Operativni sistemi I

Vežbe 2

1. KORISNICI I GRUPE

Svakom korisniku Linux sistema dodeljen je **jedinstven celobrojni identifikator – UID** (user ID) na osnovu kog kernel identifikuje korisnike. Ovaj metod predstavljanja kernelu karakterističan je za većinu operativnih sistema, uzevši u obzir da procesor brže radi sa brojnim vrednostima. Posebna baza podataka, koja radi u korisničkom režimu rada, dodeljuje tekstualna imena ovim numeričkim vrednostima, odnosno uparuje UID sa konkretnim korisničkim imenom. Dodatno, u bazi se nalaze i informacije o korisniku, kao što su opis, lokacija ličnog direktorijuma (home) i podrazumevani komandni interpreter (shell).

Na UNIX sistemima postoje dve vrste korisnika:

- **sistemski korisnici**, koji nastaju prilikom instalacije operativnog sistema i služe za specijalne namene, a ne za prijavljivanje na sistem. Jedini sistemski korisnik koji se može prijaviti na sistem je superuser **root**. Root ima sve privilegije i služi isključivo za administraciju sistema;
- **regularni korisnici**, koji služe za prijavljivanje na sistem. Regularne korisnike kreira superuser root.

1.1 Osnovno o nalozima

Na Unix-like sistemima postoje tri primarne vrste naloga:

- root nalog (superuser),
- system nalog i
- user nalog.

Skoro svi nalozi raspoređuju se po ovim kategorijama.

- **Root nalog**

  Root korisnik ima potpunu kontrolu nad sistemom, do te mere da može pokrenuti komande za uništenje sistema. Root može uraditi bilo šta bez ikakvih ograničenja, bez obzira na osobine fajlova ili direktorijuma. Princip po kome Unix-like sistemi funkcionišu je takav da se za root-a podrazumeva da zna šta radi, tako da on ako u bilo kom trenutku pokrene komande za uništavanje sistema, sistem će mu to i dozvoliti.

- **Sistemski nalog**

  Sistemski nalozi su potrebni za operacije koje izvršavaju specifične komponente sistema. One uključuju, na primer mail account i ssh account (za ssh komunikaciju). Sistemski nalozi se prave u toku instalacije sistema i asistiraju u održavanju servisa ili programa koje korisnici zahtevaju. Postoje različiti sistemski nalozi, pri čemu se samo neki nalaze na određenom sistemu. Spisak sistemskih naloga na određenom sistemu se može naći u fajlu **/etc/passwd**. Neki od njih su: alias, apache, bind, ftp, halt, mail, mysql, root i sys. Ovi

nalozi kao što je rečeno služe u obavljanju određenih operacija i ne treba ih menjati.

- **User nalog**

  User nalozi omogućuju korisniku ili grupi korisnika, pristup sistemu. Generalno gledano, user nalozi imaju određena ograničenja tj. nemaju pristupa kritičnim fajlovima. Ime naloga je isto kao i ime usera.

- **Group nalog**

  Grupni nalozi daju mogućnost da se više naloga logički povežu u smislu datih ograničenja. Ograničenja su podeljena u tri vrste i to: vlasnik tj. onaj ko je napravio fajl, grupa i drugi. Postojanje grupe daje mogućnost vlasniku da na svom fajlu da ograničenje za neku grupu korisnika. Dobra strana grupa je što jedan nalog može pripadati većem broju grupa, pri čemu se veoma precizno mogu odrediti dozvole i ograničenja bilo kog naloga.

  Svaki korisnik sistema mora pripadati najmanje jednoj grupi – tzv. primarna grupa. Primarna grupa korisnika je obavezan atribut svakog korisnika - njen GID (Group ID) je naveden u datoteci /etc/passwd.

1.2 Administracija korisnika i grupa

U administraciji korisnicima i grupama važna su sledeća tri fajla:

- **/etc/passwd** — izlistava sve naloge
- **/etc/shadow** — za svaki nalog sadrzi kriptovanu lozinku.
- **/etc/group** — sadrži podatke o grupama.

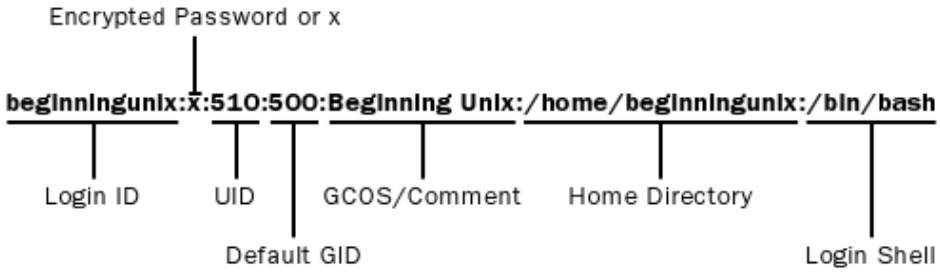
/etc/passwd

U fajlu **/etc/passwd** se nalaze podaci slični ovima:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
```

...

Za svaki nalog je vezano nekoliko atributa.



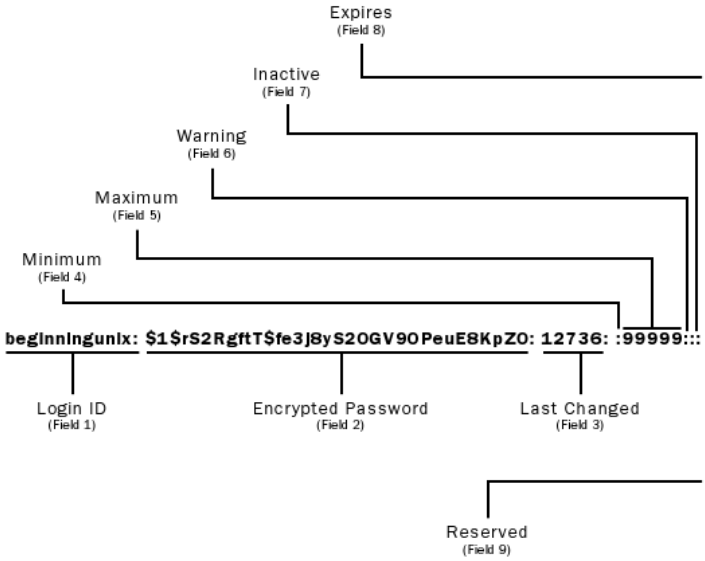
- **Login ID** atribut je ime naloga tj. korisnicko ime koje korisnik unosi pri prijavljivanju na sistem.
- **Encrypted Password** predstavljen sa “x” je mesto gde se u ranijim verzijama sistema ovde se nalazila kriptovana lozinka ali se danas zbog sigurnosti nalazi u posebnom fajlu /etc/shadow.
- **UID** je način na koji sistem prepoznaje korisnika. Korisničko ime postoji da bi se korisniku olakšao rad, dok sistem koristi ovaj broj. Na sistemu ovaj broj bi trebao da bude jedinstven, jer bi preklapanjem ovog broja za više korisnika bilo konfuzno odrediti ovlašćenja.
- **GID** je broj kojim se identifikuje grupa kojoj korisnik pripada. Ovaj broj ne mora biti jedinstven, jer više korisnika može pripadati istoj grupi. Manje vrednosti GID-a pripadaju grupama sistemskih naloga.
- **GCOS** je neki opis kao što je puno ime korisnika, kontakt ili neka informacija.
- **Home directory** opisuje putanju na kojoj se nalazi home direktorijum.
- **Login shell** predstavlja ime shella koji korisnik koristi.

/etc/shadow

Ovaj fajl sadrži kriptovane lozinke svih korisnika (korisničkih naloga), kao i vreme posle kojeg nisu validni. Npr:

```
man:*:13991:0:99999:7:::
lp:*:13991:0:99999:7:::
mail:*:13991:0:99999:7:::
…
milos:tc2kk31xv1PxQ:12735::::::
```

Podaci o svakom nalogu imaju devet mogućih mesta za podatke.



- **Login ID** predstavlja naziv korisničkog naloga.
- **Encrypted Password** je niz karaktera koji predstavlja kriptovan password. Ovo polje može sadržati 13 ili više karaktera, a ako je ovo polje prazno korisnik se na ovaj nalog može prijaviti bez lozinke.
- **Last Changed** polje predstavlja koliko je dana prošlo od poslednje promene lozinke.
- **Warning** je broj dana posle kojih će nalog biti blokiran. Uglavnom će korisnik naloga biti obavešten o datumu isteka njegovog naloga tako da se može obratiti administratoru za produženje naloga. Polja od šestog do devetog su prazna u skoro svim distribucijama Unix sistema.

/etc/group

Ovaj fajl sadrži podatke o svim grupama. Npr:

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:root
...
```

- Prvo polje predstavlja **ime grupe**.
- Sledi polje koje sadrži **lozinku** ali je ona obično kriptovana i nalazi se u fajlu /etc/gshadow.
- Broj koji zatim sledi je **jedinstveni numerički identifikator grupe**.
- Poslednje polje govori **koji korisnički nalozi pripadaju datoj grupi**.

Komande za kreiranje, menjanje i brisanje naloga i grupa je uglavnom standardizovano na svim Unix i Unix-like sistemima. Sledeće komande su dostupne na većini sistema:

useradd	Dodaje nalog.
usermod	Menja opcije naloga.
userdel	Briše nalog sa sistema.
groupadd	Dodaje grupu.
groupmod	Menja opcije grupe.
groupdel	Briše grupu sa sistema.

1.3 Administracija korisničkih naloga

Manuelno dodavanje naloga editovanjem odgovarajućih fajlova:

- Promena **/etc/passwd** fajla tako što će se dodati ili izbrisati nalog. Ova datoteka se ne sme otvoriti standardnim editorom (kao što su vi, emacs ili joe), već isključivo pomoću vipw editora. vipw datoteku zatvara za upis, tako da druge komande ne mogu istovremeno da promene njen sadržaj. Komanda se navodi bez argumenata.
- Promena **/etc/shadow** fajla.
- Promena **/etc/group** fajla pomoću vigr editora.
- I na kraju sledi kreiranje direktorijuma željenog naloga u **/home direktorijumu**.

Naravno ovi koraci se mogu izbeći koristeći sledeću komandu, podrazumevajući da ste registrovani kao administrator tj. root.

useradd

```
useradd -c komentar
        -d home direktorijum
        -e datum isteka naloga
        -f koliko dana pre isteka roka korisnik dobija obaveštenje
        -g primarna grupa
        -G sekundarna grupa
        -m kreira home direktorijum ako ne postoji
        -s ime shella koji će korisnik koristiti
        -u ID korisnika  ime naloga
```

Primer. Kreiranje naloga pod imenom **unixnewbie**, čije pravo ime je Jane Doe. Jane je potreban nalog do 4. Aprila 2010. Njena primarna grupa je **users,** a sekundarna **authors**. Ime shell-a koji koristi je Bourne Again shell (bash). Ako ako se ne prijavi na nalog u periodu od 60 dana, nalog će biti blokiran.

```
$ useradd -c "Jane Doe" -d /home/unixnewbie -e 040410 -f 60 -g users -G
authors -m -s /bin/bash -u 1000 unixnewbie
```

Nakon ove komande treba postaviti password za ovog korisnika komandom:

```
$ passwd unixnewbie
```

adduser

```
$ adduser
Enter a username to add: jsmith
Adding user jsmith...
Adding new group jsmith (1051).
Adding new user jsmith (1051) with group jsmith.
Creating home directory /home/jsmith.
Copying files from /etc/skel
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jsmith
Enter the new value, or press return for the default
```

```
Full Name []: John Smith
Room Number []: 409
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [y/n] y
```

usermod

Komanda za menjanje korisničkog naloga. Ima iste opcije kao i useradd sa dodatnom opcijom -l koja daje mogućnost promene imena korisničkog naloga. Posle ove opcije navodi se novo ime pa ime koje se menja. Treba voditi računa o tome da li sistem vrši autentifikaciju prema imenu ili prema UID numeričkoj vrednosti. Evo primera:

```
$ usermod -d /home/saraht -m -l saraht storvald
```

userdel

Brisnje naloga tj. korisnika. Ima jednu opciju -r koja nam daje mogućnost da se izbriše i home direktorijum ovog korisnika.

```
$ userdel -r saraht
```

1.4 Administracija grupa

Komande za rad sa grupama su **groupadd**, **groupmod** i **groupdel** i iste su na skoro svim distribucijama. Primer:

- **groupadd -g ID *grupa Imegrupe***
- **groupmod -n *Promenjenoimegrupe Novoimegrupe***

  pored opcije -n može se koristi i opcija -g kada se umesto imena navodi ID grupe.
- **groupdel *Imegrupe***

  Ovde se uklanja samo grupa ali ne i fajlovi koji su povezani sa tom grupom.

1.5 Identifikacija korisnika

Dve osnovne komande pomoću kojih se može odrediti ko je prijavljen na sistem su who i finger.

who

Komanda who prikazuje korisničko ime, terminal (line), vreme prijavljivanja (login-time) i host računar (from) **za sve korisnike koji su prijavljeni na sistem**. Ukoliko se komanda zada sa parametrom -H rezultat će biti prikazan sa zaglavljem. Ukoliko se zada sa parametrom -q prikazuju se samo imena i ukupan broj korisnika prijavljenih na sistem.

```
# who -H
NAME            LINE  TIME             COMMENT
root            pts/0 Mar 24 18:50     (nicotine.internal.vets.edu.rs)
jsmith          pts/1 Mar 24 19:50     (lab409.internal.vets.edu.rs)
# who -q
root            jsmith
```

```
# users=2
```

finger

Komanda finger daje sličan rezultat - prikazuje korisnike prijavljene na sistem, a pomoću nje se mogu dobiti i detaljne informacije o korisnicima iz /etc/passwd datoteke, **bez obzira da li su oni trenutno prijavljeni na sistem ili ne**. Dodatno se mogu dobiti i **informacije o korisnicima udaljenih sistema** (npr: finger coyote@acme.com), ali se takvi pokušaji najčešće završe porukom "connection refused".

```
# finger
Login     Name        Tty   Idle  Login Time
jsmith John Smith     pts/1 1     Mar 25 15:48      (nicotine)
root      root *      pts/0       Mar 25 15:47      (nicotine)
# finger jsmith
Login: jsmith                     Name: John Smith Jr.
Directory: /home/jsmith           Shell: /bin/bash
Office: 425, 39xx450              Home Phone: 44xx012
Last login Wed Mar 24 17:28 (CET) on pts/1 from nicotine
No mail.
No Plan.
```

Privremeno prijavljivanje na sistem pod drugim imenom

Korisnik se privremeno može prijaviti na sistem pod drugim imenom pomoću komande su (switch user) i na taj na in pristupiti resursima koji pripadaju drugom korisniku. Najčešće se koristi ukoliko je potrebno izvršiti promenu datoteka koje pripadaju drugom korisniku, promenu pristupnih prava ili pokretanje nekog programa. Administratori koriste ovu komandu da bi razrešili neki problem sa korisničkim nalogom ili u svrhe testiranja autorizacije i ponašanja naloga sa izvesnim aplikacijama. Sintaksa komande su je sledeća:

```
# su [-] [username]
```

Od korisnika koji pokreće komandu su (ukoliko to nije root) zahteva se da unese i lozinku za korisnički nalog koji želi privremeno da koristi. Nakon unošenja lozinke korisnik ima sve privilegije tog naloga.

Ukoliko je potrebno da se prilikom privremenog prijavljivanja na sistem pročitaju **nove inicijalizacione datoteke specifičnog korisnika, potrebno je zadati komandu sa parametrom "-"** pre korisničkog imena (npr. **su – milos**). Na taj način će se izvršiti postavljanje promenljivih i prelazak na home direktorijum tog korisnika. Povratak na originalni korisnički nalog vrši se komandom exit.

```
$ whoami
jsmith
$ pwd
/home/jsmith
$ su nmacek
Password:
$ whoami
nmacek
$ pwd
/home/jsmith
$ exit
exit
```

1.6 Stvarni i efektivni identifikatori korisnika (RUID i EUID)

ID korisnika koji je inicijalno prijavljen na UNIX sistem predstavlja je stvarni identifikator korisnika (RUID - Real User ID). Ukoliko se korisnik privremeno prijavi na sistem pod drugim imenom komandom su, njegov ID se privremeno menja. U cilju razlikovanja inicijalno i privremeno prijavljenih korisnika uvodi se efektivni identifikator korisnika (EUID - Effective User ID).

Za RUID i EUID važi sledeće:

- RUID je ID korisnika koji je inicijalno prijavljen na sistem i ne menja se tokom rada, bez obzira da li je korisnik pokrenuo komandu su i prijavio se pod drugim imenom,
- EUID je jednak RUID ukoliko korisnik nije pokrenuo komandu su, odnosno UID korisnika pod čijim imenom je privremeno prijavljen, ukoliko je izvršena zamena identiteta komandom su.

Komanda id može poslužiti za dobijanje informacija koji je UID, GID i kojim sve grupama pripada efektivni nalog (EUID).

```
$ id
uid=1051(jsmith) gid=1051(jsmith) groups=1051(jsmith)
$ whoami
jsmith pts/1 Mar 25 16:09 (nicotine.internal.vets.edu.rs)
$ su -
Password:
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
jsmith pts/1 Mar 25 16:09 (nicotine.internal.vets.edu.rs)
```

Zadaci:

1. Listanje sadržaja fajlova /etc/passwd, /etc/shadow, etc/group i /etc/gshadow, objašnjavanje sadržaja pojedinih polja.
2. Dodavanje novog korisnika na sisteme i logovanje studenata na novonapravljeni nalog korišćenjem komande “su - *novokorisnickoime*”. Komande **who, finger, id i whoami.**
3. Kreiranje praznog fajla komandom “touch” i provera vlasništva nad njim komandom “ls -l”.