

Sri Lanka Institute of Information Technology
BSc Honors in Information Technology
Specializing in Cyber Security



IE2012 - Systems and Network Programming

Exploring Bandit Levels

IT22083678
SAHAN H P T

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. 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.

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 digitalfortresses with each challenge I successfully complete. Consequently, I cordially invite you to read my riveting account, “Exploring Bandit Levels.”

Bandit0

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

The screenshot shows the OverTheWire Bandit wargame website. At the top, there's a logo of two bandit hats and a title bar with "Wargames", "Rules", and "Information". On the right, there's a "OverTheWire" logo with the tagline "We're hackers, and we are good-looking. We are the TIs." Below the title bar, there's a "SSH Information" section with the host "bandit.labs.overthewire.org", port "2220", and a "Donate!" button. The main content area is titled "Bandit" and contains information for Level 0. It includes a "Note for beginners" section with tips on using man pages and search engines, and a "Commands you may need to solve this level" section listing "ls", "cd", "cat", "file", "du", and "find". There's also a note for VM users about IPQoS throughput.

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. It has a similar layout to the main Bandit page, with a "Wargames", "Rules", and "Information" menu at the top. The "SSH Information" section shows the host "bandit.labs.overthewire.org", port "2220", and a "Donate!" button. The main content is titled "Bandit Level 0 → Level 1". It includes a "Level Goal" section stating that the password is in a file called "readme", a "Commands you may need to solve this level" section listing "ls", "cd", "cat", "file", "du", and "find", and a note for VM users.

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

The screenshot shows a terminal window on Kali Linux. The user is connected to the "bandit0" account via SSH. The terminal shows the password entry process, the OverTheWire welcome message, and the start of the game session. The terminal window has a watermark for "KALI LINUX".

```
bandit0@bandit: ~
File Actions Edit View Help
(sahan㉿kali)-[~]
$ ssh bandit.labs.overthewire.org -p2220 -l bandit0
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password:
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 "somegame", then:
* USERNAMEs are somegame0, somegame1, ...
* Most LEVELs are stored in /somegame/.
* PASSWORDs for each level are stored in /etc/somegame_pass/.
```

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

Wargames Rules Information

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

Donate! Help?

Bandit

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

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

```
bandit0@bandit:~
```

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 relro
```

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

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

-- [Tools] --

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

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

-- [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:~$
```

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

```
bandit0@bandit:~  
File Actions Edit View Help  
-- [ 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,norelro  disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
-- [ Tools ] --  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/  
* pwnools (https://github.com/Gallopsled/pwnools)  
* radare2 (http://www.radare.org/)  
  
-- [ 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  
NH2SXQwcBdpnTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$
```

To logout, run “exit”

```
bandit0@bandit:~  
File Actions Edit View Help  
-- [ 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,norelro  disable relro  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
-- [ Tools ] --  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwendbg/pwendbg) in /opt/pwendbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwnools (https://github.com/Gallopsled/pwnools)  
* radare2 (http://www.radare.org/)  
  
-- [ 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  
NH2SXQwcBdpnTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$
```

Bandit1 > Bandit2

Read the hint and try to get an idea.

The screenshot shows the OverTheWire Wargames website. At the top, there's a navigation bar with links for "Wargames", "Rules", and "Information". On the right side, there's a logo for OverTheWire with the tagline "Were hackers, and we are good-looking. We are the %". 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 Level 1 → Level 2". It contains sections for "Level Goal", "Commands you may need to solve this level", and "Helpful Reading Material". The "Level Goal" section states: "The password for the next level is stored in a file called - located in the home directory". The "Commands you may need to solve this level" section lists: "ls, cd, cat, file, du, find". The "Helpful Reading Material" section links to "Google Search for 'dashed filename'" and "Advanced Bash-scripting Guide - Chapter 3 - Special Characters".

Now log in to Bandit1, from the found password.

The screenshot shows a terminal window with a dark background. The title bar says "bandit1@bandit: ~". The terminal prompt is "(sahan㉿kali)-[~] \$". The user runs the command "ssh bandit.labs.overthewire.org -p2220 -l bandit". A password prompt appears, showing a dashed password field. The user types in the password obtained from the previous screenshot. After logging in, the terminal shows the OverTheWire welcome message, which includes a logo and the text "This is an OverTheWire game server. More information on http://www.overthewire.org/wargames". The terminal also displays the password for bandit1@bandit.labs.overthewire.org, which is a large string of characters. The message "Welcome to OverTheWire!" and instructions for reporting problems are shown at the bottom.

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

```
bandit1@bandit: ~
File Actions Edit View Help
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,norelro  disable relro

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

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

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

--[ 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!

banditi@bandit:~$ ls
banditi@bandit:~$ -
banditi@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.

```
sahan@kali: ~
File Actions Edit View Help
-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro  disable relro

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

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

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

--[ 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!

banditi@bandit:~$ ls
banditi@bandit:~$ -
banditi@bandit:~$ cat .-
rRGizSaX8MW1RTb1CNQoXTcYZWU6lgzi
banditi@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[sahani@kali:~]
```

Log out using the “exit” command.

Bandit2 > Bandit3

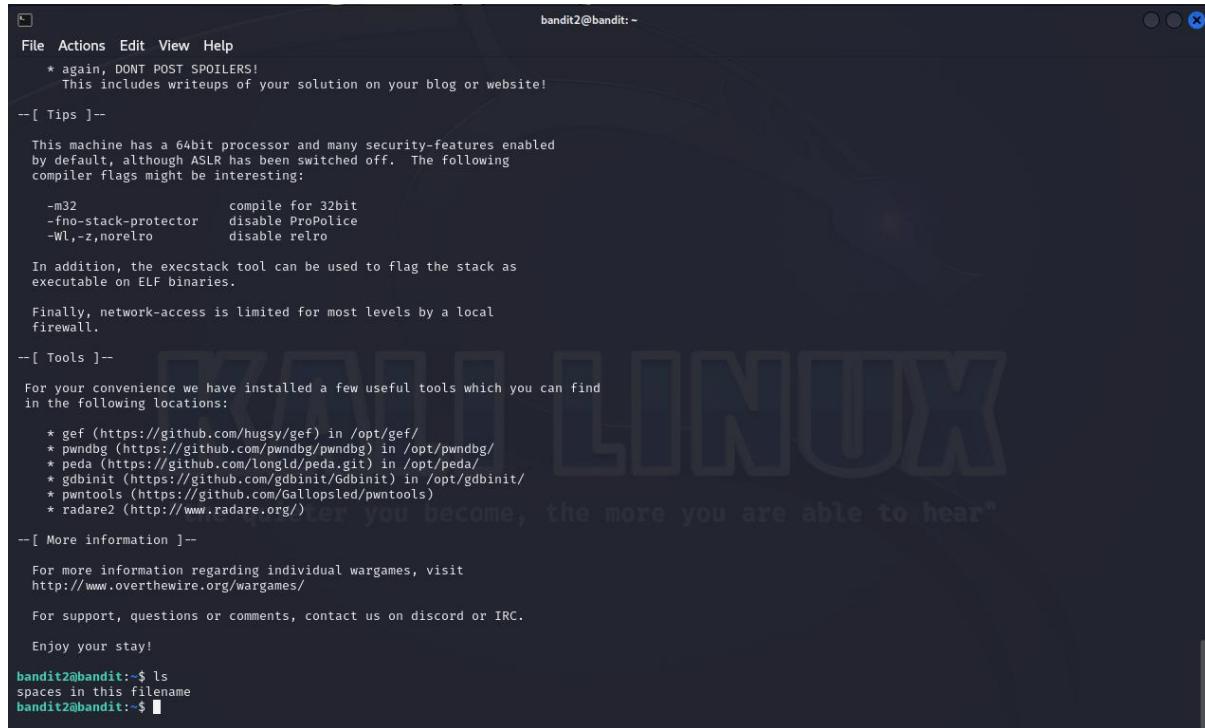
They tell us the next password is in a “spaces in this filename” file.

The screenshot shows the OverTheWire Wargames website. At the top, there's a navigation bar with links for "Wargames", "Rules", and "Information". On the right side, there's a logo for "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the %". 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 Level 2 → Level 3". It has sections for "Level Goal" (describing the password being stored in a file called "spaces in this filename"), "Commands you may need to solve this level" (listing "ls", "cd", "cat", "file", "du", "find"), and "Helpful Reading Material" (linking to a Google search for "spaces in filename").

Log into Bandit2 using the username and the password.

The screenshot shows a terminal window on a Kali Linux desktop. The title bar says "bandit2@bandit: ~". The terminal command entered is "ssh bandit.labs.overthewire.org -p2220 -l bandit2". The response shows a 2x2 grid of ASCII art cat faces. Below it, the message "This is an OverTheWire game server. More information on http://www.overthewire.org/wargames" is displayed. The prompt "bandit2@bandit.labs.overthewire.org's password:" is shown, followed by a masked password entry field containing a 2x2 grid of ASCII art cat faces. The terminal then displays a welcome message from OverTheWire, including a quote about being quiet and a note about reporting problems. It also lists some game statistics: "Playing the games", "This machine might hold several wargames.", "If you are playing 'somegame', then:", and a list of three bullet points: "* USERNAMES are somegame0, somegame1, ...", "* Most LEVELS are stored in /somegame/", and "* PASSWORDS for each level are stored in /etc/somegame_pass/".

Using the “ls” command find the file name.



```
bandit2@bandit: ~
File Actions Edit View Help
* 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,norelro  disable relro

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

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

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

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

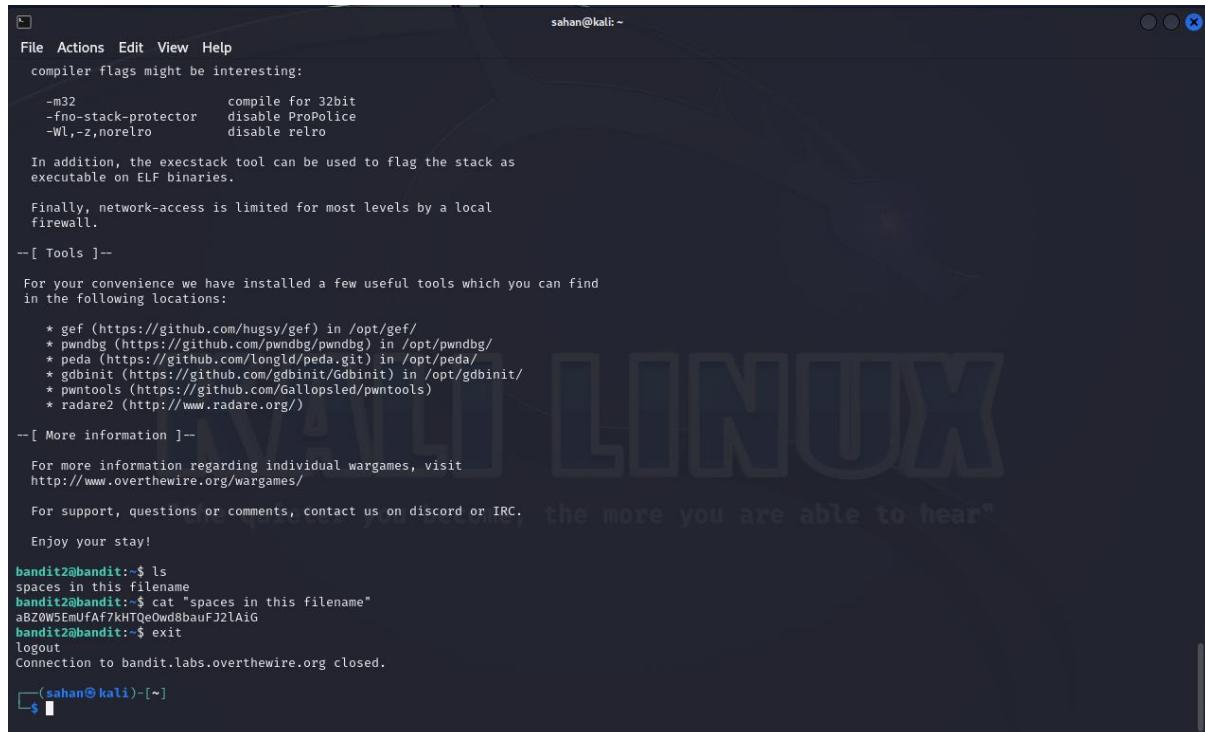
-- [ More information ] --
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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.



```
sahan@kali: ~
File Actions Edit View Help
compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro  disable relro

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

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

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

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

-- [ 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"
abZOW5EmUfAF7KHTQeOwdsbauFJ2lAiG
bandit2@bandit:$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(sahan@kali)-[~]
```

Log out using the “exit” command.

Bandit3 > Bandit4

Log Bandit 3 to use the password.

The screenshot shows the OverTheWire website's challenge interface. At the top, there are links for "Wargames", "Rules", and "Information". On the right, there are "Donate" and "Help?" buttons. The main content area is titled "Bandit Level 3 → Level 4". It includes a "Level Goal" section stating: "The password for the next level is stored in a hidden file in the `inhere` directory." Below this, a "Commands you may need to solve this level" section lists: `ls, cd, cat, file, du, find`. To the left, a sidebar titled "Bandit" provides a list of levels from 0 to 19, each with a corresponding icon.

The screenshot shows a terminal window titled "bandit3@bandit: ~". The user has logged in from a Kali Linux host (sahan@kali). The terminal session shows:

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBzOW5EmUFAf7kHTQeOwd8baufJ2lAig
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[sahan@sahan-kali:~] $ ssh bandit.labs.overthewire.org -p2220 -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]
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

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

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
File Actions Edit View Help
--[ 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,norelro      disable relro

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

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

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

--[ 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



```
sahan@kali: ~
File Actions Edit View Help
-fno-stack-protector    disable ProPolice
-Wl,-z,norelro      disable relro

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

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

--[ Tools ]--

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

--[ 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
2EW7Bsr6aMMQJ2HJW067dm8EgX26xNe
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

$(sahan@kali)-~]
```

Log out using the “exit” command.

Bandit4 -> Bandit5

The screenshot shows the OverTheWire Wargames website. At the top, there's a navigation bar with links for "Wargames", "Rules", and "Information". On the right side, there's a logo for "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the PIs." Below the navigation, there's a green box titled "SSH Information" containing the host "bandit.labs.overthewire.org" and port "2220". The main content area is titled "Bandit Level 4 → Level 5". It has a "Level Goal" section with the instruction: "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." Below that is a "Commands you may need to solve this level" section listing various Linux commands like ls, cd, cat, file, du, find, etc. A sidebar on the left is titled "Bandit" and lists the levels from 0 to 18.

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

The terminal window shows the Bandit4 shell at bandit4@bandit: ~. The user runs the "ls" command, which shows a single directory named "inhere". The terminal also displays the OverTheWire watermark "Linux" and the quote "the quieter you become, the more you are able to hear".

```
bandit4@bandit: ~
File Actions Edit View Help
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,norelro      disable relro
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
Finally, network-access is limited for most levels by a local
firewall.
-- [ Tools ] --
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/Gallopsled/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
-- [ 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
File Actions Edit View Help

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,norelro  disable relro

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

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

-- [ Tools ] --

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

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

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

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

```
bandit4@bandit: ~/inhere
File Actions Edit View Help
firewall.

-- [ Tools ] --

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

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

-- [ More information ] --

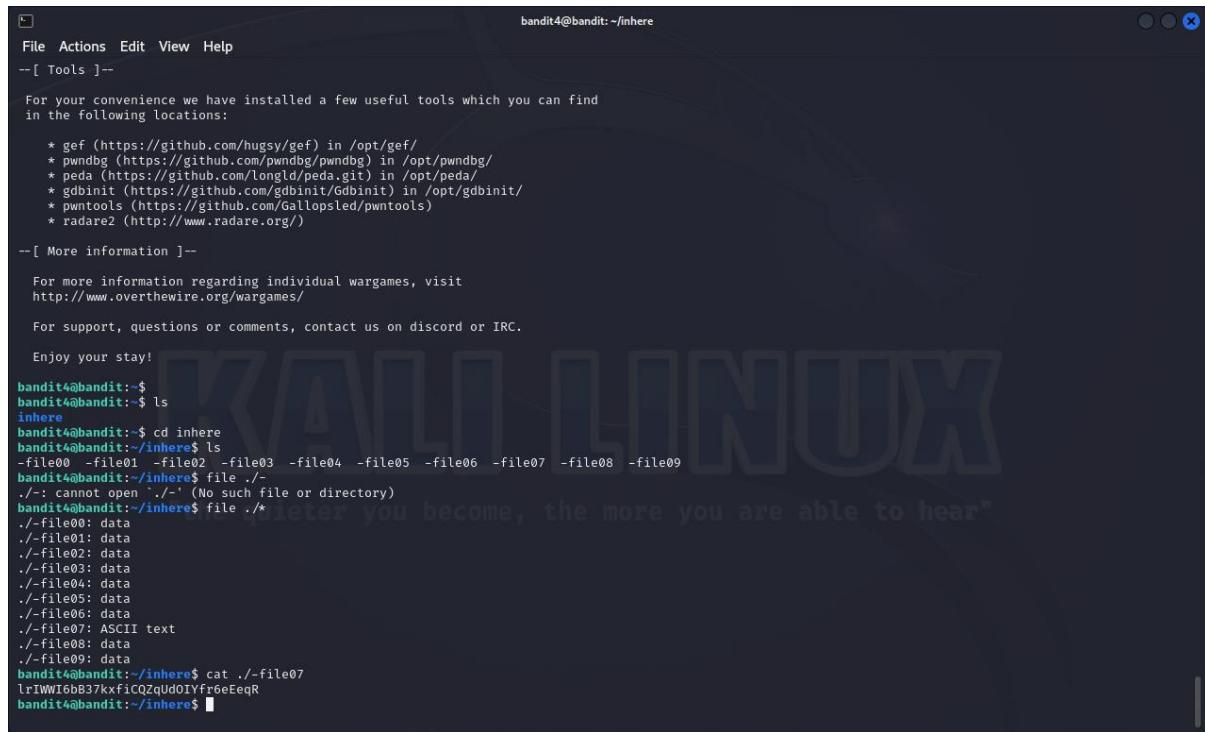
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames

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

Enjoy your stay!

bandit4@bandit:~$ 
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./*
./: cannot open './' (No such file or directory)
bandit4@bandit:~/inhere$ file ./*
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: data
bandit4@bandit:~/inhere$ 
```

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



```
bandit4@bandit:~/inhere
File Actions Edit View Help
-[ Tools ]-
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

-[ More information ]-

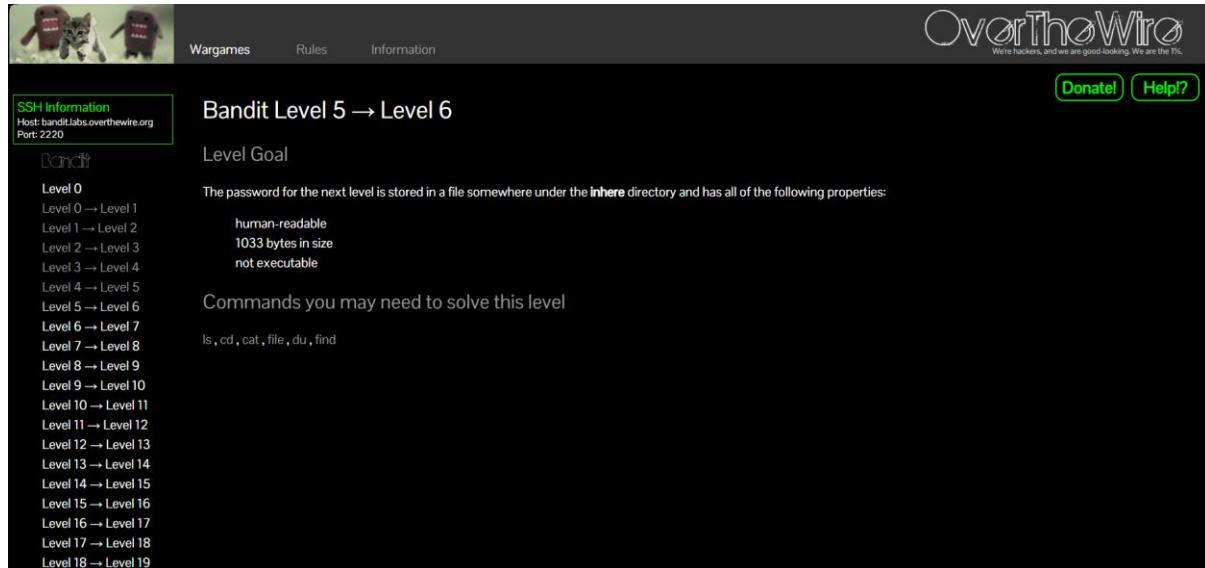
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./*
./: cannot open './' (No such file or directory)
bandit4@bandit:~/inhere$ file ./*
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWI6bB37kxfiCQzqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

Bandit05 -> Bandit06

Log in to Bandit05 using the password.



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

Bandit

Level 0

Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19

Bandit Level 5 → Level 6

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

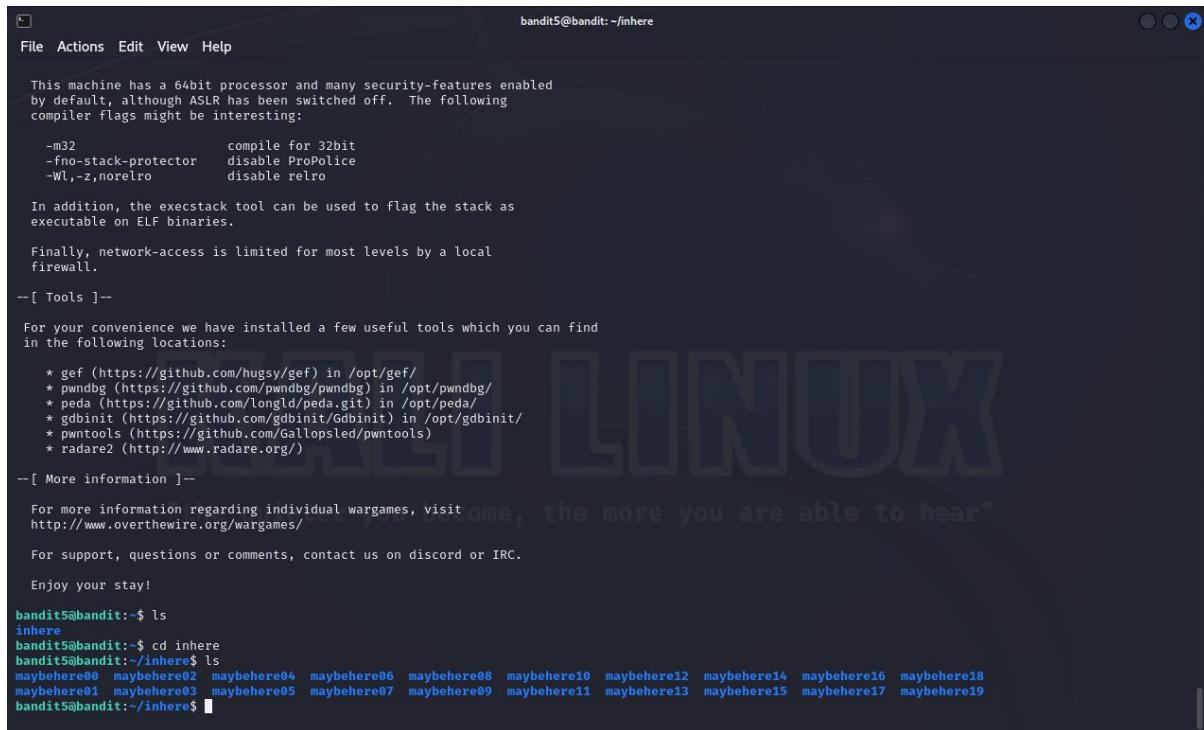
Commands you may need to solve this level

ls, cd, cat, file, du, find

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

Donate! Help?

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
File Actions Edit View Help

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,norelro      disable relro

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

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

--[ Tools ]--

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

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

--[ More information ]--

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

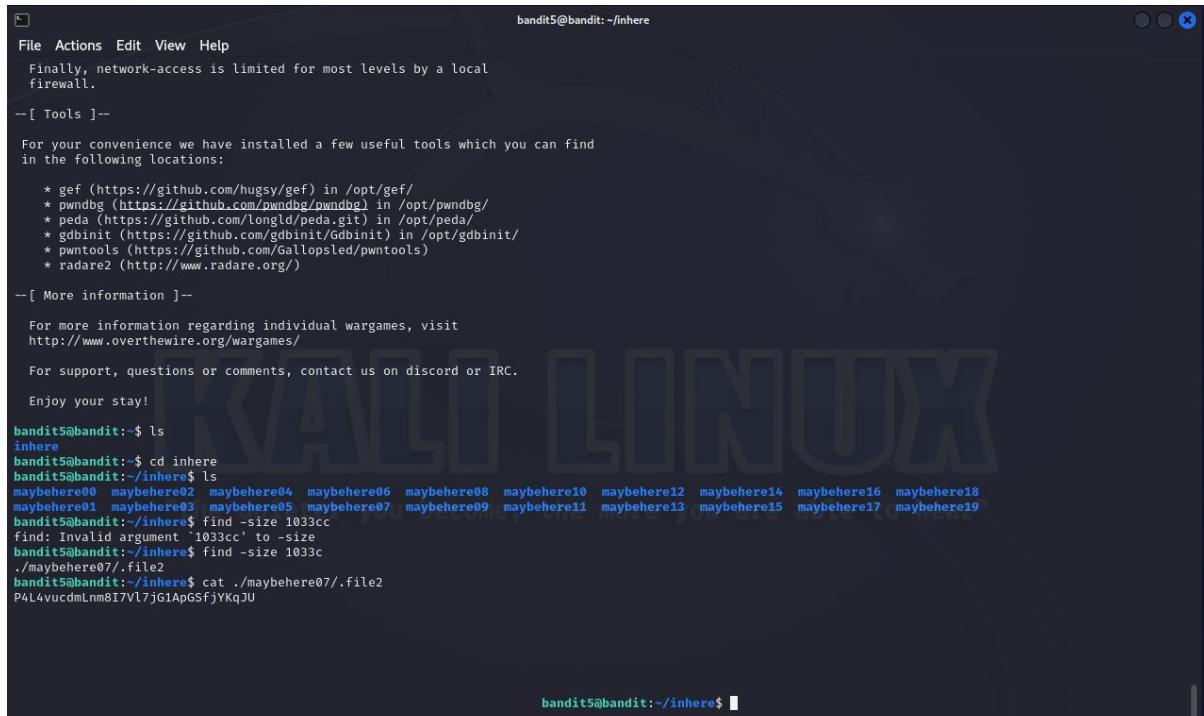
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

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

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

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



```
bandit5@bandit: ~/inhere
File Actions Edit View Help

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

--[ Tools ]--

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

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

--[ More information ]--

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

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

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12 maybehere14 maybehere16 maybehere18
maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13 maybehere15 maybehere17 maybehere19
bandit5@bandit:~/inhere$ find -size 1033c
find: Invalid argument '1033c' to -size
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

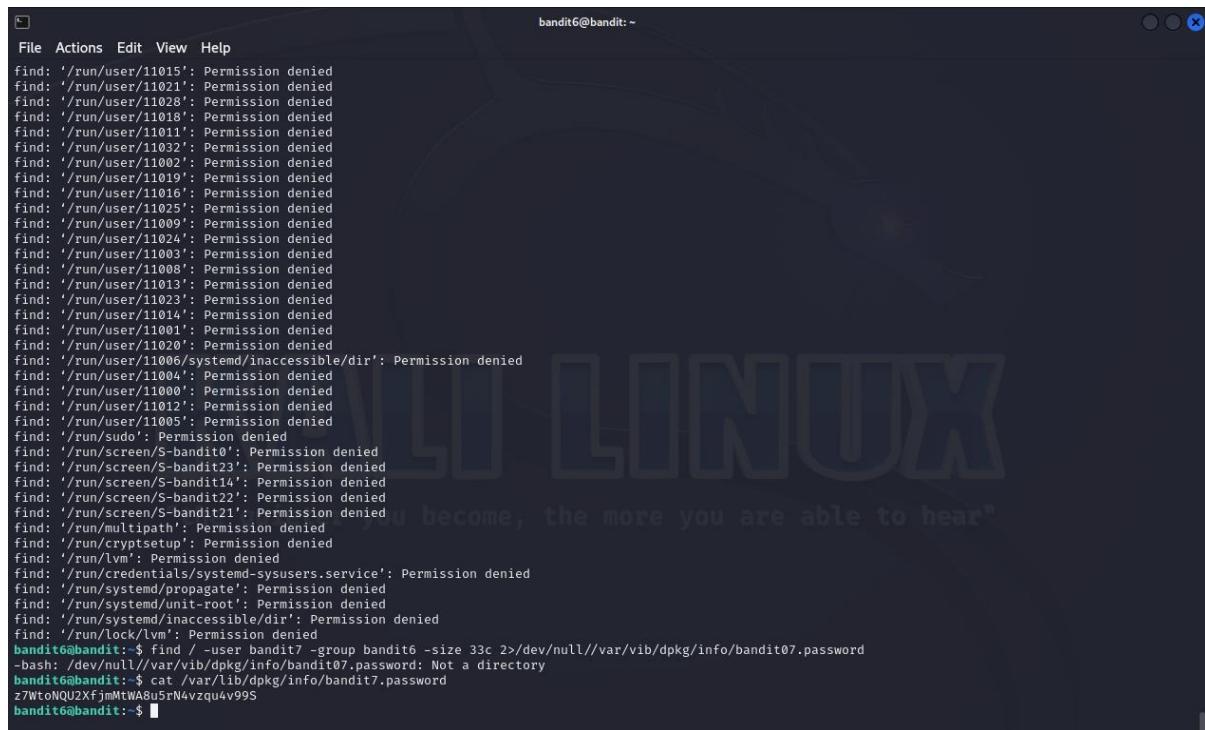
Bandit6 -> Bandit7

The screenshot shows the OverTheWire Bandit6 level 6 interface. At the top, there's a navigation bar with links for Wargames, Rules, and Information. The main content area has a title "Bandit Level 6 → Level 7". On the left, there's a sidebar titled "SSH Information" with details: Host: bandit.labs.overthewire.org, Port: 2220, and a "Bandit" logo. The main content area contains a "Level Goal" section with the text: "The password for the next level is stored somewhere on the server and has all of the following properties:" followed by a list: owned by user bandit7, owned by group bandit6, and 33 bytes in size. Below this is a "Commands you may need to solve this level" section with the command: ls, cd, cat, file, du, find, grep.

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

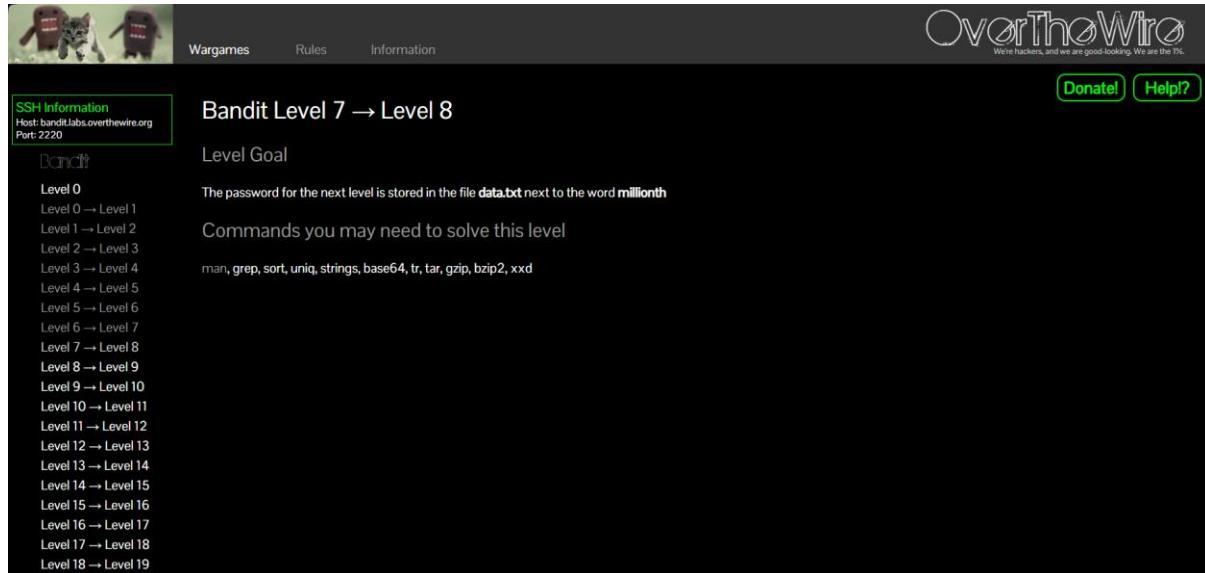
The screenshot shows a terminal window with the title "bandit6@bandit: ~". The terminal displays the output of a "find" command, which lists numerous files and directories with "Permission denied" errors, indicating a lack of root privileges. The command itself is: "find: '/run/user/11027': Permission denied find: '/run/user/11029': Permission denied ... find: '/run/user/11023': Permission denied". The terminal prompt at the bottom is "bandit6@bandit: \$".

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



```
bandit6@bandit: ~
File Actions Edit View Help
find: '/run/user/11015': Permission denied
find: '/run/user/11021': Permission denied
find: '/run/user/11029': Permission denied
find: '/run/user/11018': Permission denied
find: '/run/user/11011': Permission denied
find: '/run/user/11032': Permission denied
find: '/run/user/11002': Permission denied
find: '/run/user/11019': Permission denied
find: '/run/user/11016': Permission denied
find: '/run/user/11025': Permission denied
find: '/run/user/11009': Permission denied
find: '/run/user/11024': Permission denied
find: '/run/user/11003': Permission denied
find: '/run/user/11008': Permission denied
find: '/run/user/11013': Permission denied
find: '/run/user/11023': Permission denied
find: '/run/user/11014': Permission denied
find: '/run/user/11001': Permission denied
find: '/run/user/11020': Permission denied
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied
find: '/run/user/11004': Permission denied
find: '/run/user/11012': Permission denied
find: '/run/user/11005': Permission denied
find: '/run/sudo': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/run/credentials/systemd-sysusers.service': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/lock/lvm': Permission denied
bandit6@bandit: $ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null//var/vib/dpkg/info/bandit07.password
-bash: /dev/null//var/vib/dpkg/info/bandit07.password: Not a directory
bandit6@bandit: $ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQ2XFjMtwABu5rN4vzqu499S
bandit6@bandit: $
```

Bandit7 -> Bandit8



OverTheWire
We're hackers, and we are good-looking. We are the 1%.

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

Bandit

Level 0

Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19

Bandit Level 7 → Level 8

Level Goal

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

Commands you may need to solve this level

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

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

```
bandit7@bandit:~
```

--[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,norelro  disable relro
```

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

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

--[Tools]--

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

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

--[More information]--

"the quieter you become, the more you are able to hear"

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:~
```

--[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,norelro  disable relro
```

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

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

--[Tools]--

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

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

--[More information]--

"the quieter you become, the more you are able to hear"

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      TESKZC0xVtetK059xNwm25STk5iWrBvP
bandit7@bandit:~$
```

Bandit8 -> Bandit9

The screenshot shows the OverTheWire Wargames website. At the top, there are three tabs: "Wargames", "Rules", and "Information". On the right side, there is a logo for "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the %". Below the tabs, there is a green box labeled "SSH Information" with the host "bandit.labs.overthewire.org" and port "2220". A "Bandit" icon is also present. The main content area has a title "Bandit Level 8 → Level 9". Under "Level Goal", it says: "The password for the next level is stored in the file `data.txt` and is the only line of text that occurs only once". Under "Commands you may need to solve this level", it lists: "grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd". Under "Helpful Reading Material", it lists various levels from 0 to 19. At the bottom, there are links for "Piping and Redirection".

Log into Bandit8 using the password.

The terminal window shows the Bandit8 shell. It displays several tips and tools available on the system. The tips section includes:

- * don't post passwords or spoilers
- * again, DONT POST SPOILERS!
- This includes writeups of your solution on your blog or website!

The tools section lists:

- [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
 - fstack-protector-all 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/
 - * pwntools (<https://github.com/Gallopsled/pwntools>)
 - * radare2 (<http://www.radare.org/>)
- [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!

At the bottom, it shows the prompt: bandit8@bandit:~\$

Sort – sorts the lines of a text file

Uniq – filters input and writes to the output

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

```

bandit8@bandit: ~
File Actions Edit View Help
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 relro

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

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

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

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

-- [ 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!

bandit8@bandit: $ sort data.txt | uniq -u
EN632PlfyiZbn3PhK3XOGSlNInNE00t
bandit8@bandit: $ 

```

Bandit9 -> Bandit10

The screenshot shows the OverTheWire Wargame interface. At the top, there are icons for a cat and a person, followed by the text "Wargames", "Rules", and "Information". On the right, it says "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the 1%." Below these are "Donate!" and "Help?" buttons. The main content area is titled "Bandit Level 9 → Level 10". It says "Level Goal" and provides the 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." It also lists commands to solve the level: "grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd". To the left, there is a sidebar titled "Bandit" with a list of levels from 0 to 19.

Log into Bandit8 using the password.

```

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

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

-- [ 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: $ 

```

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

```
bandit9@bandit:~  
File Actions Edit View Help  
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,norelro      disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
-- [ Tools ] --  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
-- [ 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:~  
File Actions Edit View Help  
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,norelro      disable relro  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
Finally, network-access is limited for most levels by a local  
firewall.  
-- [ Tools ] --  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwendbg/pwendbg) in /opt/pwendbg/  
* 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/)  
-- [ 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 =  
xJTheG"  
_____ passwordk^  
_____ is  
_____ G7w8Li6j3kTb8A7j9LgrywtEUlypp6s  
bandit9@bandit:~$
```

Bandit10 -> Bandit11

The screenshot shows the OverTheWire Wargames website interface. At the top, there's a navigation bar with links for "Wargames", "Rules", and "Information". On the right side, there's a logo for "OverTheWire" with the tagline "Were hackers, and we are good-looking. We are the 1%." Below the navigation, there's a green box titled "SSH Information" containing the host "bandit.labs.overthewire.org" and port "2220". The main content area is titled "Bandit Level 10 → Level 11". It includes a "Level Goal" section stating "The password for the next level is stored in the file `data.txt`, which contains base64 encoded data". A "Commands you may need to solve this level" section lists "grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd". A "Helpful Reading Material" section links to "Base64 on Wikipedia". On the left side, there's a sidebar titled "Bandit" with a vertical list of levels from "Level 0" to "Level 19", each with a corresponding icon.

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

The screenshot shows a terminal window with a dark background and white text. The title bar says "bandit10@bandit: ~". The terminal displays the following text:

```
File Actions Edit View Help
--[ 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,norelro  disable relro

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

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

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

--[ 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
cat: data.txt: No such file or directory
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkJSS05kTllGtmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$
```

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

```

bandit10@bandit: ~
File Actions Edit View Help
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 relro

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

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

--[ Tools ]--

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

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

--[ 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
cat: data.txt: No such file or directory
bandit10@bandit:~$ cat data.txt
VGhlHBhc3N3b3JkIGlZID26UGV6auXkJSS05kTl1GTmI2blZDS3pwaGxYSEJNCg=
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezildR2RKNdNYFNb6nVCKzphlxHBM
bandit10@bandit:~$ 

```

Bandit11-> Bandit12



Wargames Rules Information

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

[Donate!](#) [Help?](#)

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

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19

Bandit Level 11 → Level 12

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: ~
File Actions Edit View Help
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,norelro    disable relro

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

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

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

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

--[ 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: ~
File Actions Edit View Help
--[ 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,norelro    disable relro

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

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

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

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

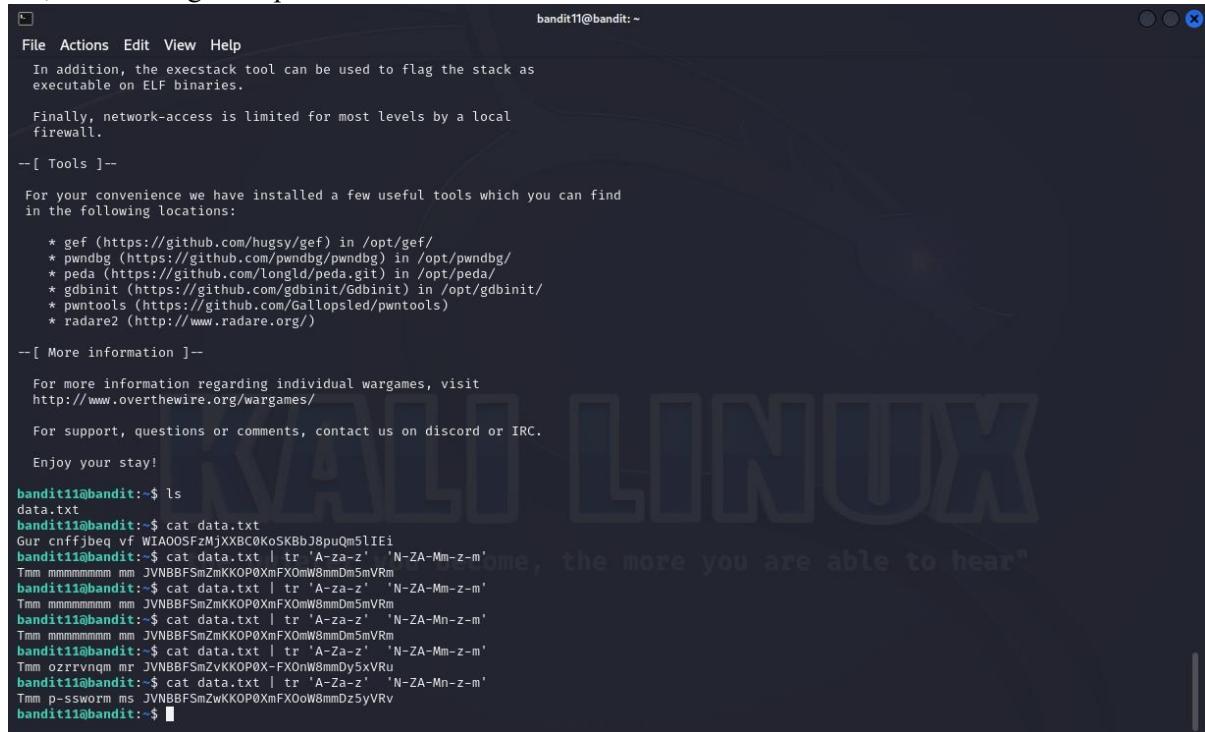
--[ More information ]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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 WIA00SFzMjXXBC0KoSKBbJ8puQm5lIEi
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: ~
File Actions Edit View Help
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

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

-[ Tools ]--

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

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

-[ More information ]--

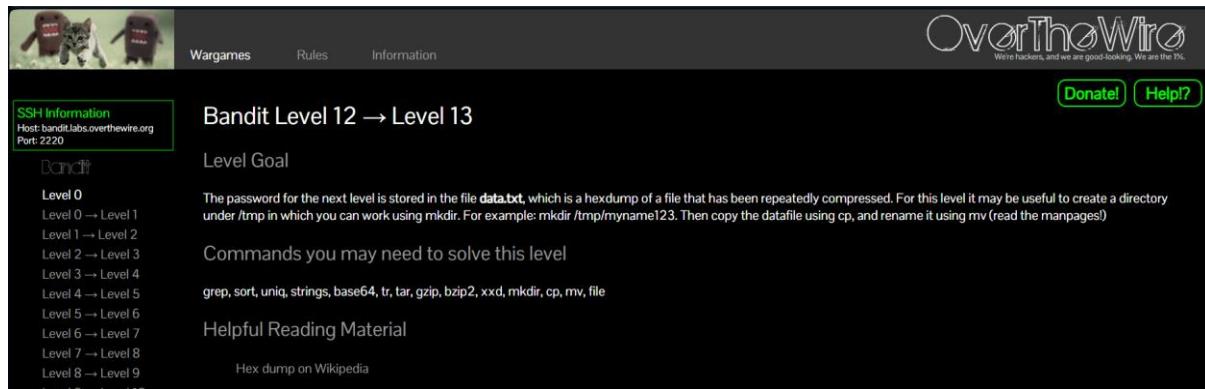
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

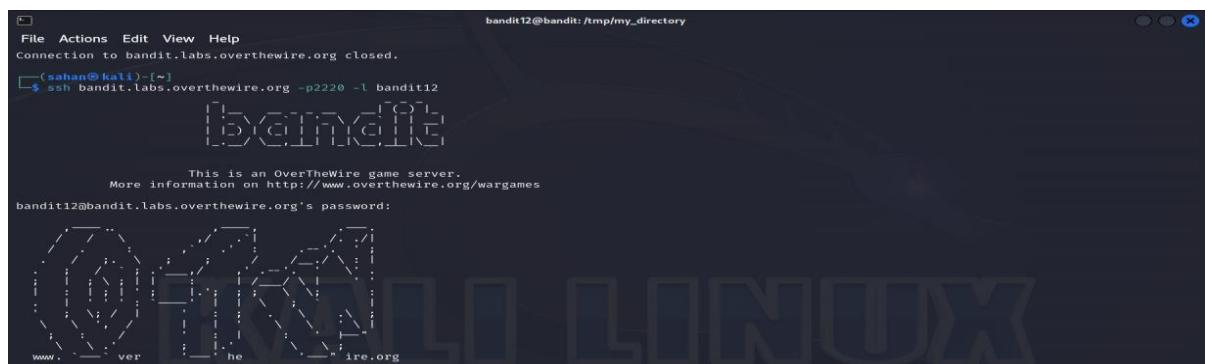
bandit11@bandit: $ ls
data.txt
bandit11@bandit: $ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbj8puQm5lIEi
bandit11@bandit: $ cat data.txt | tr 'A-zA-z' 'N-ZA-Mm-z-m'
Tmm mmmmmmmmm mm JVNBBSF5mZmKKOP0XmFxOmW8mmDm5mVRn
bandit11@bandit: $ cat data.txt | tr 'A-zA-z' 'N-ZA-Mm-z-m'
Tmm mmmmmmmmm mm JVNBBSF5mZmKKOP0XmFxOmW8mmDm5mVRn
bandit11@bandit: $ cat data.txt | tr 'A-zA-z' 'N-ZA-Mn-z-m'
Tmm mmmmmmmmm mm JVNBBSF5mZmKKOP0XmFxOmW8mmDm5mVRn
bandit11@bandit: $ cat data.txt | tr 'A-zA-z' 'N-ZA-Mm-z-m'
Tmm ozrrvnmq mr JVNBBSF5mZvKKOP0X-FXOnW8mmDy5xVRu
bandit11@bandit: $ cat data.txt | tr 'A-zA-z' 'N-ZA-Mn-z-m'
Tmm p-sswrm ms JVNBBSF5mZwKKOP0XmFxOoW8mmDz5yVRv
bandit11@bandit: $
```

Bandit12 -> Bandit13



The screenshot shows the OverTheWire website's wargame section. The top navigation bar includes links for "Wargames", "Rules", and "Information". On the right, there's a "Donate" button and a "Help?" link. The main content area is titled "Bandit Level 12 → Level 13". It features a "Level Goal" section with instructions about creating a directory under /tmp and using commands like mkdir, cp, and mv. Below that is a "Commands you may need to solve this level" section listing various Unix utilities. A "Helpful Reading Material" section points to a Wikipedia page on hex dumps. On the left, there's a sidebar with "SSH Information" for host bandit.labs.overthewire.org on port 2220, and a "Bandit" section listing levels 0 through 12.

Log into Bandit12 using the password.



```
bandit12@bandit: /tmp/my_directory
File Actions Edit View Help
Connection to bandit.labs.overthewire.org closed.
(sahan@kali)-[~]
$ ssh bandit.labs.overthewire.org -p2220 -l bandit12
[!] Exploit [!]
[!] Exploit [!]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit12@bandit.labs.overthewire.org's password:
```

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

```
bandit12@bandit: /tmp/my_directory
File Actions Edit View Help
-[ 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,norelro      disable relro

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

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

-[ Tools ]--

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

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

-[ 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:$ cd /tmp/my_directory
bandit12@bandit:/tmp/my_directory$ ls
compressed_file data.bin data_decompressed data.gz data_raw data.txt decompressed_data hexdump.txt
bandit12@bandit:/tmp/my_directory$ file data.txt
data.txt: ASCII text
```

Run the “cat data.txt”

```
bandit12@bandit:/tmp/my_directory$ cat data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/my_directory$ cat data.txt
00000000: 1f8b 0808 6855 1e65 0203 6461 7461 322e ....hU.e..data2.
00000010: 6269 6e00 013d 02c2 f042 5a68 3931 4159 bin..=...BzH9IAY
00000020: 2653 5948 1b32 0208 0019 ffff FaeC cff7 65YH.2.....
00000030: f6ff e4f7 bfbc ffff bff7 ff9f 77fb .....9...
00000040: bd31 eeff b9fb fbbf b9bf f77f b001 3b2c .1.....;
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340 .....hh ...i...@
00000060: 1a68 00d0 0d01 a1a0 0001 a680 0003 4fd4 .h,.....F.
00000070: 6434 3234 611a 340d 07a4 c351 068f 5000 d424a.4....Q..P.
00000080: 069a 0680 0000 0006 8006 8da4 681a 6868 .....h..hh
00000090: 0d06 8d00 6834 3400 d07a 9400 01a0 0341 ....h44 ..z....A
000000a0: e4e1 a190 da40 3d10 ca68 3468 6800 0088 .....@...h4h...
000000b0: 1ala 1b50 0683 d434 d069 a0d0 3100 0000 ...P...4.i..1...
000000c0: 001e a680 0000 1a00 d0d0 6864 d0c4 d0d0 .....hd...
000000d0: 000c 8641 7440 0108 032e 86b4 4cf0 22bb ...At@.....L".
000000e0: 6682 2b7e b3e2 e98d a74 dacc 028a 330d f.+~....t....3.
000000f0: bbb2 9494 d332 d933 642a 3538 d27e 09ce ....2.3d*58...-
00000100: 53da 185a 505e aada 6c75 59a2 6342 0572 S..ZP^..!uv..B.r
00000110: 2494 4600 5021 2500 1973 c18a 6881 1bef $.F.P!%..s..h..
00000120: 3f9b 1429 5b1d 3d87 68b5 804f 1d28 42fa ?...[.=.h..0.(B.
00000130: 16c2 3241 98fb 8229 e274 5a63 fe92 3aca ..2A...).tzC...
00000140: 70c3 a329 d21f 41e0 5a10 08cb 888f 30df p...).A.Z.....0.
00000150: f3da c858 418b 0379 6a65 cfa2 eeb7 9f01 ....A..yje.....
00000160: 782c da0e 288b e0c3 fe13 7af5 45ab 2b22 x,...(.z.E.+
00000170: a432 bf2f e32d b9e6 1465 2296 d805 a45e .2./.-.e"....^
00000180: d1c1 eac8 7483 6aa0 ca0e cf24 8864 bd40 ....t.j...$.d.0
00000190: 118c 644a 1dc6 a127 375c b7a6 c124 bdae ..d) ...`\..$..
000001a0: 6d31 63a0 a223 3ea0 61d4 bdf0 450f 56fb mic..#.a...E.V.
000001b0: a546 8d34 08a2 4f1d 43d3 9063 404d dd43 .F.4...O.C..c@M.C
000001c0: b4f2 e65d bcb7 5932 0f5e 6802 3892 a988 ...].Y2.^h.8...
000001d0: 443d 8e89 7e09 4fb0 499d ee4e 4470 46c0 D...~.0.I..NDpF.
000001e0: 2ba6 7c62 234a 7f76 151b aec0 23ee 4a97 +.lbfJ.v....#.J.
000001f0: bc46 e34c de8a 5724 a1c3 9b89 cd96 1879 .d.L..W$.....y
00000200: d560 0ccb 5c26 09e4 efaf 5b94 402a 7780 . ..\6....[@*W.
00000210: 4d87 30ce b8a3 946e 72c1 a643 1db7 a050 M.0.....n..C...
00000220: 6524 629c 0c7e 8e7b e0f8 820c d5cb 60a0 e$b...~.{.....
00000230: 003c a584 d4c1 61ef eb02 3f65 3a54 a3a2 .<...a...?e:T..
00000240: a565 c154 34c2 b162 d206 1ff8 bb92 29c2 .e.T4..b.....
00000250: 8482 40d9 9010 b3a9 e478 3d02 0000 ..@....x=...
bandit12@bandit:/tmp/my_directory$ xxd -r data.txt > data.bin
bandit12@bandit:/tmp/my_directory$ ls
```

Run “xxd -r data.txt >data1.bin” and next run the “ls” to find all the files.

```

bandit12@bandit: /tmp/my_directory$ cat data.txt
00000020: 2653 5948 1b32 0200 0019 ffff faee cff7 8SYH.2.....
00000030: f6ff e4f7 bfbc ffff bfff ff9 39ff 3fb . ....9...
00000040: bd31 eeff b9fb fbbb b9bf f77f b001 3b2c .1.....;,
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340 .,..hh...i...@.
00000060: 1a68 0d0d 0d01 a1a0 0001 a680 0003 46d4 .H.....F.
00000070: 6434 3234 611a 340d 07a4 c351 0687 5000 d424.4....Q..P.
00000080: 0694 0680 0000 0006 8006 8da1 681a 6868 .....h.hh
00000090: 0d0e 8d00 6834 3400 d07a 9a01 01a0 0341 ....h44.z....A
000000a0: ea1c a190 da40 3d10 ca68 3468 6800 00c8 ....@..h4h..
000000b0: 1a1a 1b50 0683 d434 d069 add0 3100 d000 ...P...4.i..1...
000000c0: 001e a680 0dd0 1a00 d0d0 6864 d0c4 d0d0 .....hd...
000000d0: 000c 8641 7440 0108 032e 86b4 4cf0 22bb ..At@.....L".
000000e0: 6682 2b7e b3e2 e98d aa74 dacc 0284 330d f.+....t....3.
000000f0: bbb2 9494 d332 d933 642a 3538 d27e 09ce ....2.3d*58.~
00000100: 53d1 185a 505e aada 6c75 59a2 b342 0572 S..ZP^..LuY..B.r
00000110: 2494 4600 5021 25b0 1973 c18c 6881 1bef $.F.P!%..s..h...
00000120: 3f98 1429 5b1d 3d87 68b5 804f 1d28 42fa ?...](=..h..O.(B.
00000130: 16c2 3241 98fb 8229 e274 5a63 fe92 3aca ..2A...)tzc:..
00000140: 70c3 a329 d21f 41e0 5a10 08ca 888f 30df p..).A.Z....0.
00000150: f3d3 c885 41b8 0379 6a65 cf2a eeb7 9f01 ....A..yj@...
00000160: 782c da0e 288b e0c3 fe13 7a51 45ab 2b22 x.,(.....z.E.+
00000170: a432 bf2f e32d b966 1465 2296 d805 a45e .2./.-...e^...
00000180: dc1c each 7483 6aaac cafe cf24 8864 bd40 ....t.j...$.d@.
00000190: 118c 644a 1dc6 629c b7a1 c124 bdae ..d.J...?7...$..
000001a0: 6d31 63a0 a223 3ea0 61d4 bdf0 450f 56fb m1c..#.a...E.V.
000001b0: a546 8d34 4f1d 43d3 9063 404d dd43 .F.4..O.C..c@M.C
000001c0: b4f2 e65d bcb7 5932 0f56 6802 3892 a988 ..l..Y2.^h.8...
000001d0: 443d 8e89 7e09 4fb0 499d ee4e 4470 46c0 De..~..O.I..NDpF.
000001e0: 2ba6 7c62 234a 7f76 151b aec0 23ee 4997 +.|bfJ.v....#.J.
000001f0: bc64 e34c de8a 5724 a1c3 9898 cd96 1879 .d.L..W$....y
00000200: d560 0ccb 5c26 09e4 eaf1 5894 402a 7780 . ..\g..[.k@w.
00000210: 4087 30c3 08a3 946e 72c1 a643 1db7 a060 M.0....n!.C...
00000220: 6524 629c 0c7e 8e7b 0f82 d5cb 60a0 e$b..~.{...
00000230: 003c a584 d4c1 61ef eb02 3f65 3a54 a3a2 .<..a...?e:T.
00000240: a565 c154 34c2 b162 d206 1ffb bb92 29c2 .e.T4..b....).
00000250: 8482 40d9 9010 b3a9 e478 3d02 0000 ..@....x=...
bandit12@bandit:/tmp/my_directory$ xxd -r data.txt > data.bin
bandit12@bandit:/tmp/my_directory$ ls
compressed_file data.bin data_decompressed data.gz data_raw data.txt decompressed_data hexdump.txt
bandit12@bandit:/tmp/my_directory$ file data.bin
data.bin: gzip compressed data, was "data2.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/my_directory$ 

```

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/my_directory$ cd /tmp/my_directory
bandit12@bandit:/tmp/my_directory$ file data.txt
data: ASCII text
bandit12@bandit:/tmp/my_directory$ xxd -r data.txt data.bin
bandit12@bandit:/tmp/my_directory$ ls -al
total 416
drwxr-x  2 bandit12 bandit12  4096 Mar 12 09:13 .
drwxr-x  706 root   root    409564 Mar 12 09:13 data.bin
-rw-r--  1 bandit12 bandit12  680 Mar 12 09:13 data.bin
-rw-r--  1 bandit12 bandit12  280 Mar 12 09:13 data.txt
bandit12@bandit:/tmp/my_directory$ file data.bin
data.bin: gzip compressed data, was "data2.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/my_directory$ gunzip -c data.bin > decompressed_data
bandit12@bandit:/tmp/my_directory$ ls -al
total 416
drwxr-x  2 bandit12 bandit12  4096 Mar 12 09:14
drwxr-x  706 root   root    409564 Mar 12 09:13 data.bin
-rw-r--  1 bandit12 bandit12  680 Mar 12 09:13 data.bin
-rw-r--  1 bandit12 bandit12  282 Mar 12 09:11 data.txt
bandit12@bandit:/tmp/my_directory$ file decompressed_data
decompressed_data: bzip2 compressed data, block size=900k
bandit12@bandit:/tmp/my_directory$ bunzip2 decompressed_data
bandit12@bandit:/tmp/my_directory$ gunzip compressed data, was "data4.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/my_directory$ file decompressed_data.out
decompressed_data.out: gzip compressed data, was "data4.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/my_directory$ gunzip -c decompressed_data.out
decompressed_data2: POSIX tar archive (GNU)
bandit12@bandit:/tmp/my_directory$ tar xv decompressed_data2
data5.bin
bandit12@bandit:/tmp/my_directory$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/my_directory$ tar archive data5.bin
data6.bin
bandit12@bandit:/tmp/my_directory$ file data6.bin
data6.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/my_directory$ tar xv data6.bin.out
data6.bin.out: compressed data, compressed size= 200k
bandit12@bandit:/tmp/my_directory$ bunzip2 -c data6.bin.out
bunzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/my_directory$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/my_directory$ tar xv data6.bin.out
data7.bin
bandit12@bandit:/tmp/my_directory$ file data7.bin
data7.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/my_directory$ gunzip -c data7.bin
bandit12@bandit:/tmp/my_directory$ file data7.bin
data7.bin: ASCII text
bandit12@bandit:/tmp/my_directory$ cat data9.bin
The password is w0W1BxE14CaE8LaPhau006pwRnrDw
bandit12@bandit:/tmp/my_directory$ 

```

Bandit13 -> Bandit14

The screenshot shows the OverTheWire Wargames website. At the top, there are icons of a cat and a person, followed by the text "Wargames", "Rules", and "Information". On the right, it says "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the %!." Below that are "Donate" and "Help?" buttons. The main content area has a green header "SSH Information" with "Host: bandit.labs.overthewire.org" and "Port: 2220". The title "Bandit Level 13 → Level 14" is displayed. Under "Level Goal", it says: "The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: localhost is a hostname that refers to the machine you are working on". Under "Commands you may need to solve this level", it lists: ssh, telnet, nc, openssh, s_client, nmap. Under "Helpful Reading Material", it lists: SSH/OpenSSH/Keys. On the left, there is a sidebar titled "Bandit" with a list of levels from 0 to 18.

Use the “ls” command to find the file.

The terminal window shows the following output:

```
bandit13@bandit: ~
File Actions Edit View Help
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,norelro  disable relro

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

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

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

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

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

Enjoy your stay!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$
```

For remote machine access and command execution, use the “ssh” command.

The “sshkey.private” file and the option “-i” are used to choose the identified file for RSA or DSA authentication.

```
bandit13@bandit: ~
File Actions Edit View Help
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 relro

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

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

--[ Tools ]--

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

--[ 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:C2ihUBV7ihmV1wUXRb4RrEcLfxC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? [
```

```
(kali㉿kali)-[~]
$ man ssh

(kali㉿kali)-[~]
$ ssh bandit14@bandit.labs.overthewire.org -p 2220 -i private.key
[REDACTED]

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

WARNING: UNPROTECTED PRIVATE KEY FILE!
Permissions 0644 for 'private.key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "private.key": bad permissions
bandit14@bandit.labs.overthewire.org's password: [REDACTED]

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

Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFT0ifF0ENq
bandit14@bandit:~$ [REDACTED]
```

Bandit14 -> Bandit15

Log into Bandit14 first.

The screenshot shows the OverTheWire Wargames website. At the top, there are links for "Wargames", "Rules", and "Information". On the right, there is a logo for "OverTheWire" with the tagline "We're hackers, and we are good-looking. We are the 1%." Below the logo are buttons for "Donate!" and "Help?". The main content area is titled "Bandit Level 14 → Level 15". It has a section titled "Level Goal" which says: "The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.". Below this is a section titled "Commands you may need to solve this level" containing "ssh, telnet, nc, openssl, s_client, nmap". There is also a "Helpful Reading Material" section with links to various Wikipedia articles. On the left side, there is a sidebar titled "Bandit" with a list of levels from 0 to 18, each with a corresponding link.

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.

The terminal window shows the Bandit14 shell. The user has run the command `id` to check their privileges, which shows they are a regular user named "bandit14". They then run the command `cat /etc/passwd` to view the password file. The output shows the password for bandit14 is "bandit14". The user then runs the command `nc -l -p 30000` to listen for a connection on port 30000. The terminal then shows a failed attempt to connect to the listener, indicating the password was entered incorrectly.

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

```

bandit14@bandit: ~
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelo  disable 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/)

--[ 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: $ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
bandit14@bandit: $ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tn

```

Bandit15 -> Bandit16

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

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18

Openssl – library for secure communication over networks.

Openssl s _client – implementation of a basic SSL/TLS client that communication 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.

```

bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Mar 14 12:54:43 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Mar 14 12:54:43 2024 GMT
verify return:1
Certificate chain
  0 s:CN = localhost
    i:CN = localhost
      a:PKCS1: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
      v:NotBefore: Mar 14 12:53:43 2024 GMT; NotAfter: Mar 14 12:54:43 2024 GMT
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAf0gAwIBAgIEQ/YB4DANBgkqhkiG9w0BAQUFADAUMRiwEAYDVQQDDA
b2NhGhv3QwHvhNMjQwMzE0MTIIMzQzhCNMjQwMzE0MTI1NDQzWjAUERiWeAYD
VQODDAbs2NhbGhv3QwggEiMA0GCSqGSIb3DQEBAQAA41BDwAwggEKAoIBAQDE
us21Jtc43d7KQLqwqfXbHN0ptqdDrEDkvaCM9GADB23YgCQdVFYkAkgSw7k2q
Rnc08+JFHRAAOhwon0/c4H4lVZw1kRwc4007g7PhRqZRT5TBC24nxZ6p+nVMzRk
WF0YDp2piVP47btueqnPOySAPt0Fy/Bv2TxizLgY8owdBf5gPdDN6uZ4e3HA
foAGytWFv5ql6iNB06eXIAkCoBbtQzIDPaMjZAJuSjGI1Ts8veTwSTFSsze6pBB
D8tIxkfovxRoDA10FJ3mNh7CPSEGM0ez/eJUmx+C0a4FNFD/KKYIGUA4+YdqR
QTGYJnxqhS3NiuKMLZAgMBAAGjZTBjMBGA1uEQNNAuCCWxvY2Fsa09zDBL
Bg1ghkgbhvhnCAQEPhy8QXv0b21hdGljWxseSbnZw5lcmf0zWqgYnkgTmNhdC4g
U2VLIGH0dhBz0i8vbmlhcC5cmcvBnhdC8uMA0GCSqGSIb3DQEBBQQA4IBAQZC
4pkOBM12hjvUK4TRLd0FGDkxxY1FVNndtuxLBafyLMEMN4m2FLDj1hdjwD23dxTp
iaWfsmVXmNeDdsFM8WY7ofx8trNq1s9hMsB/juTkHlxuruQ193D1g6cJBkAUhFx
h60GmG9FBY8mu56h1UgCh0LxmWx73CuJMMR8xgzeq0wafxFg+7C6yx8RjYUxHR
F/8CdIshnkf/BHJ4TQ0kgDw0hSUVxObMHxi91xkvWdd8dY5rgNzml8f0IW+SLtp0
t6QEioLyqCOWQvups5ZYR60DPUInjmnxKRNldO1K8CIJrJ7pUefKMX9xA4o@U50h
ve/FweHUPKmuK4jybeI
-----END CERTIFICATE-----
subject=CN = localhost
issuer=CN = localhost

```

```

bandit15@bandit:~$ openssl s_client -connect localhost:30001
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

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 10 (certificate has expired)

Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol : TLSv1.3
  Cipher   : TLS_AES_256_GCM_SHA384
  Session-ID: D9E9D28E003961D1AABD4F41E65804E09172F2BFCG64D5C30EA20736BF0D0686111D6C8188BB72DC43D470C042A6BB
  Session-ID-ctx:
  Resumption PSK: D9E9D28E003961D1AABD4F41E65804E09172F2BFCG64D5C30EA20736BF0D0686111D6C8188BB72DC43D470C042A6BB
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)
  TLS session ticket:
  0000 - b2 46 65 34 95 aa c6 53-57 49 c7 21 a4 22 b8 d5 ...Ke4 ...SWI.!."..
  0010 - b2 46 fb 19 3b 98 48 d1-14 7b 81 cb 29 69 ee b4 ..D.;.H.(..)i..
  0020 - 99 87 af 76 fo c1 8b 18-a5 df c1 f3 38 d0 78 8c ..v.....8.x.
  0030 - fd c1 e3 43 b8 5c 0d 63 ee-72 32 00 8f 39 e8 10 ..C.\.c.r2...9..
  0040 - c5 60 ef 66 19 49 8a f4-a1 d0 60 fc 3d 97 d4 c1 ..^f.I....n.=M.
  0050 - 70 44 78 a8 1d 41 e1 25-6c 57 18 a6 32 05 96 b0 pDx..A.%!W..2...
  0060 - ed 9b 5e ce fd 20 92 08-08 fe f1 c9 79 3c de 2b ..^ .. ....Y<+
  0070 - 38 16 0e 76 74 02 70 7c-db ea c6 69 75 58 da f0 8..vt.p[...iuX..
  0080 - 8a 17 9e b8 e0 20 94 3f-1b 75 e3 a5 1c e9 c4 f0 .....?..u.....
  0090 - 1d ce 18 37 b2 ba 5c d8-08 93 5d 89 95 3a c4 1a ...7..\...].:...
  00a0 - 7b cd 60 b5 7e d6 b3 0b-cb 26 90 f4 4e f8 40 01 {.^~....&..N.@.
```

After run that we need to type the password of bandit 15. When we type it shows the Bandit16 password.

```

bandit15@bandit:~

File Actions Edit View Help
—
read R BLOCK
—
Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher   : TLS_AES_256_GCM_SHA384
Session-ID: AAB2D53D464AF4A57D8AFC8EDC12ADF9CA90EBDC076A86DBBE3C90CA4BB9F7F
Session-ID-ctx:
Resumption PSK: A28739032DAE44CB1CC697B989BB296064F20A85270BAEDED50F7356E3B4B6575F2B3A3B60271940CC9C42F8EDCDC67A
PSK identity: None
PSK hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - 5f 4b 65 34 95 aa c6 53-57 49 c7 21 a4 22 b8 d5 _Ke4 ... SWI.!."..
0010 - b2 04 9c d4 28 55 75 ea-c5 b9 3a 74 0a 8d 67 0a ....(Uu...:t..g...
0020 - 9d 29 9e 7c 52 c2 36 24-93 dc 2e 01 fb ef 48 65 .).|R.6$....He
0030 - a0 73 69 f1 f6 01 32 95-79 48 cc 52 9f df 3e 6b .si...2.yH.R...>k
0040 - d8 56 00 5e b7 0f-e3 a9 3d 82 5e 95 77 96 ..V... ....<.^w.
0050 - bf f6 cd 94 8e 81 88 a2-85 0c b5 4f cd 2a 93 ca .....0.*..
0060 - 48 43 48 02 49 35 f9 c9-5e ce 3d f4 a4 77 ca 6d HCH.I5..^.= w.w.m
0070 - 0f 1c a9 e5 cd 16 9f 89-1e 05 63 dc 4b 89 fc fb .....c.K...
0080 - 36 99 73 a4 36 c8 7d 30-2a 0e 7f 1d ef da da 5f 6.s.6.{0*.....
0090 - 14 99 17 c2 1b 04 6c 13-12 5c d8 a7 62 2e aa 01 .....l..`..b...
00a0 - fb 88 d5 ff 11 74 a6 2b-5d 9b 8d 92 4a cb fb 3f .....t.+)...J.?
00b0 - 83 f7 27 bf 83 fc 4e 10-bf 8c cd d8 5b 72 29 2e ...'. N....[r].
00c0 - cc 0e c9 63 54 be 77 4d-ee 0d 48 b9 ba d1 76 41 ...ct.wM..H..VA

Start Time: 1710616836
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
—
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQtffApKAseyHwDlI9SXGR50qclOAi1i

closed
bandit15@bandit:~$ █

```

Bandit16 -> Bandit17

Login into the bandit 16.

The screenshot shows the OverTheWire Bandit Level 16 page. At the top, there are two cartoon cat avatars. The main content area has a green header bar with "SSH Information" and the host details: Host: bandit.labs.overthewire.org, Port: 2220. Below this, the title "Bandit Level 16 → Level 17" is displayed. 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." The "Commands you may need to solve this level" section lists: ssh, telnet, nc, openssl, s_client, nmap. The "Helpful Reading Material" section links to "Port scanner on Wikipedia".

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

```

bandit16@bandit: ~
File Actions Edit View Help
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/l�ngld/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/)

-- [ 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 2024-03-16 19:29 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.11 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.

```

bandit16@bandit: ~
File Actions Edit View Help
bandit16@bandit: $ openssl s_client -connect localhost:31790
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Mar 14 12:54:42 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Mar 14 12:54:42 2024 GMT
verify return:1

Certificate chain
 0 s:CN = localhost
    i:CN = localhost
      a:PKCS#12:rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
      v:NotBefore: Mar 14 12:53:42 2024 GMT; NotAfter: Mar 14 12:54:42 2024 GMT
      -----
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCAf0gAwIBAgIEaM0gijANBgkqhkiG9w0BAQUFADAUMRiwEAYDVQQDDAIs
b2NhGhvC3QwHncNMjQwzE0MTIiMzQywJhNNjQwZEMTT1NDQyWjAUERiWeAYD
VQDDA1lsb2NhGhvC3QwggiMA0GCSqGSIb3DQEBAQAA4IBDwAwggEKAoIBAQcd
ubekPn1KM8bMd+HT5JOyYpqlrwY42n50i+zB0pXXvKvuU4+5rx3HPRe9SLT
00DW9WUAOxzqtjrgu70Ez7yLxUoPrzLJw/z+Mtd83BX2RLhtUUJXCaF3m0kM
V9L2UWfpFWG1uhVvW83Wgud+c17Yb9HFmnDd0tRpbB0oHsq/SJuHpcx2mu6ht
5tj4CsyyJC0Ha/Xl6l6NMFG+Vfu2NUzjQQj0VQuHIT18eEDxNJUsaBaideMK6W4
Ufbu6x7s3/ohsAOgCoMtospMptF89wEnG7twfLf9wNccg2V1Tp/Dy6w/vn7NsP
Z5t50ugJg4buJ6Ne1a/AgMAAGjZTBjMBGAl1dEQNMuAUCCWxvY2Fsa09zdBL
Bg1ghkgBhvhaCA0EPhy8QXv0b21hdGljYwxseSbNzW5lcmf0zWQgYnkgtMNdC4g
U2V1Gh0DHbz018vb1hcC5vcmcVbmNhdC8uMA0GCSqGSIb3DQEBBQQAiBAQAM
hjaXgdXKg+a3cwQ1y2LbbAfHVtvpHeu15OTvBTel8AC341pfXkknQliBAKwnQ
/OPZrmeSyRcvkORE/TkM0R9qJHuJzQC/qdw8n2RhFD13i5Myz0fJ1HgJoBAc0i
+yhTEmx0g3HfimC72/9cEPN3GejXnIewN8GOpC6+uwySXQzj7Ahcf01KvrJ3Qqd
J56JcohfgE4i066JxFdxJYH4MbCjxzNVgXdiE7y+nDNAZy7NBusqkhdt51Kdg+
B0utjwXx4YYSkdFEfp0JTIc2kFdez8Ewe423Vjf/U0JHgolP+peFqsKxVi/LMlvk
3gAW1u6eUq1mUnmc0tZ
-----END CERTIFICATE-----
subject=CN = localhost
issuer=CN = localhost

```

Save this key locally. Use a ssh private key. “ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220”.

Bandit17 -> Bandit18

The screenshot shows the OverTheWire Wargames website with the title "Bandit Level 17 → Level 18". On the left, there's a sidebar titled "SSH Information" with the host "bandit.labs.overthewire.org" and port "2220". Below it is a "Bandit" section listing level transitions from 0 to 17. The main content area contains a "Level Goal" section with instructions about comparing files "passwords.old" and "passwords.new", a note about solving bandit18, and a list of commands ("cat, grep, ls, diff") needed to solve the level.

diff – program compares files line by line.

Run the ls command and get the file name.

The terminal window shows the user is on the Bandit17 shell, with the prompt "bandit17@bandit: ~". The window title is "File Actions Edit View Help". The terminal displays a message about the machine's processor and security features, compiler flags, and available tools like gef, pwndbg, peda, gdbinit, pwntools, and radare2. It also provides links for more information, support, and a note about network access being limited by a local firewall. At the bottom, the user runs the command "ls" which lists the files "passwords.new" and "passwords.old".

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

```

sahan@kali: ~
File Actions Edit View Help
executable on ELF binaries.

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

--[ Tools ]--

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

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

--[ 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!

bandit17@bandit: $ ls
passwords.new passwords.old
bandit17@bandit: $ diff password.old password.new
diff: password.old: No such file or directory
diff: password.new: No such file or directory
bandit17@bandit: $ diff passwords.old passwords.new
42c42
< p6ggwdNIncmCNxUAt0tkVq185ZU7AW
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit: $ exit
logout
Connection to bandit.labs.overthewire.org closed.

```

Bandit18 -> Bandit19

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

Level Goal

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.

Commands you may need to solve this level

`ssh, ls, cat`

Level	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
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																			

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.

```

(sahan@kali)-[~]
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 -t "/bin/sh"
[The quietest you become, the more you are able to hear]

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

bandit18@bandit.labs.overthewire.org's password: 

```

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

The screenshot shows a terminal window titled "sahan@kali: ~". The window displays a welcome message from the OverTheWire team, listing several useful tools installed in /opt/. It includes links for gef, pwndbg, peda, gdbinit, pwntools, and radare2. Below this, there's information about wargames, support via discord or IRC, and a "Byebye!" message indicating the connection to bandit.labs.overthewire.org has closed. The terminal then shows a user attempting to ssh into bandit18@bandit.labs.overthewire.org, which fails due to a missing command-not-found database. A command not found error is also shown for 'c:\Users\ADMIN'. Finally, the user successfully connects to bandit18@bandit.labs.overthewire.org using port 2220 and runs "/bin/sh", leading to a shell prompt. A small ASCII cat logo is displayed above the shell prompt. The terminal ends with a message from OverTheWire: "This is an OverTheWire game server. More information on http://www.overthewire.org/wargames".

Bandit19 -> Bandit20

The screenshot shows the OverTheWire Wargames website. At the top, there's a navigation bar with "Wargames", "Rules", 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 sidebar with "SSH Information" (Host: bandit.labs.overthewire.org, Port: 2220) and a "Bandit" section listing levels from 0 to 18. The main content area is titled "Bandit Level 19 → Level 20". It contains a "Level Goal" section with the instruction: "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." It also includes a "Helpful Reading Material" section with a link to "setuid on Wikipedia". At the bottom right of the main content area, there are "Donate" and "Help?" buttons.

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

```
bandit19@bandit: ~
File Actions Edit View Help
-fno-stack-protector      disable ProPolice
-Wl,-z,norelro           disable relro

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

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

--[ Tools ]--

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

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

--[ 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 Oct  5 06:19 .
drwxr-xr-x  70 root      root      4096 Oct  5 06:20 ..
-rwsr-x---  1 bandit20 bandit19 14876 Oct  5 06:19 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: ~
File Actions Edit View Help
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

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

--[ Tools ]--

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

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

--[ 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 Oct  5 06:19 .
drwxr-xr-x  70 root      root      4096 Oct  5 06:20 ..
-rwsr-x---  1 bandit20 bandit19 14876 Oct  5 06:19 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
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit: $
```

```
bandit19@bandit: ~
File Actions Edit View Help
firewall.

--[ Tools ]--

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

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

--[ 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 Oct  5  06:19 .
drwxr-xr-x  70 root      root      4096 Oct  5  06:20 ..
-rwsr-x---  1 bandit20 bandit19 14876 Oct  5  06:19 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
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit0  bandit11  bandit14  bandit17  bandit2  bandit22  bandit25  bandit28  bandit30  bandit33  bandit6  bandit9
bandit1  bandit12  bandit15  bandit18  bandit20  bandit23  bandit26  bandit29  bandit31  bandit4  bandit7
bandit10 bandit13  bandit16  bandit19  bandit21  bandit24  bandit27  bandit3  bandit32  bandit5  bandit8
bandit19@bandit:~$
```

```
bandit19@bandit: ~
File Actions Edit View Help
firewall.

--[ Tools ]--

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

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

--[ 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 Oct  5  06:19 .
drwxr-xr-x  70 root      root      4096 Oct  5  06:20 ..
-rwsr-x---  1 bandit20 bandit19 14876 Oct  5  06:19 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
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit0  bandit11  bandit14  bandit17  bandit2  bandit22  bandit25  bandit28  bandit30  bandit33  bandit6  bandit9
bandit1  bandit12  bandit15  bandit18  bandit20  bandit23  bandit26  bandit29  bandit31  bandit4  bandit7
bandit10 bandit13  bandit16  bandit19  bandit21  bandit24  bandit27  bandit3  bandit32  bandit5  bandit8
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass?bandit20
cat: '/etc/bandit_pass?bandit20': No such file or directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass bandit20
cat: /etc/bandit_pass: Is a directory
cat: bandit20: No such file or directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykJ6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$
```

All Level Passwords

Level 00 password = bandit0

Level 01 password = NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Level 02 password = rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Level 03 password = aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Level 04 password = 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Level 05 password = lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Level 06 password = P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 07 password = z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 08 password = TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 09 password = EN632PlfYiZbn3PhVK3XOGS1NIInNE00t

Level 10 password = G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 11 password = 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Level 12 password = JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Level 13 password = wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 14 password = fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Level 15 password = jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 16 password = JQttfApK4SeyHwDlI9SXGR50qclOAi11

Level 17 password = VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

Level 18 password = hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

Level 19 password = awhqfNnAbc1naukrpqDYcF95h7HoMTrC

Level 20 password = VxCazJaVykl6W36BkBU0mJTCM8rR95XT

Conclusion

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

References

1) Medium –

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

2) YouTube –

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

3) OverTheWire –

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

**IT22083678
SAHAN H P T**