

# 目錄

中文摘要 .....	iii
ABSTRACT .....	iv
圖目錄 .....	v
表目錄 .....	vi
第一章 緒論 .....	1
1.1、研究動機與背景 .....	1
1.2、研究目的 .....	2
1.3、研究範圍與主要成果 .....	3
1.4、論文結構 .....	3
第二章 DNS 安全檢測之研究內容與方法 .....	4
2.1、網路安全現況探討 .....	5
2.1.1、系統軟體安全上的弱點 .....	7
2.2、DNS 安全技術之探討 .....	8
2.2.1、DNS 簡介與設定 .....	10
2.2.2、DNS 進階設定 .....	22
2.3、Nessus 安全檢測之應用 .....	27
第三章 DNS 安全檢測之設計 .....	31
3.1、設計構想與系統模型 .....	32
3.2、設計上的考量與問題分析 .....	35
3.3、DNS 安全檢測之流程 .....	41
3.4、DNS 安全檢測封包格式 .....	43
第四章 安全偵測系統實作與應用 .....	46
4.1、系統架構 .....	46
4.2、DNS 安全檢測說明 .....	47
4.3、系統操作範例 .....	48
4.4、弱點修正連結 .....	53
第五章 結論與未來研究方向 .....	57
5.1、研究成果與貢獻 .....	57
5.2、結論與建議 .....	57
5.3、未來研究方向 .....	58
參考文獻 .....	59
附錄一：Bind 弱點 .....	61

附錄二：DNS 檢測封包格式 .....	70
----------------------	----

## 中文摘要

網際網路是一種新型態的信息溝通管道，不受時間與空間限制的特性，使用者運用此一管道即能快速進行資訊交換。網路族群透過 URL 指定網址到目標網站的同時，均不會感受到網域名稱伺服器(DNS)提供網址轉換的基本服務。DNS 使用分散式資料庫的方式及主從式(Client-Server)架構，控管區域性網路重要資訊，因而延伸出資料同步化、轄區傳送...等問題，再加上軟體設計可能存在的缺失，所造成軟體系統安全上的漏洞，這些均是防護 DNS 安全正常運作必須重視的問題。本論文針對 DNS 安全設定與弱點檢測進行網路安全研究，首先從安全設定上著手，實施 DNS 自身內部防護措施，利用收集相關弱點訊息、了解網域設定功能，考量管轄內網域的需求，並配合使用環境酌量給與限制條件。在此並不是利用設定技巧，完全隔絕 BIND 所發生的安全漏洞，而是著重於被他人入侵時，將危害程度降到最低。接著從弱點檢測的角度，進行外部檢測 DNS 的安全性，本研究提供一個 DNS 安全偵測系統，使用者可以經由瀏覽器連線到安全檢測伺服器，勾選適合的檢測項目，檢測自己網域內 DNS 的安全性，系統於檢測完成後會提供完整之檢測報告，並透過 E\_mail 方式傳送給使用者，報告內容包括 DNS 存在之弱點及弱點修正建議連結。DNS 經由內部安全設定及外部弱點安全檢測後，其安全性必能得到較佳的保障，避免遭受攻擊而導致網路服務中斷。

關鍵字： 網際網路、網域名稱伺服器、網路安全

## **ABSTRACT**

Internet is a new channel of data communication, people can exchange information quickly because of it is not constrained by time and space. Most of Internet users can't perceive the address resolution provided by DNS while they specified the domain name and connected to the desired website. DNS uses the technology of the Distributed Database and the Client-Server structure; controlling important information of the local network, as a result caused the problems of data synchronization and zone transfer. Furthermore, the unhealthy design of software may be caused the incident of invading problems. If the network administrator wants to guarantee the security of DNS, the problems as mentioned above for network security will be considered seriously. This thesis aims at security configuration and vulnerability auditing of DNS. From the outset, the security configuration of DNS can be achieved by using the collecting technology information about DNS appropriately. The correct configuration can only decrease the damage of intrusion, but it does not prevent all of the threat of intrusion. For this reason, the study provides a auditing system of DNS security; users can audit the vulnerability of DNS from the client via the browser, and selecting fit check items for vulnerability auditing. The scanning report will be sent to the user by email after the auditing process is completed. This report includes the existence of vulnerabilities of the DNS, and the patch links for these vulnerabilities. If DNS has a well-defined configuration of security and pass the vulnerability auditing, then its security will be promoted, and the Internet service was not broken due to malicious attack.

Keywords : Internet 、 DNS 、 Network Security

## 圖目錄

圖 2-1	研究步驟.....	5
圖 2-2	2002 CSI 電腦犯罪與安全調查報告.....	6
圖 2-3	澳洲境內 DNS 調查報告.....	7
圖 2-4	國內 DNS 主機版本調查.....	8
圖 2-5	DNS 解析過程.....	11
圖 2-6	named 配置說明.....	12
圖 2-7	nessusd 偵測目標網域.....	28
圖 3-1	澳洲境內 DNS 調查報告（調查 BIND 的安全性）.....	31
圖 3-2	NASL 偵測與運用.....	33
圖 3-3	NASL 模型.....	33
圖 3-4	稽核資料流向.....	34
圖 3-5	掃瞄排程運作.....	35
圖 3-6	DNS 安全檢測整體流程.....	42
圖 3-7	DNS 安全偵測系統之檢測流程.....	43
圖 4-1	DNS 安全偵測系統架構圖.....	47
圖 4-2	登入檢測系統之畫面.....	49
圖 4-3	檢測說明.....	49
圖 4-4	弱點說明.....	50
圖 4-5	單項弱點說明.....	51
圖 4-6	檢測認證.....	51
圖 4-7	檢測報告.....	52
圖 4-8	稽核結果.....	53

## 表目錄

表 2-1	named.conf 全區設定檔 .....	13
表 2-2	named.conf 區域設定檔 .....	14
表 2-3	mis.fwd 正解檔 .....	15
表 2-4	mis.rev 反解檔 .....	19
表 2-5	salve 主機的 named.conf 設定 .....	22
表 2-6	loggin 轉向記錄 .....	23
表 2-7	更改顯示版本 .....	24
表 2-8	options 進階說明(Master) .....	25
表 2-9	options 進階說明(Slave) .....	25
表 2-10	bind_iquery.nasl 稽核檔案 .....	29
表 3-1	調查 BIND 版本弱點數量 .....	40
表 3-2	Bind_query.nasl 編造 resolve 轉送封包 .....	43
表 3-3	DNS Header 區段分析 .....	44

# 第一章 緒論

資訊科技迅速的發展，經由網際網路能與世界各地相連結，開啟無限的商機與網路安全問題，前一波的電子商務風潮更讓大眾了解電子交易的潛在危險。一九九九年兩岸駭客對打，台灣與大陸部分的政府網站被置換，引起一段時間的網路互相入侵事件[1]。2000 年台灣總統選舉期間有些企業的網頁發生被入侵的問題，世界各國並於 911 事件後對網路安全的關心更加顯著，凸顯出網路安全的防護措施與相關稽核機制的重要性。

電腦與網際網路進行連結時，皆需要唯一的網際網路通訊協定(Internet Protocol,IP)位址以便識別，若只是依照 IP 位址進行分辨，對人類而言不是那麼方便區分，為了方便起見，網域名稱系統(Domain Name System,DNS)就因此而誕生，DNS 的功用是負責轉換網域名稱與 IP 位址。轉換過程中需要保護網域內所擁有的主機資訊，以防止重要資訊被駭客(Hacker)或破壞者(Cracker)取得，進而轉向攻擊目標主機。安裝 DNS 服務後必需進一步設定安全防護，防止洩漏網域內主機資訊，以免被有心人士轉為其他用途，而危害整個網域的安全。

本研究將提供在架設 DNS 服務的資訊，並且提出網路安全防護的第一步措施建議，也就是說針對 DNS 設定，提出必要的防護設定建議，再補充現有的修正套件。並且提供遠端測試系統，防範他人利用已發佈的攻擊模式與現有的安全漏洞進行攻擊，除此之外亦可做為強化自我防護偵測的效用。

## 1.1、研究動機與背景

隨著網路的快速成長、使用電腦的人數暴增，對於網際網路通訊協定位址的需求量亦成直線成長，而 DNS 是將 IP 位址翻譯成有意義的名稱，以對應到指定的 IP 位址。這是為了方便人們容易記憶或者是標記著對人們有特殊的意義的電腦，藉以方便告知與表達，免除強記數字號碼的痛苦。DNS 是現今網際網路基礎服務的組成要件之一，使用此項服務的同時，也隱藏洩漏網域內電腦資訊的風險。外部主機藉由詢問 DNS 伺服器，可獲得目標主機的名稱、服務...等資訊。DNS 伺服

器若沒做好安全設定時，則變成他人最容易取得目標網域資訊的寶庫。破壞者或駭客極力於攻擊遠端 DNS 主機，希望能從中獲得操控權限與取得資訊，甚至將受影響的主機變成攻擊第三方的跳板。為了防範此類的事件發生，網路管理者無不苦思對應策略，從系統的安裝、新增元件，即需考慮是否符合系統安全規範，例如使用防火牆(Firewall)或者是使用陷阱系統(Deception or Honeypot system)...等，建築起一道道的防護措施[2]。

以往網域伺服器主機皆有專業的系統管理者，如今電腦數量暴增，作業系統平台種類的增加，如何減少專業人員的負擔及訓練新進人員確實的防護設定技能，是非常重要的的一件事。國際電腦安全協會 (International Computer Security Association, ICISA) 對經過其認證的防火牆進行評估，有 70% 的防火牆在實際使用時會發生安全的漏洞，而發生漏洞皆是管理不善或人為設定所造成的，由此可充分顯示出資訊安全是一項非常重視管理的工作。有鑑於此，本研究以提供基本的 DNS 安全設定的建議，藉以防護系統，提供首要的工作檢視項目。再利用 Nessus 的檢測模式針對網域名稱伺服器進行遠端檢測工作，讓遠端使用者透過網際網路，針對管轄內的網域伺服器進行檢測，防範軟體產生系統安全上的漏洞，被有心人士所利用。軟體的系統安全弱點(Software Vulnerability)被 Bruce Schneider 將其歸類成為一種名叫打破玻璃越過窗戶 (檢視系統的設計及實作已發佈漏洞)，即可毫不費心進行開鎖 (破解密碼學演算法與安全協定) 的攻擊方式[3]。若不注意這方面的問題，豈不是更是給與駭客更多的機會嗎？

## 1.2、研究目的

本研究目的在於增進 DNS 主機防護能力，對於未能完整修正的系統提供相對應的解決措施，希望能達到下列的目標：

1. 提高入侵者的攻擊門檻：想入侵者可能經由 DNS 服務取得目標網域主機的資訊。即利用設定技巧進而隱藏其他主機資訊，以提高攻擊的困難度。
2. 提高系統管理者維護主機能力：利用已知的修正與核對方式，讓系統管理

員更了解主機的弱點與需要注意之處。

3. 減少已公布弱點的維護成本：檢測已存在的弱點資料，使系統免除已有公佈訊息或修正套件的攻擊，期以減少不必要的維護成本。

### 1.3、研究範圍與主要成果

網路安全的相關議題太過於廣大，本研究的出發點以資管系 DNS 主機為研究基礎，而局限於 DNS 系統的安全設定與漏洞偵測系統的實作，於有限的時間內，對下列幾個研究假設進行討論：

1. 內部管理控制網域的人員並不會對伺服器造成安全上的威脅，其風險皆來自於內部不正確的設定或外部的攻擊。
2. Linux 平台上已做好必要的安全措施，對 DNS 系統的運作不會產生威脅或不利的影響。

本研究主要成果如下：

1. 提出 DNS 安全設定上的建議。
2. 利用遠端偵測以發現 DNS 的漏洞，並且給與建議修正方式。

### 1.4、論文結構

本文共分成五章，第二章為 DNS 防護偵測研究之內容與方法，針對網路安全現況做探討，並說明 DNS 原理、安裝與設定的方法、安全防護建議等。第三章為介紹 DNS 防護偵測之原理，並詳細說明系統的設計構想與模組功能。第四章說明系統實作與防護偵測之應用；最後在第五章則作一簡短的結論並且提出未來研究方向，以供後續研究之參考。

## 第二章 DNS 安全檢測之研究內容與方法

隨著網際網路盛行，網路安全問題逐漸受到重視，因為網路安全的範疇太過於廣泛，本章主要針對 DNS 安全性做探討與分析，從設定資管系 DNS 伺服器的組態與外部弱點檢測，進行雙管齊下的防護設定與測試。由二種不同的角度相互探討，嚴密防護網域伺服器的安全並將可能發生的損壞降至最低，以增進網域伺服器的可靠性，讓各項網路服務得以正常、持續的運作。

圖 2-1 為本論文的研究架構，詳細說明如下：

1. 相關研究探討：收集網域伺服器的相關漏洞與安全性探討，找出提高安全性的方法。
2. 建構網域設定、蒐集資訊：取得資管系 DNS 伺服器的需求資訊後，即著手設定系統與規劃必要的安全限制，並且從設定系統過程中，蒐集相關知識。
3. 規劃、建構偵測系統：規劃偵測系統架構，收集伺服器已知弱點偵測，並提供修正連結與建議。建構偵測系統是使用主從(Client-Server)式服務，使偵測系統能透過網路進行操控。
4. 設定評估與系統實作：操控偵測系統對本機進行弱點測試，評估本機的安全設定是否符合需求，並針對系統設計缺失進行改善。
5. 結論與建議：本研究使用交叉式防護措施中，最後得知使用非最新版本的 DNS 服務，是無法同時顧及本機安全與系統方便運作，最後只能建議升級到最新版本，以免除惱人的弱點修補問題。

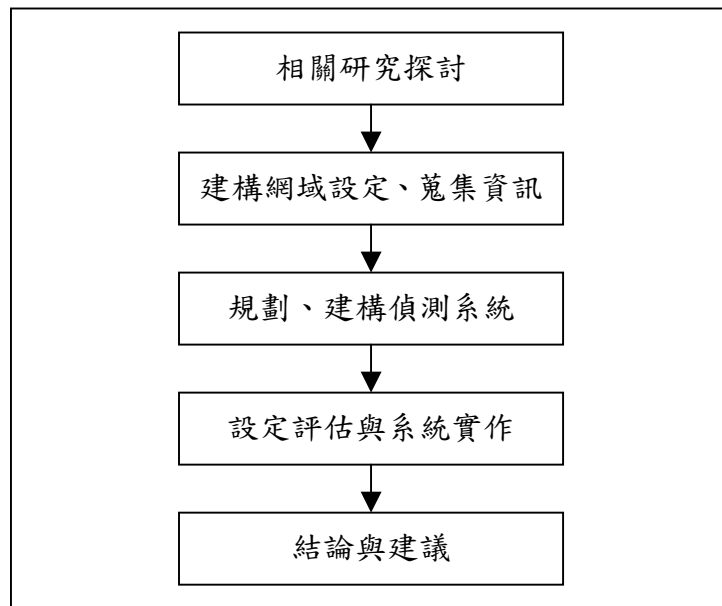
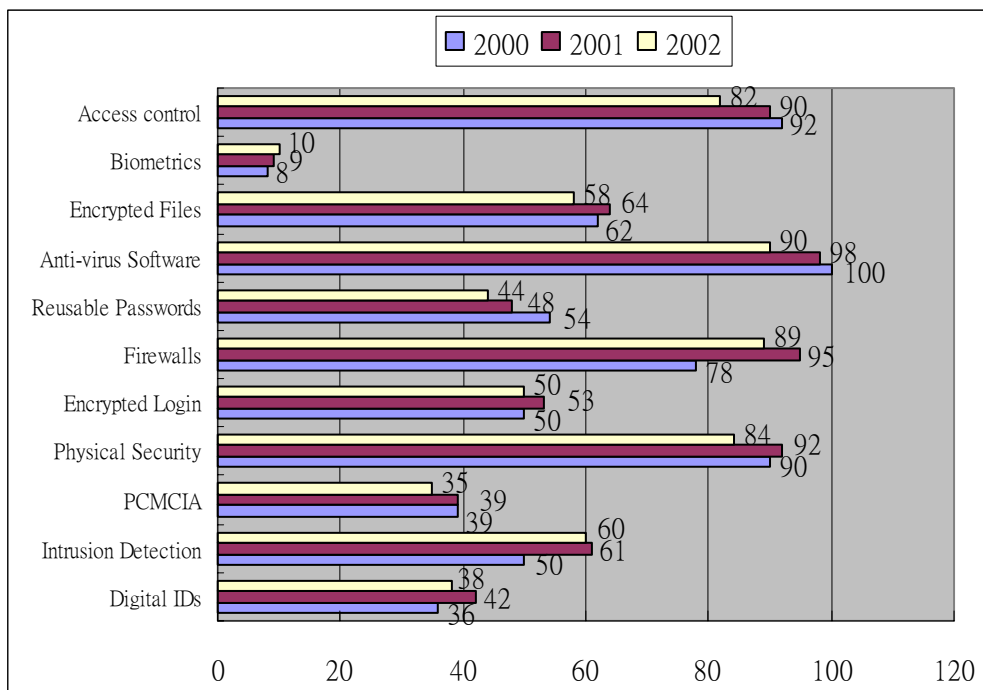


圖 2-1 研究步驟

## 2.1、網路安全現況探討

美國 CSI 與 FBI 合作調查報告顯示[4]，電腦犯罪與網路入侵事件已對美國造成經濟與對外競爭力的損害。依照美國國內 503 家電腦安全團體(美國的社團法人、政府單位、金融機構、醫學機構與大學院校...等)所回應的資訊，顯示於圖 2-2 總共歸類出 11 項入侵事件模式(分別為 Access control、Biometrics、Encrypted Files、Anti-virus Software、Reusable Passwords、Firewalls、Encrypted Login、Physical Security、PCMCIA、Intrusion Detection、Digital IDs)，並在每一種入侵事件模式下，提供 2000 年、2001 年與 2002 年間，電腦安全團體遭遇入侵事件的回應百分比。依據此調查報告得知，2001 年度總計已造成數億美元的損失。



回應的百分比

圖 2-2 2002 CSI 電腦犯罪與安全調查報告

參考來源：2002 Computer Crime and Security Survey

網際網路提供人們資訊傳輸與溝通，嚴然構成一個虛擬世界，我國網際網路用戶人數已高達到六百萬。虛擬的網路世界與實質世界不同，各項法規一時間難以制定、執行法律規範條文，無法限制規範網路活動。因此入侵事件層出不窮，尤其是透過網際網路營運的電子商務感受最為強烈[5]。

許多企業為了趕上號稱第二次工業革命的潮流，利用網際網路的便利性組合不同的配套措施，加速在新環境的應變能力、提高生產力，並且透過網路整合跨區域的關聯企業，形成網路商業自動化。防火牆可說是電子商務的必備設施之一，國際電腦安全協會指出，系統管理者若想利用建設防火牆，來阻擋攻擊者或駭客的入侵，在防火牆的安全設定上必需擁有專業知識，否則無法防治入侵事件[6]。DNS 伺服器也是如此！有網際網路大門之稱的 DNS 伺服器，也需要依靠設定、安裝修正程式與更新版本來提供防護能力，在環境與安全的設定上，因應不同的需求服務，常導致交叉限制，並且讓攻擊者有機可乘[7]。因此在滿足環境設定之餘

更需給與安全相關限制，才能將損失、風險減為最低。

### 2.1.1、系統軟體安全上的弱點

科技發展至今，電腦設施已是企業、學校、團體不可或缺的設備之一，系統軟體功能越來越強大，所包含的服務種類就越多。DNS 服務是提供網路 IP 位址與網域名稱間的轉換服務，因此許多的團體亦安裝這種服務，便於區域網路(Local Area Network,LAN)與廣域網路(Wide Area Network,WAN)間的主機辨識。然而 DNS 服務亦隱藏了某些危機。根據 DNS Security in Australia 在 2000 年六月提出一份調查報告[8]，針對網路上提供 DNS 服務的主機做隨機取樣調查，依照網域分類進行系統檢測，圖 2-3 看到每一項偵測網域內各有三條長條圖，分別為 Vulnerable Root Compromise、Vulnerable Dos 與偵測範圍內的主機數目。從圖 2-3 中可得知，澳洲境內平均 70% 以上的 DNS 主機可能存有漏洞。

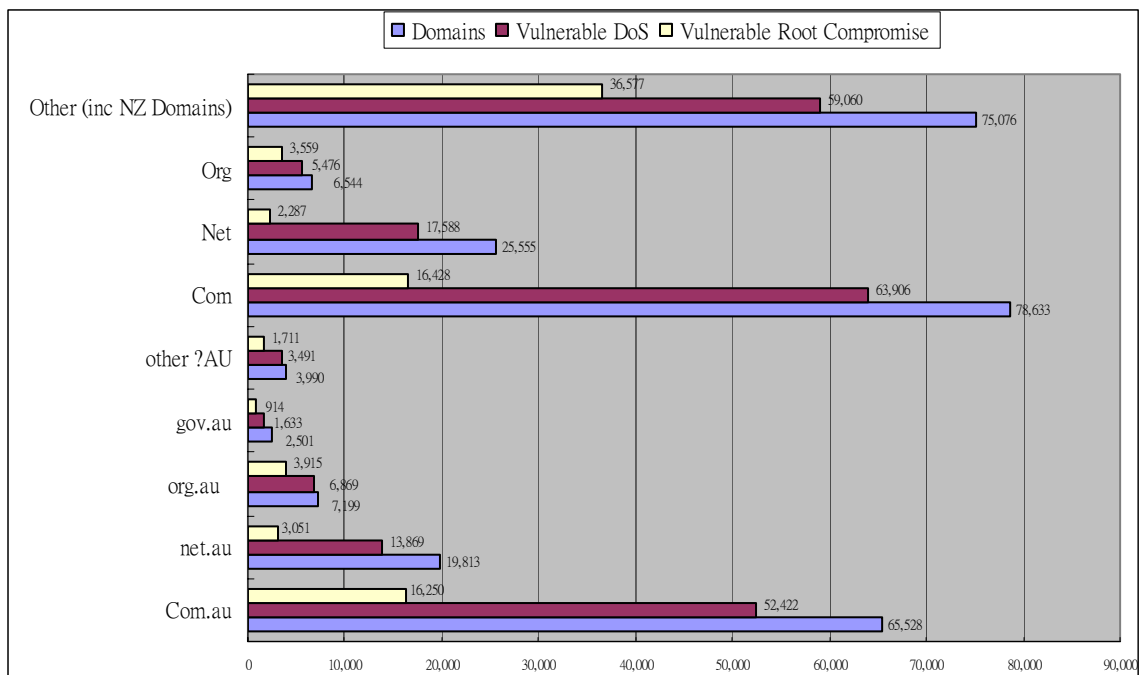


圖 2-3 澳洲境內 DNS 調查報告

參考來源：DNS Security in Australia

最近的調查顯示，台灣地區有關於 DNS 伺服器版本資訊共有 11053 筆，如圖 2-4 所示，本研究對照弱點分佈情況，將其分成五個區段，其中 Other 是指無法查

出其版本，或是不在調查範圍內。從統計數字中得知，約有 38% 左右的 DNS 伺服器使用 4.9.3~4.9.7 與 8.1.1~8.2.2 版本，這些舊版本存在著多種類型弱點，可能成為駭客攻擊的主要目標。DNS 是網際網路中最基本的服務之一，竟然有這麼高比例的伺服器存有漏洞，這是值得我們重視的問題。

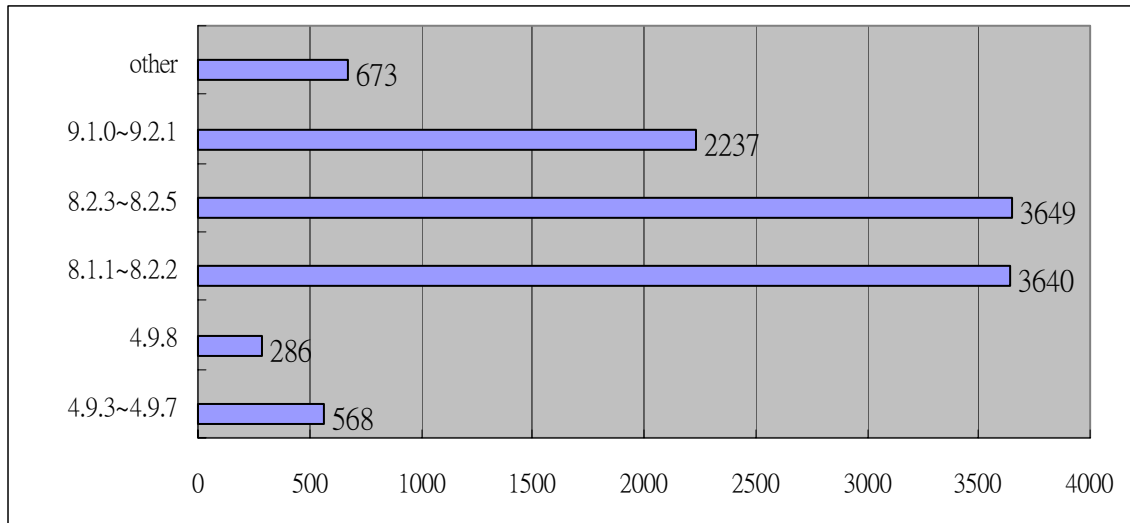


圖 2-4 國內 DNS 主機版本調查

## 2.2、DNS 安全技術之探討

建置一個 DNS 伺服器，前題是需要申請一個網域名稱，國外有些網站可提供免費的網域名稱。網域註冊應是向亞太地區網路資訊中心(APNIC)申請，在國內則是由台灣網路資訊中心(TWNIC)[9]承接管理。早期 TWNIC 未成之時，各大型的 ISP 業者已直接向 APNIC 申請，現今以 TWNIC 為主要申請處。現在亦可透過各大型的 ISP 業者申請即可，其中更提供 Whois 搜尋引擎。Whois 是一套可用來查詢網域名稱或 IP 位址的應用程式，當然必需知道網域名稱或者是 IP 位址才能找出相關資料。舉個例子說明較容易了解，以國內的台灣網路資訊中心 (<http://www.twnic.com.tw>) 網頁中，所提供的 Whois 搜尋引擎，鍵入 [www.kimo.com.tw](http://www.kimo.com.tw)，即顯示另一視窗並顯示該網域資料。資料內容有註冊的公司名稱、網域名稱、連絡對象與方式，可查到指定的 IP 位址與對應的網域名稱，並且可查詢註冊時，網域名稱的相關網址名稱或是 IP 位址登記在何種轄區(zone)下。

可查到主機的名稱，然而大多數的系統管理者為了方便管理，將網域名稱直接寫 dns.mis.stu.edu.tw、ns.mis.stu.edu.tw，攻擊者可輕鬆得知那一台主機才是正確的攻擊目標。

DNS expert[10] 是專為偵測、診斷 DNS 服務弱點所設計的軟體，主要偵測範圍在於 Bind 8，並且不限制於對被偵測方的作業系統。DNS expert 偵測軟體提供微軟與 Mac 二種不同系統安裝套件，並且提供免費的 30 天試用版，但是試用版軟體的功能並不完整，只能做出簡單的測試。試用版軟體只能使用最低偵測權限，並且無法修改系統的預設偵測選項。DNS expert 偵測軟體提供四個偵測服務：

1. Analyze Zone：提供三種預設選項(簡略、一般與完整偵測)，讓使用者直接選擇目標主機的位址即可，使用者也能自定適合偵測項目，主要可分為 A records、CNAME records、MX records、NS records、SOA records、HINFO records、PTR records、Delegation、Security 及 Miscellaneous 等十個選項，並且顯示偵測結果，最後連結回網頁中讀取相關建議事項，避免新增功能時無法即時運用，以達成掃瞄資料的同步化。
2. DNS Query：針對 A records、CNAME records、MX records、NS records、SOA records、HINFO records、PTR records、Any records type 及 zone transfer 傳送請求(query)，讀取、顯現回應請求的內容。雖然可在 DNS 主機上，經由手動鍵入指令的方式取得這些資訊，而這套軟體所提供的選項界面，較為方便與容易操作。
3. Ping Host：此項功能是電腦中最為普遍的，其優點是提供圖形介面，可輕易的改變參數，並且提供統計數字、長條圖..等，方便使用者觀看結果。
4. Trace Route to Host：此項功能在 Unix like 系統中皆提供這服務，但 DNS expert 以圖形顯示資訊，讓使用者更容易操縱與識別資訊的意義，並且提供統計數字、長條圖..等，方便使用者觀看結果。

這一套檢測軟體為 DNS 伺服器的管理網域為檢測範圍，以發覺 DNS 伺服器是否

有問題，並且適用於 Bind 8 的版本，若想檢測大量主機時，建議使用此套軟體，了解、增進 DNS 伺服器的安全性。

### 2.2.1、DNS 簡介與設定

1960 年代末期，美國國防部的先進研究計畫署(Department of Defense's Advanced Research Projects Agency, ARPA，後來稱為 DARPA)，ARPnet 中電腦都有其特殊的主機名稱與網路位址，當時以文字檔記錄相互對應的 IP 位址與主機名稱。1980 年代初期，ARPnet 採用傳輸控制協定/網際網路協定(Transmission Control Protocol/Internet Protocol, TCP/IP)，加上 1984 年南加大(USC)的 Paul Mockapetris，發表了 RFC 882 與 RFC 883，使網域名稱系統正式呈現世人的眼前，最大的推手即是柏克萊大學，將 BSD Unix 開放給各大學免費使用，因此網域名稱系統與網際網路的使用數量皆漸漸有所成長。[11]

DNS 服務在網際網路上可說是必備的功能，幾乎所有關於網路服務都需要使用到它，如：WWW、電子郵件...等。相信一般的網路使用者皆使用過這服務，但不清楚其運作模式，只有需要管理網域的系統管理者才會接觸這套服務。以樹德科技大學計算中心所架設的 BBS 站為例，其 IP 位址是 210.71.11.222，但單純看這些數字並無法直接了解其代表含意；bbs.stu.edu.tw 也是代表相同的 BBS 站，然而這些英文字可明顯的表示「台灣地區 / 教育學界 / 樹德科技大學 / bbs 站台」。從難以記憶的數值到有意義的文字，則需要依賴 DNS 伺服器的轉換服務。

DNS 是一套分散式資料庫，資料庫被分成多個區段，各個區段則是由所屬的區域性組織負責控管與維護。區段是指圖 2-5 (root)的每一個分支，所形成的樹狀圖即是一個區段。若想由網路取得各區的資訊，則必需透過主從式(Client-Server)架構取得，然而分散式資料庫最令人擔心的是同步化的問題，而 DNS 是使用複製(replication)與快取(caching)的方式，取得、儲存上層伺服器的訊息，提供穩定的查詢服務，而且不影響 DNS 服務的品質。名稱伺服器的職責是維護分散式資料庫中的區段資訊，提供用戶端查詢；用戶端又稱為解析器(resolver)，解析器是一組函式庫常式(library routine)，主要作用是產生查詢命令，經由網路傳遞到名稱伺服器，

以搜尋其他的網域空間，找出非管轄內的資料[12]。以圖 2-5 說明 DNS 的解析過程，DNS 伺服器的用戶也就是一般使用者，想進入某一網站時，需要向本端的 DNS 主機查詢網站名稱與 IP 對應資訊，使用者在取得資訊後即可順利登入網站；若 DNS 伺服器的快取記憶中沒有記載相關資訊時，伺服器則使用階層式向上層伺服器詢問，直到找到資訊為止。

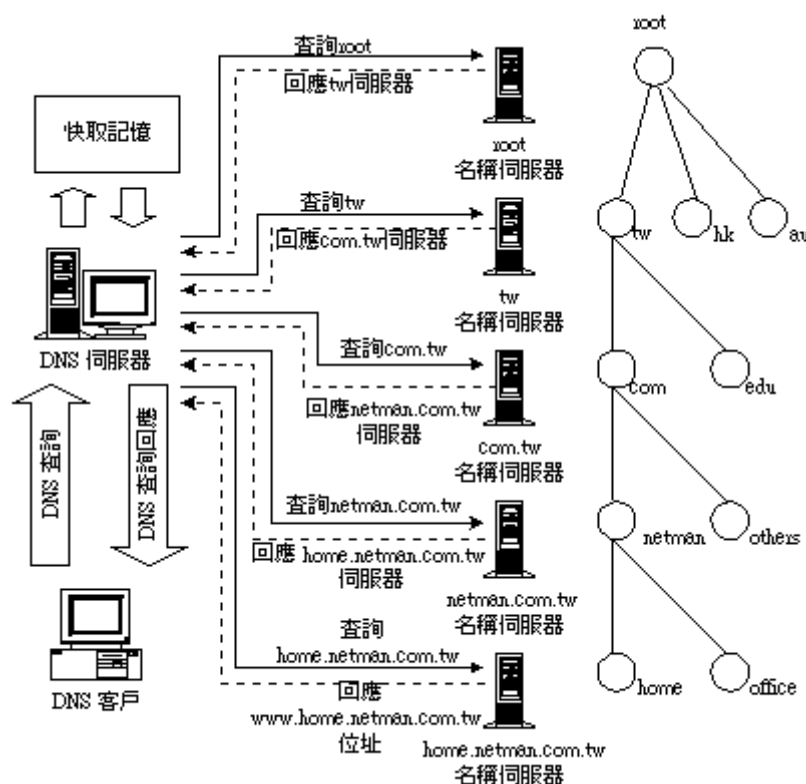


圖 2-5 DNS 解析過程

圖形來源：<http://www.study-area.net/linux/linuxfr.htm> (dns2.gif)[12]

關於 DNS 的設定參考資料總共有三個來源[11][12][13]，主要目的是設定 DNS 服務基本需求，以樹德科技大學資訊管理系的 DNS 服務作為說明實例。資管系共有 Master 與 Slave 二台 DNS 伺服器，Slave 是預防 Master 忽然中止服務時，可替代 Master 運作的伺服器。本研究的 DNS 服務是建置於 Linux 作業系統上，圖 2-6 為 Master 主機配置說明圖。DNS 伺服器的設定需求，總共使用六個設定檔案，分別存放在 /etc/ 及 /var/named 兩個目錄中：

```

/etc/
  named.conf
/var/named
  named.cache
  localhost
  127.0.0
  mis.fwd
  mis.rev

```

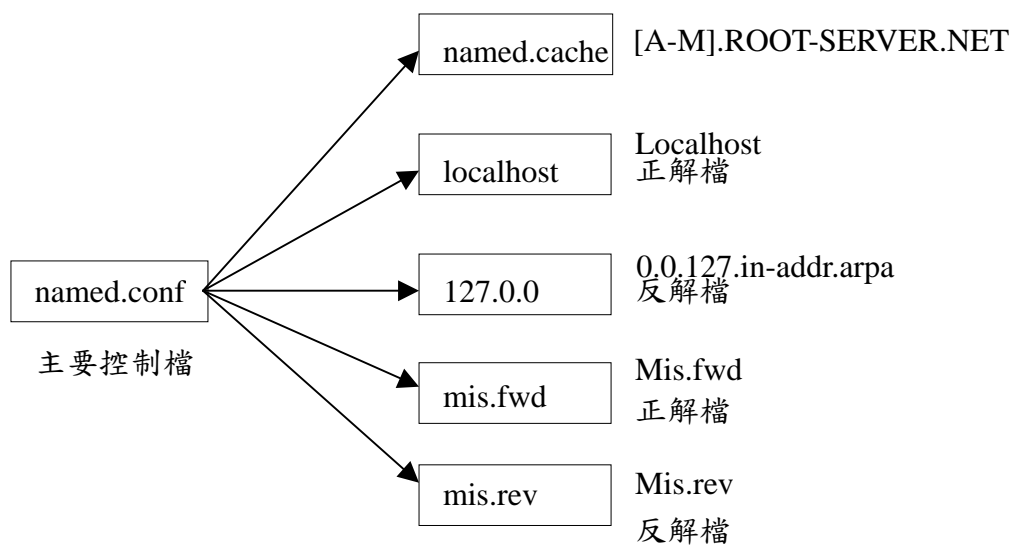


圖 2-6 named 配置說明

開始 DNS 設定介紹之前，先說明註解符號。named.conf 設定檔中，每個完整的設定結束時皆需加上”；”。BIND 8 有幾種註解符號，“//”為一整行的註解；”/\*” “\*/”是註解所包含的整段說明；”#”是為一整行註解。緊接著介紹正解與反解的意義：

1. 正解 (forward mapping)：是網域名稱對應到 IP 位址。例如：  
dns.mis.stu.com.tw -> 210.71.14.64，負責配置 mis.stu.com.tw 網域內網域名稱與 IP 位址的對應。
2. 反解 (reverse mapping)：是 IP 位址對應到網域名稱。例如：210.71.14.64

-> dns.mis.stu.com.tw。負責配置整個 IP 位址與網域名稱的對應。

表 2-1 為 named.conf 全區設定檔，也是 DNS 最重要的設定檔，關聯著其他五個設定檔案，本研究中不更改 named.cache、localhost.zone、named.local 這三個最基礎的設定檔。

表 2-1 named.conf 全區設定檔

```
options {
    check-names master fail; // default fail
    directory "/etc/named";
    pid-file  "/etc/named.pid";
    notify yes;
// fake-iquery yes; // default warn
// forwarders { 210.71.4.60; };
// host-statistics yes; // default no
transfer-format many-answers;
allow-update { none; };
recursion no;
allow-query { any; };
allow-transfer { 210.71.14.0/24; };

    key master-slave {
    algorithm hmac-md5;
    secret "ele9H+VlhBkCWf/C5NnGnw=="; };
    server 210.71.14.95 {
    transfer-format many-answers;
    keys { master-slave; }; };
};
```

解說 options 的設定內容：

1. “check-names master fail”是偵測出網域名稱錯誤時，會發出警告；若有 slave 伺服器，可加入“check-names slave fail”，也有相同的功能。
2. directory "/etc/named"：是指定 named 的讀取位置。即是指定其他五個設

定檔的所在地，在往後的設定就可以使用相對路徑，以便於讀取設定檔。

表 2-2 設定 localhost、mis.stu.edu.tw 為正解，0.0.127.in-addr.arpa、14.71.210.in-addr.arpa 為反解。若在其選項下設定規則時，只適用於區域轄區內的運作，否則比照 option 的設定值辦理。

表 2-2 named.conf 區域設定檔

```
Zone "." {
    type hint;
    file "root.cache";
};

zone "localhost" {
    type master;
    file "localhost";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "127.0.0";
};

zone "mis.stu.edu.tw" {
    type master;
    file "mis.fwd";
    also-notify { 210.71.14.95 ; };
    allow-transfer [ 210.71.14.0/24;
                    210.71.14.61;
                    210.71.14.94;
                    210.71.14.95; ];
};

zone "14.71.210.in-addr.arpa" {
    type master;
    file "mis.rev";
    allow-transfer [ 210.71.14.0/24;
```

```

                210.71.14.61;
                210.71.14.94;
                210.71.14.95; };
};

```

舉表 2-2 選項內的 mis.stu.edu.tw 轄區設定進行說明：

1. Zone 代表轄區，其後面緊接著網域名稱(mis.stu.edu.tw)與類別(IN 代表 Internet)。
2. type master：是指出伺服器的類型為 master。
3. file 是設定正解與反解轉換對應的檔案(mis.rev 反解檔)。
4. allow-transfer：是允許網域主機自行更新、讀取 DNS 轄區內的記錄。

/var/named/named.cache 是記載著 DNS 伺服器區域性最高層主機的位址資訊，啟動服務時名稱伺服器會將內容載入快取(cache)中，檔案中記載著 13 個編號由 a~m 的 ROOT-SERVER.NET 網域位址，這些 root 伺服器分別掌控 13 個最高層的網域資料。若需取得這個檔案時，可使用暱名(anonymous)登入 ftp.rs.internic.net 或 192.41.0.5 載回 name.root 檔案，再改名為 named.cache 即可。

在設定時有二點需要注意：

1. 網域伺服器可能會變動，所以每當一段時間，需要做更新的動作。
2. 註解的問題，named.conf 中是使用雙斜線“//”，而這裡則使用分號“；”。

表 2-3 mis.fwd 正解檔

```

$TTL    3600
$ORIGIN mis.stu.edu.tw.
@ IN SOA  dns.mis.stu.edu.tw. administrator.dns.mis.stu.edu.tw. (
                20020502417    ;Serial
                10800           ;Refresh
                1800            ;Retry

```

```

        604800           ;Expir
        3600 )          ;Minimum
@ IN NS dns.mis.stu.edu.tw.
  IN NS arjar.mis.stu.edu.tw.
  IN NS jscheng.mis.stu.edu.tw.
  IN NS ns2.mis.stu.edu.tw.
  IN MX 0 linux.mis.stu.edu.tw.
  IN MX 10 net.mis.stu.edu.tw.

localhost IN CNAME localhost.
loopback  IN CNAME localhost.
ad        IN A    210.71.14.87
agent     IN A    210.71.14.115
arjar     IN A    210.71.14.95
mdk       IN CNAME arjar.mis.stu.edu.tw.
bagaro    IN A    210.71.14.96
ca        IN A    210.71.14.73
cab       IN A    210.71.14.120
cclai     IN A    210.71.14.80
cclee     IN A    210.71.14.106
cclin     IN A    210.71.14.100
cclin-2   IN A    210.71.14.78
ccna      IN A    210.71.14.84
crm       IN A    210.71.14.117
crv       IN A    210.71.14.89
dns       IN A    210.71.14.64
ecg       IN A    210.71.14.99
          IN A    210.71.14.114
ec        IN A    210.71.14.111
ec8100lp  IN A    210.71.14.81
ecai      IN A    210.71.14.103
ecsa      IN A    210.71.14.112
ewap      IN A    210.71.14.98
freebsd   IN A    210.71.14.126

```

gis	IN	A	210.71.14.69
gl	IN	A	210.71.14.88
gl1	IN	A	210.71.14.68
gl2	IN	A	210.71.14.72
homepage	IN	A	210.71.14.67
hunt	IN	A	210.71.14.86
hunt-mob	IN	A	210.71.14.119
imwap	IN	A	210.71.14.75
is	IN	A	210.71.14.77
is-data	IN	A	210.71.14.118
johnw	IN	A	210.71.14.101
jscheng	IN	A	210.71.14.94
jsp	IN	A	210.71.14.108
khsu	IN	A	210.71.14.109
lcrab	IN	A	210.71.14.79
lin2	IN	A	210.71.14.91
linux	IN	A	210.71.14.99
mcom	IN	A	210.71.14.104
mis8100lp	IN	A	210.71.14.82
mobile	IN	A	210.71.14.70
net	IN	A	210.71.14.114
net1	IN	A	210.71.14.113
neumann	IN	A	210.71.14.105
ns	IN	A	210.71.14.127
ns2	IN	A	210.71.14.61
pc1	IN	A	210.71.14.71
peterw	IN	A	210.71.14.92
ra	IN	A	210.71.14.74
rab	IN	A	210.71.14.122
rose-tutorial	IN	A	210.71.14.116
salamander	IN	A	210.71.14.90
slp	IN	A	210.71.14.76
speed	IN	A	210.71.14.66
ss	IN	A	210.71.14.121

ssb	IN	A	210.71.14.123
stucjs	IN	A	210.71.14.124
sun	IN	A	210.71.14.107
sun100	IN	A	210.71.14.93
ths	IN	A	210.71.14.125
travel87	IN	A	210.71.14.83
tsn	IN	A	210.71.14.102
uml	IN	CNAME	is.mis.stu.edu.tw.
wap	IN	A	210.71.14.110
web	IN	A	210.71.14.85
wilee	IN	A	210.71.14.97
www	IN	A	210.71.14.65

表 2-3 mis.fwd 設定檔案的名詞說明如下：

1. TTL (Time To Live) 3600：是記錄檔一經讀取後，需經過 3600 秒後才會再重新讀取檔案內的設定，而 3600 秒即是一小時(60\*60)。
2. 設定 ORIGIN 網域名稱時需要注意，必需要以 “.” 做為結束。以 www (ftp, mail) 為例，會自動接上 origin 所設定的網域，即是 www.mis.stu.edu.tw.。當然也可以直接鍵入完整的名稱，如 www.mis.stu.edu.tw.。
3. @ 是一個縮寫符號，代表對應的 domain，也就是 mis.stu.edu.tw. 的縮寫，接著的二個參數是指主機的定義與負責人的電子郵件。(注意：這二個參數需要指定，最後皆需要加上 “.” 做為結尾，電子郵件部份以 “.” 替代 “@”。使用 “.” 做為結尾名稱即為 “全域名稱” (Fully Qualified Domain Name, FQDN)，，以網址全名定確主機名稱。

**Serial** 前面的數字是代表設定的年月日與修改的次數。檔案內容經過變動後，需要增加修改次數，讓 Slave 伺服器核對是否需要進行 zone transfer。

**Refresh** 通知 Slave 伺服器，每隔 10800 秒就要核對 Serial 是否有變動過。

Retry Slave伺服器無法進行核對Serial時，每隔1800秒再核對一次。

Expire 當Slave伺服器超過604800秒無法與Master連絡時，即將檔案內的資標記為過期資料。

Minimum 設定最小的TTL值為3600秒，若沒在前面使用“\$TTL”定義值，即會讀取Minimum設定值。

4. 設定網域名稱與 IP 的對應(如：arjar IN A 210.71.14.95)。  
CNAME 可讓多個網址名稱指向同一主機，arjar,mdk -> arjar.mis.stu.edu.tw。
5. SOA(Start of Authority)：用來指定轄區(zone)內的最佳權威來源(主機)。
6. NS(Name Server)：指定 domain 是那一台名稱伺服器負責。
7. A(address)：設定網址名稱與 IP 位址的對映關係，也就是網域名稱與 IP 位址的轉換。
8. PTR(pointer)：設定 IP 位址與網址名稱的對映關係，也就是 IP 位址與網域名稱的轉換。
9. CNAME (canonical name)：為主機的名稱定義別名，並且對應真實主機的網址名稱。
10. MX (mail exchanger)：設定經由 mail exchanger 轉送郵件訊息。

表 2-4 為 mis.rev 反解檔的內容，前段的使用規則與前面上述的內容相同，不同的是使用 PTR 為 IP 位址與網域名稱做為對應。

表 2-4 mis.rev 反解檔

\$TTL	3600
@ IN SOA	dns.mis.stu.edu.tw. administrator.dns.mis.stu.edu.tw. (
	2002052417
	10800

```
3600
604800
3600 )
@      IN  NS  dns.mis.stu.edu.tw.
@      IN  NS  arjar.mis.stu.edu.tw.
$ORIGIN 14.71.210.in-addr.arpa.
100 IN  PTR  cclin.mis.stu.edu.tw.
101 IN  PTR  johnw.mis.stu.edu.tw.
102 IN  PTR  tsn.mis.stu.edu.tw.
103 IN  PTR  ecai.mis.stu.edu.tw.
104 IN  PTR  mcom.mis.stu.edu.tw.
105 IN  PTR  neumann.mis.stu.edu.tw.
106 IN  PTR  clee.mis.stu.edu.tw.
107 IN  PTR  sun.mis.stu.edu.tw.
108 IN  PTR  jsp.mis.stu.edu.tw.
109 IN  PTR  khsu.mis.stu.edu.tw.
110 IN  PTR  wap.mis.stu.edu.tw.
111 IN  PTR  ec.mis.stu.edu.tw.
112 IN  PTR  ecsa.mis.stu.edu.tw.
113 IN  PTR  net1.mis.stu.edu.tw.
114 IN  PTR  net.mis.stu.edu.tw.
115 IN  PTR  agent.mis.stu.edu.tw.
116 IN  PTR  rose-tutorial.mis.stu.edu.tw.
117 IN  PTR  crm.mis.stu.edu.tw.
118 IN  PTR  is-data.mis.stu.edu.tw.
119 IN  PTR  hunt-mob.mis.stu.edu.tw.
120 IN  PTR  cab.mis.stu.edu.tw.
121 IN  PTR  ss.mis.stu.edu.tw.
122 IN  PTR  rab.mis.stu.edu.tw.
123 IN  PTR  ssb.mis.stu.edu.tw.
124 IN  PTR  stucjs.mis.stu.edu.tw.
125 IN  PTR  ths.mis.stu.edu.tw.
126 IN  PTR  freebsd.mis.stu.edu.tw.
127 IN  PTR  ns.mis.stu.edu.tw.
```

61	IN	PTR ns2.mis.stu.edu.tw.
64	IN	PTR dns.mis.stu.edu.tw.
65	IN	PTR www.mis.stu.edu.tw.
66	IN	PTR speed.mis.stu.edu.tw.
67	IN	PTR homepage.mis.stu.edu.tw.
68	IN	PTR gl1.mis.stu.edu.tw.
69	IN	PTR gis.mis.stu.edu.tw.
70	IN	PTR mobile.mis.stu.edu.tw.
71	IN	PTR pc1.mis.stu.edu.tw.
72	IN	PTR gl2.mis.stu.edu.tw.
73	IN	PTR ca.mis.stu.edu.tw.
74	IN	PTR ra.mis.stu.edu.tw.
75	IN	PTR imwap.mis.stu.edu.tw.
76	IN	PTR slp.mis.stu.edu.tw.
77	IN	PTR is.mis.stu.edu.tw.
78	IN	PTR cclin-2.mis.stu.edu.tw.
79	IN	PTR lcrab.mis.stu.edu.tw.
80	IN	PTR cclai.mis.stu.edu.tw.
81	IN	PTR ec8100lp.mis.stu.edu.tw.
82	IN	PTR mis8100lp.mis.stu.edu.tw.
83	IN	PTR travel87.mis.stu.edu.tw.
84	IN	PTR ccna.mis.stu.edu.tw.
85	IN	PTR web.mis.stu.edu.tw.
86	IN	PTR hunt.mis.stu.edu.tw.
87	IN	PTR ad.mis.stu.edu.tw.
88	IN	PTR gl.mis.stu.edu.tw.
89	IN	PTR crv.mis.stu.edu.tw.
90	IN	PTR salamander.mis.stu.edu.tw.
91	IN	PTR lin2.mis.stu.edu.tw.
92	IN	PTR peterw.mis.stu.edu.tw.
93	IN	PTR sun100.mis.stu.edu.tw.
94	IN	PTR jscheng.mis.stu.edu.tw.
95	IN	PTR arjar.mis.stu.edu.tw.
96	IN	PTR bagaro.mis.stu.edu.tw.

```
97 IN PTR wilee.mis.stu.edu.tw.
98 IN PTR ewap.mis.stu.edu.tw.
99 IN PTR linux.mis.stu.edu.tw.
linux IN MX 10 linux.mis.stu.edu.tw.
uml IN CNAME is.mis.stu.edu.tw.
```

至於 Slave 伺服器的設定是非常簡單，只需要到 named.conf 檔案下，設定成表 2-5 系統即可自行運作。

表 2-5 salve 主機的 named.conf 設定

```
options {
    pid-file "/var/run/named/named.pid";
    directory "/var/named";
zone "mis.stu.edu.tw" {
    type slave;
    masters { 210.71.14.64; };
    file "slave.file";
    allow-transfer { none; }; };
zone "14.71.210.in-addr.arpa" {
    type slave;
    masters { 210.71.14.64; };
    file "slave.rev";
    allow-transfer { none; };
};
```

### 2.2.2、DNS 進階設定

檢測 DNS 弱點與進行安全防護時，大多數的建議是更新版本與安裝修正程式，難道不使用這二種方法就無法解決問題嗎？答案是使用這二種方法最為簡易。安裝修正程式是維護安全必備的動作，然而是否要更新為最新版本則是一項爭議之處，本研究建議最佳的做法是經過大規模變革後才需安裝新版本(如：Bind 4 與 Bind 8 或 Bind 9)。若不想費時與費力升級版本時，建議使用轄區轉送(zone transfer)的特性，即是利用 Mater/Slave 關係，將主機的資訊進行轄區轉移、更新。

如此一來可節省不少重新設定的時間，請注意這種方式不適用於 Bind 4 升級至 Bind 8 或 Bind 9 版本。

進階設定主要的用途在於保存啟動 DNS 服務期間的相關紀錄，留下攻擊者或駭客攻擊行為的證據，做為網域管理員追蹤攻擊者或駭客的依據，並且可以進一步紀錄分析攻擊模式，防範再有相同的攻擊行為。本研究建議進階設定安裝在 Bind 8.2.3 之後的版本，而且網域管理員應該時常檢視是否有最新安全通告及時常觀看、分析 log 記錄檔。

表 2-6 針對 BIND DNS 服務套件進行的安全配置，並且取得完整的 log 訊息，以利於防護、限制攻擊者的行為，並且防護已知的 BIND 漏洞，將漏洞所造成的影響降為最低。本研究希望記錄整個安全事件，並且保有原來系統所收錄的訊息，也就是日誌系統。管理日誌系統需要認識類別(category)與通道 (channel)，通道是指示日誌資料可以將訊息送到多個通道。

表 2-6 login 轉向記錄

```
Logging {
  channel LAMER_log {
    file "/var/log/dns-lamer.log" versions 3 size 10m;
    severity info;          # only send priority info and higher
    print-severity yes;    print-timeyes;
  };
  channel SEC_log {
    file "/var/log/dns-sec.log" versions3 size 10m;
    severity info;          # only send priority info and higher
    print-severity yes;    print-timeyes;
  };
  channel STAT_log {
    file "/var/log/dns-stat.log" versions 3 size 10m;
    severity info;          # only send priority info and higher
    print-severity yes;    print-timeyes;
  };
}
```

```
category cname { null; };
category lame-servers { LAMER_log; };
category security { SEC_log; };
category statistics { STAT_log; };
};
```

表 2-6 最下面可看到 lame-servers、security、statistics 三個項目，其功能是用於分離 log 的訊息，lame-servers 代表偵測到不良的委任設定時，將記錄寫入 var/log/dns-lamer.log 中。security 代表偵測到有關被認可或不被認可的要求時，將記錄寫入/var/log/dns-sec.log。statistics 代表偵測到 DNS 活動的定時報告，將記錄寫入/var/log/dns-stat.log。由於這三個設定方式是相同的，所以舉 security 為例進行說明，設定通道將訊息送往指定的檔案(/var/log/dns-sec.log)，並且可設定記錄檔的個數(dns-sec0.log、dns-sec1.log、dns-sec2.log)與檔案的最大容量 10Mbites (若超過 10Mbites 的容量則除去原有內容，再寫入)。BIND 的訊息傳送可分為五個不同的嚴重等級(severity)，分別是 critical、error、warning、notice、info，在此則設定為 info(不會看到除錯的訊息)，也就是送出 info 等級以上的訊息到 dns-sec.log 檔案，此外 BIND 8 提供 debug 及 dynamic 二項功能，讓系統管理者記錄偵錯與動態服務；類別是指示資料的種類，本研究使用四種類別，cname 將不記錄查詢錯誤名稱的訊息，lame-servers 將偵測到不良的委任設定的資訊，傳送到 LAMER\_log 所指定的檔案，security 將認可或不被認可的要求，傳送到 SEC\_log 所指定的檔案，而 statistics 將 DNS 活動的定時報告，傳送到 stat\_log 所指定的檔案。

表 2-7 更改顯示版本

```
option { version "how are you ?"; };
```

表 2-7 是存在於 options 的設定，使用此種設定時，會在提供回應查詢 BIND 版本時顯示出 "how are you ?"，但本研究並不建議使用此方式，因為 DNS 防護偵測系統部份判斷弱點的資料來源正是版本編號，若加上此種設定可能影響判斷的正確性，並且無法完整地提供資訊給網域管理員。

表 2-8 options 進階說明(Master)

```
key master-slave {
algorithm hmac-md5;
secret "ele9H+VlhBkCWf/C5NnGnw==";
};
server 210.71.14.95 {
transfer-format many-answers;
keys { master-slave; };
};

options {
check-names master fail;           // default fail
    directory "/etc/named";
    pid-file  "/etc/named.pid";
    notify yes;
// fake-iquery yes;                // default warn
//     forwarders { 210.71.4.60; };
// host-statistics yes;            // default no
    transfer-format many-answers;
allow-query { any; };
recursion no;
allow-update { none; };
    allow-transfer { 210.71.14.0/24; };
};
```

表 2-9 options 進階說明(Slave)

```
key master-slave {
algorithm hmac-md5;
secret "ele9H+VlhBkCWf/C5NnGnw=="; };
server 210.71.14.64 {
transfer-format many-answers;
keys { master-slave; }; };
```

1. TSIG 傳輸記錄功能

設定 Master/Slave 伺服器間的傳輸記錄。讓伺服器傳輸記錄時能以此為憑

證。而 TSIG 存有弱點，在使用前需要將 BIND 更新到最新版本，或者是 BIND 8.2.5 與 BIND 9.1.3 以後的版本。製造 TSIG 加解密碼，可使用 BIND 所提供的 `dnskeygen` 工具生成密鑰，即產生兩個文件檔內含 TSIG 加解密碼。Master/Slave 伺服器的 TSIG 設定，請參照表 2-8 與表 2-9。

2. `forwarders { 210.71.4.60; };`

`forwarders` 是指定代詢伺服器。當接受查詢資訊時，如果本機的權威資料與快取資料存有查詢訊息時，即直接回應查詢者。如果無此項訊息時，即將查詢轉往指定的代詢伺服器，此種設定可減少伺服器負荷。設定代詢伺服器時，要注意指定的代詢伺服器是否允許轉送查詢。

3. `transfer-format many-answers;`

BIND 4 伺服器使用 `one-answer` 傳送方式，即 DNS 轄區訊息傳送是以每次傳送單一筆資源記錄(RR)。預設值使用 `one-answer` 傳送。但 BIND 8 伺服器支援一種新的轄區傳送格式，稱為 `many-answers`，此種格式能盡量放入多個資源記錄於單一 DNS 訊息中，加快讀取訊息、節省頻寬等益處，缺點是資料傳輸的時間變長。

4. `allow-query {any; };`

限制服務範圍內才可以進行查詢動作，BIND 8 的預設值為 `any`，允許所有主機查詢，而 Master/Slave 之間的轄區傳送也需使用此功能。

5. `recursion no;`

關閉 `recursive query` 功能，考量負載問題並避免漏洞的產生，只回答本機所知道訊息，不需向上層 DNS 主機查詢直到得到訊息。

6. `allow-update {none; };`

BIND 8 的預設值，關閉此項機動更新功能。假若需要使用這項更新功能

時，應限制服務範圍，allow-update 是針對動態 DNS 協定所使用的限制。

7. allow-transfer { 210.71.14.0/24; };

指定網域內的主機才能下載 mis.stu.edu.tw 轄區資料，在預設情況下是允許任何主機進行轄區傳送的要求，駭客可利用 Slave 的方式與偽造 IP，取得轄區內的資料，限制 210.71.14.0~255 網域才能允許轄區傳送，藉以保護轄區內的資料不被竊取。

檢查 DNS 是否能正常運作，可開啟/var/log/messages 檔案觀看 log 是否有錯誤訊息出現。當 DNS 服務能運作時，可使用 nslookup、dig 工具檢查設定是否正確。Log 訊息需要每天查看是否有問題，若無法時常觀看 log 訊息時，可從命令列中鍵入 kill -ILL named\_PID，並取得產生 named.stats 檔案，從資料中得知這段時間的網路流量，以方便進行簡易的分析與判斷。

## 2.3、Nessus 安全檢測之應用

Nmap[14] 是一套強大的 port scan 工具，使用 TCP、UDP 與 ICMP 方式進行連線，使用者可利用這套工具進行檢測，了解主機的 port 是否處於開啟狀態，從中可得知主機可能存有那些弱點。假若依 IP 位址連續使用 port scan 是很容易被對方發現，Nmap 則使用 connect()調節掃瞄的時間以完成掃瞄。

Nessus[15]是一套功能強大的安全稽核軟體，採用 Nmap 的 port scan 功能，輔助檢測系統漏洞的功能。1998 年在法國 Renaud Deraison 設計出最早的 Nessus 軟體，基於研究用途而發展出這套軟體，主要目的是幫助系統管理者，針對指定的網域、主機進行安全檢查，找出隱藏性的軟體缺陷，並且利用內建或新增的 Knowledge Base，以提供往後偵測弱點時所需的資訊。檢測報告的輸出支援多種格式(如：txt、html、LaTex)，並提供防護與修正軟體的建議事項。

Nessus 是一套開放原始碼(Open Source)的免費工具軟體，圖 2-7 即是說明 Nessus 所提供的服務，分成伺服器端(Server)與用戶端(Client)二種，伺服器端安裝在於

Unix like 的系統下，而用戶端則提供二種作業系統的安裝套件，此二種套件可安裝於 Unix like 與微軟視窗(Microsoft Windows)系統。Nessus 的稽核檢測現今依照不同的特性分成二十一種類別，而且系統不斷的推陳出新，未來可能新增不同類別，Nessus 使用圖形使用者介面(Graphics User Interface,GUI)，讓使用者在操作與檢視時更為便利。

Nessus 採用 Plug-in 架構，每當撰寫出一個新的 Nessus Attack Scripting Language(NASL)稽核程式，只需要依照 Plug-in 的功能要求，即可加入 Nessus 系統中，不需要更新 Nessus 系統的程式。NASL 是 Nessus 做為稽核軟體的延伸基礎，NASL 可使用 C 語言進行編寫，再進行轉換成為稽核程式，也可直接撰寫 Nessus Script。若想編寫新的稽核程式，需要熟知入侵的行為模式與 NASL 函式，此外更要注意 NASL 是否會互相造成衝突、影響。每當新的稽核程式產生時，假設可能造成對方主機損害時，需要加入警告訊息。

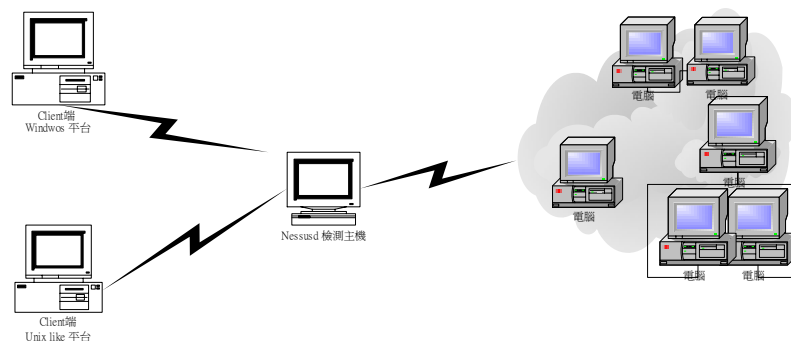


圖 2-7 nessusd 偵測目標網域

藉由表 2-10 說明 NASL 的格式，是用來測試 Berkeley Internet Name Domain (BIND)弱點。而每個 NASL 在其內容中會參雜部份說明，每篇的開頭皆需註明作者與連絡方式，假若在測試程式中，發現可能造成攻擊時，需要連絡程式撰寫者或協助改善問題。下面的範例可分成二個部份，第一部份是 description，內容是用於在系統中，解說 Nessus Script 所檢測的內容與警告。第二部份則是向外檢測的程式，運用 Nessus Script 所提供的函式，編輯詢問封包的內容，再送出封包並且

取回應訊，以回應訊來判斷是否為產生漏洞的版本。

表 2-10 bind\_iquery.nasl 稽核檔案

```
#
# This script was written by Renaud Deraison <deraison@cvs.nessus.org>
#
# See the Nessus Scripts License for details
#
#
# This script replaces bind_bof.nes
#

if(description)
{
  script_id(10329);
  script_version ("$Revision: 1.1 $");

  name["english"] = "BIND iquery overflow";
  script_name(english:name["english"]);

  desc["english"] = "
The remote BIND server, according to its
version number, is vulnerable to an inverse
query overflow.

Solution : upgrade to bind 8.1.2 or 4.9.7
Risk factor : High";

  script_description(english:desc["english"]);

  summary["english"] = "Checks the remote BIND version";
  script_summary(english:summary["english"]);
```

```
script_category(ACT_GATHER_INFO);

script_copyright(english:"This script is Copyright (C) 2002 Renaud Deraison",
                 francais:"Ce script est Copyright (C) 2002 Renaud Deraison");
family["english"] = "Gain root remotely";
family["francais"] = "Passer root ?distance";
script_family(english:family["english"], francais:family["francais"]);

script_dependencie("bind_version.nasl");
script_require_keys("bind/version");
exit(0);
}

vers = get_kb_item("bind/version");
if(!vers)exit(0);
if(ereg(string:vers,
        pattern:"8\\.((0\\.|)(1\\.|0-1)).*"))security_hole(53);

if(ereg(string:vers,
        pattern:"4\\.([0-8]|9\\.|0-6).*"))security_hole(53);
```

### 第三章 DNS 安全檢測之設計

經由網際網路的運用，使得人們能快速相互交流使用軟體的經驗，督促相關軟體廠商，加速產品的修正時間與更新速率。BIND 的最新版本已是 BIND 9.2.1，依照 2000 年六月澳洲網路安全機構所發表的調查指出[8]，還是有大量的主機採用比 BIND 8.2.2 p5 還要老舊的版本，可能是另個隱情而無法使用最新版本的服務。圖 3-1 將 BIND 版本分成 BIND 8.2.2 p5 之前的版本、BIND 8.2.2 p5、Windows 系統、Mac 系統與其他系統等五種範圍，並且分成 Vulnerable DoS、Vulnerable Root Compromise 與 Currently Secured Servers 等三種偵測類型並加以統計。從圖中可看出使用舊版服務的問題最多。因此如何維護 DNS 伺服器安全這項工作，即顯得非常重要與迫切。

假若能在網際網路上提供一套適合的 DNS 安全偵測軟體，即能減少系統管理員的負擔。大部份的偵測軟體，進行安裝時需要安裝在某主機，或者需要付費才能使用，因此本研究想開發一套使用網際網路為介面的軟體，只針對 DNS 服務進行稽核偵測，並且整理出現存的解決措施，以便利使用者操作與補強系統。

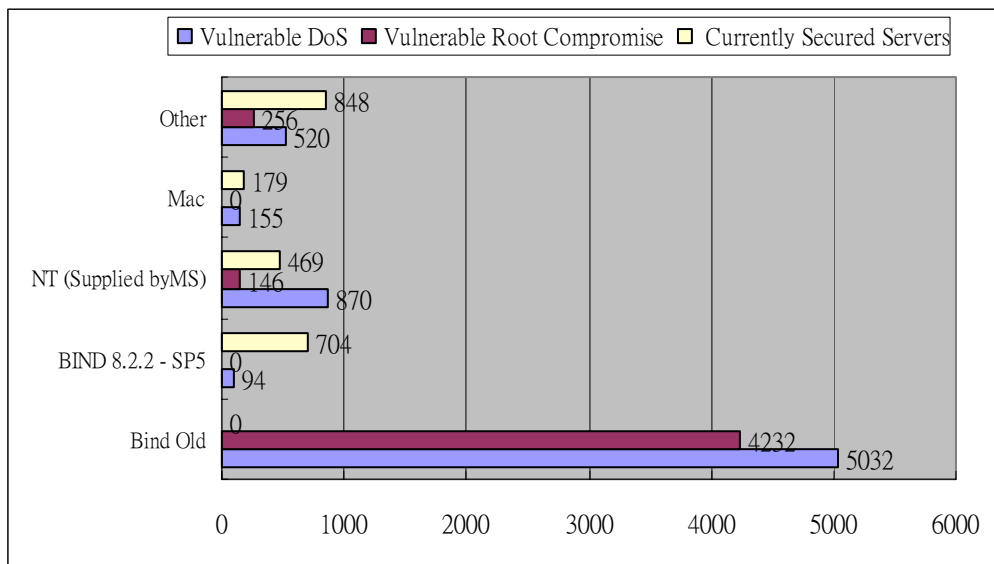


圖 3-1 澳洲境內 DNS 調查報告（調查 BIND 的安全性）

參考來源：DNS Security in Australia

### 3.1、設計構想與系統模型

網路安全是非常重要的一項課題，各個作業系統、軟體套件時常發出警告訊息，需要系統管理者針對服務，進行設定、使用政策(Policy)、修正或更新套件。除此之外更需要注意各廠商所發佈的安全通告(Advisory)與修正套件，面對龐大的修補訊息，導致系統管理者時常花費時間於維護相關系統，努力維護運作之餘也可能會遺漏訊息，因此需要適當的檢測系統協助偵測漏洞與提供修正建議，以減少系統管理者的沉重負擔。

本研究選擇 Nessus 為掃描引擎，由於這套檢測系統符合本研究的需求，對檢測目標主機後，會針對檢測結果產生報表，報表中提供可能存在的漏洞與相對應的修補建議事項。本研究於第 2.3 節中，曾對 Nessus 的 Plug-in 架構進行說明，依照其說明文件只需新增 NASL 稽核程式，不需再改寫系統核心程式，並且 NASL 使用開放原始碼的觀念，讓每個使用者有機會成為稽核程式的開發者，開發者彼此也能相互檢核程式是否會產生干擾，此套件的檢測功能是經由大量的使用者進行開發與測試，如此一來可擴充系統的功能與完整性。

每個 NASL 稽核程式皆是依據各大網路安全機構所發佈的安全通告(Advisory)發展而成，如：CERT/CC[16]、TWCERT/CC[1]、CVE[17]、Security Focus[18]等，相形之下就有如一個大型的弱點說明的資料庫，內文主要是描述漏洞發生於何種系統、服務中，並且告知如何進行修正與核對措施。

應用 Nessus 於 DNS 安全偵測系統運作模式說明如下：

#### 1. NASL 檢測與運用的模式：

NASL 的檢測模式如圖 3-2 所示，第一種是平和查詢，向目標主機送出正常的詢問封包並且取得回傳的相關訊息，與各大網路安全組織所發出的安全通告進行比對，判斷是否成為弱點與威脅的可能性，再提出建議事項。第二種是攻擊查詢，針對偵測主機送出大量封包或者傳送經由特別設計的長串封包，讓目標主機無法回應或忙於處理請求封包，導致系統運作變

慢，或者形成暫時性的阻斷服務攻擊(Denial- of-Service)而無法馬上回應其他的請求封包。

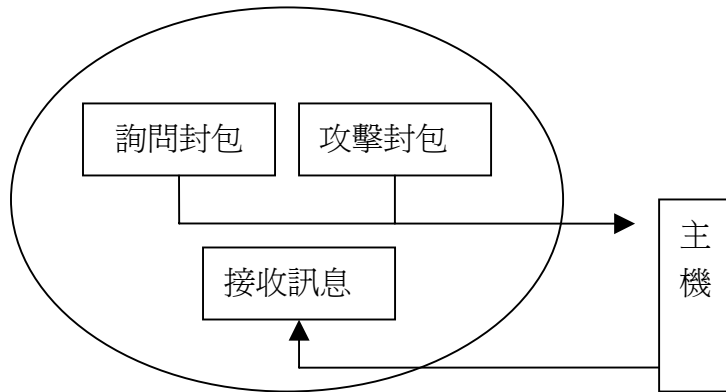


圖 3-2 NASL 偵測與運用

圖 3-3 是 NASL 檢測程式的語法架構，所有的 Nessus Plugin 程式均是以此種語法撰寫而成。[15][19]

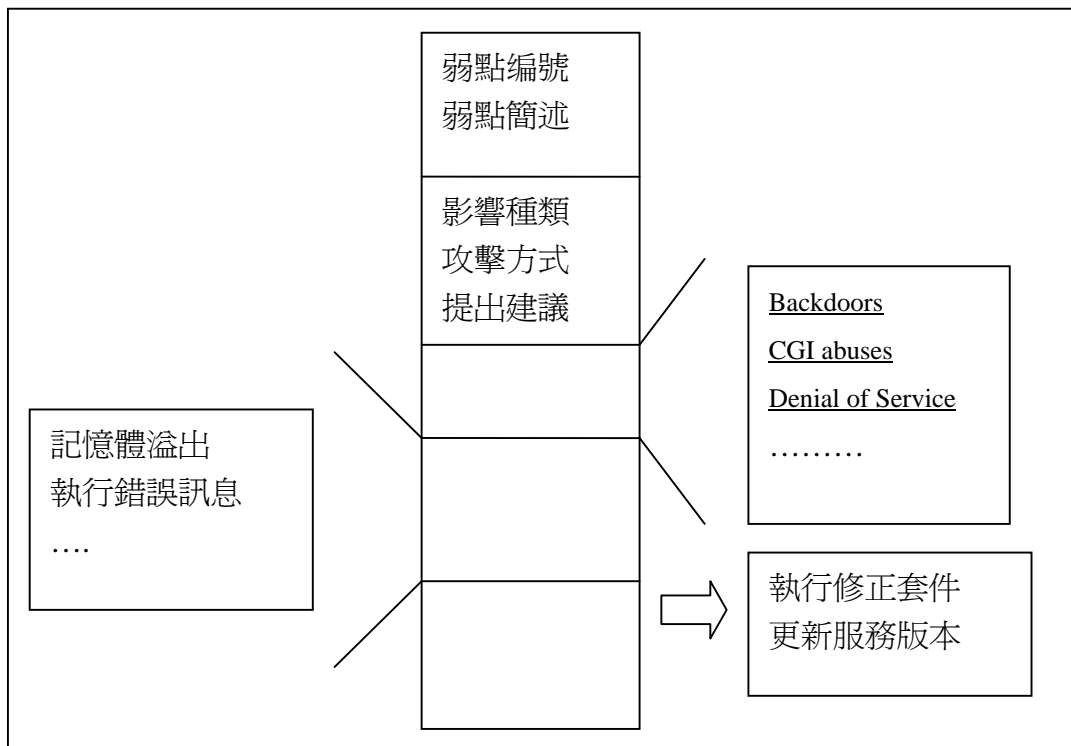


圖 3-3 NASL 模型

## 2. 網頁與軟體運作模式：

透過 Telnet 連接至 Nessus Daemon 傳送變數至檢測主機，如圖 3-4 所示，可指定檢測後回應的訊息儲存處。輔以選擇檢測項目，申請者由網頁中可清楚地看到檢測項目的相關訊息。當檢測結果傳回網頁時，系統會結合弱點的相關訊息，提出相關弱點補正建議，讓申請者更加了解更新與修正的動作。

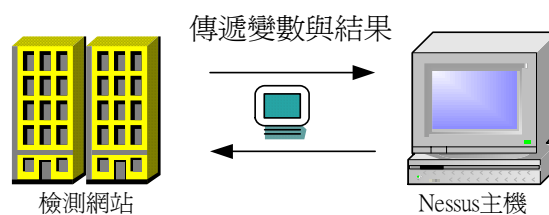


圖 3-4 稽核資料流向

## 3. 網站安全問題：

經由 TWNIC 網站完成申請者驗證後，轉向本檢測系統，並且傳送檢測相關資料。申請者確認過系統聲明文件後，即可進入檢測的主要網頁中，經由點選需檢測的項目，系統再進行二次的身份核對工作，驗證身份後才能列入安全檢測掃描的排程，系統於檢測結束後，將自動寄送電子郵件到申請者的電子信箱。

## 4. 檢測系統的設計需求：

檢測系統使用 Linux 內建的 httpd 進行架設網站，並且運用 PHP(Personal Home Page Tools)[20][21]電腦程式語言，進行編寫檢測的網頁操作介面。後端資料庫於多方因素的考量，決定使用 MySQL[21][22]以免除不必要的麻煩，並且使用 myAdmin[23]管理資料庫軟體，讓資料庫能透過網頁進行管理，也讓檢測系統管理人的操作更加便利。

## 5. 掃描排程

圖 3-5 掃瞄排程運作是使用資料庫核對申請人名單進行排程，最先將申請掃瞄者的資料存入掃瞄排程的資料庫中，經由再一一的進行掃瞄，在此運用 scanschchk 與 scansch-q 資料庫表格，比對是否還有未完成掃瞄者。當進行掃瞄程序時，先取得掃瞄者指定目標與選取掃瞄項目，即進行掃瞄。掃瞄結束後，將掃瞄結果比對弱點資料庫，再儲存成掃瞄建議檔，經由電子郵件寄送到申請人的電子信箱中。

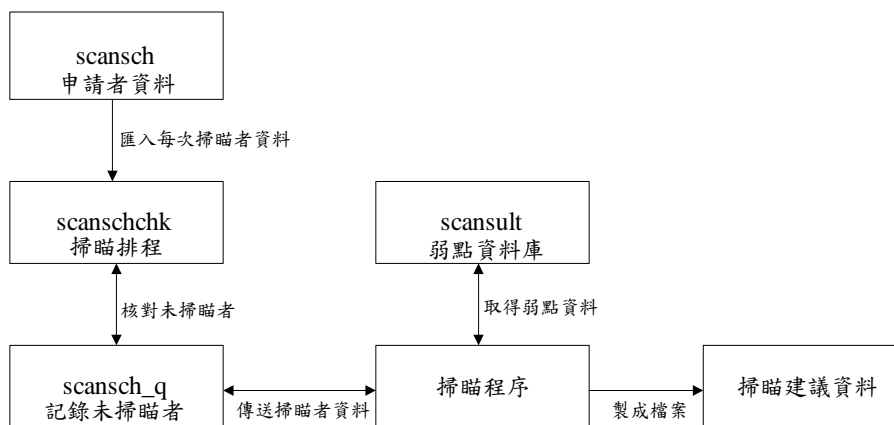


圖 3-5 掃瞄排程運作

### 3.2、設計上的考量與問題分析

Nessus 提供 Unix like 與 Windows 二種作業平台的用戶端(Clinet)，以方便選擇檢測事項，Nessus 檢測的範圍過於廣大，並且檢測服務分類並不符合本研究所需，本研究領域著重於 DNS 檢測，只需要軟體中的部份檢測程式，因此篩選與檢測 DNS 相關程式。檢測系統使用網頁形式做為操作介面，不限於作業系統平台，換言之能幫助更多的系統管理員節省時間與降低負擔。

自從 1980 年代開始發展 BIND 這項服務，至今已達到接近完美的階段，而針對 BIND 版本的問題分析可分成三個階段：[24]

1. BIND 4 是最先廣受大眾所使用，也是弱點最多的版本，假若未升級到 BIND 8 或 BIND 9 的使用者，主要原因可能是受限於硬體設備無法升級或者不在乎漏洞會影響系統正常運作。建議升級到 BIND 4.9.8 以後的版

本，將可能發生的損害降到最低，或者直接更新到 BIND 9 的最新版本，即可免除受到已發現的漏洞影響之苦。

2. BIND 8 經過廠商與網路群眾的發掘、更新錯誤，已到 BIND 8.2.3 是最趨近成熟的版本，從 ISC 網站摘錄下列幾點是 BIND 8.2.3 已修正的問題：

- (1)、修補數種漏洞，特別是針對 IXFR 與 TSIG 漏洞。
- (2)、使用新的”ndc reload – noexpired”。
- (3)、當使用更新版本的 BIND 時，name 守護程序的控制接口程序可以提供版本信息：(ndc status)。
- (4)、在長時間的轄區延遲負載時不接受舊的請求(queries)。
- (5)、Forwarders 功能使用依序

3. BIND 9 是使用不同於 BIND 8 的觀念重新改寫，從 ISC 網站摘錄下列幾點有關於改進的內容：

(1)、DNS Security

<1>、DNSSEC (使用簽章解決 zones 的問題)。

<2>、TSIG (使用簽章解決請求的問題)。

(2)、IP version 6

<1>、Answers DNS queries on IPv6 sockets (使用 IPv6 的方式回應 DNS 的請求)。

<2>、IPv6 resource records (提供 A6, DNAME, etc.)。

(3)、加強 DNS Protocol

<1>、IXFR, DDNS, Notify, EDNS0。

<2>、Improved standards conformance(改善標準規格的一致性)。

為了讓申請者在檢測前能了解系統提供的功能，選擇適合的檢測項目。本研究將弱點資訊加以整理，而有下列九項檢測選項說明：

1. Bind 9 版本檢測：

BIND 9 內含一個"authors.bind"的記錄檔，可利用下面的指令查詢：

```
dig @ns.check.com authors.bind chaos txt
```

或

```
nslookup -q=txt -class=CHAOS authors.bind. ns.check.com
```

查詢結果是顯示出所有參與程式撰寫人士的姓名。這項查詢即是利用此方式，檢測遠端 DNS 伺服器是否為 BIND 9，若有回應訊息即可判斷是 BIND 9。再針對回應的訊息進行字串比對，是否存有"Bob Halley"，假若沒有即可能是發生 TSIG 漏洞的版本(BIND 9.1.0 beta releases 與現在的 BIND 9.1.0)，建議更新程式碼或升級版本。

2. Transfers 危機檢測：

DNS 功能中包含 IP 位址與網域名稱的轉換。其中有一個功能是"Zone Transfer"，若不限制"zone transfers"的對象，任何使用者皆可透過此種方式，得知整個 IP 位址或網域名稱的資料。若可經由此方式取得資訊，也表示駭客能描繪出整個目標網路架構。因為每一台主機網域名稱，通常是使用相關服務的名稱，因此從中能得取資訊，這個問題可利用設定 DNS 加以防範。然而安裝服務的預設值為開啟 Zone Transfer 狀態，可經由 named.conf 檔案中，設定限制對象或不啟動 allow-transfer 選項，以防範這項漏洞。

3. BIND 緩衝區溢位問題偵測：

經由 Internet Software Consortium (ISC)的查證，BIND 8.1.2 or 4.9.7 之前的版本，在反向查詢(Inverse Query)時，可能造成記憶體溢出，並且讓駭客取得 root 權限。若攻擊者能建立一個特殊的反向查詢請求(Inverse Query)，就可能導致記憶體內容的洩漏，取得主機內的相關資訊。攻擊者

可能利用環境變數的設定，獲得系統訊息；也可能利用這些資訊發動攻擊造成記憶體溢出，即可覆蓋記憶體內的指令，以取得 root 權限。

4. Bind 緩衝區溢位漏洞：

這個檢測項目參照多種緩衝區溢位的漏洞，發現這此漏洞皆集中發生於 BIND 4.9.8 與 BIND 8.2.3 版本之前，若因此發生緩衝區溢位時，攻擊者可輕易地取得主機 shell 的執行權限。檢測的衡量標準則以版本的型號，判斷是否可能產生弱點。

5. BIND 版本檢測：

藉由查詢"Question Name"探測 name daemon 的版本和種類，在預設中 Server 將會回應 BIND 版本，除非額外設定不回應版本訊息，使用"version "8.0.0";"更改回應的版本編號；此項查詢並不是攻擊行為，而是一種勘查性的掃描。若是攻擊者進行查詢時，回應的訊息若為 4.9.6-REL 或 8.1.2，攻擊者即知道此系統存有緩衝區溢位的漏洞，可能會利用這些漏洞的特性入侵系統。

6. BIND zxfir 設計錯誤漏洞檢測：

攻擊者可利用這個設計錯誤的漏洞，對遠端 DNS 主機提出 zone transfer 請求，此種壓縮的 zone transfer 請求，可能導致阻斷服務攻擊(DoS)。BIND 8.2.2 版本經由特殊設計的請求，可能導致系統癱瘓。原因是 ZXFR 是使用"gzip"壓縮的轄區檔案轉換的程式，並且擁有 name 服務的優先查詢權，也不會在 Name Service 的 cached 留下任何的紀錄。當然先決條件是對方接受進行 Zone Transfer 請求。然而服務的預設值為開啟 Zone Transfer 狀態，可透過設定 named.conf 檔案，限制允許 Zone Transfer 的對象，或者不開啟 allow-transfer 選項，以防範這個漏洞。

7. Bind 漏洞偵測：

這項漏洞是發生於 DNS 伺服器上的 NXT 記錄。攻擊者送出一個 DNS 查詢請求到目標 DNS 伺服器。讓目標主機連線回到攻擊者的 DNS 伺服器。

透過攻擊者特殊設計的 DNS 伺服器，針對 NXT 記錄回傳一個約 6500 字元的資料串。讓目標 DNS 伺服器產生緩衝區溢位，假若攻擊成功即可取得遠端伺服器的控制權。此攻擊事件在 2000 年第一季時被大量的散播，而流行的主要因素是 Linux Package(RedHat 6.1)內含這個弱點。現今 ADM 已開發出破解系統的程式分別是 adm-nxt.c 和 t666.c。這就是眾所皆知的 ADMROCKS 漏洞，因為這個程式會自行建立一個名為 ADMROCKS 的子目錄，並且放置於執行 BIND 的預設路徑下。RedHat 6.1 的預設位置為 /var/named，其目錄即是下列模樣[25]：

```
total 10
drwxr-xr-x 3 root root 1024 Apr 1 11:26 .
drwxr-xr-x 23 root root 1024 Jan 17 01:55 ..
drwxr-xr-x 2 root root 1024 Apr 1 11:26
ADMROCKS -rw-r--r-- 1 root root 2769 May 12 1999
named.ca-rw-r--r-- 1 root root 422 May 12 1999
named.local -rw-r--r-- 1 root root 2075 Apr 1 11:13
named_dump.db
```

8. 遠端的 Name Server 允許本主機遞迴查詢：

這項漏洞是發生於遞迴查詢，此功能是為了增加 DNS 伺服器執行效能，而在本地端暫存網域名稱，因此無法分辨記憶體區段內需要回應訊息，因而將區段內的訊息全部送出。假若針對目標主機送出一個查詢訊息，並且額外包含轉送他人的訊息時，的伺服器版本會接受這個訊息、暫存到記憶體中，並且回覆給其他查詢的人。BIND 8.1.2 之後的 DNS 伺服器已經完畢修正。本系統檢測方式是向目標主機傳出遞迴的請求，將解析(Resolve)的目的地轉送於 [www.nessus.org](http://www.nessus.org) 網站，以證實是否存有這項漏洞。這個漏洞可能被攻擊者所利用，並且藏匿感染途徑於名稱伺服器中，藉以影響其他主機。

## 9. Winnt DNS 大規模阻斷攻擊漏洞偵測：

藉由 flooding 的特性，讓遠端 WindowsNT DNS 伺服器無法正常運作。原因是 Windows NT 4.0 與同時期的 DNS 版本都有此弱點，在接受連續大量的請求封包時，會形成 flooding 攻擊。攻擊者可能寄送連續大量的請求封包到 port 53，造成伺服器產生阻斷服務攻擊(DoS)。

收集 BIND 的弱點相關資料來源，主要依照收錄於 CVE (Common Vulnerabilities and Exposures) 列表，並且試著找出相對應受到影響的版本，由於各大網路安全團體解析受到影響的版本不同，導致產生收集版本的動機。本研究的參考對象以 CVE 為主，Internet Security Systems (ISS)、Security Focus 與 Internet Software Consortium(ISC)、CERT/CC 四個網站為輔，並且進行弱點資訊比對與統計，比對資料列成二張表格(參照附件一內的表二、表三)，表 3-1 列出弱點的數量比。然而收集資料是針對 ISC 所發出的 BIND 版本，其他如 ypbind 等則不在此調查範圍內。

依照本研究所收集的資料顯示出，BIND 8 的弱點主要集中於 BIND 8.1 到 8.2.2 p7 之間。BIND 4 的弱點主要集中於 BIND 4.9.3 到 4.9.6 之間，其中以 Infoleak(CVE-2001-0012)的弱點影響範圍最大，Maxdname (CVE-1999-0849)次之。最近的弱點則是 TSIG HMAC-MD5 (CAN-2001- 0497)，在調查中發現 CERT/CC 發佈 BIND 弱點相關訊息時，將二個 CAN (candidate)列入發佈資料時的參考資料，所以將這二個 CAN 列入這次的調查行列中。總共收集到 20 個弱點，因影響範圍不同，本研究依照弱點所受影響範圍進行分類，分類後得知每個 BIND 版本可能發生的弱點數量，統計後共有 30 個需要注意的弱點。

表 3-1 調查 BIND 版本弱點數量

BIND 名稱版本	弱點數量
BIND, 9.X	1
BIND, 8.X	18

BIND, 4.X	11
總計	30

### 3.3、DNS 安全檢測之流程

DNS 安全檢測流程，如圖 3-6 所示，主要用途是為檢測台灣網域第三層 DNS 安全性而設計，因為數量龐大，所以提供一個非破壞性檢測。雖然本系統使用的 NASL 程式，是為遠端主機做稽核等動作，但也存攻擊的稽核程式，但經過多次的審視與測試後，並發覺不會造成太大的影響，充其量只會造成遠端 DNS 主機短暫性的忙碌現象。除非是同時有多台偵測主機一起發動攻擊，才可能造成阻斷服務攻擊(DoS)。假若能同時發動多台主機進行攻擊者，即不需要使用這麼麻煩的攻擊模式。如：編寫一攻擊程式並在多台主機上執行即可。因此不需特別考慮本系統是否會造成攻擊者的跳板。

當安全檢測完成後，請依照檢測結果的建議檔，進行修正漏洞。雖然依照建議檔進行修正後，並無法保證系統有百分之百的安全性。原因是 DNS 本身仍然潛藏著尚未被發現的漏洞，或是已發佈的漏洞尚未撰寫成 NASL 檢測程式。DNS 的弱點與其版本相依性非常高，因此網域管理者應特別注意各大網路安全團體，針對 DNS 所發佈的安全通告，並且勤加補正。如此一來才能確保服務能正常運作。

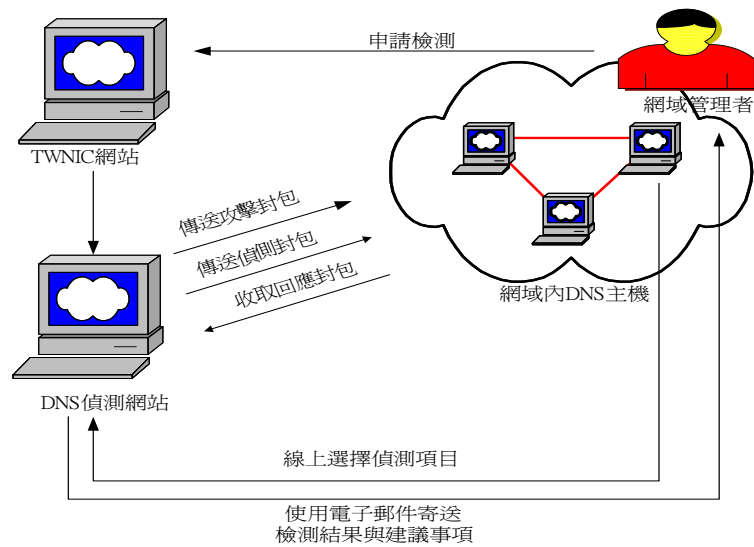


圖 3-6 DNS 安全檢測整體流程

DNS 安全偵測系統之檢測流程，如圖 3-7 所示：

1. 登入 TWNIC 使用者認證網頁：

使用者登入 TWNIC 網頁進行認證，認證成功則將網域名稱、使用者電子郵件、欲掃描主機之 IP 及登入主機之 IP，透過開啟 Socket 方式傳遞到本系統。

2. 選取掃描項目：

登入本系統後，使用者自行選取掃描項目，完成後即進入排程程序。

3. 系統進行線上掃描：

系統進行掃描之前須先執行以下檢查，確定無誤後才進行掃描檢測。

- (1)、所指定的 Name Server 是否可 ping 到。
- (2)、DNS server 是否有啟動(port 53 是否有回應)。
- (3)、這些 Name Servers 是否為該 Domain Name 的 Master/Slave servers。
- (4)、Name Servers 間之 SOA 及 NS 紀錄是否一致。

本系統將檢測的結果存入資料庫中，以便未來做學術研究，並且保護這些

原始資料不會外流。

#### 4. 檢測結果與建議事項：

檢測結果與建議，利用 Email 方式寄給使用者，提供使用者如何改善 DNS 伺服器之安全。

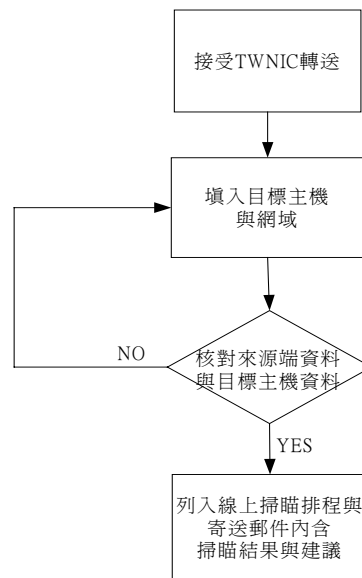


圖 3-7 DNS 安全偵測系統之檢測流程

### 3.4、DNS 安全檢測封包格式

DNS 安全檢測的 NASL 稽核程式，透過傳送封包的方式進行稽核，但是如何組合檢測封包是一件非常重要的工作，表 3-2 即是 bind\_query.nasl 程式，透過轉送檢測封包而得知是否存有漏洞，請依照附錄二的格式組合：[11][26][27][28]

表 3-2 Bind\_query.nasl 編造 resolve 轉送封包

```
# We ask the nameserver to resolve 'www.nessus.org'  
# (how original !)  
#  
req = raw_string(0xEF, 0xB3, 0x01, 0x00, 0x00, 0x01,  
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x03, 0x77,  
0x77, 0x77, 0x06, 0x6E, 0x65, 0x73, 0x73, 0x75,
```

0x73, 0x03, 0x6F, 0x72, 0x67, 0x00, 0x00, 0x01, 0x00, 0x01);
---

1. 解析編碼意義的同時，需要對照 DNS Header 區段的格式(附錄二；圖二)。ID 是一個 16 位元的辨識代碼，內容為 0xEF, 0xB3，這是二個十六進位的編碼，轉換成十進位則成為 49075，這表示 ID 的編號為 EFB3。根據 RFC 1035 的協定規範，DNS Query 的第一個欄位就是 Query ID，是用於追蹤發送到目標主機上的 DNS Query，又可同時發送許多個 Query，所以需要 Query ID 進行比對。Query ID 只需要是 0-ffffh 的任何一個數字，通常是隨機選取的。
2. 接著分析下一欄位 0x01, 0x00，可變成二進位(0000 0001 0000 0000)，參照表 3-3 可看到 RD=1，其意義為允許遞迴要求(Recursion Desired)以查詢回應訊息。

表 3-3 DNS Header 區段分析

QR	Opcode	AA	TC	RD	RA	Z	RCODE
0	0000	0	0	1	0	000	0000

3. QDCOUNT 欄位中的數值為 0x00, 0x01=>(0000000000000001)也就是 1，指著在 Question 區段中擁有 1 筆資源記錄。
4. ANCOUNT=>0x00, 0x00=>(0000000000000000)，指著在 Ancount 區段中擁有 0 筆資源記錄。
5. NSCOUNT=>0x00, 0x00 =>(0000000000000000) 指著在 Nscount 區段中擁有 0 筆資源記錄
6. ARCOUNT=>0x00, 0x00=>(0000000000000000) 指著在 Arcount 區段中擁有 0 筆資源記錄
7. 接下來則是 Question 區段的分析(附錄二；圖三)。QNAME：先出現一個顯現長度位元組 0x03，再緊連一串字元

0x03	(length)
0x77, 0x77, 0x77	(www)
0x06, 0x6E, 0x65, 0x73, 0x73, 0x75, 0x73	(nessus)
0x03, 0x6F, 0x72, 0x67	(org)
0x00	(null)

當出現空字串時，即為終止符號。

8. 0x00,0x01=>(0000 0000 0000 0001)，QTYPE 欄位所對應的意義是主機名稱與 IP 位址的對應關係

0x00,0x01=>(0000 0000 0000 0001)，QCLASS 欄位為 CLASS 的 superset(超集合)，在 254 之內皆為有效設定值。

## 第四章 安全偵測系統實作與應用

本章節介紹 DNS 安全偵測系統的實作與應用，此系統最主要用途是為第三層 DNS 伺服器做安全檢測。由於第三層 DNS 伺服器數量龐大，管理權責分散。如何有效且安全的方式進行評估目前 DNS 伺服器系統的安全狀況？針對目前的 DNS 服務安全問題該如何有效的檢測與補強？這些問題都是值得去探討的問題。本研究目前所擁有的 DNS 安全偵測系統，只能檢測出部份的漏洞並且提出補強的辦法。

### 4.1、系統架構

DNS 安全偵測系統架構如圖 4-1 所示，系統以 Nessus 為掃描引擎，並且使用 NASL 格式所撰寫的稽核程式，使用者介面是由 PHP 程式撰寫而成，可透過遠端連線掃描主機進行檢測。系統資料庫採用 MySQL 儲存檢測結果，爾後的資料可作為將來統計弱點的資訊，保障第三層 DNS 伺服器的安全與防護體系之建置。本系統初期主要是提供 TWNIC 申請網域登錄的使用者使用，因此網域管理者必須連結至 TWNIC 網頁通過認證後，才能進入此系統執行檢測功能。檢測流程說明如下：

1. 當使用者進入安全偵測系統時，即啟動核對使用者身份的模組，再度確認使用者是否正確與合法。
2. 使用者確認掃描服務條款及閱讀掃描說明，並選取合適的稽核選項。
3. 確定選項，即進入系統的排程程序，依排程進行選項中的檢測動作。
4. 完成檢測，將結果存入資料庫，並 email 檢測報告給使用者。

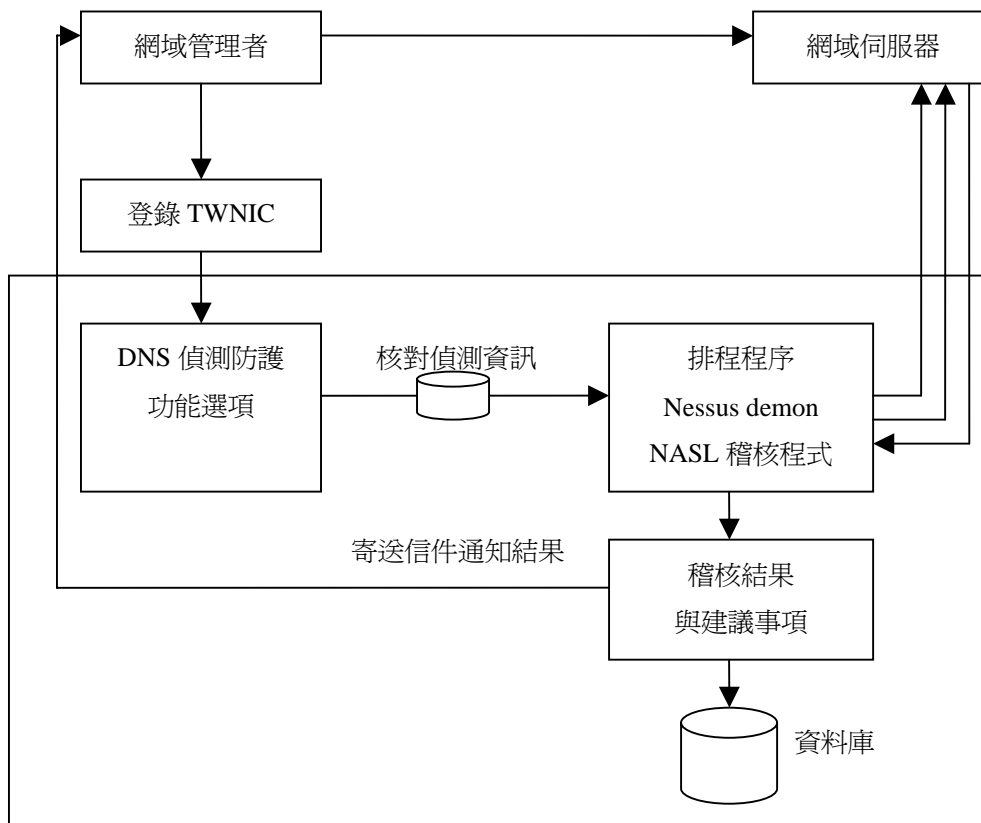


圖 4-1 DNS 安全偵測系統架構圖

## 4.2、DNS 安全檢測說明

本系統的 DNS 基本偵測模式，可分成下列四種模式：

### 1. 檢測服務的版本：

針對遠端主機送出一個查詢版本的封包，並且接收回應訊息，再比對弱點資料庫中是否為有弱點版本，可對照附錄一裡的表二、三，即可知道版本是否內含漏洞，這種判斷模式可說是最基本判斷模式。

### 2. 攻擊檢測服務：

偵測選項中所使用的攻擊模式，著重於測試是否有 flooding 的弱點，因此向 Windows NT 的 DNS 主機傳送 1024 字串封包，再傳送詢問封包測試對

方主機是否因為處於忙碌，而無法回應查詢的訊息。然而透過傳送 1024 字串封包，只是為了暫時讓目標主機處於忙碌狀態，此種方式只能達到 flooding 的基本門檻，並非是惡意攻擊，除非是以多台主機針對目標進行測試才可能發生阻斷服務攻擊(DoS)。

### 3. 轉送要求服務：

檢測選項中，利用 Name Server 允許遞迴查詢的功能，向目標主機傳送轉向遞迴查尋的訊息，即透過解析(Resolver)的特性，將查詢訊息轉向於第三者名稱(如:www.nessus.org)，此種回應訊息為 BIND 的標準傳送模式，目標主機是無法拒絕這種轉向解析的要求。攻擊者可能藏匿入侵程式於第三名稱主機上，讓使用者的主機取得錯誤的解析位址，直接登錄到已感染的網站而遭受影響。

### 4. 檢測轄區轉送：

DNS 伺服器主要功能是 IP 位址與網域名稱的轉換。為了讓伺服器得知是否更改過資料，在預設值的設定是允許所有主機進行查詢與轄區傳送(Zone Transfer)，若不限制轄區傳送(Zone Transfer)的對象，任何使用者皆可透過此種方式，得知整個 IP 位址或網域名稱的資訊，即能描繪出整個目標的網路架構。

## 4.3、系統操作範例

透過系統操作的方式，可以對安全偵測系統有更進一步的認識，本小節將對系統檢測過程的螢幕顯示作介紹：

1. 圖 4-2 是經過 TWNIC 認證後，轉向到本系統後所顯示的畫面，聲明本系統僅提供 DNS 服務弱點檢測。系統將提供詳盡的檢測報告與弱點修正建議，網域管理者可依弱點修正建議完成修正後，必能提高服務本身之安全。本系統無法保證 DNS 主機能取得全面安全，同時申請者必須詳閱圖 4-3 的檢測說明後，選擇適當的選項，以進行安全檢測。



圖 4-2 登入檢測系統之畫面



圖 4-3 檢測說明

2. 確認使用系統的聲明後，依照檢測服務的特性，分成以四個主要稽核類型，透過四種不同的檢測方式，因此建議全選稽核選項，以達到較為完整的檢測服務。若申請者要的進行檢測時，本系統即會再度核對申請者的身份，核對正確才得以進行排程檢測，此目的是為了不讓本系統被有心人士當作攻擊第三者的跳板。從圖 4-4 與圖 4-5 可看到弱點說明。
3. 圖 4-6 是顯現檢測認證是否成功，若二次身份認證成功時，即向申請者表示已列入掃描排程，請等候電子郵件，而電子郵件中會夾帶如圖 4-7 的檢測報告，若檢測出弱點時，即附上修正連結及建議。

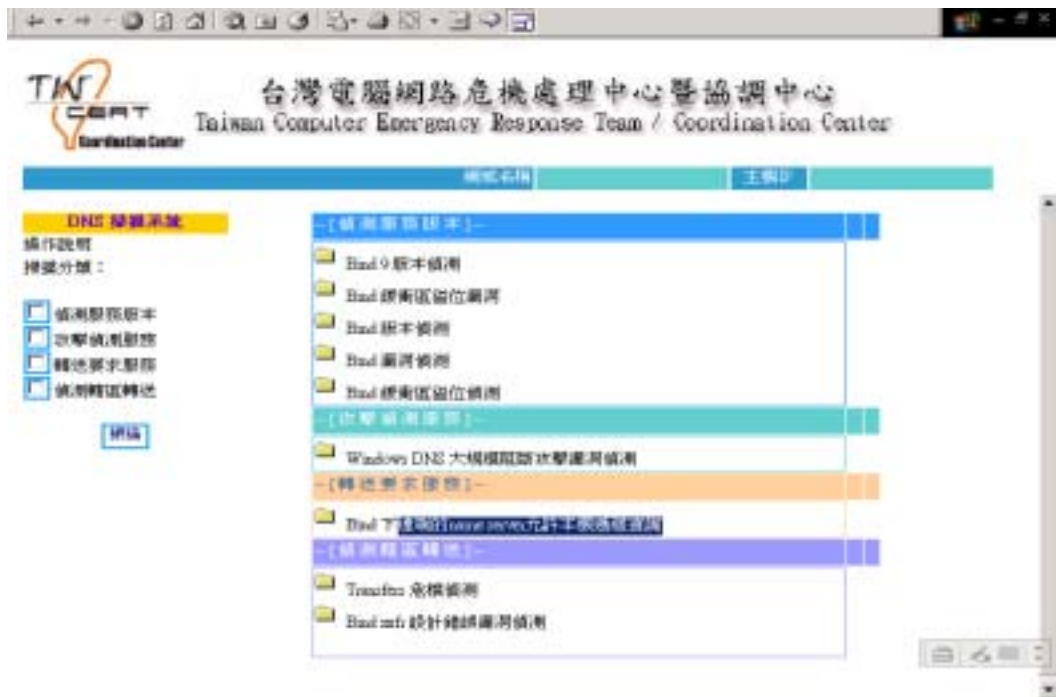


圖 4-4 弱點說明



圖 4-5 單項弱點說明

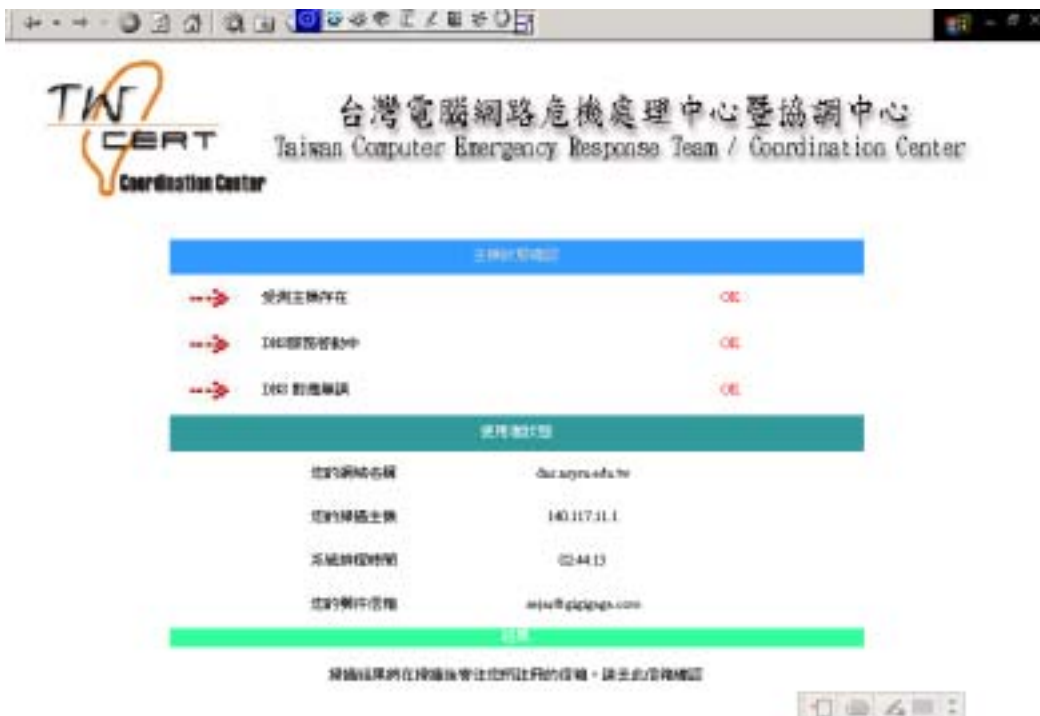


圖 4-6 檢測認證

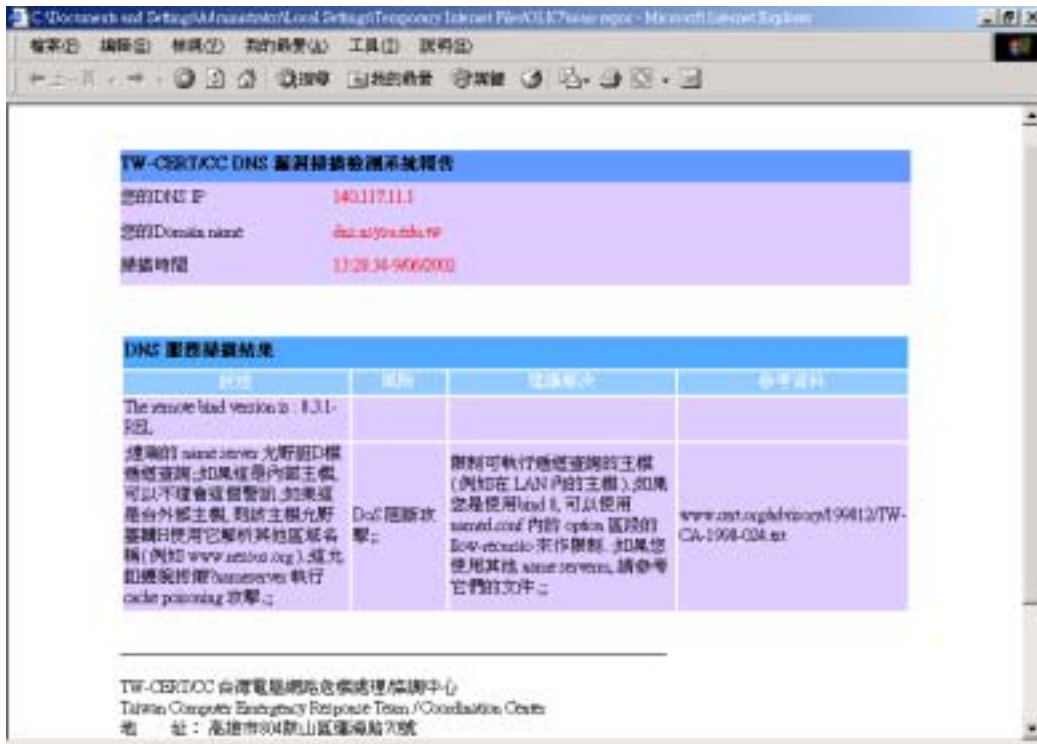


圖 4-7 檢測報告

4. DNS 安全偵測系統，是為了讓系統管理者方便管理、檢視資料，透過 myAdmin 所提供的功能，管理 MySQL 所儲存的資料，從圖 4-8 可以了解資料庫中包含那些檢測資料，並能透過網頁進行新增、刪除、修改等動作，提供系統管理者更方便的操作介。

Host	Time	Service	IP	Port	Protocol	Version	Severity	Impact
sejar@gigigaga.com	02:50:04-7/06/2002	dns.nsysu.edu.tw	140.117.11.1	domain	(53/tcp)	The remote bind version is 8.3.1-REL		
sejar@gigigaga.com	02:50:04-7/06/2002	dns.nsysu.edu.tw	140.117.11.1	domain	(53/tcp)	遠端的 name server 經過主機通過查詢，如果這是內？	DoS	限制可執行遠端查詢的主機(例如在 LAN 內的主機)如果？
hurtsam@huapc.net	12:50:03-7/06/2002	dns.nsysu.edu.tw	140.117.11.1	domain	(53/tcp)	The remote bind version is 8.3.1-REL		
hurtsam@huapc.net	12:50:03-7/06/2002	dns.nsysu.edu.tw	140.117.11.1	domain	(53/tcp)		遠端	DoS 限制

圖 4-8 稽核結果

#### 4.4、弱點修正連結

BIND 主要分成三種版本，即 BIND 4、BIND 8 與 BIND 9。BIND 的弱點與其版本有明顯的關聯性，因此升級到最新的版本是最為安全的措施(附錄一；表二、三)。雖然 BIND 版本的發展腳步不算慢，若是進行系統升級時，還是得花費許多時間。而本系統提供連結到台灣網路危機處理/協調中心及 CERT/CC 的安全通告，以便利 BIND 的使用者取得弱點資料，並且能檢測報告中的弱點進行修正，相關的弱點連結如下所述。

[ 偵測服務版本 ]

Bind 9 版本偵測

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/200102/TW-CA-2001-015.txt>

CERT/CC : <http://www.cert.org/advisories/CA-2001-02.html>

FreeBsd <http://cert.uni-stuttgart.de/archive/bugtraq/2001/01/msg00510.html>

#### Bind 緩衝區溢位漏洞

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/200102/TW-CA-2001-015.txt>

CERT/CC : <http://www.cert.org/advisories/CA-2001-02.html>

PGP : <http://www.pgp.com/research/covert/advisories/047.asp>

#### Bind 版本偵測

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/199911/TW-CA-1999-144.txt>

CERT/CC : <http://www.cert.org/advisories/CA-1999-14.html>

建議直接更新版本。

#### Bind 漏洞偵測

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/199911/TW-CA-1999-144.txt>

CERT/CC : <http://www.cert.org/advisories/CA-1999-14.html>

#### Bind 緩衝區溢位偵測

台灣電腦網路危機處理/協調中心：提供此篇安全通告的中文說明

<http://www.cert.org.tw/advisory/199812/TW-CA-1998-024.txt>

CERT/CC : [http://www.cert.org/advisories/CA-98.05.bind\\_problems.html](http://www.cert.org/advisories/CA-98.05.bind_problems.html)

<http://www.elec.ucl.ac.be/CERT/1998/msg00010.html>

--[ 攻擊偵測服務 ]--

#### Windows DNS 大規模阻斷攻擊漏洞偵測

<http://icat.nist.gov/icat.cfm?cvename=CVE-1999-0275>

[http://www.insecure.org/splouts/NT.DNS.character\\_flood.html](http://www.insecure.org/splouts/NT.DNS.character_flood.html)

下載區

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/>

--[ 轉送要求服務 ]--

Bind 下遠端的 name server 允許本機遞迴查詢

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/199812/TW-CA-1998-024.txt>

CERT/CC： [http://www.cert.org/advisories/CA-98.05.bind\\_problems.html](http://www.cert.org/advisories/CA-98.05.bind_problems.html)

--[ 偵測轄區轉送 ]--

Transfers 危機偵測

CERT/CC： <http://www.cert.org/advisories/CA-1997-22.html>

Bind zxfr 設計錯誤漏洞偵測

台灣電腦網路危機處理/協調中心：

<http://www.cert.org.tw/advisory/200011/TW-CA-2000-165.txt>

CERT/CC： <http://www.cert.org/advisories/CA-2000-20.html>

## 第五章 結論與未來研究方向

現今的作業系統已內含多種網路服務，架設網路伺服器不再是專業網路人員的專利，只要有意願架設網路伺服器，即可由網際網路取得相關安裝資訊。網域名稱伺服器所提供網際網路最基本的服務，然而 BIND 版本也一再更新，從 BIND 4、BIND 8 到 BIND 9。最新的 BIND 版本已達到完整防範已知漏洞的程度，換句話說只需安裝最新的服務版本，幾乎可以不受過往漏洞的威脅。然而有些系統無法升級到最新版本時，或者當新的漏洞不斷地被發現時，如何維護 DNS 的安全，減少系統遭受入侵攻擊，保持網路正常持續的服務是一項非常重要的工作。

### 5.1、研究成果與貢獻

本研究著重於 DNS 的安全性研究，主要是探討如何做好伺服器本身的安全設定及開發 DNS 安全偵測系統，期望能藉此協助網域管理者做好安全維護工作。本研究成果如下：

1. 針對環境的需求進行必要的限制，提出維護網域名稱伺服器安全的基本設定及進階設定，同時依樹德科技大學資訊管理系的 DNS 伺服器為測試主機，進行安全設定實作。
2. 設計開發 DNS 安全偵測系統，透過 Client-Server 的架構，位網域管理者透過瀏覽器連線到安全偵測主機，進行管轄內的 DNS 安全檢測。並獲得詳盡的檢測報告，依據弱點修正建議，修補弱點以提升伺服器安全度。
3. DNS 安全偵測系統將進一步提供給 TWNIC 的會員，進行第三層 DNS 安全檢測，以協助維護台灣網域之安全性。

### 5.2、結論與建議

整體來說 DNS 的問題不外乎環繞在軟體問題和管理人員之間，譬如使用問題軟體或者聘請非專業人員，而導致系統發生問題。為了解決這些問題，本研究提出下列幾項增進 DNS 安全的建議：

1. 盡量採用最新版本的 BIND，並定時注意任何相關的安全通報，採用適當的修正程式(patch)。
2. 主機只提供單一 DNS 伺服器的服務，此種舉動可降低其它服務可能造成的風險。
3. 注意擁有存取權限(Access control)的網域，限制 Zone transfer 的範圍。
4. 隱藏版本資訊。欺騙一般的速成駭客，避免速成駭客從網路上取得入侵(exploits)程式進行攻擊。
5. 隨時察看日誌檔(log)，檢查有無異狀。所謂早期發現早期治療。

### 5.3、未來研究方向

網際網路服務蓬勃發展，相對的系統漏洞不斷的被發掘，如何維護網路系統安全是網管人員的重要工作，因此本研究未來仍然有很大的發展空間，以持續提升伺服器安全度，分別敘述如下：

1. 針對 DNS 伺服器進階安全設定加強研究，提升伺服器安全度。
2. 研究有關加密 DNS 資料，增加服務安全性的方法。
3. 持續發展 DNS 安全偵測系統，依照最新發佈的安全通告，設計出新的安全稽核的 NASL 程式，加強安全偵測系統功能。

## 參考文獻

- [1] Taiwan Computer Emergency Response Team/Coordination Center,TWCERT/CC , <http://www.cert.org.tw/>
- [2] 陳宗裕、趙育釗、黃世昆，2000，安全虛擬誘陷執行環境，資訊安全規劃
- [3] 黃世昆，軟體系統安全弱點初探，中央研究院資訊科學研究所
- [4] 2002 Computer Crime and Security Survey ，  
<http://www.gocsi.com/press/20020407.html>
- [5] 林宜隆、楊鴻正，2001，資訊犯罪與網路警察，第三屆 2001 年網際空間：資訊、法律與社會學術研究暨實務研討會，頁 109-126，台北，12 月 24 日。
- [6] 陳昌盛，2000，DNS 系統的異常流量偵測、管理以及除錯，交通大學計算機與網路中心
- [7] 陳昱仁，2000，電子資料傳輸安全機制之研究，國立交通大學資訊管理研究所，博士論文。
- [8] DNS Security in Australia ，  
<http://www.net-security.org/text/articles/dl/DNS-Scan-Results.pdf>.
- [9] Taiwan Network Information Center,TWNIC ，<http://www.twnic.net/>
- [10] Men & Mice make DNS easy ，<http://www.menandmice.com/>
- [11] Paul Albitz, Cricket Liu 著，2000，DNS and BIND，蔣大偉編譯，第三版，美商歐萊禮股份有限公司台灣分公司，台北市
- [12] 學習 Linux，DNS 協定，<http://www.study-area.net/linux/linuxfr.htm>
- [13] DNS 介紹，<http://turtle.ee.ncku.edu.tw/~tung/dns/>
- [14] NMAP，<http://www.nmap.com>
- [15] NESSUS，<http://www.nessus.org>
- [16] CERT Corrdinate Center ，<http://www.cert.org>
- [17] Common Vulnerabilities and Exposures (CVE) ，<http://cve.mitre.org>
- [18] SecurityFocus ，<http://www.securityfocus.com>
- [19] 陳宗裕，2000，支援弱點稽核與入侵偵測之整合性後端資料庫設計研究，中原大學，碩士論文
- [20] Jesus Castagnetto, Harish Rawant, Sascha Schumann, Chris Scollo, Deepak Veliath 著，專業 PHP 程式設計，許鳴程譯，基峰資訊份有限公司
- [21] 趙啟志著，2000，PHP4+MySQL 完整自學方案，博碩文化股份有限公司，台北縣汐止市
- [22] 李立功、趙啟志編著，2000，MySQL 程式設計與資料庫管理，文魁資訊股

份有限公司，台北市

- [23] Administration of mySQL databases,myAdmin ,  
<http://www.myadmin.org/en/start.html>
- [24] Internet Software Consortium (ISC) , <http://www.isc.org/>
- [25] Internet Security Systems,鈺松國際 , <http://www.iss.com.tw/Advice/Intrusions/>
- [26] P. Mockapetris , 1987 , "Domain Names - Concepts and Facilities," RFC 1034,  
November
- [27] P. Mockapetris , 1987 , ``Domain Names - Implementation and Specification" RFC  
1035, Nov.
- [28] A. Kumar et al. , 1993 , ``Common DNS Implementation Errors and Suggested  
Fixes" RFC 1536, Oct.

## 附錄一：Bind 弱點

表一：CVE and Bind security reason

<b>CVE 編號</b>	<b>BIND Inverse-Query buffer overflow allows remote root access</b>	<b><u>CVE-1999-0009</u></b>
內容	若攻擊者能建立一個特殊的反向查詢請求(Inverse Query)，就可能導致記憶體內容的洩漏，其內容儲存大量執行相關的資訊。攻擊者可能利用其環境變數，獲取系統訊息；也可能利用這些資訊發動攻擊，造成系統無法回應，即可覆蓋記憶體內的指令，取得 root 權限。	受影響版本 ISC, BIND, 4.9.3~ ISC, BIND, 4.9.7 BIND 8~
修正	系統管理者可在 named.conf 的選項設定“fake-iquery yes;”。但在設定時需要考慮是否會產生這個漏洞，或升級最新版本。	BIND 8.1.2
<b>CVE 編號</b>	<b>Illegally formatted DNS request can crash some BIND servers</b>	<b><u>CVE-1999-0010</u></b>
內容	BIND 8 在預設上提供遞迴式定義 CNAMEs，需將權威性主機設定成拒絕存取，並且不支援遞迴式的定義 CNAMEs，才不會受到影響。	受影響版本 BIND 8
修正	1. 可在"options"設定中，加上 allow-transfer { none; };在 zone 區域，將權威性主機可設為 allow-transfer { any; };。 2. 可升級至 BIND 8.1.2 以上。	
<b>CVE 編號</b>	<b>BIND 8 can be crashed with zone-transfer for self referential record</b>	<b><u>CVE-1999-0011</u></b>
內容	DNS 伺服器提供"Zone Transfer"功能，若不限制"zone transfers"的對象，任何使用者皆可透過此種方式，得知整個 IP 位址或網域名稱的資料。假若可透過此方式取得相關資訊，也表示駭客能描繪出整個目標網路架構。因為每一台主機的網域名稱，通常是使用相關服務的名稱，因此能確切得知攻擊的目標，	受影響版本 BIND 4.9 BIND 8
修正	於 named.conf 檔案中，設定限制對象或不啟動 allow-transfer 選項，或升級最新版本。	
<b>CVE 編號</b>	<b>BIND allows attacker to change exchanged information between hosts</b>	<b><u>CVE-1999-0024</u></b>

內容	由於設計錯誤，而產生二個問題： 1. DNS service daemons 使用順序式的 ID，以達到訊息傳達。 若攻擊者使用此順序插入其他資料，可能導致 hostname/IP 對應發生錯誤。 2. 產生突發性的 API 動作，經由解析後可能產生比 MAXHOSTNAMELEN 還長的字串，引發記憶體溢出。	受影響版本 ISC, BIND, 8.1 ISC, BIND, 4.9.5
修正	只有 ISC BIND 4.9.5、8.1 會產生問題，請升級版本	
<b>CVE 編號</b>	<b>DNS allow updates can corrupt name server</b>	<b><u>CVE-1999-0184</u></b>
內容	BIND 在編譯時可加上允許動態更新的功能，因而使用 DALLOW_UPDATES 做動態更新的設定。此設計中發現弱點，而讓攻擊者有能力更改資源記錄(RR)。UNIX/NT 系統皆會發生此問題。	受影響版本 ISC, BIND,
修正	編譯時不使用 DALLOW_UPDATES 選項，或升級至最新版本。	
<b>CVE 編號</b>	<b>BIND 8.2 and 8.2.1 remote buffer overflow in the processing of NXT records</b>	<b><u>CVE-1999-0833</u></b>
內容	這項漏洞是發生於 DNS 伺服器上的 NXT 記錄。攻擊者送出一個 DNS 查詢到目標 DNS 伺服器。讓目標主機連線回到攻擊者的 DNS 伺服器。透過攻擊者特殊設計的 DNS 伺服器，對 NXT 記錄傳送一個約 6500 字元長的資料串，讓目標 DNS 伺服器產生緩衝區溢位。	受影響版本 ISC, BIND, 8.2.1 ISC, BIND, 8.2
修正	請升級至最新版本	
<b>CVE 編號</b>	<b>BIND could be remotely crashed by improper validation of SIG records</b>	<b><u>CVE-1999-0835</u></b>
內容	假若 SIG 無法在 BIND 正常運作時，會產生阻斷服務。	受影響版本
修正	建議安裝 8.2.2. Patchlevel 5 的修正程式，或升級至最新版本。	BIND 8.2.2 P5 以前的版本
<b>CVE 編號</b>	<b>BIND SO_LINGER issue could allow remote attackers to hang the service for intervals up to 120 seconds</b>	<b><u>CVE-1999-0837</u></b>
內容	關閉 TCP session 時候，蓄意違反正確的通訊協定，遠端攻擊者藉此可讓 named 暫停一段時間，最高可達 120 秒，這段時間內無法提供任何查詢功能，伺服器也不會有任何回應。	受影響版本 ISC, BIND, 8.2.1 ISC, BIND, 8.2
修正	建議安裝 8.2.2. Patchlevel 5 的修正程式，或升級至最新版本。	
<b>CVE 編號</b>	<b>BIND fdmax issue could allow remote attackers to crash the</b>	<b><u>CVE-1999-0848</u></b>

	<b>service</b>	
內容	遠端攻擊者可以故意製造大量的檔案，超過 BIND 可以管理的上限時，會導致 named 當機無法使用。(fdmax bug)	受影響版本 ISC, BIND, 8.2.1
修正	建議安裝 8.2.2. Patchlevel 5 修正程式，或升級至最新版本	ISC, BIND, 8.2
<b>CVE 編號</b>	<b>BIND maxdname buffer overflow could allow remote attackers to cause unexpected behavior</b>	<b><u>CVE-1999-0849</u></b>
內容	透過網路對於主機間的訊息交換時，更改成超長的網域名稱 (maxdname)，讓遠端攻擊者有機會能阻斷網域名稱伺服器的正常運作，或造成伺服器當機。執行 BIND 8.2.2 版本以下的所有 BIND 的主機都可能受影響。	受影響版本 BIND 4.9.5~ BIND 8.2.2 P2
修正	請安裝 BIND 8.2.2 PATCHLEVEL3(PL3)，或者升級至更新版本	
<b>CVE 編號</b>	<b>BIND server can be locally crashed by loading malformed zone info for NAPTR records</b>	<b><u>CVE-1999-0851</u></b>
內容	假若伺服器接收到有問題的 NAPTR(Naming Authority PoinTeR) 轄區訊息，可能使 BIND 無法正常讀取磁碟檔案的轄區訊息，此外不正常的讀取權限設定，也可能造成阻斷服務。	受影響版本 BIND 4.9.5~ BIND 8.2.2 P2
修正	安裝 BIND 8.2.2 PATCHLEVEL3(PL3)，或升級至最新版本	
<b>CVE 編號</b>	<b>ISC BIND named SIGINT and SIGIOT symlink Vulnerability</b>	<b><u>CAN-1999-1499</u></b>
內容	SIGINT：這個訊號通知 named，將把它的內部資料庫傾印(Dump Cache) 到/var/tmp/named_dump.db 檔案。傾印的檔案中含有這個名稱伺服器目前資料庫中的所有資料。 SIGIOT：這個訊號通知 named，將把統計資料加到 /var/tmp/named.stats。添加的檔案中含有名稱伺服器目前的統計資料。 BIND 8.1.x 是使用個人的目錄，並不會受此弱點影響。	受影響版本 ISC BIND 4.9.7 以前的版本
修正	請安裝 BIND 4.9.7 以後的版本，或者升級至更新版本	
<b>CVE 編號</b>	<b>Multiple Vendor Predictable Resolver ID Vulnerability</b>	<b><u>CVE-2000-0335</u></b>
內容	這個弱點是發生於使用 glibc 2.1.3 以前版本的解析器上，glibc 解析程序會結合機器上的時間與處理事件的編號，而產生亂數 ID，在此會產生二個同樣的號碼，在處理資訊的程序上會比對此 ID 是否正確，若不正確將其丟棄。ID 也是應用於比對回應請求訊息，若攻擊者在傳送訊息使用偽造 ID 功能，並且將其變化後，可成為多種類型的攻擊基礎。	受影響版本 glibc 2.1.3 以下 BIND 8.2.2 p5 以下

修正	升級到 glibc 2.1.3 以上的版本，或 BIND 8.2.2 p5 以上的版本	
<b>CVE 編號</b>	<b>Multiple Vendor BIND 8.2.2-P5 Denial of Service Vulnerability</b>	<b><u>CVE-2000-0887</u></b>
內容	攻擊者可利用這個設計錯誤的漏洞，而對遠端 DNS 主機提出 zone transfer 的請求，而此種經過壓縮的 zone transfer 請求，可能導致阻斷服務攻擊(DoS)。BIND 8.2.2 版本會因特殊設計的要求，導致系統癱瘓。	受影響版本 BIND, 8.2.2 p5 以下
修正	升級到 BIND 8.2.2 p5 以上，或最新版本。	
<b>CVE 編號</b>	<b>ISC BIND 8.2.2-P6 vulnerable to DoS when processing SRV records, aka the "srv bug"</b>	<b><u>CVE-2000-0888</u></b>
內容	Windows NT 4.0 與同時期的 DNS 版本都會受到影響，所提供的 DNS 服務，在接受大量的連續請求封包會形成 flooding 攻擊。攻擊者可能經由寄送大量的連續請求封包到 DNS 提供服務的 port 53，而造成主機形成阻斷服務(DoS)	受影響版本 BIND 8.2 ~ 8.2.2-P6
修正	升級到 BIND 8.2.2 p6 以上的版本，或最新版本。	
<b>CVE 編號</b>	<b>ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability</b>	<b><u>CVE-2001-0010</u></b>
內容	BIND 儲存請求(request)與產生回應(response)是使用相同的記憶體區塊，特別是用於回覆附加錯誤的程式碼與使用簽章所傳送的請求(request)。設計時是允許新的簽章覆蓋舊的簽章，覆寫後可由(請求-簽章=訊息長度)看出端倪。訊息長度對於記憶體中的資料長度無法覆寫，造成再次呼叫函數，並且堆積一連串的封包在記憶體內。入侵者可利用此弱點新增程式碼，並且加以執行。UDP 與 TCP 的請求在記憶體中是使用堆疊方式，當記憶體溢出時，入侵者即可任意執行程式。	受影響版本 ISC, BIND, 8.2~ ISC, BIND, 8.2.2 p7
修正	若使用 BIND 8.2.x 請升級到 8.2.3，或升級至最新版本	
<b>CVE 編號</b>	<b>ISC Bind 4 nslookupComplain() Buffer Overflow Vulnerability</b>	<b><u>CVE-2001-0011</u></b>
內容	BIND 4.9.8 之前的版本，使用 nslookupComplain()函數時，可能會產生記憶體溢出的弱點。這是記憶體區塊的功能轉載入 syslog 的錯誤訊息。攻擊者利用這個弱點，寄送特殊格式的 DNS 請求到目標主機上，若目標主機接受請求時，會中斷現有的處理程序，導致可能產生服斷服務或攻擊者可執行任意程式，若攻擊者可執行任意程式時，即代表取得 BIND 特權。	受影響版本 ISC, BIND, 4.9.3~ ISC, BIND, 4.9.7
修正	若使用 4.9.x 以前版本，建議升級到 4.9.8，或升級至最新版本。	

<b>CVE 編號</b>	<b>ISC BIND Internal Memory Disclosure Vulnerability</b>	<b><u>CVE-2001-0012</u></b>
內容	這個弱點是內部記憶體洩露資訊。遠端攻擊者寄送特殊格式的請求到 BIND 4 和 BIND 8，造成 ISC BIND 服務允許攻擊者存取記憶體內的堆疊資料，如此一來可能暴露系統程式或環境變數。	受影響版本 ISC, BIND, 4.9.3~
修正	請升級至 BIND 4.9.8 和 BIND 8.2.3，或者升級至最新版本。	ISC, BIND, 4.9.7 ISC, BIND, 8.2~ ISC, BIND, 8.2.2 p7
<b>CVE 編號</b>	<b>ISC Bind 4 nslookupComplain() Format String Vulnerability</b>	<b><u>CVE-2001-0013</u></b>
內容	BIND 4 版本使用 nslookupComplain() 函數時，存有格式字串 (Format String) 弱點，允許遠端攻擊者執行任意程式碼。這個問題也同樣發生於 BIND 曾報導的事件上，當服務發生錯誤時，系統會嘗試核對 IP 位址的名稱伺服器。攻擊者可能利用此方式造成記憶體溢出以達到攻擊的目的。	受影響版本 ISC, BIND, 4.9.3~ ISC, BIND, 4.9.7
修正	請升級到 BIND 4.9.8，或者升級至最新版本。	
<b>CVE 編號</b>	<b>BIND Inadvertent Local Exposure of HMAC-MD5 (TSIG) Keys</b>	<b><u>CAN-2001-0497</u></b>
內容	較早期的 BIND 8 與 BIND 9 會使用 dnskeygen 編譯出 HMAC-MD5 (TSIG) Keys，此功能是用於驗證 Master/Slave 伺服器之間的傳輸記錄和驗證動態 DNS，但是生成的 Key 是記錄於二個文件檔。只要攻擊者取得這個 Key 即可進行攻擊。	受影響版本 BIND, 8.2.4~ BIND, 8.2.4 BIND, 9.1 ~ BIND, 9.1.2
修正	更新到 BIND 8.2.5 與 BIND 9.1.3 以後的版本	

表二 弱點對照表

Reason			AXFR		NXT	NXT	SIG sigrecord	so_linger	fdmax	maxdname
Version	<u>CVE-1999-0009</u>	<u>CVE-1999-0010</u>	<u>CVE-1999-0011</u>	<u>CVE-1999-0024</u>	<u>CVE-1999-0184</u>	<u>CVE-1999-0833</u>	<u>CVE-1999-0835</u>	<u>CVE-1999-0837</u>	<u>CVE-1999-0848</u>	<u>CVE-1999-0849</u>
4.8										
4.8.1										
4.8.2.1										
4.8.3										
4.9.3		+	+							
4.9.4		+	+							
4.9.4 p1		+	+							
4.9.5		+	+	+			+			+
4.9.5 p1		+	+	+			+			+
4.9.6	+	+	+	-			+			+
4.9.7	+				+					+
4.9.8										
8.1	+	+	+	+	+		+	+	+	+
8.1.1	+	+	+	-			+	+	+	+
8.1.2							+	+	+	+
8.2					+	+	+	+	+	+
8.2 p1					+	+	+	+	+	+
8.2.1					+	+	+	+		+
8.2.2									-	+
8.2.2 p1										+
8.2.2 p2										+
8.2.2										+

p3										
8.2.2										+
p4										
8.2.2										+
p5										
8.2.2										+
p6										
8.2.2										
p7										
8.2.3										
8.2.4										
8.2.5										
9.0.0										
9.1.0										
9.1.1										
9.1.2										
9.1.3										
9.2.0										

**Vulnerable: '+', Not Vulnerable: '-', Feature does not exist: ' '**

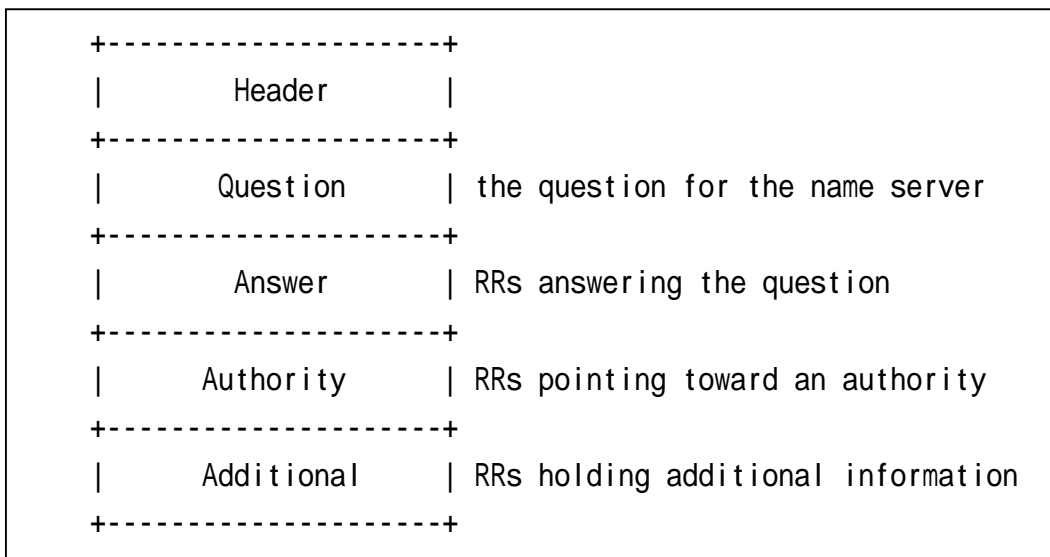
表三 弱點對照表

	naptr		resolver	ZXFR	srv	TSIG	Bind 4 Buffer	Infoleak	Bind 4 format	TSIG HMAC-MD5
version	<u>CVE-1999-0851</u>	<u>CAN-1999-1499</u>	<u>CVE-2000-0335</u>	<u>CVE-2000-0887</u>	<u>CVE-2000-0888</u>	<u>CVE-2001-0010</u>	<u>CVE-2001-0011</u>	<u>CVE-2001-0012</u>	<u>CVE-2001-0013</u>	<u>CAN-2001-0497</u>
	4.8									
4.8.1										
4.8.2.1										
4.8.3										
4.9.3		+					+	+	+	
4.9.4		+								
4.9.4 p1		+								
4.9.5	+	+					+	+	+	
4.9.5 p1	+	+					+	+	+	
4.9.6	+	+					+	+	+	
4.9.7	+	+					+	+	+	
4.9.8	+	+								
8.1	+	+						+		
8.1.1	+	+						+		
8.1.2	+	+						+		
8.2	+		+		+	+		+		+
8.2 p1	+		+		+	+		+		+
8.2.1	+		+		+	+		+		+
8.2.2	+		+	+	+	+		+		+
8.2.2 p1	+		+	+	+	+		+		+
8.2.2 p2			+	+	+	+		+		+
8.2.2			+	+	+	+		+		+

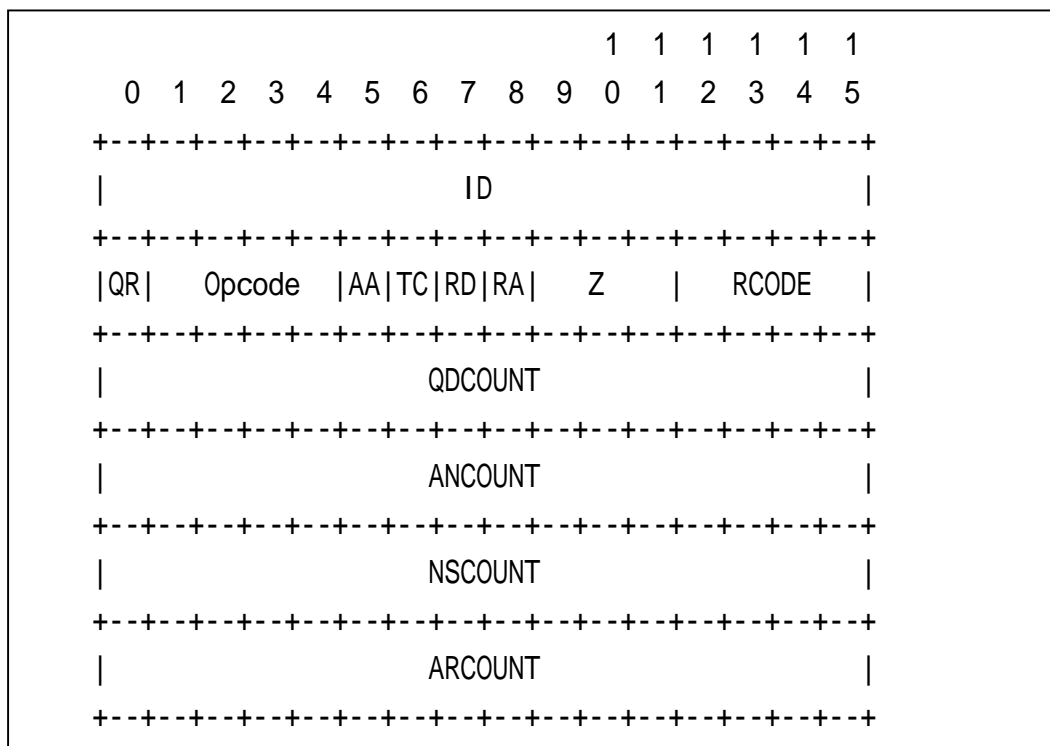
p3										
8.2.2			+	+	+	+		+		+
p4										
8.2.2			+	+	+	+		+		+
p5										
8.2.2				+	+	+		+		+
p6										
8.2.2						+		+		+
p7										
8.2.3										+
8.2.4										+
8.2.5										
9.0.0										+
9.1.0										+
9.1.1										+
9.1.2										+
9.1.3										
9.2.0										

**Vulnerable: '+', Not Vulnerable: '-', Feature does not exist: ' '**

## 附錄二：DNS 檢測封包格式



圖一：DNS 封包格式



圖二：DNS header 格式

