OverTheWire – Bandit lab
Proof of Concept Report

by

Vibhuti Naik
(Intern ID: 2046)

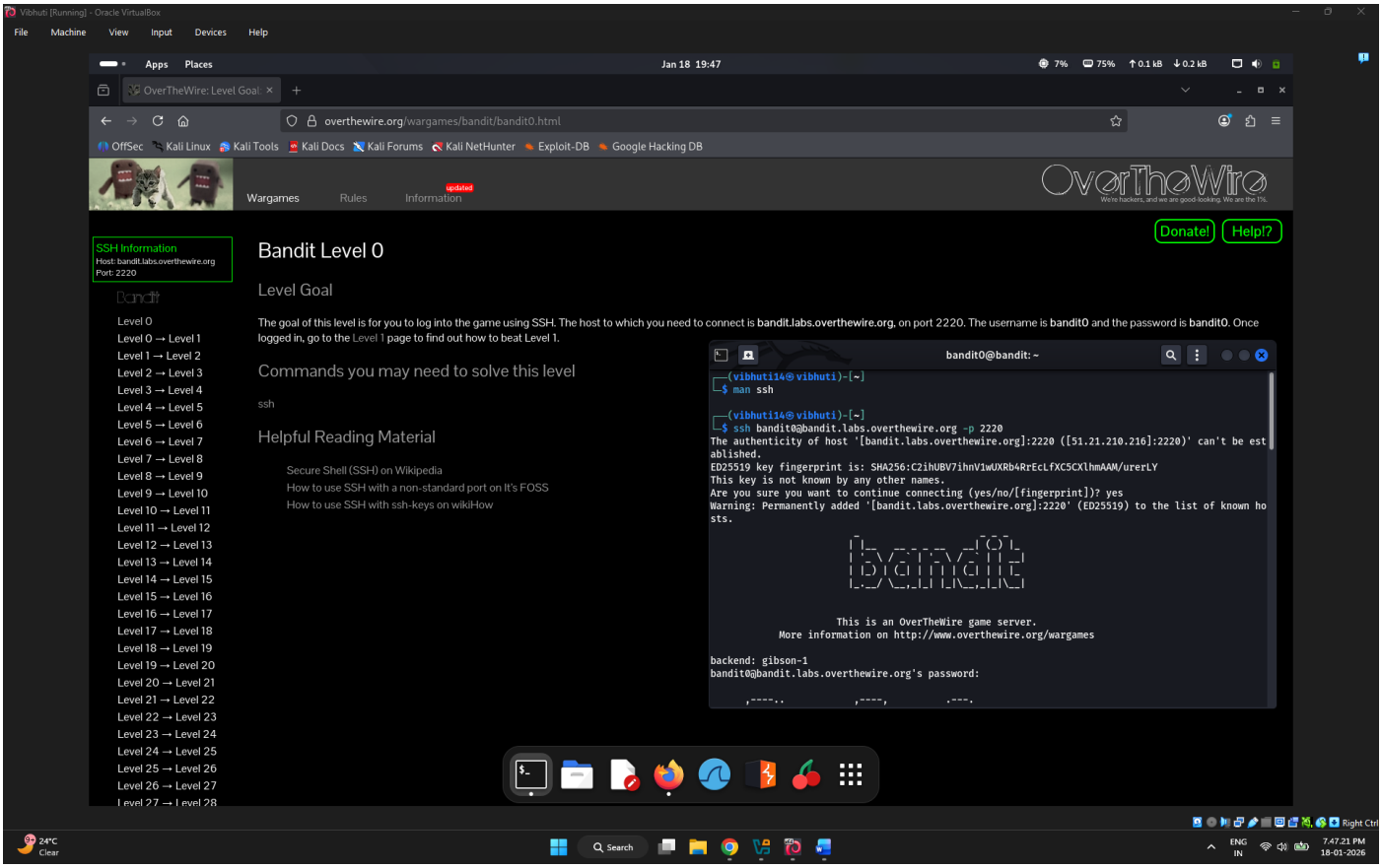
OverTheWire – Bandit

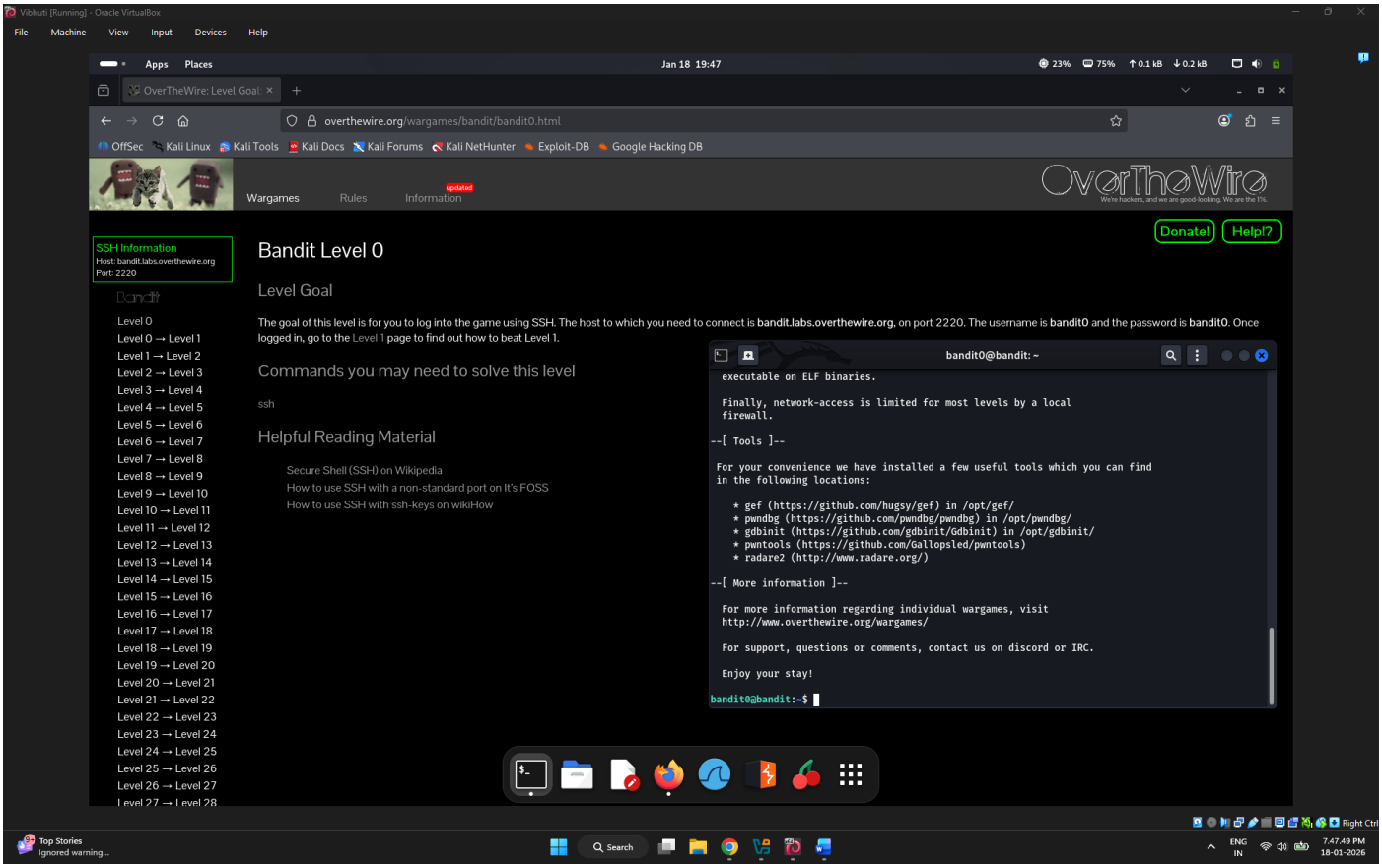
This report contains a walkthrough for all 34 levels of the Bandit wargame on OverTheWire.
Link to Bandit wargame: https://overthewire.org/wargames/bandit/

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.





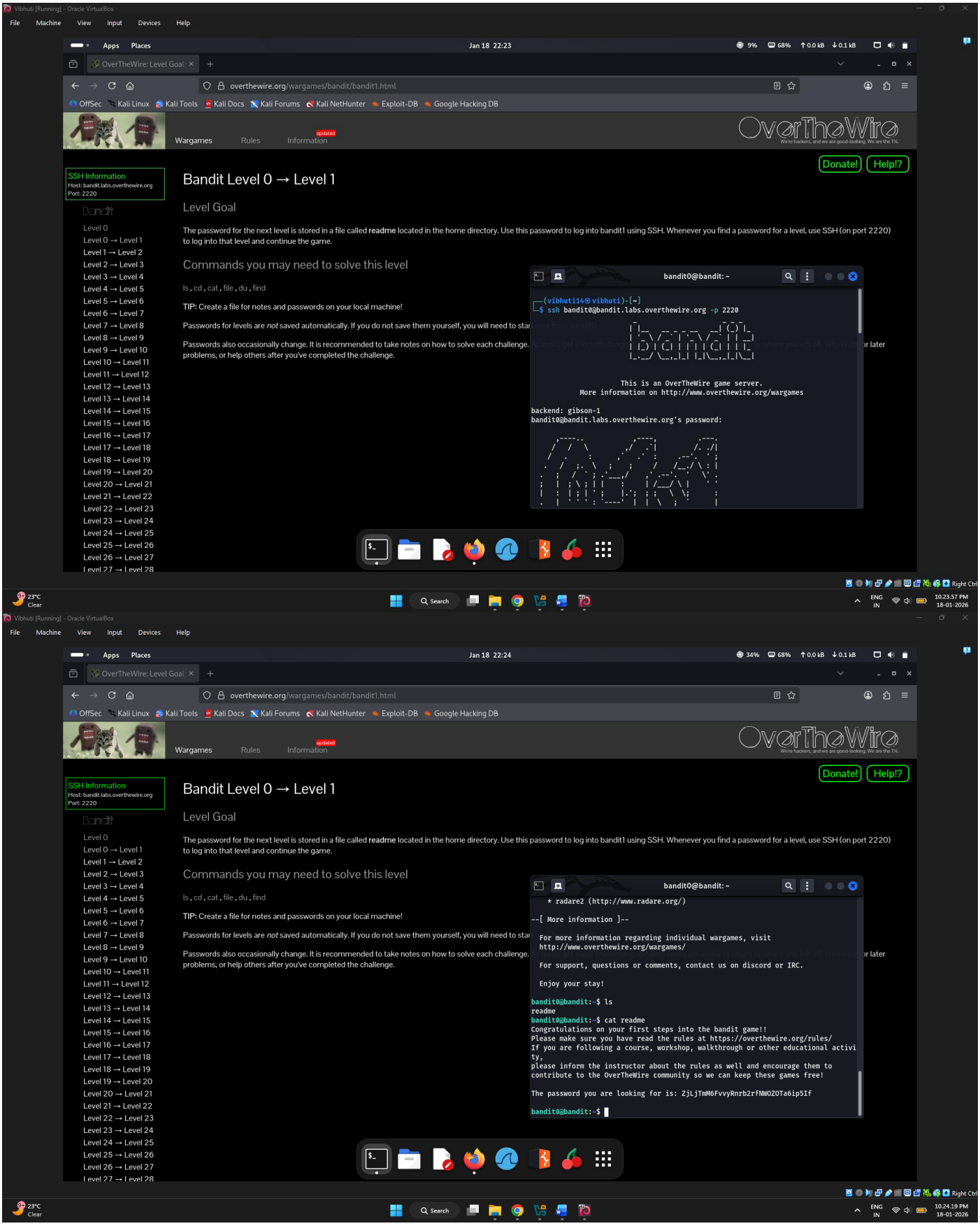
Level 0 -> Level 1

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.



Level 1 -> Level 2

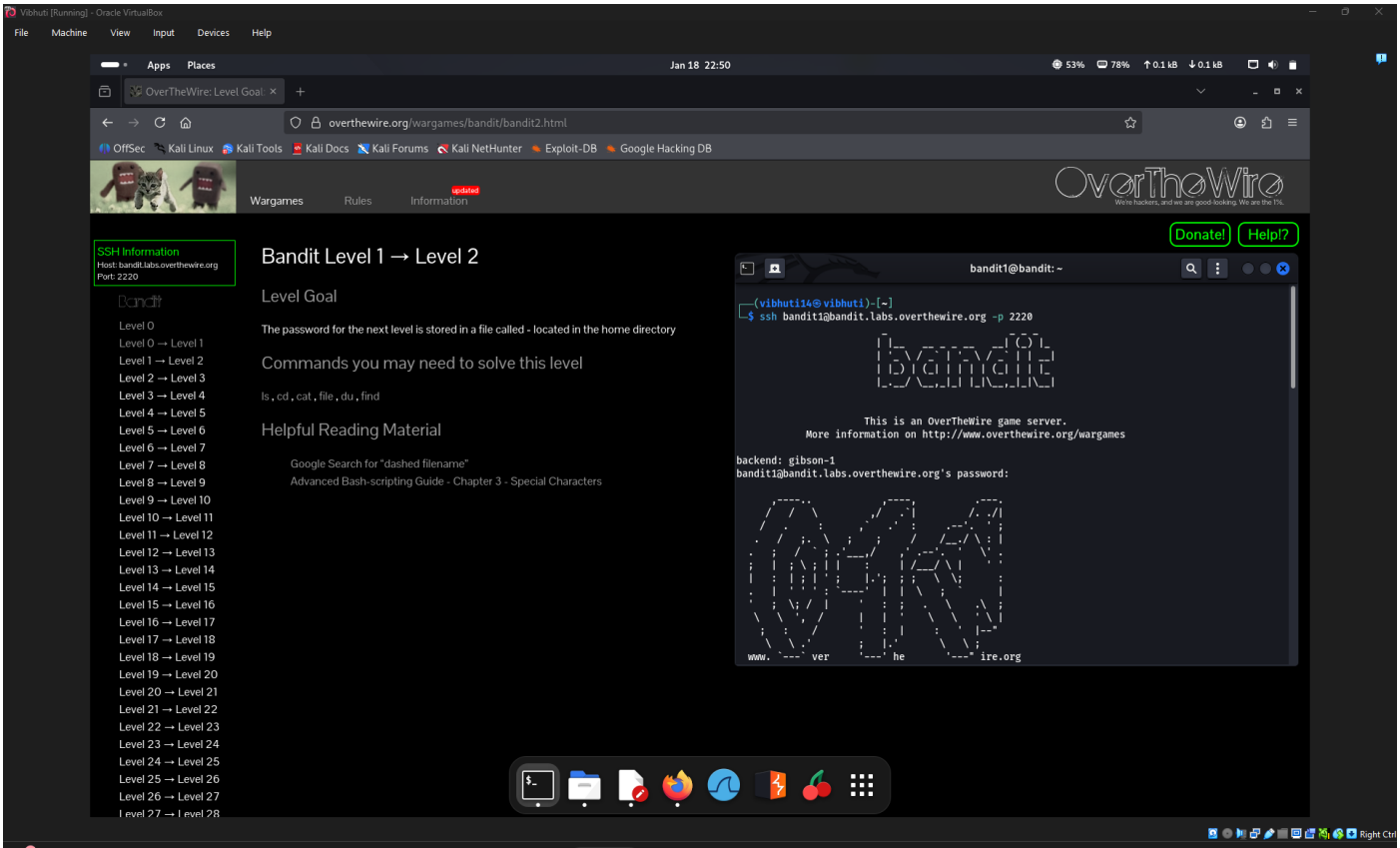
Tools Used: ls, man, cat

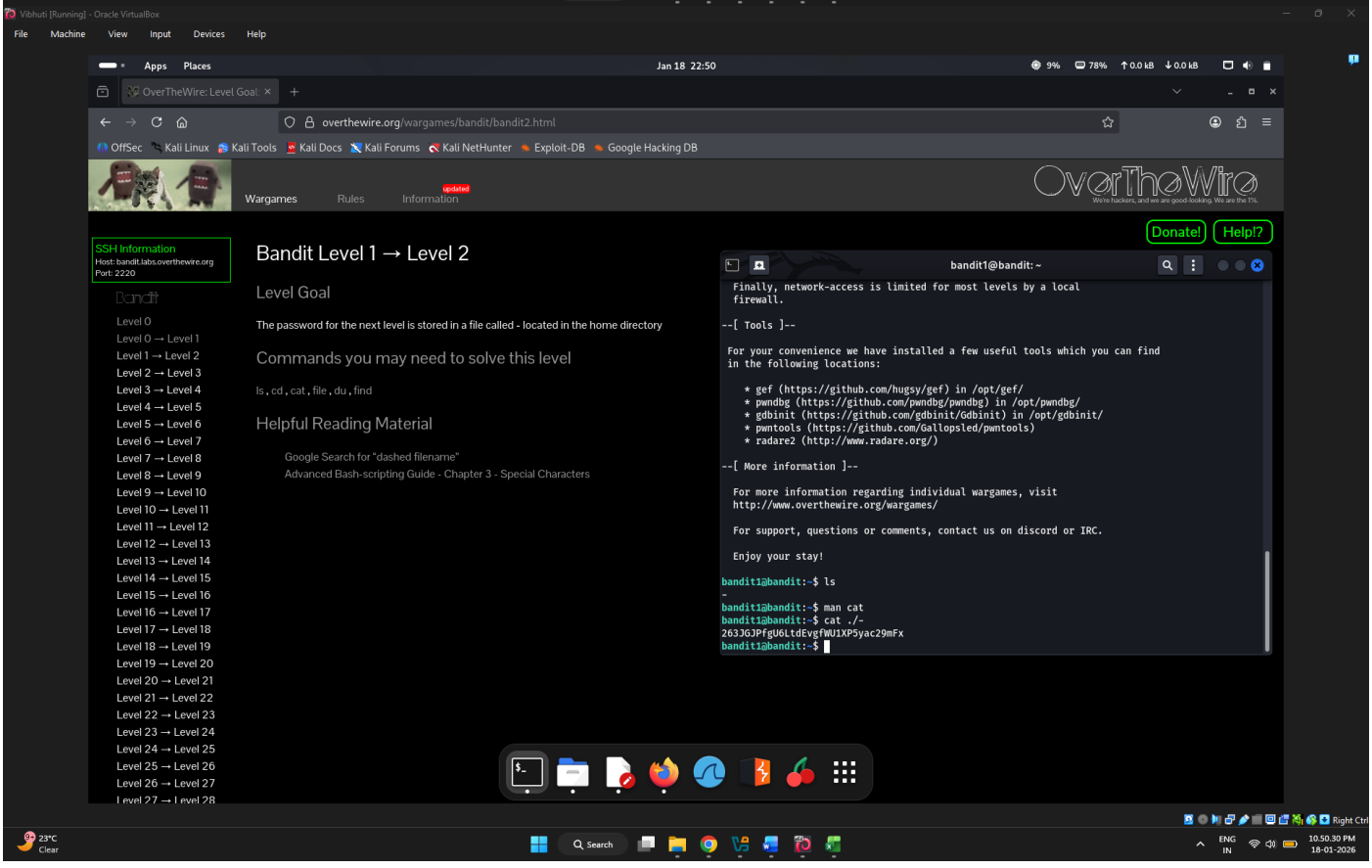
Objective: Extract password from file called '-'.

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 ./-





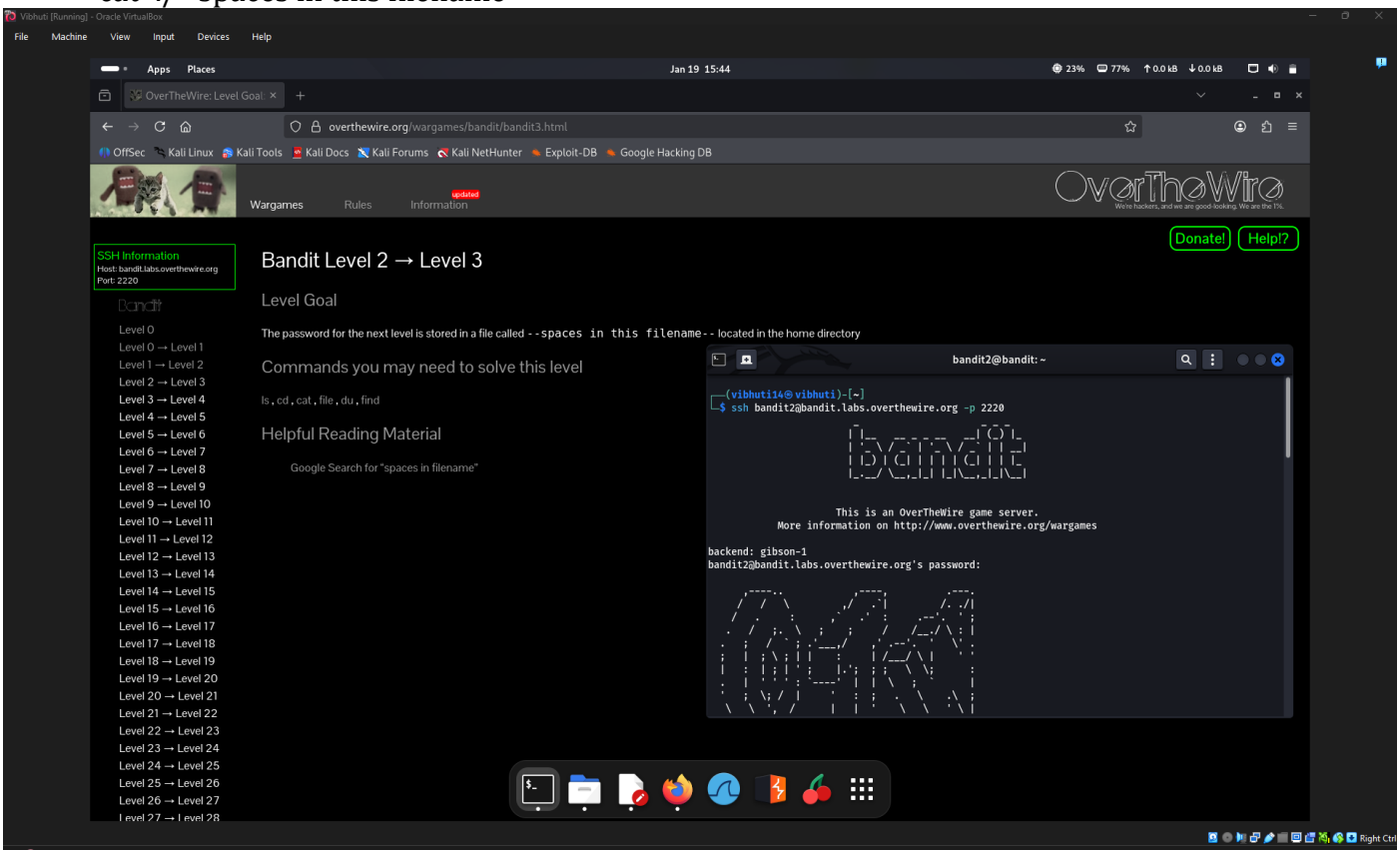
Level 2 -> Level 3

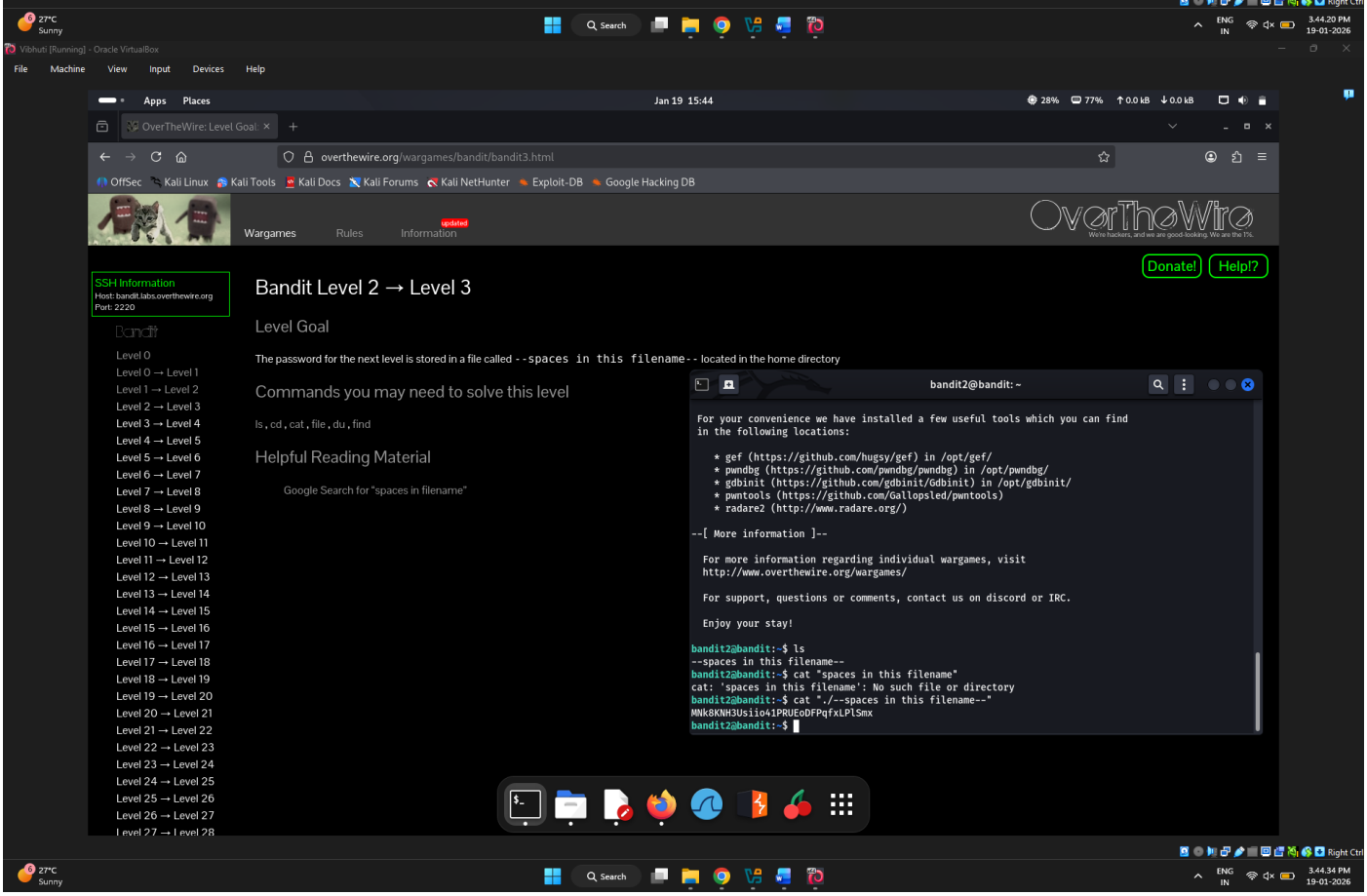
Tools Used: ls, cat

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--"

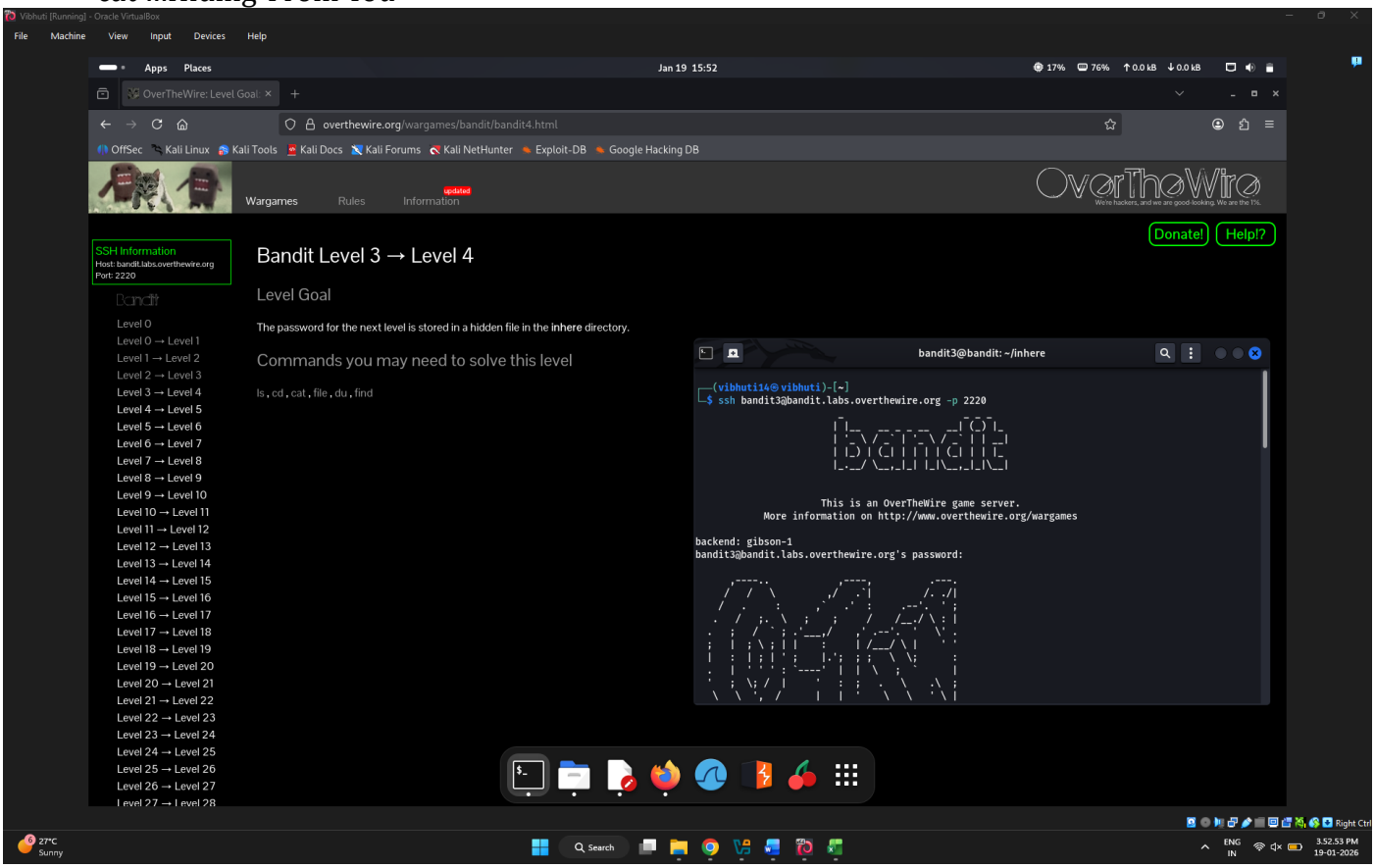


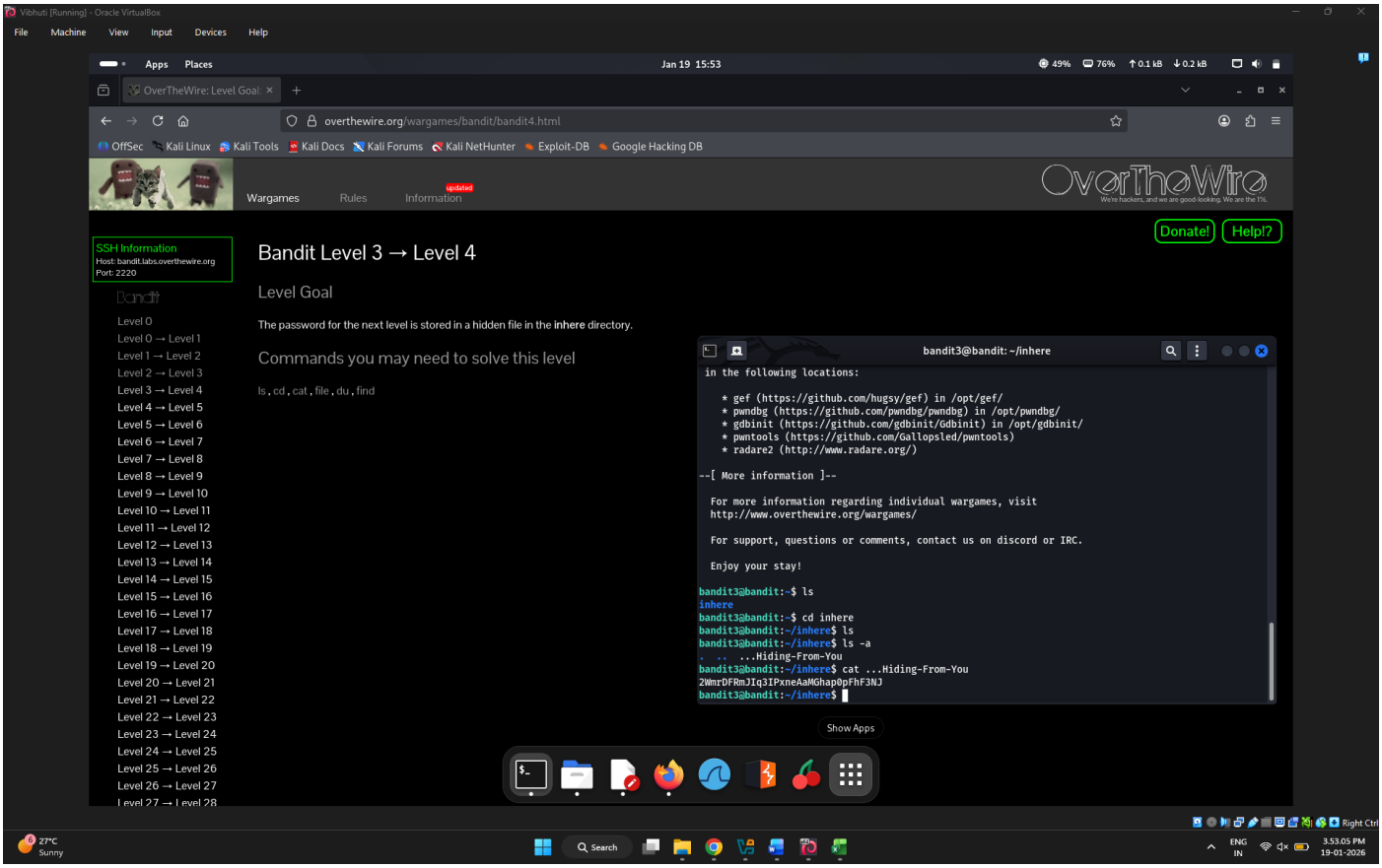


Level 3 -> Level 4

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





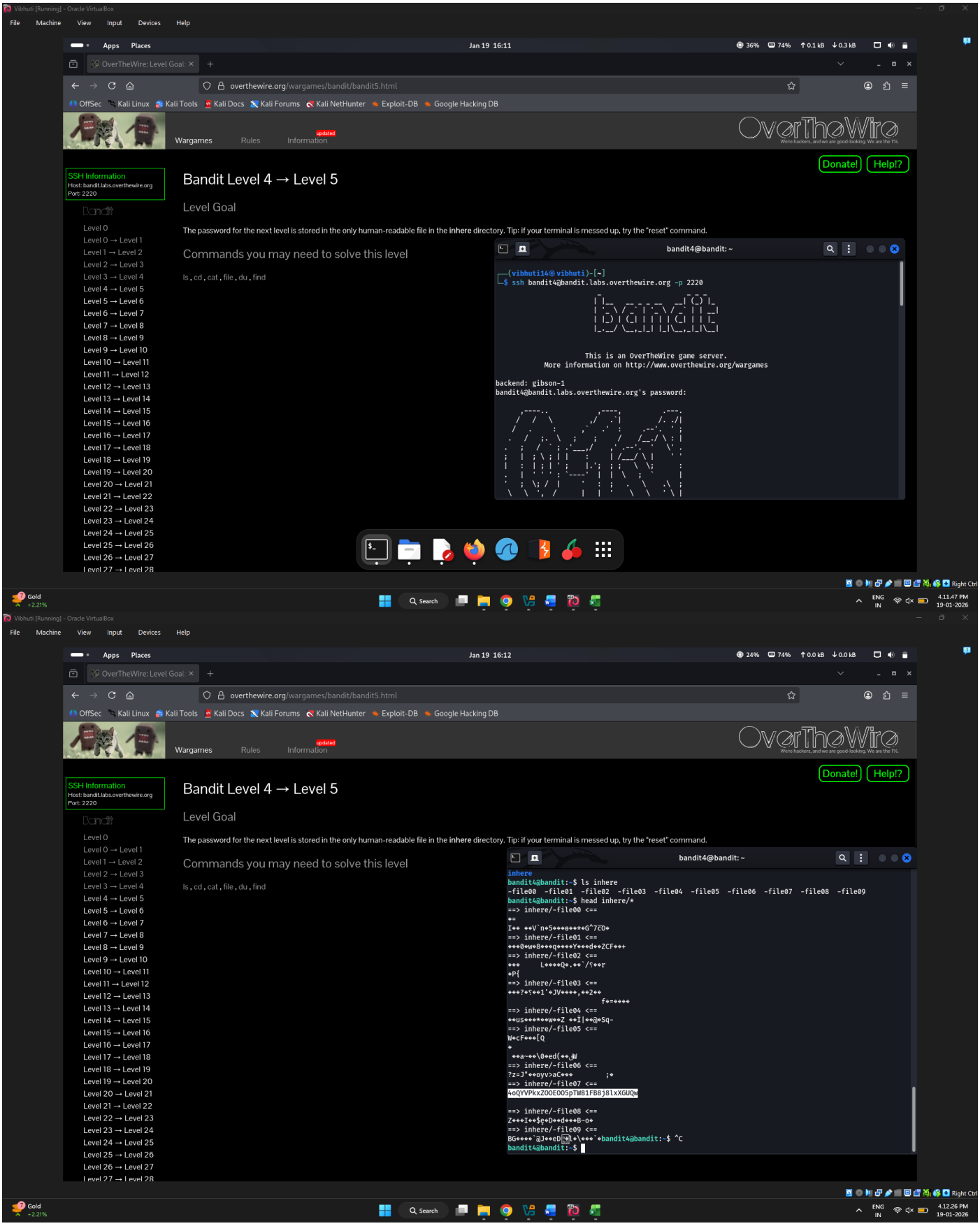
Level 4 -> Level 5

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/*



Level 5 -> Level 6

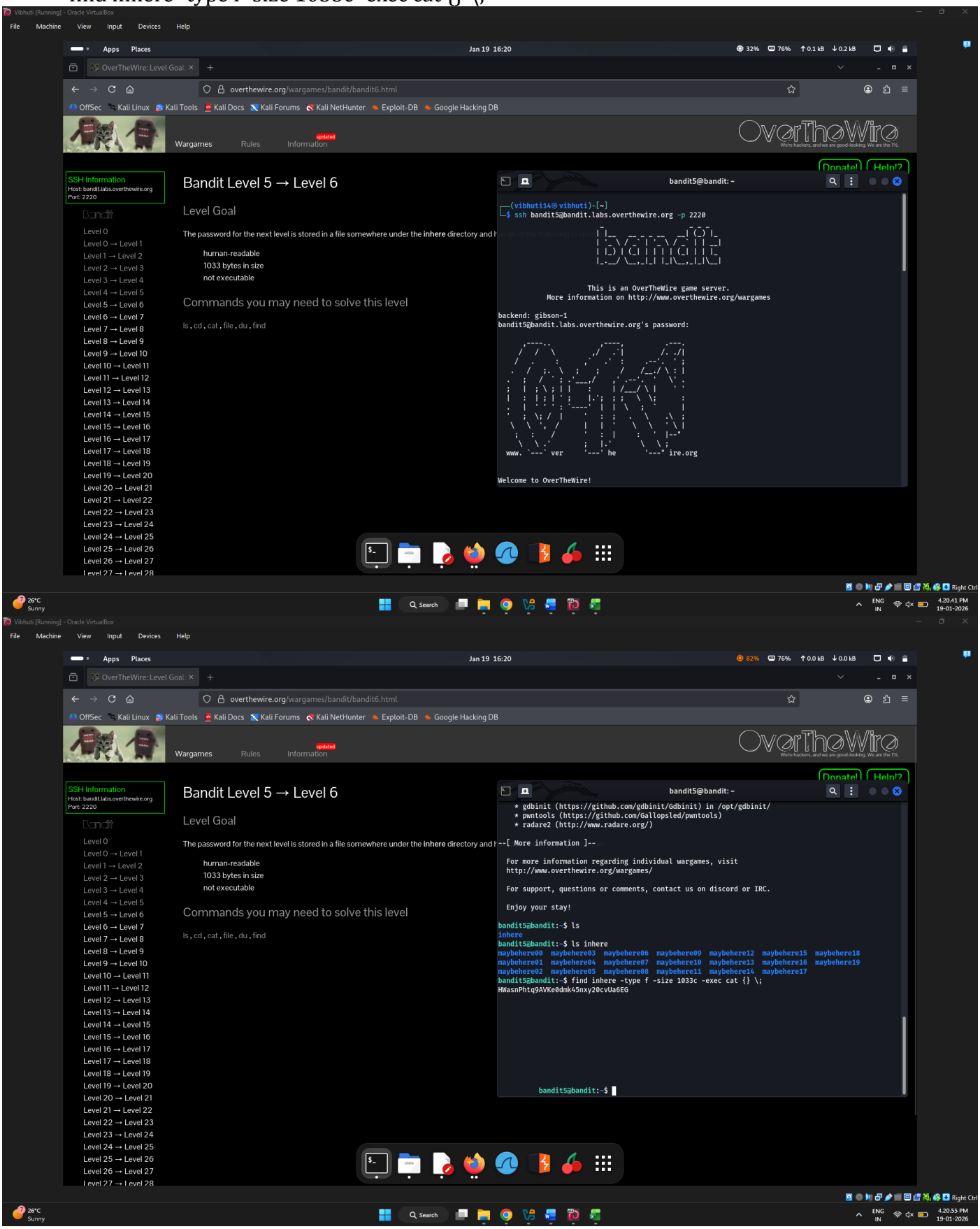
Tools Used: ls, cat, find

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 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 {} \;



Level 6 -> Level 7

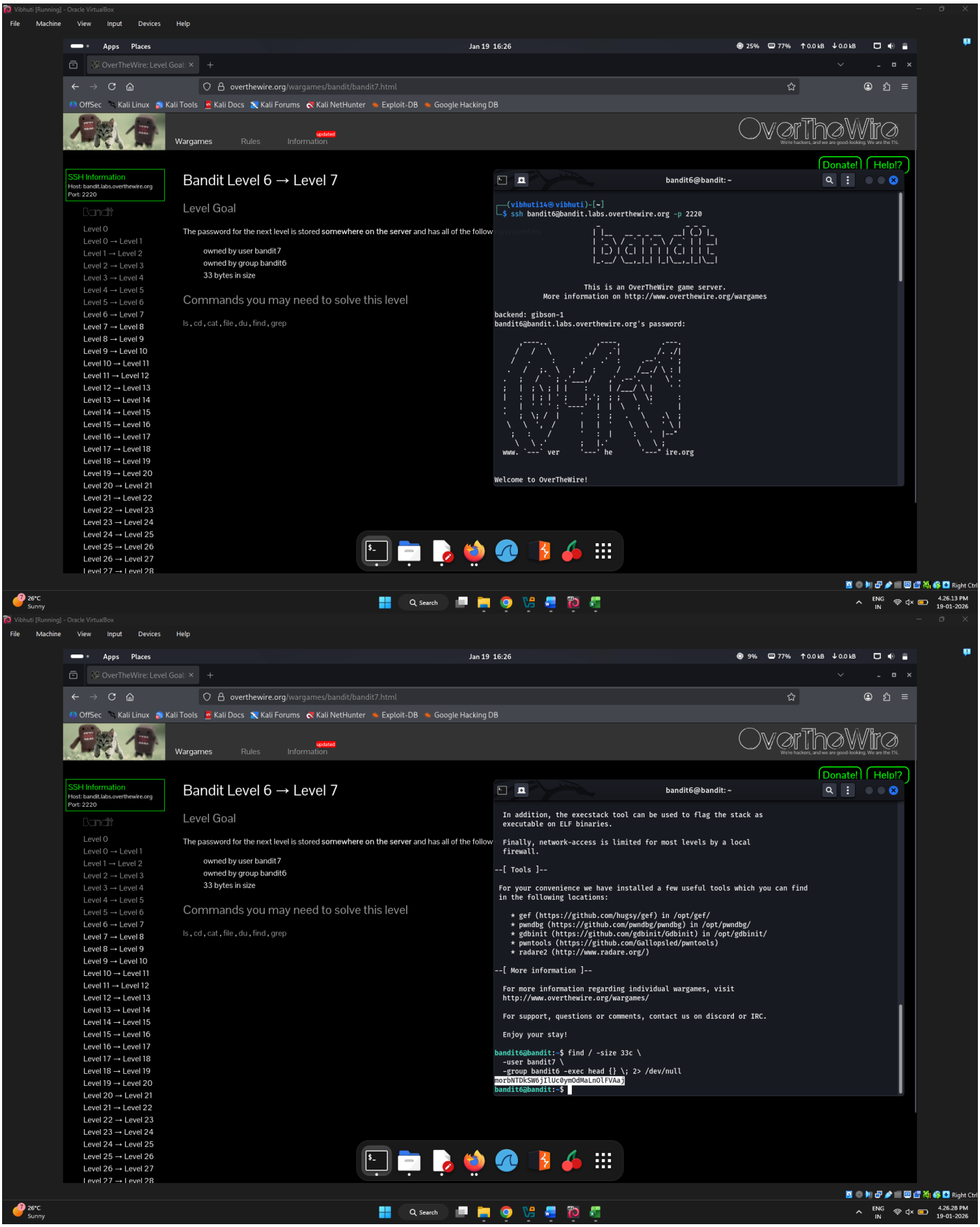
Tools Used: find

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



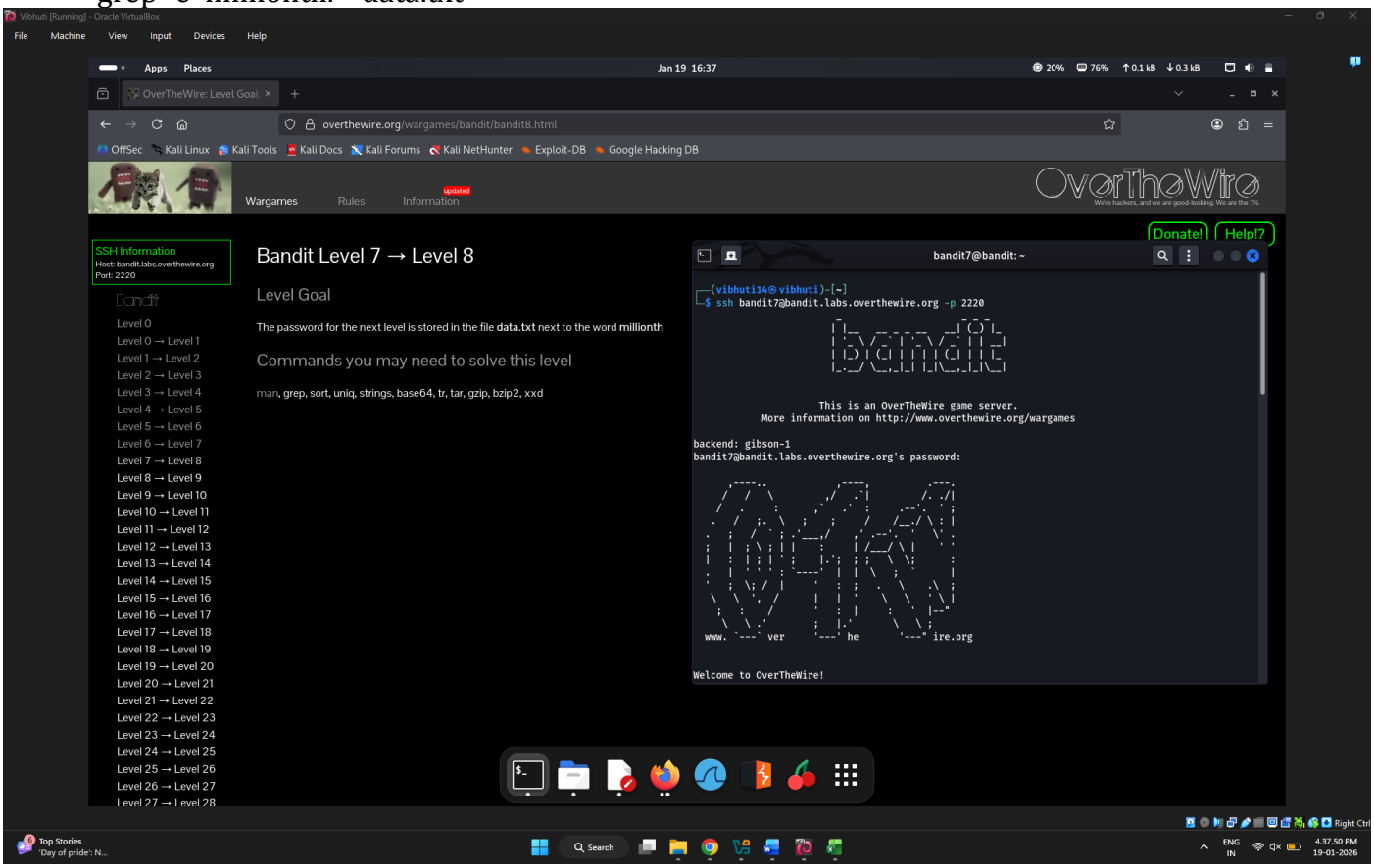
Level 7 -> Level 8

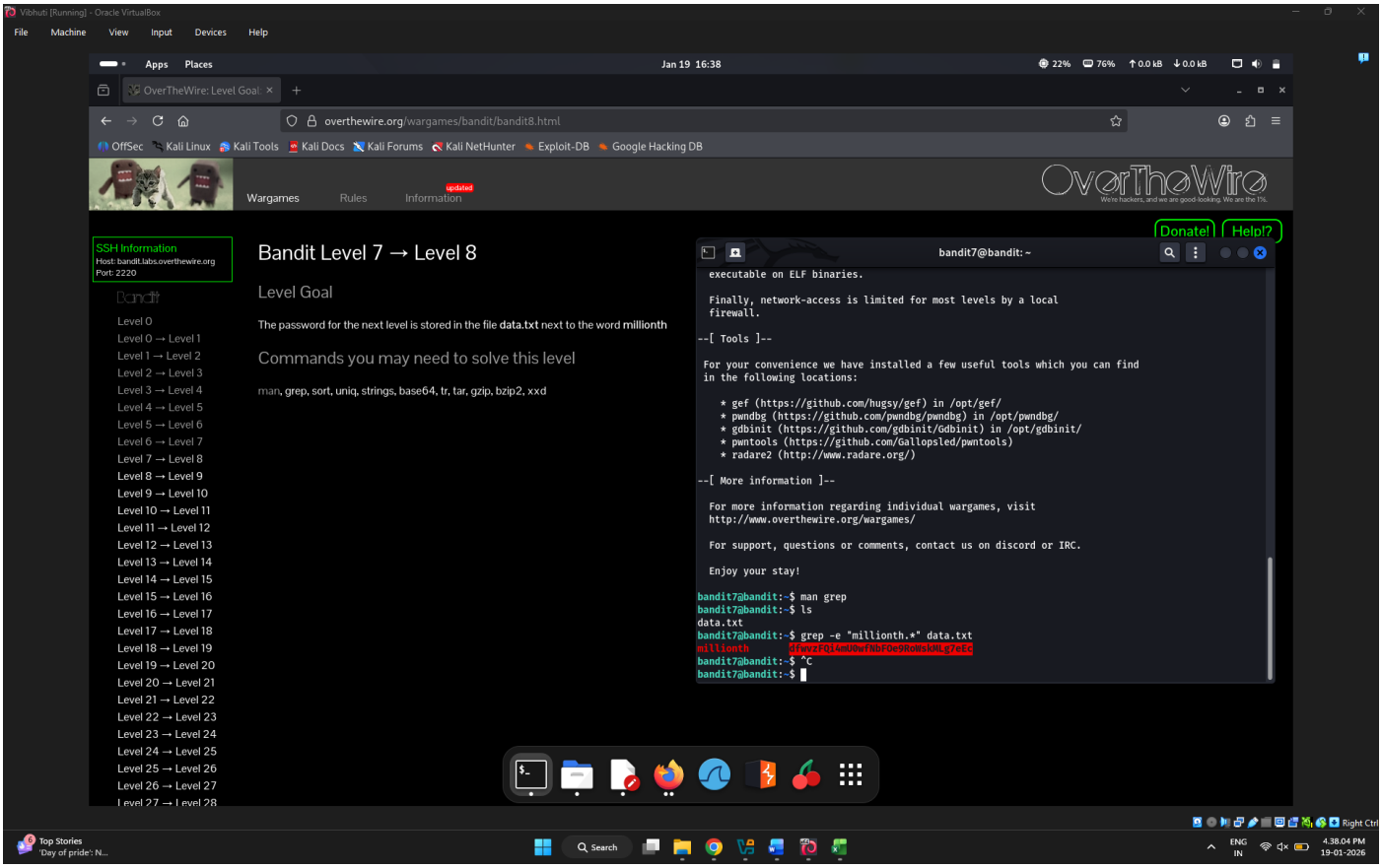
Tools Used: ls, grep

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





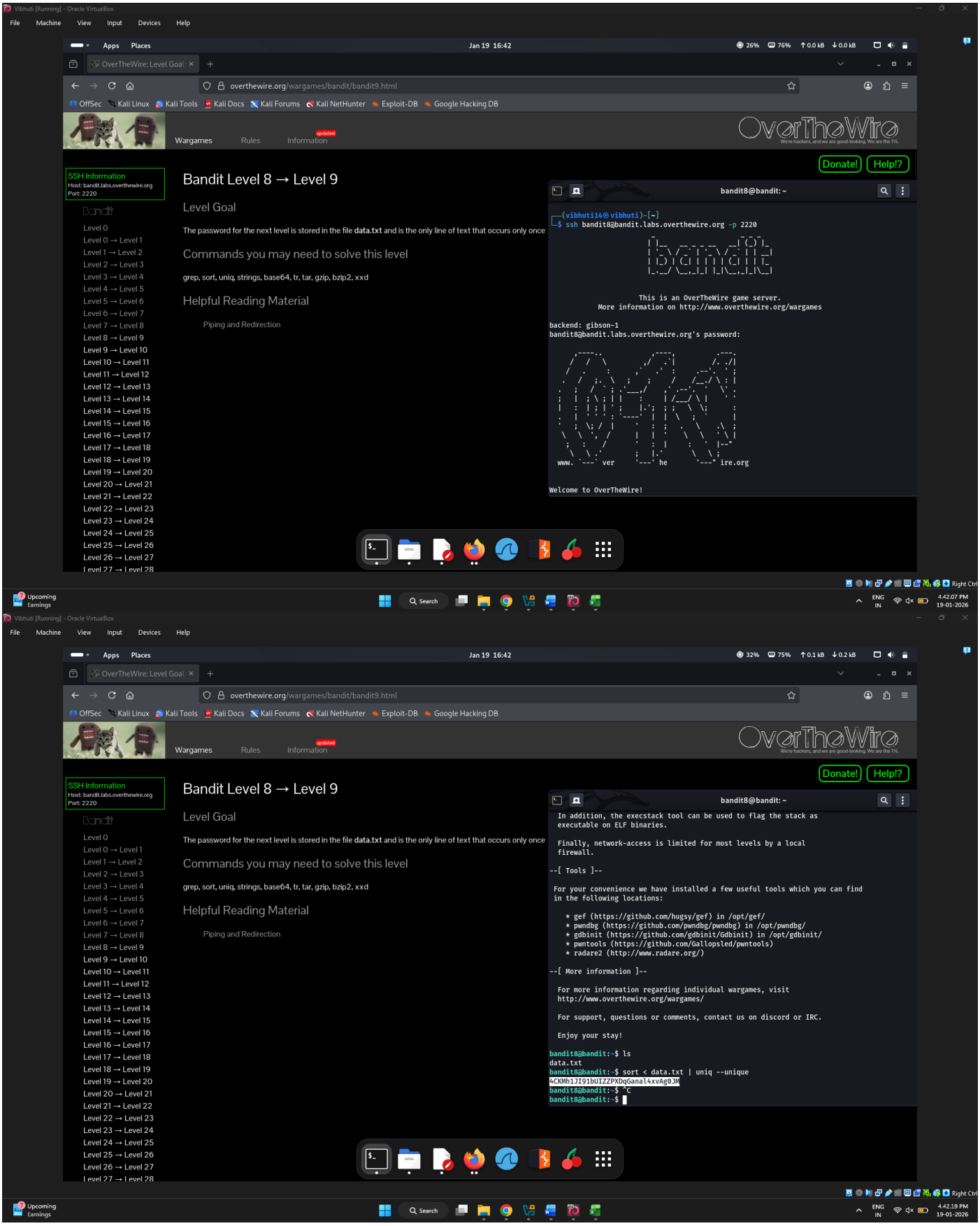
Level 8 -> Level 9

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



Level 9 -> Level 10

Tools Used: strings, grep

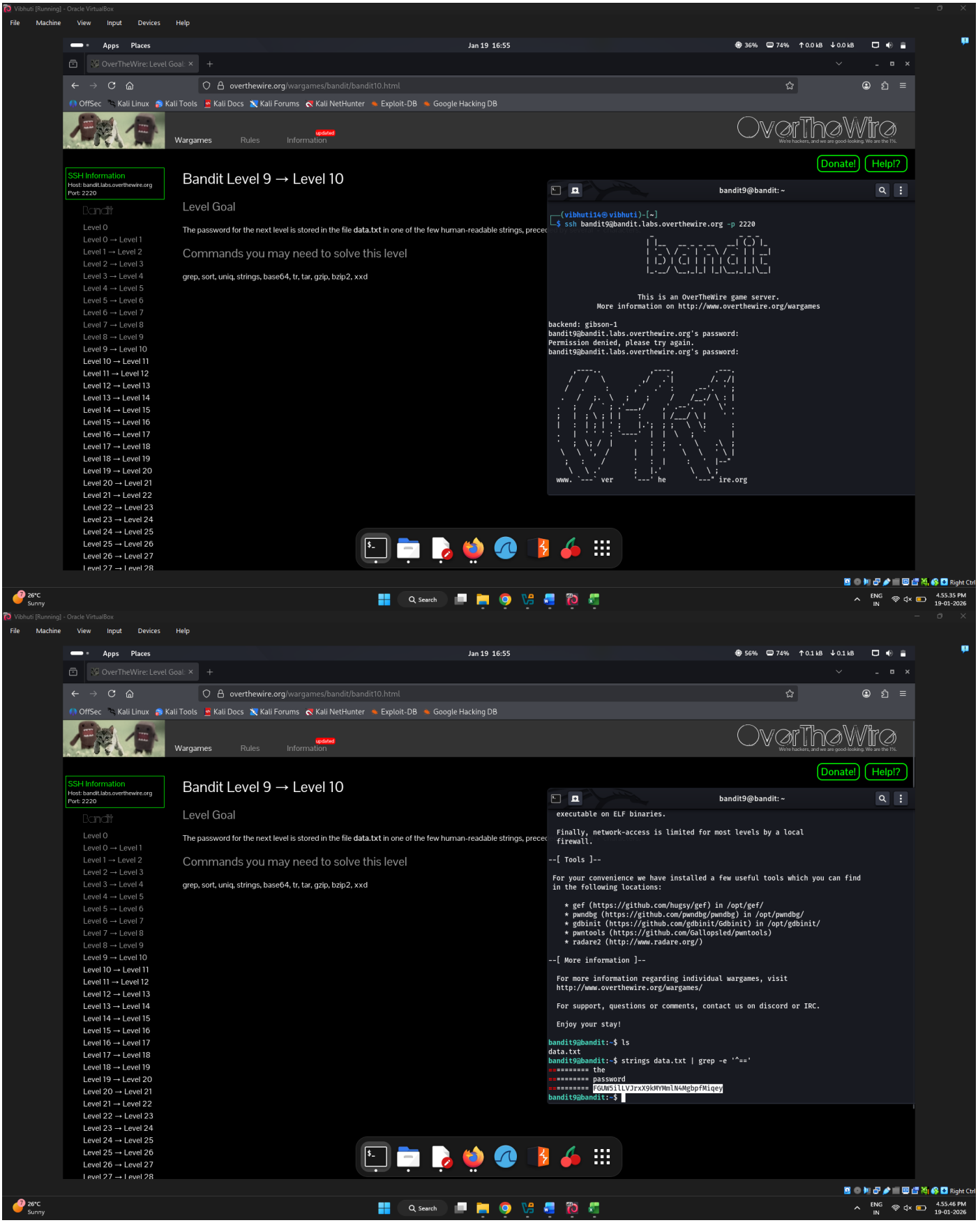
Objective: Extract password stored in the file data.txt in one of the few human-readable strings, preceded by several '=' characters.

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

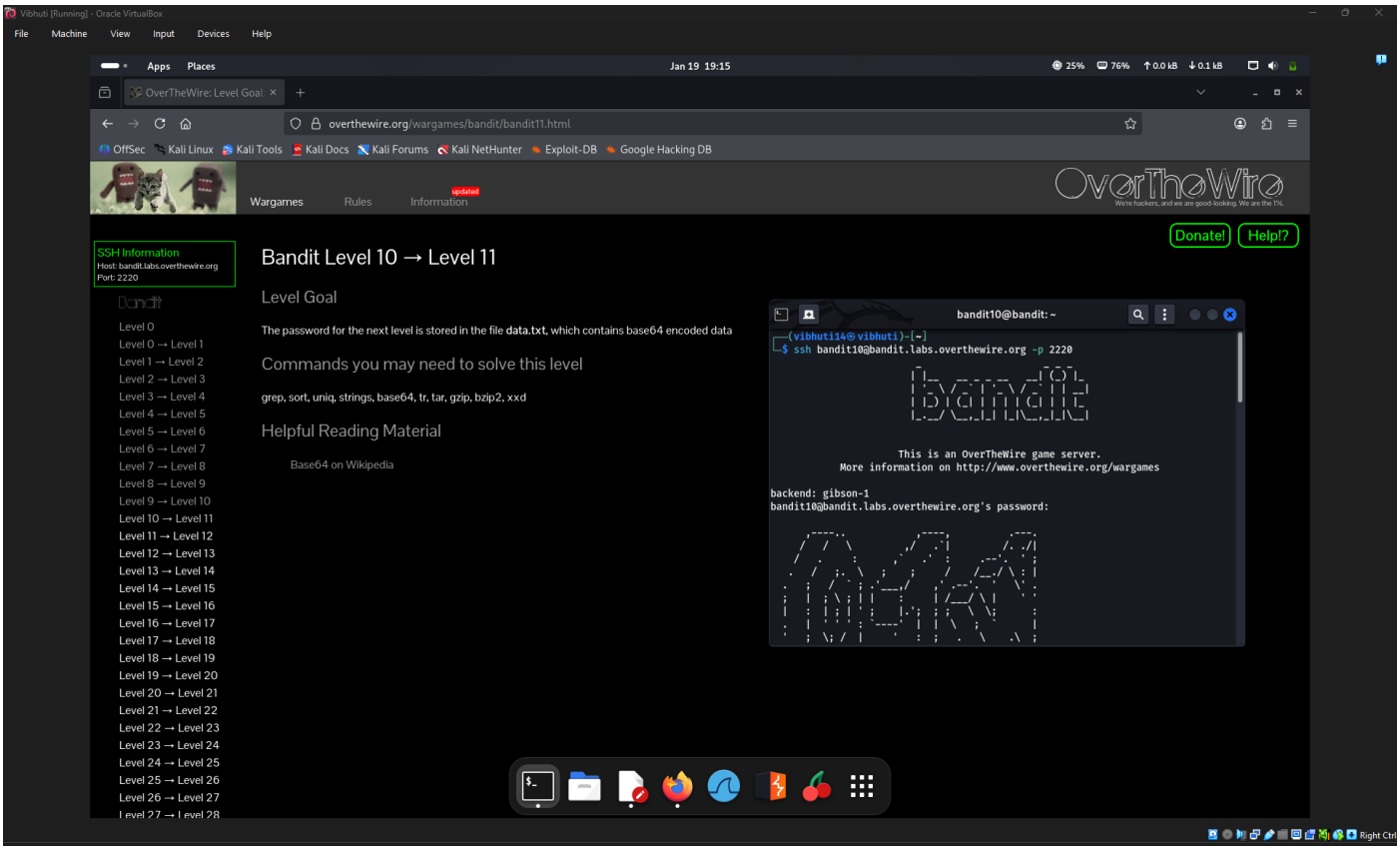
3. Use the strings command to extract human-readable strings from a file. Pipe the result into grep and only output lines that start with at least two = characters. These two commands put together look like this:
   strings data.txt | grep -e '^=='

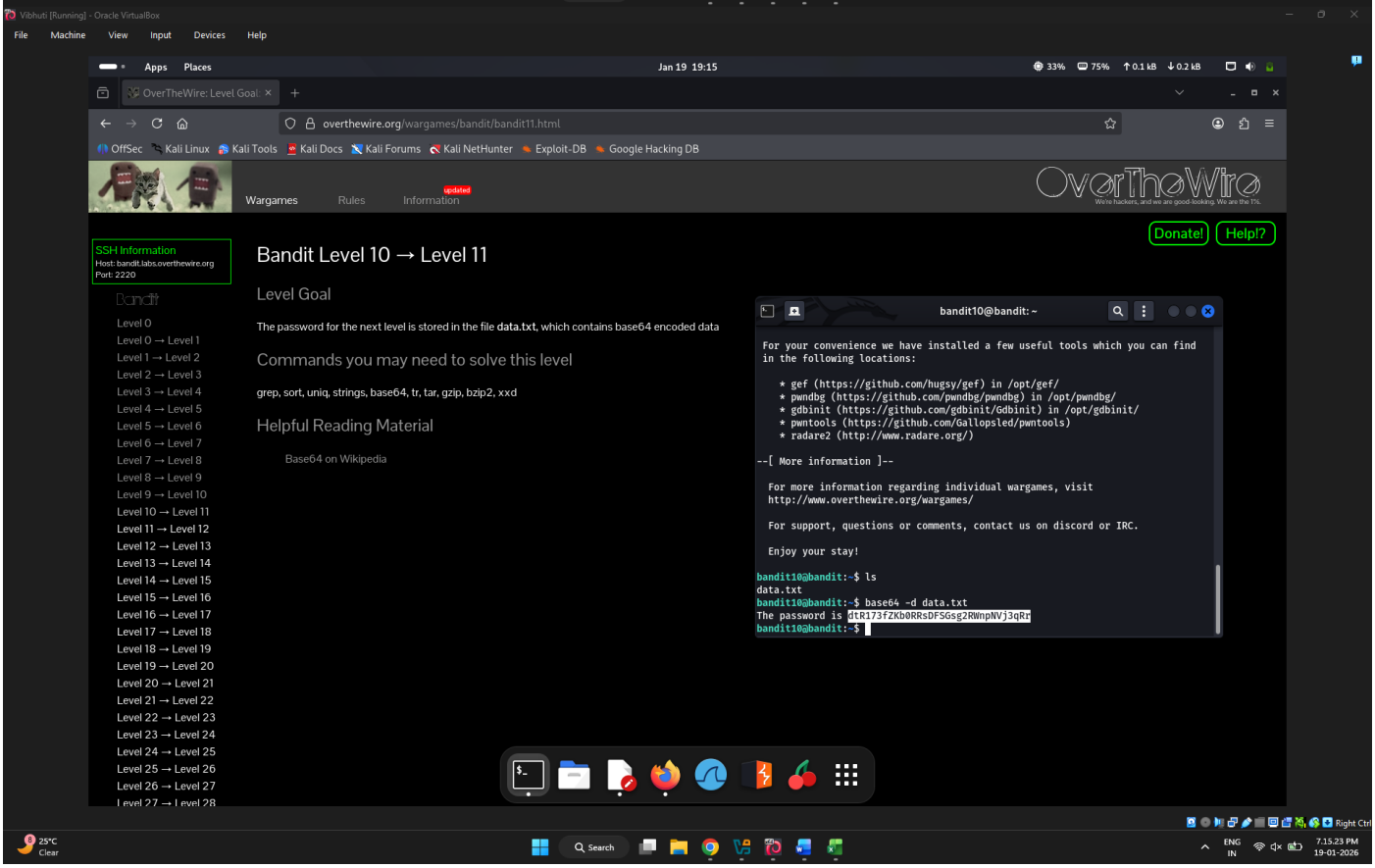


Level 10 -> Level 11

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





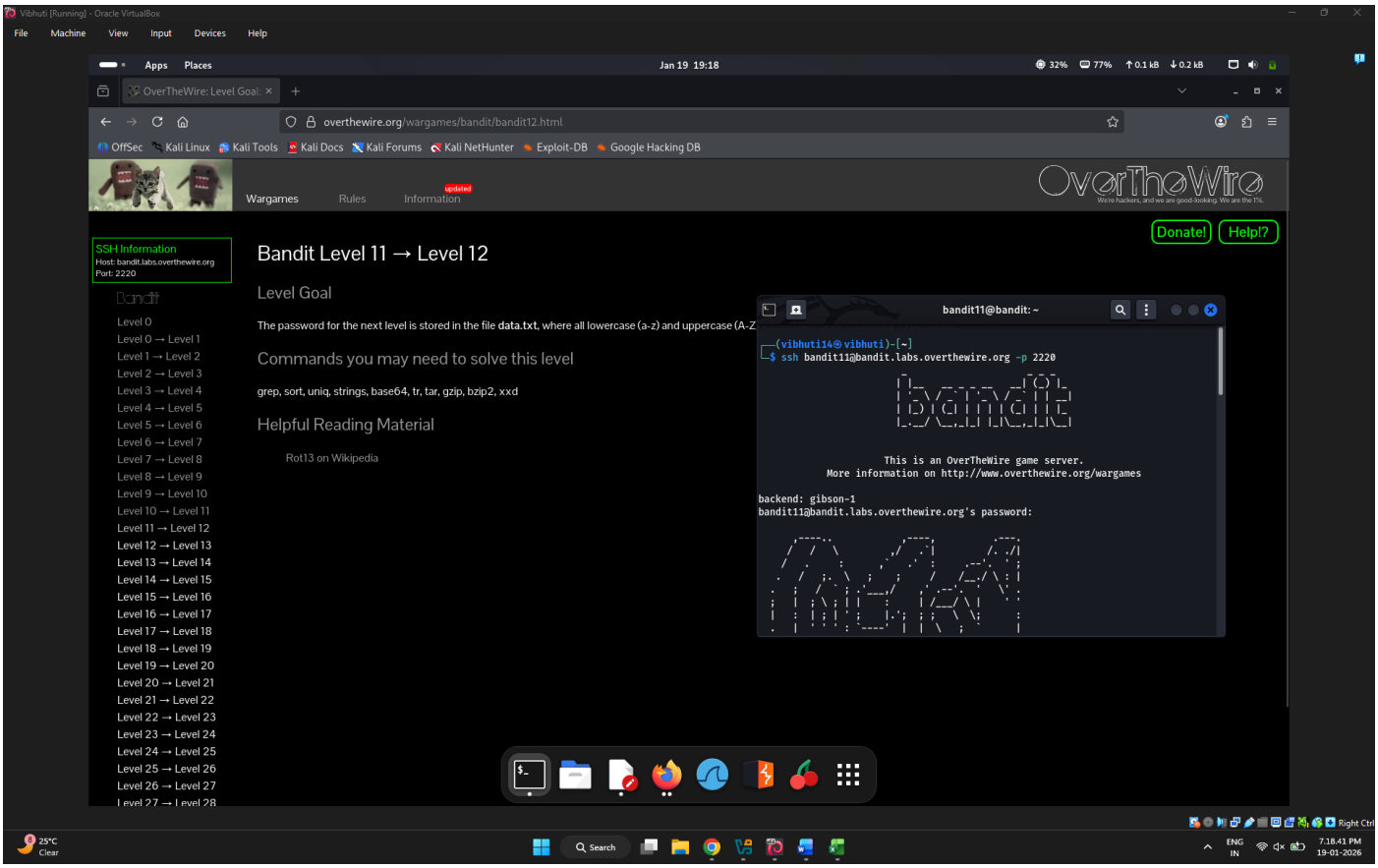
Level 11 -> Level 12

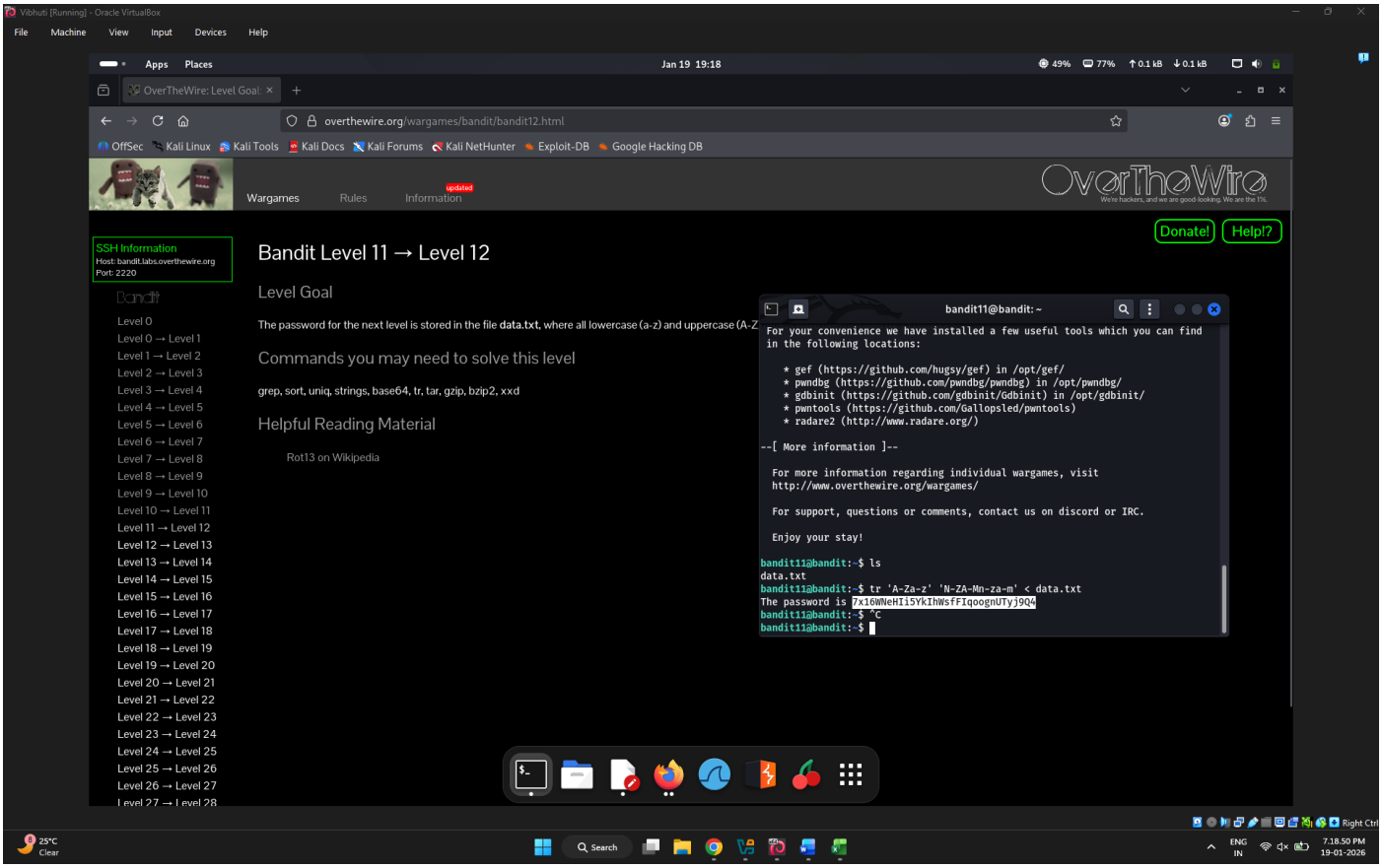
Tools Used: ls, tr

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

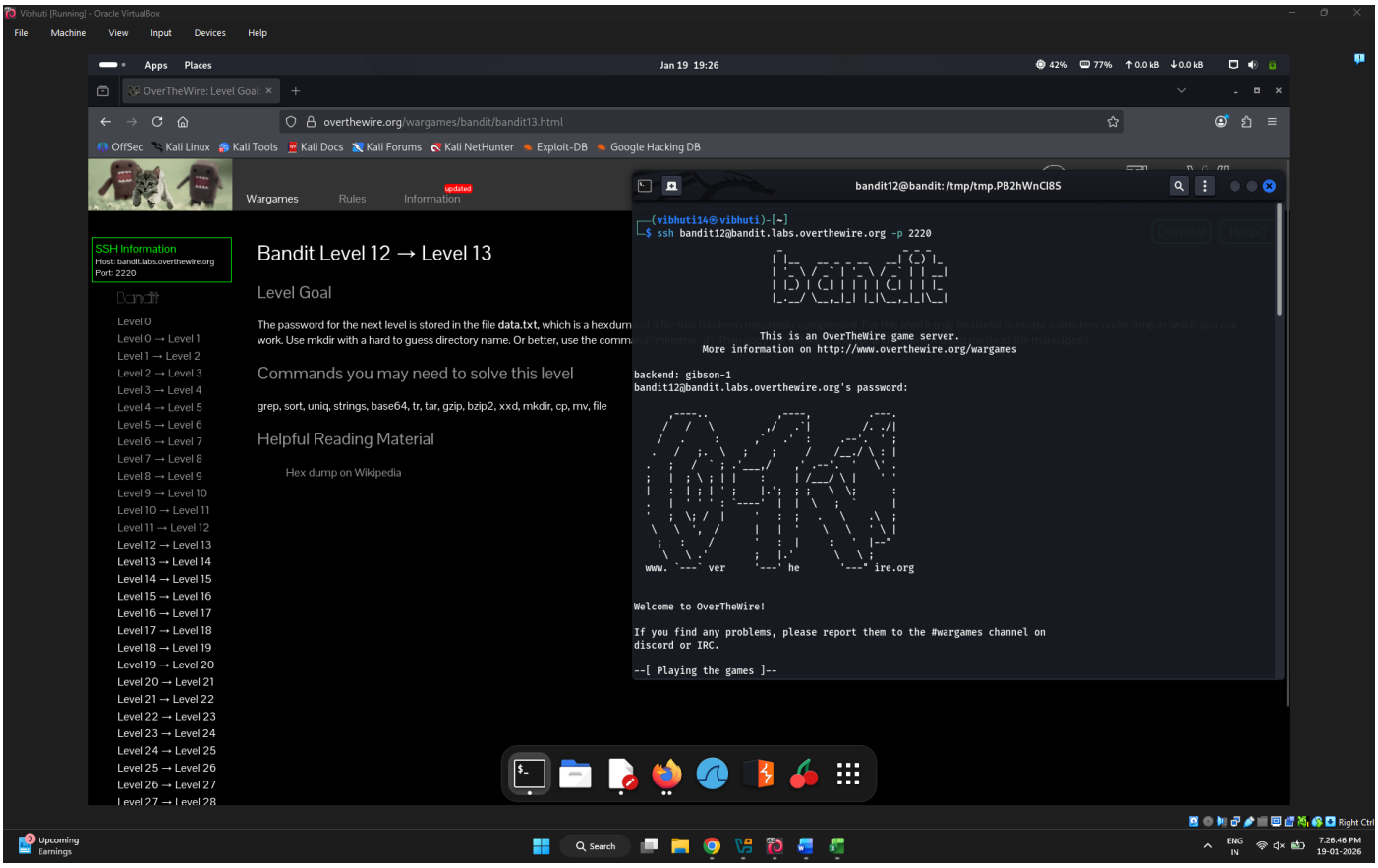
Objective: Extract the password that is stored in the file data.txt, which is a hexdump of a file that has been repeatedly compressed

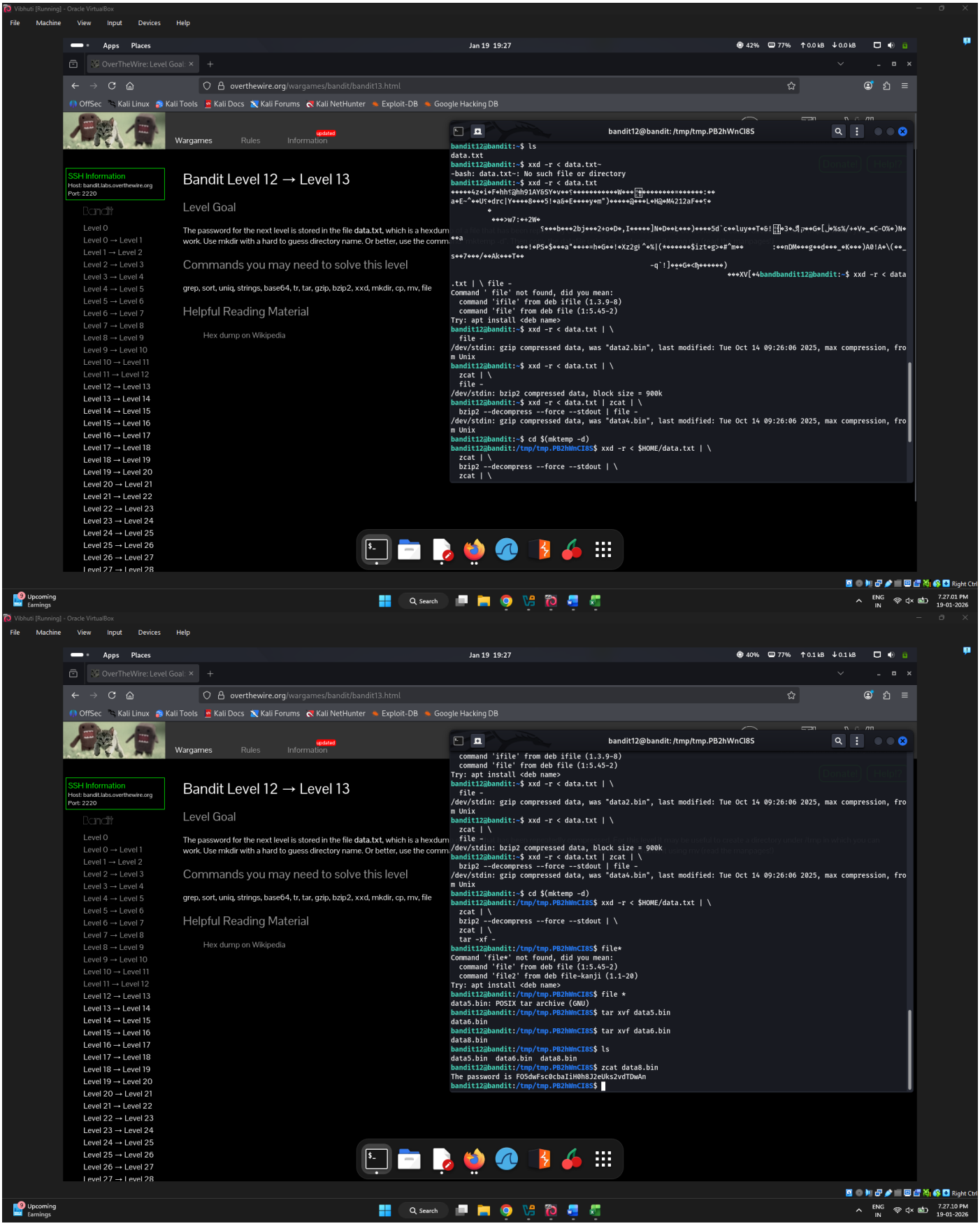
Steps Followed:

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
    ```





Level 13 -> Level 14

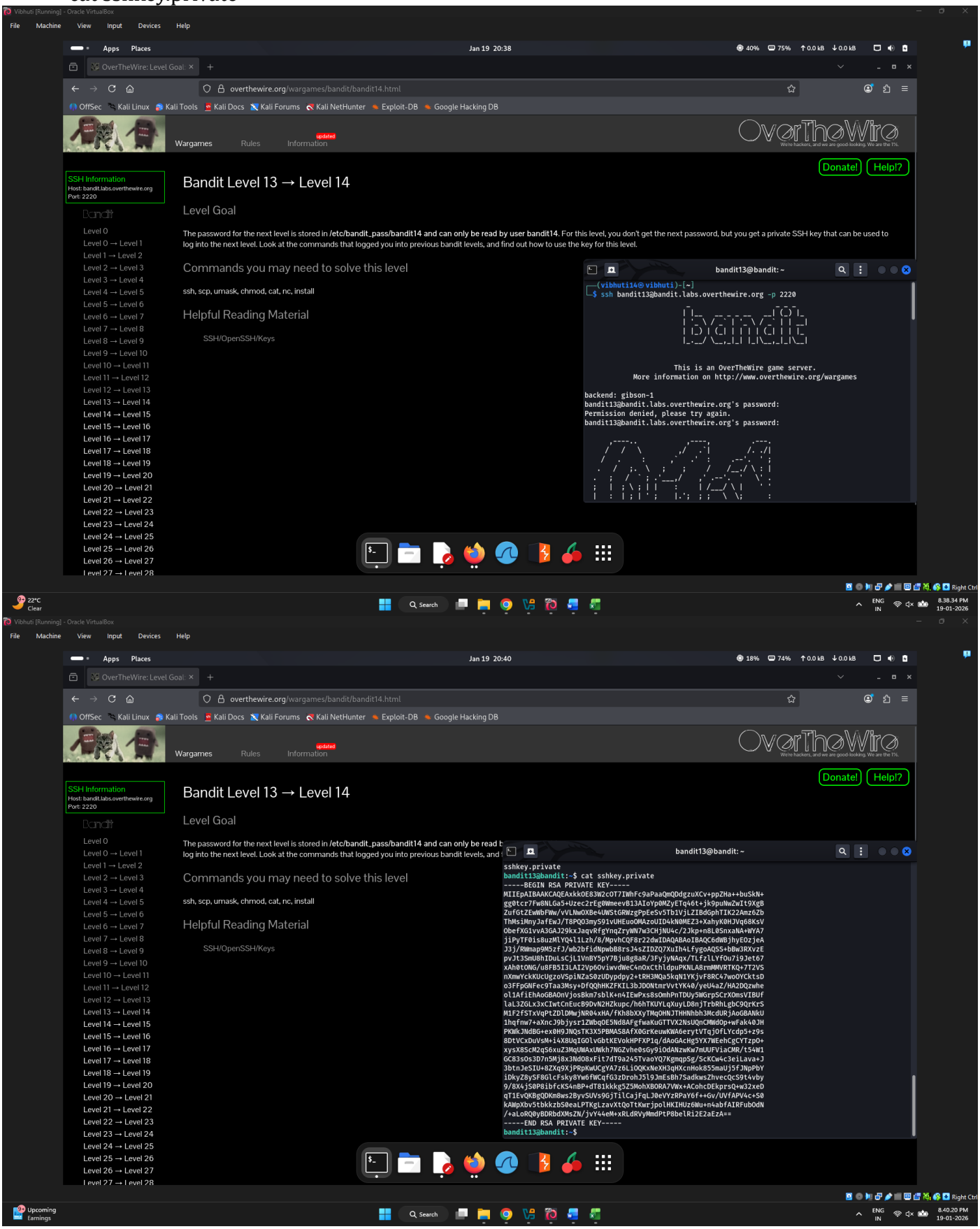
Tools Used: ls, cat

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

Steps Followed:

1. Open terminal
2. Connect with ssh by using the following command and enter password (retrieved from readme):
   ssh bandit13@bandit.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



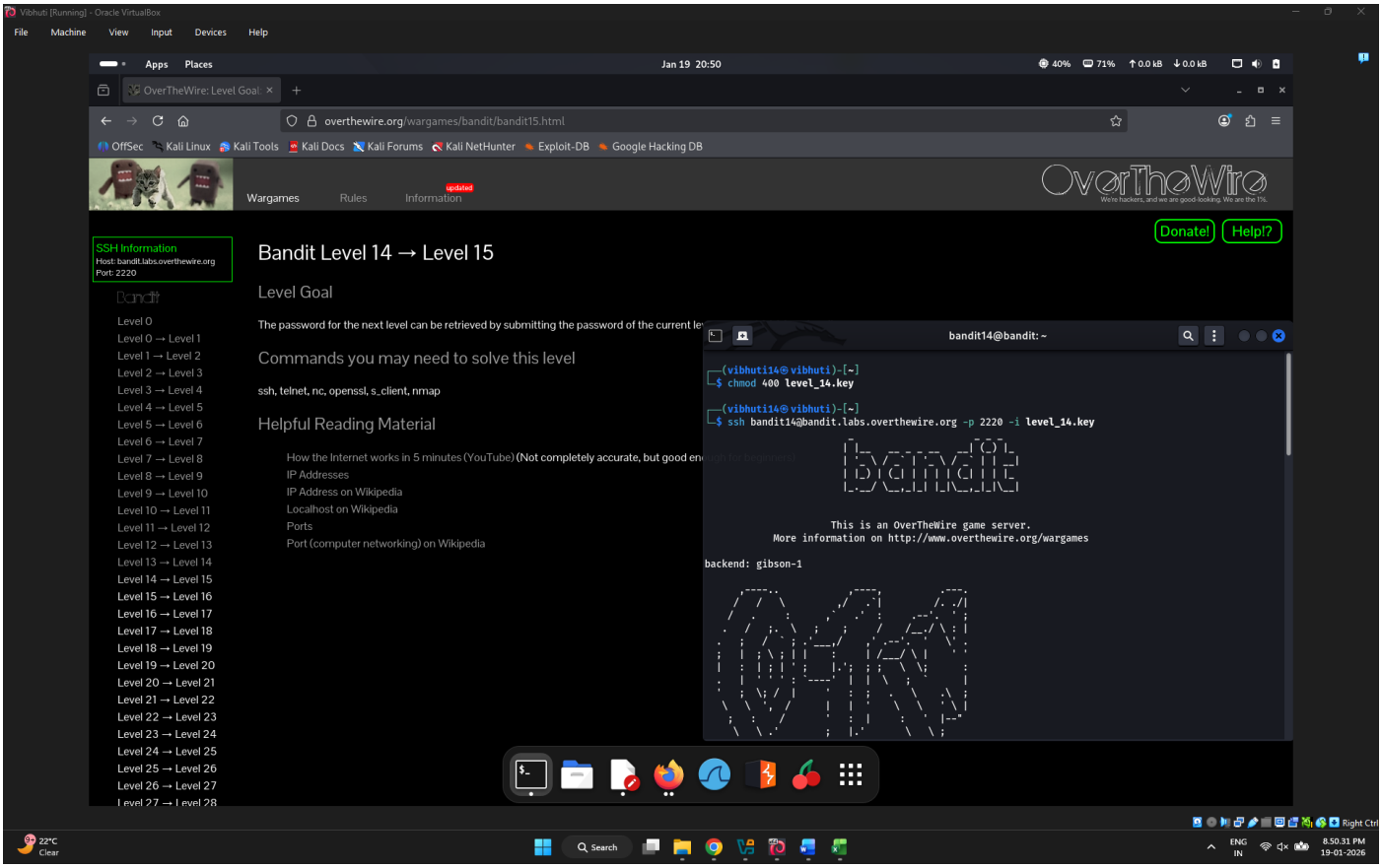
Level 14 -> Level 15

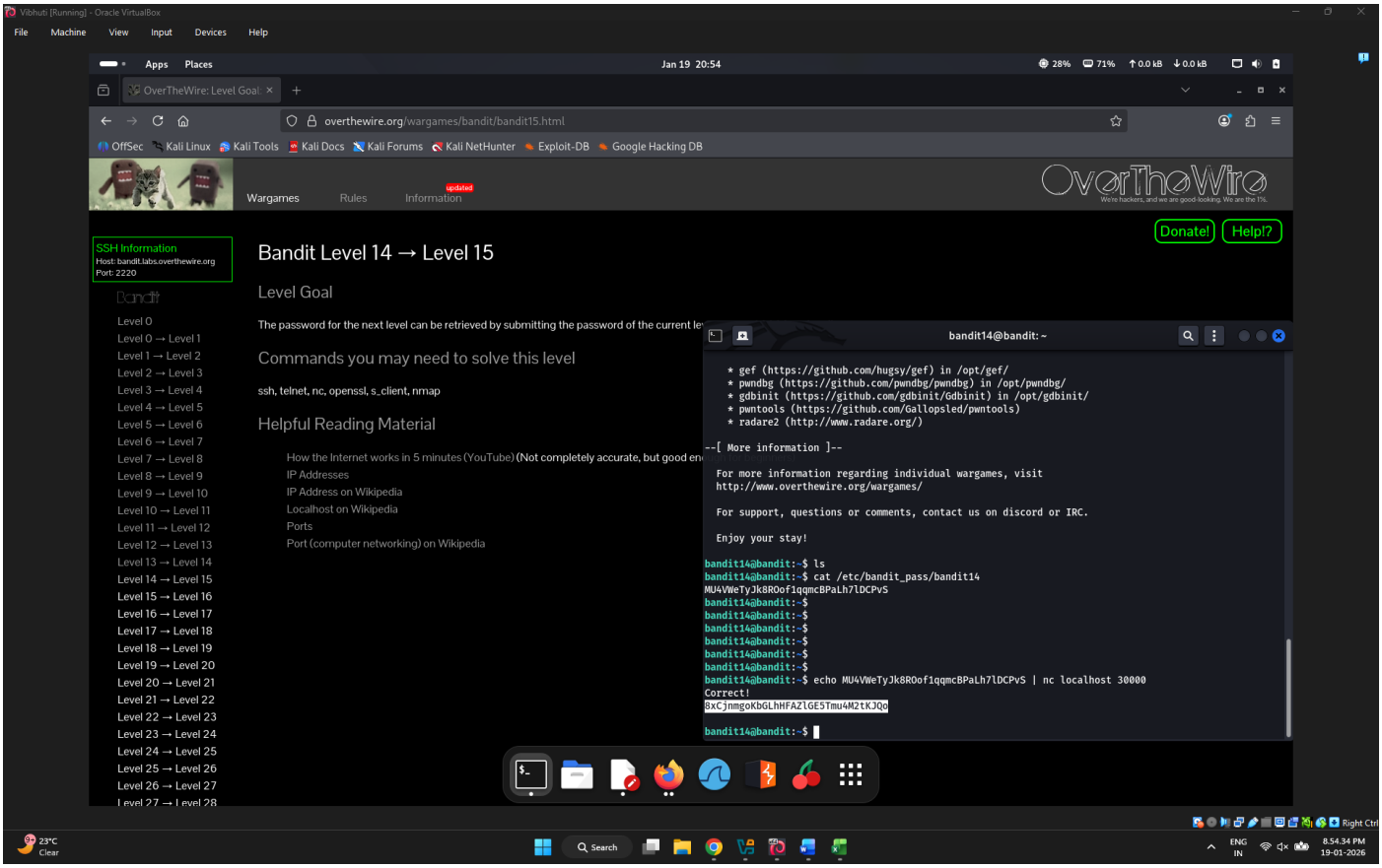
Tools Used: chmod, cat

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





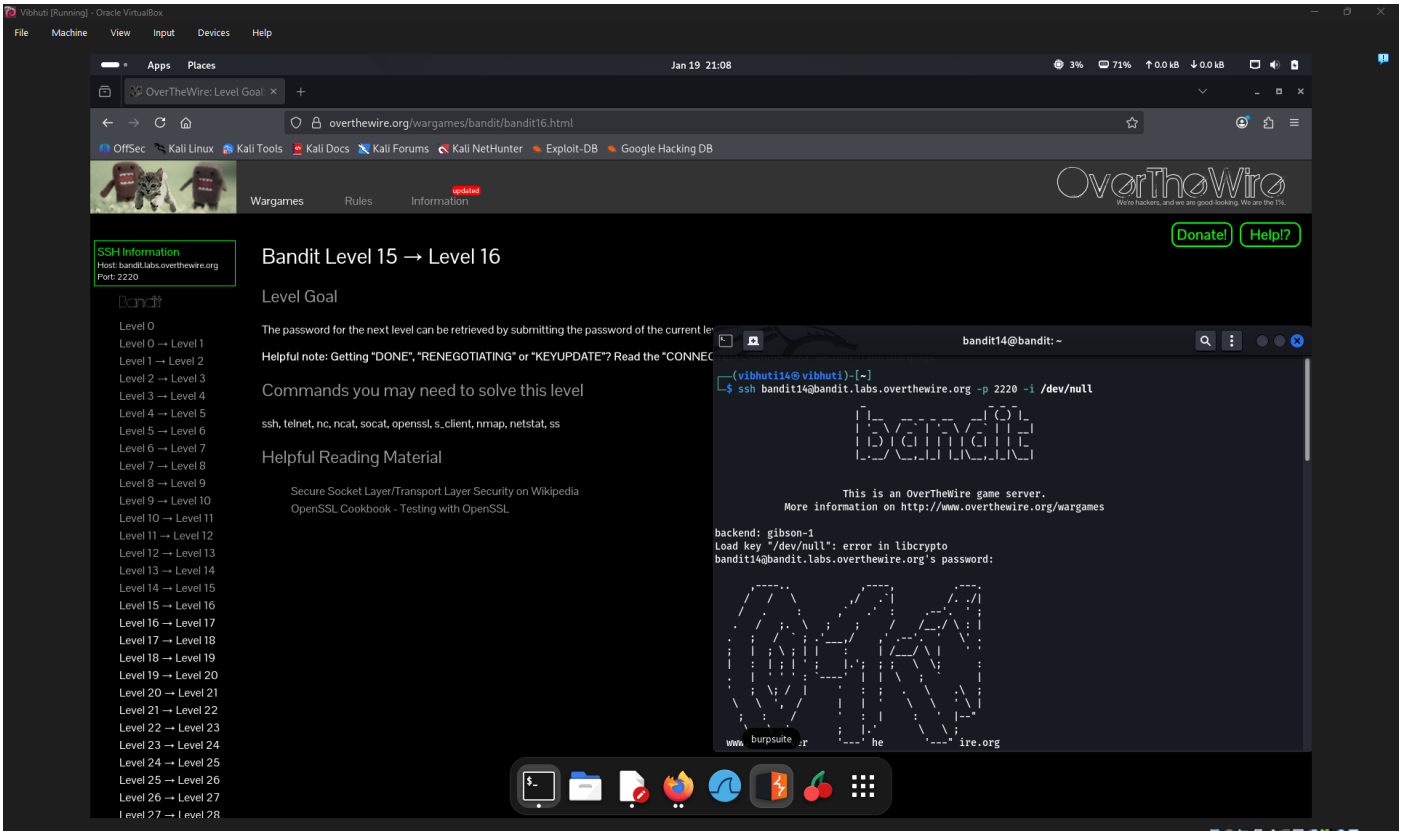
Level 15 -> Level 16

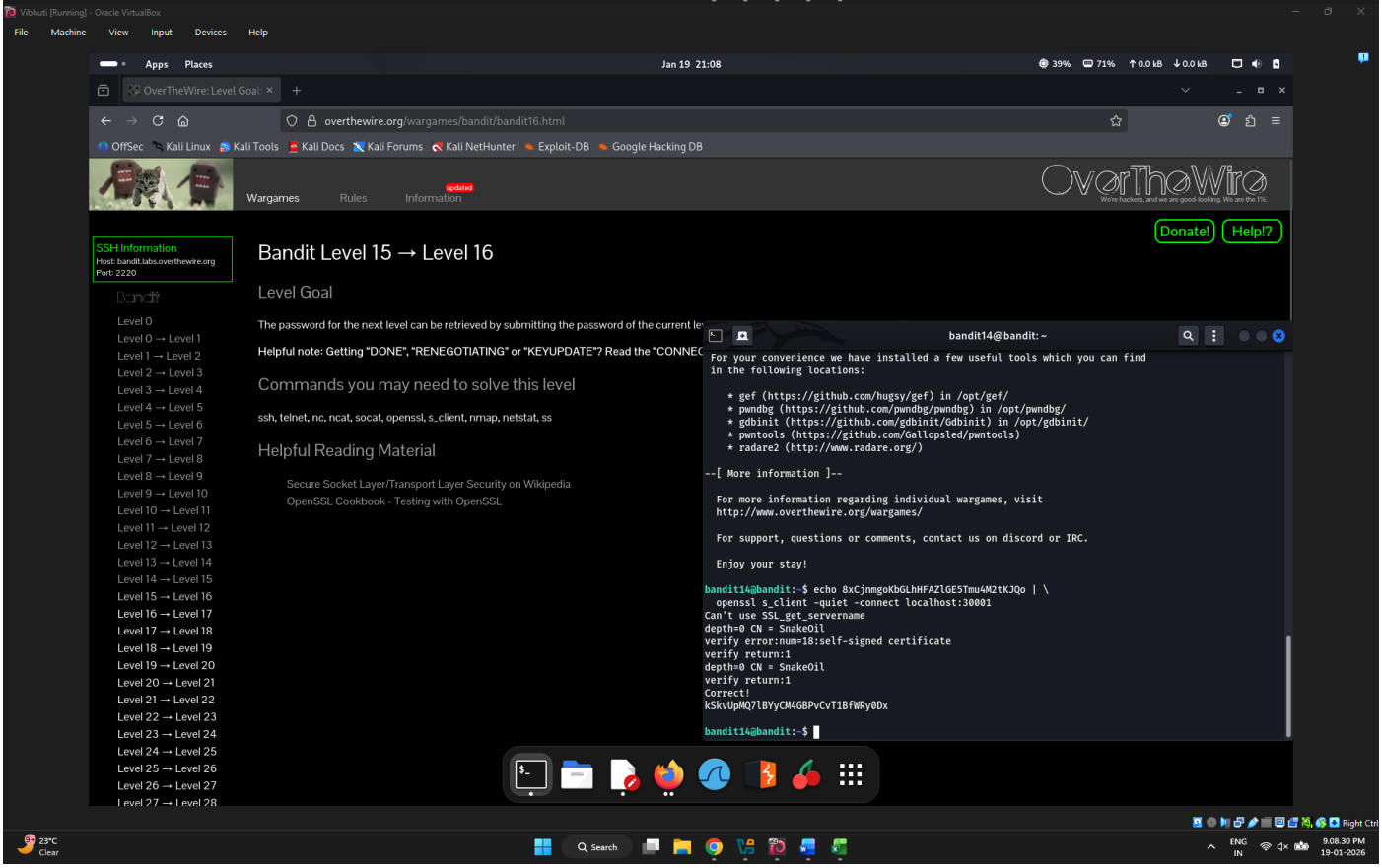
Tools Used: echo

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





Level 16 -> Level 17

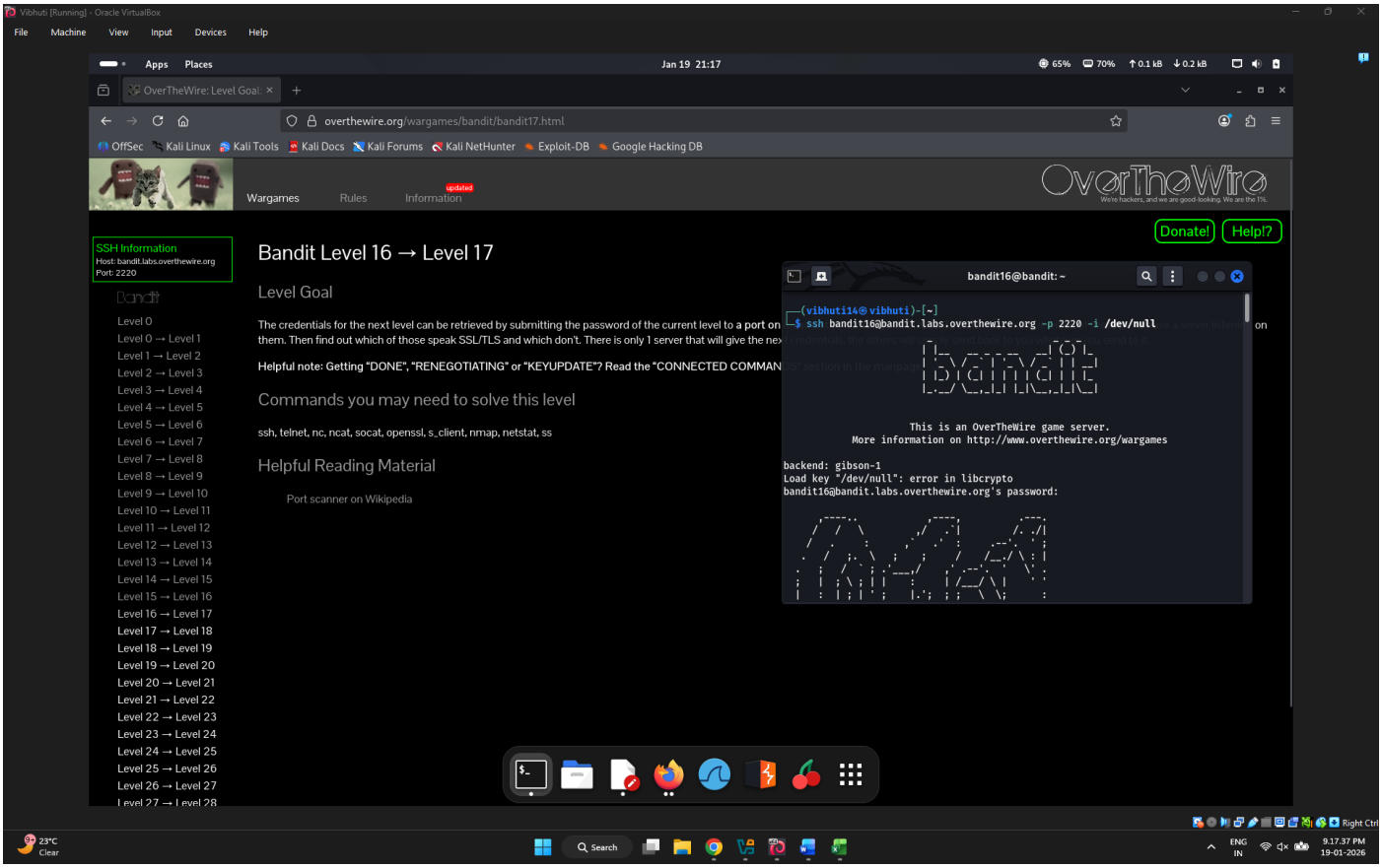
Tools Used: echo, openssl

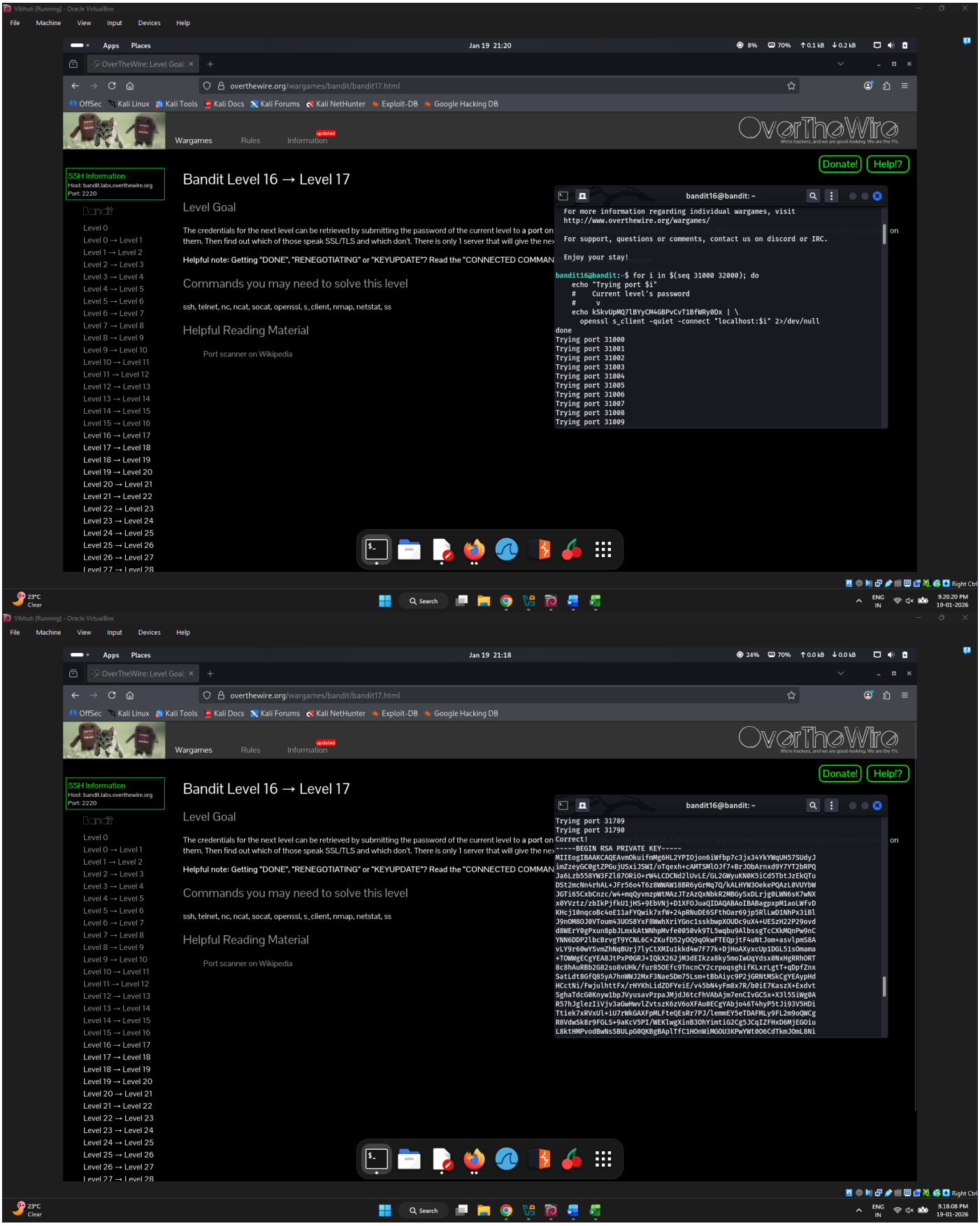
Objective: Extract credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000

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





Level 17 -> Level 18

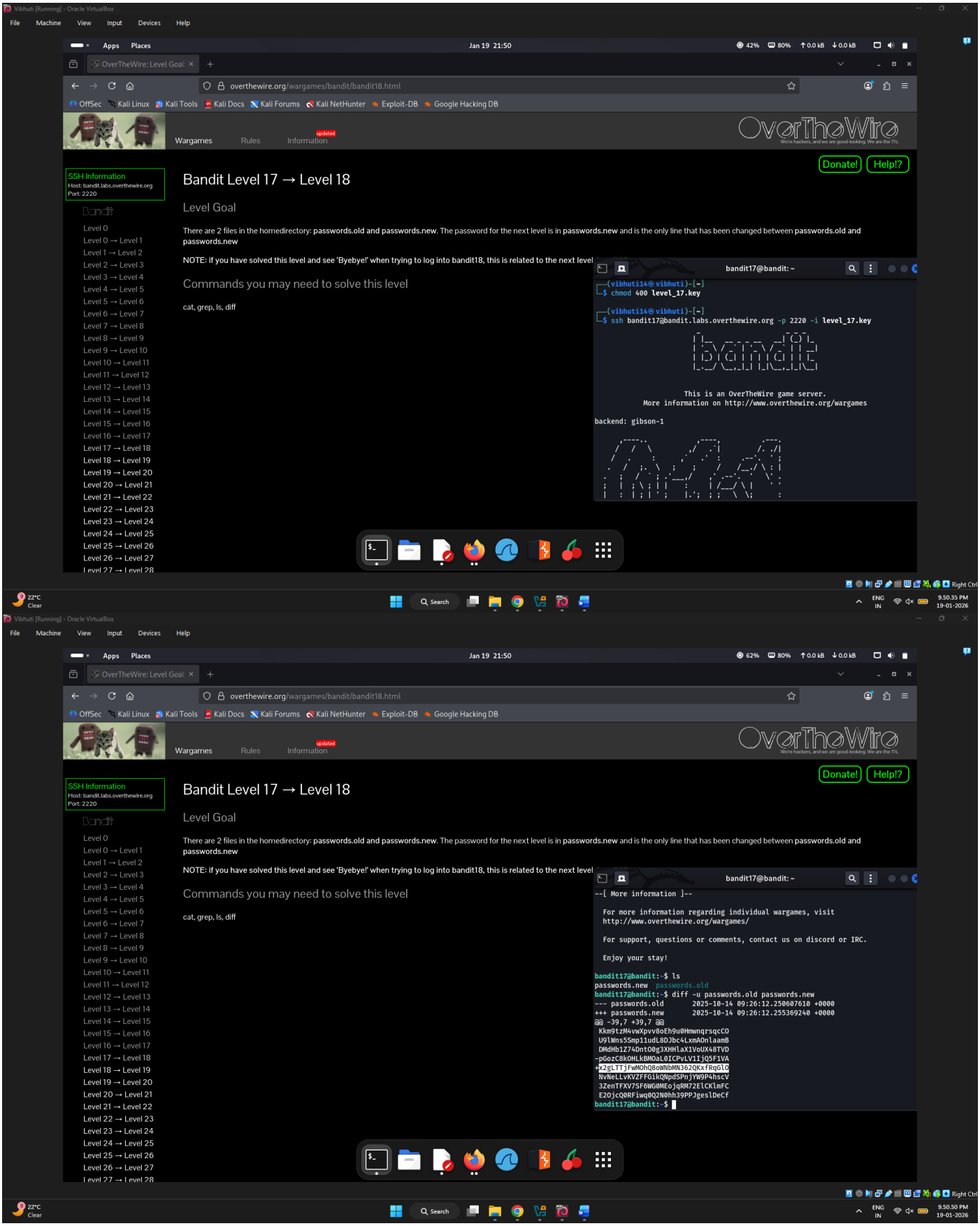
Tools Used: chmod, diff

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



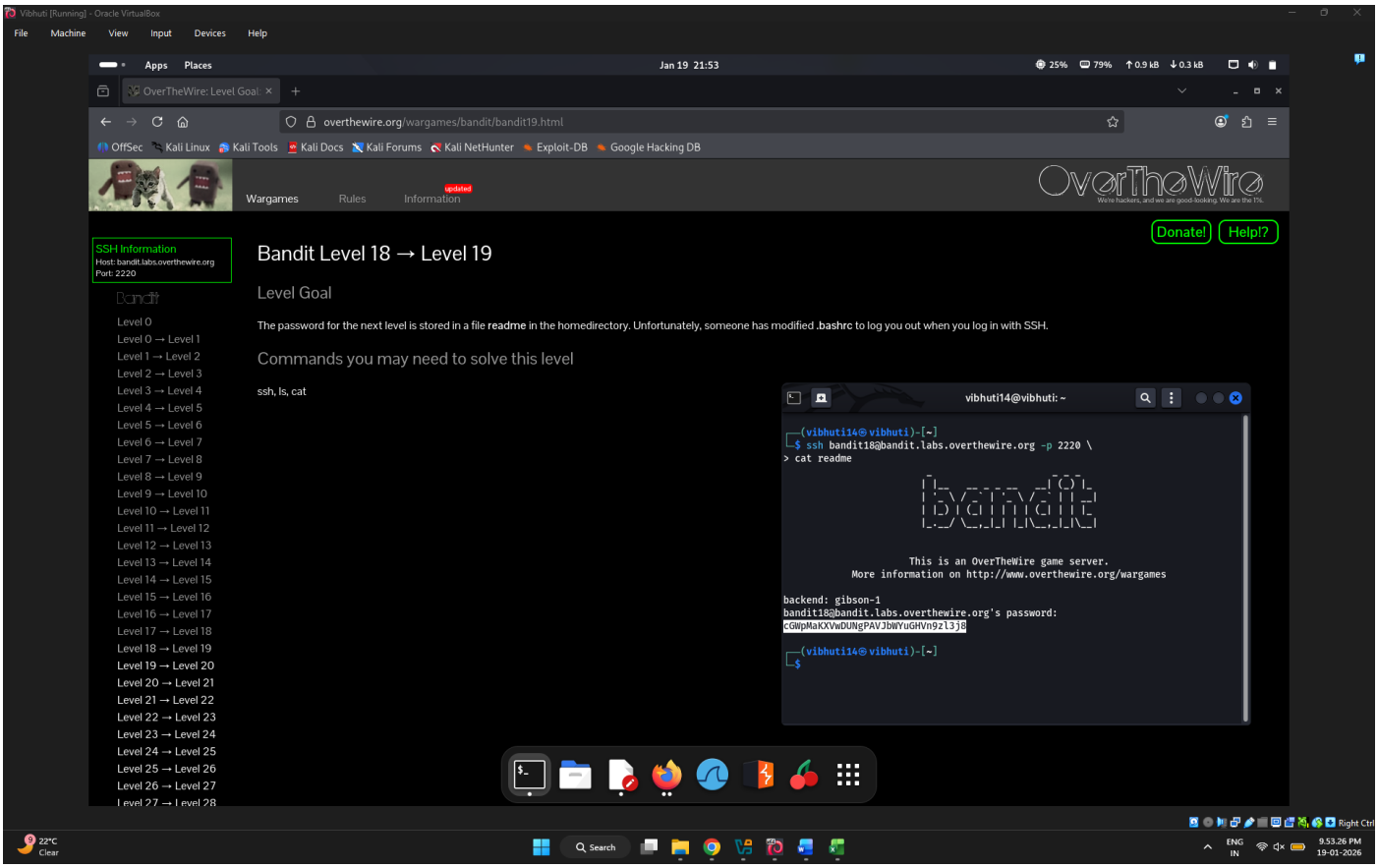
Level 18 -> Level 19

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



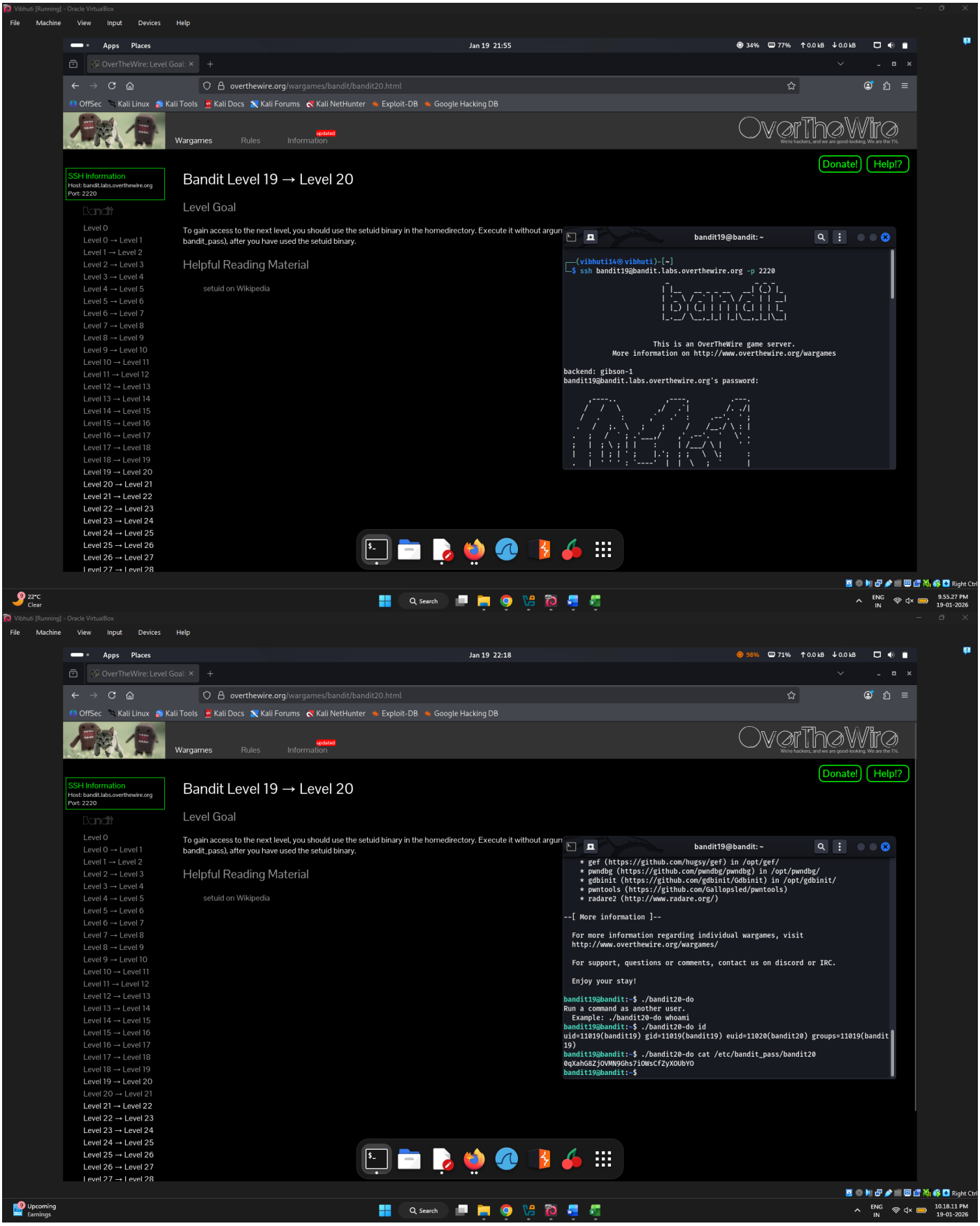
Level 19 -> Level 20

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



Level 20 -> Level 21

Tools Used: nc, fg

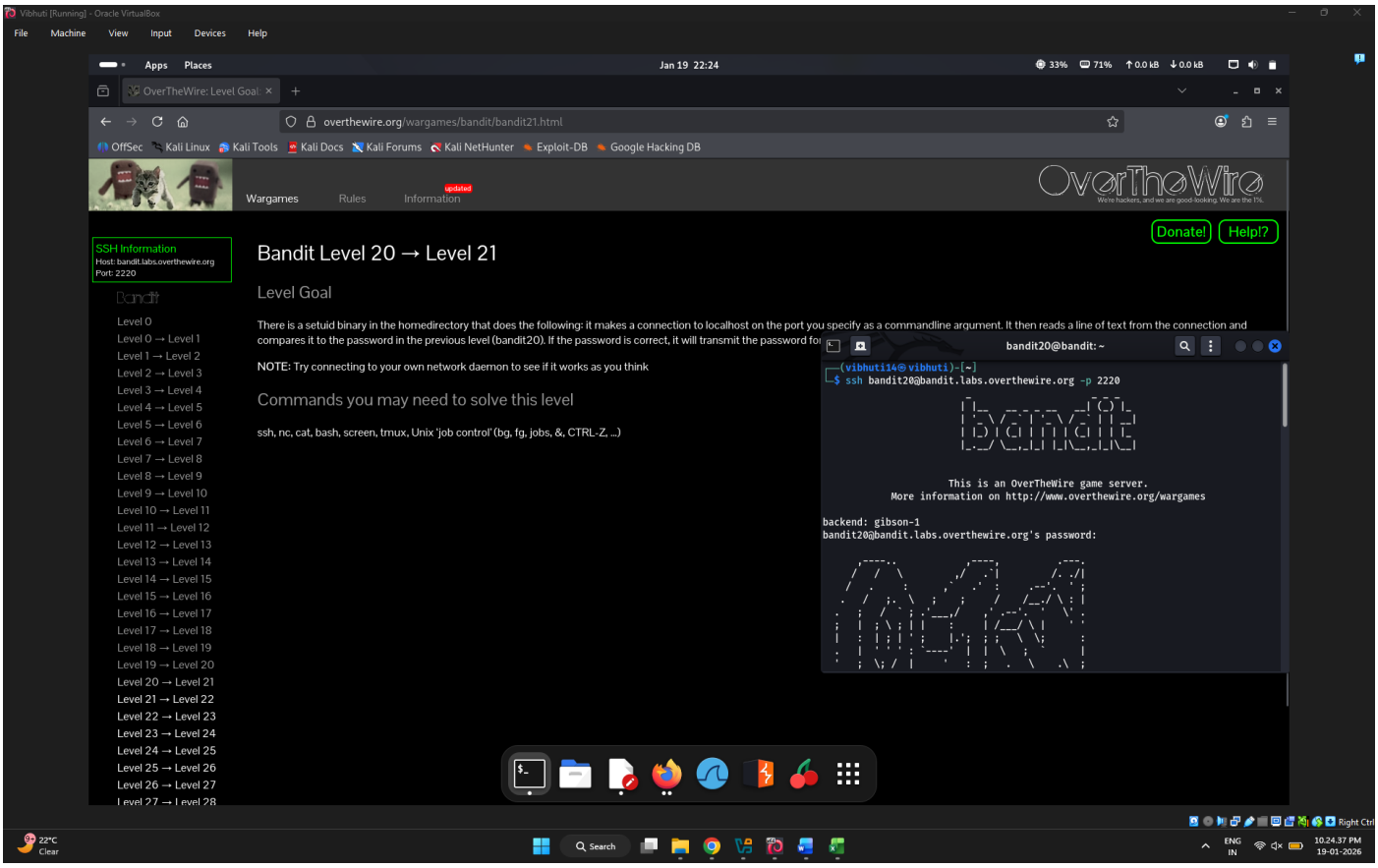
Objective: To send your password to a specific port using a setuid binary.

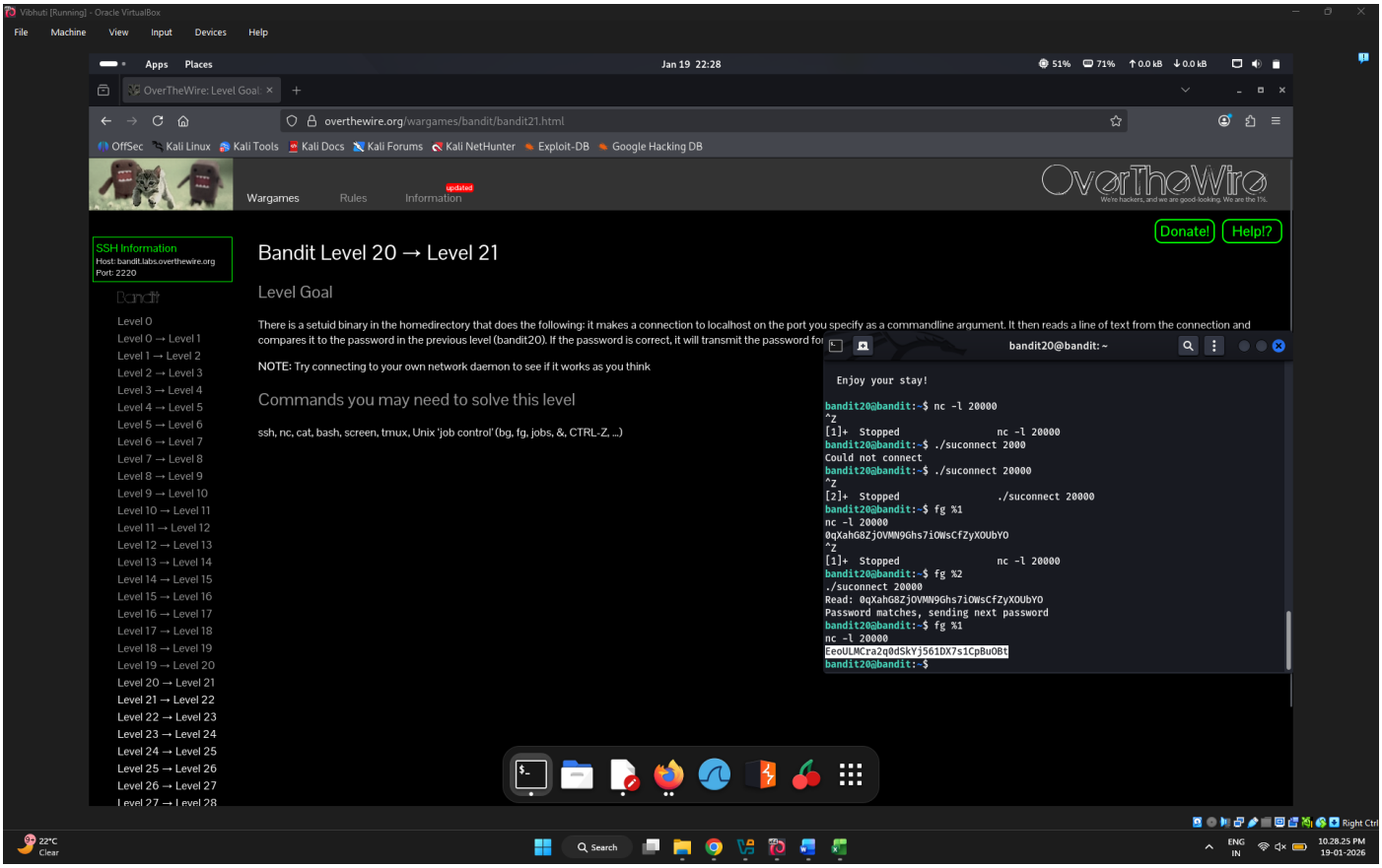
Steps Followed:

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





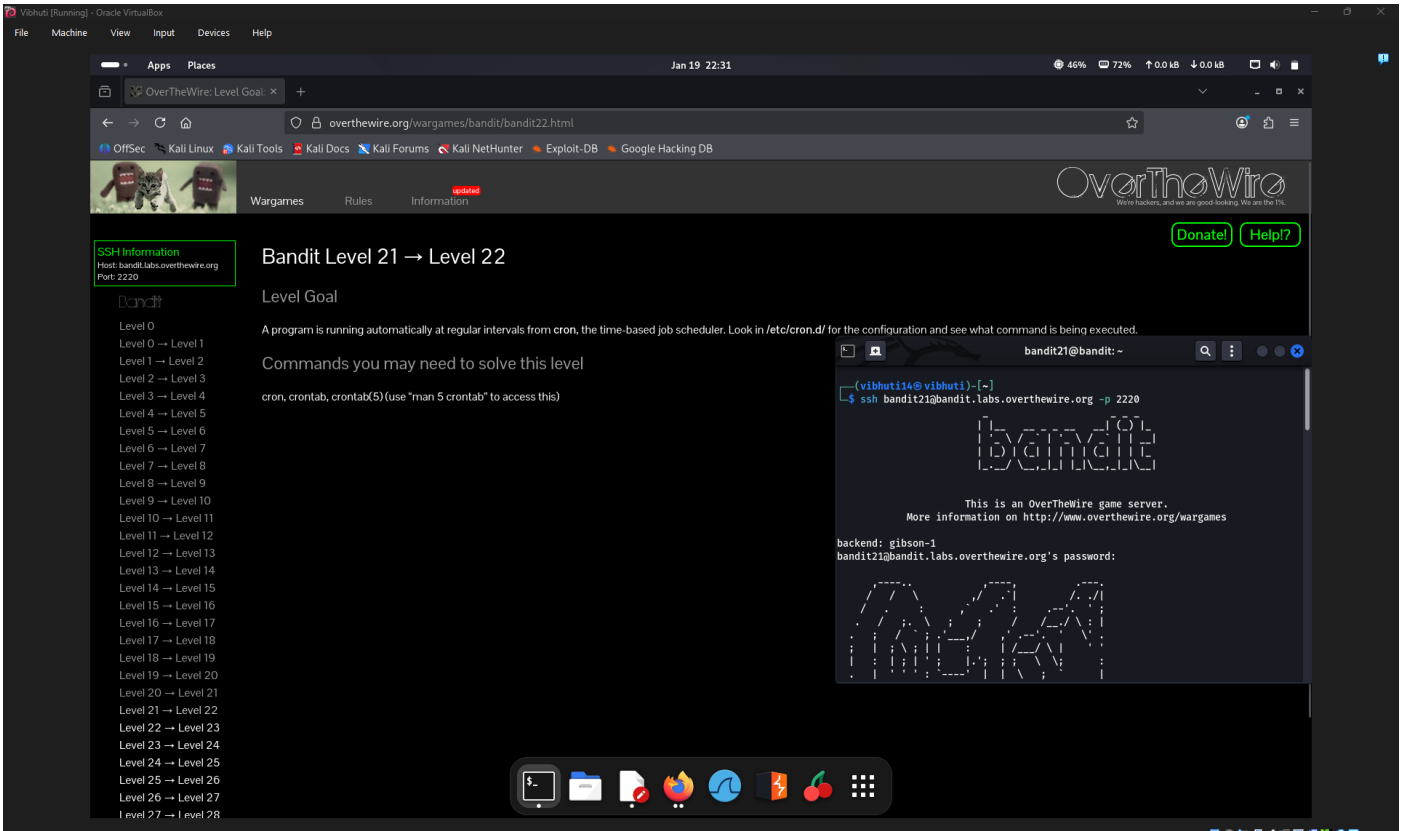
Level 21 -> Level 22

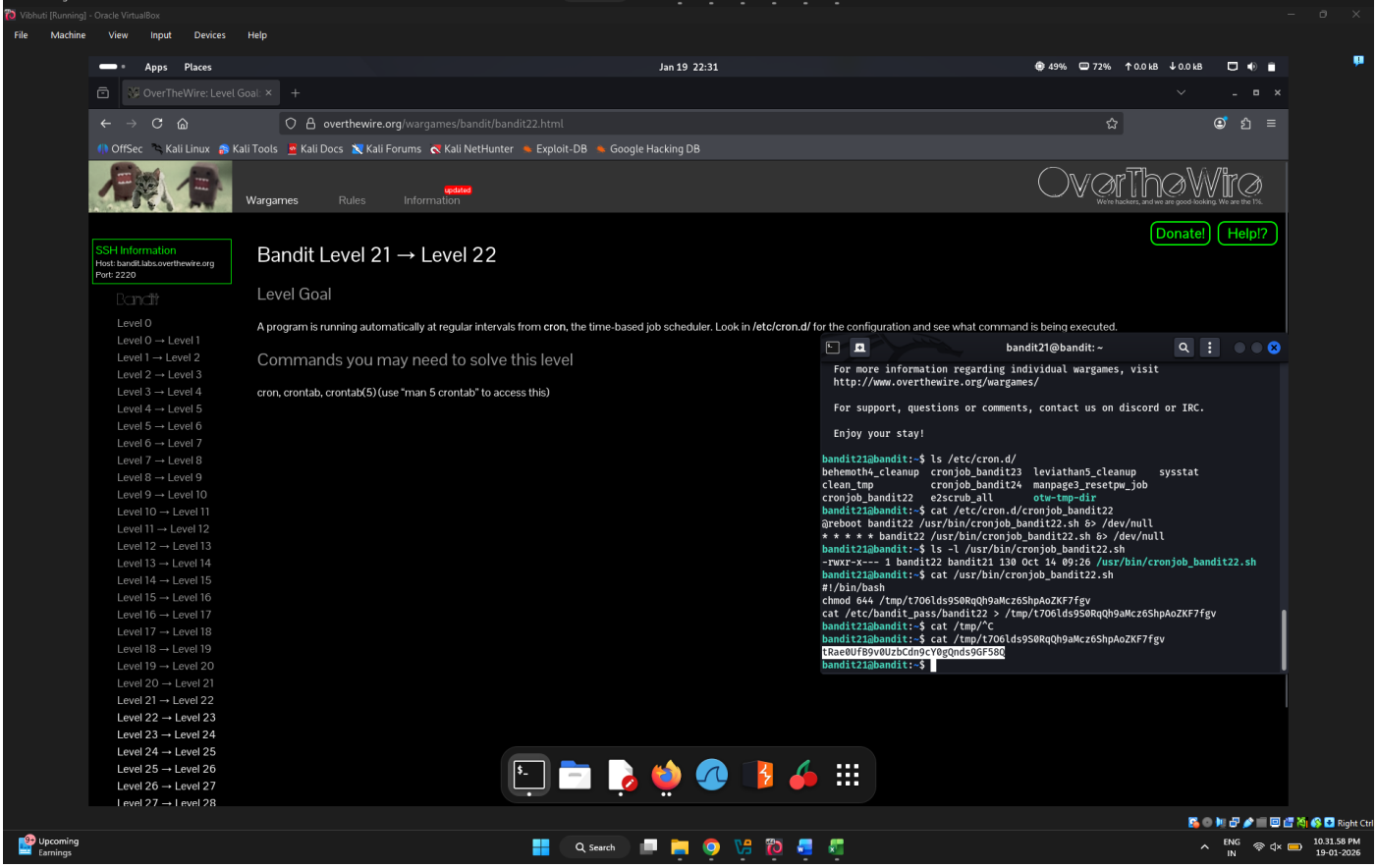
Tools Used: ls, cat

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





Level 22 -> Level 23

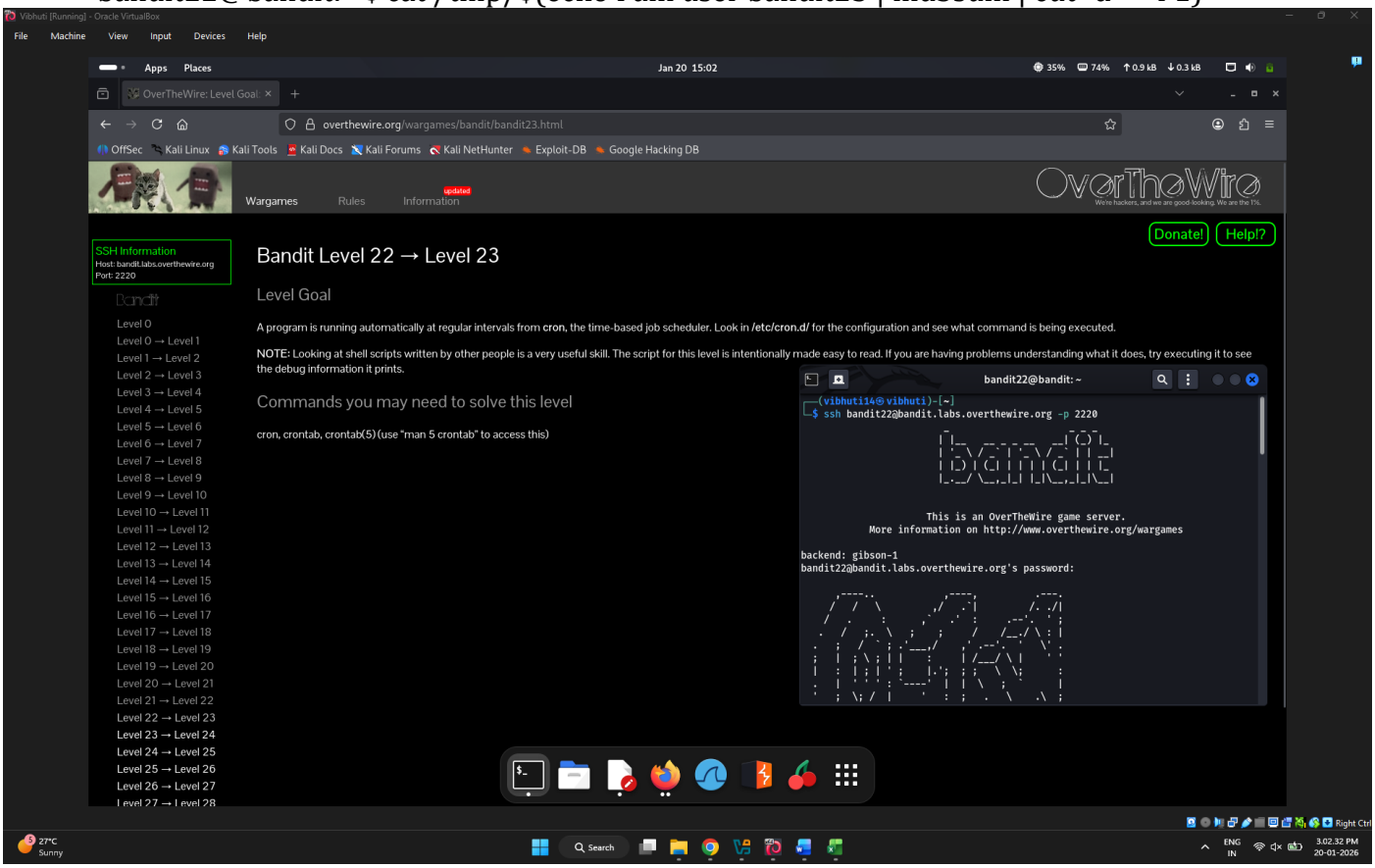
Tools Used: ls, cat, ech

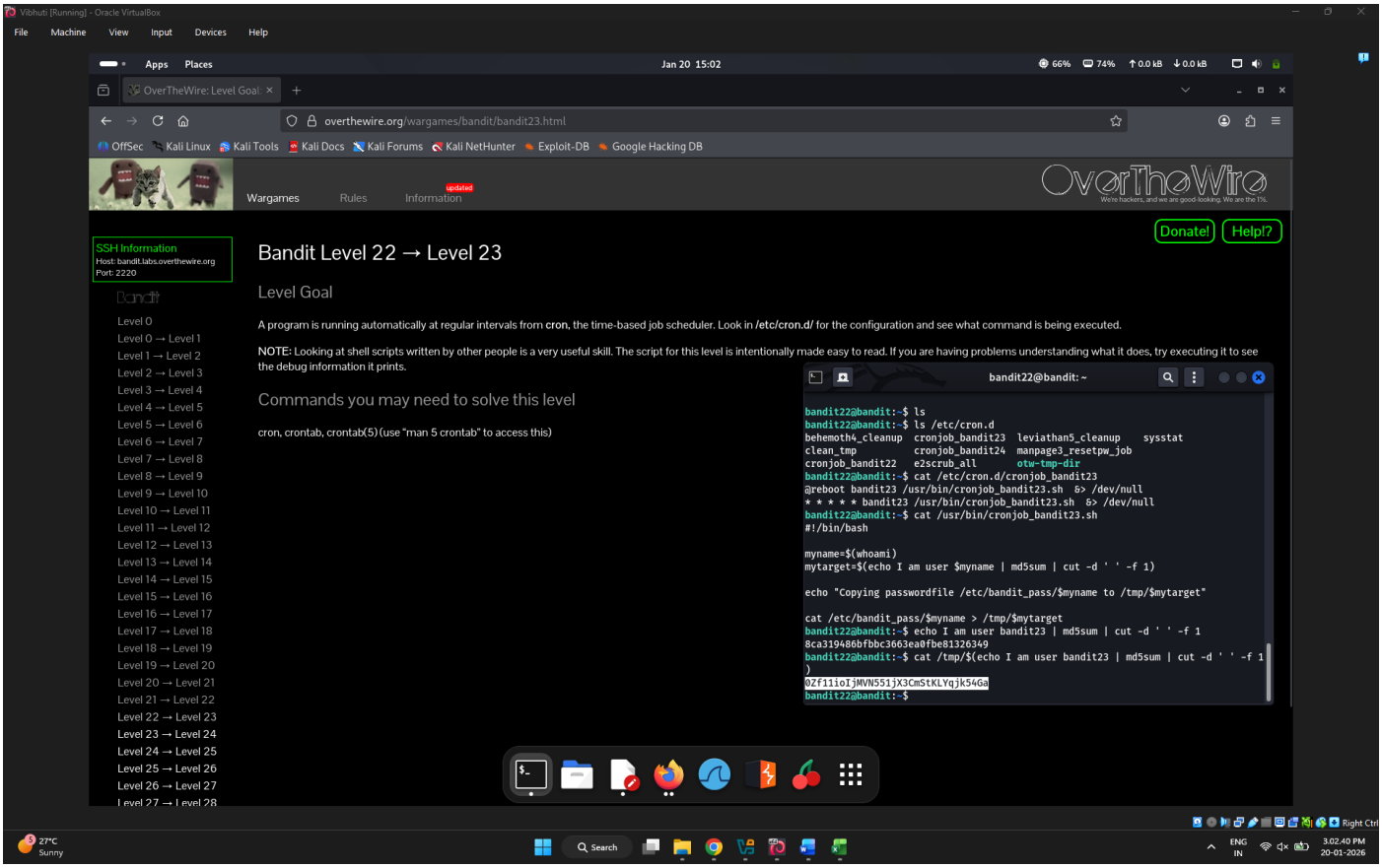
Objective: Extract password from filenames that invoke cron job.

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)





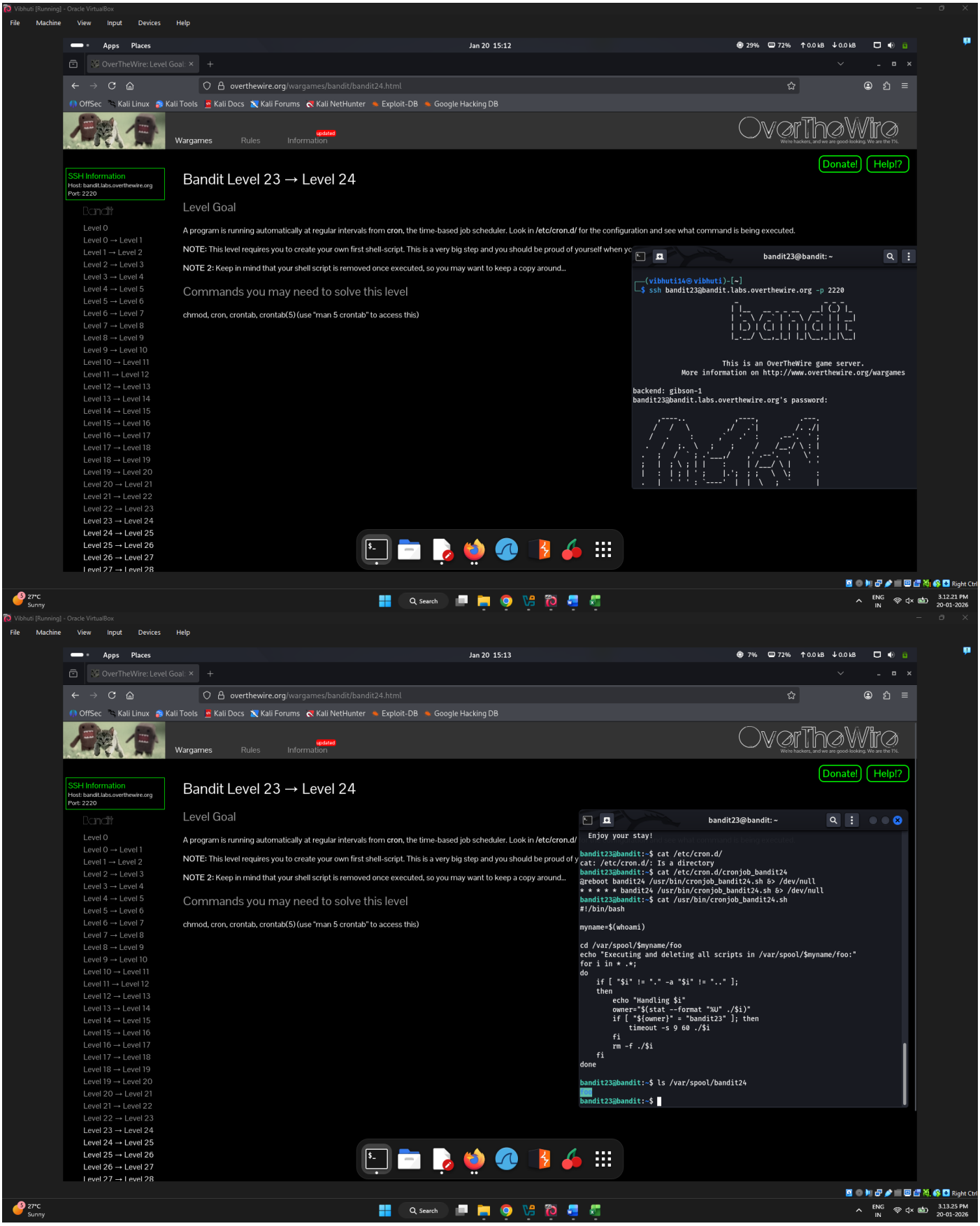
Level 23 -> Level 24

Tools Used: cat, chmod, ls

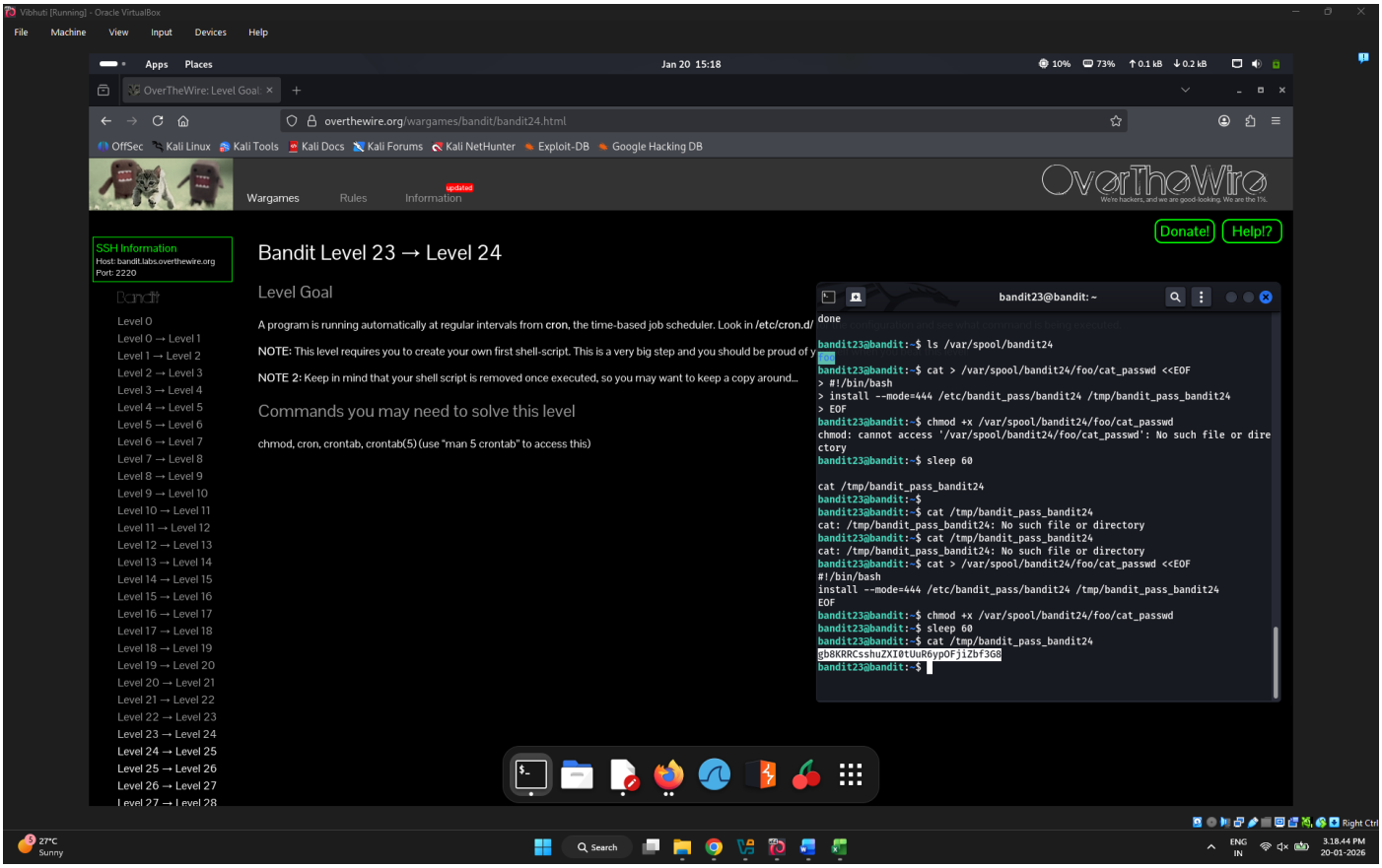
Objective: Trick a cron job into executing script instead.

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 Jan 20 15:12
OverTheWire: Level Goal
overthewire.org/wargames/bandit/bandit24.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Wargames Rules Information
OverTheWire
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
Level 27 → 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 yc
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)
bandit23@bandit: ~
(vibhuti14㉿vibhuti)-[~]
$ ssh bandit23@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
bandit23@bandit.labs.overthewire.org's password:
Right Ctrl
27°C Sunny
Search
ENG IN
3.12.21 PM 20-01-2026

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Jan 20 15:13
OverTheWire: Level Goal
overthewire.org/wargames/bandit/bandit24.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Wargames Rules Information
OverTheWire
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
Level 27 → 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/
NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of y
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)
bandit23@bandit: ~
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:~$
Right Ctrl
27°C Sunny
Search
ENG IN
3.13.25 PM 20-01-2026



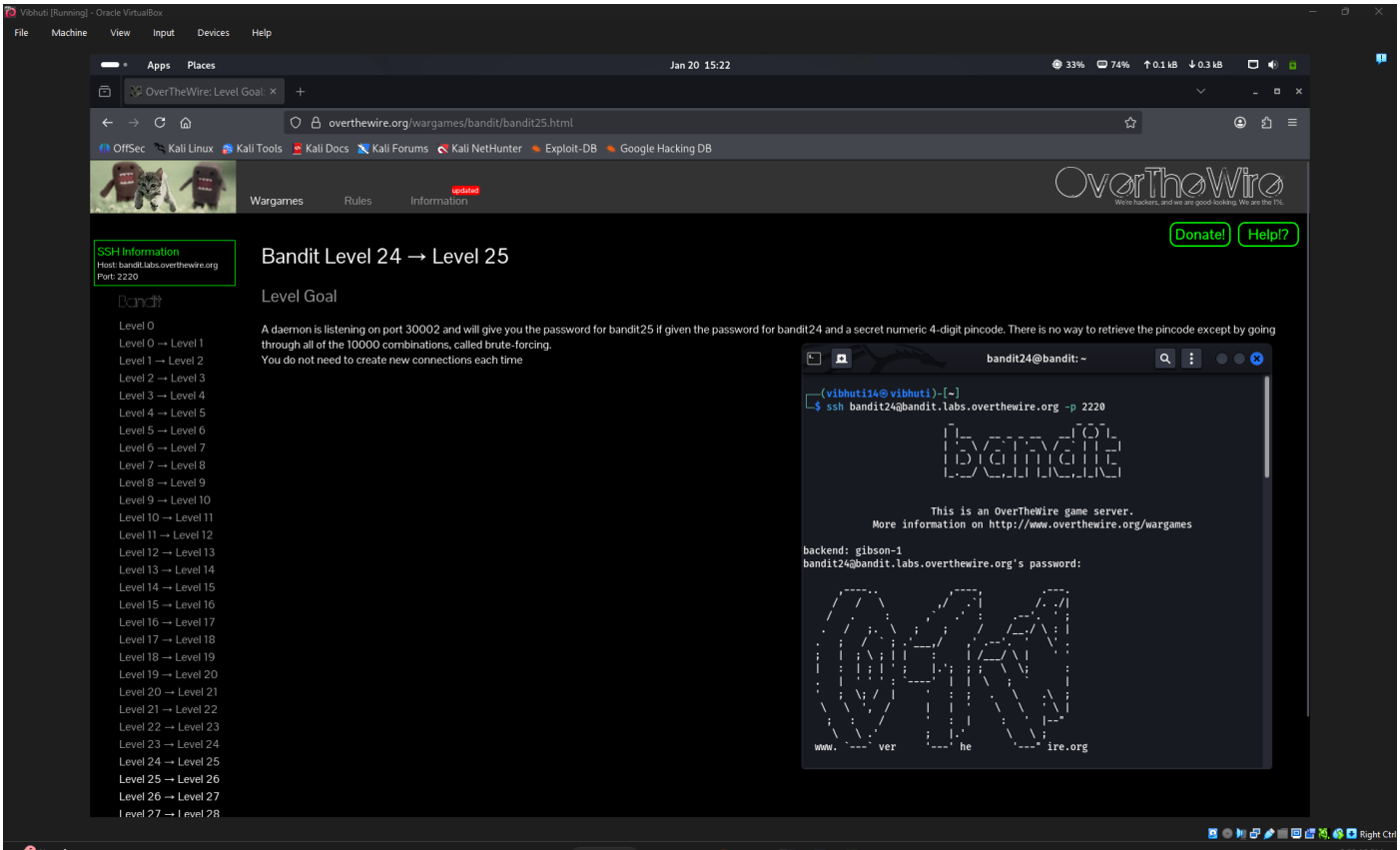
Level 24 -> Level 25

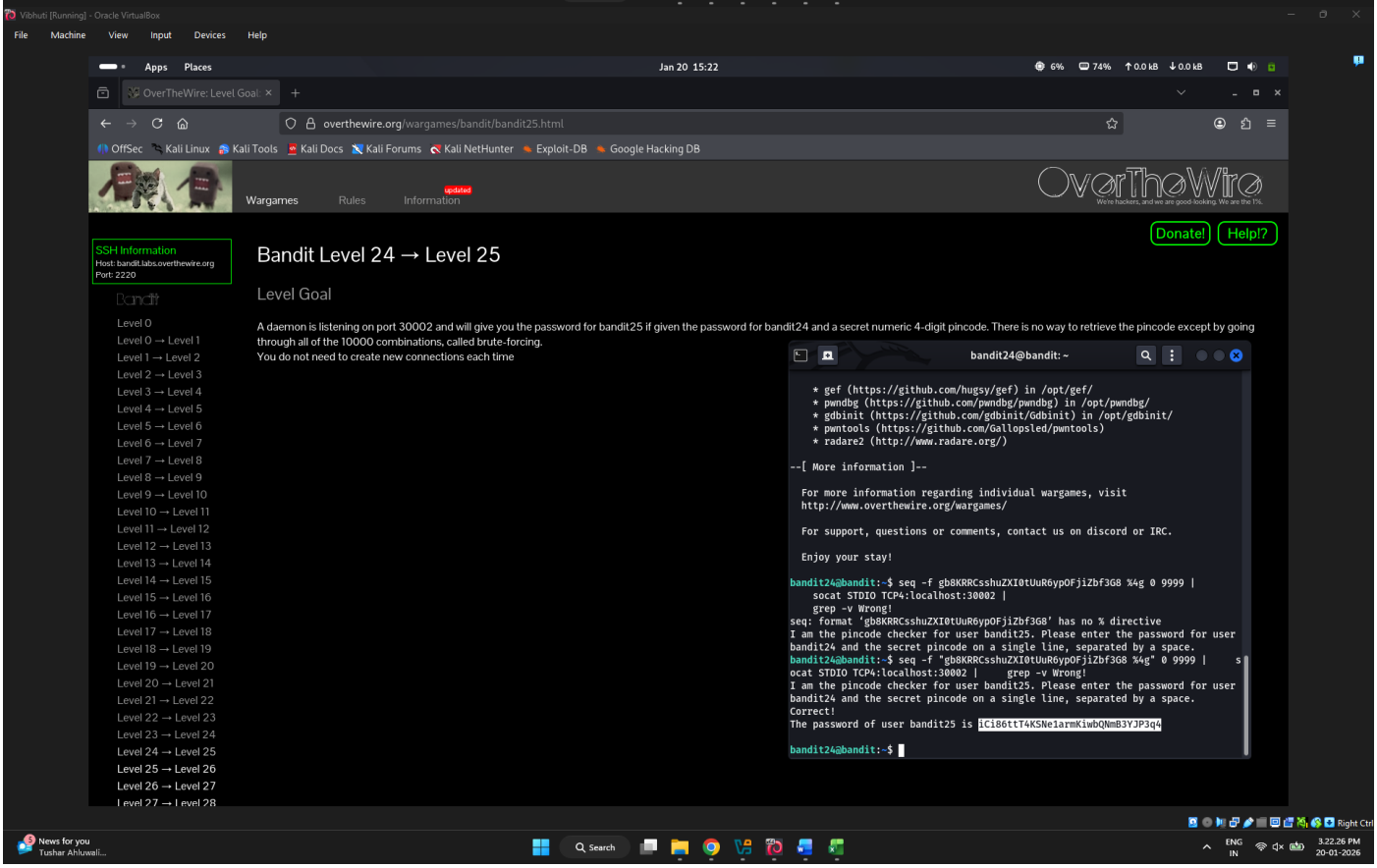
Tools Used: seq

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 2220
3. Here's the command that finds the password.
   seq -f " gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 %4g" 0 9999 |
   socat STDIO TCP4:localhost:30002 |
   grep -v Wrong!


Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Jan 20 15:22
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
OverTheWire
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
Level 27 → Level 28
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
bandit24@bandit: ~
(vibhuti14㉿vibhuti)-[~]
$ ssh bandit24@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
bandit24@bandit.labs.overthewire.org's password:
Right Ctrl
News for you
Tushar Ahluwali...
Search
ENG IN
3.22.16 PM
20-01-2026


Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Jan 20 15:22
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
OverTheWire
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
Level 27 → Level 28
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
bandit24@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!
bandit24@bandit:~$ seq -f gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 %4g 0 9999 |
socat STDIO TCP4:localhost:30002 |
grep -v Wrong!
seq: format 'gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8' 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 "gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 %4g" 0 9999 | s
ocat 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 iCi86ttT4KSNe1armKiwbQNmB3YJP3q4
bandit24@bandit:~$
Right Ctrl
News for you
Tushar Ahluwali...
Search
ENG IN
3.22.26 PM
20-01-2026