序

《防駭超級工具》一書由 Juniper Networks 的 J-Security Team 的諸位成員與兩位專家貴賓撰寫而成：史丹佛大學的 Jennifer Granick 教授與遠在法國的獨立開發者 Philippe Biondе 。這本書耗費了整個團隊相當的心力，因為網路安全的議題讓我們在各自的工作崗位上非常忙碌，而且，這本書的討論範疇相當寬廣，需要不同領域的安全防護專家齊力貢獻各自的經驗。經過幾次調查性的會議之後，我們將這些工具分組，然後花了 6 個月的時間撰寫、修訂、改寫、再修定。寫書不是我們的主要專長，如果讀者諸公碰到了一些表達不周之處，在此深表抱歉。編輯大人們告訴我們，他們白了不少頭髮試著在一整組人的不同筆調中建立出統一的表達風格，直到最後不得不放棄。我們決定不再隱藏這本書是由 12 個人撰寫而成的事實，是的，就承認吧。

為了體會這是怎麼樣的狀況，想像一下，自己正與 12 位安全防護專家共處一室，某人問了一個問題，比如說無線網路滲透（wireless penetration），正躲在筆記型電腦後面做其他事情的 8 個人全都抬起頭來提供個人的意見，其他 4 個人則轉了轉他們的眼球，等了一下，看了看他們的電腦，接著突然插入他們的意見。在這整本書裡，每一章都描述了一些稍有不同的答案，來自這 12 種聲音當中的 1 種；因此，每一章的處理風格和手法可能都有點兒不同，取決於誰在說明，以及誰的電腦是關機的，然而，所有資訊都是在聚光燈下檢視過的 — 所有的章節都經歷了團隊共同的審閱。

其他幾個我們再三斟酌的項目是作業系統的涵蓋範圍、讀者的專業知識、和工具的選擇。

本書涵蓋多種作業系統：Windows、Linux、Mac OS、Unix 等等，取決於所論述的安全防護工具為何。我們一度為了章節的安排與工具的分類爭論不休，但該議題只在我們的作者會議中持續了大約 8 分鐘。

有關讀者專業知識的部份就比較麻煩一點。我們對於讀者需要具備什麼條件的主要假設將在本序中的下面二節詳述。大體上，我們設想這本書是針對中高階的網路安全管理者，但是，在作者會議的討論中，我們也注意到這實在是取決於不同工具，有些網路安全工具簡單直覺，有些則困難異常；這也是取決於該工具是否在黑帽（壞）或白帽（好）駭客的區分上具有明確的目的。因此，如果你開始研究某一項工具，發現它對你來說太過簡單，或者太過進階，建議你稍微避開一下，先探索那些適合你的程度的工具，隨著你逐漸深入，再做適當的調整。

最後一個頗令我們掙扎的地方是要收錄的工具。O'Reilly 的編輯給我們一個理想的篇幅目標，這是我們必須遵循的第一項規則，否則這本書的售價將高達 100 美元。其次，我們當中的每個人都按照章節主題審閱過不同的工具，所依據的標準是：該工具是否能夠在多種 OS 上使用、是否具有廣大的使用族群（可適用更多的讀者）、有沒有良好的商業或社群支援（以便讀者在本書之外可以找到更多的參考材料）、以及有沒有什麼內涵可供討論（坦白說，有些工具把一項工作做得非常好並且相當單純，以致於幾乎是不言而喻且容易使用的）。最後，收錄在本書中的工具自有它們被挑出的理由，然而，不是所有最初被挑選的工具都被收錄在本書中；終究，我們必須做抉擇。對那些被剔除掉的工具，我們深感抱歉；對那些被納入的工具，我們也要為我們的嚴厲批評與吹毛求疵表達歉意，當然，這只是我們的觀點。作為讀者，所謂「盡信書不如無書」，請對我們的說法帶一點保留，自己動手試試這些工具 — 它可能就是你想要或需要的東西。

整體團隊要謝謝 Juniper Networks 公司，給我們時間完成本書的撰寫，並且提供其他資源，幫助我們寫得更快且更好。這本書的合約關係人是 O'Reilly 與 12 位作者，不包括 Juniper Networks，我們所說的任何事情與 Juniper Networks 無關，這裡的資訊純粹是我們個人的意見，而不是 Juniper Networks 或者我們部門的正式觀點。這本書收集了許多不同的觀點，討論安全防護工具如何運作以及怎樣運用。

最後，整個團隊要感謝 Avishai (Avi) Avivi，他是我們當中 10 位 Juniper 員工的部門經理（及本書前言的作者）。很多次在我們的作者會議之後，他都會嘀咕著說，「別再有下次，別再有下次」，然而，我們注意到，當本書封面的草稿第一次從 O'Reilly 送過來時，他把它印出來，並且貼在他的辦公室。

致讀者

雖然，這本書或許可以說適合任何對網路安全工具有興趣的人閱讀，但這不是對初學者說的。更確切的說法應該是：儘管初學者能夠閱讀這本書，但大部分題材都需要你花更多時間，坐在電腦螢幕前，好好研究一番網路安全的相關事宜。

大體上，這本書是為具有中高階基礎的網路安全管理者、工程師、及顧問而撰寫的。取決於你的專業知識，這本書可能對你或多或少都有些新鮮材料，或者你所沒有試驗或經歷過的新工具。你的網路安全責任可能是小的、中的、或者大的，我們已經試著為你適度地增減我們的工具實驗。

我們的編輯，這個領域的初學者，告訴我們這本書很棒，他們從不知道網路有多脆弱。從這個立場來看，這本書蠻適合丟到 COO 的桌上，以便爭取到一些新設備的經費。另外，第 1 章，探討網路安全的倫理與法律，對任何從事安全防護事業的人而言，會有相當大的助益。

因此，我們建議下列的行動方針。瀏覽一下本書的 7 大部分，再深入你覺得適合起步的安全工具。接著，開始四處跳著閱讀，善用指向其他章節和工具的交叉參考。少數人（如果有的話）會從第一頁循序閱讀到最後。進進出出某些章節，然後試試新工具 — 在你的電腦上玩一玩，然後再試試另一項工具。我們認為這是最好的做法，不要光是閱讀，而不將它應用到你的專業技能上。

本書所做的假設

我們假設讀者至少都熟悉 TCP/IP 網路和網際網路的基礎。你應該知道 IP 位址是什麼，以及 TCP 埠口號碼是什麼，而且你應該對 TCP 旗標（TCP flag）等類似題材至少具有粗略的理解。雖然我們為多種作業系統探討安全防護工具，多數工具都是透過 Unix 命令列來使用的，因此，能夠存取 Unix 機器，並且知道怎樣使用 shell（命令殼）也是必要的（假如你想要跟著做的話）。幾個更進階的章節處理有關編程的工具，因此，至少知道一種程式語言將會有所幫助（但是，如果你不是程式人員，也別擔心，許多章節根本不需要任何編程知識）。最後，電腦安全防護的基礎知識也是必需具備的。假如你真的想從本書獲得最大利益，也必須熟悉安全漏洞（vulnerability）、弱點攻擊（exploit）、服務阻絕（DoS，denial of service）之類的術語。

本書內容

《防駭超級工具》共分成 7 個部分：法律與倫理、偵察、滲透、控制、防禦、監控、與發掘。有些部分具有多個章次，有些則只有一、二章。利用這樣的分類作為一般性的參考，可幫助你更容易閱覽本書。

本書共分成 23 章。有些章次由個人撰寫，有些則由 2 或 3 個作者一起完成。我們為每一章選出一位主導的作者，簡要地提供一個介紹性的概述。

法律與倫理

第 1 章，〈法律與倫理議題〉，由 Jennifer Stisa Granick 執筆。完成本章的閱讀之後，如果具備了辨別何時要找律師談的能力，那麼我便已經達成撰寫它的目標。本章認為法律規則與條例不同於（但部分重疊於）倫理與道德的考量，然後以安全測試、安全漏洞報告、與逆向工程為例，同時探討法律與倫理兩個面向，讓你測試自己對法律模糊地帶的辨識能力。

偵察

第 2 章，〈網路掃描〉，由 Bryan Burns 撰寫。本章為網路掃描的概念提供簡單的介紹，並且詳述 3 個網路掃描程式的運作，包括可敬可佩的 *nmap*。閱讀本章之後，你將知道怎樣尋找網路上的電腦，識別出哪些服務正在遠端電腦上運作，甚至識別出服務和作業系統（執行在世界另一頭）的版本，正所謂「知此知彼百戰不殆」。本章全然關乎知道網路上有些什麼東西。

第 3 章，〈安全漏洞掃描〉，由 Julien Sobrier 撰寫。本章探討用來尋找安全漏洞的 Windows 和 Linux 工具，焦點在於從這些工具實際所得的資訊進行結果分析。本章應該能夠讓你為你的測試選擇最好的工具，並且加以調整，以便取得最好的結果，瞭解報告的意義。另外，我們也會說明這些工具常見的錯誤使用。

第 4 章，〈區域網路偵察〉，由 Eric Markham 撰寫。90 年代晚期，我服務於一家叫作 "Mom and Pop" 的 ISP 公司，接著轉換到幾家新興公司，擔任 IT 部門的經理。我選擇撰寫這一章的理由，是因為這與我的工作經驗直接相關。我採取稍微比較切合實際的方式來談論網路安全防護，並且預期你對 TCP/IP 網路、*nix 和其他作業系統之間的主要差別、以及天為什麼是藍的，具有一定程度的瞭解。

第 5 章，〈無線網路偵察〉，由 Michael Lynn 撰寫。本章從 802.11 協定的基本描述談起，接著討論各種有助於無線網路偵察的開源碼和商業工具。在無線網路的世界裡，你擁有的硬體和使用的作業系統會對你選擇部署什麼工具產生很大的影響，因此，我試著為你清楚地分析你的選項有哪些，我也試著將每一項工具的優缺點交代清楚，好讓你找到最合適的工具。在閱讀過程中，我希望能夠告訴你一些很酷的功能，而你原本可能不知道那會讓 wardriving【譯註】更容易且更成功。本章不假設你具有任何 802.11 網路的基礎知識。

第 6 章，〈自訂封包的產生〉，由 Philippe Biondi 撰寫。本章解釋：當論及發現網路、評估設備強健性、與私有協定互動、以及攻擊安全缺陷時，在現成工具與量身訂製

譯註　wardriving：掃台，參見*http://en.wikipedia.org/wiki/Wardriving*。

工具之間的差別。另外，本章也包含封包產生（或封包修改）的簡要探討，因為許多問題可藉由 on-the-fly packet（動態封包）與 stream mangling（串流修改）快速獲得解答（倘若你知道正確的工具）。因為英語是我的第二語言，我要謝謝 David Coffey 幫我重新撰稿及修辭。

滲透

第 7 章，〈Metasploit〉，由 Bryan Burns 撰寫。Metasploit 是進行跨網路遠端電腦自動化滲透極強大和受歡迎的框架和工具組。在本章，你將學習怎樣組態及使用 Metasploit，攻擊最新的軟體安全漏洞，並且控制其他電腦。因為近年來網路監控工具越來越常被部署，我們將致力於探索 Metasploit 中被用來悄悄瞞過這類設備的功能。

第 8 章，〈無線網路滲透〉，由 Bryan Burns、Steve Manzuik、與 Michael Lynn 撰寫。在第 5 章中，你學到尋找無線網路並收集其相關資訊的工具。在本章，我們提出 3 項工具，引導你進入下一個層次：無線網路滲透。Aircrack 是捕捉無線網路交通並進行離線分析的工具組，並且能夠達成破解無線網路密鑰的目標。Airpwn 讓你把自己的資料注入（inject）別人的無線網路交通，並且考慮各種細微的情況。最後，Karma 會假扮成一個合法的存取點（access point），對任何不幸能夠連上來的客戶取得完整的能見度與控制權。藉由這 3 項工具，你就能夠掌握到一些無線網路（甚至是經由 WEP 加密的無線網路）的控制權。

第 9 章，〈攻擊框架應用程式〉，由 Nicolas Beauchesne 撰寫。Metasploit 出現之後，攻擊框架變得大受歡迎。不過，這個領域中也有一些商業玩家，諸如 Core Security（Core Impact 的製造商）和 Immunity Security（Canvas 的製造商）。這些框架兼顧彈性與威力，本章說明它們的基本用法、一些進階功能、以及如何客製化以便滿足你的需求。

第 10 章，〈自訂攻擊〉，由 Philippe Biondi 撰寫。本章是一組我用來操作 Shell 指令稿及建立攻擊的技巧和工具，幫助你分析現有指令稿，以及建立和測試你自己的指令稿。因為英語是我的第二語言，我要謝謝 David Coffey 幫我重新撰稿及修辭。

控制

第 11 章，〈後門程式〉，由 Chris Iezzoni 撰寫。本章闡述一些最受歡迎、容易獲得、可作為後門程式之工具的用法和組態。VNC 是一項常見的遠端管理工具，在 Windows 和 Unix 上都可運作。在此，我說明一些方法，可輕易地將它安裝作為後門程式使用。BO2k 是運作在 Windows 上、特定用途的後門程式，本章會說明一些可供利用的較進階模組。最後但肯定不是最次要的，一些為 Unix 系統設置後門的受歡迎方法也會被涵蓋到。更進階的 Unix 後門程式未在此說明，這是因為它們具有版本特定的本質使然。

第 12 章，〈Rootkit〉，由 Nicolas Beauchesne 撰寫。本章是一篇快速導覽，說明 Windows 和 Linux 上一些已知的 rootkit，以及它們的用法和限制。相較於深入其內部運作的機制，探索這些 rootkit 的用法和偵測對讀者會比較切中要的。為了解釋每一項技術的好處，我會在偵測範例中探討它們之間的一些差異。在諸多偵測工具中，我會納入一些系統內部工具，以及 IceSword 之類的工具。結合這些工具的威力，應該能夠幫助你對付大多數的感染案例。

防禦

第 13 章，〈免疫防禦：防火牆〉，由 Dave Killion 撰寫。本章涵蓋一些基於主機的防火牆，都是免費可取得的，並且能夠運作在 3 個常見的作業系統上：Windows 上的 Windows Firewall/Internet Connection Sharing、Linux 上的 Netfilter/IPTables、以及 *BSD 上的 ipfw/natd。取決於主機怎樣被使用，這些指示也涵蓋了使用這些系統作為閘道防火牆的機制（以路由器或 NAT 模式）。還有許多防火牆的產品存在 — 當中有一些是非常好的 — 很多書籍都在討論它們。由於只有一章的篇幅可以處理這個主題，我會盡我所能地涵蓋防火牆策略、功能性、和組態的基礎知識。閱讀本章之後，你應該會對防火牆的功能性具有很好的理解，並且能夠應用到任何防火牆產品上，另外，對於在你所選擇的 OS 上進行防火牆管理方面，也會讓你有實際動手做的體驗。

第 14 章，〈主機強化〉，由 Eric Markham 與 Eric Moret 撰寫。在你學會怎樣藉由第 13 章的防火牆，透過存取控制保護你的網路之後，本章將介紹一些保護 Windows 或 Linux 電腦的工具。你將循著合乎邏輯的步驟，開始選擇要關閉什麼，以最小使用者權限執行日常工作，並且為安全防護考量將一些 Linux 核心鎖住。在本章中，SELinux 和它不可或缺的支援工具會被引進，接著，審查密碼強度的各種方法會被提出，從令人肅然起敬的 John The Ripper 到最新的 rainbow cracking 技術。最後，我們會以較進階和寬廣的虛擬化（virtualization）主題作為本章的結束。

第 15 章，〈通訊安全〉，由 Julien Sobrier 與 Eric Moret 撰寫。緊接著周邊設備和主機強化的下一個合理步驟是通訊安全。本章將帶領你走過 SSH 的使用，雖然這項工具源自於 *nix 的世界，但在 Windows 上也有很好的支援。然後，我們會介紹電子郵件加密，並且解釋兩個相互競爭的標準：OpenPGP 和 S/MIME。接著，不管它的實作如何，stunnel 被用來防護任何伺服器常駐程式的網路交通。最後但不是最次要的，我們要對抗透過竊取硬體而取得身分資料的竊案，並且提出加密整個磁碟或分割區的解決辦法。

第 16 章，〈電子郵件安全與反垃圾郵件〉，由 Julien Sobrier 撰寫，本章將幫助你保護自己的電腦，免於最常見的威脅：病毒、蠕蟲、惡意軟體，垃圾郵件、和網路釣魚（phishing）。本章可能是涵蓋技術層面最廣的一章，從初學者等級（調整你的 Windows 防毒機制）到進階等級（建立你自己的病毒特徵（virus signature）或

procmail 規則〉。正規表達式和 Shell 指令稿的知識將幫助你為本章所提供的範例進行客製化，然而，大多數的內容都是初學者能夠理解的。

第 17 章，〈設備安全測試〉，由 Julien Sobrier 撰寫。本章所提出的工具涵蓋安全測試的不同領域。貫穿全章，我們提出許多關於怎樣讓測試自動化的例子。在所有的 QA 流程裡，這些工具都是很好用的 — 不只對安全防護設備，對任何網路設備也是。

監控

第 18 章，〈網路捕捉〉，由 Dave Killion 撰寫。能夠監控、捕捉、以及分析封包會有很大的用處，既可檢修網路的效能，偵錯有問題的網路程式，也可以捕捉攻擊，供稍後進行分析或者作為告發的證據。我會帶領你試著從命令列和圖形化介面 (GUI) 使用各種跨平台的捕捉工具，包括 tcpdump 和 Wireshark，並且說明一些管理 *pcap* 檔案的技巧，以便將它們精煉成正好符合你所需的內容。當你完成本章的閱讀時，會發覺你自己正在想「我想知道那支程式在網路上看起來像什麼樣子？」，而且，你會擁有工具和知識去弄清楚。

第 19 章，〈網路監控〉，由 Nicolas Beauchesne 撰寫。本章包含 Honeyd 和 Snort 之類的工具。因為許多書籍已經介紹了這些工具，這裡所採取的做法是讓讀者快速熟悉一下它們的一般性使用，然後說明一些方法，將這些技術做進一步的運用，因為它們相當具有彈性，並且能夠用來執行許多任務。此外，本章也涵蓋了整合這些工具的做法，以便獲取網路情報（network intelligence），而不只是監控資訊。

第 20 章，〈主機監控〉，由 Eric Moret 撰寫。本章為系統管理員介紹一種實務做法，監控上線伺服器中的檔案變更，一開始說明一大組工具，接著，深入 Tripwire（我的最愛）及 Samhain 的安裝和組態。接下來，我會說明如何為 Linux 的紀錄報告使用 Logwatch，隨後附帶了撰寫新紀錄過濾器的按步驟操作指南。我會以 Prelude-IDS 作為本章的結束，這項工具被用來為大量以網路連接的設備，進行集中化的安全防護。

發掘

第 21 章，〈電腦鑑識〉，由 Chris Iezzoni 撰寫。本章涵蓋一些廣受歡迎的鑑識工具，可用於諸如攻擊和事件調查，以及發現惡意軟體的任務。我試著盡量使用免費工具，諸如 The Forensic Toolkit 與 SysInternals，僅藉由這些工具，你就可以發掘出關於系統內部運作的大量資訊。這將給你一個良好的基礎，藉以自行探索更複雜的工具，像是 The Coroner's Toolkit (TCT)。

第 22 章，〈應用程式模糊測試〉，由 Nicolas Beauchesne 撰寫。本章包含各種模糊測試工具（fuzzer）與模糊測試（fuzzing）技術，以及怎樣建立新的模糊測試工具指令稿。我會提供一些小訣竅，說明如何設置模糊測試平台（test-bed），以及如何執行有效

率的追蹤與偵錯，以便提升模糊測試工具的測試效率。此外，我也會針對模糊測試的目的，提供一種快速的網路協定反向解析，因此，在執行這些任務時，讀者將會知道要尋找的重點是什麼。

第 23 章，〈二進制逆向工程〉，由 Michael Lynn 撰寫。本章說明二進制逆向工程的藝術，使用諸如 Interactive Disassembler 和 Ollydbg 的工具。我會讓你看一個案例研究，在當中，我會告訴你如何在一個關閉原始碼的軟體中，找出真正的臭蟲。在此案例研究的進行期間，我會讓你看到怎樣使用廣受歡迎的反組譯器（disassembler）與偵錯器（debugger），甚至教你如何撰寫基本的指令稿，加強這些威力強大的工具。在本章結束時，你應該能夠使用這些工具，在缺乏原始碼的情況下找出臭蟲，並且能夠對此類型之逆向工程的實際運作獲得良好的理解。雖然具有逆向工程與組合語言的基礎知識會有所幫助，但並非必要。你應該具備基本的編程技能，才能夠從本章獲得最大的利益。

本書印刷體裁

本書使用下列印刷體裁：

純文字

指選單標題、選單選項、選單按鈕、以及鍵盤輔助鍵（諸如 Alt 和 Ctrl）。

斜體字

指新術語、URL、電子郵件、檔案名稱、副檔名、路徑名稱、指令元、以及 Unix 工具。

定寬字

指命令、選項、變數、屬性、鍵、函式、型別、類別、名稱空間、方法、模組、特性、參數、值、物件、事件、事件處理器、XML 標籤、HTML 標籤、巨集、檔案內容、程式、或命令之輸出。

粗體定寬字

表示應該由使用者逐字輸入的命令或其他文字，也用於程式碼中被強調的部分。

斜體定寬字

表示應該由使用者提供的替換文字。

此圖示指的是技巧、建言、或通則。

此圖示指的是警訊或警誡。

使用程式碼範例

這本書是為了協助你把工作做好。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，否則無需取得我們的許可。例如，使用本書的程式碼片段撰寫程式，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售或散佈，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。把本書大量的程式範例整合到你的產品的說明文件中，則需要取得授權。

雖然並非必要，但註明引用來源，我們會很感謝。註明來源通常包括書名、作者、出版商、以及 ISBN。例如，「*Security Power Tools*, by Bryan Burns et al. Copyright 2007 O'Reilly Media, Inc., 978-0-596-00963-2.」

如果覺得你對書中程式碼範例的使用有別於上述情況，不用客氣，盡量和我們連絡：*permissions@oreilly.com*。

連絡我們

在本書專屬的網頁中，我們列出勘誤表、範例、及其他額外資訊。網頁如下：

http://www.oreilly.com/catalog/9780596009632/

關於本書的意見，或者想詢問技術性問題，請寄送電子郵件到：

bookquestions@oreilly.com

有關其他書籍、研討會、資源中心、以及 O'Reilly Network 的資訊，可參考我們的網站：

http://www.oreilly.com

致謝

我們要感謝 Patrick Ames，Juniper Networks Books 的總編輯，協助我們度過長達 9 個月的撰寫流程，並且給予我們撰寫與出版本書的建議和指導。還要感謝許多 Juniper Networks 的人員幫忙審閱本書，或者以各種方式協助我們。另外，我們也想對 Juniper Networks 的管理階層表達謝意，感謝他們的支持，並且允許我們使用公司的資源研究及撰寫本書。