Universidad Tecnológica de Panamá

Facultad de Ingeniería de Sistemas Computacionales

Departamento de Sistemas de Información, Evaluación y Control de Recursos Informáticos

Licenciatura en Ingeniería de Sistemas de Información

Seguridad Informática

Tarea #3: Overthewire challenge

Profesor: José Moreno

Estudiantes:

Cutire, Fernando (8-972-906)

Diaz, Gabriel (20-53-5198)

Gamero, Jonathan (8-982-2008)

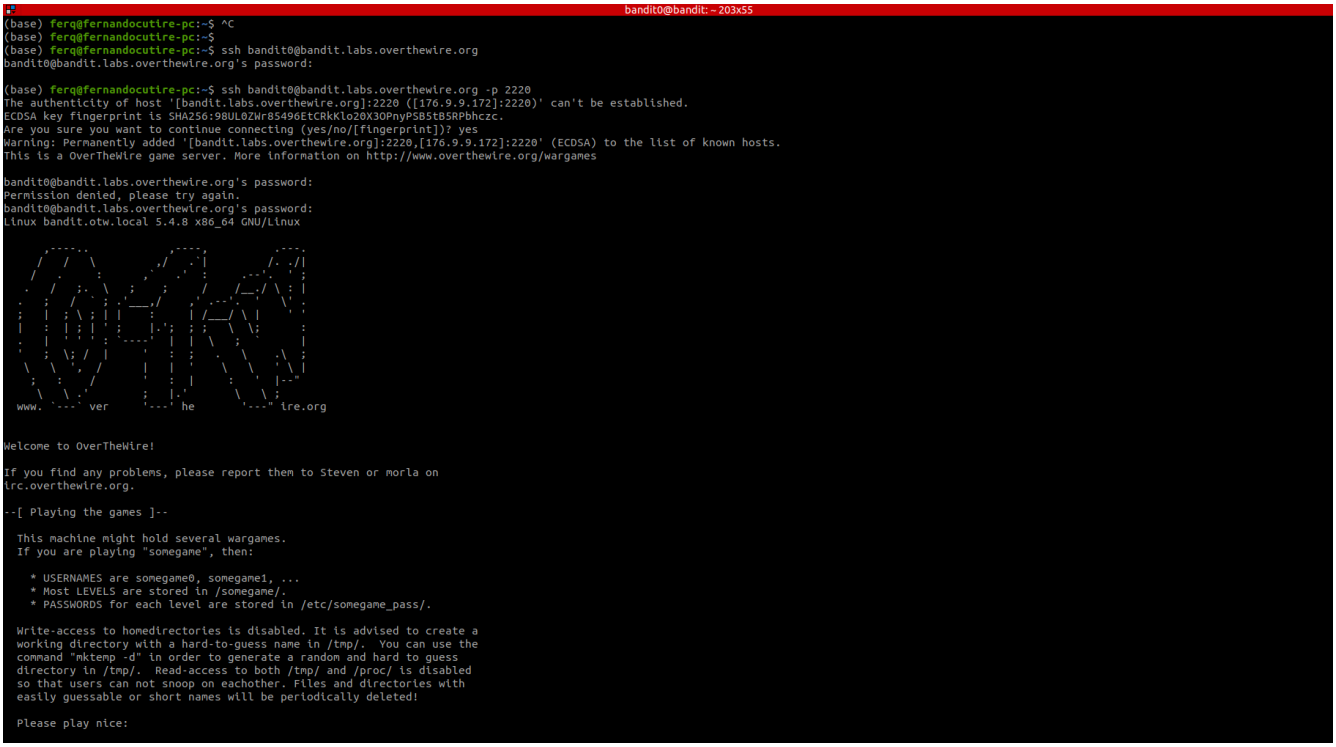
Grupo: 1IF141

I Semestre

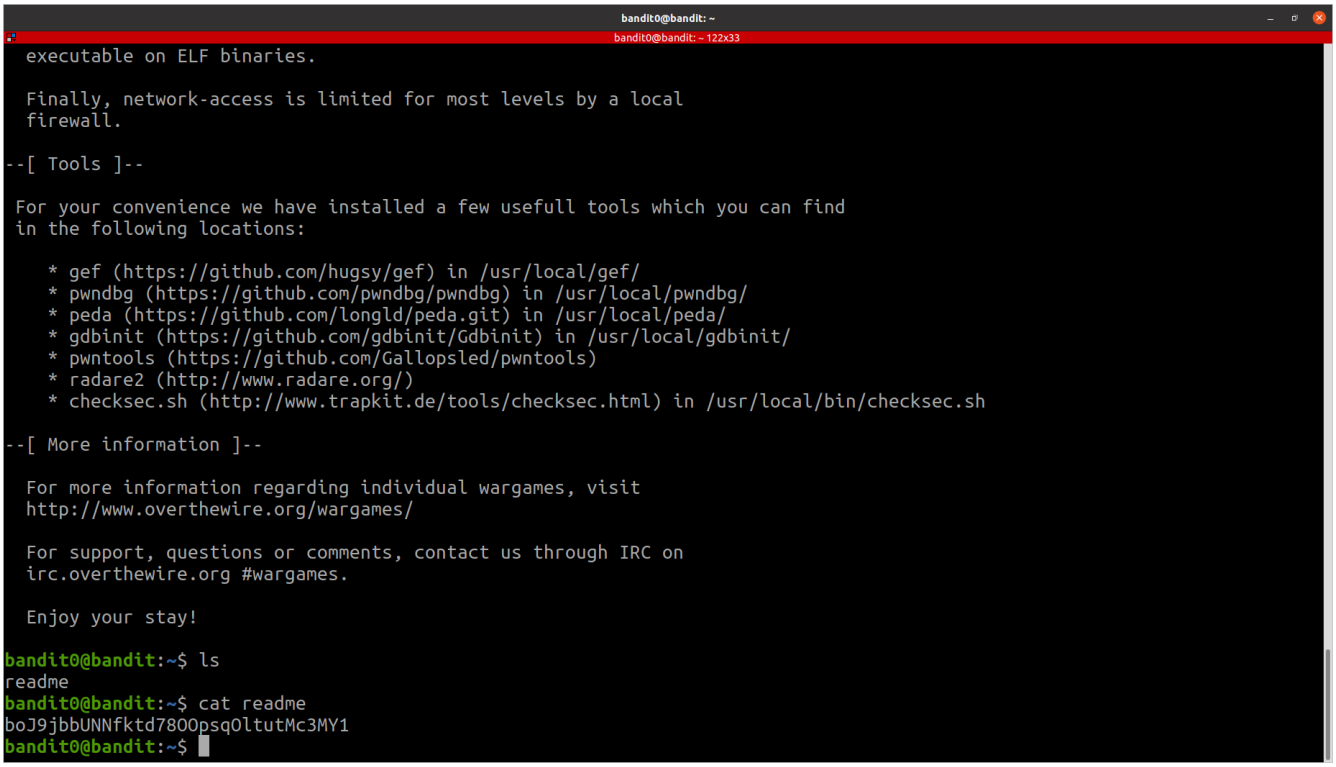
2022

Over the wire

Nivel 0



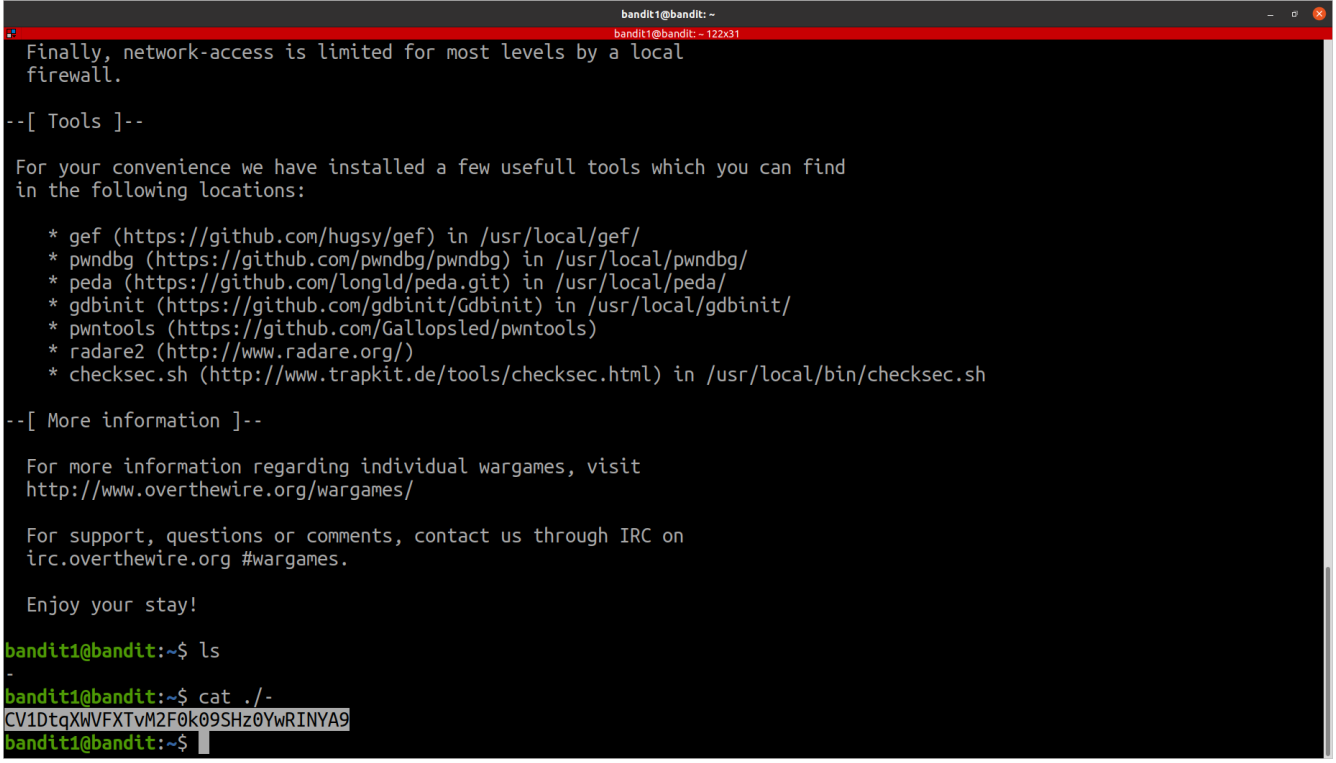
Nivel 0 to 1



Contraseña obtenida:

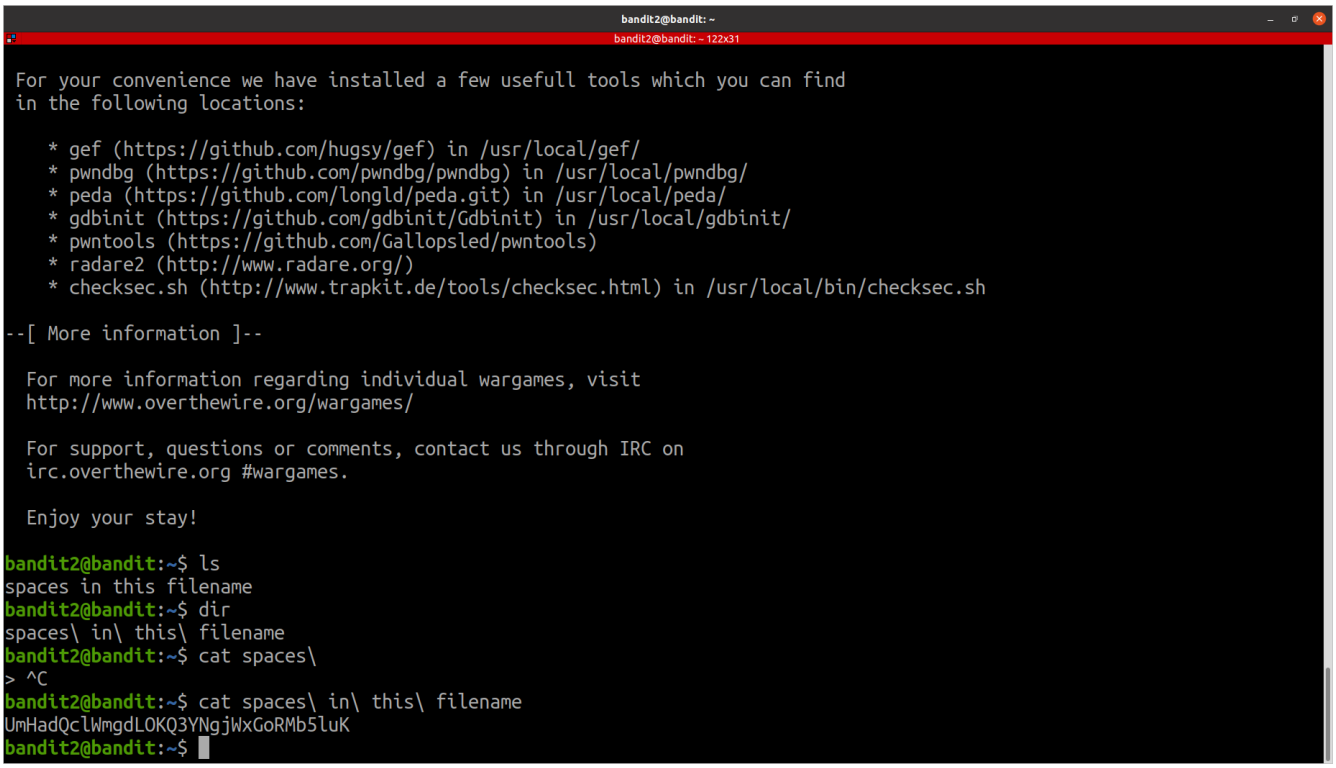
boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Nivel 1 to 2



Contraseña obtenida:
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

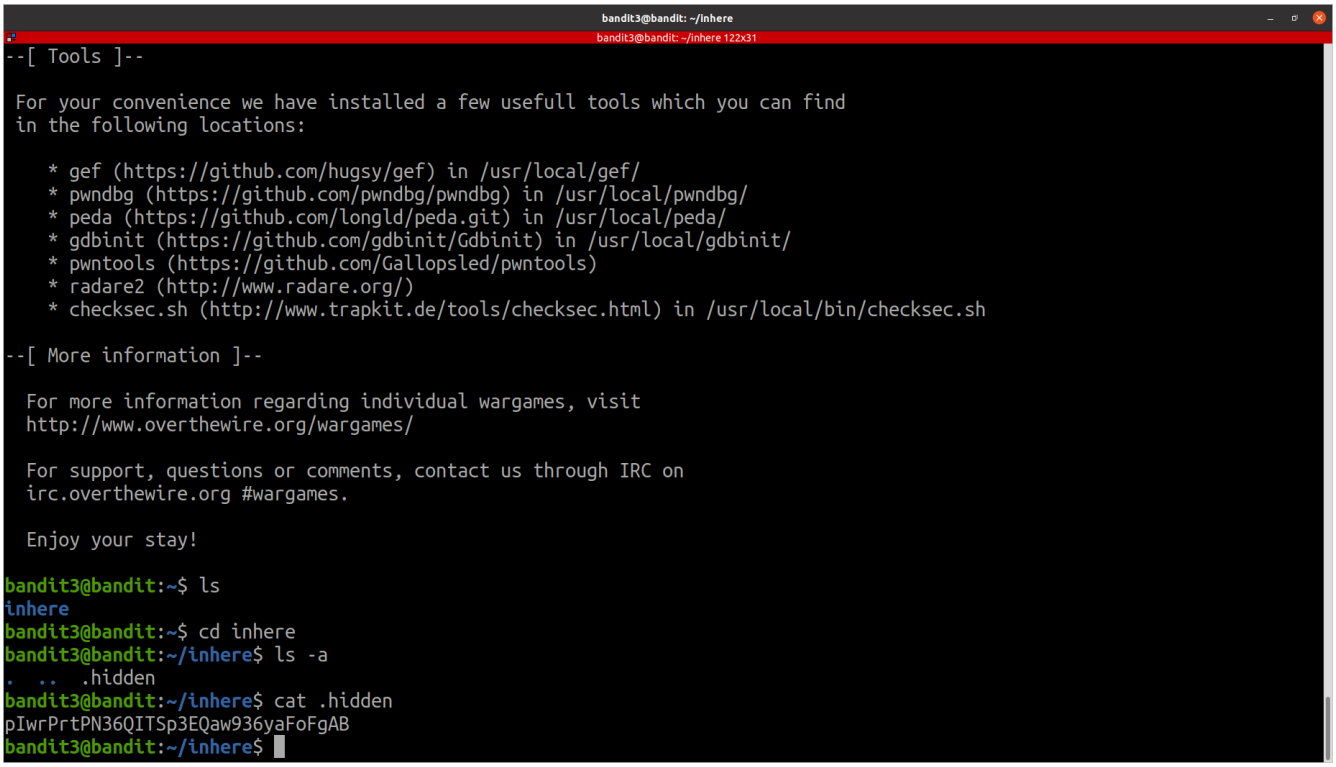
Nivel 2 to 3



Contraseña obtenida:

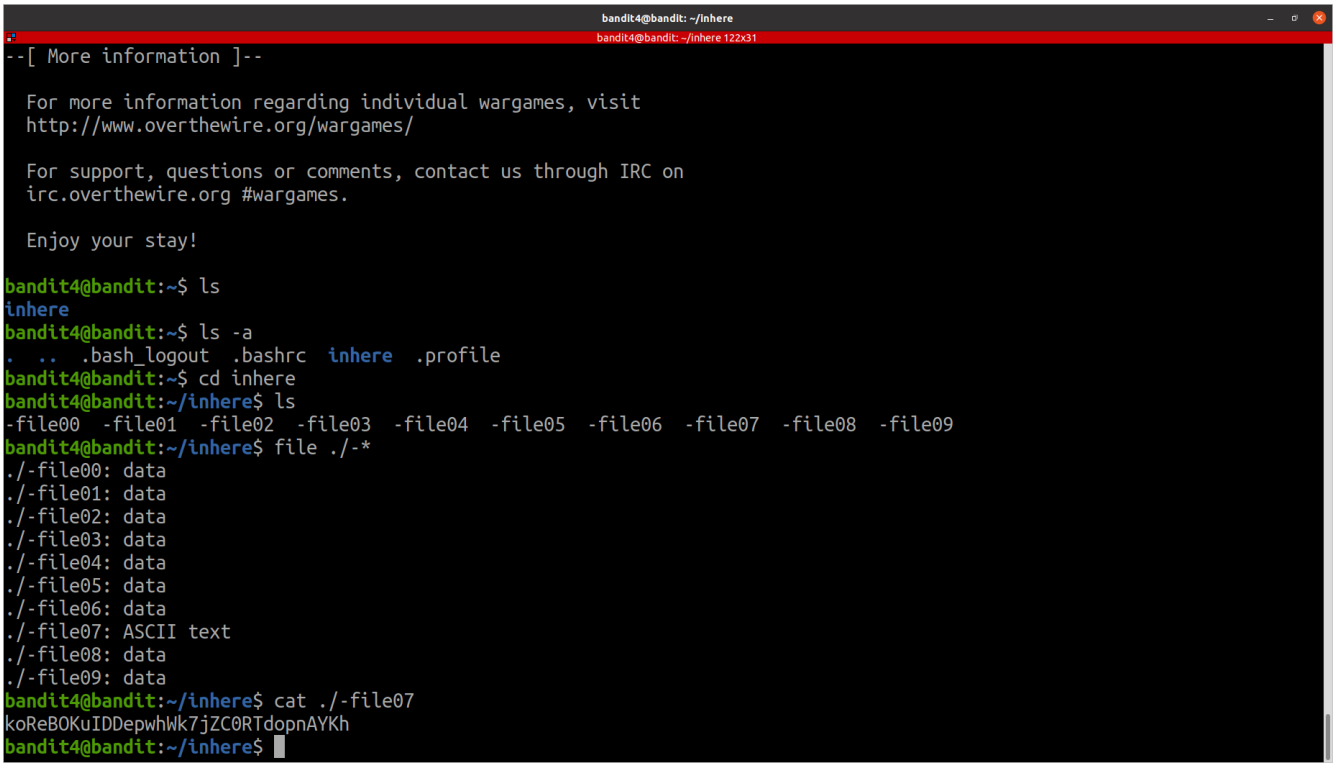
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Nivel 3 to 4



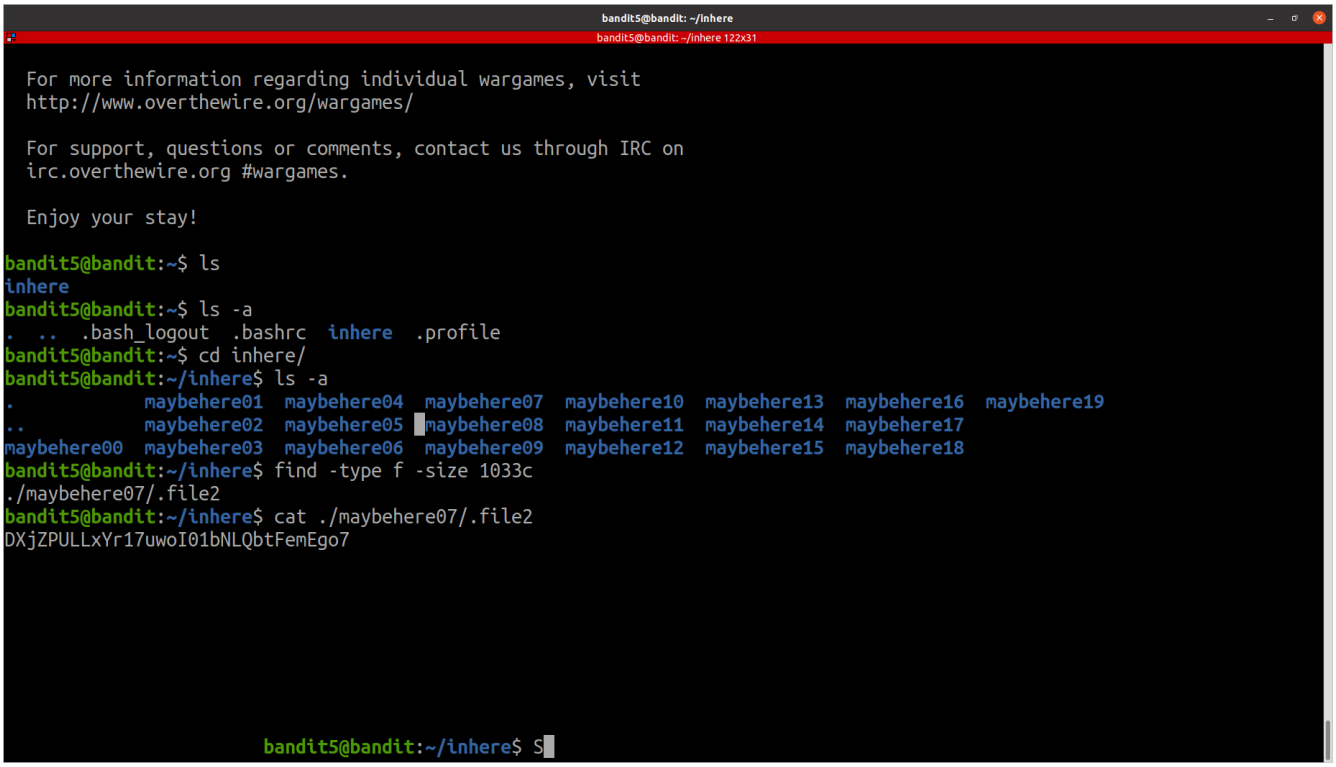
Contraseña obtenida:
pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Nivel 4 to 5



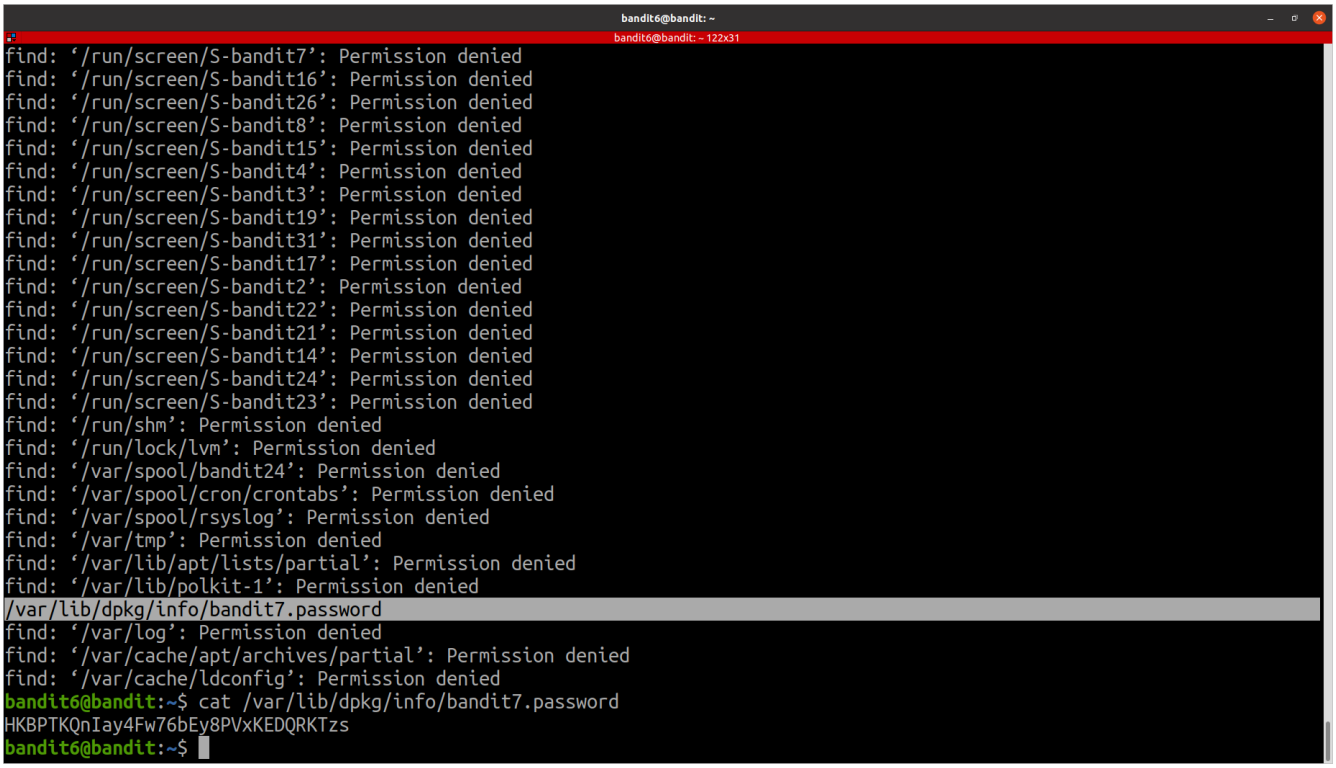
Contraseña obtenida:
koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Nivel 5 to 6



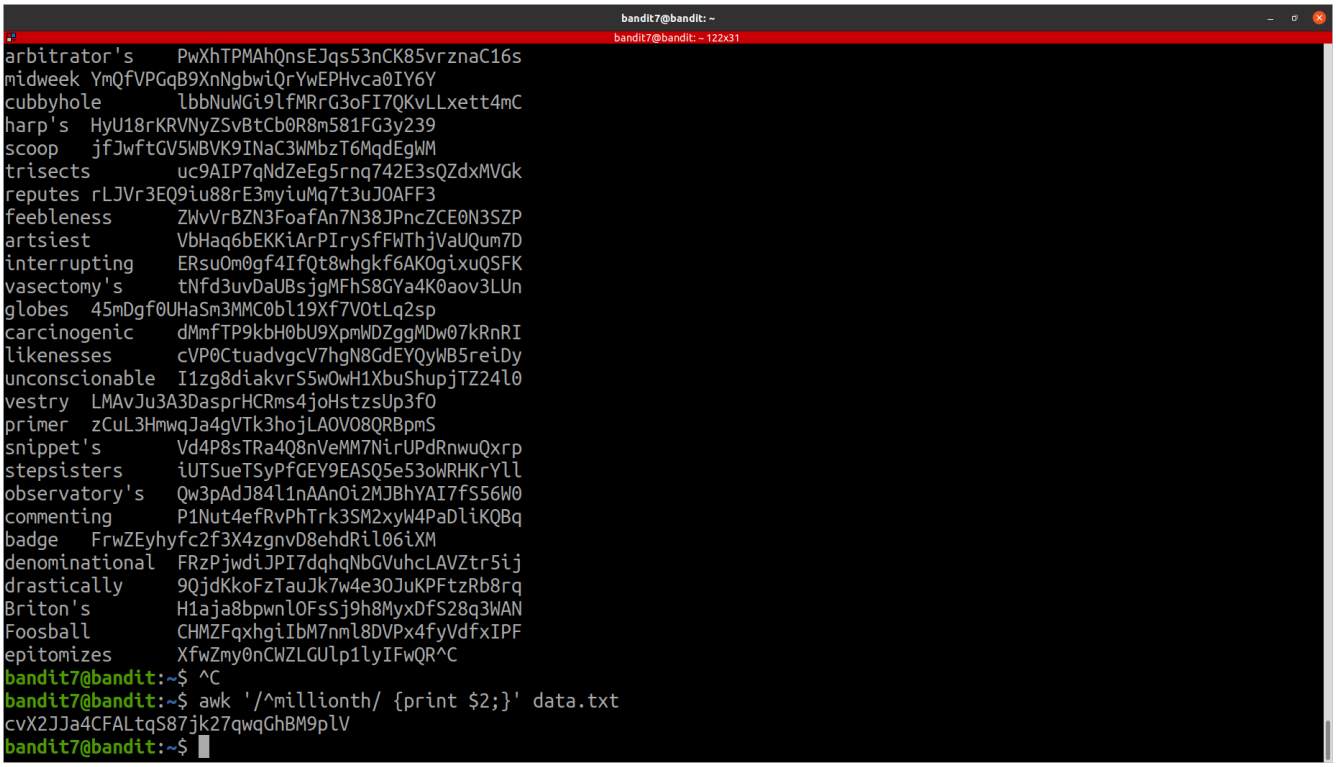
Contraseña obtenida:
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Nivel 6 to 7



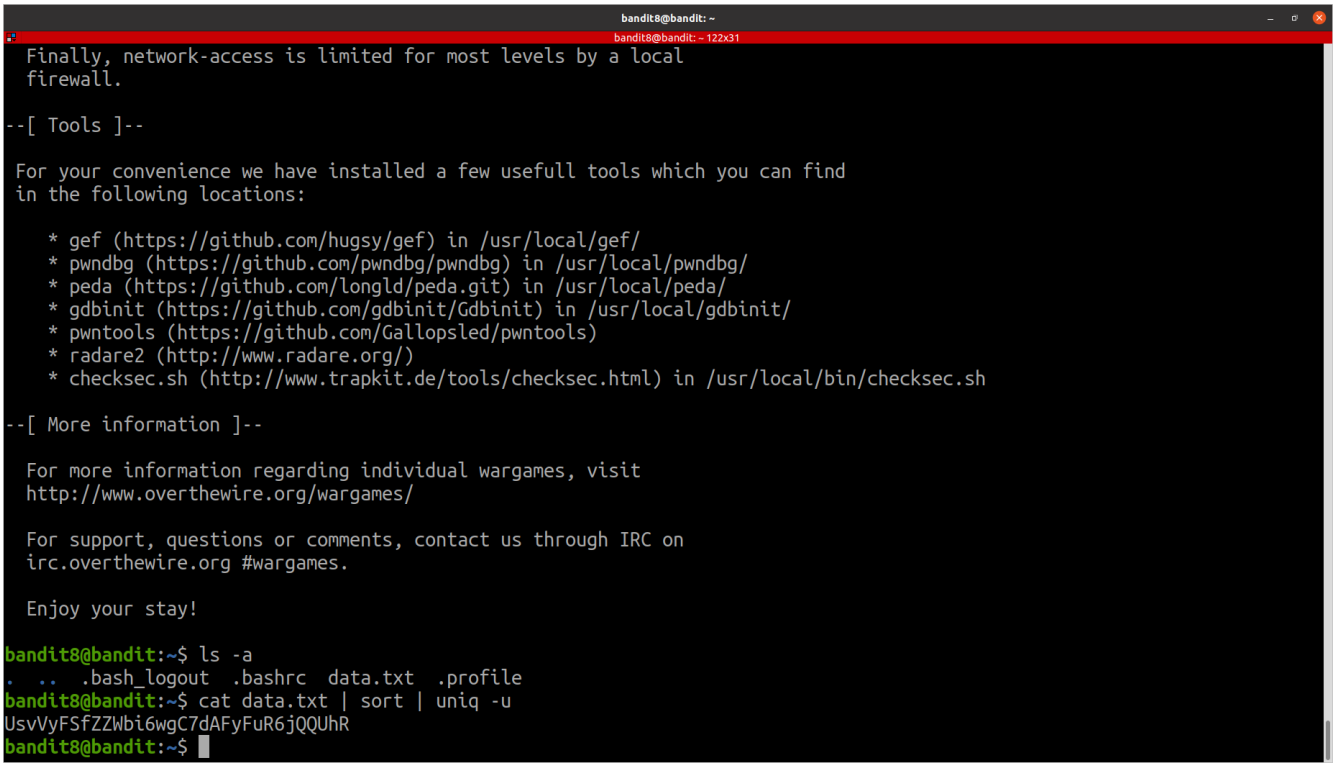
Contraseña obtenida:
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Nivel 7 to 8



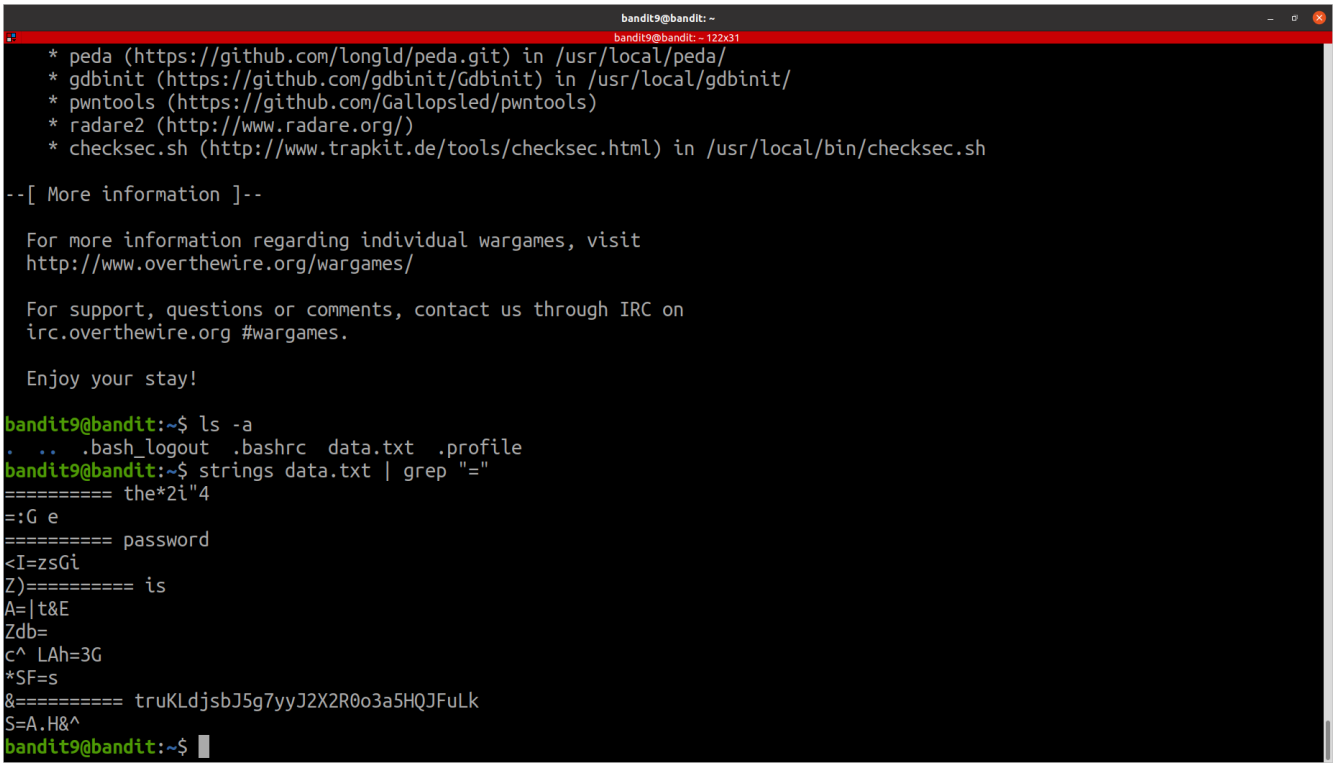
Contraseña obtenida:
cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Nivel 8 to 9



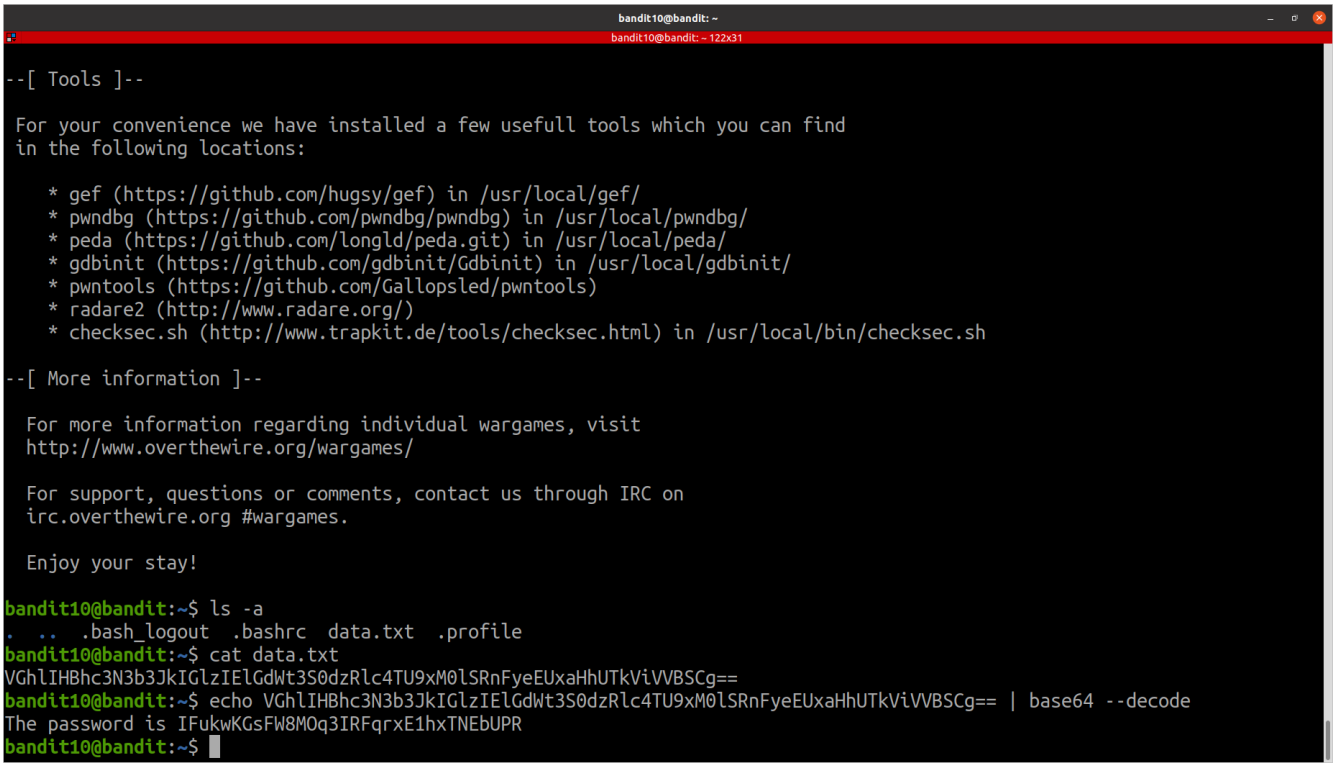
Contraseña obtenida:
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Nivel 9 to 10



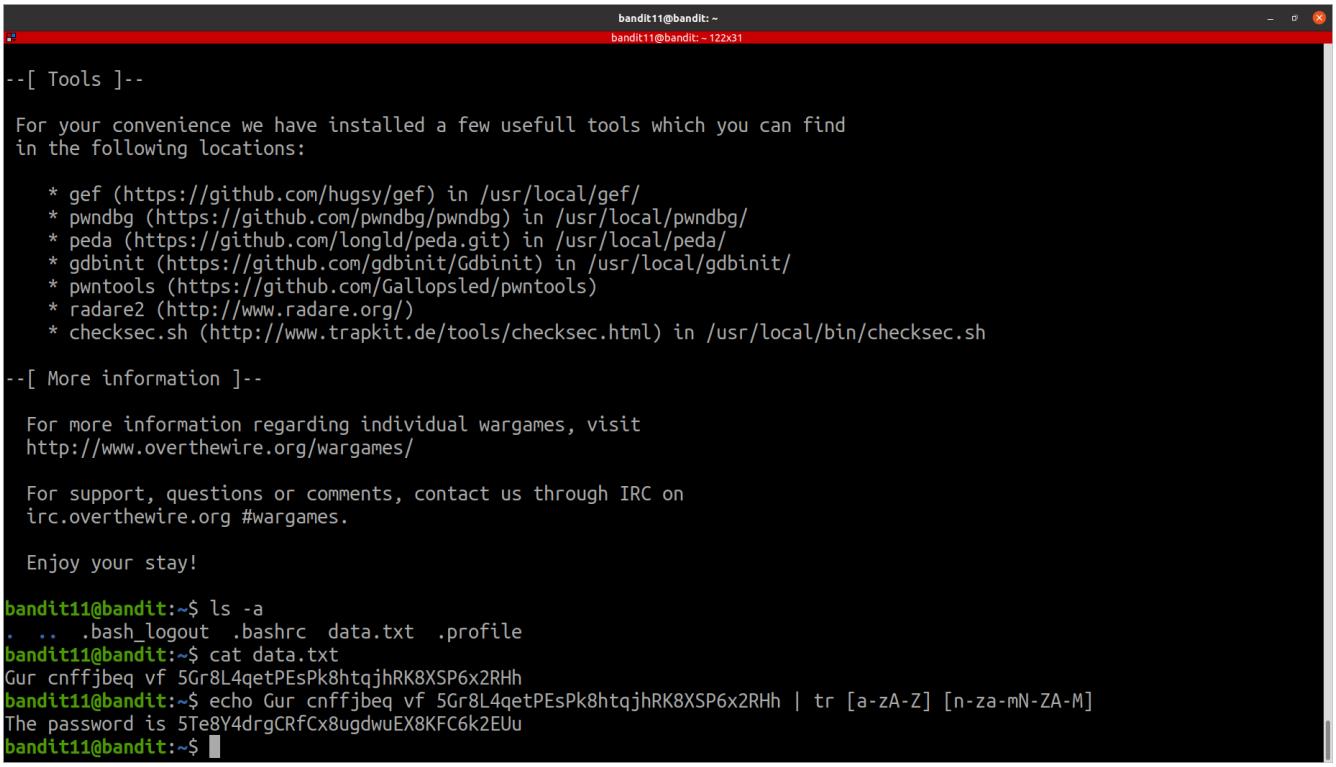
Contraseña obtenida:
truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Nivel 10 to 11



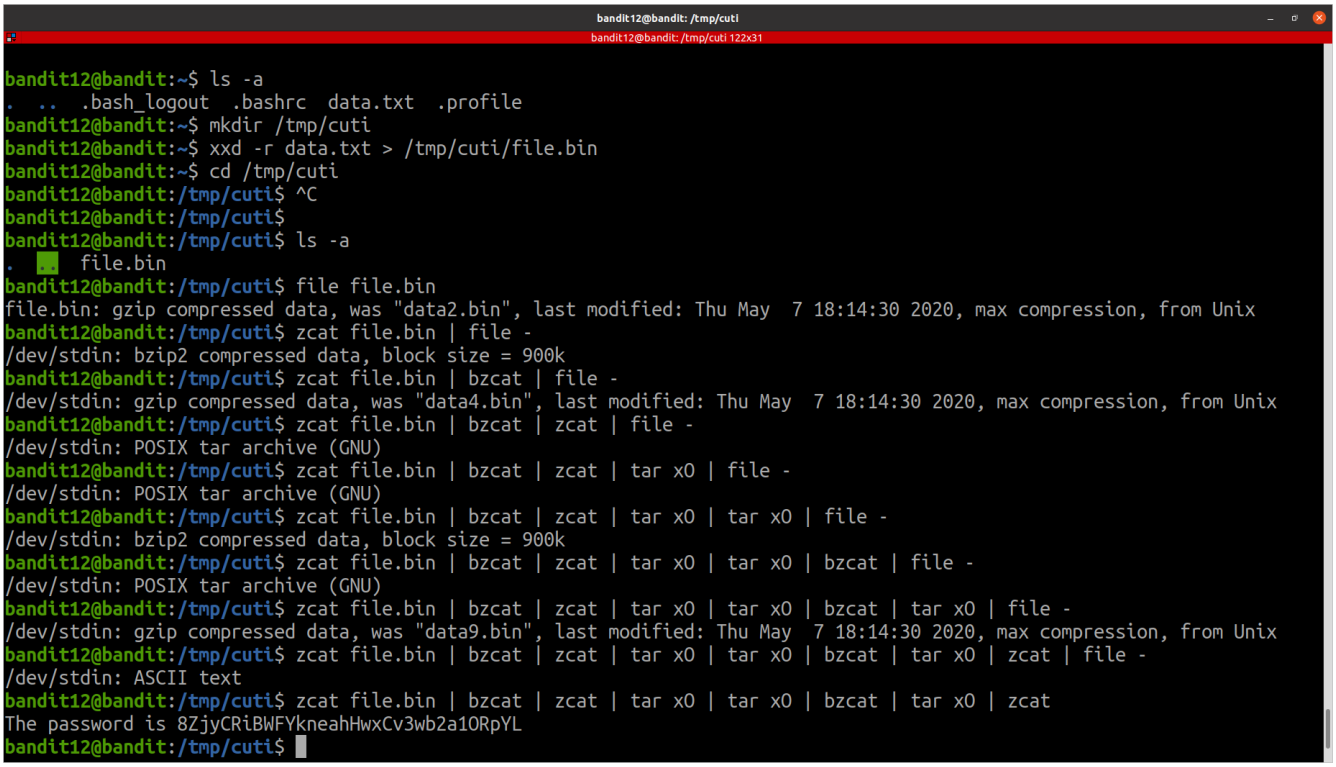
Contraseña obtenida:
IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Nivel 11 to 12



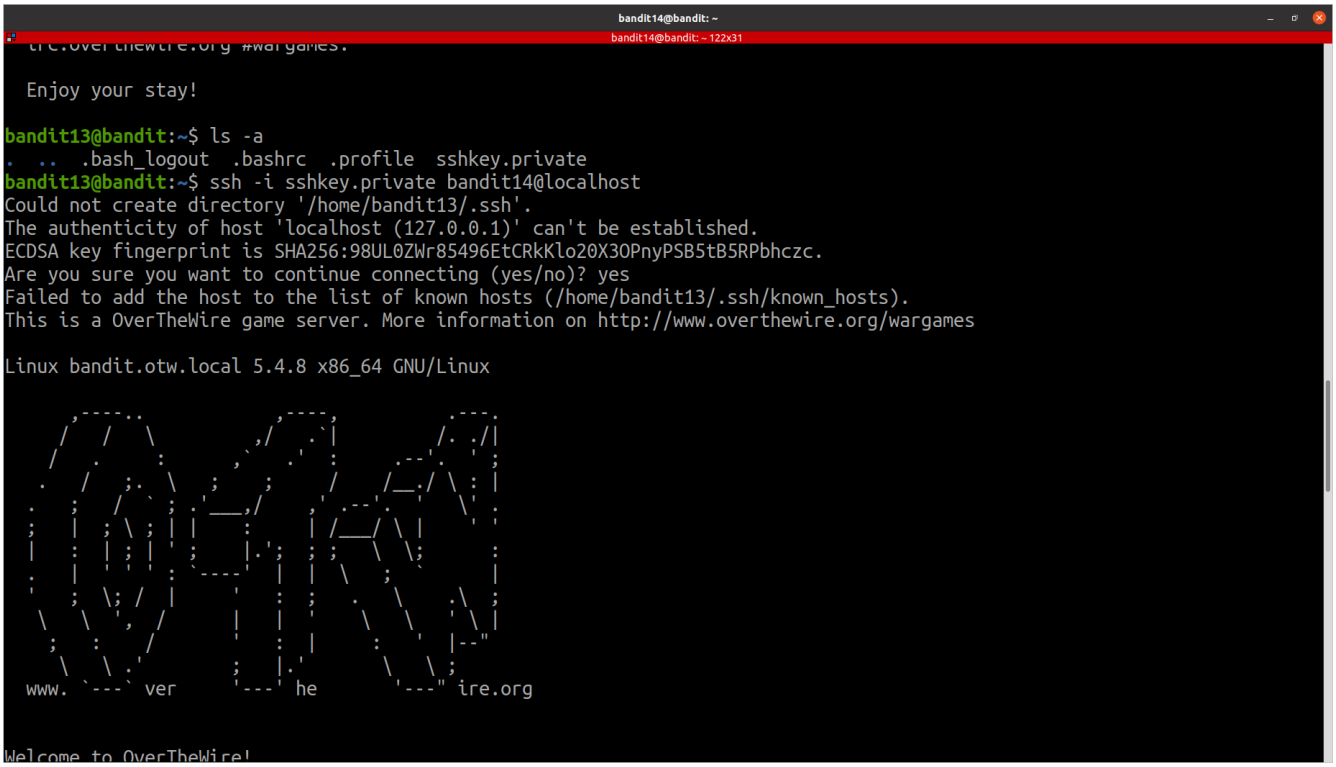
Contraseña obtenida:
5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Nivel 12 to 13



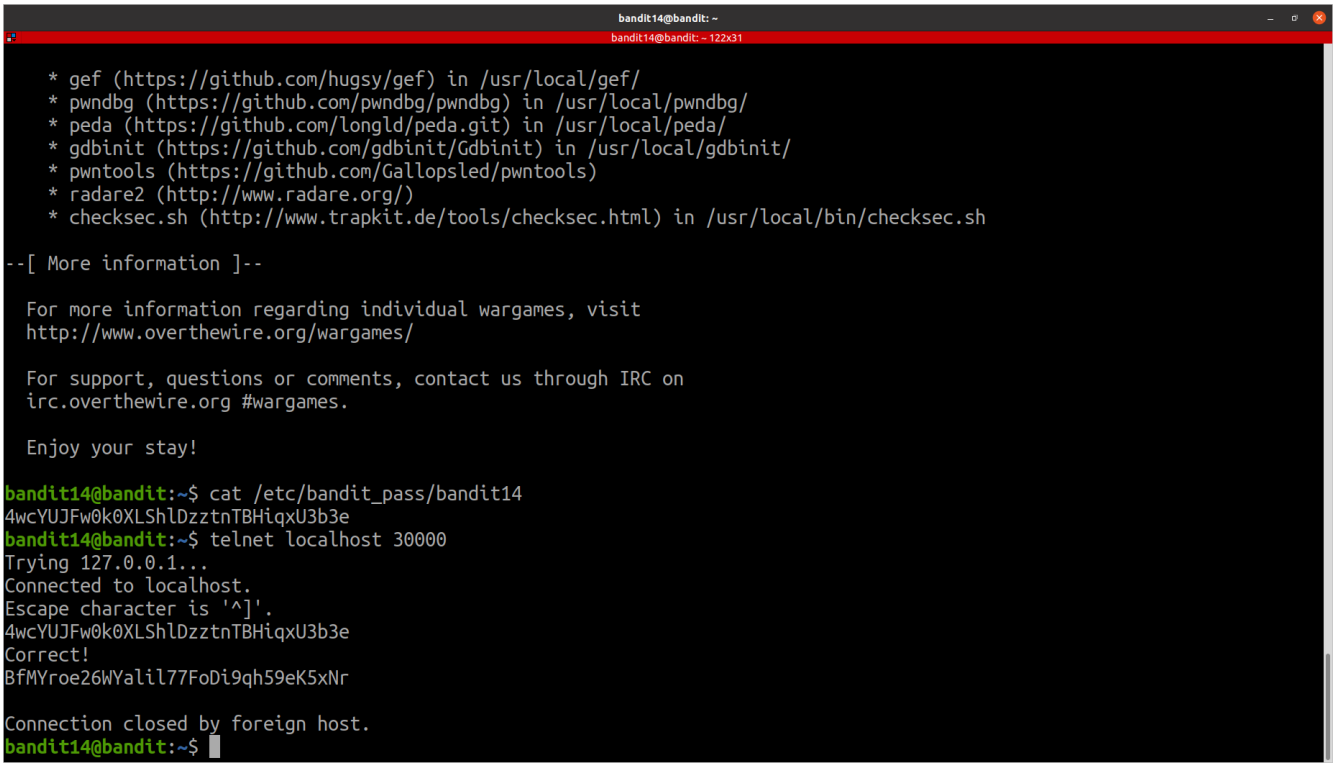
Contraseña obtenida:
8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Nivel 13 to 14



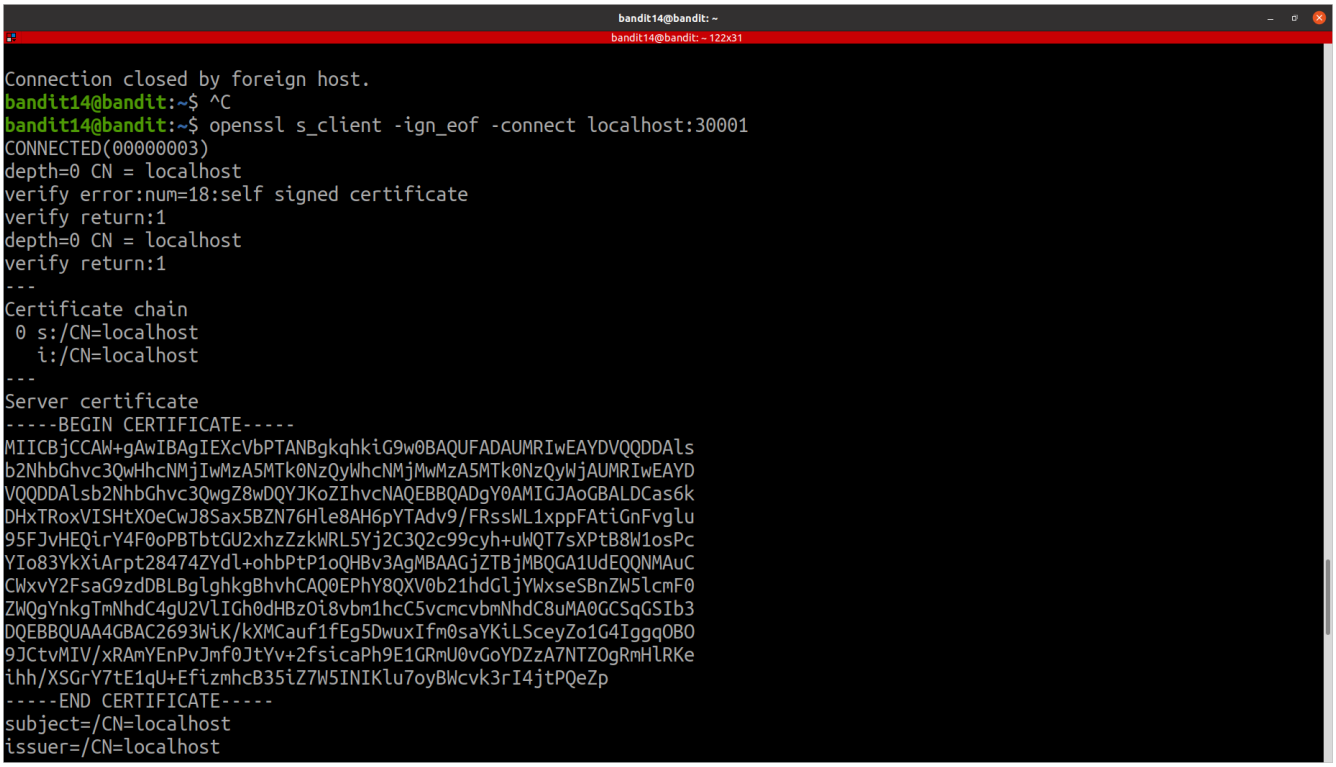
No obtenemos contraseña sino un pase ssh al siguiente nivel.

Nivel 14 to 15



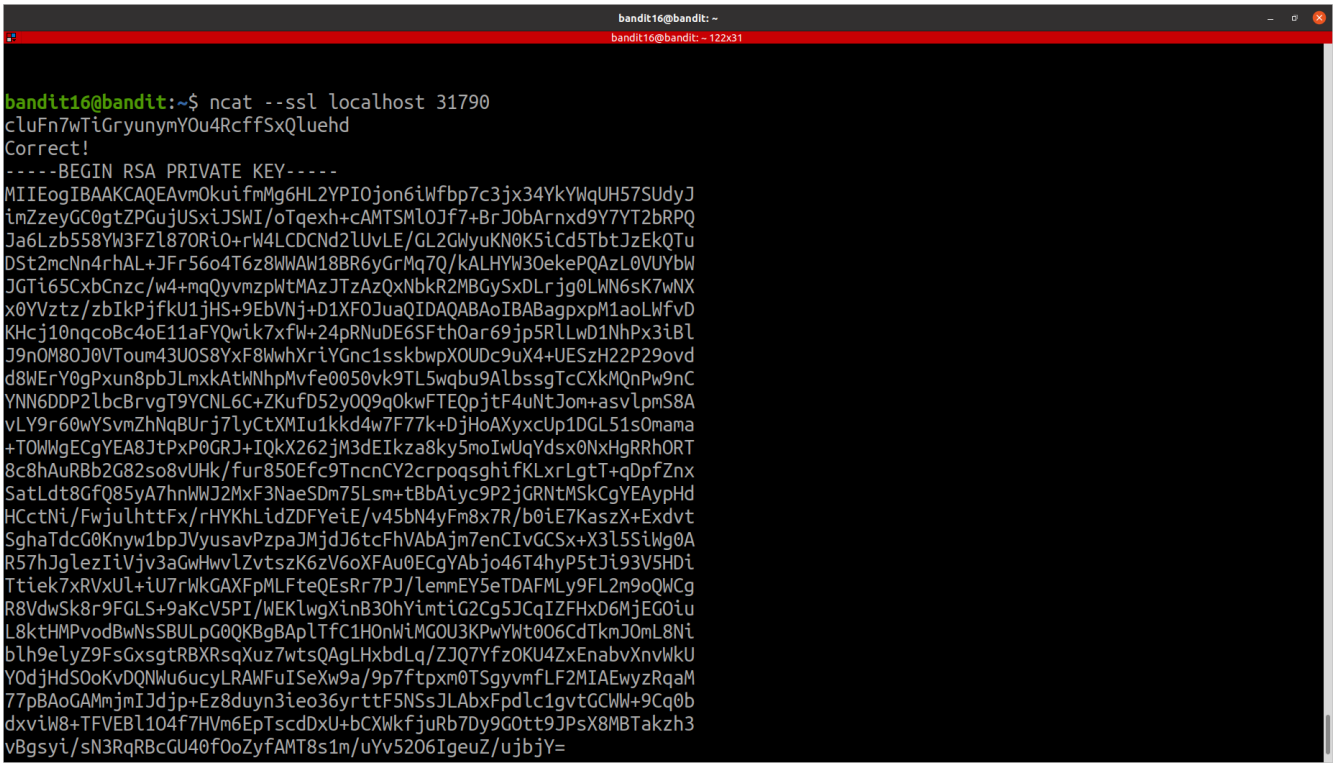
Contraseña obtenida:
BfMYroe26WYalil77FoDi9qh59eK5xNr

Nivel 15 to 16



Contraseña obtenida:
cluFn7wTiGryunymYOu4RcffSxQluehd

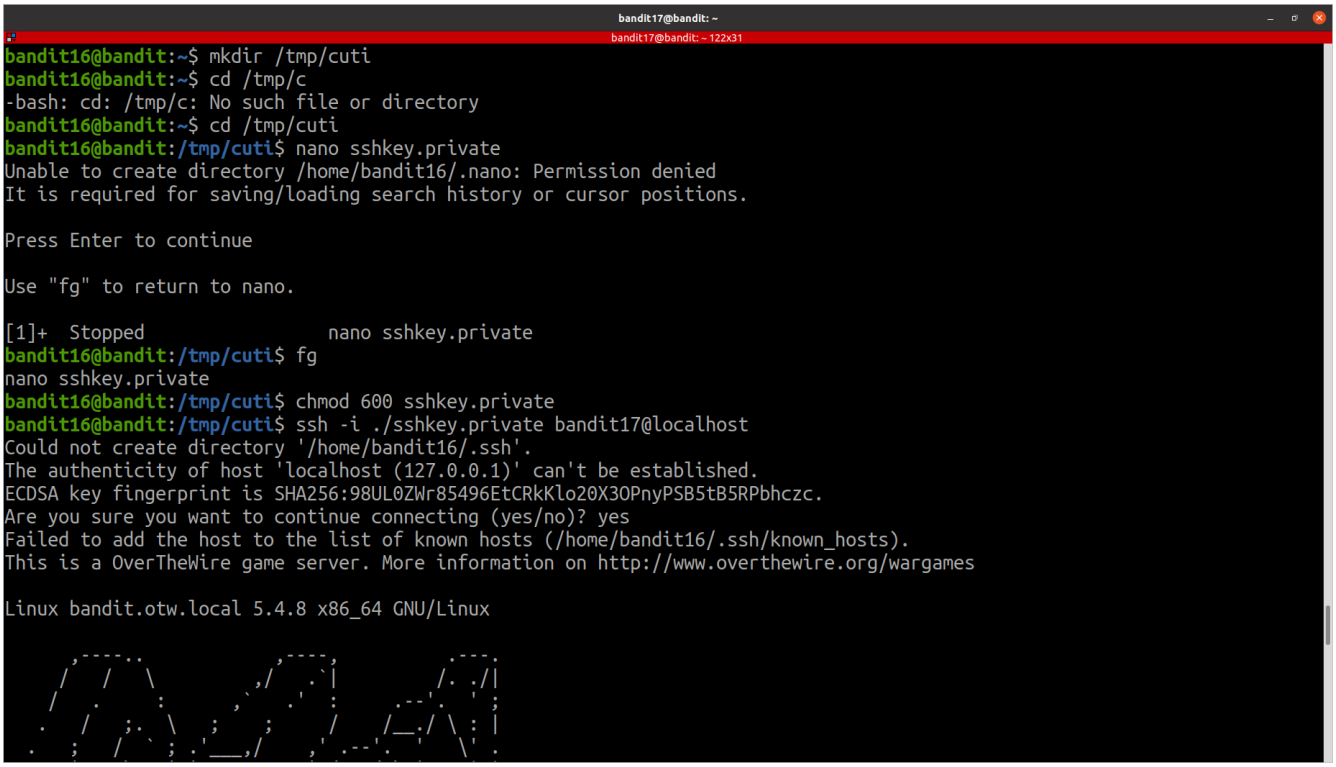
Nivel 16 to 17



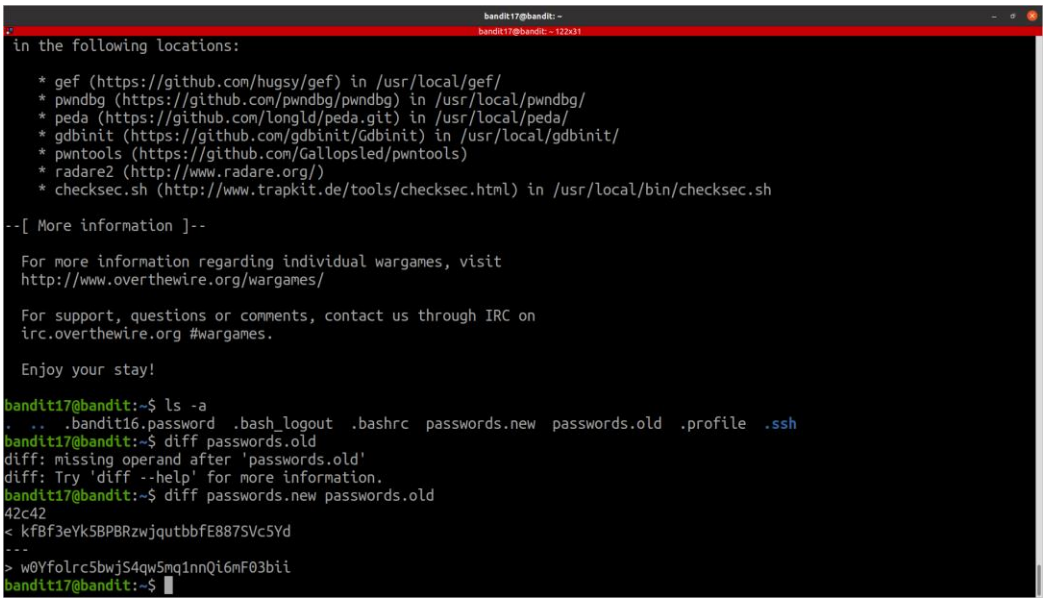
Contraseña obtenida:

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SU
dyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bR
PQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEk
QTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL
0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK
7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfv
D
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iB
l
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22
P29ovd

d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw
9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpm
S8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOma
ma
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgR
RhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEA
ypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0
A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQ
WCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEG
Oiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTk
mJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvW
kU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyz
RqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0
b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTak
zh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

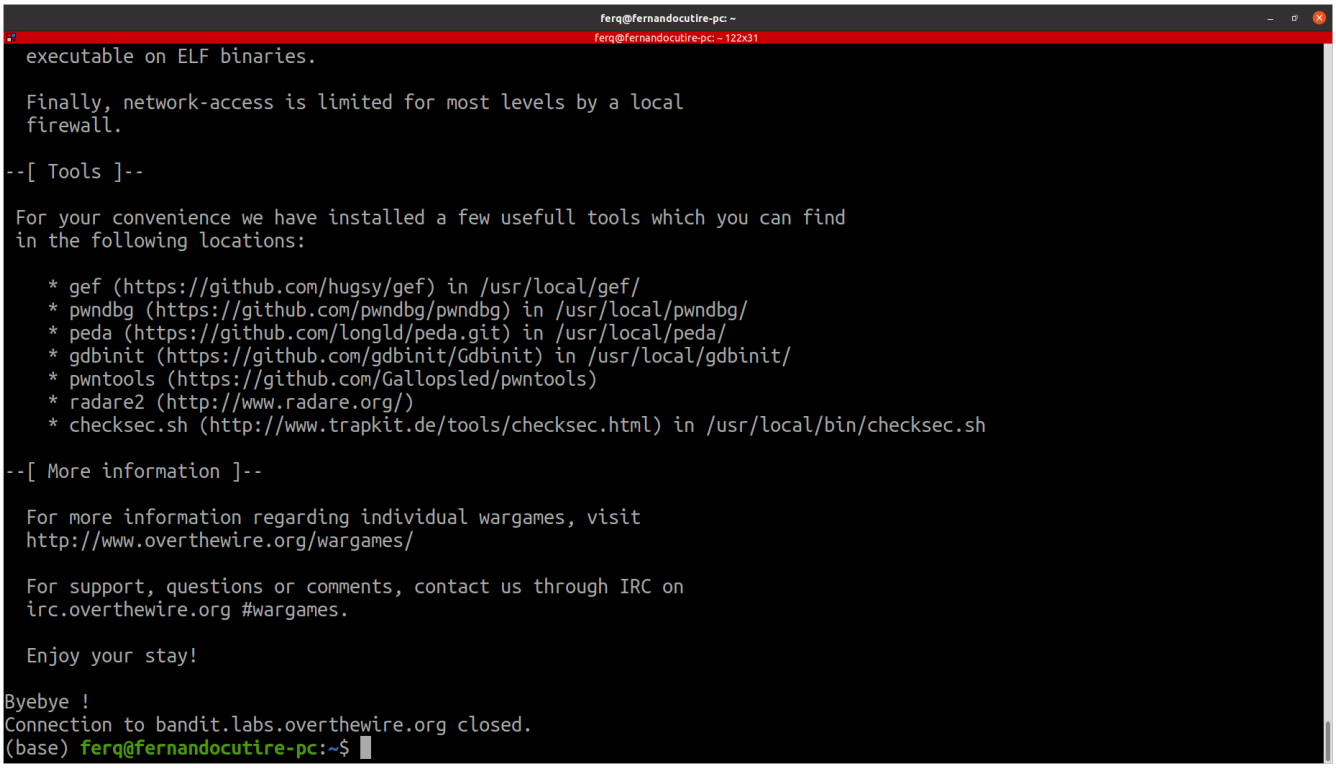


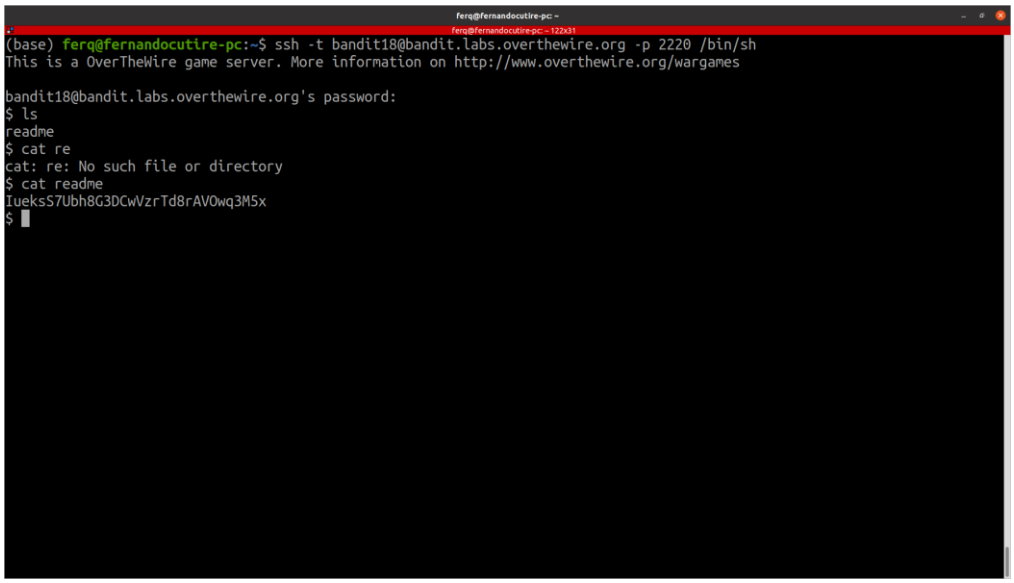
Nivel 17 to 18



Contraseña obtenida:
kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

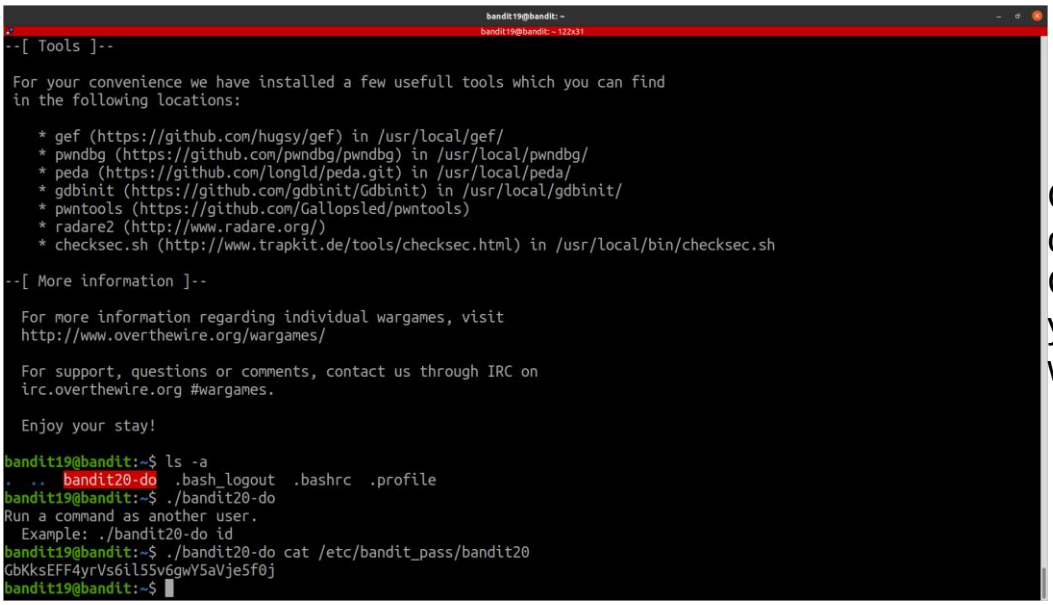
Nivel 18 to 19





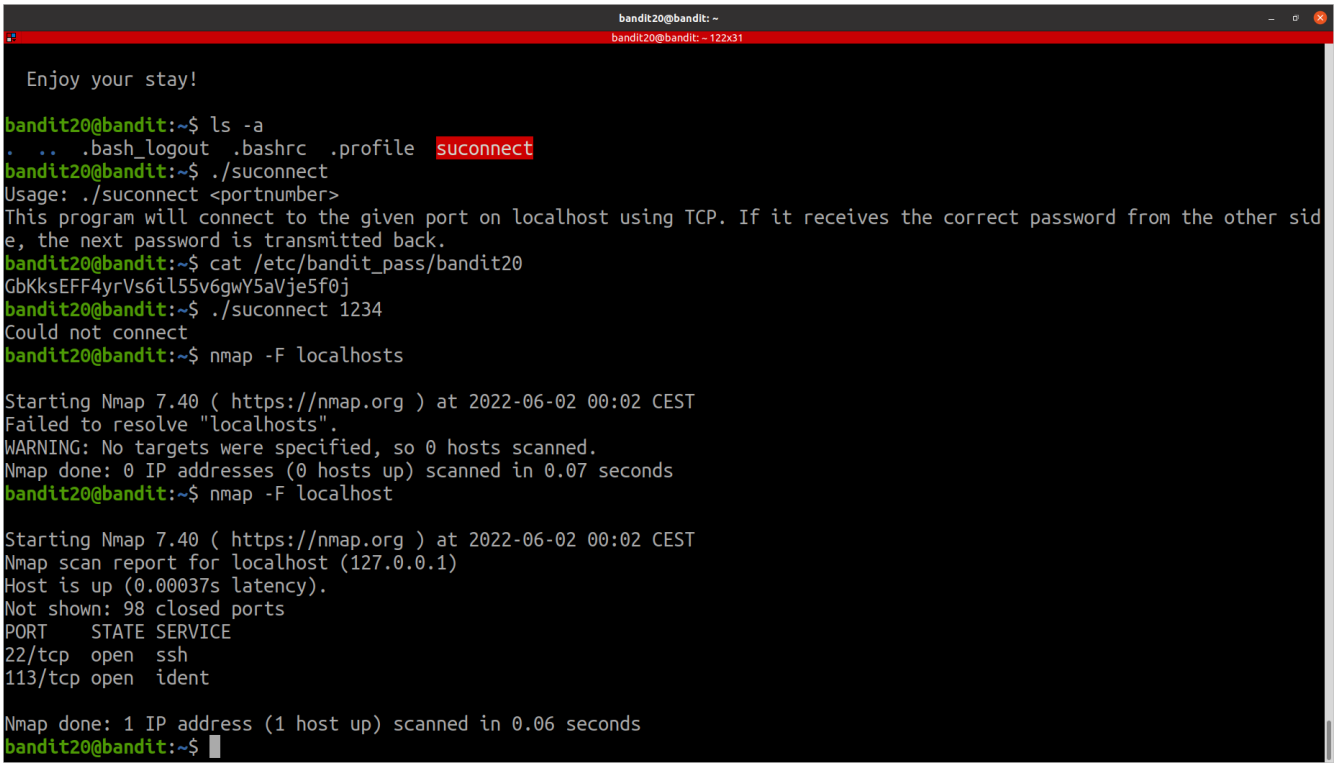
Contraseña obtenida:
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

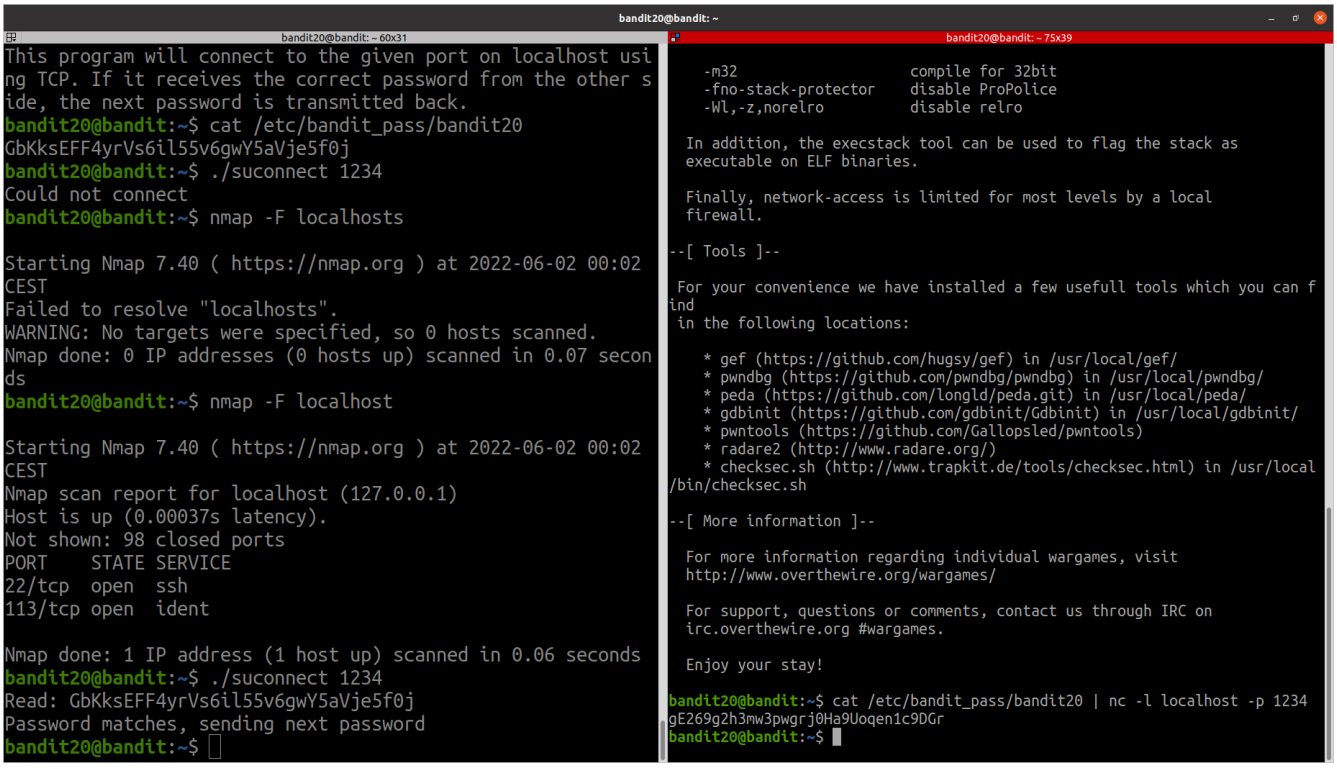
Nivel 19 to 20



Contraseña obtenida:
GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Nivel 20 to 21


bandit20@bandit: ~
bandit20@bandit: ~ 122x31
Enjoy your stay!
bandit20@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile suconnect
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other sid
e, the next password is transmitted back.
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit20@bandit:~$ ./suconnect 1234
Could not connect
bandit20@bandit:~$ nmap -F localhosts
Starting Nmap 7.40 (https://nmap.org) at 2022-06-02 00:02 CEST
Failed to resolve "localhosts".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
bandit20@bandit:~$ nmap -F localhost
Starting Nmap 7.40 (https://nmap.org) at 2022-06-02 00:02 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00037s latency).
Not shown: 98 closed ports
PORT STATE SERVICE
22/tcp open ssh
113/tcp open ident
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
bandit20@bandit:~$


bandit20@bandit: ~
bandit20@bandit: ~ 60x31
This program will connect to the given port on localhost usi
ng TCP. If it receives the correct password from the other s
ide, the next password is transmitted back.
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit20@bandit:~$ ./suconnect 1234
Could not connect
bandit20@bandit:~$ nmap -F localhosts
Starting Nmap 7.40 (https://nmap.org) at 2022-06-02 00:02
CEST
Failed to resolve "localhosts".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 secon
ds
bandit20@bandit:~$ nmap -F localhost
Starting Nmap 7.40 (https://nmap.org) at 2022-06-02 00:02
CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00037s latency).
Not shown: 98 closed ports
PORT STATE SERVICE
22/tcp open ssh
113/tcp open ident
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
bandit20@bandit:~$ ./suconnect 1234
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
bandit20@bandit:~$
bandit20@bandit: ~ 75x39
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
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 usefull tools which you can f
ind
in the following locations:
* gef (https://github.com/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local
/bin/checksec.sh
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
Enjoy your stay!
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost -p 1234
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$

Contraseña obtenida:
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr