Global Information Assurance Certification Paper

Build securely SMTP Server on Solaris 8

GSEC Practical Assignment (Version 1.4b)

Peter Yang
April 25, 2003

Abstract

SMTP server is used for relaying email messages to deliver to its destinations, and it will filter the unsolicited email that called SPAM. To stop SPAM and email VIRUS at SMTP server before it is delivered to the end user's computer is becoming more and more important to security issue for the email system in most organization.
This paper will provide an overview of SMTP server and how SPAM email can affect company's business. Then describe about Postfix MTA software, Amavisd-new content scanner software, and Sophos Anti-Virus software. Following is the step by step instruction to install and configure these software on Solaris 8 operating system, and the instruction will include how to hardening the base operating system with Sun's JASS Toolkit, openssh, and TCP Wrapper.

Introduction

Let's begin with an email example to see how SMTP server works. When you send an email from Outlook Express, the Outlook Express will talk to the SMTP server at port 25 and telling the SMTP server the sender's email address and the recipient's email address, as well as the content of the message. The SMTP server will communicate with the recipient's Domain Name Server. The DNS will reply with at least one IP address for the SMTP server for their domain, the SMTP server at sender's side connects with the SMTP server at recipient's side at port 25. After recipient's SMTP server recognizes that the email address is at in local aliases database, so it deliver the message to the POP3 server or Exchange server, and it put the message in recipients mailbox.

The internet email system provide an easy and fast way to deliver the message, because of this advantage, the spammers send unsolicited and unwanted advertisements to millions of email addresses, which not only create heavy internet traffic but also cause security problem because the Spam can carry the virus in the contents of the email. "According to Ferris

Research Inc., A San Francisco consulting group, spam will cost U.S. organizations more than $10 billion this year." (By Jonathan Krim, Washington Post Staff Writer, March 13, 2003; on page A01). For more information, more information can be found at the web site http://www.washingtonpost.com/wp-dyn/articles/A17754-2003Mar12.html. Spam cost include bandwidth charges and other problems, such as hard disk space on mail server can be fill out by Spam messages, then the mail server can be in trouble, and it can interrupt the email service to end user.

How to stop SPAM is becoming an important issue in most company. One of effective way to achieve this goal is to filter the Spam on SMTP server, which can be done by installing the Postfix MTA software, Amavisd-new content scanner software, and the Sophos Anti-Virus software. For more information, you can visi http://www.ijs.si/software/amavisd/.

Postfix

Postfix MTA is alternative to sendmail, and it attempts to be fast, easy to administrate, and it's secure. Postfix is freeware. Postfix is designed to be sendmail compatible; it uses multiple layers of defense to protect the system against intruders. Postfix does not use sendmail.cf, instead it use main.cf and master.cf. For more information, you can visit www.postfix.org

Amavisd-new

Amavisd-new is a high-performance and reliable interface between mailer (MTA) and one or more content checkers, such as Anti-Spam and Anti-Virus scanners. It is written entirely in Perl, assuring high reliability, portability and maintainability. It talks to MTA via SMTP or LMTP, or by using helper programs. No timing gaps exist in the design, which could cause a mail loss.
It is normally positioned at or near a central mailer, not necessarily where user's mailboxes and final delivery takes place When calling of Mail::SpamAssassin is enabled, it calls SA only once per message (regardless of the number of recipients), and tries very hard to correctly honor per-recipient preferences, such as pass/reject, and inserting Spam-related mail header fields.

Amavisd-new benefits from the use of Perl module Net::Server,

which offers a fast pre-forked multichild environment. Amavisd-new provides rfc2821-compliant SMTP server, rfc2033-compliant LMTP server, SMTP client, and generates rfc1892/rfc1894-compliant (non-)delivery status notifications. This makes it suitable for mail anti-virus and/or anti-spam checking on busy mail gateways that care for reliability and standards compliance. For more information about Amavisd-new software, you can visit http://www.ijs.si/software/amavisd/.

Sophos

Sophos is the one of Anti-Virus software for data security designed to counter computer viruses, Trojan horses, and virus hoaxes. Etc. Sophos Anti-Virus for Unix is virus detection and disinfections software, which can be installed on Unix file servers and workstations checking local and remote file systems and networks for the presence of viruses. Sophos Anti-Virus for Unix offers on-demand scanning on Unix file servers, and ensures 100% virus detection. Scheduled scanning is possible using Sophos Anti-Virus and standard Unix facilities.

Sophos's excellent detection rates are regularly recognized and certified by a wide variety of independent testing bodies including True Secure ICSA Labs, West Coast Labs and Virus Bulletin. Many industry magazines and journals also routinely commend the software. For more information, you can visit http://www.sophos.com/companyinfo/.

OpenSSH

OpenSSH is a suite of tools to be used to secure the network connections. The features include strong authentication, closes several security holes (e.g., IP, routing, and DNS spoofing). Improved privacy. All communications are automatically and transparently encrypted. OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them. Openssl is required by the OpenSSH software application.

Businesses have trade secrets, patent applications in preparation, pricing information, subcontractor information, client data, personnel data, financial information, etc. Currently, anyone with access to the network (any machine on the network) can listen to anything that goes in the network, without any regard to normal access restrictions.

OpenSSH is a FREE version of the SSH protocol suite of network connectivity tools that increasing numbers of people on the Internet are coming to rely on. Many users of telnet, rlogin, ftp, and other such programs might not realize that their password is transmitted across the Internet unencrypted, but it is. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods. For more information, you can visit http://www.openssh.org/.

Solaris Security Toolkit (JASS)

Jass is a useful tool to help Solaris system administrator to hardening the UNIX server by disable the unnecessary services on the system, and the script can be configured based on specific requirement since the Unix server perform it's own application functionality. Jass toolkit make hardening process automatically and effectively, it save time for System Administrators. I like the feature what jass has, such as the undo capability and the settings can be customized. For more information, you can visit http://wwws.sun.com/software/security/jass/.

TCP Wrapper

TCP Wrapper is a program to monitor and filter incoming requests for network services, such as sendmail, ftp, telnet, finger, rlogin, etc. The Unix network services are accessible to anyone on the Internet.

This program can prevent computer hacker to explore your computer, for example the hacker can use finger service to find out the user's information on the system, the information include the user's name, and the login time, etc. this information can let hacker make a plan to determine the best time to crake your system. The TCP wrapper program can be used to control and monitor the incoming network traffic to protect the weakness of the authentication. For example, the TCP wrapper can deny the network services, such as rlogin to certain pre-specified IP address and DNS domain in hosts.deny file, and The program can log these information about the network services requested by the users and it is from which IP address, and this information can be send to the systems

administrator immediately so that the problem can be detected earlier, and system administrator have more time to do something to protect the system before the system be compromised. For the UNIX server security issue, the TCP wrapper is the one of the best network security tool to install, especially the UNIX server is located in outside firewall, such as in DMZ. Remember that the TCP Wrapper is only work on programs that using the Transmission Control Protocol/Internet Protocol (TCP/IP) network communications protocol, and the programs for network service on UNIX server are not run all the time, and the TCP Wrapper program is vulnerable to IP spoofing.

We need to understand how TCP Wrapper works in the UNIX server so that you know how you can effectively configure this software. When the TCP wrapper daemon process is running, it listening for the incoming network connections, when a connection is established, The inetd daemon will run the appropriate server program, for example, when a user use telnet command to connect to your system, the telnet server process is executed on your system, then the telnet server process connects the user to a login process, and then it goes back to sleep, and waiting for next connection request. The TCP wrapper program logs the host name or address of the connected host, and it performs additional checks. When all is well, the wrapper executes the desired program, for example, the telnet server program, and then it goes away. For more information, you can visit http://www.cert.org/security-improvement/implementations/i041.07.html.

Hardware

The server hardware is a Sun Ultra 1 with 128 MB memory and an 18 GB hard drive. There is one Ethernet interface hme0, no other external SCSI device is attached to the system.
Installation and Configuration

Pre-installation

Halt to the OK prompt by sending a Stop-A
Start the installation procedure:
Insert Solaris 8 software installation CD 1 of 2, and then enter command at OK prompt:
OK: boot cdrom
After boot from CD, following the check list below to install the OS:

Initial OS Installation Check List (Install the end user bundle).

1 Networked: Yes
2 Use dhcp: No
3 Primary interface: hme0
4 Hostname: smtp.example.com
5 IP address: xxx.xxx.xxx.xxx
6 Part of a subnet: Yes
7 Netmask: 255.255.0.0
8 Enable Ipv6: No
9 Configure Kerberos: No
10 Name service: None
11 Geographic regions: United States
12 Time Zones: Eastern
13 Date: current date
14 Time: current time
15 Entire System Support Installations
16 Choose Initial install
17 Select Standard Install
18 Geographic Regions for Support: United states
19 Install 64-bit support
20 Choose System Support
21 Do not preserve data, if applicable
22 No remote file systems
23 Customize the file system layout
   1GB /, 500MB swap, 5GB /usr/local, 5GB /export/home,
   6.5GB /var
24 Auto-reboot
25 Set root password
26 Create /etc/resolv.conf
27 /bin/echo nameserver xxx.xxx.xxx.xxx /etc/resolv.conf
28 /bin/chown root:root /etc/resolv.conf
29 /bin/echo '<gateway IP address>' > /etc/defaultrouter
30 Modify /etc/nsswitch.conf to set "files" entries,
  "hosts: files dns"
31 Reboot.

Install Patches

After install Solaris operating system, you must install the Sun recommended patches. Ensure that you are in single user mode to do the patches. Download the latest patchs at ftp://sunsolve.sun.com/pub/patches/8_sparc_Recommended.zip, after download the patch, Put this file into /usr/local/src directory you need to unzip the file and install it:

```
# > init s
# > cd /usr/local/src
# > unzip 8_Recommended.zip
# > cd 8_Recommended
# > ./install_cluster
After patche installation was completed, you can check the
patch log file at
/var/sadm/install_data/Solaris_8_recommended+log.

Install zlib 1.4.0

Download zlib-1.1.4-sol8-sparc-local.gz at
ftp://mirror.aca.oakland.edu/sunfreeware/sparc/8/
Put this file into /usr/local/src directory
# > cd /usr/local/src
# > gunzip zlib-1.1.4-sol8-sparc-local.gz
# > pkgadd –d zlib-1.1.4-sol8-sparc-local

Install gcc 2.95.3

Download gcc-2.95.3-sol8-sparc-local.gz at
ftp://mirror.aca.oakland.edu/sunfreeware/sparc/8/
Put this file into /usr/local/src directory.
# > cd /usr/local/src
# > gunzip gcc-2.95.3-sol8-sparc-local.gz
# > pkgadd –d gcc-2.95.3-sol8-sparc-local

Install perl 5.8.0

Download perl-5.8.0.tar.gz at
ftp://mirror.aca.oakland.edu/sunfreeware/SOURCES/
Put this file into /usr/local/src directory.
Ensure "/usr/ccs/bin" and "/usr/local/bin" are included in the
"$PATH" before install the following software.
# > cd /usr/local/src
# > gunzip perl-5.8.0.tar.gz
# > tar xvf perl-5.8.0.tar
# > cd perl-5.8.0
# > rm –f config.sh Policy.sh
# > sh Configure –de
# > make
# > make test
# > make install

Install cdb
```

Download cdb-0.75.tar at http://cr.yp.to/cdb/install.html,
For more information, you can visit http://cr.yp.to/cdb.html.
Put this file into /usr/local/src directory.

```
# > cd /usr/local/src
# > tar xvf cdb-0.75.tar
# > cd cdb-0.75
# > make
# > make setup check
```

Install CPAN Modules

Download the following CPAM modules at
http://www.cpan.org/modules/01modules.index.html
Amavis software depends on these modules:
MIME-Tools-5.411a_2, Mail-Tools-1.48, Net-1.11.1, MIME-Base64-2.12, File-Spec-0.82, IO-stringy-2.108, Convert-Uulib-0.213, Convert-TNEF-0.17, zoo-2.10.1, unrar-3.00, unarj-2.43_1, Compress-zlib-1.6, Archive-zip-1.03, Archive-tar-0.22, arc-5.21e.8_1, lha-1.14i.
Put these modules into /usr/local/src, unpack and install.
If your machine is connected to Internet, you can use "perl –MCPAN –e shell" to install these software. For more information, you can visit
http://www.geocities.com/scottlhenderson/spamfilter.html.

Install openssl

Download openssl-0.9.7.a.tar.gz at
http://www.openssl.org/source/
For more information about openssl, you can visit
www.openssl.org
Put file into /usr/local/src,

```
# > cd /usr/local/src
# > gunzip openssl-0.9.7.a.tar.gz
# > tar xvf openssl-0.9.7.a.tar
# > cd openssl-0.9.7.a
# > ./config --prefix=/usr/local
           --openssldir=/usr/local/openssl
# > make
# > make test
# > make install
```

Install wget-1.8.2-sol8-sparc-local.gz

```
Download wget-1.8.2-sol8-sparc-local.gz at
ftp://carroll.cac.psu.edu/pub/solaris/freeware/SOURCES/
Put file into /usr/local/src directory.
# > cd /usr/local/src
# > gunzip wget-1.8.2-sol8-sparc-local.gz
# > pkgadd -d wget-1.8.2-sol8-sparc-local

Install Tcp Wrapper
Download tcp_wrapper-7.6.tar.gz at
ftp://carroll.cac.psu.edu/pub/solaris/freeware/SOURCES/
For more information, see TCP Wrapper installation README file.
Put file into /usr/local/src directory.
# > cd /usr/local/src/tcp_wrappers_7.6
# > vi Makefile
To uncomment REAL_DAEMON_DIR=/usr/sbin line.
# > make sunos5 CC=gcc
# > cp tcpd.h /usr/include/.
# > cp libwrap.a /usr/lib/.
# > cp tcpd safe_finger /usr/sbin/.

This will install the binaries in /usr/local/bin, configuration
files in /usr/local/etc, the server in /usr/local/sbin.
Create and configure the /etc/hosts.deny file and
/etc/hosts.allow file.

Install openssh

Download openssh-3.5p1.tar.gz at
ftp://carroll.cac.psu.edu/pub/solaris/freeware/SOURCES/
Put file into /usr/local/src directory.
# > gunzip openssh-3.5p1.tar.gz
# > tar xvf openssh-3.5p1.tar
# > cd openssh-3.5p1
# > ./configure –with-tcp-wrappers
# > make
# > make install
After installation, configure the /usr/local/etc/ssh_config and
the /usr/local/etc/sshd_config files.
Make a startup script in /etc/init.d/sshd, and
# > ln –s /etc/init.d/sshd /etc/etc/rc2.d/S87sshd
Start sshd daemon
# > /etc/init.d/sshd start

Then perform the following edits on the inetd configuration
file
# > vi /etc/inet/inetd.conf
```

```
    smtp    stream  tcp     nowait  root    /usr/etc/tcpd
/usr/lib/sendmail -bs
```

Then
```
# > pkill -HUP inetd
```

The tcpd program can be used to control access to the mail Service. This can let you to suspect someone trying out to broken sendmail, or when a remote site is misconfigured and keeps hammering your mail daemon.

The wrapper programs send their logging information to the syslog daemon (syslogd). The disposition of the wrapper logs is determined by the syslog configuration

```
# > vi /var/log/syslog
```

To make entry:

```
mail.debug                  /var/log/syslog
```

Then,
```
# > pkill -HUP syslogd
```

This will causes all messages of class mail with priority debug (or more urgent) to be appended to the /var/log/syslog file. By default, the wrapper logs go to the same place as the transaction logs the sendmail daemon.

Setup the access control rules in /etc/hosts.allow and /etc/hosts.deny).

Use tcpdchk program to examine all rules in the access control file

```
# > tcpchk
```

and

```
# > tcpdchk -v
```

Install Sophos

Download sophos software at
http://www.sophos.com/products/software/antivirus/savunix.html

```
Put file into /usr/local/src directory.
# > tar xvf sophos.tar

Create a user and a group named “sweep” before run the
installation script.

# > cd sav-install
# > ./install.sh

This will perform a default installation.

# > cd /usr/local/bin
# > ./sweep
# > ./icheckd

Install amavisd-new

Download amavisd-new software at
http://www.ijs.si/software/amavisd/
Put file into /ust/local/src directory.
Unpack the software
Make sure you have dependences installed, such as Archive-Tar-
0.23, Archive-Zip-1.05, Compress-Zlib-1.20, Convert-TNEF-0.17,
Convert-Uulib-0.31, Digest-MD5-2.24, IO-stringy-2.108, lha-
1.4i, MIME-Base64-2.12, MIME-Tools, MailTools, Net-
Server,libnet, Time-HiRes, Unix-Syslog, File-spec-0.82,  and
Mail-SpamAssassin-2.53 before install amavisd-new:
Create a Unix group, ‘amavis’, dedicated to run amavisd daemon.
Create a Unix user (UID), ‘amavis’ dedicated to run amavisd
daemon.
Create the home directory, /var/amavis:
# > mkdir /var/amavis
# > chown amavis:amavis /var/amavis
# > chmod 750 /var/amavis
# > cd /usr/local/src/amavis-new-20030314/
# > cp amavisd.conf /etc/
# > chown root /etc/amavisd.conf
# > chmod 644 /etc/amavisd.conf
# > cp amavisd /usr/local/sbin/
# > chown root /usr/local/sbin/amavisd
# > chmod 755 /usr/local/sbin/amavisd

create a directory, /var/virusmails, to be used by amavisd-new
as a quarantine area:

# > mkdir /var/virusmails
```

```
# > chown amavis:amavis /var/virusmails
# > chmod 750 /var/virusmails

And it's done. To start amavisd:
# > su - amavis -c /usr/local/sbin/amavisd

Install Postfix

Download postfix-2.0.6.tar.gz at
ftp://postfix.primelink1.net/mirrors/postfix-release/index.html
Before install postfix, create a user account "postfix" with a
user id and group id that are not used by any other user.
Preferably, this is an account that no-one can log into.  The
account does not need an executable login shell, and needs no
existing home directory.
The password file entry looks like this:
   postfix:*:60001:60001:postfix:/no/where:/no/shell

Make sure there is a corresponding alias in /etc/aliases:

    postfix: root

Create a group "postdrop" with a group id that is not used by
any other user account. Not even by the postfix user account.
  My group file entry looks like:

    postdrop:*:60002:

# > cd /usr/local/src/postfix-2.0.6

You may remove the original sendmail by pkgrm command before
install postfix.

# > make
# > make install

Basic Configuration settings in /etc/postfix/mail.cf:
The following information can be find at
http://www.postfix.org/basic.html

# The queue_directory specifies the location of the Postfix
queue.
queue_directory = /var/spool/postfix

# The command_directory parameter specifies the location of all
# postXXX commands.
```

```
#
command_directory = /usr/sbin

# The daemon_directory parameter specifies the location of all
Postfix
# daemon programs
daemon_directory = /usr/libexec/postfix

# The mail_owner parameter specifies the owner of the Postfix
queue
# and of most Postfix daemon processes.
mail_owner = postfix

# The myhostname parameter specifies the internet hostname of
this
# mail system.
myhostname = smtp.example.com

# The mydomain parameter is set to the local domain.
 mydomain = example.com

# The myorigin parameter specifies the domain that locally-
posted
# mail appears to come from.
myorigin = $mydomain

# The inet_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on.
inet_interfaces = all

# The mydestination parameter specifies the list of domains
that this
# machine considers itself the final destination for.
mydestination = $myhostname, localhost.$mydomain $mydomain

# The mynetworks parameter lists all networks that this machine
somehow trusts. This  #information can be used by the anti-UCE
<uce.html> features to recognize trusted SMTP # #clients that
are allowed to relay mail through Postfix.
mynetworks = xxx.xxx.0.0/16, 127.0.0.0/8

# The relay_domains parameter restricts what destinations this
system will
# relay mail to.
relay_domains = $mydestination
```

```
# The alias_maps parameter specifies the list of alias
databases used
# by the local delivery agent. The default list is system
dependent.
alias_maps = dbm:/etc/aliases

# The alias_database parameter specifies the alias database(s)
that
# are built with "newaliases" or "sendmail -bi".
alias_database = dbm:/etc/aliases

# The header_checks parameter specifies an optional table with
patterns
# that each logical message header is matched against,
including
# headers that span multiple physical lines.
# For details, see the sample-filter.cf file.
header_checks = regexp:/etc/postfix/header_checks

# The debug_peer_level parameter specifies the increment in
verbose
# logging level when an SMTP client or server host name or
address
# matches a pattern in the debug_peer_list parameter.
#
debug_peer_level = 2

# The following parameters are used when installing a new
Postfix version.
#
# sendmail_path: The full pathname of the Postfix sendmail
command.
# This is the Sendmail-compatible mail posting interface.
#
sendmail_path = /usr/lib/sendmail

# newaliases_path: The full pathname of the Postfix newaliases
command.
# This is the Sendmail-compatible command to build alias
databases.
#
newaliases_path = /usr/bin/newaliases

# mailq_path: The full pathname of the Postfix mailq command.
This
# is the Sendmail-compatible mail queue listing command.
```

```
#
mailq_path = /usr/bin/mailq

# setgid_group: The group for mail submission and queue
management
# commands.  This must be a group name with a numerical group
ID that
# is not shared with other accounts, not even with the Postfix
account.
#
setgid_group = postdrop

# manpage_directory: The location of the Postfix on-line manual
pages.
#

manpage_directory = /usr/local/man

# sample_directory: The location of the Postfix sample
configuration files.
#
sample_directory = /etc/postfix

# readme_directory: The location of the Postfix README files.
#
readme_directory = no

# Setup parameter for trouble report to the postmaster if the
mail is not delivered due to
# resource problem or it is due to the software problem or a
bounce message or the mail
# was rejected because of (UCE) policy restriction or there are
protocol errors.
notify_classes = resource, software, bounce, policy, protocol
```

Anti-Spam configuration settings in /etc/postfix/main.cf:

The following settings will reduce the SPAM significantely, and these mail
can be rejected before scan process by Amavisd, Spamassassin, and Sophos. The following information can be find at http://www.postfix.org/uce.html

A HELO(or EHLO) is required by the standard RFC mail, Some UCE software is non-standard,
so these SPAM can be stoped here.

```
smtpd_helo_required = yes
```

By default, the Postfix SMTP server accepts any garbage in the HELO (EHLO) command. There is a lot of broken or misconfigured software on the Internet.

```
smtpd_helo_restrictions = "permit_mynetworks,
reject_invalid_hostname, reject_unknown_hostname,
       reject_non_fqdn_hostname"
```

The 'permit_mynetworks' allows machines listed for the mynetworks value to be permitted without question.
The 'reject_invalid_hostname' reject the request when the client HELO or EHLO parameter has a bad hostname syntax. The invalid_hostname_reject_code specifies the response code to rejected requests (default: 501).
The 'reject_unknown_hostname' reject the request when the hostname in the client HELO (EHLO) command has no DNS A or MX record. The unknown_hostname_reject_code specifies the response code to rejected requests (default: 450).
The 'reject_non_fqdn_hostname' reject the request when the hostname in the client HELO (EHLO) command is not in fully-qualified domain form, as required by the RFC. The non_fqdn_reject_code specifies the response code to rejected requests (default: 504).

The smtpd_sender_restrictions parameter restricts what sender addresses this system accepts in MAIL FROM commands.

```
smtpd_sender_restrictions = hash:/etc/postfix/access,
reject_unknown_sender_domain, reject_non_fqdn_sender
```

The access file is another check used by postfix to block right at the front door certain senders/domains/IPaddress ranges. Below are bogus examples, create your own as you see fit. You need to have at least one entry in this file, because postfix will be looking here and expect to see SOMETHING. If you don't have any of these to create right now, just use a made up one for starters, like the last one in the COMMAND example below. Here's an example of an access file, /etc/postfix/access:

```
##Start of the access map file
```

```
#
# note: this file only accepts 3 forms of input
# [45]XX $message, REJECT, OK
#
ispy99@spamnet.cn 550 Go away
makeabuck@mlm.dom 550 You've got to be kidding me
allspam.dom 550 Spam is not accepted here
badguy.net REJECT
#250.192 REJECT
#goodguy@somewhere.com OK
justaspamminfool@allspamallthetime.com REJECT
##End of  the access map file
```

The 'reject_unknown_sender_domain' reject the request when the sender mail address has no DNS A or MX record. The unknown_address_reject_code parameter specifies the response code for rejected requests (default: 450). The response is always 450 in case of a temporary DNS error.
The 'reject_non_fqdn_sender' reject the request when the address in the client MAIL FROM command is not in fully-qualified domain form. The non_fqdn_reject_code specifies the response code to rejected requests (default: 504).

The smtpd_recipient_restrictions parameter restricts what recipient addresses this system accepts in RCPT TO commands.

```
smtpd_recipient_restrictions = reject_unknown_recipient_domain,
reject_non_fqdn_recipient
```

The 'reject_unknown_recipient_domain' reject the request when the recipient mail address has no DNS A or MX record. The unknown_address_reject_code parameter specifies the response code for rejected requests (default: 450). The response is always 450 in case of a temporary DNS error.
The 'reject_non_fqdn_recipient' reject the request when the address in the client RCPT TO command is not in fully-qualified domain form. The non_fqdn_reject_code specifies the response code to rejected requests (default: 504).

The header_checks parameter restricts what is allowed in message headers. Patterns are applied to entire logical message headers, even when a header spans multiple lines of text.

```
header_checks = regexp:/etc/postfix/header_checks
```

```
The following is the 'Content Filter' configuration with
Amavisd-new/Spamassassin and Sophos

The 'content_filter' specify how the mail will pass to amavisd
and SpamAssassin for filtering, enter the following entry in
/etc/postfix/main.cf:

content_filter=smtp-amavis:[localhost]:10024

Add the following lines in /etc/postfix/master.cf:

smtp-amavis unix -      -       n       -       2  smtp
             -o smtp_data_done_timeout=1200

127.0.0.1:10025  inet    n      -       n       -       -
smtpd
             -o content_filter=
         -o local_recipient_maps=
         -o myhostname=localhost.example.gov
         -o relay_recipient_maps=
         -o smtpd_restriction_classes=
         -o smtpd_client_restrictions=
         -o smtpd_helo_restrictions=
         -o smtpd_sender_restrictions=
         -o
smtpd_recipient_restrictions=permit_mynetworks,reject
         -o mynetworks=127.0.0.0/8
         -o strict_rfc821_envelopes=yes



To start the postfix:

# > postfix start

Install JASS Toolkit

Download jass-0.3.10.tar.Z at
http://www.sun.com/solutions/blueprints/tools/jass/jass.html
# > uncompress jass-0.3.10.tar.Z
# > tar xvf jass-0.3.10.tar
# > cd jass-0.3.10
# >
Before run jass-execute, configure the settings to fit the
application server requirement.
```

I like to enable the sendmail and disable the BSM auditing at this moment, BSM may be enabled late, edit the Drives/hardening.driver file to comment out the "enable-bsm.fin line and edit the Drivers/undoable-hardening.drive to comment out the "enable-process-accounting.fin line and the disable-sendmail.fin line.

```
# > cd Driver
# > ../jass-execute -d hardening.driver
```

For more information, visit http://wwws.sun.com/software/security/jass/.
After the process is completed, reboot the system.

```
# > postfix start
# > su - amavis -c /usr/local/sbin/amavisd
```

(After testing completed, make start up scripts for postfix and amavisd in /etc/init.d/ directory and make "ln -s" to /etc/rc2.d to auto start program when system reboot).

Testing

The following are some SPAM test examples. Setup header_checks parameter in main.cf to stop the certain SPAM. In the table of the header_checks, you can specify the certain keyword used by Spammer, when a pattern matches, the postfix can take action based on the optional settings. More information you can find in "/etc/postfix/sample-filter.cf", "/etc/postfix/sample-regexp-header.cf", and other sample files in /etc/postfix directory. The sample test messages you can find in ../amavisd-new-20030314/test-messages directory. The following is the one of the parameters, header_checks setup in main.cf file:

```
header_checks = regexp:/etc/postfix/header_checks
```

The following are some sample settings in /etc/postfix/header_checks file:

```
/^Subject: Make Money/     REJECT
/^Subject: Investment/  WARN
/^Subject: Your Mortgage/        HOLD
/^Subject: Hurry/    REJECT
/^Subject: Free Vacation/    REJECT
```

In the first line above, if the subject in the message matchs the pattern like "Make Money", then the entire message will be rejected, and the message will be send to the originator, and

it will be logged in the mail.log file. In the second line, if the subject in the message matches the pattern like "Investment", then the message will be delivered, but the message header and the optional text will be logged in the mail.log file. In the third line, if the header of the message matches the pattern like Your Mortgage, and the message will be on the Hold Queue, the message can be inspected late with the postcat command, after inspection, you can destroy the message or delivered with postsuper command. The matched header is logged with the optional text in the mail.log file. There are more parameters can be setup in postfix to restrict the SPAM, See postfix documentation for more detail.

In this example, send message with Subject: Free Vacation, and this message will be REJECTED by the postfix:

```
# > mail tester <<!
> Subject: Free Vacation
> To: tester
> This is a test message.
> !
# >
```

Logged message in mail.log file:

```
Apr 22 09:37:41 smtp postfix/pickup[18832]: [ID 197553
mail.info] D56922F401: uid=0 from=<root>
Apr 22 09:37:42 smtp postfix/cleanup[18895]: [ID 197553
mail.info] D56922F401: reject: header Subject: Free Vacation
from local; from=<root@example.com> to=<tester@example.com>:
Message content rejected
Apr 22 09:37:42 smtp postfix/cleanup[18895]: [ID 197553
mail.info] D56922F401: message-
id=<20030422133741.D56922F401@example.com>
Apr 22 09:37:42 smtp postfix/cleanup[18895]: [ID 197553
mail.info] D56922F401: to=<tester@example.com>, relay=cleanup,
delay=1, status=bounced (Message content rejected)
Apr 22 09:37:42 smtp postfix/cleanup[18898]: [ID 197553
mail.info] 708612F402: message-
id=<20030422133742.708612F402@example.com>
Apr 22 09:37:42 smtp postfix/qmgr[18833]: [ID 197553
mail.info] 708612F402: from=<>, size=1887, nrcpt=1 (queue
active)
Apr 22 09:37:42 smtp postfix/local[18899]: [ID 197553
mail.info] 708612F402: to=<root@example.com>, relay=local,
delay=0, status=sent (mailbox)
```

```
Apr 22 09:38:07 smtp postfix/qmgr[18833]: [ID 947731
mail.warning] warning: connect to transport smtp-amavisd: No
such device or address

Returned mail:

smtp: root: 1 /etc/postfix> mail
From MAILER-DAEMON  Tue Apr 22 09:37:42 2003
Delivered-To: root@example.com
Date: Tue, 22 Apr 2003 09:37:42 -0400 (EDT)
From: MAILER-DAEMON@example.com (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: root@example.com
Message-Id: <20030422133742.708612F402@example.com>

This is a MIME-encapsulated message.

--D56922F401.1051018662/example.com
Content-Description: Notification
Content-Type: text/plain

This is the Postfix program at host example.com.

I'm sorry to have to inform you that the message returned
below could not be delivered to one or more destinations.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the message returned below.

                    The Postfix program

<tester@example.com>: Message content rejected

--D56922F401.1051018662/example.com
Content-Description: Delivery error report
Content-Type: message/delivery-status

Reporting-MTA: dns; example.com
Arrival-Date: Tue, 22 Apr 2003 09:37:41 -0400 (EDT)

Final-Recipient: rfc822; tester@example.com
Action: failed
Status: 5.0.0
Diagnostic-Code: X-Postfix; Message content rejected
```

```
--D56922F401.1051018662/example.com
Content-Description: Undelivered Message
Content-Type: message/rfc822

Received: by example.com (Postfix, from userid 0)
        id D56922F401; Tue, 22 Apr 2003 09:37:41 -0400 (EDT)
Subject: Free Vacation
To: tester@example.com
Content-Type: text
Message-Id: <20030422133741.D56922F401@example.com>
Date: Tue, 22 Apr 2003 09:37:41 -0400 (EDT)
From: root@example.com (Super-User)

This is a test message.


--D56922F401.1051018662/example.com--


?

The following example, send message with "Subject:
Investment", and this message will be delivered, and the
Warning message will be logged in mail.log file:

# > mail tester <<!
> Subject: Investment
> To: tester
> This is a test message.
> !
# >

Logged message in mail.log file

Apr 22 09:55:08 smtp last message repeated 6 times
Apr 22 09:56:08 smtp postfix/qmgr[18833]: [ID 947731
mail.warning] warning: connect to transport smtp-amavisd: No
such device or address
Apr 22 09:58:08 smtp last message repeated 2 times
Apr 22 09:58:18 smtp postfix/pickup[18832]: [ID 197553
mail.info] AB82A2F401: uid=0 from=<root>
Apr 22 09:58:18 smtp postfix/cleanup[18942]: [ID 197553
mail.info] AB82A2F401: warning: header Subject: Investment
from local; from=<root@example.com> to=<tester@example.com>
```

```
Apr 22 09:58:18 smtp postfix/cleanup[18942]: [ID 197553
mail.info] AB82A2F401: message-
id=<20030422135818.AB82A2F401@example.com>
Apr 22 09:58:19 smtp postfix/qmgr[18833]: [ID 197553
mail.info] AB82A2F401: from=<root@example.com>, size=346,
nrcpt=1 (queue active)
Apr 22 09:58:19 smtp postfix/local[18944]: [ID 197553
mail.info] AB82A2F401: to=<tester@example.com>,
orig_to=<tester>, relay=local, delay=1, status=sent (mailbox)

Received mail

smtp: tester: 1 /export/home/tester> mail
From root@example.com  Tue Apr 22 09:58:19 2003
Delivered-To: tester@example.com
Subject: Investment
To: tester@example.com
Message-Id: <20030422135818.AB82A2F401@example.com>
Date: Tue, 22 Apr 2003 09:58:18 -0400 (EDT)
From: root@example.com (Super-User)

This is a test message.

?
The following example, send message with "Subject: Your
Mortgage", and this message will be on Hold Queue:

# > mail tester <<!
> Subject: Your Mortgage
> To: tester
> This is a test messages about Your Mortgage.
> !
# >

Logged message in mail.log

Apr 22 10:07:08 smtp last message repeated 5 times
Apr 22 10:07:44 smtp postfix/pickup[18832]: [ID 197553
mail.info] 524042F401: uid=0 from=<root>
Apr 22 10:07:44 smtp postfix/cleanup[18967]: [ID 197553
mail.info] 524042F401: hold: header Subject: Your Mortgage
from local; from=<root@example.com> to=<tester@example.com>
Apr 22 10:07:44 smtp postfix/cleanup[18967]: [ID 197553
mail.info] 524042F401: message-
id=<20030422140744.524042F401@example.com>
```

```
Apr 22 10:08:08 smtp postfix/qmgr[18833]: [ID 947731
mail.warning] warning: connect to transport smtp-amavisd: No
such device or address
```

Using postcat command to check the mail on Hold Queue:

```
# > postcat -v /var/spool/postfix/hold/5/524042F401
*** ENVELOPE RECORDS /var/spool/postfix/hold/5/524042F401 ***
message_size:             370             150               1
arrival_time: Tue Apr 22 10:07:44 2003
named attribute: message_origin=local
sender: root@example.com
original recipient: tester
recipient: tester@example.com
*** MESSAGE CONTENTS /var/spool/postfix/hold/5/524042F401 ***
final line fragment: Received: by example.com (Postfix, from
userid 0)
final line fragment:    id 524042F401; Tue, 22 Apr 2003
10:07:44 -0400 (EDT)
final line fragment: Subject: Your Mortgage
final line fragment: To: tester@example.com
final line fragment: Content-Type: text
final line fragment: Message-Id:
<20030422140744.524042F401@example.com>
final line fragment: Date: Tue, 22 Apr 2003 10:07:44 -0400
(EDT)
final line fragment: From: root@example.com (Super-User)
final line fragment:
final line fragment: This is a test messages about Your
Mortgage.
final line fragment:
*** HEADER EXTRACTED /var/spool/postfix/hold/5/524042F401 ***
return_receipt:
errors_to: root@example.com
*** MESSAGE FILE END /var/spool/postfix/hold/5/524042F401 ***
```

Using postsuper command to release the mail:

```
smtp: root: 1 /var/spool/postfix/hold/5> postsuper -H
524042F401
postsuper: 524042F401: released from hold
postsuper: Released from hold: 1 message
smtp: root: 1 /var/spool/postfix/hold/5>
```

Logged message in mail.log file:

```
Apr 22 10:21:07 smtp postfix/qmgr[18833]: [ID 197553
mail.info] 524042F401: from=<root@example.com>, size=370,
nrcpt=1 (queue active)
Apr 22 10:21:08 smtp postfix/local[19033]: [ID 197553
mail.info] 524042F401: to=<tester@example.com>,
orig_to=<tester>, relay=local, delay=804, status=sent
(mailbox)

Received message:

smtp: tester: 1 /export/home/tester> mail
From root@example.com  Tue Apr 22 10:21:08 2003
Delivered-To: tester@example.com
Subject: Your Mortgage
To: tester@example.com
Message-Id: <20030422140744.524042F401@example.com>
Date: Tue, 22 Apr 2003 10:07:44 -0400 (EDT)
From: root@example.com (Super-User)

This is a test messages about Your Mortgage.

?

The following example, send a large file that larger than the
value of the parameter setting, "message_size_limit =1024000",
and the message will be droped:

# > mail tester < large.txt
postdrop: warning: uid=0: File too large
sendmail: fatal: root(0): Message file too big
# >

Logged message in mail.log file:

Apr 22 11:04:24 smtp postfix/postdrop[19209]: [ID 947731
mail.warning] warning: uid=0: File too large
Apr 22 11:04:24 smtp postfix/sendmail[19208]: [ID 947731
mail.crit] fatal: root(0): Message file too big

The following is a normal message, and it is expected to
delivered to the recipient:

# > mail tester <<!
> Subject: test message
> To: tester
> This is a test message.
```

```
> !

Here is the received message:

From root@example.com  Tue Apr 22 11:13:41 2003
Delivered-To: tester@example.com
Subject: test message
To: tester@example.com
Message-Id: <20030422151340.295012F401@example.com>
Date: Tue, 22 Apr 2003 11:13:40 -0400 (EDT)
From: root@example.com (Super-User)

This is a test message.

?

Logged message in the mail.log file:

Apr 22 11:13:41 smtp postfix/pickup[19202]: [ID 197553
mail.info] 295012F401: uid=0 from=<root>
Apr 22 11:13:41 smtp postfix/cleanup[19236]: [ID 197553
mail.info] 295012F401: message-
id=<20030422151340.295012F401@example.com>
Apr 22 11:13:41 smtp postfix/qmgr[19204]: [ID 197553
mail.info] 295012F401: from=<root@example.com>, size=348,
nrcpt=1 (queue active)
Apr 22 11:13:41 smtp postfix/local[19238]: [ID 197553
mail.info] 295012F401: to=<tester@example.com>,
orig_to=<tester>, relay=local, delay=1, status=sent (mailbox)

Now, let's test amavisd-new software. Before testing, make
sure the following entries was placed in both of main.cf file
and the master.cf, and the amavisd.conf file was also
configured properly:

master.cf:
  # MTA -> amavisd
  smtp-amavisd      unix - - n - 2 smtp

  # amavisd -> MTA
  localhost:10025   inet n - n - - smtpd -o content_filter=

main.cf:
  # choose transport to amavisd
  content_filter = smtp-amavisd:localhost:10024
```

Send sample spam message:

```
# > mail tester < sample-spam.txt
# >
```

Logged message in the mail.log file:

```
Apr 22 13:36:02 smtp postfix/pickup[19470]: [ID 197553
mail.info] DF12A2F403: uid=0 from=<root>
Apr 22 13:36:02 smtp postfix/cleanup[19472]: [ID 197553
mail.info] DF12A2F403: message-id=<N1msdrbJXNPfV4wg9>
Apr 22 13:36:02 smtp postfix/qmgr[19471]: [ID 197553
mail.info] DF12A2F403: from=<root@example.com>, size=4790,
nrcpt=1 (queue active)
Apr 22 13:36:02 smtp amavis[19333]: [ID 538730 mail.info]
(19333-02) ESMTP:10024 /var/amavis/amavis-20030422T133430-
19333: <root@example.com> -> <tester@example.com> Received:
SIZE=4790 from example.com ([127.0.0.1]) by localhost (smtp
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 19333-02
for <tester@example.com>; Tue, 22 Apr 2003 13:36:02 -0400
(EDT)
Apr 22 13:36:02 smtp amavis[19333]: [ID 864722 mail.info]
(19333-02) body hash: 8c2dda5f03da62d3ac37f48d31141191
Apr 22 13:36:02 smtp amavis[19333]: [ID 714793 mail.info]
(19333-02) Checking: <root@example.com> ->
<tester@example.com>
Apr 22 13:36:02 smtp amavis[19333]: [ID 554277 mail.info]
(19333-02) cached 8c2dda5f03da62d3ac37f48d31141191 from
<root@example.com> (1,1,1)
Apr 22 13:36:02 smtp amavis[19333]: [ID 977598 mail.info]
(19333-02) local delivery: <root@example.com> -> <spam-
quarantine>, mbx=/var/virusmails/spam-
8c2dda5f03da62d3ac37f48d31141191-20030422-133602-19333-02.gz
Apr 22 13:36:02 smtp amavis[19333]: [ID 751796 mail.info]
(19333-02) SPAM, <root@example.com> -> <tester@example.com>,
Yes, hits=10.4 tag1=4.0 tag2=6.3 kill=6.3
tests=DRASTIC_REDUCED, HOME_EMPLOYMENT, INVALID_DATE,
INVALID_MSGID, MIME_HEADER_CTYPE_ONLY, MSGID_HAS_NO_AT,
NO_REAL_NAME, REMOVE_SUBJ, SMTPD_IN_RCVD, UNDISC_RECIPS,
quarantine spam-8c2dda5f03da62d3ac37f48d31141191-20030422-
133602-19333-02 (spam-quarantine)
Apr 22 13:36:02 smtp amavis[19333]: [ID 298755 mail.info]
(19333-02) Not-Delivered, <root@example.com> ->
<tester@example.com>, quarantine spam-
```

```
8c2dda5f03da62d3ac37f48d31141191-20030422-133602-19333-02,
Message-ID: <N1msdrbJXNPfV4wg9>
Apr 22 13:36:03 smtp amavis[19333]: [ID 853578 mail.info]
(19333-02) TIMING [total 816 ms] - SMTP EHLO: 17 (2%), SMTP
pre-MAIL: 7 (1%), SMTP pre-DATA-flush: 45 (5%), SMTP DATA: 93
(11%), body hash: 11 (1%), mime_decode: 272 (33%), write-
header: 167 (21%), save-to-local-mailbox: 65 (8%), unlink-1-
files: 136 (17%), rundown: 3 (0%)
Apr 22 13:36:03 smtp postfix/smtp[19474]: [ID 197553
mail.info] DF12A2F403: to=<tester@example.com>,
orig_to=<tester>, relay=127.0.0.1[127.0.0.1], delay=2,
status=bounced (host 127.0.0.1[127.0.0.1] said: 550 5.7.1
Message content rejected, id=19333-02 (in reply to end of DATA
command))
Apr 22 13:36:03 smtp postfix/cleanup[19472]: [ID 197553
mail.info] 1DA122F401: message-
id=<20030422173603.1DA122F401@example.com>
Apr 22 13:36:03 smtp postfix/qmgr[19471]: [ID 197553
mail.info] 1DA122F401: from=<>, size=6488, nrcpt=1 (queue
active)
Apr 22 13:36:03 smtp postfix/local[19483]: [ID 197553
mail.info] 1DA122F401: to=<root@example.com>, relay=local,
delay=0, status=sent (mailbox)


Returned mail:

From MAILER-DAEMON  Tue Apr 22 13:36:03 2003
Delivered-To: root@example.com
Date: Tue, 22 Apr 2003 13:36:03 -0400 (EDT)
From: MAILER-DAEMON@example.com (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: root@example.com
Message-Id: <20030422173603.1DA122F401@example.com>

This is a MIME-encapsulated message.

--DF12A2F403.1051032963/example.com
Content-Description: Notification
Content-Type: text/plain

This is the Postfix program at host example.com.

I'm sorry to have to inform you that the message returned
below could not be delivered to one or more destinations.
```

```
For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the message returned below.

                    The Postfix program

<tester@example.com>: host 127.0.0.1[127.0.0.1] said: 550
5.7.1 Message content
    rejected, id=19333-02 (in reply to end of DATA command)

--DF12A2F403.1051032963/example.com
Content-Description: Delivery error report
Content-Type: message/delivery-status

Reporting-MTA: dns; example.com
Arrival-Date: Tue, 22 Apr 2003 13:36:01 -0400 (EDT)

Final-Recipient: rfc822; tester@example.com
Action: failed
Status: 5.0.0
Diagnostic-Code: X-Postfix; host 127.0.0.1[127.0.0.1] said:
550 5.7.1 Message
    content rejected, id=19333-02 (in reply to end of DATA
command)

--DF12A2F403.1051032963/example.com
Content-Description: Undelivered Message
Content-Type: message/rfc822

Received: by example.com (Postfix, from userid 0)
        id DF12A2F403; Tue, 22 Apr 2003 13:36:01 -0400 (EDT)
Delivery-Date: Mon, 22 Jan 2001 12:36:25 +0000
Delivered-To: dev_null_sample_spam@netnoteinc.com
Received: from dogma.slashnull.org (dogma.slashnull.org
[212.17.35.15])
        by mail.netnoteinc.com (Postfix) with ESMTP id
F138F114121
        for <dev_null_sample_spam@netnoteinc.com>; Mon, 22 Jan
2001 12:36:21 +0000 (Eire)
Received: (from dev_null_sample_spam@localhost)
        by dogma.slashnull.org (8.9.3/8.9.3) id MAA17343
        for dev_null_sample_spam@netnoteinc.com; Mon, 22 Jan
2001 12:36:21 GMT
Received: from XeNT.ics.uci.edu (xent.ics.uci.edu
[128.195.21.213])
```

```
        by dogma.slashnull.org (8.9.3/8.9.3) with ESMTP id
MAA17336
        for <dev_null_sample_spam@jmason.org>; Mon, 22 Jan
2001 12:36:16 GMT
From: xl6Ety00V@fismat1.fcfm.buap.mx
Received: from blue.mydomain.com (blue.mydomain.com
[208.184.130.52])
        by XeNT.ics.uci.edu (8.8.5/8.8.5) with ESMTP id
EAA16254
        for <fork@xent.ics.uci.edu>; Mon, 22 Jan 2001 04:38:11
-0800 (PST)
Received: from ns.fundch.cl (unknown [200.28.105.254])
        by blue.mydomain.com (Postfix) with ESMTP id
C32333424F
        for <fork@xent.com>; Sun, 21 Jan 2001 20:33:02 -0500
(EST)
X-Antispam: rblchk: (RSS) 3 Relayed through blacklisted site
200.28.105.254
Received: from y068k3017  [63.10.249.142] by ns.fundch.cl
  (SMTPD32-6.00) id A92614DC012A; Sun, 21 Jan 2001 22:21:26 -
0400
DATE: 21 Jan 01 8:24:27 PM
Message-ID: <N1msdrbJXNPfV4wg9>
Subject: Home Based Business for Grownups
To: undisclosed-recipients: ;
Sender: dev_null_sample_spam@example.com
Content-Type: text



                    THIS ENTERPRISE IS AWESOMELY FEATURED
                        IN SEPTEMBER 2000 MILLIONAIRE,
                           AUGUST 2000 TYCOONS AND
                      AUGUST 2000 ENTREPRENEUR Magazine.

====> Do you have a burning desire to change the quality of
your existing life?

====> Would you like to live the life that others only dream
about?

====> The fact is we have many people in our enterprise that
earn over 50k per month
      from the privacy of their own home and are retiring in
2-3 years.
```

====> Become Wealthy and having total freedom both personal and financial.

READ ON! READ ON! READ ON! READ ON! READ ON! READ ON! READ ON!!!

How would you like to:(LEGALLY & LAWFULLY)
1. KEEP MOST OF YOUR TAX DOLLARS
2. Drastically reduce personal, business and capital gains taxes?
3. Protect all assets from any form of seizure, liens, or judgments?
4. Create a six figure income every 4 months?
5. Restoring and preserving complete personal and financial privacy?
6. Create and amass personal wealth, multiply it and protect it?
7. Realize a 3 to 6 times greater returns on your money?
8. Legally make yourself and your assets completely judgment-proof,

SEIZURE-PROOOOF, LIEN-PROOOOOOF, DIVORCE-PROOOOOOF, ATTORNEY-PROOOOOOF, IRS-PROOOOOOF

((((((((((((((((((((BECOME COMPLETELY INSULATED))))))))))))))))))))

((((((((((((((((((((((((HELP PEOPLE DO THE SAME))))))))))))))))))))))))

===> Are you a thinker, and a person that believes they deserve to have the best in life?
===> Are you capable of recognizing a once in a lifetime opportunity when
it's looking right at you?
===> Countless others have missed their shot. Don't look back years later
and wish you made the move.

===> It's to my benefit to train you for success.
===> In fact, I'm so sure that I can do so,
I'm willing to put my money where my mouth is!
===> Upon accepting you as a member on my team, I will provide you with

```
     complete Professional Training as well as FRESH inquiring
LEADS to put
     you immediately on the road to success.

If you are skeptical that's OK but don't let that stop you
from getting all the information you need.

     DROP THE MOUSE=====>  AND CALL 800-320-9895 x2068
<======= DROP THE MOUSE AND CALL
************************************800-320-9895
x2068**************************************

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
~ ~
Your E-mail Address Removal/Deletion Instructions:

We comply with proposed federal legislation regarding
unsolicited
commercial e-mail by providing you with a method for your e-
mail address
to be permanently removed from our database and any future
mailings from
our company.

To remove your address, please send an e-mail message with the
word REMOVE
in the subject line to: maillistdrop@post.com

If you do not type the word REMOVE in the subject line, your
request to
be removed will not be processed.
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
~ ~




--DF12A2F403.1051032963/example.com--

================================ Send sample non-spam message

smtp: root: 1 /var/temp/amavisd-new-20030314/test-messages>
mail tester < sample-nonspam.txt
smtp: root: 1 /var/temp/amavisd-new-20030314/test-messages>
====================== Logged message
```

```
Apr 22 13:44:57 smtp postfix/pickup[19470]: [ID 197553
mail.info] 3B7F12F403: uid=0 from=<root>
Apr 22 13:44:57 smtp postfix/cleanup[19516]: [ID 197553
mail.info] 3B7F12F403: message-
id=<v0421010eb70653b14e06@[208.192.102.193]>
Apr 22 13:44:57 smtp postfix/qmgr[19471]: [ID 197553
mail.info] 3B7F12F403: from=<root@example.com>, size=6708,
nrcpt=1 (queue active)
Apr 22 13:44:57 smtp amavis[19332]: [ID 458739 mail.info]
(19332-02) ESMTP:10024 /var/amavis/amavis-20030422T133530-
19332: <root@example.com> -> <tester@example.com> Received:
SIZE=6708 from example.com ([127.0.0.1]) by localhost (smtp
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 19332-02
for <tester@example.com>; Tue, 22 Apr 2003 13:44:57 -0400
(EDT)
Apr 22 13:44:57 smtp amavis[19332]: [ID 924006 mail.info]
(19332-02) body hash: 1ef54f63ec20de7247b365383f010019
Apr 22 13:44:57 smtp amavis[19332]: [ID 649257 mail.info]
(19332-02) Checking: <root@example.com> ->
<tester@example.com>
Apr 22 13:44:58 smtp amavis[19332]: [ID 595869 mail.info]
(19332-02) Using Sophos Anti Virus (sweep):
/usr/local/bin/sweep -nb -f -all -rec -ss -sc -archive
/var/amavis/amavis-20030422T133530-19332/parts
Apr 22 13:45:15 smtp amavis[19332]: [ID 850439 mail.info]
(19332-02) run_av: /usr/local/bin/sweep status=0 (0 Illegal
seek),
Apr 22 13:45:21 smtp amavis[19332]: [ID 210509 mail.info]
(19332-02) spam_scan: hits=-6.4 tests=PGP_SIGNATURE
Apr 22 13:45:21 smtp amavis[19332]: [ID 749459 mail.info]
(19332-02) FWD via SMTP: [127.0.0.1:10025] <root@example.com>
-> <tester@example.com>
Apr 22 13:45:21 smtp postfix/smtpd[19522]: [ID 197553
mail.info] connect from localhost[127.0.0.1]
Apr 22 13:45:21 smtp postfix/smtpd[19522]: [ID 197553
mail.info] C313E2F401: client=localhost[127.0.0.1]
Apr 22 13:45:22 smtp postfix/cleanup[19516]: [ID 197553
mail.info] C313E2F401: message-
id=<v0421010eb70653b14e06@[208.192.102.193]>
Apr 22 13:45:22 smtp postfix/smtpd[19522]: [ID 197553
mail.info] disconnect from localhost[127.0.0.1]
Apr 22 13:45:22 smtp postfix/qmgr[19471]: [ID 197553
mail.info] C313E2F401: from=<root@example.com>, size=7109,
nrcpt=1 (queue active)
```

```
Apr 22 13:45:22 smtp amavis[19332]: [ID 164176 mail.info]
(19332-02) Passed, <root@example.com> -> <tester@example.com>,
Message-ID: <v0421010eb70653b14e06@[208.192.102.193]>
Apr 22 13:45:22 smtp postfix/local[19523]: [ID 197553
mail.info] C313E2F401: to=<tester@example.com>, relay=local,
delay=1, status=sent (mailbox)
Apr 22 13:45:22 smtp amavis[19332]: [ID 221298 mail.info]
(19332-02) TIMING [total 24670 ms] - SMTP EHLO: 19 (0%), SMTP
pre-MAIL: 5 (0%), SMTP pre-DATA-flush: 48 (0%), SMTP DATA: 98
(0%), body hash: 12 (0%), mime_decode: 315 (1%), get-file-
type: 170 (1%), decompose_part: 174 (1%), get-file-type: 145
(1%), decompose_part: 12 (0%), parts: 1 (0%), AV-scan-1: 16825
(68%), SA msg read: 48 (0%), SA parse: 34 (0%), SA check: 5878
(24%), fwd-connect: 229 (1%), fwd-mail-from: 90 (0%), fwd-
rcpt-to: 22 (0%), write-header: 96 (0%), fwd-data: 84 (0%),
fwd-rundown: 63 (0%), unlink-2-files: 299 (1%), rundown: 4
(0%)
Apr 22 13:45:22 smtp postfix/smtp[19518]: [ID 197553
mail.info] 3B7F12F403: to=<tester@example.com>,
orig_to=<tester>, relay=127.0.0.1[127.0.0.1], delay=25,
status=sent (250 2.6.0 Ok, id=19332-02, from MTA: 250 Ok:
queued as C313E2F401)

========================= Received message

smtp: tester: 1 /export/home/tester> mail
From root@example.com  Tue Apr 22 13:45:22 2003
Delivered-To: tester@example.com
Delivered-To: foo@foo.com
Message-Id: <v0421010eb70653b14e06@[208.192.102.193]>
Date: Fri, 20 Apr 2001 16:59:58 -0400
To: tbtf@world.std.com
From: Keith Dawson <dawson@world.std.com>
Subject: TBTF ping for 2001-04-20: Reviving

-----BEGIN PGP SIGNED MESSAGE-----

TBTF ping for 2001-04-20: Reviving

    T a s t y  B i t s  f r o m  t h e  T e c h n o l o g
y  F r o n t

    Timely news of the bellwethers in computer and
communications
    technology that will affect electronic commerce -- since
1994
```

Your Host: Keith Dawson

ISSN: 1524-9948

This issue: < http://tbtf.com/archive/2001-04-20.html >

To comment on this issue, please use this forum at Quick Topic:
< http://www.quicktopic.com/tbtf/H/kQGJR2TXL6H >

Q u o t e O f T h e M o m e n t

Even organizations that promise "privacy for their customers" rarely
if ever promise "continued privacy for their former customers..."
Once you cancel your account with any business, their promises of
keeping the information about their customers private no longer
apply... you're not a customer any longer.

This is in the large category of business behaviors that individuals
would consider immoral and deceptive -- and businesses know are not
illegal.

-- "_ankh," writing on the XNStalk mailing list

..TBTF's long hiatus is drawing to a close

Hail subscribers to the TBTF mailing list. Some 2,000 [1] of you
have signed up since the last issue [2] was mailed on 2000-07-20.
This brief note is the first of several I will send to this list to

excise the dead addresses prior to resuming regular publication.

While you time the contractions of the newsletter's rebirth, I invite you to read the TBTF Log [3] and sign up for its separate free subscription. Send "subscribe" (no quotes) with any subject to tbtf-log-request@tbtf.com . I mail out collected Log items on Sundays.

If you need to stay more immediately on top of breaking stories, pick up the TBTF Log's syndication file [4] or read an aggregator that does. Examples are Slashdot's Cheesy Portal [5], Userland [6], and Sitescooper [7]. If your news obsession runs even deeper and you own an SMS-capable cell phone or PDA, sign up on TBTF's WebWirelessNow portal [8]. A free call will bring you the latest TBTF Log headline, Jargon Scout [9] find, or Siliconium [10].

Two new columnists have bloomed on TBTF since last summer: Ted Byfield's roving_reporter [11] and Gary Stock's UnBlinking [12]. Lately Byfield has been writing in unmatched depth about ICANN, but the roving_reporter nym's roots are in commentary at the intersection of technology and culture. Stock's UnBlinking latches onto topical subjects and pursues them to the ends of the Net. These writers' voices are compelling and utterly distinctive.

[1] http://tbtf.com/growth.html
[2] http://tbtf.com/archive/2000-07-20.html
[3] http://tbtf.com/blog/
[4] http://tbtf.com/tbtf.rdf
[5] http://www.slashdot.org/cheesyportal.shtml

[6] http://my.userland.com/
[7] http://www.sitescooper.org/
[8] http://tbtf.com/pull-wwn/
[9] http://tbtf.com/jargon-scout.html
[10] http://tbtf.com/siliconia.html
[11] http://tbtf.com/roving_reporter/
[12] http://tbtf.com/unblinking/

S o u r c e s

> For a complete list of TBTF's email and Web sources, see
http://tbtf.com/sources.html .

B e n e f a c t o r s

TBTF is free. If you get value from this publication, please visit
the TBTF Benefactors page < http://tbtf.com/the-benefactors.html >
and consider contributing to its upkeep.

TBTF home and archive at http://tbtf.com/ . To unsubscribe send
the message "unsubscribe" to tbtf-request@tbtf.com. TBTF is Copy-

---

Keith Dawson dawson@world.std.com
Layer of ash separates morning and evening milk.

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.2 for non-commercial use
<http://www.pgp.com>

```
iQCVAwUBOuCi3WAMawgf2iXRAQHeAQQA3YSePSQ0XzdHZUVskFDkTfpE9XS4fH
Qs
WaT6a8qLZK9PdNcoz3zggM/Jnjdx6CJqNzxPEtxk9B2DoGll/C/60HWNPN+Vuj
Du
Xav65S0P+Px4knaQcCIeCamQJ7uGcsw+CqMpNbxWYaTYmjAfkbKH1EuLC2VRwd
mD
wQmwrDp70v8=
=8hLB
-----END PGP SIGNATURE-----

?

Send sample virus file:

# > mail tester <sample-virus-simple.txt

Logged message in the mail.log file:

Apr 22 13:49:02 smtp postfix/pickup[19470]: [ID 197553
mail.info] 76EB82F403: uid=0 from=<root>
Apr 22 13:49:02 smtp postfix/cleanup[19542]: [ID 197553
mail.info] 76EB82F403: message-
id=<20030422174902.76EB82F403@example.com>
Apr 22 13:49:02 smtp postfix/qmgr[19471]: [ID 197553
mail.info] 76EB82F403: from=<root@example.com>, size=424,
nrcpt=1 (queue active)
Apr 22 13:49:03 smtp amavis[19333]: [ID 779969 mail.info]
(19333-03) ESMTP:10024 /var/amavis/amavis-20030422T133430-
19333: <root@example.com> -> <tester@example.com> Received:
SIZE=424 from example.com ([127.0.0.1]) by localhost (smtp
[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 19333-03
for <tester@example.com>; Tue, 22 Apr 2003 13:49:03 -0400
(EDT)
Apr 22 13:49:03 smtp amavis[19333]: [ID 966583 mail.info]
(19333-03) body hash: aa991d6e29bf8eb4c1b56c599dffce0a
Apr 22 13:49:03 smtp amavis[19333]: [ID 843775 mail.info]
(19333-03) Checking: <root@example.com> ->
<tester@example.com>
Apr 22 13:49:03 smtp amavis[19333]: [ID 663673 mail.info]
(19333-03) Using Sophos Anti Virus (sweep):
/usr/local/bin/sweep -nb -f -all -rec -ss -sc -archive
/var/amavis/amavis-20030422T133430-19333/parts
Apr 22 13:49:20 smtp amavis[19333]: [ID 557513 mail.info]
(19333-03) run_av: /usr/local/bin/sweep status=3 (768 ),>>>
```

```
Virus 'EICAR-AV-Test' found in file /var/amavis/amavis-
20030422T133430-19333/parts/part-00001
Apr 22 13:49:20 smtp amavis[19333]: [ID 862314 mail.info]
(19333-03) local delivery: <root@example.com> -> <virus-
quarantine>, mbx=/var/virusmails/virus-20030422-134920-19333-
03
Apr 22 13:49:20 smtp amavis[19333]: [ID 750566 mail.info]
(19333-03) SEND via SMTP: [127.0.0.1:10025]
<virusalert@example.com> -> <virusalert@example.com>
Apr 22 13:49:20 smtp postfix/smtpd[19547]: [ID 197553
mail.info] connect from localhost[127.0.0.1]
Apr 22 13:49:21 smtp postfix/smtpd[19547]: [ID 197553
mail.info] 101872F401: client=localhost[127.0.0.1]
Apr 22 13:49:21 smtp postfix/cleanup[19542]: [ID 197553
mail.info] 101872F401: message-id=<VA19333-03@smtp>
Apr 22 13:49:21 smtp postfix/smtpd[19547]: [ID 197553
mail.info] disconnect from localhost[127.0.0.1]
Apr 22 13:49:21 smtp postfix/qmgr[19471]: [ID 197553
mail.info] 101872F401: from=<virusalert@example.com>,
size=1678, nrcpt=1 (queue active)
Apr 22 13:49:21 smtp postfix/local[19548]: [ID 197553
mail.info] 101872F401: to=<virusalert@example.com>,
relay=local, delay=0, status=bounced (unknown user:
"virusalert")
Apr 22 13:49:21 smtp postfix/cleanup[19542]: [ID 197553
mail.info] D63322F404: message-
id=<20030422174921.D63322F404@example.com>
Apr 22 13:49:22 smtp postfix/qmgr[19471]: [ID 197553
mail.info] D63322F404: from=<>, size=3208, nrcpt=1 (queue
active)
Apr 22 13:49:22 smtp postfix/local[19548]: [ID 197553
mail.info] D63322F404: to=<virusalert@example.com>,
relay=local, delay=1, status=bounced (unknown user:
"virusalert")
Apr 22 13:49:22 smtp amavis[19333]: [ID 857317 mail.info]
(19333-03) SEND via SMTP: [127.0.0.1:10025] <> ->
<root@example.com>
Apr 22 13:49:22 smtp postfix/smtpd[19547]: [ID 197553
mail.info] connect from localhost[127.0.0.1]
Apr 22 13:49:22 smtp postfix/smtpd[19547]: [ID 197553
mail.info] 66D852F401: client=localhost[127.0.0.1]
Apr 22 13:49:22 smtp postfix/cleanup[19542]: [ID 197553
mail.info] 66D852F401: message-id=<VS19333-03@smtp>
Apr 22 13:49:22 smtp postfix/smtpd[19547]: [ID 197553
mail.info] disconnect from localhost[127.0.0.1]
```

```
Apr 22 13:49:22 smtp postfix/qmgr[19471]: [ID 197553
mail.info] 66D852F401: from=<>, size=2698, nrcpt=1 (queue
active)
Apr 22 13:49:22 smtp amavis[19333]: [ID 900759 mail.info]
(19333-03) INFECTED (EICAR-AV-Test), <root@example.com> ->
<tester@example.com>, quarantine virus-20030422-134920-19333-
03, Message-ID: <20030422174902.76EB82F403@example.com>
Apr 22 13:49:23 smtp postfix/local[19548]: [ID 197553
mail.info] 66D852F401: to=<root@example.com>, relay=local,
delay=1, status=sent (mailbox)
Apr 22 13:49:23 smtp amavis[19333]: [ID 940318 mail.info]
(19333-03) TIMING [total 20088 ms] - SMTP EHLO: 20 (0%), SMTP
pre-MAIL: 6 (0%), SMTP pre-DATA-flush: 51 (0%), SMTP DATA: 82
(0%), body hash: 6 (0%), mime_decode: 210 (1%), get-file-type:
158 (1%), decompose_part: 17 (0%), parts: 1 (0%), AV-scan-1:
16850 (84%), write-header: 128 (1%), save-to-local-mailbox: 4
(0%), fwd-connect: 535 (3%), fwd-mail-from: 94 (0%), fwd-rcpt-
to: 25 (0%), write-header: 61 (0%), fwd-data: 122 (1%), fwd-
rundown: 115 (1%), fwd-connect: 944 (5%), fwd-mail-from: 99
(0%), fwd-rcpt-to: 18 (0%), write-header: 56 (0%), fwd-data:
222 (1%), fwd-rundown: 115 (1%), unlink-1-files: 146 (1%),
rundown: 4 (0%)
Apr 22 13:49:23 smtp postfix/smtp[19544]: [ID 197553
mail.info] 76EB82F403: to=<tester@example.com>,
orig_to=<tester>, relay=127.0.0.1[127.0.0.1], delay=21,
status=sent (250 2.5.0 Ok, but 1 BOUNCE)

Returned message:

From MAILER-DAEMON  Tue Apr 22 13:49:22 2003
Delivered-To: root@example.com
Subject: VIRUS (EICAR-AV-Test) IN YOUR MAIL
Message-Id: <VS19333-03@smtp>
From: amavisd-new <postmaster@example.com>
To: <root@example.com>
Date: Tue, 22 Apr 2003 13:49:21 -0400 (EDT)

This is a multi-part message in MIME format...

------------=_1051033762-19333-1
Content-Type: text/plain; charset="iso-8859-1"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit

VIRUS ALERT
```

```
Our virus checker found
    virus: EICAR-AV-Test
in your email to the following recipient:
-> tester@example.com

Delivery of the email was stopped!

Please check your system for viruses,
or ask your system administrator to do so.

For your reference, here are headers from your email:
-------------------------- BEGIN HEADERS ----------------------
-------
Received: by example.com (Postfix, from userid 0)
        id 76EB82F403; Tue, 22 Apr 2003 13:49:02 -0400 (EDT)
From: virus-tester@example.com
To: undisclosed-recipients: ;
Subject: amavisd test - simple - virus scanner test pattern
Content-Type: text
Message-Id: <20030422174902.76EB82F403@example.com>
Date: Tue, 22 Apr 2003 13:49:02 -0400 (EDT)
-------------------------- END HEADERS ----------------------
-------

------------=_1051033762-19333-1
Content-Type: message/delivery-status
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
Content-Description: Delivery error report

Reporting-MTA: dns; smtp
Received-From-MTA: smtp; example.com ([127.0.0.1])
Arrival-Date: Tue, 22 Apr 2003 13:49:03 -0400 (EDT)

Final-Recipient: rfc822; tester@example.com
Action: failed
Status: 5.7.1
Diagnostic-Code: smtp; 550 5.7.1 Message content rejected,
id=19333-03 - VIRUS: EICAR-AV-Test
Last-Attempt-Date: Tue, 22 Apr 2003 13:49:21 -0400 (EDT)

------------=_1051033762-19333-1
Content-Type: text/rfc822-headers
Content-Disposition: inline
Content-Transfer-Encoding: 7bit
Content-Description: Undelivered-message headers
```

```
 Received: by example.com (Postfix, from userid 0)
         id 76EB82F403; Tue, 22 Apr 2003 13:49:02 -0400 (EDT)
 From: virus-tester@example.com
 To: undisclosed-recipients: ;
 Subject: amavisd test - simple - virus scanner test pattern
 Content-Type: text
 Message-Id: <20030422174902.76EB82F403@example.com>
 Date: Tue, 22 Apr 2003 13:49:02 -0400 (EDT)

 ------------=_1051033762-19333-1--
```

Send a test message with virus content to test the capability of the virus filter:

```
# > mail test@example <<!
> X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
> !
```

and the following is the virus alert message which send by virus filter software after the virus detected by content filter on smtp server.

```
From virusalert@example.com  Mon Apr  7 01:00:05 2003
Delivered-To: root@example.com
Date: Mon,  7 Apr 2003 01:00:04 -0400 (EDT)
From: virusalert@example.com
Subject: VIRUS (EICAR-AV-Test) IN MAIL TO YOU (from
<root@example.com>)
To: undisclosed-recipients: ;
Message-Id: <VR00584-10@smtp>

VIRUS ALERT

Our content checker found
    EICAR-AV-Test
virus in an email to you from:

   root@example.com

The message has been quarantined as:
   /var/virusmails/virus-20030407-010004-00584-10

Please contact your system administrator for details.
```

The result shows that the virus was identified and the message has been quarantined in the /var/virusmails directory. For more information, you can visit http://www.sophos.com/virusinfo/analyses/eicar.html.

Backup

The weekly backup will be performed on this smtp server based on the company policy.

Conclusion

Since SPAM is growing, and it causing serious problem. The email system administrators have to find an effective way to stop SPAM by filtering the SPAM and virus email messages to prevent unsolicited bulk email and virus emails enter your mail server and stop transmit these unwanted emails to the end user in your organization.

References

1) Bernstein, D. J., Data structures
Software, cdb: create and read constant databases,
http://cr.yp.to/cdb.html

2) E. V.,Eicar, The Anti-Virus test file, 2003
http://www.eicar.org/anti_virus_test_file.htm

3) Henderson, Scott, SPAMFILTER EMAIL RELAY SERVER "HOWTO" / GUIDE, Last revised: 2003-04-24.
http://www.geocities.com/scottlhenderson/spamfilter.html

4) Krim, Jonathan
Washington Post Staff Writer
Spam's Cost To Business Escalates
Bulk E-Mail Threatens Communication Arteries,
2003-03-13; Page A01
http://www.washingtonpost.com/wp-dyn/articles/A17754-2003Mar12.html

5) Martinec, Mark, system manager
Networking Infrastructure Centre,
J. Stefan Institute, Last updated: 2003-04-24
http://www.ijs.si/software/amavisd/

6) Noordergraaf, Alex, The Solaris Toolkit – Installation, Configuration and Usage Guide". June 2001
http://www.sun.com/solutions/blueprints/0601/jass_conf_install-v03.pdf

7) Venema, Dr. W.Z.
IBM T.J. Watson Research Center
http://www.postfix.org/ 2003-04-25

8) Venema, Wietse, TCP Wrapper installation README file, 1997-03-21

9) CERT Home Page, Page revised: 2000-03-01
http://www.cert.org/security-improvement/implementations/i041.07.html

10) Openssh home page, 1999-2002 OpenBSD.
index.html,v 1.171 2003-04-18,
http://www.openssh.org/

11) Openssl home page, 2003-04-25, http://www.openssl.org/

12) Postfix Web page, 2003-04-25,
http://www.postfix.org/basic.html
http://www.postfix.org/uce.html

13) Sophos company home page, 2003-04-25
http://www.sophos.com/companyinfo/

14) Sophos Company Web page, EICAR-AV-Test, 3002-04-25
http://www.sophos.com/virusinfo/analyses/eicar.html

15) SUN Micro System, Solaris Security Toolkit (JASS)
http://wwws.sun.com/software/security/jass/

16) SUN Micro Systemss, Web Page, 2003-04-25,
http://wwws.sun.com/software/security/jass/