DNS 網域安全檢測探討

作者/李武耀少校・賴威良上尉・李念平上尉

提要

網域名稱伺服器（Domain Name Server, DNS）是所有系統服務的基礎建設，其主要功能就是作名稱解析，將所有內部主機的名稱與網址進行對應，且將其記錄存放在伺服器內以利使用者查詢。由於其階層式架構蘊含大量資訊，可透視企業內部網路架構，成為駭客發動攻擊前首要佔領的灘頭堡。

沒有網域名稱伺服器來幫助名稱解析，其它伺服器設定會產生問題，換句話說，所有系統參數設定中，DNS的IP位址是其中重要設定值，若DNS沒有設定好正向與反向區域（Zone）的對應，則其它伺服器也不能正常運作。

網路環境中，若已建構目錄服務伺服器（AD）與動態主機配置伺服器（DHCP），輔之以網域名稱伺服器（DNS）提供名稱記錄動態更新的服務，則龐大的單位組織與人員架構在其登入系統時，將全部呈現在DNS對應記錄內。因此，針對DNS伺服器安全進行資訊防護檢測確有其必要性。

DNS伺服器對於國軍網路正常運作扮演相當重要的角色，本論文焦點將放置於DNS系統設定上的人為疏失及管理系統上的異常現象，讓系統管理員可以檢測DNS伺服器的設定是否適切，以防止惡意攻擊者藉由該缺失蒐集資料甚至進行攻擊。

關鍵詞：網域名稱伺服器、網路安全、網域檢測

前言

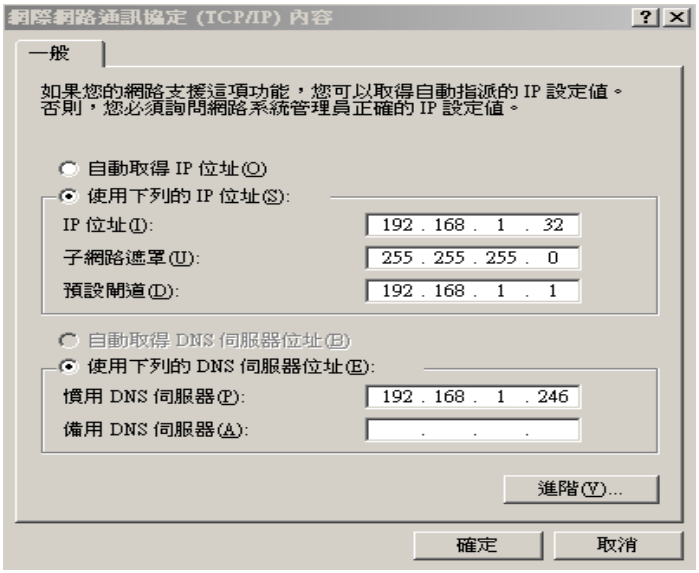
網路串連共享電腦資源，資訊分享所採用的網路架構為主從式架構（Client/Server Network），所謂主從式架構即是『客戶-伺服網路』的區域網路架構，客戶端主要負責的工作運算及應用程式的執行，同時對伺服器端提出需求的機器，如網路上的工作站（workstation）或者是個人電腦；伺服器端主要負責的工作在於處理共享的資源、存取Client端對Server端所提出對資料庫的需求及對於安全機制的控管，如名稱解析伺服器（DNS server）、檔案伺服器（File server）等等。

比起點對點網路（Peer-to-Peer Network）來說，Client/Server網路的缺點在於安裝的成本較高，維護不易，且工作站的資源不能分享，因為伺服器主宰了整個網路的運作，但卻有『集權式』管理的優點。

網路族群透過URL 指定到Server端時，網域名稱伺服器（DNS）提拱網址

轉換的基本服務，所有的網路應用都必須仰賴DNS系統進行網址轉換。DNS系統運作不正常，就算WWW伺服器、FTP 伺服器、Mail 伺服器及相關應用伺服器運作正常，仍然會因為網路位址無法轉譯，而導致找不到連線目標，而失去聯絡。

一般 Client 端主機需要在 TCP/ IP 協定中設定主機 IP 位址、子網路遮罩、路由閘道 IP 位址與 DNS 的 IP 位址（如圖一）。其中 DNS 的 IP 位址設定是告訴主機要詢問哪一台名稱解析伺服器來負責所有主機名稱對應。



圖一　TCP/IP 設定實例

一、主機名稱查詢系統（Domain Name System, DNS）

由於 IP 位址不易記憶，為便於人類記憶，將主機名稱轉換成有意義的英文字母組合，即所謂的「網路位址」或稱為「網址」來取代，創造了主機名稱查詢系統來幫助轉譯名稱與網路位址的對應。

DNS 解析作法雷同於手機撥打電話，可利用手機電話簿內收話者的姓名直接撥打，而非要使用者去記憶收話者的電話號碼。對底層機器而言，名稱不具有任何的意義，實際能辨認的是 IP 網路定址與 MAC 實體位址。「網址」的架構有：主機名稱．網域名稱．屬性別．國域別，例如 www.google.com。

二、領域類別管理

網域名稱是由網際網路網域與位址分派協會(Internet Corporation for Assigned Names and Numbers, ICANN)來分類，ICANN 是在 1998 年 10 月由網際網路業者、使用者協會、網路工程師與學術研究單位共同成立的一個非營利性組織，ICANN 的目的在於管理網際網路上的四大標的物：網際網路網域名

稱、IP 位址、網際網路所使用的通訊協定，與網域伺服器的配置。

在台灣，此項任務是交由 TWNIC 來管理，其網域名稱主要可分為三種：

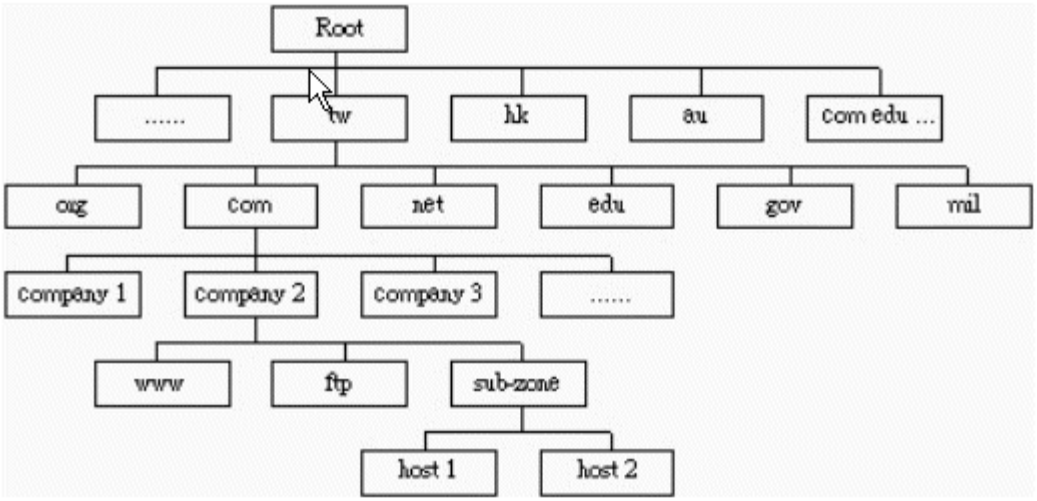
(一)通用型網域名稱：.com、.net、.org、.gov、. mil、.biz。

(二)區域型網域名稱：.tw、.jp、.cn、.uk 等各地區的網路資訊中心。

(三)多語言網域名稱：多為國外公司發展的多語言網域名稱，如繁體中文.com(BIG 5)、簡體中文.com(GB2312)、韓文.com(KSC)、日文.com(Shift JIS)等[1]。

國軍網路內的領域類別管理是由各軍種單位的資訊部門或通資部門負責。

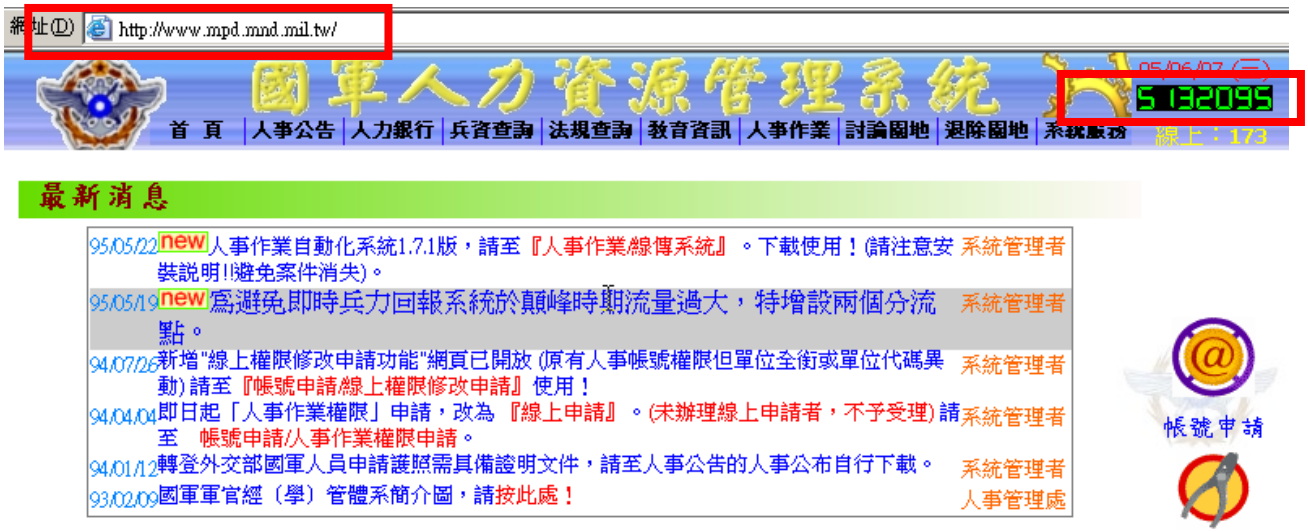
DNS 是一階層式名稱對應系統（如圖二），類似電腦目錄樹結構：全世界共有 13 個“root”，然後其下加進了諸如 tw、hk、cn 等國域名稱，再延伸分為好幾個基本類別名稱，如：com、org、edu 等；再下面是 組織名 稱，如：ibm、microsoft、intel 等；繼而是主機名稱，如：www、mail、ftp 等。故完整 DNS 名稱類似：www.xyz.com.tw，其對應的是一個（或多個）IP 位址。國軍內部的網域尾碼大多是：mil.tw，尾碼左邊為國軍各單位之網域名稱，例如：陸軍司令部資訊網網址：www.army.mil.tw。



圖二 DNS 階層式名稱對應系統

DNS 運作方式

在現行國軍網路中，每日上軍網的人數與主機數計有上萬台電腦，使用國軍管理系統已成為工作流程之一，以國軍人力資源管理系統為例，至 6 月 7 日為止已有 5 百多萬人次登錄瀏覽（如圖三），其 URL：www.mpd.mnd.mil.tw，不需記憶其對應的 IP 位址：10.24.16.1，這種網域名稱解析為 IP 位址的過程就是 DNS 的主要工作。



圖三 軍網上網人數統計與網域名稱

網域名稱解析IP位址的過程（如圖四），說明如下：

(一)當客戶端在 IE 瀏覽器網址列鍵入主機名稱(http://www.mpd.mnd.mil.tw/)時，便開始要求 DNS 伺服器解析；

(二)當被詢問到有關本域名之內的主機名稱的時候，DNS 伺服器會直接做出回答；

(三)如果所查詢的主機名稱屬於其它域名的話，會檢查快取記憶體(Cache)，看看有沒有相關資料；

(四)如果沒有發現，則會轉向 root 伺服器查詢；然後 root 伺服器會將該域名之下一層授權（authoritative）伺服器的位址告知（可能會超過一台）；

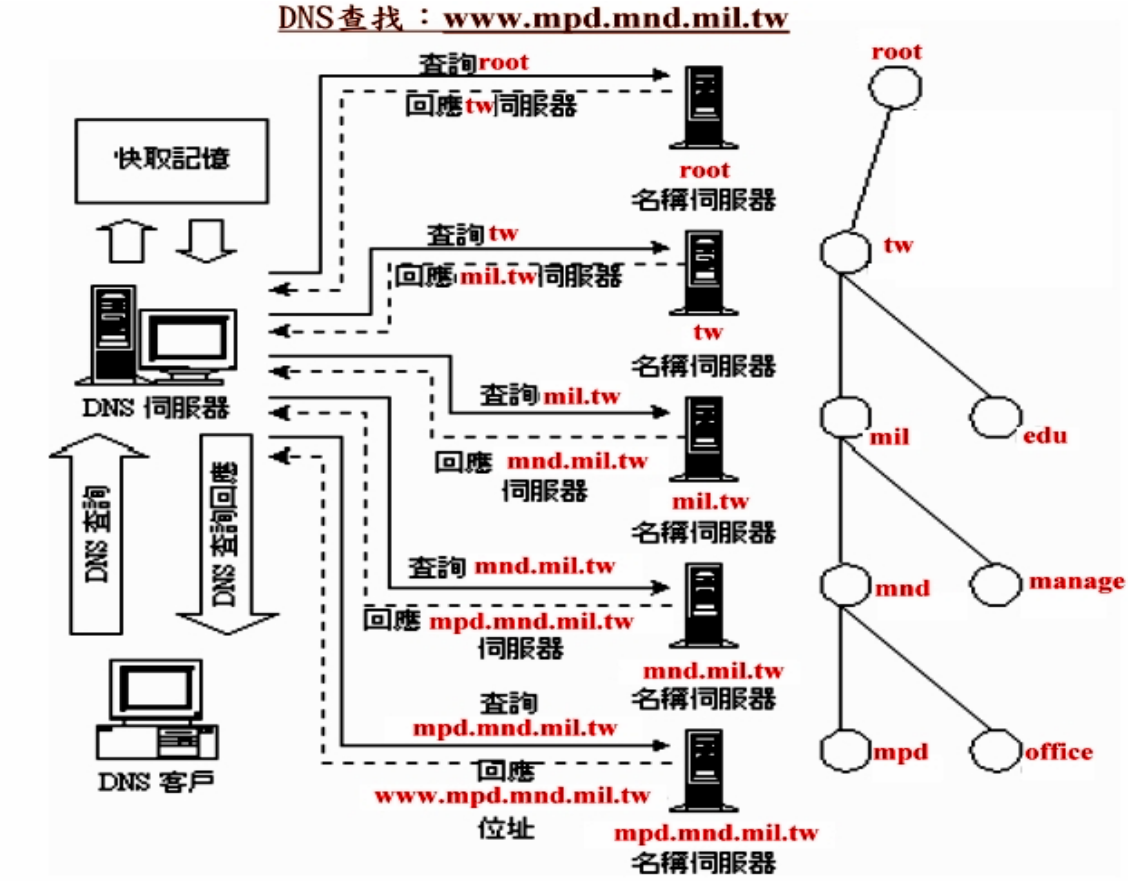
(五)本地伺服器會向其中的一台伺服器查詢，並將這些伺服器名單存到記憶體中，以備將來之需（省卻再向 root 查詢的步驟）；

(六)遠方伺服器回應查詢；

(七)若該回應並非最後一層的答案，則繼續往下一層查詢，直到獲得客戶端所查詢的結果為止；

(八)將查詢結果回應給客戶端，並同時將結果儲存一個備份在自己的快取記憶裡面；

(九)如果在存放時間尚未過時之前再接到相同的查詢，則以存放於快取記憶裡面的資料來做回應。



圖四 網域名稱解析流程

DNS 伺服器防護

孫子兵法：「知己知彼，百戰不殆」，一個有經驗的入侵者在執行入侵攻擊前，必會收集該網域之所有資料來瞭解該目標網域的架構情形[2]，透過 DNS 伺服器提供攻擊目標的清單，惡意攻擊者即可對重要主機進行弱點掃描與系統偵測，同時針對系統漏洞展開攻擊，宛如小偷已掌握了建築物的建築藍圖般，提高了攻擊成功機率。

CSI/FBI 電腦犯罪與安全調查報告中，指出入侵行為以資訊竊取為首要目標（如圖五）。在國軍網路中，國軍機密文件為首要目標，諸如：作戰、情報、人事與後勤等資訊。

因此，許多資料蒐集的行為皆會發生在DNS伺服器上，駭客會運用查詢甚至入侵方式來取得該攻擊網域相關的所有資訊，DNS伺服器安全對於整體網域安全扮演相當重要的關鍵因素。

圖四 電腦犯罪金錢損失統計圖（資料來源：電腦安全協會）

一、DNS伺服器弱點

根據以往DNS伺服器遭受攻擊的手法來進行分析與探討，可歸納出以下幾種方式[3]：

(一) Buffer overflow：緩衝區溢位的攻擊，藉由傳送特定的shell code，可能會讓攻擊者取得named[4]執行時的權限甚至是取得root 權限，造成主機遭受入侵。甚至是在入侵的主機上開啟一遠端程式，即所謂的後門，以方便下次的入侵。例如在2004年間流傳的Lion Worm（獅子網蟲）即是個最佳例子。

(二)Crash Server：藉由傳送不正常的訊息，導致DNS伺服器處理時產生錯誤而使得核心錯誤，無法再繼續提供服務，甚至是影響作業系統之運作。

(三)Denial of Server：藉由傳送不正確的封包格式，或是因為管理員的設定錯誤，造成伺服器無法正常提供，即阻斷服務攻擊（DoS Attack）。與Crash Server不同在於此種攻擊模式並未造成伺服器癱瘓，而是處於忙於處理「不正常」的查詢要求。

(四)Protocol flaws：DNS通訊協定缺陷所造成的安全問題，透過通訊協定的攻擊方式包含：DNS冒名欺騙（DNS Spoofing）、快取污染（Cache poisoning）及ID hacking 等攻擊方式，攻擊者可以透過欺騙、綁架、及滲透錯誤資訊的方式感染使用者所使用之網域，將使用者引導至所設置好的惡意網站上，連結於偽裝之網路銀行，針對用戶進行帳號密碼蒐集。

而這類的攻擊方式絕對是系統設定上的人為錯誤，及未針對查詢主機嚴格設

限所產生的問題，導致攻擊行為成功。

(五)Information leak：資訊洩漏，對於主機並無任何破壞行為，利用設定錯誤上的漏洞或是DNS伺服器未做有效限制的缺點來取得該DNS伺服器內的主機資訊，有心人士可以藉此發掘出網域內主機資訊，甚至是瞭解機器所在位置，由於容易達成，也是最常發生的攻擊方式。

為解決以上問題，TWNIC（台灣網路資訊中心）與TWCERT/CC（台灣電腦網路危機處理暨協調中心），於DNS安全資源網站，提供了針對DNS主機進行安全性掃瞄之安全掃瞄系統，藉由早先掃瞄系統弱點進行補強的方式來協助DNS用戶檢測所架設主機，並根據建議來修補主機上之漏洞，達到早先預警補強避免遭受攻擊的目的。系統運作至今，已有許多用戶透過該系統成功修正其DNS 系統於較安全之狀態。

二、DNS安全防護環境

欲建構全面化DNS安全防護環境，除了的DNS主機安全性檢測外，使用者的設定正確與否與DNS伺服器是否安全有著重要的關連，正確的管理與設定才是維持系統安全最佳的解決方案，因此，找出使用者設定上共同的問題，並給予建議及解決方案，相信是解決使用者因系統原理不熟悉卻又必須使用DNS服務時最需要的援助。針對國內外對於網域設定錯誤上進行探討，藉此尋找出共通的問題，設計自動檢測法則，完成網域安全設定掃瞄機制。

(一)台灣區DNS網域設定疏失

根據TWNIC針對台灣區各網域所進行的設定檢測[5]，歸納出台灣區常見的網域設定問題，分別敘述如下：

1.不良委任（Lame Server）：上層DNS主機將部分網域的授權給予某部主機，但該主機卻未發生功效，不良的委任關係最直接影響即是造成網路頻寬的浪費與查詢端主機資源消耗。

2.授權錯誤（Delegation error）：授權錯誤發生在於上層與下層DNS 紀錄不符合，亦會造成浪費網路頻寬且拖慢DNS查詢速度。

3.DNS容錯能力：當DNS發生錯誤時，將會造成網域與外界失去聯絡的現象出現，因此容錯能力亦成為網際網路正常運作的一項要素。

4.轄區傳送（Zone Transfer）：意指整個網域的轄區檔案可被其他任意取得，會造成整體網域資訊的洩漏，有心人士可以進一步臆測出網域內機器所在位置及提供服務，是典型的DNS 設定錯誤。

5.版本偵測：入侵網域的第一步驟為蒐集資訊，惡意攻擊者會針對系統資訊、硬體資訊及伺服器版本資訊進行蒐集。

根據上述調查結果，最常見的設定錯誤為DNS伺服器間設定錯誤，網域間設定不當甚至錯誤，所造成的影響將會擴及整體網域，造成網域查詢效率降低，浪費頻寬，嚴重者甚至造成上層網域錯誤，惡意攻擊者可以利用此一錯誤進行惡意攻擊，對於整體網域運作，是一大隱憂。

(二)國外網域設定疏失

Men＆Mice[6]於2003年針對全球網域名稱為.com 之DNS主機，以亂數選取5000部主機進行了設定上的普查，報告結果顯示，全球有68.4%在區域設定上（zone configure）有著嚴重的缺失，如表一，網域設定上的錯誤將會造成主機查找上的異常甚至是影響整體網域運作擴及所有應用伺服器（如，Web、Mail、FTP 等），影響範圍擴及整體網際網路運作效率。

表一 **Domain Health Survey for .Com （2003）**

檢測項目	2003 年結果 N=5000
Overall error Zone 設置錯誤	68.4%
單一端點錯誤	27.4%
轄區傳送完全開放	52.4%
轄區傳送限制錯誤	4.3%
完全關閉轄區傳送	43.3%
授權錯誤	18.4%
授權與 Zone 資料不符	16.1%
授權主機失效	16.4%
MX 紀錄設置錯誤	17.5%
Mail 主機與 MX 紀錄不符	6.4%
PTR 紀錄設置錯誤	11.9%
Zone 紀錄與實際主機配置不符	2.5%

(資料來源：Men&Mice inc.)

調查結果顯示出，轄區資訊（Zone Data）設置錯誤高達68.4%，顯示設定問題存在所造成網路服務不正常有極大的關聯，真正的原因是使用者不了解上下層之間真正的設定方式是有關係，且發生機率最高的錯誤分別在於：轄區傳送上的設定及授權（Delegation error）上的錯誤，這兩個原因代表了使用者在設定DNS伺服器時並未完全與上層DNS伺服器進行資訊之交換，導致上層與下層資訊不一致，在階層式的DNS 系統運作上該部DNS 伺服器將為成為該網域

的瓶頸（Bottleneck），影響網域運作效率[7]。

郵件主機紀錄（MX record）也是常見的設定錯誤，不熟悉的使用者在建置郵件伺服器時常忽略郵件伺服器是與DNS 伺服器有著相當密切關係，在不了解工作原理下，導致設定錯誤甚至是沒有設定，種種原因皆造成網域運作失效、效能低下，嚴重者可讓懷有惡意者有機可乘進行綁架、竊聽等惡意攻擊。

本文設計一DNS設定安全體檢，針對DNS網域安全健康（Domain Health）進行總體檢，來解決使用者對於網域正確設定問題，透過檢測步驟可以減少設定上的錯誤，進而改善DNS伺服系統之運作效能。

DNS 網域安全檢測機制

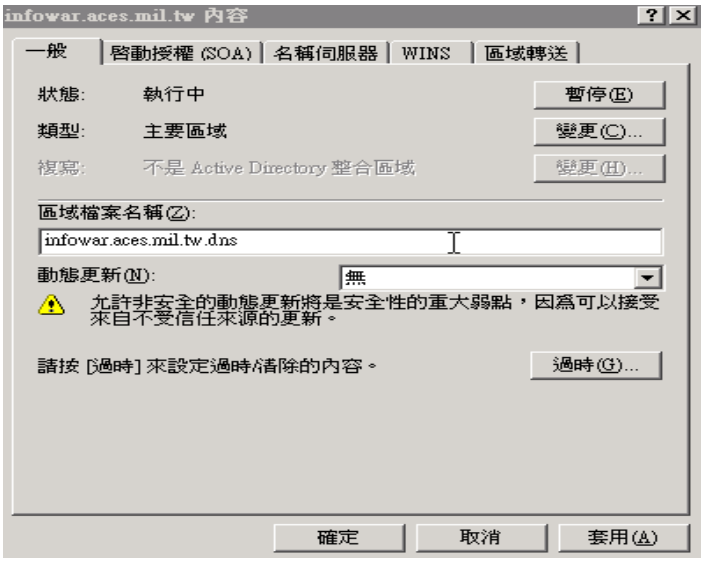
DNS 網域設定上常見的錯誤皆為上下層委任、授權、資訊傳送的錯誤，探討此類型錯誤造成之原因，使用者對於DNS伺服器組態檔的設定及轄區紀錄（Zone Record）的撰寫並非是相當明瞭。委任關係的失效常發生在於上層DNS認定下層主機為提供名稱服務，但該主機卻是一部郵件或是網頁主機，如此的設置方式，即會造成委任上的失效（Lame Server）。轄區資料設定錯誤則容易造成非經允許之DNS主機利用查詢（query）的方式來取得該DNS主機內所紀錄的所有機器資訊，攻擊者可以利用此一缺失，瞭解到所有登記服務的伺服器，因此，組態檔設定不周詳、Zone Record 撰寫錯誤、與上層架構不明，都是造成網域設定不正確的原因之一。

歸納研究DNS設定安全問題，包含了網域設定（本機DNS 設置問題）、網域主機委任問題（NS間異常）、時間常數設定（SOA問題）、郵件主機相關設定（MX 紀錄問題）、應用伺服器問題（WWW、FTP 等APS）及其他進階問題。

考量以上DNS設定可能發生之危安因素，設計以下七種設定安全檢測[8]：

一、網域完整檢測

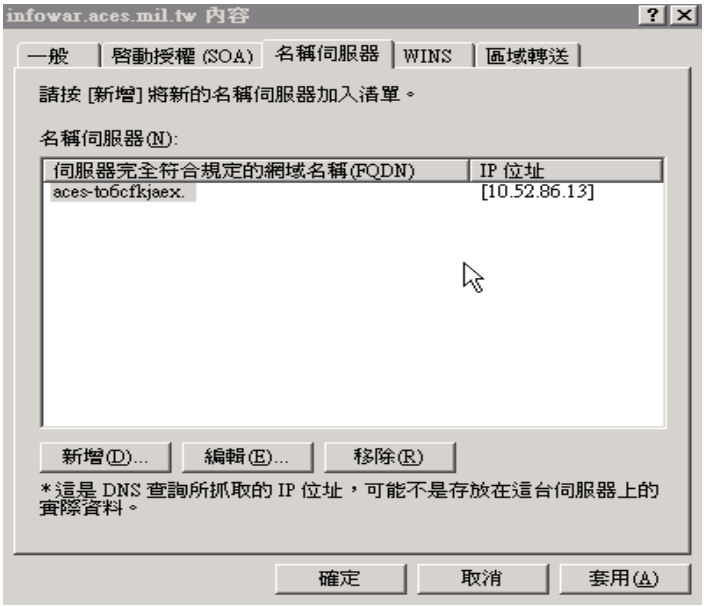
目的針對所安裝之DNS伺服器設置上的正確性做檢測，包含了查詢資訊、運作確認、是否正確設定共三項檢測（如圖六）。DNS為標準階層化設計，在判定DNS伺服器是否正常前，需先針對所架設之主機是否存在，該主機所紀錄之上層DNS主機是否存在、是否有做紀錄作確認，此為檢測第一步驟，若發生失效或檢測失敗，則無法順利進行其餘檢測項目。



圖六 網域完整檢測內容頁

二、NS設定檢測

上下層DNS間關係及設定是最常發生的錯誤，透過查詢上層與查詢自身DNS資訊來進行比對，可以瞭解上下層設定是否有誤，包含檢測Lame Server、網域名稱、主機驗證等共三項檢測，藉此來檢驗是否發生委任錯誤或是授權失效等影響運作正確性的問題（如圖七）。



圖七 NS設定檢測內容頁

三、SOA設定檢測

DNS伺服器間用來控制資訊交換及更新區域資訊，是透過所設定之時間常數來進行判斷，正確的時間設定可以改善DNS 網域間資訊交換的效率，過於頻繁或是過少的轄區紀錄交換對於正常運作的網域都不是正確的設定方式，透過SOA設定檢測，可以找出針對時間常數上的錯誤，判斷上採行RFC文件所建

議之時間長度來做為判斷的準則，模組中包含了Serial、更新時間、重試時間等七項檢測函數。

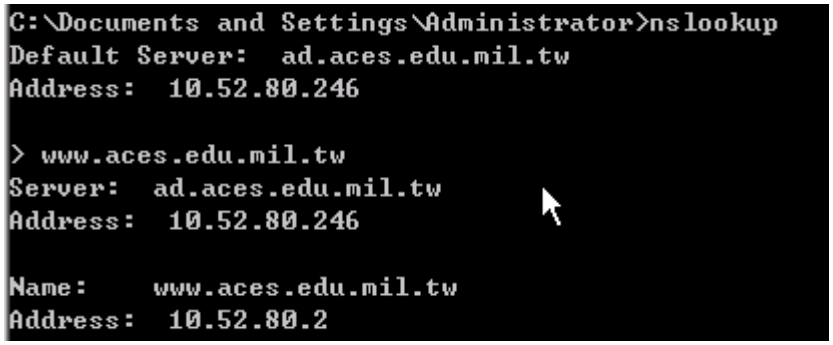
圖八 SOA設定檢測

四、MX設定檢測

郵件伺服器運作是否正確，與DNS有絕對的關係，MX 紀錄目的在於設定郵件伺服器收件次序及讓用戶端電腦知道該IP為一郵件伺服器，MX 紀錄設定上的缺失將會造成郵件無法傳遞甚至是寄出後石沈大海現象，透過檢測MX 設定正確性，可以有利於判別郵件問題是出自於DNS端還是郵件伺服器端，該設定檢測包含了與郵件相關設定。

五、應用伺服器（APs）設定檢測

DNS 伺服器最大目的在於提供網址轉譯，因此許多包含應用伺服器（如www、FTP、News）等都必須在此進行紀錄，因此針對應用伺服器正確性驗證是必要的（如圖九）。因為許多網域在設定應用伺服器時常會發生有紀錄而無主機現象，甚至是別名設置錯誤等，都需透過此檢測來驗證。

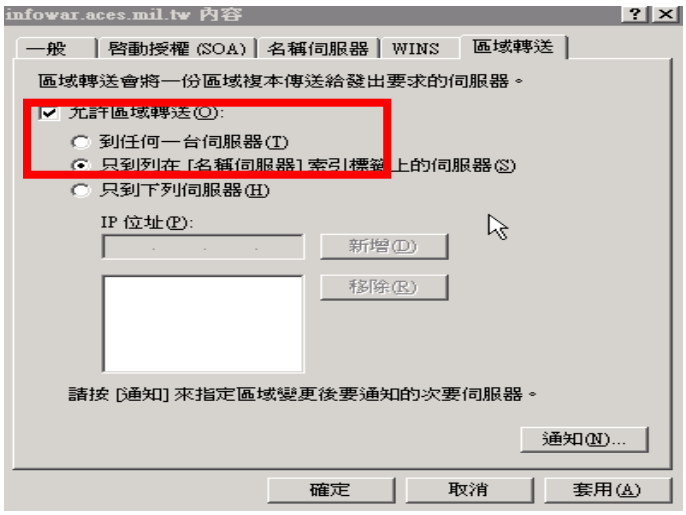


圖九 Nslookup檢測工具

六、進階項目檢測

資料交換是DNS 運作的方式之一，然而未經限制的資料交換所遭受的就是資訊遭受竊取，甚至是污染（poisoning），因此，進階項目針對DNS 較特

殊之功能進行檢測，目前檢測函數為針對轄區傳送是否正確做檢測(如圖十)，來判斷是否面臨該類問題，並提出修正建議。

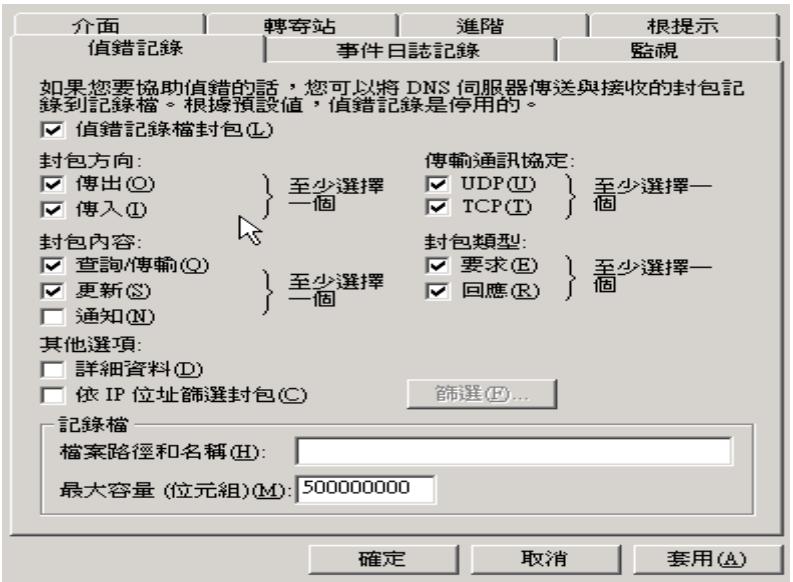


圖十 進階項目檢測

DNS 架構下常需透過更新的動作來更新 Zone 區域內的資料，DNS 主機與主機間轄區資訊是經常在進行比對與交換的，如此才能確保查詢到的資料為正確。除了主機間進行資料的傳送外，在進行人工除錯時，也常使用此方式將對方主機的轄區資料列出來，正常情況下，在一信任網域下，將資料列出是沒有問題的，若是能由外界進行查找時，那將為演變為具有危險的行為，因此，限制您的 Zone transfer 將是相當重要的設定。

七、日誌偵錯記錄

針對DNS伺服器與用戶端之間的傳送/接放封包記錄律定，使錯誤的轄區轉送設置可以察驗，成為電子鑑識證據（如圖十一）。



圖十一 日誌偵錯記錄

結論

DNS系統的工作原理既基礎又重要，系統管理員很容易造成在設定上的疏失，除影響所架設的目錄網域服務運作外，嚴重將造成有心人士入侵的管道。

國軍資訊系統管理人員透過本文的安全設定檢測，提高國軍網路的網路安全意識和能量，一方面強化系統服務安全，一方面搭配系統漏洞修補，將使系統與服務的安全防護能達到一定水準。

註釋

1.顏榮泉，馬得翔，唐任威，鄭懿讚著，「網路概論」，學貫出版社，2005。

2. Roberta Bragg,Mark Rhodes-Ousley,Keith Strassberg, “The Complete Reference Network Security”,學貫出版社, 2004年。

3.Da-Yu Kao and Shiuh-Jeng Wang, “The Behavior Analysis of Investigating Intruder Activities in Internetworks,” Forensic Science, Vol. 48, Sep 1999.

4.沈志昌，「DNS網域安全稽核防護系統之建置」，TANET2003 論文集，台北，2003年。

5.葉士豪，「.tw 網域名稱設定狀況分析」，TANET2002論文集，新竹。

6. Men&Mice, ”Survey Result - Domain Health Survey for .com - February 2004”, http://www.menandmice.com .

7.蔣大偉編譯，PualAlibitz, Cricket Liu著，DNS and BIND，台北，美商歐萊禮，2000年。

8.沈志昌，「DNS安全稽核與防護體系之建置」，樹德科技大學碩士論文，高雄，2003年。

參考資料

一、陳玄玲，許皓翔譯，Windows Server 2003目錄服務與系統管理篇，旗標出版社，2004。