Izvještaj laboratorijske vježbe

6. Linux permissions and ACLs

Zadatak

Upoznali smo se s osnovnim postupkom upravljanja korisničkim računima na Linux OS-u. Pri tome je poseban naglasak stavljen na **kontrolu pristupa (eng. *access control*)** datotekama, programima i drugim resursima Linux sustava.

1. Kreiranje 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 i gid provjeravamo pomoću naredbe **id** ili **groups.**

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ id
uid=1000(mpijuk) gid=1000(mpijuk) groups=1000(mpijuk),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugd

mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ groups
mpijuk adm dialout cdrom floppy sudo audio dip video plugdev netdev docker
```

SUDO - administratorska grupa

Kreirali smo nove korisnike naredbom **adduser** (ovo je moguće samo ako pripadamo grupi **sudo**)

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ id alice
uid=1001(alice) gid=1002(alice) groups=1002(alice)
```

Dodali smo korisnike **“alice”** i **“bob”** koji su dobili svoje uid-ove i gid-ove

2. Standardna prava pristupa datotekama

Logirali smo se kao **“alice”**, stvorili direktorij **“SRP”** te u njemu datoteku **“security.txt”** sadržaja **“Hello world”** koji možemo ispisati naredbom **“cat”.**

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ su alice
Password:

alice@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ cd
alice@DESKTOP-U5A60H8:~$ mkdir SRP
alice@DESKTOP-U5A60H8:~$ cd SRP
alice@DESKTOP-U5A60H8:~/SRP$ echo "Hello world" > security.txt
alice@DESKTOP-U5A60H8:~/SRP$ ls
security.txt
alice@DESKTOP-U5A60H8:~/SRP$ cat security.txt
Hello world
```

Informacije o novome direktoriju i datoteci možemo dobiti naredbama **“ls -l”** ili **“getfacl”**.

```
alice@DESKTOP-U5A60H8:~/SRP$ getfacl security.txt
# file: security.txt
# owner: alice
# group: alice
user::rw-
group::rw-
other::r--

alice@DESKTOP-U5A60H8:~$ getfacl SRP
# file: SRP
# owner: alice
# group: alice
user::rwx
group::rwx
other::r-x
```

Primijetimo kako su dopuštenja nad direktorijem i samom datotekom različita!

Za promjenu dopuštenja koristili smo naredbu **”chmod”** i njene varijacije.

```
# 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
```

Oduzeli smo pravo pristupa vlasniku datoteke **”security.txt”** na način da mu u tom postupku nismo oduzeli **read** dopuštenje nad datotekom. To smo realizirali naredbom **“chmod u-x .”** u direktoriju **“SRP”**(time oduzimamo vlasniku pravo ulaska u direktorij).

```
alice@DESKTOP-U5A60H8:~/SRP$ chmod u-x .
alice@DESKTOP-U5A60H8:~/SRP$ cd
alice@DESKTOP-U5A60H8:~$ cd SRP
bash: cd: SRP: Permission denied
alice@DESKTOP-U5A60H8:~$
```

Naredbom **“chmod u-r .”** oduzeli bismo pravo izlistavanja direktorija, ali ne i čitanja datoteka u direktoriju!

U drugome terminalu logirali smo se kao korisnik **“bob”** i mogli smo pročiati datoteku **“security.txt”** po “defaultu”, jer je za datoteku u sekciji **“other”** pisalo **“other::r - -”**

```
alice@DESKTOP-U5A60H8:~/SRP$ getfacl security.txt
# file: security.txt
# owner: alice
# group: alice
user::rw-
group::rw-
other::r--
```

To dopuštenje smo maknuli naredbom **“chmod o-r security.txt”**

U ovome koraku ponovo smo **“bobu”** omogućili pristup sadržaju datoteke, ali na način da on ima pristup datoteci isključivo ako je član grupe koja je vlasnik predmetne datoteke **”security.txt”.**

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ sudo usermod -aG alice bob
```

Potrebno je naredbom **“exit”** doći do korisnika koji je u administrativnoj grupi “**sudo”,** kako bismo gore navedenom naredbom “**boba”** dodali u **grupu “alice”**. Nakon ove naredbe potrebno obaviti **“logout”** i **“login”** na strani **“boba”** kako bi promjena bila vidljiva.

Korisnikom **“bob”** pokušali smo pročitati sadržaj datoteke **/etc/shadow** u koju **Linux** pohranjuje ***hash*** vrijednosti korisničkih zaporki.

```
bob@DESKTOP-U5A60H8:/home/alice/SRP$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Kontrola pristupa korištenjem *Access Control Lists (ACL)*

Korištenjem ACL, **“bobu”** možemo omogućiti pristup datoteci **“security.txt”** tako da u ACL datoteke **“security.txt”** dodamo novog korisnika sa **read** ovlastima naredbom **“setfacl”**.

```
alice@DESKTOP-U5A60H8:~/SRP$ setfacl -m u:bob:r security.txt
alice@DESKTOP-U5A60H8:~/SRP$ getfacl security.txt
# file: security.txt
# owner: alice
# group: alice
user::rw-
user:bob:r--
group::rw-
mask::rw-
other::---

bob@DESKTOP-U5A60H8:/home/alice/SRP$ cat security.txt
Hello world
```

Zapise iz **ACL-a** možemo ukloniti naredbama:

```
# Removing one entry from ACL
setfacl -x u:bob security.txt
```

```
# Removing the complete ACL
setfacl -b security.txt
```

Slično možemo napraviti, ali članstvom u grupi (dodali smo datoteci **“security.txt”** grupu gdje će biti svi korisnici koji datoteku mogu samo čitati).

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ sudo addgroup alice_reading_group
Adding group `alice_reading_group' (GID 1004) ...
Done.
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ su alice
Password:
alice@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ cd
alice@DESKTOP-U5A60H8:~$  cd SRP
alice@DESKTOP-U5A60H8:~/SRP$ setfacl -m g:alice_reading_group:r security.txt
alice@DESKTOP-U5A60H8:~/SRP$ getfacl security.txt
# file: security.txt
# owner: alice
# group: alice
user::rw-
group::rw-
group:alice_reading_group:r--
mask::rw-
other::---
```

Još moramo dodati **“boba”** grupi **“alice_reading_group”**

```
mpijuk@DESKTOP-U5A60H8:/mnt/c/Users/MARIO$ sudo usermod -aG alice_reading_group bob
```

Korisnika iz grupe uklanjamo naredbom:

```
gpasswd -d bob alice_reading_group
```

Linux procesi i kontrola pristupa

Linux procesi su programi koji se trenutno izvršavaju u odgovarajućem adresnom prostoru. Trenutno aktivne procese možemo izlistati korištnjem naredbe **”ps-ef”**. Primijetimo da proces ima vlasnika **(UID)** i jedinstveni identifikator procesa, ***process identifier*** **(PID)**.

```
alice@DESKTOP-U5A60H8:~/SRP$ ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root       603    90  0 17:56 pts/1    00:00:00 su bob
bob        604   603  0 17:56 pts/1    00:00:00 bash
root       622    73  0 18:08 pts/0    00:00:00 su alice
alice      623   622  0 18:08 pts/0    00:00:00 bash
alice      632   623  0 18:21 pts/0    00:00:00 ps -ef
```

U tekućem direktoriju kreirali smo **“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())
```

Program ispisuje **stvarnog, efektivnog** i **“saved”** vlasnika pokrenutog procesa te pokušava otvoriti već dobro poznatu datoteku **“security.txt”** za čitanje.

Skriptu odnosno program smo prvo pokrenuli prijavljeni kao **“bob”**, a potom i kao **“alice”**. Dobili smo sljedeće rezultate:

```
bob@DESKTOP-U5A60H8:/mnt/c/Users/MARIO/desktop/vj6$ python3 zd6.py
Real (R), effective (E) and saved (S) UIDs:
(1002, 1002, 1002)
Traceback (most recent call last):
  File "zd6.py", line 6, in <module>
    with open('/home/alice/SRP/security.txt', 'r') as f:
PermissionError: [Errno 13] Permission denied: '/home/alice/SRP/security.txt'

alice@DESKTOP-U5A60H8:/mnt/c/Users/MARIO/desktop/vj6$ python3 zd6.py
Real (R), effective (E) and saved (S) UIDs:
(1001, 1001, 1001)
Hello world
```

Rezultati su očekivani. Korisnik **“bob”** nije uspio pročitati datoteku **“security.txt”** i dobio je pripadni odgovor **“premission denied”**. Korisnica **“alice”** uspješno je pročitala datoteku kojoj je upravo ona vlasnica.

Zadatak 6

“U kontekstu onog što smo naučili iz prethodnih zadataka o načinu na koji Linux regulira pristup resursima, razmislite o sljedećem scenariju. Logirate se u sustav kao neprivilegirani korisnik (npr. `alice`) i želite promjeniti zaporku. Zaporku možete promjeniti korištenjem naredbe `passwd`. Sustav će vam dopustiti promjenu zaporke i ažurirat će datoteku `/etc/shadow` sa novom *hash* vrijednosti vaše zaporke. **Ako nemate prava pristupa datoteci `/etc/shadow` (vlasnik je korisnik sa `uid = 0`) a pokretanjem programa `passwd` ovaj program preuzima vaš `uid`, kako je moguće da možete napraviti promjenu u navedenoj datoteci i time ažurirati vašu zaporku?**

Jedan od mehanizama koji Linux koristi u ovakvim slučajevima je mehanizam *efektivnog vlasnika procesa*. Naime, svakom procesu je uz stvarnog vlasnika (označenog sa *real user id* - *`RUID`*) pridjeljen i *efektivni vlasnik* (*`EUID`*) koji kernel koristi pri provjeri pristupa tog procesa nekom resursu. U većini slučajeva (`RUID = EUID`) osim kad je program označen sa specijalnim `setuid` bitom” - Mario Čagalj (github)

1. Izvršili smo naredbu **“passwd”** kao neprivilegirani korisnik **“bob”**.

```
bob@DESKTOP-U5A60H8:~$ passwd
Changing password for bob.
Current password:
```

2. U drugom terminalu izvršili smo sljedeću naredbu:

```
mpijuk@DESKTOP-U5A60H8:~$ ps -eo pid,ruid,euid,suid,cmd | grep passwd
  PID  RUID  EUID  SUID CMD
  693  1002     0     0 passwd
```

Zaključak je da **“bob”** u procesu promjene lozinke ima status stvarnog vlasnika i tako može pristupiti datoteci **/etc/shadow**.

Dodatak - Što je SUID?

“The saved user ID (suid) is used **when a program running with elevated privileges needs to do some unprivileged work temporarily**; changing euid from a privileged value (typically 0) to some unprivileged value (anything other than the privileged value) causes the privileged value to be stored in suid.” - Wikipedia

Zaključak

Operacijski sustav linux ima širok spektar naredbi koje koristimo za kontrolu pristupa raznim datotekama i direktorijima kao i kreiranje **“Access Control”** listi.