入侵偵測系統

- IDS 分類
  - 誤用偵測型 (Misuse detection) vs. 異常偵測型 (Anomaly detection)
    - 誤用偵測：分析所收集的資訊並與攻擊特徵比對；僅能偵測出具 IDS 攻特徵的攻擊
    - 異常偵測：掃尋任何異常行為並通知管理者；記錄所有與一般使用者行為不同的活動
  - 被動式系統 (Passive systems) vs. 回應式系統 (Reactive systems)
    - 被動式：偵測可能危害安全的行為，記錄後發出警告
    - 回應式：系統會將可疑使用者逐出 (強制登出) 或重設定防火牆以維系統安全

入侵偵測系統 (Cont.)

- 網路型系統 (Network-based systems) vs. 主機型系統 (Host-based systems)
  - 網路型系統：分析網路訊務
  - 主機型系統：分析每台主機的行為
- IDS 使用的方法
  - 事先阻斷 (Preemptive blocking)
    - 又可稱為驅逐警戒 (Banishment vigilance)
    - 在入侵發生前加以預防
    - 注意即將發生的危險徵兆，並阻斷這些徵兆來源的使用者或 IP

入侵偵測系統 (Cont.)

- 有誤判的情況 (把合法使用者判定成入侵者)

- 滲透 （ 無間道)
  - 非某特殊軟體
  - 資訊安全管理者滲透網路上的駭客 / 怪客群組
  - 滲透行為較為少見
  - 大部份資訊安全管理者過於依賴製造商的各種安全性公告
- 入侵誘捕
  - 誘捕系統 (Honeypot)
  - 建立一個有吸引力的假系統，吸引入侵者上當
  - 引誘攻擊者進入此系統並監視攻擊者的行為

入侵偵測系統 (Cont.)

- 入侵嚇阻
  - 讓系統看起來不吸引人 (e.g. 入侵難度高，入侵動作會變監視)
  - 如何讓系統看起不吸引人？ → 隱藏有價值的資產
  - 讓系統看起來更安全 → 顯示警告與主動出現的監視警告
  - 讓想入侵者成功入侵所需花費的代價遠比所得到的價值還來得高

入侵偵測系統 (Cont.)

- 網路型系統 (Network-based systems) vs. 主機型系統 (Host-based systems)
  - 網路型系統：分析網路訊務
  - 主機型系統：分析每台主機的行為
- IDS 使用的方法
  - 事先阻斷 (Preemptive blocking)
    - 又可稱為驅逐警戒 (Banishment vigilance)
    - 在入侵發生前加以預防
    - 注意即將發生的危險徵兆，並阻斷這些徵兆來源的使用者或 IP

入侵偵測系統 (Cont.)

  - 有誤判的情況 (把合法使用者判定成入侵者)
- 滲透 （ 無間道)
  - 非某特殊軟體
  - 資訊安全管理者滲透網路上的駭客 / 怪客群組
  - 滲透行為較為少見
  - 大部份資訊安全管理者過於依賴製造商的各種安全性公告
- 入侵誘捕
  - 誘捕系統 (Honeypot)
  - 建立一個有吸引力的假系統，吸引入侵者上當
  - 引誘攻擊者進入此系統並監視攻擊者的行為

入侵偵測系統 (Cont.)

- 入侵嚇阻
  - 讓系統看起來不吸引人 (e.g. 入侵難度高，入侵動作會變監視)
  - 如何讓系統看起不吸引人？ → 隱藏有價值的資產
  - 讓系統看起來更安全 → 顯示警告與主動出現的監視警告
  - 讓想入侵者成功入侵所需花費的代價遠比所得到的價值還來得高

入侵偵測系統 (Cont.)

- 特徵偵測
  - 特徵偵測是將被找到一些固定的特徵 (signatures) 與偵測到的事件做比對，以識別可能的安全事故
  - 例如，設已知一封主題為「生日快樂」且有附檔 gift.exe 的電子郵件為惡意攻擊，IDPS 會過濾接收到的電子郵件，符合者就予以刪除
  - 特徵偵測對偵測已知的威脅非常有效；但無法偵測原先不瞭解的威脅或是改裝後的已知威脅
  - 上面例子的附檔名若被攻擊者改為 gift2.exe，IDPS 可能在比對 gift.exe 特徵不符而放這個電子郵件通過

入侵偵測系統 (Cont.)

- 特徵偵測很簡單，但 IDPS 只將眼前的一個封包或一筆記錄與資料庫內的特徵做比對，卻不了解網路或應用的協定，也無法追蹤狀態改變
- 異常偵測
  - 異常狀況 (anomaly) 為主的偵測是將觀察到的事件與定義中的「**正常活動**」做比較，以期找出重要的差異
  - 使用者、主機、應用與網路的正常活動都定義在一個**描述檔** (profile) 內，它是在監視正常活動一段時間後所記錄下來的系統特性

入侵偵測系統 (Cont.)

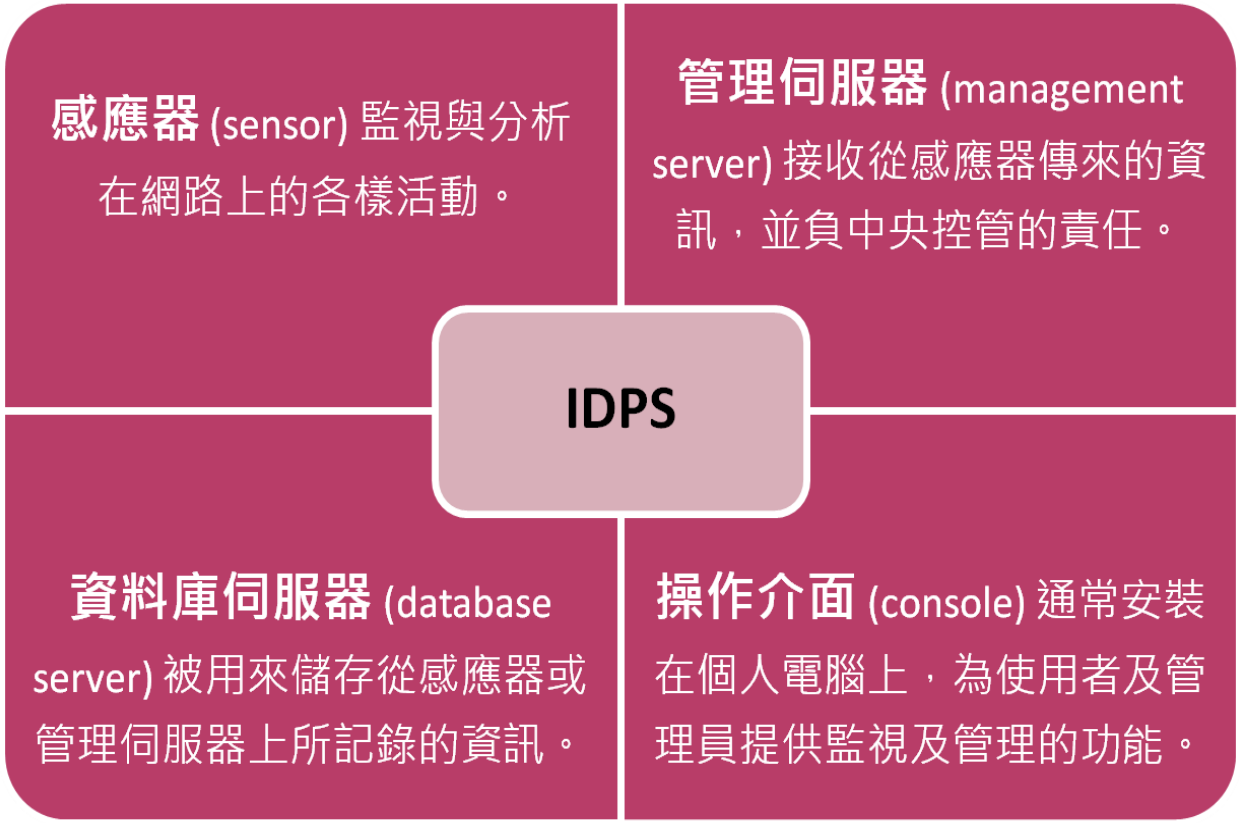
- 描述檔裡記錄各種有用的正常活動統計數據，如一段時間內組織發出和接收的電子郵件數目，每台主機的 CPU 平均使用率，以及 VPN 登入失敗的平均次數等
- 異常偵測最大的好處：可以偵測原先不瞭解的威脅
  - 例如：一個新型病毒入侵，IDPS 無法做已知病毒的特徵比對，但因為該病毒對外狂發電子郵件造成 CPU 使用率大增，而被偵測到異常狀況

入侵偵測系統 (Cont.)

- 協定狀態分析 (Stateful protocol analysis)
  - 將觀察到的事件與協定的預先定義之正常狀態做比較，以期找出重要的差異
  - 異常偵測 → 使用自己的主機或網路所產生的特定描述檔
  - 協定狀態分析 → 依靠廠商提供的描述檔，說明特定的協定該如何被使用
  - 「狀態的 (stateful)」表示這種 IDPS 可以瞭解與追蹤網路層、傳輸層、與應用層的各種協定以及它們的各種狀態

入侵偵測系統 (Cont.)

- 協定狀態分析法的**缺點**
  - 耗費運算資源，因為它需要追蹤狀態並進行複雜的分析
  - 它查不到沒有違背協定的攻擊，例如在很短的時間內進行極大量符合協定的通訊，而造成 DoS
- IDPS的元件



網路 IDPS

- 網路 IDPS監視某段網路或元件的資訊流，分析網路及應用協定的封包來識別可疑的活動
- 和防火牆類似，網路 IDPS 使用 OSI 裡的應用層 (L7)、傳輸層 (L4)、網路層 (L3) 和資料連結層 (L2)
- 網路IDPS 的伺服器與操作介面都和其它三種 IDPS 大同小異。但感應器的 NIC 設定在隨意模式，可以接收所有經過的封包，不論目的 IP 位址
- 感應器可以擺設為居間 (inline) 或是被動 (passive) 兩種模式

無線 IDPS

- 無線 IDPS 與網路 IDPS 間最大的差異在**感應器**。網路 IDPS 可以看到它所監視的網路上每一個封包；而無線 IDPS 則對資訊流取樣 (sampling)
- IEEE 802.11 將頻寬切分為十四個通道 (channels)，台灣和美國只用其中的十一個。無線感應器要在通道之間切換掃描，同時應該注意攻擊者有時候會利用國內未授權的通道

網路行為分析 (NBA) 系統

- 網路行為分析 (Network Behavior Analysis, NBA) 系統通常被動的檢查網路的資訊流或統計資料，以識別產生異常流量
- 有的 NBA 感應器與網路 IDPS 感應器類似，直接監視網路上的封包；有的則是從路由器等網路元件取得相關的流量資訊
- NBA 系統大致與網路 IDPS 類似，只是前者更重視從整體網路的統計數據上分析出異常現象；而後者著重於監視個別封包

主機 IDPS

- 主機 IDPS 使用裝置在主機上的偵測軟體，稱為代理人 (agent)，來監視主機上的可疑的事件
- 網路 IDPS 通常無法監視加密的通訊；但主機 IDPS 位居終端，因此可以看到解密後的活動
- 主機 IDPS 有兩個問題：
  - 由於裝置在主機上，若系統被攻破，IDPS 也就失去作用
  - 主機 IDPS 得分別裝置在每台受保護的主機上，因此安裝與維護都是管理員吃重的工作