e51 f6d0 .I.).....O...
00000150: d918 de31 f1f5 d149 4695 9397 0600 f046 ..1..IF..7.K.F
00000160: 0000 0000 0000 0000 0000 0000 0000 0000 ..h..dA.A.....
00000170: 6cc4 205b 8d45 0000 0000 0000 0000 0000 ..h..dA.A.....
00000180: 0806 adaa 3b5a a894 a794 1f93 c588 b160 HF.....w.B..x.).
00000190: 016e 2580 2c74 643b 5004 0150 751c 33b1 ..%.td;PFATU.3.
000001a0: c380 53d8 a959 5fdc 6c12 f2bd 02f3 2d83 ..S..Y..l.....-
000001b0: b965 3188 003c b997 0156 e950 9d00 04ff ..e1.<.AV.B.Id.
000001c0: da44 2d5b aaea 5365 27c8 1e79 8109 5f3d J..-.Se'.Y..1
000001d0: c184 46c9 7ba5 f923 5ea1 6681 f058 226e .F.t..#..h..X\l
000001e0: 5d01 5d01 0000 0000 0000 0000 0000 0000 =.A..f..w..D.Zo
000001f0: 0010 140b 2500 0000 0014 8af5 0cf1 0077 ..A..s.....R
00000200: ad30 3388 0677 6552 9940 3780 7d85 1f68 ..3..w@R.17.).
00000210: f287 1238 7639 11e2 file 0830 7500 2562 ..8.W...H.u%.
00000220: 7d64 20ff 1a69 0085 0b4c bdd6 1231 a512 ].$.i..M..1..
00000230: f9fb 109c e7ea d932 98fd eb76 f4f8 fa29 .....2...V...)
00000240: 967c e152 9c69 c607 6207 eaef 2095 0441 .J.R.i.b....A.
00000250: a604 9ffc 5dc9 14e1 4241 ed3e 597c 9f2e ..N..).BA.+Y|..
00000260: f0c8 4502 0000 ..E...
```

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

```

bandit12@bandit:~/tmp/pc ~ + v
00000009: a107 6102 a076 3683 a756 3ba9 1b98 e034 .Ga_B.-6..V;....I.
0000000f: 41fd 12d7 661d b380 00b7 cd8c b23e bdb2 A..Gf;.....>.
00000010: 1947 e803 00e5 6077 a542 e0ea 7810 29f6 .G.....w.B..x.)..
00000011: 429d e1d7 ad8b 0078 056b e37c 06df 4917 B.....x.k..I..I.
00000012: 9b46 f69d 0473 88b4 edc2 e10 4e3 3e52 .F..Ds.....R
00000013: dd34 2244 88cb 5e64 9314 9521 5656 8767 .4'D..d..P^g
00000014: 9803 1a18 6095 9295 8056 5605 f6d1 .(.).....O^...
00000015: 1a18 6095 9295 8056 5605 f6d1 .(.).....O^...
00000016: 789d 1bd9 ca69 11e8 2c94 3299 409e 8511 X.....1..2..I..
00000017: 6cad 2b5b edc8 r491 3794 5978 58c3 L. [....F.YX.
00000018: 4846 a0a9 3ba5 a89a a794 1ff9 1c88 8161 HF.....;....'.
00000019: 016e 2504 2c74 643b 5096 0154 7513 33b1 .n..td;PFATU.3.
0000001a: c3e5 53d8 a959 5fdc 6c12 f2b0 02f3 3db3 ..S..Y..l.....".
0000001b: b949 3188 0d3c b697 015e 9598 9d49 04f6 .el.<.AV.P.Id.
0000001c: dada 2080 0085 4bdc ebdb 1231 a512 ].$.i..Kl..1..
0000001d: 5365 276e 0179 0085 4bdc ebdb 1231 a512 ].$.i..Kl..1..
0000001e: 967c e152 9c69 c697 6207 eaef 2095 94a1 ].R.i.b...A
0000001f: d466 7c63 e088 048c 5a6f =.].fm.D.Zo
0000001f: 2c10 41b8 0288 108a 0018 8af4 0fc4 8bf7 ,.A.B.....
00000020: ad34 3388 0477 6552 9849 378e 7d80 1fd8 .43.@wE.R.I7.}...
00000021: f201 4049 4077 6552 9849 378e 7d80 1fd8 ..8v9....H;uH%.
00000022: 7de4 24ff 1a69 0085 4bdc ebdb 1231 a512 ].$.i..Kl..1..
00000023: f9fb 109c e7ea d932 98fd eb76 f4f8 fa29 .....2..V...).
00000024: 967c e152 9c69 c697 6207 eaef 2095 94a1 ].R.i.b...A
00000025: a64e 9ffc 5dc9 14e1 4241 ed3e 597c 9f2e ].N..).BA;>Y|..
00000026: fcc8 4562 0000 ..E..
bandit12@bandit:~/tmp/nc xxd -r myfile.txt >myfile1.bin
bandit12@bandit:~/tmp/nc ls
data8.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data8.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/pc$ |

```

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 ~ + v
00000020: ad34 3308 0477 6552 9849 378e 7d80 1fd8 .43.@wE.R.I7.}...
00000021: f201 4049 4077 6552 9849 378e 7d80 1fd8 ..8v9....H;uH%.
00000022: 7de4 24ff 1a69 0085 4bdc ebdb 1231 a512 ].$.i..Kl..1..
00000023: f9fb 109c e7ea d932 98fd eb76 f4f8 fa29 .....2..V...).
00000024: 967c e152 9c69 c697 6207 eaef 2095 94a1 ].R.i.b...A
00000025: a64e 9ffc 5dc9 14e1 4241 ed3e 597c 9f2e ].N..).BA;>Y|..
00000026: fcc8 4562 0000 ..E..
bandit12@bandit:~/tmp/nc xxd -r myfile.txt >myfile1.bin
bandit12@bandit:~/tmp/nc ls
data8.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data8.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/nc file myfile.bin
myfile.bin: cannot open 'myfile.bin' (No such file or directory)
bandit12@bandit:~/tmp/nc zcat myfile1.bin >myfile2
bandit12@bandit:~/tmp/nc ls
data8.bin data8.bin myfile1.bin myfile3 myfile7 myfile.txt
data8.bin data.txt myfile2 myfile4 myfile9
bandit12@bandit:~/tmp/nc file myfile2
myfile: cannot open 'myfile2' (No such file or directory)
bandit12@bandit:~/tmp/nc file myfile2
myfile2: bzip2 compressed data, block size = 900k
bandit12@bandit:~/tmp/nc bzcat myfile2 >myfile3
bandit12@bandit:~/tmp/nc file myfile3
myfile3: gzip compressed data, was "data8.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 20488
bandit12@bandit:~/tmp/nc xcat myfile3 >myfile4
Command 'xcat' not found, but there are 22 similar ones.
bandit12@bandit:~/tmp/nc zcat myfile3 >myfile4
bandit12@bandit:~/tmp/nc file myfile4
myfile4: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/nc tar -xvf myfile4
data8.bin
bandit12@bandit:~/tmp/nc file data8.bin
data8.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~/tmp/nc bzcat data8.bin >myfile7
bandit12@bandit:~/tmp/nc file myfile7
myfile7: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/nc tar -xvf myfile7
data8.bin
bandit12@bandit:~/tmp/nc file data8.bin
data8.bin: gzip compressed data, was "data8.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:~/tmp/nc zcat data8.bin >myfile9
bandit12@bandit:~/tmp/nc file myfile9
myfile9: ASCII text
bandit12@bandit:~/tmp/nc cat myfile9
The password is wbmwlxleir4CaEBLaPhauuoOpwRmrDw
bandit12@bandit:~/tmp/pc$ |

```

Bandit13 -> Bandit14

The screenshot shows a web browser window for the OverTheWire Wargames Bandit14 level. The URL is https://overthewire.org/wargames/bandit/bandit14.html. The page has a dark header with the OverTheWire logo and navigation links for Wargames and Information. A green sidebar on the left contains "SSH Information" for host bandit14 overthewire.org on port 2220. The main content area displays the title "Bandit Level 13 → Level 14" and a "Level Goal" section. It states that the password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14. It also notes that localhost is a hostname that refers to the machine you are working on. Below this is a "Commands you may need to solve this level" section listing various tools: ssh, telnet, nc, openssl, s_client, nmap. A "Helpful Reading Material" section links to SSH/OpenSSH/Keys. At the bottom of the page is a footer with a "Donate" button and a "Help?" link.

Use the “ls” command to find the file.

The screenshot shows a terminal window titled "bandit13@bandit:". The terminal displays a message about network access being limited by a local firewall. It then lists installed tools: gef, pwndbg, peda, gdbinit, pwnutils, and radare2. It mentions that both python2 and python3 are installed. The terminal ends with a prompt "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.

```

bandit13@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/angr/pwndbg) in /opt/pwndbg/
* peda (https://github.com/gdbinit/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/callopsled/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!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7jhnViUXRbuRtC1fXCSXlhmAAAM/uerLY.
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.

The screenshot shows a web browser window with the URL <https://overthewire.org/wargames/bandit/bandit15.html>. The page title is "Bandit Level 14 → Level 15". It contains several sections of text and links:

- SSH Information:** Host: bandit15.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
 - Port (computer networking) on Wikipedia
- Links to other levels:** 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.

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.

```
bandit14@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!

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

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

```
bandit14@bandit:~      X  +  v
--[ 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
fGRHxu02xGc7U7rxKDaxiWF0iF8ENq
bandit14@bandit:~$
```

```
bandit14@bandit:~      X  +  v
* 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/

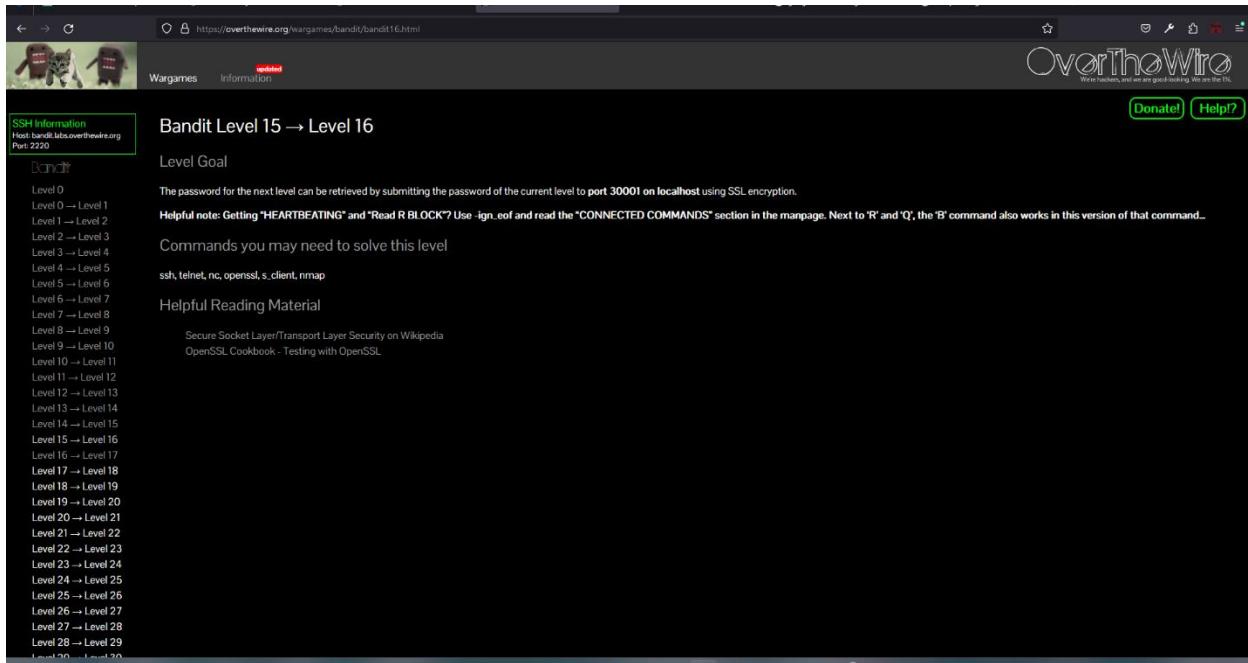
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

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

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGRHxu02xGc7U7rxKDaxiWF0iF8ENq
bandit14@bandit:~$ nc localhost 30000
fGRHxu02xGc7U7rxKDaxiWF0iF8ENq
Correct!
jN2kgmIXJ6fShzHT2avhotn4Zcka6tn
```

Bandit15 -> Bandit16

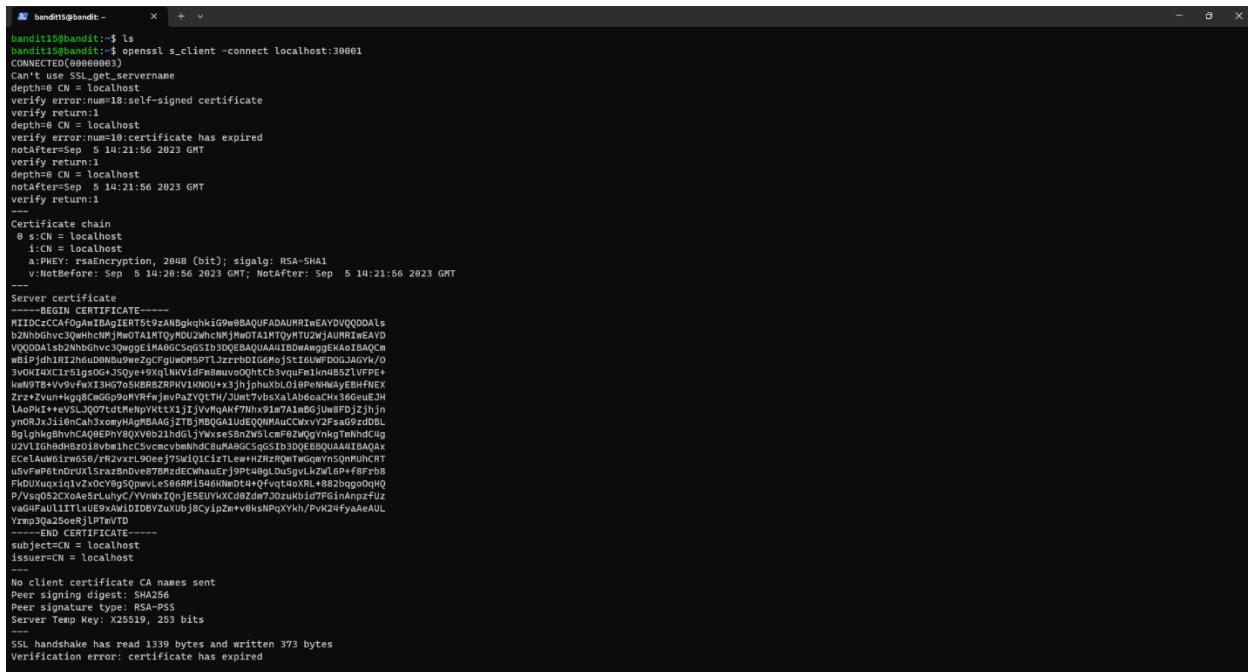


The screenshot shows a web browser displaying the OverTheWire Wargames Bandit16 page. At the top, there's a navigation bar with 'Wargames' and 'Information' tabs. On the right, there's a 'Donate!' button and a 'Help?' link. The main content area has a title 'Bandit Level 15 → Level 16' and a 'Level Goal' section. It says: '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.' Below this is a '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...' Underneath are sections for 'Commands you may need to solve this level' (ssh, telnet, nc, openssl_s_client, nmap) and 'Helpful Reading Material' (Secure Socket Layer/Transport Layer Security on Wikipedia, OpenSSL Cookbook - Testing with OpenSSL). A sidebar on the left lists levels from 0 to 20.

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.



The terminal window shows the output of the openssl s_client command. It starts with the command: 'bandit15@bandit: ~\$ ls' followed by 'bandit15@bandit: ~\$ openssl s_client -connect localhost:30001'. The response indicates a certificate error: 'Can't use SSL_get_servername', 'depth=0 CN = localhost', 'verify return:1', 'depth=0 CN = localhost', 'verify error:num=10:certificate has expired', 'notAfter: Sep 5 14:21:56 2023 GMT', 'verify return:1', 'depth=0 CN = localhost', 'verify error:num=10:certificate has expired', 'notAfter: Sep 5 14:21:56 2023 GMT', 'verify return:1'. It then shows the certificate details, including the BEGIN CERTIFICATE and END CERTIFICATE blocks. The certificate is for 'localhost' and includes various fields like 'Subject: /CN=localhost' and 'Issuers: /CN=localhost'. The session ends with 'SSL handshake read 1339 bytes and written 373 bytes' and 'Verification error: certificate has expired'.

```

bandit15@bandit: ~      +  x
0050 - ff ef dc 18 4b 04 c3 b8-7b 17 hc d5 cd 4c 46 6e ....K...{...}!Fn
0060 - 03 8d 85 d6 76 64 66 7f-42 81 13 29 7a 6d ae 8f ...vdF.B...z...
0070 - 39 f9 c2 0e 09 85 ab 89-ee 0f d7 de 0a 85 53 2b 9.....#+...I...
0080 - 9e 34 ca d4 94 0c 05 23-84 2b f9 49 5c a3 a3 c2 .4.....#.+...I...
0090 - 9e 56 3e db b4 43 94 b6-e6 c2 e1 2c d3 cc 07 cc .>...C.....g...
00a0 - 3b ab a2 6f 94 44 da 24-b5 e8 b3 0f 66 6e f1 d5 8...o.D.$...fn...
00b0 - 2c b5 da b7 08 77 9d d7-f8 a8 83 71 bb 51 de ce .,...w...q.Q...
00c0 - 29 05 9e 03 df 2d-a4 b2 1e e5 17 9f c7 58 )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: FC0D00420F5798834C8CDA83CF048E6794C3C421D11F6E77C50C481E3B6E372D6C
Session-ID-ctx:
Resumption PSK: A6C0AAADE192BF5005BE6218B5E178A7F124745DE019779D9C6173C0BEFC850302C1E66464E6499AE54E04B2022D46
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 0e 48 a5 32 54 0e cb 4c-36 de e2 24 47 c1 4f 66 .H.2T..L6..$G.OF
0010 - 30 03 93 9d 98 c2 38 9b 73-7a 7d 7f 89 ff 2d cc 9e 6C...8.sz}...$.
0020 - 30 03 93 9d 98 c2 38 9b 73-7a 7d 7f 89 ff 2d cc 9e ..e5V...L...L.
0030 - 37 b1 38 25 03 9d 98 c2 38 9b 73-77 0d 39 69 12 08 66 ..4.R...Y.C...6
0040 - cd f3 30 91 61 85 f4 59-0d 63 b3 f6 e6 58 d7 ea .N...<...t...
0050 - 2f af 40 af aa 91 27 3c-5d fb 85 f7 eb 8d 74 a9 /N...<...t...
0060 - 69 b5 92 54 5b ac 58 al-c8 92 8f 11 78 21 c8 8f i..T[X...x!...
0070 - 39 f9 8c c5 92 63 db 3d-4u 13 17 e8 27 a5 52 b3 9....c=d...!R.
0080 - c1 19 7c 57 c3 da 4f 3d-52 13 43 83 eb 3c 65 62 .|W..0=R.C..+eb
0090 - 2b 94 27 a1 b9 3a f6-27 b1 6d da 9c 26 2d 7b (.^...,'m..k-p
00a0 - 87 08 dd 35 a8 7e 2f 6e-9d a9 78 79 11 c2 31 69 .@.5..~n..xy..1l
00b0 - 2d a5 a9 1b ce c5 26 52-c7 79 95 cf 42 08 09 43 .....R.y..B.C
00c0 - 75 5a 52 20 f4 e5 34 65-5a 7c 83 47 29 7d 9d 8c u2R ..4eZ|.G).. 

Start Time: 1693935286
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK

bandit15@bandit: ~      +  x
00a0 - af 88 e8 35 4c e9 b8 44-ab c1 e4 cf 11 ba 28 25 ...5L..D.....%
00b0 - 57 aa 25 ba a6 6a e6 9f-b6 4a cc 75 df 88 22 7b W%.j...J.u..*{
00c0 - 39 b2 52 4b e1 32 87 51-6e 02 b6 24 3b d6 62 b4 9.RK.2.Qn..$; b.

Start Time: 1693935361
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: 925D9CB123A2B8B200443B1FEF29AF429C868402DE8D03D90B3A2333EA27A2F2
Session-ID-ctx:
Resumption PSK: 6CE7422EB6C9CA60240BWB34F1F8EFB4CDB839FF3DA81FE227C35186B8488BEF529C7E0B2DA4A5BACA0EB0E042C0636
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 9a 08 a5 32 54 0e cb 4c-36 de e2 24 47 c1 4f 66 .H.2T..L6..$G.OF
0010 - d1 88 57 77 3c bb 92-07-ba 95 d3 4f d7 05 ad ca ..Ww<...0.E...
0020 - 8a 46 8b 5a 7b 28 fd 06-7e ee 82 72 69 7e ce 7c .F.Z{ ...-ri-|.
0030 - fa 6d 9e 8f 07 8a 88 6c-0e f0 85 05 c9 a9 56 61 .W...l...*a
0040 - 0e f3 13 13 56 0e d2 6c-d2 46 a8 1b 1b d5 1e 3f ....V..l.F....?
0050 - 0a 6a 5f e9 3d 5c 9d-0u ae 6f e9 c9 db cc e0 .J...=J.o.....
0060 - 72 66 0b 72 66 Be-3y...cc ..,....W.B.GI.
0070 - 0d 6f d6 66 b7 6b 61 6c 66 0b 59 6a t0...A...D.A...Y.
0080 - db 5b e6 dd ee 0d 66 1f-a3 87 13 0e 09 0c da 15 [....f.....
0090 - f5 11 41 50 44 7b 78 ce-ed 85 62 a7 b2 71 aa 5e .APD|x..b..q....
00a0 - a3 5c 5b b3 33 d8 36 ae-52 a9 64 71 bc 8b 0e b6 .X.3.6.R.dq.....
00b0 - e4 d8 23 c8 93 65 9e d4-31 bd 04 88 32 ae 5f bd ..R..e..1.D.2...
00c0 - bf d9 b5 b1 04 6a e6 13-2e 8f a8 01 f9 ed e6 14 ....j.....
Start Time: 1693935361
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
jN2kgmtXjfsfhzhT2avhotn4Zcka6tn
Correct!
$0ttApK4SeYHwDl19SXGR50qc10Aill

closed
bandit15@bandit: ~ |

```

Bandit16 -> Bandit17

Log into the Bandit16.

The screenshot shows a browser window with the URL <https://overthewire.org/wargames/bandit/bandit17.html>. The page title is "Bandit Level 16 → Level 17". The "Level Goal" section contains the following text: "The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it." Below this, under "Commands you may need to solve this level", are links for ssh, telnet, nc, openssl, s_client, and nmap. The "Helpful Reading Material" section includes a link to "Port scanner on Wikipedia". At the bottom left, there is a sidebar with "SSH Information" and a list of levels from Level 0 to Level 29, with Level 17 highlighted in blue.

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

```
bandit16@bandit:~$ ls
bandit16@bandit:~$ gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
bandit16@bandit:~$ pwnools (https://github.com/Gallopsled/pwnools)
bandit16@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!

bandit16@bandit:~$ ls
bandit16@bandit:~$ nmap localhost -p31000-32000
Starting Nmap 7.80 ( 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
31000/tcp open  unknown
31010/tcp open  unknown
31091/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

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

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.

```
bandit17@bandit:~$ openssl s_client -connect localhost:31790
Verify return code: 0 (ok)
-----  
bandit17@bandit:~$ openssl s_client -connect localhost:31790  
CONNECTED(0x00000003)  
Can't use SSL_get_servername  
depth=0 CN = localhost  
verify error:num=18:self-signed certificate  
verify return  
depth=0 CN = localhost  
verify error:num=10:certificate has expired  
depth=0 CN = localhost  
verify return  
depth=0 CN = localhost  
notAfter Sep 5 14:21:57 2023 GMT  
verify return  
-----  
Certificate chain  
0 s:CN = localhost  
i:CN = localhost  
a:KEY: rsaEncryption 2048 (bit) , sha1; RSA-SHA1  
v:NotBefore: Sep 5 14:20:57 2023 GMT , NotAfter: Sep 5 14:21:57 2023 GMT  
-----  
Server certificate  
-----  
BEGIN CERTIFICATE-----  
MIIDCgECAQBgBdgITEBhDMEhjQnI4G9w0BAQUTADAURE-E5YD/QQQ201s  
b2Nhbslzb2nhbhGhvN3QwpE1M49GCSqSib13DCEBAAQAA1D0whwggEKA1BACU  
Vh4w4vQOxbhhG/c3CP9LRExUoUivYv0blocuvQd0f509C6dUnQp  
Wrcfchf21gl1l8cPMU1ZbenLqlz8f6dzCao8uMvd4cF2THGjuKfdIC  
is...  
-----  
SSL handshake has read 1339 bytes and written 373 bytes  
Verification error: certificate has expired  
-----  
New, TLSv1.3, Cipher: TLS_AES_256_GCM_SHA384  
Server public key is 2048 bit  
Secure Renegotiation IS NOT supported  
Compression: NONE  
-----  
No client certificate CA names sent  
Peer signing digest: SHA256  
Peer signature type: RSA-PSS  
Server Temp Key: X25519, 253 bits  
-----  
SSL handshake has read 1339 bytes and written 373 bytes  
Verification error: certificate has expired  
-----  
Save this key locally. Use a ssh private key.  
"ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220"
```

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 "somename", then:  
* USERNAMES are somename, somename_1, ...  
* Most LEVELS are stored in /somename/  
* PASSWORDS for each level are stored in /etc/somename_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 -d" in order to generate a random name to store files under. Be sure to keep /tmp/ disabled so that /proc restricted so that users cannot snop on eachother. Files and directories with easily guessable short names will be periodically deleted! The /tmp directory is regularly wiped.  
Please play nice!  
* don't leave orphan processes running  
* don't leave exploit-files laying around  
* don't annoy other players  
* don't be a nosy nosy spiller  
* DON'T POST SPOILERS!  
This includes writeups of your solution on your blog or website!  
-----  
[ Tips ]  
This machine has a DEBUT processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:  
-fPIR -fno-stack-protector -fno-explicit-linkage  
-fPIR, -fstack-protector -fno-explicit-linkage  
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/  
* fzf (https://github.com/junegunn/fzf) in /opt/fzf/  
* radare2 (https://github.com/radareorg/radare2) in /opt/radare2/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwnools (https://github.com/gallopsquad/pwnools)  
* radare2 (https://www.radare.org/)  
Both python 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!
```

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$ 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 -hal
total 1M
drwxrwxr-x  2 bandit16 4.0K Sep  5 18:16 .
drwxrwxrwt 20  root    11M Sep  5 18:16 ..
-rw-r--r--  1 bandit16 1.7K Sep  5 18:16 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:C2ihUBV7JhnvlwUXRb4RtEclfxC5CxLhmAAAM/uerLY.
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 is a sidebar titled "SSH Information" with the text "Host: bandit18s.OverTheWire.org Port: 2220". Below this is a "Level Goal" section containing a list of levels from 0 to 29. The main content area contains instructions and a command list:

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 'Byebyel' 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:
-#2           compile for 32bit
-fno-stack-protector    disable ProPolice
-Wl,-z,noexecro        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!
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/
* 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:~$ ls
passwords.new passwords.old
bandit7@bandit:~$ diff passwords.old passwords.new
0c242
< g1ZreTEH1V3cGK6g4cnyqZqaEj0mte
> hg45tuuCLF6ffzIuonagjMN8ssu9LFrdg
bandit7@bandit:~$ |
```

Bandit18 -> Bandit19

The screenshot shows a browser window with the URL <https://overthewire.org/wargames/bandit/bandit19.html>. The page header includes the OverTheWire logo and navigation links for "Wargames" and "Information". A sidebar on the left titled "SSH Information" lists levels from Level 0 to Level 29, with "Level 18" highlighted in green. The main content area displays the title "Bandit Level 18 → Level 19" and a "Level Goal" section containing the text: "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, a "Commands you may need to solve this level" section lists various Linux commands like ssh, ls, cat, and rm.

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.

```
Windows PowerShell X + v
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
    -m32          compile for 32bit
    -fno-stack-protector    disable ProPolice
    -fPIE,-fPIEonly      disable PIE
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/
    * pmrtools (https://github.com/dalltopsted/pmrtools)
    * 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"
[1] 11923 - - - - - [1] 11923
[1] 11923 \ / - - - - [1] 11923
[1] 11923 | G | | | | | G | | | |
[1] 11923 / - - - - [1] 11923 \ / - - - - [1] 11923

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit19@bandit.labs.overthewire.org's password:
$ ls
```

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

Bandit19 -> Bandit20



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

Wargames Information updated

OverTheWire
We're hackers, and we are good-hacking. We are the IT!

SSH Information
Host: bandit10s.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:~      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!

bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root    4896 Apr 23 18:04 .
drwxr-xr-x 70 root      root    4896 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:06 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     807 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:~      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!

bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root    4896 Apr 23 18:04 .
drwxr-xr-x 70 root      root    4896 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:06 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     807 Jan  6 2022 .profile
bandit19@bandit:~$ ./bandit20-do id
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$

```

```

bandit19@bandit:~      X  +  v
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

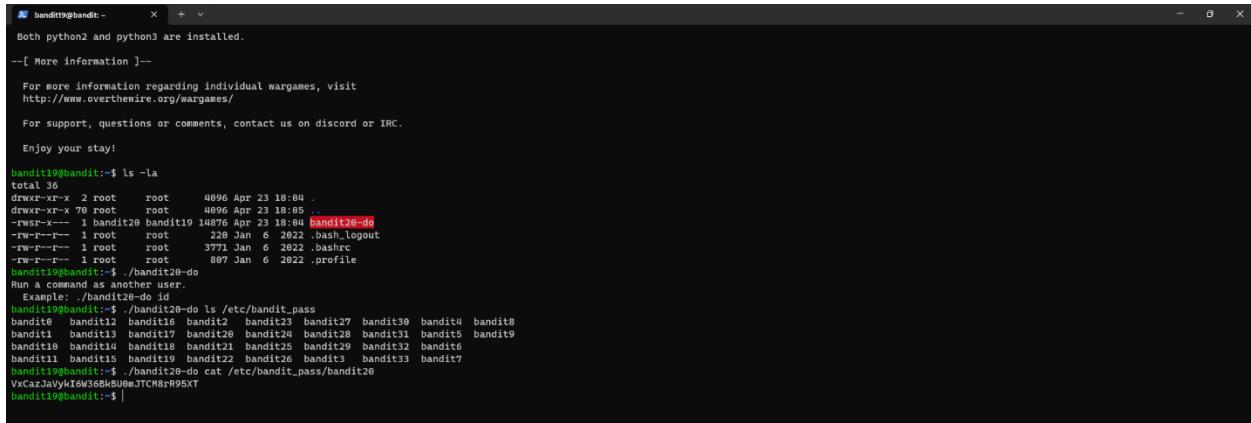
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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    4896 Apr 23 18:04 .
drwxr-xr-x 70 root      root    4896 Apr 23 18:05 ..
-rw-r--r--  1 bandit20 bandit19 14876 Apr 23 18:06 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     807 Jan  6 2022 .profile
bandit19@bandit:~$ ./bandit20-do id
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
ls: /etc/bandit_pass: Permission denied
bandit1  bandit13  bandit17  bandit20  bandit26  bandit31  bandit5  bandit9
bandit2  bandit14  bandit18  bandit21  bandit25  bandit32  bandit6
bandit3  bandit15  bandit19  bandit22  bandit26  bandit33  bandit7
bandit19@bandit:~|

```



```
bandit19@bandit:~      X  +  v
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 70 root      root        16384 Apr 23 18:04 ..
-rwsr-xr--  1 bandit28 bandit19 14876 Apr 23 18:04 bandit28-dd
-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
bandit19@bandit:~$ ./bandit28-do
Run a command as another user.
Example: ./bandit28-do id
bandit19@bandit:~$ ./bandit28-do ls /etc/bandit_pass
bandit1  bandit10  bandit15  bandit2  bandit23  bandit27  bandit39  bandit6  bandit8
bandit11 bandit13  bandit17  bandit20  bandit28  bandit31  bandit35  bandit9
bandit12 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit7
bandit13 bandit16  bandit19  bandit22  bandit26  bandit3  bandit33  bandit6
bandit19@bandit:~$ ./bandit28-do cat /etc/bandit_pass/bandit2
VxCazJaVykIGW36Bk8U0mJTCM8rR95XT
bandit19@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-17-c137701b3af1>
 - <https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-12-level-13-e5b687760d15>
- 2) YouTube –
 - <https://www.youtube.com/watch?v=hvSFPyqLizw>
 - <https://www.youtube.com/watch?v=H8LOP5oKcP0>
- 3) OverTheWire - <https://overthewire.org/wargames/bandit/bandit20.html>