網路安全

戴江淮／編著

全威圖書有限公司

網路安全

網路安全

戴江淮／編著

全威圖書有限公司

國家圖書館出版品預行編目資料

網路安全 / 戴江淮編著. -- 初版，-- 臺北縣五股鄉：全威圖書，民 96.07
面： 公分

ISBN 978-986-6964-31-2 (平裝)

1. 資訊安全

312.976 96012419

網路安全 (書號：220913)

中華民國 96 年 8 月 10 日初版發行
編 著：戴 江 淮
發行人：楊 明 德
出版者：全 威 圖 書 有 限 公 司
電 話：(02)22900319 郵撥：16750860
網 址：www.gau-lih.com.tw
住 址：台北縣五股工業區五工三路116巷3號
登記證：行政院新聞局局版臺業字第5361號

定價：580 元整

ISBN：978-986-6964-31-2

序 Preface

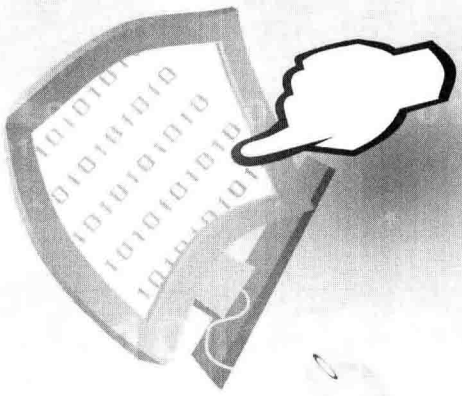
事實上這本書的出版與否，作者內心十分掙扎，回想起第一次(1998 年）教這門課時，有四個學生居然在課堂上，利用教室的電腦對系上主機來個實際演練，不僅入侵系上主機，同時也把主機內的檔案全部殺光，害得系主任要做出把這些學生死當及記過的處分。這對我實在很為難，因為這四個學生真的學到了精髓，要當掉他們真的沒道理，反而應該給他們通過才對啊！只不過我沒有教他們如何不留下痕跡而已（嘻嘻）。所以自從那次之後，作者七年來就不願再教授這一門課。然而實在有感於目前國內對培養網路安全的人才實在是太少，尤其是無線網路及大系統的設計更是缺乏，因此重新興起教授這一門課的念頭，也促使這一本書的誕生。

在撰寫這本能夠讓讀者設計網路安全接取系統的前提下，作者找遍所有的書籍，發現幾乎都著重在理論方面，除了 TCP/IP 系統設計的書籍以外，沒有一本是用得上的。至於坊間所看到的書籍大部分都是談論資訊安全，全都是一些紙上談兵的言論，沒有教導讀者該如何應用、規劃與設計。有些書標示的是網路安全，但是大部分都在討論密碼學，而密碼學上談的都是一些訊息加密的方法，這與真正的網路安全相差甚遠（雖然是其基礎）。另外有些書則告訴你如何操作系統與設備，如何去設定你的機器，但這種方式是針對低階的工程人員而精心設計的，因此作者才想要編寫本書，希望對讀者在網路安全上能有真正的助益。這一本書與第一次教授時的講義相差很多，因為是正式出版的關係，因此對於駭客手法諸多保留。

這一本書的程式是以 Visual Basic、Visual C 與 Linux C 為主，但是在 SIP 設計上則以 JAVA 來概略性講解（有興趣的可以參考本人寫的「網路電話 SIP 原理與應用」）。因為牽涉到的題材甚多，本書僅將目前最常用到或遇到的設備與協定（不含 TCP/IP）作一詳盡解說。這一本書並不著重在程式說明，所以你必須具備 Visual Basic 以及 Visual C 的基本指令與設計基礎，否則你將看不懂程式。至於程式的來龍去脈，也請詳細地把理論看懂，這樣才能讓你很快進入網路安全設計的行列。

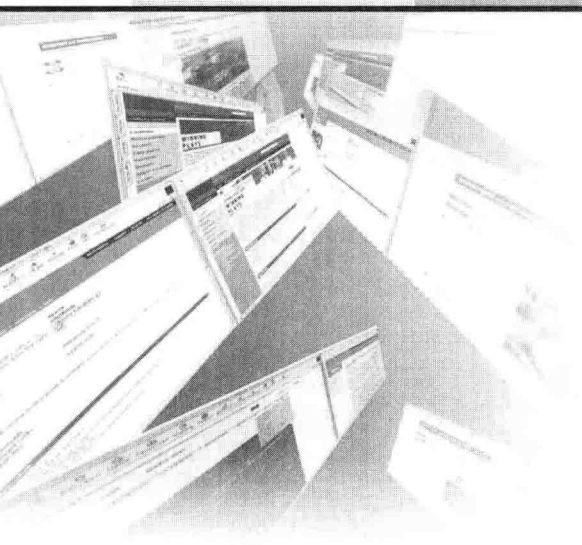
這本書有些內容談到駭客的手法（雖然已經僅可能把它移除這些章節程式），但這些程式只是作為理論上的參考，也只是提醒一個網路管理人員對安全性的注重與系統缺失上的修改，沒有教你犯罪的企圖。如果你學會之後，將這些用於犯罪上，那責任請自己負責，作者可不負任何責任。若有任何建議亦歡迎指教。

戴江淮
於大葉大學電機工程系



目錄

第一篇 系統概論



Chapter 1

前　言

網際網路的快速發展，客戶端即時需求也勢必日益殷切，但在開放網路服務的同時，網路安全即成為重要的考量。邇來網路入侵事件時有所聞，實應強化入侵偵測系統，並建立網路安全作業管制辦法，及加強內部資訊安全教育，方能具備足夠的網路安全防禦，以確保資訊系統之可用性、完整性及機密性。市場上出現許多產品來提供保衛網路免於駭客入侵的威脅，常見的系統架構是將防火牆與網路串接，藉由 IP 位址或通訊埠來過濾網路信文；並透過入侵偵測系統來監控廣播的信文，這樣的架構在理論上可以阻擋駭客的入侵。不幸的是隨著入侵手法的日新月異，這個假設在發生諸多網路入侵案例後被逐一推翻。許多有經驗的駭客有能力藉由 ICMP、CGI 等入侵技巧，欺瞞防火牆，藉由合法的網頁存取，輸入特殊存取碼，一路過五關斬六將進入網路系統取得有用的情報資訊。

針對網路安全的建置需藉由精心設計的整合型網路防衛系統。即使是建立在同樣的基礎架構上，但為了有效管理整體網路暨系統所隱含的弱點，在系統的建置過程中，應搭配系統及網路弱點稽核等輔助工具，以掃描內部以 TCP/IP 為通訊基礎的網路設備或伺服器。對於較重要的資料伺服器則可進一步對系統上的存取設定進行掃描檢查，以強化安全性。

除了以架構上的設計來提昇安全性外，整個安全機制的部署過程更是我們所應該加以重視的，以確實反應出安全性的問題上“攻”與“防”的方法，而非只是單方面由產品來提供防衛功能。要落實網路安全，每一個機關單位或部門均應該成立資訊安全建置小組，以落實網路安全防衛縱深。資訊安全建置小組（以下各章節中我們簡稱為資安小組）可採用美國 ISS 的 ADDME (Access Design Deployment Manage Educate) 網路安全解決方

Figure 圖 1.1 ADDME 網路安全解決方案

案，由環境評估、設計如何部署、軟體部署、管理與維護與教育訓練，構成完整的組織網路安全解決方案。

SafeSuite Decision 整合防衛工具以支援資訊安全決策的迴路圖則如圖 1.2 所示。

1.1 資訊內容的安全性

雖然密碼係身份識別與授權權限驗證過程中的核心，但它只是最基本的保護機制而已，它並不是全功能的安全工具。加密系統的弱點是：(1) 我們需能找出一最複雜的密碼才能保證不被破解，或者可能都無法破解；(2) 密碼本身很容易洩漏。在此我們必需知道一個系統唯有良好的管理功能才能發揮真正的效用，否則加密方式常會造成人們一種錯誤的安全意識。另外，保密方式可分為傳統密碼學與現代密碼學兩種方式。對傳統的保密方式並沒有複雜的計算，而是採用幾何方式加以執行。其缺點在於很容易被有心人士解除其密碼。

密鑰技術不僅可以防止未經授權的用戶在網路上竊取資料外，也可以防止軟體工具在網路上惡意的攔截與破壞 (例如 sniffer 軟體的曲解與運用)。一般而言，資料加密依照通訊的技術層面而言，又可以分為鏈路加密、節點加密與端點對端點間的加密。這些名詞意義的不同點，現區分如下：所謂端點至端點間的加密係指在訊息發送的來源之處，至訊息傳抵的目標端點處之間的訊息傳送，永遠都是以密文的形式來完成的，而且在由訊息的來源處被發送之後，直至目的地抵達之前，這訊息在傳送過程中是不會被任何中繼站或節點加以解密的。