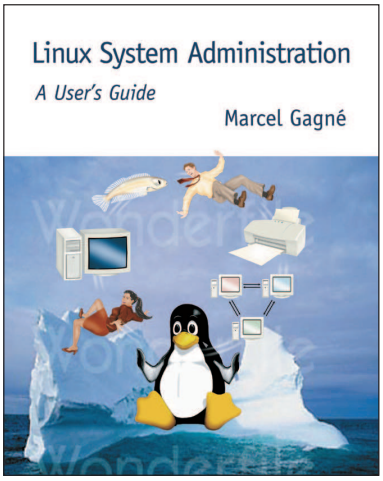
Linux-rendszerfelügyelet

Kóstoló francia konyhafőnökünk nemrég megjelent könyvéből.

Legújabb könyvem, a Linux rendszerfelügyelet – felhasználói kézikönyv még az idén felkerül a hazai könyvesboltok polcaira. Mind a Linux Journal, mind a Linuxvilág munkatársai olyan fenemód jószívűek voltak, hogy helyet biztosítottak arra, hogy ebben a számban a könyvből egy kis ízelítőt adjak. Vért izzadtam, mire kitaláltam, mit tudnék ilyen kis helyen bemutatni belőle, hiszen annyi mindent választhatnék. Lapolvasó telepítése? Vagy inkább CD-íróé? A hálózat megvédése a betolakodóktól? Nyomtatás? Mentések? Levelezési fogások? Melyiket szeressem? Végül is úgy döntöttem, hogy egy olyan témával foglalkozom, amelyik mai internetes világunkban nem kap elég nagy nyilvánosságot, s ez nem más, mit a jó öreg felhasználói biztonság. A könyv hetedik, Felhasználók és felhasználói csoportok című fejezetéből fogok szemezgetni. Nem az egész fejezet olvasható itt és nem is részletek sorozata. Már hallom a kifogást: „A szakács túl sokat kortyolgat a saját borából!”. Valójában mintát, vagy ha úgy tetszik, kóstolót szerettem volna adni mindabból, amivel az olvasó az új könyvem oldalain találkozhat. Mintha csak csipegetnénk egy büféasztalról. Ahogy Chef Marcel mondaná: Bon appétit!



Adatok

Cím: Linux-rendszerfelügyelet
Szerző: Marcel Gagné
Kiadó: Addison-Wesley
ISBN: 0-201-71934-7

Élet egy többfelhasználós világban

A Linux többfelhasználós operációs rendszer, ami azt jelenti, hogy egy időben egynél több felhasználó is dolgozhat rajta. Minden felhasználóra a felhasználói nevével hivatkozhatunk, s ezek mindegyikéhez egy felhasználói azonosító (UID) tartozik, amely egy vagy több felhasználói csoporttal társítható. A felhasználói nevekhez hasonlóan ezek a csoportok is egy-egy numerikus azonosítóval rendelkeznek, amit ebben az esetben csoportazonosítónak (GID) hívunk. Mindkét azonosítófajta egyedi értékekkel rendelkezik.
Az állományok és könyvtárak biztonsága a Linuxban olyan engedélyek révén valósítható meg, amelyek a felhasználói azonosítóval közvetlen kapcsolatban állnak. A felhasználók lehetnek közönséges és felügyeleti jogokkal rendelkező felhasználók. A legfőbb felügyeleti feladatkört ellátó felhasználó neve: root. A felhasználói azonosítótól függ, hogy az adott személy milyen parancsokat futtathat, milyen állományokba tud betekinteni vagy milyeneket tud módosítani. Minden felhasználói azonosítóhoz jelszó tartozik, amelyek megváltoztatása csak szabályozott keretek között történhet(ne).

Mikor ne használjuk a rendszergazdai jogosultságot?

A kérdésre a legrövidebb válasz: soha ne használd, csak ha nagyon muszáj. A veszély abban rejlik, hogy a rendszergazda gyakorlatilag a rendszer teljhatalmú ura, s egy pici hiba is komoly következményekkel járhat, vagyis akár az egész rendszert tönkreteheti. Ha egy mód van rá, közönséges felhasználói azonosítóval dolgozz. További indokok is felsorolhatók.
Az első a biztonság kérdése: mivel a rendszergazda mindenhez hozzáfér, csak azzal érdemes megosztani a jelszót, akinek valóban szüksége van rá. Minél kevesebben ismerik, annál jobb. Miért érdemes ilyen féltékenyen őrizni ezt a jogosultságot? Mert sokkal egyszerűbb a biztonságkezelés és csökken annak a veszélye, hogy a hibák az egész rendszert befolyásolják. Valóban egy közönséges felhasználó is komoly kárt okozhat egy rendszerben, de ennek kockázata sokkal-sokkal kisebb.

A jelszóállomány ellenőrzése

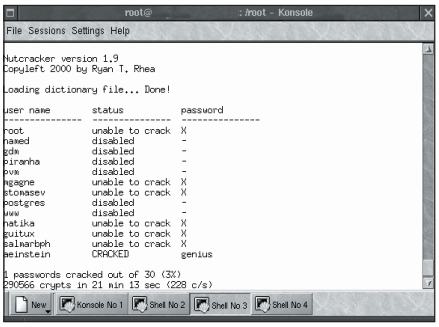
Ha még mindig nem lenne elég feladatod, itt a következő munka: szabályos rendszerességgel ki kell gyűjtened a használaton kívüli felhasználói azonosítókat. A könyv egy korábbi fejezete bemutatja a `finger` parancsot, amely az azonosítók használatának legutóbbi időpontjáról jelenít meg adatokat. Próbáld ki, hogyan lehet a parancs beírásával az összes felhasználói azonosítót és az utolsó belépés időpontját kiíratni. A parancsban lévő (az aposztróf a `sort` parancs és a pipa előtt) a ~ (tildejel) billentyűjén találod meg (az angol billentyűzeten, a magyaron pedig az 1-es a számbillentyűzeten – a szerk.).

```
finger ·sort /etc/passwd | cut -f1 -d":"·
      ➥| grep -i log | more
```

A parancs kimenete valahogy így néz ki:

```
Login: aeinstein          Name: A. Einstein
Never logged in.
Login: guitux             Name: Tux the Penguin
Last login Mon Jan  8 14:54 (EST) on tty2
Login: halt               Name: halt
Never logged in.
Login: lp                 Name: lp
Never logged in.
Login: mail               Name: mail
Never logged in.
Login: mgag               Name: Marcel Gagne
Last login Wed Mar  7 17:29 (EST) on 1 from
➥website
Login: named              Name: Named
Never logged in.
Login: natika             Name: Natika the Cat
```

Figyelmeztetésként fogadd meg a jótanácsomat: használd a józan ítélőképességedet (rendszergazdák számára alapvető követelmény). A felhasználói azonosítók egy része – például a `sync` vagy az `lp` – a rendszer része. Megszokott esetben ezekkel soha senki nem léphet be a rendszerbe. Másrészt Mr. Einstein (a lista tetején) sem lépett még be soha, és ez természetesen nem is rendszerfelhasználói név. Az is megeshet, hogy ez új azonosító (most az), vagy akad egy felhasználó, aki még soha nem lépett be ezen a néven. A második esetben a legjobb minél előbb megszabadulni az azonosítótól. Az előbbi példa parancssori jártasságodat volt hivatott növelni, de meg kell mondanom, járhatóbb út is létezik. Linux-rendszereddel egy `lastlog` nevű ügyes kis parancsot kapsz, amely éppen ezt csinálja.



Amiért ne szótár szavakat használjunk jelszóként…

```
[root@scigate /root]# lastlog | more
Username    Port    From     Latest
root        tty1       Wed Mar 7 17:18:40
                       -0500 2001
bin                    **Never logged in**
daemon                 **Never logged in**
adm                    **Never logged in**
lp                     **Never logged in**
sync                   **Never logged in**
shutdown               **Never logged in**
mgagne      1scigate Wed Mar 7 17:29:55
                       -0500 2001
postgres               **Never logged in**
www                    **Never logged in**
natika      8localhost.locald      Thu Dec 7
                                   ➥14:30:15
                       -0500 2000
guitux      tty2       Mon Jan  8 14:54:55
                       -0500 2001
```

A `lastlog` parancs az adatokat a */var/log/lastlog* nevű állományból veszi, amely kézzel nem módosítható.
Maradt még egy teendőd, amit rendszeres időközönként el kell végezned: ez a `pwck` futtatása. Alapértelmezésben a program végiglépked a */etc/passwd* és a */etc/shadow* állományokon és végrehajt egy ellenőrzést annak vizsgálatára, hogy a megfelelő számú mező szerepel-e, és minden név egyértelműen azonosítható-e. A csoportazonosító vizsgálatára a `grpck` parancs használható.

Miként törik fel jelszavainkat a kalózok?

Arról, hogy miért érdemes gondosan megválasztani a jelszót, a könyv korábbi részében olvashattál, a jelszóállomány leírásánál – kifejezetten jelszómezőről a nem árnyékállományokban (nonshadow). Egy gyors emlékeztető:

```
root:2IsjW45pb4L56:0:0:root:/root:/bin/bash
```

A jelszó mezője (a második) egy nyalábolóindexelés-algoritmus (hashing) szerint kódolt állapotban látható. Ha nagyon alapos vagy, és érdekel a részletes leírás, csak gépeld be a `man crypt` parancsot, és itt mindent megtalálhatsz, amit a jelszavak kódolásáról valaha is tudni szerettél volna. Röviden összefoglalva: a felbukkanó furcsa jelszó valójában jelszavadnak egy véletlenszerűen előállított kétkarakteres szó (a ***salt***) segítségével kódolt formája. Ezt a saltot átadva a kódoló-nyalábolóindexelési eljárásnak előáll a végleges karaktercsoport. A nyalábolóindexelés kifejezés olyan eljárást takar, melynek során az adat gyors visszanyerésére egy karaktersor (például egy személy vezetékneve) segítségével (eszményi esetben) egyedi kulcs áll elő. Amit teszünk, az a szöveg kódolása rövidebb, rendszerint numerikus megfelelőjére.
A jelszótörők ezt a saltot használják fel jelszólétrehozásra a szótárban szereplő minden egyes szót kipróbálva. Bár ez kicsit bonyolultnak tűnik, mégsem az. Egy egyszerű program meghívja a titkosító eljárást, lefuttatja egy szón, és összehasonlítja a */etc/passwd* állomány jelszóbejegyzésével. Ha egyezik: bingó! Megszerezték a jelszavadat. Ha nem, veszik a következő szót. Egy elég gyors rendszeren nem tart túl sokáig, hogy a kalózok minden jelszóhoz megtalálják az utat.
Nem hiszel nekem? Csak vess egy pillantást a képen látható, a szabad felhasználású Nutcracker által előállított listára. Ez a programocska épp az imént felvázolt „nyers erő” (brute-force) jelszófeltörő módszer egy fajtáját alkalmazza.
Ahogy a *képen* is látszik, a jól megjegyezhető szavak – mivel túl gyakoriak – jelszóként rossz választásnak bizonyulhatnak.

Honnan jelentkeztem be?

Nézzük, mi történik, amikor bejelentkezünk egy gépre. Minden rendben lévőnek tűnik. Megvan a felhasználói nevem, kéri a jelszavamat, beírom és voilá, bent vagyok.

```
login: mgagne
Password:
Last login: Mon Jan   8  16:00:39 from energize
```

De várjunk csak! Mi az a kis üzenet, ami a jelszóbeírás után megjelent? Mi a fene az az ***energize***? Az ***energize*** nyilván annak a gépnek a neve, amelyikről a legutóbb bejelentkeztem. Kivéve ha nincs ilyen nevű gépem. Sőt, tételezzük fel, hogy nem is ismerek ilyen nevű gépet és mindig ugyanonnan jelentkezem be. Az egyetlen magyarázat, hogy egy ***energize*** nevű gépről valaki az én nevemmel és jelszavammal lépett be a rendszerbe. Ez csak kitalált eset, de jól szemléltet egy szokást, amire esetleg érdemes a felhasználóinkat megtanítani. Ha nap mint nap ugyanarról a számítógépről jelentkeznek be, ez az üzenet nem változhat. Amennyiben a gép nevét az üzenetben nem ismerik fel, bölcsen teszik, ha értesítenek.
A biztonság kérdése nem kizárólag a rendszergazdára tartozik, bőven akad tennivalója enélkül is. Minden segítség elkél, tehát a felhasználók bevonására is szükségünk van. Hadd tudják és érezzék, hogy a rendszer biztonságának kérdése legalább annyira az ő ügyük, mint a tiéd.

Marcel Gagné (mggagne@salmar.com) Mississaugaban (Ontario, Kanada) él, a Salmar Consulting Inc. rendszerépítéssel és hálózati tanácsadással foglalkozó cég elnöke. Pilóta és sci-fi író egy személyben. A Világhálón elérhető honlapján sok hasznos dolgot találhatunk. ➲ http://www.salmar.com/marcel/

FORDUL A LINUXVILÁG

Kedves Olvasóink!

Tájékoztatni szeretnénk Önöket a lapunk életében történt változásokról.

Keressék az újságárusoknál!

Előfizetés

Idén 11 számmal jelenünk meg, mivel a januári és a februári számot összevontuk, terveink szerint most utoljára. Önök továbbra is nyugodtak lehetnek: előfizetésük a jövőben is lapszámokra vonatkozik majd: az egyéves előfizetés 12, a féléves pedig 6 számra vonatkozik (hiszen összevont számunk egynek számít).

Felemeltük előfizetőink kedvezményeit 8, illetve 20%-ra:
féléves (6 lapszám): 10 930 Ft
egyéves (12 lapszám): 19 008 Ft

A pénz beszél...

Ebben az évben belső köreinkből kiléptünk ország-világ színe elé.
A Linuxvilág szakmai írásaival kívánja meghódítani Olvasói szívét, ezért már a kezdetektől fogva a minőségre helyeztük a hangsúlyt és továbbra sem kívánunk csupán „hirdetőoszloppá" válni. A január–februári számtól kezdődően magazinunkat az újságárusoknál is megtalálhatják.

Éves előfizetéssel olcsóbb, számonként csak 1584 Ft.

Biztos megérkezés

Előfizetőink számára választási lehetőséget kínálunk: vagy ajánlott küldeményként juthatnak hozzá lapunkhoz (vállalva ennek költségeit), vagy pedig az eddig megszokott módon egyszerű postai küldeményként kapják meg.

Már ajánlott küldeményként is megrendelhető (+90 Ft/küldemény).

Akció!

Új Olvasóink számára legelső négy számunkat

- 2000. november,
- 2000. december,
- 2001. január,
- 2001. február–március

óriási, 50%-os kedvezménnyel kínáljuk.

További lehetőségek: a 2002 január előtt megjelent régi számaink (az első négy szám kivételével) ára változatlanul 1484 forint marad.
Az áremelés bejelentése előtt beérkezett előfizetéseket természetesen még a régi áron fogadtuk, aki tehát megrendelését már előzőleg meghosszabbította, még a régi áron juthatott magazinunkhoz.

Terjesztés: telefon: (06-1) 303-9119
fax: (06-1) 303-1619
e-mail: terjesztes@linuxvilag.hu

Ha bármilyen kérdésük, gondjuk támad, kérjük, írják meg az **info@linuxvilag.hu** címre.

További kellemes és hasznos olvasást kívánunk!

A Linuxvilág munkatársai