網路安全面面觀

/台灣思科系統提供

隨著業界逐漸將目光焦點投注於網際網路，網路安全已成為全球企業關心的重要議題，也因此，網管人員須花費更多的精力去維護網路安全，而非將時間應用在實際的網路設定與管理工作上。目前各種用來偵測系統弱點的工具，例如分析網路用的安全管理員工具(SATAN)，以及新問市的掃瞄檢測入侵封包與程式的工具，皆能協助網管人員進行保護工作，但這些工具僅能找出潛藏弱點的區域，卻無法提供一套有效的機制來阻擋所有可能的網路攻擊。因此，網管人員必須持續掌握現今世界中的大量安全知識。本文章將介紹許多有關將私人網路串連至網際網路而衍生的安全議題。

保護網路安全：維持內部網路系統完整性

當連上網際網路時，您的電腦就開始與超過 5 萬個未知網路以及其使用者進行連線。雖然這種連線會開啟許多管道，讓您連結多項有用應用系統並享受資訊分享的機會，但大多數私有網路的資料皆不宜讓外部使用者隨意取得，更何況，並非所有網際網路使用者的行為都會遵循法律的規範。

資訊通常以兩種狀態存在於網路中，分別為實體媒體，例如像硬碟、記憶體，或是以封包的型態在實體網路線路中傳輸。而這兩種資訊狀態卻顯示出內部網路以及網際網路上的使用者有許多機會能發動攻擊。在規劃網路防護時，應注意如何維護實體網路的完整性、網路軟體以及其它網路資源。網路的完整性包括電腦與使用者的身份、網路提供的服務運作能力、以及最佳化的網路效能，這些都是維繫最佳網路環境的重要因素。

網路封包監聽器〔Network Packet Sniffers〕

由於網路連線的電腦採用序列通訊模式(資訊單位依序傳送)，因此大容量的資訊會因電腦的緩衝區容量有限，而被切割成許多較小的傳輸單位。即使網路採取平行傳輸模式，資訊流亦會被分割成較小的單位，其稱為網路封包。許多網路應用系統會以未編碼(*clear text*) 的模式散佈網路封包 – 也就是資訊在網路上傳輸時並未加密。

因為網路封包未經加密，因此任何應用程式都能從網路上將這些封包進行處理與解譯，導致第三者可輕易截取網路封包並開發封包監聽程式。

而網路駭客則可利用網路封包監聽器取得正確帳戶資訊使用您的網路，並修改對系統極重要的檔案，例如系統管理員帳號密碼、檔案伺服器上服務與權限清單、其它含有機密資訊的電腦在登入時詳細資料。此外，網路封包監聽程式能加以修改，將新資訊存入原有的封包或是變更封包內的現有資訊。透過這些動作，駭客能讓網路連線永遠中斷亦能變更封包中的重要資訊。

IP 位址欺偽(IP Spoofing)

IP 位址欺偽攻擊是指網路外部駭客〔attacker〕假冒成一部安全的電腦，以存取您網路中特定資源。一般而言，IP 位址欺偽攻擊的行為僅限於將資料或指令嵌入至現有資料流中，這些資料會在客戶端與伺服器應用程式或對等式網路連線中進行傳輸。為支援雙向通訊，駭客必須變更所有的路由表〔routing table〕，讓封包位址指向欺偽的 IP 位址。若駭客成功變更路由表而將封包指向欺偽的 IP 位址，他就會接收到所有指向該偽造位址的網路封包，並能和任何受信任的使用者一樣進行回覆動作。

IP 位址欺偽除了讓駭客取得使用者帳號與密碼，亦能應用在其它類型的攻擊。例如，其可假冒內部使用者的身份，傳送電子郵件訊息至其它商業夥伴，讓該訊息看似是由您組織中某人所發出，而對企業組織造成不利影響。

密碼攻擊

密碼攻擊可使用許多不同方式，其中包括暴力型攻擊、木馬程式、IP 位址欺偽、以及封包監聽程式。雖然封包監聽程式與 IP 位址欺偽都能取得使用者帳戶與密碼，但密碼攻擊通常是指重複嘗試辨識一組使用者帳戶與/或密碼，也稱之為暴力型攻擊。

如同封包監聽程式與 IP 位址欺偽攻擊一樣，暴力型密碼攻擊亦能取得合用帳號，用來修改重要網路檔案與服務。例如修改網路的路由表，破壞網路完整性。透過這種行為，駭客可確保所有網路封包都轉送至自己所在節點，之後再將封包傳送至最終目的地。

拒絕服務攻擊

拒絕服務攻擊與其它攻擊行為大不相同，因為它的目標不是存取您的網路或網路中的資訊。這類攻擊目標是讓服務無法正常供應，通常是透過將網路、作業系統、或應用程式的資源耗盡，直到超過上限值為止。

當涉及特定的網路伺服器應用時，例如 HTTP 伺服器或檔案傳輸通訊協定(FTP)伺服器時，這類攻擊主要在取得連線控制權，並讓所有伺服器可用的連線保持開啟狀態，使其它欲存取伺服器或服務的使用者無法連線。拒絕服務攻擊可使用各種通用的網際網路通訊協定，例如 TCP 以及網際網路控制訊息通訊協定(ICMP)。大多數的拒絕服務攻擊會針對整體架構中的弱點，而非鎖定軟體 bug 或安全漏洞進行攻擊。然而，部份攻擊會發出極大量的無用封包，並提供有關網路資源的假冒資訊，以降低您網路的效能。

應用層攻擊

應用層攻擊可運用許多不同方式，其中最常見的是利用伺服器中軟體的常見弱點進行攻擊，例如 sendmail、PostScript、以及 FTP。網路駭客可透過這些弱點取得該應用系統的帳號權限來存取電腦。

木馬攻擊是指駭客假冒一般程式的偽造軟體進行攻擊。這些程式具備所有正常程式或服務所提供的一切功能，以及僅有駭客知道的其它功能，例如監視登入動作以擷取使用者帳號與密碼。應用層攻擊最早出現的模式是使用木馬程式顯示一組螢幕畫面、橫幅、或提示字串，讓使用者誤信它是一個合法的登入程序。之後程式會擷取使用者鍵入的資訊或將資訊傳回給駭客。隨後，木馬程式再將資訊轉送至正常的登入程序或直接發出錯誤訊息、離開系統、或是啟動正常的登入程序。使用者會誤以為自己輸入錯誤的密碼，並重新輸入登入資訊以便進入系統。

最新的應用層攻擊方式是運用許多新技術本身的開放特性，如：超本文標記語言(HTML)規格、Web 瀏覽器功能、以及 HTTP 協定等。這些攻擊行為包括使用 Java applets 以及 ActiveX 控制項，以便在網路上傳送有害的程式，並透過使用者的瀏覽器讓這些程式能被載入至系統。

建立安全周圍網路

當您在擬定網路安全策略時，必須規劃相關的作業程序來保護網路，避免其中的內容與使用者遭受損失或損壞。從這個角度來看，網路安全策略扮演的角色就是推動組織整體安全策略執行者。

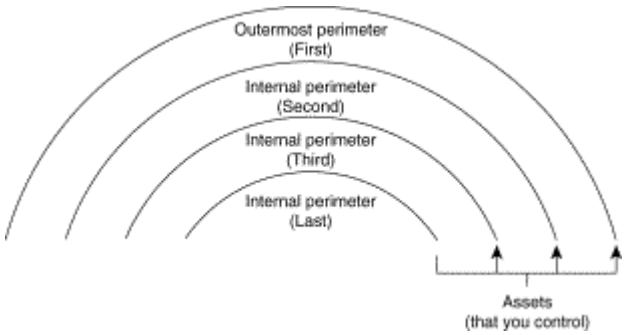
網路防火牆是整體安全解決方案的重要部份，它負責根據安全策略監視跨越各周圍網路的資料流。周圍路由器配置在網路邊界，例如像私有網路、內部網路、外部網路、或是網際網路之間。防火牆大都負責區隔內部(私有)與外部(公共)網路。網路安全策略主要應用在控制網路流量與使用權

限。其定義網路的各種資源與威脅狀況、規範網路的使用與責任、以及當違反安全策略時的細部作業計畫。

周圍網路(Perimeter Networks)

當您在建立周圍網路時，必須指定欲保護的電腦網路成員，並擬定保護其網路安全機制。每種網路可包含許多周圍網路，在描述周圍網路與其它網路的相對位置時，我們可以描繪出三種周圍網路：最外層周圍網路、內部周圍網路、以及最內層周圍網路。圖 1-1 列出不同周圍網路之間的配置。其中多組內部周圍網路對特定的資源有關連，例如內部周圍網路正好配置在防火牆伺服器的內部。

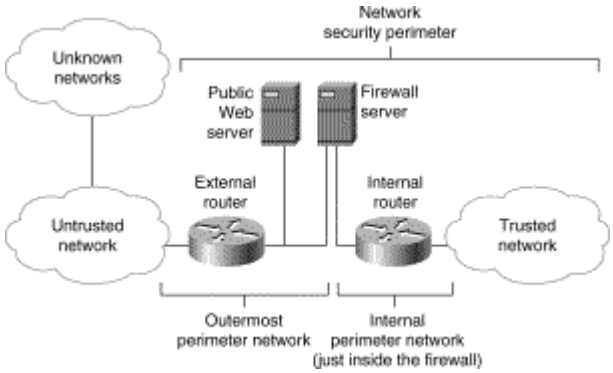
圖 1-1: 現有的三種周圍網路: 最外層、內層、以及最內層



最外層周圍網路是可控制以及無法控制區域間的分水嶺，而通常該點則是用來區隔網路以及 ISP 網路的路由器。內部周圍網路代表額外配置邊界，其中包含其它安全機制，例如內部防火牆與過濾路由器。

圖 1-2 顯示兩種周圍網路(一組最外層周圍網路以及內部周圍網路)，由內部與外部路由器搭配防火牆伺服器共同組成。

圖 1-2: 下圖顯示雙周圍型網路安全設計



將您的防火牆置於外部與內部路由器之間，雖對不能大幅提高對內、外部駭客的防禦力，但卻能大幅降低防火牆伺服器必須處理的資料流量，進而提升防火牆的效能。從外部網路使用者的角度來看，防火牆伺服器代表受信任網路中所有可存取的電腦。防火牆代表一個集中點或控制點，兩端網路的所有通訊都必須透過防火牆方能傳送至另一端。

最外層周圍網路是整個網路基礎建設中最不安全的區域。這個區域通常保留給路由器、防火牆伺服器、以及各種公用網際網路伺服器使用，其中包括 HTTP、FTP、以及 Gopher 伺服器。這個網路區域是最早被存取的部份，因此當駭客嘗試存取內部網路時，最外層周圍遭受攻擊的頻率最高。所有僅供內部使用的敏感企業資訊絕不能置放於最外層周圍網路。

結論

詳細評估網路狀況以及可用性需求，並將這些需求進行評估，以便為您的組織擬定安全策略時，可保護網路與資源，以免遭受攻擊，以及讓系統難以支援合法用途導致生產力不彰。更重要的是，網路駭客除了是外界身份不明的人外，一有可能是內部使用者，因此保護工作的第一步應瞭解涉及網路功能以及互動的各種元素。在了解網路安全問題及防範法則後，相信將為企業帶來更便利與安全的網路使用環境。