Operációs rendszerek

3. gyakorlat:
UNIX rendszergazdai ismeretek 3

A UNIX felhasználói adatbázisa

Minden több felhasználós operációs rendszernek nyilván kell tartania felhasználókat és azok tulajdonságait.

Hogy megértsük a felhasználó menedzsmentet meg kell ismerkednünk azokkal az adatfájlokkal és struktúrákkal, miben a felhasználói adatbázis megvalósul. A gyakorlatokon csak felhasználó menedzsmenttel foglalkozunk, csoport menedzsmenttel nem.

UNIX rendszereken a felhasználói adatbázis alapvető fájlja a */etc/passwd* fájl. Maga a fájl szöveges, sorai rekordok, melyeken belül a mezőket (:) kettősponttal választják el. Hozzáférési jogok tekintetében egyedül a rendszergazda (ill. a rendszergazdai jogokkal futó programok) írhatja, de mindenki olvashatja. Struktúrája a következő:

login:passwd:UID:GID:gecos:homedir:shell

login – a felhasználó bejelentkezési neve, amivel azonosítja magát

passwd – a felhasználó jelszavának titkosított alakja. A titkosítás egy nem visszafordítható eljárással történik, ami biztosítja, hogy a titkosított karaktersorozatból, ne lehessen következtetni az eredeti jelszóra.

UID – a felhasználó azonosító száma, amivel az operációs rendszer azonosítja a felhasználót.

GID – a felhasználó bejelentkezési csoportjának azonosítója. A csoportok adatfájlja az */etc/group*

Gecos – a felhasználó egyéb adatait tartalmazó rekord.

Homedir – a felhasználó home jegyzéke

Shell – a felhasználó login shell-je, vagyis az a program, ami a sikeres bejelentkezés után elindul.

A jelszó titkosítása kezdetben elégségesnek bizonyult, de a számítási teljesítménynövekedése (és a felhasználók felelőtlen jelszóválasztása) egyre több lehetőséget kínált a jelszavak feltörésére, a titkosított alak ismeretében. Ehhez hozzájöttek olyan igények is, mint a jelszó öregítése, jelszóváltások kötelezővé tétele, felhasználók letiltásának lehetősége. Ezeket a lehetőségeket minden korszerű operációs rendszertől elvárhatjuk.

A problémák megoldása egy újabb fájl bevezetését hozta, a */etc/shadow* néven. A fájlt olvasása korlátozott és egyszerű felhasználók elől rejtett marad a tartalma. Struktúráját tekintve hasonlít a *passwd* fájlra (szöveges, a mezőelválasztó a kettőspont), a mező jelentése viszont eltér:

Login:pw:lastch:min_age:max_age:warn:inact:disabled:reserved

Login – a felhasználó bejelentkezési neve. Ez a mező kapcsolja össze a *shadow* rekordot a *passwd* rekorddal.

Pw – a titkosított jelszó. Ha itt van egy felhasználónak a jelszava tárolva, akkor a *passwd* fájlban a jelszó helyén egy x áll.

Lastch – az utolsó módosítás napja (1970 jan. 1-tól számítva)

Min_age – a jelszó minimális élettartama napokban. Jelszóváltást követően ennyi nap után lehet csak újra jelszót változtatni.

Max_age – a jelszó maximális élettartama napokban. Ha a megadottnál régebben váltott jelszót a felhasználó, akkor a következő bejelentkezésnél a rendszer rá fogja kényszeríteni a felhasználót a jelszó megváltoztatására.

Warn – a jelszó érvénytelenné válása előtt az itt megadott napok számával a rendszer elkezdi figyelmeztetni a felhasználót.

Inact – a jelszó érvénytelenné válásának ideje napokban. Ha az utolsó jelszó módosítás óta, az itt megadottnál több nap telt el, akkor a felhasználó jelszava érvénytelenné válik – a rendszer kitiltja. Ezt csak a rendszergazda tudja feloldani, a felhasználó nem tud bejelentkezni még jelszóváltás céljából sem.

Reserved – nem használt, de fenntartott mező.

A rendszergazda két segédprogram használatával állíthatja, hogy a rendszer működését. A *pwconv* utasítás létrehozza a */etc/shadow* fájlt, belemásolja az összes felhasználó jelszavát és feltölti a további mezőket alapértelmezett adatokkal. Ezután a rendszer a felhasználók azonosítására együtt használják a */etc/passwd* és a

/etc/shadow fájlokat. A *pwunconv* utasítás visszamásolja a titkosított jelszavakat a */etc/passwd* fájlba. Ezután a rendszer csak a */etc/passwd* fájlt használja.

Felhasználók felvétele, módosítása és törlése

Erre alapvetően két módszert kell megismernünk.

- Kézzel történő felhasználó menedzsmentet, amikor a rendszergazda nem használ semmilyen speciális segédprogramot.
- Szkriptek és segédprogramok használata. Ezek közül meg kell különböztetnünk 3 csoportot: az első csoportba soroljuk azokat a segédprogramokat, amiknek a meglétét a POSIX szabvány írja elő. A második csoportban megismerkedünk a GNU által kifejlesztett segédprogramokkal. Egy harmadik csoportba sorolhatjuk az egyéb programokat (pl. az egyes operációs rendszerek saját felhasználó menedzsment programjait), de ezekkel nem foglalkozunk.

A passwd program lehetőségei

A *passwd* programot minden felhasználó használja, saját jelszavának megváltoztatására. A rendszergazda ennél többre is tudja használni.
Pl.

passwd login

Ezzel a megadott login nevű felhasználó jelszavát lehet megváltoztatni. Alapvető különbség a program működésében, hogy a rendszergazdától a program nem kérdezi a régi jelszót.

passwd [-x max] [-n min] [-i inact] [-w warn] login

A megadott login nevű felhasználó jelszavának a maximális ill. minimális korát, az inaktívvá válás korát és az ezt megelőző figyelmeztetést állíthatjuk be.

passwd [-l] | [-u] login

A megadott login nevű felhasználót letilthatjuk (l) és újra engedélyezhetjük (u).

POSIX segédprogramok

useradd [-c gecos] [-d homedir] [-e exp] [-f inact]
[-g GID] [-G group1,…] [-m [-k skel]]
[-p passwd] [-s shell] [-u UID] login

Az utasítás hatására létrejön egy megadott login nevű felhasználó, a megadott paraméterekkel. Ha nem adunk meg bizonyos paramétereket, akkor azok alapértelmezett értéket kapnak.

A *usermod* utasítás felhasználó módosítására szolgál. Ugyanúgy kell megadni, mint a *useradd* utasítást, azzal a különbséggel, hogy itt már létező login nevet kell megadni és amelyik paramétert nem adjuk meg az nem változik.

userdel [-r] login

A megadott login nevű felhasználót törli. Az „r” kapcsoló megadásával a törlendő felhasználónak a home jegyzékét is törli.

A GNU segédprogramok

adduser login

Új felhasználó létrehozását szolgálja. A létrehozás paramétereit a */etc/adduser.conf* konfigurációs fájl tartalmazza, a felhasználó gecos adatait és a jelszavát interaktívan bekéri.

deluser [--remove-home] [--remove-all-files] [--backup] login

Felhasználó törlésére való segédprogram. A „remove-home” kapcsoló hatására törli a felhasználó home jegyzékét is, a „remove-all-files” kapcsoló hatására keresést indít a teljes jegyzék struktúrában és törli a felhasználó tulajdonában lévő összes fájlt. Biztonsági mentést készít a felhasználó home jegyzékéről a „backup” kapcsoló megadásakor. A mentés *login.tar.gz* néven a rendszergazda home jegyzékébe kerül.

Felhasználó létrehozása kézzel

Egy rendszergazdának tudnia kell, hogyan lehet létrehozni felhasználót, minden segédprogram nélkül is. Ehhez nézzük meg az alábbi 5 pontot, mellyel shadow nélküli.

1. Be kell jegyezni a felhasználót az adatfájlba.

   # echo 'felh:!:1234:100:teljes nev:/home/users/felh:/bin/bash' >> /etc/passwd

   Itt egy *felh* nevű felhasználót hozunk létre, akinek a titkosított jelszavát nem tudjuk kézzel generálni. A „!” azt jelenti, hogy nincs jelszava és le van tiltva. Az UID úgy választjuk, hogy ne legyen ugyanaz a szám más felhasználóé. A GID esetén meg kell nézni, hogy melyik csoportba akarjuk tenni a

felhasználót. A 100-as csoport szokásosan „users” megnevezésű.

2. Létre kell hozni a home jegyzéket.

   # *mkdir /home/users/felh*

3. Az új felhasználók kapnak induló fájlokat, ezeket oda kell másulnunk.

   # *cp /etc/skel/.* /home/users/felh*

4. A home jegyzéket a felhasználó tulajdonába kell adni.

   # *chown –R felh.users /home/users/felh*

5. Jelszót kell adni a felhasználónak.

   # *passwd felh*