Lab 6

> kontrola pristupa datotekama,programima i drugim resursima Linux sustava

Linux sustav:

- svaka datoteka ima vlasnika
- svakom korisniku pridjeljen je jedinstveni identifikator - User ID
- svaki korisnik mora pripadati barem jednoj grupi ; više korisnika može dijeliti istu
- grupe imaju jedinstvene identifikatore - Group ID

✔️ **Kreiranje novog korisničkog računa**

1. naredbom `id` u shell-u u WSL se provjerava pripadnost grupama
2. uvjerili smo se da pripadamo grupi **sudo** (bitno da bismo mogli dodavati nove korisnike)
    a. **sudo → SuperUser do →** ne moramo imati glavnu lozinku od root accounta da bismo nešto napravili, već upišemo svoju lozinku i izvršimo naredbu koju inače ne bismo mogli izvršiti “običnim” accountom
3. naredbom `sudo adduser alice` dodajemo novu korisnicu alice i postavljamo šifru
4. naredbom `su - alice` dolazimo u home-direktorij od alice, a to se provjeri naredbom `id`
5. izlazimo iz shell-a alice u shell koji ima administratorske ovlasti naredbom `exit` i dodajemo korisnika bob naredbom `sudo adduser bob`
6. ulogiramo se kao alice `su - alice`

✔️ Standardna prava pristupa datotekama

1. provjeravamo u kojem smo direktoriju naredbom `pwd` (*/home/alice*)
2. naredbom `mkdir` stvaramo direktorij srp te sa `cd srp` ulazimo u taj direktorij
3. stvaramo datoteku sa tekstom naredbom `echo Hello world > security.txt`
4. naredbom `cat security.txt` čitamo datoteku
5. naredbama `ls -l` i `getfacl srp` dobijemo informacije o vlasnicima resursa i dopuštenjima definiranima na njima
6. naredbom `chmod u-r security.txt` oduzimamo pravo čitanja datoteke vlasniku (alice), a time i pravo listanja njegovog sadržaja (ls)
7. naredbom `chmod u-x security.txt` vlasniku oduzimamo pravo pristupa datoteci bez da mu oduzimamo pravo čitanja (read)
8. u dopunskom terminalu logiramo se kao drugi korisnik bob `su - bob`
    a. naredbom `cat /home/alice/srp/security.txt` čitamo sadržaj (*Hello world*) datoteke security.txt →želimo oduzeti dozvolu čitanja novom korisniku
    b. u primarnom terminalu naredbom `chmod o-r security.txt` oduzimamo pravo drugima da čitaju datoteku ,a time i bobu
    c. želimo da korisnik ima pristup datoteci isključivo ako je član grupe koja je vlasnik predmetne datoteke security.txt
    d. naredbom `getfacl security.txt` saznajemo grupu (*alice*) koja posjeduje tu datoteku
    e. moramo se vratiti u shell koji ima administratorske ovlasti naredbom `exit` da bismo boba dodali u grupu *alice* koju smo saznali u prethodnom koraku
    f. naredbom `usermod -aG alice bob` dodajemo boba u grupu *alice*
    g. naredbom `id` provjeravamo grupu kojoj pripada bob, a naredbom `chmod g+x security.txt` dajemo bobu pristup datoteci security.txt i on sad može pročitati sadržaj jer je član grupe koja je vlasnik te datoteke

9. Linux pohranjuje hash korisničkih lozinki u datoteku /etc/shadow, tu datoteku može čitati samo administrator
10. naredbama `gpasswd -d bob alice` i `gpasswd -d bob shadow` mičemo boba iz grupa alice i shadow

✔️ Kontrola pristupa korištenjem *Access Control Lists (ACL)*

- Za provjeru i modifikaciju ACL-ova resursa (datoteka, direktorija) koristimo programe `getfacl` i `setfacl`
- naredbom `getfacl security.txt` vidimo trenutne dozvole definirane nad datotekom
- naredbom `setfacl -m u:bob:r security.txt` dodajemo boba na ACL listu datoteke sa dozvolom za čitanje
- naredbom `getfacl security.txt` provjeravamo ažurirane dozvole definirane nad datotekom
- prijavimo se kao bob naredbom `su - bob` i pomoću `cat security.txt` pročitamo sadržaj
- brisanje jedne prijave iz ACL liste naredbom `setfacl -x u:bob security.txt` ,a brisanje cijele ACL liste `setfacl -b security.txt`
- želimo omogućiti novom korisniku pristup sadržaju datoteke `security.txt` ali kroz članstvo u grupi (novu grupu nazovemo `alice_reading_group`)
- novu grupu kreiramo naredbom `groupadd alice_reading_group` i za to nam trebaju administratorske ovlasti

✔️ Linux procesi i kontrola pristupa

- linux procesi su programi koji se trenutno izvršavaju u odgovarajućem adresnom prostoru

- trenutno aktivne procese možemo izlistati korištenjem naredbe `ps -ef`
- proces ima vlasnika UID i jedinstveni identifikator procesa ID

1. korisnika bob uklanjamo iz grupe u koju smo ga prethodno dodali naredbom `gpasswd -d bob alice_reading_group` tako da više nema pristup datoteci security.txt
2. otvorimo *WSL shell* i u tekućem direktoriju kreiramo 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())
```

3. uđemo u svoj direktorij `cd lpelai/lpelai` i naredbom `python lab6.py` izlistamo UIDs