Squirrelmailov dodatak "Squirrel Logger"

Squirrelmail je jedan od najpopularnijih webmail sustava, vjerojatno ga imate instaliranog zahvaljujući tome što dolazi u obliku CARNetova paketa. Postoji nekoliko desetaka plugina za Squirrelmail. Upoznat ćemo vas sa "Squirrel Logger" pluginom, jer on upotpunjava niz od nekoliko članaka koje smo planirali oko problema zloporabe mail poslužitelja.

Dakle, ponekad želimo znati tko to točno i kada šalje mailove iz Squirrelmaila, jer on te informacije sam "nerado" prikazuje. Razlog zašto bi željeli znati tko šalje mailove preko Squirrelmaila je najčešće provala u sustav, odnosno činjenica da je netko otkrio zaporku korisnika i počeo zlorabiti vaš sustav za spamiranje. Drugi razlozi mogu uključivati discipliniranje i praćenje korisnika koji ne poštuju dogovore o načinima uporabe sustava i slično.

Squirrelmail Logger plugin se instalira kao i svaki drugi plugin za Squirrelmail. Potrebno je skinuti arhivu na adresi:

http://www.squirrelmail.org/plugin_view.php?id=52 [1]

Arhivu squirrel_logger-2.3.1-1.2.7.tar.gz raspakirajte u direktoriju /usr/share/squirrelmail/plugins, te iskopirajte demo konfiguraciju:

```
# cd /usr/share/squirrelmail/plugins
# tar xvfz squirrel_logger-2.3.1-1.2.7.tar.gz
# cd squirrel_logger
# cp config_example.php config.php
# /usr/share/squirrelmail/config/conf.pl
```

Sa 8 odaberite "Plugins", te potom plugin "squirrel_logger". Snimite sa "s" i izađite sa "q".

Za početak, dovoljno je da odkomentirate sljedeće unose:

```
   $sl_log_events = array(
                              'LOGIN',
                              'LOGOUT',
//                            'TIMEOUT',
//                            'OUTGOING_MAIL',
                              'MASS_MAILING',
//                            'LOGIN_ERROR',
//                            'ERROR',
//                            'CAPTCHA',
//                            'RESTRICT_SENDERS',
//                            'LOCKOUT',
   );

   $sl_logs = array(
      'SYSTEM:LOG_INFO:LOG_MAIL' => array(
         'LOGIN'            => "Successful webmail login: by %2 (%3) at %4 on %6: %7"
,
```

```
        'LOGOUT'           => "Webmail logout: by %2 (%3) at %4 on %6: %7",
//      'TIMEOUT'          => "Webmail session timed out: by %2 (%3) at %4 on %6: %7"
,
...
```

Prvo polje ($sl_log_events) određuje koje ćete događaje logirati, a drugo polje ($sl_logs) kako će se ti događaji bilježiti (syslog, datoteka, sql baza) i što će se u njih upisivati.

Gornje promjene će biti dovoljne da u logovima (/var/log/syslog, /var/log/mail.log) dobijete unose poput ovih:

```
Dec 28 14:22:43 server 0: Successful webmail login: by korisnik
 at 161.53.XX.YYY on 12/28/2011 13:22:43:

Dec 28 14:30:23 server 0: Webmail logout: by korisnik (server.domena.hr) at
 161.53.XX.YYY on 12/28/2011 13:30:23:

Dec 29 15:54:02 po 0: Possible outgoing spam: by korisnik (server.domena.hr) at 161.5
3.XX.YYY
  on 12/28/2011 14:54:02: Total 18 recipients
```

To nije sve, jer je moguće logirati i druge stvari. Najzanimljivija je mogućnost logiranja mailova ako broj primatelja prelazi određeni (konfigurabilni) iznos. U terminologiji ovog plugina, to se zove "*mass mailing*":

'MASS_MAILING'   => "Possible outgoing spam: by %2 (%3) at %4 on %6: %7",

Kao što možete pretpostaviti, sve je dosta konfigurabilno, te možete promijeniti što će se logirati pomoću parametara:

%1 - ime događaja
%2 - ime korisnika
%3 - naziv domene
%4 - adresa udaljenog računala
%5 - timestamp (vrijeme događaja)
%6 - datum
%7 - neki komentar koji sami definirate

No, to nije sve (znamo, znamo, zvučimo kao u TV reklami). Pomoću ovog plugina možete, umjesto zapisivanja u logove, poslati mail na neku e-mail adresu. Kako ovo može izazvati dosta maila, predviđeno je da se šalju samo kritične obavijesti:

```
   $sl_send_alerts = array(
      'MASS_MAILING'  =>  "Possible outgoing spam: by %2 (%3) at %4 on %6: %7",
      'LOGIN_ERROR'   =>  "Failed webmail login: by %2 (%3) at %4 on %6: %7",
      'ERROR'         =>  "Webmail error: by %2 (%3) at %4 on %6: %7",    );
```

Adresa na koju se šalje pošta je u standardnoj vrijednosti naslovljena na postmastera, što zapravo ne treba mijenjati, jer bi alias postmaster trebao biti preusmjeren na root korisnika, a rootov mail bi trebali dobijati vi. Naravno da možete promijeniti ovu vrijednost ukoliko želite mailove slati na, primjerice, GMail. Obavijesti izgledaju ovako:

Naslov: [WEBMAIL ALERT] MASS_MAILING - korisnik
Šalje: noreply@server.domena.hr
Datum: Čet, prosinac 29, 2011 4:45 pm
Prima: postmaster@domena.hr

Prioritet: običan
Postavke: Pregled cijelog zaglavlja | Prikaži verziju za tisak | Spusti kao datoteku

Possible outgoing spam: by korisnik (server) at 161.53.XX.YYY on 12/29/2011 15:45:05: Total 27 recipients

VAŽNO: za slanje pošte morat ćete instalirati "Compatibility Plugin", inačice barem 2.0.11 (aktualna je 2.0.16)

Ostale postavke su manje-više same po sebi razumljive. Možete podesiti što će logovi i izvješća sadržavati (koja zaglavlja), na koga će glasiti mail obavještenja, koji će se mail poslužitelj rabiti i slično.

Osim preko *syslog* mehanizma, moguće je zapisivati i direktno u SQL bazu. Za ovu se brinu polja

```
'FILE'   => array(
    'LOGIN'         =>  "%6 [%1] %2 (%3) from %4: %7\n",
    'LOGOUT'        =>  "%6 [%1] %2 (%3) from %4: %7\n",
    'TIMEOUT'       =>  "%6 [%1] %2 (%3) from %4: %7\n",
)
```

i

```
'SQL'    => array(
   'LOGIN'         =>  'LOGIN',
   'LOGOUT'        =>  'LOGOUT',
   'TIMEOUT'       =>  'TIMEOUT',
   'MASS_MAILING'  =>  'MASS_MAILING',
   'LOGIN_ERROR'   =>  'INVALID',
   'ERROR'         =>  'ERROR',
)
```

A ostalo je na vama...

- Logirajte [2] se za dodavanje komentara

čet, 2011-12-29 15:28 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Software [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (4 votes)

Source URL: https://sysportal.carnet.hr/node/906

Links
[1] http://www.squirrelmail.org/plugin_view.php?id=52
[2] https://sysportal.carnet.hr/sysportallogin
[3] https://sysportal.carnet.hr/taxonomy/term/17

[4] https://sysportal.carnet.hr/taxonomy/term/25