Global Information Assurance Certification Paper

GSEC Practical Assignment v1.4

Building a secured open source mail system for Small Medium Enterprise (SME)

submitted
by

Tan Ming Han

28 August 2003

Table of Contents

Abstract

Nowadays, most Small and Medium Enterprise (SME) need to host their own mail servers for their global business needs. Nevertheless, the growth of viruses/worms is enormous and the security solution for them is getting more complex and costly.

This document aims to provide the possibility of using secured open source mail system solution for SME. It begins with the selection of the current open source mail system. A typical scenario would be used for the risk assessment before setting up the mail system. The mail system would be equipped with all necessary packages for anti-spamming, anti-virus, content filtering & etc. Thereafter, various testing methods would be used to verify the mail server are well protected and secure.

Lastly, the reader would be able to know how to implement a secure open source mail server in a typical SME environment.

1.0 Introduction

Email is the term given to an electronic message, usually a form of simple text message, which the sender wants to send to the recipients across a network. It accelerates the exchange of information, lowers communications costs and improves reliability. With its rapidly increasing popularity, companies are becoming dependent on it for their daily business operations.

However, most companies are small in scale and have limited resources for acquiring the mail server. Apart from the highly cost software licensing and the server hardware, companies also faced additional cost of acquiring commercial security product for protecting their mail server.

Nevertheless, it is possible for SME to implement a secured mail system using open source solution without incurring high setup cost.

2.0 Open Source Mail System

There is a number of popular open source Mail Transfer Agent (MTA) available in the market namely are: SendMail, Qmail and Postfix.

However, Qmail is selected for the following reasons:

Secure

Qmail is designed and developed with security in mind, the author, D.J Bernstein, has proclaimed that the software is very secure and is willing to offer US$ 500.00 as a reward for anyone who can find the security hole in it. The reward has not been claimed at the point of writing of this report as shown below. (Please refer to http://cr.yp.to/qmail/guarantee.html for reference)

Furthermore, searches for Qmail vulnerabilities and incidents in CERT does not return any related results. (Please refer to http://search.cert.org/query.html?col=certadv+incnotes+vulnotes&ht=0&qp=&qs=&qc=&pw=100%25&la=en&charset=iso-8859-1&si=1&ws=1&qm=0&ql=&qt=mail&oldqt=qmail for reference)

Reliable

It uses a unique user mailbox format (Maildir) that will not be corrupted even if the mail system crashes upon delivery. Thus, once an email message is accepted by the system, it will never be lost.

Efficient:

It does not require high processing power for the system.

"On a Pentium under BSD/OS, Qmail can easily sustain 200000 local messages per day---that's separate messages injected and delivered to mailboxes in a real test! Although remote deliveries are inherently limited by the slowness of DNS and SMTP, Qmail overlaps 20 simultaneous deliveries by default, so it zooms quickly through mailing lists. (This is why I finished Qmail: I had to get a big mailing list set up.)" (Quoted from D.J. Bernstein http://cr.yp.to/qmail.html)

Simple

It is smaller than any other Internet MTA and has a simple forwarding mechanism that allows the users handle their own mailing lists.

3.0 System Design

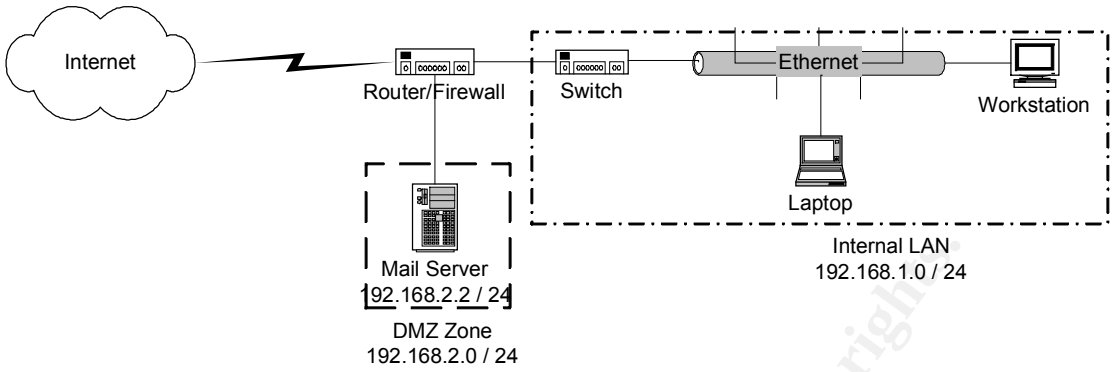

Figure 3.1

3.1 Typical Scenario

A typical scenario for mail server is shown in Figure 3.1. The above network layout shows that the mail server is situated at the Demilitarized Zone (DMZ). The gateway has a firewall separating the DMZ and the local subnet (internal LAN).

All incoming requests (internal/external) to port 25 (SMTP) will be forwarded to the mail server at the DMZ by the gateway. The retrieval of company mails (via POP3) and remote management of the mail server via port 22 (SSH) are only allowed from local subnet (internal LAN).

3.2 Risk Assessment

Before proceeding to the system implementation, risk assessment should be done as followed:

Possible Threats

1. SMTP Open Relay

   From the above, it is shown that SMTP is the only services exposed to the Internet. As such, any incorrect configuration of mail server may cause to be a SMTP open relay. It will cause the mail server to be used as a "launch pad" for mail spamming, thus being blacklisted by the DSNBL sites.

Resolution

The mail server should be installed with all essential packages to ensure the mail server perform authentication for any incoming SMTP relay for legitimate users. Log file monitoring could be used to detect any abuse activity of SMTP relay.

2. Virus/Worm Attack

Due the enormous number of virus/worm attacks come via email attachments. Many new virus/worm had successfully escaped from various email virus scanners and executed by unaware email users.

Resolution

The mail server should be equipped with content filtering function to quarantine suspicious emails at server level. The filtering rules should work according to the company's acceptable email policy that defines legitimate file attachments. This way, new virus/worm attachments that are not legitimate (e.g. src files, pif files) will be quarantined at the mail server.

The content filtering could also be used in conjunction with antivirus software to identify known viruses/worms.

3. Mail Spamming

Nowadays, the abuse of email marketing has caused million of unsolicited mails transverse across the Internet.

Resolution

The mail server should be installed with anti-spamming packages to perform DNSBL checking on all incoming SMTP connections for known spammers or blacklisted SMTP servers.

Rate Limit Spam Guard could be used to block any incoming mails from the same source once its mails have exceeded a predefined threshold within a time period.

Content filtering could also be used to block any emails containing some popular marketing jargons or sensitive strings used in the message subject.

4. POP3 Authentication

Since POP3 authentication is based on clear text password, any mail retrievals across the network may reveal the POP3 password by malicious user.

Resolution

POP3 service should only be accessed by local subnet, and the local subnet should be a switched network to prevent packet sniffing.

A well-defined password policy could also be enforced across the company and regular network monitoring could be used to identify any suspicious sniffing client.

Ultimately, the virtual POP account should be used, as each POP account does not have a valid system account in the mail server. This way, malicious user cannot get enough information to gain control of the mail server.

5. Remote Management with SSH.

Remote management of the mail server via SSH using the default setting is not good enough, as it can be subjected to brute force attack or password guessing.

Resolution

The SSH server (mail server) should be configured using public/private key pairs for the login. This way, any malicious user could not perform password guessing without using the correct key for the user authentication.

6. Denial of Service (DOS) attack

This attack is most difficult to counter especially if the attacker has more bandwidth capacity than the mail server. The mail server could be denied to serve incoming requests if the traffic is too great for it to handle.

Resolution

Bandwidth throttling at the gateway router could help to mitigate the risk of bringing down the entire network. Only necessary services should be allowed listening at the mail server, so as to minimize the exploits and weakness of other unused services being exposed. Regular check for DOS vulnerability of the mail server from alert service (Bugtraq, www.securityfocus.com) could help us on keeping up to date on any available patches for the mail server.

4.0 System Implementation

Since the risks has been identified, there is a series of steps to be carried out as followed:

1. Operating System (OS) Setup
2. OS Hardening
3. Qmail Patching and Setup
4. Virus Scan Setup
5. Qmail Scanner Setup
6. Spam Guard Setup
7. OpenSSH Setup

4.1 Operating System Setup

The minimum hardware requirement for the mail server is as followed:

Processor : Intel PII 400 MHz
RAM : 192 MB
Harddisk : 4.3 GB

The first step of the system implementation is to setup the OS by installing only those required packages to prevent any exploits and weakness that may be introduced by packages that are not required by the mail server.

Based on the minimum required hard disk space, the recommended partitions is as followed:

/	1 GB
/boot	101 MB
/var	715 MB
/home	2 GB
<swap>	384 MB (double of the RAM size)

4.1.1 Red Hat 8.0 Linux Packages Installation

The setup mode should be in graphical mode for ease of installation, and a custom minimal setup should be chosen with select individual packages checked. (Assume GRUB as default boot loader with password set)

Packages added:

Binutils
cpp
gcc
gcc++

gdb gdbmdevel glibc-devel glibc-kernheaders libstdc++ devel patch perl_DB_File perl_suidperl perl_Time_HiRes rpm-build zlib-devel packages

Packages removed:

finger ftp gnome-libs gtk+ imlib libungif net_snmp net_snmp_utils rsh rsyn sendmail talk XFree86-libs XFree86_Mesa_LibGL ypbind yp-tools

Install all necessary packages, and continue with default settings for the installation.

4.2 OS Hardening

After installing the OS, it is essential for us to perform OS hardening to reduce any possible exploits and weakness before setting up the mail server. (Please refer to bibliography [1] for more information)

4.2.1 Disable CTRL-ALT-Delete

In the case for the mail server with poor physical security, it is advisable to disable the CTRL-ALT-Delete function to prevent malicious user from restarting the mail server.

Use vi editor to edit /etc/inittab as followed:

#ca::ctrlaltdel:/sbin/shutdown –t3 –r now

Restart the service to take effect.

```
# /sbin/init q
```

4.2.2 Kernel Settings

The kernel settings can be modified to improve the overall network security by modifying sysctl.conf file.

Use vi editor to append /etc/sysctl.conf as followed:

```
net.ipv4.ip_forward =  0                          #disable IP forwarding
net.ipv4.conf.all.accept_source_route = 0         #disable IP source routing
net.ipv4.tcp_max_syn_backlog = 4096               #enable SYN flood protection
net.ipv4.conf_all.rp_filter = 1                   #enable IP Spoofing Protection
net.ipv4.tcp_syncookies = 1                       #enable SYN flood protection
net.ipv4.conf.all.send_redirects = 0              #disable outgoing ICMP redirects
net.ipv4.conf.all.accept_redirects = 0            #disable incoming ICMP redirects
net.ipv4.conf.default.accept_redirects=0          #disable incoming ICMP redirects
```

From the above setting, the IP forwarding is disabled since the mail server does not need to transverse any IP packets. Any ICMP redirect request is disabled to ignore any rerouting requests. IP spoofing protection and SYN flooding protection are enabled to prevent any malformed/malicious packets coming into the server. (Please refer to bibliography [2] for more information)

change the ownership of the file and restart the service

```
# chown root:root /etc/sysctl.conf        #change file ownership to root
# chmod 0600 /etc/sysctl.conf             #allow read/write to root only
# /etc/rc.d/init.d/network restart        #restart the network service
```

4.2.3 Removal of unnecessary services

By default, there are a number of services (started upon system boot up) running in the background listening for any incoming service request. Some of these services are not required for the mail server to work.

Hence, it would be advisable to disable any unnecessary services so as to reduce any possible exploits that these services may introduce. (Please refer to bibliography [3] for more information)

To list all services configured to run upon system boot up.

```
# /sbin/chkconfig --list | grep -e "\(:.*on\|xinetd based\)"
```

Result in tabular format:

Service Name	Run Levels						
syslog	0:off	1:off	2:on	3:on	4:on	5:on	6:off
netfs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
network	0:off	1:off	2:on	3:on	4:on	5:on	6:off
random	0:off	1:off	2:on	3:on	4:on	5:on	6:off
rawdevices	0:off	1:off	2:off	3:on	4:on	5:on	6:off
apmd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
gpm	0:off	1:off	2:on	3:on	4:on	5:on	6:off
autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
keytable	0:off	1:off	2:on	3:on	4:on	5:on	6:off
kudzu	0:off	1:off	2:off	3:on	4:on	5:on	6:off
sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off
rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
pcmcia	0:off	1:off	2:on	3:on	4:on	5:on	6:off
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off
portmap	0:off	1:off	2:on	3:on	4:on	5:on	6:off
netfslock	0:off	1:off	2:on	3:on	4:on	5:on	6:off

Disable services at all run-levels using the following steps:

```
# /etc/init.d/<service name> stop
# /sbin/chkconfig --level 0123456 <servicename> off
```

Repeat the above steps to disable all services except for the followings:

keytable
syslog
network
random
crond
anacron
iptables
sshd

4.2.4 Host based Firewall

Conditions:

1. All public services (SMTP) must be protected by using the built-in stateful firewall.

2. SSH and POP3 services can only be accessed by the local subnet (internal).

3. All Reserved IP (except local subnet) must be blocked from entering the server. However, the gateway router must also enable ingress filtering. (Please refer to bibliography [4] for more information)

4. Only established/related packets are allowed to enter the server. (Please refer to bibliography [5] for more information)

IPTables Configuration

Firewall Rules for Mail Server (Default Drop Policy)

Description	Protocol	Source Addr	Source Port	Dest Addr	Dest Port	Chain	Action	State
Reserved IP	Any	0.0.0.0 /8	Any	Any	Any	INPUT	DROP	ALL
	Any	10.1.1.0 /8	Any	Any	Any	INPUT	DROP	ALL
	Any	127.0.0.0 /8	Any	Any	Any	INPUT	DROP	ALL
	Any	172.16.0.0 /12	Any	Any	Any	INPUT	DROP	ALL
	Any	224.0.0.0 /4	Any	Any	Any	INPUT	DROP	ALL
	Any	240.0.0.0 /5	Any	Any	Any	INPUT	DROP	ALL
Invalid TCP Flags	TCP	Any	Any	Any	Any	INPUT	DROP	NO TCP Flags
	TCP	Any	Any	Any	Any	INPUT	DROP	SYN, FIN
	TCP	Any	Any	Any	Any	INPUT	DROP	SYN, RST
	TCP	Any	Any	Any	Any	INPUT	DROP	FIN, RST
	TCP	Any	Any	Any	Any	INPUT	DROP	FIN
	TCP	Any	Any	Any	Any	INPUT	DROP	PSH
	TCP	Any	Any	Any	Any	INPUT	DROP	URG
Outgoing Request	Any	Mail Server IP	Any	Any	Any	OUTPUT	ACCEPT	NEW, ESTABLISHED, RELATED
Incoming Response	Any	Any	Any	Mail Server IP	Any	INPUT	ACCEPT	ESTABLSIHED, RELATED
Incoming mail	TCP	Any	PRIVPT	Mail Server IP	25	INPUT	ACCEPT	NEW
Incoming POP request	TCP	LOCAL	PRIVPT	Mail Server IP	110	INPUT	ACCEPT	NEW
Incoming SSH request	TCP	LOCAL	PRIVPT	Mail Server IP	22	INPUT	ACCEPT	NEW

LOCAL – 192.168.1.0 /24
PRIVPT - 1024:65535 (port #)
Assuming the gateway is performing ingress filtering.

Use vi editor to create firewall startup script (/etc/rc.bastion) as shown below.

```
#
# Variables Assignment
#
INET_IP=`ifconfig eth1 | grep "inet addr:" | \
awk -F: {'print $2'} | cut -d\  -f 1`
INET_IFACE="eth0"

LO_IFACE="lo"
LO_IP="127.0.0.1"

LAN_IP="192.168.1.0/24"
LAN_BCAST="192.168.1.255"

CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_D="224.0.0.0/4"
CLASS_E="240.0.0.0/5"
LOOPBACK="127.0.0.0/8"
RESERVED="0.0.0.0/8"

BCAST_SRC="0.0.0.0"
BCAST_DEST="255.255.255.255"

PUBLICPORTS="0:1023"
PRIVATEPORTS="1024:65535"
ALLPORTS="0:65535"

#
# IPTables Configuration.
#
IPTABLES="/sbin/iptables"

#
# Module loading.
# Needed to initially load modules
#

/sbin/depmod -a

#
# Required modules
#

/sbin/modprobe ip_tables
```

```
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_limit
/sbin/modprobe ipt_state

#
# /proc set up.
# Required proc configuration
#
echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
echo "1" > /proc/sys/net/ipv4/conf/all/proxy_arp
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo "1" > /proc/sys/net/ipv4/tcp_syncookies
echo "1" > /proc/sys/net/ipv4/tcp_timestamps
echo "0" > /proc/sys/net/ipv4/conf/default/accept_redirects

#
# Remove all existing rules from all chains
#

$IPTABLES --flush
$IPTABLES -t nat --flush
$IPTABLES -t mangle --flush

$IPTABLES --delete-chain
$IPTABLES -t nat --delete-chain
$IPTABLES -t mangle --delete-chain

#
# Set default policies to DROP
#
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

#
# Source IP Spoofing
#
$IPTABLES -A INPUT -i $INET_IFACE -s $CLASS_A -j DROP
$IPTABLES -A INPUT -i $INET_IFACE -s $CLASS_B -j DROP
$IPTABLES -A INPUT -i $INET_IFACE -s $CLASS_D -j DROP
```

```
$IPTABLES -A INPUT -i $INET_IFACE -s $CLASS_E -j DROP
$IPTABLES -A INPUT -i $INET_IFACE -s $RESERVED -j DROP

#
# Stealth Scans and TCP State Flag
#

#All tcp flags are clear
$IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

#SYN & FIN SET
$IPTABLES -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP

#SYN & RST SET
$IPTABLES -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

#FIN & RST SET
$IPTABLES -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j DROP

#FIN SET
$IPTABLES -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j DROP

#PSH SET
$IPTABLES -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j DROP

#URG SET
$IPTABLES -A INPUT -p tcp --tcp-flags ACK,URG URG -j DROP

#
# Public Services
#

#Allow SSH Traffic
$IPTABLES -A INPUT -i $INET_IFACE \
-p tcp –s $LAN_IP --sport $PRIVATEPORTS --dport 22 \
-m state --state NEW -j ACCEPT

#Allow incoming SMTP
$IPTABLES -A INPUT -i $INET_IFACE \
-p tcp --dport 25 -m state --state NEW -j ACCEPT

#Allow incoming POP3
$IPTABLES -A INPUT -i $INET_IFACE \
-p tcp –s $LAN_IP –-sport $PRIVATEPORTS --dport 110 -m state \
--state NEW -j ACCEPT
```

```
#
# Connection State
#
$IPTABLES -A OUTPUT -o $INET_IFACE \
-m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

$IPTABLES -A INPUT -i $INET_IFACE \
-m state --state ESTABLISHED,RELATED -j ACCEPT

#
# Unlimted traffic on Loopback Interface
#
$IPTABLES -A INPUT -i $LO_IFACE -j ACCEPT
$IPTABLES -A OUTPUT -o $LO_IFACE -j ACCEPT
```

Make it executable.

```
# chmod 700 /etc/rc.bastion
```

Execute the firewall script.

```
# /etc/rc.bastion
```

Configure the firewall script to run upon startup (at run level 3).

```
# ln –s /etc/rc.bastion /etc/rc.d/rc3.d/S81Firewall
```

4.3 Qmail Patching and Setup

4.3.1 Setup Preparation

```
# su
# umask 022
# mkdir –p /usr/local/src
# cd /usr/local/src
```

4.3.2 Installing ucspi-tcp

This package is developed by D.J. Bernstein, which consists of various useful programs, which 2 of them are known as tcpserver and rblsmtpd. (Please refer to bibliography [6] for more information)

tcpserver is a daemon program that waits for any incoming connections on a configured port for any specified program. The local and remote host names, IP addresses and port number for each connection can be accessed, via environment variables, by the specified program.

It protects the server from running out of processes and memory using a concurrency threshold limit. If the incoming simultaneous connections exceed the predefined threshold (e.g. 40), it can smoothly deter acceptance of new connections.

It also provides faster TCP access control features as compared to tcp-wrapper due to its access control rules are compiled into hashed cdb format. This cdb fie is used to specify allowed hosts that can connect to the daemon. By default, all hosts not in the cdb file will be denied access.

rblsmtpd is daemon program that check if the source of incoming smtp connections are being black listed by the DNS-based Blackhole List site (e.g. relays.ordb.org).

These DNSBL sites are usually non-profitable anti-spam organizations that blacklist any open relays SMTP servers that are being used or potentially to be used for spamming.

If any incoming SMTP connections come from those blacklisted SMTP servers, rblsmtpd will reject the connection and thus reject the mail.

Download and setup the ucspi-tcp package.

```
# wget --passive ftp://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
# tar -zxvf ucspi-tcp-0.88.tar.gz
# rm –f ucspi-tcp-0.88.tar.gz
# cd ucspi-tcp-0.88
# make && make setup check
```

4.3.3 Installing daemontools

This package, written by D.J. Bernstein, is a collection of small utility programs for controlling and monitoring all daemons running from a single directory, /service. (Please refer to bibliography [7] for more information)

Daemon can be set to run by having a run file in the /service/daemon-name/ directory. This run file will contains the daemon program to be called upon when the supervise starts at every startup.

Optionally, the logging function (multilog) for the daemon program can be set by specifying a run file in the /service/daemon-name/log/ directory.

Some programs in the package which are as followed:

supervise

It is started by the svscan program to start and monitor each daemon specified to run from the /service/daemon-name/run. It will restart any daemon process it monitored that die unexpectedly.

svscan

It starts the supervise program to monitor each daemon program.

svc

It provides a command-line tool to start, stop or signal the daemon program reliably.

multilog

It is a logging program that will listen to each daemon and log messages from it to a specified path. It supports log file size limitation and log file rotating mechanism for each daemon.

With the specified log file size limitation and log file rotation; any incoming log messages will not be discarded even if the log file is full. This is more efficient and reliable as compared to syslog daemon.

svstat

It display the status of the daemon monitored by supervise.

softimit

It is used to specify the resource limits for each daemon program.

Download and setup the package

```
# mkdir –p /package
# chmod 1755 /package
# cd /package
# wget --passive ftp://cr.yp.to/daemontools/daemontools-0.76.tar.gz
# tar -zxvf daemontools-0.76.tar.gz
# rm –f daemontools-0.76.tar.gz
# cd admin/daemontools-0.76
# package/install
```

4.3.4 Installing djbdns

This package is also written by D.J. Bernstein, it is designed to provide a secure (please refer to http://cr.yp.to/djbdns/guarantee.html), stable and faster DNS name resolution functions as compared to BIND. (Please refer to bibliography [8] for more information)

Download and setup djbdns package

```
# cd /usr/local/src
# wget http://cr.yp.to/djbdns/djbdns-1.05.tar.gz
# tar -zxvf djbdns-1.05.tar
# cd djbdns-1.05
# make && make setup check
# groupadd –r –g 405 djbdns
# useradd –d /etc/dnscache –g 405 –u 410 –M –r –s /bin/true dnscache
# useradd –d /etc/dnscache –g 405 –u 411 –M –r –s /bin/true dnslog
```

Configure dnscache to act as local caching name server

```
# dnscache-conf dnscache dnslog /etc/dnscache 127.0.0.1
# ln –s /etc/dnscache /service
# mv /etc/resolv.conf /etc/resolv.conf.old
# echo “nameserver 127.0.0.1” > /etc/resolv.conf
# /usr/local/src
# rm –f djbdns-1.05.tar.gz
```

4.3.5 Patching Qmail

Before we proceed to patch qmail, the package has to be installed first.

Download and unpack the Qmail package

```
# wget --passive ftp://cr.yp.to/software/qmail-1.03.tar.gz
# tar -zxvf qmail-1.03.tar.gz
# rm –f qmail-1.03.tar.gz
```

Qmail queue patching

This patch is needed to that allow any program to do content filtering, rewrite broken headers & etc.

Download and patch Qmail.

```
# wget http://www.qmail.org/qmailqueue-patch
```

Use vi editor to remove all top lines until the first line begin as followed:

diff -u qmail-1.03-orig/Makefile qmail-1.03/Makefile

Apply the patch.

```
# cd /usr/local/src/qmail-1.03
# patch < ../qmailqueue-patch
```

0.0.0.0 patching

This patch is to enable Qmail to recognize 0.0.0.0 as a local IP address, which is part of RFC 822

Download and apply the patch.

```
# cd /usr/local/src
# wget http://www.suspectclass.com/~sgifford/qmail/qmail-0.0.0.0.patch
# cd /usr/local/src/qmail-1.03
# patch < ../qmail-0.0.0.0.patch
```

SMTP authentication patching

This patch enables Qmail to support an ESMTP service extension (RFC 2554) whereby the SMTP client may indicate an authentication mechanism to SMTP server, perform an authentication protocol exchange, and negotiate a security layer for subsequent protocol interactions (optional).

Hence, it can be served as an extra security layer to the SMTP server by allowing only legitimate SMTP clients to send e-mail from anywhere.

Ultimately, it helps to prevent the SMTP server from being an open relay and stop any unauthorized people or spammers from using it for relaying. This is to prevent it from being blacklisted by the DSNBL sites and other anti spam organization.

Download and apply the patch.

```
# cd /usr/local/src
#  wget http://members.elysium.pl/brush/qmail-smtpd-auth/dist/qmail-smtpd-auth-0.31.tar.gz
# tar –zxvf qmail-smtpd-auth-0.31.tar.gz
# cd qmail-smtpd-auth-0.31
# cp base64.c base64.h ../qmail-1.03
# patch -d ../qmail-1.03 < auth.patch
# rm –f qmail-smtpd-auth-0.31.tar.gz
```

Anti-Spam patching

This patch helps to prevent any emails that has '@','%' or '!' symbols in the local part of the email address.

With this patch applied, the SMTP server is able to reduce unnecessary mail relaying and bouncing.

Download and apply the patch.

```
# cd /usr/local/src
# wget http://qmail.glasswings.com.au/qmail-smtpd-relay-reject
# patch -d qmail-1.03 < qmail-smtpd-relay-reject
```

4.3.6 Setting up Qmail and VPOPMail

Setting up Qmail and VPOPMail can be quite confusing, however, there are some good references available in the market. (Please refer to bibliography [9], [10], [11] for more information)

Setup Qmail package.

```
# cd /usr/local/src/qmail-1.03
# mkdir /var/qmail
```

Adding user and user group is essential in Qmail Setup as the qmail services should not have root privillieages.

```
# groupadd –g 2108 nofiles
# useradd –u 7790 –g nofiles –d /var/qmail/alias alias –s /bin/true
# useradd –u 7791 –g nofiles –d /var/qmail qmaild –s /bin/true
# useradd –u 7792 –g nofiles –d /var/qmail qmaill –s /bin/true
# useradd –u 7793 –g nofiles –d /var/qmail qmailp –s /bin/true
# groupadd –g 2107 qmail
# useradd –u 7794 –g qmail –d /var/qmail qmailq –s /bin/true
# useradd –u 7795 –g qmail –d /var/qmail qmailr  –s /bin/true
# useradd –u 7796 –g qmail –d /var/qmail qmails –s /bin/true
# make setup check
# ./config-fast mailbox.domain.com
```

Setup VPOPMail package

Create necessary group and user essential for the vpopmail.

```
# groupadd –g 89 vchkpw
# useradd –g vchkpw –u 89 vpopmail
```

```
# mkdir ~vpopmail/etc
```

Allow smtp relay for localhost

```
# echo 127.0.0.:allow,RELAYCLIENT=\"\" > /etc/tcp.smtp
```

Allow smtp relay (virtual domain) for localhost

```
# echo 127.0.0.:allow,RELAYCLIENT=\"\" > /home/vpopmail/etc/tcp.smtp
```

Allow POP3 access from local subnet and local host

```
# echo 192.168.2.:allow > /etc/tcp.pop3
# echo 127.:allow >> /etc/tcp.pop3
# deny >> /etc/tcp.pop3
```

Setup Vpopmail

```
# cd /usr/local/src
# wget http://www.inter7.com/vpopmail/vpopmail-5.2.1.tar.gz
# tar –zxvf vpopmail-5.2.1.tar.gz
# cd vpopmail-5.2.1
# /configure --enable-roaming-users=y --enable-defaultquota=10M --enable-
default-domain=domain.com
# make && make install-strip
```

Configure to clear any open smtp connections every 40 mins.

```
# crontab –e
```

Add the following entry.

```
40 * * * * /home/vpopmail/bin/clearopensmtp 2>&1 /dev/null
```

Set all required controls files.

```
# echo ./Maildir/ >/var/qmail/control/defaultdelivery
# echo 20 > /var/qmail/control/concurrencyincoming
# chmod 644 /var/qmail/control/concurrencyincoming
# echo 20 > /var/qmail/control/concurrencypop3
# chmod 644 /var/qmail/control/concurrencypop3
# echo “Unauthorised access are strictly prohibited by law. Any access to the
system are logged.” > /var/qmail/control/smtpgreeting
```

Create log directories for all daemons.

```
# mkdir –p /var/qmail/supervise/qmail-send/log
# mkdir –p /var/qmail/supervise/qmail-smtpd/log
# mkdir –p /var/qmail/supervise/qmail-pop3d/log
```

Use vi editor to create /var/qmail/rc startup script

```
#!/bin/sh
exec env –PATH=”/var/qmail/bin:$PATH” \
qmail-start “`cat /var/qmail/control/defaultdelivery`”
```

Make the script executable.

```
# chmod 755 /var/qmail/rc
```

Use vi editor to create /var/qmail/supervise/qmail-send/run script

```
#!/bin/sh
exec /var/qmail/rc
```

Use vi editor to create /var/qmail/supervise/qmail-send/log/run script

```
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill /usr/local/bin/multilog t /var/log/qmail
```

Use vi editor to create /var/qmail/supervise/qmail-smtpd/run script

```
#!/bin/sh
QMAILDUID=`id –u qmaild`
NOFILESGID=`id –g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 8000000 \
/usr/local/bin/tcpserver -v –R -H –l0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" -u \
"$QMAILDUID" -g "$NOFILESGID" 0 25 \
/usr/local/bin/rblsmtpd -r relays.ordb.org \
/var/qmail/bin/qmail-smtpd mailbox.domain.com \
 /home/vpopmail/bin/vchkpw /bin/true 2>&1
```

From the above, the ***/usr/local/bin/softlimit –m 8000000*** is used to allocate 8 MB memory for the mail server to process and scan each email message. ***/usr/local/bin/tcpserver –v –R –H –l0*** is used to tell tcpserver to log any errors, and to skip IDENT information lookup and DNS lookup on remote/local host. This is to speed up the mail server performance.

/usr/local/bin/rblsmtpd –r relay.ordb.org is used for DNSBL checking on each incoming smtp connection to see if it is blacklisted by relay.rbdb.org.

/home/vpopmail/bin/vchkpw is used to perform password authentication for any incoming smtp relaying.

Use vi editor to create /var/qmail/supervise/qmail-smtpd/log/run file

```
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill /usr/local/bin/multilog t s1000000 \
 /var/log/qmail/smtpd
```

/usr/local/bin/multilog t s1000000 is used to state 1 MB log file size before multilog rotate to the next file (10 file per cycle).

Use vi editor to create /var/qmail/supervise/qmail-pop3d/run script

```
#!/bin/sh
MAXPOP3D=`head –1 /var/qmail/control/concurrecnypop3`
exec /usr/local/bin/softlimit –m 2000000 \
/usr/local/bin/tcpserver –v –R –H –l0 –x /etc/tcp.pop3.cdb –c "$MAXPOP3D" \
0 110 /var/qmail/bin/qmail-popup mailbox.domain.com \
home/vpopmail/bin/vchkpw /var/qmail/bin/qmail-pop3d Maildir 2>&1
```

Use vi editor to create /var/qmail/supervise/qmail-pop3d/log/run script

```
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill /usr/local/bin/multilog t \
/var/log/qmail/pop3d
```

Create qmailctl file

```
# cd /var/qmail/bin
# wget http://www.lifewithqmail.org/qmailctl-script-dt70
# mv qmailctl-script-dt70 qmailctl
# chmod 755 /var/qmail/bin/qmailctl
```

Use vi editor to amend qmailctl script file

Under the start section, add the following entries.

```
if svok /service/qmail-pop3d; then
    svc -u /service/qmail-pop3d
else
    echo "qmail-pop3d supervise not running"
fi
```

Under the stop section, add the following entries.

```
echo "  qmail-pop3d"
svc -d /service/qmail-pop3d
```

Under the stat section, add the following entries.

```
svstat /service/qmail-pop3d
svstat /service/qmail-pop3d/log
```

Under the pause section, add the following entries.

```
echo "Pausing qmail-pop3d"
svc -p /service/qmail-pop3d
```

Under the continue section, add the following entries.

```
echo "Continuing qmail-pop3d"
svc -c /service/qmail-pop3d
```

Under the restart section, add the following entries.

```
echo "* Restarting qmail-pop3d."
svc -u /service/qmail-pop3d
```

Under the cdb section, add the following entries.

```
tcprules /etc/tcp.pop3.cdb /etc/tcp.pop3.tmp < /etc/tcp.pop3
chmod 644 /etc/tcp.pop3.cdb
echo "Reloaded /etc/tcp.pop3."
```

(Please refer to Appendix A for a complete listing of qmailctl)

Link the script as a system command

```
# ln –s /var/qmail/bin/qmailctl /usr/bin
```

Make all run scripts executable.

```
# chmod 755 /var/qmail/supervise/qmail-send/run
# chmod 755 /var/qmail/supervise/qmail-send/log/run
# chmod 755 /var/qmail/supervise/qmail-smtpd/run
# chmod 755 /var/qmail/supervise/qmail-smtpd/log/run
# chmod 755 /var/qmail/supervise/qmail-pop3d/run
# chmod 755 /var/qmail/supervise/qmail-pop3d/log/run
```

Create log directories and change ownership to qmaill.

```
# mkdir /var/log/qmail
# mkdir –p /var/log/qmail/smtpd
# chmod +t /var/qmail/supervise/qmail-pop3d
# mkdir –p /var/log/qmail/pop3d
# chown qmaill /var/log/qmail /var/log/qmail/smtpd /var/log/qmail/pop3d
```

Create new virtual domain and email aliases for the new domain.

```
# cd /home/vpopmail/bin
# ./vadddomain domain.com <password for postmaster>
# /.vadduser admin@domain.com <user password>
# echo admin@domain.com > /var/qmail/alias/.qmail-root
# echo admin@domain.com > /var/qmail/alias/.qmail-postmaster
# echo admin@domain.com > /var/qmail/alias/.qmail-mailer-daemon
```

Configure qmail to run at all run levels.

```
# cd /etc/rc.d
# ln -s /var/qmail/bin/qmailctl /etc/rc.d/init.d/qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc0.d/K30qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc1.d/K30qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc2.d/S80qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc3.d/S80qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc4.d/S80qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc5.d/S80qmail
# ln -s /etc/rc.d/init.d/qmail /etc/rc.d/rc6.d/K30qmail
```

Link all daemons to run under /service

```
# ln –s /var/qmail/supervise/qmail-send /var/qmail/supervise/qmail-smtpd
/var/qmail/supervise/qmail-pop3d /service
```

Restart the mail server to update the access rules for all incoming connections.

```
# qmailctl stop
# qmailctl cdb
# qmailctl start
```

4.4 Antivirus Setup

Antivirus can be used in conjunction with the content filtering function so as to provide additional protection layer for the mail server.

Any incoming/outgoing mails will be scanned by the Anti-Virus application for any known virus.

Due to demonstration purpose, an open source antivirus, clamav 0.60 is used.

Create the necessary group and user for the antivirus package.

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

Setting up clamav-0.60 package

```
# cd /usr/local/src
# wget http://aleron.dl.sourceforge.net/sourceforge/clamav/clamav-0.60.tar.gz
# tar –zxvf clamav-0.60.tar.gz
# cd clamav-0.60
# ./configure --sysconfdir=/etc
# make && make install
```

Update the latest virus definition file

```
# freshclam
# touch /var/log/clam-update.log
# chmod 600 /var/log/clam-update.log
# chown clamav /var/log/clam-update.log
```

Run freshclam as daemon.

```
# freshclam -d -c 2 -l /var/log/clam-update.log
```

Configure the update of Anti-Virus application to run at 8 am everyday automatically.

```
# crontab –e
```

Add the following line.

```
0 8     * * *     /usr/local/bin/freshclam --quiet -l /var/log/clam-update.log
```

4.5 Content Filtering with Qmail-Scanner

This package is selected for its better performance due to its low level integration with the qmail server.

It provides qmail server the ability to scan all incoming, outgoing and traversing mails for certain characteristics such as specific strings in particular headers, or particular attachment filenames or file types (e.g. *.VBS attachments).

It quarantines any incoming/outgoing mails that have violated the specified filtering rules and send an email alert to the administrator.

The filtering rules are defined in the same format as shown below:

Rule<TAB>Filter Rule Type<TAB>Remark
The filtering rules has the following types:

Virus-Content-Type
e.g. *message/partial Virus-Content-Type Message/partial MIME attachments*

Virus-Date
e.g. *.{100,}Virus-Date MIME Header Buffer Overflow*
Virus-MAILFROM
e.g. **@sex.com Virus-MAILFROM Spam Mail*

Virus-Mime-Version
e.g. *{100,} Virus-Mime-Version MIME Header Buffer Overflow*

Virus-Resent-Date
e.g. *{100,} Virus-Resent-Date MIME Header Buffer Overflow*

Virus-Subject
e.g. ** sex.* Virus-SubjectSpam Mail*

Virus-TCPREMOTEIP
e.g. *205.158.62.24 Virus-TCPREMOTEIP Spam Mail*

Virus-To
e.g. **@playboy.com Virus-To Spam Mail*

File Size
e.g. *.exe 0 Executable File (.exe)*
e.g. *Happy99.exe 10000 Happy99 Trojan*

In addition, it can be used in conjunction with open virus scanner (Clamav) for server-level anti-virus protection.

Installing maildrop 1.5.2 package

```
# cd /usr/local/src
# wget http://download.sourceforge.net/courier/maildrop-1.5.2.tar.bz2
```

```
# rpmbuild –ta maildrop-1.5.2.tar.bz2
# cd /usr/src/redhat/BUILD/maildrop-1.5.2
# ./configure
# make
# make install-strip
# make install-man
```

Installing tnef-1.1.4 package

```
# cd /usr/local/src
# wget http://easynews.dl.sourceforge.net/sourceforge/tnef/tnef-1.1.4.tar.gz
# tar –zxvf tnef-1.1.4.tar.gz
# cd tnef-1.1.4
# ./configure
# make && make install
```

Installing qmail-scanner 1.16

```
# cd /usr/local/src
# wget http://easynews.dl.sourceforge.net/sourceforge/qmail-scanner/qmail-scanner-1.16.tgz
# tar –zxvf qmail-scanner-1.16.tgz
# cd qmail-scanner-1.16
# ./configure --spooldir /var/spool/qmailscan/ --bindir /var/qmail/bin/ --scanners clamscan --admin admin --notify admin --domain domain.com --local-domains "domain.com" --unzip no --install
```

Choose default setting for the rest of the steps (Please refer to bibliography [12] for troubleshooting)

Use vi editor to insert the following line at the first line in the /var/qmail/supervise/qmail-smtpd/run script file.

```
QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"; export QMAILQUEUE
```

Configuring filtering rules for qmail-scanner 1.16

The filtering rule is configured by editing /var/spool/qmailscan/quarantine-attachment.txt (Please refer to Appendix B for recommended filtering list).

Updating filtering rules for scanner

```
# /var/qmail/bin/qmail-scanner-quarantine.pl –g
```

Noted: All quarantined mails will be stored under /var/spool/qmailscan/quarantine/new.

4.6 Rate Limit with Spam Guard

This small program is designed to automatically monitor any possible malicious spammer activity that can be found in the mail server log files at /var/log/qmail/smtpd directory. (Please refer to bibliography [13] for more information)

It scans the log files within a predefined time intervals via crontab service, and if a sending address is found exceeding the predefined threshold, the program will alert the system administrator and mark that address as bad mailer, thus reject any mails sent by this sender in future.

There are 3 types of thresholds used by the function:

Warning Threshold (wcnt)

Email alert will be sent to the system administrator once this threshold is exceeded.

Blocking Threshold (bcnt)

Blocking the sender and email alert will be sent to the system administrator once this threshold is exceeded.

Paranoid Threshold (pcnt)

Blocking of all incoming mails and email alert will be sent to the system administrator once this threshold is exceeded.

As shown above, this rate limit function can be used to prevent any potential spam activity against the mail server.

Nevertheless, there is an ignore file (/usr/local/etc/spam-ignore.txt) known as white list used by the program to bypass any legitimate users (e.g. postmaster@domain.com) from the scanning.

Installing spamguard-1.6

```
# cd /usr/local/src
# wget http://www.enderunix.org/spamguard/spamguard-1.6.tar.gz
# tar -zxvf spamguard-1.6.tar.gz
# cd spamguard-1.6
# make && make install
```

Setting up spamguard-1.6

```
# cd /usr/local/etc
# cp spamguard.conf.sample spamguard.conf
# cp spam-ignore.txt.sample spam-ignore.txt
```

Configuring spamguard –1.6

Use vi editor to edit /usr/local/etc/spamguard.conf as followed

```
#spamguard 1.6 Configuration file
logtype = "qmail" #log type qmail, sendmail, postfix
logfile = "/var/log/qmail/current" #
ignorefile = "/usr/local/etc/spam-ignore.txt" #
badmailfile = "/var/qmail/control/badmailfrom" #
sysadmin = "admin@domain.com" #
hostname = "domain.com" #
mail_command = "/usr/bin/mail"
makemap_command = "makemap hash /etc/mail/access < /etc/mail/access"
#sendmail , postfix only
wcnt = 10 #Warning Count
bcnt = 20 #Blocking Count
pcnt = 100 #Paranoid Count
statfile = "/usr/local/etc/spamguard.stat";
```

Use vi editor to edit */usr/local/etc/spam-ignore.txt* as followed

```
*@sans.org
netfilter-request@lists.netfilter.org
notification@lists.sophos.com
postmaster@domain.com
```

Configure spamguard to run every 5 mins

```
# crontab -e
```

Add the following line:

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * /usr/local/bin/spamguard
```

4.7 Remote Access with SSH

Remote access of the mail server can only be done via SSH service using public/private DSAv2 1024 bits key pairs.

Therefore, all traffic sessions for the mail server remote access is encrypted and secure. This protects it from brute force attack across the network. All successful access can only be achieved with the correct private key and the login pass phrase.

The following setup is used to support remote access from window client using putty client to the mail server.

Use vi editor to edit /etc/ssh/sshd_config (Please refer to bibliography [14] for more information) as followed

sshd_config

Option	Recommedation
AuthorizedKeysFile	~/.ssh/authorized_keys
Ciphers	Blowfish-cbc
DSAAuthentication	Yes
HostKey	/etc/ssh/ssh_host_dsa_key
IgnoreRhosts	Yes
IgnoreUserKnownHosts	Yes
KeyRegenerationInterval	3600
LogLevel	INFO
LoginGraceTime	600
PasswordAuthentication	No
PermitEmptyPasswords	No
PermitRootLogin	No
Protocol	2
Port	22
RhostsAuthentication	No
RhostsRSAAuthentication	No
RSAAuthentication	Yes
ServerKeyBits	1024
StrictModes	Yes
SyslogFacility	AUTHPRIV
X11Forwarding	No

Download PuttyGen.exe in window platform.

http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe

Generating DSA Key (1024 bits) with PuttyGen.exe

In Window platform

1. Select the SSH2 DSA key to generate.
2. Click the generate button.
3. Move the mouse in any pattern over the blank area to generate some randomness.

4. Key in the passphrase and confirm it.
5. Save the private key to a removable media (e.g. floppy disk)
6. Copy the public key text string from the program and save it under a text file to a removable media (e.g. floppy disk).

In Linux platform

7. Copy the public key text file from the removable media (e.g. floppy disk) and save it as ~.ssh/authorized_keys under the authorized user home directory.
8. Type the following command to restart the ssh daemon.
   # service sshd restart

5.0 System Testing

5.1 Running Services and Open ports Testing

Execute the following command to check for the running services.

```
# netstat –a

Active Internet connections (servers and established)
Proto Recv-Q Send-Q  Local Address      Foreign Address    State
tcp        0      0  *:pop3             *:*                LISTEN
tcp        0      0  mailbox:domain     *:*                LISTEN
tcp        0      0  *:ssh              *:*                LISTEN
tcp        0      0  *:smtp             *:*                LISTEN
udp        0      0  mailbox:domain     *:*
```

From the above result, it is shown that the mail server is running only the required services as followed:

1. smtp
2. pop3
3. ssh
4. dnscache.

Nevertheless, we need to check which ports are opened to the public. The following test will reveal if the mail server firewall are allowing only smtp access from the public.

Run nmap on external machine (on the Internet) to perform port scan on the mail server.

```
# nmap –v –sS <mailbox.domain.com>

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (xxx.xxx.xxx.xxx) appears to be up ... good.
Initiating SYN Stealth Scan against  (xxx.xxx.xxx.xxx)
Adding open port 25/tcp

adjust_timeout: packet supposedly had rtt of 10857094 microseconds.  Ignoring time.
adjust_timeout: packet supposedly had rtt of 24415280 microseconds.  Ignoring time.
adjust_timeout: packet supposedly had rtt of 49905826 microseconds.  Ignoring time.
The SYN Stealth Scan took 188 seconds to scan 1601 ports.
Interesting ports on  (xxx.xxx.xxx.xxx):
```

```
(The 1598 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
```

Noted: The ip address and domain is hidden or changed to a fictitious value.

Nmap run completed -- 1 IP address (1 host up) scanned in 188 seconds

From the result shown above, the mail server only offers smtp and ssh services to the public network.

5.2 DNSBL (DNS-based Blackhole List) Testing

The following test is to see if the DNSBL is working in the mail server.

```
# telnet 127.0.0.2 25
Trying 127.0.0.2...
Connected to 127.0.0.2.
Escape character is '^]'.
220 rblsmtpd.local
mail from:<me>
250 rblsmtpd.local
rcp to:<me>
451 Listed by ORDB - for testing purposes only
quit
221 rblsmtpd.local
Connection closed by foreign host.
```

5.3 Mail Relay Testing

The mail relay testing is done from a remote system to see if the mail server subjected to open relaying.

```
# Telnet 192.168.2.2 25
Trying 192.168.2.2...
Connected to 192.168.2.2.
Escape character is '^]'.
220 NOTICE: Unauthorised access are strictly prohibited by law. Any access to
the system are logged. ESMTP
mail from:<spamtest@domain.com>
250 ok
rcpt to:<abuse.net!relaytest@domain.com>
553 we don't relay (#5.7.1)
RSET
250 flushed
mail from:<spamtest@domain.com>
250 ok
```

```
rcpt to:<relaytest@abuse.net>
553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
QUIT
```

Noted: The ip address and domain is hidden or changed to a fictitious value.

The above test result is extracted from the testing via www.abuse.net/relay.html (Please see Appendix C for reference)

5.4 Content Filtering and POP3 Testing

Before testing the POP3, a spam mail is created and sent to the mail server, as shown below.

```
# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 NOTICE: Unauthorised access are strictly prohibited by law. Any access to
the system are logged. ESMTP
mail from: admin@domain.com
250 ok
rcpt to: admin@domain.com
250 ok
data
354 go ahead
Subject: good sex!
.
250 ok 1061263962 qp 31793
quit
221 NOTICE: Unauthorised access are strictly prohibited by law. Any access to
the system are logged.
Connection closed by foreign host.
```

From the above, it is shown that the email has violated the recommended filtering rule (please refer to Appendix B for reference). Thus, this email will be quarantined and an email alert will be sent to the administrator by the qmail scanner.

To test if administrator has the incoming email alert using POP3.

```
# telnet 192.168.2.2 110
Trying 192.168.2.2...
Connected to 192.168.2.2.
Escape character is '^]'.
+OK <31682.1061262460@mailbox.domain.com>
user admin@domain.com
```

```
+OK
pass <password>
+OK
list
+OK
1 2199
2 1860
.
retr 1
quit
+OK
Connection closed by foreign host.
```

As mentioned above, the mail alert (result from message 1, please see Appendix D for reference) will be sent to the administrator.

6.0 Conclusion

This document has provided all necessary steps for setting up a secure mail server using qmail package as well as the other packages for anti-spamming, anti-virus, content filtering features & etc.

The document has also shown various testing methods to verify that all public services are well protected and secure.

By implementing strict content filtering rules together with antivirus software, the possibility of the virus outbreak is greatly reduced.

Thus, SME is able to implement a secure open source mail server for their company, which will help to reduce their administrative overhead and also reduce their Total Ownership Cost (TOC) in a long run.

7.0 Recommendation

Despite the mail server is secure and well protected, a regular monitor of log files is crucial to detect any sign of intrusion. In addition, Tripwire could be used to monitor the control files (/var/qmail/control) and binary files; trigger alert for any suspicious amendment of those files.

Nevertheless, the email security protection should not only rely on the mail server alone.

The overall email security policy should be enforced across the company. User security awareness is a very important essence in security defense model.

Users education on security matters (i.e. latest worm attacks) and email acceptable policy should be updated

Updated personal firewall and antivirus software at the client systems also acts as additional layer of defense.

Various security tools like Network Intrusion Detection System (NIDS) could also be deployed to provide parameter defense that may detect or stop any initial attacks.

8.0 Bibliography

[1] David Koconis "Securing Linux: A Survival Guide for Linux Security", SANS Press, 2003

[2] CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
Original issue date: September 19, 1996
Last revised: November 29, 2000
http://www.cert.org/advisories/CA-1996-21.html

[3] Offer only essential network services and operating system services on the server host machine, CERT, 2001
http://www.cert.org/security-improvement/practices/p068.html

[4] P. Ferguson "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", 1998
http://www.faqs.org/rfcs/rfc2267.html

[5] Robert L. Ziegler "Linux Firewall", 2nd edition, New Riders, 2002

[6] D.J. Bernstein "ucspi-tcp"
http://cr.yp.to/ucspi-tcp.html

[7] Carla Schroder "Daemons Running Amok? Daemontools to the Rescue!"
http://networking.earthweb.com/netos/article.php/1551951

[8] D.J. Bernstein "BIND versus djbdns"
http://cr.yp.to/djbdns/blurb/easeofuse.html

[9] Dave Sill "The qmail Handbook", Apress, 2002

[10] Dave Sill "Life With qmail", 2003
http://www.lifewithqmail.org/lwq.html

[11] Ken Jones "vpopmail Adminstration Guide"
http://www.inter7.com/vpopmail/vpopmail.html

[12] Jason Haar "Qmail-Scanner Frequently Asked Questions"
http://qmail-scanner.sourceforge.net/FAQ.php

[13] Ismail Yenigul "spamGuard 1.6 README"
http://www.enderunix.org/spamguard/spamguard-1.6/README

[14] Installing, configuring, and operating the secure shell (SSH) on systems running Solaris 2.x, CERT, 2000
http://www.cert.org/security-improvement/implementations/i062_01.html

Appendix A: qmailctl listing

```
#!/bin/sh

# For Red Hat chkconfig
# chkconfig: - 80 30
# description: the qmail MTA

PATH=/var/qmail/bin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
export PATH

QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`

case "$1" in
  start)
    echo "Starting qmail"
    if svok /service/qmail-send ; then
      svc -u /service/qmail-send /service/qmail-send/log
    else
      echo "qmail-send supervise not running"
    fi
    if svok /service/qmail-smtpd ; then
      svc -u /service/qmail-smtpd /service/qmail-smtpd/log
    else
      echo "qmail-smtpd supervise not running"
    fi
    if svok /service/qmail-pop3d; then
      svc -u /service/qmail-pop3d
    else
      echo "qmail-pop3d supervise not running"
    fi
    if [ -d /var/lock/subsys ]; then
      touch /var/lock/subsys/qmail
    fi
    ;;
  stop)
    echo "Stopping qmail..."
    echo "  qmail-smtpd"
    svc -d /service/qmail-smtpd /service/qmail-smtpd/log
    echo "  qmail-send"
    svc -d /service/qmail-send /service/qmail-send/log
    echo "  qmail-pop3d"
    svc -d /service/qmail-pop3d
    if [ -f /var/lock/subsys/qmail ]; then
      rm /var/lock/subsys/qmail
    fi
    ;;
  stat)
    svstat /service/qmail-send
    svstat /service/qmail-send/log
    svstat /service/qmail-smtpd
    svstat /service/qmail-smtpd/log
    svstat /service/qmail-pop3d
    svstat /service/qmail-pop3d/log
```

```
  qmail-qstat
  ;;
doqueue|alrm|flush)
  echo "Flushing timeout table and sending ALRM signal to qmail-send."
  /var/qmail/bin/qmail-tcpok
  svc -a /service/qmail-send
  ;;
queue)
  qmail-qstat
  qmail-qread
  ;;
reload|hup)
  echo "Sending HUP signal to qmail-send."
  svc -h /service/qmail-send
  ;;
pause)
  echo "Pausing qmail-send"
  svc -p /service/qmail-send
  echo "Pausing qmail-smtpd"
  svc -p /service/qmail-smtpd
  echo "Pausing qmail-pop3d"
  svc -p /service/qmail-pop3d
  ;;
cont)
  echo "Continuing qmail-send"
  svc -c /service/qmail-send
  echo "Continuing qmail-smtpd"
  svc -c /service/qmail-smtpd
  echo "Continuing qmail-pop3d"
  svc -c /service/qmail-pop3d
  ;;
restart)
  echo "Restarting qmail:"
  echo "* Stopping qmail-smtpd."
  svc -d /service/qmail-smtpd /service/qmail-smtpd/log
  echo "* Sending qmail-send SIGTERM and restarting."
  svc -t /service/qmail-send /service/qmail-send/log
  echo "* Restarting qmail-smtpd."
  svc -u /service/qmail-smtpd /service/qmail-smtpd/log
  echo "* Restarting qmail-pop3d."
  svc -u /service/qmail-pop3d
  ;;
cdb)
  tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
  chmod 644 /etc/tcp.smtp.cdb
  echo "Reloaded /etc/tcp.smtp."
  tcprules /etc/tcp.pop3.cdb /etc/tcp.pop3.tmp < /etc/tcp.pop3
  chmod 644 /etc/tcp.pop3.cdb
  echo "Reloaded /etc/tcp.pop3."
  ;;
help)
  cat <<HELP
 stop -- stops mail service (smtp connections refused, nothing goes out)
start -- starts mail service (smtp connection accepted, mail can go out)
pause -- temporarily stops mail service (connections accepted, nothing leaves)
 cont -- continues paused mail service
```

```
   stat -- displays status of mail service
    cdb -- rebuild the tcpserver cdb file for smtp
restart -- stops and restarts smtp, sends qmail-send a TERM & restarts it
doqueue -- schedules queued messages for immediate delivery
 reload -- sends qmail-send HUP, rereading locals and virtualdomains
  queue -- shows status of queue
   alrm -- same as doqueue
  flush -- same as doqueue
    hup -- same as reload
HELP
    ;;
  *)
    echo "Usage: $0 {start|stop|restart|doqueue|flush|reload|stat|pause|cont|cdb|queue|help}"
    exit 1
    ;;
esac

exit 0
```

Appendix B: Recommended quarantine-attachments.txt

Noted: unsafe extension is based on (http://support.microsoft.com/?kbid=290497)

.ade	0	Access Project Extension (.ade)
.adp	0	Access Project (.adp)
.asx	0	Windows Media Audio / Video(.asx)
.bas	0	Visual Basic Class Module (.bas)
.bat	0	Command.com batch file (.bat)
.btm	0	JP Software fast batch (.btm)
.chm	0	Compiled HTML help file (.chm)
.cmd	0	cmd .exe NT batch (.cmd)
.com	0	Non relocable MSDOS executable binary (.com)
.cpl	0	Control Panel Library (.cpl)
.crt	0	Security Certificate (.crt)
.css	0	Cascading Style Sheets (.css)
.dbx	0	Graphics DataBeam image or Table file Visual Foxpro (.dbx)
.dll	0	Dynamic Link Library (.dll)
.exe	0	Executable File (.exe)
.hlp	0	Windows Help File (.hlp)
.hqx	0	WinZip Executable (.hqx)
.hta	0	HTML Application (.hta)
.inf	0	Windows INF file (.inf)
.ins	0	Internet Naming Service (.ins)
.isp	0	Internet Communication Settings (.isp)
.js	0	JavaScript (.js)
.jse	0	JavaScript Encoded (.jse)
.lnk	0	Windows Explorer Links (.lnk)
.mda	0	Microsoft Access add-in program (.mda)
.mdb	0	Microsoft Access Program (.mdb)
.mde	0	Microsoft Access MDE database (.mde)
.mdt	0	Microsoft Access workgroup information (.mdt)
.mdw	0	Microsoft Access workgroup information (.mdw)
.mdz	0	Microsoft Access wizard program (.mdz)
.msc	0	Microsoft Common Console document (.msc)
.msi	0	Microsoft Windows Installer package (.msi)
.msp	0	Microsoft Windows Installer patch (.msp)
.mst	0	Windows Installer transform or Test source file (.mst)
.nch	0	Newsgroup Internet Explorer or Microsoft Outlook (.nch)
.ops	0	Office XP settiings (.ops)
.pcd	0	Photo CD image; Microsoft Visual compiled script (.pcd)
.pif	0	Windows Program Information Files (.pif)
.prf	0	Microsoft Outlook profile settings (.prf)
.reg	0	Windows Registry file (.reg)
.scf	0	Windows Explorer command (.scf)
.scr	0	Sceen Saver (.scr)
.sct	0	Windows Script Component (.sct)
.shb	0	Shell Scrap Object (.shb)
.shs	0	Shell automation code (.shs)
.vb	0	VBScript file (.vb)
.vba	0	Visual Basic Application (.vba)
.vbe	0	VBScript Encoded script file (.vbe)
.vbs	0	Visual Basic Script (.vbs)
.vxd	0	Virtual device driver for Microsoft Windows (.vxd)
.wsc	0	Windows Script Component (.wsc)

```
.wsf    0       Windows Scripting File (.wsf)
.wsh    0       Windows Script Host Settings file (.wsh)
message/partial Virus-Content-Type      Message/partial MIME attachments blocked by policy
.{100,} Virus-Date      MIME Header Buffer Overflow
message/partial Virus-Content-Type:     Message/partial MIME attachments blocked by policy
.{100,} Virus-Date:     MIME Header Buffer Overflow
.{100,} Virus-Mime-Version:     MIME Header Buffer Overflow
.{100,} Virus-Resent-Date:      MIME Header Buffer Overflow
```

Appendix C: Mail Relay Testing via www.abuse.net/relay.html

Connecting to <domain.com> for anonymous test ...
<<< 220 NOTICE: Unauthorised access are strictly prohibited by law. Any access to the system a re logged. ESMTP
>>> HELO www.abuse.net
<<< 250 NOTICE: Unauthorised access are strictly prohibited by law. Any access to the system a re logged.
Relay test 1
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@abuse.net>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 2
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 3
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 4
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 5
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@[xxx.xxx.xxx.xxx]>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 6
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<relaytest%abuse.net@domain.com>
<<< 553 we don't relay (#5.7.1)
Relay test 7
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok

>>> RCPT TO:<relaytest%abuse.net@[xxx.xxx.xxx.xxx]>
<<< 553 we don't relay (#5.7.1)
Relay test 8
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<"relaytest@abuse.net">
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 9
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<"relaytest%abuse.net">
<<< 553 we don't relay (#5.7.1)
Relay test 10
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net@domain.com>
<<< 553 we don't relay (#5.7.1)
Relay test 11
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<"relaytest@abuse.net"@domain.com>
<<< 553 we don't relay (#5.7.1)
Relay test 12
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<relaytest@abuse.net@[xxx.xxx.xxx.xxx]>
<<< 553 we don't relay (#5.7.1)
Relay test 13
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<@domain.com:relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 14
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<@[xxx.xxx.xxx.xxx]:relaytest@abuse.net>
<<< 553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)
Relay test 15
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok

>>> RCPT TO:<abuse.net!relaytest>
<<< 553 we don't relay (#5.7.1)
Relay test 16
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<abuse.net!relaytest@domain.com>
<<< 553 we don't relay (#5.7.1)
Relay test 17
>>> RSET
<<< 250 flushed
>>> MAIL FROM:<spamtest@domain.com>
<<< 250 ok
>>> RCPT TO:<abuse.net!relaytest@[xxx.xxx.xxx.xxx]>
<<< 553 we don't relay (#5.7.1)
Relay test result
All tests performed, no relays accepted.

Appendix D: Email Alert to Administrator for Spam Mail

Attention: admin@domain.com

A virus was found in an Email message sent to you.
This Email scanner intercepted it and stopped the entire message
before it reached you. No further action is required on your part.

The virus was reported to be:

Spam Mail

Please contact your I.T support personnel with any queries regarding this policy.

The message sent to you had the following envelope:

MAIL FROM: admin@domain.com
RCPT TO: admin@domain.com

... and with the following headers:

MAILFROM: admin@domain.com
Received: from unknown (HELO demo) (127.0.0.1)
by 0 with SMTP; 19 Aug 2003 03:07:30 -0000
Received: (qmail 20989 invoked by uid 7794); 19 Aug 2003 02:53:27 -0000
Received: from admin@domain.com by mailbox by uid 89 with qmail-scanner-1.16
(Clear:.
Processed in 0.0976590000000001 secs); 19 Aug 2003 02:53:27 -0000
Received: from unknown (HELO demo) (admin@domain.com@127.0.0.1)
by 0 with SMTP; 19 Aug 2003 02:53:26 -0000
From: "Administrator" <admin@domain.com>
To: <admin@domain.com>
Subject: good sex
Date: Tue, 19 Aug 2003 10:42:49 +0800
Message-ID: <CNEFLMPJPPBDLLKMANMCGEAGCCAA.bentan@domain.com>
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

The original message is kept in:

mailbox:/var/spool/qmailscan//quarantine

where the System Anti-Virus Administrator can further diagnose it.

The Email scanner reported the following when it scanned that message:

---perlscanner results ---
virus 'Spam Mail' found in file /var/spool/qmailscan//mailbox106126245042631662/