Vírusellenőrzés a Squid proxykiszolgálón

A rendszergazdák természetes igénye, hogy minél több vírusellenőrzési pontot iktassanak be a számítógépes hálózatokba. Az egyik ilyen pont a HTTP-proxykiszolgáló, ugyanis ezen haladnak keresztül azok az Internetről letöltött fájlok, amelyeket a felhasználók böngészői szednek le.

Amennyiben e ponton sikerül kiszűrni a vírusos állományokat, el sem jutnak a felhasználók gépeihez.
A Squid általánosan használt proxykiszolgáló, vele működik együtt a `viralator` program, amelynek segítségével elvégezhetjük a víruskeresést.
A `viralator` Perlben írt CGI-héjprogram, amely képes a bemeneti értékként megadott fájlokat letölteni a kiszolgálóra, és a letöltött állományokon egy külső vírusirtó programot futtat. Eközben a felhasználóval az ügyfélgépen futó internetböngészőn keresztül tartja a kapcsolatot, azaz tájékoztat a letöltés menetéről, és arról, hogy vírusos-e a fájl. Nézzük meg működés közben!
A böngésző ablakában a kívánt hivatkozásra kattintva kezdjük meg a letöltést. A böngésző a letöltési kérést elküldi a távoli kiszolgálóhoz – ezt a kérést kapja el a viralator program (*1. kép*). A böngészőnek visszaküld egy „downloading…” tartalmú oldalt, ezután nyit egy kék hátterű ablakot, ahol a letöltés menetét láthatjuk – az ablak alján a vírusellenőrzés eredményével. A kék ablakban egy ***Stop*** gomb segítségével a folyamatot megállíthatjuk. Ha a teljes állomány a kiszolgálóra került és nem volt vírusos, előugrik a böngésző letöltési ablaka és menthetjük a fájlt. Miután az állomány az ügyfélgépre is megérkezett, térjünk vissza a viralator kék ablakához, és nyomjuk meg a ***Close window*** gombot. Ezután egy ablak tájékoztat arról, hogy a program a kiszolgálóról letörli az állományt, majd el is tűnik.

A viralator működéséhez szükséges programok

Vírusirtó program: a viralatorba nincs vírusirtó beépítve, külső programot indít el. A múlt havi számban ismertettem a Sophos `sweep` telepítését, a viralator képes vele együttműködni.

`wget`: a böngésző által kért állományt a `wget` programmal tölti le. Mindenképpen telepítsük, nagyon hasznos program.

HTTP-proxykiszolgáló: esetünkben a Squid, azonban most sem a telepítésére, sem a beállítására nem térek ki (lásd még ***Linuxvilág*** 2001. február–márciusi számának 74. oldalát). Az ügyfelek böngészőinek az Internetet a Squiden keresztül kell elérniük.

Átirányító program: ez a Squidhez intézett letöltési kéréseket egy külső programnak küldi át. A viralatorhoz ajánlott átirányító a Squirm.

Webkiszolgáló: a `wget`-tel letöltött fájl a webkiszolgálón keresztül jut el az ügyfélgépre. Apache-kiszolgáló működését feltételezem, a telepítést pedig Debian Potato rendszerre írom le.

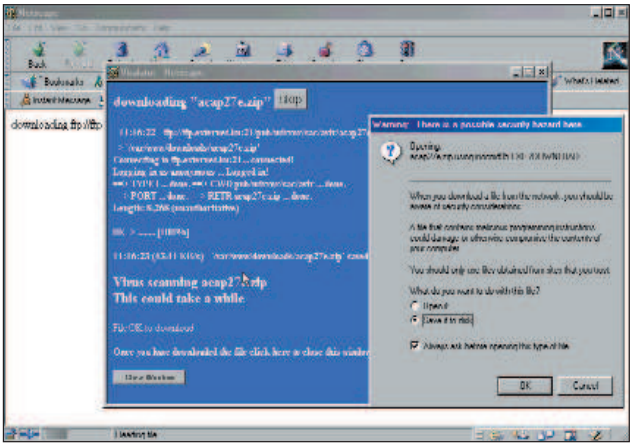
A Squirm telepítése

A Squirm honlapján a ➲ http://squirm.foote.com.au címen részletes telepítési leírást találunk, a forrást pedig a ➲ http://squirm.foote.com.au/squirm-1.0betaB.tar.gz címről tölthetjük le. Amennyiben ezt megtettük, csomagoljuk ki a */usr/src*-be, majd lépjünk be a ***squirm-1.0betaB*** könyvtárba. Adjuk ki a

```
cd regex
./configure
make clean
make
```

parancsot. A ***regex*** könyvtárban létrejövő két fájlt az eggyel feljebb lévő könyvtárba kell másolnunk:

```
cp -p regex.o regex.h ..
```



1. kép Letöltés Netscape-pel

Meg kell tudnunk, hogy a Squid milyen felhasználóként fut, amit a

```
grep cache_effective_user /etc/squid.conf
```

utasítással tehetünk meg. Debianon ez a `proxy` felhasználó, míg a Squirm a `squid` felhasználóra van beállítva. Ennek szellemében kell a Squirm Makefile-ját az `install` résznél módosítani:

```
install -m 755 -o root -g root
➥-d /usr/local/squirm \
/usr/local/squirm/bin
install -m 770 -o root -g proxy
➥-d /etc/squirm
install -m 750 -o proxy -g proxy
➥-d /var/log/squirm
install -m 660 -o root -g proxy
➥squirm.local.dist squirm.patterns.dist \
```

```
/etc/squirm
install -m 755 -o root -g root --strip squirm
➥/usr/local/squirm/bin
```

A program a beállítóállományokat eredetileg a */usr/local/squirm/etc*, a naplófájlokat pedig a */usr/local/squirm/log* könyvtárba tette. Mivel erre nem találtam elégséges indokot

2. kép A Viralator weboldala

és zavaró is lehet, ezeket is átírtam, így a fenti mintában már */etc/squirm* és */var/log/squirm* szerepel.
Ezután a ***paths.h*** fájlt is módosítani kell ott, ahol az eredeti elérési útvonalak voltak:

```
#define LOG_MATCH "/var/log/squirm/squirm.match"
#define LOG_FAIL "/var/log/squirm/squirm.fail"
#define LOG_ERROR "/var/log/squirm/squirm.error"
#define LOG_WHERE "/var/log/squirm/squirm.where"
#define LOG_DEBUG "/var/log/squirm/squirm.debug"
#define LOG_INFO "/var/log/squirm/squirm.info"

/****** Configuration file locations *******/
#define LOCAL_ADDRESSES "/etc/squirm/squirm.local"
#define REDIRECT_PATTERNS "/etc/squirm/squirm.patterns"
```

Adjuk ki a

```
make
make install
```

parancsokat és próbáljuk ki, hogy az átirányító fut-e rendszergazdaként a rendszerünkön:

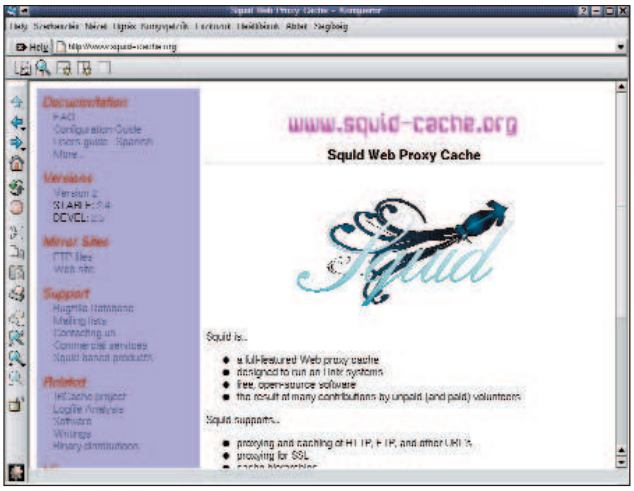
```
/usr/local/squirm/bin/squirm

Squirm running as UID 0: writing logs to stderr
Wed Nov 21 10:55:01 2001:unable to open local
➥addresses file [/etc/squirm/squirm.local]
Wed Nov 21 10:55:01 2001:unable to open
➥redirect patterns file
Wed Nov 21 10:55:01 2001:Invalid condition
➥- continuing in DODO mode
Wed Nov 21 10:55:01 2001:Squirm (PID 24924)
➥started
```

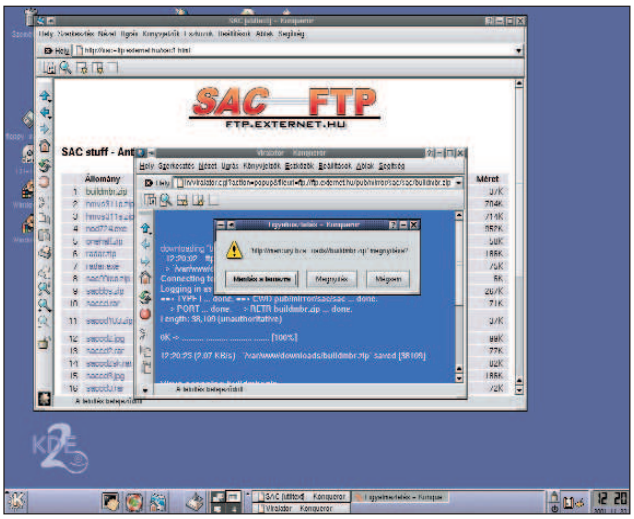
Mivel a Squirmnek a */etc/squirm* könyvtárban még nem készítettünk beállítóállományokat és csak dodo-módban indult el, CTRL+C-vel lépjünk ki.
A */etc/squid.conf* fájlban keressük meg a `redirect_program` részt és módosítsuk:

```
#redirect_program none

redirect_program /usr/local/squirm/bin/squirm
redirect_children 10
```



3. kép Hasznos programok tárháza



4. kép Letöltés Konquerorral

A Squidet indítsuk újra. A */var/log/squid/cache.log* állományban megjelenő

```
helperOpenServers: Starting 10 'squirm'
➥processes
```

bejegyzés tájékoztat arról, hogy a Squirm elindult.

A Squirm beállítása

A Squirm telepítésekor a */etc/squirm* könyvtárba két mintafájlt hoz létre: a ***squirm.local.dist***-t és a ***squirm.patterns.dist***-t. Másoljuk át őket ***squirm.local*** és ***squirm.patterns*** néven ugyanebbe a könyvtárba.