HTTP 隱藏通道之安全性探討

作者/夏伯倫少校

提要

近年來網路攻擊的手法已不再像從前，由網路閘道器正面的向前刺探進而突擊入侵，由於網路安全防禦的觀念已普及於單位的資安政策當中，惡意的攻擊者想要正面進攻已有相當的難度，內部使用者就算被植入後門也因為單位的防禦縱深的保護，攻擊者也難以進行遠端連線遙控，攻擊者的手法也因此改變了原有的思考邏輯，改由內部使用者透過許可通行的服務來向攻擊者報到，藉以躲避單位的防禦機制。

一般來說，系統管理員會為了保護單位或企業內部網路，在與內部區域網路與外界互聯的地方放置一個或多個防火牆，用以保護及控制網內外用戶所能使用的服務，例如僅開放使用HTTP 服務，關閉所有其他可能較危險的應用服務，這也是目前許多單位防火牆所制定安全政策之一，但這能確保只有HTTP 的服務在執行嗎？若將將欲傳輸的情資，摻雜於合法的封包中，以合法掩護非法的通訊管道以掩人耳目[1]，所以這種隱藏通道的使用就是一個安全上的隱憂，能夠區別正常的HTTP連線及使用HTTP 隱藏通道，也就是本文所要討論的。

壹、緒論

一、研究動機

設置網路安全防禦機制，是每個單位必須的建置項目，系統管理者也不敢輕忽安全防護的重要性，但每當發生有單位被惡意攻擊者入侵成功並竊取重要情資時，常常聽到使用者在抱怨明明防火牆已經做好限制、防毒軟體也正常運作、入侵偵測也佈署完善，那為什麼還會被入侵，還會被植入後門被人遠端遙控等等的疑問，一般來說可能的方法有利用系統弱點攻擊主機，如不當的權限設定、RPC 等弱點；利用程式撰寫不當攻擊主機，如 SQL Injection、BufferOver Flow 等弱點；利用社交工程方法攻擊 End User，以電子郵件引誘法誘使 user 開啟惡意附檔植入後門程式，或誘使 user 瀏覽惡意網站植入後門程式等等，但試想就算被植入後門，駭客也連不進來內部網路來遙控電腦啊？防火牆不是已經

[1]方仁威，余俊賢，「內部網路遭駭客攻擊方式與防護之研究」，國防通信電子資訊半年刊，第七期，2004 年。

擋掉了嗎？這就有可能攻擊者所用的方法，是單位或系統所許可的服務之一，如網站 WEB 的連結。

在網際網路上最常使用的應用服務就是 WWW，而所使用的協定為 HTTP，在許多的防火牆政策制定上，由內而外使用 WWW 這項服務的存取大多是被允許的，也因為如此常被管理者所忽略，如此就產生了使用 HTTP 隱藏通道的方法，來欺騙防火牆達到其目的，運用隱藏通道技術將其他應用服務隱藏在 HTTP 之中，讓防火牆以為是在使用 WWW 的存取服務進而放行。

對於系統管理者這是一個嚴重的安全隱憂，因為管理者通常不會去特別注意組織內的使用者存取 WWW 的服務，防火牆也不會有異常的警訊，因為這是被允許的服務之一，所以能夠從 HTTP 連線中發覺異常現象，產生適當的訊息提醒管理者，就很重要了。

二、研究目的

藉由實際運用 HTTP 隱藏通道的連線方式，紀錄並分析其流量的特性，以其能發覺區別正常的 HTTP 連線及使用 HTTP 隱藏通道的方法，並對此種手法提出建議的解決途徑，這也就是本研究主要的目的。

三、研究方法與架構

依據行政院國家資通安全會報之資訊安全管理系統及美國國家標準技術研究院，所提出之資訊技術安全[2][2]，進行研討。

(一)資料蒐集：蒐集隱藏通道系統運作方式及目前主要運作其原理的程式。

(二)系統建立：建置多樣運用隱藏通道之系統，例如 softether、http-tunnel 等軟體，經由實驗環境分析其封包。

(三)數據分析：經由網路行為模式分析出正常流量狀況，以及隱藏通道的流量狀況進行比對。

(四)實驗過程

1.在實驗中對於採用 HTTP 協定的服務做測試，包含一般網頁連線、網頁式電子郵件系統 Webmail（收/發信件）及具有 SSL(Secure Socket Layer)加密的網頁連線、網頁式電子郵件系統 Webmail（收/發信件）。

2.在實驗中對於採用 HTTP 隱藏通道技術的服務做測試，測試使用 FTP 檔案傳輸協定及 TELNET 遠端登入協定。

3.實驗結果比對分析。

[2]台灣網路危機處理暨協調中心(www.cert.org.tw)，「資訊安全的發展」，https://www.cert.org.tw/document/column/show.php?key=64，August 2003。

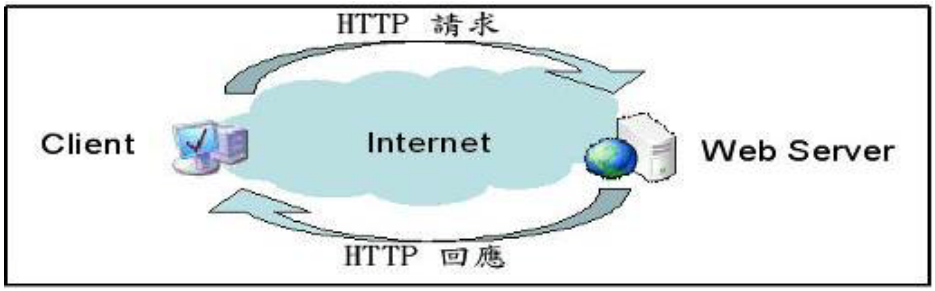
貳、本文

一、定義

在分析正常的 HTTP 連線及使用 HTTP 隱藏通道之前，先要對其特性具有一定程度的了解。

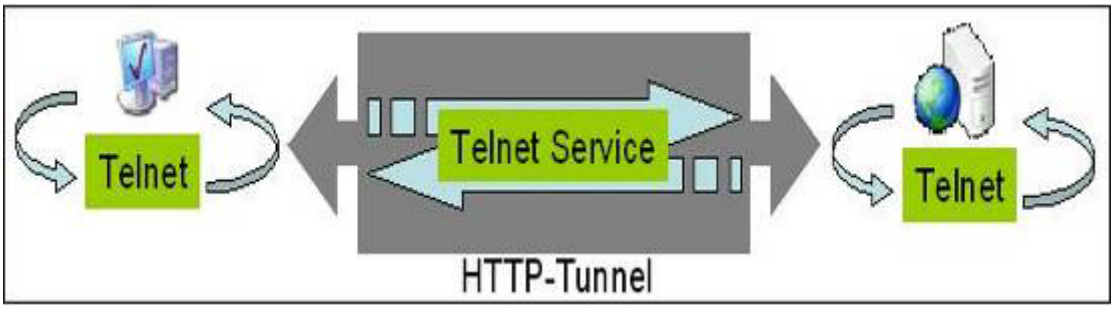
WWW 中最主要的通訊協定，就是 HTTP 協定。超文件傳輸協定（HyperText Transfer Protocol，HTTP）是 Web 的應用層協定，並且是 Web 的核心部分。它是由[RFC 1945]和[RFC 2616]所定義。由於 WWW 是一種以主從式（Client/Server）為架構的大型網路，也就是有所謂的伺服端和客戶端，而主從式架構需要在兩者之間作一些協定才能讓資料得以傳輸。用戶端程式和伺服器端程式會在不同的終端系統上執行，並且藉著交換 HTTP 訊息來相互通訊。常見的 Web 伺服器包括 Apache 和微軟的 IIS。HTTP 跟 FTP 一樣，都是用來在客戶端與伺服器端互傳資料的通訊協定。與 FTP 最大的不同在於 HTTP 採用了一種無記錄狀態（stateless）的設計，意思是說每次的通訊內容都是獨立的，不需要像 FTP 要先登入使用者帳號跟密碼才能把檔案傳回來。採用這種無記錄狀態的技術有個最大的好處就是伺服器端的設計比較簡單，而且可以快速的處理更多的服務請求。WWW 客戶端軟體（也就是瀏覽器）就利用了這個特性，一次使用多個執行緒（Thread）來開啟多個連線，使得在相同頻寬的條件下，使用者可以比較快的看到文件的各部份。

不同的服務（如 Ftp、E-mail、Telnet、Gopher 等）就必須有不同的 Server 或 Server 軟體來相對應，而 HTTP 也不例外，像是 WWW 就必須要有 HTTP 伺服器。瀏覽網頁時，會在網址列上打上「http://xxx.xxx.xxx」，這就是所謂的 URL，也稱作「網址」，可以說是 WWW 中某台伺服器的位置所在，當使用瀏覽器發出一個要求瀏覽某網頁的訊息後，透過 URL 的資料定位找到這台伺服器，而 HTTP 協定也在同時起了作用，因為 WWW 中的伺服器支援 HTTP 程式，而使用者所使用的瀏覽器也支援 HTTP 程式，所以當此一傳輸協定達成，伺服端便會將所需的網頁資料提供給使用者（如圖一）。



圖一 HTTP 請求/回應的行為模式

而本文所提的通道是指一種在通訊模式中能夠偽冒另一種通訊模式。一端的通訊數據封包在另一種通訊模式上，然後與對端通訊，當封包的數據到達對端時，再將數據封包還原，並將還原後的數據交送到相應的服務上。舉例如下：A主機系統想以Telent 方式到B主機系統上，這個時候若使用Http-tunnel技術[3][3]，在A機器上將Telent client數據封包指引到遠端B主機的 80 埠上，在B主機上指引 80 埠的來自client的數據封包轉發到本機的Telnet server的 23 服務埠上，當數據封包需要由B主機到A主機返回時，同樣由 80 埠再回送，如此就是利用Http tunnel來使用Telnet 的服務了（如圖二）[4]。



圖二 HTTP-Tunnel 連線使用 Telnet 的行為模式

二、實驗分析

實驗主要目的在利用正常HTTP 連線建立時，所產生的封包數量及大小，與使用HTTP-TUNNEL隱藏其他應用服務時，所產生的封包數量及大小比例之間的差距關係[5]。

在實驗環境中我們使用一般個人電腦來作為使用端的設備：CPU為Intel P4 2.0G、記憶體為 256MB、硬碟空間為 40GB、作業系統為Windows XP SP2，瀏覽器為Microsoft Internet Explorer 6.0，安裝Ethereal (version0.10.7)作為分析封包之工具[6]，來檢視基本HTTP 連線請求/回應的行為模式。

在HTTP-Tunnel實驗環境中，伺服器端的設備：CPU為Intel P4 2.0G、記憶體為 256MB、硬碟空間為 40GB、作業系統為Fedora Core 3，並採用Lars Brinkhoff的http-tunnel 3.0.5 的版本[7]，使用端則使用Tom Moses的http-tunnel Windows平台的介面[8]。

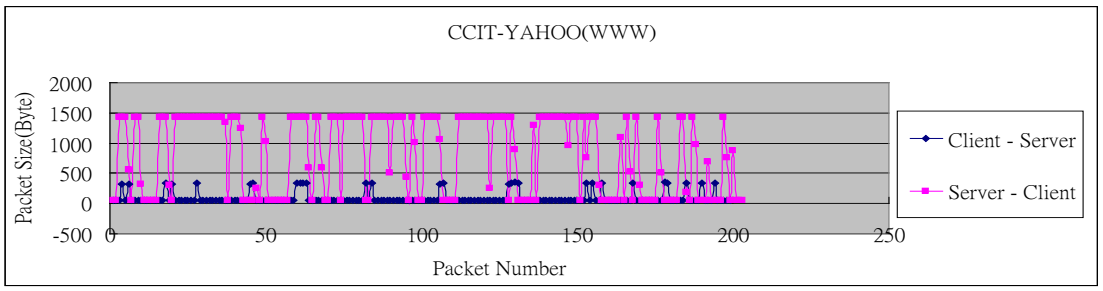
---

[3] HTTP-TUNNEL 網站，http://www.nocrew.org/software/httptunnel.html。
[4] 宮一鳴，「由 http 暗藏通道看網路安全」，http://www-900.ibm.com/developerWorks/cn/security/l-httpunnel/index.shtml#author1。
[5] Daniel J. Clark，“Backdoor Encrypted Tunnels: Detection and Analysis”， GIAC GCIA Practical，1 June 2003。
[6] Ethereal: A Network Protocol Analyzer，http://www.ethereal.com/download.html。
[7] HTTP-TUNNEL SERVER 端程式下載，http://www.nocrew.org/software/httptunnel/httptunnel-3.0.5.tar.gz。
[8] Tom Moses HTTP-TUNNEL CLIENT for Windows NT 程式下載，

(一)HTTP 連線封包流量分析

在實驗中對於採用 HTTP 協定的服務做測試，包含一般網頁連線、網頁式電子郵件系統 Webmail（收/發信件）及具有 SSL(Secure Socket Layer)加密的網頁連線、網頁式電子郵件系統 Webmail（收/發信件）。

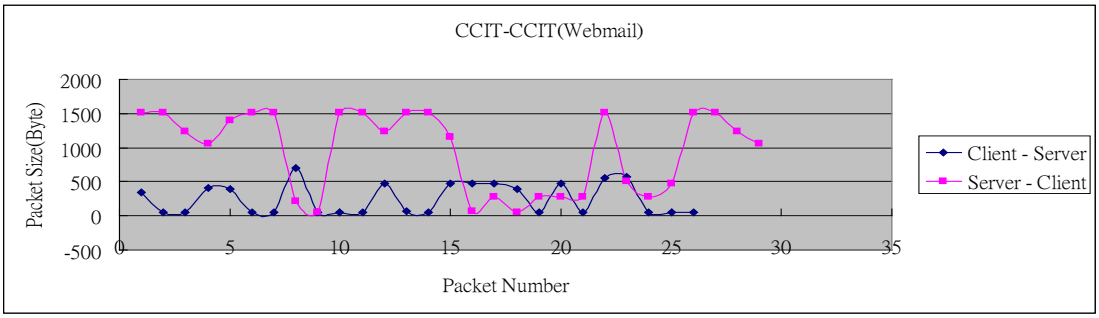
1.一般網頁連線請求/回應：在這個實驗中以台灣 Yahoo 奇摩網站的首頁(http://tw.yahoo.com/)作 為分析的目標。我們以瀏覽器連結 Yahoo 奇摩網站的首頁，從使用端提出請求到伺服器端回應完成，整個封包傳輸分析圖如圖三，圖中顯示使用端所傳輸的封包檔案大小，比較於伺服器端來的小，因為伺服器端會將網站的文字、圖片及多媒體檔案傳送給使用端，所以可以很明顯的看出伺服器傳送給使用端的封包檔案相對的較多。



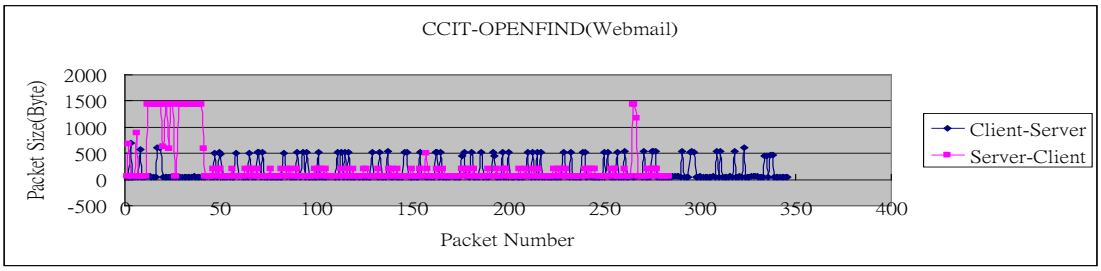
圖三　連接 Yahoo 網頁流量封包圖

2.Webmail 連線請求/回應：接下來以瀏覽器連結網頁型態的電子郵件伺服器，連結國防大學中正理工學院的 Webmail Server(http://webmail.ccit.edu.tw/nocc/)以及網景 Openfind Webmail Server(http://mail2000.com.tw/)的封包傳輸分析圖(如圖四、五)，圖四所顯示的封包數量較少，原因是國防大學中正理工學院的 Webmail 所呈現的網頁內容較簡單，並無太多圖形及文字，但仍可以看出伺服器端所傳給使用端的資料較多，其中可以初步描繪出 Webmail 的連線架構模式，首先使用者提出連線請求，第二伺服器回應，第三使用者輸入登入資料，第四伺服器驗證成功並提供資訊等等。而圖五所呈現的連線架構仍不脫基本模式，只不過因網景 Openfind Webmail 網頁所提供資料較多圖文，所以獲得較多的封包數及檔案。基於此種連線可以歸類成一個 Webmail 的連線模式如圖六。

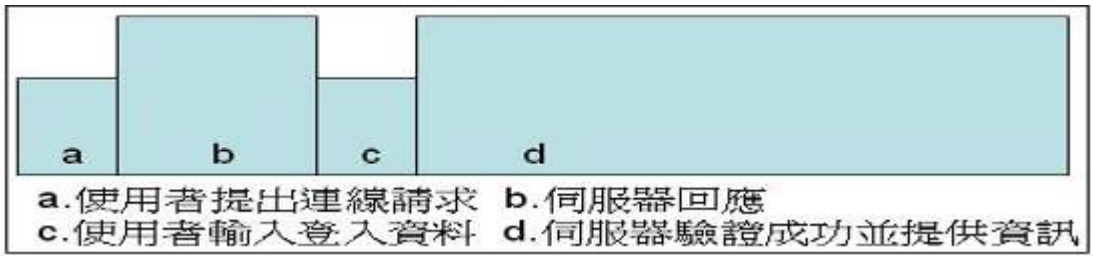
http://userpages.umbc.edu/~tmoses1/hypertunnelNT.zip。



圖四　連接中正理工學院 Webmail 網頁流量封包圖

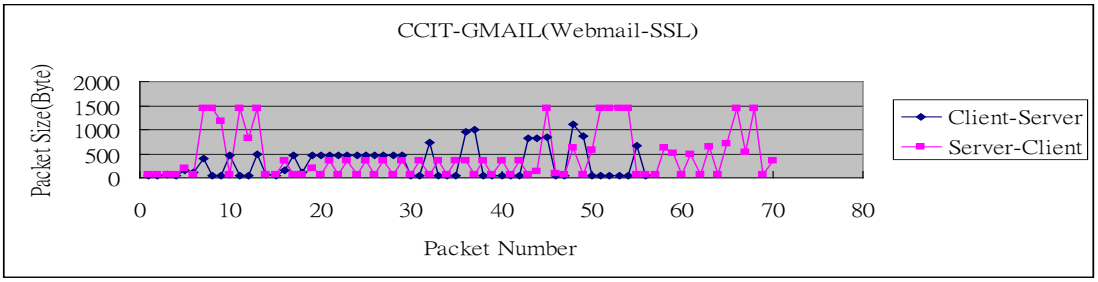


圖五　連接網景 OPENFIND Webmail 網頁流量封包圖

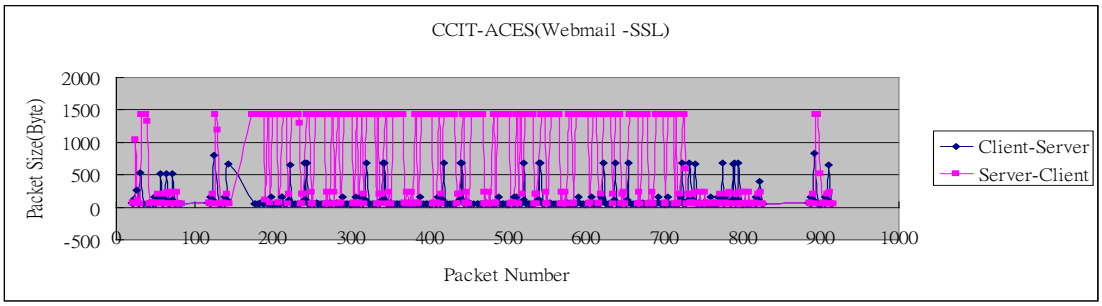


圖六　Webmail 的簡易基本連線模式

3.Webmail (SSL)連線請求/回應：對於使用加密網頁 SSL(Secure Socket Layer)的 Webmail 網頁連線是否仍會如基本連線模式(如圖六)，我們以 Google 的 Gmail(https://gmail.google.com/)以及陸軍通信電子資訊學校的 Webmail (https://mail.aces.edu.tw/)來測試。圖七及圖八為 Gmail 及陸軍通校 Webmail 封包傳輸分析圖，雖然使用端與伺服器端連線傳輸過程中經過 SSL 的加密處理，無法得知其傳輸內容，但其連線型態仍有其基本模式，使用端向伺服器端提出連線請求(如圖七封包數第 1-7 個)，伺服器端開始提供網頁資料(如圖七封包數第 8-15 個)，使用端進一步輸入登入資料(如圖七封包數第 40-45 個)，伺服器端經過驗證後開始提供資訊(如圖七封包數第 48 個以後)，圖八仍依此模式架構。

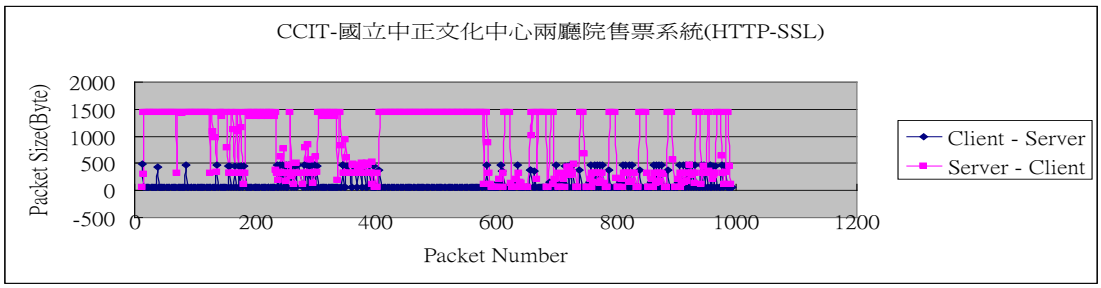


圖七　連接 GMAIL Webmail-SSL 網頁流量封包圖

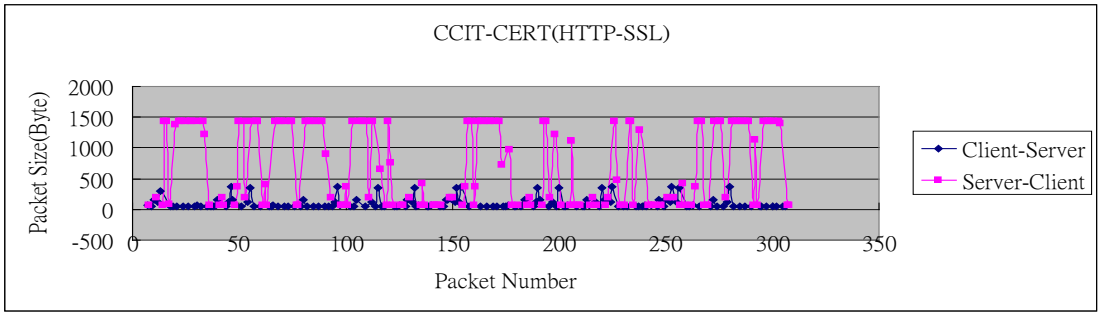


圖八　連接 ACES Webmail-SSL 網頁流量封包圖

4.具有 SSL(Secure Socket Layer)加密的網頁連線請求/回應：連結國立中正文化中心兩廳院售票系統(如圖九)及連結台灣電腦網路危機處理暨協調中心(TWCERT/CC)(如圖十)，兩者為一般經過 SSL 處理程序的網頁，與圖三未經過 SSL 處理程序的網頁相比，從封包數及檔案大小分析圖中，較難發現其特殊之處。

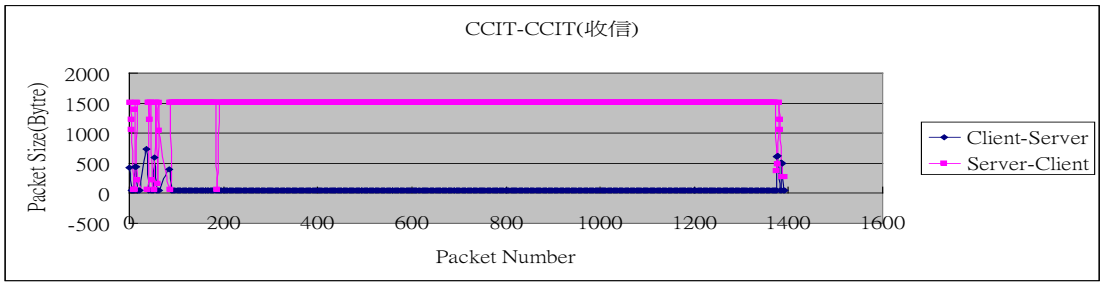


圖九　連接國立中正文化中心兩廳院售票系統 SSL 網頁流量封包圖

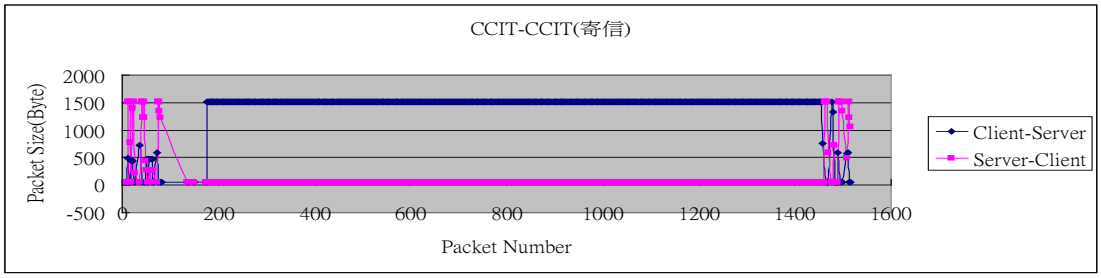


圖十　連接 TWCERT/CC SSL 網頁流量封包圖

5.Webmail 收／發信連線請求/回應：連接 Webmail 時進行信件的收發動作，連接國防大學中正理工學院的 Webmail 來測試，收發信件時均附加約 1.2MB 測試檔，在收信時（如圖十一）中得知，Webmail 在經歷過連線基本模式之後，由伺服器端提供檔案給使用端，在寄信時（如圖十二）中得知 Webmail 在經歷過連線基本模式之後，由使用端提供檔案給伺服器端，並且傳輸過程中均以網路封包最大傳輸值傳輸。



圖十一　連接中正理工學院 Webmail 收信流量封包圖

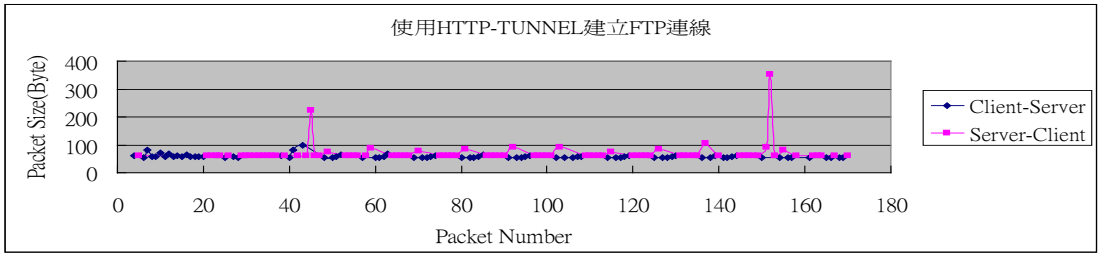


圖十二　連接中正理工學院 Webmail 寄信流量封包圖

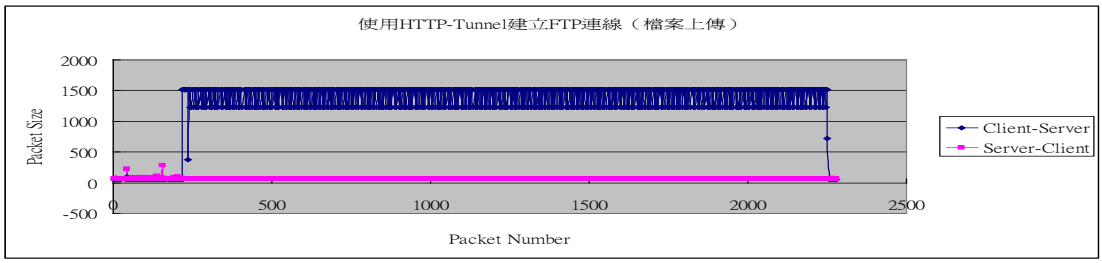
(二)HTTP-通道連線封包流量分析

在實驗中對於採用 HTTP 通道技術的服務做測試，測試使用 FTP 檔案傳輸協定及 TELNET 遠端登入協定。

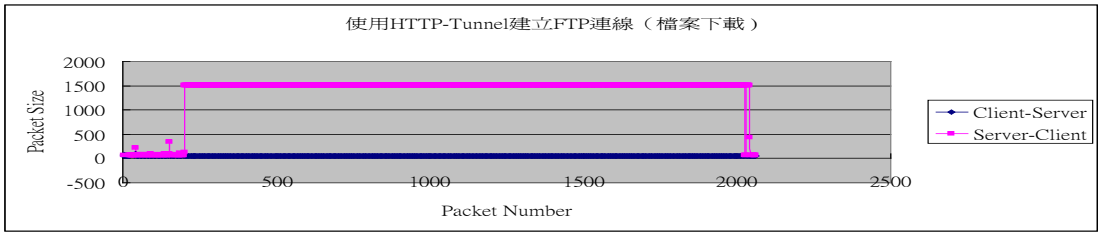
1.HTTP-TUNNEL 建立 FTP 連線請求/回應：在伺服器端安裝 FTP 的應用服務，並利用 HTTP-TUNNEL SERVER 來架構，使用端同樣的使用 HTTP-TUNNEL CLIENT 來與伺服器端構連，並測試使用 FTP 進行檔案的上、下傳動作。



圖十三　使用 HTTP-Tunnel 建立 FTP 連線（Login）的流量封包圖



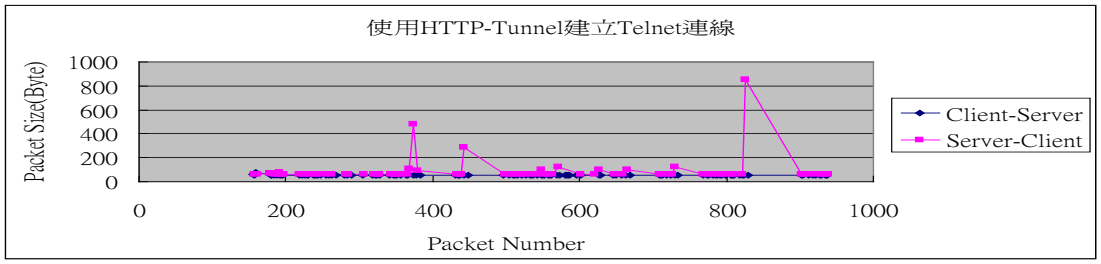
圖十四　使用 HTTP-Tunnel 建立 FTP 連線（檔案上傳）的流量封包圖



圖十五　使用 HTTP-Tunnel 建立 FTP 連線（檔案下載）的流量封包圖

FTP 檔案傳輸協定是使用 21 的通信埠，透過 HTTP-TUNNEL 隱藏在 80 埠之中，圖十三是使用端登入到伺服器端的連線封包流量圖，可以發現封包的大小很小，似乎跟一般 HTTP 連線不同，而從圖十四－圖十五中可以發現，進行檔案傳輸過程中，封包很大持續傳輸直到檔案傳送完畢，在使用者進行連線建立時，跟一般的 HTTP 連線建立時封包有較小的現象，因為 FTP 伺服器並不像 WWW 伺服器會提供較多的圖文資料的關係，之後所進行的檔案上下傳則與 Webmail 收發信件時相似。

2.HTTP-TUNNEL 建立 Telnet 連線請求/回應：在伺服器端安裝 Telnet 的應用服務，並利用 HTTP-TUNNEL SERVER 來架構，使用端同樣的使用 HTTP-TUNNEL CLIENT 來與伺服器端構連，並測試使用 Telnet 進行登入、下達指令等動作。



圖十六　使用 HTTP-Tunnel 建立 Telnet 連線的流量封包圖

TELNET 遠端登入協定是使用 23 的通信埠，透過 HTTP-TUNNEL 隱藏在 80 埠之中，從圖十六中同樣發現在兩端連線建立時，伺服器端提供的封包大小，

跟一般的 HTTP 連線建立時有較小的現象。

(三)實驗結果分析

從實驗中比對正常 HTTP 連線建立時，所產生的封包數量及大小，與使用 HTTP-TUNNEL 隱藏其他應用服務時，所產生的封包數量大小來分析。

正常使用 HTTP 連線建立時，因為伺服器端需要提供文字、圖形、音效等多媒體檔案，在相同網路架構模式下，會產生伺服器端流向使用端的封包數量及大小較多的現象；而使用 HTTP-TUNNEL 來建立兩端之連線，使用端雖然透過 80 埠與伺服器端構聯，但連線所產生的封包數量及大小，則與所隱藏的應用服務有關,例如使用 Telnet 應用服務則兩端封包數量及大小都很少,使用 FTP 應用服務則兩端封包數量及大小取決於是否進行檔案傳遞行為而定，由此可知 HTTP-TUNNEL 兩端連線封包數量及大小仍不脫其所隱藏的應用服務本身的性質。

使用 HTTP-TUNNEL 的技術持續在發展中，使用 HTTPS 來進行 TUNNEL 更是難以偵測，這對於組織內的安全影響越來越大，許多的即時通訊軟體例如 Microsoft MSN Messenger、PChome- Skype、Yahoo!奇摩 Messenger 都可以利用 HTTP 的管道來進行連線溝通,目前或許可以經由檢查封包內容來查看是否屬於正常的 HTTP 連線，例如檢查是否具有一般常見的基本指令 GET、PUT、POST 等來判斷是否有問題，但是經過加密後檢視封包內容卻成為一大難題，所以或許從流量的角度去思考比較可以發覺異常的現象。

從一般網頁存取的過程中，可以看出絕大部分的流量方向，是由伺服器端流向使用端，尤其是連線剛建立開始階段，使用網頁式電子郵件系統或是其他具有檔案上傳功能的網頁服務，也僅在上傳期間造成流量反向傳輸（使用端流向伺服器端的流量較大)，所以可以從流量過程中比對出異常的傳輸行為，提高發覺出隱藏通道使用的機率。

三、建議的解決方案

從實驗結果的分析中可以得知 HTTP 隱藏通道的使用，雖然可藉由流量的異常模式中尋找到蛛絲馬跡，但需要花相當的時間進行資料蒐集與比對，並且需要記錄所有網頁連線的過程，在無開發出自動偵測的系統之前，此方法對於實際偵測的成效有限，但本文主要用意在於提供可發覺隱藏通道之思考方向，作為未來其他先進可運用之參考。

目前雖無可主動即時偵測之系統來提供管理者警告訊息，但仍可藉由管理之手段及要求，強化資訊安全作為（如圖十五)，來避免使用隱藏通道現象發生

之機率。

圖十五　強化資訊安全作為示意圖

(一)個人電腦安全系統之建立

在以往大多的安全防護的作為，都在保護伺服器的可用性、完整性與保密性等工作上，往往忽略了一般使用者的保護，如此才讓攻擊者有機可趁，藉由內部使用者的個人電腦作為攻擊內部伺服器的跳板，所以安全防禦機制必須是整體的、完整的，個人電腦的防護基本的選項包括：

1.作業系統的更新：絕大部分的攻擊手法，都是運用被攻擊者本身系統上的漏洞來進行，尤其“0day”攻擊（在修補程式尚未產生前，攻擊運用方式或工具已產生），修補速度已趕不上攻擊速度的狀況下，一直不斷的修補似乎是目前減少被攻擊的方法之一。

2.防毒（防惡意程式）軟體的安裝及更新：目前大多數的防毒系統均屬於特徵（PATTERN）比對式的系統，在資料庫中沒有的特徵，防毒系統就不會認定該程式是病毒，所以我們必須經常的更新病毒碼，才能發覺或阻絕新病毒的感染；當然不是說安裝防毒（駭）的軟體並更新至最新版本，就不會被病毒感染或被植入後門，因為有些病毒從防毒公司發現到產生特徵及修補或移除的程式，是有一段空窗期，以 2006 年 8 月份發現的巴克雷病毒為例，剛開始各家防毒公司也是無解，事後有些防毒系統經過了一到二個月才能提供完成修補方法及移除程式；在惡意程式的部份，在經過加殼（packing）包裝處理，改變原有的特徵，要是防毒系統對解殼（unpacking）功能稍差，可就難偵測出惡意程式了。

3.簡易個人防火牆的啟用：個人端的主機型防火牆在目前作業系統中，幾乎均有內建提供，作者本身不建議額外安裝使用其他功能強大的個人防火牆，因

為越是功能強大，在各項安全保護的層面越是深入，也因為越深入所以在各項功能的設定上越是複雜，更因為深入核心對於系統的監控越是周延，個人電腦上的任何活動訊息都可能會觸發警告訊息，通知使用者，這原本對於個人電腦安全是好事，但並非人人都是資訊安全專家，對於各項警告訊息，也大多一知半解甚至完全不解，很多使用者遇到這些訊息，都是直覺的按下“是”、“允許”、“接受”選項或甚至點選“永久接受”等，久而久之這些功能強大的防火牆，也就被訓練成“呆呆”的防火牆，喪失了原有的功能，所以單純的防火牆反而對大多數的使用者才是有利的。

(二)積極管理、有效開放

單位網路使用的控管，應由先緊縮政策，再依據使用的需要進行逐一的開放，並針對這些特殊的使用需求，進行嚴密的使用控管，單位內部區域網路的使用上，就應考慮各種安全作為：

1.IP 分配的管控：IP 分配的主要目的，就是要能夠對於網路來源使用者的身份進行控管及驗證，但網管人員可能會面臨到動態 IP 使用者身份無法確認的問題、惡意使用者盜用 IP、偽造 IP 來進行攻擊，或者是 MAC Flooding 攻擊造成網路癱瘓等現象，所以要能夠確保 IP 的唯一性，才能在任何的稽核紀錄中，追查到使用者真正的來源位置。

2.存取網際網路的管制：內部區域網路中，重要的部門或單位，應進行網路隔離或阻止連接網際網路的使用權限，並可藉由代理伺服器（Proxy server）的功能，保留連線的相關紀錄，並對其紀錄分析，可作為日後鑑識稽核的參考依據（如圖十六）。

ACES to MINET Squid User Access Reports

分析期間: 2007Jan16-2007Jan16
資料排序: BYTES, reverse
Topuser 報告

Topsites 報告
網站 & 使用者 報告
要求被拒絕 報告

數字		使用者帳號	連線成功數	資料量(Bytes)	%資料量(Bytes)	寫入	快取	讀出	使用的時間	千分之一秒	%時間
1	日期/時間	10.52	1,903	66,799,213	23.30%	6.14%	93.86%		00:40:32	2,432,464	26.79%
2	日期/時間	10.52	277	29,923,532	10.44%	0.52%	99.48%		00:04:56	296,218	3.26%
3	日期/時間	10.52	1,224	25,142,930	8.77%	0.97%	99.03%		00:05:18	318,479	3.51%
4	日期/時間	10.52.	326	21,907,848	7.64%	88.94%	11.06%		00:07:24	444,578	4.90%
5	日期/時間	10.52.	118	17,693,226	6.17%	16.62%	83.38%		00:01:53	113,946	1.25%
6	日期/時間	10.52	307	17,613,364	6.14%	3.40%	96.60%		00:02:34	154,394	1.70%
7	日期/時間	10.52.	659	12,379,265	4.32%	6.67%	93.33%		00:02:10	130,322	1.44%
8	日期/時間	10.52.	627	9,983,213	3.48%	12.58%	87.42%		00:01:48	108,635	1.20%
9	日期/時間	10.52.	369	8,777,058	3.06%	33.03%	66.97%		00:02:52	172,895	1.90%
10	日期/時間	10.52	275	5,877,579	2.05%	22.94%	77.06%		00:01:52	112,063	1.23%
11	日期/時間	10.52	497	5,413,008	1.89%	2.86%	97.14%		00:03:21	201,085	2.21%

圖十六 代理伺服器紀錄分析報表範例

3.連線需求限制：網路連線的要求不論是內部區域、外部區域或非軍事區域（DMZ），彼此之間應做好詳細限制規則，例如單位要求內部使用者連外部區域需使用代理伺服器，則在防火牆的規則上就應該只有代理伺服器可對外部區域進行存取；或在專屬伺服器之間的存取做好限制，例如資料庫伺服器與網站伺服器之間的關係，資料庫就只有網站伺服器使用上的需要，就可以在資料庫伺服器的規則中加入只有網站伺服器可進行存取等；但再多的規則與限制只要有一條設錯，就有可能前功盡棄，所以必須經常的檢查與測試規則的合法性與適用性。共通的網路連線環境設置完成後，接著就是有額外特殊的連線需求，例如某人事線傳系統、公文交換系統等，所使用的服務埠是特殊的，使用的對象是少數的，類似這些就必須針對各專屬用戶來逐一設定規則了，保持有需求再開放的原則。

(三)稽核檢查、完整追蹤

針對各系統產生的事件訊息，必須搭配比對分析，並且對於異常事件追查到底，找出真正問題所在，例如單位中某使用者發生中毒事件，就必須開始詳加追查：

1.是哪一台電腦中毒？（找出中毒的電腦位於何處）

2.使用者是誰？（是哪個使用者操作過程中產生中毒事件）

3.是何時中毒？（發生的時間是否為上班時間，如果不是？為何使用電腦）

4.中的病毒是哪一種？（是屬於檔案型病毒、蠕蟲或是木馬程式）

5.是哪些檔案中毒？（檔案是何種程式）

6.為什麼檔案會中毒？（是做了哪些動作怎麼會感染）

7.檔案從何而來？（這個程式或檔案是誰裝的，是怎麼灌到電腦去的，是從網路上取得、使用光碟\磁碟片\其他儲存媒體，那這些是怎麼帶進單位，有無申請攜入……等等）

從以上範例可知雖然僅發生一件中毒事件，但背後所可能的原因卻是都有相關性的連結，仔細的調查下去就會發現背後的真相了。

(四)風險評估、消弭弱點

弱點管理系統(Vulnerability Management System)是目前在安全管理上常見的防禦策略之一，在每隔一段時間或在重大弱點資訊公布後，進行系統安全檢查，使得弱點可在公布後且尚未被攻擊者運用之前被發現，進而採取補救措施。

弱點掃描是指借助工具，協助使用者瞭解自己，所使用的系統和軟體是否含有目前已知的安全弱點。藉由弱點掃描所得的結果，使用者可以即早修復弱

點，對於目前尚無法修復的部份，也能夠事先採取加強監控的方法來降低受到入侵的機率。弱點掃描系統能夠根據本身的弱點資料庫中擁有的各種弱點偵測工具程式，檢查受測目標是否有安全弱點。要開發這些弱點偵測工具程式，必須先掌握足夠的弱點資料，依據每一弱點的特性設計出，可以侵入系統或突顯出弱點危險性的程式。然而這種工具若是被入侵者早一步對攻擊目標使用，則亦成為攻擊程式的一部份。弱點隨著應用程式持續開發而不斷增多，弱點掃描系統背後所依據的弱點資料庫，也必須不斷更新與擴充。

(五)強化教育、觀念提升

1.應定期對所屬同仁進行資訊安全教育及訓練，促使全體人員均瞭解資訊安全的重要性，各種可能的安全風險，以提高人員資訊安全意識，促其遵守資訊安全規定。

2.應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資訊安全教育及訓練；資訊安全教育及訓練的內容應包括：資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等。

3.在同意及授權使用者存取系統前，應教導使用者登入系統的程序，以及如何正確操作及使用軟體。

4.對人員進行資訊安全教育及訓練之政策，除適用所屬人員外，對單位外部的使用者，亦應一體適用。

參、結論

在正常行為模式中，從分析 HTTP 流量狀況來比對隱藏通道的使用，只是輔助系統管理者提早偵測發覺異常使用狀況的一個方法，以期能夠針對其中產生異常事件的警訊，讓管理者對其放入心力去了解異常行為產生的原因，進而早期發覺問題提早處理。

隨著科技的發展，網路在資訊傳遞的過程中扮演了重要的媒介角色，各個公司及政府部門更是依賴網路上的應用系統運作，所以網路安全是非常重要的，系統管理者必須思考如何讓單位內部的資產能有效保護，避免入侵者在網路上予取予求所有資訊。

整體安全防護，必須每一個環節層層相扣，不是只要單一政策或設備來維護，架構上更是要相互重疊配合，並且必須結合人員教育訓練，落實資安觀念與保密警覺，讓單位整體資訊防護強化，所以現在在考 量安全性的相關問題時，要從各種角度來考量與評估。