LAB 6

Linux Permissions and ACLs

- osnovni postupak upravljanja korisničkim računima na Linux OS-u: **kontrola pristupa** datotekama, programima i drugim resursima Linux sustava
- pokrenuli smo WSL i izvođenjem naredbe id
- svakom korisniku pridjeljen je jedinstveni UID i mora biti pripadnik barem jedne grupe. (GID).
- kreirali smo korisnike *alice3* i *bob3* sljedećim naredbama:

```
id

sudo adduser alice3
sudo adduser bob3
```

- iz prethodnih naredbi vidimo da je kreiranje novih korisnika moguće isključivo od strane *super user-a*

```
su - alice3
su - bob3
```

- Oba korisnika pripadaju samo jednoj grupi, alice3, odnosno bob3.
- kreiranje novog foldera *srp* te unutar tog foldera *file-a security.txt.*

```
mkdir srp
echo “Hello World” > security.txt
```

- naredbama:

```
ls -l srp
ls -l srp/security.txt
```

```
getfacl srp
getfacl srp/security.txt
```

- dobili smo uvid u vlasnike resursa i dopuštenja definirana nad njima.

FILE:

- r (read) → čitanje file-a
- w (write) → pisanje u file
- x (execute) → izvršavanje file-a

FOLDER:

- r (read) → uvid u sadržaj folder-a
- w (write) → kreiranje novih stvari unutar foldera
- x (execute) → pozicioniranje unutar folder-a
- izvršavanjem naredbe:

```
chmod u-r security.txt
```

- oduzeli smo pravo čitanja *file-a* vlasniku istog
- logirali smo se kao Bob i provjerili imamo li pristup file-u security.txt.

```
cat /home/alice3/srp/security.txt
```

- Bob je korisnik koji pripada grupi *others.* Ta grupa je imala pravo čitanja *file-a* pa je prethodna naredba uspješno izvedena
- ovisno o tome gdje se trenutno nalazimo, ispravnim pozicioniranjem unutar folder-a srp mogli bismo izvršiti sljedeće:

```
chmod u-x .
```

- Bob, korisnik koji pripada grupi *others,* i dalje ima pravo čitanja navedenog *file-a*.
- Alice je izvorna prava dobila naredbom

```
chmod u+x  .
```

- Da bismo Bobu onemogućili čitanje file-a, morali smo grupi kojoj Bob pripada oduzeti određena prava.

```
chmod o-r security.txt
```

- Boba ćemo dodati u grupu kojoj pripada Alice i dobit će sva prava nad file-om.

```
usermod -aG alice3 bob3
```

- izlistom svih prava definiranih nad navedenim folderom vidjeli smo da Bob, odnosno Alice, ne pripadaju grupi shadow što znači da nemaju pristup navedenom folderu.
- Boba smo u ACL datoteke *security.txt* dodali sljedećom naredbom:

```
setfacl -m u:bob:r /home/alice3/srp/security.txt
```

- Bob će nakon ove naredbe imati pravo čitanja file-a.
- napravili smo neku novu grupu i nju dodali u ACL datoteke *security.txt*. Kreirali smo grupu *alice_reading_group* i nju dodali u ACL sljedećom naredbom:

```
sudo setfacl -m g:alice_reading_group:r /home/alice3/srp/security.txt
```

- Na ovaj način smo sebi olakšali posao jer je sada potrebno samo *user-a* dodati u neku grupu da bi mogao obavljati određene operacije na *file-om/folder-om*.
- Za kraj smo pripremili python skriptu sa sljedećim kodom:

```
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())
```

- izvršavanjem skripte dobili smo *permission denied*
- trenutno logirani *user* s kojim smo izvršili skriptu nema nikakva prava nad *file-om*.
- Probali smo file pokrenuti i kao user Bob, ali tada nije bilo nikakvih problema zbog toga što Bob ima prava nad tim *file-om*.
- Postoji poseban flag koji nam omogućava da se effective UID uzme od vlasnika tog *file-a* i da se sukladno tome izvrši promjena lozinke.
- Izvršavanjem naredbe `ps -eo pid,ruid,euid,suid,cmd` u drugom terminalu dobili smo uvid u sve tekuće procese. Vidjeli smo da je RUID odgovara Bob-ovom dok je EUID onaj od *super user-a*.