Lab 6

Šesta laboratorijska vježba se bavi osnovnim postupcima upravljanja korisničkim računima na Linux OS-u s naglaskom na kontrolu pristupa datotekama i sl.

Zadatak a

Treba kreirati dva nova korisnička računa: alice2 i bob2.

Provjeravamo pripadamo li **sudo** grupi koja ima ovlasti kreiranja novih korisnika.

Provjeru vršimo naredbom groups.

Dodajemo nove korisnike:

```
sudo adduser alice2
sudo adduser bob2
```

Prijavljujemo se na korisnički račun:

```
su - alice2
```

Zadatak b

Zadatak je prijaviti se u alice2 ili bob2, napraviti novi direktorij i unutar njega pohraniti security.txt

Naredba **getfacl** daje informacije o direktoriju i dopuštenja nad njim:

```
user::rwx     read-vidimo sadržaj
group::rwx    write-dodajemo sadržaj
other::r-x    execute-ulazak u direktorij
```

Diskrecijska kontrola pristupa jer korisnik ima mogućnost oduzimanja ili davanja prava pristupa.

Ako pristupimo security.txt (vlasnika alice2), kao bob2, pristup je **odbijen**.

Boba2 trebamo dodati u grupu alice, jer oni imaju mogućnost čitanja security.txt.

Nakon ponovne prijave, bob2 će moći pristupiti.

Zadatak c

Moramo maknuti bob2 iz grupe alice.

Želimo demonstrirati kontrolu pristupa korištenjem ACL.

Bobu2 ćemo dati pristup datoteci tako što ćemo ga dodati u ACL željenje datoteke, tako ga ne treba dodavati u grupu.

```
setfacl -m u:bob2:r security.txt
```

Uklanjanje iz ACL vrši se:

```
setfacl -x u:bob2 security.txt
```

Ako u ACL dodajemo predefinirane grupe, onda govorimo o **kontroli pristupa temeljenoj na ulogama**.

Zadatak D

Demonstrirat ćemo kako Linux tretira procese, sa stajališta kontrole pristupa.

Bob2 ima pravo pristupa security.txt čiji je vlasnik alice2.

Student je vlasnik datoteke, ali nema pravo pristupa. ???

Student pokušava pristupiti i zahtjev mu je odbijen.

Bob2(nije vlasnik) pokušava pristupiti i uspijeva.

Bob2 je uspio pristupiti zato što Linux OS gleda id korisnika koji je pokrenuo proces, a ne tko je vlasnik.

Sara Ćurak

računarstvo 120