Windows 主機網路芳鄰分享(NetBIOS—Windows network shares)之安全隱憂

一、說明

Windows 主機使用 Server Message Block (SMB)協定，或稱為 Common Internet File System (CIFS)的協定，實現 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一般地使用，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)。

二、可能產生之安全問題

鑒於 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的 Windows 主機上，以致造成感染病毒的速度加快。所以經由開放網路芳鄰分享於外界使用者，來增加與其他單位(如所屬機關、外部辦公室或駐外機構)的聯繫方便，同時亦可能形成安全上的漏洞，尤其是對保護不週的 Windows 主機而言。

三、建議補強方法

（一）對於不需要的網路芳鄰分享建議取消，若主機不需要網路芳鄰分享協定時，可將主機內有關”file and printer sharing for Microsoft network” 網路設定功能取消。

（二）對於內部區域網路(LAN)作檔案分享時始開啟網路芳鄰存取功能，對於 Internet 的檔案分享建議使用 FTP 或 HTTP 的方式存取。同時開啟網路芳鄰功能亦應遵循下列原則：

1.對於需要分享的目錄一定要設定存取權限控制，禁止未有密碼保護的網路芳鄰分享。設定之密碼應符合同時包含有英文大小寫，特殊字元且長度在 8 個字元以上。

2.將需分享的檔案集中在同一目錄下，並僅開放讀取的權限，除非必要不要開放寫入的權限。

（三）為阻斷 Internet 使用者透過網路芳鄰功能存取區域網路內 Windows 主機相關檔案資訊，建議使用 firewall 等相關軟硬體阻擋外界對內部主機的 port 137-139(Transmission Control Protocol, TCP 與 User Datagram Protocol, UDP)，及 port 445(TCP 與 UDP)存取權限。

（四）除非特殊必要，始開放 Internet 分享網路芳鄰功能，並在所在網段的出入節點(如 firewall)限制可以連入有網路芳鄰分享的主機的來源 IP(建議避免使用 hostname 方式辨認，因 hostname 較容易被偽造)。

四、參考資訊：http://www.sans.org/top20/。