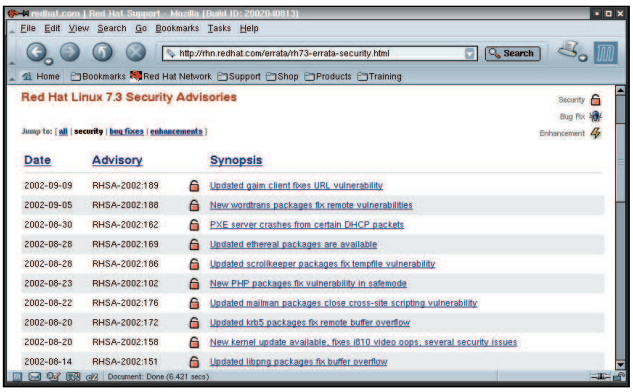
Biztonsági öveket becsatolni!

Amint rászabadulunk a Világhálóra, célpontjai lehetünk a kívülről érkező támadásoknak.

A Linux biztonsági szempontból alapvetően abban különbözik a Windows 95/98/ME rendszerektől, hogy senki sem teheti azt, ami éppen az eszébe jut. A rendszergazdát kivéve mindenkire komoly megkötések vonatkoznak. Nemcsak az, hogy az egyik felhasználó nem túrhat a másik felhasználó „cuccába”, de semmi olyasmit sem csinálhat, ami a rendszer biztonságát, illetve üzembiztosságát csak a legkisebb mértékben is veszélyezteti. A Windows esetében (kivéve az NT-ket és a 2000-et) semmi ehhez hasonló kijátszhatatlan védelemmel nem találkozhatunk. A Linuxban viszont ezek a védelmi módszerek mélyen az operációs rendszerben találhatók, tehát nincs út a kikerülésükre.

Biztonsági kiskáté

Legalábbis elméletileg. A Linuxot és alkalmazásait is emberek írták, tehát előfordulhatnak bennük hibák. Ezek a hibák (még a unixos időkből származó nevükön bugok) általában veszélytelenek, viszont nem egyszer volt rá példa, hogy ilyen programhibák kihasználásával olyan jogosultságokat lehetett szerezni a rendszerben, amilyen eredetileg nem járt volna nekünk.
Félreértés ne essék: a Linux biztonságos rendszer, de csak akkor, ha odafigyelünk bizonyos dolgokra. Hogy pontosan mire is, ez lesz sorozatunk jelenlegi részének témája.
Manapság az Internetről érkező legnagyobb fenyegetést a különböző vírusok, illetve trójai programok jelentik. A Windows CE (95/98/ME) rendszerekben az a gond, hogy a felhasználó bármiféle megkötés nélkül bármelyik állományt átírhatja, törölheti stb. A Linux- (és a Unix-) rendszerekben azonban az a bevált szokás, hogy a felhasználó egyetlen program binárisába sem piszkálhat bele. Sőt, írásjoga csak a saját könyvtárára van és az alkalmazásokhoz tartozó személyes beállításait is kizárólag itt tárolhatja.
Ez a módszer hatékony védelmet nyújt a vírusokkal szemben. Ha egy átlagos felhasználó (azaz nem rendszergazda) elindít egy vírust tartalmazó programot, az nem képes más alkalmazásokat megfertőzni, mivel a felhasználónak nincs írási jogosultsága, csak olvasni és végrehajtani tud. Ha azonban rendszergazdaként indítjuk el ugyanazt a fertőzött programot, kellemetlen helyzet állhat elő: a vírus tetszés szerint bármelyik másik alkalmazásba is befészkelheti magát.
Ezért a legfontosabb alapszabály, hogy sohase lépjünk be fölöslegesen rendszergazdaként, csak akkor, ha feltétlenül szükséges! Ha valamilyen rendszerbeállítást szeretnénk megváltoztatni vagy egy új alkalmazást telepíteni, azt természetesen csak rendszergazdaként tehetjük meg. De sohase böngésszünk rendszergazdai jogosultságokkal az Interneten, és így bejelentkezve ne indítgassunk el innen-onnan szerzett programokat! Ez az oka annak, hogy a legtöbb terjesztés már a telepítés folyamán létrehozat velünk egy saját felhasználót, amellyel majd dolgozni fogunk.
A másik fontos feladat jelszavunk helyes megválasztása és titokban tartása. A Linux- (és a többi Unix) rendszer távolról is felügyelhető, azaz nincs olyan dolog, amit csak a konzolról tudnánk megtenni. Ha gépünk futtat `telnet`, illetve `ssh`



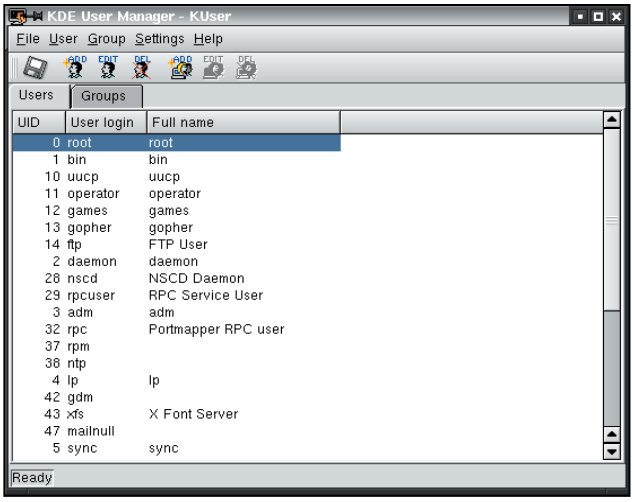
Legalább havonta egyszer keressük fel a Linux honlapját, és nézzük meg, milyen új hibákra derült fény az elmúlt időszakban

(a `telnet` titkosított „változata”) szolgáltatást, a megfelelő jelszavak ismeretében bárki megkaphatja Linuxunk parancssorát. Igaz, általában nincs megengedve, hogy távolról közvetlenül rendszergazdaként jelentkezzünk be. Először ezt a saját felhasználói nevünkön kell megtennünk, majd az `su` parancs kiadásával és a rendszergazdai jelszó begépelésével kaphatjuk meg a rendszergazdai parancssort.
Akinek jelszavaink a birtokába kerülnek, annak csak pillanatnyi IP-címünket kell kiderítenie, és már gyakorolhatja is az uralmat gépünk felett. Ezért ne használjunk könnyen kitalálható jelszót, sőt ha erős üldözési mániánk van, a `telnet`, illetve az `ssh` szolgáltatás elérését akár korlátozhatjuk is (ennek miként jét rövidesen részletesen is bemutatjuk).
Ha ezt a két irányelvet betartjuk, máris sokat tettünk rendszerünk biztonsága érdekében, de még korántsem mondhatjuk atombiztosnak.

Egy kis démonológia

A rendszerekbe ugyanis úgy is be lehet törni, hogy kihasználják bizonyos programok hibáit, illetve hiányosságait. Egy kívülről érkező támadó szerencsére csak a gépünk nyújtotta szolgáltatások biztonsági réseit próbálja kihasználni. Ha tehát egy FTP-kiszolgálót futtatunk, gépünk FTP-szolgáltatást nyújt, és az FTP-kiszolgálódémon számára kívülről adatokat lehet küldeni. Az FTP-démon általában rendszergazdai jogosultságokkal fut, és könnyen előfordulhat, hogy bizonyos programhibából eredően arra is rávehetjük, hogy úgynevezett idegen kódot (a támadó által írt programot) futtasson le. Ha az FTP-kiszolgáló rendszergazdai módban fut, az idegen kód is örökli ezeket a jogköröket, tehát a betörés sikeres volt.
A tanulság tehát az, hogy minden általunk futtatott szolgáltatás (például FTP, Web stb.) lehetséges behatolási pont a rendszerünkbe. Ezért a harmadik alapelv: csak olyan szolgáltatásokat futtassunk, amelyekre valóban szükségünk van.
Hogy milyen szolgáltatásokat futtatunk, azt a legegyszerűbben kapuink pásztázásával tudhatjuk meg. Linux alatt az egyik legnépszerűbb kapupásztázó program az `nmap` (lásd Linux-

világ 6. szám, 45–49. oldal), amit a legtöbb Linux-változat is tartalmaz. Használata rendkívül egyszerű, csak írjuk be az `nmap localhost` utasítást, és rögvest kiderül, hogy éppen milyen szolgáltatások futnak a gépünkön.
Az `nmap` nemcsak a kapu számát, hanem a futó szolgáltatás nevét is kiírja nekünk. Csak azokkal a kapukkal érdemes foglalkoznunk, amelyek `open` állapotúak. Sorozatunk egyik korábbi részében már említettük, hogy a szolgáltatások megvalósítása



Sose használjuk a rendszergazdai jogosultságot az Interneten való barangolásra. Ha idáig nem tettük volna meg, hozzunk létre egy külön – korlátozottabb jogkörökkel bíró – felhasználót

a démonok feladata. Minden démon más-más szolgáltatásért felelős. A feladatunk annyi, hogy a megfelelő démont leállítsuk, és ezután az általa nyújtott szolgáltatás már nem lesz elérhető (a démonokat, leállításukat és újbóli elindításukat sorozatunk negyedik részében már áttekintettük, lásd Linuxvilág 16. szám, 38–39. oldal). Sajnos nem mindig egyszerű kitalálni, hogy az adott szolgáltatás melyik démonhoz tartozik, de segítségünkre lehet a folyamatlista (`ps ax` parancs), ebben tekinthetjük meg a futó démonok (és egyéb alkalmazások) névsorát.
A démonok tárgyalásakor szót ejtettünk az `inetd`-ről (Internet Daemon) is. Ennek célja, hogy ne kelljen folyamatosan futtatnunk azokat a démonokat, amelyekre viszonylag ritkán van szükségünk. Mint tudjuk, a démonok csak akkor képesek dolgozni, ha munkájuk is van, egyébként a háttérben unatkoznak, viszont a memóriát ugyanúgy foglalják. Ha például olyan kiszolgálót üzemeltetünk, ahol az FTP-szolgáltatást csak weblapunk frissítésére használjuk, az FTP-démont gazdaságtalan folyamatosan futtatni, mivel átlagosan napi 1–2 alkalommal lehet rá szükségünk. Ugyanakkor a webkiszolgálót nem érdemes ki-bekapcsolgatni, mert egyrészt viszonylag gyakran szükség van rá (weboldalunkat naponta akár több százan, esetleg ezren is megnézhetik), másrészt indítása és leállítása hosszadalmas feladat, tehát lelassulna a kiszolgálás sebessége.
A megoldás: a webkiszolgálót igen, de az FTP-démont ne indítsuk el a rendszer betöltése után, hanem bízzuk az `inetd`-re! Az `inetd` észleli, ha egy kapun kívülről kapcsolatot akarnak kezdeményezni. Ekkor megnézi, hogy az adott kapuhoz melyik szolgáltatás van hozzárendelve, majd elindítja a megfelelő démont. A démon a kiszolgálást követően nem marad a memóriában, hanem befejezi a futását.
Egy otthoni rendszeren érdemes minél több szolgáltatást az `inetd`-be pakolni. Számos terjesztés esetén seregnyi felesleges szolgáltatás be van állítva, amely nem feltétlenül jelent veszélyt a rendszerre, de nincs is sok értelme benne hagyni. Az `inetd` beállításait az */etc/inetd.conf* állományban találhatjuk.
A fájlban minden sor egy-egy szolgáltatást jelöl. Az első oszlop a szolgáltatás neve. A második, harmadik és negyedik oszlop a kapcsolat típusára vonatkozik. Ezután a felhasználó neve következik, akinek jogosultságaival az utolsó oszlopban megadott démon futhat. Ez általában a rendszergazda.
Ha egy szolgáltatást ki szeretnénk iktatni az `inetd`-ből, egyszerűen tegyünk egy # (kettős keresztet) a megfelelő sor elejére. Ne felejtsük el, hogy a beállítás csak akkor lép érvénybe, ha előtte újraindítjuk az `inetd`-t.
Sok terjesztés (mint például a Red Hat is) az `inetd` helyett másikat használ (például az `xinetd`-t – eXtended Internet service Daemon).
Minden szolgáltatáshoz külön beállítófájl tartozik, amelyeket a */etc/xinet.d/* könyvtár alatt találunk. Amennyiben egy szolgáltatást ki szeretnénk iktatni, a `disable = no` sort a megfelelő állományban állítsuk `disable = yes`-re.
Ha ezzel készen vagyunk, keressük fel Linux-változatunk honlapját, és nyálazzuk végig a hibalistát. Leginkább azokra a hibákra összpontosítsunk, ahol fel van tüntetve, hogy a rendszer biztonságát is veszélyezteti. Ebben az esetben azt is megtudhatjuk, hogy az adott biztonsági lyukat csak belülről (local) vagy kívülről is (remote) is ki lehet-e használni.
Mit jelent ez? A támadásokat két csoportra bonthatjuk: belsőre és külsőre. Külső támadás esetén a támadó nem rendelkezik számlával (account) a rendszerben, azaz nem férhet hozzá a parancssorhoz, tehát például nem futtathat különböző programokat. Kizárólag csak a hálózati szolgáltatásokat nyújtó démonokat „zaklathatja”. Belső támadásról akkor beszélünk, amikor sötét lelkű hősünk bejelentkezik vagy `telnet`-en, vagy `ssh`-n keresztül és a rendszergazdai jogkörökkel futó programok biztonsági réseit próbálja kihasználni. Ilyenkor tehát jóval nagyobb a támadási felület, viszont a betörőnek ismernie kell egy felhasználói nevet és a hozzá tartozó jelszót.
Egy otthoni rendszer esetében nyilvánvalóan csak a külső támadásokra érzékeny hibákat kell befoltoznunk (kivéve, ha fűnek-fának elérést adunk), de azt javasoljuk, hogy egyetlen ismert biztonsági rést se hagyjunk nyitva. Különben is egy hibás program „befoltozása” nem ördöngös művelet: Linux-változatunk honlapján le van írva, hogy egyrészt merre találjuk a frissítést, másrészt mit kell vele tennünk. Egy RPM-csomag esetében általában elég, ha kiadjuk az `rpm -Fvh csomag.rpm` parancsot.
Ha ez is megvan, nem árt végiggondolnunk: valóban szükséges-e, hogy egy adott szolgáltatás a világ bármely pontjáról elérhető legyen? Például bizonyos címtartományokra korlátozhatnánk, amire több út is kínálkozik, ám ez már a következő rész témája, amelyben alapszinten megismerkedünk a Linux-rendszermagban lévő úgynevezett állapotfüggő csomagszűrő tűzfallal.
Ez egy otthoni rendszeren is hasznos lehet, például megvédhet bennünket a DoS- (Denial of Service) támadásoktól, de ugyanitt állíthatjuk be a több gép közti internetmegosztást is (masqueradingbújtatás). A részletekről egy hónap múlva ugyanitt.

Garzó András
(garzoand@interware.hu) körülbelül három éve foglalkozik Linux- és más Unix-rendszerekkel. Legjobban az operációs rendszerek lelkivilága érdekli, de nyitott egyéniség. Kedvenc étele a palacsinta, és van egy Richard nevű macskája. Minden észrevételt, megjegyzést, levelet szívesen fogad.