

序

……所有武士都應學習兵法。但是，將兵法用於邪道，會使武士自傲，蔑視其他武士，作出不滿而錯誤的評價，如此一來，也只會誤導年輕一輩，毒害他們的心靈。此類武士洋洋大論，看似正確和恰當，但是，實際上，他只是想追求效果，只想著自己的利益，所以，結果就是他的人格墮落，失去武士真正的精神。這種錯誤源自於對兵法的膚淺研究，所以，那些開始研究兵法的人，絕不能半途而廢，而猶為自滿，一定要堅持不懈，直到他們瞭解所有奧妙之處，也只有如此，才能回到他們先前的純真，過著寧靜的生活……

大道寺友山
《武士道》【註】

本書提供獨特的方法讓你磨練資訊安全技術（infosec）。適合的讀者是中級到高級的實踐家。但是，我們之中誰才是適合的讀者呢？我們每個人都以獨特的訓練和技巧朝著資訊安全之路邁進。然而，在你把辛苦賺來的錢花在這本書前，我們要試著說明適合的讀者。

●.....
註 引言摘錄自 <http://www.samurai-archives.com>。

舉例來說，如果你對網路有經驗，也會用一兩種語言寫程式，也許你會喜歡這本書。雖然你可能才剛剛開始對資訊安全感興趣而已，但是你至少有幾本此類主題的技術書籍了，像是 O'Reilly 的《Practical UNIX & Internet Security》。你發現這些書籍的資訊性十足，你還想多讀點類似的書，但是，希望談點新主題，有更高等的層次。不只從防禦方的角度對安全做介紹性的探討，你也想從攻擊者的角度看事情。

你已熟悉基本的網路攻擊，諸如嗅探 (sniffing)、欺騙 (spoofing) 以及阻絕服務 (denial-of-service)。你會閱讀線上安全文章以及弱點郵件論壇，而且你也知道這是擴展你的知識的最佳方式。然而，現在，你想要有一本書可以快速讓你的知識再轉幾個齒輪。

你想深入瞭解底層概念，諸如封包分段 (packet fragmentation)、溢位攻擊 (overflow attacks) 以及作業系統特徵探測 (operating system fingerprinting)，而非只是閱讀簡單的軟體工具型錄。你可能想對鑑識 (forensics)、蜜罐 (honeypots) 以及社交工程的心理學基礎 (psychological basis of social engineering) 有些瞭解。你也很喜歡新奇的挑戰，諸如實作 Bayesian 入侵偵測 (intrusion detection)，以及防禦無線「空運」(airborne) 病毒。相信微軟的 Trustworthy Computing (可信賴運算) 計畫前，你想深入瞭解 Windows XP 攻擊以及 Windows Server 的弱點。

這些是我們所論及的一些主題。雖然對更高階讀者而言，有些部分一定只算複習，但是我們也有一些特別的主題，可能會讓資深的高手感到滿意。例如，我們談到軟體逆向工程 (reverse code engineering，簡稱 RCE)，包括不好懂的 Linux RCE 和嵌入式 RCE 這些主題。對於解析惡意程式、揭露公司間諜軟體以及找出應用程式弱點而言，RCE 是不可或缺的，但是本書出版前，都只散見於一些文獻中。

本書並非針對特定作業系統，因為很多人都要負責保護混合型網路。我們決定從攻擊方的角度談安全，而非從防禦方。建立有效防禦的良好方式就是瞭解以及預測潛在的攻擊。

整本書中，我們試著不要表達太多自己的想法。然而某種程度也必須這麼做，否則與一本無聊的實況型錄有何不同。希望你原諒我們在報導過程中插入自己的意見，但是我們也不會說我們的意見是權威意見，甚至連是否正確也不能拍胸脯保證。人類的意見很分歧，本質上都有缺陷。至少，我們希望在爭議性十足的主題上能提供和你的觀點對立的看法。我們還提供了許多有趣的範例，讓一些沉重的主題有點朝氣。

我們特別在每章結尾處提供有用的參考資料。這些參考資料是一些經典資訊安全的資料來源，可讓你進一步探索你最感興趣的領域。但是這本書絕非網路安全的全方位介紹。相反的，這是一本指南，讓你在幾個關鍵領域內可以快速提升技能。我們希望你在閱讀時也能獲得我們在撰寫時的樂趣。

本書架構

你不用循序漸進閱讀這本書。多數章次都可獨立閱讀。然而，很多讀者寧願把技術書籍拿起來，然後逐章閱讀。因此，我們試著以有用的結構來組織這本書。下面幾個部分勾勒出了本書的主要結構，並且我們會對每章的重點做些提示。

第一部分：破解軟體

本書第一部分的主要焦點是軟體逆向工程 (software reverse engineering，也稱為 reverse code engineering 或簡稱 RCE)。屆時你會瞭解到，RCE 在網路安全中扮演重要的角色。然而，直到本書出版前，RCE 只散見於一些資訊安全的文獻。第一部分在簡介過組合語言 (第 1 章) 之後，會開始談論 Windows 平台的 RCE 工具和技術 (第 2 章)，其中包括了一些相當特別的破解練習。接著會討論 Linux RCE 這個比較神秘的領域 (第 3 章)。然後會介紹嵌入式平台的 RCE (第 4 章)，明確的講，就是破解使用 ARM 型處理器的 Windows Mobile 平台 (Windows CE、Pocket PC、Smartphone) 的應用程式。最後會探討溢位攻擊 (第 5 章)，而且會根據前幾章所學得的 RCE 知識，以實際之緩衝區溢位進行 exploits (也就是，利用安全漏洞或弱點進行攻擊)。

第二部分：網路追蹤

第二部分所奠定的基礎可讓你瞭解本書後面將介紹之網路攻擊技術。第 6 章中會探討 TCP/IP 的各種安全面向，包括 IPv6，而且也會談到分段攻擊 (fragmentation attack) 的工具和技術。第 7 章將以獨特的方法說明社交工程，使用心理學理論來探索可能的攻擊。第 8 章將談網路勘察，而第 9 章會討論 OS 辨識技術，包括被動辨識技術，以及全新的工具，像是 XProbe 和 Ring。第 10 章會進一步討論駭客如何隱藏其行蹤，包括反鑑識 (anti-forensics) 和 IDS 躲避 (evasion)。

第三部分：平台攻擊

第三部分在探討 Unix 攻擊 (第 12 章) 前，會先複習 Unix 安全基礎 (第 11 章)。接著有兩章和 Windows 安全有關，包括用戶端 (第 13 章) 和伺服器 (第 14 章) 攻擊，因為這兩種平台上的 exploits 有其特質。例如，在 Windows XP 上頭，我們會說明如何攻擊遠端協助 (Remote Assistance) 裡的弱點，然後在 Windows Server 上頭，我們會說明破解 Kerberos 認證機制的理論方式。第 15 章將談論 SOAP XML Web Service 的安全，而第 16 章會檢視 SQL 注入攻擊。最後，我們會談論無線安全 (第 17 章)，包括無線區域網路和嵌入式行動惡意軟體，像是「空運病毒」(airborne viruses)。

第四部分：高階防禦

第四部分將談論高階的網路防禦方法。例如，第 18 章會談論日誌分析，內容包括日誌的聚集和分析。第 19 章將以全新的實務手法把 Bayes 理論用於網路 IDS 之設置。第 20 章會提供逐步藍圖，讓你得以建立自己的蜜罐（honeypot）以誘捕攻擊者。第 21 章將介紹意外事件之應變的基礎，而第 22 章會探討（Unix 和 Windows 的）鑑識工具以及技巧。

第五部分：附錄

最後，本書尾端的附錄將列出有用的 SoftICE 命令和斷點。

本書印刷體裁

本書將使用下列印刷體裁：

純文字

選單標題、選單選項、選單按鈕以及鍵盤輔助鍵（諸如 Alt 和 Ctrl）。

斜體字

URL、郵件信箱、檔名、副檔名、路徑名稱、目錄以及 Unix 工具。

定寬字

命令、選項、開關、變數、屬性、關鍵字、函式、型態、類別、名稱空間、方法、模組、內容屬性、參數、值、物件、事件、事件處理常式、XML 標籤、HTML 標籤、巨集、檔案內容或者命令的輸出。

定寬粗體字

應該由使用者鍵入的命令或其他文字。

定寬斜體字

應該由使用者提供值以替換的文字。



此圖示表示技巧、建言或一般附註。



此圖示表示警訊或小心之語。

程式範例

這本書的目的是協助你把工作做好。一般而言，你可以在你的程式和說明文件中使用本書的程式碼。除非你要重製重要的程式碼，否則無須取得我們的許可。例如，使用本書片片斷斷的程式碼寫了一個程式，並不需要取得我們的許可。但是，把 O'Reilly 書籍的程式範例燒成光碟片販賣或散佈，就需要取得授權。引用本書的文句和範例程式碼來回答問題，不需要取得許可。

建議和問題

歐萊禮公司是世界性的電腦資訊出版公司。我們永遠樂意聽到讀者對出版品的意見，包括如何讓本書可以更好的建議、指正本書的錯誤、或是讀者建議本書往後改版時，應該再加進來的其它主題。以下是本公司的聯絡資料：

美商歐萊禮股份有限公司台灣分公司

電話：(02) 2709-9669 傳真：(02) 2703-8802

網頁：<http://www.oreilly.com.tw>

電子郵件：mail@oreilly.com.tw

與本書有關的線上資訊（可能包括勘誤、範例程式、相關連結）：

原文書

<http://www.oreillynet.com/catalog/swarrior/>

中文書

http://www.oreilly.com.tw/product2_security.php?id=a215

誌謝

繼續下去前，我們想感謝許多專家對我們建言、批評以及鼓勵。我們要特別感謝兩位有所貢獻的寫作者：Seth Fogie 和 Mammon。沒有他們的貢獻，這本書會縮水很多。Colleen Gorman 和 Patricia Peikari 做了其他的校對。技術審查者有（沒有按特定次序排列）Jason Garman、John Viega、Chris Gerg、Bill Gallmeister、Bob Byrnes 以及 Fyodor（Nmap 的作者）。

--Cyrus Peikari

--Anton Chuvakin