第三層DNS安全檢測系統

報告人：沈志昌

內容

- 簡介
  - 系統目標
  - DNS安全檢測執行流程
  - 網路現況分析
  - 網路安全探討
  - TWCERT/CC大規模掃描DNS資訊
  - 常見DNS攻擊方式
  - 台灣區DNS常見問題
- 第三層檢測
  - 主動式安全掃描
  - DNS安全檢測系統
  - DNS安全檢測系統實作
  - 安全檢測掃瞄結果

內容

- DNS Security 資源網站
  - 目的
  - 功能
- 未來發展
  - 系統功能
  - 漏洞通報
  - DNS 相關資訊
  - 線上滿意度調查
- 結論

系統目標

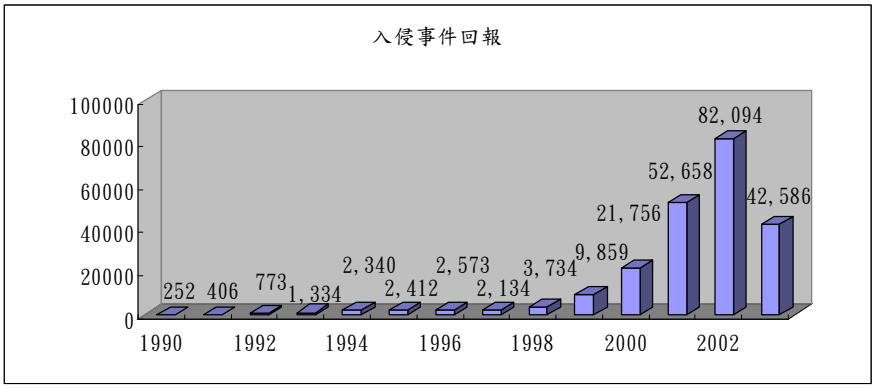
- 保持整體DNS資料的正確性與完整性，將是提供良好網路服務的重要一環
- 目標將著重在第三層DNS的安全檢測與防護體系之建立

DNS 安全檢測執行流程

網路現況分析

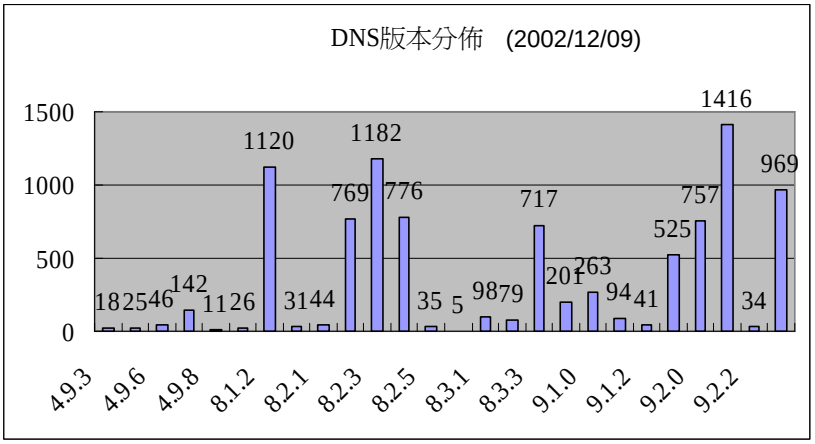
	2000年	2001年	成長率
對外頻寬	7.2 Gbps	14.8Gbps	105%
連網主機數量	343萬部	392萬部	14%
寬頻上網用戶數	114萬戶	210萬戶	85%
TANET用戶數	291萬戶	344萬戶	18%
企業連網普及率	44.4 %	61.6 %	17.2%

網路安全探討



資料來源：CERT/CC（http://www.cert.org）2003.04

TWCERT/CC大規模掃描DNS資訊



常見DNS攻擊方式

- Buffer overflow
- Crash server
- Denial of Service
- Information leak

台灣區DNS常見問題

- 不良委任關係（Lame Server）
- 授權錯誤（Delegation Error）
- DNS容錯能力
- 轄區傳送（Zone Transfer）
- 版本偵測

主動式安全掃描

- 遭遇問題
  - 第三層DNS權責分散
  - 數量繁多
  - 自行設計檢測系統困難度高
- 設計考量
  - 降低管理權責問題
  - Web操作介面
  - 使用者無須安裝額外系統

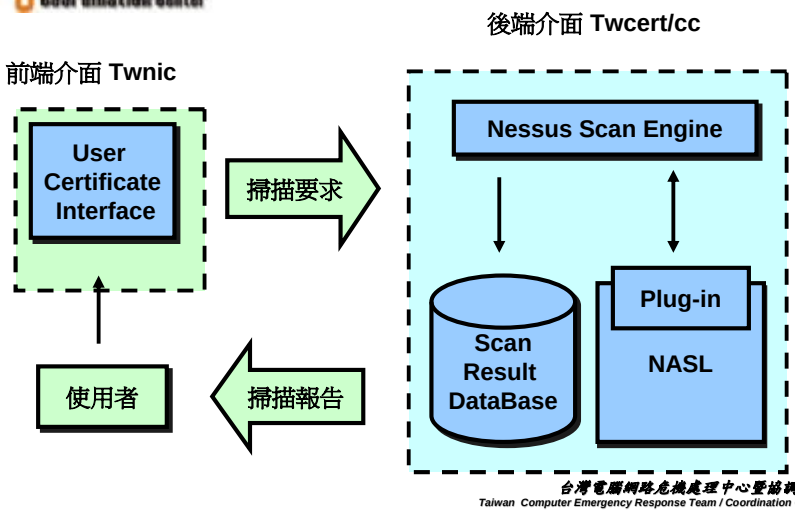
DNS安全檢測系統

- 檢測方式
  - 利用判斷漏洞來檢測主機是否具安全上疑慮。
- 目的
  - 儘早提醒使用者系統上漏洞。
  - 使用者藉由掃描報告可修正系統弱點。

系統架構

- User Certificate Interface
  - Twnic 提供前端使用者驗證介面
- Nessus Scan Engine (NSE)
  - 掃描核心引擎
- NASL-plugin
  - 中文化DNS 弱點掃描稽核程式
- Scan Result DataBase

系統方塊



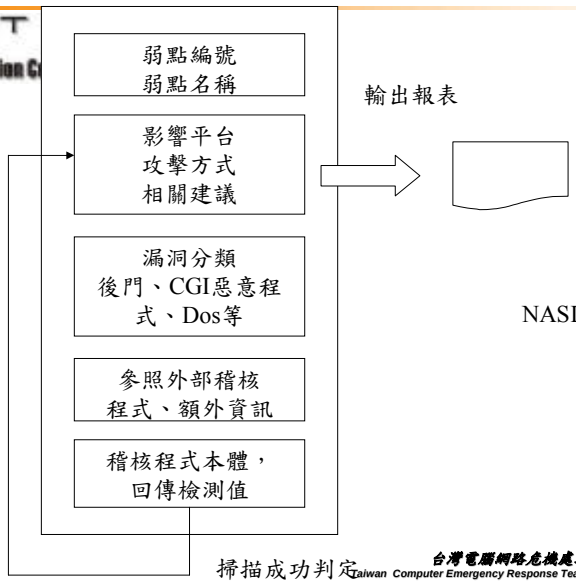
使用者前端驗證（User Certificate Interface）

- 由TWNIC端登入
- 驗證TWNIC用戶資料庫資訊
- 取得註冊主機網域、IP位置、郵件信箱
- 預防惡意人士藉由系統掃描他人主機

NSE（Nessus Scan Engine）

- 分散式架構
- 重編譯核心建構中文化檢測環境
- Web設計理念
- 更換稽核程式可以增加檢測能力

NASL（Nessus Attack Script Language）



NASL 設計模型

Scan Result DateBase

- 紀錄使用者掃描狀態
- 內容
  - 漏洞敘述
  - 建議修正
  - 相關資訊鏈結
- 提供線上即時分析、用戶狀態分析

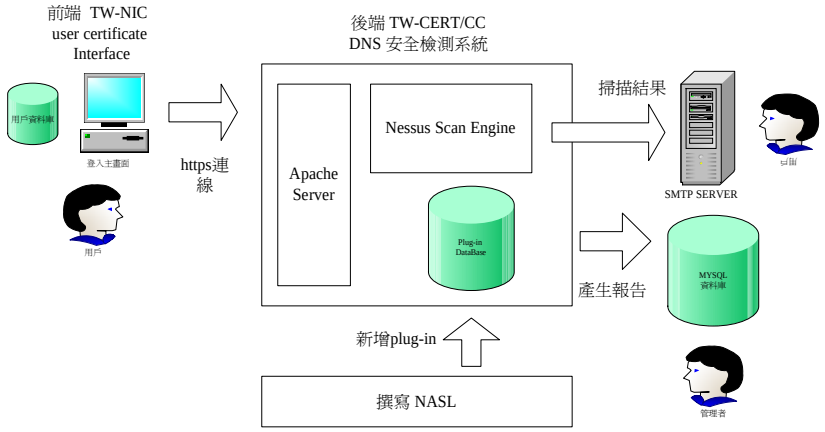
檢測分類

- 檢測服務版本
- 攻擊服務檢測
- 轉送服務要求
- 轄區轉送檢測
- DNS蠕蟲
- DNS相關問題

系統特色

- 分類化漏洞檢測模式
  -- 六大類、21支稽核程式
- 漏洞分析及風險說明
- 中文化檢測報告
- 具建議修正及相關漏洞通報連結
- 具新增漏洞稽核程式能力
- 自動產生報表
- 資料庫統計自動產生圖表

檢測流程程示意圖



掃描流程

- 前端使用者登入
  - 由NIC資料庫中驗證使用者合法性及主機對應
- 後端掃描主機連線
  - 後端TWCERT/CC檢測主機連線
  - DNS漏洞介紹、掃描說明
  - 進行掃描項目選擇及開始掃描
- 系統排程進行掃描
  - 掃描結果以電子郵件寄出供使用者觀看
  - 使用者根據結果進行主機漏洞修補

系統掃描狀態

- 上線時間 91.7～92.6
- 累積至今結果
  - 累積用戶數：1399 (不包含重複掃描)
  - 掃描主機數：1483 部

DNS版本分佈狀態

DNS 版本	數量(部)	佔有率（%）
BIND 9系列	426	28.73%
BIND 8系列	270	18.21%
BIND 4系列	8	0.54%
Windows DNS	677	45.65%
隱藏伺服器版本	102	6.88%
掃瞄主機（TOTAL）	1483	100%

DNS漏洞分佈

DNS 版本	數量(部)	佔有率（%）
DNS TRf 漏洞	1252	84.42%
DNS XRf 漏洞	7	0.47%
ZONE TRANS 漏洞	28	1.89%
bind 廣播風暴漏洞	31	2.09%
BIND9_DoS	45	3.03%
未含漏洞	118	7.96%
掃瞄主機（TOTAL）	1483	100%

掃描情況分析

- Bind 9及windows系列仍為DNS系統大宗
- 漏洞產生情形多屬於人為設定的部分，系統設計上的漏洞因安裝新版DNS系統後已解決，應注意人為的設定
- 主動進行掃描人次仍嫌少，顯示具DNS安全知識的管理者仍屬少數，需進行推廣使其瞭解DNS安全性對於網域之重要性

DNS資源網站

- 長期維持整體DNS服務之安全性，協助使用單位提升管理與技術能力。
- 結合DNS安全檢測系統，在動態方面提供使用者一個主動掃瞄環境，在靜態方面，提供漏洞通報，學習及提升管理技能園地 。

DNS security 資源網站功能

- DNS安全檢測系統
- 台灣區DNS調查
- ISC BIND弱點調查
- DNS相關資訊
- DNS相關工具
- DNS檢測相關資訊
- 問題回應系統

DNS 安全檢測系統

- 使用者可以直接進入此一系統進行實體的主機掃瞄檢測。
- 對於檢測方面的疑問將可以經由檢測說明來瞭解整體檢測流程和系統介紹。

台灣區DNS調查

- 包含TWNIC、TWCERT/CC網路普查的資料。
- ISC BIND版本分佈、.tw、.gov.tw、.net、.edu.tw、.net.tw、idv.tw、.org.tw及BIND漏洞列表等九項資訊。
- 有助於使用者瞭解整體DNS伺服器在網路上的概況。

ISC BIND弱點調查

- 提供了經過整理後的漏洞分佈表。
- 定期更新的BIND DNS 漏洞通報。
- 整理後的資料將可成為有用的資訊來提供DNS管理人員在DNS安全上的管理和參考 。

DNS相關資訊

- 使用者可參考RFCs來瞭解其所需要的資訊 。
- 安全性文件則針對漏洞原理及安全議題進行更深入的探討。
- 工作群組則提供使用者在DNS領域上的網路資源或供應商 ，使其可以直接連結至所需的網站來進行更進一步的詢問或資料蒐集。

DNS相關工具

- 攻擊工具在此處較為敏感，其目的在於提供使用者測試自身的伺服器設定及安全性上是否適當。
- 管理工具提供DNS伺服器設定及除錯的便利工具。
- 稽核工具用來稽核設定上的安全性及DNS組態設定上的正確性，有助於安裝及維護DNS系統。

DNS檢測相關資訊

- 安全掃瞄統計為DNS安全檢測系統之子系統，圖表方式來讓使用者能進一步瞭解DNS版本、漏洞分佈的情形，對於瞭解整體DNS服務環境將有所幫助。

問題回應系統

- 為達成與會員更進一步的互動，問題回應系統，提供使用者可以更進一步向TWNIC及TWCERT/CC反映DNS問題。

未來方向

- 藉由多方管道進行DNS檢測系統推廣，增加上線掃描人數
- 除產生報告外，預計在報告中附加設計掃描滿意度問卷來進行滿意度及建議之收集
- 新增弱點掃描稽核程式
- 整合DNS資源網站，建立一提供完整DNS資訊之專門網站

漏洞通報及DNS相關資訊

- 提供關於DNS的漏洞通報，未來將持續更新並隨時發佈給使用者，並定期利用電子報功能自動發送安全通報，達到即時資訊流通及預警的目的。
- 預計將來提供更新穎的DNS安全工具、系統漏洞文件、安全修補程式（patch），系統安全檢測工具及其他相關技術文件的下載。

滿意度問卷調查統計

- 預計朝向DNS安全檢測系統使用情形、DNS security資源網站使用情形、使用者DNS安全常識及設定技巧三部分進行滿意度問卷調查。
- 目的為使服務達到符合使用者需求提供最佳安全性解決方案 。

系統展示

- DNS安全稽核檢測系統
- DNS安全稽核檢測

DNS Domain Test

DNS Domain Test

DNS設定常見問題建議

- 隱藏版本
- 禁止遞迴查詢
- 限制Zone Transfer區域
- 修正DNS版本
- 閱讀弱點通報

結語

- 建構完整的DNS伺服器安全檢測與防護體系，TWCERT/CC亦持續進行後續的改進和更新的動作。
- TWCERT/CC將提供網路安全相關資訊，並定期舉辦教育訓練及網安課程，培養更多具有網路安全知識人才來確保網路安全的概念能夠持續推廣。

問題與指教