

Sigurnost računala i podataka (Lab 6)

Lab 6 - Linux permissions and ACLs

U okviru ove vježbe upoznat ćemo se s postupkom upravljanja korisničkim računima na Linux-u.

A. Kreiranje novog korisničkog računa

Otvaramo shell i izvršimo wsl naredbu.

Svaki korisnik ima svoj UID i mora pripadati bar jednoj grupi. U to se možemo uvjeriti naredbama *id* i *groups*.

Dodajemo novi korisnički račun:

```
sudo adduser alice5
```

Postavljamo lozinku alice.

Logiramo se kao alice i saznajemo odgovarajuće identifikatore korisnika i grupa kojima alice pripada.

```
su - alice5
```

Dodajemo još jedan korisnički račun:

```
sudo adduser bob5
```

Postavljamo lozinku bob.

Naredbom *exit* vraćamo se u shell korisnika koji ima administratorske ovlasti.

B. Standardna prava pristupa datotekama

Potom se logiramo kao alice i kreiramo novi direktorij *srp* i u njemu datoteku *security.txt*.

```

a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ su - alice5
Password:
alice5@DESKTOP-LH5GUL2:~$ id
uid=1008(alice5) gid=1010(alice5) groups=1010(alice5)
alice5@DESKTOP-LH5GUL2:~$ mkdir srp
alice5@DESKTOP-LH5GUL2:~$ cd srp
alice5@DESKTOP-LH5GUL2:~/srp$ dir
alice5@DESKTOP-LH5GUL2:~/srp$ echo Hello world > security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ ls
security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ cat security.txt
Hello world
alice5@DESKTOP-LH5GUL2:~/srp$ |

```

Activate Windows

Izlistajemo informacije o novom direktoriju i datoteci i određujemo vlasnike ovih resursa kao i dopuštenja definirana na njima. Koristimo sljedeće naredbe: `ls -l` ili `getfacl`.

```

alice5@DESKTOP-LH5GUL2:~/srp$ echo Hello world > security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ ls
security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ cat security.txt
Hello world
alice5@DESKTOP-LH5GUL2:~/srp$ ls -l
total 4
-rw-rw-r-- 1 alice5 alice5 12 Jan 18 11:14 security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice5
# group: alice5
user::rw-
group::rw-
other::r--

```

Activate Windows

```

alice5@DESKTOP-LH5GUL2:~/srp$ getfacl .
# file: .
# owner: alice5
# group: alice5
user::rwx
group::rwx
other::r-x
alice5@DESKTOP-LH5GUL2:~/srp$ |

```

Onemogućavamo korisniku da čita (read) sadržaj datoteke *security.txt*.

```
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice5
# group: alice5
user::rw-
group::rw-
other::r--

alice5@DESKTOP-LH5GUL2:~/srp$ chmod u-r security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ cat security.txt
cat: security.txt: Permission denied
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice5
# group: alice5
user::-w-
group::rw-
other::r--
```

Activate Windows
Go to Settings to activate Windows.

Vraćamo korisniku read dopuštenje nad datotekom *security.txt*.

```
alice5@DESKTOP-LH5GUL2:~/srp$ chmod u+r security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ cat security.txt
Hello world
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice5
# group: alice5
user::rw-
group::rw-
other::r--
```

Activate Windows

Ako se logiramo kao Bob možemo pročitati sadržaj datoteke *security.txt*.

```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ su - bob5
Password:
bob5@DESKTOP-LH5GUL2:~$ cat /home/alice5/srp/security.txt
Hello world
```

Preko Alice mićemo prava čitanja s other korisnika (i Boba).

```

bob5@DESKTOP-LH5GUL2:~$ cat /home/alice5/srp/security.txt
cat: /home/alice5/srp/security.txt: Permission denied
bob5@DESKTOP-LH5GUL2:~$ |

# file: security.txt
# owner: alice5
# group: alice5
user::rw-
group::rw-
other::r--

alice5@DESKTOP-LH5GUL2:~/srp$ chmod o-r security.txt
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice5
# group: alice5
user::rw-
group::rw-
other::---

```

Dodajemo boba u grupu alice5 kako bi on kao član grupe mogao pročitati sadržaj datoteke *security.txt*. Prije toga preko *exit* komande vraćamo se u korisnika s administratorskim ovlastima.

```

a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ sudo usermod -aG alice5 bob5
[sudo] password for a507:

```

```

bob5@DESKTOP-LH5GUL2:~$ su - bob5
Password:
bob5@DESKTOP-LH5GUL2:~$ groups
bob5 alice5
bob5@DESKTOP-LH5GUL2:~$ cat /home/alice5/srp/security.txt
Hello world
bob5@DESKTOP-LH5GUL2:~$ |

```

Potom pokušavamo pročitati sadržaj datoteke */etc/shadow*. Nismo u grupi shadow, nemamo owner prava (nismo root) i other nema nikakva prava pa ne možemo vidjeti shadow.

```
alice5@DESKTOP-LH5GUL2:~/srp$ getfacl /etc/shadow
getfacl: Removing leading '/' from absolute path names
# file: etc/shadow
# owner: root
# group: shadow
user::rw-
group::r--
other::---
```

Mičemo boba iz grupe alice5.

```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ sudo gpasswd -d bob5 alice5
Removing user bob5 from group alice5
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$
```

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

Bob više nema pristup sadržaju datoteke *security.txt*.

Želimo Boba dodati u ACL kako bi mogao čitati sadržaj datoteke *security.txt*.

Modificiramo ACL listu.

```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ sudo setfacl -m u:bob5:r /home/alice5/srp/security.txt
```

Kao što smo ubacili Boba u ACL listu, možemo ubaciti cijelu grupu u ACL.

```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ sudo groupadd alice_reading_group5
```

Omogućavamo grupi pravo pristupa datoteci *security.txt*.

```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507$ sudo setfacl -m g:alice_reading_group5:r /home/alice5/srp/security.txt
```

```

bob5@DESKTOP-LH5GUL2:~$ getfacl /home/alice5/srp/security.txt
getfacl: Removing leading '/' from absolute path names
# file: home/alice5/srp/security.txt
# owner: alice5
# group: alice5
user::rw-
user:bob5:r--
group::rw-
group:alice_reading_group5:r--
mask::rw-
other:---

```

D. Linux procesi i kontrola pristupa

Svaki linux proces u izvršavanju ima svoj jedinstveni identifikator, *process identifier* PID. Osim toga, svakom od procesa se pridijeli id trenutno logiranog *user-a*, UID. Na temelju UID-ja Kernel će odlučivati ima li proces pristup određenim resursima ili ne.

Trenutno aktivne procese možemo izlistati korištenjem naredbe `ps -ef`.

Oduzimamo Bobu prava čitanja datoteke *security.txt* tako da ga maknemo iz grupe koja ima prava čitanja.

```
gpasswd -d bob alice_reading_group5
```

Otvaramo WSL shell i u 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())

```

Izvršavanjem ove skripte dobili smo *permission denied* jer trenutno logirani user nema nikakva prava nad datotekom.

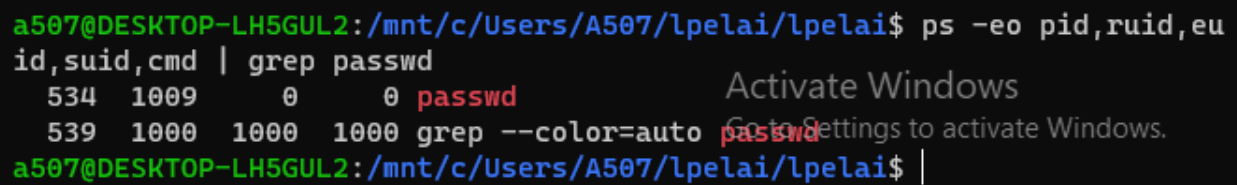
Ako pokrenemo skriptu kao Bob onda je pokretanje uspješno zbog Bobovih prava.

Ako kao Bob pokrenemo komandu *passwd*, dobit ćemo mogućnost promijeniti lozinku iako nemamo pristup */etc/shadow* folderu.

Izvršavamo naredbu koja ispisuje tekuće procese sa njihovim stvarnim i efektivnim vlasnicima:

```
ps -eo pid,ruid,euid,suid,cmd
```

.



```
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507/lpelai/lpelai$ ps -eo pid,ruid,euid,suid,cmd | grep passwd
534 1009 0 0 passwd
539 1000 1000 1000 grep --color=auto passwd
a507@DESKTOP-LH5GUL2:/mnt/c/Users/A507/lpelai/lpelai$
```

RUID odgovara Bobu, a EUID super useru.