逢 甲 大 學

資訊工程學系專題報告

郵件防毒處理系統

金　　山 (四乙)

學　　生：林 韋 成 (四乙)

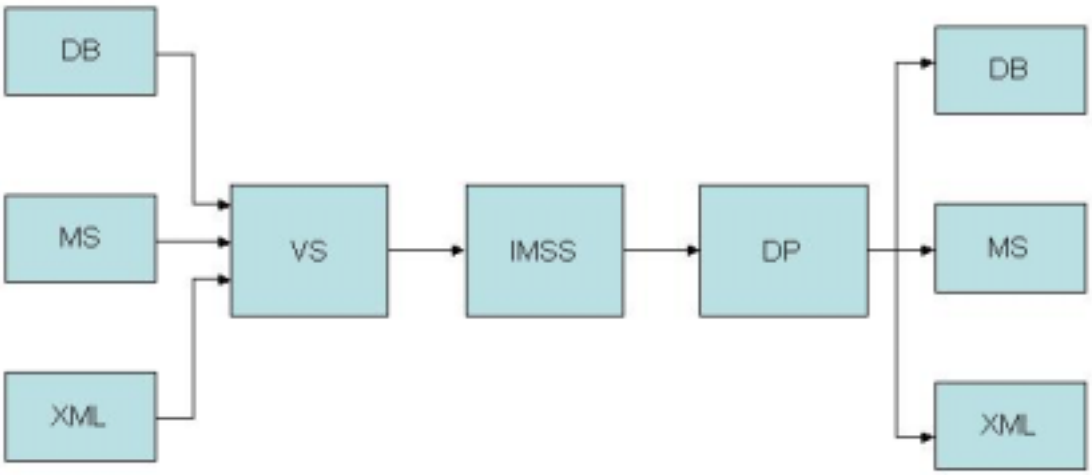
蕭 盛 鴻 (四乙)

指導教授：李 維 斌

中華民國九十二年十二月

==目　錄==

系統架構



第一章　動機

人們總是使用防毒軟體消極的面對一次又一次的病毒,但是真正對防毒的了解卻是少之又少,花了大錢買了防毒軟體卻只能靠專業人員去解決和設定,我的動機很簡單,我要做一份網管人員必看,企業顧主必看的郵件防毒處理系統,在面對病毒未來洶湧攻勢之下,奠定更多防護,讓損失降到最低。

第二章

2.1 SMTP 協定原始命令碼和工作原理

1. SMTP 是工作在兩種情況下:一是電子郵件從客戶機傳輸到伺服器

二是從某一個伺服器傳輸到另一個伺服器。

2.SMTP 是個請求/回應協定，命令和回應都是基於 ASCII 文本，並以 CR 和 LF 符結束。回應包括一個表示返回狀態的三位元數位代碼。

3.SMTP 在 TCP 協定 25 號埠監聽連接請求。

4.連接和發送過程：

a.建立 TCP 連接。

b.用戶端發送 HELO 命令以標識發件人自己的身份，然後用戶端發送 MAIL 命令伺服器端正希望以 OK 作爲回應，表明準備接收。

c.用戶端發送 RCPT 命令，以標識該電子郵件的計劃接收人，可以有多個 RCPT 行伺服器端則表示是否願意爲收件人接受郵件。

d.協商結束，發送郵件，用命令 DATA 發送。

e.以.表示結束輸入內容一起發送出去。

f.結束此次發送，用 QUIT 命令退出。

5.另外兩個命令：

VRFY---用於驗證給定的用戶郵箱是否存在，以及接收關於該用戶的詳細資訊。

EXPN---用於擴充郵件列表。

6.郵件路由過程：

SMTP 伺服器基於功能變數名稱服務 DNS 中計劃收件人的功能變數名稱來路由電子郵件。SMTP 伺服器基於 DNS 中的 MX 記錄來路由電子郵件，MX 記錄註冊了功能變數名稱和相關的 SMTP 中繼主機，屬於該域的電子郵件都應向該主機發送。

若 SMTP 伺服器 mail.abc.com 收到一封信要發到 123@sh.abc.com:

a.Sendmail 請求 DNS 給出主機 sh.abc.com 的 CNAME 記錄，如有，假若 CNAME 到 shmail.abc.com，則再次請求 shmail.abc.com 的 CNAME 記錄，直到沒有爲止。

b.假定被 CNAME 到 shmail.abc.com,然後 sendmail 請求@abc.com 域的 DNS 給出 shmail.abc.com 的 MX 記錄，

shmail	MX	5	shmail.abc.com
		10	shmail2.abc.com

c. Sendmail 最後請求 DNS 給出 shmail.abc.com 的 A 記錄，即 IP 位址，若返回值爲 1.2.3.4。

d. Sendmail 與 1.2.3.4 連接，傳送這封給 123@sh.abc.com 的信到 1.2.3.4 這台伺服器的 SMTP 後臺程式。

7.SMTP 基本命令集：

命令	描述
HELO	向伺服器標識用戶身份發送者能欺騙，說謊，但一般情況下伺服器都能檢測到。
MAIL mail from:	初始化郵件傳輸
RCPT	標識單個的郵件接收人；常在 MAIL 命令後面可有多個 rcpt to:
DATA	在單個或多個 RCPT 命令後，表示所有的郵件接收人已標識，並初始化資料傳輸，以.結束。
VRFY	用於驗證指定的用戶/郵箱是否存在；由於安全方面的原因，伺服器常禁止此命令
EXPN	驗證給定的郵箱列表是否存在，擴充郵箱列表，也常被禁用
HELP	查詢伺服器支援什麼命令
NOOP	無操作，伺服器應回應 OK
QUIT	結束會話
RSET	重置會話，當前傳輸被取消

8.MAIL FROM 命令中指定的位址是稱作 envelope from 位址，

不需要和發送者自己的位址是一致的。RCPT　TO　與之等同，指明的接收者地址稱爲 envelope　to 地址，而與實際的 to：行是什麼無關。

9.爲什麼沒有 RCPT　CC 和 RCPT　BCC:?

所有的接收者協商都通過 RCPT　TO 命令來實現，如果是 BCC，則協商發送後在對方接收時被刪掉信封接收者。

10.郵件被分爲信封部分，信頭部分和信體部分。

envelope from, envelope to 與 message from:, message to:完全不相干。

evnelope 是由伺服器主機間 SMTP 後臺提供的，而 message　from/to 是由用戶提供的。有無冒號也是區別。

2.2　E-mail 工作原理及安全漏洞

E-mail 工作原理

一個郵件系統的傳輸包含了用戶代理（user Agent）。傳輸代理（Transfer　Agent 及接受代理(Doelivery A_gent）三大部分。用戶代理是一個用戶端發信和收信的程式，負責將信按照一定的標準包裝，然後送至郵件伺服器，將信件發出或由郵件伺服器收回。

傳輸代理負責信件的交換和傳輸，將信件傳送至適當的郵件主機，再由接受代理將信件分發至不同的郵件信箱。

傳輸代理必須要能夠接受用戶郵件程式送來的信件，解讀收信人的地址，根據 SMTP(Simpie Mail Transport proto_col）協定將它正確無誤地傳遞 d 到目的地。現在一般的傳輸代理已採用 Sendmail 程式完成工作， 到達郵件主機在經接收代理 POP（Post Office Protocol，網路郵局協定或網路中轉協定）來使郵件被用戶讀取至自己的主機。

E-mail 的安全漏洞

當用 e 戶與你或站點交換 E-mail 時，應確保他們是安全的。

E-mail 在 Internet 上傳送時，會經過很多點，如果中途沒有什麼阻止它，最終會到達目的地。

資訊在傳送過程中通常會做幾次短暫停留，因爲其他的 E-mail 伺服器會查看信頭，以確定該資訊是否發往自己，如果不是，伺服器會將其轉送到下一個最可能的地址。

E-mail 伺服器有一個“路由表”，在那裏列出了其他 E-mail 伺服器的目的地的位址。當伺服器讀完信頭，意識到資訊不是發給自己時，它會迅速將資訊送到目的地伺服器或離目的地最近的伺服器。E-mail 伺服器向全球開放，他們很容易受到黑客的襲擊，從而暴露隱私。資訊可能攜帶會損害伺服器的指令，

例如，Morris bug 內有一種會損壞 Sendmail 的指令，這個指令可使其執行黑客發出的命令。

Web 提供的閱讀器更容易受到這類侵擾。因爲，與標準的基於文本的 Intelnet 郵件不同， Web 上的圖形介面需要執行腳本或 applet 才能顯示資訊。

例如，在一條資訊中加進了一個小的腳本，並發給公司內的每一個用戶。 這個腳本在資訊中作爲一個小圖示，下面有"click me"。因爲他來自於 MIS，組織內的每一個人都知道它，人們一擊這個圖像，就會打開一個小程式，重新映射(map)驅動器，並安裝想要發佈的應用程式。這個步驟在很多組織中採用，但可能有人欺騙郵件記錄，改變信件頭，將同樣的資訊發出，但與資訊中攜帶的圖示相聯繫的腳本卻發生了改變。因爲用戶以爲資訊是從 MIS 發出的，他們會敲擊圖示。圖示攜帶的指令，會刪去他們的本地硬碟驅動器，上載某個文件甚至系統資訊。 這個資訊甚至可以不包括圖示。他可以要求用戶改變口令，用戶可能因爲資訊來自 MIS 而真的改變口令。

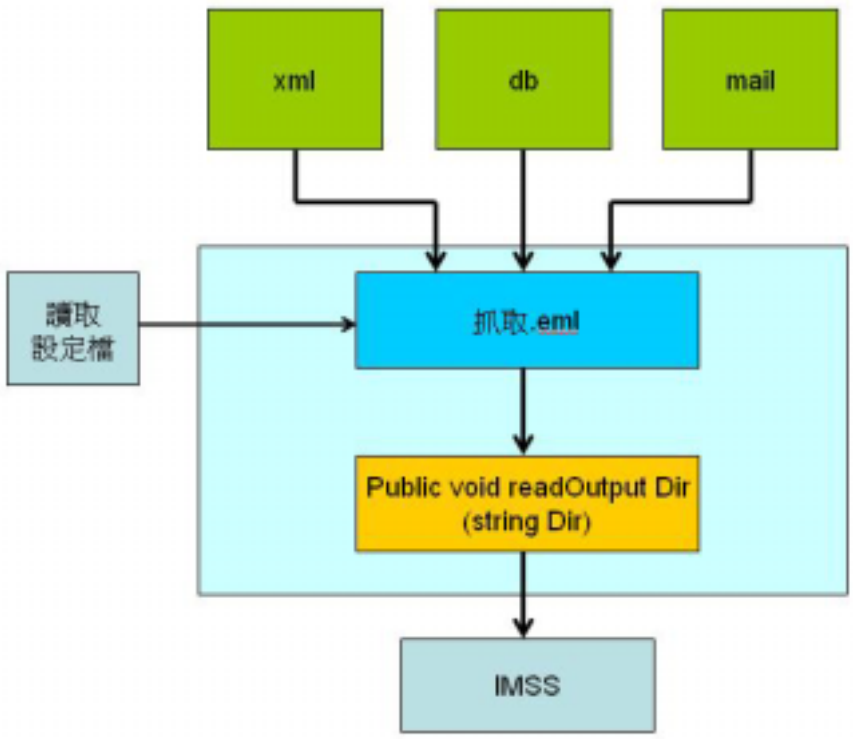
防火牆也不可能識別所有惡意的 applet 和腳本，最多，也只能濾去郵件位址中有風險的字元， 這些字元還應是防火牆識別得出來的。

原理 ：

用 SMTP 協定的方式去將多個資料夾內的.eml 信件寄給 Interscan 掃毒

```
if( outputFilesList != null )
{
for( int i=0; i<outputFilesList.length; i++ )
{
if( outputFilesList[i].isFile() &&
outputFilesList[i].getName().endsWith(".eml") )
{
                vt.addElement( outputFilesList[i] );}
}
}
```

判斷 outputFilesList 不爲 null 變去抓取.eml 副檔名的郵件將之寄給 Interscan



第三章　病毒造成的大量損失和 IMSS 的使用

3.1　摘要

一直以來我們都會搜集有關病毒相關的資料和程式碼做自己興趣的研究，病毒的危害究竟有多嚴重，讓我們用損失來告訴你。

3.1.1　服務阻斷攻擊(DoS)

2000 年二月，「服務阻斷攻擊」(DoS)用大量資料阻塞了 Yahoo、eBay、CNN 及 ZDNet 的網路，致使用戶無法正常造訪長達兩、三小時之久。

3.1.2　梅莉莎變種重現江湖 Mac 文件檔也遭殃

CNET 新聞專區：Ian Fried 報導　　19/01/2001

電腦病毒專家說，梅莉莎（Melissa）病毒的新變種正在蔓延中，這一回是藏身於蘋果麥金塔（Macintosh）格式的微軟 Office 檔案(.doc)中。

Network Associates 的 McAfee 防毒緊急研究小組主任 Vincent Gullotto 指出，新變種的樣本約一個月前已送到他的工作室，但直到最近一、兩天，已傳報超過 24 件中毒事件。

如同其他梅莉莎變種，新病毒（稱 Melissa -X 或 Melissa 2001）主要作用是自我複製。系統被感染後，日後凡是用微軟 Word 製作文

件檔案，就可能夾帶這隻病毒，而且如果在 Windows 環境下執行微軟電子郵件軟體 Outlook，病毒就會使用此軟體的通訊錄，自動傳出 50 封夾帶病毒程式 anniv.doc 的電子郵件。

3.1.3 紅色警戒(Code Red)病毒的損失

2001 年 09 月美國國會一個獨立調查小組 29 日在眾院作證表示，上月導致連接網路的電腦遭受約 24 億美元(約新台幣 828 億元)損失的「紅色警戒」(Code Red)病毒。

3.1.4 新網路病毒 藍色代碼肆虐

記者梁家榮／綜合報導

中共人民網六日報導，紅色代碼病毒對電腦用戶造成的恐慌尚未平息，一種名爲藍色代碼(Worm. IIS. Code Blue)的新型網路病毒已經現身，該病毒利用了 WINDOWS2000 的漏洞來傳播，比紅色代碼更具強大的攻擊性，並已開始在大陸網路用戶中流傳。

報導指出，中共國家計算機病毒應急處理中心成員單位—北京江民公司，接到受害用戶投訴後，已連夜編寫出了新的升級殺毒庫，並立即將該病毒上報國家計算機病毒應急處理中心。

中共權威反病毒專家指出，該病毒比紅色代碼秖有更強大的攻擊性，電腦一旦感染該病毒，將大量占用系統記憶體，導致系統運行速度下

降直至系統癱瘓。專家告誡廣大網路用戶，儘快升級防病毒軟體，如最新版反病毒軟體 KV3000，這樣可有效的防範該病毒的侵犯。

3.1.5 TANet 學術網路的癱瘓

台灣最近這幾天都可以明顯感受到紅色警戒病蟲的影響，目前包括台北縣政府、中研院、中華電信、教育部學術網路、鄉鎮市公所等都傳出遭到入侵的消息。台北縣政府 4 日晚上遭到第 3 代紅色警戒病蟲入侵，就是因爲某市公所的電腦遭入侵，影響到相連的台北縣政府網站，同時與台北縣政府網站相連的網站全部癱瘓，其中包括地政局網路系統，使得各鄉鎮市公所的地政局網路系統等，也疑似受影響，目前部份網路已經恢復運作，不過可讓民眾申辦各式謄本的地政網路服務暫停一星期。TANet 學術網路也受到嚴重影響，由於學術網路是全國各級學校所使用的網路系統，因此其中一個學校網站受到紅色警戒病蟲入侵後，病蟲即自動蔓延至所有學校網站，教部並於 2 日發出緊急通知，表示 CodeRed 病蟲已經嚴重影響 TANet 網路流量，因此教育部限制了 WWW 的流量，並列出近 50 台可能受到入侵的主機 IP 位址，要求相關人員盡速修復。

3.1.6 觀念突破性病毒－Nimda

【記者許明煌報導】

風災善後才正如火如荼展開，散播速度史無前例的 Nimda 病毒卻趁機製造混亂。18 日才在美國地區現身的 Nimda 病毒，三天內至少已經癱瘓全球數十萬企業網路。這隻被防毒軟體廠商稱爲「觀念突破性」的病毒，由於結合了電腦病毒與駭客攻擊兩種特性，因此傳播速度遠比之前才剛肆虐全球的「紅色警戒（CodeRed）快三倍以上，預估造成的損害情況也將遠超過紅色警戒。

台灣趨勢科技企劃專員廖立茹表示，前天上班第一天趨勢已經接到 160 家企業客戶向趨勢回報感染 Nimda 病毒，經過短短一天，昨天回報企業已經暴增到 300 家，傳染速度之快，遠高於之前的紅色警戒。台灣賽門鐵克許叔菁也表示，一天內至少接到超過 60 家企業的求助電話，表示 Nimda 的疫情正持續擴大，要不是許多公司因爲斷電還未能恢復正常作業，否則回報情形可能更高。

廖立茹指出，Nimda 傳染速率之所以高過紅色警戒，原因在於 Nimda 病毒的傳染途徑非常多，除了最傳統的電子郵件夾帶病毒檔(readme.exe)外，由於 Nimda 設計時針對採用微軟 IIS 架構設計網站的漏洞進行攻擊，因此使用者只要瀏覽遭受 Nimda 病毒感染的網站，就

會立即感染病毒。而遭受感染的電腦，又會立即透過網路芳鄰的資源分享功能，立刻主動感染公司網路上的其他電腦。因此幾乎可以說是一人中毒，公司網路立即遭殃，許多電腦使用者就發現這幾天根本沒上網、沒收信，卻感染了 Nimda 病毒。

台灣賽門鐵克指出，遭受感染的企業網路會出現明顯的遲緩狀況，同時郵件系統也會如同紅色警戒一般遭到癱瘓。

防毒軟體公司在度提醒公司，除了立即更新防毒軟體病毒碼以外，企業 IIS 主機及微軟 IE 瀏覽器的用戶最好立即下載微軟最新的修正程式來填補漏洞。像趨勢或賽門鐵克等公司都已經緊急推出了防毒與修復工具。尚未掃毒的電腦，可以藉由這些免費下載的程式來偵測是否已經感染 Nimda，如果發現已經感染，也可以藉由修復工具來清除系統所造成的損害，以免疫情擴大。

3.1.7 疾風病毒災情持續上飆!!

疾風病毒災情持續上飆!!全球估計有百萬電腦用戶中毒「疾風病毒」**WORM_MSBLAST.A** 災情持續向上飆漲，受感染電腦用戶數再創新高！網路安全領導廠商趨勢科技今天(13 日)針對「疾風病毒」公佈目前最新國內外受感染電腦用戶的數字，根據趨勢科技目前掌握的最新消息，在台灣方面，短短數日之內受感染的大型企業客戶已急速擴增

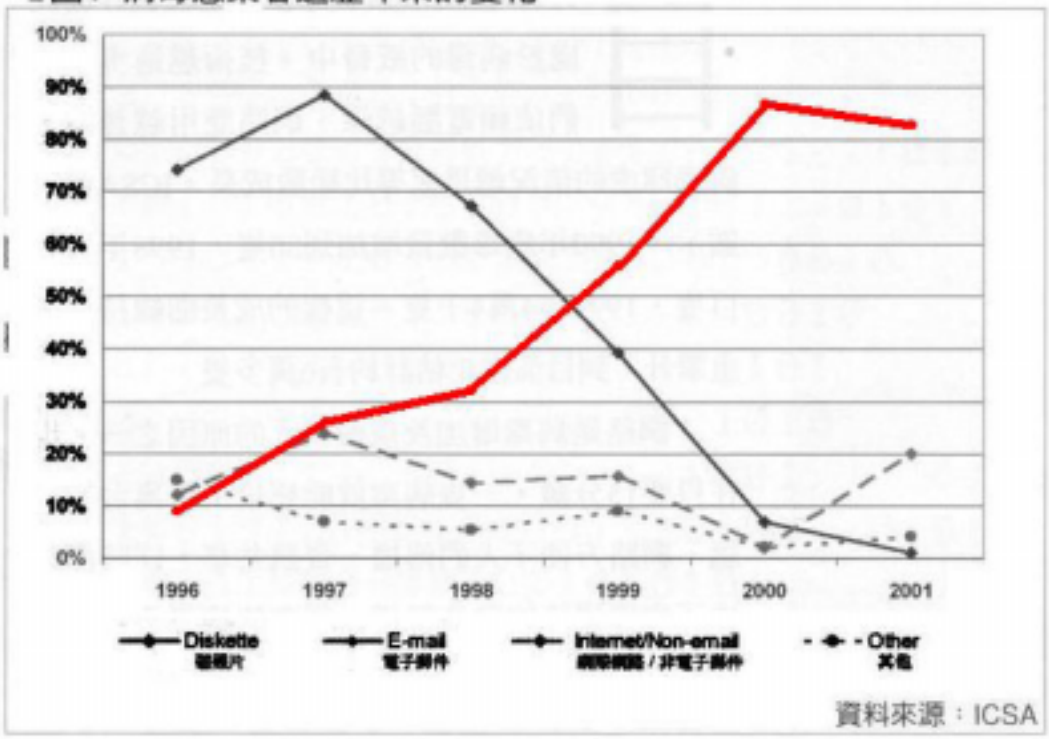
到兩百多家，中小型企業用戶更是多達數千家以上，估計全台個人電腦主機已經有超過五萬台以上受到病毒嚴重感染無法正常作業；趨勢科技更近一步表示，由「疾風病毒」驚人的感染力看來，預估全球受到病毒感染的電腦用戶將突破百萬台以上，受災企業用戶亦達數萬家之多。

3.2 資料分析

電子郵件的「即時性」和「方便性」使得傳統交易的模式產生革命性的變革，資訊可即時取得，加速商業交易，降低企業內部營運成本，爲企業界帶來新的營運方式，和無限的商機，不過，由於網路的「便利性」也同時讓惡意駭客可以輕易的攻擊公眾網路上的伺服主機，造成對外聯繫中斷，電子郵件的「快捷性」更讓有心人士將病毒快速散佈流竄，導致企業和個人使用者的重大損失，更甚至造成企業的郵件主機癱瘓，不當的使用電子郵件，例如帶大量的色情圖片和廣告郵件，濫用公司對外的頻寬，抑或蓄意洩漏公司機密文件，皆會造成企業不可磨滅的損失。據 ICSA 資料顯示，1990 年病毒數量增加到 80 隻，1998 年 2 萬 5 百隻，1999 年是 4 萬 4 千隻，這樣的成長曲線持續向上攀升，到目前爲止估計有六萬五千隻。現在的病毒不再像過去只能用磁片一個一個感染，多半是藉由網路來傳播，尤其是電子郵件。就以 1999 年暴發的梅莉莎（Melissa）就結合了病毒和蠕蟲的特

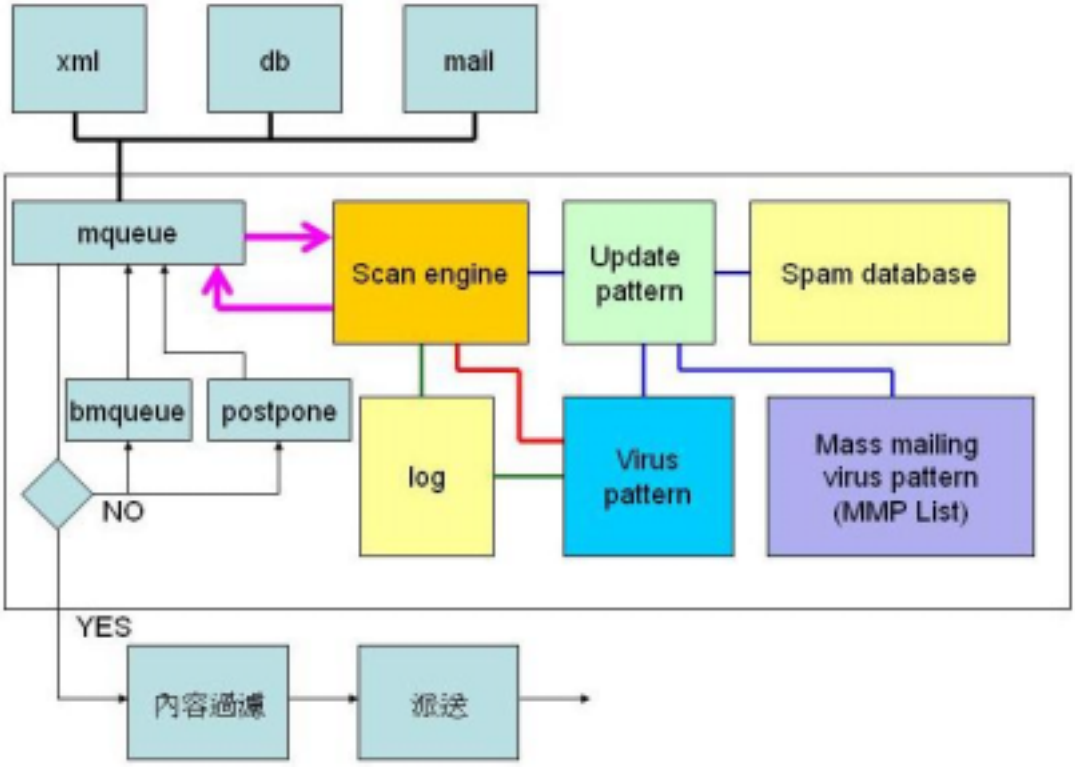
性，除了感染 Word 檔之外，且透過電子郵件大量散發，是首隻利用電子郵件管道大量複製散播的病毒，至此之後，不管是那一類型的病毒也都仿造著這一般的攻擊模式，帶有可造成大量郵件擴散的程式(Mass Mailing Payload) 。而製作病毒的技術門檻卻是逐漸降低中，網路上有許多現成可以產生病毒的工具，就算是給新手，也可以在幾分鐘內製作一隻病毒。

圖1 病毒感染管道歷年來的變化



如圖一所示，其中的紅線是指感染源是電子郵件歷年來的變化，你會發現逐年增加比例實在快速的驚人。

3.3 採用 IMSS 對抗郵件病毒



———	採用 SMTP 的傳送方式將信件給 IMSS
→	信件收下之後，會在此處拆解準備進行掃毒，以 A 代表已掃毒的信件，以 B 代表未掃毒的信件。
———	更新的部分
———	Scan engine 向 Virus pattern 取得最新的病毒碼進行掃瞄
———	Log 裡紀錄了相關所有的變動和掃完之後的紀錄

第四章　內容過濾及信件派送

內容過濾

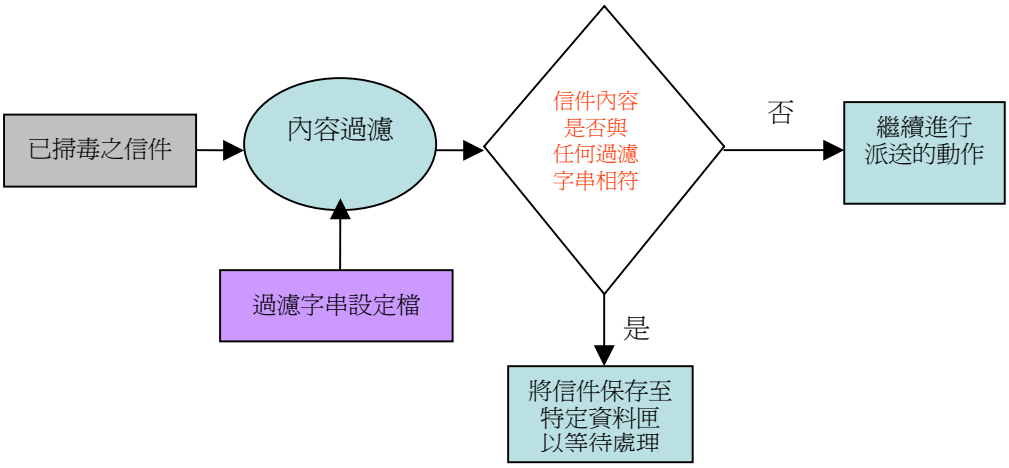
功能需求：

由於本郵件系統爲信件往來傳送之郵件系統，皆爲極爲機密之重要文件以及訊息。因此爲了嚴防機密的洩漏，必須對往來傳送的信件進行過濾，以確保傳送出去或是收進來的該信件沒有涉及任何機密相關之內容。

實作內容：

在本郵件系統中，設置一個可定義過濾內容的設定檔，將要過濾的字串加在此設定檔內。由此設定檔裡面所列出的所有字串，對每一封郵件的內容做比對，比對看看有沒有跟設定檔內的字串相符合的內容。如果有相符合的字串，就會將該信件存放在一個特定的資料匣之中等待處理，而該信件不進行傳送之動作；倘若沒有相符合的字串，該信件則會繼續進行派送的動作，進而將信件傳送出去。

如下圖所示



信件派送

本郵件系統與一般的郵件系統迥然而異，爲一專門提供某特定單位傳送信件之郵件系統，故其運作方式也跟一般的電子郵件系統不甚相同，其信件之傳送方式如下：

1.本單位內部信件之傳送

例如：軟微公司台北分公司各處室相互傳送信件

2.本單位外部單位信件之傳送：

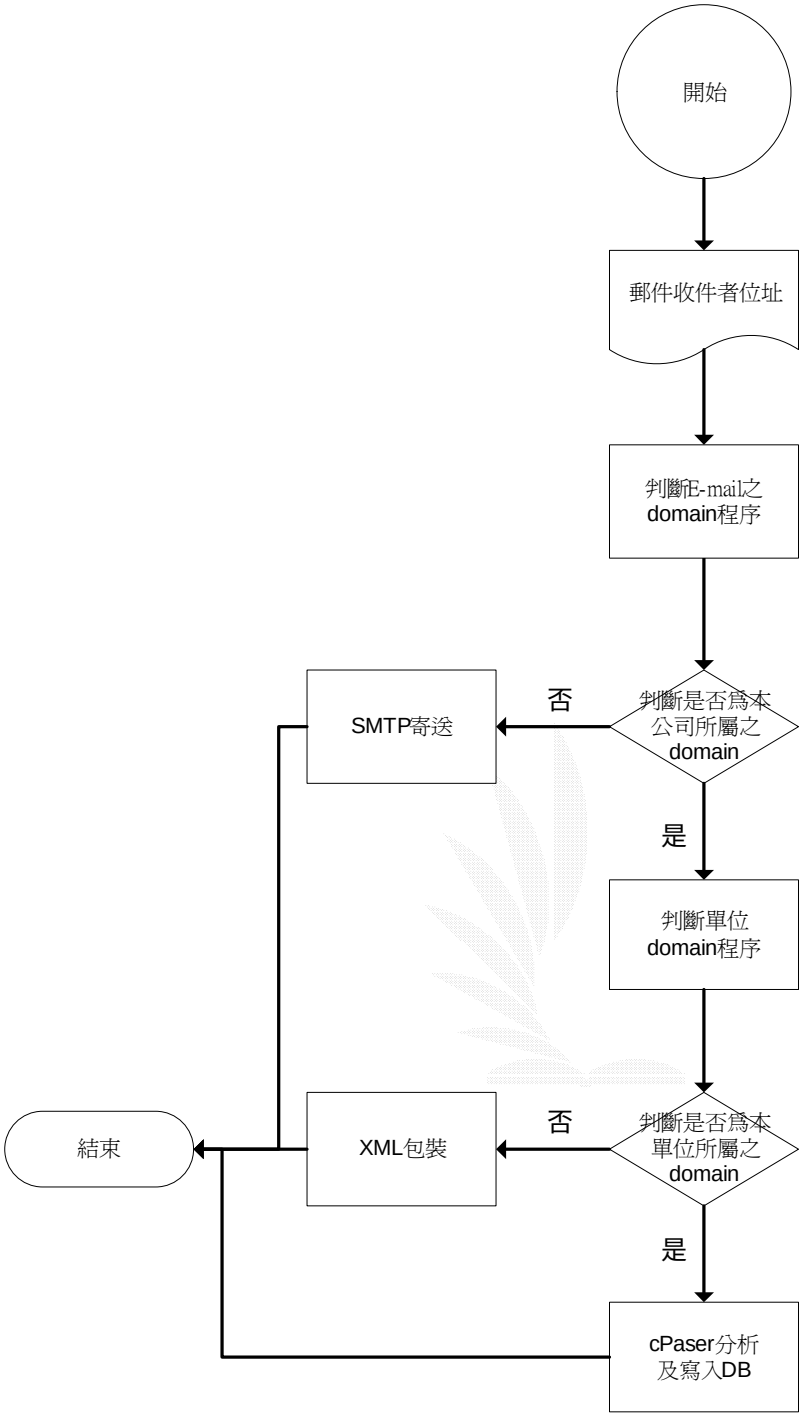
例如：軟微公司台北與台中分公司之間信件之傳送

3.非單位信件之傳送

例如：軟微公司與其它公司之間信件之傳送

判斷流程：

1. 先查看是否爲本公司
2. 若比對結果爲否就表示是其他公司
3. 比對結果爲是就代表目的地是本公司的單位，再從系統設定值找出本地代號爲何
4. 依不同目的地分別送至不同之路徑



程式實作架構

內容過濾及信件派送的程式以下列兩個 java 程式構成：

Monitor.java , ContentFilter.java 與 Dispatcher.java

而兩個程式的概略說明如下：

Monitor.java

內容過濾及信件派送程式的各類別檔均用 Monitor.java 來控制，包括參數值和程式運作流程。簡單的說，Monitor.java 是爲好掌控而設計的主類別檔。故在啓動內容過濾及信件派送程式時，只須在 compiler 後，執行 "#java Monitor" 即可。

ContentFilter.java

執行內容過濾

Dispatcher.java

Step:

1. 過濾副檔名，只對副檔名爲*.eml 的做事
2. 取得暫存檔和中間檔(VS 和 DP 同步用)的目錄內的所有檔案或資料夾的物件
3. VS 和 DP 階段性工作的判斷:

   a)Temp 資料夾是否爲空(爲空表示 VS 做完階段性工作)

   b)再判斷 Eml 資料夾是否爲空(不爲空表示有 mail 要派送了)

   c)Temp 資料夾爲空 && Eml 資料夾不爲空時, DP 才工作

4. 分析一中間檔名:

```
XXXXXXXXXXXXXXXXX.eml
^^^^^^^^^^^^^^^^^^^^^^^^^
        同步字串          副檔名
```

同步字串共 17 個 char 長度

5. 對單封 mail, 得到所有需收到 mail 的人的 E-Mail

6. 派送:

   a) 內容過濾

   b) 根據該封所有 E-Mail, 判斷須把該郵件送至

      MS 或 DB 或 XML 或 ILLEGAL_MAIL_DIR

   c) 複製該郵件至該到達的地方

      (MS 或 DB 或 XML 或 ILLEGAL_MAIL_DIR)

   d) 重覆 b 直到所有要派送的 mail 都送完

7. 移除已派送的 mail

第五章　遇到的困難和解決的過程

做專題不外乎要軟體、硬體一起努力之下才能完成，一開始在做的時候，在軟體的取得一直是我們頭痛的部分，面對一個 server 等級的防毒軟體，實在不容易拿到。拿到也只是 30 天的舊板測試軟體，在網路上找不到相關的資料書籍，更別提會在圖書館等相關的地方找到相關的資料，那是防毒軟體公司賣錢的軟體，要拿到相關的資料實在是很難，只能自己去看軟體裡的 help，不過，感覺很明顯的是那好像是業務員寫的說明，實在有看沒有懂，所以我只能一個參數、一個參數慢慢去做測試，去了解它各別的功能是做什麼用的，在硬體的設備方面，需要有完善的網路環境和 server 的等級的 os，從一般的個人電腦進級使用到 server 級的管理者，不是那麼容易的，有關 window 2000 server 的設定和進階的認識，需要我一點一滴花時間去從新學習，不過，我自己的電腦一直撐不起 server 龐大的資源耗費，加上一時實驗室沒多的機器可以借我，在東借西借的努力之下才借到一台筆記型電腦，才能把相關的軟體灌好，才沒有不穩的情形出現，此時的金山正在使用 server－client 的機制，以丟 IP address 和 port 的方式進行傳送，不過，在一切都弄好的同時專題的另一端出了問題，學長堅持要我們使用某一個函式去寫程式，不過，那方面的資料並不是太多，我一連在圖書館裡找了好幾天的書，才找到相關的程式和資料開始著手寫程

式，在寫完程式之後移植程式到 Free BSD 的環境之時，才發現學長當初的堅持並沒有做過評估，作業系統本身並不支持這一個函式，之前寫的程式沒辦法使用，所以在花了許多時間完成的程式必須重寫，而我本身在防毒軟體那邊的測試又要往後延，金山也花了好一段時間程式改用 JAVA 實做，終於把程式寫好也同時可以來做防毒軟體的設定測試，雖然我對舊系統的功能有七八成的把握，不過，卻還是發現信件一直沒辦法送過去的問題，所以學長要求說要換系統，換成新板的防毒系統，距發表的日子越來越接近，我換系統所剩下的時間只剩下不到三個星期，過來我每一天一沒課就一直在實驗室裡做新系統的設定和了解，這一次有學長從防毒軟體公司拿回來的安裝設定的書籍，不過，新板的系統比舊有的系統功能強上許多，短時間要上手真的很急迫。多虧 逢甲大學 系統維運組 系統工程師 葉國樑先生 和趨勢公司 IMSS 部門 的技術人員，的幫忙，讓我在短時間內可以知道舊系統和新系統的差異，更了解一些內部基本的觀念，利用 DNS 的權限將寄至主機的信件導向防毒軟體的主機上進行防護，在短短一個星期內我才上手，偏偏另外一台機器又發生問題，無法正常運作，必須重灌，之前安裝好的程式，也必須重新安裝。

有關於「內容過濾及信件派送」這個部份，在一剛開始的時候，由於對於整個系統架構的不瞭解，因此陷入了膠著不前與迷思之中。

一再的嚐試，卻是一再的原地踏步，完全沒有進展。

直到確定了整個架構，包括處理流程以及各個處理方式，才能夠突破先前的困境，一步一步的完成這個部份。

剛開始的時候，我並不知道我的內容過濾部份是要去哪邊收信，也就是說無法確定要在哪個路徑之下去收已經掃完毒的信件，在跟其他的組員討論之後，瞭解了 IMSS 在掃完毒之後是怎麼把信送回來的，也知道了要去哪邊拿取已掃完毒的信件，因此就這樣解決了內容過濾的信件來源的問題。

另外，在信件派送的方面，由於對於email address的"@"之後的domain name 判斷收信者的身份並不是很清楚，也拖了一段時間才與相關人員探討這方面的問題。相關人員在瞭解了我的問題之後，回去也將判斷規則詳細說明的內容，以 email 的方式寄給我。也因此讓我能由收信者的 Email Address 來判斷要先將該信件覆製到哪個暫存資料匣，再由該暫存資料匣做後續的處理，例如：加解密、壓縮、解壓縮、傳送或續傳…等等後續動作。以完成該封信件的傳送工作。

由這個小地方可以得知，不管是多麼細節的地方，都必須很小心注意的確立與訂定規格，不然在實作的時候，一定會碰到模擬兩可、模糊不清的狀況，而導致沒有辦法順利完成。

第六章　參考資料

[1] 精通 windows 2000 server 網路規劃及架設篇 中文板

Mark Minast / Chista Anderson / Brian M. Smith / Doug Toombs 原著

陳玄玲 / 許皓翔 編譯　松崗出版

[2] Unix 系統程式設計

David A. Curry 原著

蕭伯剛 編譯　松格出版 O’ REILLY

[3] TCP/IP 網路管理

Craig Hunt 原著

王旭 編譯　O’ REILLY 出版

[4] sendmail 安裝管理

Bryan Costales / Eric Allman 原著

汪若文 譯　O’ REILLY 出版

[5] qmail 快速入門

Richard Blum 原著

張世敏 譯　博碩出版

[6] DNS BIND 網路管理

Paul / Cricket 原著

松格出版　O’ REILLY 出版

[7] 資傳網 http://infopro.com/

[8] msdn http://msdn.microsoft.com/default.aspx

[9] O’ REILLY http://www.oreilly.com/

[10] SEND MAIL http://www.sendmail.com/

[11] SOPHOS http://www.sophos.com/

[12] TREAD http://www.trendmicro.com/tw/home/enterprise.htm

[13] **OPENFIND** http://www.openfind.com.tw/

[14]人民網 http://www.people.com.cn/

[15] CNET 新聞專區 http://taiwan.cnet.com/news/

[16]奇摩新聞 http://tw.news.yahoo.com/

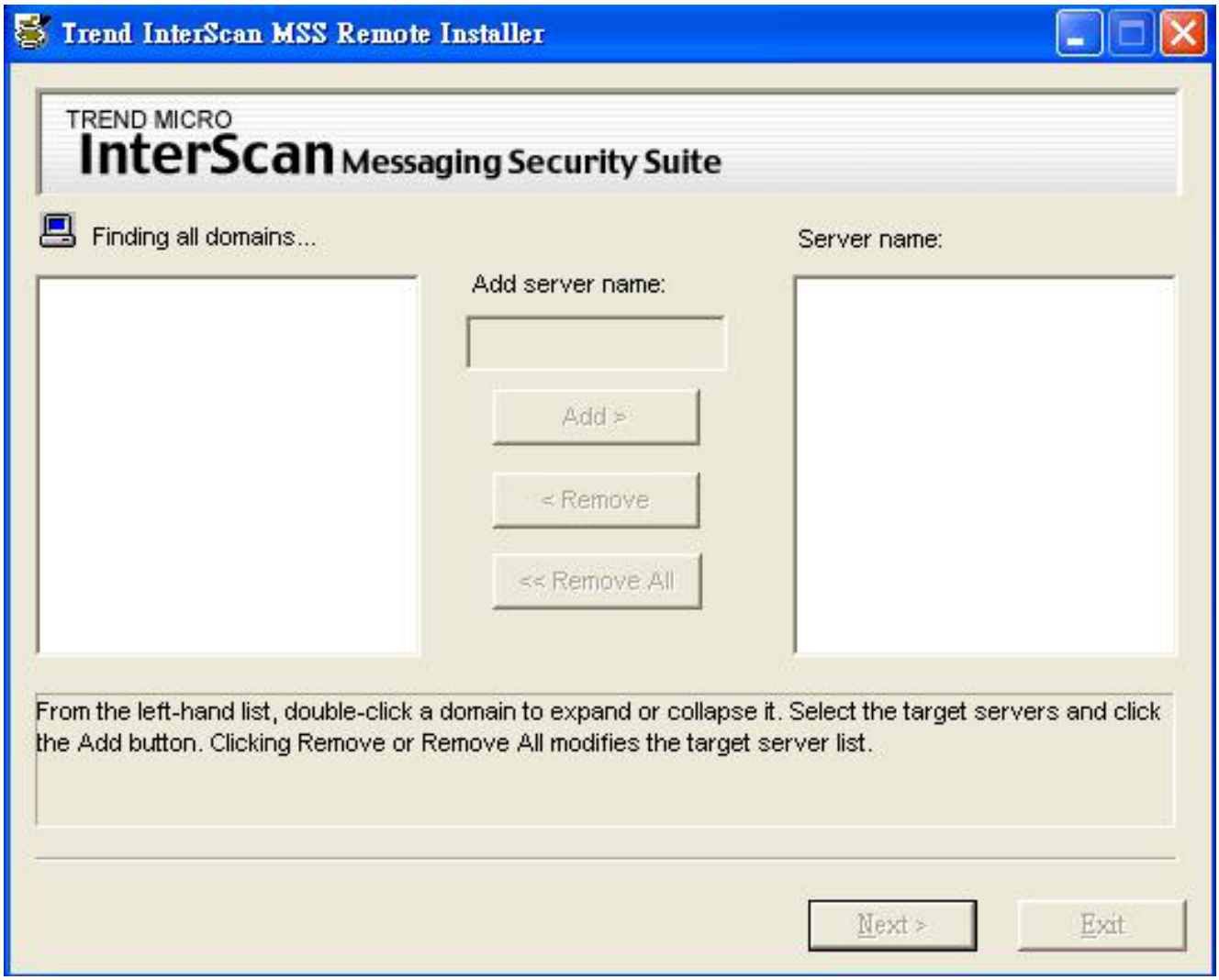
[17] CIO 資訊傳真周刊

[18]資訊安全通訊雜誌

第七章　附錄

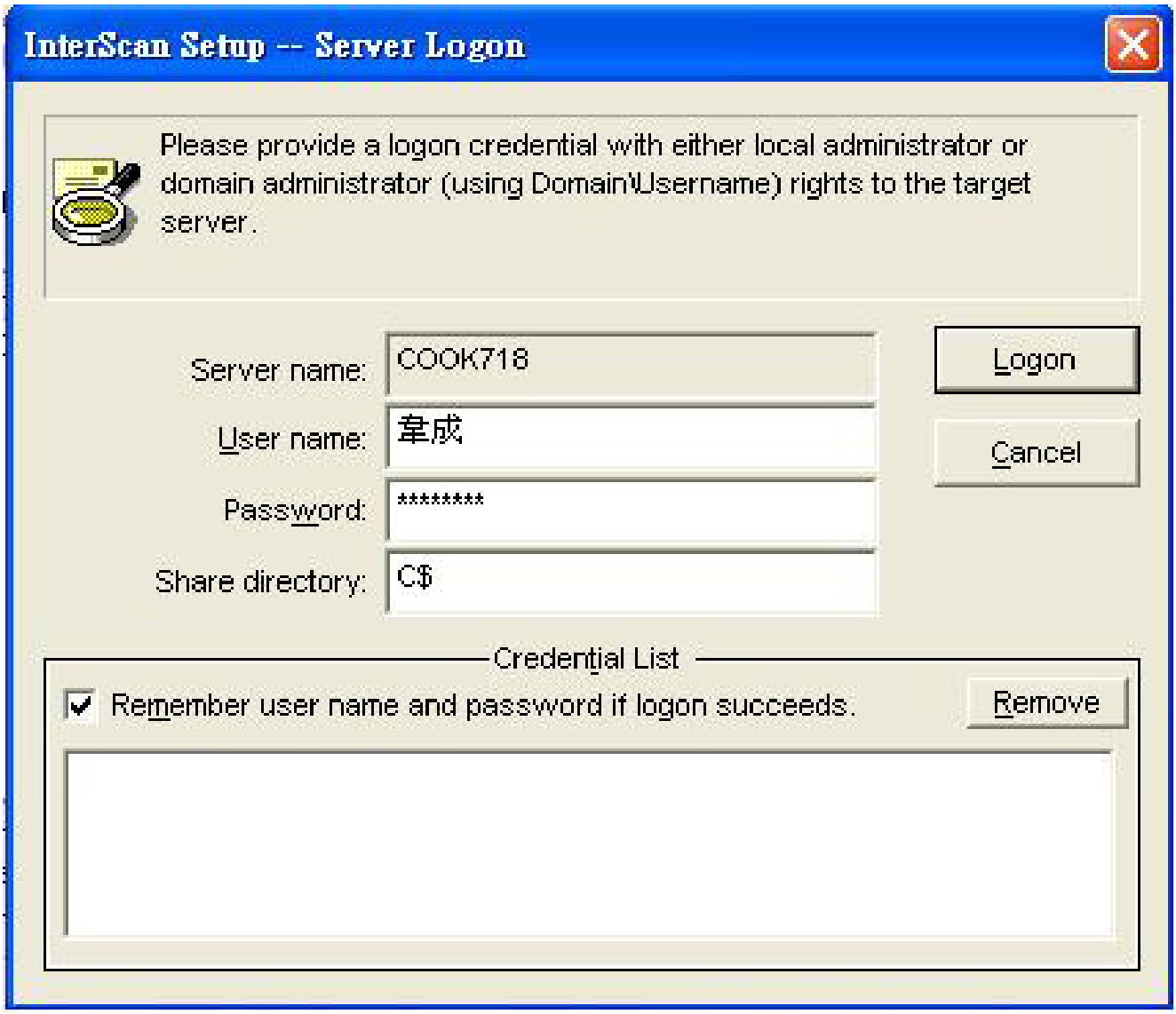
附錄一　IMSS 的安裝與設定

針對整個網域做搜尋，找尋網域上所有群組及電腦。

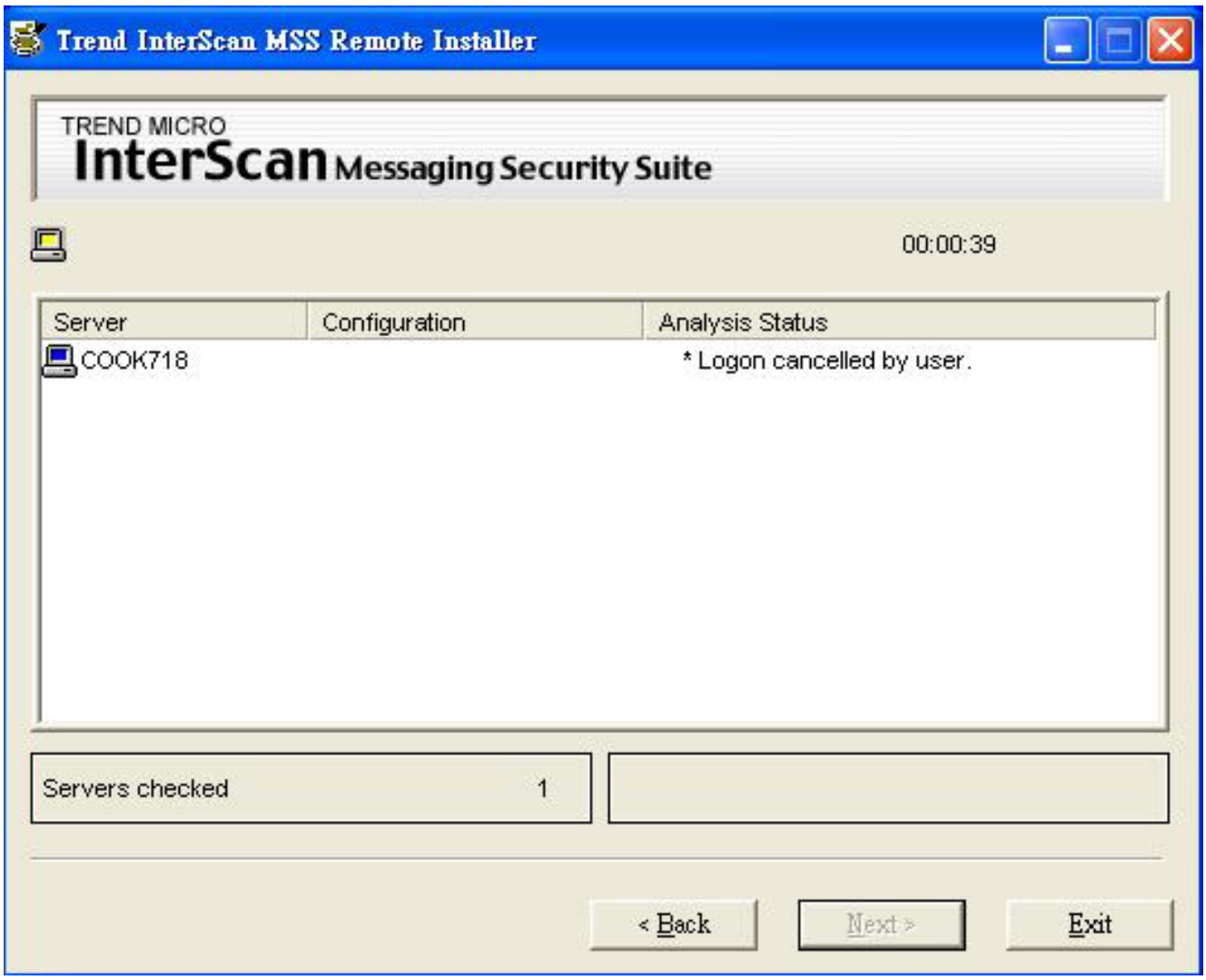


點選要安裝的主機(可以同時遠端安裝多台主機)。

在安裝主機之前，會要求你輸入主機的管理帳號和密碼並且把 C 槽 share 出來。

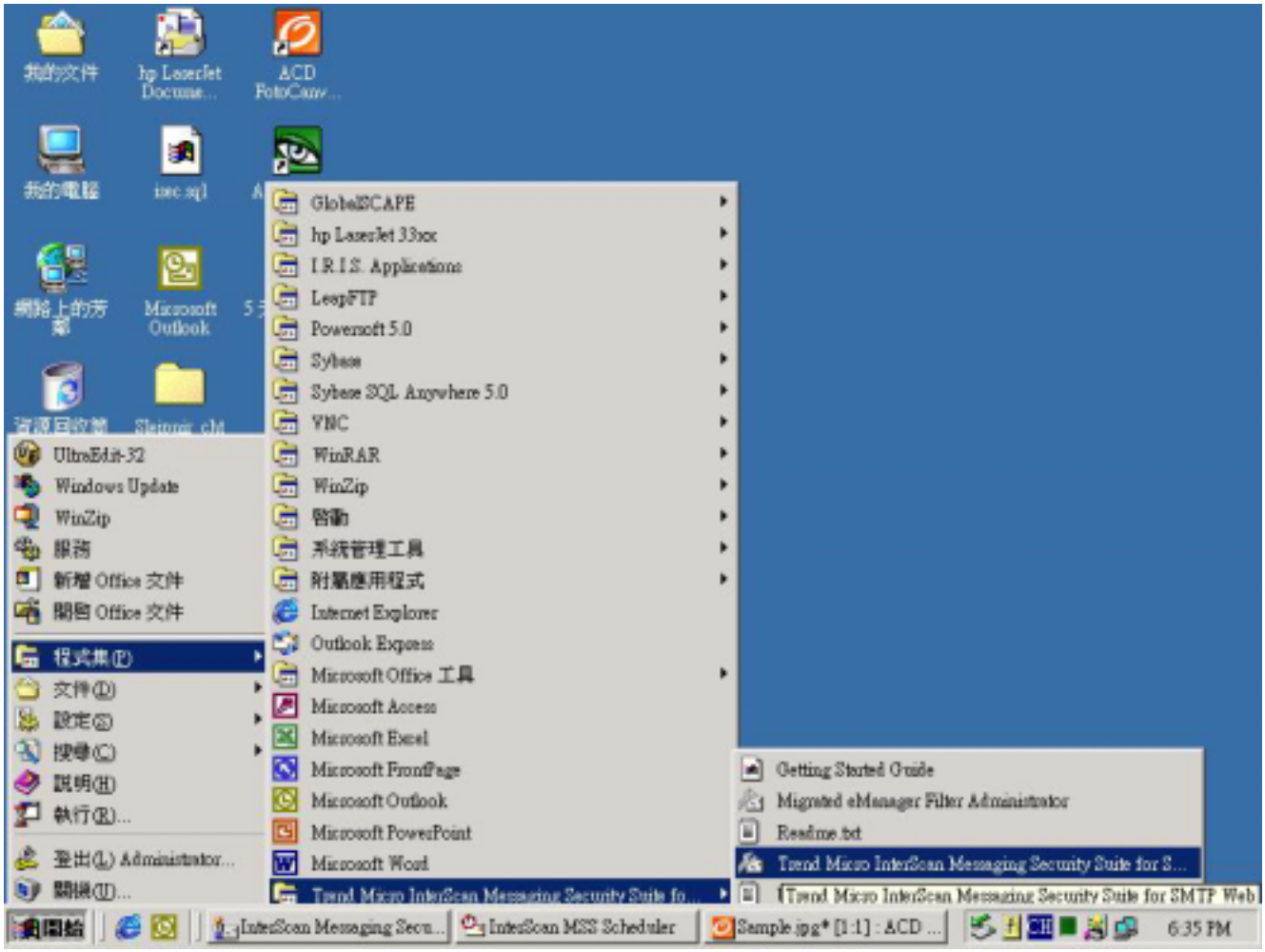


正在安裝中。

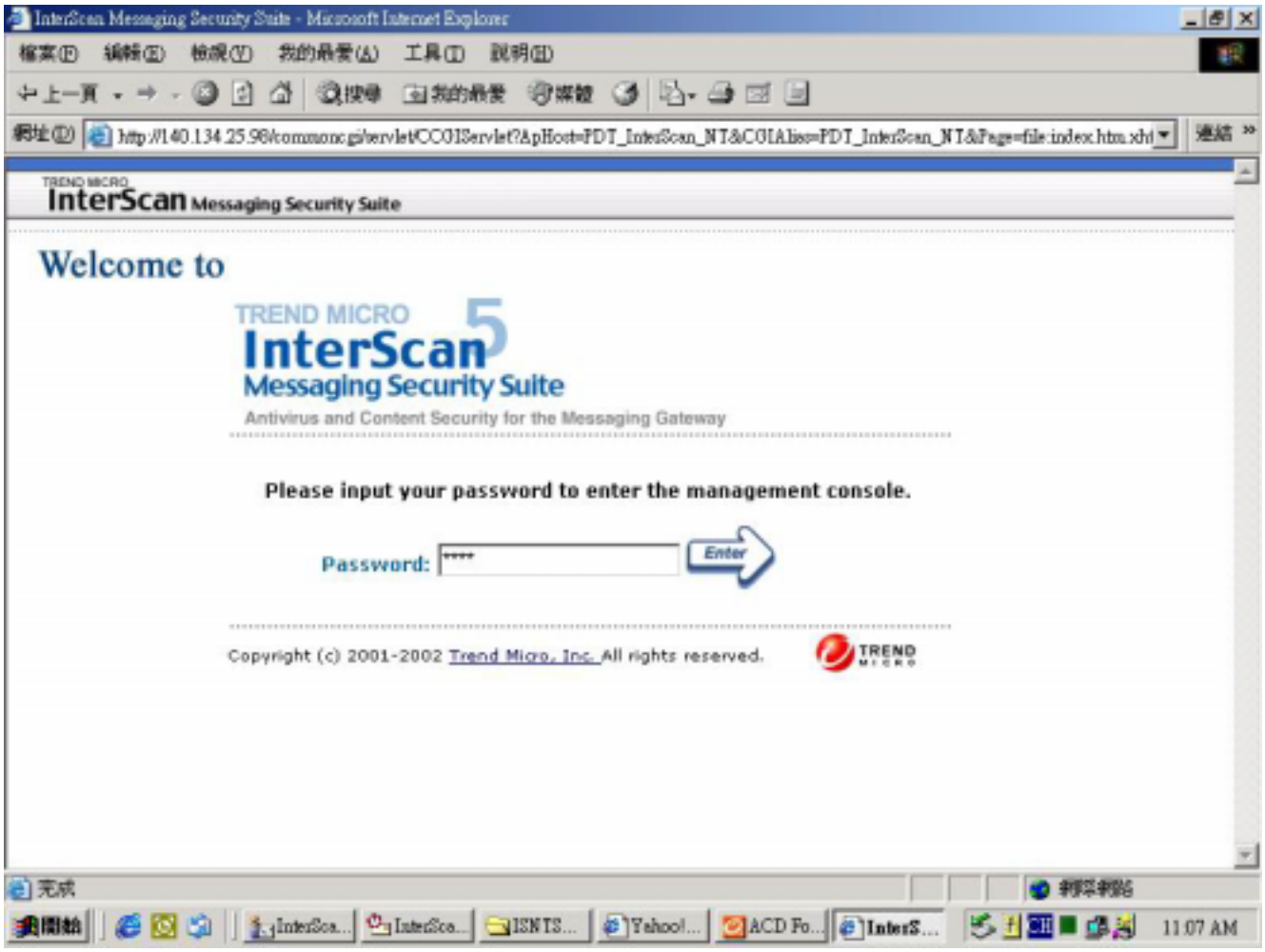

Trend InterScan MSS Remote Installer
TREND MICRO
InterScan Messaging Security Suite
00:00:39
Server
Configuration
Analysis Status
COOK718
* Logon cancelled by user.
Servers checked 1
< Back
Next >
Exit

安裝軟體完成之後，進入管理控制台或是

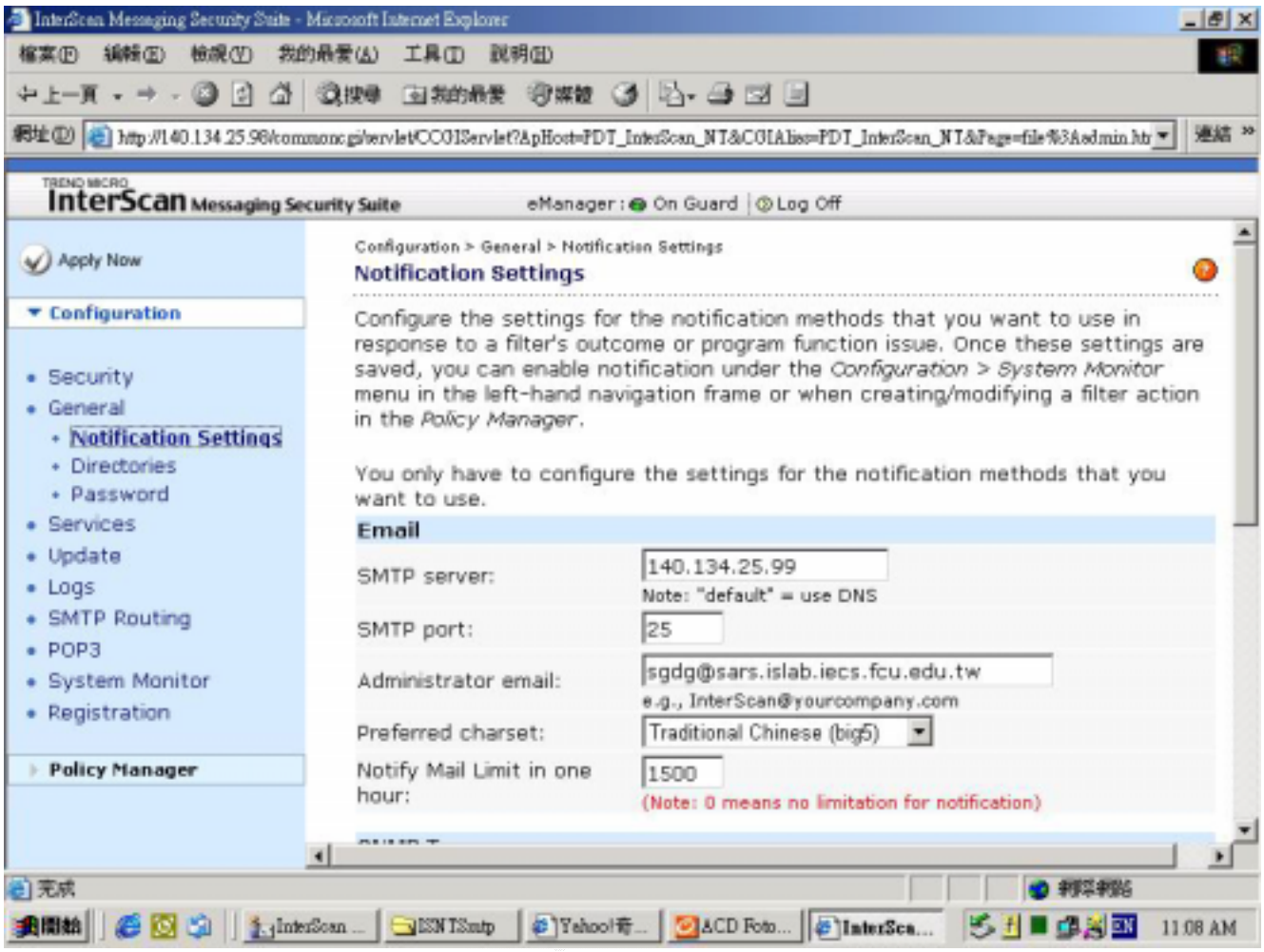
http://<target server's IP address>InterScaMSSConfig.html 。



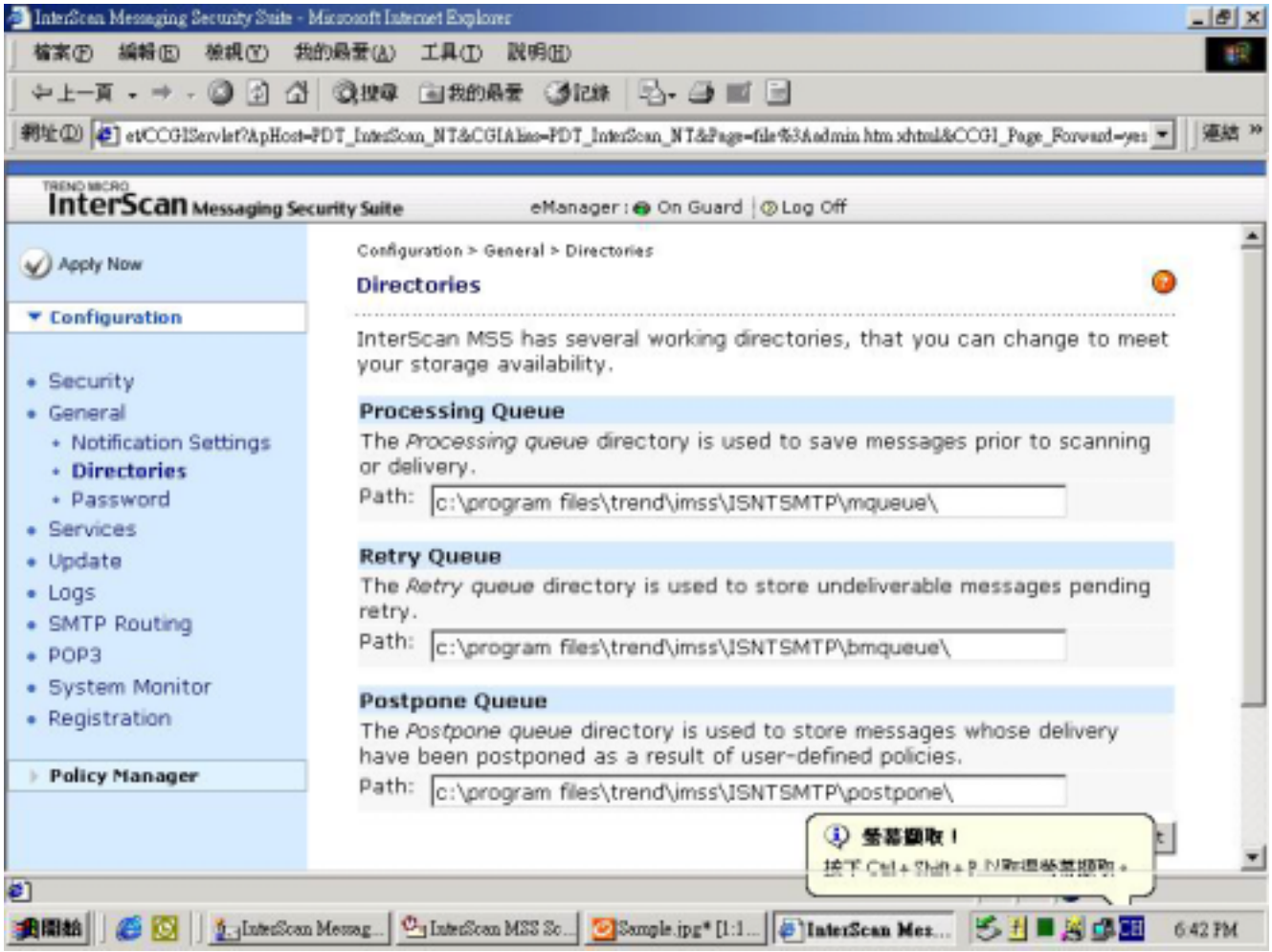
過來就是進到整個防毒軟體的內部設定，當然需要 IMSS 管理者才能進去。



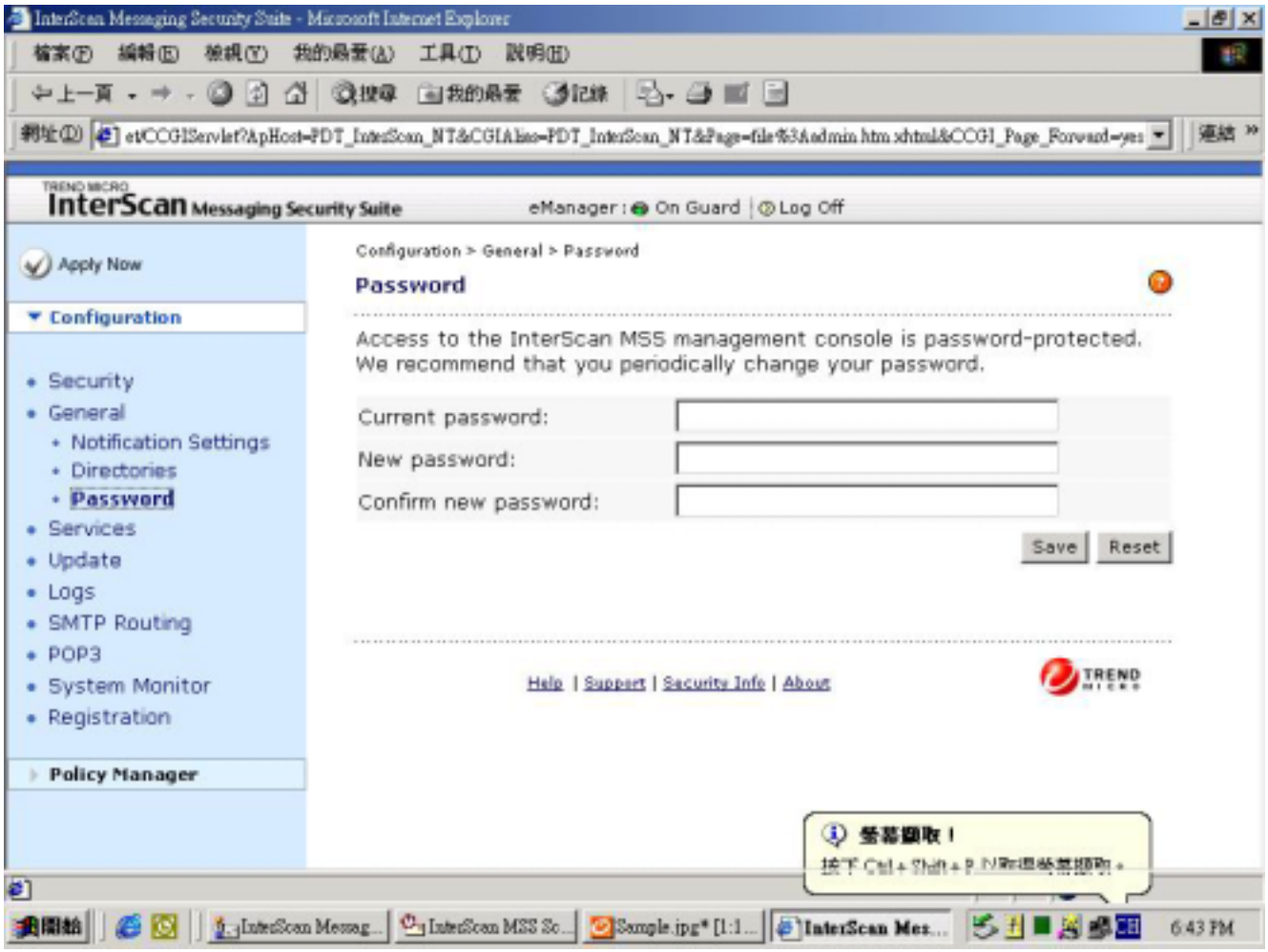
設定 SMTP 的 IP address 和 Port 及管理者信箱。



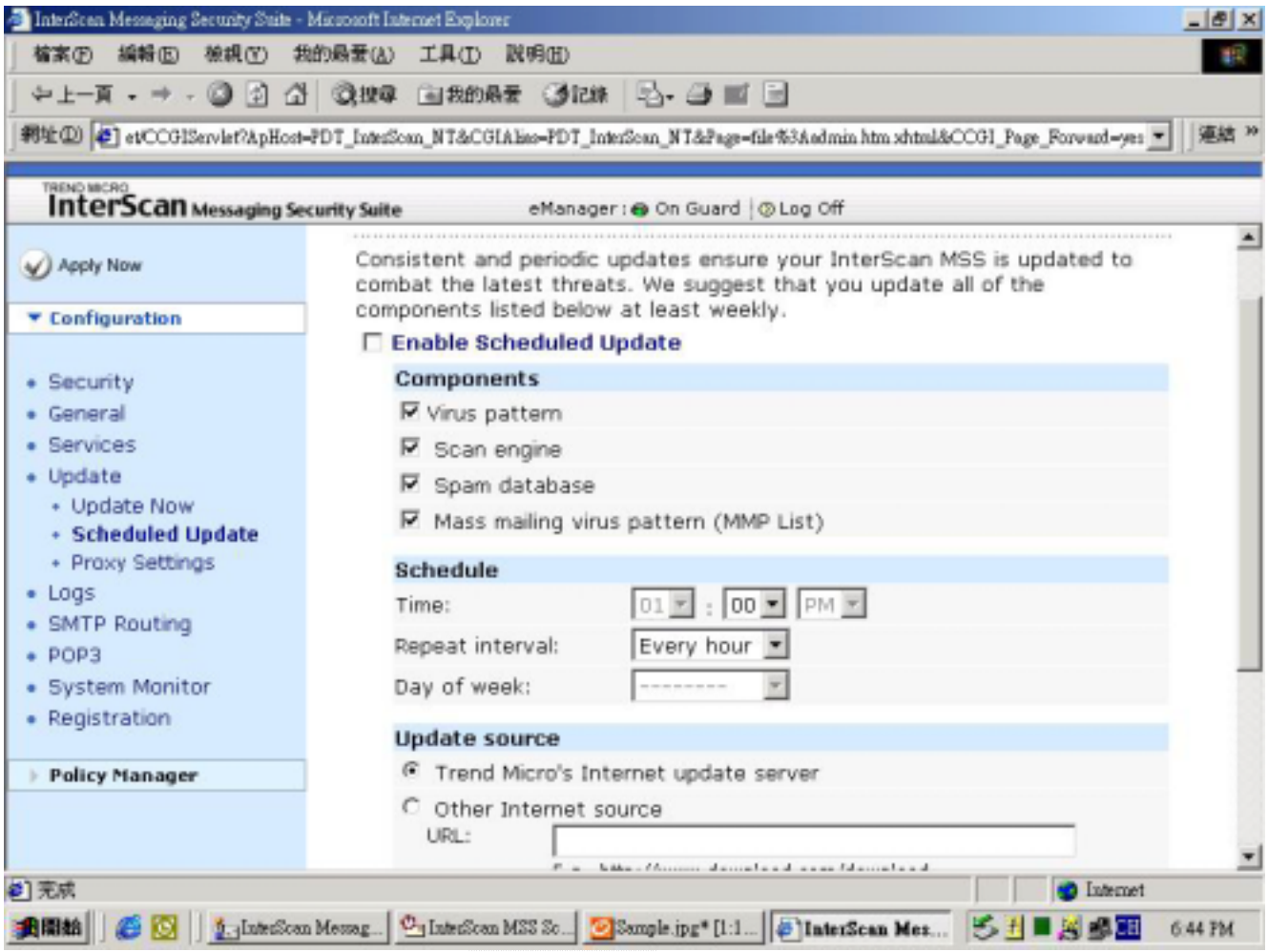
這三個資料夾，分別是 mqueue、bmqueue 和 postpone，是 IMSS 用來存放剛收下的郵件和不能傳遞的郵件及稍後傳送或有特殊規定的郵件。



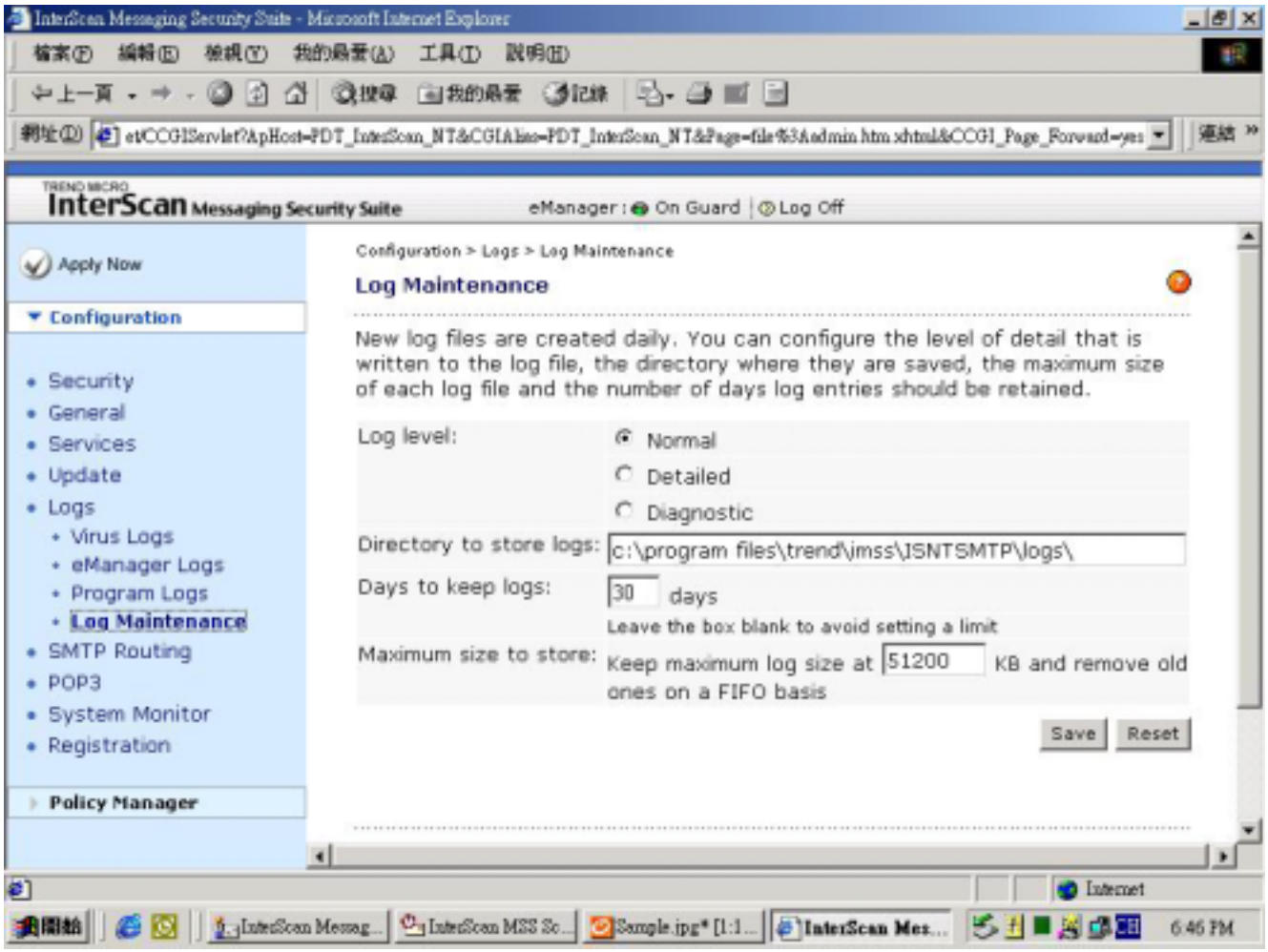
IMSS 一開始並沒設定密碼，所以管理者必須在第一次進入系統之後，把系統密碼設定好。

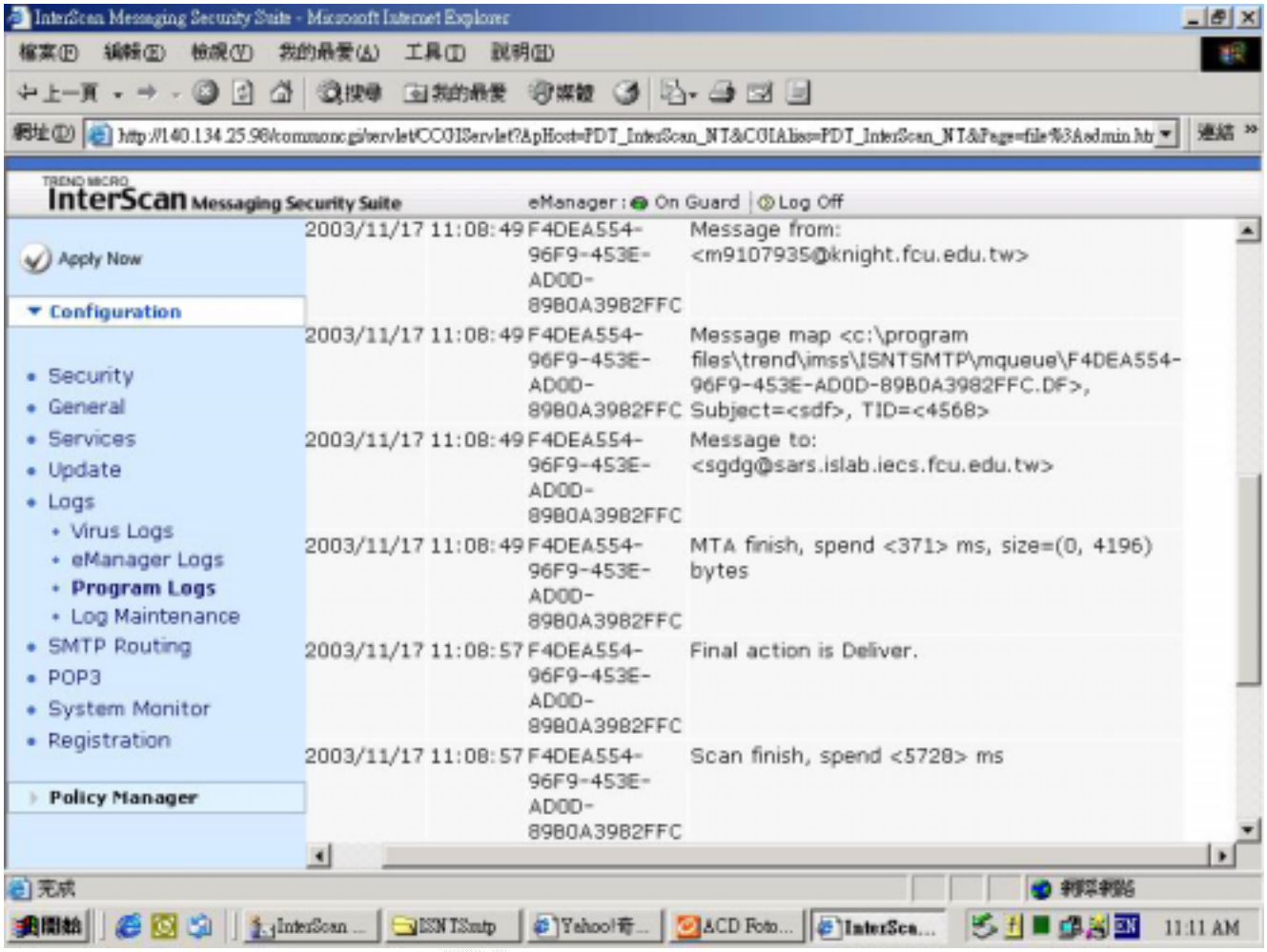


選擇要更新的 pattern，和更新的日期。

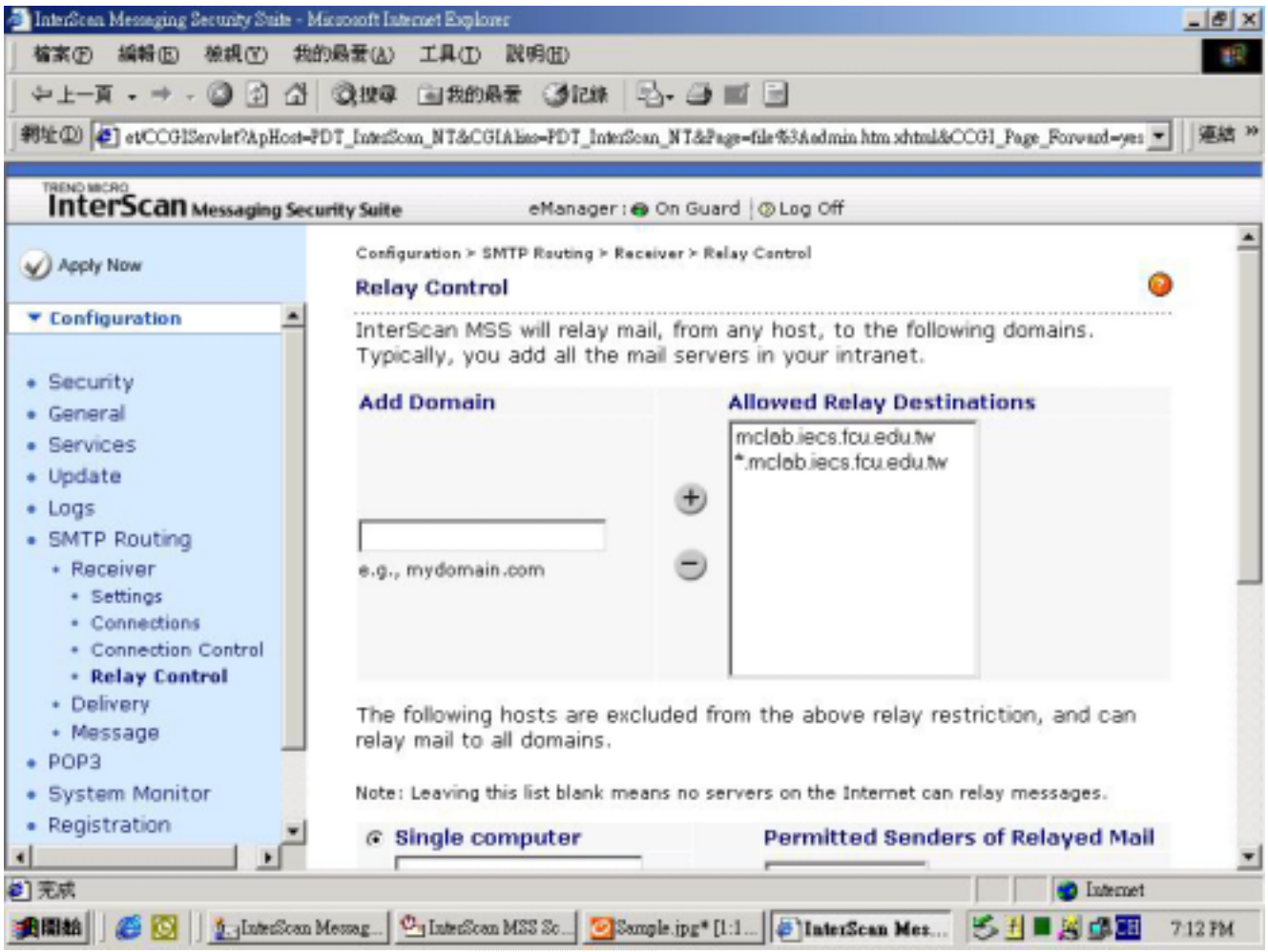


這邊是 log 檔的部分，可以從這邊看到有關 Virus pattern 和郵件的收發是否正常及問題出現在那。

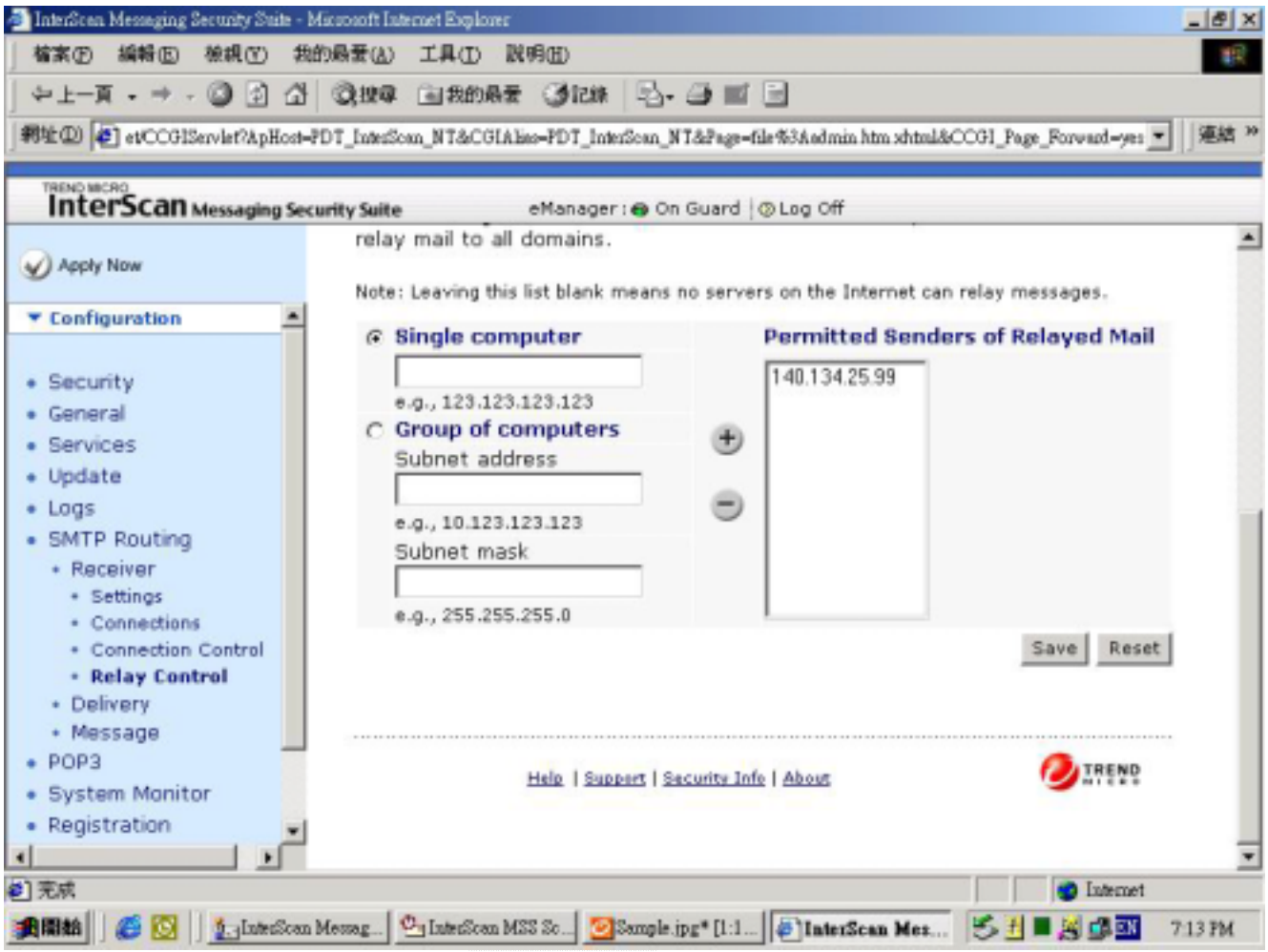



InterScan Messaging Security Suite - Microsoft Internet Explorer
InterScan Messaging Security Suite
eManager : On Guard | Log Off
Apply Now
Configuration
Security
General
Services
Update
Logs
Virus Logs
eManager Logs
Program Logs
Log Maintenance
SMTP Routing
POP3
System Monitor
Registration
Policy Manager
2003/11/17 11:08:49 F4DEA554-96F9-453E-AD0D-89B0A3982FFC Message from: <m9107935@knight.fcu.edu.tw>
2003/11/17 11:08:49 F4DEA554-96F9-453E-AD0D-89B0A3982FFC Message map <c:\program files\trend\imss\ISNTSMTP\mqueue\F4DEA554-96F9-453E-AD0D-89B0A3982FFC.DF>, Subject=<sdf>, TID=<4568>
2003/11/17 11:08:49 F4DEA554-96F9-453E-AD0D-89B0A3982FFC Message to: <sgdg@sars.islab.iecs.fcu.edu.tw>
2003/11/17 11:08:49 F4DEA554-96F9-453E-AD0D-89B0A3982FFC MTA finish, spend <371> ms, size=(0, 4196) bytes
2003/11/17 11:08:57 F4DEA554-96F9-453E-AD0D-89B0A3982FFC Final action is Deliver.
2003/11/17 11:08:57 F4DEA554-96F9-453E-AD0D-89B0A3982FFC Scan finish, spend <5728> ms

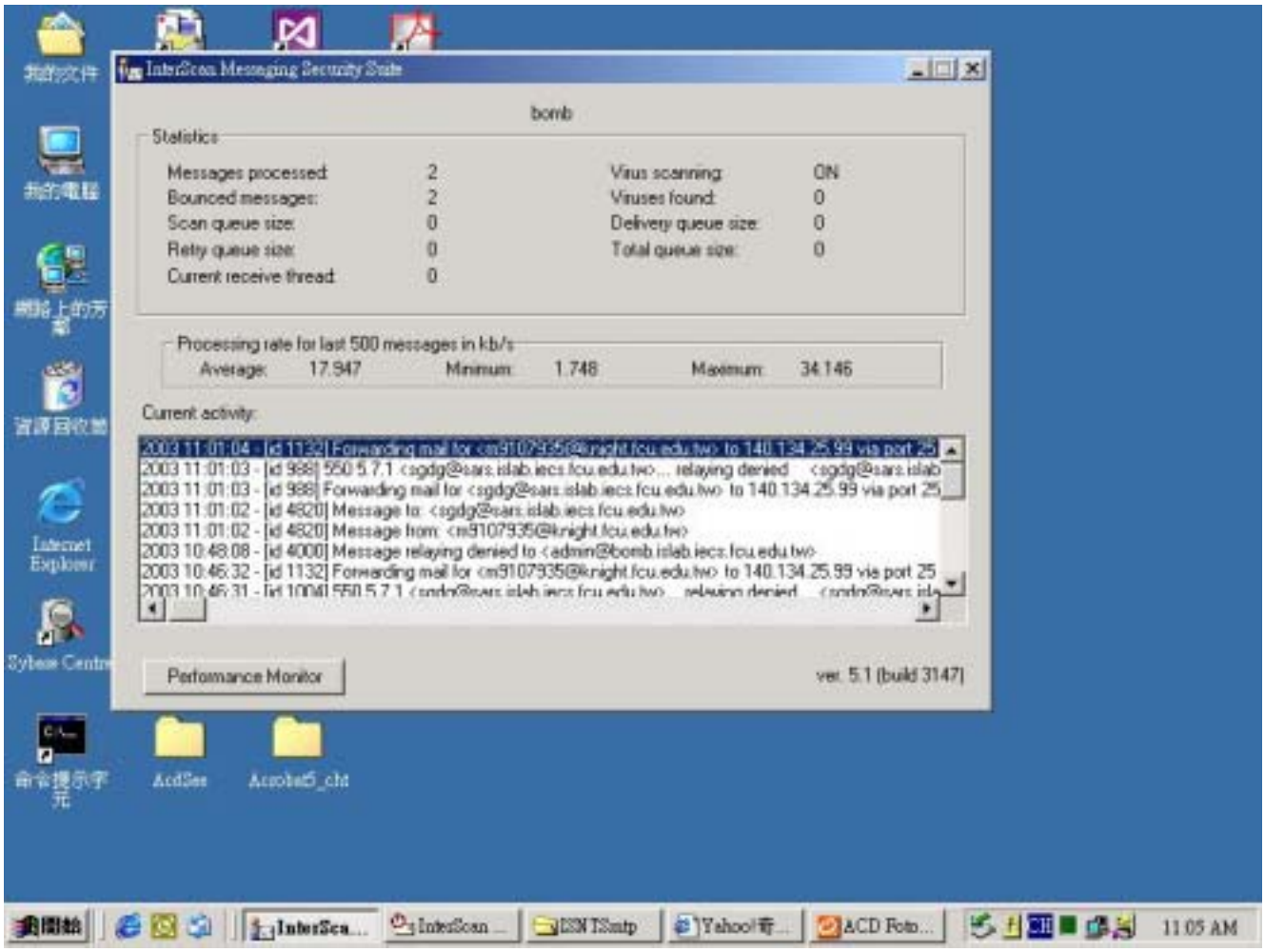
設定要郵件收集的網域，以便 IMSS 判斷來源。



設定掃完病毒郵件傳送的主機。



出現在桌面的訊息視窗，會把收發的郵件記錄以精簡的訊息呈現出來。



附錄二　郵件轉換站記錄(Mail Exchanger Record)

DNS 在郵件遞送上提供了一個用來詳細記載主機位置的備份機制。這個機制也允許主機來確信對於其他主機的郵件處理責任。這使得沒有磁碟機的主機能夠經由其他的伺服器來提供郵件地址，而不需要執行寄郵件的程式。DNS 使用了逼個單一的資源記錄的型態來實做增強式的郵件繞路法，也就是 MX 記錄。早期，這個功能是分成兩個記錄，MD(mail destination)和 MF(mail forwarder)兩個組成。MD 記錄詳細記載了最終目的的主機，也就是該訊息所記載要接收的主機位址，MF 記錄則記載了要將郵件送到最終目的地的一個主機名稱。不過，寄件者必須同時要知道兩個記錄，缺一不可，那也代表執行寄郵件程式所花費的系統負擔會比執行其他的服務程式來的高上許多，所以，爲了解決這一個問題，它將這兩個記錄合在一起變成 MX 記錄。現在，寄郵件程式只要某一個特定目的地的網域名稱的所有的 MX 記錄，便可以使用路由法來決定傳送路徑。同時爲了避免出現電子郵件繞路迴圈(mail routing loops) ，因此在 MX 記錄之中加入了一個額外的參數，一個優先權的值(也有人用成本來形容) ，這一個優先權是一個無號的 16 位元的數字(0 ~ 65535) ，它用來代表該電子郵件交換器的優先權，數字越小優先權越高(也可以詮釋成所花的成本越小的越先傳送)。以下是 MX 的格式：

[name][ttl] IN MX preference host

name

主機或網域的名稱，也就是郵件地址所寫的地方，把它想成郵件地址@符號後面的部分，寫給這個名稱的郵件，會被送到指定的郵件伺服器。

ttl

存活的時間，通常是空白。

IN

位址類別是 IN。

MX

郵件轉換站記錄的類別是 MX。

preference

與某一個主機或網域有關的 MX 記錄可能不只一個，preference 欄位指定嘗試這些郵件伺服器的順序，preference 數值小的伺服器先試。所以最受歡迎的偏好值是 0，通常一次增加 5 或 10，這麼一來，新的伺服器就可以插入現有的伺服器之間，而不用更改之前原來的 MX 記錄。

host

郵件伺服器的名稱，寫給 name 欄位裡的主機或網域的郵件，傳送到這個郵件伺服器。

舉幾個例子來說明：

testone.com.tw IN MX 0 relayone.com.tw
testone.com.tw IN MX 1 relaytwo.com.tw

它說明了 relayone.com.tw 是 testone.com.tw 的一個郵件交換器，而它的優先權的值是 0 ，凡是寄到 testone.com.tw 的電子郵件會先轉送到 relayone.com.tw 去，如果不能傳送過去，會看 MX 記錄，將郵件轉到 relaytwo.com.tw。