A hálózat rejtett zugai

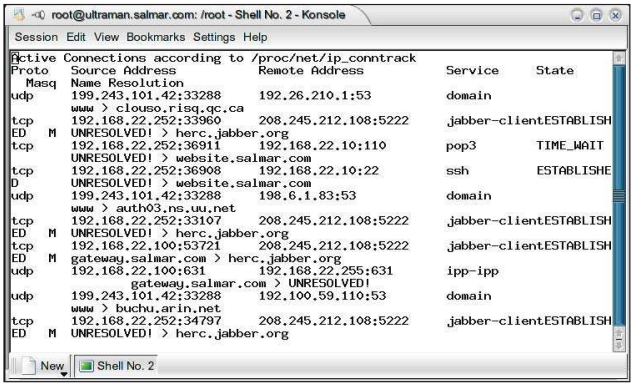
Hálózatunk legsötétebb sarkainak megvilágításához Marcel a hálózatmegfigyelő eszközökből állított össze egy különleges menüt.

Nem, François, ennek a szimatolónak semmi köze a borhoz. A bor az a terület, ahol az emberi orr bármilyen programnál jobban teljesít, függetlenül attól, hogy milyen okos a programozó. Őszintén szólva, mon ami, a borkóstolás – természetesen minőségellenőrzési célzattal – olyan feladat, amit nem szívesen automatizálnék. Azoknak a szimatolóknak, amikkel a Linuxszal való kotyvasztás közben találkozhatunk, más a rendeltetése.

Nézz csak ide, mon ami! Figyeld meg, hogy a sávszélességünk mekkora része van használatban itt és itt. Kíváncsi vagy, hogy ezek a kapcsolatok mekkora sávszélességeket jelentenek? François, miért nem ide figyelsz? Á, megérkeztek a vendégeink! Miért nem szóltál?

Bonsoir, mes amis! Örömmel üdvözöllek titeket ismét Chez Marcelnél, a kitűnő Linux-konyha, a világ legjobb borai és a nyílt forrású dolgok iránt érzett általános szeretet házában. Üljetek csak le, és helyezzétek magatokat kényelembe! Mielőtt megérkeztetek, éppen arról beszéltem François-nak, hogy mennyi rejtett adat áramlik keresztül egy átlagos hálózaton. Ha már a rejtett élvezeteknél tartunk, François, kérlek, siess a borospincébe, irány a nyugati szárny, és hozd fel az 1995-ös Rioja Imperial Gran Reservát. Ez a spanyol vörös egy tökéletes hálózatos bor, nemde?

Éppen azt ecseteltem hűséges pincéremnek, hogy egy átlagos hálózaton mennyi minden történik, és sokan teljesen megfeledkeznek azokról a kapcsolatokról, amiket korábban ők kezdeményeztek. A működő kapcsolataink ellenőrzésére szolgáló legegyszerűbb eszköz, a Netstat minden Linux-rendszercsomagban megtalálható. A `-a` és `-p` kapcsoló segítségével rendszerünk szinte összes nyitott hálózati kapcsolata (vagy kapuja) feltérképezhető, és azt is megtudhatjuk, hogy melyiket melyik program használja. Figyeljük meg, mi történik akkor, amikor a programot futtatom. Használni fogom a `-n` kapcsolót is, ami a Netstatot arra utasítja, hogy ne habozzon az IP-címeket szimbolikus címekké alakítani. Ez egy kicsit gyorsítja a program futását, mert így nem hajt végre névfeloldást. Az eredmény egy meglehetősen hosszú lista is lehet, ezért a kimenetet a `more`-ra irányítottam, lásd a *listánkon*. Á, François, megérkeztél a borral, nagyszerű. Kérlek, tölts a vendégeinknek! A lent látható lista nem teljes, de az általam kapott is hiányos. Ennek oka, hogy az álcázott (masqueraded) kapcsolatok IP-táblái a Netstat számára nem láthatóak; ez az



1. kép A conntrack figyelőprogram megjeleníti az álcázott kapcsolatokat

adat egy másik helyen található, mégpedig a */proc/net/ip_conntrack* fájlban. A PID a kapcsolatot használó program folyamatazonosítója. Éppenséggel kiadhatunk egy `cat` parancsot a */proc/net/ip_conntrack* fájlra vonatkozóan, de az eredmény nem lesz egy szemnyugtató olvasmány. Pillantsunk az alábbi példára (a kimenet egyetlen burkolt sor):

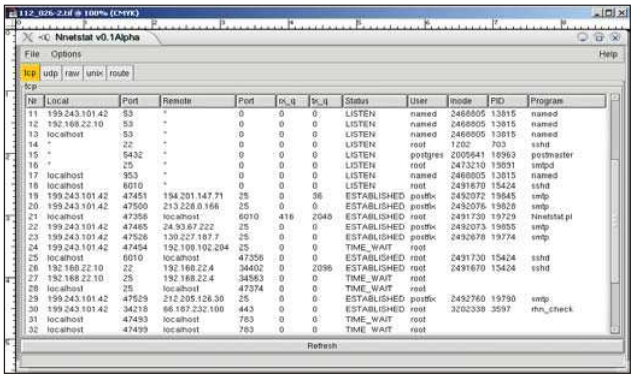
```
tcp       6 431253 ESTABLISHED
➥src=192.168.22.5 dst=192.168.22.10
➥sport=34212 dport=22 src=192.168.22.10
➥dst=192.168.22.5 sport=22
➥dport=34212 [ASSURED] use=1
```

Patrick Lagacé is nyilván nehezen olvashatónak találta ezt a szöveget. Az ő Conntrack-néző parancsfájlja a ➲ http://cv.intellos.net címen érhető el. Mivel egy Perl nyelvű parancsfájlról van szó, a letöltés után a jogosultságok megváltoztatásával egyszerűen tegyük futtathatóvá a fájlt, és adjuk ki a következő parancsot:

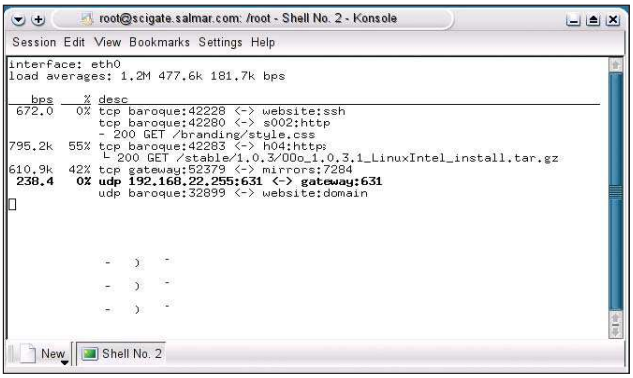
```
chmod +x conntrack-viewer.pl
./contrack-viewer.pl
```

A kimenet alapértelmezésben az összes kapcsolatot megmutatja, az álcázottakat is beleértve. A `-m` kapcsolóval korlátoz-

```
#netstat -apn | more
Active Internet connections (servers and estabilished)
Proto  Recv-Q  Send-Q   Local Adress        Foregin Adress       State         PID/Program name
Tcp         0      20   192.168.22.100:22   192.168.22.100:1014  ESTABILISHED  4003/sshd
Tcp         0       0   192.168.22.100:22   192.168.22.100:1015  ESTABILISHED  6122/named
Tcp         0       0   192.168.22.100:53   0.0.0.0:*            LIStEN        6122/named
Tcp         0       0   127.0.0.1:53        0.0.0.0:*            LIStEN        6122/named
Tcp         0       0   0.0.0.0:*           0.0.0.0:*            LIStEN        1231/httpd
Tcp         0       0   0.0.0.0:443         0.0.0.0:*            LIStEN
```



2. kép Az Nnetstat egy tetszetős grafikus Netstat



4. kép Az azonosított fájlnevek a pktstat megjelenítőjén

3. kép A Driftnet munkában: minden képetek hozzám tartozik!

hatjuk a kimenetet az álcázott kapcsolatokra, az ellenkező hatás (az álcázott kapcsolatok elrejtése) a `-d` kapcsolóval érhető el. Vessünk egy pillantást az *1. képre*, amelyen a program kimeneti képe látható.

Alexander Neptun Nnetstat nevű programja tetszetős külsejű grafikus segédprogram a működő hálózati kapcsolatok, útválasztó táblázatok és egyebek megjelenítésére. Saját legfrissebb példányunkat a ➲ http://www.aneptun.de/linux/Nnetstat címről tölthetjük le. A program alapjában véve egy Perl-parancsfájl, így telepítésre nincs is szükség, elég lehetőséget teremteni arra, hogy a ***Nnetstat.pl*** fájl futtatható legyen. Mint kiderül, a Nnetstat futtatásához szükség van még a ***Gtk.pm*** modulkönyvtárakra, és míg a Perl minden bizonnyal a rendszerünkön van már, ez a modul valószínűleg nincs. A beszerzés legegyszerűbb módja a Perl CPAN adattárról való letöltés, és a telepítő parancssor is egész barátságos:

```
perl -MCPAN -e "install Gtk"
```

Ha ez az első alkalom, amikor ilyen módon telepítünk Perl-modulokat, először keresztül kell jutnunk egy kis kérdés–felelet részen. Menjünk végig rajta, és fogadjuk el a felajánlott értékeket – bízzunk a rendszerben. Amit meg kell adnunk, az a legközelebbi CPAN-tükrözések címe. Amikor a rendszer felteszi a kérdést, válasszuk ki a földrészt és az országot, majd az elérhető helyi tükrözéseket. Ha ezzel készen vagyunk, a Gtk telepítése magától folytatódik.

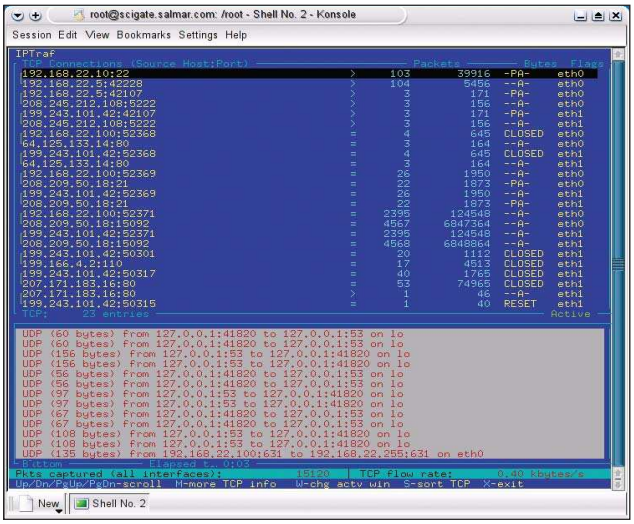
A Gtk Perl-modulok telepítése eltart egy darabig. Talán nem árt felhívnom a figyelmet, hogy a telepítés végefelé még egy tesztsorozat lefut. Ne lepődjünk meg, ha egy grafikus ablak jelenik meg a képernyőn, azt kérve, hogy a csomaggal kapcsolatos grafikus varázslatok kipróbálása céljából kattintsunk a ***Run*** feliratra. Amikor elégedettek vagyunk az eredménnyel, a próba befejezéséhez kattintsunk a ***Close*** gombra, és végezzük el a telepítésből hátralévő részt.

Ha igazán rémisztő – vagy szórakoztató, ez nézőpont kérdése – módon szeretnénk látni, hogy pontosan mi folyik keresztül a rendszerünkön, használjuk a Driftnetet. Már maga a név (vonóháló) elég ahhoz, hogy az embernek a hideg kezdjen futkosni a hátán. Röviden a Driftnet figyeli a kiválasztott csatolófelületen áthaladó kép- vagy videofájlokat (csak az MPEG típusúakat), és a talált képeket megjeleníti. Hogy ez a felfedés a rendszergazda számára félelmetesebb-e, hiszen kiderül számára, hogy a felhasználók miket néznek, esetleg maguknak a felhasználóknak, az több tényezőtől függ. A képgyűjtemény teljesen válogatás nélküli, semmilyen módon nem utal egy valóságos felhasználóra.

Saját példányunk beszerzéséhez keressük fel ***Chris Lightfoot*** honlapját a ➲ http://www.ex-parrot.com/~chris/driftnet címen, és töltsük le a forráskódot. Mielőtt a köztetek lévő szellemidézők megkérdeznék – amikor utoljára ellenőriztem, a honlap még nem szűnt meg és nem is költözött melegebb éghajlatra. A Driftnet lefordításához szükség van néhány programkönyvtárra, ezek közül a legjelentősebb a ***libungif***, a ***libjpeg*** és a ***libcap***. Ha még nem telepítettük őket, a hivatkozások a cikk végén, a ***Kapcsolódó címek*** között megtalálhatók, de először a rendszercsomag lemezein érdemes keresnünk. A csomag lefordítása ettől kezdve egy egyszerű tarcsomag-kibontás és a `make` futtatása a forráskód könyvtárában. Ezután már futtathatjuk is a kicsomagolt programot a könyvtárból, vagy átmásolhatjuk egy megfelelőbb helyre:

```
./driftnet -i eth0
```

Mivel a Driftnet futtatásához a csatolófelületet vegyes módra kell állítani, a futtatásához rendszergazdai jogosultságra van szükség. A *3. képen* a Driftnet működés közben látható. Kétségtelen, hogy a hálózatunkon keringő képek nézegetése jó szórakozás, ha nem törődünk a folyamat sávszélességigé-



5. kép Az IPTraf alapértelmezett megfigyelőablaka

nyével. De milyen egyéb érdekes dolgok mozognak ezekben a vezetékekben? Világhálós kérések, fájlletöltések, elektronikus levelek, üzenetváltások és még egy csomó más. A legtöbb hálózatfigyelő program – a Netstatot is beleértve – megmutatja a működő kapcsolatokat, de a következő kérdés az, hogy ezek pontosan mekkora forgalmat képviselnek.

David Leonard írt egy `ncurses`-alapú programot, amely a `pktstat` nevet viseli (➲ http://www.itee.uq.edu.au/~leonard/personal/software/#pktstat), és igen jó munkát végez az egyes kapcsolatok által lefoglalt sávszélesség bemutatásának terén. Az üzemben töltött idő formájában tárolja a mindenkori hálózatterhelési értéket, de nem a futtatási sor folyamatainak, hanem az átviteli sebesség nyomon követésével. A többi programtól az a képessége különbözteti meg, hogy a hálózatunkon lévő ügyfélgépekről letöltött vagy a webkiszolgálón áthaladó adatcsomagokhoz rendelt fájlneveket meg tudja jeleníteni. A pktstat fordítása a forráskód kicsomagolásából, a megfelelő könyvtárra való váltásból és a `make` parancs futtatásából áll:

```
tar -xzvf pktstat-1.7.2q.tar.gz
cd pktstat-1.7.2q
make
su -c "make install"
```

A program futtatásakor a `-i` kapcsolóval adhatjuk meg azt a csatolót, amelyiknek a forgalmát vizsgálni szeretnénk:

```
pktstat -i eth1
```

Ekkor egy, a *4. képen* láthatóhoz hasonló ablak jelenik meg. Mint látható, elkezdtem letölteni a legfrissebb Openoffice.org-csomagot. A tényleges fájlnév a kapcsolat adatai alatt jelenik meg, ugyanez érvényes a HTTP-webkérésekre. Nemcsak a letöltés alatt álló fájl címe látszik, hanem a fájl neve is, legyen akár egy HTML-oldal vagy egy kép.

Ha már a hálózati forgalomról esett szó, és ha egyszerűen arra akarjuk fáradozásainkat összpontosítani, hogy éppen hol és mire használják a hálózatunkat, ennek kiderítésére a mai menü legutolsó fogásaként felszolgált IPTraf a legmegfelelőbb. Szerény konyhafőnökötök egyik kedvenc IP-forgalomfigyelő segédprogramja, amihez időről időre mindig visszatér, az IPTraf. Ez egy `ncurses` alapú program, ami megjeleníti az IP-forgalmat, a csomagok és bájtok számát (beleértve a nem IP-csomagokat is), az UDP-forgalmat, a bejövő és kimenő adatok mennyiségét és még sok egyebet. Az IPTraf az a csomag, amelynek mindenkinél kéznél kell lennie, akit egy hálózat felügyeletével bíztak meg.

Látogassunk el ***Gerard Paul*** Java-honlapjára (➲ http://iptraf.seul.org), és töltsünk le egy IPTraf-példányt magunknak. Csomagoljuk ki a `tar` és `gzip` programokkal becsomagolt fájlt, lépjünk a könyvtárba, és a program lefordításához futtassuk a ***Setup***-ot. A telepítési folyamat a bináris állomány ***/usr/local/bin*** könyvtárba való másolásával fejeződik be. Az IPTraf futtatásához gépeljük be az `iptraf` parancsot, nyomjunk ENTER-t, és már sínen is vagyunk (az *5. kép* egy működő IPTraf-folyamatot szemléltet).

Miközben az IPTraf összegyűjti és megjeleníti az adatokat, a képernyő nagyon hamar megtelhet. Érdemes nagyobb, például 80×40 méretű X-terminálon futtatni a programot. Az ESC gomb megnyomásával visszatérhetünk a pillanatnyi nézetből vagy folyamatból. Innen megváltoztathatjuk a beállításokat, szűrőket adhatunk hozzá vagy távolíthatunk el, majd folytathatjuk az adatgyűjtést. Az IPTraf különböző nézeteket kínál többek között az alapértelmezett állomások közötti forgalomról, a csatoló forgalmi kimutatásának alap- és részletezett adatairól, egyéb fizikai statisztikákról és a csomagméret-hibákról. Ne tévesszen meg a program látszólagos egyszerűsége. Az IPTraf elég rugalmas ahhoz, hogy az IP-megfigyelés számos igényét kielégítse.

Nos, mes amis, a záróra rohamosan közeledik. Mialatt François újratölti a poharaitokat, én annak a reményemnek adok hangot, hogy amikor elmentek, pontos képpel fogtok rendelkezni arról, hogy mi történik a hálózataitokon. A jó rendszergazdák tudják, hogy mi folyik a hálózatukon, ám emellett azt is tudják, hogy mit nem szabad észrevenniük. Ezzel emelem poharamat rátok, mes amis. A votre santé!

Bon appétit!

Linux Journal 2003. augusztus, 112. szám

Marcel Gagné (mggagne@salmar.com)
Mississaguában, Ontario államban él.
Ő a szerzője a Kiskapu kiadásában tavaly szeptemberben megjelent Linux-rendszerfelügyelet (ISBN 96-9301-40) című könyvnek (jelenleg is egy könyvön dolgozik).

KAPCSOLÓDÓ CÍMEK

Conntrack nézőke ➲ http://cv.intellos.net
Driftnet ➲ http://www.ex-parrot.com/~chris/driftnet
IPTraf ➲ http://iptraf.seul.org
Libjpeg (Independent JPEG Group) ➲ http://www.ijg.org
Libpcap (csomagbefogó programkönyvtár) ➲ http://www.tcpdump.org
Nnetstat ➲ http://www.aneptun.de/linux/Nnetstat
Marcel borlapja ➲ http://www.marcelgagne.com/wine.html
Libungif ➲ http://prtr-13.ucsc.edu/~badger/software/libungif
Pktstat ➲ http://www.itee.uq.edu.au/~leonard/personal/software/#pktstat