網路安全重要性與防範策略之研究

戴建耘 袁煥助 劉真妮

前言

有鑑於日前發生美中駭客(hacker)網路大戰以及紅色警戒(Code Red)、娜妲(Nimda)等病毒重創台灣各網站等事件，突顯出網路安全的重要性愈來愈高。本文先就網路的安全性做初步的分析，並舉例說明在軍事、商業及個人方面的重要性，接著探討常見的網站攻擊方式，如阻斷服務(DoS, Denial of Service)、分散式阻斷服務(DDoS, Distributed Denial of Service)、密碼破解或植入後門程式(back door)等，進而探討網站基本的安全防護機制及防範之道，如防火牆(firewall)、網路位址轉譯(NAT, Network Address Translating)、修補漏洞或監控掃描等，藉此揭開網路安全的神祕面紗，使網管人員或大眾了解網站安全的重要性，以進一步採取防範之道。

壹、緣起

近年來，由於網際網路與WWW(World Wide Web)的盛行，資訊的流通更為方便迅速，加上電子商務的快速發展，許多的安全問題便慢慢的浮現出來。無論是軍事上或商業上，均不斷傳出駭客入侵的事件，日前發生的美中駭客網路大戰事件，以及網路銀行盜領事件，只是冰山一角。根據電腦安全協會(Computer Security Institute, CSI)及FBI在1999年針對電腦犯罪與安全性所做的調查公佈：連續三年受外界入侵系統的比例上升，自1996年的37%急劇上升至1999年的57%；另外，根據美國國防部資訊部門的統計，目前約20秒就有一個網站被入侵，但透過網路入侵被查獲的比率卻不及4%，而且去年因駭客入侵所造成的損失粗估超過8兆元新台幣(鈺松新聞，民90)。使得網際網路經濟的安全性及資訊的有效性就顯得相當重要。

自從之前中美撞機事件之後，中國大陸的網友，幾乎都是義憤填膺，常常在網路上宣洩對美方的不滿。由規模最龐大的「中國紅客聯盟」主持協同作戰，正式對美國發動所謂的「第六次網路衛國戰爭」，目標鎖定美國各政府單位及民間企業的網站，發動猛烈攻擊。除了美國白宮、美國聯邦調查局(FBI)、美國太空總署(NASA)、美

國國會、紐約時報、洛彬磯時報，以及美國有線新聞網(CNN)的網站，均遭到電子郵件「炸彈」的攻擊外，美國白宮歷史網站的首頁，亦被駭客蓋上中國五星旗(圖1)。不過，美國駭客當然也不是省油的燈，中國大陸北京人民網播電台，就被美國駭客換成色情網站。

此外，近日喧騰一時的「紅色警戒」蠕蟲(Code Red Worm)出現之來，就不斷在網路上搜尋及感染有安全漏洞的電腦和網路設備，並以每小時感染超過五千台電腦速度擴散中。據估計，約有四十萬台IIS伺服器遭到「紅色警戒」的毒手，全球造成的損失則在40億美元左右(鈺松新聞，民90)。而另一隻比「紅色警戒」更嚴重的「娜坦」(Nimda)病毒，主要是經由電子郵件、網路資源分享和微軟IIS伺服器三種途徑散播，只要瀏覽已經中毒的網站也會遭到感染，中毒電腦的使用者會明顯發現網路速度變慢，而且不只會感染Windows 2000或NT的伺服器，連一般使用者的Windows 98或Windows ME也會中毒，災情可謂慘重。

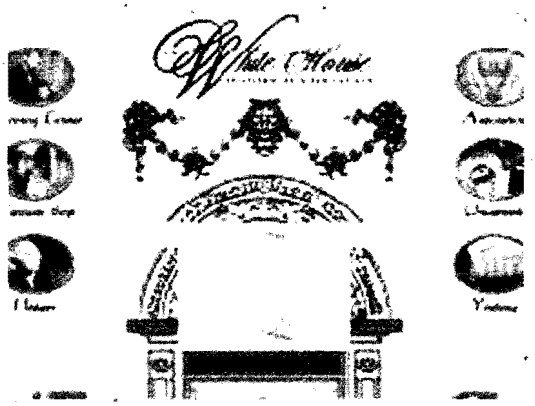


圖1 美國白宮歷史網站首頁被蓋上中國五星旗

網路駭客的入侵破壞，基本上可分為兩種方式，一種是單純的改網頁，例如美國與中共的駭客大戰，即是屬於這種類型；另一種則是以流量方式破壞電腦系統、主機等，如灌爆郵件主機或佔據頻寬使服務癱瘓等，是屬於較嚴重的破壞，像「紅色警戒」及「娜坦」病毒均屬此類。本文將探討常見的網站入侵方式及防範策略，並整理出一般使用者、高階主管及網管人員常犯的錯誤，期使相關人員都能具備網路安全的基本概念，進而加強網路的安全管理及防範之道。

貳、網路安全的重要性

一、軍事方面

根據美國外交事務雙月刊報導，包括中國、俄羅斯、印度、伊拉克等國家在內，全球目前有超過30個國家正發展具有攻擊性的電腦作戰計畫，而中國更在兩年前，由軍官喬良、王湘穗發表「超限戰」一書，點明網路作戰是高明的「不對稱」戰略，只要以極少的資源，就能獲得不對稱的優勢。

號稱資訊科技最發達的美國，在1998年3月遭到一群駭客侵入，五角大廈將此次受襲行動稱為「月光迷陣」，包括美國太空總署、五角大廈、大學、實驗機構在內的數百個網站，被駭客入侵竊走大批科技文件、機密檔案，「月光迷陣」行動造成美國國防作戰企劃系

統受創甚深。但案發後美國情報單位展開有史以來最大規模的調查行動，但只追出攻擊行動是由俄羅斯境內的七個網址發動，其餘毫無頭緒。

另一次教訓是美國曾在近年一項朝鮮半島危機演習中，由國安局派出35人扮演北韓駭客，模擬駭客作戰，結果，這些對美國情報網一無所知、只能在網路上下載普通資料的「北韓駭客」雖未成功阻止美軍行動，卻導致美國九個城市的發電系統、119救援系統癱瘓。

職司太空作戰、導彈防禦預警、太空追蹤來襲的美國四星上將艾伯哈特表示，中國「解放軍報」早在1999年即刊登計畫提升資訊戰的消息，且強調陸海空三軍並重。美國情報官員強調，中國實際已展開資訊攻擊訓練，並涉嫌攻擊台灣的電腦系統。

面對各方電子戰的威脅，自許全力發展高科技的台灣，卻驚傳60%的電腦有明顯軟硬體缺失，成為中國木馬程式的溫床，而這種間諜程式影響力比任何病毒更強大，就像不定時的超級炸彈一像，若再不未雨稠繆，將隨時可能未戰而先亡。

二、商業方面

根據美國海軍戰爭學院以及多位資訊科技專家透露，美國銀行業遭到海內外駭客入侵其電腦系統的問題頗為嚴重，導致美國銀行業損失數以十億計的美元。然而這些遭到駭客攻擊的銀行為維護商譽，大都排斥報警處理，因此外界也都不清楚此一問題的嚴重性。

根據資訊科技專家指出，最近有多家金融機構遭到駭客入侵，包括在紐約的兩家金融機構、加州兩家銀行，以及多家保險業者。目前駭客入侵已是美國銀行業的一個大問題，然而遭到破壞的銀行卻都不願報警，這是因為銀行業的業務是植基於客戶的信心上，如果客戶失去信心，生意也就丟了。因此，正確的金融損失無法估算出，但可想而知的是，此一問題日益嚴重，防駭行動已刻不容緩。

三、個人方面

國內一個名為「NoHack」的軟體資訊網站隨機接受網友線上掃描服務，發現高達81%參加掃描者的電腦有安全漏洞，情況可能遠比官方統計更加嚴重。這些漏洞正是駭客入侵的最佳途徑，像是使用者喜歡使用電子郵件傳遞訊息，許多後門程式正一傳十、十傳百的到處擴散，或者一些線上聊天的軟體，在使用它便利通訊的同時，也隱藏著某種程度的危險，輕則個人財產損失，重則國家機密資料外洩。

另外，隨著電子商務的趨勢發展，網路交易的需求愈來愈高，之前發生網路銀行客戶被駭客盜走百餘萬元的事件，造成社會大眾對網路安全的疑慮。此外，許多網站要求留下使用者的基本資料，甚至是信用卡號，無意中暴露了自己的機密隱私，若不提高警覺，容易造成名譽或財產的損失，由此更顯示出網路安全的重要性。

參、常見的攻擊方式

一、阻斷服務(DoS, Denial of Service)

Denial of Service Attacks的範圍相當廣，通常定義為：「某使用者大量使用系統共享資源，讓其他使用者無法正常使用共享資源，而達到阻斷服務的目的。」(楊子翔和蔡錫鈞，民89)。共享資源可以是硬碟空間、CPU使用率、網路頻寬等。

阻斷服務通常是攻擊者發送大量的網路封包(packet)，到被害端的伺服主機，使其網路頻寬耗盡，網路完全癱瘓；或是讓伺服主機在同一時間內所需要服務的數目暴增，超出伺服器所能服務的上限。此類攻擊是讓伺服器無法正常回應使用者的要求，因而造成阻斷服務。之前美國白宮網站遭到的攻擊就是屬於DoS，它是被大量的電子郵件入侵，拖垮電子郵件伺服器，使網路無法正常運作，這種攻擊方式也稱為「電子郵件炸彈」。另外，造成嚴重災情的「紅色警戒」病毒，是由中毒的電腦一直發送搜尋與感染的訊息至其它網站，以便一傳十、十傳百的速度擴散，因此會嚴重影響網路的頻寬及流量，亦是DoS的一種模式。

二、分散式阻斷服務(DDoS, Distributed Denial of Service)

從上節中，我們已經大致了解DoS的意義，DDoS則是將原本的DoS攻擊模式再延伸，成為分散式的攻擊方式，因此DDoS的攻擊程式都有遠端操控功能，能夠掌握對某台伺服器同時發動攻擊(圖2)。

這種攻擊方式需要先在多台主機上執行攻擊程式，然後同時發動攻擊來達成癱瘓網路或伺服器的效果，因此駭客

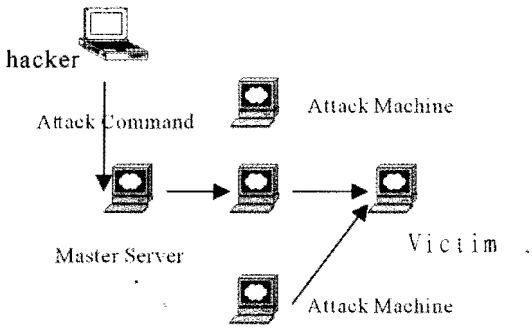


圖2 DDoS攻擊架構圖

必須先取得其它伺服器上的主機帳號，利用盜用、竊聽等得到不合法的帳號之後，再將攻擊程式植入該主機內，等待到達一定數量後，同時發動攻擊，如此可瞬間產生大量的攻擊，造成嚴重的破壞。這種攻擊方式不易被反追縱，但是難度也相對較高。

三、密碼破解法

這類型的攻擊是指使用程式或其它方法來破解密碼，通常分為猜測法、解米字法或暴力法(brute force)。猜測法是利用一般人的習慣去猜測密碼，如生日、電話、英文名字、身份證字號等常被使用來當作密碼，容易被有心人士猜出，像之前破獲國內首宗駭客侵入網路銀行盜領客戶存款案，嫌犯就是利用存款人設定的代碼、密碼都相同，經反覆測試，讓他成功入侵兩個帳戶，盜領共新台幣一百一十多萬元存款。

另一種也是由於一般人的習慣所造

成的疏忽，在Windows底下有個貼心的設計，就是記憶密碼的功能，像IE、Outlook Express或Windows NT的使用者管理，以及其它如Ftp等軟體，均有記憶密碼成為「*****」的功能，只要執行一些破解程式，密碼就現出原形了，這種方法稱為解米字法。

暴力法則是使用攻擊程式對一個加密過的檔案進行破解，通常是為了取得系統管理者的密碼，例如Unix系統的passwd檔和Windows NT系統的SAM檔，破解程式就是利用這些檔案來猜測密碼。

四、植入後門程式

這類型的攻擊方式通常是攻擊者在入侵成功後，為了方便下次入侵而安裝的程式，由於行為類似古希臘特洛伊城的木馬屠城計，因此這種程式也稱為木馬程式。之前3.2節所提的DDoS攻擊方式，就是利用植入後門程式來進行阻斷攻擊的例子。

另外一種則是透過電子郵件的附加檔案，藉由使用者的輕忽太易，在沒有防備下執行了木馬程式，等於將自己的電腦開了一扇大門，讓駭客從遠處竊取你的資料而不自覺，例如前陣子中國駭客會將木馬程式潛藏在類似「我愛你」等病毒功能的E-MAIL中，被「寄宿」的電子郵件會透過他人的通訊錄自動轉寄郵件，造成連鎖感染，災情實在難以估算及掌握。

五、利用系統漏洞

這類型的攻擊方式通常是利用軟體在設計、實作或操作上的錯誤，入侵尚未修補漏洞的電腦，像「紅色警戒」病毒就是針對Windows的IIS伺服器漏洞，快速入侵並癱瘓網站；而「娜妲」病毒則利用到IE瀏覽器的漏洞來大量感染，此種感染途徑毫無防備，不知不覺已入侵有漏同的電腦，因此容易造成重大災情。此外，隨著Linux的使用者愈來愈多，其漏洞亦不比Windows作業系統少，像舊版的BIND、SSH、Wu-Ftpd等均存在許多漏洞，而駭客正好利用這些漏洞入侵電腦，取得管理者帳號。

肆、網站防禦方法與對策

一、防火牆(Firewall)的建置

防火牆是一種保護內部網路免於遭受外部網路威脅與破壞的裝置，它能將內部網路隱形，避免未經授權的資訊外流，通常基本架構如圖3所示。防火牆分為硬體與軟體兩種，通常硬體防火牆強調的是較高的效能，針對作業系統作最佳化的防火牆，同時使用防火牆廠商設計的作業系統，相較於常用的作業系統在安全漏洞上會比較少(謝坤余，民90)。

軟體防火牆則是提供較高的彈性與擴充性，通常可以將購買的軟體防火牆安裝在現有的閘道伺服器上，而不需要變更網路架構。另一方面，軟體防火牆也提供較佳的整合性，例如常與防火牆搭配的VPN、內容過濾、加解密工具、防毒工具等(謝坤余，民90)。一套完整的防火牆至少須要有使用者認證、過濾封包、log分析工具，線上監控等相關功能。因此，防火牆的建置是維護網站安全的基本要項之

一。

二、使用 NAT 隔離網站

NAT(Network Address Translating)是指網路位址轉譯，就是用一台 NAT Router 來擔任內部網路與外部網路的中介者，NAT Router 在接收到內部網路送來的封包時，會改寫封包裡頭的 TCP/UDP 標頭(header)，將虛擬 IP 改為合法 IP 之後再傳輸出去；同樣的從外部網路進來的封包，也會經轉譯再傳輸給相對應的內部工作站或伺服器，其架構如圖 4。

利用 NAT Router 埠轉送的特性，亦可達到保護網站的目的，外界送到 NAT Router 某個特定埠的封包，轉送給內部特定伺服器作處理，像是網站伺服器(HTTP)使用 TCP Port 80、收取電子郵件(POP3)使用 TCP Port 110 等等。對於外部網路來說，認為所有的服務均由 NAT Router 這台電腦所提供，實際上卻是由隱藏在內部網路的多台伺服器對外提供各種服務。由於內部伺服器使用虛擬 IP.，因此外部網路無法直接接觸主機，必須依靠 NAT Router 以改寫封包方式來進行轉送，所以相對能提高內部伺服器的安全性(李忠憲，民 89)，例如圖 4 所示：某公司只申請到一個真實 IP210.73.207.27，公司內部分別設置一台 Web Server 及 Mail Server 並且設成 192.168.1.10 及 192.168.1.11 兩個虛擬 IP，透過 NAT Router 的存取設定，可將外界對 211.73.207.27 的 Web 需求直接轉送給 192.168.1.10 或是 Mail 需求轉給 192.168.1.11 來處理，即可避免 Server 直接被攻擊。

三、及時修補系統漏洞

從理論上說，任何軟體系統都可能存在漏洞，也就是 Bug，作業系統當然也不例外，作業系統的 Bug 尤其嚴重，尤其利用這些漏洞所製造的病毒，透過網際網路可以不知不覺地迅速感染至尚

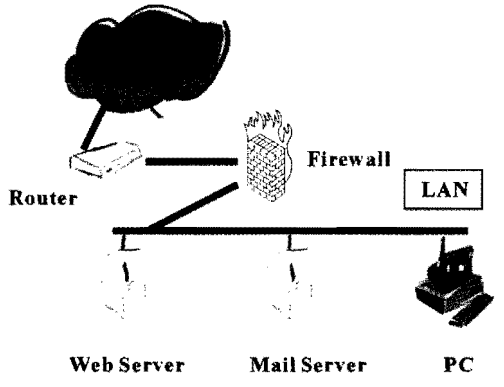


圖 3 防火牆基本架構圖

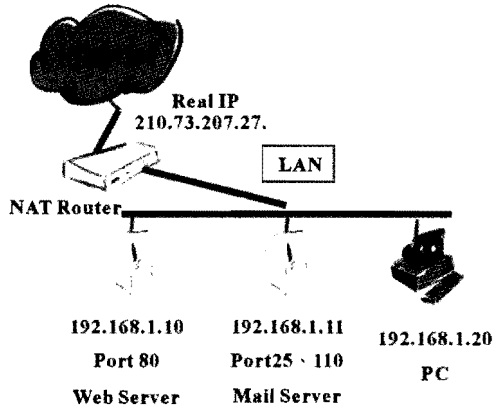


圖 4 NAT 架構圖

未修補的作業系統，造成重大的災情。因此，網管人員必須時常查看是否有無新的系統修補程式，並且適時更新系統，以防止此類病毒或入侵事件。

四、使用監控及掃描程式

網管人員必須經常監控系統或網路是否有異常的活動，才能適時發現問題與解決問題，通常是使用系統掃描程式或網路監聽程式等，藉由攔截網路中的封包，並且分析這些封包及流量對網路內主機是否有不正常的影響，然後做出適當的反應。因此，使用監控及掃描程式是網管人員必備的知識與能力之一。

五、留意不正常的網路流量變化

網管人員必須經常留意網路流量的變化，尤其當遭到DoS或DDoS攻擊時，網路速度會明顯下降且持續擁塞，會讓你及同個子網路的所有主機都受到牽連，因此，經常留意網路的流量是否有不正常的增加，並找出原因排除掉亦是重要的能力之一。

六、養成良好的習慣

鑑於電子郵件的使用頻繁，為避免被植入後門程式或病毒，應該養成不隨便開啟來路不明檔案的習慣，甚至加裝如Trend PC-Cillin或Norton Anti-Virus等防毒軟體多一層防護，並且定期更新病毒碼。另外，盡量不要使用生日、電話、英文名字、身份份字號等容易被猜到的文字或數字當密碼，以防止有心人士的嘗試。

伍、結論

一般採用入侵的手段實際上相當普通，大部分受害網站都是沒有設防火牆系統或是安裝系統的修補程式，在主機之外的駭客，只要透過一些程式即可輕易獲得超級用戶(administrator)許可權或是植入後門程式，這對於駭客來說簡直就等於大門洞開。網管人員平日就應多加強防範，而一般使用者更要有網路安全的意識，表一為高階主管、網管人員、一般使用者常犯的錯誤(SANS Institute resources, 2001)，若大家能儘量避免這些錯誤，就能降低網路安全的風險。

網路安全是一個必須多方面考量的問題，俗語說：「外敵易擋，內賊難防」，雖有堅強的防火牆機制也難抵擋內部的入侵事件，一般來說，內部入侵事件主要可分成四個來源為內部員工、離職員工、網路設備承包商及供應鏈中的上下游廠商。因此，內部的資訊控管就顯得格外重要，必須以「先安內後攘外」來架構資訊安全的先後觀念。隨著科技的發展與進步，任何系統及機制均可能有漏洞，再加上人為的疏失所造成的影響，因此不可忽視網路安全的重要性。本文所提供的攻防之道也僅是常見的部分，大家平時就應多多吸取網路安全新知，以提高個人防護或網路安全為目標。

陸、參考文獻

楊子翔和蔡錫鈞(民89)，Network DoS/DDoS攻擊及預防方法之研究，TANet2000研討會論文集。

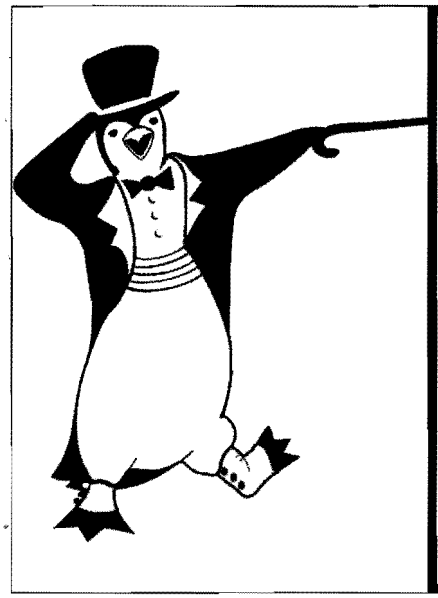
張智晴和林盈達(民89)，網路的攻擊與防護機制，TANet2000研討會論文集。

表1 高階主管、網管人員、一般使用者常犯的錯誤(摘自SANS Institute resources, 2001)

高階主管	● 指派沒有經驗的員工負責資訊安全，並且未給予相關的訓練及時間去學習處理相關問題。 ● 不瞭解資訊安全對組織運作的影響。 ● 未能妥善處理資訊安全相關作業程序。 ● 僅依?防火牆維護組織資訊系統的安全。 ● 未能正確估算資訊系統及組織形象的實際價值。 ● 以為只要忽略問題，問題就會自動消失。
網管人員	● 未強化系統的安全性前，即與網際網路連線。 ● 在測試系統連上網際網路時，使用系統內定的帳號及密碼。 ● 發現系統漏洞時，未予以修補。 ● 使用telnet或其它未加密的通訊協定管理伺服器、防火牆及網路設備等資訊系統。 ● 在未確認對方身份的情況下，給予使用者密碼或協助使用者修改密碼。 ● 未有效維護並測試備份資料。 ● 於系統上提供沒有必要的服務。 ● 未正確設定防火牆控管規則。 ● 未安裝或更新防毒軟體。 ● 未教育使用者，當發現系統安全可能的問題時，該採取的步驟及因應措拖。 ● 網管人員未經過訓練或資格認證就負責重要系統的安全防護。
一般使用者	● 任意開啟未確認來源的郵件附檔。 ● 未安裝MS Office、IE或Netscape的安全修補程式。 ● 安裝不明來源的程式。 ● 資料未備份且未驗證備份資料的正確性。 ● 在區域網路內任意分享資料夾。

宋振華等(民89)，資訊系統入侵與偵防，TANet2000研討會論文集。
國科會科資中心、林秉忠(民89)，2001年台灣Web伺服器安全性調查，TANet2000研討會論文集。
吳賢明(民89)，由電腦系統安全談校園網路防駭之道，資訊與教育雜誌。
黃繼民(民89)，企業網路VS.電腦駭客攻防戰，網路通訊。
鈺松新聞(民90)，資訊安全技術應用國際研討會，鈺松國際資訊股份有份公司http://www.iss.com.tw/newscenter/。
謝坤余(民90)，防火牆趨勢探討，臺華科技股份有份公司http://www.gennet.com.tw/b5/forum/firewall.html。
劉大川等(民88)，Scalable WWW Proxy Cache Server之建置與分析研究，TANet99研討會論文集。
李忠憲(民89)，以Windows 2000架構企業網路，台北市教育網路中心。
SANS Institute resources(2001), Mistakes People Make that Lead to Security Breaches, http://www.sans.org/mistakes.htm。
http://news.kimo.com.tw/。
http://www.ettoday.com/。
http://www.cna.com.tw/。
http://www.money.idv.tw/。

(作者：戴建耘為台灣師大工教系副教授，袁榮助和劉真妮為工教所研究生)



教師在九年一貫課程推動中扮演的角色：

1. 課程發展與落實的關鍵者
2. 課程設計者
3. 教學執行者
4. 行動研究者
5. 教改推動者
6. 同儕視導者