Plesk: Plesk & Qmail: Greylisting mit spamdyke

Über Greylisting selbst möchte ich hier mal keine Worte verlieren. Einfach meinen Artikel darüber lesen.

Der Entwickler von spamdyke wollte Spam bereits zum Zeitpunkt des Empfangs zu erkennen und ggf. zurück zu weisen. Insbesondere war dies auch der richtige Ort zum Einsatz eines Greylisting-Mechanismus.

Ein primäres Ziel war es, das alles ohne Neukompilierung von Qmail zu schaffen.

Aufgrund dessen ist spamdyke nicht nur für Plesk geeignet, sondern auch für VISAS/ServerAdmin24, welches ebenfalls Qmail als MTA nutzt.

Installation von Spamdyke

Dieses Howto entstammt mehreren Quellen. Am nähsten ist es folgendem angelehnt:

Mini-HOWTO: Spam-Abwehr für Plesk und qmail mit spamdyke

Vorbereitung

Wir brauchen die üblichen (verdächtigen) Programme um Spamdyke zu kompilieren: gcc und openssl-Devel

```
# OpenSuSE Linux
yast -i gcc openssl-devel
# Debian oder Ubuntu Linux
aptitude install gcc libssl-dev
# Fedora, RHEL oder CentOS
yum install gcc openssl-devel
```

Download & Kompilieren

Vor dem Download auf aktualisierte Version prüfen!

```
#Download
cd /usr/local/src
wget http://www.spamdyke.org/releases/spamdyke-4.0.1.tgz
tar -xzf spamdyke-4.0.1.tgz
cd spamdyke-4.0.1
cd spamdyke

#Kompilieren
```

```
./configure && make
make install
```

Wer noch weitere Spamdyke-Tools nutzten möchte, sollte noch die `utils` kompilieren.

Da diese Tools nicht für das Greylisting nötig sind, sind diese hier auch nicht das Thema. Bitte lest dazu die spamdyke-Doku.

```
cd utils
./configure && make
cp dnsa dnsany dnsany_libc dnsmx dnsns dnsptr dnssoa dnstxt domain2path domainsplit
/usr/local/bin
```

Konfiguration von spamdyke

Hier eine `/etc/spamdyke.conf` die auf Plesk zugeschnitten ist (Danke an Roger Wilco!):

```
#für das Plesk-Addon von Haggybear:
log-level=info

local-domains-file=/var/qmail/control/rcpthosts
tls-certificate-file=/var/qmail/control/servercert.pem

#Copy&Paste from xinetd-conf
smtp-auth-command=/var/qmail/bin/smtp_auth /var/qmail/bin/true
/var/qmail/bin/cmd5checkpw /bin/true
smtp-auth-level=ondemand-encrypted

#wichtiger Timeout:
idle-timeout-secs=300
graylist-level=always-create-dir
graylist-dir=/var/qmail/spamdyke/greylist
#300 Sek. = 5 Min.
graylist-min-secs=300
#1814400 Sek. = 3 Wochen
graylist-max-secs=1814400

sender-blacklist-file=/var/qmail/spamdyke/blacklist_senders
recipient-blacklist-file=/var/qmail/spamdyke/blacklist_recipients
ip-in-rdns-keyword-blacklist-file=/var/qmail/spamdyke/blacklist_keywords
ip-blacklist-file=/var/qmail/spamdyke/blacklist_ip
rdns-whitelist-file=/var/qmail/spamdyke/whitelist_rdns
ip-whitelist-file=/var/qmail/spamdyke/whitelist_ip
sender-whitelist-file=/var/qmail/spamdyke/whitelist_senders
```

```
greeting-delay-secs=5

#ggf. auskommentieren:
dns-blacklist-entry=ix.dnsbl.manitu.net
dns-blacklist-entry=zen.spamhaus.org
dns-blacklist-entry=list.dsbl.org
dns-blacklist-entry=zombie.dnsbl.sorbs.net
dns-blacklist-entry=dul.dnsbl.sorbs.net
dns-blacklist-entry=bogons.cymru.com

reject-missing-sender-mx
reject-empty-rdns
reject-unresolvable-rdns
reject-ip-in-cc-rdns
```

Als nächstes müssen noch Dateien und Verzeichnisse mit den richtigen Nutzerrechten für Qmail angelegt werden.

Der jeweilige Inhalt ist bereits im Namen erkenntlich. Hier können also Whitlisten und Blacklisten verwaltet werden.

```
mkdir /var/qmail/spamdyke
mkdir /var/qmail/spamdyke/greylist
touch /var/qmail/spamdyke/blacklist_ip
touch /var/qmail/spamdyke/blacklist_recipients
touch /var/qmail/spamdyke/whitelist_ip
touch /var/qmail/spamdyke/whitelist_senders
touch /var/qmail/spamdyke/blacklist_keywords
touch /var/qmail/spamdyke/blacklist_senders
touch /var/qmail/spamdyke/whitelist_rdns
chown -R qmaild:qmail /var/qmail/spamdyke
```

Damit wäre spamdyke soweit einsatzbereit. Nun binden wir ihn in die SMTP-Verarbeitung ein.

Dazu wird spamdyke einfach vor den Aufruf von `qmail-smtpd` in die `inetd`- bzw. `xinetd` -Konfiguration gesetzt

Hier ein Beispiel einer `/etc/xinetd.d/smtp_psa` (also Plesk mit `xinetd`):

```
service smtp {
 ...
 server          = /var/qmail/bin/tcp-env
```

```
 server_args     = -Rt0 /var/qmail/bin/relaylock /usr/local/bin/spamdyke -f
/etc/spamdyke.conf /var/qmail/bin/qmail-smtpd /var/qmail/bin/smtp_auth
/var/qmail/bin/true /var/qmail/bin/cmd5checkpw /var/qmail/bin/true
}
```

Es kann theoretisch auch vor den `relaylock` gesetzt werden. Aber in der Praxis findet man es meistens dahinter.

Im Falle von Plesk muß auch die `smtps_psa` bearbeitet werden.

Nach einem Reload/Neustart von `xinetd` ist spamdyke in Betrieb. Erste Erfolge kann man im Verzeichnis `/var/qmail/spamdyke/greylist/` händisch nachsehen.

Hier ein Beispiel für die inetd.conf. (Achtung: alles in eine Zeile!)

```
smtp stream tcp nowait.100 root /var/qmail/bin/tcp-env tcp-env
 /usr/bin/env SMTPAUTH=1
 /var/qmail/bin/relaylock /usr/local/bin/spamdyke -f /etc/spamdyke.conf
 /var/qmail/bin/qmail-smtpd /var/qmail/bin/smtp_auth /var/qmail/bin/true
/var/qmail/bin/cmd5checkpw /var/qmail/bin/true
```

Beachtet, daß die (Gesamt-)Zeilenlänge bei `inetd` auf 255 Zeichen beschränkt ist.

Das bedeutet, daß die zusätzlich dazuwischen geschaltete Programme wie z.B. `rblsmtp` keinen Platz mehr haben. (Macht ja auch keinen Sinn, da Spamdyke ebenfalls RBL's prüfen kann.)

Alternativ kann man auch alles in ein Script auslagern. Dort unterliegt man nicht mehr dieser Zeichenbegrenzung.

Aufräum-Script

Auch spamdyke kommt leider ohne eigenem Aufräum-Script daher. Damit die Platte nicht voll läuft, bauen wir uns ein eigenes Script, welches die Verzeichnisstruktur nach zu alten einträgen durchsucht und direkt löscht:

Wir erstellen die Datei /etc/cron.daily/spamdyke.sh

```
#!/bin/sh
```

```
# leeren Eintraegen loeschen (aelter als 10080 Minuten (=1 Woche))
/usr/bin/find /var/qmail/spamdyke/greylist/ -type f -mmin +10080 -size 0 -delete

if [ -f /usr/bin/bc ] ; then
 #Wenn bc installiert ist, kann es automatisch ermittelt werden
 GRAYLIST_MAX_SECS=`grep 'graylist-max-secs' /etc/spamdyke.conf | cut -d = -f 2`
 GRAYLIST_MAX_SECS=`echo "scale=0 ; $GRAYLIST_MAX_SECS / 60" | bc -l`
else
 #Achtung: sollte mit graylist-max-secs /60 in /etc/spamdyke.conf identisch sein
 #aelter als 30240 Minuten (=3 Wochen)
 GRAYLIST_MAX_SECS=30240
fi
# veraltete Eintraege loeschen
/usr/bin/find /var/qmail/spamdyke/greylist/ -type f -mmin +$GRAYLIST_MAX_SECS -delete
#Erweiterung von Haggybear:
for i in `ls -1 /var/qmail/spamdyke/greylist`; do
     /usr/bin/find /var/qmail/spamdyke/greylist/$i/ -depth -type d -empty -delete; 2›&1
›/dev/null
done
```

Nicht vergessen: Die Datei mit `chmod +x /etc/cron.daily/spamdyke.sh` ausführbar machen.

Die eingetragenen Zeiten sind nur Beispielhaft. Wer mehr Mail-Traffic auf seinem Server hat und die Greylisting-Daten entsprechend mehr Platz einnehmen, kann die Werte nach unten anpassen. 3 Tage Wartezeit sollte man aber schon mindestens einhalten.

Achtung!!!

Spamdyke ist noch nicht ganz ausgereift!

Aufgrund einiger Programmfehler stürzt Spamdyke ab, bzw. erkennt nicht, daß die SMTP-Connection abgebrochen ist. Dies führt dazu, daß sich die Spamdyke-Prozesse anhäufen.

Abhilfe schaft ein `/usr/bin/killall spamdyke` an beliebige Stelle im o.g. Aufräum-Script.

Weitere Links

- Haggybear's Plesk Spamdyke Control Panel
- Greylisting: Vor- und Nachteile
- Plesk/Qmail: Spamdyke mit MySQL-Logging

Plesk: Plesk & Qmail: Greylisting mit spamdyke

- Plesk & Qmail: Spamprotection mit Greylisting
- Debian/Postfix: Greylisting mit Postgrey
- SuSE/Postfix: Greylisting mit Postgrey
- Artikel bei Wikipedia: Greylisting
- Offizielle Site: spamdyke

  - Readme
  - FAQ

Eindeutige ID: #1324
huschi
2008-11-10 12:27