6. laboratorijska vježba: Linux permissions and ACLs

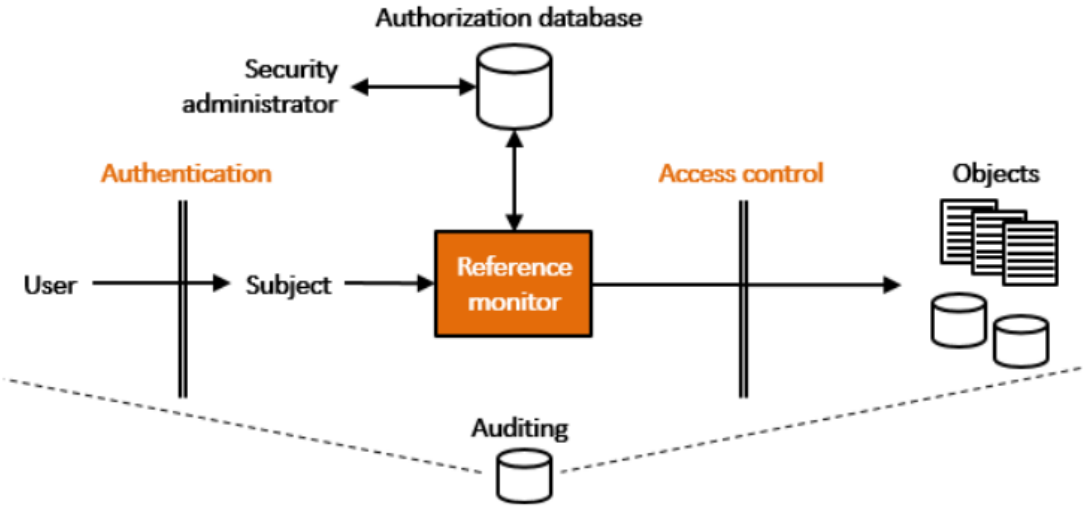
Studentica: Emilija Sarić

Smjer: 112

Predmet: Sigurnost računala i podataka

→Kontrola pristupa ograničava korisnicima i programima radnje kako bi se spriječio proboj sigurnosti i kako bi se spriječile maliciozne prijetnje nadziranjem čitanja, pisanja i izvršavanja datoteka i programa.

→ Naslanja se na identifikaciju i autentikaciju i centralni je element računalne sigurnosti. Provodi se referentnim monitorom, a elementi su subjekti, objekti i dozvole pristupa.



→U ovoj se vježbi koriste osnovni mehanizmi za upravljanje korisničkim računima u Linux operativnom sustavu.

IZVOĐENJE VJEŽBE:

1. kreiranje novih korisničkih računa *alice* i *bob* naredbom *sudo adduser <ime>* (”sudo” dodajemo jer za ovu radnju trebamo imati administratorske ovlasti)
2. logiranje u korisnički račun naredbom *su -alice/bob*
3. stvaranje novog direktorija i tekstualne datoteku u njemu

4. ispis informacija o datoteci naredbom *ls -l* ili *getfacl <ime>,* gdje se mogu vidjeti i informacije o tome tko im pristup datoteci
5. mijenjanje dopuštenja prema kreiranoj datoteci naredbom chmod a+(-) b <ime datoteke>

-a može biti u (user), g (group) ili o (other), ovisno o tome kome se mijenja dopuštenje

-nakon a stavljamo znak + ili - ovisno o tome pridodajemo li ili oduzimamo pravo

-b označava pravo koje dodajemo/oduzimamo, može označavati r (read), w (write), e (execute)

6. dodavanje korisnika u grupu naredbom

usermod -aG <owner_group> bob

7. uklanjanje korisnika iz grupe naredbom

gpasswd -d <user> <group>

8. dodavanjem pristupa novom korisniku korištenjem ACL-a naredbom: setfacl -m u:<user>:r/w/e <datoteka>
9. kreiranje i izvršavanje skripte u python-u

ZAKLJUČAK:

Iz ove se vježbe uočava se da pojedine radnje kontrole pristupa možemo obavljati na više načina, primjerice oduzimanje prava pristupa korisnika nekoj datoteci možemo provesti tako da korisniku oduzmemo ili pravo čitanja ili pravo ulaska u direktorij gdje se ona nalazi. Kod upravljanja kontrolom pristupa za većinu radnji dodavanja korisničkih računa i upravljanja njima trebamo imat administratorske ovlasti. Ako želimo samo pojedinom korisniku dati pravo pristupa nečemu, a ostalima ne to možemo učiniti dodavanjem korisnika u grupu. Korištenjem naredbe za promjenu lozinke *passwd* uočavamo da iako je root vlasnik datoteke /etc/shadow ipak u datoteku možemo pisati i modificirati je, to možemo zahvaljujući bitu setUID kojim se omogućuje da se datotekama upravljama prema dozvolama vlasnika.