入侵防禦系統設計之研究

陳毓璋 李俊毅 高志孝 楊陳俊
樹德科技大學 資訊工程系
sclass@ms1.hinet.net s94639101@mail.student.stu.edu.tw
s95639102@mail.student.stu.edu.tw s92113107@mail.student.stu.edu.tw

摘要

現今資訊越來越發達，每個人對於網路的需求量越來越大，網路上所存在的危險性也越來越大。尤其目前無線網路的興起，提供使用者更加方便的網路環境。因此，隨時隨地上網的願景遂成為可能，無線網路雖然帶來便利，但也可能形成企業資訊安全防護上的漏洞。

本文主要讓管理者進行安全管理及行為分析，提升入侵行為的辨識率，並達到流程自動化和提供即時反制能力。本文系統重點在於可即時偵測、防範來自異質網路攻擊及入侵行為，如果入侵發生，系統可立即採取回應與隔絕措施，以確保網路使用者及重要主機的安全。

關鍵詞：網路安全、入侵偵測、入侵防禦、蜜罐

Abstract

At the present, the technology is keep getting improved, the requirement of Internet to everyone is getting more, and that make Internet become more danger. Especially the wireless network is more popularize, provide more convenient network environment for everyone. Therefore, connect to the Internet at any time anywhere become possible, although the wireless network brings the convenience, but also may a loophole for the business network security.

The main of this article tell user to work on security management and the behavior analysis, to upgrade the rate of invaded recognize, also achieved the process support auto anti-invaded. The main goal of this article is to detect and protect automatically from the heterogeneous network attack and the invaded. If invasion has occurrence, the system will be response and separate immediately, so it can guarantees of user and the server computer in this system security.

Keywords: Network security、Intrusion Detection、Intrusion Prevention、Honey pot

1. 前言

隨者資訊科技以及網際網路技術不斷的進步，人們也越來越習慣在網路上進行各式交易、個人金融等各種服務，但伴隨而來的卻是更多危害系統的技術，如駭客入侵、木馬、蠕蟲、病毒攻擊..等，充斥於整個網際網路。而 Internet 本身如同雙面刃一樣，在使用的同時也威脅到系統的安全性，且越來越多的重大網路攻擊事件，也顯示資訊安全的重要性。

傳統入侵偵測系統防禦的效果不足，當偵測到異常行為連線時，只能發出警告訊息，而入侵防禦系統 IPS (Intrusion Prevention System, IPS)則會在偵測到異常行為連線時，除了能夠發出警告訊息通知管理者，也能依照系統所設定的條件進行對應的防禦動作。但以目前現有的 IPS 系統，大多僅能依照現有的特徵進行比對，或需管理者手動輸入特徵行為資料來提升辨別率，其成效僅能將連線分類為正常或異常連線，無法辨別可疑連線。本系統結合入侵防禦系統、網路管理系統及鏡像防護系統(Mirror System)，將辨別為可疑連線導入鏡像防護系統，進而記錄並分析該連線的行為，最後再將其特徵加入特徵資料庫中，用來增加日後異常行為連線的辨別率，以便解決行為特徵缺乏的問題，進而達到提升正確率與減少誤判的機率。

如何提供管理者進行安全管理及行為分析，提升入侵行為辨識率，以及達到流程自動化以及即時的反制能力，隔離不必要的危險行為，讓網路使用者能夠安心的存取有線及無線網路，並隔絕惡意人士進入網路，是本文欲達成的目的。

2. 文獻探討

2.1 入侵偵測簡介

入侵偵測系統(Intrusion Detection System，IDS) [1][2][6]在網路裡扮演著監控網路中各項活動的警衛，大部分的 IDS 都是以解讀各種封包內容、執行網路流量監測或是分析系統紀錄等方式來找尋可能入侵的行為，並且做出適當的反應。根據這種特性可以發現IDS 需要一套規則來判定是否該行為已達到入侵的意圖，這些規則就是所謂的特徵(signatures)，符合特徵就可以判定為蓄意的入侵或有攻擊的意圖。若是特徵定得太鬆或者太嚴，都會失去使用的意義，因此，IDS 最重要的部分就是在於特徵的訂定。

2.1.1 入侵偵測技術介紹

2.1.1.1 Signature-based detection

類似病毒軟體掃描的方式，將每一個入侵事件事先定義好，並且給予它們識別標誌或序號，當攻擊發生時，系統便可立即發現進而保護系統。其優點是降低攻擊誤判率（false positive rate），因為攻擊手法都是定義完整的，但缺點是若出現尚未定義過的入侵攻擊事件時就無法正確的判定。

2.1.1.2 Anomaly-based detection

事先將正常的操作行為定義成範本（profile），把其他的偏差行為(deviations)當成是入侵事件，並會隨即對正常行為範本做更新。其優點是可偵測出以往從沒發生過的攻擊，缺點則是攻擊誤判率較高，因為使用者的行為模式很難預測。

2.1.1.3 Specification-based detection

是先定義出程式或通訊協定正確運作的限制條件（constraints），並根據這些條件監控程式的執行狀況。此偵測技術不但可偵測出以往從沒發生過的攻擊，同時它也能降低攻擊誤判率。

2.1.2 入侵偵測系統部署方式

入侵偵測系統依照偵測的範圍可以分為Network-Based (網路端部署)以及 Host-Based (本機端部署)二種[3][8]。

2.1.2.1 Network-Based (網路端部署)

網路是入侵者最可能選擇的攻擊路徑，所以威脅評估的掃描器也必須從網路上進行，模擬可能敵人的掃描、入侵、甚至暴力的服務阻斷動作，以便檢查自身網路面對來自網路的威脅時，可能的安全漏洞。另外，也可以用軟體在網路上對來往通信進行即時偵測。

2.1.2.2 Host-Based (本機端部署)

雖然網際網路是最可能的威脅來源，但並不是唯一。敵人仍然可能潛入組織內部、或者買通內部人員而實際接觸到重要電腦主機，竊取資料或埋設方便日後入侵的木馬程式。因此對每台重要主機需要專門的貼身護衛監視可疑的操作，以及可針對系統安全漏洞的稽核工具。

2.2 入侵防禦簡介

入侵防禦系統（Intrusion Prevention System，IPS）[4][9]簡單來說就是 IDS 入侵偵測系統的加強版，除了可以擁有 IDS 偵測發出警訊的功能，更重要的就是 IPS 能夠主動地將符合資格的攻擊行為給立即地斬斷，可依照 IP 位址、協定、服務..等，將符合資格的攻擊行為的特徵立即停止、丟棄攻擊封包、防止惡意封包的傳送，並透過流量的狀態分析來檢測入侵行為。

2.2.1 入侵防禦系統部署方式

以 IPS 所檢視分析對象的資料來源來看，分成網路型入侵防禦系統(Network IPS)，也就是檢視分析的對象來源是網路上傳輸的封包，透過檢查網路封包內容的方式來防範是否有入侵行為，故稱為網路型的 IPS。主機型入侵防禦系統(Host IPS) ，也就是檢視分析的來源是重要主機上的一些日誌檔案或目錄，透過檢查這些主機上檔案目錄的狀態完整性來防範是否有入侵行為，故稱為主機型的 IPS。

2.2.2 入侵防禦系統防禦機制

IPS 針對進入系統的資料依照資料鏈結層、網路層、傳輸層、應用層的資料進行檢查，並且依照所設定的動作主動回應，如表 1 所示。

表 1　IPS 防禦機制

資料鏈結層	觀察並控制因攻擊產生的大量資料量，設定在一段時間內一個允許傳輸的資料量，若超過此量則採取相對應的回應動作。
網　路　層	當系統識別出可疑的攻擊來源端位址後，就把所有來自此來源位址的網路封包全部丟棄，使得來源端無法進一步與目的端連線而達成防禦的效果。
傳　輸　層	將識別為攻擊行為後阻斷封包的連接至目的連接埠的連線，使得攻擊者收到無法到達目地端的錯誤訊息，進而達到防禦效果。
應　用　層	將可疑資料的封包給丟掉或拒絕掉，並可以針對封包內容進行修改或替換。

2.2.3 入侵防禦系統與入侵偵測系統比較

IDS 在偵測到攻擊行為時，並不會即時性處理，導致系統一樣遭受到攻擊，但 IDS 的架構並不影響現有的網路架構，且網路透通性佳、誤判亦無影響。IPS 雖在偵測攻擊行為可即時性的處裡，但架構複雜、不易與現有網路結合，且若特徵比對不完全，則會造成誤判，影響到合法使用者的權利。

2.3 入侵誘捕系統簡介

Honey pot[9]是專為引誘潛在的駭客而設計，使他們遠離網路上重要的系統。Honey pot 應被部署在整個企業與財務單位中，並與網路型與主機型 IDS 一起運作。Honey pot 可偵測到慢速掃描(當其他 IDS 無法做到時)使它可以作為一種輔助性的解決方案。這個系統看起來要很像是真的，有真的資料、夠重要的資料來使攻擊者持續被吸引，同時捕捉到他們。一旦捕捉到攻擊者時，你就可以知道他是如何得逞的，隨時瞭解針對此網路區域發動的最新的攻擊和漏洞。

3. 研究方法

依照前面所探討的問題，可以發現現有防護系統無法自行新增特徵行為比對，必須依靠管理人員自行新增，若管理人員無法即時新增比對偵測規則，將會讓內部所保護的系統遭受新的攻擊威脅。現有 Honey Pot 系統可雖監控連線行為模式，但若該連線為正常行為，會造成使用者在 Honey Pot 系統內做的行為是無用行為，讓使用者花費額外時間在 Honey Pot 系統白費工夫。本文依照前面所討論出的問題，來設計整個系統。

3.1 系統架構

圖一為本文所設計的系統架構，系統可透過 Mirror System 偵測可疑連線相關行為，若該連線為正常連線，可讓該連線在受保護主機中做相同動作，也可透過偵測可疑行為分析，新增入侵行為特徵，讓內部保護網路不會受到較新的攻擊威脅。

本系統架構規劃方式如圖五所示，下列為各子系統設備功能說明：

(1) Attacker

- 利用網路攻擊工具在此電腦上透過有線或無線網路向 Target A/B 進行攻擊與入侵行為。

(2) Target A/B

- 利用伺服器及網路上的安全漏洞，作為 Attacker 之網路攻擊目標。

(3) Mirror A/B

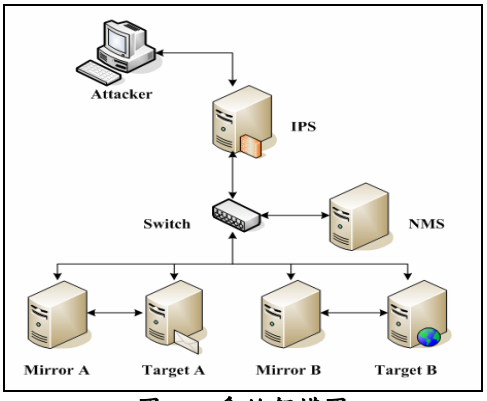
- 於使用者執行命令時，可透過監聽程式將傳輸至系統核心的指令複製一份，與系統限制規則進行比對。
- 使用者執行命令後，可查核系統記錄及系統資源，檢查是否有執行超出系統權限的行為。

(4) IPS Server

- 偵測流進/流出內部網路的封包，比對網路攻擊特徵資料。
- 依照網管人員所制定的規則，對網路入侵及攻擊行為執行對應防護動作。
- 當內部網路遭受攻擊及入侵行為時，可發佈攻擊警報至網管系統及管理者。

(5) NMS Server

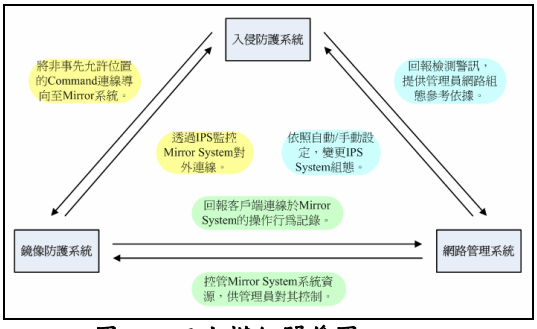
- 網路流量與設備狀態監控及記錄。
- 提供網管人員在網路上進行管理安全防護系統設定的環境。



圖一　系統架構圖

3.2 系統模組

圖二為本系統架構，功能可分為三大模組系統：入侵防護系統、鏡像防護系統及網路管理系統。模組系統之間相互依賴溝通，可確實達到防護的功能。採用模組化的設計，主要考慮到往後系統若有需要增加其他模組系統，可以很快的增加至系統環境內，並且不需要更改現有的系統環境。



圖二　三大模組關係圖

3.2.1 入侵防護系統與鏡像防護系統

入侵防護系統在解析進入內部網路的封包後，會將符合行為特徵的封包丟棄。反之，則會針對即將進入內部網路的該封包之目的埠號進行分析，找出是否為屬於使用 Telnet 或 SSH 協定的封包，再檢查封包的來源位置，當該封包來源位置是屬於不被允許與受保護的主機進行直接連線，系統會將該封包轉送至鏡像防護系統。

使用者於鏡像防護系統上，對於外部網路的存取依然受到入侵防禦系統監控，並且在使用者離開內部網路時，會由入侵防禦系統將封包內的原始來

源位置取代為該鏡像防護系統所保護的主機位置。

3.2.2 鏡像防護系統與網路管理系統

鏡像防護系統會記錄使用者在系統上的一舉一動，以及使用者所執行指令的系統回應訊息，並依據事先所定義的規則判別其執行的指令及回覆進行行為，若該使用者的行為未違反事先所定義的規則時將會轉送封包至內部網路中的真實主機；反之，將會被強制中斷該連線，當使用者連線中斷後，鏡像防護系統將會所記錄到的特徵行為資料傳送至網路管理系統內存放。

當網路管理系統接收到來自鏡像防護系統的訊息之後，會將訊息分析處理並且儲存至特徵行為資料庫中，再查詢並且分析該使用者所使用的網路位置歷史使用記錄，系統會依據網管人員所制定規則條件將該網路位置加入或移出正常連線位置，用以提供往後入侵分析系統在做為比對封包特徵行為的依據。

3.2.3 網路管理系統與入侵防護系統

入侵防護系統在解析進入內部網路的封包後，會將符合攻擊特徵的封包丟棄，並且把該攻擊的時間、來源位置及攻擊型態等相關資料傳至網管理系統內的特徵行為資料庫儲存，作為提供網管人員做為調整系統及網路安全組態的參考依據。

網路管理系統在接收到來自入侵防護系統的訊息之後，會將訊息分析處理並儲存至特徵行為資料庫中，再依照管理者事先所設定的特徵行為比對規則條件，進行該次入侵攻擊行為做分析，最後依據網管人員所設定的特徵行為比對規則，進行通知網管人員或自動變更入侵防禦系統的相關組態。

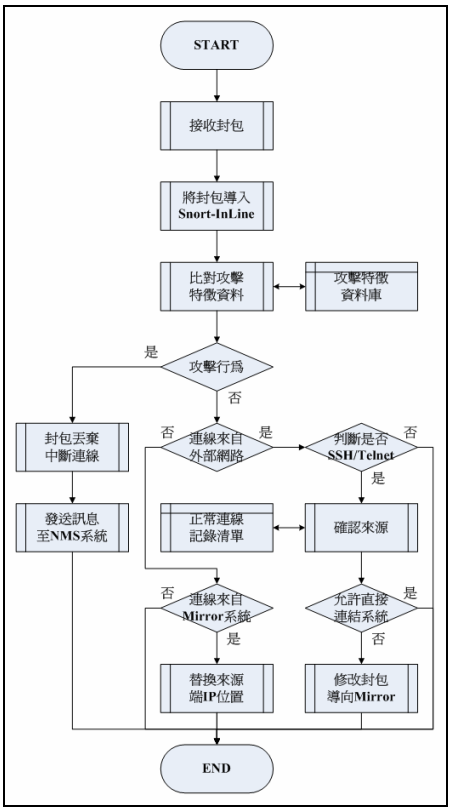
3.2.4 入侵防禦系統動作流程

圖三為入侵防禦系統流程圖，當外部網路的封包經由入侵防禦系統流入內部受保護網路時，入侵防禦系統會先由 iptable 將流入的封包放入佇列當中，然後將佇列中的封包導向至 Snort-InLine 中做分析及處理，當 Snort-InLine 接收到封包後，會將分析封包中的資訊，並且與特徵行為資料庫中所記錄的特徵資料進行比對動作，用來判斷該封包是否屬於網路攻擊的封包。

當特徵的比對是符合時，即表示該封包為網路入侵攻擊的封包，系統將會把封包丟棄，並且發出包含攻擊的時間、攻擊來源及目的位置、攻擊型態等相關的特徵行為訊息通知網路管理系統；反之，系統會檢查封包是否來自外部網路，藉以進行不同的處理方法，因為只有來自外部網路的連線封包，才可進行連線執行指令的偵測檢查。

當該封包來自於外部網路時，系統會再檢查封包的目的埠號，判斷該封包是否為連結至 Telnet 或 SSH 服務的封包，若是則系統會將該封包與事前定義的正常連線清單做比對，以確認該封包的來源位置是否為允許直接連結至受保護主機正常連線清單的一員。如果該封包的來源位置為允許直接連結至受保護主機的一員，Snort-InLine 將修改封包內的目的位置，而用鏡像防護系統的位置取代之，再將封包轉送至鏡像防護系統內進行檢測。

當該封包為來自內部網路時，系統會檢查該封包的來源位置是否為鏡像防護系統的位置，若封包的來源位置為鏡像防護系統的位置，則 Snort-InLine 將修改封包內的來源位置，把鏡像防護系統所保護的主機位置取代封包中來源位置。



圖三　入侵防禦系統動作流程圖

3.2.5 鏡像防護系統動作流程

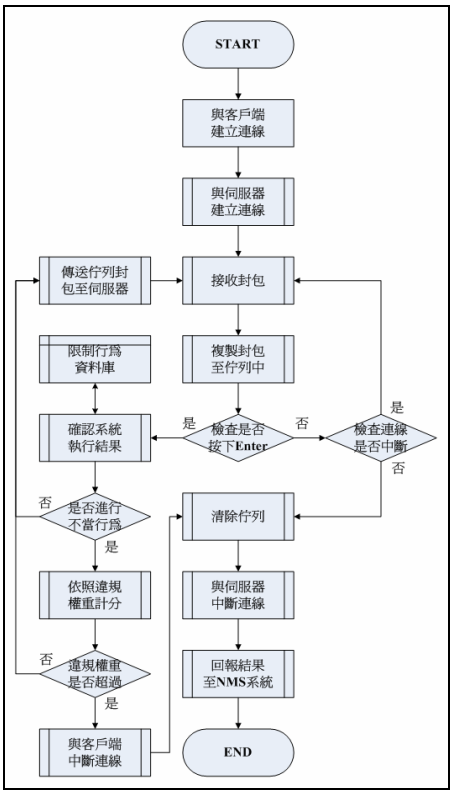
圖四為鏡像防護系統流程圖，當客戶端與鏡像防護系統建立連線時，系統會與客戶端欲連線的受保護主機建立連線，此行為是用來轉送檢測過的指令至受保護主機使用。當鏡像防護系統接收到來自客戶端封包時，會將該封包複製一份至佇列中存放，主要檢查若該封包的行為特徵為正常行為，會在受保護主機上做相同動作執行，並持續檢查使用者是否送出 Enter 的訊號，以便檢查使用者所執行的指令，並且持續檢查與客戶端的連線是否中斷。

當使用者送出 Enter 訊號之後，系統會抓取執行 Enter 之前所輸入的指令時，鏡像防護系統會檢查使用者所輸入的指令與指令執行之後的系統回應資訊，並與系統內所事先定義的限制行為資料庫

進行比對，若使用者執行的指令沒違反限制行為資料庫所定義的規則時，將會把佇列中的封包傳送至受保護的主機執行同樣的動作；反之，將針對所違反的規則權重進行計算。

如果使用者違規行為經由系統計算後沒有超出網管人員定義的標準時，系統將會把佇列中的封包傳送至受保護的主機執行；反之，將會中斷與該客戶端的連線。

當與客戶端連線中斷時，系統將清除佇列中存放的封包資料、中斷與伺服器的連線，之後會將使用者為於鏡像防護系統上所執行的記錄，包含時間、使用者來源端位置、執行的指令、系統回應資訊等相關資料回傳至網路管理系統作儲存，作為往後系統在比對是否為入侵攻擊行為的相關依據。



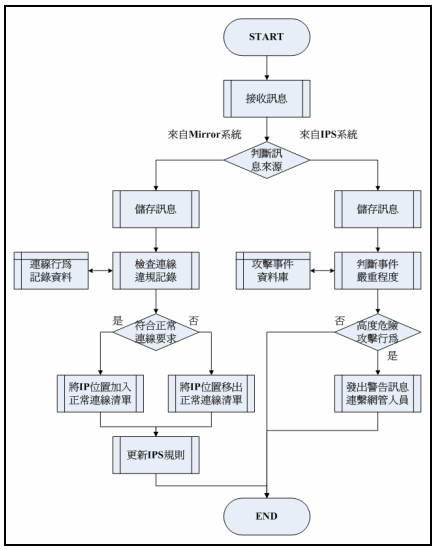
圖四　鏡像防護系統動作流程圖

3.2.6 網路管理系統動作流程

圖五為網路管理系統流程圖，網路管理系統在接收到回報的訊息時，會先判斷該回報訊息是來自入侵防禦系統或是來自鏡像防護系統，進行訊息的分析處理，並且依據訊息的來源位置進行儲存訊息至特徵資料庫中供系統往後的後續處理及備查。

當訊息來自入侵防禦系統時，網路管理系統會依照特徵資料庫中所定義的相關的攻擊行為資訊，進行危險性分析，若經由分析之後，得知該次攻擊是屬於高度危險性的攻擊行為，則系統會發出警告訊通知網管人員，以便網管人員做相關處裡。

當訊息來自於鏡像防護系統時，網路管理系統將檢查特徵資料庫中以往的連線特徵行為記錄，再依據網管人員所制定的規則進行分析及比對，如果該訊息符合網管人員所制定的規則，系統會將該來源位置加入正常連線清單中，反之，系統會將該來源位置從正常連線清單中移出，最後將正常連線清單傳送至入侵防禦系統，作為入侵防禦系統往後在判斷連線的相關依據。



圖五　網路管理系統動作流程圖

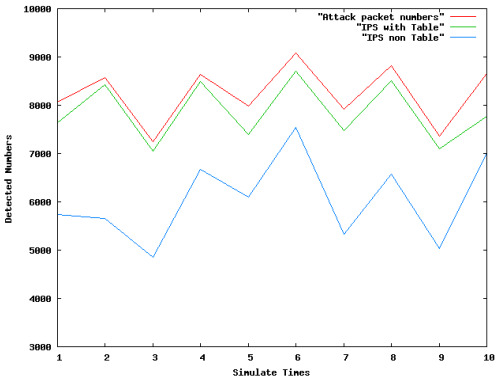
4. 系統模擬

圖六為採用本文所設計的方法及一般方式所偵測出的攻擊數目比較圖，本文所設計方式主要有著高學習性，會依照管理者所自定的規則，去判定某個時間點所進入封包的攻擊權值，若攻擊權值大於管理者所制定數值，系統會自動直接做相關的處裡並且將此一封包的攻擊行為特徵做紀錄，往後若有相同的攻擊行為特徵發生，系統將不會計算權值，則會直接做相關處裡。一般的偵測方式會去檢測每一個封包內容去計算權值，若此連線封包確認為攻擊行為，行為特徵並不在系統內部資料庫，偵測出的權值有可能小於管理者的數值，進而造成誤判。本模擬進行 10 次攻擊，每次模擬傳送 10,000 個封包，其中包含攻擊行為及正常行為的封包，而攻擊封包採用隨機產生，本模擬所採用的攻擊行為皆為系統內部資料庫內無特徵行為紀錄的攻擊。

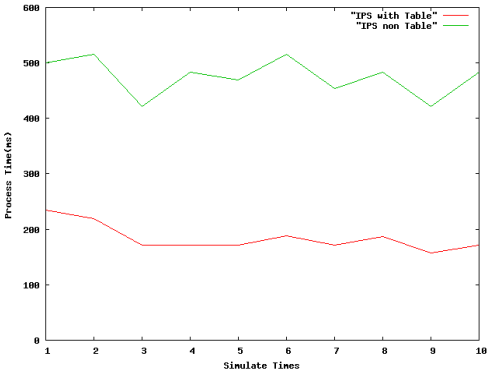
圖七為系統偵測 10,000 個封包的執行時間，本文所設計的方式，一開始系統會對每一個封包內容進行檢測及計算權值，若為此封包是攻擊行為封包，系統會將此一封包特徵紀錄至資料庫內，之後會先依照資料庫內的特徵做比對；若在資料庫內查無特徵行為才會進行檢測封包內容，一般方式則需要對每一個封包內容進行檢測並且計算其權值，故花費時間會比較多。

圖八為鏡像防護系統與 Honey pot 指令執行的比例，在鏡像防護系統內若使用者所執行的指令不在系統黑名單內，系統會自動將指令傳至內部主機執行，以防止使用者攻擊內部主機。而 Honey pot

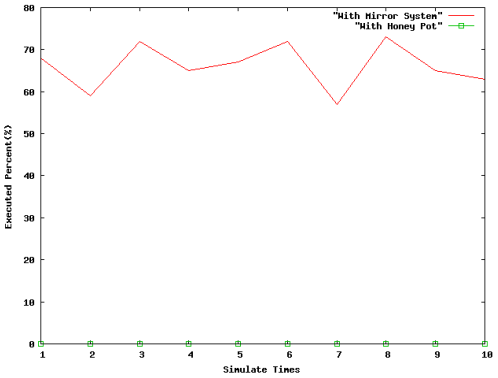
只記得使用者於 Honey pot 所執行的指令，而無法將指令傳至內部主機執行，反之，則會無法達到使用者真正的目的。



圖六　偵測攻擊數比較



圖七　系統偵測封包執行時間



圖八　指令執行比例

5. 結論

從以上的模擬測試可看出本文所提出的方式可確實提供系統偵測攻擊行為的辨識率，並且系統可自行將攻擊行為特徵紀錄於系統內的特徵資料庫內，作為之後比對封包的依據。本文的系統中的特徵資料庫內資訊可不斷新增，系統可不必檢測每一個封包內容，就可知道此一封包是否屬於攻擊行為，整體執行效率會比一般系統高，而一般系統內的資料庫無法自動新增新的攻擊行為，只能針對未知的封包內容做檢測及計算。

以往只能可疑連線導入 Honey pot 中，若此連線不屬於攻擊行為，會讓使用者在系統中所執行的動作無法達到目的，進而降低使用效率。而本系統所設計鏡像防護系統會依照使用者於系統內執行的指令，作權值的計算，若權值未達到系統內所管理者制定的數值，會將使用者在系統內所執行的指令轉送至內部主機執行，讓使用者可以真正達到目的，而不會浪費過多時間做無意義的動作。

誌謝

本研究承蒙國科會計畫經費之補助，計畫編號 NSC-95-2745-E-366-005-URD，特此致謝。

參考文獻

[1] D.Anderson, T.Frivold and A.Valdes, “Next-generation Intrusion Detection Expert System(NIDES)”, Technical report, SRI-CSL-95-07, Computer Sience Lab, SRI International, 1995.

[2] Dong Seong Kim, Ha-Nam Nguyen, Jong Sou Park ,“Genetic Algorithm to Improve SVM Based Network Intrusion Detection System”, Advanced Information Networking and Applications, 19th International Conference on, pp155-158, 2005.

[3] E. Biermann et al., “A comparison of Intrusion Detection systems”, Computer & Security, Elsevier, pp676-683, 2001.

[4] Jakub Botwicz, Piotr Buciak, and Piotr Sapiecha ,”Building Dependable Intrusion Prevention Systems”, Dependability of Computer Systems, DepCos-RELCOMEX '06. International Conference on, pp135-142, 2006.

[5] J. Levine, R. LaBella, H. Owen, D. Contis and B. Culver.,” The Use of Honeypots to Detect Exploited Systems Across Large Enterprise Networks”, Proceedings of the 2003 IEEE Workshop on Information Assurance, pp92-99, 2003.

[6] Joseph S. sheriff, Rod Ayers, “Intrusion detection: Methods and system. Part II” , Information Management and computer security, pp222-229, 2003.

[7] J. Sherif, T. Dearmond, “Intrusion Detection: Systems and Models”, Proceedings of 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02), pp115-133, 2002.

[8] Paul E. Proctor, The Practical Intrusion Detection Handbook, Prentice Hall, 2000.

[9] Xinyou Zhang,Chengzhong Li,Wenbin Zheng,” Intrusion Prevention System Design”, Computer and Information Technology, 2004. CIT '04. The Fourth International Conference on, pp386-390, 2004.