



# Sigurnost računala i podataka (Lab 6)

## Lab 6 - Linux permissions and ACLs

### A. Kreiranje novog korisničkog računa

U Linux-u svaka datoteka ili program ima vlasnika. Svakom korisniku pridjeljen je jedinstveni identifikator *User ID*. Svaki korisnik mora pripadati barem jednoj grupi, pri čemu više korisnika može dijeliti istu grupu. Linux grupe također imaju jedinstvene identifikatore *Group ID*.

Isprobali smo naredbu `id`.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ id
uid=1000(student) gid=1000(student) groups=1000(student),4(adm),20(dialog),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46
```

Napravili smo novi korisnički račun pomoću naredbe: `sudo adduser alice`

Logirali smo se kao Alice i dobili informacije o identifikatoru i grupama kojim pripada.

Potom smo kreirali još jedan korisnički račun Bob.

### B. Standardna prava pristupa datotekama

Ulogirali smo se kao Alice, napravili novi direktorij `srp` te u njemu datoteku `security.txt`.

Koristili smo naredbu `getfacl`.

```
alice@DESKTOP-7Q0BASR:~$ getfacl srp
file: srp
owner: alice
group: alice
user::rwx
group::rwx
other::r-x
```

Iako smo vlasnik oduzeli smo si pravo čitanja dokumenta i pokušali ga pročitati.

```
alice@DESKTOP-7Q0BASR:~/srp$ chmod u-r security.txt
alice@DESKTOP-7Q0BASR:~/srp$ cat security.txt
cat: security.txt: Permission denied
```

Oduzeli smo i pravo pristupa datoteci.

```
alice@DESKTOP-7Q0BASR:~$ chmod u-x srp
alice@DESKTOP-7Q0BASR:~$ ls -l
total 4
drw-rwxr-x 2 alice alice 4096 Jan 10 13:17 srp
```

```
alice@DESKTOP-7Q0BASR:~$ cat srp/security.txt
cat: srp/security.txt: Permission denied
```

Prijavili smo se kao Bob i mogli smo pročitati sadržaj jer Bob spada pod others, a oni imaju pravo na to. Oduzeli smo mu pravo pristupa pa ga opet vratili tako što smo ga dodali u grupu koja za to ima pravo.

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ sudo usermod -aG alice bob
```

Izašli smo i opet se prijavili kao Bob da provjerimo može li pristupiti dokumentu.

```
bob@DESKTOP-7Q0BASR:~$ cat /home/alice/srp/security.txt
Hello world
```

Bob pokušava pročitati sadržaj datoteke `/etc/shadow` u koju Linux pohranjuje *hash* vrijednosti korisničkih zaporki, ali on nema prava za to.

```
bob@DESKTOP-7Q0BASR:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Dali smo mu ovlasti kao u prethodnom zadatku pa je na kraju mogao pročitati.

## C. Kontrola pristupa korištenjem *Access Control Lists (ACL)*

U prethodnom zadatku pristup sadržaju smo omogućili dodavanjem novog korisnika u grupu koja je vlasnik predmetne datoteke. Korištenjem ACL, ovo možemo jednostavnije riješiti tako da u ACL datoteke `security.txt` dodamo novog korisnika sa `(r)ead` ovlastima.

Dodali smo Boba u ACL listu s dopuštenjem za čitanje.

```
student@DESKTOP-7Q0BASR:/home/alice/srp$ sudo setfacl -m u:bob:r security.txt
```

Bob nakon te naredbe može pročitati dokument.

```
bob@DESKTOP-7Q0BASR:~$ cat /home/alice/srp/security.txt
Hello world
```

## D. Linux procesi i kontrola pristupa

U tekućem direktoriju smo kreirali Python skriptu sljedećeg sadržaja:

```
import os

print('Real (R), effective (E) and saved (S) UIDs:')
print(os.getresuid())

with open('/home/alice/srp/security.txt', 'r') as f:
    print(f.read())
```

Kada se to izvrši vidimo da svi imaju različit ID, Bob=1003, student:1000..