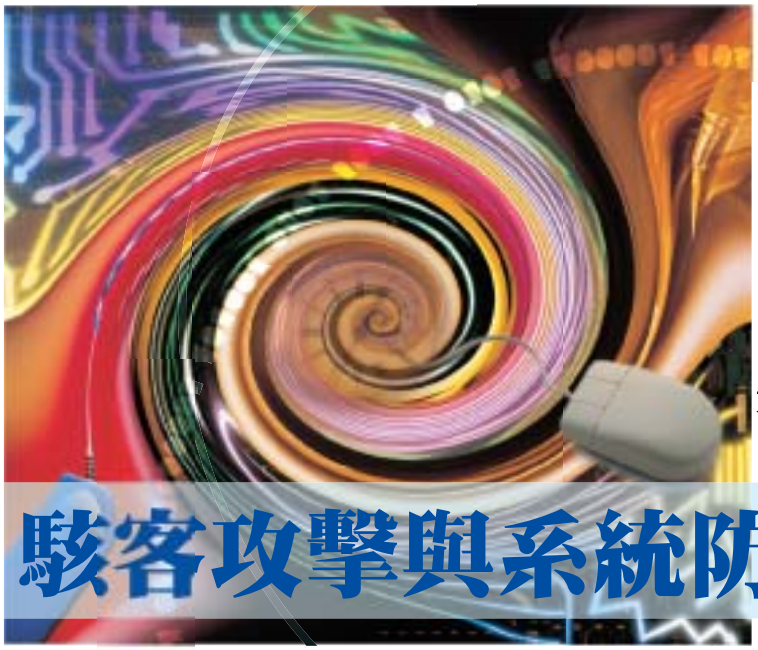


文／李武耀　上尉・王福東　中校
李佳青　上尉

駭客攻擊與系統防護之研究

提要

在網路這個混沌的世界裡，我們對於層出不窮的系統安全漏洞顯得手足無措。即使已知的安全漏洞修補完成，未知的安全漏洞又不斷發現。

過去，一個錯誤的網路安全觀念，認為所謂的「安全防護」是針對那些大中型企業單位和網站而言。然而，駭客攻擊目標主機，擁有超級用戶權限後，便可輕易地在該主機上修改資源配置、安置"特洛伊"後門程式、隱藏行蹤、執行任意程式等等，利用受害主機成為跳板採取網路攻擊或違法行動。因此，具備系統防護的基本概念，才能在面對安全威脅時，採取必要的處置措施。

前言

1999年8月7日上午，監察院電腦資訊網站遭大陸湖南省駭客攻擊，網站資料全部遭覆蓋，螢幕資訊只留下中英文對照的「中國不能分裂」等文字內容，網站首頁出現一個自稱爲「中國駭客」的聲明，其中強調「世界只有一個中國，也只需要一個中國」，並對「臺獨分裂國土企圖」表達強烈抗議。在監察院資訊室的緊急修復下，當天下午刪除攻擊網站系統的不法網頁，並向司法單位報案，將交由檢調查辦不法攻擊來源①、②。

全球最大發卡機構威士卡(VISA)證實，於1999年7月該機構電腦系統曾遭駭客攻擊。在2000年1月，一個駭客團體向VISA勒索一千萬英鎊（約五億新台幣），否則就要摧毀該機構的電腦系統。英國「周日泰晤士報」報導稱，包括VISA在內，至少有十二家跨國公司遭到相同的威脅，這是英國史上最嚴重的公司保全破壞事件，英國蘇格蘭場傾全力調查此一案件③。

① 陳邦鈺，「政府三網站遭不明駭客攻擊」，中央日報，1999年8月9日。
② 劉添財，「湖南駭客攻擊監院網站」，中央日報，1999年8月9日。
③ 英電腦駭客攻擊，勒索VISA卡五億台幣，中時電子報，2000年1月16日。

2000年2月初，駭客以「阻斷服務(Denial of Service)」手法攻擊美國數個大型網站。2月7日，網際網路巨擘雅虎(Yahoo)遭襲擊，駭客對雅虎網站傳送大量資料，造成網路大塞車，迫使服務中斷。這是雅虎第一次發生如此嚴重的意外，該公司發言人韓特女士表示，雅虎的搜尋引擎和入門網站因此停頓了將近三小時④。除此之外，Amazon網路書店也面臨相同的問題，有一大堆垃圾流量直指Amazon，造成服務受影響長達一小時之久⑤。

由上述國內外案例可知，系統如果受到駭客攻擊，就可能發生資料受到篡改、服務中斷或資產蒙受損失。所以，避免系統被駭客攻擊是每個資訊系統管理部門非常重要的課題。在蒐集時下常見之駭客攻擊系統的工具與有關攻擊程式的文件，實際進行系統的攻擊，藉由駭客攻擊方法的驗證，找出各攻擊方法的對策與預防之道。最後將這些駭客攻擊方法與對策，彙整製作出一份駭客攻防檢查表，試著從駭客角度來檢測資訊網路系統的安全程度與弱點。

文獻探討

一、駭客的定義

駭客(Hacker)又稱爲「駭客」、「害客」，其定義可分爲廣義與狹義兩種。廣義的駭客可定義爲「行爲人未經授權逕行進出電腦系統」⑥。狹義的駭客大致可定義爲「具有電腦(Computer)、系統(System)、網路(Network)等專業知識，並具備程式語言寫作能力的人，因個人興趣而未經授權逕行嘗試進出他人電腦系統」。

駭客雖攻擊系統，卻並未破壞該系統。眞正的駭客文化爲「視攻擊行動爲一種藝術，目的在考驗系統安全」。令系統管理者頭痛的其實是鬼客(Cracker)，鬼客又稱爲「怪客」、「快客」，可定義爲「不經過身分認證，想盡辦法存取電腦系統的人，目的在中斷與破壞系統、篡改系統資料、奪取使用權限與從中獲利，與駭客僅一線之隔」。要成爲一位電腦駭客，本身除了技術能力要強，能夠了解作業系統與通訊協定的深層技術，更清楚了解到系統的弱點與漏洞，並在攻擊過程中與攻擊之後能不被察覺。

此次研究所探討的駭客攻擊，採用廣義的定義，包含駭客與鬼客的攻擊行爲。

二、駭客攻擊的方法

目前常見的駭客攻擊方法，有下列幾種：⑦、⑧、⑨、⑩、⑪、⑫

㈠阻斷服務。

㈡網路監看。

---

④ 奇摩新聞中央社分類新聞，「雅虎遭駭客襲擊服務中斷三小時」，2000年2月8日。
⑤ 奇摩新聞C/NET分類新聞，「eBay、CNN、Amazon相繼遭駭客騷擾」，2000年2月3日。
⑥ 王旭正，高大宇，「規範駭客行為於網路安全之隱憂與未來發展」，資訊安全通訊，第5卷第3期，（1999年6月），頁97-106。
⑦ Kenny H.，「網路系統的攻擊與保護I、II」，高商圖書公司，（1999年5月）。
⑧ 同⑥。
⑨ 李麒麟，林美娜，「電腦犯罪終結者」，松崗電腦圖書資料公司，（1993年4月）。
⑩ 李麒麟，「駭客攻防」，資訊安全通訊，第5卷第3期，（1999年6月），頁86-96。
⑪ 黃世昆，「軟體系統安全弱點初探」，資訊安全通訊，第5卷第1期，（1998年12月），頁41-50。
⑫ 蘇澈，「駭客的秘密－網際網路篇、系統安全篇」，碁峰資訊公司，（1999年6月）。

㈢特洛依木馬。
㈣系統漏洞。
㈤網路掃描。
㈥暴力攻擊法。
㈦仿冒攻擊法。
㈧記憶體溢載攻擊法。
㈨病毒攻擊。
㈩大量垃圾信件與匿名信件。
(十一)密碼的竊取。
(十二)奪取管理員權限。
(十三)其他。

如果駭客擁有系統管理權限，就可直接對系統進行侵害，例如：直接破壞硬體設備、在未鎖住的畫面中輸入或讀取資料、在主機前使用駭客程式等。除此之外，還有「按鍵紀錄」方式的駭客程式，藉以紀錄受害者電腦上所有的按鍵資料，以判別出帳號密碼等有用資訊。人際關係上的溝通疏失所造成的密碼、資料外洩，也是駭客常用的手法之一。

根據以上所述13種攻擊方法，成爲此次研究整理駭客工具與攻擊程式、駭客攻防檢查表的13個類別。

三、駭客攻擊的對策

預防駭客攻擊的方法有很多，下列爲幾種常見的方法，能有效降低被駭客攻擊的機會。⑬、⑭、⑮、⑯、⑰、⑱、⑲

㈠密碼的管理。
㈡資料亂碼加密與數位簽章。
㈢回撥式安全系統。
㈣分析系統時序紀錄。
㈤稽核機制。
㈥封包過濾與防火牆。
㈦存取控制機制。
㈧安全弱點的偵測。
㈨攻擊者的偵測。
㈩使用駭客技術找出系統安全漏洞。
(十一)防毒軟體的使用。
(十二)隨時更新軟體版本，修正系統漏洞。
(十三)測試及評估安全措施或技術。
(十四)其它。

其他的對策，如：主機未使用到的通訊埠與服務應該予以關閉；不要執行與系統不相干的程式；重要資料應經常備份；檢查實體線路是否被偷接；機房要妥善的管理，避免被外人實體破壞等。另外，教育訓練資訊安全知識、確保安全與稽核政策的執行也是避免駭客攻擊的有效方法。

研究方法與步驟

一、研究方法與步驟

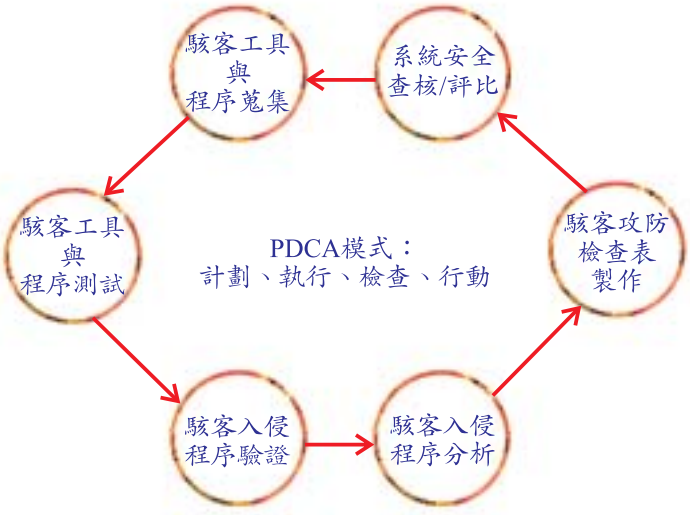
此次研究透過實際操作駭客工具與攻擊程式，以深入了解駭客攻擊系統的手法，並找出對策與防禦之道。

此次的研究步驟，如圖一。首先，是蒐集駭客工具與攻擊程式的文件。第二步就是

⑬ 同⑦。
⑭ 同⑥。
⑮ 同⑨。
⑯ 同⑩。
⑰ 林詠章，黃明祥，「網路系統安全之技術」，資訊安全通訊，第5卷第3期，（1999年6月），頁12-22。
⑱ 劉國昌，劉國興，「資訊安全」，儒林圖書公司，（1995年6月）。
⑲ 同⑫。

加以個別測試，其中有很多駭客工具是攻擊過程或攻擊後所要用到的輔助工具。第三步研究駭客攻擊系統的可能步驟與對策，並加以舉例、模擬與驗證。攻擊系統時，因爲攻擊種類的不同，所以步驟、需要的工具與程式、以及對策也會有所不同。

前面的三個研究步驟，是在學習及體會駭客如何攻擊系統，已深入了解其手法，進而找出對策。眞正研究的重點是在製作駭客攻防檢查表，以供資訊部門查核系統安全的漏洞，同時爲系統安全評等，供資訊部門主管參考。



圖一　研究步驟之模型

二、研究限制

此次研究僅針對Windows NT作業系統作研究，因此其他作業系統(Unix Like、Novell、OS/2等等)並不在研究的範圍。所蒐集的攻擊工具與程式中，有許多因爲作業平台需求、作業系統版本不同、時間、環境等因素無法驗證。因此檢查表的所涵蓋的項目與工具會因此而減少。

此外，檢查表中各類別雖因駭客工具與程式數量不同而檢查項目的數量便有所差異，但並非檢查項目的數量少便是重要性較低。其中，檢查項目因風險程度不同，重要性也有所差異，因此採用高、中、低三級評判其風險權重。然而高低評判的權重標準不易客觀，評分方式與評等均爲主觀建議，爲此次研究的限制。

驗證與對策

一、駭客攻擊系統可能步驟的驗證與對策

在個別測試各項駭客工具與攻擊程式之後，就是要開始應用這些工具與程式來嘗試攻擊資訊系統。駭客實際在攻擊系統時，除了單一駭客工具或程式的使用，也常綜合多種駭客工具與攻擊程式來進行。攻擊系統的種類很多，每個種類所需使用到的步驟、花費的時間與心力、使用的駭客工具與攻擊程式、以及因應的對策都有所不同。

由於駭客攻擊系統的種類與手法相當繁多，且日新月異，此次研究透過驗證方法，將可能的攻擊系統種類及其步驟與對策舉例於下。

㈠利用系統漏洞攻擊網路主機

1.攻擊步驟

⑴偵測欲攻擊主機作業系統、程式軟體版本。

⑵在網際網路上查詢該版本作業系統、程式軟體的漏洞資訊，取得攻擊所需工具技術。

⑶利用系統漏洞取得一般帳號。

⑷用各種駭客工具軟體或攻擊程式取得系統管理員權限。

⑸清除攻擊記錄與系統連線記錄。

⑹掌控與控制受害主機。

2.防護對策

隨時更新系統，修復系統漏洞，並且隨時注意系統時序紀錄檔有無可疑紀錄。

㈡特洛伊木馬攻擊

1.攻擊步驟

⑴架設FTP或WWW站台，將附有特洛依木馬Server端的檔案供人下載。

⑵讀取FTP或WWW站台連線紀錄，了解有哪些IP、使用者已經下載這些檔案。

⑶以特洛依木馬程式Client端來進行操控那些下載特洛依木馬Server端程式並且執行的受害者電腦。

⑷掌控與控制受害主機。

2.防護對策

不隨意下載來路不明的檔案，隨時檢查系統是否藏有特洛依木馬程式。

㈢阻絕服務

1.攻擊步驟

⑴利用網路掃描的工具，對欲攻擊的對象網路進行IP與Port的掃描，以得知欲攻擊對象網路中所有電腦IP與各電腦有開放使用的Port服務。

⑵對有開放使用的Port編號，以轟炸Port的駭客工具進行干擾。

⑶利用Ping of Dead或Ping Flooding方式造成大量封包來攻擊。

⑷被攻擊電腦的服務受到影響、網路流量爆增甚至癱瘓，嚴重時將造成原先所提供的服務暫時性或永久性中斷。

2.防護對策

使用防火牆、關閉未使用的Port、更新系統與TCP/IP伺服程式，避免被Ping of Dead方式的攻擊。分析系統時序紀錄，查出駭客來源位址，採取法律行動。

㈣竊取密碼檔，暴力攻擊法破解後攻擊

1.攻擊步驟

⑴以Anonymous FTP進入欲攻擊的系統中，或以其他方式竊取目錄下的password檔案。

⑵將所盜取來的密碼檔，以軟體工具進行字典攻擊或隨機碼攻擊，來破解密碼檔中使用者的密碼。其中，字典檔案的製作有程式來產生。

⑶盡可能破解出擁有root權限的帳號，或是以一般帳號登入系統後用各種工具軟體或方法取得系統管理員權限。

2.防護對策

做好密碼的管理，並經常性更新系統。

㈤監聽取得帳號密碼

1.攻擊步驟

⑴在己方電腦上執行監聽程式Sniffer（例如：Net XRay的Capture功能），捕捉流向被攻擊目標的封包。

⑵分析捕捉下來的資訊，判讀出帳號與密碼資訊。

⑶利用帳號密碼攻擊該目標。

2.防護對策

對於重要資訊在網路上流通時要加密、使用者密碼應經常更換、實體線路檢查有無被偷接。

㈥網頁仿冒(Web Spoofing)

1.攻擊步驟

⑴選定欲攻擊的網頁，以網頁複製軟體（例如：Telepro）將該網頁複製一份到己端電腦中。

⑵修改該網頁內容後，設立一個極似眞正網站伺服器的假網站伺服器。

表一　駭客工具總表例子

類別	軟體名稱	檔名	功能
阻斷服務	PortFuck 1.0b2	Portfuck.zip	拼命的攻擊主機的某port
	Internet Packet Tools v1.0	Ipt.zip	可以丟封包到某機器某port
網路監看	Net X Ray 3.0	Netxray.zip	管理監控整個網域，捉封包、測流量
特洛依木馬	Back Orifice 2000	bo2k.zip	爲特洛依木馬Server/Client程式
系統漏洞	CGSi OOB Messager	cg_oob.zip	攻擊未patch的95或未安裝SP3的NT，爲OOB攻擊工具
	WinGenocide	WinGenocide.zip	攻擊未patch的95或未安裝SP3的NT，爲OOB攻擊工具
網路掃描	AnyClassC 1.0	AnyClassC.zip	掃描所有calss c有用到的IP
暴力攻擊	John The Ripper_1.6	john-16w.zip	暴力或字典攻擊passwd檔案(Unix的密碼檔)
仿冒攻擊	IP Spoof	cha0sspoof.zip	IP僞造
電腦病毒	PC-cillin 98 v6.0	http://www.trend.com.tw/	趨勢科技的防毒軟體
信件干擾	Up Yours 4.0b3	uy4beta3.zip	功能很強的信箱炸彈
盜取密碼	SendBoy's Revelation	sendboy.zip	破解撥號網路中所記下的*號密碼資訊
奪取管理員權限	GetAdmin	getadmin.exe	將NT的一般帳號轉成管理員權限帳號

表二　駭客工具與攻擊程式已測試之列表

類別	工具或程式	過程	對策
系統漏洞	Wingenoc.zip	Wingenoc程式可以一次進行多個IP的攻擊，沒有patch過的NT就會當機	取得並安裝patch程式或安裝SP3以上的版本
特洛依木馬	Bo2k	首先將木馬想辦法放到對方電腦並執行後，即可遠端控制該電腦	利用cleaner v2.0探測並移除電腦中的特洛依木馬server
奪取管理者權限	GetAdmin.EXE	非Admin權限使用者登入NT Server本機後執行GetAdmin程式可以奪取Administrator權限	非Administrator或是一般使用者不可登入本機
暴力攻擊	L0phtcrack.exe	提供三種方式讀取NT密碼檔，再以字典法或暴力法來進行密碼破解	使用者應取無意義且夾雜英文數字的密碼
阻斷服務	Ping	利用Ping所發出的大量ICMP封包，造成對方網路負荷過重甚至癱瘓	將主機節點隱藏或是使用防火牆

⑶將假網站的網址登入到其他著名的搜尋引擎網站下，讓查詢的使用者受騙。

⑷使用者透過瀏覽器，查詢搜尋引擎連到假造的網頁，駭客從中得取使用者與網站間傳遞的資料。

2.防護對策

網頁管理者應經常查看各大搜尋引擎的連結有無問題，對於重要資訊在網路上流通時要加密，並採用數位簽章與具公信力第三者的認證（CA認證）。

駭客攻擊步驟

一、網路攻擊的步驟

㈠第一步：隱藏自己的位置

普通駭客都會利用別人的電腦隱藏他們眞實的IP地址，盜用他人的帳號上網。

㈡第二步：尋找目標主機並分析

駭客首先要尋找目標主機並分析。在Internet上能眞正標識主機的是IP地址，域名（DNS）是爲了便於記憶主機的IP地址而另起的名字，只要利用域名和IP地址就可以順利地找到目標主機。了解攻擊目標的位置之後，還須將主機的操作系統類型及其所提供服務等資料作個全面的了解。駭客們會使用一些掃描器工具，輕鬆獲取目標主機運行的是哪種操作系統的哪個版本，系統有哪些帳戶，WWW、FTP、Telnet 、SMTP等服務程式是何種版本等資料，爲攻擊作好充分的準備。

㈢第三步：獲取帳號和密碼，登錄主機

駭客要想攻擊一台主機，首先要有該主機的一個帳號和密碼，否則連登錄都無法進行。這樣常迫使他們先設法盜竊帳戶文件，進行破解，從中獲取某用戶的帳戶和密碼，再尋覓合適時機以此身份進入主機。當然，利用某些工具或系統漏洞登錄主機也是駭客常用的一種作法。

㈣第四步：獲得控制權

駭客們用FTP、Telnet等工具利用系統漏洞進入目標主機系統，獲得控制權之後，就會做兩件事：清除記錄和留下後門。更改某些系統配置、置入特洛伊木馬或其他一些遠端操縱程式，以便日後可以不被覺察地再次進入系統。大多數後門程式是預先編譯好的，只需要想辦法修改時間和權限就可以使用了，甚至新文件的大小都和原文件一模一樣。駭客一般會使用rep傳遞這些文件，以便不留下FTB記錄。清除日誌、刪除拷貝的文件等手段來隱藏自己的蹤跡之後，駭客就開始下一步的行動。

㈤第五步：竊取網路資源和特權

駭客找到攻擊目標後，會繼續下一步的攻擊。如：下載敏感訊息、實施竊取帳號密碼與信用卡號、網路癱瘓。

二、網路攻擊的原理和手法

㈠密碼攻擊

所謂密碼攻擊是指使用某些合法用戶的帳號和密碼登錄到目的主機，然後再實施攻擊活動。這種方法的前提是必須先得到該主機上的某個合法用戶的帳號，然後再進行合法用戶密碼的破解。

獲得普通用戶帳號的方法很多，例如：利用目標主機的Finger功能。當用Finger命令查詢時，主機系統會將保存的用戶資料（如用戶名、登錄時間等）顯示出來；利用目標主機的X.500服務：有些主機沒有關閉X.500的目錄查詢服務，也給駭客提供了獲得訊息的一條簡易途徑；從電子郵件地址中收集：

有些用戶電子郵件地址常會透露其在目標主機上的帳號；查看主機是否有習慣性的帳號：有經驗的用戶都知道，很多系統會使用一些習慣性的帳號，造成帳號的洩漏。

另外還有三種方法可以測知密碼：

1.通過網路監聽非法得到用戶密碼，這類方法有一定的局限性，但危害性極大。監聽者往往採用中途截擊的方法來獲取用戶帳號和密碼。很多網路協定本身就沒有採用任何加密或身份認證技術，例如在 Telnet(Port 23)、FTP (Port 21)、HTTP (Port 80)、SMTP (Port 25)等網路傳輸協議中，用戶帳號和密碼都是以明文格式傳輸的，此時若駭客利用封包截取工具便可很容易收集到你的帳號和密碼。還有一種中途截擊攻擊方法可以在使用者終端與伺服器端完成「三方交握」(Three-way Handshake)建立連線之後，在通信過程中扮演「第三者」的角色，假冒伺服器身份欺騙你，再假冒你向伺服器發出不當請求，其造成的後果不堪設想。另外，駭客有時還會利用軟體和硬體工具時刻監視系統主機的工作，等待記錄用戶登錄訊息，從而取得用戶密碼；或者編製有緩衝區溢出錯誤的 SUID 程式來獲得超級用戶權限。

2.在知道用戶的帳號後（如電子郵件 @ 前面的部分）利用一些專門軟體強行破解用戶密碼，這種方法不受網段限制，但駭客要有足夠的耐心和時間。如：採用字典窮舉法（或稱暴力破解法）來破解用戶的密碼。駭客可以利用工具程式，自動地從電腦字典中取出一個單字，作爲用戶的密碼，再輸入給遠端的主機，申請進入系統；若密碼錯誤，就按序取出下一個單字，進行下一個嘗試，並一直循環下去，直到找到正確的密碼或字典的單字試完爲止。由於這個破解過程由電腦程式來自動完成，因而幾個小時就可以把十萬多條記錄的字典裡所有單字都嘗試一遍。

3.利用系統管理員的失誤。在現代的 Unix 操作系統中，用戶的基本資料存放在 passwd 文件中，而所有的密碼則經過 DES 加密方法加密後專門存放在一個叫 shadow 的文件中。駭客們獲取密碼文件後，就會使用專門的破解 DES 加密法的程式來解密碼。同時，由於爲數不少的操作系統都存在許多安全漏洞、Bug 或一些其他設計缺陷，這些缺陷一旦被找出，駭客就可以長驅直入。例如，讓 Windows95/98 系統後門洞開就是利用 Windows 的基本設計之缺陷。

㈡放置特洛伊木馬程式

特洛伊木馬程式可以直接侵入用戶的電腦並進行破壞，它常被僞裝成工具程式或者遊戲等程式，誘使用戶打開帶有特洛伊木馬程式的郵件附件或從網上直接下載，一旦用戶打開了這些郵件的附件或者執行了這些程式之後，它們就會像古特洛伊人在敵人城外留下的藏滿士兵的木馬一樣留在自己的電腦中，並在自己的電腦系統中隱藏一個可以在 windows 啓動時悄悄執行的程式。當您連接到網路時，這個程式就會通知駭客，來報告您的 IP 地址以及預先設定的端口。駭客在收到這些訊息後，再利用這個潛伏在其中的程式，就可以任意地修改你系統的參數設定、複製文件、窺視你整個硬碟中的內容等，從而達到控制電腦主機之目的。

㈢WWW 的欺騙技術

在網路上的用戶可以利用 IE 等瀏覽器進行各種各樣的 Web 網站的訪問，如閱讀

新聞組、諮詢產品價格、訂閱報紙、電子商務等。然而一般的用戶恐怕不會想到有這些問題存在。假若正在訪問的網頁已經被駭客篡改過，網頁上的資料則是虛假的！例如駭客將用戶要瀏覽的網頁URL改寫爲指向駭客自己的伺服器，當用戶瀏覽目標網頁的時候，實際上是向駭客伺服器發出請求，那麼駭客就可以達到欺騙的目的了。

Web欺騙使用兩種手段，第一種手段是將URL地址重寫技術，利用URL地址，使這些地址都向駭客的Web伺服器，即駭客可以將自己的Web地址加在所有URL地址的前面。這樣，當用戶與網站進行安全連接時，就會毫不防備地進入駭客的伺服器，於是所有訊息便處在駭客的監視之中。第二種手段是訊息掩蓋技術，駭客往往在URL網址重寫的同時，利用相關訊息掩蓋技術，即一般是用JavaScript程式來重寫網址，以達到其欺騙的目的。

㈣電子郵件攻擊

電子郵件是網際網路上運用得十分廣泛的一種通訊協定。駭客可以使用郵件炸彈軟體或 CGI 程式向目的郵件信箱發送大量內容重複、無用的垃圾郵件，從而使目的郵件信箱被灌爆而無法使用。當垃圾郵件的發送超量時，郵件系統對於正常的郵件傳送工作則表現遲緩，甚至癱瘓。電子郵件系統的攻擊具有方法簡單、受損範圍廣等優點，歸納電子郵件攻擊主要表現有兩種方式：

1.電子郵件轟炸

通常指的是郵件炸彈，利用僞造的IP地址和電子郵件地址向同一信箱發送數以千計、萬計甚至無窮多次的內容相同的垃圾郵件，致使受害人郵箱被灌爆，嚴重者可能會癱瘓電子郵件伺服器。

2.電子郵件欺騙

駭客利用社交工程，佯稱自己爲系統管理員（郵件地址和系統管理員完全相同），給用戶發送郵件要求用戶修改密碼（密碼可能爲指定字串）或在貌似正常的附件中加載病毒或其他木馬程式。

㈤跳板攻擊

駭客攻擊主機後，往往會以此主機爲跳板，攻擊其他主機（以隱蔽其攻擊路徑，避免留下蛛絲馬跡）。利用網路監聽的方法（例如：Sniffer監聽程式），嘗試攻擊同一網域內的其他主機，由於彼此間都具備一定的信任關係，因此，滲透進入其它主機是很容易的。

SoftEther（虛擬網卡）是類比乙太網卡與集線器功能，進而使用 Tunnel 特性，實現VPN的功能，可以實現從 Internet 攻擊具防火牆的內部網路的目標。這個技術可讓駭客出入防火牆如入無人之地。

其主要實作觀念是：

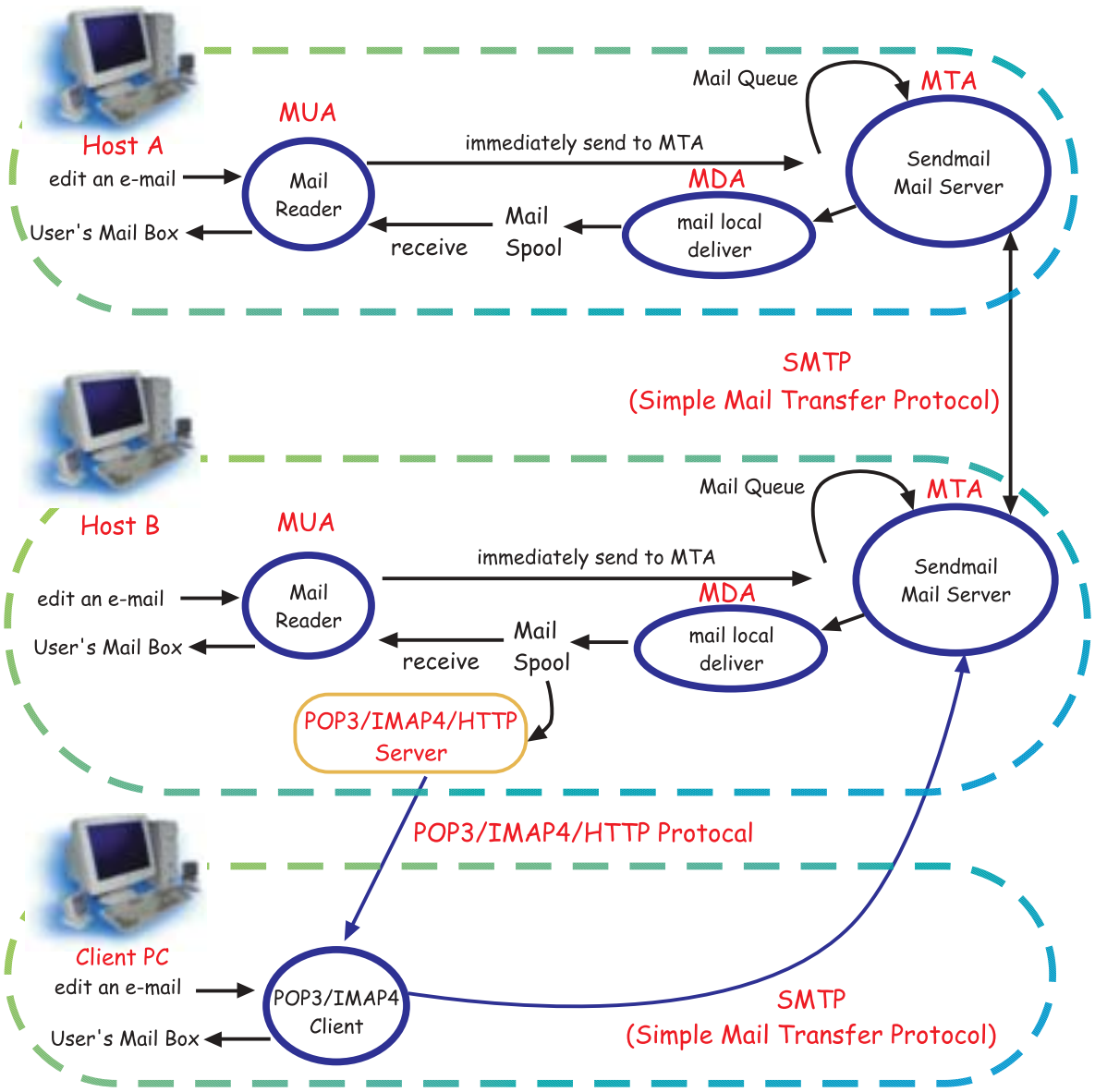
1.在OSI Level2（資料連結層）上軟體類比網路通訊，把物理層的通訊內容封包到 TCP Package 裏去（軟體類比 Ethernet）。

2.把自己的通訊包變成 SSL Session，用 HTTPS 協議穿越 Internet，甚至混過 Firewall (128bit RC4)。

有了這個東西，可以毫不誇張地說，所有的 Firewall 保護下的 LAN 都要面臨重大的安全性挑戰了，因爲只要內網中有一台機器通過此軟體虛擬成 LAN 網卡，就可以通過 Internet 毫無障礙地訪問內部網路。

㈥安全漏洞攻擊

許多系統都有安全漏洞(Bugs)，依照



圖二　郵件傳送接收流程

CERT/CC 之統計資料，自1995 年至2003年爲止，共計出現12,946 項系統弱點報告⑳，其中一些是操作系統或應用軟體本身具有的，如緩衝區溢位。

由於很多系統在不檢查程式與緩衝之間變化的情況，就任意接受任意長度的數據輸入，把溢出的數據放在暫存區裡，系統還照常執行命令。這樣駭客只要發送超出緩衝區所能處理的長度的指令，系統便進入不穩定狀態。若駭客配置有效的攻擊字串，系統執行後可以顯示整個根目錄，進而擁有主機的控制權。

⑳ CERT/CC Statistics 1988-2003(n.d.)Retrieved, March 15, 2004, http://www.cert.org/stats/cert_stats.html.

另外利用協定漏洞進行攻擊。例如駭客利用POP3的協定漏洞，或是利用ICMP協定發動阻斷服務攻擊。它的具體手法就是向目的伺服器發送大量的封包，幾乎占去該伺服器所有的網路頻寬，從而使其無法對正常的服務請求進行處理，而導致網站無法進入，網站處理速度大大降低或癱瘓。

現在常見的蠕虫病毒或與其同類的病毒都可以對伺服器進行阻斷服務攻擊的進攻。它們的繁殖能力極強，一般通過Microsoft Outlook軟體中的通訊錄中的衆多郵件地址發出帶有病毒的郵件，而使郵件伺服器無法承擔如此龐大的處理量而癱瘓。

駭客常用的攻擊工具

一、D.O.S攻擊工具

利用 WinNuke 針對系統漏洞發送大量封包，導致系統癱瘓；利用 Bonk 通過發送大量僞造的 UDP 封包導致系統重啓；利用 TearDrop 通過發送重疊的 IP 碎片導致系統的 TCP/IP 協定崩潰；利用 WinArp 通過發出特殊封包在對方機器上產生大量的窗口；利用 Land 發送大量僞造 IP，使得 SYN 的 TCP 連線請求，導致系統重啓；利用 FluShot 發送特定 IP 封包導致系統癱瘓；利用 Bloo 發送大量的 ICMP 封包導致系統癱瘓；利用 PIMP 針對 IGMP 漏洞，導致系統緩慢甚至重新啓動；利用 Jolt 發送大量僞造的 ICMP 和 UDP 封包，導致系統變的非常慢甚至重新啓動。

二、木馬程式

㈠BO2000(BackOrifice)

它是功能最健全的攻擊工具，可以搜集訊息，執行系統命令，重新設置機器，重新定向網路的客戶端／伺服器應用程式。BO2000支持多個網路協議，它可以利用TCP或UDP來傳送，還可以用XOR加密算法或更高級的3DES加密算法加密。感染BO2000後機器就完全在別人的控制之下，駭客成了超級用戶。

㈡「冰河」

冰河是一個國產木馬程式，具有簡單的中文使用界面，且只有少數流行的反病毒、防火牆才能查出冰河的存在。它可以自動跟蹤目標機器的螢幕變化，可以完全模擬鍵盤及滑鼠輸入。同時，可以同步記錄各種密碼訊息，包括開機密碼、螢幕保護密碼、各種共享資源密碼以及絕大多數在對話框中出現過的密碼訊息、系統訊息。

㈢NetSpy

可以運行Windows95/98/NT/2000等多種平台上，是一個簡單的文件傳送軟體，但實際上你可以將它看作一個沒有權限控制的增強型FTP伺服器。通過它，駭客可以神不知鬼不覺地下載和上傳目標機器上的任意文件，並可以執行一些特殊的操作。

㈣Glacier

該程式可以自動跟蹤目標電腦的螢幕變化、獲取目標電腦登錄密碼及各種密碼訊息、獲取目標電腦系統訊息、限制目標電腦系統功能、任意操作目標電腦文件及目錄、遠程關機、發送訊息等多種監控功能。

㈤KeyboardGhost

Windows系統是一個以消息循環(MessageLoop)爲基礎的操作系統。系統的核心區保留了一定的字節，作爲鍵盤輸入的緩衝區。鍵盤幽靈是擷取使用者在網路上輸入帳號與密碼過程中的鍵盤記錄，僅管密碼在

螢幕上是以星狀符號隱藏，但是所有符號都會被記錄下來，並在系統根目錄下產生一文件名爲KG.DAT的隱藏檔。

㈥ExeBind

將指定的攻擊程式內建到任何一個熱門軟體上，使宿主程式執行時，寄生程式也在後端被執行，且支持多重隱藏。實際上是通過多次分割文件，從父程序中載入子程序來實現的。

駭客攻防檢查表

由於駭客攻擊手法與對策的種類十分繁多，所以資訊部門在架構與測試系統安全時，不易顧及到所有的種類。因此此次研究在驗證駭客攻擊與對策後，製作出一份駭客攻防檢查表（表三），試著從駭客角度來檢測資訊網路系統的安全程度與弱點。填答的同時，系統管理員可根據檢查表所提供的選項進行檢查，如未做到但能改善的選項，可即時改善後再勾選，因此本檢查表有提醒與查核系統安全的功能。填答完後的評等可提供資訊部門主管對資訊網路系統安全的參考與了解。

一、填寫檢查表的步驟

表三　駭客攻防檢查表

駭客攻防檢查表		如果有做到，請在安全欄打勾	回答（勾選）判斷	填答	填答	風險評估
類別	項目	偵測防禦工具或方法		是	否	
1.阻斷服務	Port轟炸		是否不受干擾？			2
	Port管理	關閉未使用的Port	是否有關閉？			3
	Ping of Dead	系統是否更新以避免DDOS攻擊	是否有更新？			3
	Ping Flooding		是否不受干擾？			2
2.網路監看	封包截取		是否無法從被截取封包中分析出資訊？			2
	防火牆使用	防火牆的使用	是否有使用防火牆？			3
	加密傳輸	傳輸資料有加密	是否有加密？			3
3.特洛依木馬	特洛依木馬		是否沒有特洛伊？			3
	特洛依木馬	Cleaner v2.1	是否有定期掃描系統中藏有特洛伊？			3
	程式比較	比較兩支相同版本的程式以確定無被附加特洛依的程式	是否有比較？			2
4.系統漏洞	Log檔案檢視	定期檢視Log檔案內容	是否定期檢視Log？			3
	更新系統	勤於更新系統程式patch或升級系統	是否勤於更新系統？			3
	Port掃描		是否掃描失敗？			2
5.網路掃描	Port管理	關閉未使用的Port	是否有關閉？			3
	密碼破解password檔		密碼是否沒有被破解？			3

6.暴力攻擊	密碼破解		密碼是否沒有被破解？			3
	密碼破解	使用不規則且夾雜數字與字母的密碼	密碼是否如此？			3
	管理員仿冒登入	Dial-Back Systems	是否有使用回撥系統？			2
7.仿冒攻擊	網站仿冒	定期到各大搜尋引擎站台檢查網站連結是否有誤	是否經常檢查？			3
	數位簽章	數位簽章的應用	是否有使用？			2
	程式溢位	更新有問題的程式與系統	是否有更新？			3
8.記憶體溢載攻擊	Exchange主機緩衝區溢位		是否沒有當機？			3
	防毒軟體	安裝並常駐掃毒程式	是否有安裝常駐？			3
9.電腦病毒	防毒軟體	定期更新病毒碼	是否有定期更新？			2
	控制程式的執行	不執行來路不明的程式	是否確實落實？			3
10.信件干擾	Mail Bomb	(可利用deflooder或bomsquad程式來清理被轟炸的信箱)	是否沒有被轟炸到？			1
	防止垃圾信件	安裝filter檔掉大量相同信件進入信箱	是否有安裝？			3
	匿名信		是否沒有收到匿名信？			1
	密碼保護	經常或定期更換密碼	是否有經常或定期更換？			2
11.盜取密碼	撥接帳號密碼盜取		是否無法獲得帳號密碼？			1
	FTP盜取密碼檔		是否無法抓到passwd檔？			2
	盜取Shadow過的password檔案		是否無法破解Shadow過的password檔案？			2
	變成Admin		是否無法變成Admin？			3
12.奪取管理員權限	管理員的確認	定期查詢有誰擁有管理者權限	是否有定期查詢？			3
	按鍵紀錄		是否無法紀錄？			2
13.其他	使用稽核軟體	BindView稽核軟體	是否有使用稽核軟體？			3

㈠當系統在執行檢查時可能會造成服務中斷、系統當機、執行速度變慢等情形，所以在執行檢查前應先對系統使用者先行聲明。

㈡欲檢查作業系統版本爲何？系統所提供的服務爲何？請調查清楚。

㈢配合欲填答的項目，將所需使用到的工具依類別從光碟中準備好。

㈣依照類別順序一一填答其中項目，每做完一個類別再進行下一個類別。

㈤填答完整份檢查表後，請依照下列說明計算分數：

1.「風險評估」欄中的1、2、3代表加權值。加權值的多少，純屬主觀建議。

2.各項目填答「否」的要計算加權，填

答「是」的則不用。

3.計算出各類別中填答「否」的加權總分。

4.計算出各類別有填答項目的總加權值。

5.將各類別加權總分除以各類別的填答項目總加權值得到平均分數，爲類別評分。

6.將13個類別評分加總，計算出整份檢查表的總評分。

二、檢查表的評等與分析

填完整份檢查表，並統計完各項數據後，請依照以下敘述進行評等與分析。檢查表的計分方式與評等均屬此次研究主觀的建議，僅供參考。

㈠各類別評分最佳得分爲0分，最差得分爲1分，得分愈高代表風險程度愈高。

㈡檢查表總評分最高爲13分，代表風險度最高，最低爲0分，代表風險度最低。

㈢若檢查表總評分達8分以上，評等爲「劣等」，表示該系統容易被駭客攻擊成功，其系統安全必須馬上加以檢討與改進。

㈣若檢查表總評分在4～8分，評等爲「中等」，表示該系統安全仍有漏洞，請詳細參閱13項類別評分。找出評分最高分的類別開始改善，直到總評分接近0分。

㈤若檢查表總評分在4分以下，評等爲「優等」，表示該系統有確實執行防禦駭客攻擊的措施，擁有較好的系統安全。

㈥本檢查表有一特性，分數愈高表示被攻擊的風險愈高，愈容易被攻擊成功，因此總評分4分以上的都還有改善的空間，應依各類別各項目一一檢討改進。

主管可依據檢查表總評分了解系統安全的程度，依據類別評分以了解系統安全措施尚需加強改進的地方。

結論

此次研究有下列主要成果、結論或發現：

一、製作出一份駭客攻防檢查表。除了能提供資訊系統安全的評等給予資訊部門主管參考之外，在填寫這份檢查表的同時，可以讓資訊部門人員查核系統的安全漏洞以圖改進。

二、此次研究於驗證的過程中，發現駭客攻擊的對策，主要是在針對「駭客工具」或「攻擊程式」上。在駭客攻擊系統過程中，如果能有效對抗其中單一或少數步驟，就能大幅降低攻擊系統的成功率。

三、透過驗證，此次研究將可能的攻擊系統種類及其步驟與對策舉例出來。這些攻擊的種類有下列特性：

㈠實際操作並非十分困難。

㈡用到的駭客工具，任何人都能容易取得。

㈢攻擊程式易於理解且容易嘗試。

㈣破壞的成效大。

㈤以低成本得到最有效的攻擊成果。

因此在對駭客攻擊進行上述分析與識別的基礎上，我們應當認眞制定有針對性的策略與安全對象，設置強有力的安全保障體系。在網路中層層設防，發揮網路的每層作用，使每一層都成爲一道關卡，從而讓駭客無隙可鑽、無計可使。還必須做到未雨稠繆，預防爲主，將重要的數據備份並時刻注意系統運行狀況。以下是針對衆多令人擔心的網路安全問題，提出的幾點建議：

一、提高安全意識

㈠不要隨意打開來歷不明的電子郵件及文件，不要隨便執行陌生人給你的程式，例如

「特洛伊」木馬駭客程式就是利用社交工程騙你執行。

㈡盡量避免從Internet下載不知名的軟體、遊戲程式。即使從知名的網站下載的軟體也要及時用最新的病毒和木馬偵測軟體對軟體和系統進行掃描。

㈢密碼設置盡可能使用字母數字混排，單純的英文或者數字很容易窮舉。將常用的密碼設置不同，防止被人查出一個，連帶到重要密碼。重要密碼最好經常更換。

㈣及時下載安裝系統更新程式。

㈤不隨便運行駭客程式，不少這類程式運行時會發出你的個人訊息。

㈥在網路上發現輸入帳號與密碼的提交警告，先看來源代碼，很可能是騙取密碼的陷阱。

二使用防毒、防攻擊的防火牆軟體。防火牆是一個用以阻止網路駭客攻擊的基本網路屏障，也可稱之爲控制進／出兩個方向通信的咽喉點。在網路邊界上通過建立起來的相應網路通信監控系統來隔離內部和外部網路，以阻檔外部網路的侵入。

三設置代理伺服器，隱藏自己的IP地址。保護自己的IP地址是很重要的。事實上，即便你的機器上被安裝了木馬程式，若沒有你的IP地址，駭客也是沒有辦法攻擊，而保護IP地址的最好方法就是設置代理伺服器。代理伺服器能扮演外部網路瀏覽內部網路的中間轉介角色，其功能類似一個NAT轉換，它主要控制哪些用戶能訪問哪些服務類型。當外部網路向內部網路申請某種網路服務時，代理伺服器接受申請，然後它根據其服務類型、服務內容、被服務的對象、服務者申請的時間、申請者的網域名稱等來決定是否接受此項服務，如果接受，它就向內部網路轉發這項請求。

四將防毒、防駭當成日常例性工作，定時更新病毒碼，將防毒軟體保持在常駐狀態，以徹底防毒。

五駭客經常會針對特定日期發動攻擊，電腦用戶在此期間應特別提高警戒。

六重要個人資料做好嚴密的保護，並養成資料備份的習慣。

參考資料

一駭客攻防指南2002.3系統漏洞（多個個人防火牆外出包可繞過漏洞）。

二駭客攻防指南2002.3駭客入門（攻擊手法）。

三駭客攻防指南2002.3駭客技術（網路常見攻擊與防範完全手冊）。

四駭客攻防指南2002.3駭客入門（用DOS命令破除UNIX管理員密碼）。

作者簡介

李武耀上尉，國防大學中正理工學院資訊科學系86年班、國防大學中正理工學院電子工程研究所92年班，曾任排長、資訊安全官，現任陸軍通信電子資訊學校資訊作戰組教官。

王福東中校，中正理工學院正48期電機系，中央大學資訊及電子研究所碩士、中央大學電機研究所博士，曾任排長、自動資料處理官、主任教官，現任陸軍通信電子資訊學校資訊作戰組主任教官。

李佳青上尉，國防大學中正理工學院資訊科學系86年班、國立臺灣師範大學資訊教育所92年班，曾任排長、組長、教官，現任陸軍通信電子資訊學校資訊作戰組教官。