

OVER THE WIRE: BANDIT

NIVEL 0

Nos conectamos con el usuario **bandit0**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit.labs.overthewire.org -p 2220 -l bandit0
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([51.20.13.48]: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])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.

      OoTOL
    OoTOL
  OoTOL
OoTOL

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

Ahora vamos a escribir la contraseña **bandit0**.

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

      OoTOL
    OoTOL
  OoTOL
OoTOL

www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

NIVEL 0-1

Haciendo **ls** veremos que hay un archivo **readme**. Luego usamos **cat** para ver el contenido.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ file readme
readme: ASCII text
bandit0@bandit:~$ cat readme
NH2SXQwcBdpnTEzi3bvBHMM9H66vVXjL
```

NIVEL 1-2

Ahora tenemos que cerrar sesión con el otro usuario.

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Nos conectamos con el usuario **bandit1** y ponemos la contraseña que habíamos visto antes, es decir **NH2SXQwcBdpnTEzi3bvBHMM9H66vVXjL**.

Iniciamos con el usuario 3 y ponemos la contraseña que hemos averiguado **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
bandit3@bandit.labs.overthewire.org:~$
[bandit3@bandit.labs.overthewire.org ~]$

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

bandit3@bandit.labs.overthewire.org's password:
[bandit3@bandit.labs.overthewire.org ~]$

Welcome to OverTheWire!
```

Ahora vemos que hay un directorio llamado **inhere**, entonces, nos metemos en el directorio y con **ls -la** veremos los archivos ocultos, se sabe porque tiene un punto delante del nombre. Para que muestre la contraseña haremos un **cat .hidden**.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 3 root root 4096 Oct 5 06:19 ..
-rw-r----- 1 bandit4 bandit3 33 Oct 5 06:19 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EqX26xNe
```

NIVEL 4-5

Ahora nos conectamos con el usuario **bandit4** y usamos la contraseña que hemos descubierto **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
bandit4@bandit.labs.overthewire.org:~$
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit4@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Si nos metemos en el directorio **inhere** y usamos **ls** veremos que se muestran una serie de archivos. Usamos el comando **file** para saber cual es el que es solo legible por humanos, veremos que da error porque los nombres empiezan por un guión.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file02 -file04 -file06 -file08
-file01 -file03 -file05 -file07 -file09
bandit4@bandit:~/inhere$ file -file00
file: Cannot open '-file00' (No such file or directory)
```

Con **file inhere/*** podremos ver una lista de los archivos del directorio y el tipo de archivo. Luego vemos el **07** que es el que buscamos.

```
bandit4@bandit:~/inhere$ cd ..
bandit4@bandit:~$ file inhere/*
inhere/-file00: data
inhere/-file01: data
inhere/-file02: data
inhere/-file03: data
inhere/-file04: data
inhere/-file05: data
inhere/-file06: data
inhere/-file07: ASCII text
inhere/-file08: data
inhere/-file09: data
```

Con **cat \$(find . -name -file07)** podremos encontrar el archivo en el directorio actual por su nombre.

```
bandit4@bandit:~$ cat $(find . -name -file07)
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

NIVEL 5-6

Ahora nos conectamos con el usuario **bandit5** y usamos la contraseña que encontramos **lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220

      |-----|
      |  W A R G A M E  |
      |-----|

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

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

      |-----|
      |  W A R G A M E  |
      |-----|

www. ver he ire.org

Welcome to OverTheWire!
```

Con **ls** vemos que el directorio **inhere** tiene muchas carpetas y dentro de ellas varios archivos.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ ls inhere
maybehere00 maybehere04 maybehere08 maybehere12 maybehere16
maybehere01 maybehere05 maybehere09 maybehere13 maybehere17
maybehere02 maybehere06 maybehere10 maybehere14 maybehere18
maybehere03 maybehere07 maybehere11 maybehere15 maybehere19
bandit5@bandit:~$ ls inhere/maybehere00
-file1 -file2 -file3 spaces file1 spaces file2 spaces file3
```

Usando el comando **find . -type f -readable ! -executable -size 1033c** podemos encontrar el archivo, nos pide que sea legible por humanos que pese 1033 bytes y que no sea ejecutable. Luego podremos ver la contraseña con un **cat**.

```
bandit5@bandit:~$ find . -type f -readable ! -executable -size 1033c
./inhere/maybehere07/.file2
bandit5@bandit:~$ cat ./inhere/maybehere07/.file2
P4L4vucdmLnm8I7VL7jG1ApGSfjYKqJU
```

NIVEL 6-7

Ahora nos conectamos con el usuario **bandit6** y usamos la contraseña **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
bandit6@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

bandit6@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Con **find / -user bandit7 -group bandit6 -size 33c 2>/dev/null** podremos ver donde está la contraseña. Como dice el enunciado el usuario propietario es bandit07, el grupo propietario bandit6 y ocupa 33 bytes. Es importante poner **2>/dev/null** ya que si no, nos dará una serie de errores, así de esta forma los moverá a la carpeta /dev/null.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
```

Ahora con **cat** podremos ver la contraseña.

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

NIVEL 7-8

Ahora nos conectamos con el usuario **bandit7** y usamos la contraseña **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**.

[illegible]

Hacemos **ls** y veremos que nos sale el archivo **data.txt**.

```
bandit7@bandit:~$ ls
data.txt
```

Por tanto, si intentamos usar el comando **cat** nos saldrán un montón de palabras.

```
wildness      qeIJjHR6ESNmpSVjvLaJgEHEQ8ZvojXR
cryptic      tDsKFKCFiJN3AKZUA2jo9zk9zHPMob8v
insulated    hap7ekKNxREY26lFei4pDc109HeePBfZ
Galilean's   etjIu4p0t12g7cFsTKBZDn7bSPukrNSP
spottier     wjfxRvrkUDeA17HVSgoLbS1LYNKNPrEk
Leninist     psBW9GDj2hE7UHnqnFC35CFXRwkbrfl2
keg's        P0NngyFAZ3lklgeL6CpsdABYyIeTmPfh
wombats      orIlxWpS1HEEhGLFKUxxIVNgnuBLdQn
Oz's         R5YIBsxwrKYerFS6B1dferVW2v9BTDWU
trammelled   gXQy4Ia4PovoRHGBrYtxswFjk2h29U6X
ruckus       wUNLhit1obu9tccaewibY5e9MirLdJea
beware      oqYmAJWZS59576ZeXU7fcLADWNeefPd
anorak       CXCKC8kX2UGbQxCRSzhPl9UkzOd9htiT
enlistee     hyE5fxvDgVwZLsi6MoFLwEpbGuQLQ4s
explicitness KwAt377RLDakqHaUluMlR0NzOHlkowYX
promiscuously wkvgsAxHqTTFihMpoYGI7ojZHvpMhAyV
productive   sDl4qmTXNPs15x9D3IsLxGVF10EqwzYX
disordered   a6x1lMdSqVvY100rjAZySLqLGPdAJhQ
adore        jT53V0fLPJAIKUYTF5p3vZQLkkGanc9e
upending     YYYx41JatyNx4I6N5j5XG0d39bnCcBQq
Bovary's     f1xzomJ85L6gg7ewxh8m8A30QAD9Dtms
sixth        D7dGB7XgRs8Uqm9FE8zRZ18kEpyYVH2V
Crest        6l4s07m7ZGzTxkyh85Svto4R28VW80ws
clubbed      obq9NDKPZDKIUzE6JRzt130l137nz11A
crooned      zfm58FFtG7U0vvazyCsKIXvooTD9KDXm
diploma      b4a6aY5kZyCXPJOZZmS8RpFsh8jP0ehs
shoptalk's   zu2tSr30KyKufqCUZt1lwRfqmILRy4PR
Perseid's    B2TLmqpVfdirIA18X1tTD80qMs1LWfua
notarized    DZCHHVgDtruR4ZeAYa1md6ZU7Eu8AImF
privies      FBl6q70x52dMF9tspmAJzsju2KBjT05h
phosphorescent 8DgDBMF5bNU1Q6rnfIviZ29WniQLjNSs
ruminated    LwRTPPBaZ20MRsGqjvdCWLEL84aQHAz8
mousiness    I4NqrYM9ac2iNzWKjaOdLERMPQHsKUOI
Porsche      EFNbtfxuQMTkg77eILOvAe6FWpYv5Ez3
profligacy   1ku0bHBpMAEWNu1bhkpZHqr2Pe7QDJ1I
emirate's    LrCzySLRE6EIuOwgUwaS00EMb987Fsc9
Ursuline     IUGThLCrfxbdyGol0CXH06Uou2ISQYs
recurs       16nqw1mkfJa4ifh00aVossCnCKAdoKSc
Ruiz's       wYCIww6mLLr4Wy0U2GVlAx9WN1vYxR7
singulars     MnkXULrqBiMXhrgk0epEjHSgpdReZ0cY
rumpling     GwBw3Qzlp6qa6f8n1KqZv3SfU3ZrIG8o
disgracing   9nzKnRG7y6CAAzkbvae2dYx6Sij4WbU
nationalists vLV3DpQkkgUpnHp4h4WhIaN49x704N7e
innovated    lmEWKqVZgaxsoyneBTWmuJRVAZXK4R1R
gestures     eNDgsa09GI1ogI746fu9VSex0Ct1gzSG
flecking     7gti82GK0jLpdhbsPMnx6ltfTgtqYc80
polygon's    ygpK8xLIHAERsacu0bNDLDTUTDRTupID
```

Para poder encontrar la palabra **millionth** escribiremos **grep "millionth" data.txt** para que muestre la línea donde está la palabra que buscamos.

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


NIVEL 8-9

Ahora nos conectamos con el usuario **bandit8** y usamos la contraseña **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
bandit8@bandit.labs.overthewire.org:~$
      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/_/_/_/_/_/

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

bandit8@bandit.labs.overthewire.org's password:
OverTheWire
www. ver he ire.org

Welcome to OverTheWire!
```

Para encontrar la línea de texto que no se repite ordenaremos y borraremos las líneas repetidas con **sort -u data.txt**.

```
bandit8@bandit:~$ sort -u data.txt
18DyJwhN856SsMx8bNrFSvr6rJxNQKhE
1iyGemEgn3qU00FcAJyGPH0iewqZyp1y
2CQ5DQRdtoe9Ft8YpMHqCwQcN1Bk9LCI
365RauAVsFlxktPMpoLtIf1uxijU1TfV
4K2MoVHd1gXfo0DdjvLaRxFNZWmi4A4C
52p0CnGhAvm4m3fPKqz9mTxVDeVYCVnG
5Y76FifuxKStZi4CVovF2uPhgLrZnLzG
7A4l2BI3lPJgNdWAmYXAGlfB8uvCQLX0
8cxarYi5VoKRj3lzo2baLOJaMgUtzoRH
97Qwmy18JE8aGIud1stpTs0r0tUMHeGI
9d8exmGtSsGcU1gz6HmqTfSxmnmi4FBo
A16BW831T94qcsYcGDSkgzYhxnX2xUdK
aAd8RbcAAGVRifo0gE2x1nPIGH2fjgZi
ahwL1iJ5EDLT9wpBjrp2DY8pv6FLdrLy
AiYd84l00VTA4gqJPX7f6DH8eG3zwq1W
anIL5AEkrKcj4mFR1ujwPZdtF4z1SAin
b0XUx8jfewYAUGln0GGAYVRxdNziM4SF
bJDV415o5UyGPR98w9x5pX6nqws0U2ra
br26ueVSoLeZd8HqErTJpNVctwFufHG0
BVego10uHFYy1glUiCH3m5dQxEPV8D6d
bW08QpLAdUvLTPoI07UdQc6zKv0N0WS3
cEqNrEqHVIIi9fQKdcvAxa1p1brmsSxT
DmL3j9ydZQj13Q6xVRPHVumHd9pt0NbT
drJxnp5fJxeVRYlCldsIEtrEEwBdyRIL
eJZcdtHKg9jLpvpK9v31fj1opqlA1A9K
EN632PlfYiZbn3PhVK3XOGSLNInNE00t
eNdwlpf6iBeQ3o11iHefoHd9GYKDTIfQ
euIPhAlMI8n0DxPCbaAhJ9RTB03fx4UE
EzkkJebPKsBh9ERGT3vffA2NhtMCbFS5
EzyaX0FuwjLARDRsbctadMvVgZA1y1Sj
fGJ2YQ92lVRRgQ9dC0TlEMacCsw8Lm9
FJS8eDt5xeeyabbeEqyRV9W8uQ62BYnX
FQIgWPiUPKftkFhIy9Nzm94sWdNGTLHd
fuBEcq8TyETrSmuD2yQRmvp42K2jLwH
fWBv5AzQI14holge9okDa0vrgL7NGNTr
gAAoAApNgD1pS0c90TGWdsGTIwRDgY0M
g0tGle2Dg1bG8Ua5S5hN6CjIF14eGM4Qu
GuRn8oi7ecl8kSzTh1GrLHXhcfANBF7f
H4ZQ34QTylVVE6Q8nSQVQjtt7gAVztVX
hA2abugfwKD50EdFW4hSBacALoJiJSKg
HbIahMn0Q6vzNgo1RFXG7GPP8nQ90056
HmDZyN0zxPJAwcaZKhrU6S9vFbGuJ0g
```

Ahora con **cat data.txt | sort | uniq -u** ordenaremos las palabras y buscaremos la que no se repite.

```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
EN632PlfYiZbn3PhVK3XOGSLNInNE00t
```

Ahora nos conectamos con el usuario **bandit9** y usamos la contraseña **EN632PlfYiZbn3PhVK3XOGSINlnNE00t**.

Si usamos **file data.txt** veremos que es un archivo de datos y con **cat** podemos ver que salen símbolos raros.

```
bandit9@bandit:~$ file data.txt
data.txt: data
bandit9@bandit:~$ cat data.txt
~0Mk0Axj0ek0;0Jb0emi0~0j0]怪0ux0R~800004SA&l"000x0    6m0q00bf0es00
0-n0000n0000
      00~-00=| ǂ Jǁ<0==0uu0Jv00010`0;0s0eg0M-02k000ho(0010o00;T0;00DE*'
3ei,000x0dgiSn306E0p:000M000O!0d000etW000000]0j4&070FR^+06U000000#
                                                                d0wo'q0ǃ
                                                                0
0x0)0,V00*"0300_03+2)`00SHF000x[
0i0: 0i00}y00M203Hu0000i0[00U0(0.B09'0z,
                                W90Z0Pf0007A*000f0l0nd}00M00#0~
000=0000V000t60c000B90000~V2$0kyN000          00700\_;000q[V000~00%0Ŧc?G0000h00xkj
                                                    u+
Z00^gjb0
      000±0NE000u0zVC&0=pH00000`00=2""L(0hR"0!040D0000☪0%ñ0z0000000☒0w00|
000b00`00000Qu:qo000eN00W0k00
                        h00>3;00Z00
e0*02$A(00%0'000_)x0 0?0dm0WT0o00000&-0X000)0!
                                W0I0$}0000yr000cc'J020Z000N0ñ}0
0000Q0HI\}7 H00GH
      00R0%0]%0z000y v0T0C0(0000X0AE0000B"/kf"00tjh0ke/'#00D0206u0
!~\00)00s0ä0Xk0J007hoot0S0T0}0y902j20000I<00VI003X#90tk00i0s
                                0I00<0\
"x0000$0WI00G000gq00B0ş0q60p0|r90000K0|0[0l000000#0jb07u00uf'eY0000   ?>0?00
0F00){0x%010c3 00l0X0ZeU000
```

Ahora con **strings data.txt | grep "="** buscaremos los iguales eliminando todos los símbolos que no sean caracteres.

```
nN++<tM%LHZy;u_ nNoqbandit9@bandit:-$ strings data.t  
xt | grep "="  
=2""L(  
x]T===== theG)"  
===== passwordk^  
Y=xW  
t%=q  
===== is  
4=}D3  
{1}=  
FC&=z  
=V!m  
$/2`)=Y  
4_Q=\nMO=(  
?=|J  
WX=DA  
{Tbj;=l  
[=lI  
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s  
>8=6  
=r=_  
=uea  
zl=4
```

Para ordenar mejor la frase podemos usar **strings data.txt | grep "==" | awk {'print \$2'}**.

```
bandit9@bandit:~$ strings data.txt | grep "==" | awk {'print $2'}
theG)"
passwordk^
is
G7w8LIi6J3kTb8A7i9LqrvwTEULvvp6s
```

NIVEL 10-11

Ahora nos conectamos con el usuario **bandit10** y usamos la contraseña **G7w8Lli6J3kTb8A7j9LgrywtEUlryp6s**.

```
eduardo@eduardo-virtual-machine:~$ 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:
```

```

  _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-
 /  _   _   _   _   _   _   _   _   _   _   _   _   _   \
|  _   _   _   _   _   _   _   _   _   _   _   _   _   |
| _   _   _   _   _   _   _   _   _   _   _   _   _   |
|_   _   _   _   _   _   _   _   _   _   _   _   _   _|
 \  _   _   _   _   _   _   _   _   _   _   _   _   _   /
  _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-

www.         ver          he           "       ire.org

Welcome to OverTheWire!
```

Usamos **cat** y vemos que el contenido de **data.txt** está encriptado.

```
bandit10@bandit:~$ cat data.txt
VGhlIH8hc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==
```

Para averiguar la contraseña podemos usar el decodificador **base64 -d**.

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

NIVEL 11-12

Ahora nos conectamos con el usuario **bandit11** y luego la contraseña **6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
bandit11@bandit.labs.overthewire.org:~$
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit11@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Ahora con cat podemos acceder al archivo, pero vemos que solo salen letras sin sentido ya que se han rotado 13 posiciones.

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA00SFzMjXXBC0KoSKBbJ8puQm5lIEi
```

Para descifrarlo usaremos **cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'**.

```
bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'
The password is JVNBBFSmZwKKOP0XbFX0oW8chDz5yVRv
```

NIVEL 12-13

Ahora nos conectamos con el usuario **bandit12** y usamos la contraseña **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
bandit12@bandit.labs.overthewire.org:~$
[bandit12@bandit.labs.overthewire.org ~]$

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

bandit12@bandit.labs.overthewire.org's password:
[bandit12@bandit.labs.overthewire.org ~]$

Welcome to OverTheWire!
```

Mostramos el contenido de data.txt con cat y veremos que nos aparece esto.

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 6855 1e65 0203 6461 7461 322e ....hU.e..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin..=...BZh91AY
00000020: 2653 5948 1b32 0200 0019 ffff faee cff7 &SYH.2.....
00000030: f6ff e4f7 bfb9 ffff bff7 ffb9 39ff 7ffb .....9...
00000040: bd31 eeff b9fb fbbb b9bf f77f b001 3b2c .1.....;;
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340 .....hh...i...@
00000060: 1a68 00d0 0d01 a1a0 0001 a680 0003 46d4 .h.....F.
00000070: 6434 3234 611a 340d 07a4 c351 068f 5000 d424a.4....Q..P.
00000080: 069a 0680 0000 0006 8006 8da4 681a 6868 .....h.hh
00000090: 0d06 8d00 6834 3400 d07a 9a00 01a0 0341 ....h44..z....A
000000a0: ea1e a190 da40 3d10 ca68 3468 6800 00c8 ....@=..h4hh...
000000b0: 1a1a 1b50 0683 d434 d069 a0d0 3100 d000 ...P...4.i..1...
000000c0: 001e a680 00d0 1a00 d0d0 6864 d0c4 d0d0 .....hd....
000000d0: 000c 8641 7440 0108 032e 86b4 4cf0 22bb ...At@.....L."
000000e0: 6682 2b7e b3e2 e98d aa74 dacc 0284 330d f.+~.....t....3.
000000f0: bbb2 9494 d332 d933 642a 3538 d27e 09ce .....2.3d*58.~..
00000100: 53da 185a 505e aada 6c75 59a2 b342 0572 S..ZP^..luY...B.r
00000110: 249a 4600 5021 25b0 1973 c18a 6881 1bef $.F.P!%.s..h...
00000120: 3f9b 1429 5b1d 3d87 68b5 804f 1d28 42fa ?..)[.=.h..O.(B.
00000130: 16c2 3241 98fb 8229 e274 5a63 fe92 3aca ..2A...).tZc...
00000140: 70c3 a329 d21f 41e0 5a10 08cb 888f 30df p..)..A.Z.....0.
00000150: f3da ce85 418b 0379 6a65 cfa2 eeb7 9f01 ....A..yje.....
00000160: 782c da0e 288b e0c3 fe13 7af5 45ab 2b22 x,..(.....z.E.+"
00000170: a432 bf2f e32d b9e6 1465 2296 d805 a45e .2./.-...e"....^
00000180: d1c1 eacb 7483 6aac ca0e cf24 8864 bd40 ....t.j....$.d.@
00000190: 118c 644a 1dc6 a127 375c b7a6 c124 bdae ..dJ....'7\...$.
000001a0: 6d31 63a0 a223 3ea0 61d4 bdf0 450f 56fb m1c..#>.a...E.V.
000001b0: a546 8d34 08a2 4f1d 43d3 9063 404d dd43 .F.4...O.C..c@M.C
000001c0: b4f2 e65d bcb7 5932 0f5e 6802 3892 a988 ...].Y2.^h.8...
000001d0: 443d 8e89 7e09 4fb0 499d ee4e 4470 46c0 D=...~.O.I..NDpF.
000001e0: 2ba6 7c62 234a 7f76 151b aec0 23ee 4a97 +.|b#J.v....#.J.
000001f0: bc64 e34c de8a 5724 a1c3 9b89 cd96 1879 .d.L..W$......y
00000200: d560 0cbb 5c26 09e4 efaf 5b94 402a 7780 .'\&....[.@*w.
00000210: 4d87 30ce b8a3 946e 72c1 a643 1db7 a060 M.0....nr..C...`
00000220: 6524 629c 0c7e 8e7b e0f8 820c d5cb 60a0 e$b...~.{.....`
00000230: 003c a584 d4c1 61ef eb02 3f65 3a54 a3a2 .<....a...?e:T..
00000240: a565 c154 34c2 b162 d206 1ff8 bb92 29c2 .e.T4..b.....)
00000250: 8482 40d9 9010 b3a9 e478 3d02 0000 ..@.....x=...
```

Vamos a crear un directorio en **/tmp** con **mkdir /tmp/nombreDirectorio** y lo vamos a copiar con **cp data.txt/tmp/lara**.

```
bandit12@bandit:~$ mkdir /tmp/eduardo
bandit12@bandit:~$ cp data.txt /tmp/eduardo
```

Ahora seguimos los pasos hasta que nos salga un archivo ASCII que será donde está la contraseña.

```
bandit12@bandit:/tmp/eduardo$ xxd -r data.txt n1
bandit12@bandit:/tmp/eduardo$ file n1
n1: 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/eduardo$ mv n1 data2.gz
bandit12@bandit:/tmp/eduardo$ ls
data2.gz  data.txt
```

```
bandit12@bandit:/tmp/eduardo$ gzip -d data2.gz
bandit12@bandit:/tmp/eduardo$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/eduardo$ mv data2 data3.bz2
bandit12@bandit:/tmp/eduardo$ bzip2 -d data3.bz2
bandit12@bandit:/tmp/eduardo$ file data3
data3: 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/eduardo$ mv data3 data4.gz
bandit12@bandit:/tmp/eduardo$ gzip -d data4.gz
bandit12@bandit:/tmp/eduardo$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/eduardo$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/eduardo$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/eduardo$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/eduardo$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/eduardo$ mv data6.bin data7.bz2
bandit12@bandit:/tmp/eduardo$ bzip2 -d data7.bz2
bandit12@bandit:/tmp/eduardo$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/eduardo$ tar -xvf data7
data8.bin
bandit12@bandit:/tmp/eduardo$ 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/eduardo$ mv data8.bin data9.gz
bandit12@bandit:/tmp/eduardo$ file data9
data9: cannot open 'data9' (No such file or directory)
bandit12@bandit:/tmp/eduardo$ gzip -d data9.gz
bandit12@bandit:/tmp/eduardo$ file data9
data9: ASCII text
bandit12@bandit:/tmp/eduardo$ cat data9
The password is wBwDlBxEir4CaE8LaPhauuOo6pwRmrDw
```

NIVEL 13-14

Ahora nos conectamos con el usuario **bandit13** y usamos la contraseña **wBwDlBxEir4CaE8LaPhauuOo6pwRmrDw**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
bandit13@bandit.labs.overthewire.org:~$

  _ _ _ _ _
 | B | A | N | D | I | T |
 | _ | _ | _ | _ | _ | _ |
  | | | | |

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

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

  _ _ _ _ _
 | O | v | e | r |
 | _ | _ | _ | _ |
  | | | | |

  _ _ _ _ _
 | w | w | w | . |
 | _ | _ | _ | _ |
  | | | | |

  _ _ _ _ _
 | v | e | r | |
 | _ | _ | _ | _ |
  | | | | |

  _ _ _ _ _
 | h | e | | |
 | _ | _ | _ | _ |
  | | | | |

  _ _ _ _ _
 | i | r | e | . |
 | _ | _ | _ | _ |
  | | | | |

  _ _ _ _ _
 | o | r | g | |
 | _ | _ | _ | _ |
  | | | | |

Welcome to OverTheWire!
```

Con **ssh bandit14@bandit.labs.overthewire.org -p 2220 -i sshkey.private** nos podremos conectar con el usuario **bandit14**.

```

bandit13@bandit:~$ ssh bandit14@bandit.labs.overthewire.org -p 2220 -i sshkey.private
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrECLfXC5CXlhmAAM/uerLY.
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

```

NIVEL 14-15

Ahora con **cat /etc/bandit_pass/bandit14** podemos ver la contraseña del usuario **bandit14**. Si ponemos esa contraseña en el puerto **30000** del **localhost** nos saldrá la contraseña de **bandit15**.

```

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Connection closed by foreign host.

```

NIVEL 15-16

Ahora nos conectamos con el usuario **bandit15** y usamos la contraseña **jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**.

```

eduardo@eduardo-virtual-machine:~$ ssh bandit15@bandit.labs.overthewire.org -p 2220
[bandit.labs.overthewire.org]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit15@bandit.labs.overthewire.org's password:
www. ver he " tre.org
Welcome to OverTheWire!

```

Ahora nos conectamos al puerto 30001 y le ponemos la contraseña del anterior usuario.


```
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
```

```
read R BLOCK
JQtTfApK4SeyHwDlI9SXGR50qcl0Ail1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIeogIBAAKCAQEAvM0kufmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJ0bArnd9Y7YT2bRPQ
Ja6Lzb558YW3FZL870RiO+rW4LDCND2lUvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mQYvmzpwTMAzJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
```

Creamos un directorio y pegamos la clave dentro.

```
bandit16@bandit:~$ mkdir /tmp/soyEdu
bandit16@bandit:~$ cd /tmp/soyEdu
```

```
bandit16@bandit:/tmp/soyEdu$ nano soyEdu
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.

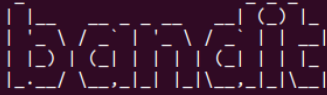
bandit16@bandit:/tmp/soyEdu$ cat soyEdu
-----BEGIN RSA PRIVATE KEY-----
MIIeogIBAAKCAQEAvM0kufmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJ0bArnd9Y7YT2bRPQ
Ja6Lzb558YW3FZL870RiO+rW4LDCND2lUvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mQYvmzpwTMAzJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQBAoIBABagpxpM1aoLWfvd
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RlLwD1NhPx3iB1
J9n0M80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESZH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtf4uNtJom+asvlpms8A
vLY9r60wY5vmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXycUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuR3b2G82so8vUHk/fur850Efc9TncnCY2crpoqsgghifKLxrlgt+qDpfZnx
SatLdt8GfQ85yA7hnWJ2Mx3NaeSDm75Lsm+tBbAlyc9P2jGRntMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZFYeiE/v45bN4yFm8x7R/b0ie7KaszX+Exdvt
SghatdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3L5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmLy9FL2m9oQWcg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwGXlnB30hYlmtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPltFc1H0nWiMGOU3KPwYwT006CdTkMJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdS0okVDQNWu6ucyLRAWFuISexw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIjDjp+Ez8duyn3ieo36yrTtF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVM6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

Con chmod 600 aplicamos permisos de lectura y escritura para el usuario.

```
bandit16@bandit:/tmp/soyEdu$ chmod 600 soyEdu
```


Ahora nos conectamos con **bandit17**

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



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

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



Welcome to OverTheWire!

Nivel 17-18

diff passwords.old passwords.new nos da la diferencia entre la contraseña antigua y nueva.

```
bandit17@bandit:~$ ls
passwords.new passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHcnmCNxuAt0KtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```

Accedemos con el usuario **bandit18** y la contraseña **hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220
bandit18@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

bandit18@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

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

NIVEL 18-19

Ahora volvemos a acceder, pero añadimos **cat readme** y nos saldrá la contraseña.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220
bandit18@bandit.labs.overthewire.org's password:
cat readme
Welcome to OverTheWire!

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

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

Ahora nos conectamos con el usuario **bandit19** y usamos la contraseña **awhqfNnAbc1naukrpqDYcF95h7HoMTTrC**.

Para ver el contenido de **bandit20** usamos el comando **./bandit20-do cat /etc/bandit_pass/bandit20**.

```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVyki6W36BkBU0mJTCM8rR95XT
```

NIVEL 20-21

Ahora nos conectamos con el usuario **bandit20** y usamos la contraseña **VxCazJaVykl6W36BkBU0mJTCM8rR95XT**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit20@bandit.labs.overthewire.org -p 2220
bandit20@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

bandit20@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

El comando **echo -n "VxCazJaVykl6W36BkBU0mJTCM8rR95XT" | nc -l -p 1234 &** envía la cadena "VxCazJaVykl6W36BkBU0mJTCM8rR95XT" a través de la red a un servidor que escucha en el puerto 1234 utilizando Netcat (nc).

```
bandit20@bandit:~$ echo -n "VxCazJaVykl6W36BkBU0mJTCM8rR95XT" | nc -l -p 1234 &
[1] 275832
bandit20@bandit:~$ ./suconnect 1234
Read: VxCazJaVykl6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
```

NIVEL 21-22

Ahora nos conectamos con el usuario **bandit21** y usamos la contraseña **NvEJF7oVjkddltPSrdKEFOllh9V1IBcq**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit21@bandit.labs.overthewire.org -p 2220
bandit21@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

bandit21@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Ahora accedemos a **cron.d** y miramos el contenido con **ls**. Después miramos el contenido del script que lee la contraseña del usuario **bandit22** y la guarda en el fichero **/tmp/t706../**.

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit23      e2scrub_all
cronjob_bandit17_root  cronjob_bandit24      otw-tmp-dir
cronjob_bandit22       cronjob_bandit25_root sysstat
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlnwMfj4EZff
```

NIVEL 22-23

Ahora nos conectamos con el usuario **bandit22** y usamos la contraseña **WdDozAdTM2z9DiFEQ2mGlnwMfj4EZff**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit22@bandit.labs.overthewire.org -p 2220
bandit22@bandit.labs.overthewire.org's password:
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit22@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Ahora volvemos al directorio **cron.d** y miramos el contenido de **cronjob_bandit23**. Vemos el contenido de la ruta que nos sale y copiamos el comando.

```
bandit22@bandit:/etc/cron.d$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit23      e2scrub_all
cronjob_bandit17_root  cronjob_bandit24      otw-tmp-dir
cronjob_bandit22       cronjob_bandit25_root sysstat
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

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

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

cat /etc/bandit_pass/$myname > /tmp/$mytarget

bandit22@bandit:/etc/cron.d$ echo I am user $myname | md5sum | cut -d ' ' -f 1
7db97df393f40ad1691b6e1fb03d53eb
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

NIVEL 23-24

Ahora nos conectamos con el usuario **bandit23** y usamos la contraseña **QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit23@bandit.labs.overthewire.org -p 2220
[bandit23@bandit23 ~]$

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

bandit23@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit23@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!
```

Ahora repetimos el proceso, pero con **cronjob_bandit24**.

```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit23      e2scrub_all
cronjob_bandit17_root  cronjob_bandit24      otw-tmp-dir
cronjob_bandit22        cronjob_bandit25_root 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$ 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 un directorio en **/tmp** y escribimos el script **#!/bin/bash cat /etc/bandit_pass/bandit24 >> /tmp/pizza/nivel24**. Lo que va a hacer es leer la contraseña de bandit24 y almacenarla en /tmp/pizza/.

```
bandit23@bandit:/etc/cron.d$ mkdir /tmp/chipa
bandit23@bandit:/etc/cron.d$ cd /tmp/chipa
bandit23@bandit:/tmp/chipa$ nano bandit24.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
```

```
bandit23@bandit:/tmp/chipa$ cat bandit24.sh
cat /etc/bandit_pass/bandit24 > /tmp/chipa/nivel24
```

Damos permisos a **bandit24.sh** y al directorio chipa.

```
bandit23@bandit:/tmp/chipa$ chmod 777 bandit24.sh
bandit23@bandit:/tmp/chipa$ cd ..
bandit23@bandit:/tmp$ chmod 777 chipa
bandit23@bandit:/tmp$ cd chipa
```

Lo copiamos al siguiente directorio.

```
bandit23@bandit:/tmp/chipa$ cp bandit24.sh /var/spool/bandit24/foo
```

Y vemos que aparece.

```
bandit23@bandit:/tmp/chipa$ ls
bandit24.sh  nivel24
bandit23@bandit:/tmp/chipa$ cat nivel24
VAFGXJ1PBSsPSnvsjI8p759leLZ9GGar
```

NIVEL 24-25

Ahora nos conectamos con el usuario **bandit25** y usaremos la contraseña **VAFGXJ1PBSsPSnvsjI8p759leLZ9GGar**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit24@bandit.labs.overthewire.org -p 2220

  _____
 | _   _  _   _ |
 | | | | | | | |
 | |_| | | |_| |
 |  __/ |  __/ |
 |_____|_____|

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

bandit24@bandit.labs.overthewire.org's password:

  _____
 | _   _  _   _ |
 | | | | | | | |
 | |_| | | |_| |
 |  __/ |  __/ |
 |_____|_____|

www.OverTheWire.org

Welcome to OverTheWire!
```

Creamos un directorio en **/tmp** y dentro un script.

```
bandit24@bandit:~$ mkdir /tmp/arroz
bandit24@bandit:~$ cd /tmp/arroz
bandit24@bandit:/tmp/arroz$ nano bruteforcer.sh
Unable to create directory /home/bandit24/.local/share/nano/: No such file or direct
ory
It is required for saving/loading search history or cursor positions.
```

Generamos un listado con todos los números posibles.

```
bandit24@bandit: /tmp/arroz
GNU nano 6.2 bruteforcer.sh *
#!/bin/bash

passwd="VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar"

for i in {8000..9999}
do echo $passwd '$i' >> output.txt
done
```

Damos permisos, ejecutamos el script y enviamos los resultados a través de la red a localhost en el puerto 30002, y luego guardamos esos resultados en result.txt

```
bandit24@bandit:/tmp/arroz$ chmod 777 bruteforcer.sh
bandit24@bandit:/tmp/arroz$ ./bruteforcer.sh
bandit24@bandit:/tmp/arroz$ cat output.txt | nc localhost 30002 >> result.txt
bandit24@bandit:/tmp/arroz$ sort result.txt | uniq -u

Correct!
Exiting.
The password of user bandit25 is p7TaowMYRmu230l8hiZh9UvD009hpx8d
```

NIVEL 25-26

Ahora nos conectamos con el usuario **bandit25** y usaremos la contraseña **p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d**.

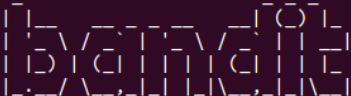
[illegible]

Vemos que si accedemos se nos cierra la conexión.

NIVEL 27-28


Ahora accedemos con el usuario **bandit27** y usamos la contraseña **YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit27@bandit.labs.overthewire.org -p 2220
```



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

```
bandit27@bandit.labs.overthewire.org's password:  
Permission denied, please try again.  
bandit27@bandit.labs.overthewire.org's password:
```



```
www.ver he ire.org
```


```
Welcome to OverTheWire!
```

Creamos un directorio en **/tmp**.

```
bandit27@bandit:~$ ls
bandit27@bandit:~$ cd /tmp
bandit27@bandit:/tmp$ mkdir maiz
bandit27@bandit:/tmp$ cd maiz
bandit27@bandit:/tmp/maiz$
```

Dentro clonamos el repositorio de git.

```
bandit27@bandit: /tmp/maiz$ 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:C2ihUBV7ihnV1wUXRb4RreCLFXC5CKlhmAAM/urcrLY.
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.
```

Dentro encontramos la contraseña.

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

NIVEL 28-29

Ahora accedemos con el usuario **bandit28** y usamos la contraseña **AVanL161y9rsbcJIsFHuw35rjaOM19nR**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit28@bandit.labs.overthewire.org -p 2220
bandit28@bandit.labs.overthewire.org's password:
bandit28@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit28@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```

Hacemos los mismos pasos que antes.

```
bandit28@bandit: /tmp/harina$ 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:C2ihUBV7ihhV1wUXRb4RrEcLFXC5CXlhmAAM/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).

  _ _ _ _ _
 | B | A | N | D | I | T |
 | _ | _ | _ | _ | _ |
  | | | | |

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/harina$ ls
repo
bandit28@bandit: /tmp/harina$ cd repo
bandit28@bandit: /tmp/harina/repo$ ls
README.md
bandit28@bandit: /tmp/harina/repo$ cat README.MD
cat: README.MD: No such file or directory
bandit28@bandit: /tmp/harina/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxxxx
```

Con **git log** veremos el historial de commits y **git show** muestra los detalles.

```
bandit28@bandit: /tmp/harina/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/harina/repo$ git show
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

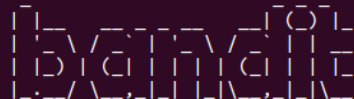
diff --git a/README.md b/README.md
index b302105..5c6457b 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

- username: bandit29
-- password: tQKvrcwNYcFS6vmPHIUSI3ShmsrQZK8S
+- password: xxxxxxxxxxxx
```

NIVEL 29-30


Ahora accedemos con el usuario **bandit29** y usamos la contraseña **tQKvmcwNYcFS6vmPHIUSl3ShmsrQZK8S**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit29@bandit.labs.overthewire.org -p 2220
```



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


```
bandit29@bandit.labs.overthewire.org's password:  
Permission denied, please try again.  
bandit29@bandit.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!
```

Repetimos los pasos.

```
bandit29@bandit:/tmp/pan$ 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:C2ihUBV7ihhV1wUXRb4RrEcLfXC5CXlhmAAM/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/pan$ cat README.md
cat: README.md: No such file or directory
bandit29@bandit:/tmp/pan$ ls
repo
bandit29@bandit:/tmp/pan$ cd repo
bandit29@bandit:/tmp/pan/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>
```


Cambiamos a la rama **dev**.

```
connection closed by 172.01.15.10 port 2220
eduardo@eduardo-virtual-machine:~$ ssh bandit30@bandit.labs.overthewire.org -p 2220

      _____
     |   _   _   |
    |  ( ) ( )  |
    |  _   _   |
    | / \ / \  |
    |/_\_\/\_\\_|

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

bandit30@bandit.labs.overthewire.org's password:
```



```
www. ver he ire.org

Welcome to OverTheWire!
```


git tag lista las etiquetas del repositorio y **git show** muestra su contenido.

```
bandit30@bandit:/tmp/aceite$ 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:C2ihUBV7lhnV1wUXRb4RrEcLfXC5CXlhmAAM/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).

      _ _ _ _ _
     /   /   /
    /___/___/
   /___/___/
  /___/___/
 /___/___/
/___/___/

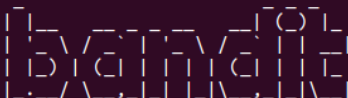
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

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/aceite$ ls
repo
bandit30@bandit:/tmp/aceite$ cd repo
bandit30@bandit:/tmp/aceite/repo$ ls
README.md
bandit30@bandit:/tmp/aceite/repo$ cat README.md
just an empty file... muahaha
bandit30@bandit:/tmp/aceite/repo$ git tag
secret
bandit30@bandit:/tmp/aceite/repo$ git show secret
0offzGDLzhAlerFJ2cAiz1D41JW1Mhmt
```


NIVEL 31-32

Ahora nos conectamos con el usuario **bandit31** y usamos la contraseña **OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt**.

```
eduardo@eduardo-virtual-machine:~$ ssh bandit31@bandit.labs.overthewire.org -p 2220
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit31@bandit.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!
```

Otra vez repetimos los pasos.

```
bandit31-git@localhost:~$ cd /tmp/cebolla
bandit31@bandit:/tmp/cebolla$ 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:C2lhUBV7ihhV1wUXRb4RreCLFXC5CKlhmAAM/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/cebolla$ ls
repo
bandit31@bandit:/tmp/cebolla$ cd repo/
bandit31@bandit:/tmp/cebolla/repo$ ls
README.md
bandit31@bandit:/tmp/cebolla/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

Editamos el archivo **key.txt** con el contenido que salía. Luego hacemos un **commit** añadiendo los cambios y hacemos un **push**.

```
bandit31@bandit: /tmp/cebolla/repo
GNU nano 6.2 key.txt *
May I come in?
```



```
WELCOME TO THE UPPERCASE SHELL
>> ls
sh: 1: LS: Permission denied
>> $0
$ ls
uppershell
$ ls -al
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 bandit33 bandit32 15128 Oct  5 06:19 uppershell
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqclWWJG9rLiLDtPm45KzUKy
```

Ahora nos conectamos con el usuario **bandit33** y usaremos la contraseña **odHo63fHiFqcWWJG9rLiLDtPm45KzUKy**.

Al hacer un **ls** nos encontramos un archivo de texto, si mostramos el contenido con **cat** podemos leer que hemos llegado al último nivel.

```
bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ 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!
```