第十一單元

MailScanner 伺服器管理

1.實驗目的

提供可阻擋廣告信和病毒信件的安全郵件服務

2.實驗設備

- 安裝 Linux 系統之電腦
- Webmin(http://www.webmin.com)
- Sendmail(http://www.sendmail.org)
- MailScanner(http://www.sng.ecs.soton.ac.uk/mailscanner)

3.背景資料

網路時代到來，家家戶戶每個人都會上網，而且不是瀏覽網頁，就是收發 E-mail；雖然現在有很多免費的 E-mail 信箱，但是有二個問題非常嚴重：廣告信和病毒信。日前全世界的電腦才被一種叫做疾風的病毒所摧殘，損失相當慘重；然而，許多病毒除了靠檔案的傳輸來教唆散播之外，絕大部份的網路病毒都是透過 mail 來傳送，而一般使用者又對防毒、防駭的觀念缺乏，導致時常有資訊災難產生。為了解決這個不定時炸彈，許多廠商都提供了付費的防毒信箱機制，希望使用者不要因此而蒙受傷害。

MailScanner 已經是一個高度受尊重的開放性原始碼電子郵件的安全系統，使用者非常的廣泛，新的版本更增進了它的效能及穩定性，而且每天處理超過五億封的郵件、移除二百萬封的病毒信件及辨識七百五十萬封 spam 訊息；MailScanner 已經被使用在超過二萬個站台，保護著政府部門、商業機構及學校單位，它已經變成了許多 ISP 及使用者在過濾病毒信件及廣告信時的必要工具。MailScanner 可以偵測所有已知的信件病毒、spam 及任何有攻擊行動的非善意訊息郵件，它並不是一個單一的 virus scanner，而是一個可以和超過十四種 virus scanner 搭配的套件，可以允許任何使用者去搭配一個最適合的 scanner 核心來使用，例如本章介紹的 sophos，它主要的目的在於增加網路安全，所以它扮演的是一個安全的服務，雖然 MailScanner 是一個頂尖的套件，但是並不商業化，而且一直遵守著 GNU 的公用版權來發展。

SOPHOS 是在歐洲最大的防毒軟體開發者，在全球防毒市場中排名行前五大，分公司與經銷商以遍及全球 120 多個國家，SOPHOS 的技術團隊都通過專業工程師認證，能提供完整的防毒保護技術與售後服務，每個月還會在各種平台上測試 Sophos Anti-virus（SAV）對各種病毒的防護能力，提供真正跨平台的保護，並開放溝通管道給技術性惡護，讓使用者可預先查看並受到保護。

4.實驗方法

下載 MailScanner 及 Sophos 主程式

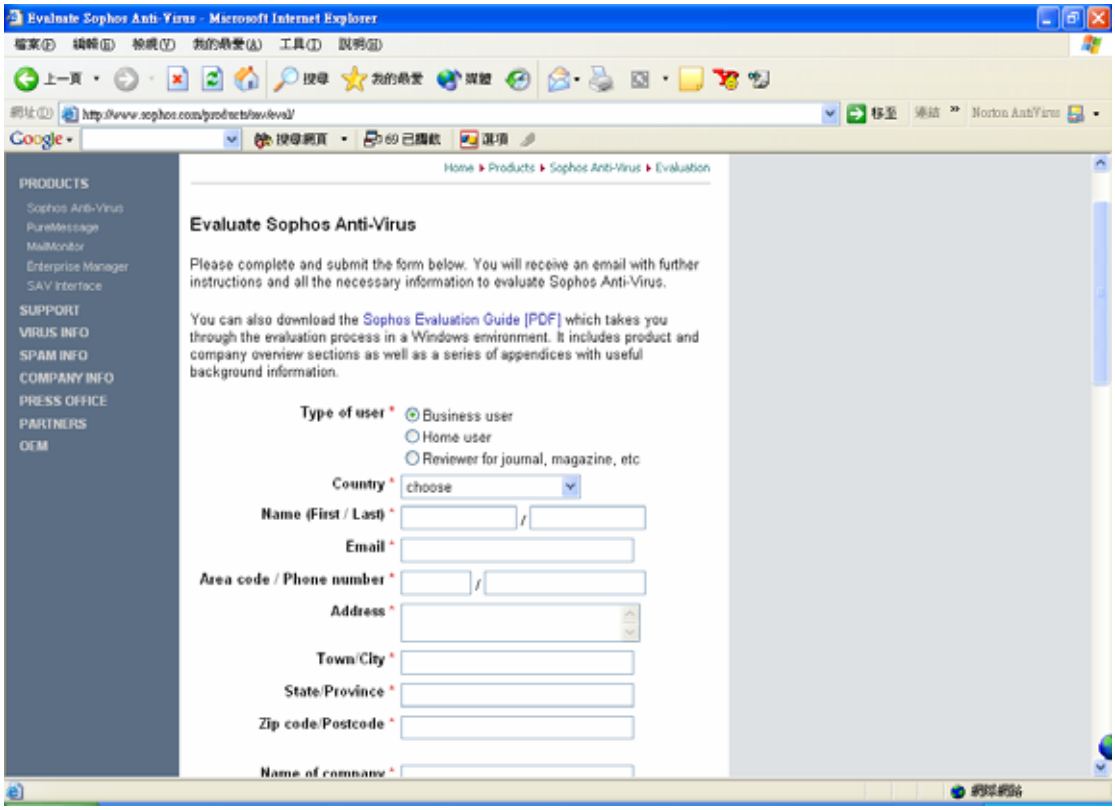
首先至 Mail Scanner 的官方網站（http://www.sng.ecs.soton.ac.uk/mailscanner/）下載 RPM 檔的主程式。

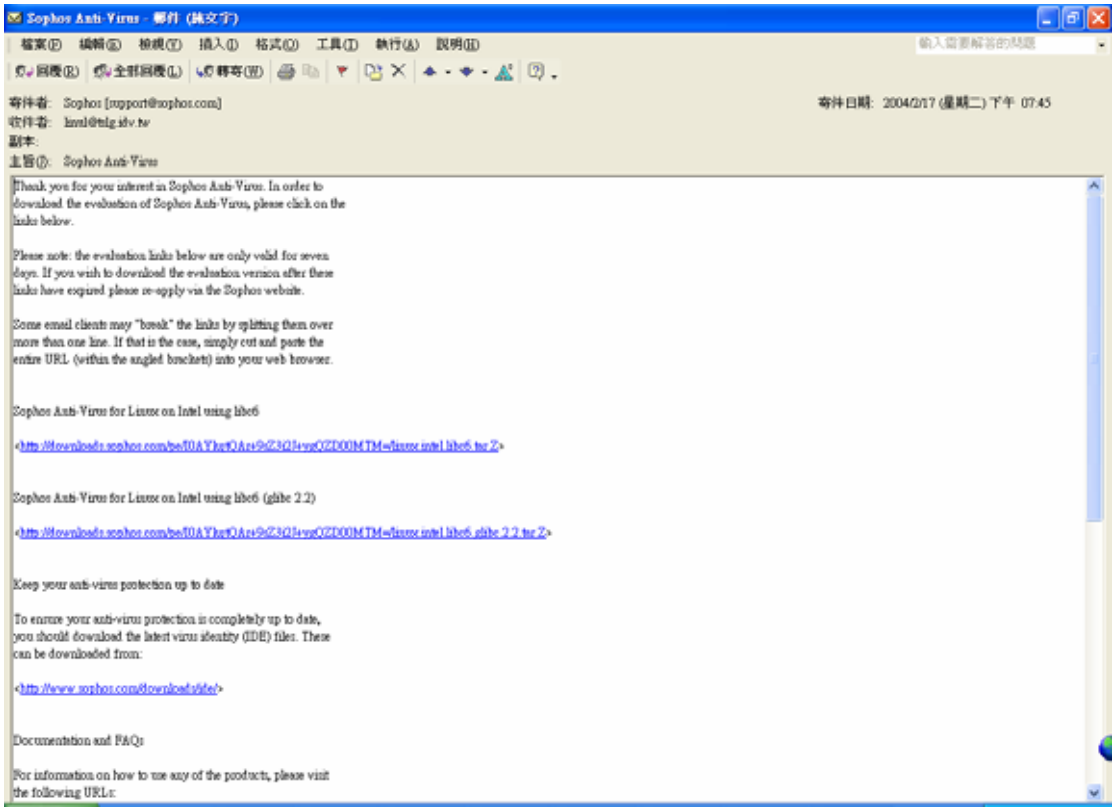
筆者在撰寫時，最新的版本為 4.26.8-1，選擇第二項 Redhat 的 rpm 版本來下載。

接著下載 Sophos 主程式，連上 Sophos 的官方網站（http://www.sophos.com），下載主程式需要先行註冊，所以連結至左方【PRODUCTS】這個連結，進入以下的畫面。

點選進入後，要尋找一個叫做【Evaluate Sophos Anti-Virus】的選項，如下圖所示。

點選進入後，請輸入註冊資訊，重點是 E-mail 位置，系統之後會寄一封信請你去下載，所以作業系統的選項要選正確。





接著要收信，並直接點選信件中的位址就可以下載程式碼了。

設定及安裝

將 MailScanner-4.26.8-1.rpm.tar.gz 上傳至目錄後，進行解壓縮動作，指令如下：

```
[root@net122 linul]# tar zxvf MailScanner-4.26.8-1.rpm.tar.gz
```

接下來安裝 MailScanner，首先補足不夠的套件，使用./Update_MakeMaker.sh 的指令來進行安裝，指令如下：

```
[root@net122 MailScanner-4.26.8-1]# ./Update-MakeMaker.sh
```

將所有的套件補足後，就要開始安裝 MailScanner 的主要程式，指令如下：

```
[root@net122 MailScanner-4.26.8-1]# ./install.sh
```

再來是安裝 Sophos 的主程式，將下載回來的檔案解壓縮，指令如下：

```
[root@net122 linul]# tar zxvf linux.intel.libc6.tar.Z
```

切換換到 sav-install 下，接著要新增一名使用者 sweep，此使用者沒有家目錄，指令如下：

```
[root@net122 sav-install]# useradd -M -s /bin/true sweep
```

接著安裝 Sophos 的主程式，指令如下：

```
[root@net122 sav-install]# ./install.sh
```

安裝完畢後，可以確認下面的目錄是否已被建立而且有完整的檔案：

```
    - binaries in /usr/local/bin
    - the shared library in /usr/local/lib
    - the virus data in /usr/local/sav
    - manual pages in /usr/local/man
```

或者可以在 sav-install 這個目錄下執行安裝，指令如下：

```
[root@net122 sav-install]# /usr/sbin/Sophos.install
```

如此一來，系統會在/usr/local/Sophos 的目錄下建立所有的 sophos 環境，當然也可以選擇第一種安裝模式。

也可以啟動 Sophos 的 InterCheck 的服務，指令如下：

```
[root@net122 sav-install]# icheckd -d
InterCheck Server virus detection utility
Version 3.74, October 2003 [Linux/Intel]
Includes detection for 84992 viruses, trojans and worms
Copyright (c) 1989,2003 Sophos Plc, www.sophos.com

WARNING: Changing user id to user sweep.
InterCheck is now active
```

修改/etc/MailScanner/MailScanner.conf。

將：

```
    Virus Scanners = none
```

修改為：

```
    Virus Scanners = sophos
```

如果是使用第一種安裝模式，因為 MailScanner 預設是將所有的檔案放在/usr/local/Sophos 這個目錄下，所以設定上會有點問題，這時要將下列兩行參數修正：

將：

```
Sophos IDE Dir = /usr/local/Sophos/ide
```

修改為：

```
    Sophos IDE Dir = /usr/local/sav
```

將：

```
Sophos Lib Dir = /usr/local/Sophos/lib
```

修改為：

```
    Sophos IDE Dir = /usr/local/lib
```

修改/usr/lib/MailScanner/sophos-wrapper

將：

PackageDir = $1

修改為：

PackageDir = /usr/local

將：

SAV_IDE = $PackageDir/ide

修改為：

SAV_IDE = $PackageDir /sav

將：

LD_LIBRARY_PATH = $PackageDir/lib

修改為：

LD_LIBRARY_PATH = /usr/local/lib

修改/etc/mail/sendmail.mc

將：

DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl

修改為：

dnl DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl

然後重新 m4，指令如下：

[root@net122 mail]# m4 sendmail.mc >sendmail.cf

接下來要停止 Sendmail 的服務讓它不再啟動，然後使用 MailScanner 來代替，指令如下：

[root@net122 MailScanner-4.23-11]# /etc/rc.d/init.d/sendmail stop

```
關閉 sendmail:                                              [  確定  ]
關閉 sm-client:                                             [  確定  ]
```

讓 Sendmail 不在開機的時候自動啟動。

```
[root@net122 MailScanner-4.23-11]# chkconfig sndmail off
```

讓 MailScanner 在開機的時候啟動。

```
[root@net122 MailScanner-4.23-11]#chkconfig --level 2345 MailScanner on
```

最後啟動 MailScanner 的服務。

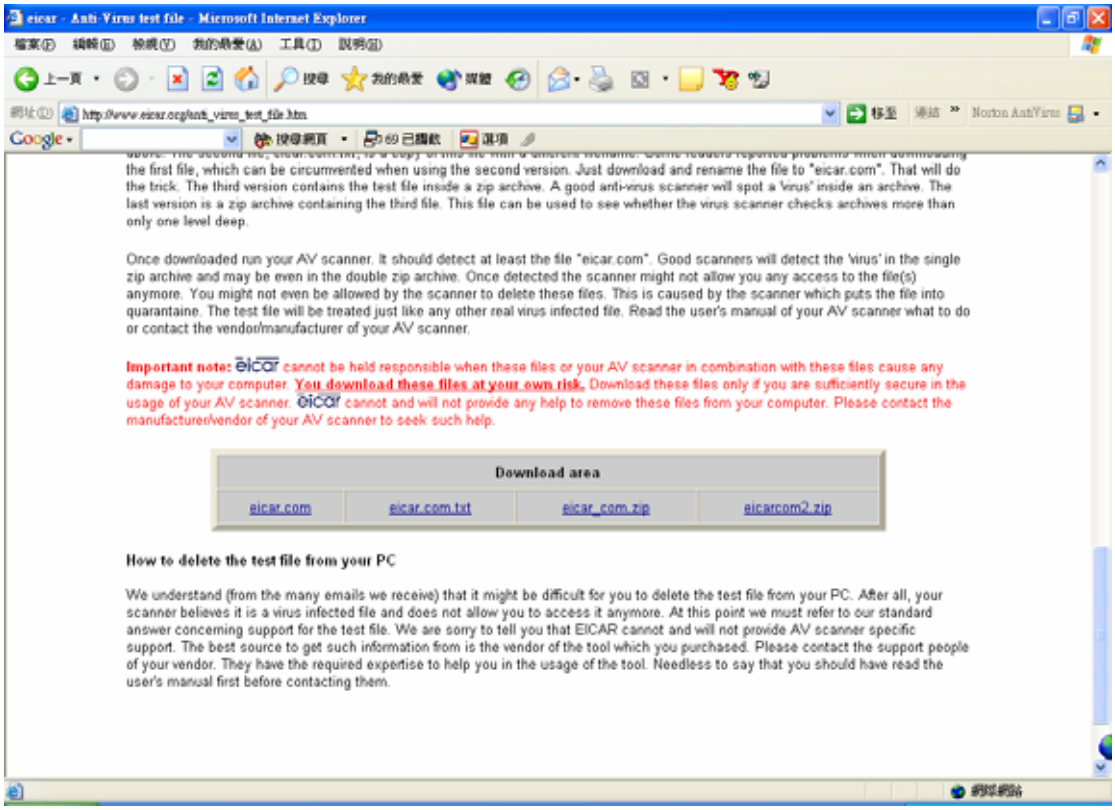
```
[root@net122 root]# /etc/rc.d/init.d/MailScanner start

Starting MailScanner daemons:
        incoming sendmail:                                  [  確定  ]
        outgoing sendmail:                                  [  確定  ]
        MailScanner:                                        [  確定  ]
```

該怎麼進行測試呢？如果可以在/var/log/maillog 中看見以下的訊息，即表示 mailscanner 已經在進行掃描的動作。

```
Feb 18 12:59:30 net122 MailScanner[2324]: Virus and Content Scanning: Starting
Feb 18 12:59:37 net122 MailScanner[2324]: Uninfected: Delivered 1 messages
```

如果要使用有毒的信件來進行測試，可以連到以下的網址來下載測試病毒檔：

http://www.eicar.org/anti_virus_test_file.htm



選擇其中之一來下載然後寄到伺服器，收到的信件內容就會變成如下圖所示的畫面。

而 maillog 中也會留下記錄：

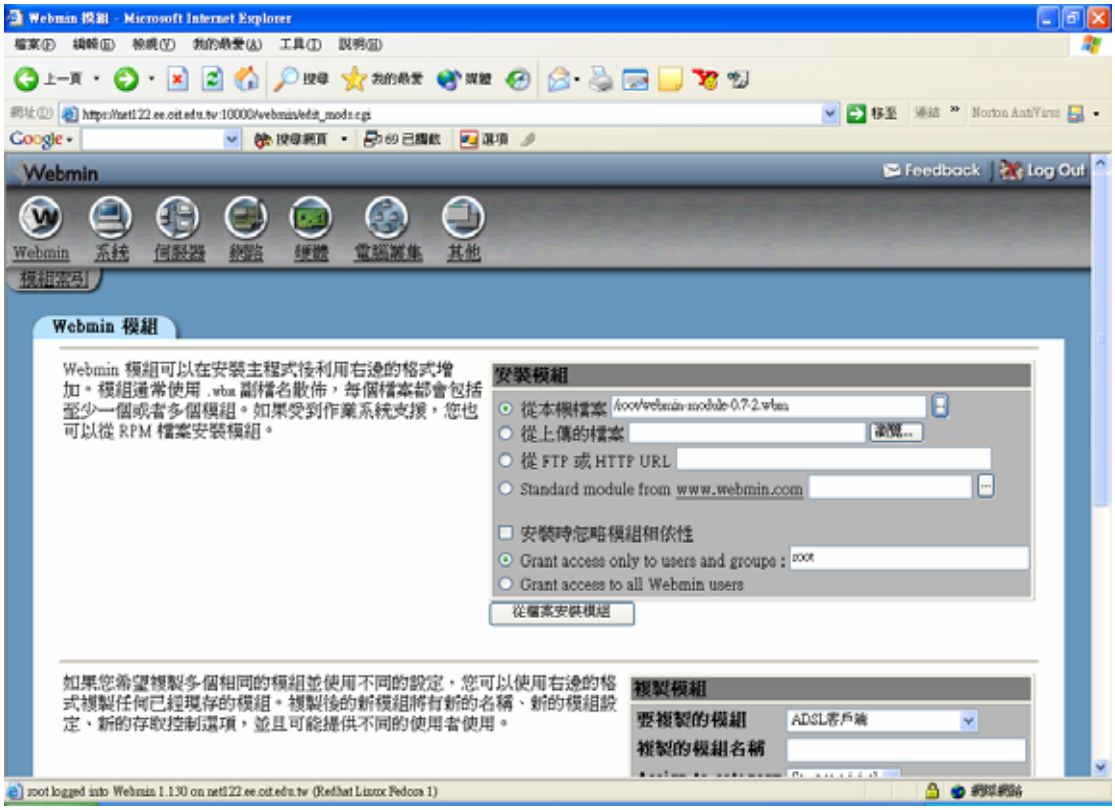
```
Feb 18 22:41:16 net122 MailScanner[2181]: >>> Virus 'EICAR-AV-Test' found in
file ./i1IEeqAp010169/eicar.com.txt
Feb 18 22:41:16 net122 MailScanner[2181]: Virus Scanning: Sophos found 1
infections
Feb 18 22:41:16 net122 MailScanner[2181]: Infected message i1IEeqAp010169 came
from 61.62.103.105
Feb 18 22:41:16 net122 MailScanner[2181]: Virus Scanning: Found 1 viruses
Feb 18 22:41:16 net122 ipop3d[10198]: pop3 service init from 61.62.103.105
Feb 18 22:41:16 net122 MailScanner[2181]: Saved infected "eicar.com.txt" to
/var/spool/MailScanner/quarantine/20040218/i1IEeq
Ap010169
```

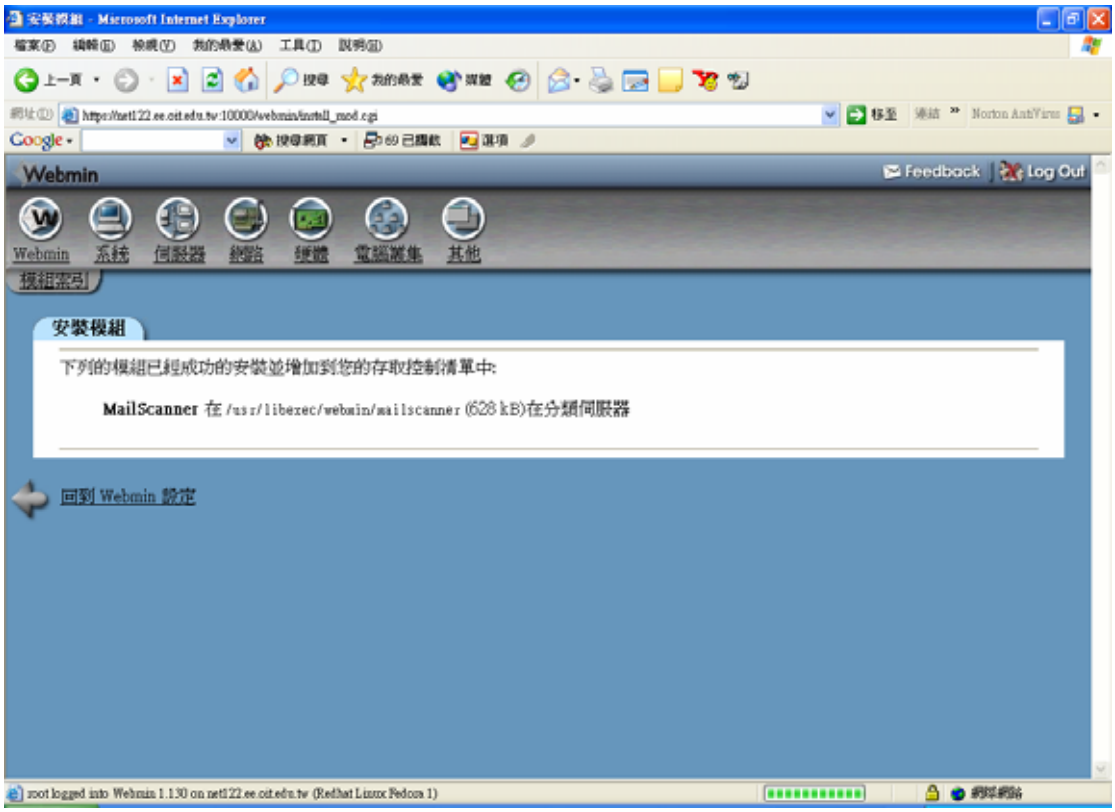
如此就成功的完成基本的設定了。

安裝 MailScanner 的 Webmin 模組，可以到以下的下載點來下載 Webmin 的 MailScanner 的管理模組：

```
[root@net122 root]# wget
http://lushsoft.dyndns.org/mailscanner-webmin/webmin-module-0.7-2.wbm
```

進入 Webmin 的管理頁面，選擇『webmin 設定』內的『webmin 模組』。將檔案的路徑指定好後就直接進行安裝。





安裝完畢後，到『伺服器』中選擇『MailScanner』，接著進行組態設定，將：**Full path to MailScanner program**

設定為：

/usr/sbin/MailScanner

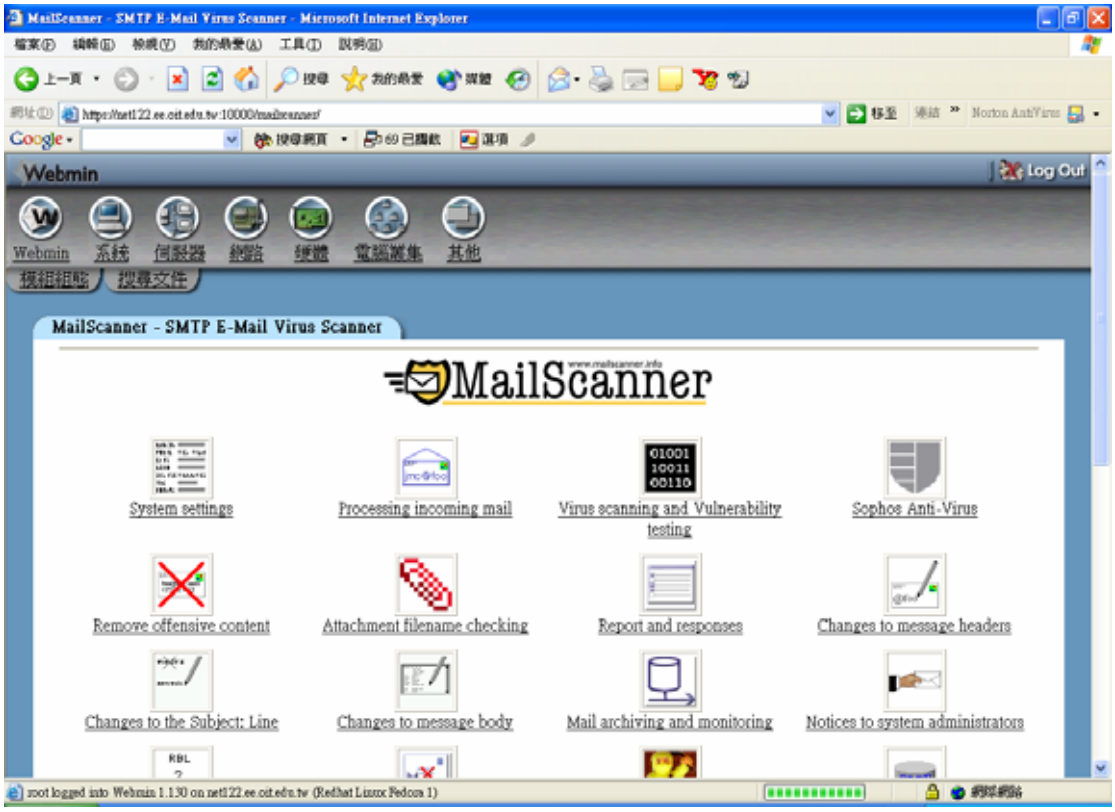
然後將：

Full path to MailScanner config file

設定為：

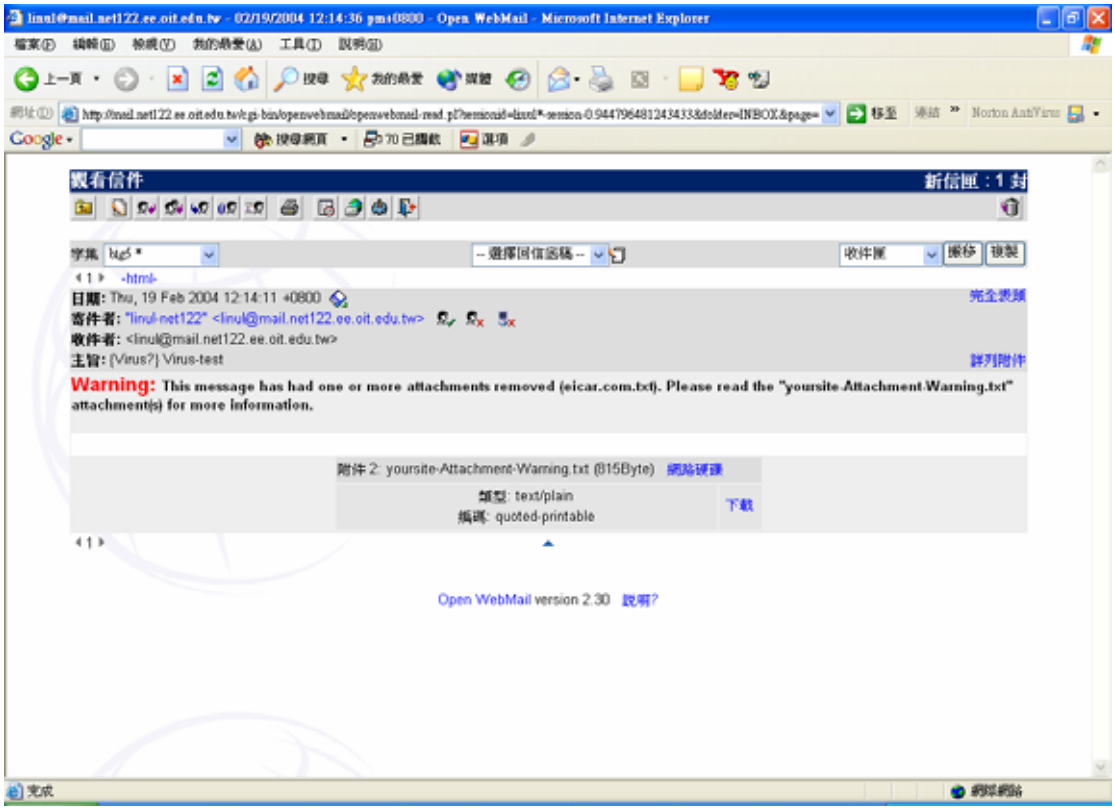
/etc/MailScanner/MailScanner.conf

完成後的畫面如下圖所示。



使用 openwebmail 搭配 MailScanner

同樣的，也可以利用 openwebmail 來搭配 MailScanner，收到的信件如下圖所示。



另外，openwebmail 也提供了使用者編輯郵件規則的機制，這樣一來就可以針對某一些病毒的特性來撰寫條件，增加防護的能力。預設的 openwebmail 有一些設置規則，如下圖所示。

相關參數配置

系統設定

Max Children

Default: 5

MailScanner 會使用伺服器在同一時間內有效的進行好幾個行程來處理（processing）郵件，這個設定就是設置同時進行的行程數，假設處理非常多的郵件，調高這個數字會對伺服器性能會有改變，一個好的數字會被設定成每個 CPU 可同時處理 5 個行程，所以假設擁有四個 CPU 的話，可以設定為 20。

Run As User

Default 不要改變此使用者

提供給 Exim 的使用者（絕不要使用 root 作為 sendmail 的使用者），這個選項是改變運行 MailScanner 的使用者。

Run As Group

Default 不要改變此群組

提供給 Exim 的使用者（絕對不要使用 root 作為 sendmail 的使用者），這個選項是改變運行 MailScanner 的群組。

Incoming queue dir

Default:/var/spool/mqueue.in

MailScanner 該掃描的郵件目錄。

Outgoing queue dir

Default:/var/spool/mqueue

MailScanner 所掃描過後的郵件目錄。

Incoming work dir

Default:/opt/MailScanner/var/incoming

在進行掃描動作的期間，用來放置被解壓縮的 MIME 訊息的暫存目錄。

Quarantine dir

Default:/opt/MailScanner/var/quarantine

一個放置感染病毒的郵件中被隔離附件的目錄。

PID dir

Default:/opt/MailScanner/var

存放 MailScanner 行程 id 檔的目錄。

MTA

Default:sendmail (sendmail 或 Exim）

指定要使用那個 MTA 套件。

Sendmail

Default:/usr/lib/sendmail

Sendmail 的程式位置。

Sendmail2

Default 是 Sendmail 這個選項的設置

使用在傳送 outgoing/cleaned 訊息的狀態下（MailScanner 有分 incoming 及 outgoing 的模式）。提供給 Exim 使用者，所以他們可以指定一個不同的 exim.conf 檔，用來轉送 outgoing 的佇列。

病毒掃描設定

Virus Scanning

Default: yes

掃描郵件病毒嗎？ 若將此選項設定為 "no" 會完全關閉病毒掃描的功能。

Virus Scanners

Default: none(sophos, mcafee, command, kaspersky, inoculate, inoculan, nod32, f-prot, f-secure, antivir, panda, rav, none)

指定要使用那個 anti-viurs 的套件。注意：假如要使用好幾個套件，請用空白鍵將每一個名稱分開。

Deliver Disinfected Files

Default: yes

當一個被感染的文件被解毒成功後，是否要將之寄回原來的目的地？

Still Deliver Silent Viruses

Default: yes

如果這個選項設定為 "yes" 的時候，解毒後的郵件還是會傳回給原始的收信人，即使這些位址是被那些被感染的 PC 使用隨機的方式選出來的，且並不是那些使用者想寄的，設定此選項為 "yes" 會讓使用者知道 MailScanner 是有在保護他們的，但是如果有許多人抱怨收到太多的病毒通知時，那就設定為"no"吧。

廣告信選項

Spam List Definitions

Default: /opt/MailScanner/etc/spam.lists.conf

Defualt Linux: /etc/MailScanner/spam.lists.conf

Default FreeBSD: /usr/local/etc/MailScanner/spam.lists.conf

這個檔案包含了所有能被偵測為廣告信信來源的 "Spam Lists" （同樣叫做 RBL's or DNSBL's），許多的 Spam Lists 都可被加入到這個檔案中，但它一開始已經包含了大部份的廣告信列表（Spam Lists）。

Virus Scanner Definitions

Default:
/opt/MailScanner/etc/virus.scanners.conf
Default Linux:
/etc/MailScanner/virus.scanners.conf
Default FreeBSD:
/usr/local/etc/MailScanner/virus.scanners.conf

這個檔案包含了所有 virus scanner 指令的位置，在啟動 MailScanner 前先確認這個檔案是否正確，則 MailScanner 可能無法啟動。

5.問題與討論

1. 試著在你的系統中安裝 Openwebmail。
2. 比較 MailScanner 和 Openwebmail 阻擋廣告信和掃描病毒信件的效能。
3. 廣告信的定義何？目前有無法令的限制？
4. MailScanner 主系統和定義檔如何更新？
5. MailScanner 如何搭配不同 MTA 使用？