GOTOP E&T

基峰學苑

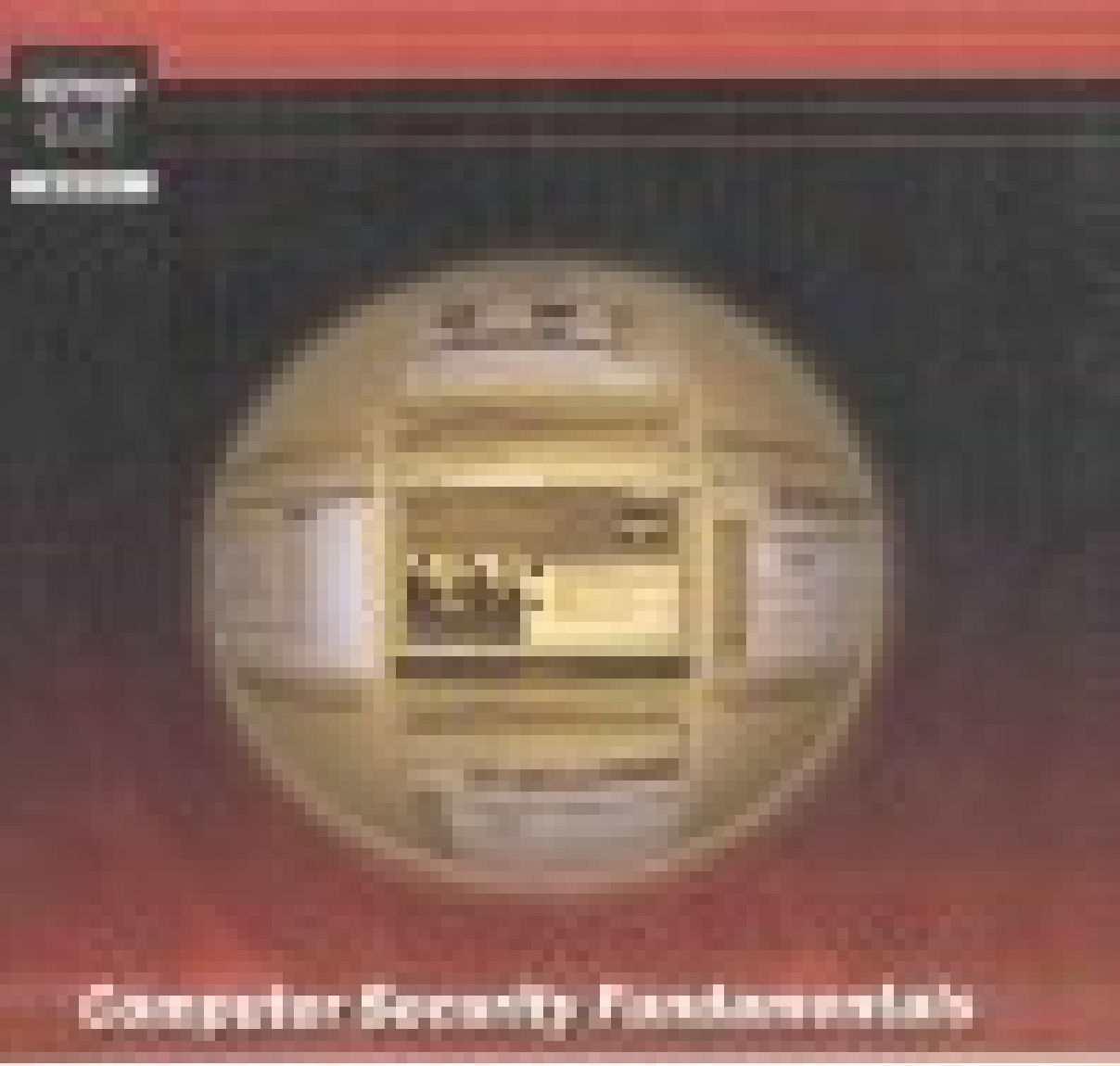
Computer Security Fundamentals

資訊安全
基礎概論

Chuck Easttom 著
蘇維宗/黃志雄/林安迪 譯

PEARSON Prentice Hall

碁峰 www.gotop.com.tw



Computer Security Fundamentals

資訊安全
基礎概論

Chuck Easttom II

資訊安全

基礎概論

Computer Security Fundamentals

Chuck Easttom 著

蘇維宗、黃志雄、林安迪 譯

碁峰資訊股份有限公司
GOTOP INFORMATION INC.

PEARSON Education Taiwan
台灣培生教育出版股份有限公司
Pearson Education Taiwan Ltd.

國家圖書館出版品預行編目資料

資訊安全 / Chuck Easttom著 ; 蘇維宗, 黃志雄, 林安迪譯. -- 初版. -- 臺北市 : 碁峰資訊, 2008. 2
面 ; 公分
譯自 : Computer security fundamentals
ISBN 978-986-181-326-4(平裝)

1. 資訊安全 2. 電腦網路

312.976 96023871

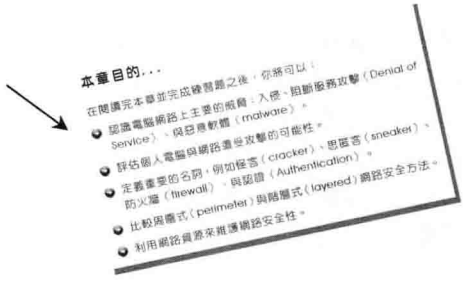
資訊安全基礎概論

原著	Chuck Easttom
譯者	蘇維宗、黃志雄、林安迪
出版者	台灣培生教育出版股份有限公司
	地址／台北市重慶南路一段147號5樓
	電話／02-2370-8168
	傳真／02-2370-8169
	網址／www.PearsonEd.com.tw
	E-mail／hed.srv@PearsonEd.com.tw
發行所	碁峰資訊股份有限公司
	地址／台北市南港路三段52號7樓
	電話／02-2788-2408
	傳真／02-2788-1031
	網址／www.gotop.com.tw
總經銷	碁峰資訊股份有限公司
出版日期	2008年2月一刷
書號	AEE009800
定價	490元
ISBN	978-986-181-326-4

書籍的使用方式

Prentice Hall 資訊安全書籍提供了專家的實際建議與實際操作練習，讓學生可以為跨入 IT 產業作準備。書中包含了許多真實的範例，幫助學習者將所學習的知識運用在實務工作上，同時也提供了很多可以幫助學習所設計的重要元素。

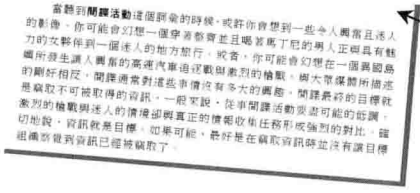
本章目的：以簡短扼要的方式條列出各章所包含的內容與目的


本章目的...

在閱讀完本章並完成練習題之後，你將可以：

- 認識電腦網路上主要的威脅：入侵、阻斷服務攻擊（Denial of Service）、與惡意軟體（malware）。
- 評估個人電腦與網路遭受攻擊的可能性。
- 定義重要的名詞，例如駭客（cracker）、思客客（sneaker）、防火牆（firewall）、與認證（Authentication）。
- 比較周邊式（perimeter）與階層式（layered）網路安全方法。
- 利用網路資源來維護網路安全性。

章節介紹：各章皆從解釋這些主題的重要性以及該章與全書整體的關係開始進行


介紹

當聽到**間諜活動**這個詞彙的時候，或許你會想到一些令人興奮且迷人的影像。你可能會幻想一個穿著整齊並且喝著馬丁尼的男人正與具有魅力的女郎伴到一個迷人的地方想行，或者，你可能會幻想在一個異國島國所發生讓人興奮的高速汽車追逐戰與激烈的槍戰。縱大章裸體所描述的剛好相反，間諜通常對這些事情沒有多大的興趣。間諜最好的目標就是竊取不可被取得的資訊，一般來說，從事間諜活動要盡可能的低調，激烈的槍戰與迷人的情境卻與真正的情報收集任務形成強烈的對比。確切地說，資訊就是目標。如果可能，最好是在竊取資訊時並沒有讓目標組織察覺到資訊已經被竊取了。

實務練習：說明各章的概念如何被運用在實際作業上

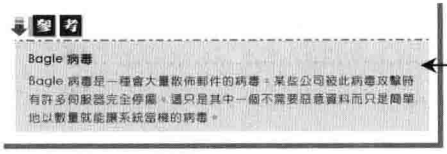

實務練習

在 Windows 作業系統中過濾通訊埠

Windows 2000 與 Windows XP 都有通訊埠過濾服務。（此通訊埠過濾服務無法根據每個介面設定。任何在此通訊埠過濾服務上的設定會套用在所有介面上。）

1. 到「控制台」並雙擊「網路連線（Network Connections）」（譯註：在 Windows XP 中，「網路連線」在「網路和網際網路連線」選項下）。你可以看到一個與圖 6.3 類似的視窗。
2. 右擊「區域連線（Local Area Connection）」並選擇「內容（Properties）」。你會看到一個與圖 6.4 類似的對話盒。

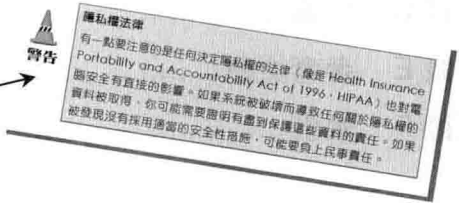
參考：提供本書範圍之外的資訊


參考

Bagle 病毒

Bagle 病毒是一種會大量散佈郵件的病毒。某些公司被此病毒攻擊時有許多伺服器完全停擺。還只是其中一個不需要惡意資料而只是簡單地以數量就能癱系統當機的病毒。

警告：與本文直接相關且重要、不能被遺忘的資訊


警告

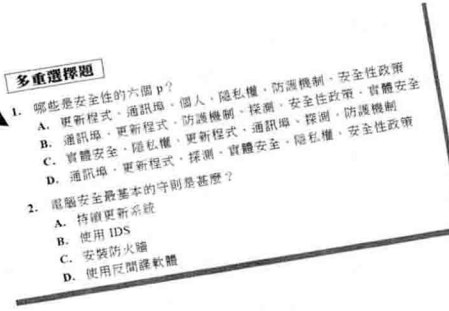
隱私權法律

有一點要注意的是任何決定隱私權的法律（像是 Health Insurance Portability and Accountability Act of 1996，HIPAA）也對電腦安全有直接的影響。如果系統被破壞而導致任何關於隱私權的資料被取得，你可能需要證明有盡到保護這些資料的責任。如果被發現沒有採用適當的安全性措施，可能要負上民事責任。

測試能力

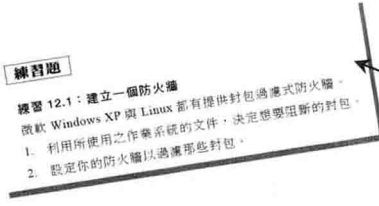
各章末提供了經過設計的練習題，包含四種評量形態：

多重選擇題：測試學習者對於各章內容的了解程度


多重選擇題

1. 哪些是安全性的六個 p？
   A. 更新程式、通訊埠、個人、隱私權、防護機制、安全性政策
   B. 通訊埠、更新程式、防護機制、探測、安全性政策、實體安全
   C. 實體安全、隱私權、更新程式、通訊埠、探測、防護機制
   D. 通訊埠、更新程式、探測、實體安全、隱私權、安全性政策
2. 電腦安全最基本的守則是甚麼？
   A. 持續更新系統
   B. 使用 IDS
   C. 安裝防火牆
   D. 使用反間諜軟體

練習題：針對每章各個單一觀念所設計的小型專案練習

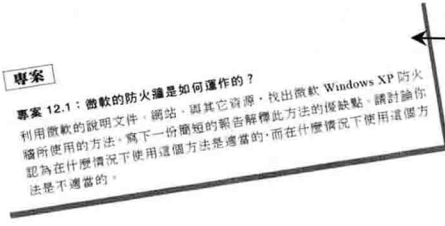

練習題

練習 12.1：建立一個防火牆

微軟 Windows XP 與 Linux 都有提供封包過濾式防火牆。

1. 利用所使用之作業系統的文件，決定想要阻斷的封包。
2. 設定你的防火牆以過濾那些封包。

專案：結合每章多個觀念的大型專案


專案

專案 12.1：微軟的防火牆是如何運作的？

利用微軟的說明文件、網站，與其它資源，找出微軟 Windows XP 防火牆所使用的方法。寫下一份簡短的報告解釋此方法的優缺點。請討論你認為在什麼情況下使用這個方法是適當的，而在什麼情況下使用這個方法是不適當的。

學習案例：必須運用每章所學習的內容來解決實際的案例


學習案例

Jane Doe 在小型醫院承包商中擔任負責資訊安全的網際網路管理者。她的公司負責處理一些較低層級的資料。她已經實作了一個非常安全的方法，包含：

- 利用防火牆關閉所有不需要的通訊埠。
- 在所有機器上安裝病毒掃描器。
- 被護每個網段之間路由器的安全。
- 所有機器會在每個月進行作業系統的更新。
- 密碼很長、很複雜、而且每 90 天必須進行變更。

你還會給 Jane Doe 甚麼其它的建議嗎？請解釋每一個建議的理由。

前言

此書被定位為一本入門書籍，對資訊安全領域提供一般性的介紹。本書說明了駭客如何鎖定一個系統、取得資訊、以及利用這些資訊來入侵系統。學生可以學習到如何利用密碼與網路掃描工具來保護自己的系統。雖然本書會說明一些破壞安全性的細節，但並不是一本駭客手冊。書中的說明、定義、與範例都是用來強調維護資料、電腦、與網路安全的重要性。在這些內容之後總是會有為了保護貴重資訊所應該採取的步驟。

最後，本書主要是以 Windows 的角度來探討安全性。選擇 Windows 是因為它被廣泛地使用而且經常成為攻擊的目標，然而實際上本書所包含的觀念可以應用在任何系統上。

讀者

本書是為了給想要獲得關於此領域完整介紹的學生所撰寫的入門書籍。雖然，這本書只是概論，但是內容假設讀者為稱職的電腦使用者 — 這代表會在工作場所或家中使用電腦、會使用電子郵件與網頁瀏覽器、而且知道 RAM 和 USB 這些術語所代表的意義。讀者應該具備對於個人電腦的基本認識，但並不一定需要先修過正式的電腦課程。

非正規電腦科學與電腦資訊系統部門的人可能也會發現這本書很有用，特別是執法人員、刑事司法單位人員與企業主管。

本書內容

此書以電腦網路犯罪和安全的概論作為開端。第 1 章，網路犯罪和安全介紹，詳述了網際網路犯罪的嚴重性以及為何學習如何讓系統免於攻擊是如此重要。本章介紹一些電腦安全的基礎 — 威脅的型態、常見的攻擊、術語、安全形態 — 並說明關於安全性的法律議題。最後，會介紹一些可以容易取得的安全性資源並在課文最後的練習和專案中指導學生探究這些工具。

第 2 章，電腦網路和網際網路，介紹了成功的網路安全所需要最重要的元素之一：優秀的網路運作實用知識。某些具有許多電腦經驗的讀者可能已經非常熟悉這裡所提到的內容，因此可以將略讀本章並當作參考。然而，缺乏經驗的讀者就應該學習基本的網路模型與運作方式。本章最後關於 IPConfig、tracert、與 ping 的實務練習可以說明瞭解一個網路與其運作方式將有助於維護網路安全。

第 3 章，評估系統安全性，強調一些駭客用來評估目標系統弱點的工具 — 並說明網路安全管理者如何使用相同的工具來評估系統的安全性以避免成為目標系統。實務練習可以帶領學生使用一些最常見的通訊埠掃描器，而本章最後的練習題可以讓學生進一步了解這些工具。

第 4 與第 5 章深入探討駭客可能發動的特定攻擊型態。第 4 章，阻斷服務攻擊，特別檢視了 SYN 洪泛攻擊、Smurf、與分散式阻斷服務攻擊。本章也包含了一些分散式阻斷服務攻擊的真實案例，用來展現它們可以造成的損害並且解釋如何避免這些攻擊。第 5 章，惡意軟體，介紹了病毒、特洛依木馬程式、緩衝區溢位攻擊、與間諜軟體。相同地，在檢視完真實案例後也會介紹並展示用來偵測及移除惡意軟體的特定工具，包含 Norton 與 McAfee 等防毒軟體。

到目前為止，本書的讀者已經了解到系統所可能遭受到的各種威脅以及一些用來避免、偵測、與移除這些危險的方法。第 6 章，評估與維護系統安全的基本原理，以及第 7 章，加密，不再探討特定的攻擊和防禦，而是更廣泛的去看待電腦安全管理。在第 6 章中，讀者將學習到一些安全性的基礎：偵測弱點、訂定政策、鑑定顧問資格、維護工作站與伺服器的安全、以及安全地瀏覽網頁。第 7 章介紹加密的相關知識，包含該領域的歷史與現代密碼學的方法。這些章節以較廣泛的角度來看安全管理領域，至少讓學生有足夠的資訊去”問對的問題”並為將來課程中所進行的深入研究做準備。

第 8、9 與 10 章涵蓋了在網際網路上各種不同的犯罪方式。第 8 章，網際網路詐騙與電腦網路犯罪，討論身分盜用與電腦網路監聽；第 9 章說明了電腦網路上的產業間諜活動；而第 10 章檢視了電腦網路恐怖主義與資訊戰。第 11 章，電腦網路偵探，延續前三章節的內容，說明駭客如

何利用網際網路上的資訊來進行犯罪，並且主張瞭解這些方法是防止電腦網路犯罪的關鍵。每一章都會利用真實案例來證明本書第一部分所提到的方法如何被用來危害人們及財產以強調網路安全的重要性。

第 12 章，電腦安全的硬體和軟體，轉向探討更多關於電腦安全的技術、檢視相關的硬體與軟體，其中有一些已經在前面的章節中簡短地提過。本章的用意是讓讀者更詳細地了解病毒掃描器、防火牆、入侵偵測系統、與反間諜軟體。本章包含許多實用的資訊對於未來想朝電腦安全發展的學生來說特別有用。

最後的幾個附錄將提供講師與學生額外的資源，包含有用的網站連結清單、檢查項目範本、字彙、以及撰寫本書時所參考的資料。

教師和學生的資源

教師資源中心

http://vig.prenhall.com/catalog/academic/product/0,1144,0131711296,00.html

教師資源中心是一個只提供給教師的互動式網站內容和連結，本書在該網站上的資源包含：

- 講師手冊。提供教學提示、每個章節的介紹、教學主題、教學建議、以及每章最後的問題與習題的解答。
- 教學投影片。提供在課堂上用來對本書的內容進行逐章複習時使用。
- 測驗資料庫。這是一個相容於 TestGen 的測驗資料庫檔案並且必須搭配 Prentice Hall 出版社的 TestGen 軟體才能使用（可以在 **www.prenhall.com/testgen** 網站上免費下載）。TestGen 是一個測驗產生器，可以讓你很容易地瀏覽與編輯測驗資料庫中的問題、將問題轉成測驗卷、並提供各種格式的列印以符合教學情況。此程式也提供許多選項來組織與顯示測試資料驗與測驗內容。內建的隨機數值和文字產生器可以產生多種測驗版本，包含計分與提供比測試資料庫還多的測驗問題。強大的搜尋與排序功能可以讓你容易地找到問題並且依照你的喜好進行排序。

指南網站

指南網站（**www.prenhall.com/security**）是 Pearson 提供學生和教師的網路資源，在這裡可以找到：

- 互動式學習手冊，網頁上的互動式測驗提供給學生一個方便的機制來自我測試對書本內容的理解程度。
- 額外的網頁專案與資源可以用來實踐每章所提到的概念。
- 認證資訊（來自附錄 A），連結到有用的網站資源（來自附錄 B）以及政策範本與檢查項目（來自附錄 C）。

註：上述網址是專為本書及系列書籍所設的連結，有可能因為書籍停版或該出版社網址異動而變更，敬請知悉，謝謝！

關於作者

Chuck Easttom 在 IT 產業工作多年之後，有三年在技術學院教授電腦科學的經驗，包括電腦安全的課程。離開學術界後回到位於德州達拉斯的公司擔任 IT 經理。在他的工作職責中，包含負責系統的安全。他是其它七本關於程式設計、網頁開發、與 Linux 等書籍的作者。Chuck 擁有超過 20 張不同的產業認證，包含 CIW Security Analyst、MCSE、MCSA、MCDBA、MCAD、Server+等等。他曾擔任電腦科技工業協會（Computer Technology Industry Association, CompTIA）的課程題材專家並參與其中四種認證的發展或改版，包含 Security+ 認證的發起。目前 Chuck 仍然在達拉斯的區域大學擔任兼任老師教授各種課程，包括電腦安全。他偶而也會接下電腦安全諮詢工作。

Chuck 是電腦團體經常邀約討論電腦安全的客座講師。你可以到 Chunk 的個人網站（**www.chuckeasttom.com**）或透過電子郵件 chuckeasttom@yahoo.com 與他取得聯繫。

品質保證團隊

在這裡，我們要深深的感謝品質保證團隊，有他們對於細節上的注意以及努力才能確保本書的正確性。

技術編輯

David Easton
Information Systems
Waubonsee Community College

David Parker
Computer Science
St. Charles Community College

審查委員

Charles R. Esparza
Business Information Technology
Glendale Community College

Charles Hamby
Computer Systems Technology
Matanuska-Susitna College

Suresh C. Sonkavelly
Information Technology
Gibbs College

目錄

CHAPTER 1　電腦網路犯罪與安全介紹

CHAPTER 2　電腦網路與網際網路

CHAPTER 3　評估系統安全性

CHAPTER 4　阻斷服務攻擊

CHAPTER 5　惡意軟體

CHAPTER 6　評估與維護系統安全的基本原理

CHAPTER 7　加密

CHAPTER 8　網際網路詐騙與電腦網路犯罪

CHAPTER 9　電腦網路上的產業間諜活動

CHAPTER 10　電腦網路恐怖主義與資訊戰

CHAPTER 11　電腦網路偵探

CHAPTER 12　電腦安全的硬體和軟體

CHAPTER

1

電腦網路犯罪與安全介紹

本章目的...

在閱讀完本章並完成練習題之後，你將可以：

- 認識電腦網路上主要的威脅：入侵、阻斷服務攻擊（Denial of Service）、與惡意軟體（malware）。
- 評估個人電腦與網路遭受攻擊的可能性。
- 定義重要的名詞，例如怪客（cracker）、思匿客（sneaker）、防火牆（firewall）、與認證（Authentication）。
- 比較周圍式（perimeter）與階層式（layered）網路安全方法。
- 利用網路資源來維護網路安全性。