

- Identificați, din fișierul /etc/passwd utilizatorii cu nume de persoane și încercați să vă logați în unul dintre conturi (nu toate sunt accesibile) cu comanda su de pe userul aso

```
aso@aso-lab5:~$ cat /etc/passwd | grep -E ":[0-9]{4}:"  
tudor:x:1000:1000:tudor:/home/tudor:/bin/bash  
ionel:x:1001:1001:ionel:/home/ionel:/bin/bash  
costel:x:1002:1002::/home/costel:/bin/sh  
dorel:x:1003:1003::/home/dorel:/bin/sh  
aso:x:1004:1006:aso:/home/aso:/bin/bash  
baba-dochia:x:1005:1007:baba-dochia:/home/baba-dochia:/bin/ba  
admin:x:1006:1008:admin:/home/admin:/bin/bash  
andrei:x:1007:1009:andrei:/home/andrei:/bin/bash  
ana:x:1008:1010:ana:/home/ana:/bin/bash  
alexutzu:x:1009:1011:alexutzu:/home/alexutzu:/bin/bash
```

```
aso@aso-lab5:~$ su ionel  
ionel@aso-lab5:/home/aso$
```

- Unul dintre acești utilizatori deține un folder în /home. Aflați utilizatorul și intrați în folder

```
aso@aso-lab5:~$ ll /home/  
total 24  
drwxr-xr-x  6 root  root   4096 Oct  30  2019 ./  
drwxr-xr-x 24 root  root   4096 Nov  11 07:08 ../  
drwxr-xr-x  2 admin admin   4096 Oct  30  2019 admin/  
drwxr-xr-x  4 aso   aso    4096 Oct  30  2019 aso/  
drwxrwsrwx  6 ionel proiect 4096 Oct  30  2019 ionel/  
drwxr-xr-x  6 tudor tudor   4096 Oct  30  2019 tudor/  
aso@aso-lab5:~$
```

Utilizatorul ionel are un folder in home cu conținutul:

```
aso@aso-lab5:~$ ll /home/ionel  
total 44  
drwxrwsrwx 6 ionel  proiect 4096 Oct  30  2019 ./  
drwxr-xr-x  6 root   root    4096 Oct  30  2019 ../  
-rw----- 1 ionel  ionel    1024 Nov  11 07:10 .bash_history  
-rw-r--r-- 1 ionel  ionel     220 Apr   4  2018 .bash_logout  
-rw-r--r-- 1 ionel  ionel    3771 Apr   4  2018 .bashrc  
drwx----- 3 dorel  proiect 4096 Oct  30  2019 comun/  
drwxrwxr-x  2 costel proiect 4096 Oct  30  2019 costel/  
drw-rw-rw-  2 dorel  proiect 4096 Oct  30  2019 dorel/  
drwxrwxr-x  2 ionel  proiect 4096 Oct  30  2019 ionel/  
-rw-r--r--  1 ionel  ionel     807 Apr   4  2018 .profile  
-rwxrwxrwx  1 ionel  proiect  168 Oct  30  2019 rulare-proiect.sh*
```

3. În acest folder se află un proiect împărțit în 4 fișiere, care se află în subdirectoare. Fișierul ./rulare-proiect.sh asigură buna funcționare a proiectului. Citiți fișierul, înțelegeți ce face și setați permisiunile utilizatorilor corespunzător astfel încât acest script să ruleze.

```
aso@aso-lab5:/home/ionel$ cat rulare-proiect.sh
su -l ionel -c '/home/ionel/comun/ionel/1.sh'
su -l dorel -c '/home/ionel/dorel/2.sh'
su -l costel -c '/home/ionel/costel/3.sh'
su -l ionel -c '/home/ionel/ionel/4.sh'
aso@aso-lab5:/home/ionel$ ll
total 44
drwxrwsrwx 6 ionel  project 4096 Oct 30  2019 .
drwxr-xr-x  6 root   root    4096 Oct 30  2019 ..
-rw-----  1 ionel  ionel   1102 Nov 11 07:36 .bash_history
-rw-r--r--  1 ionel  ionel   220  Apr  4  2018 .bash_logout
-rw-r--r--  1 ionel  ionel   3771 Apr  4  2018 .bashrc
drwx----- 3 dorel  project 4096 Oct 30  2019 comun/
drwxrwxr-x  2 costel project 4096 Oct 30  2019 costel/
drw-rw-rw-  2 dorel  project 4096 Oct 30  2019 dorel/
drwxrwxr-x  2 ionel  project 4096 Oct 30  2019 ionel/
-rw-r--r--  1 ionel  ionel   807  Apr  4  2018 .profile
-rwxrwxrwx  1 ionel  project 168  Oct 30  2019 rulare-proiect.sh*
aso@aso-lab5:/home/ionel$ su ionel
ionel@aso-lab5:~$ chmod +x /home/ionel
ionel@aso-lab5:~$ chmod +x /home/ionel/ionel/
ionel@aso-lab5:~$ chmod +x /home/ionel/ionel/4.sh
ionel@aso-lab5:~$ su dorel
```

Am dat permisiuni de executie la ce am putut pentru ionel, si dupa am incercat pentru dorel:

```
ionel@aso-lab5:~$ su dorel
$ chmod +x /home/ionel/comun
$ cd /home/ionel/comun
$ ls
ionel
$ stat ionel
  File: ionel
  Size: 4096          Blocks: 8          IO Block: 4096   dire
ctory
Device: 802h/2050d      Inode: 532803      Links: 2
Access: (0755/drwxr-xr-x) Uid: ( 1001/    ionel)  Gid: ( 1004/
project)
Access: 2025-11-11 07:27:24.733833534 +0000
Modify: 2019-10-30 07:41:30.384478877 +0000
Change: 2019-10-30 07:41:30.384478877 +0000
 Birth: -
$
```

Am dat permisiuni de executie pentru /home/ionel/comun dar pentru /home/ionel/comun/ionel, trebuie sat rec iar pe ionel

```
ionel@aso-lab5:~$ ls
comun costel dorel ionel rulare-proiect.sh
ionel@aso-lab5:~$ chmod +x /home/ionel/comun/ionel
ionel@aso-lab5:~$ chmod +x /home/ionel/comun/ionel/1.sh
```

Am dat permisiuni de executie si pentru celalalt folder al lui dorel:

```
ionel@aso-lab5:~$ su dorel
$ chmod +x /home/ionel/dorel
$ chmod +x /home/ionel/dorel/2.sh
```

Am dat permisiuni de executie pentru parcurgerea foilederului lui costel, dar trebuie sa ma intorc pe ionel sad au permisiuni de executie si pe fisierul 3.sh deoarece e al lui ionel

```
ionel@aso-lab5:~$ su costel
$ chmod +x /home/ionel/costel
$ chmod +x /home/ionel/costel/3.sh
chmod: changing permissions of '/home/ionel/costel/3.sh': Operation not permitted
$ stat 3.sh
stat: cannot stat '3.sh': No such file or directory
$ ls
comun costel dorel ionel rulare-proiect.sh
$ cd costel
$ ls
3.sh
$ stat 3.sh
  File: 3.sh
  Size: 8          Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 532806      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1001/    ionel)  Gid: ( 1004/
project)
Access: 2019-10-30 07:43:41.525108391 +0000
Modify: 2019-10-30 07:43:41.525108391 +0000
Change: 2019-10-30 07:43:47.389287028 +0000
 Birth: -
$
```

```
ionel@aso-lab5:~$ ls
comun costel dorel ionel rulare-proiect.sh
ionel@aso-lab5:~$ chmod +x /home/ionel/costel/3.sh
ionel@aso-lab5:~$
```

Rularea:

```
aso@aso-lab5:/home/ionel$ ./rulare-proiect.sh
Totul
No directory, logging in with HOME=/
Este
No directory, logging in with HOME=/
In
Regula
```

4. Grupul din care fac parte utilizatorii implicați în proiect conține 5 membri, pe lângă aso. Identificați membrul echipei care nu a făcut nimic.

```
aso@aso-lab5:/home/ionel$ grep proiect /etc/group
proiect:x:1004:ionel,costel,dorel,aso,baba-dochia
```

Membrul echipei care nu a facut nimic este **baba-dochia**

5. Logați-vă din nou cu user-ul aso și mergeți în directorul acestuia (/home/aso)

```
aso@aso-lab5:/home/ionel$ cd /home/aso
aso@aso-lab5:~$
```

6. În mod normal, pe un server securizat, fișierul /etc/shadow nu poate fi citit de către utilizatorii normali. Listați conținutul acestuia și observați linia unde se află user-ul admin. Identificați utilizatorii fără parolă.

```
uucp:*:18113:0:99999:7:::  
proxy:*:18113:0:99999:7:::  
www-data:*:18113:0:99999:7:::  
backup:*:18113:0:99999:7:::  
list:*:18113:0:99999:7:::  
irc:*:18113:0:99999:7:::  
gnats:*:18113:0:99999:7:::  
nobody:*:18113:0:99999:7:::  
systemd-network:*:18113:0:99999:7:::  
systemd-resolve:*:18113:0:99999:7:::  
syslog:*:18113:0:99999:7:::  
messagebus:*:18113:0:99999:7:::  
_apt:*:18113:0:99999:7:::  
lxd:*:18113:0:99999:7:::  
uuidd:*:18113:0:99999:7:::  
dnsmasq:*:18113:0:99999:7:::  
landscape:*:18113:0:99999:7:::  
pollinate:*:18113:0:99999:7:::  
sshd:*:18191:0:99999:7:::  
tudor:$6$J7fBY3.X$QK.iAvENeC2CUwEs3ZOMg87i1jijjBgxmLT4x1woErTNe2  
PYg.Wxk740ltvMfij.CffhkFwGEy.hjzpGBLEJA/:18199:0:99999:7:::  
ionel!:18199:0:99999:7:::  
costel!:18199:0:99999:7:::  
dorel!:18199:0:99999:7:::  
aso:$1$kaefQVdK$mztc9z0umJGTJAYQ0slsK.:18199:0:99999:7:::  
baba-dochia:$1$K4EfhgzY$G4plr1a.hNyU/beoiHx1R/:18199:0:99999:7:::  
:  
admin:$1$a$44cUw6Nm5bX0muHWNIwub0:18199:0:99999:7::: ←  
andrei:$1$VRfc/QMD$PNqFJ5kR3xuCRWnUixXTM.:18199:0:99999:7:::  
ana:$1$uGPrd4CI$WDvV3aS0fr/vKFFz8PLY61:18199:0:99999:7:::  
alexutzu:$1$Aqr12q/1$QMT3javrtT4/ZroQ1/gcf1:18199:0:99999:7:::  
aso@aso-lab5:~$
```

Utilizatorii fără parola:

```
aso@aso-lab5:~$ cat /etc/shadow | grep -E ":[!]:"  
ionel!:18199:0:99999:7:::  
costel!:18199:0:99999:7:::  
dorel!:18199:0:99999:7:::  
aso@aso-lab5:~$
```

7. Copiați user-ul și hash-ul parolei user-ului admin într-un fișier din directorul /home/aso.

```
aso@aso-lab5:~$ grep admin /etc/shadow > /home/aso/admin_hash.txt
aso@aso-lab5:~$ ls
admin_hash.txt
aso@aso-lab5:~$ cat admin_hash.txt
admin:$1$a$44cUw6Nm5bX0muHwNIwub0:18199:0:99999:7:::
aso@aso-lab5:~$ |
```

8. Examinați ce fel de hash este acesta și salt-ul său.

Salt-ul e cel subliniat cu rosu:

```
aso@aso-lab5:~$ grep admin /etc/shadow > /home/aso/admin_hash.txt
aso@aso-lab5:~$ ls
admin_hash.txt
aso@aso-lab5:~$ cat admin_hash.txt
admin:$1$a$44cUw6Nm5bX0muHwNIwub0:18199:0:99999:7:::
aso@aso-lab5:~$ |
```

\$1\$ inseamna ca hash-ul e MD5

9. Utilizând utilitarul john spargeți parola adminului și logați-vă cu parola obținută.

```
aso@aso-lab5:~$ john /home/aso/admin_hash.txt
Created directory: /home/aso/.john
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
a          (admin)
1g 0:00:00:00 100% 2/3 2.564g/s 15969p/s 15969c/s 15969C/s a..ne
tware
Use the "--show" option to display all of the cracked passwords
reliably
Session completed
aso@aso-lab5:~$ john --show /home/aso/admin_hash.txt
admin:a:18199:0:99999:7:::

1 password hash cracked, 0 left
aso@aso-lab5:~$ su admin
Password:
To run a command as administrator (user "root"), use "sudo <comm
and>".
See "man sudo_root" for details.

admin@aso-lab5:/home/aso$
```

10. Creați și adăugați utilizatorul Gerogică cu parola "euchiarfactreaba" în grupul proiectului și scoateți utilizatorul descoperit la cerința 4.

Am create user-ul Gerogica:

```
admin@aso-lab5:/home/aso$ sudo useradd -c "Georgica" -m -d /home/Georgica -s /bin/bash -p $(openssl passwd -1 -salt 146 euchiarfactreaba) Georgica
admin@aso-lab5:/home/aso$ cat /etc/shadow | grep Georgica
Georgica:$1$146$87xyPiTU7jmhbOUeg1Qha0:20403:0:99999:7:::
admin@aso-lab5:/home/aso$ su Georgica
Password:
Georgica@aso-lab5:/home/aso$ ls
admin_hash.txt
Georgica@aso-lab5:/home/aso$
```

L-am adaugat in grup:

```
admin@aso-lab5:/home/aso$ sudo usermod -a -G proiect Georgica
admin@aso-lab5:/home/aso$ cat /etc/group | grep proiect
proiect:x:1004:ionel,costel,dorel,aso,baba-dochia,Georgica
admin@aso-lab5:/home/aso$
```

Am sters utilizatorul baba-dochia:

```
admin@aso-lab5:/home/aso$ sudo gpasswd -d baba-dochia proiect
Removing user baba-dochia from group proiect
admin@aso-lab5:/home/aso$ cat /etc/group | grep proiect
proiect:x:1004:ionel,costel,dorel,aso,Georgica
admin@aso-lab5:/home/aso$
```

11. Setați shell-ul utilizatorului de la cerința 4 la /bin/false și încercați să intrați cu su în el de pe un utilizator al grupului proiectului. Ce se întâmplă?

Am aflat mai intai parola:

```
aso@aso-lab5:~$ grep baba-dochia /etc/shadow > /home/aso/baba_hash.txt
aso@aso-lab5:~$ cat baba_hash.txt
baba-dochia:$1$K4EfhgzY$G4plrla.hNyU/beoiHx1R/:18199:0:99999:7::
:
aso@aso-lab5:~$ john /home/aso/baba_hash.txt
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
hahaha          (baba-dochia)
1g 0:00:00:00 100% 2/3 1.086g/s 16288p/s 16288c/s 16288C/s hahah
a..poop
Use the "--show" option to display all of the cracked passwords
reliably
Session completed
aso@aso-lab5:~$ john --show /home/aso/admin_hash.txt
admin:a:18199:0:99999:7:::

1 password hash cracked, 0 left
aso@aso-lab5:~$ john --show /home/aso/baba_hash.txt
baba-dochia:hahaha:18199:0:99999:7:::

1 password hash cracked, 0 left
aso@aso-lab5:~$
```

Am setat shell-ul ca /bin/false, iar acum cand incerc sa ma conectez ma deconecteaza instant:

```
admin@aso-lab5:/home/aso$ sudo usermod -s /bin/false baba-dochia
admin@aso-lab5:/home/aso$ su baba-dochia
Password:
admin@aso-lab5:/home/aso$
admin@aso-lab5:/home/aso$
```

```
aso@aso-lab5:~$ su ionel
ionel@aso-lab5:/home/aso$ su baba-dochia
Password:
ionel@aso-lab5:/home/aso$
```

12. Urmăriți în /home permisiunile directoarelor și identificați o anomalie printre acestea. Explicați ce face și testați comportamentul.

```
aso@aso-lab5:~$ ll /home
total 28
drwxr-xr-x 7 root      root      4096 Nov 11 08:29 .
drwxr-xr-x 24 root     root      4096 Nov 11 07:08 ..
drwxr-xr-x 2 admin    admin      4096 Nov 11 08:39 admin/
drwxr-xr-x 5 aso       aso       4096 Nov 11 08:39 aso/
drwxr-xr-x 2 Georgica Georgica 4096 Nov 11 08:30 Georgica/
drwxrwsrwx 6 ionel    project   4096 Oct 30 2019 ionel/
drwxr-xr-x 6 tudor   tudor     4096 Oct 30 2019 tudor/
aso@aso-lab5:~$
```

Acel semnifica că tot ce e create (fisier/director) în folderul ionel va avea automat grupul project.

```
aso@aso-lab5:/home/ionel$ touch test.txt
aso@aso-lab5:/home/ionel$ ll
total 44
drwxrwsrwx 6 ionel  project 4096 Nov 11 08:48 .
drwxr-xr-x 7 root   root    4096 Nov 11 08:29 ..
-rw----- 1 ionel  ionel   1737 Nov 11 08:45 .bash_history
-rw-r--r-- 1 ionel  ionel   220 Apr  4 2018 .bash_logout
-rw-r--r-- 1 ionel  ionel  3771 Apr  4 2018 .bashrc
drwx--x--x 3 dorel  project 4096 Oct 30 2019 comun/
drwxrwxr-x 2 costel project 4096 Oct 30 2019 costel/
drwxrwxrwx 2 dorel  project 4096 Oct 30 2019 dorel/
drwxrwxr-x 2 ionel  project 4096 Oct 30 2019 ionel/
-rw-r--r-- 1 ionel  ionel   807 Apr  4 2018 .profile
-rwxrwxrwx 1 ionel  project  168 Oct 30 2019 rulare-project.sh*
-rw-rw-r-- 1 aso    project    0 Nov 11 08:48 test.txt
aso@aso-lab5:/home/ionel$ |
```

13. Schimbați parola adminului astfel încat să nu mai poată fi spartă ușor
Am pus parola admin1234

```
admin@aso-lab5:/home/ionel$ passwd
Changing password for admin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
You must choose a longer password
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
admin@aso-lab5:/home/ionel$
```

14. Securizați fișierul /etc/shadow pentru a nu fi citit de către utilizatori malicioși

```
admin@aso-lab5:/home/ionel$ ll /etc/shadow
-rw-r--r-- 1 root shadow 1498 Nov 11 08:59 /etc/shadow
admin@aso-lab5:/home/ionel$ sudo chmod 400 /etc/shadow
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
admin@aso-lab5:/home/ionel$ ll /etc/shadow
-r----- 1 root shadow 1498 Nov 11 08:59 /etc/shadow
admin@aso-lab5:/home/ionel$
```

Bonus: Faceti astfel incat ./rulare_proiect.sh sa afiseze doar ce trebuie.

```
aso@aso-lab5:/home/ionel$ cat rulare-proiect.sh
su ionel -c '/home/ionel/comun/ionel/1.sh'
su dorel -c '/home/ionel/dorel/2.sh'
su costel -c '/home/ionel/costel/3.sh'
su ionel -c '/home/ionel/ionel/4.sh'
aso@aso-lab5:/home/ionel$ ./rulare-proiect.sh
Total
Este
In
Regula
aso@aso-lab5:/home/ionel$
```