SpamAssassin – segítőtárs a mindennapokban

Könnyű és légáteresztő, a levélszemetet azonban csaknem százszázalékosan nyakon csípi.

A Linuxvilág olvasói táborának igen nagy százaléka valószínűleg azzal kezdi hétköznapjait, hogy otthon vagy a munkahelyén elektronikus postafiókját kezdi böngészni. Az elmúlt időszak kéretlen levélözöne miatt naponta akár tucatszám kapjuk a kéretlen levélszemetet. Elég egy óvatlan mozdulat és elektronikus levélcímünk máris közkincsé válhat. Vajon hogyan is történhet mindez? Például egy weboldal karbantartásával foglalkozunk, és nyilvánosságra hozott címünket egy robot leszedi. Esetleg egy nyilvános levelezési listára postáztunk egy levelet, amelynek irattárából az előbb említett robotprogram csemegézik. Előfordulhat az is, hogy egy feltört szolgáltató címlistájából jutnak hozzá stb. A sor szinte a végtelenségig folytatható.

Miként lehetséges azonban az, hogy a csupán egy-két napja létező címre özönlenek a kéretlen levelek? A kérdés inkább az, hogy miért is káros ez számunkra? Nem is olyan régen azt taglaltam, hogyan oldjuk meg, hogy leveleinkről egy telefon segítségével SMS-értesítést kapjunk. Tehát minél több a kéretlen levél, annál több a fizetett SMS. Ennél sokkal fontosabb szempont, hogy minden egyes levélszemét elolvasása után akár többezer idegsejtünk is odavész, ugyanis a folyamatos idegfeszültség miatt e kincset érő sejtjeink nagy mennyiségben pusztulnak. Az ember és a számítógép kapcsolata a nagyszámú hiba miatt amúgy sem felhőtlen, ezért ezt az amúgy sem rózsás helyzetet nem célszerű tovább rontani. Mennyivel egyszerűbb feltelepíteni egy levélszemétszűrőt, amely megteremtheti számukra a csaknem felhőtlen levelezést!

A SpamAssassin egy olyan szűrőprogram, amelynek beállítását egy teljesen kezdő is bármikor meg tudja tenni. Ugyanakkor finomhangolása megfelelő, sőt még a kéretlennek ítélt levelek sem vesznek el, hanem egy külön erre a célra fenntartott állományba kerülnek, hiszen ki tudja, lehet, hogy egy levélszemétnek nyilvánított levél mégis értéket képviselhet. A legegyszerűbb, ha letöltjük a ➲ http://www.spamassassin.org címről.

A Debian Woody-felhasználók az `apt-get install spamassassin` parancs kiadásával is telepíthetik. Azok, akik forrásból telepítenék: egy rendkívül részletes ***README*** állomány áll a rendelkezésükre, amely lépésről lépésre leírja, hogyan telepítsük. Ezek után nincs másra szükségünk, mint hogy saját könyvtárunkban egy ***.procmailrc***-t helyezzünk el, ugyanis a szűrőprogramot a Procmail fogja meghívni, az összes fogadott levelünk így kerül elemzésre. A következő sorokat tehát a */home/felhasználónevem/.procmailrc* állományban helyezzük el:

```
:0fw
| spamassassin -P

:0:
* ^X-Spam-Status: Yes
caughtspam
```

Így a bejövő levél először átadódik a Spamassassinnek, amely eldönti róla, hogy kiszűrendő levél-e vagy sem. Ezek után a levél fejlécrészébe befűzi a kiértékelés eredményét. Ha kéretlen, a levél tárgya kiegészül a

```
*********SPAM********
```

szöveggel, valamint a levéltestbe egy indoklás kerül, hogy miért is lett kiszűrve, valamint a `X-Spam: Yes` sor is megjelenik benne. Amikor a Procmail a levelet visszakapja, a következő szabályon (`[X-Spam-Status]`) fennakadva a ***Caughtspam*** postaládába kerül. Így nem fordulhat elő, hogy egy ismerősünk fontos levele végképpen kárba vész.

Álljon itt egy jellegzetes levélszemét kiértékelése (lásd a *listán*). Jól látható, hogy a program leveleinket az előre beállított szabályok szerint pontozza, és ha a levélben hivatkozás található vagy az `unsubscribe` felirat szerepel – ami a levélszemétre

```
SPAM: ---------------- Start SpamAssassin results ----------------------
SPAM: This mail is probably spam.  The original message has been altered
SPAM: so you can recognise or block similar unwanted mail in future.
SPAM: See http://spamassassin.org/tag/ for more details.
SPAM:
SPAM: Content analysis details:   (19.4 hits, 5 required)
SPAM: Hit! (2.3 points)  BODY: Gives a lame excuse about why you were sent this SPAM
SPAM: Hit! (0.7 points)  BODY: Talks about email marketing
SPAM: Hit! (1.5 points)  BODY: Asks you to click below
SPAM: Hit! (3.5 points)  URI: URL of page called "unsubscribe"
SPAM: Hit! (1.3 points)  URI: Includes a 'remove' email address
SPAM: Hit! (4.8 points)  BODY: Frontpage used to create the message
SPAM: Hit! (2.1 points)  BODY: FONT Size +2 and up or 3 and up
SPAM: Hit! (0.0 points)  BODY: Includes a URL link to send an email
SPAM: Hit! (3.2 points)  HTML-only mail, with no text version
SPAM:
SPAM: --------------- End of SpamAssassin results ---------------------
```


```
1:Kilép  -:Előző  <Space>:Következő  v:Melléklet  d:Töröl  r:Válasz  j:Köv. ?:Súgó
*2002/04/06 19:28:30 hughescr Exp $)
X-Spam-Prev-Content-Type: text/html
X-Spam-Prev-Content-Transfer-Encoding: 8bit

SPAM: -------------------- Start SpamAssassin results ----------------------
SPAM: This mail is probably spam.  The original message has been altered
SPAM: so you can recognise or block similar unwanted mail in future.
SPAM: See http://spamassassin.org/tag/ for more details.
SPAM:
SPAM: Content analysis details:   (18.7 hits, 5 required)
SPAM: Hit! (2.4 points)  'Message-Id' was added by a relay (2)
SPAM: Hit! (3.8 points)  BODY: Gives instructions for removal from list
SPAM: Hit! (2.7 points)  BODY: Claims you can be removed from the list
SPAM: Hit! (1.5 points)  BODY: Asks you to click below
SPAM: Hit! (1.4 points)  BODY: Claims you can be removed from the list
SPAM: Hit! (-1.6 points) BODY: Contains a claim of copyright
SPAM: Hit! (3.5 points)  URI: URL of page called "unsubscribe"
SPAM: Hit! (1.8 points)  BODY: Tells you to click on a URL
SPAM: Hit! (3.2 points)  HTML-only mail, with no text version
SPAM:
SPAM: -------------------- End of SpamAssassin results ---------------------
-0  --  4/6: Free 4 You              *****SPAM***** Your Freebies Have Arri --  (55%)
```

jellemző –, akkor egy bizonyos pontértéket kap. Mivel nem lenne jó, ha például egy hivatkozás miatt a levelünk levélszemét-értékelést kapna, hiszen ismerőseinktől naponta több tucat értékes hivatkozás futhat be, a kéretlen levél csak akkor lesz bélyegezve, ha több pontban is bűnösnek találtatott. Ilyen pontrendszert mi is bármikor felállíthatunk. Fontos azonban, hogy amennyiben levelezési listákra is feliratkoztunk, ezt vagy a szűrési szabályzatba vegyük bele, vagy ennél jóval egyszerűbb, ha a Spamassassint a Procmail legutolsó soraiba rakjuk, hiszen ilyenkor feltehetően a levelezési listákat már különböző szabályok alkalmazásával leválogattuk, és csak ez után kerül sor a levélszemétszűrésre. Például így:

```
:0
* ^Reply-To: linux@mlf.linux.rulez.org
$MAILDIR/linux/

:0
* ^(From|Cc|To|Reply\-To|Delivered-\To):.
➥*bugtraq@lists.securityfocus.com
$MAILDIR/bugtraq/
```

Ekkor a `mlf` és `bugtraq` listákat leválogatjuk, a levélszemétszűrő sorokat csak utána írjuk.
Ezek után garantáltan nem fogunk idegeskedni. A ***caughtspam*** állományba került leveleket naponta érdemes átnézni, hogy nem akadt-e bele mégis egy rendes levél, a személyes tapasztalatom azonban az, hogy az ember jókat mulat egy-egy elfogott levélen. Jó vadászatot!

Varga S. Csaba
(guska@guska.hu) az 1.1-es Slackware óta linuxozik. Kedvtelései közé tartozik a fotózás és Linux telepítése PDA-kra. Legszívesebben a Gerecsében túrázik a barátaival.

Biztonsági indítólemez készítése

Amikor operációs rendszert telepítünk, és a telepítő megkérdi, hogy akarunk-e biztonsági indítólemezt létrehozni, a helyes válasz: Yes (Igen). Ha valamilyen különös oknál fogva ezt a lépést átugrottuk volna a telepítés során, soha nem késő, hogy visszatérjünk és létrehozzunk egyet.
A lemez elkészítésének egyik oka, hogy amikor a rendszert telepítettük, lehetőségünk volt a LILO-t választani rendszerindító eszköznek. Megszokott körülmények között ez a legkézenfekvőbb. A LILO lehetővé teszi a több rendszermag közül való választást, és a választható rendszerindítást, amellyel a Linux és Windows felváltva történő használata egyszerűen megoldható. Amennyiben a jövőben valamilyen okból a LILO mellőzése mellett döntünk, az indítólemez lehet az eszköz, amellyel a Linux-rendszer indítható marad. Így vagy úgy, de mindenképpen jó, ha a biztonság kedvéért rendelkezünk indítólemezzel.
A következőkben bemutatom, hogyan lehet utólag létrehozni egyet. Szükség lesz egy üres, formázott, nem írásvédett lemezre. Mivel a művelet minden adatot felülír a lemezen, az üres lemezre vonatkozó javaslatom betartásával elkerülhetjük, hogy esetleg fontos adatainkat veszítsük el. Helyezzük a lemezt a meghajtóba, majd adjuk ki a következő parancsot:

```
mkbootdisk magvÆltozat
```

A rendszermagváltozat részt azzal a változattal kell helyettesíteni, amelyikről a rendszert indítottuk. Ezt a parancssorba gépelt `uname -r` parancs segítségével tudhatjuk meg. Amikor próbarendszeremen ezt a parancsot kiadtam, a következő eredményt kaptam:

```
2.2.14-test
```

A `-r` kapcsoló utasítja az `uname` parancsot az operációs rendszer változatszámának közlésére. Ezzel az adattal és a parancs futtatásával létrehozhatjuk az indítólemezt:

```
mkbootdisk 2.2.14-test
```

Megjegyzendő, hogy az `mkbootdisk` parancs egy *vmlinuz-változatszám* nevű rendszermagot, valamint a */lib/modules* elérési útvonalon egy *változatszám* nevű modulkönyvtárat keres. Az előző példa alapján tehát egy */boot/vmlinuz-2.2.14-test* nevű rendszermaggal és egy */lib/modules/2.2.14-test* modulkönyvtárral kellett volna rendelkeznem. Azért említem mindezt, mert a rendszermagot tetszőleges néven menthetjük, azonban a */lib/modules* bejegyzés ettől különbözhet. Jó ötlet *vmlinuz-változatszám* formában menteni az új rendszermagokat a */boot* könyvtár alá.
Tudnunk kell azonban, hogy az `mkbootdisk` parancs nem található meg minden rendszeren. Például Debian próbarendszeremen az `mkboot` parancsot használtam indítólemez létrehozására (bár a rendszer alkalmat adott rá, hogy már a telepítéskor megtegyem):

```
# mkboot
```

Itt egy kisebb nehézség adódott: az `mkboot` parancs a *vmlinuz* állományt (a Linux rendszermagját) a */boot* könyvtárban keresi.

Részlet Marcel Gagné: Linux-rendszerfelügyelet című könyvéből