

校園網路安全性之評估

TW-CERT 台灣電腦網路危機處理中心

E-mail : twcert@cert.org.tw

摘要

鑑於國內網際網路環境日益成熟,越來越多的學校單位建立網路服務網站提供學生便民服務,加上校園內所使用的教育部網路經常掌握有龐大的網路頻寬,但是卻沒有企業裝置防火牆的機制,因此校園網路經常是駭客喜愛的攻擊對象。為了避免 90 年 7 月嚴重影響網路連線速度、消耗網路頻寬的 Code Red Worm 和 90 年 9 月的 Nimda Worm 攻擊的等事件再度重演,以及提供穩定的服務品質,網路安全是非常重要的環。因此台灣電腦網路危機處理中心針對國立中山大學進行網路主機安全之檢查與統計工作。

本研究針對中山大學 35 部網路上的電腦主機進行系統弱點的調查,其中一共包含八個單位。希望能提供詳細的安全相關資訊,評估其可靠度及安全性,加以分析檢討並提出改善的建議,期使教育部服務網路能提供更穩定和更安全的服務品質。

關鍵字：弱點掃描器,弱點資料庫,安全稽核,網路安全,校園網路,網際網路

1. 序論

台灣學術網路(Taiwan Academic Network; 以下簡稱 TANet)係由各主要國立大學及教育部,於民國 79 年 7 月起,所共同建立的一個全國性教學研究用之電腦網路。它的主要目的是為了支援全國各級學校及研究機構間之教學研究活動,以相互分享資源並提供合作機會。TANet 具有骨幹(Back bone)和區域(Regional)的網路架構與研究相關資訊應用之基台(Information Infrastructure)。

由於 TANet 是網際網路的使用先趨,以及其強調的教學和分享資源,使得 TANet 所使用的網路頻寬經常不下於一般 ISP 的骨幹網路。更由於政府推動中小學全民上網,網路普及至各級學校中,學校的行政流程以及學生的教學互動大量倚賴電腦系統的正常運作。網路的應用逐漸普及之後,伴隨而起的將是網路上種種越權存取(unauthenticated access)、入侵(cracking)、電腦犯罪(computer crime)的新挑戰。因此,如何評估網路的安全性,保持公眾服務的持續性,以及網站內存放資料之完整性和隱密性,成為網路應用中迫在眉睫的重要安全工作,如何對網路安全進行加強,是在踏入資訊化社會之前必須研究的重要課題。

由於校園網路的使用者流動率大,一台電腦主機經常不是專屬於一個人所使用,尤其是在電腦教室的主機,經常是全校的師生皆有權利可以使用。因此難於控管電腦主機內所安裝的軟體程式,使得病毒程式常常在校園內散播。再者因為學校受經費以及權責的限制,經常無法安裝防火牆或是封包過濾軟體,讓入侵者常常可以有機可趁,利用系統的漏洞、網蟲以及木馬後門程式來攻擊

網路主機。

由於 TaNet 上的網路主機控管不易，所以當有重大的網路危機發生的時候，TaNet 也常常成為最大的受害者。就像是 90 年八月導致網路連線速度變慢、消耗網路頻寬發生的 Code Red Worm 事件。八月二日國外告知教育部 tanetadm@moesun.edu.tw 表明在其所管轄下的 1670 台電腦主機已經在七月的時候，就已經感染了 Code Red。教育部為了因應 Code Red 所造成的可能影響，暫時將 TAnet Backbone http 的使用限制在 163.28.x.x 的 ip，也就是如果您要透過 TAnet Backbone 存取網頁必須透過各區網中心的 proxy server，而其它的 service port 並不受影響。當天教育部的流量監測顯示，各區網中心對國外都是輸出遠大於輸入，教育部電算中心查得結果是因為有大量掃描國外 port 80 web services 的封包導致正常連線搶不到頻寬，情形相當的嚴重。顯示由於 web 使用頻寬異常暴增導致國內骨幹與出國頻寬滿載而無法動彈，使得使用者上網速度變慢、hinet 的 DNS 運作不正常，無法寄發電子郵件、以及造成許多網站無法被使用者連結上。

因此 TWCERT 在 2001 年 4 月，進行中山大學網路站台的安全性總檢查，並做彙整統計，期望分析中山大學所申請的八個單位 35 台網路主機的安全性評估，來推測整體 TaNet 網路主機的安全性，以及使用掃描分析出來的資料，與去年 TWCERT 所做的政府網站分析資料相互比對，期望能夠幫助學術網路建立起網站安全體系，在緊急事件的處理及反應速度上，提供更完整、快速的解決方案。

2. 安全檢測方法

此次檢查方法使用的網路安全掃描主要工具包括 Nmap[11]、httptype、Nessus[16]及 CyberCop Scanner[4]等，Nmap 是一個在 unix 上檢測系統所提供之服務項目的工具軟體；httptype 用來檢測 Web 伺服器的版本型態；Nessus、CyberCope scanner 為系統偵測弱點工具其功能各有不同，但是皆為系統安全掃描軟體，可以增加模組，針對不同的弱點進行測試以及使用一般網路安全檢測技術。

藉由 Nmap 的掃描，可以輕易迅速的得知遠端主機上所執行的服務，可以猜測遠端主機的作業系統以及版本，也可以針對子網路進行掃描，偵測子網路上有哪些主機存在，由掃描結果，可輕易且快速得知，這台主機上對外所有的服務名稱以及 port number。入侵者藉由得知系統所開的服務、埠號、作業系統、版本等資訊，對主機狀況進行大略了解和初步檢視。本身只負責確認服務的存在，並沒有進一步確認服務本身是否有漏洞，這時就要搭配 Nessus 安全掃描軟體來幫我們檢測這些服務的弱點。

使用 httptype 來檢測目標主機的 port 80(http) 送出要求頁面的請求。此時對方主機會回應版本訊息。回應的訊息除了版本資訊以外，還包含了是否安裝其他的外掛模組，例如 SSL、PHP、Front Page Extension、SQL、mod_perl 等等。

Nessus 及 NAI CyberCop Scanner 可以進一步針對這些服務可能存在的弱點進行測試，並列出可能的問題，以及解決的建議方法。Nessus 的運作過程如下：

1. 尋找有哪些 port 有服務正在進行, Nessus 的 port scan 部分是依靠 Nmap 來完成。
2. 測試這個 port 的服務有哪些可能的漏洞存在。
3. 產生測試報告。
4. 提出系統可能的漏洞。
5. 提出系統可能問題的解決方案。

除了使用上述軟體及工具之外,大部份還是要由人工手動的方式來搭配檢測程式[1]或是諮詢報告[5-10,12-15]及追蹤,以避免因軟體的誤判而影響報告正確性。

3. 檢測對象

本研究所檢測的對象為國立中山大學內的八個學術以及行政單位, 共計有三十五部主機。誠如以上所言, 由於校園網路經常沒有安裝防火牆或是入侵偵測系統, 使得校園網路上的每一台主機都直接的暴露在網際網路上, 導致學術以及行政單位內助理所使用的主機和伺服器, 一樣都可以直接被入侵者攻擊。而對於入侵者來說, 取得助理所使用主機的存取權限, 便可以 and 伺服器享有一樣的網路頻寬, 以及取得敏感性的校務資訊。

4. 檢測結果與分析

本研究於 2001 年 4 月針對中山大學八個單位 35 部網路主機作深入掃描

圖(1)是被檢測主機所提供服務的分佈情形。圖中所列的服務只是排名前十大的服務, 沒有列出來的並不代表主機就沒有開那些服務, 也不表示我們只對圖中所列的服務進行檢測而已。

以下為其中相關的補充說明:

smtp(25/tcp): Mail Server 是所有服務中佔最多的, 全部的 35 台主機有 24 台開啟此項服務。

ftp(21/tcp): FTP Server 檔案傳輸服務, 有 22 台主機有開此項服務。

sunrpc(111/tcp): RPC 此通訊協定是用來進行遠端檔案傳輸工作用的通訊協定, 有開此服務的有 20 台。

netbios-ssn(139/tcp): NETBIOS session service, 有開此服務的有 20 台。

telnet(23/tcp): 通訊過程資料沒有經過加密的遠端登入服務, 有開此服務的有 19 台。

www(80/tcp): Web Server 網站伺服器, 有開此服務的有 19 台。

netbios-ns(137/tcp): NETBIOS Name Service, 有 19 台主機有開此項服務。

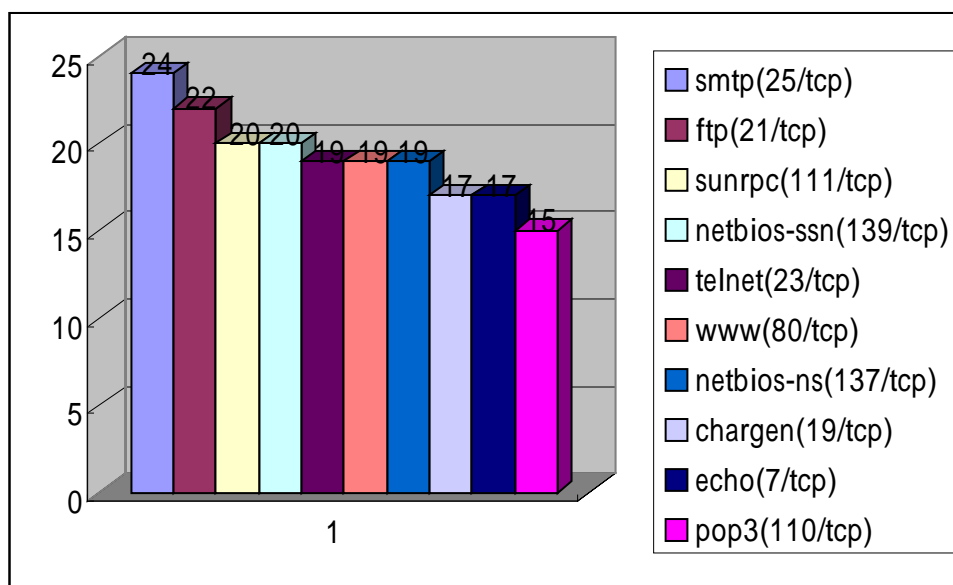
chargen(19/tcp): Character Generator 字元產生器, 有 17 台主機有開此項服務。

echo(7/tcp): 回應和 Client 所傳送的不同字元的服務, 有 17 台主機有開此項服務。

pop3(110/tcp): 信差服務, 有 15 台主機有開此項服務。

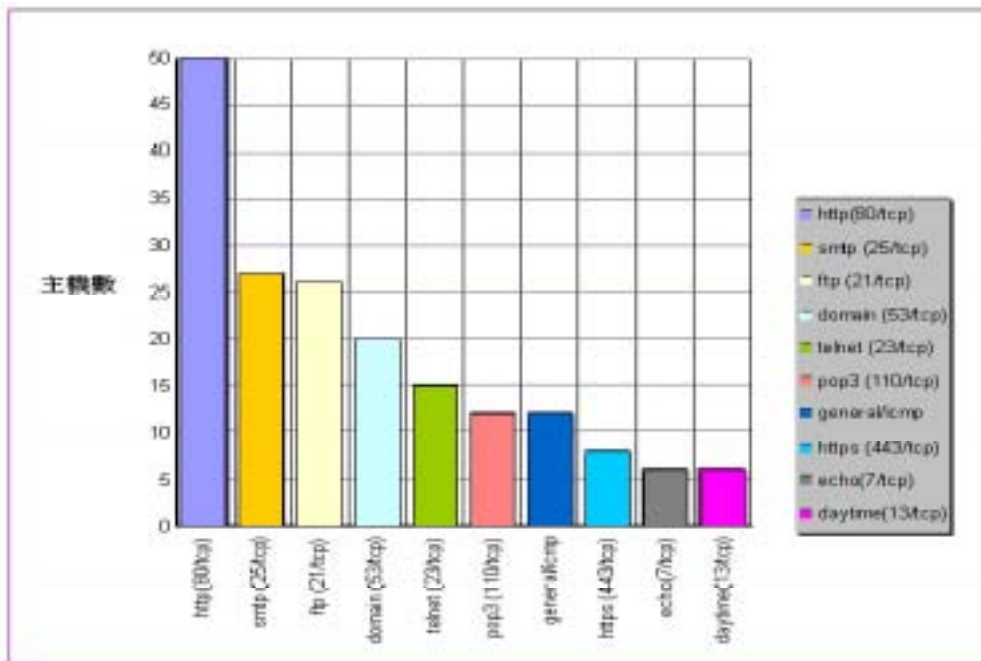
由此可看出學校所提供的主要服務, 還是主要以電子郵件服務為主。這也說明了 TaNet 上的使用者利用電子郵件服務來進行溝通、交流、資訊分享的頻

繁。而且大部分受檢測的網路主機除了充當單一的伺服器外，還執行其他多項網路服務。提供愈多的服務網路主機本身就有愈多漏洞。目前 PC 價格普遍低落，可將其他網路服務分散於多台機器上，理想情況下一台主機負責一項網路服務，以分散其危險性，也可以提高服務的效能。各單位助理、助教所使用的電腦，由於常常會存放敏感的校務資訊，所以在安全的考量下，建議關閉所有不需要開啟的服務。



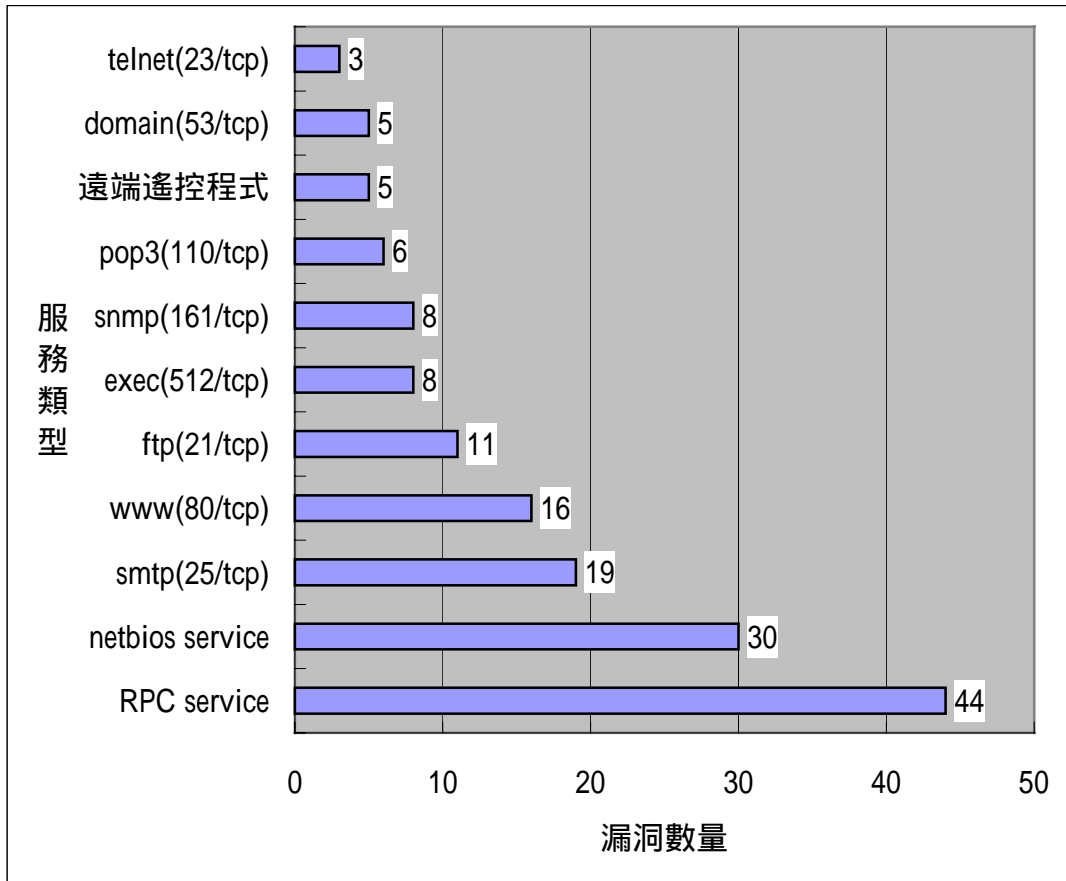
圖(2) 35 個校園網路主機所提供服務之分佈統計圖

比較去年 TWCERT 所進行的政府網站安全性分析,的前十大服務分布圖(圖 3), 我們可以發現, 校園網路所提供的服務主軸和政府網站是非常不同的。政府網路主機所提供的所有服務中佔最多的是 http(80/tcp), 而學術網路卻是以 smtp(25/tcp)為主要的服務。從校園網路主機所提供服務之分佈統計圖來看, 校園網路所強調的為, 資訊的分享, 所以前四大的服務才會是以檔案訊息的傳輸服務為主; 而政府網路主機, 強調的是資訊的告知, 所以才會是以網站伺服器為第一大的服務。所以由此可以得知, 網際網路服務的使用, 是和使用實體的特性息息相關的, 每一個網際網路的使用實體, 必須了解自己的特性, 才能知道應該多加注意加強, 哪些服務的安全性補強。



圖(2) 50 個政府網站所提供服務之分佈統計圖

圖(3)為校園網路安全性漏洞分佈圖，在被檢測的所有主機上所開啟服務中發現的安全性漏洞的數量統計圖。其中以 RPC Service 服務所發現的安全性漏洞數量為最多，共 44 個約佔總數的 26%，其次分別為 NetBios 服務及 SMTP 服務各發現安全性漏洞數量為 30 以及 19 個，而這些安全性漏洞對系統來說是相當具危險性的，極容易使主機遭受到入侵的，因此這些漏洞必須列為即時修補首要工作。



圖(3) 校園網路安全性漏洞分佈圖

以下為其中幾個漏洞相關的補充說明：

rpc service 發現的漏洞：共有 44 個為所發現的安全性漏洞數量最高，其中包含 rpc.statd、rpc.cmsd、rpc.nfsd、rpc.sadmin 服務，過去這幾個服務都曾發生過嚴重的安全性漏洞包含遠端取得 root 權限等等。

netbios service 發現的漏洞：NetBios 為一檔案分享的協定，包含 netbios-ssn(139/tcp)以及 netbios-ns(137/tcp)，NetBios 會洩漏出遠端主機的卡號以及網域內的主機名稱，入侵者更可以使用密碼破解工具，對分享的磁碟機進行字典攻擊的破解。

smtp(25/tcp)發現的漏洞：存在著許多的緩衝區溢位漏洞，允許入侵者可對該主機執行任意指令。

http(80/tcp)發現的漏洞：主要的漏洞是使用了含有漏洞的 CGI 程式、沒有移除 IIS 預設的一些可以被入侵者利用的範本檔 以及一些常見的 IIS 漏洞。

ftp(21/tcp)發現的漏洞：允許 FTP 匿名使用者可移除、寫入檔案至 FTP 根目錄、而使使用者能遠端執行程式。允許使用者使用 Port 指令來使主機對其它網路上的主機來進行掃描工作而成為攻擊跳板等等。

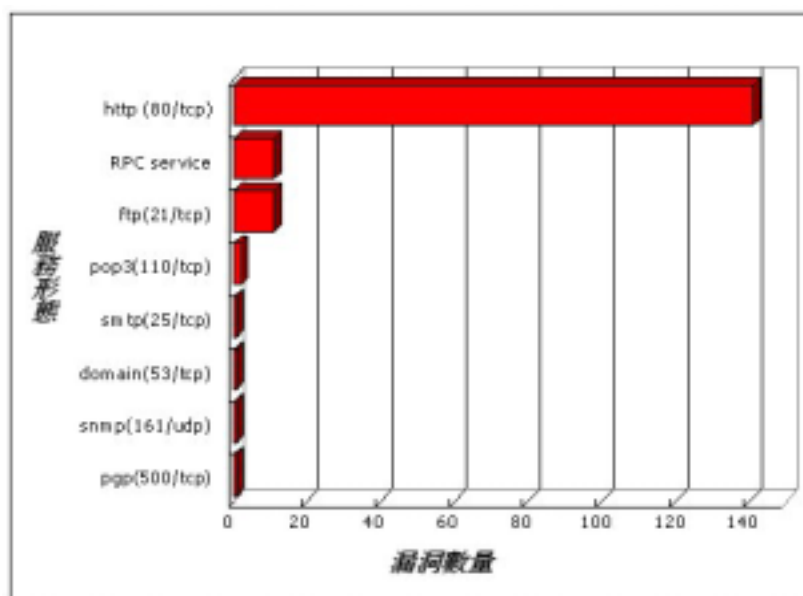
pop3(110/tcp)發現的漏洞：有 buffer overflow 的漏洞，使用者可以遠端執行程式。

domain(53/tcp)發現的漏洞：Bind 版本過於老舊沒有更新，可遠端取得 root 權限。

snmp(161/tcp)發現的漏洞：SNMP 預設密碼為 public，這樣別人可以讀取到網路的相關重要資訊。

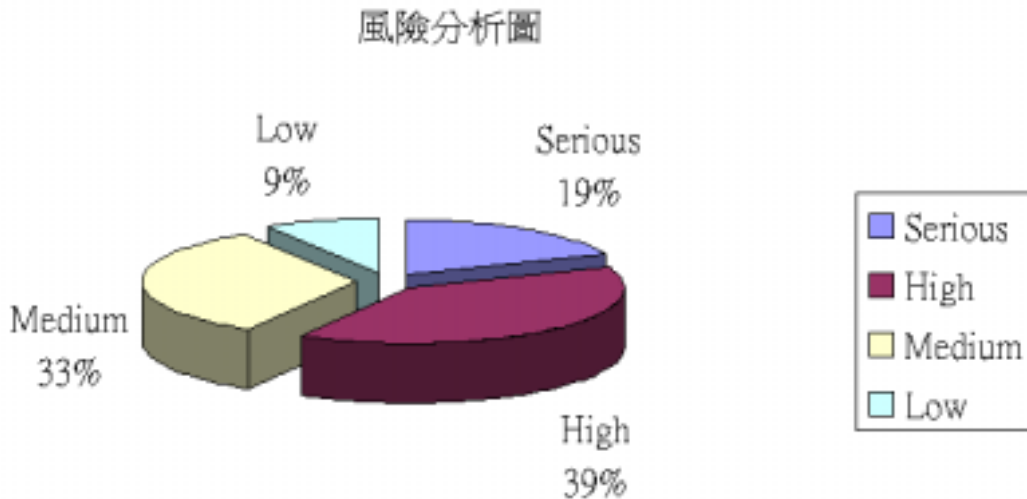
除此之外，我們發現，將近有六成的網域之 DNS 允許 Zone transfers，也就是說一般 Internet 使用者可得知 DNS 所設定的主機資訊。

比較去年 TWCERT 所進行的政府網站安全性分析,的安全性漏洞分析 (圖 4)，我們可以發現，所發現的漏洞種類數量和校園網路也是相差許多。政府網站漏洞分析中，漏洞數量最多的服務為 http(80/tcp)網站伺服器服務。而校園網路漏洞數量最多的反而是在政府網站排名第二的 RPC service。而校園網路第二多漏洞的 NetBios service，反而沒有在政府網站中出現，最大的原因就在於，校園網路普遍沒有使用防火牆來過濾內外部網路的連線，所以一般網際網路上的使用者也可以輕易的使用 NetBios 來連線到校園網路的主機。



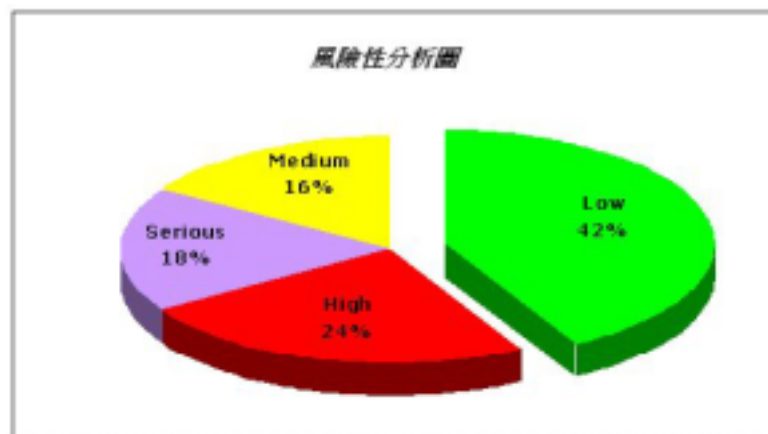
圖(4) 政府網站安全性漏洞分佈圖

校園網路 35 部網路主機之細部安全檢測的結果顯示如圖(5)，風險性為嚴重的佔總比例的 19%、風險性為高的佔 39%、風險性為中的佔 33%、風險性低的佔 9%。將近九成左右的機器存在有高於中風險性之漏洞。一般而言，風險性高於中的以上便可能對系統造成威脅，亦即，十台主機就約有九台可能受到攻擊或入侵的風險存在。因此學術網路上的網路主機管理者應多注意系統之安全性，避免系統入侵發生。



圖(5) 風險性分析圖

比較去年 TWCERT 所進行的政府網站安全性分析，的安全性分析(圖 6)，我們可以發現，校園網路的安全風險程度遠遠的大於政府網站的風險。政府網站將近六成左右的機器存在有中或高風險性之漏洞，可是校園網路卻高達九成的機器存在有中或高風險性之漏洞。以比例來看，校園網路以及政府網站風險性為嚴重的比例都在兩成左右，可是校園網路風險性為高的比例就高出了政府網站 15 個百分比。造成這樣的原因，應該是政府網站的主機大都是由資訊部門專門管理，訂定有嚴謹的使用者規範；校園網路的網路主機，大都是由主機的使用者自行管理，而這些使用者通常可能是非資訊相關的行政助理，以及剛接管伺服器的學生。再者，校園網路經常沒有訂定嚴謹的使用者規範，強調使用者自律，然而在使用者沒有正確的網路安全觀念的狀況下，就造成了高比例的風險程度。



圖(6) 政府網站風險性分析圖

5. 分析與建議

校園網路的網路主機，大部分採用的作業系統，和行政單位、學術系所有絕對的關係。從掃描資料中發現，對政治所掃描的六台主機，皆是 Windows

的系統，而資工系所掃描的五台主機，有四台的主機安裝 FreeBSD 以及一台的 SunOS，皆是 UNIX 相關的系統。然而使用 UNIX 相關系統的主機，並沒有相對的比較安全，因為依據掃描的結果，政治所的五台主機都只有被分析出來有風險性為中或高的 NetBios 安全性漏洞。可是資工所的五台主機，就有三台主機存在著有嚴重以及高風險的安全性漏洞。

值得注意的是，35 台被掃描的網路主機中，有 21 台主機有開啟數量眾多未知功用的服務埠，如果這些服務埠是安裝後門後所開啟的服務埠，就代表者已經有六成的校園網路主機被放置了後門程式。

大部份校園網路主機置於防火牆外部，無法受到防火牆的保護，建議調整防火牆設定[3]，將對外服務設於 DMZ「De-militarized Zone，受防火牆保護的區域」中。如此對外服務能夠受到防火牆保護，且與內部網路隔離。而防火牆設定及效能的問題第一件要務就是作線上監控觀察，進一步對 log 檔案存成資料庫方式，便於往後防火牆或系統被入侵時，作為記錄追蹤的根據。基於安全的考量，防火牆本身必須做好主機保全(host security)的工作，儘量關閉不必要的服務，而且除了系統管理者外，不要建立任何使用者帳號，以增加防火牆主機的安全性，關閉 DNS Zone transfers。定期備份 2~3 份重要檔案，並存放在不同地方，注意存放環境是否適合資料的保存，請注意員工之安全教育，內部人員控管與稽核，並對於重要資料的存取設立稽核機制，相關安全稽核設定，例：統一密碼長度的限制等系統管理環境。

由於校園網路使用著龐大的網路頻寬，應注意病毒和後門軟體[2,17]傳播的可能性，並採用適合之防毒軟體，對於及做好檔案存取稽核。並且建議使用 Microsoft IIS 的單位應該注重 IIS 程式的更新與漏洞的補漏發布。這些資訊可以在微軟所提供的 Microsoft Security Bulletin[18]中找到。請注意 TWCERT 最新的研討會訊息及重要公佈事項或是由本中心的電子郵件群組 (Mailing List) 中獲得。並且系統管理員時常參考系統安全設定相關文獻，關閉不必要之網路服務、定期檢視系統紀錄檔、定期進行系統備份以及建立網路安全重大事件聯絡之管道。

參考資料

- [1] Anticode 弱點資料庫, <http://www.anticode.com/>
- [2] cDc BO2k 遠端操控程式, <http://www.cultdeadcow.com/>
- [3] CERIAS Firewall Testing Project, <http://www.cerias.purdue.edu/firewall/>
- [4] CyberCop 弱點掃描器, <http://www.nai.com/>
- [5] Elitehackers.org, <http://www.elitehackers.org/Exploits/index.html>
- [6] Enslaver 弱點資料庫, <http://www.enslaver.com/exploit/>
- [7] Futher Kill Security Database,
<http://users.succeed.net/~kill9/security/database/index.html>
- [8] Kao ' s UNIX Security Library, <http://www.tacd.com/hack/index.html>
- [9] IOpht.弱點資料庫, <http://www.iopht.com>
- [10] NegativeZero 弱點資料庫, <http://www.negativezero.com/exploits/>
- [11] Nmap, <http://www.insecure.org/nmap/>
- [12] NT Bugtraq 弱點諮詢報告, <http://www.ntbugtraq.com/>

- [13] Rootshell 弱點資料庫, <http://www.rootshell.com/>
- [14] The Brotherhood of Darkness Exploit Archive,
<http://www.ilf.net/brotherhood/filez/xploits.html>
- [15] The Legacy Hacking Archive II, <http://www.jabukie.com/Archivell.html>
- [16] The Nessus Project, <http://www.nessus.org/>
- [17] Trojan 特洛伊木馬列表, <http://www.dark-e.com/archive/trojans/>
- [18] Microsoft Security Bulletin, <http://www.microsoft.com/security/>