

中文摘要

近年來網際網路和資訊技術發展快速，各項網路服務帶給人們更為便利的生活環境，並開啟資訊社會的新時代。但隨著網路的蓬勃發展和其不受時空限制的特性，也引起人們對於網路安全的重視。因此，為了維持網路服務的可靠性、持續性及品質，網域管理者必須有效掌握網域內各節點最新資訊，才能在安全事件發生前進行預防措施或事件發生後即時提出因應之道。本論文的主要目的就是建置大規模網路掃描系統，協助網域管理者能夠快速取得網路節點資訊和自動化分析掃描所得到的資料。本研究以主動掃描(Active Scanning)和被動掃描(Passive Scanning)的方式對目標網域的網路節點進行探索，收集 Web Server、FTP Server、Mail Server、DNS Server、作業系統等版本資訊及 SSL 資訊，將所獲得的網路節點資訊存入資料庫，作為進一步統計分析的基礎，以利獲得各類伺服器的數量比。另外可透過 CVE(Common Vulnerabilities and Exposures)弱點資料庫找尋相關網路服務的弱點資訊，並評估被掃描網域各類伺服器的整體弱點比。本系統可以定期和持續對特定網路區域進行掃描，並將數據以 HTML 方式呈現給網域管理者作為查詢之用。在系統驗證方面，本研究以台灣網域作為實測目標網域，針對目前普遍使用的伺服器作一探索，並獲得台灣網域中各類伺服器的數量比和整體弱點比，另外也提出維護網路安全的相關建議。

關鍵字：網際網路、網路安全、大規模掃描、網路服務

Abstract

Internet services are becoming more popular and convenience as the information technology and network applications advance daily in the last few years. To ensure the quality and accessibility of Internet, the network security is an important concern. In order to maintain the reliability, continuity and its quality of Internet services, domain administrators must have access to the most updated information of every node within the network domain, so that they can take any precautionary steps or provide immediate solutions to decrease damages of network security incidents. The purpose of this thesis is to establish a Large-scale network security scanning system, which assists domain administrators in obtaining network nodes information efficiently, and analyzes the scanning data automatically. The research evaluate the targeted network nodes by using both Active Scanning and Passive Scanning methods; and collecting version information of Web Server, FTP Server, Mail Server, DNS Server, Operational System, and SSL. Furthermore, store those networks nodes information into the database for further analysis and comparison. Moreover, collecting the vulnerabilities of Internet service by using Common Vulnerabilities and Exposures (CVE) Information database, and then the vulnerabilities ratings of various Internet services can be obtained. The network security scanning system can be used to scan the targeted network domain periodically and consistently, and the scanning reports are available to domain administrators in HTML format. This research used Taiwan network domain for evaluation purpose, the study covers the most common used servers, obtained the version information and overall vulnerabilities rating of various server in this domain. At the same time, the recommendations for insuring network securities are provided.

Keywords: Internet, Network Security, Large-scale scanning, Network Services

誌謝

大學畢業後能夠順利考上研究所，讓我對這一段日子十分珍惜，尤其是這二年的求學生涯一眨眼就過去，在這段時間中，不僅僅校園生活伴隨著我渡過，以及同學之間的相互扶持，讓我的人生旅途上畫下一段美好的回憶。

在這段求學生涯當中，承蒙多位老師的悉心指點，讓我的論文得以順利完成。首要感謝的是我的指導教授鄭進興教授，鄭教授對於學術上的嚴謹態度，以及平日的諄諄教誨，讓我在撰寫論文時候受益匪淺。經過鄭老師的指點後，也讓我對於論文的架構有更完善的規劃，撰寫時也更加流順。此外在論文口試時，也十分感謝陳嘉玫教授、楊中皇教授等口試委員審試論文，並給予諸多寶貴的意見，讓我能夠針對論文的缺失作修正，以其獲得更完善的結果。

在這裡要由衷的感謝同窗好友承銓、國志、右龍、文弘、世哲...等一起度過求學歷程，與你們一起組電腦、玩遊戲和打球等等，讓我這二年來的日子過得更加充實，此外也要特別感謝學弟志昌和淵鐘，因為有你們的支持與幫助，使得一些問題能夠迎刃而解。最重要的是特別感謝台灣網路危機處理中心(CERT/CC)的各個成員，包括了陳年興教授、陳嘉玫教授的大力支持與幫忙、以及群佑、守廉、淑娟、慧芬、佳明等人的鼎力相助，殷殷期盼，讓此篇論文能夠順利的完成。因為有你們的陪伴，一起的學習，也使得我獲得更多寶貴知識與經驗，讓我這二年來研究生的日子，有你們而不寂寞。

最後，必須感謝我的家人以及妹妹，有你們的照顧，鼓勵和包容，讓我能夠順利完成論文，僅以此篇論文獻給我最愛的家人。

林柏宇 謹致於

樹德科技大學資訊管理研究所

中華民國九十一年六月

目錄

中文摘要	i
Abstract.....	ii
誌謝	iii
表目錄	v
圖目錄	vii
第一章 緒論	1
1.1 前言	1
1.2 研究背景	1
1.3 研究動機與目的	4
1.4 章節結構	5
第二章 研究內容與方法	6
2.1 研究範圍與假設	6
2.2 研究流程	6
2.3 網路安全檢查步驟	7
第三章 大規模網路安全檢查系統設計	13
3.1 製作原理說明	13
3.2 安全檢測系統設計問題之探討	17
3.3 掃描結果數據分析設計	19
3.4 研究限制	20
第四章 伺服器安全性檢查	21
4.1 調查目的	21
4.2 實驗環境	21
4.3 蒐集資料統計分析	22
4.4 安全性評估	45
第五章 結論與未來研究方向	52
5.1 研究成果與貢獻	52
5.2 結論與建議	53
5.3 未來研究方向	53
參考文獻	55

表目錄

表 1-1	弱點報告 (Vulnerabilities Reported).....	3
表 2-1	HOST 資料表	8
表 2-2	Date 資料表	8
表 2-3	Class C IP 資料表	9
表 2-4	Service 資料表	9
表 2-5	風險程度分類	10
表 2-6	弱點資料庫欄位格式	10
表 3-1	通訊埠範圍列表	13
表 3-2	HTTP/1.1 規範	14
表 3-3	Xprobe 辨識的作業系統類別	17
表 4.1	實驗環境	22
表 4-2	Web Server 版本統計表	23
表 4-3	Microsoft IIS 分布表	24
表 4-4	Apache 分布表	24
表 4-5	Netscape 分布表	24
表 4-6	Web Server 版本細項數量統計表	24
表 4-7	Microsoft IIS 系列版本細項數量統計表	25
表 4-8	Apache 系列版本細項數量統計表	25
表 4-9	Netscape 系列版本細項數量統計表	25
表 4-10	Web Server 其他版本細項數量統計表	26
表 4-11	Mail Server 版本細項數量統計表	27
表 4-12	Sendmail 系列分布表	27
表 4-13	Microsoft ESMTP MAIL Service v5.0 系列分布表	28
表 4-14	Microsoft Exchange v5.5 系列分布表	28
表 4-15	Mail Server 版本細項統計表	28
表 4-16	Sendmail 系列版本分類統計表	29
表 4-17	Mail Server 其他版本分類統計表	29
表 4-18	FTP Server 版本統計表	30
表 4-19	Microsoft IIS 系列分布表	30
表 4-20	Serv-U 系列分布表	31
表 4-21	Wu-FTP 系列分布表	31

表 4-22	FTP Server 版本細項統計表.....	31
表 4-23	Microsoft IIS 系列版本分類統計表.....	32
表 4-24	Serv-U 系列版本分類統計表.....	32
表 4-25	Wu-FTP 系列版本分類統計表.....	33
表 4-26	FTP Server 其他版本分類統計表.....	33
表 4-27	SSL 分布表.....	34
表 4-29	作業系統版本分類統計表.....	37
表 4-30	作業系統版本細項統計表.....	37
表 4-31	Windows Base 分類統計表.....	40
表 4-32	Windows Base 細項統計表.....	40
表 4-33	UNIX Base 分類統計表.....	41
表 4-34	UNIX Base 細項統計表.....	41
表 4-35	作業系統其他分類統計表.....	43
表 4-36	作業系統其他細項統計表.....	43
表 4-37	Web Server 整體安全性評估.....	45
表 4-38	Microsoft IIS 系列安全性評估.....	45
表 4-39	Apache 系列安全性評估.....	46
表 4-40	IIS/5.0 和 Apache/1.3.x 安全性評估比較.....	46
表 4-41	Mail Server 安全性評估.....	47
表 4-42	Sendmail 系列安全性評估.....	47
表 4-43	FTP Server 安全性評估.....	48
表 4-44	DNS 安全性評估.....	48
表 4-45	作業系統安全性評估.....	49

圖目錄

圖 1-1	全球連網主機數	2
圖 1-2	台灣連網主機數	2
圖 1-3	台灣 WWW Server 累計	3
圖 1-4	入侵事件回報統計	4
圖 2-1	研究流程	7
圖 3-1	Web Server 掃描	15
圖 3-2	Mail Server 掃描	15
圖 3-3	FTP Server 掃描	16
圖 3-4	DNS 掃描	16
圖 4-1	安全檢查方法	21
圖 4-2	Web Server 版本統計	23
圖 4-3	全球 Web Server 版本統計	26
圖 4-4	Mail Server 版本統計	27
圖 4-5	FTP Server 版本統計	30
圖 4-6	SSL 佔有比率統計	34
圖 4-7	DNS 版本統計	35
圖 4-8	作業系統版本統計	37
圖 4-9	Windows Base 細項版本統計	40
圖 4-10	UNIX Base 細項版本統計	41
圖 4-11	作業系統其他細項版本統計	43
圖 4-12	BIND Bug	49

第一章 緒論

1.1 前言

電腦科技日新月異，網際網路蓬勃發展，讓人們與電腦之間有著密不可分的相依關係。此外，政府大力推動基礎網路建設，將許多政策宣導及公眾服務放置在公開的網站上，提供便民化服務，而公司企業進行電子化，從製造、行銷到服務均與網路息息相關，讓人們的生活與網路有更良好的互動及密切結合。

網際網路的盛行，不僅僅帶來便利性，也帶來新型態的犯罪行為。駭客入侵事件層出不窮，利用作業系統或應用軟體的弱點，進而竊取資訊或不當存取網路資源。根據美國電腦網路危機處理/協調中心(CERT/CC)調查報告顯示，系統相關的弱點(Vulnerabilities)統計由 2000 年的 1,090 件增加到 2001 年的 2,437 件。這個數據顯示系統的弱點有逐漸增加的趨勢，能夠利用的範圍也隨之擴大。因此個人或企業組織，都必須了解網路安全的現況以及威脅性，進而設法有效降低電腦主機被入侵破壞的風險。

網際網路帶來的便利性有目共睹，但是透過網路傳播病毒或進行入侵的動作也隨著增加。日前曾有兩次大規模網蟲(Internet Worm)感染事件。一次是一隻名為 CodeRed(別名為紅色警戒、紅色代碼)的網蟲，在六天之內感染 250,000 台電腦；另一次是一隻名為 Nimda 的網蟲，利用 Windows 作業系統的網路芳鄰、Outlook 電子郵件和感染 IIS 伺服器作為其散播的根源地，在一天之內感染超過 100,000 台電腦。這樣的事件很清楚的表示現今病毒或網蟲已經不再被動式的感染，而是主動式的利用作業系統或應用軟體的弱點，透過網際網路的便利性，進行入侵與破壞的行為。

1.2 研究背景

根據美國 Network Wizards 公司統計，截至 2002 年 1 月止全球連網主機數已

突破一億四千萬台（如圖 1-1），也可由圖 1-2 中知道台灣連網主機數突破三百萬台。從這二個數據可以很明顯的看出，不論台灣地區或是全球區域，網路正在蓬勃發展，相對的網路服務也隨之增多，最明顯的例子就是 WWW Server。圖 1-3 為財團法人台灣網路資訊中心(TWNIC)所作統計，台灣地區 WWW Server 成長數量截至 2002 年 2 月止已達到 54,952 部，與 2001 年底比較，二個月之內增加了六千多部 WWW Server，因此網路服務與網路發展有著密切的關係。

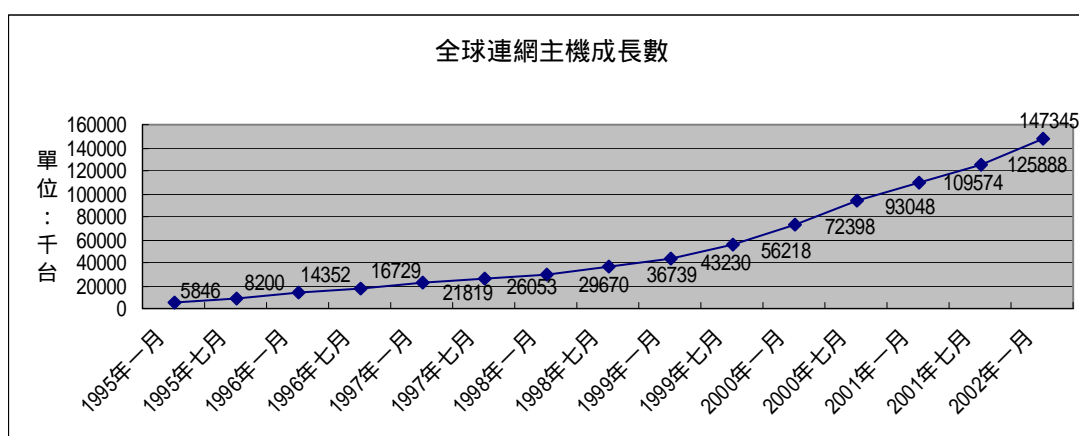


圖 1-1 全球連網主機數

資料來源：Network Wizards (<http://www.find.org.tw/>)

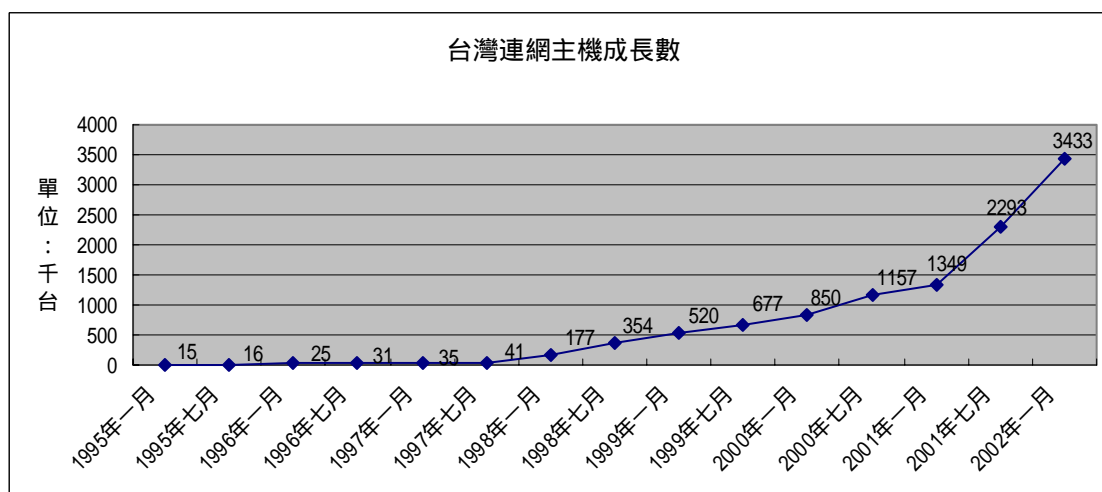


圖 1-2 台灣連網主機數

資料來源：Network Wizards (<http://www.find.org.tw/>)

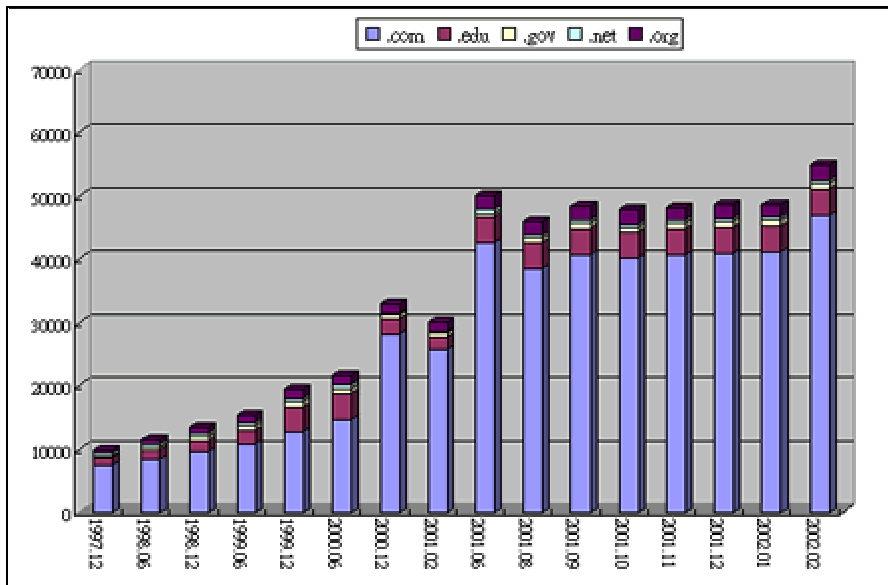


圖 1-3 台灣 WWW Server 累計

資料來源：<http://www.twNIC.com.tw/>

拜網際網路發達所賜，人們開始注意到開放的網路世界所存在的危險。雖然網路上的服務能夠帶給人們更多發展空間，但近幾年來，這些相關服務以及作業系統或應用程式的缺失也陸續被發現，不論個人或企業都深怕成為駭客攻擊的目標。有鑑於此，許多國家都紛紛成立 CERT(Computer Emergency Response Team) 組織，例如德國的 DFN-CERT、韓國的 CERT-kr、澳洲的 AUSCERT、以及台灣的 TWCERT。這些機構負責安全事件的處理或提供回報狀況，期望加強網路的安全性。因此根據 CERT/CC 的統計，從 1995 年至 2001 年的弱點報告總共有五千多個(表 1-1 所示)，並且截至 2001 年總共接獲了 100,369 個入侵事件的求助，歷年來詳細的統計資訊如圖 1-4 所示，可見近兩年入侵事件增加迅速，因此提昇網路系統之安全性是當務之急。

表 1-1 弱點報告 (Vulnerabilities Reported)

年份	1995	1996	1997	1998	1999	2000	2001	Total
數量	171	345	311	262	417	1,090	2,437	5033

資料來源：<http://www.cert.org/>

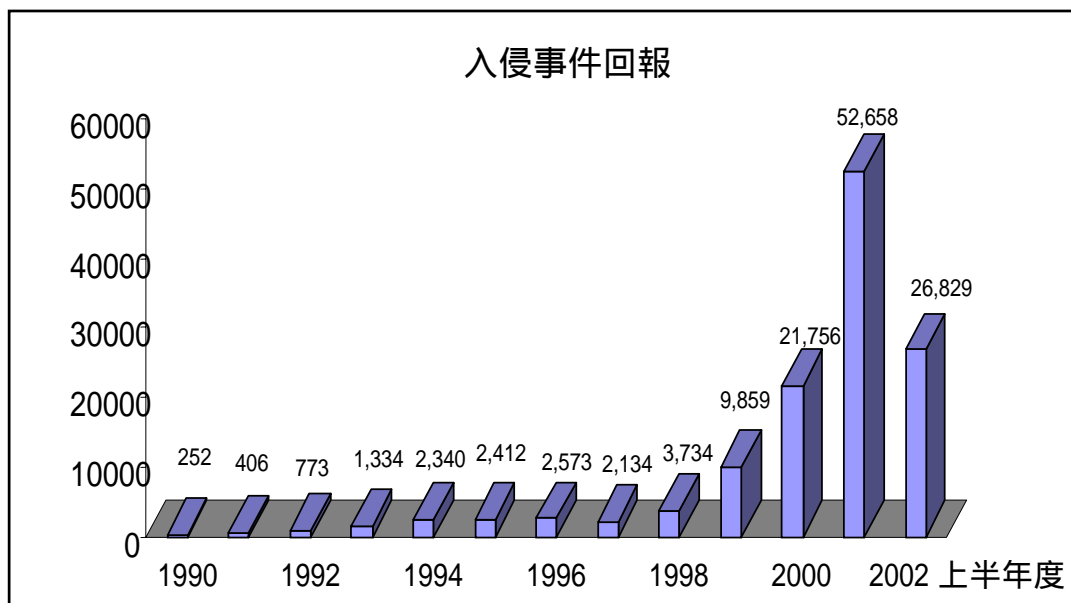


圖 1-4 入侵事件回報統計
資料來源：<http://www.cert.org/>

1.3 研究動機與目的

電腦資訊網路科技迅速發展，並普遍運用到各種企業組織中，作為資訊交換、資源分享及企業各項營運管理等，扮演重要角色的地位已無法取代。近期政府和相關單位也逐漸重視網路安全問題，成立資通安全會報，進行電腦網路和安全性相關議題的研究與整合，期望透過這些研究與整合的成果能夠促進台灣網域的安全性，並帶給網路使用者實質上的幫助。但對一般大眾而言，資訊系統的安全度在意識型態上仍然是很薄弱的，許多人並未實體感受到資訊安全的重要性而漫不經心。因此，審慎評估網站的安全性、保持公眾服務的持續性，以及網站內存放資料之完整性和隱密性，成為網路應用中迫在眉睫的重要工作。本研究的目的是在於建置自動化大規模網路掃描機制，以達成以下目標：

1. 研究如何有效率的延伸掃描廣度，收集網路資訊，使得擁有最大涵蓋率。

2. 建立自動化大規模網路掃描機制，建立資訊安全掃描自動化收集系統。
3. 建立網路節點資訊資料庫，增進自動化分析的能力，使得能掌握最新網路資訊狀況。

本研究以台灣網域作為實測目標網域，大規模收集網路節點作業系統平台及網路服務版本資訊，建立台灣網域網路節點資訊資料庫，並針對不同的作業系統平台及各類網路服務收集其安全弱點資訊，存成弱點資料庫。利用此資料庫，能夠與蒐集的網路節點資料進行分析統計並作比對，即可了解台灣地區整體網路之安全性。此調查結果也可作為如何提升台灣地區網路安全性的參考指標，每當有最新的安全弱點發佈時，亦可經由網路節點資訊資料庫分析與統計，得知此弱點對台灣網域的威脅程度。

1.4 章節結構

本論文共分成五章：第一章為緒論，主要介紹本論文研究背景和研究動機，並說明章節結構；第二章為研究內容與方法，針對本研究的研究範圍、研究流程和網路安全檢查步驟有深一層的探討與分析；第三章為大規模網路安全檢查系統設計，針對系統製作原理、設計方式、安全檢測的考量、掃描結果數據分析設計和研究限制提出說明；第四章是伺服器安全性檢測實作，對台灣網域進行掃描，收集資訊、分析數據並提供建議；最後在第五章做一總結，將本研究的應用做一說明，並提出未來研究方向，以供後續研究之參考。

第二章 研究內容與方法

2.1 研究範圍與假設

科技帶來了新型態的犯罪，網路已然成為新興的犯罪方式，只是火力來自鍵盤，而非槍砲。駭客入侵的案例層出不窮，且入侵手法持續翻新，但主要還是利用作業系統或網路應用程式之弱點。在入侵行動過程中，通常先針對目標電腦主機開啟的服務，蒐集相關資訊以利入侵，所以系統上的設定及網路應用程式的資訊，都有可能讓有心人士作為入侵的依據。因此本研究將建置一大規模網路安全檢查系統，針對台灣網域進行網路大規模掃描，收集網路節點作業系統版本資訊，檢測是否提供 WWW、MAIL、FTP、DNS、SSL 等網路應用程式及其版本資訊，並與弱點資料庫進行比對，以評估整體網路安全性。

2.2 研究流程

本研究以台灣網域為系統實證目標網域，並針對網路節點作業系統平台及網路服務版本資訊做一探索，以期望得到相關資訊，並藉此分析其安全性，讓網域管理者充分掌握網路最新資訊狀況。

本論文的研究架構方面，提出五個研究流程(如圖 2-1 所示)，詳細說明如下：

1. 針對相關工具、服務辨識(Service Fingerprinting)、掃描方式做一研究，探討何種方法能夠幫助本研究探索網路節點資訊。
2. 分析相關工具之後，規劃網路安全檢查系統架構，並針對此系統各項環境因素或變數做考量，以利達成所需的目的。
3. 建構網路節點資訊蒐集工具。
4. 本研究以台灣網域做為研究環境，利用建構好的資訊蒐集工具，蒐集各項

網路節點資訊做為原始資料，評估此實驗結果。

5. 結論與建議。針對收集的資訊做詳細的探討和分析，並提出結論和建議。

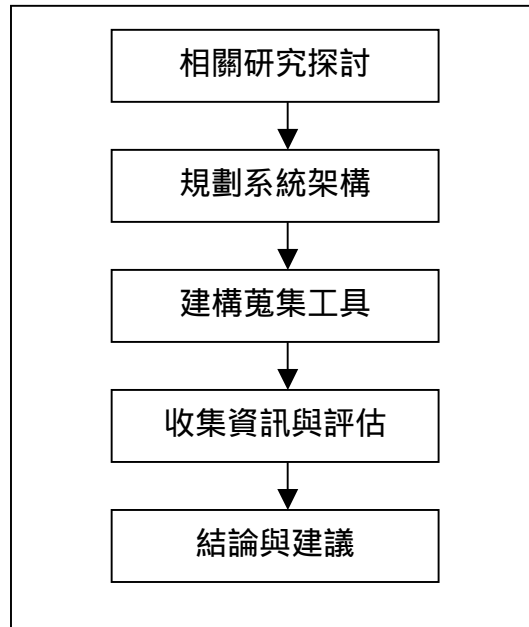


圖 2-1 研究流程

2.3 網路安全檢查步驟

針對大規模網路安全檢查，可分為三部分。第一部分在掃描主機端先行建置網路節點資訊資料庫架構及大規模自動化網路掃描機制；第二部分針對選定的範圍做掃描和探索；第三部分為分析數據以及評估安全性。根據三大部分可以規劃出五個步驟，詳細內容與做法說明如下：

步驟一、規劃大規模掃網路描資料庫格式

自動化大規模網路節點資訊收集系統，收集的網路節點資訊包括作業系統版本資訊及網路服務資訊，其中網路服務資訊將以 Web Server、FTP Server、Mail Server、SSL 及 DNS Server 資訊為主。資料庫系統採用 MySQL[1]，資料庫架構如

表 2-1~2-4 所示，以便將收集的資料妥善分類，以利查詢和應用。各資料表說明如下：

Host 資料表：主要用來儲存網路節點之基本資訊。

Class C IP 資料表：存放掃描目標網域之 IP Address。

Date 資料表：存放掃描日期。

Service 資料表：儲存網路節點之網路服務軟體種類及版本資訊。

表 2-1 HOST 資料表

名稱	型態	長度	索引	備註
IP	VarChar	15	P	IP 位址 範例：210.71.14.90
HostName	VarChar	100		主機名稱 範例：www.stu.edu.tw
Type	Int(Unsigned)			主機名稱歸類(以代號表示) 1 edu 5 org 2 gov 6 mil 3 com 7 idv 4 net 8 other
OS_Version	VarChar	100		作業系統版本資訊 範例：Sun Solaris 2.3-2.8
Date_ID	Int(Unsigned)			做為 Service 掃描時間記錄 範例： 1(90.01.01) 2(90.01.16)

表 2-2 Date 資料表

名稱	型態	長度	索引	備註
Date_ID	Int(Unsigned)		P	1(90.01.01) 2(90.01.16)
Date	Char	8		90.01.01

表 2-3 Class C IP 資料表

名稱	型態	長度	索引	備註
IP	VarChar	11		IP 位址 範例：210.71.14.90

表 2-4 Service 資料表

名稱	型態	長度	索引	備註
IP	VarChar	15		IP 位址 範例：210.71.14.90
Stype	Int(Unsigned)			網路服務種類(以代號表示) 1 WWW 4 SSL 2 FTP 5.DNS 3 MAIL
S_version	VarChar	150		網路服務版本資訊 範例：Microsoft-IIS/5.0
Domain_ID	Int(Unsigned)			主機名稱歸類(以代號表示) 1 edu 5 org 2 gov 6 mil 3 com 7 idv 4 net 8 other
Date_ID	Int(Unsigned)			做為 Service 掃瞄時間記錄 範例： 1(90.01.01) 2(90.01.16)

步驟二、收集作業系統及網路服務安全弱點資料

大部分的弱點來自於作業系統或應用程式的缺陷，而這些弱點很容易讓攻擊者加以利用，進而越權非法存取電腦資源。因此收集作業系統及網路服務安全弱點資訊並存入資料庫，可以了解網路安全情況。本研究弱點資料庫以網路服務版本做為關鍵查詢，主要從 CVE[2]資料庫中收集相關弱點資訊。

由於弱點型態有多種形式，包括 Buffer Overflow、Design Error 等，並且在不同的研究當中其代表的意義又不盡相同，針對這些多變的形式，多數學者[3][4]提出弱點分類的觀念，將弱點型態依照其造成的影響歸類。在此我們也對所收集的弱點資訊做一分類，風險程度如表 2-5 所示：

表 2-5 風險程度分類

分類	說明
DoS	阻斷服務攻擊(Denial of Service)。 說明：利用應用程式或系統的漏洞對目標電腦進行攻擊，並耗盡目標電腦的資源，導致目標電腦無法提供網路服務。另外如果使用多台電腦進行攻擊，則會造成 DDoS(Distributed Denial of Service)。
Gain Privilege	取得權限。 說明：利用應用程式或系統的漏洞，進而取得額外的權限。這範圍包括系統管理者(root、administrator 或 supervisor)權限、修改檔案的權限或其他相關的權限，並利用取得的權限執行攻擊者想要的命令或程式。
Info Leak	資料洩漏。 說明：攻擊者能夠由遠端取得本地端的資料。
Miscellaneous	惡意程式。 說明：其他種類的弱點影響，包括 Virus、Worm 等。

依照上表的分類，將此分類納入資料庫的欄位中，並制訂一弱點資料庫做為本研究之用。此資料庫架構如表 2-6 所示：

表 2-6 弱點資料庫欄位格式

欄位名稱	型態	長度	備註
ID	Int(Unsigned)		弱點編號
Server	VarChar	10	網路服務總類 範例：WWW、FTP、MAIL...
Vname	VarChar	100	漏洞名稱 範例：Sendmail mail.local Vulnerabilities

CVE	Int(Unsigned)		CVE 編號 範例：CVE-2000-0319
Description	text		弱點描述 範例：mail.local in Sendmail 8.10.x does not properly id...
Platform	VarChar	100	影響平台，作業系統名稱或網路服務 範例：Sendmail 8.10x
Impact	text		影響情形 範例：Failure to Handle Exceptional Conditions
DoS	Char	1	風險程度：阻斷服務攻擊
Gain Privilege	Char	1	風險程度：取得權限
Info Leak	Char	1	風險程度：資料洩漏
Miscellaneous	Char	1	風險程度：惡意程式

步驟三、大規模網路掃描系統設計及實作

1. 撰寫掃描系統的主程式。
2. 選定目標網域作為檢測的範圍。
3. 針對目標網域做網路節點檢測，蒐集的資訊如下所示：
 - (1). Web Server 軟體種類及版本資訊
 - (2). Mail Server 軟體種類及版本資訊
 - (3). FTP Server 軟體種類及版本資訊
 - (4). DNS Server 軟體種類及版本資訊
 - (5). SSL 資訊
 - (6). 作業系統軟體種類及版本資訊

4. 蒐集上述的資訊，並根據步驟一所制定的資料表，將資訊寫入資料庫。

步驟四、蒐集弱點資訊

蒐集各作業系統廠商所發佈的安全通報，以及相關研究單位發佈的弱點資訊，並加以歸類。

步驟五、掃描結果統計與分析及安全性評估

將本研究所收集的網路節點資訊存入資料庫，並整理成圖表，以利未來能夠快速查詢及安全性評估。

第三章 大規模網路安全檢查系統設計

3.1 製作原理說明

根據網際網路通信協定參數總註冊中心(Internet Assigned Numbers Authority, [5])所提出的通訊埠列表[6]定義通訊埠分為三個範圍，如表 3-1 所示。本研究所要探討的五種網路服務型態為 Web Server、Mail Server、FTP Server、DNS Server 和 SSL 位於常見的通訊埠範圍內，並得知 Web Server 的通訊埠為 80(HTTP)、Mail Server 的通訊埠為 25(SMTP)、FTP Server 的通訊埠為 21(FTP)、DNS Server 的通訊埠為 25(DOMAIN)以及 SSL(HTTPS)的通訊埠為 443。至於擁有相同服務而採用不同埠號的 IP 位址，不在本研究的掃描範圍內。

表 3-1 通訊埠範圍列表

分類	範圍 (埠號)
常見的通訊埠 (Well Known Ports)	0 - 1023
已註冊的通訊埠 (Registered Ports)	1024 - 49151
動態或私人通訊埠 (Dynamic or Private Ports)	49152 - 65535

資料來源：<http://www.iana.org/>

大規模網路安全檢查系統的製作原理說明分為五部分，為了收集相關資訊，本研究以 C 或 Perl 程式語言實作本系統，收集網路節點之作業系統及網路服務資訊，以達成探索的目的。以下為製作原理說明：

3.1.1 Web Server 資訊掃描程式

根據網際網路資訊標準組織(World Wide Web Consortium,[7])所提出的 Hypertext Transfer Protocol -- HTTP/1.1 中定義的規範。本研究參考此規範中的定義(如表 3-2 所示)，對目標主機作通訊埠 80 的連結並送出 HEAD / HTTP/1.0 的請求，

即可由回傳的訊息中得知此目標主機的 Web Server 服務版本資訊。

表 3-2 HTTP/1.1 規範

Method	Content
OPTIONS	The OPTIONS method represents a request for information about the communication options available on the request/response chain identified by the Request-URI.
GET	The GET method means retrieve whatever information (in the form of an entity) is identified by the Request-URI.
HEAD	The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response.
POST	The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.
PUT	The PUT method requests that the enclosed entity be stored under the supplied Request-URI.
DELETE	The DELETE method requests that the origin server delete the resource identified by the Request-URI.
TRACE	The TRACE method is used to invoke a remote, application-layer loop-back of the request message.
CONNECT	Request a forwarded network connection to a remote server.

資料來源：<http://www.w3.org/>

依照上述的方法作一檢測實驗,如圖 3-1 所示,可以取得目標主機的 Web Server 種類及版本資訊為 Apache-AdvancedExtranetServer/1.3.23[8],也能夠獲得外掛模組的資訊,以此範例而言就是 mod_ssl/2.8.7 OpenSSL/0.9.6c PHP/4.1.2。因此本研究撰寫相關程式對目標主機進行主動掃描,以便取得所需要的資訊,並設定連線逾時以及改變特定服務版本名稱,刪減不需要的資料回傳。

```
Trying 210.71.14.250...
Connected to ev.mis.stu.edu.tw (210.71.14.250).
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 401 Authorization Required
Date: Tue, 07 May 2002 16:18:43 GMT
Server: Apache-AdvancedExtranetServer/1.3.23 (Mandrake Linux/4mdk) mod_ssl/2.8.7 OpenSSL/0.9.6c PHP/4.1.2
WWW-Authenticate: Basic realm="使用者密碼"
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```

圖 3-1 Web Server 掃描

3.1.2 Mail Server 資訊掃描程式

大部分的 Mail Server 都建構在 Unix-like 系統上，但受到設定方式以及版本的影響，多項人為因素的缺失也隨之浮現。一般而言，一些舊版本的 Mail Server 很容易找到相關攻擊程式，藉此由遠端取得權限，或造成 Mail Relay 問題。因此本掃描程式對 Mail Server 作版本的探測，與目標主機作通信埠 25 的連結，以便取得相關資訊。

依照上述的方式作一實驗，如圖 3-2 所示，可以取得目標主機的 Mail Server 種類及版本為 ESMTP Postfix [9] (Postfix-20010228-pl08) (Mandrake Linux)[10]。因此本研究撰寫相關程式對目標主機進行主動掃描，以便取得所需要的資訊，並設定連線逾時以及改變特定服務版本名稱，刪減不需要的資料回傳。

```
[root@ev salamander]# telnet 210.71.14.9 25
Trying 210.71.14.9...
Connected to yen-mdk.mis.stu.edu.tw (210.71.14.9).
Escape character is '^]'.
220 yen-mdk.stu.edu.tw ESMTP Postfix (Postfix-20010228-pl08) (Mandrake Linux)
```

圖 3-2 Mail Server 掃描

3.1.3 FTP (File Transfer Protocol) Server 資訊掃描程式

FTP Server 是提供檔案交換中最常使用到的伺服器，且易於架設與取得相關程式。FTP Server 版本探測是對目標主機作通信埠 21 的連結，即可由回傳的訊息中得知此目標主機的 FTP Server 服務種類與版本資訊，如圖 3-3 所示，可以得知目標主機的 FTP Server 種類與版本資訊為 ProFTP 1.2.5rc1[11]，本研究撰寫相關程式對目標機器主動掃描，以便取得所需要的資訊，並設定連線逾時以及改變特定服務版本名稱，刪減不需要的資料回傳。

```
[root@ev salamander]# telnet 210.71.14.250 21
Trying 210.71.14.250...
Connected to ev.mis.stu.edu.tw (210.71.14.250).
Escape character is '^]'.
220 ProFTPD 1.2.5rc1 Server ready.
```

圖 3-3 FTP Server 掃描

3.1.4 DNS (Domain Name Server) 資訊掃描程式

透過 Unix 底下的 dig 程式作為查詢 BIND DNS[12]版本資訊的工具，透過此方法作一實驗，如圖 3-4 所示，可以得知目標主機的版本為 BIND 9.2.0。

```
[root@ev salamander]# dig @210.71.14.99 version.bind chaos txt
; <<>> DiG 9.2.0 <<>> @210.71.14.99 version.bind chaos txt
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29544
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                0      CH      TXT      "9.2.0"

;; Query time: 6 msec
;; SERVER: 210.71.14.99#53(210.71.14.99)
;; WHEN: Wed May 8 02:09:46 2002
;; MSG SIZE rcvd: 48
```

圖 3-4 DNS 掃描

3.1.5 SSL (Secure Sockets Layer) 資訊掃描程式

SSL 是一種加密機制，透過此加密機制和伺服器上的認證能夠提昇資料傳遞的保密性。一般而言，在網路上進行電子商務活動都是透過 SSL 安全機制。本研究使用 Alexey Semenov 所撰寫的 tcpscan.c，並於作者網頁 (<http://www.geocities.com/SiliconValley/Way/7914/>) 下載此程式，進行資料收集。

3.1.6 作業系統 (Operation System) 資訊掃描程式

本研究利用 The Sys-Security Group[13]所開發的 Xprobe[14]作為判斷作業系統版本的工具，此工具以 ICMP Usage In Scanning Research project[15]為基礎而發展。作業系統的掃描方法有多種[16][17]，本研究利用被動掃描[18][19][20][21][22]的方式，進而得知目標主機的作業系統版本資訊。目前能夠判斷的作業系統平台如表 3-3 所示。

表 3-3 Xprobe 辨識的作業系統類別

Unix Like Base	如 Linux、FreeBSD[23]、Solaris[24]...
Windows Base	如 Windows 95、Windows 98、Windows 2000[25]...
其他	如 Cisco IOS[26]...

3.2 安全檢測系統設計問題之探討

本研究實施安全檢測的對象為台灣網域，並收集六種網路節點資訊進行統計分析。因此在開始大規模掃描之前，先對區域網路作初步掃描測試，收集相關資訊，作為系統修正改進的依據。另外對網路掃描而言，最重要的是速度、友善性、準確性等特性，因此在作初步掃描的時候，也根據這幾項特性而作程式修改。本研究選定樹德科技大學網域為對象，對校園內部分區域網路(Class C)作一初步檢測，此一小規模初步掃描能夠獲知樹德科技大學網域內各目標主機之作業系統及網路服務資訊。藉此我們可以對回應資料的處理方法、未知的網路服務型態歸類

以及網域檢測探索等問題，提出三個解決方法如下：

1. 增進掃描速度：

- (1). 判定目標主機是否存在：先採用 ping 目標主機檢測是否有回應。沒有回應時，有三種可能性：(a) 目標主機不存在 (b) 目標主機關機 (c) 目標主機裝設防火牆，不對 ICMP 封包作回應。根據初步檢測結果，沒有 ping 而直接掃描一 Class C 所需時間約為六分鐘；而利用 ping 取得 Class C 中目標主機的存活後，再進行掃描，所需時間約為三分鐘，由此數據發現利用 ping 過再掃描能夠縮減一半時間。本研究掃描的對象屬為台灣網域，掃描的時效性是必須考量的重點，所以本研究採用 ping 之後再掃描，以縮短掃描時間，至於裝設防火牆而不回應 ping 的目標主機，本研究假設其已經做好安全防範與規劃，而不去探索。
- (2). 逾時時間設定：在初步掃描時發現，掃描某些目標主機時程式會被對方主機 Hold 住，因此設定 TimeOut 時間以解決此問題，在設定時間內沒有回應則放棄此一 IP 位址之掃描。

2. 增進友善性：

- (1). 亂數 IP 位址掃描：由於掃描的動作在認知上都是屬於非法入侵的行為，而採用循序 IP 位址掃描，會讓網路管理者輕易的發現正在進行探索檢測的動作，因此本研究利用亂數打散欲進行掃描的 IP 位址，藉此減低風險，避免不必要的抱怨及抗議。
- (2). 本研究對有防火牆保護的區域不作探索，但有防火牆保護並不代表其區域是絕對安全的，因為防火牆有許多種類的廠牌，各有不同的存取設定策略 (Policy)，目前本研究所發展的系統為顧及掃描廣度、速度，沒有做到穿透防火牆進行大規模掃描。

3. 增進準確性：

- (1). 修改已知服務的版本名稱：有些回應的版本名稱略有出入，例如針對 Microsoft Exchange SMTP Server v5.5 作探索則回傳值是 ESMTP spoken here。因此本研究對特定的服務型態重新分析並歸類。
- (2). 分析：有些回傳資訊並非在本研究中用到，因此在程式中增加分析(parse)的動作，擷取符合本研究所需要的資訊，並減少人工除錯的時間。

另外針對如何增進系統掃描效能，以期快速取得資訊，本研究也提出下列幾項方式：

1. 系統資源問題：解決資源不足有下列方法：(1) 增加記憶體。本系統需要大量的 process，因此增加記憶體能夠減輕系統負荷 (2) 定期卸除逾時過久的 process。由於網路或目標主機的問題，可能造成此 process hold，因此一段時間就必須卸除被 hold 的程序 (3) 在每一個 process 之間設定延遲時間，每一 process 掃描時間約為 3~5 秒鐘，因此設定延遲 3 秒有助於程序之間的系統負荷量減至最輕 (4) 調整系統 Kernel 設定。對於系統 Kernel 不必要的設定可以刪除，並針對上述的三點情況再加以修改。
2. 平行處理：利用多台掃描主機進行大規模網路節點資訊收集，分擔所需要掃描網域的不同網段範圍，或是分別收集不同的網路服務資訊，將可以大幅度增加掃描效率，縮短掃描時間。
3. 增加網路頻寬：若將掃描主機放在網路骨幹上進行資訊收集掃描，可以避免因為網路壅塞，而無法收集到資訊。

3.3 掃描結果數據分析設計

利用網頁的便利性製作出良好的使用者介面，本研究將掃描後的數據，依網路服務的種類呈現在網頁中。在此網頁的報表中針對每項網路服務的分佈作分析，並且將這些數據與弱點資料庫相比較以獲得該項網路服務的整體弱點比，以

快速掌握台灣網域之網路節點資訊及安全性評估。

3.4 研究限制

掃描行為在一般的認知上都是屬於非法入侵行為，而本研究所掃描的區域為台灣網域，相對的掃描到一些公司或企業網路的情況無可避免。針對這些掃描過程中以及在初步掃描所發生的問題，本研究盡量排除，在此提出幾項研究限制說明：

1. 掃描流程限制

- (1). Intranet 掃描問題：本研究主要是針對網域的實體 IP 位址而非虛擬 IP 位址作掃描，因此企業組織內部虛擬 IP 位址的機器不做掃描。
- (2). 掃描請求問題：由於掃描的動作是屬於非法，因此在作研究時先針對掃描的區域作一判斷，確定責任範圍，並向相關單位提出申請，以免遭到不必要的抱怨。
- (3). 服務版本問題：多數系統的預設安裝(Default Setup)就已經包含有部分基本服務，例如 RedHat[27]和 FreeBSD 會預設安裝 Sendmail[28]，而 Windows 2000 Server 以上版本預設也會安裝 Microsoft ESMTP MAIL Service。因此本系統只針對網路節點是否有安裝該項網路服務，而實際上並不判斷是否真有提供此服務。

2. 弱點資料庫限制

- (1). 弱點資料庫問題：本研究採用 CVE 的弱點資料，並根據 CVE 的 ID 至 Securityfocus[29]或相關伺服器/作業系統廠商蒐集安全通報詳細內容。
- (2). 弱點資料正確性：目前本研究只是單純針對版本作弱點預測，因此如果要更準確的作弱點預測則必須引入完善的弱點資料庫[3]，才能獲得更高的準確率。

第四章 伺服器安全性檢查

4.1 調查目的

現今網際網路成為生活的一部分，資訊的交換也隨之增加，因此確保網路節點上各主機的安全持續運作是必要的。本研究以台灣網域作為主要探索區域，收集作業系統平台以及網路服務版本資訊，並藉由收集的資料做分析統計，評估台灣網域各類服務的安全性，調查方式如圖 4-1 所示。

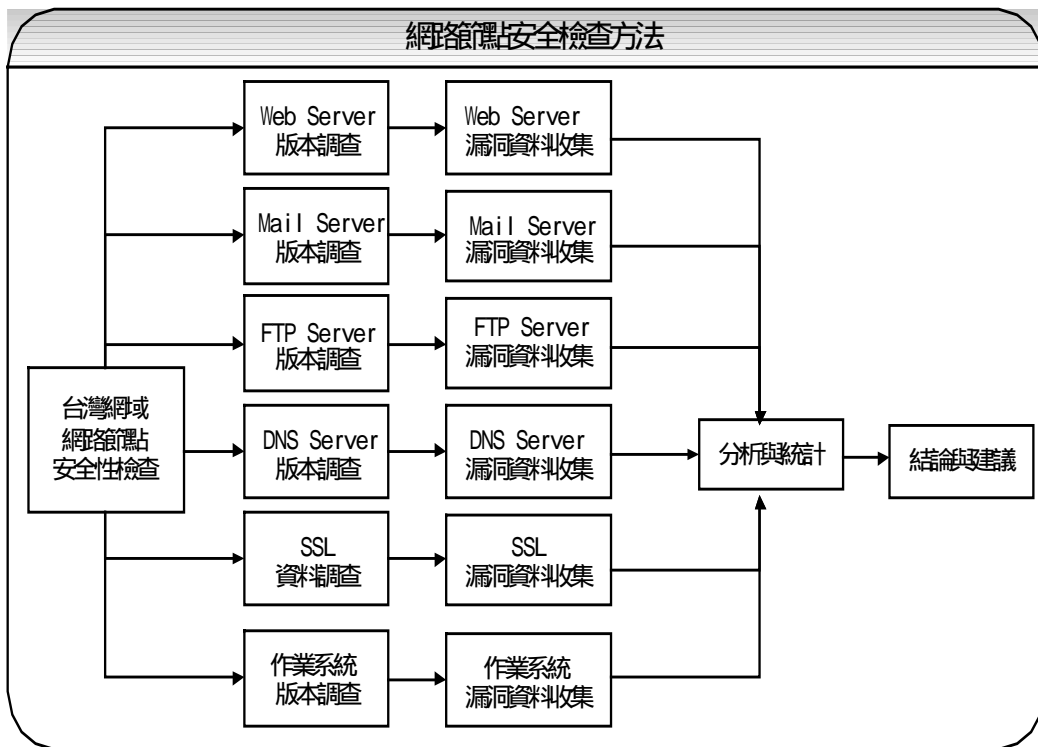


圖 4-1 安全檢查方法

4.2 實驗環境

本研究實驗環境如下：

表 4.1 實驗環境

掃描主機等級	Pentium 4-1.5G PC
記憶體	128MB
作業系統	Mandrake Linux 8.1
資料庫版本	MySQL 3.23.47
程式語言	C 及 Perl
主機放置地點	國立中山大學
掃描時間	約一個月 (2002/04/10 ~ 2002/05/1)
掃描範圍	根據教育部所提供的台灣區網際網路網路位址範圍 [30]做為實驗,得知共有 28,904 筆 Class C,利用 ping 做回應查詢後有 397,580 筆 IP,因此實際掃描 IP 數為 397,580 筆。

4.3 蒐集資料統計分析

本次調查台灣地區各網路節點伺服器的數據簡述如下：

1. Web Server 共有 51,315 筆資料,佔有比例依次為 Microsoft IIS (45.874%), Apache (34.682%), Netscape (3.432%), 其他 (16.013%)。
2. Mail Server 共有 43,577 筆資料,佔有比例依次為 Sendmail (46.598%), Microsoft ESMTP MAIL Server v5.0 (27.260%), Microsoft Exchange 5.5 (8.059%), 其他 (18.083%)。
3. FTP Server 共有 49,058 筆資料,佔有比例依次為 Microsoft FTP (24.669%), Serv-U (14.876%), Wu-FTP (14.524%), 其他 (45.931%)。
4. SSL 共有 22,114 筆資料,在 Web Server 中佔有比例為 43.094%。
5. DNS Server(BIND)共有 11,053 筆資料,佔有比例依次為 8.2.3 (21.795%), 8.1.2 (16.602%), 8.2.2 (14.548%)。
6. OS 版本資訊共有 317,113 筆資料,佔有比例依次為 Windows Base

(48.728%)，Unix Base (23.110%)，其他 (28.161%)。

各項服務圖表統計如下所示：

4.3.1 Web Server 版本數量統計

在 397,580 筆 IP 中共有 51,315 筆 Web Server，並由圖表得知，台灣地區的 Web Server 仍然以微軟的 IIS 為多數，其次為 Apache，第三才是 Netscape[31]系列的伺服器。

依照單一版本統計，則以 Apache/1.3 系列版本為最多，其次是 Microsoft-IIS/5.0，接著是 Microsoft-IIS/4.0。

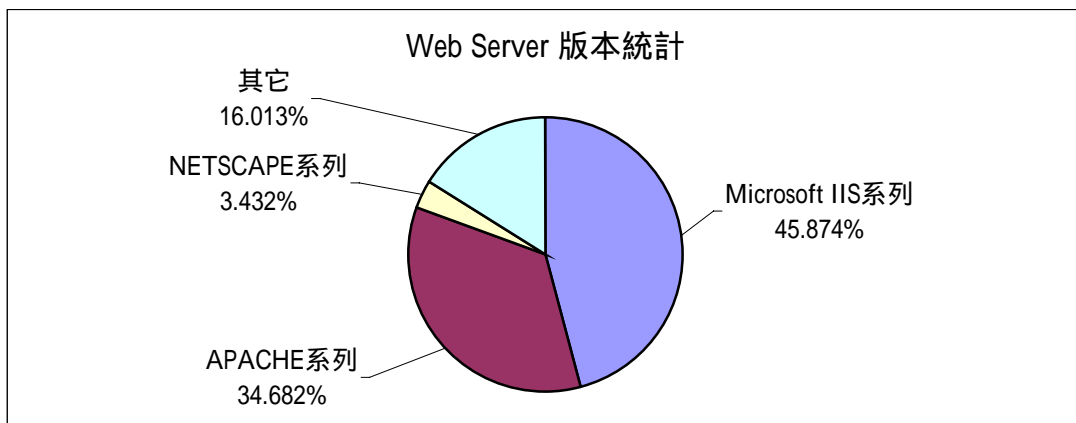


圖 4-2 Web Server 版本統計

表 4-2 Web Server 版本統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft IIS 系列	23,540	45.874%
Apache 系列	17,797	34.682%
Netscape 系列	1,761	3.432%
其他	8,217	16.013%
總數	51,315	100%

表 4-3 Microsoft IIS 分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
6,490	234	1,401	1,595	113	0	4	13,703	23,540
27.57%	0.99%	5.95%	6.78%	0.48%	0%	0.02%	58.21%	100%

表 4-4 Apache 分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
6,827	304	1,363	1,044	201	0	20	8,038	17,797
38.36%	1.71%	7.66%	5.87%	1.13%	0%	0.11%	45.16%	100%

表 4-5 Netscape 分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
106	32	92	75	8	0	0	1,448	1,761
6.02%	1.82%	5.22%	4.26%	0.45%	0%	0%	82.23%	100%

表 4-6 Web Server 版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft IIS 系列	23,540	45.874%
Microsoft-IIS/5.1	705	1.374%
Microsoft-IIS/5.0	15,240	29.699%
Microsoft-IIS/4.0	6,773	13.199%
Microsoft-IIS/3.0 含以下	822	1.602%
Apache 系列	17,797	34.682%
Apache/1.3.x	15,794	30.779%
Apache/1.2.x	1,096	2.136%
Apache/1.1.x 含以下	907	1.768%
Netscape 系列	1,761	3.432%
Netscape-Enterprise	1,201	2.340%
Netscape-FastTrack	547	1.066%
Netscape-Communications	9	0.018%
其他	4	0.008%
其他	8,217	16.013%
Lotus	555	1.082%

	Website	203	0.396%
	NCSA	93	0.181%
	CERN	100	0.195%
	其他	7,266	14.160%
總數		51,315	100%

針對每一版本詳細數量統計表如下所示：

表 4-7 Microsoft IIS 系列版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft-IIS/5.1	705	2.995%
Microsoft-IIS/5.0	15,240	64.741%
Microsoft-IIS/4.0	6,773	28.772%
Microsoft-IIS/3.0 含以下	822	3.492%
總數	23,540	100%

表 4-8 Apache 系列版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Apache/1.3.x	15,794	88.745%
Apache/1.2.x	1,096	6.158%
Apache/1.1.x 含以下	907	5.096%
總數	17,797	100%

表 4-9 Netscape 系列版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Netscape-Enterprise	1,201	68.200%
Netscape-FastTrack	547	31.062%
Netscape-Communications	9	0.511%
其他	4	0.227%
總數	1,761	100%

表 4-10 Web Server 其他版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Lotus	555	6.754%
Website[32]	203	2.470%
NCSA	93	1.132%
CERN	100	1.217%
其他	7,266	88.426%
總數	8,217	100%

結論：

在此次掃描結果中，可以很清楚的了解目前台灣地區使用微軟公司的 IIS 當作 Web Server 比例為最多，其次才是 Apache 伺服器。本研究也根據 netcraft[33]對全球作 Web 調查中可以得知，全球是以使用 Apache 當作伺服器的比例最高，且與微軟公司的伺服器有此消彼漲的微妙關係，請詳見圖 4-3。此發展剛好與台灣地區的走向不盡相同，這與台灣地區大部分的人口都使用微軟公司發展的作業系統有很大的關係。

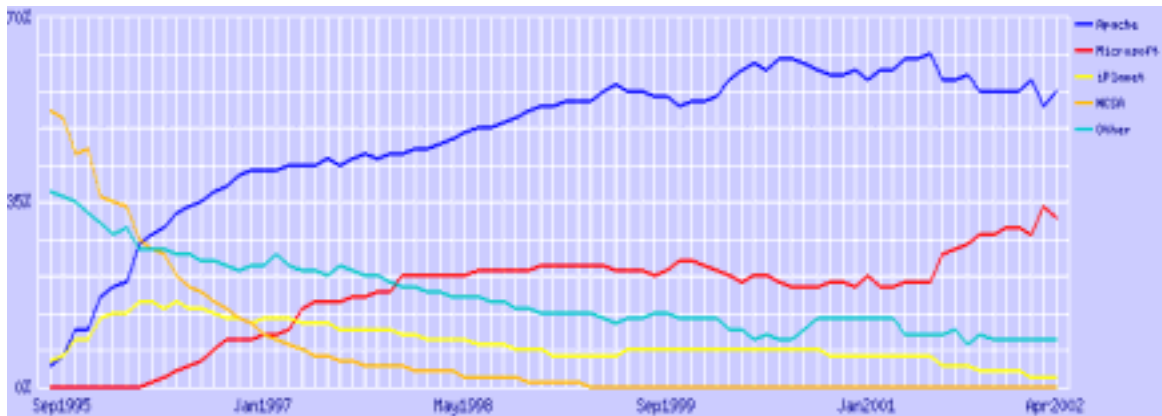


圖 4-3 全球 Web Server 版本統計

資料來源：netcraft (<http://www.netcraft.com/survey/>)

4.3.2 Mail Server 版本數量統計

在 397,580 筆 IP 中共有 43,577 筆 Mail Server，並由圖表得知，台灣地區的 Mail Server 以 Sendmail 為多數，接著才是微軟公司的伺服器，另依照單一版本統計，則以 Microsoft ESMTTP MAIL Service v5.0 系列版本為最多，其次是 Sendmail 8.9.x，第三為 Sendmail 8.11.x。

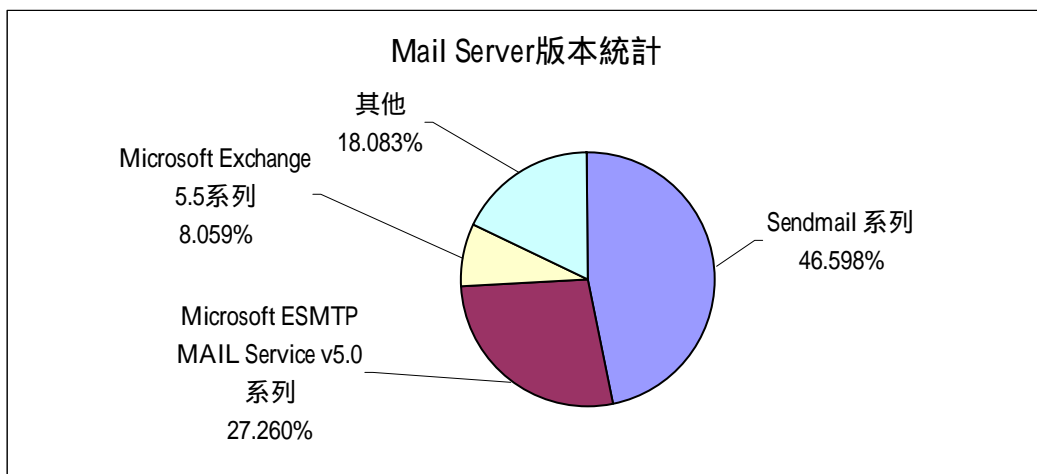


圖 4-4 Mail Server 版本統計

表 4-11 Mail Server 版本細項數量統計表

伺服器名稱	數量(筆)	佔有比率(%)
Sendmail 系列	20,306	46.598%
Microsoft ESMTTP MAIL Service v5.0 系列	11,879	27.260%
Microsoft Exchange v5.5 系列	3,512	8.059%
其他	7,880	18.083%
總數	43,577	100%

表 4-12 Sendmail 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
6,056	115	1,881	988	151	0	22	11,093	20,306
29.824%	0.566%	9.263%	4.866%	0.744%	0%	0.108%	54.629%	100%

表 4-13 Microsoft ESMTP MAIL Service v5.0 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
3,653	66	723	669	107	0	2	6,659	11,879
30.752%	0.556%	6.086%	5.632%	0.901%	0%	0.017%	56.057%	100%

表 4-14 Microsoft Exchange v5.5 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
553	18	113	143	19	0	0	2,666	3,512
15.746%	0.513%	3.218%	4.072%	0.541%	0%	0%	75.911%	100%

針對每一版本詳細數量統計表如下所示：

表 4-15 Mail Server 版本細項統計表

伺服器名稱	數量(筆)	佔有比率(%)
Sendmail 系列	20,306	46.598%
Sendmail 8.12.x	459	1.053%
Sendmail 8.11.x	5,332	12.236%
Sendmail 8.10.x	860	1.974%
Sendmail 8.9.x	11,659	26.755%
Sendmail 8.8.x	1,312	3.011%
Sendmail 8.7.x	24	0.055%
其他	660	1.515%
Microsoft ESMTP MAIL Service v5.0 系列	11,879	27.26%
Microsoft Exchange v5.5 系列	3,512	8.06%
其他	7,880	18.08%
Postfix	808	1.854%
IMail	672	1.542%
MDaemon	376	0.863%
checkPoint FireWall SMTP server	320	0.734%
ArGosoft	233	0.535%
雷電	128	0.294%
WinRoute	30	0.069%

	其他	5,313	12.192%
總數		43,577	100%

表 4-16 Sendmail 系列版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
Sendmail 8.12.x	459	2.260%
Sendmail 8.11.x	5,332	26.258%
Sendmail 8.10.x	860	4.235%
Sendmail 8.9.x	11,659	57.417%
Sendmail 8.8.x	1,312	6.461%
Sendmail 8.7.x	24	0.118%
其他	660	3.250%
總數	20,306	100%

表 4-17 Mail Server 其他版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
Postfix	808	10.254%
IMail	672	8.528%
MDaemon	376	4.772%
checkPoint FireWall SMTP server	320	4.061%
ArGosoft	233	2.957%
雷電	128	1.624%
WinRoute	30	0.381%
其他	5,313	67.424%
總數	7,880	100%

結論：

在此次掃描結果中，可以了解目前仍然以 Sendmail 佔最多比例，遠遠超過其他版本數量，這與 Sendmail 取得容易有相當大的關係(RedHat 和 FreeBSD 等 UNIX-like 系統預設就會安裝 Sendmail 伺服器)。另外在其他項目方面，也有多種好用的 Mail Server，如 Postfix、Mdaemon 等 Mail Server 軟體。

4.3.3 FTP Server 版本數量統計

在 397,580 筆 IP 中共有 49,058 筆 FTP Server，並由圖表得知，台灣地區的 FTP Server 以微軟公司的 IIS 為多數，接著是 Serv-U[34]和 Wu-FTP[35]。另依照單一版本統計，則以 Microsoft-FTP/5.0 為最多，其次是 Serv-U 2.x，第三為 Wu-FTP 2.6。

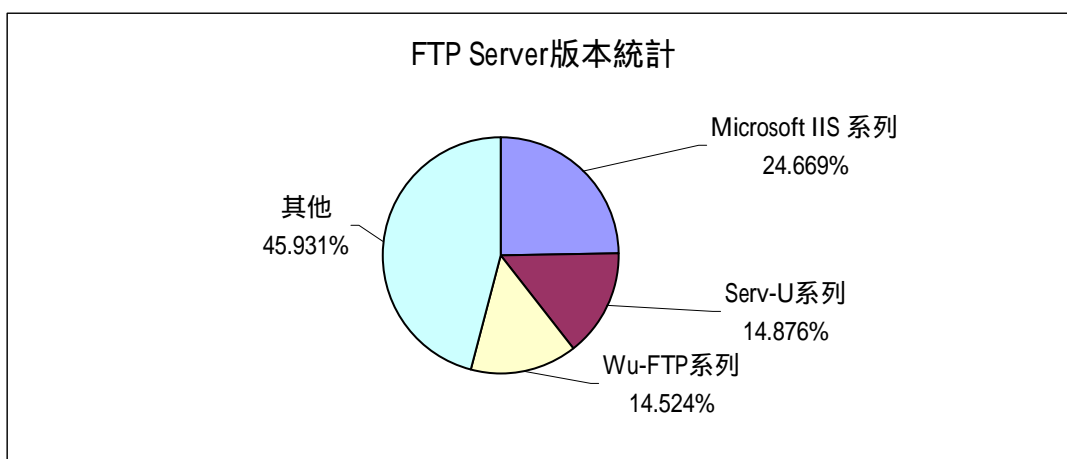


圖 4-5 FTP Server 版本統計

表 4-18 FTP Server 版本統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft IIS 系列	12,102	24.669%
Serv-U 系列	7,298	14.876%
Wu-FTP 系列	7,125	14.524%
其他	22,533	45.931%
總數	49,058	100%

表 4-19 Microsoft IIS 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
3,695	72	565	739	63	0	2	6,966	12,102
30.532%	0.595%	4.669%	6.106%	0.521%	0%	0.017%	57.561%	100%

表 4-20 Serv-U 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
3,703	25	125	239	12	0	1	3,193	7,298
50.740%	0.343%	1.713%	3.275%	0.164%	0%	0.014%	43.752%	100%

表 4-21 Wu-FTP 系列分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
2,383	33	792	427	44	0	8	3,438	7,125
33.446%	0.463%	11.116%	5.993%	0.618%	0%	0.112%	48.253%	100%

針對每一版本詳細數量統計表如下所示：

表 4-22 FTP Server 版本細項統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft IIS 系列	12,102	24.669%
Microsoft-FTP/5.1	1	0.002%
Microsoft-FTP/5.0	7,209	14.695%
Microsoft-FTP/4.0	3,179	6.480%
Microsoft-FTP/3.0	974	1.985%
Microsoft-FTP/2.0	176	0.359%
Microsoft-FTP/1.0	14	0.029%
其他	549	1.119%
Serv-U 系列	7,298	14.876%
Serv-U 3.x	671	1.368%
Serv-U 2.x	6,257	12.754%
其它	370	0.754%
Wu-FTP 系列	7,125	14.524%
wu-FTP 2.6	5,407	11.022%
wu-FTP 2.5	343	0.699%
wu-FTP 2.4	1,373	2.799%
其它	2	0.004%
其他	22,533	45.931%
SunOS FTP Server	3,534	7.204%

	ProFTPD	2,106	4.293%
	HP JetDirect FTP Service	1,269	2.587%
	Check Point FireWall-1 Secure FTP server	461	0.940%
	OmniStack FTP server ready	466	0.950%
	G6 FTP	177	0.361%
	CesarFTP	106	0.216%
	其它	14,414	29.382%
總數		49,058	100%

表 4-23 Microsoft IIS 系列版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
Microsoft-FTP/5.1	1	0.008%
Microsoft-FTP/5.0	7,209	59.569%
Microsoft-FTP/4.0	3,179	26.268%
Microsoft-FTP/3.0	974	8.048%
Microsoft-FTP/2.0	176	1.454%
Microsoft-FTP/1.0	14	0.116%
其他	549	4.536%
總數	12,102	100%

表 4-24 Serv-U 系列版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
Serv-U 3.x	671	9.194%
Serv-U 2.x	6,257	85.736%
其它	370	5.070%
總數	7,298	100%

表 4-25 Wu-FTP 系列版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
wu-FTP 2.6	5,407	75.888%
wu-FTP 2.5	343	4.814%
wu-FTP 2.4	1,373	19.270%
其它	2	0.028%
總數	7,125	100%

表 4-26 FTP Server 其他版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
SunOS FTP Server	3,534	15.684%
ProFTPD	2,106	9.346%
HP JetDirect FTP Service	1,269	5.632%
Check Point FireWall-1 Secure FTP server	461	2.046%
OmniStack FTP server ready	466	2.068%
G6 FTP	177	0.786%
CesarFTP	106	0.470%
其它	14,414	63.968%
總數	22,533	100%

結論：

在此次掃描結果中，可以發現 FTP Server 版本不是獨佔的場面，且多種相關軟體發展的十分迅速。以 Serv-U 伺服器來說，由於該軟體取得容易以及設定方式簡單，並且能夠架設在任一 Windows 平台上的 Third Party FTP 架站軟體，所以成為多數人架站的選擇。

4.3.4 SSL 數量統計

在 Web Server 總數 51,315 筆中，發現有開放 SSL 連線的主機數目為 22,114 筆，約佔全部 Web Server 數的 43.095%。表 4-17 為分布表。

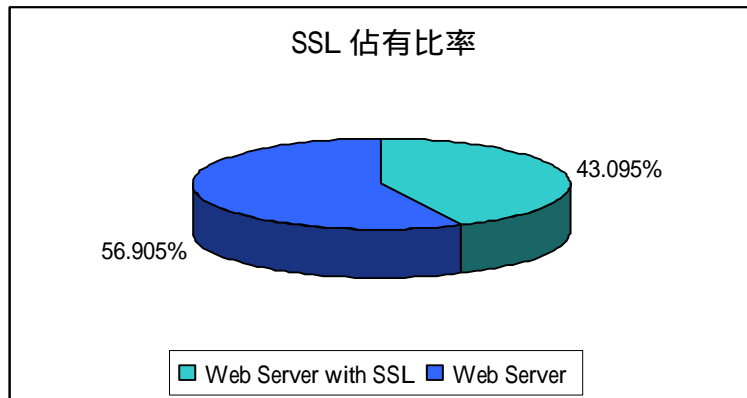


圖 4-6 SSL 佔有比率統計

表 4-27 SSL 分布表

EDU	GOV	COM	NET	ORG	MIL	IDV	其他	總數
8,128	166	1,115	1,436	103	0	7	11,159	22,114
36.755%	0.751%	5.042%	6.494%	0.466%	0%	0.032%	50.461%	100%

結論：

在此次掃描結果中，可以發現 Web Server 的主機中有 43.095% 皆有開啟 SSL 功能，這個數據了解大部分的站台尚未重視用戶認證與資料傳輸的安全性。因此應該多宣導相關觀念，政府也可訂立相關法規，讓使用者了解資料的正確性和隱密性必須架構在安全的傳輸環境之中。

4.3.5 DNS 數量統計

在 397,580 筆 IP 中共有 11,053 筆 DNS Server，並由圖表得知，台灣地區的 DNS Server 以 BIND 8.2.3 為最多，其次是 BIND 8.1.2。

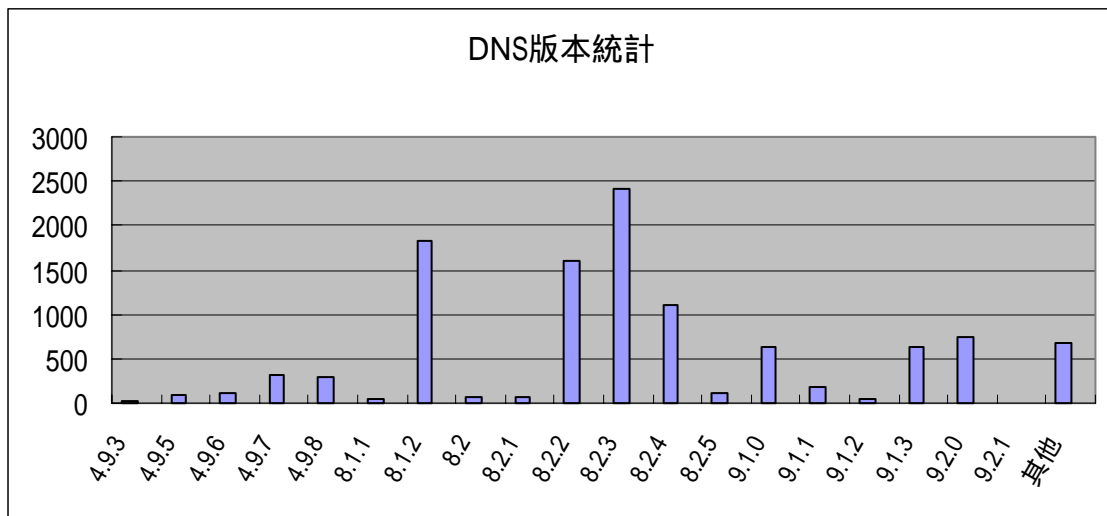


圖 4-7 DNS 版本統計

表 4-28 DNS 版本分類統計表

BIND 版本	數量(筆)	佔有比率(%)
4.9.3	32	0.290%
4.9.5	97	0.878%
4.9.6	120	1.086%
4.9.7	319	2.886%
4.9.8	286	2.588%
8.1.1	53	0.480%
8.1.2	1,835	16.602%
8.2	71	0.642%
8.2.1	73	0.660%
8.2.2	1,608	14.548%
8.2.3	2,409	21.795%

8.2.4	1,116	10.097%
8.2.5	124	1.122%
9.1.0	629	5.691%
9.1.1	175	1.583%
9.1.2	56	0.507%
9.1.3	621	5.618%
9.2.0	752	6.804%
9.2.1	4	0.036%
其他	673	6.089%
總數	11,053	100%

結論：

在此次掃描中，可以清楚的了解目前 BIND8.2.3 還是最多人使用，縱使版本已經更新到 9.2.1，但 BIND8.2.3 仍然是最穩定的版本，因此多數人還是會選擇此一版本。

4.3.6 作業系統版本版本數量統計

在 397,580 筆 IP 中共有 317,113 筆資料, 並由圖表得知, 台灣地區使用 Windows Base 的使用者佔大多數, 其次才是 Unix Base。另依照單一版本統計, 則以 Windows 98/98SE 為最多, 其次為 Windows 2000 SP1, SP2/Windows XP。

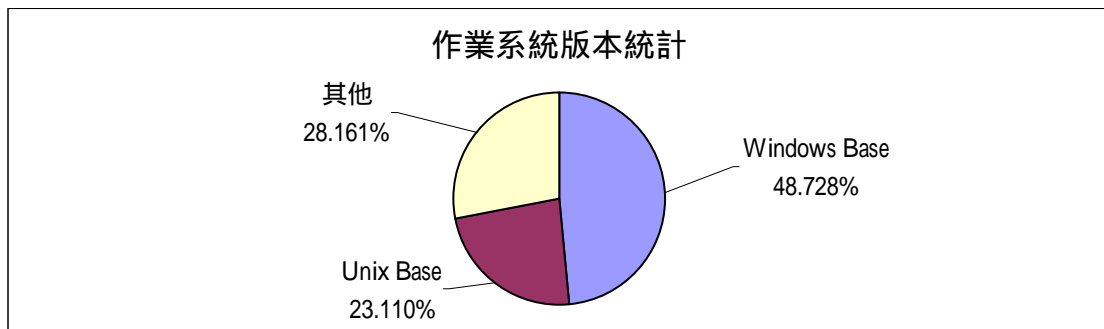


圖 4-8 作業系統版本統計

表 4-29 作業系統版本分類統計表

伺服器名稱	數量(筆)	佔有比率(%)
Windows Base	154,524	48.728%
Unix Base	73,286	23.110%
其他	89,303	28.161%
總數	317,113	100%

表 4-30 作業系統版本細項統計表

分類	名稱	數量(筆)	佔有比率(%)
Windows Base		154,524	48.728%
	Windows 98/98SE	80,052	25.244%
	Windows 2000 SP1, SP2/Windows XP	58,096	18.320%
	Windows ME	5,995	1.890%
	Windows NT SP4+	4,855	1.531%
	Windows 95	2,825	0.891%

	Windows NT SP3-	2,701	0.852%
Unix Base		73,286	23.110%
	Ultrix HPUX 10.20	13,247	4.177%
	Linux 2.2.x/2.4.5+ kernel	10,797	3.405%
	OpenBSD 2.4-2.5 NetBSD 1.5, 1.4.1, 1.4	10,104	3.186%
	Sun Solaris 2.3-2.8	7,749	2.444%
	Novell (FreeBSD 4.3-current)	7,484	2.360%
	Unknown Unix (Accuracy dropped)	6,093	1.921%
	NetBSD	4,760	1.501%
	Linux 2.4.x kernel	3,262	1.029%
	FreeBSD 2.2.x - 4.1	2,723	0.859%
	HPUX 10.x	2,310	0.728%
	AIX	1,238	0.390%
	Linux kernel 2.0.x	920	0.290%
	Little endian BSDI/NetBSD 1.1.x-1.2.x MacOS X 1.0-1.2	765	0.241%
	Linux kernel 2.2.x 2.4.x	651	0.205%
	HP-UX 11.x MacOS 7.x-9.x	512	0.161%
	DGUX/Compaq Tru64	417	0.131%
	ULTRIX	116	0.037%
	SunOS4.x	69	0.022%
	OpenBSD 2.1-2.3	50	0.016%
	OpenBSD 2.6-2.9	19	0.006%
其他		89,303	28.161%
	NFR IDS Appliance	37,119	11.705%
	Windows Based. Open/Net/FreeBSD/DG-UX/HP-UX 10.x etc	25,862	8.155%
	Cisco IOS 11.x-12.x	18,811	5.932%

	IBM OS/390	3,144	0.991%
	Router and Others	2,287	0.721%
	Extreme Networks switch Network Systems Router NS6114 (NSC 6600 Series)	986	0.311%
	Extreme Network Switches.	734	0.231%
	OpenVMS with Process Software TCPWare	329	0.104%
	OpenVMS with Digital TCP Services	21	0.007%
	Apollo Domain/OS SR 10.4 NFR IDS Appliance	10	0.003%
總數		317,113	100%

結論：

在此次掃描結果中，可以發現在台灣地區將近一半的使用者都使用微軟公司發展的作業系統，而 Unix Base 只佔了五分之一強，此項數據了解台灣地區使用者仍然以圖形介面的作業系統為主，但近年來 Unix Base 作業系統也逐漸朝這一方面改進，因此未來這數據的趨勢值得注意。

Windows Base 細項統計

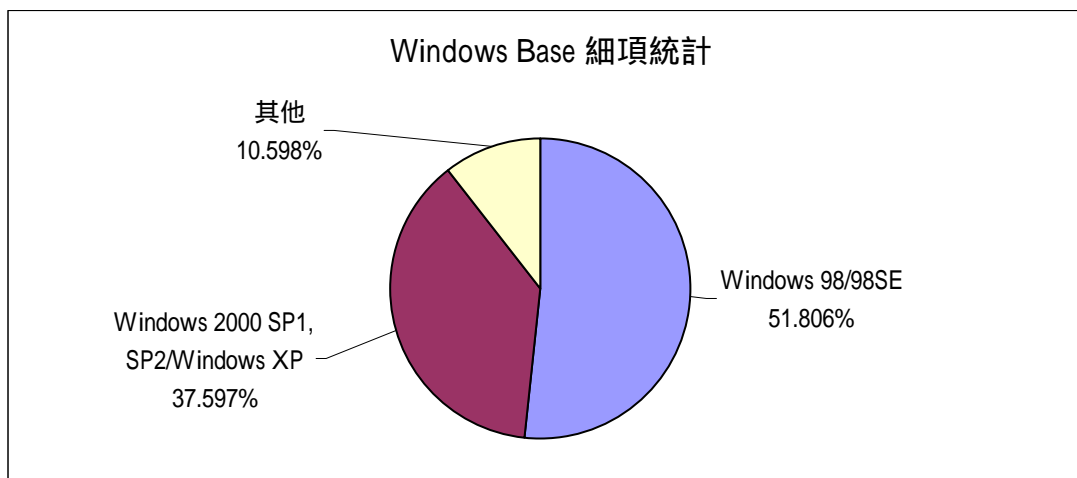


圖 4-9 Windows Base 細項版本統計

表 4-31 Windows Base 分類統計表

作業系統名稱	數量(筆)	佔有比率(%)
Windows 98/98SE	80,052	51.806%
Windows 2000 SP1, SP2/Windows XP	58,096	37.597%
其他	16,376	10.598%
總數	154,524	100%

表 4-32 Windows Base 細項統計表

作業系統名稱	數量(筆)	佔有比率(%)
Windows 98/98SE	80,052	51.806%
Windows 2000 SP1, SP2/Windows XP	58,096	37.597%
其他	16,376	10.598%
Windows ME	5,995	3.880%
Windows NT SP4+	4,855	3.142%
Windows 95	2,825	1.828%
Windows NT SP3-	2,701	1.748%
總數	154,524	100%

UNIX Base 細項統計

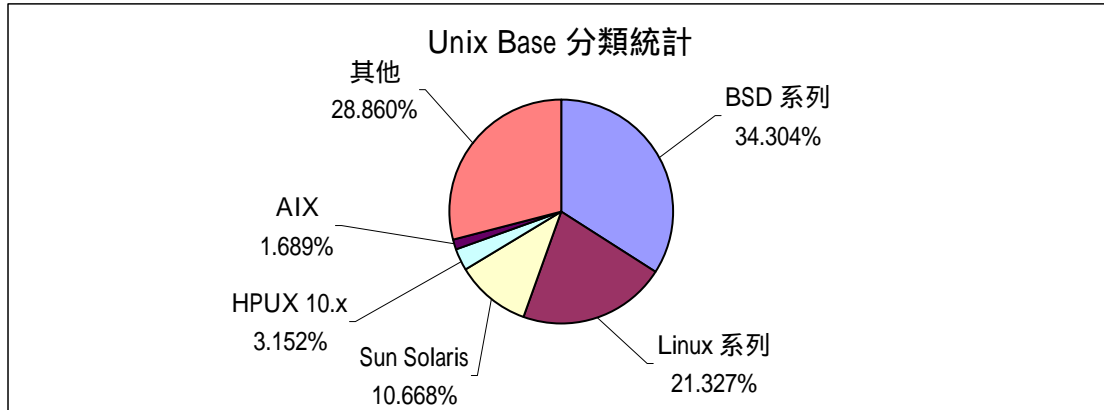


圖 4-10 UNIX Base 細項版本統計

表 4-33 UNIX Base 分類統計表

作業系統名稱	數量(筆)	佔有比率(%)
BSD 系列	25,140	34.304%
Linux 系列	15,630	21.327%
Sun Solaris	7,818	10.668%
HPUX 10.x	2,310	3.152%
AIX	1,238	1.689%
其他	21,150	28.860%
總數	73,286	100%

表 4-34 UNIX Base 細項統計表

作業系統名稱	數量(筆)	佔有比率(%)
BSD 系列	25,140	34.304%
OpenBSD 2.4-2.5 NetBSD 1.5, 1.4.1, 1.4	10,104	13.787%
Novell (FreeBSD 4.3-current)	7,484	10.212%
NetBSD	4,760	6.495%
FreeBSD 2.2.x - 4.1	2,723	3.716%
OpenBSD 2.1-2.3	50	0.068%
OpenBSD 2.6-2.9	19	0.026%

Linux 系列		15,630	21.327%
	Linux 2.2.x/2.4.5+ kernel	10,797	14.733%
	Linux 2.4.x kernel	3,262	4.451%
	Linux kernel 2.0.x	920	1.255%
	Linux kernel 2.2.x 2.4.x	651	0.888%
Sun Solaris		7,818	10.668%
	Sun Solaris 2.3-2.8	7,749	10.574%
	SunOS4.x	69	0.094%
HPUX 10.x		2,310	3.152%
AIX		1,238	1.689%
其他		21,150	28.860%
	Ultrix HPUX 10.20	13,247	18.076%
	Little endian BSDI/NetBSD 1.1.x-1.2.x MacOS X 1.0-1.2	765	1.044%
	HP-UX 11.x MacOS 7.x-9.x	512	0.699%
	DGUX/Compaq Tru64	417	0.569%
	ULTRIX	116	0.158%
總數		73,286	100%

針對其他版本細項統計表如下所示：

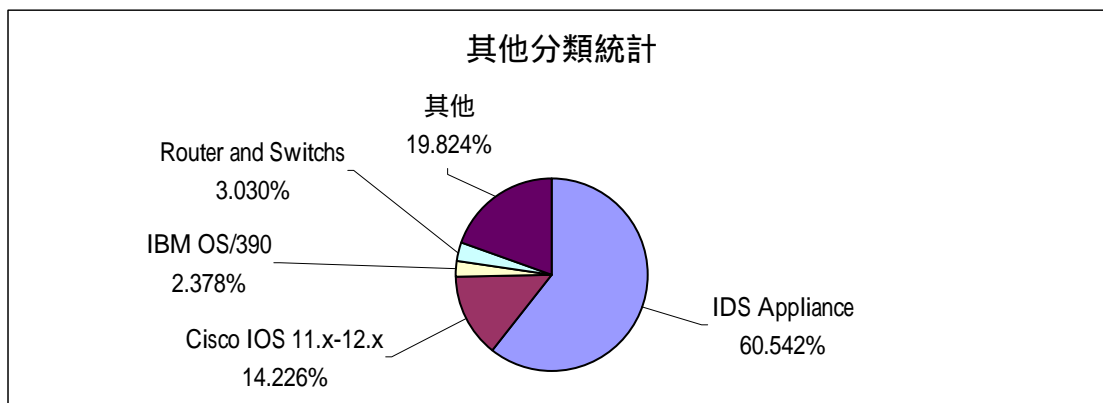


圖 4-11 作業系統其他細項版本統計

表 4-35 作業系統其他分類統計表

作業系統名稱	數量(筆)	佔有比率(%)
IDS Appliance	80,052	41.576%
Cisco IOS 11.x-12.x	18,811	21.064%
IBM OS/390	3,144	3.521%
Router and Switch	4,007	4.487%
其他	26,212	29.352%
總數	89,303	100%

表 4-36 作業系統其他細項統計表

作業系統名稱	數量	佔有比率(%)
IDS Appliance	80,052	41.576%
NFR IDS Appliance	37,119	41.565%
Apollo Domain/OS SR 10.4 NFR IDS Appliance	10	0.011%
Cisco IOS 11.x-12.x	18,811	21.064%
IBM OS/390	3,144	3.521%
Router and Switch	4,007	4.487%
Router and Others	2,287	2.561%

	Extreme Networks switch Network Systems Router NS6114 (NSC 6600 Series)	986	1.104%
	Extreme Network Switches.	734	0.822%
	其他	26,212	29.352%
	Windows Based. Open/Net/FreeBSD/DG-UX/HP-UX 10.x etc	25,862	28.960%
	OpenVMS with Process Software TCPWare	329	0.368%
	OpenVMS with Digital TCP Services	21	0.024%
總數		89,303	100%

結論：

綜觀上述 Windows Base 細項統計、UNIX Base 細項統計以及其他版本細項統計可以發現，以單一版本數量來比較，台灣地區使用 Windows 98/98SE 作為作業系統佔多數，其次是 Windows 2000/XP，接著才是 UNIX Base 系統。由於 Windows 98/98SE 的安裝容易，相容性高，因此多數人仍舊選用 Windows 98/98SE 作為系統；此外，在 UNIX Base 上由於系統核心眾多，但仍可規劃出相同分類，在這些分類中，則以使用 BSD 佔大多數。

4.4 安全性評估

4.4.1 Web Server 安全性評估

表 4-37 Web Server 整體安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Microsoft IIS 系列	23,540(53.440%)	67(52.344%)	27.973%
Apache 系列	17,797(40.403%)	29(22.656%)	9.154%
Netscape 系列	1,761(3.998%)	15(11.719%)	0.468%
Lotus Domino	555(1.260%)	4(3.125%)	0.039%
Web Site/Pro	203(0.461%)	7(5.469%)	0.025%
NCSA	93(0.211%)	5(3.906%)	0.008%
CERN	100(0.227%)	1(0.781%)	0.002%
總計(不含其他)	44,049	128	37.669%

說明：

以 IIS 而言，想要發現有弱點的機率約為 27.973%，則代表一百部裡面約有 28 部有 IIS 的弱點。而想找到有任意弱點的伺服器機率約為 37.669%，這表示一百部裡面有將近 38 部伺服器是有弱點。

表 4-38 Microsoft IIS 系列安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Microsoft-IIS/5.1	705(2.995%)	0(0%)	0%
Microsoft IIS/5.0	15,240(64.741%)	20(29.851%)	19.326%
Microsoft IIS 4.0	6,773(28.772%)	38(56.716%)	16.319%
Microsoft IIS 3.0 含以下	822(3.492%)	9(13.433%)	0.469%
總計	23,540	67	36.113%

說明：

此表格可以得之，Microsoft IIS/5.0 的整體弱點比為 19.326%，此數據代表在

未經修補任何弱點的 IIS/5.0 中，有 20%左右的機率是有弱點，也就是說有 20%的機會會造成伺服器溢位、被入侵以及感染病毒。另外，IIS/5.1 是目前 Microsoft 推出的 XP 作業系統中所搭載的伺服器，由於版本較新，尚未有弱點發生。

表 4-39 Apache 系列安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Apache/1.3.x	15,794(88.745%)	13(44.828%)	39.782%
Apache/1.2.x	1,096(6.158%)	2(6.897%)	0.425%
Apache/1.1.x 含以下	907(5.096)	14(48.276%)	2.460%
總計	17,797	29	42.667%

說明：

此表格可以得之，Apache/1.3.x 的整體弱點比為 39.782%，由於此 Apache/1.3.x 是集合了 Apache/1.3 各版本的集合，因此整體弱點比比 Microsoft IIS/5.0 的整體弱點比還要來得高。另外，如果以單項數據來檢視(如表 4-40)，可以發現 Apache/1.3.x 的弱點比 Microsoft IIS/5.0 的弱點比少。

表 4-40 IIS/5.0 和 Apache/1.3.x 安全性評估比較

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Microsoft IIS/5.0	15,240(49.107%)	20(60.606%)	29.762%
Apache/1.3.x	15,794(50.893%)	13(39.394%)	20.049%
總計	31,034	33	

結論與建議：

近年來，許多網蟲或病毒皆針對 IIS 的弱點進行攻擊，因此使用者和管理者應該隨時注意微軟安全通報[36]或 CERT 安全通報[37][38]的發佈，並定期利用安全掃描工具如 Nessus 等做檢測，以利取得最安全狀態。

4.4.2 Mail Server 安全性評估

表 4-41 Mail Server 安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Sendmail 系列	20,306(85.255%)	26(70.270%)	59.909%
Microsoft Exchange SMTP Server v5.5 系列	3,512(14.745%)	11(29.730%)	4.384%
總計(不含其他)	23,818	37	55.423%

表 4-42 Sendmail 系列安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Sendmail 8.12.x	459(2.260%)	6(23.077%)	0.522%
Sendmail 8.11.x	5,332(26.258%)	0(0%)	0.000%
Sendmail 8.10.x	860(4.235%)	3(11.538%)	0.489%
Sendmail 8.9.x	11,659(57.417%)	3(11.538%)	6.625%
Sendmail 8.8.x	1,312(6.461%)	7(26.923%)	1.740%
Sendmail 8.7.x	24(0.118%)	2(7.692%)	0.009%
其他	660(3.250%)	5(19.231%)	0.625%
總計(不含其他)	20,306	26	10.009%

結論與建議：

由此表格可以得知，Sendmail 雖然使用率相當的高，但其弱點數量也為數不少，而相關的弱點不僅可能造成 Mail Relay，也有可能被利用來取得權限，因此 Sendmail 的使用者或管理者必須確認該服務版本為最新或者已經完成漏洞修正工作。

4.4.3 FTP Server 安全性評估

表 4-43 FTP Server 安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Microsoft IIS 系列	12,102(38.630%)	4(19.048%)	7.358%
Serv-U 系列	7,298(23.295%)	6(28.571%)	6.656%
Wu-FTP 系列	7,125(22.743%)	4(19.048%)	4.332%
SunOS FTP server	3,534(11.281%)	1(4.762%)	0.537%
JD FTP server	1,269(4.051%)	6(28.571%)	1.157%
總計(不含其他)	31,328	21	20.040%

結論與建議：

由此表格可以得知，目前以 Serv-U 和 JD FTP server 的弱點比例為最高，而 Microsoft IIS 和 Wu-FTP 次之。因此使用上列軟體的使用者或管理者必須確認該服務版本為最新或者已經完成漏洞修正工作。

4.4.4 DNS 安全性評估

表 4-44 DNS 安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
BIND 9.x	2237(21.551%)	1(4.545%)	0.980%
BIND 8.x	7289(70.222%)	15(68.182%)	47.878%
BIND 4.x	854(8.227%)	6(27.273%)	2.244%
總計(不含其他)	10380	22	51.10%

結論與建議：

由此表格可以得知，BIND 8.x 系列的弱點非常多，以達 68.182%。而此類弱點可以被用來癱瘓伺服器的服務(Denial of Service)、欺騙(Spoofing)甚至是 BIND 本身也有的弱點問題(圖 4-12 所示)。因此 ISC 強烈建議使用者或管理者升級到最新版本。

Summary												
The following table summarizes the vulnerability to the bugs mentioned for all versions of BIND distributed by ISC. Upgrading to BIND version 8.3.1 or higher is strongly recommended for all users of BIND.												
version	zxf	sigdiv0	svr	noxt	sig	naptr	maxdname	solinger	fdmax	complain	infoleak	tsig
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	-	+	+	+	+	+	+	+	+	-	+	+
8.2.2	+	+	+	-	-	+	+	-	-	-	+	+
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	-	-	-	-	-	-	-	-	-	-	-	-
8.3.0	-	-	-	-	-	-	-	-	-	-	-	-
8.3.1	-	-	-	-	-	-	-	-	-	-	-	-
9.0.0	-	-	-	-	-	-	-	-	-	-	-	-
9.0.1	-	-	-	-	-	-	-	-	-	-	-	-
9.1.0	-	-	-	-	-	-	-	-	-	-	-	-
9.1.1	-	-	-	-	-	-	-	-	-	-	-	-
9.1.2	-	-	-	-	-	-	-	-	-	-	-	-
9.1.3	-	-	-	-	-	-	-	-	-	-	-	-
9.2.0	-	-	-	-	-	-	-	-	-	-	-	-
9.2.1	-	-	-	-	-	-	-	-	-	-	-	-

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

圖 4-12 BIND Bug

資料來源：ISC (<http://www.isc.org/products/BIND/bind-security.html>)

4.4.5 作業系統安全性評估

表 4-45 作業系統安全性評估

伺服器版本	佔有數量(A)	弱點數量(B)	整體弱點(A*B)
Windows Base	154,524(67.830%)	107(36.271%)	24.60282%
Windows 98/98SE	80,052(35.140%)	16(5.4237%)	1.9061%

	Windows 2000 SP1, SP2/Windows XP	58,096(25.502%)	41(13.8983%)	3.5443%
	Windows ME	5,995(2.632%)	12(4.0678%)	0.1078%
	Windows NT SP4+	4,855(2.131%)	9(3.0508%)	0.0658%
	Windows 95	2,825(1.240%)	19(6.4407%)	0.0801%
	Windows NT SP3-	2,701(1.186%)	10(3.3898%)	0.0403%
	Unix Base	73,286(32.170%)	188(63.729%)	20.50143%
	Ultrix HPUX 10.20	13,247(5.8149%)	3(1.0169%)	0.05913%
	Linux 2.2.x/2.4.5+ kernel	10,797(4.7395%)	4(1.3559%)	0.06426%
	OpenBSD 2.4-2.5 NetBSD 1.5, 1.4.1, 1.4	10,104(4.4353%)	11(3.7288%)	0.16538%
	Sun Solaris 2.3-2.8	7,749(3.4015%)	15(5.0847%)	0.17296%
	Novell (FreeBSD 4.3-current)	7,484(3.2852%)	3(1.0169%)	0.03341%
	Unknown Unix (Accuracy dropped)	6,093(2.6746%)	22(7.4576%)	0.19946%
	NetBSD	4,760(2.0895%)	20(6.7797%)	0.14166%
	Linux 2.4.x kernel	3,262(1.4319%)	4(1.3559%)	0.01942%
	FreeBSD 2.2.x - 4.1	2,723(1.1953%)	19(6.4407%)	0.07699%
	HPUX 10.x	2,310(1.0140%)	21(7.1186%)	0.07218%
	AIX	1,238(0.5434%)	24(8.1356%)	0.04421%
	Linux kernel 2.0.x	920(0.4038%)	3(1.0169%)	0.00411%
	Little endian BSDI/NetBSD 1.1.x-1.2.x MacOS X 1.0-1.2	765(0.3358%)		
	Linux kernel 2.2.x 2.4.x	651(0.2858%)	10(3.3898%)	0.00969%
	HP-UX 11.x MacOS 7.x-9.x	512(0.2247%)	10(3.3898%)	0.00762%

	DGUX/Compaq Tru64	417(0.1830%)		
	ULTRIX	116(0.0509%)	4(1.3559%)	0.00069%
	SunOS4.x	69(0.0303%)		
	OpenBSD 2.1-2.3	50(0.0219%)	7(2.3729%)	0.00052%
	OpenBSD 2.6-2.9	19(0.0083%)	8(2.7119%)	0.00023%
	總計(不含其他)	227,810	295	45.10425%

結論與建議：

由此表格可以得知，目前以 Unix Base 和 Windows Base 的弱點比十分接近，因此建議這些作業系統版本的使用者或管理者能夠隨時注意相關廠商所發行的安全通報，掌握最新資訊，勤於修補漏洞，以降低風險。

第五章 結論與未來研究方向

5.1 研究成果與貢獻

本研究主要是開發一大規模網路安全掃描系統，並針對台灣網域進行安全檢測。此系統能夠迅速蒐集網路節點相關資訊，以便了解目前網路伺服器種類概況與其安全性。本研究成果如下：

1. 蒐集到網路伺服器及作業系統版本的佔有率，此一資訊除了讓使用者了解網路發展現況外，更可以經由定期資料收集，提供決策者預估未來網路發展趨勢。
2. 蒐集相關網路服務及作業系統弱點並比對網路節點資訊，可以快速評估網域安全性，提供改善網路安全之策略和方法。
3. 本系統以 C 與 PERL 進行開發，因此適用於不同作業系統平台，在移轉過程中不會因為作業系統不同而喪失其功能，並且能夠輕易的讓使用者根據需求新增或改變掃描項目。

本系統的特點如下：

1. 系統透過亂數掃描方式進行資料收集，減少被誤認入侵的機率。
2. 系統能自動分析統計收集到的資訊，大量降低人力和時間成本，並自動產生清晰明瞭的圖表。
3. 快速評估網域伺服器的安全性及整體弱點比。

5.2 結論與建議

本研究在執行台灣網域的大規模安全檢查過程中，同時進行相關的系統防護和設定研究，提出下列幾項增進網路安全的建議：

1. 加強加密通訊的機制，在伺服器端建構加密系統，並加強 client 端的使用加密方式進行連線作業。
2. 減少同一伺服器上的網路服務項目，以避免不必要的風險。
3. 建立良好使用者習慣，並對人員加強網路安全觀念和本職學能訓練。
4. 建立防火牆機制，做好系統規劃及設定適當的規則來控管網路資訊的存取。
5. 建立嚴謹的稽核原則，利用稽核工具來監控網路活動，定期做檢視以及早發現問題，並做相關防範或補救措施。
6. 隨時注意各系統廠商發布的安全通報，以便取得最新的更新程式，補正系統弱點，保障系統安全。
7. 針對伺服器提供網路服務的版本資訊嘗試隱藏或更改，讓入侵者無法猜測伺服器提供網路服務的版本資訊，或是讓其造成誤判，以減低被入侵的風險。

5.3 未來研究方向

系統缺陷不斷的被發現，入侵的手法千奇百怪且數量驚人，為了維護系統的安全性，知己知彼是非常重要的工作。本系統以防護的觀點可以達到知己的要求，站在攻擊的立場可達知彼的目標。因此本研究未來還可加入不同的掃描方式或收集不同的網路服務資訊，以持續提昇系統功能，分別敘述如下：

1. 針對弱點資料庫的建置，提供自動化收集、儲存網路服務弱點的功能，並提出更便利的修補方式及明確的風險程度分類，以增進網域安全性評估的準確性及網路安全改善的效率。

2. 未來可以將系統的設計朝 plug-in 方向作研究，進行模組化設計，以提升系統的可擴充性，改善系統使用效率和方便性。
3. 針對使用者的習慣和服務的設定方式進行調查和研究，將來也可藉此研究開發類似的系統。
4. 針對本系統的掃描方式進行檢討和修正，使系統的運作更加隱密。
5. 可根據本系統建置的網路節點資訊資料庫結合事件通報系統，當有重大安全弱點發佈時，及時主動提出警告，以避免發生嚴重的損害。

參考文獻

- [1]. MySQL, <http://www.mysql.com>
- [2]. Common Vulnerabilities and Exposures, CVE, <http://www.cve.mitre.org>
- [3]. 陳宗裕, “支援弱點稽核與入侵偵測之整合性後端資料庫設計研究”, 中原資工所碩士論文, 2001.
- [4]. 林秉忠, “網路環境下之系統安全評估”, 中山資管所碩士論文, 1998.
- [5]. Internet Assigned Numbers Authority, <http://www.iana.org>
- [6]. Port Numbers, <http://www.iana.org/assignments/port-numbers>
- [7]. World Wide Web Consortium, <http://www.w3.org>
- [8]. The Apache Software Foundation, <http://www.apache.org>
- [9]. PostFix, <http://www.postfix.com>
- [10]. Linux Mandrake, <http://www.mandrakelinux.com>
- [11]. ProFTPD Project, <http://www.proftpd.org>
- [12]. Internet Software Consortium, <http://www.isc.org/products/BIND>
- [13]. Sys-Security Group, <http://www.sys-security.com>
- [14]. Ofir Arkin, “ICMP Usage in Scanning - The Complete Know-How”, The Sys-Security Group, June, 2001. <http://www.sys-security.com>
- [15]. Ofir Arkin, Fyodor Yarochkin, “X remote ICMP based OS fingerprinting techniques”, August, 2001. <http://www.sys-security.com>
- [16]. f0bic, “Examining Advanced Remote OS Detection Methods/Concepts using Perl”, Feb, 2001. <http://www.low-level.net>

- [17]. Fyodor, “Remote OS detection via TCP/IP Stack FingerPrinting”, October 1998.
<http://www.insecure.org/nmap/nmap-fingerprinting-article.txt>
- [18]. Lance Spitzner, “IDing remote hosts, without them knowing”, May, 2000.
<http://packetstorm.decepticons.org/papers/IDS/fingerprinting.txt>
- [19]. Lance Spitzner, “Know Your Enemy - The Tools and Methodologies of the Script Kiddie”, July, 2000. <http://project.honeynet.org/papers/enemy>
- [20]. Lance Spitzner, “Know Your Enemy: II - Tracking the blackhat's moves”, June, 2001. <http://project.honeynet.org/papers/enemy2>
- [21]. Lance Spitzner, “Know Your Enemy: Passive Fingerprinting”, March, 2002.
<http://project.honeynet.org/papers/finger>
- [22]. Wayne Huang, Shih-Kuh Huang, “A Survey and Assessment of Network Mapping Methods and Techniques”, Journal of Computer, 2001.
- [23]. FreeBSD, <http://www.freebsd.org>
- [24]. Solaris, <http://www.sun.com>
- [25]. Microsoft Corporation, <http://www.microsoft.com>
- [26]. Cisco, <http://www.cisco.com>
- [27]. Red Hat Linux, <http://www.red-hat.com>
- [28]. Sendmail, <http://www.sendmail.org>
- [29]. Security Focus, <http://www.securityfocus.com>
- [30]. 李長樹, 台灣區網際網路位址(IP Address)範圍,
<http://www.edu.tw/tanet/bulletin/ip.txt>
- [31]. Netscape.com, <http://www.netscape.com>
- [32]. WebSite – Dynamic Web Server, <http://website.deerfield.com>

- [33]. Netcraft, <http://www.netcraft.com>
- [34]. Rhino Soft, <http://www.serv-u.com>
- [35]. WU-FTPD Development Group, <http://www.wu-ftp.org>
- [36]. Microsoft Security Bulletins, <http://www.microsoft.com/security>
- [37]. CERT, <http://www.cert.org>
- [38]. 台灣電腦網路危機處理/協調中心, <http://www.cert.org.tw>
- [39]. The Nessus Project, <http://www.nessus.org>