資訊謀略戰—
誘捕式網路防禦技術之研究

作者/賴威良上尉、李武耀少校、廖秀華中尉

提要

「資電優勢」與「資電作戰」是國軍作戰構想中強調的兩大課題，資訊攻擊是屬於不對稱戰爭中最省經費，且最具效益，影響最深遠的攻擊手段。例如在波灣戰爭中，美國將病毒晶片嵌入在送往伊拉克作戰指揮中心的印表機中，進而造成整個作戰指管中心癱瘓，此例即可顯見資訊作戰重要。

然近年來，網路系統的規模、複雜度和易受攻擊程度大幅成長。同時，攻擊者能取得的知識、工具與技巧也與日俱增。遺憾的是，由於防禦是一種反應行為，防禦技術並沒有像攻擊技術發展來得快。因此面對現在和未來的各類威脅，我們必須更加落實良好的資訊安全基礎。但在現今各單位資訊防護裝備缺乏，資安洩密事件又層出不窮的情況下，國軍網路雖然具有實體隔離的封閉網路環境特性，在強制要求不可外接民網的命令下，來自外部的威脅源（如：駭客、病毒製造者）可以假設性不構成威脅。但是內部的威脅源（有心人士情報收集、病毒或後門攻擊）卻不得不預防，人員管制是關鍵因素，但在各單位資訊人力精簡後，危機應變人力明顯不足的情況下，所造成的傷害是相當可怕的。

因此本文針對資訊防護這個課題提供誘捕式網路防禦的概念與研究，希冀供各單位建置基本資訊防護能量之參考，同時亦可藉此建立資訊戰攻防之研究資料庫，用以分析收集網路活動資料，強化資訊防護戰力。

關鍵詞：資訊防護、入侵偵測、誘捕式網路防禦技術。

前言

網路串連共享電腦資源，方便之餘，也給有心人士一個最佳入侵途徑，不管其入侵目的為何，每個人所業管的機密資料是保護重點。現行國軍網路環境在安全實體隔離的政策執行下，似乎保有了一塊網路淨土。但資安洩密事件仍頻傳，木馬攻擊事件仍發生，就表示系統漏洞、人員管制、資訊貯存媒體攜出入管理都出現了嚴重的問題。

根據CERT/CC在 1995 年至 2006 年第一季的統計資料，現行作業系統廠商所發現的系統漏洞共有 24,313 項系統弱點報告[1]，這是官方的統計數據。從駭客社群、黑帽駭客（Black Hat）社群等非官方網站中，則流傳許多未公開的系

統漏洞，根本無法統計，因此，面對尚未發現的漏洞要如何防範，不明的入侵行為模式如何察覺，是資訊防護需要努力的課題。

從趨勢科技全球病毒實驗室 TrendLabs 發表的 2005 年上半年度病毒報告[2]中可得知，蠕蟲、特洛依木馬、手機病毒、混合式攻擊(Malware Tandem)等四大病毒威脅性為全部病毒之冠。主要的病毒型態仍以特洛依木馬病毒為主，共偵測到 2,997 隻的木馬程式，佔所有病毒的 39％；其中高達 2,292 隻為新產生的特洛伊木馬，高居所有新型病毒型態的 47％。特洛依木馬程式的隱匿入侵功能、蠕蟲的迅速散播能力、再加上間諜程式高超的混合式攻擊愈來愈普及，而目的意在竊取系統與使用者的相關資訊、機密文件、網路銀行帳戶與密碼。

間諜軟體會突破反間諜軟體的偵測，進而終止程式並刪除之，輕易地竊取機密檔案。而在 2005 年 2 月 9 日現身的間諜軟體 TSPY_ASH.A 造成反間諜軟體（Microsoft Antispyware）程式被終止，並且刪除其相關檔案，然後潛入網路銀行竊取受害者重要資料。而變種的間諜軟體 TSPY_ASH.B 會修改 IE 首頁設定，甚至具備遠端下載自我更新的能力。

針對以上系統漏洞的程式缺陷，再加以病毒、木馬、蠕蟲混合式攻擊的不斷變化，假設不知情的人員將來路不明的軟體在國軍「封閉式網路」中執行，電腦發生中毒現象，可以想像其所面臨的危機是何等巨大。

綜合上論，雖然資訊安全的範疇雖不斷的推展，但是良好的資訊基礎是永久不變的，其包含著所謂的安全三D：防禦（Defense）、遏阻（Deterrence）、偵察（Detection），並藉以訂定適用的資安政策。因此傳統的資訊安全技巧，主要是在阻擋攻擊（防火牆）或即時偵測攻擊（IDS入侵偵測系統）。這兩種技術都非常重要，但也有其限制。只要有足夠的時間和資訊，攻擊者就可以得知防火牆允許外界存取哪些服務。一旦攻擊者可通過防火牆存取內部伺服器，防火牆就無法提供進一步的防護。IDS只有在攻擊開始時才會提供資訊。但這卻無法為您爭取足夠的時間，以適度的保護所有易被攻擊的系統。此外，IDS 無法判斷新的攻擊是否成功，或者被入侵系統是否成為跳板，成功攻擊其它系統。

而網路誘捕系統便是一個成功的反制措施，可以實質上拖延攻擊者，同時能提供防禦者足夠的資訊來瞭解敵人，避免攻擊造成的損失。若能成功使用，就可以達到上述目標。藉由欺騙攻擊者，防衛者透過提供錯誤資訊，迫使對方浪費時間做無益的進攻，以減弱後續的攻擊力量。此外，良好的誘捕機制讓企業無須付出被成功入侵的代價，即可為防衛者提供攻擊者手法和動機的相關資訊。這項資訊日後可以用來強化現有的安全措施，例如防火牆規則和 IDS 配置等。

本文

一、誘捕式網路防禦技術之研究目的

「兵者，詭道也。故能而示之不能，用而示之不用，近而示之遠，遠而示之近；……攻其無備，出其不意。此兵家之勝，不可先傳也。」──《孫子兵法》

數千年來，軍事領袖為了戰勝，都曾經欺騙過敵人。第二次世界大戰期間，盟軍誘使德國人相信，真正的攻擊會發生在加來（Pas de Calais）而不是諾曼第；甚至在諾曼地登陸之後，希特勒還確信這是佯攻，因此未能及時回應。在「沙漠風暴」軍事行動時，美國使用假士兵、軍營，甚至戰車來分散伊拉克軍隊的注意力，而真正的士兵卻從別處攻進伊拉克，幾乎如入無人之境。

在戰場上運用的技巧，同樣也可以用來防禦網路上的資產不受今日狡獪的攻擊者破壞。網際網路為攻擊者提供了一個自動化的公共知識庫，可以用來向企業發動新型態的戰爭。例如，攻擊者可以使用網際網路，沉著地研究新的弱點。或者，只要下載一個自動化的駭客工具（exploit），一個新手也可能看似擁有專家的技能。在網路上甚至可以輕鬆的搜尋到如何繞過防火牆及「入侵偵測系統」（IDS）的相關資訊。此外，自動化技術意味著攻擊者可以花費幾個月的時間找尋防禦漏洞，而不必採取可能引人注意的互動方式。最後，由於網路的互連特性，來自各地的攻擊者可對他們選定的任何系統發動攻擊。

因此誘捕式（decoy-based）網路防禦系統技術或所謂的“Honeypot”便在此扮演一重要的角色。所謂「誘捕」有隱藏本體、佈置陷阱、放入誘餌、吸引獵物這四層涵意，引申其意，在資訊安全領域中，誘捕式網路防禦技術的目的便是讓重要的主機或設備被隱藏保護起來，在可能被攻擊的前線佈置陷阱等，例如防火牆的非軍事區（DMZ）建置虛擬誘捕系統，或是在企業網路內部（Intrant）混合建置虛擬誘捕系統。同時，在誘捕系統中放入讓駭客心動的假情報或假資料（誘餌），當駭客或有心人士採取行動的時候，除了目標錯誤而誤中副車外，其具備的監控機制回報機制也能讓管理人員立即處理、管制與預警和收集電子證物等。

二、網路誘捕系統的演進

Honeypot 其實並不是一個新的概念。自從電腦開始互連以來，資訊安全研究人員與專家就使用過不同形式的 Honeypot。電腦的誘捕系統會被部署成吸引攻擊者的目標，如一罐用來吸引並會困住昆蟲的蜂蜜。使用 Honeypot 可以獲得許多的好處。第一，它會消耗攻擊者的時間。看誘敵深入到什麼程度，攻擊者可能耗費大量時間嘗試刺探及研究誘捕系統 ─因此用在攻擊 Honeypot 的時間，

就不會用來攻擊真實主機。第二，這會讓攻擊者對於現有的安全措施產生錯誤的印象，對方可能會花很多時間尋找工具攻擊 Honeypot，但這些工具在真實系統上可能無法運作。第三，有 Honeypot 的存在，可降低真實系統受到隨機攻擊或刺探的可能性。

許多攻擊者會大規模掃描電腦，來找尋受害者。即使是針對特定機構的攻擊，也會掃描該機構所擁有的公眾系統，尋找一台電腦來入侵，做為攻擊的起點。使用 Honeypot 會降低攻擊者選擇一台重要電腦作為目標的機率，而誘補系統也會偵測並記錄最初的掃描，以及任何後續的攻擊。

不像其它的入侵偵測機制，Honeypot 不會有任何誤報（false positive）。IDS 產品大都會產生不同程度的誤報，這是因為正常的通訊總是有可能剛好符合 IDS 用來偵測攻擊的特徵。但 Honeypot 就不會有這種情形。任何連往 Honeypot 的通訊都是可疑的，因為這個裝置除了偵測攻擊之外並沒有任何其它的用途。換句話說，沒有任何合法的通訊會產生誤報。

如此一來，Honeypot 可以比其它任何 IDS 解決方案偵測到更多攻擊。Honeypot 可以發現和分析新的弱點，因為攻擊者採取的所有行動都會被記錄下來。通往 Honeypot 的所有通訊都是可疑的，所以新的攻擊工具可根據其與系統的互動被偵測出來─即使是所謂的「第八層」攻擊，如針對資訊流而不是針對程式或通訊協定等 OSI 七層架構下的攻擊，亦可被偵測出來。例如將假資訊輸入某個服務或資料庫，或使用已被破解的憑證來取得未經授權的存取。最後，Honeypot 能偵測和記錄可能持續數月的資安事端（incident）。這些所謂的「慢速掃描」（slow scan）很難透過 IDS 偵測到，因為它所用的時間很長，讓它看起來像正常的通訊內容。

Honeypot 可以分為三大類：待宰羔羊 （sacrificial lamb）、偽裝系統（facade） 以及傀儡系統（instrumented system）。

第一代發展出來的 Honeypot 是「待宰羔羊」，由數台設定為攻擊目標的電腦所組成。待宰羔羊通常是由一個「現成」或「現有」的系統所構成，它會放在某個易被攻擊的位置，留在那裡當犧牲品。它是攻擊者最顯著的目標─但遺憾的是，分析攻擊資料非常耗時，而且待宰羔羊本身也可能被攻擊者用來作為攻擊其它電腦的跳板。

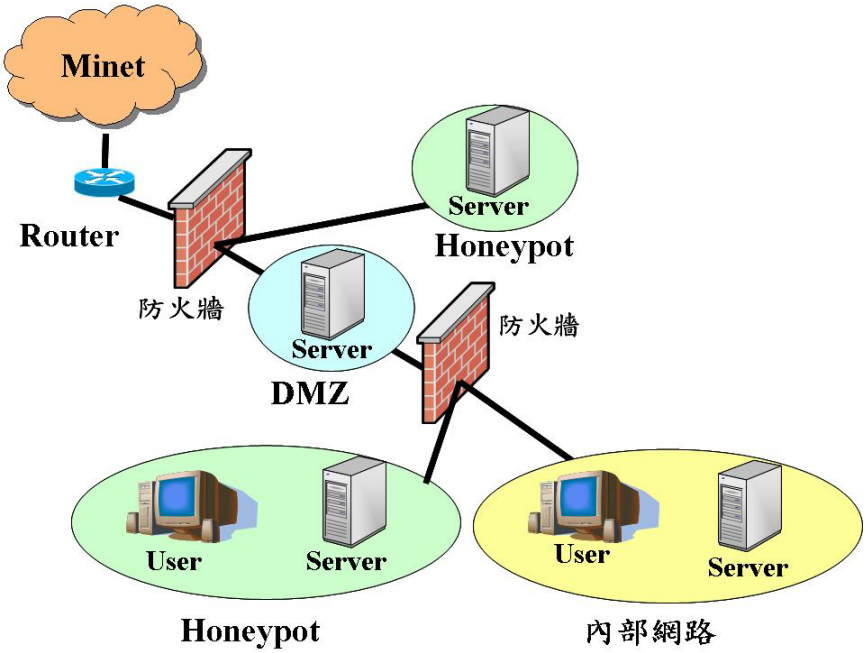
第二代的 Honeypot，因為它只有模擬網路服務，而不會讓真正的電腦受到攻擊，排除了遭入侵的誘捕系統所造成的資訊安全威脅。這些「偽裝系統」通常具有待宰羔羊的弱點，但不會提供這麼豐富的資料。偽裝系統提供的攻擊資料記錄更容易存取，因此讓攻擊者更難躲避偵測。偽裝系統是最輕量級的

Honeypot 形式，通常是由某種模擬的服務應用程式所構成，目的是要提供受害系統的假象。

新一代的「傀儡系統」則兼具了待宰羔羊和偽裝系統的優點。類似待宰羔羊，它們也提供非常可信的系統，讓攻擊者進行破壞。也就像偽裝系統那樣，這些系統很容易存取卻很難迴避，因為它們會記錄攻擊資訊。此外，進階的傀儡系統提供了預防攻擊者使用這台系統作為進一步攻擊的基地防禦機制。傀儡系統型的 Honeypot 是一種現有的系統，但做了額外的修改，因此可提供更多資訊、牽制或控制。

三、網路誘捕系統之建置架構

本系統建置的架構圖如下：



圖一　網路誘捕系統架構圖

(一)平台建構

基於成本考量及系統便利性、安全性，本文選用Vmware[3]這套軟體來構建網路模擬系統，Vmware可以模擬任何作業系統的運作環境，假若電腦的設備等級較高的條件下，亦可模擬多台電腦，也就是建立多台虛擬作業系統。所以，不論你的主機作業系統為何，都可以跑另一個不同或相同的作業系統。例如：在Linux 的作業系統跑一個Windows系統模擬環境，或是在Windows的作業系統跑一個Linux系統模擬環境。Vmware不同於多重開機系統，它算是在主機作業系統中跑的一個程式，而這個程式在模擬另一個作業系統，以致於在感受上像是兩個作業系統同時在一台電腦啟動運作。

為了明確區別作業系統的主副關係，將安裝執行VMware軟體的作業系統

稱為「主機作業系統」，而VMware虛擬機器下所安裝的作業系統稱為「虛擬作業系統」；假若，同時啟動許多虛擬機器，每一台機器都擁有自己的網路位址，再加上主機作業系統的數量，在網路上便形成一個誘捕系統網（Honey Net）。

VMware 在主機作業系統與虛擬作業系統間有一層虛擬層（VMware Virtualization Layer），虛擬層的功能是把實際的硬體資源對映到虛擬機器上的硬體資源，因此每一個虛擬機器都有它自己獨立的CPU、記憶體、硬碟及各項I/O設備，同時，VMware使用了X86 的保護模式，讓各作業系統是獨立運作的，不會互相影響，因此在一台X86 電腦上同時模擬多個不同的作業系統是可行的。

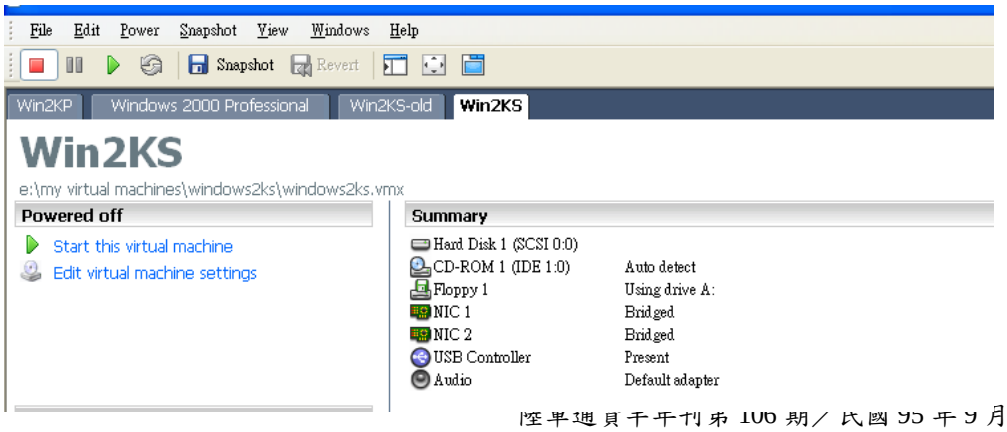
VMware的虛擬網路功能提供了三種網路模式：Bridged模式、NAT模式與Host-only模式。

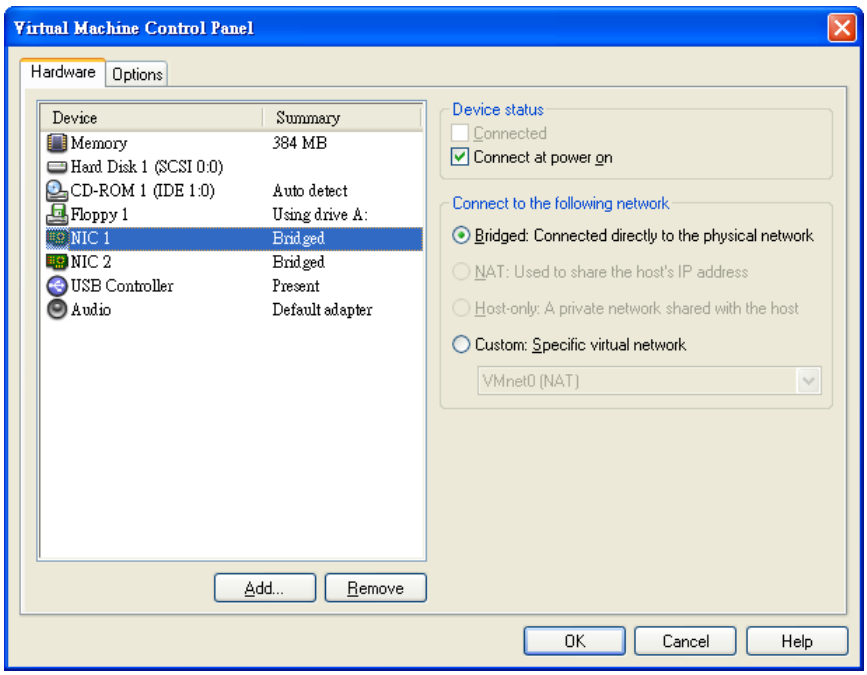
1.Bridged 模式：可直接存取網路的模式，簡單地來說，虛擬作業系統可獨立設定網路參數，例如：IP 位址、子網路遮罩、閘道器、DNS 位址等 TCP/IP 參數，成為一台可直接上網的電腦，所以，在交換器（switch）上會保留這台虛擬主機的記錄。

2.NAT 模式：當虛擬作業系統的網路設定為此模式，就是與主機作業系統共用同一個網路位址。例如，主機網路位址是 192.168.1.1，則虛擬作業系統在此模式上網，便使用相同的主機位址(192.168.1.1)來上網，共享相同的網路介面。

3.Host-only 模式：當虛擬作業系統的網路設定為此模式，便分開成為內部私有網路（Private Network）與外部公用網路（Public Network）兩大部份，透過這個方式建立一個與外界隔離的獨立網路環境，若虛擬作業系統要上網，須透過在主機作業系統的 routing 設定、NAT 設定、Proxy 設定或是 Bridge 設定，讓虛擬乙太網路卡透過實體網路卡連接到外部網路上。

綜合上論，Bridged網路模式設定是建置安全虛擬模擬環境時很好的一個選擇，因此本文之監控架構設定如圖二、三。





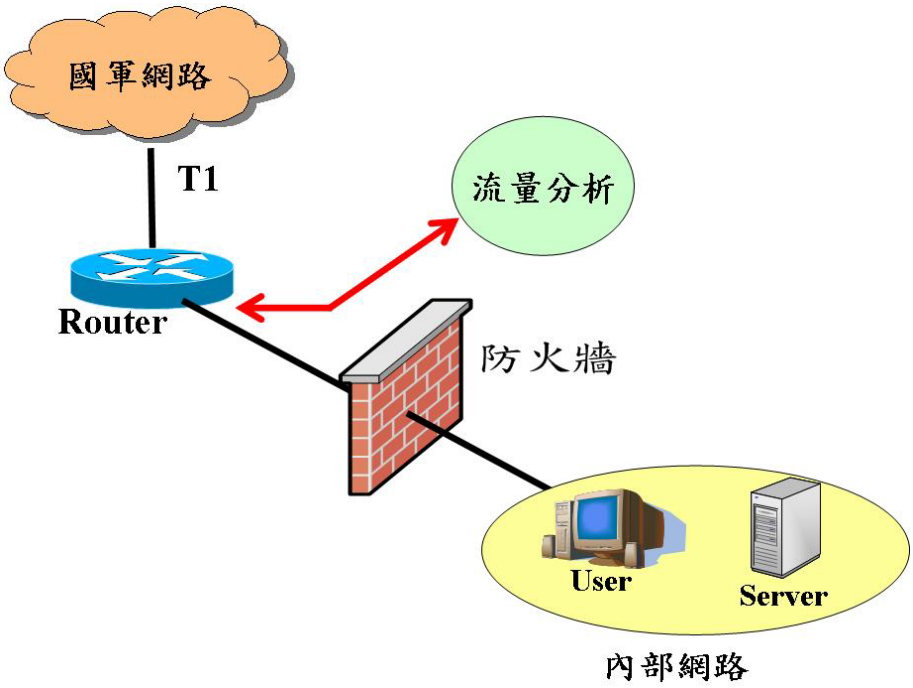
圖二　VMware虛擬機器環境參數設定

圖三　VMware Bridged mode 運作模式

(二)誘捕系統網（Honey Net）的運作方式

Honeynet[4]的目的是對入侵者群體進行研究，透過我們所佈置的網狀誘捕陷阱，虛虛實實的網路配置形成蜘蛛網般的架構，只要觸動一個虛擬網站，便能展開追蹤他們的行為舉動。傳統的網路監控方式是對網路流量進行異常比對或門檻值設定，如圖四的網路流量擷取架構是從對外路由器的流量資料上，透過SNMP的網管協定來詢問其流量記錄，進而分析網路流量異常現象。然而，過大的網路資訊量使安全網管人員無法分析隱藏在其中的異常入侵連線，除非是分散式阻斷服務攻擊（DDOS）大量封包讓網路流量異常增加，其網路分析是顯而易見的，否則，浩浩流量中要找出異常連線是不容易的，假若，我們可以過濾出何者是正常流量，何者是惡意活動，則針對網路異常監控能力勢必更精準、更快速。

Honeynet的配置目的是追蹤、研究系統被侵害過程的記錄，歸納出入侵行為模式，進而分析其因應之道。一般而言，一個正常的伺服器在沒有執行網路連線的動作時，是保持靜態服務狀態。在此我們可使用Windows內建的程式「netstat」來檢查網路連線狀態，在命令提示字元模式下輸入「netstat」加上參數（n：以IP顯示連線狀態；a：顯示所有已連接的連線和傾聽中的連接埠）。如圖五所示，伺服器服務埠保持等候狀態。



圖四　網路流量擷取圖

圖五 伺服器服務埠靜候圖

一旦有使用者連線伺服器Port 80，則伺服器的網路狀態會建立一個TCP連線，如圖六。

```
  TCP    10.52.86.241:80        10.52.86.57:2899       TIME_WAIT
  TCP    10.52.86.241:80        10.52.86.57:2900       ESTABLISHED
```

圖六　網路TCP連線建立圖

以上所述可歸納為正常連線，反觀，除了Windows Update、防毒軟體病毒碼自動更新或其它防護機制有主動連線到外部網路去作更新的動作外，伺服器理應不會自動從內部連線到外部網路，因此，假若發現這種連線狀況，則可視為異常連線，也就表示系統有中毒的可能、駭客進行入侵、掃描與探測的動作，甚而主機被當作跳板、被植入木馬程式等攻擊行為。

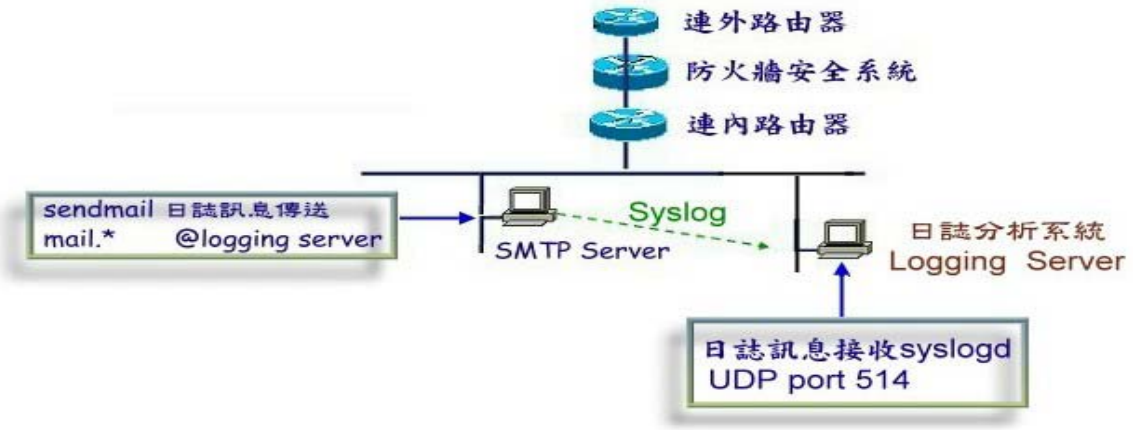
```
C:\Documents and Settings\wuyao.ACES-SIAD>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
```

四、網路誘捕系統之訊息監控機制

透過以上連線方向性的區分，我們界定由外至內的連線為正常連線，由內至外的連線為異常連線，簡易地區分出網路正常行為。接下來探討相關監控機制的訊息控制與分析。

(一)系統服務之訊息控制與分析

由外至內的正常連線中也有可能針對服務的漏洞進行攻擊，這需要從服務系統的日誌檔來分析異常，因此，日誌分析系統扮演了處理與分析異常日誌的問題，下圖七這個例子便是針對郵件伺服器所產生的日誌所構想的日誌分析系統架構圖[5]。



圖七　郵件日誌分析系統圖

檢查系統日誌（LOG）是系統管理上很容易被忽略的重要細節，原因在於大部分的system logs 傳達的資訊是不易判讀的，以至於將系統重要警訊流失掉。syslog-ng [6]是用以取代syslogd 的new generation版本，原來的syslog是只能夠依facility及priority/level作分類，syslog-ng可以根據log的內容，以regular expression自訂分類及log的處理方式，並且支援以tcp/udp 將log送到遠端的server，或是即時通知在線上的系統管理者，甚至能將log值當成某個program的標準輸入字串，直接將log 作加工及分析，Syslog-ng 還支持資料庫系統，並可依據log 的pattern 來進行更有效率的分類及監控，因此，將防火牆IPtables及入侵預防系統Snort-inline 的LOG 均以syslog-ng 分類後存入資料庫中，並以php-syslog-ng [7]這個Web顯示介面顯示LOG，並透過郵件將異常連線反應給系統管理員。

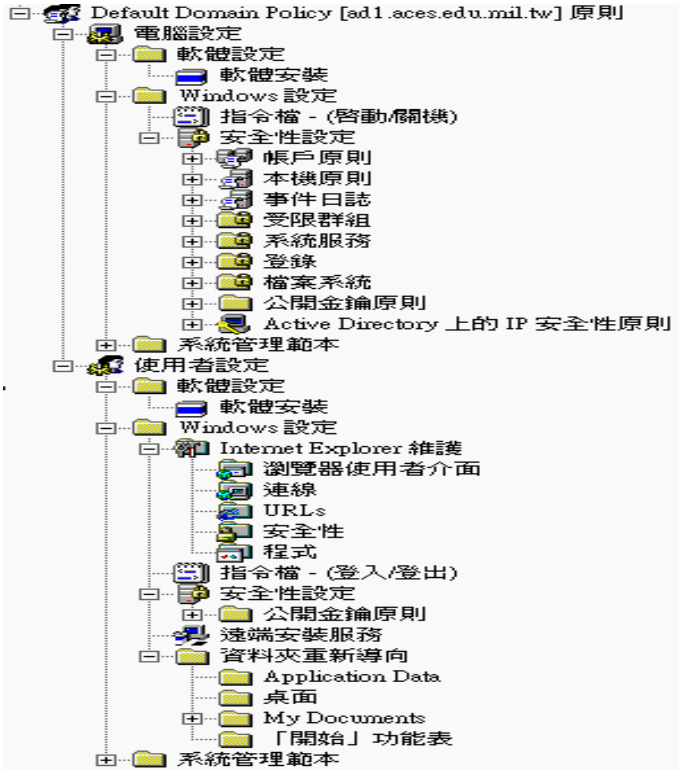
(二)系統記錄之訊息控制與分析

在Honeynet Project[8]中提到，要成功的建立Honeynet，需要面對兩個問

題：訊息控制及訊息捕捉。訊息控制之目的是規範適當的遊戲規則，當Honeynet裡面的誘捕系統主機被入侵之後，它不會癱瘓主機的正常服務，也不會被用來當做跳板攻擊其它主機。訊息捕捉則是要擷取入侵者的所有網路流量，包括他們在鍵盤上的敲擊行為以及他們傳送出去及接收到的封包，如此，我們才能夠了解分析入侵者他們所使用的工具、策略及目的。

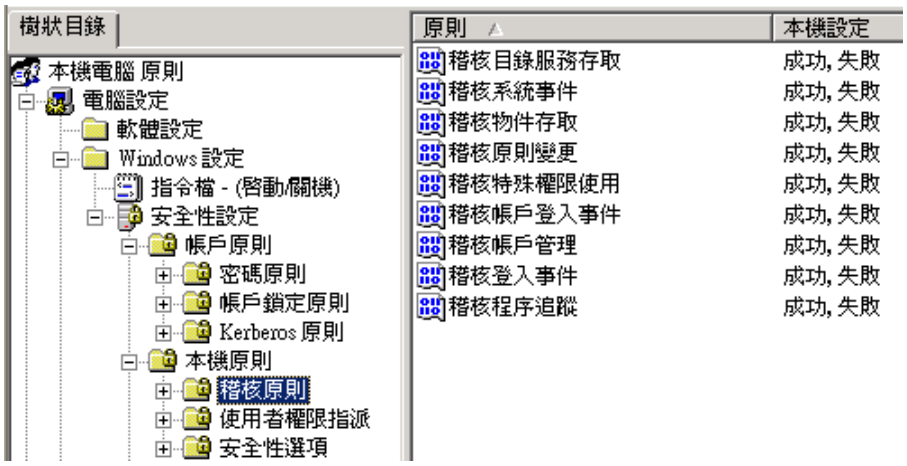
訊息控制是對於入侵者的行為進行規則上的定義，管制他們能做的以及不能做的事情。由於駭客入侵到一個作業環境時，第一件事是先建立一個權限高的帳號，再利用控制台或MMC的機制瀏覽整個系統設定，進而更改設定或植入木馬後門程式，等完全掌控這台電腦後，進行跳板攻擊其它電腦。為了讓入侵者在虛擬環境感到執行自由，但又不能讓其任意攻擊非虛擬誘捕系統外的主機，徒然冒生許多資安風險或法律問題，本研究是利用微軟伺服器的目錄服務（Active Directory）來進行系統環境規則定義，同時，捕捉入侵者活動訊息。

1.目錄服務的群組原則[9]設定：當入侵者進來環境之後，其最需要的是網路連線，因此，在虛擬環境中儘可能給予最大的網路執行能力，然而在系統設定方面，儘可能不給任何控制權限，不能更改任何系統參數。群組原則基於目錄服務的技術可以完成安全管理、系統管理、網路管理、軟體部署及使用者作業環境設定，所以，當我們統一律定登錄原則設定、安全性設定、軟體安裝、Script、資料夾重新導向、遠端安全服務、Internet Explorer 維護等環境限制，讓入侵者以最小權限登入系統，便可以管制其所能影響的範圍，如圖八所示。



圖八 群組原則架構圖

2.目錄服務的稽核項目[10]：目錄服務中，所有存取都有記錄，這些記錄稱為安全性日誌，透過日誌分析可以追蹤入侵者在系統中所執行的活動。目錄服務支援九個稽核項目：稽核帳戶登入事件、稽核登入事件、稽核帳戶管理、稽核目錄服務存取、稽核原則變更、稽核系統事件、稽核程序追蹤、稽核物件存取與稽核特殊權限使用等九個，透過以上的稽核項目讓入侵者在登入系統時，系統管理員可以監控入侵者從頭到尾的活動，無論是建立新帳號、更動系統設定或是存取物件都在掌握之中。



圖九　稽核項目圖

(三)防火牆之訊息控制與分析

防火牆是誘捕系統網（Honeynet） 中相當重要的系統，它安裝在Honeynet的gateway 上，用來分隔誘捕系統及其他的系統，大致上區分成三個部分：一是誘捕系統，二是國軍網路，三是管理控制平台，讓所有進出誘捕系統的訊息封包都必須通過防火牆，在這裡防火牆是主要控制網路流入以及流出量的機制，並收集分析Honeynet上的封包以及網路連線資訊，針對每一個連線進行追蹤。當誘捕系統由內至外的異常連線和訊息符合我們預先所設定的防火牆規則時，防火牆便會阻擋那些訊息封包。一方面可以確保在誘捕系統網路內的機器不會被當跳板執行攻擊行動，一方面觀察入侵者在虛擬環境內的入侵行為與攻擊方法。

防火牆應對誘捕系統對外的連線數量進行管制，如允許 15-20 個連線等(此數據為概略值，連線限制數量過少無法滿足正常使用者需求；限制數量過多卻又失去其限制的意義），這樣才能管制入侵者不能任意對其它重要主機進行攻擊，因為，當到達這個連線上限時，任何超出的連線都會被防火牆阻擋掉。所以，當連線限制發生的時候，防火牆會發出相關的警告訊息以告知系統管理員

來進行處理。

(四)入侵預防系統之訊息控制與分析

為防止攻擊者入侵誘捕系統後，以它為跳板來攻擊其他無辜的系統，利用防火牆是不夠的，因防火牆只能限制誘捕系統網路對外的流量，然而，有些攻擊並不會達到流量的上限就完成了系統漏洞的攻擊，因此，針對這種我們無法防範的狀況，必須建置一個入侵預防系統。

入侵預防系統（Intrusion Prevention System）的防護機制是可以把這些攻擊行為的封包丟棄或改寫，以達預防的效果，簡言之，針對已知的攻擊行動，讓入侵者無法執行，同時將捕捉到的封包透過圖形介面轉換成攻擊訊息告知系統管理者。入侵預防系統記錄機制可以擷取到系統中所有網路的活動行為，進行網路的訊息流量監控、分析記錄所有入侵者在網路上的攻擊行為，並把這些攻擊行為的封包丟棄以免其他無辜的系統受害。

入侵預防系統都會有一個入侵特徵資料庫，當網路上的連線訊息封包的特徵字串符合資料庫中的某些特定項目的時候，就會把封包丟棄或改寫並發出警報。因此，入侵預防系統可以對所有的連線進行詳細的訊息收集擷取，也就是封包解析的功能。

在所有擷取訊息記錄最難的是要如何捕捉入侵者在誘捕系統中所下的指令，以及對其螢幕的監控，在本文中我們在Windows Base 作業系統下使用sebek誘捕系統軟體，這軟體是Honeynet Project這個組織的成員Edward Balas 所發展的一套誘捕軟體，主要是讓我們了解當入侵者進入了我們的系統後，在裡面做了什麼事。然而，假若入侵者使用加密機制（如SSH）來進行連線攻擊，就沒辦法記錄其行為。因為封包加密後呈現出亂碼，除非能立即解密，否則無法判讀其記錄。

Sebek 是一個Client/Server 架構的軟體，Client負責擷取入侵者的資料然後透過網路傳送到Server端以便收集起來，Server 端支援資料庫系統，所以收集到的資料可以由資料庫進行分析。

五、網路誘捕系統的應用

「預警應變機制」是本文中所期望建立的目標，透過主動式防護觀念來爭取防禦準備時間。所以，在一個多變的網路環境，我們預期建置的誘捕系統目的有：

(一)網路攻防平台

建立模擬網路攻擊與防禦的戰場演習環境，透過網路上所獲得的攻擊軟體或駭客軟體來進行測試，搜集整個攻擊過程中的攻擊行為、入侵指令或執行參

數，進而建立駭客攻擊模式資料庫，並演練網路攻防技術。

(二)區域聯防平台

虛擬誘捕系統是朝建立一可監控、可預判與可控制之虛擬模擬環境，讓網路安全防護成為全面性的防護網，只要防護網有任何動靜，監控中心可立即偵測，進而採取必要措施，以提升並強化整體系統危機應變處理能力。對於未知的網路攻擊，誘捕系統對攻擊的敏感度與偵測率越強，越能降低入侵行為所造成的損失。例如：在視窗系統環境下，利用VMWare軟體虛擬Windows-base或Unix-base的作業系統，針對其可掌控的缺陷服務來進行監控，使入侵者認為已經達到入侵目的，但實際上卻被監控系統掌握、監督及控制。

(三)共通掃毒平台

從趨勢科技的報告中指出，混合式病毒攻擊結合了木馬、蠕蟲與病毒等攻擊特性，因此，假若在某台電腦中毒的情況下不去處理，可想見其病毒散播的速度是呈現倍數的成長。誘捕系統亦可定位在預警防毒機制，因混合式病毒的行為類似駭客攻擊的模式，若能預期偵測到病毒可能爆發的黃金時間，採取必要的手段，不管是關機、拔網路線或掃毒，都可避免資訊安全上的危險。

(四)訓練教學平台

從管理作業系統的安裝、服務的建立、系統的設定、安全機制的整合，乃至於對整個系統的監控，日誌資料的判讀，都是一整套的訓練教學，對目前所有通資教育的培育、訓練與測驗、演習有很大的幫助。因此，將預定模擬的攻防活動項目，置於誘捕系統的主機上來執行，可加強學員的實務經驗，印證學科理論與觀念，將會提昇各單位的整體資訊戰力。

(五)資安驗證平台

資安政策制定是否符合認證標準，例如：BS7799、CISSP 等標準，是需要不斷地驗證與稽核。由於防火牆系統具有對網路不正常活動的警示功能，可以對誘捕系統設定警示，注意誘捕系統是否被攻陷，因此，將誘捕系統的系統主機置於監控系統之後，控制和記錄網路存取活動，進而驗證資安政策是否落實在每個單位平時作業環境中，定期稽核單位資安環境之易損性，完成「計劃-執行-檢查-行動 」（Plan-Do-Check-Act, PDCA）的資安模式，應用於資訊安全管理系統的所有過程。而易損性（Vulnerability）之定義有下列說明：

1.Maskery 將易損性定義為：「由於極端事件導致損失的可能性」。

2.Tobin 和 Montz 將易損性定義為：「潛在的損失」。

3.聯合國 1992 年公佈了易損性的定義：“潛在損害現象可能造成的損失程度”。

引申其意，在作業系統、系統軟體或其它應用程式內部往往都隱藏一些安全性弱點，這些系統安全的弱點都可稱為其系統的易損性。網路化資訊系統的地域廣泛性和通信協議的開放性，也決定了它的易損性，進而促使資訊網路安全保密技術，在系統的設計中成為不可忽視的重要組成部分，因為它成為資訊戰中最重要的打擊對象和最好的情報來源。

結論

資訊安全的重要性，相信每一位享受著資訊化便利的人都能朗朗上口提上幾句，但對大部分未親身體驗過的人總覺得相當虛無飄渺。而在眾多且繁雜的資安規定下，如何讓學員在不危害實體架構下，實際的感受到建立資安防護的重要性，並且觀察及學習到異常或入侵的徵兆。進而建構一個具備網路攻防平台、區域聯防平台、共通掃毒平台、訓練教學平台、資安驗證平台等的網路誘捕系統便是本文的目標。而網路誘捕系統可透過國軍現有的軟體建置快速部署的主動式資訊防護環境，不但節省經費，也可建立資訊防護的種能，讓各單位具備掌握、監控與控制入侵者的能力。

然而，駭客攻擊手法日新月異，誘捕系統也需時時做好更新的準備，尤其是系統更新、網路維護與備援機制的建立都是基本防護作為，否則，系統本身就容易因軟體、硬體上的問題而無法運作正常。定期稽核系統環境變數是否被變更，新的入侵行為是否放到資料庫，以及弱點掃描是否定期作系統的總體檢等都是確保誘捕系統能持續的重要步驟。下列歸納其優缺點供作參考：

(一)網路誘捕系統的優點

誘捕系統的建置只需要幾部電腦和軟體（Vmware、ISA、Sebek、BlackIce、Sniffer）建構而成，節省不少經費的支出，而且系統操作容易，一旦被入侵後可快速恢復運作，在VMware 中，每台虛擬機器都是由檔案組成的，要復原時，只要把檔案的備份回存就可以了。

同時，入侵者的跡證保留容易，只要把虛擬機器的檔案複製到其他安全的、有安裝VMware 的機器上，再把它開啟，就可以進行相關的鑑識工作。

(二)網路誘捕系統的缺點

安裝網路誘捕系統的主機硬體要求需較為高階的配備，且主作業系統的安全問題需要特別注意，否則還沒讓誘捕系統運作之前，本機主作業系統已產生問題，將會導致誘捕系統的所有功能停止。

廣佈誘捕系統是分散被攻擊風險的最佳方式，讓入侵者在勘查目的網路資訊或執行掃瞄時就誤觸誘捕系統。最後建議在放置誘捕系統時，儘量採廣泛性

的佈建，利用低互動性的誘捕系統，不但可以減少時間及資源的浪費，又可以提供大量的誘捕目標，例如：網路上提供了像Honeyd這種低互動性的誘捕系統，它不需高階的硬體配備，並且可以快速建置數量龐大的誘捕系統，可以將這個子網路中所有沒有用到的網路位址，全部以Honeyd來虛擬誘捕系統，如此便可達到本文所要達成的目標。

註釋

1. CERT/CC Statistics 1988-2003（n.d.）Retrieved March 15, 2004, from the World Wide Web: http://www.cert.org/stats/cert_stats.html .
2. 趨勢科技，2005 年上半年病毒特報，http://www.trendmicro.com/tw/about/news/pr/archive/2005/pr050711.htm
3. VMware Workstation User's Manual Version 4.0. (2003), 9/3/2003, http://www.vmware.com/support/ws40/doc/index.html
4. The Honeynet Project.,12/25/2002, http://project.honeynet.org/ .
5. 李武耀、江清泉，電子郵件日誌分析系統，TANET2003 網際網路研討會，2003 年 10 月 30 日。
6. Balázs Scheidler（n.d.）,syslog-ng reference manual, http://www.balabit.com/products/syslog_ng/reference/book1.html
7. Php-syslog-ng（n.d.）,1/5/2004,http://www.vermeer.org/projects/php-syslog-ng/
8. Hisham Kotry（2/17/2002）.Building a Virual Honeynet, http://www.linuxsecurity.com/feature_stories/feature_story-100.html
9. 彭輝，實戰群組原則，2005 年 5 月 1 日，IT焦點。
10. Mark Minasi, Christa Anderson，Windows Server 2003 目錄服務與系統管理篇，旗標出版社 2003 年 12 月 11 日。

參考資料

一、Roberta B. , Mark R. and Keith S.著，尤焙麟，邱孝賢與劉育銘譯，網路安全徹底研究，初版，台北，學貫行銷，2004 年 10 月。

二、William R. C. , Steven M. B.and Aviel D. R.著，夏雲浩譯，防火牆與網路安全，初版二刷，台北，台灣培生，2004 年 9 月。

三、高大宇，王旭正，資訊密碼暨建構實驗室，資訊安全，初版，台北，博碩文化，2003 年 6 月。