Visszaélések az Interneten

Segíts a levélszemét megállításában, készíts teszteket a diákjaidnak, és természetesen figyeld a csomagokat.

Néhány hónapja egy érdekes telefonbeszélgetés részese voltam. Nagyjából így folyt le (helyszűke miatt rövidítve közlöm):
– Szevasz, David, van egy kis gond az egyik ügyfelem levélkiszolgálójával (Caldera eServer 2.3). Két évvel ezelőtt telepítettem, azóta remekül ment, de nemrég volt egy kis áramszünet, ami miatt leállt. Most a gép elindul ugyan, de az ethernet-csatolók nem kelnek életre.
– Hm, indítsd el őket kézzel, aztán kiderül, miért nem indulnak el bekapcsoláskor. Az `fsck` nem talál semmit?
– Nem, semmi. Próbáltam futtatni az `ifconfig`-ot, de nem állítja be a csatolókat.
– Futtasd az `lsmod`-ot, talán nincsenek felrakva az illesztőprogramok. Az lsmod után próbálkozz újra az ifconfiggal.
– A modulok telepítve vannak, az ifconfig `segfault`-tal száll el.
– Segfault? – Ekkor mintha félrevertek volna egy harangot a fejemben. – Az ifconfig RPM-et cseréld le, lehet, hogy a gép leállásakor megsérült – az ifconfig ugyanis nem az a fajta program, ami csak hipp-hopp elszállogat – gondoltam.
– A csomagot a `--force` beállítással tudod lecserélni.
– Úgy látom, nem lehet lecserélni az `ifconfig`-ot, még a `--force` is hatástalan.
– Akkor futtasd le az `lsattr ifconfig` parancsot, és mondd, mit látsz.
– Egy „i” betű van a neve mellett.
Eközben az Űrszekerekből ismerős vészjelző fények és hangok zsongtak a fejemben. – Akkor figyelj ide, futtasd a `locate ifconfig` parancsot.
– A következőt látom: ***/sbin/ifconfig; /dev/sdg/.azgub/backup/ifconfig, /usr/man/man8/ifconfig.8.gz***.
– Remek, találtunk egy rejtett támadócsomagot (rootkit) a ***/dev*** könyvtárban. Betörtek az ügyfeled gépére. Egyébként a kiszolgáló felrakása óta telepítettél valamilyen biztonsági foltot? – Válasz nem érkezett, de feltételeztem, hogy nem.
Egy hónap telt el azóta, hogy ajánlatot küldtem neki, ami szerint megoldanám a biztonsági gondjait, és néhány egyéb szolgáltatás mellett telepítenék neki egy tűzfalat is. A behatoló azóta is szabadon garázdálkodik a gépen, az ethernet-kártyák lehallgató üzemmódban vannak, a tisztelt ügyfél pedig valószínűleg könnyen múlónak tartja a biztonsági gondokat; hát igen, megváltoztatta a jelszavát, elővigyázatos volt – szerintem ez is több a semminél. Hogy ki tört be? Miért? Hogy a derekasan aláaknázott gépet felhasználták-e más rendszerek feltörésére, DDOS-támadásokhoz zombiként, ne adj' isten mindkét célra? Néhány embert egyszerűen el kellene tiltani az Internettől. Vajon egyedül van? Aligha. Kiszolgálóimat naponta megpróbálják feltörni, a sávszélességemet vírusok, önműködő támadások és egyéb vackok emésztik fel. Én pedig fizetek érte. Szerintem egy jó kis törvényre lenne szükségünk…

SmtpRC

Ellenőrizd, hátha a saját hálózatodról is küldözget valaki levélszemetet! Ezzel a kiegészítővel minden bizonnyal megoldhatod az e téren jelentkező gondokat. A futtatásához libpthread és glibc szükséges.
➲ http://sourceforge.net/projects/smtprc

GTK-Agenda

Kiváló kezdeményezés egy tetszetős, GTK-alapú naptár készítésére. PostgreSQL-adatbázisban tárol neveket, telefonszámokat és elektronikus levélcímeket. Jelenleg sajnos csak spanyol nyelven érhető el, ám a feliratok és egyéb szövegek módosítása nem lehet túl bonyolult, így remélhetőleg hamarosan más nyelveken is elérhető lesz. Az alkalmazásból leveleket is lehet küldeni, ha rendelkezünk futó SMTP-démonnal. Ha további elvárásaink vannak az adatbázissal szemben, a bővítése – úgy tűnik – könnyen megoldható. A futtatáshoz szükséges: libgtk, libgdk, libgmodule, libglib, libdl, libXext, libX11, libm, libpq, libssl, libcrypto, libcrypt, libresolv, libnsl és glibc.
➲ http://pbrufal.kleenux.org/proyectos.shtml

x86info

Ha nem elégedsz meg a ***/proc/cpuinfo*** segítségével megszerezhető adatokkal, erre van szükséged. Közvetlenül a processzor regisztereiből olvas, így annyi adatot szolgáltat, amennyit a legtöbbünk soha nem fog megérteni és sohasem fog használni. A futtatásához glibc szükséges.
➲ http://sourceforge.net/projects/x86info

ILIAS

Ha az Interneten keresztül szeretnél feladatokat és vizsgalapokat kiosztani a diákoknak, megtaláltad a megfelelő eszközt. A hallgatók adatai, a vizsgaeredmények és a további tudnivalók egy MySQL-adatbázisba kerülnek. A futtatáshoz szükséges: Apache, PHP és MySQL, MySQL kiszolgáló, GD, zlib, freetype, libjpeg, ImageMagick, zip és unzip.
➲ http://www.ilias.uni-koeln.de/ios/index-e.html

pktstat

Rengeteg olyan alkalmazás érhető el, ami a hálózati csomagokat figyeli, ez azonban egy kicsit más. Ez ugyanis a csomagok sávszélesség-használatát figyeli. Apró gyöngyszem, a segítségével pillanatok alatt észreveszed, ha valamelyik felhasználód mondjuk Kazaaval foglalja le a sávszélesség 99,7 százalékát. Futtatásához libm és glibc szükséges.
➲ http://www.itee.uq.edu.au/~leonard/personal/software/#pktstat

DNSMan

Webes alkalmazás, talán a legegyszerűbb módja annak, hogy a BIND zónafájljait karbantartsd, szerintem még a webmin BIND moduljánál is jobb. A követelmények között kevés dolog szere-

pel, viszont a DNS-es rendszeren webkiszolgálót kell üzemeltetned. Fejlesztését továbbra is figyelemmel fogom kísérni, ugyanis a készítője jó pár érdekes ötletet vonultatott fel a tennivalók listájában. A futtatáshoz szükséges: webkiszolgáló (Apache), amely képes CGI-parancsfájlok futtatására, továbbá Perl, BIND 8 vagy 9.
➲ http://www.xsta.cc/dnsman

ntop

A három évvel ezelőtti emlékek felidézésekor erősen ingadoztam két nagyszerű program között. Az ntop és a stickerbook voltak versenyben, az utóbbi remek fejlesztés gyerekeknek – jómagam nagyon szeretem, de végül mégis az ntop nyert. Három év alatt sokat fejlődött: egyszerű ncurses segédprogramból HTTP- vagy HTTPS-protokoll felett használható, nagy tudású webes ügyféllé nőtte ki magát, amely gdgraph segítségével grafikus megjelenítésre is alkalmas, ha úgy kívánjuk. Az ntop kevéssé hasonlít korábbi önmagára, használata is sokkal könnyebb lett. Ha top jellegű hálózati programra van szükséged, ne keresgélj túl sokat. A futtatáshoz szükséges: libmysqlclient, libcrypt, libm, libssl, libpthread, libresolv, libnsl, libdl, libgdbm, libz és glibc.
➲ http://www.ntop.org

Nessus

Három évvel ezelőtt írtam még a Tedről, egy kiváló RTF szövegszerkesztőről, a Nessusról, egy biztonságellenőrző programról és az Nmapról, amely hálózatpásztázó. Nehéz volt, mégis a Nessust választottam közülük.
Na jó, csaltam is egy kicsit. A Nessus ugyanis az Nmapot is használja. A Nessus talán a legteljesebb és legnagyobb tudású biztonság-felülvizsgálati eszköz, amit csak meg lehet szerezni – ráadásul ingyenes is. Ha a fejlesztői kiadást használod, akkor az összes biztonsági hiányosságról áttekintést kapsz, és megteheted a szükséges intézkedéseket. Ha te felelsz a hálózat biztonságért, nélküle neki se állj semminek. A futtatáshoz szükségesek: libX11, libXext, libXi, glibc, libdl, libgdk, libglib, libg mp2, libgtk, libm, libnsl és libresolv.
➲ http://www.nessus.org

xlog

Rádióamatőrök számára kiváló naplózó eszköz a megismert emberek elérhetőségének nyilvántartására. Több naplót is vezethetsz, a sávokat pedig a ***Preferences*** (Tulajdonságok) menüben törölheted vagy adhatod hozzá a listához. A dátumot már a program írja be, a kapcsolat létrehozásakor pedig elég rákattintani a ***Time*** (Idő) gombra, és az időpont is megjelenik. Ezután elég megadni a ***Hívó/válaszoló állomás***-t, bepötyögni a megjegyzéseket, kiválasztani a frekvenciát, és az ***Add*** (Hozzáadás) gombra kattintani. A naplókban később – többek között – keresni is lehet. A felület párját ritkító mértékben felhasználóbarát, a naplókkal akár egy kívülálló is dolgozni tud. Nekem is menni fog. A futtatáshoz szükségesek: libgtk, libgdk, libgmodule, libglib, libdl, libXext, libX11, libm és glibc.
➲ http://people.debian.org/~pa3aba/xlog.html

axelq

Az Axel segédprogramban nem alakítható ki olyan letöltési sor, amellyel a letöltéseket későbbre állíthatnánk. A kiegészítés segítségével ezt is megtehetjük, és a megadott lista tagjait egy későbbi időpontban az Axel segítségével tölthetjük le. Ha megtetszik az Axel, érdemes letölteni. A futtatáshoz `/bin/sh` szükséges.
➲ http://electron.its.tudelft.nl/~hemmin98/axelq.html

integrit

Ez az érdekes kis program a Tripwire és az AIDE mellé sorolja magát. Újabb eszköz a rendszer megfigyelésére, és egész jól működik. Könnyen használható, és beállítható a legfontosabb állományok és könyvtárak változásainak követésére. Az integrit statikusan van lefordítva, így a futtatásához nem kell külső fájl.
➲ http://integrit.sourceforge.net

GRPN

Ebben a hónapban eléggé megkavarodtam, amikor a három évvel ezelőtti felhozatalból válogattam. A Keystone-t eladták a WhitePajamasnak, fejlesztését leállították, számos más alkalmazás pedig kevés fejlődésen ment keresztül, már ha egyáltalán dolgoztak rajta. Sok más programmal ellentétben nem lett ugyan a kedvencem, mégis a GRPN-t választottam. Valószínűleg nem sokan emlékeznek a fordított lengyel ábrázolásra, azonban elég sok számításnál használtuk, és ha jól emlékszem, szinte az összes tudományos számításnál előkerült. Ha szükséged van a lengyel módszerre, vagy egyszerűen csak megtetszett, akkor ez a számológép neked készült. Kezeli az általános matematikai műveleteket, valamint az exponenciális, logaritmikus és trigonometrikus függvényeket. A futtatáshoz szükséges: libgtk, libgdk, libmodule, libglib, libdl, libXext, libX11, libm és glibc.
➲ http://lashwhip.com/grpn.html

TuxTyping

Gyermekeknek készült gépelésoktató program. A betűk lehulló halakkal érkeznek, amelyeket Tuxnak, a pingvinnek el kell kapnia. Ha valami bonyolultabbra vágyunk, rövidebb, túlnyomórészt hárombetűs szavakat is kérhetünk, a feladat nem változik. A grafika és a remek játszhatóság kiváló szórakozást nyújt a gyerekeknek, és eközben még gépelni is megtanulnak. A futtatáshoz szükséges: libSDL, liSDL_image, libSDL_mixer, libm, libdl, libartsc, libpthread, libX11, libjpeg, libpng, libz, libtiff, libvorbisfile, libvorbis, libogg, libsmpeg, glibc.
➲ http://www.geekcomix.com/dm/tuxtype

di

A `di` segédprogram (disk information – lemezinformációk) rengeteg hasznos adatot árul el a merevlemezedről. Ezek jelentős részét a `df` is elárulja, ám nem mindet. Az utóbbi időben például a ReiserFS és az ext3 fájlrendszer egyaránt bekerültek a rendszermagba (hogy az LVM-et már ne is említsük), és sokszor nem árt tudni, milyen fájlrendszerrel van dolgunk. A `df` ezt nem árulja el, a `di` ellenben azonnal megmutatja. A kimenet formátuma is letisztultabb, mint a `df` esetében, különösen a hosszú devfs elnevezésekkel rendelkező rendszerek esetében. A futtatásához glibc szükséges.
➲ http://www.gentoo.com/di

Ennyit erre a hónapra.

Linux Journal 2002. augusztus, 100. szám.

David A. Bandel
(dbandel@pananix.com) jelenleg Panamában él, Linux- és Unix-tanácsadással foglalkozik. Társszerzője a Que Special Edition: Using Caldera OpenLinux című könyvnek.