ez a program kideríti. Ámde hogyan bízhatnánk meg az esetlegesen gyanúba keveredett gépen lévő ellenőrzőösszegekben? Sehogy. Mindenesetre egyelőre tisztának tűnt minden, tehát meghívtam a `netstat` programot. Ez a program a hálózathoz kapcsolódó programok állapotáról ad tájékoztatást. Megmutatja, hogy a kiszolgáló milyen kapcsolatot kezel jelenleg. Én a *2. listán* látható módon indítottam el. Természetesen a kimeneten kívül több más érték is szerepel itt. A program ezekkel a kapcsolókkal mutatja meg, hogy melyik program vár kapcsolatot melyik kapun, és milyen IP-címen teszi azt. Itt ért az első szívroham, ugyanis egy számomra ismeretlen kaput fedeztem fel ismeretlen démonnal. Majd megnyugodtam, mert csupán az otthoni gépemen futó kísérleti program várta a kapcsolatokat. Még otthon kezdtem el kipróbálni és a gépemen maradt. Másodszor már a kiszolgálón sikerült lefuttatnom a programot, ahol mindent rendben lévőnek találtam. A biztonság kedvéért azonban tovább piszkáltam a rendszert. Átnéztem az összes parancsfájlt, amely a `cron`, az `at` és a Postfix programokhoz kapcsolódik, ugyanis ezeket a szolgáltatásokat le akartam állítani. Azt azonban mindenképpen el szerettem volna kerülni, hogy amennyiben a kiszolgálót mégis feltörték, és esetleg huncut `rm -rf /` parancsot írtak a vezérlő parancsfájlba, annak következményei legyenek. Miután mindent rendben találtam, a szolgáltatásokat leállítottam. Miért volt ez fontos? Ha a rendszert feltörték, és egy olyan binárist módosítottak, amelyet a `cron` is használ, a rendszer esetleg önműködően újra meg újra megnyílik. Ráadásul a Postfix még számos helyre el akarta küldeni a leveleket. Ezeket a leveleket a leállítás után töröltem. Jó néhány akadt, ezért miután meggyőződtem róla, hogy „rendes" levél nincs a sorban, az egész várakozási sort töröltem (szerencsére hétvége volt, ezért ez csaknem természetesnek tekinthető). Ezután a ➲ http://www.debian.org-ról leszedtem a binárisokhoz tartozó MD5-ös ellenőrző összegeket és átmásoltam őket a gépre, majd így ellenőriztem a binárisokat. Ezt az átjárón is megismételtem. Mindkét rendszer teljesen rendben volt, tehát a törést és a nyílt levéltovábbító gondokat elfelejthettem. Már csak egyetlen lehetőség maradt.

2
```
[ago@mdk ago]$ netstat -antl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address     Foreign Address         State
tcp        0      0     0.0.0.0:25          0.0.0.0:*           LISTEN
```

Harmadik felvonás

Mivel a kiszolgáló csak egy helyről fogadott el leveleket továbbításra, nem volt nehéz dolgom, hogy behatároljam a következő keresési területet. Ez a gép az átjáró volt – az egyetlen gép, amely felől a küldés engedélyezett. Ezen az átjárón igazából nem fut semmi, csak címeket fordít és kapcsolatokat továbbít. A támadás tehát a mögötte lévő egész belső hálózatról jött. Hogyan lehet megkeresni a saját berkeinkben megbúvó támadót? Miután ismét elindítottam minden szolgáltatást a levelezőkiszolgálón, figyelmemet az átjáróra, pontosabban a naplófájlokra összpontosítottam. Mivel a levelezőkiszolgáló eléréséhez címet kell fordítanom, vagyis álcáznom (masquerading) kell, a csomagszűrővel az erre vonatkozó szabály volt beállítva. Csakhogy a szabály végén megadtam, hogy fordításnál *minden* kimenő csomagról írjon jelentést a naplófájlba. A parancs hasonlóan néz ki:

```
/sbin/ipchains -A forward -i -p tcp
➥-s 192.168.1.0/24 -d mail.ceg.hu 25
➥-j MASQ -l
```

Ez fordította át a belső hálózat címeit az átjáró IP-címére, amennyiben az ügyfelek kapcsolatba akartak kerülni a levelezőkiszolgálóval. A `-l` kapcsolta be a naplózást. Az előző napi naplófájlból kikerestem – természetesen a segédprogramok használatával –, hogy melyik ügyfél kapcsolódott kiemelkedően sokszor a levelezőkiszolgálóhoz. A segédprogram saját készítésű volt, ezért a kiosztott címtartomány minden ügyfelére összesítést készített, és hogy hány bejegyzést talál az adott IP-címhez. Majd a kiemelkedően nagy számú küldő címét felhasználva kikerestem a listából, hogy kihez tartozik a cím. Ekkor csörrent meg a telefon. Maga az elkövető volt. Honnan tudta meg, hogy nyomozok? Az egyik felháborodott partner ugyanis nemcsak nekem küldte el panaszát, hanem a levél küldőjének is – mármint arra a címre, amit az elkövető írt be, és ahova a válaszleveleket a megrendelésekkel együtt várta (ugyanis egy szolgáltatást hirdetett). Mivel csoportos választ nyomtam, ő is megkapta válaszomat – ez idegességemben fel sem tűnt nekem. Nos, próbálta magát mentegetni, hogy nem gondolta, mekkora baj lesz ebből, és különben is otthonról akarta végezni. Ennek azonban jócskán ellentmondott, hogy a saját bevallása szerint is mailbomber programot használt. A következő héten hétfőn leadtam a jelentést a cég vezetőjének és szóban is tájékoztattam az eseményekről. Ennek eredményeképpen az illetőt még aznap elbocsátották.

Miért is? A cég erőforrásait használta és mivel levélszemét jött a levelezőkiszolgálóról, néhány másik levelezőkiszolgálóról kitiltották a tőle érkező *összes* levelet. Ezenkívül a céget erkölcsi kár is érte.

Összegzés

Egyszer minden „csínytevésre" fény derül, és egy ilyen nyomozás inkább fárasztó és idegesítő, semmint jó móka. Gondolom, jövője ismeretében a vétkes is másképp cselekedett volna.

Deim Ágoston (ago@lsc.hu)
Kedveli a sört, szereti a futást és imádja Szabó Lőrinc verseit. Nem hisz vakon egyik rendszerben sem. Vonzódik a BSD-hez is. Tagja az LME-nek és a MBE-nek. Mottója: a gép nem lehet fontosabb az embernél.

A 2001. évi LinuxJournal szerkesztői szavazásának eredménye

Sokat változott a Linux világa a tavalyi szerkesztői szavazás óta. Az idő tájt a technológiai és .com-fellendülés korát éltük, most viszont a gazdasági hanyatlásában tengődünk. Múlt évben panaszkodtunk, milyen nehéz kiválasztani a számos jelentkező közül a győztest, s felvetettük, kevesebb versenytárs esetén nyilván könnyebb lenne a döntés. Most már tudjuk, hogy ez nem feltétlenül igaz.

Noha az egyes tárgykörökben kevesebb gyártó (főleg gépet, alkatrészt termelő) indult, a kínálat változatlanul bőséges (mind a szabad, mind a kereskedelmi termékek terén), és jelentős minőségjavulást értek el az elmúlt év során, mind a termékek, mind a Linux-rendszermag fejlesztése terén.

A *Linux Journal szerkesztői díjaira* nyílt forrású és védett programok egyaránt pályázhattak, s a programok idei kiválasztottjai között mindkét típus képviselői egyformán szerepelnek. Bár jelenleg mindannyiunkat nagy elégedettséggel tölt el, hogy olyan sok nyílt forrású termék közül válogathattunk, ne feledkezzünk meg róla, hogy nem sokáig marad ez így, amennyiben nem védekezünk minden erőnkkel az SSSCA-féle törvényi szabályozás veszélyei ellen. Ez ugyanis a Digital Rights Management (amolyan digitális jogvédelem) kötelező alkalmazását vezetné be, amelynek eredményeként a szabad, sőt a nyílt forrású operációs rendszerek is törvénybe ütközők lennének.

Amennyiben valamelyik nyertesünk a végsőkig felbosszantana titeket, nézzétek meg előző számunk 20. oldalán az olvasói szavazás eredményeit is.

Kiszolgáló

Filanet Interjak 200 802.11b

Kellene egy 802.11b hálózat nagyteljesítményű antennával az olcsó WAN-kapcsolatok létesítésére? Szeretnétek egy VPN-szolgáltatást nyújtó 802.11b alapállomást, amely a felhasználók noteszgépeinek biztonságáról gondoskodik? Központilag kezelt postarendszerrel, Samba- és VPN-kiszolgálókkal kellene ellátni a vállalat minden otthon dolgozó munkatársát? A Filanet egy sor kis költségű, ventilátor nélküli, beágyazott Linuxszal ellátott hálózati eszközt gyárt, amelyeket saját ASIC alaplapra épít ARM processzormaggal és 3DES-titkosítást támogató alkatrészekkel. Segítségükkel a vállalatok és ISP-szervezetek számos gondja megoldható, s alig kerülnek többe, mint egy ostoba DSL-doboz.

Biztonsági eszköz

Nmap

Egy program elterjedésének biztos jele, ha a nevét igeként kezdik használni. Mára bevett adatbiztonsági gyakorlat, hogy minden új Linux-kiszolgáló felállításakor az Nmapet futtatják le, és rendszeresen ellenőrzik vele a hálózati változásokat. Nem véletlen, hogy az Nmap ugyanakkor terjedt el, amikor a különböző Linux-változatok megritkították az alapértelmezés szerint felkínált szolgáltatások listáját. Üdvözöljük az Nmapet mint a rendszergazdák és Linux-változatok könnyen kezelhető „biztonsági jelzőfényét"!

Webkiszolgáló

APPRO1124

Mi e rendszer kétprocesszoros Athlon MP alaplapját tettük a linuxos csúcsgépünkbe. Az APPRO azonban – a VA Linux Systems eredeti tervei alapján – egy egyszerű IU-kiszolgálóba helyezte négy működés közben cserélhető SCSI-meghajtó és egy vékony CD-ROM-meghajtó társaságában. A nagy teljesítményű ventilátoroknak és az egyedi tápegységnek köszönhetően olyan webkiszolgálót alkottak, amit annak idején nagyon szívesen láttunk volna az alkatrészpiacon, amikor a webkiszolgálókra még külön keretünk volt.

Webügyfél

Konqueror

Linuxosok, itt az ideje eldobni a Netscape 4.x böngészőt, mert mára már ósdi kacatnak számít! Mostanra mind a Mozilla, mind a Konqueror elérte a megfelelő megbízhatósági szintet, és eléggé széles körű szolgáltatásokat kínál ahhoz, hogy örökre megszabadulhassunk az avítt Motif-alapú Netscape-től. A szerkesztői díjat végül a Konquerornak ítéltük a KDE-környezetbe való tökéletes illeszkedés elismeréséül, a sebességéért, és amiért lehetővé teszi a Flash-animációk vagy -mozik egyszerű lejátszását.

3D-s modellezőeszköz

Maya 4

Ahogyan *Robin Rowe* a legutóbbi írásában már beszámolt róla (*Linuxvilág* 6–7. szám, 44. oldal), a Linux szó szerint meghódítja a filmipart: segíti a különleges képi hatások és animációk gyors előállítását. Egyetlen más iparágban sem tapasztalható ilyen tömeges áttérés Linuxra. A Maya ugyancsak kiveszi ebből saját részét, amikor ügyfelei igényének megfelelően termékét Linuxra ülteti. Ezzel *Linus* elismerését is elnyerték, aki szerint ez „minden idők legösszetettebb és leglenyűgözőbb Linuxon futó 3D-s grafikus alkalmazása".

Biztonságimentés-készítő eszköz

BRU-Pro

Már azt hittük, hogy a BRU örökre elveszett a vállalati útvesztőkben, de szerencsére *Tim Jones*, a BRU régi pártfogója nem hagyta elenyészni e jól bevált, régimódi mentési eszközt. Tim korábban a BRU eredeti gyártójának, az EST-nek volt a fejlesztési alelnöke, most pedig a Tolis Group márkanév alatt kínálja a BRU-t. Ezzel a segédeszközzel a biztonsági mentésterv és az ügyfél által használt szalagegységek egyszerűen állíthatók be. Az sem mellékes, hogy a BRU támogatja a ➲ http://www.linuxtapecert.org weboldalt, ahol a Linux alatt kipróbált és jóváhagyott szalagmeghajtók listája található.

Egyéb segédprogramok

Acronis OS Selector

Íme egy remek betöltés- és lemezterületkezelő, amelynek nagy előnye, hogy a fokozott adatvédelem érdekében a ReiserFS fájlrendszert is támogatja.