常見系統漏洞與防護策略

宏碁電子化服務事業群
安全技術與管理處

資深技術經理 黃瓊瑩

ISSAP, CISSP, CISA, CISM

講師介紹

現任	宏碁電子化資訊管理中心 安全技術與管理處　資深技術經理
學歷	英國曼徹斯特科技大學　碩士
年資	13 年
專業資格	ISSAP 認證合格 (國際資訊安全系統架構專家) CISSP 認證合格 (國際資訊系統安全專家) CISA 認證合格 (國際資訊系統稽核師) CISM 認證合格 (國際資訊安全管理師) AT&T Bell Lab 資訊安全技術移轉訓練結業 NFR 入侵偵測技術移轉訓練結業 IDI VPN 技術移轉訓練結業 Verisign 資訊安全營運中心建置、營運訓練結業
專業經歷	1. 某國家級資訊安全營運中心技術長 2. 異康股份有限公司安全技術部專案經理、協理 3. 資訊工業策進會副工程師、工程師、系統安全中心專案經理，分項計畫主持人 4. 國軍 Web Mail 安全機制整合研發專案負責人 5. 國軍 VPN 技術移轉專案負責人 6. SSL 前瞻性性資訊技術研發並技術移轉中華電信研究所 7. PKI 憑證管理中心(Certificate Authority)系統研發並技術移轉中山科學研究院 8. 金融交易安全系統研發
專長	密碼學、入侵偵測技術、資安事件應變處理、資安事件鑑識

二十項相關國際認定重要弱點

- ☑ 分為主機弱點與個人電腦弱點　　10 分鐘
  - 個人主機弱點與補強方法
- ☑ 基本資訊安全守則　　10 分鐘
- ☑ 主機弱點與補強方法　　重點說明
- ☑ 資料來源
  - 國家資通安全會報技術服務中心
  - **SAN Institute**

Nimda 弱點

- 問題描述:
  - 此病毒的主要破壞行為是透過電子郵件大量散播夾帶檔名為Readme.exe的電子郵件，造成網路頻寬的壅塞，使用者將明顯發現網路的速度變慢。
  - 病蟲會透過多重感染管道在網路上大量散播
    - 收取包含該病毒的E-mail 而感染
    - 瀏覽受駭網頁而感染
    - 開放資源共享而感染
    - 有漏洞的IIS 主機遭病毒入侵
- 修正方式:
  - 執行Nimda病毒清除程式
    - 賽門鐵克的清除程式為fixnimda.com
      - http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.removal.tool.html
    - 趨勢的清除程式FIX_NIMDA4.0.COM
      - http://www.trend.com.tw/corporate/techsupport/cleanutil/index.htm
  - 將C:\WINDOWS\SYSTEM.INI 檔案中的SHELL=explorer.exe load.exe -dontrunold 改成 SHELL=explorer.exe
  - 移除不必要的資源分享，並對實際需要的資源分享設定
  - 嚴格的密碼，最好是將需分享的資源隱藏起來(在分享目錄名稱最後加上$)
  - 將administrator 群組中的guest 帳號移除掉(如果有的話)。
  - 安裝 IIS 修正檔(MS01-20,MS01-44)
    - http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
    - http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
  - 安裝防毒軟體，修補漏洞
- 影響系統
  - Windows 2000 SP4以後無此問題

感染Nimda的線索

- 根目錄下存在 admin.dll，可能包含的路徑有 C:\、D:\、E:\、…等，其檔案大小約為 57K。
- 電腦中存有 readme.eml(有少數受感染電腦中存有 readme.wav 或 readme.com)。
- 在“C:\Windows\Temp” 目錄下存 mepXXXX.tmp.exe 這個檔案(XXXX 為任意字元)。
- 電腦的系統目錄中有 load.exe，且大小通常為 57344 bytes。
- 電腦中的 riched32.dll 檔案大小為 57344 bytes。
- 不預期的資源分享被開啟，比如將根目錄(C:\, D:\,E:\, ...)分享出來，而且不設權限。
- IIS Log 中有如下的紀錄:(x.x.x.x 為 IP 位址)/c+tftp%20-i%20x.x.x.x%20GET%20Admin.dll%20d:Admin.dll 200。
- 在 wininit.ini 中有 mepXXXX.tmp.exe 這個字串(XXXX 為任意字元)。
- 在 system.ini 中出現一行:Shell = explorer.exe load.exe –ontrunold。
- 新增一個 guest 使用者，並且其權限為 Administrator。
- 網頁(通常是首頁)有一段 JavaScript，通常藏在網頁的最下方，而各種形式的網頁檔案(html, htm, htt,, asp, shtml, shtm)都有可能。

未設定安全密碼之微軟系統弱點

- 問題描述:
  - Windows主機使用Server Message Block (SMB)協定，或稱為Common Internet File System (CIFS)的協定
  - 密碼設定不夠安全或是未設定密碼,常讓外界使用者經此網路芳鄰分享，洩漏區域網路內相關檔案或系統上的機密資訊
- 修正方式:
  - 遵照之密碼原則設定，強化密碼之複雜度.
    - 密碼中應至少含有以下四種中的三種：
      - 英文小寫字母
      - 英文大寫字母
      - 數字
      - 特殊字元：如!、$、*等
    - 長度應為8 個字元以上，並且避免選擇字典中可找到的簡單字之組合。
    - 好的密碼範例
      - !D0ct0r$
  - 不需要共用，最好立即取消
  - 如需共用，預設係設為everyone完全控制
  - 需先移除everyone權限，再新增使用者並設定權限

Windows 遠端登錄資料存取

- 問題描述:
  - **Window做作業系統使用register key 登錄資料庫,管理系統上的設定,主機的行為,使用者環境等重樣資訊**
  - 許多病毒皆會修改**register key ,使得該系統在充新開機後會自動執行**
- 修正方式:
  - 將來自Internet，對系統的port 139(tcp)及445(tcp)等ports 的連線請求，以防火牆阻擋。避免來自Internet 的攻擊者得以存取系統上的register key。
  - 安裝防毒軟體

Microsoft RPC DCOM 弱點(MS03-026)

- 問題描述:
  - 微軟的RPCSS(Remoterocedure Call-遠端程序呼叫)含有緩衝區溢位弱點 (MS 03-026)
  - 攻擊者可利用此弱點在未經授權下,透過網路於有弱點的系統執行任意程式碼,或對系統發動阻斷服務攻擊
  - RPC Dcom Worm 即msblaster 疾風病毒既為利用此弱點的電腦蠕蟲
- 修正方式:
  - 安裝MS 03-026修補程式.Microsoft RPC DCOM弱點 MS 03-026)
    - http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp
  - 使用自動檢測安裝此修補程式Windows Hotfix – KB823980. 以Windows Update 即可
  - 對於Windows RPC 所用的port 135(tcp/udp)，請使用防火牆之類的設備阻擋來自Internet 的存取，若發現內部網路由不斷對外發出port 135請求，也可能是內部有機器受此蠕蟲感染的徵兆。
  - 對於此worm 所安裝的後門程式所使用的port 4444也應該阻擋，而為求安全起見，應該連網芳所用的port 139(tcp/udp)及port 445(tcp/udp)也阻擋。
  - 安裝防毒軟體，修補漏洞
- 影響系統
  - Windows NT、2000、XP與Server 2003。

常見的資訊安全威脅

- 威脅(threat)是任何會直接導致資訊資產受到損害的事
- 常見的資安事件威脅：
  - 惡意程式碼的攻擊(病毒)
  - 入侵破壞(網頁竄改)
  - 刺探或掃描
  - 阻斷服務攻擊(DoS)
  - 間諜活動(公司機密資料，如IC設計圖…等)
  - 欺瞞、詐騙及竊取(客戶名單資料)
  - 未授權資料存取，或未授權的利用服務(內部資訊外洩)
  - 系統或軟體漏洞

一般資訊安全問題

- 所以我要注意什麼 ???
  - 考慮以下狀況
    - 使用攜帶型資訊設備
      - 加密
      - 竊取
      - 遠端存取
    - 列印文件或使用傳真的機密性
    - 使用桌上型 PC
      - 組織的政策
      - 使用警覺性
    - 使用E-mail
      - E-Mail使用政策
      - 不亂給E-Mail Address
    - 防範病毒

一般資訊安全問題

- 所以我要注意什麼 ???
  - 考慮以下狀況
    - 個人資料備份:
    - 辦公室進出管制
    - 非法軟體管制
      - 法律因素：隱私權與智財權
      - 惡意程式、病毒的防範
    - 資安事件通報
      - 甚麼事件該通報？ C.I.A.
      - 如何通報？
      - “Make sure” 是指定的通報對象，查證對方身份
      - 確認得到處理結果的回覆

攜帶型資訊設備資訊安全問題

- ☑ 機場飯店等公共場所有沒有注意不離身
- ☑ 有沒有將資訊設備留置於車內
- ☑ 下班時有沒將資訊設備放入辦公室櫃子並上鎖
- ☑ 在辦公室使用時有無使用專用的固定裝置(ca
- ☑ 必要時有沒有將攜帶筆記型的手提袋經過偽裝
- ☑ 對於硬碟中的資料有有採取適當的加密保護
- ☑ 遠端存取公司內部網路時，有沒有注意不同時連接其它網路或Internet

列印或傳真設備之資訊安全問題

- 機密資料有沒有依照專用的機器，專用的紙張，專用的顏色及專人管理的方式處理及收發
- 列印、傳真設備有無實體控管
- 有沒有立刻至列印或傳真設備
  - 監督處理過程並領走文件

Email之資訊安全問題

- 有沒有使用**auto reply**功能
- 是否瞭解**E-mail**不保密，不透過**E-mail**談論機密事務
- 是否瞭解附帶執行檔的危險性,不開啟執行檔
- 是否傳布未經證實的消息
- 是否回答陌生人的**E-mail**

桌上型PC之資訊安全問題

- 有沒有遵守螢幕淨空及桌面淨空的原則
- 有沒有注意旁邊是否有人在觀看
- 對於可攜式儲存設備之使用是否符合公司的規範
- 對於Modem的使用是否符合公司的規範
  - 在公司內部對外撥接時有沒有先切斷與公司內部的網路連線
- PC送修或暫時移出辦公室時有沒有先將重要資料及電子郵件備份
  - 有沒有將機密資料及電子郵件刪除
  - 有沒有清空資源回收筒
  - 有沒有將電子郵件帳號移除
  - 是否需要將可登入公司網路的帳號暫停
  - 有沒有清空流覽器中的Cache及cookie
- PC送回時有無立即檢查軟硬體及檔案
  - 是否有新增或改變
  - 有沒有立刻更改密碼

個人資料之資訊安全問題

- 個人資料備份:
  - 有沒有定期備份
  - 有沒有確定可以回復
  - 備份有沒有存放在安全的場所
- 帳號密碼保護
- 個人隱私資訊

辦公室之資訊安全問題

- 辦公室進出管制
  - 如果有人尾隨進辦公室 該如何處理
  - 不要只由一個人代表簽辦進出,形成漏洞
  - 最好有兩重管制：大門門禁，部門門禁
  - 對於穿制服的人員，有沒有提高警覺
  - 是否會主動幫陌生人或攜帶東西的人開門
  - 主動詢問可疑的人事物

電腦病毒的醒思

- 電腦病毒都是有害的嗎？
- 病毒利用的漏洞，也可能被駭客所利用？
- 如果沒有電腦病毒，漏洞可能永遠存在？

歸納相關弱點

- 網頁(IIS or Apache)漏洞
- SSH連線漏洞
- 密碼強度不足
- RPC(Remote Process Call)漏洞
- 其他…SMTP, SNMP,DNS …

個人資訊安全防護要務

- 安裝防毒軟體
  - 需要啟動病毒碼自動下載機制，確保病毒碼為最新版本
- 確實安裝修正程式，補強系統漏洞
- 確實使用強健密碼
- 非必要不分享檔案、硬碟給網路芳鄰

主機弱點與補強方法

IIS worm 弱點

- 問題描述:
  - 使用沒有安裝修正檔的IIS系統及版本7以及以上的Solaris系統
  - 網蟲使用兩個著名的漏洞來攻擊系統以及置換網頁. (MS00-078. MS00-057)
- 修正方式:
  - 若系統上有Root.exe程式的話,將其移除
  - 安裝修正檔,可在微軟網站取得修正檔
  - (MS00-078. MS00-057)
  - http://www.microsoft.com/technet/security/bulletin/MS00-0
  - 78.asp
- 影響系統
  - **Windows 2000 SP4以後無此問題**

CodeRed 弱點

- 問題描述:
  - **CodeRed 為利用 IIS Indexing Service DLL弱點惡意程式碼**
  - 利用IIS伺服器所產生的安全性漏洞導致此一網蟲能輕易入侵沒有修補過的**IIS WEB** 伺服器
  - 可讓攻擊者得以執行系統上的任意程式
- 修正方式:
  - 下載微軟對此病毒的清除程式， 名稱為**coderedcleanup.exe**
    - **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31878**
  - 安裝 **IIS** 修正檔**(MS01-33,MS01-44)**
    - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp
    - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp
- 影響系統
  - **Windows 2000 SP4以後無此問題**

FrontPage Server Extension (FPSE) 無權限控管弱點

- 問題描述:
  - **FPSE**為微軟所提供之遠端網站管理程式，管理者可在有安裝**FrontPage**的遠端機器上，直接修改**IIS**伺服器上之網頁。
  - 未正確設定存取權限，會使惡意使用者可在未經授權的情況下，任意修改該**IIS**伺服器上之網頁。
- 修正方式:
  - 若系統不需使用**FPSE**，請將其移除
  - 若需使用**FPSE**，請設定適當權限
  - 若此系統需使用FPSE，請設定適當權限。將網頁所在目錄(C:\Inetpub \wwwroot)及FPSE 使用目錄 之Everyone 權限設成只允許“讀取及執行、清單資料夾內容與讀取”。
  - 系統上不要有不需要之帳號，必須之帳號則需設定強健之密碼。
- 影響系統
  - **Windos IIS Server**

Apache Chunked 弱點

- 問題描述:
  - Apache web server當收到以Chunked方式編碼的資料，會產生buffer overflow情況結果會造成攻擊者可以執行系統上任意程式的弱點
  - 發生在Apache 1.2.2即以前的版本，或是Apache 1.3到1.3.24的版本，或Apache 2.0到2.0.36的版本
- 修正方式:
  - 下載Apache chunk 弱點的偵測工具進行偵測
    - http://www.eeye.com/html/Research/Tools/RetinaApacheChunked.exe
  - 升級Apache版本，或是安裝各作業平台維護廠商或團體所提供的修補程式。
    - 升級到Apache 1.3.26 或之後的版本，或是Apache 2.0.39 或之後的版本http://www.apache.org

OpenSSL OverFlow 弱點

- 問題描述:
  - **OpenSSL 0.9.6d及0.9.7-beta2之前的版本，存在緩衝區溢位的弱點，攻擊者可利用此弱點獲取系統上的shell，進而執行任意命令。**
  - **Apache/mod_ssl Worm (Slapper worm)的電腦蠕蟲，會透過使用OpenSSL的Apache伺服器感染網路上的主機，並進而達到分散式阻斷服務 (DDoS) 攻擊。**
- 修正方式:
  - 升級至最新版之**OpenSSL,**級至最新版之OpenSSL，可至http://www.openssl.org 下載。
  - 安裝**Service Pack**

DNS zone transfer 弱點

- 問題描述:
  - DNS server 上註冊的資訊，含有單位內的 hostname 與 ip 的對應資訊，對於洩漏這些資訊可能導致攻擊者可以進一步判斷攻擊的目標
  - 攻擊者藉由DNS zone transfer 的 request 可以獲得此 DNS server 上註冊的資訊(其中亦可能含有主機名稱的內部對應 ip 資訊)
- 修正方式:
  - 限制可執行DNS zone transfer 的對象
- 影響系統
  - (NT 4.0)

IIS Sample 弱點

- 問題描述:
  - **IIS Sample** 是**IIS** 在一開始安裝後所提供給使用者的範例。然而在這些範例裡面卻存在著許多安全上的漏洞，包括了一些**CGI**的**script** 等等。一般來說都用不到這些**Sample**，所以建議一並將之移除。
    - **http://hostname/iisamples/exair/search/advsearch.asp**
    - **http://hostname/iisamples/exair/search/search.asp**
    - **http://hostname/iisamples/exair/search/query.asp**
    - **http://hostname/msadc/Samples/SELECTOR/showcode.asp**
    - **http://hostname/iisamples/exair/howitworks/codebrws.asp**
- 修正方式:
  - 提供服務之主機不要安裝範例程式，將所在目錄**iisamples/** 及 **msadc/Samples/** 移除

IIS 5.0 WebDAV overflow 弱點(MS03-007)

- 問題描述:
  - Microsoft Windows 2000有一個名為ntdll.dll 的動態連結資料庫(DLL)中有一個緩衝區滿溢(buffer overflow)的安全弱點
  - 攻擊者可以藉由傳送一個假造 的 WebDAV 請求給 IIS 伺服器而以 LocalSystem 的權限執行任意程式碼， 等於給攻擊者完整的系統控制權。
- 修正方式:
  - 安裝修補程式：ms03-007 sp3之hotfix
  - 檢查win2k 安裝sp4 即可
- 影響系統
  - Win 2000 Server

MS-SQL2000 與 MSDE 2000 之 Slammer worm 弱點

- 問題描述:
  - Slammer worm利用的為Microsoft security bulletin MS 02-039及MS 02-061上所提的弱點
  - 攻擊者可藉由送出特殊封包至**MS SQL 2000**或**MSDE 2000**的**port 1434(UDP)**的**Resolution Service**，得以產生**DDoS**的情況，導致效能降低。
- 修正方式:
  - 安裝 **MS-SQL2000** 與 **MSDE 2000** 修補程式阻檔
  - 關閉非必要的**SQL**通訊埠
  - 使用防毒軟體

MS-SQL 預設帳號密碼之弱點

- 問題描述:
  - SQL 7或是SQL 2000在安裝的過程中，皆可能產生SQL上存在帳號為sa，密碼為空的情況

- 修正方式:
  - sa帳號之預設為空，改設具強度之密碼
  - 如Authentication設為windows可存取對於本 機帳號administrator之密碼，應設具強度之密碼

FrontPage Server Extension (FPSE) 密碼偵測

- 問題描述:
  - 對於**FPSE**設定不安全密碼
  - 對於**FPSE**未做密碼權限設定
- 修正方式:
  - 遵照密碼強化原則設定，強化密碼之複雜度
  - 對於本機帳號**administrator**之密碼，應設具強度之密碼
  - 檢查本機是否有非必要之帳號，將其停用

Microsoft RPC DCOM 弱點(MS03-039)

- 問題描述:
  - 微軟的**RPCSS(Remoterocedure Call-**遠端程序呼叫)含有緩衝區溢位弱點
  - 攻擊者可利用此弱點在未經授權下,透過網路於有弱點的系統執行任意程式碼,或對系統發動阻斷服務攻擊
- 修正方式:
  - 安裝**MS 03-039**修補程式.**Microsoft RPC DCOM**弱點 **MS 03-039)**
  - 使用自動檢測安裝此修補程式**Windows Hotfix – KB824416.** 以**Windows Update** 即可

Cisco IOS Dos 弱點

- 問題描述:
  - Cisco IOS 是非常廣泛使用的網路作業系統
  - 攻擊者 利用傳送惡意IPv4 封包(protocol type 為53、55、77或103)給一個有弱點的設備上的界面，將造成該設備停止處理傳送給該界面的封包，會導至輸入介面的queue buffer被填滿，無法在處理其它封包，造成DoS攻擊。
- 修正方式:
  - 設定ACL (access control list)緩和此弱點的影響。

SNMP 預設 Community Name 弱點

- 問題描述:
  - 攻擊者如果知道可寫入**Community String ,**則可藉此修改網路設定
- 修正方式:
  - 若不需使用**SNMP** 建議將其關閉
  - 若須使用,請設定較複雜**Community ,**並利用防火牆及路由器阻檔**SNMP**所使用的**PORT (TCP 161,UDP 161/162)**

Sendmail Prescan() overflow 弱點

- 問題描述:
  - **Sendmail Prescan()**函數對於攻擊者送來特殊郵件會造成攻擊者得到**sendmail daemon** 權限
  - 弱點存在於**senmail 8.12.10**前的版本

- 修正方式:
  - 安裝各系統所出的**senmail**修補程式

Bind Overflow 弱點

- 問題描述:
  - UNIX 系統上之弱點
  - Bind(Berkley Internet Name Domain)存有緩衝區溢位弱點,可讓攻擊者得到系統上的執行權限(如root權限)
- 修正方式:
  - 安裝新版的Bind
  - 各系統的修補程式