BSc (Hons) in Information Technology – Year 2

IE2012 – Systems and Network Programming (C/Python) Semester 1, 2023

BANDIT

IT NUMBER: IT22345332

NAME: G.P DINUJAYA THAMARA

WEEKEND BATCH

MALABE CAMPUS

What is Bandit?

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the side menu on the left of webpage.

In this report it contains walkthrough from Level 0 to Level 20

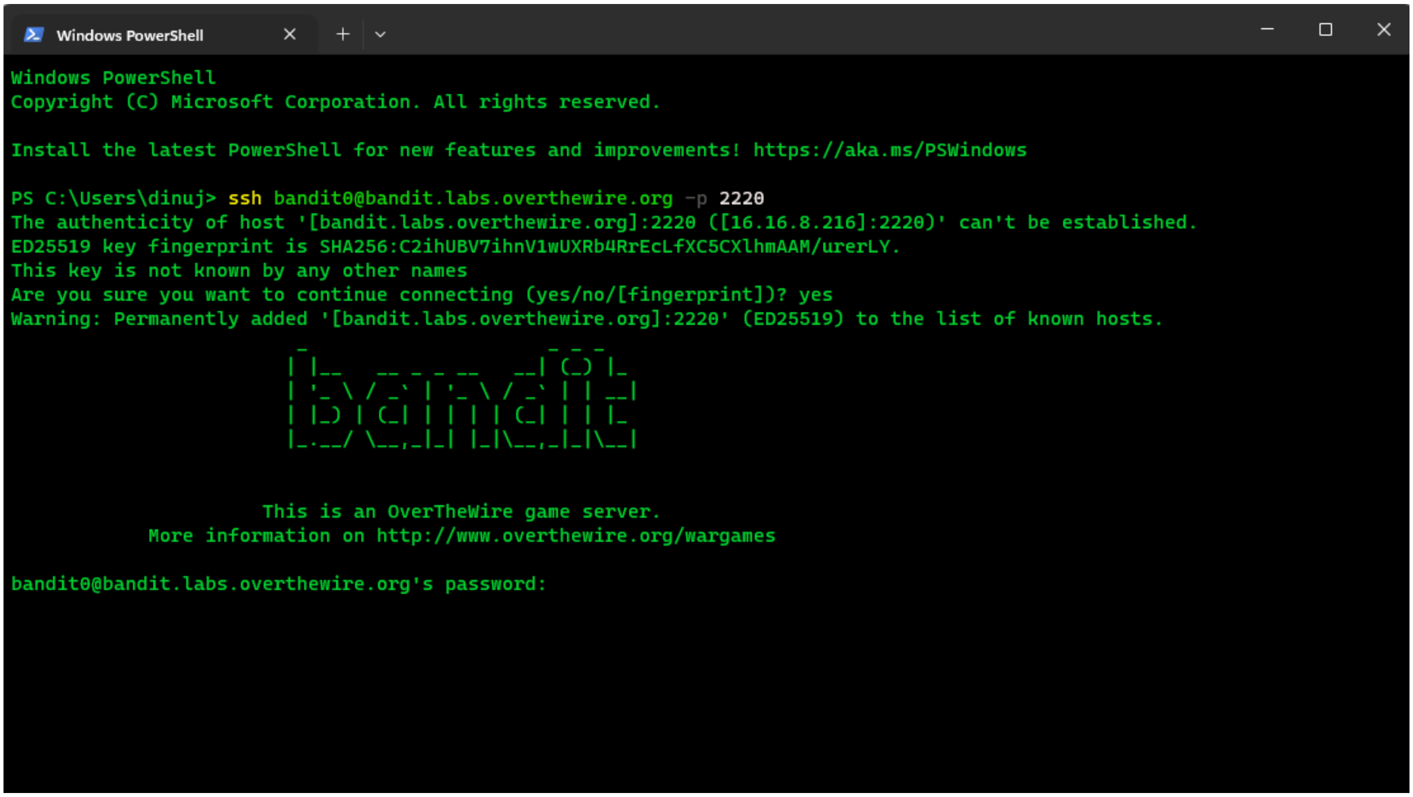
Level0
Level0→Level1
Level1→ Level2
Level2→ Level3
Level3→ Level4
Level4→ Level5
Level5→ Level6
Level6→ Level7
Level7→ Level8
Level8→ Level9
Level9→ Level10
Level10→ Level11
Level11→ Level12
Level12→ Level13
Level13→ Level14
Level14→ Level15
Level15→ Level16
Level16→ Level17
Level17→ Level18
Level18→ Level19
Level19→ Level20

Level 0

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the [Level 1]() page to find out how to beat Level 1**.**

Commands you may need to solve this level.

SSH - it's important to encrypt your connection so your passwords and other data remain secure. An easy way to do this is to install an SSH client on your computer and use that to make a command-line connection.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\dinuj> ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([16.16.8.216]:2220)' 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])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

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

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

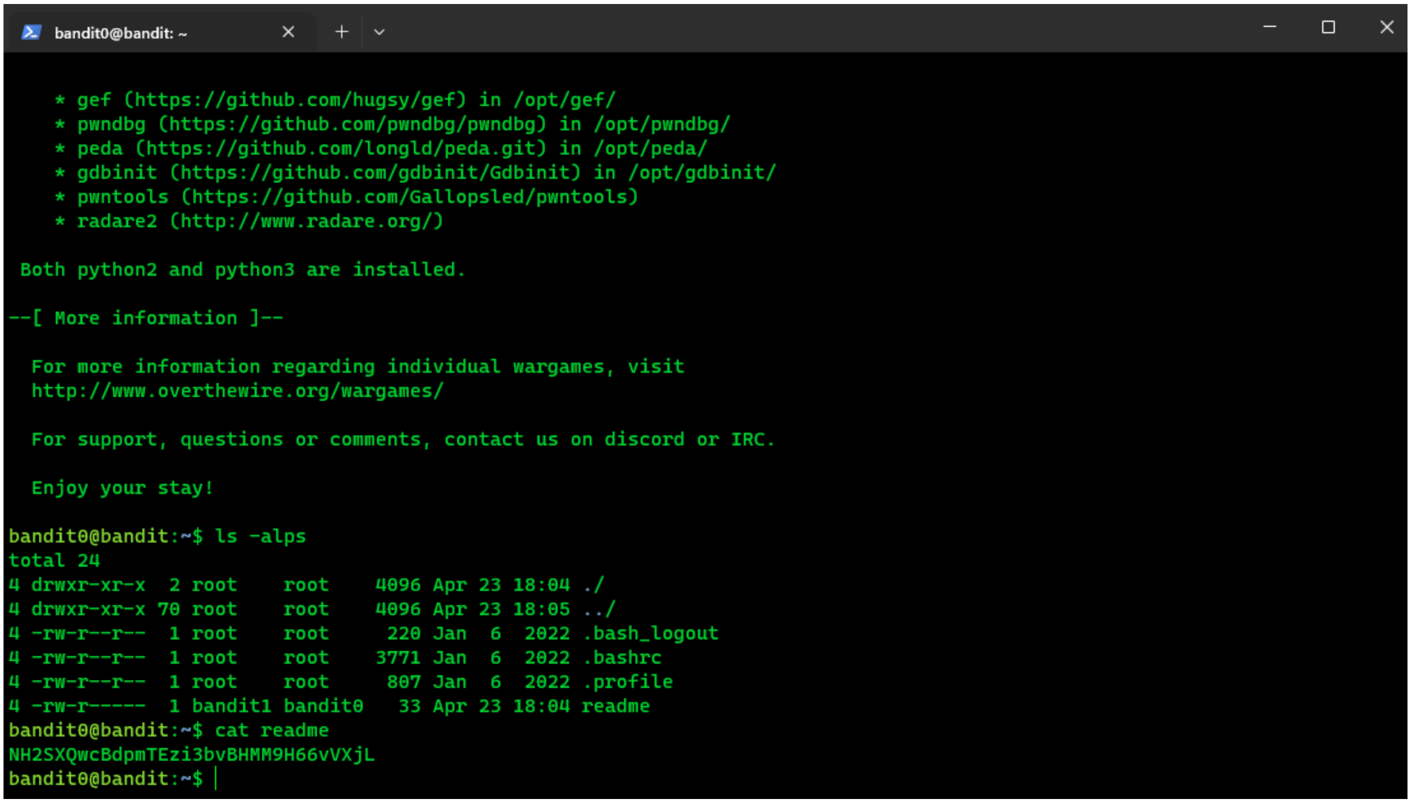
-p defines the port number

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



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

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit1 bandit0   33 Apr 23 18:04 readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ |
```

ls- alps

- "**ls**": This stands for "list." It's a command that's used to show the files and folders in a directory.
- "**-alps**": These are options you can add to the "ls" command to customize how the list is displayed:

- "**-a**": This option means "all." It shows hidden files and folders that start with a dot (.), which are normally not shown.
- "**-l**": This option means "long." It provides more detailed information about each file or folder, such as permissions, size, and modification date.
- "**-p**": This option adds a slash (/) to the end of directory names to make it clear that they're folders.
- "**-s**": This option shows the size of each file in blocks.

Cat

This command is used in a computer's command line to display the contents of a file.

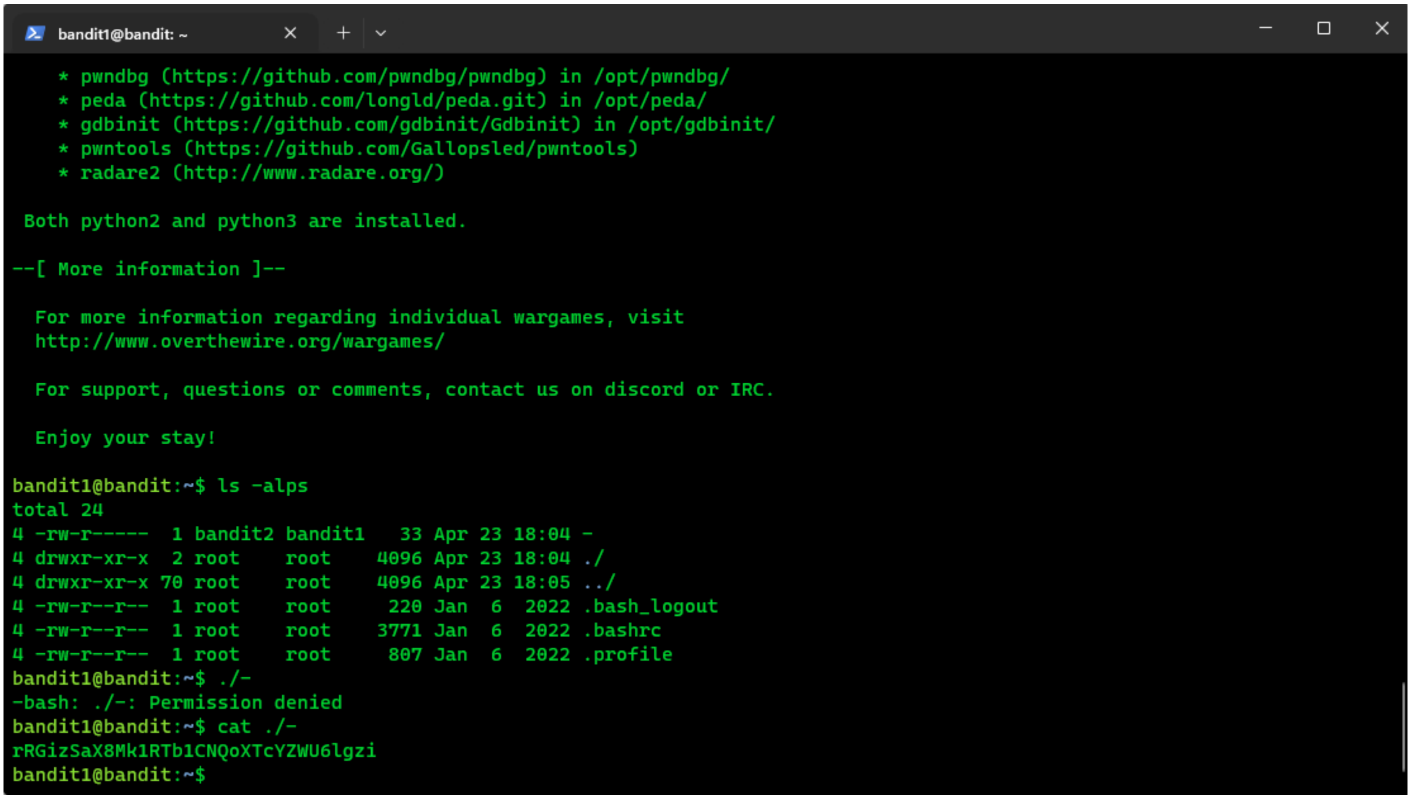
Level 1→Level 2

Level Goal

The password for the next level is stored in a **file called -** located in the home directory.

Commands you may need to solve this level.

ls, cd , cat , file , du , find



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

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit1@bandit:~$ ls -alps
total 24
4 -rw-r-----  1 bandit2 bandit1   33 Apr 23 18:04 -
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit1@bandit:~$ ./-
-bash: ./-: Permission denied
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

When access directories with special names these can be used

Use the Full Path: **cd ./-**

Use Quotes: **cd "-"**

Use Escape Characters: **cd \-**

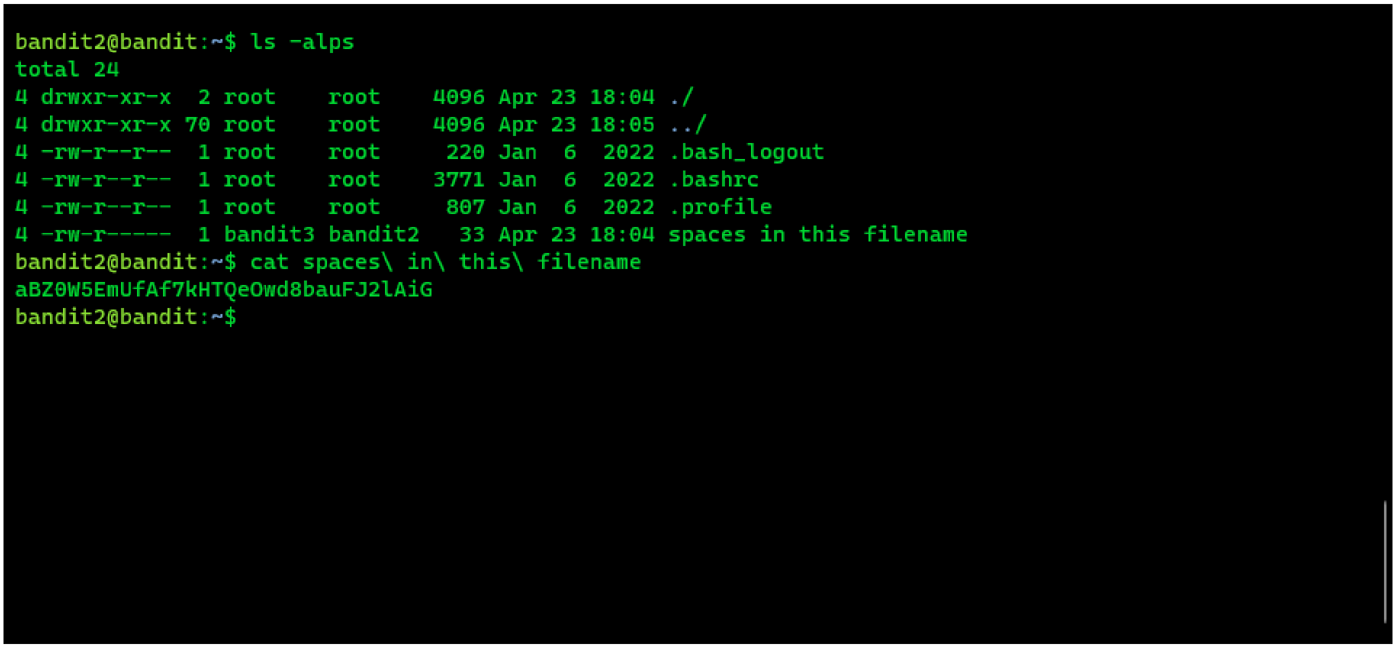
Level 2→Level 3

Level Goal

The password for the next level is stored in a file called spaces in this filename located in the home directory.

Commands you may need to solve this level.

ls, cd , cat , file , du , find



```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit3 bandit2   33 Apr 23 18:04 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

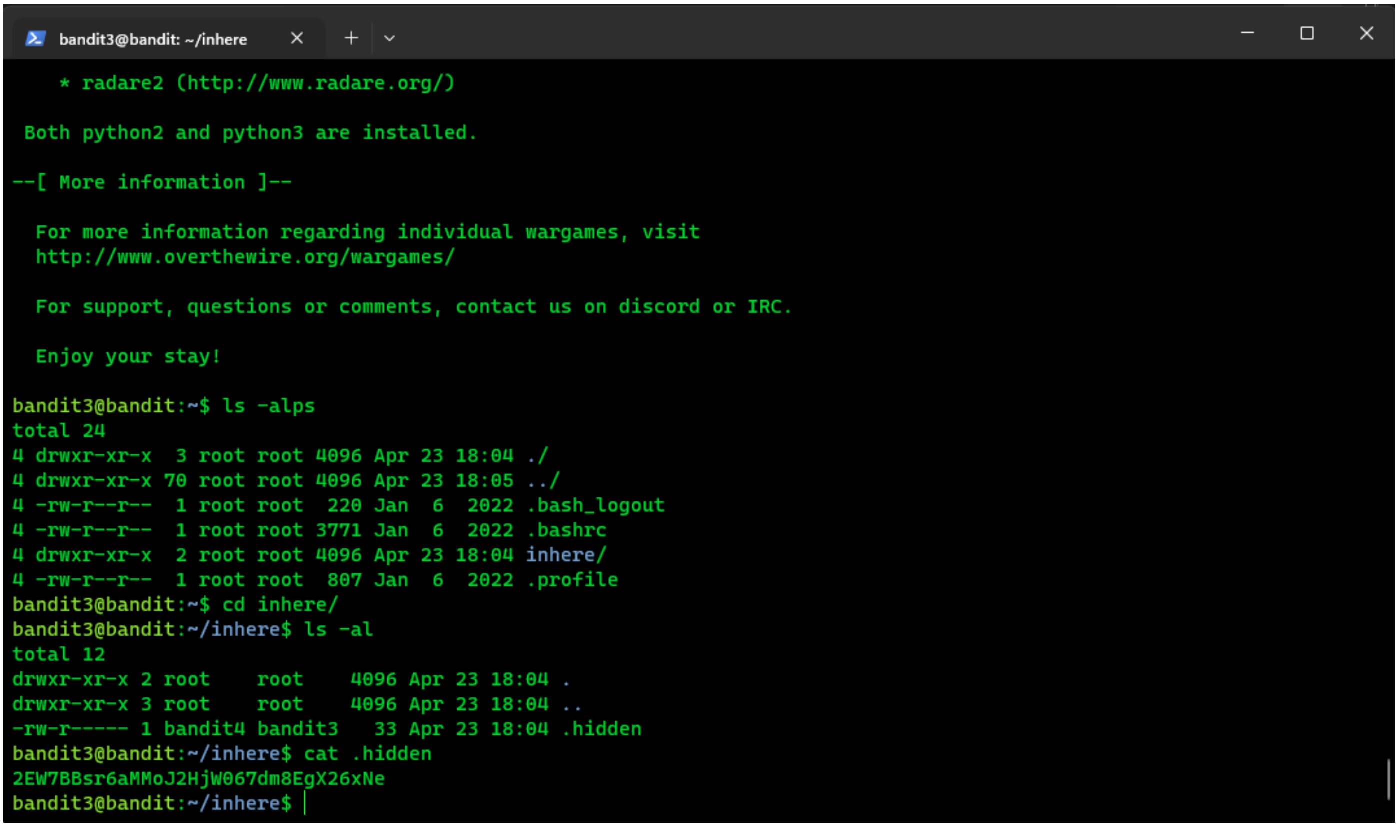
Level 3→Level 4

Level Goal

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

Commands you may need to solve this level.

ls , cd , cat , file , du , find



```
    * radare2 (http://www.radare.org/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root root 4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Apr 23 18:04 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 Apr 23 18:04 .
drwxr-xr-x 3 root    root    4096 Apr 23 18:04 ..
-rw-r----- 1 bandit4 bandit3   33 Apr 23 18:04 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ 
```

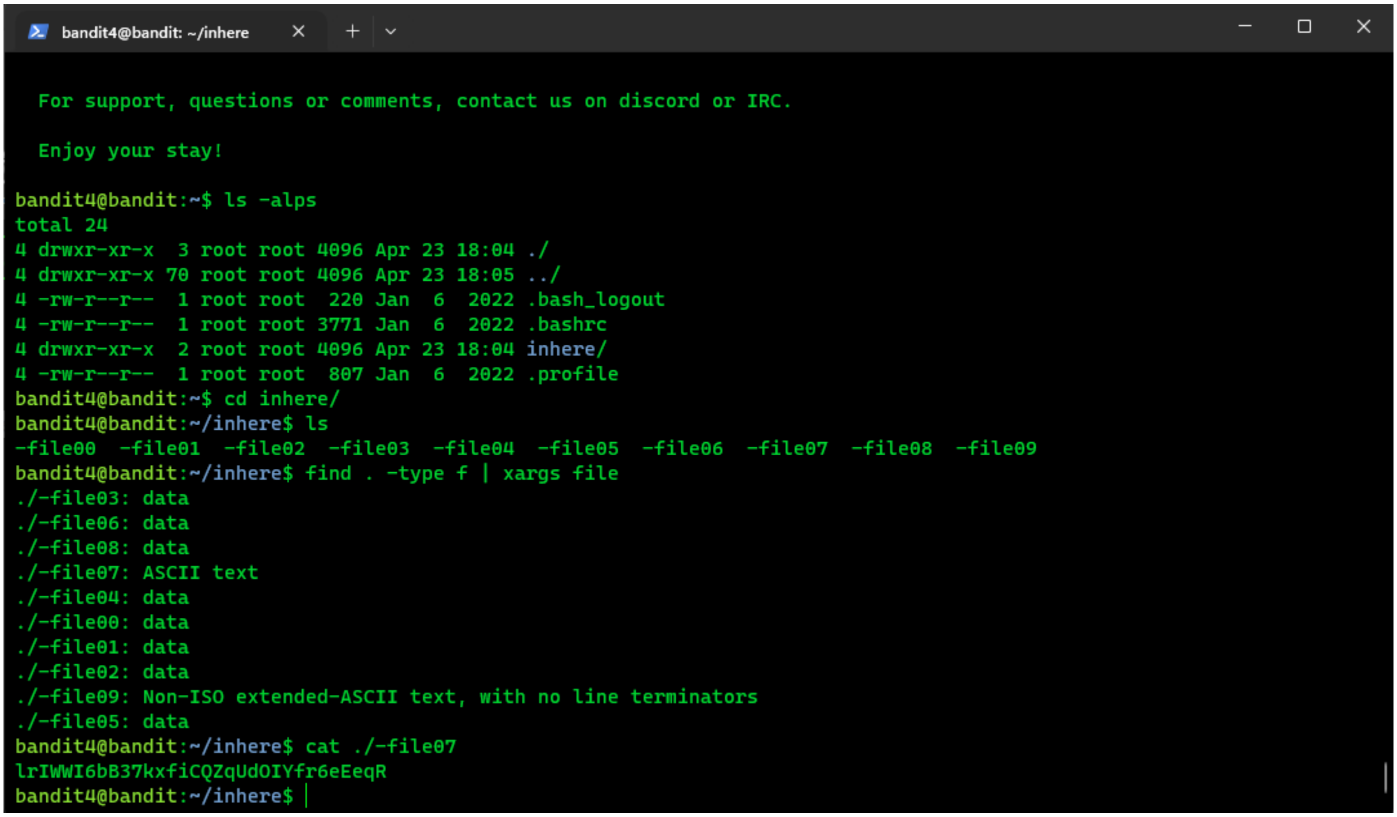
Level 4→Level 5

Level Goal

The password for the next level is stored in the only human-readable file in the inhere directory. Tip: if your terminal is messed up, try the “reset” command.

Commands you may need to solve this level.

ls , cd , cat , file , du , find



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

  Enjoy your stay!

bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root root 4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Apr 23 18:04 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file03: data
./-file06: data
./-file08: data
./-file07: ASCII text
./-file04: data
./-file00: data
./-file01: data
./-file02: data
./-file09: Non-ISO extended-ASCII text, with no line terminators
./-file05: data
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$ 
```

find . -type f | xargs file

find: This is the command used to search for files and directories

-type f: This option specifies that you're looking for files (**f** stands for "file," and **d** would stand for "directory").

|: This symbol, called a pipe, is used to send the output of the command on the left side to the input of the command on the right side. It's used to connect commands together and process data sequentially.

xargs file: This part of the command takes the list of file paths generated by the previous **find** command and passes them as arguments to the **file** command. **xargs** is a utility that takes input from standard input

Level 5→Level 6

Level Goal

The password for the next level is stored in a file somewhere under the inhere directory and has all of the following properties:

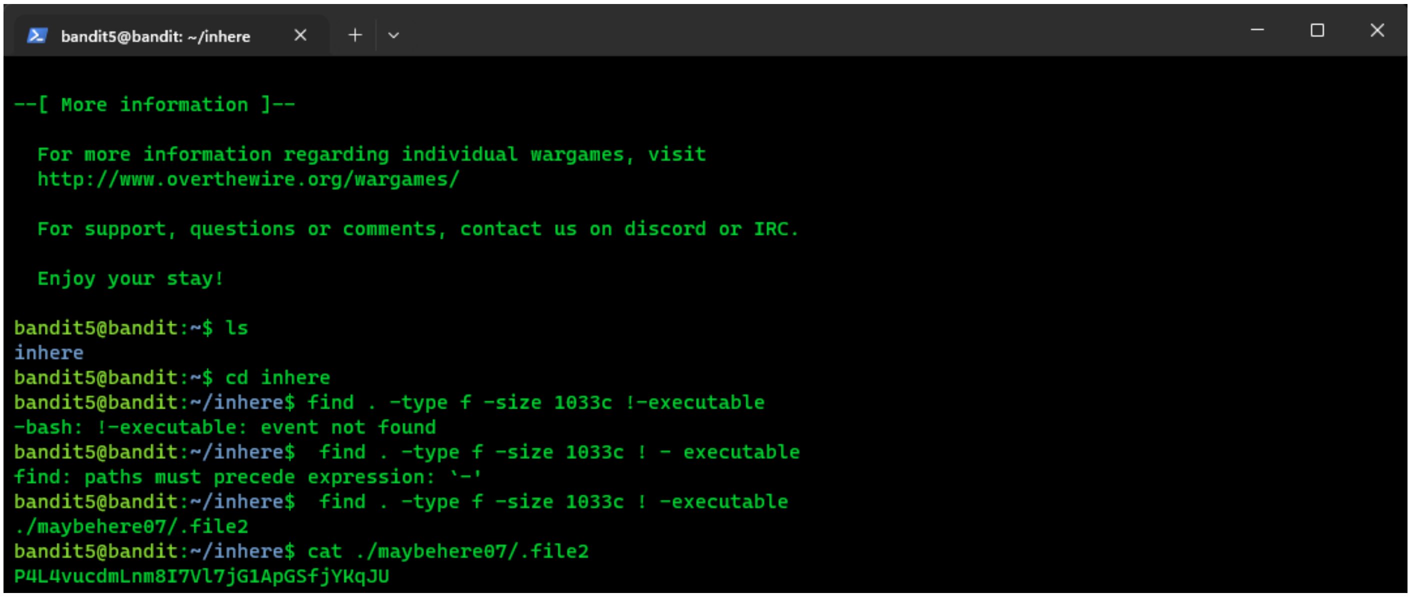
human-readable

1033 bytes in size

not executable

Commands you may need to solve this level**.**

ls , cd , cat , file , du , find



```
--[ More information ]--

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

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

  Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c !-executable
-bash: !-executable: event not found
bandit5@bandit:~/inhere$  find . -type f -size 1033c ! - executable
find: paths must precede expression: `-'
bandit5@bandit:~/inhere$  find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

find . -type f -size 1033c ! -executable

c – bytes we are not using **b** because it defines **blocks**

-size 1033c: This option specifies the size of the files you're looking for. **-size** is used to filter files based on their size, and **1033c** means files that are 1033 bytes in size

. specify the current working directory

! -executable: This part of the command is used to filter out files that are executable. The **!** symbol is used for negation, meaning it excludes files that match the condition that follows

-executable: Checks if a file has the executable permission set, meaning it's an executable binary or script

Level 6→Level 7

Level Goal

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

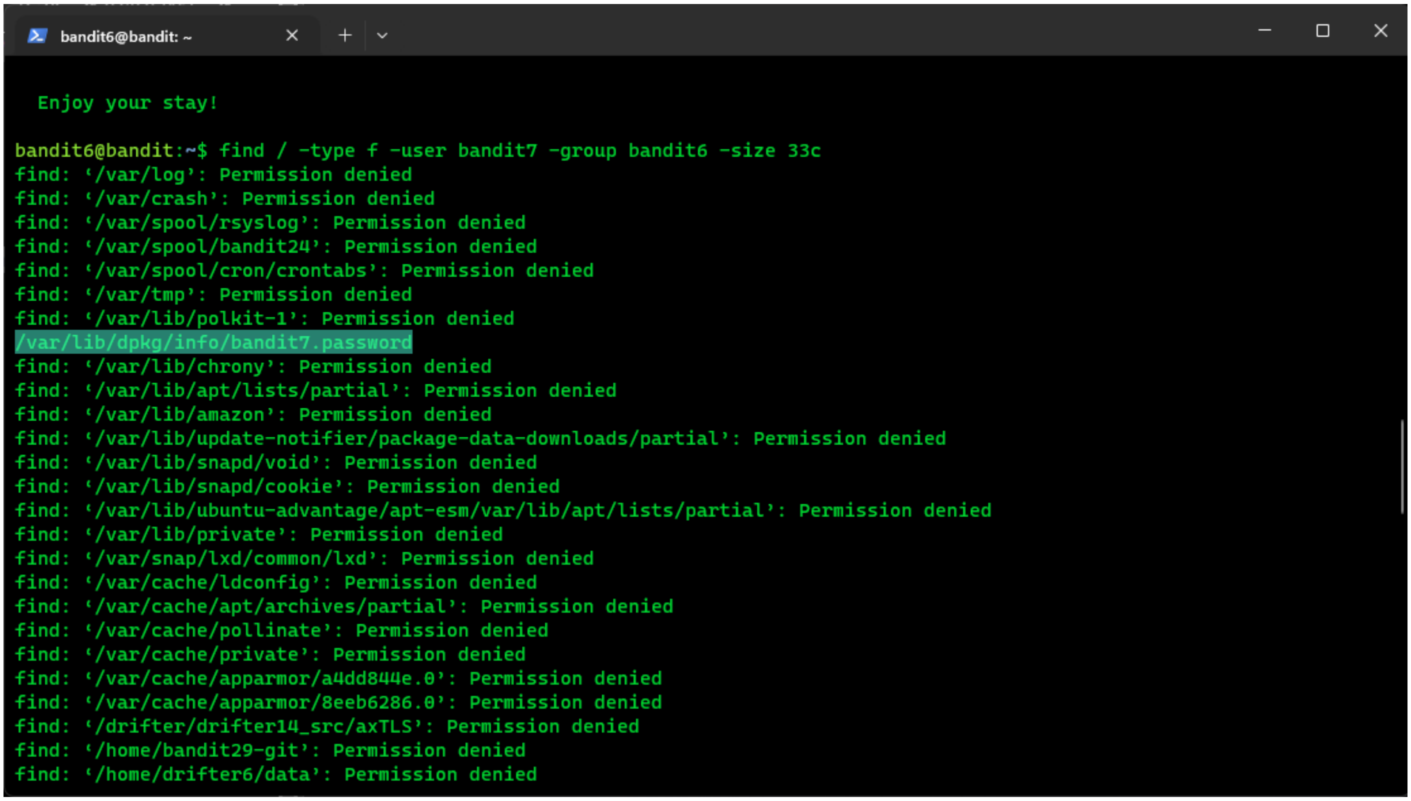
owned by user bandit7

owned by group bandit6

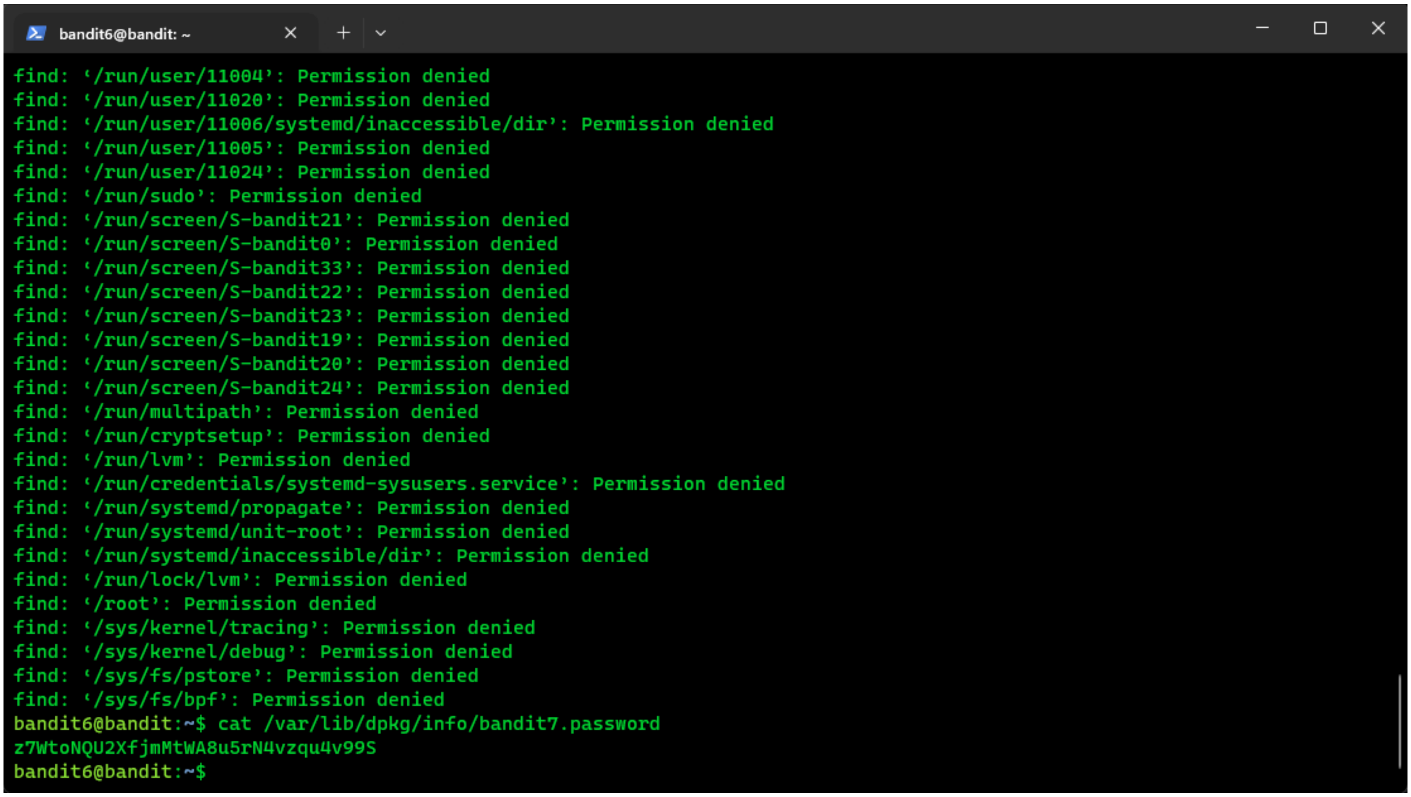
33 bytes in size

Commands you may need to solve this level.

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



```
  Enjoy your stay!

bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: ‘/var/log’: Permission denied
find: ‘/var/crash’: Permission denied
find: ‘/var/spool/rsyslog’: Permission denied
find: ‘/var/spool/bandit24’: Permission denied
find: ‘/var/spool/cron/crontabs’: Permission denied
find: ‘/var/tmp’: Permission denied
find: ‘/var/lib/polkit-1’: Permission denied
/var/lib/dpkg/info/bandit7.password
find: ‘/var/lib/chrony’: Permission denied
find: ‘/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/amazon’: Permission denied
find: ‘/var/lib/update-notifier/package-data-downloads/partial’: Permission denied
find: ‘/var/lib/snapd/void’: Permission denied
find: ‘/var/lib/snapd/cookie’: Permission denied
find: ‘/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/private’: Permission denied
find: ‘/var/snap/lxd/common/lxd’: Permission denied
find: ‘/var/cache/ldconfig’: Permission denied
find: ‘/var/cache/apt/archives/partial’: Permission denied
find: ‘/var/cache/pollinate’: Permission denied
find: ‘/var/cache/private’: Permission denied
find: ‘/var/cache/apparmor/a4dd844e.0’: Permission denied
find: ‘/var/cache/apparmor/8eeb6286.0’: Permission denied
find: ‘/drifter/drifter14_src/axTLS’: Permission denied
find: ‘/home/bandit29-git’: Permission denied
find: ‘/home/drifter6/data’: Permission denied
```



```
find: '/run/user/11004': Permission denied
find: '/run/user/11020': Permission denied
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied
find: '/run/user/11005': Permission denied
find: '/run/user/11024': Permission denied
find: '/run/sudo': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit33': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/multipath': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/credentials/systemd-sysusers.service': Permission denied
find: '/run/systemd/propagate': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/root': Permission denied
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$
```

find / -type f -user bandit7 -group bandit6 -size 33c

- **-type f**: Specifies that you're looking for files (not directories).
- **-user bandit7**: Filters files that are owned by the user named "bandit7."
- **-group bandit6**: Filters files that belong to the group named "bandit6."
- **-size 33c**: Filters files that are exactly 33 bytes in size.

cat /var/lib/dpkg/info/bandit7.pasword

- **cat** command to display the contents of a file named "bandit7.pasword" located in the "/var/lib/dpkg/info/" directory.

Level 7→Level 8

Level Goal

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

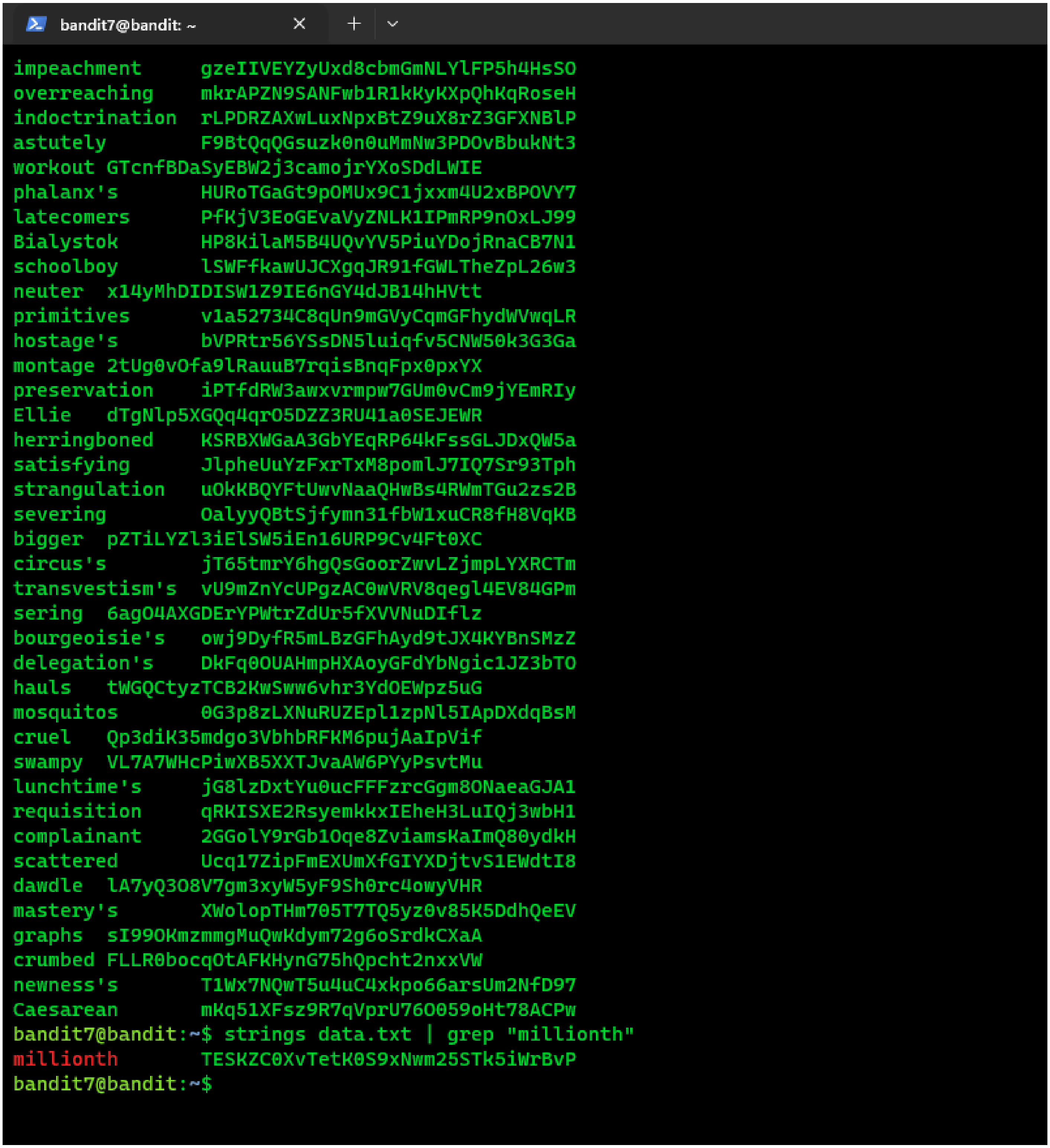
Commands you may need to solve this level.

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

```
strings data.txt  | grep "millionth"
```

strings data.txt: This part of the command uses the **strings** utility to extract human-readable text strings from the file "data.txt." The **strings** command is used to scan sequences of printable characters in a binary file, which can be helpful for extracting text from non-text files.

grep "millionth": This part of the command uses the **grep** utility to search for lines that contain the word "millionth." The **grep** command is used to search for patterns within text.



```
impeachment     gzeIIVEYZyUxd8cbmGmNLYlFP5h4HsSO
overreaching    mkrAPZN9SANFwb1R1kKyKXpQhKqRoseH
indoctrination  rLPDRZAXwLuxNpxBtZ9uX8rZ3GFXNBlP
astutely        F9BtQqQGsuzk0n0uMmNw3PDOvBbukNt3
workout GTcnfBDaSyEBW2j3camojrYXoSDdLWIE
phalanx's       HURoTGaGt9pOMUx9C1jxxm4U2xBPOVY7
latecomers      PfKjV3EoGEvaVyZNLK1IPmRP9nOxLJ99
Bialystok       HP8KilaM5B4UQvYV5PiuYDojRnaCB7N1
schoolboy       lSWFfkawUJCXgqJR91fGWLTheZpL26w3
neuter  x14yMhDIDISW1Z9IE6nGY4dJB14hHVtt
primitives      v1a52734C8qUn9mGVyCqmGFhydWVwqLR
hostage's       bVPRtr56YSsDN5luiqfv5CNW50k3G3Ga
montage 2tUg0vOfa9lRauuB7rqisBnqFpx0pxYX
preservation    iPTfdRW3awxvrmpw7GUm0vCm9jYEmRIy
Ellie   dTgNlp5XGQq4qrO5DZZ3RU41a0SEJEWR
herringboned    KSRBXWGaA3GbYEqRP64kFssGLJDxQW5a
satisfying      JlpheUuYzFxrTxM8pomlJ7IQ7Sr93Tph
strangulation   uOkKBQYFtUwvNaaQHwBs4RWmTGu2zs2B
severing        OalyyQBtSjfymn31fbW1xuCR8fH8VqKB
bigger  pZTiLYZl3iElSW5iEn16URP9Cv4Ft0XC
circus's        jT65tmrY6hgQsGoorZwvLZjmpLYXRCTm
transvestism's  vU9mZnYcUPgzAC0wVRV8qegl4EV84GPm
sering  6agO4AXGDErYPWtrZdUr5fXVVNuDIflz
bourgeoisie's   owj9DyfR5mLBzGFhAyd9tJX4KYBnSMzZ
delegation's    DkFq0OUAHmpHXAoyGFdYbNgic1JZ3bTO
hauls   tWGQCtyzTCB2KwSww6vhr3YdOEWpz5uG
mosquitos       0G3p8zLXNuRUZEpl1zpNl5IApDXdqBsM
cruel   Qp3diK35mdgo3VbhbRFKM6pujAaIpVif
swampy  VL7A7WHcPiwXB5XXTJvaAW6PYyPsvtMu
lunchtime's     jG8lzDxtYu0ucFFFzrcGgm8ONaeaGJA1
requisition     qRKISXE2RsyemkkxIEheH3LuIQj3wbH1
complainant     2GGolY9rGb1Oqe8ZviamsKaImQ80ydkH
scattered       Ucq17ZipFmEXUmXfGIYXDjtvS1EWdtI8
dawdle  lA7yQ3O8V7gm3xyW5yF9Sh0rc4owyVHR
mastery's       XWolopTHm705T7TQ5yz0v85K5DdhQeEV
graphs  sI99OKmzmmgMuQwKdym72g6oSrdkCXaA
crumbed FLLR0bocqOtAFKHynG75hQpcht2nxxVW
newness's       T1Wx7NQwT5u4uC4xkpo66arsUm2NfD97
Caesarean       mKq51XFsz9R7qVprU76O059oHt78ACPw
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@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.

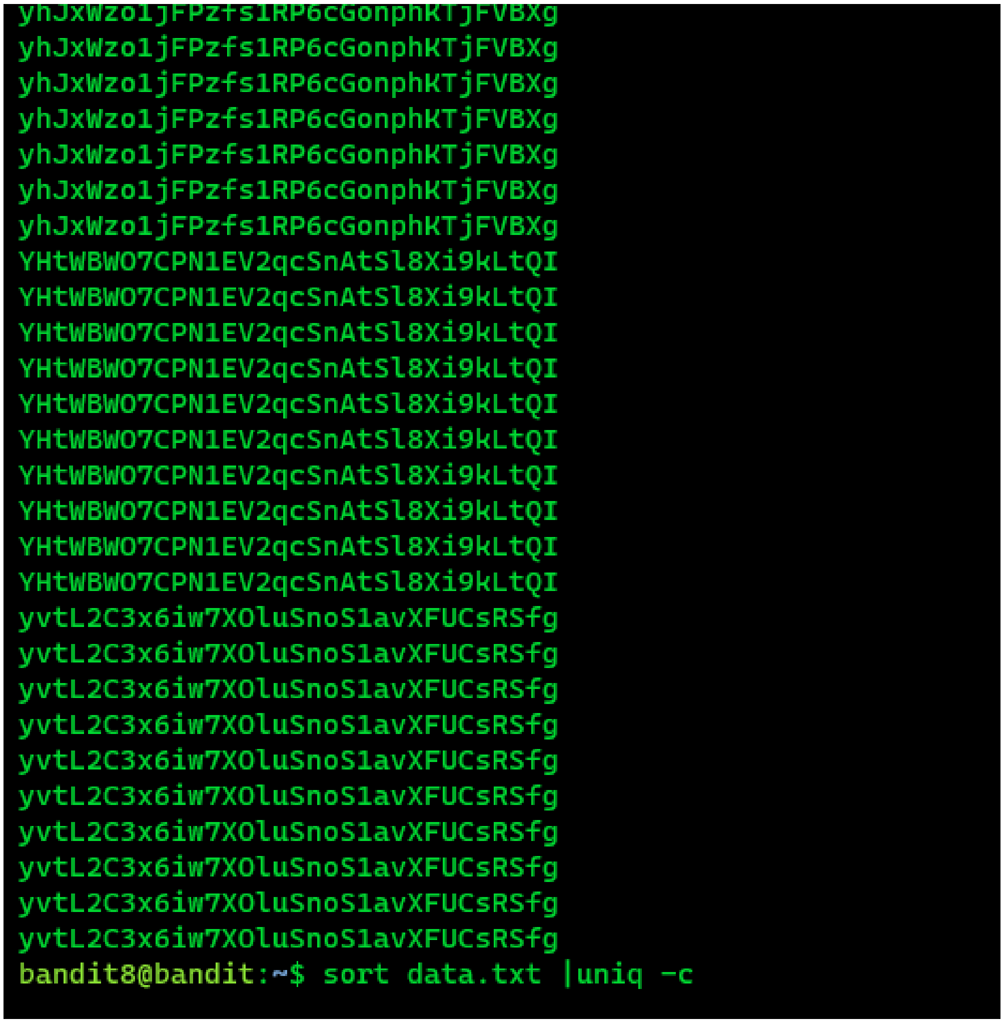
Commands you may need to solve this level.

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

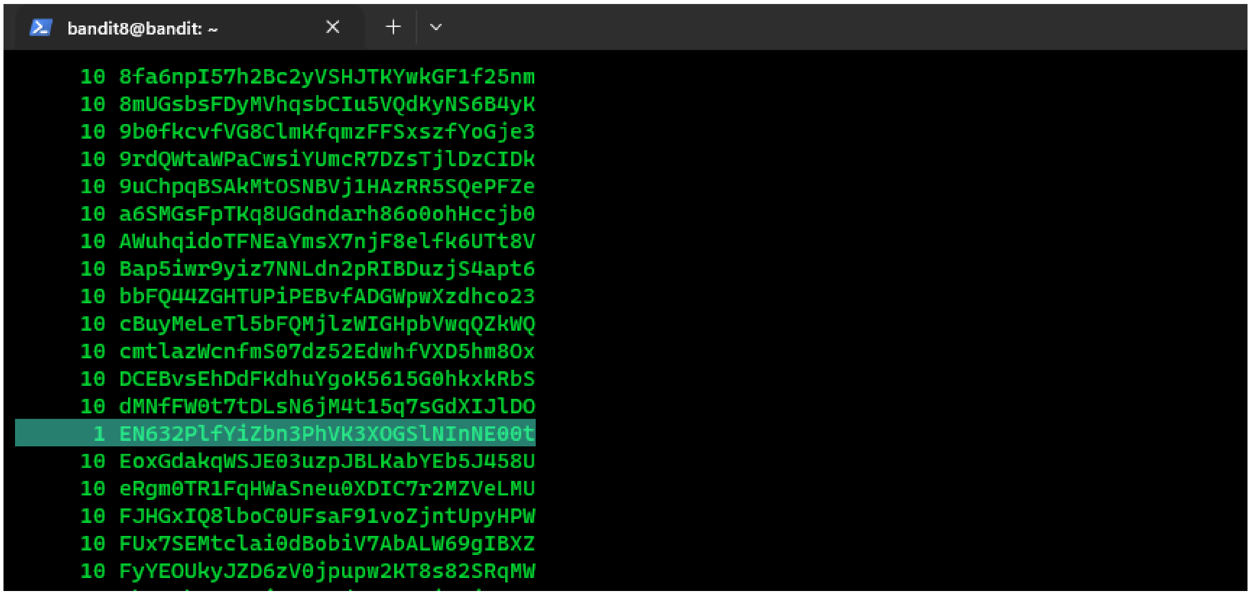
sort data.txt | uniq -c

The sort command is used to arrange lines of text or data in a specific order.

uniq -c: This part of the command uses the **uniq** utility to find and count unique lines in the input. The **-c** flag is used to show the count of occurrences for each unique line.



```
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
yhJxWzo1jFPzfs1RP6cGonphKTjFVBXg
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
YHtWBWO7CPN1EV2qcSnAtSl8Xi9kLtQI
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
yvtL2C3x6iw7XOluSnoS1avXFUCsRSfg
bandit8@bandit:~$ sort data.txt |uniq -c
```



```
     10 8fa6npI57h2Bc2yVSHJTKYwkGF1f25nm
     10 8mUGsbsFDyMVhqsbCIu5VQdKyNS6B4yK
     10 9b0fkcvfVG8ClmKfqmzFFSxszfYoGje3
     10 9rdQWtaWPaCwsiYUmcR7DZsTjlDzCIDk
     10 9uChpqBSAkMtOSNBVj1HAzRR5SQePFZe
     10 a6SMGsFpTKq8UGdndarh86o0ohHccjb0
     10 AWuhqidoTFNEaYmsX7njF8elfk6UTt8V
     10 Bap5iwr9yiz7NNLdn2pRIBDuzjS4apt6
     10 bbFQ44ZGHTUPiPEBvfADGWpwXzdhco23
     10 cBuyMeLeTl5bFQMjlzWIGHpbVwqQZkWQ
     10 cmtlazWcnfmS07dz52EdwhfVXD5hm8Ox
     10 DCEBvsEhDdFKdhuYgoK5615G0hkxkRbS
     10 dMNfFW0t7tDLsN6jM4t15q7sGdXIJlDO
      1 EN632PlfYiZbn3PhVK3XOGSlNInNE00t
     10 EoxGdakqWSJE03uzpJBLKabYEb5J458U
     10 eRgm0TR1FqHWaSneu0XDIC7r2MZVeLMU
     10 FJHGxIQ8lboC0UFsaF91voZjntUpyHPW
     10 FUx7SEMtclai0dBobiV7AbALW69gIBXZ
     10 FyYEOUkyJZD6zV0jpupw2KT8s82SRqMW
```

Level 9→Level 10

Level Goal

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

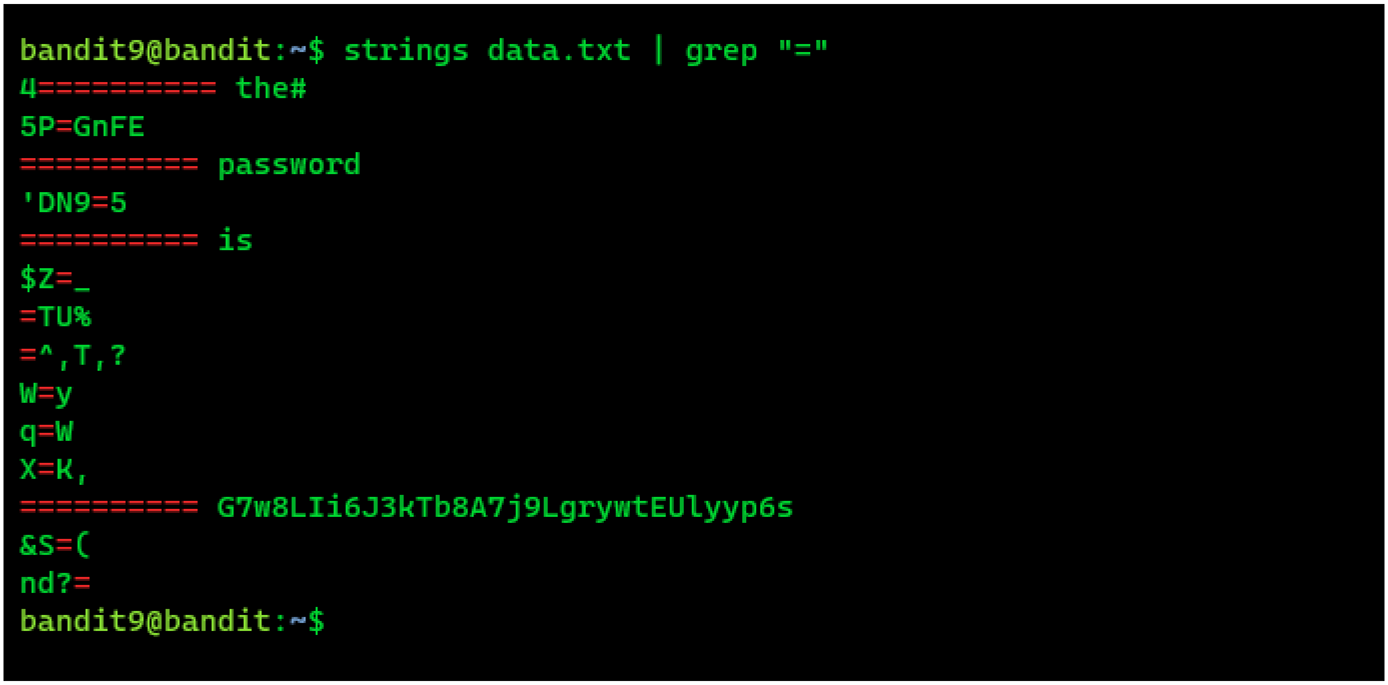
Commands you may need to solve this level

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

strings data.txt |grep "="

strings data.txt: This part of the command uses the **strings** utility to extract human-readable text strings from the file "data.txt." The **strings** command is used to scan for sequences of printable characters in a binary file and extract them as text.

grep "=": This part of the command uses the grep utility to search for lines that contain the character **"="** within the extracted text strings. The **grep** command is used to search for patterns within text.



```
bandit9@bandit:~$ strings data.txt | grep "="
4========== the#
5P=GnFE
========== password
'DN9=5
========== is
$Z=_
=TU%
=^,T,?
W=y
q=W
X=K,
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
&S=(
nd?=
bandit9@bandit:~$
```

Level 10→Level 11

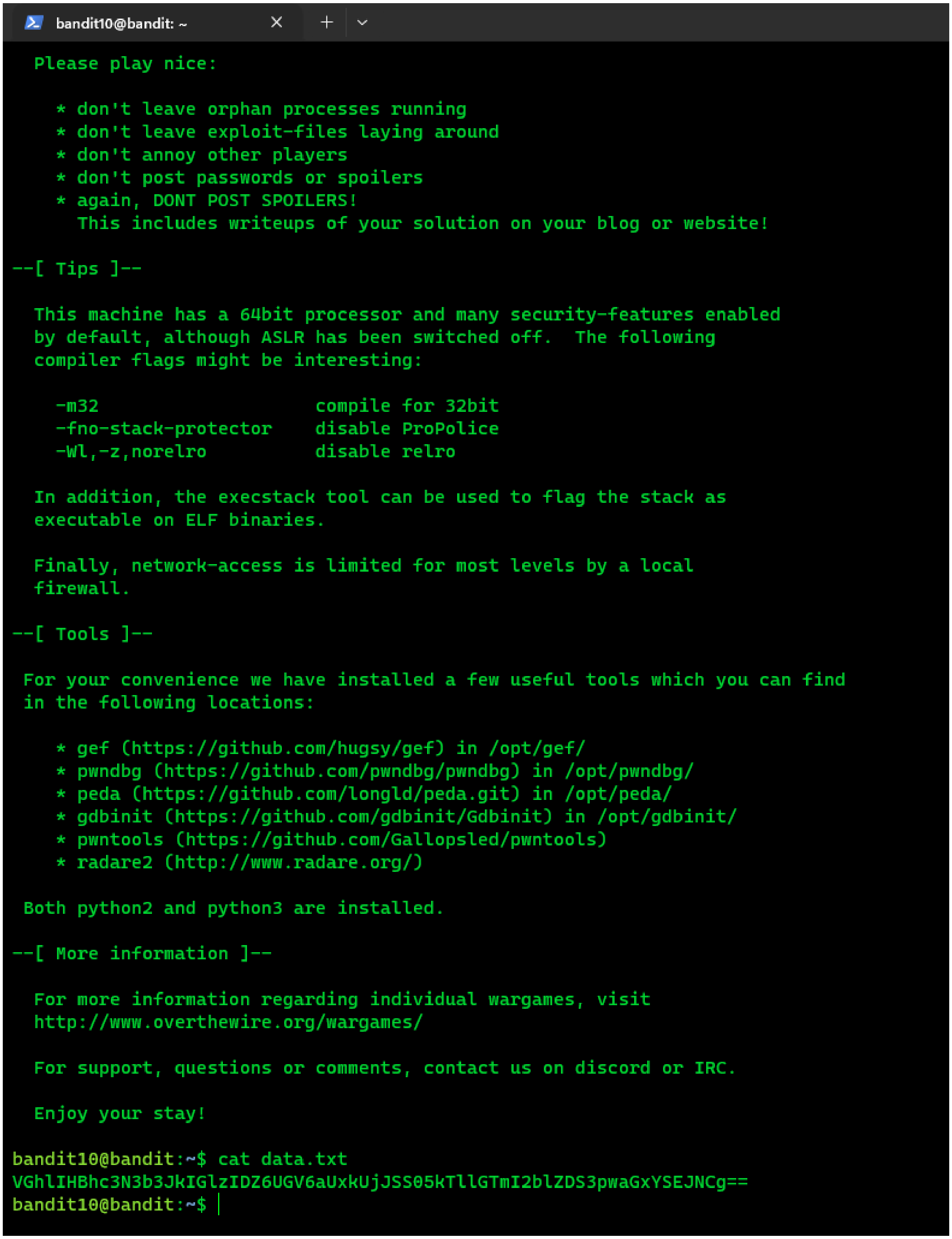
Level Goal

The password for the next level is stored in the file data.txt, which contains base64 encoded data.

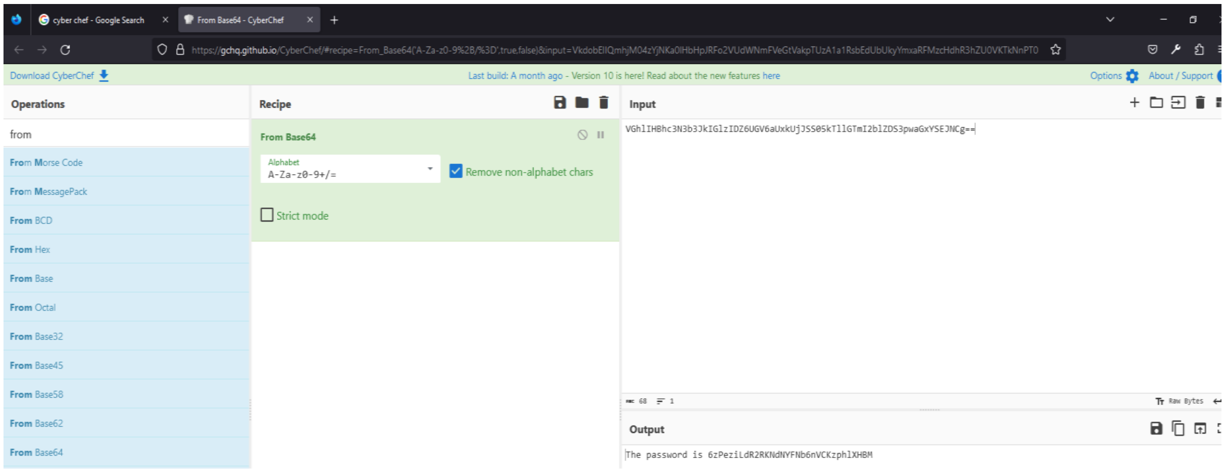
Commands you may need to solve this level.

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

After obtaining the string it must be decoded accordingly



```
  Please play nice:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
    * don't annoy other players
    * don't post passwords or spoilers
    * again, DONT POST SPOILERS!
      This includes writeups of your solution on your blog or website!

--[ Tips ]--

  This machine has a 64bit processor and many security-features enabled
  by default, although ASLR has been switched off.  The following
  compiler flags might be interesting:

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

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ 
```



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input

```
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
```

68 1

Output

```
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

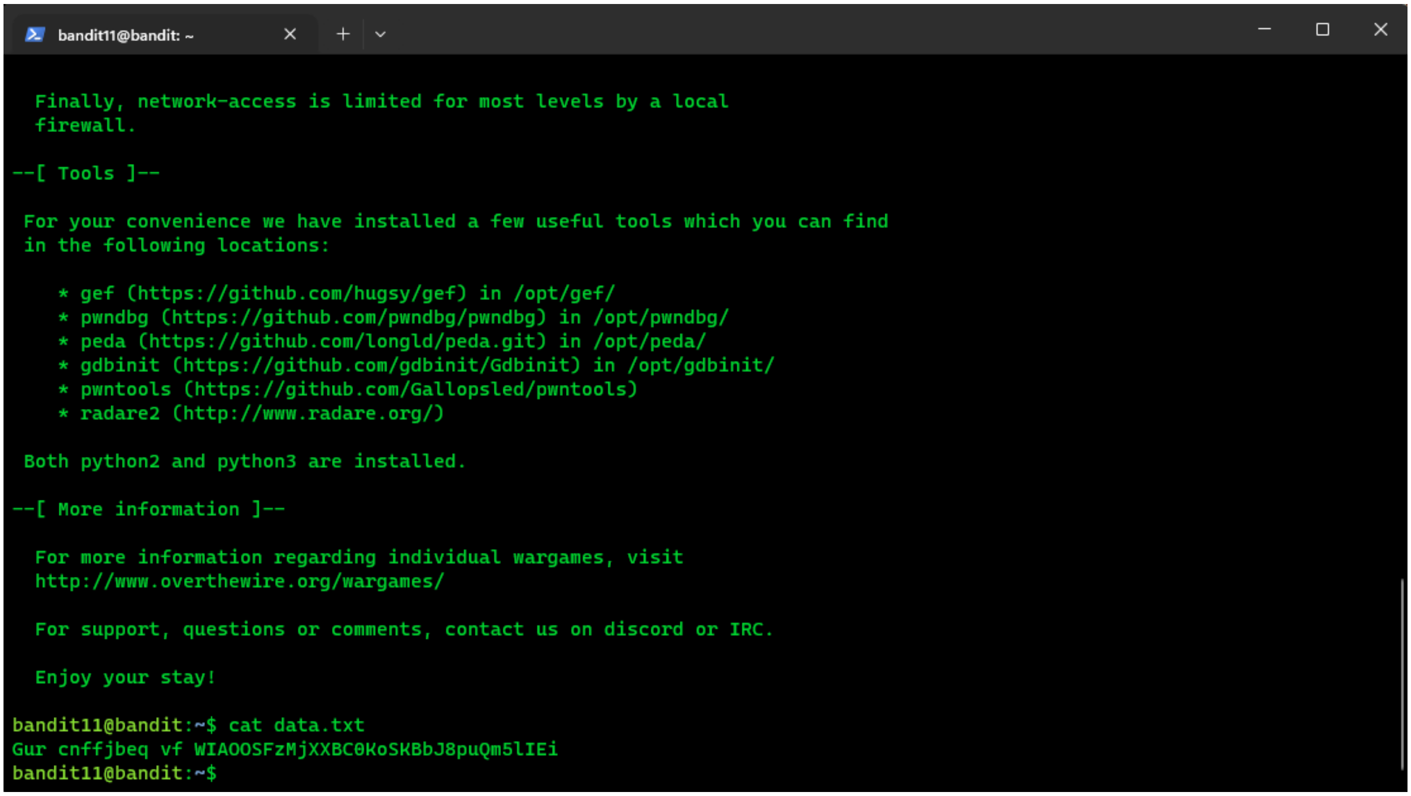
Level 11→Level 12

Level Goal

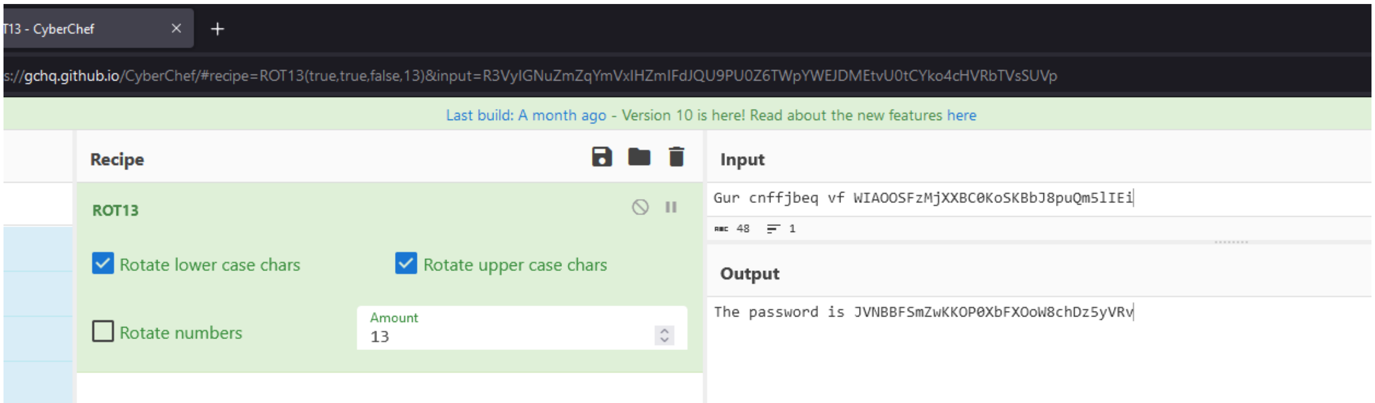
The password for the next level is stored in the file data.txt, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions.

Commands you may need to solve this level.

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



```
  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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$
```


T13 - CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Recipe
Input
Output

s://gchq.github.io/CyberChef/#recipe=ROT13(true,true,false,13)&input=R3VyIGNuZmZqYmVxIHZmIFdJQU9PU0Z6TWpYWEJDMEtvU0tCYko4cHVRbTVsSUVp

ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars

□ Rotate numbers Amount 13

```
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
```

48 1

```
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
```

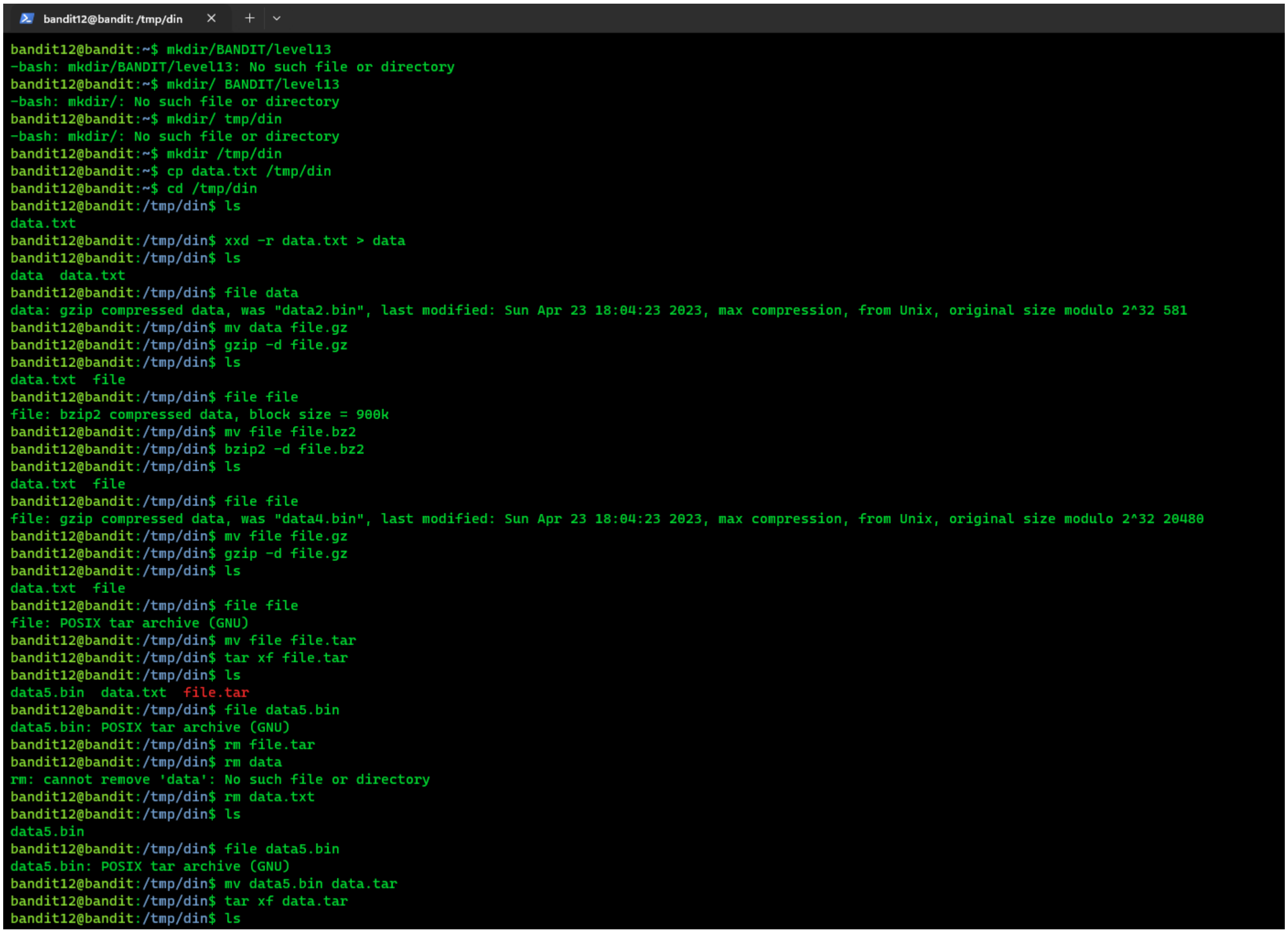
Level 12→Level 13

Level Goal

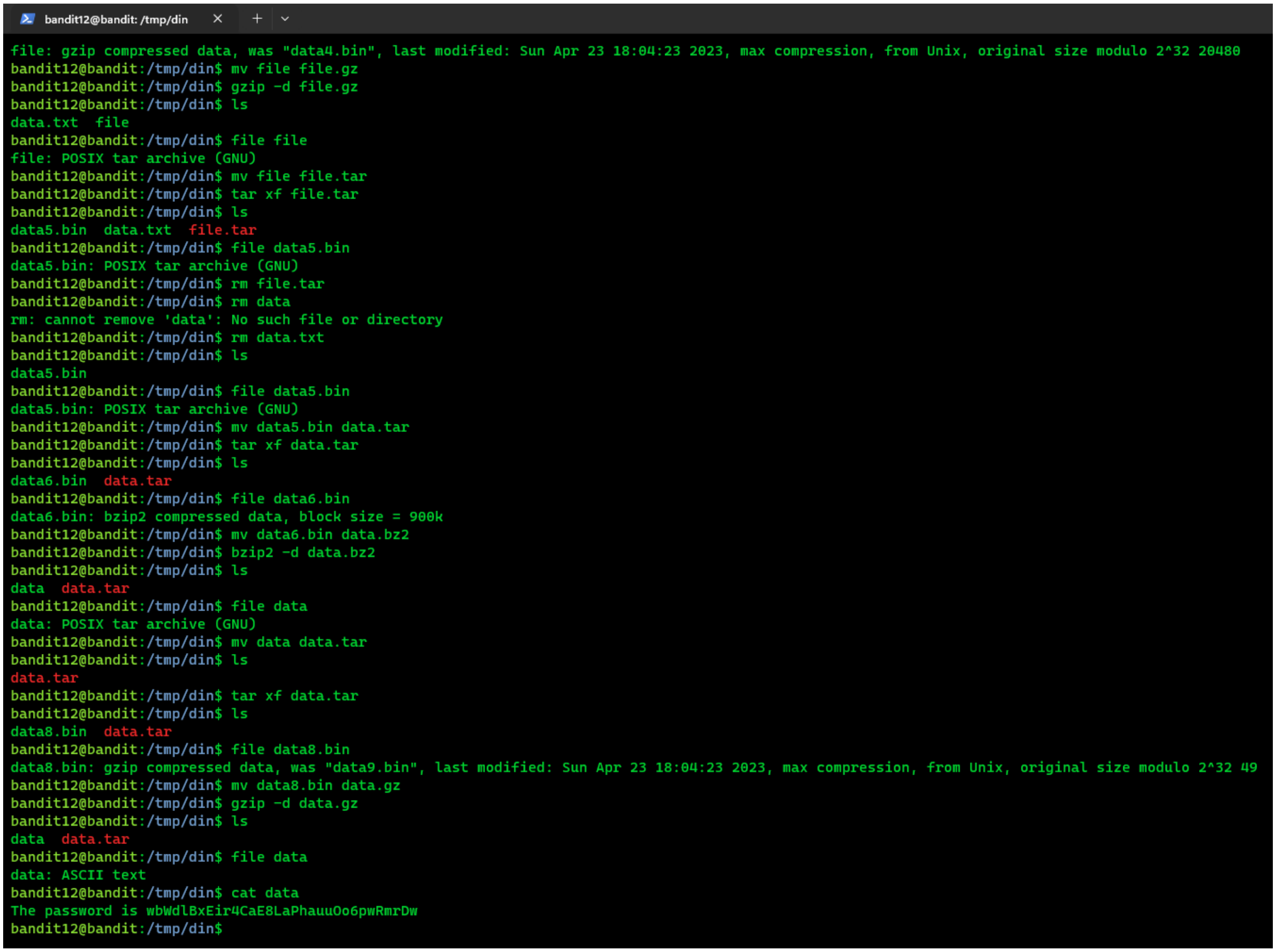
The password for the next level is stored in the file data.txt, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

Commands you may need to solve this level.

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv, file



```
bandit12@bandit:~$ mkdir/BANDIT/level13
-bash: mkdir/BANDIT/level13: No such file or directory
bandit12@bandit:~$ mkdir/ BANDIT/level13
-bash: mkdir/: No such file or directory
bandit12@bandit:~$ mkdir/ tmp/din
-bash: mkdir/: No such file or directory
bandit12@bandit:~$ mkdir /tmp/din
bandit12@bandit:~$ cp data.txt /tmp/din
bandit12@bandit:~$ cd /tmp/din
bandit12@bandit:/tmp/din$ ls
data.txt
bandit12@bandit:/tmp/din$ xxd -r data.txt > data
bandit12@bandit:/tmp/din$ ls
data  data.txt
bandit12@bandit:/tmp/din$ file data
data: gzip compressed data, was "data2.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 581
bandit12@bandit:/tmp/din$ mv data file.gz
bandit12@bandit:/tmp/din$ gzip -d file.gz
bandit12@bandit:/tmp/din$ ls
data.txt  file
bandit12@bandit:/tmp/din$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/din$ mv file file.bz2
bandit12@bandit:/tmp/din$ bzip2 -d file.bz2
bandit12@bandit:/tmp/din$ ls
data.txt  file
bandit12@bandit:/tmp/din$ file file
file: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/din$ mv file file.gz
bandit12@bandit:/tmp/din$ gzip -d file.gz
bandit12@bandit:/tmp/din$ ls
data.txt  file
bandit12@bandit:/tmp/din$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ mv file file.tar
bandit12@bandit:/tmp/din$ tar xf file.tar
bandit12@bandit:/tmp/din$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/din$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ rm file.tar
bandit12@bandit:/tmp/din$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/din$ rm data.txt
bandit12@bandit:/tmp/din$ ls
data5.bin
bandit12@bandit:/tmp/din$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ mv data5.bin data.tar
bandit12@bandit:/tmp/din$ tar xf data.tar
bandit12@bandit:/tmp/din$ ls
```



```
file: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/din$ mv file file.gz
bandit12@bandit:/tmp/din$ gzip -d file.gz
bandit12@bandit:/tmp/din$ ls
data.txt  file
bandit12@bandit:/tmp/din$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ mv file file.tar
bandit12@bandit:/tmp/din$ tar xf file.tar
bandit12@bandit:/tmp/din$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/din$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ rm file.tar
bandit12@bandit:/tmp/din$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/din$ rm data.txt
bandit12@bandit:/tmp/din$ ls
data5.bin
bandit12@bandit:/tmp/din$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ mv data5.bin data.tar
bandit12@bandit:/tmp/din$ tar xf data.tar
bandit12@bandit:/tmp/din$ ls
data6.bin  data.tar
bandit12@bandit:/tmp/din$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/din$ mv data6.bin data.bz2
bandit12@bandit:/tmp/din$ bzip2 -d data.bz2
bandit12@bandit:/tmp/din$ ls
data  data.tar
bandit12@bandit:/tmp/din$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/din$ mv data data.tar
bandit12@bandit:/tmp/din$ ls
data.tar
bandit12@bandit:/tmp/din$ tar xf data.tar
bandit12@bandit:/tmp/din$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/din$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/din$ mv data8.bin data.gz
bandit12@bandit:/tmp/din$ gzip -d data.gz
bandit12@bandit:/tmp/din$ ls
data  data.tar
bandit12@bandit:/tmp/din$ file data
data: ASCII text
bandit12@bandit:/tmp/din$ cat data
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/din$
```

1. **mkdir /bandit/level13**
   - This command creates a new directory named "level13" inside the "/bandit" directory. It's creating a subdirectory for organizing files.
2. **cp data.txt /tmp/din**
   - This command copies the file "data.txt" to the "/tmp" directory and renames it to "din."

3. **xxd -r data.txt > data**
   - This command converts the hexadecimal representation of a file (like the one generated by the **xxd** command) back into binary format. It takes the contents of "data.txt," which are likely in hexadecimal format, and converts them back to binary. The output is redirected to a file named "data."
4. **mv data file.gz**
   - This command renames the file "data" to "file.gz." The new name suggests that the file might be a GZIP-compressed file.
5. **gzip -d file.gz**
   - This command decompresses the GZIP-compressed file "file.gz," creating an uncompressed file named "file."
6. **mv file file.bz2**
   - This command renames the decompressed file "file" to "file.bz2." The new name suggests that the file might be a BZIP2-compressed file.
7. **bzip2 -d file.bz2**
   - This command decompresses the BZIP2-compressed file "file.bz2," creating an uncompressed file named "file."
8. **mv file file.tar**
   - This command renames the decompressed file "file" to "file.tar." The new name suggests that the file might be a TAR archive.
9. **tar xf file.tar**
   - This command extracts the contents of the TAR archive "file.tar" to the current directory. The options "x" and "f" are used to extract and specify the file name.

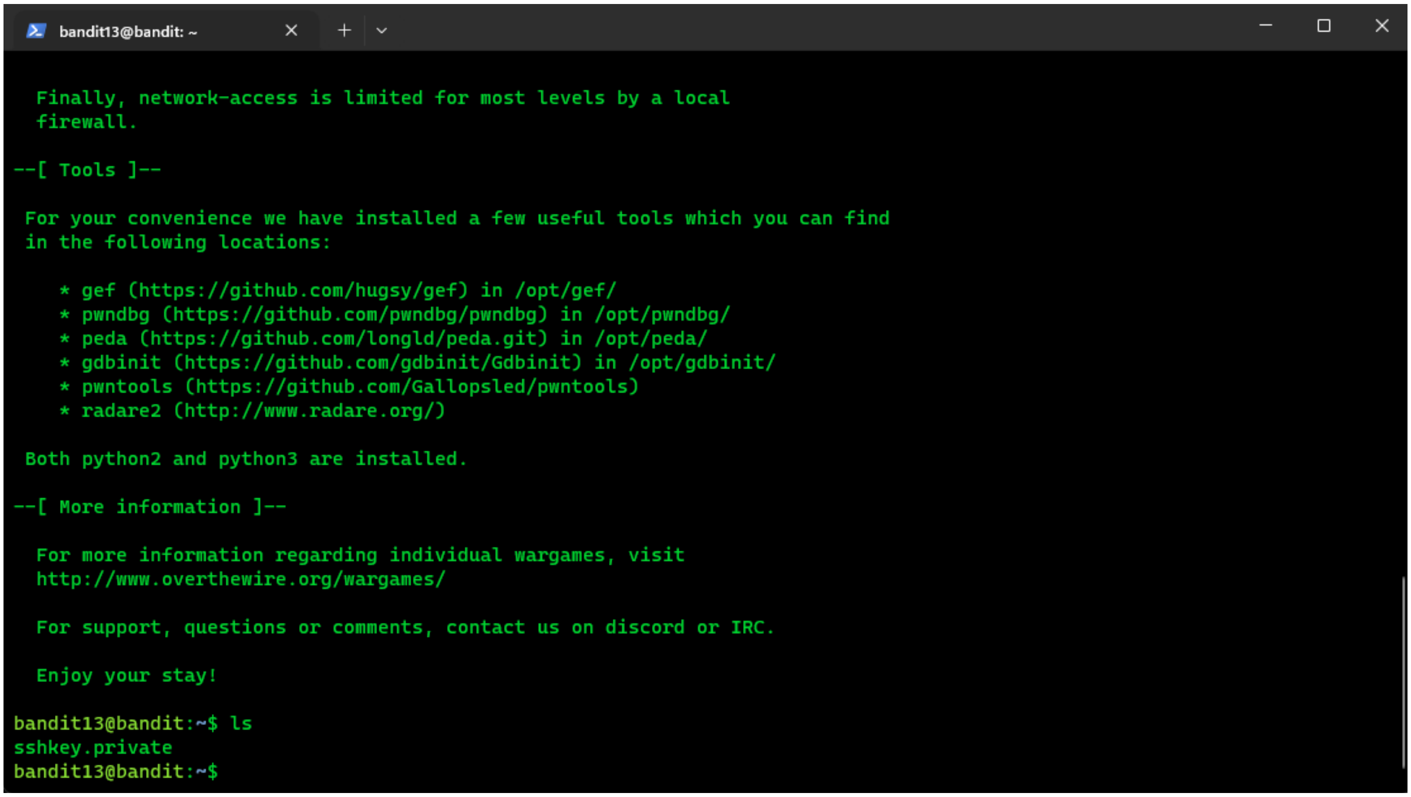
Level 13→Level 14

Level Goal

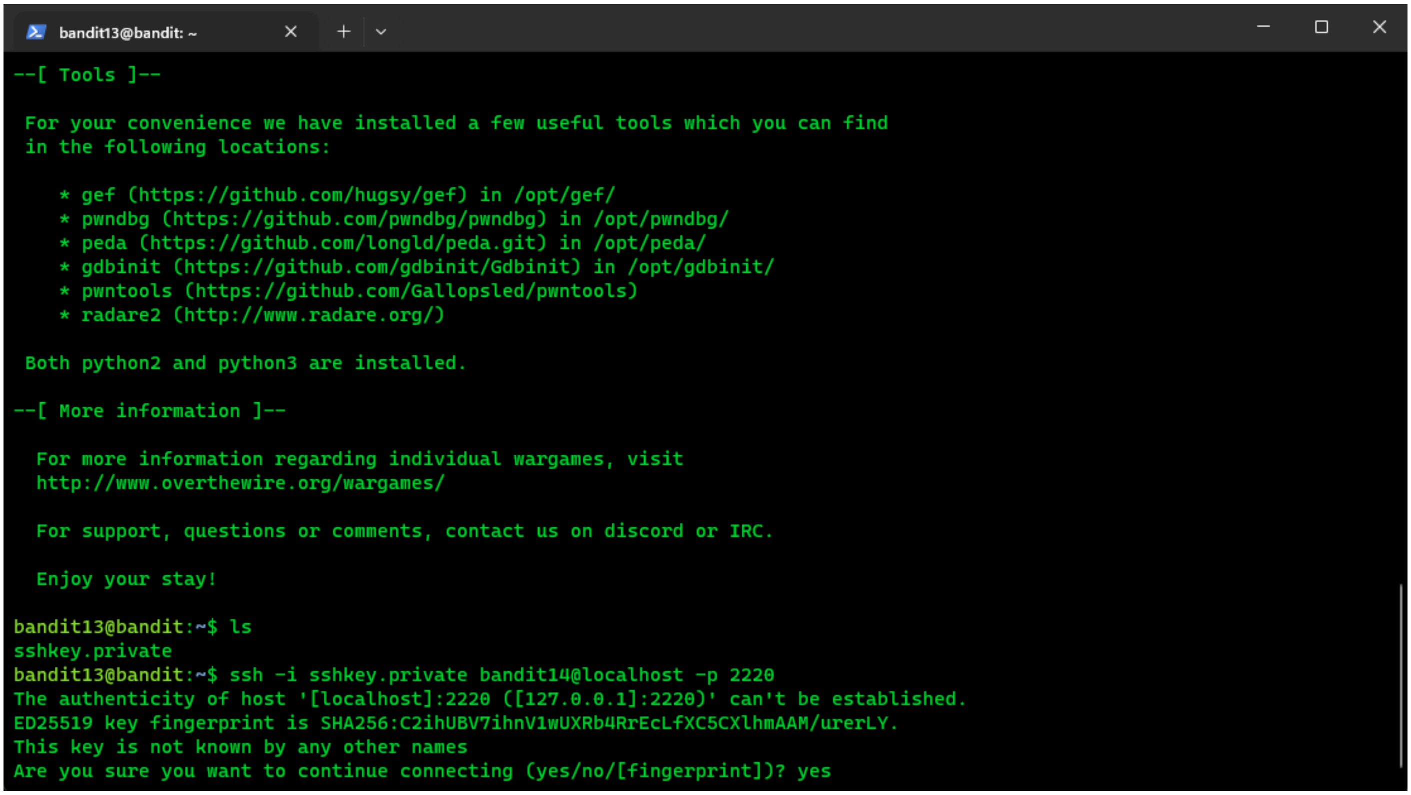
The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: localhost is a hostname that refers to the machine you are working on

Commands you may need to solve this level.

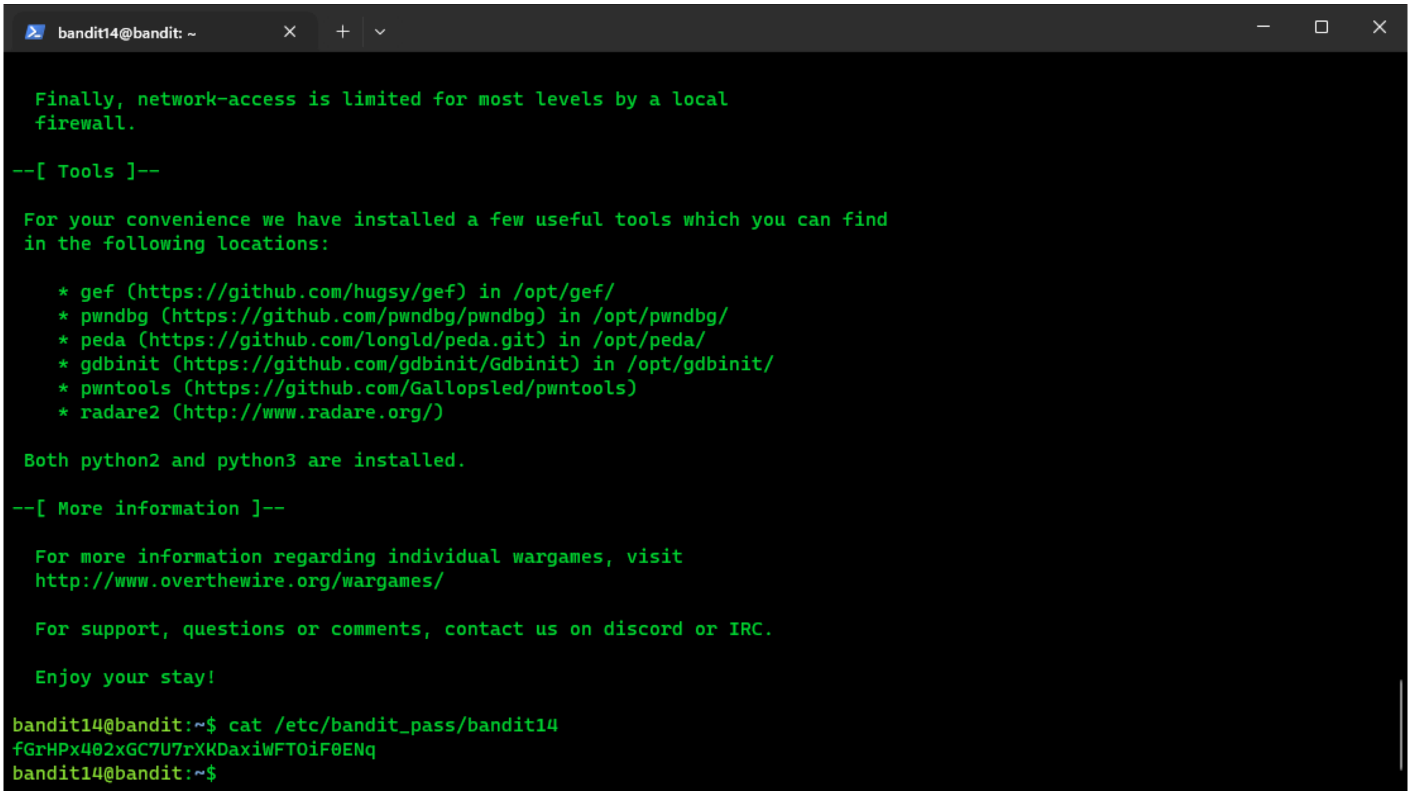
ssh, telnet, nc, openssl, s_client, nmap



```
  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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

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



```
--[ 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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' 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])? yes
```



```

  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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$
```

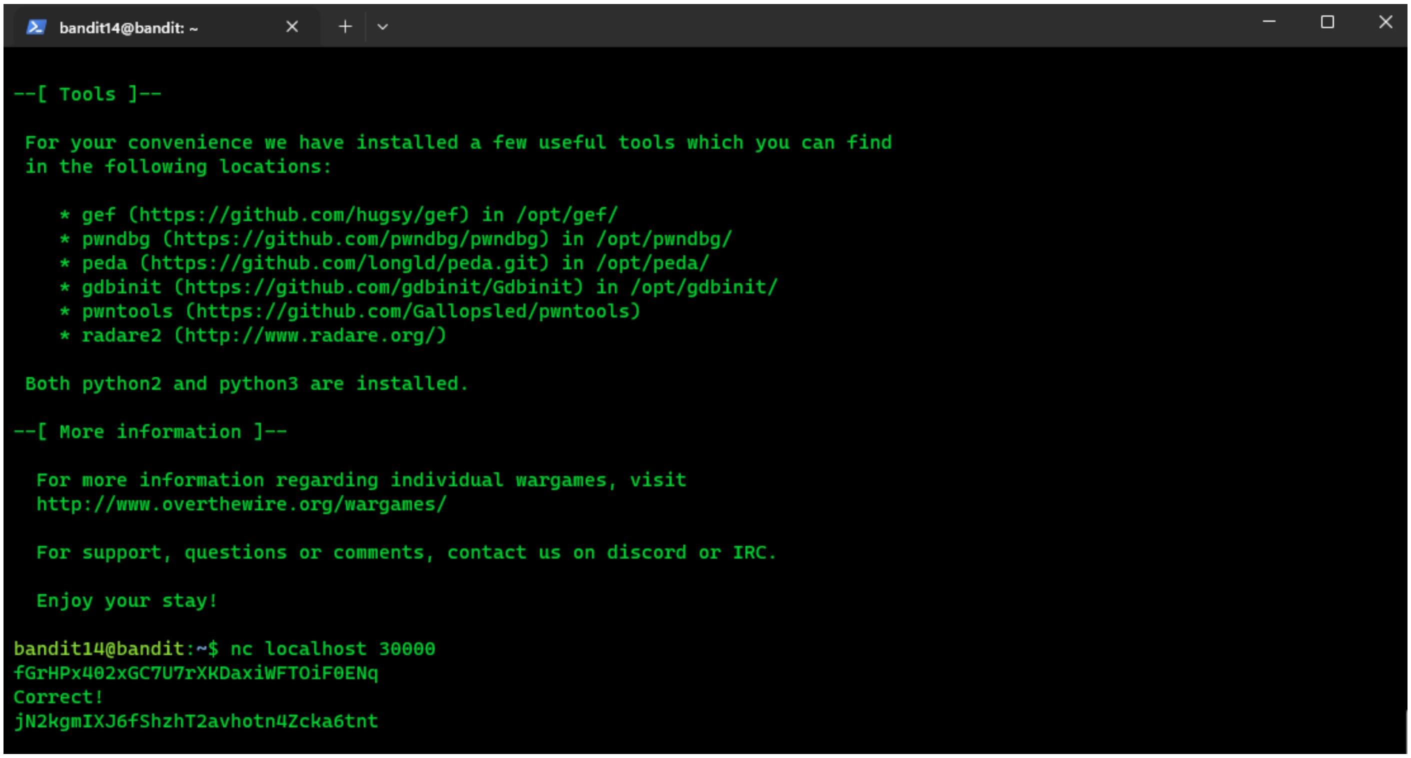
Level 14→Level 15

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

Commands you may need to solve this level.

ssh, telnet, nc, openssl, s_client, nmap



```
--[ 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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

nc localhost 30000

nc: This stands for "netcat," which is a versatile networking utility used for reading from and writing to network connections.

localhost: This refers to the hostname of the local machine itself. It's a way to specify that you want to connect to the computer currently using.

30000: This is the port number that specifying to connect to

Level 15→Level 16

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption.

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command**…**

Commands you may need to solve this level.

ssh, telnet, nc, openssl, s_client, nmap

cat /etc/bandit_pass/bandit15 – getting the password of the current level.

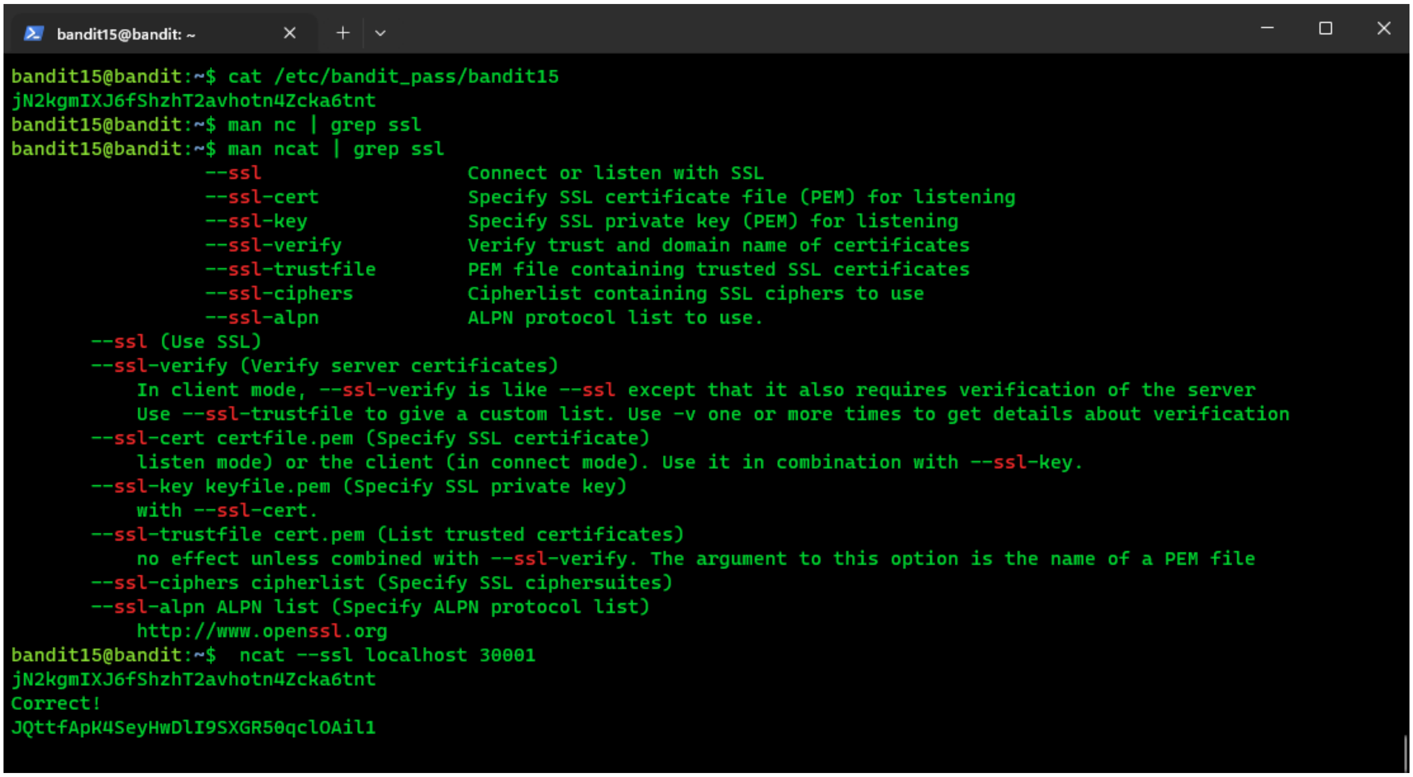
ncat --ssl localhost 30001

jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

then can obtain the password of the next level.

ncat: This is a utility similar to **nc** (netcat) but with additional features and capabilities. It's used for creating and managing network connections.

--ssl: This option tells **ncat** to use SSL/TLS encryption when establishing the network connection. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols used to secure communication over a computer network.



```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man ncat | grep ssl
                 --ssl                      Connect or listen with SSL
                 --ssl-cert                 Specify SSL certificate file (PEM) for listening
                 --ssl-key                  Specify SSL private key (PEM) for listening
                 --ssl-verify               Verify trust and domain name of certificates
                 --ssl-trustfile            PEM file containing trusted SSL certificates
                 --ssl-ciphers              Cipherlist containing SSL ciphers to use
                 --ssl-alpn                 ALPN protocol list to use.
       --ssl (Use SSL)
       --ssl-verify (Verify server certificates)
           In client mode, --ssl-verify is like --ssl except that it also requires verification of the server
           Use --ssl-trustfile to give a custom list. Use -v one or more times to get details about verification
       --ssl-cert certfile.pem (Specify SSL certificate)
           listen mode) or the client (in connect mode). Use it in combination with --ssl-key.
       --ssl-key keyfile.pem (Specify SSL private key)
           with --ssl-cert.
       --ssl-trustfile cert.pem (List trusted certificates)
           no effect unless combined with --ssl-verify. The argument to this option is the name of a PEM file
       --ssl-ciphers cipherlist (Specify SSL ciphersuites)
       --ssl-alpn ALPN list (Specify ALPN protocol list)
           http://www.openssl.org
bandit15@bandit:~$  ncat --ssl localhost 30001
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

Level 16→Level 17

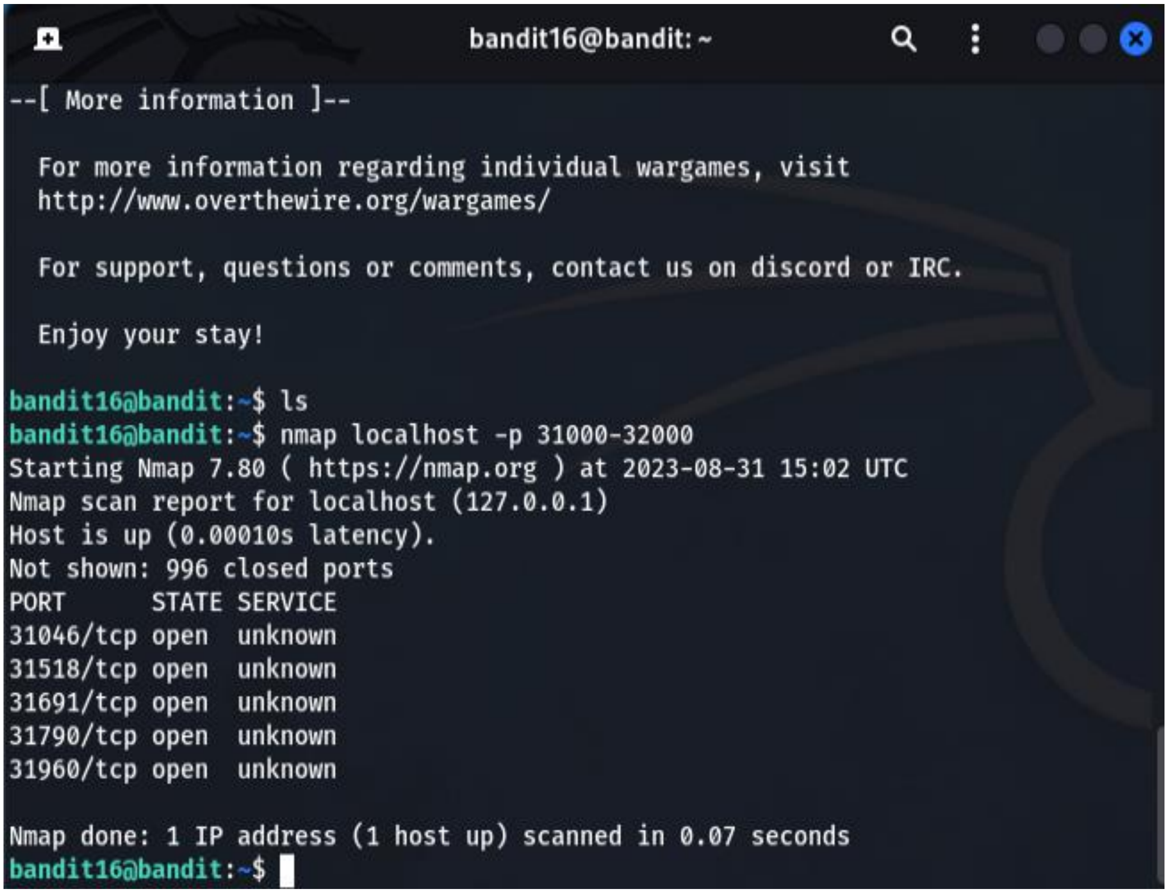
Level Goal

The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

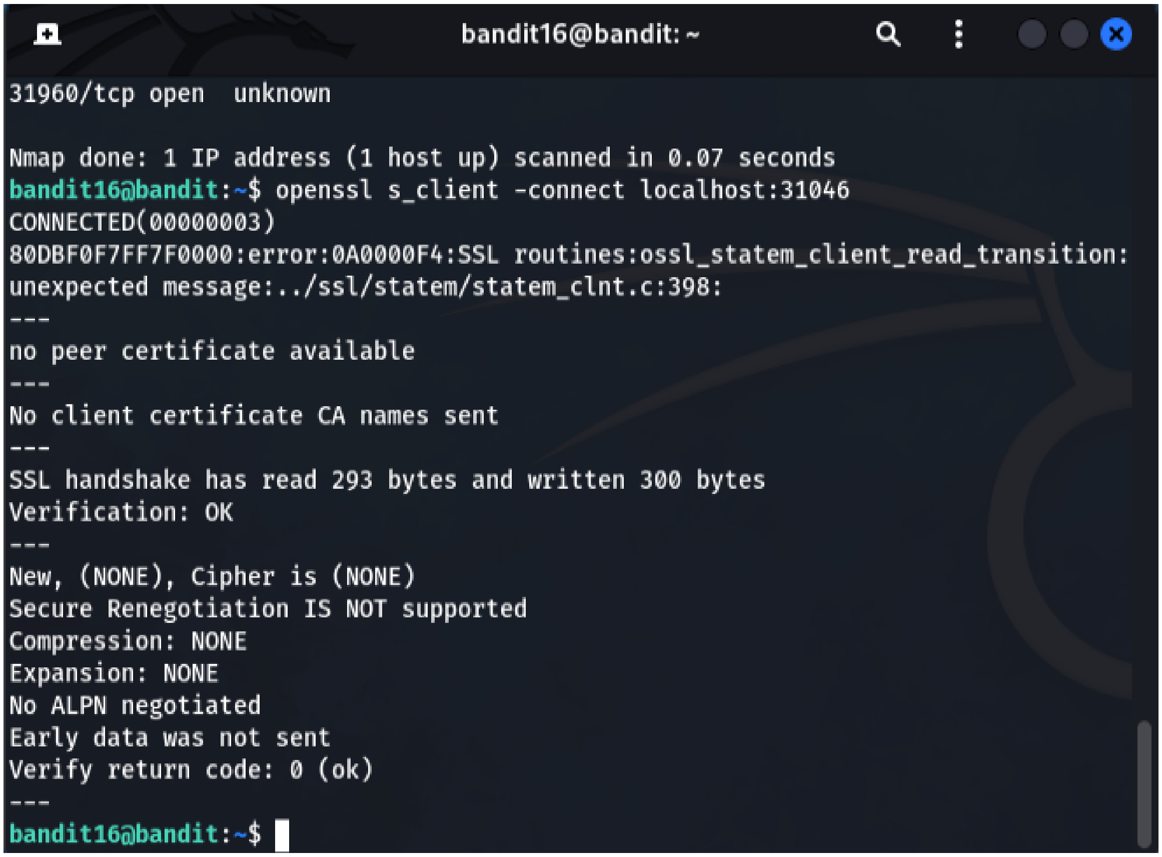
Commands you may need to solve this level.

ssh, telnet, nc, openssl, s_client, nmap

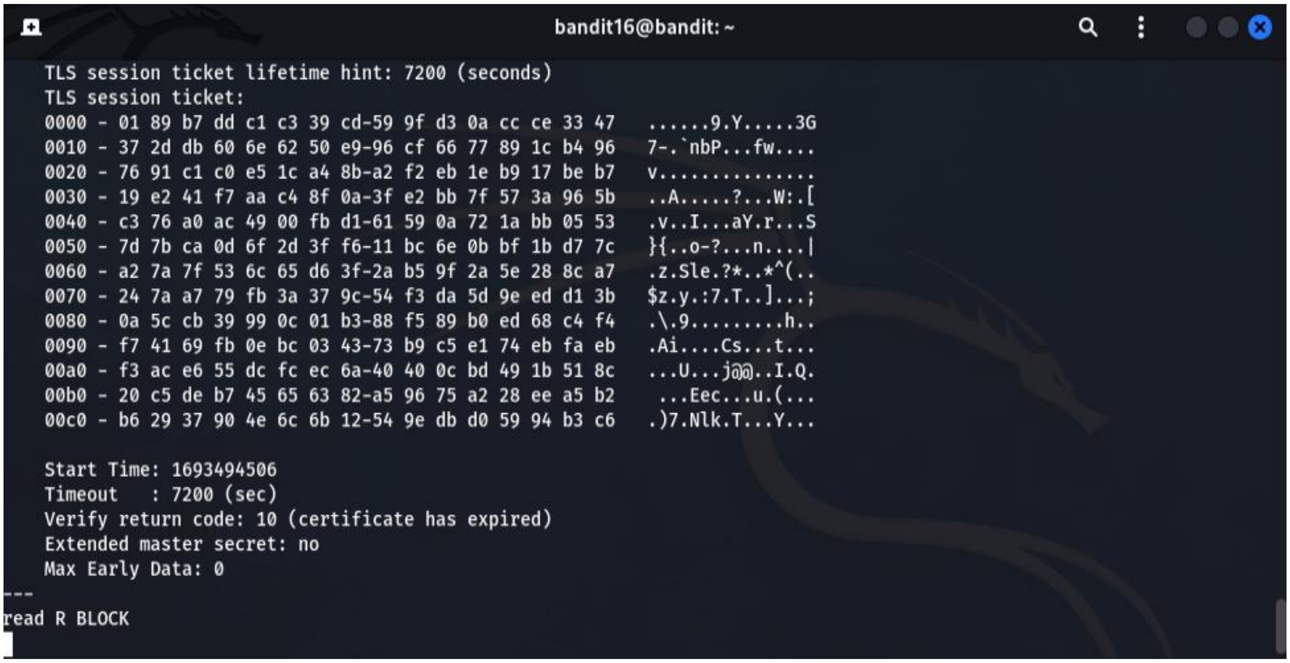
This is done in **kali Linux machine** because this level required to change permissions of the create file for that must use **chmod command** which is not supported by windows PowerShell



```
--[ More information ]--

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

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

  Enjoy your stay!

bandit16@bandit:~$ ls
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-31 15:02 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
bandit16@bandit:~$ 
```

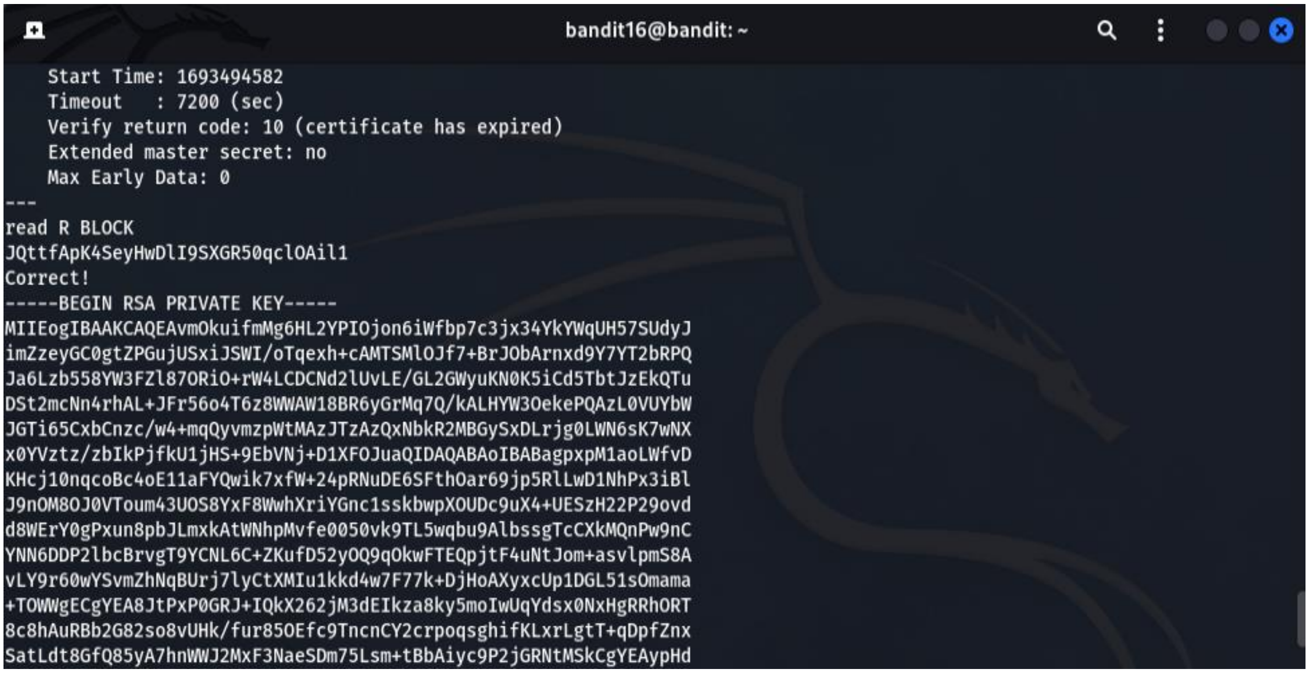


```
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
bandit16@bandit:~$ openssl s_client -connect localhost:31046
CONNECTED(00000003)
80DBF0F7FF7F0000:error:0A0000F4:SSL routines:ossl_statem_client_read_transition:
unexpected message:../ssl/statem/statem_clnt.c:398:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 293 bytes and written 300 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
bandit16@bandit:~$ 
```

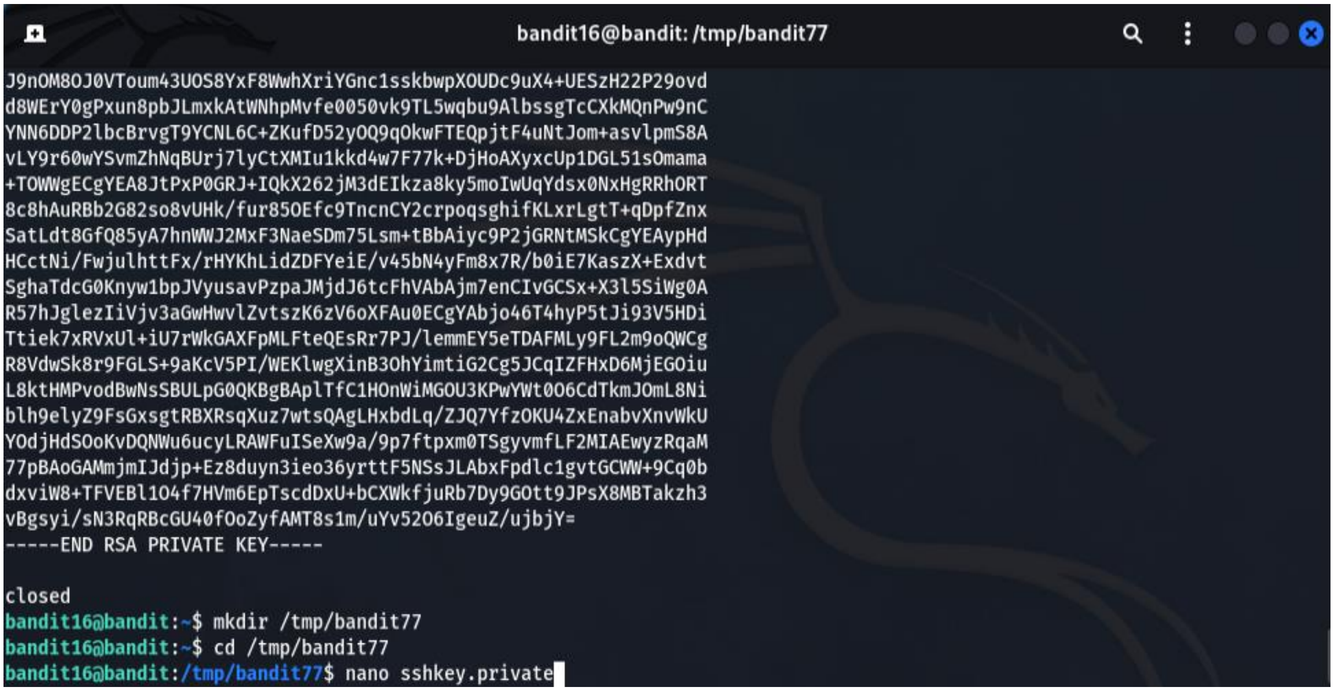


```
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 01 89 b7 dd c1 c3 39 cd-59 9f d3 0a cc ce 33 47   ......9.Y.....3G
    0010 - 37 2d db 60 6e 62 50 e9-96 cf 66 77 89 1c b4 96   7-.`nbP...fw....
    0020 - 76 91 c1 c0 e5 1c a4 8b-a2 f2 eb 1e b9 17 be b7   v...............
    0030 - 19 e2 41 f7 aa c4 8f 0a-3f e2 bb 7f 57 3a 96 5b   ..A.....?...W:.[
    0040 - c3 76 a0 ac 49 00 fb d1-61 59 0a 72 1a bb 05 53   .v..I...aY.r...S
    0050 - 7d 7b ca 0d 6f 2d 3f f6-11 bc 6e 0b bf 1b d7 7c   }{..o-?...n....|
    0060 - a2 7a 7f 53 6c 65 d6 3f-2a b5 9f 2a 5e 28 8c a7   .z.Sle.?*..*^(..
    0070 - 24 7a a7 79 fb 3a 37 9c-54 f3 da 5d 9e ed d1 3b   $z.y.:7.T..]...;
    0080 - 0a 5c cb 39 99 0c 01 b3-88 f5 89 b0 ed 68 c4 f4   .\.9.........h..
    0090 - f7 41 69 fb 0e bc 03 43-73 b9 c5 e1 74 eb fa eb   .Ai....Cs...t...
    00a0 - f3 ac e6 55 dc fc ec 6a-40 40 0c bd 49 1b 51 8c   ...U...j@@..I.Q.
    00b0 - 20 c5 de b7 45 65 63 82-a5 96 75 a2 28 ee a5 b2    ...Eec...u.(...
    00c0 - b6 29 37 90 4e 6c 6b 12-54 9e db d0 59 94 b3 c6   .)7.Nlk.T...Y...

    Start Time: 1693494506
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

In here password of the current level is given and press enter



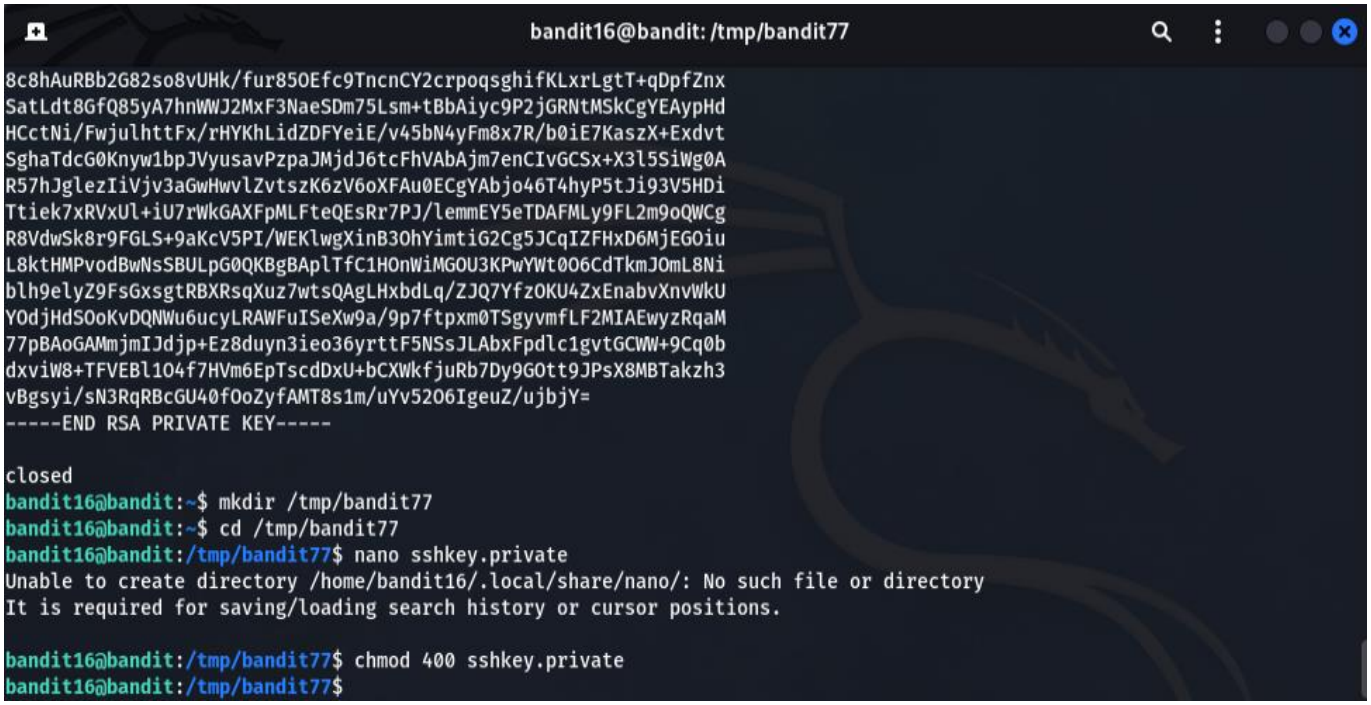
```
    Start Time: 1693494582
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
```



```
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit16@bandit:~$ mkdir /tmp/bandit77
bandit16@bandit:~$ cd /tmp/bandit77
bandit16@bandit:/tmp/bandit77$ nano sshkey.private
```

In here I am doing coping the entire private key and save it sshkey.private file

1. **mkdir /tmp/bandit77**
    - This command creates a new directory named "bandit77" inside the "/tmp" directory. The **/tmp** directory is commonly used to store temporary files and data.
2. **nano sshkey.private**
    - This command launches the **nano** text editor and opens a file named "sshkey.private" for editing. The **nano** text editor is a simple and user-friendly command-line text editor that allows you to view and modify the contents of files



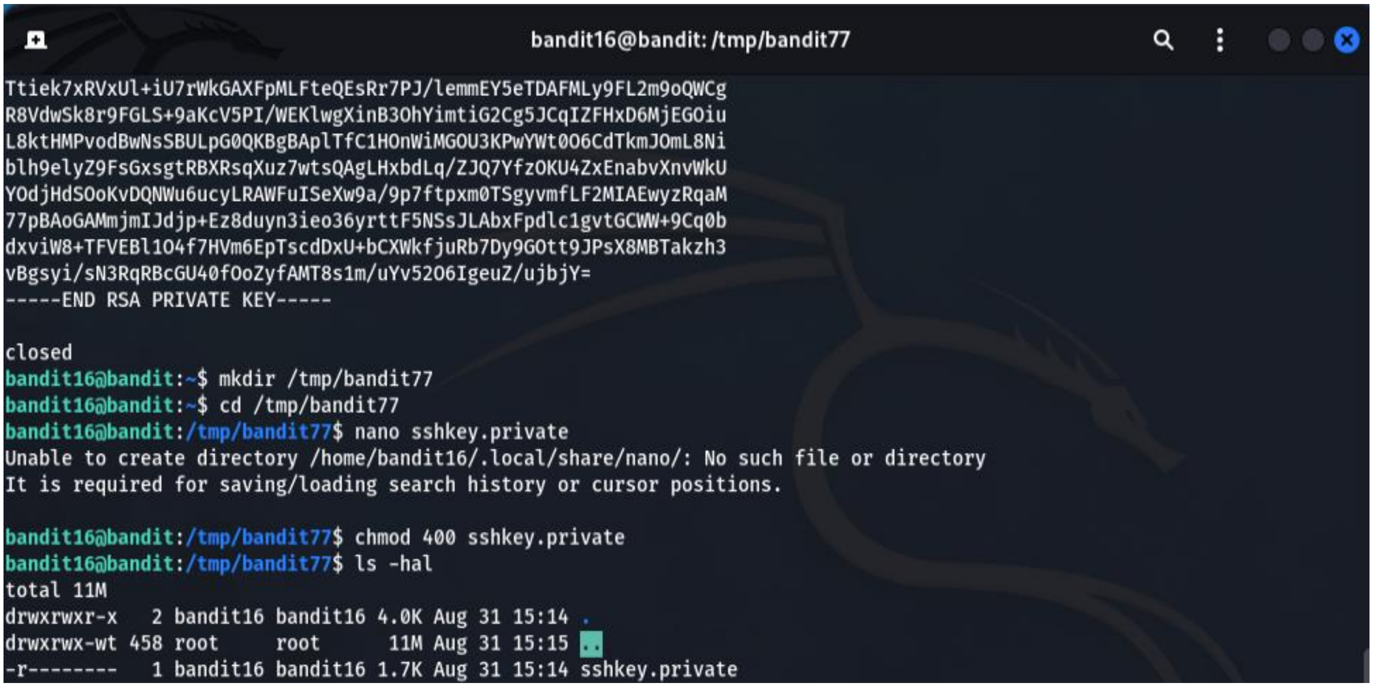
```
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit16@bandit:~$ mkdir /tmp/bandit77
bandit16@bandit:~$ cd /tmp/bandit77
bandit16@bandit:/tmp/bandit77$ nano sshkey.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/bandit77$ chmod 400 sshkey.private
bandit16@bandit:/tmp/bandit77$
```

chmod: This stands for "change mode.

400: This is the permission setting you're applying to the file

- The first digit (4) corresponds to the owner's permission.
- The second digit (0) corresponds to the group's permission.

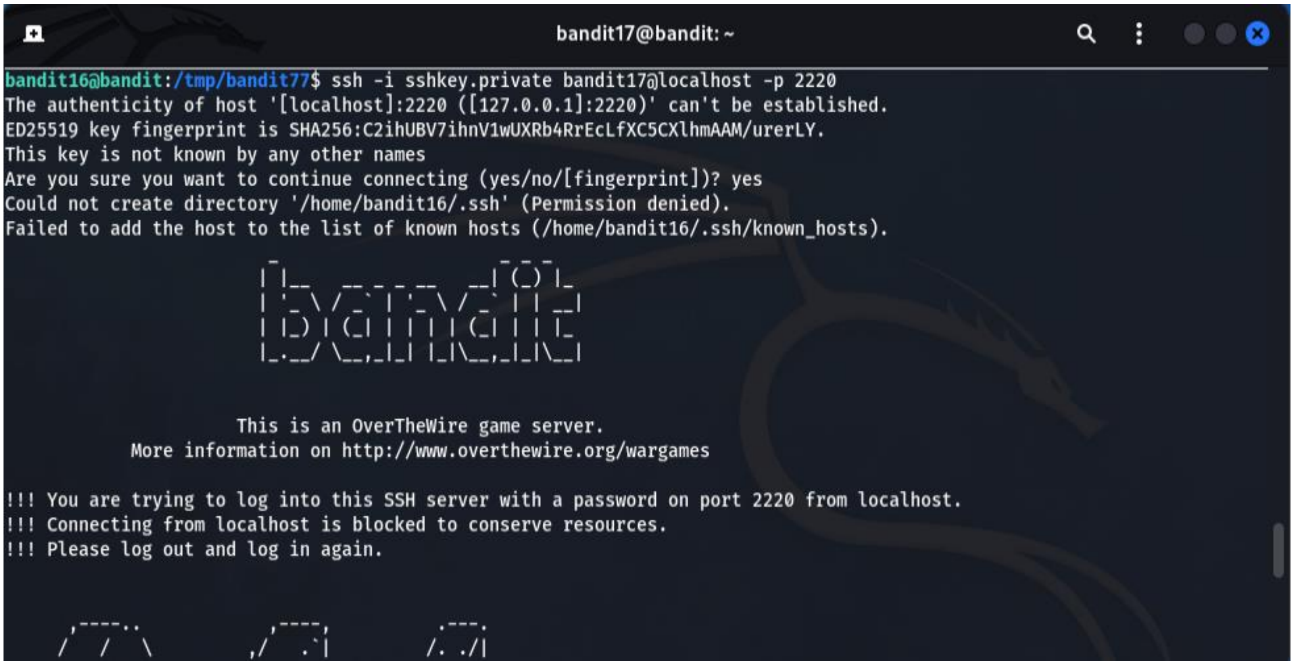
- The third digit (0) corresponds to others' permission.



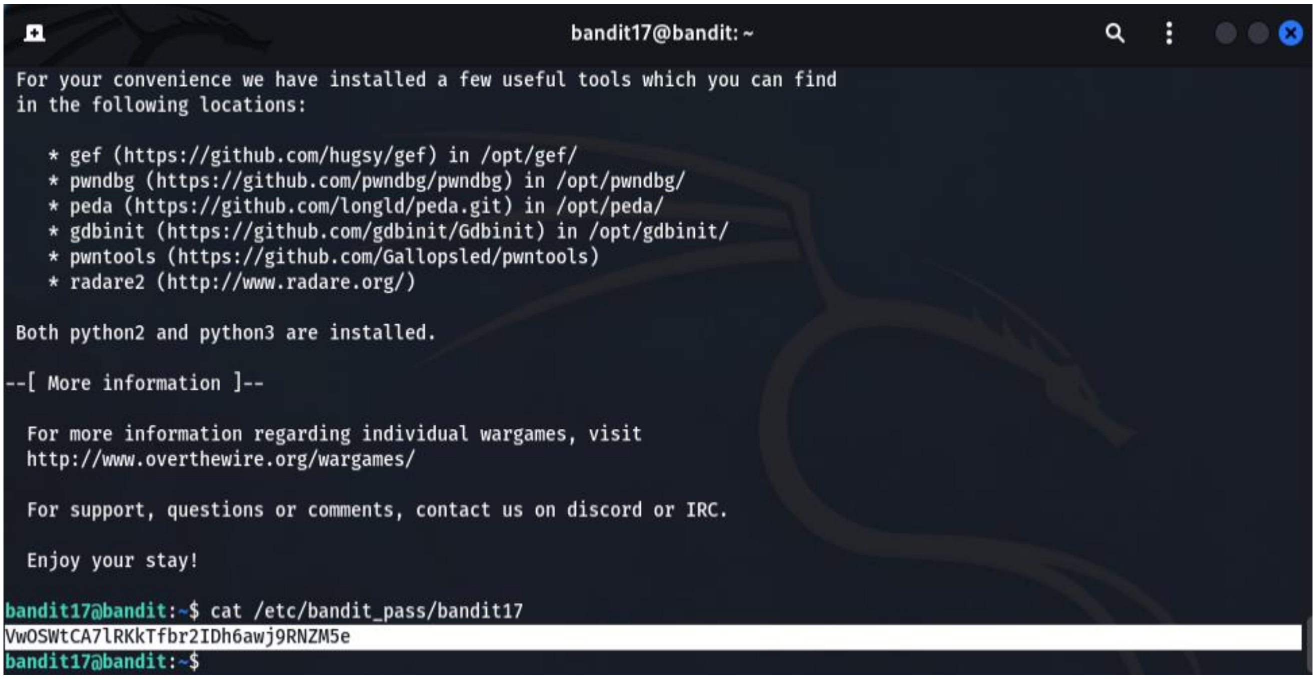
```
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit16@bandit:~$ mkdir /tmp/bandit77
bandit16@bandit:~$ cd /tmp/bandit77
bandit16@bandit:/tmp/bandit77$ nano sshkey.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/bandit77$ chmod 400 sshkey.private
bandit16@bandit:/tmp/bandit77$ ls -hal
total 11M
drwxrwxr-x   2 bandit16 bandit16 4.0K Aug 31 15:14 .
drwxrwx-wt 458 root     root      11M Aug 31 15:15 ..
-r--------   1 bandit16 bandit16 1.7K Aug 31 15:14 sshkey.private
```

ls – hal

- **ls**: This is the command used to list the contents of a directory.
- **-h**: This is an option that stands for "human-readable." It's used to make file sizes more readable by showing them in a format like "KB," "MB," etc., instead of just bytes.
- **-a**: This is an option that stands for "all." It's used to show hidden files and directories that start with a dot (.) in the listing.
- **-l**: This is an option that stands for "long." It's used to display detailed information about each file or directory, including permissions, owner, group, size, and modification date.



```
bandit16@bandit:/tmp/bandit77$ ssh -i sshkey.private bandit17@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' 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])? yes
Could not create directory '/home/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ssh/known_hosts).

                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.


     ,----..            ,----,          .---.
    /   /   \         ,/   .`|         /. ./|
```



```
 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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e
bandit17@bandit:~$
```

Level 17→Level 18

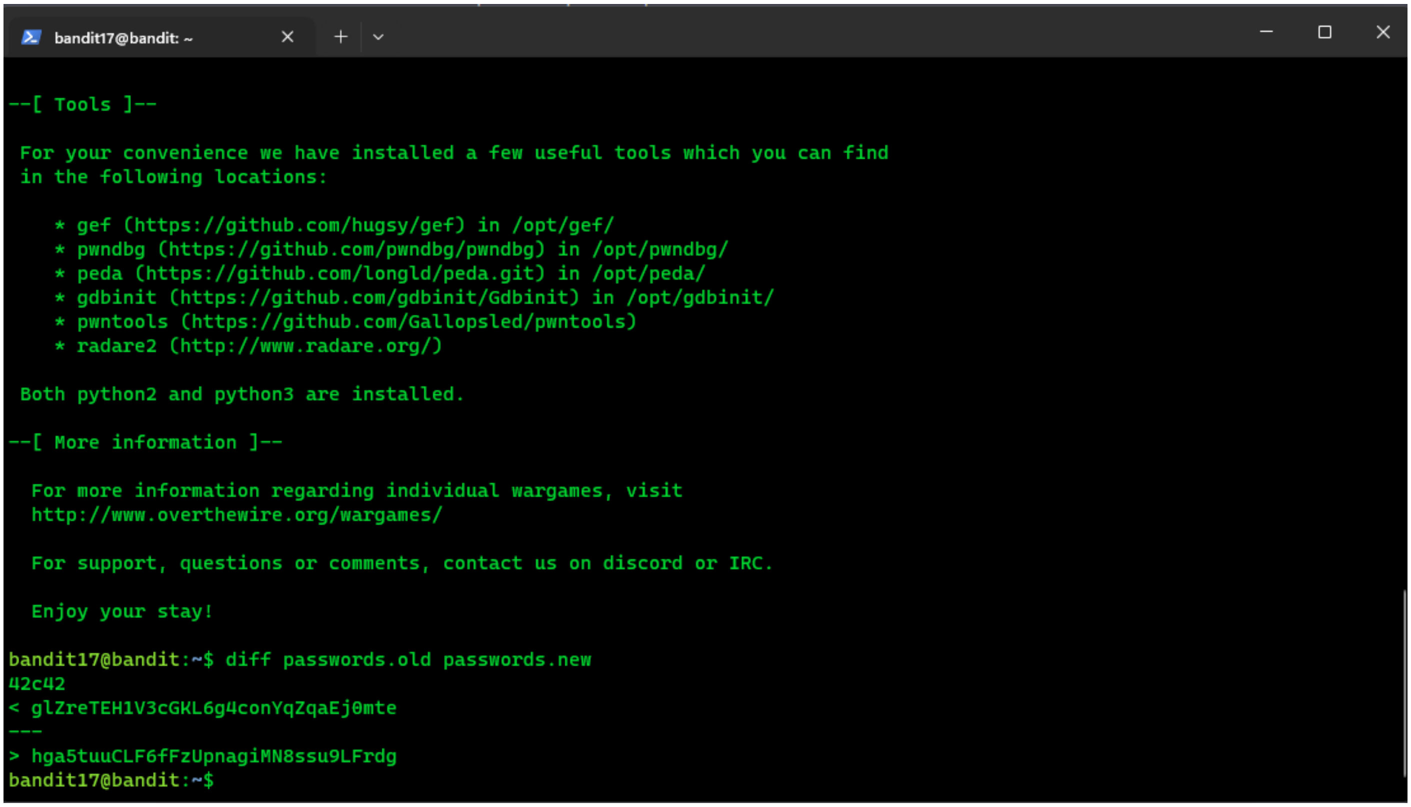
Level Goal

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, bandit19

Commands you may need to solve this level.

cat, grep, ls, diff

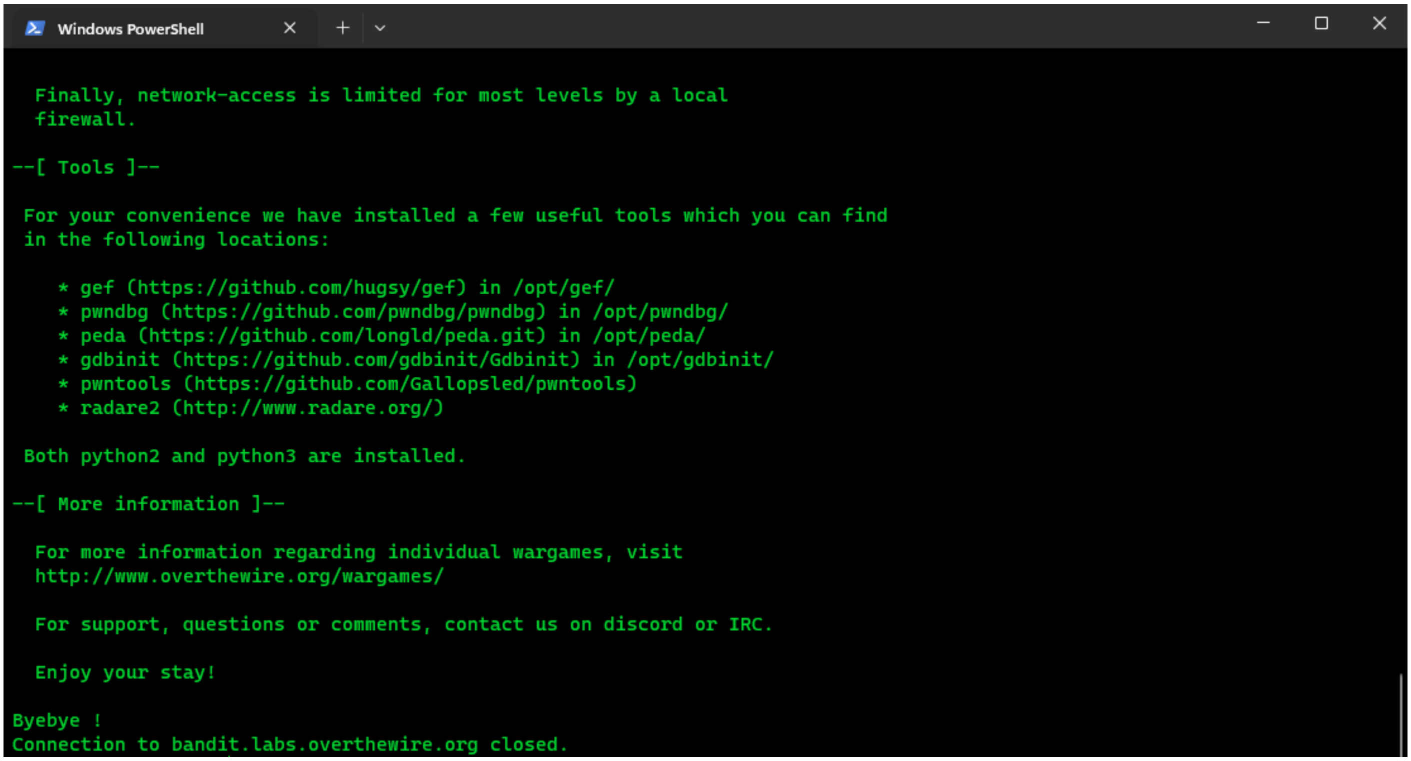


```
--[ Tools ]--

 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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< glZreTEH1V3cGKL6g4conYqZqaEj0mte
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$
```

diff passwords.old and passwords.new

- **diff**: This is the command used to compare files and display the differences between them.

- **passwords.old** and **passwords.new**: These are the names of the two files you want to compare. The first file is "passwords.old," and the second file is "passwords.new



```
  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/)

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.
```

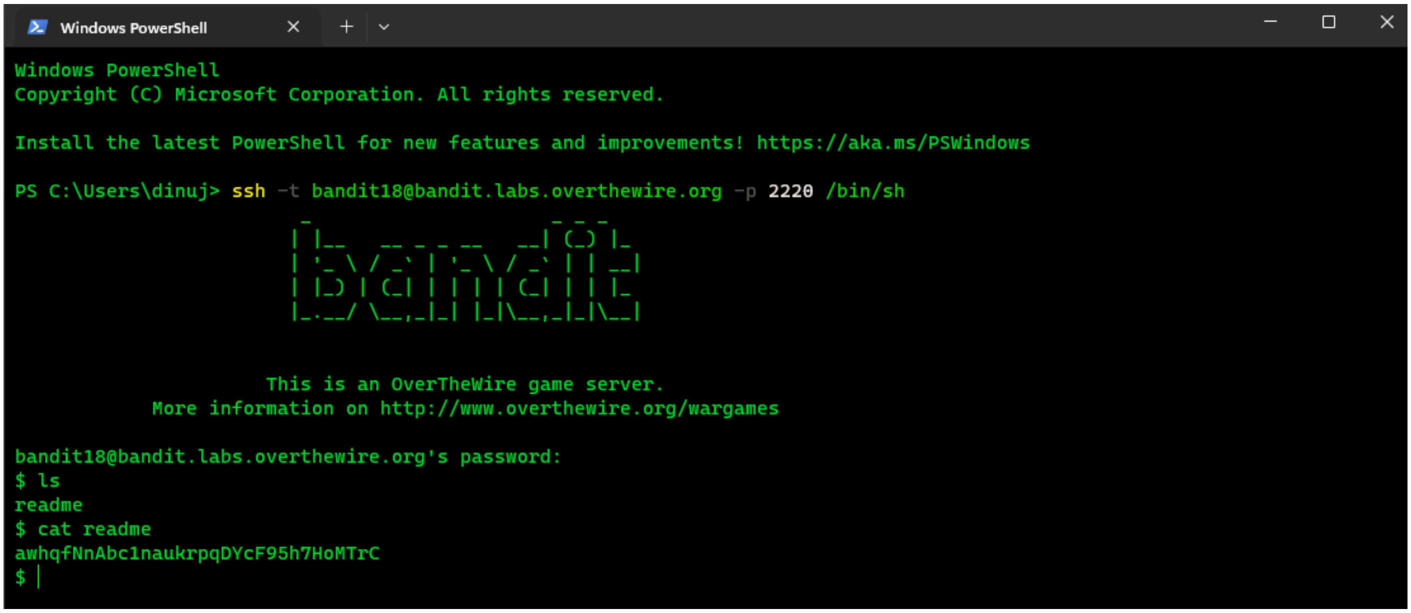
Level 18→Level 19

Level Goal

The password for the next level is stored in a file **readme** in the homedirectory. Unfortunately, someone has modified. bashrc to log you out when you log in with SSH.

Commands you may need to solve this level.

ssh, ls, cat



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\dinuj> ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit18@bandit.labs.overthewire.org's password:
$ ls
readme
$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
$ |
```

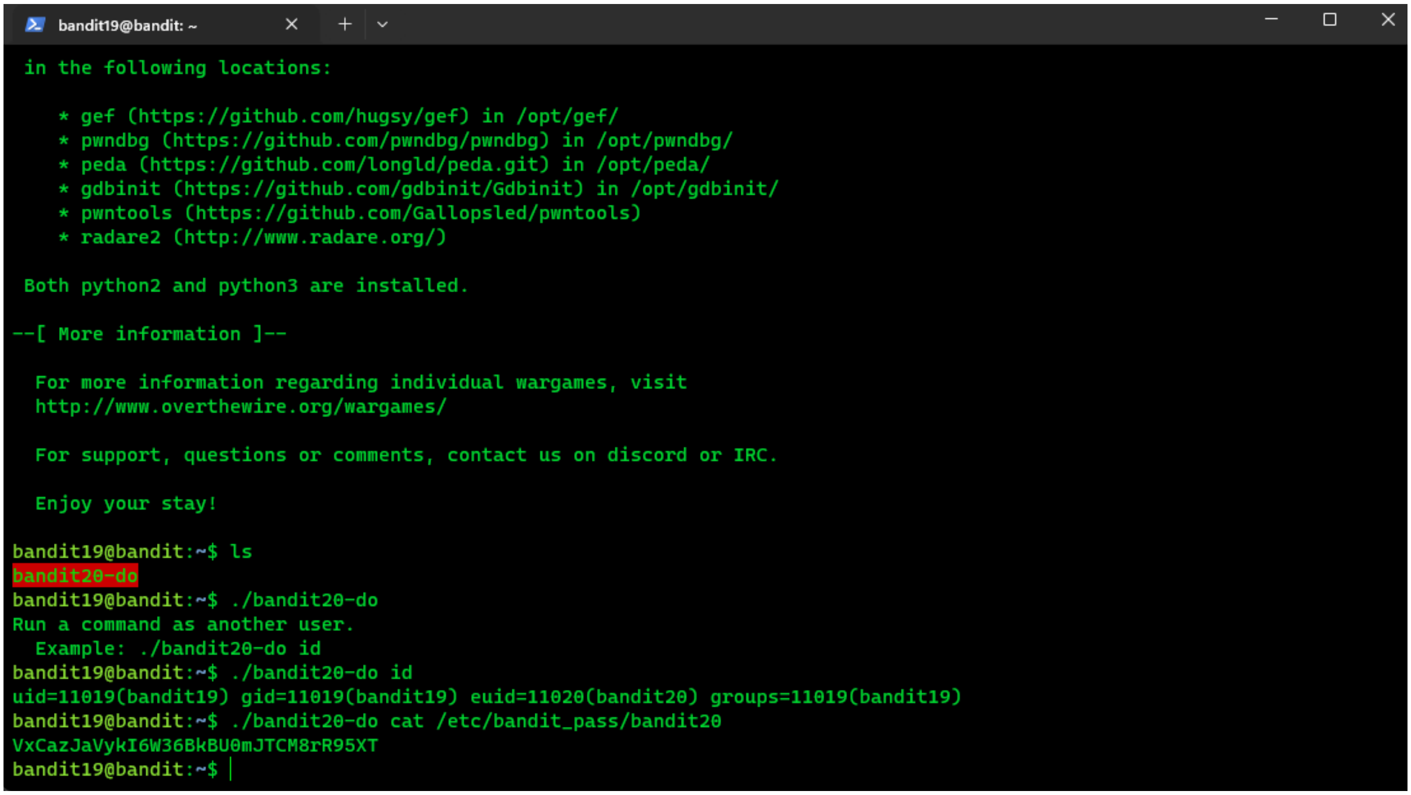
ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh

- **ssh**: This is the command used to establish a Secure Shell (SSH) connection to a remote server.
- **-t**: This is an option used with the SSH command to allocate a pseudo-terminal. It's often used when you want to run interactive commands on the remote server.
- **-p 2220**: This is an option that specifies the port number to use for the SSH connection. The default SSH port is 22, but here you're explicitly specifying port 2220.
- **/bin/sh**: This is the shell command you're instructing SSH to run on the remote server. In this case, you're running the **/bin/sh** shell, which is a basic Unix shell

Level 19→Level 20

Level Goal

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.



```
 in the following locations:

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

 Both python2 and python3 are installed.

--[ More information ]--

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

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

  Enjoy your stay!

bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$ 
```

- **./bandit20**: This is executing a program or script named "bandit20" in the current directory. The **./** indicates that the program is located in the current directory.
- **-do**: These are likely options or arguments for the "bandit20" program.

Level 20→Level 21

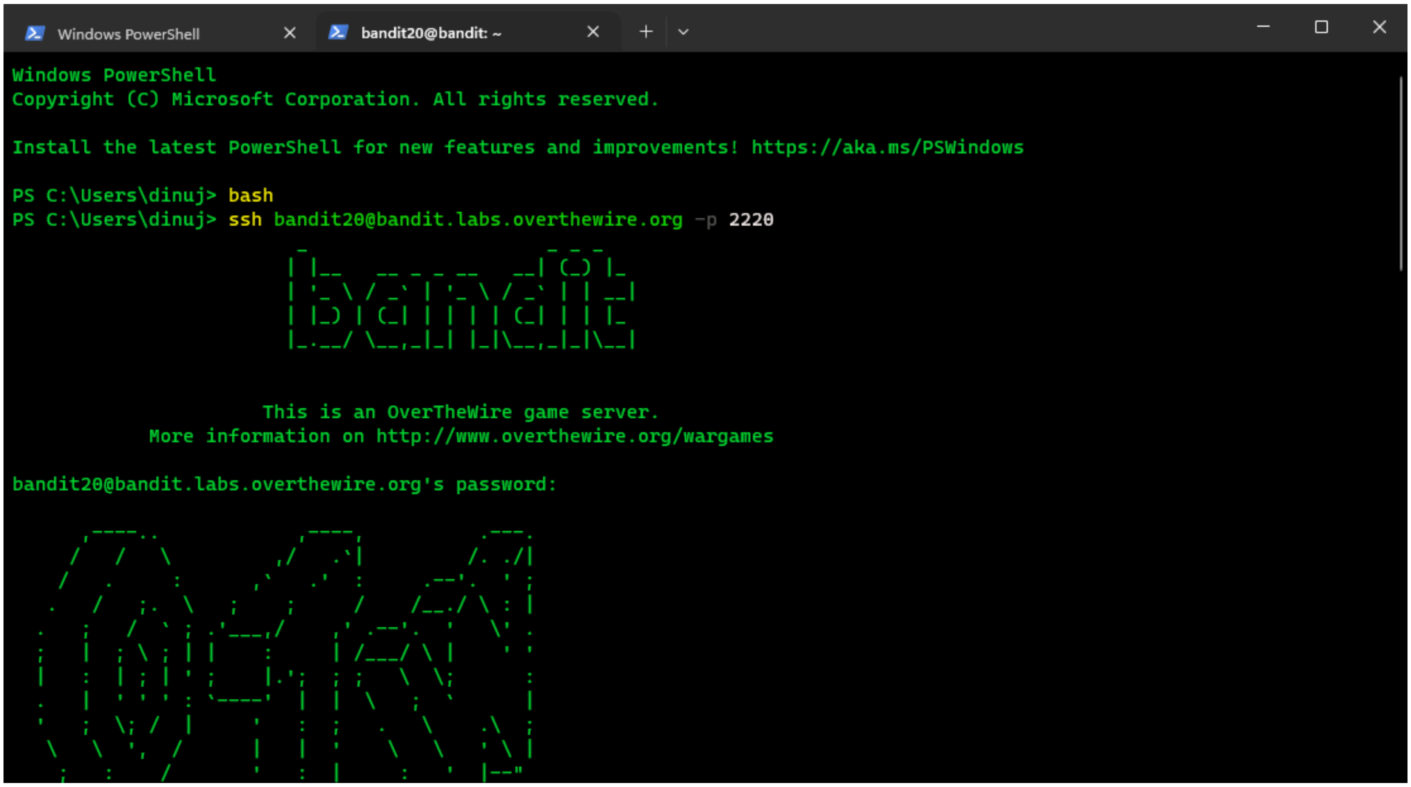
Level Goal

There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

Commands you may need to solve this level.

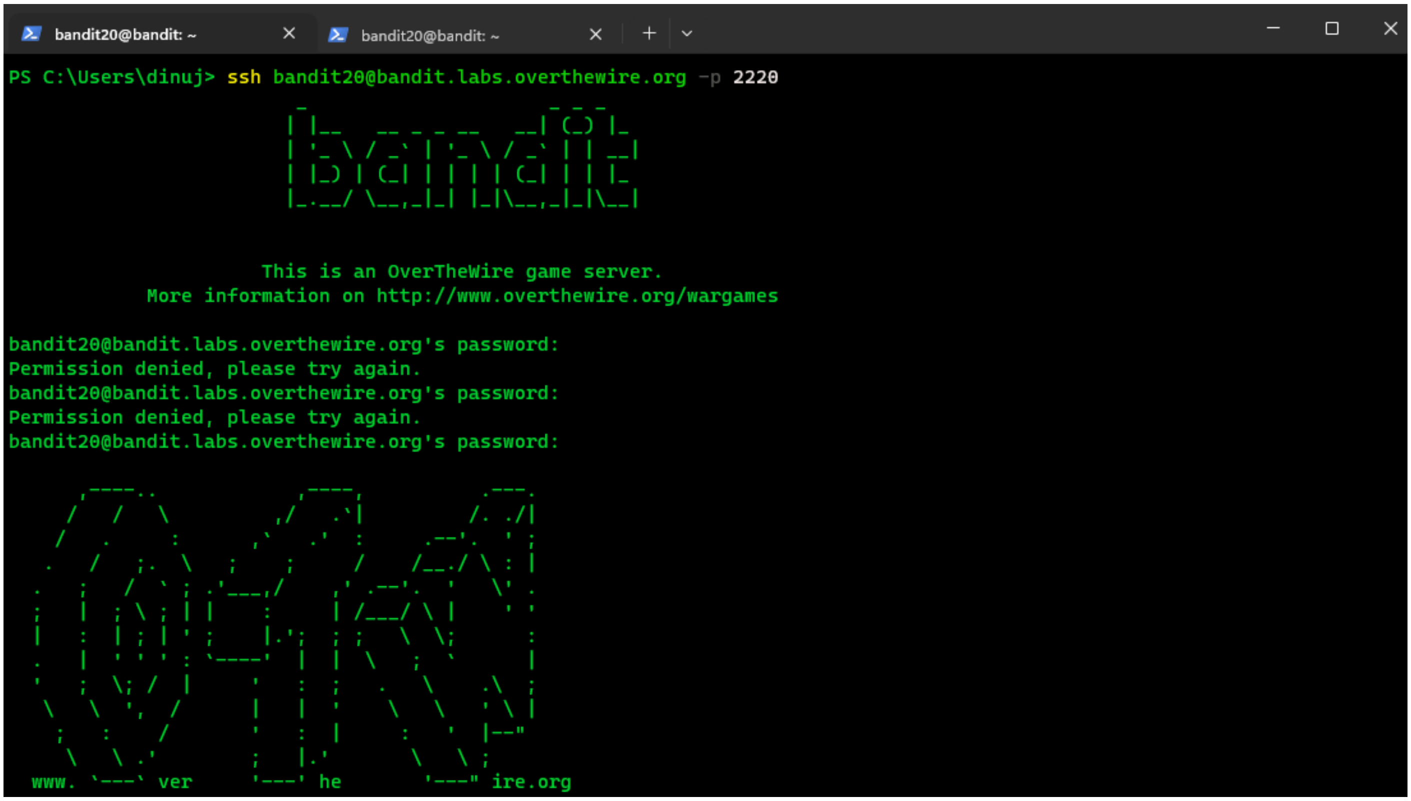
ssh, nc, cat, bash, screen, tmux, Unix 'job control' (bg, fg, jobs, &, CTRL-Z, …)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\dinuj> bash
PS C:\Users\dinuj> ssh bandit20@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit20@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
```

In this is we have to open two terminals one started with bash

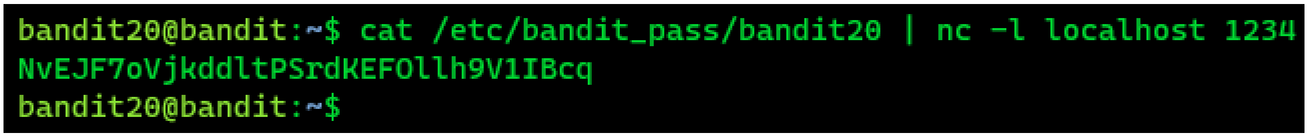
And a terminal without the bash command at the beginning



```
PS C:\Users\dinuj> ssh bandit20@bandit.labs.overthewire.org -p 2220
                        _                     _ _ _
                       | |__   __ _ _ __   __| (_) |_
                       | '_ \ / _` | '_ \ / _` | | __|
                       | |_) | (_| | | | | (_| | | |_
                       |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit20@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit20@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit20@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org
```

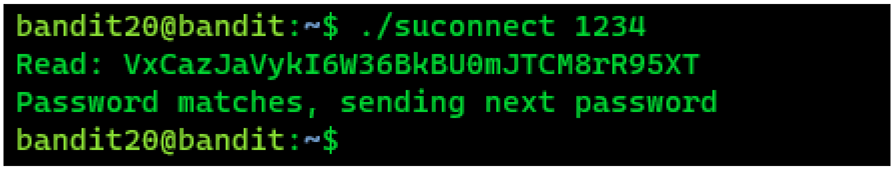
And after login with the new terminal too you must type the following commands with the terminal started with the bash.

cat /etc/badit_pass/bandit20 | nc -l localhost -p 1234



```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost 1234
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
bandit20@bandit:~$
```

Once the above command is typed and press enter in the second terminal where we started normally without bash you must type the following command

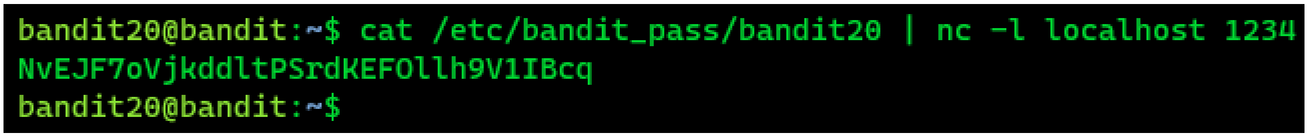


```
bandit20@bandit:~$ ./suconnect 1234
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
bandit20@bandit:~$
```

Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT

Password matches, sending next password

Read means the terminal has read the password of the current level and states that it matches **Password matches** and **sending next password** means sending the next level's password for the other terminal.



```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost 1234
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
bandit20@bandit:~$
```

Next levels password = NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

Passwords for all the levels

level 1	NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
level 2	rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
level 3	aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
level 4	2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
level 5	lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
level 6	P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
level 7	z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
level 8	TESKZC0XvTetK0S9xNwm25STk5iWrBvP
level 9	EN632PlfYiZbn3PhVK3XOGSlNInNE00t
level 10	G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
level 11	6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
level 12	JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
level 13	wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
level 14	fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
level 15	jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
level 16	JQttfApK4SeyHwDlI9SXGR50qclOAil1
level 17	VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e
level 18	hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
level 19	awhqfNnAbc1naukrpqDYcF95h7HoMTrC
level 20	VxCazJaVykI6W36BkBU0mJTCM8rR95XT
level 21	NvEJF7oVjkddltPSrdKEFOllh9V1IBcq