Maradjunk naprakészek terjesztésünk biztonsági frissítéseivel

A kezdő Linux rendszergazdák számára a programok naprakészen tartása az első lecke. Jeremy ennek a népszerű frissítő eszközök segítségével való elvégzését tárgyalja, kattintásról kattintásra.

Ha a *Linuxot* asztali vagy kiszolgáló környezetben meg akarjuk őrizni első számú játékosnak, akkor ügyelnünk kell arra, hogy a biztonsági foltok segítségével naprakészek maradjunk. Hiába tesszük meg a szükséges biztonsági intézkedéseket a hálózat és a vas szintjén, ha egyetlen apró rés miatt az egész rendszer sebezhetővé válik. Minden felhasználónak, legyen szó akár üzleti, akár nonprofit, akár otthoni használatról, tisztában kell lennie azzal, rendszerét és alkalmazásait miként frissítheti, és rendszeresen meg is kell ezt tennie.

A rendszer sértetlenségének megőrzéséhez két lépésre van szükség: tudni kell, mikor kell frissíteni, és valóban végre is kell hajtani a frissítést. Az első feladatot a terjesztéshez tartozó biztonsági témájú levelezőlista figyelésével teljesíthetjük. A második elvégzésére számos mód kínálkozik, végrehajtásához grafikus és parancssori eszközöket egyaránt használhatunk. Néhány terjesztés önműködő frissítő segédeszközt is tartalmaz, melynek segítségével könnyebben figyelemmel követhetjük rendszerünk állapotát.

Az adott alkalmazás újabb változatának telepítését frissítésnek vagy foltozásnak is nevezhetjük, a két művelet lényege ugyanaz. Ugyanakkor arra is érdemes figyelni, hogy a frissítés során ne telepítsünk olyan csomagváltozatot, amelyet eredetileg nem akartunk feltenni. A csomagok fejlesztői változatai általában külön sorszámsorozatból kapják változatszámukat. Ha a változatszám túlságosan különbözik, vizsgáljuk meg, milyen egyéb változatokat tudunk elérni.

Írásomban a linuxos rendszerek naprakészen tartására használható eszközök grafikus és parancssori változatával egyaránt foglalkozok. Részletesebben a ***Debian 3.0 (Woody)***, a ***Mandrake 10.0***, a ***SuSE 9.1*** és a ***Fedora Core 2*** terjesztésről lesz szó.

Mikor frissítsünk?

Honnan tudhatjuk, hogy mikor kell frissítést végeznünk? A legjobb módszer az, hogy feliratkozunk a terjesztésünkkel kapcsolatos biztonsági értesítők levelezőlistájára. Az internetes források között az itt tárgyalt terjesztésekre és a megfelelő biztonsági levelezőlistákra vezető hivatkozások egyaránt megtalálhatók. Ezek általában kis forgalmú listák, általuk a biztonsági jellegű foltokról vagy frissítésekről értesülhetünk. Általában közvetlen hivatkozásokat is tartalmaznak a frissített csomagok letöltéséhez, a csomagok helyességének megőrzését pedig ***MD5*** ellenőrző összegekkel segítik. Ennél a módszernél a csomagokat kézzel kell telepítenünk, és a függőségeket is magunknak kell feloldanunk. A frissítések megjelenéséről úgy is értesülhetünk, hogy írunk egy a frissítéseket rendszeresen lekérdező parancsfájlt. ***SuSE 9.1*** és ***Fedora Core 2*** alatt meglévő programjainkat könnyedén, grafikus felületről tudjuk frissíteni. Debian és Mandrake alá szintén léteznek jól áttekinthető grafikus eszközök, ezeket parancsfájlokkal arra is rávehetjük, hogy az éjszaka közepén töltsék le a frissítéseket, amelyek telepítését a számunkra kényelmes időpontra tolhatjuk el. Muszáj megemlítenem a programok felügyelet nélküli frissítésének veszélyeit. Nálam például az ***Apache*** webkiszolgáló pontos beállítása komoly munkát jelent. Frissítéskor mindig szembesülök a kérdéssel: szeretném-e felülírni meglévő beállító fájljaimat? A legtöbbször a `diff` segítségével átnézem, milyen változtatásokra számíthatok, és a beállító fájl felülírását általában nem engedélyezem. Ha létfontosságú alkalmazásokat is futtatunk, mindig fordítsunk kellő gondot a változtatások rögzítésére, a beállító fájlokról pedig készítsünk biztonsági mentéseket.

RPM alapú terjesztések

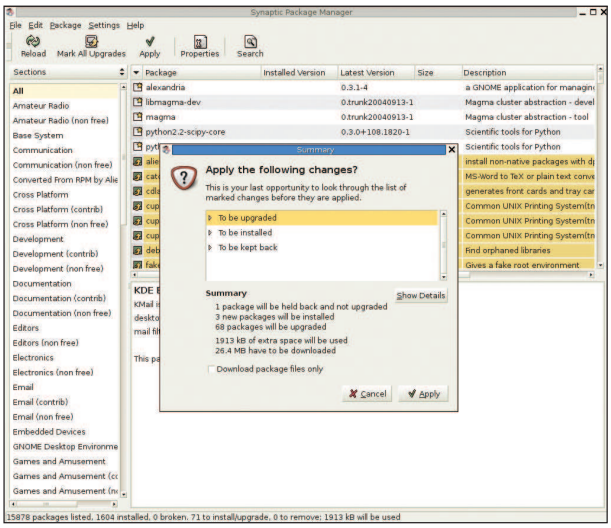
Az ***RPM*** parancssori eszköz megbízható, kézi módszert kínál a biztonsági frissítések telepítésére. Az rpm parancsnak rengeteg kapcsolója van, ám a csomagok frissítéséhez csupán a következő utasítást kell kiadnunk:

```
# rpm -Uv csomag.rpm
```

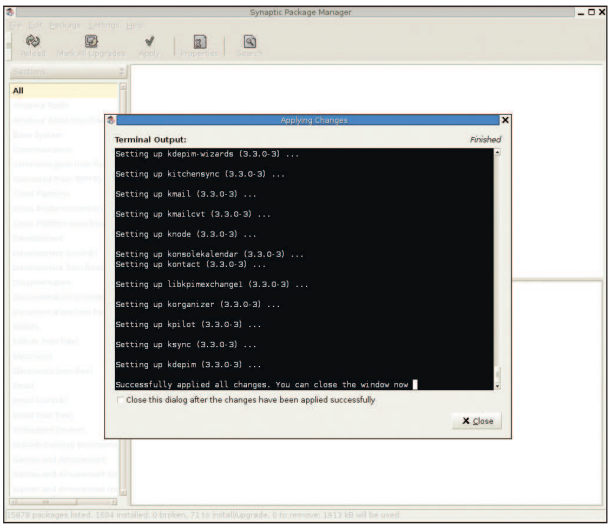
Az ***RPM*** fájl helyi fájl is lehet, de ***FTP***-n vagy ***HTTP***-n keresztül elérhető fájlt is megadhatunk. Ha a biztonsági levelezési listán közvetlen URL-eket kapunk a frissített csomagokra, akkor a parancssori frissítés roppant egyszerűvé válik. Az `rpm` parancssori eszközről az ***RPM*** webhelyen vagy a megfelelő `man` oldalon találunk további tájékoztatást.

Debian alapú terjesztések

A ***Debian*** és az egyéb, ***Debianra*** épülő terjesztések csomagkezelője a `dpkg`. Neve a ***Debian GNU/Linux package***



1. ábra A módosítandó alkalmazások a Synaptic listájában



2. ábra A Synaptic az összes frissítés telepítése után

manager, ***Debian GNU/Linux csomagkezelő*** kifejezésből származik. A `dpkg` ***GYK*** szerint a név mára elveszítette jelentőségét, hiszen a `dpkg`-t nem ***Debian*** rendszerek is használják, sőt, a ***Linuxtól*** eltérő operációs rendszerek alá is létezik. Ez a csomagkezelő lényegében aládolgozik például a ***APT***-nek (***Advanced Packaging Tool, fejlett csomagkezelő eszköz***) és a grafikus eszközöknek, például a ***Synapticnek***. Az ***RPM***-hez hasonlóan a dpkg is milliónyi parancssori kapcsolót ismer, ám mi most csak a frissítésre használhatóval foglalkozunk, amelynek alkalmazásakor a kiadandó parancs a következőképpen fest:

```
# dpkg -i csomag.deb
```

A `-i` kapcsoló a csomag telepítésére utasítja a `dpkg`-t. Ha a csomagból korábbi változat is telepítve van, a `dpkg` először eltávolítja azt, majd felteszi az újabb változatot. Az `rpm`-től eltérően a `dpkg`-nak a csomag telepítés előtti letöltéséhez a wget-re vagy curl-re is szüksége van.

Debian 3.0 (Woody)

Debian alatt csomagkezelő feladataink túlnyomó részét valószínűleg az ***APT*** segítségével fogjuk elvégezni. Az ***APT*** egy listát vezet az elérhető csomagokat tároló forrásokról. Ha egy forrás listájában újabb csomagváltozat szerepel, akkor az ***APT*** letölti a csomagot, majd átadja a vezérlést a `dpkg`-nek. Először ellenőrizzük, hogy a biztonsági frissítések forrása szerepel-e a sources.conf fájlban. A fájlban a következő sornak kell szerepelnie:

```
deb http://security.debian.org/ stable/updates main
```

A `stable` szó helyett lehet, hogy a `woody` szerepel – teljesen mindegy. A ***sources.conf*** fájl átnézése-átírása után frissítenünk kell a rendelkezésre álló csomagok listáját. A frissítés és a foltozás végrehajtásához az apt-get parancsot kétszer kell kiadnunk:

```
# apt-get update
# apt-get upgrade
```

Ekkor csak azoknak a csomagoknak a frissítésére kerül sor, amelyek más csomagok módosítását nem igénylik. Ha a függőségekkel is rendelkező csomagokat is frissíteni akarjuk, a következő parancsokat kell kiadnunk:

```
# apt-get update
# apt-get -u dist-upgrade
```

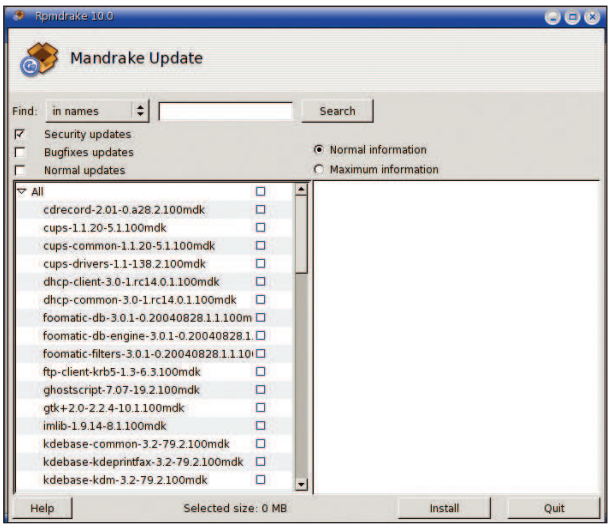
A `-u` kapcsoló segítségével pontosan láthatjuk, hogy mely csomagok kerülnek frissítésre, újonnan telepítésre vagy eltávolításra. A fenti parancsokat `crontab` segítségével is futtathatjuk, valamint arra is rávehetjük gépünket, hogy mindig töltse le a legújabb csomagokat, de ne telepítse őket. A `crontab` fájlba az alábbihoz hasonló parancsot kell beírnunk:

```
(apt-get update && apt-get -dy upgrade)
➥| mail -s "`hostname` frissítés" root
```

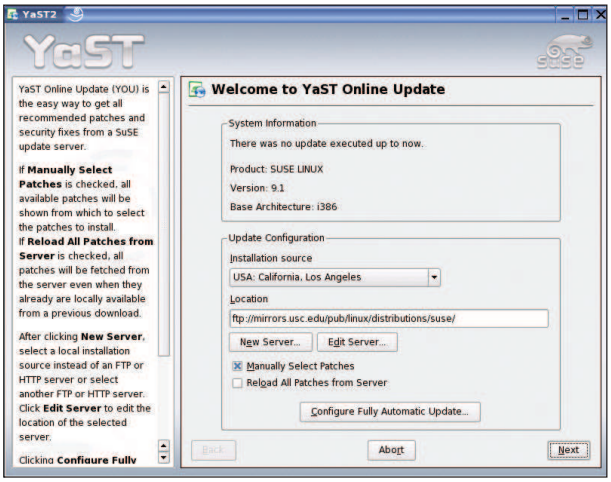
A parancs letölti a legújabb csomagok listáját, és ha ez sikeres, akkor letölti a frissítést igénylő csomagokat is. Az eredményről elektronikus levélben tájékoztatja a root felhasználót. Szükség szerint használjuk saját felhasználónevünket vagy levélcímünket. Ha értesítő levelet kaptunk a frissítésekről, a következő parancsot kell kiadnunk:

```
# apt-get upgrade
```

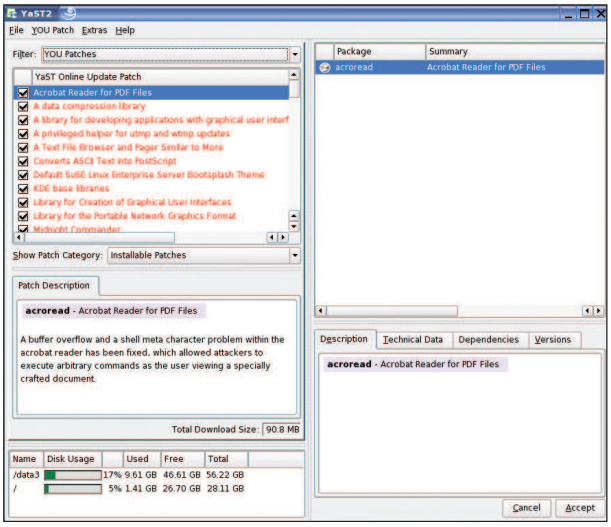
Ekkor megtörténik a korábban letöltött csomagok telepítése, melynek folyamatát konzolról vagy terminálról tudjuk figyelemmel kísérni. Bizonyos csomagok telepítésekor további beavatkozásra is szükség lehet, ezért érdemes lehet tartózkodni a teljes mértékben automatizált módszer használatától.
A grafikus oldalt szemlélve a ***Debiant*** használók számára a ***Synaptic*** teljes értékű felületet biztosít a dpkg-hoz.
A ***Synaptic*** futtatásához ablakkezelőnk ***Debian*** menüjéből az ***Apps›System›Synaptic Package Manager (Alkalmazások› Rendszer›Synaptic csomagkezelő)*** parancsot kell választanunk. A ***Synaptic*** működése sokban hasonlít az ***APT***-éhez. Ha frissíteni szeretnénk a rendelkezésre álló csomagok listáját, kattintsunk az ablak bal felső részén található ***Reload (Újratöltés)*** gombra. Egy ablakban megjelenik a frissített csomaglista tartalma. Amikor a ***Synaptic*** végzett a csomaglisták letöltésével, az összes rendelkezésre álló frissítést megtekinthetjük. A frissítést igénylő csomagokat egy zöld négyzet és egy felfelé mutató nyíl jelzi. Az újonnan elérhető csomagoknál a négyzet-



3. ábra Az rpmdrake listája a rendelkezésre álló csomagfrissítésekről



4. ábra A YaST2 Online Update tükörválasztó folyamata



5. ábra A YaST2 Online Update listája az elérhető csomagfrissítésekről

ben egy sárga csillag látható. A már telepített csomagoknál a négyzet zöld, a még nem telepítetteknél pedig fehér színű.

Ha az összes csomagfrissítést le szeretnénk tölteni és fel szeretnénk telepíteni, akkor kattintsunk az ***Apply (Alkalmaz)*** gombra. Az ezután megjelenő ablakból megtudhatjuk, hogy mely csomagok kerülnek frissítésre, telepítésre, visszatartásra vagy eltávolításra (*1. ábra*). A visszatartott csomagok esetében további, részletesebben meg nem adott függőségekkel kell számolni. Ha rákattintunk az ***Apply (Alkalmaz)*** gombra, megkezdődik a frissítések letöltése. A letöltés után a frissítések telepítését egy terminálszerű szövegterületen követhetjük, az esetleges kérdésekre is itt adhatunk választ. Ha végeztünk, kattintsunk a ***Close (Bezár)*** gombra. (*2. ábra*)

Mandrake 10.0

A ***Mandrake 10.0*** telepítésekor az első bejelentkezés előtti záró lépések egyike a fontosabb frissítések lekérdezése. Ha nulláról indulva telepítjük a terjesztést, akkor mindenképpen szakítsunk időt erre a műveletre. Mit tegyünk azonban, ha Mandrake rendszerünk már telepítve van, és be kellene foltoznunk egy biztonsági rést?

A ***Mandrake 10.0*** használóinak egy csinos, grafikus felületű csomagkezelő alkalmazás áll rendelkezésére, ez az rpmdrake. A ***KDE*** csillag menüjére kattintva, majd a ***System›Configuration›Packaging›Mandrake Update (Rendszer›Beállítások›Csomagkezelés›Mandrake frissítés)*** parancsot választva indíthatjuk el, de a parancssorból root felhasználóként az `rpmdrake` parancsot is kiadhatjuk. Válaszoljuk meg a felbukkanó kérdéseket, és máris megjelenik a biztonsági okból frissítést igénylő csomagok listája. (*3. ábra*) Ha mindegyiket frissíteni szeretnénk, kattintsunk az ***All (Mind)*** sorban található négyzetre, majd az ***Install (Telepít)*** gombra – aztán bontsunk egy sört, és dőljünk hátra. Az összes frissítés letöltése és telepítése után párbeszédpanel értesít a művelet sikeres elvégzéséről. Ilyen egyszerű az egész.

A parancssoros ***urpmi*** csomag nálam a ***Mandrake 10.0*** alapelemeként települt. Az `urpmi` működése sokban hasonlít az ***APT***-éhez, és szintén lehetővé teszi több forrás használatát a csomagok frissítésére. A forrás lehet CD-lemez, helyi ***RPM*** könyvtár, vagy ***FTP*** vagy ***HTTP*** alapú internetes erőforrás. A biztonsági javítások telepítéséhez az alábbihoz hasonló parancsot kell futtatnunk:

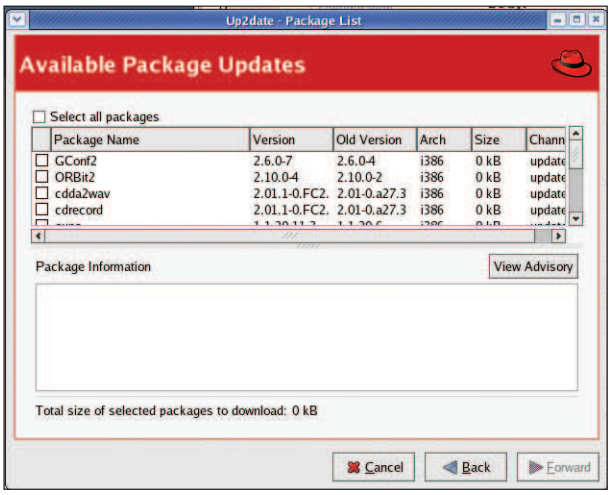
```
# urpmi.addmedia –update updates
➥ftp://pelda.com/Mandrake10.0/RPMS
➥with ../base/hdlist.cz
```

Ezzel egy ***FTP***-tükör biztonsági frissítéseit adhatjuk hozzá a források listájához. Természetesen az ***ftp://*** ***URL***-t egy valós hely címével kell helyettesítenünk. Az ***Easy urpmi*** weboldalról könnyen átlátható, webes felületről választhatjuk ki a hozzánk legközelebb eső tükörhelyet, gépünk típusát és azt, hogy mely forráskészletekből kívánjuk letölteni a frissítéseket.

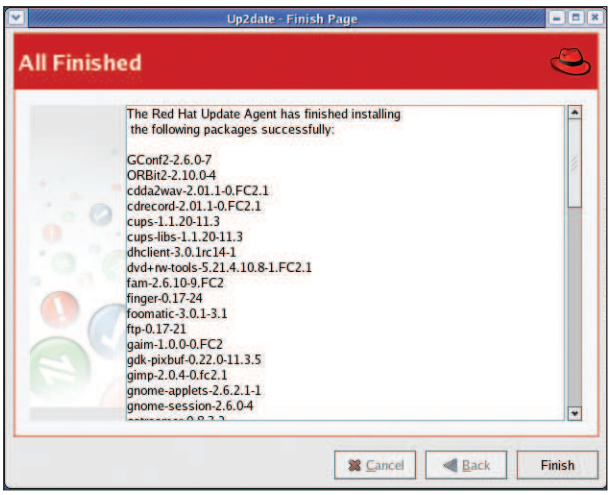
Ha le szeretnénk tölteni az elérhető csomagok listáját, majd telepíteni szeretnénk az összes csomagfrissítést, a következő két parancsot kell kiadnunk:

```
# urpmi.update -a
# urpmi –auto-select
```

Ezután megkezdhetjük a frissített csomagok és a függőségek miatt szükségesnek ítélt csomagok telepítését.



6. ábra Az Up2date listája a rendelkezésre álló csomagokról



7. ábra Az Up2date végzett a letöltéssel és a telepítéssel

SuSE 9.1

A ***SuSE 9.1*** hasonló módszert kínál a frissítések telepítésére, melyben a ***YaST2 Online Update (YOU)*** grafikus eszköz segít bennünket. A ***SuSE*** ikonra, majd a ***System›YaST (Rendszer›YaST)*** parancsra kattintva indíthatjuk el. Írjuk be a root jelszavát, majd kattintsunk a ***Software (Szoftver)*** és az ***Online Update (Online frissítés)*** parancsra. Válasszuk ki a telepítési forrást, vagy adjunk hozzá kézzel egy új kiszolgálót. (*4. ábra*) A ***YOU***-t úgy is beállíthatjuk, hogy minden nap megadott időpontban önműködően töltse le és/vagy telepítse a frissítéseket. A ***Next (Tovább)*** gombra kattintva letölthetjük azokat az adatokat, amelyek alapján felmérhető a frissítést igénylő csomagok köre. A lista frissítése után megkapjuk a csomagok listáját, a foltok leírását és a lemezhely-használattal kapcsolatos adatokat. (*5. ábra*) A foltok listájában vörös vonalak jelzik a biztonsági frissítéseket, kék vonalak az ajánlott frissítéseket és feketék az elhagyhatókat. A rendszerfrissítést az ***Accept (Elfogad)*** gombbal indíthatjuk el. Ha a frissítés befejeződött, kattintsunk a ***Finish (Befejez)*** gombra, ezt követően még sor kerül néhány rendszerszolgáltatás beállítására. A ***YOU*** mellett, ha akarjuk, a parancssorból az `rpm` parancsot is használhatjuk.

Fedora Core 2

A ***Red Hat*** frissítő ügynöke, az `up2date` számos ***Red Hat*** terjesztésben szerepelt, és a ***Fedora Core 2***-ben is megtalálható. Ha ***Fedora Core 2*** alatt le szeretnénk kérdezni az elérhető frissítéseket, akkor kattintsunk az egér jobb gombjával a rendszertálcán található piros felkiáltójelre, majd válasszuk a ***Check for updates (Frissítések lekérdezése)*** parancsot. A legújabb frissítések letöltését és telepítését a piros felkiáltójelre az egér jobb gombjával kattintva és a ***Launch up2date (up2date indítása)*** parancsot választva indíthatjuk el. Adjuk meg az alapbeállításokat. Az `up2date` első futtatásakor a program megkérdezi, hogy telepíteni akarjuk-e a ***Red Hat GPG*** kulcsaláírását. Én a saját gépemen igennel válaszoltam. A ***Channels (Csatornák)*** menüben két csatornára vagy frissítésforrásra iratkozhatunk fel, ezek a ***fedora-core-2*** és az ***updates-released-fc2***. Az `up2date` csatornái hasonlók az ***APT*** vagy az `urpmi` forrásaihoz. Következőként megadhatjuk az átlépni kívánt csomagokat. Nálam az eleve megjelenő csomag egy rendszermagfrissítés volt. A ***Forward (Tovább)*** gombra kattintva megkapjuk az elérhető frissítések listáját. (*6. ábra*) Ha az összes frissítést telepíteni akarjuk, akkor jelöljük be a ***Select all packages (Minden csomag kijelölése)*** jelölőnégyzetet.

Újra a ***Forward*** gombra kattintva elindíthatjuk a csomagok letöltését. Ezen a ponton megismételném a sörözéssel és a pihenéssel kapcsolatos ajánlatomat. Ha a letöltés befejeződött, újfent kattintsunk a ***Forward*** gombra, ezzel elindítjuk a telepítést. Ha a telepítés is véget ért, a program megjeleníti, hogy pontosan mely csomagokat és milyen számú változatban telepítette. (*7. ábra*)

A ***Fedora Core 2*** ugyancsak ***RPM*** alapú, vagyis terminál alól használhatjuk az rpm parancsot is.

Egy további ismert csomagkezelő felület a ***Yellow dog Updater Modified***, röviden ***Yum***. A ***Yum*** sokban hasonlít az ***APT***-hez, ám sokban el is tér tőle, a különbségeket a szerző részletesen ismerteti a ***Yum*** weboldalon. A ***Yum*** az `urpmi` és az ***APT*** esetében látottakhoz hasonló csomagforrásokkal dolgozik, és a csomagok telepítését az ***RPM***-re bízza. Az ***anaconda*** telepítő ***Python*** kötéseket használ az ***RPM*** elérésére, így a ***Python*** támogatásának fennmaradására bátran számíthatunk.

Összefoglalás

Van egy mondás a baseballban: „Annyira vagy jó, amennyire az utolsó ütésed.” A számítógépek világában ezt úgy fogalmazhatnánk meg, hogy egy gép annyira biztonságos, amennyire az utolsó frissítés révén azzá vált. Egy jó tűzfal vagy egy mágneskártyás beléptetős bejárat kiváló kezdő lépés a biztonság megteremtése felé, ám ne feledjük, ha elmulasztjuk a frissítések telepítését, és elavult ***Apache***- vagy ***OpenSSH***-változatot futtatunk, teljes rendszerünk veszélybe kerülhet.

Linux Journal 2005. január, 129. szám

Jeremy Turner több mint öt éve használja a Linuxot. Szenvedélye, hogy segítsen másokat a nyílt alkalmazások megismerésében. PHP-ben programoz, egy kórusban első tenor, rengeteg baseballt néz, elektronikus leveleit pedig rendszeresen olvassa (jeremy@linuxwebguy.com).