

MHKT 4:

users: po
sm
ed

ITCROWD:

ssid: iphone de Jiale
pssword: adsoitcrowd
ID:179.20.10.10
port: 3022

Equip1:

SSID: Equip1
psswd. equip123
IP 192.168.40.84
Port: 3022

po2:

No es pot entrar a la carpeta PO:

```
po2 (jue nov 23) /home > cd P0/  
-bash: cd: P0/: Permisó denegado  
po2 (jue nov 23) /home > █
```

sm2:

```
root@francesco0 (Thu Nov 23):<~># ssh -p 3022 sm2@192.168.40.84  
sm2@192.168.40.84's password:  
Linux ernestA 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64  
-----  
Welcome to the system!  
  
For assistance or support, you can contact the system administrators  
via email: admin@example.com  
  
Thank you for using this system.  
-----  
Last login: Thu Nov 23 08:36:42 2023 from 10.0.2.2
```

Entrar a l'usuari aso:

```
sm2 (jue nov 23) /home/SM > cd ..  
sm2 (jue nov 23) /home > ls  
aso asosh ED lost+found PO SM  
sm2 (jue nov 23) /home > cd PO  
-bash: cd: PO: Permisó denegado  
sm2 (jue nov 23) /home > cd ED  
sm2 (jue nov 23) /home/ED > cd..  
-bash: cd.: orden no encontrada  
sm2 (jue nov 23) /home/ED > cd..  
sm2 (jue nov 23) /home > cd aso  
sm2 (jue nov 23) /home/aso > ls  
apts bin Desktop Documents Downloads jdk-6u45-linux-x64.bin Music Pictures Public Templates Videos  
sm2 (jue nov 23) /home/aso > █
```

Crear directori des de aso:

```

apts bin Desktop Documents Downloads jdk-6u45-linux-x64.bin Music Pictures Public Templates Videos
sm2 (jue nov 23) /home/aso > mkdir file
sm2 (jue nov 23) /home/aso > ls
apts bin Desktop Documents Downloads jdk-6u45-linux-x64.bin Music Pictures Public Templates Videos
sm2 (jue nov 23) /home/aso >

```

Accedir a l'usuari aso:

```

sm2 (jue nov 23) /home/aso > su aso
Contraseña:
su: Fallo de autenticación
sm2 (jue nov 23) /home/aso > su aso
Contraseña:
aso (jue nov 23) ~ > ls
apts bin Desktop Documents Downloads jdk-6u45-linux-x64.bin Music Pictures Public Templates Videos
aso (jue nov 23) ~ > cd ..
aso (jue nov 23) /home > sudo -su
sudo: la opción requiere un argumento -- 'u'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command [arg ...]]
usage: sudo [-ABbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user]
           [VAR=value] [-i | -s] [command [arg ...]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
aso (jue nov 23) /home > sudo su
[sudo] contraseña para aso:
aso is not in the sudoers file.
aso (jue nov 23) /home > cd ..
aso (jue nov 23) / > ls
admin boot etc initrd.img lib lib64 lost+found mnt proc run srv var vmlinuz.old
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
aso (jue nov 23) / >

```

ed:

4ADSO

ssid: 4ADSO

password: 1234567

x ID:179.20.10.10

port: 3022

Equip: Pachanga sin puertas

Usuarios + contraseñas:

User: PO1

Cont: 123

User: SM1

Cont: 123

User: ED1

Cont: 123

User: PO1

Vulnerabilidades:

No hay carpetas que separen los grupos:

```
P01@ (jue nov 23) > :~$ pwd
/home/P01
P01@ (jue nov 23) > :~$ cd ..
P01@ (jue nov 23) > :/home$ ls
aso carrascalm ED2 ED4 ED6 P01 P03 P05 puertasm SM2 SM4 SM6
asosh ED1 ED3 ED5 lost+found P02 P04 P06 SM1 SM3 SM5
```

User: SM1

Vulnerabilidades:

No hay carpetas que separen los grupos:

```
P01@ (jue nov 23) > :~$ pwd
/home/P01
P01@ (jue nov 23) > :~$ cd ..
P01@ (jue nov 23) > :/home$ ls
aso carrascalm ED2 ED4 ED6 P01 P03 P05 puertasm SM2 SM4 SM6
asosh ED1 ED3 ED5 lost+found P02 P04 P06 SM1 SM3 SM5
```

User: ED1

Vulnerabilidades:

No hay carpetas que separen los grupos:

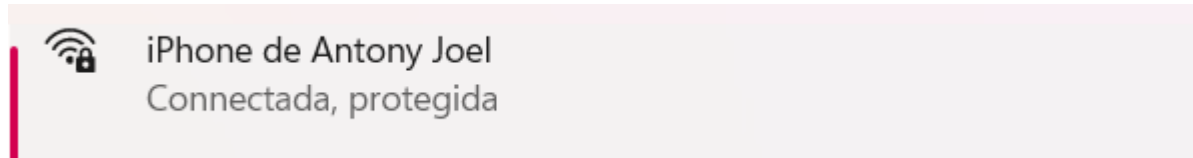
```
P01@ (jue nov 23) > :~$ pwd
/home/P01
P01@ (jue nov 23) > :~$ cd ..
P01@ (jue nov 23) > :/home$ ls
aso carrascalm ED2 ED4 ED6 P01 P03 P05 puertasm SM2 SM4 SM6
asosh ED1 ED3 ED5 lost+found P02 P04 P06 SM1 SM3 SM5
```

NONAMESO:

SSID: Iphone de Anthony Joel

passw:doraemon

IP:172.20.10.4



USER:pro2

CONTRA:pro2

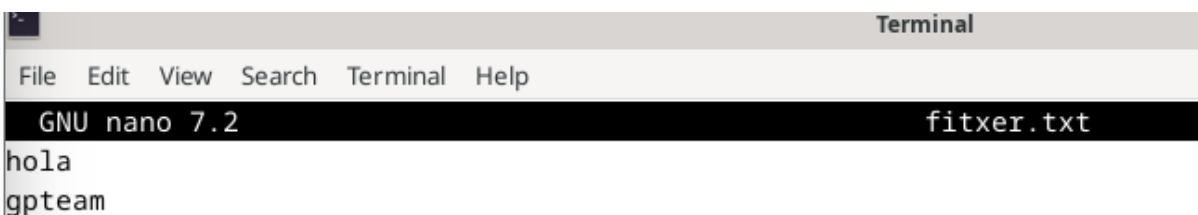
```
Connection to 172.20.10.2 closed.  
root@marionaF (Thu Nov 23):<~># ssh -p 2222 pro2@172.20.10.2  
pro2@172.20.10.2's password:  
Linux michaelZ 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
  
##### Support Contact #####  
# michael.alberto.zerpa@estudiantat.upc.edu #  
# alex.rocamora@estudiantat.upc.edu #  
# antony.joel.bano@estudiantat.upc.edu #  
# massimo.wang@estudiantat.upc.edu #  
# roger.hurtado@estudiantat.upc.edu #  
#####
```

VULNERABILITAT: pro2 entra en altre PRO4

```
pro2@michaelZ (jue nov 23):</home/po>$ cd pro4  
pro2@michaelZ (jue nov 23):</home/po/pro4>$
```

Crear fitxers des de diferents POs:

```
pro2@michaelZ (jue nov 23):</home/po/pro4>$ nano fitxer.txt  
pro2@michaelZ (jue nov 23):</home/po/pro4>$ ls  
fitxer.txt
```



USER:smc2

CONTRA:smc2

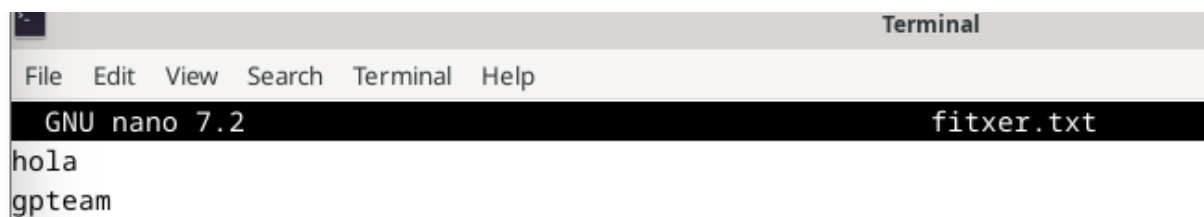
```
root@marionaF (Thu Nov 23):<~># ssh smc2@172.20.10.4
The authenticity of host '172.20.10.4 (172.20.10.4)' can't be established.
ED25519 key fingerprint is SHA256:IxBgEcoC0uaYu4wyjGPh2G0Pv30bUQ/twyEsD6ZwYac.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.10.4' (ED25519) to the list of known hosts.
smc2@172.20.10.4's password:
Linux michaelZ 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

VULNERABILITATS: Crear fitxers en la carpeta smc2

```
smc2@michaelZ (jue nov 23):<~>$ nano fitxer.txt
smc2@michaelZ (jue nov 23):<~>$ ls
fitxer.txt
```



```
Terminal
File Edit View Search Terminal Help
GNU nano 7.2 fitxer.txt
hola
gpteam
```

VULNERABILITAT: des de pro2 no es veu el fitxer que s'ha creat

```
pro2@michaelZ (jue nov 23):<~>$ cd /home/sm/sm2
pro2@michaelZ (jue nov 23):</home/sm/sm2>$ ls
```

USER:ed2

CONTRA: ed2

```
root@marionaF (Thu Nov 23):<~># ssh -p 2222 ed2@172.20.10.2
The authenticity of host '[172.20.10.2]:2222 ([172.20.10.2]:2222)' can't be established.
ED25519 key fingerprint is SHA256:IxBgEcoC0uaYu4wyjGPh2G0Pv30bUQ/twyEsD6ZwYac.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.10.2]:2222' (ED25519) to the list of known hosts.
ed2@172.20.10.2's password:
Linux michaelZ 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

VULNERABILITAT: entra altres userrs ASO ADMIN1 ADMIN2 BACKUPS

```
ed2@michaelZ (jue nov 23):</home>$ ls
admin1  admin2  aso  asosh  backups  ed  lost+found  po  sm
ed2@michaelZ (jue nov 23):</home>$ cd asosh/
-bash: cd: asosh/: Permisó denegado
ed2@michaelZ (jue nov 23):</home>$ cd aso
ed2@michaelZ (jue nov 23):</home/aso>$ ls
Descargas  Documentos  Escritorio  Imágenes  Música  Plantillas  Público  Vídeos
ed2@michaelZ (jue nov 23):</home/aso>$ █

ed2@michaelZ (jue nov 23):</home/aso>$ cd
ed2@michaelZ (jue nov 23):<~>$ cd /home/admin1
ed2@michaelZ (jue nov 23):</home/admin1>$ cd
ed2@michaelZ (jue nov 23):<~>$ cd /home/admin2
ed2@michaelZ (jue nov 23):</home/admin2>$ cd
ed2@michaelZ (jue nov 23):<~>$ cd /home/backups/
ed2@michaelZ (jue nov 23):</home/backups>$ ls
```

Equip: itcrowd

Usuaris + contrasenyes:

User: PO2

Cont: po2

User: SM2

Cont: sm2

User: ED2

Cont: ed2

User: PO2

Vulnerabilitats:

Desde el PO pots entrar a PO4, PO5 i PO6

```
P02 (jueves noviembre 23) >cd P02
P02 (jueves noviembre 23) >ls
P02 (jueves noviembre 23) >cd
P02 (jueves noviembre 23) >cd /home/homeB/P0/P03
-bash: cd: /home/homeB/P0/P03: Permisó denegado
P02 (jueves noviembre 23) >cd /home/homeB/P0/P04
P02 (jueves noviembre 23) >ls
P02 (jueves noviembre 23) >pwd
/home/homeB/P0/P04
P02 (jueves noviembre 23) >
```

```
P02 (jueves noviembre 23) >cd /home/homeB/P0/P05
P02 (jueves noviembre 23) >pwd
/home/homeB/P0/P05
P02 (jueves noviembre 23) >cd /home/homeB/P0/P06
P02 (jueves noviembre 23) >pwd
/home/homeB/P0/P06
P02 (jueves noviembre 23) >|
```

User: SM1

Vulnerabilitats:

User: ED1

Vulnerabilitats:

4DS0:

Vulnerabilitats:

```
SMgpt (Thu Nov 23) > cd /home
SMgpt (Thu Nov 23) > ls
EDgpt EDnname EDsergio P01 P03 P0gpt P0nname P0sergio SM2 SMgpt SMnname SMsergio admin2 backups ilariont oriola samuelj
EDgpt EDnname EDsergio P02 P0equip P0it P0psp SM1 SMequip SMit SMpsp admin1 aso fitxer.txt lost+found paur
SMgpt (Thu Nov 23) > cd P01
-bash: cd: P01: Permission denied
SMgpt (Thu Nov 23) > cd P0nname
SMgpt (Thu Nov 23) >
```

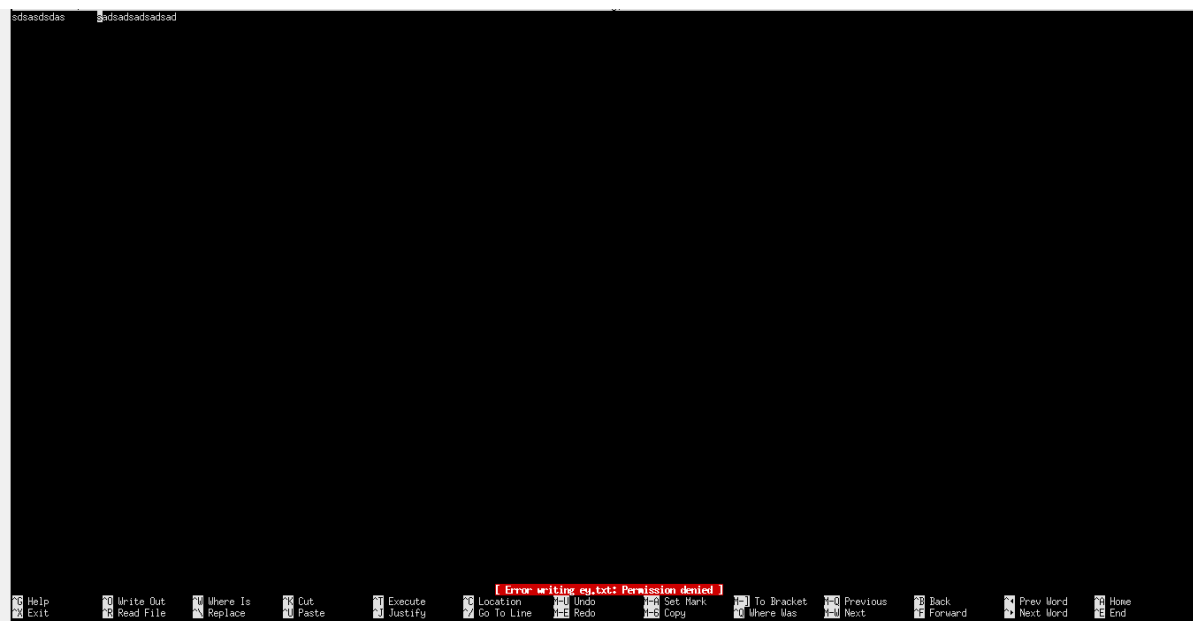
Podem accedir a una carpeta PO(usuari amb jerarquia major) des del nostre usuari SM.

```
SMgpt (Thu Nov 23) > cd P0nname
SMgpt (Thu Nov 23) > ls
EDgpt EDnname EDsergio P01 P03 P0gpt P0nname P0sergio SM2 SMgpt SMnname SMsergio admin2 backups ilariont oriola samuelj
EDgpt EDnname EDsergio P02 P0equip P0it P0psp SM1 SMequip SMit SMpsp admin1 aso fitxer.txt lost+found paur
SMgpt (Thu Nov 23) > cd SMnname
SMgpt (Thu Nov 23) >
```

També podem accedir a carpetes d'usuaris "horitzontals", com SMnname, des de SMgpt.

Hem creat un arxiu key.txt des de SMgpt. Al connectar-nos des de P0gpt, podem veure aquest arxiu, pero al intentar editar-lo veiem que no tenim permisos:

```
P0gpt (Thu Nov 23) > cd SMgpt
P0gpt (Thu Nov 23) > ls
ey.txt
P0gpt (Thu Nov 23) > nano ey.txt
```



[Error writing ey.txt: Permission denied]

De la mateixa manera, podem veure l'arxiu prova.txt de ED des de PO, pero no tenim permisos d'escriptura:

```
POgpt (Thu Nov 23) > cd /home/EDgpt/  
POgpt (Thu Nov 23) > ls  
prova.txt  
POgpt (Thu Nov 23) > nano prova.txt
```

```
[ File 'prova.txt' is unwritable ]  
POgpt (Thu Nov 23) > ^M
```

No podem crear un arxiu a una carpeta de jerarquia inferior, ja que no estan ben definits els permisos (hem intentat crear un arxiu a la carpeta EDgpt des de POgpt):

```
POgpt (Thu Nov 23) > ls  
EDequip  EDit    EDpsp    P01  P03    POgpt  POname  POsergio  SM2    SMgpt  SMname  SMsergio  admin2  backups  fitxer.txt  lost+found  paur  
EDgpt    EDname  EDsergio  P02  P0equip  POit   POpsp    SM1     SMequip  SMit    SMpsp    admin1  aso      ernest     ilariont    oriola      samuelj  
POgpt (Thu Nov 23) > cd EDgpt  
POgpt (Thu Nov 23) > nano arxiuPO
```

```
[ Directory '.' is not writable ]  
POgpt (Thu Nov 23) > ^M
```

Un altre exemple d'això seria usant un copy d'un arxiu.txt de POgpt cap a SMgpt, on veiem que se'ns denega, ja que no tenim permisos d'escriptura.

```
cp: cannot create regular file '/home/SMgpt/prova.txt': Permission denied  
POgpt (Thu Nov 23) > pwd  
/home/POgpt  
POgpt (Thu Nov 23) > cp prova.txt /home/SMgpt  
cp: cannot create regular file '/home/SMgpt/prova.txt': Permission denied  
POgpt (Thu Nov 23) > █
```