A SUSE 10.0 biztonsági szolgáltatásai

A SUSE terjesztés a biztonság híve – rengeteg biztonsággal kapcsolatos eszközt kínál.

Az évek során tapasztalhattuk, hogy egyre több és jobb biztonsági szolgáltatást építenek be a kedvenc ***Linux*** terjesztéseinkbe. A terjesztésfüggő biztonságtudatosság számos formában jelenik meg, például

- A biztonságnövelő alkalmazások elérhetőségében.
- A telepítő parancsfájlok „megerősítő" működésében
- A foltok kezelésének módjában
- A hálózati alkalmazások alapértelmezett beállításaiban

Ebben a hónapban egy három cikkből álló sorozatot indítunk a ***SUSE Linux***, a ***Debian GNU/Linux*** és a ***Red Hat Enterprise Linux*** terjesztésre jellemző biztonságáról. Ezzel a három terjesztéssel szereztem a legtöbb tapasztalatot, és sokak szerint ez a három a legnépszerűbb.
Kezdjük a ***SUSE 10.0***-val. A ***SUSE*** egy általános célú, kereskedelmi kiadású ***Linux*** terjesztés, amelyet 32 és 64 bites ***Intel*** környezetekhez fejlesztettek.
A ***Novell*** tulajdonába került ***SUSE*** eredetileg ***Németországból*** származik, és jórészt ma is ott fejlesztik. Számos különböző ***SUSE*** termék létezik: a ***SUSE Linux***, amely kiskereskedelmi forgalomban elérhető „személyes" változat; a ***SUSE Linux Enterprise Server***, egy „vállalkozás-szintű" változat, amely közvetlenül a ***Novelltől*** szerezhető be; és az ***OpenSUSE***, amely gyakorlatilag megegyezik a ***SUSE Linuxszal***, de telepítő hordozók (csak az interneten keresztül lehet telepíteni), nyomtatott kézikönyvek és telepítési támogatás nélkül.
A cikk alapjául a ***SUSE Linux 10.0***, vagyis a kereskedelmi „személyes felhasználású" változat szolgál. Az itt leírtakat elvileg azonos módon lehet alkalmazni az ***OpenLinux 10.0*** változatban, és a ***SUSE Enterprise*** változataiban is jórészt helytállónak kell lenniük. Az ***Enterprise*** változatok feltételezhetően további biztonsággal kapcsolatos csomagokat és szolgáltatásokat tartalmaznak.

A SUSE Linux 10.0 telepítése

A rendszerbiztonság a telepítésnél kezdődik. Itt van először lehetőségünk lényeges döntéseket hozni arról, hogy milyen szerepet szánunk a rendszernek, hogy milyen programrendszert futtatunk majd, illetve hogy milyen beállításokat határozunk meg a rendszerben. Ezért nem árt, ha a telepítési folyamatnál kezdjük a SUSE biztonságának tárgyalását.
A ***SUSE*** összes változata a ***YaST***-ot (***Yet Another Setup Tool***) használja, a rendszer először telepítéséhez és a folyamatos rendszerfelügyelethez egyaránt. Az évek során a ***YaST*** egyszerű ***RPM*** felhasználói felületből (front end) egy moduláris, átfogó felügyeleti eszközzé vált, amely nem csak alacsony szintű rendszerprogramok, hanem összetett kiszolgáló alkalmazások, például az ***Apache*** és a ***Postfix*** beállítására is alkalmas.
Rövidesen bővebben is szót ejtünk a ***YaST***-ról, az operációs rendszer első telepítésekor azonban a legsürgősebb probléma annak eldöntése, hogy melyik programcsomagot telepítsük.
Ha valaki a biztonságot tartja a legfontosabbnak, akkor ez kellemes probléma. A ***SUSE Linux 10.0*** széles választékot kínál a biztonsági alkalmazásokból – ezek közül válogathatunk.
Megítélésem szerint ezek az alkalmazások két csoportra oszthatók: rendszer-biztonság-alkalmazásokra és biztonság-pásztázó alkalmazásokra. Az előbbiekhez tartoznak a hatékony biztonsági szolgáltatásokkal rendelkező általános célú alkalmazások – a ***Postfix*** a legkézenfekvőbb példa –, valamint az olyan alkalmazások, amelyek fő célja az, hogy biztonsági vezérlőeszközöket biztosítsanak más alkalmazások vagy a mögöttes operációs rendszer számára – tipikusan ilyen például a ***tcwrappers***. Az *1. Táblázat* a ***SUSE Linux 10.0*** biztonságot erősítő csomagjait sorolja fel.
Az *1. Táblázat* hosszú csomaglistája valójában csak bizonyos személyes kedvenceket és néhány ***SUSE***-ra jellemző választást tartalmaz. A ***SUSE***-ban sokkal, sokkal több biztonsági eszköz található, például a ***tcpd (tcpwrappers)***, az ***openssl***, a ***chkrootkit***, a ***sudo*** és a ***wipe***. A ***SUSE Linuxba*** épített csomagok teljes felsorolását a ➲ ***www.novell.com/products/linuxpackages/professional/index_all.html*** címen tekinthetjük meg.
Azon kívül, hogy biztonságossá tesszük azt a rendszert, amelyre a ***SUSE***-t telepítjük, érdemes lehet más rendszerek vagy akár teljes hálózatok biztonságát is ***SUSE*** rendszerrel megerősíteni. A ***SUSE*** remekül alkalmazható erre a feladatra. A *2. Táblázat* olyan ***SUSE Linux 10.0*** csomagokat mutat be, amelyeket biztonsági pásztázásra használhatunk. Ügyeljünk, hogy ezeket a csomagokat (talán a ***Snort*** kivételével) soha nem szabad internetre kapcsolódó kiszolgálón telepíteni. Ilyen környezetben a csomagok a támadóknak nagyobb hasznot jelentenek, mint nekünk. A programok pásztázását olyan rendszerről kell végezni, amely egyébként nincs veszélyben.
Annak, aki most ismerkedik a ***SUSE***-

1. táblázat *Néhány SUSE Linux 10.0-hoz tartozó biztonságnövelő csomag*

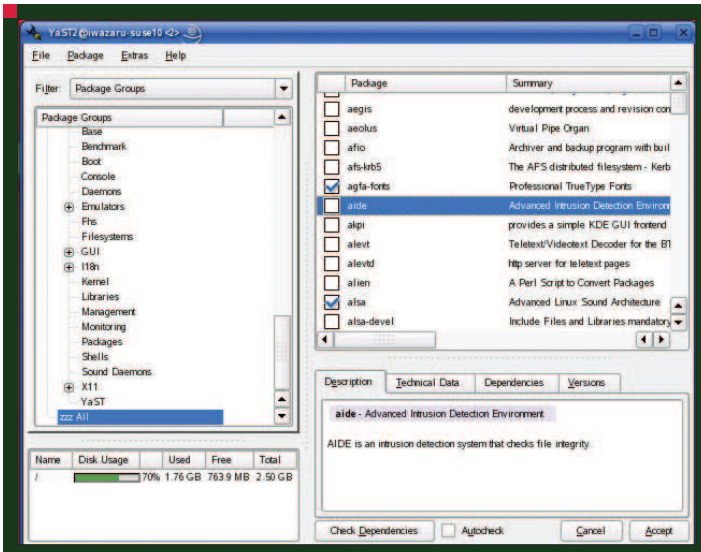
Csomag neve	Leírás
aide, fam	A fájlok épségét ellenőrzik - mindkettő a hasonlít a Tripwire-re
bind-chrootenv	Automatikusan létrehoz egy chroot környezetet, amelyben a BIND (a DNS démon)biztonságosabban futhat.
clamav, antivir	Vírusölő csomagok – a clamav teljesen ingyenes, de az antivir kereskedelmi program (személyes használatra ingyenes).
cracklib	Olyan könyvtárak és eszközök, amelyek megakadályozzák, hogy a felhasználók könnyen kitalálható jelszavakat válasszanak.
gpg, gpg2, gpa	A GNU Privacy Guard (gpg) egy sokoldalú és elterjedt e-mail-, illetve fájltitkosító eszköz.
ipsectools, openswan	IPsec alapú virtuális magánhálózat építésére szolgáló eszközök.
openldap, freeradius	Nyílt forráskódú hitelesítő démonok.
proxy-suite	A SUSE által fejlesztett biztonsági FTP-proxy.
seccheck	A SUSE által testreszabott cron parancsfájlok, amelyek különböző biztonsági ellenőrzéseket futtatnak naplófájlokon, a rendszerállapoton és egyebeken, majd e-mail jelentéseket küldenek.
subdomain-utils, subdomain-profiles, mod-change-hat és más csomagok	Az AppArmor egy kötelező hozzáférés-vezérlés (Mandatory Access Control – MAC) rendszer, amely korlátozza bizonyos bináris fájlok viselkedését. A SUSE ezt használja az SELinux helyett, amelyre nagyon hasonlít.
squid, SquidGuard	A Squid népszerű HTTP/HTTPS proxy. A SquidGuard hozzáférés-vezérlést és egyéb biztonsági szolgáltatásokat kínál.
SUSEfirewall	A SUSE kényelmes felhasználói felülete a Linux netfilter-hez illetve iptables-hez.
syslog-ng	A syslogd-nél jóval hatékonyabb fejlett rendszernaplózó. A syslog-ng a SUSE alapértelmezett naplózója.
tinyca2	Az OpenSSL felhasználói felülete, amely a tanúsítvány hatóságok kezelésére szolgál.
yast2-firewall	Tűzfal szolgáltatás.
vsftpd	Very Secure FTP Daemon
xen, FAUmachine, uml-utilities, bochs	A Xen, a FAUmachine, a User Mode Linux és a BOCHS virtuális gép (virtual machine) környezetek.

val, tudnia kell, hogy a ***YaST*** alapértelmezésben a ***Selections (Válogatás)*** szűrőt (nézetet) alkalmazza, amelyben a rendelkezésre álló csomagok csak egy kisebb részét kínálja fel. Ha valami, ami számunkra szükséges – például a ***nessus-core*** – nem szerepel ebben a nézetben, a ***Pacakage Groups (Csomagcsoportok)*** szűrő segítségével a kategóriák egy teljesebb halmazát jeleníthetjük meg. Amennyiben az összes csomagot egyetlen listában, betűrendben szeretnénk látni, egyszerűen válasszuk a szűrő Package Groups beállítását, majd kattintsunk a *zzz* ***All (Összes)*** csoportra (*1. ábra*). A szűrő ***Search (Keresés)*** beállításával név vagy kulcsszó alapján kereshetünk csomagokat.

2. táblázat *A SUSE Linux 10.0-ban használt biztonsági pásztázók*

Csomag neve	Leírás
ethereal, tcpdump	Kitűnő csomagfigyelő
fping	Elárasztásos ping (több célpontú ping)
john	John the Ripper – jelszófeltörő eszköz (gyenge jelszavakat azonosítására használható jogszerűen).
kismet	Vezeték nélküli LAN-figyelő
nessus-core, nessu-libraries	Nessus – általános célú biztonsági pásztázó
snort	Kiváló csomagfigyelő, csomagnaplózó és betörésérzékelő rendszer

Az összes programcsomag kijelölése és telepítése után a ***YaST*** lehetővé teszi a rendszergazda jelszó beállítását és az első (nem rendszergazda) felhasználói fiók létrehozását. A ***SUSE*** alapértelmezésben a ***Blowfish***-t



1. ábra A YaST összes rendelkezésre álló csoportjának megtekintése

használja a jelszavak titkosításához, a ***YaST*** pedig ellenőrzi a begépelt jelszó bonyolultságát. (A túl egyszerű jelszavakat a támadók könnyen kitalálhatják vagy nyers erővel feltörhetik.)
A helyi tűzfal-parancsfájlok (alaphelyzetben engedélyezett), valamint az ***SSH*** és a ***VNC*** távoli héj démonok (alaphelyzetben mindkettő tiltott) engedélyezésére is lehetőségünk van. Megjegyzendő, hogy az utóbbi kettő közül az ***SSH*** a legalkalmasabb a bástya gépek (megerősített internetes kiszolgálók) felügyeletére – egyebek mellett azért, mert – hacsak nincs valamilyen nagyon különleges és nagyon megkerülhetetlen indokunk – bástyagépeken nem szabad ***X Window*** rendszert használni. Ki kell emelni, hogy a ***YaST*** tökéletesen fut szöveges (***ncurses***) üzemmódban, az X változattal pontosan megegyező modulokkal és lehetőségekkel. Ráadásul, a ***SUSE***-hez tartozó ***VNC*** távoli asztal változat, a ***tightvnc*** csak a hitelesítési adatokat titkosítja, a munkamenet-adatokat nem.
Azt is meg kell említeni, hogy a telepítéskor nincs lehetőségünk a helyi tűzfalbeállítások testreszabására. Kezdetben egy alapértelmezett parancsfájl érvényesül, amely egy egyszerű „összes kimenő művelet engedélyezése, összes nem helyben kezdeményezett bejövő forgalom tiltása” szabályrendszert biztosít. Más szóval, az alapértelmezett ***SUSEfirewall*** parancsfájl tökéletesen megfelel a legtöbb asztali rendszeren, de kiszolgálón történő használathoz nem alkalmas. A ***YaST Firewall (Tűzfal)*** modulját futtatva ezt később megváltoztathatjuk.
A ***YaST*** ezután a következő módszereket biztosítja a nem rendszergazda felhasználók hitelesítésére:

- helyi /etc/passwd fájl (alapértelmezett)
- LDAP
- NIS
- Samba (Windows NT tartományok)

A ***SUSE Linux 10.0*** az ***Active Directory*** hitelesítést és lehetővé teszi, a ***Kerberoson*** keresztül.
A hitelesítési módszer kiválasztása után létrehozhatjuk az első nem rendszergazda felhasználói fiókot. Ügyeljünk, hogy az ***Automatic Logon (Automatikus bejelentkezés)*** lehetőséget hagyjuk tiltott állapotban, kivéve, ha a rendszer biztonsági követelményei valóban nagyon alacsonyak. Ha engedélyezzük ezt a lehetőséget, a számítógép induláskor automatikusan belépteti a nem rendszergazda felhasználót. (Csak a nyilvános – ***kiosk*** – típusú rendszerek esetében tudom elképzelni, hogy ez hasznos lehet.)

3. táblázat ***Biztonsághoz kapcsolódó YaST modulok***

YaST csoport	Modul neve	Leírás
Software (Programok)	Online Update (Hálózati frissítés)	Kézi és automatikus programfrissítések beállítására szolgál
	Software Management (Programkezelés)	Csomagok telepítésére és eltávolítására szolgál.
	Virtual Machine Installation (Virtuális gép telepítés – XEN)	Virtuális gépeket hoz létre a Xen 3 virtuális gép környezet számára
System (Rendszer)	/etc/sysconfig Editor (Szerkesztő)	Démonok indítási paramétereit szerkeszti
	System Services (Runlevel) – Rendszerszolgáltatások (Futási szint)	Indító parancsfájlok kezelésére szolgál
	Powertweak	További rendszermag-paramétereket, például TCP timewait aljzatokat állít be
Network Services (Hálózati szolgáltatások)	DNS Server (DNS kiszolgáló)	A BIND beállítására szolgál

3. táblázat *folytatás*

YaST csoport	Modul neve	Leírás
Network Services (Hálózati szolgáltatások)	HTTP Server (HTTP kiszolgáló)	Az Apache beállítását végzi
	LDAP Client (LDAP ügyfél)	LDAP hitelesítést és kereséseket határoz meg
	Mail Transfer Agent (Levéltovábbító ügynök)	Beállítja a Postfixet vagy a Sendmailt
	Kerberos Client (Kerberos ügyfél)	Kerberos hitelesítés, többek között Active Directory beállítására szolgál
	Remote Administration (Távoli felügyelet)	Beállítja a TightVNC-t
Novell AppArmor	Various (Vegyes)	Az AppArmor kötelező hozzáférés-vezérlés kezelésére szolgál meghatározott bináris fájlokon.
Security and Users (Biztonság és felhasználók)	Firewall (Tűzfal)	Netfilter/iptables beállítások kezelésére szolgál.
	Local Security (Helyi biztonság)	Meghatározza a jelszavak bonyolultságát illetve hosszát, a jelszó-öregedést, fájl-hozzáférés sémákat és egyéb más rendszerbiztonsági paramétereket.
	Group Management (Csoportkezelés)	Csoportfiókok létrehozására, szerkesztésére és törlésére szolgál.
	User Management (Felhasználó-kezelés)	Felhasználói fiókok létrehozására, szerkesztésére és törlésére szolgál (valójában megegyezik a Group Management modullal, ami kettős célt szolgál).

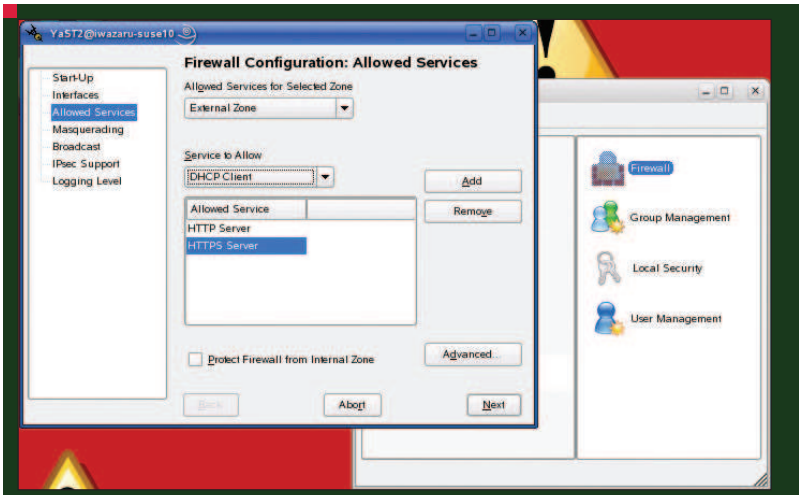
Készen is vagyunk: befejeződött a ***SUSE*** telepítése. A biztonságtudatos rendszergazda feladatai azonban nem érnek véget itt.

Biztonsághoz kapcsolódó YaST modulok

Az újonnan felhúzott ***SuSE Linux*** rendszer első indításakor azonnal jelentkezzünk be a jogokkal nem rendelkező felhasználóval, és hívjuk meg a ***YaST***-ot. Ha ezt a ***KDE***-ből vagy a ***GNOME***-ból tesszük, a rendszer automatikusan kéri a rendszergazda jelszót, de szövegkonzolos munkamenetben a `su -c` parancsot kell alkalmazni az ***/sbin/yast*** fájl hívásához.
Ahogy korábban említettem, a ***YaST*** számos beépített biztonsági szolgáltatással rendelkezik. A *3. Táblázat* a rendszerbiztonság szempontjából kifejezetten fontos ***YaST*** modulokat sorolja fel.
A fenti ***YaST*** modulok közül az ***Online Update*** az egyik legfontosabb. Érdemes azonnal alkalmazni az automatikus foltletöltések, valamint – ha a rendszerben nem működik változtatásvezérlő folyamat – az automatikus folttelepítések beállításához. A ***YaST Online Update*** volt az első, egy nagyobb ***Linux***-terjesztés által kínált automatikus folt eszköz, és még ma is az egyik legjobb. A használatával élvezhetjük a ***SUSE*** azon kiváló gyakorlatának előnyeit, amely során friss és jól ellenőrzött foltokat bocsát rendelkezésre.
A ***Firewall*** modul (*2. ábra*) szintén rendkívül hasznos, különösen akkor, ha valaki nem szívesen hoz létre és kezel saját tűzfal-parancsfájlokat (elismerem, hogy kevés az olyan ember, aki hozzám hasonlóan izgalmasnak és szórakoztatónak találja ezt).
A ***Group/User Management*** hasonlóképpen feleslegessé teszi, hogy valaha kézzel kelljen szerkeszteni a ***/etc/group*** vagy a ***/etc/passwd*** fájlt.
A ***Virtual Machine*** modul és a ***Novell AppArmor*** csoport szintén különösen említésre méltó. Olyannyira, hogy érdemes némi időt szánni a ***SUSE*** virtuális gép illetve kötelező hozzáférés-vezérlés rendszereinek részletesebb tárgyalására.

Virtuális gépek a SUSE Linuxban

Lehet, hogy vannak, akik emlékeznek a ***„The Future of Linux Security" (A Linux biztonság jövője – Linux Journal, 2005. augusztus)*** című cikkemre, amelyben virtuális gép környezeteket és hypervisorokat (más néven biztonsági megfigyelőket) vizsgáltam a rendszerbiztonság fontos, új irányvonalaként. Ha valaki nem emlékezne, összefoglalva az volt az indok, hogy a ***MAC*** (kötelező hozzáférés-vezérlés) sémákat, például az ***SELinuxot*** sokan túl bonyolultnak tartják. Egyszerűbb megoldás, ha minden nagyobb alkalmazást vagy szolgáltatást saját virtuális gépen futtatunk. Így ha az a virtuális gép, amelyben például a ***Sendmail*** fut, veszélyeztetett, az ***Apache2***-t fizikailag azonos vason futtató virtuális



2. ábra A YaST Firewall modulja

gép nem kerül azonnali vagy közvetlen veszélybe.
A virtuális gépek ezért hatékony és könnyen érthető módszert biztosítanak a bonyolult alkalmazások egymástól történő elkülönítéséhez.
A ***SUSE Linux*** pedig nem kevesebb, mint három különböző virtuális gép eljárást tartalmaz.
A ***SUSE*** „technológiai előzetesként" biztosítja a ***Cambridge University*** berkeiből származó ***Xen 3*** környezetet. Amennyire meg tudom állapítani, ez csupán annyit jelent, hogy mivel a ***Xen 3*** kiforratlan és esetleg ingatag alkalmazás, a ***SUSE*** egyszerűen nem akar hiú reményeket kelteni az emberekben a használhatóságát illetően – a ***Xen 3 SUSE Linux 10.0***-ban szereplő változata nem különleges előzetes–, illetve próbaváltozat vagy ehhez hasonló. A ***Xen 3*** a ***Linux***, a ***FreeBSD***, a ***NetBSD*** és a ***Plan9*** „vendég-" (virtuális) rendszereket támogatja.
Másik lehetőségként a ***FAUmachine*** virtualizáló környezet olyan ***RPM*** csomagokat tartalmaz, amelyek a ***SUSE 9***, a ***Debian 3.0***, az ***OpenBSD 3.5/3.6*** és a ***Red Hat 9*** vendégrendszer támogatását teszi lehetővé. A ***FAUmachine*** egyik előnye a ***Xen 3***-mal szemben az, hogy a ***FAUmachine***-nál a vendégrendszerek magjai nem rendszergazda (jogokkal nem rendelkező felhasználó) hozzáféréssel futnak a gazdarendszeren.
A ***User Mode Linux*** egy újabb virtualizáló környezet, amelyet a ***SUSE Linux 10.0*** az ***uml-utilities*** csomagon keresztül biztosít.
A ***FAUmachine***-hoz hasonlóan a vendég rendszermagok rendszergazda jogok nélkül futnak.

Novell (Immunix) AppArmor

Ennek ellenére nem mindenki mondott le a ***MAC***-alapú rendszerbiztonságról, ráadásul a ***SUSE*** az ***Immunix AppArmor*** (más néven ***Subdomain***) alkalmazásának megvásárlásával és újracsomagolásával elegánsan lefedte ezt a területet. Az ***AppArmor az SELinuxhoz*** hasonlóan lehetővé teszi bizonyos folyamatok viselkedésmódjának korlátozását, hasonló eredménnyel, de hatékonyabban, mint ha ***chroot*** ketrecekben futtatnánk azokat. (Érdemes megjegyezni, hogy ugyan a ***SUSE***-ben rendelkezésre áll a ***libselinux*** csomag, az alapértelmezett rendszermagban pedig szerepel az ***SELinux*** működés, hivatalosan a ***SUSE*** Linux mégsem támogatja az ***SELinuxot***.
Az ***SELinux SUSE Linuxban*** történő futtatásához a ➲ ***www.cip.ifi.lmu.de/~bleher/selinux*** címen elérhető csomagokra van szükség.
A ***subdomain-docs*** csomagban található ***/usr/share/doc/packages/subdomain-docs/ug_apparmor.pdf*** dokumentum az ***AppArmor*** használati útmutatója, ami az ***AppArmor*** beállításával és használatával kapcsolatos összes tudnivalót leírja. Egyelőre elég annyit elmondani, hogy ha egyszerűen futtatjuk a ***YaST AppArmor Control Panel (Vezérlőpult)*** modult, és engedélyezzük az ***AppArmort***, betöltődik egy alapértelmezett profil, amely számos elterjedt démon és parancs – például ***netstat***, ***ping***, ***traceroute***, ***firefox***, ***evolution***, ***gaim***, ***syslogd***, ***acroread***, ***ethereal***, ***appropos***, ***procmail***, ***postfix*** (***smtpd*** és számos más), ***Apache2*** (***httpd2-prefork***), ***nscd***, ***identd***, ***ntpd***, ***sshd*** és ***squid*** – beállításait tartalmazza.
Ez az ***AppArmor*** egy korlátozott szolgáltatásokkal ellátott változata, tehát nyilvánvalóan a teljes, 1250 dolláros US változatban elérhető szolgáltatásoknak csupán egy részét biztosítja. Számomra viszont nem teljesen világos, hogy pontosan mi a különbség – minden, amit a ***SUSE Linux 10.0*** változattal kipróbáltam, rendesen működött, tehát nem valószínű, hogy ez egy jelentősen lebutított kiadás lenne. Elképzelhető, hogy a teljes változatban több előre beállított alkalmazás található.

Összegzés

A cikkben nem szerepel a ***SUSE Linux 10.0*** összes biztonsági szolgáltatása. Nem beszéltem arról, hogy sok alkalmazás mennyire biztonságos alapértelmezett beállításokkal rendelkezik (általában elég biztonságosak – amikor csak lehetséges, a démonok nem rendszergazda hozzáféréssel futnak, az olyan hálózati figyelők, mint az ***sshd*** általában alapértelmezésben tiltottak, és még sorolhatnám).
A ***SUSE Linux*** ezen változata valóban nagyon biztonságbarát. Ne feledjük azért, hogy a valódi biztonság kulcsa a mi kezünkben van – a ***SUSE*** biztonsági lehetőségeinek csak kis része valósul meg, amíg azokat nem állítjuk be vagy legalább engedélyezzük saját magunk! Remélhetőleg ez a cikk segít az olvasóknak képet alkotni, hogy milyen nagyok ez a lehetőségek.
A következő hónapban a ***Debian 3.1***-ről lesz szó. Addig is mindenki vigyázzon magára!

Linux Journal 2006., 144. szám

Mick Bauer
(darth.elmo@wiremonkeys.org)
Hálózatbiztonsági mérnök az Egyesült Államok egyik legnagyobb bankjánál. Az O'Reilly kiadó gondozásában megjelent Linux Server Security 2. kiadásának (korábbi címén Building Secure Servers With Linux) szerzője, időnként előadóként vesz részt informatikai biztonsági konferenciákon, valamint a „Network Engineering Polka" zeneszerzője.