國防大學中正理工學院

資訊科學研究所

碩士學位論文

用程序方法判斷與整合入侵偵測系統之關聯警示

研究生：刁建強

指導教授：蔡輝榮

中華民國九十四年六月廿四日

誌謝

時間過的很快，轉眼間學生生涯即將結束。在這二年當中，我自認為不是一個用功的學生，但是與兩年前的自己比較起來，卻還是有些進步吧！然而學海無涯，當我看的文章越多，就越覺得自己的知識淺薄。而這段時間最大的收穫，應該就是學會一些整理資料的功夫吧！

本論文之所以能夠順利完成，首先感謝恩師蔡輝榮老師細心教誨、耐心指導與督促，使本人不僅能在學識上有所獲益，更能在為人處世及事理分析等各方面更成熟穩健，師恩浩蕩，特於卷首致上最誠摯的謝意！

論文口試期間，幸蒙淡江大學黃仁俊副教授、中國技術學院吳宗禮副教授、本院羅裕群副教授及賴義鵬副教授，鼎力斧正，使論文更完整，衷心感謝。在學習過程中，感謝同期李武雄學長、魏子文學長、余琬瑜學妹、吳怡興學弟及賴泰宏學弟的互相勉勵，加上好友趙怡梅於論文撰寫期間，及碩九十五年班學弟謝富庭、梁世忠在論文口試期間的多方協助，在此一併誌謝。

衷心感謝教養我的母親，使本人能無後顧之憂在課業上專心研究。特別是好友秀慈在人生路途及求學過程中的陪伴與無悔付出，若不是有她的激勵及督促，則這篇論文不會這麼順利的產出。最後謹將這份成果獻給每一位幫助過我的貴人，有你們支持及鼓勵，才能使本論文達臻善臻美。

摘要

隨著網路發展日新月異，上網人數也與日俱增。再加上攻擊工具取得容易，使得入侵他人電腦不再是屬於專業駭客的事情。許多入門駭客(Script Kid)藉由簡易的入侵工具，隨意入侵他人的電腦。因此，要如何在最短的時間之內發現入侵跡象並完成後續處理，變成一件很重要的事情。

目前的入侵偵測系統多使用特徵值來進行入侵事件的判斷。但是有些時候，符合特徵值的封包可能為正常封包，而異常封包卻可能會被入侵偵測系統遺失。本研究透過使用者的行為及事件警示的關聯性進行分析，提出一個以程序為基礎之關聯警示分析器。藉由關聯性的機率模型，建立入侵者行為分析之雛形系統。透過這樣的分析器，能讓入侵事件在還沒有造成更大危害之前，針對入侵行為提出預警，以提醒系統管理者預先進行事件處置。

ABSTRACT

Change with the development of Internet by time, getting to the Internet the number also increases with each passing day. And attacking tools could get easy, make to intrude into the others computer is not the thing that belongs to the professional hacker any more. Many script kid hackers attack the computers by attacking tools simple. To discover the invasion sign and completes following processing within the shortest time turns a very important matter.

Today, the IDS (Intrusion Detection System) usually adopt the pattern to judge intrusion events. However, sometimes the system might treat normal packets as anomaly ones or skip the anomaly packet. This paper presents a approach to detect network intrusion based on the Rule-based IDS. This approach uses associational probability to analyze the alerts of IDS step by step. These alerts are classified into five groups: denial of service, pre-attack probe, protocol signature, suspicious activity, and unauthorized access attempt. To monitor those alerts, the attacks could be detected earlier.

目錄

表目錄

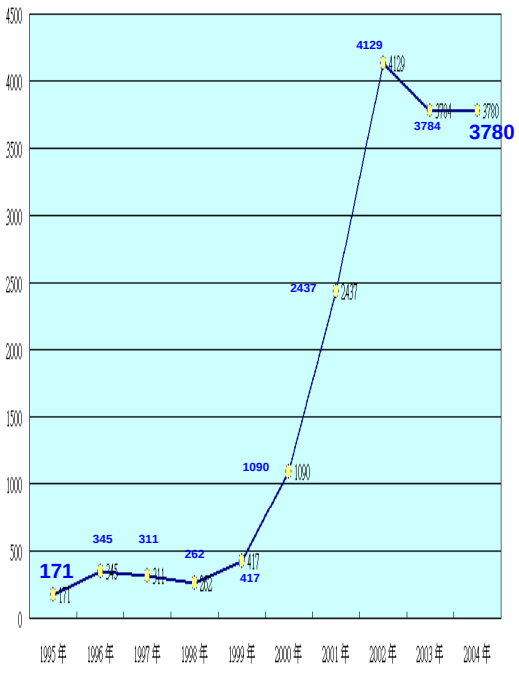
圖目錄

1. 緒論

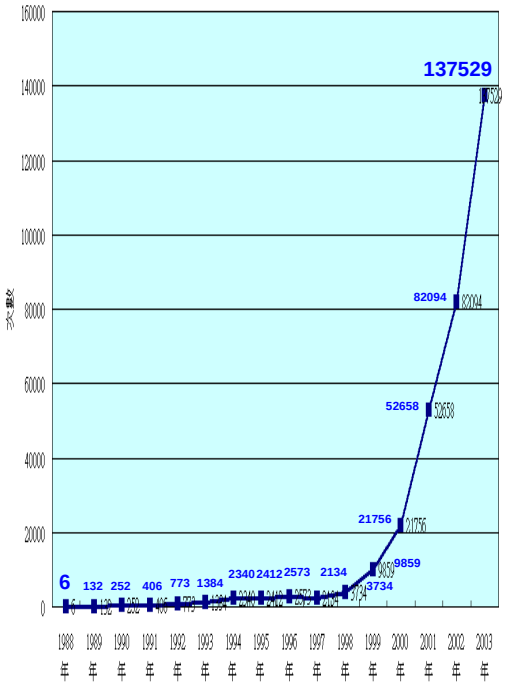
1.1 研究背景

隨著網路發展日新月異，上網人數也與日俱增。再加上攻擊工具取得容易，使得入侵他人電腦不再是屬於專業駭客的事情。許多入門駭客(Script Kid)藉由簡易的入侵工具，隨意入侵他人的電腦。因此，要如何在最短的時間之內發現入侵跡象並完成後續處理，變成一件很重要的事情。

根據美國電腦緊急事件反應小組協調中心(Computer Emergency Response Team / Coordination Center, CERT/CC)的統計(如圖1.1)，從1995年到2003年的短短九年之間，每年發現的弱點由171個攀升到3784個；而所回報的資安事件，也從1988年的6件暴增到2003年的137529件。



1995-2004弱點回報數



1988-2003資安事件回報數

圖1.1　弱點及資安事件回報數量分析圖
錄自 CERT/CC 網頁統計資料[1,2]

同時，在美國電腦緊急事件反應小組協調中心的攻擊趨勢概述(Overview of Attack Trends)[3]一文中，說明了攻擊方式朝向四個方向發展：

(1) 自動化，攻擊工具的速度增快

(2) 入侵工具日趨複雜

(3) 系統漏洞被發現的速度加快

(4) 對於防火牆的滲透能力的增加

因此可以知道，資安事件對於一般使用者的威脅越來越大。而對於網管人員來說，要如何來判斷這是入侵事件或者僅為一般網路活動所造成的誤判，是需要相當的經驗與能力。

依據美國卡內基美隆大學軟體工程學院(CMU/SEI)的分析報告[4]指出，未來入侵偵測系統(Intrusion Detection System, IDS)的架構將朝向具有擴充性(Scalability)的方向發展；入侵偵測系統對於不同來源、不同類型資料的關聯分析能力，與其他入侵偵測系統的合作、互動能力，也愈來愈受到重視。由此可知，入侵偵測系統之整合與關聯分析，將成為降低入侵偵測系統誤報率的趨勢。

過去許多關於入侵偵測系統的研究，都僅針對整體架構與通訊協定等模式來進行探討，對於入侵行為的關聯分析較少著墨。因此本研究希望能找出入侵偵測系統警示的關聯性。透過分析與整合，提出一個與關聯性有關的機率模型。透過這樣的模型，讓管理人員在入侵的損害行為尚未真正開始前，就能提早發覺問題，並作出進一步的處理。

1.2 研究動機與目的

在沒接觸入侵偵測系統前，原本以為入侵偵測系統只要放在網路之中，設定好偵測策略，就能辨識出所有的入侵事件。然而在建置入侵偵測系統時，才發現設置一套入侵偵測系統並不是這麼簡單。首先，由於電腦硬體的限制，不

論是中央處理器(CPU)、隨機存取記憶體(RAM)、硬碟(Hard Disk)、或網路卡……都可能會造成入侵偵測系統遺失封包的狀況。若遺失的是入侵封包，則入侵偵測系統就偵測不到這個攻擊。

其次，偵測策略的嚴謹程度影響偵測率及誤判率(如圖1.2)，若偵測策略寬鬆，就會發生大量的誤報，這樣的狀況稱為誤報(False Positives)；但為了減少誤報，而提高偵測策略的嚴謹度，隨之而來的就是無法偵測到某些入侵行為，而這樣的情況，則是被稱之為漏報(False Negatives)。可是不論誤報或漏報都屬於錯誤警報(False Alarm)。因此，要如何定義合適的偵測策略，是件相當需要經驗的事情。

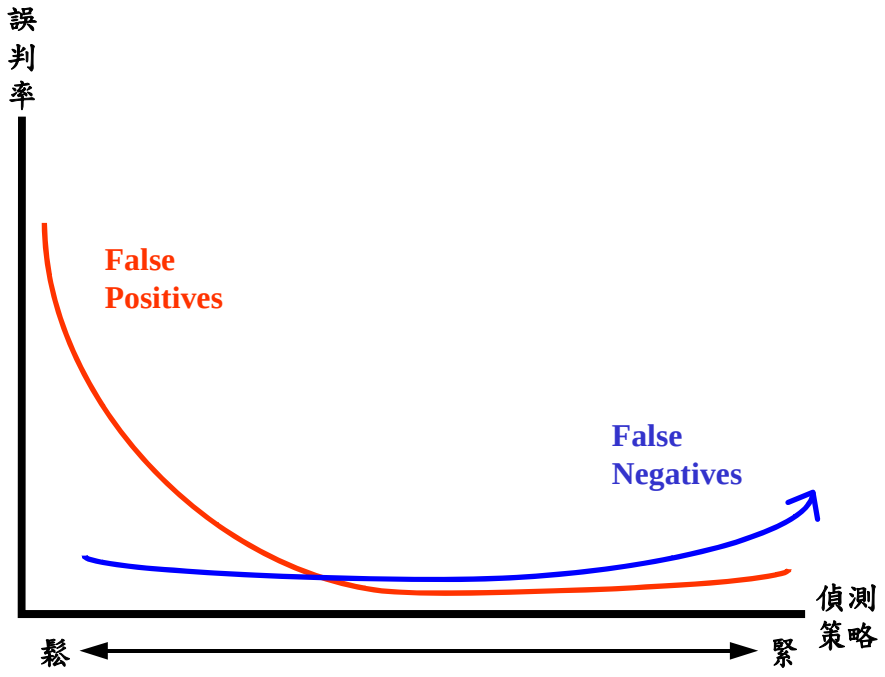


圖1.2　偵測策略與誤判率
錄自Ranum(2003)[5]

由前面所述可以知道，當入侵偵測系統在正式工作之前，必須要有一段調校期。這段時間，快則一、二個月，慢則可能需要近半年的時間。管理人員利

用這段時間，觀察單位網路狀況，並過濾單位網路的錯誤警訊。這樣才能在入侵偵測系統發出警訊時，依照警示來進行緊急應變處理。調校入侵偵測系統之作業流程如 圖 1.3。但是如何判斷是否為錯誤警報，則要依賴管理人員的豐富經驗。若管理人員為新手，無法判斷入侵偵測系統所發出之警訊，何者為真，何者為錯誤警報。安裝入侵偵測系統，不但沒有任何效果，反而是一種累贅。為了解決這樣的狀況，業界推出了入侵偵測系統的委外管理，藉由業界的豐富經驗，代為管理與調校入侵偵測系統。

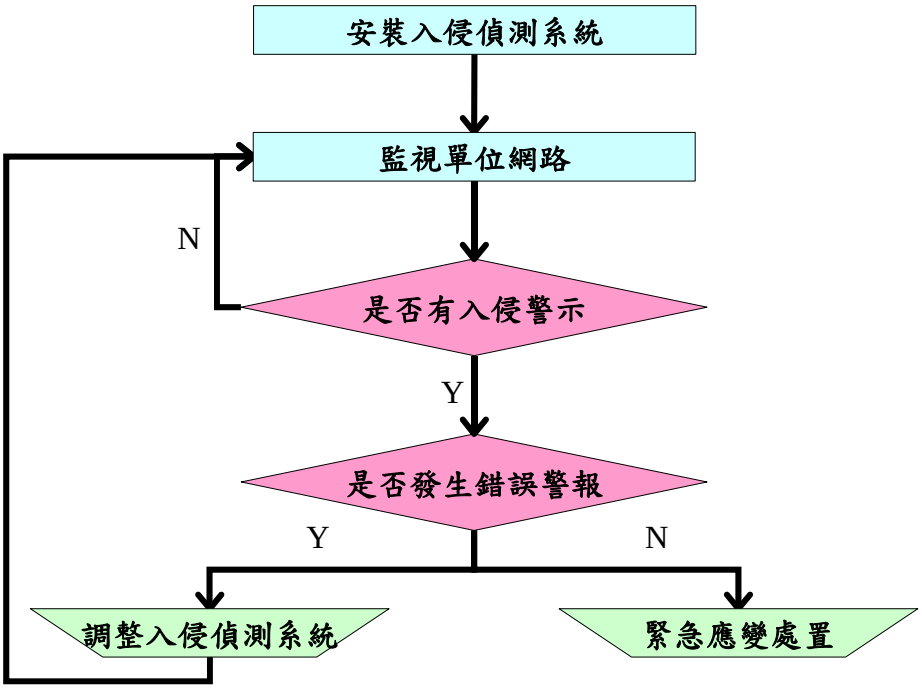


圖1.3　調校入侵偵測系統之作業流程圖

以軍方目前的狀況來看，若將入侵偵測系統委外管理，則是牽涉到二個問題。第一，入侵偵測系統紀錄了單位網路進出的所有封包，將入侵偵測系統委外管理，則單位透過網路進行的各項作業，有洩密的可能性。第二，軍方所使用之網路為封閉網路，將入侵偵測系統委外管理，則勢必要將這個封閉網路連接到網際網路之上，這樣就失去了封閉網路的意義了。隨著精實案、精進案的

進行，國軍人力不斷精簡。讓單位額外找專人來負責入侵偵測系統的可能性也越來越低。若將「調整入侵偵測系統」與「判斷是否有入侵」這兩項工作自動化，對於管理人員來說，可減輕相當多的負擔。

本研究透過使用者的行為及事件警示的關聯性進行分析，提出一個以程序為基礎之關聯警示分析器。藉由關聯性的機率模型，建立入侵者行為分析之雛形系統。透過這樣的分析器，能讓入侵事件在還沒有造成更大危害之前，針對入侵行為提出預警，以提醒系統管理者預先進行事件處置。

2. 文獻探討

2.1 入侵偵測系統的介紹

Guy Bruneau在 The History and Evolution of Intrusion Detection[6]一文中指出：1980年，James P. Anderson發表了一篇專題論文，指出自動化入侵偵測的最初想法是如何使用帳號稽核檔案來偵測未被授權的存取。這篇文章為大型電腦系統的不當使用行為偵測(Misuse Detection)奠定了基礎。從1984到1986年之間，Dorothy Denning與Peter Neumann研究並發展出即時入侵偵測系統(Real-time IDS)的第一個模型。這個原型稱為「入侵偵測專家系統(Intrusion Detection Expert System, IDES)」。它是一個以規則為基礎(Rule-based)的專家系統，可以用來偵測已知的惡意活動。從入侵偵測專家系統(IDES)開始，一直到九〇年代，美國政府提供了大量的資金來資助入侵偵測系統的研究。像是Discovery, Haystack, Multics Intrusion Detection and Alerting System (MIDAS), Network Audit Director and Intrusion Reporter (NADIR)等，這些計畫都是發展來偵測入侵行為，而這些計畫也奠定了現今入侵偵測系統的發展基礎。

美國國家標準與技術學會(National Institute of Standards and Technology, NIST)在2001年11月所發表的報告[7]中，曾針對入侵、入侵偵測與入侵偵測系統有一個明確的定義。當有人嘗試危及電腦資料之機密性、完整性、可用性、或繞過安全機制的行為，被視為「入侵」。而「入侵偵測」是一種程序，用來監控電腦系統或網路上所發生的事件，並利用已知的入侵特徵值來分析它們。至於「入侵偵測系統」則是將上述的程序以軟體或硬體來進行自動處理。入侵偵測系統同時可結合多種資訊安全措施，入侵偵測系統結合防火牆，成為入侵防禦系統(Intrusion Prevention System, IPS)；可以結合Honey pot[8]，用來蒐集駭客的入侵軌跡與分析入侵手法；監控端能分布在各個網路節點，形成分散式入侵

偵測系統。這些整合方案，都是入侵偵測系統的研究方向。然而大家所研究的焦點，更是放在資料的各種分析方法。希望藉由分析方法的改良，讓入侵偵測系統能夠偵測率更高，同時誤報率更低。

2.2 入侵偵測系統的主要型式

目前入侵偵測系統有很多種型式，而這些型式的區分，主要是從監控及分析的方法來看。因此，美國國家標準與技術學會(NIST)將這些方法歸納在一起，建立一個通用的模型，把入侵偵測系統區分為：(1)資料來源(Information Sources)、(2)分析(Analysis)、及(3)回應(Response)等三大功能元件：

(1) 資料來源(Information Sources)：可以區分為網路封包與電腦系統稽核紀錄，因此入侵偵測系統可以區分為網路型入侵偵測系統(Network-based IDS, NIDS)與主機型入侵偵測系統(Host-based IDS, HIDS)。在 The History and Evolution of Intrusion Detection[6]一文中定義了這兩者的不同：

   a. 主機型：資料來自於單一主機，用來偵測主機進出封包中的入侵徵兆。
   b. 網路型：來自於網路的資料依靠資料庫進行詳細的檢查，並標示那些可疑的跡象。所要稽核的資料來自於一台或是多台主機，同樣的用來偵測入侵徵兆。

(2) 分析(Analysis)：可分為不當行為偵測(Misuse Detection)與異常行為偵測(Anomaly Detection)。

   a. 不當行為偵測是指入侵偵測系統認識某些可疑行為，並可搜尋違反指定政策的行為。這也就表示它所尋找的是已知的惡意或不必要的行為。因此，它會先定義出入侵行為的特徵值，再透過比對特徵值來抓出入侵行為。由於它的效能較好，以及錯誤警報率也較低，所以它大多用在商用系統。

b. 異常行為偵測則是指入侵偵測系統所認識的是正常的行為，所以它能從正常行為所建立的基準線，來搜尋異常或越軌的行為。另言之，異常行為偵測是透過某些工具來分析使用者行為，以歸納出正常行為模式。如果使用者不符合這樣的模式，便會被宣告為入侵行為。異常行為偵測最大的問題是它的誤報率很高，但是由於只要有所異常，就會發出警示，所以異常行為偵測具有未知入侵的偵測能力。

(3) 回應(Response)：可分為主動式回應與被動式回應。主動式回應又可分為三種類別：(1)它會蒐集攻擊行為的更多資訊。它藉由攻擊者的入侵紀錄，來調查攻擊者來源並蒐集相關犯罪證據。(2)它改變當時的網路或作業系統之環境。透過改變當時主機或網路的設定，來封鎖攻擊者，藉此終止入侵行為。(3)反擊入侵者。這是一種很冒險的行為，因為入侵來源可能只是攻擊者的跳板。貿然的採取反擊，不但可能會攻擊到無辜的第三者，更有違法的疑慮。而被動式回應，則主要是將相關入侵資訊回應給系統管理者。因此，許多商用系統大多採用這一種方式，像是在螢幕上發出警訊、傳送警訊到行動電話或呼叫器、或透過簡單網路管理通訊協定(Simple Network Management Protocol, SNMP)[9]的方式，將警訊傳給網路管理系統。

2.3 資料分析方法

當入侵偵測系統開始記錄系統事件時，合法的行動與入侵行為的明顯跡象將會在所紀錄的資料中顯露出來。要從大量的紀錄資料中發現系統動作的行為模式，需要一個有效率與聰明的資料分析方法。因此，在這裡討論幾種學習型的分析方法，如資料掘取(Data Mining)分析法[10,11,12]、類神經網路(Neural Network)分析法[13,14]、統計(Statistic)分析法[15]、與貝氏網路(Bayesian Network)分析法[16]等。以便能清楚的分辨出這幾種資料分析方法的適用與限制之處。

2.3.1 資料掘取分析法(Data Mining Analysis)

當稽核機制開始記錄系統事件時，合法的行動與入侵行為的明顯跡象將會在稽核資料中顯露出來。要從大量的稽核資料中發現系統動作的行為模式，需要一個有效率與聰明的資料分析工具。

資料掘取是一個從大量的儲存資料中進行掘取的程序，近年來資料掘取快速發展，讓許多種技術都能使用在資料掘取中。然而，如何來掘取這麼大量的資料呢？目前多用三種方法來進行，(1)分類法(2)關聯性分析(3)時間序列分析。

(1) 分類法：將資料項對映到幾種預先定義的分類之中。這個方法正常輸出的是類別，如：決策樹或規則的形式。在入侵偵測上的理想應用，將需要蒐集足夠正常(Normal)與異常(Anomaly)的使用者或程式的稽核資料，然後利用監督式(Supervised)演算法或非監督式(Unsupervised)演算法來學習類別，就算是新型未見過的稽核資料，也能歸類或預測。也就是在使用資料掘取的入侵偵測中，資料來源能以學習型的演算法來標註或是不被標註。監督式演算法只能用在標註資料，而非監督式演算法則能適用於未標註的資料。

a. 監督式(Supervised)演算法：在監督式演算法的學習過程中，訓練資料在交給演算法進行訓練之前，必須先被標註。圖 2.1顯示使用監督式學習演算法的入侵偵測程序。首先，原始資料必須被分析並被資安專家標註是一般的連線或是攻擊。隨後，學習型的演算法從訓練資料中歸納出規則。最後，分類器使用歸納出的規則來區分新的網路連線。監督式演算法的學習困難點在於標註資料。如果有大量的資料被用來訓練，資安專家在標註資料這一方面的負擔可能會非常艱苦。但若因此而選擇一小部份的訓練資料，其所選擇出的樣本對於學習結果有著決定性的影響。

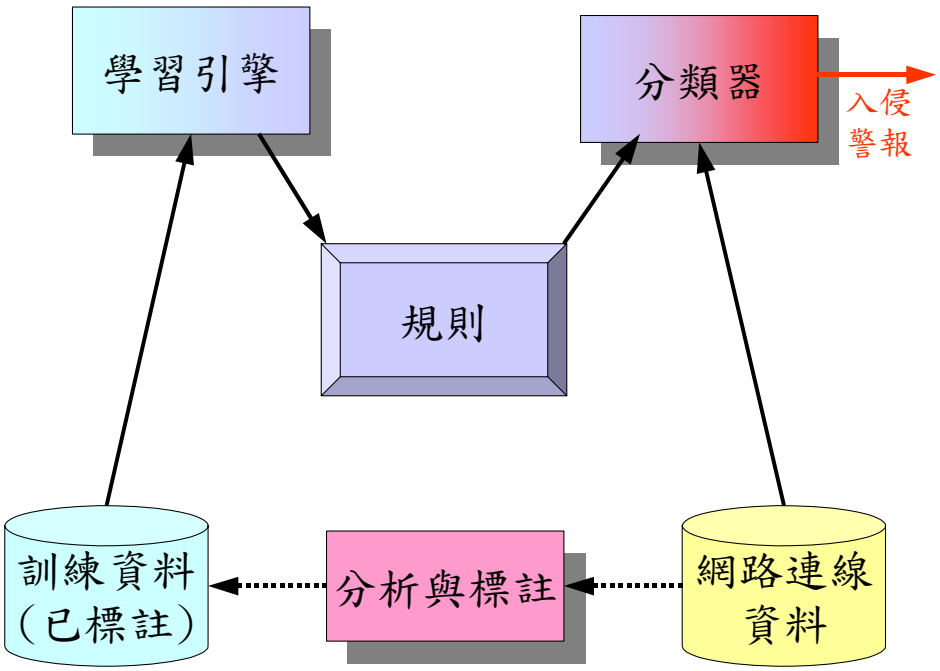


圖2.1　使用標註資料的入侵偵測
錄自 Lei and Ghorbani(2004)[14]

b. 非監督式(Unsupervised)演算法：不像監督式學習演算法只能使用在標註的資料，非監督式學習演算法同時具有學習非標註資料的能力。在 圖 2.2中，說明了偵測程序使用非標註資料。首先，訓練資料被群集式演算法分群起來。其次，群集的權值向量能被標註程序標註起來。各種不同的方法能被應用在這個程序中。有一個方法是標註一個群集中心，從這個任意選的群集中選取一群資料樣本，並以這樣本的主要類型來標註這群集。最後，標註的權值向量就能被用在分類網路連線。

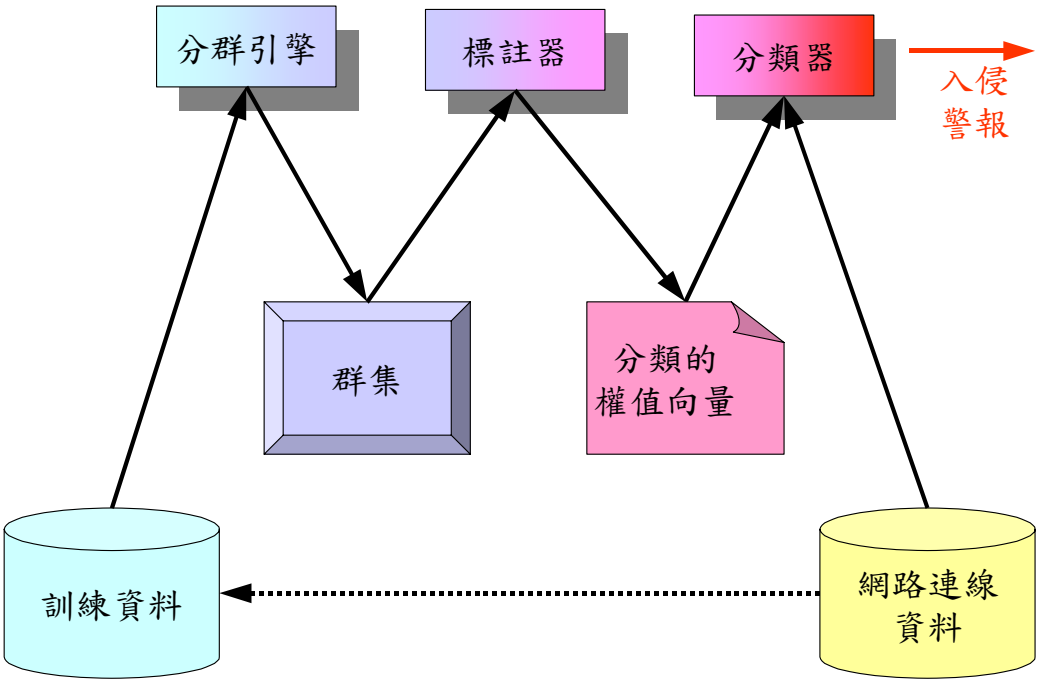


圖2.2　使用未標註資料的入侵偵測
錄自 Lei and Ghorbani(2004)[14]

(2) 關聯性分析：在資料庫記錄中決定兩個領域(field)的關聯性，如：shell的歷史指令中，指令與參數的關聯性。在稽核資料中，系統特徵的關聯性能提供建構正常使用基本資料(Profile)的基礎。有經驗證明，程式執行與使用者行動在系統之中，顯示出頻繁的相關性。如舉例來說，某些特定的程式只能在特殊的目錄存取某些系統檔案，程式設計者時常編輯與編譯c的檔案等，如：程式設計者使用的emacs程式，可能與副檔名為". c"的檔案有很高的關聯性。這些前後一致的行為樣本應該包含在正常使用的基本資料中。掘取聯想規則的目標是從資料庫的資料表中，推導出多重特徵值(或屬性)的相互關係。如 表 2.1，在telnet連線過程期間，從shell輸入的指令。這裡只保持了檔名延伸的部分，移除郵件的本體的內容與檔案，並使用am來代表所有早上的時戳。在分析程式或使用者

行為時，並不是所有聯想都切合實際(如：hostname = pascal → arg1 = tex)。

表2.1　shell的指令紀錄
錄自Lee, Stolfo, and Mok(1999)[11]

time	hostname	command	arg1	arg2
am	pascal	mkdir	dir1	
am	pascal	cd	dir1	
am	pascal	vi	tex	
am	pascal	tex	vi	
am	pascal	mail	fredd	
am	pascal	subject	progress	
am	pascal	vi	tex	
am	pascal	vi	tex	
am	pascal	mail	williamf	
am	pascal	subject	progress	
	……	……	……	……
am	pascal	vi	tex	
am	pascal	latex	tex	
am	pascal	dvips	dvi	-o
	……	……	……	……
am	pascal	logout		

表2.2　網路連線紀錄
錄自Lee, Stolfo, and Mok(1999)[11]

timestamp	duration	service	src_host	dst_host	src_bytes	Dst_bytes	flag	……
1.1	0	http	spoofed_1	victim	0	0	S0	……
1.1	0	http	spoofed_2	victim	0	0	S0	……
1.1	0	http	spoofed_3	victim	0	0	S0	……
1.1	0	http	spoofed_4	victim	0	0	S0	……
1.1	0	http	spoofed_5	victim	0	0	S0	……
1.1	0	http	spoofed_6	victim	0	0	S0	……
1.1	0	http	spoofed_7	victim	0	0	S0	……
……	……	……	……	……	……	……	……	……
10.1	2	ftp	A	B	200	300	SF	……
12.3	1	smtp	B	D	250	300	SF	……
13.4	60	telnet	A	D	200	12100	SF	……
13.7	1	smtp	B	C	200	300	SF	……
15.2	1	http	D	A	200	0	REJ	……
……	……	……	……	……	……	……	……	……

(3) 序列分析：這演算法能發現同時不斷發生的稽核事件的時間序列，這樣的事件樣本提供了一種基準線，它納入了時間統計測量值放在入侵偵測模型當中。與關聯性分析所不同的是，這裡增加了時間的因素進去。如表 2.2的網路連線紀錄，這些從一般網路分析效果得到的固有特徵，對入侵偵測來說並不特別。但是它所能呈現的是SYN Flood的攻擊紀錄。這攻擊者使用許多偽造的來源位址，在非常短的時間之中進行連線。例如：在所有時戳(Timestamp) 1.1 時，傳送許多S0 連線(只傳送第一個SYN封包) 給受害主機的http服務。

透過分類、關聯性分析、及序列分析，可以構成一個入侵偵測的支援環境。這個支援環境使得系統建立者能以互動與反覆的方式，來驅使建構與評估偵測模型的程序啟動。最後的產物是能偵測入侵行為的一種規則。用這樣的方法可以將學習到的規則，取代人工編碼的入侵樣本與基本資料(Profile)，及從統計樣本所選定的系統特徵與測量值。

2.3.2 類神經網路分析法(Neural Network Analysis)

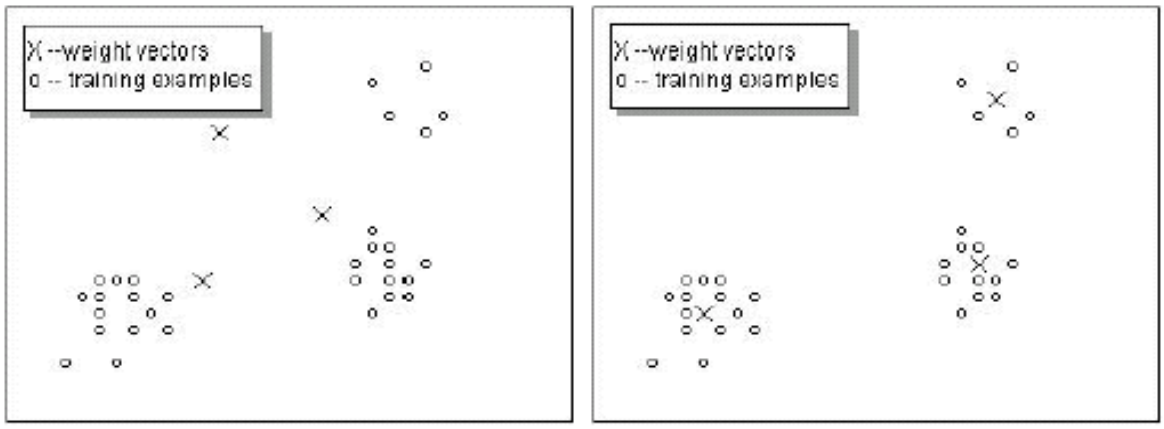
這是一種具有學習能力的演算法，大多使用於異常行為。若經由適當的訓練，可具有偵知未知行為入侵的能力。首先，它會針對一般正常的作業蒐集資料，而這樣的資料會成為類神經網路的輸入值。透過大量的資料來訓練類神經網路，可以把網路當中各個神經元間的連接調整為不同的權值，而構成一個只認識正常行為的類神經網路模型。透過這樣的模型，可以辨識出不當使用行為與異常行為，甚至於還可以用此種方法可辨識出未知攻擊。因為發生未知攻擊行為時，它的特徵是不同於正常行為模型。

以標準競爭學習網路(Standard Competitive Learning Network, SCLN)為例[14]，它是一種單層的類神經網路，每一個輸出神經元都完整的連接到輸入節

點。在標準競爭學習網路中，類神經網路的輸出神經元因為競爭狀態而變的活躍。當訓練樣本(Training Sample)被提交到網路時，輸出神經元會與它們相互競爭。如果某個神經元贏得這個競爭，權值向量(Weight Vector)將會被更新。

$$\omega_j(n+1) = \omega_j(n) + \eta(n)(x - \omega_j(n)) \tag{2.1}$$

η 是學習率，w_j是勝利神經元j的權值向量(Weight Vector)。



(a)起始的權值向量　　(b)分群後的結果

圖2.3　標準競爭學習網路的原理
錄自Lei and Ghorbani(2004)[14]

根據標準競爭學習網路的規則，權值(Weight)更新是依照公式(2.1)的更新規則來計算。網路起始於一些隨機選的神經元。起始的神經元學習藉由移轉它們的突觸權值朝向輸入節點而去。在訓練之後，每一個輸出神經元應該透過讓它自己的突觸權值向量朝向那個群集的中心移動，藉以描繪出一群輸入資料集。這程序顯示出標準競爭學習網路有執行分群的能力。然而，標準競爭學習網路的效能嚴重依賴起始的權值向量，以及輸出神經元的數量。一旦輸出神經元的數量設定之後，群集的數量也就不會顧慮到資料的分布。從另一方面來看，不同起始權值向量可能引導出不同的最後群集，因為透過公式(2.1)，只能讓獲勝神

經元的權值朝向附近的樣本移動。因此，標準競爭學習網路的關鍵缺點就是它可能會把一個群集分割變成幾個小群集。如圖2.3，兩個神經元起始於一個群集。雖然預期只有三個群集，但標準競爭學習網路的分群結果將會產生出四個群集。

2.3.3 統計分析法(Statistic Analysis)

統計分析法有兩種分析方式，一種是先監控並紀錄網路活動狀況，並透過統計的方法把網路活動狀況進行量化，建立網路活動模型。如果網路狀況與所建立的網路活動模型有所不同時，就對這樣的異常行為發出警訊。另一種方式，是假定不正常的網路行為將觸發異常的網路流量，若量測到這樣的異常流量特徵，則當成是惡意或是可疑行為的徵兆。透過比較現有流量狀況與所提出的特徵樣本，就可以偵測入侵的行為了。舉例來說，若設定網路活動模型來監控網路流量的值，透過接收端操作特性曲線(Receiver Operating Characteristic, ROC)來歸納流量活動，以正常連線及攻擊連線的差異來量化網路活動模型的效能。

定義：目的端的連線數量

$X_N^T(k)$：在$kT \sim (k+1)T$的時間間隔中，正常連線的起始數目。

$X_A^T(k)$：在$kT \sim (k+1)T$的時間間隔中，攻擊連線的起始數目。

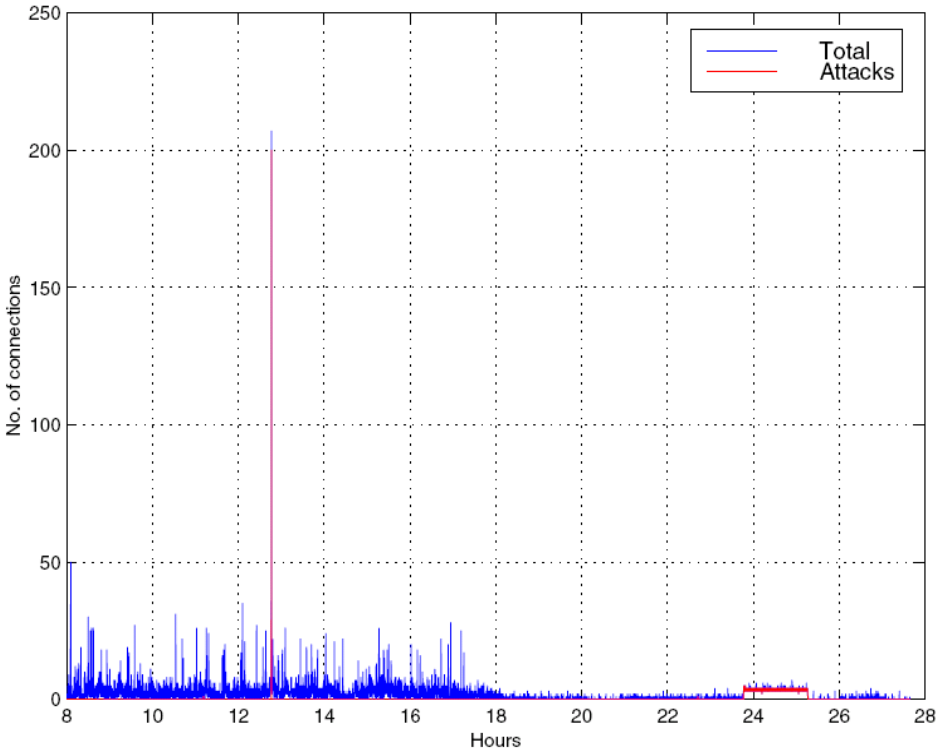
$X_C^T(k)$：在$kT \sim (k+1)T$的時間間隔中，所有連線的起始數目。

簡單的來說，$X_C^T(k) = X_N^T(k) + X_A^T(k)$。圖2.4描繪了$X_C^T(k)$與$X_A^T(k)$在取樣時，四種不同時間比例的演變。

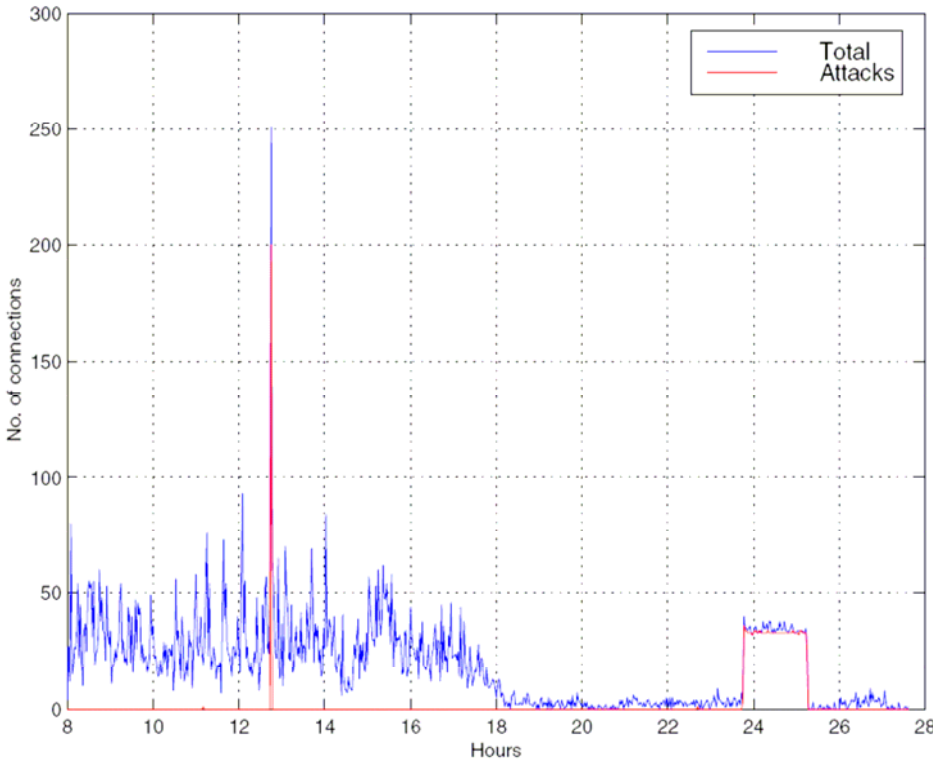
(1) 在T = 12:46:20，有一個阻絕服務(Denial of Service, DoS)攻擊-Teardrop，在10秒及100秒的時間比例中，能清楚的被觀察出來。而在1000秒及3600秒的時間比例中，會由於自然增加的網路活動而被誤認。Teardrop攻擊是傳送大量錯誤的ICMP封包碎片給主機。在這個例子中，在2秒內傳送超過200個封包(或ICMP連線)。

(2) 在T = 22:42:37，有一個使用者提昇權限(User to Root, U2R)攻擊-Eject。這個攻擊在任何時間比例都不會引人注目。因為它是影響單一的telent連線，這表示需要不同技術才能偵測這樣的攻擊。

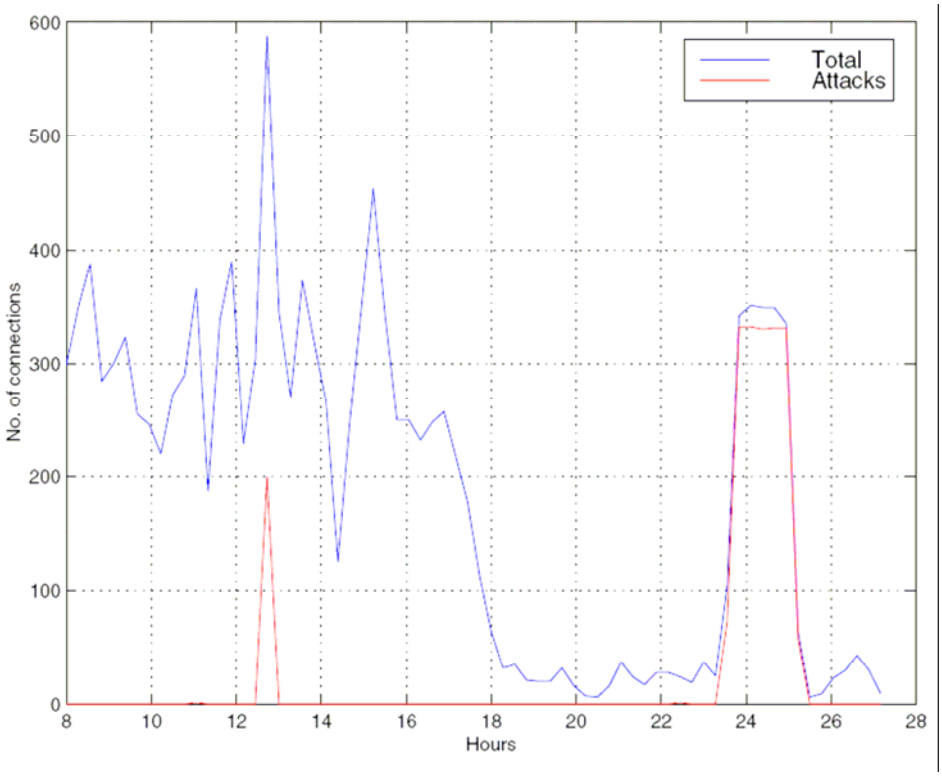
(3) 在T = 23:46:35，有一個偵測(Probe)攻擊-Ipsweep。這個攻擊在任何時間比例都很明顯，特別是100、1000、及3600秒的區間。Ipsweep攻擊是單一來源傳送許多ICMP的封包給網路上不同的機器。在這個狀況中，最後一個封包是在T = 1:16:19被傳送，所以我們可以知道這個攻擊持續了一個半小時。



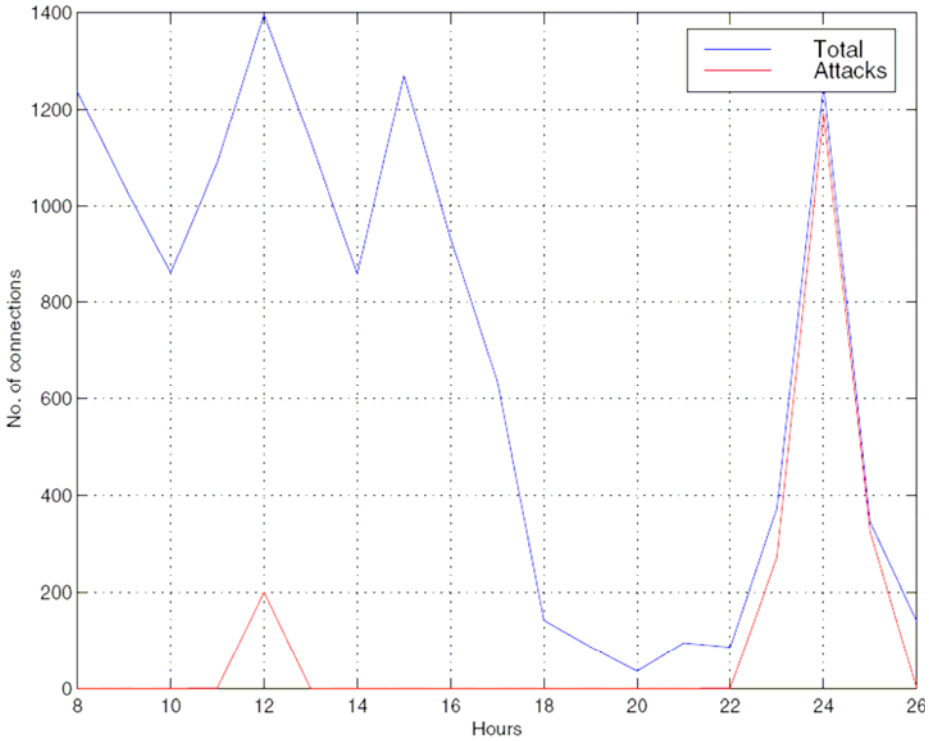
(a) T=10秒



(b) T=100秒



(c) T=1000秒



(d) T = 3600秒

圖2.4　1998年DARPA資料集(第五週星期三)：不同時間比例之連線數量圖
錄自Caberera, Ravichandran, Mehra, and Woburn(2000)[15]

在接收端操作特性曲線(ROC)圖中，阻絕服務(DoS)與偵測(Probe)攻擊會呈現出突然爆發的模式，但是卻不會增加相同的幅度，因此具有很難統計的特點。而使用者提升權限(U2R)攻擊，則會呈現在單獨的連線當中。若將一定的時間內所能觀察到的連線數量，設定為一個門檻值，這樣只要在相同的時間比例中，發現連線數超過門檻值就可以推論出攻擊的存在了。

2.3.4 貝氏網路分析法(Bayesian Network Analysis)

這是一個利用關聯性的機率概念所延伸出來的一種學習演算法，大多也是用於不當行為偵測。首先，它將各個特徵發生的機率值建立起來，再根據彼此的關係計算出它們之間的條件機率，建立出完整的貝氏網路架構。這樣的分析法，關鍵點在於要如何建立特徵的機率狀態分佈，如果使用的特徵無法由機率

方式表現，則此種方法無效。同時還可以利用許多已知條件去推測各種可能發生的事件及其條件機率，因此貝氏網路也有預測未知事件發生的能力。

舉例來說，有個農民有一瓶牛奶，它可能是被污染或無污染的。他能夠以一個準確率很高的測試來判定牛奶是否污染(如：測試的結果是確定的或否定的) 。這個情況能夠用兩個隨機的布林代數變數來表示，污染和陽性反應。當牛奶實際上被污染時，污染的變數為是，否則為否。當測試宣稱牛奶被污染時，陽性反應的變數為是，若為否，則為陰性反應。注意測試可能會是陽性反應，但牛奶卻沒有污染，而反之亦然。

可以利用貝氏網路將這個狀況作成一種模式，如圖2.5中之呈現。兩個隨機變數代表網路中的兩個節點。假設農民知道陽性反應變數的條件機率表，也就是測驗出為陽性反應，而牛奶為污染或無污染的機率。他知道污染變數的條件機率表，那說明了瓶子含有污染牛奶的機率。從污染到陽性反應節點的箭頭，在這兩個變數之間，指示出一個因果關係。在這種情況下, 我們期望測驗的結果取決於牛奶的真實狀態(污染或未污染)。這些變數沒有繼承其他直接影響它們的變數。

若是以單純貝氏網路為例，它是一個受限制的網路，只有二個階層，並且假設在資訊節點之間完全獨立。(換言之，隨機變數能夠被觀察及測量)。這些限制因素導出一個單一前提節點(根節點)的樹狀網路，它的箭頭指出一些資訊節點(子節點)。所有子節點完全只有一個父節點(也就是根節點)，並且許可的節點之間沒有其他的因果關係。在圖2.6，單純貝氏網路被用來執行網路事件的入侵偵測。不幸的是，單純貝氏網路的分類能力與以門檻值為準的系統相似，後者是計算從子節點獲得的輸出總和。這是由於所有模組(子節點)是獨立操作的，並且只有影響到根節點的機率值。這個在根節點的單一機率值以傳統的方法能夠以門檻值來描述。

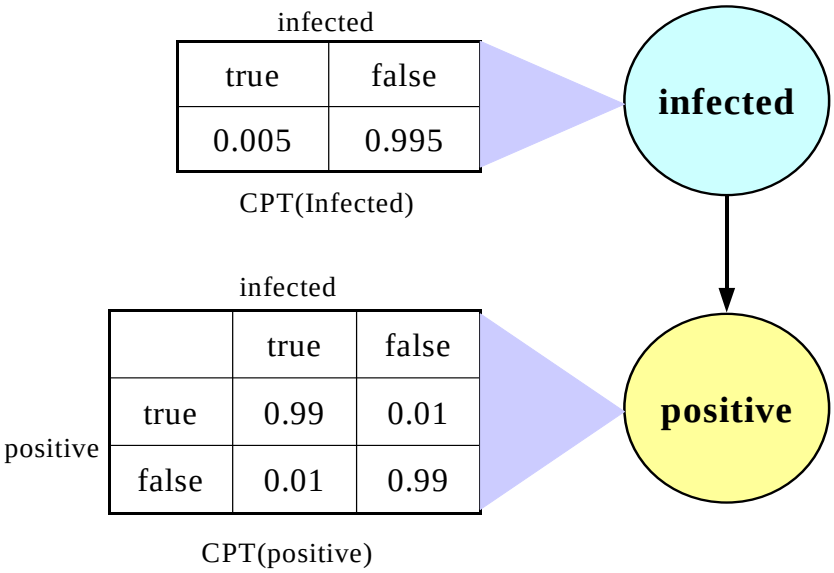


圖2.5　污染牛奶的貝氏網路與條件機率表(CPT)
錄自Kruegel, Mutz, Robertson, and Valeur(2003)[16]

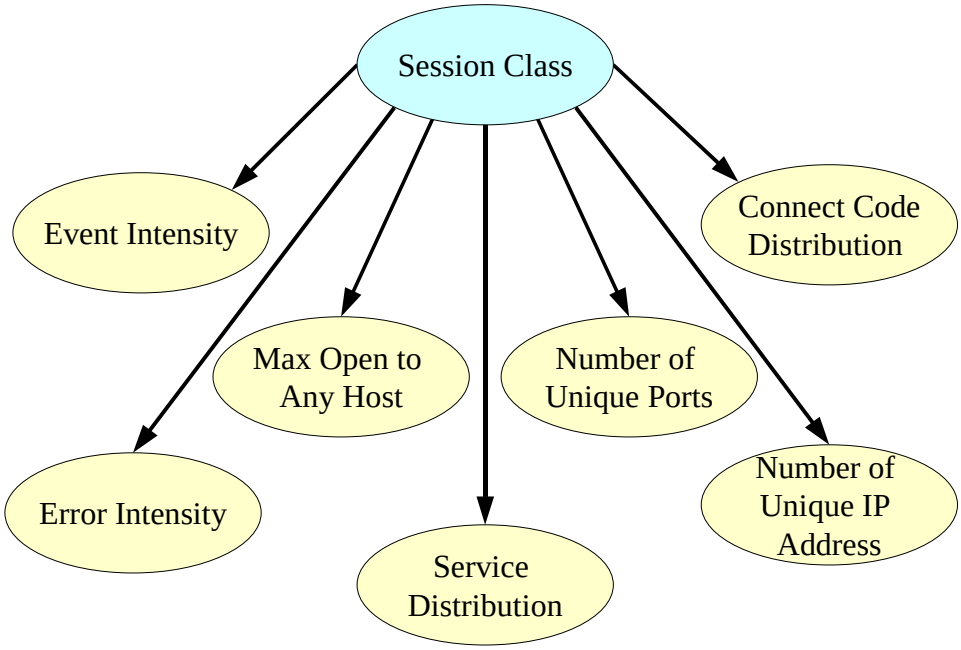


圖2.6　單純貝氏網路
錄自Kruegel, Mutz, Robertson, and Valeur(2003)[16]

3. 研究方法

3.1 程序方法

本研究所指之程序，係指「將某個事物拆解為多個步驟，每一個步驟彼此具有先後時間性或關聯性。」從整個流程來看，從入侵事件→入侵偵測→事件警示，這一連串的動作就可以視為是一種程序。也就是入侵事件的各個動作，被入侵偵測系統蒐集之後，由入侵偵測系統依據程序來對網管人員做出警示。

因此，本研究從入侵偵測的過程、入侵事件的動作、以及所產生的警示相互之關聯性，來討論這三者之間如何以程序來構成。

3.1.1 入侵偵測的程序

美國國家標準與技術學會(NIST)將入侵偵測系統拆解成三大模組：(1)資料來源模組、(2)資料分析模組及(3)回應模組。因此，可以了解入侵偵測的程序如圖3.1所示：

首先，資料蒐集模組將網路上的封包或主機的稽核紀錄讀入，並將資料進行預先處理；而後資料分析模組將所讀入的資料進行分析，如果判斷是入侵行為，則交由系統回應模組作出回應；如果不是，則返回資料蒐集模組繼續蒐集資料。其中，資料蒐集模組的資料正確率取決於電腦硬體與蒐集資料的策略。假如，電腦硬體的處理資料速度跟不上擷取資料的速度，就可能會造成入侵偵測系統遺失封包。若又正好遺失入侵封包，那麼入侵偵測系統就抓不到這樣的攻擊。其次，偵測策略的嚴謹程度，則會影響偵測率及誤判率，當偵測策略越寬鬆時，會發生大量的誤報(False Positives)；但是若為了減少誤報，而提高偵測策略的嚴謹度，隨之而來的就是會有一些入侵行為是漏報(False Negatives)。

系統回應模組則依照資料分析模組所判斷的緊急程度，以及系統管理者所

定義的方式，給予入侵事件不同的回應。因此，若資料分析模組所分析的結果是準確的，則系統回應模組就會給予正確的回應；反之，則會獲得錯誤的回應。由上述情況可知，在相同的硬體及網路環境下，要提升偵測率並降低誤報率，最重要的在於資料分析模組。而本研究則是針對市面所使用之入侵偵測系統(ISS的RealSecure)所產生的入侵警示進行再分析。另言之，在比對所偵測的封包產生警示之後，將警示整合與分析，藉以提早預警可疑的入侵事件。

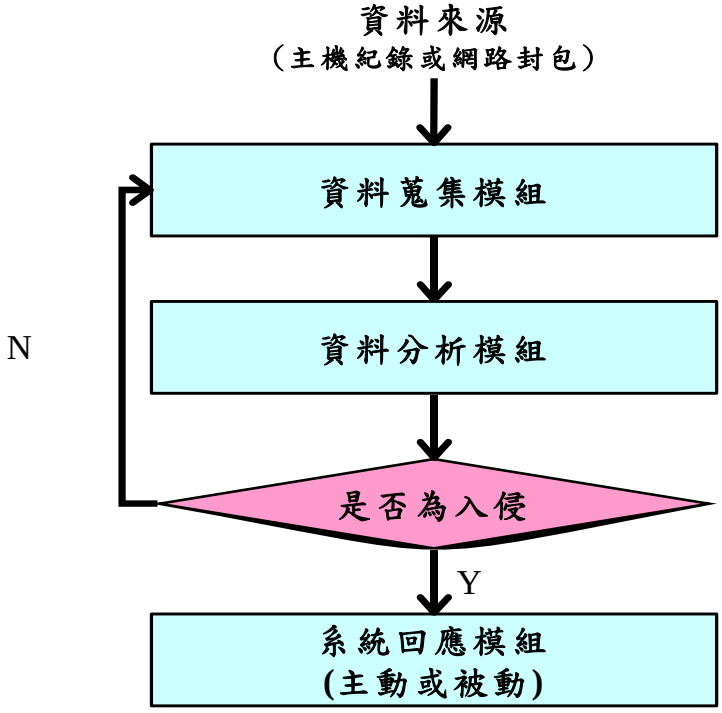


圖3.1　入侵偵測程序圖

3.1.2 入侵事件(Event)的程序

美國電腦緊急事件反應小組協調中心在2003年五月於事件與弱點趨勢概說(CERT/CC Overview- Incident and Vulnerability Trends)[17]當中，提出典型的網路攻擊程序(圖3.2)。攻擊者為了找出受害主機的服務、弱點，會對受害主機進行探測，以嘗試獲取使用者的存取權限或特殊權限(系統或網路管理者的權限)。當攻

擊者取得管理員的權限之後，便會設法隱藏自己的蹤跡，在遠端電腦中安裝後門，以便下次可輕易進入系統。當獲得管理員權限後，攻擊者可能就會攻擊其他主機、取得或改變資訊、或者進行其他未經授權的動作。

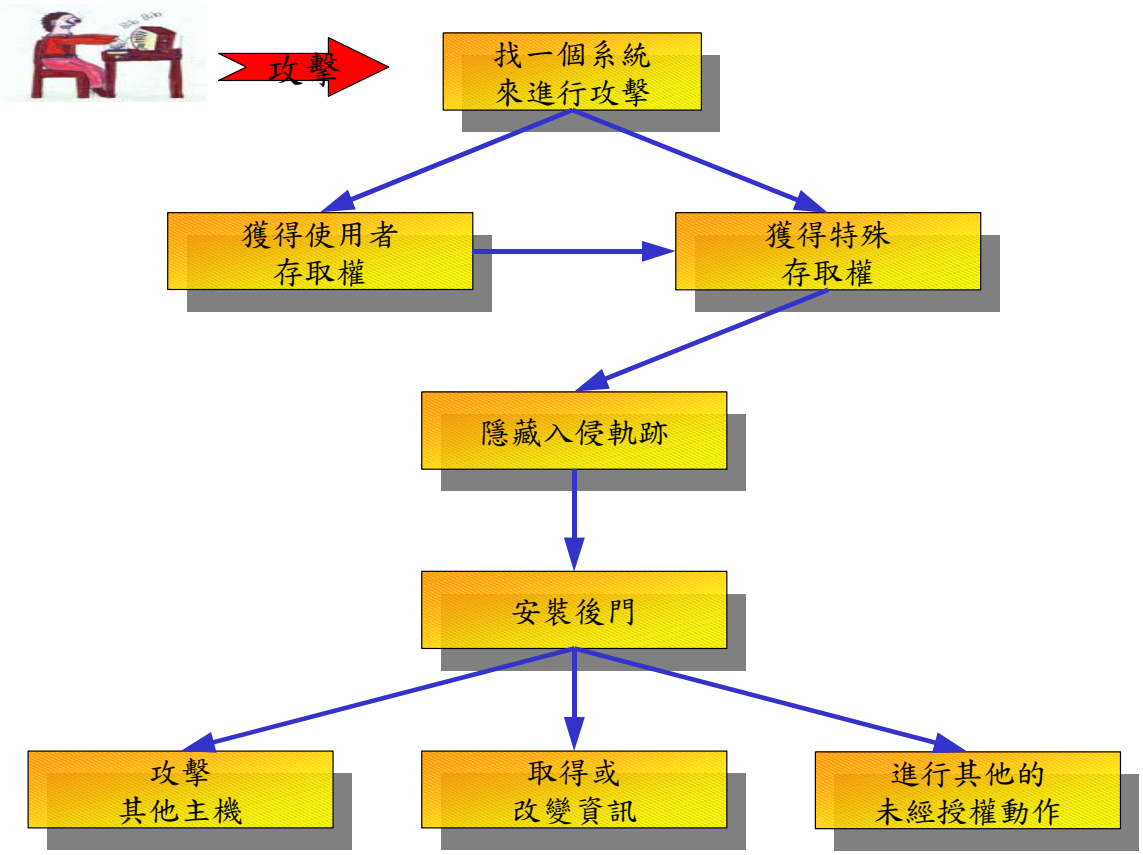


圖3.2　典型的網路攻擊程序圖
錄自CERT/CC [17]

入侵事件雖然非常多樣化，但是歸納起來，可以大致分為四種攻擊方式[11,15]：(1)監視/探測(Surveillance/Probing)、(2)阻絕服務(Denial of Service, DoS)、(3)使用者非法提升權限(User to Root, U2R)及(4)遠端控制(Remote to Local, R2L)。而典型的網路攻擊程序圖可以依照這樣的分類成為網路攻擊程序關聯圖(如圖3.3)。

(1)監視/探測(Surveillance/Probing, Probe)：通常是攻擊者在發動攻擊的前置

作業，他們對受害的主機發出偵測封包，透過所得到的回應封包，了解受害主機作業系統或其他軟體的弱點等。像是通訊埠掃描(Port Scan)、弱點掃描等攻擊方式。

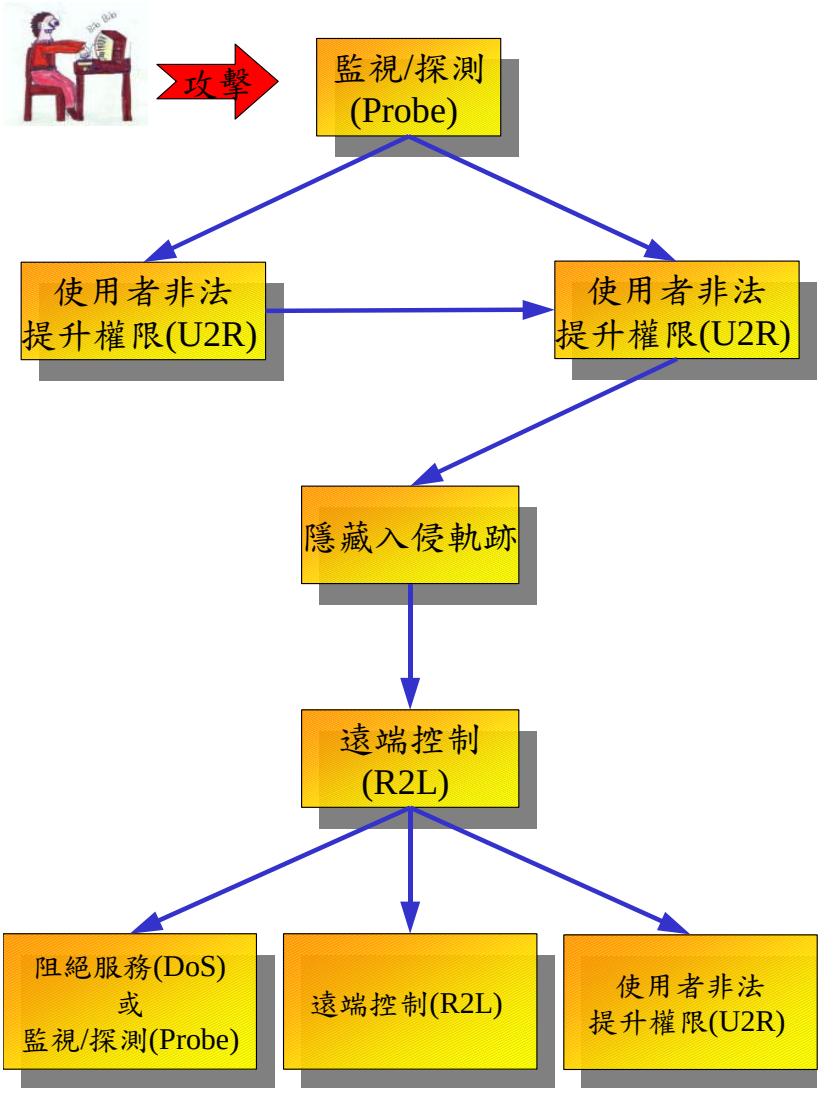


圖3.3　網路攻擊程序關係圖

(2) 阻絕服務(Denial of Service, DoS)：攻擊者利用本身的機器或經由操控其他大量存有攻擊程式的跳板主機發動攻擊(DDoS)，使得受害主機的中央處理器(CPU)、記憶體等資源耗盡讓服務無法正常運作。像是SYN封包的洪水攻擊(SYN Flood)[18]、Ping封包的洪水攻擊(Ping of Death)[19]、

Teardrop、或Smurf等攻擊方式。

(3) 使用者非法提升權限(User to Root, U2R)：攻擊者經由正常管道或其他方式取得帳號密碼，在取得一般使用者權限之後，再透過系統中某些軟體的弱點(如：緩衝區溢位)，藉以取得系統管理者權限。

(4) 遠端控制(Remote to Local, R2L)：攻擊者無須在受害主機上有任何的帳號，只需透過發送封包至受害主機即有可能達到取得敏感資料或對主機造成破壞，也可利用受害主機在網路提供的服務程式進行攻擊。如：微軟IIS的Unicode漏洞。

對於入侵偵測系統而言，不同的攻擊程序會產生不同的事件警示。舉例而言，若將上述的四種攻擊程序對應於Internet Security System(ISS)公司的RealSecure，可以把事件警示區分為五種群組(詳如附錄壹)：包括了阻絕服務(Denial of Service)、預備攻擊前的偵測(Pre-Attack Probe)、通訊協定的特徵(Protocol Signature)、可疑的動作(Suspicious Activity)、以及未經授權的存取(Unauthorized Access Attempt)。若將這樣的分類群組，套用在典型的攻擊程序中，可得到入侵事件警示關係圖(如圖3.4)。

(1) 阻絕服務(Denial of Service)：這個攻擊通常是由於受害者的關鍵性資源超過負載，導致它所提供的服務部分或全部停止。舉例來說：阻絕服務攻擊包含了SYN封包的洪水攻擊(SYN Flood)[18]、Ping封包的洪水攻擊(Ping of Death)[19]、及Windows Out of Band data (Win-oob)[20] 等攻擊。

(2) 預備攻擊前的偵測(Pre-Attack Probe)：這個攻擊是用來蒐集網路相關資訊(如使用者名稱、密碼)，以便後續用在未經授權的存取行為上。像是SATAN的掃描動作(SATAN scan)[21]、通訊埠的掃描(IP port scan)[22]、及TCP half 掃描(TCP half scan)[23]。

(3) 通訊協定的特徵(Protocol Signature)：透過被解碼的通訊協定資訊來指示

出不受歡迎的動作，藉以幫助管理員發現可能的危險事件。如FTP User[24]及Portmapper Proxy解碼[25]等。

(4) 可疑的動作(Suspicious Activity)：不是正常的網路連線，很可能是需要注意的不安全事件。像是IP位址的重複使用(Duplicate IP Address)[26]、以及無法識別IP 協定的事件(IP Unknown Protocol)[27]。

(5) 未經授權的存取(Unauthorized Access Attempt)：攻擊者試圖讀、寫、或執行被保護的檔案，也包含了嘗試得到被保護的存取權限。如：FTP root[28]及Sendmail wizard(WIZ)攻擊[29]。

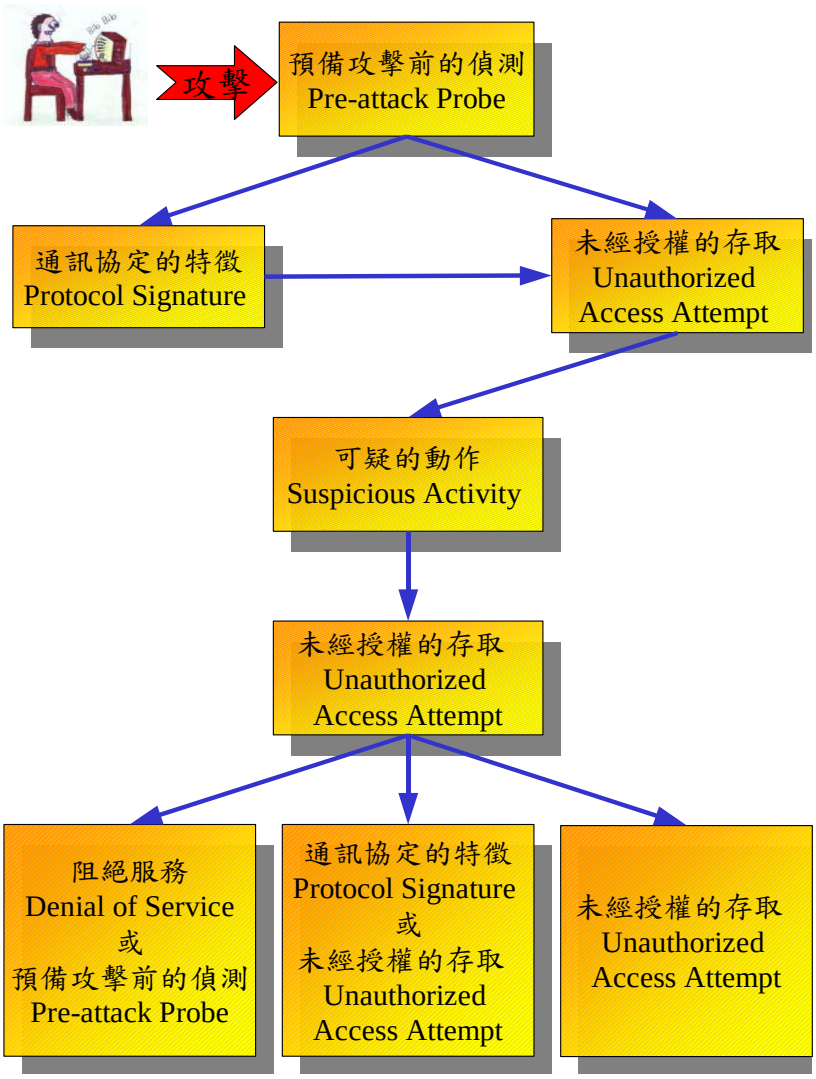


圖3.4　入侵事件警示關係圖

這五種事件警示群組可分為三大類。第一類，探測性質的事件，對系統無明顯影響或破壞的行為，如「預備攻擊前的偵測(Pre-Attack Probe)」及「通訊協定的特徵(Protocol Signature)」；第二類，可能是入侵事件，需要管理人員密切注意，如「可疑的動作(Suspicious Activity)」；第三類，屬於入侵或攻擊事件，對於系統有某種程度的影響，如「未經授權的存取(Unauthorized Access Attempt)」及「阻絕服務(Denial of Service)」。

而這裡所指的「阻絕服務」及「預備攻擊前的偵測」這二個群組，與之前討論的「阻絕服務(Denial of Service)」及「監視/探測(Surveillance/Probing)」具有相同的意義；但是後三者群組裡面，則混合包含了「遠端控制(Remote to Local)」、「使用者非法提升權限(User to Root)」這二類攻擊。以IE Cookie Local Zone[30]這個事件警示為例，它屬於「遠端控制(Remote to Local)」的攻擊事件，但若依照RealSecure的分類，卻是「未經授權的存取(Unauthorized Access Attempt)」的攻擊。因此為求分類清楚而明確，本研究依照入侵偵測系統自身的分類，以避免過多的人為干涉。

從入侵事件警示關係圖當中，可以發現攻擊總是會先進行探測的動作，而這樣的動作，會以「攻擊前的偵測」呈現出來。最重要的原因，在於攻擊者要針對受害主機的服務、弱點、並依照自身的目的，挑選適當的攻擊手法。所以當入侵偵測系統在發現有來源位址開始進行探測的動作時，就應該開始監控那一個位址，並在適當的時候提醒系統管理者注意。如果要等到入侵行為真正對受害主機有所危害時，在緊急應變處理上就會有些緩不濟急。

3.1.3 關聯警示的分析程序

判斷發生之警示是否為入侵事件，可以從以下三點來看：

(1) 同一來源端是否發出過多的掃描封包：通常正常的網路通聯，來源端很

少會發出針對整個網域的探索封包。舉例來說，某單位的網段是x.168.0.0，若看到有個來源IP對於x.168.0.0發出攻擊前的偵測封包，這表示那個IP在對這個網段進行某種行為。無論是有意或無意，這樣的舉動是一種異常行為。

(2) 從目的端來看，如果發現有不屬於這個網段的封包，卻出現在這個網段裡，這也是一種異常狀況。像是在x.168.0.0的網段之中，發現有某個IP傳送封包到x.143.0.0的網段。

(3) 分析事件的因果關係：每一個事件都有形成的前因(Precondition)與後果(Consequences)。依照這兩個特性來分析，並透過關聯性的機率將事件的關連性建立起來。如表3.1，x.131.51.111從10/12 07:14～10/14 00:58這段時間之間，先對x.142.0.0網段進行攻擊前的偵測攻擊，會造成一個SMB_Service_Sweep的事件警示，隨後在10/14 02:02時，先後發生MSRPC_LSASS_Request_Detected (通訊協定的特徵)及MSRPC_LSASS_Bo (未經授權的存取)等事件警示。

表3.1 x.131.51.111的入侵紀錄表

日期/時間	來源位址	目標位址	事件名稱	威脅程度	類別
2004/10/12 7:14	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 8:10	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 10:04	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 11:00	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 11:52	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 13:07	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 13:47	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 14:50	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 15:58	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 17:00	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 17:58	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/12 19:18	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe

2004/10/13 0:16	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 1:40	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 3:10	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 3:39	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 4:28	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 5:20	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 6:06	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 6:44	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 7:51	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 9:06	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 11:49	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 13:10	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 16:01	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 18:08	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 21:11	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/13 23:01	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/14 0:58	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/14 2:02	×.131.51.111	×.142.78.10	MSRPC_LSASS_Request_Detected	3	Protocol Signature
2004/10/14 2:02	×.131.51.111	×.142.78.10	MSRPC_LSASS_Bo	1	Unauthorized Access Attempt
2004/10/14 2:02	×.131.51.111	×.142.78.10	MSRPC_LSASS_Request_Detected	3	Protocol Signature
2004/10/14 2:02	×.131.51.111	×.142.78.10	MSRPC_LSASS_Bo	1	Unauthorized Access Attempt
2004/10/14 3:57	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/14 6:30	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/14 9:00	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe
2004/10/14 10:36	×.131.51.111	×.142.0.0	SMB_Service_Sweep	3	Pre-attack Probe

從圖3.4的入侵事件警示關係圖中，假設從起始狀態(Init)可能會進入五種事件警示群組，「預備攻擊前的偵測(Pre-Attack Probe)」、「通訊協定的特徵(Protocol Signature)」、「可疑的動作(Suspicious Activity)」、「未經授權的存取(Unauthorized Access Attempt)」及「阻絕服務(Denial of Service)」，而這五種事件群組分別依序以X_1、X_2、X_3、X_4及X_5代表。並且同時以五個位元來紀錄狀態，從右向左分別為，第一個位元代表X_1、第二個位元代表X_2、第三個位元代表X_3、第四個位元

代表X_4、及第五個位元代表X_5。其中1代表具有這樣的事件狀態；0代表沒有這樣的事件狀態；而X則代表Both，也就是0與1都有可能性。可以推論得出入侵事件狀態樹狀圖，如圖3.5。舉例來說，從起始狀態(Init)進入「預備攻擊前的偵測(Pre-Attack Probe)」事件警示群組，其狀態表示方式為"XXXX1"，若繼續進入「通訊協定的特徵(Protocol Signature)」群組，則狀態表示方式變成"XXX11"。

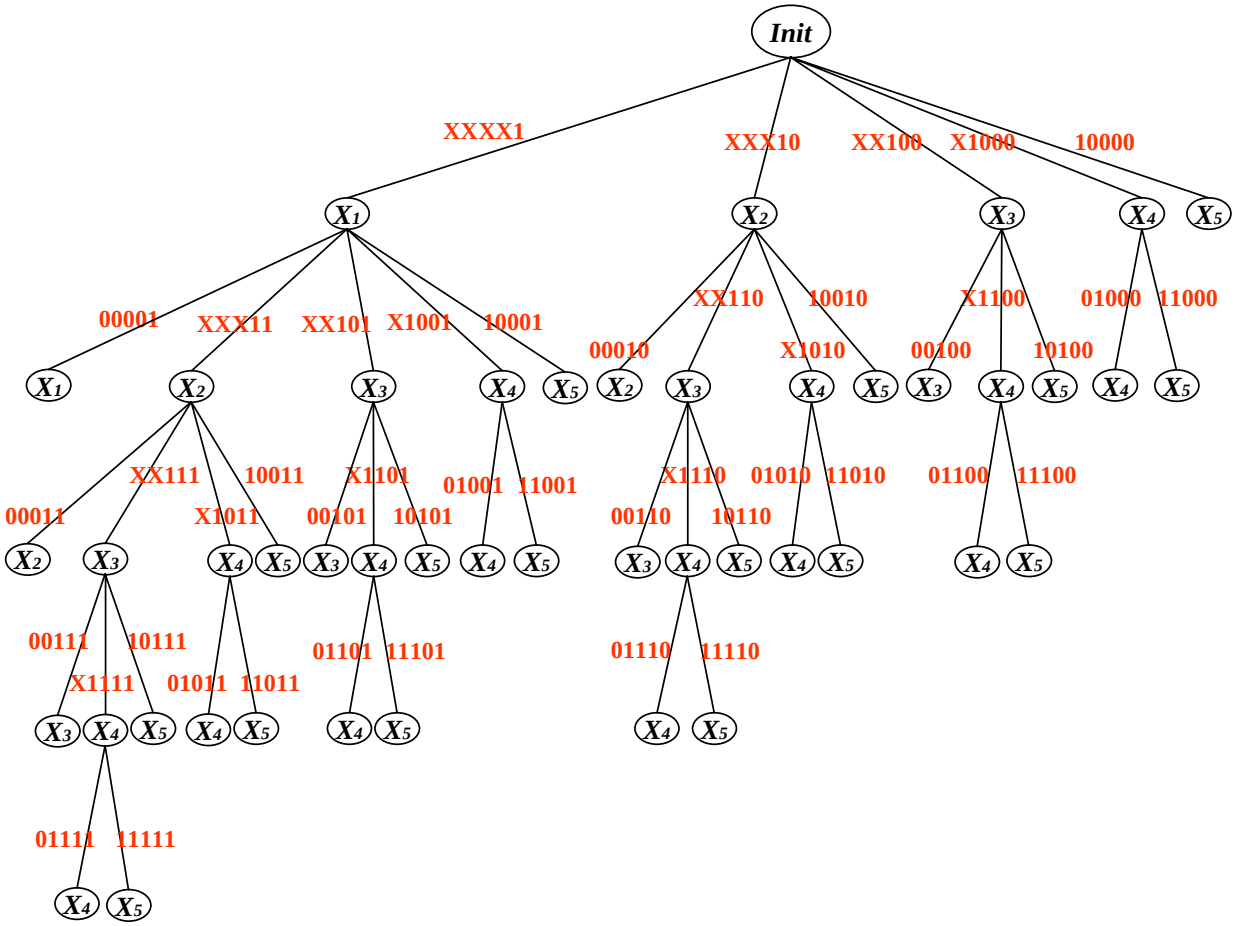


圖3.5　入侵事件狀態樹狀圖

3.2 關聯性的機率模型

以圖3.5來看，五種事件警示群組分別是X_1、X_2、X_3、X_4及X_5。

定義下列事件集合：

X_{all} ：發生全體事件警示的集合

X_1：發生預備攻擊前偵測(Pre-Attack Probe)的全部事件警示集合。

X_2：發生通訊協定特徵(Protocol Signature)的全部事件警示集合。

X_3：發生可疑動作(Suspicious Activity)的全部事件警示集合。

X_4：發生未經授權存取(Unauthorized Access Attempt)的全部事件警示集合。

X_5：發生阻絕服務(Denial of Service)的全部事件警示集合。

$n(A)$：表示發生A事件的警示個數，如 $n(X_{all})$表示全體事件警示的發生個數、$n(X_1)$表示全部預備攻擊前偵測事件警示集合的發生個數.....。

$P(A)$：表示發生A事件的機率，如 $P(X_{all})$表示全體事件警示的發生機率、$P(X_1)$表示全部預備攻擊前偵測事件警示的發生機率、.....。

依照機率的定義，可以求得五個事件警示群組之發生機率分別為

$$P(X_{all}) = 1 \tag{3.1}$$

$$P(X_1) = \frac{n(X_1)}{n(X_{all})} \tag{3.2}$$

$$P(X_2) = \frac{n(X_2)}{n(X_{all})} \tag{3.3}$$

$$P(X_3) = \frac{n(X_3)}{n(X_{all})} \tag{3.4}$$

$$P(X_4) = \frac{n(X_4)}{n(X_{all})} \tag{3.5}$$

$$P(X_5) = \frac{n(X_5)}{n(X_{all})} \tag{3.6}$$

也就是說

$P(X_1)$：發生預備攻擊前偵測(Pre-Attack Probe)的全部事件機率。

$P(X_2)$：發生通訊協定特徵(Protocol Signature)的全部事件機率。

$P(X_3)$：發生可疑動作(Suspicious Activity)的全部事件機率。

$P(X_4)$：發生未經授權存取(Unauthorized Access Attempt)的全部事件機率。

$P(X_5)$：發生阻絕服務(Denial of Service)的全部事件機率。

若將前述之入侵事件程序的每一個狀態，以機率來表示，則可得以下之入侵事件狀態機率樹狀圖(如圖3.6)。將入侵事件的全部可能狀態區分為五層，其中第一層的機率是$P(X_1)$、$P(X_2)$、$P(X_3)$、$P(X_4)$、及$P(X_5)$。而第二層與X_1關聯的機率是$P(X_1|X_1)$、$P(X_2|X_1)$、$P(X_3|X_1)$、$P(X_4|X_1)$、及$P(X_5|X_1)$；與X_2關聯的機率是$P(X_2|X_2)$、$P(X_3|X_2)$、$P(X_4|X_2)$、及$P(X_5|X_2)$；與X_3關聯的機率是$P(X_3|X_3)$、$P(X_4|X_3)$、及$P(X_5|X_3)$；與X_4關聯的機率是$P(X_4|X_4)$、及$P(X_5|X_4)$。因此，當機率為$P(X_3|X_{123})$、$P(X_4|X_{123})$、或$P(X_5|X_{123})$時，可以知道它是第三層與X_1、X_2、X_3關聯的機率。而依機率定義及警示之相互的關聯性，可定義下列關聯性的機率：

$P(X_1|X_1)$：在發生預備攻擊前偵測事件的條件下，依然停留在預備攻擊前偵測事件的機率。

$P(X_2|X_1)$：在發生預備攻擊前偵測事件的條件下，發生通訊協定特徵事件的機率。

$P(X_3|X_1)$：在發生預備攻擊前偵測事件的條件下，發生可疑動作事件的機率。

$P(X_4|X_1)$：在發生預備攻擊前偵測事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_1)$：在發生預備攻擊前偵測事件的條件下，發生阻絕服務事件的機率。

$$n(X_1) = n(X_1 \mid X_1) + n(X_2 \mid X_1) + n(X_3 \mid X_1) + n(X_4 \mid X_1) + n(X_5 \mid X_1) \qquad (3.7)$$

$$P(X_1 \mid X_1) = \frac{n(X_1 \mid X_1)}{n(X_1)} \qquad (3.8)$$

$$P(X_2 \mid X_1) = \frac{n(X_2 \mid X_1)}{n(X_1)} \tag{3.9}$$

$$P(X_3 \mid X_1) = \frac{n(X_3 \mid X_1)}{n(X_1)} \tag{3.10}$$

$$P(X_4 \mid X_1) = \frac{n(X_4 \mid X_1)}{n(X_1)} \tag{3.11}$$

$$P(X_5 \mid X_1) = \frac{n(X_5 \mid X_1)}{n(X_1)} \tag{3.12}$$

$P(X_2|X_2)$：在發生通訊協定特徵事件的條件下，依然停留在通訊協定特徵事件的機率。

$P(X_3|X_2)$：在發生通訊協定特徵事件的條件下，發生可疑動作事件的機率。

$P(X_4|X_2)$：在發生通訊協定特徵事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_2)$：在發生通訊協定特徵事件的條件下，發生阻絕服務事件的機率。

$$n(X_2) = n(X_2 \mid X_2) + n(X_3 \mid X_2) + n(X_4 \mid X_2) + n(X_5 \mid X_2) \tag{3.13}$$

$$P(X_2 \mid X_2) = \frac{n(X_2 \mid X_2)}{n(X_2)} \tag{3.14}$$

$$P(X_3 \mid X_2) = \frac{n(X_3 \mid X_2)}{n(X_2)} \tag{3.15}$$

$$P(X_4 \mid X_2) = \frac{n(X_4 \mid X_2)}{n(X_2)} \tag{3.16}$$

$$P(X_5 \mid X_2) = \frac{n(X_5 \mid X_2)}{n(X_2)} \tag{3.17}$$

$P(X_3|X_3)$：在發生可疑動作事件的條件下，依然停留在可疑動作事件的機率。

$P(X_4|X_3)$：在發生可疑動作事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_3)$：在發生可疑動作事件的條件下，發生阻絕服務事件的機率。

$$n(X_3) = n(X_3 \mid X_3) + n(X_4 \mid X_3) + n(X_5 \mid X_3) \tag{3.18}$$

$$P(X_3 \mid X_3) = \frac{n(X_3 \mid X_3)}{n(X_3)} \tag{3.19}$$

$$P(X_4 \mid X_3) = \frac{n(X_4 \mid X_3)}{n(X_3)} \tag{3.20}$$

$$P(X_5 \mid X_3) = \frac{n(X_5 \mid X_3)}{n(X_3)} \tag{3.21}$$

$P(X_4|X_4)$：在發生未經授權行為事件的條件下，依然停留在未經授權行為事件的機率。

$P(X_5|X_4)$：在發生未經授權行為事件的條件下，發生阻絕服務事件的機率。

$$n(X_4) = n(X_4 \mid X_4) + n(X_5 \mid X_4) \tag{3.22}$$

$$P(X_4 \mid X_4) = \frac{n(X_4 \mid X_4)}{n(X_4)} \tag{3.23}$$

$$P(X_5 \mid X_4) = \frac{n(X_5 \mid X_4)}{n(X_4)} \tag{3.24}$$

$P(X_5|X_5)$：在發生阻絕服務事件的條件下，依然停留在阻絕服務事件的機率。

$$n(X_5) = n(X_5 \mid X_5) \tag{3.25}$$

$$P(X_5 \mid X_5) = \frac{n(X_5 \mid X_5)}{n(X_5)} \tag{3.26}$$

……

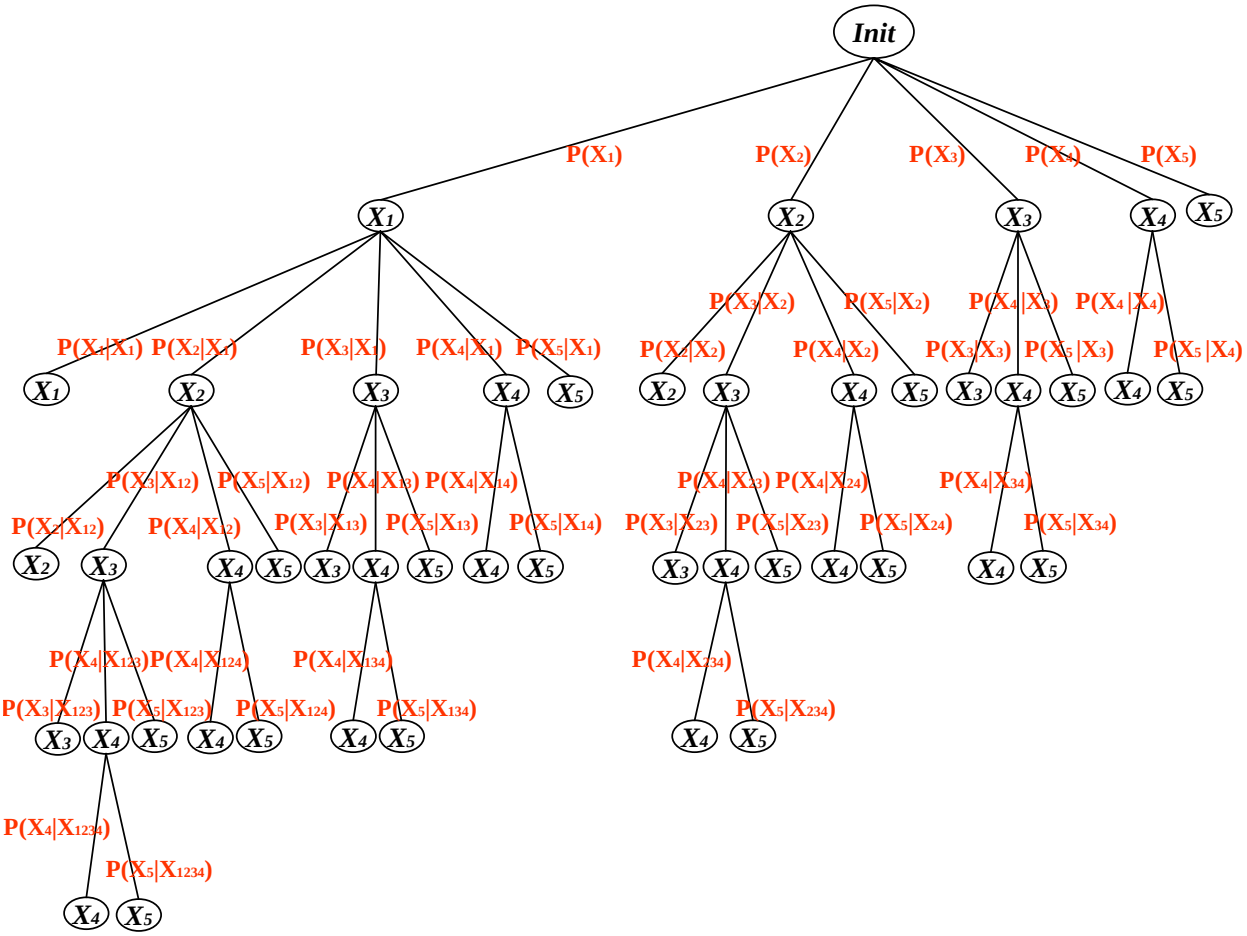


圖3.6　入侵事件狀態機率樹狀圖

以此類推，可以求得各層之關聯機率通式：

第一層：

$$P(X_i) = \frac{n(X_i)}{n(X_{all})} \tag{3.27}$$

第二層：

$$n(X_i) = \sum_{j=i}^{5} n(X_j \mid X_i) \tag{3.28}$$

$$P(X_j \mid X_i) = \frac{n(X_j \mid X_i)}{n(X_i)} \quad 1 \le i \le 5, i \le j \le 5 \tag{3.29}$$

第三層：

$$n(X_{ij}) = \sum_{k=j}^{5} n(X_k \mid X_{ij}) \tag{3.30}$$

$$P(X_k \mid X_{ij}) = \frac{n(X_k \mid X_{ij})}{n(X_{ij})} \quad 1 \le i \le 5, i \le j \le 5, j \le k \le 5 \tag{3.31}$$

第四層：

$$n(X_{ijk}) = \sum_{l=k}^{5} n(X_l \mid X_{ijk}) \tag{3.32}$$

$$P(X_l \mid X_{ijk}) = \frac{n(X_l \mid X_{ijk})}{n(X_{ijk})} \quad 1 \le i \le 5, i \le j \le 5, j \le k \le 5, k \le l \le 5 \tag{3.33}$$

第五層：

$$n(X_{ijkl}) = \sum_{m=l}^{5} n(X_m \mid X_{ijkl}) \tag{3.34}$$

$$P(X_m \mid X_{ijkl}) = \frac{n(X_m \mid X_{ijkl})}{n(X_{ijkl})} \quad 1 \le i \le 5, i \le j \le 5, j \le k \le 5, k \le l \le 5 \tag{3.35}$$

RealSecure入侵偵測系統的回應是以事件警示來進行，而事件警示則依威脅及嚴重程度而有所不同。有經驗的網路管理人員，還可以透過低威脅程度的警示來判斷是否有入侵事件發生。但較無經驗的人員，就僅能針對高威脅程度的警示來做出事件處理。不然所有事件警示動輒一、二千項，若要針對所有事件作出處理，不僅耗時更會花費大量的人力成本。

本研究先將各種狀況的機率值計算出來，在前述五種事件警示群組中，「攻擊前的偵測」或「通訊協定的特徵」等事件警示群組僅需要密切注意；而「可疑的動作」有可能是入侵行為；至於「未經授權的行為」或「阻絕服務」等事

件警示群組則是較為明顯之入侵行為，需要由管理人員予以處理。也就是若偵測時發現「攻擊前的偵測」警示群組時，暫時先不發出警報，並等待下一個來自同樣來源的封包進入；若仍為「攻擊前的偵測」或「通訊協定的特徵」事件警示，則持續等待下去；若發生「可疑的動作」、「未經授權的行為」或「阻絕服務」等事件時，便可以藉由這樣警示的關聯性對管理人員發出警報。也就是若發生兩種以上的事件警示，就會對管理者提出警報。如表3.2，狀態S_0～S_5，為需密切注意之狀況；狀態S_6～S_{31}，則判斷為疑似入侵事件的狀況。

表3.2　事件警示關聯狀態表

狀態	事件警示					入侵事件
	Denial of Service	Unauthorized Access Attempt	Suspicious Activity	Protocol Signature	Pre-Attack Probe	
	X_5	X_4	X_3	X_2	X_1	
S_0	0	0	0	0	0	0
S_1	0	0	0	0	1	0
S_2	0	0	0	1	0	0
S_3	0	0	0	1	1	0
S_4	0	0	1	0	0	0
S_5	0	0	1	0	1	1
S_6	0	0	1	1	0	1
S_7	0	0	1	1	1	1
S_8	0	1	0	0	0	1
S_9	0	1	0	0	1	1
S_{10}	0	1	0	1	0	1
S_{11}	0	1	0	1	1	1
S_{12}	0	1	1	0	0	1
S_{13}	0	1	1	0	1	1
S_{14}	0	1	1	1	0	1
S_{15}	0	1	1	1	1	1
S_{16}	1	0	0	0	0	1
S_{17}	1	0	0	0	1	1
S_{18}	1	0	0	1	0	1

S_{19}	1	0	0	1	1	1
S_{20}	1	0	1	0	0	1
S_{21}	1	0	1	0	1	1
S_{22}	1	0	1	1	0	1
S_{23}	1	0	1	1	1	1
S_{24}	1	1	0	0	0	1
S_{25}	1	1	0	0	1	1
S_{26}	1	1	0	1	0	1
S_{27}	1	1	0	1	1	1
S_{28}	1	1	1	0	0	1
S_{29}	1	1	1	0	1	1
S_{30}	1	1	1	1	0	1
S_{31}	1	1	1	1	1	1

透過這樣的提早警訊，若攻擊的主機所在之網域為網路管理者所負責，則管理人員可先讓攻擊主機離開網路，並進行檢查；若僅有被攻擊的電腦是管理人員所負責的，則管理人員可用其他手段(如防火牆、路由器等)將攻擊封包隔絕於網域之外。如此一來，必能大幅減少單位中被入侵或是入侵之後所造成的損害。

表3.3　RealSecure與關聯警示分析之差異

	RealSecure入侵偵測系統	關聯警示分析
相同處	以Rule-base方法判斷入侵事件	是，因為要依靠RealSecure的事件警示
	以事件警示的方式作出回應	以事件警示的方式作出回應
相異處	無法判斷未知的入侵事件。	若這個未知事件是由多項已知入侵事件警示組合，則可判斷這種類型的未知事件。
	擷取封包與資料庫中之特徵值(Pattern)比對，可即時發出警示。	要先以離線方式分析關聯警示，依照所得出來的機率值，再來進行進一步的線上判斷。但是在判斷時需要計算機率，因此是近即時發出警示，較RealSecure慢。

	只要符合資料庫中的特徵值，即發出事件警示	佐以關聯性的機率判斷，不會所有狀況都發出警訊
	網管人員的經驗對於判斷入侵事件安全扮演重要的角色	網管人員對判斷入侵事件的涉入比較不深

3.3 電腦緊急應變處理

當事件警示被判斷為疑似或真實的入侵事件時，網路或系統管理人員，應當遵循一定的步驟來逕行處置。而這樣的步驟，是屬於一種緊急應變處理。以目前來看，若是發生入侵事件，以公務機關來說，有一套電腦緊急應變回報的機制；而民間單位則可以向台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC)進行安全事件回報。

然而當入侵偵測系統提出警示時,應如何處置。有以下幾點該注意的[31,32]:

(1) 發現疑似入侵的動作

a. 查出入侵者來源，通知該網域之系統管理人員。

b. 檢查入侵者的入侵途徑，確認是否存在已知的漏洞。

c. 檢查同一網域的系統，是否同樣都有被入侵的跡象。

(2) 發現已經被入侵時

a. 分析所有的資料

b. 聯絡相關的單位(如上一級單位的電腦緊急應變小組、TWCERT/CC等專業單位)。

c. 收集入侵者所留下的痕跡，並確保系統中之資料無洩漏之虞。

d. 中斷入侵的動作

e. 修補系統漏洞，消除入侵的途徑

f. 回復系統正常操作

g. 分析並學習本次事件的處理經驗

4. 系統設計與驗證

4.1 系統設計

本研究之系統實驗架構如圖4.1所示：

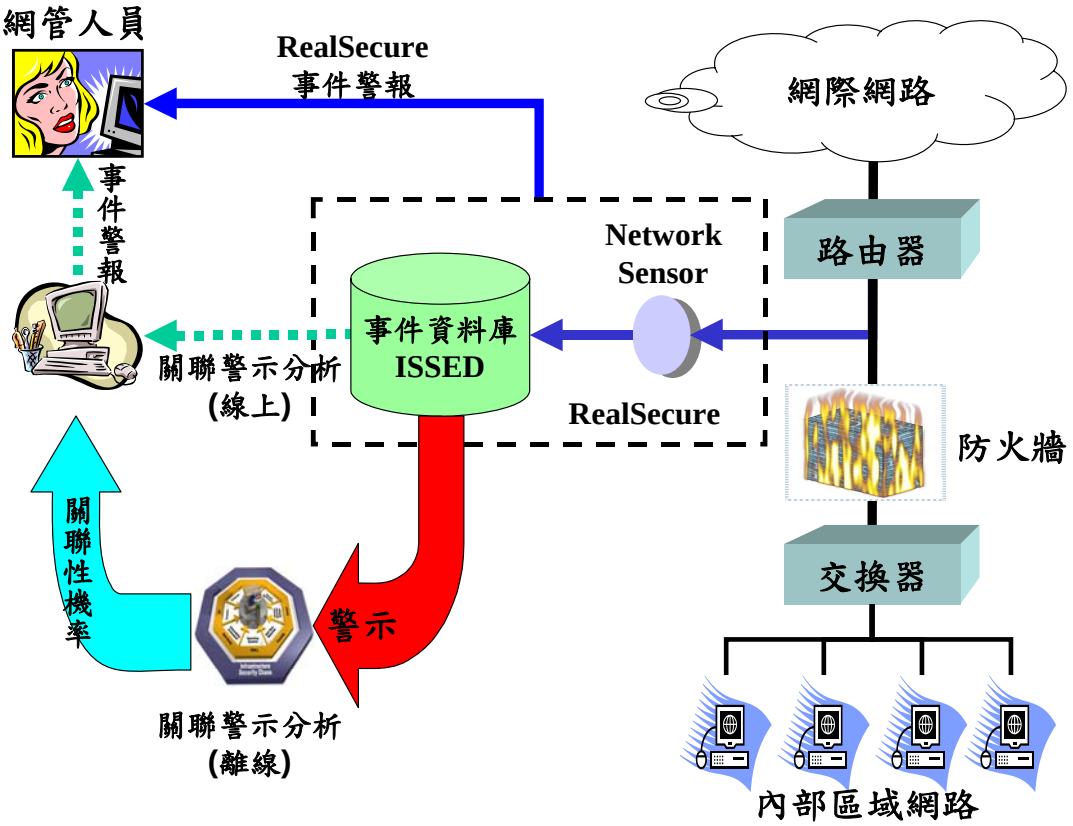


圖4.1　系統實驗架構圖

一般而言，RealSecure的資料流向如圖4.1中之實線箭頭(藍色)。事件蒐集器(Event Collector)透過網路感測器(Network Sensor)將網路上所通過的封包完整的拷貝一份，並與預先設定好的策略相比。能符合策略的封包即被宣告為一個事件(Event)，除了紀錄在事件資料庫(Internet Security System Events Database, ISSED)之外，尚對網路管理人員發出事件警報。然而對於網路管理人員來說，若策略過於寬鬆，過多的事件警報只是讓管理者疲於奔命，最後反而什麼都不

處理了；而過於嚴苛的策略，可能會錯失應有的事件警報。因此，本研究先以離線的方式整合與分析事件資料庫中的「events」資料表。該資料表共計有45個欄位(如表4.1)，本研究僅擷取與警示關聯性相關的欄位，如EventDate(事件日期)、SrcIPAddress(來源位址)、SrcPort(來源埠)、DestIPAddress(目的位址)、DestPort(目的埠)、OrigEventName(事件名稱)、及EventPriority(威脅程度)等資料。並將所有事件警示紀錄分成五個群組，透過群組之間的相互關聯，找出機率值，這個機率值可以用來進行事件警示的篩選。也就是以虛線箭頭(綠色)來進行關聯警示的線上分析，並提供事件警報。這樣的方式會較原有的警報方式慢一點，但透過機率值的篩選，會讓發出警報的事件都是明顯有問題的真實狀況。這樣讓管理者在處理上，也會減少一些困擾。

表4.1　事件資料庫欄位表[33]

欄位名稱	資料型別	資料長度	是否允許空值	備註
SecChkID	int	4	F	事件的資安檢查碼(SecurityCheckID)，與資安檢查結果有關
ProtocolID	int	4	F	事件的通訊協定識別碼(ProtocolID)，與採用的通訊協定有關
DayID	int	4	F	事件的日期識別碼(ProtocolID)，與事件日期有關
TimeID	smallint	2	F	事件的時間識別碼(ProtocolID)，與事件時間有關
EventID	int	4	T	每一筆紀錄的識別碼
ActionID	int	4	T	事件的動作識別碼(ProtocolID)，與事件所採取的動作有關
EventDate	datetime	8	F	事件紀錄的日期與時間
SrcPort	int	4	T	來源端所指定的通訊埠
SrcIPAddress	varchar	60	T	來源端所指定的IP位址
SrcPortName	varchar	60	T	來源端所指定的通訊埠名稱
DestPort	int	4	T	目標端所指定的通訊埠
DestIPAddress	varchar	60	T	目標端所指定的IP位址
DestPortName	varchar	60	T	目標端所指定的通訊埠名稱
SrcEthernetAddr	varchar	60	T	來源端的MAC位址

SrcEthernetVendor	varchar	60	T	目前沒有被使用
DestEthernetAddr	varchar	60	T	目標端的MAC位址
DestEthernetVendor	varchar	60	T	目前沒有被使用
TCPFlags	varchar	50	T	目前沒有被使用
ICMPType	varchar	50	T	ICMP封包的型式
ICMPCode	varchar	50	T	ICMP封包的編碼
EventPriority	int	4	T	1=High, 2=Medium, 3=Low
MonitorIPAddress	varchar	47	T	網路/主機的監控端所被指派的IP位址
RemoteEventID	int	4	F	來自ISSED資料庫中每一筆紀錄的識別碼
AlertID	varchar	26	T	每一筆警示資料記錄的唯一關鍵值
AlertTimeSeqID	int	4	T	雖然許多警示發生在同一秒的區間，但還是以時間/日期來考慮那個選擇的警示。從第一個警報產生時，這個數值被重設為1，以及在同一秒期間每一個產生的成功警示不斷增加。
SensorAddress	varchar	60	T	在企業網路中指定的感測器位置。可能是IP或其他的網路位址。這與感測器名稱是不同的。
AlertType	int	4	T	這數值代表警示名稱的型式 1 = ISS SecChkID的型式 2 = XFDB TagName的型式 3 = CVE Number的型式 4 = User Defined的型式 5 = Product Defined的型式
SensorName	varchar	60	T	對於所有感測器分享同一個感測器位址來說，感測器的識別名稱必須是唯一的。
LocalTimezoneOffset	int	4	T	感測器在短時間內來自於UTC的區域時區偏移量。這個值與AlertDateTime在一起，能夠用來重建事件發生感測器的區域時間。
AlertTimePrecision	int	4	T	這個數值以更精準的秒數資訊來增強AlertDateTime。
AlertNameType	int	4	T	這是ISS SecChkID的數值、XFDB TagName 字串、CVE數值、User Defined字串、或Product Defined的字串
AttackSuccessful	tinyint	1	T	表示那個可疑的網路行為是成功的攻擊、不成功的攻擊、或不知道。註：Server Sensor的Windows 6.0.1版及之後，以0代表成功、1代表不成功、2代表不知道
AttackFragmented	tinyint	1	T	一個布林代數值，如果那個可疑的網路行為變成碎裂的封包則是True，如果不是則是False
DisplaySrcIPAddress	varchar	60	T	顯示來源IP位址，用於回報
DisplayDestIPAddress	varchar	60	T	顯示目標IP位址，用於回報
DisplaySensorAddress	varchar	60	T	顯示感測器IP位址，用於回報

OrigEventName	varchar	60	T	來自於感測器的原始事件名稱
AttackOrigin	varchar	60	T	表現出攻擊的來源
ResourceID	int	4	T	1=Disk; 2=Memory.
ResourceSubID	varchar	60	T	辨識資源接近枯竭的特殊實例。
Application	varchar	60	T	讓警示產生的應用程式名稱
UserName	varchar	60	T	特殊主機的使用者名稱
State	tinyint	1	F	一個數值用來指示事件的現行狀態。可能的狀態包括活動(Active)，休眠(Dormant)，及結束(Concluded)。
AlertFlags	int	4	T	一個位元資料旗標使用在混雜的警示屬性。

4.2 警示分析

本研究是以ISS公司入侵偵測系統的事件警示為準，也就是以RealSecure所產生的事件警示作為關聯判斷的目標。所分析的警示，是從十月十二日至卅日，從某單位的內部網路上，蒐集了近2 Giga Bytes的事件警示資料。由於本研究中的警示關聯性，是依照來源位址、目的位址及時間來決定的。但是所蒐集的警示之中，部分是屬於入侵偵測系統本身所產生的警示，如：EventCollector_Info、EventCollector_Error、EventCollector_Warning、及Sensor_Info，而這部分的警示，它的來源位址是空字串(null)。因此，在進行警示分析之前，須先移除來源位址是null的封包，這樣易於進行後續的整合與判斷的工作。其次，由於來源位址為0.0.0.0的封包，無法確切判定入侵來源，故亦需移除。

全部的警示資料共有364284筆紀錄，若移除來源位址為空字串(Null)及0.0.0.0的紀錄，計有312629筆紀錄。透過SQL查詢程式如表4.2，可計算出全部資料區分為248種不同的警示。而這些警示如3.1.2節中所述，共區分為五個群組 (警示個數、種類，均詳如附錄壹)。計有阻絕服務(Denial of Service)、預備攻擊前的偵測(Pre-Attack Probe)、通訊協定的特徵(Protocol Signature)、可疑的動作(Suspicious Activity)、以及未經授權的存取行為(Unauthorized Access Attempt)等五個群組。

表4.2　查詢並計算個別警示的個數

```
USE          ISSED
GO
SELECT       OrigEventName,COUNT(*)   AS  次數
FROM         Events
WHERE        SrcIPAddress IS NOT NULL
GROUP BY     OrigEventName
GROUP BY     OrigEventName
GO
```

(1) 預備攻擊前的偵測(Pre-Attack Probe)：屬於這個群組的警示有34種。常見的是TCP_Service_Sweep、SMB_Service_Sweep、TCP_Port_Scan、Ping_Sweep等警示。

(2) 通訊協定的特徵(Protocol Signature)：屬於這個群組的警示有34種。常見的警示有OSPF_Null_Authentication、ISAKMP_Vendor_Id、SNMP_ifTable等。

(3) 可疑的動作(Suspicious Activity)：屬於這個群組的警示有51種，從威脅程度最高的SMB_Empty_Password、HTTP_Nimda_Worm到輕微的HTTP_Frontpage_Path、DCOM_SystemActivation等警示。

(4) 未經授權的存取行為(Unauthorized Access Attempt)：屬於這個群組的警示有110種。其中最常出現的是SNMP_Default_Backdoor、HTTP_POST_repeated_char；而威脅程度最高的有UDP_Port_Scan、HTTP_Unix_Passwords、POP_Command_Overflow等警示。

(5) 阻絕服務(Denial of Service)：屬於這個群組的警示有19個，最常見的是FTP_Windows_Drive_Path、 Smurf_Attack等警示。

定義下列事件機率：

$P(X_1)$：發生預備攻擊前偵測(Pre-Attack Probe)的全部事件機率。

$P(X_2)$：發生通訊協定特徵(Protocol Signature)的全部事件機率。

$P(X_3)$：發生可疑動作(Suspicious Activity)的全部事件機率。

$P(X_4)$：發生未經授權存取(Unauthorized Access Attempt)的全部事件機率。

$P(X_5)$：發生阻絕服務(Denial of Service)的全部事件機率。

$P(X_1|X_1)$：在發生預備攻擊前偵測事件的條件下，依然停留在預備攻擊前偵測事件的機率。

$P(X_2|X_1)$：在發生預備攻擊前偵測事件的條件下，發生通訊協定特徵事件的機率。

$P(X_3|X_1)$：在發生預備攻擊前偵測事件的條件下，發生可疑動作事件的機率。

$P(X_4|X_1)$：在發生預備攻擊前偵測事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_1)$：在發生預備攻擊前偵測事件的條件下，發生阻絕服務事件的機率。

$P(X_2|X_2)$：在發生通訊協定特徵事件的條件下，依然停留在通訊協定特徵事件的機率。

$P(X_3|X_2)$：在發生通訊協定特徵事件的條件下，發生可疑動作事件的機率。

$P(X_4|X_2)$：在發生通訊協定特徵事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_2)$：在發生通訊協定特徵事件的條件下，發生阻絕服務事件的機率。

$P(X_3|X_3)$：在發生可疑動作事件的條件下，依然停留在可疑動作事件的

機率。

$P(X_4|X_3)$：在發生可疑動作事件的條件下，發生未經授權行為事件的機率。

$P(X_5|X_3)$：在發生可疑動作事件的條件下，發生阻絕服務事件的機率。

$P(X_4|X_4)$：在發生未經授權行為事件的條件下，依然停留在未經授權行為事件的機率。

$P(X_5|X_4)$：在發生未經授權行為事件的條件下，發生阻絕服務事件的機率。

$P(X_5|X_5)$：在發生阻絕服務事件的條件下，依然停留在阻絕服務事件的機率。

$n(A)$：表示發生A事件的警示個數，如$n(X_{all})$表示全體事件警示的發生個數、$n(X_1)$表示全部預備攻擊前偵測事件警示集合的發生個數……。

$P(A)$：表示發生A事件的機率，如$P(X_{all})$表示全體事件警示的發生機率、$P(X_1)$表示全部預備攻擊前偵測事件警示的發生機率……。

則計算出第一層的事件機率為

$$P(X_{all}) = 1$$

$$P(X_1) = \frac{n(X_1)}{n(X_{all})} = \frac{144564}{312629} = 0.5584$$

$$P(X_2) = \frac{n(X_2)}{n(X_{all})} = \frac{132939}{312629} = 0.4252$$

$$P(X_3) = \frac{n(X_3)}{n(X_{all})} = \frac{1688}{312629} = 0.0054$$

$$P(X_4) = \frac{n(X_4)}{n(X_{all})} = \frac{1705}{312629} = 0.0053$$

$$P(X_5) = \frac{n(X_5)}{n(X_{all})} = \frac{1733}{312629} = 0.0053$$

第二層的事件機率計算為

$$\begin{aligned} n(X_1) &= n(X_1 \mid X_1) + n(X_2 \mid X_1) + n(X_3 \mid X_1) + n(X_4 \mid X_1) + n(X_5 \mid X_1) \\ &= 134878 + 38821 + 239 + 421 + 205 \\ &= 174564 \end{aligned}$$

$$P(X_1 \mid X_1) = \frac{n(X_1 \mid X_1)}{n(X_1)} = \frac{134878}{174564} = 0.7727$$

$$P(X_2 \mid X_1) = \frac{n(X_2 \mid X_1)}{n(X_1)} = \frac{38821}{174564} = 0.2224$$

$$P(X_3 \mid X_1) = \frac{n(X_3 \mid X_1)}{n(X_1)} = \frac{239}{174564} = 0.0014$$

$$P(X_4 \mid X_1) = \frac{n(X_4 \mid X_1)}{n(X_1)} = \frac{421}{174564} = 0.0024$$

$$P(X_5 \mid X_1) = \frac{n(X_5 \mid X_1)}{n(X_1)} = \frac{205}{174564} = 0.0012$$

$$\begin{aligned} n(X_2) &= n(X_2 \mid X_2) + n(X_3 \mid X_2) + n(X_4 \mid X_2) + n(X_5 \mid X_2) \\ &= 129863 + 356 + 2720 + 0 \\ &= 132939 \end{aligned}$$

$$P(X_2 \mid X_2) = \frac{n(X_2 \mid X_2)}{n(X_2)} = \frac{129863}{132939} = 0.9769$$

$$P(X_3 \mid X_2) = \frac{n(X_3 \mid X_2)}{n(X_2)} = \frac{356}{132939} = 0.0027$$

$$P(X_4 \mid X_2) = \frac{n(X_4 \mid X_2)}{n(X_2)} = \frac{2720}{132939} = 0.0205$$

$$P(X_5 \mid X_2) = \frac{n(X_5 \mid X_2)}{n(X_2)} = \frac{0}{132939} = 0$$

$$n(X_3) = n(X_3 \mid X_3) + n(X_4 \mid X_3) + n(X_5 \mid X_3) = 1466 + 183 + 39 = 1688$$

$$P(X_3 \mid X_3) = \frac{n(X_3 \mid X_3)}{n(X_3)} = \frac{1466}{1688} = 0.8685$$

$$P(X_4 \mid X_3) = \frac{n(X_4 \mid X_3)}{n(X_3)} = \frac{183}{1688} = 0.1084$$

$$P(X_5 \mid X_3) = \frac{n(X_5 \mid X_3)}{n(X_3)} = \frac{39}{1688} = 0.0231$$

$$n(X_4) = n(X_4 \mid X_4) + n(X_5 \mid X_4) = 1088 + 617 = 1705$$

$$P(X_4 \mid X_4) = \frac{n(X_4 \mid X_4)}{n(X_4)} = \frac{1088}{1705} = 0.6381$$

$$P(X_5 \mid X_4) = \frac{n(X_5 \mid X_4)}{n(X_4)} = \frac{617}{1705} = 0.3619$$

$$P(X_5 \mid X_5) = \frac{n(X_5 \mid X_5)}{n(X_5)} = \frac{n(X_5)}{n(X_5)} = 1$$

以此方式，可以分別求出各個狀況的機率。將計算之機率填入圖3.6，可得出入侵事件機率分布圖(如圖4.2)。

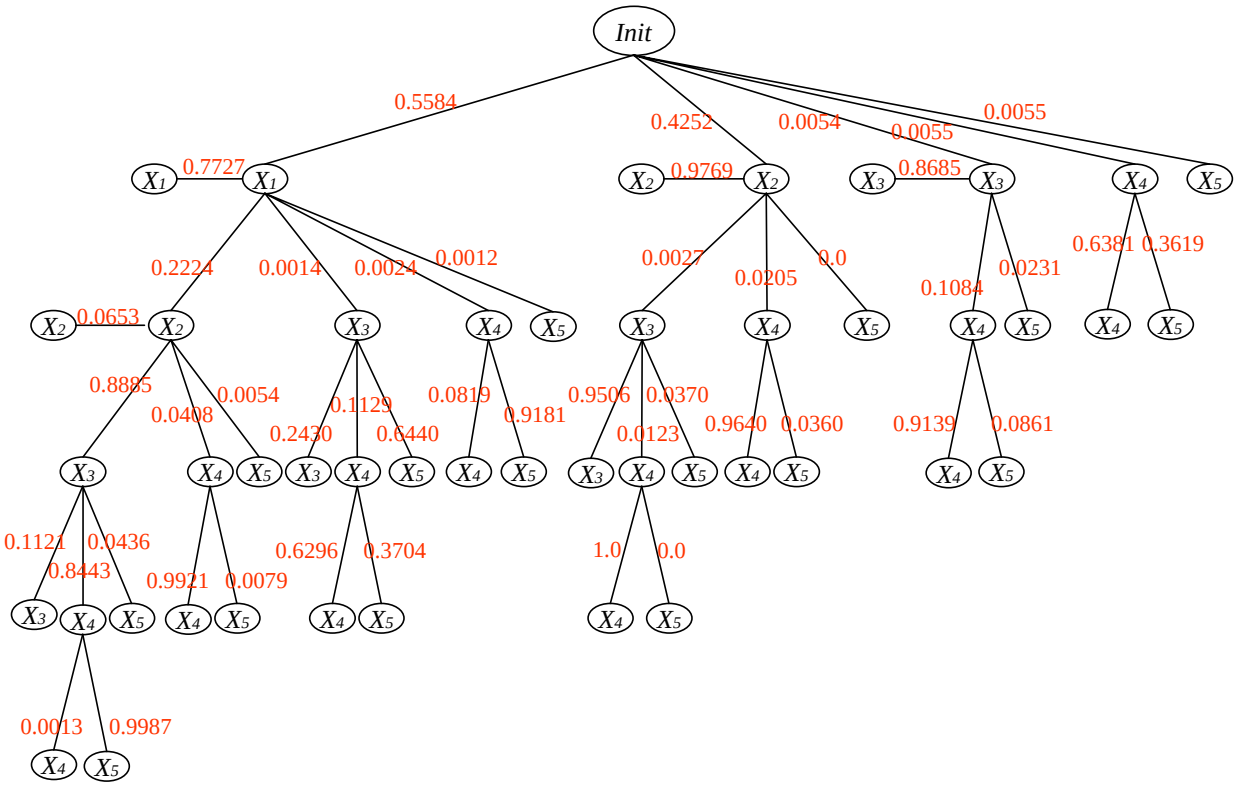


圖4.2　入侵事件機率分布圖

從圖4.2之入侵事件機率分布圖中，可以計算得出各個狀況之關聯性機率。

$P(X_{11}) = P(X_1) \times P(X_1|X_1) = 0.5584 \times 0.7727 = 0.43147568$

$P(X_{22}) = P(X_2) \times P(X_2|X_2) = 0.4252 \times 0.9769 = 0.41537788$

$P(X_{33}) = P(X_3) \times P(X_3|X_3) = 0.0054 \times 0.8685 = 0.00468990$

$P(X_{44}) = P(X_4) \times P(X_4|X_4) = 0.0055 \times 0.6381 = 0.00350955$

$P(X_{55}) = P(X_5) \times P(X_5|X_5) = 0.0055 \times 1 = 0.0055$

$P(X_{122}) = P(X_1) \times P(X_2|X_1) \times P(X_2|X_{12}) = 0.5584 \times 0.2224 \times 0.0653$

$= 0.00810949$

$P(X_{133}) = P(X_1) \times P(X_3|X_1) \times P(X_3|X_{13}) = 0.5584 \times 0.0014 \times 0.2430$

$= 0.00018997$

$P(X_{144}) = P(X_1) \times P(X_4|X_1) \times P(X_4|X_{14}) = 0.5584 \times 0.0024 \times 0.0819$

$= 0.00010976$

$P(X_{233}) = P(X_2) \times P(X_3|X_2) \times P(X_3|X_{23}) = 0.4252 \times 0.0027 \times 0.9506$

$= 0.00109133$

$P(X_{244}) = P(X_2) \times P(X_4|X_2) \times P(X_4|X_{24}) = 0.4252 \times 0.0205 \times 0.9640$

$= 0.00840280$

$P(X_{344}) = P(X_3) \times P(X_4|X_3) \times P(X_4|X_{34}) = 0.0054 \times 0.1084 \times 0.9139$

$= 0.00053496$

$P(X_{1233}) = P(X_1) \times P(X_2|X_1) \times P(X_3|X_{12}) \times P(X_3|X_{123})$

$= 0.5584 \times 0.2224 \times 0.8885 \times 0.1121 = 0.01236925$

$P(X_{1244}) = P(X_1) \times P(X_2|X_1) \times P(X_4|X_{12}) \times P(X_4|X_{124})$

$= 0.5584 \times 0.2224 \times 0.0408 \times 0.9921 = 0.00502685$

$P(X_{1344}) = P(X_1) \times P(X_3|X_1) \times P(X_4|X_{13}) \times P(X_4|X_{134})$

$= 0.5584 \times 0.0014 \times 0.1129 \times 0.6296 = 0.00005557$

$P(X_{2344}) = P(X_2) \times P(X_3|X_2) \times P(X_4|X_{23}) \times P(X_4|X_{234})$

$= 0.4252 \times 0.0027 \times 0.0123 \times 1.0 = 0.00001412$

$P(X_{12344}) = P(X_1) \times P(X_2|X_1) \times P(X_3|X_{12}) \times P(X_4|X_{123}) \times P(X_4|X_{1234})$

$= 0.5584 \times 0.2224 \times 0.8885 \times 0.8443 \times 0.0013 = 0.00012111$

$P(X_{15}) = P(X_1) \times P(X_5|X_1) = 0.5584 \times 0.0012 = 0.00067008$

$P(X_{25}) = P(X_2) \times P(X_5|X_2) = 0.4252 \times 0 = 0$

$P(X_{35}) = P(X_3) \times P(X_5|X_3) = 0.0054 \times 0.0231 = 0.00012474$

$P(X_{45}) = P(X_4) \times P(X_5|X_4) = 0.0055 \times 0.3619 = 0.00199045$

$P(X_{125}) = P(X_1) \times P(X_2|X_1) \times P(X_5|X_{12}) = 0.5584 \times 0.2224 \times 0.0054$

$= 0.00067062$

$P(X_{135}) = P(X_1) \times P(X_3|X_1) \times P(X_5|X_{13}) = 0.5584 \times 0.0014 \times 0.6440$

$= 0.00050345$

$P(X_{145}) = P(X_1) \times P(X_4|X_1) \times P(X_5|X_{14}) = 0.5584 \times 0.0024 \times 0.9181$

$= 0.00123040$

$P(X_{235}) = P(X_2) \times P(X_3|X_2) \times P(X_5|X_{23}) = 0.4252 \times 0.0027 \times 0.0370$

$= 0.00004248$

$P(X_{245}) = P(X_2) \times P(X_4|X_2) \times P(X_5|X_{24}) = 0.4252 \times 0.0205 \times 0.0360$

$= 0.00031380$

$P(X_{345}) = P(X_3) \times P(X_4|X_3) \times P(X_5|X_{34})$

$= 0.0054 \times 0.1084 \times 0.0861 = 0.00005040$

$P(X_{1235}) = P(X_1) \times P(X_2|X_1) \times P(X_3|X_{12}) \times P(X_5|X_{123})$

$= 0.5584 \times 0.2224 \times 0.8885 \times 0.0436 = 0.00481088$

$P(X_{1245}) = P(X_1) \times P(X_2|X_1) \times P(X_4|X_{12}) \times P(X_5|X_{124})$

$= 0.5584 \times 0.2224 \times 0.0408 \times 0.0079 = 0.00004003$

$P(X_{1345}) = P(X_1) \times P(X_3|X_1) \times P(X_4|X_{13}) \times P(X_5|X_{134})$

$= 0.5584 \times 0.2224 \times 0.1129 \times 0.3404 = 0.00477270$

$P(X_{2345}) = P(X_2) \times P(X_3|X_2) \times P(X_4|X_{23}) \times P(X_5|X_{234})$

$= 0.4252 \times 0.0027 \times 0.0123 \times 0 = 0$

$P(X_{12345}) = P(X_1) \times P(X_2|X_1) \times P(X_3|X_{12}) \times P(X_4|X_{123}) \times P(X_5|X_{1234})$

$= 0.5584 \times 0.2224 \times 0.8885 \times 0.8443 \times 0.9987 = 0.09303995$

由以上算式可計算出各種狀態所關連出來的機率值，結果如表4.3。

表4.3　事件警示關聯機率表

狀態	事件警示群組					入侵警示	機率
	Denial Of Service	Unauthorized Access Attempt	Suspicious Activity	Protocol Signature	Pre-Attack Probe		
	X_5	X_4	X_3	X_2	X_1		
S_0(Init)	0	0	0	0	0	0	0.0
$S_1(X_{11})$	0	0	0	0	1	0	0.43147568
$S_2(X_{22})$	0	0	0	1	0	0	0.41537788
$S_3(X_{122})$	0	0	0	1	1	0	0.00810949
$S_4(X_{33})$	0	0	1	0	0	0	0.00468990
$S_5(X_{133})$	0	0	1	0	1	1	0.00018997
$S_6(X_{233})$	0	0	1	1	0	1	0.00109133
$S_7(X_{1233})$	0	0	1	1	1	1	0.01236925
$S_8(X_{44})$	0	1	0	0	0	1	0.00350955
$S_9(X_{144})$	0	1	0	0	1	1	0.00010976
$S_{10}(X_{244})$	0	1	0	1	0	1	0.00840280
$S_{11}(X_{1244})$	0	1	0	1	1	1	0.00502685
$S_{12}(X_{344})$	0	1	1	0	0	1	0.00053496
$S_{13}(X_{1344})$	0	1	1	0	1	1	0.00005557
$S_{14}(X_{2344})$	0	1	1	1	0	1	0.00001412
$S_{15}(X_{12344})$	0	1	1	1	1	1	0.00012111
$S_{16}(X_5)$	1	0	0	0	0	1	0.0055
$S_{17}(X_{15})$	1	0	0	0	1	1	0.00067008
$S_{18}(X_{25})$	1	0	0	1	0	1	0.0
$S_{19}(X_{125})$	1	0	0	1	1	1	0.00067062
$S_{20}(X_{35})$	1	0	1	0	0	1	0.00012474
$S_{21}(X_{135})$	1	0	1	0	1	1	0.00050345
$S_{22}(X_{235})$	1	0	1	1	0	1	0.00004248
$S_{23}(X_{1235})$	1	0	1	1	1	1	0.00481088
$S_{24}(X_{45})$	1	1	0	0	0	1	0.00199045
$S_{25}(X_{145})$	1	1	0	0	1	1	0.00123040
$S_{26}(X_{245})$	1	1	0	1	0	1	0.00031380
$S_{27}(X_{1245})$	1	1	0	1	1	1	0.00004003
$S_{28}(X_{345})$	1	1	1	0	0	1	0.00005040
$S_{29}(X_{1345})$	1	1	1	0	1	1	0.00477270
$S_{30}(X_{2345})$	1	1	1	1	0	1	0.0
$S_{31}(X_{12345})$	1	1	1	1	1	1	0.09303995

4.3 驗證結果

以表3.1 x.131.51.111的事件警示紀錄為例，10/12 07:14時發生一個 SMB_Service_Sweep事件警示。以傳統的入侵偵測系統來看，這個是屬於第三等級的事件，不需要處置。持續二天傳輸這樣的偵測封包，一直到10/14 00:58時，這樣的偵測封包才停止。而等到一個小時後，也就是10/14 02:02時，下一個狀況又繼續進行。所發生的事件警示MSRPC_LSASS_Request_Detected還是第三等級的事件，必須要到了MSRPC_LSASS_Bo事件發生之後，管理者才會正視這個狀況並進行緊急應變處理。這樣算起來，從第一次的事件發生到管理員處理，大約花費了二日左右的時間。

以本研究來說，SMB_Service_Sweep是屬於預備攻擊前偵測(X_1)的群組，而在這個群組中，有0.7727的機率會繼續停留在預備攻擊前偵測(X_1)事件警示群組，有0.2224的機率會演變成為通訊協定的特徵(X_2)事件警示群組，由於這兩種群組的事件是屬於探測類的事件，因此還不需要向管理人員發出警報。但是當MSRPC_LSASS_ Request_Detected事件發生後，這是屬於通訊協定特徵(X_2)群組的事件。在這個群組中，會繼續停留在通訊協定特徵(X_2)事件群組的機率是0.0653，而發生可疑動作(X_3)事件的機率是0.8885，所以分析器就會告訴管理人員即將發生可疑動作的(X_3)事件。透過警示相互關聯的機率值，來判斷下一個警示的傾向。也就是發生可疑動作(X_3)、未經授權存取的行為(X_4)或阻絕服務(X_5)等三個群組事件警示時，則管理人員應先進行緊急應變處理。而不需要等到最後的MSRPC_LSASS_Bo事件發生之後才要做。

若發生的事件為預備攻擊前偵測(X_1)與通訊協定特徵(X_2)事件的警示群組，由計算出之機率可知，絕大多數的警示都是屬於這兩個群組，再加上這兩個群組的警示為探測性質，因此管理人員不需要進行緊急應變處理。若發生的警示是屬於可疑動作(X_3)的群組，則應當回溯之前的相關警示，假如有預備攻擊前偵

測或通訊協定特徵群組的事件警示時，則應當向管理人員發出警報，由管理人員來進行緊急應變處理。假設發生的事件為未經授權存取的行為(X_4)或阻絕服務(X_5)群組時，由於這兩者發生的機率很低，若發生事件時，則管理人員均應當優先進行緊急應變處理。因此判斷入侵之規則如表4.4。

表4.4　判斷入侵之規則

令 A_n 爲第 *n* 個事件警示
Do
　if $A_n \in X_4$ *then*
　　發出警報－疑爲Unauthorized Access Attempt 入侵事件
　end if
　if $A_n \in X_5$ *then*
　　發出警報－疑爲Denial Of Service入侵事件
　end if
　if $A_n \in X_3$ *then*
　　for $i = 1$ *to* $n-1$ *then*
　　if $A_i \in X_1$ *or* $A_i \in X_2$ *then*
　　發出警報－疑爲Suspicious Activity入侵事件
　　end if
　　next
　end if
Loop

5. 結論與未來研究方向

5.1 結論

一般Rule-based的入侵偵測系統，都要等到最後的警示出現了，系統管理者才能做緊急應變處置。假設有一台電腦感染了蠕蟲，若它剛開始還在發送掃描封包的時候就發現，那麼所需要處理的就只有一台電腦。但是，目前的入侵偵測系統大多都要等到它的特徵封包出現之後，才會發出警訊。但是當特徵封包出現，同時也代表這隻蠕蟲感染其他電腦了。如此一來，所要處理的電腦就不只一台了。

以表3.1 ×.131.51.111的事件警示紀錄為例，10/12 07:14時發生一個 SMB_Service_Sweep事件警示。以傳統的入侵偵測系統來看，這個是屬於第三等級的事件，不需要處置。持續二天傳輸這樣的偵測封包，一直到10/14 00:58時，這樣的偵測封包才停止。而等到一個小時後，也就是10/14 02:02時，下一個狀況又繼續進行。所發生的事件警示MSRPC_LSASS_Request_Detected還是第三等級的事件，必須要到了MSRPC_LSASS_Bo事件發生之後，管理者才會正視這個狀況並進行緊急應變處理。這樣算起來，從第一次的事件發生到管理員處理，大約花費了二日左右的時間。

以本研究來說，SMB_Service_Sweep是屬於預備攻擊前偵測(X_1)的群組，而在這個群組中，有0.7727的機率會繼續停留在預備攻擊前偵測(X_1)事件警示群組，有0.2224的機率會演變成為通訊協定的特徵(X_2)事件警示群組，由於這兩種群組的事件是屬於探測類的事件，因此還不需要向管理人員發出警報。但是當MSRPC_LSASS_ Request_Detected事件發生後，這是屬於通訊協定特徵(X_2)群組的事件。在這個群組中，會繼續停留在通訊協定特徵(X_2)事件群組的機率是0.0653，而發生可疑動作(X_3)事件的機率是0.8885，所以分析器就會告訴管理人

員即將發生可疑動作的(X_3)事件。透過警示相互關聯的機率值，來判斷下一個警示的傾向。也就是發生可疑動作(X_3)、未經授權存取的行為(X_4)或阻絕服務(X_5)等三個群組事件警示時，則管理人員應先進行緊急應變處理。而不需要等到最後的MSRPC_LSASS_Bo事件發生之後才要做。

若發生的事件為預備攻擊前偵測(X_1)與通訊協定特徵(X_2)事件的警示群組，由計算出之機率可知，絕大多數的警示都是屬於這兩個群組，再加上這兩個群組的警示為探測性質，因此管理人員不需要進行緊急應變處理。若發生的警示是屬於可疑動作(X_3)的群組，則應當回溯之前的相關警示，假如有預備攻擊前偵測或通訊協定特徵群組的事件警示時，則應當向管理人員發出警報，由管理人員來進行緊急應變處理。假設發生的事件為未經授權存取的行為(X_4)或阻絕服務(X_5)群組時，由於這兩者發生的機率很低，若發生事件時，則管理人員均應當優先進行緊急應變處理。

以往的入侵偵測系統所發生的每一個事件警示，都需要去分析判斷是否需要進行處理，然而管理人員會因為過多的事件警示而疲乏，最後反而無法精確研判入侵事件。本研究過濾了對系統沒有明顯影響或破壞的事件警示，並將管理人員的注意力集中於有破壞性質或可疑的事件警示。由於對系統沒有明顯影響或破壞的事件警示佔全體事件警示約80%，故本研究僅需要針對那20%的明顯入侵事件進行處理。同時，本研究的偵測模型，可預判入侵事件的傾向，讓管理人員提前從事緊急應變之準備。雖然剛開始的時候，依然會有誤報的情況發生。但隨著長時間的網路封包蒐集，以及定期重新計算機率值，能將整個系統慢慢調整成為符合這個網域需求的分析器。

5.2 未來研究方向

(1) 本研究將攻擊者的行為模式分成五大攻擊群組，並依照所蒐集的警示

進行整體性的關聯分析，可明確地瞭解駭客的攻擊手法，並依照所建立之偵測規則來判定是否為駭客的入侵行為。由於本研究使用機率之偵測規則，當未知攻擊是屬於幾種已知攻擊的組合，就有一定程度的能力可以偵測得到。但是因為架構於Rule-based的入侵偵測系統之上，必須要入侵偵測系統能夠辨識的出來並發出警示，才能做出更進一步的判斷。而後續研究亦可針對機率的偵測規則進行修正。

(2) 由於本研究係針對事件資料庫進行資料處理，與入侵偵測系統所使用之廠牌無關。因此，未來全軍所建置之資電戰情中心與資安防護控制中心，如面臨入侵偵測系統各家廠牌互異的問題，亦可以本研究之概念來進行整合，以提供性能提昇之可能性。

(3) 本研究目前僅探討攻擊手法及入侵警示種類之關聯性，然而為求單純，刻意將時間因素省略。舉例來說，本研究將 $X_1 \rightarrow X_3$ 與 $X_3 \rightarrow X_1$ 視為同一種類型。但是若加入時間因素，這兩種狀況則需要分開另外計算。而後續研究可以對此進行更深入的探討。

(4) 在本研究中，係將警示依照ISS的RealSecure之群組，區分為阻絕服務(Denial of Service)、預備攻擊前的偵測(Pre-attack Probe)、通訊協定的特徵(Protocol Signature)、可疑的動作(Suspicious Activity)、以及未經授權的存取(Unauthorized Access Attempt)等五種群組。然而這樣的區分類別是否適當，警示該如何分類，又該如何將警示分配到適當的群組，這些都是另一個值得探究的課題。

參考文獻

[1] CERT/CC, “CERT/CC Statistics 1988-2005,” http://www.cert.org/stats/cert_stats.html #incidents.

[2] CERT/CC, “CERT/CC Statistics 1988-2005,” http://www.cert.org/stats/cert_stats.html#vulnerabilities.

[3] CERT/CC, “Overview of Attack Trends,” http://www.cert.org/archive/.

[4] Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner E., “State of the Practice of Intrusion Detection Technologies,” *Technical Report CMU/SEI-99-TR-028*, CMU/SEI, Jan 2000.

[5] Ranum, J. M., “False Positives: A User’s Guide to Making Sense of IDS Alarms,” ICSA Labs IDSC February 2003 Participating Vendors, http://www.icsalabs.com /html/communities/ids/whitepaper/FalsePositives.pdf, Feb 2003.

[6] Bruneau, G., “The History and Evolution of Intrusion Detection,” http://www.sans.org /rr/whitepapers/detection/, Oct 2001.

[7] Bace1, R., and Mell2, P., “Intrusion Detection Systems,” http://csrc.nist.gov/publications/nistpubs/, Nov 2001.

[8] Hernacki, B., Bennett, J., and Lofgren, T., “入侵偵測系統：誘捕式網路防禦技術的演進,” http://www.symantec.com/region/tw/enterprise/article/mantrap.html.

[9] Case, J., Fedor, M., Schoffstall, M., and David, J., “A Simple Network Management Protocol,” *RFC 1157*, May 1990.

[10] 林順傑、曾憲雄、林耀聰、周志明，”網路行為模式之探勘”，2001 TANET 研討會論文，民國90年10月。

[11] Lee, W., Stolfo, S.J., Mok, K.W., “A data mining framework for building intrusion detection models,” IEEE Symposium on Security and Privacy Proceedings of the 1999, pp.120-132, 1999.

[12]Chan, K. P., and Stolfo, J. S., “On the Accuracy of Meta-Learning for Scalable Data Mining,” *Journal of Intelligent Information System*, Vol. 8, No.1, pp. 5-28, 1997.

[13]丘偉權，”以類神經網路建構入侵偵測系統”，碩士論文，國立成功大學電機工程所，台南，民國90年。

[14]Lei, Z. J., and Ghorbani, A., “Network Intrusion Detection Using an Improved Competitive Learning Neural Network,” *IEEE Second Annual Conference on Communication Networks and Services Research*, pp.190-197, May 2004.

[15]Caberera, J.B.D., Ravichandran, B., Mehra, R. K., and Sci. Syst. Co., Woburn, “Statistical traffic modeling for network intrusion detection,” Proceedings of the 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, pp 466-473, 2000.

[16]Kruegel, C., Mutz, D., Robertson, W., and Valeur, F., “Bayesian event classification for intrusion detection,” *IEEE Computer Security Applications Conference*, pp. 14-23, Dec 2003.

[17]CERT/CC, “CERT/CC Overview-Incident and Vulnerability Trends,” http:// www.cert.org/present/cert-overview-trends/module-4.pdf, pp.5, May 2003.

[18]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/ 95,Jan 1997.

[19]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/ 135,Oct 1996.

[20]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/ 173.

[21]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/ 426, Apr 1995.

[22]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/ 633.

[23]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/405.

[24]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/652.

[25]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/673.

[26]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/406.

[27]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/408.

[28]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/8255,Feb 2002.

[29]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/131.

[30]Internet Security Systems, “X-Force Database,” http://xforce.iss.net/xforce/xfdb/8701,Mar 2002.

[31]TWCERT/CC，”網路安全危機處理”，http://www.cert.org.tw/news/conference/cist_ 20021127_handle.pdf, Nov 2002.

[32]TWCERT/CC，”Windows平台下的安全事件處理”，Aug 2004。

[33]Internet Security Systems, User Guide, http://documents.iss.net/literature/RealSecure/RS_WGM_UG_6.7.pdf, pp.286-288, Sep 2003.

附錄

附錄壹　事件警示分類表

一、預備攻擊前的偵測(Pre-Attack Probe)

事件名稱	威脅程度	類型	次數
UDP_Service_Sweep	1	Pre-attack Probe	74
HTTP_Passwd_Txt	1	Pre-attack Probe	11
HTTP_testcgi	1	Pre-attack Probe	3
TCP_Port_Scan	2	Pre-attack Probe	10658
Ping_Sweep	2	Pre-attack Probe	3772
FTP_Cwd_dotdot	2	Pre-attack Probe	669
TCP_Network_Scan	2	Pre-attack Probe	508
HTTP_URLscan	2	Pre-attack Probe	120
HTTP_ColdFusion_Debug	2	Pre-attack Probe	14
HTTP_Htaccess	2	Pre-attack Probe	11
HTTP_PhpRocket_Traversal	2	Pre-attack Probe	9
SMTP_Probe_Root	2	Pre-attack Probe	8
Email_Expn	2	Pre-attack Probe	4
Email_Vrfy	2	Pre-attack Probe	4
HTTP_NetwareWebserver_Traversal	2	Pre-attack Probe	3
HTTP_NphTestCgi	2	Pre-attack Probe	3
HTTP_Netscape_SpaceView	2	Pre-attack Probe	1
TCP_Service_Sweep	3	Pre-attack Probe	118887
SMB_Service_Sweep	3	Pre-attack Probe	39305
Netbios_Name_Scan	3	Pre-attack Probe	173
pcAnywhere_Probe	3	Pre-attack Probe	71
ICMP_Subnet_Mask_Request	3	Pre-attack Probe	62
pcAnywhere_Ping	3	Pre-attack Probe	61
DNS_Chaos_Request	3	Pre-attack Probe	52
MSRPC_Dump	3	Pre-attack Probe	43
DNS_Version_Request	3	Pre-attack Probe	36
Trace_Route	3	Pre-attack Probe	35
Nessus_Scanner	3	Pre-attack Probe	34
HTTP_Groupwise_Path	3	Pre-attack Probe	14
MSRPC_Security_Id_Lookup	3	Pre-attack Probe	12

Trace_Route_UDP	3	Pre-attack Probe	11
SNMP_Lanman_Enum	3	Pre-attack Probe	8
IIS_Reveal_Address	3	Pre-attack Probe	7
HTTP_Empower	3	Pre-attack Probe	1
小計			174684

二、通信協定的特徵(Protocol Signature)

事件名稱	威脅程度	類型	次數
HTTP_Windows_Executable	1	Protocol Signature	679
SNMP_Packet_Underflow	1	Protocol Signature	36
SNMP_Bad_Variable_Type	1	Protocol Signature	2
SNMP_InvalidTag_OID	1	Protocol Signature	2
SNMP_Value_Underflow	1	Protocol Signature	2
SMB_Guessable_Password	1	Protocol Signature	1
OSPF_Null_Authentication	2	Protocol Signature	86609
HSRP_Default_Password	2	Protocol Signature	1066
HTTP_IIS_Double_Eval_Evasion	2	Protocol Signature	468
SNMP_Counter64	2	Protocol Signature	277
STUN_Message_Attribute	2	Protocol Signature	186
SNMP_TooManyVariables	2	Protocol Signature	160
HTTP_IIS_Percent_Evasion	2	Protocol Signature	123
SNMP_Crack	2	Protocol Signature	102
HTTP_IIS_Hex_Evasion	2	Protocol Signature	91
SMB_Client_Cleartext_Password	2	Protocol Signature	19
SNMP_Set	2	Protocol Signature	14
RDP_Login	2	Protocol Signature	8
HTTP_Trace	2	Protocol Signature	5
Email_Turn	2	Protocol Signature	2
FTP_Site_Cmd	2	Protocol Signature	2
ISAKMP_Vendor_Id	3	Protocol Signature	43419
SNMP_ifTable	3	Protocol Signature	467
MSRPC_Share_Enum	3	Protocol Signature	1236
SMB_Auth_Failed	3	Protocol Signature	1014
TCP_Probe_Telnet	3	Protocol Signature	317
LDAP_Message	3	Protocol Signature	319
STUN_Message	3	Protocol Signature	186
MSRPC_LSASS_Request_Detected	3	Protocol Signature	185
MSRPC_Popup_Message	3	Protocol Signature	62
ICMP_Timestamp_Request	3	Protocol Signature	59
LanMan_Share_Enum	3	Protocol Signature	15
OSPF_Hello_Multicast	3	Protocol Signature	14
SQL_SSRP_Enum_Response	3	Protocol Signature	2
小計			137149

三、可疑的動作(Suspicious Activity)

事件名稱	威脅程度	類型	次數
SMB_Empty_Password	1	Suspicious Activity	499
HTTP_Nimda_Worm	1	Suspicious Activity	124
Mstream_Zombie_Request	1	Suspicious Activity	62
Avaya_Cajun_Default_SNMP	1	Suspicious Activity	43
TCP_Probe_Sub7	1	Suspicious Activity	31
HTTP_Shells_Perl	1	Suspicious Activity	14
HTTP_Shells_Perl_Exe	1	Suspicious Activity	14
TCP_Data_Changed	1	Suspicious Activity	7
HTTP_Apache_Jakarta_Format_String	1	Suspicious Activity	3
HTTP_IndexServer_Source_Disclosure	1	Suspicious Activity	3
HTTP_FaxSurvey	1	Suspicious Activity	2
HTTP_Translate_F_SourceRead	1	Suspicious Activity	1
SQL_SSRP_Slammer_Worm	1	Suspicious Activity	1
FTP_Auth_Failed	2	Suspicious Activity	847
HTTP_Field_With_Binary	2	Suspicious Activity	670
SMB_Winreg_File	2	Suspicious Activity	137
Email_Outlook_URL_Spoof	2	Suspicious Activity	83
Email_Executable_Extension	2	Suspicious Activity	65
HTTP_URL_Bad_Hex_Code	2	Suspicious Activity	29
HTTP_repeated_character	2	Suspicious Activity	9
HTTP_PHPNuke_Admin_Overwrite	2	Suspicious Activity	8
Email_Potential_BO_Attachment	2	Suspicious Activity	6
HTTP_URL_MS_ADC_Samples	2	Suspicious Activity	5
HTTP_IIS_Track	2	Suspicious Activity	4
HTTP_CobaltRAQ_alert	2	Suspicious Activity	3
HTTP_DotDotDot	2	Suspicious Activity	3
HTTP_InterscanViruswall_ChgCfg	2	Suspicious Activity	3
HTTP_Webplus	2	Suspicious Activity	3
Email_Virus_Double_Extension	2	Suspicious Activity	2
HTTP_POST_Script	2	Suspicious Activity	2
SMB_Filename_Overflow	2	Suspicious Activity	2
Email_Relay_Spam	2	Suspicious Activity	1
HTTP_IIS_Bdir_Htr	2	Suspicious Activity	1
HTTP_IIS_Trailing_Incomplete_Unicode	2	Suspicious Activity	1
HTTP_Fields_With_Binary	2	Suspicious Activity	1

HTTP_Frontpage_Path	3	Suspicious Activity	1072
DCOM_SystemActivation	3	Suspicious Activity	140
Echo_Reply_Without_Request	3	Suspicious Activity	62
HTTP_URL_dotpath	3	Suspicious Activity	21
FTP_Commands_With_Binary	3	Suspicious Activity	16
Email_Error	3	Suspicious Activity	15
DNS_Malformed	3	Suspicious Activity	14
HTTP_WebFinger	3	Suspicious Activity	14
Telnet_Abuse	3	Suspicious Activity	12
HTTP_Auth_Failed	3	Suspicious Activity	11
SMB_Executable_Access	3	Suspicious Activity	9
HTTP_Tilde	3	Suspicious Activity	8
HTTP_Domino_Web_Access	3	Suspicious Activity	3
DCOM_RemoteActivate	3	Suspicious Activity	2
DNS_NonInternet	3	Suspicious Activity	2
Email_Encap_Relay	3	Suspicious Activity	2
小計			4092

四、未經授權的存取行為(Unauthorized Access Attempt)

事件名稱	威脅程度	類型	次數
UDP_Port_Scan	1	Unauthorized Access Attempt	399
HTTP_Unix_Passwords	1	Unauthorized Access Attempt	368
POP_Command_Overflow	1	Unauthorized Access Attempt	308
FTP_Invalid_Port_Cmd	1	Unauthorized Access Attempt	278
HTTP_FileTypeLnk	1	Unauthorized Access Attempt	201
MSRPC_LSASS_Bo	1	Unauthorized Access Attempt	185
HTTP_Cisco_IOS_Admin_Access	1	Unauthorized Access Attempt	180
FTP_List_dotdot	1	Unauthorized Access Attempt	110
HTTP_GET_DotDot_Data	1	Unauthorized Access Attempt	99
MSRPC_RemoteActivate_Bo	1	Unauthorized Access Attempt	75
BackOrifice_Ping	1	Unauthorized Access Attempt	69
HTTP_DotDot	1	Unauthorized Access Attempt	59
Sasser_Propagation	1	Unauthorized Access Attempt	49
Cisco_ILMI_SNMP_Community	1	Unauthorized Access Attempt	44
HP_OpenView_SNMP_Backdoor	1	Unauthorized Access Attempt	41
Sun_SNMP_Backdoor	1	Unauthorized Access Attempt	23
Cisco_Cable_Docsis_SNMP_Community	1	Unauthorized Access Attempt	39
WinTrin00_Daemon_Request	1	Unauthorized Access Attempt	31
Trin00_Daemon_Request	1	Unauthorized Access Attempt	28
FTP_Glob_Implementation	1	Unauthorized Access Attempt	23
HTTP_Content_Disposition_DotDot	1	Unauthorized Access Attempt	17
FTP_Cwd_Overflow	1	Unauthorized Access Attempt	16
HTTP_Dir_Manager_exe	1	Unauthorized Access Attempt	15
HTTP_Listrec_Execute	1	Unauthorized Access Attempt	12
HTTP_Hassan_Execute	1	Unauthorized Access Attempt	11
FTP_User_Root	1	Unauthorized Access Attempt	9
HTTP_IIS_Trailing_Slash	1	Unauthorized Access Attempt	9
HTTP_IERedir_Zone_Bypass	1	Unauthorized Access Attempt	8
HTTP_ColdFusion_Expr_Evaluator	1	Unauthorized Access Attempt	6
HTTP_TektronixPrinter	1	Unauthorized Access Attempt	6
SNMP_Cisco_VACM_MIB	1	Unauthorized Access Attempt	5
HTTP_Content_Type_HTA	1	Unauthorized Access Attempt	4
Telnet_Too_Many_AYTs	1	Unauthorized Access Attempt	4
HTTP_$DATA_Source_Disclosed	1	Unauthorized Access Attempt	3
HTTP_BAT_Execute	1	Unauthorized Access Attempt	3

HTTP_Campas	1	Unauthorized Access Attempt	3
HTTP_Cdomain	1	Unauthorized Access Attempt	3
HTTP_Guestbook	1	Unauthorized Access Attempt	3
HTTP_HTDIG_htsearch	1	Unauthorized Access Attempt	3
HTTP_HTMLScript	1	Unauthorized Access Attempt	3
HTTP_PHF_CommandExec	1	Unauthorized Access Attempt	3
HTTP_SGI_Infosrch	1	Unauthorized Access Attempt	3
HTTP_webgais	1	Unauthorized Access Attempt	3
HTTP_Websendmail	1	Unauthorized Access Attempt	3
HTTP_WebSite_Uploader	1	Unauthorized Access Attempt	3
HTTP_Webspeed_Admin	1	Unauthorized Access Attempt	3
SMB_Admin_Sneak	1	Unauthorized Access Attempt	3
FTP_Cwd_Root	1	Unauthorized Access Attempt	2
LDAP_Server_ASN1_Overflow	1	Unauthorized Access Attempt	2
MSRPC_Registry_Permissions	1	Unauthorized Access Attempt	2
POP_Response_Client_Bo	1	Unauthorized Access Attempt	2
FTP_Retr_Very_Long	1	Unauthorized Access Attempt	1
FTP_Size_Very_Long	1	Unauthorized Access Attempt	1
HTTP_CobaltRAQ_OverflowCGI	1	Unauthorized Access Attempt	1
HTTP_FileTypeUrl	1	Unauthorized Access Attempt	1
HTTP_IIS_Unicode_Encoding	1	Unauthorized Access Attempt	1
HTTP_JRun_Double_Slash	1	Unauthorized Access Attempt	1
HTTP_PHPMyAdmin_Sql_Include	1	Unauthorized Access Attempt	1
LPRng_Format_String	1	Unauthorized Access Attempt	1
SNMP_Default_Backdoor	2	Unauthorized Access Attempt	1418
HTTP_POST_repeated_char	2	Unauthorized Access Attempt	1302
HTTP_OWC_Vulnerable_Client	2	Unauthorized Access Attempt	64
HTTP_URL_repeated_char	2	Unauthorized Access Attempt	24
FTP_PrivilegedPort	2	Unauthorized Access Attempt	16
FTP_Port_Bounce	2	Unauthorized Access Attempt	14
POP3_Auth_Failed	2	Unauthorized Access Attempt	13
HTTP_Cross_Site_Scripting	2	Unauthorized Access Attempt	11
HTTP_Axis_Storpoint	2	Unauthorized Access Attempt	10
HTTP_WebPALS	2	Unauthorized Access Attempt	10
HTTP_Carbo_Server	2	Unauthorized Access Attempt	9
HTTP_YaBB	2	Unauthorized Access Attempt	9
HTTP_Squid_ACL_Bypass	2	Unauthorized Access Attempt	8
HTTP_Zero_Hex_Code	2	Unauthorized Access Attempt	8

HTTP_POST_dotdotdot_data	2	Unauthorized Access Attempt	7
HTTP_IndexServer_IDQ	2	Unauthorized Access Attempt	6
HTTP_BigBrother_History	2	Unauthorized Access Attempt	5
HTTP_Commerce	2	Unauthorized Access Attempt	5
HTTP_Pfdispaly_Read	2	Unauthorized Access Attempt	5
HTTP_POST_dotdot_data	2	Unauthorized Access Attempt	5
HTTP_WebStore_Misconfig	2	Unauthorized Access Attempt	5
FTP_Retr_dotdot	2	Unauthorized Access Attempt	4
HTTP_StoreCGI	2	Unauthorized Access Attempt	4
Allaire_JRun_Sample_Files	2	Unauthorized Access Attempt	3
Allaire_JRun_WebInf_DotSlash	2	Unauthorized Access Attempt	3
FTP_dotdotdot	2	Unauthorized Access Attempt	3
HTTP_Cachemgr	2	Unauthorized Access Attempt	3
HTTP_EZMall_Malllogfile	2	Unauthorized Access Attempt	3
HTTP_IIS3_Asp_Dot	2	Unauthorized Access Attempt	3
HTTP_KnowledgeBuilder_CodeExecution	2	Unauthorized Access Attempt	3
HTTP_PHP_ReadFile	2	Unauthorized Access Attempt	3
HTTP_Road_Search	2	Unauthorized Access Attempt	3
HTTP_SendTempPl	2	Unauthorized Access Attempt	3
HTTP_Sojourn	2	Unauthorized Access Attempt	3
HTTP_URL_NewDsnExe	2	Unauthorized Access Attempt	3
HTTP_Wayboard_Fileview	2	Unauthorized Access Attempt	3
HTTP_Webinf_Dot_FileRetrieval	2	Unauthorized Access Attempt	3
HTTP_WebLogic_FileServlet_ShowCode	2	Unauthorized Access Attempt	3
HTTP_Weblogic_SSIServlet_ShowCode	2	Unauthorized Access Attempt	3
Telnet_Password_Overflow	2	Unauthorized Access Attempt	3
FTP_Unix_RemoteHost_File	2	Unauthorized Access Attempt	2
HTTP_IIS_Obtain_Code	2	Unauthorized Access Attempt	2
FTP_Size_dotdot	2	Unauthorized Access Attempt	1
HTTP_BrownOrifice	2	Unauthorized Access Attempt	1
HTTP_JSP_SourceRead	2	Unauthorized Access Attempt	1
HTTP_NT8.3_Filename	2	Unauthorized Access Attempt	1
MSRPC_Share_Enum_Sweep	3	Unauthorized Access Attempt	22
Telnet_Login_Overflow	3	Unauthorized Access Attempt	12
Email_Invalid_Command	3	Unauthorized Access Attempt	4
FTP_Fname_Lnk	3	Unauthorized Access Attempt	3
SMTP_Malformed_Rcpt_Cmd	3	Unauthorized Access Attempt	1
小計			5852

五、阻絕服務攻擊(Denial of Service)

事件名稱	威脅程度	類型	次數
HTTP_Generic_Intel_Overflow	1	Denial of Service	8
Kerberos_ASN1_Overflow	1	Denial of Service	3
Smurf_Attack	2	Denial of Service	7479
HTTP_Lock_Method_DOS	2	Denial of Service	346
HTTP_Frontpage_Publish	2	Denial of Service	288
ICMP_Unreachable_Storm	2	Denial of Service	76
ICMP_Flood	2	Denial of Service	30
HTTP_IISExAir_DOS	2	Denial of Service	11
Fraggle_Attack	2	Denial of Service	6
SYN Flood	2	Denial of Service	6
HTTP_Apache_DOS	2	Denial of Service	1
HTTP_ColdFusion_Admin	2	Denial of Service	1
HTTP_URL_Many_Slashes	2	Denial of Service	1
HTTP_URL_Name_Very_Long	2	Denial of Service	1
ICMP_Protocol_Unreachable_TCP	2	Denial of Service	1
Portmaster_Reboot	2	Denial of Service	1
FTP_Windows_Drive_Path	3	Denial of Service	3133
HTTP_CobaltRAQ_service	3	Denial of Service	3
HTTP_ZmlCgi	3	Denial of Service	3
小計			11398

自傳

作者刁建強(Chien-Chiang Tiao)，民國60年3月1日出生於台北市，民國79年於國立台灣師範大學附屬高級中學畢業後，旋即考入中正理工學院電子科電算組81年班就讀，畢業後分發至陸軍獨立51旅(現陸軍裝步351旅前身)擔任排長、及營通信官等職務。復於83年考入中正理工學院資訊科學系就讀，於民國86年畢業後，回到陸軍獨立51旅接任副連長、及旅作戰科通信官等職務。於旅作戰科通信官任職期間，有感於通資安全之重要性，民國89年考入通資安全正規班第一期就讀，並於89年8月調任陸軍總司令部通信電子資訊署資訊中心資訊戰緊急應變科，專門負責資訊戰等相關工作。於92年8月進入國防大學中正理工學院資訊科學所實務組進修碩士學位。