第十一章 入侵偵測與網路病毒

『明槍易躲、暗箭難防』『保密防諜、人人有責』；攻擊者總是表現出最善良的一面，讓您失去戒心；目的是破壞、盜取，步驟是入侵，方法是病毒散播。

11-1 入侵偵測系統簡介

就私有網路安全觀點而言，『防火牆』較偏重於防護的功能，它限制封包進出私有網路，功能好像警衛管制人員進出一樣。儘管如此，攻擊者總是可以透過偽裝或防護漏洞，入侵私有網路從事盜取或破壞的工作。『入侵偵測』(Intrusion Detection) 主要的工作是檢視是否有入侵者進入私有網路內，從事未經授權允許的行為。它收集主機系統內或網路流通訊息，再進行分析比對，從中發現是否有違反安全政策的行為或破壞的軌跡，而此專屬設備(硬體或軟體)就稱之為『入侵偵測系統』(Intrusion Detection System, IDS) [10, 15, 17, 52, 53, 112]。由此可見，IDS 與防火牆似乎是相輔相成的，缺一便無法建立一個完整的安全網路系統，所以眾多防火牆設備都具有 IDS 功能，然如此果真就是一個完美無缺的理想組合？其實有待商榷，但不管怎麼說，它在網路安全方面扮演的角色仍不容忽視。本章除了探討 IDS 應具有的功能外，更進一步會討論到如何架設 IDS。

如果從入侵的觀點來看，入侵者最終目的還是希望能進入主機內，從事盜取或破壞的工作，但整個過程中又可區分為兩個階段：第一階段是入侵者僅於窺視網路，但還未真正進入主機系統，第二階段入侵者才成功進入主機內。若從另一角度來看，既然無法完全阻擋入侵者，何不乾脆製作一個陷阱讓入侵者進入再將其逮捕，因此，IDS 系統在製作方面可區分為下列三大類：

- 主機型入侵偵測系統 (Host-based IDS, HIDS)：表示偵測對象是主機設備本身，判別是否遭受入侵攻擊，至於該主機可能是網路設備 (如防禦主機)，或是應用系統主機 (如 Web Server 主機。)，因此又有下列兩種型態：
  - 防火牆入侵偵測：偵測防火牆設備是否遭入侵。
  - 主機入侵偵測：偵測主機系統是否遭入侵。

◈ 網路型入侵偵測系統（Network-based IDS, NIDS）：表示偵測的對象是網路流通訊息，與偵測器本身無關，譬如，透過網路監視器（如 Sniffer）收集封包後，判斷是否有入侵封包進入。

◈ 誘捕防禦系統(Deception Defense System, DDS):就是故意在私有網路上留下破綻，吸引駭客攻擊，使駭客攻擊點集中於某一特定位置，再觀察駭客的攻擊方法，並分析駭客身份及目的。

11-2 入侵偵測與防火牆架設

圖 11-1 為上述三種 IDS 與 DMZ 防火牆之間的配置方法，它們之間所扮演的角色如下：一般外部路由器大多扮演封包過濾的功能，我們將『防火牆 IDS』配置於該路由器上，偵測是否有駭客入侵，此為 IDS 第一道防護功能；萬一駭客封包通過防火牆進入 DMZ 網路，『網路型 IDS』則負責監視 DMZ 網路上的封包，搜尋出可疑的訊息傳輸。駭客入侵系統之後，首要的目標是要進入防禦主機，如果安全操縱防禦主機便能順利阻擋入侵內部網路，因此，可在防禦主機上安裝『主機型 IDS』檢視是否有入侵軌跡。另一方面，駭客入侵後，也可能直接攻擊內部路由器，因此，需安裝『防火牆 IDS』於內部路由器來檢視是否被入侵；假使駭客還是通過內部路由器，或是內部人員越權存取系統資源，當然在主機系統上安裝『主機型 IDS』是不可或缺的。為了更安全起見，可以在內部網路配置『網路型 IDS』監視封包的流量。雖然架設『誘捕系統』可以捕捉駭客，但仍需防止駭客將計就計攻擊系統，因此，還是將它安置於 DMZ 網路上來得安全。

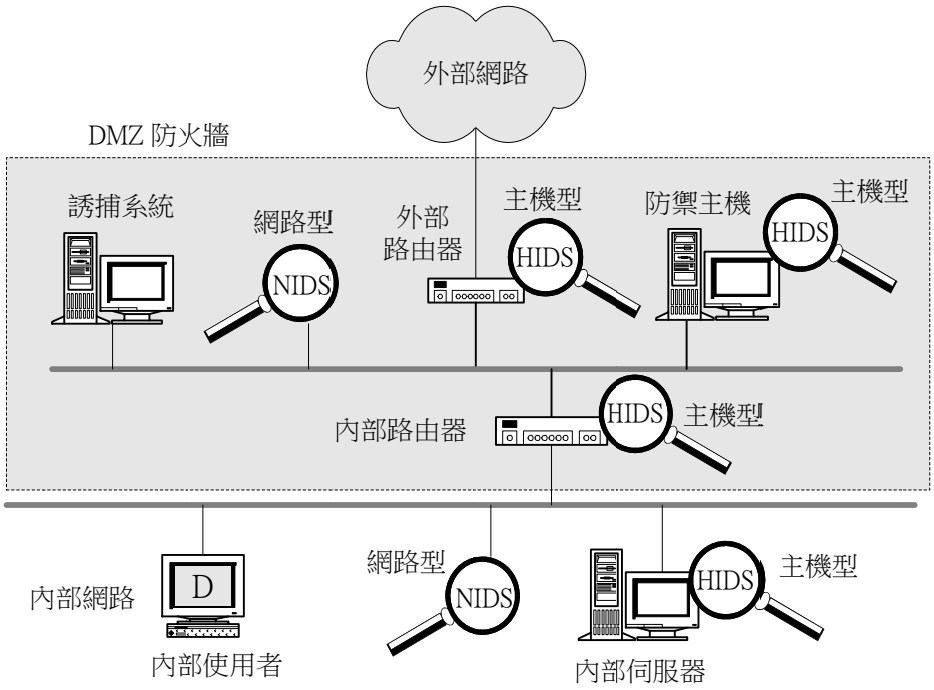

圖 11-1 入侵偵測與防火牆

並非所有防火牆與 IDS 設備都像圖 11-1 那麼完善，至於需要何種程度的安全措施，完全看私有網路所從事的工作而定。我們將圖 11-1 以安全性考量重繪成圖 11-2，可能比較容易理解，其中第一層的防禦設施為防火牆，駭客滲透第一道防護措施後，需經過第二道的防火牆入侵偵測、第三道的網路型入侵偵測、再迴避過第四道的主機型入侵偵測，最後才算真正擊破系統。當然，只要擊破任何一道防護措施都會造成相當的損害，因此，防禦系統必須儘速將其偵測出來使損失降至最低。

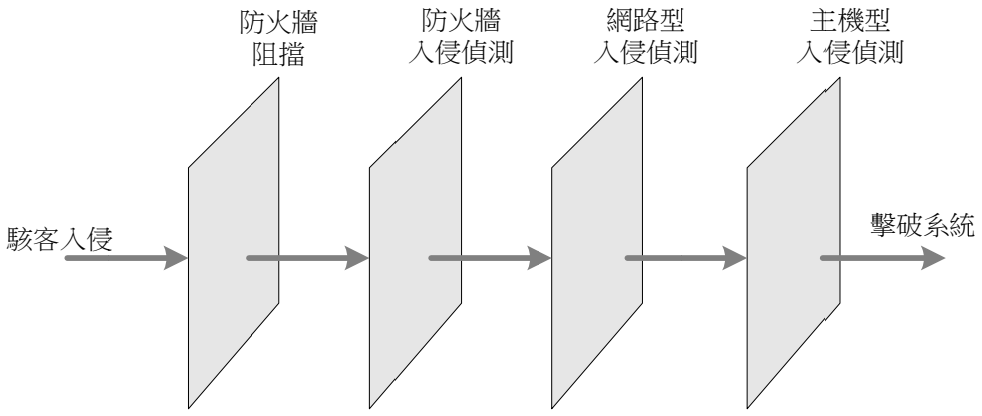

圖 11-2 私有網路的防護能力

11-3 駭客身份

回顧我們介紹密碼學時強調的一個重要觀念，即『再複雜的密碼演算法都有被破

解的可能，破解因素只不過是計算上的成本多寡而已』，也就是說，沒有價值的訊息，可能不會引起攻擊者興趣。但這種觀念完全不適用網路安全，千萬不要認為自己的電腦並不從事機密的工作而疏於防範，攻擊者永遠試著去尋找最不起眼的電腦做為跳板，一旦進入一個不被重視的電腦之後，再由此電腦進入次要電腦，一層一層推進，最後就有可能入侵至最重要的主機系統。另一方面，大部份的私有網路都僅防範外來攻擊者，完全忽略內部的工作人員；其實家賊才是難防，豈可不正視。

一般將入侵者稱為『駭客』(Hacker)，意指不受歡迎或未經允許便進入系統者稱之，我們簡單歸納如下：

- ◈ 網路安全專家：入侵者本身具有相當的網路安全技術，並利用它的技能入侵其他網路，盜取所需的資料。
- ◈ 學生：早期入侵網路並非一件容易的事，非專業人員不可為，但目前知識流通非常快速，已有許多入侵技巧逕行公佈於網路上供人任意下載。任何人只要取得入侵工具，即使沒有具備完整的網路安全知識，也可隨意入侵其他網路；再者，許多學生為了測試及學習，無意中入侵重要的網路系統，縱然無心，但也可能造成嚴重的後果。
- ◈ 犯罪型入侵者：入侵者進入網路系統之後，目的在於盜取機密，並從事犯罪行為，如入侵銀行系統，就是為了盜取客戶帳號再盜領其存款。
- ◈ 商業間諜：進入競爭對手的網路系統內，目的在於盜取設計藍圖或客戶資料。
- ◈ 恐怖份子：網路已成為國家的經濟、政治、文化的動脈，因此已成為恐怖份子的攻擊目標；譬如，中國不定時發動『網軍』入侵台灣或西方國家就是一例。
- ◈ 內部使用者：『駭客』不一定要千辛萬苦越過防火牆攻擊目標網路，可能直接『人』滲透進入內部網路並從事破壞或盜取的行為。記住，只要越過使用者本身權限，執行閱讀、複製、竄改資料等行為，都屬於『駭客』的範疇，而且這些現象多半來自內部使用者。

11-4 入侵技巧

瞭解『駭客』身份之後，還是需要『知彼知己』方能『百戰百勝』，認識到底有那些入侵技巧。我們先來了解一些典型入侵技巧的種類：

11-4-1 竊聽與窺視

所謂竊聽與窺視，即是由公眾網路上蒐集攻擊目標所傳送或接收訊息，再由這些訊息之中找出所期望的資訊。一般來講，入侵者都會嘗試下列的攻擊行為：

- 竊取密碼：許多網路伺服器利用明文來傳輸密碼，或者僅利用簡單的『挑戰與回應』機制來辨識密碼。攻擊者可經由所竊聽的訊息當中，分析得到密碼明文，或取得加密後的密碼，還是可以直接用來登入目標主機。
- 訊務分析：由目標主機與其他電腦之間的交換訊息中，可以了解該主機所扮演的角色，或者提供那些服務。
- 網路位址掃描：若在選定目標之前或之後，並不瞭解目標內有多少網路設備，此時可設定一個網路範圍並尋找有那些設備，從中找出新的攻擊目標。
- 連接埠口掃描：找出網路（或主機）設備之後，可再利用埠口掃描找出可以進入的入口。這種入侵技巧最常見，尤其針對那些不常用或較不起眼的傳輸埠口，管理者容易疏忽，常常被當成攻擊的目標。另一種情況是，入侵成功之後，駭客也會開啟某些較容易疏忽的埠口，讓其他入侵者進入。
- 網路命令探索：入侵者利用一些較普遍的網路命令來探索內部狀態。譬如，使用 finger 命令探索主機內有那些使用者；利用 whois 命令觀察使用者的資料（如 E-mail 位址等等），或 nslookup 命令探索主機 DNS Cache 內的記錄等等。
- SNMP 資料蒐集：一般主機或網路設備都裝設有『簡易網路管理協定』（SNMP，請參考 [3] 第八章介紹），它是 Internet 網路上最基本的管理工具，但因其『共同體』（Community）管理機制太過於鬆散，造成許多入侵者的盜用工具。只要經由 SNMP 資料的蒐集，可以完全了解整個網路的運作狀態。

雖然許多網路監視軟體（如 sniffer）可以竊聽或窺視他人網路狀態，但除非找出可窺視位址，才可能蒐集到目標主機的訊息，尤其目標與攻擊者之間的地理位置太遠的

話，除非在目標主機附近埋入蒐集設備（或入侵軟體），否則還是很困難達成目的。

11-4-2 阻斷服務

『阻斷服務』(Denial of Service, DoS) 即是攻擊者不進入目標，僅讓攻擊目標癱瘓而無法正常工作。值得注意的是，除非攻擊者是惡作劇，否則 DoS 攻擊絕非是駭客真正目的。入侵者癱瘓某一部主機一定有它的特殊目的存在，譬如說，當它癱瘓某 DNS 系統主機時，一定會將原主機上的訊務轉移到它所設立的另一部偽裝主機上。再說，網路設備大多是自動化的，一旦該部主機無法服務時，必定會尋找其他主機要求服務，如此一來，攻擊者便可以進入第二階段的入侵行為。因此，當系統某一部主機被無形之中癱瘓掉之後，此時除了加強該主機的防護功能之外，仍必須透過其他路徑去尋找有相關損害。一般『阻斷服務』攻擊法有下列技巧：

- Ping 到死：連續對目標主機發動 ping 命令，讓主機無暇應付而癱瘓，攻擊來源可以來自全球各地，所以屬於分散式攻擊法。最簡單的方法是，攻擊者首先發佈網路病毒，該病毒會在同一時間內向該目標主機發出 ping 命令。

- SYN 攻擊：採用 Ping 到死的攻擊法很容易被察覺，SYN 攻擊是另一種不知不覺的攻擊法。TCP 封包標頭上將 SYN 設定為 1 (SYN =1) 時，則表示要求對方連線的意思，主機收到連線要求之後，會配置記憶體空間並啟動子程序來處理連線動作。如果攻擊者連續發動（或分散式攻擊）要求連線封包 (SYN=1)，將使目標主機的記憶體滿載，導致無法正常運作。

- ICMP 氾濫：如果攻擊對象是網路設備（如路由器）而非主機系統，ICMP 氾濫攻擊可能比 SYN 攻擊來得有效。攻擊者連續（或分散攻擊）對某一目標設備發出無法完成的 ICMP 訊號（如時間訊息要求），目標主機得連續回應 ICMP 訊息（如時間訊息回應）給原發送端，如此一來，亦可耗費許多網路設備的資源，並可能導致該設備癱瘓。

- 弱點攻擊：目前許多網路設備大多是公開的系統，攻擊者如果知道攻擊目標的機種，接著再試圖找出該機種的弱點，直攻要害的入侵弱點，這是最快使目標癱瘓的方式。譬如，連續向 Windows 系列的 WINS 服務發出 DNS 要求訊號，WINS 必須花

費許多時間來分辨及回應訊息，如此一來，亦可達到耗費系統資源的目的。

◈ DNS Cache 污染：主機上 DNS Cache 是經由查詢 DNS 位址後再記錄起來，作為下一個需要查詢 DNS 位址時使用。攻擊者可透過其他管道去竄改主機上 DNS Cache，或者發佈不實的 DNS 回應讓主機登錄。如此一來，可能重導該主機的連結動作，致使該主機癱瘓。

◈ 路由重導：駭客可能透過 RIP、BGP、OSPF(請參考 [3] 第六章說明)或 ICMP 協定，與攻擊目標的路由器之間交換偽裝訊息，如此一來，該路由器所建立的路由表就完全受攻擊者掌控，攻擊者欲讓目標網路系統癱瘓，再容易不過了。

11-4-3 取代服務

取代服務表示攻擊者偽裝一部與目標系統相同的服務設備，取而代之它的服務，從中騙取之間的交換訊息。首先攻擊者利用路由重導、DNS Cache 污染或癱瘓目標主機，將原來與目標主機通訊的連線重新導至偽裝主機 (或服務) 上。一般取代服務攻擊有下列技巧：

◈ 來源路由替換：發送 IP 封包時，可在 IP 封包的選項 (Option) 欄位中填入來源路由，當封包進入路由器時，路由器會依照該欄位所登錄的路徑依序轉送，並且該欄位內的訊息可任意讀取或修改。攻擊者就利用這個弱點，從中修改所登錄的路徑，無形之中該目標主機的通訊連線將會被重導至另一個偽裝系統上。

◈ 伺服器取代：即是攻擊者偽裝目標主機的伺服器，較常見的攻擊目標是 DHCP、WINS 與 DNS 伺服器。攻擊者取代這些伺服器之後，目標系統上所有通訊連線將完全操縱於攻擊者的手上。

◈ 登入伺服器取代：更嚴重的，攻擊者偽裝了登入伺服器 (如 Windows 2000 或 Kerberos 伺服器)，從中騙取登入者的密碼，如此一來，縱使再複雜的用戶管理系統也是枉然。一般來講，偽裝登入伺服器的時間不會很長，只要騙取到某些密碼便恢復原來的狀態，因此，許多用戶被騙取了密碼還不知覺。

11-4-4 中間人扮演

如果攻擊者成功地讓客戶端導向（如路由導向或 DNS Cache 污染），將客戶端連線轉向到入侵系統上，入侵系統扮演著客戶端與目標主機之間的中間人。當客戶端向伺服主機要求連線時，入侵系統取得通往伺服主機的信任訊息（如密碼），則可取得主機的信任；又當主機回應給客戶端時，入侵系統也攫取了這份訊息，再偽裝成主機回應訊息給客戶端。如此一來，客戶端與主機之間確認了雙方的身份，卻不知道入侵系統從中扮演著中間人的角色，接著它們之間所傳送的機密訊息也都被入侵系統擷取了。

由此可見，中間人扮演是一種非常可怕的攻擊技巧，本書前面所介紹幾種認證技巧，都是在研議何種方法可以避免中間人攻擊。

11-5 入侵偵測系統

11-5-1 入侵偵測系統 – 功能

由『入侵』(Intrusion) 的概念而言，不僅包括攻擊者取得超出合法的系統控制權範圍，還包含收集系統漏洞，避免造成阻斷服務 (DoS) 等可能造成危害電腦系統的行為。『入侵偵測』(Intrusion Detection) 即表示對入侵行為的發覺；它透過網路或主機系統中得到若干關鍵點收集資料，並進行比對及分析，從中發現系統中是否有違反安全策略的行為，從中找出被攻擊的軌跡。進行入侵偵測的專屬設備(含硬體與軟體)，一般稱之為『入侵偵測系統』(Intrusion Detection System, IDS)。基本上，其入侵偵測系統主要的功能有：

- 監視並分析用戶與系統的活動。
- 檢查系統配置與漏洞。
- 評估系統關鍵性資源與資料的完整性。
- 辨識已知的攻擊行為。
- 統計及分析異常行為。
- 管理作業系統之日誌檔案，並識別違反安全政策的存取行為。

11-5-2 入侵偵測系統 - 元件

圖 11-3 為入侵偵測系統的典型模型，其中包含四個主要元件：事件產生器(Event Generators)、事件分析器（ Event Analysis)、事件資料庫（ Event Database ）與反應元件（ Response Units ）等。以下分別敘述這四個元件之功能。

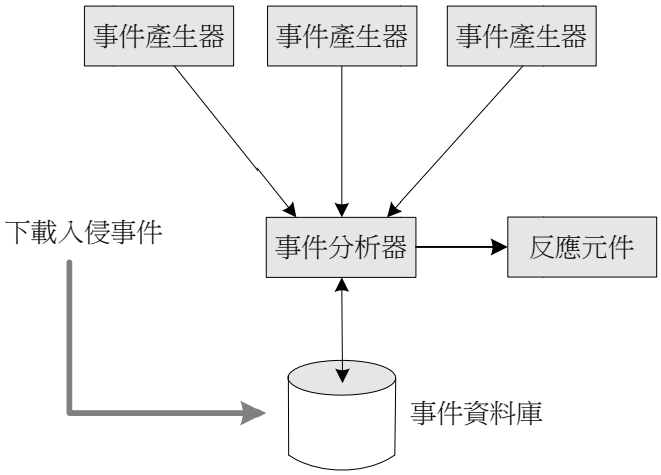

圖 11-3 入侵偵測系統的典型模型

【(A) 事件產生器】

我們將 IDS 所欲分析的資訊稱為『事件』(Event)，它可能來自使用者存取系統的動作程序，或是系統資料被存取的記錄，也可能擷取自網路之間的訊務內容，甚至來自與電腦系統無關的社交行為、電話錄音等等。事件產生器儘可能收集有關入侵行為，或被入侵後所留下的軌跡，並將這些訊息格式化，以標準資料型態表現出來。也就是說，事件產生器是所有入侵偵測資料的來源，針對不同型態的 IDS，有不同事件收集方法，如主機型 IDS 較偏重被入侵後所留下的軌跡，而網路型 IDS 的事件產生則較著重於傳輸訊務的內容。

【(B) 事件分析器】

如何從多個事件之中找出可疑的入侵對象，是事件分析器的主要工作，基本上，分析的方法分『特徵型』(Signature-based) 與『異常型』(Anomaly-based) 兩種 (容後介紹)。

【(C) 事件資料庫】

將可疑或已確定的入侵事件儲存於『事件資料庫』之中，日後如果有相同事件發生時，便可直接判斷入侵已發生。這種做法非常類似目前的防毒系統，隨著各種病毒的出現，病毒防範公司通常製造許多病毒的特徵，隨時下載到用戶電腦上；用戶每次收到訊息時，再由病毒資料庫中比對是否有相同的資料，如果有則隔離該資料(視同病毒)進入系統。目前許多入侵軟體皆可自由下載取得，再說許多入侵方法也非常相似，IDS 系統公司可以隨時收集這些入侵行為的特徵，並下載到用戶的事件資料庫上，如此一來，可以減低用戶端入侵偵測的負荷。

【(D) 反應元件】

當事件分析系統找出入侵的可疑對象之後，必須立即通知系統管理員做適當的回應。反應單元有兩種做法，一者為通知系統管理員，另一者為自動處理入侵事件。目前 IDS 最大的困擾是誤報情況過多，讓許多管理人員不堪負荷；另外，當入侵事件發生時，如管理人員怠慢處理，則可能會遭受嚴重損失。比較折衷的辦法是，IDS 如能肯定某一訊息確是入侵事件的話（如比對事件資料庫），則直接切斷該入侵連線，並做適當的補救措施（如關閉某些服務），若僅是懷疑某一連線為入侵事件，再通知管理人員處理。

11-5-3 入侵偵測系統 – 事件

入侵偵測的第一步是事件資訊的收集，內容包括系統、網路、資料、以及用戶活動的狀態與行為。也就是說，IDS 是否可以精準的找出入侵者，多半取決於事件收集的正確性與完整性，尤其訊息收集地點也會直接影響到它的有效性。基本上，事件訊息的收集有下列五種方法：

【(A) 系統和網路日誌】

『系統日誌』(System Log)是記錄所有存取系統資源的行為；『網路日誌』(Network Log) 則記錄主機上網路通訊的行為。充分利用系統與網路日誌資料是偵測入侵的必要條件，日誌檔案包含網路與系統發生不尋常的活動記錄，由這些記錄中可以瞭解是否有人試圖入侵或已入侵成功，並可以即時啟動相對應的防護措施。日誌檔案記錄各種行為的類型，每個類型包含不同資訊，如『用戶活動』類型的日誌，就包含登入、用戶變更密碼、用戶存取那些文件、用戶授權與認證資訊等等。一般來講，系統日誌會將所有系

統的運作做記錄，如此一來，日誌檔案勢必非常的大，尤其在高流通量的網路系統裡，IDS 要找出可疑的事件發生可不容易，因此，利用『稽核』(Audit) 可能較容易達成。

【(B) 目錄及檔案稽核】

駭客入侵系統最主要的目是要盜取或破壞內部的資料，如果記錄了所有資料或目錄被存取的過程，則該日誌檔案勢必變得非常大，甚至許多 IDS 來不及處理日誌檔案便將一些記錄拋棄掉，如此一來大大減低 IDS 的偵測能力。因此，我們可以將某些較關鍵性的檔案設定『稽核』(Audit) 條件，譬如，某一檔案被讀取時，便會記錄讀取者的用戶識別名稱及時間，並且累計該目錄或檔案被讀取的次數。IDS 週期性檢視稽核檔案，從中發現是否有異常的存取行為，再評估是否為駭客入侵行為。譬如說，如果發現某一個不起眼的檔案連續多次被存取的話，也許該檔案就是有心人士故意建立的，接著再追查存取該檔案的用戶，並追查存取該檔案的意圖如何。另外，當用戶發生異常登入失敗、逾時登入、登入期間過長、或存取超出權限的資料時，都是安全稽核的記錄要項。

【(C) 程式執行稽核】

網路系統上所執行的程式，如作業系統、網路服務、用戶啟動程式、以及應用程式等等，每一個程式多半由多個程序 (Process) 共同來完成，並且每一個程序都應該在他被允許的環境中運作，此環境控制程序可以存取那些資源、程式或資料檔案。當某個程序有異常的存取行為發生時，這就意味可能是駭客已入侵該系統，因此，可由程式執行的稽核記錄中，追查出發出該程序的用戶，並找出入侵對象。

【(D) 訊務收集】

『訊務收集』(Traffic Collection) 表示收集網路上所流通的封包，從中搜尋出可疑的入侵訊息。一般網路是以 IP 封包為傳輸單位，所以可利用網路監視器收集可疑的 IP 封包，再分析找出入侵對象。

【(E) 實體網路架構】

駭客欲透過網路入侵目標系統，無論從何觀點來看都是不容易的事，再說許多防火牆也都著重於網路攻擊。於是乎，何不乾脆找一部電腦偷偷地安裝在目標網路內，雖

然有點過分，但利用實體網路入侵並非不可能，尤其針對無線網路則更容易不過。一般私有網路對於網路的連線，多半不會特別注意每個細節，駭客只要安裝一部電腦作為內應，如此一來，再嚴謹的安全政策也是枉然。因此，IDS 除了監視外部訊息之外，還必須監視內部是否有非管轄內的電腦出現，所以系統管理員必須擁有整體網路的實體配置圖，方便定期檢查是否有盜接網路，或不明電腦出現。

11-6 入侵偵測技術

11-6-1 入侵偵測技術 – 簡介

無論所蒐集到的『系統日誌』、『網路日誌』、『網路訊務』、以及『安全稽核』資料，還是必須經過分析才可以分辨出那些資料是屬於駭客入侵。目前 IDS 系統上有『誤用偵測』(Misuse Detection) 與『異常偵測』(Anomaly Detection) 兩種主要辨識技術。在未介紹這兩種技術之前，首先需釐清『入侵行為』的概念？應如何由許多正當的資料之中分辨出來？我們可由兩個方面來思考：

1. 如果訊息的行為超出正常的行為範圍，或是訊息行為當中有『不應該出現的動作』，則判斷為入侵行為，這種方法稱為『異常偵測』技術。
2. 如果訊息的行為與其他入侵行為相同 (或類似) 時，則判斷為入侵行為，此種方法稱為『誤用偵測』或『特徵偵測』技術。

上述兩種偵測技術需要一套完善的『資料引擎』(Data Engine) 來實現，以下分別介紹之。

11-6-2 入侵偵測技術 – 特徵型

『誤用偵測』(Misuse Detection)又稱為『特徵型偵測』(Signature-based Detection) 或『知識基礎入侵偵測』(Knowledge-based Intrusion Detection)，其實是用已知攻擊手法及系統漏洞的資訊為基礎，將網路攻擊或試圖利用系統安全漏洞入侵的過程中，將所可能產生的『特徵』集合成一個知識庫。IDS 將所有實際發生的事件 (無論是否為攻擊事件)都與此知識庫進行特徵比對，作為評估是否為攻擊或可疑事件的依據。由此可見，『誤用』的邏輯思考為：除非攻擊動作具應有的特徵之外，所有動作都將會被視為合理

正常的。

由此可見，誤用偵測與一般所熟悉的病毒掃描一樣，必須有足夠完整的『攻擊特徵』(Attack Signature) 知識庫，才能偵測出所有已知攻擊手法，並且必須定期下載最新的攻擊特徵，使可偵測出最新的攻擊手法。就現況而言，可供下載的攻擊特徵已超過 2000 個以上，相信還會不斷的成長；比對攻擊特徵遠比掃描病毒來得複雜許多，對於高速流量的網路設備而言，已漸漸會感覺到處理速度的不足。

11-6-3 入侵偵測技術 – 異常型

傳統的『異常偵測』(Anomaly Detection) 採取異常行為偵測 (Behavioral Anomaly Detection) 的策略，此策略是假設每一個人行為模式都有固定的軌跡可尋，並認為經過一段時間的學習及觀察之後，理論上可以分析出使用者的『正常』與『合法』活動。當一些偏離這些平常活動的事件發生時，即意味著可能有資源被盜用或是潛在攻擊事件的可能。因此，所有和過去學習得來的行為模式資訊不符時，皆會被認定為潛在的可能入侵意圖。

由於網路間溝通，基本上是以通訊協定為基礎，理論上所有活動都必須依循通訊協定的要求進行，因此只要出現某些活動未依照規範進行時，即代表可能隱藏可疑的攻擊行為，這種做法被稱為『協定異常偵測』(Protocol Anomaly Detection)。

協定異常偵測可能會引發另一個疑問：既然所有網路活動都必須依循協定規範而為，違反協定規範的行為理應被接收端拒絕才對，如此又何必去偵測它呢？當然，理論上可能是如此，但實際上卻完全不是這麼一回事。由於許多網路服務或用戶端軟體的程式設計也有類似的想法，在撰寫程式時往往會假設或預期通訊的另一端『應該』會依照協定規範來進行通訊，因此就忽略了對方所傳送過來的資料是否依照協定規範來檢查，或是對預期之外的對話進行異常處理。此時，當接收到非標準規範的對話時，可能就會出現不可預期的結果，輕則程式停止運作，重則導致資料毀壞或執行不應該執行的程式，這些不可預期的結果往往就是攻擊者利用的目標。

事實上，許多安全弱點都是由使用者不正常操作狀況下，看到不正常反應之後發現的。惡意攻擊者多半利用這種手法，尋找系統的安全漏洞。譬如，攻擊者常利用特殊

字元、過長參數、不正常路徑、或異常封包等方式，作為測試程式是否可以被利用進行攻擊的途徑。尤其目前『緩衝器溢位』(Buffer Overflow) 攻擊法就是在這種情況下被發揮的淋漓盡致，此種方法是攻擊者盡其可能嘗試每一個可以輸入參數的地方，並餵給可能超過長度的參數，再觀察該程式是否會因為預留的變數長度不足而產生緩衝器溢位的問題。由此可見，偵測異常協定也有相當好的偵測效果，尤其對某些具有清楚的狀態 (State) 的協定而言，透過協定異常偵測不僅可以偵測到可疑的異常事件，還可以偵測出攻擊者是否成功入侵。

譬如，駭客經常利用連接 POP3 伺服器時，使用過長的使用者名稱來測試系統的的弱點；一般 POP3 伺服器多半預留 100 Byte 作為儲存使用者名稱的空間，但當輸入名稱過長時，便會發生緩衝器溢位的問題。此時，POP3 伺服器的服務連線會中斷，而回到 Shell Script，結果駭客可不經由登入程序便進入系統。

當然協定異常偵測並不針對過長的參數而造成緩衝器溢位而已，許多其他異常現象也可以當作協定異常的判斷指標，譬如：

- 在 HTTP、POP、IMAP 等協定中出現伺服器傳回的 Shell 提示字元時。
- 嘗試使用伺服器不支援的指令。
- 伺服器出現超出協定範圍或預期的回應訊息。
- ICMP 封包超出正常比率值。

- 封包重組會造成資料重疊或被覆蓋的現象時。
- 來源 IP、Port 與目的 IP、Port 相同時。
- 異常封包標頭。
- 參數中出現可執行的二進位檔時。

上述僅列出較常出現的範例，攻擊者多半會再研究出更多奇奇怪怪的非典型封包格式，來攻擊主目標系統。

11-6-4 入侵偵測技術 - 資料引擎

有了上述兩種檢測技術之後，接著必須探討如何將所蒐集的資料，利用這兩種技術分析找出入侵跡象。簡單的說，某一個資料處理設備具有異常偵測或誤用偵測處理能

力，並可由一大筆的資料中，找出所期望的入侵訊息，一般將此設備稱之為『資料引擎』（Data Engine），常用技術如下：

- 專家系統（Expert System）：將非法行為（或合法行為）以規則化（Rule-based，if-then 敘述）建立推論引擎，每當事件發生時，再進入推論引擎內比對，找出可疑事件（或合法事件）。
- 有限狀態機（Finite State Machine）：以有限狀態機描述非法行為（或合法行為），並建立一個知識庫。當事件發生時，再依照事件運作的程序比對有限狀態是非法事件還是合法事件。
- 統計分析（Statistical Measure）：以統計技術為基礎，找出非法行為（或合法行為）的輪廓，並建立一個知識庫，當事件發生時，再比對該事件的輪廓是否為目標事件（合法或非法）。
- 類神經網路（Neural Network）：利用類神經網路的適應性學習技巧，學習現有的目標事件，使其改變各網路端點上的加權量，隨著學習事件越多，判斷非法事件（或合法事件）的準確度相對越高。
- 資料探勘（Data Mining）：資料探勘是目前最熱門的入侵偵測技術。它是由雜亂無章的資料內萃取所需資訊，經『分類』（Classification）後，再由『連結分析』（Link Analysis）與『序列分析』（Sequence Analysis）找出可疑目標。

以上僅列出較常見的資料引擎方法，並沒有詳述其相關技術；讀者對這方面有興趣的話，請自行參考其他相關文獻，本書限於篇幅無法一一介紹。

11-7 主機型入侵偵測系統

『主機型入侵偵測』（Host-based Intrusion Detection）表示偵測點在主機本身，至於主機可能是網路設備（如防禦主機）或應用系統（如 Win2k 伺服器）。

11-7-1 防火牆入侵偵測

無論防禦主機或封包過濾器皆是駭客最主要的攻擊目標，雖然在兩設備上設定有

嚴密的封包過濾原則，但是攻擊者還是會想盡各種方法入侵系統。最常見的入侵方法是『開後門』(Trap Backdoor) 與網路阻斷攻擊，以下分別介紹之。

【(A) 後門偵測】

駭客可能採取『誤用攻擊法』掃描各個傳輸埠口的弱點，再依此路徑進入系統之內，接著再開啟其他較少用的埠口讓其他駭客進入。由此可見，預防被入侵的方法，除了必須找出系統弱點之外，還必須隨時掃描是否有不明埠口，無緣無故被開取。目前網路上許多埠口掃描程式 (如 PortScan)，可供下載使用。讀者可試著利用 Java 寫一個掃描程式，範例如下：(僅掃描 0 ~ 1023 埠口)

```
import java.net.*;
import java.io.*;

public class lookForPorts {
	public static void main(String[] args) {
		Socket theSocket;
		String host = "localhost";
		if (args.length >0)
			host = args[0];
		for (int i=0; i<1024; i++) {
			try {
				theSocket = new Socket(host, i);
				System.out.println("There is a server on port "+i+" of " + host);
			}
			catch (UnknownHostException e ) {
				System.err.println(e);
				break;
			}
			catch (IOException e) {
			}
		}
	}
}
```

【(B) 網路阻斷偵測】

網路阻斷攻擊表示攻擊者不讓合法使用者使用網路，亦即攻擊者試圖佔滿整個網路資源，讓其他人無法使用該網路通訊，一般網路阻斷攻擊法有下列三種：

- 服務過載（Service Overloading）：攻擊者針對某一個伺服器提出多個服務請求，如果請求數量過於龐大時，可能讓系統忙於服務這些請求與網路封包，無暇再為其他人服務。欲造成服務過載的攻擊者不困難，只要成功散播病毒，再由這些病毒於指定時間同時向某一系統發出服務請求，即可達到目的；這也是目前許多知名網站被攻擊的困境。

- 訊息洪流（Message Flooding）：即是攻擊者發動許多訊息指向某一特定的攻擊目標，導致該目標停止其他服務。攻擊訊息可以僅僅是簡單的訊息，但被攻擊者為了要回應這些訊息，會佔據絕大部分的資源與系統時間。

- 阻塞攻擊（Clogging Attack）：此攻擊法比較特殊，攻擊者必須非常瞭解網路的運作程序，再依照其特點進行攻擊。譬如，TCP 連線動作是三向握手連絡法，攻擊者每次的要求連線只進行到一半便停止，則系統會耗費許多時間等待下一個訊號進入，或執行不完全連線的相關措施，造成系統的『阻塞』（Clogging）。只要攻擊者發動過多的阻塞連線的話，極有可能造成系統停頓。

偵測與防範阻斷攻擊的方法，唯有不停的檢測系統是否有異常的現象發生，然而這些動作大多是正常的程式運作，欲檢測出來實在不容易。一般會配合網路型入侵偵測，利用封包檢視器（如 Sniffer）過濾一些可疑的封包，再利用『特徵』比對或其他統計方法，找出攻擊者並攔截使其無法進入系統。

11-7-2 伺服主機入侵偵測

『伺服主機入侵偵測』可以說是網路安全最後一道防線，當入侵者已成功進入系統，並且開始盜取或破壞系統時，應該採取何種方法才可將這些『壞份子』揪出來。駭客入侵系統除了做了一些破壞的工作之外，最終目的是要盜取內部資料，如何在最後階段將其偵測出來，就是主機入侵偵測最主要的工作。但話說回來，依照過去使用的經驗，駭客欲入侵主機實在不容易，必須經過防火牆、網路入侵偵測等防護措施。其實最常見的入侵者通常發生在內部管理，亦即是內部合法員工盜取資訊，也可能是駭客堂堂進入辦公室操作電腦。因此，防止主機入侵的首要工作是要做好內部人員的管理，可以從『安全稽核』（Security Audit）與『系統日誌』（System Log）兩方面著手，以下分別介紹之。

【(A)系統日誌】

一般系統(如 Unix)會將某些使用者登入、操作命令、異常登入、或者某些資源被存取的情況，都記錄在日誌檔案(Log File)內，入侵偵測系統只要將這些檔案內的資料轉換成資料庫格式型態，再從中搜尋出駭客的蛛絲馬跡；雖然這種操作看起來非常笨拙，卻是最徹底的偵測方法。一般系統通常非常忙碌，所產生的日誌檔案也非常的大，如何由這些資料中找出可疑的對象，的確不是一件容易的事。目前許多入侵系統都採用『資料探勘』(Data Miming)技術，由大筆的資料當中找出所需要的資訊。

到底系統日誌記錄了那些東西，相信這是讀者最期望知道的答案。基本上，系統日誌記錄的資料，視該部主機執行的應用程式(或網路伺服器)而定，更重要的是，必須系統管理者啟動它，才會真正記錄日誌。我們以 Linux 7.x 版為例，日誌檔案位於 /var/log 目錄下，包含有下列日誌檔案：

- lastlog：此日誌會記錄使用者帳號、通訊埠口、以及最後登入的時間，這些資料可以用來追蹤使用者登入系統的時間(利用 last 命令來讀取此檔案內容)。
- xferlog:此檔案記錄 FTP 檔案傳送的操作，每一筆記錄表示系統執行一次 FTP 傳輸動作，其中包含運作時間、傳輸檔案名稱、使用者名稱等訊息。
- httpd：此目錄下包含兩個檔案：access_log 與 error_log，前者儲存一般存取資訊，包含何人、何時、以及如何存取 HTTP 伺服器內資源；後者記錄有那些存取錯誤的情況發生。
- syslogd：記錄許多行程(Process)類型，包含程式名稱、功能型態、優先性、以及累積記錄訊息等。
- klogd：攔截並記錄 Kernel 的訊息。
- message：接收 syslogd 與 klogd 所輸出的訊息。

以上皆是較基本的日誌檔案，管理者可依照需求更改其記錄型態；譬如，由 syslog.conf 檔案去規劃 syslogd 檔案內的記錄訊息，並且可以利用 syslog 函數呼叫，來存取 syslogd 檔案內的資料。

【(B) 安全稽核】

雖然從日誌檔案中搜尋入侵者的軌跡最為徹底，但礙於檔案過於龐大實在不容易達成。以 Unix/Linux 為例，當使用者由登入系統再執行一次 ls 命令之後，各種日誌檔案所記錄的資料大約有 30 筆訊息，由此可見，搜尋日誌檔案多半在處理一些無關緊要的資料。何不反過來思考，我們將一些敏感較高的資源設定有事件警告，任何人存取這些資源，或者有人越權試著想變更這些資源再將其記錄起來，只要由這些記錄中即可搜尋出可疑份子，這就是『安全稽核』的基本理念。

一般多人使用環境裡，針對每一使用者都有其權限的限制，另一方面，針對目錄檔案也會規劃那些使用者可以存取，以及存取權限如何。有了上述兩種規劃之後，就可以在某些檔案上設定稽核處理，作為記錄該檔案被存取的事實。當使用者越權，或者有異常狀態發生時，便會將這些事實登錄於安全稽核檔案內。我們以 Windows 為例來說明安全稽核的記錄型態；Windows 系統內定規劃有『應用程式記錄』、『安全性記錄』與『系統記錄』等三種檔案，每一種記錄檔的格式如圖 11-6 所示。它以格式化的資料型態記錄各個事件，每個事件記錄依功能分成三部份：表頭、事件描述與一個選擇性的額外資料，然而安全稽核是由前面兩個欄位所構成。

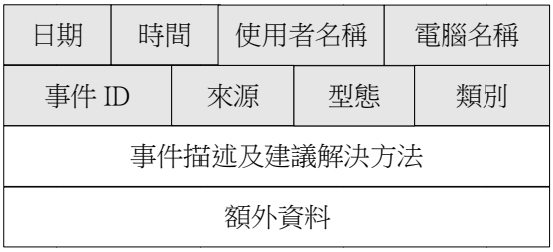

圖 11-6 Windows 事件記錄

安全稽核的表頭包含下列欄位：

- ◈ 日期：事件發生日期。
- ◈ 時間：事件發生時間。
- ◈ 使用者名稱：發生事件者。
- ◈ 電腦名稱：發生事件所在的電腦名稱。
- ◈ 事件 ID：以數字表示發生事件名稱。

◈ 來源：產生事件的來源；可能是一個應用程式、一項系統服務、或是驅動程式。

◈ 型態：如果是一般日誌的話，可能是錯誤、警告或資訊型態；如果是安全稽核，則有成功稽核與失敗稽核兩種型態。

◈ 類別：主要使用於安全日誌，指出該稽核事件是否已被啟動。

三個事件記錄檔中，系統日誌記錄本身作業系統所發生的事件；應用程式日誌檔記錄應用程式所發生的事件；安全日誌則登錄安全性相關事件。管理者除了透過瀏覽該檔案發覺發生事件的原因外，也可以編寫入侵偵測軟體，搜尋可疑的駭客入侵的軌跡。

【(C) 主機阻斷偵測】

主機阻斷是一種獨佔共享資源的攻擊，利用佔據大部分的共享資源，致使他人無法使用資源。主機阻斷攻擊危及資源的可用性，這些資源包含行程、磁碟空間、CPU 使用率、數據機、以及讓管理者無暇應付的寶貴時間。一旦遭受此類型攻擊，輕者降低服務品質，重者癱瘓系統運作，基本上，有下列兩種攻擊方法：

◈ 毀滅性攻擊：直接破壞系統運作，這種攻擊法大多必須擁有較高的系統使用權限才行，但我們也無法保證管理者密碼不會外洩。一旦攻擊者擁有這些權限，就可以直接下達毀滅性的攻擊，攻擊方法有：

- 直接格式化磁碟機：攻擊者取得權限之後，可直接下達格式化磁碟機，如此一來，所有資料必毀於一旦。
- 刪除重要檔案：刪除某些檔案使系統無法運作，譬如刪除 /et/passwd 檔案，讓使用者無法登入系統。
- 關掉電腦電源：攻擊者進入主機房，直接切斷主機電源。雖然這種攻擊很無聊，但還是會造成很大的損傷。
- 切斷網路連線：切斷網路連線，造成網路癱瘓。

◈ 過載攻擊：它是指一共享資源或服務的請求，超過了系統所能負荷的程度，使其無法滿足其他使用者的請求，可能有下列幾種攻擊法：

- 行程攻擊 (Process Attack)：攻擊者產生過多的行程，讓其他人無法使用。

- 磁碟攻擊 (Disk Attack): 攻擊者針對某一個磁碟分割區，攻擊使其填滿，則其他人無法使用該磁區而癱瘓系統。

11-8 網路型入侵偵測系統

隨著防火牆設備 (防禦主機或封包過濾器) 或伺服主機的『主機型入侵偵測系統』(Host-based IDS, HIDS)，多半與該設備上的作業系統有所關聯，不同系統之間很少可以交互使用，所以一般廠商所販賣的入侵偵測系統大多屬於網路型。『網路型入侵系統』(Network-based IDS，NIDS) 可隨需要安裝在任何地方，包含外部網路、DMZ 網路或內部網路，基本上，它是一個獨立系統，與運作環境系統無關。

11-8-1 NIDS 系統缺陷

NIDS 系統的偵測技術可以是誤用偵測或異常偵測，甚至將兩種技術整合而成的『混合型偵測系統』(Hybrid IDS)，其運作原理是儘可能由網路蒐集所有流通的 IP 封包，再利用偵測技術去尋找出可疑的流通訊息。然而，問題在於 HIDS 在蒐集可能的封包時，可能會發生的問題有：

1. 處理能力問題：網路流通是『線』的傳輸速率，一般至少有 100 Mbps 的流通速率。如果訊務流通過於忙碌的話，HIDS 可能無法及時處理所有流通封包，勢必將某些封包拋棄，然而拋棄越多的封包，其檢測能力將會受到限制。

2. 交換器隔離：目前一般私有網路多半利用 Switch/Hub 來架構區域網路，甚至需利用交換器來延伸網路範圍。然而，交換器是利用 Ethernet 位址來轉送訊框，如果目的位址不在某一傳輸埠口上時，訊框將不會被轉送到該埠口上。因此，利用 HIDS 來窺視網路傳輸訊息，如果架設位置不理想的話，可能蒐集不到任何封包，或僅能蒐集到某一部份的訊息。

3. HIDS 安全性問題：入侵偵測系統本身也是一個主機設備，必須經由 TCP/IP 裝置才能蒐集網路上流通的訊息，主機通常包含大量待搜尋的資料，因此，極可能成為被入侵對象。

解決第一個問題，可由兩方面來思考，一者提高 HIDS 的處理速度，即使用較快

的 CPU 或較大的記憶體空間；另一者是加強『資料引擎』的處理能力，一般來講誤用偵測技術會比異常偵測來得快，這是一般 HIDS 多半採用誤用偵測技術的主要原因。

解決第二個問題的關鍵，在於不要讓 HIDS 設備安裝於交換器上即可。由圖 11-7 連接方式可以看出，唯有通往 HIDS 設備的封包才會被轉送到該連接埠口上，如此一來，HIDS 將無法蒐集到其他電腦之間的流通封包。另一個解決方案是在某些交換器都預留一個通訊埠口，由此埠口上可以蒐集到所有該交換器的訊務，但也侷限於所連接的交換器而已，再說並非所有交換器都有此通訊埠口。

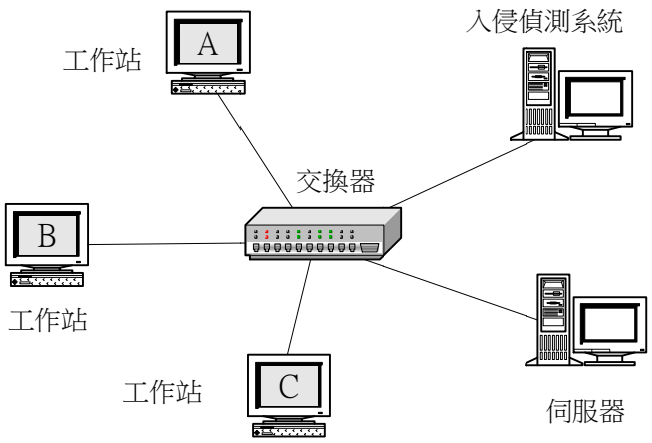

圖 11-7 HIDS 無法蒐集訊務的連接方式

解決第三個問題最為棘手，IDS 會成為被入侵對象的主因是，所儲存的資料正是駭客最期望盜取或竄改的資料。譬如 HIDS 採用誤用偵測技術，則該系統內必須收集許多入侵行為的『特徵』，駭客只要修改這些資料的話，便成為入侵系統最明顯的漏洞。有一個最簡單的解決方法是，蒐集設備不要與分析軟體安裝於同一部主機內，甚至另外安裝的分析主機也必須與原網路分離，如此一來，入侵者就找不到攻擊的對象，如圖 11-8 所示。其中蒐集主機上安裝有兩片網路卡，一者連接到私有網路上，並負責蒐集流通訊務；另一片網路卡連接到分析主機上，將所蒐集的訊務透過該網路傳送給分析主機，並且蒐集主機必須取消兩片網路卡之間的路由轉送功能。

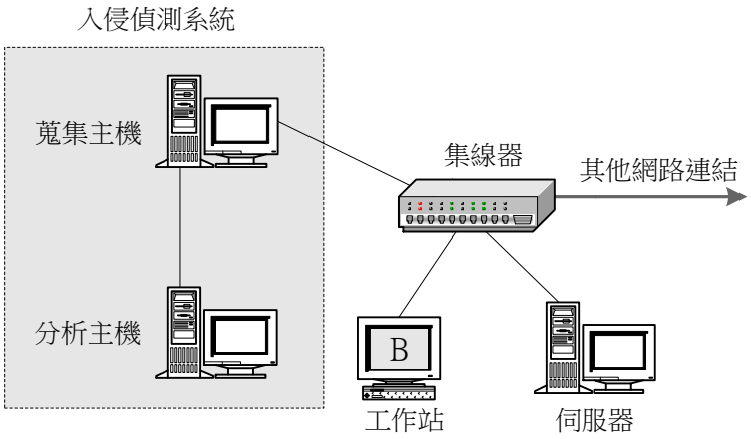

圖 11-8 NIDS 設備的裝置

11-8-2 NIDS 系統配置

如果可以將 NIDS 分成蒐集主機與分析主機兩者分別處理相關工作的話，則前面所述的三個問題都可以迎刃而解。第一個問題，如分析主機採用較高速的處理設備，並且不用處理蒐集訊務的工作，應該可以提高許多處理能力。第二個問題，我們不可能將所有網路設施都改成 Hub 連線，如此一來，不但網路連線範圍會受到限制，傳輸效率也會降低許多。然而，僅負責蒐集訊務的主機並不需要很昂貴的伺服主機，只要一般個人電腦層次的工作站即可。因此，我們可以將多部蒐集主機分別裝設於各個通訊節點，再將所蒐集的訊務集中傳送給分析主機即可。圖 11-9 即是由上述概念所建構的 IDS 配置。

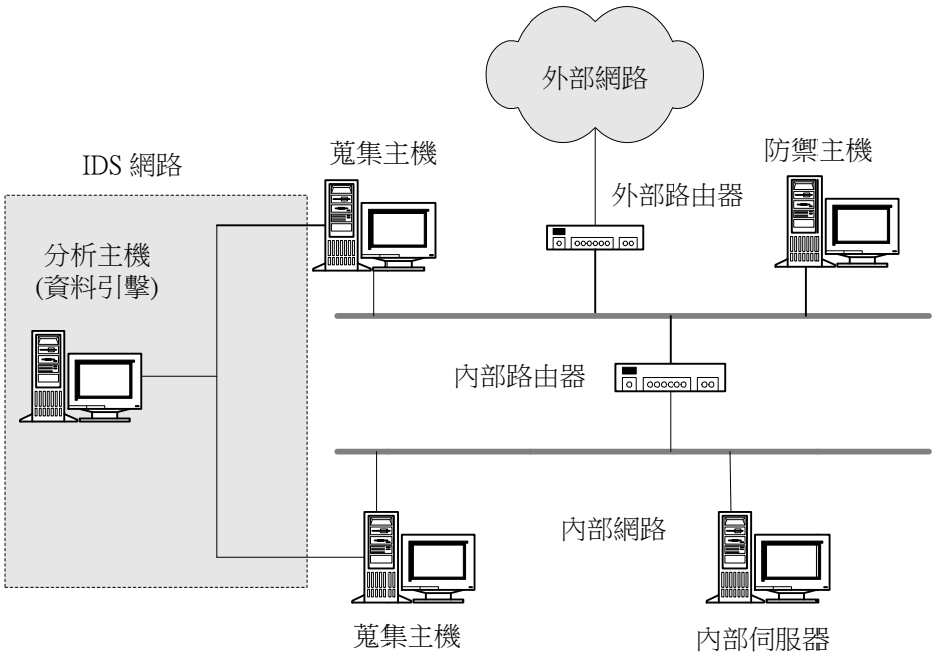

圖 11-9 安全性 HIDS 配置

圖 11-9 並沒有繪出 Hub 連線配置，這方面請讀者於實務架設時必須特別留意。另存在一個困難點，目前 HIDS 多半採用『誤用偵測技術』，而入侵行為的特徵大多由 IDS 廠商提供，並且隨時下載到客戶端的資料引擎上（與防毒措施類似）。如果採用圖 11-9 網路配置的話，則廠商將無法直接由網路下載最新發現的入侵特徵，需由人工下載來解決這個問題。

11-9 誘捕型防禦系統

『誘捕系統』（Deception System）即是製作一部偽裝設備讓駭客攻擊，不但可以從中逮捕入侵者，也可由它的攻擊行為瞭解其攻擊技倆，依此研議出更嚴密的安全防範技術。既然駭客入侵方法是無孔不入，僅利用防火牆阻擋進入是不夠的，還是需要配合入侵偵測系統，找出入侵者的蛛絲馬跡，若是還無法阻擋入侵，乾脆製作一個偽裝系統，引君入甕再將其逮捕。換句話說，我們可以製作一個防護能力較低的偽裝系統，使其成為攻擊目標，不但可以延長攻擊者進入主系統的時間，同時它也提供防禦者足夠的資訊來了解攻擊者；藉由欺騙攻擊者，防衛者提供錯誤資訊，迫使對方浪費時間作無益的進攻，以減弱後續的攻擊力量。而此偽裝系統則稱為『蜜蜂罐』（Honeypot）。

誘捕系統並非新的觀念，許多安全人員與專家試著用各種蜜蜂罐，作為轉移攻擊者的目標，使用蜜蜂罐可達到下列功能：

- ◈ 消耗攻擊者時間：攻擊者可能耗費大量時間嘗試刺探及研究誘捕系統，在這階段裡就不會去攻擊真實主機。
- ◈ 錯誤安全措施：讓攻擊者對現有的安全措施產生錯誤的印象，對方可能浪費許多時間尋找攻擊蜜蜂罐的工具，但這些工具並無法攻擊真實主機。
- ◈ 降低被攻擊可能：如果蜜蜂罐存在的話，可減低真實系統隨時遭受攻擊的可能。

同樣的，蜜蜂罐也有被識破的可能；攻擊者可能將計就計，入侵蜜蜂罐之後，將它視為跳板，再入侵其他真實系統。由此可見，建立蜜蜂罐的誘捕系統並非想像中那麼容易，必須隨時變更蜜蜂罐的組態，以減少被識破的可能。基本上，蜜蜂罐的防禦措施

有下列四種型態。(資料來自 IIS 網站)

◈ 『待宰羔羊』(Sacrificial Lamb): 即是在現有的系統上，故意留下容易攻擊的弱點，讓入侵者攻擊，並從中收集被攻擊的資料。基本上，待宰羔羊大多安裝在現有的網路設備上，如路由器或防火牆設施；對攻擊者而言，很難去分辨攻擊目標的真偽，但對防禦者而言，卻是不難捏準的安全措施。

◈ 『偽裝系統』(Facade): 即是偽裝一個與目標主機相類似的假象系統，吸引攻擊者的攻擊目標。一般都是利用軟體模擬某個特定服務或應用程式，每當這個偽裝受到攻擊時，便可收集攻擊資訊。然而，偽裝程度越深，則可收集到的資訊就越完整。

◈ 『傀儡系統』(Instrumented System): 整合待宰羔羊與偽裝系統之技術，建立一個專屬的誘捕系統，即成為傀儡系統，其中包含資料收集、攻擊赫阻、政策式警示、以及企業級管理功能。簡單的說，傀儡系統是一個專家級的誘捕工具，它可能是由一套包含硬體與軟體所構成的蜜蜂罐。

◈ 『蜜蜂網』(Heneynet): 當組織過於龐大時，可能會出現多個被攻擊點，另外，攻擊者也可能以聲東擊西的方式來入侵系統。組織內出現多個攻擊點的情況，多半不是偶發的現象，這些攻擊點多會存在一些關聯性的行為。如此一來，僅憑設立一個或多個蜜蜂罐並不能達到預期效果，需更進一步的整合這些蜜蜂罐，之間互相交換所收集的資料，或互相支援誘捕的功能，即成為『蜜蜂網』的防範措施。蜜蜂網也是屬於專家型的誘捕工具，需有一套功能強大的入侵偵測功能，這也是目前許多網路安全專家研究的對象。

誘捕系統最能表現出爾虞我詐的攻擊與防禦行為，使諜對諜戰鬥觀念在網路上表現得淋漓盡致，因此成為近年來網路安全專家最為熱門的研究課題。

11-10 網路病毒

相信網路病毒是目前網路公認最困擾的問題，幾乎每一部上網的電腦都有防毒措施，這是網路發展的障礙之一，然而，病毒似乎與網路入侵之間有緊密性的關聯，許多入侵行為都是藉由病毒散播作為攻擊的先頭部隊。說實在的，經由防火牆、網路入侵偵

測等等的安全防護，駭客如想要以非法路徑入侵系統，是極不容易的事，唯有藉由合法路徑來散播病毒，較容易入侵系統。譬如，攻擊者可藉由發送郵件給內部工作人員，員工讀信之後無形之中已將病毒載入系統之中，此病毒在某一特定時間內會開啟系統一些較不惹眼的埠口，外部攻擊程式再經由該埠口堂堂進入系統，從事破壞的工作。類似這種攻擊法不勝枚舉，我們也可發現偵測入侵攻擊是離不開網路病毒的偵測。

11-10-1 惡意的程式

電腦是一組硬體與軟體所組合而成的機械，不會受到天氣變化而感冒，也不會受到 SARS 侵襲，何來『病毒』(Virus) 感染之有？其實『病毒』是一種惡意程式，只不過這些程式會自行複製給其他電腦，如果惡意程式有意破壞系統的話，它所複製的程式同樣也具有這些功能；然而，它是無形之中散播或自行複製給其他人，當然也必須有接觸到才會受它感染，其動作就像『細菌』傳播一樣。我們將網路上常出現之惡意程式的型態歸納如下：

- ◈ 開後門 (Trap Backdoor): 後門程式執行後，會去開啟某一特定的傳輸埠口，讓其他攻擊程式由此埠口進入系統。
- ◈ 邏輯炸彈 (Logic Bomb): 此類型的惡意程式會在某一特定時間內摧毀系統。
- ◈ 特洛伊木馬 (Trojan Horses): 該類型程式會隱藏在其他程式內，進而入侵系統或跨越較高權利，再從事破壞的工作。一般系統都有防護措施來隔離不明程式的進入，但特洛伊木馬程式會附加在其他程式內，當原程式被執行時，惡意程式會跟隨著執行其入侵或破壞的工作，而且它的執行權限與原程式相同。
- ◈ 電腦病毒(Virus): 此類型程式會感染給其他程式，感染途徑多半是經由接觸而來。譬如，某部電腦上執行已被感染的程式，該病毒程式便會常駐在記憶體中。當再執行其他程式時，則該病毒程式便會再值入該程式之中，接下來，已感染的程式被執行時，會再感染其他程式，如此散佈出去。
- ◈ 網路蠕蟲 (Worm): 網路蠕蟲與電腦病毒相類似，可能是值入特洛伊木馬或其他破壞程式，但它感染路徑多半是透過網路傳輸，一般傳輸路徑有：
  - ■ 電子郵件：蠕蟲病毒透過電子郵件傳遞，感染者只要開啟郵件，病毒程式就會

自動被啟動，並值入系統內，這也是目前入侵或病毒傳播最常見的傳播方式。

- 遠端登入：登入到遠端具有病毒感染的主機，蠕蟲程式也可以由此通訊連線進入系統。
- 遠端執行程式：蠕蟲透過遠端執行程式入侵系統。客戶端瀏覽一個被病毒感染的網頁，客戶端電腦也會受到蠕蟲病毒入侵。

◈ 巨集病毒（Macro Virus）：一般病毒多半屬於可執行檔，但最可怕的病毒是由巨集命令所構成的巨集病毒。許多資料或程式都必須在特定工作平台（如 Word）上執行，然而大多是利用巨集命令的 Script 來規劃執行程序，巨集病毒就是附加在這 Script 命令上，隨著散播及從事破壞的工作，如感染 Word 文件檔的病毒就是這種類型。

上述各種病毒類型並非各自獨立，相互之間也有連帶性關係；譬如，某一巨集病毒可能也具有網路蠕蟲或特洛伊木馬病毒的功能。

11-10-2 病毒的生命週期

簡單的說，病毒也是一種程式，它必須經過執行之後才會有破壞力，一般由病毒的產生到結束的生命週期可區分為下列四個階段：

◈ 潛伏期（Dormant Phase）：病毒入侵後處於閒置狀態。病毒遲早會被某一特定事件所觸發，譬如，某個日期、某個程式或檔案存在時，或是磁碟容量超過某些上限時，但並非所有病毒都需經過這個階段。

◈ 散播期（Propagation Phase）：病毒複製本身到其他程式或他人磁碟空間的階段。每個被感染的程式都會得到一個病毒副本，並且進入散播期感染給其他人。

◈ 觸發期（Triggering Phase）：病毒被啟動並準備執行預定動作。啟動原因如同潛伏期一樣，多半事經由特殊事件觸發所引起。

◈ 執行期（Execution Phase）：執行的功能被啟動。在這階段裡，病毒可能執行破壞或入侵的工作。

由此可見，防治病毒必須在它的執行期之前找出來，一般來講，病毒由入侵進入潛

伏期到執行期之間尚有一段時間，掃描病毒就是期望在這段時間內將病毒揪出。

11-10-3 病毒的類型

既然病毒也是一種程式，但這程式如何被執行？如果不去執行它可能會被破壞嗎？其實有些病毒是自我執行程式，它會自行啟動並進入 CPU 工作排序內。另有些病毒則必須附加在其他程式內，當該程式被執行時，病毒也隨著被執行，如此就不會牽涉到 CPU 排序的問題。我們將病毒的類型歸類如下：

- 寄生病毒（Parasitic Virus）：此類型病毒必須附加在其他程式內，巨集病毒多半屬於這個類型。
- 記憶體常駐病毒（Memory-resident Virus）：此類型病毒會自我執行並進駐於主記憶體內，當系統執行其他程式時，才會感染到該程式上。
  - 啟動磁區病毒（Boot Sector Virus）：此類型病毒會感染主機開機磁區，當主機開機後便具有病毒感染能力。
  - 隱形病毒（Stealth Virus）：此類型病毒被設計成可以躲過病毒掃描，一般都是將病毒壓縮後，再複製到其他系統上，如此一來，掃描程式欲找出壓縮後的病毒實在很困難。
- 多型病毒（Polymorphous Virus）：此類型病毒每經一次的複製後，都會改變其形貌，因此可以躲過病毒『特徵』掃描。

11-10-4 防毒的技巧

早期防毒的口號是『不要複製來路不明的檔案』，後來是『不要開啟來路不明的信件或檔案』，但目前這兩個口號似乎已不靈光。現在是唯有不上網才可能避開病毒的感染，變化無窮的病毒也並非簡單的掃描程式足以防範。一般掃描病毒皆是以『偵測』、『辨認』與『清除』三個步驟來達成，其中『辨識』多半以病毒的特徵作為比對。一般使用者並無能力隨時隨地蒐集可能出現病毒的『特徵』，這方面大多仰賴廠商提供，也就是說，病毒掃描軟體廠商隨時隨地蒐集可能出現的病毒，並尋找出病毒可以比對的特徵，再自動下載給客戶端，存入於客戶端的資料引擎內，客戶端開啟檔案或收取信件時，可

經由資料引擎比對該檔案或信件是否含有病毒。基本上，防毒軟體有下列四種層次的防禦功能：

- ◈ 特徵掃描：利用病毒特徵掃描檔案或系統是否有病毒感染。
- ◈ 啟發式掃描：不僅利用病毒特徵掃描，還利用啟發式探測病毒可能變形的型態。
- ◈ 行為陷阱：是一種常駐記憶體的軟體，並監視系統是否有異常行為，如有則判斷可能病毒入侵。
- ◈ 整合性防範：將上述防毒功能整合一個完整的系統，一般簡單的病毒特徵由客戶電腦執行掃描的工作，對於需要經過較複雜推論才能分辨病毒(如多型病毒)時，則在組織內設立一個資料引擎，專門處理推論的工作。

病毒防範是一門非常專業的技術，然而許多組織單位多半忽略它，尤其從事於網路安全工作者，應需特別研習有關病毒入侵的伎倆。