計畫名稱：雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究－雲端環境中持續且目標性攻擊偵測之研究

執行單位：國立中山大學 資訊管理學系

主持人：陳嘉玫 教授

計畫編號：MOST 103－2221－E－110－049－MY3

一、 摘要

近年來，駭客組織攻擊的型態已由單一攻擊型態轉變成複雜性且多階段性的攻擊方式，其攻擊目標通常具有針對性，以政府和企業中重要的部門為主要攻擊對象，目的在於竊取所需要的特定且重要的機密資訊。故其攻擊的手法與媒介呈現多元化複雜的攻擊方式，攻擊週期可能長達幾個月甚至幾年。

本研究針對目標式攻擊進行偵測的階段中，首先利用駭客最常使用的社交攻擊方式作為偵測的第一階段；接下來，將收集的 log 資料進行關聯分析決定可能攻擊的動作，並利用貝式網路理論計算每個攻擊階段發生的機率，藉此作為擷取特徵的基礎；最後再利用設定的特徵作為分析風險評估的依據以預測被攻擊的可能性。

二、 架構功能

本研究是設計一套以貝氏網路模型為理論基礎的偵測系統，透過數個不同入侵偵測系統之間所發出的警訊做關聯分析之後，藉由觀察出的特徵來進行偵測系統的建置，希望能夠從中找出警訊是否符合進階持續性滲透攻擊的攻擊階段，藉此來降低進階持續性滲透攻擊事件發生機率的系統。

本研究的系統架構主要使用網路流量警訊紀錄、Mail 紀錄以及社交網路存取紀錄，運用偵測模型進行風險值計算之後帶入目標攻擊偵測模組，最後產出結果，本系統的系統架構流程圖如下圖表示：

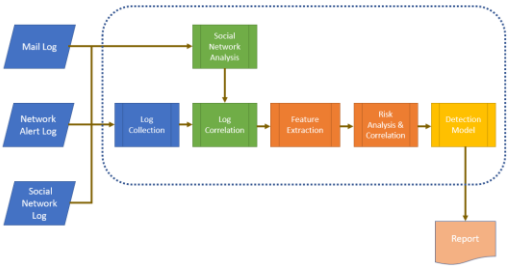

圖 1 系統架構圖

三、 技術特色

貝氏網路在處理具有不確定性的相關知識時具有相當優勢，因為貝氏網路可以經由觀測到的證據或已知的背景知識對未知或具有不確定性的狀態進行推論。因此本研究將採用貝氏網路之優點，提高系統應變能力與偵測率。

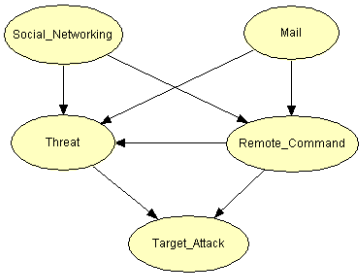

圖 2 目標式攻擊之貝氏網路偵測模型

其特色如下：

- ✧ 結合多個 IDS 日誌資料，取得對應的日誌資料
- ✧ 處理具有不確定性的相關知識時具有相當優勢
- ✧ 低成本的設備需求

四、 實驗結果

本測試實驗主要目的在驗證本系統在真實環境中偵測目標式攻擊之成效以及在不同的時間區段的組合是否會影響到偵測結果。以實際組織之網路資訊做系統評估，該組織屬於中大型組織。資料時間為長達 6 個月，總資料收集筆數約為一億筆。

由於目標式攻擊是一種長時間潛伏的攻擊型態，往往很難立即被察覺。本實驗的目的便是利用測試不同的時間區段組合，依照其影響系統偵測成果程度，來找出偵測目標式攻擊之有效時間區間。

本研究首先將先將收集到的資料進行關聯與分析之後，取得目前內部網路中可能遭受到目標式攻擊的受害者。本測試將時間區段分別為 4 周、6 周、8 周、10 周、12 周、14 周以及 16 周。本系統在第 14 周時能達到最高的偵測率。不同時間區段之偵測結果與偵測率如下圖：

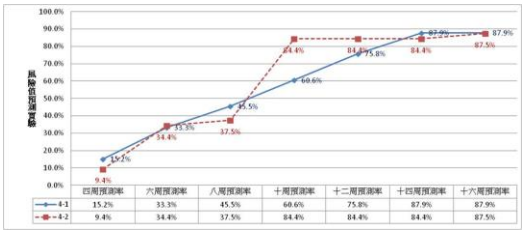

圖 2 不同時間區段之偵測率

五、 技術應用範圍

透過本計畫所提出的入侵偵測系統，可以成功找出目前可能已經成為攻擊目標的名單，更能依其風險值評估預測受害目標，並提供給其他子計畫作為分析。