高中電腦科教師電腦網絡培訓課程

電腦網絡學習平台

第六節

如對本課程有任何意見或投訴，請聯絡
課程管理委員會電話 2136-1936 或電郵至
supervisory@welkin.com.hk

Should you have any comment or complaint on
our training courses, please contact our
Training Administration Committee at 2136-1936 or email to
supervisory@welkin.com.hk

目錄

1. 網絡的安全威脅

1.1. 網絡安全的由來

爲什麼需要顧及網絡安全？試想想以下幾則事例：

機密性 (Confidentiality) - 避免把資訊向未經許可人士披露

例子：你提供給某一個網站的個人資料應只供該公司的指定員工作爲事先同意的用途，其他人士不可出於好奇而取用該等資料，或將之用作非法用途。

完整性 (Integrity) – 避免把資訊被未經許可人士更改

例子：你提供給某一個網站的個人資料不應在數據傳輸過程中或被該網站公司更改。

可用性 (Availability) – 讓資訊可供許可人士在需要時使用

例子：你可自由地存取及檢視寄存於某一個網站的個人資料。

不可否認性 (Non-repudiation) – 提供證據使發件人不能否認曾發出信息，而收件人也不能否認曾收取信息

例子：當你在網上商店進行電子交易時，該商店不能否認曾收取你的訂購指示。

認證 (Authentication) – 辨識、證明用戶身分

例子：當你不想他人使用你的電腦發出信息或存取數據，你可以設定進入操作系統的登入名稱及密碼，以防他人取用你電腦內的數據。

1.2. 黑客

黑客(Hacker)一詞本來是精於電腦技術的人，最初的黑客是一些在電腦程式技術領域中能夠不斷探索並與他人分享成果的人，隨著時代的發展，黑客的性質發生了變化，某些「黑客」借助其技術專長，偷偷進入政府、企業網絡或個人電腦系統，進行不正當的行爲或造成破壞，使得黑客成爲網絡破壞者的同義詞。人們對黑客褒貶不一，畢竟不是所有黑客都以破壞他人系統爲目標。

1.3. 入侵

黑客要破壞他人的電腦或網絡，必須進入其系統或網絡，這種利用非正常手段進入系統的過程稱爲「入侵」 (Intrusion)。

一般黑客入侵的常見管道是系統本身或是使用者設定不當所造成的漏洞。因此，爲了預防入侵，電腦或網絡管理員必須即時修補已知的系統漏洞，並經常測試系統，以發現因設定不當造成的漏洞。

1.4. 木馬程式

木馬程式又稱爲「特洛伊木馬」(Trojan Horse)，泛指黑客植入到他人的電腦的一段程式。利用木馬程式，黑客可以在被入侵的電腦完全沒有察覺的情況下，開啓該部電腦的一扇「後門」，利用這扇門自由進出與存取資料，所以木馬程式也稱爲「後門程式」。

1.5. 病毒(Virus)與掃毒

電腦病毒也是一種程式，只不過這種程式不同於正常的程式，它的特性就像是自然界的病毒，會嘗試不斷複製本身並感染其他電腦，由於這種程式會在電腦與電腦之間傳播，所以一旦病毒發作(即啓動破壞行爲)，所帶來的危害非常大。電腦病毒的特徵包括：

- 隱蔽性：電腦病毒與普通電腦程式不同的地方在於使用者無法輕易察覺病毒程式的存在。即使電腦病毒正在感染檔案或電腦，也不容易發現，只有等到病毒發作，才能發現已「中毒」，但此時系統已經遭到病毒程式的破壞而無法修復。

- 寄生性：自然界的許多病毒通常都寄存於其他生命體中，電腦病毒「寄生」在電腦的檔案或程式中，目的之一是爲了有更好的隱蔽性，二是爲了能夠隨著電腦程式執行來啓動病毒程式。

- 傳染性：所有病毒都具有傳染性，早期的電腦病毒主要透過檔案複製的方式來散播到其他其他的電腦上，代表性的媒介是磁碟、光碟；不過，今日的電腦病毒傳染途徑更多也更快，除了磁碟，利用網絡傳輸的檔案、電子郵件等也會攜帶病毒進行傳播。

- 觸發性：一般的電腦病毒都會設定在某個條件下發作，只要條件符合，病毒就會啓動一連串的行爲，開始執行程式設計初時賦予的目標。

- 破壞性：大部分電腦病毒都具有破壞性，病毒被觸發後，就開始對系統檔案，甚至是硬體進行破壞。過去已知的病毒以刪除檔案及破壞作業系統爲主。曾經赫赫有名的 CIH 病毒，會在每個月的 26 日發作，將主機板上的 BIOS 破壞。

  一般來說，電腦病毒的破壞性分爲以下幾種形式：
  - 刪除檔案：大量刪除硬碟中的資料，造成重要資料無法挽回。
  - 佔用系統資源與記憶體：系統速度變慢，影響工作效率。
  - 破壞硬體：到目前爲止，只有 CIH 病毒造成了實質的損壞。隨著黑客技術提升，未來很難避免類似的攻擊模式。

- 不可預見性：病毒的產生是人們不能預見的，所以任何防毒措施都不可能完全防止病毒感染電腦。

電腦病毒入侵區域網絡的原理：
一般來說，電腦病毒會首先進入到有硬盤的電腦，再進入網絡，然後開始在網上傳播。情形可如下：

1) 病毒直接從工作站電腦拷貝到伺服器中或通過郵件在網內傳播；
2) 病毒先傳染工作站電腦，在工作站電腦記憶體駐留，待運行網絡程式時再傳染給伺服器；
3) 病毒先傳染工作站電腦，在工作站電腦記憶體駐留，在病毒運行時直接通過連接的路徑傳染到伺服器中 ；或
4) 如果遠端工作站被病毒侵入，病毒也可以通過資料交換進入網絡服務器中。

1.6. 蠕蟲

蠕蟲 (Worm)與傳統的電腦病毒有所不同。蠕蟲會利用作業系統和應用程式的漏洞主動進行攻擊。

蠕蟲病毒需要依靠網絡進行傳播，被感染的電腦會耗用大部分系統資源與網絡資源，對網絡的其他電腦發起攻擊，一旦成功感染，該電腦就成爲另一部攻擊主機，這種模式讓病毒迅速擴散，最終癱瘓整個網絡運作。蠕蟲病毒具備傳統電腦病毒所共有的特性，例如傳染性、隱蔽性、破壞性、不可預見性等等。

從觀察過去數個有名的事件可以發現，今後的電腦病毒將會以蠕蟲病毒爲主，並且越來越難以事先防範，預料未來可能發展的趨勢如下：

- 繼續利用作業系統或程式本身的漏洞主動發起攻擊，作業系統的對象是以新版本的 Windows 與其應用程式爲主。2001 年著名的紅色警戒 (Code Red) 蠕蟲使用微軟的互聯網伺服器 (IIS) 漏洞進行入侵，造成重大損失。這種經典的攻擊模式，讓許多蠕蟲病毒起以效尤，而且不斷改進，攻擊形式與修復難度更加複雜。紅色警戒本身不會在硬碟上產生檔案，而是以處理程式的形式存在記憶體當中，並且不斷產生新的處理程序，然後透過網絡尋找具有同樣漏洞的伺服器加以攻擊，最後讓伺服器效能急劇下降，網絡近乎停頓。

- 傳播方式多樣化，最初的蠕蟲病毒主要是透過電子郵件的方式傳播，「求職信病毒」就是一個典型的例子，但蠕蟲病毒已經演化到可以直接感染網絡伺服器，或是在區域網絡中透過共用資料夾傳播。甚至在以電子郵件傳播時，使用者接收郵件後根

本不需開啓附加檔，含有病毒的附加檔會自動開啓及執行，典型的代表爲 Nimda 病毒。

- 與黑客技術相結合，使伺服器或個人電腦在感染電腦病毒後，黑客可以進入系統之中，進行更多破壞。

- 蠕蟲病毒大多使用目前流行的程式語言編寫，容易被人刻意修改成爲全新的電腦病毒，使得病毒變種的速度非常快。

1.7. 混合模式病毒

以蠕蟲、木馬與傳統病毒相互結合形式所產生的新病毒，其預防和移除的難度日益提高。例如數年前曾經轟動一時的「梅莉莎」(Melissa) 便結合蠕蟲與傳統電腦病毒的特性。該病毒會感染 Word 程式的 Normal.dot，而且還會透過 Outlook 大量散播。

1.8. 間諜軟件 (Spyware)

「間諜軟件」是指未經用戶允許的情況下，將用戶網上活動的資料秘密地轉送至別人的這類軟件。這些網上活動資料通常被用作市場推廣，例如針對用戶的上網習慣和喜好，以彈出式視窗、垃圾郵件等形式，向用戶發送個人化的廣告。很多廣告軟件同時也是間諜軟件，會於電腦運行時在顯示器顯示廣告標語。

間諜／廣告軟件通常隱藏於其他軟件並被一起下載至用戶的電腦，其中以互聯網上的免費軟件最爲常見。大部分瀏覽器輔助工具和檔案分享軟件，例如 Kazaa、Xupiter、Grokster 和 Morpheus 等均藏有間諜／廣告軟件。雖然在大多數情況下，這些免費程式的終端用戶許可證協議（EULA）都會說明軟件中的間諜／廣告功能成份，但由於這些聲明冗長複雜，大部分用戶在未閱讀或理解其細節前，便已按了「接受」按鈕。

間諜／廣告軟件也可以在瀏覽網頁時，以流動程式碼的方式，由遠端伺服器傳送至客戶的電腦系統內安裝執行。這些軟件通常聲稱安裝後可增強瀏覽有關網站的效果，開發商也可能以其他不誠實手法欺騙用戶下載。

間諜／廣告軟件的影響一般並不嚴重，但亦不無影響：

個人私隱

記錄用戶的網上活動，例如曾經瀏覽的網站、在搜尋引擎曾經輸入的搜索條件、甚至是信用卡資料或用戶密碼等敏感個人資料。

用戶控制電腦的能力

包括「劫持」瀏覽器設定、安裝不需要的程式及令某些系統功能失效。這樣可能會和合法應用軟件發生衝突或彼此干擾，以及耗用系統資源而最終令致系統性能下降。

系統保安

間諜／廣告軟件本身可能有的保安弱點或會構成新的保安漏洞，令攻擊者有機可乘。一些間諜／廣告軟件也包含了後門功能，讓其開發商可以無聲無息地將版本升級，變相容許開發商可以對受影響的電腦爲所欲爲。而有些間諜／廣告軟件則爲免被一些如個人防火牆等的保安軟件影響其運作，將這些保安軟件的功能關掉。

2. 網絡安全管制策略

2.1. 防火牆

現代都市樓房密集林立，若是失火，將一發不可收拾，爲了防止火災由一棟房子延燒到另一棟，建築師便在房屋與房屋之間建立了一道牆壁，用以阻隔火勢的蔓延，達到保護防火牆內的房屋與財產，這就是防火牆 (Firewall)。

將防火牆的概念套用到網絡環境時，個人電腦或區域網絡就相當於需要保護在防火牆內的房屋財產。防火牆阻隔了互聯網上的黑客或病毒入侵，擔任防火牆任務者，通常是安全驗證的硬體或軟體。

黑客或病毒試圖入侵電腦時，會經過防火牆而被攔截，不能進一步到達電腦上。而正常的網絡資料，防火牆允許其穿透，並到達目標電腦。

一般來說，防火牆有硬體與軟體兩種，對於企業網絡來說，建議採用硬體防火牆。

硬體防火牆效能與防護能力佳，但是價格較昂貴，因此適合企業網絡使用，以滿足區域網絡眾多電腦的防護需求。對於一般的家庭使用者，軟體防火牆符合預算，在效能可以兼顧的情況下，提供硬體防火牆一樣的安全功能。

目前軟體防火牆分爲個人用或企業等級兩種，前者的功能與彈性較小，後者則考慮到防火牆需要另外與網絡服務結合的情況。要求的功能必須更爲強大複雜（例如微軟開發的 ISA）。Windows XP 與 Windows Server 2003 也內建了 一個互聯網連線的防火牆，是微軟提供給 Windows 使用者一個簡單實用、免費的軟體防火牆。

2.2. 加密/解密

儘管有嚴密的防黑客入侵措施，也不能絕對保護電腦的安全。黑客的攻擊手法很多，例如使用網絡竊聽的功能，就可以在不入侵電腦的情況下，獲得電腦經網絡發送的資料。

通常電腦經網絡發送一筆資料後，只有指明的接收者才可以接收該數據包。但在網絡通訊過程中，該數據包會廣播給所有的電腦，只不過其他電腦收到該數據包後發現目的地不是本機，就會將數據包丟棄。開啓了網絡數據包監視軟體(例如 Sniffer)的電腦也會收到此數據包，它不僅會保留也同時進行內容解析，如果資料以明文 (Plain Text) 形式傳送，則網絡監視軟體可直接看到監視軟體中的內容。

在網絡傳輸的資料很可能是機密資料，例如使用者的帳戶和密碼，如果這些東西以明文傳送，一旦黑客截獲這些資料，就能以該使用者的身份登入系統，後果不堪設想。

爲了保護資料的安全，一般會在發送資料到網絡前，對資料進行加密。加密資料的方式有很多種，例如 Windows XP 經常採用資料加密標準(Data Encryption Standard, DES)來加密資料，在發送之前，發送端還需與接收資料的電腦協商，以便接收端獲得發送端加密時的金鑰，協商完成後，發送端才會將加密過的資料透過網絡發送給接收端，此時接收端再利用協商產生的的金鑰解密收到的資料。

常見的加密技術可分爲「對稱式」和「非對稱式」：

- 對稱式加密是指加密和解密使用同一個密鑰 (Session Key)，這種加密技術目前被廣泛採用，例如美國政府所採用的 DES 加密標準就是一種典型的對稱式加密法，它的密鑰長度爲 56Bits。
- 非對稱式加密是指加密和解密所使用的不是同一個密鑰，分別爲「公鑰」和「私鑰」，它們兩個需要配對使用，否則不能開啓加密的檔案。公鑰是可以對外公佈的，而私鑰則只有持有者自己知道。

2.3. 帳戶與密碼

爲了識別使用者身份，大部分作業系統都採用了「帳戶」這個基本的身份識別功能，讓系統知道目前使用電腦的人是誰，應該給他甚麼權利。例如電腦開機進入 Windows XP 系統之前，使用者必須輸入一個使用者名稱，這個名稱就是使用者的帳戶，不同的帳戶對應不同的識別碼 (Identification Code)，系統根據這個唯一的識別碼來判別使用者的身份，決定允許或拒絕他登入系統，以及登入後可以執行的工作內容。

使用者名稱(帳戶)是給人們方便使用與記憶的，而每一個使用者名稱對應的識別碼，是系統真正用來辨識使用者的依據，系統操作者可以對使用者名稱進行變更、刪除或重建，但是識別碼由系統控制，操作者無法得知與變更，而且每一個使用過的識別碼在系統中不會重覆。

除了在登入系統時就需要用到帳戶，離開本機電腦後的很多場合也要用到帳戶，例如連線到網絡上的伺服器、存取伺服器中的檔案、執行程式、安裝硬體驅動程式等等，爲了保護帳戶不被非法使用者濫用，帳戶通常都會搭配一組密碼，所以在登入系統時，除了輸入正確的帳戶，還必須提供與之搭配的密碼，兩者必須吻合系統中的記錄，其中有一個錯誤，都將被視爲非法使用者，試圖登入的使用者都會被拒絕登入，在其他需要提供帳戶的場合也是如此，只要未提供正確的帳戶或密碼，都無法完成正常的操作。

2.4. 身份認證

對於一般家庭網絡來說，並不需要太嚴厲的身份認證機制，使用 Windows 預設的 NTLM 或 Kerberos 認證機制，就可以滿足安全需求。但是對於企業網絡，對於使用者的身份就不能輕忽，所以在條件許可的情況下，他們可能會採用更爲嚴格的 Smart Card、憑證形式的身份認證。

2.5. 預防 間諜／廣告軟件

現時很多防毒產品的最新版本均設有間諜／廣告軟件的檢測和移除功能；用戶亦可使用個人防火牆來檢測及防止這些軟件。此外，亦有一些專門檢測間諜／廣告軟件的掃描程式，例如 Ad-Aware (www.lavasoft.de) 和 Spybot S&D (www.safer-networking.org)等。但是，用戶選用掃描程式時應謹慎從事，因爲有些間諜軟件會把自己僞裝成掃描軟件來欺騙用戶。其實，很多防毒方法亦適用於預防間諜軟件，包括：

- 不要從互聯網下載不可信或未經授權的軟件
- 不要瀏覽可疑網站
- 不要啓動來源有可疑的檔案
- 不要打開或轉發可疑的電郵，而應立即將它刪除

2.6. 病毒掃描軟件

安裝防毒掃描軟件可防範電腦被病毒入侵。每天工作前應更新病毒定義檔案，使防病毒軟件維持於最佳狀態。最少每星期進行一次電腦病毒掃瞄，而設定掃瞄時間最好在非繁忙工作時間，例如：放工時間，或午飯時間。緊記要選擇「掃瞄所有檔案」，不要只選擇性地掃瞄程式檔案。因爲很多流行的電腦病毒和蠕蟲會依附在 .EML，.VBS 和 .SHS 等檔案上。

要有效管理全公司的防毒軟件，可啓動防毒軟件「集中管理」模式。「集中管理」模式讓用戶在一台電腦上同時管理及監察所有網絡上電腦的病毒定義檔案更新、病毒掃描排程、病毒掃描報告及病毒感染狀態。

2.7. 其他防範病毒的技巧

如果用戶正在使用 Windows 2000 專業版或伺服器版本，而沒有需要網頁服務 (IIS) 時，可將它解除安裝／停止(預設是已安裝和啓動的)。因爲現時流行的蠕蟲，很多會透過 IIS 的漏洞感染其他電腦。

使用 MS Office 的文件閱讀器 (Word/ Excel/ PowerPoint Viewers) 開啓電子郵件內的辦公室文件，文件閱讀器不會執行文件內的巨集程式 (Macro) ，可以防止巨集程式病 毒。文件閱讀器可在 Microsoft 網址下載。

若有軟磁碟，光碟或從互聯網下載的外來檔案，需先用防毒軟件檢查後才開啓。

使用非法的軟件是很危險的，因爲這類型的軟件可能已含有病毒，蠕蟲或木馬程式。當用戶安裝此類型的軟件時，可能會讓有害的程式感染你的電腦系統。

3. 保安漏洞掃描軟件

每年新發現的保安漏洞數以千計，而每月發放的修正程式亦爲數不少。系統及網絡管理員對系統的潛在保安風險作出評估及管理已越來越重要。進行保安漏洞掃描，有助找出有欠妥善的服務或系統漏洞，避免問題惡化至造成破壞。

3.1. 甚麼是保安漏洞掃描軟件？

掃描保安漏洞的軟件，可就網絡或主機系統的漏洞，進行探測和分析，顯示掃描結果並提供修正方法，讓使用者得以迅速修補一些關鍵性的漏洞。

3.2. 保安漏洞掃描軟件的種類

種類	用途
網絡掃描軟件	主要就網絡的保安漏洞進行掃描，找出連接在網絡系統上的保安漏洞，例如錯誤配置的防火牆或有漏洞的互聯網伺服器
主機掃描軟件	• 直接接達主機的操作系統內部、特定服務及配置，以進行深入的掃描 • 找出用戶行爲中的潛在風險，例如找出空白或容易被猜中的密碼 • 檢查檔案系統
撥號式掃描軟件	• 撥出設定或隨機號碼，以尋找應答的調解器 • 檢查任何未經許可使用或不安全的調解器，避免它們一旦受到侵擾，會破壞防火牆的保護功能
數據庫掃描軟件	• 就數據庫系統的特許權、身份鑑定及完整性進行詳細的保安分析 • 辨認數據庫內的保安漏洞，包括簡單的密碼、錯誤的保安配置及特洛依木馬
分布式網絡掃描軟件	• 專爲評估企業網絡的保安漏洞而設計 • 由遠程掃描接口程式、接口程式的插入式更新機制和中央管理點所組成，以便從單一的位置評估分佈在各地網絡中的保安漏洞

選擇掃描軟件時，應考慮以下因素：

- 保安漏洞檢查數據庫的更新頻率
  保安漏洞掃描軟件使用數據庫來檢查保安漏洞。產銷商越頻密推出插件的最新修正版，越能提高掃描軟件探測新保安漏洞的

功能。一些掃描軟件提供了「自動更新」功能，以便定期自動下載及安裝最新修正版的插件。

- 能否準確地探測主要的系統漏洞，以及能否探測各種不同的系統漏洞，均同樣重要。較客觀的方法，是比較不同掃描軟件所能檢查出的 Common Vulnerabilities and Exposures (CVE) 的數量。CVE 是大眾公認漏洞及保安漏洞的標準名稱列表。

- 報告的水平
  掃描軟件所提供的報告，應載有清晰簡明的資料，用以修正任何被發現的漏洞。此外，軟件最好能儲存多次的掃描結果，以便互相比較。

- 掃描軟件的裝設
  這個裝設適用於網絡掃描。把掃描軟件系統裝設在防火牆的前面或背後，會產生不同的效果。通常應該進行內外掃描，以得出較全面的保安慨況。

- 掃描範圍
  部分掃描軟件已設定埠掃描範圍。系統管理員應注意這些既定的範圍設定，確保適當的埠都會被測試到。

- 設定底線
  一個良好的掃描方法會預先設定一個測試準則作爲底線。初次掃描後，必須修正發現的漏洞。然後使用第一次測試時的準則，即底線，進行第二次的掃描。這樣能確保發現的漏洞會獲得修正。掃描結果的紀錄須妥善保存，作爲日後比較及分析之用。

4. 修補程式管理

由於經常發現保安漏洞，而相應推出的修補程式也與日俱增，修補程式管理程序便成爲保障資訊系統安全的重要一環。

4.1. 計劃修補程式管理

編製及備存機構內部硬件和軟件清單

系統管理員應編製及備存一份清單，用以記錄硬件設備、軟件程式和最常用軟件程式的版本編號。這份清單有助系統管理員監控保安漏洞，以及找出適用於機構內部硬件、軟件和應用系統的修補程式。

統一配置(例如：硬件和軟件的品牌)

各主要類別的資訊科技資源，例如用戶工作站電腦和檔案伺服器等可統一配置。統一配置可簡化修補程式測試和應用程序，並可減少修補程式管理所需的人手。

教育用戶

如果沒有終端用戶的參與，修補程序不可能完善。如果用戶清楚認識資訊科技保安和修補程式管理對日常操作的重要性，並獲得足夠的培訓，懂得自行對工作站和桌上電腦進行簡單的修補，定能減輕系統管理員的工作量，提高對保安漏洞的警覺性。

4.2. 找出漏洞和適用的修補程式

系統管理員應按硬件及軟件記錄清單，經常留意資訊科技保安來源是否有發放有關的漏洞信息和修補程式。對於一些尚未有修補程式的漏洞，系統管理員應採取折衷解決方案或其他風險防範措施。 兩個主要的資料來源是：

- 供應商網站和郵寄名單
  有關特定產品的漏洞和修補程式的資料，供應商網站大抵是最可靠的來源。
- 第三者保安漏洞諮詢網站
  第三者漏洞諮詢網站可涵蓋大量產品，並可能比產品供應商更早公布最新的漏洞。這些第三者網站可提供有關漏洞的詳細資料。

4.3. 爲修補程序編定時間表和先後次序

由於資源有限，系統管理員可能需要爲修補程序編定先後次序，並進行風險評估，以判斷應優先修補的系統。系統管理員一般可根據以下元素編定先後次序：

- 保安威脅
  保安威脅是針對資訊或系統的任何潛在危機。保安威脅可以是

人爲或自然產生。經常面對較大保安威脅的系統包括網站伺服器、電郵伺服器和儲存敏感資料的伺服器。

- 漏洞
  漏洞是可能導致系統保安受破壞的薄弱環節。漏洞的特點是缺乏保障措施或保障措施薄弱以致攻擊者有機可乘。漏洞包括防火牆的開放埠、不再使用的用戶賬戶、不受限制的調解器撥號上網等。供應商會根據不同的嚴重程度（例如高、中、低）報告漏洞。

- 重要程度
  重要程度取決於系統對業務運作的重要性或價值。常被視爲對業務至關重要的系統包括郵件伺服器、數據庫伺服器和網絡基建。 所受威脅較大、漏洞較多或對業務至關重要的系統，一般在修補程式管理程序中應予以優先處理。 在編定修補工作的先後次序後，應制訂行動計劃，以便進行測試、分發修補程式、安裝修補程式、例外情況處理和報告等工作。

4.4. 測試修補程式

測試修補程式的主要目的是：
- 確定修補程式不會影響現有軟件的正常操作；
- 確保漏洞已獲預期般修復及糾正。

爲確保測試準確無誤，可按照以下步驟進行測試：
1. 檢驗修補程式的來源和完整性，以確保修補程式爲有效，而且沒有被意外竄改。
2. 對要修補的系統或類似配置的系統進行測試。
3. 檢查所有相關的軟件，以確保在安裝修補程式後軟件操作正常。
4. 檢查修補程式是否已按供應商的說明文件所載，糾正擬修補的所有檔案和配置設定。

4.5. 安裝修補程式

有關安裝修補程式，並沒有一套所有軟件和操作系統均適用的方法。修補漏洞可能涉及安裝全新版本的軟件，亦有可能只須簡單地修改配置設定。因此，修補程式管理程序往往與更改管理程序互相配合。

各操作系統和應用系統的供應商均有安裝修補程式和更新產品的獨特方法。所以，系統管理員宜細閱供應商提供的相關說明文件。

在安裝修補程式前，系統管理員還應爲應變、備份和復原制訂計劃。如果修補程式對主機產生意料之外或無法預料的影響，系統管理員便能夠及時將系統還原到安裝修補程式前的狀態。

4.6. 修補程式管理方案

市面上有各種不同的修補程式開發工具。其中一部分由產品供應商提供，另一些則由第三者供應商開發。第三者修補程式管理方案包括 BigFix Enterprise Suite 、 Ecora Patch Manager 、 HFNetChkPro、Patchlink Update、Service Pack Manager 2000 和 UpdateExpert。這些工具能夠找出各系統和網絡缺少了的修補程式，並提供部署修補程式的方法及追蹤修補程式狀態的報告，因而有助簡化修補程式管理程序。 產品供應商微軟也提供了「使用軟件更新服務（SUS）」和「使用系統管理服務器（SMS）」等修補程式管理解決方案。透過 SUS，整個網絡的電腦均能自動部署關鍵更新和即時修補程式，用戶無需開啓每一部電腦或編寫指令集。SMS 是爲微軟視窗伺服器和工作站操作系統提供配置和更改管理的企業管理工具。

5. 練習

5.1. 課堂練習

1) 黑客入侵技巧示範。
2) 建立 Windows 2003 的用戶守則。
3) Windows 2003 防火牆的設定。

5.2. 教學練習

年級：中四
課題：找出網絡安全的漏洞
學生已有知識：對電腦網絡有基本認知
教節：一節
教學目的：此節讓學生明白網絡安全的重要性。

教案內容：

步驟	教學目標	教學重點	教師活動	學生活動	時間 (分鐘)	評估
引入	學生能說出網絡安全的重要性	引起動機	教師介紹網絡安全的概念		20	
發展	學生能就不同的網絡設計及用戶特性找出漏洞	找出網絡安全的漏洞	教師示範建立 SOHO 網絡		40	學生能否就課堂上所介紹的網絡設計找出漏洞
延展活動	學生能列舉維護網絡安全的守則				10	