92 年第三季 偵測弱點之說明修補方式

一、未設定安全密碼之微軟系統弱點

1. 簡要說明

Windows 主機使用 Server Message Block (SMB)協定，或稱為 Common Internet File System (CIFS)的協定，使 windows 主機可以將另一 Windows 主機目錄檔案當成是本機上的目錄檔案使用，即所謂的網路芳鄰分享。而這個協定亦可以用於 Internet 網段，即位於不同網段的 Windows 主機也可使用此協定進行目錄檔案的分享(假如傳送過程中未有其他的網路設備阻擋時)或是遠端管理功能用途。

雖然 SMB 協定具有相當的便利性，但設定不夠完善的 Windows 主機(如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，甚至讓網路駭客完全控制該部主機。譬如 2001 年中的 Nimda 病毒就是經由網路芳鄰的方式散佈病毒至另一台保護不週(密碼設定不夠安全)的 Windows 主機上，以致造成感染病毒的速度加快。此外亦常見病毒在其中含有網芳密碼猜測的功能，以利其散播。

2. 檢測方法

技服中心將針對網芳密碼強度使用檢測工具進行檢測，檢測是否得以測到不安全的密碼，關於密碼設定的原則，特別是對於系統上的重要帳號，例如管理者的帳號，務必嚴格設定，而原則則是密碼中應至少含有以下四種中的三種：(1)英文小寫字母、(2)英文大寫字母、(3)數字或(4)特殊字元：如!、$、*等，而長度則應為 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。

3. 解決方法

(1) 阻擋非必要的網芳分享：

特別是對於來自 Internet 的連線請求，建議與以阻擋。阻擋方式為使用防火牆設定僅有需要的 ports 才開放(如 IIS 所使用的 port 80)，而關閉網芳或 Windows 遠端管理所使用的 ports(如 port 135、137-139、445)。另不論是否關閉上述的 ports，仍需設定安全之密碼。

(2)密碼設定方式：

建議將 Windows 系統上的帳號設定成符合密碼設定原則的密碼。

(a) NT 4：

可直接同時按下 Ctrl+Alt+Del，在其中可以輸入欲變更密碼之帳號，輸入舊密碼後即可輸入新密碼。或是從<開始>→<程式集>→<系統管理工具(公用)>→<網域使用者管理員>→<本機使用者與群組>，在其中選取使用者並設定新密碼即可。

(b) Windows 2000

可直接同時按下 Ctrl+Alt+Del，在其中可以輸入欲變更密碼之帳號，輸入舊密碼後即可輸入新密碼。或是從<開始>→<程式集>→<系統管理工具>→<電腦管理>→<本機使用者與群組>，在其中的使用者選取

欲變更密碼之帳號，設定密碼即可。若是 Windows 2000 professional 版，則其<系統管理工具>位置與 Windows 2000 server 不同，請由<控制台>中選取。或者直接在<控制台>中選取<使用者與密碼>設定系統上帳號的密碼。

註：依據越簡單越容易管理的原則，請檢查系統上的是否存在有不必要的帳號，尤其是屬於 Administrator 群組的帳號，更須檢查是否有非必要之帳號。另若系統是屬於網域控制站(Domain Controller)的話，亦可使用其中的密碼設定原則，設定網域成員(Domain member)上的密碼複雜度。反之若系統是屬於網域成員(Domain member)的話，同樣可由網域控制站來設定其密碼複雜度。

4. 參考資訊

http://www.sans.org/top20/#W7

二、MS-SQL 2000 與 MSDE 2000 之 Slammer worm 弱點

1. 簡要說明

在大約今年一月 24 日左右，網路出現專門攻擊 MS SQL 2000 與 MSDE 2000 的 worm—Slammer worm。其攻擊未安裝修補程式的 MS SQL 2000 與 MSDE 2000，它會感染至有弱點的主機，並使該主機繼續送出大量攻擊封包至其他主機，試圖散佈至其他主機，而在短短幾天內造成嚴重的網路壅塞的問題。在 MS SQL 2000 中使用所謂的 Resolution Service 使得在同一台主機上可以同時有多個 SQL server 的 instances。其中第一個 instance 使用 port 1433，其他的 instance 則使用動態的 port number，當 MS SQL client 欲與 MS SQL 連線時，首先連至 port 1434 (UDP)的 Resolution Service，由其告知使用者欲連線的 instance 使用何 port。此 worm 所利用的為 Microsoft security bulletin MS 02-039 及 MS 02-061 上所提的弱點，即在 Resolution Service 下，存有 keep alive 的機制區別 instance 的狀態。然而此機制存在 DDoS 的弱點，亦即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。

2. 檢測方法

由於 MS SQL 2000 與 MSDE 在安裝修補程式後，會有不同的行為，因此可據此進行偵測，技服中心將依據測試封包回應的不同，判斷有無弱點。另外亦可判斷在主機上的\MSSQL\Binn 目錄(可能位於 C:\Program Files\Microsoft SQL Service\MSSQL\Binn)下的 ssnetlib.dll 檔案的版本，若是版本是 2000.80.636.0 或之後(如 2000.80.760.0)的版本，則代表系統已經安裝了修補程式。若是這個檔案的版本是比 2000.80.636.0 這個版本還舊的話，則代表系統尚未安裝修補程式。

3. 解決方法

(1) 阻擋非必要的 MS-SQL 通訊埠的開放

MS-SQL 2000 與 MSDE 2000 使用 port 1434(UDP)作為不同資料庫的狀態溝通用途，而這也是 slammer worm 入侵所用的 port，因此避免 Slammer worm 的感染，可考慮阻擋 Internet 對 port 1434(UDP)的連線。

(2) 安裝 MS SQL 2000 與 MSDE 的修補程式

安裝關於 MS SQL 的最新修補程式，關於 MS SQL 的修補程式皆可在此網址下載，http://www.microsoft.com/sql/(目前 MS SQL 2000 的最新修補程式為 Service Pack 3a)。另外該網站亦有介紹關於 MS SQL 的設定與安全議題，亦可參考。

(3) 使用防毒軟體

若是懷疑系統上有 Slammer worm 的感染的跡象，請參考防毒公司網站關於此 worm 的清除工具。

參考：

http://securityresponse1.symantec.com/sarc/sarc.nsf/html/w32.sqlexp.worm.html
http://www.trendmicro.com/vinfo/zh-tw/virusencyclo/default5.asp?VName=WORM_SQLP1434.A

4. 參考資訊

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-039.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-061.asp
http://www.microsoft.com/sql/

三、 MS-SQL 預設帳號密碼之弱點

1. 簡要說明

MS-SQL 為微軟的資料庫產品，不論是 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(雖然安裝過程中系統會提醒將 sa 帳號設定密碼，但仍然可以不設密碼)，另外在系統上安裝其他應用程式的情況下，也可能出現預設帳號密碼的情況，在攻擊者獲得 SQL 帳號密碼時，他可獲得、修改或刪除系統上資料庫資訊，另外由於 MS-SQL 預設支援執行系統上指令(像是執行系統上的 MS-DOS 模式，或是看系統上的 register key 等等)的功能，因此攻擊者在獲得 MS-SQL 的帳號密碼後，也可能有機會使用此功能。

2. 偵測方法

技服中心將使用 MS-SQL 預設之帳號 sa 與空密碼，或是預設之帳號與密碼直接與 MS-SQL 進行連線測試。若得以順利連線，代表 MS-SQL 上的預設帳號：sa，存在有空密碼與預設密碼的問題。

3. 解決方式

(1) 阻擋非必要的 MS-SQL 通訊埠的開放

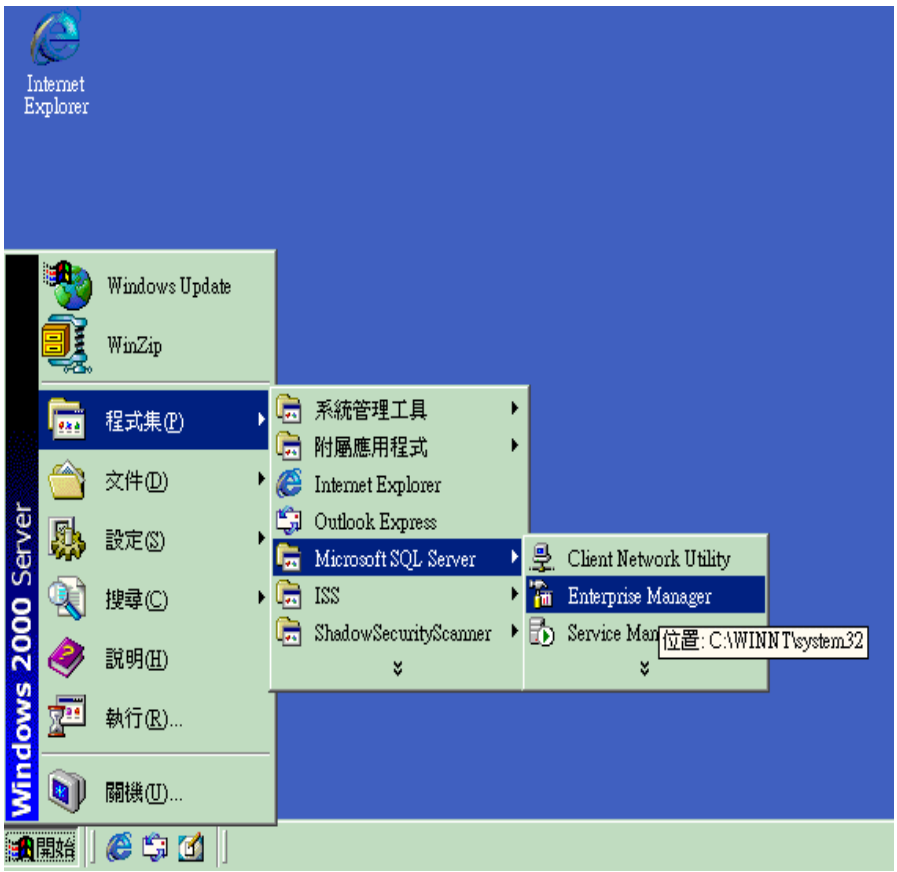
由於 MS-SQL 所使用的 port 為 1433(TCP)，另外若是 MS-SQL 2000 的話，則額外有 port 1434(UDP)作為不同資料庫的狀態溝通用途，而 port 1433 即是 MS-SQL 作為連線所使用的通訊埠，因此若是 MS-SQL 主機的 port 1433 不需要遠端管理的話，建議以防火牆將來自 Internet 至 port 1433(TCP)的連線請求與以阻擋。另外 port 1434(UDP)也建議阻擋，像今年初的 slammer worm 便是經由 port 1434(UDP)散播的。

(2) 設定 sa 帳號的密碼

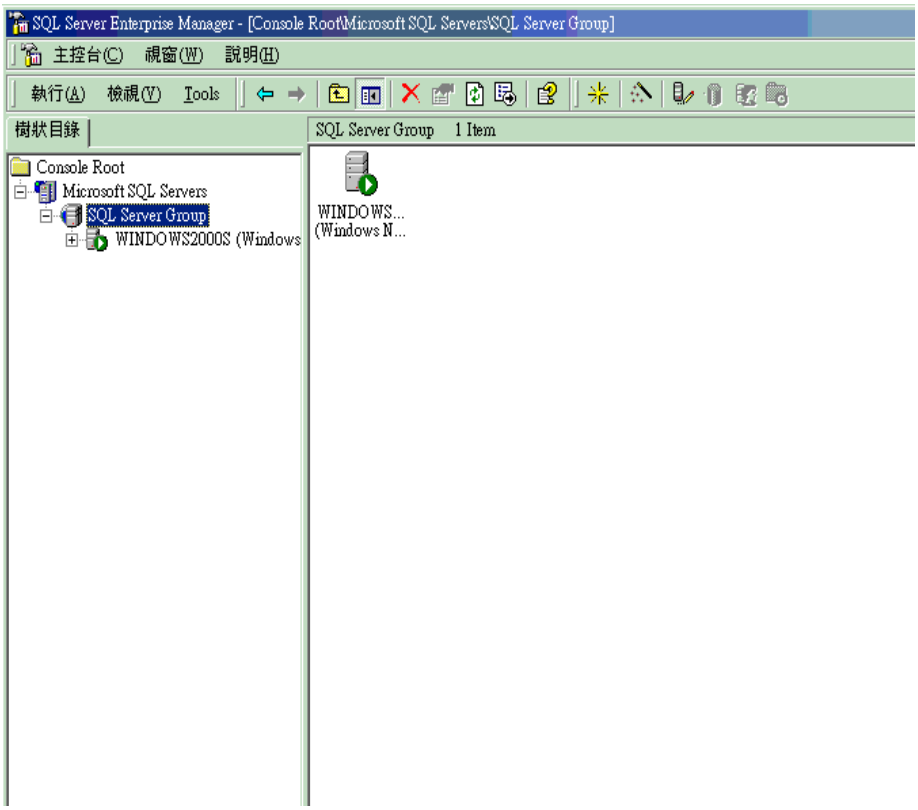
就算已經阻擋了來自 Internet 對 port 1433 的連線請求，但仍然應該為 MS-SQL 的 sa 帳號設定密碼，設定的方式為：

(a) SQL 2000：

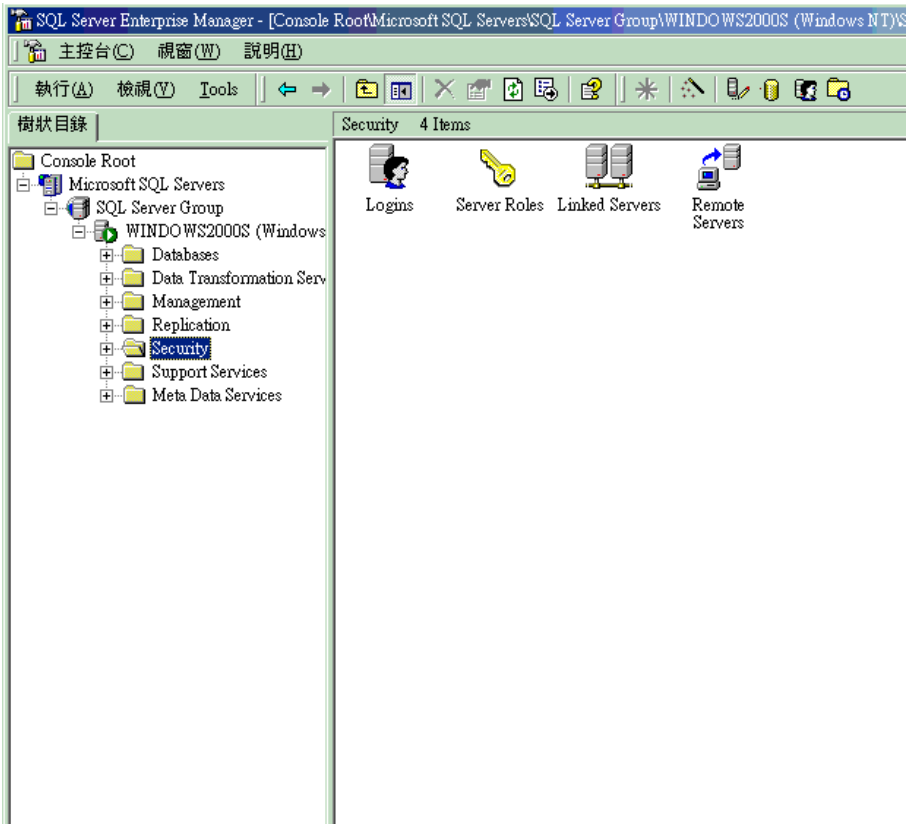
<I>開啟 SQL 的 Enterprise Manager



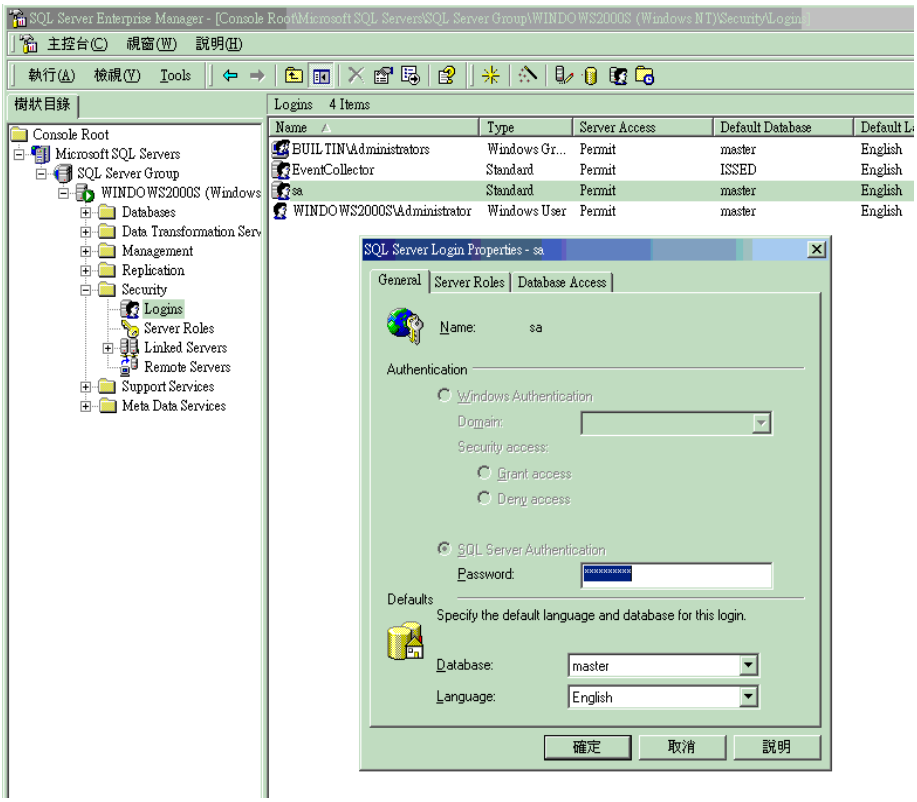
<II>選擇其中的 SQL Server Group



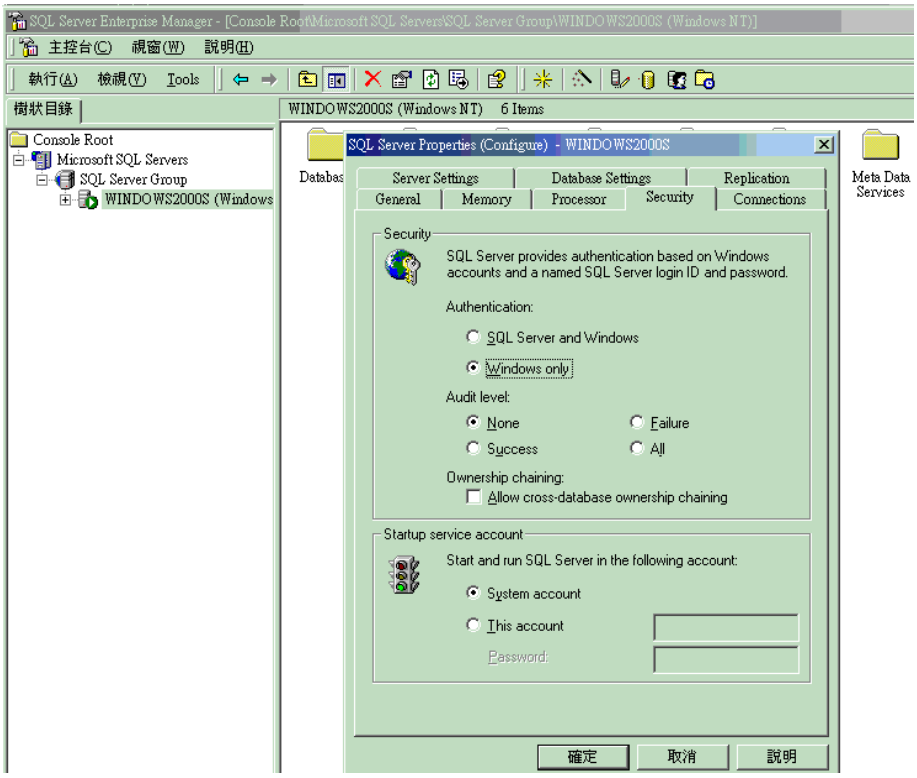
<III>選取欲變更密碼的資料庫，並選擇其中的 security



<IV>選取 Logins，選取 sa，並設定密碼。



註：另外雖然 MS-SQL 可以接受使用 sa 帳號進行與 MS-SQL 連線或是使用 windows 系統上帳號進行連線，但依據微軟的建議，建議使用 windows 系統帳號進行連線，設定方法為，在資料庫內容直接按滑鼠右鍵選內容，在其中點選 security，在 Authentication 中選擇 Windows Only。



(3) 更新 MS-SQL 的修補程式

參考以下網址進行 MS-SQL 的設定與修補程式的安裝。目前 SQL 7 最新的為 service pack 4，SQL 2000 最新的是 service pack 3a。

http://www.microsoft.com/sql/

4. 參考資訊

http://www.microsoft.com/sql/

四、Front Page Server Extension(FPSE)密碼偵測

1. 簡要說明

延續本中心於今年(2003 年)第一季針對 FPSE 未設定密碼的偵測，因當時並未針對設定不安全密碼的情況進行偵測，以致仍有許多設定不夠安全的情況存在，技服中心將在本季的弱點掃描中加入 FPSE 密碼設定不夠安全的偵測，期望大幅減少不安全的 IIS 伺服器(有 FPSE 支援者)。

2. 檢測方法

針對有 FPSE 支援之 IIS 伺服器，技服中心將使用帳號：Administrator 及若干簡單密碼組合，進行系統登入測試，若得以順利登入。並具有足夠的權限進行網頁更換，則代表系統上的 FPSE 具有權限設定不夠安全的問題。

3. 解決方法

關於解決此問題，可分為兩個方式：

(1) 移除 FPSE：

關於移除的方式請參考 92 年第一季的偵測弱點之說明與修補方式(92 年

第 1 季)，網址為：http://www.icst.org.tw/template/ncert/leakrepair.zip

並請在移除後檢查系統是否仍有"_vti_bin"目錄存在(建議使用<開始>→<搜尋>找尋)，若有則代表 FPSE 仍未移除，此時可再重新移除，或者將"_vti_bin"移掉，或是更換該目錄名稱，如將"_vti_bin"換成"_vti_bin_remove"或其他的名稱，亦可使得 FPSE 無法使用。

(2) 設定 FPSE 使用目錄之"everyone"群組之權限，並設定系統使用者(尤其是 Administrator 帳號)的密碼：

其中設定 FPSE 使用目錄之"everyone"群組之權限在防止 FPSE 允許任何人可以不輸入帳號密碼的情況及登入 FPSE。關於"everyone"群組之權限建議設成僅有"讀取"、"執行"、"清單資料夾的內容"的權限，亦即僅給"everyone"群組有最小可接受的權限。(設定細項同樣請參考偵測弱點之說明與修補方式(92 年第 1 季))至於設定系統使用者的密碼則是防止使用者設定不安全的密碼，導致 FPSE 雖然要求使用者輸入密碼，但是使用者仍然輸入空密碼或是簡單的密碼即可登入。因此需要對系統使用者設定安全的密碼，防止網頁內容遭竄改。

4. 參考資訊

http://www.icst.org.tw/template/ncert/leakrepair.zip