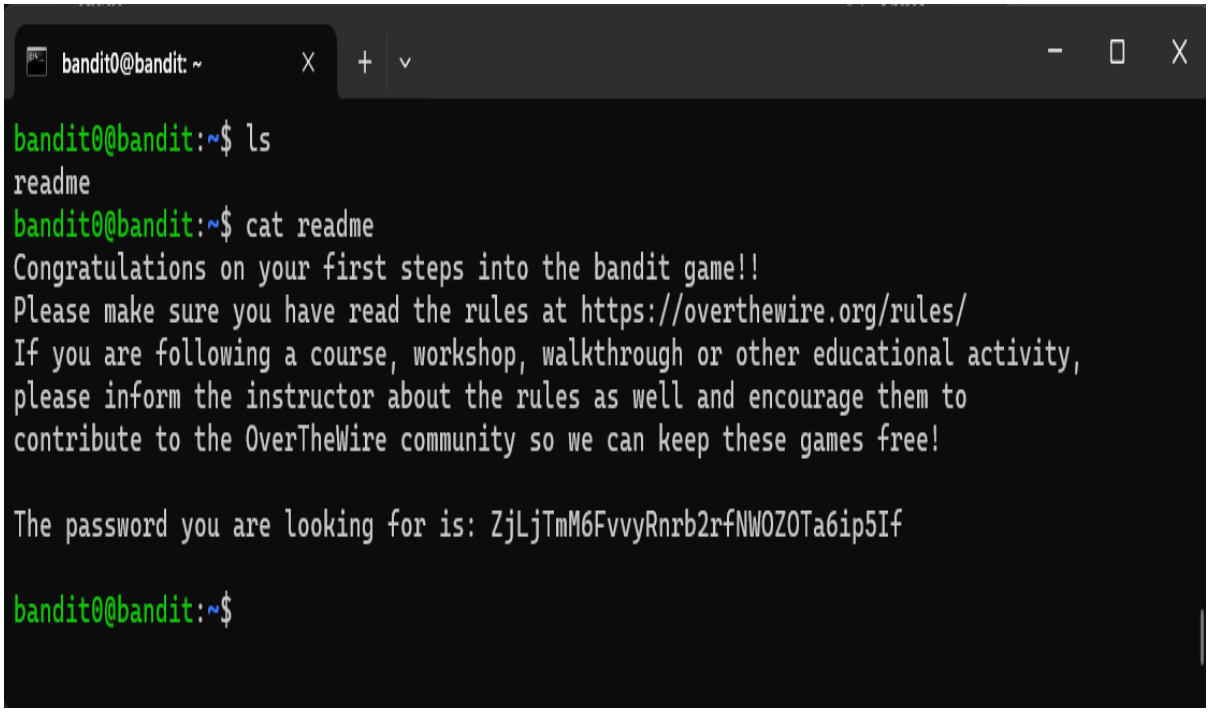
WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

The Bandit wargame is an online game offered by the OverTheWire community. It helps me to learn various linux commands and understand some basic features of this system.

BANDIT 0-0 SOLUTION:

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



WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (0->1):

After getting the password of level 0 enter exit command and use ssh command to enter into next level. The password for the next level is stored in a file which is located in the home directory.

Use cat command to view the file.

BANDIT LEVEL (1->2):

```
  http://www.overthewire.org/wargames/

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

  Enjoy your stay!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

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

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

  Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (2->3):

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

Explanation: In the Linux operating system, a **hidden** file is any file that begins with a **".".** When a file is hidden it can not been seen with the bare ls command. If you need to see hidden files using
the ls command you need to add the **-a** switch.

```
bandit3@bandit: ~/inhere
bandit3@bandit: ~/inhere
trl+alt+1
~$ ls
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

BANDIT LEVEL (3->4):

The password for the next level is stored in the only human-readable file in the **inhere** directory.

Explanation: Here, we use the file command with a *wildcard* on the filename to find the file containing only ASCII text.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ cat -- -file00
◆p◆◆&◆y◆,◆(jo◆.at◆:uf◆^◆◆◆@bandit4@bandit:~/inhere$ cat -- -file01
i◆R◆,◆Λ◆:Y◆◆◆?◆%◆A◆◆◆◆B◆◆ ◆bandit4@bandit:~/inhere$ cat -- -file02
3◆      ◆)[◆#Y◆◆-6c◆◆IR-◆$◆◆◆◆:◆◆bandit4@bandit:~/inhere$ cat -- -file03
◆◆◆/◆
     ◆◆◆◆◆◆qGi◆◆,◆2◆Yb◆
dbandit4@bandit:~/inhere$ cat -- -file04
◆rOx◆◆◆◆h0~ey
◆◆c◆~◆h◆n◆◆G1bandit4@bandit:~/inhere$ cat -- -file05
}◆◆◆F◆◆◆W>◆◆#lk◆d◆◆◆yE◆◆bandit4@bandit:~/inhere$ cat -- -file06
6◆0]◆\◆$◆1◆%◆◆◆◆◆◆◆o@◆◆b/◆◆bandit4@bandit:~/inhere$ cat -- -file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (4->5):

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

Explanation: The find command is really useful when you look for a specific file. Here, we use the - readable, ! -executable and -size 1033c parameters to find a file with the specified properties.

```
bandit5@bandit:~$ find . -type f -size 1033c ! -executable
./inhere/maybehere07/.file2
bandit5@bandit:~$ cat < ./inhere/maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

BANDIT LEVEL (5->6):

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

Explanation: Same as the previous level except that we redirect the files we cannot read to **stderr**. Also we tell find to look into the **root** of the file system as we don't know where the file is located.

```
bandit6@bandit: ~
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/d
ev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (6->7):

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

Explanation: Here we use the -exec argument of find with the grep command to find the file containing the word **millionth**.

```
--[ 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!

bandit7@bandit:~$ grep -i millionth data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

BANDIT LEVEL (7->8):

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

Explanation: First we use sort to sort alphabetically the data in the **data.txt** file then, we use uniq to count the number or occurances and find the line of text that occurs only once.

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

  Enjoy your stay!

bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt\uniq -u
sort: cannot read: data.txtuniq: No such file or directory
bandit8@bandit:~$ sort data.txt|uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

BANDIT LEVEL (8->9):

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

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

Explanation: The strings command helps us to find the human-readable strings and then grep the strings beginning with several **'='** characters.

```
  Enjoy your stay!

bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | strings |grep -e ===
}========== the
3JprD========== passwordi
~fDV3========== is
D9========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$
```

BANDIT LEVEL (9->10):

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

Explanation: Read the **data.txt** and redirect the output to the base64 command. The **-d** argument is used to decode the string.

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit10@bandit:~$ base64 data.txt
VkdobElIQmhjM04zYjNKa0lHbHpJR1IwVWpFM00yWmFTMkl3VWxKelJFWlRSM05uTWxKWGJuQk9W
bW96Y1ZKeUNnPT0K
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

BANDIT LEVEL (10->11):

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.

Explanation: The tr command is used to translate the first set of characters **'A-Za-z'** to **'N-ZA-Mn-za- m'** which is a rotation of 13 positions of the first set.

```
  Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt |tr 'A-Za-z' 'N-Za-Mn-za-m'
tr: range-endpoints of 'a-M' are in reverse collating sequence order
bandit11@bandit:~$ cat data.txt |tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$
```

BANDIT LEVEL (11->12):

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.

Explanation: The -r switch of xxd convert an hexdump to binary. Then we use the file command to find out which compression tool has been used and recursively decompress the files with the right tool.

```
bandit12@bandit: /tmp/vish
bandit12@bandit:/tmp/vish$ rm data.txt
bandit12@bandit:/tmp/vish$ ls
data5.bin
bandit12@bandit:/tmp/vish$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/vish$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/vish$ mv data5.bin data.tar
bandit12@bandit:/tmp/vish$ tar xf data.tar
bandit12@bandit:/tmp/vish$ ls
data6.bin  data.tar
bandit12@bandit:/tmp/vish$ file data6.bim
data6.bim: cannot open `data6.bim' (No such file or direc
tory)
bandit12@bandit:/tmp/vish$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/vish$ mv data6.bin data.bz2
bandit12@bandit:/tmp/vish$ bzip2 -d data.bz2
bandit12@bandit:/tmp/vish$ ls
data  data.tar
bandit12@bandit:/tmp/vish$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/vish$ mv data data.tar
bandit12@bandit:/tmp/vish$ ls
data.tar
bandit12@bandit:/tmp/vish$ tar xf data.tar
bandit12@bandit:/tmp/vish$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/vish$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last mo
dified: Thu Sep 19 07:08:15 2024, max compression, from U
nix, original size modulo 2^32 49
bandit12@bandit:/tmp/vish$ mv data8.bin data.gz
bandit12@bandit:/tmp/vish$ gzip -d data.gz
bandit12@bandit:/tmp/vish$ ls
data  data.tar
bandit12@bandit:/tmp/vish$ file data
data: ASCII text
bandit12@bandit:/tmp/vish$ cat data
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/vish$
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (13->14):

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.

Explanation: Here, we download the private key to login to the next level. The scp command will do the trick.

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be esta
blished.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerL
Y.
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/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.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.
```

BANDIT LEVEL (14->15):

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

Explanation: After login to **bandit14** with the private key, you can redirect the content of **/etc/bandit_pass/bandit14** to netcat using the nc command.

```
  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
cat: etcbandit_passbandit14: No such file or directory
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (15->16):

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.

Explanation: Here, we send the content of **/etc/bandit_pass/bandit15** to openssl.
The s_client implements a generic SSL/TLS client which can establish a transparent connection to a remote server speaking SSL/TLS.

```
bandit15@bandit: ~
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man nc
bandit15@bandit:~$
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
                    --ssl                    Connect or listen with SSL
                    --ssl-cert               Specify SSL certificate file (PEM) f
or listening
                    --ssl-key                Specify SSL private key (PEM) for li
stening
                    --ssl-verify             Verify trust and domain name of cert
ificates
                    --ssl-trustfile          PEM file containing trusted SSL cert
ificates
                    --ssl-ciphers            Cipherlist containing SSL ciphers to
 use
                    --ssl-servername         Request distinct server name (SNI)
                    --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
            Use --ssl-trustfile to give a custom list. Use -v one or more
        --ssl-cert certfile.pem (Specify SSL certificate)
            client (in connect mode). Use it in combination with --ssl-key.
        --ssl-key keyfile.pem (Specify SSL private key)
            file that goes with the certificate named with --ssl-cert.
        --ssl-trustfile cert.pem (List trusted certificates)
            combined with --ssl-verify. The argument to this option is the
        --ssl-ciphers cipherlist (Specify SSL ciphersuites)
        --ssl-servername name (Request distinct server name)
        --ssl-alpn ALPN list (Specify ALPN protocol list)
            http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (16->17):

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.

Explanation: You can write a simple port scanner in **bash** and try to connect to the open ports with openssl.

```
bandit16@bandit: /tmp/randc

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

  Enjoy your stay!

bandit16@bandit:~$ nmap -sV -T4 -p 31000-32000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 16:59 UTC

[1]+  Stopped                 nmap -sV -T4 -p 31000-32000 localhost
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
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-----
```

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

BANDIT LEVEL (17->18):

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

Explanation: The diff command will compare 2 files line by line and show you the differences.

```
$ ssh -i sshkey bandit17@bandit.labs.overthewire.org -p 2220

bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< 6vcSC74ROI95NqkKaeEC2ABVMDX9TyUr
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

BANDIT LEVEL (18->19):

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.

Explanation: You can pass the command you want to execute directly to the ssh command to bypass the issue.

```
$ ssh bandit18@bandit.labs.overthewire.org -p 2220
Byebye !
Connection to bandit.labs.overthewire.org closed.

$ ssh bandit18@bandit.labs.overthewire.org -p 2220 "cat readme"
bandit18@bandit.labs.overthewire.org's password:
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

BANDIT LEVEL (19->20):

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.

Explanation: Nothing to explain here, pretty straightforward.

WRITE-UPS FOR THE BANDIT WARGAME IN THE OVERTHEWIRE

```
$ ssh bandit19@bandit.labs.overthewire.org -p 2220

bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```