Izvještaj šeste laboratorijske vježbe

- Cilj vježbe: student će se upoznati s osnovnim postupkom upravljanja korisničkim računima na Linux OS-u. Pri tome će se poseban naglasak staviti na **kontrolu pristupa (eng. *access control*)** datotekama, programima i drugim resursima Linux sustava.

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*.
- Identifikatore `uid`, `gid` i pripadnost grupama provjeravamo naredbom

```
id
```

- Provjeravamo pripadamo li grupi `sudo`, tj. imamo li administratorske ovlasti naredbom:

```
groups
```

- Kreirajmo novi račun i saznajmo `uid`, `gid` i sve dodatne grupe kojima pripadamo.

Ovo možemo izvršiti samo ako pripadamo sudo grupi ,tj. ako imamo administratorske ovlasti.

```
sudo adduser alice
su - alice
```

- Korisnika bob kreirali smo na isti način kao i alice.

B. Standardna prava pristupa datotekama

- Logirajte se u sustav kao `alice`. U korisnikovom home direktoriju kreirali smo novi direktorij `srp` te u njemu datoteku `security.txt`.

```
# navigate to home directory
cd

# create a new directory
mkdir

# create a file with text
echo "Hello world" > security.txt

# print file content
cat security.txt
```

- Izlistali smo informacije o novom direktoriju i datoteci koristeći naredbu `getfacl`.

Oduzmimo pravo pristupa datoteci `security.txt` vlasniku datoteke modifikacijom dopuštenja (*access permissions*). Za promjenu dopuštenja koristili smo naredbu `chmod`. Testirajte ispravnost vaših rješenja. U nastavku su dani neki primjeri primjene `chmod` naredbe:

```
# Remove (u)ser (r)ead permission
chmod u-r security.txt

# Add (u)ser (r)ead permission
chmod u+r security.txt

# Remove both (u)ser and (g)roup (w)rite permission
chmod ug-w security.txt

# Add (u)ser (w)rite and remove (g)roup (r)ead permission
chmod u+w,g-r security.txt

# Add (u)ser (r)read, (w)rite permissions and remove e(x)ecute permpission
chmod u=rw security.txt
```

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 rješiti tako da u ACL datoteke `security.txt` dodamo novog korisnika sa `(r)ead` ovlastima (potrebne su administratorske ovlasti).

```
# 1. Read/record current permissions defined on the file
getfacl security.txt

# 2. Add (u)ser bob to the ACL list of the file with (r)ead premission
setfacl -m u:bob:r security.txt

# 3. Check the updated permissions defined on the file
getfacl security.txt

# 4. Login as bob, navigate to the file and try to read its content
cat security.txt
```

D. Linux procesi i kontrola pristupa

- Linux procesi su programi koji se trenutno izvršavaju u odgovarajućem adresnom prostoru. Trenutno aktivne procese možete izlistati korištnjem naredbe `ps -ef`.