

OVER THE WIRE: BANDIT

NIVEL 0

Nos conectamos con el usuario **bandit0**.


```
lara@lara-virtual-machine:~$ 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/urerLY.
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.
```



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

Luego escribimos la contraseña **bandit0**.

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



```
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

Si hacemos un **ls** veremos que hay un archivo **readme**. Usamos **cat** para ver el contenido.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ file readme
readme: ASCII text
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

NIVEL 1-2

Primero cerramos sesión con el otro usuario.

```
bandit1@bandit.labs.overthewire.org: Permission denied (publickey).
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

[illegible]

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

Iniciamos con el usuario **bandit2** y la contraseña anterior **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
aBZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG
```

Iniciamos con el usuario 3 y ponemos la contraseña que hemos averiguado **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2IAiG**.

Vemos que hay un directorio llamado **inhere**. 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

Nos conectamos con el usuario **bandit4** y la contraseña que hemos descubierto **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**.

```
lara@lara-virtual-machine:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
bandit4@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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. Al usar 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 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -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. Podemos ver que el **07** 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)
lrIWWI6bB37kxfiCQzUd0IYfr6eEeqR
```

NIVEL 5-6

Nos conectamos con el usuario **bandit5** y la contraseña que encontramos **IrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**.

```
lara@lara-virtual-machine:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
bandit5@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

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

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

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ ls inhere
maybe00 maybe02 maybe04 maybe06 maybe08 maybe10 maybe12 maybe14 maybe16 maybe18
maybe01 maybe03 maybe05 maybe07 maybe09 maybe11 maybe13 maybe15 maybe17 maybe19
bandit5@bandit:~$ ls inhere/maybe00
-file1 -file2 -file3 spaces file1 spaces file2 spaces file3
```

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

```
bandit5@bandit:~$ find . -type f -readable ! -executable -size 1033c
./inhere/maybe07/.file2
bandit5@bandit:~$ cat ./inhere/maybe07/.file2
P4L4vucdmLnm8I7VL7jG1ApGSfjYKqJU
```

NIVEL 6-7

Nos conectamos con el usuario **bandit6** y la contraseña **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**.

```
lara@lara-virtual-machine:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
bandit6@bandit.labs.overthewire.org:~$
[bandit]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit6@bandit.labs.overthewire.org's password:
[over]
www. ver he " ire.org
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 **bandit7**, 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

Nos conectamos con el usuario **bandit7** y la contraseña **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**.

```
lara@lara-virtual-machine:~$ ssh bandit7@bandit.labs.overthewire.org -p 2220
bandit7@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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

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

Welcome to OverTheWire!
```

Si hacemos **ls** veremos que nos sale el archivo **data.txt**.

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

Sin embargo, si intentamos usar el comando **cat data.txt** nos saldrán un montón de palabras.

```
tabulates b7Hc249ePLOfckFhH0CzfneurkfcFvLv
roughnecklng ahnj1jwkNC74DVZzFLkau1HtUxUXYhz
parboiling JZhWlXtc9dDE5EEdHxeyF4B0Vlx7hzqo
stupor's lhy3LJEUqhQqMXD03LF9wNKVMaGhMWqn
woes rpkIAQasUDyHozuvTecOhClyXwNACGxJ
squishy s1jQrdXUFnVL5Lx3pgSGembLHLQqdfde
megahertz's z7UsBdhjMUoAeXsFKE1p0RqPABvmxsn
potter's FZ6xOabRT9uYuzU3rvvHyAPaW8lLqG
Josefina AdMsMLajW4cgv63rVg702Aye84Qv766h
gondolier TZngnrKIKEL7wGx6aXTdjDyxR2Nxs9L
Kazan gAs0n0ZQ7Ft41UuengeMQlKxmAayohXZ
colony's ZqoB0TKLxectQJ2WZXLHrXk13BLDCAP6
ultrasound's 6MaYnsNm07FvFDtGskBF1a49qRkCpZCK
webb LAXTBWtjaHdrcXw7ULq99gvU0KDXMWvF
autographs oxfSj0T2LkAaong8E73cd50HZxtZpHfn
slather t0AahjY8nje6a4ZGH0zcl7oA08AhjWla
lapel VJVVEvpkLwLAhhMPqYKVK0ksBFCCM9rD
crystals UVvn460u0usPe6RwF53ha6NKM9qpPXi
dilemmas pLOMl5cBohyJD4jUaGfL0Bzqz2V5SbzK
existence EgvP4X40bLDNhsdUBkvYafUZkPAaM2s
phantasmagoria's elyslNmBwJOFKF2ouRo5LcbqK9KZha0
hairdo AYTjHzE8QIUaFX9keCFypMn69e80J3
he'd cX1hDFuscZUaFLWfNGImUwsOFHRdVER
shuttlecocking tBSLG10b0kLEJrWUlnYvGKL9sotBK5qk
dispels 5DAboUXnULYjxm08z0ndlm6rdNL9KPVT
guileful spcGVFF97JkTrXN80opoX0ZdbA480yu7
ruinous odrzAD0GucskT750U0j54600A1xectXT
demagog u4Qrk4KiGR7afpbdy5pC7FQHXqE70ES
impatience EFEGETd00EJU0F09qrX7reAX10hysg
cooling XEgZpHXCNM7dmxlf6eryRskJGPNnKSdf
purposely LReccMMuokWRCKVCES1ISUqIEtbs59Sf8
manhole CzxA0vJpvoxEOLGXpMbrxp99S5X2PWl7t
Thomson's HgAtRcR6ymhgnyu26WfNj4rxS5LMaTr
voltage's 95WZqHep7GxERMyJGxS3g7B1rmqL9CQ2
dentifrice's SxwWnGT0qhr6h2UBUQdcMv0cqqTwfB8h
browsing WiHmLJP9VJ66Z9VMCE1VGdfzHaFVnHp1
antimony V0jdsKtTurSXFtrUJKZusrI8uqxGtLn
Mohacs r9hIugnXQLCzB04CPAQMT4PQubJ0KX
Esperanza's 6yRplZxXEQ3LzU0VCJnImMz01J0j8sL
Hansen's 2WKFAtU99xg9iLo0Drq5yThMLb220ky
Mentholatum 7LYHoNagOp1Q1Mhz7Lg4jDIITSa6wLJ
broiled IliqbuH2Kr5UGczbvUuS5aJ09cVMVE4n
napping JhdPv2IRlyq8RCMuus61VLqC39sCgASA
sautés NcMuhzwVnyUfc9Q5wQEU4CgX7wptucy6
planned TsuTwVaxLpFsULQlTwzooy5JysKK6KW
escapades WGIwZYV86mCF73rf7U9iIIFg4N7czTr
Nam's x7tFqUtoHAKjP3g56Vl7QRjU96XWlZ0b
overtook zyLxYDXDbXU6WMDLoC4zDhcvkxLxSRZa
semprlvate Ltu6ME6fsb2J4CQWKnIx71b4pu6q13h
```

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

[illegible]

```
bandit8@bandit:~$ sort -u data.txt
18DyJwhN856S5xm8BnRf5vr6rJxNQKhE
1lyGemEgn3qU00fCAJyGPH0lEwqYp1C
2CQ5DQrdtoe9fT8yPmGhcWcQN1BK9LrI
365RauAVsFlxktPMpoLtif1uxijU1Tfv
4K2MoVhd1gXfoOdDj3v9ArfXNZwm1A4AC
52p0CnGhAvm4d31fPKqJzlrTxVDeYcVnG
5Y76F1fuxKStz124CvovF2mPhVrZnLzG
7A4L2BI3LPjgNdWAmYXAGlfB8uvCQLX0
8cxarY5iVoKrJ3lzo2baL0rJAmgUtZoRH
97Qwmy18JEF8aG1ud1stpsL0r0tUMHGeGI
9d8exnGtS5GcU1gz6HmqTfSxmnnI4FBo
A16B8B31T94qcsYcGDSkgYhxnX2zUdK
aAd8R8cAAGVRi0e0gE2n1IPGH2fjgzI
ahwL1lJ5EDL1t9wpB3rPD2Y8p6vFLdrLy
AiYd84l0OVTA4gqJPKX7f6DH8EG3zwq1W
anX15AEakRcJ4mFR1UjGwYrDfz4z1SAin
b0XUX8jfeWYAUGL10GGAPVrXdNz1M4SF
b3DV412o5yGPR98w9x5pX6nqWsoU2ra
br26ueVSoLeZd8HqEfT3pNVctwFvFHGO
BVego10uHFy1g1uIC3m5dZcxEPV8D6d
bw80qPlAdUvLTpO7I9du0c62kvON0WS3
cEqNrEqHVIIi9fQKdcvAxaip1brmsSxT
DnL3j9ydzQj13Q6xVRPHVUeHd9pt0NBt
drJxnp5fJxeVRYLCLdsItrEEW8BdyRIL
e3ZcdtKg9j1lpvpK9v31Fj10pqlA1A9k
EN632PlfYiZbn3PhvK3XOGSLInN00t
endUwPlf61BeQ3o111HeFoHD9GYKdTFfQ
euTPHAIml8o0yPCbaAh19RT803FX4IIE
```



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

Nos conectamos con el usuario **bandit9** y la contraseña **EN632PifYiZbn3PhVK3XOGSINlnNE00t.**

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
--eMk0eeAXj0ekoe;eeJbeonlee-e]ee]玿eUXeeR-8eeeeee4SA&l'eeeeXe    6meqeecbfeseee-nneeeeneeee
                                     ee--ee=ei ǀǂJeceee=eUueJ/eeeIe'e;saegeM-e2Keeehhe(ee1oee0;
[48e7eFR^+e6Ueeeeee#
      deeeH'e'qez}
          eex)e,e,Vee*"e3ee_ee3+2)'ee5HFeeeX[
eeie: eiee]yeeM2e3HUeeeeie[eUee(e.Be9'ez,
W9eZeepFeee7A*eeefleNd]eeMe#e~
eeeeeeeeVeeetGeceeeB9eeee-V2SekyeNnee   ee7ee_\;eeeq[Veeee-ee%Fc?Geeohheoxkj
                                         u+ZeeAggje
eee       eeeQu:qqeOeneNeelIekeee
             hee>3;e02ee           eeeeeNeEeeUzVC&e=pHeeeDe'e'ee=2'"L(whR'e!e4eDeeee_e'%nenzeeee
e"*e2SA(eee%'eeee_]xe  ee?edneeWTeo,eeeeeB-eXeee)!
WeIeS]eeeeeyreec'e'/je2eZeeNeh]eeeeQeHI\]7 HeeGH
DeRe%e]%zeeezy vTtCee(eeeeXeeAEeeeeB"/kef'etjheke/'#
3X#9etk0eles
      eTeece\
"xeeeeSWIeeGeeegqeeBeSeqq6epe[r9eeeeeKe|ee[e1e0eeeee#8jbe7ueuf'e'VeYee     ?>e?eeFFee]{xx%iec3    eeLeXQzeU0ee
```

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

```
bandit9@bandit:~$ strings data.txt | grep "="
=2"L(
x]T===== theG)"
===== passwordk^
Y=xW
t%=q
===== is
4=}D3
{1\=
FC&=z
=Y!m
$ /2`) =Y
4_Q=\
MO=(
?=|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
G7w8LIi6J3kTb8A7j9LgrywtEULyyp6s
```

NIVEL 10-11

Nos conectamos con el usuario **bandit10** y la contraseña **G7w8Lli6J3kTb8A7j9LgrywtEUllyp6s**.

```
lara@lara-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:



Welcome to OverTheWire!

Si usamos **cat** vemos que el contenido de **data.txt** está encriptado.

```
bandit10@bandit:~$ cat data.txt
VGh1IHBhc3N3b3JkIGlzIDZ6UGV6aUxkuJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==
```

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

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

NIVEL 11-12

Nos conectamos con el usuario **bandit11** y la contraseña **6zPezilDR2RKNdNYFNb6nVCKzphiXHBM**.

```
lara@lara-virtual-machine:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
```

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

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

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

Welcome to OverTheWire!

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 WIA00SFzMjXXBC0KoSKBbJ8pu0m5lIEi
```

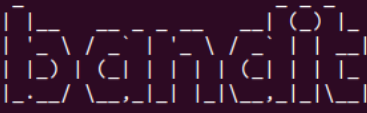
Para descifrarlo usaremos **cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'**.

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

NIVEL 12-13


Nos conectamos con el usuario **bandit12** y la contraseña **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**.

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



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

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



Welcome to OverTheWire!

Si mostramos el contenido de data.txt con cat 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 bfb3 ffff bff7 ffb9 39ff 7ffb .....9...
00000040: bd31 eeff b9fb fb3b 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 $.F.P!%..s..h...
00000120: 3f9b 1429 5b1d 3d87 68b5 804f 1d28 42fa ?..)[.=.h..O.(B.
00000130: 16c2 3241 98fb 8229 e274 5a63 fe92 3aca ..2A...).tZc...
00000140: 70c3 a329 d21f 41e0 5a10 08cb 888f 30df p...).A.Z.....0.
00000150: f3da ce85 418b 0379 6a65 cfa2 eeb7 9f01 ....A..yje.....
00000160: 782c da0e 288b e0c3 fe13 7af5 45ab 2b22 x,..(....z.E.+"
00000170: a432 bf2f e32d b9e6 1465 2296 d805 a45e .2./-...e"....^
00000180: d1c1 eac3 7483 6aac ca0e cf24 8864 bd40 ....t.j....$.d.@
00000190: 118c 644a 1dc6 a127 375c b7a6 c124 bdae .dJ...'7\...$.
000001a0: 6d31 63a0 a223 3ea0 61d4 bdf0 450f 56fb mic..#>...E.V.
000001b0: a546 8d34 08a2 4f1d 43d3 9063 404d dd43 .F.4..O.C...c@M.C
000001c0: b4f2 e65d bcb7 5932 0f5e 6802 3892 a988 ...].Y2.^h.8...
000001d0: 443d 8e89 7e09 4fb0 499d ee4e 4470 46c0 D=...~.O.I..NDpF.
000001e0: 2ba6 7c62 234a 7f76 151b aec0 23ee 4a97 +.|b#J.v....#.J.
000001f0: bc64 e34c de8a 5724 a1c3 9b89 cd96 1879 .d.L..WS.....y
00000200: d500 0cbb 5c26 09e4 efaf 5b94 402a 7780 .'\&....[.@*w.
00000210: 4d87 30ce b8a3 946e 72c1 a643 1db7 a060 M.0....nr..C...`
00000220: 6524 629c 0c7e 8e7b e0f8 820c d5cb 60a0 e$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=...
```

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

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

bandit12@bandit:/tmp/lara$ gzip -d data2.gz
bandit12@bandit:/tmp/lara$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/lara$ mv data2 data3.bz2
bandit12@bandit:/tmp/lara$ bzip2 -d data3.bz2
bandit12@bandit:/tmp/lara$ 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/lara$ mv data3 data4.gz
bandit12@bandit:/tmp/lara$ gzip -d data4.gz
bandit12@bandit:/tmp/lara$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lara$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/lara$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lara$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/lara$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/lara$ mv data6.bin data7.bz2
bandit12@bandit:/tmp/lara$ bzip2 -d data7.bz2
bandit12@bandit:/tmp/lara$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lara$ tar -xvf data7
data8.bin
bandit12@bandit:/tmp/lara$ file data8.bin
data: cannot open 'data' (No such file or directory)
8.bin: cannot open '8.bin' (No such file or directory)
bandit12@bandit:/tmp/lara$ 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/lara$ mv data8.bin data9.gz
bandit12@bandit:/tmp/lara$ gzip -d data9.gz
bandit12@bandit:/tmp/lara$ file data9
data9: ASCII text
bandit12@bandit:/tmp/lara$ cat data9
The password is wBwDl8xEir4CaE8LaPhauuU0o6pwrMrDw
```

Nos conectamos con el usuario **bandit13** y la contraseña **wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw**.

[illegible]

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

```
bandit13@bandit:~$ ls
sshkey.private
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/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
```

NIVEL 14-15

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 '^J'.
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnT

Connection closed by foreign host.
```


NIVEL 15-16

Nos conectamos con el usuario **bandit15** y la contraseña **jN2qgmIXJ6fShzhT2avhotn4Zcka6tnt**.

```
lara@lara-virtual-machine:~$ ssh bandit15@bandit.labs.overthewire.org -p 2220
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit15@bandit.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!
```

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

```
closed
bandit15@bandit:~$ openssl s_client -connect localhost:30001 -ign_eof
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
```

```
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qcLOAi1
```

NIVEL 16-17

Nos conectamos con el usuario **bandit16** y la contraseña **JQttfApK4SeyHwDlI9SXGR50qcLOAi1**.

```
lara@lara-virtual-machine:~$ ssh bandit16@bandit.labs.overthewire.org -p 2220
[bandit16@bandit.labs.overthewire.org ~]$

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

bandit16@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!
```

Con **nmap -A localhost -p 31000-32000** escaneamos los servicios en el rango de puertos especificado y vemos que el puerto **31960** está abierto.

```
bandit16@bandit:~$ nmap -A localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-09 19:03 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Not valid before: 2024-02-09T03:53:52
|_ Not valid after: 2024-02-09T03:54:52
31691/tcp open  echo
31790/tcp open  ssl/unknown
| fingerprint-strings:
|_  FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, K
|_  Wrong! Please enter the correct current password
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Not valid before: 2024-02-09T03:53:53
|_ Not valid after: 2024-02-09T03:54:53
31960/tcp open  echo
|_  service unrecognized despite returning data. If you know the service
SF-Port31790-TCP:V=7.80%T=SSL%I=7%D=2/9%Time=65C67727%P=x86_64-pc-lin
SF:u=r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
65C67727%P=x86_64-pc-linux-gnu%T=SSL%I=7%D=2/9%Time=65C67727%P=x86_64-pc-lin
```


Con **openssl s_client -connect localhost:31790** nos conectamos al puerto **31790** y ponemos la contraseña del usuario. Copiamos la clave que nos sale.

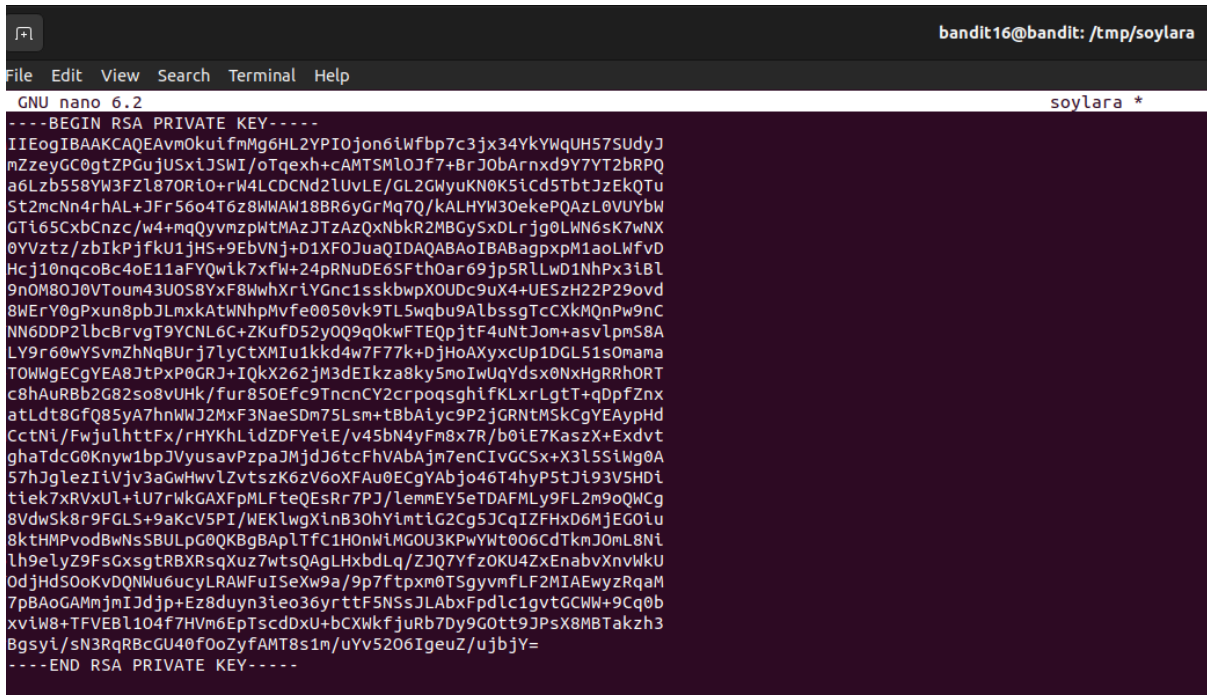
```
bandit16@bandit:~$ openssl s_client -connect localhost:31790
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1

read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qc10Ail1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvM0kufmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZL870RiO+rW4LCDCNd2LuvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
```

Creamos un directorio y pegamos la clave dentro.

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

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



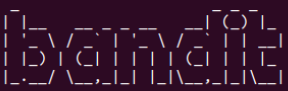
The screenshot shows a terminal window with the nano editor open. The title bar indicates the current directory is /tmp/soylara. The nano editor interface includes a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (GNU nano 6.2, soylara *). The main text area contains the RSA private key that was copied in the previous step, starting with '-----BEGIN RSA PRIVATE KEY-----' and ending with '-----END RSA PRIVATE KEY-----'.

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

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



Nos conectamos con **bandit17**.

```
bandit16@bandit:/tmp/soylara$ ssh -t soylara 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**.

```
lara@lara-virtual-machine:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220
```



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

Volvemos a acceder pero añadimos **cat readme** y nos saldrá la contraseña.

```
lara@lara-virtual-machine:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme  
bandit18@bandit.labs.overthewire.org's password:  
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

NIVEL 19-20

Nos conectamos con el usuario **bandit19** y la contraseña **awhqfNnAbc1naukrpqDYcF95h7HoMTrC**.

```
lara@lara-virtual-machine:~$ ssh bandit19@bandit.labs.overthewire.org -p 2220  
bandit19@bandit.labs.overthewire.org's password:  
Welcome to OverTheWire!
```

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

Nos conectamos con el usuario **bandit20** y la contraseña **VxCazJaVykl6W36BkBU0mJTCM8rR95XT**.

```
Lara@Lara-virtual-machine:~$ ssh bandit20@bandit.labs.overthewire.org -p 2220
```



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

bandit20@bandit.labs.overthewire.org's password:



www. ver he ire.org

Welcome to OverTheWire!

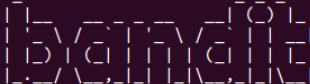
El comando **echo -n "VxCazJaVykl6W36BkBU0mJTCM8rR95XT" | nc -l -p 1234 &** envía la cadena "VxCazJaVykl6W36BkBU0mJTCM8rR95XT" a través de la red a un servidor que escucha en el puerto 1234 utilizando Netcat (nc).

```
bandit20@bandit:~$ echo -n "VxCazJaVykiW36BkBU0mJTCM8r95XT" | nc -l -p 1234 &
[1] 1615142
bandit20@bandit:~$ ./suconnect 1234
Read: VxCazJaVykiW36BkBU0mJTCM8r95XT
Password matches, sending next password
bandit20@bandit:~$ NvEJF7oVjkdldtPSrdKEFOllh9V1IBCq
```

NIVEL 21-22


Nos conectamos con el usuario **bandit21** y la contraseña **NvEJF7oVjkddltPSrdKEFOllh9V1IBcq**.

```
lara@lara-virtual-machine:~$ ssh bandit21@bandit.labs.overthewire.org -p 2220
```



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

bandit21@bandit.labs.overthewire.org's password:



www.OverTheWire.org

Welcome to OverTheWire!

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 el fichero **/tmp/t706..**.

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit17_root  cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  cronjob_bandit25_root  e2scrub_all  otw-tmp-dir  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
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

NIVEL 22-23

Nos conectamos con el usuario **bandit22** y la contraseña **WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff**.

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

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:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit17_root  cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  cronjob_bandit25_root  e2scrub_all  otw-tmp-dir  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

Nos conectamos con el usuario **bandit23** y la contraseña **QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G**.

```
lara@lara-virtual-machine:~$ ssh bandit23@bandit.labs.overthewire.org -p 2220
bandit23@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

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

bandit23@bandit.labs.overthewire.org's password:
```

Repetimos el proceso pero con **cronjob_bandit24**.

```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls
cronjob_bandit15_root cronjob_bandit17_root cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 cronjob_bandit25_root e2scrub_all otw-tmp-dlr 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/pizza
bandit23@bandit:/etc/cron.d$ cd /tmp/pizza
bandit23@bandit:/tmp/pizza$ 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.

GNU nano 6.2 bandit24.sh *
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/pizza/nivel24
```

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

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

```
bandit23@bandit:/tmp$ chmod 777 pizza
bandit23@bandit:/tmp$ cd pizza
```

Lo copiamos al siguiente directorio.

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

Y vemos que aparece.

```
bandit23@bandit:/tmp/pizza$ ls
bandit24.sh  nivel24
bandit23@bandit:/tmp/pizza$ cat nivel24
VafGXJ1PBSsPSnvsjI8p759leLZ9GGar
```

NIVEL 24-25

Nos conectamos con el usuario **bandit25** y la contraseña **VafGXJ1PBSsPSnvsjI8p759leLZ9GGar**.

```
lara@lara-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. ver he ire.org
```

Welcome to OverTheWire!

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

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

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

passwd="VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar"

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

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

Correct!
Exiting.
The password of user bandit25 is p7TaowMYrmu230l8hiZh9UvD009hpx8d
```

Nos conectamos con el usuario **bandit25** y la contraseña **p7TaowMYrmu23OI8hiZh9UvD0O9hpx8d**.

Vemos que si accedemos se nos cierra la conexión.

```
bandit25@bandit:~$ ls
bandit26.sshkey
bandit25@bandit:~$ ssh -i bandit26.sshkey bandit26@localhost -p 2220
```

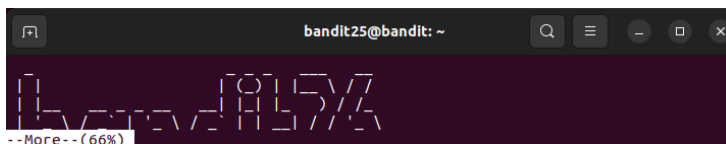
```
bandit25
Connection to localhost closed.

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
```

Volvemos a acceder con el usuario con la ventana minimizada. Pulsamos **v** para acceder al modo visual de **more**.



Dentro escribiremos **:set shell=/bin/bash** para establecer la shell.

```
:set shell=/bin/bash
```

NIVEL 26-27

Dentro accedemos a la shell con **:shell** y escribimos **./bandit27-do cat /etc/bandit_pass/bandit27** para ver la contraseña.

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

NIVEL 27-28

Accedemos con el usuario **bandit27** y la contraseña **YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS**.

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

bandit27@bandit.labs.overthewire.org:~$

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

bandit27@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

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


Creamos un directorio en **/tmp**.

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

Dentro clonamos el repositorio de git.

```
bandit27@bandit:/tmp/macarron$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihNV1wUXRb4RReCLFXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

      _ _ _ _ _
     /   /   /
    /_   /_   /
   / _ _/ _ _/
  /_   /_   /
 /   /   /
/_ _/_/_/_

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

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

Dentro encontramos la contraseña.

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

NIVEL 28-29

Accedemos con el usuario **bandit28** y la contraseña **AVanL161y9rsbcJIsFHuw35rjaOM19nR**.

```
lara@lara-virtual-machine:~$ ssh bandit28@bandit.labs.overthewire.org -p 2220

      _ _ _ _ _
     /   /   /
    /_   /_   /
   / _ _/ _ _/
  /_   /_   /
 /   /   /
/_ _/_/_/_

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

bandit28@bandit.labs.overthewire.org's password:

      _ _ _ _ _
     /   /   /
    /_   /_   /
   / _ _/ _ _/
  /_   /_   /
 /   /   /
/_ _/_/_/_

www. over the wire.org

Welcome to OverTheWire!
```

Hacemos los mismos pasos que antes.

```
bandit28@bandit:/tmp/fideo$ 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:C2ihUBV7ihnV1wUXRb4RfEcLfXC5CXlhmaAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit28/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit28/.ssh/known_hosts).
```



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

```
bandit28-git@localhost's password:
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (2/2), done.
bandit28@bandit:/tmp/fideo$ ls
repo
bandit28@bandit:/tmp/fideo$ cd repo
bandit28@bandit:/tmp/fideo/repo$ ls
README.md
bandit28@bandit:/tmp/fideo/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.
```

```
## credentials

- username: bandit29
- password: xxxxxxxxxx
```

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

```
bandit28@bandit:/tmp/fideo/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/fideo/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 @@ Some notes for level29 of bandit.
## credentials

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

NIVEL 29-30

Accedemos con el usuario **bandit29** y la contraseña **tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S**.

```
lara@lara-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:
```



Welcome to OverTheWire!

Volvemos a repetir los pasos.

```
bandit29@bandit:~$ cd /tmp
bandit29@bandit: /tmp$ mkdir patata
bandit29@bandit: /tmp$ cd patata
bandit29@bandit: /tmp/patata$ 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:C2ihUBV7lhnV1wUXRb4RrEcLfXC5CXlhmAAM/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/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).
```

The logo for OverTheWire, featuring the words "OverTheWire" in a stylized, blocky font where the letters are interconnected.

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/patata$ ls
repo
bandit29@bandit: /tmp/patata$ cd repo
bandit29@bandit: /tmp/patata/repo$ ls
README.md
bandit29@bandit: /tmp/patata/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**.

```
bandit29@bandit:/tmp/patata/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/sploits-dev
bandit29@bandit:/tmp/patata/repo$ git checkout dev
Branch 'dev' set up to track remote branch 'dev' from 'origin'.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/patata/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOs
```

NIVEL 30-31

Nos conectamos con el usuario **bandit30** y la contraseña **xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOs**.

```
lara@lara-virtual-machine:~$ ssh bandit30@bandit.labs.overthewire.org -p 2220
[bandit30@bandit.labs.overthewire.org ~]$

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

bandit30@bandit.labs.overthewire.org's password:
[bandit30@bandit.labs.overthewire.org ~]$

Welcome to OverTheWire!
```

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

```
bandit30@bandit:/tmp/tortilla/repo$ git tag
secret
bandit30@bandit:/tmp/tortilla/repo$ git show secret
OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
```

NIVEL 31-32

Nos conectamos con el usuario **bandit31** y la contraseña **OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt**.

```
Lara@lara-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@bandit:/tmp/tomate/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. Hacemos un **commit** añadiendo los cambios y hacemos un **push**.

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

```
bandit31@bandit:/tmp/tomate/repo$ nano key.txt
Unable to create directory /home/bandit31/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit31@bandit:/tmp/tomate/repo$ git add -f key.txt
bandit31@bandit:/tmp/tomate/repo$ git commit -m "dale"
[master 88f0dcd] dale
1 file changed, 1 insertion(+)
create mode 100644 key.txt
bandit31@bandit:/tmp/tomate/repo$ git push origin
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLFXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).

      | _ _ _ _ _ | _ _ _ _ _ | | | | | | | | | |
      | | | | | | | | | | | |
      | | | | | | | | | | | |
      | | | | | | | | | | | |
      | | | | | | | | | | | |

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

bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 317 bytes | 317.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ###
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: rmCBvG56y58BXzv98yZGd07ATVL5dW8y
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
 ! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
```

NIVEL 32-33

Nos conectamos con el usuario **bandit32** y la contraseña **rmCBvG56y58BXzv98yZGdO7ATVL5dW8y**.

```
lara@lara-virtual-machine:~$ ssh bandit32@bandit.labs.overthewire.org -p 2220
bandit32@bandit.labs.overthewire.org:~$
[O][V][E][R][T][H][E][W][I][R][E]

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

bandit32@bandit.labs.overthewire.org's password:
[O][V][E][R][T][H][E][W][I][R][E]
www. over the wire.org

Welcome to OverTheWire!
```

Todo lo que escribimos lo convierte en mayúsculas, entonces no vamos a poder ejecutar ningún comando. Podemos utilizar la variable \$0, que contiene el nombre del programa que se ejecuta (en este caso, bash), para invocar la shell.

```
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
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
```

NIVEL 33-34

Nos conectamos con el usuario **bandit33** y la contraseña **odHo63fHiFqcWWJG9rLiLDtPm45KzUKy**.

```
lara@lara-virtual-machine:~$ ssh bandit33@bandit.labs.overthewire.org -p 2220
bandit.labs.overthewire.org:2220: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAK2p258
bandit33@bandit.labs.overthewire.org's password:
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit33@bandit.labs.overthewire.org's password:
www.OverTheWire.org
Welcome to OverTheWire!
```

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!
```