


```
bandit0@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit0@bandit:~$
```

bandid 1

Para obtener la contraseña para el siguiente nivel debemos obtenerlo del archivo de texto readme el cual se puede obtener con el comando cat. Pero primero para verificar que el archivo se encuentra en el fichero podemos ver los archivos no ocultos con el comando ls.

ls

cat readme


```
bandit1@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit1@bandit:~$
```

bandit 2

Para este ejercicio volveremos a usar el comando cat, sin embargo el archivo tiene un nombre que inicia con el carácter especial “-” por lo cual tendemos que hacer una modificación a como escribimos el fichero.

cat ./-

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

pass: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Únicamente resta desloguearse y loguearse con el nuevo usuario y contraseña.

cat .hiden

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

Nos desloguearse y loguearse con el nuevo usuario y contraseña.

[illegible]

```
bandit4@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit4@bandit:~$
```

Bandit5

Para este ejercicio si confirmamos los ficheros en el directorio home con el comando ls notaremos el directorio inhere, si entramos con el comando cd y ejecutamos un ls notaremos que habrá varios archivos disponibles.

```
ls  
  
cd inhere/  
  
ls
```

```
bandit4@bandit: ~/inhere  
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$
```

En lugar de revisarlos uno por uno lo haremos todos de golpe regresando al directorio home y utilizando el comando file, para que revise todos los archivos agregaremos un /* al final del directorio.

```
cd  
  
file inhere/*
```



```
bandit5@bandit: ~  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit5@bandit:~$
```

Bandit6

El ejercicio nos menciona que el archivo se encuentra en el directorio `inhere` y nos da ciertas características del mismo por lo cual podremos ejecutar el comando `find` con algunos parámetros de búsqueda ya que si inspeccionamos el directorio `inhere` notaremos varios subdirectorios por lo que revisarlos uno a uno tomaría demasiado tiempo.

`ls`

`cd inhere`

`ls -a`

`ls -h`

```
bandit5@bandit: ~/inhere  
bandit5@bandit:~$ ls  
inhere  
bandit5@bandit:~$ cd inhere/  
bandit5@bandit:~/inhere$ ls -a  
.  
..  
maybeh ere00  
maybeh ere01  
maybeh ere02  
maybeh ere03  
maybeh ere04  
maybeh ere05  
maybeh ere06  
maybeh ere07  
maybeh ere08  
maybeh ere09  
maybeh ere10  
maybeh ere11  
maybeh ere12  
maybeh ere13  
maybeh ere14  
maybeh ere15  
maybeh ere16  
maybeh ere17  
maybeh ere18  
maybeh ere19  
bandit5@bandit:~/inhere$ |
```

```
bandit5@bandit:~/inhere$ ls -l
total 80
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere00
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere01
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere02
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere03
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere04
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere05
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere06
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere07
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere08
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere09
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere10
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere11
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere12
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere13
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere14
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere15
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere16
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere17
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere18
drwxr-x--- 2 root bandit5 4096 Jan 11 19:19 maybehere19
bandit5@bandit:~/inhere$
```

Para usar el comando find le indicaremos con “.” Que la búsqueda iniciara desde el directorio actual, “-type f” para indicar que lo que queremos es tipo archivo, “-readable” que sea leible. “! -executable” que no sea ejecutable y por ultimo su tamaño con “-size 1033c”.

```
find . -type f -readable ! -executable -size 1033c
```

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

Ya que hay un unico archivo con las características de la usqueda podemos realizar un cat para obtener la contraseña.

```
cat ./maybehere07/.file2
```

```
bandit5@bandit: ~/inhere
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU
bandit5@bandit:~/inhere$
```

Pass P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU

Comprobamos

[illegible]

```
bandit6@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit6@bandit:~$
```

Bandit 7

Para este ejercicio nuevamente nos pide buscar la contraseña en algún lugar, esta vez del servidor, y nos da algunas características. Si por curiosidad ejecutamos un `ls` normal notaremos que no nos muestra ningún directorio solo hasta agregar el modificador `-a` encontraremos alguno.

Ls

ls -a

ls -a -l

```
bandit6@bandit: ~  
bandit6@bandit:~$ ls  
bandit6@bandit:~$ ls -a  
.  .. .bash_logout .bashrc .profile  
bandit6@bandit:~$ ls -a -l  
total 20  
drwxr-xr-x  2 root root 4096 Jan 11 19:18 .  
drwxr-xr-x 70 root root 4096 Jan 11 19:19 ..  
-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  
bandit6@bandit:~$
```

Así que esta vez probaremos realizar una búsqueda en todo el servidor usando "/" en lugar de "." Para buscar desde la raíz.

find / -user bandit7 -group bandit6 -size 33c

```
bandit6@bandit: ~  
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c  
find: '/dev/mqueue': Permission denied  
find: '/dev/shm': Permission denied  
find: '/var/spool/bandit24': Permission denied  
find: '/var/spool/rsyslog': Permission denied  
find: '/var/spool/cron/crontabs': Permission denied  
find: '/var/crash': Permission denied  
find: '/var/snap/lxd/common/lxd': Permission denied  
find: '/var/cache/ldconfig': Permission denied  
find: '/var/cache/apt/archives/partial': Permission denied  
find: '/var/cache/apparmor/e10c1cf9.0': Permission denied  
find: '/var/cache/apparmor/c47eabf7.0': Permission denied  
find: '/var/cache/private': Permission denied  
find: '/var/cache/pollinate': Permission denied  
find: '/var/log': Permission denied  
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied  
find: '/var/lib/polkit-1': Permission denied  
find: '/var/lib/chrony': Permission denied  
find: '/var/lib/napd/void': Permission denied  
find: '/var/lib/napd/cookie': Permission denied  
find: '/var/lib/amazon': Permission denied  
/var/lib/dpkg/info/bandit7.password  
find: '/var/lib/apt/lists/partial': Permission denied  
find: '/var/lib/private': Permission denied  
find: '/var/tmp': Permission denied
```

Notaremos varios resultados que nos dieron error por tener permisos denegados y uno nombrado .password que podemos suponer es la contraseña, pero para fines mas instructivos puleremos mas este comando para tener un resultado mas legible en caso de necesitarlo. Para ello primero indicaremos que todos los errores (representados con un 2 en los tipos de salidas) sean dirigidos (con el carácter mayor que ">")a vacio "null" añadiendo al comando "2>/dev/null"

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

Si quisieramos ser aun mas concretos podriamos indicar que esta salida sea la entrada de otro comando usando |, y utilizando xargs para entrada de entrada estándar en argumentos a un comando, en este caso el comando cat

`find / -user bandit7 -group bandit6 -size 33c 2>/dev/null | xargs cat`

```
bandit6@bandit: ~  
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null | xargs cat  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S  
bandit6@bandit:~$
```

Pass z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Comprobamos.

Vi data.tx

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

```
bandit7@bandit: ~  
aboding ErTQm1TafRb8szvTLpbV25MPOPEexBsH  
locket's f08zz1eLIJmv24fTys7e7zAwVYdnTbfg  
melt HVLgPRIrjbzrbjwFZ5M8aQCavUuRdQtb  
popular Rjy5b8oEjivOe4gX82ErCZ78FZDgVkJp  
odious 6JV4M56xFJkIUriwUcJzImGcs55THFQT  
taxonomies 0TXcsyXyX08nCpuojmbChQf1RZIZj5nM  
land 3jvaD1qNXximI2En8FaIO6HQqhy1pucs  
elevator bqmu0YYKbkoZyK1abxwjbNM6ZpB3y9eG  
vacationed 2EabBTby3LfwR5y9IHxdvSvqhUSTUEeQ  
termed hKPxiEJFj0hPdoVvfq15am94F6Azhof  
playgoer's 2AX7IxtDuc1j0aYcIN2uCsCi8Rjx0WL  
millionth TESKZC0XvTetK0S9xNwm25Stk5iWrBvP  
fancies kuthgIL6KI7FpG88yLumXiHNK6i8XHCg  
effrontery s42Nm2Epse3L12rhttZHeZ13YuBTPwMd  
heavy FZolxGLi03cQebJBae4nJ4tnkpuRUC5y  
psychiatrists Xi5sibqB4pLQR6bqWZ6EQMv7xy9tIFbT  
piffle M12acskE21rV0RRS6v8yN9ZXwWqELzrt  
misdo 7MyxRpqnsuVTz9IhYTSwNz0A1SMo4UYt  
criteria 1RgIJGiE5tQ4emxurSkW9PwF9QCDTkh  
bushwhacks WJmRA2YxAaamGHwZ1VXUT1s9hmRmp91x  
dish's 1K2hpJkIw5LnmjRgcet6RPIOb0ERxbz8  
shorting NqGPS1fPxoM1w2UCqPR5vvGy56eFHTvq  
facial 5BPb4JEUWoY50nPYGb9b5rEPTgOd1CeY  
agglutinating b1fMxTnd6XexL5MsQZmJorihwP8B1bzx  
"data.txt" [readonly] 98567L, 4184396B 1,1 Top
```

Utilizaremos el comando grep para buscar la linea que contenga la palabra “millionth” en el archivo

grep millionth

```
bandit7@bandit: ~  
bandit7@bandit:~$ grep "millionth" data.txt  
millionth TESKZC0XvTetK0S9xNwm25Stk5iWrBvP  
bandit7@bandit:~$
```

Para depurar más esta salida podemos utilizarla como entrada para el comando awk, indicando que nos devuelva unicamente el segundo argumento

grep "millionth" data.txt | awk '{print \$2}'

```
bandit7@bandit: ~  
bandit7@bandit:~$ grep "millionth" data.txt | awk '{print $2}'  
TESKZC0XvTetK0S9xNwm25Stk5iWrBvP  
bandit7@bandit:~$
```


Comprobamos.

[illegible]

```
bandit8@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit8@bandit:~$ |
```

En este ejercicio de nuevo se nos indica que la contraseña esta en un archivo y que es la unica que aparece solo una vez. Para describir cual es esta linea podemos utilizar el comando `uniq` con el modificador `-u`, sin embargo este comando nos pide una entrada ya

ordenada por lo cual primero debemos procesar el archivo, en este caso con el comando `sort` que nos ordenara las lineas del archivo por orden alfabetico.

```
cat data.txt | sort | uniq -u
```

```
bandit8@bandit: ~  
bandit8@bandit:~$ cat data.txt | sort | uniq -u  
EN632P1fYiZbn3PhVK3XOGS1NInNE00t  
bandit8@bandit:~$
```

Pass EN632P1fYizbn3PhvK3X0GS1NInNE00t

Comprobamos.

[illegible]

```
bandit9@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit9@bandit:~$
```

Bandit10

En este ejercicio se nos indica que la contraseña esta presedida por el carácter “=”. Sin embargo si utilizamos el comando grep como en el ejercicio anterior, nos indicara que hay coincidencias en archivo bynario, por lo que no podremos verificar la contraseña.

```
bandit9@bandit: ~  
bandit9@bandit:~$ ls -l  
total 20  
-rw-r----- 1 bandit10 bandit9 19379 Jan 11 19:18 data.txt  
bandit9@bandit:~$ grep '=' data.txt  
grep: data.txt: binary file matches
```

Para resolver esto utilizaremos el comando strings el cual extrae cadenas de caracteres imprimibles para poderlo usar como entrada de grep. Con lo que se nos muestra las lineas que ontengan el carácter pedido y obserbamos un mensaje que nos indica la contrase “the password ist”

```
strings data.txt | grep "="
```



```
bandit10@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit10@bandit:~$ |
```

Bandit11

En este ejercicio se nos indica que el archivo esta codificado en base 64. Si ejecutamos un cat al unico archivo visible en el servidor obtendremos una linea que paresiera una contraseña sin embargo hemos visto que estas son mas cortas.

```
bandit10@bandit: ~  
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ cat data.txt  
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==  
bandit10@bandit:~$
```

Podrimos decodificarlo manualmente con la tabla que se muestra a continuacion (extraida de Wikipedia.org en el articulo pertinente). Tras obtener el valor en binario de cada carácter y posteriormente transformando el resultado en conjunto a código ASCII.

Valor	Carácter	Valor	Carácter	Valor	Carácter	Valor	Carácter
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	ø
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

O bien podemos usar el comando base64 de la consola de linux, brindandole como entrada el resultado de la lectura del archivo y añadiendo el modificador -d para que haga una decodificación.

```
cat data.txt | base64 -d
```

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

Pass 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Comprobamos.


```
bandit12@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit12@bandit:~$ |
```

Bandit13

Para este ejercicio se nos recomienda primero crear un directorio donde poder trabajar con una copia del archivo data.txt-

```
mkdir /tmp/roberto  
cp data.txt /tmp/roberto  
cd /tmp/roberto
```

```
bandit12@bandit: /tmp/roberto  
bandit12@bandit:~$ mkdir /tmp/roberto  
cp data.txt /tmp/roberto  
cd /tmp/roberto  
bandit12@bandit:/tmp/roberto$ ls  
data.txt  
bandit12@bandit:/tmp/roberto$ |
```

Una vez echo esto, el ejercicio indica que el archivo data.txt es un “hexdump” o volcado de datos en hexadecimal, por lo que lo siguiente que hay que hacer es revertir esta operación.

Para ello nos podemos valer del mismo comando con el cual se realiza “xxd” con el modificador -d. También se nos indica que este volcado se hizo de un archivo comprimido por lo cual revertiremos este proceso hacia un archivo .gz

```
xxd -r data.txt > archivo  
ls
```

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ xxd -r data.txt > archivo
ls
archivo data.txt
bandit12@bandit:/tmp/roberto$
```

Resta seguir una serie de descompresiones hasta hallar el archivo que tenga la contraseña. Para saber cual comando usaremos para dicha descompresion, primero debemos averiguar que tipo de archivo tenemos con el comando file, luego de ello le cambiaremos el nombre para agregar la extension correspondiente y usar el comando adecuado (tar para .tar, gzip para .gz, bzip2 para .bz2).

file archivo

mv archivo archivo.gz

gzip -d archivo.gz

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file archivo
archivo: gzip compressed data, was "data2.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 572
bandit12@bandit:/tmp/roberto$ mv archivo archivo.gz
bandit12@bandit:/tmp/roberto$ gzip -d archivo.gz
```

file archivo

mv archivo archivo.bz2

bzip2 -d archivo.bz2

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file archivo
archivo: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/roberto$ mv archivo archivo.bz2
bandit12@bandit:/tmp/roberto$ bzip2 -d archivo.bz2
```

file archivo

mv archivo archivo.gz

gzip -d archivo.gz

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file archivo
archivo: gzip compressed data, was "data4.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/roberto$ mv archivo archivo.gz
bandit12@bandit:/tmp/roberto$ gzip -d archivo.gz
```

file archivo

mv archivo archivo.tar

tar -xvf archivo.tar

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file archivo
archivo: POSIX tar archive (GNU)
bandit12@bandit:/tmp/roberto$ mv archivo archivo.tar
bandit12@bandit:/tmp/roberto$ tar -xvf archivo.tar
data5.bin
```

ls

file data5.bin

mv data5.bin data5.tar

tar -xvf data5.tar

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ ls
archivo.tar  data5.bin  data.txt
bandit12@bandit:/tmp/roberto$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/roberto$ mv data5.bin data5.tar
bandit12@bandit:/tmp/roberto$ tar -xvf data5.tar
data6.bin
```

ls

file data6.bin

mv data6.bin data6.bz2

bzip2 -d data5.bz2

ls

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ ls
archivo.tar  data5.tar  data6.bin  data.txt
bandit12@bandit:/tmp/roberto$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/roberto$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/roberto$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/roberto$ ls
archivo.tar  data5.tar  data6  data.txt
```

file data6

mv data6 data6.tar

tar -xvf data6.tar

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/roberto$ mv data6 data6.tar
bandit12@bandit:/tmp/roberto$ tar -xvf data6.tar
data8.bin
```

ls

file data8.bin

mv data8.bin data8.gz

gzip -d data8.gz

ls

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ ls
archivo.tar data5.tar data6.tar data8.bin data.txt
bandit12@bandit:/tmp/roberto$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jan 11 19:18:38 2023, max
compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/roberto$ mv data8.bin data8.gz
bandit12@bandit:/tmp/roberto$ gzip -d data8.gz
bandit12@bandit:/tmp/roberto$ ls
archivo.tar data5.tar data6.tar data8 data.txt
```

file data8

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ file data8
data8: ASCII text
bandit12@bandit:/tmp/roberto$ |
```

Llegamos a un archivo de texto por lo que podemos usar un cat para ver su contenido

Cat data8

```
bandit12@bandit: /tmp/roberto
bandit12@bandit:/tmp/roberto$ cat data8
The password is wbWd1BxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/roberto$
```

Pass wbWd1BxEir4CaE8LaPhauuOo6pwRmrDw

Comprobamos.


```
bandit14@bandit: ~  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit14@bandit:~$
```

En esta ocacion se uso localhost en lugar de bandit para el servidor, debido a que ya estabamos conectados al mismo.

Una vez conectados como el usuario bandid 14 procedemos a dirigirnos al directorio indicado por el ejercicio, para poder leer el archivo que contiene la contraseña.

```
cd /etc/bandit_pass/
```

```
bandit14@bandit: /etc/bandit_pass  
bandit14@bandit:~$ cd /etc/bandit_pass  
bandit14@bandit:/etc/bandit_pass$ ls  
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8  
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9  
bandit10 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6  
bandit11 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7  
bandit14@bandit:/etc/bandit_pass$ cat bandit14  
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq  
bandit14@bandit:/etc/bandit_pass$
```

Pass fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Comprobamos.


```
nc localhost 30000 < bandit14
```

Pass jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

[illegible]

```
bandit15@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit15@bandit:~$
```

Bandit16

En este ejercicio se nos pide enviar el password de este nivel, encriptado en el protocolo ssl, el puerto 30000 Para ello usaremos el comando openssl con la herramienta s_client, para hacer conecciones usaremos la opcion -connect para especificar el servidor y el puerto (30000 + 1) , y añadimos la opcion -quiet para tener una mejor lectura del resultado.

```
openssl s_client -connect localhost:30001 -quiet
```

```
bandit15@bandit: ~  
bandit15@bandit:~$ openssl s_client -connect localhost:30001 -quiet  
Can't use SSL_get_servername  
depth=0 CN = localhost  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = localhost  
verify error:num=10:certificate has expired  
notAfter=Feb 13 06:43:06 2023 GMT  
verify return:1  
depth=0 CN = localhost  
notAfter=Feb 13 06:43:06 2023 GMT  
verify return:1  
|
```

Aquí ingresaremos la contraseña del ejercicio

```
bandit15@bandit: ~  
bandit15@bandit:~$ openssl s_client -connect localhost:30001 -quiet  
Can't use SSL_get_servername  
depth=0 CN = localhost  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = localhost  
verify error:num=10:certificate has expired  
notAfter=Feb 13 06:43:06 2023 GMT  
verify return:1  
depth=0 CN = localhost  
notAfter=Feb 13 06:43:06 2023 GMT  
verify return:1  
jN2kgmIXJ6fShzhT2avhotn4Zcka6tn  
Correct!  
JQtffApK4SeyHwDlI9SXGR50qc10Ai1l  
  
bandit15@bandit:~$
```

Pass JQttfApK4SeyHwDlI9SXGR50qc10Ai11

Comprobamos

[illegible]

```
bandit16@bandit: ~  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit16@bandit:~$ |
```

Bandit17

Este ejercicio se resuelve de manera similar al anterior, solo que esta vez no nos indican el puerto por el cual podemos enviar el mensaje, si no que nos dan un rango de puertos donde solo uno puede aceptar el mensaje en ssl. Para averiguar que puerto es nos valdremos de la herramienta nmap, la usaremos con la opcion -A para ejecutar un escaneo de fuerza bruta y posteriormente definiremos el rango de accion (para ver el porsentaje completado del escaneo podemos oprimir enter)

```
nmap -A -p31000 -p32000 localhost
```

```
bandit16@bandit: ~  
bandit16@bandit:~$ nmap -A -p31000-32000 localhost  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-15 01:44 UTC  
Verbosity Increased to 1.  
Verbosity Increased to 2.  
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 0.00% done  
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 80.00% done; ETC: 01:46 (0:00:18 remaining)  
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 80.00% done; ETC: 01:46 (0:00:20 remaining)  
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 80.00% done; ETC: 01:46 (0:00:23 remaining)  
Completed Service scan at 01:46, 97.92s elapsed (5 services on 1 host)  
NSE: Script scanning 127.0.0.1.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 01:46  
Completed NSE at 01:46, 0.03s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 01:46  
Completed NSE at 01:46, 0.06s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 01:46  
Completed NSE at 01:46, 0.00s elapsed  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.00012s latency).
```

Si nos fijamos en el informe del puerto 31790 el cual es capas de leer ssl, nos fijaremos en un mensaje de error el cual nos pide qe ingresemos una contraseña

```
31790/tcp open  ssl/unknown  
| fingerprint-strings:  
|_ FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPSearchReq, L  
PDString, RTSPRequest, SIPOptions, SSLSessionReq, TLSSessionReq, TerminalServerCookie:  
|_ Wrong! Please enter the correct current password  
|_ ssl-cert: Subject: commonName=localhost  
| Subject Alternative Name: DNS:localhost  
| Issuer: commonName=localhost  
| Public Key type: rsa  
| Public Key bits: 2048  
| Signature Algorithm: sha1WithRSAEncryption  
| Not valid before: 2023-02-13T06:42:06  
| Not valid after: 2023-02-13T06:43:06  
| MD5: b142 f7f7 5f5d cc78 ebc3 2ed7 fd9e 130d  
| SHA-1: f091 5d3c 4419 2c22 c466 a12f 1c70 8d42 8880 1f3d  
| -----BEGIN CERTIFICATE-----  
| MIIDCzCCAF0gAwIBAgIEGA4i7jANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAIs  
| b2NhbgHvc3QwHhcNMjEzMDYOMjA2WhcNMjEzMDYOMjA2WjAUMRIwEAYD  
| VQDDA1sb2NhbgHvc3QwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC  
| ddd+yKL6tk9uUPMQpELUWETiZ/tmrFcSygw+ccXIyGQKsnnf5houUXmDHdNI3/P  
| pNQzJjvsVQLjUlmVRcUtDUC9sJQMURbdwc51BHv49pv009bqG79ZKKi1hridJPXk  
| MYNYeuwlhJmQ1f8LQ5K+Yt/AFdwdKR2L0tp/rARtvUgMj2dzloZdf2Am79mXzi50  
| ve1sP50plFgzqJEP8MT8r6i7spmXA0hoJxTrQ6oT1eq3uHu0j6JOz46wd90jI2AK  
| 6EdWGIWgr1xfMaRPEPQJbEZKgyrARbpkbo4086Hnc3GDzMorc8T8rd6M15Bu6jTR  
| RR2FJdzYdoQoAq4oOg6jAgMBAAGjZTBjMBQGA1UdEQQNMAuCCWxvY2FsAG9zdDBL  
| BglghkgBhvhCAQ0EPHY8QXV0b21hdG1jYWxsZS8nZW51cmF0ZWQgYnkgTmNhdc4g  
| U2VlIGh0dHBzO18vbm1hcC5vcmcvbmNhdc8uMAOGCSqGSIb3DQEBAQUAA4IBAQAZ  
| 9EO/wp0y2q4DLnoF6p2faG7mE3L5bZXIkkWileA/yYQxgKCwRw93Qzqsdhpuap  
| RtywtYU7Khgfkev/p1vNUa13wgF6QZ3nC9MnrM1Y/uHT530sv1dZN0sknjU3f1zg  
| PUT/Z8RdTgu6qvPDyT8KTJ0oi7UNECuhyres5s8bhWvG/eZeX4x5+1YmYDQy90fS  
| j2dM5yknKHUKxbIQQXMoqQImT31VaPz4/loT/1Ld4RL0+zeL+rZbewS0zL1RYIh  
| F0FeRh06xJ+stFiS+H8+vHFmv4u9jaqcuYdGkJkw6be3eXvVwvLLmZ/svAKs6XT2  
| x7I4FKGqzLCTzS1j0Pma  
| -----END CERTIFICATE-----
```

Probamos ingresar la contraseña a este puerto

openssl s_client -connect localhost:31790 -quiet

JQtffApK4SeyHwDII9SXGR50qcIOAi11

```
bandit16@bandit: ~
bandit16@bandit:~$ openssl s_client -connect localhost:31790 -quiet
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb 13 06:43:06 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb 13 06:43:06 2023 GMT
verify return:1
JQtffApK4SeyHwDII9SXGR50qcIOAi11
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuiFmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl7870Ri0+rW4LDCND2lUvLE/GL2GwyuKNOK5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WwAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpwTMAZJTzAZQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAOIBABagppxPM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xFW+24pRNUDE6SFthOar69jp5R1LwD1NhPx3iB1
J9nOM80J0VToum43UOS8YxF8WwhXr-iYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvFe0050vk9TL5wqbu9A1bssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKuFD52yOQ9q0kwFTEQpjtf4uNtJom+asv1pmS8A
-----END RSA PRIVATE KEY-----
```

```
bandit16@bandit: ~
DSt2mcNn4rhAL+JFr56o4T6z8WwAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpwTMAZJTzAZQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAOIBABagppxPM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xFW+24pRNUDE6SFthOar69jp5R1LwD1NhPx3iB1
J9nOM80J0VToum43UOS8YxF8WwhXr-iYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvFe0050vk9TL5wqbu9A1bssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKuFD52yOQ9q0kwFTEQpjtf4uNtJom+asv1pmS8A
vLY9r6WYsVmZhnqB8Uj7lYctXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghiFKLxrlgtT+qDpfZnx
SatLdt8GFQ85yA7hnlWJ2Mx3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/Fwju1httfX/rHYKHLidZDFYeiE/v45bN4yFm8x7R/b0iE7KasZx+Exdvt
SghaTdcG0Knyw1bpJvYusavPzpaJMjdJ6tcFhVAbAjm7enCivGC5x+X315SiWg0A
R57hJg1ezIiVjv3aGwHwv1ZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxU1+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWcg
R8VdwSk8r9FGL5+9aKcV5PI/WEK1wgXinB30hYimtiG2Cg5JCqIZFHxD6MjEGoiu
L8ktHMPvodBwNsSUBLPg0QKBgBAp1TfC1H0nWiMGOU3KPwYwt006CdtkmJ0mL8Ni
b1h9elyZ9FsGxsgtRBXRsqXuz7wtsQAGLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAwFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZRqaM
77pBAoGAMmjmiJdjp+Ez8duyn3ieo36yrTtF5N5sJLABxPfd1c1gvtGCWw+9Cq0b
dxviw8+TFVEB1104f7HvM6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPxX8MBTakzh3
vBgsyi/sN3RqRBcGU40FoZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
bandit16@bandit:~$
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuiFmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl7870Ri0+rW4LDCND2lUvLE/GL2GwyuKNOK5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WwAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpwTMAZJTzAZQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAOIBABagppxPM1aoLWfvD
```



```
KHCj10nqcoBc4oE11aFYQwik7xfw+24pRNUDE6SFthOar69jp5RlLwD1NhPx3iB1
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESZH22P29ovd
d8WERY0gPxun8pbJLmXkAtWNhpMvfe0050vk9TL5wqbu9A1bssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKuFd52yOQ9qOkwFTEQpjtf4uNtJom+asvlpms8A
vLY9r60wYsvmZhnqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRbB2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghfKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnwWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRntMSkCgYEAypHd
HCctNi/Fwju1httfX/rHYKhLiDZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpjVvusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X315SiWg0A
R57hJg1ezIiVjv3aGwHwv1ZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxU1+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmLy9FL2m9oQwCg
R8VdWsk8r9FGLS+9aKcV5PI/WEK1wgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodbWnsSBULpG0QKBgBAp1TfC1H0nWiMGOU3KPWYwt006CdTkmJ0mL8Ni
b1h9e1yZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdSOokvDQNWu6ucyLRAWFuISexw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZrQaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrTtF5NsSjLABxPdp1c1gvtGCWw+9Cq0b
dxviw8+TFVEB1104f7HVM6EpTscDxU+bCXwkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

Observamos que nos otora una llave privada. Para usarla debemos crear un archivo tipo private, pero como no tenemos permisos de escritura en este directorio tendemos que hacerlo en el directorio tmp.

The screenshot shows a terminal window titled 'bandit16@bandit: /tmp'. Inside, the GNU nano 6.2 text editor is open, editing a file named 'clave.private'. The file contains an RSA private key, starting with '-----BEGIN RSA PRIVATE KEY-----' and ending with '-----END RSA PRIVATE KEY-----'. The key data is a long string of base64-encoded text. The terminal window has standard window controls (minimize, maximize, close) in the top right corner. At the bottom, there is a navigation bar with keyboard shortcuts for various editor functions like Help, Write Out, Where Is, Cut, Execute, Location, Exit, Read File, Replace, Paste, Justify, and Go To Line.

```
bandit16@bandit: /tmp/roberto2
bandit16@bandit:/tmp/roberto2$ nano clave.private
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/roberto2$ cat clave.private
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvM0kufmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558Yw3FZl870RiO+rW4LDCdNd2lUvLE/GL2GwyuKNOK5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WwAw18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmzpwMazJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjFkU1jH5+9EbVNj+D1XF0JuaQIDAQABoIABAggxpM1aoLWfVd
KHcj10nqcoBc4oE1laFYQwik7xfw+24pRNUDE6SFth0ar69jp5RlLwD1NhPx3iB1
J9nOM80J0VToum43U058YxwF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH2P29ovd
d8WErY0gPxun8pbJLmXkAtWNhpMvfe0050vk9TL5wqbu9A1bssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpms8A
vLY9r60wYSvmZhnqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRh0RT
8c8hAuRb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRntMSkCgYEAypHd
HCctNi/Fwju1httFx/rHYKhLiDZDFYeiE/v45bN4yFm8x7R/b0ie7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGC5x+X3l5SiWg0A
R57hJg1ezIiVjv3aGwHwv1ZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtiEk7xRVxU1+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWcg
R8VdwSk8r9FGLS+9aKcV5PI/wEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEGoiu
L8ktHMPvodBwNsSBULpG0QK8gBAp1TfC1H0nWiMG0U3KPwYwT006CdTkmJ0mL8Ni
b1h9e1yZ9FsGxsgtRBXRsqXuz7wtsQAglHxbdlQ/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHd50oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLABxPpd1c1gvtGCWw+9Cq0b
dxviW8+TFVEB1104f7HVM6EpTsCdDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgsyi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
```

Echo esto para poder enviar este archivo requerimos que el archivo tenga los permisos necesarios de escritura y lectura para el usuario. Para ello utilizaremos el comando `chmod` con la configuracion 400, luego de esto lo compribamos.

```
chmod 400 clave.private
```

```
ssh -i clave.private bandit17@localhost -p 2220
```


Por ultimo buscamos nuestra contraseña como en el ejercicio 15.

```
cd /etc/bandit_pass/
```

```
bandit17@bandit: /etc/bandit_pass
bandit17@bandit:~$ cd /etc/bandit_pass/
bandit17@bandit:/etc/bandit_pass$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10  bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11  bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit17@bandit:/etc/bandit_pass$ cat bandit17
Vw05WtCA7lRkkTfbr2IDh6awj9RNZM5e
bandit17@bandit:/etc/bandit_pass$
```

Pass VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

Comprobamos.

[illegible]

```
bandit17@bandit: ~  
  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* peda (https://github.com/longld/peda.git) in /opt/peda/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
bandit17@bandit:~$ |
```

Referencias

- <https://es.wikipedia.org/wiki/Base64>