


OverTheWire Wargames: Bandit

Level 0

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is `bandit.labs.overthewire.org`, on port 2220. The username is `bandit0` and the password is `bandit0`.

Se conecta vía SSH al puerto número 2220 ejecutando el comando `ssh bandit0@bandit.labs.overthewire.org -p 2220` para acceder al servidor.


```
(kali㉿kali)-[~]
$ 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.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEclfXC5CXlhmaAM/userLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
```



```
Carpenter's
```

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

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



www. ver he ire.org

Welcome to OverTheWire!

Level 0 → Level 1

The password for the next level is stored in a file called `readme` located in the home directory. Use this password to log into `bandit1` using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

Ejecutando el comando `ls` se consigue averiguar la ubicación del archivo que contiene la contraseña para el siguiente nivel y se lee aplicando el comando `cat`.

```
bandit0@bandit:~$ ls /home
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  band
bandit1  bandit13  bandit17  bandit20  bandit24  bandit27-git  band
bandit10  bandit14  bandit18  bandit21  bandit25  bandit28  band
bandit11  bandit15  bandit19  bandit22  bandit26  bandit28-git  band
bandit0@bandit:~$ ls /home/bandit0
readme
bandit0@bandit:~$ ls /home/bandit0/readme
/home/bandit0/readme
bandit0@bandit:~$ cd /home/bandit0/readme
-bash: cd: /home/bandit0/readme: Not a directory
bandit0@bandit:~$ cat /home/bandit0/readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Level 1 → Level 2

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

Ejecutando el comando `cat <-` se podrá leer el contenido del fichero, dado que al tener este un nombre compuesto por caracteres especiales se debe usar `<` para que el comando interprete lo escrito a continuación como una cadena de texto.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat <-me bandi
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Level 2 → Level 3

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

Obtendremos la contraseña leyendo el archivo cuyo nombre es la cadena que se indica mediante el comando `cat <"spaces in this filename"`.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat <spaces in this filename
-bash: spaces: No such file or directory
bandit2@bandit:~$ cat <"spaces in this filename"
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Level 3 → Level 4

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

Ejecutando el comando `ls -a` podremos visualizar todos los archivos del directorio, incluidos los ocultos, y con el comando `cat <"./.hidden"` podremos leer el archivo que contiene la contraseña.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat <"./.hidden"
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Level 4 → Level 5

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

Con el comando `cat` podemos mostrar por pantalla el contenido de cada uno de los diez ficheros hasta encontrar al único que tiene texto interpretable, que es la contraseña.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ ls -a
.  ..  -file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ cat <"-file00"
QRrtZ+i
bandit4@bandit:~/inhere$ cat <"-file01"
7L3++Y+ W++++E+Y+
bandit4@bandit:~/inhere$ cat <"-file02"
+++y++++0++\+e-Hx++2++Kbandit4@bandit:~/inhere$ cat <"-file03"
++i+x++#++e>+V0++p{+
bandit4@bandit:~/inhere$ cat <"-file04"
++gQ++++eE}:+g+++j8+++++<+ebandit4@bandit:~/inhere$ cat <"-file05"
++S+++ 0+++++7+++++b<+~bandit4@bandit:~/inhere$ cat <"-file06"
G=1+++
bandit4@bandit:~/inhere$ cat <"-file07"
lrIWWI6bB37kxfiCQZqUdOIYfr6eEqR
```

lrIWWI6bB37kxfiCQZqUdOIYfr6eEqR

Level 5 → Level 6

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

- human-readable

- 1033 bytes in size
- not executable

Para encontrar el archivo concreto tendremos que usar el comando *find* especificando las condiciones que se nos han detallado escribiendo a continuación

-type f -size 1033c ! -executable

```
bandit5@bandit:~/inhere/maybehere00$ cd ../
bandit5@bandit:~/inhere$ ls -l
total 80
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere00
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere01
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere02
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere03
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere04
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere05
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere06
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere07
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere08
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere09
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere10
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere11
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere12
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere13
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere14
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere15
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere16
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere17
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere18
drwxr-xr-x 2 root bandit5 4096 Oct  5 06:19 maybehere19
bandit5@bandit:~/inhere$ find -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat <".file2"
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 6 → Level 7

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

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Para encontrar el archivo concreto tendremos que usar el comando *find* especificando las condiciones que se nos han detallado escribiendo a continuación

/-user bandit7 -group bandit6 -size 33c y 2>/dev/null para que no se muestren por pantalla los mensajes de error.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat <"/var/lib/dpkg/info/bandit7.password"  
-bash: ./var/lib/dpkg/info/bandit7.password: No such file or directory  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 7 → Level 8

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

Ejecutando el comando `cat data.txt | grep millionth` encontraremos la línea de texto en dicho archivo que se sitúa al lado de la cadena de texto especificada.

```
biceps's InBCsYpHt8o1atjygiRFnVE2ExoyirYv  
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 8 → Level 9

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

Para localizar dentro del archivo data.txt la única línea de texto que no está duplicada ejecutaremos el comando `sort data.txt | uniq -icu`, gracias al que no se muestran las líneas duplicadas, se diferencian entre mayúsculas y minúsculas y se indica la cantidad de repeticiones de la línea.

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

EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 9 → Level 10

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

Ejecutando el comando `cat data.txt | strings | grep ^=` conseguiremos que solo se muestren por pantalla las líneas del archivo `data.txt` que contengan texto legible y comiencen por el caracter `=`.

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | strings | grep ^=
-2"L(
-===== passwordk^
-===== is
-Y!m
-===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
-r=_
-uea
```

G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 10 → Level 11

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

Ejecutando el comando `cat data.txt | base64 --decode` podremos leer el contenido del archivo `data.txt` al haberlo descodificado en base 64.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is 6zPezilDR2RKNdNYFNb6nVCKzphlXHBM
```

6zPezilDR2RKNdNYFNb6nVCKzphlXHBM

Level 11 → Level 12

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

Para hacer la transliteración de los caracteres del fichero `data.txt` por trece posiciones se deberá ejecutar el comando `cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'`.


```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA00SFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKKOP0XbFX0oW8chDz5yVRv
```

JVNBBFSmZwKKOP0XbFX0oW8chDz5yVRv

Level 12 → Level 13

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

Para obtener la contraseña en este nivel deberemos descomprimir y comprimir los archivos que nos son proporcionados múltiples veces utilizando los comandos *xxd*, *gzip*, *bzip2* y *tar*.

```
bandit12@bandit:~$ mkdir /tmp/b12m
bandit12@bandit:~$ cat data.txt | xxd -r > /tmp/b12m/data
bandit12@bandit:~$ cd /tmp/b12m
bandit12@bandit:/tmp/b12m$ file data
data: 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/b12m$ gzip -d data
gzip: data: unknown suffix -- ignored
bandit12@bandit:/tmp/b12m$ mv data data.gz
bandit12@bandit:/tmp/b12m$ gzip -d data
bandit12@bandit:/tmp/b12m$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/b12m$ bzip2 -d data
bzip2: Can't guess original name for data -- using data.out
bandit12@bandit:/tmp/b12m$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/b12m$ mv data.out data.gz
bandit12@bandit:/tmp/b12m$ gzip -d data.gz
bandit12@bandit:/tmp/b12m$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/b12m$ tar xvf data
data5.bin
bandit12@bandit:/tmp/b12m$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/b12m$ tar xvf data5.bin
data6.bin
bandit12@bandit:/tmp/b12m$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/b12m$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/b12m$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/b12m$ tar xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/b12m$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Oct 5 06:19:20 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/b12m$ mv data8.bin.data8.gz
mv: missing destination file operand after 'data8.bin.data8.gz'
Try 'mv --help' for more information.
bandit12@bandit:/tmp/b12m$ mv data8.bin data8.gz
bandit12@bandit:/tmp/b12m$ gzip -d data8.gz
bandit12@bandit:/tmp/b12m$ file data8
data8: ASCII text
bandit12@bandit:/tmp/b12m$ cat data8
The password is wBwDlBxEir4CaE8LaPhauuOo6pwRmrDw
```

wBwDlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 13 → Level 14

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

Con la clave privada que nos ha sido proporcionada deberemos entrar en el siguiente nivel ejecutando el comando `ssh -i sshkey.private bandit14@localhost -p 2220`. Una vez dentro podemos acceder al fichero que contiene la contraseña.

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkk0E83W2c0T7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AioYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQ03myS91vUHEuo0MAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29KxJaqrRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxANA+WYA7
jiPyTF0is8uzMLYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyE0zjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfYgoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyfyNAqx/TLfzLLYf0u7i9Jet67
xAh0tONG/u8FB5I3LA12Vp60viwvDWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUCUgzoVSPinZaS0zUDypdp2+tRH3MQa5kqN1YKjvF8RC47wo0YCKtsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONTmrVvtYK40/yeU4aZ/HA2DQzwe
ol1AfiEhAoGBA0nVjosBkm7sblK+n4IEwPxs8s0mhPnTDUy5WGrpSCrX0msVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkucp/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDLDMwjNR04xHA/fKh8bXXyTMqOHNJTHHnhb3McdURjAoGBANKU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNBG+ex0H9JNQsTK3X5PBMA8AfX0GrKeuwKWA6erytVTqj0fLYcdp5+z9s
8DtVcxDuVsM+i4X8UqIG0LvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzp0+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9i0dANzwKw7mUUFViacMR/t54W1
GC83s0s3D7n5Mj8x3Nd08xFit7dT9a245Tva0YQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8Zxq9XjPRpKwUCgYA7z6Li0QKxNeXH3qHXcnHok855maUj5fJNpBY
idkyZ8ySF8glcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4js0P8ibfckS4nBP+dT81kkkg5Z5MohXB0RA7VWx+ACohcDEkprsq+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYZRPaY6f++Gv/UVfAPV4c+S0
kAwpxbv5tbkzbs0eaLPTKgZlavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFub0dN
/aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA=
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
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).
```

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

fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Level 14 → Level 15

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

Desde el nivel actual deberemos ejecutar el comando `nc localhost 30000` para enviar la contraseña actual al puerto que se ha indicado y que a cambio nos sea devuelta la contraseña del siguiente nivel.


```
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 15 → Level 16

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

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

Para recibir la próxima contraseña se debe enviar la contraseña actual al puerto indicado mediante el protocolo SSL. Para ello ejecutaremos el comando *openssl s_client -connect localhost:30001* y enviaremos la contraseña actual cuando sea requerido.

```
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=Nov 18 19:21:26 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Nov 18 19:21:26 2023 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
```

```
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
```

JQtTfApK4SeyHwDlI9SXGR50qclOAil1

Level 16 → Level 17

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

Para encontrar cuál es el puerto indicado debemos ejecutar el comando `nmap -sV -p31000-32000 localhost` y obtendremos como resultado que el puerto 31790 cumple las condiciones. Una vez que hemos conectado con ese puerto mediante SSL nos pedirá enviar la contraseña anterior y se nos proporcionará una clave privada. Si accedemos al siguiente nivel usando dicha clave privada nos dejará entrar y podremos llegar hasta el archivo donde se encuentra almacenada la contraseña.

```
bandit16@bandit:~$ nmap -sV -p31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-20 20:09 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
31960/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following
SF-Port31790-TCP:V=7.80%T=SSL%I=7%D=11/20%Time=655BBCFA%P=x86_64-pc-linux-
SF:gnu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20c
SF:urrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\x20th
SF:e\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\x20Ple
SF:ase\x20enter\x20the\x20correct\x20current\x20password\n")%r(RTSPRequest
SF:,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20password
SF:e\n")%r(Help,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SSLSessionReq,31,"Wrong!\x20Please\x20enter\x20the\x2
SF:0correct\x20current\x20password\n")%r(TerminalServerCookie,31,"Wrong!\x
SF:20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(TLSSES
SF:sionReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20p
SF:assword\n")%r(Kerberos,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
SF:x20current\x20password\n")%r(FourOhFourRequest,31,"Wrong!\x20Please\x20
SF:enter\x20the\x20correct\x20current\x20password\n")%r(LPDString,31,"Wron
SF:g!\x20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(LD
SF:APSearchReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SIPOptions,31,"Wrong!\x20Please\x20enter\x20the\x20co
SF:rrect\x20current\x20password\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.67 seconds
```

```
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=Nov 18 19:21:27 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Nov 18 19:21:27 2023 GMT
```

```
read R BLOCK
JQtTfApK4SeyHwDlI9SXGR50qcl0Ail1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvm0kuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQAABoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLWd1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrlgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaESDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5SiWg0A
R57hJgleZiIvJv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/LemMEY5eTDAFmly9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBApLTfC1H0nWiMG0U3KPwYwT006CdTkmJ0mL8Ni
blh9ely29FsGxsgtRBXRsQXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZRqaM
77pBAoGAMmjmIjdjp+Ez8duyn3ieo36yrtrtF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxvIw8+TFVEB1104f7HvM6EpTscDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgysi/sN3RqRbCGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----


closed
```

```
bandit16@bandit:~$ mkdir /tmp/sshkey
mkdir: cannot create directory '/tmp/sshkey': File exists
bandit16@bandit:~$ cat /tmp/sshkey
cat: /tmp/sshkey: Is a directory
bandit16@bandit:~$ ls /tmp/sshkey
sshkey
bandit16@bandit:~$ cat /tmp/sshkey/sshkey
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvm0kuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQAABoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLWd1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrlgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaESDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5SiWg0A
R57hJgleZiIvJv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/LemMEY5eTDAFmly9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBApLTfC1H0nWiMG0U3KPwYwT006CdTkmJ0mL8Ni
blh9ely29FsGxsgtRBXRsQXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZRqaM
77pBAoGAMmjmIjdjp+Ez8duyn3ieo36yrtrtF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxvIw8+TFVEB1104f7HvM6EpTscDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgysi/sN3RqRbCGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```



```
bandit16@bandit:~$ mkdir /tmp/random_sshkey/random_sshkey
bandit16@bandit:~$ cat /tmp/random_sshkey/random_sshkey
cat: /tmp/random_sshkey/random_sshkey: Is a directory
bandit16@bandit:~$ ls /tmp/random_sshkey/random_sshkey
bandit16@bandit:~$ cd /tmp/sshkey
bandit16@bandit:/tmp/sshkey$ touch private.key
```

```
bandit16@bandit:/tmp/sshkey$ ssh -i private.key bandit17@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ssh/known_hosts).
```



```
message: 0x7f73ea
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

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

```
bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
VwOSWtCA7lRKKtFbr2IDh6awj9RNZM5e
```

VwOSWtCA7lRKKtFbr2IDh6awj9RNZM5e

Level 17 → Level 18

There are 2 files in the homedirectory: passwords.old and passwords.new. The password for the next level is in passwords.new and is the only line that has been changed between passwords.old and passwords.new.

NOTE: if you have solved this level and see 'Byebye!' when trying to log into bandit18, this is related to the next level, bandit19

Para obtener la contraseña debemos comparar los dos archivos que nos son proporcionados y quedarnos con el contenido único del archivo passwords.new. Para ello ejecutaremos el comando *diff passwords.old passwords.new*.

```
bandit17@bandit:~$ ls -la
total 36
drwxr-xr-x  3 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ..
-rw-r----- 1 bandit17 bandit17  33 Oct  5 06:19 .bandit16.password
-rw-r--r--  1 root     root     220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root     root    3771 Jan  6 2022 .bashrc
-rw-r----- 1 bandit18 bandit17 3300 Oct  5 06:19 passwords.new
-rw-r----- 1 bandit18 bandit17 3300 Oct  5 06:19 passwords.old
-rw-r--r--  1 root     root      807 Jan  6 2022 .profile
drwxr-xr-x  2 root     root    4096 Oct  5 06:19 .ssh
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW
_____
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```

[illegible]

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

Tras ejecutar el archivo que se nos ha indicado con el comando `./bandit20-do id` podremos obtener la contraseña leyendo el archivo donde se sitúa.

```
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ..
-rwsr-x---  1 bandit20 bandit19 14876 Oct  5 06:19 bandit20-do
-rw-r--r--  1 root    root      220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root    root      807 Jan  6 2022 .profile
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVyki6W36BkBU0mJTCM8rR95XT
```

VxCazJaVyki6W36BkBU0mJTCM8rR95XT

Level 20 → Level 21

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

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

En este nivel es necesario crear dos consolas para enviar comandos de una a la otra y conseguir que devuelva la contraseña para el siguiente nivel.

```
bandit20@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ..
-rw-r--r--  1 root    root      220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root    root      807 Jan  6 2022 .profile
-rwsr-x---  1 bandit21 bandit20 15600 Oct  5 06:19 suconnect
bandit20@bandit:~$ file suconnect
suconnect: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=4d95c75f0fe296f2477bfaad8b17039de5a56534, for GNU/Linux 3.2.0, not stripped
bandit20@bandit:~$ echo -n 'VxCazJaVyki6W36BkBU0mJTCM8rR95XT' | nc -l -p 1234 &
[1] 319311
```

```
bandit20@bandit:~$ ./suconnect 1234
Read: VxCazJaVyki6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
bandit20@bandit:~$
```

```
[1] 319311
bandit20@bandit:~$ NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

```

NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

Level 21 → Level 22

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

Al leer el contenido del archivo cronjob_bandit22 se nos indica la ruta donde está el archivo cronjob_bandit22.sh. Al leer el contenido de este archivo se indica la ruta donde se obtiene la contraseña para acceder al siguiente nivel.

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Oct  5 06:20 .
drwxr-xr-x 106 root root 12288 Oct  5 06:20 ..
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit22
-rw-r--r--  1 root root  122 Oct  5 06:19 cronjob_bandit23
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit24
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit25_root
-rw-r--r--  1 root root  201 Jan  8  2022 e2scrub_all
-rwx-----  1 root root   52 Oct  5 06:20 otw-tmp-dir
-rw-r--r--  1 root root  102 Mar 23  2022 .placeholder
-rw-r--r--  1 root root  396 Feb  2  2021 sysstat
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 /usr/bin
-bash: cd: /usr/bin: No such file or directory
bandit21@bandit:/$ cd /usr/bin
bandit21@bandit:/usr/bin$ cat cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/usr/bin$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff

Level 22 → Level 23

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

Al leer el contenido del archivo cronjob_bandit23 se nos indica la ruta donde está el archivo cronjob_bandit23.sh. Al leer el contenido de este archivo se obtiene un script de bash con el

comando que se deberá usar para obtener la ruta al archivo donde se encuentra la contraseña para acceder al siguiente nivel.

```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cd /usr/bin
bandit22@bandit:/usr/bin$ cat 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:/usr/bin$ echo I am user bandit23
I am user bandit23
bandit22@bandit:/usr/bin$ echo I am user bandit23 | md5sum
8ca319486bfbbc3663ea0fbe81326349 -
bandit22@bandit:/usr/bin$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/usr/bin$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G

Level 23 → Level 24

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Al leer el contenido del archivo cronjob_bandit24 se nos indica la ruta donde está el archivo cronjob_bandit2.sh. Al leer el contenido de este archivo se obtiene un script de bash que nos indica que el contenido de la carpeta que contiene la contraseña será borrado cuando se ejecute. Para poder obtener la contraseña crearemos otro archivo al que moveremos el contenido del archivo de la contraseña usando vim, le otorgaremos los permisos necesarios y leeremos el contenido de dicho archivo.

```

bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Oct  5 06:20 .
drwxr-xr-x 106 root root 12288 Oct  5 06:20 ..
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit22
-rw-r--r--  1 root root  122 Oct  5 06:19 cronjob_bandit23
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit24
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit25_root
-rw-r--r--  1 root root  201 Jan  8 2022 e2scrub_all
-rwx-----  1 root root   52 Oct  5 06:20 otw-tmp-dir
-rw-r--r--  1 root root  102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root  396 Feb  2 2021 sysstat
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$ cd /usr/bin
bandit23@bandit:/usr/bin$ cat cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

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

```

```

bandit23@bandit:/usr/bin$ cd ..
bandit23@bandit:/usr$ cd ..
bandit23@bandit:/$ mkdir /tmp/contra
bandit23@bandit:/$ cd /tmp/contra
bandit23@bandit:/tmp/contra$ vim contra.sh

```

```

#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/contra/destino.txt
~
~

```



```

bandit23@bandit:/tmp/contra$ ls -la
total 408
drwxrwxr-x  2 bandit23 bandit23  4096 Jan  7 17:14 .
drwxrwx-wt 2051 root      root    405504 Jan  7 17:15 ..
-rw-rw-r--  1 bandit23 bandit23    69 Jan  7 17:14 contra.sh
bandit23@bandit:/tmp/contra$ cat contra.sh
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/contra/destino.txt
bandit23@bandit:/tmp/contra$ man chmod
bandit23@bandit:/tmp/contra$ chmod o+x contra.sh
bandit23@bandit:/tmp/contra$ ls -la
total 408
drwxrwxr-x  2 bandit23 bandit23  4096 Jan  7 17:14 .
drwxrwx-wt 2052 root      root    405504 Jan  7 17:17 ..
-rw-rw-r-x  1 bandit23 bandit23    69 Jan  7 17:14 contra.sh
bandit23@bandit:/tmp/contra$ chmod o+w /tmp/contra
bandit23@bandit:/tmp/contra$ ls -la
total 408
drwxrwxrwx  2 bandit23 bandit23  4096 Jan  7 17:14 .
drwxrwx-wt 2057 root      root    405504 Jan  7 17:21 ..
-rw-rw-r-x  1 bandit23 bandit23    69 Jan  7 17:14 contra.sh
bandit23@bandit:/tmp/contra$ cp contra.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/contra$ ls -la /var/spool/bandit24
total 12
dr-xr-x---  3 bandit24 bandit23  4096 Oct  5 06:19 .
drwxr-xr-x  5 root      root    4096 Oct  5 06:19 ..
drwxrwx-wx 43 root      bandit24 4096 Jan  7 17:23 foo
bandit23@bandit:/tmp/contra$ ls -la /var/spool/bandit24/foo
ls: cannot open directory '/var/spool/bandit24/foo': Permission denied
bandit23@bandit:/tmp/contra$ ls -la /var/spool/bandit24/foo/contra.sh
ls: cannot access '/var/spool/bandit24/foo/contra.sh': No such file or directory
bandit23@bandit:/tmp/contra$ ls -la
total 412
drwxrwxrwx  2 bandit23 bandit23  4096 Jan  7 17:24 .
drwxrwx-wt 2061 root      root    405504 Jan  7 17:26 ..
-rw-rw-r-x  1 bandit23 bandit23    69 Jan  7 17:14 contra.sh
-rw-rw-r--  1 bandit24 bandit24    33 Jan  7 17:24 destino.txt
bandit23@bandit:/tmp/contra$ cat destino.txt
VAfGXJ1PBSsPSnvsjl8p759leLZ9GGar

```

VAfGXJ1PBSsPSnvsjl8p759leLZ9GGar

Level 24 → Level 25

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

You do not need to create new connections each time

Para hallar la contraseña de este nivel debemos ejecutar un ataque de fuerza bruta al puerto 30002 mediante un fichero bash con un script.


```

bandit24@bandit:~$ ls -la
total 20
drwxr-xr-x  2 root root 4096 Oct  5 06:19 .
drwxr-xr-x 70 root root 4096 Oct  5 06:20 ..
-rw-r--r--  1 root root  220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root root  807 Jan  6 2022 .profile
bandit24@bandit:~$ mkdir /tmp/fuerzabruta
bandit24@bandit:~$ cd /tmp/fuerzabruta
bandit24@bandit:/tmp/fuerzabruta$ ls -la
total 404
drwxrwxr-x  2 bandit24 bandit24  4096 Jan  7 18:48 .
drwxrwx-wt 2111 root      root    405504 Jan  7 18:49 ..
bandit24@bandit:/tmp/fuerzabruta$ vim archivo.sh
bandit24@bandit:/tmp/fuerzabruta$ car archivo.sh
Command 'car' not found, but can be installed with:
apt install ucommon-utils
Please ask your administrator.
bandit24@bandit:/tmp/fuerzabruta$ cat archivo.sh
#!/bin/bash

pw=VAfGXJ1PBsSPsnvsjI8p759leLZ9GGar

for code in {000..9999}
do
    echo "$pw $code"
done | netcat localhost 30002
bandit24@bandit:/tmp/fuerzabruta$ chmod u+x archivo.sh
bandit24@bandit:/tmp/fuerzabruta$ ./archivo.sh | grep -v "Wrong! Please enter the correct pincode. Try again."
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a
single line, separated by a space.
Correct!
The password of user bandit25 is p7TaowMYrmu230l8hiZh9UvD009hpx8d
Exiting.

```

p7TaowMYrmu230l8hiZh9UvD009hpx8d

Level 25 → Level 26

Logging in to bandit26 from bandit25 should be fairly easy... The shell for user bandit26 is not /bin/bash, but something else. Find out what it is, how it works and how to break out of it.

Al entrar en el servidor vemos que existe un fichero con una clave privada que debemos usar para acceder al siguiente nivel. Al intentar usarlo cerrará la conexión y ni dejará acceder. Al buscar información sobre dónde encontrar la contraseña encontraremos un directorio en el que se sitúa un archivo con un script en bash en el que se menciona un archivo llamado text.txt. Lo que debemos hacer es ejecutar el comando para acceder a la siguiente máquina con la clave privada, pero con la ventana de la consola de comandos mínimamente pequeña. Esto hará que no se cargue del todo antes de que cierre conexión, dejándonos tiempo suficiente para acceder con Shell y cambiar la configuración por defecto y poder visualizar el contenido del archivo txt mencionado anteriormente en el que se hallaba la contraseña.

```

bandit25@bandit:~$ ls
bandit26.sshkey
bandit25@bandit:~$ ssh bandit26@localhost -i bandit26.sshkey
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/ur

```

```

Connection to localhost closed.
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$ ssh bandit26@localhost -i bandit26.sshkey -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.

```

```

~
:shell
bandit26@bandit:~$ ls -la
total 44
drwxr-xr-x  3 root    root      4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root      4096 Oct  5 06:20 ..
-rwsr-x---  1 bandit27 bandit26 14876 Oct  5 06:19 bandit27-do
-rw-r--r--  1 root    root       220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root    root      3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root    root       807 Jan  6 2022 .profile
drwxr-xr-x  2 root    root      4096 Oct  5 06:19 .ssh
-rw-r-----  1 bandit26 bandit26  258 Oct  5 06:19 text.txt
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1

```

c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1

Level 26 → Level 27

Good job getting a shell! Now hurry and grab the password for bandit27!

Todavía dentro de la consola de Shell del apartado anterior deberemos buscar el archivo que contiene las contraseñas para el siguiente nivel y leer su contenido ejecutando el comando `./bandit-do cat /etc/bandit_pass/bandit27`

```

:shell
bandit26@bandit:~$ ls -la
total 44
drwxr-xr-x  3 root    root      4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root      4096 Oct  5 06:20 ..
-rwsr-x---  1 bandit27 bandit26 14876 Oct  5 06:19 bandit27-do
-rw-r--r--  1 root    root       220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root    root      3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root    root       807 Jan  6 2022 .profile
drwxr-xr-x  2 root    root      4096 Oct  5 06:19 .ssh
-rw-r-----  1 bandit26 bandit26  258 Oct  5 06:19 text.txt
bandit26@bandit:~$ cat ./bandit27-do
ELF4454
(444`~`◆◆◆DD ◆

```

```
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit/_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
bandit26@bandit:~$
```

YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

Level 27 → Level 28

There is a git repository at `ssh://bandit27-git@localhost/home/bandit27-git/repo` via the port 2220. The password for the user `bandit27-git` is the same as for the user `bandit27`.

Clone the repository and find the password for the next level.

Para hallar la contraseña crearemos un directorio nuevo en el que clonar el directorio de Git indicado con el comando `git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo` y posteriormente leer el contenido del archivo README.

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

```
bandit27@bandit:/tmp/clonado$ 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/ureryLY.
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).

bandit27@bandit:/tmp/clonado$ ls -la
total 408
drwxrwxr-x  3 bandit27 bandit27  4096 Feb 16 18:56 .
drwxrwx-wt 527 root      root    405504 Feb 16 18:58 ..
drwxrwxr-x  3 bandit27 bandit27  4096 Feb 16 18:57 repo
bandit27@bandit:/tmp/clonado$ cd repo
bandit27@bandit:/tmp/clonado/repo$ ls -la
total 16
drwxrwxr-x 3 bandit27 bandit27 4096 Feb 16 18:57 .
drwxrwxr-x 3 bandit27 bandit27 4096 Feb 16 18:56 ..
drwxrwxr-x 8 bandit27 bandit27 4096 Feb 16 18:57 .git
-rw-rw-r-- 1 bandit27 bandit27  68 Feb 16 18:57 README
bandit27@bandit:/tmp/clonado/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
```

AVanL161y9rsbcJIsFHuw35rjaOM19nR

Level 28 → Level 29

There is a git repository at `ssh://bandit28-git@localhost/home/bandit28-git/repo` via the port 2220. The password for the user `bandit28-git` is the same as for the user `bandit28`.

Clone the repository and find the password for the next level.

Para hallar la contraseña crearemos un directorio nuevo en el que clonar el directorio de Git indicado con el comando `git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo` y posteriormente leer el contenido del archivo `README.md` con el comando `git log -p`.

```
bandit28@bandit:~$ cd /tmp
bandit28@bandit:/tmp$ mkdir clonar
bandit28@bandit:/tmp$ cd clonar
bandit28@bandit:/tmp/clonar$ 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.
```

```
bandit28@bandit:/tmp/clonar/repo$ git log -p
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

diff --git a/README.md b/README.md
index b302105..5c6457b 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

- username: bandit29
-- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
+- password: xxxxxxxxxx
```

tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

Level 29 → Level 30

There is a git repository at `ssh://bandit29-git@localhost/home/bandit29-git/repo` via the port 2220. The password for the user `bandit29-git` is the same as for the user `bandit29`.

Clone the repository and find the password for the next level.

Para hallar la contraseña crearemos un directorio nuevo en el que clonar el directorio de Git indicado con el comando `git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo` y posteriormente al leer el contenido del archivo `README.md` con el comando `git log -p` se comprueba que la contraseña está oculta por lo que se analiza el resto del directorio con el comando `git branch -a`. Hacemos un cambio de rama a `remotes/origin/dev` ejecutando el comando `git checkout remotes/origin/dev` y ahora si ejecutamos el comando `cat README.md` para leer el archivo podremos visualizar la contraseña.

```

bandit29@bandit:/tmp/clon/repo$ git log -p
commit 4364630b3b27c92aff7b36de7bb6ed2d30b60f88 (HEAD -> master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date: Thu Oct 5 06:19:43 2023 +0000

    fix username

diff --git a/README.md b/README.md
index 2da2f39..1af21d3 100644
--- a/README.md
+++ b/README.md
@@ -3,6 +3,6 @@
@@ -3,6 +3,6 @@ Some notes for bandit30 of bandit.

## credentials

-- username: bandit29
+- username: bandit30
- password: <no passwords in production!>
04-06 pcap

commit fca34ddb7d1ff1f78df36538252aea650b0b040d
Author: Ben Dover <noone@overthewire.org>
Date: Thu Oct 5 06:19:43 2023 +0000

    initial commit of README.md

diff --git a/README.md b/README.md
new file mode 100644
index 0000000..2da2f39
--- /dev/null
+++ b/README.md
@@ -0,0 +1,8 @@
+# Bandit Notes
+Some notes for bandit30 of bandit.
+
+## credentials
+
+- username: bandit29
+- password: <no passwords in production!>
+

```

```

bandit29@bandit:/tmp/clon/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/sploits-dev
bandit29@bandit:/tmp/clon/repo$ ls -l
total 4
-rw-rw-r-- 1 bandit29 bandit29 131 Feb 16 19:40 README.md
bandit29@bandit:/tmp/clon/repo$ ls -la
total 16
drwxrwxr-x 3 bandit29 bandit29 4096 Feb 16 19:40 .
drwxrwxr-x 3 bandit29 bandit29 4096 Feb 16 19:40 ..
drwxrwxr-x 8 bandit29 bandit29 4096 Feb 16 19:40 .git
-rw-rw-r-- 1 bandit29 bandit29 131 Feb 16 19:40 README.md
bandit29@bandit:/tmp/clon/repo$ git checkout remotes/origin/dev
Note: switching to 'remotes/origin/dev'.

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 1d160de add data needed for development
bandit29@bandit:/tmp/clon/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

```

xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

Level 30 → Level 31

There is a git repository at `ssh://bandit30-git@localhost/home/bandit30-git/repo` via the port 2220. The password for the user `bandit30-git` is the same as for the user `bandit30`.

Clone the repository and find the password for the next level.

Para hallar la contraseña crearemos un directorio nuevo en el que clonar el directorio de Git indicado con el comando `git clone ssh://bandit30-git@localhost:2220/home/bandit30-git/repo` y posteriormente al leer el contenido del archivo `README.md` con el comando `git log -p` se comprueba que la contraseña no se encuentra ahí por lo que deberemos buscarla en otro lugar. Si ejecutamos el comando `git tag` comprobaremos que existe un archivo destacado de nombre “secret”. Al ejecutar el comando `git show secret` visualizaremos el contenido de este archivo y encontraremos la contraseña.

```
bandit30@bandit:/tmp/clonacion/repo$ cat README.md
just an empty file ... muahaha
```

```
bandit30@bandit:/tmp/clonacion/repo/.git$ git tag
secret
bandit30@bandit:/tmp/clonacion/repo/.git$ git show
commit d39631d73f786269b895ae9a7b14760cbf40a99f (HEAD → master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date: Thu Oct 5 06:19:45 2023 +0000

    initial commit of README.md

diff --git a/README.md b/README.md
new file mode 100644
index 0000000..029ba42
--- /dev/null
+++ b/README.md
@@ -0,0 +1 @@
+just an empty file ... muahaha
bandit30@bandit:/tmp/clonacion/repo/.git$ git show secret
OoffzGDIzhAlerFJ2cAiz1D41JW1Mhmt
```

OoffzGDIzhAlerFJ2cAiz1D41JW1Mhmt

Level 31 → Level 32

There is a git repository at `ssh://bandit31-git@localhost/home/bandit31-git/repo` via the port 2220. The password for the user `bandit31-git` is the same as for the user `bandit31`.

Clone the repository and find the password for the next level.

Para hallar la contraseña crearemos un directorio nuevo en el que clonar el directorio de Git indicado con el comando `git clone ssh://bandit31-git@localhost:2220/home/bandit31-git/repo` y posteriormente al leer el contenido del archivo `README.md` comprobaremos que piden hacer un push a un repositorio de un archivo con unas características en específico. Deberemos crear el archivo ejecutando el comando `echo 'May I come in?' > key.txt` y subirlo a la rama `master` del repositorio.

Al entrar en el servidor comprobaremos que estamos en una consola de Shell. La forma más rápida de salir de ahí es ejecutando el comando `$0`. Una vez fuera deberemos buscar la contraseña en el directorio de contraseñas con el comando `cat /etc/passwd/passwd`.

```
--[ More information ]--

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

For support, questions or comments, contact us on

Enjoy your stay!

WELCOME TO THE UPPERCASE SHELL
>> ls -la
sh: 1: LS: Permission denied
>> $0
$ whoami
bandit33
$ cat /etc/passwd/passwd
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
$
```

odHo63fHiFqcWWJG9rLiLDtPm45KzUKy

Level 33 → Level 34

Si estamos situados dentro del nivel anterior podemos acceder al archivo de contraseñas del siguiente nivel y al leerlo recibiremos un mensaje de felicitaciones por haber llegado hasta el final.

```
$ cd bandit33
$ ls -la
total 24
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
-rw-r--r-- 1 bandit33 bandit33 430 Oct 5 06:19 README.txt
$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
```