**User Managment i Login**

Četiri su moguća scenarija korištenja sustava za upravljanje korisnicima (datoteka *usermgmt.py*):

1. [lokacija] add [korisnicko\_ime] – u sustav se dodaje novi korisnik s korisničkim imenom korisnicko\_ime;
2. [lokacija] passwd [korisnicko\_ime] – mijenja se lozinka za korisnički račun s korisničkim imenom korisnicko\_ime;
3. [lokacija] forcepass [korisnicko\_ime] – pri sljedećoj prijavi u sustav, od korisnika s korisničkim imenom korisnicko\_ime zatražit će se postavljanje nove lozinke;
4. [lokacija] del [korisnicko\_ime] – briše se korisnički račun s korisničkim imenom korisnicko\_ime.

Pri korištenju programa za prijavu u sustav (datoteka *login.py*), samo je jedan mogući scenarij korištenja: [lokacija] [korisnicko\_ime], nakon čega se od korisnika traži unos lozinke za navedeno korisničko ime te se, ukoliko je lozinka ispravna, na ekranu ispisuje poruka o uspješnoj prijavi u sustav.

Sustavu za upravljanje korisnicima pristupa samo administrator sustava. Pri dodavanju novog korisnika, nekoliko je koraka zaštite njegove lozinke. Prvi način zaštite jest činjenica da je unos nevidljiv, što je postignuto pomoću *getpass* funkcionalnosti. To štiti lozinku od napadača koji bi inače mogli jednostavno iščitati lozinku s ekrana za vrijeme unosa. Nadalje, unesena lozinka prolazi nekoliko provjera i mora zadovoljiti četiri uvjeta: mora biti dvaput unesena ispravno, ne smije biti kraća od osam znakova te mora sadržavati i slova i znamenke. Na taj je način spriječena ranjivost sustava koju bi korisnik mogao izazvati unosom prejednostavne lozinke. No, „prava“ zaštita lozinke dolazi s hashiranjem. Prvo se generira salt vrijednost duljine 32 bajta, koja se koristi skupa s lozinkom za izračunavanje funkcije sažetka (hashiranje). Na disk se pohranjuju korisničko ime, salt i hash tag dobiven iz generirane funkcije sažetka – nema pohrane lozinke, što potencijalnom napadaču dodatno otežava posao.

Kod „forsiranja“ promjene lozinke pomoću odgovarajuće naredbe, od korisnika se prije unosa nove lozinke traži da prvo unese staru lozinku kako bi se utvrdio njegov identitet.

U sustav se mogu prijaviti samo postojeći korisnici, ali valja napomenuti da, ako korisnik unese nepostojeće korisničko ime, na ekranu se ispisuje poruka da je korisničko ime ili lozinka netočna, što dodatno pojačava sigurnost sustava. Sama lozinka je pri unosu i ovdje nevidljiva iz ranije objašnjenih razloga. Ukoliko je administrator postavio zastavicu koja označava da korisnik mora promijeniti lozinku, o tome ga se obavještava pri uspješnoj prijavi u sustav. Zatim se od njega prvo traži da unese staru lozinku, a onda postavi novu. Na novu lozinku postavljeni su isti zahtjevi kao i pri postavljanju lozinke za novog korisnika, uz jedan dodatan zahtjev da nova lozinka ne smije biti jednaka staroj.

Provjera ispravnosti unesene lozinke pri prijavi u sustav ili unosu stare lozinke pri promjeni lozinke obavlja se uspoređivanjem hash tagova. Prvo se izračuna funkcija sažetka za novu lozinku te se njezin tag uspoređuje s tagom koji je dotada bio pohranjen za uneseno korisničko ime.