建置防範病毒信及廣告信之郵件伺服器

Ⅰ. 實驗目的

隨著寬頻網際網路的普及，以及架設郵件伺服器日趨簡易，生活中電子郵件的使用率已經越來越高，相對的利用電子郵件發送廣告信的軟體也越來越多，粗估垃圾郵件約佔一般信箱中 1/2 的郵件量。另外病毒信也是不容忽視的，當公司有一員工中毒，病毒利用電腦發送病毒信件來感染其他使用者，在短時間內就可以造成巨大的損失，要如何讓信箱不要接收這些信件總是讓網管人員非常頭痛。事實上，阻擋病毒郵件與廣告郵件可以很簡單且便宜。本實驗主要目的有二：

1. 訓練同學熟悉 FreeBSD 操作環境，利用 FreeBSD 建構無毒無廣告之郵件伺服器。
2. 在實際操作中了解郵件寄送傳遞過程與郵件掃描之原理。

操作本實驗的同學應具基本網路常識、了解電子郵件傳遞之原理、具有 Windows 作業系統操作能力，與基本使用 FreeBSD 的經驗。

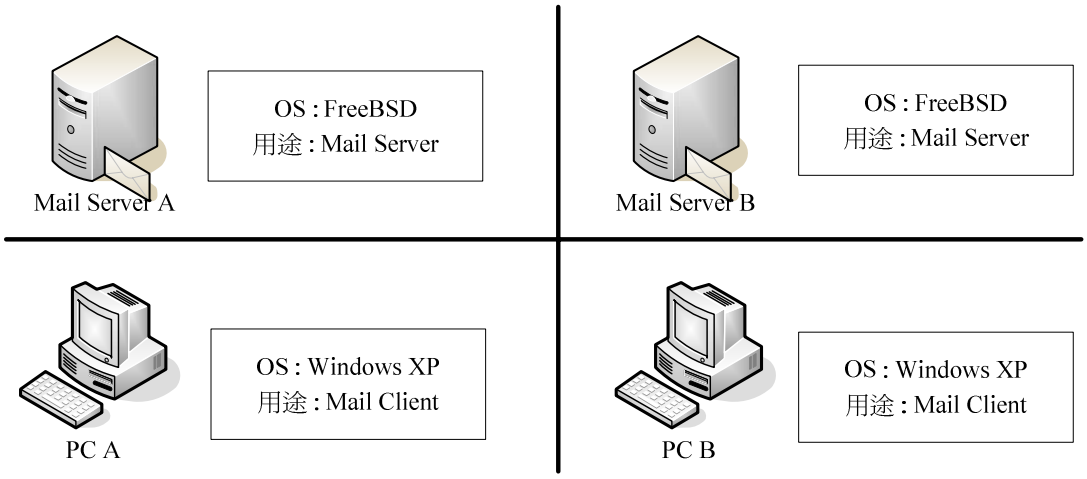
Ⅱ. 實驗設備

硬體：

項目	數量	備註
個人電腦	4	2 台 PCs 安裝 FreeBSD 2 台 PCs 安裝 Windows XP
Adaptor	4	NE2000 compatible
網路線	4	連接 PC
Switching HUB	1	連接 Server

軟體：

軟體名稱	數量	軟體種類	描述
FreeBSD 6.1	1	OS	Freeware 可由網路上下載
Windows XP	1	OS	Microsoft 公司出版
Postfix	1	Mail Server	由 ports 安裝
Amavisd-new	1	Interface between MTA and content checkers	由 ports 安裝
ClamAV	1	Anti-Virus	由 ports 安裝
SpamAssassin	1	Anti-Spam	由 ports 安裝
OutlookExpress	1	Mail Client	WindowsXP 內建

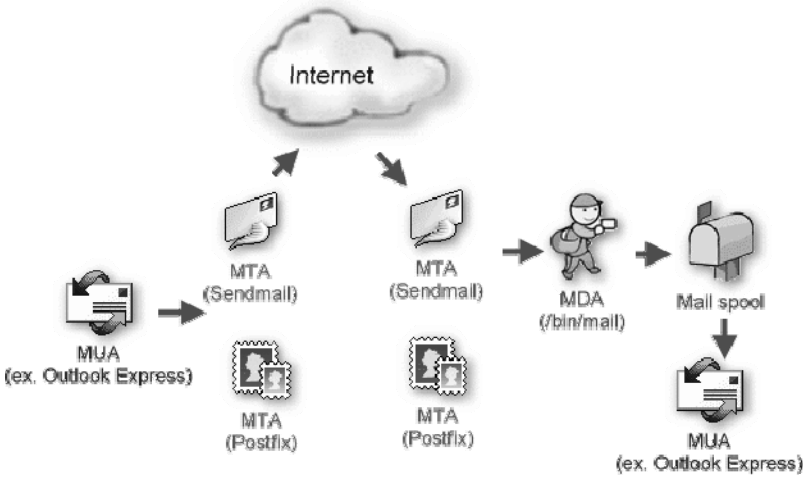


圖一、 實驗環境。

Ⅲ. 背景資料

如何防範廣告與病毒郵件的攻擊對企業來說非常重要，唯有有效的控制才能降低廣告與病毒郵件對企業的傷害。廣告與病毒郵件與一般的電子郵件並沒有什麼不同，一般來說過濾的方式不外乎兩種：一種爲根據郵件伺服器的設定，直接拒收該垃圾郵件；另一種爲將郵件收下後在利用軟體掃描過濾。此兩種方式各有優劣，前者可以直接拒收信件降低伺服器的負擔，不過也很容易將正常的用戶阻擋在外。後者雖然需要將郵件接收下來後再進行掃描過濾，卻可以降低誤擋的情況，再由伺服器對郵件分析並且加上標示，最後讓使用者或是系統決定是否刪除判定的問題郵件，似乎是目前非商業性質的郵件過濾最好的方式。

電子郵件工作原理如下：



圖二、 電子郵件工作原理。

- **Mail User Agent (MUA)：郵件使用者代理人**
  使用者平常所使用的信件閱讀與撰寫的程式，接收使用者的命令提供一個方便的介面來收發信件。
- **Mail Transfer Agent (MTA)：郵件轉送代理人**
  真正負責在 Internet 上轉送信件的程式，FreeBSD 內建的是 Sendmail，但是 Sendmail 有較多的安全性及較難設定的問題，因此我們這邊採用 Postfix；MTA 在收到 MUA 傳來的信件後，會根據信件的目的地做一些位址判斷的工作，然後將信件送往目的地。
  有時候信件不會直接送往目的地的主機，例如目的地主機故障時候，這時候會先送往其他主機的 MTA，等目的地主機正常後，再轉送過去。MTA 除了接收 MUA 送過來的信件外也叫接收其他 MTA 傳送過來的信件，並幫忙把信件送往目的主機，這種動作稱爲〈**Relay**〉。
- **Mail Deliver Agent (MDA)：郵件遞送代理人**
  MTA 在收到一封信件後，會先判斷該信件的目的地是不是自己，如果不是則會繼續幫忙轉送，如果是自己 MTA 則會把信件交給 MDA 來處理，MDA 會真正的把信件送到主機上收件人的信箱中。

Amavisd-new

爲了能該 Postfix 與過濾及病毒掃瞄軟體協同運作，我們這邊的作法是將 Postfix 接收的郵件先轉送到 10024 埠(預設值)，待 Amavisd-new 呼叫掃瞄軟體檢查完後再轉送到 Postfix 的 10025 埠，接下來我們簡單比較未啓動掃瞄軟體與啓動掃瞄軟體的郵件處理流程的差異。

在系統未安裝任何郵件過濾的軟體之前，郵件的處理流程如下：
Incoming Mail → Postfix(MTA) → MDA → User Mail Box
在系統啓動過濾機制後，郵件的處理流程如下：
Incoming Mail → Postfix (MTA) Incoming Queue(*:25) → Amavisd-new(127.0.0.1:10024) → Postfix (MTA) Outgoing Queue (127.0.0.1:10025) → MDA → User Mail Box

Anti-Spam

廣告郵件的過濾技術我們可以參考表 1，而在本實驗中我們利用 SpamAssassin 來過濾廣告郵件，這也是一套經由管理者設定一些郵件檢查的規則來過濾郵件。不過 SpamAssassin 並不是經由設定的規則來直接判定該郵件是否爲廣告郵件，而是經由規則來產生相對應的分數，最後再經由加權來判定該郵件是否爲廣告郵件。另外 SpamAssassin 比較特殊的是可以經由統計分析的方式，自動地藉由所接收到的郵件來學習並調整郵件評分方式。另外 SpamAssassin 也可以對外部的郵件資料庫作查詢來決定該郵件是否爲廣告郵件，不過本實驗並不對此部分作介紹，有興趣的讀者可以自行研究。

SpamAssassin 利用統計分析的方式爲利用 Bayes 方法去分析，Bayes 分析方法大略介紹如下：

首先，需要大量的廣告郵件與非廣告郵件，接下來取出郵件主題與內容中的 token，計算該 token 出現的次數，然後將非廣告郵件放進 hashtable_good、廣告郵件放進 hashtable_bad，並經由公式計算 token 出現的機率，使得之後的郵件可以透過 Bayes 去比對目前的資料庫加以分析，決定該郵件的分數，最後再以該分數判斷郵件是否爲廣告信，並且把該封信件的分析加入資料庫。

需求	方法	技術
Restrict illegal sender	藉由過濾郵件的發送者來標示該信件爲廣告郵件	Header Filter
Restrict illegal keyword	藉由過濾郵件的特定關鍵字來標示該信件爲廣告郵件	Content Filter
阻擋特定的圖片或是多媒體檔案	藉由過濾郵件的 MIME Header 來標示該信件爲廣告郵件	MIME headers Filter

表一、 廣告郵件之特性與其過濾技術。

另外，目前常見檔廣告信的方式還有使用 Greylist，其原理是接收信件的伺服器會依據來源 IP、寄件者與收件者先判斷 SMTP 的連線是否爲第一次，若是第一次則先應對方 450 Server busy. Try again later.的訊息，並且拒收信件，並等到第二次連線時，再收下來，如此一來，每一封信件都必須經由兩次以上的投遞，才會順利收下。但是一般廣告信寄發通常都爲了效率，而採取寄後不理的策略，因此藉由此方法能夠擋下部分的廣告信。在 Postfix 也可以使用 greylist，有興趣的使用者可以連到此連結參考：
http://www.postfix.org/SMTPD_POLICY_README.html

Anti-Virus

本實驗中我們利用 ClamAV 來過濾病毒郵件，伺服器在接收到信件後，會經由 Amavisd-new 來呼叫 ClamAV，如同傳統的掃毒軟體，ClamAV 利用病毒定義檔來判斷該郵件是否有含病毒，而判別病毒郵件的方法可以參考表 2。若發現病毒則移除病毒或是直接刪除該郵件，並告知使用者與管理員該封郵件含有病毒。

良好的掃毒軟體必須定期更新病毒定義檔，來保持軟體的掃毒能力，本實驗中也會提及如何利用 ClamAV 所提供的程式來定期的向 ClamAV 官方網站更新病毒定義檔。

需求	方法	技術
掃描郵件附加檔案	藉由過濾郵件的附加檔案來隔離病毒	File Scan
掃描壓縮檔案	藉由過濾郵件的附加壓縮檔來避免病毒經由壓縮躲過掃描	Compressed File Scan
掃描郵件 Header 或是 Body	藉由過濾郵件的 MIME Header 或是內嵌的程式碼，	MIME headers Scan

	避免惡意的病毒通過	

表二、 病毒郵件之特性與其過濾技術。

SpamAssassin 與 ClamAV 爲 Open Source 軟體，可以在 UNIX 平台上輕鬆地與各種郵件伺服器軟體搭配運作，本實驗的操作環境是以 FreeBSD + Postfix + Amavisd-new + SpamAssassin + ClamAV 來完成。FreeBSD 因爲系統穩定，一些常用的伺服器端的軟體都維護地相當不錯，可以很容易安裝好所需要的軟體，使用者只需設定好軟體的設定。

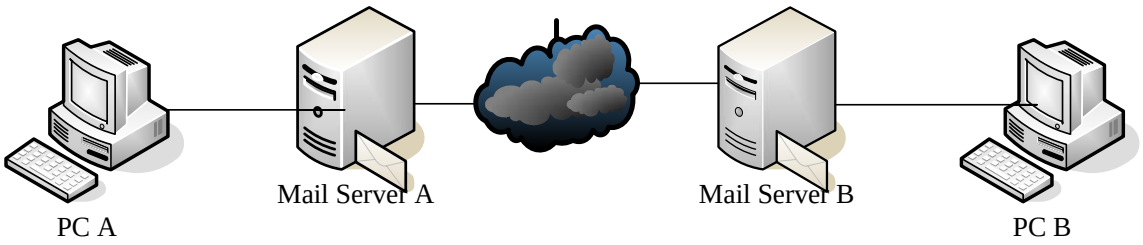
Ⅳ. 實驗方法

本實驗練習安裝與建置一個符合現實環境需求的 Anti-Spam/Anti-Virus 郵件伺服器，操作環境可在一個開放的環境下進行測試。利用 Mail Client (Outlook Express)與 Mail Server (Postfix)來模擬真實環境中電子郵件傳送的過程，再利用電子郵件伺服器所設定的過濾廣告病毒郵件來達到防堵廣告信與防毒的功能。

爲了模擬真實世界的環境，本實驗分成幾個階段：

第一階段：

模擬使用者經由未安裝防廣告與防毒的郵件寄送郵件，透過網路傳遞由另一台郵件伺服器所接收。安裝兩台 Server 與兩台 Client，並設定好 Server 與 Client，確定由 PC A 所寄發的郵件可以透過 Mail Server A 寄到 Mail Server B 上，PC B 可以從 Mail Server B 上接收郵件；反之 PC B 所寄送的郵件也可以根據這樣的路徑由 PC A 所接收到。在確定雙向都可以收發信後，接著就可以開始第二階段的實驗。



圖三、 第一階段之架構。

第二階段：

爲安裝與設定SpamAssassin與ClamAV，詳細請參考實驗步驟二。

第三階段：

爲測試所安裝的防堵廣告信件與防毒的過濾軟體是否正常工作。設定Mail Server B

的SpamAssassin將由PC A帳號寄送過來的郵件視爲廣告信件，由PC B接收信件並確定郵件標題有標上SPAM字眼；PC A再透過Mail Server A利用病毒範例檔寄送病毒信件給Mail Server B，PC A收取信件，確認是否有收到Server B退回的信件，說明該封信件帶有病毒。

V. 實驗步驟

在實驗開始之前，假設各位已經熟悉 Windows 的基本操作，並了解 Windows 下網路與郵件相關的設定，熟悉 Internet 架構與運作元理，以及了解各種郵件通訊協定的原理(例如：SMTP、POP3、IMAP)。

一、建置 Postfix 收發信平台：

Server 端爲安裝與設定 Postfix 使得 Client 可以正常收發信；Client 端則需要正確的設定收發信相關資訊。最後在雙方互相寄送信件，確定環境正常運作。

A. 先將 FreeBSD 的 port tree update 到最新的版本 (keyword => csup)
B. 從 port 安裝 Postfix，安裝時的選項都用預設的設定即可
C. 安裝 imap-uw (提供 pop3 與 imap 收信服務)
D. 設定/usr/local/etc/postfix/main.cf 相關設定，使 Postfix 可以正常運作
E. 修改/etc/rc.conf 將 Postfix 取代內建的 Sendmail (作法在安裝完 Postfix 後有說明)

二、安裝與設定 Amavisd-new

安裝 Amavisd-new 並設定 Postfix 將接收的郵件傳送給 Amavisd-new 作垃圾信及病毒檢查，最後再設定 Postfix 多聽 port 10025 接收 Amavisd-new 檢查完的信件。

A. 安裝與設定 Amavisd-new

由 port 安裝 Amavisd-new

```
# cd /usr/ports/security/amavisd-new
# make install
```

安裝選項都不要選

設定 Amavisd-new，修改/usr/local/etc/amavisd.conf

```
$mydomain = 'example.com'
$sa_tag_level_deflt    = 0.0;
```

另外在 Amavisd 判斷爲有夾帶病毒或是廣告信時，預設 Amavid 會將該郵件傳送給 virusalert 及 spam.police 這兩位使用者，因此若我們的主機上沒有這兩位使用者則必需更改以下設定：

```
$mailfrom_notify_admin    = "root\@$mydomain";
$mailfrom_notify_recip = " root \@$mydomain";
```

```
$mailfrom_notify_spamadmin = " root \@$mydomain";
```

設定開始自動啓動 Amavisd-new，在/etc/rc.conf 增加以下：

```
amavisd_enable="YES"
```

B. 設定 Postfix

設定 Postfix 將收到郵件轉送給 Amavisd-new，在/usr/local/etc/postfix/main.cf 最後多增加：

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

讓 Postfix 多聽 10025 port，增加以下內容至/usr/local/etc/postfix/master.conf：

```
smtp-amavis unix - - n - 2 smtp
   -o smtp_data_done_timeout=1200
   -o disable_dns_lookups=yes
127.0.0.1:10025 inet n - n - - smtpd
   -o content_filter=
   -o local_recipient_maps=
   -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
```

C. 重新啓動 Postfix 及 Amavisd-new

```
# /usr/local/etc/rc.d/postfix restart
# amavisd start
```

三、安裝與設定 SpamAssassin/ClamAV：

配合 Postfix 使其掃描由使用者經由 Mail Server 發送之郵件，或是由其他 Mail Server 所寄送過來之郵件。

A. 安裝與設定 SapmAssassin

從 Port 安裝 SpamAssassin

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin/
# make install
```

設定 /usr/local/etc/mail/spamassassin/local.cf，複製 local.cf.sample 至 local.cf 並

修改它：

```
# cd /usr/local/etc/mail/spamassassin
# cp local.cf.sample local.cf
# vim local.cf
```

設定開機自動執行，增加下行至/etc/rc.conf

```
spamd_enable="YES"
```

啓動 SpamAssassin

```
# /usr/local/etc/rc.d/sa-spamd.sh start
Starting spamd.
```

B. 安裝與設定 ClamAV

從 Port 安裝 ClamAV

```
# cd /usr/ports/security/clamav
# make install
```

安裝選項都不要選

/usr/local/etc/clamd.conf 及/usr/local/etc/freshclam.conf 使用內定的值即可，有興趣的同學可以自行參照檔案內的說明自行修改。

設定開機自動執行，在/etc/rc.conf 增加以下內容

```
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"
```

四、PC A 寄一封正常信件給 B：

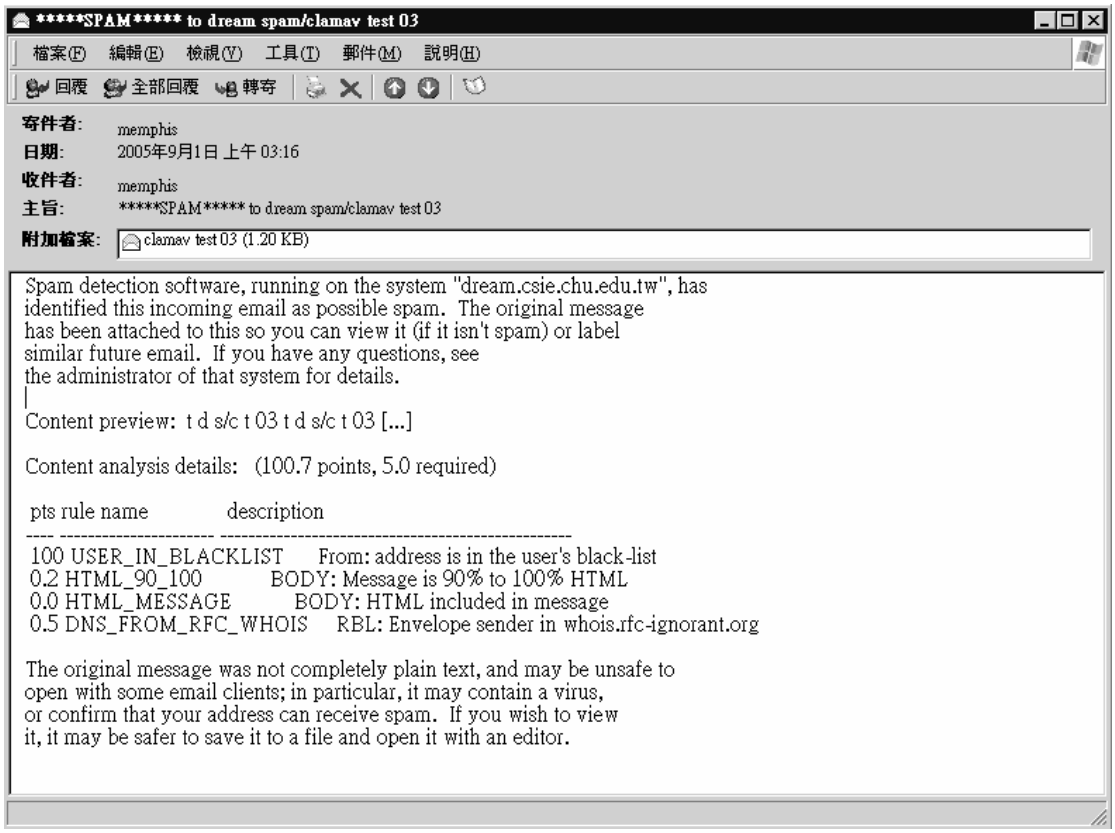
確定安裝 SpamAssassin/ClamAV 後並不影響正常信件的收發，在 mail header 可以發現以下資訊：

```
X-Virus-Scanned: amavisd-new at fcwu.no-ip.org
X-Spam-Status: No, score=0.852 tagged_above=0 required=6.31 tests=[AWL=0.373,
  DNS_FROM_RFC_ABUSE=0.479]
X-Spam-Score: 0.852
X-Spam-Level:
```

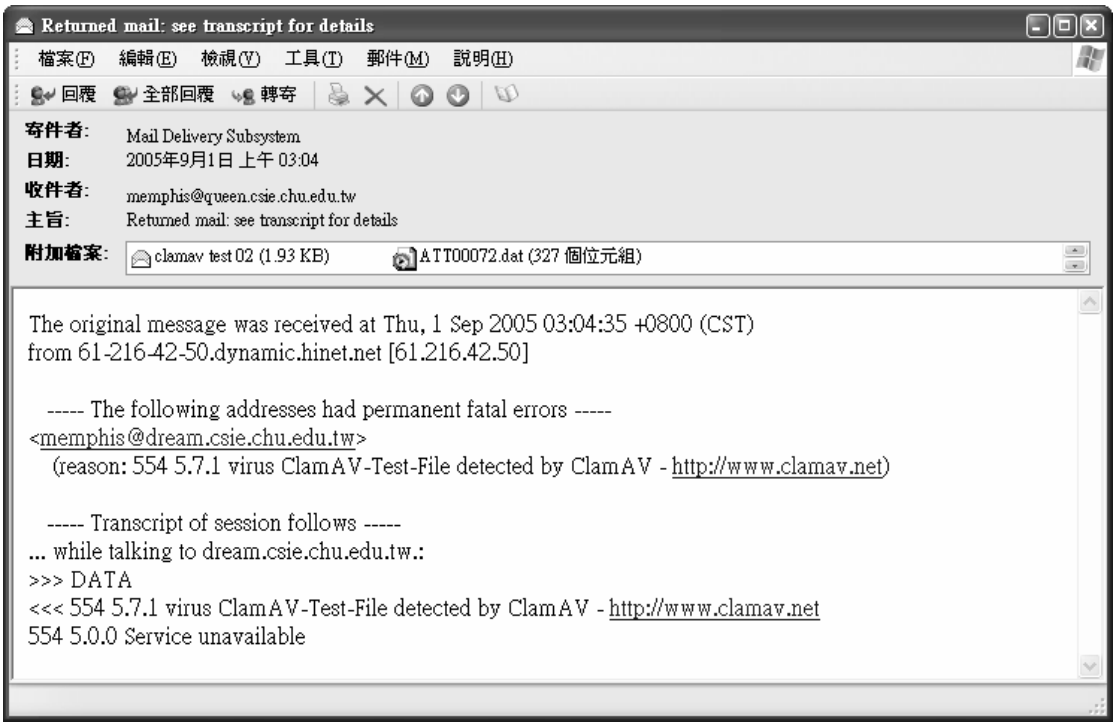
五、Server B 開啓過濾功能：

使用者利用 PC A 經由 Server A 將郵件寄往 Server B，PC A 分別寄一封廣告與病毒信件。以下附上範例畫面供同學參考。

廣告信(利用增加黑名單的方式來測試)



病毒信(PC A 所收到的回信)



最後同學們可以仔細觀察兩邊 Mail Server，以及由 PC B 發送信病毒信與廣告信，觀察兩邊 Mail Server 與由 PC A 發送有何不同。

VI. 實驗記錄

實驗紀錄一： 環境建置-各 Server and PC IP and Function

機器名稱	IP	Function
Mail Server A		
Mail Server B		
PC A		
PC B		

實驗紀錄二：Mail Server 啓動 SpamAssassin and ClamAV 的訊息

啓動情形	訊息描述
成功	
失敗	

實驗紀錄三：PC A 寄送正常信件給 PC B，Server A 與 Server B 的 log 與 PC B 所收到的正常信信件標題

項目	詳細內容
Server A log	
Server B log	
PC B mail header	

實驗紀錄四：PC A 寄送廣告信件給 PC B，Server A 與 Server B 的 log 與 PC B 所收到的廣告信信件標題

項目	詳細內容
Server A log	
Server B log	
PC B mail header	

實驗紀錄五：PC A 寄送病毒信件給 PC B，Server A 與 Server B 的 log 與 PC B 所收到的病毒信信件標題

項目	詳細內容

Server A log	
Server B log	
PC B mail header	

實驗紀錄六：將實驗紀錄三改爲由 PC B 寄送郵件給 PC A

項目	詳細內容
Server A log	
Server B log	
PC B mail header	

實驗紀錄七：將實驗紀錄四改爲由 PC B 寄送郵件給 PC A

項目	詳細內容
Server A log	
Server B log	
PC B mail header	

實驗紀錄八：將實驗紀錄五改爲由 PC B 寄送郵件給 PC A

項目	詳細內容
Server A log	
Server B log	
PC B mail header	

實驗紀錄十：在操作這個實驗的時候有哪些訊息讓你注意？

Filter 種類	Message
SpamAssassin	
ClamAV	

Ⅶ. 問題與討論

注意：請針對問題中每一項目回答，並避免引述「太」多資料。

一、SpamAssassin 的過濾規則有哪些? 試著比較其差異，以自己的方式敘述

二、SpamAssassin 可以略過某些郵件不掃描嗎？用如何的方式達成？
三、SpamAssassin 利用 bayes 分析出來的資料庫，套用在另一台 Mail Server 上是否可以有相同的效果，爲什麼？
四、ClamAV 是否可以掃描壓縮檔？若壓縮檔中有壓縮檔，是否依然可以正確的掃描出內含的病毒？
五、ClamAV 的病毒碼部分，若有新種類的病毒，ClamAV 是如何更新病毒碼？
六、若有商業性質的掃毒軟體，與免費的 ClamAV，該如何選擇與其原因？
七、若 ClamAV 掃描到帶有病毒的信件，是否可以留存備份於 Mail Server 上，需要如何達成此目的？
八、SpamAssassin 若採用 Bayes 分析來過濾郵件，Bayes 詳細的計算分數的過程爲何，試舉一範例說明之。

Ⅷ. 參考文獻

1. FreeBSD, http://www.freebsd.org/.
2. Sendmail, http://www.sendmail.org/.
3. The Apache SpamAssassin Project, http://spamassassin.apache.org/.
4. Clam AntiVirus, http://www.clamav.net/.
5. Unix Docs and Tools, http://networking.ringofsaturn.com/Unix/.
6. Postfix, http://www.postfix.org/.
7. 張傑生、唐瑤瑤、許凱平、陳啓煌、李秀惠、賴飛羆，“使用 Open Source 軟體進行 SPAM Mail 防制處理——以台灣大學電子郵件系統爲例”， http://antispam.ncu.edu.tw/paper/tanet2005-C52.pdf。
8. Postfix + Amavisd-new + SpamAssassin + ClamAV, http://freebsd.ntut.idv.tw/document/postfix_amavisd-new_spamassassin_clamav.html.