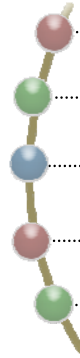


資安控管實務技術教育訓練 -資安弱點稽核工具-

97年06月25日
97年06月30日
97年07月03日
報告人：王吉祥

課程大綱

- 
- 認識威脅與漏洞
 - 弱點稽核工具與ISO 27001控制點對應
 - 整體網路應用工具強化ISMS
及網站應用工具強化ISMS
 - 資安弱點稽核工具實作介紹
 - 資安弱點稽核工具報告解析與實例討論

認識威脅與漏洞

前言

- ▶ 網路對於生活影響程度與日俱增，駭客利用網路從事電腦犯罪也屢見不鮮。
- ▶ 要如何保護在網路中傳遞及儲存於電腦系統之機密資料，免於遭受未經授權人員之竊取、篡改、偽造，則是資訊時代當務之急。

了解你的敵人

➤內部的潛在危機

- 心生不滿的在職員工。
- 惡意的離職員工。
- 好奇與惡作劇。

➤人為的因素

- 測試作業的不小心。
- 工程人員的誤動作。
- 正常使用揭露了系統弱點。
- 管理上的疏失。



外來的不速之客

- 駭客
- 怪客
- 商業間諜
- 恐怖份子
- Script Kiddies



駭客v. s怪客

➤駭客(Hacker)是什麼？

- 受道德倫理與法律約束，以研究技術為出發點的團體或是個人。
- 不從事破壞、竊取機密等違反法律的行為。

➤怪客(Cracker)是什麼？

- 不受道德倫理與法律約束，擁有高級技術，以自我主觀思想為主的團體或是個人。
- 恣意破壞、入侵與竊取他人隱私與資訊以換取自身之利益。

➤所以，駭客不等於怪客！



各色的駭客

- 白帽駭客：研究技術為主，必要時會提供防禦協助。
- 黑帽駭客：雖以研究技術為主，有時會因研究技術入侵目標。
- 灰帽駭客：技術高超的團體或個人，有時會像白帽駭客有時會像黑帽駭客，有時則為收取利益入侵目標。

什麼是 Hacking ?

➤ 什麼是 Hacking ?

- 使用反向思考的方式，揭露系統的弱點與漏洞。
- Hacking不是使用自動化工具。
- Hacking不是因為系統自動揭露。
- Hacking不是透過監聽與竊取帳號密碼。
- Hacking不是因為你知道帳號與密碼。

➤ 入侵是...

- 未經過他人的允許與承諾。
- 揭露或是探尋他人的隱私。
- 不受任何的道德與倫理的約束。
- 入侵的結果僅對入侵者有利，對受害者造成莫大的，有型與無形的損失。
- 不受任何法律的保障。
- 最後：入侵是會坐牢的！



入侵的方式

➤ 外部網路與內部網路

- 來自於外部的的方式
 - 網際網路 (INTERNET)
 - 外部企業網路 (EXTRANET)
 - 遠端存取服務 (RAS)
 - 無線網路 (Wireless Network)

➤ 來自於內部的方式

- 內部企業網路 (INTRANET)

➤ 實體環境

- 門禁
- 線路
- 電力
- 社交工程



駭客攻擊手法

1. 病毒、蠕蟲 Virus, Worm
2. 木馬、後門 Trojan Horse, Backdoor
3. 暴力猜解密碼 Brute Force
4. 阻絕服務 DoS, DDoS
5. 緩衝區溢位 Buffer Overflow
6. 監聽與側錄 Sniffing, Key-Logger
7. 欺騙與偽裝 Spoof, Smurf
8. 資料隱碼 SQL Injection
9. 無線網路滲入 Wireless LAN Intrusive
10. 社交工程 Social Engineering

病毒、蠕蟲、邏輯炸彈 (1)

- 病毒
 - 一段完整且具基本人工智慧之程式碼，該程式碼之執行會造成電腦設備資料毀損、作業異常等惡意破壞行為
 - 通常具備自我隱藏、複製與再生等基本人工智慧。
 - 早期病毒不具備資訊網路通訊能力。
- 蠕蟲
 - 早期出現於 Unix 系統，除具備病毒之自我散佈、複製、攻擊、破壞與隱藏之能力外，最常透過網路散佈
- 邏輯炸彈
 - 早期出現於某些特定場合，主要因為不具自我增生能力與特定病毒特徵，因此防毒系統往往無法發現與查殺

病毒、蠕蟲、邏輯炸彈 (2)

- 病毒、蠕蟲、邏輯炸彈的防治方法

1. 安裝防毒軟體
2. 郵件過濾
3. 更新 Patch
4. 郵件附件不預覽
5. 使用者教育



木馬、後門 (1)

- 木馬 Trojan Horse

- 特洛伊木馬程式, 特洛伊木馬式病毒 (係一種電腦病毒, 此程式貌似合法而實際上起破壞作用, 將其比喻為特洛伊木馬, 意指潛在的危險性)

- 後門 Backdoor

- 以提供非傳統的便利途徑, 得以非授權存取資料、程式、服務和進入系統。



木馬、後門 (2)

- 一隻完整的木馬往往包含兩個 winsock 程式, 一個是 Client 一個是 Server。Server 端的功能主要是提供下面幾項資訊以及服務給 Client 端程式:

1. 主機名稱, 記憶體大小, 硬碟空間等系統資訊
2. 對所有磁碟機的檔案目錄有讀、寫、新增、及刪除的權利
3. 下載上傳檔案
4. 取得鍵盤/滑鼠輸入/移動訊息
5. 強迫關機
6. 取得目標主機螢幕畫面
7. 開啟/移除資源分享
8. 遠端執行目標主機上的 Process 或 AP
9. 執行跳板攻擊, 攻擊其他主機或連線到其他主機
10. 雙向聊天送訊息

木馬、後門 (3)

- 常見後門程式

- Windows Backdoors

1. Netcat (nc) (may listen on any tcp/udp port)
2. Back Orifice (default port tcp 54320 or udp 54321, 31337)
3. NetBus (default port 12345, 12346 or 20034)
4. WinVNC (default port 5800, 5900)
5. SubSeven (default port 27374).....

- Unix Backdoors

1. 典型在網路埠綁定 SHELL
2. 跳過存取控制或其他安全機制來非授權交換資料
3. 隱密性通道

木馬、後門 (4)

• 防治方法：

1. 委外開發軟體惡意程式檢查
2. 系統通訊埠檢查
3. 服務檢查
4. 系統常駐程式檢查



暴力猜解密碼 (1)

- 暴力猜解密碼是以自動化工具強制性猜測某一系統帳號的密碼，通常使用所謂的字典檔，或是挑選字元類型及密碼長度。
- 傳統的駭客是以破主機帳號密碼為達成自我成就感的方式之一。
 - Linux 採用的 DES 演算法如果拿到加密後的密文早已可以使用字典檔的方式用暴力方式加以破解。
 - Windows NT 上的密碼檔可用 DumpACL 以及 Pwdump 等工具來破解 SAM 密碼檔，同時也有在網路上竊聽 SMB 密碼 hash 的軟體出現。

暴力猜解密碼 (2)

• 防治方法：

1. 密碼檔加密
2. 密碼複雜度、長度及定期變更
3. 憑證



阻絕服務 (1)

- 阻絕服務 (DoS, DDoS) 攻擊手法是利用 TCP/IP 協定當初設計的缺失，以及作業系統針對 TCP/IP 協定實際 implement 方式的不同來設計攻擊方式。
 - 駭客使用大量封包或是特異畸形的封包來癱瘓目標主機上的服務；
 - 輕則使目標主機服務停止，重則讓主機當機；
 - 針對 DDoS 的攻擊則往往很難抵擋，事後也很難追查真正的攻擊發起人。

阻絕服務 (2)

- 防治方法：
 - 過濾 ICMP
 - 建置IDS
 - 修補重大漏洞



緩衝區溢位 (1)

- 緩衝區溢位(Buffer Over Flow) 攻擊存在於任何一套軟體甚至是作業系統中，也可能是你我寫的程式或是你我天天在用的程式，最厲害的駭客可以精心設計出造成 Buffer Overflow之後跳到他設計好的程式程序裡面，此時如果這個程序有 SET UID 的程式將會使駭客擁有root的權限，他可以為所欲為而你卻完全無法察覺。目前針對這方面攻擊的預防不外乎就是程式設計時不光以功能為導向，還要注意系統安全的環節，而不是趕著交差了事的心態設計程式，此外要善選安全的 compiler，對會造成問題的函式盡量不要使用。

緩衝區溢位 (2)

- 防治方法：
 - 1.委外開發軟體惡意程式檢查
 - 2.系統通訊埠檢查
 - 3.服務檢查
 - 4.系統常駐程式檢查



欺騙與偽裝 (1)

- DNS Spoofing
- IP Spoofing
 - IP Spoofing 可欺騙路由器或防火牆，假裝入侵者是來自於可信任的網路，而順利進入私人網路。
 - IP Spoofing 會更改封包的表頭，讓封包看起來像是來自於可信任的網路而允許進入路由器或防火牆。
- ARP Spoofing
 - 利用系統或設備中 ARP Table授受Request時，以大量偽裝MAC Address或IP來造成ARP Table Full，使系統或設備癱瘓。

欺騙與偽裝 (2)

- 防治方法：
 - 過濾 ICMP
 - 建置IDS、IPS
 - 建置防火牆

監聽與側錄 (1)

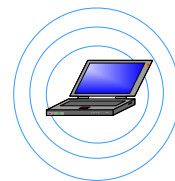
- 監聽 (Sniffing)
 - 監聽器的出現來自於網管人員對於網路流量的管理監控需求，因此需要一套軟體來記錄 LAN 裡面傳遞的封包資訊，流量等紀錄，但被有心人士拿來當作竊取資訊的手法。
- 側錄 (Key-Logger)
 - 鍵盤記錄器，可將使用者所有使用鍵盤輸入的字元完整的記錄下來，並配合木馬程式可將記錄檔傳送給攻擊者，以竊取密碼和敏感資訊。

監聽與側錄 (2)

- 防治方法：
 - 安裝 SSH 或是其他建立遠端連線加密服務
 - 安裝防 Sniffer 軟體

無線網路滲入 (1)

- 無線網路滲入 (Wireless LAN Intrusive) 是利用企業無線區域網路存取點 (Access Point) 設定上的安全弱點，連接企業內部網路來進行入侵與攻擊行為。

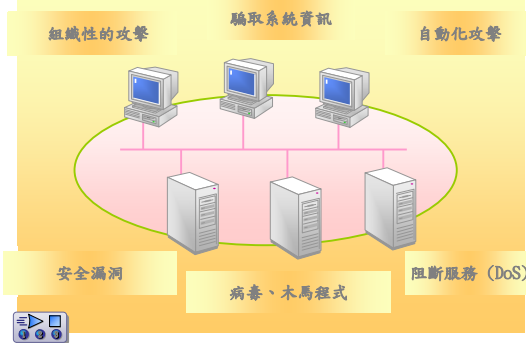


無線網路滲入 (2)

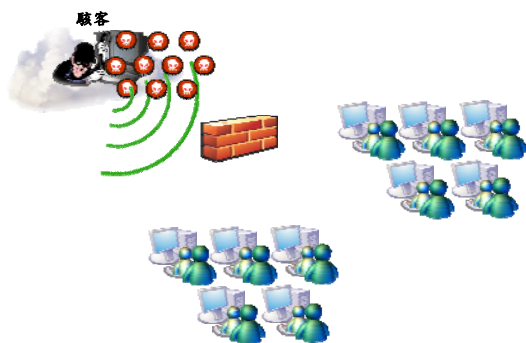
- 防治方法：
 - SSID Broadcast
 - WEP Key 加密
 - Trust



常見的攻擊型態展示



系統弱點攻擊



電子郵件攻擊

寄送經過設計的e-mail, 夾帶惡意程式的附件
進行後門植入的攻擊



網站植入木馬

攻擊網站，植入網頁後門，等不知情的民眾上網站時下載後門



SQL Injection(資料隱碼)

- 新式攻擊手法
- 不需植入後門程式
- 不需入侵主機
- 防火牆、入侵偵測器無法防禦
- 利用AP未做輸入字串檢核取得資料庫權限
- 竊取資料或竄改、破壞資料庫



SQL Injection

• SQL Injection

- Authentication Bypass
 - Select * from UserTable where id=' or 1=1 and pwd=' or 1=1
- Database enumeration
- Command Execution
 - Exec master..xp_cmdshell 'dir'



SQL 指令隱碼範例

```
sqlString = "SELECT HasShipped
FROM"
+ " OrderDetail WHERE OrderID ="
+ ID + "';";
```

- 如果 ID 這個變數的值是直接取自表單上的文字方塊，
- 那麼使用者可以輸入：


```
ALFKI1001
ALFKI1001' or 1=1 --
ALFKI1001'; DROP TABLE OrderDetail --
ALFKI1001'; exec xp_cmdshell('fdisk.exe') --
```

防範 SQL 指令隱碼攻擊

- 不要使用動態 SQL 語法
 - 在預存程序或 ADO 中使用參數
 - 不要在預存程序中使用 EXECUTE('.....')
- 檢查所有的使用者輸入
 - 只放行符合規則的輸入資料
- 使用最低的權限來連接資料庫管理系統
 - 永遠不要使用 "sa"
 - 針對內建的預存程序加以限制
- 不要直接顯示任何資料庫錯誤訊息

社交工程 Social Engineering

- 社交工程為利用**人性的弱點**進行詐騙，是一種非技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。駭客通常由**電話**、**Email**或是**假扮身份**，問些看似無關緊要的問題等各種方法來進行社交工程。



網路釣魚



防治方法

- 人員認知訓練
- 郵件伺服器身份鑑別
- 宣導
- 罰則



弱點稽核工具與ISO 27001控制點對應

A.12.6 技術脆弱性管理

資訊系統獲取、開發及維護

- A.12.6 技術脆弱性管理
- 目標：降低因利用已公佈的技術脆弱性所導致的風險

A.12.6 技術脆弱性管理

- A.12.6.1 技術脆弱性控制

- + 根據現有及完整的資產清冊，決定需要支援技術脆弱性管理的特定資料，包含軟體廠商、版本號碼、目前的佈署狀態及組織內的相關負責人員。採取適當與及時的行動以回應被認出的潛在技術脆弱性。
- + 視技術脆弱性需要因應的緊急程度決定依循變更管理相關控制措施或資訊安全事故反應程序。
- + 所有針對技術脆弱性所採取過的程序需有稽核日誌可供查詢。
- + 定期監視與評估技術脆弱性管理過程，以確保其有效性及效率。

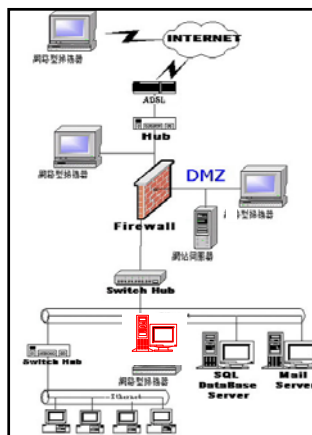
資安弱點稽核工具實作介紹

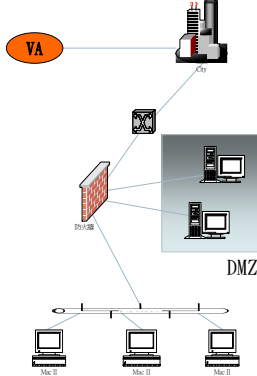
要如何有效的運用弱點掃描(VA)

- 在網路各個角落
- VA與IDS orIPS
- VA與DMZ
- VA與Wireless
- VA與VPN
- 網路安全金三角

VA可安裝在網路各個角落

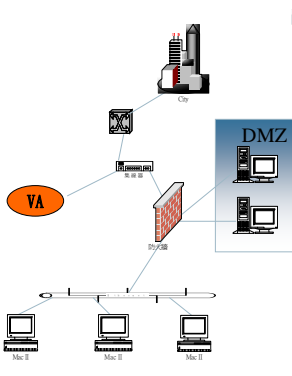
- Internet
- Firewall前
- DMZ區
- Ethernet





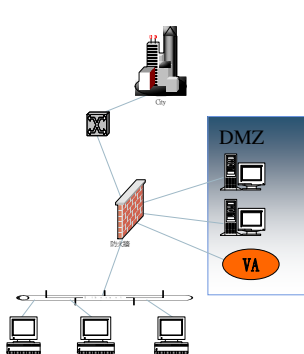
當VA在網際網路上可以模擬成駭客

當有分公司又無VPN環境時，可隨時監測分公司網路的安全性並測試網路設備是否夠堅固。



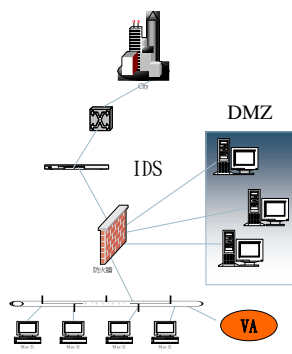
當VA在Firewall前可模擬成駭客

加快Scan速度



當VA在DMZ區跟DMZ區電腦IP Range 要一樣

測試DMZ區的安全性



VA與IDS

當公司若有安裝IDS時請注意設定：

如設定不當可能造成IDS與SCANNER的誤判

IDS對內必須設定允許從架設DSS機器來不正常封包IP位址

如要Scan Internet上的機器，則IDS要再加上對外允許來自欲Scan在Internet IP位址

TANet 網路中心導入資訊安全管理制度及資訊安全專業人才培訓計畫

VA與DMZ

當公司如有DMZ區時要如何設定

VA可安裝在Ethernet的電腦上

TANet 網路中心導入資訊安全管理制度及資訊安全專業人才培訓計畫

VA與Wireless

VA要如何運用在無線網路上：
Wireless單純上Internet

TANet 網路中心導入資訊安全管理制度及資訊安全專業人才培訓計畫

VA與VPN

當公司如有VPN要如何運用：

VA需架在加入VPN的PC

可遠端Scan分公司的電腦

TANet 網路中心導入資訊安全管理制度及資訊安全專業人才培訓計畫

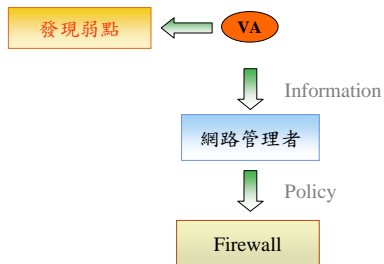
IDS入侵偵測

Information

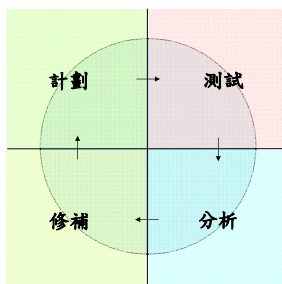
網路管理者

Policy

Firewall

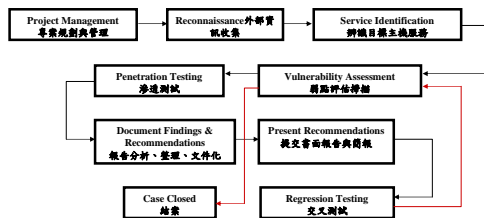


測試流程



- 計劃
 - 確立目標及範圍
 - 計畫工作程序
- 測試
 - 進行弱點評估
 - 滲透測試
- 分析
 - 進行比對及風險分析
- 修補
 - 提供修補建議
 - 檢查修補成效

測試步驟與流程說明



專案規劃與管理

- 目的
 - 確定需求、服務範圍、聯絡窗口、時程並保持進度溝通
- 方法
 - 會議討論、電話、Email
- 工具
 - 專案管理工具



外部資訊收集

目的

- 找出目標網路與主機的位址與名稱。模擬駭客無所不用其極盡可能蒐集最多的目標資料

方法

- 利用 Internet 網路資源，搜尋引擎 (包含 Google Hacking)
- Whois、ARIN、DNS Zone Transfer 測試

工具

- Nslookup、Whois Query、SiteDigger
- Search Engine、ARIN search、Google Hacking

辨識目標主機服務

目的

- 辨識目標主機與網路所開放與提供的網路服務與所使用的作業系統版本。這些資料可做為後續攻擊的途徑。

方法

- ICMP Ping、TCP/UDP 埠號掃描、SYN/FIN Scan、Netbios Scan

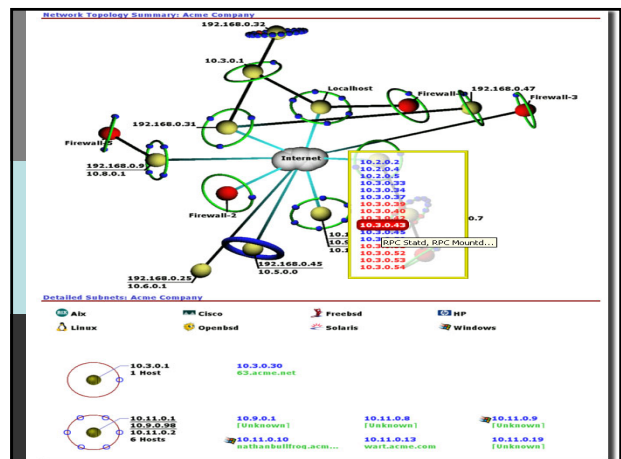
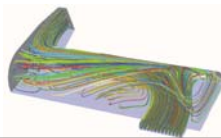
工具

- Nmap、Fping、NetCat、traceroute、Neo Trace、Nbtstat、ScanMachine

網路架構拓樸

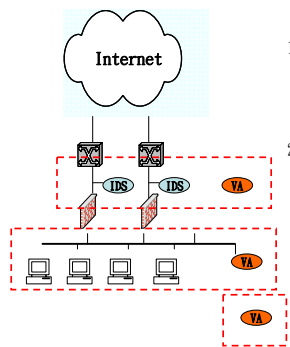
以圖形化的方式拓樸網路安全架構，並完整地呈現在您的風險評估報告中。

評估服務可搜尋網路上的路由器、防火牆、伺服器、主機的相對位置，而此架構圖有助從駭客觀點了解整體網路安全架構，從網路架構中找出漏洞修補之優先順序。



個案範例

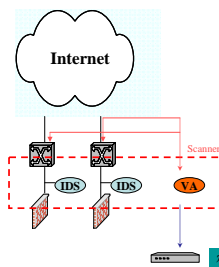
某中型客戶



1. 無法確定安全區域為何?
→ 何處可放棄、或逐步改善
→ 何處為必要一定得馬上改進
2. 無法有效落實稽核
→ 無實際缺失報告、明列各項問題
→ 或無從學習修正方法
採用3套 VA 組成基本架構

個案範例

第一套 VA



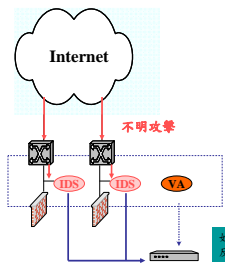
➢ 建置在最外與IDS / IPS互補結合

狀況一、不斷地從外去確認安全政策以及有無新的弱點產生而疏忽並將資料匯入整合資料庫並結合IDS / IPS

定期將弱點資料匯入資料庫分析管理

個案範例

➢ 建置在最外與IDS / IPS互補結合



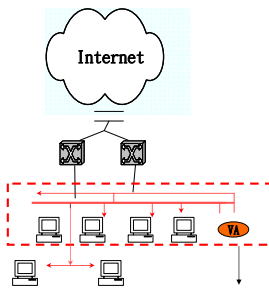
IDS若測到某一IP的攻擊訊息則檢查該IP是否存在相關弱點, 並透過整合過之資料庫進行其他類似之比對

如果被攻擊IP, 很快連比對, 確認是否可承受, 則只需紀錄存盤反之, 若可被攻擊成功, 務必錄外, 高層第一時間通知管理者

DSS 結合IDS / IPS 將大幅改善IDS
過去為人詬病的誤判與錯誤並避免針對外漏的弱點攻擊

個案範例

第二套 VA



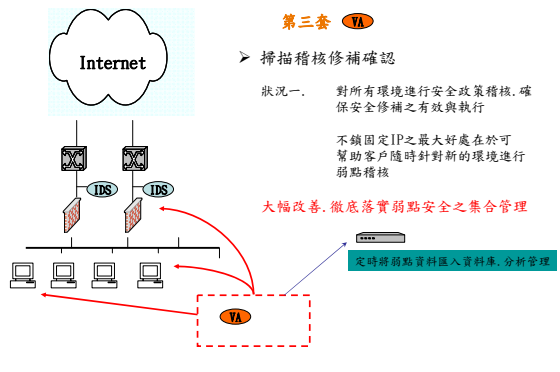
➢ 建置在內不斷地定時掃描稽核

狀況一、不斷地從內進行安全稽核, 確保重要的伺服器及新加入的機台與應用程式, 可修正至最新的版本
透過單一主控台整合資料庫進行內部的弱點比對與修復。

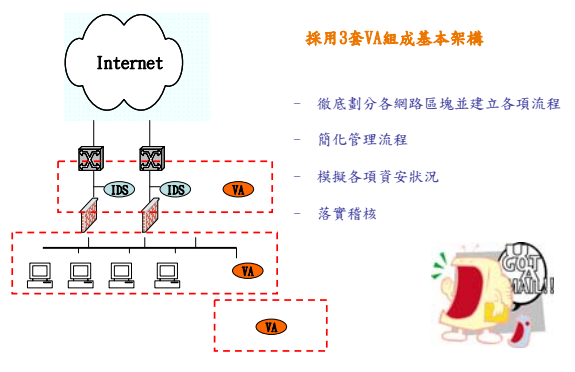
大幅改善, 單一的整合資料庫簡單管控所有的弱點稽核資訊與修補狀況

定期將弱點資料匯入資料庫, 分析管理

個案範例



個案範例



資安弱點稽核工具報告解析 與實例討論

弱點評估掃描

- 目的
 - 辨識目標主機上之潛在漏洞、不當設定、不當使用者帳號密碼設定、分享資料、以及木馬與後門
- 方法
 - 利用多種手動及自動化弱點掃描工具執行弱點掃描
- 工具
 - Nessus、Foundstone、Nikto、WebInspect、Acunetix、N-Stealth...
 - 手動檢測

進階掃描與測試

風險評估服務不僅協助您找出既有的安全弱點與漏洞，同時主動做進階的探測與串連。

發現有某一漏洞存在，則將視該主機為被成功入侵的受駭主機，並利用此主機與已知的漏洞，做進一步的掃描，以便準確得知何者對網路安全的影響最重大。



報告分析、整理、文件化

目的

- 將測試結果文件化，針對客戶主管與技術人員提供相關的修正建議與補救辦法

方法

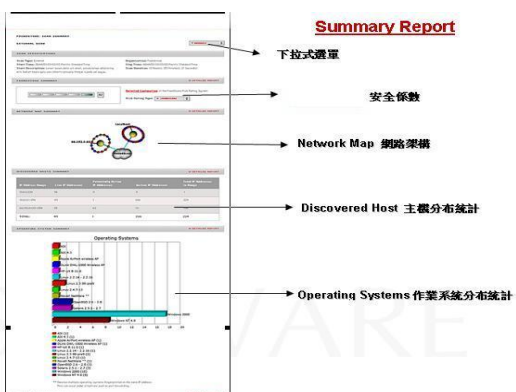
- Executive Summary
- Details Technical Findings & Recommendations

工具

- 電子檔報告
- 書面報告



風險評估範例報告(一)



風險評估範例報告(二)



風險評估與需求分析

來自外部的威脅(Threat)與內部的漏洞(Vulnerabilities)會影響風險的強度；我們採取的資訊安全對策則是降低風險的母數；當然一個組織的資訊價值愈高，也意味著發生安全事件時，所受的傷害愈高。

資訊安全的持續性管理經營，同時著眼於降低系統的漏洞及可能威脅並強化資訊安全政策，才能公允的計算出一個組織所面臨的風險，採取適當措施來謀求資訊安全並提高可信度。

弱點及威脅分析

風險評估要點為適時發現弱點與漏洞並即時做好漏洞修補的工作，大略可分為以下幾點：

軟體本身之漏洞(Software Bugs)：

- Buffers overflow 、Unexpected combinations 、
- Unhandled input 、Race conditions 。

系統之設定問題(System Configuration)：

- Default configurations 、Lazy administrators 、Hole creation 、Trust relationships 。

密碼被竊取>Password Cracking)：

- Really weak passwords 、Dictionary attacks 、Brute force attacks 。

監看未經加密的流量(Sniffing unsecured Traffic)：

- Shared medium 、Server sniffing 、Remote sniffing 。

設計的瑕疵 (Design Flaws)：

- TCP/IP protocol 、UNIX design flaws 。

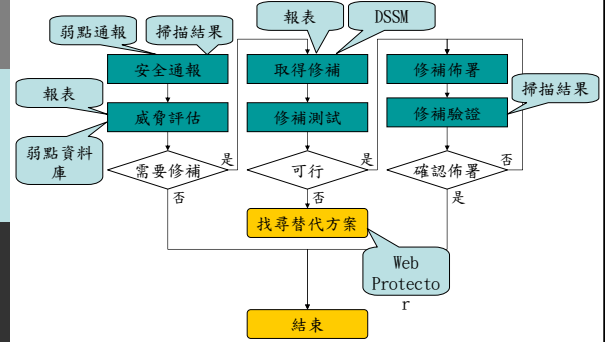
影響風險因子-相互關係示意圖



整體網路應用工具強化ISMS 及網站應用工具強化ISMS

實例分享

修補管理六步驟



修補管理軟體

網路型 (有管理功能)

- PatchLink Update
- Shavlik HFNetChkPro Security Patch Management
- SMS 2.0 wit SUS Feature Pack / SMS 2003
- SUS / WUS

單機型 (僅做修補下載及安裝動作)

- Automatic Updates feature in Windows
- DragonSoft System Security Manager
- Linux Online Update Service
 - Redhat up2date
 - Mandrake MandrakeUpdate
- Windows Update / Office Update



安全通報

資訊的時效性

- 弱點從公佈到利用的時間越來越短, 由 1-6 個月的時間, 到 2004 年只用 20 天的時間。

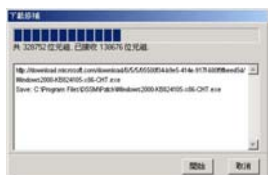
即時 / 正確的安全弱點通報
快速 / 方便的弱點資料庫更新



修補取得

修補管理工具 線上更新服務

- Microsoft
 - Windows Update
 - Office Update
- RedHat
 - up2date
- Mandrake
 - MandrakeUpdate



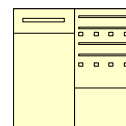
修補資訊

- 弱點稽核工具
- 弱點資料庫
- 軟體原廠提供的線上資訊

修補測試

是否需要

- 測試環境建制不是簡單的工作，應評估資產重要性及組織能力，決定最適當的對策



測試環境建制

- 盡量模擬真實環境
- Virtual Machine 可用以減低困難度

常見避免弱點的方式

移除受影響軟體 / 服務

- 非必要的軟體 / 服務應該盡量避免
- 替已經沒有支援 / 更新的軟體找尋替代方案

經由軟體設定避免弱點發生

- 軟體功能限制
- 檔案 / 目錄權限

防火牆，或其他禁止存取方法

- 限制存取主機的範圍
- DragonSoft Secure Scanner 可依據弱點情形提供防火牆設定建議
- Application Firewall
 - DragonSoft Web Protector, URLScan, etc.

一般事務電腦修補解決方案建議

Windows 2000 / XP / Server 2003

- Automatic Update 自動修補系統重大更新
- AD 環境可用群組原則設定減輕管理負擔
- 可視組織狀態決定是否引入 SUS / WUS 服務搭配 Automatic Update

其他 Windows

- 定期執行 Windows Update、Linux
- 定期執行線上更新

應用程式

- 定期執行線上更新 (如 Office Update)

定期稽核弱點及修補狀況

Google Hacking

- 利用搜尋引擎的進階搜尋，找出企業網站的敏感資訊

- 搜尋引擎

- Google
- Yahoo
- Dogpile
- ...

- 搜尋工具

- Webferret



預防Google Hacking的方法

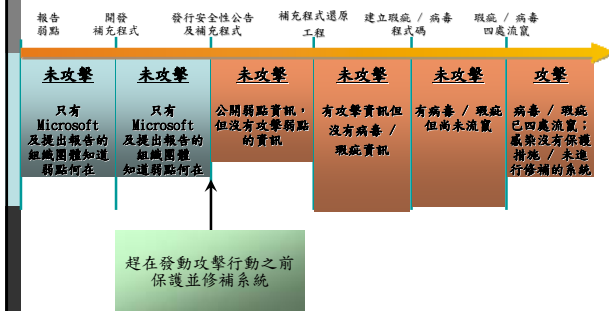
- 機密文件 **不連上URL**
- 利用相關工具進行在互聯網進行搜索，如果有資訊被濫用，到 <http://www.google.com/remove.html> 提交你希望刪除的資訊
- 採用客制化錯誤訊息處理回應
- 避免將URL清單存放在檔案夾中

最低權限賦予原則 (Least Privilege)

- 資源存取控制的安全性原則
- 設定權限時，必需依據使用者可以完成被指派的電腦作業所需的最少權限即可，絕不能賦予超出的權限。
- 最低權限賦予原則應同時應用於權限對象與權限等級
- 例如：公司有一應用程式目錄，希望提供給企業員工有讀取與執行能力，則預設NTFS權限與共用權限是否符合最低權限賦予原則？



攻擊時間表



Microsoft 嚴重性分級

分級	定義
嚴重	不需要使用者的動作，即可傳播網路網路瑕疵（例如 Code Red 或 Nimda）進行攻擊
重要	攻擊行動可能導致危害到使用者資料的機密性、完整性或可用性、或者處理資源的完整性或可用性
中等	攻擊行動很嚴重，但因為預設組態、稽核、需要使用者的動作，或其他導致難以攻擊等因素，得以減輕威脅程度
輕微	攻擊行動非常難以展開，或所造成的影響極小

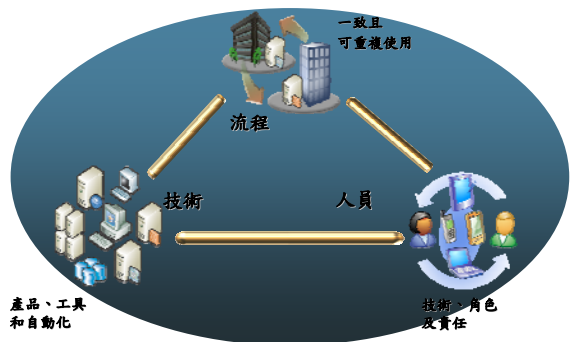
修補的時間範圍

嚴重性分級	建議的修補時間範圍	建議的最大時間範圍
嚴重	在 24 小時內	在 2 週內
重要	在 1 個月內	在 2 個月內
中等	等候下一版包含補程式的 Service Pack 或補程式彙總套件，或在 4 個月內部署補程式，需視何者先發行	在 6 個月內部署軟體更新
輕微	等候下一版包含補程式的 Service Pack 或補程式彙總套件，或在 1 年內部署補程式，需視何者先發行	在 1 年內部署軟體更新，或是選擇完全不要部署

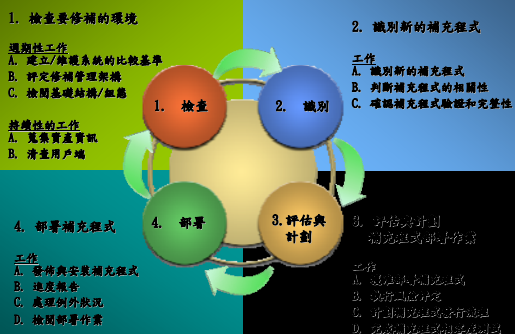
影響發行時間範圍的因素

因素	潛在影響
對高價值或具有高度的侵害威脅的資產造成的影響	縮短時間範圍
對過去曾受到攻擊的資產造成的影響	縮短時間範圍
減輕威脅的因素已經具備或可快速就緒	增加時間範圍
受影響的資產所具備的受侵害風險低	增加時間範圍

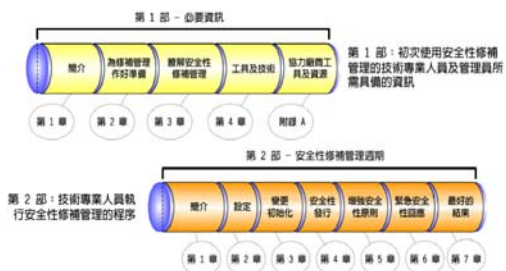
成功的修補管理



修補管理流程



《Microsoft 修補管理指南》



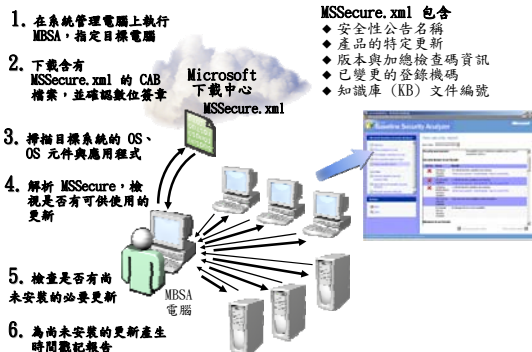
<http://www.microsoft.com/taiwan/technet/security/guide.htm>

MBSA - 優點

- 自動找出尚未安裝的安全性補充程式與安全性設定問題
- 允許系統管理員集中掃描多個系統
- 可以與各種 Microsoft 軟體搭配使用



MBSA - 如何運作



MBSA - 預設掃描選項

- MBSA 圖形化使用者介面 (Windows 應用程式)
 - 使用 `-baseline`、`-v`、`-nosum`
 - `-baseline` 會以 WU 嚴重的安全性更新為基準
 - 依預設值，會顯示注意與警告
 - 不執行加總檢查碼的檢查 (與 WU 配合)
- MBSA 命令列介面 (`mbsacli.exe`)
 - 使用 `-sum`
 - 執行加總檢查碼檢查
 - 依預設值，會顯示注意與警告
- HFNetChk 掃描 (`mbsacli.exe /hf`)
 - 使用 `-sum`
 - 執行加總檢查碼檢查
 - 依預設值，會顯示注意與警告

如何使用 MBSA

1. 下載並安裝 MBSA (只要一次)
2. 啟動 MBSA
3. 選取要掃描的一或多部電腦
4. 選取相關的選項
5. 按一下 [Start Scan]
6. 檢閱 [Windows Scan Result] 清單
7. 按一下 [Result Details] 連結
8. 檢閱尚未安裝的更新清單

微軟基準線安全分析工具(MBSA)

- MBSA 是微軟提供的免費安全性評估工具，可用來對微軟作業系統與應用程式進行各種弱點評估。
 - 掃描微軟作業系統與應用程式的安全弱點。
 - 檢查未更新的修正檔
 - 檢查不安全的預設組態設定
 - 提供發現弱點的解決方案
- 支援的平台
 - Windows 2000/XP/2003/Vista
- 支援的應用程式
 - IIS、IE、Office、Media Player、MDAC、MSXML、SQL、BizTalk、Host Integration、Exchange Server

MBSA 的使用特色

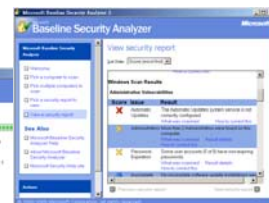
- 圖形介面：MBSA.exe
- 命令列介面：MBSAcli.exe
- 支援MBSAcli.exe /hf HFNetChk風格
- 可同時掃描一部或多部電腦
 - 執行 MBSA 的帳戶必須是 Administrators 群組成員
 - Mbsacli.exe -r 192.168.1.1-192.168.1.254
- XML 格式的安全性基準的報告儲存於 %userprofile% 的 SecurityScans 中
- 免費下載
 - http://www.microsoft.com/technet/security/tools/mbsa_home.asp

MBSA 工具掃描步驟

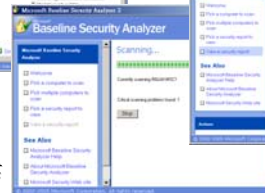
1. 執行掃描前設定



3. 產生掃描結果報表



2. 執行掃描作業



停用有安全性疑慮的網路功能

- 空連線 (Null Session)
- NetBIOS over TCP/IP
- File and Printers Sharing for Microsoft Network
- 其它

空連線(Null Session)

- Null Session連線 (又稱匿名登入) 是一種讓使用者不需經過身分認證, 就可以經由網路以匿名的取得使用者名稱和分享檔案等訊息的機制。
- Null Session連線可能導致資料不當的外洩
- 駭客只要用「Null Session」連線到NetBIOS Session Service, 就可以取得使用者和群組資訊 (使用者名稱、登入日期、密碼原則、RAS資訊)、系統資訊及登錄機碼 (register), 作為下一階段攻擊 (如密碼) 的輔助工具。



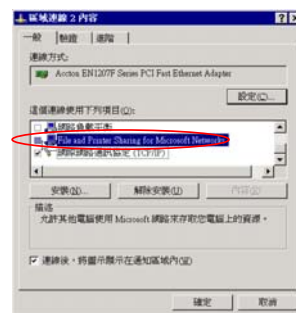
停用資源分享服務

- SMB/CIFS提供Windows資源共享服務
- SMB/CIFS存在潛在的弱點, 易受攻擊
- 強化安全性原則
 - 停用公用面向介面上的 NetBIOS 和 SMB
 - 停用一般用戶端機器介面上的 NetBIOS 和 SMB
 - 停用無線網卡的NetBIOS 和 SMB



File and Printer Sharing for Microsoft Network

- 停用 NetBIOS 對於防止 SMB 通訊的攻擊是不夠的
- 因為若沒有標準 NetBIOS 連接埠的話, SMB 將會利用TCP連接埠 445, 即是 SMB 直接主機或「常見網際網路檔案系統 (CIFS)」連接埠。
- 不提供共用資源的機器或網際網路伺服器建議關閉此項功能
- 透過移除 [File and Printer Sharing for Microsoft Networks] 來停用 SMB。關閉TCP 445



實例應用-使用者及電腦規範

範例:微軟系統漏洞修補



從以下的表格，我們可以清楚的看出影響網路安全的幾個因素。

	技術層面	社會層面 (使用者)
無心之過	軟體設計不良、當機、病毒	忘記密碼、人為疏忽
惡意為之	密碼破解、病毒、木馬	駭客、職員故意破壞

Q&A 問題與討論



簡報完畢，敬請指教。