

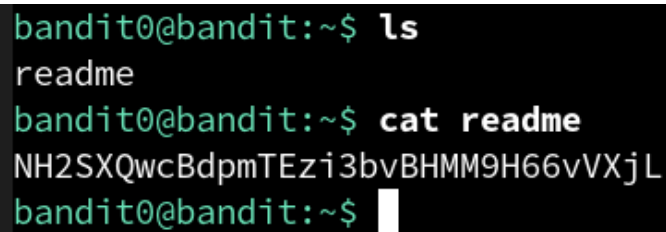
# Tarea 1 - Terminal de Sistemas basados en UNIX

Iñaki Cornejo

February 6, 2024

Level0 → Level1

Imagen Evidencia



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

Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: lo usé para ver que archivos había en el directorio actual.
- cat - comando para mostrar el contenido de un archivo de texto: para ver el contenido del archivo readme.

## Level1 → Level2

### Imagen Evidencia

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

### Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: lo usé para ver que archivos había en el directorio actual.
- cat - comando para mostrar el contenido de un archivo de texto: como cat toma el caracter - como stdin usé './-' para poder leer el archivo -.

## Level2 → Level3

### Imagen Evidencia

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

### Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: lo usé para ver los archivos en el directorio actual.
- cat - comando para mostrar el contenido de un archivo de texto: para poder leer el archivo como tenía espacios tuve que correr cat con el

nombre del archivo entre comillas para que no interpretara que quería leer varios archivos.

## Level3 → Level4

### Imagen Evidencia

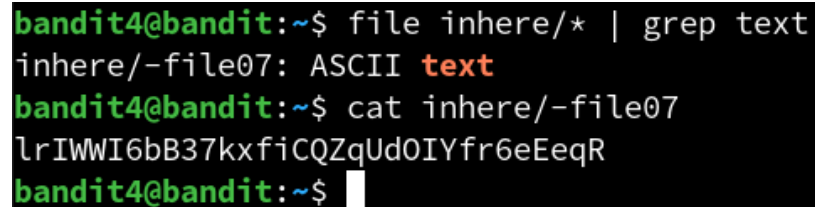
```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

### Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: usé el comando para ver que archivos habían en el directorio actual y luego para ver los archivos ocultos dentro del directorio ls.
- cd - comando para cambiar el directorio actual del shell: lo usé para entrar al directorio inhere.
- cat - comando para mostrar el contenido de un archivo de texto: lo use para leer el archivo .hidden.

## Level4 → Level5

### Imagen Evidencia



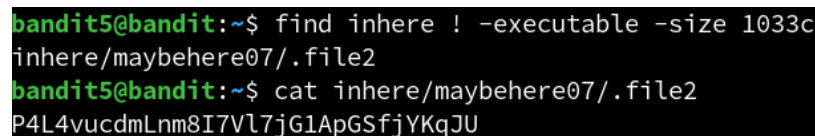
```
bandit4@bandit:~$ file inhere/* | grep text
inhere/-file07: ASCII text
bandit4@bandit:~$ cat inhere/-file07
lrIWWI6bB37kxfiCQZqUd0IYfr6eEeqR
bandit4@bandit:~$
```

### Comandos Usados

- file - comando para mostrar información sobre el tipo de un archivo: use file con un wildcard para ver el tipo de archivo de todos los archivos dentro del directorio inhere.
- grep - comando para buscar texto de acuerdo a un patrón específico (posiblemente regex) en stdin o archivos: con un pipe pasé los tipos de archivos que había en inhere a grep para ver que archivo era de texto.
- cat - comando para mostrar el contenido de un archivo de texto: una vez que encontré el archivo ASCII lo pude leer con cat.

## Level5 → Level6

### Imagen Evidencia



```
bandit5@bandit:~$ find inhere ! -executable -size 1033c
inhere/maybehere07/.file2
bandit5@bandit:~$ cat inhere/maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

### Comandos Usados

- find - comando para buscar recursivamente archivos que cumplen ciertas características: use find negando el predicho executable y usando

size para encontrar un archivo que cumpliera con las características del nivel.

- cat - comando para mostrar el contenido de un archivo de texto: una vez que encontré el archivo con find lo pude leer usando cat.

## Level6 → Level7

### Imagen Evidencia

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>&-  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S  
bandit6@bandit:~$
```

### Comandos Usados

- find - comando para buscar recursivamente archivos que cumplen ciertas características: use find con los predicados user, group y size para encontrar el archivo que cumpliera las características del reto. Cierre el stream stderr para no recibir todos los errores de permisos.
- cat - comando para mostrar el contenido de un archivo de texto: lo usé para poder leer el archivo indicado.

## Level7 → Level8

### Imagen Evidencia

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

### Comandos Usados

- grep - comando para buscar texto de acuerdo a un patrón específico (posiblemente regex) en stdin o archivos: use grep para buscar la palabra millionth en el archivo data.txt y así la contraseña.

## Level8 → Level9

### Imagen Evidencia

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

### Comandos Usados

- sort - comando para organizar líneas de texto de forma alfabética: usé sort para tener todas las líneas ordenadas para uniq.
- uniq - comando para identificar/manipular líneas repetidas: con un pipe pasé las líneas ordenadas a uniq con la opción -u para sólo mostrar las líneas no repetidas.

## Level9 → Level10

### Imagen Evidencia

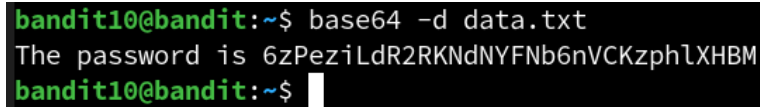
```
bandit9@bandit:~$ strings data.txt | grep '=\\{3,\\}'
x]T===== theG)"
===== passwordk^
===== is
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
bandit9@bandit:~$
```

### Comandos Usados

- strings - comando para imprimir las cadenas de texto legible de archivos: usé esto para imprimir todas las cadenas de texto de data.txt.
- grep - comando para buscar texto de acuerdo a un patrón específico (posiblemente regex) en stdin o archivos: con un pipe pasé las cadenas de texto a grep para filtrar las que contienen al menos 3 signos de igual.

## Level10 → Level11

### Imagen Evidencia



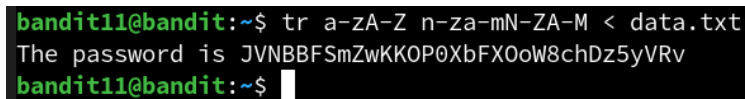
```
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

### Comandos Usados

- base64 - comando para codificar y decodificar información en formato base64: usé base64 con la opción -d para decodificar el contenido de data.txt.

## Level11 → Level12

### Imagen Evidencia



```
bandit11@bandit:~$ tr a-zA-Z n-za-mN-ZA-M < data.txt
The password is JVNBBFSmZwKKOP0XbFX0oW8chDz5yVRv
bandit11@bandit:~$
```

### Comandos Usados

- tr - comando para convertir un rango de caracteres a otro: para hacer el ROT13 mandé el contenido de data.txt a tr usando del rango a-zA-Z a n-za-mN-ZA-M.

## Level12 → Level13

### Imagen Evidencia

```
bandit12@bandit:~$ mkdir /tmp/hfc
bandit12@bandit:~$ cp data.txt /tmp/hfc
bandit12@bandit:~$ cd /tmp/hfc
bandit12@bandit:/tmp/hfc$ xxd -r data.txt outfile
bandit12@bandit:/tmp/hfc$ file outfile
outfile: gzip compressed data, was "data2.bin", last modified: Thu Oct 5 06:19:20 202
3, max compression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/hfc$ mv outfile outfile.gz
bandit12@bandit:/tmp/hfc$ gunzip outfile.gz
bandit12@bandit:/tmp/hfc$ file outfile
outfile: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/hfc$ mv outfile outfile.bz
bandit12@bandit:/tmp/hfc$ bunzip2 outfile.bz
bandit12@bandit:/tmp/hfc$ file outfile
outfile: gzip compressed data, was "data4.bin", last modified: Thu Oct 5 06:19:20 202
3, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/hfc$ mv outfile outfile.gz
bandit12@bandit:/tmp/hfc$ gunzip outfile.gz
bandit12@bandit:/tmp/hfc$ file outfile
outfile: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hfc$ tar xvf outfile
data5.bin
bandit12@bandit:/tmp/hfc$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hfc$ tar xvf data5.bin
data6.bin
bandit12@bandit:/tmp/hfc$ file data
data5.bin data6.bin data.txt
bandit12@bandit:/tmp/hfc$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/hfc$ mv data6.bin outfile.bz
bandit12@bandit:/tmp/hfc$ bunzip2 outfile.bz
Command 'bunzip2' not found, did you mean:
  command 'gunzip' from deb gzip (1.10-4ubuntu4.1)
  command 'bunzip2' from deb bzip2 (1.0.8-5build1)
  command 'runzip' from deb rzzip (2.1-4.1)
  command 'funzip' from deb unzip (6.0-26ubuntu3.1)
  command 'lunzip' from deb lunzip (1.13-1)
  command 'unzip' from deb unzip (6.0-26ubuntu3.1)
  command 'ebunzip' from deb eb-utils (4.4.3-13)
Try: apt install <deb name>
bandit12@bandit:/tmp/hfc$ bunzip2 outfile.bz
bunzip2: Output file outfile already exists.
bandit12@bandit:/tmp/hfc$ rm outfile
bandit12@bandit:/tmp/hfc$ bunzip2 outfile.bz
bandit12@bandit:/tmp/hfc$ file outfile
outfile: POSIX tar archive (GNU)
bandit12@bandit:/tmp/hfc$ tar xvf outfile
data8.bin
bandit12@bandit:/tmp/hfc$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Oct 5 06:19:20 2
023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/hfc$ mv data8.bin data8.gz
bandit12@bandit:/tmp/hfc$ gunzip data8.gz
bandit12@bandit:/tmp/hfc$ file data9.bin
data9.bin: cannot open 'data9.bin' (No such file or directory)
bandit12@bandit:/tmp/hfc$ file data8
data8: ASCII text
bandit12@bandit:/tmp/hfc$ cat data8
The password is wbWd1BxEir4CaE8LaPhauU0o6pwRmrDw
bandit12@bandit:/tmp/hfc$
```

### Comandos Usados

- mkdir - comando para crear un directorio: usé el comando para crear un directorio en /tmp.
- cp - comando para copiar un archivo: usé el comando para copiar data.txt al directorio temporal.
- file - comando para mostrar información sobre el tipo de un archivo:



usé este comando con cada archivo resultante para averiguar el formato del nuevo archivo.

- `xxd` - comando para convertir entre octal, binario, hexadecimal: usé el comando con la opción `-r` para decodificar el archivo hexdump.
- `mv` - comando para mover/renombrar archivos: usé el comando para renombrar los archivos para que tengan la extensión adecuada.
- `gunzip` - comando `gzip` pero exclusivamente para descomprimir: usé el comando para descomprimir archivos comprimidos con `gzip`.
- `bunzip2` - comando `bzip2` pero exclusivamente para descomprimir: usé el comando para descomprimir archivos comprimidos con `bzip2`.
- `tar` - comando para crear y abrir archivos del formato GNU tar posiblemente comprimidos en una variedad de formatos: use el comando para descomprimir el archivo formato tar.
- `cat` - comando para mostrar el contenido de un archivo de texto: usé el comando para ver el contenido del archivo en formato ASCII.

## Level13 $\rightarrow$ Level14

## Imagen Evidencia

[illegible]

## Comandos Usados

- ssh - comando para ejecutar comandos/shell de forma remota y segura: usé ssh con la opción -i para usar la llave privada.
- cat - comando para mostrar el contenido de un archivo de texto: usé el comando para leer la contraseña del nivel una vez hecho el login con ssh.

## Level14 → Level15

### Imagen Evidencia



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

### Comandos Usados

- echo - comando para imprimir texto a stdout: usé el comando para mandar la contraseña al stdin de netcat.
- netcat - comando para conectar stdin con un puerto específico (connect mode): use netcat para mandar la contraseña a localhost en el puerto 30000.

## Level15 → Level16

### Imagen Evidencia

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb  6 04:53:11 2024 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb  6 04:53:11 2024 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
  i:CN = localhost
  a:PKKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
  v:NotBefore: Feb  6 04:52:11 2024 GMT; NotAfter: Feb  6 04:53:11 2024 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAF0gAwIBAgIEW40gODANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQDDA1s
b2NhbgHvc3QwHhcNMjQwMDQ1MjExWhcNMjQwMDQ1MzExWjAUMRIwEAYD
VQDDA1sb2NhbgHvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB
ucWVxpWHhB2ZzfjR+qdB044xcJtC3bqt+WCV9hZLiBFBSULj8kKZTHpQbscQnWyn
tu48xoUQBmPscJC70UdXs09oT0ub0SwwybPK9a2DXzY0LIBFc+Dcg4IkutpeRaFp
TsCAl0ZdqJr01iSx8ASrVn8kfcjh30ZoS7G+Gy0+D3Z4PXw1T7WIB/7IkMSAH+f
+ujo1bZNLyDLrhckxHxu7YwavRip2JyGoHydZ0eFP0K6ksED1T9pFaZ0QJUD6p9e
2z4C4S+3TScrKagZwcSU8UKNl0WKNm908sYvMVN426D2JdLk30+NxDHSr+vE9MMg
G84pWVYKJcX4hN7m/S8/AgMBAAGjZTBjMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDBL
BgLghkgBhvhCAQ0EPhY8QXV0b21hdGJjYWxseSBnZW5lcmF0ZWQgYnkgTmNhdC4g
U2VlIGh0dHBz0i8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3DQEBAQUAA4IBAQBk
feac/s0NKlq/yFwlrSMBzlwqvTsME0gwJtiWJKIjwNZX/jnZ+/bqpvwmKGjlsF
JEKHv64Ed0k4fAodQVBX3LaoAu5FT0y09rbegDQJqYHJfYmmF+XmtBwk9Bt49kuF
ku+2mLWL+WPEojEiksA7paMnD03XY5gCw9ElhcjKfzJvRokfjJLaRvs28vf3WT2W
f2gaG3j113Kz8B6ad4NH0Wzra8tyRHLXLF4WCcnw8V8P44KZbDGGJBB3nTv63xwIM
kHJBYrgBy39SE8390lQHEDi+wyNHP11D0m67fNhKLCMGj6B17r57fs38FJfYa/P6
BhbgwPhXw+K1YrgsKX0e
-----END CERTIFICATE-----
```

### Comandos Usados

- `openssl-s_client` - comando parte de openssl para realizar conexiones con el protocolo TLS: usé el comando con la opción `-connect` para conectar a `localhost:30001`.

## Level16 → Level17

### Imagen Evidencia

```
bandit16@bandit:~$ nmap -A -T4 localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-06 17:39 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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: 2024-02-06T04:52:12
|_Not valid after: 2024-02-06T04:53:12
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help,
chReq, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, TLSSession
rCookie:
|_   Wrong! Please enter the correct current password
```

```

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuiFmMg6HL2YPI0jon6iWfbp7c3jx34YkVwQUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LDCDnd2LUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30eKePQAZL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAZJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLLwD1NhPx3iB1
J9nOM80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LDCDnd2LUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30eKePQAZL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAZJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLLwD1NhPx3iB1
J9nOM80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPXun8pbJLmXkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcXkMqNpW9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtf4uNtJom+asvlpms8A
vLY9r60wYsvmZhNqBURj7LyCtXMIu1kkd4w7F77k+DjHoAXycUp1DGL51s0mama
+TOWWgECgYEABJtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NhgRRhR0T
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpogsgHfKLxrlgt+qDpfZnx
SatLdt8GfQ85yA7hnWwJ2Mx3F3NaeSDm75Lsm+tBbAiyC9P2jGRntMSKcGvEAYpHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iETKaszX+Exdvt
SghaTdcG0Knyw1bp3VyusavPzpaJmjdJ6tcFhVAbAjm7enCivGCSx+X3L5SiWg0A
R57hJglezIiVjv3aGwHwv1ZvtszK6zV6oXFAu0ECgYABj046T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iU7rWkGAXFpMLFteQEsRr7PJ/LemmEY5eTDAFMY9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwGxinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLTFc1H0nWiMGOU3KPwYwt006CdTkMjOmL8Ni
b1h9elyZ9FsGxsgrtRBXRsqXuz7wtsQAGLHxbdlq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YodHjdS0okvDQNWu6ucyLRAWFuISexw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLabxFpdlc1gvtGCWw+9Cq0b
dxviW8+TFVEB1104f7HVm6EpTscDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgSyj/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit16@bandit:~$ mkdir /tmp/hfc
bandit16@bandit:~$ vim /tmp/hfc/private.key
bandit16@bandit:~$
bandit16@bandit:~$
bandit16@bandit:~$ ll /tmp/hfc/private.key
-rw-rw-r-- 1 bandit16 bandit16 1675 Feb  6 17:53 /tmp/hfc/private.key
bandit16@bandit:~$ chmod 600 /tmp/hfc/private.key
bandit16@bandit:~$ ssh -i /tmp/hfc/private.key bandit17@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihNv1wUXRb4RrEcLFC5CXlhmAAM/urerLY.
This key is not known by any other names

```

## Comandos Usados

- nmap: usé nmap corriendo en cuatro hilos para hacer un port scan en el rango 31000-32000 y obtuve un puerto ssl abierto.
- openssl-s\_client - comando parte de openssl para realizar conexiones con el protocolo TLS: usé el comando para conectarme al puerto que encontré donde escribí la contraseña y recibí una llave ssh.
- vim - editor de texto avanzado que corre en terminal (igual hay un GUI): usé el editor para guardar la llave en un archivo.
- chmod - comando para cambiar los permisos de un archivo: usé el comando para darle los permisos adecuados a la llave ssh.

- ssh - comando para ejecutar comandos/shell de forma remota y segura: usé el comando para hacer login como el usuario del siguiente nivel y obtener la contraseña.

## Level17 $\rightarrow$ Level18

## Imagen Evidencia

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$
```

## Comandos Usados

- diff - comando para ver las líneas diferentes entre dos archivos: usé el comando para ver que línea había cambiado y obtener la contraseña.

## Level18 $\rightarrow$ Level19

## Imagen Evidencia

```
pink@heartofgold:~/...ejercicios/bandit$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat  
readme
```

```
_ _  
| |__ / __/_ _ \ (_)_||_  
| '_\ / ___'___ \| || |_||_|_||  
| |_) | (___) | | | | | | | |_  
|-._./ \_____-||_| |_|_\_-||\___|
```

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

```
bandit18@bandit.labs.overthewire.org's password:  
awhqfNnAbcInaukrpqDYcf95h7HoMTrC  
pink@heartofgold:~/...ejercicios/bandit$ █
```

## Comandos Usados

- ssh - comando para ejecutar comandos/shell de forma remota y segura: usé ssh para establecer la conexión con el servidor y correr un comando.

- cat - comando para mostrar el contenido de un archivo de texto: corrí cat a través de ssh para ver la contraseña del nivel.

## Level19 → Level20

### Imagen Evidencia

```
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
bandit19@bandit:~$
```

### Comandos Usados

- bandit20-do: usé el comando suid para leer la contraseña del siguiente nivel.

## Level20 → Level21

### Imagen Evidencia

```
bandit20@bandit:~$ echo VxCazJaVyki6W36BkBU0mJTCM8rR95XT | netcat -l -p 4242&
[1] 1850935
bandit20@bandit:~$ ./suconnect 4242
Read: VxCazJaVyki6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
NvEJF7oVjkdldtPSrdKEF0llh9V1IBcq
bandit20@bandit:~$
```

### Comandos Usados

- netcat - comando para conectar stdin con un puerto específico (listening mode): usé el comando en listening mode para esperar una conexión a un puerto específico y entonces escribir la contraseña.
- suconnect: el comando para conectarme al puerto donde estaba escuchando netcat.



## Level21 → Level22

### Imagen Evidencia

```
bandit21@bandit:~$ ls /etc/cron.d/
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24      e2scrub_all  sysstat
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root  otw-tmp-dir
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mG1wngMfj4EZff
bandit21@bandit:~$
```

### Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: usé el comando para ver el cronjob indicado.
- cat - comando para mostrar el contenido de un archivo de texto: usé cat para ver el cronjob y luego el archivo temporal con la contraseña.

## Level22 → Level23

### Imagen Evidencia

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

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

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

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ cat /tmp/$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1)
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:~$
```

### Comandos Usados

- ls - comando para mostrar los contenidos de un directorio: usé el comando para ver el cronjob indicado.

- cat - comando para mostrar el contenido de un archivo de texto: usé el comando para leer el cronjob y el archivo temporal una vez que recree el nombre indicado.
- echo - comando para imprimir texto a stdout: usé echo para replicar la cadena creada en el script.
- md5sum - comando para codificar y decodificar del hash md5: usé md5sum en un pipe para replicar la cadena creada en el script.
- cut - comando para imprimir/borrar campos específicos de una línea de texto: usé cut en un pipe para replicar la cadena creada en el script.

## Level23 → Level24

### Imagen Evidencia

```
bandit23@bandit:~$ cat /etc/cron.d/
cronjob_bandit15_root cronjob_bandit23 e2scrub_all sysstat
cronjob_bandit17_root cronjob_bandit24 otw-tmp-dir
cronjob_bandit22 cronjob_bandit25_root .placeholder
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:~$ 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

bandit23@bandit:~$ mkdir /tmp/hfc
mkdir: cannot create directory '/tmp/hfc': File exists
bandit23@bandit:~$ mkdir /tmp/h42
bandit23@bandit:~$ chmod 777 /tmp/h42
bandit23@bandit:~$ echo 'cat /etc/bandit_pass/bandit24 > /tmp/h42/pass' > /var/spool/bandit24/
foo/script.sh && chmod a+x /var/spool/bandit24/foo/script.sh
bandit23@bandit:~$ watch ls /tmp/h42/
bandit23@bandit:~$ cat /tmp/h42/pass
VAFGXJIPBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:~$
```

### Comandos Usados

- cat - comando para mostrar el contenido de un archivo de texto: usé el comando para leer el cronjob y luego para leer la contraseña en el

archivo temporal.

- `mkdir` - comando para crear un directorio: usé el comando para crear un directorio temporal a donde escribir la contraseña.
- `chmod` - comando para cambiar los permisos de un archivo: usé el comando para volver ejecutable mi script.
- `echo` - comando para imprimir texto a `stdout`: usé `echo` con un redirect para crear el script.
- `watch` - comando para monitorear el output de un comando: usé el comando para monitorear los contenidos del directorio temporal hasta que apareciera el archivo con la contraseña.

## Level24 $\rightarrow$ Level25

## Imagen Evidencia

[illegible]

```
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Correct!  
The password of user bandit25 is p7TaowMYrmu230l8hiZh9UvD009hpx8d  
Exiting.  
bandit24@bandit:~$
```

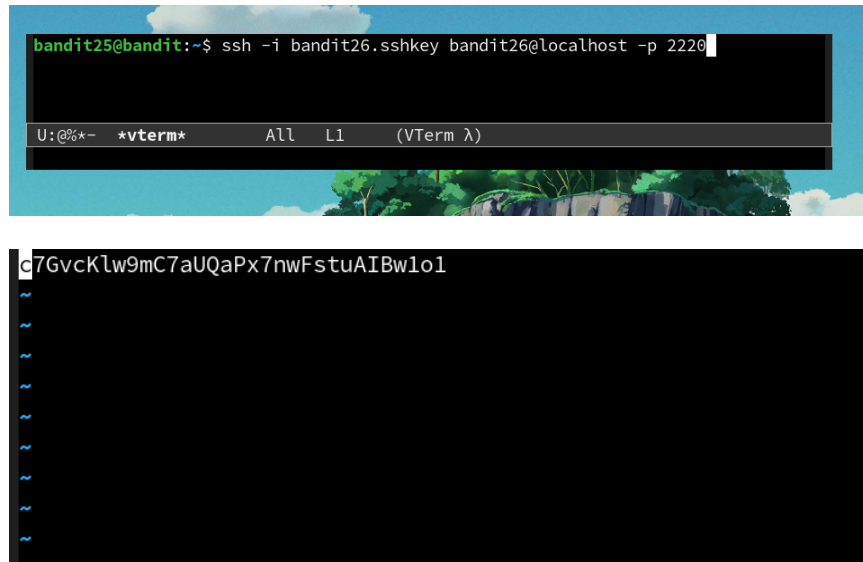
## Comandos Usados

- seq - comando para generar una secuencia de números: usé el comando con la opción -w para generar todas las combinaciones de cuatro dígitos.
- echo - comando para imprimir texto a stdout: usé el comando para mandar la contraseña junto al PIN generado a netcat.

- netcat - comando para conectar stdin con un puerto específico (connect mode): usé el comando para mandar el texto al puerto 30002

## Level25 → Level26

### Imagen Evidencia



### Comandos Usados

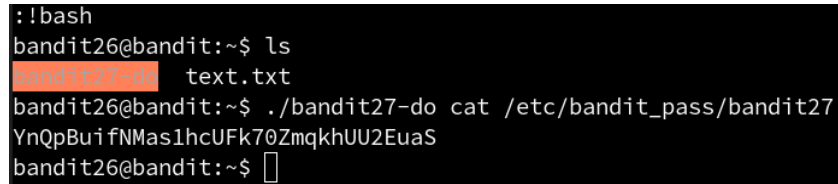
- more - comando para mostrar el contenido de un archivo en terminal: use el comando v para poder abrir el editor de texto vi desde more.
- vi - editor avanzado de texto en terminal: usé el comando para abrir el archivo con la contraseña del próximo nivel.

### Comentarios

Para el nivel 25 si tuve que buscar soluciones para encontrar el truco de hacer pequeña la terminal para poder interactura con el lector more. Ya con ese truco lo demás lo pude resolver a base de leer el manual de more.

## Level26 → Level27

### Imagen Evidencia



```
:!bash
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
bandit26@bandit:~$
```

### Comandos Usados

- more - comando para mostrar el contenido de un archivo en terminal: usé el comando v para abrir vi desde more.
- vi - editor avanzado de texto en terminal: usé los comandos dentro de vi para configurar el shell como bash y después ejecutar bash para obtener un shell.
- bandit27-do: usé el suid para obtener la contraseña del nivel.

## Level27 → Level28

### Imagen Evidencia

```
bandit27@bandit:~$ mkdir /tmp/hfc42
bandit27@bandit:~$ cd /tmp/hfc42
bandit27@bandit:/tmp/hfc42$ 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:C2ihUBV7ihnV1wUXRb4RrEcLFXC5CX1hmAAM/urLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

      _-_-_-_-_-_-_-_-_-_-
      |  _-_-_-_-_-_-_-_-_-_-| ( ) | | | |
      | ' \ / _-_-_-_-_-_-_-_-_-| | |
      | | _/ | _-_-_-_-_-_-_-_-_-| | |
      | | _/ | _-_-_-_-_-_-_-_-_-| | |
      | _-_-_-_-_-_-_-_-_-_-| | _-_-_-_-_-_-_-_-_-|

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

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/hfc42$ cd repo/
bandit27@bandit:/tmp/hfc42/repo$ ls
README
bandit27@bandit:/tmp/hfc42/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rja0M19nR
bandit27@bandit:/tmp/hfc42/repo$
```

### Comandos Usados

- `mkdir` - comando para crear un directorio: usé el comando para crear un directorio temporal donde trabajar.
- `cd` - comando para cambiar el directorio actual del shell: usé el comando para ingresar al directorio temporal.
- `git-clone` - comando para clonar un directorio remoto de git a un directorio local: usé el comando para clonar el directorio indicado.
- `ls` - comando para mostrar los contenidos de un directorio: usé el comando para ver que archivos había en el repo.
- `cat` - comando para mostrar el contenido de un archivo de texto: usé el comando para leer el contenido de README.

## Level28 → Level29

### Imagen Evidencia

```
bandit28@bandit:/tmp/mydir/repo$ git diff f08b9cc63fala4602fb065257633c2dae6e5651b
diff --git a/README.md b/README.md
index b302105..5c6457b 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

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

bandit28@bandit:/tmp/mydir/repo$
```

### Comandos Usados

- mkdir - comando para crear un directorio: usé el comando para crear un directorio temporal donde trabajar.
- cd - comando para cambiar el directorio actual del shell: usé el comando para ingresar al directorio temporal.
- git-clone - comando para clonar un directorio remoto de git a un directorio local: usé el comando para clonar el directorio indicado.
- git-log - comando para enseñar los commits de un repo git: usé el comando para ver que commits había en el repo.
- git-diff - comando de git para ver las diferencias entre commits: usé el comando para ver que había cambiado de un commit y obtener la contraseña.

## Level29 → Level30

### Imagen Evidencia

```
bandit29@bandit:/tmp/mymydir/repo$ git branch --all
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/spl0its-dev
bandit29@bandit:/tmp/mymydir/repo$ git checkout remotes/origin/dev
Note: switching to 'remotes/origin/dev'.

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

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

    git switch -c <new-branch-name>

Or undo this operation with:

    git switch -

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

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

## credentials

- username: bandit30
- password: xbhV3HpNGLTIIdnjUrdAlPzc2L6y9E0nS

bandit29@bandit:/tmp/mymydir/repo$
```

### Comandos Usados

- mkdir - comando para crear un directorio: usé el comando para crear un directorio temporal donde trabajar.
- cd - comando para cambiar el directorio actual del shell: usé el comando para ingresar al directorio temporal.
- git-clone - comando para clonar un directorio remoto de git a un directorio local: usé el comando para clonar el directorio indicado.
- cat - comando para mostrar el contenido de un archivo de texto: usé el comando para leer el contenido del README.md.



- git-branch - comando para ver las ramas del repo: usé el comando con la opción `-all` para ver todas las ramas del repo.
- git-checkout - comando para poder cambiar el repo a otra rama: usé el comando para cambiar a la rama dev donde sí estaba la contraseña.

## Level30 → Level31

### Imagen Evidencia

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

### Comandos Usados

- mkdir - comando para crear un directorio: usé el comando para crear un directorio temporal donde trabajar.
- cd - comando para cambiar el directorio actual del shell: usé el comando para ingresar al directorio temporal.
- git-clone - comando para clonar un directorio remoto de git a un directorio local: usé el comando para clonar el directorio indicado.
- git-tag - comando para ver los tags de un repo: usé el comando para ver los tags que tenía el repo.
- git-show - comando para ver tags/commits: usé el comando para ver el texto del tag secret.

### Comentarios

Me tardé un gran rato en recordar los tags pero me ayudó ver los subcomandos de git en la manpage.

## Level31 $\rightarrow$ Level32

## Imagen Evidencia

[illegible]

## Comandos Usados

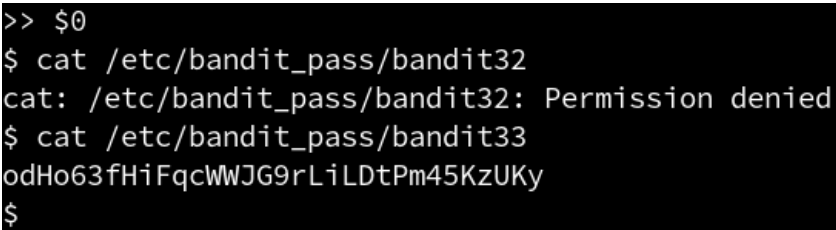
- mkdir - comando para crear un directorio: usé el comando para crear un directorio temporal donde trabajar.
- cd - comando para cambiar el directorio actual del shell: usé el comando para ingresar al directorio temporal.
- git-clone - comando para clonar un directorio remoto de git a un directorio local: usé el comando para clonar el directorio indicado.
- git-add - comando para agregar archivos y cambios de archivos al staging area del repo: usé el comando con la opción -f para agregar el

archivo ignorando el gitignore y poder hacer commit.

- git-push - comando para empujar cambios en un repo local a un repo remoto: usé el comando para mandar el cambio al remoto y recibir la contraseña.

## Level32 → Level33

### Imagen Evidencia



```
>> $0
$ cat /etc/bandit_pass/bandit32
cat: /etc/bandit_pass/bandit32: Permission denied
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
$
```

### Comandos Usados

- bash: usé el parametro especial \$0 para poder abrir el shell original y obtener la contraseña.

### Comentarios

La primera vez que hice este reto lo hice con puras wildcards y no me acuerdo como pude.