Linux Kullanıcıları Derneği
ve
Elektrik Mühendisleri Odası

Linux Seminerleri

www.linux.org.tr
www.emo.org.tr

Qmail E-Posta Sunucusu ve qSheff ile Virus/Spam Filtreleme

Afşin TAŞKIRAN

EnderUNIX Yazılım Geliştirme Takımı
afsin@enderunix.org
www.EnderUNIX.org/afsin

-Sunum İçeriği

- D. J. Bernstein
- qmail
- qSheff

-- D. J. Bernstein Kimdir ?

1971 doğumludur. Chicago'daki Illinois Üniversitesi Bilgisayar Bilimleri Bölümü'nde profesör ünvanıyla bulunmaktadır. Matematik bölümü mezunudur. Asıl ilgi alanı kriptografidir.

-- D. J. Bernstein'in Bazı Yazılımları

- Qmail
- djbDNS
- ucspi-tcp (tcp wrapper, recordio, rblsmtpd...)
- Daemontools (UNIX service management system)
- Cdb (fast, reliable, simple package for creating and reading constant databases.)
- Ezmlm liste yöneticisi

-- Qmail Nedir ?

qmail, Unix işletim sistemleri üzerinde MTA (Mail Transport Agent) olarak çalışan bir yazılımdır.

-- Qmail Nedir ?

MTA'nın en temel görevi, hizmet vermekte olduğu kullanıcıların başka kullanıcılara e-posta göndermesini sağlamak ve başka kullanıcılardan gelen e-postaları yerel kullanıcılara iletmek üzere teslim almaktır.

-- Qmail Nedir ?

Kullanıcılar genellikle MTA'ları doğrudan kullanmazlar, bunların yerine MUA (Mail User Agent) denen yazılımları kullanırlar.

-- Qmail Geliştirme Süreci

Sendmail'in güvenlik açıklarından bıktığını belirten D. J. Bernstein, bunun yerine kullanılmak üzere qmail'i yazmıştır. D. J. Bernstein, ilk sürümünü beta 0.70 olarak 24 Ocak 1996'da duyurmuştur.

-- Qmail Geliştirme Süreci

Yazılım geliştirme süreci sonrasında tam kullanılabilir halde 1.0 versiyonu 20 Şubat 1997'de kullanıcılara sunulmuştur.

-- Qmail Geliştirme Süreci

1.0 sürümünün duyurulmasından sonra yazılım geliştirilmeye devam edilmiş ve şu anda kullanılabilir sürümü olan 1.03 versiyonu 15 Haziran 1998'de duyurulmuştur.

- Neden Qmail ?

-- Güvenlik

-- Basitlik

-- Performans

-- Güvenilirlik

-- Modüler Yapı

- Neden Qmail ?

--Güvenlik:

Qmail, güvenlik özellikleri düşünülerek yazılmıştır.

- Neden Qmail ?

--Güvenlik:

D. J. B. , qmail yazılımında güvenlik zaafı bulan ilk kişiye 500$ ödül verileceğini bildirmiştir.

Mart 1997'de yapılan bu duyurudan sonra henüz bu ödülü kazanabilecek birileri çıkmamıştır.

http://cr.yp.to/qmail/guarantee.html

- Neden Qmail ?

--Güvenlik:

--- Sendmail'e göre daha az root veya setuid olarak çalışan program vardır.

--- Güvenlik sebebiyle qmail'de sadece qmail-queue programı root olarak çalışmaktadır.

--- qmail'de işler farklı kullanıcı haklarıyla çalışan farklı programlar tarafından yapılmaktadır.

---qmail programları kendi aralarında haberleşirken ayrıştırma yapmak yerine veri yapıları kullanırlar.

--- Standart C kütüphanesiyle temiz kod yazılmıştır.

- Neden Qmail ?

--Basitlik:

“Keep it simple”

Kısa ve sade kod yapısı ile aynı anda yüzlerce e-posta gönderebilir, az bellek kullanır, güvenlik açığı yaratmaz.

- Neden Qmail ?

--Performans:

qmail, pek çok maili aynı anda paralel olarak gönderir. Özellikle e-posta listecileri için tercih sebebidir. E-posta listecilerinin mailleri yönetebilmesi için ilave başlık bilgileri tutar.

- Neden Qmail ?

--Güvenilirlik:

qmail, bir mesaj aldığında onun kaybolmayacağını garanti eder. qmail ile birlikte Maildir posta kutusu türü ortaya çıkmıştır.

Maildir sayesinde kilit değişkeni kullanılmaz ve aynı posta kutusuna eşzamanlı olarak birden fazla kullanıcı erişim sağlayabilir. Çünkü posta kutusu bir dosya değil bir dizindir.

- Neden Qmail ?

--Modüler Yapı:

qmail, tasarım itibariyle modüler yapıda yazılmıştır.

Her işlevi en iyi şekilde gören bir program vardır ve bu programlar da oldukça anlaşılır ve esnek yazıldığı için qmail'e üçüncü parti bir yazılım yazmak çok kolay hale gelmiştir.

- qmail Lisansı

qmail'in lisansı, yazarın izni olmadan kaynak kodlarında değişiklik yapılıp dağıtılmasına izin vermemektedir.

qmail'in kodlarını istediğiniz şekilde kullanabilir, fakat değiştirilmiş kaynak kodunu dağıtamazsınız.

Lisansdaki bu kısıtlamanın en büyük sebebi yazar D.J.B.'nin qmail'e eklenecek kod parçası ile qmail'de herhangi bir sorun oluşacağı düşüncesidir.

- qmail Referansları

- Yahoo Mail
- Yahoo Groups
-Network Solutions
- Mynet Mail
- Superonline
...

- qmail Kurulumu

qmaild, qmaill, qmailp, qmailq, qmailr, qmails kullanıcıları; nofiles, qmail grupları sistemde tanımlanır.

ftp://ftp.ntnu.no/pub/unix/mail/qmail/qmail-1.03.tar.gz

Adresinden qmail kaynak kodları indirilir ve `make setup check; ./config` ile kurulur.

/var/qmail/alias dizininin altında .qmail-root, .qmail-postmaster, .qmail-mailer-daemon dosyalarına takma isimler tanımlanır.

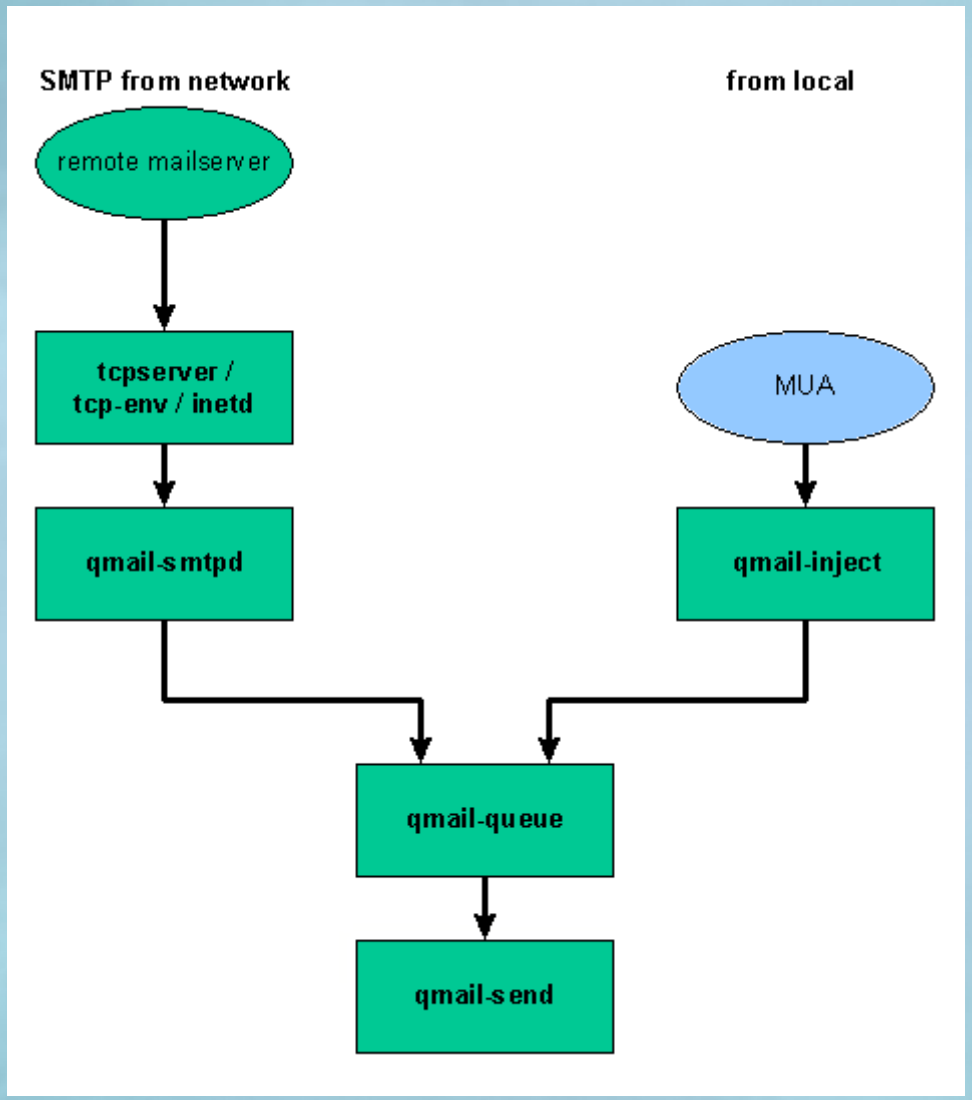
http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
http://cr.yp.to/daemontools/daemontools-0.76.tar.gz

Adreslerinden indirilerek kurulur.

-qmail Kurulumu

- echo ./Maildir > /var/qmail/control/defaultdelivery
- /var/log/qmail ve yapılandırmaya bağlı olarak altındaki dizinler oluşturulur.
- /var/qmail/supervise/ dizinleri ve altındaki çalıştırma (run) betikleri oluşturulur.
- echo '127.:allow,RELAYCLIENT="" >> /etc/tcp.smtp
- /var/qmail/bin/maildirmake /home/afsin/Maildir
- qmailctl start

- qmail çalışma prensibi



qSheff Projesi

qSheff Nedir ?

qSheff, qmail mail kuyruğuna girecek emaillerin virüs ve spam filtreleme programları tarafından konrol edilebilmesi için bir ara programdır.

qSheff Projesi

- Yazar

EnderUNIX Yazılım Geliştirme Takımı'ndan Barış ŞİMŞEK tarafından geliştirilmiştir.

www.enderunix.org/simsek

qSheff Projesi

- Özellikler

Basit, hızlı ve gelişmeye açık C kodu
Değişik Antivirus ve programlarla çalışabilme
ClamAV ile doğrudan konuşabilme
Özel hata mesajları tanımlayabilme
Spam olan maillerin konu kısımlarnı işaretleme
Yerel kullanıcıları filtrelerden hariç tutma
Spam yapanlara cevap dönmeme özelliği
Başlık ve gövdeyi ayrı ayrı tarayabilme
Düzenli ifade desteği
İsim ve uzantıya göre eklentileri engelleme
Kara liste desteği
Basit kurulum ve yönetim
Detaylı kayıt
Kolay sorun giderme
Karantina ve tüm mail trafiğinin yedeklenmesi
Bozuk başlıklı mailleri engelleme

qSheff Projesi
- Spam Filtreleme

- qSheff ile maillerin bölümlerine ayrı ayrı filtremele kuralları tanımlayabilirsiniz. (body, header). qSheff bu şekilde mail içeriğinde tam denetim sağlar.

- Düzenli ifade (regular exp.) desteği ile esnek kural tanımlayabilme.

qSheff Projesi
- Spam Filtreleme

#vi /usr/local/etc/qsheff/qsheff.rules

h:(^X-Mailler: spammer mailler v.1)
h:(^Subject: [Vv]iagra)(pharmacy)
b:(save)(rate)(per)(month)

Buradaki "h" mail'in başlık kısmı (From, To, Subject, X-Mailler, ...), "b" ise mesajin gövde (body) kısmını ifade eder.

qSheff Projesi
- subject tag

Bu özellikle birlikte spam olarak belirlenen maillerin konu kısımlarının başına ***SPAM*** kelimesi eklenir ve mail kullanıcıya teslim edilir.

Bu özellik ile masum maillerin spam algılanması nedeni ile oluşabilecek mail kayıpları ortadan kalkacaktır. Spam'lar MUA'da filtre yazarak bir klasöre düşürülür.

qSheff Projesi
- Yerel kullanıcılar

Öntanımlı olarak yerel (local) kullanıcılar taranmaz, qsheff.log'da görünmez.

Ancak büyük ISS'lerde yerel mail alışverişi çok olacağından yerel kullanıcıların da taranması gerekebilir. Qsheff bunu seçimlik özellik olarak sunmaktadır.

qSheff Projesi

- Göndericiye Özel Hata Mesajları

qmail "permanently" hata mesajları yerine göndericiye kendi istediğiniz mesajların dönülmesini sağlar.

Bu mesajlar main.h içerisinde yer alır, istenilirse değiştirilebilir. qSheff, tanımlı mesajın sonuna spam ise spam kelimesini, virus ise virus adını otomatik olarak ekler.

qSheff Projesi
- Virus Filtremele

- ClamAV ile birlikte çalışabilmektedir. Diğer tarayıcılardan farklı olarak clamav sokete doğrudan bağlanarak en az sistem kaynağını kullanır.
- custom-prog özelliği sayesinde dönüş değerleri bilinen bir çok virus tarayısı ile birlikte çalışabilmektedir. Kendi istediğiniz özel betik veya programları da qsheff ile tetikleyebilirsiniz.

qSheff Projesi

- Tüm Mail Trafiğinin Yedeklenmesi

Gelen ve giden tüm mail trafiğinin /var/qsheff/backup klasörünün altına kaydedilmesini sağlar.

Tüm trafik yerine sadece reddedilen spam veya virüslerin saklanması da sağlanabilir. (Karantina)

qSheff Projesi
- qSheff Yamaları

- qsheff-patch Yaması

Bu yamanın içerisinde hem custom-error hem de qmailqueue yaması mevcuttur. qsheff_patch'i herhangi bir çevre değişkeni okumadığından ve doğrudan qsheff'i çalıştırdığından hem daha güvenli hem de daha hızlıdır.

Bu yamaları kullanmak için qmail'in kaynak kodlarının olduğu dizine gidilir ve yama uygulanır.

```
# cd /usr/local/src/qmail-1.03/
# cp /usr/local/src/qsheff-2.0/contribute/qsheff_patch.diff .
# patch < qsheff_patch.diff
patching file qmail.c
patching file qmail.h
# make setup check
```

qSheff Projesi
- qSheff Yamaları

- **qmailqueue Yaması**

Eğer Bruce Guenter'in qmailqueue yamasını kullanıyorsanız (netqmail'de bu yama uygulanmıştır.) tcp.smtp aracılığıyla QMAILQUEUE çevre değişkeninin tcp.smtp dosyasında atanması gerekmektedir.

192.168.1.:allow,QMAILQUEUE="/var/qmail/bin/qmail-qsheff"

Yukarıdaki satır 192.168.1 networkunden gelen kullanıcılar için qmail-queue yerine qmail-qsheff'in çalıştırılmasını sağlar. Tüm networkler için aşağıdaki satırı eklemelisiniz:

:allow,QMAILQUEUE="/var/qmail/bin/qmail-qsheff"

NOT: Bu yama custom-error içermez.

qSheff Projesi
- qSheff Yamaları

- **custom-error Yaması**

Kullanıcı tanımlı hata mesajı dönmeyi sağlar. qsheff_patch yaması bu yamayı zaten içermektedir. qmail-queue veya qsheff_patch yamalarını kullanmadan sadece bu yamayı kullanmak istiyorsanız qmail kaynak kodunu contribute dizinindeki qmail-queue-custom-error.patch ile yamalamanız gerekmektedir.

Yamaların çalıştığını görmek için qsheff.log dosyasını kontrol edebilirsiniz.

qSheff Projesi
- Gelişmiş Kayıt Tutma

23/03/2006 04:58:42: [qSheff] QUEUE 4875 in 4951 out, queue=q-1143082721-559223-80793, recvfrom=216.136.204.119, from=`pb@ludd.ltu.se', to=`hselasky@c2i.net (Hans Petter Selasky)', subj=`Re: usb2 iscochronous transfer', size=4875

24/03/2006 05:06:09: [qSheff] SPAM 17189 in 17276 out, queue=q-1143169567-834623-7207, recvfrom=64.90.164.206, from=`[%from_email%]', to=`[%to%]', subj=`Need S0ftware?', size=17189, spam=`Subject: Need S0ftware?', rule=`(Subject: Need S0ftware)‘

24/03/2006 23:51:04: [qSheff] SPAM 8486 in 8573 out, queue=q-1143237060-423177-25605, recvfrom=218.18.125.109, from=`wuhan@seng.com', to=`ismail@enderunix.org', subj=`¡¶µç ´Å¼æÈİEMCÕû¸ÄÓë¶Ô²ß¡·', size=8486, spam=`Content-Type: text/plain; charse', rule=`(charset="[gG][bB]2312")'

24/03/2006 21:40:33: [qSheff] ATTACH 66723 in 0 out, queue=q-1143229228-612508-22296, recvfrom=85.107.54.223, from=`mts@lebanon-online.com.lb', to=`ismail@yenigul.net', subj=`Status', size=66723, spam=`document.pif', rule=`.pif‘

25/03/2006 00:02:09: [qSheff] CLAMD 1867 in 0 out, queue=q-1143237728-731561-26201, recvfrom=68.222.196.116, from=`online@services.com', to=`', subj=`New email address added to your ', size=1867, error=`connect_clamd', hint=`No such file or directory'

- qSheff Kurulumu

- # cd /usr/local/src/qsheff-2.0-r1/
  # ./configure --with-clamav=/opt/clamav/ --with-clamd-socket=/tmp/clamd --enable-qmailqueue-patch --enable-custom-error
  # make
  # make install
  # /usr/local/etc/qsheff/install-wrapper.sh

- Daha ayrıntılı kurulum için;

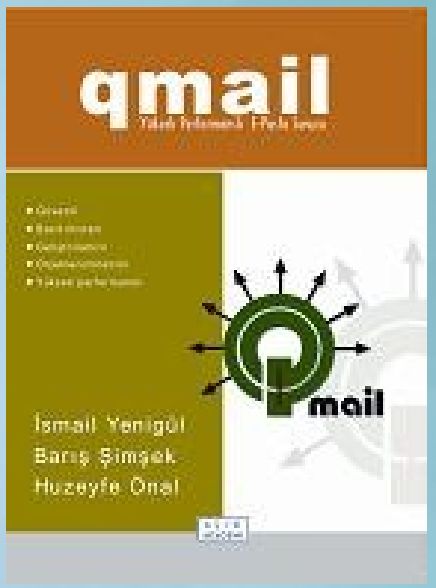
http://www.enderunix.org/qsheff/docs/qSheff-Klavuzu.html

qmail E-posta Sunucusu ve qSheff ile Virus/Spam Filtreleme

Bağlantılar:

http://cr.yp.to/
http://www.enderunix.org/qsheff
http://www.enderunix.org/qsheff/docs/qSheff-Klavuzu.html
http://www.qmail.org

qmail E-posta Sunucusu ve qSheff ile Virus/Spam Filtreleme



qmail: Yüksek Performanslı E-Posta Sunucu

Yazarlar: İsmail Yenigül, Barış Şimşek, Huzeyfe Önal

http://www.acikakademi.com/catalog/qmail/

qmail E-posta Sunucusu ve qSheff ile Virus/Spam Filtreleme

Teşekkürler

Afşin TAŞKIRAN

afsin@enderunix.org
www.EnderUNIX.org/afsin