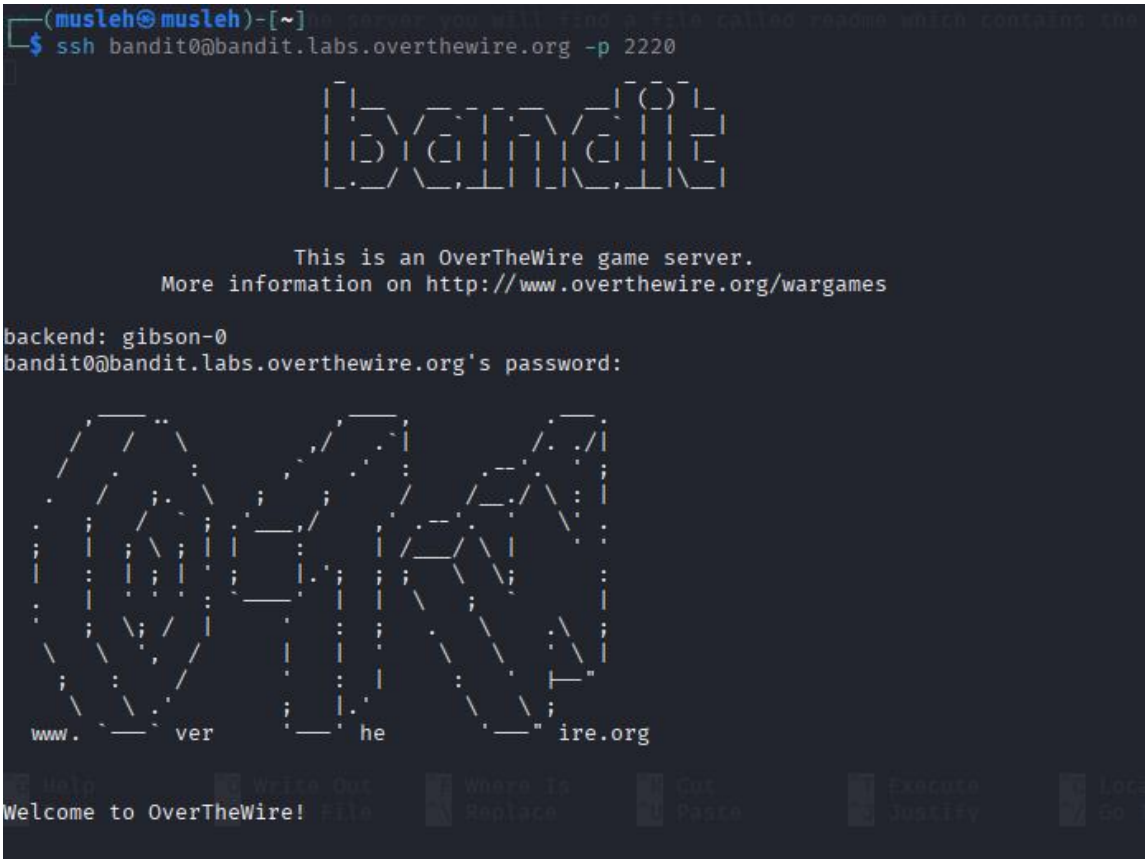
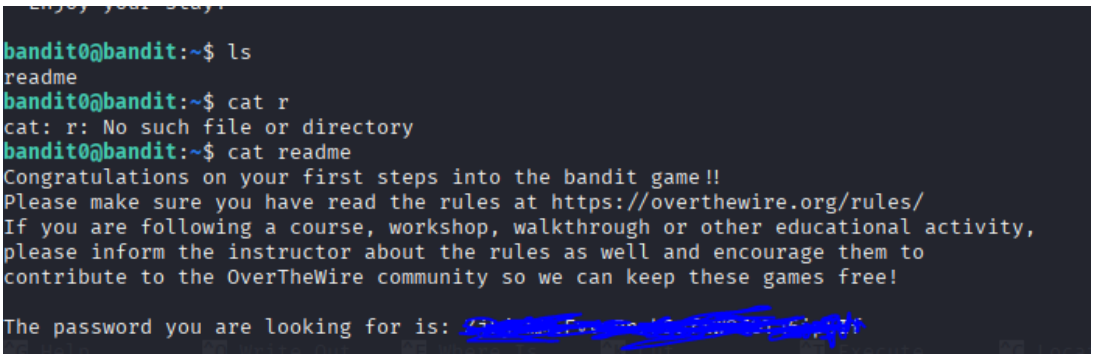
Bandit Writeup: OverTheWire Walkthrough

Level 0 → Level 1

Goal: Log into the game using SSH.





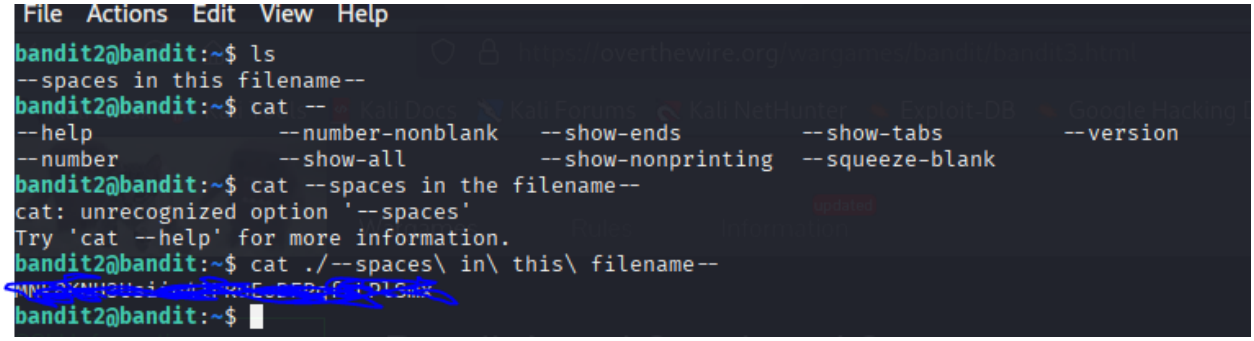
Level 1 → Level 2

Goal: The password is stored in a file called `readme` in the home directory.

Basic file navigation and reading. The `cat` command is used to concatenate and print file contents to the standard output (your terminal).

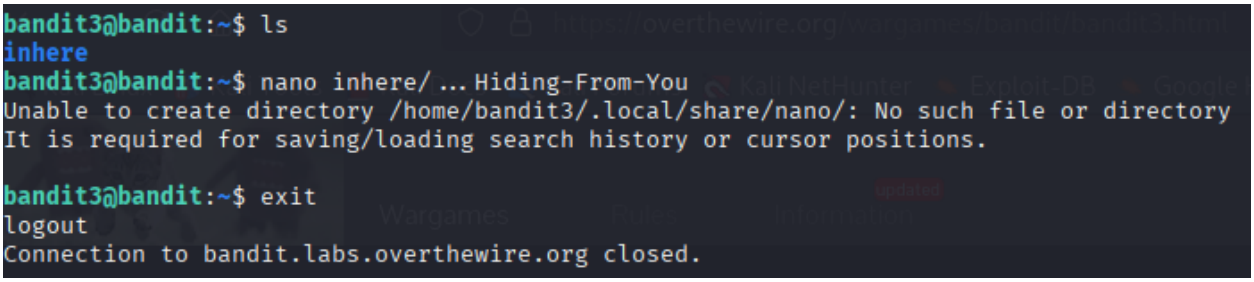
Level 2 → Level 3

The password is in a file named `-`



Handling special characters in filenames. The hyphen (`-`) is normally interpreted by the shell as an indicator for a command-line option. Prefixing it with `./` explicitly tells the command that it's a file in the current directory

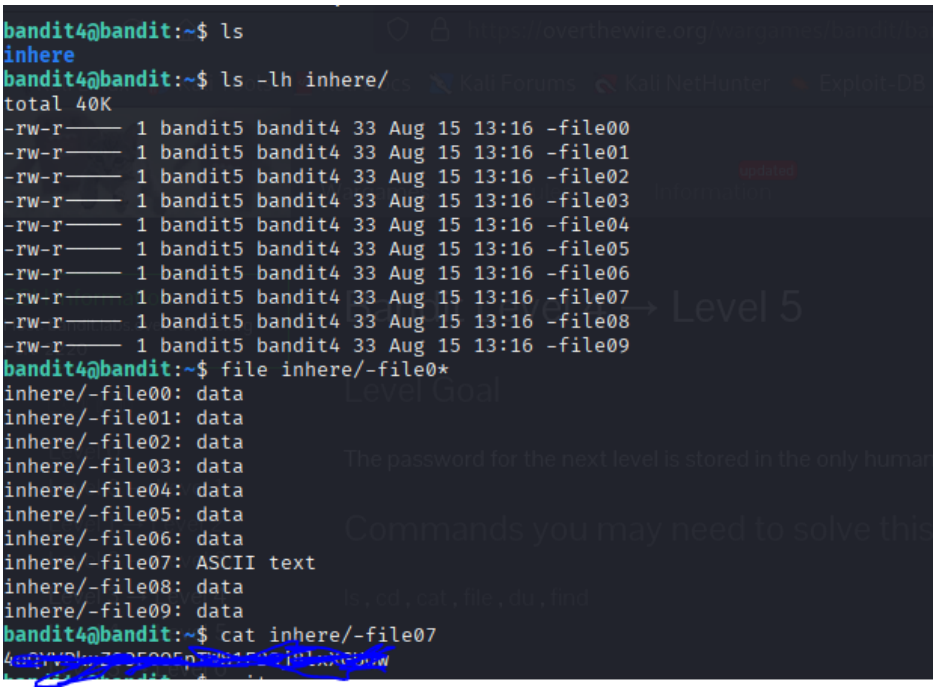
Level 3 → Level 4



How to handle filenames containing spaces or special characters. The shell uses spaces to separate arguments, so enclosing the entire filename in quotes tells the shell to treat it as a single argument

Level 4 → Level 5

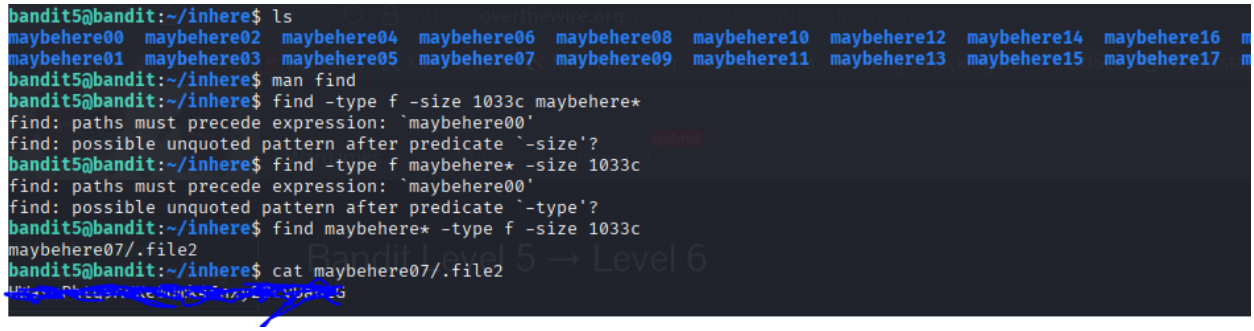
Goal: The password is in a hidden file in the `inhere` directory.



Hidden files in Linux. Files and directories whose names begin with a dot (.) are hidden by default. The `ls -a` command is used to reveal them, a common practice for storing configuration files.

Level 5 → Level 6

Goal: The password is in the only human-readable file in the `inhere` directory.

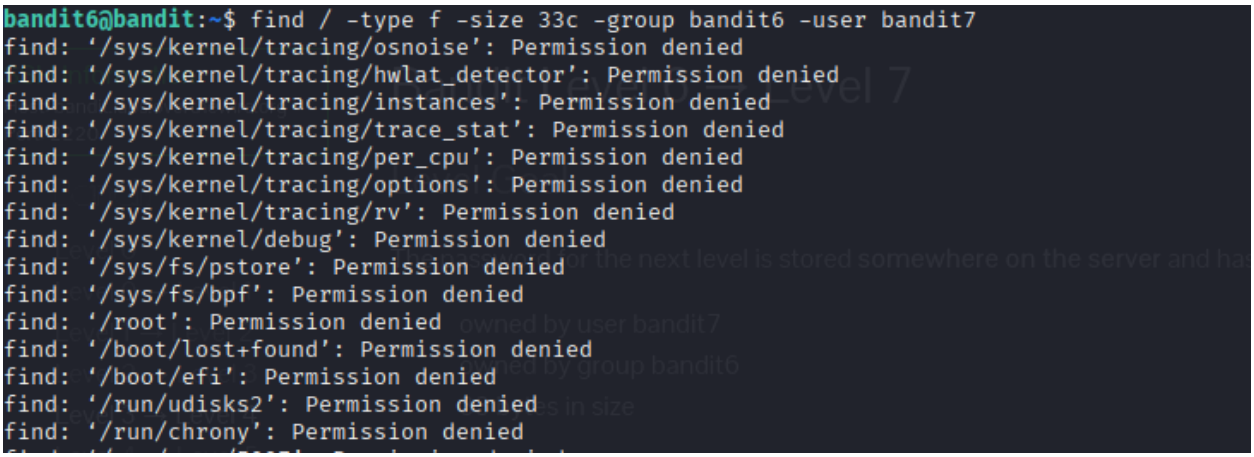


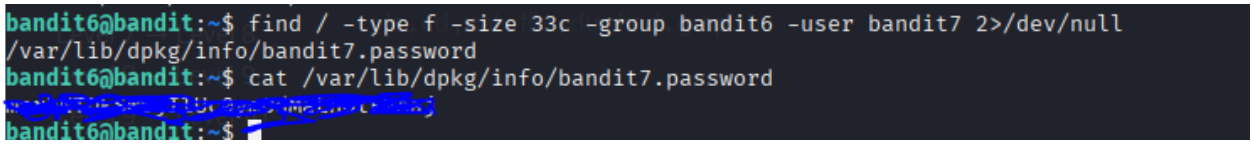
Identifying file types. The `file` command is crucial for determining what type of data a file contains (e.g., text, binary, executable), especially when file extensions are missing or misleading.

Level 6 → Level 7

Goal: Find a file somewhere under the `inhere` directory with the properties:

- Human-readable
- 1033 bytes in size
- Not executable

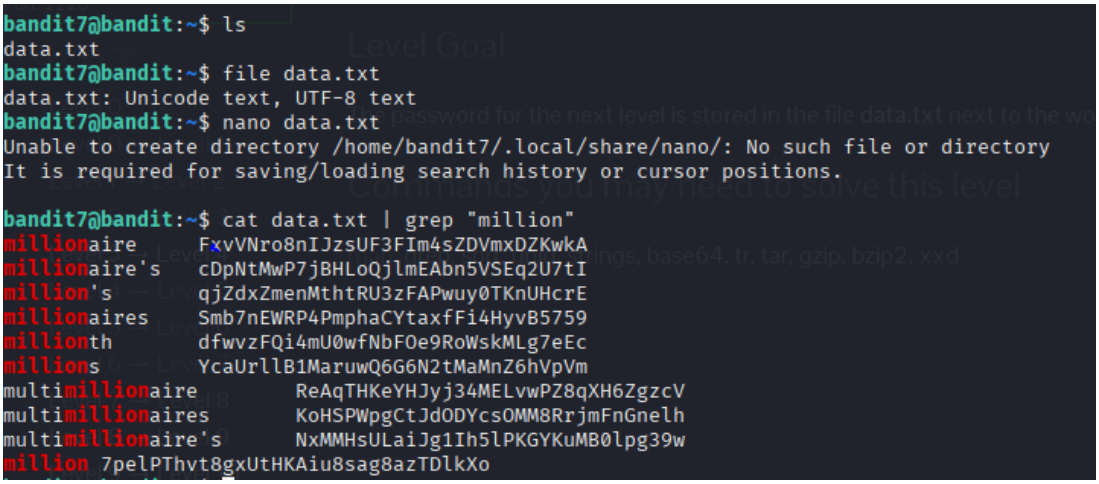




Advanced file searching with `find`. This powerful command can locate files based on a wide array of criteria like type (`-type f`), size (`-size`), and permissions (`! -executable`).

Level 7 → Level 8

Goal: Find a file on the server owned by user `bandit7`, group `bandit6`, and is 33 bytes in size.



System-wide searching and error handling. Searching the entire filesystem (`/`) will generate "Permission denied" errors. Redirecting these errors to `/dev/null` (`2>/dev/null`) cleans up the output, showing only relevant results.

Level 8 → Level 9

Goal: The password is in `data.txt` next to the word `millionth`

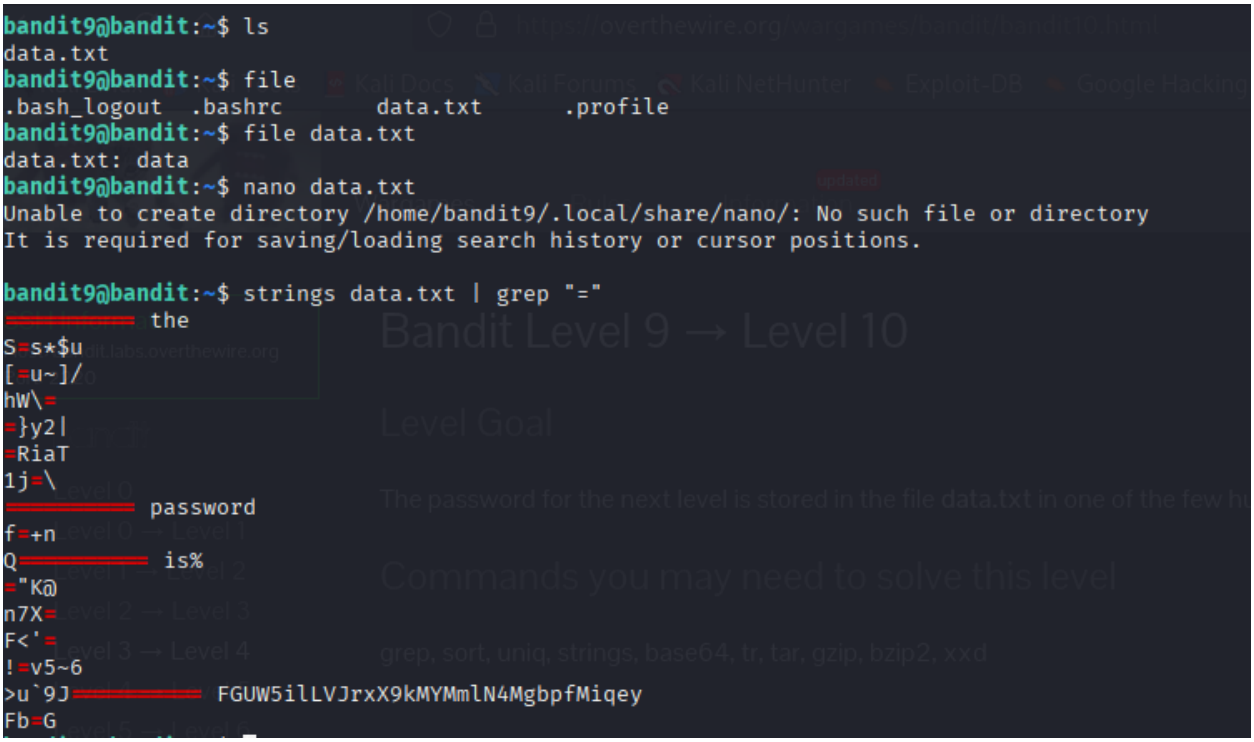
```
bandit8@bandit:~$ ls -lh
total 36K
-rw-r----- 1 bandit9 bandit8 33K Aug 15 13:16 data.txt
bandit8@bandit:~$ file data.txt
data.txt: ASCII text
bandit8@bandit:~$ nano data.txt
Unable to create directory /home/bandit8/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit8@bandit:~$ sort -d data.txt>sort.txt
-bash: sort.txt: Permission denied
bandit8@bandit:~$ mktemp -d
/tmp/tmp.FkxTsLIPcJ
bandit8@bandit:~$ cd /tmp/tmp.FkxTsLIPcJ && touch sort.txt
bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ nano /home/bandit8/data.txt
Unable to create directory /home/bandit8/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ cat /home/bandit8/data.txt
```

```
bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ nano sort.txt
Unable to create directory /home/bandit8/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ sort -d sort.txt >sorted.txt
bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ nano sorted.txt
Unable to create directory /home/bandit8/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$ uniq -u sorted.txt
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:/tmp/tmp.FkxTsLIPcJ$
```

Pattern searching with `grep`. This is an essential tool for filtering text and searching for specific patterns or words within files, especially large ones where manual searching is impractical.

Level 9 → Level 10

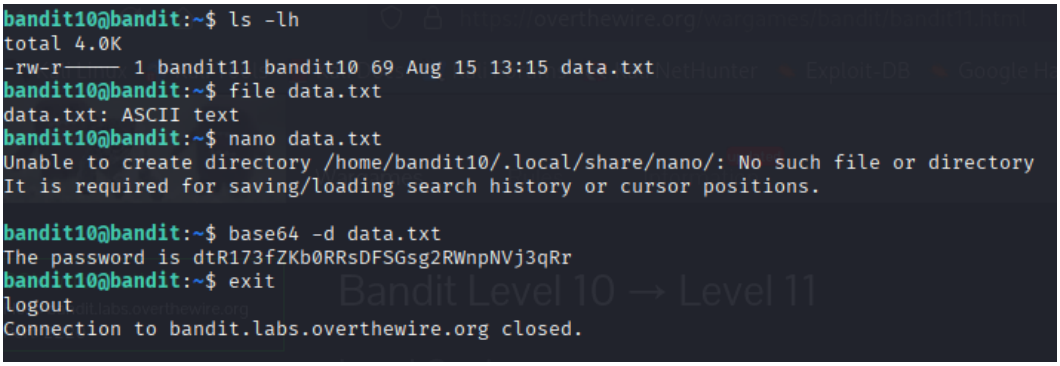
Goal: The password in `data.txt` is the only line of text that occurs only once.



Data processing and filtering. The `sort` command orders lines, which allows `uniq` to work correctly by comparing adjacent lines. The `-u` flag for `uniq` prints only unique lines, instantly revealing the password

Level 10 → Level 11

Goal: The password in `data.txt` is a human-readable string preceded by several '=' characters.



Extracting text from binaries. The `strings` command pulls out human-readable characters from any file type. Piping its output to `grep` allows for easy pattern matching to find the desired data.

Level 11 → Level 12

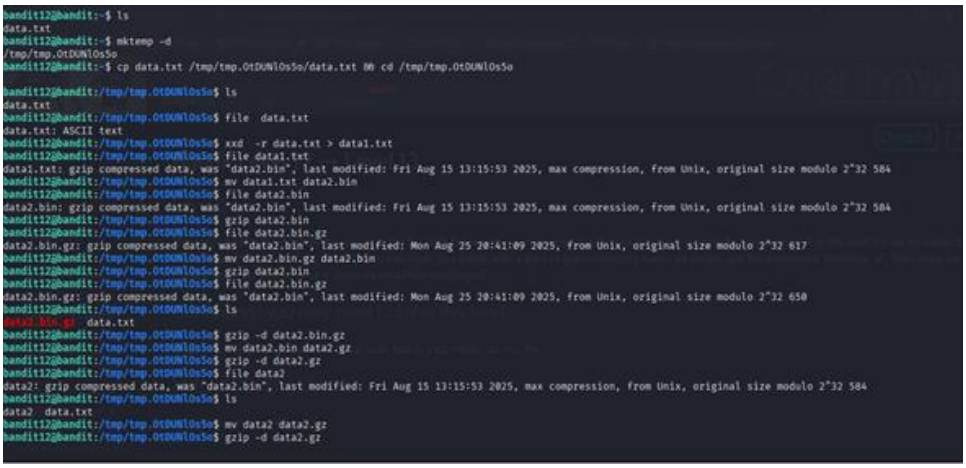
Goal: All lowercase and uppercase letters in `data.txt` have been rotated by 13 positions (ROT13 cipher).

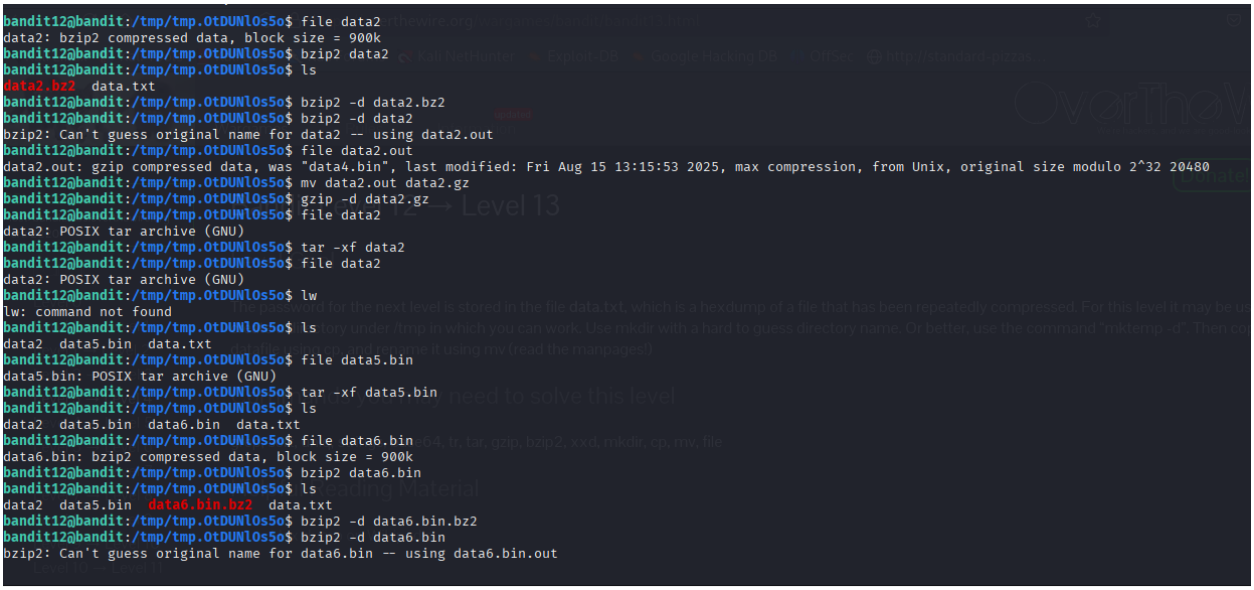
```
bandit11@bandit:~$ ls -lh
total 4.0K
-rw-r----- 1 bandit12 bandit11 49 Aug 15 13:15 data.txt
bandit11@bandit:~$ file data.txt
data.txt: ASCII text
bandit11@bandit:~$ nano data.txt
Unable to create directory /home/bandit11/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit11@bandit:~$ echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ mktemp -d
/tmp/tmp.RamA78SWve
bandit11@bandit:~$ cd /tmp/tmp.RamA78SWve && nano rot.txt

Unable to create directory /home/bandit11/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit11@bandit:/tmp/tmp.RamA78SWve$  tr 'A-Za-z' 'N-ZA-Mn-za-m' rot.txt >rot2.txt
tr: extra operand ‘rot.txt’
Try 'tr --help' for more information.
bandit11@bandit:/tmp/tmp.RamA78SWve$ tr 'A-Za-z' 'N-ZA-Mn-za-m' rot.txt rot2.txt
tr: extra operand ‘rot.txt’
Try 'tr --help' for more information.
bandit11@bandit:/tmp/tmp.RamA78SWve$ tr 'A-Za-z' 'N-ZA-Mn-za-m' Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
tr: extra operand ‘Gur’
Try 'tr --help' for more information.
bandit11@bandit:/tmp/tmp.RamA78SWve$ echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4 |tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7×16WNeHIi5YkIhWsfFIqoognUTyj9Q4
```

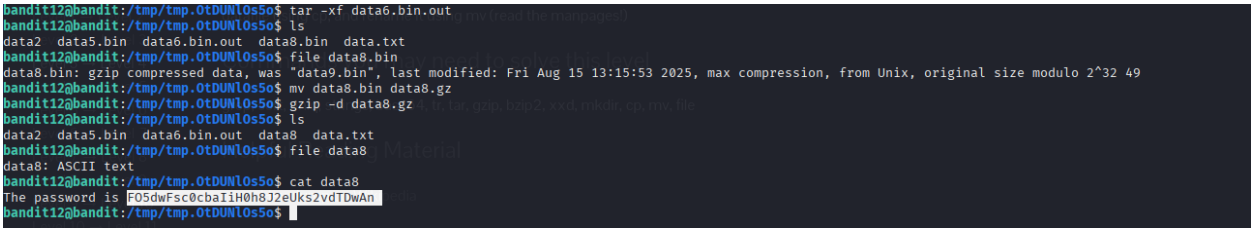
Basic cryptography and character translation. The `tr` (translate) command is used for simple substitution ciphers like ROT13, which is its own inverse (applying it twice decodes the message).

Level 12 → Level 13

The file `data.txt` is a hexdump of a repeatedly compressed file. Extract the password.



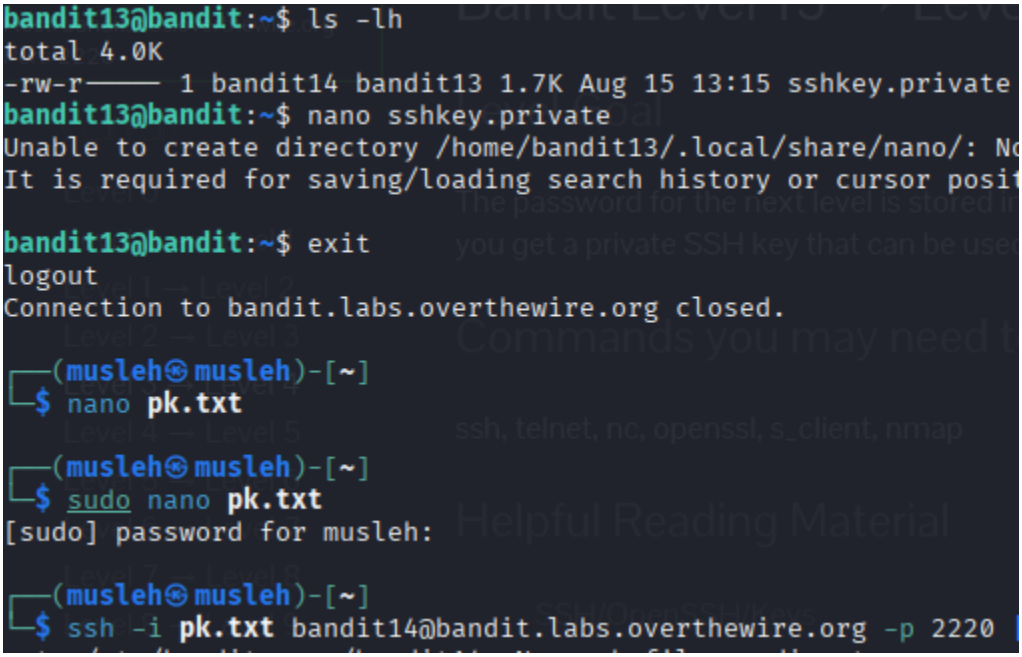


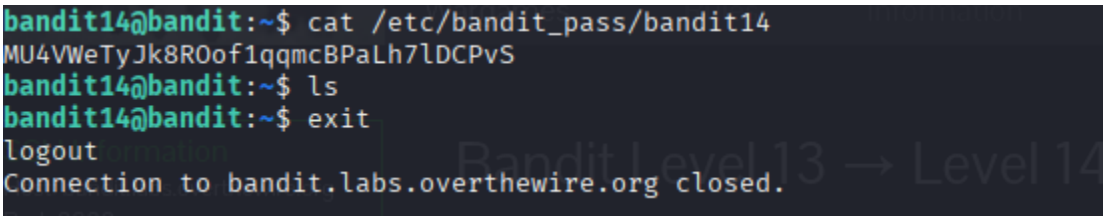


File compression, archiving, and format recognition. This level is a puzzle that requires understanding various compression utilities (`gzip`, `bzip2`, `tar`) and using tools like `file` and `xxd` to identify and reverse data transformation steps.

Level 13 → Level 14

You are given a private SSH key to log into the next level. The password for bandit14 is in `/etc/bandit_pass/bandit14`





SSH key-based authentication. This is a more secure method than passwords for logging into remote systems. The critical step is protecting the private key file with correct permissions (`chmod 600`) to prevent other users on your system from reading it

Level 14 → Level 15

Goal: Submit the current level's password to port 30000 on localhost.

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ nc localhost 30000

Wrong! Please enter the correct current password.

bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

Basic network communication with Netcat (`nc`). Netcat is a versatile tool for reading from and writing to network connections. This simulates sending data to a network service listening on a specific port.

Level 15 → Level 16

Goal: Submit the current level's password to port 30001 on localhost using SSL encryption.

```
bandit15@bandit:~$ ls -alh
total 24K
drwxr-xr-x   2 root     root     4.0K Aug 15 13:15 .
drwxr-xr-x 150 root     root     4.0K Aug 15 13:18 ..
-rw-r-----   1 bandit15 bandit15   33 Aug 15 13:15 .bandit14.password
-rw-r--r--   1 root     root      220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root     root     3.8K Aug 15 13:09 .bashrc
-rw-r--r--   1 root     root      807 Mar 31  2024 .profile
bandit15@bandit:~$ openssl s_client localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAu+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBANI+P5QXm9Bj21FIPsQqbqZRb5XmSZZJYaam7EIJ16Fxedf+
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0lAfN33h+RMTjRoMb8yBsZsC063MLfXCk4p+
09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/
```

```
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$
```

Secure encrypted communication. While `nc` handles plaintext connections, `openssl s_client` is used to interact with services secured by SSL/TLS, which encrypts data in transit. This is fundamental for real-world secure communications.

Level 16 → Level 17

Goal: Find which port between 31000 and 32000 is serving SSL, then submit the password to it.

```
bandit16@bandit:~$ nmap -sV -p 31000-32000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-26 06:58 UTC
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the follow
vice :
SF-Port31790-TCP:V=7.94SVN%T=SSL%I=7%D=8/26%Time=68AD5B48%P=x86_64-pc-linu
SF:x-gnu%r(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password\.\n")%r(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")%r(RTS
SF:PRequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password\.\n")%r(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x2
SF:0enter\x20the\x20correct\x20current\x20password\.\n")%r(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password\.\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.90 seconds
```

```
bandit16@bandit:~$ openssl s_client -ign_eof localhost:31790
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
```

```
read R BLOCK
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
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
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:~$ exit
logout
```

Network reconnaissance and SSL communication. `nmap` is the industry-standard tool for network discovery and security auditing. This level combines port scanning with the previous skill of SSL communication to find and interact with a specific secure service.

Level 17 → Level 18

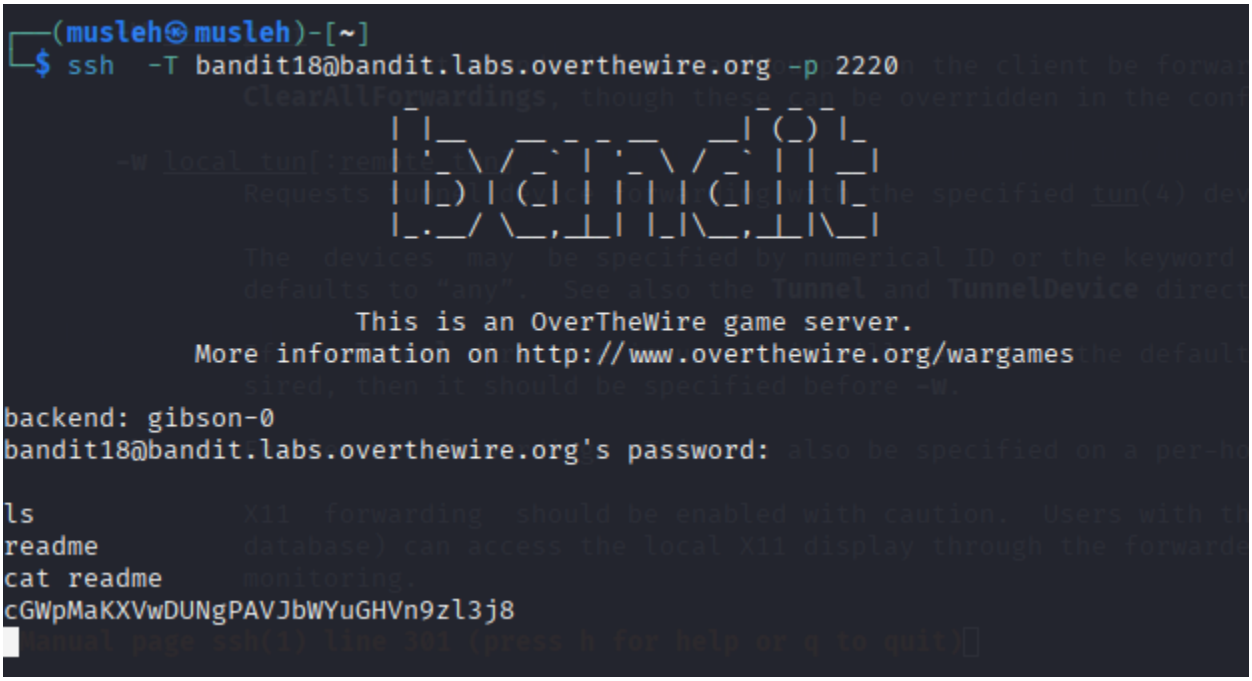
Goal: The passwords for the next level are in files `passwords.old` and `passwords.new`. Find the one line that has been changed

```
bandit17@bandit:~$ ls -lh
total 8.0K
-rw-r----- 1 bandit18 bandit17 3.3K Aug 15 13:15 passwords.new
-rw-r----- 1 bandit18 bandit17 3.3K Aug 15 13:15 passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> gvE89l3AhAhg3Mi9G2990zGnn42c8v20
```

: File comparison. The `diff` utility is used to compare files line by line, highlighting the differences. It's invaluable for spotting changes in configuration files, code, or data.

Level 18 → Level 19

Goal: The password is in a `readme` file, but the `.bashrc` logs you out on login.

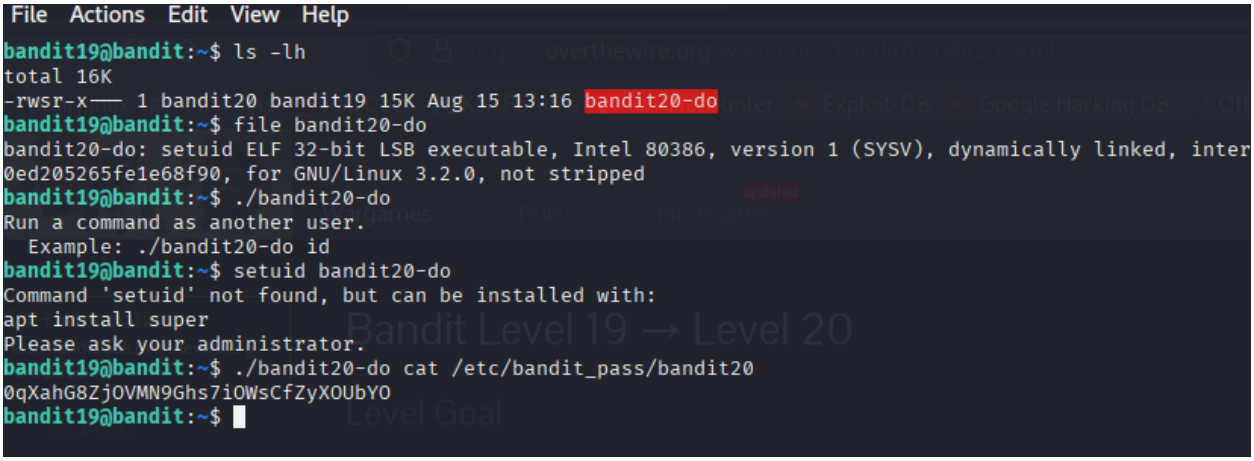


Normally, SSH creates a pseudo-terminal so you can interact with the shell. But in this level, the shell startup files (.bashrc) are blocking us.

By adding -T, we disable pseudo-terminal allocation, which means SSH won’t start a normal interactive shell. Instead, it runs the command we pass directly — letting us bypass the restriction

Level 19 → Level 20

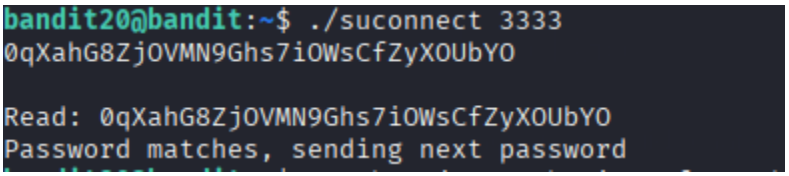
Goal: Use the `setuid` binary `bandit20-do` to read the password for bandit20.

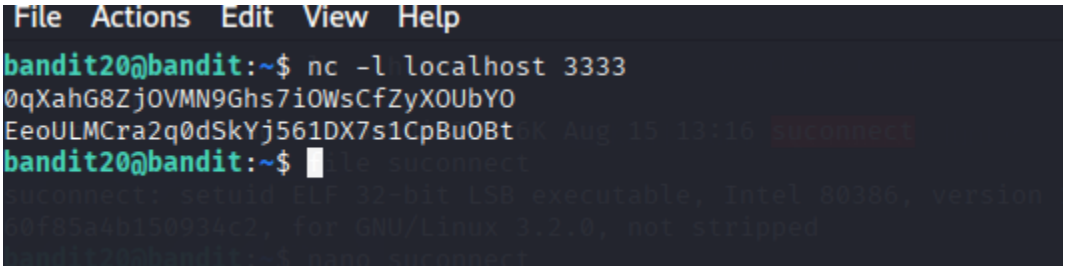


Setuid (Set User ID) binaries. An executable with the setuid permission bit set runs with the privileges of the file's owner (bandit20), not the user executing it (bandit19). This is a fundamental Linux privilege concept and a common privilege escalation vector.

Level 20 → Level 21

The `suconnect` binary connects to a port you specify. If it receives the current level's password on that port, it will send back the next password

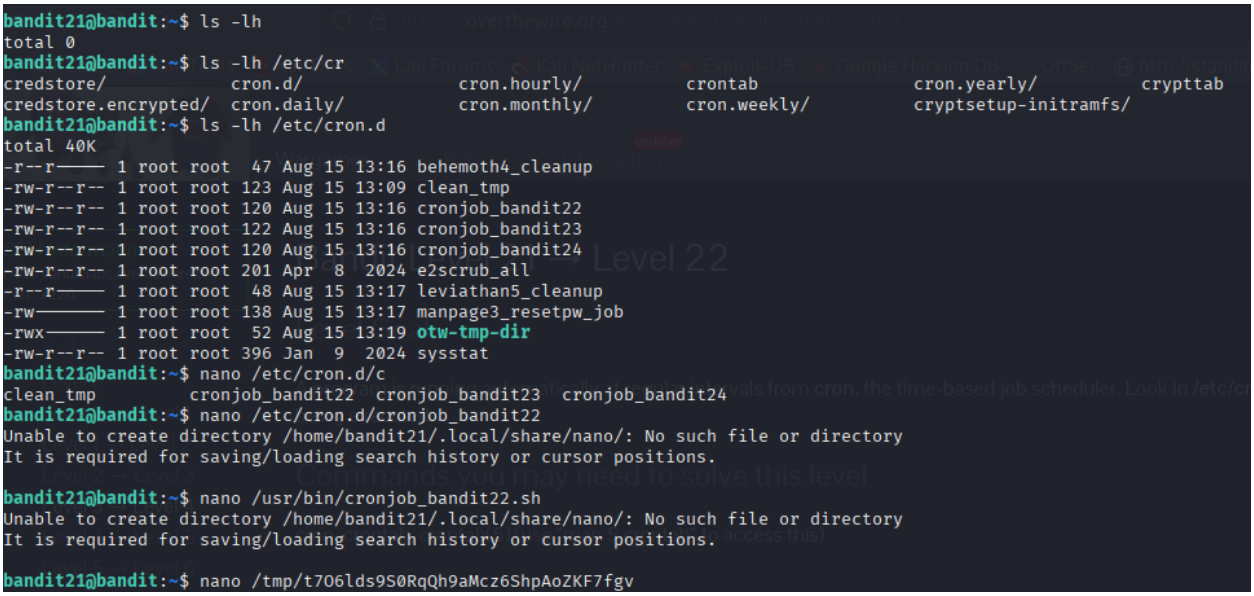




Networked application interaction. This requires understanding how to make two processes communicate over a local network port, combining knowledge of `netcat` for listening and the behavior of a custom SUID binary.

Level 21 → Level 22

Goal: A cron job is running. Find what it is doing and where it is writing the password



Cron jobs. Cron is a time-based job scheduler in Linux. Understanding how to read crontab files (`/etc/cron.d/`) and the scripts they execute is crucial for system administration and security auditing, as automated tasks can often lead to privilege escalation.

Level 22 → Level 23

Goal: A cron job for bandit23 runs a script that creates a password file based on an MD5 hash of the username.

```
bandit22@bandit:/etc/cron.d$ nano cronjob_bandit23
Unable to create directory /home/bandit22/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ mktemp -d
/tmp/tmp.FdJ9FzYdZC
bandit22@bandit:/etc/cron.d$ cd /tmp/tmp.FdJ9FzYdZC
bandit22@bandit:/tmp/tmp.FdJ9FzYdZC$ nano test.sh
Unable to create directory /home/bandit22/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit22@bandit:/tmp/tmp.FdJ9FzYdZC$ chmod +x test.sh
bandit22@bandit:/tmp/tmp.FdJ9FzYdZC$ ./test.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddbb4412f91573b38db3
bandit22@bandit:/tmp/tmp.FdJ9FzYdZC$ cat /tmp/8169b67bd894ddbb4412f91573b38db3
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
```

```
bandit22@bandit:/etc/cron.d$ ls
behemoth4_cleanup  clean_tmp  cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  e2sc
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ cat "I am user bandit23" | md5sum
cat: 'I am user bandit23': No such file or directory
d41d8cd98f00b204e9800998ecf8427e  -
bandit22@bandit:/etc/cron.d$ cd /tmp/tmp.d41d8cd98f00b204e9800998ecf8427e
-bash: cd: /tmp/tmp.d41d8cd98f00b204e9800998ecf8427e: No such file or directory
bandit22@bandit:/etc/cron.d$ myname=bandit23
bandit22@bandit:/etc/cron.d$ echo I am user $myname | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
```

Analyzing script behavior. This requires reading a shell script, understanding how it generates a dynamic filename (using `md5sum`), and replicating that process to predict the filename and access the data.

Level 23 → Level 24

A cron job runs every minute that executes any script placed in the directory `/var/spool/bandit24/foo`. Use this to get the bandit24 password

```
bandit23@bandit:/etc/cron.d$ ls
behemoth4_cleanup  clean_tmp  cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  e2scrub_all  leviathan5_cleanup
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

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

bandit23@bandit:/etc/cron.d$ mktemp -d
/tmp/tmp.Ooxg8N2hRI
bandit23@bandit:/etc/cron.d$ cd /tmp/tmp.Ooxg8N2hRI && nano test.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/tmp.Ooxg8N2hRI$ chmod +x test.sh
bandit23@bandit:/tmp/tmp.Ooxg8N2hRI$ ./test.sh
./test.sh: line 5: cd: /var/spool/bandit23/foo: No such file or directory
```

```
bandit23@bandit:~$ cd /var/spool/bandit24/foo
bandit23@bandit:/var/spool/bandit24/foo$ echo "cat /etc/bandit_pass/bandit24" > myscript.sh
bandit23@bandit:/var/spool/bandit24/foo$ chmod +x myscript.sh
bandit23@bandit:/var/spool/bandit24/foo$ cd /var/spool/bandit23/foo
-bash: cd: /var/spool/bandit23/foo: No such file or directory
bandit23@bandit:/var/spool/bandit24/foo$ mkdir /tmp/alex1234
bandit23@bandit:/var/spool/bandit24/foo$  cd /tmp/alex1234
bandit23@bandit:/tmp/alex1234$ vi script.sh
bandit23@bandit:/tmp/alex1234$ ls
bandit23@bandit:/tmp/alex1234$ nano script.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/alex1234$ chmod 777 script.sh
bandit23@bandit:/tmp/alex1234$  cp script.sh /var/spool/bandit24
cp: cannot create regular file '/var/spool/bandit24/script.sh': Operation not permitted
bandit23@bandit:/tmp/alex1234$  cp script.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/alex1234$ chmod 777 /tmp/alex1234/
bandit23@bandit:/tmp/alex1234$ ls
script.sh
bandit23@bandit:/tmp/alex1234$ ls
bandit24pass  script.sh
bandit23@bandit:/tmp/alex1234$ cat bandit24pass
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8
```

Exploiting cron job permissions. This demonstrates a classic privilege escalation technique: if a cron job runs with elevated privileges and executes scripts from a world-writable directory, any user can place a malicious script there to be executed with those higher privileges.

Level 24 → Level 25

Goal: A daemon is listening on port 30002. It requires the bandit24 password and a 4-digit PIN. Bruteforce the PIN to get the bandit25 password

```
bandit24@bandit:~$ mktemp -d
/tmp/tmp.Ag02kknWnU
bandit24@bandit:~$ cd /tmp/tmp.Ag02kknWnU
bandit24@bandit:/tmp/tmp.Ag02kknWnU$ nano script.sh
Unable to create directory /home/bandit24/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit24@bandit:/tmp/tmp.Ag02kknWnU$ nano script.sh
```

```
 GNU nano 7.2
#!/bin/bash

for i in {0000 .. 9999}
do
        echo "gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 $i" >> musleh.txt
done
```

```
bandit24@bandit:/tmp/tmp.Ag02kknWnU$ ./script.sh
bandit24@bandit:/tmp/tmp.Ag02kknWnU$ cat musleh.txt
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0000
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0001
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0002
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0003
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0004
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0005
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 0006
```

```
File  Actions  Edit  View  Help
bandit24@bandit:/tmp/tmp.Ag02kknWnU$ cat musleh.txt |nc localhost 30002
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret
Wrong! Please enter the correct current password and pincode. Try again.
```

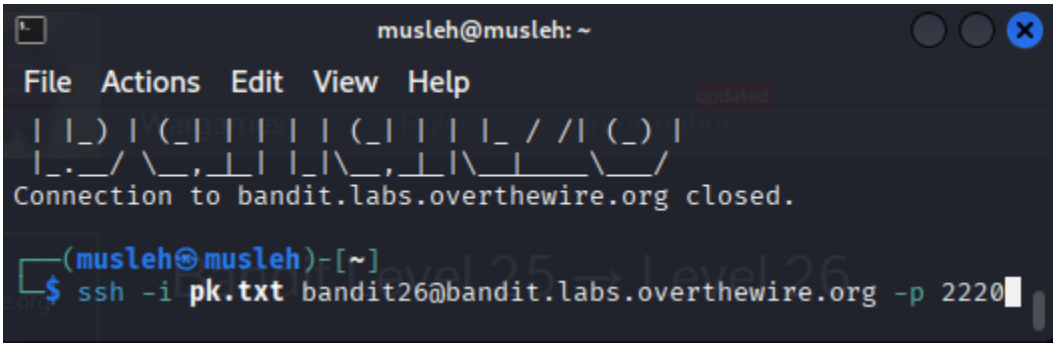
Goal: A daemon is listening on port 30002. It requires the bandit24 password and a 4-digit PIN. Bruteforce the PIN to get the bandit25 password

Level 25 → Level 26

Goal: Log in as bandit25 using the provided private key. The shell closes immediately, but the password is visible if you can view the connection output.

After connecting using the private key the connection closed right away

So using more utility you minimize the terminal as you can so it needed more to show of the content



Once you are in more press v

Then :e /etc/bandit_pass/bandit26

Bandit 26-27: on the same place press v to switch to vim then type in :set shell=/bin/bash

Then type :shell

```
:shell
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ cat text.txt
  _                     _ _ _   ___   __
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
 |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB
bandit26@bandit:~$
```

Level 27 → Level 28

Goal: The password for the next level is in a Git repository in the home directory.

```
bandit27@bandit:~$ ls
bandit27@bandit:~$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo.git/
fatal: could not create work tree dir 'repo': Permission denied
bandit27@bandit:~$ mktemp -d
/tmp/tmp.NpaabBx6oa
bandit27@bandit:~$ cd /tmp/tmp.NpaabBx6oa
bandit27@bandit:/tmp/tmp.NpaabBx6oa$ ssh://bandit27-git@localhost/home/bandit27-git/repo.git/
-bash: ssh://bandit27-git@localhost/home/bandit27-git/repo.git/: No such file or directory
bandit27@bandit:/tmp/tmp.NpaabBx6oa$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo.git/
Cloning into 'repo'...
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])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.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 on port 22, which is not intended.
!!! If you are trying to log in to an OverTheWire game, use the port mentioned in
!!! the "SSH Information" on that game's webpage (in the top left corner).

bandit27-git@localhost: Permission denied (publickey).
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
bandit27@bandit:/tmp/tmp.NpaabBx6oa$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo.git/
Cloning into 'repo'...
```

```
bandit27@bandit:/tmp/tmp.NpaabBx6oa$ ls
repo
bandit27@bandit:/tmp/tmp.NpaabBx6oa$ cd repo/
bandit27@bandit:/tmp/tmp.NpaabBx6oa/repo$ ls
README
bandit27@bandit:/tmp/tmp.NpaabBx6oa/repo$ cat README
The password to the next level is: Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN
bandit27@bandit:/tmp/tmp.NpaabBx6oa/repo$
```

Version control with Git. This introduces the concept of cloning a repository from a remote source (in this case, via SSH) to examine its contents, a common task in development and security analysis.

Level 28 → Level 29

Goal: The password is in the Git repository, but it's in an older commit.

```
bandit28@bandit:~$ mktemp -d
/tmp/tmp.Ry79al1wx3
bandit28@bandit:~$ cd /tmp/tmp.Ry79al1wx3
bandit28@bandit:/tmp/tmp.Ry79al1wx3$ git clone ssh://bandit28-git@localhost:2220/home/bandit28
Cloning into 'repo'...
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/bandit28/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit28/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

backend: gibson-0
bandit28-git@localhost's password:
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (2/2), done.
bandit28@bandit:/tmp/tmp.Ry79al1wx3$
```

```
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ ls
README.md
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx

bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git log
commit 710c14a2e43cfd97041924403e00efb00b3a956e (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    fix info leak

commit 68314e012fbaa192abfc9b78ac369c82b75fab8f
Author: Morla Porla <morla@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    add missing data

commit a158f9a82c29a16dcea474458a5ccf692a385cd4
Author: Ben Dover <noone@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    initial commit of README.md
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git revert 710c14a2e43cfd97041924403e00efb00b3a956e
Unable to create directory /home/bandit28/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

[master 3b8fbc6] Revert "fix info leak"
```

```
    initial commit of README.md
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git revert 710c14a2e43cfd97041924403e00efb00b3a956e
Unable to create directory /home/bandit28/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

[master 3b8fbc6] Revert "fix info leak"
 1 file changed, 1 insertion(+), 1 deletion(-)
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ cat commit 68314e012fbaa192abfc9b78ac369c82b75fab8f
cat: commit: No such file or directory
cat: 68314e012fbaa192abfc9b78ac369c82b75fab8f: No such file or directory
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git commit 68314e012fbaa192abfc9b78ac369c82b75fab8f
error: pathspec '68314e012fbaa192abfc9b78ac369c82b75fab8f' did not match any file(s) known to git
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git  68314e012fbaa192abfc9b78ac369c82b75fab8f
git: '68314e012fbaa192abfc9b78ac369c82b75fab8f' is not a git command. See 'git --help'.
bandit28@bandit:/tmp/tmp.Ry79al1wx3/repo$ git show  68314e012fbaa192abfc9b78ac369c82b75fab8f
commit 68314e012fbaa192abfc9b78ac369c82b75fab8f
Author: Morla Porla <morla@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    add missing data

diff --git a/README.md b/README.md
index 7ba2d2f..d4e3b74 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

 - username: bandit29
-- password: <TBD>
+- password: 4pT1t5DENaYuqnqvadYs1oE4QLCdjmJ7
```

Git history inspection. Sensitive data is often committed to a repository and then removed in a later commit. However, it remains forever in the repository's history. The `git log` and `git checkout` commands are used to inspect this history and retrieve old versions of files.