Sri Lanka Institute of Information Technology

BSc Honors in Information Technology

Specializing in Cyber Security

IE2012 - Systems and Network Programming

Exploring Bandit Levels

IT22083678
SAHAN H P T

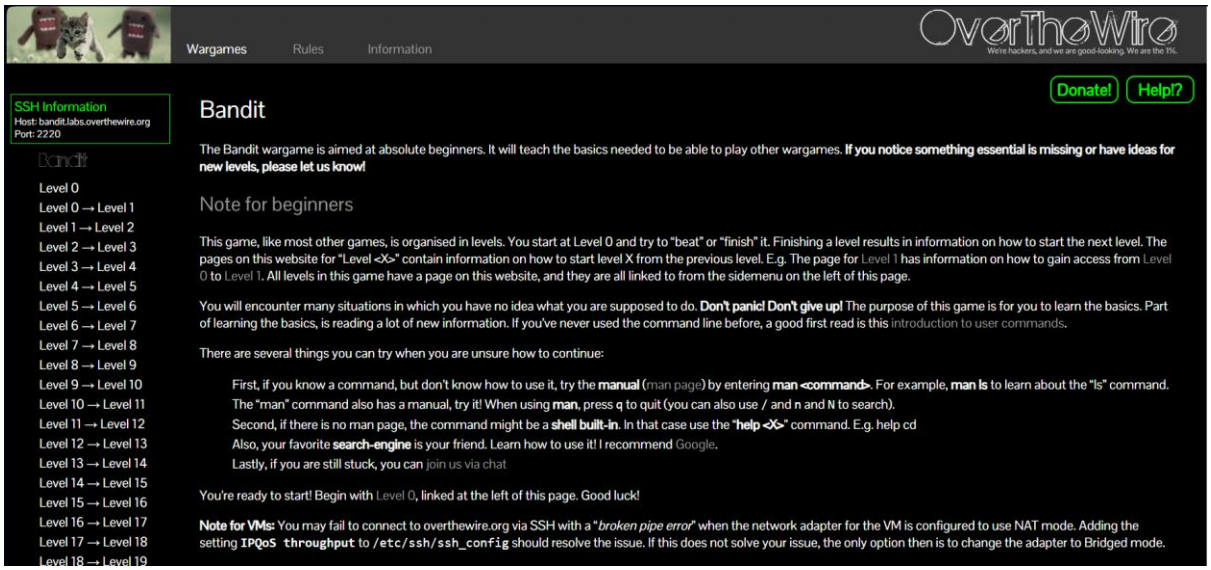
Introduction to the topic

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

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

Bandit0

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



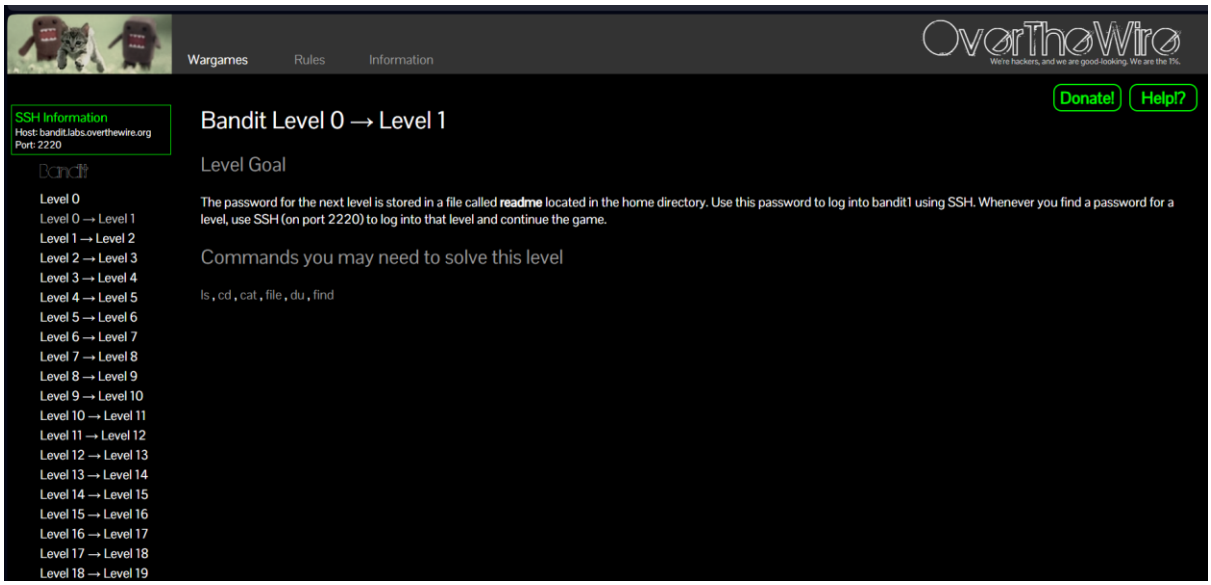
Here we can continue the Bandit game on Windows or Linux. Must log in via SSH to start. We have been given the username and password for Bandit 0.

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

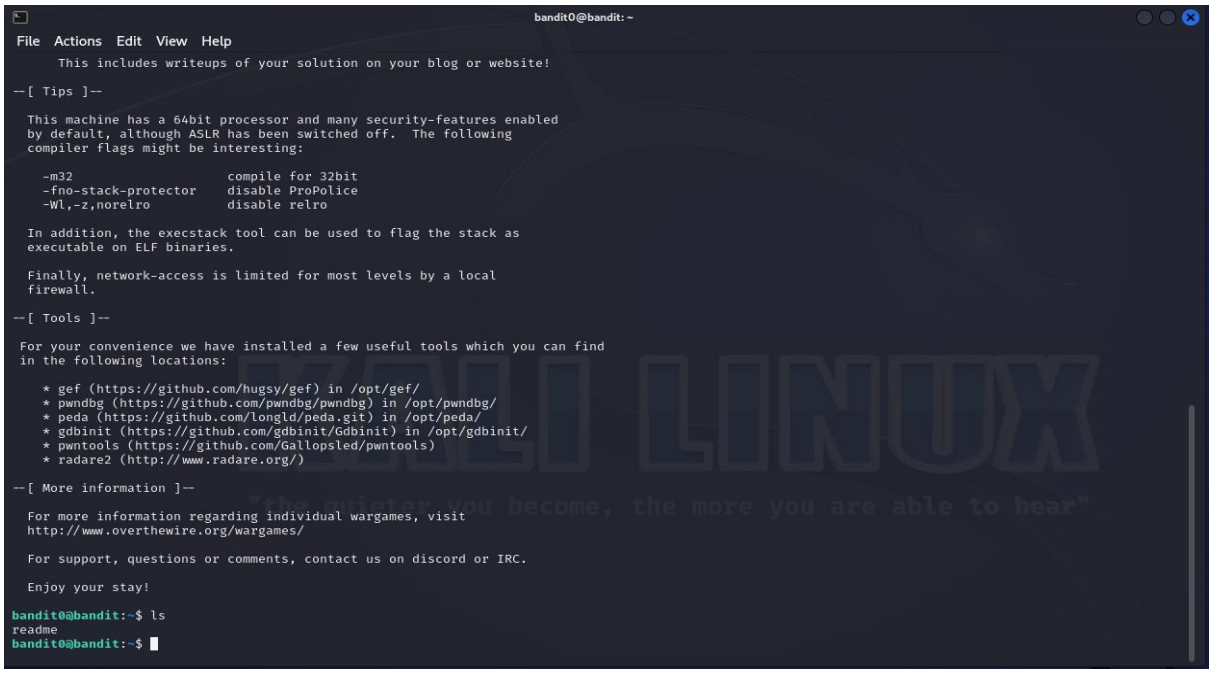
Bandit0 -> Bandit1

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

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



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

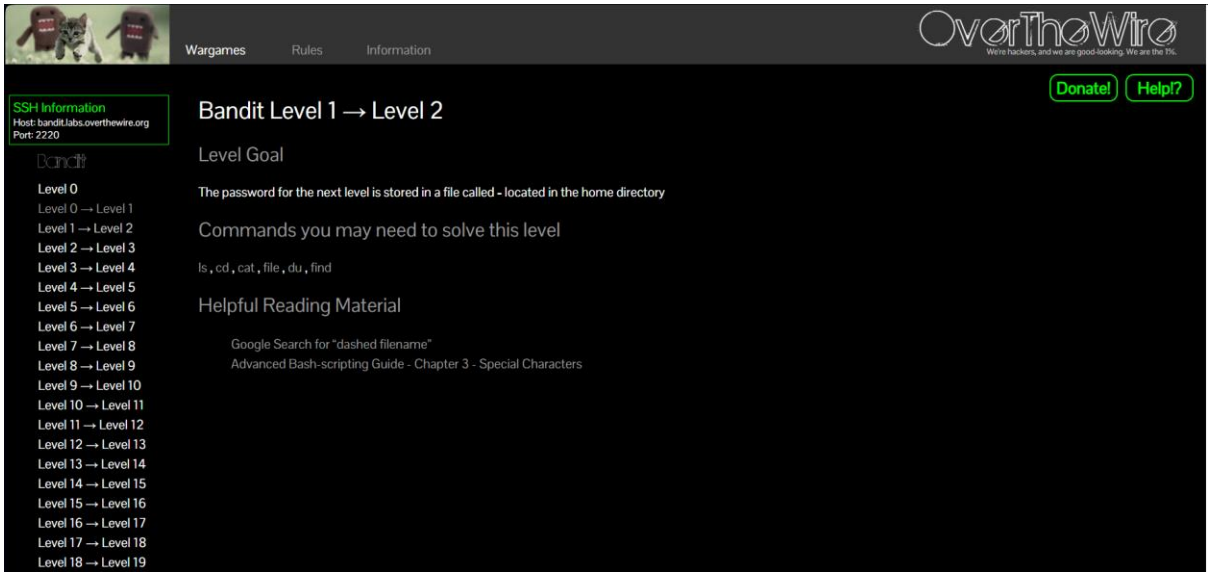


Run “cat readme” to see the contents of the readme and to get the password.

To logout, run “exit”

Bandit1 > Bandit2

Read the hint and try to get an idea.



Now log in to Bandit1, from the found password.

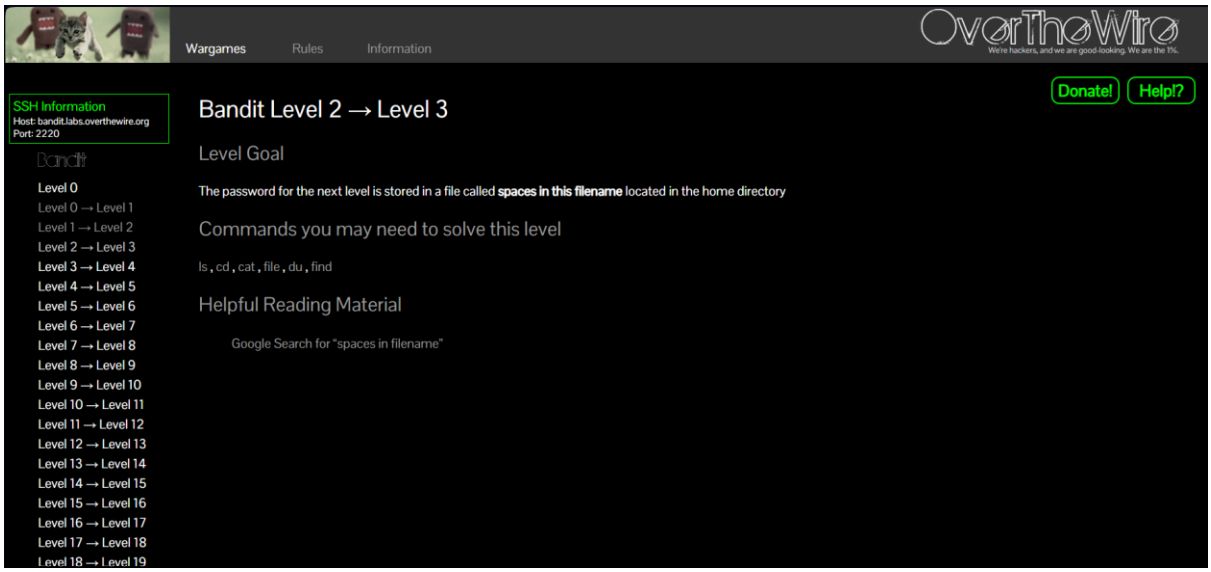
Run the “ls” command and find the “-“ file

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

Log out using the “exit” command.

Bandit2 > Bandit3

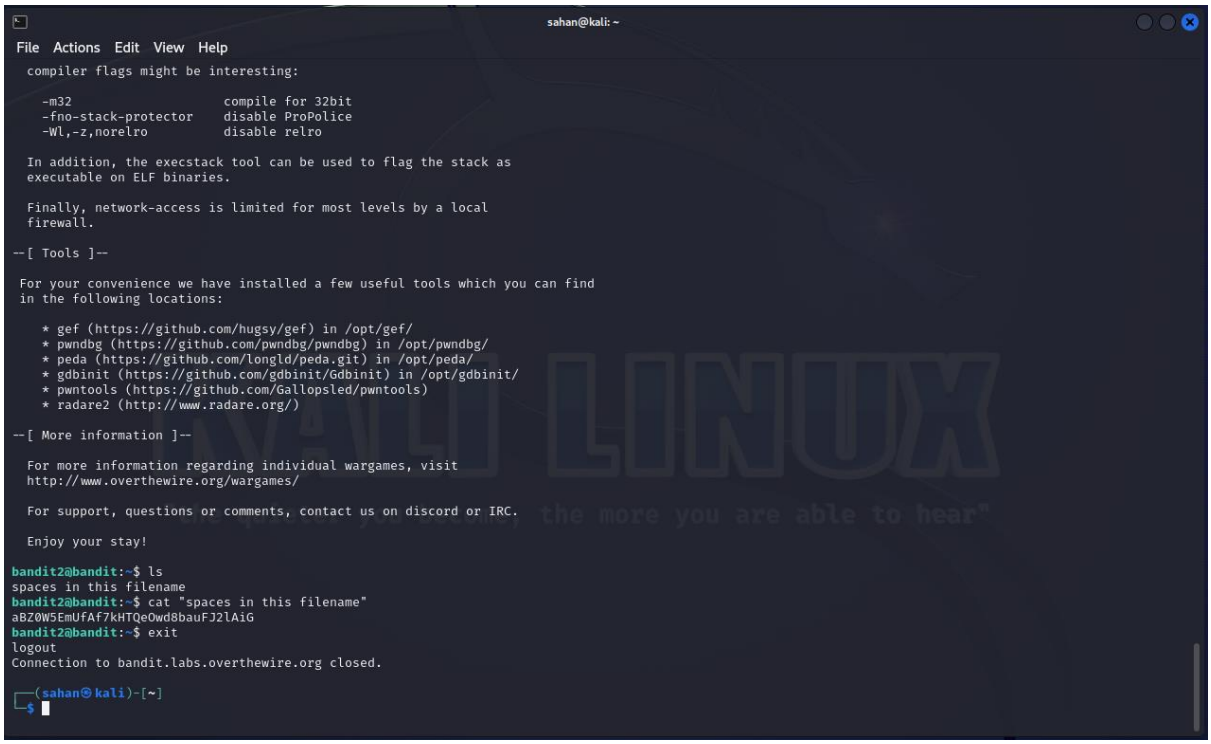
They tell us the next password is in a “spaces in this filename” file.



Log into Bandit2 using the username and the password.

Using the “ls” command find the file name.

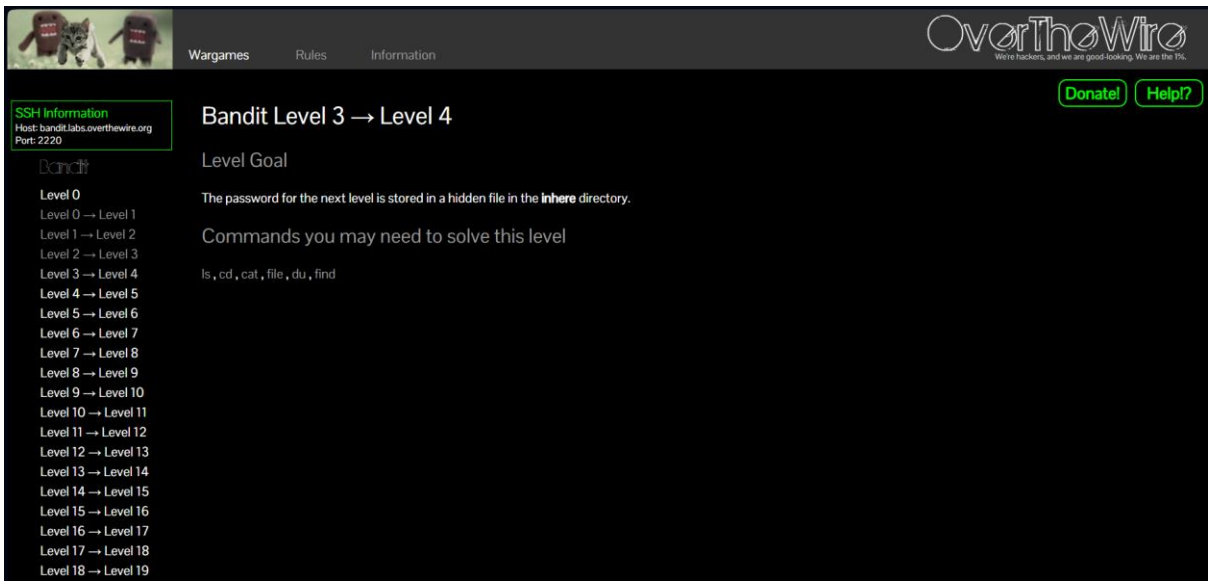
Run the “cat” command with the file name. You can get the Bandit3 password.

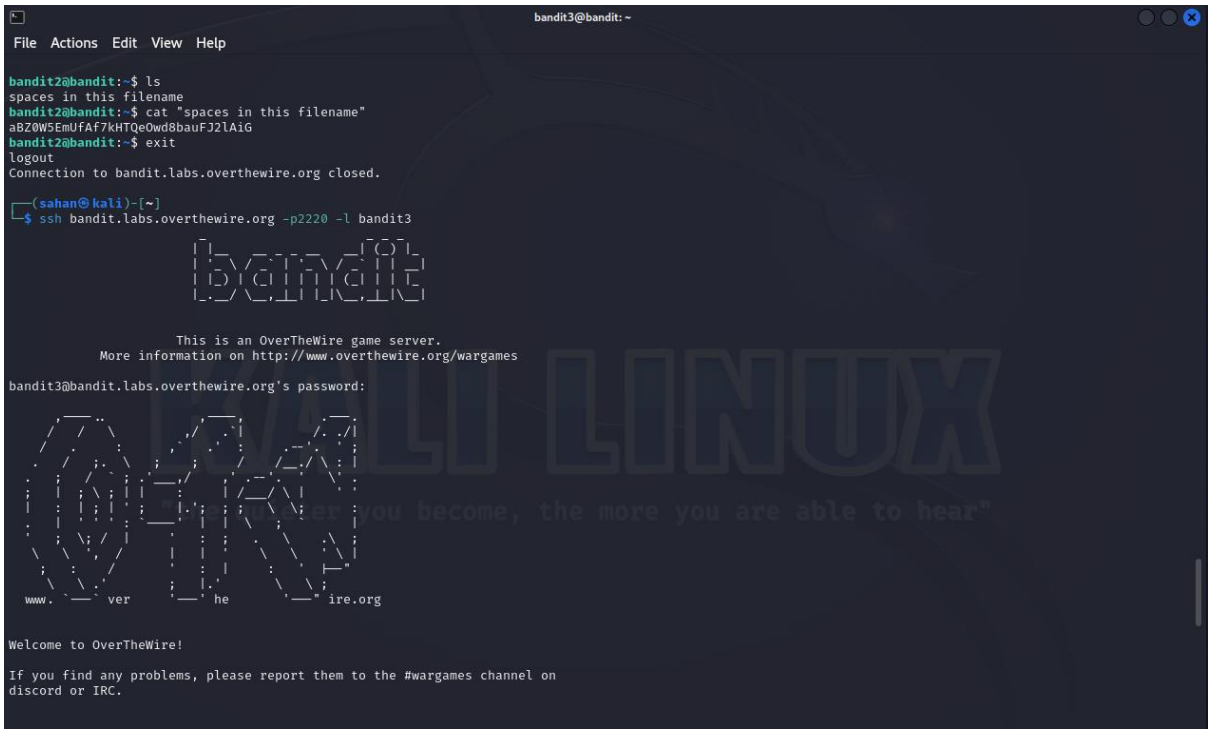


Log out using the “exit” command.

Bandit3 > Bandit4

Log Bandit 3 to use the password.





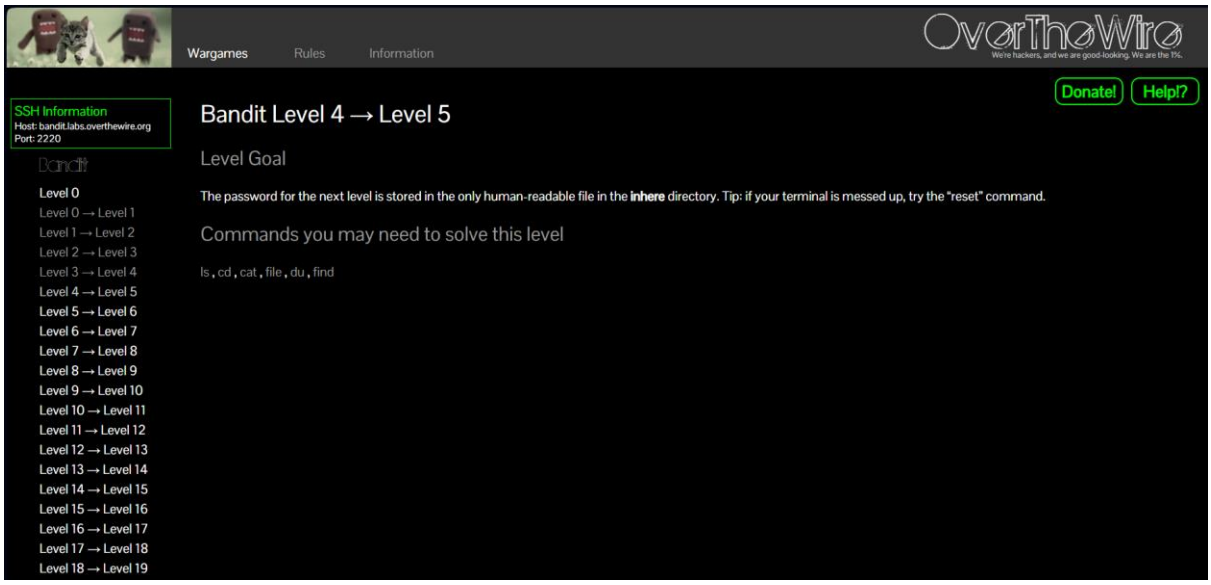
The next level password is hidden in the inhere file. Using the “ls” command find the “inhere” file name.

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

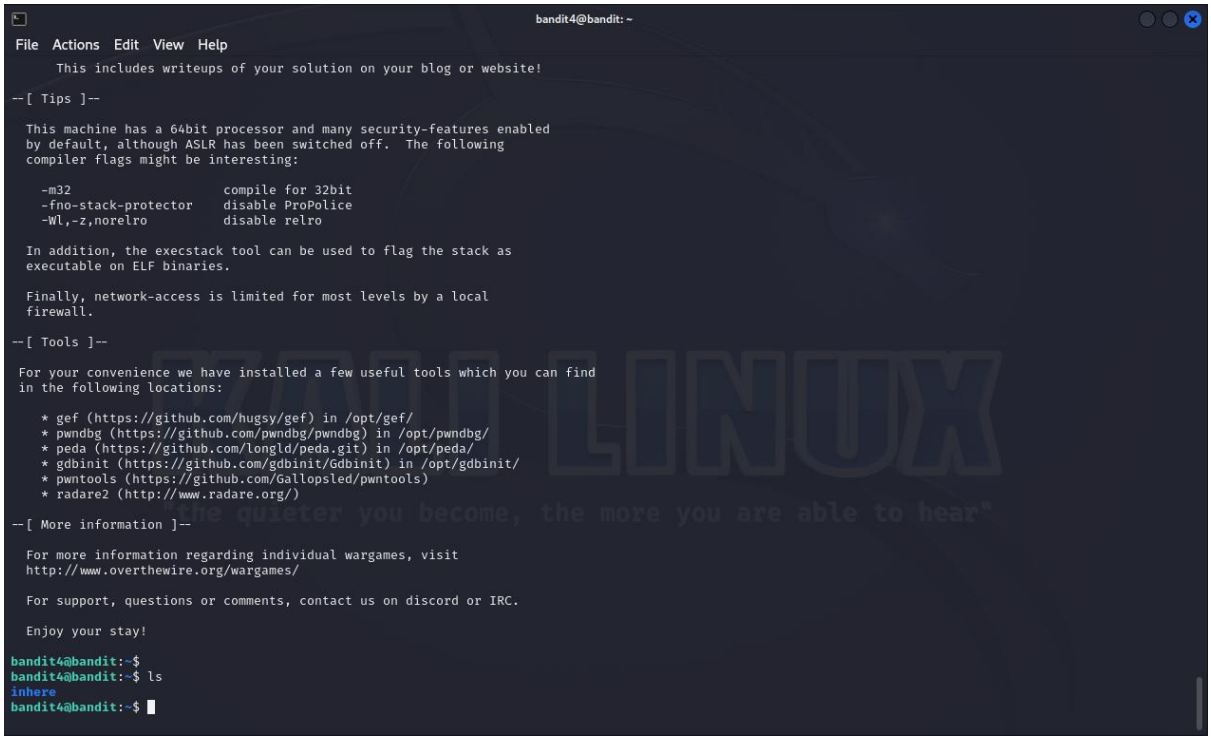
We can read the contents of the file because it is named “.hidden” and includes the password

Log out using the “exit” command.

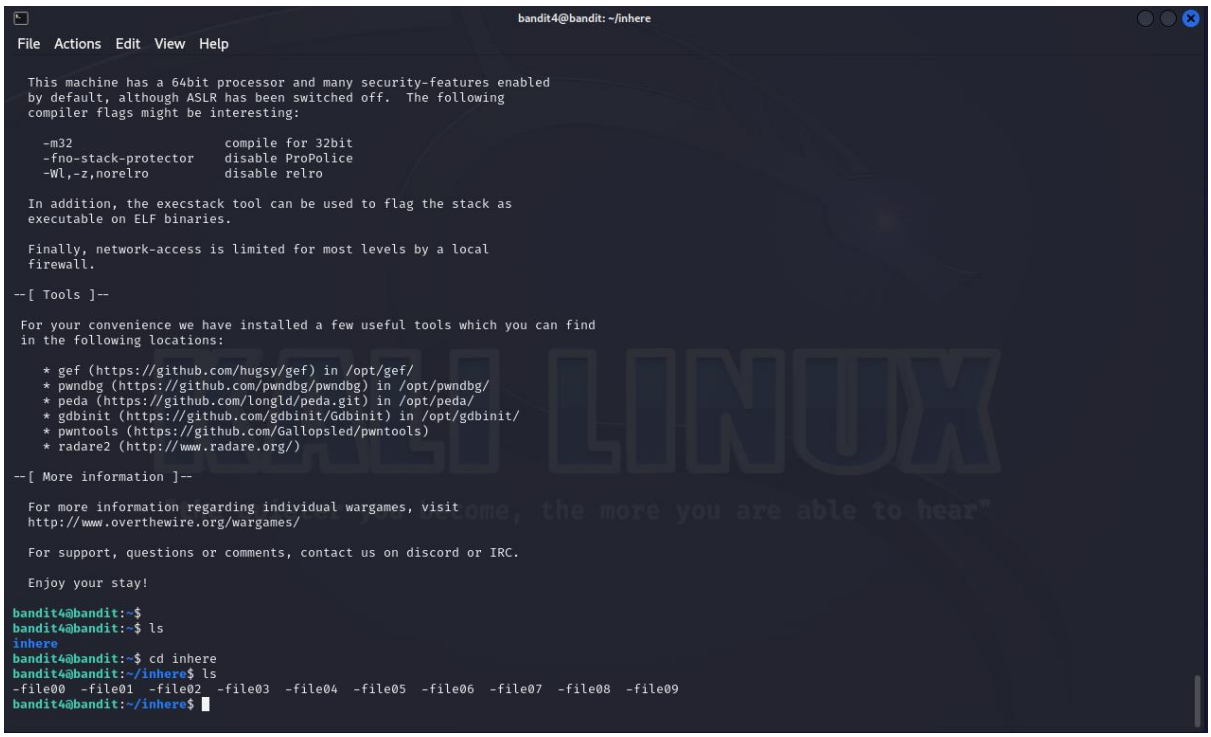
Bandit4 -> Bandit5



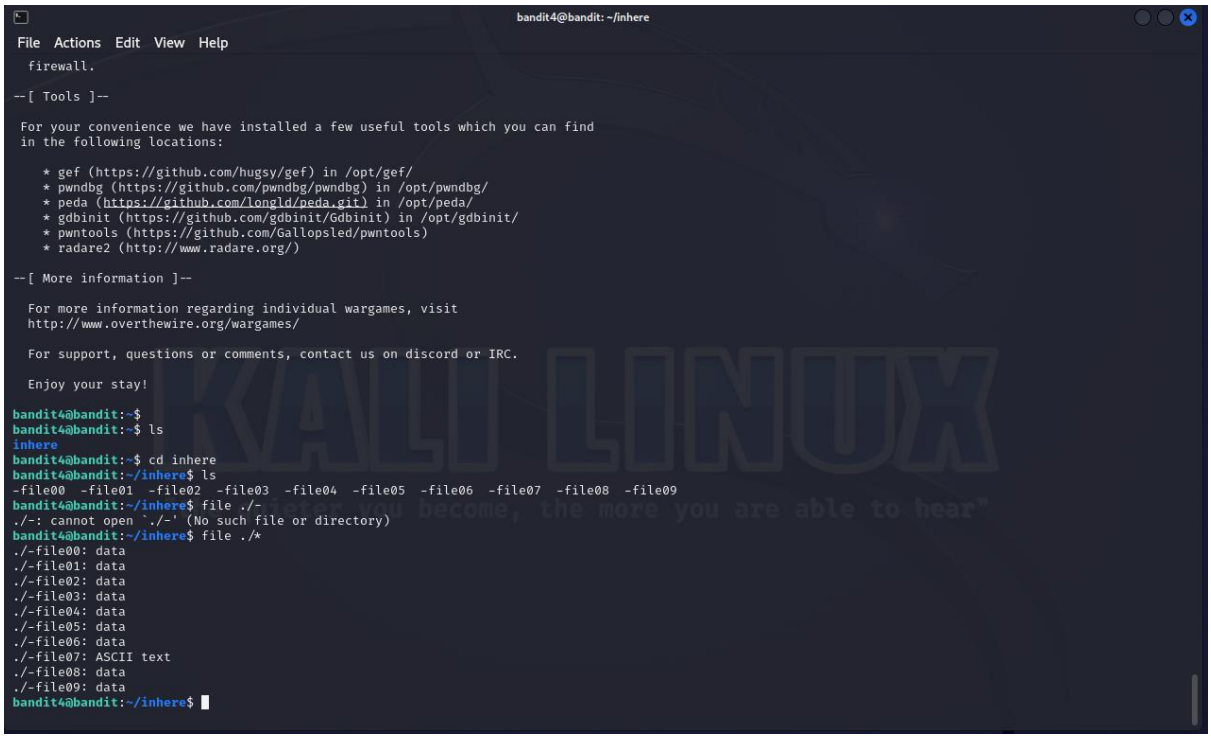
Log into the Bandit4 using the password. Use the “ls” command and find the file.



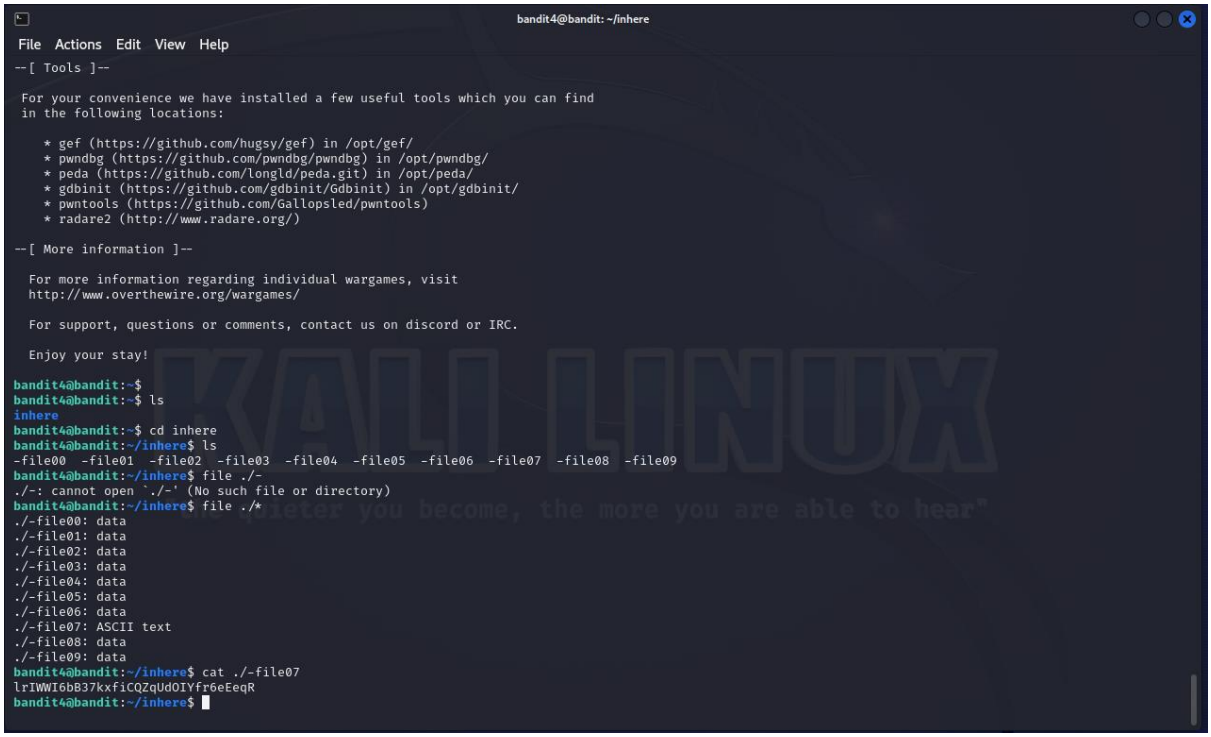
Using the “cd” command change the directory. And use the “ls” command.



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

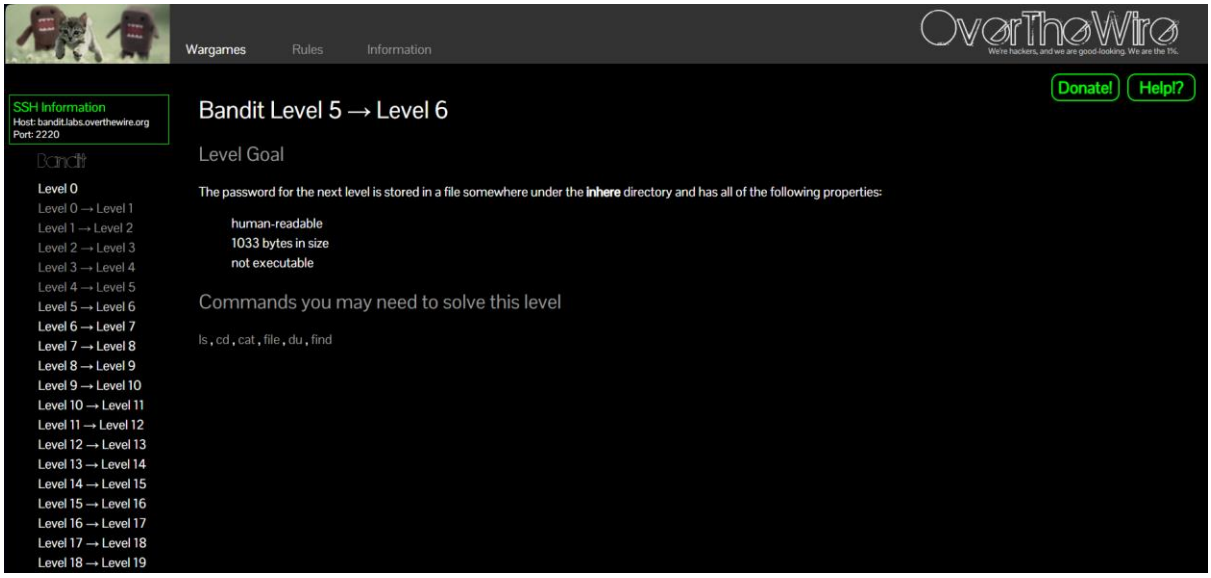


The “-file07” has ASCII text. Type “cat ./-file07” to get the password of Bandit5.

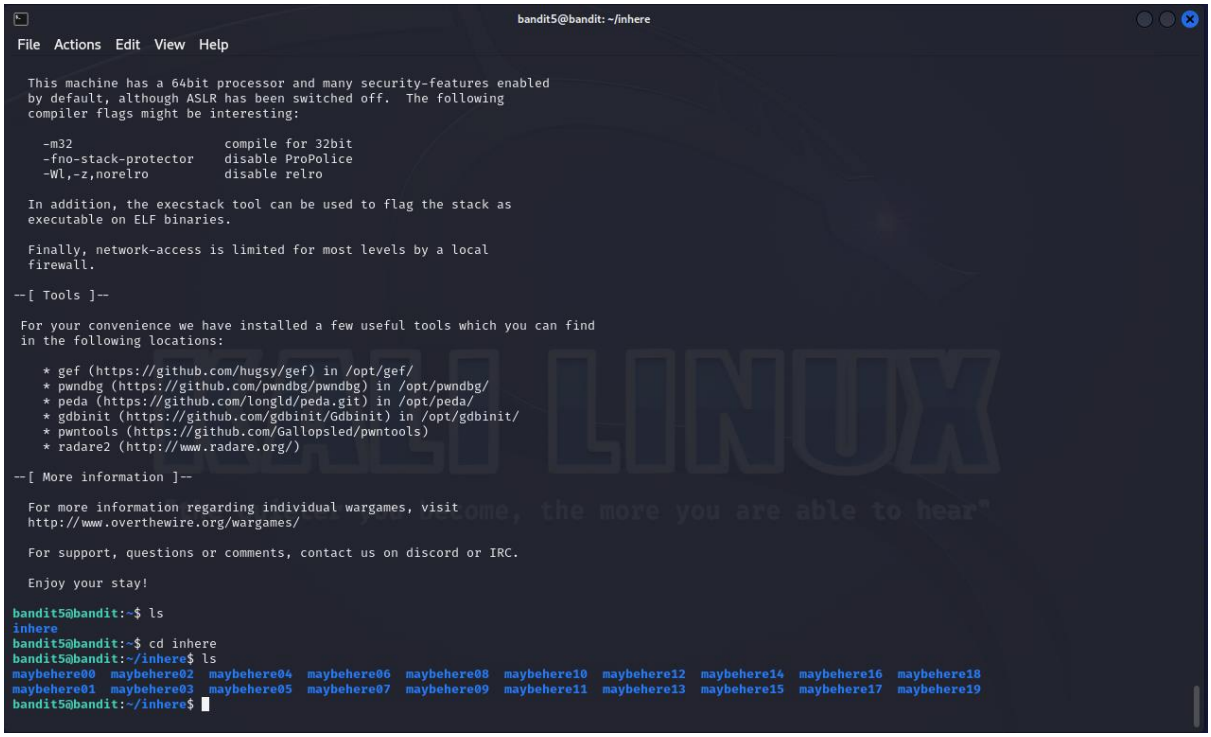


Bandit05 -> Bandit06

Log in to Bandit05 using the password.

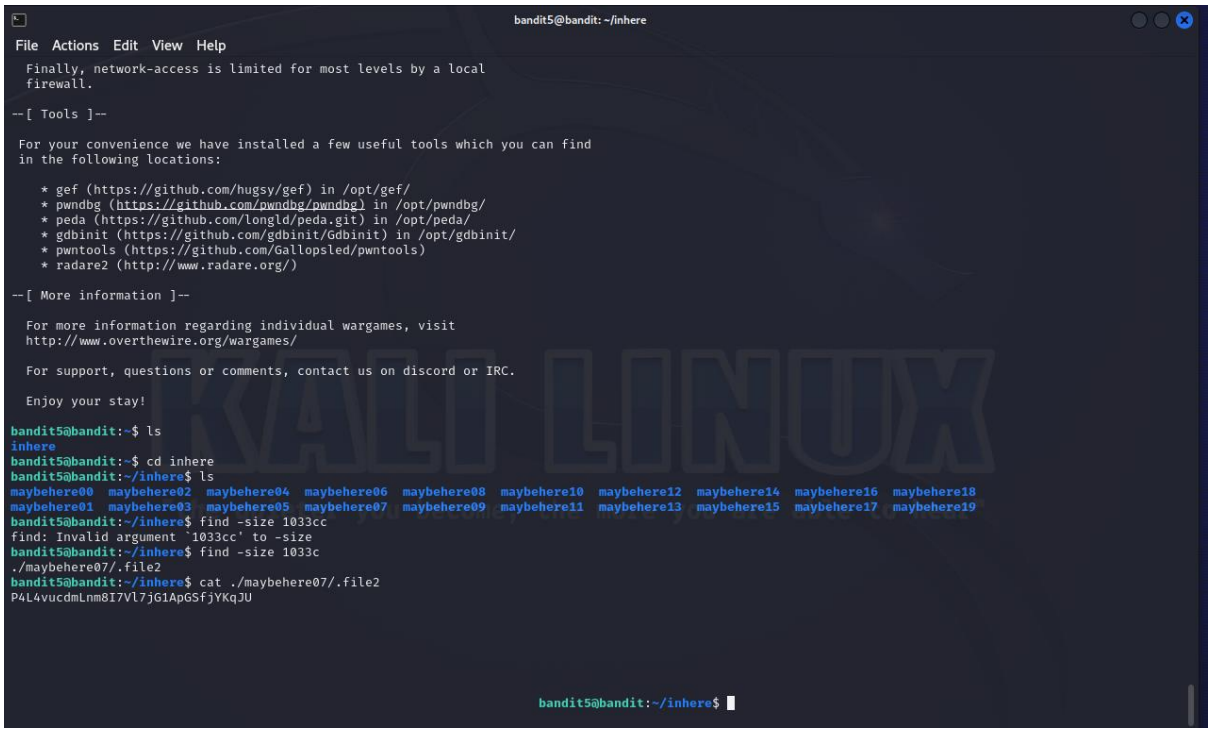


Type the “ls” to find the file name. Next type the “cd inhere” to change the directory. Again type the “ls” to list directory.

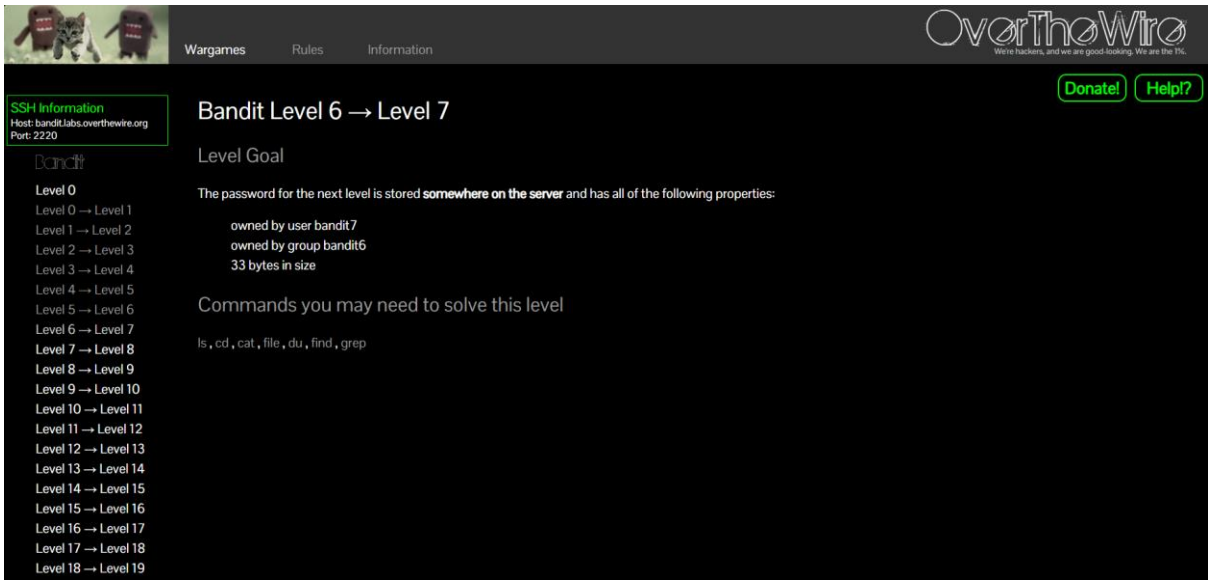


Type the “find -size 1033c” to find files that are readable with a size of 1033c.

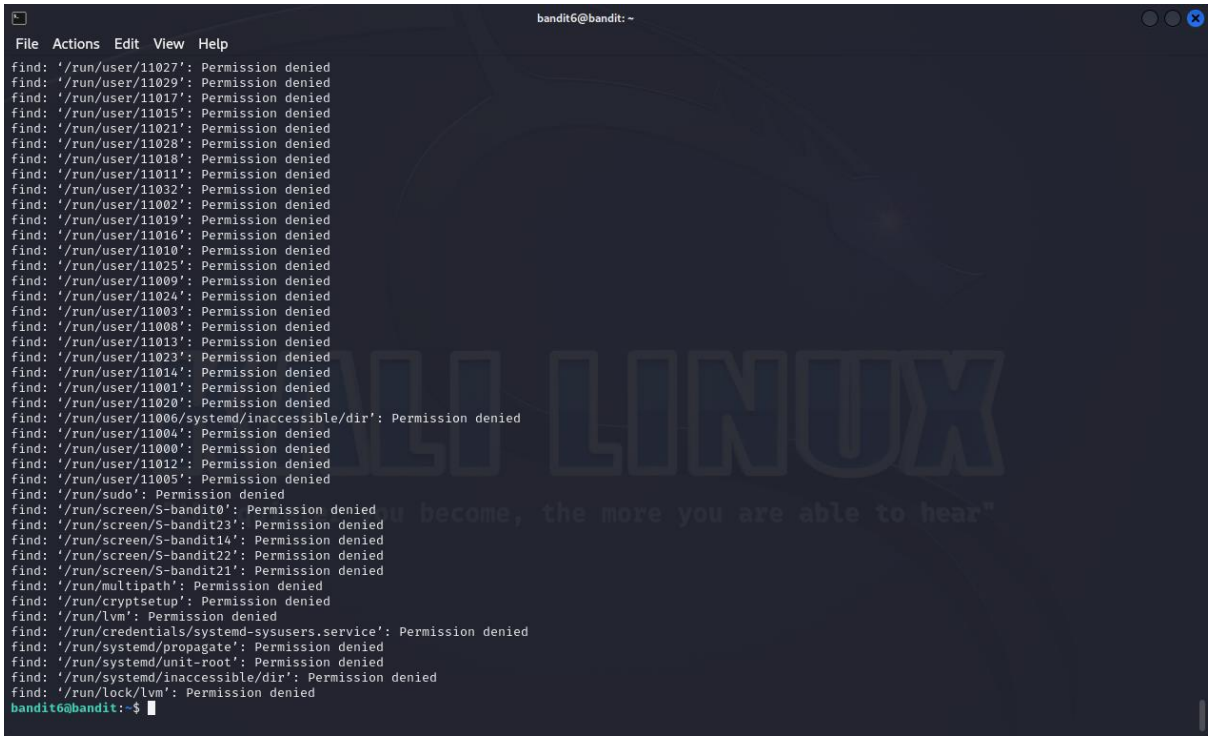
For get the password, type “cat .maybehere07/.file2”



Bandit6 -> Bandit7

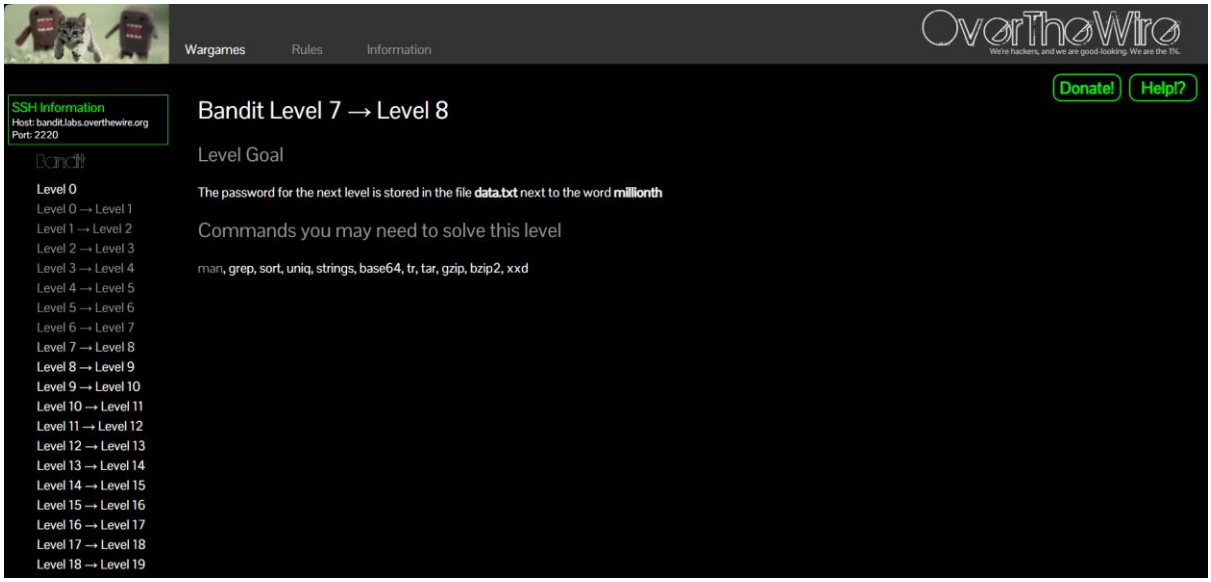


Log into the Bandit6 using the password. Use the root directory command to search the system.

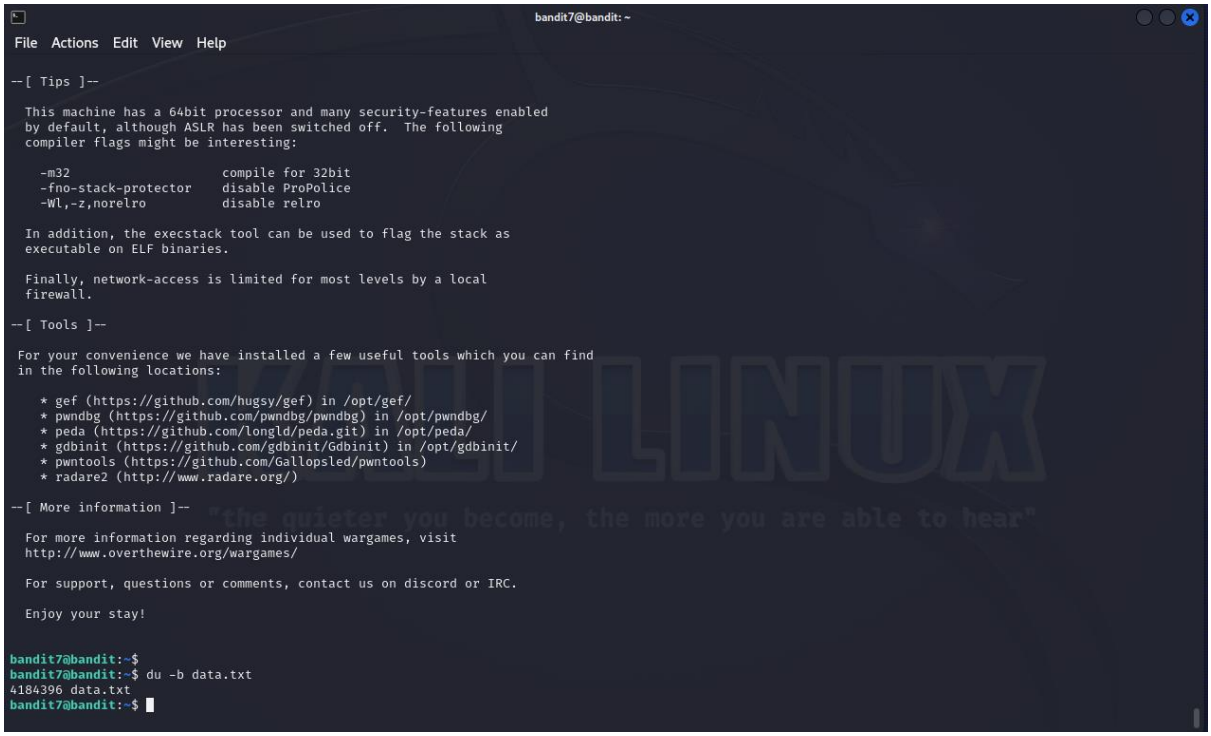


Type this command “cat /var/lib/dpkg/info/bandit7.password” and find the password.

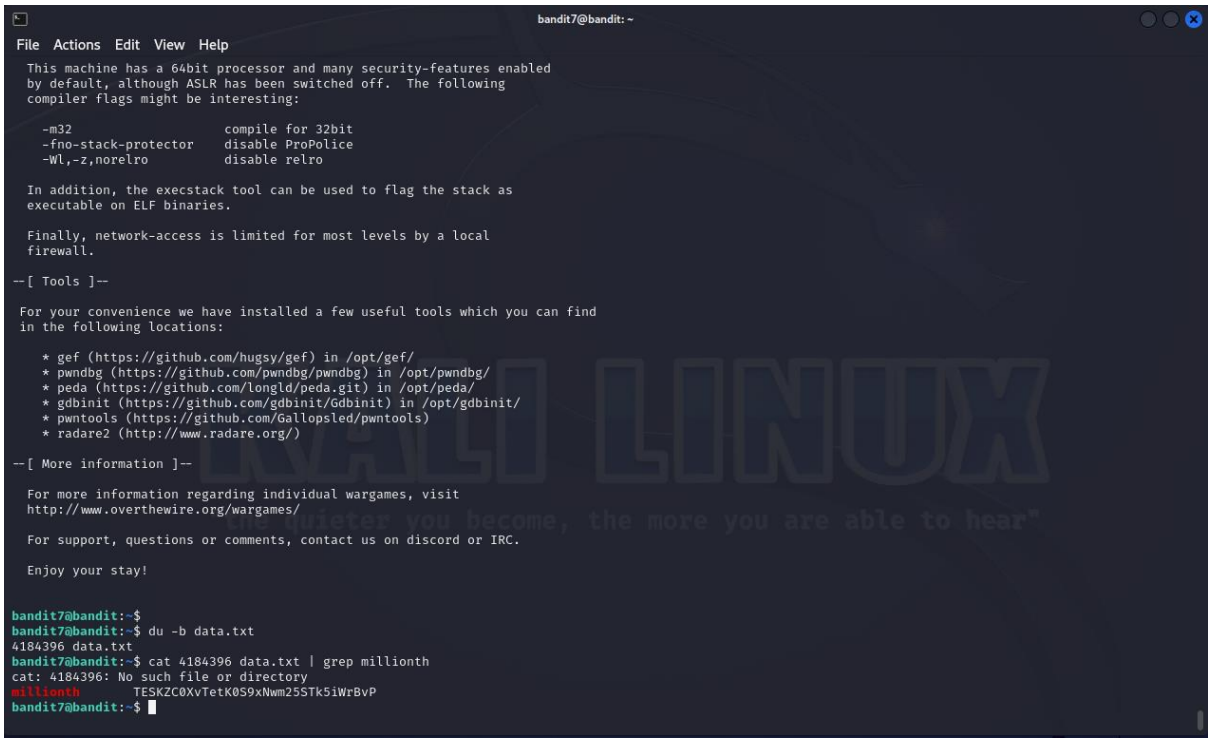
Bandit7 -> Bandit8



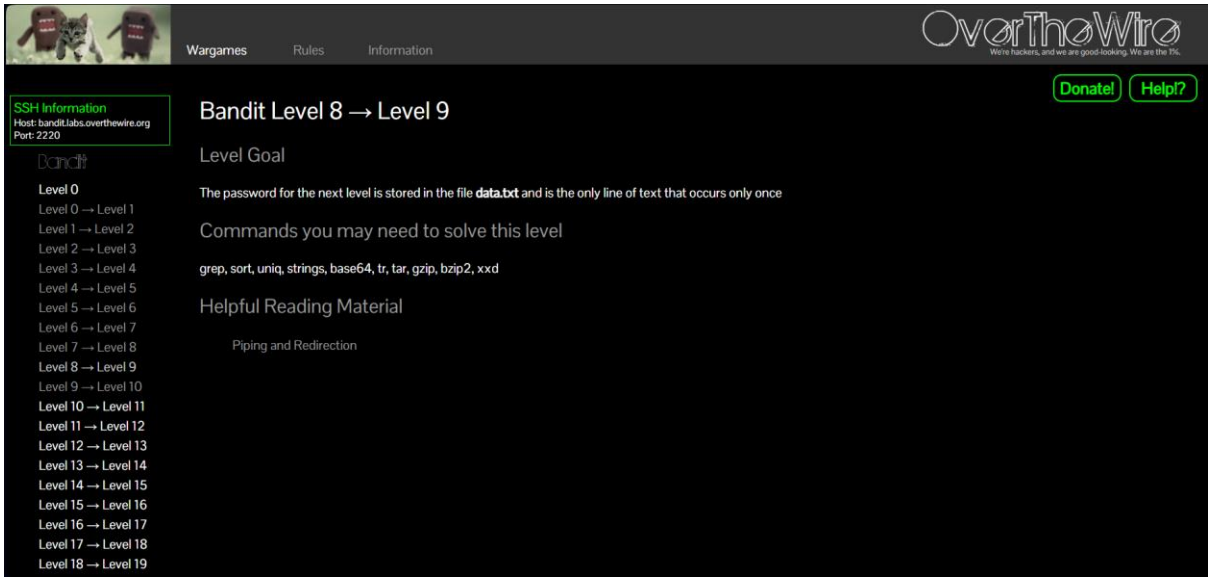
Log into Bandit7 using the password and first check the size of the “data.txt” file.



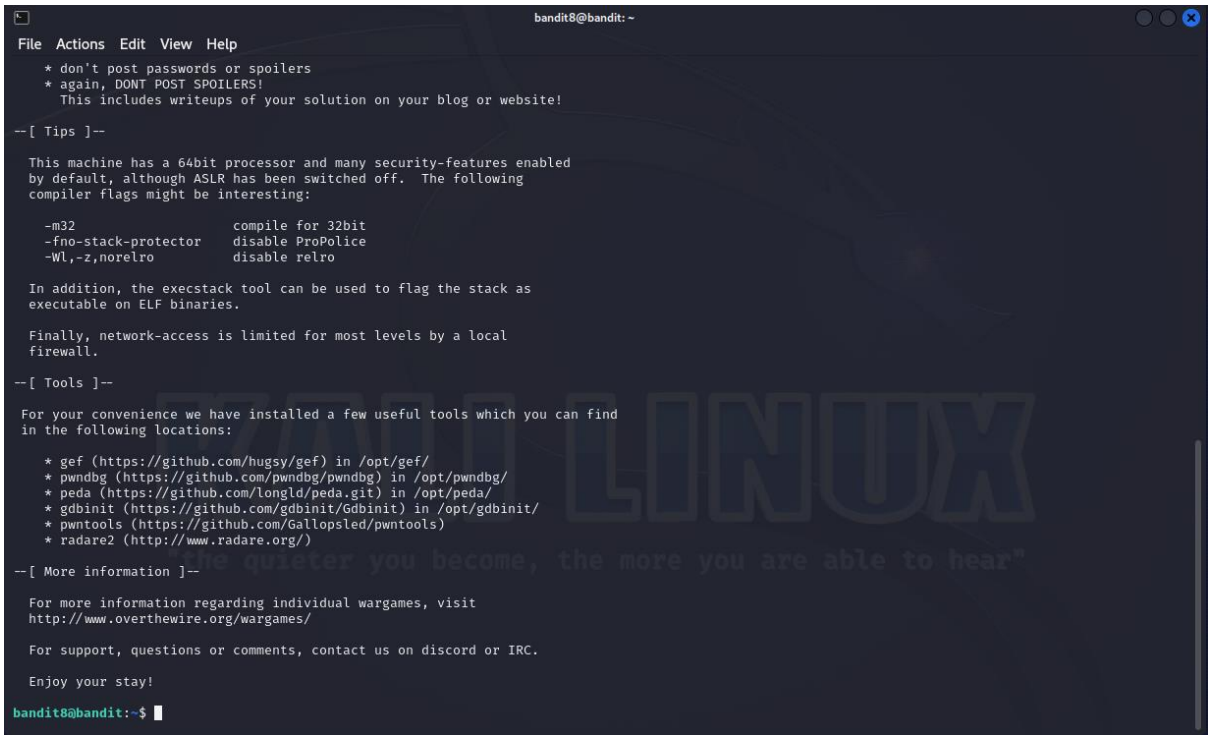
Now we need to use the “grep” command. grep command can be used to search lines that follow a particular pattern. Using the “grep” command and the pipe“|” we can find the password.



Bandit8 -> Bandit9



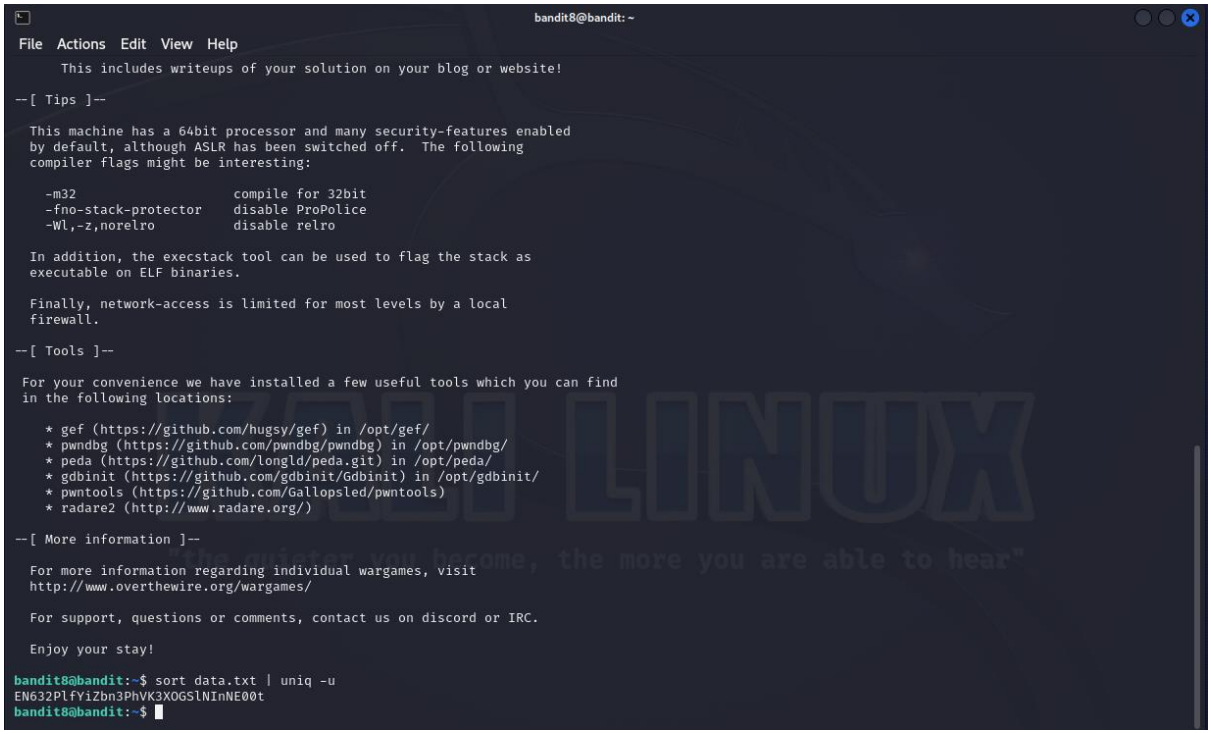
Log into Bandit8 using the password.



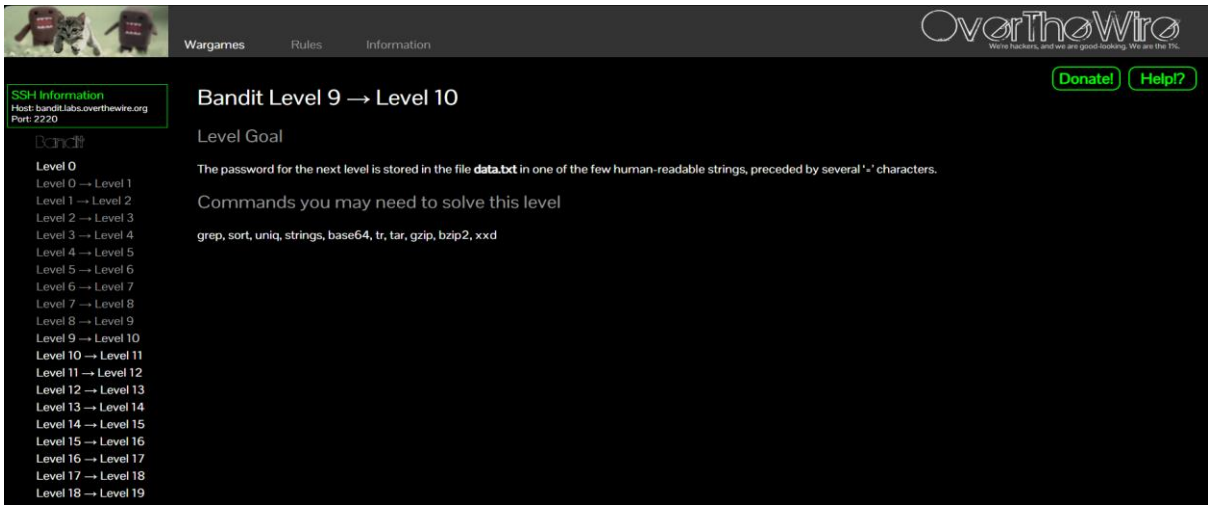
Sort – sorts the lines of a text file

Uniq – filters input and writers to the output

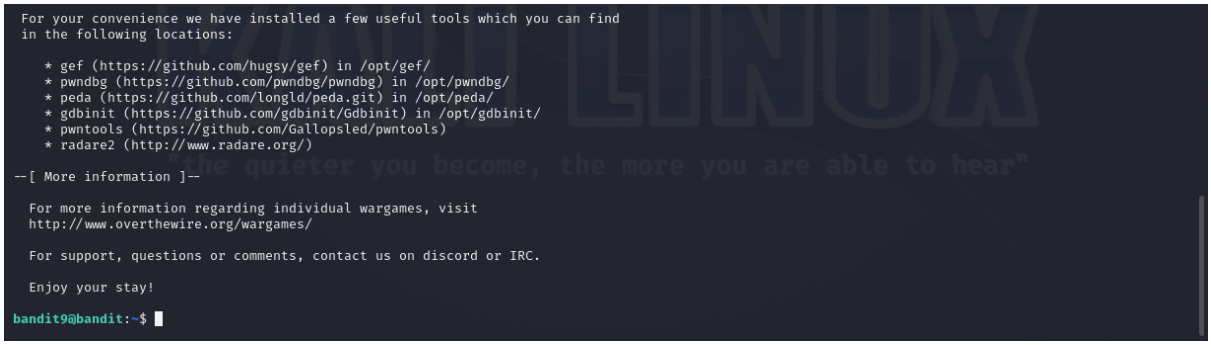
So, using “sort data.txt | uniq -u” we can get the password.



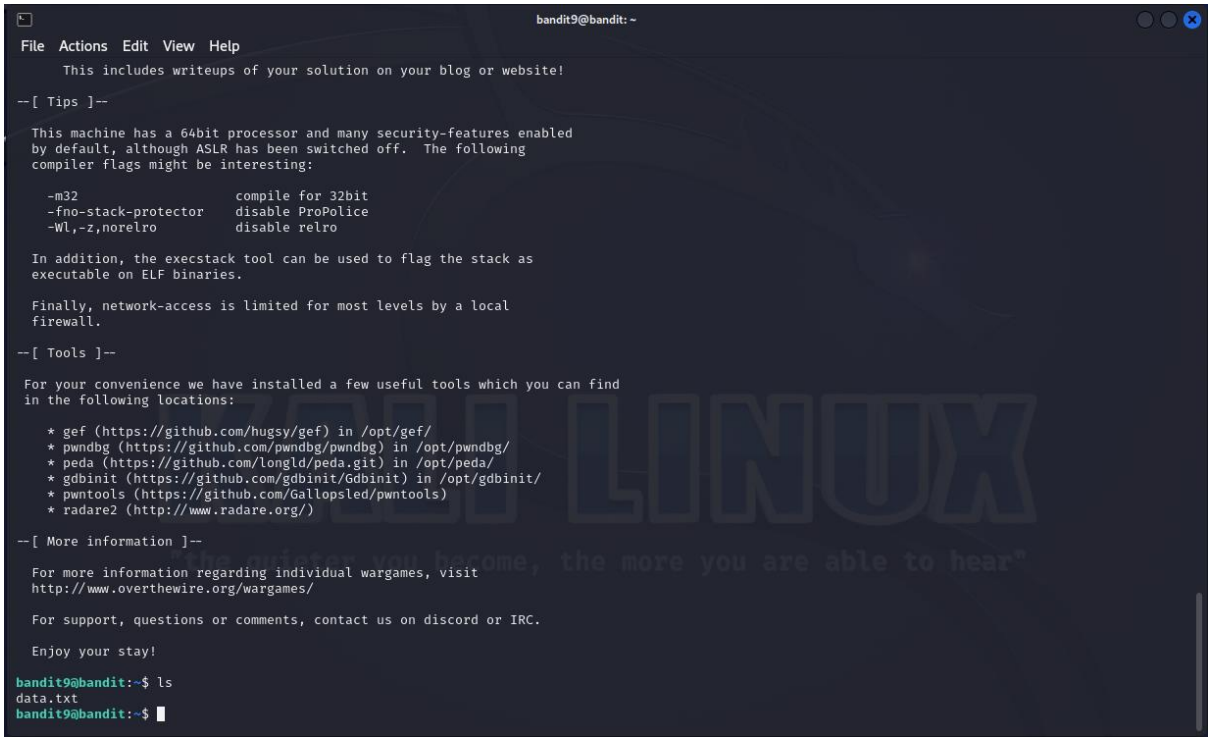
Bandit9 -> Bandit10



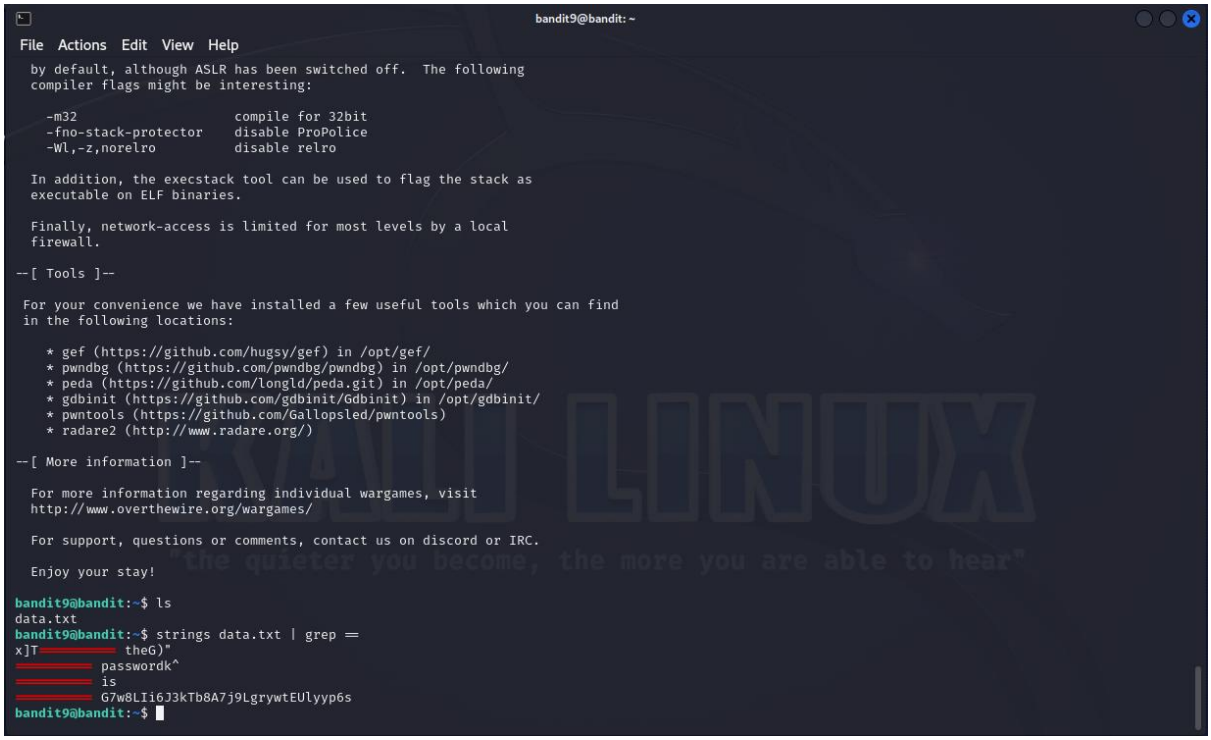
Log into Bandit8 using the password.



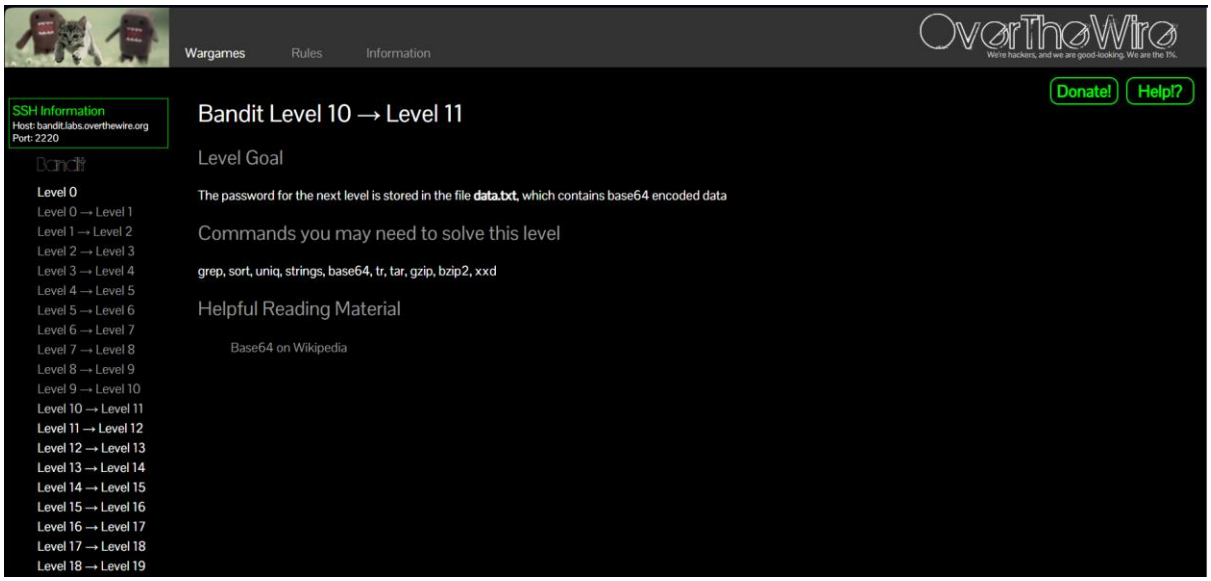
Using the “ls” command find the “data.txt” file.



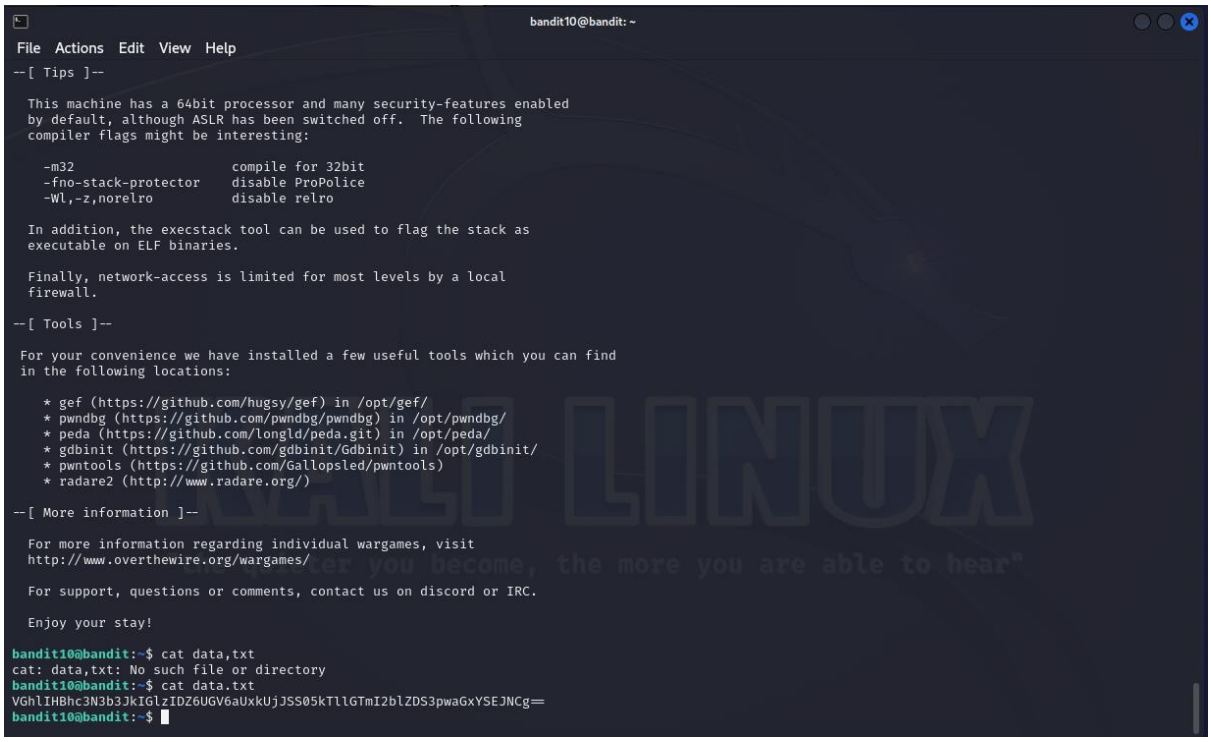
We need to use the “string” command to separate human-readable strings in “data.txt”. And use “grep” within the equal sign “=”.



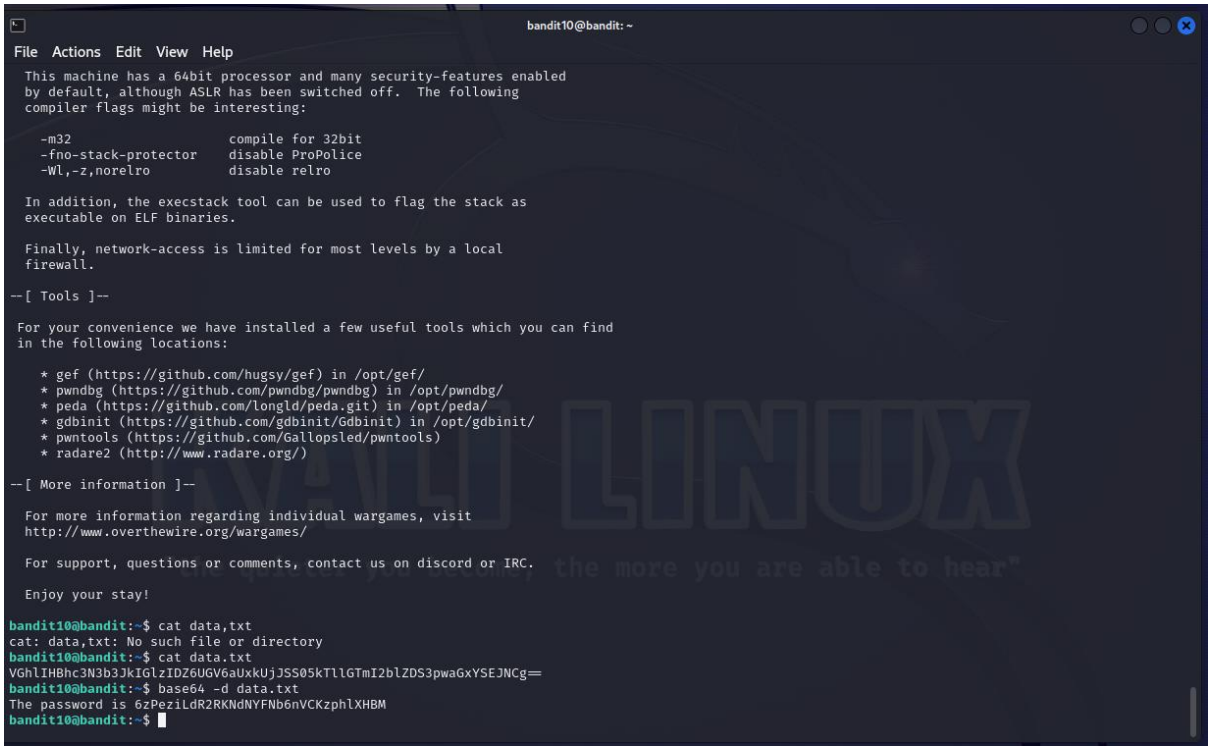
Bandit10 -> Bandit11



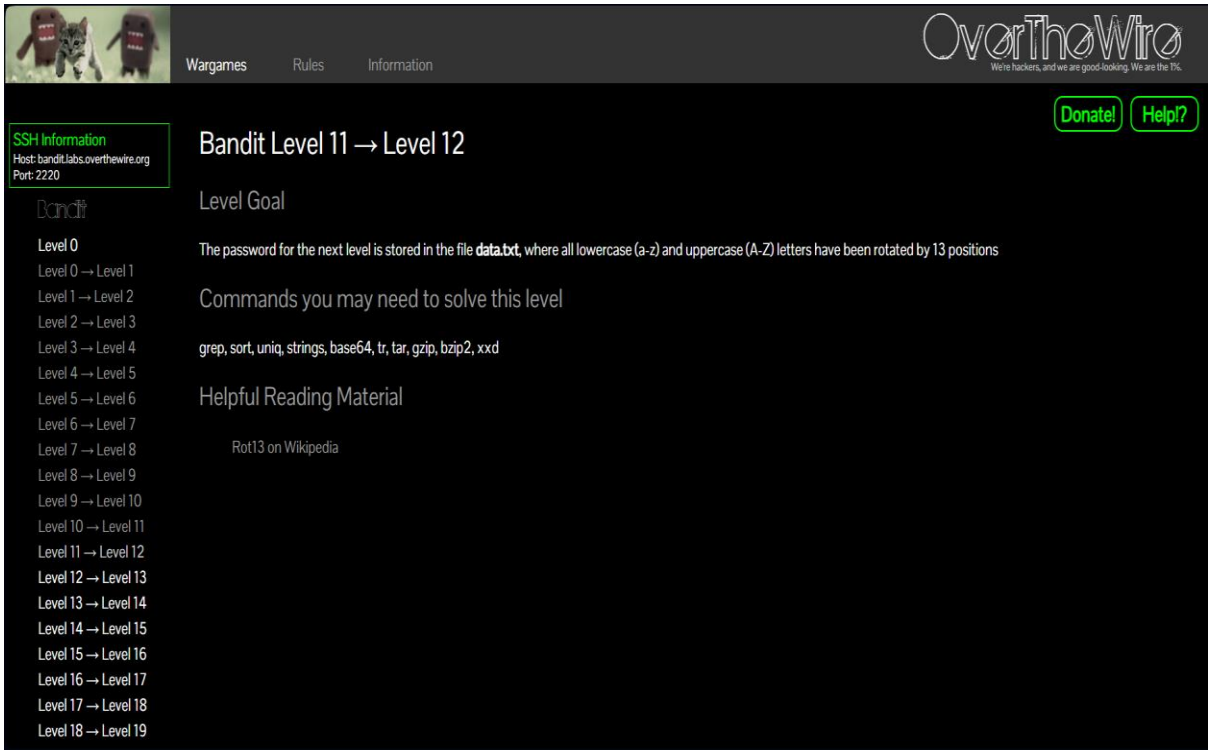
First, log into Bandit10. Run the “cat” command with the file name.



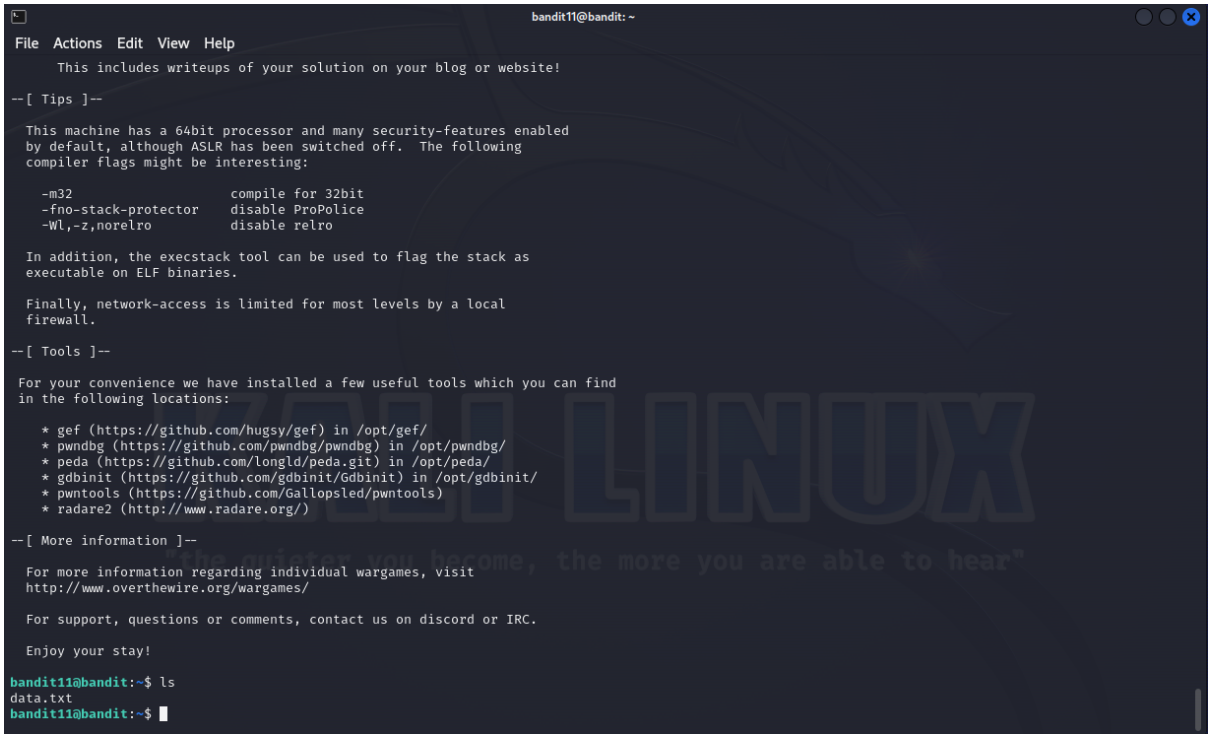
Use the “base64 -d data.txt” command for decoding to the password.



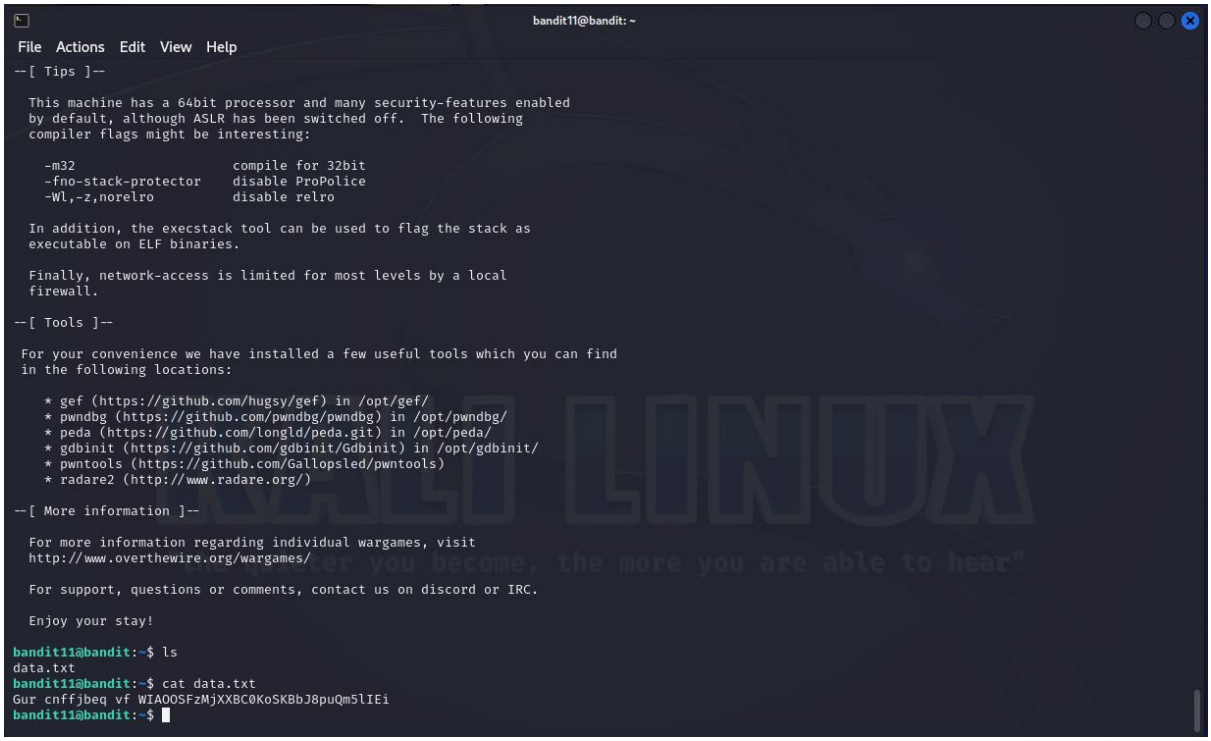
Bandit11-> Bandit12



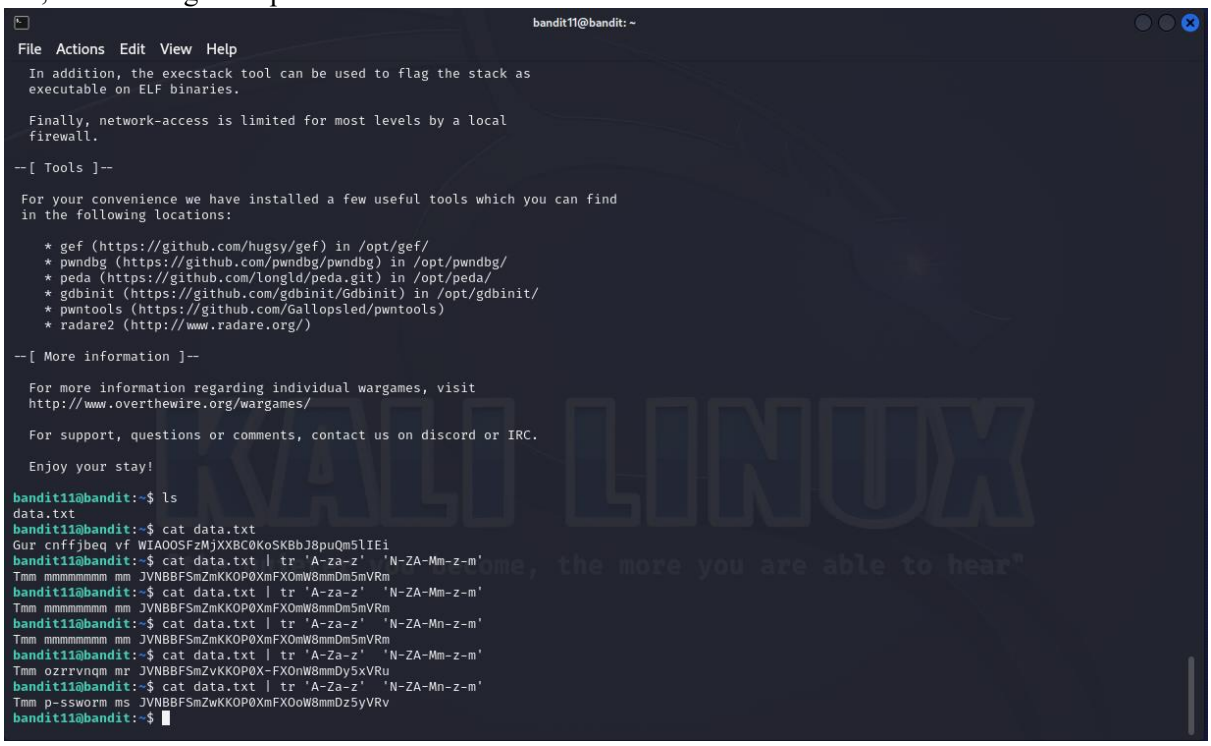
Log into Bandit11 with the password. Use the “ls” command.



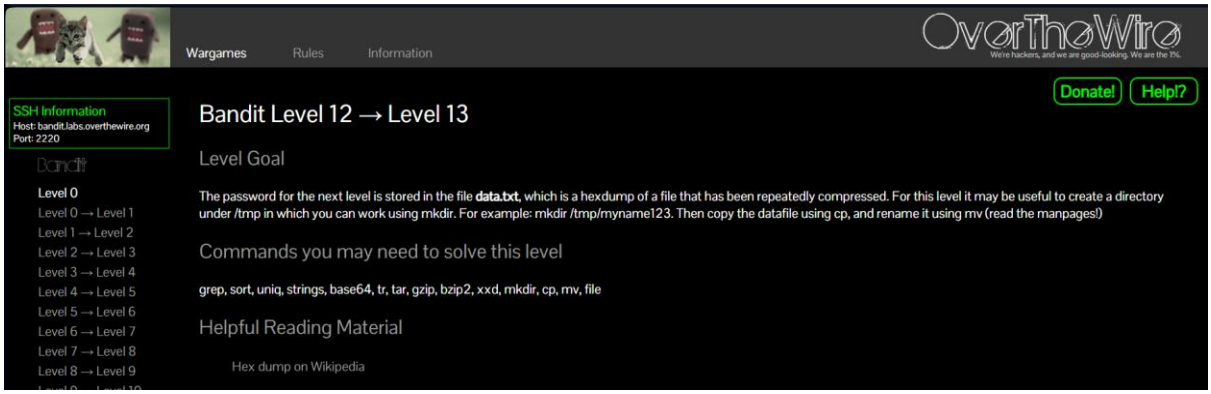
Use the “cat” command to get the password.



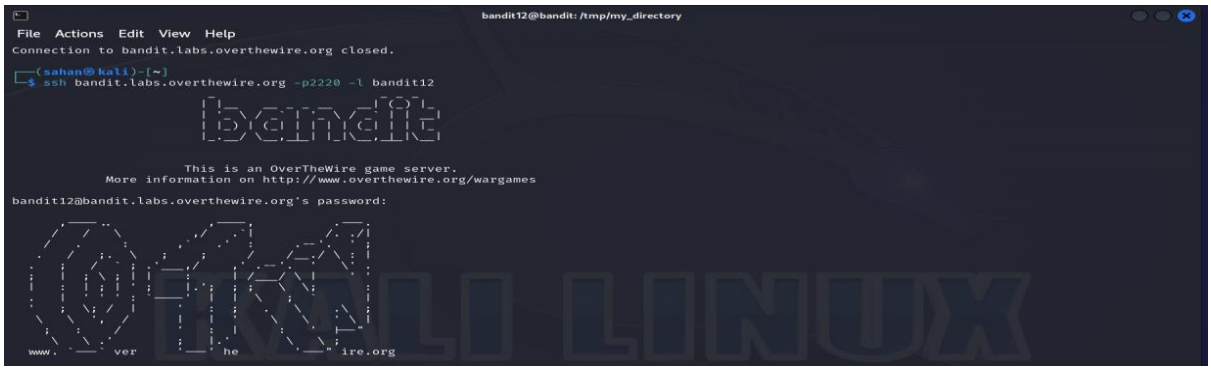
Now use the “tr” command for translation, allowing replacing the characters with others. And “A ->N, …., Z ->M” to get the password.



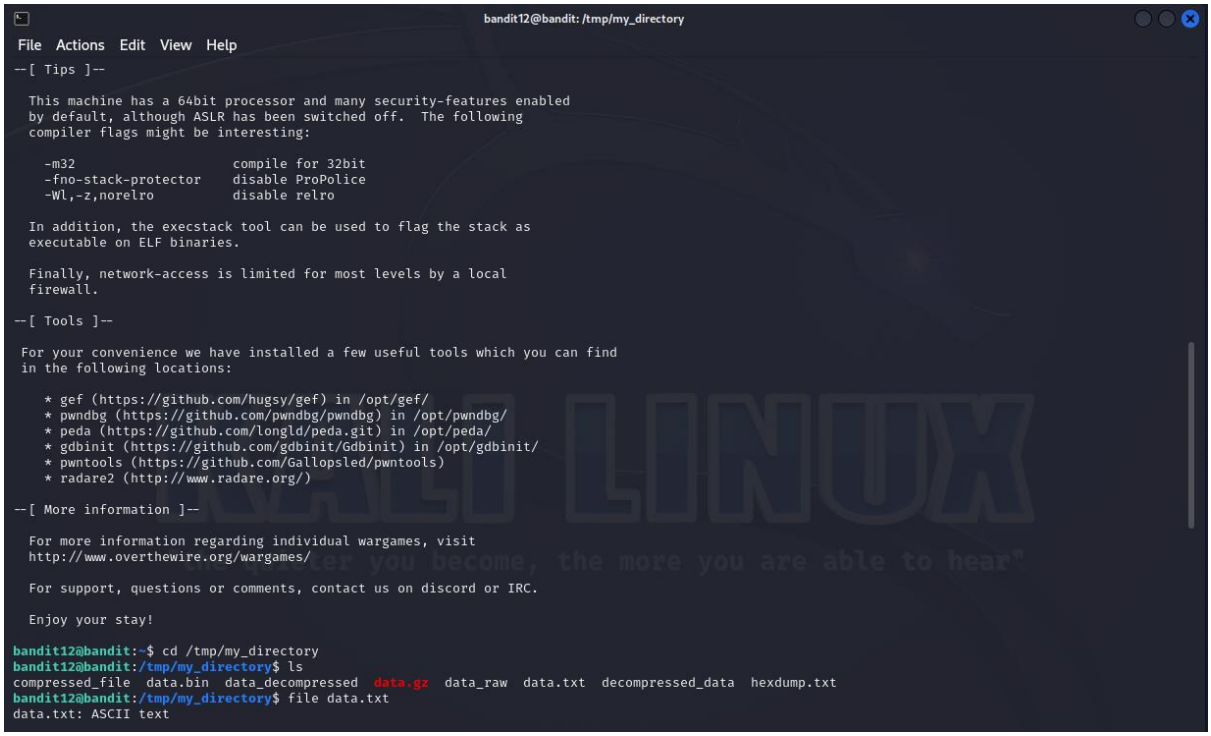
Bandit12 -> Bandit13



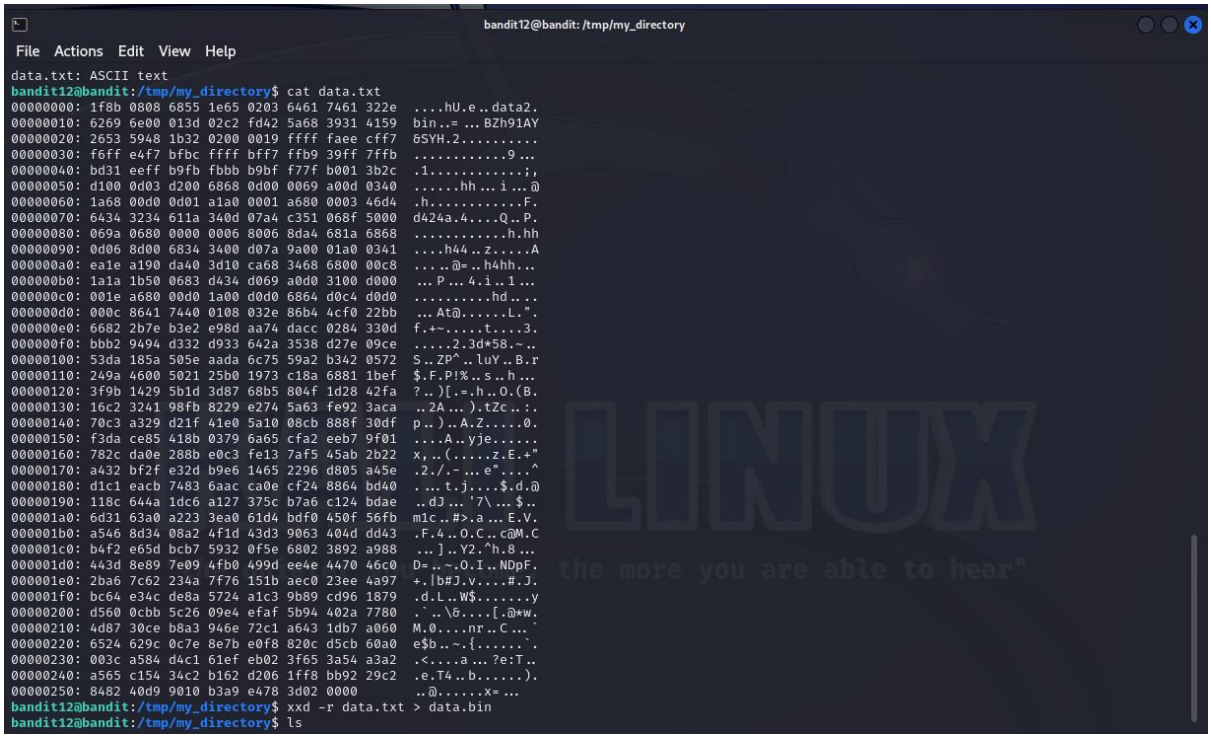
Log into Bandit12 using the password.



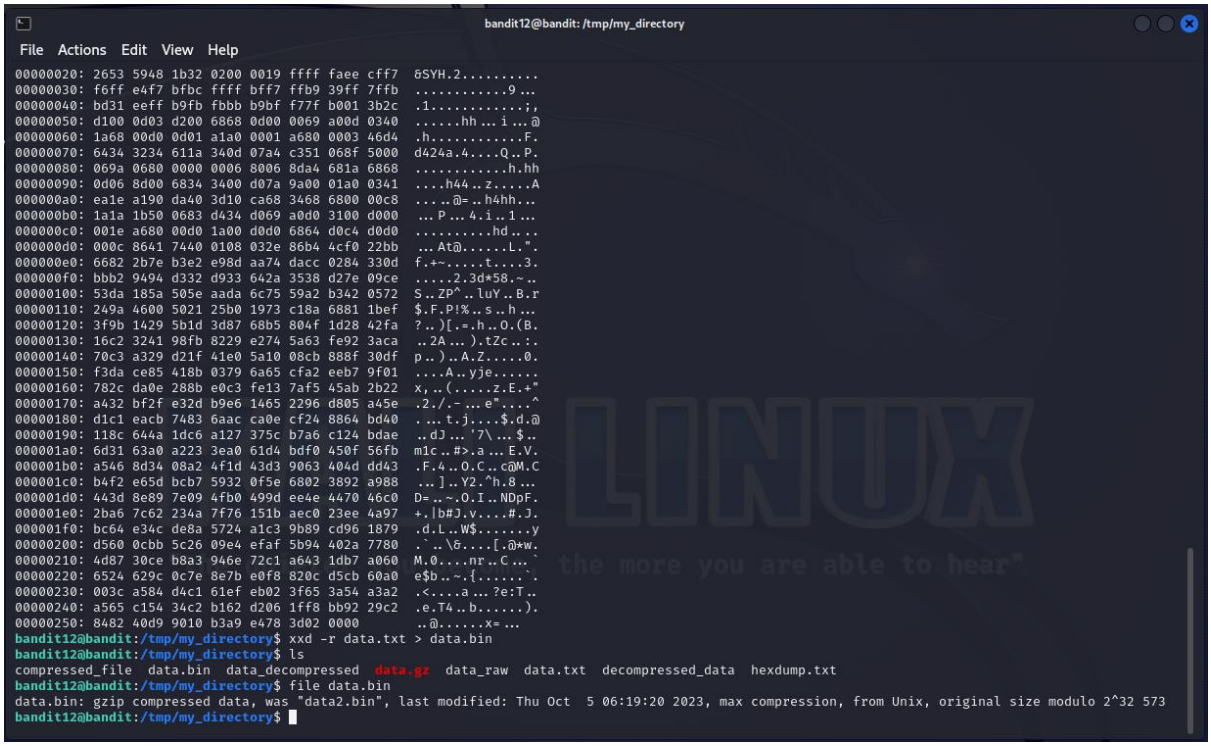
Type “ls” and find the list. Use the “data.txt” and find the file to know what the password is.



Run the “cat data.txt”

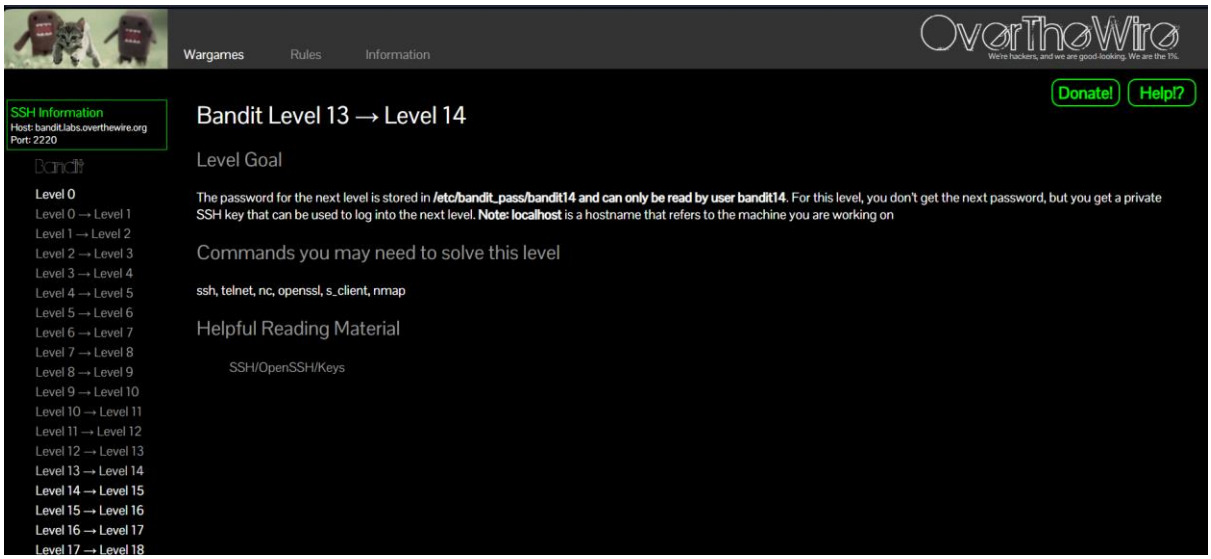


Run “xxd -r data.txt >data1.bin” and next run the “ls” to find all the files.

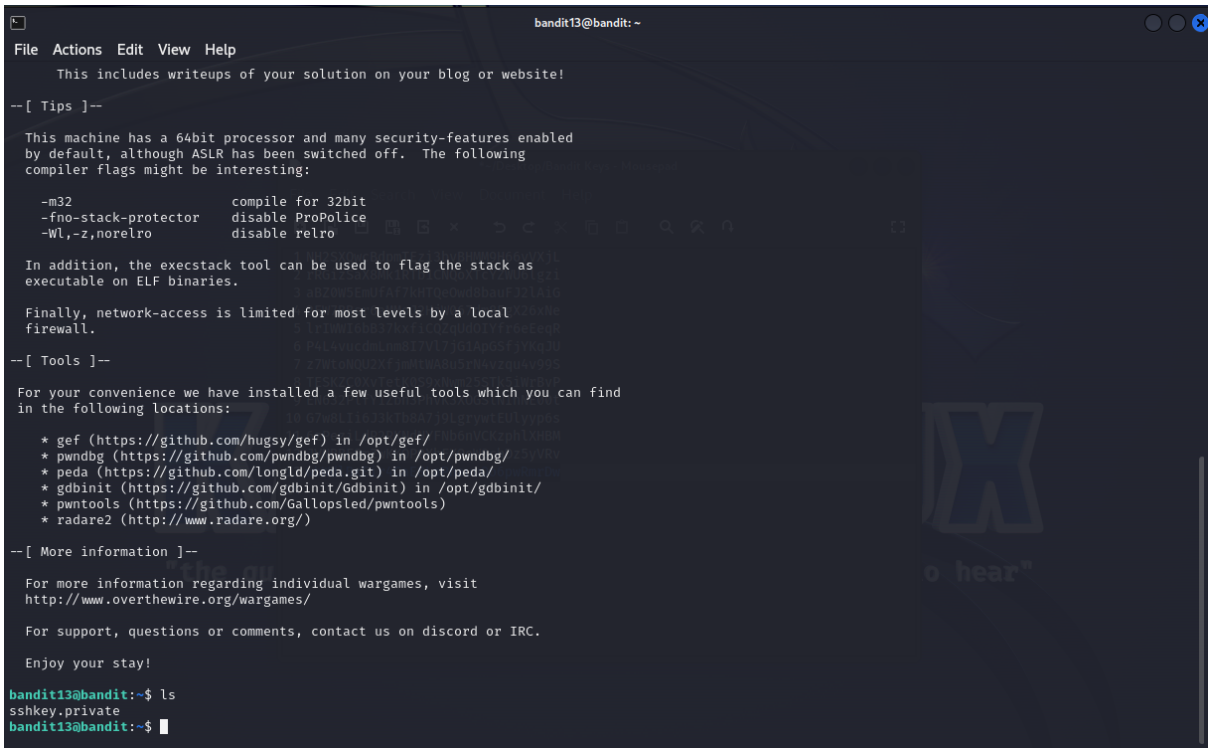


A command called “zcat” is included with “gzip” and is used to decompress “gzip” compressed files. Using the file command on myfile2, we can find bzip2 compressed data. Use that command to all 9 files and use the “tar” for archiving files and options. Finally, we can find the password.

Bandit13 -> Bandit14

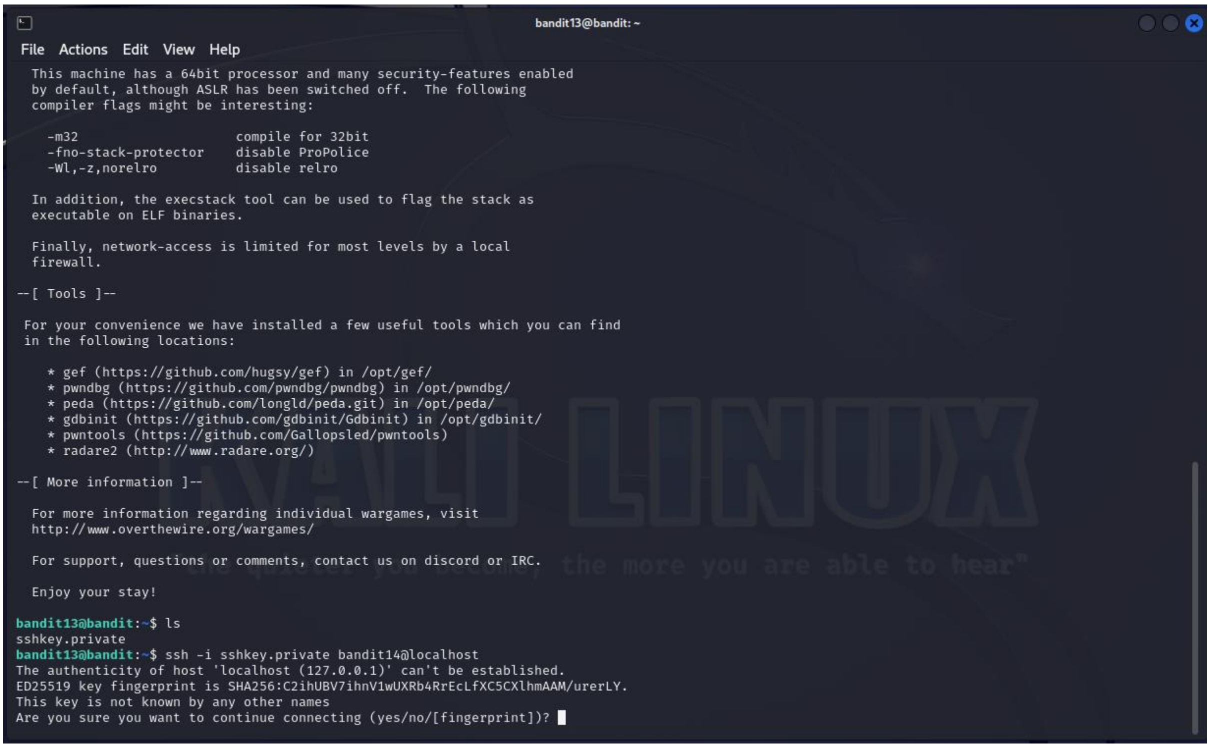


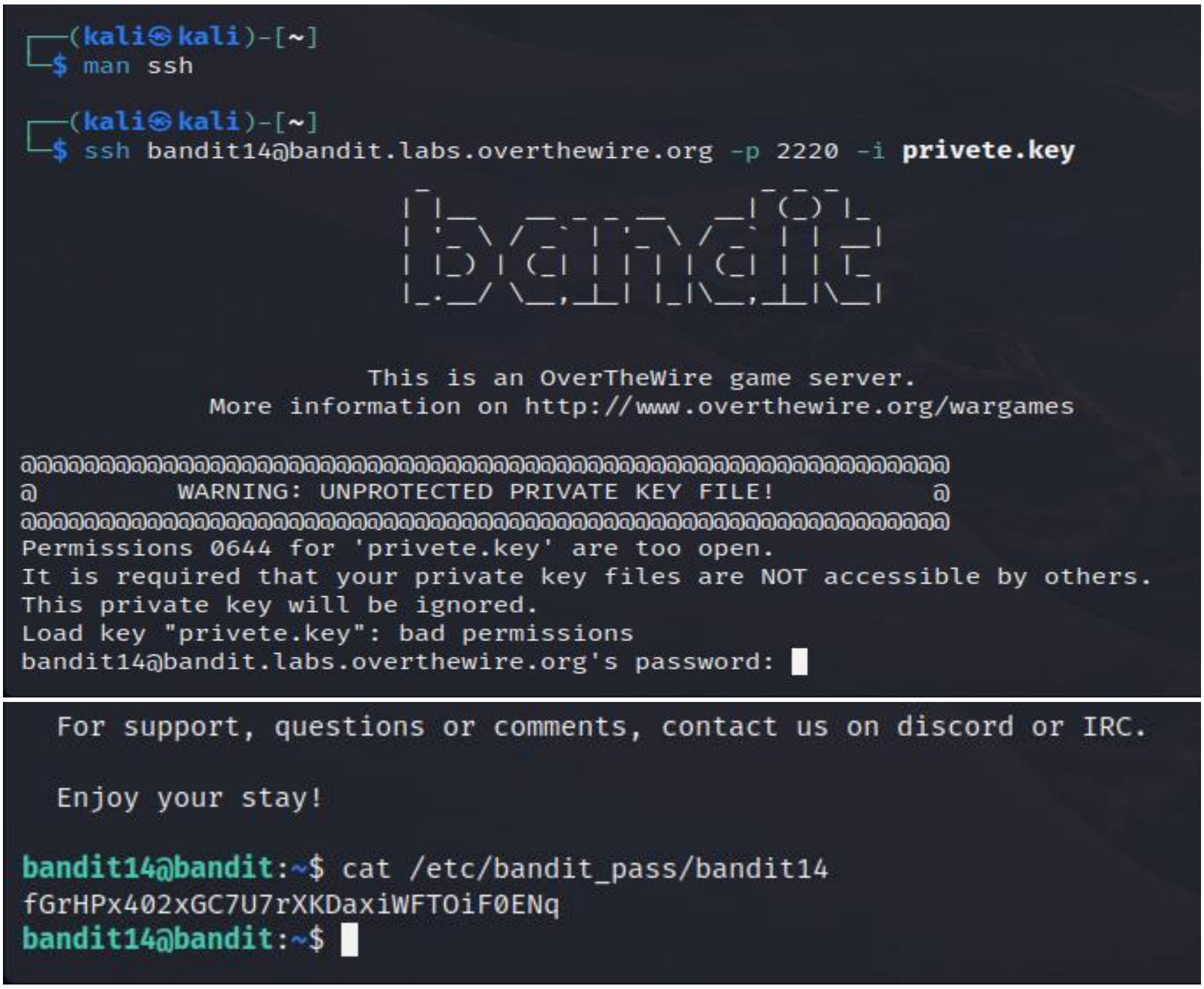
Use the “ls” command to find the file.



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

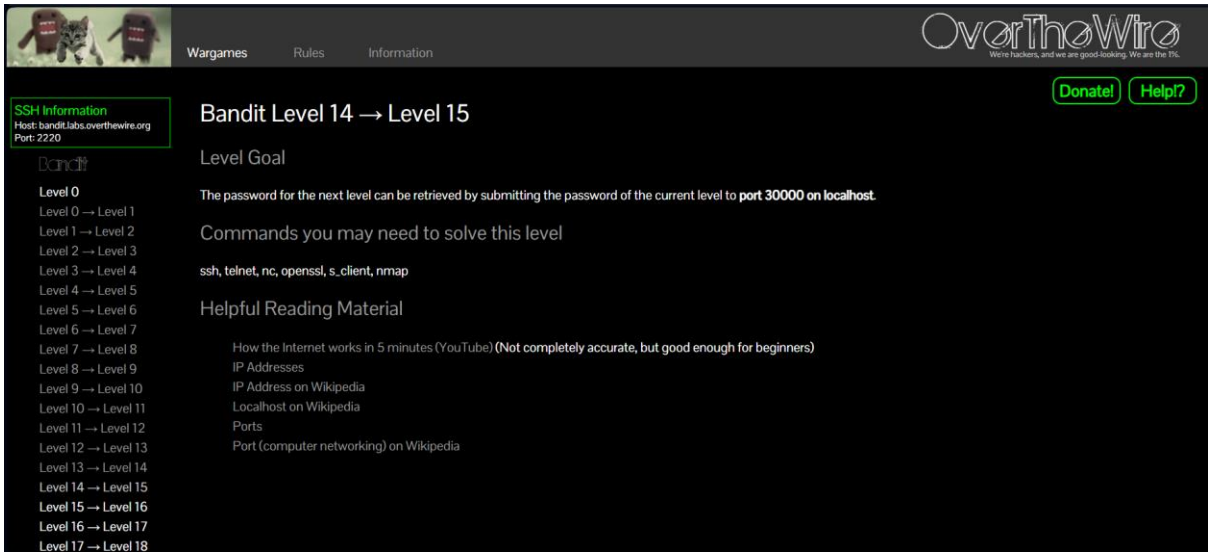
The “sshkey.private” file and the option “-i” are used to choose the identified file for RSA or DSA authentication.


bandit13@bandit: ~
File Actions Edit View Help
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
Finally, network-access is limited for most levels by a local
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?

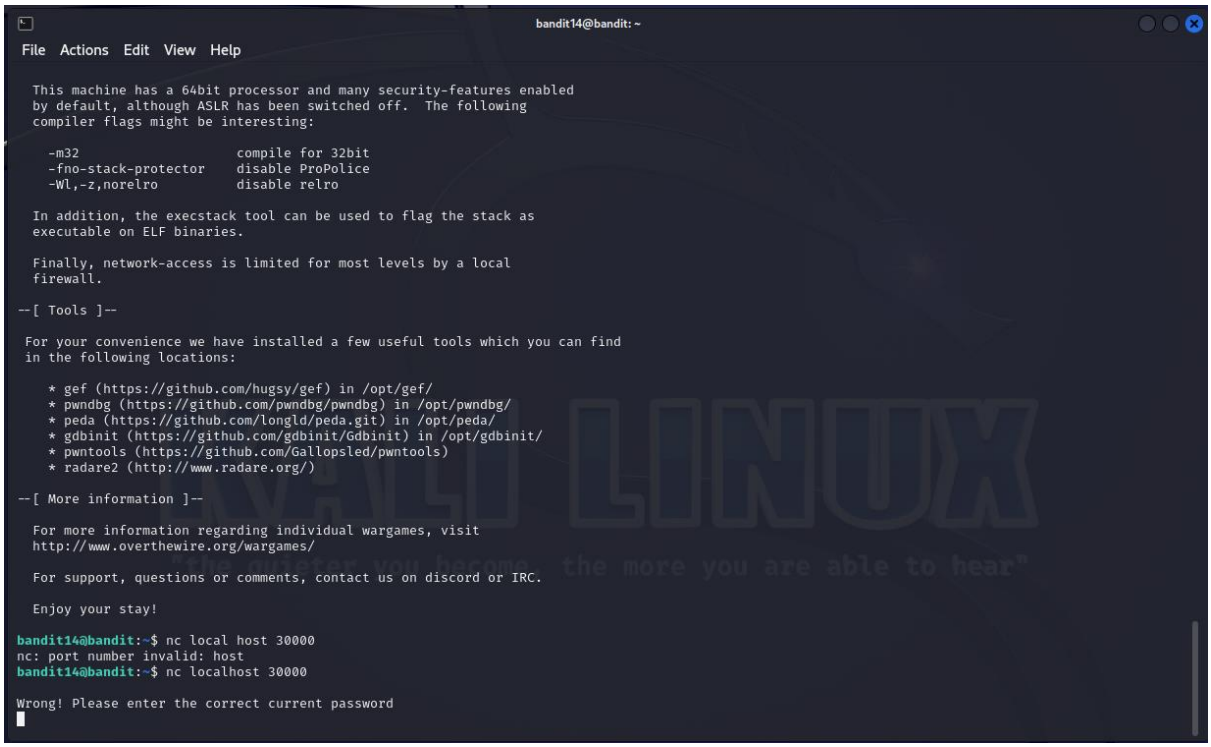

(kali㉿kali)-[~]
$ man ssh
(kali㉿kali)-[~]
$ ssh bandit14@bandit.labs.overthewire.org -p 2220 -i privete.key
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
@@@
@ WARNING: UNPROTECTED PRIVATE KEY FILE! @
@@@
Permissions 0644 for 'privete.key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "privete.key": bad permissions
bandit14@bandit.labs.overthewire.org's password:
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$

Bandit14 -> Bandit15

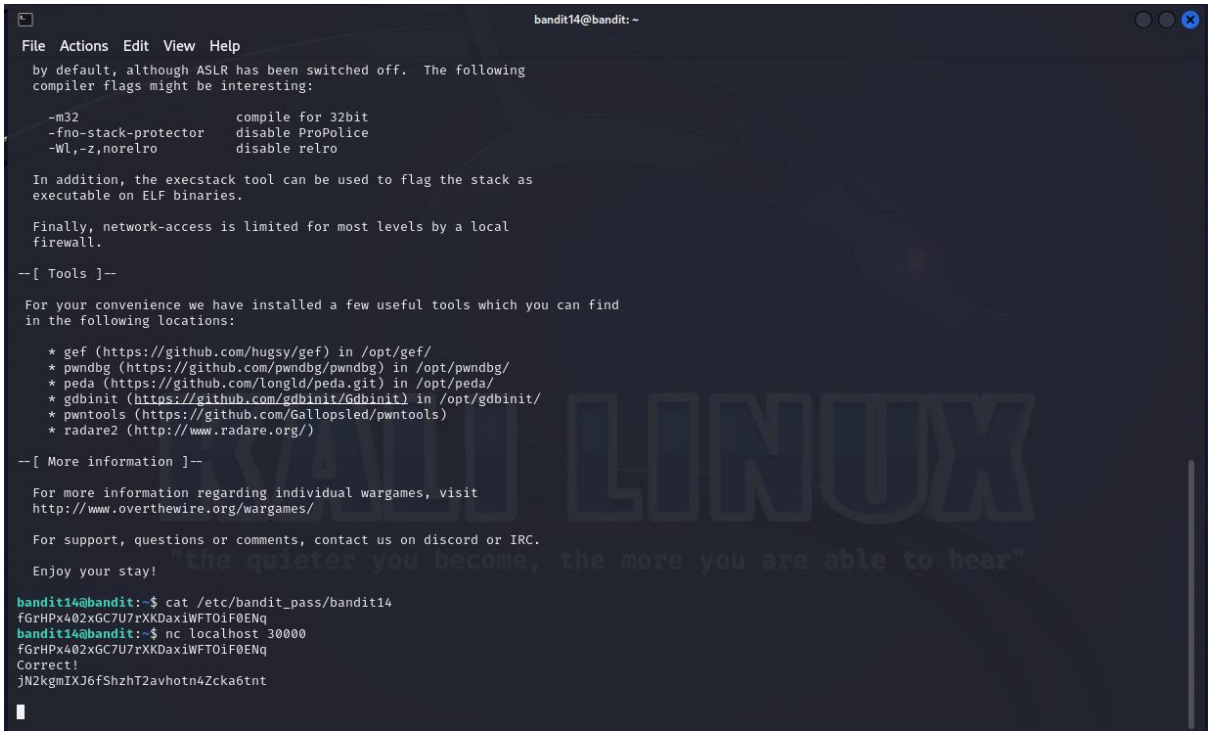
Log into Bandit14 first.



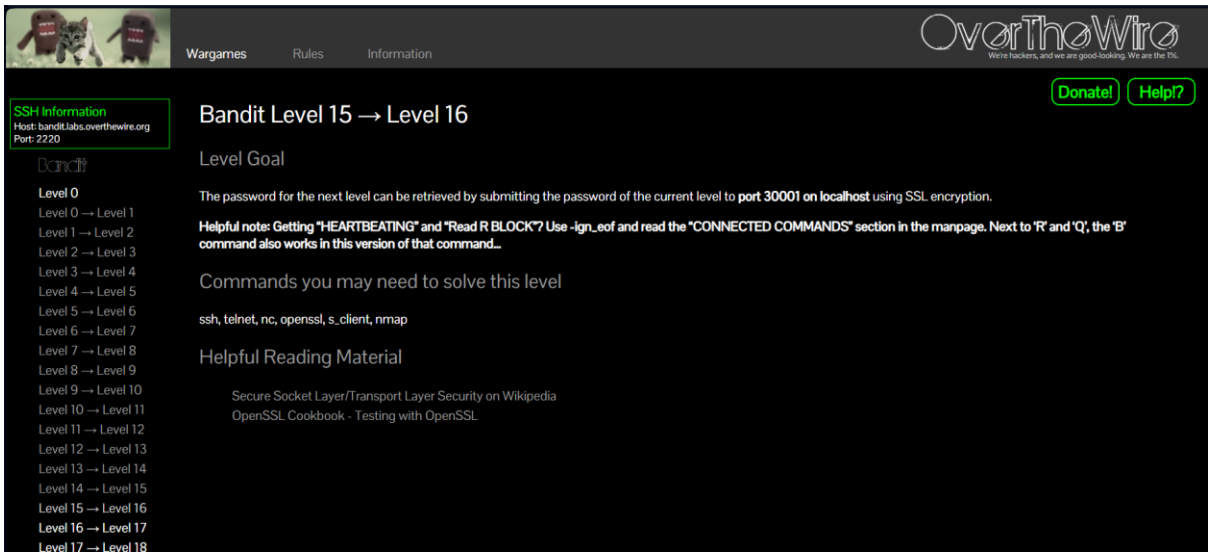
The command “nc” enables the reading and writing of data across a network connection. Both TCP and UDP connections are supported by it. Use that command and try to get the password. But they asked us for the password. So we need to find the password first.



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



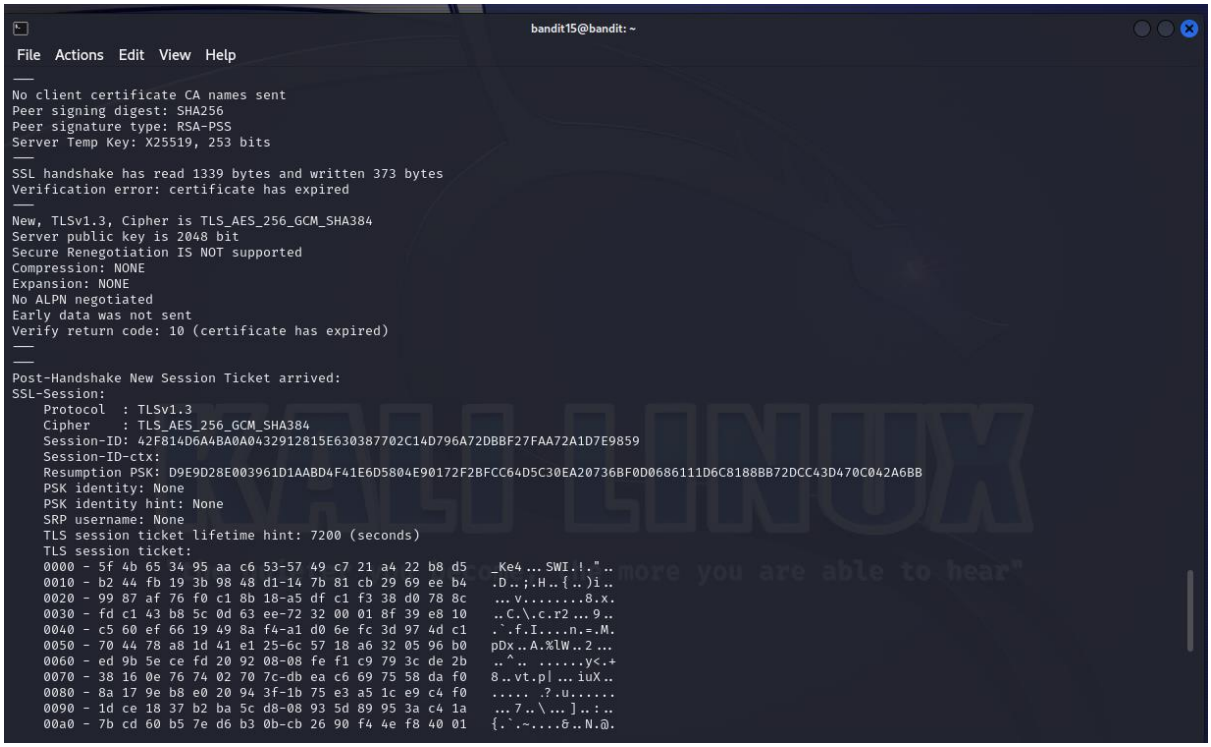
Bandit15 -> Bandit16



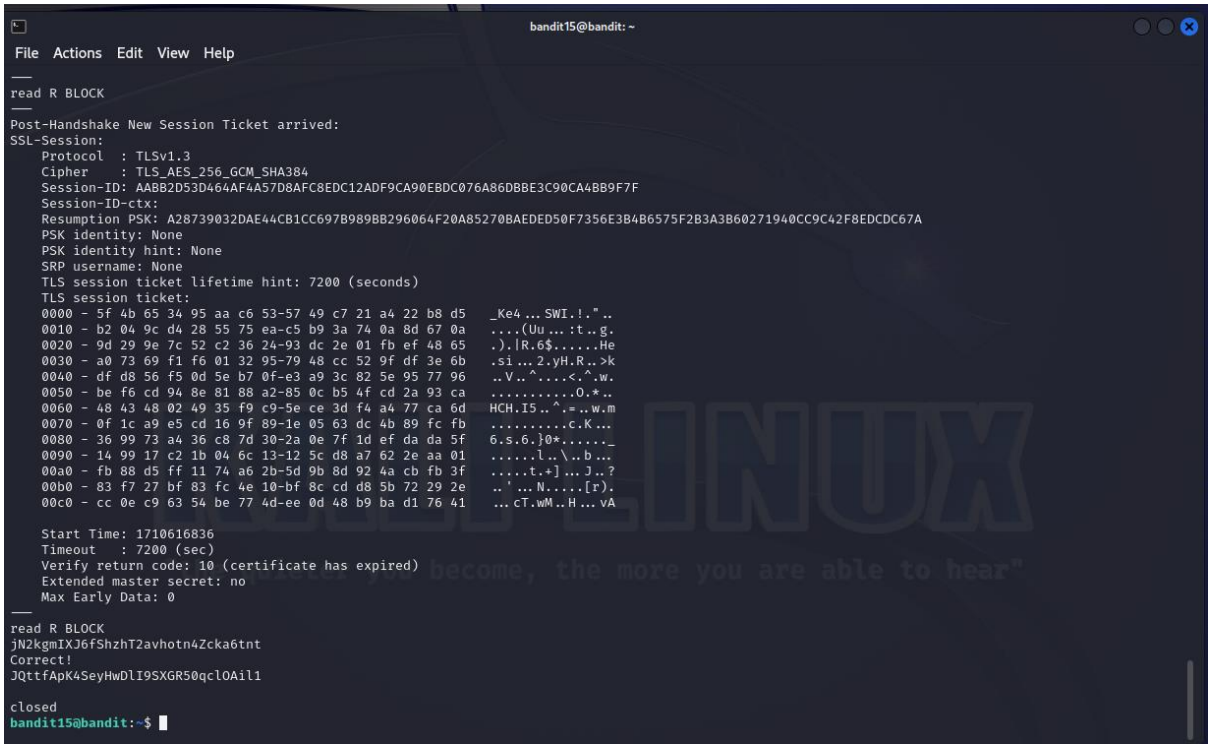
Openssl – library for secure communication over networks.

Openssl s_client – implementation of a basic SSl/TLS client that communication with a server.

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

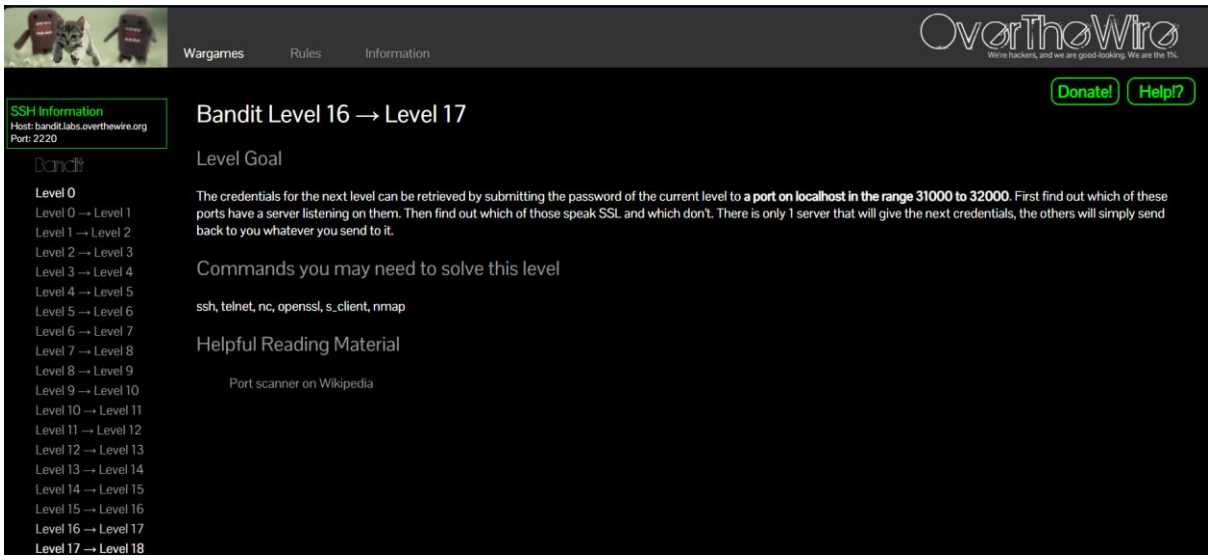


After run that we need to type the password of bandit 15. When we type it shows the Bandit16 password.

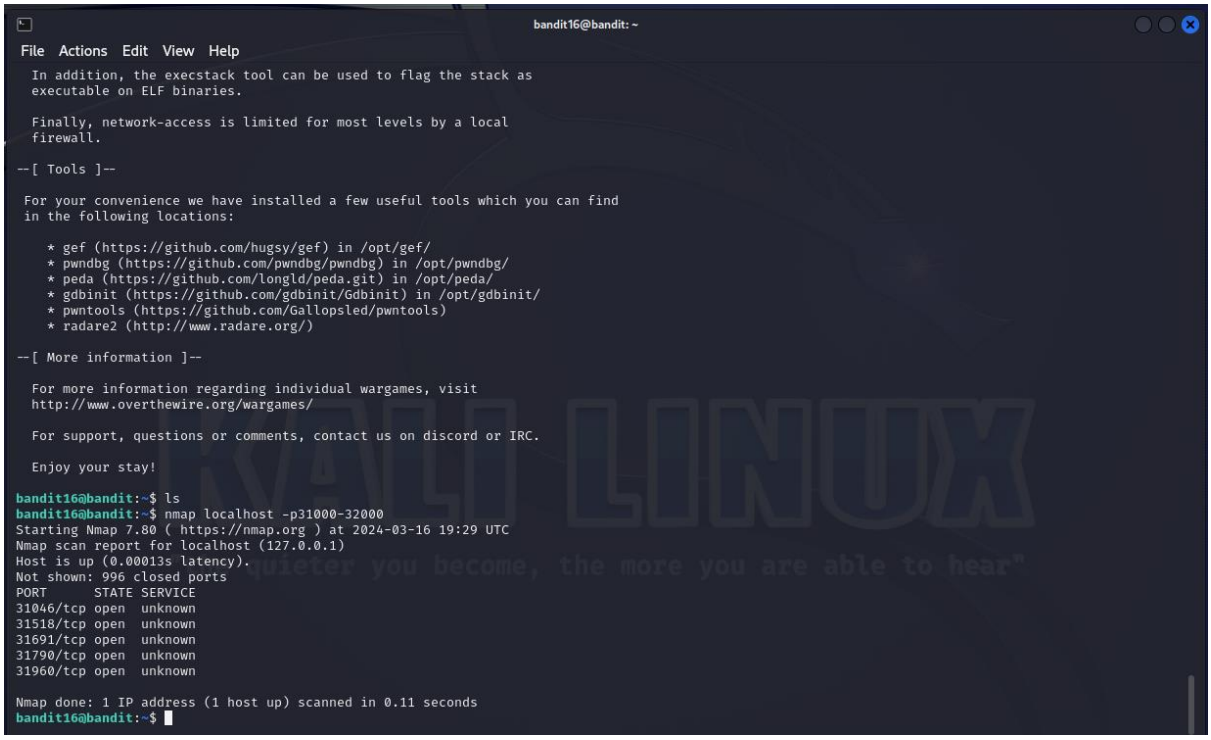


Bandit16 -> Bandit17

Login into the bandit 16.

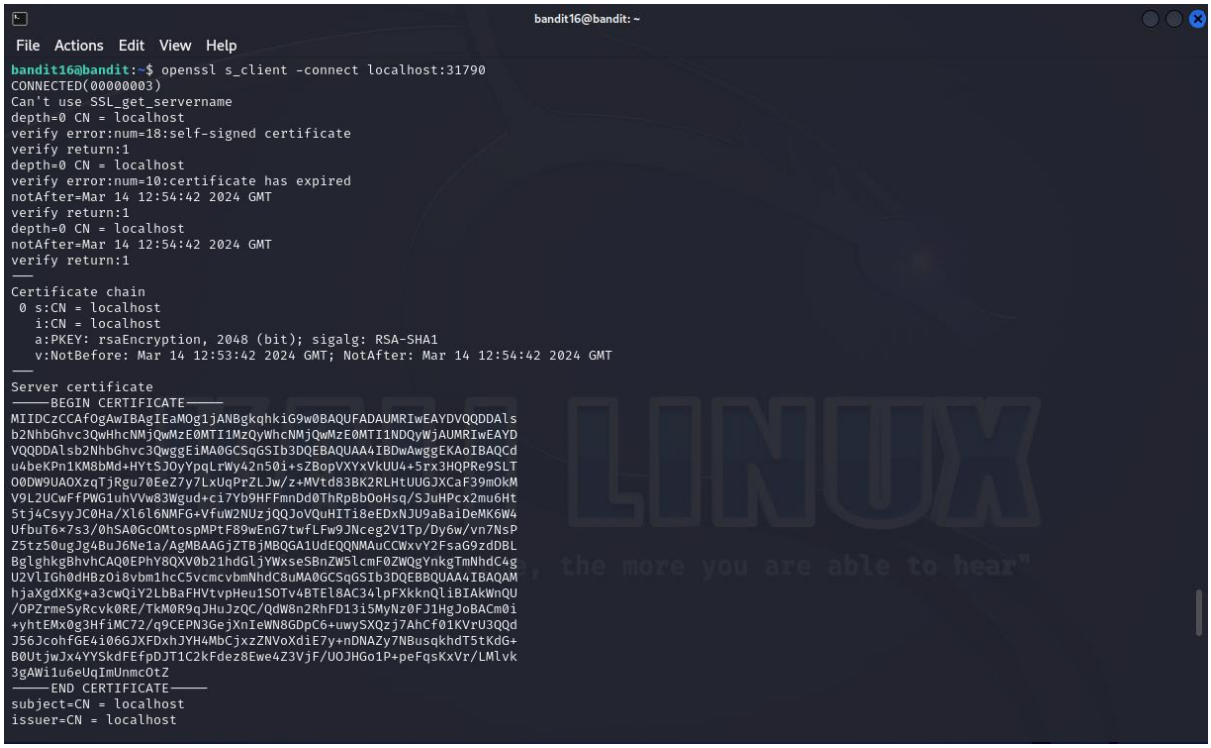


Run “nmap localhost -p31000-32000” to check what services are running on them.



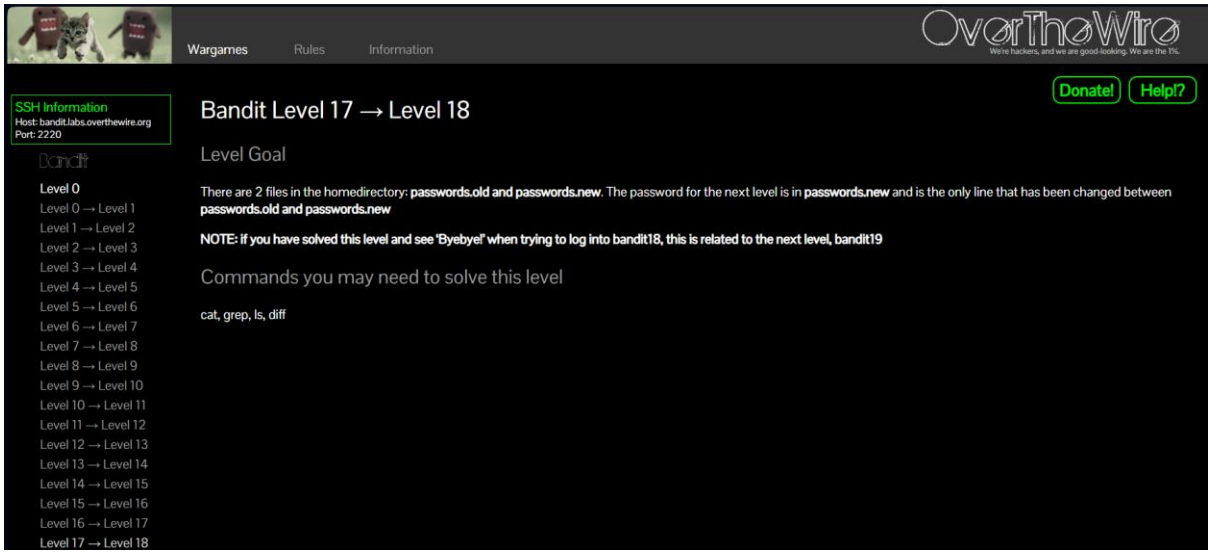
The port that shows promise appears to be 31790, which is used by an unidentified service.

Use “Openssl” and connect to this port on localhost.



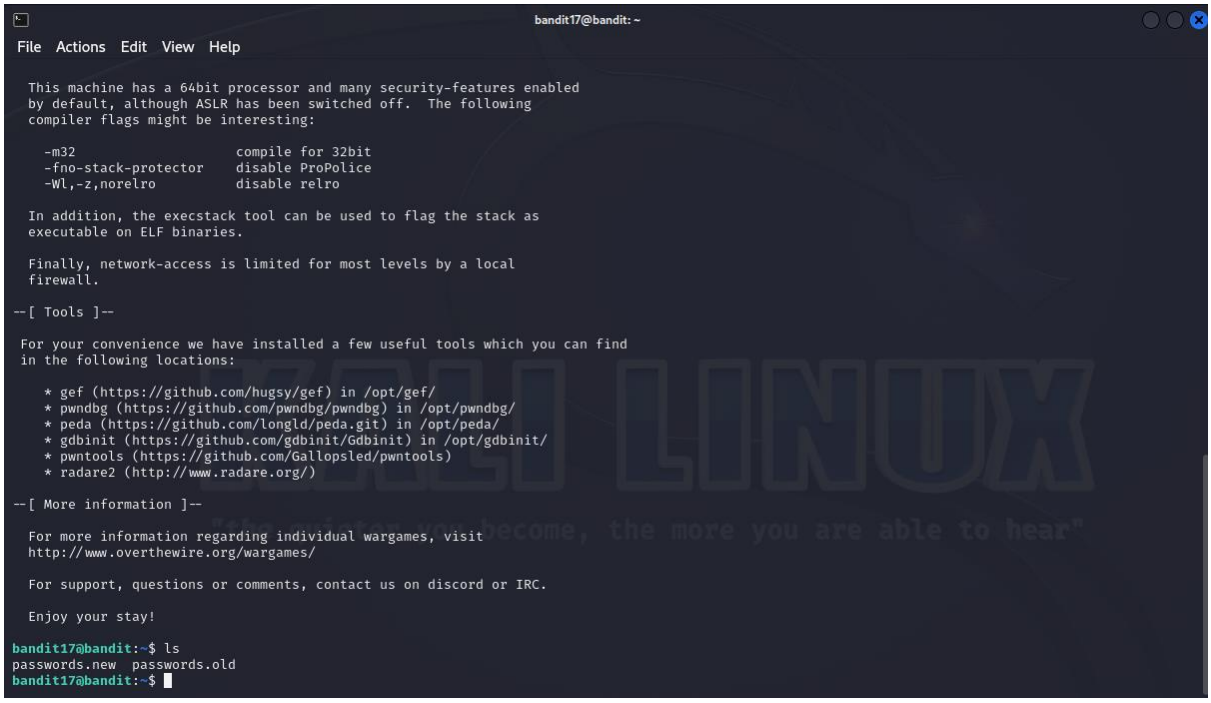
Save this key locally. Use a ssh private key. “ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220”.

Bandit17 -> Bandit18

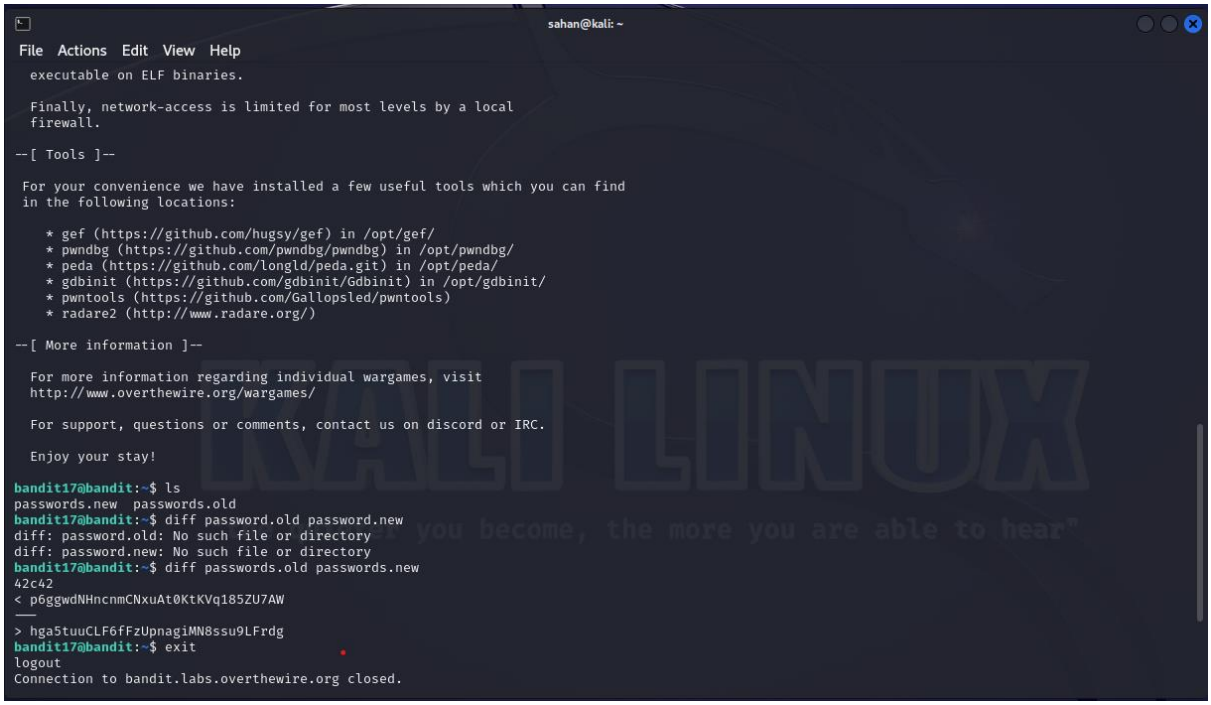


diff – program compares files line by line.

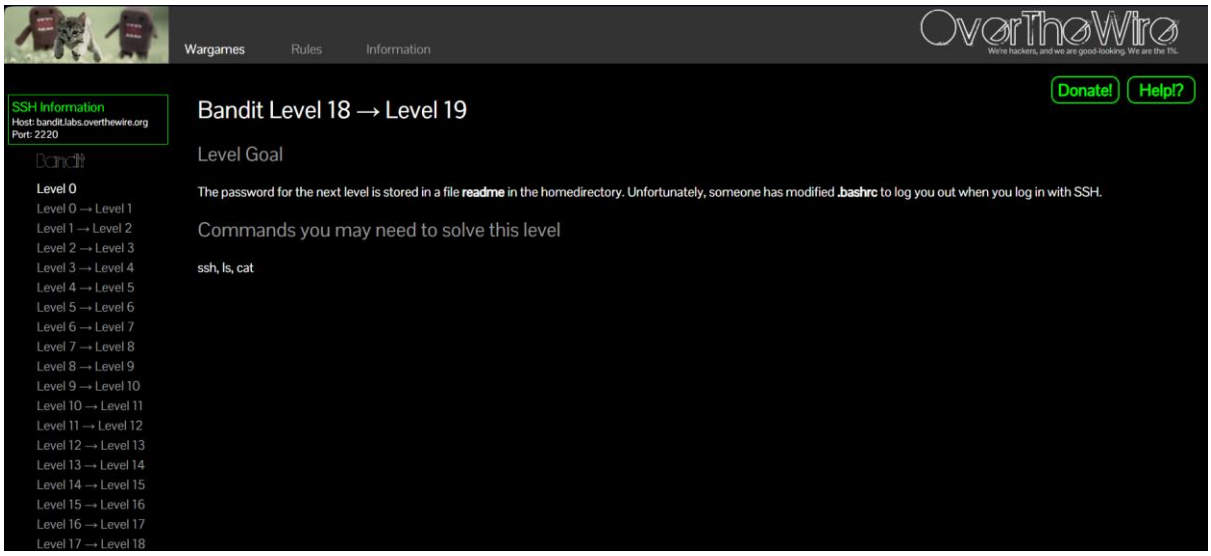
Run the ls command and get the file name.



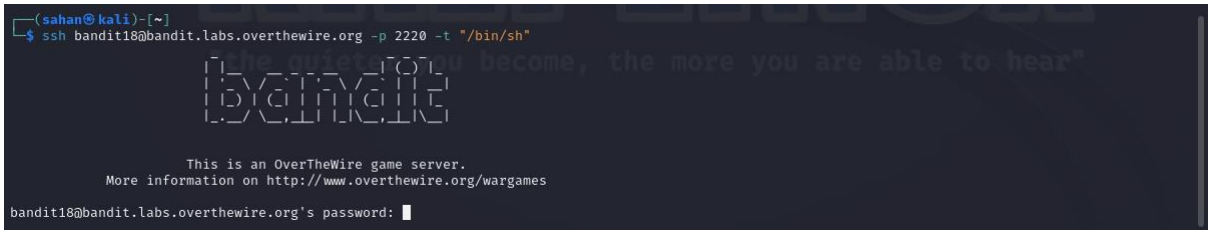
Now run the “diff passwords.old passwords.new” to get different passwords called old and new.



Bandit18 -> Bandit19

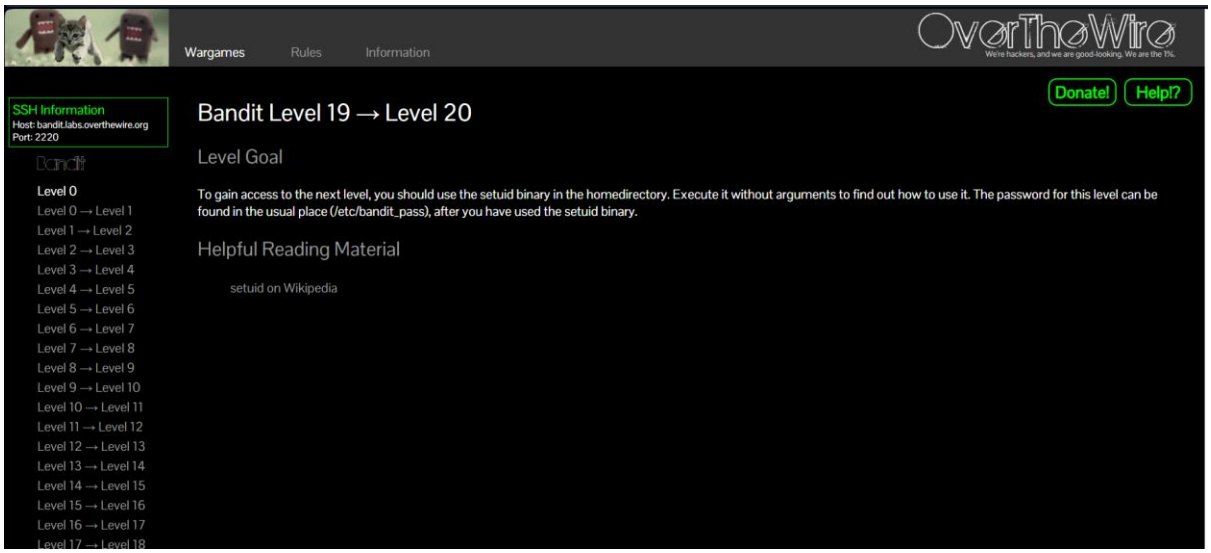


We can try using SSH to log in with them. The terminal window to be used to log into the system is specified using the "-t" flag of the SSH command.

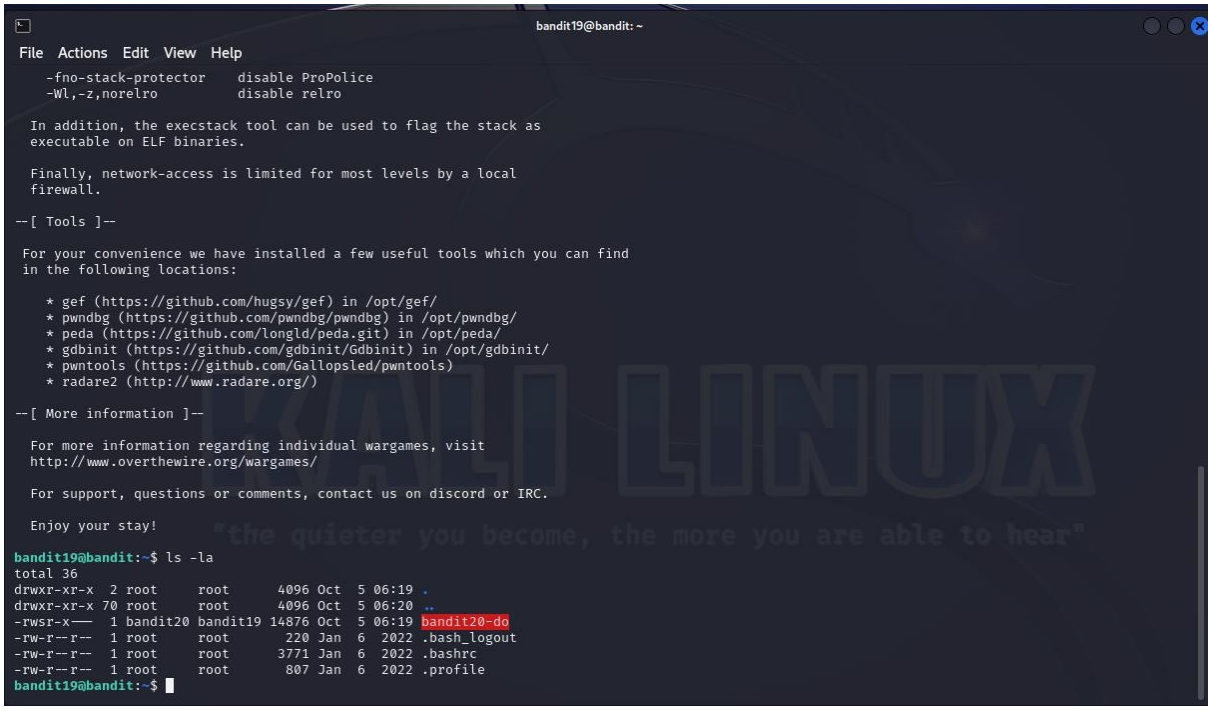


Run the “ls” command and then run the “cat readme” command. When we run those commands wen can find the flag.

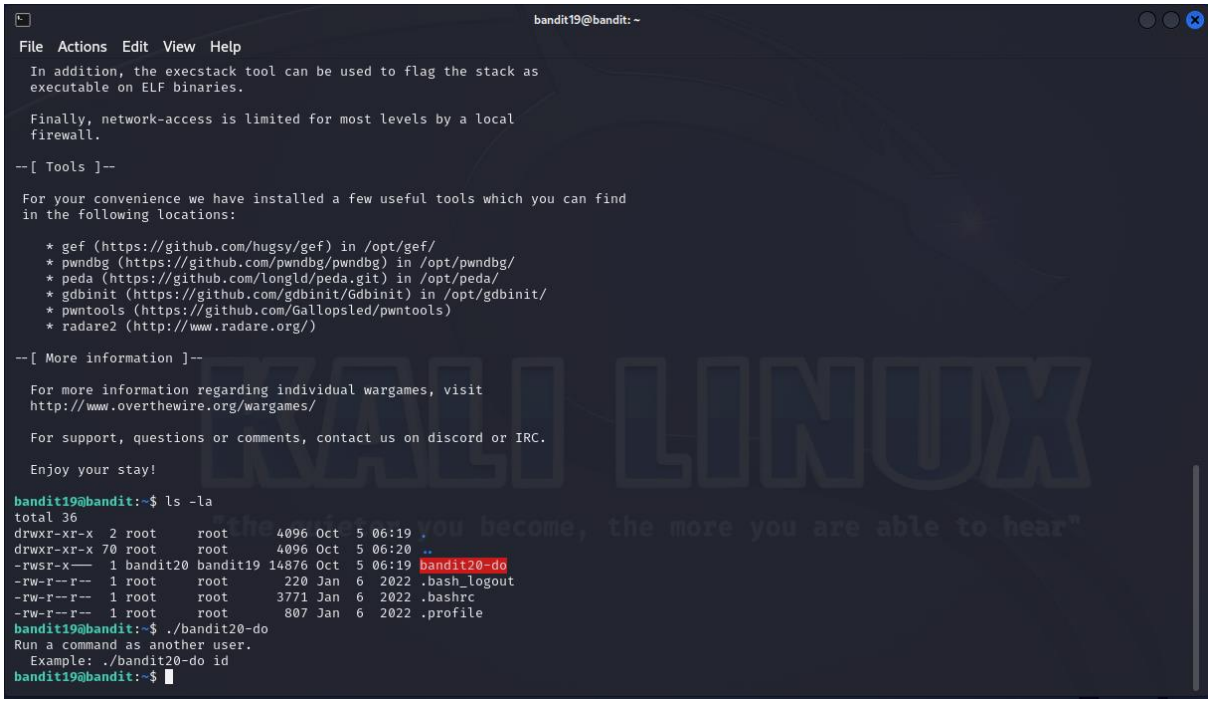
Bandit19 -> Bandit20

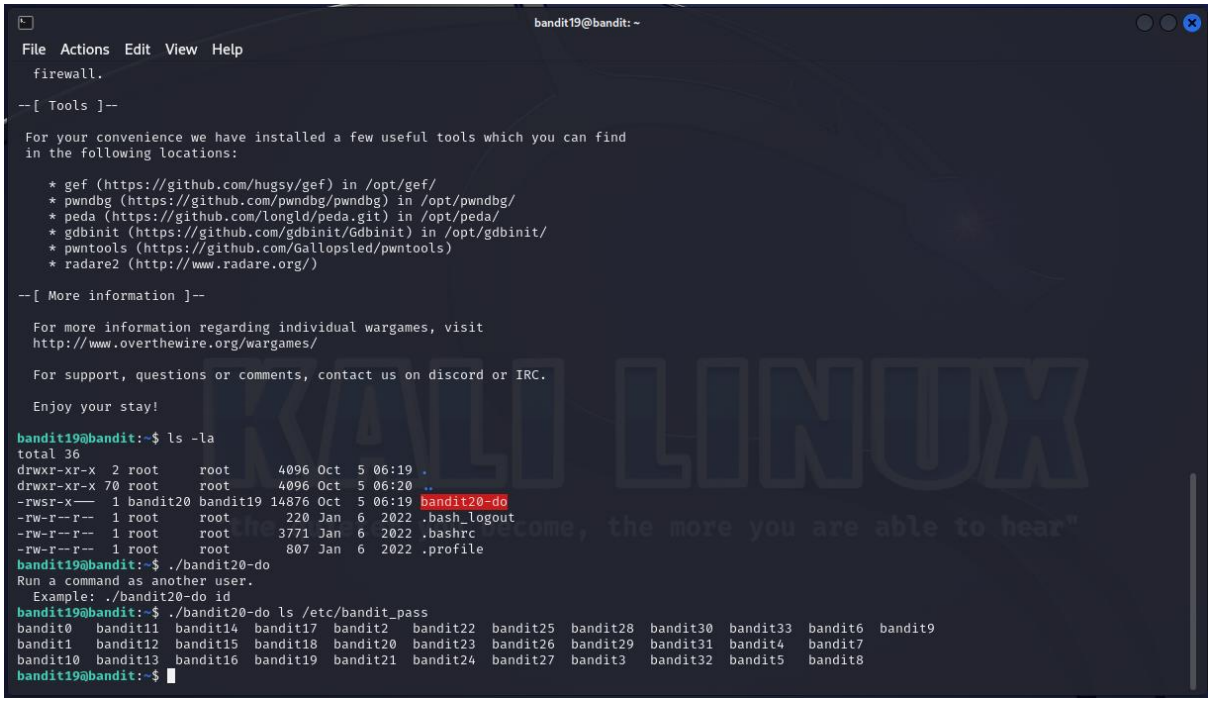


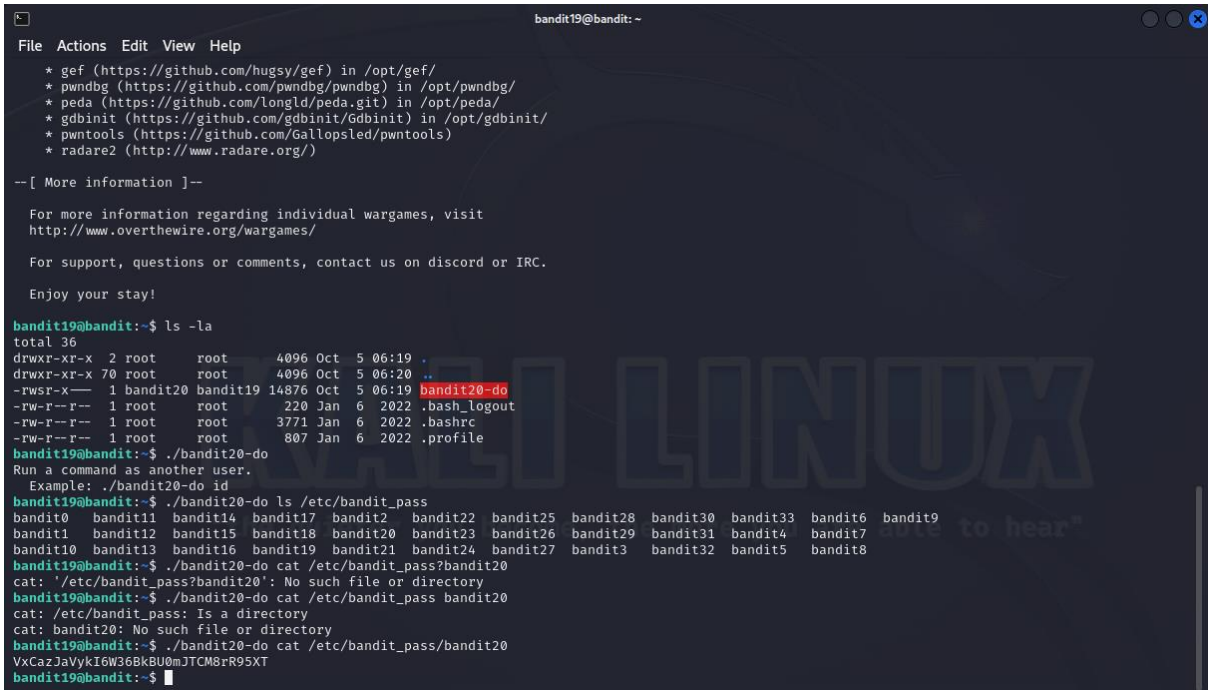
Log into Bandit19 and first we need to check the owner of the setuid binary.



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




bandit19@bandit: ~
File Actions Edit View Help
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-rwsr-x--- 1 bandit20 bandit19 14876 Oct 5 06:19 bandit20-do
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit0 bandit11 bandit14 bandit17 bandit2 bandit22 bandit25 bandit28 bandit30 bandit33 bandit6 bandit9
bandit1 bandit12 bandit15 bandit18 bandit20 bandit23 bandit26 bandit29 bandit31 bandit4 bandit7
bandit10 bandit13 bandit16 bandit19 bandit21 bandit24 bandit27 bandit3 bandit32 bandit5 bandit8
bandit19@bandit:~$


bandit19@bandit: ~
File Actions Edit View Help
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-rwsr-x--- 1 bandit20 bandit19 14876 Oct 5 06:19 bandit20-do
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit0 bandit11 bandit14 bandit17 bandit2 bandit22 bandit25 bandit28 bandit30 bandit33 bandit6 bandit9
bandit1 bandit12 bandit15 bandit18 bandit20 bandit23 bandit26 bandit29 bandit31 bandit4 bandit7
bandit10 bandit13 bandit16 bandit19 bandit21 bandit24 bandit27 bandit3 bandit32 bandit5 bandit8
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass?bandit20
cat: '/etc/bandit_pass?bandit20': No such file or directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass bandit20
cat: /etc/bandit_pass: Is a directory
cat: bandit20: No such file or directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$

All Level Passwords

Level 00 password = bandit0

Level 01 password = NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Level 02 password = rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Level 03 password = aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Level 04 password = 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Level 05 password = lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Level 06 password = P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 07 password = z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 08 password = TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 09 password = EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 10 password = G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 11 password = 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Level 12 password = JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Level 13 password = wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 14 password = fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Level 15 password = jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 16 password = JQttfApK4SeyHwDlI9SXGR50qclOAil1

Level 17 password = VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

Level 18 password = hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

Level 19 password = awhqfNnAbc1naukrpqDYcF95h7HoMTrC

Level 20 password = VxCazJaVykI6W36BkBU0mJTCM8rR95XT

Conclusion

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

References

1) Medium –

•https://david-varghese.medium.com/overthewire-bandit-level-16-level-17c137701b3af1

•https://medium.com/@theGirlWhoEncrypts/overthewire-bandit-level-12-level-13-e5b687760d15

2) YouTube –

•https://www.youtube.com/watch?v=hvSFPyqLizw

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

3) OverTheWire –

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

IT22083678
SAHAN H P T